ISSN 2432-6089

法と情報雑誌

The Law and Information Magazine

第 8 巻第 4 号（通巻第 54 号・2023 年 12 月）

法と情報研究会　編

本 号 目 次

指令(EU) 2022/2555（NIS2 指令）

[参考訳]

2023 年 11 月 29 日
明治大学法学部教授
夏 井 高 人

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)（OJ L 333, 27.12.2022, p. 80-152）のテキスト（英語版）に基づいて和訳を試みた。

原文のテキストを入手できるサイトの URL は，下記のとおりである。

http://data.europa.eu/eli/dir/2022/2555/oj
[2023 年 10 月 31 日確認]

－解 説－

1 指令(EU) 2022/2555（NIS2 指令）について

指令(EU) 2022/2555（以下「NIS2 指令」という。）は，NIS 指令(EU) 2016/1148 (OJ L 194, 19.7.2016, p. 1)を全面改正する EU の法令である。

NIS2 指令は，2022 年 12 月 14 日に採択され，2023 年 1 月 16 日に発効した。

NIS2 指令に定める条項に定める規範内容を構成国の国内法として移植して実装する国内法化の期限は，2024 年 10 月 17 日である。

NIS2 指令に基づき構成国の国内法として移植されることにより実装された条項は，2024 年 10 月 18 日から適用される（第 41 条第 1 項参照）。

NIS 指令(EU) 2016/1148 は，2024 年 10 月 17 日の経過をもって廃止される（第 44 条参照）。

1．1 NIS2 指令における概念の混乱について

NIS2 指令には，概念と用語の混乱が多数見られる。それらの混乱の大部分は，「cyber」の語義を「cyberspace」からの転用としてではなく「cybernetics」の応用に切り替えるというパラダイム変換を断行することによって多数の解決策を見出し得る（夏井高人「アシモフの原則の終焉－ロボット法の

可能性ー」法律論叢第 89 巻第 4･5 合併号 175～212 頁参照)。

しかし，一般に，(関連分野の法学者を含め)このことの関係者の大部分は，既存の思考方法や語彙に染まってしまっていて，それらを全部自己否定しなければ始まらないような根本的な部分での発想の転換ができない。立法及び執行の関与者が，ある学説や理論を前提としなければ成立しないような経済的利益(利権)または社会的名誉と深く結びついているような場合には，特にそうである。
そのため，NIS2 指令に含まれている本質的な問題は，これからも未解決のままで残されることになるであろう。

NIS2 指令の法解釈の過程において，本質的な問題の解決が無理である以上，この参考訳の解説の中で本質的な問題を解決するための何らかの提案をしても無意味である。

そこで，この解説では，NIS2 指令の中にある混乱及び問題点の中でも「cyber」という語を用いているために発生している混乱の一部を指摘し，その検討結果の一部を開示し，そして，この参考訳を作成する上で検討した諸点に関して簡単に解説するのにとどめることにする。

1. 1. 1 NIS2 指令における「サイバーな脅威」について

NIS2 指令で使用されている法概念の中で最も多くの問題を含む法概念は，「cyber threats」である。

この法概念を理解するための大前提として，「cyber threats」及び「threat」の両者を含め，EU における情報セキュリティ行政の中枢機関である ENISA が「threat」の概念をどのように理解しているのかを知ることが重要である。それを知ることのできる最も良い最新の資料は，下記の資料である。
この資料の中で触れられている全項目から帰納法によって推論すれば，ENISA によって理解されているものとして「cyber threats」及び「threat」の概念それ自体の内容及び構造を把握できる。

> ENISA Threat Landscape 2023
> October 19, 2023
> https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
> [2023 年 11 月 15 日確認]

ENISA による理解を一応離れ，NIS2 指令の前文及び条項それ自体を観察してみると，「cyber threats」に関し，NIS2 指令の第 6 条第 10 号は，「規則(EU) 2019/881 の第 2 条第 8 号に定義するサイバーな脅威のことを意味」すると規定している。
NIS2 指令の第 6 条第 10 号が参照している規則(EU) 2019/881 (OJ L 151, 7.6.2019, p.15-69)の第 2 条第 8 号は，「ネットワーク及び情報システムに対し，そのようなシステムの利用者に対し及びそれ以外の者に対し損害，混乱またはそれ以外の負の影響を与え得る潜在的な状況，出来事または行動のことを意味(‘cyber threat’ means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and

other persons）」すると定義している。

つまり，NIS2 指令では，「cyber threat」または「cyber threats」という語が用いられる場合，一般用語としての「cyber」という属性をもつ脅威の全てを法適用の対象としているのではなく，「threat」の対象を「ネットワーク及び情報システム」に関して生じた脅威並びに「そのようなシステムの利用者及びそれ以外の者」に関して生じた脅威だけに限定し，非常に狭い意味で用いられていることになる。

NIS2 指令の第 6 条第 10 号におけるこのような限定があるため，例えば，現時点においては最も深刻な脅威であり得る M2M（Machine to Machine）の通信プロセスや自律的に機能する Cyber physical objects と関係するサイバー攻撃の脅威は，それが「ネットワーク及び情報システム」の一部であるか，または，「ネットワーク及び情報システム」との間で直接に通信するものであるかのいずれかに該当しない限り，原則として，NIS2 指令に定義する「cyber threat」の中には包摂されていないと考えられる。
これらの M2M や Cyber physical objects を攻撃対象とするサイバー攻撃は，それ自体としては，例外的な場合を除き，原則として，製造物責任及び機械装置に適用される EU 及び構成国の法令に基づき，それらの事項を所管する職務権限のある機関の監督に服することになると考えられる。そのような機関は，基本的には，ENISA ではない。

「cyber threat」または「cyber threats」の定義と関係してこのような結果となっているのは，ENISA の職務権限の中で，その法律上の根拠を NIS2 指令（または廃止された NIS 指令(EU) 2016/1148）とする職務権限に関し，規則(EU) 2019/881 と NIS2 指令との間で ENISA 及び関連する職務権限のある機関の職務権限の性質・範囲を整合性のとれたものにしようとする立法上の意図から生じたものと推定される。

ところが，NIS2 指令の第 6 条第 10 号（規則(EU) 2019/881 の第 2 条第 8 号）によって定義された「cyber threats」の語義は，一般的な用語としての「cyber threats」から受ける語感とは相当に異なるものなので，「cyber threats」に関しては，NIS2 指令の適用範囲を不合理に狭めていることになるという自己矛盾を抱えていることともなり得る。

通常，一般的な用語としての「cyber threats」という語は，ネットワーク及び情報システムとその利用者等に限定されず，もっと広い意味で使用されている。

このことが，NIS2 指令の中にある「cyber threats」の用語上の混乱の根源的な原因となっていると考えられる。
特に，ENISA との関係や条文上の定義を一応措いて，NIS2 指令中の関連条文や前文等を文それ自体として理解しようとする場合，かなり大きな混乱を生じさせ得ることともなっている。

以下，「cyber threats」の用法と関連する問題点に関し，より具体的に述べる。

まず，NIS2 指令の第 7 条第 1 項(g)及び第 13 条第 5 項のそれぞれの文の構造及び表現は，

「cyber threats」の定義と関連して伏在している法解釈上の問題を顕在化させるものとなっている。

NIS2 指令の第 7 条第 1 項(g)の英語版は，「on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents」となっている。

この文は，一見すると，特に問題があるようには読めないかもしれない。

しかし，NIS2 指令の第 7 条第 1 項(g)のドイツ語版を調べてみると，「über Risiken, Bedrohungen und Sicherheitsvorfälle sowie über nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle」となっており，英語版とは異なる意味内容を示している。
このドイツ語版の文を英語の文に直訳すると，「on risks, threats and incidents as well as on non-cyber risks, threats and incidents」となる。直訳ではなく，「Risiken, Bedrohungen und Sicherheitsvorfälle」が「nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle」した残余のものを意味すると論理解釈した場合，すなわち，「cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle」を黙示で意味する文であると解することができるとすれば，そのような論理解釈を経た後の「über Risiken, Bedrohungen und Sicherheitsvorfälle sowie über nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle」の英語文による意訳は，「on cyber risks, threats and incidents as well as on non-cyber risks, threats and incidents」となる。
NIS2 指令の第 7 条第 1 項(g)のフランス語版は，「aux risques, aux menaces et aux incidents dans les domaines cyber et non cyber」であり，その意味内容を英語文で表現すると，「on cyber risks, threats and incidents in cyber domain as well as on risks, threats and incidents in non-cyber domain」または「on cyber risks, threats and incidents as well as on non-cyber risks, threats and incidents」となる。
適用対象がネットワーク及び情報システムに限定されているという「cyber threats」の定義を一応措いた文それ自体の論理性の評価としては，フランス語版の文が最も正しく，完全であると言える。

ところで，各構成国は，それぞれの国の版の条項に従って NIS2 指令を実装（国内法化）することになるので，NIS2 指令の第 7 条第 1 項(g)に関する限り，立法の時点で既に，構成国法の整合化（harmonisation）とは反対の方向で各国の対応国内法が立法されることが予定されていると言える。
他方，NIS2 指令の第 7 条第 1 項(g)の英語版の「on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents」の論理構造を文それ自体として考察してみると，単純に対照した場合には，「as well as」の前後で，「risks」と「non-cyber risks」，「cyber threats」と「threats」，「incidents」と「incidents」がそれぞれ対応している文のように見える。このこと自体が（「incidents」が重複していることになる点，「non-cyber risks」と「risks」とが同義であるとすれば，「risks」も重複していることになる点を含め）非論理的であることは言うまでもないことなので，このような単純な対照による形式的な法解釈ではなく，論理性を重視した合理的な法解釈を行う必要がある。

そして，形式的な法解釈による論理的な破綻を避けて唯一成立可能な合理的な解釈は，「as well as」の前後で，「cyber risks, threats, and incidents (=cyber (risks, threats, and incidents))」と「non-cyber risks, threats, and incidents (=non-cyber (risks, threats, and incidents))」が対比して表現されているという解釈，または，この文の大部分が誤記であり，かつ，「non-cyber risks」と「risks」とが同義であると仮

定した上で，「on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents」は「on risks, threats, including cyber threats, and incidents」を意味するという解釈だけである。
加えて，そのように解する場合，「cyber threats」に関し，NIS2 指令の第 6 条第 10 号（規則(EU) 2019/881 の第 2 条第 8 号）によって限定された意味をもつものではない一般的な語義をもつ語として「cyber threats」が用いられていると解するのが最も正当である。しかし，「cyber threats」に関し，NIS2 指令の第 6 条第 10 号（規則(EU) 2019/881 の第 2 条第 8 号）の定義の適用を重視するとすれば，「cyber risks, threats, and incidents (=cyber (risks, threats, and incidents)) with exception of threats to which any systems other than the network and information systems」というような意味をもつ文であると解するしかない。

このような論理解釈としての法解釈上の問題を避けるためには，文の中で「cyber threats」が登場しないように表現すべきであるので，「cyber threat」に関する NIS2 指令の第 6 条第 10 号（規則(EU) 2019/881 の第 2 条第 8 号）の定義の適用を排除するという意味で「cyber risks, threats, and incidents as well as non-cyber risks, threats, and incidents」で十分ではないかと考えられる。
しかし，ここでも NIS2 指令の第 6 条第 10 号（規則(EU) 2019/881 の第 2 条第 8 号）の定義が排除されず，同定義を適用しなければならないという解釈は成立可能の範囲内にある。

そこで，その適用を完全に排除しようとするのであれば，別途，読み替え条項等を定めておくか，そもそも定義条項の中で例外処理条項を組み込んでおくというやり方が明確性の目的に最も奉仕するやり方だったのではないかと考えられる。

更に，この問題と直接に関連する法令である指令(EU) 2022/2557（OJ L 333, 27.12.2022, p. 164-198）の第 4 条第 2 項第 1 副項(g)では，情報共有の対象となる情報の種類に関し，「on cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents」と定められており，その実質的意味は，「on cyber risks, threats and incidents as well as on non-cyber risks, threats and incidents」と均等（equivalent）となる。
そして，同指令の第 4 条第 2 項第 1 副項(g)においてもまた，フランス語版は，「sur les risques, menaces et incidents en matière de cybersécurité ainsi que sur les risques, menaces et incidents non liés à la cybersécurité」となっており，実質的にみて「on cyber risks, threats and incidents as well as on non-cyber risks, threats and incidents」と均等な文である。
なお，このフランス語版の文を英語で直訳するとすれば「on cybersecurity risks, threats and incidents as well as non-cybersecurity risks, threats and incidents」となる。
他方，同指令の同条同項同副項(g)は，ドイツ語版では「über Cybersicherheitsrisiken, Cyberbedrohungen und Cybersicherheitsvorfälle und über nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle」となっており，実質的にみて「on cyber risks, threats and incidents as well as on non-cyber risks, threats and incidents」と均等な文である。

加えて，指令(EU) 2022/2557 の前文(38)の中では，「a comprehensive framework for cyber and non-cyber resilience of critical entities」との表現が用いられており，（厳格な定義条項の存否は一応措いた上で）立法者の脳裡においては，「cyber」と「non-cyber」とが対比された構図でものごとがとらえら

れているということを知ることができる。

NIS2 指令の第 7 条第 1 項(g)の法解釈と関連して以上に述べたことと全く同じ問題は，NIS2 指令の第 13 条第 5 項にもある。

NIS2 指令の第 13 条第 5 項のドイツ語版における表現は，「zu Risiken, Cyberbedrohungen und Sicherheitsvorfällen sowie zu nicht cyberbezogenen Risiken, Bedrohungen und Sicherheitsvorfällen」となっており，また，フランス語版の表現は「les risques, les cybermenaces et les incidents, ainsi que sur les risques, menaces et incidents non cyber」となっており，意味的に英語版と同じであるので，どちらの版も非論理的で無効な条項であることを示していると言える。

NIS2 指令の条文だけを法解釈の対象とするとすれば，ここで述べたような事柄は，かなり致命的なものであると言い得る。
しかし，NIS2 指令とペアになった法令として実装・適用される指令(EU) 2022/2557 の第 2 条第 2 項第 2 文は，「必須法主体の物理的な防護とサイバーセキュリティとの間の関係に照らし，構成国は，この指令及び指令(EU) 2022/2555 が調整された態様で実装されることを確保する（In light of the relationship between the physical security and cybersecurity of critical entities, Member States shall ensure that this Directive and Directive (EU) 2022/2555 are implemented in a coordinated manner）」と定めている。すなわち，これら 2 つの指令は，各構成国における実装の段階で，矛盾がないように調整される。
その結果，ここで問題にした NIS2 指令の第 7 条第 1 項(g)及び第 13 条第 5 項を移植して実装する構成国の国内法の条項が，整合化されない可能性があることが，指令(EU) 2022/2557 の第 2 条第 2 項第 2 文によって予定されているとも解釈され得る。

1．1．2 NIS2 指令における「インシデント」の概念について

NIS2 指令において用いられている「risks」と「incidents」に関し，単純に法解釈すると，NIS2 指令の第 7 条第 1 項(g)及び第 13 条第 5 項に重複の問題が称すること，「non-cyber risks」が独立した熟語であるとすればこの語の定義が存在しないために「risks」と「non-cyber risks」を同義と解することになり，その結果として，「risks」にも重複があることは既述のとおりである。

このような形式面の問題を一応措くとしても，NIS2 指令の中で用いられている「risks」と「incidents」の概念内容に関しては，詳密に再検討する必要があると考えられる。

例えば，NIS2 指令の中で使用されている「incidents」の概念が「cyber incidents」と「non-cyber incidents」の両者を包摂していると解すべきであるか，それとも，「incidents = non-cyber incidents」と解すべきであるかは，一つの問題である。
NIS2 指令の立法者にはこの点に関する問題意識が存在しなかったか，または，明瞭ではなかった可能性が高い。そのことが，「incidents」の概念に関しても問題を生じさせていると考えられる。

以上に述べたことは，「incidents」の概念に関してだけではなく「risks」の概念に関してもそのまま妥当すると考えられる。

1．1．3 NIS2 指令における「リスク」の概念について

指令(EU) 2022/2557 の前文(9)では，NIS2 指令で用いられている概念を指すものとして「cyber risks」との語が使用されている。
しかし，実際には，NIS2 指令の中では「cyber risks」との語が使用されていない（上述の NIS2 指令の第 7 条第 1 項(g)に関する解説部分参照）。

このことから，指令(EU) 2022/2557 と NIS2 指令との間で，「risks」及び「cyber risks」の概念の内容理解及び論理構造に関してもまた，重大な齟齬が存在することが明らかとなっていると言える。

なお，リスクの中には，自然災害のような非人為的なリスクとサイバー攻撃のような人為的なリスクが含まれる。
そして，人為的なリスクの中には，ハイブリッドな脅威（hybrid threats）または敵対的な脅威（antagonistic threats）と関連するものも含まれる。
これらのハイブリッドな脅威または敵対的な脅威と関するリスクのような構成国の国家安全保障及び国防と深く関係する人為的なリスクは，指令(EU) 2022/2557 の中で定められている構成国リスク評価の過程で調査・検討の対象とされる。

1．2 AI システムに起因するインシデントと関連する問題

一般に，完全に自律的であり，いかなる人間による制御にも服さない AI システムが存在し，かつ，人間による制御に服さずに自律的に稼働していることが特定の脅威の根本原因（root cause）として存在している場合，当該 AI システムは，（人間による制御が不可能である以上）マネジメントシステムによる管理（control）の適用対象外となるので，ICT プロセスのマネジメントによる管理の適用対象外であり，また，一般的な意味におけるリスク管理及びインシデント管理との関係においても適用対象外となる。
つまり，そのような完全に自律的な AI システムは，非人為的な自然災害の一種として理解されるべきであるので，所定の要件を満たす限り，そのような完全に自律的な AI システムからの脅威を避けるために当該 AI システムを破壊する行為は，その行為者が誰であるにしても，原則として，世界各国の基本的な法原則によって承認されている緊急避難行為となり，当該 AI システムを破壊する行為の違法性が阻却される。
なお，未来の時点において当該完全に自律的な AI システムに関し，関連法令によって法人格が認められているときは，そのような法人格をもつ自律的な AI システムからの攻撃的なふるまいに対する防衛行為は，世界各国の基本的な法原則によって承認されている（「人」からの攻撃に対する）正当防衛となり，当該 AI システムを破壊する行為の違法性が阻却され得ると解されることになるであろう。

しかしながら，そのようなタイプの AI システムによる脅威が緊急避難行為（または未来において法人格が認められれば正当防衛行為）として即座に対処できない法的性質のものであるときは，本質的にはサイバネティクス（cybernetics = automaton）という意味でのサイバーで深刻な脅威でありながら，EU の NIS2 指令の条項の適用との関係においては，（法的には，人為的なものではない自然災害と全く同じ扱いになるという意味で）非サイバーな脅威（non-cyber threats）として分類されるべきであろう。

NIS2 指令においては，前文の中で，サイバーセキュリティのための「人工知能（AI）」の技術の応用及びそれに伴う個人データ保護に関して言及されている。
しかし，AI システムの存在が防護との関係においてリスクまたはインシデントとなる可能性に関する言及はない。
サイバーセキュリティのために導入される生成 AI のシステムの制御が仮想敵の工作員等によって奪われ，自然人に対する洗脳と同様の意図的に歪められた学習処理が実行され，仮想敵のためのサイバー攻撃のための手段として利用され得るという脆弱性要素と関連するリスクまたは「man-in-AI」とでも表現すべきようなタイプのサイバー攻撃のリスクは，現に存在する。ChatGPT のような生成 AI 応用技術がサービスとして提供されるネット環境を含め，人間にとって疑似意味論（pseudo-semantics）を含むような態様で AI 応用技術が使用される場面では，常に存在している。
しかし，NIS2 指令の中ではそのことへの言及はない。

要するに，NIS2 指令は，基本的に，AI のような最も肝心な現代的脅威に全く対応しておらず，いまだに大型電子計算機を中心とする前時代的な発想を基礎として立法された法令であると評価すべきであり，そのような法令として NIS2 指令の個々の条項を解釈すべきである。

AI と関連する諸問題の中には，一般に「サイバーな問題」の一種として理解されている問題でありながら，「cyberspace」とは無関係の孤立した存在と関連するものが無数に含まれている。

それゆえ，「cyber」の概念は，「cyberspace」から派生する概念として限定的に理解されるべきではなく，インターネットのようなサイバー空間もまた多種多様で自律的な無数のフィードバックの集合体という意味でのサイバネティクスの一種であると理解し，より広い対象を含む概念空間を想定した上で，「cyber」の概念を「cybernetics」から派生する語として定義し直すべきである。

そして，EU における今後の課題としても，「cyber」の概念を「cyberspace」からの派生ではなく「cybernetics」からの派生として広くとらえた上で，NIS2 指令の基本骨格を全部置き換えるような全面改正が早急に検討されるべきである。

1．3 個人データ保護及び非個人データと個人データが混在する場合の処理との関係

非個人データ（non-personal data）に関しては，個人データと非個人データとが混在する場合を含め，規則(EU)2022/868（データ統治法）（OJ L 152, 3.6.2022, p. 1-44）の中で関連する事項が詳細に定められている。何が問題であるのかを正確に理解する必要がある。

特に，匿名化された個人データであっても複数のデータを関連づけることによって個人識別性を回復することがあり得るという意味で，匿名化されたデータであっても（個人識別性のある）個人データと同じ扱いをすべき場合があるという点は極めて重要である。

情報セキュリティの場合，暗号化された個人データ，匿名化された個人データ及び仮名化された個人データを含め，一般的には個人識別性がないように見えるデータであっても精密な分析と論理解釈によって個人識別性要素を発見し，サイバー攻撃の主体である個人または個人の集団（AI が自律的な攻撃主体となっている場合にはシステムもしくはアプリケーションまたはそれらの集団）を特定することが，（潜在的な被疑者を発見し，特定するという捜査機関の通常の犯罪捜査活動と同様に）サイバー防護のための非常に重要な仕事となっているので，潜在的な個人データ及び（暗号化された個人データ，匿名化された個人データ及び仮名化された個人データから）個人識別力が復元されたデータを処理する際の GDPR（規則(EU) 2016/679）の適用が問題となり得る。

この点に関し，NIS2 指令を基礎とするサイバーセキュリティのための業務遂行は，個人データ保護のための法令を遵守して実施されるべきことが明記されている（前文(92)及び前文(106)参照）。NIS2 指令の第 2 条第 12 項は，NIS2 指令が指令 2002/58/EC，指令 2011/93/EU27 及び指令 2013/40/EU28 並びに指令(EU) 2022/2557 の適用を妨げないことを定めており，また，NIS2 指令の第 2 条第 14 項は，「法主体，職務権限のある機関，単一連絡部局及び CSIRT」に関し，GDPR に準拠して業務遂行すべきことを定めている。前文(14)にもその旨の記述がある。

このことは，サイバーセキュリティのための業務遂行中に個人データ保護のための監督業務が競合的に発生してしまった場合，当然のことながら，混乱が発生することがあり得る。それゆえ，そのような場合における調整のための条項が必要になる。

ところが，GDPR に定める個人データ保護のための監督機関の権限との調整が実行される具体的な場面に関しては，NIS2 指令の第 35 条に定める場合を除き，必ずしも明確ではない。NIS2 指令の第 35 条は，個人データの侵害を伴う違反行為の場合に関して，やや詳細に定めている。
他には第 31 条第 3 項に NIS2 指令に基づいて権限を行使する職務権限のある機関が GDPR に定める個人データ保護のための監督機関と協力して監督の措置及び執行の措置を実施すべきことを定める条項があるだけである（前文(108)参照）。

以上を踏まえた上で，EU の個人データ保護監督機関の権限との優先関係及びそのような機関との協力と関連する点に関し，実際に適用される条項は，NIS2 指令に定める条項それ自体ではなく，構成国の国内法制の中に移植され，実装された国内法令の条項なので，当然のことながら，各構成国の国家体制や行政組織の構造を反映して，異なる制度や仕組みが多数併存することになると予想される。
それゆえ，この点に関しては，NIS2 の条項を読んでいるだけでは何も解決できず，全ての構成国の個人データ保護法制と NIS2 指令の関連条項の実装法令を精密に調べ，共通点と相違点を見出すために精密に比較検討するという作業が必須になる。

GDPR は，EU の規則なので，GDPR の仕組みそれ自体を理解するためには GDPR に定める条項を理解するだけで足りるのであるが，EU 及び構成国の他の機関の権限との調整に関しては，EU 法全部及び関連する構成国の国内法中の関連する条項の少なくとも主要部分を一応理解している必要性があり，そのような調査と検討の作業を経ていない場合，GDPR の運用に関して十分に理解できていないということになるだろう。

一般に，EU 法に関しては，EU に存在する法規範（制定法及び判例法）の全体を可能な限り漏れなく知るための努力を尽くし，かつ，全体像としての EU 法の構造解析と EU 法の構成要素となっている EU の個々の法令と構成国の関連国内法及び EU の判例法の細密な調査・検討の努力を継続的に重ねている研究者だけが「EU 法の研究者」である。

なお，日本国においては，個人情報保護法に定める個人情報保護委員会の権限が，NIS2 指令が要求するような「協力」と関連する業務を遂行するための権限を含んでいるとは解されない。
仮に自由裁量によりそれが可能であると解するとしても，現在の個人情報保護委員会には，（「State sponsored attack」のような軍事上のサイバー攻撃の場合には特に）情報セキュリティのための高度に専門的な業務を遂行するため，または，そのような事柄を精密かつ正確に理解し，妥当な判断を形成するための権限，人的・物的資源及び関連予算が存在しない。

それゆえ，日本国においては，現行の個人情報保護法を全面改正し，かつ，必要な予算及び人的資源の確保が実施されない限り，現状を打開することは不可能であると考えられる。

1．4 NIS2 指令の別紙Ⅱにおける NACE Rev. 2 の参照

NIS2 指令の別紙Ⅱでは，NIS2 指令に定める重要法主体（important entities）を識別するための基準として NICE Rev.2 を参照するだけの箇所があるので，少なくともそのような箇所に関しては，NACE Rev.2 の該当項目を調べ，その適用範囲を理解する必要がある。

NIS2 指令の別紙IIの中で参照されているのは，NACE Rev.2 の Division 21 及び Division 26 ないし Division 30 である。

NACE Rev.2 は，規則(EC) No 1893/2006（OJ L 393, 30.12.2006, p. 1-39）によって定められている。NICE Rev.2 の公式解説書は，下記のところで入手できる。

> NICE Rev.2: Statistical classification of economic activities in the European Community
> https://ec.europa.eu/eurostat/documents/3859598/5902521/KS-RA-07-015-EN.PDF
> [2023 年 11 月 17 日確認]

NACE Rev.2 の Division 21 及び Division 26 ないし Division 30 の項目名によって示される産業類型は，NIS2 指令の別紙Ⅰ及び別紙Ⅱによって分類される産業類型をより具体的に類別可能にするものであり，一定の有用性をもつ。

しかし，NACE Rev.2 の Division 21 及び Division 26 ないし Division 30 の項目名によって示される産業類型は，あくまでも観念的な類型の名称（符号列）に過ぎない。
実際には，現実に存在する個々の企業等が，それらの名称（符号列）によって表現されているどの類型の企業または事業体に属するかの当てはめという識別（identification）の作業を経る必要性がある。

また，そのような類型毎の一般的なリスク評価や個々の企業等の個別のリスク評価が行われなければ，脅威やリスクに対する対応策を具体的に検討することができず，また，想定されるインシデントや現実に発生しているインシデントからの復旧のための回復力を増強するための方策を検討することもできない。

１．５ NIS2 指令における基礎法主体（必須法主体）のあてはめ

現実に存在する個々の企業等の中で NIS2 指令における基礎法主体（＝指令(EU) 2022/2557 における必須法主体）が NIS2 指令の別紙Iによって示される産業類型によって分類される産業類型のどれに該当するかを判別するための構成国による識別に関しては，NIS2 指令ではなく，指令(EU) 2022/2557 の中で定められている。
また，このような産業類型（部門及び副部門）に対応して実施される構成国リスク評価に関しても，NIS2 指令ではなく，指令(EU) 2022/2557 の中で関連条項が定められている。

NIS2 指令における基礎法主体（＝指令(EU) 2022/2557 における必須法主体）の類型は，NIS 指令では別紙Ⅰの中で示され，指令(EU) 2022/2557 の中では別紙の中で示されている。これらの別紙を比較対照して検討してみると，概ね同一の内容となってはいるが，細部においては異なっている。例えば，NIS2 指令では基礎法主体（essential entity）ではなく重要法主体（important entity）の類型を示す別紙Ⅱに入れられている食品製造業・食品加工業の法主体が，指令(EU) 2022/2557 の中では別紙の中に入れられ，必須法主体（critical entity）として扱われている。
別紙の記載は，些細なことのように思われるかもしれないが，法適用の対象となる企業等を識別するための極めて重要な識別子（identifier）の集合体なので，決して軽視してはならない。

これらの諸点に関し，企業の実務においては，NIS2 指令を実装する各構成国の国内法に定める条項の現実の適用を知るためには，NIS2 指令を理解する前に，指令(EU) 2022/2557 を理解することが不可欠である。

そして，企業の実務においては，指令(EU) 2022/2557 を実装する各構成国の国内法に定める条項とその運用のための細則等を精密に調査・理解する必要がある。
指令(EU) 2022/2557 によって，NIS2 指令における基礎法主体（＝指令(EU) 2022/2557 における必須法主体）の識別基準の骨格部分が整合化されるが，NIS2 指令及び指令(EU) 2022/2557 は，ミニマムな整合化（minimum harmonisation）のための最低基準を定めるだけであるので，欧州連合内において完全に画一的に同一の識別基準が適用されることにはならない（NIS2 指令の第 5 条及び指令(EU) 2022/2557 の第 3 条参照）。

しかも，現在の世界の厳しい状況を前提に考えると，法主体の識別基準に関しても，各構成国における実際の運用，監督及び執行に関しても，更に大きな変化や修正が生ずる可能性がないとは言えない。

それゆえ，ある時点の観察結果だけに基づき，固定的な判断基準または不動の判断基準が存在すると想定して政策判断や経営判断等を行うことは，極めて危険なことである。

また，学術の側面においてだけではなく，日本国の経済政策及び産業政策の側面においても，そして，日本国の個々の企業等の法令遵守，デューディリジェンス及び情報セキュリティの側面においても，当該の国が少なくとも日本国の企業の主要な取引相手国である限り，欧州連合を構成している個々の構成国の国内法を個別に理解するための精密な調査研究を今後もずっと継続する必要がある。

以上を踏まえた上で，日本国の企業の中で NIS2 指令における基礎法主体（＝指令(EU) 2022/2557 における必須法主体）及び NIS2 指令における重要法主体に包摂され得る類型の企業等を想定してみると，日本国の主要産業のかなり多数が，既に，潜在的に NIS2 指令の適用を受けているということを理解できるであろう。

より具体的には，EU からみて第三国である日本国内に主たる拠点のある日本企業は，例えば，NIS2 指令の第 26 条第 3 項及び第 27 条第 2 項を移植して実装した構成国の国内法に基づき，NIS2 指令が定めるような監督の措置と執行の措置を受け，かつ，報告の義務を負うことになる。

1．6 NIS2 指令の原文中にある誤記等の問題

NIS2 指令の原文（英語版）には（空白や句読点等の誤記等を含め）明らかな誤りが見られる。不完全な文なのではないかと疑われる箇所も存在する。

それらが訂正されるべき誤記等に該当すると欧州委員会が判断する場合，所定の手続を経て EU 官報上で公表されるその正誤表（corrigendum）によっていずれ訂正されることになると予想されるが，Eur-lex 上で 2023 年 11 月 27 日の時点において確認できた範囲内では，NIS2 指令の原文（英語版）に適用される正誤表は公表されていない。

そのため，この参考訳においては，誤記等のある箇所に関し，適宜意訳し，または，意識的に原文のままで訳出することにしたが，特に留意すべき点に関しては，「参考訳作成において留意した事項」の項で個別に指摘することにした。

2. 参考訳作成における基本方針

この参考訳においては，NIS2 指令の前文（recital），条文（articles）及び別紙（Annex）の全文を訳出した。

この参考訳においては対訳方式を採用することにした。ただし，原文を表示することが無意味な部分（特に脚注内）に関しては，原文または訳文の表示を省略した。

この参考訳は，あくまでも NIS2 指令の私的な和訳である。公式訳でも確定訳でもない。

この参考訳は，現時点における研究成果を反映するものである。将来，更に研究を深めた結果として修正すべき部分を発見したときは，その時点において，改訂版等を作成すべきかどうかを検討する。

参考訳の訳出に際しては原則として直訳とすることとしたが，直訳のままでは日本語になりにくい箇所に関しては，やむを得ず意訳とした。

この参考訳に訳注はない。参考訳中にある脚注は，全て原注である。訳注等による個別の説明がなければ当該箇所の訳出の理由がわかりにくいと想定される箇所に関しては，必要に応じて，「参考訳作成において留意した事項」の中で説明を加えることにした。

読みやすさを重視し，条文中の号(point)の表記を一部省略した。例えば，「point(a)」は「第(a)号」であるが，「第」と「号」を省略し，「(a)」と表記することにした。

この参考訳は，Eur-lex のデータ二次利用条件を遵守して作成した。

3. 参考訳作成において留意した事項

この参考訳は NIS2 指令の注釈書ではないので，それらの箇所の全てを指摘することは避け，必要に応じて合理的に解釈した上で訳文を作成することにした。

ここでは，特に説明を加えないと誤訳ではないかと誤解される危険性がある箇所を中心にして，この参考訳作成において留意した事項を摘記する。

＊＊＊

上述のとおり，NIS2 指令の第 7 条第 1 項(g)及び第 13 条第 5 項にはかなり深刻な問題がある。
結論として，NIS2 指令の前文(30)の中にある「risks, cyber threats, and incidents」との箇所は，「cyber risks, threats and incidents」の誤記である。
同様に，NIS2 指令の第 7 条第 1 項(g)は，「on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents」と定めている。この箇所もまた，集合論及び意味論のいずれから検討してみても，明らかに誤記である。正しい文は，「on cyber risks, threats and incidents as well as on non-cyber risks, threats and incidents」である。
NIS2 指令の前文(30)及び第 7 条第 1 項(g)は，「cyber risks, threats and incidents」と「non-cyber risks, threats and incidents」とが対になった概念として存在していると理解可能な文とするのが正しい。
更に，NIS2 指令の第 13 条第 5 項にも同様の誤りがある。
この参考訳においては，NIS2 指令の前文(30)，第 7 条第 1 項(g)及び第 13 条第 5 項のいずれに関しても，上述の NIS2 指令の第 7 条第 1 項(g)のフランス語版を底本として採用することにし，合理的に解釈した上で訳出することにした。
ただし，形式的には原文とは異なる内容のものとして理解した内容を訳出していることになるので，該当箇所の文字を灰色で表示し，識別できるようにした。

NIS2 指令の前文(45)の第 2 文の中にある「with the national computer security incident response teams or competent authorities of third countries」との箇所は，「with the computer security incident response teams or competent authorities of third countries」または「with the domestic computer security incident response teams or competent authorities of third countries」の誤記と解される。
EU 法においては，通常，「national」は，EU の機関及び組織等との関係において主権国家である構成国の国内機関及び国内組織等であることを示すために使用される。
当該第三国が連邦国家または国家連合であるような場合を除き，第三国の国内組織であることを示す場合には「domestic」を使用するか，「national」を使用しない文とするように工夫するかのいずれかである。
そもそも，連邦国家や国家連合のような場合を除き，特定の国の国家機関以外には国家機関が存在しないのが当然のことなので，（少なくとも論理的には）当該国の国家主権に服さない国家機関と識別するために「national」という概念を用いる必要性が全くない。
他方において，連邦制をとる国家の部分国家（アメリカ合衆国の場合には州）の中には，当該国の機関と連邦の機関とが併存するのが普通である。例えば，アメリカ合衆国の州の中には，連邦裁

判所（連邦巡回区控訴裁判所など）と州裁判所とが併存しているところがあり，また，連邦軍の施設と州軍の施設が併存しているところがある。しかし，例えば，単立の国であって，いかなる連邦国家にも国家連合にも属さない国においては，当該国の機関しか存在しない。
そのように当該国の機関しか存在しないときは識別の必要がないので，「national」という概念も不要となる。逆に，そのような単立の国家であるにも拘わらず「national」ではない統治機関が併存し得ることを含意する「national」の概念を使用することは，国際政治の観点からすれば，当該単立の国の国家主権を否定または軽視することともなり得る極めて失礼な態度であるとの批判を招きかねない。
これと同じ問題は，第 10 条第 7 項及び第 8 項の「third countries' national computer security incident response teams」に見られる。この場合の「national」は，全て誤記である。
この参考訳においては，以上のように解した上で，NIS2 指令の前文(45)と第 10 条第 7 項及び第 8 項を適宜意訳することにした。
ただし，形式的には原文とは異なる内容のものとして理解した内容を訳出していることになるので，該当箇所の文字を灰色で表示し，識別できるようにした。

NIS2 指令の前文(76)の第 1 文中にある「the operational capabilities of the CSIRTs」との箇所は，「the level of operational capabilities of the CSIRTs」の誤記の一種と考えられる。
ただし，この参考訳においては，原文のまま訳出することにした。

NIS2 指令の(78)の第 3 文中にある「systemic analysis」との箇所は，「systematic analysis」の誤記である可能性が高い。
ただし，この参考訳においては，原文のまま「systemic analysis」を「システミック分析」と訳出することにした。
この箇所を「systematic analysis」の誤記であると解釈した上で合理的に訳出するときは，「体系的な分析」という訳になる。
NIS2 指令の(78)の第 3 文中にある「taking into account the human factor」の「the human factor」の中には，例えば，SNS 等を介した偽情報（fake information）の大規模な流布・伝達等の行為も含まれると解される。
なお，NIS2 指令の条文中では，「systemic」との語は，第 2 条第 2 項(d)において「disruption of the service provided by the entity could induce a significant systemic risk」として使用されているだけである。この第 2 条第 2 項(d)における「systemic risk」の用例と同じ意味をもつ用例としての「systemic risk」に関しては，主として，規則(EU)2022/2065（デジタルサービス法）（OJ L 277, 27.10.2022, p. 1-102）の中に多数の関連条項が含まれている。

NIS2 指令の前文(84)及び第 21 条第 5 項の中にある「managed security service providers, providers of online market places」との箇所は，誤記による不完全な文であると思われる。正しい文は，「managed security service providers, as well as providers of online marketplaces」である。
この参考訳においては，いずれの箇所に関しても原文のまま訳出することにした。

NIS2 指令の前文(95)の第 1 文の「thereby building on the knowledge and skills already acquired under

Directive (EU) 2018/1972」との部分は，要するに，NIS2 指令の関連条項を構成国の国内法として移植して国内法化する際，欧州電子通信法指令(EU) 2018/1972 の関連条項を構成国の国内法として移植して国内法化された際に得られた実装のための知識・経験・技能等を基礎とすべきであり，そのために，欧州電子通信法指令(EU) 2018/1972 の実装の際に各構成国において採択された運用指針等を参考にすべきことが述べられている。
意味内容としてはそのようなことを述べる文であり，そのように補って意訳することも検討したが，結論として，直訳とすることにした。そのため，この参考訳の訳文のままでは非常にわかりにくい面がある。

NIS2 指令の前文(96)の第 2 文は，不完全な文であると解される。この参考訳においては，合理的に解釈した上で，意訳することにした。
NIS2 指令の前文(96)の第 3 文の「increasing the likelihood of incidents involving the exploitation of personal data, and, by extension, the security of network and information systems」との箇所は，不完全な文である可能性もあるが，合理的に解釈するとすれば，その趣旨としては，（フィッシングの場合を含め）ある種のサイバー攻撃において，被害者を偽サイトへ誘導して入力させるなどして入手した個人データ（二段階認証のための電話番号や個人識別コードや顔画像等の生体要素など）を濫用し，その個人データをクレデンシティアルとする別のサイトへの無権限アクセスを実行し，更に関連データを濫用することにより，完全ななりすましに成功すると，より重要な情報システムへの無権限アクセスへと進むことができるといったようなことを述べたいのだろうと考えられる。
このようなタイプの攻撃プロセスの最初の段階は，単なる個人データの無権限入手だけであるが，その個人データを識別子とする情報システムを攻撃対象としてその個人データが使用される段階では，本来は防御手段であるはずの個人データと識別機能が濫用され，より高度なサイバー攻撃が成功してしまうことになる。
NIS2 指令の前文(96)の中には一般に承認され難いと考えられる論述部分も含まれており，理解が容易ではないかもしれないが，それらの点を理解する上では，IPA（独立行政法人情報処理推進機構）セキュリティセンター「サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2023 年 7 月～9 月]」（2023 年 11 月 9 日）が参考になる。
以上のような諸点を踏まえた上で，前文(96)の中にあるわかりにくい箇所に関しては，合理的に意訳することにした。

NIS2 指令の前文(112)の第 1 文の中にある「the preamble of Regulation (EU) 2016/679」との箇所は，明白な誤りを含む文である。正しい文は，「the recital (14) of Regulation (EU) 2016/679」である。
一般に，EU 法においては，前文は「recital」であり，「preamble」ではない。これと対照的に，Council of Europe (CoE)の条約（国際協定）においては，一般に，前文は「preamble」であり，「recital」ではない。
ただし，日本語訳の表現としてはどちらの場合でも同一の日本語文となるので，NIS2 指令の前文(112)の第 1 文の中にある誤りは，日本語の翻訳文には影響を与えない。

NIS2 指令の第 3 条第 3 項の「at least every two years thereafter」との箇所にある「thereafter」は，起算日の計算根拠となる要件が明示では定められていないので，誤記の一種である可能性がある。

ただし, この参考訳においては, 原文どおりに訳出することにした。

NIS2 指令の第 9 条第 5 項第 1 文には, NIS2 指令の第 3 条第 3 項と同種の問題が存在する。
ただし, この参考訳においては, 原文どおりに訳出することにした。

NIS2 指令の第 15 条第 3 項(k)の中にある「where necessary, request guidance in that regard」との箇所は, 「where necessary, to request guidance in that regard」の誤記と思われる。
この参考訳においては, 合理的に解釈した上で訳出することにした。

NIS2 指令の第 16 条第 3 項(c)の中にある「and propose possible mitigation measures」との箇所は, 「and to propose possible mitigation measures」の誤記と思われる。
この参考訳においては, 合理的に解釈した上で訳出することにした。

NIS2 指令の第 16 条第 3 項(d)の中にある「and support decision-making at political level」との箇所は, 「and to support decision-making at political level」の誤記と思われる。
この参考訳においては, 合理的に解釈した上で訳出することにした。

NIS2 指令の第 19 条第 5 項第 1 文の中にある「and provide that self-assessment」との箇所は, 「and provide the results of that self-assessment」の誤記と思われる。
この参考訳においては, 合理的に解釈した上で訳出することにした。

NIS2 指令の第 23 条第 4 項第 1 副項の柱書及び(a)～(d)の部分と(e)の部分との間には文法上の断絶があり, 崩れた文となっている。
本来, (e)の部分は, (a)～(d)の部分と並ぶ文ではなく, 柱書の中に但書として組み込まれるべき文または別の副項として構成されるべき文である。(e)の部分は, 校正の際のミスにより現在のような体裁になってしまった文である可能性もある。
この参考訳においては, 合理的に解釈した上で訳出することにした。なお, 日本語文の文法構造上の特性から, 原文の外見的な体裁とは異なる体裁の訳文となっている。

NIS2 指令の第 23 条第 6 項第 3 文の中にある「preserve the entity's security and commercial interests as well as the confidentiality of the information provided」との箇所は, 「protect the entity's security and commercial interests as well as preserve the confidentiality of the information provided」の誤記の一種と思われる（第 2 条第 13 項参照）。
ただし, この参考訳においては, 原文のまま訳出することにした。

NIS2 指令の第 26 条第 1 項(b)の中にある「managed security service providers, as well as providers of online marketplaces」との箇所は, 「managed security service providers, or providers of online marketplaces」の誤記と思われる（前文(116)参照）。
ただし, この参考訳においては, 原文のまま訳出することにした。

NIS2 指令の第 27 条第 2 項(d)の中にある「entity and, where applicable, its representative」との箇所には疑問がある。このままで正しい文かもしれないが，例えば，「entity and, where applicable, of its representative」のような文が正しい文であるかもしれない（第 27 条第 2 項(c)）。これらのどちらの場合であってもそのままで意味が通る。無論，意図的に現在のような（第 27 条第 2 項(c)とは異なる）文とした可能性は否定されない。
この参考訳では，整合性と合理性を評価した上で，「entity and, where applicable, of its representative」のような文が正しい文であり，誤記の一種であると解し，そのように訳出することにした。

NIS2 指令の第 30 条には，NIS2 指令の第 30 条にも第 7 条第 1 項(g)と同様の誤りが存在する可能性が否定されない。
ただし，この参考訳においては，原文のまま訳出することにした。

NIS2 指令の第 32 条第 10 項第 2 文の中にある「pursuant to Article 31 of Regulation (EU) 2022/2554. with this Directive」との箇所は，明白に，「pursuant to Article 31 of Regulation (EU) 2022/2554 with this Directive」の誤記である。
この参考訳においては，そのように解した上で訳出することにした。

NIS2 指令の第 33 条第 4 項柱書の中にある「Member States shall ensure that the competent authorities」との箇所は，「Member States shall ensure that their competent authorities」の誤記ではないかと考えられる。
ただし，この参考訳においては，原文のまま訳出することにした。

NIS2 指令の第 33 条第 6 項第 2 文の中にある「pursuant to Article 31 of Regulation (EU) 2022/2554. with this Directive」との箇所は，明白に，「pursuant to Article 31 of Regulation (EU) 2022/2554 with this Directive」の誤記である。
この参考訳においては，そのように解した上で訳出することにした。

NIS2 指令の第 35 条第 3 項は，不完全な文である可能性がある。
この参考訳においては，合理的に解釈した上で，適宜意訳することにした。

4. 訳語に関する補足的説明

Common Vulnerabilities and Exposures

「CVE」と略称される「Common Vulnerabilities and Exposures」に関しては，「共通脆弱性識別子」との訳が定着しているようであるが，「and Exposures」は，どのような角度から考察・検討しても「識別子」と訳すことができない。
この参考訳においては，誤訳であるとの誤解を避けるため，直訳を原則とするという参考訳作成上の基本方針に従い，「Common Vulnerabilities and Exposures」を「共通脆弱性及び危殆」と訳すことにした。

Systemic risks

一般に，「systemic risks」は，当該リスクが直接に発生する組織，制度または情報システムだけではなく，関連性のある他の組織，制度または情報システムに対しても大きな悪影響を波及させ得るような性質をもつリスクのことを意味する。

現時点において適切な訳語が見当たらない。

そのため，この参考訳においては，「systemic risks」を「システミックリスク」とカタカナ表記することにした。もし他に良い訳語が存在するときは，その訳語によるべきである。

Constituency

「constituency」は，一般的には，「選挙区」という意味をもつ。

しかし，CSIRT 及びその業務と関連する文脈においては，「constituency」が提供するセキュリティサービスの対象コミュニティのことを指す（RFC 2350 - Expectations for Computer Security Incident Response, 1998 参照）。
この場合のコミュニティとは，法令上の規定や関係者間の合意により，特定の CSIRT がその業務の対象としている社会的活動単位（特定の行政機関，行政区，企業，教育機関，研究機関，組織・団体等）のことを指し，限定的な意味をもつもので，一般的な意味でのコミュニティという意味をもたない。特定の CSIRT は，複数の「constituency」をもち得る。
特定の CSIRT は，当該 CSIRT の特定の「constituent」である「community」において発生したインシデントに関して緊急対応すべき職責を負うが，当該 CSIRT の「constituent」ではない「community」において発生したインシデントに関しては，何らの権利も義務もない。
それゆえ，個々の CSIRT の業務遂行だけでは，広域で発生しているインシデントや広域に影響が波及するおそれのあるインシデントに対して適切に緊急対応することは，そもそも不可能なことである。
一般に，広域の影響を想定しなければならない大規模なサイバーセキュリティのインシデントとの

関係においては，可能な限り多くの CSIRT の連携と情報交換を確保する必要がある。
ところが，EU においては，EU を構成する構成国それぞれが独立の主権国家であり，また，CSIRT は個々の構成国の担当当局が所管する行政機関または民間組織となっている。
そのことから，EU において，広域の大規模なサイバーセキュリティのインシデントに適切に緊急対応するための適切な準備態勢（preparedness）を整えるためには，それぞれの構成国の国家主権（jurisdiction）を超えた国家間の連携と情報交換が必須となる。
NIS2 指令は，そのような意味での CSIRT の広域の連携と情報交換の枠組みの法的根拠を提供しており，それを実現するための（欧州連合レベル及び構成国レベルの）具体的な手段を定めている。

CSIRT 及びその業務と関連する文脈における「constituency」の定訳は存在しないと思われる。
他方，日本国においては，（情報セキュリティの専門家などを除き）CSIRT の活動それ自体があまり知られていないため，「constituency」を単純にカタカナ表記するとかなり多くの誤解を生む危険性がある。

以上の諸点を踏まえた上で，この参考訳においては，「constituency」を「対象コミュニティ」と意訳することにした。

Handover

「handover」は，一般用語としての文脈，一般的な情報通信の文脈，インシデントに対する緊急対応の文脈の相違により，異なる意味をもつ。

一般用語としては，スラングの場合を含め，非常に多様なので，「handover」という語を用いる当の表現者の意図を完全に精査しないと意味を確定できず，その意味に対応する日本語を確定することもできない。
一般的な情報通信の文脈では，「handover」は，情報通信のための通信基地局の「切替え」という意味で使用されることが多い。
インシデントに対する緊急対応の文脈では，インシデント緊急対応チーム（Incident Response Team）からインシデント管理チーム（Incident Management Team）への当該案件の「引継ぎ」という意味で使用されることがある。インシデント緊急対応チームが当該インシデント案件を扱うのは，最初の数時間だけとされている（ENISA の「Incident response team」の定義参照）。

NIS2 指令の第 11 条第 1 項(c)の「handover」の意味内容は，必ずしも一義的明確であるとは言い難い面があり，かつ，NIS2 指令が想定している構成国内のサイバーセキュリティ対応の仕組みと一致していないのではないかと疑われる面もないわけではない。
しかし，この参考訳においては，とりあえず，通常の理解に従い，インシデント緊急対応チームからインシデント管理チームへの当該案件の「引継ぎ」という意味に理解し，そのように訳出することにした。

Landscape

「landscape」は，一般的には，風景画や鳥観図または軍事上の作戦図のような概況を示す図画，または，そのような概況を示す図画から理解・感得される全体的な状況認識または全体的な印象のことを指す。一般的には，「景観」または「情景」等と訳される。

風景画や鳥観図は，大まかなものとは限らない。例えば，『洛中洛外図』及びその写本等（1500～1600 年代）は，いずれも全体の構図と描写が優れているというだけではなく，それを構成する細部要素も全て詳密に描かれており，総合図鑑的な機能を併有している。一般に，日本国内に現存している合戦図や寺社縁起の類は，概ねそのような構成と機能をもっていることが多い。
外国の絵画作品の中にある具体例としては，例えば，ピーテル・ブリューゲル（Pieter Bruegel）作『バベルの塔』（1500 年代）が同様の構成と機能をもっていると評価できる。

サイバー攻撃の文脈に限定すると，この「景観」の実質的な意味は，現況の「全体的把握」である。その全体的把握の対象は，およそ全ての種類の脅威ではなく，対象地域または対象部門（領域）を限定した上で観察されたサイバー攻撃と関連性のある脅威である。
このような全体的把握は，「木を見て森を見ず」の愚に陥ることなく，考察対象の全体も細部も同時に観察・理解し，より優れた理解と洞察を導くための思考手法を実現可能にする。そのような思考手法による観察と考察を勤勉に実践し続けることにより，次第に，全体把握と細部の（現況及び相互作用の）理解を同時に得られるようになる。

NIS2 指令においては，既述の「ENISA Threat Landscape 2023」の表題にも見られるとおり，「landscape」は，（象徴的な表現としての）「景観」である。
しかし，全ての箇所に関して「景観」と訳すと，意味をとりにくくなってしまうという難がある。一般に，象徴的な表現に関しては，どのような法律文書においても共通の難がある。

そこで，この参考訳においては，象徴的な意味で「landscape」が用いられている箇所に関しては「景観」と直訳し，他方，「landscape」の実質的な意味を示すべきだと判断した箇所に関しては「全体的把握」と意訳することにした。

Critical entity

「critical entity」は，「重要法主体」または「必須法主体」と訳し得る。
しかし，NIS2 指令において，指令(EU) 2022/2557 の「critical entity」と NIS2 指令の「important entities」とを識別する必要があること，そして，指令(EU) 2022/2557 においては，TFEU の第 114 条の適用範囲内にある重要な社会的機能または経済活動の維持のために必須なサービス（essential service）を提供する法主体を指すものとして「critical entity」が用いられていることから，この参考訳においては，指令(EU) 2022/2557 に定める「critical entity」のことを指す場合には，「必須法主体」と訳すことにした。

5. 関連参考訳

NIS 指令(EU) 2016/1148 の参考訳・再訂版は，法と情報雑誌 6 巻 6 号 467～548 頁にある。
指令(EU) 2022/2557 の参考訳は，法と情報雑誌 8 巻 4 号 207～304 頁にある。
規則(EU) 2019/881（サイバーセキュリティ法）の参考訳・改訂版は，法と情報雑誌 4 巻 8 号 16～86 頁にある。指令 2013/40/EU の参考訳・改訂版は，法と情報雑誌 2 巻 8 号 164～185 頁にある。

規則 (EU) 2016/679（一般データ保護規則）の参考訳・再訂版は，法と情報雑誌 3 巻 5 号 1～114 頁にある。規則(EU)2018/1725 の参考訳は，法と情報雑誌 4 巻 1 号 1～81 頁にある。指令 2002/58/EC の参考訳・改訂版は，法と情報雑誌 2 巻 5 号 158～187 頁にある。
電子識別規則(EU) No 910/2014 の参考訳は，法と情報雑誌 2 巻 10 号 147～196 頁にある。
規則(EU)2022/868（データ統治法）の参考訳は，法と情報雑誌 8 巻 3 号 1～130 頁にある。

規則(EU) 2021/694 の参考訳は，法と情報雑誌 6 巻 1 号 1～104 頁にある。
欧州電子通信法指令(EU) 2018/1972 の参考訳は，法と情報雑誌 4 巻 2 号 1～212 頁にある。
指令 2011/24/EU の参考訳は，法と情報雑誌 3 巻 6 号 133～168 頁にある。ITS 指令 2010/40/EU の参考訳は，法と情報雑誌 2 巻 9 号 27～47 頁にある。
電子商取引指令 2000/31/EC の参考訳は，法と情報雑誌 3 巻 1 号 110～141 頁にある。規則(EU) 2022/ 2065（デジタルサービス法）の参考訳は，法と情報雑誌 8 巻 2 号 1～299 頁にある。
金融商品市場規則(EU) No 600/2014（MiFIR）の参考訳は，法と情報雑誌 3 巻 3 号 1～79 頁にある。金融商品市場指令 2014/65/EU（MiFID II）の参考訳は，法と情報雑誌 3 巻 3 号 1～175 頁にある。OTC デリバティブ規則(EU) No 648/2012 の参考訳は，法と情報雑誌 3 巻 8 号 1～96 頁にある。
指令(EU) 2015/1535 の参考訳は，法と情報雑誌 3 巻 7 号 1～20 頁にある。

規則(EU) No 182/2011 の参考訳は，法と情報雑誌 3 巻 5 号 168～179 頁にある。

この参考訳の校正等に関し，唐亀侑久氏（株式会社ラック）の助力を得た。

＊＊＊

欧州全域の共通の高いレベルのサイバーセキュリティのための措置に関する，規則(EU) No 910/2014 及び指令(EU) 2018/1972 を改正し，並びに，指令(EU) 2016/1148 を廃止する 欧州議会及び理事会の 2022 年 12 月 14 日の指令(EU) 2022/2555（NIS2 指令）

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

（EEA に適用される正文）
(Text with EEA relevance)

欧州議会及び欧州連合の理事会は，
欧州連合の機能に関する条約，とりわけ，その第 114 条に鑑み，
欧州委員会からの提案に鑑み，
立法案を国内議会に送付した後，
欧州中央銀行の意見書に鑑み[1]，
欧州経済社会委員会の意見書に鑑み[2]，
地域委員会の意見を聴取した後，
通常の立法手続に従って審議し[3]，

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,
Having regard to the proposal from the European Commission,
After transmission of the draft legislative act to the national parliaments,
Having regard to the opinion of the European Central Bank (1),
Having regard to the opinion of the European Economic and Social Committee (2),
After consulting the Committee of the Regions,
Acting in accordance with the ordinary legislative procedure (3),

Whereas:

---

1 OJ C 233, 16.6.2022, p. 22.
2 OJ C 286, 16.7.2021, p. 170.
3 欧州議会の 2022 年 11 月 10 日付けの意見書（官報未搭載）及び理事会の 2022 年 11 月 28 日付け決定.
Position of the European Parliament of 10 November 2022 (not yet published in the Official Journal) and decision of the Council of 28 November 2022.

(1) 欧州議会及び理事会の指令(EU) 2016/1148[4]は，欧州連合全域のサイバーセキュリティの実現能力を構築すること，鍵となる諸部門において必須のサービスを提供するために使用されるネットワーク及び情報システムに対する脅威を緩和すること，並びに，インシデントに直面した場合にそのようなサービスの継続性を確保すること，そして，欧州連合のセキュリティに貢献し，及び，欧州連合の経済と社会の実効的な稼働に貢献することを狙いとした。

Directive (EU) 2016/1148 of the European Parliament and the Council(4) aimed to build cybersecurity capabilities across the Union, mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing incidents, thus contributing to the Union's security and to the effective functioning of its economy and society.

(2) 指令(EU) 2016/1148 の発効の後，欧州連合のサイバー回復力のレベルの向上には大きな進捗があった。同指令の見直しの結果は，同指令が，欧州連合内のサイバーセキュリティへの組織的かつ法令によるアプローチのための触媒を提供し，思考方法を大きく変えるための道を拓いているということを示した。同指令は，ネットワーク及び情報システムの防護に関する国内戦略を構築し，国内の実現能力を構築することにより，そして必須のインフラと個々の構成国によって指定された法主体に対して適用される法令上の措置を実装することにより，ネットワーク及び情報システムの防護に関する国内枠組みを完成することを確保した。指令(EU) 2016/1148 は，協力グループと国内コンピュータセキュリティインシデント対応チームのネットワークの設置を通じて，欧州連合レベルの協力にも貢献した。それらが達成されたのにも拘わらず，指令(EU) 2016/1148 の見直しの結果は，現在のサイバーセキュリティの検討課題及び発生しつつあるサイバーセキュリティの検討課題に対して同指令が実効的に対処することを妨げる固有の欠点をもつことを明らかにした。

Since the entry into force of Directive (EU) 2016/1148, significant progress has been made in increasing the Union's level of cyber resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks on the security of network and information systems by establishing national strategies on security of network and information systems and establishing national capabilities and by implementing regulatory measures covering essential infrastructures and entities identified by each Member State. Directive (EU) 2016/1148 has also contributed to cooperation at Union level through the establishment of the Cooperation Group and the network of national computer security incident response teams. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively current and emerging cybersecurity challenges.

---

[4] 欧州連合全域にわたるネットワーク及び情報システムの共通の高いレベルのセキュリティのための措置に関する欧州議会及び理事会の 2016 年 7 月 6 日の指令(EU) 2016/1148 (OJ L 194, 19.7.2016, p. 1).
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

(3) ネットワーク及び情報システムは，国境を越える交流を含め，社会の迅速なデジタル変革と相互接続によって，日々の生活の中心となる機能に発展した。その発展は，全ての構成国における適応性があり，調整されかつ革新的な対応を要求する新たな検討課題をもたらすサイバーな脅威の景観の拡大を導くことになった。インシデントの数，深刻度，巧妙さ，頻度及び影響は，増大しており，かつ，ネットワーク及び情報システムの稼働に対する重大な脅威をもたらしている。結果として，インシデントは，域内市場における経済活動の遂行を妨げ，金銭的損失を生じさせ，利用者の信頼を損ね，そして，欧州連合の経済と社会に重大な損害を発生させ得る。それゆえ，今日，域内市場の適正な稼働にとって，サイバーセキュリティの準備態勢と実効性は，かつてないほど必須のものとなっている。更に，多数の重要部門にとって，サイバーセキュリティは，デジタル変革の受容を成功させるための，そして，デジタル化による経済的，社会的及び持続的な利益を全面的に掴むための鍵となる実現可能化要素である。

Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cyber threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, incidents can impede the pursuit of economic activities in the internal market, generate financial loss, undermine user confidence and cause major damage to the Union's economy and society. Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market. Moreover, cybersecurity is a key enabler for many critical sectors to successfully embrace the digital transformation and to fully grasp the economic, social and sustainable benefits of digitalisation.

(4) 指令(EU) 2016/1148 の法律上の根拠は，欧州連合の機能に関する条約（TFEU）の第 114 条だった。同条の目的は，国内規定を近似させるための措置を拡大することによる域内市場の設置と稼動である。経済的に重要なサービスを提供する法主体または経済的に重要な活動を遂行する法主体に対して課されるサイバーセキュリティの要件は，要件のタイプ，要件の詳細さのレベル及び監督手法の面において，構成国間で大きく異なっている。それらの格差は，付加的なコストを伴い，また，国境を越えて物品またはサービスを提供する法主体に対して困難をつくり出す。ある構成国によって課される要件であって，別の構成国によって課される要件とは異なる要件，または，別の構成国によって課される要件と抵触することさえある要件は，そのような国境を越える活動に対して大きな影響を与え得る。更に，とりわけ，国境を越える交流の頻度に鑑み，ある構成国においてサイバーセキュリティの要件の不適切な設計または実装があり得ることは，別の構成国のサイバーセキュリティのレベルに対して影響を及ぼす可能性がある。指令(EU) 2016/1148 の見直しの結果は，同指令の適用範囲との関係を含め，構成国による同指令の実装において広範な格差があることを示していた。その適用範囲の区切りは，大規模に構成国の自由裁量に任されたままとなっていた。指令(EU) 2016/1148 は，同指令に定める防護義務及びインシデント報告義務の実装に関しても，構成国に対して広範な自由裁量を提供していた。それゆえ，それらの義務は，国内レベルにおいて大きく異なる方法で実装されていた。指令(EU) 2016/1148 の監督及び

執行に関する条項の実装には同様の格差が存在する。

The legal basis of Directive (EU) 2016/1148 was Article 114 of the Treaty on the Functioning of the European Union (TFEU), the objective of which is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules. The cybersecurity requirements imposed on entities providing services or carrying out activities which are economically significant vary considerably among Member States in terms of type of requirement, their level of detail and the method of supervision. Those disparities entail additional costs and create difficulties for entities that offer goods or services across borders. Requirements imposed by one Member State that are different from, or even in conflict with, those imposed by another Member State, may substantially affect such cross-border activities. Furthermore, the possibility of the inadequate design or implementation of cybersecurity requirements in one Member State is likely to have repercussions at the level of cybersecurity of other Member States, in particular given the intensity of cross-border exchanges. The review of Directive (EU) 2016/1148 has shown a wide divergence in its implementation by Member States, including in relation to its scope, the delimitation of which was very largely left to the discretion of the Member States. Directive (EU) 2016/1148 also provided the Member States with very wide discretion as regards the implementation of the security and incident reporting obligations laid down therein. Those obligations were therefore implemented in significantly different ways at national level. There are similar divergences in the implementation of the provisions of Directive (EU) 2016/1148 on supervision and enforcement.

(5) それらの全ての格差は，域内市場の断片化を伴うものであり，また，とりわけ，種々の措置を適用することのゆえに，国境を越えるサービスの提供とサイバー回復力のレベルに対して影響を与え，域内市場の稼働に対する阻害的な影響をもち得る。究極的には，それらの格差は，欧州連合全域への潜在的な波及効果をもつ，幾つかの構成国のサイバーな脅威に対するより高度な脆弱性を導き得る。この指令は，とりわけ，調整された法令上の枠組みの稼働と関連するミニマムの規定を定めることにより，個々の構成国内の職責のある機関の間における実効的な協力の仕組みを定めることにより，サイバーセキュリティの義務に服する部門及び活動のリストをアップデートすることにより，そして，それらの義務の実効的な執行の鍵となる実効的な解決と執行の措置を提供することにより，構成国間におけるそのような広範な格差を除去することを狙いとしている。それゆえ，指令(EU) 206/1148 は，廃止され，この指令によって置き換えられるべきである。

All those divergences entail a fragmentation of the internal market and can have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and the level of cyber resilience due to the application of a variety of measures. Ultimately, those divergences could lead to the higher vulnerability of some Member States to cyber threats, with potential spill-over effects across the Union. This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and enforcement measures which are key to the effective enforcement of those obligations.

Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.

(6) 指令(EU) 2016/1148 の廃止と共に，部門毎の適用の範囲は，域内市場において鍵となる社会的活動及び経済活動に対して極めて大きな重要性をもつ部門及びサービスの包括的な包摂を提供するため，経済のより大きな部分に拡大されるべきである。とりわけ，この指令は，基礎サービスの運営者とデジタルサービスプロバイダの間で区別することの欠点を克服することを狙いとしている。その区別は，域内市場における社会的活動及び経済活動に対する部門またはサービスの重要性を反映するものではなく，時代遅れであることが証明されている。

With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy to provide a comprehensive coverage of sectors and services of vital importance to key societal and economic activities in the internal market. In particular, this Directive aims to overcome the shortcomings of the differentiation between operators of essential services and digital service providers, which has been proven to be obsolete, since it does not reflect the importance of the sectors or services for the societal and economic activities in the internal market.

(7) 指令(EU) 2016/1148 の下において，構成国は，基礎サービスの運営者として分類するための基準に適合する法主体を識別特定する職責を負っていた。その点に関する構成国間の広範な格差を解消するため，そして，関連する全ての法主体に関するサイバーセキュリティのリスク管理の措置及び報告義務と関連する法的確実性を確保するため，この指令の適用範囲内にある法主体を決定する統一的な基準が設けられるべきである。当該基準は，それが適用されれば，委員会勧告 2003/361/EC[5]の別紙の第 2 条に下にある中規模企業として分類され，または，同条第 1 項に定める中規模企業の上限を超過し，かつ，その部門内で運営され，この指令によって包摂されるタイプのサービスを提供しもしくは活動を遂行する全ての法主体がこの指令の適用範囲内となる規模上限規定の適用によって，構成されるべきである。構成国は，同別紙の第 2 条第 2 項及び第 3 項に定義する一定の小企業及びマイクロ企業であって，社会，経済にとって，または，特別の部門もしくはタイプのサービスにとって，鍵となる役割を示す特定の基準を満たすものが，この指令の適用範囲内とすることも定めるべきである。

Under Directive (EU) 2016/1148, Member States were responsible for identifying the entities which met the criteria to qualify as operators of essential services. In order to eliminate the wide divergences among Member States in that regard and ensure legal certainty as regards the cybersecurity risk-management measures and reporting obligations for all relevant entities, a uniform criterion should be established that determines the entities falling within the scope of this Directive. That criterion should consist of the application of a size-cap rule, whereby all entities which qualify as medium-sized enterprises under

[5] マイクロ企業，小企業及び中規模企業の定義に関する 2003 年 5 月 6 日の委員会勧告 2003/361/EC (OJ L 124, 20.5.2003, p. 36).
Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

Article 2 of the Annex to Commission Recommendation 2003/361/EC [(5)], or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which operate within the sectors and provide the types of service or carry out the activities covered by this Directive fall within its scope. Member States should also provide for certain small enterprises and microenterprises, as defined in Article 2(2) and (3) of that Annex, which fulfil specific criteria that indicate a key role for society, the economy or for particular sectors or types of service to fall within the scope of this Directive.

(8) この指令の適用範囲からの行政機関である法主体の適用除外は，当該法主体の活動が，専ら，国家安全保障，公共の保安，国防の分野，または，犯罪行為の防止，捜査，検知及び訴追を含め，法執行の分野において遂行されている法主体に対して適用されるべきである。ただし，その活動が当該分野と僅かに関連するだけの行政機関である法主体は，この指令の適用範囲から除外されるべきではない。この指令の目的のために，規制の職務権限のある法主体は，法執行の分野における活動を遂行しているとは判断されず，それゆえ，当該根拠によっては，この指令の適用範囲から除外されない。国際協定に従って第三国と共同で設置されている行政機関である法主体は，この指令の適用範囲から除外される。この指令は，構成国の第三国における外交の職務及び領事館の職務には適用されず，または，そのような職務のシステムが領事館の施設内に所在している限り，もしくは，第三国内の利用者のために運用されている限り，当該領事館のネットワーク及び情報システムには適用されない。

The exclusion of public administration entities from the scope of this Directive should apply to entities whose activities are predominantly carried out in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences. However, public administration entities whose activities are only marginally related to those areas should not be excluded from the scope of this Directive. For the purposes of this Directive, entities with regulatory competences are not considered to be carrying out activities in the area of law enforcement and are therefore not excluded on that ground from the scope of this Directive. Public administration entities that are jointly established with a third country in accordance with an international agreement are excluded from the scope of this Directive. This Directive does not apply to Member States' diplomatic and consular missions in third countries or to their network and information systems, insofar as such systems are located in the premises of the mission or are operated for users in a third country.

(9) 構成国は，国家安全保障上の必須の利益の保護を確保するため，公共政策と公共の保安を防護するため，そして，犯罪行為の防止，捜査，検知及び訴追を可能とするために必要となる措置を講ずることができるべきである。その目的のために，構成国は，国家安全保障，公共の保安，国防の分野，または，犯罪行為の防止，捜査，検知及び訴追を含め，法執行の分野における活動を遂行する特定の法主体から，それらの活動と関連してこの指令に定める一定の義務を免除できるべきである。ある法主体が，専ら，この指令の適用範囲から除外される行政機関である法主体に対してサービスを提供する場合，構成国は，当該法主体から，当該サービスと関連してこの指令に定める一定の義務を免除できるべきである。更に，いかなる構成国も，その情報を開示することがその構成国の国家安全保障，公共の保安または国防という必須の利益と矛盾するような情

報を提供することを要求されてはならない。その文脈においては，機密情報の保護に関する欧州連合の規定または国内規定，不開示合意，及び，トラフィックライトプロトコルのような非公式の不開示合意が考慮に入れられるべきである。トラフィックライトプロトコルは，別の目的のために情報を拡散することと関連する制限に関する情報を提供するための手段として理解されるべきである。ほとんど全てのコンピュータセキュリティインシデント対応チーム（「CSIRT」）において，及び，幾つかの情報分析共有拠点において，それが使用されている。

Member States should be able to take the necessary measures to ensure the protection of the essential interests of national security, to safeguard public policy and public security, and to allow for the prevention, investigation, detection and prosecution of criminal offences. To that end, Member States should be able to exempt specific entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, from certain obligations laid down in this Directive with regard to those activities. Where an entity provides services exclusively to a public administration entity that is excluded from the scope of this Directive, Member States should be able to exempt that entity from certain obligations laid down in this Directive with regard to those services. Furthermore, no Member State should be required to supply information the disclosure of which would be contrary to the essential interests of its national security, public security or defence. Union or national rules for the protection of classified information, non-disclosure agreements, and informal non-disclosure agreements such as the traffic light protocol should be taken into account in that context. The traffic light protocol is to be understood as a means to provide information about any limitations with regard to the further spreading of information. It is used in almost all computer security incident response teams (CSIRTs) and in some information analysis and sharing centres.

(10) この指令は，原子力発電所において電気を生産する活動を遂行する法主体に対して適用されるが，それらの活動の幾つかは，国家安全保障と結びつくものであり得る。そのような場合に該当するときは，構成国は，諸条約に従い，原子力の価値連鎖の中にある活動を含め，それらの活動と関係する国家安全保障を守るためのその構成国の職責を果たすことができるべきである。

Although this Directive applies to entities carrying out activities in the production of electricity from nuclear power plants, some of those activities may be linked to national security. Where that is the case, a Member State should be able to exercise its responsibility for safeguarding national security with respect to those activities, including activities within the nuclear value chain, in accordance with the Treaties.

(11) 幾つかの法主体は，信頼サービスも提供しつつ，国家安全保障，公共の保安，国防の分野，または，犯罪行為の防止，捜査，検知及び訴追を含め，法執行の分野における活動を遂行している。欧州議会及び理事会の規則(EU) No 910/2014[6]の適用範囲内にある信頼サービスのプロバイダ

[6] 域内市場における電子的なやりとりのための電子識別及び信頼サービスに関する，及び，指令 1999/93/EC を廃止する欧州議会及び理事会の 2014 年 7 月 23 日の規則(EU) No 910/2014 (OJ L 257, 28.8.

は，信頼サービスのプロバイダと関係して従前は同規則の中で定められていたのと同じレベルのセキュリティの要件と監督を防護するため，この指令の適用範囲内にあるべきである。一定の個別のサービスの規則(EU) No 910/2014 からの適用除外に沿って，国内法から帰結する，または，定義されたセットの参加者間の合意から帰結する，専らクローズドのシステム内で使用される信頼サービスの提供に対し，この指令を適用してはならない。

Some entities carry out activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, while also providing trust services. Trust service providers which fall within the scope of Regulation (EU) No 910/2014 of the European Parliament and of the Council (6) should fall within the scope of this Directive in order to secure the same level of security requirements and supervision as that which was previously laid down in that Regulation in respect of trust service providers. In line with the exclusion of certain specific services from Regulation (EU) No 910/2014, this Directive should not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.

(12) 宅配便サービスのプロバイダを含め，欧州議会及び理事会の指令 97/67/EC[7]に定義する郵便サービスのプロバイダは，ネットワーク及び情報システムにおける当該プロバイダの依存性の程度を考慮に入れつつ，当該プロバイダが郵便物配達網内の少なくとも 1 つの手立てを提供するきは，とりわけ，集荷サービスを含め，郵便物の通関，仕分け，配送または配達を提供するときは，この指令に服すべきである。それらの手立て中のいずれとも組み合わされて実施されていない配送サービスは，郵便サービスの適用範囲から除外されるべきである。

Postal service providers as defined in Directive 97/67/EC of the European Parliament and of the Council (7), including providers of courier services, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain, in particular clearance, sorting, transport or distribution of postal items, including pick-up services, while taking account of the degree of their dependence on network and information systems. Transport services that are not undertaken in conjunction with one of those steps should be excluded from the scope of postal services.

(13) サイバーな脅威の激化とその巧妙さの増大に鑑み，構成国は，この指令の適用範囲から除外さ

2014, p. 73).

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

7 欧州共同体の郵便サービスの域内市場の発展及びサービス品質の向上のための共通の規定に関する欧州議会及び理事会の 1997 年 12 月 15 日の指令 97/67/EC (OJ L 15, 21.1.1998, p. 14).

Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service (OJ L 15, 21.1.1998, p. 14).

れている法主体が高いレベルのサイバーセキュリティを達成することを確保するため，そして，当該法主体の機微な性質を反映する均等なサイバーセキュリティのリスク管理の措置の実装を支援するため，努力すべきである。

Given the intensification and increased sophistication of cyber threats, Member States should strive to ensure that entities that are excluded from the scope of this Directive achieve a high level of cybersecurity and to support the implementation of equivalent cybersecurity risk-management measures that reflect the sensitive nature of those entities.

(14) 欧州連合のデータ保護法及び欧州連合のプライバシー法は，この指令の下にある個人データの処理に対して適用される。とりわけ，この指令は，欧州議会及び理事会の規則(EU) 2016/679[8]並びに欧州議会及び理事会の指令 2002/58/EC[9]を妨げない。それゆえ，この指令は，就中，適用可能な欧州連合のデータ保護法及び欧州連合のプライバシー法の遵守を監視する職務権限のある機関の職務及び権限に影響を与えてはならない。

Union data protection law and Union privacy law applies to any processing of personal data under this Directive. In particular, this Directive is without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council [(8)] and Directive 2002/58/EC of the European Parliament and of the Council [(9)]. This Directive should therefore not affect, inter alia, the tasks and powers of the authorities competent to monitor compliance with the applicable Union data protection law and Union privacy law.

(15) サイバーセキュリティのリスク管理の措置及び報告義務の遵守の目的のためにこの指令の適用範囲内にある法主体は，当該法主体が提供するサービスの部門またはタイプと関連して当該法主体が重要である程度及び当該法主体の規模を反映して，基礎法主体と重要法主体という 2 つの類型に分類されるべきである。この点に関し，それが適用可能なときは，職務権限のある機関による関連部門別のリスク評価及びガイドが適正に考慮に入れられるべきである。それら 2 つの類型の法主体に関する監督と執行の制度は，一方におけるリスクベースの要件及び義務と，他方における遵守の監督から派生する管理運営上の負担との間の公正なバランスを確保するため，区別されるべきである。

---

[8] 個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する，並びに，指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679（一般データ保護規則）(OJ L 119, 4.5.2016, p. 1).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[9] 電子通信部門における個人データ処理及びプライバシー保護に関する欧州議会及び理事会の 2002 年 7 月 12 日の指令 2002/58/EC（プライバシー及び電子通信に関する指令）(OJ L 201, 31.7.2002, p. 37).

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

Entities falling within the scope of this Directive for the purpose of compliance with cybersecurity risk-management measures and reporting obligations should be classified into two categories, essential entities and important entities, reflecting the extent to which they are critical as regards their sector or the type of service they provide, as well as their size. In that regard, due account should be taken of any relevant sectoral risk assessments or guidance by the competent authorities, where applicable. The supervisory and enforcement regimes for those two categories of entities should be differentiated to ensure a fair balance between risk-based requirements and obligations on the one hand, and the administrative burden stemming from the supervision of compliance on the other.

(16) パートナー企業をもつ法主体または連結された企業である法主体が，そのことが比例的ではないようであるのに基礎法主体または重要法主体であると判断されることを避けるため，構成国は，勧告 2003/361/EC の別紙の第 6 条第 2 項を適用する際，その法主体のパートナー企業または連結された企業との関係において法主体が享受している独立性の程度を考慮に入れることができる。とりわけ，構成国は，当該法主体がその法主体のサービス提供において使用しているネットワーク及び情報システムの面において，及び，その法主体が提供しているサービスの面において，その法主体のパートナー企業または連結された企業からその法主体が独立していることを考慮に入れることができる。それを基礎とした上で，それが適切なときは，構成国は，そのような法主体が，勧告 2003/361/EC の別紙の第 2 条の下にある中規模企業としては分類されないと判断でき，または，当該法主体の独立性の程度を考慮に入れた上で，当該法主体が，中規模企業として分類されるべきものとは判断されなかったときは，もしくは，その法主体自身が保有するデータが考慮に入れられる場合において，それらの上限を超過しているとは判断されなかったときは，同条第 1 項に定める中規模企業の上限を超過していないと判断できる。このことは，この指令の適用範囲内にあるパートナー企業または連結された企業のこの指令に定める義務に対して影響を与えないものとする。

In order to avoid entities that have partner enterprises or that are linked enterprises being considered to be essential or important entities where this would be disproportionate, Member States are able to take into account the degree of independence an entity enjoys in relation to its partner or linked enterprises when applying Article 6(2) of the Annex to Recommendation 2003/361/EC. In particular, Member States are able to take into account the fact that an entity is independent from its partner or linked enterprises in terms of the network and information systems that that entity uses in the provision of its services and in terms of the services that the entity provides. On that basis, where appropriate, Member States are able to consider that such an entity does not qualify as a medium-sized enterprise under Article 2 of the Annex to Recommendation 2003/361/EC, or does not exceed the ceilings for a medium-sized enterprise provided for in paragraph 1 of that Article, if, after taking into account the degree of independence of that entity, that entity would not have been considered to qualify as a medium-sized enterprise or to exceed those ceilings in the event that only its own data had been taken into account. This leaves unaffected the obligations laid down in this Directive of partner and linked enterprises which fall within the scope of this Directive.

(17) 構成国は，この指令が発効する前に指令(EU) 2016/1148 に従って基礎サービスの運営者として識別されていた法主体が基礎法主体であると判断されるべきことを決定できるべきである。

Member States should be able to decide that entities identified before the entry into force of this Directive as operators of essential services in accordance with Directive (EU) 2016/1148 are to be considered to be essential entities.

(18) この指令の適用範囲内にある法主体の明確な見通しを確保するため，構成国は，基礎法主体及び重要法主体並びにドメイン名登録サービスを提供する法主体のリストを作成すべきである。その目的のために，構成国は，法主体に対し，少なくとも以下の情報，すなわち，その法主体の名称，住所，及び，電子メールアドレス，IP アドレス範囲及び電話番号を含め，最新の連絡先，それが適用可能なときは，その別紙の中で示されている関連部門及び副部門，並びに，それが適用可能なときは，当該法主体がこの指令の適用範囲内にあるサービスを提供している構成国のリストを職務権限のある機関に提出することを要求すべきである。その目的のために，欧州委員会は，サイバーセキュリティに関する欧州連合の部局（ENISA）の補佐により，不適切な遅滞なく，情報を提出すべき義務と関連する指針及び雛型を提供すべきである。基礎法主体及び重要法主体並びにドメイン名登録サービスを提供する法主体のリストの作成及びアップデートを容易にするため，構成国は，法主体がその法主体自身を登録するための国内の仕組みを設置できるべきである。国内レベルの登録場所が存在するときは，構成国は，この指令の適用範囲内にある法主体を識別できる適切な仕組みに関して決定できる。

In order to ensure a clear overview of the entities falling within the scope of this Directive, Member States should establish a list of essential and important entities as well as entities providing domain name registration services. For that purpose, Member States should require entities to submit at least the following information to the competent authorities, namely, the name, address and up-to-date contact details, including the email addresses, IP ranges and telephone numbers of the entity, and, where applicable, the relevant sector and subsector referred to in the annexes, as well as, where applicable, a list of the Member States where they provide services falling within the scope of this Directive. To that end, the Commission, with the assistance of the European Union Agency for Cybersecurity (ENISA), should, without undue delay, provide guidelines and templates regarding the obligation to submit information. To facilitate the establishing and updating of the list of essential and important entities as well as entities providing domain name registration services, Member States should be able to establish national mechanisms for entities to register themselves. Where registers exist at national level, Member States can decide on the appropriate mechanisms that allow for the identification of entities falling within the scope of this Directive.

(19) 構成国は，少なくとも，別紙に示す各部門及び副部門の基礎法主体と重要法主体の数，並びに，識別された法主体の数，及び，当該組織が識別される根拠となった，この指令に定める条項からの条項，及び，当該法主体が提供するサービスのタイプに関する関連情報を欧州委員会に対して提出することの職責を負うべきである。構成国は，欧州委員会との間で，基礎法主体及び重要

法主体に関する情報を交換し，また，大規模なサイバーセキュリティのインシデントの場合，関係する法主体の名称のような情報を交換することが推奨される。

Member States should be responsible for submitting to the Commission at least the number of essential and important entities for each sector and subsector referred to in the annexes, as well as relevant information about the number of identified entities and the provision, from among those laid down in this Directive, on the basis of which they were identified, and the type of service that they provide. Member States are encouraged to exchange with the Commission information about essential and important entities and, in the case of a large-scale cybersecurity incident, relevant information such as the name of the entity concerned.

(20) 欧州委員会は，協力グループと協力し，かつ，関連する利害関係者の意見を聴取した後，当該企業がこの指令の適用範囲内にあるかどうかの評価のためにマイクロ企業及び小企業に対して適用可能な基準の実装に関する指針を提供すべきである。欧州委員会は，この指令の適用範囲内にあるマイクロ企業及び小企業に対して適切な指針が与えられることも確保すべきである。欧州委員会は，構成国の補助を得て，その点に関し，マイクロ企業及び小企業に対して情報を利用できるようにすべきである。

The Commission should, in cooperation with the Cooperation Group and after consulting the relevant stakeholders, provide guidelines on the implementation of the criteria applicable to microenterprises and small enterprises for the assessment of whether they fall within the scope of this Directive. The Commission should also ensure that appropriate guidance is given to microenterprises and small enterprises falling within the scope of this Directive. The Commission should, with the assistance of the Member States, make information available to microenterprises and small enterprises in that regard.

(21) 欧州委員会は，適用範囲に関するこの指令の条項の実装において，及び，この指令により講じられた措置の比例性の評価において，とりわけ，それによって法主体が基礎法主体と重要法主体の両者の割当てられる基準を同時に満たし得る，または，その活動の一部はこの指令の適用範囲内にあるが他の一部はこの指令の適用範囲から除外される活動を同時に遂行し得る複雑なビジネスモデルまたは業務運営環境をもつ法主体に関し，構成国を補助するための指針を提供し得る。

The Commission could provide guidance to assist Member States in implementing the provisions of this Directive on scope and evaluating the proportionality of the measures to be taken pursuant to this Directive, in particular as regards entities with complex business models or operating environments, whereby an entity may simultaneously fulfil the criteria assigned to both essential and important entities or may simultaneously carry out activities, some of which fall within and some of which are excluded from the scope of this Directive.

(22) この指令は，この指令の適用範囲内にある諸部門を横断するサイバーセキュリティのリスク管理

の措置及び報告義務に関する基線を定める。欧州連合の法行為のサイバーセキュリティ条項の断片化を避けるため，サイバーセキュリティのリスク管理の措置及び報告義務に関する別の部門別の欧州連合の法行為が，欧州連合全域にわたる高いレベルのサイバーセキュリティを確保するために必要なものであると判断されるときは，欧州委員会は，この指令の実装行為の中でそのような別の条項が定められ得るかどうかを評価すべきである。そのような実装行為が当該目的のために適切ではないときは，部門別の欧州連合の法行為は，関係する諸部門の特性及び複雑性を完全に考慮に入れつつ，欧州連合全域にわたる高いレベルのサイバーセキュリティを確保するために貢献し得る。その目的のために，この指令は，包括的かつ一貫性のあるサイバーセキュリティの枠組みの必要性を適正に考慮に入れるサイバーセキュリティのリスク管理の措置及び報告義務に対処する別の部門別の欧州連合の法行為の採択を排除しない。この指令は，輸送及びエネルギーを含め，多数の部門において欧州委員会に与えられた既存の実装権限を妨げない。

This Directive sets out the baseline for cybersecurity risk-management measures and reporting obligations across the sectors that fall within its scope. In order to avoid the fragmentation of cybersecurity provisions of Union legal acts, where further sector-specific Union legal acts pertaining to cybersecurity risk-management measures and reporting obligations are considered to be necessary to ensure a high level of cybersecurity across the Union, the Commission should assess whether such further provisions could be stipulated in an implementing act under this Directive. Should such an implementing act not be suitable for that purpose, sector-specific Union legal acts could contribute to ensuring a high level of cybersecurity across the Union, while taking full account of the specificities and complexities of the sectors concerned. To that end, this Directive does not preclude the adoption of further sector-specific Union legal acts addressing cybersecurity risk-management measures and reporting obligations that take due account of the need for a comprehensive and consistent cybersecurity framework. This Directive is without prejudice to the existing implementing powers that have been conferred on the Commission in a number of sectors, including transport and energy.

(23) 部門別の欧州連合の法行為が，基礎法主体または重要法主体に対してサイバーセキュリティのリスク管理の措置を採択することまたは重要なインシデントを通知することを要求する条項を含んでおり，かつ，当該要求が，この指令に定める義務と少なくとも均等な効果をもつときは，監督及び執行に関する条項を含め，当該部門別の法行為の条項は，そのような法主体に対して適用されるべきである。部門別の欧州連合の法行為が，この指令の適用範囲内にある個々の部門の全ての法主体を包摂しないときは，当該法行為によって包摂されない法主体に対し，この指令の関連条項が適用され続けるべきである。

Where a sector-specific Union legal act contains provisions requiring essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, those provisions, including on supervision and enforcement, should apply to such entities. If a sector-specific Union legal act does not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive should continue to apply to the entities not covered by that act.

(24) 部門別の欧州連合の法行為の条項が，基礎法主体または重要法主体に対してこの指令に定める報告義務と少なくとも均等な効果をもつ報告義務を遵守することを要求する場合，インシデント通知の取扱いの一貫性及び実効性が確保されるべきである。その目的のために，部門別の欧州連合の法行為のインシデント通知に関する条項は，CSIRT，職務権限のある機関またはこの指令に基づくサイバーセキュリティに関する単一連絡部局（単一連絡部局）に対し，その部門別の欧州連合の法行為に従って提出されたインシデント通知への即時のアクセスを提供すべきである。とりわけ，そのような即時のアクセスは，インシデント通知が，不適切な遅滞なく，CSIRTs，職務権限のある機関またはこの指令に基づく単一連絡部局に対して転送されれば，確保され得る。それが適切なときは，構成国は，そのようなインシデント通知の取扱いに関し，CSIRT，職務権限のある機関または単一連絡部局との間で情報を自動的かつ即時に共有することを確保する自動化された即時の報告の仕組みを設けるべきである。報告の簡素化の目的及び自動化された即時の報告の仕組みの実装の目的のために，構成国は，その部門別の欧州連合の法行為に従い，単一エントリポイントを使用できる。

Where provisions of a sector-specific Union legal act require essential or important entities to comply with reporting obligations that are at least equivalent in effect to the reporting obligations laid down in this Directive, the consistency and effectiveness of the handling of incident notifications should be ensured. To that end, the provisions relating to incident notifications of the sector-specific Union legal act should provide the CSIRTs, the competent authorities or the single points of contact on cybersecurity (single points of contact) under this Directive with an immediate access to the incident notifications submitted in accordance with the sector-specific Union legal act. In particular, such immediate access can be ensured if incident notifications are being forwarded without undue delay to the CSIRT, the competent authority or the single point of contact under this Directive. Where appropriate, Member States should put in place an automatic and direct reporting mechanism that ensures systematic and immediate sharing of information with the CSIRTs, the competent authorities or the single points of contact concerning the handling of such incident notifications. For the purpose of simplifying reporting and of implementing the automatic and direct reporting mechanism, Member States could, in accordance with the sector-specific Union legal act, use a single entry point.

(25) この指令に定めるサイバーセキュリティのリスク管理の措置及び報告義務と少なくとも均等な効果をもつサイバーセキュリティのリスク管理の措置及び報告義務を定める部門別の欧州連合の法行為は，そのような法行為の下にある職務権限のある機関が，この指令の下にある職務権限のある機関の補助を得て，そのような措置または義務と関係するそのような法行為の下にある職務権限のある機関の監督の権限及び執行の権限を行使することを定め得る。その目的のために，関係する職務権限のある機関は，協力覚書を定め得る。そのような協力覚書は，就中，国内法に従った調査及び施設内における検査の手続を含め，監督活動の調整に関する手続，並びに，この指令に基づき職務権限のある機関から要求されるサイバー関連情報へのアクセスを含め，職務権限のある機関の間における監督及び執行に関する関連情報の交換のための仕組みを定め得る。

Sector-specific Union legal acts which provide for cybersecurity risk-management measures or reporting

obligations that are at least equivalent in effect to those laid down in this Directive could provide that the competent authorities under such acts exercise their supervisory and enforcement powers in relation to such measures or obligations with the assistance of the competent authorities under this Directive. The competent authorities concerned could establish cooperation arrangements for that purpose. Such cooperation arrangements could specify, inter alia, the procedures concerning the coordination of supervisory activities, including the procedures of investigations and on-site inspections in accordance with national law, and a mechanism for the exchange of relevant information on supervision and enforcement between the competent authorities, including access to cyber-related information requested by the competent authorities under this Directive.

(26) 部門別の欧州連合の法行為が，法主体に対し，重大なサイバーな脅威を通知することを要求し，または，そのインセンティブを提供している場合，構成国は，サイバーな脅威の全体的把握の当該組織の拡大されたレベルの認識を確保するため，及び，重大なサイバーな脅威が具体化したときは，実効的に，かつ，適時の態様で当該組織が対応できるようにするため，CSIRT，職務権限のある機関またはこの指令に基づく単一連絡部局との間で重大なサイバーな脅威を共有することも推奨されるべきである。

Where sector-specific Union legal acts require or provide incentives to entities to notify significant cyber threats, Member States should also encourage the sharing of significant cyber threats with the CSIRTs, the competent authorities or the single points of contact under this Directive, in order to ensure an enhanced level of those bodies' awareness of the cyber threat landscape and to enable them to respond effectively and in a timely manner should the significant cyber threats materialise.

(27) 将来の部門別の欧州連合の法行為は，この指令に定める定義並びに監督と執行の枠組みを適正に考慮に入れるべきである。

Future sector-specific Union legal acts should take due account of the definitions and the supervisory and enforcement framework laid down in this Directive.

(28) 欧州議会及び理事会の規則(EU) 2022/2554[10]は，この指令との関係において，金融の法主体と関連する部門別の欧州連合の法行為の 1 つであると判断されるべきである。規則(EU) 2022/2554 の情報通信技術（ICT）のリスク管理，ICT 関連インシデントの管理，及び，とりわけ，重大な ICT 関連インシデントの報告と関連する条項，並びに，デジタル業務運営回復力試験，情報共有の合意

[10] 金融部門のデジタル業務運営回復力に関する，並びに，規則(EC) No 1060/2009，規則(EU) No 648/2012，規則(EU) No 600/2014，規則(EU) No 909/2014 及び規則(EU) 2016/1011 を改正する欧州議会及び理事会の 2022 年 12 月 14 日の規則(EU) 2022/2554（この官報の 1 頁参照）.
Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (see page 1 of this Official Journal).

及び ICT 第三者リスクに関する条項は，この指令に定める条項の代わりに適用されるべきである。それゆえ，構成国は，規則(EU) 2022/2554 の適用を受ける金融の法主体に対し，サイバーセキュリティのリスク管理及び報告義務並びに監督と執行に関するこの指令の条項を適用してはならない。それと同時に，この指令の下にある金融部門との間の強力な関係と情報交換を維持することが重要である。その目的のために，規則(EU) 2022/2554 は，欧州監督機関（ESAs）と同規則の下にある職務権限のある機関が，協力グループの活動に参加すること，並びに，単一連絡部局との間，CSIRT 及びこの指令の下にある職務権限のある機関との間で情報交換すること及び協力することを許容している。規則(EU) 2022/2554 の下にある職務権限のある機関は，CSIRT，職務権限のある機関またはこの指令に基づく単一連絡部局に対し，重大な ICT 関連インシデントの詳細，及び，それが関連するときは，重大なサイバーな脅威の詳細も伝送すべきである。このことは，インシデント通知への即時アクセスを提供することによって，また，直接にまたは単一エントリポイントを介して当該通知を転送することによって，達成され得る。更に，構成国は，その構成国のサイバーセキュリティ戦略の中に金融部門を含めることを継続すべきであり，また，CSIRTs は，その活動の中に金融部門を含め得る。

Regulation (EU) 2022/2554 of the European Parliament and of the Council [(10)] should be considered to be a sector-specific Union legal act in relation to this Directive with regard to financial entities. The provisions of Regulation (EU) 2022/2554 relating to information and communication technology (ICT) risk management, management of ICT-related incidents and, in particular, major ICT-related incident reporting, as well as on digital operational resilience testing, information-sharing arrangements and ICT third-party risk should apply instead of those provided for in this Directive. Member States should therefore not apply the provisions of this Directive on cybersecurity risk-management and reporting obligations, and supervision and enforcement, to financial entities covered by Regulation (EU) 2022/2554. At the same time, it is important to maintain a strong relationship and the exchange of information with the financial sector under this Directive. To that end, Regulation (EU) 2022/2554 allows the European Supervisory Authorities (ESAs) and the competent authorities under that Regulation to participate in the activities of the Cooperation Group and to exchange information and cooperate with the single points of contact, as well as with the CSIRTs and the competent authorities under this Directive. The competent authorities under Regulation (EU) 2022/2554 should also transmit details of major ICT-related incidents and, where relevant, significant cyber threats to the CSIRTs, the competent authorities or the single points of contact under this Directive. This is achievable by providing immediate access to incident notifications and forwarding them either directly or through a single entry point. Moreover, Member States should continue to include the financial sector in their cybersecurity strategies and CSIRTs can cover the financial sector in their activities.

(29) 航空部門の法主体に対して課されるサイバーセキュリティの義務の間の格差または重複を避けるため，欧州議会及び理事会の規則(EC) No 300/2008[11]及び規則(EU) 2018/1139[12] の下にある国

[11] 民間航空の安全の分野における共通の規定に関する，及び，規則(EC) No 2320/2002 を廃止する欧州議会及び理事会の 2008 年 3 月 11 日の規則(EC) No 300/2008 (OJ L 97, 9.4.2008, p. 72).

内機関並びにこの指令に下にある職務権限のある機関は，サイバーセキュリティのリスク管理の措置の実装，及び，当該措置の国内レベルにおける遵守の監督との関係において，協力すべきである。法主体による規則(EC) No 300/2008 及び規則(EU) 2018/1139 並びにこれらの規則により採択された関連する委任される行為及び実装行為に定めるセキュリティの要件の遵守は，この指令の下においてこの指令に定める対応する要件の遵守を同時に満たすことになる職務権限のある機関によって判断され得る。

In order to avoid gaps between or duplications of cybersecurity obligations imposed on entities in the aviation sector, national authorities under Regulations (EC) No 300/2008 [(11)] and (EU) 2018/1139 [(12)] of the European Parliament and of the Council and the competent authorities under this Directive should cooperate in relation to the implementation of cybersecurity risk-management measures and the supervision of compliance with those measures at national level. The compliance of an entity with the security requirements laid down in Regulations (EC) No 300/2008 and (EU) 2018/1139 and in the relevant delegated and implementing acts adopted pursuant to those Regulations could be considered by the competent authorities under this Directive to constitute compliance with the corresponding requirements laid down in this Directive.

(30) 法主体のサイバーセキュリティと物理的なセキュリティとの間の相互関連を考慮し，欧州議会及び理事会の指令(EU) 2022/2557[13]とこの指令との間で，一貫性のあるアプローチが確保されるべきである。それを達成するため，指令(EU) 2022/2557 の下で必須法主体として識別された法主体は，この指令の下にある基礎法主体として判断されるべきである。更に，各構成国は，その構成国の国内サイバーセキュリティ戦略が，サイバーなリスク，脅威及びインシデント，並びに，非サイバーなリスク，脅威及びインシデント，そして，監督の職務の執行に関する情報共有の過程における，この指令の下にあるその構成国の職務権限のある機関と指令(EU) 2022/2557 の下にある職務権

Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

12 民間航空の分野における共通規定及び欧州連合航空安全局の設置に関する，並びに，欧州議会及び理事会の規則(EC) No 2111/2005，規則(EC) No 1008/2008，規則(EU) No 996/2010，規則(EU) No 376/2014 及び指令 2014/30/EU，指令 2014/53/EU を改正し，欧州議会及び理事会の規則(EC) No 552/2004，規則(EC) No 216/2008 及び理事会規則(EEC) No 3922/91 を廃止する欧州議会及び理事会の 2018 年 7 月 4 日の規則(EU) 2018/1139 (OJ L 212, 22.8.2018, p. 1).

Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).

13 必須法主体の回復力に関する，及び，理事会指令 2008/114/EC を廃止する欧州議会及び理事会の 2022 年 12 月 14 日の指令(EU) 2022/2557（この官報の 164 頁参照）.

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (see page 164 of this Official Journal).

限のある機関との間の当該構成国内の拡大された調整のための政策枠組みを定めることを確保すべきである。この指令の下にある職務権限のある機関及び指令(EU) 2022/2557 の下にある職務権限のある機関は，とりわけ，必須法主体の識別，サイバーなリスク，脅威及びインシデントとの関係において，並びに，必須法主体によってとられたサイバーセキュリティの措置と物理的な措置，及び，そのような法主体と関連して実施された監督活動の結果を含め，必須法主体に影響を与える非サイバーなリスク，脅威及びインシデントとの関係において，協力し，かつ，不適切な遅滞なく，情報を交換すべきである。

In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) 2022/2557 of the European Parliament and of the Council[13] and this Directive. To achieve this, entities identified as critical entities under Directive (EU) 2022/2557 should be considered to be essential entities under this Directive. Moreover, each Member State should ensure that its national cybersecurity strategy provides for a policy framework for enhanced coordination within that Member State between its competent authorities under this Directive and those under Directive (EU) 2022/2557 in the context of information sharing about risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents, and the exercise of supervisory tasks. The competent authorities under this Directive and those under Directive (EU) 2022/2557 should cooperate and exchange information without undue delay, in particular in relation to the identification of critical entities, risks, cyber threats, and incidents as well as in relation to non-cyber risks, threats and incidents affecting critical entities, including the cybersecurity and physical measures taken by critical entities as well as the results of supervisory activities carried out with regard to such entities.

更に，この指令の下にある職務権限のある機関と指令(EU) 2022/2557 の下にある職務権限のある機関との間で監督活動を合理化するため，そして，関係する法主体に関する管理運営上の負担をミニマムなものにするため，当該職務権限のある機関は，インシデント通知の雛型と監督のプロセスを整合化するための努力を尽くすべきである。それが適切なときは，指令(EU) 2022/2557 の下にある職務権限のある機関は，この指令の下にある職務権限のある機関に対し，指令(EU) 2022/2557 の下において必須法主体として識別された法主体との関係において，この指令の下にある職務権限のある機関の監督の権限及び執行の権限を行使することを要請できるべきである。この指令の下にある職務権限のある機関及び指令(EU) 2022/2557 の下にある職務権限のある機関は，それが可能なときはリアルタイムで，その目的のために協力しかつ情報を交換すべきである。

Furthermore, in order to streamline supervisory activities between the competent authorities under this Directive and those under Directive (EU) 2022/2557 and in order to minimise the administrative burden for the entities concerned, those competent authorities should endeavour to harmonise incident notification templates and supervisory processes. Where appropriate, the competent authorities under Directive (EU) 2022/2557, should be able to request the competent authorities under this Directive to exercise their supervisory and enforcement powers in relation to an entity that is identified as a critical entity under Directive (EU) 2022/2557. The competent authorities under this Directive and those under

Directive (EU) 2022/2557 should, where possible in real time, cooperate and exchange information for that purpose.

(31) デジタルインフラ部門に属する法主体は，本質的に，ネットワーク及び情報システムを基礎としており，それゆえ，この指令により当該法主体に課される義務は，包括的な態様で，当該法主体のサイバーセキュリティのリスク管理の措置及び報告義務の一部としてそのようなシステムの物理的なセキュリティに対応すべきである。それらの事項はこの指令によって包摂されているので，指令(EU) 2022/ 2557 の第Ⅲ章，第Ⅳ章及び第Ⅵ章に定める義務は，そのような法主体に対して適用されない。

Entities belonging to the digital infrastructure sector are in essence based on network and information systems and therefore the obligations imposed on those entities pursuant to this Directive should address in a comprehensive manner the physical security of such systems as part of their cybersecurity risk-management measures and reporting obligations. Since those matters are covered by this Directive, the obligations laid down in Chapters III, IV and VI of Directive (EU) 2022/2557 do not apply to such entities.

(32) 信頼でき，回復力があり，かつ，安全なドメイン名システム（DNS）を支えること及び維持することは，インターネットの完全性を維持する上での鍵となる要素であり，かつ，その上にデジタルの経済と社会が依存するインターネットの継続的かつ安定した業務運営のために必須である。それゆえ，この指令は，トップレベルドメイン名レジストリ（TLD）及び DNS サービスのプロバイダに対して適用されるべきである。DNS サービスのプロバイダは，インターネットのエンドユーザのための公衆が利用可能で再帰的なドメイン名の解決サービスまたは第三者の利用のための権威あるドメイン名解決サービスを提供する法主体として理解されるべきである。ルート名サーバに対してこの指令を適用してはならない。

Upholding and preserving a reliable, resilient and secure domain name system (DNS) are key factors in maintaining the integrity of the internet and are essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to top-level-domain (TLD) name registries, and DNS service providers that are to be understood as entities providing publicly available recursive domain name resolution services for internet end-users or authoritative domain name resolution services for third-party usage. This Directive should not apply to root name servers.

(33) クラウドコンピューティングサービスは，そのような資源が複数の場所にわたって分散している場合を含め，共有可能なコンピュータ処理資源の拡張可能で伸縮可能なプールのオンデマンドの管理及びそのプールへの広域のリモートアクセスを実現可能にするデジタルサービスを包摂すべきである。コンピュータ処理資源は，ネットワーク，サーバまたはそれ以外のインフラ，オペレーティングシステム，ソフトウェア，ストレージ，アプリケーション及びサービスのような資源を含む。クラウドコンピューティングのサービスモデルは，就中，インフラストラクチャアズアサービス（IaaS），プラットフォームアズアサービス（PaaS），ソフトウェアアズアサービス（SaaS）及びネットワークアズアサービス（NaaS）を含む。クラウドコンピューティングの配置モデルは，プライベートク

ラウド，コミュニティクラウド，パブリッククラウド及びハイブリッドクラウドを含むべきである。クラウドコンピューティングサービス及び配置モデルは，ISO/IEC 17788: 2014 標準の下で定義されているサービス及び配置モデルという用語と同じ意味をもつ。サーバタイムやネットワークストレージのような，そのクラウドコンピューティングサービスのプロバイダによる人間の介在のない，コンピュータ処理能力の一方向的な自己提供のためのクラウドコンピューティング利用者の実現能力は，オンデマンド管理として説明され得る。

Cloud computing services should cover digital services that enable on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations. Computing resources include resources such as networks, servers or other infrastructure, operating systems, software, storage, applications and services. The service models of cloud computing include, inter alia, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and Network as a Service (NaaS). The deployment models of cloud computing should include private, community, public and hybrid cloud. The cloud computing service and deployment models have the same meaning as the terms of service and deployment models defined under ISO/IEC 17788:2014 standard. The capability of the cloud computing user to unilaterally self-provision computing capabilities, such as server time or network storage, without any human interaction by the cloud computing service provider could be described as on-demand administration.

「広域のリモートアクセス」という用語は，クラウドの実現能力がネットワーク全体で提供されており，かつ，携帯電話，タブレット，ラップトップ及びワークステーションを含め，異種のシンクライアントプラットフォームまたはシッククライアントプラットフォームの利用を促進する仕組みを介してアクセスされることを説明するために用いられる。「拡張可能」という用語は，要求の変動を取扱うために，その資源の地理的な場所とは無関係に，クラウドサービスプロバイダによって柔軟に割当てられるコンピュータ処理資源のことを指す。「伸縮可能なプール」という用語は，利用可能な資源を仕事量に応じて迅速に増減させるため，要求に応じて，提供及び解放されるコンピュータ処理の資源を説明するために用いられる。「共有可能な」という用語は，そのサービスに対する共通のアクセスを共有する複数の利用者に対して提供されるが，同一の電子機器からそのサービスが提供される場合でも個々の利用者毎に区分されてその処理が遂行されるコンピュータ処理の資源を説明するために用いられる。「分散」という用語は，ネットワーク上の異なるコンピュータまたは機器に所在しており，かつ，メッセージパッシングによって当該コンピュータまたは機器の中で通信及び調整するコンピュータ処理の資源を説明するために用いられる。

The term ‘broad remote access’ is used to describe that the cloud capabilities are provided over the network and accessed through mechanisms promoting use of heterogeneous thin or thick client platforms, including mobile phones, tablets, laptops and workstations. The term ‘scalable’ refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term ‘elastic pool’ is used to describe computing resources that are provided and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term ‘shareable’ is used to describe computing

resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment. The term 'distributed' is used to describe computing resources that are located on different networked computers or devices and which communicate and coordinate among themselves by message passing.

(34) 革新的な技術と新たなビジネスモデルの出現に鑑み，進化する顧客の需要に対応して，新たなクラウドコンピューティングサービスと配置モデルが域内市場に登場すると予想されている。その過程において，クラウドコンピューティングサービスは，データが生成または収集されている場所と近接しているときでさえ，そのようにして，伝統的なモデルから高度に分散したモデル（エッジコンピューティング）に遷移し，高度に分散的な形態で伝達されるかもしれない。

Given the emergence of innovative technologies and new business models, new cloud computing service and deployment models are expected to appear in the internal market in response to evolving customer needs. In that context, cloud computing services may be delivered in a highly distributed form, even closer to where data are being generated or collected, thus moving from the traditional model to a highly distributed one (edge computing).

(35) データセンターサービスのプロバイダから提供されるサービスは，常にクラウドコンピューティングサービスの形態で提供されるとは限らない。従って，データセンターは，常にクラウドコンピューティングインフラの一部を構成するとは限らない。それゆえ，ネットワーク及び情報システムの防護に対して示される全てのリスクを管理するため，この指令は，クラウドコンピューティングサービスではないデータセンターサービスのプロバイダを包摂すべきである。この指令の目的のために，「データセンターサービス」という用語は，配電及び環境管理のための全ての設備及びインフラと共にデータの記録保存，処理及び移転のサービスを提供する情報技術（IT）及びネットワークの機器の集中的な収容，相互接続及び運用に特化した構造物または構造物のグループを包含するサービスの提供を包摂すべきである。「データセンターサービス」という用語は，関係する法主体自身の目的のために，その法主体によって保有及び運用される社内データセンターに対して適用してはならない。

Services offered by data centre service providers may not always be provided in the form of a cloud computing service. Accordingly, data centres may not always constitute a part of cloud computing infrastructure. In order to manage all the risks posed to the security of network and information systems, this Directive should therefore cover providers of data centre services that are not cloud computing services. For the purposes of this Directive, the term 'data centre service' should cover provision of a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology (IT) and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control. The term 'data centre service' should not apply to in-house corporate data centres owned and operated by the entity concerned, for its own purposes.

(36) 調査研究活動は，新たな製品及びプロセスの開発において鍵となる役割を演ずる。それらの活動の多くは，商業上の目的のためにその法主体の調査研究の結果を共有，伝達または活用する法主体によって遂行されている。それゆえ，当該法主体は，その法主体のネットワーク及び情報システムの防護を域内市場の全体的なサイバーセキュリティの不可欠な部分とする価値連鎖の中において，重要な役割を演ずる者であり得る。調査研究組織は，商業上の目的のためにその法主体の調査研究の結果を活用するため，製品もしくはプロセスの製造もしくは開発，サービスの提供またはそれらのマーケティングのような，経済協力開発機構のフラスカティマニュアル 2015：調査研究及び試験的開発に関するデータの収集及び報告のためのガイドラインの意味における応用的な調査研究または試験的開発の遂行にその法主体の活動の必須の部分の焦点を当てている法主体を含むものとして理解されるべきである。

Research activities play a key role in the development of new products and processes. Many of those activities are carried out by entities that share, disseminate or exploit the results of their research for commercial purposes. Those entities can therefore be important players in value chains, which makes the security of their network and information systems an integral part of the overall cybersecurity of the internal market. Research organisations should be understood to include entities which focus the essential part of their activities on the conduct of applied research or experimental development, within the meaning of the Organisation for Economic Cooperation and Development's Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development, with a view to exploiting their results for commercial purposes, such as the manufacturing or development of a product or process, the provision of a service, or the marketing thereof.

(37) 相互依存が増大しているのは，エネルギー，輸送，デジタルインフラ，上下水道，医療，公行政の一定の側面のような部門において，並びに，構成国または民間の者によって保有，管理及び運用されている地上ベースのインフラに依存する一定のサービスの提供と関係する限り，それゆえ，欧州連合によってまたは欧州連合の代わりに欧州連合の宇宙計画の一部として保有，管理または運営されているインフラを包摂していない限り，宇宙のような部門において，欧州連合全域の鍵となるインフラを用いるサービス提供の国境を越えかつ相互依存するネットワークが増加していることの結果である。それらの相互依存があるということは，いかなる混乱も，当初は 1 つの法主体または 1 つの部門にそれが限定されていたとしても，より広範なカスケード効果をもち得るということ，潜在的には，域内市場全域にわたるサービスの伝達に対して広範囲かつ長期にわたる負の影響をもたらし得るということを意味する。COVID-19 パンデミックの間においてサイバー攻撃が激化したことは，蓋然性の低いリスクに直面する際における，相互依存性を増大させている社会の脆弱性を証明した。

The growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in sectors such as energy, transport, digital infrastructure, drinking water and waste water, health, certain aspects of public administration, as well as space in so far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not

covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programme. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The intensified cyberattacks during the COVID-19 pandemic have shown the vulnerability of increasingly interdependent societies in the face of low-probability risks.

(38) 国内統治構造の相違を考慮し，また，既に存在する部門別の覚書または欧州連合の監督組織及び規制組織を守るため，構成国は，この指令に基づくサイバーセキュリティに関して及び監督の職務に関して職責を負う 1 または複数の職務権限のある国内機関を指定または設置できるべきである。

In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, Member States should be able to designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks under this Directive.

(39) 国境を越える協力及び機関間の通信を容易にするため，また，この指令が実効的に実装され得るようにするため，欧州連合レベルのネットワーク及び情報システムの防護及び国境を越える協力と関連する問題の調整に関して職責を負う単一連絡部局を各構成国が指定する必要がある。

In order to facilitate cross-border cooperation and communication among authorities and to enable this Directive to be implemented effectively, it is necessary for each Member State to designate a single point of contact responsible for coordinating issues related to the security of network and information systems and cross-border cooperation at Union level.

(40) 単一連絡部局は，別の構成国の関連機関との間における，並びに，それが適切なときは，欧州委員会及び ENISA との間における，実効性のある国境を越える協力を確保すべきである。それゆえ，単一連絡部局は，CSIRT または職務権限のある機関の要請に応じて，国境を越える影響をもつ重大なインシデントの通知を，その影響を受ける別の構成国の単一連絡部局に対して転送する職務をもつべきである。国内レベルにおいて，単一連絡部局は，別の職務権限のある機関との間の円滑な部門横断の協力を実現できるべきである。単一連絡部局は，規則(EU) 2022/2554 の下にある職務権限のある機関からの金融の法主体と関係するインシデントに関する関連情報の名宛人ともなり得る。その単一連絡部局は，CSIRT またはこの指令の下にある職務権限のある機関に対し，しかるべく転送できるべきである。

The single points of contact should ensure effective cross-border cooperation with relevant authorities of other Member States and, where appropriate, with the Commission and ENISA. The single points of contact should therefore be tasked with forwarding notifications of significant incidents with cross-border impact to the single points of contact of other affected Member States upon the request of the CSIRT or

the competent authority. At national level, the single points of contact should enable smooth cross-sectoral cooperation with other competent authorities. The single points of contact could also be the addressees of relevant information about incidents concerning financial entities from the competent authorities under Regulation (EU) 2022/2554 which they should be able to forward, as appropriate, to the CSIRTs or the competent authorities under this Directive.

(41) 構成国は，インシデント及びリスクを防止し，検出し，それに対応し及びそれを緩和するため，技術上の能力及び組織上の実現能力の両者の面において，適切に具備すべきである。それゆえ，構成国は，この指令に基づく 1 または複数の CSIRT を設置または指定すべきであり，かつ，CSIRT が十分な資源及び技術上の実現能力をもつことを確保すべきである。CSIRT は，インシデント及びリスクに対処するための実効的かつ互換性のある実現能力を保証するため，そして，欧州連合レベルの効率的な協力を確保するため，この指令に定める要件を遵守すべきである。構成国は，既存のコンピュータ緊急対応チーム（CERT）を CSIRT として指定できるべきである。法主体と CSIRT との間の信頼関係を拡大するため，CSIRT が職務権限のある機関の一部であるときは，構成国は，とりわけ，情報共有及びその法主体に対して提供される援助の関係において，CSIRT によって提供される業務運営上の職務と，職務権限のある機関の監督活動との間の機能上の分離を検討できるべきである。

Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate incidents and risks. Member States should therefore establish or designate one or more CSIRTs under this Directive and ensure that they have adequate resources and technical capabilities. The CSIRTs should comply with the requirements laid down in this Directive in order to guarantee effective and compatible capabilities to deal with incidents and risks and to ensure efficient cooperation at Union level. Member States should be able to designate existing computer emergency response teams (CERTs) as CSIRTs. In order to enhance the trust relationship between the entities and the CSIRTs, where a CSIRT is part of a competent authority, Member States should be able to consider functional separation between the operational tasks provided by the CSIRTs, in particular in relation to information sharing and assistance provided to the entities, and the supervisory activities of the competent authorities.

(42) CSIRT は，インシデントを取り扱う職務をもつ。この職務は，大量の時として機微のデータの処理を含んでいる。構成国は，CSIRT が，情報の共有と処理のためのインフラ，並びに，CSIRT の業務運営の機密性と信頼性を確保する十分な能力のある職員をもつことを確保すべきである。CSIRT はまた，その点に関する行動準則を採択し得る。

The CSIRTs are tasked with incident handling. This includes the processing of large volumes of sometimes sensitive data. Member States should ensure that the CSIRTs have an infrastructure for information sharing and processing, as well as well-equipped staff, which ensures the confidentiality and trustworthiness of their operations. The CSIRTs could also adopt codes of conduct in that respect.

(43) 個人データに関し，CSIRT は，規則(EU) 2016/679 に従い，基礎法主体または重要法主体の要請に応じて，その法主体のサービスの提供のために使用されるネットワーク及び情報システムのプロアクティブスキャニングを提供できるべきである。それが適用可能なときは，構成国は，部門別 CSIRT の全てに関して同じレベルの技術上の実現能力を確保することを狙いとすべきである。構成国は，その構成国の CSIRT の発展において，ENISA の補助を要請できるべきである。

As regards personal data, the CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679, upon the request of an essential or important entity, a proactive scanning of the network and information systems used for the provision of the entity's services. Where applicable, Member States should aim to ensure an equal level of technical capabilities for all sectoral CSIRTs. Member States should be able to request the assistance of ENISA in developing their CSIRTs.

(44) CSIRT は，基礎法主体または重要法主体の要請に応じて，新たに発見されたサプライチェーン侵害または致命的な脆弱性と関連するその法主体の全体的な組織上のリスクを発見，理解及び管理するため，施設及び施設外の両者において，その法主体のインターネットと接続している資産を監視する能力をもつべきである。特権管理インタフェイスは実施中の緩和活動の速度に影響を及ぼすので，その法主体は，CSIRT に対し，その法主体が特権管理インタフェイスを走らせているかどうかを通知することが推奨されるべきである。

The CSIRTs should have the ability, upon an essential or important entity's request, to monitor the entity's internet-facing assets, both on and off premises, in order to identify, understand and manage the entity's overall organisational risks as regards newly identified supply chain compromises or critical vulnerabilities. The entity should be encouraged to communicate to the CSIRT whether it runs a privileged management interface, as this could affect the speed of undertaking mitigating actions.

(45) サイバーセキュリティに関する国際協力の重要性に鑑み，CSIRT は，この指令によって設置される CSIRT ネットワークに加え，国際的な協力ネットワークに参加できるべきである。それゆえ，CSIRT の職務を遂行する目的のために，CSIRT 及び職務権限のある機関は，第三国のコンピュータセキュリティインシデント対応チームとの間で，または，第三国の職務権限のある機関との間で，第三国に対する個人データの移転に関する欧州連合のデータ保護法に基づく条件，就中，規則(EU) 2016/679 の第 49 条に適合することを条件として，個人情報を含め，情報を交換できるべきである。

Given the importance of international cooperation on cybersecurity, the CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive. Therefore, for the purpose of carrying out their tasks, the CSIRTs and the competent authorities should be able to exchange information, including personal data, with the national computer security incident response teams or competent authorities of third countries provided that the conditions under Union data protection law for transfers of personal data to third countries, inter alia those of Article 49 of Regulation (EU) 2016/679, are met.

(46) この指令の目的に適合するため，並びに，職務権限のある機関及び CSIRT がこの指令に定める職務を遂行できるようにするための十分な資源を確保することは，必須である。構成国は，この指令によりその構成国内のサイバーセキュリティに関する職責を負う公的法主体の職務の遂行と関係する必要な支出を包摂する資金提供の仕組みを国内レベルで導入できる。そのような仕組みは，欧州連合法を遵守すべきであり，かつ，比例的かつ非差別であるべきであり，かつ，安全なサービスを提供するための異なるアプローチを考慮に入れるべきである。

Ensuring adequate resources to meet the objectives of this Directive and to enable the competent authorities and the CSIRTs to carry out the tasks laid down herein is essential. The Member States can introduce at the national level a financing mechanism to cover necessary expenditure in relation to the conduct of tasks of public entities responsible for cybersecurity in the Member State pursuant to this Directive. Such mechanism should comply with Union law and should be proportionate and non-discriminatory and should take into account different approaches to providing secure services.

(47) CSIRT ネットワークは，信用と信頼を強化することに寄与すること，及び，構成国間の業務運営上の迅速かつ実効的な協力を促進することに寄与することを継続すべきである。欧州連合レベルの業務運営上の協力を拡大するため，CSIRT ネットワークは，Europol のような，サイバーセキュリティ政策に包摂される欧州連合の組織及び部局を CSIRT ネットワークの仕事に参加させるために招請することを検討すべきである。

The CSIRTs network should continue to contribute to strengthening confidence and trust and to promote swift and effective operational cooperation among Member States. In order to enhance operational cooperation at Union level, the CSIRTs network should consider inviting Union bodies and agencies involved in cybersecurity policy, such as Europol, to participate in its work.

(48) 高いレベルのサイバーセキュリティを達成及び維持するという目的のために，この指令の下で要求される国内サイバーセキュリティ戦略は，サイバーセキュリティの分野における戦略上の目標及び優先順序並びにそれらを達成するための統治を提供する一貫性のある枠組みによって構成されるべきである。当該戦略は，1 または複数の立法文書または非立法文書によって組成される。

For the purpose of achieving and maintaining a high level of cybersecurity, the national cybersecurity strategies required under this Directive should consist of coherent frameworks providing strategic objectives and priorities in the area of cybersecurity and the governance to achieve them. Those strategies can be composed of one or more legislative or non-legislative instruments.

(49) サイバー衛生の基本方針は，ネットワーク及び情報システムのインフラ，ハードウェア，ソフトウェア及びオンラインアプリケーションのセキュリティ，並びに，法主体が依拠する事業者またはエンドユーザのデータを保護するための基礎を提供する。ソフトウェア及びハードウェアのアップデート，パスワードの変更，新たなインストールの管理，管理者レベルのアクセスアカウントの制限，

並びに，データのバックアップを含め，実務の共通の基線のセットによって組成されるサイバー衛生の基本方針は，プロアクティブな準備態勢の枠組み，並びに，インシデントまたはサイバーな脅威の場合における全体的な安全性及び防護を実現可能にする。ENISA は，構成国のサイバー衛生の基本方針を監視及び分析すべきである。

Cyber hygiene policies provide the foundations for protecting network and information system infrastructures, hardware, software and online application security, and business or end-user data upon which entities rely. Cyber hygiene policies comprising a common baseline set of practices, including software and hardware updates, password changes, the management of new installs, the limitation of administrator-level access accounts, and the backing-up of data, enable a proactive framework of preparedness and overall safety and security in the event of incidents or cyber threats. ENISA should monitor and analyse Member States' cyber hygiene policies.

(50) サイバーセキュリティの認識及びサイバー衛生は，とりわけ，サイバー攻撃において使用されることが増えているネット接続された機器の数が増加していることに照らし，欧州連合内のサイバーセキュリティのレベルを拡大するために必須である。欧州連合レベルの評価は，域内市場内のそのようなリスクの共通理解を確保することを助け得るが，そのような機器と関連するリスクの全体的な認識を拡大するための努力が尽くされるべきである。

Cybersecurity awareness and cyber hygiene are essential to enhance the level of cybersecurity within the Union, in particular in light of the growing number of connected devices that are increasingly used in cyberattacks. Efforts should be made to enhance the overall awareness of risks related to such devices, while assessments at Union level could help ensure a common understanding of such risks within the internal market.

(51) 構成国は，人工知能を含め，その技術を使用することがサイバー攻撃の検出と防止を向上させ得るものであり，より実効的に資源がサイバー攻撃に向けられることを実現可能とする全ての革新的な技術の利用を推奨すべきである。それゆえ，構成国は，その構成国の国内サイバーセキュリティ戦略の中で，そのような技術の利用，とりわけ，サイバーセキュリティにおける自動化または半自動化されたツールの利用を容易にするための調査研究及び開発の活動を推奨し，また，それが関連するときは，そのような技術の利用者を訓練するため，及び，そのような技術を向上させるために必要なデータを共有することを推奨すべきである。人工知能を含め，全ての革新的な技術の利用は，データの正確性，データのミニマム化，公正性及び透明性というデータ保護の基本原則，並びに，最新の暗号技術のような，データの防護を含め，欧州連合のデータ保護法を遵守すべきである。規則(EU) 2016/679 に定めるバイデザイン及びバイデフォルトのデータ保護の要件は，全面的に活用されるべきである。

Member States should encourage the use of any innovative technology, including artificial intelligence, the use of which could improve the detection and prevention of cyberattacks, enabling resources to be diverted towards cyberattacks more effectively. Member States should therefore encourage in their

national cybersecurity strategy activities in research and development to facilitate the use of such technologies, in particular those relating to automated or semi-automated tools in cybersecurity, and, where relevant, the sharing of data needed for training users of such technology and for improving it. The use of any innovative technology, including artificial intelligence, should comply with Union data protection law, including the data protection principles of data accuracy, data minimisation, fairness and transparency, and data security, such as state-of-the-art encryption. The requirements of data protection by design and by default laid down in Regulation (EU) 2016/679 should be fully exploited.

(52) オープンソースのサイバーセキュリティツールとアプリケーションは，より高い程度のオープン性に寄与し得るものであり，また，産業界の技術革新の効率性に対して積極的な影響をもち得る。オープンスタンダードは，セキュリティツール間の相互運用性と，産業界の利害関係者が防護を受益することを容易にする。オープンソースのサイバーセキュリティツールとアプリケーションは，供給者の多様化を実現可能にする，より拡大された開発者コミュニティを強化し得る。オープンソースは，サイバーセキュリティ関連ツールのより透明性のある検証プロセスと，コミュニティ主導型の脆弱性発見プロセスを導き得る。それゆえ，構成国は，透明性によるセキュリティの一部としてのオープンデータとオープンソースの利用と関連する基本方針を推進することにより，オープンソースのソフトウェアとオープンスタンダードの利用を促進できるべきである。オープンソースのサイバーセキュリティツールの導入及び持続的な利用を促進する基本方針は，実装のための大きなコストと直面している小企業及び中規模企業にとって特に重要性をもつ。そのコストは，特定のアプリケーションまたはツールの必要性を削減することによって，ミニマム化され得る。

Open-source cybersecurity tools and applications can contribute to a higher degree of openness and can have a positive impact on the efficiency of industrial innovation. Open standards facilitate interoperability between security tools, benefitting the security of industrial stakeholders. Open-source cybersecurity tools and applications can leverage the wider developer community, enabling diversification of suppliers. Open source can lead to a more transparent verification process of cybersecurity related tools and a community-driven process of discovering vulnerabilities. Member States should therefore be able to promote the use of open-source software and open standards by pursuing policies relating to the use of open data and open-source as part of security through transparency. Policies promoting the introduction and sustainable use of open-source cybersecurity tools are of particular importance for small and medium-sized enterprises facing significant costs for implementation, which could be minimised by reducing the need for specific applications or tools.

(53) 都市交通網を向上させること，水供給施設及び塵処理施設をアップグレードすること，並びに，建物の光熱の効率性を増加させることという目的のために，公共役務提供は，都市内のデジタルネットワークと接続されることが増加している。それらのデジタル化された公共役務提供は，サイバー攻撃に対して脆弱であり，また，サイバー攻撃が成功している場合において，それらの公共役務提供の相互接続のゆえに，市民に対して大規模に危害を及ぼすリスクを走らせている。構成国は，その構成国の国内サイバーセキュリティ戦略の一部として，そのようなネット接続された都市またはスマート都市の発展とそれらの発展が社会に対して与える潜在的な影響に対処する基

本方針を策定すべきである。

Utilities are increasingly connected to digital networks in cities, for the purpose of improving urban transport networks, upgrading water supply and waste disposal facilities and increasing the efficiency of lighting and the heating of buildings. Those digitalised utilities are vulnerable to cyberattacks and run the risk, in the event of a successful cyberattack, of harming citizens at a large scale due to their interconnectedness. Member States should develop a policy that addresses the development of such connected or smart cities, and their potential effects on society, as part of their national cybersecurity strategy.

(54) 近年, 欧州連合は, マルウェアがデータとシステムを暗号化し, その開放のための身代金の支払いを要求する, ランサムウェア攻撃の指数関数的な増加と直面してきた。ランサムウェア攻撃の頻度と深刻度の増大は, 異なる攻撃パターン, 「ランサムウェアアズアサービス」のような犯罪的ビジネスモデル及び暗号通貨, 身代金の要求, 並びに, サプライチェーン攻撃の増加のような幾つかの要因によって駆動され得る。構成国は, その構成国の国内サイバーセキュリティ戦略の一部として, ランサムウェア攻撃の増加に対処する基本方針を策定すべきである。

In recent years, the Union has faced an exponential increase in ransomware attacks, in which malware encrypts data and systems and demands a ransom payment for release. The increasing frequency and severity of ransomware attacks can be driven by several factors, such as different attack patterns, criminal business models around ‘ransomware as a service’ and cryptocurrencies, ransom demands, and the rise of supply chain attacks. Member States should develop a policy addressing the rise of ransomware attacks as part of their national cybersecurity strategy.

(55) サイバーセキュリティの分野における官民パートナーシップ（PPP）は, 知識の交換, ベストプラクティスの共有及び利害関係者間における共通のレベルの理解の構築のための適切な枠組みを提供できる。構成国は, サイバーセキュリティに特化した PPP の構築を支える基本方針を促進すべきである。それらの基本方針は, 就中, 包摂される利害関係者の範囲, 統治モデル, 利用可能な資金提供の選択肢, 及び, 参加する利害関係者間における PPP と関連する相互のやりとりを明確化すべきである。PPP は, 情報交換, 早期警戒, サイバーな脅威及びインシデントの演習, 危機管理及び回復力の計画策定を含む最新のサービス及びプロセスの開発において職務権限のある機関を補助するための民間部門の法主体の専門知識を強化し得る。

Public-private partnerships (PPPs) in the field of cybersecurity can provide an appropriate framework for knowledge exchange, the sharing of best practices and the establishment of a common level of understanding among stakeholders. Member States should promote policies underpinning the establishment of cybersecurity-specific PPPs. Those policies should clarify, inter alia, the scope and stakeholders involved, the governance model, the available funding options and the interaction among participating stakeholders with regard to PPPs. PPPs can leverage the expertise of private-sector entities to assist the competent authorities in developing state-of-the-art services and processes including

information exchange, early warnings, cyber threat and incident exercises, crisis management and resilience planning.

(56) 構成国は，その構成国の国内サイバーセキュリティ戦略の中で，小企業及び中規模企業のサイバーセキュリティ上の個別の必要性に対処すべきである。小規企業及び中規模企業は，欧州連合全域の産業及び事業の市場の大きな割合を占めており，かつ，しばしば，労働者が自宅で働き，事業がオンラインで遂行されることが増えている，よりネット接続された世界における新たな事業実務への適応とデジタル環境への適応に苦しんでいる。幾つかの小企業及び中規模企業は，サイバーな認識の低さ，リモートの IT セキュリティの欠如，高コストのサイバーセキュリティソリューション，及び，ランサムウェアのような脅威のレベルの増大といったサイバーセキュリティ上の個別の検討課題に直面しており，それらの検討課題に関し，それらの企業は，ガイドと補助を受けるべきである。小企業及び中規模企業は，当該企業の厳格ではないサイバーセキュリティのリスク管理の措置及び攻撃管理のゆえに，及び，当該企業が限定されたセキュリティ資源しかもっていないということのゆえに，サプライチェーン攻撃の標的となることが増えている。そのようなサプライチェーン攻撃は，小企業及び中規模企業とそれらの企業の孤立した業務運営に影響を与えるだけではなく，それらの企業がサプライを提供している法主体に対するより大きな攻撃のカスケード効果ももつ。構成国は，その構成国の国内サイバーセキュリティ戦略を介して，小企業及び中規模企業が，当該企業のサプライチェーンが直面している検討課題に対処することを助けるべきである。構成国は，国内レベルまたは地域レベルで，サイバーセキュリティと関連する問題に関し，小企業及び中規模企業に対してガイド及び補助を提供し，または，それらの企業に対してガイド及び補助のための適切な組織を指示する，小企業及び中規模企業のための連絡先をもつべきである。構成国は，それらの実現能力を欠いているマイクロ企業及び小企業のために，Web サイトの設定及びログ記録を実現できるようにすることのようなサービスを提供することも推奨される。

Member States should, in their national cybersecurity strategies, address the specific cybersecurity needs of small and medium-sized enterprises. Small and medium-sized enterprises represent, across the Union, a large percentage of the industrial and business market and often struggle to adapt to new business practices in a more connected world and to the digital environment, with employees working from home and business increasingly being conducted online. Some small and medium-sized enterprises face specific cybersecurity challenges such as low cyber-awareness, a lack of remote IT security, the high cost of cybersecurity solutions and an increased level of threat, such as ransomware, for which they should receive guidance and assistance. Small and medium-sized enterprises are increasingly becoming the target of supply chain attacks due to their less rigorous cybersecurity risk-management measures and attack management, and the fact that they have limited security resources. Such supply chain attacks not only have an impact on small and medium-sized enterprises and their operations in isolation but can also have a cascading effect on larger attacks on entities to which they provided supplies. Member States should, through their national cybersecurity strategies, help small and medium-sized enterprises to address the challenges faced in their supply chains. Member States should have a point of contact for small and medium-sized enterprises at national or regional level, which either provides guidance and

assistance to small and medium-sized enterprises or directs them to the appropriate bodies for guidance and assistance with regard to cybersecurity related issues. Member States are also encouraged to offer services such as website configuration and logging enabling to microenterprises and small enterprises that lack those capabilities.

(57) その構成国の国内サイバーセキュリティ戦略の一部として，構成国は，拡大された防衛戦略の一部としての能動的サイバー防御の促進に関する基本方針を採択すべきである。受動的に対応するのではなく，能動的なサイバー防御は，被攻撃ネットワークの内外に配置された実現能力を束ねた，能動的な態様によるネットワークのセキュリティ侵害の防止，検出，監視，分析及び緩和である。これは，構成国が，一定の法主体に対し，セルフチェックシステム，検出ツール及び削除サービスを含め，無料のサービスやツールを提供することを含み得る。脅威の情報と分析，サイバー活動の警報及び対処の活動を迅速かつ自動的に供給及び理解するための能力は，ネットワーク及び情報システムに対する攻撃を成功裏に防止，検出，対処及びブロックするための努力の統合を実現可能とするために重要である。能動的なサイバー防御は，攻撃的な手段を排除した防衛戦略を基礎とする。

As part of their national cybersecurity strategies, Member States should adopt policies on the promotion of active cyber protection as part of a wider defensive strategy. Rather than responding reactively, active cyber protection is the prevention, detection, monitoring, analysis and mitigation of network security breaches in an active manner, combined with the use of capabilities deployed within and outside the victim network. This could include Member States offering free services or tools to certain entities, including self-service checks, detection tools and takedown services. The ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and response action is critical to enable a unity of effort in successfully preventing, detecting, addressing and blocking attacks against network and information systems. Active cyber protection is based on a defensive strategy that excludes offensive measures.

(58) ネットワーク及び情報システムにおける脆弱性の悪用は，重大な混乱と危害を生じさせ得るので，そのような脆弱性を迅速に発見すること及び是正することは，リスクを削減する際の重要な要素の 1 つである。それゆえ，ネットワーク及び情報システムを開発または管理運営する法主体は，脆弱性が発見されたときに脆弱性を取扱うための適切な手続を設けるべきである。脆弱性は，しばしば，第三者によって発見され，開示されるので，ICT 製品または ICT サービスの製造者または提供者は，第三者から脆弱性情報を受けるために必要となる手続も設けるべきである。その点に関し，国際規格 ISO/IEC 30111 及び ISO/IEC 29147 は，脆弱性の取扱及び脆弱性開示に関するガイドを提供している。報告者である自然人及び法人と ICT 製品または ICT サービスの製造者または提供者との間の調整を強化することは，脆弱性開示の任意の枠組みを促進する目的のために，とりわけ重要である。調整された脆弱性開示は，詳細な脆弱性情報が第三者または公衆に開示される前に，その脆弱性を診断及び解決できるようにする態様で，そのプロセスを介して，潜在的に脆弱性のある ICT 製品または ICT サービスの製造者または提供者に対し，脆弱性が報告される構造化されたプロセスを定める。調整された脆弱性開示は，報告者である自然人及び法人と潜

在的に脆弱性のあるICT製品またはICTサービスの製造者または提供者との間の，脆弱性の解決及び公表の時機に関する調整も含むべきである。

Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying such vulnerabilities is an important factor in reducing risk. Entities that develop or administer network and information systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and disclosed by third parties, the manufacturer or provider of ICT products or ICT services should also put in place the necessary procedures to receive vulnerability information from third parties. In that regard, international standards ISO/IEC 30111 and ISO/IEC 29147 provide guidance on vulnerability handling and vulnerability disclosure. Strengthening the coordination between reporting natural and legal persons and manufacturers or providers of ICT products or ICT services is particularly important for the purpose of facilitating the voluntary framework of vulnerability disclosure. Coordinated vulnerability disclosure specifies a structured process through which vulnerabilities are reported to the manufacturer or provider of the potentially vulnerable ICT products or ICT services in a manner allowing it to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. Coordinated vulnerability disclosure should also include coordination between the reporting natural or legal person and the manufacturer or provider of the potentially vulnerable ICT products or ICT services as regards the timing of remediation and publication of vulnerabilities.

(59) 欧州委員会，ENISA 及び構成国は，サイバーセキュリティのリスク管理の分野において，例えば，サプライチェーンのセキュリティ評価，情報共有及び脆弱性開示の分野において，国際標準と産業界の既存のベストプラクティスを揃えることの推進を継続すべきである。

The Commission, ENISA and the Member States should continue to foster alignments with international standards and existing industry best practices in the area of cybersecurity risk management, for example in the areas of supply chain security assessments, information sharing and vulnerability disclosure.

(60) 構成国は，ENISA と協力して，関連する国内基本方針を設けることにより，調整された脆弱性開示を促進するための措置を講ずるべきである。その構成国の国内基本方針の一部として，構成国は，可能な範囲内で，国内法に従い，脆弱性の調査研究者が刑事上の法的責任に潜在的に晒されていることを含め，それらの者が直面している検討課題に対処することを狙いとすべきである。幾つかの構成国においては，脆弱性を調査研究する自然人及び法人が刑事及び民事の法的責任に晒され得ることに鑑み，構成国は，情報セキュリティの調査研究者の非訴追及びそれらの者の活動に関する民事上の法的責任の免除に関する指針を採択することが推奨される。

Member States, in cooperation with ENISA, should take measures to facilitate coordinated vulnerability disclosure by establishing a relevant national policy. As part of their national policy, Member States should aim to address, to the extent possible, the challenges faced by vulnerability researchers, including their potential exposure to criminal liability, in accordance with national law. Given that natural and legal

persons researching vulnerabilities could in some Member States be exposed to criminal and civil liability, Member States are encouraged to adopt guidelines as regards the non-prosecution of information security researchers and an exemption from civil liability for their activities.

(61) 構成国は，必要に応じて，1 つの CSIRT を，報告者である自然人または法人と，脆弱性による影響を受けている可能性のある ICT 製品または ICT サービスの製造者または提供者との間の信頼できる媒介者として活動する調整者として指定すべきである。調整者として指定された CSIRT の職務は，関係する法主体を特定すること及びその法主体と連絡をとること，脆弱性の報告者である自然人または法人を補助すること，複数の法主体に影響を与える脆弱性の開示日程を交渉すること及びその脆弱性を管理すること（複数関係者の調整された脆弱性開示）を含めるべきである。報告された脆弱性が，複数の構成国の法主体に対して重大な影響をもち得るときは，調整者として指定された CSIRT は，それが適切なときは，CSIRT ネットワーク内において，協力すべきである。

Member States should designate one of its CSIRTs as a coordinator, acting as a trusted intermediary between the reporting natural or legal persons and the manufacturers or providers of ICT products or ICT services, which are likely to be affected by the vulnerability, where necessary. The tasks of the CSIRT designated as coordinator should include identifying and contacting the entities concerned, assisting the natural or legal persons reporting a vulnerability, negotiating disclosure timelines and managing vulnerabilities that affect multiple entities (multi-party coordinated vulnerability disclosure). Where the reported vulnerability could have significant impact on entities in more than one Member State, the CSIRTs designated as coordinators should cooperate within the CSIRTs network, where appropriate.

(62) 脆弱性が影響を及ぼす ICT 製品及び ICT サービスに関する正確かつ適時の情報へのアクセスは，拡大されたサイバーセキュリティのリスク管理に寄与する。脆弱性に関する公衆が利用可能な情報源は，その法主体にとって及びその法主体のサービスの利用者にとってだけではなく，職務権限のある機関及び CSIRT にとっても，重要なツールの 1 つである。それゆえ，ENISA は，欧州脆弱性データベースを設置すべきである。そのデータベースにおいて，その法主体がこの指令の適用範囲内にあるかどうかに拘わらず，法主体，その法主体へのネットワーク及び情報システムの供給者，並びに，職務権限のある機関及び CSIRT は，任意ベースで，利用者が適切な緩和措置をとることができるようにする目的のために，周知の脆弱性を開示及び登録できる。当該データベースの狙いは，欧州連合の法主体に対してリスクによって示されている固有の検討課題に対処することにある。更に，ENISA は，法主体に対してその法主体の脆弱性に関して緩和措置を講ずるための時間を与えるため，そして，最新のサイバーセキュリティのリスク管理の措置並びに機械読取可能なデータセット及び対応するインタフェイスを採用するための公表過程に関する適切な手続を設けるべきである。脆弱性の開示の文化を推進するため，開示は，報告者である自然人または法人に対し，有害な影響をもってはならない。

Access to correct and timely information about vulnerabilities affecting ICT products and ICT services contributes to an enhanced cybersecurity risk management. Sources of publicly available information

about vulnerabilities are an important tool for the entities and for the users of their services, but also for the competent authorities and the CSIRTs. For that reason, ENISA should establish a European vulnerability database where entities, regardless of whether they fall within the scope of this Directive, and their suppliers of network and information systems, as well as the competent authorities and the CSIRTs, can disclose and register, on a voluntary basis, publicly known vulnerabilities for the purpose of allowing users to take appropriate mitigating measures. The aim of that database is to address the unique challenges posed by risks to Union entities. Furthermore, ENISA should establish an appropriate procedure regarding the publication process in order to give entities the time to take mitigating measures as regards their vulnerabilities and employ state-of-the-art cybersecurity risk-management measures as well as machine-readable datasets and corresponding interfaces. To encourage a culture of disclosure of vulnerabilities, disclosure should have no detrimental effects on the reporting natural or legal person.

(63) 類似の脆弱性登録所またはデータベースは存在しているが，それらは，欧州連合内に拠点のない法主体によってホストされ，維持管理されている。ENISA によって維持管理される欧州脆弱性データベースは，その脆弱性が公衆に開示される前の公表過程と関連する改善された透明性を提供し，また，類似のサービスの混乱または途絶の場合における回復力を提供するであろう。可能な範囲内で，努力の重複と避け，そして，相補性を求めるため，ENISA は，第三国の管轄権の下にある類似の登録所またはデータベースとの間で，構造化された協力協定を結ぶことの可能性を模索すべきである。とりわけ，ENISA は，共通脆弱性及び危殆(CVE)システムの運営者との間の緊密な協力の可能性を模索すべきである。

Although similar vulnerability registries or databases exist, they are hosted and maintained by entities which are not established in the Union. A European vulnerability database maintained by ENISA would provide improved transparency regarding the publication process before the vulnerability is publicly disclosed, and resilience in the event of a disruption or an interruption of the provision of similar services. In order, to the extent possible, to avoid a duplication of efforts and to seek complementarity, ENISA should explore the possibility of entering into structured cooperation agreements with similar registries or databases that fall under third-country jurisdiction. In particular, ENISA should explore the possibility of close cooperation with the operators of the Common Vulnerabilities and Exposures (CVE) system.

(64) 協力グループは，戦略的な協力及び情報交換を支援及び促進し，かつ，構成国間の信頼と信用を強化すべきである。協力グループは，2 年毎に，作業計画を作成すべきである。作業計画は，協力グループの目的及び職務を実装するためにその作業グループによって実施される活動を含めるべきである。この指令に基づく最初の作業計画の作成のための時間枠は，協力グループの作業における潜在的な混乱を避けるため，指令(EU) 2016/1148 の下で作成された直近の作業計画の時間枠と揃えられるべきである。

The Cooperation Group should support and facilitate strategic cooperation and the exchange of information, as well as strengthen trust and confidence among Member States. The Cooperation Group should establish a work programme every two years. The work programme should include the actions to

be undertaken by the Cooperation Group to implement its objectives and tasks. The timeframe for the establishment of the first work programme under this Directive should be aligned with the timeframe of the last work programme established under Directive (EU) 2016/1148 in order to avoid potential disruptions in the work of the Cooperation Group.

(65) ガイド文書を策定する際，協力グループは，一貫性を保って，国内のソリューションと経験をマッピングし，国内のアプローチに関する協力グループの成果の影響を評価し，実装上の検討課題を討論し，かつ，とりわけ，構成国の間においてこの指令の国内法化を揃えることを容易にすること，既存の規定のより良い実装を介して対処されるべきことに関して，個別の推奨事項を作成すべきである。協力グループは，欧州連合全域にわたって個別の各部門に対して適用されるサイバーセキュリティのソリューションの互換性を向上させるため，国内ソリューションをマッピングすることもできる。このことは，国際的な性質または国境を越える性質をもつ部門と特に関連する。

When developing guidance documents, the Cooperation Group should consistently map national solutions and experiences, assess the impact of Cooperation Group deliverables on national approaches, discuss implementation challenges and formulate specific recommendations, in particular as regards facilitating an alignment of the transposition of this Directive among Member States, to be addressed through a better implementation of existing rules. The Cooperation Group could also map the national solutions in order to promote compatibility of cybersecurity solutions applied to each specific sector across the Union. This is particularly relevant to sectors that have an international or cross-border nature.

(66) 協力グループは，柔軟なフォーラムを維持すべきであり，かつ，利用可能な資源を考慮に入れつつ，変化しつつある新たな政策上の優先順序及び検討課題に対応できるべきである。協力グループは，協力グループによって遂行される活動を討議するため，欧州連合全域からの関連する民間利害関係者との定期的な共同会合を計画でき，また，生起する政策上の検討課題に関するデータ及び入力を収集できる。加えて，協力グループは，ランサムウェアのような，サイバーな脅威またはインシデントの現況の定期的な評価を遂行すべきである。欧州連合レベルの協力を拡大するため，協力グループは，欧州議会，Europol，欧州データ保護委員会，規則(EU) 2018/1139によって設置された欧州連合航空安全局，並びに，欧州議会及び理事会の規則(EU) 2021/696[14]によって設置された欧州連合宇宙計画局のような，サイバーセキュリティの政策に関与している欧州連合の関連する機関，組織，事務局及び部局を，協力グループの作業の中に参加させるために招請することを検討すべきである。

---

[14] 欧州連合宇宙計画及び欧州連合宇宙計画局を設ける，並びに，規則(EU) No 912/2010，規則(EU) No 1285/2013，規則(EU) No 377/2014 及び決定 No 541/2014/EU を廃止する欧州議会及び理事会の 2021 年 4 月 28 日の規則(EU) 2021/696 (OJ L 170, 12.5.2021, p. 69).
Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU (OJ L 170, 12.5.2021, p. 69).

The Cooperation Group should remain a flexible forum and be able to react to changing and new policy priorities and challenges while taking into account the availability of resources. It could organise regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Cooperation Group and gather data and input on emerging policy challenges. Additionally, the Cooperation Group should carry out a regular assessment of the state of play of cyber threats or incidents, such as ransomware. In order to enhance cooperation at Union level, the Cooperation Group should consider inviting relevant Union institutions, bodies, offices and agencies involved in cybersecurity policy, such as the European Parliament, Europol, the European Data Protection Board, the European Union Aviation Safety Agency, established by Regulation (EU) 2018/1139, and the European Union Agency for Space Programme, established by Regulation (EU) 2021/696 of the European Parliament and the Council(14), to participate in its work.

(67) 職務権限のある機関及び CSIRT は，構成国間における協力を改善し，信頼を強化するため，個別の枠組みの範囲内において，かつ，それが適用可能なときは，そのような交換制度に参加する官吏に対して要求されるセキュリティクリアランスに服して，別の構成国の官吏の人事交換制度に参加できるべきである。職務権限のある機関は，別の構成国の官吏が，ホストである職務権限のある機関またはホスト CSIRT の活動において，実効的に役割を果たすことができるようにするために必要となる措置を講ずるべきである。

The competent authorities and the CSIRTs should be able to participate in exchange schemes for officials from other Member States, within a specific framework and, where applicable, subject to the required security clearance of officials participating in such exchange schemes, in order to improve cooperation and strengthen trust among Member States. The competent authorities should take the necessary measures to enable officials from other Member States to play an effective role in the activities of the host competent authority or the host CSIRT.

(68) 構成国は，既存の協力ネットワークを介して，とりわけ，欧州サイバー危機連絡組織ネットワーク（EU-CyCLONe），CSIRT ネットワーク及び協力グループを介して，委員会勧告(EU) 2017/1584[15]に定める EU サイバーセキュリティ危機対応枠組みの設置に寄与すべきである。EU-CyCLONe 及び CSIRT ネットワークは，当該協力の詳細を定め，職務の重複を避ける手続覚書を基礎として協力すべきである。EU-CyCLONe の手続規則は，ネットワークの役割，協力の手段，他の関連する関与者との間のやりとり及び情報共有のための雛型並びに通信手段を含め，それによって当該ネットワークが機能すべき手立てを更に定めるべきである。欧州連合レベルの危機管理に関し，関連する関与者は，理事会実装決定(EU) 2018/1993[16]に基づく EU 統合政治的危機対応覚書

[15] 大規模なサイバーセキュリティのインシデント及び危機への調整された対応に関する 2017 年 9 月 13 日の委員会勧告(EU) 2017/1584 (OJ L 239, 19.9.2017, p. 36).
Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

[16] EU 統合政治的危機対応覚書に関する 2018 年 12 月 11 日の理事会実装決定(EU) 2018/1993 (OJ L 320,

（IPCR 覚書）に依るべきである。欧州委員会は，当該目的のために，ARGUS ハイレベル部門横断危機調整プロセスを用いるべきである。その危機が，重要な対外的な局面または共通保安防衛政策の局面を伴うときは，欧州対外行動庁危機管理メカニズムが発動されるべきである。

Member States should contribute to the establishment of the EU Cybersecurity Crisis Response Framework as set out in Commission Recommendation (EU) 2017/1584 (15) through the existing cooperation networks, in particular the European cyber crisis liaison organisation network (EU-CyCLONe), the CSIRTs network and the Cooperation Group. EU-CyCLONe and the CSIRTs network should cooperate on the basis of procedural arrangements that specify the details of that cooperation and avoid any duplication of tasks. EU-CyCLONe's rules of procedure should further specify the arrangements through which that network should function, including the network's roles, means of cooperation, interactions with other relevant actors and templates for information sharing, as well as means of communication. For crisis management at Union level, relevant parties should rely on the EU Integrated Political Crisis Response arrangements under Council Implementing Decision (EU) 2018/1993 (16) (IPCR arrangements). The Commission should use the ARGUS high-level cross-sectoral crisis coordination process for that purpose. If the crisis entails an important external or Common Security and Defence Policy dimension, the European External Action Service Crisis Response Mechanism should be activated.

(69) 勧告(EU) 2017/1584 の別紙に従い，大規模なサイバーセキュリティのインシデントとは，そのインシデントに対応するための構成国の能力を超過するレベルの混乱を生じさせるインシデント，または，少なくとも 2 つの構成国に対して重大な影響をもつインシデントのことを意味すべきである。そのインシデントの原因及び影響の別に応じて，大規模なサイバーセキュリティのインシデントは，エスカレートし，域内市場の適正な稼働ができなくなり，または，複数の構成国もしくは欧州連合全域の法主体または市民に対する公共の保安及び防護の上での重大なリスクを示す本格的な危機に発展し得る。そのようなインシデントの非常に広範な影響範囲に鑑み，また，ほとんどの場合において，そのようなインシデントの国境を越える性質に鑑み，構成国，並びに，関連する欧州連合の機関，組織，事務局及び部局は，欧州連合全域の対応を適正に調整するため，技術上のレベル，運用上のレベル及び政治上のレベルで協力すべきである。

In accordance with the Annex to Recommendation (EU) 2017/1584, a large-scale cybersecurity incident should mean an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States. Depending on their cause and impact, large-scale cybersecurity incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market or posing serious public security and safety risks for entities or citizens in several Member States or the Union as a whole. Given the wide-ranging scope

17.12.2018, p. 28).

Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements (OJ L 320, 17.12.2018, p. 28).

and, in most cases, the cross-border nature of such incidents, Member States and the relevant Union institutions, bodies, offices and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union.

(70) 欧州連合レベルの大規模なサイバーセキュリティのインシデント及び危機は，部門間及び構成国間の高い程度の相互依存のゆえに，迅速かつ実効的な対応を確保するための調整された活動を要求する。サイバー回復力のあるネットワーク及び情報システムの可用性と，データの可用性，機密性及び完全性は，欧州連合のセキュリティにとって，インシデント及びサイバーな脅威に抗する欧州連合の市民，事業者及び機関の保護にとって，並びに，人権，基本的な自由，民主主義及び法の支配を基盤とするグローバルで，オープンで，自由で，安定し，かつ，安全なサイバー空間を促進及び保護するための欧州連合の能力への個人及び組織の信頼を拡大することにとって，重要である。

Large-scale cybersecurity incidents and crises at Union level require coordinated action to ensure a rapid and effective response because of the high degree of interdependence between sectors and Member States. The availability of cyber-resilient network and information systems and the availability, confidentiality and integrity of data are vital for the security of the Union and for the protection of its citizens, businesses and institutions against incidents and cyber threats, as well as for enhancing the trust of individuals and organisations in the Union's ability to promote and protect a global, open, free, stable and secure cyberspace grounded in human rights, fundamental freedoms, democracy and the rule of law.

(71) EU-CyCLONe は，大規模なサイバーセキュリティのインシデント及び危機の間における技術レベルと政治レベルとの間の媒介者として働くべきであり，また，運用レベルの協力を拡大すべきであり，また，政治レベルにおける意思決定を支援すべきである。欧州委員会との協力において，危機管理の分野における欧州委員会の職務権限に鑑み，EU-CyCLONe は，CSIRT ネットワークの判断を基礎とすべきであり，かつ，大規模なサイバーセキュリティのインシデント及び危機の影響評価をつくり出すための EU-CyCLONe 自体の実現能力を用いるべきである。

EU-CyCLONe should work as an intermediary between the technical and political level during large-scale cybersecurity incidents and crises and should enhance cooperation at operational level and support decision-making at political level. In cooperation with the Commission, having regard to the Commission's competence in the area of crisis management, EU-CyCLONe should build on the CSIRTs network findings and use its own capabilities to create impact analysis of large-scale cybersecurity incidents and crises.

(72) サイバー攻撃は，国境を越える性質をもち，また，重大なインシデントは，その上に域内市場の円滑な稼働が依拠している重要な情報インフラを混乱させ，毀損し得る。勧告(EU) 2017/1584 は，関連する全ての関与者の役割に対処している。更に，欧州委員会は，欧州議会及び理事会の決定 No 1313/2013/ EU[17] によって設置された欧州連合市民保護の仕組みの枠組み内において，緊急対応調整センター及び共通緊急通信情報システムの管理，状況認識と分析の実現能力の維

持及び更なる発展，並びに，構成国または第三国からの補助の要請の場合における専門家チームの動員及び派遣の実現能力の管理を含む一般的な準備態勢の活動に関して職責を負う。欧州委員会は，サイバーセキュリティの状況認識及び準備態勢との関係を含め，実装決定(EU) 2018/1993 に基づく IPCR 覚書に関する分析報告書を提供することに関する職責，並びに，農業，悪い気象条件，紛争のマッピングと予測，自然災害の早期警戒システム，医療上の緊急事態，感染症の監視，植物の健康，化学インシデント，食品及び飼料の安全性，動物の健康，移民，関税，原子力及び放射線の緊急事態並びにエネルギーの分野における状況認識及び危機対応に関する職責も負う。

Cyberattacks are of a cross-border nature, and a significant incident can disrupt and damage critical information infrastructures on which the smooth functioning of the internal market depends. Recommendation (EU) 2017/1584 addresses the role of all relevant actors. Furthermore, the Commission is responsible, within the framework of the Union Civil Protection Mechanism, established by Decision No 1313/2013/EU of the European Parliament and of the Council [17], for general preparedness actions including managing the Emergency Response Coordination Centre and the Common Emergency Communication and Information System, maintaining and further developing situational awareness and analysis capability, and establishing and managing the capability to mobilise and dispatch expert teams in the event of a request for assistance from a Member State or third country. The Commission is also responsible for providing analytical reports for the IPCR arrangements under Implementing Decision (EU) 2018/1993, including in relation to cybersecurity situational awareness and preparedness, as well as for situational awareness and crisis response in the areas of agriculture, adverse weather conditions, conflict mapping and forecasts, early warning systems for natural disasters, health emergencies, infection disease surveillance, plant health, chemical incidents, food and feed safety, animal health, migration, customs, nuclear and radiological emergencies, and energy.

(73) 欧州連合は，それが適切なときは，TFEU の第 218 条に従い，第三国または国際機関との間で，とりわけ，協力グループ，CSIRT ネットワーク及び EU-CyCLONe の活動への第三国または国際機関の参加を認め及び計画する国際的な合意を締結できる。そのような合意は，欧州連合の利益及びデータの十分な保護を確保すべきである。このことは，脆弱性の管理及びサイバーセキュリティのリスク管理に関して第三国との間で協力し，欧州連合法に従った報告及び一般的な情報共有を促進する構成国の権利を排除してはならない。

The Union can, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in particular activities of the Cooperation Group, the CSIRTs network and EU-CyCLONe. Such agreements

---

17 欧州連合の市民保護の仕組みに関する欧州議会及び理事会の 2013 年 12 月 17 日の決定 No 1313/2013/EU (OJ L 347, 20.12.2013, p. 924).
Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

should ensure the Union's interests and the adequate protection of data. This should not preclude the right of Member States to cooperate with third countries on management of vulnerabilities and cybersecurity risk management, facilitating reporting and general information sharing in accordance with Union law.

(74) 就中，脆弱性の管理，サイバーセキュリティのリスク管理の措置，報告義務及びサイバーセキュリティの情報共有覚書と関連するこの指令の実効的な実装を容易にするため，構成国は，第三国と協力し，また，サイバーな脅威，インシデント，脆弱性，ツール及び手法，戦術，技術及び手順，サイバーセキュリティの危機管理の準備態勢及び演習，訓練，信頼構築及び構造化された情報共有覚書に関する情報交換を含め，当該目的のために適切と判断される活動を実施できる。

In order to facilitate the effective implementation of this Directive with regard, inter alia, to the management of vulnerabilities, cybersecurity risk-management measures, reporting obligations and cybersecurity information-sharing arrangements, Member States can cooperate with third countries and undertake activities that are considered to be appropriate for that purpose, including information exchange on cyber threats, incidents, vulnerabilities, tools and methods, tactics, techniques and procedures, cybersecurity crisis management preparedness and exercises, training, trust building and structured information-sharing arrangements.

(75) 共有された経験から学習すること，相互の信頼を強化すること及び共通の高いレベルのサイバーセキュリティを達成することを助けるため，相互評価が導入されるべきである。相互評価は，サイバーセキュリティの全体的な実現能力を強化し，構成国横断のベストプラクティスの共有のための別の機能上の経路をつくり出し，そして，サイバーセキュリティにおける構成国の熟達レベルを拡大するために寄与する価値ある意見及び推奨を導き得る。更に，相互評価は，CSIRT ネットワークの相互評価システムのような類似の仕組みの結果を考慮に入れるべきであり，また，価値を付加すべきであり，かつ，重複を避けるべきである。相互評価の実装は，秘密情報または機密情報の保護に関する欧州連合法または国内法を妨げてはならない。

Peer reviews should be introduced to help learn from shared experiences, strengthen mutual trust and achieve a high common level of cybersecurity. Peer reviews can lead to valuable insights and recommendations strengthening the overall cybersecurity capabilities, creating another functional path for the sharing of best practices across Member States and contributing to enhance the Member States' levels of maturity in cybersecurity. Furthermore, peer reviews should take account of the results of similar mechanisms, such as the peer-review system of the CSIRTs network, and should add value and avoid duplication. The implementation of peer reviews should be without prejudice to Union or national law on the protection of confidential or classified information.

(76) 協力グループは，サイバーセキュリティのリスク管理の措置及び報告義務の実装レベル，実現能力のレベル及び職務権限のある機関の職務の執行の実効性，CSIRT の業務運営上の実現能力，相互補助の実装のレベル，サイバーセキュリティ情報共有覚書の実装のレベル，または，国境を越える性質もしくは部門横断の性質をもつ個別の問題のような要素を包摂することを狙いとする

構成国のための自己評価の手法を定めるべきである。構成国は，定期的に自己評価を遂行すること，そして，協力グループ内において，その構成国の自己評価の結果を提示及び討議することが推奨される。

The Cooperation Group should establish a self-assessment methodology for Member States, aiming to cover factors such as the level of implementation of the cybersecurity risk-management measures and reporting obligations, the level of capabilities and the effectiveness of the exercise of the tasks of the competent authorities, the operational capabilities of the CSIRTs, the level of implementation of mutual assistance, the level of implementation of the cybersecurity information-sharing arrangements, or specific issues of cross-border or cross-sector nature. Member States should be encouraged to carry out self-assessments on a regular basis, and to present and discuss the results of their self-assessment within the Cooperation Group.

(77) ネットワーク及び情報システムの防護を確保する責任は，その大部分について，基礎法主体及び重要法主体が負っている。リスク評価を含めリスク管理の文化，及び，直面するリスクにとって適切なサイバーセキュリティのリスク管理の措置の実装が促進され，発展させられるべきである。

Responsibility for ensuring the security of network and information system lies, to a great extent, with essential and important entities. A culture of risk management, involving risk assessments and the implementation of cybersecurity risk-management measures appropriate to the risks faced, should be promoted and developed.

(78) サイバーセキュリティのリスク管理の措置は，基礎法主体または重要法主体のネットワーク及び情報システムへの依存の程度を考慮に入れるべきであり，かつ，インシデントのリスクを発見するための措置，インシデントを防止し，検出し，インシデントに対応し及びインシデントから復旧するための措置，並びに，インシデントの影響を緩和するための措置を含めるべきである。ネットワーク及び情報システムの防護は，記録保存され，移転され及び処理されるデータの防護を含めるべきである。サイバーセキュリティのリスク管理の措置は，ネットワーク及び情報システムの防護の完全な見取図をもつため，人的要因を考慮に入れるシステミック分析を定めるべきである。

Cybersecurity risk-management measures should take into account the degree of dependence of the essential or important entity on network and information systems and include measures to identify any risks of incidents, to prevent, detect, respond to and recover from incidents and to mitigate their impact. The security of network and information systems should include the security of stored, transmitted and processed data. Cybersecurity risk-management measures should provide for systemic analysis, taking into account the human factor, in order to have a complete picture of the security of the network and information system.

(79) ネットワーク及び情報システムの防護に対する脅威は異なる原因をもち得るので，サイバーセキュリティのリスク管理の措置は，窃盗，火災，洪水，通信途絶もしくは電源途絶，または，基礎法主

体もしくは重要法主体の情報及び情報処理施設への無権限の物理的なアクセス及びそれらに対する毀損並びにそれらに対する妨害のような，記録保存され，移転されまたは処理されるデータの可用性，真正性，完全性もしくは機密性，または，ネットワーク及び情報システムから提供され，もしくは，それらを介してアクセス可能なサービスの可用性，真正性，完全性もしくは機密性を損ない得る出来事からネットワーク及び情報システムと当該システムの物理環境を保護することを狙いとするオールハザードアプローチを基礎とすべきである。それゆえ，サイバーセキュリティのリスク管理の措置は，ISO/IEC 27000 シリーズに収録されている標準のような，欧州の技術標準及び国際的な技術標準に沿って，そのようなシステムをシステム障害，ヒューマンエラー，悪意ある行動または自然現象から保護するための措置を含めることにより，ネットワーク及び情報システムの物理的な防護とその環境の防護にも対処すべきである。この点に関し，基礎法主体及び重要法主体は，当該法主体のサイバーセキュリティのリスク管理の措置の一部として，人的資源の防護にも対処すべきであり，かつ，適切なアクセス管理の基本方針を設けるべきである。それらの措置は，指令(EU) 2022/2557 と一貫性があるべきである。

As threats to the security of network and information systems can have different origins, cybersecurity risk-management measures should be based on an all-hazards approach, which aims to protect network and information systems and the physical environment of those systems from events such as theft, fire, flood, telecommunication or power failures, or unauthorised physical access and damage to, and interference with, an essential or important entity's information and information processing facilities, which could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems. The cybersecurity risk-management measures should therefore also address the physical and environmental security of network and information systems by including measures to protect such systems from system failures, human error, malicious acts or natural phenomena, in line with European and international standards, such as those included in the ISO/IEC 27000 series. In that regard, essential and important entities should, as part of their cybersecurity risk-management measures, also address human resources security and have in place appropriate access control policies. Those measures should be consistent with Directive (EU) 2022/2557.

(80) サイバーセキュリティのリスク管理の措置の遵守を示す目的のために，かつ，欧州議会及び理事会の規則(EU) 2019/881[18]に従って採択された適切な欧州サイバーセキュリティ認証制度が存在しない場合において，構成国は，協力グループ及び欧州サイバーセキュリティ認証グループの意見を聴取した上で，基礎法主体及び重要法主体による関連する欧州の技術標準及び国際的

[18] ENISA（欧州連合サイバーセキュリティ局）に関する及び情報通信技術のサイバーセキュリティ認証に関する並びに規則(EU) No 526/2013 を廃止する欧州議会及び理事会の 2019 年 4 月 17 日の規則(EU) 2019/881（サイバーセキュリティ法）(OJ L 151, 7.6.2019, p. 15)
Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

な技術標準の利用を促進すべきであり，また，法主体に対し，認証された ICT 製品，ICT サービス及び ICT プロセスの利用を要求できる。

For the purpose of demonstrating compliance with cybersecurity risk-management measures and in the absence of appropriate European cybersecurity certification schemes adopted in accordance with Regulation (EU) 2019/881 of the European Parliament and of the Council[(18)], Member States should, in consultation with the Cooperation Group and the European Cybersecurity Certification Group, promote the use of relevant European and international standards by essential and important entities or may require entities to use certified ICT products, ICT services and ICT processes.

(81) 基礎法主体及び重要法主体に対して比例的ではない資金上及び管理運営上の負担を課すことを避けるため，サイバーセキュリティのリスク管理の措置は，そのような措置が最新のものであることを考慮に入れ，また，それが適用可能なときは，関連する欧州の技術標準及び国際的な技術標準並びに当該技術標準の実装のための費用を考慮に入れた上で，関係するネットワーク及び情報システムに対して示されているリスクと比例的であるべきである。

In order to avoid imposing a disproportionate financial and administrative burden on essential and important entities, the cybersecurity risk-management measures should be proportionate to the risks posed to the network and information system concerned, taking into account the state-of-the-art of such measures, and, where applicable, relevant European and international standards, as well as the cost for their implementation.

(82) サイバーセキュリティのリスク管理の措置は，基礎法主体または重要法主体がリスクに晒されている程度と，そして，インシデントがもち得る社会的及び経済的な影響と比例的であるべきである。基礎法主体及び重要法主体向けに調整されたサイバーセキュリティのリスク管理の措置を設けるときは，その法主体の重要度，社会的リスクを含めその法主体が晒されているリスク，その法主体の規模，インシデント発生の蓋然性，並びに，そのインシデントの社会的及び経済的影響を含め，そのインシデントの深刻度のような，基礎法主体及び重要法主体が多様にリスクに晒されていることが適正に考慮に入れられるべきである。

Cybersecurity risk-management measures should be proportionate to the degree of the essential or important entity's exposure to risks and to the societal and economic impact that an incident would have. When establishing cybersecurity risk-management measures adapted to essential and important entities, due account should be taken of the divergent risk exposure of essential and important entities, such as the criticality of the entity, the risks, including societal risks, to which it is exposed, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

(83) 基礎法主体及び重要法主体は，当該法主体がその活動において使用しているネットワーク及び情報システムの防護を確保すべきである。それらのシステムは，基本的には，その基礎法主体及び重要法主体の内部 IT 職員によって管理されている，または，そのネットワーク及び情報システ

ムの防護がアウトソースされた私的なネットワーク及び情報システムである。この指令に定めるサイバーセキュリティのリスク管理の措置及び報告義務は，当該法主体が当該法主体のネットワーク及び情報システムを内部的に維持管理しているか，そのネットワーク及び情報システムの維持管理をアウトソースしているかに拘わらず，関連する基礎法主体及び重要法主体に対して適用されるべきである。

Essential and important entities should ensure the security of the network and information systems which they use in their activities. Those systems are primarily private network and information systems managed by the essential and important entities' internal IT staff or the security of which has been outsourced. The cybersecurity risk-management measures and reporting obligations laid down in this Directive should apply to the relevant essential and important entities regardless of whether those entities maintain their network and information systems internally or outsource the maintenance thereof.

(84) 当該サービスの国境を越える性質を考慮に入れた上で，DNS サービスのプロバイダ，TLD 名レジストリ，クラウドコンピューティングサービスのプロバイダ，データセンターサービスのプロバイダ，コンテント伝達ネットワークのプロバイダ，マネージドサービスのプロバイダ，マネージドセキュリティサービスのプロバイダ，オンライン市場のプロバイダ，オンライン検索エンジンのプロバイダ及びソーシャルネットワーキングサービスプラットフォームのプロバイダ並びに信頼サービスのプロバイダは，欧州連合レベルの高い程度の整合化に服するべきである。それゆえ，当該法主体と関連するサイバーセキュリティのリスク管理の措置の実装は，実装行為によって容易にされるべきである。

Taking account of their cross-border nature, DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, of online search engines and of social networking services platforms, and trust service providers should be subject to a high degree of harmonisation at Union level. The implementation of cybersecurity risk-management measures with regard to those entities should therefore be facilitated by an implementing act.

(85) 法主体がサイバー攻撃の被害者となった場合，並びに，悪意のある加害者が，サードパーティの製品及びサービスに対して影響を与える脆弱性を悪用することによって，法主体のネットワーク及び情報システムの防護を損なうことができた場合におけるインシデントが拡大する範囲の広さに鑑み，法主体のサプライチェーンから派生するリスク，及び，その法主体と，データストレージ及び処理のサービスのプロバイダ，または，マネージドセキュリティサービスプロバイダ及びソフトウェアエディタのような，その法主体の供給者との間の関係から派生するリスクに対処することは，とりわけ重要である。それゆえ，基礎法主体及び重要法主体は，製品及びサービスの全体的な品質及び回復力，当該製品及びサービスに具備されているサイバーセキュリティのリスク管理の措置，並びに，当該製品及びサービスの安全な開発手順を含め，当該製品及びサービスの供給者及びサービスプロバイダのサイバーセキュリティの実務を評価し，かつ，考慮に入れるべきである。基礎法主体及び重要法主体は，とりわけ，当該法主体の直接の供給者及びサービスプ

ロバイダとの間の契約上の手立ての中にサイバーセキュリティのリスク管理の措置を組み込むことが推奨されるべきである。当該法主体は，別のレベルの供給者及びサービスプロバイダから派生するリスクを検討し得る。

Addressing risks stemming from an entity's supply chain and its relationship with its suppliers, such as providers of data storage and processing services or managed security service providers and software editors, is particularly important given the prevalence of incidents where entities have been the victim of cyberattacks and where malicious perpetrators were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third-party products and services. Essential and important entities should therefore assess and take into account the overall quality and resilience of products and services, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures. Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers. Those entities could consider risks stemming from other levels of suppliers and service providers.

(86) サービスプロバイダの中でも，インシデント対応，ペネトレーションテスト，セキュリティ監査及びセキュリティコンサルタントのような分野におけるマネージドセキュリティサービスプロバイダは，インシデントの防止，検出，インシデントへの対応またはインシデントからの回復のための法主体の努力において法主体を補助するという特に重要な役割を演ずる。ただし，マネージドセキュリティサービスプロバイダは，そのプロバイダ自身もサイバー攻撃の標的となってきたし，法主体の業務運営における当該プロバイダの緊密な統合のゆえに，特別のリスクを示してきた。それゆえ，基礎法主体及び重要法主体は，マネージドセキュリティサービスプロバイダの選択において，増加された勤勉さを実施すべきである。

Among service providers, managed security service providers in areas such as incident response, penetration testing, security audits and consultancy play a particularly important role in assisting entities in their efforts to prevent, detect, respond to or recover from incidents. Managed security service providers have however also themselves been the target of cyberattacks and, because of their close integration in the operations of entities pose a particular risk. Essential and important entities should therefore exercise increased diligence in selecting a managed security service provider.

(87) 職務権限のある機関は，その機関の監督の職務の過程において，セキュリティ監査，ペネトレーションテストまたはインシデント対応のようなサイバーセキュリティサービスからも受益し得る。

The competent authorities, in the context of their supervisory tasks, may also benefit from cybersecurity services such as security audits, penetration testing or incident responses.

(88) 基礎法主体及び重要法主体は，産業スパイに対抗すること及び営業秘密を保護することと関連

するものを含め，より広いエコシステムの中で，他の利害関係者とのやりとり及び関係から派生するリスクにも対処すべきである。とりわけ，当該法主体は，その法主体と学術機関及び調査研究機関との間の協力が，その法主体のサイバーセキュリティの基本方針に沿って，かつ，安全なアクセスと情報の伝達一般及び特に知的財産の保護に関するグッドプラクティスに従って行われることを確保するための適切な措置を講ずるべきである。同様に，基礎法主体及び重要法主体の活動にとってのデータの重要性及び価値に鑑み，サードパーティからのデータ変換サービス及びデータ分析サービスに依拠するときは，当該法主体は，全ての適切なサイバーセキュリティのリスク管理の措置を講ずるべきである。

Essential and important entities should also address risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem, including with regard to countering industrial espionage and protecting trade secrets. In particular, those entities should take appropriate measures to ensure that their cooperation with academic and research institutions takes place in line with their cybersecurity policies and follows good practices as regards secure access and dissemination of information in general and the protection of intellectual property in particular. Similarly, given the importance and value of data for the activities of essential and important entities, when relying on data transformation and data analytics services from third parties, those entities should take all appropriate cybersecurity risk-management measures.

(89) 基礎法主体及び重要法主体は，ゼロトラスト原則，ソフトウェアのアップデート，機器の設定，ネットワークセグメンテーション，識別名及びアクセスの管理，または，利用者の認識向上，のような，広範囲で基礎的なサイバー衛生実務を導入し，その法主体の職員のための訓練を計画し，かつ，サイバーな脅威，フィッシングまたはソーシャルエンジニアリングの手法に関して注意喚起すべきである。更に，当該法主体は，その法主体自身のサイバーセキュリティの実現能力を評価し，かつ，それが適切なときは，その法主体の実現能力を拡大するための人工知能システムまたは機械学習システムのようなサイバーセキュリティ拡張技術と，ネットワーク及び情報システムの防護との統合を検討すべきである。

Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques. Furthermore, those entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems.

(90) 鍵となるサプライチェーンのリスクに更に対処するため，並びに，この指令によって包摂される部門において業務運営する基礎法主体及び重要法主体がサプライチェーンと関連するリスク及び供給者と関連するリスクを適切に管理することを補助するため，協力グループは，欧州委員会及び ENISA と協力し，かつ，それが適切なときは，産業界の利害関係者を含め関連する利害関係

者からの意見聴取を経た後，不可欠な ICT サービス，ICT システムまたは ICT 製品，関連する脅威及び脆弱性を部門別に識別することを狙いとして，委員会勧告(EU) 2019/534[19]に従う 5G ネットワークに関して遂行されるような，重要サプライチェーンの調整されたセキュリティリスク評価を遂行すべきである。そのような調整されたセキュリティリスク評価は，サプライチェーンと関連する致命的な依存性，潜在的な単一障害点，脅威，脆弱性及びそれら以外のリスクに抗するための措置，緩和計画及びベストプラクティスを発見し，かつ，当該措置，計画及びベストプラクティスが基礎法主体及び重要法主体によって広範に導入されることを更に推奨するための方途を開拓すべきである。とりわけ，異なる国家統治モデルの場合における，第三国から供給者及びサービスプロバイダに対する不適切な影響のような，潜在的な非技術上のリスク要素は，とりわけ，技術上のロックインまたはプロバイダへの依存の場合において，隠された脆弱性またはバックドア，及び，潜在的にシステミックな供給の混乱を含む。

To further address key supply chain risks and assist essential and important entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related risks, the Cooperation Group, in cooperation with the Commission and ENISA, and where appropriate after consulting relevant stakeholders including from the industry, should carry out coordinated security risk assessments of critical supply chains, as carried out for 5G networks following Commission Recommendation (EU) 2019/534 (19), with the aim of identifying, per sector, the critical ICT services, ICT systems or ICT products, relevant threats and vulnerabilities. Such coordinated security risk assessments should identify measures, mitigation plans and best practices to counter critical dependencies, potential single points of failure, threats, vulnerabilities and other risks associated with the supply chain and should explore ways to further encourage their wider adoption by essential and important entities. Potential non-technical risk factors, such as undue influence by a third country on suppliers and service providers, in particular in the case of alternative models of governance, include concealed vulnerabilities or backdoors and potential systemic supply disruptions, in particular in the case of technological lock-in or provider dependency.

(91) 重要なサプライチェーンの調整されたセキュリティリスク評価は，勧告(EU) 2019/534，EU の 5G ネットワークのサイバーセキュリティの調整されたリスク評価，及び，協力グループが同意した 5G サイバーセキュリティに関する EU ツールボックスの中で定義されている諸要素を含め，関係する部門の特徴に照らし，技術上の要素，及び，それが関連するときは，非技術上の要素の両者を考慮に入れるべきである。調整されたセキュリティリスク評価の対象とされるべきサプライチェーンを識別するため，以下の諸基準が考慮に入れられるべきである：すなわち，(i)基礎法主体及び重要法主体が特定の重要な ICT サービス，ICT システムまたは ICT 製品を利用し，それらに依拠する範囲;(ii)個人データの処理を含め，重要な機能または機微の機能を遂行するための特定の重要な ICT サービス，ICT システムまたは ICT 製品の適正性;(iii)代替的な ICT サービス，ICT

[19] 2019 年 3 月 26 日の委員会勧告(EU) 2019/534－5G ネットワークのサイバーセキュリティ (OJ L 88, 29.3.2019, p. 42).
Commission Recommendation (EU) 2019/534 of 26 March 2019 – Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).

システムまたは ICT 製品の可用性;(iv) ICT サービス, ICT システムまたは ICT 製品のサプライチェーン全体のそれらのライフサイクルを通じた破壊的な出来事に抗する回復力;並びに, (v)出現しつつある ICT サービス, ICT システムまたは ICT 製品に関しては, 法主体の活動に対する当該 ICT サービス, ICT システムまたは ICT 製品の潜在的な将来の重要性。更に, 第三国から波及している特別の要件に服する ICT サービス, ICT システムまたは ICT 製品に対しては, 特に重点が置かれるべきである。

The coordinated security risk assessments of critical supply chains, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU coordinated risk assessment of the cybersecurity of 5G networks and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated security risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, ICT systems or ICT products; (ii) the relevance of specific critical ICT services, ICT systems or ICT products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, ICT systems or ICT products; (iv) the resilience of the overall supply chain of ICT services, ICT systems or ICT products throughout their lifecycle against disruptive events; and (v) for emerging ICT services, ICT systems or ICT products, their potential future significance for the entities' activities. Furthermore, particular emphasis should be placed on ICT services, ICT systems or ICT products that are subject to specific requirements stemming from third countries.

(92) 公共電子通信ネットワークまたは公衆が利用可能な通信サービスのプロバイダ及び信頼サービスのプロバイダに課される当該プロバイダのネットワーク及び情報システムの防護と関連する義務を合理化するため, 並びに, 欧州議会及び理事会の指令(EU) 2018/1972[20]及び規則(EU) No 910/2014 それぞれの下にある当該法主体及び職務権限のある機関が, インシデントの取扱いに関する職責を負う CSIRT の指定, 協力グループ及び CSIRT ネットワークの活動への関係する職務権限のある機関の参加を含め, この指令によって設けられる法的枠組みから受益できるようにするため, 当該法主体は, この指令の適用範囲内にあるべきである。それゆえ, それらのタイプの法主体に対して防護の要件と通知の要件を課すことに関連する規則(EU) No 910/2014 及び指令(EU) 2018/1972 に定める対応する条項は, 削除されるべきである。この指令に定める報告義務に関する規定は, 規則(EU) 2016/679 及び指令 2002/58/EC を妨げてはならない。

In order to streamline the obligations imposed on providers of public electronic communications networks or of publicly available electronic communications services, and trust service providers, related

[20] 欧州電子通信法を定める欧州議会及び理事会の 2018 年 12 月 11 日の指令(EU) 2018/1972 (OJ L 321, 17.12.2018, p. 36).
Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

to the security of their network and information systems, as well as to enable those entities and the competent authorities under Directive (EU) 2018/1972 of the European Parliament and of the Council[20] and Regulation (EU) No 910/2014 respectively to benefit from the legal framework established by this Directive, including the designation of a CSIRT responsible for incident handling, the participation of the competent authorities concerned in the activities of the Cooperation Group and the CSIRTs network, those entities should fall within the scope of this Directive. The corresponding provisions laid down in Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 related to the imposition of security and notification requirements on those types of entity should therefore be deleted. The rules on reporting obligations laid down in this Directive should be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC.

(93) この指令に定めるサイバーセキュリティの義務は，規則(EU) No 910/2014 の下で信頼サービスのプロバイダに課されていた要件の補完であると考えられるべきである。信頼サービスのプロバイダは，顧客及び依拠するサードパーティと関係するものを含め，そのプロバイダのサービスに対して示されているリスクを管理するための，並びに，この指令に基づきインシデントを報告するための，適切かつ比例的な全ての措置を講ずることを要求されるべきである。そのようなサイバーセキュリティの義務及び報告義務は，提供されるサービスの物理的な保護とも関係すべきである。規則(EU) No 910/2014 の第 24 条に定める適格信頼サービスプロバイダに関する要件は，引き続き適用される。

The cybersecurity obligations laid down in this Directive should be considered to be complementary to the requirements imposed on trust service providers under Regulation (EU) No 910/2014. Trust service providers should be required to take all appropriate and proportionate measures to manage the risks posed to their services, including in relation to customers and relying third parties, and to report incidents under this Directive. Such cybersecurity and reporting obligations should also concern the physical protection of the services provided. The requirements for qualified trust service providers laid down in Article 24 of Regulation (EU) No 910/2014 continue to apply.

(94) 構成国は，現在の実務の継続を確保するため，及び，同規則の適用において得られた知識及び経験を基礎とするため，信頼サービスに関する職務権限のある機関の役割を規則(EU) No 910/2014 の下にある監督機関に対して割当て得る。そのような場合，この指令の下にある職務権限のある機関は，この指令及び規則(EU) No 910/2014 に定める要件の実効的な監督及び信頼サービスプロバイダによる遵守を確保するための関連情報を交換することにより，緊密に，かつ，適時の態様で，それらの監督機関と協力すべきである。それが適用可能なときは，CSIRT またはこの指令の下にある職務権限のある機関は，規則(EU) No 910/2014 の下にある監督機関に対し，信頼サービスに影響を与える通知された重大なサイバーな脅威またはインシデントに関して，並びに，信頼サービスプロバイダによるこの指令の違反行為に関して，直ちに連絡すべきである。報告の目的のために，構成国は，それが適用可能なときは，規則(EU) No 910/2014 の下にある監督機，及び，CSIRT の両者またはこの指令の下にある職務権限のある機関の両者に対する，共通かつ自動化されたインシデント報告を達成するために設置される単一エントリポイントを利用で

きる。

Member States can assign the role of the competent authorities for trust services to the supervisory bodies under Regulation (EU) No 910/2014 in order to ensure the continuation of current practices and to build on the knowledge and experience gained in the application of that Regulation. In such a case, the competent authorities under this Directive should cooperate closely and in a timely manner with those supervisory bodies by exchanging relevant information in order to ensure effective supervision and compliance of trust service providers with the requirements laid down in this Directive and in Regulation (EU) No 910/2014. Where applicable, the CSIRT or the competent authority under this Directive should immediately inform the supervisory body under Regulation (EU) No 910/2014 about any notified significant cyber threat or incident affecting trust services as well as about any infringements by a trust service provider of this Directive. For the purpose of reporting, Member States can, where applicable, use the single entry point established to achieve a common and automatic incident reporting to both the supervisory body under Regulation (EU) No 910/2014 and the CSIRT or the competent authority under this Directive.

(95) それが適切なときは，かつ，無用の混乱を避けるため，指令(EU) 2018/1972 の第 40 条及び第 41 条に定める防護措置と関連する規定の国内法化のために採択された既存の国内指針は，それによって，指令(EU) 2018/1972 の下で既に獲得されている防護措置及びインシデント通知と関係する知識及び技能を基礎とするこの指令の国内法化において，考慮に入れられるべきである。ENISA は，公共電子通信ネットワークのプロバイダ向けのまたは公衆が利用可能な電子通信サービスのプロバイダ向けの，整合化及び移植を容易にするための，及び，混乱をミニマム化するための，セキュリティの要件に関するガイド及び報告義務に関するガイドを策定し得る。構成国は，現在の実務の継続を確保するため，及び，同指令の実装の結果として得られた知識及び経験を基礎とするため，指令(EU) 2018/1972 の下にある国内規制当局に対し，電子通信に関する職務権限のある機関の役割を割当て得る。

Where appropriate and in order to avoid unnecessary disruption, existing national guidelines adopted for the transposition of the rules related to security measures laid down in Articles 40 and 41 of Directive (EU) 2018/1972 should be taken into account in the transposition of this Directive, thereby building on the knowledge and skills already acquired under Directive (EU) 2018/1972 concerning security measures and incident notifications. ENISA can also develop guidance on security requirements and on reporting obligations for providers of public electronic communications networks or of publicly available electronic communications services to facilitate harmonisation and transition and to minimise disruption. Member States can assign the role of the competent authorities for electronic communications to the national regulatory authorities under Directive (EU) 2018/1972 in order to ensure the continuation of current practices and to build on the knowledge and experience gained as a result of the implementation of that Directive.

(96) 指令(EU) 2018/1972 に定義する番号に依存しない個人間通信サービスの重要性が増加している

ことに鑑み，そのようなサービスもまた，そのようなサービスの特別の性質及び経済的重要性を考慮した適切なセキュリティ要件に服することを確保する必要がある。攻撃領域が拡大しているので，メッセージングサービスのような番号に依存しない個人間通信サービスは，広範囲にわたる攻撃ベクトルとなってきている。悪意ある加害者は，被害者と通信し，安全ではない Web ページを開かせるように被害者を誘導するためにプラットフォームを利用しており，それゆえに，個人データの濫用を含むインシデントの蓋然性，更には，ネットワーク及び情報システムの防護の濫用を含むインシデントの蓋然性が増加している。番号に依存しない個人間通信サービスのプロバイダは，ネットワーク及び情報システムの防護が，示されているリスクに対して適切なレベルであることを確保すべきである。番号に依存しない個人間通信サービスのプロバイダが，通常は，ネットワーク上の信号の伝送に対して現実の支配を実行しないことに鑑み，そのようなサービスに対して示されているリスクは，ある点で，在来の電子通信サービスよりも低いと考えられ得る。同様のことは，指令(EU) 2018/1972 に定義する個人間通信サービスであって，番号を利用し，信号の伝送に対して現実の支配を実行しないものに対して適用される。

Given the growing importance of number-independent interpersonal communications services as defined in Directive (EU) 2018/1972, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. As the attack surface continues to expand, number-independent interpersonal communications services, such as messaging services, are becoming widespread attack vectors. Malicious perpetrators use platforms to communicate and attract victims to open compromised web pages, therefore increasing the likelihood of incidents involving the exploitation of personal data, and, by extension, the security of network and information systems. Providers of number-independent interpersonal communications services should ensure a level of security of network and information systems appropriate to the risks posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risks posed to such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services as defined in Directive (EU) 2018/1972 which make use of numbers and which do not exercise actual control over signal transmission.

(97) 域内市場は，かつてないほど，インターネットの稼働により多く依拠している。ほとんど全ての基礎法主体及び重要法主体のサービスが，インターネット上で提供されるサービスに依存している。基礎法主体及び重要法主体から提供されるサービスの円滑な提供を確保するため，全ての公共電子通信ネットワークのプロバイダが，適切なサイバーセキュリティのリスク管理の措置を設け，かつ，当該プロバイダと関係する重大なインシデントを報告することが重要である。構成国は，公共電子通信ネットワークの防護が維持されること，そして，当該ネットワークの重要なセキュリティ上の利益が妨害行為やスパイ行為から保護されることを確保すべきである。国際的な接続性が，欧州連合の競争力のあるデジタル化と欧州連合の経済を拡大し，加速させているので，海底通信ケーブルに影響を与えるインシデントは，CSIRT に対して，または，それが適用可能なときは，職務権限のある機関に対して，報告されるべきである。国内サイバーセキュリティ戦略は，それが関連するときは，海底通信ケーブルのサイバーセキュリティを考慮に入れるべきであり，かつ，潜

在的なサイバーセキュリティのリスクのマッピング，及び，当該海底通信ケーブルの最高度の保護を防護するための緩和措置を含めるべきである。

The internal market is more reliant on the functioning of the internet than ever. The services of almost all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that all providers of public electronic communications networks have appropriate cybersecurity risk-management measures in place and report significant incidents in relation thereto. Member States should ensure that the security of the public electronic communications networks is maintained and that their vital security interests are protected from sabotage and espionage. Since international connectivity enhances and accelerates the competitive digitalisation of the Union and its economy, incidents affecting undersea communications cables should be reported to the CSIRT or, where applicable, the competent authority. The national cybersecurity strategy should, where relevant, take into account the cybersecurity of undersea communications cables and include a mapping of potential cybersecurity risks and mitigation measures to secure the highest level of their protection.

(98) 公共電子通信ネットワーク及び公衆が利用可能な電子通信サービスの防護を守るため，暗号技術，特に，エンドツーエンドの暗号，並びに，地図のようなデータ中心のセキュリティ概念，セグメンテーション，タグ付け，アクセスポリシー及びアクセス管理及び自動化されたアクセス決定の利用が促進されるべきである。それが必要なときは，この指令の目的のためのバイデフォルト及びバイデザインのセキュリティ及びプライバシーの原則に従い，公共電子通信ネットワークのプロバイダ及び公衆が利用可能な電子通信サービスのプロバイダに関し，暗号，特に，エンドツーエンドの暗号の利用が義務であるべきである。エンドツーエンドの暗号の利用は，その構成国の必須の防衛上の利益の保護及び公共の保安を確保するため，並びに，欧州連合法に従って犯罪行為の防止，捜査，検知及び訴追ができるようにするための構成国の権限に反しないものとすべきある。ただし，このことは，データ及びプライバシーの実効的な保護並びに通信の防護のための不可欠の技術であるエンドツーエンドの暗号を弱体化させてはならない。

In order to safeguard the security of public electronic communications networks and publicly available electronic communications services, the use of encryption technologies, in particular end-to-end encryption as well as data-centric security concepts, such as cartography, segmentation, tagging, access policy and access management, and automated access decisions, should be promoted. Where necessary, the use of encryption, in particular end-to-end encryption should be mandatory for providers of public electronic communications networks or of publicly available electronic communications services in accordance with the principles of security and privacy by default and by design for the purposes of this Directive. The use of end-to-end encryption should be reconciled with the Member States' powers to ensure the protection of their essential security interests and public security, and to allow for the prevention, investigation, detection and prosecution of criminal offences in accordance with Union law. However, this should not weaken end-to-end encryption, which is a critical technology for the effective protection of data and privacy and the security of communications.

(99) 公共電子通信ネットワーク及び公衆が利用可能な電子通信サービスの防護を守り，濫用と操作を防止するため，インターネットアクセスサービスプロバイダのエコシステム全域にわたるルーティング機能の完全性と堅牢性を確保するための安全なルーティングの技術標準の利用が促進されるべきである。

In order to safeguard the security, and to prevent abuse and manipulation, of public electronic communications networks and of publicly available electronic communications services, the use of secure routing standards should be promoted to ensure the integrity and robustness of routing functions across the ecosystem of internet access service providers.

(100) インターネットの機能性及び完全性を守るため，そして，DNS の防護と回復力を促進するため，欧州連合の民間部門の法主体を含む関連する利害関係者，公衆が利用可能な電子通信サービスのプロバイダ，とりわけインターネットアクセスサービスプロバイダ，及び，オンライン検索エンジンのプロバイダは，DNS の解決の多様化戦略を採用することが推奨されるべきである。更に，構成国は，公開で安全な欧州の DNS リゾルバサービスの開発及び利用を推奨すべきである。

In order to safeguard the functionality and integrity of the internet and to promote the security and resilience of the DNS, relevant stakeholders including Union private-sector entities, providers of publicly available electronic communications services, in particular internet access service providers, and providers of online search engines should be encouraged to adopt a DNS resolution diversification strategy. Furthermore, Member States should encourage the development and use of a public and secure European DNS resolver service.

(101) 一方における，重大なインシデントの潜在的な拡散の緩和を助け，基礎法主体及び重要法主体が補助を求めることができるようにする迅速な報告と，他方における，個々のインシデントから価値ある教訓を引き出し，個々の法主体及び部門全体のサイバー回復力を徐々に向上させる詳細な報告との間の正しいバランスをとるため，この指令は，重大なインシデントの報告のための多段階のアプローチを定める。この点に関し，この指令は，当該法主体に対してそのサービスの業務運営上の重大な混乱または金銭的な損失を生じさせ，または，有形もしくは無形の甚大な損害を生じさせることによって他の自然人もしくは法人に影響を及ぼすインシデントの，関係する法主体によって実施された当初評価を基礎とする報告を含めるべきである。そのような当初評価は，就中，影響を受けたネットワーク及び情報システム，とりわけ，その法主体のサービスを提供する上での当該ネットワーク及び情報システムの重要性，サイバーな脅威の深刻度及び技術上の特性，根底にある悪用されている脆弱性，並びに，その法主体の類似のインシデントの経験を考慮に入れるべきである。そのサービスの稼働が影響を受けている範囲，インシデントの持続期間，または，影響を受けたサービスの受け手の数のような指標は，そのサービスの業務運営上の混乱が深刻なものかどうかを識別する上で重要な役割を演じ得る。

This Directive lays down a multiple-stage approach to the reporting of significant incidents in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread

of significant incidents and allows essential and important entities to seek assistance, and, on the other, in-depth reporting that draws valuable lessons from individual incidents and improves over time the cyber resilience of individual entities and entire sectors. In that regard, this Directive should include the reporting of incidents that, based on an initial assessment carried out by the entity concerned, could cause severe operational disruption of the services or financial loss for that entity or affect other natural or legal persons by causing considerable material or non-material damage. Such initial assessment should take into account, inter alia, the affected network and information systems, in particular their importance in the provision of the entity's services, the severity and technical characteristics of a cyber threat and any underlying vulnerabilities that are being exploited as well as the entity's experience with similar incidents. Indicators such as the extent to which the functioning of the service is affected, the duration of an incident or the number of affected recipients of services could play an important role in identifying whether the operational disruption of the service is severe.

(102) 基礎法主体または重要法主体が重大なインシデントに気づいたときは，当該法主体は，不適切な遅滞なく，かつ，いかなる場合においても 24 時間以内に，早期警戒を提出することを要求されるべきである。その早期警戒には，インシデント通知が付されるべきである。関係する法主体は，不適切な遅滞なく，かつ，いかなる場合においても重大なインシデントに気づいた時から 72 時間以内に，早期警戒を介して提出された情報をアップデートすること，及び，それが利用可能なときは，そのインシデントの深刻度及び影響並びに侵害指標を含め，重大なインシデントの当初評価を示すことを狙いとするインシデント通知を提出すべきである。インシデント通知の後，1 か月以内に，最終報告書が提出されるべきである。早期警戒は，CSIRT を，または，それが適用可能なときは職務権限のある機関を，重大なインシデントに気づくようにさせるため，及び，それが必要なときは，関係する法主体が補助を求め得るようにするために必要となる情報のみを含めるべきである。そのような早期警戒は，それが適用可能なときは，その重大なインシデントが，違法な行為または悪意ある行為によって生じさせられた疑いがあるかどうか，及び，そのインシデントが，国境を越える影響をもちそうであるかどうかを示すべきである。インシデント報告義務が，重大なインシデントに対応する取扱いの資源を減らすことを防止するため，または，それ以外の，その点に関するその法主体の努力を混乱させることを防止するため，構成国は，その早期警戒またはその後のインシデント通知を提出すべき義務が，通知元法主体の優先されるべきインシデントの取扱いと関連する活動の資源を減らすことがないことを確保すべきである。最終報告書の提出時においてインシデントが進行中の場合，構成国は，関係する法主体が，当該の時点では進行状況報告書を提供し，そして，その重大なインシデントに対するその法主体の取扱いの後の 1 か月以内に最終報告書を提供することを確保すべきである。

Where essential or important entities become aware of a significant incident, they should be required to submit an early warning without undue delay and in any event within 24 hours. That early warning should be followed by an incident notification. The entities concerned should submit an incident notification without undue delay and in any event within 72 hours of becoming aware of the significant incident, with the aim, in particular, of updating information submitted through the early warning and indicating an initial assessment of the significant incident, including its severity and impact, as well as indicators of

compromise, where available. A final report should be submitted not later than one month after the incident notification. The early warning should only include the information necessary to make the CSIRT, or where applicable the competent authority, aware of the significant incident and allow the entity concerned to seek assistance, if required. Such early warning, where applicable, should indicate whether the significant incident is suspected of being caused by unlawful or malicious acts, and whether it is likely to have a cross-border impact. Member States should ensure that the obligation to submit that early warning, or the subsequent incident notification, does not divert the notifying entity's resources from activities related to incident handling that should be prioritised, in order to prevent incident reporting obligations from either diverting resources from significant incident response handling or otherwise compromising the entity's efforts in that respect. In the event of an ongoing incident at the time of the submission of the final report, Member States should ensure that entities concerned provide a progress report at that time, and a final report within one month of their handling of the significant incident.

(103) それが適用可能なときは，基本法主体及び重要法主体は，当該法主体のサービスの受け手に対し，不適切な遅滞なく，重大なサイバーな脅威から生じているリスクを緩和するために当該の受け手がとることのできる手段または解決策を通知すべきである。当該法主体は，それが適切なときは，及び，とりわけ，重大なサイバーな脅威が具体化しそうなときは，当該法主体のサービスの受け手に対し，その脅威それ自体について連絡すべきである。当該法主体のサービスの受け手に対して重大なサイバーな脅威について連絡すべき要件は，最善の努力を基礎として充足されるべきであるが，当該法主体の自己負担により，そのような脅威を防止または解消し，かつ，正常なセキュリティレベルのサービスに復旧するための適切かつ迅速な措置を講ずるべき義務を当該法主体に対して課してはならない。サービスの受け手に対する重大なサイバーな脅威に関するそのような情報の提供は，無料とすべきであり，かつ，容易に理解できる言語で作成されるべきである。

Where applicable, essential and important entities should communicate, without undue delay, to their service recipients any measures or remedies that they can take to mitigate the resulting risks from a significant cyber threat. Those entities should, where appropriate and in particular where the significant cyber threat is likely to materialise, also inform their service recipients of the threat itself. The requirement to inform those recipients of significant cyber threats should be met on a best efforts basis but should not discharge those entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any such threats and restore the normal security level of the service. The provision of such information about significant cyber threats to the service recipients should be free of charge and drafted in easily comprehensible language.

(104) 公共電子通信ネットワークのプロバイダまたは公衆が利用可能な電子通信サービスのプロバイダは，バイデザイン及びバイデフォルトのセキュリティを実装すべきであり，かつ，当該法主体のサービスの受け手に対し，重大なサイバーな脅威について，及び，例えば，特別のタイプのソフトウェアまたは暗号技術を利用することにより，当該サービスの受け手の機器と通信の安全を保護するために当該サービスの受け手がとることのできる手段について，連絡すべきである。

Providers of public electronic communications networks or of publicly available electronic communications services should implement security by design and by default, and inform their service recipients of significant cyber threats and of measures they can take to protect the security of their devices and communications, for example by using specific types of software or encryption technologies.

(105) サイバーな脅威に対するプロアクティブなアプローチは，有形または無形の甚大な損害を生じさせ得るインシデントへとサイバーな脅威が具体化することを職務権限のある機関が実効的に防止できるようにすべきサイバーセキュリティのリスク管理の重要な構成要素の 1 つである。その目的のために，サイバーな脅威の通知は，鍵となる重要性をもつ。その目的のために，法主体は，任意ベースで，サイバーな脅威を報告することが推奨される。

A proactive approach to cyber threats is a vital component of cybersecurity risk management that should enable the competent authorities to effectively prevent cyber threats from materialising into incidents that may cause considerable material or non-material damage. For that purpose, the notification of cyber threats is of key importance. To that end, entities are encouraged to report on a voluntary basis cyber threats.

(106) この指令の下において要求される情報の報告を単純化するため，及び，法主体にかかる管理運営上の負担を軽減するため，構成国は，それらの手段がこの指令の適用範囲内にあるかどうかに拘わらず，単一エントリポイント，自動化されたシステム，オンライン書式，ユーザフレンドリなインタフェイス，雛型，法主体の利用のための専用プラットフォームのような，報告されるべき関連情報の提出のための技術上の手段を提供すべきである。とりわけ，欧州議会及び理事会の規則(EU) 2021/694[21]によって設けられたデジタル欧州計画の範囲内にある，この指令の実装を支える欧州連合の資金提供は，単一エントリポイントのための支援を含み得る。更に，法主体は，しばしば，その法主体の特性のゆえに，ある特定のインシデントが，様々な法律文書に含まれている通知義務の結果として，様々な機関に対して報告されることを要するという状況の中にある。そのような場合には，付加的な管理運営上の負担がつくり出され，そして，そのような通知の書式及び手続と関連する不確実性も導かれ得る。単一エントリポイントが設けられれば，構成国は，規則(EU) 2016/679 及び指令 2002/58/EC のような他の欧州連合法の下で要求されるセキュリティインシデントの通知のために，当該単一エントリポイントを利用することも推奨される。規則(EU) 2016/679 及び指令 2002/58/EC の下にあるセキュリティインシデントの報告のためのそのような単一エントリポイントの利用は，規則(EU) 2016/679 及び指令 2002/58/EC の条項，とりわけ，それらの規則及び指令に示されている機関の独立性と関連する条項の適用に対して影響を与えてはならない。ENISA は，協力グループと協力して，欧州連合法の下で報告されるべき情報を簡素化及び合理化するため，そして，通知する法主体にかかる管理運営上の負担を軽減するための指

[21] デジタル欧州計画を設ける，及び，決定(EU) 2015/2240 を廃止する欧州議会及び理事会の 2021 年 4 月 29 日の規則(EU) 2021/694 (OJ L 166, 11.5.2021, p. 1).
Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (OJ L 166, 11.5.2021, p. 1).

針により，通知の共通雛型を策定すべきである。

In order to simplify the reporting of information required under this Directive as well as to decrease the administrative burden for entities, Member States should provide technical means such as a single entry point, automated systems, online forms, user-friendly interfaces, templates, dedicated platforms for the use of entities, regardless of whether they fall within the scope of this Directive, for the submission of the relevant information to be reported. Union funding supporting the implementation of this Directive, in particular within the Digital Europe programme, established by Regulation (EU) 2021/694 of the European Parliament and of the Council [21], could include support for single entry points. Furthermore, entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional administrative burden and could also lead to uncertainties with regard to the format and procedures of such notifications. Where a single entry point is established, Member States are encouraged also to use that single entry point for notifications of security incidents required under other Union law, such as Regulation (EU) 2016/679 and Directive 2002/58/EC. The use of such single entry point for reporting of security incidents under Regulation (EU) 2016/679 and Directive 2002/58/EC should not affect the application of the provisions of Regulation (EU) 2016/679 and Directive 2002/58/EC, in particular those relating to the independence of the authorities referred to therein. ENISA, in cooperation with the Cooperation Group, should develop common notification templates by means of guidelines to simplify and streamline the information to be reported under Union law and decrease the administrative burden on notifying entities.

(107) インシデントが，欧州連合法または国内法に基づく重大犯罪活動と関連しているという疑いがあるときは，構成国は，基礎法主体及び重要法主体に対し，欧州連合法に従って適用可能な刑事手続規定に基づき，重大犯罪の性質をもつ疑いのあるインシデントを関連法執行機関に報告することを推奨すべきである。それが適切なときは，かつ，Europol に対して適用される個人データ保護の規定を妨げることなく，欧州サイバー犯罪センター（EC3）及び ENISA によって，職務権限のある機関と異なる構成国の法執行機関との間の調整が促進されることが望ましい。

Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage essential and important entities, on the basis of applicable criminal proceedings rules in accordance with Union law, to report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. Where appropriate, and without prejudice to the personal data protection rules applying to Europol, it is desirable that coordination between the competent authorities and the law enforcement authorities of different Member States be facilitated by the European Cybercrime Centre (EC3) and ENISA.

(108) 多数の場合において，個人データは，インシデントの結果として侵害される。その文脈において，職務権限のある機関は，規則(EU) 2016/679 及び指令 2002/58/EC に示す機関との間で協力し，かつ，全ての関連事項に関して情報を交換すべきである。

Personal data are in many cases compromised as a result of incidents. In that context, the competent authorities should cooperate and exchange information about all relevant matters with the authorities referred to in Regulation (EU) 2016/679 and Directive 2002/58/EC.

(109)ドメイン名登録データ（WHOIS データ）の正確かつ完全なデータベースを維持管理すること，そして，そのようなデータへの適法なアクセスを提供することは，DNS の防護，安定性及び回復力を確保するために必須であり，それは，更に，欧州連合全域にわたる共通の高いレベルのサイバーセキュリティに貢献する。その特別の目的のために，TLD 名レジストリ及びドメイン名登録サービスを提供する法主体は，その目的を達成するために必要となる一定のデータを処理することを要求されるべきである。そのような処理は，規則(EU) 2016/679 の第 6 条第 1 項(c)の意味における法律上の義務を組成すべきである。その義務は，例えば，契約上の合意を基礎として，または，別の欧州連合法もしくは国内法の中で定められた法律上の要件を基礎として，別の目的のためにドメイン名登録データを収集できることを妨げない。その義務は，完全かつ正確なセットの登録データを達成することを狙いとし，かつ，同一のデータを複数回にわたって収集する結果となってはならない。TLD 名レジストリ及びドメイン名登録サービスを提供する法主体は，当該職務の重複を避けるため，相互に協力すべきである。

Maintaining accurate and complete databases of domain name registration data (WHOIS data) and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity across the Union. For that specific purpose, TLD name registries and entities providing domain name registration services should be required to process certain data necessary to achieve that purpose. Such processing should constitute a legal obligation within the meaning of Article 6(1), point (c), of Regulation (EU) 2016/679. That obligation is without prejudice to the possibility to collect domain name registration data for other purposes, for example on the basis of contractual arrangements or legal requirements established in other Union or national law. That obligation aims to achieve a complete and accurate set of registration data and should not result in collecting the same data multiple times. The TLD name registries and the entities providing domain name registration services should cooperate with each other in order to avoid the duplication of that task.

(110) 正当なアクセスを求める者にとってのドメイン名登録データの可用性及び適時のアクセシビリティは，DNS の濫用の防止及びそれとの闘いのために，そして，インシデントの防止と検出及びインシデントに対する対応のために必須である。正当なアクセスを求める者は，欧州連合法または国内法により要求を行う自然人または法人として理解されるべきである。それらの者は，この指令の下において職務権限のある機関，及び，犯罪行為の防止，捜査，検知または訴追に関して欧州連合法または国内法の下において職務権限のある機関，並びに，CERT または CSIRT を含み得る。TLD 名レジストリ及びドメイン名登録サービスを提供する法主体は，欧州連合法及び国内法に従った正当なアクセスを求める者に対し，アクセス要求の目的のために必要となる特定のドメイン名登録データへの適法なアクセスをできるようにすることを要求されるべきである。正当なアクセスを求める者の要求は，そのデータへのアクセスの必要性の評価を許容する，理由の説明を

添えるべきである。

The availability and timely accessibility of domain name registration data to legitimate access seekers is essential for the prevention and combating of DNS abuse, and for the prevention and detection of and response to incidents. Legitimate access seekers are to be understood as any natural or legal person making a request pursuant to Union or national law. They can include authorities that are competent under this Directive and those that are competent under Union or national law for the prevention, investigation, detection or prosecution of criminal offences, and CERTs or CSIRTs. TLD name registries and entities providing domain name registration services should be required to enable lawful access to specific domain name registration data, which are necessary for the purposes of the access request, to legitimate access seekers in accordance with Union and national law. The request of legitimate access seekers should be accompanied by a statement of reasons permitting the assessment of the necessity of access to the data.

(111) 正確かつ完全なドメイン名登録データの可用性を確保するため，TLD 名レジストリ及びドメイン名登録サービスを提供する法主体は，ドメイン名登録データを収集し，かつ，その完全性と可用性を保証すべきである。とりわけ，TLD 名レジストリ及びドメイン名登録サービスを提供する法主体は，欧州連合のデータ保護法に従い，正確かつ完全なドメイン名登録データを収集及び維持するため，並びに，不正確な登録データを防止及び訂正するため，基本方針及び手順を策定すべきである。それらの基本方針及び手順は，可能な範囲内で，国際レベルの多角的な利害関係者の統治構造によって策定された技術標準が考慮に入れられるべきである。TLD 名レジストリ及びドメイン名登録サービスを提供する法主体は，ドメイン名登録データを検証するための比例的な手順を採用し，実装すべきである。それらの手順は，産業界の中で使用されているベストプラクティス，及び，可能な範囲内で，電子識別の分野において行われた発展を反映すべきである。検証手順の例は，登録の時点において実施される事前管理，及び，登録後に実施される事後管理を含み得る。TLD 名レジストリ及びドメイン名登録サービスを提供する法主体は，とりわけ，登録者の少なくとも 1 つの連絡手段を検証すべきである。

In order to ensure the availability of accurate and complete domain name registration data, TLD name registries and entities providing domain name registration services should collect and guarantee the integrity and availability of domain name registration data. In particular, TLD name registries and entities providing domain name registration services should establish policies and procedures to collect and maintain accurate and complete domain name registration data, as well as to prevent and correct inaccurate registration data, in accordance with Union data protection law. Those policies and procedures should take into account, to the extent possible, the standards developed by the multi-stakeholder governance structures at international level. The TLD name registries and the entities providing domain name registration services should adopt and implement proportionate procedures to verify domain name registration data. Those procedures should reflect the best practices used within the industry and, to the extent possible, the progress made in the field of electronic identification. Examples of verification procedures may include *ex ante* controls carried out at the time of the registration and *ex post* controls carried out after the registration. The TLD name registries and the entities providing domain name

registration services should, in particular, verify at least one means of contact of the registrant.

(112) TLD 名レジストリ及びドメイン名登録サービスを提供する法主体は，規則(EU) 2016/679 の前文に沿って，法人に関するデータのような，欧州連合のデータ保護法の適用範囲外にあるドメイン名登録データを公表することを要求されるべきである。法人に関しては，TLD 名レジストリ及びドメイン名登録サービスを提供する法主体は，少なくとも登録者名及び連絡先電話番号を公表すべきである。電子メールのエイリアスまたは職場アカウントの場合のような，その電子メールアドレスが個人データを含まないことを条件として，連絡先電子メールアドレスも公表されるべきである。TLD 名レジストリ及びドメイン名登録サービスを提供する法主体は，欧州連合のデータ保護法に従い，正当なアクセスを求める者に対し，自然人に関する特定のドメイン名登録データへの適法なアクセスもできるようにすべきである。構成国は，TLD 名レジストリ及びドメイン名登録サービスを提供する法主体に対し，正当なアクセスを求める者からのドメイン名登録データの開示を求める要求に対し，適切な遅滞なく回答することを要求すべきである。TLD 名レジストリ及びドメイン名登録サービスを提供する法主体は，正当なアクセスを求める者からのアクセスを求める要求に対処するためのサービスレベル合意を含め，登録データの公表及び開示に関する基本方針及び手順を策定すべきである。それらの基本方針と手続は，可能な範囲内で，国際レベルの多角的な利害関係者の統治構造によって策定された指針及び技術標準が考慮に入れるべきである。アクセスの手続は，登録データの要求及びアクセスのための効率的なシステムを提供するためのインタフェイス，ポータルまたはそれら以外の技術上のツールの利用を含め得る。域内市場全域にわたる整合化された実務を促進するという観点から，欧州委員会は，欧州データ保護委員会の職務権限を妨げることなく，可能な範囲内で国際レベルの多角的な利害関係者の統治構造によって策定された技術標準を考慮に入れた，そのような手順と関連する指針を提供できる。構成国は，個人データ及び非個人データであるドメイン名登録データへの全てのタイプのアクセスが無料であることを確保すべきである。

TLD name registries and entities providing domain name registration services should be required to make publicly available domain name registration data that fall outside the scope of Union data protection law, such as data that concern legal persons, in line with the preamble of Regulation (EU) 2016/679. For legal persons, the TLD name registries and the entities providing domain name registration services should make publicly available at least the name of the registrant and the contact telephone number. The contact email address should also be published, provided that it does not contain any personal data, such as in the case of email aliases or functional accounts. TLD name registries and entities providing domain name registration services should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States should require TLD name registries and entities providing domain name registration services to respond without undue delay to requests for the disclosure of domain name registration data from legitimate access seekers. TLD name registries and entities providing domain name registration services should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. Those policies and procedures should take into account, to the extent possible, any guidance and the standards

developed by the multi-stakeholder governance structures at international level. The access procedure could include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission can, without prejudice to the competences of the European Data Protection Board, provide guidelines with regard to such procedures, which take into account, to the extent possible, the standards developed by the multi-stakeholder governance structures at international level. Member States should ensure that all types of access to personal and non-personal domain name registration data are free of charge.

(113) この指令の適用範囲内にある法主体は，当該法主体の拠点がある構成国の管轄権の下にあると判断されるべきである。ただし，公共電子通信ネットワークのプロバイダまたは公衆が利用可能な電子通信サービスのプロバイダは，当該プロバイダが当該プロバイダのサービスを提供する構成国の管轄権の下にあると判断されるべきである。DNS サービスのプロバイダ，TLD 名レジストリ，ドメイン名登録サービスを提供する法主体，クラウドコンピューティングサービスのプロバイダ，データセンターサービスのプロバイダ，コンテント伝達ネットワークのプロバイダ，マネージドサービスのプロバイダ，マネージドセキュリティサービスのプロバイダ，並びに，オンライン市場のプロバイダ，オンライン検索エンジンのプロバイダ及びソーシャルネットワーキングサービスプラットフォームのプロバイダは，当該プロバイダが当該プロバイダの欧州連合内における主たる拠点をもつ構成国の管轄権の下にあると判断されるべきである。行政機関である法主体は，当該法主体を設置した構成国の管轄権の下にあると判断されるべきである。その法主体が複数の構成国においてサービスを提供しまたは設置されている場合，その法主体は，それらそれぞれの構成国の個別的な管轄権または競合する管轄権の下にあると判断されるべきである。それらの構成国の職務権限のある機関は，協力し，互いに相互補助を提供し，また，それが適切なときは，共同で監督活動を遂行すべきである。構成国が管轄権を行使する場合，一事不再理の原則に沿って，同一の行為に対し，複数回にわたり執行措置または制裁を加えてはならない。

Entities falling within the scope of this Directive should be considered to fall under the jurisdiction of the Member State in which they are established. However, providers of public electronic communications networks or providers of publicly available electronic communications services should be considered to fall under the jurisdiction of the Member State in which they provide their services. DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms should be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union. Public administration entities should fall under the jurisdiction of the Member State which established them. If the entity provides services or is established in more than one Member State, it should fall under the separate and concurrent jurisdiction of each of those Member States. The competent authorities of those Member States should cooperate, provide mutual assistance to each other and, where appropriate, carry out joint supervisory actions. Where Member States exercise jurisdiction, they should not impose

enforcement measures or penalties more than once for the same conduct, in line with the principle of *ne bis in idem*.

(114) DNS サービスのプロバイダ，TLD 名レジストリ，ドメイン名登録サービスを提供する法主体，クラウドコンピューティングサービスのプロバイダ，データセンターサービスのプロバイダ，コンテント伝達ネットワークのプロバイダ，マネージドサービスのプロバイダ，マネージドセキュリティサービスのプロバイダ，並びに，オンライン市場のプロバイダ，オンライン検索エンジンのプロバイダ及びソーシャルネットワーキングサービスプラットフォームのプロバイダのサービス及び業務運営の国境を越える性質を考慮に入れるため，当該法主体に対し，1 つの構成国だけが管轄権をもつべきである。管轄権は，関係する法主体が欧州連合内における主たる拠点をもつ構成国に属するべきである。この指令の目的のための拠点の判断基準とは，永続的な配置を介した活動の実効的な実施のことを意味する。そのような配置の法形式は，法人格をもつ支店または子会社であるか否かを問わず，その点に関する判断を決める要素とはならない。当該判断基準を満たしているか否かは，そのネットワーク及び情報システムが当の場所に物理的に位置しているかどうかに依拠してはならない；そのようなシステムの存在及び利用は，それ自体としては，そのような主たる拠点を組成せず，それゆえ，主たる拠点を決めるための決定的な判断基準ではない。主たる拠点は，欧州連合内におけるサイバーセキュリティのリスク管理の措置と関連する決定が主として行われる構成国にあると判断されるべきである。これは，典型的には，その法主体の欧州連合内における中枢管理のある場所に対応するであろう。そのような構成国が決定され得ない場合，または，そのような決定が欧州連合内では行われない場合，その主たる拠点は，サイバーセキュリティの業務運営が実施される構成国にあると判断されるべきである。そのような構成国が決定され得ない場合，その主たる拠点は，その法主体が，欧州連合内における最多従業者数の拠点をもつ構成国にあると判断されるべきである。サービスが事業者のグループによって実施される場合，支配的な事業者の主たる拠点がその事業者グループの主たる拠点であると判断されるべきである。

In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, only one Member State should have jurisdiction over those entities. Jurisdiction should be attributed to the Member State in which the entity concerned has its main establishment in the Union. The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. Whether that criterion is fulfilled should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not decisive criteria for determining the main establishment. The main establishment should be considered to be in the Member State where the decisions related to the cybersecurity risk-management measures are predominantly taken in the Union. This will typically correspond to the place of the entities' central administration in the Union. If such a Member State cannot

be determined or if such decisions are not taken in the Union, the main establishment should be considered to be in the Member State where cybersecurity operations are carried out. If such a Member State cannot be determined, the main establishment should be considered to be in the Member State where the entity has the establishment with the highest number of employees in the Union. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings.

(115) 公衆が利用可能な再帰的 DNS サービスが，公共電子通信ネットワークのプロバイダまたは公衆が利用可能な電子通信サービスのプロバイダから，インターネットアクセスサービスの一部としてのみ提供されているときは，その法主体は，その法主体のサービスが提供されている全ての構成国の管轄権の下にあると判断されるべきである。

Where a publicly available recursive DNS service is provided by a provider of public electronic communications networks or of publicly available electronic communications services only as a part of the internet access service, the entity should be considered to fall under the jurisdiction of all the Member States where its services are provided.

(116) 欧州連合内に拠点がない DNS サービスのプロバイダ，TLD 名レジストリ，ドメイン名登録サービスを提供する法主体，クラウドコンピューティングサービスのプロバイダ，データセンターサービスのプロバイダ，コンテント伝達ネットワークのプロバイダ，マネージドサービスのプロバイダ，マネージドセキュリティサービスのプロバイダ，または，オンライン市場のプロバイダ，オンライン検索エンジンのプロバイダもしくはソーシャルネットワーキングサービスプラットフォームのプロバイダが，欧州連合内でサービスを提供するときは，その法主体は，欧州連合内における代理者を指定すべきである。そのような法主体が欧州連合内においてサービスを提供しているかどうかを決定するため，その法主体が，1 または複数の構成国内の者に対してサービスを提供することを計画しているかどうかが確認されるべきである。その法主体もしくは中間介在者の Web サイトまたは電子メールアドレス及びそれら以外の連絡先が欧州連合内においてアクセス可能であるということだけでは，または，その法主体が拠点をもつ第三国内において一般に使用されている言語が使用されていることだけでは，そのような意図を確認するためには不十分であると判断されるべきである。ただし，1 もしくは複数の構成国において一般に使用されている言語もしくは通貨が利用されており，当該言語によりサービスの申込みができること，または，欧州連合内にいる顧客もしくは利用者についての言及のような要素は，その法主体が欧州連合内においてサービスを提供することを計画していることを明らかにし得る。代理者は，その法主体の代わりに行動すべきであり，かつ，職務権限のある機関または CSIRT は，代理者を名宛人とし得るべきである。代理者は，インシデント報告を含め，この指令に定める法主体の義務と関連してその法主体の代わりに行動するために，その法主体の書面による委任によって明示で指定されるべきである。

Where a DNS service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider or a provider of an online

marketplace, of an online search engine or of a social networking services platform, which is not established in the Union, offers services within the Union, it should designate a representative in the Union. In order to determine whether such an entity is offering services within the Union, it should be ascertained whether the entity is planning to offer services to persons in one or more Member States. The mere accessibility in the Union of the entity's or an intermediary's website or of an email address or other contact details, or the use of a language generally used in the third country where the entity is established, should be considered to be insufficient to ascertain such an intention. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that language, or the mentioning of customers or users who are in the Union, could make it apparent that the entity is planning to offer services within the Union. The representative should act on behalf of the entity and it should be possible for the competent authorities or the CSIRTs to address the representative. The representative should be explicitly designated by a written mandate of the entity to act on the latter's behalf with regard to the latter's obligations laid down in this Directive, including incident reporting.

(117) この指令の適用範囲内にあるサービスを欧州連合全域において提供する DNS サービスのプロバイダ，TLD 名レジストリ，ドメイン名登録サービスを提供する法主体，クラウドコンピューティングサービスのプロバイダ，データセンターサービスのプロバイダ，コンテント伝達ネットワークのプロバイダ，マネージドサービスのプロバイダ，マネージドセキュリティサービスのプロバイダ，並びに，オンライン市場のプロバイダ，オンライン検索エンジンのプロバイダ及びソーシャルネットワーキングサービスプラットフォームのプロバイダの明確な概観を確保するため，ENISA は，それが適用可能なときは，法主体が自らを登録するために設けられた国内の仕組みを介し，構成国によって受領された情報を基礎とする，そのような法主体の登録簿を創設し，かつ，維持管理すべきである。単一連絡部局は，ENISA に対し，その情報及びその情報の変更を転送すべきである。当該登録簿に収録されるべき情報の正確性及び完全性を確保するという観点から，構成国は，ENISA に対し，当該法主体に関する国内登録簿内で利用可能な情報を提出できる。ENISA 及び構成国は，秘密情報または機密情報の保護を確保しつつ，そのような登録簿の相互運用性を促進するための措置を講ずるべきである。ENISA は，開示された情報の防護及び機密性を確保し，かつ，想定される利用者に対し，そのような情報のアクセス，記録保存及び伝送を制限するための適切な情報分類及び情報管理のプロトコルを策定すべきである。

In order to ensure a clear overview of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, which provide services across the Union that fall within the scope of this Directive, ENISA should create and maintain a registry of such entities, based on the information received by Member States, where applicable through national mechanisms established for entities to register themselves. The single points of contact should forward to ENISA the information and any changes thereto. With a view to ensuring the accuracy and completeness of the information that is to be included in that registry,

Member States can submit to ENISA the information available in any national registries on those entities. ENISA and the Member States should take measures to facilitate the interoperability of such registries, while ensuring protection of confidential or classified information. ENISA should establish appropriate information classification and management protocols to ensure the security and confidentiality of disclosed information and restrict the access, storage, and transmission of such information to intended users.

(118) 欧州連合法または国内法に従って機密である情報が，この指令に基づいて交換され，報告され，または，それ以外に共有される場合，機密情報の取扱いに関して対応する規定が適用されるべきである。加えて，ENISA は，EU 機密情報を保護するための適用可能な防護規定に従い，機微の機密情報を取扱うためのインフラ，手続及び規定を設けるべきである。

Where information which is classified in accordance with Union or national law is exchanged, reported or otherwise shared under this Directive, the corresponding rules on the handling of classified information should be applied. In addition, ENISA should have the infrastructure, procedures and rules in place to handle sensitive and classified information in accordance with the applicable security rules for protecting EU classified information.

(119) サイバーな脅威がより複雑で巧妙になってきていることに伴い，そのような脅威の良好な検出及びそれらの脅威の防止の措置は，広範囲に，法主体間における脅威及び脆弱性の情報の恒常的な共有に依存している。情報共有は，サイバーな脅威の認識向上に寄与し，それは，更に，そのような脅威がインシデントへと具体化することを防止するための法主体の実現能力を拡大し，かつ，法主体がインシデントの影響をより良く封じ込め，また，より効率的に回復できるようにする。欧州連合レベルのガイドがない中で，様々な要素が，とりわけ，競争の規定及び法的責任の規定との互換性に関する不確実性が，そのような情報の共有を困難にさせているようである。

With cyber threats becoming more complex and sophisticated, good detection of such threats and their prevention measures depend to a large extent on regular threat and vulnerability intelligence sharing between entities. Information sharing contributes to an increased awareness of cyber threats, which, in turn, enhances entities' capacity to prevent such threats from materialising into incidents and enables entities to better contain the effects of incidents and recover more efficiently. In the absence of guidance at Union level, various factors seem to have inhibited such intelligence sharing, in particular uncertainty over the compatibility with competition and liability rules.

(120) 法主体は，インシデントを適切に防止，検出し，インシデントに対応し，もしくは，インシデントから回復するための法主体の実現能力を拡大するため，または，インシデントの影響を緩和するため，法主体の個々の知識及び実務経験を，戦略レベル，戦術レベル及び運用レベルで集団的に活用することを，構成国によって推奨され，かつ，その助けを受けるべきである。そして，任意のサイバーセキュリティ情報共有覚書が欧州連合レベルで存在できるようにする必要がある。その目的のために，構成国は，サイバーセキュリティサービス及び調査研究を提供する法主体のような

法主体に対し，並びに，この指令の適用範囲内にはない関連法主体に対し，能動的に，そのようなサイバーセキュリティ情報共有覚書に参加することを助け，推奨すべきである。それらの覚書は，欧州連合の競争規定及び欧州連合のデータ保護法に従って定められるべきである。

Entities should be encouraged and assisted by Member States to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhancing their capabilities to adequately prevent, detect, respond to or recover from incidents or to mitigate their impact. It is thus necessary to enable the emergence at Union level of voluntary cybersecurity information-sharing arrangements. To that end, Member States should actively assist and encourage entities, such as those providing cybersecurity services and research, as well as relevant entities not falling within the scope of this Directive, to participate in such cybersecurity information-sharing arrangements. Those arrangements should be established in accordance with the Union competition rules and Union data protection law.

(121) 基礎法主体及び重要法主体によるネットワーク及び情報システムの防護を確保する目的のために必要かつ比例的な範囲内にある個人データの処理は，規則(EU) 2016/679 の第 6 条第 1 項(c)及び第 6 条第 3 項の要件に従い，管理者が服するべき法律上の義務をそのような処理が遵守していることを根拠として，適法であると判断され得る。個人データの処理は，サイバーセキュリティ情報共有覚書またはこの指令に従った関連情報の任意の通知のためにそのような処理が必要となる場合を含め，規則(EU) 2016/679 の第 6 条第 1 項(f)により，基礎法主体及び重要法主体，並びに，当該法主体の代わりに行動するセキュリティ技術及びサービスのプロバイダによって求められる正当な利益のためにも必要であり得る。インシデントの防止，検出，識別，封じ込め，分析及びインシデントへの対応と関連する措置，特定のサイバーな脅威と関係する注意喚起の措置，脆弱性の修復及び調整された脆弱性開示の過程における情報の交換，それらのインシデント，及び，サイバーな脅威と脆弱性，侵害指標，戦略，技法と手順，サイバーセキュリティ警報及び構成ツールに関する任意の情報交換は，IP アドレス，統一資源位置指定子（URL），ドメイン名，電子メールアドレス，及び，それが個人データを明らかにするときは，タイムスタンプのような，一定の類型の個人データの処理を要求し得る。職務権限のある機関，単一連絡部局及び CSIRT による個人データの処理は，規則(EU) 2016/679 の第 6 条第 1 項(c)もしくは(e)及び第 6 条第 3 項により，公共の利益における職務の遂行または管理者に属する公的権限の行使における職務の遂行のための，または，同規則の第 6 条第 1 項(f)に示す，基礎法主体及び重要法主体の正当な利益を求めるための，法的義務を組成し得るものであり，または，それらのために必要であると判断され得る。更に，国内法は，とりわけ，特別類型のデータの二次利用に関する技術上の制限並びに仮名化のような最新のセキュリティ措置及びプライバシー保存措置の使用，または，求める目的に対して匿名化が大きな影響を与え得る場合における暗号化を含め，自然人の基本的な権利及び利益を守るための適切な特別の措置を定めることによって，職務権限のある機関，単一連絡部局及び CSIRT が，基礎法主体及び重要法主体のネットワーク及び情報システムの防護を確保する目的のために必要かつ比例的な範囲内で，規則(EU) 2016/679 の第 9 条に従って特別類型の個人データを処理できるようにする規定を定め得る。

The processing of personal data, to the extent necessary and proportionate for the purpose of ensuring security of network and information systems by essential and important entities, could be considered to be lawful on the basis that such processing complies with a legal obligation to which the controller is subject, in accordance with the requirements of Article 6(1), point (c), and Article 6(3) of Regulation (EU) 2016/679. Processing of personal data could also be necessary for legitimate interests pursued by essential and important entities, as well as providers of security technologies and services acting on behalf of those entities, pursuant to Article 6(1), point (f), of Regulation (EU) 2016/679, including where such processing is necessary for cybersecurity information-sharing arrangements or the voluntary notification of relevant information in accordance with this Directive. Measures related to the prevention, detection, identification, containment, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated vulnerability disclosure, the voluntary exchange of information about those incidents, and cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools could require the processing of certain categories of personal data, such as IP addresses, uniform resources locators (URLs), domain names, email addresses and, where they reveal personal data, time stamps. Processing of personal data by the competent authorities, the single points of contact and the CSIRTs, could constitute a legal obligation or be considered to be necessary for carrying out a task in the public interest or in the exercise of official authority vested in the controller pursuant to Article 6(1), point (c) or (e), and Article 6(3) of Regulation (EU) 2016/679, or for pursuing a legitimate interest of the essential and important entities, as referred to in Article 6(1), point (f), of that Regulation. Furthermore, national law could lay down rules allowing the competent authorities, the single points of contact and the CSIRTs, to the extent that is necessary and proportionate for the purpose of ensuring the security of network and information systems of essential and important entities, to process special categories of personal data in accordance with Article 9 of Regulation (EU) 2016/679, in particular by providing for suitable and specific measures to safeguard the fundamental rights and interests of natural persons, including technical limitations on the re-use of such data and the use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.

(122) 実効的な遵守の確保を助ける監督の権限と措置を強化するため，この指令は，それを介して職務権限のある機関が基礎法主体及び重要法主体を監督できる監督の措置と手段のミニマムのリストを定めるべきである。加えて，基礎法主体及び重要法主体の義務と職務権限のある機関の義務の適正なバランスを確保するという観点から，この指令は，基礎法主体と重要法主体との間の監督制度の区別を定めるべきである。それゆえ，基礎法主体は，包括的な事前及び事後の監督制度に服すべきであるが，重要法主体は，軽い事後監督制度のみに服すべきである。それゆえ，重要法主体は，サイバーセキュリティのリスク管理の措置の遵守を自動的に文書化することを要求されてはならないが，職務権限のある機関は，監督のための事後対応的なアプローチを実装すべきであり，従って，当該法主体を監督すべき一般的義務をもたない。重要法主体の事後監督は，この指令の潜在的な違反行為を示唆すると職務権限のある機関によって判断され，それらの職務権限のある機関の注意を喚起した証跡，兆候または情報によって発動され得る。例えば，そ

のような証跡，兆候または情報は，他の機関，法主体，市民，報道機関またはそれ以外の情報源もしくは公衆が利用可能な情報によってその職務権限のある機関に対して提供されるタイプのものであり得るし，または，その職務権限のある機関の職務を満たす上で，その職務権限のある機関によって実施された別の活動から生じ得る。

In order to strengthen the supervisory powers and measures that help ensure effective compliance, this Directive should provide for a minimum list of supervisory measures and means through which the competent authorities can supervise essential and important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important entities with a view to ensuring a fair balance of obligations on those entities and on the competent authorities. Therefore, essential entities should be subject to a comprehensive *ex ante* and *ex post* supervisory regime, while important entities should be subject to a light, *ex post* only, supervisory regime. Important entities should therefore not be required to systematically document compliance with cybersecurity risk-management measures, while the competent authorities should implement a reactive *ex post* approach to supervision and, hence, not have a general obligation to supervise those entities. The *ex post* supervision of important entities may be triggered by evidence, indication or information brought to the attention of the competent authorities considered by those authorities to suggest potential infringements of this Directive. For example, such evidence, indication or information could be of the type provided to the competent authorities by other authorities, entities, citizens, media or other sources or publicly available information, or could emerge from other activities conducted by the competent authorities in the fulfilment of their tasks.

(123) 職務権限のある機関による監督の職務の執行は，関係する法主体の企業活動を無用に阻害してはならない。職務権限のある機関が，施設内における点検及び施設外の監督の実施，この指令の違反行為の調査，並びに，セキュリティ監査またはセキュリティ検査の実施を含め，基礎法主体と関係するその職務権限のある機関の監督の職務を執行するときは，当該職務権限のある機関は，関係する法主体の企業活動に対する影響をミニマム化すべきである。

The execution of supervisory tasks by the competent authorities should not unnecessarily hamper the business activities of the entity concerned. Where the competent authorities execute their supervisory tasks in relation to essential entities, including the conduct of on-site inspections and off-site supervision, the investigation of infringements of this Directive and the conduct of security audits or security scans, they should minimise the impact on the business activities of the entity concerned.

(124) 事前の監督の執行において，職務権限のある機関は，比例的な態様で自由に，監督の措置及び手段の利用の優先順位を決定できるべきである。このことは，その職務権限のある機関が，リスクベースのアプローチに従うべき監督手法を基礎としてそのような優先順位を決定できるということを伴う。より個別的には，そのような手法は，施設内における検査，的を絞ったセキュリティ監査またはセキュリティ検査の利用，頻度またはタイプ，要求される情報のタイプ，及び，当該情報の詳細さのレベルのような，リスク類型による基礎法主体の分類のための基準または指標並びにそれ

と対応するリスク類型毎に推奨される監督の措置及び手段を含み得る。そのような監督の手法は，作業計画も伴い得るものであり，また，資源の配分及び需要のような側面に関するものを含め，定期的に評価され，見直され得る。行政機関である法主体に関しては，監督の権限は，国内の立法及び国家組織の枠組みに沿って執行されるべきである。

In the exercise of *ex ante* supervision, the competent authorities should be able to decide on the prioritisation of the use of supervisory measures and means at their disposal in a proportionate manner. This entails that the competent authorities can decide on such prioritisation based on supervisory methodologies which should follow a risk-based approach. More specifically, such methodologies could include criteria or benchmarks for the classification of essential entities into risk categories and corresponding supervisory measures and means recommended per risk category, such as the use, frequency or types of on-site inspections, targeted security audits or security scans, the type of information to be requested and the level of detail of that information. Such supervisory methodologies could also be accompanied by work programmes and be assessed and reviewed on a regular basis, including on aspects such as resource allocation and needs. In relation to public administration entities, the supervisory powers should be exercised in line with the national legislative and institutional frameworks.

(125) 職務権限のある機関は，基礎法主体及び重要法主体と関係するその職務権限のある機関の監督の職務が，訓練を受けた専門家によって遂行されることを確保すべきであり，その者は，とりわけ，施設内における検査及び施設外の監督の実施に関し，データベース，ハードウェア，ファイアウォール，暗号及びネットワークにある弱点の識別を含め，それらの監督の職務を遂行するために必要となる技能をもつべきである。それらの施設内における点検及び施設外の監督は，客観的な態様で実施されるべきである。

The competent authorities should ensure that their supervisory tasks in relation to essential and important entities are carried out by trained professionals, who should have the necessary skills to carry out those tasks, in particular with regard to conducting on-site inspections and off-site supervision, including the identification of weaknesses in databases, hardware, firewalls, encryption and networks. Those inspections and that supervision should be conducted in an objective manner.

(126) 重大なサイバーな脅威または差し迫ったリスクに気づいており，それが適正に根拠づけられる場合において，職務権限のある機関は，インシデントの防止またはインシデントに対する対応を狙いとする即時の執行決定を行い得るべきである。

In duly substantiated cases where it is aware of a significant cyber threat or an imminent risk, the competent authority should be able to take immediate enforcement decisions with the aim of preventing or responding to an incident.

(127) 執行を実効性のあるものとするため，この指令に定めるサイバーセキュリティのリスク管理の措置及び報告義務の違反に対して執行され得る執行の権限の，欧州連合全域におけるそのような執

行のための明確かつ一貫性のある枠組みを定めるミニマムのリストが定められるべきである。この指令の違反行為の性質，重大性及び持続期間，発生した有形または無形の損害，その違反行為が意図的だったか，過失によるものだったか，有形または無形の損害の防止または緩和のためにとられた行動，責任の程度または関連する既往の違反行為，職務権限のある機関との間の協力の程度，並びに，それら以外の，増悪または緩和の諸要素を適切に考慮に入れるべきである。行政上の制裁金を含め，執行の措置は，比例的であるべきであり，それらの執行の実施は，実効的な救済及び公正な裁判の権利，無罪の推定並びに防御の権利を含め，欧州連合法及び欧州連合基本権憲章（「憲章」）の基本原則に従った適切な手続上の安全確保に服するべきである。

In order to make enforcement effective, a minimum list of enforcement powers that can be exercised for breach of the cybersecurity risk-management measures and reporting obligations provided for in this Directive should be laid down, setting up a clear and consistent framework for such enforcement across the Union. Due regard should be given to the nature, gravity and duration of the infringement of this Directive, the material or non-material damage caused, whether the infringement was intentional or negligent, actions taken to prevent or mitigate the material or non-material damage, the degree of responsibility or any relevant previous infringements, the degree of cooperation with the competent authority and any other aggravating or mitigating factor. The enforcement measures, including administrative fines, should be proportionate and their imposition should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union (the ‘Charter’), including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.

(128) この指令は，構成国に対し，この指令の違反行為の結果として第三者が被った損害に関し，法主体がこの指令を遵守することを確保することに責任を負う自然人と関連する刑事上または民事上の法的責任を定めることを要求しない。

This Directive does not require Member States to provide for criminal or civil liability with regard to natural persons with responsibility for ensuring that an entity complies with this Directive for damage suffered by third parties as a result of an infringement of this Directive.

(129) この指令に定める義務の実効的な執行を確保するため，個々の職務権限のある機関は，行政上の制裁金を科す権限またはそれを科すことを要求する権限をもつべきである。

In order to ensure effective enforcement of the obligations laid down in this Directive, each competent authority should have the power to impose or request the imposition of administrative fines.

(130) 事業者である基礎法主体または重要法主体に対して行政上の制裁金が科される場合，事業者は，それらの目的のために TFEU の第 101 条及び第 102 条に従った事業者であると理解されるべきである。事業者ではない者に対して行政上の制裁金が科される場合，職務権限のある機関は，

妥当な制裁金額を検討する際，その構成国内の一般的な収入レベル及びその者の経済状態を考慮に入れるべきである。行政機関が行政上の制裁金に服するべきかどうか，その範囲で服するべきかを決定するのは，構成国とすべきである。行政上の制裁金を科すことは，職務権限のある機関の他の権限の適用，または，この指令を国内法化する国内規定に定める他の制裁の適用に対して影響を与えない。

Where an administrative fine is imposed on an essential or important entity that is an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where an administrative fine is imposed on a person that is not an undertaking, the competent authority should take account of the general level of income in the Member State as well as the economic situation of the person when considering the appropriate amount of the fine. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines. Imposing an administrative fine does not affect the application of other powers of the competent authorities or of other penalties laid down in the national rules transposing this Directive.

(131) 構成国は，この指令を国内法化する国内規定の違反行為に対する刑事上の制裁に関する規定を定め得るべきである。ただし，そのような国内規定の違反行為に対して刑事上の制裁を科すこと及び関連する行政上の制裁金を科すことは，欧州連合司法裁判所によって解釈されるものとしての一事不再理の原則の違反を導いてはならない。

Member States should be able to lay down the rules on criminal penalties for infringements of the national rules transposing this Directive. However, the imposition of criminal penalties for infringements of such national rules and of related administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice of the European Union.

(132) この指令が行政上の制裁金を整合化しない場合，または，それら以外に必要がある場合，例えば，この指令の重大な違反行為の場合において，構成国は，実効的であり，比例的であり，かつ，抑止力のある制裁を定める制度を実装すべきである。そのような制裁の性質及びその制裁を刑事制裁とするか行政制裁とするかは，国内法によって決定されるべきである。

Where this Directive does not harmonise administrative penalties or where necessary in other cases, for example in the event of a serious infringement of this Directive, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties and whether they are criminal or administrative should be determined by national law.

(133) この指令の違反行為に対して適用可能な執行措置の実効性及び抑止力を更に強化するため，職務権限のある機関は，基礎法主体から提供される関連サービスまたは基礎法主体によって遂行される関連活動の一部または全部に関し，認証または認可を一時的に停止し，または，その一時的な停止を要求する権限，並びに，最高執行責任者または法律上の代理者のレベルで経営上の責任を負う自然人による経営上の権能の行使の一時的な禁止を課すことを要求する権限を

与えられるべきである。それらの一時的な停止または禁止の厳しさ及び法主体の活動に対する影響と究極的には利用者に対する影響に鑑み，そのような一時的な停止または禁止は，その違反行為の深刻度に比例してのみ，かつ，その違反行為が意図的だったか，過失によるものだったか，及び，有形または無形の損害の防止または緩和のためにとられた行動を含め，個々の事案の状況を考慮に入れた上でのみ，適用されるべきである。そのような一時的な停止または禁止は，最後の手段としてのみ，すなわち，この指令に定める関連する他の執行措置が尽きた後に限り，かつ，関係する法主体が，その欠点を解消するために必要となる活動を行うまで，または，それを求めてそのような一時的な停止もしくは禁止が適用された，その職務権限のある機関の要求を遵守ために必要となる活動を行うまでに限り，適用されるべきである。そのような一時的な停止または禁止を課すことは，実効的な救済及び公正な裁判の権利，無罪の推定並びに防御の権利を含め，欧州連合法及び憲章の基本原則に従った適切な手続上の安全確保に服するべきである。

In order to further strengthen the effectiveness and dissuasiveness of the enforcement measures applicable to infringements of this Directive, the competent authorities should be empowered to suspend temporarily or to request the temporary suspension of a certification or authorisation concerning part or all of the relevant services provided or activities carried out by an essential entity and request the imposition of a temporary prohibition of the exercise of managerial functions by any natural person discharging managerial responsibilities at chief executive officer or legal representative level. Given their severity and impact on the entities' activities and ultimately on users, such temporary suspensions or prohibitions should only be applied proportionally to the severity of the infringement and taking account of the circumstances of each individual case, including whether the infringement was intentional or negligent, and any actions taken to prevent or mitigate the material or non-material damage. Such temporary suspensions or prohibitions should only be applied as a last resort, namely only after the other relevant enforcement measures laid down in this Directive have been exhausted, and only until the entity concerned takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such temporary suspensions or prohibitions were applied. The imposition of such temporary suspensions or prohibitions should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.

(134) この指令に定める法主体の義務の法主体による遵守を確保する目的のために，とりわけ，法主体が複数の構成国においてサービスを提供する場合において，または，法主体のネットワーク及び情報システムが，その法主体がサービスを提供する構成国以外の構成国内に所在している場合において，構成国は，監督の措置及び執行の措置に関し，協力し，かつ，相互に補助すべきである。補助を提供するときは，要請先である職務権限のある機関は，国内法に従って監督の措置または執行の措置を講ずるべきである。この指令に基づく相互補助の円滑な稼働を確保するため，職務権限のある機関は，案件について討議するための，及び，とりわけ，補助を求める要請について討議するためのフォーラムとして，協力グループを利用すべきである。

For the purpose of ensuring entities' compliance with their obligations laid down in this Directive, Member States should cooperate with and assist each other with regard to supervisory and enforcement measures, in particular where an entity provides services in more than one Member State or where its network and information systems are located in a Member State other than that where it provides services. When providing assistance, the requested competent authority should take supervisory or enforcement measures in accordance with national law. In order to ensure the smooth functioning of mutual assistance under this Directive, the competent authorities should use the Cooperation Group as a forum to discuss cases and particular requests for assistance.

(135) とりわけ，国境を越える局面をもつ状況において，実効的な監督と執行を確保するため，相互補助の要請を受けた構成国は，当該要請の期限内に，当該要請の適用対象となっており，かつ，当該構成国の領土内でサービスを提供する法主体，または，その構成国の領土内にネットワーク及び情報システムをもつ法主体と関係する適切な監督の措置及び執行の措置を講ずるべきである。

In order to ensure effective supervision and enforcement, in particular in a situation with a cross-border dimension, a Member State that has received a request for mutual assistance should, within the limits of that request, take appropriate supervisory and enforcement measures in relation to the entity that is the subject of that request, and that provides services or has a network and information system on the territory of that Member State.

(136) この指令は，個人データと関連するこの指令の違反行為に対処するための，職務権限のある機関と規則(EU) 2016/679 の下にある監督機関との間の協力の規定を定めるべきである。

This Directive should establish cooperation rules between the competent authorities and the supervisory authorities under Regulation (EU) 2016/679 to deal with infringements of this Directive related to personal data.

(137) この指令は，基礎法主体及び重要法主体のレベルにおいて高いレベルの，サイバーセキュリティのリスク管理の措置及び報告義務に関する責任を確保することを狙いとすべきである。それゆえ，基礎法主体及び重要法主体の経営陣は，サイバーセキュリティのリスク管理の措置を承認し，そして，その実装を監督すべきである。

This Directive should aim to ensure a high level of responsibility for the cybersecurity risk-management measures and reporting obligations at the level of the essential and important entities. Therefore, the management bodies of the essential and important entities should approve the cybersecurity risk-management measures and oversee their implementation.

(138) この指令を基礎とし，欧州連合全域にわたる共通の高いレベルのサイバーセキュリティを確保するため，どの類型の基礎法主体及び重要法主体が，一定の認証を受けた ICT 製品，ICT サービス及び ICT プロセスを使用することを要求されるべきか，または，欧州サイバーセキュリティ認証

制度の下にある認証を得るべきかを定めることによってこの指令を補完することに関し，TFEU の第 290 条に従って行為を採択する権限は，欧州委員会に対して委任されるべきである。欧州委員会が，その準備作業の間，専門家レベルのものを含め，適切な意見聴取を実施すること，当該意見聴取が，より良い立法のための 2016 年 4 月 13 日の機関間合意[22]に定める基本原則に従って遂行されることは，特に重要なことである。とりわけ，委任される行為の準備への平等な参加を確保するため，欧州議会及び理事会は，構成国の専門家と同時に全ての文書を受領し，かつ，それらの専門家は，自動的に，委任される行為の準備を取り扱う欧州委員会の専門家グループの会合へのアクセスをもつ。

In order to ensure a high common level of cybersecurity across the Union on the basis of this Directive, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of supplementing this Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making [(22)]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(139) この指令の実装のための統一的な条件を確保するため，協力グループの稼働のために必要な手続覚書，サイバーセキュリティのリスク管理の措置と関係する技術上の要件，手法上の要件及び部門別の要件を定めるための実装権限，並びに，情報のタイプ，インシデント，サイバーな脅威及びニアミスの通知，重大なサイバーな脅威の通知の書式と手続，並びに，あるインシデントが重大であると判断されるべき場合をより細かく定めるための実装権限は，欧州委員会に対して与えられるべきである。当該権限は，欧州議会及び理事会の規則(EU) No 182/2011[23]に従って行使されるべきである。

In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission to lay down the procedural arrangements necessary for the functioning of the Cooperation Group and the technical and methodological as well as sectoral requirements concerning the cybersecurity risk-management measures, and to further specify the type of

---

22 OJ L 123, 12.5.2016, p. 1.

23 欧州委員会の実装権限の行使の構成国による管理のための仕組みに関する規定及び一般原則を定める欧州議会及び理事会の 2011 年 2 月 16 日の規則(EU) No 182/2011 (OJ L 55, 28.2.2011, p. 13).
Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

information, the format and the procedure of incident, cyber threat and near miss notifications and of significant cyber threat communications, as well as cases in which an incident is to be considered to be significant. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[(23)].

(140) 欧州委員会は，とりわけ，社会的条件，政治的条件，技術上の条件または市場の条件の変化に照らし，改正を提案することが適切であるかどうかを判定するという観点から，利害関係者の意見聴取を経た上で，この指令を定期的に見直すべきである。それらの見直しの一部として，欧州委員会は，関係する法主体の規模，この指令の別紙に示す部門，副部門及び法主体のタイプ，サイバーセキュリティと関係する経済及び社会の稼働にとっての適切性を評価すべきである。欧州委員会は，就中，欧州議会及び理事会の規則(EU)2022/2065[24]の第 33 条の意味における非常に大きなオンラインプラットフォームとして指定されており，この指令の適用範囲内にあるプロバイダが，この指令の下にある基礎法主体として識別され得るかどうかを評価すべきである。

The Commission should periodically review this Directive, after consulting stakeholders, in particular with a view to determining whether it is appropriate to propose amendments in light of changes to societal, political, technological or market conditions. As part of those reviews, the Commission should assess the relevance of the size of the entities concerned, and the sectors, subsectors and types of entity referred to in the annexes to this Directive for the functioning of the economy and society in relation to cybersecurity. The Commission should assess, inter alia, whether providers, falling within the scope of this Directive, that are designated as very large online platforms within the meaning of Article 33 of Regulation (EU) 2022/2065 of the European Parliament and of the Council[(24)] could be identified as essential entities under this Directive.

(141) この指令は，ENISA の新たな職務をつくり出し，それによって，ENISA の役割を拡大し，また，規則(EU) 2019/811 に基づく ENISA の既存の職務をこれまでのレベルよりも高いレベルで遂行することを要求されるという結果をもたらし得る。既存の職務及び新たな職務を遂行するために必要となる資金及び人間資源を ENISA がもつことを確保するため，並びに，ENISA の拡大された役割から帰結するそれらの職務のより高いレベルの執行に適合するため，ENISA の予算は，しかるべく増額されるべきである。加えて，資源の効率的な使用を確保するため，ENISA は，その職務を実効的に遂行し，期待に応ずるという目的のために，資源を内部的に割当てることのできる方法において，より大きな柔軟性を与えられるべきである。

This Directive creates new tasks for ENISA, thereby enhancing its role, and could also result in ENISA being required to carry out its existing tasks under Regulation (EU) 2019/881 to a higher level than before.

---

[24] デジタルサービスのための単一市場に関する及び指令 2000/31/EC を改正する欧州議会及び理事会の 2022 年 10 月 19 日の規則(EU) 2022/2065（デジタルサービス法） (OJ L 277, 27.10.2022, p. 1).
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1).

In order to ensure that ENISA has the necessary financial and human resources to carry out existing and new tasks, as well as to meet any higher level of execution of those tasks resulting from its enhanced role, its budget should be increased accordingly. In addition, in order to ensure the efficient use of resources, ENISA should be given greater flexibility in the way that it is able to allocate resources internally for the purpose of effectively carrying out its tasks and meeting expectations.

(142) この指令の目的，すなわち，欧州連合全域にわたる共通の高いレベルのサイバーセキュリティを達成することは，構成国によっては十分に達成され得ず，その活動の効果のゆえに，欧州連合レベルでより良く達成され得るので，欧州連合は，欧州連合条約の第 5 条に定める補完性の原則に従い，措置を採択できる。同条に定める比例性の原則に従い，この指令は，その目的を達成するために必要なところを超えることがない。

Since the objective of this Directive, namely to achieve a high common level of cybersecurity across the Union, cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(143) この指令は，基本的な権利を尊重し，かつ，憲章によって認められた基本原則，とりわけ，私生活の尊重及び通信の権利，個人データの保護，企業活動を営む自由，財産の権利，実効的な救済及び公正な裁判の権利，無罪の推定並びに防御の権利を尊重する。実効的な救済の権利は，基礎法主体及び重要法主体から提供されるサービスの受け手に拡大される。この指令は，それらの権利及び基本原則に従って実装されるべきである。

This Directive respects the fundamental rights, and observes the principles, recognised by the Charter, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence. The right to an effective remedy extends to the recipients of services provided by essential and important entities. This Directive should be implemented in accordance with those rights and principles.

(144) 欧州データ保護監督官は，欧州議会及び理事会の規則(EU) 2018/1725[25]の第 42 条第 1 項に従

[25] 欧州連合の機関，組織，事務局及び部局による個人データの処理と関連する自然人の保護に関する並びにそのデータの支障のない移動に関する，並びに，規則(EC) No 45/2001 及び決定 No 1247/2002/EC を廃止する欧州議会及び理事会の 2018 年 10 月 23 日の規則(EU) 2018/1725 (OJ L 295, 21.11.2018, p. 39).
Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

って意見聴取を受け, 2021 年 3 月 11 日にその意見を伝達した[26],

The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council (25) and delivered an opinion on 11 March 2021 (26),

HAVE ADOPTED THIS DIRECTIVE:

以上のとおりであるので, この指令を採択する:

[26] OJ C 183, 11.5.2021, p. 3.

第I章 総則的な条項
Chapter I General Provisions

第 1 条 対象事項
Article 1 **Subject matter**

1. この指令は，域内市場の稼働を向上させるという観点から，欧州連合全域にわたる共通の高いレベルのサイバーセキュリティを達成するための措置を定める。

   This Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market.

2. 当該目的のため，この指令は，以下のことを定める：
   (a) 国内サイバーセキュリティ戦略を採択すること，並びに，職務権限のある機関，サイバー危機管理機関，サイバーセキュリティに関する単一連絡部局（単一連絡部局）及びコンピュータセキュリティインシデント対応チーム（CSIRT）を指定または設置することを構成国に対して求める義務；
   (b) 別紙Ⅰまたは別紙Ⅱに示すタイプの法主体並びに指令(EU) 2022/2557 の下で必須法主体として識別された法主体のサイバーセキュリティのリスク評価の措置及び報告義務；
   (c) サイバーセキュリティ情報共有の規定及び義務；
   (d) 構成国の監督義務及び執行義務。

   To that end, this Directive lays down:
   (a) obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs);
   (b) cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities under Directive (EU) 2022/2557;
   (c) rules and obligations on cybersecurity information sharing;
   (d) supervisory and enforcement obligations on Member States.

第 2 条 適用範囲
Article 2 **Scope**

1. この指令は，勧告 2003/361/EC の別紙の第 2 条の下にある中規模企業として分類され，または，同条第 1 項に定める中規模企業の上限を超過し，かつ，欧州連合内においてその法主体のサービスを提供し，もしくは，活動を遂行する別紙Ⅰまたは別紙Ⅱに示すタイプの公的法主体及び民間法主体に対して適用される。

This Directive applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which provide their services or carry out their activities within the Union.

この指令の目的のために同勧告の別紙の第 3 条第 4 項を適用してはならない。

Article 3(4) of the Annex to that Recommendation shall not apply for the purposes of this Directive.

2. その法主体の規模に拘わらず，以下の場合においても，この指令は，別紙Ⅰまたは別紙Ⅱに示すタイプの法主体に対して適用される：
   (a) サービスが，以下のプロバイダから提供されている場合：
      (i) 公共電子通信ネットワークのプロバイダまたは公衆が利用可能な電子通信サービスのプロバイダ；
      (ii) 信頼サービスのプロバイダ；
      (iii) トップレベルドメイン名レジストリ及びドメイン名システムサービスのプロバイダ；
   (b) その法主体が，重要な社会活動または経済活動の維持のために必須であるサービスの構成国内において唯一のプロバイダである場合；
   (c) その法主体から提供されるサービスの混乱が，公共の安全，公共の保安または公衆衛生に対して重大な影響をもち得る場合；
   (d) その法主体から提供されるサービスの混乱が，とりわけ，そのような混乱が国境を越える影響を持ち得る部門に対し重大なシステミックリスクを誘発し得る場合；
   (e) 特別の部門もしくはタイプのサービスに対する，または，それ以外の構成国内の相互依存する諸部門に対するその法主体の国内レベルまたは地域レベルの特別の重要性のゆえに，その法主体が重要である場合；
   (f) その法主体が以下の行政機関である法主体である場合：
      (i) 国内法に従ってその構成国によって定義された中央政府の；または
      (ii) リスクベースの評価に従い，そのサービスの混乱が重要な社会活動もしくは経済活動に対して重大な影響をもち得るサービスを提供する，国内法に従ってその構成国によって定義された地域レベルの。

Regardless of their size, this Directive also applies to entities of a type referred to in Annex I or II, where:
   (a) services are provided by:
      (i) providers of public electronic communications networks or of publicly available electronic communications services;
      (ii) trust service providers;
      (iii) top-level domain name registries and domain name system service providers;
   (b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;
   (c) disruption of the service provided by the entity could have a significant impact on public safety,

public security or public health;
(d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;
(e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;
(f) the entity is a public administration entity:
  (i) of central government as defined by a Member State in accordance with national law; or
  (ii) at regional level as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities.

3. その法主体の規模に拘わらず, この指令は, 指令(EU) 2022/2557 の下において必須法主体として識別された法主体に対して適用される。

Regardless of their size, this Directive applies to entities identified as critical entities under Directive (EU) 2022/2557.

4. その法主体の規模に拘わらず, この指令は, ドメイン名登録サービスを提供する法主体に対して適用される。

Regardless of their size, this Directive applies to entities providing domain name registration services.

5. 構成国は, この指令を以下の法主体に対して適用することを定め得る:
(a) 地方レベルで, 行政機関である法主体;
(b) とりわけ, 当該教育機関が重要な調査研究活動を遂行する場合において, 教育機関。

Member States may provide for this Directive to apply to:
(a) public administration entities at local level;
(b) education institutions, in particular where they carry out critical research activities.

6. この指令は, その国の領土の完全性を確保すること及び法と秩序を維持することを含め, 構成国の国家安全保障を守る職責, 及び, それ以外の必須の国家機能を防護するためのその構成国の権限を妨げない。

This Directive is without prejudice to the Member States' responsibility for safeguarding national security and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.

7. この指令は, 国家安全保障, 公共の保安, 国防の分野, または, 犯罪行為の防止, 捜査, 検知及び訴追を含め, 法執行の分野において当該法主体の活動を遂行する行政機関である法主体に

対しては，適用されない。

This Directive does not apply to public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences.

8. 構成国は，国家安全保障，公共の保安，国防の分野，もしくは，犯罪行為の防止，捜査，検知及び訴追を含め，法執行の分野において活動を遂行する特定の法主体，または，専ら，本条の第 7 項に示す行政機関である法主体に対してサービスを提供する特定の法主体に対し，当該法主体の活動またはサービスと関連して第 21 条または第 23 条に定める義務を免除し得る。そのような場合，それらの特定の活動またはサービスとの関係においては，第Ⅶ章に示す監督及び執行の措置を適用してはならない。法主体が，専ら，本項に示すタイプの活動を遂行し，または，サービスを提供するときは，構成国は，当該法主体に対しても，第 3 条及び第 27 条に定める義務を免除することを決定できる。

Member States may exempt specific entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in paragraph 7 of this Article, from the obligations laid down in Article 21 or 23 with regard to those activities or services. In such cases, the supervisory and enforcement measures referred to in Chapter VII shall not apply in relation to those specific activities or services. Where the entities carry out activities or provide services exclusively of the type referred to in this paragraph, Member States may decide also to exempt those entities from the obligations laid down in Articles 3 and 27.

9. 法主体が信頼サービスのプロバイダとして行動するときは，第 7 項及び第 8 項を適用してはならない。

Paragraphs 7 and 8 shall not apply where an entity acts as a trust service provider

10. 規則(EU) 2022/2554 の第 2 条第 4 項に従って構成国が同規則の適用範囲から除外した法主体に対しては，この指令を適用してはならない。

This Directive does not apply to entities which Member States have exempted from the scope of Regulation (EU) 2022/2554 in accordance with Article 2(4) of that Regulation.

11. この指令に定める義務は，その情報の開示が構成国の国家安全保障，公共の保安または国防という必須の利益に反するような情報の供給を伴ってはならない。

The obligations laid down in this Directive shall not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or

defence.

12. この指令は，欧州議会及び理事会の規則(EU) 2016/679，指令 2002/58/EC，指令 2011/93/EU[27] 及び指令 2013/40/EU[28] 並びに指令(EU) 2022/2557 を妨げることなく，適用される。

This Directive applies without prejudice to Regulation (EU) 2016/679, Directive 2002/58/EC, Directives 2011/93/EU (27) and 2013/40/EU (28) of the European Parliament and of the Council and Directive (EU) 2022/2557.

13. TFEU の第 346 条を妨げることなく，企業秘密に関する規定のような，欧州連合の規定または国内規定により秘密である情報は，この指令の適用のために当該交換が必要である場合に限り，この指令に従い，欧州委員会及びそれ以外の関連機関との間で交換される。交換される情報は，当該交換の目的のために適切かつ比例的な情報に限定される。情報の交換は，当該情報の機密性を保持し，かつ，関係する法主体の防護と商業上の利益を保護する。

Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union or national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities in accordance with this Directive only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of entities concerned.

14. 法主体，職務権限のある機関，単一連絡部局及び CSIRT は，この指令の目的のために必要な範囲内で，かつ，規則(EU) 2016/679 に従って個人データを処理し，とりわけ，そのような処理は，同規則の第 6 条に準拠する。

Entities, the competent authorities, the single points of contact and the CSIRTs shall process personal data to the extent necessary for the purposes of this Directive and in accordance with Regulation (EU) 2016/679, in particular such processing shall rely on Article 6 thereof.

この指令による，公共電子通信ネットワークのプロバイダまたは公衆が利用可能な電子通信サー

---

[27] 児童の性的虐待と性的搾取及び児童ポルノとの闘いに関する，並びに，理事会枠組み決定 2004/68/JHA を廃止する欧州議会及び理事会の 2011 年 12 月 13 日の指令 2011/93/EU (OJ L 335, 17.12.2011, p. 1).
Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

[28] 情報システムに対する攻撃に関する，及び，理事会枠組み決定 2005/222/JHA を廃止する欧州議会及び理事会の 2013 年 8 月 12 日の指令 2013/40/EU (OJ L 218, 14.8.2013, p. 8).
Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

ビスのプロバイダによる個人データの処理は，欧州連合のデータ保護法及び欧州連合のプライバシー法，とりわけ，指令 2002/58/EC に従って遂行される。

The processing of personal data pursuant to this Directive by providers of public electronic communications networks or providers of publicly available electronic communications services shall be carried out in accordance with Union data protection law and Union privacy law, in particular Directive 2002/58/EC.

第 3 条　基礎法主体及び重要法主体

Article 3 **Essential and important entities**

1. この指令の目的のために，以下の法主体は，基礎法主体であると判断される：
   (a) 別紙 I に示すタイプの法主体であって，勧告 2003/361/EC の別紙の第 2 条第 1 項に定める中規模企業の上限を超えるもの；
   (b) 当該プロバイダの規模に拘らず，適格信頼サービスのプロバイダ及びトップレベルドメイン名レジストリ並びに DNS サービスのプロバイダ；
   (c) 公共電子通信ネットワークのプロバイダまたは公衆が利用可能な電子通信サービスのプロバイダであって，勧告 2003/361/EC の別紙の第 2 条の下で中規模企業として分類されるもの；
   (d) 第 2 条第 2 項(f)(i)に示す行政機関である法主体；
   (e) 上記以外の別紙 I または別紙 II に示すタイプの法主体であって，第 2 条第 2 項(b)ないし(e)により，基礎法主体として構成国によって識別されたもの；
   (f) この指令の第 2 条第 3 項に示す，指令(EU) 2022/2557 の下で必須法主体として識別された法主体；
   (g) 構成国がそのように定めるときは，指令(EU) 2016/1148 または国内法に従って基礎サービスの運営者として 2023 年 1 月 16 日よりも前に構成国が指定した法主体。

   For the purposes of this Directive, the following entities shall be considered to be essential entities:
   (a) entities of a type referred to in Annex I which exceed the ceilings for medium-sized enterprises provided for in Article 2(1) of the Annex to Recommendation 2003/361/EC;
   (b) qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of their size;
   (c) providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC;
   (d) public administration entities referred to in Article 2(2), point (f)(i);
   (e) any other entities of a type referred to in Annex I or II that are identified by a Member State as essential entities pursuant to Article 2(2), points (b) to (e);
   (f) entities identified as critical entities under Directive (EU) 2022/2557, referred to in Article 2(3) of

this Directive;

(g) if the Member State so provides, entities which that Member State identified before 16 January 2023 as operators of essential services in accordance with Directive (EU) 2016/1148 or national law.

2. この指令の目的のために，別紙 I または別紙 II に示すタイプの法主体であって，本条第 1 項により基礎法主体として分類されないものは，重要法主体であると判断される。これは，第 2 条第 2 項(b)ないし(e)により重要法主体として構成国によって指定された法主体を含む。

For the purposes of this Directive, entities of a type referred to in Annex I or II which do not qualify as essential entities pursuant to paragraph 1 of this Article shall be considered to be important entities. This includes entities identified by Member States as important entities pursuant to Article 2(2), points (b) to (e).

3. 2025 年 4 月 17 日までに，構成国は，基礎法主体及び重要法主体並びにドメイン名登録サービスを提供する法主体のリストを作成する。構成国は，定期的に，かつ，少なくともその後は 2 年毎に，同リストを見直し，かつ，それが適切なときは，アップデートする。

By 17 April 2025, Member States shall establish a list of essential and important entities as well as entities providing domain name registration services. Member States shall review and, where appropriate, update that list on a regular basis and at least every two years thereafter.

4. 第 3 項に示すリストを作成する目的のために，構成国は，同項に示す法主体に対し，少なくとも以下の情報を職務権限のある機関に提出することを要求する：

(a) その法主体の名称;
(b) 住所，及び，電子メールアドレス，IP アドレス範囲及び電話番号を含め，最新の連絡先;
(c) それが適用可能なときは，別紙 I または別紙 II に示す関連する部門及び副部門;並びに
(d) それが適用可能なときは，当該法主体がこの指令の適用範囲内にあるサービスを提供する構成国のリスト。

For the purpose of establishing the list referred to in paragraph 3, Member States shall require the entities referred to in that paragraph to submit at least the following information to the competent authorities:

(a) the name of the entity;
(b) the address and up-to-date contact details, including email addresses, IP ranges and telephone numbers;
(c) where applicable, the relevant sector and subsector referred to in Annex I or II; and
(d) where applicable, a list of the Member States where they provide services falling within the scope of this Directive.

第 3 項に示す法主体は，遅滞なく，かつ，いかなる場合においてもその変更の日から 2 週間以内

に，本項第 1 副項により提出した詳細の変更を通知する。

The entities referred to in paragraph 3 shall notify any changes to the details submitted pursuant to the first subparagraph of this paragraph without delay, and, in any event, within two weeks of the date of the change.

欧州委員会は，サイバーセキュリティに関する欧州連合の部局（ENISA）の補佐により，不適切な遅滞なく，本項に定める義務と関連する指針及び雛型を提供する。

The Commission, with the assistance of the European Union Agency for Cybersecurity (ENISA), shall without undue delay provide guidelines and templates regarding the obligations laid down in this paragraph.

構成国は，法主体が自らを登録するための国内の仕組みを設け得る。

Member States may establish national mechanisms for entities to register themselves.

5. 2025 年 4 月 17 日までに，その後は 2 年毎に，職務権限のある機関は，以下のとおり通知する：
   (a) 欧州委員会及び協力グループに対し，別紙 I または別紙 II に示す各部門及び副部門毎に第 3 項により列挙された基礎法主体及び重要法主体の数を；並びに
   (b) 欧州委員会に対し，第 2 条第 2 項(b)ないし(e)により識別された基礎法主体及び重要法主体の数，当該法主体が属する別紙 I または別紙 II に示す部門及び副部門，当該法主体が提供するサービスのタイプ，並びに，その条項によって当該法主体が識別された第 2 条第 2 項(b)ないし(e)に定める条項の中にある条項からの条項に関する関連情報を。

   By 17 April 2025 and every two years thereafter, the competent authorities shall notify:
   (a) the Commission and the Cooperation Group of the number of essential and important entities listed pursuant to paragraph 3 for each sector and subsector referred to in Annex I or II; and
   (b) the Commission of relevant information about the number of essential and important entities identified pursuant to Article 2(2), points (b) to (e), the sector and subsector referred to in Annex I or II to which they belong, the type of service that they provide, and the provision, from among those laid down in Article 2(2), points (b) to (e), pursuant to which they were identified.

6. 2025 年 4 月 17 日までに，かつ，欧州委員会の要請に応じて，構成国は，欧州委員会に対し，第 5 項(b)に示す基礎法主体及び重要法主体の名称を通知できる。

   Until 17 April 2025 and upon request of the Commission, Member States may notify the Commission of the names of the essential and important entities referred to in paragraph 5, point (b).

第 4 条 部門別の欧州連合法

Article 4 **Sector-specific Union legal acts**

1. 部門別の欧州連合の法行為が，基礎法主体または重要法主体に対し，サイバーセキュリティのリスク管理の措置を採択すること，または，重大なインシデントを通知することを要求しており，かつ，それらの要件がこの指令に定める義務と少なくとも均等な効果をもつときは，第Ⅶ章に定める監督及び執行に関する条項を含め，そのような法主体に対してこの指令の関連条項を適用してはならない。部門別の欧州連合の法行為が，この指令の適用範囲内にある特定の部門内の全ての法主体を包摂していないときは，この指令の関連条項は，それらの部門別の欧州連合の法行為によって包摂されない法主体に対し，適用され続ける。

Where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VII, shall not apply to such entities. Where sector-specific Union legal acts do not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive shall continue to apply to the entities not covered by those sector-specific Union legal acts.

2. 本条の第 1 項に示す要件は，以下の場合においては，この指令に定める義務と効果において均等であると判断される：
   (a) サイバーセキュリティのリスク管理の措置が，第 21 条第 1 項及び第 2 項に定める措置と少なくとも効果において均等である場合；または
   (b) 部門別の欧州連合の法行為が，この指令の下にある CSIRT，職務権限のある機関もしくは単一連絡部局によるインシデント通知への即時のアクセス，それが適切なときは自動化された直接のアクセスを定めており，かつ，重大なインシデントを通知する要件が，この指令の第 23 条第 1 項ないし第 6 項に定める要件と少なくとも効果において均等な場合。

The requirements referred to in paragraph 1 of this Article shall be considered to be equivalent in effect to the obligations laid down in this Directive where:
   (a) cybersecurity risk-management measures are at least equivalent in effect to those laid down in Article 21(1) and (2); or
   (b) the sector-specific Union legal act provides for immediate access, where appropriate automatic and direct, to the incident notifications by the CSIRTs, the competent authorities or the single points of contact under this Directive and where requirements to notify significant incidents are at least equivalent in effect to those laid down in Article 23(1) to (6) of this Directive.

3. 欧州委員会は，2023 年 7 月 17 日までに，第 1 項及び第 2 項の適用を明確化する指針を提供する。欧州委員会は，それらの指針を定期的に見直す。それらの指針を準備する際，欧州委員会は，協力グループ及び ENISA の監視結果を考慮に入れる。

The Commission shall, by 17 July 2023, provide guidelines clarifying the application of paragraphs 1 and 2. The Commission shall review those guidelines on a regular basis. When preparing those guidelines, the Commission shall take into account any observations of the Cooperation Group and ENISA.

第 5 条 ミニマムの整合化

Article 5 **Minimum harmonisation**

この指令は，そのような条項が欧州連合法に定める構成国の義務と一貫性があることを条件として，構成国が，より高いレベルのサイバーセキュリティを確保する条項を採択または維持することを排除してはならない。

This Directive shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law.

第 6 条 定義

Article 6 **Definitions**

この指令の目的のために，以下の定義が適用される：

(1) 「ネットワーク及び情報システム」とは：
   (a) 指令(EU) 2018/1972 の第 2 条第 1 号に定義する電子通信ネットワーク；
   (b) それらの機器中の 1 または複数のものが，プログラムにより，デジタルデータの自動的な処理を遂行する機器または相互接続された機器もしくは関連づけられた機器；または
   (c) それらの要素の運用，利用，保護及び維持管理の目的のために，(a)及び(b)の下に包摂される要素によって記録保存され，処理され，検索されまたは伝送されるデジタルデータ；
   のことを意味し；

(2) 「ネットワーク及び情報システムの防護」とは，記録保存され，伝送されもしくは処理されるデータの可用性，真正性，完全性もしくは機密性，または，当該ネットワーク及び情報システムによって提供されもしくは当該ネットワーク及び情報システムを介してアクセス可能なサービスの可用性，真正性，完全性もしくは機密性を侵害するかもしれない出来事に対し，所定の信頼レベルで抗するネットワーク及び情報システムの能力のことを意味し；

(3) 「サイバーセキュリティ」とは，規則(EU) 2019/881 の第 2 条第 1 号に定義するサイバーセキュリティのことを意味し；

(4) 「国内サイバーセキュリティ戦略」とは，サイバーセキュリティの分野における戦略上の目標及び優先順序並びに当該構成国内においてそれらの目標を達成するための統治を提供する，構成国の一貫性のある枠組みのことを意味し；

(5) 「ニアミス」とは，記録保存され，伝送されもしくは処理されるデータの可用性，真正性，完全性もしくは機密性，または，ネットワーク及び情報システムによって提供されもしくはネットワーク及び情報システムを介してアクセス可能なサービスの可用性，真正性，完全性もしくは機密性を侵害し得た出来事ではあるが，その侵害が現実化の防止に成功した出来事またはその侵害が現実化しなかった出来事のことを意味し；

(6) 「インシデント」とは，記録保存され，伝送されもしくは処理されるデータの可用性，真正性，完全性もしくは機密性，または，ネットワーク及び情報システムによって提供されもしくはネットワーク及び情報システムを介してアクセス可能なサービスの可用性，真正性，完全性もしくは機密性を侵害する出来事のことを意味し；

(7) 「大規模なサイバーセキュリティのインシデント」とは，そのインシデントに対応するための構成国の能力を超過するレベルの混乱を生じさせるインシデント，または，少なくとも 2 つの構成国に対して重大な影響をもつインシデントのことを意味し；

(8) 「インシデントの取扱い」とは，インシデントを防止し，検出し，分析し，並びに，インシデントを封じ込め，または，インシデントに対応し，及び，インシデントから復旧することを狙いとする活動及び手続のことを意味し；

(9) 「リスク」とは，インシデントによって生ずる損失または混乱の可能性のことを意味し，そのような損失または混乱の大きさとそのインシデントの発生の蓋然性の組み合わせとして表現されるべきであり；

(10) 「サイバーな脅威」とは，規則(EU) 2019/881 の第 2 条第 8 号に定義するサイバーな脅威のことを意味し；

(11) 「重大なサイバーな脅威」とは，その脅威の技術上の特性を基礎として，法主体のネットワーク及び情報システムまたは法主体のサービスの利用者に対し，有形または無形の重大な損害を生じさせることによって，重大な影響をもつ可能性があると推定され得るサイバーな脅威のことを意味し；

(12) 「ICT 製品」とは，規則(EU) 2019/881 の第 2 条第 12 号に定義する ICT 製品のことを意味し；

(13) 「ICT サービス」とは，規則(EU) 2019/881 の第 2 条第 13 号に定義する ICT サービスのことを意味し；

(14) 「ICT プロセス」とは，規則(EU) 2019/881 の第 2 条第 14 号に定義する ICT プロセスのことを意味し；

(15) 「脆弱性」とは，ICT 製品または ICT サービスの弱点，被感染性または瑕疵であって，サイバーな脅威によって濫用され得るもののことを意味し；

(16) 「技術標準」とは，欧州議会及び理事会の規則(EU) No 1025/2012[29]の第 2 条第 1 号に定義

[29] 欧州の標準化に関する，理事会決定 89/686/EEC 及び理事会決定 93/15/EEC，欧州議会及び理事会の指令 94/9/EC，指令 94/25/EC，指令 95/16/EC，指令 97/23/EC，指令 98/34/EC，指令 2004/22/EC，指令 2007/23/EC，指令 2009/23/EC 及び指令 2009/105/EC を改正する，並びに，理事会決定 87/95/EEC 及び欧州議会及び理事会の決定 No 1673/2006/EC を廃止する欧州議会及び理事会の 2012 年 10 月 25 日の規則(EU) No 1025/2012 (OJ L 316, 14.11.2012, p. 12).

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European

する技術標準のことを意味し；

(17) 「技術仕様」とは，規則(EU) No 1025/2012 の第 2 条第 4 号に定義する技術仕様のことを意味し；

(18) 「インターネット相互接続点」とは，基本的にはインターネットのトラフィックの交換を容易にする目的のために，複数の独立したネットワークの相互接続をできるようにするネットワーク機能（自律システム）であって，自律システムに対してのみ相互接続を提供し，かつ，いかなる組み合わせの参加自律システム間のインターネットトラフィックの通過対しても第三自律システムを介する通過を要求せず，かつ，そのようなトラフィックの改変またはそれ以外の干渉を要求しないもののことを意味し；

(19) 「ドメイン名システム」または「DNS」とは，階層構造の分散した命名システムであって，インターネットのサービス及び資源の識別をできるようにし，当該サービス及び資源に到達するためのインターネットルーティング及び接続性サービスをエンドユーザの機器が利用できるようにするもののことを意味し；

(20) 「DNS サービスのプロバイダ」とは：

(a) インターネットのエンドユーザのための公衆が利用可能な再帰的ドメイン名解決サービス；または

(b) ルート名サーバを除き，第三者の利用のための権威あるドメイン名解決サービス；

を提供する法主体のことを意味し；

(21) 「トップレベルドメイン名レジストリ」または「TLD 名レジストリ」とは，特定の TLD の委任を受け，かつ，その TLD の下にあるドメイン名の登録を含む TLD の管理運営に責任を負い，かつ，当該業務運営がその法主体自身によって遂行されるか，アウトソースされるかに拘わらず，ただし，TLD 名がそのレジストリ自身の利用に限定してレジストリによって利用される場合を除き，その TLD のネームサーバの運用を含め，その TLD の技術上の業務運営，その TLD のデータベースの維持管理及びネームサーバ全部にわたる TLD ゾーンファイルの配置に責任を負う法主体のことを意味し；

(22) 「ドメイン名登録サービスを提供する法主体」とは，登録者，または，プライバシー／プロキシ登録サービスのプロバイダもしくは再販者のような，登録者の代わりに行動する代理者のことを意味し；

(23) 「デジタルサービス」とは，欧州議会及び理事会の指令(EU) 2015/1535[30]の第 1 条第 1 項(b)に定義するサービスのことを意味し；

(24) 「信頼サービス」とは，規則(EU) No 910/2014 の第 3 条第 16 号に定義する信頼サービスのことを意味し；

(25) 「信頼サービスのプロバイダ」とは，規則(EU) No 910/2014 の第 3 条第 19 号に定義する信

Parliament and of the Council and repealing Council decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

[30] 技術の規則及び情報社会サービスに関する規定の分野における情報提供のための手続を定める欧州議会及び理事会の 2015 年 9 月 9 日の指令(EU) 2015/1535 (OJ L 241, 17.9.2015, p. 1).

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

頼サービスのプロバイダのことを意味し；

(26) 「適格信頼サービス」とは，規則(EU) No 910/2014 の第 3 条第 17 号に定義する適格信頼サービスのことを意味し；

(27) 「適格信頼サービスのプロバイダ」とは，規則(EU) No 910/2014 の第 3 条第 20 号に定義する適格信頼サービスのプロバイダのことを意味し；

(28) 「オンライン市場」とは，欧州議会及び理事会の指令 2005/29/EC[31]の第 2 条(n)に定義するオンライン市場のことを意味し；

(29) 「オンライン検索エンジン」とは，欧州議会及び理事会の規則(EU) 2019/1150[32]の第 2 条第 5 号に定義するオンライン検索エンジンのことを意味し；

(30) 「クラウドコンピューティングサービス」とは，そのような資源が複数の場所にわたって分散している場合を含め，共有可能なコンピュータ処理資源の拡張可能で伸縮可能なプールのオンデマンドの管理及びそのプールへの広域のリモートアクセスを実現可能にするデジタルサービスのことを意味し；

(31) 「データセンターサービス」とは，配電及び環境管理のための全ての設備及びインフラと共にデータの記録保存，処理及び移転のサービスを提供する IT 及びネットワークの機器の集中的な収容，相互接続及び運用に特化した構造物または構造物のグループを包含するサービスのことを意味し；

(32) 「コンテント伝達ネットワーク」とは，コンテントプロバイダ及びサービスプロバイダの代わりに，インターネット利用者に対するデジタルコンテント及びデジタルサービスの高度の可用性，アクセシビリティまたは高速の伝達を確保する目的のために地理的に分散しているサーバのネットワークのことを意味し；

(33) 「ソーシャルネットワーキングサービスプラットフォーム」とは，エンドユーザが，とりわけ，チャット，投稿，ビデオ及び推奨を介して，多角的な機器全体の中で相互に接続し，共有し，発見し，及び，通信するプラットフォームのことを意味し；

(34) 「代理者」とは，欧州連合内に拠点がない DNS サービスのプロバイダ，TLD 名レジストリ，ドメイン名登録サービスを提供する法主体，クラウドコンピューティングサービスのプロバイダ，データセンターサービスのプロバイダ，コンテント伝達ネットワークのプロバイダ，マネージ

---

31 域内市場における事業者と消費者間の不公正な商業上の実務に関する，並びに，理事会指令 84/450/EEC，欧州議会及び理事会の指令 97/7/EC，指令 98/27/EC 及び指令 2002/65/EC，欧州議会及び理事会の規則(EC) No 2006/2004 を改正する欧州議会及び理事会の 2005 年 5 月 11 日の指令 2005/29/EC（「不公正な商業上の実務指令」）(OJ L 149, 11.6.2005, p. 22).

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (OJ L 149, 11.6.2005, p. 22).

32 オンライン中間介在サービスの事業者利用者に関する公正性及び透明性を向上させることに関する欧州議会及び理事会の 2019 年 6 月 20 日の規則(EU) 2019/1150(OJ L 186, 11.7.2019, p. 57).

Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019, p. 57).

ドサービスのプロバイダ，マネージドセキュリティサービスのプロバイダ，または，オンライン市場のプロバイダ，オンライン検索エンジンのプロバイダもしくはソーシャルネットワーキングサービスプラットフォームのプロバイダの代わりに行動するために明示で指定された欧州連合内に拠点をもつ自然人または法人であって，この指令の下にある当該法主体の義務に関し，その法主体自身の代わりに，職務権限のある機関または CSIRT によって名宛人とされ得る者のことを意味し；

(35) 「行政機関である法主体」とは，国内法に従い，構成国においてそのようなものとして承認された法主体であって，法務当局，議会または中央銀行を含まず，以下の基準を満たすもののことを意味し；

(a) その法主体は，一般的な利益における必要性に適合する目的のために設けられており，かつ，産業上の性質または商業上の性質をもたない；

(b) その法主体は，法人格をもち，または，法人格をもつ別の法主体の代わりに行動するための法律上の資格をもつ；

(c) その法主体は，その資金の大部分において，国，地域機関またはそれ以外の公法によって規律される組織から提供されており，当該機関または組織による運営管理上の監督に服しており，または，その構成員の半数以上が国，地域機関またはそれ以外の公法によって規律される組織から指名された者である業務運営，運営管理または監督の委員会をもつ；

(d) その法主体は，自然人または法人に対し，人，物品，サービスまたは資本の国境を越える移動に際し，当該自然人または法人の権利に影響を与える行政上の決定または規制上の決定を発令する権限をもつ；

(36) 「公共電子通信ネットワーク」とは，指令(EU) 2018/1972 の第 2 条第 8 号に定義する公共電子通信ネットワークのことを意味し；

(37) 「電子通信サービス」とは，指令(EU) 2018/1972 の第 2 条第 4 号に定義する電子通信サービスのことを意味し；

(38) 「法主体」とは，自然人，または，その法人の拠点のある地の国内法の下でそのようなものとして創設または承認された法人であって，その名の下で行動し，権利を行使し，かつ，義務に服する者のことを意味し；

(39) 「マネージドサービスプロバイダ」とは，顧客の施設において実施され，または，リモートで実施される補助または能動的な管理運営を介して，ICT 製品，ネットワーク，インフラ，アプリケーションまたはそれ以外のネットワーク及び情報システムの設置，管理，運営または維持と関連するサービスを提供する法主体のことを意味し；

(40) 「マネージドセキュリティサービスプロバイダ」とは，サイバーセキュリティのリスク管理と関連する活動のための補助を遂行し，または，提供するマネージドサービスプロバイダのことを意味し；

(41) 「調査研究組織」とは，商業上の目的のためにその当該調査研究の結果を活用するために，応用的な調査研究または試験的開発を遂行することをその法主体の基本的な目的とする法主体のことを意味するが，教育機関を含まない。

For the purposes of this Directive, the following definitions apply:

(1) ‘network and information system’ means:
   (a) an electronic communications network as defined in Article 2, point (1), of Directive (EU) 2018/1972;
   (b) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or
   (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

(2) ‘security of network and information systems’ means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems;

(3) ‘cybersecurity’ means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881;

(4) ‘national cybersecurity strategy’ means a coherent framework of a Member State providing strategic objectives and priorities in the area of cybersecurity and the governance to achieve them in that Member State;

(5) ‘near miss’ means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise;

(6) ‘incident’ means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;

(7) ‘large-scale cybersecurity incident’ means an incident which causes a level of disruption that exceeds a Member State’s capacity to respond to it or which has a significant impact on at least two Member States;

(8) ‘incident handling’ means any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident;

(9) ‘risk’ means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;

(10) ‘cyber threat’ means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;

(11) ‘significant cyber threat’ means a cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity’s services by causing considerable material or non-material damage;

(12) ‘ICT product’ means an ICT product as defined in Article 2, point (12), of Regulation (EU) 2019/881;

(13) ‘ICT service’ means an ICT service as defined in Article 2, point (13), of Regulation (EU) 2019/881;

(14) ‘ICT process’ means an ICT process as defined in Article 2, point (14), of Regulation (EU) 2019/881;

(15) ‘vulnerability’ means a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat;

(16) ‘standard’ means a standard as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council[29];

(17) ‘technical specification’ means a technical specification as defined in Article 2, point (4), of Regulation (EU) No 1025/2012;

(18) ‘internet exchange point’ means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic;

(19) ‘domain name system’ or ‘DNS’ means a hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources;

(20) ‘DNS service provider’ means an entity that provides:

(a) publicly available recursive domain name resolution services for internet end-users; or

(b) authoritative domain name resolution services for third-party use, with the exception of root name servers;

(21) ‘top-level domain name registry’ or ‘TLD name registry’ means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers, irrespective of whether any of those operations are carried out by the entity itself or are outsourced, but excluding situations where TLD names are used by a registry only for its own use;

(22) ‘entity providing domain name registration services’ means a registrar or an agent acting on behalf of registrars, such as a privacy or proxy registration service provider or reseller;

(23) ‘digital service’ means a service as defined in Article 1(1), point (b), of Directive (EU) 2015/1535 of the European Parliament and of the Council[30];

(24) ‘trust service’ means a trust service as defined in Article 3, point (16), of Regulation (EU) No 910/2014;

(25) ‘trust service provider’ means a trust service provider as defined in Article 3, point (19), of Regulation (EU) No 910/2014;

(26) ‘qualified trust service’ means a qualified trust service as defined in Article 3, point (17), of Regulation (EU) No 910/2014;

(27) ‘qualified trust service provider’ means a qualified trust service provider as defined in Article 3, point (20), of Regulation (EU) No 910/2014;

(28) ‘online marketplace’ means an online marketplace as defined in Article 2, point (n), of Directive

2005/29/EC of the European Parliament and of the Council[31];

(29) ‘online search engine’ means an online search engine as defined in Article 2, point (5), of Regulation (EU) 2019/1150 of the European Parliament and of the Council[32];

(30) ‘cloud computing service’ means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations;

(31) ‘data centre service’ means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of IT and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control;

(32) ‘content delivery network’ means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;

(33) ‘social networking services platform’ means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations;

(34) ‘representative’ means a natural or legal person established in the Union explicitly designated to act on behalf of a DNS service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider, or a provider of an online marketplace, of an online search engine or of a social networking services platform that is not established in the Union, which may be addressed by a competent authority or a CSIRT in the place of the entity itself with regard to the obligations of that entity under this Directive;

(35) ‘public administration entity’ means an entity recognised as such in a Member State in accordance with national law, not including the judiciary, parliaments or central banks, which complies with the following criteria:

  (a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;

  (b) it has legal personality or is entitled by law to act on behalf of another entity with legal personality;

  (c) it is financed, for the most part, by the State, regional authorities or by other bodies governed by public law, is subject to management supervision by those authorities or bodies, or has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities or by other bodies governed by public law;

  (d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital;

(36) ‘public electronic communications network’ means a public electronic communications network as defined in Article 2, point (8), of Directive (EU) 2018/1972;

(37) ‘electronic communications service’ means an electronic communications service as defined in

Article 2, point (4), of Directive (EU) 2018/1972;

(38) ‘entity’ means a natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;

(39) ‘managed service provider’ means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers’ premises or remotely;

(40) ‘managed security service provider’ means a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management;

(41) ‘research organisation’ means an entity which has as its primary goal to conduct applied research or experimental development with a view to exploiting the results of that research for commercial purposes, but which does not include educational institutions.

第II章 調整されたサイバーセキュリティの枠組み
Chapter II Coordinated Cybersecurity Frameworks

第 7 条 国内サイバーセキュリティ戦略
Article 7 National cybersecurity strategy

1. 各構成国は，高いレベルのサイバーセキュリティを達成及び維持するため，戦略上の目標，当該目標を達成するために要する資源，並びに，適切な基本方針及び法令上の措置を定める国内サイバーセキュリティ戦略を採択する。国内サイバーセキュリティ戦略は，以下の事項を含める：
   (a) とりわけ，別紙 I 及び別紙 II に示す部門を包摂する構成国のサイバーセキュリティ戦略の目標及び優先順序；
   (b) 第 2 項に示す基本方針を含め，本項(a)に示す目標及び優先順序を達成するための統治枠組み；
   (c) 国内レベルにおける関連する利害関係者の役割と責任を明確化し，この指令の下にある職務権限のある機関，単一連絡部局及び CSIRT の間の国内レベルの協力と調整，並びに，当該組織と，部門別の欧州連合の法行為の下にある職務権限のある機関との間の協力と調整の基礎となる統治枠組み；
   (d) 当該構成国内における関連資産及びリスク評価を識別するための仕組み；
   (e) 公的部門と民間部門との間の協力を含め，インシデントに対する準備態勢，インシデントへの対応及びインシデントからの復旧を確保する措置の識別名；
   (f) 国内サイバーセキュリティ戦略の実装に関与する様々な機関及び利害関係者のリスト；
   (g) サイバーなリスク，脅威及びインシデント，並びに，非サイバーなリスク，脅威及びインシデントに関する情報交換の目的のための，そして，しかるべく，監督の職務の執行に関する情報交換の目的のための，この指令の下にある職務権限のある機関と指令(EU) 2022/2557 の下にある職務権限のある機関との間の拡大された調整の政策枠組み；
   (h) 必要な措置を含め，市民の間における一般的なレベルのサイバーセキュリティの認識を拡大するための計画。

   Each Member State shall adopt a national cybersecurity strategy that provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include:
   (a) objectives and priorities of the Member State's cybersecurity strategy covering in particular the sectors referred to in Annexes I and II;
   (b) a governance framework to achieve the objectives and priorities referred to in point (a) of this paragraph, including the policies referred to in paragraph 2;
   (c) a governance framework clarifying the roles and responsibilities of relevant stakeholders at national level, underpinning the cooperation and coordination at the national level between the competent authorities, the single points of contact, and the CSIRTs under this Directive, as well as coordination

and cooperation between those bodies and competent authorities under sector-specific Union legal acts;

(d) a mechanism to identify relevant assets and an assessment of the risks in that Member State;

(e) an identification of the measures ensuring preparedness for, responsiveness to and recovery from incidents, including cooperation between the public and private sectors;

(f) a list of the various authorities and stakeholders involved in the implementation of the national cybersecurity strategy;

(g) a policy framework for enhanced coordination between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2557 for the purpose of information sharing on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks, as appropriate;

(h) a plan, including necessary measures, to enhance the general level of cybersecurity awareness among citizens.

2. 国内サイバーセキュリティ戦略の一部として，構成国は，とりわけ，以下の基本方針を採択する：

(a) 法主体のサービスの提供のためにその法主体によって使用される ICT 製品及び ICT サービスのためのサプライチェーン内におけるサイバーセキュリティに対処する基本方針；

(b) サイバーセキュリティ認証，暗号，及び，オープンソースのサイバーセキュリティ製品の利用と関係するものを含め，公共調達における ICT 製品及び ICT サービスに関するサイバーセキュリティ関連要件の包摂及び仕様に関する基本方針；

(c) 第 12 条第 1 項に基づく調整された脆弱性開示の促進と容易化を包含する，脆弱性の管理の基本方針；

(d) それが関連するときは，海底通信ケーブルのサイバーセキュリティを含め，オープンなインターネットの公共基幹部分の一般的な可用性，完全性及び機密性を維持することと関連する基本方針；

(e) 最新のサイバーセキュリティのリスク管理の措置を実装することを狙いとする，関連する高度技術の開発と統合を促進する基本方針；

(f) サイバーセキュリティに関する教育と訓練，サイバーセキュリティの技能，認識向上及び調査研究と開発の取り組み，並びに，市民，利害関係者及び法主体を想定した良いサイバー衛生の実務と管理に関するガイドを促進し，開発する基本方針；

(g) サイバーセキュリティのツール及び安全なネットワークインフラの配置を発展させ，拡大し，かつ，促進するために学術機関及び調査研究機関を支援する基本方針；

(h) 欧州連合法に従った法主体間の任意のサイバーセキュリティの情報共有を支えるための関連手続及び適切な情報共有ツールを包摂する基本方針；

(i) 小企業及び中規模企業の特別の需要のための容易にアクセスできるガイドと補助を提供することによる，サイバー回復力及び小企業及び中規模企業のサイバー衛生のベースライン，とりわけ，この指令の適用範囲外にあるサイバー回復力及び小企業及び中規模企業のサイバー衛生のベースラインを強化する基本方針；

(j) 能動的なサイバー防護を促進する基本方針。

As part of the national cybersecurity strategy, Member States shall in particular adopt policies:

(a) addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services;
(b) on the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including in relation to cybersecurity certification, encryption and the use of open-source cybersecurity products;
(c) managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure under Article 12(1);
(d) related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables;
(e) promoting the development and integration of relevant advanced technologies aiming to implement state-of-the-art cybersecurity risk-management measures;
(f) promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, stakeholders and entities;
(g) supporting academic and research institutions to develop, enhance and promote the deployment of cybersecurity tools and secure network infrastructure;
(h) including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities in accordance with Union law;
(i) strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope of this Directive, by providing easily accessible guidance and assistance for their specific needs
(j) promoting active cyber protection.

3. 構成国は，欧州委員会に対し，その構成国の国内サイバーセキュリティ戦略を，その採択から 3 か月以内に通知する。構成国は，その構成国の国家安全保障と関連する情報をそのような通知から除外できる。

Member States shall notify their national cybersecurity strategies to the Commission within three months of their adoption. Member States may exclude information which relates to their national security from such notifications.

4. 構成国は，定期的に，かつ，少なくとも 5 年毎に，主要達成度評価指標を基礎として，その構成国の国内サイバーセキュリティ戦略を評価し，かつ，それが必要なときは，その構成国の国内サイバーセキュリティ戦略をアップデートする。構成国の国内サイバーセキュリティ戦略をこの指令に定める要件及び義務と揃えるため，ENISA は，構成国の要請に応じて，国内サイバーセキュリティ戦略の策定またはアップデートにおいて，及び，当該戦略の評価のための主要達成度評価指標の策定またはアップデートにおいて，構成国を補助する。

Member States shall assess their national cybersecurity strategies on a regular basis and at least every five

years on the basis of key performance indicators and, where necessary, update them. ENISA shall assist Member States, upon their request, in the development or the update of a national cybersecurity strategy and of key performance indicators for the assessment of that strategy, in order to align it with the requirements and obligations laid down in this Directive.

第 8 条　職務権限のある機関及び単一連絡部局

Article 8 **Competent authorities and single points of contact**

1. 各構成国は，サイバーセキュリティに関して，及び，第Ⅶ章（職務権限のある機関）に示す監督の職務に関して職責を負う 1 または複数の職務権限のある機関を指定または設置する。

   Each Member State shall designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VII (competent authorities).

2. 第 1 項に示す職務権限のある機関は，国内レベルでこの指令の実装を監視する。

   The competent authorities referred to in paragraph 1 shall monitor the implementation of this Directive at national level.

3. 各構成国は，単一連絡部局を指定または設置する。第 1 項により構成国が職務権限のある機関を 1 つだけ指定または設置したときは，当該職務権限のある機関は，当該構成国のための単一連絡部局ともなる。

   Each Member State shall designate or establish a single point of contact. Where a Member State designates or establishes only one competent authority pursuant to paragraph 1, that competent authority shall also be the single point of contact for that Member State.

4. 各単一連絡部局は，別の構成国の関連機関との間で，及び，それが適切なときは，欧州委員会及び ENISA との間で，その単一連絡部局の構成国の機関の国境を越える協力を確保するため，並びに，その単一連絡部局の構成国内の他の職務権限のある機関との間の部門横断の協力を確保するため，連絡官の権限を行使する。

   Each single point of contact shall exercise a liaison function to ensure cross-border cooperation of its Member State's authorities with the relevant authorities of other Member States, and, where appropriate, with the Commission and ENISA, as well as to ensure cross-sectoral cooperation with other competent authorities within its Member State.

5. 構成国は，その構成国の職務権限のある機関及び単一連絡部局が，実効的かつ効率的な態様で，当該機関に対して割当てられた職務を遂行し，それによって，この指令の目的を満たすため

の十分な資源をもつことを確保する。

Member States shall ensure that their competent authorities and single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive.

6. 各構成国は，欧州委員会に対し，不適切な遅滞なく，第 1 項に示す職務権限のある機関の識別名及び第 3 項に示す単一連絡部局の識別名，当該機関の職務，並びに，それらの事項のその後の変更を通知する。各構成国は，その構成国の職務権限のある機関の識別名を公表する。欧州委員会は，単一連絡部局のリストを公表する。

Each Member State shall notify the Commission without undue delay of the identity of the competent authority referred to in paragraph 1 and of the single point of contact referred to in paragraph 3, of the tasks of those authorities, and of any subsequent changes thereto. Each Member State shall make public the identity of its competent authority. The Commission shall make a list of the single points of contact publicly available.

第 9 条 国内サイバー危機管理の枠組み

Article 9 National cyber crisis management frameworks

1. 各構成国は，大規模なサイバーセキュリティのインシデント及び危機の管理に関して職責を負う 1 または複数の職務権限のある機関（サイバー危機管理機関）を指定または設置する。構成国は，当該サイバー危機管理機関が，実効的かつ効率的な態様で，当該機関に対して割当てられた職務を遂行するための十分な資源をもつことを確保する。構成国は，一般的な国内危機管理の既存の枠組みとの一貫性を確保する。

Each Member State shall designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities). Member States shall ensure that those authorities have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them. Member States shall ensure coherence with the existing frameworks for general national crisis management.

2. 第 1 項により構成国が複数のサイバー危機管理機関を指定または設置するときは，その構成国は，それらのどの機関が，大規模なサイバーセキュリティのインシデント及び危機の管理のための調整者としての職務を遂行すべきかを明確に指示する。

Where a Member State designates or establishes more than one cyber crisis management authority pursuant to paragraph 1, it shall clearly indicate which of those authorities is to serve as the coordinator for the management of large-scale cybersecurity incidents and crises.

3. 各構成国は，この指令の目的のために，危機の場合において配置され得る実現能力，資産及び手続を定める。

Each Member State shall identify capabilities, assets and procedures that can be deployed in the case of a crisis for the purposes of this Directive.

4. 各構成国は，大規模なサイバーセキュリティのインシデント及び危機の管理のための目標及び覚書を定める大規模なサイバーセキュリティのインシデント及び危機の国内対応計画を採択する。同計画は，とりわけ，以下の事柄を定める：
   (a) 国内準備態勢の措置及び活動の目標；
   (b) サイバー危機管理機関の職務及び職責；
   (c) 一般的な国内危機管理の枠組みへのサイバー危機管理の統合及び情報交換の経路を含め，サイバー危機管理の手順；
   (d) 演習及び訓練の活動を含め，国内準備態勢措置；
   (e) 関連する公的部門及び民間部門の利害関係者及び包摂されるインフラ；
   (f) 欧州連合レベルの大規模なサイバーセキュリティのインシデント及び危機の調整された管理への構成国の実効的な参加及び支援を確保するための，国内の関連する機関及び組織の間の国内の手順及び覚書。

Each Member State shall adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. That plan shall lay down, in particular:
   (a) the objectives of national preparedness measures and activities;
   (b) the tasks and responsibilities of the cyber crisis management authorities;
   (c) the cyber crisis management procedures, including their integration into the general national crisis management framework and information exchange channels;
   (d) national preparedness measures, including exercises and training activities;
   (e) the relevant public and private stakeholders and infrastructure involved;
   (f) national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.

5. 第 1 項に示すサイバー危機管理機関の指定または設置から 3 か月以内に，各構成国は，欧州委員会に対し，その構成国の機関の識別名及びその後の指定または設置の変更を通知する。構成国は，欧州委員会及び欧州サイバー危機連絡組織ネットワーク（EU-CyCLONe）に対し，大規模なサイバーセキュリティのインシデント及び危機の国内対応計画の採択から 3 か月以内に，同計画に関する第 4 項の要件と関連する関連情報を提出する。構成国は，その構成国の国家安全保障のためにそのような除外が必要な場合においては，それが必要な範囲内で，情報を除外できる。

Within three months of the designation or establishment of the cyber crisis management authority referred to in paragraph 1, each Member State shall notify the Commission of the identity of its authority and of any subsequent changes thereto. Member States shall submit to the Commission and to the European cyber crisis liaison organisation network (EU-CyCLONe) relevant information relating to the requirements of paragraph 4 about their national large-scale cybersecurity incident and crisis response plans within three months of the adoption of those plans. Member States may exclude information where and to the extent that such exclusion is necessary for their national security.

第 10 条 コンピュータセキュリティインシデント対応チーム（CSIRTs）

Article 10 **Computer security incident response teams (CSIRTs)**

1. 各構成国は，1 または複数の CSIRT を指定または設置する。CSIRT は，職務権限のある機関の中で指定または設置できる。CSIRT は，第 11 条第 1 項に定める要件を遵守し，少なくとも，別紙Ⅰ及び別紙Ⅱに示す部門，副部門及びタイプの法主体を包摂し，かつ，明確に定義されたプロセスに従ったインシデントの取扱いに関して職責を負う。

   Each Member State shall designate or establish one or more CSIRTs. The CSIRTs may be designated or established within a competent authority. The CSIRTs shall comply with the requirements set out in Article 11(1), shall cover at least the sectors, subsectors and types of entity referred to in Annexes I and II, and shall be responsible for incident handling in accordance with a well-defined process.

2. 構成国は，各 CSIRT が，第 11 条第 3 項に定める CSIRT の職務を実効的に遂行するための十分な資源をもつことを確保する。

   Member States shall ensure that each CSIRT has adequate resources to carry out effectively its tasks as set out in Article 11(3).

3. 構成国は，各 CSIRT が，そのインフラを介して基礎法主体及び重要法主体並びにそれら以外の関連する利害関係者との間で情報を交換するための適切で，安全かつ回復力のある通信及び情報のインフラを自由に使えることを確保する。その目的のために，構成国は，各 CSIRT が，安全な情報共有ツールの配置のために寄与することを確保する。

   Member States shall ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure through which to exchange information with essential and important entities and other relevant stakeholders. To that end, Member States shall ensure that each CSIRT contributes to the deployment of secure information-sharing tools.

4. CSIRT は，協力し，かつ，それが適切なときは，基礎法主体及び重要法主体の部門別または部門横断のコミュニティとの間で，第 29 条に従って関連情報を交換する。

The CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 29 with sectoral or cross-sectoral communities of essential and important entities.

5. CSIRT は，第 19 条に従って組織構成される相互評価に参加する。

The CSIRTs shall participate in peer reviews organised in accordance with Article 19.

6. 構成国は，CSIRT ネットワークの中におけるその構成国の CSIRT の実効的，効率的かつ安全な協力を確保する。

Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network.

7. CSIRT は，第三国のコンピュータセキュリティインシデント対応チームとの間で，協力関係を構築できる。そのような協力関係の一部として，構成国は，当該第三国のコンピュータセキュリティインシデント対応チームとの間における，トラフィックライトプロトコルを含め，関連する情報共有プロトコルを使用する実効的，効率的かつ安全な情報交換を促進する。CSIRT は，欧州連合のデータ保護法に従った個人データを含め，第三国のコンピュータセキュリティインシデント対応チームとの間で関連情報を交換できる。

The CSIRTs may establish cooperation relationships with third countries' national computer security incident response teams. As part of such cooperation relationships, Member States shall facilitate effective, efficient and secure information exchange with those third countries' national computer security incident response teams, using relevant information-sharing protocols, including the traffic light protocol. The CSIRTs may exchange relevant information with third countries' national computer security incident response teams, including personal data in accordance with Union data protection law.

8. CSIRT は，とりわけ，第三国のコンピュータセキュリティインシデント対応チームまたは均等な第三国の組織に対してサイバーセキュリティの補助を提供する目的のために，当該コンピュータセキュリティインシデント対応チームまたは組織と協力できる。

The CSIRTs may cooperate with third countries' national computer security incident response teams or equivalent third-country bodies, in particular for the purpose of providing them with cybersecurity assistance.

9. 各構成国は，欧州委員会に対し，不適切な遅滞なく，本条の第 1 項に示す CSIRT 及び第 12 条第 1 項により調整者として指定された CSIRT の識別名，基礎法主体及び重要法主体との関係におけるそれらの構成国のそれぞれの CSIRT の関連する職務，並びに，それらに対するその後の変更を通知する。

Each Member State shall notify the Commission without undue delay of the identity of the CSIRT referred to in paragraph 1 of this Article and the CSIRT designated as coordinator pursuant to Article 12(1), of their respective tasks in relation to essential and important entities, and of any subsequent changes thereto.

10. 構成国は, その構成国の CSIRT の発展において, ENISA の補助を要請できる。
Member States may request the assistance of ENISA in developing their CSIRTs.

第 11 条 CSIRT の要件, 技術上の実現能力及び職務

Article 11 **Requirements, technical capabilities and tasks of CSIRTs**

1. CSIRT は, 以下の要件を遵守する:
   (a) CSIRT は, 単一障害点を避けることによってその CSIRT の通信経路の高いレベルの可用性を確保し, かつ, 常時, 他者から連絡を受けるため及び他者と連絡するための複数の手段をもち;CSIRT は, 通信経路を明確に特定し, かつ, 対象コミュニティ及び協力関係者に対してその通信経路を知らせ;
   (b) CSIRT の施設及び活動を支える情報システムは, 安全な場所に所在するものとし;
   (c) とりわけ, 実効的かつ効率的な引継ぎを容易にするため, 管理運営及びルーティングの要求のための適切なシステムを具備し;
   (d) CSIRT は, その CSIRT の業務の機密性及び信頼性を確保し;
   (e) CSIRT は, その CSIRT のサービスの可用性を常時確保するための適切な職員をもち, かつ, CSIRT は, その CSIRT の職員が適切に訓練を受けることを確保し;
   (f) CSIRT は, その CSIRT のサービスの継続性を確保するための冗長システム及びバックアップ作業スペースを具備する。

   The CSIRTs shall comply with the following requirements:
   (a) the CSIRTs shall ensure a high level of availability of their communication channels by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times; they shall clearly specify the communication channels and make them known to constituency and cooperative partners;
   (b) the CSIRTs' premises and the supporting information systems shall be located at secure sites;
   (c) the CSIRTs shall be equipped with an appropriate system for managing and routing requests, in particular to facilitate effective and efficient handovers;
   (d) the CSIRTs shall ensure the confidentiality and trustworthiness of their operations;
   (e) the CSIRTs shall be adequately staffed to ensure availability of their services at all times and they shall ensure that their staff is trained appropriately;
   (f) the CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of their services.

CSIRT は，国際的な協力ネットワークに参加できる。

The CSIRTs may participate in international cooperation networks.

2. 構成国は，その構成国の CSIRT が，第 3 項に示す職務を遂行するために必要な技術上の実現能力を共同でもつことを確保する。構成国は，その構成国の CSIRT に対し，その CSIRT の技術上の実現能力を開発できるようにする目的のためにその CSIRT が適切なレベルで職員をもつことを確保するため，十分な資源が割当てられることを確保する。

Member States shall ensure that their CSIRTs jointly have the technical capabilities necessary to carry out the tasks referred to in paragraph 3. Member States shall ensure that sufficient resources are allocated to their CSIRTs to ensure adequate staffing levels for the purpose of enabling the CSIRTs to develop their technical capabilities.

3. CSIRT は，以下の職務をもつ：
   (a) サイバーな脅威，脆弱性及びインシデントを国内レベルで監視及び分析すること，並びに，要請に応じて，関係する基礎法主体及び重要法主体に対し，当該法主体のネットワーク及び情報システムのリアルタイムの監視またはリアルタイムに近い監視と関連する補助を提供すること；
   (b) 関係する基礎法主体及び重要法主体に対し，並びに，職務権限のある機関及びそれら以外の関連する利害関係者に対し，可能であれば，リアルタイムに近い状態で，サイバーな脅威，脆弱性及びインシデントに関する早期警戒，警報，告知及び情報の伝達を提供すること；
   (c) インシデントに対応すること，並びに，それが適用可能なときは，関係する基礎法主体及び重要法主体に対し，補助を提供すること；
   (d) 法科学のデータを収集し，分析すること，並びに，動的なリスク及びインシデントの分析並びにサイバーセキュリティと関連する状況認識を提供すること；
   (e) 基礎法主体または重要法主体の要請に応じて，潜在的な重大な影響をもつ脆弱性を検出するため，関係する法主体のネットワーク及び情報システムのプロアクティブスキャニングを提供すること；
   (f) CSIRT ネットワークに参加すること，及び，その CSIRT の実現能力及び職務権限に従って，CSIRT ネットワークの他の構成 CSIRT に対し，その構成 CSIRT の要請に応じて，相互補助を提供すること；
   (g) それが適用可能なときは，第 12 条第 1 項に基づく調整された脆弱性開示の目的のための調整者として行動すること；
   (h) 第 10 条第 3 項による安全な情報共有ツールの配置に寄与すること。

The CSIRTs shall have the following tasks:
   (a) monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or

near real-time monitoring of their network and information systems;

(b) providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time;

(c) responding to incidents and providing assistance to the essential and important entities concerned, where applicable;

(d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;

(e) providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;

(f) participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request;

(g) where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure under Article 12(1);

(h) contributing to the deployment of secure information-sharing tools pursuant to Article 10(3).

CSIRT は，基礎法主体及び重要法主体の公衆がアクセス可能なネットワーク及び情報システムの非侵害的なプロアクティブスキャニングを実施できる。そのようなスキャニングは，脆弱性のある，または，安全ではないように設定されたネットワーク及び情報システムを検出し，関係する法主体に対して連絡するために実施される。そのようなスキャニングは，その法主体のサービスの稼働に対して負の影響を与えてはならない。

The CSIRTs may carry out proactive non-intrusive scanning of publicly accessible network and information systems of essential and important entities. Such scanning shall be carried out to detect vulnerable or insecurely configured network and information systems and inform the entities concerned. Such scanning shall not have any negative impact on the functioning of the entities' services.

第 1 副項に示す職務を遂行する際，CSIRT は，リスクベースのアプローチを基礎として，特定の職務の優先順序を決め得る。

When carrying out the tasks referred to in the first subparagraph, the CSIRTs may prioritise particular tasks on the basis of a risk-based approach.

4. CSIRT は，この指令の目的を達成するという観点から，関連する民間部門の利害関係者との間で協力関係を構築する。

The CSIRTs shall establish cooperation relationships with relevant stakeholders in the private sector, with a view to achieving the objectives of this Directive.

5. 第 4 項に示す協力を容易にするため，CSIRT は，以下の事項と関係する共通のまたは標準化された実務，分類手法及び分類学の採用及び利用を促進する：
   (a) インシデントの取扱いの手順；
   (b) 危機管理；及び
   (c) 第 12 条第 1 項に基づく調整された脆弱性開示。

   In order to facilitate cooperation referred to in paragraph 4, the CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to:
   (a) incident-handling procedures;
   (b) crisis management; and
   (c) coordinated vulnerability disclosure under Article 12(1).

第 12 条 調整された脆弱性開示及び欧州脆弱性データベース

Article 12 **Coordinated vulnerability disclosure and a European vulnerability database**

1. 各構成国は，その構成国の CSIRT 中の 1 つを，調整された脆弱性開示の目的のための調整者として指定する。調整者として指定された CSIRT は，それが必要なときは，脆弱性を報告する自然人または法人と潜在的に脆弱性のある ICT 製品または ICT サービスの製造者または提供者のいずれかの要請に応じて，それらの者の間のやりとりを容易にする，信頼できる媒介者として行動する。調整者として指定された CSIRT の職務は，以下の職務を含む：
   (a) 関係する法主体を特定すること及びその法主体と連絡をとること；
   (b) 脆弱性を報告する自然人または法人を補助すること；並びに
   (c) 複数の法主体に影響を与える脆弱性の開示日程を交渉すること及びその脆弱性を管理すること。

   Each Member State shall designate one of its CSIRTs as a coordinator for the purposes of coordinated vulnerability disclosure. The CSIRT designated as coordinator shall act as a trusted intermediary, facilitating, where necessary, the interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party. The tasks of the CSIRT designated as coordinator shall include:
   (a) identifying and contacting the entities concerned;
   (b) assisting the natural or legal persons reporting a vulnerability; and
   (c) negotiating disclosure timelines and managing vulnerabilities that affect multiple entities.

   構成国は，当該の者がそのように求めるときは，自然人または法人が，匿名で，調整者として指定された CSIRT に対し脆弱性を報告できることを確保する。調整者として指定された CSIRT は，報告された脆弱性と関連して勤勉な事後活動が遂行されることを確保し，かつ，脆弱性を報告する自然人または法人の匿名性を確保する。報告された脆弱性が，複数の構成国の法主体に対して重大な影響をもち得るときは，関係する各構成国の調整者として指定された CSIRT は，それが適

切なときは，CSIRT ネットワーク内において，他の調整者として指定された CSIRT と協力する。

Member States shall ensure that natural or legal persons are able to report, anonymously where they so request, a vulnerability to the CSIRT designated as coordinator. The CSIRT designated as coordinator shall ensure that diligent follow-up action is carried out with regard to the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability. Where a reported vulnerability could have a significant impact on entities in more than one Member State, the CSIRT designated as coordinator of each Member State concerned shall, where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRTs network.

2. ENISA は，協力グループの意見聴取を経た上で，欧州脆弱性データベースを開発及び維持管理する。その目的のために，ENISA は，適切な情報システム，基本方針及び手順を開発及び維持管理し，かつ，とりわけ，その法主体がこの指令の適用範囲内にあるかどうかに拘わらず，法主体，その法主体へのネットワーク及び情報システムの供給者が，任意ベースで，ICT 製品または ICT サービスの周知の脆弱性を開示及び登録できるようにするため，欧州脆弱性データベースの防護及び完全性を確保するために必要となる技術上の措置及び運用上の措置を採択する。全ての利害関係者は，欧州脆弱性データベースに収録されている脆弱性に関する情報へのアクセスの提供を受ける。同データベースは，以下の情報を含める：
   (a) 脆弱性を記述する情報；
   (b) 影響を受ける ICT 製品または ICT サービス及びその脆弱性が悪用され得る状況を前提とするその脆弱性の深刻度；
   (c) 関連するパッチの可用性，及び，利用可能なパッチが存在しないときは，脆弱性のある ICT 製品及び ICT サービスの利用者向けの，開示された脆弱性から帰結するリスクがどのようにして緩和され得るかに関する，職務権限のある機関または CSIRT から提供されるガイド。

ENISA shall develop and maintain, after consulting the Cooperation Group, a European vulnerability database. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures, and shall adopt the necessary technical and organisational measures to ensure the security and integrity of the European vulnerability database, with a view in particular to enabling entities, regardless of whether they fall within the scope of this Directive, and their suppliers of network and information systems, to disclose and register, on a voluntary basis, publicly known vulnerabilities in ICT products or ICT services. All stakeholders shall be provided access to the information about the vulnerabilities contained in the European vulnerability database. That database shall include:
   (a) information describing the vulnerability;
   (b) the affected ICT products or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited;
   (c) the availability of related patches and, in the absence of available patches, guidance provided by the competent authorities or the CSIRTs addressed to users of vulnerable ICT products and ICT services as to how the risks resulting from disclosed vulnerabilities can be mitigated.

第 13 条 国内レベルにおける協力

Article 13 **Cooperation at national level**

1. 当該機関が分離されている場合，同一の構成国の職務権限のある機関，単一連絡部局及び CSIRT は，この指令に定める義務を満たすことに関し，相互に協力する。

   Where they are separate, the competent authorities, the single point of contact and the CSIRTs of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive.

2. 構成国は，その構成国の CSIRT，または，それが適用可能なときは，その構成国の職務権限のある機関が，第 23 条による重大なインシデントの通知，並びに，第 30 条によるインシデント，サイバーな脅威及びニアミスの通知を受けることを確保する。

   Member States shall ensure that their CSIRTs or, where applicable, their competent authorities, receive notifications of significant incidents pursuant to Article 23, and incidents, cyber threats and near misses pursuant to Article 30.

3. 構成国は，その構成国の CSIRT，または，それが適用可能なときは，その構成国の職務権限のある機関が，その構成国の単一連絡部局に対し，この指令により提出されたインシデント，サイバーな脅威及びニアミスの通知を連絡することを確保する。

   Member States shall ensure that their CSIRTs or, where applicable, their competent authorities inform their single points of contact of notifications of incidents, cyber threats and near misses submitted pursuant to this Directive.

4. 職務権限のある機関，単一連絡部局及び CSIRT の職務及び義務が実効的に遂行されることを確保するため，構成国は，可能な範囲内で，当該組織と，法執行機関，データ保護機関，規則(EC) No 300/2008 及び規則(EU) 2018/1139 の下にある国内機関，規則(EU) No 910/2014 の下にある監督組織，規則(EU) 2022/2554 の下にある職務権限のある機関，指令(EU) 2018/1972 の下にある国内規制当局，指令(EU) 2022/2557 の下にある職務権限のある機関並びにそれら以外の部門別の欧州連合の法行為の下にある職務権限のある機関との間の，当該構成国内における適切な協力を確保する。

   In order to ensure that the tasks and obligations of the competent authorities, the single points of contact and the CSIRTs are carried out effectively, Member States shall, to the extent possible, ensure appropriate cooperation between those bodies and law enforcement authorities, data protection authorities, the national authorities under Regulations (EC) No 300/2008 and (EU) 2018/1139, the supervisory bodies under Regulation (EU) No 910/2014, the competent authorities under Regulation (EU) 2022/2554, the national regulatory authorities under Directive (EU) 2018/1972, the competent authorities under Directive (EU) 2022/2557, as well as the competent authorities under other sector-specific Union legal

acts, within that Member State.

5. 構成国は，この指令の下にあるその構成国の職務権限のある機関と，指令(EU) 2022/2557 の下にあるその構成国の職務権限のある機関が，必須法主体の識別に関し，サイバーなリスク，脅威及びインシデントに関し，並びに，指令(EU) 2022/2557 の下において必須法主体として識別された法主体に影響を与える非サイバーなリスク，脅威及びインシデント，並びに，そのような非サイバーなリスク，脅威及びインシデントに対する対応において講じられた措置に関し，協力し，かつ，定期的に情報を交換することを確保する。構成国は，この指令の下にあるその構成国の職務権限のある機関と，規則(EU) No 910/2014，規則(EU) 2022/2554 及び指令(EU) 2018/1972 の下にあるその構成国の職務権限のある機関が，関連するインシデント及びサイバーな脅威と関係する情報を含め，関連する情報を定期的に交換することも確保すべきである。

Member States shall ensure that their competent authorities under this Directive and their competent authorities under Directive (EU) 2022/2557 cooperate and exchange information on a regular basis with regard to the identification of critical entities, on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents affecting entities identified as critical entities under Directive (EU) 2022/2557, and the measures taken in response to such risks, threats and incidents. Member States shall also ensure that their competent authorities under this Directive and their competent authorities under Regulation (EU) No 910/2014, Regulation (EU) 2022/2554 and Directive (EU) 2018/1972 exchange relevant information on a regular basis, including with regard to relevant incidents and cyber threats.

6. 構成国は，第 23 条及び第 30 条に示す通知のための技術手段を介して，報告を簡素化する。

Member States shall simplify the reporting through technical means for notifications referred to in Articles 23 and 30.

第Ⅲ章 欧州連合レベル及び国際レベルの協力
Chapter III Cooperation at Union and International Level

第 14 条 協力グループ
Article 14 Cooperation Group

1. 戦略的な協力と構成国間の情報交換を支援及び促進し，かつ，信頼と信用を強化するため，協力グループが設置される。

   In order to support and facilitate strategic cooperation and the exchange of information among Member States, as well as to strengthen trust and confidence, a Cooperation Group is established.

2. 協力グループは，第 7 条に示す隔年作業計画に基づき，その職務を遂行する。

   The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 7.

3. 協力グループは，構成国の代表，欧州委員会及び ENISA によって構成される。欧州対外行動局は，オブザーバーとして，協力グループの活動に参加する。欧州監督当局（ESAs）及び規則(EU) 2022/2554 の下にある職務権限のある機関は，同規則の第 47 条第 1 項に従い，協力グループの活動に参加できる。

   The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) and the competent authorities under Regulation (EU) 2022/2554 may participate in the activities of the Cooperation Group in accordance with Article 47(1) of that Regulation.

   それが適切なときは，協力グループは，欧州議会及び関連する利害関係者の代表に対し，協力グループの作業に参加することを招請できる。

   Where appropriate, the Cooperation Group may invite the European Parliament and representatives of relevant stakeholders to participate in its work.

   欧州委員会は，事務局を提供する。

   The Commission shall provide the secretariat.

4. 協力グループは，以下の職務をもつ：

(a) この指令の国内法化及び実装と関係する職務権限のある機関に対し，ガイドを提供する職務；
(b) 第 7 条第 2 項(c)に示す調整された脆弱性開示の基本方針の策定及び実装と関係する職務権限 のある機関に対してガイドを提供する職務；
(c) サイバーな脅威，インシデント，脆弱性，ニアミス，認識向上の取り組み，訓練，演習及び技能，実現能力の構築，技術標準及び技術仕様，並びに，第 2 条第 2 項(b)ないし(e)による基礎法主体及び重要法主体の識別を含め，この指令の実装と関係するベストプラクティス及び情報を交換する職務；
(d) 生成中のサイバーセキュリティ基本方針の取り組みに関し及び部門別のサイバーセキュリティの要件の全体的な一貫性に関し，欧州委員会との間で助言を交換し，欧州委員会と協力する職務；
(e) この指令により採択される委任される行為案または実装行為案に関し，欧州委員会との間で助言を交換し，欧州委員会と協力する職務；
(f) 関連する欧州連合の機関，組織，事務局及び部局との間でベストプラクティス及び情報を交換する職務；
(g) サイバーセキュリティに関する条項を含んでいる部門別の欧州連合の法行為の実装に関し，見解を交換する職務；
(h) それが関連するときは，第 19 条第 9 項に示す相互評価に関する報告の討議をし，また，結論及び推奨事項を記載する職務；
(i) 第 22 条第 1 項に従い，重要なサプライチェーンの調整されたセキュリティリスク評価を遂行する職務；
(j) 第 37 条に示す国境を越える共同監督活動の経験及び結果を含め，相互補助の案件を討議する職務；
(k) 1 または複数の関係する構成国の要請に応じて，第 37 条に示す相互補助を求める個別の要請を討議する職務；
(l) 生じつつある具体的な問題に関し，CSIRT ネットワーク及び EU-CyCLONe に対し，戦略上のガイドを提供する職務；
(m) CSIRT ネットワーク及び EU-CyCLONe の学び取った教訓を基礎として，大規模なサイバーセキュリティのインシデント及び危機の後の事後活動に関する基本方針に関し，見解を交換する職務；
(n) 職務権限のある機関または CSIRT からの職員が参加する能力構築計画を通じて，国内官吏の交換を促進することにより，欧州連合全域のサイバーセキュリティの実現能力に貢献する職務；
(o) 協力グループによって遂行される活動を討議し，生じつつある基本方針の検討課題に関する入力を収集するため，欧州連合全域にわたる関連する民間の利害関係者との間の定例の共同会合を計画する職務；
(p) ENISA によって行われた作業を含め，サイバーセキュリティの演習と関係して実施された作業を討議する職務；
(q) 第 19 条第 1 項に示す相互評価の手法の側面及び組織構成の側面を定める職務，並びに，欧州委員会及び ENISA の補助を得て，かつ，欧州委員会及び ENISA と協力して，第 19

条第 5 項に従って構成国のための自己評価の手法を定める職務，第 19 条第 6 項に従って指定されたサイバーセキュリティの専門家の作業手法を支える行動準則を策定する職務；

(r) 戦略レベルで，相互評価から得られた経験に関し，第 40 条に示す見直しの目的のための報告書を準備する職務；

(s) ランサムウェアのような，サイバーな脅威またはインシデントの現況の評価を定期的に討議し，遂行する職務。

The Cooperation Group shall have the following tasks:

(a) to provide guidance to the competent authorities in relation to the transposition and implementation of this Directive;

(b) to provide guidance to the competent authorities in relation to the development and implementation of policies on coordinated vulnerability disclosure, as referred to in Article 7(2), point (c);

(c) to exchange best practices and information in relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, training, exercises and skills, capacity building, standards and technical specifications as well as the identification of essential and important entities pursuant to Article 2(2), points (b) to (e);

(d) to exchange advice and cooperate with the Commission on emerging cybersecurity policy initiatives and the overall consistency of sector-specific cybersecurity requirements;

(e) to exchange advice and cooperate with the Commission on draft delegated or implementing acts adopted pursuant to this Directive;

(f) to exchange best practices and information with relevant Union institutions, bodies, offices and agencies;

(g) to exchange views on the implementation of sector-specific Union legal acts that contain provisions on cybersecurity;

(h) where relevant, to discuss reports on the peer review referred to in Article 19(9) and draw up conclusions and recommendations;

(i) to carry out coordinated security risk assessments of critical supply chains in accordance with Article 22(1);

(j) to discuss cases of mutual assistance, including experiences and results from cross-border joint supervisory actions as referred to in Article 37;

(k) upon the request of one or more Member States concerned, to discuss specific requests for mutual assistance as referred to in Article 37;

(l) to provide strategic guidance to the CSIRTs network and EU-CyCLONe on specific emerging issues;

(m) to exchange views on the policy on follow-up actions following large-scale cybersecurity incidents and crises on the basis of lessons learned of the CSIRTs network and EU-CyCLONe;

(n) to contribute to cybersecurity capabilities across the Union by facilitating the exchange of national officials through a capacity building programme involving staff from the competent authorities or the CSIRTs;

(o) to organise regular joint meetings with relevant private stakeholders from across the Union to

discuss activities carried out by the Cooperation Group and gather input on emerging policy challenges;

(p) to discuss the work undertaken in relation to cybersecurity exercises, including the work done by ENISA;

(q) to establish the methodology and organisational aspects of the peer reviews referred to in Article 19(1), as well as to lay down the self-assessment methodology for Member States in accordance with Article 19(5), with the assistance of the Commission and ENISA, and, in cooperation with the Commission and ENISA, to develop codes of conduct underpinning the working methods of designated cybersecurity experts in accordance with Article 19(6);

(r) to prepare reports for the purpose of the review referred to in Article 40 on the experience gained at a strategic level and from peer reviews;

(s) to discuss and carry out on a regular basis an assessment of the state of play of cyber threats or incidents, such as ransomware.

協力グループは, 欧州委員会, 欧州議会及び理事会に対し, 第 1 副項(r)に示す報告書を提出する。

The Cooperation Group shall submit the reports referred to in the first subparagraph, point (r), to the Commission, to the European Parliament and to the Council.

5. 構成国は, 協力グループ内におけるその構成国の代表の実効的で, 効率的かつ安全な協力を確保する。

Member States shall ensure effective, efficient and secure cooperation of their representatives in the Cooperation Group.

6. 協力グループは, CSIRT ネットワークに対し, 特定の話題に関する技術上の報告を要請できる。

The Cooperation Group may request from the CSIRTs network a technical report on selected topics.

7. 2024 年 2 月 1 日までに, 及び, その後は 2 年毎に, 協力グループは, 協力グループの目的及び職務を実装するために実施されるべき活動に関する作業計画を策定する。

By 1 February 2024 and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks.

8. 欧州委員会は, 協力グループの稼働のために必要となる手続覚書を定める実装行為を採択できる。

The Commission may adopt implementing acts laying down procedural arrangements necessary for the

functioning of the Cooperation Group.

同実装行為は，第 39 条第 2 項に示す審議手続に従って採択される。

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

欧州委員会は，第 4 項(e)に従った本項の第 1 副項に示す実装行為案に関し，協力グループとの間で助言を交換し，協力グループと協力する。

The Commission shall exchange advice and cooperate with the Cooperation Group on the draft implementing acts referred to in the first subparagraph of this paragraph in accordance with paragraph (4), point (e).

9. 協力グループは，戦略的な協力と情報交換を促進し，容易にするために指令(EU) 2022/2557 に基づいて設置された必須法主体回復力グループとの間で，定期的に，かつ，いかなる場合においても少なくとも年 1 回，会合する。

The Cooperation Group shall meet on a regular basis and in any event at least once a year with the Critical Entities Resilience Group established under Directive (EU) 2022/2557 to promote and facilitate strategic cooperation and the exchange of information.

第 15 条 CSIRT ネットワーク

Article 15 **CSIRTs network**

1. 信用と信頼の発展に寄与するため，及び，構成国間の迅速かつ実効的な業務運営上の協力を促進するため，国内 CSIRT のネットワークが設置される。

In order to contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States, a network of national CSIRTs is established.

2. CSIRT ネットワークは，第 10 条により指定または設置された CSIRT の代表，並びに，欧州連合の機関，組織及び部局のためのコンピュータ緊急対応チーム（CERT-EU）によって構成される。欧州委員会は，オブザーバーとして CSIRT ネットワークに参加する。ENISA は，事務局を提供し，かつ，CSIRT 間の協力のための補助を能動的に提供する。

The CSIRTs network shall be composed of representatives of the CSIRTs designated or established pursuant to Article 10 and the computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU). The Commission shall participate in the CSIRTs network as an observer. ENISA

shall provide the secretariat and shall actively provide assistance for the cooperation among the CSIRTs.

3. CSIRT ネットワークは，以下の職務をもつ：
   (a) CSIRT の実現能力に関する情報を交換する職務；
   (b) CSIRT の間において，技術及び関連措置，基本方針，ツール，手順，ベストプラクティス及び枠組みの共有，移転及び交換を容易にする職務；
   (c) インシデント，ニアミス，サイバーな脅威，リスク及び脆弱性に関する関連情報を交換する職務；
   (d) サイバーセキュリティの刊行物及び推奨事項と関連する情報を交換する職務；
   (e) 情報共有の仕様及びプロトコルと関連する相互運用性を確保する職務；
   (f) インシデントによる影響を潜在的に受けている CSIRT ネットワークのメンバーの要請に応じて，当該インシデント並びに関連するサイバーな脅威，リスク及び脆弱性と関係する情報を交換し，討議する職務；
   (g) CSIRT ネットワークのメンバーの要請に応じて，当該構成国の管轄権の範囲内で発見されたインシデントに対する調整された対応を討議し，それが可能なときは，実装する職務；
   (h) 構成国に対し，この指令による国境を越えるインシデントに対応する補助を提供する職務；
   (i) 複数の構成国の法主体に対して重大な影響をもち得る脆弱性の調整された開示の管理運営に関し，協力し，ベストプラクティスを交換し，及び，第 12 条第 1 項により調整者として指定された CSIRT に対して補助を提供する職務；
   (j) 以下と関係するものを含め，別の形態の業務運営上の協力を討議し，識別する職務；
      (i) サイバーな脅威及びインシデントの類型；
      (ii) 早期警戒；
      (iii) 相互補助；
      (iv) 国境を越えるリスク及びインシデントへの対応における調整に関する基本原則及び覚書；
      (v) 構成国の要請に応じて，第 9 条第 4 項に示す大規模なサイバーセキュリティのインシデント及び危機の国内対応計画への寄与；
   (k) 協力グループに対し，CSIRT ネットワークの活動及び(j)により討議された別の形態の業務運営上の協力を連絡し，並びに，それが必要なときは，その点に関するガイドを要請する職務；
   (l) ENISA によって計画されたサイバーセキュリティ演習を含め，サイバーセキュリティ演習を精査する職務；
   (m) 個々の CSIRT の要請に応じて，当該 CSIRT の実現能力及び準備態勢を討議する職務；
   (n) 欧州連合全域のインシデント及びサイバーな脅威に関する共通の状況認識を向上させるための，地域レベル及び欧州連合レベルのセキュリティ運用拠点（SOC）と協力し，SOC との間で情報を交換する職務；
   (o) それが関連するときは，第 19 条第 9 項に示す相互評価報告を討議する職務；
   (p) 業務運営上の協力に関する本条の条項の適用に関する業務運営上の実務の包摂を促進するための指針を提供する職務。

The CSIRTs network shall have the following tasks:

(a) to exchange information about the CSIRTs' capabilities;

(b) to facilitate the sharing, transfer and exchange of technology and relevant measures, policies, tools, processes, best practices and frameworks among the CSIRTs;

(c) to exchange relevant information about incidents, near misses, cyber threats, risks and vulnerabilities;

(d) to exchange information with regard to cybersecurity publications and recommendations;

(e) to ensure interoperability with regard to information-sharing specifications and protocols;

(f) at the request of a member of the CSIRTs network potentially affected by an incident, to exchange and discuss information in relation to that incident and associated cyber threats, risks and vulnerabilities;

(g) at the request of a member of the CSIRTs network, to discuss and, where possible, implement a coordinated response to an incident that has been identified within the jurisdiction of that Member State;

(h) to provide Member States with assistance in addressing cross-border incidents pursuant to this Directive;

(i) to cooperate, exchange best practices and provide assistance to the CSIRTs designated as coordinators pursuant to Article 12(1) with regard to the management of the coordinated disclosure of vulnerabilities which could have a significant impact on entities in more than one Member State;

(j) to discuss and identify further forms of operational cooperation, including in relation to:

  (i) categories of cyber threats and incidents;

  (ii) early warnings;

  (iii) mutual assistance;

  (iv) principles and arrangements for coordination in response to cross-border risks and incidents;

  (v) contribution to the national large-scale cybersecurity incident and crisis response plan referred to in Article 9(4) at the request of a Member State;

(k) to inform the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (j), and, where necessary, request guidance in that regard;

(l) to take stock of cybersecurity exercises, including those organised by ENISA;

(m) at the request of an individual CSIRT, to discuss the capabilities and preparedness of that CSIRT;

(n) to cooperate and exchange information with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and cyber threats across the Union;

(o) where relevant, to discuss the peer-review reports referred to in Article 19(9);

(p) to provide guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation.

4. 2025 年 1 月 17 日までに, 及び, その後は 2 年毎に, CSIRT ネットワークは, 第 40 条に示す見直しの目的のために, 業務運営上の協力に関して行われた進捗状況を評価し, かつ, 報告書を採択する。その報告書は, とりわけ, 国内 CSIRT との関係において遂行される, 第 19 条に示す相

互評価の結果を基礎とする結論及び推奨事項を記載する。当該報告書は，協力グループに対して提出される。

By 17 January 2025, and every two years thereafter, the CSIRTs network shall, for the purpose of the review referred to in Article 40, assess the progress made with regard to the operational cooperation and adopt a report. The report shall, in particular, draw up conclusions and recommendations on the basis of the outcome of the peer reviews referred to in Article 19, which are carried out in relation to the national CSIRTs. That report shall be submitted to the Cooperation Group.

5. CSIRT ネットワークは，その手続規則を採択する。

The CSIRTs network shall adopt its rules of procedure.

6. CSIRT ネットワーク及び EU-CyCLONe は，手続覚書に合意し，その手続覚書に基づいて協力する。

The CSIRTs network and EU-CyCLONe shall agree on procedural arrangements and cooperate on the basis thereof.

第 16 条 欧州サイバー危機連絡組織ネットワーク(EU-CyCLONe)

Article 16 **European cyber crisis liaison organisation network (EU-CyCLONe)**

1. 大規模なサイバーセキュリティのインシデント及び危機の調整された管理を業務運営レベルで支援するため，そして，構成国並びに欧州連合の機関，組織，事務局及び部局の間における関連情報の定期的な交換を確保するため，EU-CyCLONe が設置される。

EU-CyCLONe is established to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies.

2. EU-CyCLONe は，構成国のサイバー危機管理機関によって，並びに，潜在的または進行中の大規模なサイバーセキュリティのインシデントが，この指令の適用範囲内にあるサービス及び活動に対して重大な影響をもつ場合または重大な影響をもちそうな場合においては，欧州委員会によって構成される。それ以外の場合においては，欧州委員会は，オブザーバーとして，EU-CyCLONe の活動に参加する。

EU-CyCLONe shall be composed of the representatives of Member States' cyber crisis management authorities as well as, in cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have a significant impact on services and activities falling within the scope of this Directive, the

Commission. In other cases, the Commission shall participate in the activities of EU-CyCLONe as an observer.

ENISA は, EU-CyCLONe の事務局を提供し, かつ, 安全な情報交換を支援し, かつ, 安全な情報交換を確保する構成国間の協力を支援するために必要となるツールを提供する。

ENISA shall provide the secretariat of EU-CyCLONe and support the secure exchange of information as well as provide necessary tools to support cooperation between Member States ensuring secure exchange of information.

それが適切なときは, EU-CyCLONe は, 関連する利害関係者の代表に対し, オブザーバーとして EU-CyCLONe の活動に参加することを招請できる。

Where appropriate, EU-CyCLONe may invite representatives of relevant stakeholders to participate in its work as observers.

3. EU-CyCLONe は, 以下の職務をもつ:
   (a) 大規模なサイバーセキュリティのインシデント及び危機の管理の準備態勢のレベルを向上させる職務;
   (b) 大規模なサイバーセキュリティのインシデント及び危機に関する共有された状況認識を発展させる職務;
   (c) 関連する大規模なサイバーセキュリティのインシデント及び危機の結果及び影響を評価し, 可能な緩和措置を提案する職務;
   (d) 大規模なサイバーセキュリティのインシデント及び危機の管理を調整し, そのようなインシデント及び危機と関係する政治レベルの意思決定を支援する職務;
   (e) 関係する構成国の要請に応じて, 第 9 条第 4 項に示す大規模なサイバーセキュリティのインシデント及び危機の国内対応計画を討議する職務。

   EU-CyCLONe shall have the following tasks:
   (a) to increase the level of preparedness of the management of large-scale cybersecurity incidents and crises;
   (b) to develop a shared situational awareness for large-scale cybersecurity incidents and crises;
   (c) to assess the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigation measures;
   (d) to coordinate the management of large-scale cybersecurity incidents and crises and support decision-making at political level in relation to such incidents and crises;
   (e) to discuss, upon the request of a Member State concerned, national large-scale cybersecurity incident and crisis response plans referred to in Article 9(4).

4. EU-CyCLONe は, その手続規則を採択する。

EU-CyCLONe shall adopt its rules of procedure.

5. EU-CyCLONe は，協力グループに対し，大規模なサイバーセキュリティのインシデント及び危機の管理に関し，並びに，基礎法主体及び重要法主体に対する当該大規模なサイバーセキュリティのインシデント及び危機の影響に焦点を当てて，その動向に関し，定期的に報告する。

EU-CyCLONe shall report on a regular basis to the Cooperation Group on the management of large-scale cybersecurity incidents and crises, as well as trends, focusing in particular on their impact on essential and important entities.

6. EU-CyCLONe は，第 15 条第 6 項に定める合意された手続覚書に基づき，CSIRT ネットワークと協力する。

EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements provided for in Article 15(6).

7. 2024 年 7 月 17 日までに，及び，その後は 18 か月毎に，EU-CyCLONe は，欧州議会及び理事会に対し，EU-CyCLONe の作業を評価する報告書を提出する。

By 17 July 2024 and every 18 months thereafter, EU-CyCLONe shall submit to the European Parliament and to the Council a report assessing its work.

第 17 条　国際的な協力

Article 17 **International cooperation**

それが適切なときは，欧州連合は，TFEU の第 218 条に従い，第三国または国際機関との間で，とりわけ，協力グループ，CSIRT ネットワーク及び EU-CyCLONe の活動への第三国または国際機関の参加を認め及び計画する国際的な合意を締結できる。そのような合意は，欧州連合のデータ保護法を遵守する。

The Union may, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in particular activities of the Cooperation Group, the CSIRTs network and EU-CyCLONe. Such agreements shall comply with Union data protection law.

第 18 条 欧州連合内のサイバーセキュリティの状態に関する報告

Article 18 **Report on the state of cybersecurity in the Union**

1. ENISA は，欧州委員会及び協力グループと協力して，欧州連合内のサイバーセキュリティの状態に関する隔年の報告書を採択し，かつ，欧州議会に対し，当該報告書を提出して提示する。その報告書は，就中，機械読取り可能なデータで利用できるようにされ，かつ，以下の評価を含める：
   (a) サイバーな脅威の全体的把握を考慮に入れた，欧州連合レベルのサイバーセキュリティのリスク評価；
   (b) 欧州連合全域の公的部門及び民間部門におけるサイバーセキュリティの実現能力の発展の評価；
   (c) 小企業及び中規模企業を含め，市民及び法主体の中における一般的なレベルのサイバーセキュリティの認識及びサイバー衛生の評価；
   (d) 第 19 条に示す相互評価の結果の総合評価；
   (e) 部門レベルの熟達レベルを含め，欧州連合全域のサイバーセキュリティの実現能力及び資源の熟達レベルの総合評価，並びに，構成国の国内サイバーセキュリティ戦略が揃えられている範囲の総合評価。

   ENISA shall adopt, in cooperation with the Commission and the Cooperation Group, a biennial report on the state of cybersecurity in the Union and shall submit and present that report to the European Parliament. The report shall, inter alia, be made available in machine-readable data and include the following:
   (a) a Union-level cybersecurity risk assessment, taking account of the cyber threat landscape;
   (b) an assessment of the development of cybersecurity capabilities in the public and private sectors across the Union;
   (c) an assessment of the general level of cybersecurity awareness and cyber hygiene among citizens and entities, including small and medium-sized enterprises;
   (d) an aggregated assessment of the outcome of the peer reviews referred to in Article 19;
   (e) an aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union, including those at sector level, as well as of the extent to which the Member States' national cybersecurity strategies are aligned.

2. その報告書は，欧州連合全域のサイバーセキュリティの欠点とレベルの向上に対処するという観点から，基本方針上の特定の推奨事項，並びに，規則(EU) 2019/881 の第 7 条第 6 項に従って ENISA により準備されるインシデント及びサイバーな脅威に関する EU サイバーセキュリティ技術状況報告書からの特定の期間に関する判断結果の要旨を含める。

   The report shall include particular policy recommendations, with a view to addressing shortcomings and increasing the level of cybersecurity across the Union, and a summary of the findings for the particular period from the EU Cybersecurity Technical Situation Reports on incidents and cyber threats prepared

by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.

3. ENISA は，欧州委員会，協力グループ及び CSIRT ネットワークと協力して，定量的指標及び定性的指標のような関連変数を含め，第 1 項(e)に示す総合評価の手法を開発する。

ENISA, in cooperation with the Commission, the Cooperation Group and the CSIRTs network, shall develop the methodology, including the relevant variables, such as quantitative and qualitative indicators, of the aggregated assessment referred to in paragraph 1, point (e).

第 19 条 相互評価

Article 19 **Peer reviews**

1. 協力グループは，2025 年 1 月 17 日，欧州委員会及び ENISA，並びに，それが関連するときは，CSIRT ネットワークの補助を得て，共有された経験から学習し，相互の信頼を強化し,共通の高いレベルのサイバーセキュリティを達成し，かつ，構成国のサイバーセキュリティの実現能力及びこの指令を実装するために必要となる基本方針を拡大するため，相互評価の技術的側面及び組織的側面を定める。相互評価への参加は，任意である。相互評価は，サイバーセキュリティの専門家によって遂行される。そのサイバーセキュリティの専門家は，評価を受ける構成国とは別の少なくとも 2 つの構成国によって指定される。

The Cooperation Group shall, on 17 January 2025, establish, with the assistance of the Commission and ENISA, and, where relevant, the CSIRTs network, the methodology and organisational aspects of peer reviews with a view to learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity, as well as enhancing Member States' cybersecurity capabilities and policies necessary to implement this Directive. Participation in peer reviews is voluntary. The peer reviews shall be carried out by cybersecurity experts. The cybersecurity experts shall be designated by at least two Member States, different from the Member State being reviewed.

相互評価は，以下の少なくとも 1 つの事項を包摂する：

(a) 第 21 条及び第 23 条に定めるサイバーセキュリティのリスク管理の措置及び報告義務の実装のレベル；
(b) 利用可能な資金，技術上の資源及び人的資源を含め，実現能力のレベル，並びに，職務権限のある機関の職務の執行の実効性；
(c) CSIRT の業務運営上の実現能力；
(d) 第 37 条に示す相互補助の実装のレベル；
(e) 第 29 条に示すサイバーセキュリティ情報共有覚書の実装のレベル；
(f) 国境を越える性質または部門横断の性質をもつ個別の問題。

The peer reviews shall cover at least one of the following:

(a) the level of implementation of the cybersecurity risk-management measures and reporting obligations laid down in Articles 21 and 23;
(b) the level of capabilities, including the available financial, technical and human resources, and the effectiveness of the exercise of the tasks of the competent authorities;
(c) the operational capabilities of the CSIRTs;
(d) the level of implementation of mutual assistance referred to in Article 37;
(e) the level of implementation of the cybersecurity information-sharing arrangements referred to in Article 29;
(f) specific issues of cross-border or cross-sector nature.

2. 第 1 項に示す手法は，その基準を基礎として構成国が相互評価を遂行するサイバーセキュリティの専門家を指定する客観的で，非差別で，公正かつ透明性のある基準を含める。欧州委員会及び ENISA は，オブザーバーとして，相互評価に参加する。

The methodology referred to in paragraph 1 shall include objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States designate cybersecurity experts eligible to carry out the peer reviews. The Commission and ENISA shall participate as observers in the peer reviews.

3. 構成国は，相互評価の目的のために，第 1 項(f)に示す個別の問題を指定できる。

Member States may identify specific issues as referred to in paragraph 1, point (f), for the purposes of a peer review.

4. 第 1 項に示す相互評価を開始する前に，構成国は，参加する構成国に対し，第 3 項により指定された個別の問題を含め，その相互評価の範囲を通知する。

Before commencing a peer review as referred to in paragraph 1, Member States shall notify the participating Member States of its scope, including the specific issues identified pursuant to paragraph 3.

5. 相互評価の開始前に，構成国は，評価された側面の自己評価を遂行し，指定されたサイバーセキュリティの専門家に対し，当該自己評価の結果を提供できる。協力グループは，欧州委員会及び ENISA の補助を得て，構成国の自己評価の手法を定める。

Prior to the commencement of the peer review, Member States may carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated cybersecurity experts. The Cooperation Group shall, with the assistance of the Commission and ENISA, lay down the methodology for the Member States' self-assessment.

6. 相互評価は，物理的または仮想の施設内の訪問及び施設外の情報交換を伴う。良い協力の原則に沿って，相互評価を受ける構成国は，秘密情報または機密情報の保護に関する欧州連合法

または国内法を妨げることなく，かつ，国家安全保障のような必須の国家機能の安全確保を妨げることなく，指定されたサイバーセキュリティの専門家に対し，その評価のために必要な情報を提供する。協力グループは，欧州委員会及び ENISA と協力して，指定されたサイバーセキュリティの専門家の作業手法を支える適切な行動準則を策定する。相互評価を通じて得られた情報は，当該目的のために限り，使用される。相互評価に参加するサイバーセキュリティの専門家は，当該相互評価の過程において入手した機微の情報または機密情報を第三者に対して開示してはならない。

Peer reviews shall entail physical or virtual on-site visits and off-site exchanges of information. In line with the principle of good cooperation, the Member State subject to the peer review shall provide the designated cybersecurity experts with the information necessary for the assessment, without prejudice to Union or national law concerning the protection of confidential or classified information and to the safeguarding of essential State functions, such as national security. The Cooperation Group, in cooperation with the Commission and ENISA, shall develop appropriate codes of conduct underpinning the working methods of designated cybersecurity experts. Any information obtained through the peer review shall be used solely for that purpose. The cybersecurity experts participating in the peer review shall not disclose any sensitive or confidential information obtained in the course of that peer review to any third parties.

7. 一度相互評価に服した後は，ある構成国において評価されたのと同一の側面は，その構成国から別異に要請された場合，または，協力グループの提案に応じて合意された場合を除き，その相互評価の完了後 2 年間は，当該構成国において別の相互評価に服してはならない。

Once subject to a peer review, the same aspects reviewed in a Member State shall not be subject to a further peer review in that Member State for two years following the conclusion of the peer review, unless otherwise requested by the Member State or agreed upon after a proposal of the Cooperation Group.

8. 構成国は，その相互評価の開始の前に，指定されたサイバーセキュリティの専門家と関係する利益相反のリスクが，別の構成国，協力グループ，欧州委員会及び ENISA に対して明らかにされることを確保する。その相互評価を受ける構成国は，指定元である構成国に対して通知される適正に根拠づけられた理由に基づき，特定のサイバーセキュリティの専門家の指定に対して異議を申立て得る。

Member States shall ensure that any risk of conflict of interest concerning the designated cybersecurity experts is revealed to the other Member States, the Cooperation Group, the Commission and ENISA, before the commencement of the peer review. The Member State subject to the peer review may object to the designation of particular cybersecurity experts on duly substantiated grounds communicated to the designating Member State.

9. 相互評価に参加するサイバーセキュリティの専門家は，その相互評価の判断及び結論に関する

報告書を作成する。相互評価を受ける構成国は，その相互評価に関する報告書案に対するコメントを提供でき，そのようなコメントは，その報告書に添付される。その報告書は，その相互評価によって包摂される側面に関して改善できるようにするための推奨事項を含める。その報告書は，協力グループに対し，及び，それが関連するときは，CSIRT ネットワークに対し，提出される。相互評価を受ける構成国は，その相互評価の報告書またはその報告書の抜粋版を公表することを決定できる。

Cybersecurity experts participating in peer reviews shall draft reports on the findings and conclusions of the peer reviews. Member States subject to a peer review may provide comments on the draft reports concerning them and such comments shall be attached to the reports. The reports shall include recommendations to enable improvement on the aspects covered by the peer review. The reports shall be submitted to the Cooperation Group and the CSIRTs network where relevant. A Member State subject to the peer review may decide to make its report, or a redacted version of it, publicly available.

第IV章 サイバーセキュリティのリスク管理措置及び報告義務

Chapter IV Cybersecurity Risk-Management Measures and Reporting Obligations

第 20 条 統治

Article 20 **Governance**

1. 構成国は，基礎法主体及び重要法主体の経営陣が，第 21 条を遵守するために当該法主体によって講じられたサイバーセキュリティのリスク管理の措置を承認すること，その措置の実装を監督すること，そして，その法主体による同条の違反行為に関して法的責任を負い得ることを確保する。

   Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.

   本項の適用は，行政機関に適用可能な法的責任の規定，並びに，公務員及び選任されまたは任命された官吏の法的責任に関する国内法を妨げてはならない。

   The application of this paragraph shall be without prejudice to national law as regards the liability rules applicable to public institutions, as well as the liability of public servants and elected or appointed officials.

2. 構成国は，それらの者がリスクを識別できるようにするため，そして，サイバーセキュリティのリスク管理の実務とその法主体から提供されるサービスに対するそれらのリスクの影響を評価できるようにするための十分な知識及び技能をそれらの者が獲得するため，基礎法主体及び重要法主体の経営陣の構成員が訓練を受けることを要求されることを確保し，かつ，基礎法主体及び重要法主体に対し，定期的にその法主体の従業者に対して類似の訓練を提供することを推奨する。

   Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

第 21 条 サイバーセキュリティのリスク管理措置

Article 21 **Cybersecurity risk-management measures**

1. 構成国は，基礎法主体及び重要法主体が，当該法主体が当該法主体の業務運営のためもしくは当該法主体のサービスの提供のために使用するネットワーク及び情報システムの防護に対して

示されたリスクを管理するための，そして，当該法主体のサービスの受け手に対する及びそれら以外のサービスに対するインシデントの影響を防止または緩和するための，適切かつ比例的な技術上の措置，業務運営上の措置及び組織上の措置を講ずることを確保する。

Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

最新の技術標準，及び，それが適用可能なときは，関連する欧州の技術標準と国際的な技術標準，並びに，実装の費用を考慮に入れた上で，第 1 副項に示す措置は，示されたリスクに対して適切なレベルのネットワーク及び情報システムの防護を確保するものとする。当該措置の比例性を評価する際，その法主体がリスクに晒されている程度，及び，その法主体の規模，並びに，インシデント発生の蓋然性，及び，そのインシデントの社会的影響及び経済的影響を含め，そのインシデントの深刻度が適正に考慮に入れられるものとする。

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

2. 第 1 項に示す措置は，ネットワーク及び情報システムと当該システムの物理環境をインシデントから保護することを狙いとするオールハザードアプローチを基礎とし，かつ，少なくとも以下の事項を含める：
   (a) リスク分析及び情報システムの防護に関する基本方針；
   (b) インシデントの取扱い；
   (c) バックアップ管理と災害からの復旧のような事業継続性，及び，危機管理；
   (d) 法主体とその法主体の直接の供給者またはサービスプロバイダそれぞれとの間の関係に関する防護関連の側面を含め，サプライチェーンの防護；
   (e) 脆弱性の取扱い及び開示を含め，ネットワーク及び情報システムの獲得，開発及び維持管理における防護；
   (f) サイバーセキュリティのリスク管理の措置の実効性を評価するための基本方針及び手順；
   (g) 基本的なサイバー衛生実務及びサイバーセキュリティ訓練；
   (h) 暗号学の利用，及び，それが適切なときは，暗号の利用と関連する基本方針及び手順；
   (i) 人的資源の防護，アクセス管理の基本方針及び資産管理；
   (j) それが適切なときは，その法主体内における，多要素認証または継続認証ソリューション，秘話通信，セキュアビデオ通信及びセキュアテクスト通信並びに安全な緊急通信システムの利用。

The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;
(b) incident handling;
(c) business continuity, such as backup management and disaster recovery, and crisis management;
(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
(g) basic cyber hygiene practices and cybersecurity training;
(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;
(i) human resources security, access control policies and asset management;
(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

3. 構成国は，本条の第 2 項(d)に示すどの措置が適切であるかを判断する際，法主体が，直接の供給者及びサービスプロバイダそれぞれに特有の脆弱性，並びに，当該製品の安全な開発手順を含め，当該法主体の供給者及びサービスプロバイダの製品の全体的な品質及びサイバーセキュリティの実務を考慮に入れることを確保する。構成国は，同項に示すどの措置が適切であるかを判断する際，法主体が，第 22 条第 1 項に従って遂行される重要サプライチェーンの調整されたセキュリティリスク評価の結果を考慮に入れることが要求されることも確保する。

Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).

4. 構成国は，第 2 項に定める措置を遵守していないと判断する法主体が，不適切な遅滞なく，必要な全ての適切かつ比例的な是正の措置を講ずることを確保する。

Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.

5. 2024 年 10 月 17 日までに，欧州委員会は，DNS サービスのプロバイダ，TLD 名レジストリ，クラウドコンピューティングサービスのプロバイダ，データセンターサービスのプロバイダ，コンテント伝達ネットワークのプロバイダ，マネージドサービスのプロバイダ，マネージドセキュリティサービスのプロバイダ，オンライン市場のプロバイダ，オンライン検索エンジンのプロバイダ及びソーシャルネットワーキングサービスプラットフォームのプロバイダ並びに信頼サービスのプロバイダに関し，第 2 項に示す措置の技術上及び手法上の要件を定める実装行為を採択する。

By 17 October 2024, the Commission shall adopt implementing acts laying down the technical and the methodological requirements of the measures referred to in paragraph 2 with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.

欧州委員会は，本項の第 1 副項に示す法主体以外の基礎法主体及び重要法主体に関し，第 2 項に示す措置の技術上及び手法上の要件，並びに，必要に応じて，部門別の要件を定める実装行為を採択できる。

The Commission may adopt implementing acts laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures referred to in paragraph 2 with regard to essential and important entities other than those referred to in the first subparagraph of this paragraph.

本項の第 1 副項及び第 2 副項に示す実装行為を準備する際，欧州委員会は，可能な範囲内で，欧州の技術標準及び国際的な語術標準並びに関連する技術仕様に従う。欧州委員会は，第 14 条第 4 項(e)に従い，実装行為案に関し，協力グループ及び ENISA との間で，助言を交換し，かつ，それらと協力する。

When preparing the implementing acts referred to in the first and second subparagraphs of this paragraph, the Commission shall, to the extent possible, follow European and international standards, as well as relevant technical specifications. The Commission shall exchange advice and cooperate with the Cooperation Group and ENISA on the draft implementing acts in accordance with Article 14(4), point (e).

同実装行為は，第 39 条第 2 項に示す審議手続に従って採択される。

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

第 22 条　重要サプライチェーンの欧州連合レベルの調整されたセキュリティリスク評価
Article 22 **Union level coordinated security risk assessments of critical supply chains**

1. 協力グループは，欧州委員会及び ENISA と協力し，技術上のリスク要素，及び，それが関連するときは，非技術上のリスク要素を考慮に入れた上で，特定の重要な ICT サービス，ICT システムまたは ICT 製品のサプライチェーンの調整されたセキュリティリスク評価を遂行できる。

   The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors.

2. 欧州委員会は，協力グループ及び ENISA の意見聴取を経た上で，並びに，それが必要なときは，関連する利害関係者の意見聴取を経た上で，第 1 項に示す調整されたセキュリティリスク評価に服し得る特定の重要な ICT サービス，ICT システムまたは ICT 製品を識別する。

   The Commission, after consulting the Cooperation Group and ENISA, and, where necessary, relevant stakeholders, shall identify the specific critical ICT services, ICT systems or ICT products that may be subject to the coordinated security risk assessment referred to in paragraph 1.

第 23 条　報告義務
Article 23 **Reporting obligations**

1. 各構成国は，基礎法主体及び重要法主体が，不適切な遅滞なく，その構成国の CSIRT に対し，または，それが適用可能なときは，その構成国の職務権限のある機関に対し，第 4 項に従い，第 3 項に示す当該法主体のサービスの提供に対する重大な影響をもつインシデント（重大なインシデント）を通知することを確保する。それが適切なときは，関係する法主体は，不適切な遅滞なく，当該法主体のサービスの受け手に対し，当該サービスの提供に負の影響を与えるおそれのある重大なインシデントを通知する。各構成国は，就中，CSIRT，または，それが適用可能なときは，職務権限のある機関がそのインシデントの国境を越える影響の有無を決定できるようにする情報を，当該法主体が報告することを確保する。通知の行為があったというだけで通知元である法主体の法的責任を増加させてはならない。

   Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident). Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere

act of notification shall not subject the notifying entity to increased liability.

関係する法主体が職務権限のある機関に対して第 1 副項の重大なインシデントを通知したときは，構成国は，当該職務権限のある機関が，受領次第，CSIRT に対してその通知を転送することを確保する。

Where the entities concerned notify the competent authority of a significant incident under the first subparagraph, the Member State shall ensure that that competent authority forwards the notification to the CSIRT upon receipt.

国境を越える重大なインシデントまたは部門横断の重大なインシデントの場合においては，構成国は，その構成国の単一連絡部局が，適時に，第 4 項に従って通知された関連情報の提供を受けることを確保する。

In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with paragraph 4.

2. それが適用可能なときは，構成国は，基礎法主体及び重要法主体が，不適切な遅滞なく，重大なサイバーな脅威によって潜在的な影響を受ける当該法主体のサービスの受け手に対し，当該脅威への対応において当該の受け手がとることのできる手段または解決策を通知することを確保する。それが適切なときは，その法主体は，当該サービスの受け手に対し，重大なサイバーな脅威それ自体も連絡する。

Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.

3. 以下の場合においては，インシデントは，重大であると判断される：
   (a) 関係する法主体に関し，そのサービスの業務運営上の深刻な混乱または金銭的な損失を生じさせた場合，または，生じさせる得る場合；
   (b) 有形または無形の甚大な損害を生じさせることによって，他の自然人または法人に対して影響を与えた場合，または，影響を与え得る場合。

An incident shall be considered to be significant if:
   (a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

4. 構成国は，第 1 項に基づく通知の目的のために，関係する法主体が，CSIRT に対し，または，それが適用可能なときは，職務権限のある機関に対し：
   (a) 不適切な遅滞なく，かつ，いかなる場合においても重大なインシデントに気づいた時から 24 時間以内に，それが適用可能なときは，違法な行為もしくは悪意ある行為によって生じさせられている重大なインシデントであるかどうか，または，国境を越える影響をもち得るインシデントであるかどうかを示す早期警戒を：
   (b) 不適切な遅滞なく，かつ，いかなる場合においても重大なインシデントに気づいた時から 72 時間以内に，それが適用可能なときは，(a)に示す情報をアップデートし，かつ，そのインシデントの深刻度及び影響を含め，並びに，それが利用可能なときは，侵害指標を含め，重大なインシデントの当初評価を示すインシデント通知を；
   (c) CSIRT の要請に応じて，または，それが適用可能なときは，職務権限のある機関の要請に応じて，関連する状態のアップデートに関する中間報告書を；
   (d) (b)に基づくインシデント通知の提出後遅くとも 1 か月以内に，以下の事項を含め，最終報告書を：
      (i) 深刻度及び影響を含め，そのインシデントの詳細な記述；
      (ii) そのインシデントの引き金となった可能性のある脅威または根本原因のタイプ；
      (iii) 適用された緩和措置及び現在適用中の緩和措置；
      (iv) それが適用可能なときは，そのインシデントの国境を越える影響；
   提出することを確保し，
   (e) (d)に示す最終報告書の提出時においてインシデントが進行中の場合，構成国は，関係する法主体が，当該の時点では進行状況報告書を提供し，そして，そのインシデントに対する当該法主体の取扱いの 1 か月以内に最終報告書を提供することを確保する。

Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority:
(a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;
(b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;
(c) upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates;
(d) a final report not later than one month after the submission of the incident notification under point (b), including the following:
   (i) a detailed description of the incident, including its severity and impact;
   (ii) the type of threat or root cause that is likely to have triggered the incident;
   (iii) applied and ongoing mitigation measures;
   (iv) where applicable, the cross-border impact of the incident;

(e) in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.

第 1 副項(b)からの特例により，信頼サービスのプロバイダは，そのプロバイダの信頼サービスの提供に対して影響をもつ重大なインシデントに関し，CSIRT に対し，または，それが適用可能なときは，職務権限のある機関に対し，不適切な遅滞なく，かつ，いかなる場合においても重大なインシデントに気づいた時から 24 時間以内に，通知する。

By way of derogation from the first subparagraph, point (b), a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify the CSIRT or, where applicable, the competent authority, without undue delay and in any event within 24 hours of becoming aware of the significant incident.

5. CSIRT または職務権限のある機関は，不適切な遅滞なく，かつ，可能であれば，第 4 項(a)に示す早期警戒の受領から 24 時間以内に，その重大なインシデントに関する最初のフィードバックを含め，また，その法主体の求めに応じて，可能な緩和措置の実装に関するガイドまたは業務運営上の助言を含め，通知元法主体への回答を提供する。その CSIRT が第 1 項に示す通知の最初の受領者ではないときは，そのガイドは，その CSIRT と協力して，職務権限のある機関から提供される。CSIRT は，関係する法主体がそのように求めるときは，追加的な技術上の支援を提供する。その重大なインシデントが犯罪の性質をもつインシデントであると疑われるときは，CSIRT または職務権限のある機関は，法執行機関に対する重大なインシデントの報告に関するガイドも提供する。

The CSIRT or the competent authority shall provide, without undue delay and where possible within 24 hours of receiving the early warning referred to in paragraph 4, point (a), a response to the notifying entity, including initial feedback on the significant incident and, upon request of the entity, guidance or operational advice on the implementation of possible mitigation measures. Where the CSIRT is not the initial recipient of the notification referred to in paragraph 1, the guidance shall be provided by the competent authority in cooperation with the CSIRT. The CSIRT shall provide additional technical support if the entity concerned so requests. Where the significant incident is suspected to be of criminal nature, the CSIRT or the competent authority shall also provide guidance on reporting the significant incident to law enforcement authorities.

6. それが適切なときは，及び，とりわけ，その重大なインシデントが複数の構成国と関係するときは，CSIRT，職務権限のある機関または単一連絡部局は，不適切な遅滞なく，他の影響を受ける構成国及び ENISA に対し，その重要なインシデントを連絡する。そのような情報は，第 4 項に従って受けた情報のタイプを含める。そのようにする際，CSIRT，職務権限のある機関または単一連絡部局は，欧州連合法または国内法に従い，その法主体の防護及び商業上の利益並びに提供された情報の機密性を保持する。

Where appropriate, and in particular where the significant incident concerns two or more Member States, the CSIRT, the competent authority or the single point of contact shall inform, without undue delay, the other affected Member States and ENISA of the significant incident. Such information shall include the type of information received in accordance with paragraph 4. In so doing, the CSIRT, the competent authority or the single point of contact shall, in accordance with Union or national law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.

7. 重大なインシデントを防止するためもしくは進行中の重大なインシデントに対処するために公衆の認識が必要な場合，または，重大なインシデントを開示することが，そうしなければ公共の利益にかかわる場合においては，構成国の CSIRT，または，それが適用可能なときは，構成国の職務権限のある機関，及び，それが適切なときは，関係する別の構成国の CSIRT または職務権限のある機関は，関係する法主体の意見聴取を経た上で，公衆に対してその重大なインシデントを連絡し，または，その法主体に対してそのようにすることを要求し得る。

Where public awareness is necessary to prevent a significant incident or to deal with an ongoing significant incident, or where disclosure of the significant incident is otherwise in the public interest, a Member State's CSIRT or, where applicable, its competent authority, and, where appropriate, the CSIRTs or the competent authorities of other Member States concerned, may, after consulting the entity concerned, inform the public about the significant incident or require the entity to do so.

8. CSIRT または職務権限のある機関の要請に応じて，単一連絡部局は，影響を受ける別の構成国の単一連絡部局に対し，第 1 項により受領した通知を転送する。

At the request of the CSIRT or the competent authority, the single point of contact shall forward notifications received pursuant to paragraph 1 to the single points of contact of other affected Member States.

9. 単一連絡部局は，ENISA に対し，3 か月毎に，本条の第 1 項及び第 30 条に従って通知された重大なインシデント，インシデント，サイバーな脅威及びニアミスに関する匿名化され集約されたデータを含む概況報告書を提出する。比較可能な情報の提供に貢献するため，ENISA は，その概況報告書の中に含められるべき情報のパラメータに関する技術上のガイドを採択できる。ENISA は，6 か月毎に，協力グループ及び CSIRT ネットワークに対し，受領した通知に関する ENISA の判断に関して連絡する。

The single point of contact shall submit to ENISA every three months a summary report, including anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 30. In order to contribute to the provision of comparable information, ENISA may adopt technical guidance on the parameters of the information to be included in the summary report. ENISA shall inform the Cooperation Group and the CSIRTs network about its findings on notifications received every six months.

10. CSIRT, または, それが適用可能なときは, 職務権限のある機関は, 指令(EU) 2022/2557 の下にある職務権限のある機関に対し, 指令(EU) 2022/2557 の下において必須法主体として指定された法主体によって本条の第 1 項及び第 30 条に従って通知された重大なインシデント, インシデント, サイバーな脅威及びニアミスに関する情報を提供する。

The CSIRTs or, where applicable, the competent authorities shall provide to the competent authorities under Directive (EU) 2022/2557 information about significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 30 by entities identified as critical entities under Directive (EU) 2022/2557.

11. 欧州委員会は, 情報のタイプ, 本条の第 1 項及び第 30 条により提出される通知並びに本条の第 2 項により提出される通知の書式及び手順を別に定める実装行為を採択できる。

The Commission may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraph 1 of this Article and to Article 30 and of a communication submitted pursuant to paragraph 2 of this Article.

2024 年 10 月 17 日までに, 欧州委員会は, DNS サービスのプロバイダ, TLD 名レジストリ, クラウドコンピューティングサービスのプロバイダ, データセンターサービスのプロバイダ, コンテント伝達ネットワークのプロバイダ, マネージドサービスのプロバイダ, マネージドセキュリティサービスのプロバイダ, 並びに, オンライン市場のプロバイダ, オンライン検索エンジンのプロバイダ及びソーシャルネットワーキングサービスプラットフォームのプロバイダに関し, 第 3 項に示す重大であると判断されるインシデントの場合を別に定める実装行為を採択する。欧州委員会は, それら以外の基礎法主体及び重要法主体に関し, そのような実装行為を採択し得る。

By 17 October 2024, the Commission shall, with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, adopt implementing acts further specifying the cases in which an incident shall be considered to be significant as referred to in paragraph 3. The Commission may adopt such implementing acts with regard to other essential and important entities.

欧州委員会は, 第 14 条第 4 項(e)に従い, 本項の第 1 副項及び第 2 副項に示す実装行為案に関し, 協力グループとの間で, 助言を交換し, かつ, 協力グループと協力する。

The Commission shall exchange advice and cooperate with the Cooperation Group on the draft implementing acts referred to in the first and second subparagraphs of this paragraph in accordance with Article 14(4), point (e).

同実装行為は，第 39 条第 2 項に示す審議手続に従って採択される。

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

第 24 条 欧州サイバーセキュリティ認証制度の利用

Article 24 **Use of European cybersecurity certification schemes**

1. 第 21 条に示す特別の要件の遵守を示すため，構成国は，基礎法主体及び重要法主体に対し，規則(EU) 2019/881 の第 49 条により採択された欧州サイバーセキュリティ認証制度の下で認証を受けている，基礎法主体もしくは重要法主体によって製造され，または，第三者から調達された，特別の ICT 製品，ICT サービス及び ICT プロセスを利用することを要求できる。更に，構成国は，基礎法主体及び重要法主体に対し，適格信頼サービスを利用することを推奨する。

   In order to demonstrate compliance with particular requirements of Article 21, Member States may require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. Furthermore, Member States shall encourage essential and important entities to use qualified trust services.

2. 欧州委員会は，第 38 条に従い，どの類型の基礎法主体及び重要法主体が，規則(EU) 2019/881 の第 49 条により採択された欧州サイバーセキュリティ認証制度の下において認証を受けた一定の ICT 製品，ICT サービス及び ICT プロセスを利用することを要求され，または，その認証を獲得することを要求されるかを定めることによってこの指令を補完するための委任される行為を採択する権限が与えられる。それらの委任される行為は，不十分なレベルのサイバーセキュリティが発見された場合に採択され，かつ，実装の期限を含める。

   The Commission is empowered to adopt delegated acts, in accordance with Article 38, to supplement this Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881. Those delegated acts shall be adopted where insufficient levels of cybersecurity have been identified and shall include an implementation period.

   そのような委任される行為を採択する前に，欧州委員会は，影響評価を実施し，かつ，規則(EU) 2019/881 の第 56 条に従い，意見聴取を実施する。

   Before adopting such delegated acts, the Commission shall carry out an impact assessment and shall carry

out consultations in accordance with Article 56 of Regulation (EU) 2019/881.

3. 本条の第 2 項の目的のための適切な欧州サイバーセキュリティ認証制度が利用可能ではないときは，欧州委員会は，協力グループ及び欧州サイバーセキュリティ認証グループの意見聴取を経た上で，ENISA に対し，規則(EU) 2019/881 の第 48 条第 2 項による制度候補を準備することを要求できる。

Where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 of this Article is available, the Commission may, after consulting the Cooperation Group and the European Cybersecurity Certification Group, request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881.

第 25 条 標準化

Article 25 **Standardisation**

1. 第 21 条第 1 項及び第 2 項の収斂的な実装を促進するため，構成国は，特定のタイプの技術の利用の支持を義務化または差別化することなく，ネットワーク及び情報システムの防護と関連する欧州の技術標準及び国際的な技術標準並びに技術仕様の利用を推奨する。

In order to promote the convergent implementation of Article 21(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security of network and information systems.

2. ENISA は，構成国と協力して，かつ，それが適切なときは，関連する利害関係者の意見聴取を経た上で，第 1 項と関係して検討されるべき技術分野に関する助言及びガイド，並びに，国内技術標準を含め，当該分野が包摂され得るような既存の技術標準に関する助言及びガイドを作成する。

ENISA, in cooperation with Member States, and, where appropriate, after consulting relevant stakeholders, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including national standards, which would allow for those areas to be covered.

第Ⅴ章 管轄権及び登録

Chapter V Jurisdiction and Registration

第 26 条 管轄権及び地理的適用範囲

Article 26 **Jurisdiction and territoriality**

1. この指令の適用範囲内にある法主体は，以下の場合を除き，当該法主体の拠点のある構成国の管轄権の下にあると判断される：
   (a) 公共電子通信ネットワークのプロバイダまたは公衆が利用可能な電子通信サービスのプロバイダであって，当該プロバイダが当該プロバイダのサービスを提供する構成国の管轄権の下にあると判断されるもの；
   (b) DNS サービスのプロバイダ，TLD 名レジストリ，ドメイン名登録サービスを提供する法主体，クラウドコンピューティングサービスのプロバイダ，データセンターサービスのプロバイダ，コンテント伝達ネットワークのプロバイダ，マネージドサービスのプロバイダ，マネージドセキュリティサービスのプロバイダ，並びに，オンライン市場のプロバイダ，オンライン検索エンジンのプロバイダまたはソーシャルネットワーキングサービスプラットフォームのプロバイダであって，第 2 項に基づき，当該プロバイダが当該プロバイダの欧州連合内の主たる拠点をもつ構成国の管轄権の下にあると判断されるもの；
   (c) 行政機関である法主体であって，当該法主体を設置した構成国の管轄権の下にあると判断されるもの。

   Entities falling within the scope of this Directive shall be considered to fall under the jurisdiction of the Member State in which they are established, except in the case of:
   (a) providers of public electronic communications networks or providers of publicly available electronic communications services, which shall be considered to fall under the jurisdiction of the Member State in which they provide their services;
   (b) DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines or of social networking services platforms, which shall be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union under paragraph 2;
   (c) public administration entities, which shall be considered to fall under the jurisdiction of the Member State which established them.

2. この指令の目的のために，第 1 項(b)に示す法主体は，サイバーセキュリティのリスク管理の措置と関連する決定が主として行われる構成国において，その法主体の欧州連合内の主たる拠点をもつと判断される。そのような構成国が決定され得ない場合，または，そのような決定が欧州連合内では行われない場合，その主たる拠点は，サイバーセキュリティの業務運営が実施される構成

国にあると判断される。そのような構成国が決定され得ない場合，その主たる拠点は，関係する法主体が，欧州連合内における最多従業者数の拠点をもつ構成国にあると判断される。

For the purposes of this Directive, an entity as referred to in paragraph 1, point (b), shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity risk-management measures are predominantly taken. If such a Member State cannot be determined or if such decisions are not taken in the Union, the main establishment shall be considered to be in the Member State where cybersecurity operations are carried out. If such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the entity concerned has the establishment with the highest number of employees in the Union.

3. 第 1 項(b)に示す法主体が欧州連合内に拠点をもたないが，欧州連合内でサービスを提供するときは，その法主体は，欧州連合内における代理者を指定する。その代理者は，そのサービスが提供される構成国中の 1 つに拠点をもつ。そのような法主体は，その代理者が拠点をもつ構成国の管轄権の下にあると判断される。本項の下で指定される欧州連合内における代理者が存在しないときは，その法主体がサービスを提供する構成国は，いずれも，この指令の違反行為に関し，その法主体を相手方として，法律上の行動をとり得る。

If an entity as referred to in paragraph 1, point (b), is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established. In the absence of a representative in the Union designated under this paragraph, any Member State in which the entity provides services may take legal actions against the entity for the infringement of this Directive.

4. 第 1 項(b)に示す法主体による代理者の指定は，法律上の行動を妨げてはならず，その法律上の行動は，その法主体自身を相手方として開始され得る。

The designation of a representative by an entity as referred to in paragraph 1, point (b), shall be without prejudice to legal actions, which could be initiated against the entity itself.

5. 第 1 項(b)に示す法主体と関係する相互補助の要請を受けた構成国は，当該要請の期限内に，当該構成国の領土内でサービスを提供する関係法主体との関係において，または，その構成国の領土内にネットワーク及び情報システムをもつ関係法主体との関係において，適切な監督の措置及び執行の措置を講じ得る。

Member States that have received a request for mutual assistance in relation to an entity as referred to in paragraph 1, point (b), may, within the limits of that request, take appropriate supervisory and enforcement measures in relation to the entity concerned that provides services or which has a network and information system on their territory.

第 27 条 法主体の登録

Article 27 **Registry of entities**

1. ENISA は，第 4 項に従って単一連絡部局から受領した情報を基礎として，DNS サービスのプロバイダ，TLD 名レジストリ，ドメイン名登録サービスを提供する法主体，クラウドコンピューティングサービスのプロバイダ，データセンターサービスのプロバイダ，コンテント伝達ネットワークのプロバイダ，マネージドサービスのプロバイダ，マネージドセキュリティサービスのプロバイダ，並びに，オンライン市場のプロバイダ，オンライン検索エンジンのプロバイダ及びソーシャルネットワーキングサービスプラットフォームのプロバイダの登録所を創設し，かつ，維持管理する。要求に応じて，ENISA は，職務権限のある機関に対し，それが適用されるときは情報の機密性が保護されることを確保しつつ，当該登録所へのアクセスを認める。

ENISA shall create and maintain a registry of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, on the basis of the information received from the single points of contact in accordance with paragraph 4. Upon request, ENISA shall allow the competent authorities access to that registry, while ensuring that the confidentiality of information is protected where applicable.

2. 構成国は，第 1 項に示す法主体に対し，2025 年 1 月 17 日までに，職務権限のある機関に対して以下の情報を提出することを要求する：
   (a) その法主体の名称:
   (b) それが適用可能なときは，別紙Iまたは別紙IIに示す関連する部門，副部門及び法主体のタイプ；
   (c) その法主体の主たる拠点の住所及びその法主体の主たる拠点以外の欧州連合内における適法な拠点の住所，または，欧州連合内に拠点をもたないときは，第 26 条第 3 項により指定されたその法主体の代理者の住所;
   (d) その法主体の，及び，それが適用可能なときは，第 26 条第 3 項により指定されたその法主体の代理者の，電子メールアドレスと電話番号を含め，最新の連絡先，；
   (e) その法主体がサービスを提供する構成国;並びに
   (f) その法主体の IP アドレス範囲。

Member States shall require entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025:
   (a) the name of the entity;
   (b) the relevant sector, subsector and type of entity referred to in Annex I or II, where applicable;
   (c) the address of the entity's main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 26(3);
   (d) up-to-date contact details, including email addresses and telephone numbers of the entity and,

where applicable, its representative designated pursuant to Article 26(3);
(e) the Member States where the entity provides services; and
(f) the entity's IP ranges.

3. 構成国は，第 1 項に示す法主体が，職務権限のある機関に対し，第 2 項に基づいて当該法主体が提出した情報の変更に関し，遅滞なく，かつ，いかなる場合においてもその変更の日から 3 か月以内に，通知することを確保する。

Member States shall ensure that the entities referred to in paragraph 1 notify the competent authority about any changes to the information they submitted under paragraph 2 without delay and in any event within three months of the date of the change.

4. 第 2 項及び第 3 項に示す情報を受領した後，第 2 項(f)に示す情報を除き，関係する構成国の単一連絡部局は，不適切な遅滞なく，その情報を ENISA に対して転送する。

Upon receipt of the information referred to in paragraphs 2 and 3, except for that referred to in paragraph 2, point (f), the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA.

5. それが適用可能なときは，本条の第 2 項及び第 3 項に示す情報は，第 3 条第 4 項第 4 副項に示す国内の仕組みを介して提出される。

Where applicable, the information referred to in paragraphs 2 and 3 of this Article shall be submitted through the national mechanism referred to in Article 3(4), fourth subparagraph.

第 28 条 ドメイン名登録データのデータベース

Article 28 **Database of domain name registration data**

1. DNS の防護，安定性及び回復力に貢献する目的のために，構成国は，TLD 名レジストリ及びドメイン名登録サービスを提供する法主体に対し，個人データであるデータと関連する欧州連合のデータ保護法に従ったデューディリジェンスをもって，専用データベース内で，正確かつ完全なドメイン名登録データを収集及び維持管理することを要求する。

For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall require TLD name registries and entities providing domain name registration services to collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence in accordance with Union data protection law as regards data which are personal data.

2. 第 1 項の目的のために，構成国は，ドメイン名登録データのデータベースが，そのドメイン名の

保有者及び TLD の下でドメイン名を管理する接点者を特定し，連絡をとるために必要な情報を収録すべきことを要求する。そのような情報は，以下の情報を含める:

(a) ドメイン名；
(b) 登録の日；
(c) 登録者名，連絡先電子メールアドレス及び電話番号;
(d) ドメイン名を管理する接点者の連絡先電子メールアドレス及び電話番号が登録者の連絡先電子メールアドレス及び電話番号と異なる場合においては，ドメイン名を管理する接点者の連絡先電子メールアドレス及び電話番号。

For the purposes of paragraph 1, Member States shall require the database of domain name registration data to contain the necessary information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs. Such information shall include:

(a) the domain name;
(b) the date of registration;
(c) the registrant's name, contact email address and telephone number;
(d) the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.

3. 構成国は，第 1 項に示すデータベースが正確かつ完全な情報を収録することを確保するため，TLD 名レジストリ及びドメイン名登録サービスを提供する法主体に対し，検証手順を含め，基本方針及び手順を設けることを要求する。構成国は，そのような基本方針及び手順が公表されることを要求する。

Member States shall require the TLD name registries and the entities providing domain name registration services to have policies and procedures, including verification procedures, in place to ensure that the databases referred to in paragraph 1 include accurate and complete information. Member States shall require such policies and procedures to be made publicly available.

4. 構成国は，TLD 名レジストリ及びドメイン名登録サービスを提供する法主体に対し，ドメイン名の登録の後不適正な遅滞なく，個人データではないドメイン名登録データが公表されることを要求する。

Member States shall require the TLD name registries and the entities providing domain name registration services to make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data.

5. 構成国は，TLD 名レジストリ及びドメイン名登録サービスを提供する法主体に対し，欧州連合のデータ保護法に従い，正当なアクセスを求める者からの適法かつ適正に根拠づけられた要求に基づいて，特定のドメイン名登録データへのアクセスを提供することを要求する。構成国は，TLD 名レジストリ及びドメイン名登録サービスを提供する法主体に対し，不適切な遅滞なく，かつ，い

かなる場合においてもアクセスを求める要求を受けた時から 72 時間以内に，回答することを要求する。構成国は，そのようなデータの開示と関連する基本方針及び手順が公表されることを要求する。

Member States shall require the TLD name registries and the entities providing domain name registration services to provide access to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers, in accordance with Union data protection law. Member States shall require the TLD name registries and the entities providing domain name registration services to reply without undue delay and in any event within 72 hours of receipt of any requests for access. Member States shall require policies and procedures with regard to the disclosure of such data to be made publicly available.

6. 第 1 項ないし第 5 項に定める義務の遵守は，ドメイン名登録データを収集することの重複をもたらしてはならない。その目的のために，構成国は，TLD 名レジストリ及びドメイン名登録サービスを提供する法主体に対し，相互に協力することを要求する。

Compliance with the obligations laid down in paragraphs 1 to 5 shall not result in a duplication of collecting domain name registration data. To that end, Member States shall require TLD name registries and entities providing domain name registration services to cooperate with each other.

第VI章 情報共有
Chapter VI **Information Sharing**

第 29 条 サイバーセキュリティ情報共有覚書
Article 29 Cybersecurity information-sharing arrangements

1. 構成国は，そのような情報の共有が：
   (a) インシデントの防止，検出，インシデントへの対応またはインシデントからの復旧またはインシデントの影響の緩和を狙いとし；
   (b) とりわけ，サイバーな脅威，そのような脅威が拡散する能力の制限または阻止，幅広い防衛能力の支援，脆弱性の解消と開示，脅威の検出，封じ込めと防止の技法，緩和の戦略，または，対応と復旧の段階，または，公的法主体と民間法主体との間のサイバーな脅威の共働的な調査研究の促進と関係する認識向上を介して，サイバーセキュリティのレベルを拡大する；

   場合には，この指令の適用範囲内にある法主体，及び，それが関連するときは，それ以外の，この指令の適用範囲内にはない法主体が，サイバーな脅威，ニアミス，脆弱性，技法と手順，侵害指標，敵対的戦術，脅威行為者特定情報，サイバーセキュリティ警報，及び，サイバー攻撃を検出するためのサイバーセキュリティツールの設定に関する推奨事項と関連する情報を含め，関連するサイバーセキュリティの情報を，それらの法主体間において，任意ベースで交換できることを確保する。

   Member States shall ensure that entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive are able to exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks, where such information sharing:
   (a) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;
   (b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities.

2. 構成国は，基礎法主体及び重要法主体のコミュニティ，並びに，それが関連するときは，当該法主体の供給者またはサービスプロバイダの間において，情報の交換が行われることを確保する。そのような交換は，交換される潜在的に機微な性質の情報と関係するサイバーセキュリティ情報共有覚書を介して実装される。

Member States shall ensure that the exchange of information takes place within communities of essential and important entities, and where relevant, their suppliers or service providers. Such exchange shall be implemented through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared.

3. 構成国は，本条の第 2 項に示すサイバーセキュリティ情報共有覚書の策定を促進する。そのような覚書は，専用の ICT プラットフォームと自動化ツールの利用，情報共有覚書の内容と条件を含め，業務運営上の諸要素を定め得る。そのような覚書への行政機関の関与の詳細を定める際，構成国は，職務権限のある機関または CSIRT によって利用される情報に関して条件を加え得る。構成国は，第 7 条第 2 項(h)に示すその構成国の基本方針に従い，そのような覚書の適用に関する補助を提供する。

Member States shall facilitate the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 of this Article. Such arrangements may specify operational elements, including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements. In laying down the details of the involvement of public authorities in such arrangements, Member States may impose conditions on the information made available by the competent authorities or the CSIRTs. Member States shall offer assistance for the application of such arrangements in accordance with their policies referred to in Article 7(2), point (h).

4. 構成国は，基礎法主体及び重要法主体が，第 2 項に示すサイバーセキュリティ情報共有覚書への当該法主体の参加をそのような覚書への加入後に，または，そうであるときは，そのような覚書からの当該法主体の離脱をその離脱が有効となった後に，職務権限のある機関に対して通知することを確保する。

Member States shall ensure that essential and important entities notify the competent authorities of their participation in the cybersecurity information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.

5. ENISA は，ベストプラクティスを交換すること及びガイドを提供することにより，第 2 項に示すサイバーセキュリティ情報共有覚書の策定に関し，補助を提供する。

ENISA shall provide assistance for the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by exchanging best practices and providing guidance.

第 30 条 関連情報の任意の通知

Article 30 **Voluntary notification of relevant information**

1. 構成国は，第 23 条に定める通知義務に加え，CSIRT に対し，または，それが適用可能なときは，職務権限のある機関に対し，任意に：
   (a) 基礎法主体及び重要法主体から，インシデント，サイバーな脅威及びニアミスに関し；
   (b) その法主体がこの指令の適用範囲内にあるかどうかに拘わらず，(a)に示す法主体以外の法主体から，重大なインシデント，サイバーな脅威及びニアミスに関し；
   通知が提出され得ることを確保する。

   Member States shall ensure that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis, by:
   (a) essential and important entities with regard to incidents, cyber threats and near misses;
   (b) entities other than those referred to in point (a), regardless of whether they fall within the scope of this Directive, with regard to significant incidents, cyber threats and near misses.

2. 構成国は，第 23 条に定める手続に従い，本条の第 1 項に示す通知を処理する。構成国は，任意の通知よりも義務的な通知の処理を優先させ得る。

   Member States shall process the notifications referred to in paragraph 1 of this Article in accordance with the procedure laid down in Article 23. Member States may prioritise the processing of mandatory notifications over voluntary notifications.

   それが必要なときは，CSIRT，及び，それが適用可能なときは，職務権限のある機関は，単一連絡部局に対し，通知元法主体から提供された情報の機密性及び適切な保護を確保しつつ，本条により受領した通知に関する情報を提供する。犯罪行為の防止，捜査，検知及び訴追を妨げることなく，任意の報告は，通知元法主体に対し，その法主体がその通知を提出しなかったとすれば服することがなかったような付加的な義務を強制することになってはならない。

   Where necessary, the CSIRTs and, where applicable, the competent authorities shall provide the single points of contact with the information about notifications received pursuant to this Article, while ensuring the confidentiality and appropriate protection of the information provided by the notifying entity. Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the notifying entity to which it would not have been subject had it not submitted the notification.

第Ⅶ章 監督及び執行
Chapter **VII Supervision and Enforcement**

第 31 条 監督及び執行の一般的な側面
Article 31 **General aspects concerning supervision and enforcement**

1. 構成国は，その構成国の職務権限のある機関が実効的に監督し，かつ，この指令の遵守を確保するために必要となる措置を講ずることを確保する。

   Member States shall ensure that their competent authorities effectively supervise and take the measures necessary to ensure compliance with this Directive.

2. 構成国は，その構成国の職務権限のある機関が，監督の職務の優先順序を決めることを認め得る。そのような優先順序の決定は，リスクベースのアプローチを基礎とする。その目的のために，第 32 条及び第 33 条に定める当該職務権限のある機関の監督の職務を執行する際，その職務権限のある機関は，リスクベースのアプローチに従ってそのような職務の優先順序を決めるための監督手法を定め得る。

   Member States may allow their competent authorities to prioritise supervisory tasks. Such prioritisation shall be based on a risk-based approach. To that end, when exercising their supervisory tasks provided for in Articles 32 and 33, the competent authorities may establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach.

3. 職務権限のある機関は，個人データの侵害を帰結するインシデントに対処する場合，規則(EU) 2016/679 の下にある監督機関の職務権限及び職務を妨げることなく，同規則の下にある監督機関と緊密に協力して，作業する。

   The competent authorities shall work in close cooperation with supervisory authorities under Regulation (EU) 2016/679 when addressing incidents resulting in personal data breaches, without prejudice to the competence and tasks of the supervisory authorities under that Regulation.

4. 国内立法上及び国内組織上の枠組みを妨げることなく，構成国は，行政機関である法主体によるこの指令の遵守の監督において，及び，この指令の違反行為と関連して執行の措置の実施において，職務権限のある機関が，監督を受ける行政機関である法主体それぞれとの間において業務遂行上の独立性をもつそのような職務を遂行するための適切な権限をもつことを確保する。構成国は，国内立法上及び国内組織上の枠組みに従い，当該行政機関である法主体との関係において，適切であり，比例的かつ実効的な監督の措置及び執行の措置の実施に関して定め得る。

   Without prejudice to national legislative and institutional frameworks, Member States shall ensure that,

in the supervision of compliance of public administration entities with this Directive and the imposition of enforcement measures with regard to infringements of this Directive, the competent authorities have appropriate powers to carry out such tasks with operational independence vis-à-vis the public administration entities supervised. Member States may decide on the imposition of appropriate, proportionate and effective supervisory and enforcement measures in relation to those entities in accordance with the national legislative and institutional frameworks.

第 32 条　基礎法主体と関係する監督の措置及び執行の措置

Article 32 **Supervisory and enforcement measures in relation to essential entities**

1. 構成国は，この指令に定める義務と関係して基礎法主体に対して実施される監督の措置または執行の措置が，個々の個別案件の状況を考慮に入れた上で，実効的であり，比例的であり，かつ，抑止力があることを確保する。

Member States shall ensure that the supervisory or enforcement measures imposed on essential entities in respect of the obligations laid down in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. 構成国は，職務権限のある機関が，基礎法主体との関係において当該職務権限のある機関の監督の職務を執行する際，当該法主体を少なくとも以下の措置に服させる権限をもつことを確保する：
   (a) 訓練を受けた専門家によって実施される無作為抽出検査を含め，施設内における点検及び施設外の監督；
   (b) 独立の組織または職務権限のある機関によって遂行される定期的かつ的を絞ったセキュリティ監査；
   (c) 重大なインシデントまたは基礎法主体によるこの指令の違反行為を根拠として正当化される場合を含め，アドホックな監査；
   (d) それが必要なときは関係する法主体の協力を受け，客観的であり，非差別であり，公正かつ透明性のあるリスク評価基準を基礎とするセキュリティ検査；
   (e) 文書化されたサイバーセキュリティ基本方針を含め，関係する法主体によって採用されたサイバーセキュリティのリスク管理の措置を評価し，並びに，第 27 条により職務権限のある機関に対して情報を提出すべき義務の遵守を評価するために必要となる情報を求める要求；
   (f) 当該職務権限のある機関の監督の職務を遂行するために必要となるデータ，文書及び情報へのアクセスの要求；
   (g) 適格な監査者によって遂行されたセキュリティ監査結果及びそれを支えるそれぞれの証跡のような，サイバーセキュリティの基本方針の実装の証拠を求める要求。

Member States shall ensure that the competent authorities, when exercising their supervisory tasks in

relation to essential entities, have the power to subject those entities at least to:

(a) on-site inspections and off-site supervision, including random checks conducted by trained professionals;
(b) regular and targeted security audits carried out by an independent body or a competent authority;
(c) ad hoc audits, including where justified on the ground of a significant incident or an infringement of this Directive by the essential entity;
(d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned;
(e) requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;
(f) requests to access data, documents and information necessary to carry out their supervisory tasks;
(g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

第 1 副項(b)に示す的を絞ったセキュリティ監査は，職務権限のある機関もしくは被監査法主体によって実施されたリスク評価，または，それ以外の，リスクと関連する利用可能な情報を基礎とする。

The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.

的を絞ったセキュリティ監査の結果は，職務権限のある機関が利用できるようにされる。独立の組織によって遂行されたそのような的を絞ったセキュリティ監査の費用は，職務権限のある機関が別異に決定する適正に根拠づけられる場合を除き，被監査法主体から支払われる。

The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the competent authority decides otherwise.

3. 第 2 項(e), (f)または(g)に基づく当該職務権限のある機関の権限を行使するときは，その職務権限のある機関は，その要求の目的を述べ，かつ，要求される情報を特定する。

When exercising their powers under paragraph 2, point (e), (f) or (g), the competent authorities shall state the purpose of the request and specify the information requested.

4. 構成国は，その構成国の職務権限のある機関が，基礎法主体との関係において当該職務権限のある機関の執行の権限を行使する際，少なくとも以下の権限をもつことを確保する：

(a) 関係する法主体によるこの指令の違反行為に関する警告を発する権限；
(b) インシデントを防止または解消するために必要となる措置，並びに，そのような措置を実装

するための期限及び当該措置の実装を報告するための期限と関連する指示を含め，拘束力のある指示を採択する権限，または，関係する法主体に対し，発見された欠点もしくはこの指令の違反行為を解消することを要求する命令を採択する権限；

(c) 関係する法主体に対し，この指令に違反する行為をやめ，かつ，当該行為を繰り返すことをやめることを命ずる権限；

(d) 関係する法主体に対し，当該法主体のサイバーセキュリティのリスク管理の措置が第 21 条を遵守することを確保することを命ずる権限，または，定められた態様で，かつ，定められた期限内に，第 23 条に定める報告義務を満たすことを命ずる権限；

(e) 関係する法主体に対し，当該法主体が重大なサイバーな脅威によって潜在的に影響を受けているサービスを提供しまたは活動を遂行したことと関係する自然人または法人に対して，その脅威の性質について，並びに，当該脅威に対応して当該自然人または法人によってとられ得る可能な防護措置または解消措置について連絡することを命ずる権限；

(f) 関係する法主体に対し，セキュリティ監査の結果として提供された推奨事項を合理的な期限内に実装することを命ずる権限；

(g) 関係する法主体による第 21 条及び第 23 条の遵守を監督するための，定められた期間内の明確に定義された職務をもつ監視担当官を任命する権限；

(h) 関係する法主体に対し，定められた態様でこの指令の違反行為の様相を公表することを命ずる権限；

(i) 本項の(a)ないし(h)に示すいずれかの措置に付加して，第 34 条による行政上の制裁金を科す権限，または，国内法に従い，関連する組織，裁判所または法廷がそれを科すことを要請する権限。

Member States shall ensure that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to:

(a) issue warnings about infringements of this Directive by the entities concerned;

(b) adopt binding instructions, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation, or an order requiring the entities concerned to remedy the deficiencies identified or the infringements of this Directive;

(c) order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct;

(d) order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period;

(e) order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat;

(f) order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;

(g) designate a monitoring officer with well-defined tasks for a determined period of time to oversee the compliance of the entities concerned with Articles 21 and 23;
(h) order the entities concerned to make public aspects of infringements of this Directive in a specified manner;
(i) impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (h) of this paragraph.

5. 第 4 項(a)ないし(d)及び(f)により採択された執行の措置が実効的ではないときは，構成国は，その構成国の職務権限のある機関が，欠点を解消しまたは当該職務権限のある機関の要求を遵守するために必要となる活動を行うことをその基礎法主体が要求される期限を定める権限をもつことを確保する。定められた期限内に要求された活動が行われなかったときは，構成国は，当該構成国の職務権限のある機関が，以下の権限をもつことを確保する：
(a) 国内法に従い，その基礎法主体によって提供される関連サービスもしくはその基礎法主体によって遂行される活動の全部もしくは一部に関する認証もしくは認可を一時的に停止し，または，認証もしくは認可の組織もしくは裁判所もしくは法廷に対し，その一時的な停止を要求する権限；
(b) 国内法に従い，関連する組織もしくは裁判所もしくは法廷に対し，その基礎法主体における最高執行責任者または法律上の代理者のレベルで経営上の責任を負う自然人による当該法主体内の経営上の権能の行使の一時的な禁止を要求する権限。

Where enforcement measures adopted pursuant to paragraph 4, points (a) to (d) and (f), are ineffective, Member States shall ensure that their competent authorities have the power to establish a deadline by which the essential entity is requested to take the necessary action to remedy the deficiencies or to comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that their competent authorities have the power to:
(a) suspend temporarily, or request a certification or authorisation body, or a court or tribunal, in accordance with national law, to suspend temporarily a certification or authorisation concerning part or all of the relevant services provided or activities carried out by the essential entity;
(b) request that the relevant bodies, courts or tribunals, in accordance with national law, prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level in the essential entity from exercising managerial functions in that entity.

本項により課される一時的な停止または禁止は，関係する法主体が，その欠点を解消するために必要となる活動を行うまで，または，それを求めてそのような執行の措置が適用された，その職務権限のある機関の要求を遵守するに必要となる活動を行うまでに限り，適用される。そのような一時的な停止または禁止を課すことは，実効的な救済及び公正な裁判の権利，無罪の推定並びに防御の権利を含め，欧州連合法及び憲章の基本原則に従った適切な手続上の安全確保に服する。

Temporary suspensions or prohibitions imposed pursuant to this paragraph shall be applied only until the entity concerned takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such enforcement measures were applied. The imposition of such temporary suspensions or prohibitions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.

本項に定める執行の措置は，この指令に服する行政機関である法主体に対して適用してはならない。

The enforcement measures provided for in this paragraph shall not be applicable to public administration entities that are subject to this Directive.

6. 構成国は，基礎法主体を代理するための権限，その基礎法主体の代わりに判断を行う権限，または，その基礎法主体の管理を実施する権限に基づいて，その基礎法主体に対して法律上の代理者の職責を負い，または，法律上の代理者として活動する自然人が，その代理者のこの指令の遵守を確保するための権限をもつことを確保する。構成国は，この指令の遵守を確保するためのその自然人の義務の違反について当該自然人が法的責任を負うことができることを確保する。

Member States shall ensure that any natural person responsible for or acting as a legal representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the power to ensure its compliance with this Directive. Member States shall ensure that it is possible to hold such natural persons liable for breach of their duties to ensure compliance with this Directive.

行政機関である法主体に関しては，本項は，公務員及び選任または任命された官吏の法的責任と関連する国内法を妨げてはならない。

As regards public administration entities, this paragraph shall be without prejudice to national law as regards the liability of public servants and elected or appointed officials.

7. 第 4 項または第 5 項に示すいずれかの執行の措置を講ずるときは，職務権限のある機関は，防御の権利を尊重し，かつ，個々の個別案件の状況を考慮に入れ，かつ，ミニマムのものとして，以下のことを適正に考慮に入れる：
   (a) 就中，いかなる場合においても，以下の重大な違反行為を組成する，違反行為の重大性及び違反のあった条項の重要性：
      (i) 反復された違反；
      (ii) 重大なインシデントの通知または解消をしないこと；
      (iii) 職務権限のある機関からの拘束力のある指示の後に欠点の解消をしないこと；
      (iv) 違反行為の判定の後に職務権限のある機関から命ぜられた監査活動または監視活

動の妨害;
(v) 第 21 条及び第 23 条に定めるサイバーセキュリティのリスク管理の措置または報告義務との関係における虚偽情報または著しく不正確な情報の提供;
(b) 違反行為の持続期間;
(c) 関係する法主体による関連する既往の違反行為;
(d) 金銭的または経済的な損失を含め，発生した有形または無形の損害，他のサービスに対する影響及び影響を受けた利用者の数;
(e) その違反行為の加害者の側における意図または過失;
(f) 有形または無形の損害の防止または緩和のためにその法主体によってとられた措置;
(g) 承認された行動準則または承認された認証の仕組みの準拠;
(h) 責任を負う自然人または法人の，職務権限のある機関との協力のレベル。

When taking any of the enforcement measures referred to in paragraph 4 or 5, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of:
(a) the seriousness of the infringement and the importance of the provisions breached, the following, inter alia, constituting serious infringement in any event:
(i) repeated violations;
(ii) a failure to notify or remedy significant incidents;
(iii) a failure to remedy deficiencies following binding instructions from competent authorities;
(iv) the obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement;
(v) providing false or grossly inaccurate information in relation to cybersecurity risk-management measures or reporting obligations laid down in Articles 21 and 23;
(b) the duration of the infringement;
(c) any relevant previous infringements by the entity concerned;
(d) any material or non-material damage caused, including any financial or economic loss, effects on other services and the number of users affected;
(e) any intent or negligence on the part of the perpetrator of the infringement;
(f) any measures taken by the entity to prevent or mitigate the material or non-material damage;
(g) any adherence to approved codes of conduct or approved certification mechanisms;
(h) the level of cooperation of the natural or legal persons held responsible with the competent authorities.

8. 職務権限のある機関は，当該職務権限のある機関の執行の措置の詳細な理由を示す。そのような措置を採択する前に，職務権限のある機関は，関係する法主体に対し，当該職務権限のある機関の仮判定を通知する。そうしなければインシデントの防止またはインシデントに対する対応のための即時の活動が妨げられるような適正に根拠づけられる場合を除き，当該職務権限のある機関は，当該法主体に対し，意見書を提出するための合理的な期間を認めることもできる。

The competent authorities shall set out a detailed reasoning for their enforcement measures. Before adopting such measures, the competent authorities shall notify the entities concerned of their preliminary findings. They shall also allow a reasonable time for those entities to submit observations, except in duly substantiated cases where immediate action to prevent or respond to incidents would otherwise be impeded.

9. 構成国は，この指令の下にあるその構成国の職務権限のある機関が，指令(EU) 2022/2557 の下において必須法主体として識別された法主体によるこの指令の遵守を確保することを狙いとする当該職務権限のある機関の監督の権限及び執行の権限を行使するときは，指令(EU) 2022/2557 の下にある同じ構成国内の関連する職務権限のある機関に対して連絡することを確保する。それが適切なときは，指令(EU) 2022/2557 の下にある職務権限のある機関は，この指令の下にあるその職務権限のある機関に対し，当該職務権限のある機関の監督の権限及び執行の権限を，指令(EU) 2022/2557 の下において必須法主体として識別された法主体との関係において行使することを要請できる。

Member States shall ensure that their competent authorities under this Directive inform the relevant competent authorities within the same Member State under Directive (EU) 2022/2557 when exercising their supervisory and enforcement powers aiming to ensure compliance of an entity identified as a critical entity under Directive (EU) 2022/2557 with this Directive. Where appropriate, the competent authorities under Directive (EU) 2022/2557 may request the competent authorities under this Directive to exercise their supervisory and enforcement powers in relation to an entity that is identified as a critical entity under Directive (EU) 2022/2557.

10. 構成国は，この指令の下にあるその構成国の職務権限のある機関が，規則(EU) 2022/2554 の下にある関係する構成国の関連する職務権限のある機関と協力することを確保する。とりわけ，構成国は，この指令の下にある当該構成国の職務権限のある機関が，規則(EU) 2022/2554 の第 31 条により重要 ICT の第三者サービスプロバイダとして指定されている基礎法主体によるこの指令の遵守を確保することを狙いとする当該職務権限のある機関の監督の権限及び執行の権限を行使するときは，規則(EU) 2022/2554 の第 32 条第 1 項により設置された監視フォーラムに対して連絡することを確保する。

Member States shall ensure that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554. In particular, Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554. with this Directive.

第 33 条　重要法主体と関係する監督の措置及び執行の措置

Article 33 **Supervisory and enforcement measures in relation to important entities**

1. 重要法主体が，この指令，とりわけ，この指令の第 21 条及び第 23 条を遵守していないと主張する証跡，兆候または情報が提供されたときは，構成国は，職務権限のある機関が，それが必要なときは，事後の監督の措置を通じて，行動をとることを確保する。構成国は，個々の個別案件の状況を考慮に入れた上で，当該措置が，実効的であり，比例的であり，かつ，抑止力があることを確保する。

When provided with evidence, indication or information that an important entity allegedly does not comply with this Directive, in particular Articles 21 and 23 thereof, Member States shall ensure that the competent authorities take action, where necessary, through *ex post* supervisory measures. Member States shall ensure that those measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. 構成国は，職務権限のある機関が，重要法主体との関係において当該職務権限のある機関の監督の職務を執行する際，当該法主体を少なくとも以下の措置に服させる権限をもつことを確保する：
   (a) 訓練を受けた専門家によって実施される施設内における点検及び施設外の事後監督；
   (b) 独立の組織または職務権限のある機関によって遂行される的を絞ったセキュリティ監査；
   (c) それが必要なときは関係する法主体の協力を受け，客観的であり，非差別であり，公正かつ透明性のあるリスク評価基準を基礎とするセキュリティ検査；
   (d) 文書化されたサイバーセキュリティ基本方針を含め，関係する法主体によって採用されたサイバーセキュリティのリスク管理の措置を事後的に評価し，並びに，第 27 条により職務権限のある機関に対して情報を提出すべき義務の遵守を事後的に評価するために必要となる情報を求める要求；
   (e) 当該職務権限のある機関の監督の職務を遂行するために必要となるデータ，文書及び情報へのアクセスの要求；
   (f) 適格な監査者によって遂行されたセキュリティ監査結果及びそれを支えるそれぞれの証跡のような，サイバーセキュリティの基本方針の実装の証拠を求める要求。

Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to:
   (a) on-site inspections and off-site *ex post* supervision conducted by trained professionals;
   (b) targeted security audits carried out by an independent body or a competent authority;
   (c) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned;
   (d) requests for information necessary to assess, *ex post*, the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to

Article 27;

(e) requests to access data, documents and information necessary to carry out their supervisory tasks;

(f) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

第 1 副項(b)に示す的を絞ったセキュリティ監査は，職務権限のある機関もしくは被監査法主体によって実施されたリスク評価，または，それ以外の，リスクと関連する利用可能な情報を基礎とする。

The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.

的を絞ったセキュリティ監査の結果は，職務権限のある機関が利用できるようにされる。独立の組織によって遂行されたそのような的を絞ったセキュリティ監査の費用は，職務権限のある機関が別異に決定する適正に根拠づけられる場合を除き，被監査法主体から支払われる。

The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the competent authority decides otherwise.

3. 第 2 項(d), (e)または(f)に基づく当該職務権限のある機関の権限を行使するときは，その職務権限のある機関は，その要求の目的を述べ，かつ，要求される情報を特定する。

When exercising their powers under paragraph 2, point (d), (e) or (f), the competent authorities shall state the purpose of the request and specify the information requested.

4. 構成国は，その職務権限のある機関が，重要法主体との関係において当該職務権限のある機関の執行の権限を行使する際，少なくとも以下の権限をもつことを確保する：

(a) 関係する法主体によるこの指令の違反行為に関する警告を発する権限；

(b) 関係する法主体に対し，発見された欠点またはこの指令の違反行為を解消することを要求する拘束力のある指示または命令を採択する権限；

(c) 関係する法主体に対し，この指令に違反する行為をやめ，かつ，当該行為を繰り返すことをやめることを命ずる権限；

(d) 関係する法主体に対し，当該法主体のサイバーセキュリティのリスク管理の措置が第 21 条を遵守することを確保することを命ずる権限，または，定められた態様で，かつ，定められた期限内に，第 23 条に定める報告義務を満たすことを命ずる権限；

(e) 関係する法主体に対し，当該法主体が重大なサイバーな脅威によって潜在的に影響を受けているサービスを提供しまたは活動を遂行したことと関係する自然人または法人に対して，その脅威の性質について，並びに，当該脅威に対応して当該自然人または法人によってとられ得る可能な防護措置または解消措置について連絡することを命ずる権限；

(f) 関係する法主体に対し，セキュリティ監査の結果として提供された推奨事項を合理的な期限内に実装することを命ずる権限；
(g) 関係する法主体に対し，定められた態様でこの指令の違反行為の様相を公表することを命ずる権限；
(h) 本項の(a)ないし(g)に示すいずれかの措置に付加して，第 34 条による行政上の制裁金を科す権限，または，国内法に従い，関連する組織，裁判所または法廷がそれを科すことを要請する権限。

Member States shall ensure that the competent authorities, when exercising their enforcement powers in relation to important entities, have the power at least to:
(a) issue warnings about infringements of this Directive by the entities concerned;
(b) adopt binding instructions or an order requiring the entities concerned to remedy the deficiencies identified or the infringement of this Directive;
(c) order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct;
(d) order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period;
(e) order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat;
(f) order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;
(g) order the entities concerned to make public aspects of infringements of this Directive in a specified manner;
(h) impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (g) of this paragraph.

5. 第 32 条第 6 項，第 7 項及び第 8 項は，重要法主体に関して本条に定める監督の措置及び執行の措置に準用して適用される。

Article 32(6), (7) and (8) shall apply *mutatis mutandis* to the supervisory and enforcement measures provided for in this Article for important entities.

6. 構成国は，この指令の下にあるその構成国の職務権限のある機関が，規則(EU) 2022/2554 の下にある関係する構成国の関連する職務権限のある機関と協力することを確保する。とりわけ，構成国は，この指令の下にある当該構成国の職務権限のある機関が，規則(EU) 2022/2554 の第 31 条により重要 ICT の第三者サービスプロバイダとして指定されている重要法主体によるこの指令

の遵守を確保することを狙いとする当該職務権限のある機関の監督の権限及び執行の権限を行使するときは，規則(EU) 2022/2554 の第 32 条第 1 項により設置された監視フォーラムに対して連絡することを確保する。

Member States shall ensure that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554. In particular, Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an important entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554. with this Directive.

第 34 条　基礎法主体及び重要法主体に対して行政上の制裁金を科すための一般的な条件

Article 34 **General conditions for imposing administrative fines on essential and important entities**

1. 構成国は，この指令の違反行為と関係して本条により基礎法主体及び重要法主体に対して科される行政上の制裁金が，個々の個別案件の状況を考慮に入れた上で，実効的で，比例的かつ抑止力があることを確保する。

   Member States shall ensure that the administrative fines imposed on essential and important entities pursuant to this Article in respect of infringements of this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. 行政上の制裁金は，第 32 条第 4 項(a)ないし(h)，第 32 条第 5 項及び第 33 条第 4 項(a)ないし(g)に示すいずれかの措置に付加して科される。

   Administrative fines shall be imposed in addition to any of the measures referred to in Article 32(4), points (a) to (h), Article 32(5) and Article 33(4), points (a) to (g).

3. 行政上の制裁金を科すかどうかを決定する際，及び，個々の個別案件におけるその行政上の制裁金の額を決定する際，ミニマムのものとして，第 32 条第 7 項に定める諸要素を適切に考慮に入れる。

   When deciding whether to impose an administrative fine and deciding on its amount in each individual case, due regard shall be given, as a minimum, to the elements provided for in Article 32(7).

4. 構成国は，当該法主体が第 21 条または第 23 条に違反するときは，基礎法主体が，本条の第 2 項及び第 3 項に従い，少なくとも上限を 1000 万ユーロとする額，または，少なくとも上限をその基礎法主体が属する事業者の前年における全世界の年次総売上の 2%とする額のいずれか高額

の方の行政上の制裁金に服することを確保する。

Member States shall ensure that where they infringe Article 21 or 23, essential entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 10 000 000 or of a maximum of at least 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.

5. 構成国は，当該法主体が第 21 条または第 23 条に違反するときは，重要法主体が，本条の第 2 項及び第 3 項に従い，少なくとも上限を 700 万ユーロとする額，または，少なくとも上限をその重要主体が属する事業者の前年における全世界の年次総売上の 1.4%とする額のいずれか高額の方の行政上の制裁金に服することを確保する。

Member States shall ensure that where they infringe Article 21 or 23, important entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 7 000 000 or of a maximum of at least 1,4 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher.

6. 構成国は，基礎法主体または重要法主体に対して，職務権限のある機関の事前の決定に従ってこの指令の違反行為をやめることを強制するため，定期制裁金を科す権限を定め得る。

Member States may provide for the power to impose periodic penalty payments in order to compel an essential or important entity to cease an infringement of this Directive in accordance with a prior decision of the competent authority.

7. 第 32 条及び第 33 項による職務権限のある機関の権限を妨げることなく，各構成国は，行政機関である法主体に対して行政上の制裁金を科し得るか否か，及び，どの範囲で科し得るかに関する規定を定め得る。

Without prejudice to the powers of the competent authorities pursuant to Articles 32 and 33, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public administration entities.

8. 構成国の法制度が行政上の制裁金を定めていないときは，当該構成国は，当該法律上の是正策が実効的であり，かつ，職務権限のある機関によって行政上の制裁金が科されるのと均等な効果をもつことを確保しつつ，職務権限のある機関によってその手続が開始され，かつ，職務権限のある国内裁判所もしくは法廷によって制裁金が科されるというような態様で，本条が適用されることを確保する。いかなる場合においても，科される制裁金は，実効的で，比例的かつ抑止力のあるものとする。構成国は，欧州委員会に対し，2024 年 10 月 17 日までに，本項により構成国が採択する法律の条項を通知し，かつ，遅滞なく，その後の改正法または当該法律に影響を与える改正を通知する。

Where the legal system of a Member State does not provide for administrative fines, that Member State shall ensure that this Article is applied in such a manner that the fine is initiated by the competent authority and imposed by competent national courts or tribunals, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by the competent authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. The Member State shall notify to the Commission the provisions of the laws which it adopts pursuant to this paragraph by 17 October 2024 and, without delay, any subsequent amendment law or amendment affecting them.

第 35 条　個人データの侵害を伴う違反行為

Article 35 Infringements entailing a personal data breach

1. 職務権限のある機関が，監督または執行の過程において，基礎法主体または重要法主体によるこの指令の第 21 条及び第 23 条に定める義務の違反行為が規則(EU) 2016/679 の第 4 条第 12 号に定義する個人データの侵害を伴い得るものであって，同規則の第 33 条により通知されるべきものであることに気づいたときは，当該職務権限のある機関は，不適切な遅滞なく，同規則の第 55 条または第 56 条に示す監督機関に対して連絡する。

Where the competent authorities become aware in the course of supervision or enforcement that the infringement by an essential or important entity of the obligations laid down in Articles 21 and 23 of this Directive can entail a personal data breach, as defined in Article 4, point (12), of Regulation (EU) 2016/679 which is to be notified pursuant to Article 33 of that Regulation, they shall, without undue delay, inform the supervisory authorities as referred to in Article 55 or 56 of that Regulation.

2. 規則(EU) 2016/679 の第 55 条または第 56 条に示す監督機関が同規則の第 58 条第 2 項(i)により行政上の制裁金を科すときは，職務権限のある機関は，規則(EU) 2016/679 の第 58 条第 2 項(i)による行政上の制裁金に服する行為と同一の行為から生ずる本条の第 1 項に示す違反行為に対するこの指令の第 34 条による行政上の制裁金を科してはならない。ただし，職務権限のある機関は，この指令の第 32 条第 4 項(a)ないし(h)，第 32 条第 5 項及び第 33 条第 4 項(a)ないし(g)に定める執行の措置を実施し得る。

Where the supervisory authorities as referred to in Article 55 or 56 of Regulation (EU) 2016/679 impose an administrative fine pursuant to Article 58(2), point (i), of that Regulation, the competent authorities shall not impose an administrative fine pursuant to Article 34 of this Directive for an infringement referred to in paragraph 1 of this Article arising from the same conduct as that which was the subject of the administrative fine under Article 58(2), point (i), of Regulation (EU) 2016/679. The competent authorities may, however, impose the enforcement measures provided for in Article 32(4), points (a) to (h), Article 32(5) and Article 33(4), points (a) to (g), of this Directive.

3. 職務権限のある機関の構成国とは別の構成国内に規則(EU) 2016/679 による職務権限のある監

督機関が設けられているときは，職務権限のある機関は，その職務権限のある機関自身の構成国内に設けられている監督機関に対し，第 1 項に示す潜在的な個人データの侵害を連絡する。

Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority shall inform the supervisory authority established in its own Member State of the potential data breach referred to in paragraph 1.

第 36 条 罰則

Article 36 **Penalties**

構成国は，この指令により採択された国内措置の違反行為に対して適用可能な罰に関する規定を定め，かつ，当該規定が実装されることを確保するために必要となる全ての措置を講ずる。定められる罰は，実効的であり，比例的かつ抑止力のあるものとする。構成国は，2025 年 1 月 17 日までに，欧州委員会に対し，当該規定及び当該措置を通知し，かつ，欧州委員会に対し，遅滞なく，当該規定に影響を与えるその後の改正を通知する。

Member States shall lay down rules on penalties applicable to infringements of national measures adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by 17 January 2025, notify the Commission of those rules and of those measures and shall notify it, without delay of any subsequent amendment affecting them.

第 37 条 相互補助

Article 37 **Mutual assistance**

1. 法主体が複数の構成国においてサービスを提供するときは，または，1 もしくは複数の構成国においてサービスを提供し，かつ，その法主体のネットワーク及び情報システムが 1 もしくは複数の別の構成国に所在しているときは，関係する構成国の職務権限のある機関は，協力し，かつ，必要に応じて互いに補助する。当該協力は，少なくとも，以下のことを伴う：
   (a) ある構成国において監督の措置または執行の措置を適用している職務権限のある機関は，単一連絡部局を介して，講じられた監督の措置及び執行の措置に関し，関係する別の構成国の職務権限のある機関に連絡し，かつ，協議する；
   (b) 職務権限のある機関は，別の職務権限のある機関に対し，監督の措置または執行の措置を講ずることを要請できる；
   (c) 職務権限のある機関は，別の職務権限のある機関からの根拠づけられた要請を受領した後，監督の措置または執行の措置が実効的であり，効率的であり，かつ，一貫性のある態様で実装され得るようにするため，他の職務権限のある機関に対し，その機関自身の資源と比例的な相互補助を提供する。

Where an entity provides services in more than one Member State, or provides services in one or more Member States and its network and information systems are located in one or more other Member States, the competent authorities of the Member States concerned shall cooperate with and assist each other as necessary. That cooperation shall entail, at least, that:

(a) the competent authorities applying supervisory or enforcement measures in a Member State shall, via the single point of contact, inform and consult the competent authorities in the other Member States concerned on the supervisory and enforcement measures taken;

(b) a competent authority may request another competent authority to take supervisory or enforcement measures;

(c) a competent authority shall, upon receipt of a substantiated request from another competent authority, provide the other competent authority with mutual assistance proportionate to its own resources so that the supervisory or enforcement measures can be implemented in an effective, efficient and consistent manner.

第 1 副項(c)に示す相互補助は，施設内における点検もしくは施設外の監督または的を絞ったセキュリティ監査を遂行することの要請を含め，情報提供の要請及び監督の措置を包摂し得る。補助の要請の受け手となっている職務権限のある機関は，その職務権限のある機関が，要請を受けた補助を提供するための職務権限をもっていないこと，要請を受けた補助が，職務権限のある機関の監督の職務と比例的ではないこと，または，その要請が，もし開示されもしくは遂行されれば，その構成国の国家安全保障，公共の保安もしくは国防という必須の利益に反するような情報と関係し，もしくは，そのような活動を伴うことが明らかにされない限り，当該要請を拒否してはならない。そのような要請を拒否する前に，職務権限のある機関は，関係する別の職務権限のある機関と協議し，並びに，関係するいずれかの構成国からの要請に応じて，欧州委員会及び ENISA と協議する。

The mutual assistance referred to in the first subparagraph, point (c), may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed shall not refuse that request unless it is established that it does not have the competence to provide the requested assistance, the requested assistance is not proportionate to the supervisory tasks of the competent authority, or the request concerns information or entails activities which, if disclosed or carried out, would be contrary to the essential interests of the Member State's national security, public security or defence. Before refusing such a request, the competent authority shall consult the other competent authorities concerned as well as, upon the request of one of the Member States concerned, the Commission and ENISA.

2. それが適切なときは，かつ，共通の合意により，様々な構成国の職務権限のある機関は，共同で監督活動を遂行できる。

Where appropriate and with common agreement, the competent authorities of various Member States may carry out joint supervisory actions.

第VIII章 委任される行為及び実装行為
Chapter VIII **Delegated and Implementing Acts**

第 38 条 委任の実行
Article 38 **Exercise of the delegation**

1. 委任される行為を採択する権限は，本条に定める条件に従い，欧州委員会に対して与えられる。

   The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. 第 24 条第 2 項に示す委任される行為を採択する権限は，2023 年 1 月 16 日から 5 年間，欧州委員会に対して与えられる。

   The power to adopt delegated acts referred to in Article 24(2) shall be conferred on the Commission for a period of five years from 16 January 2023.

3. 第 24 条第 2 項に示す権限の委任は，いつでも，欧州議会または理事会によって取消され得る。取消しの決定は，同決定の中で指示される権限の委任を終了させる。その決定は，EU 官報上でその決定が公示された翌日に発効し，または，その決定の中で指定された後の日に発効する。その決定は，既に発効している委任される行為の有効性に影響を与えてはならない。

   The delegation of power referred to in Article 24(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. 委任される行為を採択する前に，欧州委員会は，より良い立法に関する 2016 年 4 月 13 日の機関間合意に定める基本原則に従い，各構成国から指定された専門家から意見聴取する。

   Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. 欧州委員会が委任される行為を採択したときは直ちに，欧州委員会は，欧州議会及び理事会に対し，同時に通知する。

   As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European

Parliament and to the Council.

6. 第 24 条第 2 項によって採択された委任される行為は，欧州議会及び理事会に対する当該行為の通知から 2 か月以内に欧州議会もしくは理事会のいずれからも異議が表明されないとき，または，その期間が満了する前に，欧州議会及び理事会の両者が欧州委員会に対して異議を述べない旨を連絡したときに限り発効する。その期間は，欧州議会の発意または理事会の発意により，2 か月まで延長される。

A delegated act adopted pursuant to Article 24(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

第 39 条 委員会の手続

Article 39 Committee procedure

1. 欧州委員会は，委員会による補佐をうける。同委員会は，規則(EU) No 182/2011 の意味における委員会である。

The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. 本項に対する参照があるときは，規則(EU) No 182/2011 の第 5 条が適用される。

Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. 委員会の意見が書面手続によって得られるべき場合において，当該手続は，意見伝達のための期限内に，委員会の議長がそのように決定し，または，委員会の構成員がそのように要請したときは，結論を得ないで結了する。

Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests.

第IX章 最終規定
Chapter IX Final Provisions

第 40 条 見直し
Article 40 **Review**

2027 年 10 月 17 日までに, かつ, その後は 36 か月毎に, 欧州委員会は, この指令の稼働を見直し, かつ, 欧州議会及び理事会に対して報告する。その報告は, とりわけ, 関係する法主体の規模, 別紙 I 及び別紙Ⅱに示す部門, 副部門及び法主体のタイプの, サイバーセキュリティと関係する経済及び社会の稼働にとっての適切性を評価する。その目的のために, そして, 戦略上の協力及び業務運営上の協力を更に発展させるという観点から, 欧州委員会は, 戦略レベル及び業務運営レベルで獲得された経験に関する協力グループ及び CSIRT ネットワークの報告書を考慮に入れる。それが必要なときは, その報告には立法上の提案が添えられる。

By 17 October 2027 and every 36 months thereafter, the Commission shall review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the relevance of the size of the entities concerned, and the sectors, subsectors and types of entity referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. To that end and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. The report shall be accompanied, where necessary, by a legislative proposal.

第 41 条 国内法化
Article 41 **Transposition**

1. 2024 年 10 月 17 日までに, 構成国は, この指令を遵守するために必要となる措置を採択及び公示する。当該構成国は, 欧州委員会に対し, 直ちに, 当該措置を連絡する。

   By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

   当該構成国は, 2024 年 10 月 18 日から当該措置を適用する。

   They shall apply those measures from 18 October 2024.

2. 構成国が第 1 項に示す措置を採択する際, 当該措置は, この指令に対する参照を含めるものとし, または, 当該措置の公示の際にそのような参照を添えるものとする。そのような参照を行う手

法は，構成国によって定められる。

When Member States adopt the measures referred to in paragraph 1, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

第 42 条 規則(EU) No 910/2014 の改正

Article 42 **Amendment of Regulation (EU) No 910/2014**

規則(EU) No 910/2014 の第 19 条は，2024 年 10 月 18 日から発効するものとして削除される。

In Regulation (EU) No 910/2014, Article 19 is deleted with effect from 18 October 2024.

第 43 条 指令(EU) 2018/1972 の改正

Article 43 **Amendment of Directive (EU) 2018/1972**

指令(EU) 2018/1972 の第 40 条及び第 41 条は，2024 年 10 月 18 日から発効するものとして削除される。

In Directive (EU) 2018/1972, Articles 40 and 41 are deleted with effect from 18 October 2024.

第 44 条 廃止

Article 44 **Repeal**

指令(EU) 2016/1148 は，2024 年 10 月 18 日から発効するものとして廃止される。

Directive (EU) 2016/1148 is repealed with effect from 18 October 2024.

廃止される指令に対する参照は，この指令に対する参照として解釈され，かつ，別紙Ⅲに定める新旧対照表に従って読み替えられる。

References to the repealed Directive shall be construed as references to this Directive and shall be read in accordance with the correlation table set out in Annex III.

第 45 条　発効
Article 45 **Entry into force**

この指令は，EU 官報上のその公示の 20 日後に発効する。

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

第 46 条　発出
Article 46 **Addressees**

この指令は，構成国に対して発出される。

This Directive is addressed to the Member States.

ストラスブールにおいて，2022 年 12 月 14 日に行われた。

Done at Strasbourg, 14 December 2022.

欧州議会として For the European Parliament	理事会として For the Council
議長　R. METSOLA The President R. METSOLA	議長　M. BEK The President M. BEK

別紙Ⅰ　高度の重要性のある諸部門
ANNEX I SECTORS OF HIGH CRITICALITY

部門 Sector	副部門 Subsector	法主体のタイプ Type of entity
1.エネルギー Energy	(a)電力 Electricity	－欧州議会及び理事会の指令(EU) 2019/944[1] の第 2 条第 57 号に定義する電力事業者であって，同指令の第 2 条第 12 号に定義する「供給」の機能を遂行する者 Electricity undertakings as defined in Article 2, point (57), of Directive (EU) 2019/944 of the European Parliament and of the Council(1), which carry out the function of 'supply' as defined in Article 2, point (12), of that Directive
		－指令(EU) 2019/944 の第 2 条第 29 号に定義する配電システムの運営者 Distribution system operators as defined in Article 2, point (29), of Directive (EU) 2019/944
		－指令(EU) 2019/944 の第 2 条第 35 号に定義する送電システムの運営者 Transmission system operators as defined in Article 2, point (35), of Directive (EU) 2019/944
		－指令(EU) 2019/944 の第 2 条第 38 号に定義する製造者 Producers as defined in Article 2, point (38), of Directive (EU) 2019/944
		－欧州議会及び理事会の規則(EU) 2019/943[2] の第 2 条第 8 号に定義する指定された電力市場の運営者 Nominated electricity market operators as defined in Article 2, point (8), of Regulation (EU) 2019/943 of the European Parliament and of the Council (2) －指令(EU) 2019/944 の第 2 条第 18 号，第 20 号及び第 59 号に定義する集約サービス，需要対応サービスまたは蓄電サービスを提供する規則(EU) 2019/943 の第 2 条第 25 号に定義する市場参加者 Market participants as defined in Article 2, point (25), of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services as defined in Article 2, points (18), (20) and (59), of Directive (EU) 2019/944 －その名でまたはモビリティサービスのプロバイダの代わりに提供する場合を含め，エンドユーザに対して再充電サービスを提供する，再充電器設置場所に責任を負う再充電器設置場所の

		運営者 Operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider
	(b) 地域冷暖房 District heating and cooling	－欧州議会及び理事会の指令(EU) 2018/2001[3] の第 2 条第 19 号に定義する地域冷暖房の運営者 Operators of district heating or district cooling as defined in Article 2, point (19), of Directive (EU) 2018/2001 of the European Parliament and of the Council (3)
	(c)石油 Oil	－送油パイプラインの運営者 Operators of oil transmission pipelines
		－石油の製造, 精製及び管理施設, 貯蔵及び送油の運営者 Operators of oil production, refining and treatment facilities, storage and transmission
		－理事会指令 2009/119/EC[4] の第 2 条(f)に定義する中央備蓄機関 Central stockholding entities as defined in Article 2, point (f), of Council Directive 2009/119/EC (4)
	(d)ガス Gas	－欧州議会及び理事会の指令 2009/73/EC[5] の第 2 条第 8 号に定義する供給事業者 Supply undertakings as defined in Article 2, point (8), of Directive 2009/73/EC of the European Parliament and of the Council (5)
		－指令 2009/73/EC の第 2 条第 6 号に定義する配給システムの運営者 Distribution system operators as defined in Article 2, point (6), of Directive 2009/73/EC
		－指令 2009/73/EC の第 2 条第 4 号に定義する送出システムの運営者 Transmission system operators as defined in Article 2, point (4), of Directive 2009/73/EC
		－指令 2009/73/EC の第 2 条第 10 号に定義する貯蔵システムの運営者 Storage system operators as defined in Article 2, point (10), of Directive 2009/73/EC
		－指令 2009/73/EC の第 2 条第 12 号に定義する LNG システムの運営者 LNG system operators as defined in Article 2, point (12), of Directive 2009/73/EC
		－指令 2009/73/EC の第 2 条第 1 号に定義する天然ガス事業者

		Natural gas undertakings as defined in Article 2, point (1), of Directive 2009/73/EC
		－天然ガスの精製施設及び管理施設の運営者 Operators of natural gas refining and treatment facilities
	(e)水素 Hydrogen	－水素の製造, 貯蔵及び送出の運営者 Operators of hydrogen production, storage and transmission
2.輸送 Transport	(a)空 Air	－商業目的のために用いられる規則(EC) No 300/2008 の第 3 条第 4 号に定義する航空会社 Air carriers as defined in Article 3, point (4), of Regulation (EC) No 300/2008 used for commercial purposes
		－欧州議会及び理事会の規則(EU) No 1315/2013[7]の別紙 II の第 2 節に列挙する中核空港を含め, 欧州議会及び理事会の指令 2009/12/EC[6]の第 2 条第 2 号に定義する空港管理組織, 同指令の第 2 条第 1 号に定義する空港, 並びに, 空港内に含まれている付属施設を運用する法主体 Airport managing bodies as defined in Article 2, point (2), of Directive 2009/12/EC of the European Parliament and of the Council[(6)], airports as defined in Article 2, point (1), of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council[(7)], and entities operating ancillary installations contained within airports
		－欧州議会及び理事会の規則(EC)No 549/2004[8]の第 2 条第 1 号に定義する航空機運航管理（ATC）のサービスを提供する航空管制の運営者 Traffic management control operators providing air traffic control (ATC) services as defined in Article 2, point (1), of Regulation (EC) No 549/2004 of the European Parliament and of the Council[(8)]
	(b)鉄道 Rail	－欧州議会及び理事会の指令 2012/34/EU[9]の第 3 条第 2 号に定義するインフラ管理者 Infrastructure managers as defined in Article 3, point (2), of Directive 2012/34/EU of the European Parliament and of the Council[(9)]
		－指令 2012/34/EU の第 3 条第 12 号に定義するサービス施設の運営者を含め, 同指令の第 3 条第 1 号に定める鉄道事業者 Railway undertakings as defined in Article 3, point (1), of Directive 2012/34/EU, including operators of service facilities as defined in Article 3, point (12), of that Directive
	(c)水上 Water	－当該会社によって運用される個々の船舶を含めることなく, 欧州議会及び理事会の規則(EC) No 725/2004[10]の別紙 I の中で

		水上運送に関して定義する内水面, 海及び沿岸の旅客及び貨物の水上輸送会社 Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council [(10)], not including the individual vessels operated by those companies
		－規則(EC) No 725/2004 の第 2 条第 11 号に定義する当該組織の港湾施設を含め, 欧州議会及び理事会の指令 2005/65/EC[11] の第 3 条第 1 号に定義する港湾管理組織, 並びに, 港湾内に含まれている作業及び設備を運用する法主体 Managing bodies of ports as defined in Article 3, point (1), of Directive 2005/65/EC of the European Parliament and of the Council [(11)], including their port facilities as defined in Article 2, point (11), of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports
		－欧州議会及び理事会の指令 2002/59/EC[12] の第 3 条(o)に定義する船舶交通サービス（VTS）の運営者 Operators of vessel traffic services (VTS) as defined in Article 3, point (o), of Directive 2002/59/EC of the European Parliament and of the Council [(12)]
	(d)道路 Road	－高度輸送システムの交通管理または運営が当該法主体の一般的な活動中の不可欠ではない部分となっている公的部門の法主体を除き, 委員会委任規則(EU)2015/962[13] の第 2 条第 12 号に定義する交通管理の職責を負う道路当局 Road authorities as defined in Article 2, point (12), of Commission Delegated Regulation (EU) 2015/962 [(13)] responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their general activity
		－欧州議会及び理事会の指令 2010/40/EU[14] の第 4 条第 1 号に定義する高度輸送システムの運営者 Operators of Intelligent Transport Systems as defined in Article 4, point (1), of Directive 2010/40/EU of the European Parliament and of the Council [(14)]
3.銀行 Banking		欧州議会及び理事会の規則(EU) No 575/2013[15] の第 4 条第 1 号に定義する与信機関 Credit institutions as defined in Article 4, point (1), of Regulation (EU) No 575/2013 of the European Parliament and of the Council [(15)]

4.金融市場インフラ Financial market infrastructures		ー欧州議会及び理事会の指令 2014/65/EU[16]の第 4 条第 24 号に定義する取引所の運営者 Operators of trading venues as defined in Article 4, point (24), of Directive 2014/65/EU of the European Parliament and of the Council[(16)]
		ー欧州議会及び理事会の規則(EU) No 648/2012[17]の第 2 条第 1 号に定義する中央清算機関（CCPs） Central counterparties (CCPs) as defined in Article 2, point (1), of Regulation (EU) No 648/2012 of the European Parliament and of the Council[(17)]
5.医療 Health		ー欧州議会及び理事会の指令 2011/24/EU[18]の第 3 条(g)に定義する医療のプロバイダ Healthcare providers as defined in Article 3, point (g), of Directive 2011/24/EU of the European Parliament and of the Council[(18)]
		ー欧州議会及び理事会の規則(EU) 2022/2371[19]の第 15 条に示す EU 参照試験所 EU reference laboratories referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council[(19)]
		ー欧州議会及び理事会の指令 2001/83/EC[20]の第 1 条第 2 号に定義する医療製品の調査研究及び開発を遂行する法主体 Entities carrying out research and development activities of medicinal products as defined in Article 1, point (2), of Directive 2001/83/EC of the European Parliament and of the Council[(20)] ーNACE Rev. 2 の section C division 21 に示す基礎医薬品及び医薬調合品を製造する法主体 Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2 ー欧州議会及び理事会の規則(EU) 2022/123[21]の第 22 条の意味における公的医療の緊急事態の間に重要であると判断された医療機器（緊急事態時公的医療重要機器リスト）を製造する法主体 Entities manufacturing medical devices considered to be critical during a public health emergency (public health emergency critical devices list) within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council[(21)]
6.飲料水 Drinking water		人間の消費のための水の流通が，他の商品及び物品の流通という当該流通業者の一般的な活動中の不可欠ではない部分となっている流通業者を除き，欧州議会及び理事会の指令(EU) 2020/

		2184[22] の第 2 条第 1 号(a)に定義する人間の消費のために準備された水の供給者及び流通業者 Suppliers and distributors of water intended for human consumption as defined in Article 2, point (1)(a), of Directive (EU) 2020/2184 of the European Parliament and of the Council [(22)], excluding distributors for which distribution of water for human consumption is a non-essential part of their general activity of distributing other commodities and goods
7.廃水 Waste water		都市廃水，生活廃水または産業廃水の収集，処理または取扱いが当該事業者の一般的な活動中の不可欠ではない部分となっている事業者を除き，理事会指令 91/271/EEC[23] の第 2 条第 1 号，第 2 号及び第 3 号に定義する都市廃水，生活廃水または産業廃水を収集し，処理しまたは取り扱う事業者 Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water as defined in Article 2, points (1), (2) and (3), of Council Directive 91/271/EEC [(23)], excluding undertakings for which collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water is a non-essential part of their general activity
8.デジタルインフラ Digital infrastructure		－インターネット相互接続点のプロバイダ Internet Exchange Point providers
		－ルート名サーバの運営者を除き，DNS サービスのプロバイダ DNS service providers, excluding operators of root name servers
		－TLD 名レジストリ TLD name registries
		－クラウドコンピューティングサービスのプロバイダ Cloud computing service providers
		－データセンターサービスのプロバイダ Data centre service providers
		－コンテント伝達ネットワークのプロバイダ Content delivery network providers
		－信頼サービスのプロバイダ Trust service providers
		－公共電子通信ネットワークのプロバイダ Providers of public electronic communications networks
		－公衆が利用可能な電子通信サービスのプロバイダ Providers of publicly available electronic communications services
9.ICT サービスの管理(企業対企業)		－マネージドサービスのプロバイダ Managed service providers

ICT service management (business-to-business)		－マネージドセキュリティサービスのプロバイダ Managed security service providers
10.公行政 Public administration		－国内法に従って構成国によって定義された中央政府の行政機関である法主体 Public administration entities of central governments as defined by a Member State in accordance with national law
		－国内法に従って構成国によって定義された地域レベルの行政機関である法主体 Public administration entities at regional level as defined by a Member State in accordance with national law
11.宇宙 Space		公共電子通信ネットワークのプロバイダを除き，宇宙ベースのサービスの提供を支援し，構成国または民間の者によって保有，管理及び運営されている地上ベースのインフラの運営者 Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks

---

1 電力のための域内市場の共通規定に関する及び指令 2012/27/EU を改正する欧州議会及び理事会の 2019 年 6 月 5 日の指令(EU) 2019/944 (OJ L 158, 14.6.2019, p. 125).
Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p. 125).

2 電力のための域内市場に関する欧州議会及び理事会の 2019 年 6 月 5 日の規則(EU) 2019/943 (OJ L 158, 14.6.2019, p. 54).
Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).

3 再生可能資源からのエネルギーの利用の促進に関する欧州議会及び理事会の 2018 年 12 月 11 日の指令(EU) 2018/2001 (OJ L 328, 21.12.2018, p. 82).
Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).

4 原油及びまたは石油製品のミニマムの備蓄を維持する義務を構成国に負わせる 2009 年 9 月 14 日の理事会指令 2009/119/EC (OJ L 265, 9.10.2009, p. 9).
Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p. 9).

[5] 天然ガスの域内市場の共通規定に関する及び指令 2003/55/EC を廃止する欧州議会及び理事会の 2009 年 7 月 13 日の指令 2009/73/EC (OJ L 211, 14.8.2009, p. 94).
Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).

[6] 空港使用料に関する欧州議会及び理事会の 2009 年 3 月 11 日の指令 2009/12/EC (OJ L 70, 14.3.2009, p. 11).
Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p. 11).

[7] 欧州横断輸送ネットワークの開発のための欧州連合の指針に関する及び決定 No 661/2010/EU を廃止する欧州議会及び理事会の 2013 年 12 月 11 日の規則(EU) No 1315/2013 (OJ L 348, 20.12.2013, p. 1).
Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p. 1).

[8] 欧州の単一の空の創始のための枠組みを定める欧州議会及び理事会の 2004 年 3 月 10 日の規則 (EC) No 549/2004（枠組み規則）(OJ L 96, 31.3.2004, p. 1).
Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p. 1).

[9] 欧州の単一鉄道領域を設ける欧州議会及び理事会の 2012 年 11 月 21 日の指令 2012/34/EU (OJ L 343, 14.12.2012, p. 32).
Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p. 32).

[10] 船舶及び港湾施設の防護の拡大に関する欧州議会及び理事会の 2004 年 3 月 31 日の規則(EC) No 725/2004 (OJ L 129, 29.4.2004, p. 6).
Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6).

[11] 港湾の防護の拡大に関する欧州議会及び理事会の 2005 年 10 月 26 日の指令 2005/65/EC (OJ L 310, 25.11.2005, p. 28).
Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).

[12] 欧州共同体の船舶航行監視情報システムを設置し及び理事会指令 93/75/EEC を廃止する欧州議会及び理事会の 2002 年 6 月 27 日の指令 2002/59/EC (OJ L 208, 5.8.2002, p. 10).
Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p. 10).

[13] EU 全域のリアルタイム交通情報サービスの提供に関する 2014 年 12 月 18 日の欧州議会及び理事会の指令 2010/40/EU を補完する委員会委任規則(EU) 2015/962 (OJ L 157, 23.6.2015, p. 21).
Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-

time traffic information services (OJ L 157, 23.6.2015, p. 21).

14 道路交通の分野における高度交通システムの配置及び他の態様の交通とのインタフェイスのための枠組みに関する欧州議会及び理事会の 2010 年 7 月 7 日の指令 2010/40/EU (OJ L 207, 6.8.2010, p. 1).
Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).

15 与信機関の健全性要件に関する及び規則(EU) No 648/2012 を改正する欧州議会及び理事会の 2013 年 6 月 26 日の規則(EU) No 575/2013 (OJ L 176, 27.6.2013, p. 1).
Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

16 金融商品市場に関する並びに指令 2002/92/EC 及び指令 2011/61/EU を改正する欧州議会及び理事会の 2014 年 5 月 15 日の指令 2014/65/EU (OJ L 173, 12.6.2014, p. 349).
Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

17 OTC デリバティブ，中央清算機関及び取引情報蓄積機関に関する欧州議会及び理事会の 2012 年 7 月 4 日の規則(EU) No 648/2012 (OJ L 201, 27.7.2012, p. 1).
Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

18 国境を越える医療における患者の権利の適用に関する欧州議会及び理事会の 2011 年 3 月 9 日の指令 2011/24/EU (OJ L 88, 4.4.2011, p. 45).
Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

19 医療に対する国境を越える重大な脅威に関する及び決定 No 1082/2013/EU を廃止する欧州議会及び理事会の 2022 年 11 月 23 日の規則(EU) 2022/2371 (OJ L 314, 6.12.2022, p. 26).
Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU (OJ L 314, 6.12.2022, p. 26).

20 人間の利用のための医療製品と関連する欧州共同体法に関する欧州議会及び理事会の 2001 年 11 月 6 日の指令 2001/83/EC (OJ L 311, 28.11.2001, p. 67).
Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p. 67).

21 医療製品及び医療機器の危機準備態勢及び危機管理における欧州医療局の役割の強化に関する欧州議会及び理事会の 2022 年 1 月 25 日の規則(EU) 2022/123 (OJ L 20, 31.1.2022, p. 1).
Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (OJ L 20, 31.1.2022, p. 1).

22 人間の消費のために準備される水の品質に関する欧州議会及び理事会の 2020 年 12 月 16 日の指令(EU) 2020/2184 (OJ L 435, 23.12.2020, p. 1).

Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the quality of water intended for human consumption (OJ L 435, 23.12.2020, p. 1).

[23] 都市の廃水処理に関する 1991 年 5 月 21 日の理事会指令 91/271/EEC (OJ L 135, 30.5.1991, p. 40). Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991, p. 40).

別紙Ⅱ　その他の重要な諸部門
ANNEX II OTHER CRITICAL SECTORS

部門 Sector	副部門 Subsector	法主体のタイプ Type of entity
1.郵便サービス及び宅配サービス Postal and courier services		宅配サービスのプロバイダを含め，指令 97/67/EC の第 2 条(1a)に定義する郵便サービスのプロバイダ Postal service providers as defined in Article 2, point (1a), of Directive 97/67/EC, including providers of courier services
2.廃棄物管理 Waste management		廃棄物管理が当該事業者の主要な経済活動ではない事業者を除き，欧州議会及び理事会の指令 2008/98/EC[1] の第 3 条第 9 号に定義する廃棄物管理を遂行する事業者 Undertakings carrying out waste management as defined in Article 3, point (9), of Directive 2008/98/EC of the European Parliament and of the Council [(1)], excluding undertakings for whom waste management is not their principal economic activity
3.化学品の生産，製造及び流通 Manufacture, production and distribution of chemicals		欧州議会及び理事会の規則(EC) No 1907/ 2006[2] の第 3 条第 9 号及び第 14 号に示す物質の生産及び物質または混合物の流通を遂行する事業者，並びに，物質または混合物からの，同規則第 3 条第 3 号に定義するアーティクルの製造を遂行する事業者 Undertakings carrying out the manufacture of substances and the distribution of substances or mixtures, as referred to in Article 3, points (9) and (14), of Regulation (EC) No 1907/2006 of the European Parliament and of the Council [(2)] and undertakings carrying out the production of articles, as defined in Article 3, point (3), of that Regulation, from substances or mixtures
4.食品の製造，加工及び流通 Production, processing and distribution of food		欧州議会及び理事会の規則(EC) No 178/ 2002[3] の第 3 条第 2 号に定義する食品企業であって，卸売販売並びに工業製造及び加工に従事する者 Food businesses as defined in Article 3, point (2), of

		Regulation (EC) No 178/2002 of the European Parliament and of the Council[3] which are engaged in wholesale distribution and industrial production and processing
5.生産 Manufacturing	(a)医療機器及び体外診断用医療機器の生産 Manufacture of medical devices and *in vitro* diagnostic medical devices	この指令の別紙 I の第 5 号第 5 段に示す医療機器を製造する法主体を除き，欧州議会及び理事会の規則(EU) 2017/745[4] の第 2 条第 1 号に定義する医療機器を生産する法主体，並びに，欧州議会及び理事会の規則(EU) 2017/746[5] の第 2 条第 2 号に定義する体外診断用医療機器を生産する法主体 Entities manufacturing medical devices as defined in Article 2, point (1), of Regulation (EU) 2017/745 of the European Parliament and of the Council [4], and entities manufacturing *in vitro* diagnostic medical devices as defined in Article 2, point (2), of Regulation (EU) 2017/746 of the European Parliament and of the Council [5] with the exception of entities manufacturing medical devices referred to in Annex I, point 5, fifth indent, of this Directive
	(b)コンピュータ，電子製品及び光学製品の生産 Manufacture of computer, electronic and optical products	NACE Rev. 2 の section C division 26 に示す経済活動のいずれかを遂行する事業者 Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2
	(c)電気機器の生産 Manufacture of electrical equipment	NACE Rev. 2 の section C division 27 に示す経済活動のいずれかを遂行する事業者 Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2
	(d)他に分類されない機械及び機器の生産 Manufacture of machinery and equipment n.e.c.	NACE Rev. 2 の section C division 28 に示す経済活動のいずれかを遂行する事業者 Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2
	(e)自動車，トレーラー及びセミトレーラーの生産	NACE Rev. 2 の section C division 29 に示す経済活動のいずれかを遂行する事業者 Undertakings carrying out any of the economic

	Manufacture of motor vehicles, trailers and semi-trailers	activities referred to in section C division 29 of NACE Rev. 2
	(f)その他の輸送装置の生産 Manufacture of other transport equipment	NACE Rev. 2 の section C division 30 に示す経済活動のいずれかを遂行する事業者 Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2
6.デジタルプロバイダ Digital providers		ーオンライン市場のプロバイダ Providers of online marketplaces
		ーオンライン検索エンジンのプロバイダ Providers of online search engines
		ーオンラインソーシャルネットワーキングサービスプラットフォームのプロバイダ Providers of social networking services platforms
7.調査研究 Research		調査研究組織 Research organisations

---

1 廃棄物に関する及び一定の指令を廃止する欧州議会及び理事会の 2008 年 11 月 19 日の指令 2008/98/EC (OJ L 312, 22.11.2008, p. 3).
Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008, p. 3).

2 化学物質の登録, 評価, 認可及び制限（REACH）に関する, 欧州化学局を設置する, 指令 1999/45/EC を改正する, 並びに, 理事会規則(EEC) No 793/93, 委員会規則(EC) No 1488/94, 理事会指令 76/769/EEC, 委員会指令 91/155/EEC, 委員会指令 93/67/EEC, 委員会指令 93/105/EC 及び委員会指令 2000/21/EC を廃止する欧州議会及び理事会の 2006 年 12 月 18 日の規則(EC) No 1907/2006 (OJ L 396, 30.12.2006, p. 1).
Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 396, 30.12.2006, p. 1).

3 食品法の一般原則及び要件を定め, 欧州食品安全局を設置し, 食品安全事項の手続を定める欧州議会及び理事会の 2002 年 1 月 28 日の規則(EC) No 178/2002 (OJ L 31, 1.2.2002, p. 1).
Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying

down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p. 1).

4 医療機器に関する, 指令 2001/83/EC, 規則(EC) No 178/2002 及び規則(EC) No 1223/2009 を改正する, 並びに, 理事会指令 90/385/EEC 及び理事会指令 93/42/EEC を廃止する欧州議会及び理事会の 2017 年 4 月 5 日の規則(EU) 2017/745 (OJ L 117, 5.5.2017, p. 1).

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).

5 体外診断用医療機器に関する, 並びに, 指令 98/79/EC 及び委員会決定 2010/227/EU を廃止する欧州議会及び理事会の 2017 年 4 月 5 日の規則(EU) 2017/746 (OJ L 117, 5.5.2017, p. 176).

Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

別紙Ⅲ　新旧対照表

ANNEX III CORRELATION TABLE

指令 (EU) 2016/1148	この指令
第 1 条第 1 項	第 1 条第 1 項
第 1 条第 2 項	第 1 条第 2 項
第 1 条第 3 項	―
第 1 条第 4 項	第 2 条第 12 項
第 1 条第 5 項	第 2 条第 13 項
第 1 条第 6 項	第 2 条第 6 項及び第 11 項
第 1 条第 7 項	第 4 条
第 2 条	第 2 条第 14 項
第 3 条	第 5 条
第 4 条	第 6 条
第 5 条	―
第 6 条	―
第 7 条第 1 項	第 7 条第 1 項及び第 2 項
第 7 条第 2 項	第 7 条第 4 項
第 7 条第 3 項	第 7 条第 3 項
第 8 条第 1 項ないし第 5 項	第 8 条第 1 項ないし第 5 項
第 8 条第 6 項	第 13 条第 4 項
第 8 条第 7 項	第 8 条第 6 項
第 9 条第 1 項, 第 2 項及び第 3 項	第 10 条第 1 項, 第 2 項及び第 3 項
第 9 条第 4 項	第 10 条第 9 項
第 9 条第 5 項	第 10 条第 10 項
第 10 条第 1 項, 第 2 項及び第 3 項第 1 副項	第 13 条第 1 項, 第 2 項及び第 3 項
第 10 条第 3 項第 2 副項	第 23 条第 9 項
第 11 条第 1 項	第 14 条第 1 項及び第 2 項
第 11 条第 2 項	第 14 条第 3 項
第 11 条第 3 項	第 14 条第 4 項第 1 副項(a)ないし(q)及び(s)並びに第 7 項
第 11 条第 4 項	第 14 条第 4 項第 1 副項(r)及び第 2 副項
第 11 条第 5 項	第 14 条第 8 項
第 12 条第 1 項ないし第 5 項	第 15 条第 1 項ないし第 5 項
第 13 条	第 17 条
第 14 条第 1 項及び第 2 項	第 21 条第 1 項ないし第 4 項
第 14 条第 3 項	第 23 条第 1 項
第 14 条第 4 項	第 23 条第 3 項

指令 (EU) 2016/1148	この指令
第 14 条第 5 項	第 23 条第 5 項, 第 6 項及び第 8 項
第 14 条第 6 項	第 23 条第 7 項
第 14 条第 7 項	第 23 条第 11 項
第 15 条第 1 項	第 31 条第 1 項
第 15 条第 2 項第 1 副項(a)	第 32 条第 2 項(e)
第 15 条第 2 項第 1 副項(b)	第 32 条第 2 項(g)
第 15 条第 2 項第 2 副項	第 32 条第 3 項
第 15 条第 3 項	第 32 条第 4 項(b)
第 15 条第 4 項	第 31 条第 3 項
第 16 条第 1 項及び第 2 項	第 21 条第 1 項ないし第 4 項
第 16 条第 3 項	第 23 条第 1 項
第 16 条第 4 項	第 23 条第 3 項
第 16 条第 5 項	―
第 16 条第 6 項	第 23 条第 6 項
第 16 条第 7 項	第 23 条第 7 項
第 16 条第 8 項及び第 9 項	第 21 条第 5 項及び第 23 条第 11 項
第 16 条第 10 項	―
第 16 条第 11 項	第 2 条第 1 項, 第 2 項及び第 3 項
第 17 条第 1 項	第 33 条第 1 項
第 17 条第 2 項(a)	第 32 条第 2 項(e)
第 17 条第 2 項(b)	第 32 条第 4 項(b)
第 17 条第 3 項	第 37 条第 1 項(a)及び(b)
第 18 条第 1 項	第 26 条第 1 項(b)及び第 2 項
第 18 条第 2 項	第 26 条第 3 項
第 18 条第 3 項	第 26 条第 4 項
第 19 条	第 25 条
第 20 条	第 30 条
第 21 条	第 36 条
第 22 条	第 39 条
第 23 条	第 40 条
第 24 条	―
第 25 条	第 41 条
第 26 条	第 45 条
第 27 条	第 46 条
別紙 I (1)	第 11 条第 1 項
別紙 I (2)(a)(i)ないし(iv)	第 11 条第 2 項(a)ないし(d)
別紙 I (2)(a)(v)	第 11 条第 2 項(f)

指令 (EU) 2016/1148	この指令
別紙Ⅰ(2)(b)	第 11 条第 4 項
別紙Ⅰ(2)(c)(i)及び(ii)	第 11 条第 5 項(a)
別紙Ⅱ	別紙Ⅰ
別紙Ⅲ(1)及び(2)	別紙Ⅱ(6)
別紙Ⅲ(3)	別紙Ⅰ(8)

指令(EU) 2022/2557

[参考訳]

2023 年 11 月 29 日
明治大学法学部教授
夏 井 高 人

DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC（OJ L 333, 27.12.2022, p. 164-198）のテキスト（英語版）に基づいて和訳を試みた。

原文のテキストを入手できるサイトの URL は，下記のとおりである。

http://data.europa.eu/eli/dir/2022/2557/oj
[2023 年 11 月 20 日確認]

―解 説―

1 指令(EU) 2022/2557 について

指令(EU) 2022/2557 は，欧州の重要インフラの識別及び安全性確保を目的とする理事会指令 2008/114/EC (OJ L 345, 23.12.2008, p. 75)を全面改正する EU の法令である。

それと同時に，指令(EU) 2022/2557 は，従前は NIS 指令(EU) 2016/1148 (OJ L 194, 19.7.2016, p. 1) の関連条項によって定められていた重要インフラを運営する法主体の識別の手続等に関する事項を合併して定める EU の法令である。これらの事項に関しては，NIS 指令の後継法令である NIS2 指令（OJ L 333, 27.12.2022, p. 80-152）では定められていない。
その意味で，指令(EU) 2022/2557 は，NIS 指令(EU) 2016/1148 の改正法令でもある。

指令(EU) 2022/2557 は，2022 年 12 月 14 日に採択され，2023 年 1 月 16 日に発効した。

指令(EU) 2022/2557 に定める条項に定める規範内容を構成国の国内法として移植して実装する国内法化の期限は，2024 年 10 月 17 日である。

指令(EU) 2022/2557 に基づき構成国の国内法として移植されることにより実装された条項は，2024 年 10 月 18 日から適用される（第 26 条第 1 項参照）。

理事会指令 2008/114/EC は，2024 年 10 月 17 日の経過をもって廃止される（第 27 条参照）。

NIS 指令(EU) 2016/1148 は，2024 年 10 月 17 日の経過をもって廃止される（NIS2 指令の第 44 条参照）。

1．1 NIS 指令及び NIS2 指令との関係

NIS 指令に定められていた事項の中で指令(EU) 2022/2557 に移された事項を明確化するため，試みに新旧対照表的なものを作成してみると，以下のとおりとなる。

なお，NIS2 指令の別紙Ⅲ（新旧対照表）は，NIS 指令の条項と NIS2 指令の条項の関係を示すものであり，NIS 指令の条項と指令(EU) 2022/2557 の条項との関係を示すものではない。指令(EU) 2022/2557 の中には，理事会指令 2008/114/EC の条項及び NIS 指令の条項との関係を示す新旧対照表が含まれていないので，これらの法令の法解釈によって関連条項の対応関係を確定するしかない。

事項	NIS 指令	指令(EU) 2022/2557	NIS2 指令
運営者の識別	第 5 条	第 6 条	－
重大な混乱の影響	第 6 条	第 7 条	－
国内戦略	第 7 条	第 4 条	－
職務権限のある機関	第 8 条	第 9 条	第 8 条
単一連絡部局	第 8 条	第 9 条	第 8 条
CSIRT	第 9 条	－	第 10 条
協力グループ	第 11 条	－	第 14 条
CSIRT ネットワーク	第 12 条	－	第 15 条
構成国間の協力	－	第 11 条	第 16 条
法主体のリスク評価	－	第 12 条	－
法主体の回復力措置	－	第 13 条	－
身辺調査	－	第 14 条	－
リスク管理措置	－	－	第 21 条
インシデント評価	第 14 条	第 15 条	－
インシデント通知	第 16 条	第 15 条	第 23 条
監督及び執行	第 15 条	第 21 条	第 31 条～第 34 条
情報共有	－	－	第 29 条

この対応関係を見ればわかるとおり，サイバーな脅威，リスク及びインシデントと非サイバーな脅威，リスク及びインシデントの両者を含む統合的な国内戦略は，指令(EU) 2022/2557 に基づいて定められる。
ネットワーク及び情報システム（NIS）と関係するサイバーな脅威，リスク及びインシデントの集合は，全体としての脅威，リスク及びインシデントの部分集合であるので，サイバーな脅威，リスク及びインシデントに関して定める NIS2 指令は，この点に関する限り，指令(EU) 2022/2557 のサブセットと

いう意味での特別法であることになる。

このことは，少なくとも重要インフラと情報システムの防護に関する限り，日本国の関連法制全体の見直しを迫るものであるとも言える。

1．2 個人データ保護との関係

指令(EU) 2022/2557 の運用上では様々な個人データの処理が伴う。

指令(EU) 2022/2557 では，第 1 条第 9 項において，規則(EU) 2016/679（GDPR）(OJ L 119, 4.5.2016, p. 1)及び指令 2002/58/EC(OJ L 201, 31.7.2002, p. 37)を妨げない旨を定めている。

一般に，構成国の行政機関による個人データの処理には規則(EU) 2016/679（GDPR）が適用される。

指令(EU) 2022/2557 に基づくリスク評価及びリスク管理等と関係する業務遂行の過程で何らかの犯罪と関連している疑いが生じたときは，構成国の職務権限のある機関が当該構成国の法執行機関（警察）と協力して事態に対処することになると思われる。
そのような場合，指令(EU) 2022/2557 の中では明示されていないが，指令(EU)2016/680 (OJ L 119, 4.5.2016, p. 89)が適用される。

これに対し，欧州委員会のような欧州連合の機関，組織，事務局及び部局による個人データの処理に関しては，指令(EU) 2022/2557 の中では明示されていないが，規則(EU) 2018/1725 (OJ L 295, 21.11.2018, p. 39)が適用される。

なお，第三国を攻撃元とするサイバー戦に該当する場合を含め，構成国の国家安全保障や国防と関係する場合及び欧州連合の対外関係と関係する場合においては，規則(EU) 2016/679（GDPR）及び規則(EU) 2018/1725 が適用されない。

1．3 脅威，リスク及びインシデントについて

NIS2 指令とは異なり，指令(EU) 2022/2557 は，基本的には，欧州の重要インフラの防護と欧州の社会活動及び経済活動にとって必須の重要なサービスの提供の防護を目的とする法令である。それゆえ，重要インフラと関係するものまたは欧州の社会活動及び経済活動にとって必須の重要なサービスと関係するものである限り，情報システムや情報通信ネットワークの防護だけではなく，様々な脅威が想定される非サイバーな脅威，リスク及びインシデントに対する対処と関連する条項も多数含まれている。

大規模自然災害等の非人為的なリスクに関する事柄と併せ，サイバーな脅威と非サイバーな脅威との複合体としてのハイブリッドな脅威に関する事柄にも十分に留意すべきである。

1. 3. 1 非人為的なリスク

指令(EU) 2022/2557 の前文(3)及び前文(15)の中には，自然災害に関する言及があり，同指令の第 5 条において，リスク評価の内容として自然災害（natural disasters）のリスクと人為的なリスク（man-made risks）を含めている。
指令(EU) 2022/2557 に定める欧州の特別に重要な必須法主体（critical entities of particular European significance）と特に強い関連性をもつ EU の法令である欧州電子通信法指令(EU) 2018/1972（OJ L 321, 17.12.2018, p. 36–214）もまた，自然災害として分類されるインシデントとその対応を定めている。

指令(EU) 2022/2557 において想定されている非人為的なリスクを検討してみると，火山噴火，大地震，大洪水，豪雪，異常乾燥状態下の自然発火による山林火災等の純粋な大規模自然災害が考えられる。
しかし，一般論としては，そのような大規模自然災害だけではなく，例えば，化学物質による海洋汚染による魚介類の大量死に起因する水路閉塞等の結果としての水冷式冷却システムの機能停止のようなトラブル，天候不順による農作物や山林の大量枯死に伴って飛散する砂礫・微粒子の増加による化学的腐食や物理的汚損・微細な破損等の結果としての各種電子機器の劣化，異常気象による特定の微生物の大繁殖に起因する生物学的腐食の結果としての各種電子機器や送電網の劣化，強度の酸性雨に起因する化学的腐食の結果としての各種電子機器や送電網の劣化，環境ホルモンを含め各種化学薬品による環境汚染の結果としての情報システム管理要員となる自然人の全体的な知的能力や身体状態の劣化のようなリスクも当然に予想されなければならない。

ここで一般論として例にあげた生物や化学物質の中には，人工的に設計・製造された生物化学兵器またはその原料として分類される生物及び物質が含まれ得る。
それらの生物化学兵器等が人為的に用いられたときには単なる軍事攻撃のための手法（戦術）の 1 つということになる。
しかし，例えば，特定の生物兵器が，その開発者の想定を超えて進化して新生物となり，誰も制御できなくなってしまったような場合，または，得的の化学兵器が想定外の何らかの要因によって化学変化を生じさせて別の化学物質となり，誰も制御できなくなってしまったような場合には，現在の通常の法体系の下では，自然災害の一種として扱うしかない（米国の Morris worm 事件参照）。

他方において，一般に，機器や施設の物理的な耐性は，気候や気象と関係する自然界の条件が一定であることを大前提としていることが多い。
例えば，乾燥した砂漠地帯向けに設計・製造される自動車と湿潤な熱帯雨林地帯向けに設計・製造される自動車とでは，同じ型式で登録されている自動車であっても，基本的な部品の耐性が異なっており，特にタイヤは（現地の気候に合わせた）全く別のタイプのものでなければ走行不可能となる。
それらの耐性の中には，一般的には，乾湿の耐性，温度変化の耐性，粘菌，藻類，細菌，カビ，コケなどの微生物とその分泌物（化学物質）に対する耐性，砂礫中に含有される塩分等への耐性ま

たは耐久性も含まれている。

ところが気候変動が恒常的になると，簡単には置き換えできない大規模工場施設等では特に，自然条件の変化に伴う腐食や劣化が急速に進むことが十分にあり得る。また，従来は津波や洪水のリスクを想定しなくても誰も不思議に思わなかったような地域において，大規模な津波や洪水が発生し，地盤ごと大規模に崩壊してしまうこともあり得る。

一班に，現代社会においては，従来は「定数」として理解されていた要素の大半がどのように変化するかが予測不可能な「変数」として理解されるべき状態へと遷移してしまっている事象が非常に多い。
簡単に言えば，過去に蓄積された自然科学上の知識や経験が完全に反故にされてしまうような分野が急激に増加している。

これらのような多変量的な自然災害のリスクも考慮に入れられるべきである。また，現在では客観的な正当性や有用性を完全に喪失してしまった理論や実務等に関し，適切な対処を検討する必要性もある。

1．3．2 ハイブリッドな脅威（hybrid threats）

一般に，ハイブリッドな脅威は，サイバーな脅威と非サイバーな脅威との混合またはサイバーな攻撃と非サイバーな攻撃を巧妙に組み合わせた高等戦術の脅威として理解されている。例えば，ある国（A 国）の電力供給と関連する重要インフラを担当している企業の株式の大多数を仮想敵国（B 国）のエージェントである（普通の民間会社を装った）組織等が買収することに成功し，当該企業を支配できるようになれば，当該企業が提供する電力供給の役務が存在することを必須の前提としている情報通信もまた，仮想敵国（B 国）の支配下に置かれることになる。
また，そのようにしてある国（A 国）の情報通信部門の企業が仮想敵国（B 国）のエージェントである組織等によって徐々に買収されれば，当該買収された企業が担当していた国家全体の情報セキュリティの一部を崩壊させることに成功したことにもなる。
それらの国際的な規模での企業買収活動は，究極的には，仮想敵国（B 国）によるサイバーな包括的支配（＝当該国家の電子的な侵略行為）を準備するものである。

このことから，自由経済体制の下においても，国家秩序の根幹に深刻な影響を与え得る外国企業等による経済活動に対する警戒が強まり，EU においても，可能な限りの対応策が講じられるようになった。
そのような意味での外国企業等による経済活動に対する警戒を含め，サイバーな脅威と非サイバーな脅威の複合体としてのハイブリッドな脅威に対応するための EU の基本姿勢は，ハイブリッドな脅威報告書 JOIN(2018) 14 final の参考訳（法と情報雑誌 3 巻 11 号 178～198 頁）及びハイブリッドな脅威通知 JOIN(2018) 16 final の参考訳（法と情報雑誌 3 巻 9 号 281～295 頁）の中で示されている。

これらの EU の文書が作成された時点で想定されていたのは，より具体的には，中国の巨大資本による欧州企業の大規模買収とそれによって生じ得る欧州の経済的・文化的な自律の喪失への危惧だったのではないかと考えられる。

一般に，電子的な侵略行為を準備行為として，その後に物理的な侵略行為が実行され得ることは，現在進行中のロシアによってウクライナ国内で現実に実行された行為を観察・検討するだけで容易に理解できることである。

ロシアの脅威が現実のものとして世界中で理解されるようになったのは，現在進行中のウクライナに対する物理的な侵攻の後のことである。ロシアがウクライナへの侵攻を開始する前の段階において，EU は，ロシアから供給される天然ガスへの依存を強めていたので，ロシアに対して警戒心を抱かない構成国が少なくなかったし，特にドイツではそうだった。
ただし，情報セキュリティの専門家や関係各国の諜報機関の専門家または NATO の関係者の中には，ウクライナの発電所や送電施設等に対する大規模なサイバー攻撃が実行され，（ウクライナ軍の防空施設を含め）非常に広範囲にわたる停電などの深刻な被害を発生させた時点で，その次の軍事侵攻段階である戦車部隊や空挺部隊等による物理的な侵攻が近未来に実行される可能性が非常に高いということを明確に理解していた者が決して少なくなかった。
未来の歴史学者は，ロシアからの天然ガスの積極的供給政策に関し，経済学の観点だけではなく，情報戦やサイバー攻撃を含め，ハイブリッドな侵略という文脈の中で，そのための戦術上の手段の一部として，この一連の出来事を理解することになるだろう。

指令(EU) 2022/2557 は，多種多様な脅威をサイバーな脅威と非サイバーな脅威とに分別するだけではなく，それらが混合していることがあり得るハイブリッドな脅威に関しても見逃してはならない重要な言及を含んでいる。

そのことを理解できるようになるためには，個別具体的な攻撃手法の正確な理解と，自然災害のような非人為的な要素の自然科学上のメカニズムの諸密な理解の両方を必要とする。それらの全部を理解しなければ，ハイブリッドな脅威を含め，サイバーな要素と非サイバーな要素が混在するような状況に対する包括的な理解に達することは不可能であるし，まして，そのような状況に対応する適切な措置を正しく検討することは，完全に不可能である。

なお，ハイブリッドな脅威であり得る国際的なテロ行為への対応を含め，EU キュリティ連合戦略の実装に関しては，その第 2 次進捗状況報告書 COM(2021) 440 final（2021 年 6 月 23 日）及び第 6 次進捗状況報告書 COM(2023) 665 final（2023 年 10 月 18 日）が参考になる。

1．4 指令(EU) 2022/2557 の原文中にある誤記等の問題

指令(EU) 2022/2557 の原文（英語版）には明らかな誤りが見られる。不完全な文なのではないかと疑われる箇所も存在する。

それらが訂正されるべき誤記等に該当すると欧州委員会が判断する場合，所定の手続を経て EU 官報上で公表されるその正誤表（corrigendum）によっていずれ訂正されることになると予想されるが，Eur-lex 上で 2023 年 11 月 27 日の時点において確認できた範囲内では，指令(EU) 2022/2557 の原文（英語版）に適用される正誤表は公表されていない。

そのため，この参考訳においては，誤記等のある箇所に関し，適宜意訳し，または，意識的に原文のままで訳出することにしたが，特に留意すべき点に関しては，「参考訳作成において留意した事項」の項で個別に指摘することにした。

2. 参考訳作成における基本方針

この参考訳においては，指令(EU) 2022/2557 の前文（recital），条文（articles）及び別紙（Annex）の全文を訳出した。

この参考訳においては対訳方式を採用することにした。ただし，原文を表示することが無意味な部分（特に脚注内）に関しては，原文または訳文の表示を省略した。

この参考訳は，あくまでも指令(EU) 2022/2557 の私的な和訳である。公式訳でも確定訳でもない。

この参考訳は，現時点における研究成果を反映するものである。将来，更に研究を深めた結果として修正すべき部分を発見したときは，その時点において，改訂版等を作成すべきかどうかを検討する。

参考訳の訳出に際しては原則として直訳とすることとしたが，直訳のままでは日本語になりにくい箇所に関しては，やむを得ず意訳とした。

この参考訳に訳注はない。参考訳中にある脚注は，全て原注である。訳注等による個別の説明がなければ当該箇所の訳出の理由がわかりにくいと想定される箇所に関しては，必要に応じて，「参考訳作成において留意した事項」の中で説明を加えることにした。

読みやすさを重視し，条文中の号(point)の表記を一部省略した。例えば，「point(a)」は「第(a)号」であるが，「第」と「号」を省略し，「(a)」と表記することにした。

この参考訳は，Eur-lex のデータ二次利用条件を遵守して作成した。

3. 参考訳作成において留意した事項

この参考訳は指令(EU) 2022/2557 の注釈書ではないので，それらの箇所の全てを指摘することは避け，必要に応じて合理的に解釈した上で訳文を作成することにした。

ここでは，特に説明を加えないと誤訳ではないかと誤解される危険性がある箇所を中心にして，この参考訳作成において留意した事項を摘記する。

＊＊＊

指令(EU) 2022/2557 の前文(5)の中にある「in respect of all hazards, whether natural or man-made, accidental or intentional」との箇所の中にある「in respect of」との箇所は，フランス語版では「en ce qui concerne」となっており，英語版とほぼ同じニュアンスであるが，ドイツ語版では「gegenüber」となっており，若干ニュアンスが異なる。
英語版の「in respect of」を「～に関する」と普通に訳すことは不可とは言えないが，意味的に少しずれているように思われる。
この「in respect of all hazards」との部分は，本来であれば，「in respect for an all-hazards approach」または「based on an all-hazards approach」というような文とすべきだったのではないかとも考えられる。
以上の諸点を考慮した上で，この箇所に関しては，合理的に意訳することにした。

指令(EU) 2022/2557 の前文(15)の第 1 文の中にある「The actions of Member States to identify and help ensure the resilience of critical entities」との箇所は，不完全な文である疑いがある。
指令(EU) 2022/2557 の第 5 条及び第 6 条に定める内容から考えると，この箇所は，「The actions of Member States to identify those critical entities and to help ensuring the resilience of such entities」という意味をもつ文であると解される。
この参考訳においては，そのように解した上で，合理的に意訳することにした。

指令(EU) 2022/2557 の前文(30)の第 3 文の中にある「with the requirements of this Directive」との箇所は，明白に，「with the obligations of this Directive」の誤記である（前文(28)，第 12 条第 2 項，第 13 条第 2 項参照）。
この参考訳においては，そのように解した上で，合理的に訳出することにした。

指令(EU) 2022/2557 の第 1 条第 4 項第 3 文の中にある「The exchange of information shall preserve the confidentiality of that information and the security and commercial interests of critical entities」との箇所は，「The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of critical entities」の誤記の可能性がある（NIS2 指令(EU) 2022/2555 の第 2 条第 13 項第 3 文参照）。
ただし，この参考訳においては，原文のまま訳出することにした。

指令(EU) 2022/2557 の第 4 条第 3 項は，不完全な文である可能性がある。

ただし，この参考訳においては，原文のまま訳出することにした。

指令(EU) 2022/2557 の第 9 条第 2 項第 3 文の中にある「a Member State may provide that」との箇所は，このままでも誤りとは言えないかもしれないが，要するに，「a Member State may provide for that」という趣旨の文と解される。
この参考訳においては，そのように解した上で訳出することにした。

指令(EU) 2022/2557 の第 9 条第 3 項第 2 副項第 2 文の中にある「The competent authorities may use」との箇所は，「The single points of contact may use」の誤記ではないかと考えられる。
ただし，この参考訳においては，原文のまま訳出することにした。

指令(EU) 2022/2557 の第 13 条第 1 項柱書の中にある「based on the relevant information provided by Member States on the Member State risk assessment」との箇所は，明白に，「based on the relevant information provided by Member States, on the Member State risk assessment」の誤記である。
この参考訳においては，そのように解した上で訳出することにした。

指令(EU) 2022/2557 の第 17 条第 2 項第 1 副項の中にある「informs its competent authority」との箇所の「its」は，単数形なので，「informs those competent authorites」の誤記であると解さない限り，複数形で表現されている「構成国（Member States）」を指すと解することができない。
そこで，「its」を「必須法主体（a critical entity）」を指すものとして解解することが可能かどうか検討してみると，形式的な文法論としては可能ではあっても，法解釈論上では無理だと考えられる。
他方，「its competent authority」に関し，第 6 条第 1 項に基づいて当該法主体を必須法主体として識別し，その通知をした構成国の職務権限のある機関のことを指すと解することは，合理的に可能な法解釈の範囲内あると考える（第 18 条第 1 項参照）。
以上の諸点を踏まえた上で，この参考訳においては，第 17 条第 2 項第 1 副項の中にある「its competent authority」を「その通知をした構成国の職務権限のある機関」と訳すのが無難であると判断し，そのように訳すことにした。

指令(EU) 2022/2557 の第 17 条第 3 項の中にある「through its competent authority」との箇所の「its」が何を指すのかは，明確ではない。
指令(EU) 2022/2557 の第 17 条第 2 項第 1 副項と関連して上述した諸点を踏まえた上で，この参考訳においては，第 17 条第 3 項の中にある「through its competent authority」を「その通知をした構成国の職務権限のある機関を介して」と訳すのが無難であると判断し，そのように訳すことにした。

指令(EU) 2022/2557 の別紙の中にある表のエネルギー部門の列の途中，エネルギー部門・電力副部門の列の途中，輸送部門の列の途中，輸送部門・水上副部門の列の途中，医療部門の列の途中，デジタルインフラ部門の列の途中には，それぞれ趣旨不明な区切り線がある。これらの区切り線は，いずれ合理性のないものであり，誤記の一種だと考えられる。
この参考訳においては，当該区切り線が存在しないものとして扱うことにした。

4. 訳語に関する補足的説明

Exclusively と predominantly

指令(EU) 2022/2557 の前文中では，同じような文脈の中で「exclusively」と「predominantly」が使用されており，実質的には同じことを意味していると解される。別異に解すべき法解釈上の実益は全く存在しない。
指令(EU) 2022/2557 の英語版においてこのように異なる表現の英単語が使用されているのは，法解釈上の重要な相違があるためではなく，単純に，英語版作成者または校正担当者が複数存在していてそれぞれの校正担当者の趣味・嗜好が異なっていただけに過ぎないか，または，校正作業中のミスにより表現が不統一になってしまっただけに過ぎないと推定される。そのようなことは，EU 法の英語版では現実にしばしばあることであり，ドイツ語版でもフランス語版でも同様にみられることである。
それゆえ，この参考訳においては，「exclusively」と「predominantly」のいずれについても「専ら」と訳すのが妥当と考えたが，英語それ自体としては異なる単語が使用されているので，そのことを反映するという単純に機械的・形式的な理由により，「exclusively」を「専ら」と訳し，「predominantly」を「主として」と訳すことにした。

Substantial updates

「substantial updates」は，「実質的なアップデート」と訳すことができるが，これでは日本語としてどのような意味をもつのか曖昧とならざるを得ない。
この場合の「substantial」は，誤記訂正のような，規範内容には実質的に影響を与えないアップデートや，指令(EU) 2022/2557 を移植して実装される国内法の運用に影響を与えない軽微な改訂を除き，意味のあるアップデートに限定する趣旨であると理解される。

そこで，この参考訳においては，「substantial updates」を「実質的に意味のあるアップデート」と意訳することにした。

Advisory missions

指令(EU) 2022/2557 の前文(35)及び前文(36)，第 13 条並びに第 18 条は，組織体としての諮問機関（advisory missions）と職務内容としての諮問の任務（advisory missions）に関して定めている。

この「advisory missions」は，1 名の自然人による審議官のような独任制の職ではなく，諮問機関的な組織体を想定しているように読める（第 18 条第 5 項参照）。

指令(EU) 2022/2557 の第 13 条は組織体としての諮問機関（advisory missions）に関する条項が中心となっている。
指令(EU) 2022/2557 の第 18 条の中には，職務内容としての諮問の任務（advisory missions）に関

する条項と組織体としての諮問機関（advisory missions）に関する条項が混在している。
指令(EU) 2022/2557 の前文(35)及び前文(36)の中には，第 18 条が定める内容を反映して，職務内容としての諮問の任務（advisory missions）に関する条項と組織体としての諮問機関（advisory missions）に関する記述が混在している。

この参考訳においては，組織体としての諮問機関（advisory missions）を指していると解される部分と職務内容としての諮問の任務（advisory missions）を指していると解される部分とで，それぞれ合理的に訳し分けることにした。

5. 関連参考訳

NIS2 指令(EU) 2022/2555 の参考訳は，法と情報雑誌 8 巻 4 号 1～206 頁にある。NIS 指令(EU) 2016/1148 の参考訳・再訂版は，法と情報雑誌 6 巻 6 号 467～548 頁にある。
指令(EU) 2017/541 の参考訳は，法と情報雑誌 2 巻 8 号 1～29 頁にある。規則(EU) 2021/1149 の参考訳は，法と情報雑誌 6 巻 3 号 1～103 頁にある。規則(EU) 2021/887 の参考訳は，法と情報雑誌 6 巻 2 号 1～95 頁にある。
規則(EU) 2018/1862 の参考訳は，法と情報雑誌 4 巻 6 号 1～70 頁にある。ECRIS-TCN 規則(EU) 2019/816 の参考訳は，法と情報雑誌 4 巻 6 号 176～208 頁にある。ECRIS 改正指令(EU) 2019/884 による改正後の理事会枠組み決定 2009/315/JHA の参考訳は，法と情報雑誌 4 巻 6 号 162～175 頁にある。規則(EU) 2018/1862 の参考訳は，法と情報雑誌 4 巻 6 号 1～70 頁にある。
ハイブリッドな脅威報告書 JOIN(2018) 14 final の参考訳は，法と情報雑誌 3 巻 11 号 178～198 頁にある。ハイブリッドな脅威通知 JOIN(2018) 16 final の参考訳は，法と情報雑誌 3 巻 9 号 281～295 頁にある。

規則 (EU) 2016/679（一般データ保護規則）の参考訳・再訂版は，法と情報雑誌 3 巻 5 号 1～114 頁にある。規則(EU)2018/1725 の参考訳は，法と情報雑誌 4 巻 1 号 1～81 頁にある。指令 2002/58/EC の参考訳・改訂版は，法と情報雑誌 2 巻 5 号 158～187 頁にある。指令(EU) 2016/680 の参考訳は，法と情報雑誌 2 巻 1 号 41～140 頁にある。
電子識別規則(EU) No 910/2014 の参考訳は，法と情報雑誌 2 巻 10 号 147～196 頁にある。

欧州電子通信法指令(EU) 2018/1972 の参考訳は，法と情報雑誌 4 巻 2 号 1～212 頁にある。
指令 2011/24/EU の参考訳は，法と情報雑誌 3 巻 6 号 133～168 頁にある。ITS 指令 2010/40/EU の参考訳は，法と情報雑誌 2 巻 9 号 27～47 頁にある。
金融商品市場規則(EU) No 600/2014（MiFIR）の参考訳は，法と情報雑誌 3 巻 3 号 1～79 頁にある。金融商品市場指令 2014/65/EU（MiFID II）の参考訳は，法と情報雑誌 3 巻 3 号 1～175 頁にある。OTC デリバティブ規則(EU) No 648/2012 の参考訳は，法と情報雑誌 3 巻 8 号 1～96 頁にある。

規則(EU) No 182/2011 の参考訳は，法と情報雑誌 3 巻 5 号 168～179 頁にある。

この参考訳の校正等に関し，唐亀侑久氏（株式会社ラック）の助力を得た。

＊＊＊

必須法主体の回復力に関する及び理事会指令 2008/114/EC を廃止する 欧州議会及び理事会の 2022 年 12 月 14 日の指令(EU) 2022/2557

DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC

（EEA に適用される正文）
(Text with EEA relevance)

欧州議会及び欧州連合の理事会は,
欧州連合の機能に関する条約, とりわけ, その第 114 条に鑑み,
欧州委員会からの提案に鑑み,
立法案を国内議会に送付した後,
欧州経済社会委員会の意見書に鑑み[1],
地域委員会の意見書に鑑み[2],
通常の立法手続に従って審議し[3],

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,
Having regard to the proposal from the European Commission,
After transmission of the draft legislative act to the national parliaments,
Having regard to the opinion of the European Economic and Social Committee[(1)],
Having regard to the opinion of the Committee of the Regions[(2)],
Acting in accordance with the ordinary legislative procedure[(3)],

Whereas:

(1) 必須サービスの提供者としての必須法主体は, 相互依存を高めている欧州連合の経済の中にある域内市場において, 重要な社会的機能または経済活動を維持する上で不可欠の役割を演じている。それゆえ, 整合化されたミニマムの規定を定めることによって, 域内市場内の必須法主体の回復力を拡大すること, 及び, 一貫性があり, 特化した支援と監督の措置により, それらの必須法主体を補助することの両者を狙いとする欧州連合の枠組みを定めることが不可欠である。

Critical entities, as providers of essential services, play an indispensable role in the maintenance of vital

[1] OJ C 286, 16.7.2021, p. 170.
[2] OJ C 440, 29.10.2021, p. 99.
[3] 欧州議会の 2022 年 11 月 22 日付けの意見書（官報未搭載）及び理事会の 2022 年 12 月 8 日付け決定.
Position of the European Parliament of 22 November 2022 (not yet published in the Official Journal) and Council decision of 8 December 2022.

societal functions or economic activities in the internal market in an increasingly interdependent Union economy. It is therefore essential to set out a Union framework with the aim of both enhancing the resilience of critical entities in the internal market by laying down harmonised minimum rules and assisting them by means of coherent and dedicated support and supervision measures.

(2) 理事会指令 2008/114/EC[4]は，その混乱または破壊が少なくとも 2 つの構成国に対して国境を越える重大な影響をもつような，エネルギー部門及び輸送部門における欧州の重要インフラを指定するための手続を定めている。同指令は，専ら，そのようなインフラの保護に焦点を当てている。しかしながら，2019 年に実施された指令 2008/114/EC の評価は，重要インフラを用いる業務運営が，相互接続され国境を越えるという性質を高めているため，全ての混乱の発生を防止するためには，個々の資産と関連する保護の措置だけでは不十分であると結論づけた。それゆえ，リスクがより良く考慮に入れられること，域内市場の稼働のための必須サービスの提供者としての必須法主体の役割と義務がより良く定義され，一貫性があること，そして，必須法主体の回復力を拡大するための欧州連合の規定が採択されることを確保することへと，そのアプローチを方向転換する必要がある。必須法主体は，必須サービスの提供を混乱させる可能性のあるインシデントを防止し，インシデントから保護し，インシデントに対応し，インシデントに抗し，インシデントを緩和し，インシデントを吸収し，インシデントを封じ込め，そして，インシデントから復旧するための当該必須法主体の能力を強化する立場にあるべきである。

Council Directive 2008/114/EC (4) provides for a procedure for designating European critical infrastructure in the energy and transport sectors the disruption or destruction of which would have a significant cross-border impact on at least two Member States. That Directive focuses exclusively on the protection of such infrastructure. However, the evaluation of Directive 2008/114/EC conducted in 2019 found that, due to the increasingly interconnected and cross-border nature of operations using critical infrastructure, protective measures relating to individual assets alone are insufficient to prevent all disruptions from taking place. Therefore, it is necessary to shift the approach towards ensuring that risks are better accounted for, that the role and duties of critical entities as providers of services essential to the functioning of the internal market are better defined and coherent, and that Union rules are adopted to enhance the resilience of critical entities. Critical entities should be in a position to reinforce their ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from incidents that have the potential to disrupt the provision of essential services.

(3) 重要インフラの保護のための欧州計画のような欧州レベルの及び国内レベルの多数の措置が，欧州連合内の重要インフラの保護を支えることを狙いとしているが，そのような重要インフラを運営する法主体に対し，必須サービスの提供の混乱をもたらし得るような当該重要インフラの業務

---

[4] 欧州の重要インフラの識別及び指定並びに同インフラの保護を向上させる必要性の評価に関する2008 年 12 月 8 日の理事会指令 2008/114/EC (OJ L 345, 23.12.2008, p. 75).
Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

運営を妨げるリスクに対処することをより良く具備させるためのより多くのことが行われるべきである。進化しつつあるハイブリッドな脅威とテロの脅威，インフラと諸部門との間の相互依存関係の増加を包摂する動的な脅威の全体把握があることからも，そのような必須法主体に対し，より良く具備させるためのより多くのことが行われるべきである。更に，異常気象事態の頻度と規模を激化させ，かつ，平均的な気候条件の長期的な変化をもたらすものであって，もし気候に適応する措置が設けられないとすれば一定のタイプのインフラの実現能力，効率性及び寿命を減衰させ得る自然災害及び気候変動による，高まりつつある物理的なリスクが存在する。加えて，関連する諸部門及び法主体の類型が，全ての構成国において一貫性をもって重要であると認識されていないため，域内市場は，必須法主体の識別に関しては，断片化によって特徴づけられている。それゆえ，この指令は，この指令の適用範囲内にある諸部門及び法主体の類型の面において安定的なレベルの整合化を達成すべきである。

While a number of measures at Union level, such as the European Programme for Critical Infrastructure Protection, and at national level aim to support the protection of critical infrastructure in the Union, more should be done to better equip the entities operating such infrastructure to address the risks to their operations that could result in the disruption of the provision of essential services. More should also be done to better equip such entities because there is a dynamic threat landscape, which includes evolving hybrid and terrorist threats, and growing interdependencies between infrastructure and sectors. Moreover, there is an increased physical risk due to natural disasters and climate change, which intensifies the frequency and scale of extreme weather events and brings long-term changes in average climate conditions that can reduce the capacity, efficiency and lifespan of certain infrastructure types if climate adaptation measures are not in place. In addition, the internal market is characterised by fragmentation in respect of the identification of critical entities because relevant sectors and categories of entities are not recognised consistently as critical in all Member States. This Directive should therefore achieve a solid level of harmonisation in terms of the sectors and categories of entities falling within its scope.

(4) エネルギー部門及び輸送部門のような一定の経済部門は，部門別の欧州連合の法行為によって既に規律されているが，それらの法行為は，当該部門において業務運営する法主体の一定の側面の回復力だけに関連する条項を含んでいる。域内市場の適正な稼働にとって必須であるそれらの必須法主体の回復力に包括的な態様で対処するため，この指令は，自然のものであるか人為的なものであるか，偶発的なものであるか意図的なものであるかを問わず，全ての危険との関係における必須法主体の回復力に対処する包括的な枠組みをつくり出す。

While certain sectors of the economy, such as the energy and transport sectors, are already regulated by sector-specific Union legal acts, those legal acts contain provisions which relate only to certain aspects of resilience of entities operating in those sectors. In order to address in a comprehensive manner the resilience of those entities that are critical for the proper functioning of the internal market, this Directive creates an overarching framework that addresses the resilience of critical entities in respect of all hazards, whether natural or man-made, accidental or intentional.

(5) インフラと諸部門との間の相互依存が増大しているのは，エネルギー，輸送，銀行，飲料水，廃水，食品の製造，加工及び流通，医療，宇宙，金融市場インフラ及びデジタルインフラの諸部門並びに公行政部門の一定の側面において，欧州連合全域にわたる鍵となるインフラを用いるサービス提供の国境を越える相互依存するネットワークが増加していることの結果である。宇宙部門は，構成国または民間の者によって保有，管理及び運営されている地上ベースのインフラに依存する一定のサービスの提供との関係においてこの指令の適用範囲内にあり；その結果として，欧州連合の宇宙計画の一部として欧州連合によってまたは欧州連合の代わりに保有され，管理されまたは運営されるインフラは，この指令の適用範囲内にはない。

The growing interdependencies between infrastructure and sectors are the result of an increasingly cross-border and interdependent network of service provision using key infrastructure across the Union in the energy, transport, banking, drinking water, waste water, production, processing and distribution of food, health, space, financial market infrastructure and digital infrastructure sectors and in certain aspects of the public administration sector. The space sector falls within the scope of this Directive with respect to the provision of certain services that depend on ground-based infrastructure owned, managed and operated either by Member States or by private parties; consequently, infrastructure owned, managed or operated by or on behalf of the Union as part of its space programme does not fall within the scope of this Directive.

エネルギー部門に関し，及び，とりわけ，（電気の供給との関係における）発電及び送電の手法に関し，それが適切であると判断されるときは，発電は，原子力プラントの送電部分を含めるけれども，原子力に関する欧州連合の関連法行為を含め条約及び欧州連合法の適用のある個別の放射性元素を除外することが了解された。食品部門における必須法主体を識別するための過程は，同部門の域内市場の性質並びに食品法及び食品の安全の基本原則及び要件と関連する欧州連合の広範な規定を適切に反映すべきである。それゆえ，比例的なアプローチが存在することを確保するため，及び，当該必須法主体の国内レベルにおける役割と重要性を適切に反映させるため，必須法主体は，営利目的の事業者であるか否かを問わず，かつ，公的事業者であるか民間事業者であるかを問わず，専ら，物流に従事する食品事業者，並びに，卸売販売に従事する事業者及び国内レベルで認識されるものとしての大きな市場占有率をもつ大規模な工業製造及び加工に従事する食品事業者の中においてのみ，識別されるべきである。それらの相互依存があるということは，必須サービスのいかなる混乱も，当初は 1 つの法主体または 1 つの部門にそれが限定されていたとしても，より広範なカスケード効果をもち得るということ，潜在的には，域内市場全域にわたるサービスの伝達に対して広範囲かつ長期にわたる負の影響をもたらし得るということを意味する。COVID-19 パンデミックのような大規模な危機は，大きな影響をもつけれども蓋然性の低いリスクに直面する際における，相互依存性を増大させている我々の社会の脆弱性を証明した。

In terms of the energy sector and in particular the methods of electricity generation and transmission (in respect of supply of electricity), it is understood that, where deemed appropriate, electricity generation can include electricity transmission parts of nuclear power plants but excludes the specifically nuclear elements covered by treaties and Union law, including relevant legal acts of the Union concerning nuclear

power. The process for identifying critical entities in the food sector should adequately reflect the nature of the internal market in that sector and the extensive Union rules relating to the general principles and requirements of food law and food safety. Therefore, in order to ensure that there is a proportionate approach and to adequately reflect the role and importance of those entities at national level, critical entities should only be identified among food businesses, whether for profit or not and whether public or private, that are engaged exclusively in logistics and wholesale distribution and large-scale industrial production and processing with a significant market share as observed at national level. Those interdependencies mean that any disruption of essential services, even one which is initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in a far-reaching and long-term negative impact on the delivery of services across the internal market. Major crises, such as the COVID-19 pandemic, have shown the vulnerability of our increasingly interdependent societies in the face of high-impact low-probability risks.

(6) 必須サービスの提供に関与する法主体は，国内法の下において課される多様な要件に服することが増加している。幾つかの構成国が，当該法主体に対する，より厳しくないセキュリティ上の要件をもっているということは，様々なレベルの回復力を導くだけではなく，欧州連合内の重要な社会的機能または経済活動を維持することに対して負の影響を与えるリスクも導き，また，域内市場の適正な稼働を妨げる障碍を導く。投資家と会社は，回復力のある必須法主体を信用及び信頼でき，そして，信用と信頼は，良好に稼働する域内市場の礎石である。類似するタイプの法主体が，幾つかの構成国では重要として判断されているが，別の構成国においてはそうではなく，そして，重要であるとして識別されている法主体が，別の構成国においては，異なる要件に服する。このことは，国境を越えて業務運営する会社に対し，付加的で無用な管理運営上の負担をもたらし，とりわけ，複数の構成国において能動的な会社に対し，より厳しい要件をもたらす。それゆえ，欧州連合の枠組みは，欧州連合全域にわたり，必須法主体のための競争の場を平等にする効果ももち得る。

The entities involved in the provision of essential services are increasingly subject to diverging requirements imposed under national law. The fact that some Member States have less stringent security requirements on those entities not only leads to various levels of resilience but also risks negatively impacting the maintenance of vital societal functions or economic activities across the Union and leads to obstacles to the proper functioning of the internal market. Investors and companies can rely on and trust critical entities that are resilient, and reliability and trust are the cornerstones of a well-functioning internal market. Similar types of entities are considered as critical in some Member States but not in others, and those which are identified as critical are subject to divergent requirements in different Member States. That results in an additional and unnecessary administrative burden for companies operating across borders, in particular for companies active in Member States with more stringent requirements. A Union framework would therefore also have the effect of levelling the playing field for critical entities across the Union.

(7) 域内市場における必須サービスの提供を確保するため，必須法主体の回復力を拡大するため，

そして，職務権限のある機関の間における国境を越える協力を向上させるための，整合化されたミニマムの規定を定める必要がある。当該規定が，必要な柔軟性を許容しつつ，当該規定の設計及び実装の面における将来耐性をもつことが重要である。多様なセットのリスクと直面する際において必須サービスを提供するための必須法主体の実現能力を向上させることも不可欠なことである。

It is necessary to lay down harmonised minimum rules to ensure the provision of essential services in the internal market, to enhance the resilience of critical entities and to improve cross-border cooperation between competent authorities. It is important that those rules be future proof in terms of their design and implementation while allowing for necessary flexibility. It is also crucial to improve the capacity of critical entities to provide essential services in the face of a diverse set of risks.

(8) 高いレベルの回復力を達成するため，構成国は，特別の要件及び監督に服することになり，かつ，関連する全てのリスクと直面する際，特別の支援とガイドの提供を受けることになる必須法主体を識別すべきである。

In order to achieve a high level of resilience, Member States should identify critical entities that will be subject to specific requirements and supervision and that will be provided with particular support and guidance in the face of all relevant risks.

(9) 必須法主体の回復力のためのサイバーセキュリティの重要性に鑑み，かつ，一貫性の利益において，それが可能な限り，この指令と欧州議会及び理事会の指令(EU) 2022/2555[5]との間の一貫性のあるアプローチが確保されるべきである。サイバーなリスクのより高い頻度と特別の性質に照らし，指令(EU) 2022/2555 は，大きなセットの法主体に対し，当該法主体のサイバーセキュリティを確保する包括的な要件を課している。指令(EU) 2022/2555 の中でサイバーセキュリティが大きく対処されていることに鑑み，同指令に包摂される事項は，デジタルインフラ部門にある法主体に関する特別の制度を妨げることなく，この指令の適用範囲から除外されるべきである。

Given the importance of cybersecurity for the resilience of critical entities and in the interests of consistency, a coherent approach should be ensured, wherever possible, between this Directive and Directive (EU) 2022/2555 of the European Parliament and of the Council [(5)]. In light of the higher frequency and particular characteristics of cyber risks, Directive (EU) 2022/2555 imposes comprehensive requirements on a large set of entities to ensure their cybersecurity. Given that cybersecurity is addressed

[5] 欧州全域の共通の高いレベルのサイバーセキュリティのための措置に関する，規則(EU) No 910/2014 及び指令(EU) 2018/1972 を改正し，並びに，指令(EU) 2016/1148 を廃止する欧州議会及び理事会の 2022 年 12 月 14 日の指令(EU) 2022/2555（NIS2 指令）（この官報の 80 頁参照）.
Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (see page 80 of this Official Journal).

sufficiently in Directive (EU) 2022/2555, the matters covered by that Directive should be excluded from the scope of this Directive, without prejudice to the particular regime for entities in the digital infrastructure sector.

(10) 欧州連合の部門別の法行為の条項が，必須法主体に対し，当該必須法主体の回復力を拡大するための措置を講ずることを求めており，かつ，当該要件が，この指令に定める対応義務と少なくとも均等であることが構成国によって承認されているときは，重複及び無用の負担を避けるため，この指令に定める関連条項を適用してはならない。そのような場合，そのような欧州連合の法行為の関連条項が適用されるべきである。この指令の関連条項が適用されないときは，この指令に定める監督及び執行に関する条項を適用してはならない。

Where provisions of sector-specific Union legal acts require critical entities to take measures to enhance their resilience, and where those requirements are recognised by Member States as at least equivalent to the corresponding obligations laid down in this Directive, the relevant provisions of this Directive should not apply, so as to avoid duplication and unnecessary burden. In that case, the relevant provisions of such Union legal acts should apply. Where the relevant provisions of this Directive do not apply, the provisions on supervision and enforcement laid down in this Directive should not apply either.

(11) この指令は，行政上の自律性の面における構成国及びその機関の能力に対し，または，国家安全保障及び国防を守る構成国及びその機関の職責に対し，または，それら以外の必須の国家機能を防護するためのその構成国及びその機関の権限に対し，とりわけ，公共の保安，領土の完全性及び法と秩序の維持に関する権限に対し，影響を与えない。この指令の適用範囲からの行政機関である法主体の除外は，当該法主体の活動が，主として，国家安全保障，公共の保安，国防の分野，または，犯罪行為の捜査，検知及び訴追を含め，法執行の分野において遂行される法主体に対して適用されるべきである。ただし，その活動が当該分野と僅かに関連するだけの行政機関である法主体は，この指令の適用範囲内にあるべきである。この指令の目的のために，規制の職務権限のある法主体は，法執行の分野における活動を遂行しているとは判断されず，それゆえ，当該根拠によっては，この指令の適用範囲から除外されない。国際協定に従って第三国と共同で設置されている行政機関である法主体は，この指令の適用範囲から除外される。この指令は，構成国の第三国における外交の職務及び領事館の職務には適用されない。

This Directive does not affect the competence of Member States and their authorities in terms of administrative autonomy or their responsibility for safeguarding national security and defence or their power to safeguard other essential State functions, in particular concerning public security, territorial integrity and the maintenance of law and order. The exclusion of public administration entities from the scope of this Directive should apply to entities whose activities are predominantly carried out in the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences. However, public administration entities whose activities are only marginally related to those areas should fall within the scope of this Directive. For the purposes of this Directive, entities with regulatory competences are not considered to be carrying out activities in the area

of law enforcement and are therefore not excluded on that ground from the scope of this Directive. Public administration entities that are jointly established with a third country in accordance with an international agreement are excluded from the scope of this Directive. This Directive does not apply to Member States' diplomatic and consular missions in third countries.

一定の必須法主体は，国家安全保障，公共の保安，国防の分野，または，犯罪行為の捜査，検知及び訴追を含め，法執行の分野において活動を遂行し，または，専らそれらの分野において活動を遂行する行政機関である法主体に対してサービスを提供する。国家安全保障及び国防を守る構成国の職責に照らし，当該必須法主体が提供するサービスまたは当該必須法主体が遂行する活動が，主として，国家安全保障，公共の保安，国防の分野，または，犯罪行為の捜査，検知及び訴追を含め，法執行の分野と関連するときは，構成国は，当該必須法主体に対し，この指令に定める必須法主体の義務の全部または一部が適用されないことを決定できるべきである。そのサービスまたは活動が当該分野と僅かに関連するだけの必須法主体は，この指令の適用範囲内にあるべきである。いかなる構成国も，その情報を開示することがその構成国の国家安全保障という必須の利益と矛盾するような情報を供給することを求められてはならない。機密情報の保護に関する欧州連合の規定または国内規定及び不開示合意が適切である。

Certain critical entities carry out activities in the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences, or provide services exclusively to public administration entities that carry out activities predominantly in those areas. In light of the Member States' responsibility for safeguarding national security and defence, Member States should be able to decide that the obligations on critical entities laid down in this Directive do not apply, in whole or in part, to those critical entities if the services they provide or the activities they perform are predominantly related to the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences. Critical entities whose services or activities are only marginally related to those areas should fall within the scope of this Directive. No Member State should be required to supply information the disclosure of which would be contrary to the essential interests of its national security. Union or national rules for the protection of classified information and non-disclosure agreements are of relevance.

(12) 国家安全保障または必須法主体の防護及び商業上の利益を危険に晒さないため，機微の情報は，慎重に，かつ，使用される送信経路及び記録保存能力に対して特別の注意を払って，アクセスされ，交換され，そして，取扱われるべきである。

In order not to jeopardise national security or the security and commercial interests of critical entities, sensitive information should be accessed, exchanged and handled prudently and with particular attention to the transmission channels and storage capacities used.

(13) 必須法主体の回復力に向けた包括的なアプローチを確保するという観点から，各構成国は，必須法主体の回復力を拡大するための戦略（「戦略」）を設けるべきである。戦略は，戦略上の目標

及び実装される政策上の措置を定めるべきである。一貫性及び効率性の利益において，その戦略は，それが可能な限り，既存の国内戦略及び部門別戦略，計画または類似の文書を基礎として，既存の基本方針を継ぎ目なく統合するために設計されるべきである。包括的なアプローチを達成するため，構成国は，当該構成国の戦略が，サイバーセキュリティ上のリスク，サイバーな脅威及びサイバーなインシデント，並びに，非サイバーなリスク，脅威及びインシデントに関する情報交換の過程において，そして，監督の職務の執行の過程において，この指令の下にある職務権限のある機関と指令(EU) 2022/2555 の下にある職務権限のある機関との間の拡大された調整の政策枠組みを定めることを確保すべきである。当該構成国の戦略を設ける際，構成国は，必須法主体に対するハイブリッドな性質の脅威を適切に考慮に入れるべきである。

With a view to ensuring a comprehensive approach to the resilience of critical entities, each Member State should have in place a strategy for enhancing the resilience of critical entities (the 'strategy'). The strategy should set out the strategic objectives and policy measures to be implemented. In the interests of coherence and efficiency, the strategy should be designed to seamlessly integrate existing policies, building, wherever possible, upon relevant existing national and sectoral strategies, plans or similar documents. In order to achieve a comprehensive approach, Member States should ensure that their strategies provide for a policy framework for enhanced coordination between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2555 in the context of information sharing on cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents and in the context of the exercise of supervisory tasks. When putting in place their strategies, Member States should take due account of the hybrid nature of threats to critical entities.

(14) とりわけ，国内レベルにおける必須法主体の回復力に向けた政策上のアプローチに関するこの指令の正確な適用を欧州委員会が評価できるようにするため，構成国は，欧州委員会に対し，当該構成国の戦略を通知し，かつ，同戦略の実質的に意味のあるアップデートを通知すべきである。それが必要なときは，戦略は，機密情報として通知され得る。欧州委員会は，必須法主体回復力グループの枠組み内におけるベストプラクティスと共通の利害のある問題を発見するための交換の基礎として提供するため，構成国から通知された戦略の要旨報告書を作成すべきである。機密であるか否かを問わず，要旨報告書の中に含まれる集約された情報の機微な性質のゆえに，欧州委員会は，必須法主体，構成国及び欧州連合の防護に関して適切なレベルの注意を払ってその要旨報告書を管理すべきである。要旨報告書及び戦略は，違法な行為または悪意ある行為から安全確保されるべきであり，かつ，この指令の目的を満たすための権限のある者に限りアクセス可能であるべきである。戦略及び同戦略の実質的に意味のあるアップデートの通知は，欧州委員会が，必須法主体の回復力に向けたアプローチの発展を欧州委員会が理解し，そして，この指令の影響及び付加価値の監視の中にフィードすることも助けるべきである。欧州委員会は，それらを定期的に見直すべきである。

Member States should communicate their strategies and substantial updates thereto to the Commission, in particular to enable the Commission to assess the correct application of this Directive as regards policy approaches to the resilience of critical entities at national level. Where necessary, the strategies could be

communicated as classified information. The Commission should draw up a summary report of the strategies communicated by Member States to serve as a basis for exchanges to identify best practices and issues of common interest in the framework of a Critical Entities Resilience Group. Due to the sensitive nature of the aggregated information included in the summary report, whether classified or not, the Commission should manage the summary report with the appropriate level of awareness with respect for the security of critical entities, Member States and the Union. The summary report and the strategies should be safeguarded against unlawful or malicious action and should be accessible only to authorised persons in order to fulfil the objectives of this Directive. The communication of the strategies and substantial updates thereto should also help the Commission to understand developments in approaches to the resilience of critical entities and feed into the monitoring of the impact and added value of this Directive, which the Commission is to review periodically.

(15) 必須法主体を識別するため及び必須法主体の回復力を確保することを助けるための構成国の活動は，重要な社会機能または経済活動の遂行能力と最も関連性のある法主体に焦点を当てるリスクベースのアプローチに従うべきである。そのような的を絞ったアプローチを確保するため，各構成国は，整合化された枠組み内において，部門横断の性質または国境を越える性質をもつリスクを含め，関連する自然のリスク及び人為的なリスクであって，事故，自然災害，パンデミックのような公衆衛生上の緊急事態を含め，必須サービスの提供に影響を与え得るものの評価，並びに，テロリスト行為，犯罪的な潜入及び犯罪的な妨害を含め，ハイブリッドな脅威またはそれ以外の敵対的な脅威の評価（「構成国リスク評価」）を遂行すべきである。構成国リスク評価を遂行する際，構成国は，欧州連合の他の法行為によって遂行される別の一般的なリスク評価及び部門に特化したリスク評価を考慮に入れるべきであり，かつ，別の構成国及び第三国内の諸部門に関するものを含め，諸部門が相互に依存している程度を判断すべきである。構成国リスク評価の結果は，必須法主体を識別する目的のため，及び，当該必須法主体の回復力の要件の適合において当該必須法主体を補助する目的のために使用されるべきである。この指令は，構成国及び欧州連合内で業務運営する必須法主体に対してのみ適用される。ただし，とりわけリスク評価を通じて職務権限のある機関によって生成された専門知識及び知識並びにとりわけ様々な形態の支援及び協力を通じて欧州委員会によって生成された専門知識及び知識は，それが適切なときは，かつ，適用可能な法律文書に従って，回復力に関する既存の協力の中にフィードすることによって，第三国の利益のために，とりわけ欧州連合の直接の隣国の利益のために使用され得る。

The actions of Member States to identify and help ensure the resilience of critical entities should follow a risk-based approach that focuses on the entities most relevant for the performance of vital societal functions or economic activities. In order to ensure such a targeted approach, each Member State should carry out, within a harmonised framework, an assessment of the relevant natural and man-made risks, including those of a cross-sectoral or cross-border nature, that could affect the provision of essential services, including accidents, natural disasters, public health emergencies such as pandemics and hybrid threats or other antagonistic threats, including terrorist offences, criminal infiltration and sabotage (‘Member State risk assessment’). When carrying out Member State risk assessments, Member States should take into account other general or sector-specific risk assessments carried out pursuant to other

Union legal acts and should consider the extent to which sectors depend on one another, including on sectors in other Member States and third countries. The outcome of Member State risk assessments should be used for the purposes of identifying critical entities and assisting those entities in meeting their resilience requirements. This Directive applies only to Member States and critical entities that operate within the Union. Nevertheless, the expertise and knowledge generated by competent authorities, in particular through risk assessments, and by the Commission, in particular through various forms of support and cooperation, could be used, where appropriate and in accordance with the applicable legal instruments, for the benefit of third countries, in particular those in the direct neighbourhood of the Union, by feeding into existing cooperation on resilience.

(16) 関連する全ての法主体が，この指令の回復力の要件に服することを確保し，その点に関する格差の削減するため，国内レベルにおける当該必須法主体の役割と重要性を構成国が適切に反映できるようにもしつつ，欧州連合全域にわたる必須法主体の一貫性のある識別ができるようにする整合化された規定を定めることが重要である。この指令に定める基準を適用する際，各構成国は，1 または複数の必須サービスを提供する法主体，及び，その構成国の領土上に所在する重要インフラを運用及び保有している法主体を識別すべきである。法主体は，当の 1 または複数の必須サービスのために必要な活動をその法主体が遂行しており，かつ，当該 1 または複数のサービスを提供するために使用される当該法主体の重要インフラが所在する構成国の領土上で業務運営していると判断されるべきである。構成国内においてそれらの基準に適合する法主体が存在しないときは，当該構成国は，対応する部門または副部門の中にある必須法主体を識別する義務を負わされてはならない。実効性，効率性，一貫性及び法的確実性の利益において，構成国が必須法主体として識別した法主体の通知に関し，適切な規定が定められるべきである。

In order to ensure that all relevant entities are subject to the resilience requirements of this Directive and to reduce divergences in that respect, it is important to lay down harmonised rules allowing for a consistent identification of critical entities across the Union, while also allowing Member States to adequately reflect the role and importance of those entities at national level. When applying the criteria laid down in this Directive, each Member State should identify entities that provide one or more essential services and that operate and have critical infrastructure located on its territory. An entity should be considered to operate on the territory of a Member State in which it carries out activities necessary for the essential service or services in question and in which that entity's critical infrastructure, which is used to provide that service or those services, is located. Where no entity meets those criteria in a Member State, that Member State should be under no obligation to identify a critical entity in the corresponding sector or subsector. In the interests of effectiveness, efficiency, consistency and legal certainty, appropriate rules should be established as regards notifying entities that they have been identified as critical entities.

(17) 構成国は，欧州委員会に対し，この指令の目的を満たす態様で，必須法主体のリスト，別紙に定めるそれぞれの部門及び副部門毎に，及び，個々の法主体が提供する 1 または複数の必須サービス毎に識別された必須法主体の数，並びに，それが適用されるときは，閾値を提出すべきである。閾値をそのようなものとして，または，集約された形態で提出することが可能であるべきであ

り，そのことは，その情報が，地理的領域毎に，年毎に，部門毎に，副部門毎に，または，他の手段毎に平均化され得ること，そして，提供される指標の幅に関する情報を含め得ることを意味する。

Member States should submit to the Commission, in a manner that fulfils the objectives of this Directive, a list of essential services, the number of critical entities identified for each of the sectors and subsectors set out in the Annex and for the essential service or services that each entity provides and, if applied, thresholds. It should be possible to present thresholds as such or in aggregated form, meaning that the information can be averaged by geographic area, by year, by sector, by subsector or by other means, and can include information on the range of the indicators provided.

(18) インシデントによってつくり出される混乱の影響の大きさを判定するための基準が定められるべきである。当該基準は，欧州議会及び理事会の指令(EU) 2016/1148[6]に定義する基礎サービスの運営者を識別するために構成国によって遂行された努力及びその点に関して得られた経験を活かすため，同指令に定める基準を基礎とすべきである。COVID-19 パンデミックのような大規模な危機は，サプライチェーンのセキュリティを確保することの重要性を証明し，また，サプライチェーンの混乱が，多数の部門を横断し，国境を越えて，経済的及び社会的な負の影響をどのようにもち得るかを明らかにした。それゆえ，構成国は，別の部門及び副部門が必須法主体から提供される必須サービスに依存する程度を判定する際，可能な範囲内で，サプライチェーンに対する影響も判断すべきである。

Criteria should be established to determine the significance of a disruptive effect produced by an incident. Those criteria should build on the criteria set out in Directive (EU) 2016/1148 of the European Parliament and of the Council[(6)] in order to capitalise on the efforts carried out by Member States to identify operators of essential services as defined in that Directive and the experience gained in that regard. Major crises, such as the COVID-19 pandemic, have shown the importance of ensuring the security of the supply chain and have demonstrated how its disruption can have a negative economic and societal impact across a large number of sectors and across borders. Therefore, Member States should also consider effects on the supply chain, to the extent possible, when determining the extent to which other sectors and subsectors depend on the essential service provided by a critical entity.

(19) 欧州連合内への外国からの直接投資の審査のための枠組みを設ける欧州議会及び理事会の規則(EU) 2019/452[7]を含め，適用可能な欧州連合法及び国内法に従い，サービス，経済及び欧州

---

[6] 欧州連合全域におけるネットワーク及び情報システムの共通の高いレベルのセキュリティのための措置に関する欧州議会及び理事会の 2016 年 7 月 6 日の指令(EU) 2016/1148 (OJ L 194, 19.7.2016, p. 1).
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

[7] 欧州連合内への外国の直接投資の審査のための枠組みを設ける欧州議会及び理事会の 2019 年 3 月 19 日の規則(EU) 2019/452 (OJ L 79 I, 21.3.2019, p. 1).
Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (OJ L 79 I, 21.3.2019, p. 1).

連合の市民の支障のない移動と安全は重要インフラの適正な稼働に依存しているので，欧州連合内にある重要インフラの外国保有によって示される潜在的な脅威が認識されるべきである。

In accordance with applicable Union and national law, including Regulation (EU) 2019/452 of the European Parliament and of the Council [7], which establishes a framework for the screening of foreign direct investments in the Union, the potential threat posed by foreign ownership of critical infrastructure within the Union is to be acknowledged because services, the economy and the free movement and safety of Union citizens depend on the proper functioning of critical infrastructure.

(20) 指令(EU) 2022/2555 は，デジタルインフラ部門に属し，この指令の下において必須法主体として識別され得るような法主体に対し，ネットワーク及び情報システムの防護に対して示されたリスクを管理するための適切かつ比例的な技術上の措置，業務運営上の措置及び組織上の措置を講ずること，並びに，重大なインシデント及びサイバーな脅威を通知することを求めている。ネットワーク及び情報システムの防護に対する脅威は異なる起源をもち得るので，指令(EU) 2022/2555 は，ネットワーク及び情報システム並びに当該システムの物理的な構成要素及び環境の回復力を含むオールハザードアプローチを適用する。

Directive (EU) 2022/2555 requires entities belonging to the digital infrastructure sector, which might be identified as critical entities under this Directive, to take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems and to notify significant incidents and cyber threats. Since threats to the security of network and information systems can have different origins, Directive (EU) 2022/2555 applies an all-hazards approach that includes the resilience of network and information systems, as well as the physical components and environment of those systems.

この点に関して指令(EU) 2022/2555 に定める要件がこの指令に定める対応する義務と少なくとも均等であることに鑑み，重複及び無用な管理運営上の負担を避けるため，この指令の第 11 条並びに第Ⅲ章，第Ⅳ章及び第Ⅵ章に定める義務は，デジタルインフラ部門に属する法主体に対して適用してはならない。ただし，デジタルインフラ部門に属する法主体によって他の全ての部門に属する必須法主体に対して提供されるサービスの重要性を考慮し，構成国は，この指令に定める基準を基礎とし，この指令に定める手続を用いて，デジタルインフラ部門に属する法主体を必須法主体として識別すべきである。その結果として，戦略，構成国リスク評価及びこの指令の第Ⅱ章に定める支援の措置が適用されるべきである。構成国は，当該条項が，適用可能な欧州連合法と一貫性があることを条件として，当該必須法主体に関し，より高いレベルの回復力を達成するための国内法の条項を採択または維持できるべきである。

Given that the requirements laid down in Directive (EU) 2022/2555 in that regard are at least equivalent to the corresponding obligations laid down in this Directive, the obligations laid down in Article 11 and Chapters III, IV and VI of this Directive should not apply to entities belonging to the digital infrastructure sector in order to avoid duplication and unnecessary administrative burden. However, considering the

importance of the services provided by entities belonging to the digital infrastructure sector to critical entities belonging to all other sectors, Member States should identify, based on the criteria and using the procedure provided for in this Directive, entities belonging to the digital infrastructure sector as critical entities. Consequently, the strategies, the Member State risk assessments and the support measures set out in Chapter II of this Directive should apply. Member States should be able to adopt or maintain provisions of national law to achieve a higher level of resilience for those critical entities, provided that those provisions are consistent with applicable Union law.

(21) 欧州連合の金融サービス法は，金融の法主体に対し，業務運営上のリスクを含め，当該金融の法主体が直面する全てのリスクを管理し，かつ，事業継続性を確保すべき包括的な要件を設けている。そのような法律は，欧州議会及び理事会の規則(EU) No 648/2012[8]，規則(EU) No 575/2013[9]及び規則(EU) No 600/2014[10]，並びに，欧州議会及び理事会の指令 2013/36/EU[11]及び指令 2014/65/EU[12]を含む。当該法的枠組みは，金融の法主体に適用可能な，物理的な ICT インフラの保護に関するリスクを含め，情報通信技術（ICT）のリスクを管理すべき要件を定める欧州議会及び理事会の規則(EU) 2022/2554[13]によって補完される。それゆえ，当該法主体の回復力が包括的

[8] OTC デリバティブ，中央清算機関及び取引情報蓄積機関に関する欧州議会及び理事会の 2012 年 7 月 4 日の規則(EU) No 648/2012 (OJ L 201, 27.7.2012, p. 1).
Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

[9] 与信機関の健全性要件に関する及び規則(EU) No 648/2012 を改正する欧州議会及び理事会の 2013 年 6 月 26 日の規則(EU) No 575/2013 (OJ L 176, 27.6.2013, p. 1).
Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

[10] 金融商品の市場に関する及び規則(EU) No 648/2012 を改正する欧州議会及び理事会の 2014 年 5 月 15 日の規則(EU) No 600/2014 (OJ L 173, 12.6.2014, p. 84).
Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (OJ L 173, 12.6.2014, p. 84).

[11] 与信機関の活動へのアクセス並びに与信機関及び投資企業の健全性監督に関する，指令 2002/87/EC を改正する，並びに，指令 2006/48/EC 及び指令 2006/49/EC を廃止する欧州議会及び理事会の 2013 年 6 月 26 日の指令 2013/36/EU (OJ L 176, 27.6.2013, p. 338).
Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

[12] 金融商品市場に関する並びに指令 2002/92/EC 及び指令 2011/61/EU を改正する欧州議会及び理事会の 2014 年 5 月 15 日の指令 2014/65/EU (OJ L 173, 12.6.2014, p. 349).
Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

[13] 金融部門のデジタル業務運営回復力に関する，並びに，規則(EC) No 1060/2009，規則(EU) No 648/2012，規則(EU) No 600/2014，規則(EU) No 909/2014 及び規則(EU) 2016/1011 を改正する欧州議会及び理事会の 2022 年 12 月 14 日の規則(EU) 2022/2554（この官報の 1 頁参照）.
Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (see page 1 of this Official Journal).

に包摂されているので，重複及び無用な管理運営上の負担を避けるため，この指令の第 11 条並びに第III章，第IV章及び第VI章は，当該法主体に対して適用してはならない。

Union financial services law establishes comprehensive requirements on financial entities to manage all risks they face, including operational risks, and to ensure business continuity. Such law includes Regulations (EU) No 648/2012 [8], (EU) No 575/2013 [9] and (EU) No 600/2014 [10] of the European Parliament and of the Council and Directives 2013/36/EU [11] and 2014/65/EU [12] of the European Parliament and of the Council. That legal framework is complemented by Regulation (EU) 2022/2554 of the European Parliament and of the Council [13], which lays down requirements applicable to financial entities to manage Information and Communication Technology (ICT) risks, including concerning the protection of physical ICT infrastructure. Since the resilience of those entities is therefore comprehensively covered, Article 11 and Chapters III, IV and VI of this Directive should not apply to those entities in order to avoid duplication and unnecessary administrative burden.

ただし，金融部門にある法主体から他の全ての部門に属する必須法主体に対して提供されるサービスの重要性を考慮し，構成国は，この指令に定める基準を基礎とし，この指令に定める手続を用いて，金融部門にある法主体を必須法主体として識別すべきである。その結果として，戦略，構成国リスク評価及びこの指令の第 II 章に定める支援の措置が適用されるべきである。構成国は，当該条項が，適用可能な欧州連合法と一貫性があることを条件として，当該必須法主体に関し，より高いレベルの回復力を達成するための国内法の条項を採択または維持できるべきである。

However, considering the importance of the services provided by entities in the financial sector to critical entities belonging to all other sectors, Member States should identify, based on the criteria and using the procedure provided for in this Directive, entities in the financial sector as critical entities. Consequently, the strategies, the Member State risk assessments and the support measures set out in Chapter II of this Directive should apply. Member States should be able to adopt or maintain provisions of national law to achieve a higher level of resilience for those critical entities provided that those provisions are consistent with applicable Union law.

(22) 構成国は，この指令の規定の適用の監督する職務権限のある機関，及び，それが必要なときは，この指令の規定を執行する職務権限のある機関を指定または設置し，かつ，当該職務権限のある機関が，適切に権限を与えられ，かつ，資源を与えられることを確保すべきである。国内統治構造の相違に照らし，既存の部門別の手立てまたは欧州連合の監督組織及び規制組織を守るため，そして，重複を避けるため，構成国は，複数の職務権限のある機関を指定または設置し得るべきである。構成国が複数の職務権限のある機関を指定または設置するときは，当該構成国は，関係する機関それぞれの権限を明確に定義し，かつ，当該職務権限のある機関が円滑かつ実効的に協力することを確保すべきである。全ての職務権限のある機関は，欧州連合レベル及び国内レベルで，他の関連する機関とより一般的にも協力すべきである。

Member States should designate or establish authorities competent to supervise the application of and,

where necessary, enforce the rules of this Directive and ensure that those authorities are adequately empowered and resourced. In light of the differences in national governance structures, in order to safeguard existing sectoral arrangements or Union supervisory and regulatory bodies, and in order to avoid duplication, Member States should be able to designate or establish more than one competent authority. Where Member States designate or establish more than one competent authority, they should clearly delineate the respective tasks of the authorities concerned and ensure that they cooperate smoothly and effectively. All competent authorities should also cooperate more generally with other relevant authorities, at both Union and national level.

(23) 国境を越える協力及び通信を容易にするため，また，この指令の実効的な実装ができるようにするため，各構成国は，欧州連合の部門別の法行為の要件を妨げることなく，必須法主体の回復力と関連する問題並びに欧州連合レベルの国境を越える協力と関連する問題の調整に関して職責を負う 1 つの単一連絡部局（「単一連絡部局」）を指定し，それが適切なときは，職務権限のある機関の中で指定すべきである。各単一連絡部局は，それが適切なときは，当該単一連絡部局の構成国の職務権限のある機関との間，別の構成国の単一連絡部局との間，及び，必須法主体回復力グループとの間で連絡をとり，かつ，通信を調整すべきである。

In order to facilitate cross-border cooperation and communication and to enable the effective implementation of this Directive, each Member State should, without prejudice to the requirements of sector-specific Union legal acts, designate one single point of contact responsible for coordinating issues related to the resilience of critical entities and cross-border cooperation at Union level (‘single point of contact’), where relevant within a competent authority. Each single point of contact should liaise and coordinate communication, where relevant, with the competent authorities of its Member State, with the single points of contact of other Member States and with the Critical Entities Resilience Group.

(24) この指令の下にある職務権限のある機関と指令(EU) 2022/2555 の下にある職務権限のある機関は，必須法主体に対して影響を与えるサイバーセキュリティ上のリスク，サイバーな脅威及びサイバーなインシデント，並びに，非サイバーなリスク，脅威及びインシデントとの関係において，並びに，この指令の下にある職務権限のある機関及び指令(EU) 2022/2555 の下にある職務権限のある機関によって講じられた関連措置と関連して，協力し，かつ，情報を交換すべきである。この指令に定める要件と指令(EU) 2022/2555 に定める要件が補完的な態様で実装されること，そして，必須法主体が，この指令の目的及び指令(EU) 2022/2555 の目的を達成するために必要なところを超える管理運営上の負担に服さないことを構成国が確保することが重要である。

The competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2555 should cooperate and exchange information in relation to cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents affecting critical entities as well as in relation to relevant measures taken by competent authorities under this Directive and competent authorities under Directive (EU) 2022/2555. It is important that Member States ensure that the requirements provided for in this Directive and in Directive (EU) 2022/2555 are implemented in a

complementary manner and that critical entities are not subject to an administrative burden beyond that which is necessary to achieve the objectives of this Directive and that Directive.

(25) 構成国は，当該必須法主体の回復力を強化する際，この指令に定める構成国の義務を遵守し，そのような遵守を確保すべき必須法主体自身の法律上の責任を妨げることなく，小企業または中規模企業として分類される必須法主体を含め，必須法主体を支援すべきであり，かつ，そのようにする際，過剰な管理運営上の負担を避けるべきである。とりわけ，構成国は，ガイド資料及び手法を作成し，必須法主体の回復力を試すための演習の計画を支援し，かつ，必須法主体の要員に対して助言と訓練を提供し得る。それが必要であり，かつ，公共の利益の目的によって正当化されるときは，構成国は，資金を提供し得るものとし，かつ，欧州連合の機能に関する条約（TFEU）に定める競争の規定の適用を妨げることなく，必須法主体間の任意の情報共有及びグッドプラクティスの交換を促進すべきである。

Member States should support critical entities, including those that qualify as small or medium-sized enterprises, in strengthening their resilience, in compliance with Member State obligations laid down in this Directive, without prejudice to the critical entities' own legal responsibility to ensure such compliance and, in so doing, prevent excessive administrative burden. Member States could, in particular, develop guidance materials and methodologies, support the organisation of exercises to test the resilience of critical entities and provide advice and training to the personnel of critical entities. Where necessary and justified by public interest objectives, Member States could provide financial resources and should facilitate voluntary information sharing and the exchange of good practices between critical entities, without prejudice to the application of competition rules laid down in the Treaty on the Functioning of the European Union (TFEU).

(26) 構成国によって識別された必須法主体の回復力を拡大することを狙いとし，かつ，当該必須法主体にかかる管理運営上の負担を削減するため，職務権限のある機関は，それが適切なときは，この指令が一貫性のある態様で適用されることを確保する目的のために，相互に意見聴取すべきである。当該意見聴取は，いずれかの利害関係のある職務権限のある機関の要請により開始されるべきであり，複数の構成国の間で物理的に結び付けられた重要インフラを使用する相互関連のある必須法主体に関し，同一のグループまたは共同構造体に属する相互関連のある必須法主体に関し，または，1 つの構成国の中で識別され，かつ，別の構成国に対しまたは別の構成国の中で必須サービスを提供する相互関連のある必須法主体に関し，収斂的なアプローチを確保することに焦点を当てるべきである。

With the aim of enhancing the resilience of critical entities identified by Member States and in order to reduce the administrative burden on those critical entities, the competent authorities should consult one another, whenever appropriate, for the purpose of ensuring that this Directive is applied in a consistent manner. Those consultations should be entered into at the request of any interested competent authority and should focus on ensuring a convergent approach regarding interlinked critical entities that use critical infrastructure which is physically connected between two or more Member States, that belong to the same

groups or corporate structures, or that have been identified in one Member State and that provide essential services to or in other Member States.

(27) 欧州連合法または国内法の条項が，必須法主体に対し，この指令の目的のために関連するリスクを評価すること，及び，当該必須法主体自身の回復力を確保するための措置を講ずることを求めているときは，当該要件は，必須法主体によるこの指令の遵守を監督する目的のために，適切に判断されるべきである。

Where provisions of Union or national law require critical entities to assess risks relevant for the purposes of this Directive and to take measures to ensure their own resilience, those requirements should be adequately considered for the purpose of supervising the compliance of critical entities with this Directive.

(28) 必須法主体は，当該必須法主体が晒されている関連リスクと当該リスクを分析すべき義務の包括的な理解をもつべきである。その目的のために，当該必須法主体は，当該必須法主体の特別な状況及び当該リスクの進化を考慮して必要があるときはいつでも，かつ，いかなる場合においても 4 年毎に，当該必須法主体の必須サービスの提供を混乱させ得る全ての関連リスクを評価するためのリスク評価（「必須法主体リスク評価」）を遂行すべきである。必須法主体が，別のリスク評価を遂行したとき，または，当該必須法主体の必須法主体リスク評価と関連する別の法行為の中で定められた義務により文書を作成したときは，当該必須法主体は，この指令に定める必須法主体リスク評価と関係する要件に適合するために，当該評価及び文書を利用できるべきである。職務権限のある機関は，関連リスクに対処する必須法主体によって遂行された，関連リスク及び関連する依存性の程度に対処する現行のリスク評価が，その全部または一部において，この指令に定める義務を遵守していることを宣言できるべきであるべきである。

Critical entities should have a comprehensive understanding of the relevant risks to which they are exposed and a duty to analyse those risks. To that end, they should carry out risk assessments whenever necessary in view of their particular circumstances and the evolution of those risks and, in any event, every four years, in order to assess all relevant risks that could disrupt the provision of their essential services (‘critical entity risk assessment’). Where critical entities have carried out other risk assessments or drawn up documents pursuant to obligations laid down in other legal acts that are relevant for their critical entity risk assessment, they should be able to use those assessments and documents to meet the requirements set out in this Directive concerning critical entity risk assessments. A competent authority should be able to declare that an existing risk assessment carried out by a critical entity that addresses the relevant risks and the relevant extent of dependence is compliant, in whole or in part, with the obligations laid down in this Directive.

(29) 必須法主体は，インシデントを防止し，インシデントから保護し，インシデントに対応し，インシデントに抗し，インシデントを緩和し，インシデントを吸収し，インシデントを封じ込め，そして，インシデントから復旧するための適切かつ比例的な技術上の措置，防護上の措置及び組織上の措置を講ずるべきである。必須法主体は，この指令に従って当該措置を講ずるべきであるが，そのよ

うな措置の細目及び範囲は，その必須法主体の必須法主体リスク評価の一部として個々の必須法主体が識別した異なるリスク及びそのような法主体の特殊性を，適切かつ比例的な方法で反映すべきである。欧州連合の一貫性のあるアプローチを促進するため，欧州委員会は，必須法主体回復力グループの意見聴取を経た上で，それらの技術上の措置，防護上の措置及び組織上の措置の細目を定める拘束力のない指針を採択すべきである。構成国は，各必須法主体が，職務権限のある機関との間の連絡場所として，連絡担当者またはそれと均等な者を指定することを確保すべきである。

Critical entities should take technical, security and organisational measures that are appropriate and proportionate to the risks they face so as to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident. While critical entities should take those measures in accordance with this Directive, the details and extent of such measures should reflect the different risks that each critical entity has identified as part of its critical entity risk assessment and the specificities of such entity in an appropriate and proportionate way. To promote a coherent Union approach, the Commission should, after consulting the Critical Entities Resilience Group, adopt non-binding guidelines to further specify those technical, security and organisational measures. Member States should ensure that each critical entity designate a liaison officer or equivalent as point of contact with the competent authorities.

(30) 実効性及び説明責任の利益において，必須法主体は，回復力計画の中で，または，回復力計画と均等な 1 または複数の文書の中で，識別されたリスクを考慮し，実効性及び説明責任という狙いを十分に達成するレベルの詳細度で，当該必須法主体が講ずる措置を説明し，かつ，当該計画を実際に適用すべきである。必須法主体が，技術上の措置，防護上の措置及び組織上の措置を既に講じており，かつ，この指令の下にある回復力拡大措置と関連する別の法行為による文書を作成しているときは，重複を避けるため，その必須法主体は，この指令の下にある回復力の措置と関連する要件に適合するために，当該措置及び文書を使用できるべきである。重複を避けるため，職務権限のある機関は，この指令による技術上の措置，防護上の措置及び組織上の措置を講ずるべきその必須法主体の義務に対処する必須法主体によって講じられた既存の回復力の措置が，その全部または一部において，この指令に定める義務を遵守しているとして，宣言できるべきである。

In the interests of effectiveness and accountability, critical entities should describe the measures they take, with a level of detail that sufficiently achieves the aims of effectiveness and accountability, having regard to the risks identified, in a resilience plan or in a document or documents that are equivalent to a resilience plan, and apply that plan in practice. Where a critical entity has already taken technical, security and organisational measures and drawn up documents pursuant to other legal acts that are relevant for resilience-enhancing measures under this Directive, it should be able, in order to avoid duplication, to use those measures and documents to meet the requirements as regards resilience measures under this Directive. In order to avoid duplication, a competent authority should be able to declare existing resilience measures taken by a critical entity that address its obligation to take technical, security and organisational

measures pursuant to this Directive as compliant, in whole or in part, with the requirements of this Directive.

(31) 欧州議会及び理事会の規則(EC) No 725/2004[14]及び規則(EC) No 300/2008[15]並びに欧州議会及び理事会の指令 2005/65/EC[16]は，違法な行為によって生ずるインシデントを防止するため，及び，そのようなインシデントの結果に抗し及びそれを緩和するための，航空部門及び海上輸送部門の組織に対して適用可能な要件を定めている。この指令の下において求められる措置は，対処されるリスク及び講じられる措置のタイプの面において広範であるが，当該部門の必須法主体は，それらの欧州連合の別の法行為によって講じられた措置を，当該必須法主体の回復力計画またはそれと均等な文書の中に反映すべきである。必須法主体は，欧州議会及び理事会の指令 2008/96/EC[17]も考慮に入れるべきである。同指令は，既存の道路または道路区間の現地視察を基礎として，事故や負傷のリスクを増加させる危険な条件，欠点及び問題を発見するために，事故のリスクを地図化するための道路網全体の道路評価，及び，的を絞った道路安全検査を導入する。必須法主体の保護及び回復力を確保することは，鉄道部門にとっては最も重要なことであり，この指令に基づく回復力の措置を実装する際，必須法主体は，委員会決定 2018/C 232/03[18]によって設置された EU 鉄道旅客防護プラットフォームのような，部門別のワークストリームの下で策定された拘束力のない指針及びグッドプラクティスの文書を参照することが推奨される。

Regulations (EC) No 725/2004 (14) and (EC) No 300/2008 (15) of the European Parliament and of the Council and Directive 2005/65/EC of the European Parliament and of the Council (16) establish requirements applicable to entities in the aviation and maritime transport sectors to prevent incidents caused by unlawful acts and to resist and mitigate the consequences of such incidents. While the measures

---

14 船舶及び港湾施設の防護の拡大に関する欧州議会及び理事会の 2004 年 3 月 31 日の規則(EC) No 725/2004(OJ L 129, 29.4.2004, p. 6).
Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6).

15 民間航空の安全の分野における共通の規定に関する，及び，規則(EC) No 2320/2002 を廃止する欧州議会及び理事会の 2008 年 3 月 11 日の規則(EC) No 300/2008 (OJ L 97, 9.4.2008, p. 72).
Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

16 港湾の防護の拡大に関する欧州議会及び理事会の 2005 年 10 月 26 日の指令 2005/65/EC (OJ L 310, 25.11.2005, p. 28).
Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).

17 道路インフラの安全性の管理に関する欧州議会及び理事会の 2008 年 11 月 19 日の指令 2008/96/EC (OJ L 319, 29.11.2008, p. 59).
Directive 2008/96/EC of the European Parliament and of the Council of 19 November 2008 on road infrastructure safety management (OJ L 319, 29.11.2008, p. 59).

18 EU 鉄道旅客防護プラットフォームを設置する 2018 年 6 月 29 日の委員会決定 2018/C 232/03 (OJ C 232, 3.7.2018, p. 10).
Commission Decision of 29 June 2018 setting up the EU Rail Passenger Security Platform 2018/C 232/03 (OJ C 232, 3.7.2018, p. 10).

required under this Directive are broader in terms of risks addressed and types of measures to be taken, critical entities in those sectors should reflect in their resilience plan or equivalent documents the measures taken pursuant to those other Union legal acts. Critical entities are also to take into consideration Directive 2008/96/EC of the European Parliament and of the Council (17), which introduces a network-wide road assessment to map the risk of accidents and a targeted road safety inspection to identify hazardous conditions, defects and problems that increase the risk of accidents and injuries, based on site visits of existing roads or sections of roads. Ensuring the protection and resilience of critical entities is of the utmost importance for the railway sector and, when implementing resilience measures under this Directive, critical entities are encouraged to refer to non-binding guidelines and good practices documents developed under sectorial workstreams, such as the EU Rail Passenger Security Platform set up by Commission Decision 2018/C 232/03 (18).

(32) 必須法主体の従業者または必須法主体の請負業者が，必須法主体の組織内において加害し，損害を生じさせるために，例えば，当該の者のアクセスの権利を濫用するリスクは，懸念を高めているリスクである。それゆえ，構成国は，適正に根拠づけられる案件において，かつ，構成国リスク評価を考慮に入れた上で，その必須法主体の特定の要員類型内にある者に関し，必須法主体が身辺調査を求める要請書を提出することが認められるための条件を定めるべきである。関連当局が，合理的な時間枠内にそのような要請書を審査し，国内法及び国内手続に従って，並びに，個人データの保護に関する欧州連合法を含め，関連する適用可能な欧州連合法に従って当該申請書を処理することが確保されるべきである。身辺調査の対象となっている者の同一性を確認するため，構成国が，適法可能な法律に従い，パスポート，国民識別カードまたはデジタルの方式による身分証明書のような，同一性の証明を要求することが適切である。

The risk of employees of critical entities or their contractors misusing, for instance, their access rights within the critical entity's organisation to harm and cause damage is of increasing concern. Member States should therefore specify the conditions under which critical entities are permitted, in duly reasoned cases and taking into account Member State risk assessments, to submit requests for background checks on persons falling within specific categories of its personnel. It should be ensured that the relevant authorities assess such requests within a reasonable timeframe and process them in accordance with national law and procedures and relevant and applicable Union law, including on the protection of personal data. In order to corroborate the identity of a person who is the subject of a background check, it is appropriate for Member States to require proof of identity, such as a passport, a national identity card or a digital form of identification, in accordance with applicable law.

身辺調査は，関係する者の犯罪記録の検査を含めるべきである。構成国は，他の構成国によって保有されている犯罪記録から情報を入手する目的のために，理事会枠組み決定 2009/315/JHA[19]に定める手続に従い，及び，それが関連しかつ適用可能なときは，欧州議会及び理事会の

[19] 構成国間における犯罪記録から抽出された情報の交換の組織化及び内容に関する 2009 年 2 月 26 日の理事会枠組み決定 2009/315/JHA (OJ L 93, 7.4.2009, p. 23).

規則(EU) 2019/816[20]に定める手続に従い，欧州犯罪記録情報システムを使用すべきである。枠組み決定 2009/315/JHA の第「3 条第 1 項及び規則(EU) 2019/816 の第 3 条第 5 号に示す中央当局は，枠組み決定 2009/315/JHA の第 8 条第 1 項に従って要請を受領した日から 10 業務日以内に，そのような情報を求める要請に対する回答を提供する。構成国は，それが関連しかつ適用可能なときは，欧州議会及び理事会の規則(EU) 2018/1862[21]によって設置された第二世代シェンゲン情報システム（SIS II），諜報機関の情報，及び，それら以外の，その職位と関係してその必須法主体が身辺調査を要請した職位の仕事と結びつけられた者の適格性を判定するために必要となり得る利用可能な客観的な情報にも依拠し得る。

Background checks should include a check of the criminal records of the person concerned. Member States should use the European Criminal Records Information System in accordance with the procedures set out in Council Framework Decision 2009/315/JHA (19) and, where relevant and applicable, Regulation (EU) 2019/816 of the European Parliament and of the Council (20) for the purpose of obtaining information from criminal records held by other Member States. Member States might also, where relevant and applicable, draw on the Second Generation Schengen Information System (SIS II) established by Regulation (EU) 2018/1862 of the European Parliament and of the Council (21), intelligence and any other objective information available that might be necessary to determine the suitability of the person concerned to work in the position in relation to which the critical entity has requested a background check.

(33) 職務権限のある機関が迅速かつ適切にインシデントに対応できるため，そして，必須法主体が取扱うインシデントの影響，性質，原因及びあり得る結果の包括的な概観をもつため，一定のインシデントの通知のための仕組みが構築されるべきである。必須法主体は，職務権限のある機関に対し，不適切な遅滞なく，必須サービスの提供に対して重大な混乱を発生させるインシデント，または，重大な混乱を発生させる可能性のあるインシデントを通知すべきである。業務運営上その

Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (OJ L 93, 7.4.2009, p. 23).

[20] 欧州犯罪記録情報システムを補完するため，第三国の国民及び無国籍の者に関する構成国保有の前科情報の識別のための集中化されたシステム（ECRIS-TCN）を設置し，規則(EU) 2018/1726 を改正する欧州議会及び理事会の 2019 年 4 月 17 日の規則(EU) 2019/816 (OJ L 135, 22.5.2019, p. 1).

Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 (OJ L 135, 22.5.2019, p. 1).

[21] 警察の協力及び刑事上の法務上の協力の分野におけるシェンゲン情報システム（SIS）の設置，運用及び利用に関する，理事会決定 2007/533/JHA を改正及び廃止し，欧州議会及び理事会の規則(EC) No 1986/2006 及び委員会決定 2010/261/EU を廃止する欧州議会及び理事会の 2018 年 11 月 28 日の規則(EU) 2018/1862 (OJ L 312, 7.12.2018, p. 56).

Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).

ようにすることが不可能な場合を除き，必須法主体は，インシデントに気づいてから遅くとも 24 時間以内に，最初の通知を提出すべきである。最初の通知は，職務権限のある機関に対してそのインシデントに気づかせ，かつ，もし必要であれば，その必須法主体が補助を求めることができるために厳格に必要な情報のみを含めるべきである。そのような通知は，それが可能なときは，そのインシデントの推定される原因を示すべきである。構成国は，当該最初の通知を提出すべき要件が，その必須法主体の優先されるべきインシデントの取扱いと関連する活動の資源を減らすことがないことを確保すべきである。最初の通知は，それが適切なときは，そのインシデントから遅くとも 1 か月以内に，詳細報告書によって事後対応されるべきである。詳細報告書は，最初の通知を補完し，かつ，そのインシデントのより完全な概観を提供すべきである。

A mechanism for the notification of certain incidents should be established to allow the competent authorities to respond to incidents rapidly and adequately and to have a comprehensive overview of the impact, nature, cause and possible consequences of incidents with which the critical entities deal. Critical entities should notify, without undue delay, the competent authorities of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. Unless operationally unable to do so, critical entities should submit an initial notification no later than 24 hours after becoming aware of an incident. The initial notification should only include the information strictly necessary to make the competent authority aware of the incident and allow the critical entity to seek assistance, if required. Such a notification should indicate, where possible, the presumed cause of the incident. Member States should ensure that the requirement to submit that initial notification does not divert the critical entity's resources from activities related to incident handling, which should be prioritised. The initial notification should be followed, where relevant, by a detailed report no later than one month after the incident. The detailed report should complement the initial notification and provide a more complete overview of the incident.

(34) 標準化は，基本的には，市場駆動型のプロセスのままとすべきである。ただし，特定の技術標準の遵守を要求することが適切である状況が，なお存在し得る。構成国は，それが有用なときは，必須法主体に対して適用可能な防護の措置及び回復力の措置と関連する欧州の技術標準及び国際的な技術標準並びに技術仕様の利用を推奨すべきである。

Standardisation should remain primarily a market-driven process. However, there might still be situations in which it is appropriate to require compliance with specific standards. Member States should, where useful, encourage the use of European and international standards and technical specifications relevant to the security and resilience measures applicable to critical entities.

(35) 必須法主体は，次第に相互接続されるようになっているサービス提供とインフラのネットワークの一部として業務運営し，かつ，しばしば，複数の構成国において必須サービスを提供するが，幾つかの必須法主体は，6 以上の構成国に対しまたは 6 以上の構成国内で当該必須法主体が必須サービスを提供していることから，欧州連合及びその域内市場にとって特に重要であり，また，それゆえに，欧州連合レベルの特別の支援を受益し得る。それゆえ，そのような欧州の特別に重

要な必須法主体と関係する諮問機関に関する規定が設けられるべきである。同規定は，この指令に定める監督及び執行に関する規定を妨げない。

While critical entities generally operate as part of an increasingly interconnected network of service provision and infrastructure and often provide essential services in more than one Member State, some of those critical entities are of particular significance for the Union and its internal market because they provide essential services to or in six or more Member States and, therefore, could benefit from specific support at Union level. Rules on advisory missions in respect of such critical entities of particular European significance should therefore be established. Those rules are without prejudice to the rules on supervision and enforcement set out in this Directive.

(36) 欧州委員会からの理由を付した要請またはその構成国に対しもしくはその構成国内で必須サービスが提供される 1 もしくは複数の構成国からの理由を付した要請に応じて，この指令に基づく必須法主体の義務に適合する上で必須法主体に助言できるため，または，欧州の特別に重要な必須法主体による当該必須法主体の義務の遵守を評価できるために追加的な情報が必要なときは，欧州の特別に重要な必須法主体を必須法主体として識別した構成国は，欧州委員会に対し，この指令に定める一定の情報を提供すべきである。その欧州の特別に重要な必須法主体を必須法主体として識別した構成国の同意を得て，欧州委員会は，当該法主体によって設けられた措置を評価するための諮問機関を置き得るべきである。そのような諮問の任務が適正に遂行されることを確保するため，とりわけ，諮問機関の組織及び行動，とられるべき事後対応の活動，並びに，関係する欧州の特別に重要な必須法主体の義務に関し，補完的な規定が定められるべきである。諮問機関は，諮問の任務が遂行される構成国及び関係する必須法主体が，この指令に定める規定を遵守すべき必要性を妨げることなく，例えば，関連する施設または文書へのアクセスを得るため満たされるべき詳細条件に関し，及び，法務上の救済に関し，当該構成国の法律の細目規定に服して行動すべきである。そのような諮問機関に対して求められる特別の専門知識は，それが適切なときは，欧州議会及び理事会の決定 No 1313/2013/EU[22]によって設置された緊急対応調整拠点を介して要求され得る。

On a reasoned request from the Commission or from one or more Member States to or in which the essential service is provided, where additional information is necessary to be able to advise a critical entity in meeting its obligations under this Directive or to assess the compliance of a critical entity of particular European significance with those obligations, the Member State that has identified a critical entity of particular European significance as a critical entity should provide the Commission with certain information as set out in this Directive. In agreement with the Member State that has identified the critical entity of particular European significance as a critical entity, the Commission should be able to organise

[22] 欧州連合の市民保護の仕組みに関する欧州議会及び理事会の 2013 年 12 月 17 日の決定 No 1313/2013/EU (OJ L 347, 20.12.2013, p. 924).
Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

an advisory mission to assess the measures put in place by that entity. In order to ensure that such advisory missions are carried out properly, complementary rules should be established, in particular on the organisation and conduct of the advisory missions, the follow-up actions to be taken and the obligations for the critical entities of particular European significance concerned. The advisory mission should, without prejudice to the need for the Member State in which the advisory mission is conducted and the critical entity concerned to comply with the rules laid down in this Directive, be conducted subject to the detailed rules of the law of that Member State, for instance on the precise conditions to be fulfilled in order to obtain access to relevant premises or documents and on judicial redress. Specific expertise required for such advisory missions could, where relevant, be requested through the Emergency Response Coordination Centre established by Decision No 1313/2013/EU of the European Parliament and of the Council[(22)].

(37) 欧州委員会を支援するため，そして，構成国間の協力，及び，ベストプラクティスを含め，この指令と関連する問題に関する情報の交換を容易にするため，欧州委員会の専門家グループとして，必須法主体回復力グループが設置されるべきである。構成国は，それが適切なときは，セキュリティクリアランスをもつ代表を指名することによる場合を含め，必須法主体回復力グループ内における当該構成国の職務権限のある機関の指名された代表が実効的かつ効率的に協力することを確保することに努めるべきである。必須法主体回復力グループは，この指令の国内法化期間内における適切な協力のために付加的な手段を提供するため，可及的速やかにその職務の遂行を開始すべきである。必須法主体回復力グループは，関連する他の部門別専門家作業グループとの間で交流すべきである。

In order to support the Commission and facilitate cooperation among Member States and the exchange of information, including best practices, on issues relating to this Directive, a Critical Entities Resilience Group should be established as a Commission expert group. Member States should endeavour to ensure that the designated representatives of their competent authorities in the Critical Entities Resilience Group effectively and efficiently cooperate, including by designating representatives who hold security clearance, where appropriate. The Critical Entities Resilience Group should begin to perform its tasks as soon as possible, so as to provide additional means for appropriate cooperation during the transposition period of this Directive. The Critical Entities Resilience Group should interact with other relevant sector-specific expert working groups.

(38) 必須法主体回復力グループは，指令(EU) 2022/2555 の下において設置された協力グループとの間で，必須法主体のサイバーな回復力及び非サイバーな回復力に関する包括的な枠組みを支えるという観点から，協力すべきである。必須法主体回復力グループ及び指令(EU) 2022/2555 の下において設置された協力グループは，この指令の下にある職務権限のある機関と指令(EU) 2022/2555 の下にある職務権限のある機関との間の協力を促進するため，及び，とりわけ，両者のグループと関連する話題に関し，情報の交換を容易にするための定例の対話に従事すべきである。

The Critical Entities Resilience Group should cooperate with the Cooperation Group established under Directive (EU) 2022/2555 with a view to supporting a comprehensive framework for cyber and non-cyber resilience of critical entities. The Critical Entities Resilience Group and the Cooperation Group established under Directive (EU) 2022/2555 should engage in a regular dialogue to promote cooperation between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2555 and to facilitate the exchange of information, in particular on topics of relevance to both groups.

(39) この指令の目的を達成するため，かつ，この指令に定める構成国と必須法主体それぞれの義務の遵守を確保するための構成国と必須法主体の法律上の責任を妨げることなく，欧州委員会は，それが適切であると欧州委員会が判断するときは，職務権限のある機関と必須法主体それぞれの義務の職務権限のある機関と必須法主体それぞれの遵守を容易にすることを狙いとして，職務権限のある機関及び必須法主体を支援すべきである。この指令に基づく義務の実装において構成国及び必須法主体に対して支援を提供するときは，欧州委員会は，決定 No 1313/2013/EU によって設置された欧州連合の市民保護の仕組みに基づく構造及びツールのような，既存の構造及びツール，並びに，重要インフラ保護のための欧州レファレンスネットワークを基礎とすべきである。加えて，欧州委員会は，構成国に対し，欧州議会及び理事会の規則(EU) 2021/1149[23]によって設けられた域内保安基金，欧州議会及び理事会の規則(EU) 2021/695[24]によって設けられた Horizon Europe,または，それら以外の，必須法主体の回復力と関連する法律文書の中にある資源のような，欧州連合レベルで利用可能な資源に関し，情報提供すべきである。

In order to achieve the objectives of this Directive and without prejudice to the legal responsibility of Member States and critical entities to ensure compliance with their respective obligations laid down therein, the Commission should, where it considers it appropriate, support competent authorities and critical entities with the aim of facilitating their compliance with their respective obligations. When providing support to Member States and critical entities in the implementation of obligations under this Directive, the Commission should build on existing structures and tools, such as those under the Union Civil Protection Mechanism, established by Decision No 1313/2013/EU, and the European Reference Network for Critical Infrastructure Protection. In addition, it should inform Member States about

---

[23] 域内保安基金を設ける欧州議会及び理事会の 2021 年 7 月 7 日の規則(EU) 2021/1149 (OJ L 251, 15.7.2021, p. 94).
Regulation (EU) 2021/1149 of the European Parliament and of the Council of 7 July 2021 establishing the Internal Security Fund (OJ L 251, 15.7.2021, p. 94).

[24] Horizon Europe－調査研究及び技術革新のための枠組み計画を設ける，参加及び普及のための同計画の規定を定める，並びに，規則(EU) No 1290/2013 及び規則(EU) No 1291/2013 を廃止する欧州議会及び理事会の 2021 年 4 月 28 日の規則(EU) 2021/695 (OJ L 170, 12.5.2021, p. 1).
Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (OJ L 170, 12.5.2021, p. 1).

resources available at Union level, such as within the Internal Security Fund, established by Regulation (EU) 2021/1149 of the European Parliament and of the Council [23], Horizon Europe, established by Regulation (EU) 2021/695 of the European Parliament and of the Council [24], or other instruments relevant for the resilience of critical entities.

(40) 構成国は，当該構成国の職務権限のある機関が，当該法主体がこの指令の中で定められている管轄権の下にある場合において，必須法主体と関係するこの指令の適正な適用及び執行のための一定の具体的な権限をもつことを確保すべきである。同権限は，とりわけ，検査及び監査を行う権限，監督の権限，必須法主体の義務を遵守するために当該必須法主体が講じた措置と関連する情報及び証拠を提供することを必須法主体に対して要求する権限，並びに，それが必要なときは，発見された違反行為を是正することの命令を発令する権限を含むべきである。そのような命令を発令する場合，構成国は，とりわけ，その違反行為の重大性及び関係する必須法主体の経済的能力を考慮に入れた上で，関係する必須法主体の遵守を確保するために必要かつ比例的なところを超えた措置を要求してはならない。より一般的には，それらの権限は，欧州連合基本権憲章に従って国内法の中で定められる適切かつ実効的な安全確保を伴うべきである。この指令に定める必須法主体の義務の必須法主体による遵守を評価する際，この指令の下にある職務権限のある機関は，指令(EU) 2022/2555 の下にある職務権限のある機関に対し，この指令の下において必須法主体として識別された指令(EU) 2022/2555 の下における法主体との関係において，当該職務権限のある機関の監督と執行の権限を行使することを要請できるべきである。この指令の下にある職務権限のある機関及び指令(EU) 2022/2555 の下にある職務権限のある機関は，当該目的のために，協力し，かつ，情報を交換すべきである。

Member States should ensure that their competent authorities have certain specific powers for the proper application and enforcement of this Directive in relation to critical entities, where those entities fall under their jurisdiction as specified in this Directive. Those powers should include, in particular, the power to conduct inspections and audits, the power to supervise, the power to require critical entities to provide information and evidence relating to the measures they have taken to comply with their obligations and, where necessary, the power to issue orders to remedy identified infringements. When issuing such orders, Member States should not require measures which go beyond what is necessary and proportionate to ensure the compliance of the critical entity concerned, taking account of, in particular, the seriousness of the infringement and the economic capacity of the critical entity concerned. More generally, those powers should be accompanied by appropriate and effective safeguards to be specified in national law in accordance with the Charter of Fundamental Rights of the European Union. When assessing the compliance of a critical entity with its obligations as laid down in this Directive, the competent authorities under this Directive should be able to request the competent authorities under Directive (EU) 2022/2555 to exercise their supervisory and enforcement powers in relation to an entity under that Directive that has been identified as a critical entity under this Directive. The competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2555 should cooperate and exchange information for that purpose.

(41) 実効的かつ一貫性のある態様でこの指令を適用するため，TFEU の第 290 条に従い，必須サービスのリストを作成することによってこの指令を補遺する行為を採択する権限は，欧州委員会に対して委任されるべきである。同リストは，構成国リスク評価を実施する目的のために，及び，この指令により必須法主体を識別する目的のために，職務権限のある機関によって利用されるべきである。この指令のミニマムの整合化のアプローチに照らし，同リストは非網羅的であり，かつ，構成国は，必須サービスの提供における国内の特殊性を考慮に入れるため，国内レベルで，付加的な必須サービスをもって同リストを補遺し得る。欧州委員会の準備作業の間，欧州委員会が，専門家レベルのものを含め，適切に意見聴取を遂行すること，そして，当該意見聴取が，より良い立法に関する 2016 年 4 月 13 日の機関間合意[25]に定める基本原則に従って実施されることは，特に重要なことである。とりわけ，委任される行為の準備への平等な参加を確保するため，欧州議会及び理事会は，構成国の専門家と同時に全ての文書を受領し，かつ，それらの専門家は，自動的に，委任される行為の準備を取り扱う欧州委員会の専門家グループの会合へのアクセスをもつ。

In order to apply this Directive in an effective and consistent manner, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to supplement this Directive by drawing up a list of essential services. That list should be used by competent authorities for the purpose of conducting Member State risk assessments and identifying critical entities pursuant to this Directive. In light of the minimum harmonisation approach of this Directive, that list is non-exhaustive, and Member States could complement it with additional essential services at national level in order to take into account national specificities in the provision of essential services. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making [(25)]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(42) この指令の実装のための統一的な条件を確保するため，実装権限は，欧州委員会に対して与えられるべきである。当該権限は，欧州議会及び理事会の規則(EU) No 182/2011[26]に従って行使されるべきである。

In order to ensure uniform conditions for the implementation of this Directive, implementing powers

---

[25] OJ L 123, 12.5.2016, p. 1.

[26] 欧州委員会の実装権限の行使の構成国による管理のための仕組みに関する規定及び一般原則を定める欧州議会及び理事会の 2011 年 2 月 16 日の規則(EU) No 182/2011 (OJ L 55, 28.2.2011, p. 13).
Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council [26].

(43) この指令の目的, すなわち, 重要な社会的機能及び経済活動の維持のために必須のサービスが域内市場において支障のない態様で提供されることを確保すること, そして, そのようなサービスを提供する必須法主体の回復力を拡大することは, 構成国によっては十分に達成され得ず, その行為の影響のゆえに, 欧州連合レベルでより良く達成され得るので, 欧州連合は, 欧州連合条約の第 5 条に定める補完性の原則に従い, 措置を採択できる。同第 5 条に定める比例性の原則に従い, この指令は, それらの目的を達成するために必要なところを超えることがない。

Since the objectives of this Directive, namely to ensure that services essential for the maintenance of vital societal functions or economic activities are provided in an unobstructed manner in the internal market and to enhance the resilience of critical entities providing such services, cannot be sufficiently achieved by the Member States, but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on the European Union. In accordance with the principle of proportionality as set out in that Article 5, this Directive does not go beyond what is necessary in order to achieve those objectives.

(44) 欧州データ保護監督官は, 欧州議会及び理事会の規則(EU) 2018/1725[27]の第 42 条第 1 項に従って意見聴取を受け, 2021 年 8 月 11 日にその意見を伝達した。

The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council [27] and delivered an opinion on 11 August 2021.

(45) それゆえ, 指令 2008/114/EC は, 廃止されるべきである,

Directive 2008/114/EC should therefore be repealed,

以上のとおりであるので, この指令を採択する:

HAVE ADOPTED THIS DIRECTIVE:

---

[27] 欧州連合の機関, 組織, 事務局及び部局による個人データの処理と関連する自然人の保護に関する並びにそのデータの支障のない移動に関する, 並びに, 規則(EC) No 45/2001 及び決定 No 1247/2002/EC を廃止する欧州議会及び理事会の 2018 年 10 月 23 日の規則(EU) 2018/1725 (OJ L 295, 21.11.2018, p. 39).
Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

第I章 総則的な規定

Chapter I General Provisions

第 1 条 対象事項及び適用範囲

Article 1 **Subject matter and scope**

1. この指令は:
   (a) TFEU の第 114 条の適用範囲内にある重要な社会的機能または経済活動の維持のために必須のサービスが, 域内市場において支障のない態様で提供されることを確保することを狙いとする具体的な措置を講ずる構成国の義務, とりわけ, 必須法主体を識別する義務, 及び, 当該法主体に課される義務への適合において必須法主体を支援する義務を定め;
   (b) 当該法主体の回復力及び域内市場内において(a)に示すサービスを提供する能力を拡大することを狙いとする必須法主体の義務を定め;
   (c) 以下に関する規定を定め:
      (i) 必須法主体の監督に関する規定;
      (ii) 執行に関する規定;
      (iii) 欧州の特別に重要な必須法主体の識別に関する規定, 及び, そのような法主体が第Ⅲ章の下にある当該法主体の義務に適合するために設ける措置を評価するための諮問機関に関する規定;
   (d) この指令の適用に関する協力及び報告のための共通の手続を定め;
   (e) 欧州連合内の必須サービスの提供を確保するため, 及び, 域内市場の稼働を向上させるために必須法主体の高いレベルの回復力を達成するための措置を定める。

   This Directive:
   (a) lays down obligations on Member States to take specific measures aimed at ensuring that services which are essential for the maintenance of vital societal functions or economic activities within the scope of Article 114 TFEU are provided in an unobstructed manner in the internal market, in particular obligations to identify critical entities and to support critical entities in meeting the obligations imposed on them;
   (b) lays down obligations for critical entities aimed at enhancing their resilience and ability to provide services as referred to in point (a) in the internal market;
   (c) establishes rules:
      (i) on the supervision of critical entities;
      (ii) on enforcement;
      (iii) for the identification of critical entities of particular European significance and on advisory missions to assess the measures that such entities have put in place to meet their obligations under Chapter III;
   (d) establishes common procedures for cooperation and reporting on the application of this Directive;
   (e) lays down measures with a view to achieving a high level of resilience of critical entities in order to

ensure the provision of essential services within the Union and to improve the functioning of the internal market.

2. この指令は，この指令の第 8 条を妨げることなく，指令(EU) 2022/2555 に包摂される事項に対して適用してはならない。必須法主体の物理的な防護とサイバーセキュリティとの間の関係に照らし，構成国は，この指令及び指令(EU) 2022/2555 が調整された態様で実装されることを確保する。

This Directive shall not apply to matters covered by Directive (EU) 2022/2555, without prejudice to Article 8 of this Directive. In light of the relationship between the physical security and cybersecurity of critical entities, Member States shall ensure that this Directive and Directive (EU) 2022/2555 are implemented in a coordinated manner.

3. 欧州連合の部門別の法行為の条項が，必須法主体に対し，当該必須法主体の回復力を拡大するための措置を講ずることを求めており，かつ，当該要件が，この指令に定める対応義務と少なくとも均等であることが構成国によって承認されているときは，第VI章に定める監督及び執行に関する条項を含め，この指令に定める関連条項を適用してはならない。

Where provisions of sector-specific Union legal acts require critical entities to take measures to enhance their resilience and where those requirements are recognised by Member States as at least equivalent to the corresponding obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VI, shall not apply.

4. TFEU の第 346 条を妨げることなく，企業秘密に関する規定のような，欧州連合の規定または国内規定により秘密である情報は，この指令の適用のために当該交換が必要である場合に限り，この指令に従い，欧州委員会及びそれ以外の関連機関との間で交換される。交換される情報は，当該交換の目的のために適切かつ比例的な情報に限定される。情報の交換は，構成国の防護を尊重しつつ，当該情報の機密性及び必須法主体の防護と商業上の利益を保持する。

Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union or national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities in accordance with this Directive only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and the security and commercial interests of critical entities, while respecting the security of Member States.

5. この指令は，その国の領土の完全性を確保すること及び法と秩序を維持することを含め，構成国の国家安全保障及び国防を守る職責，及び，それら以外の必須の国家機能を防護するためのその構成国の権限を妨げない。

This Directive is without prejudice to the Member States' responsibility for safeguarding national security and defence and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.

6. この指令は，国家安全保障，公共の保安，国防の分野，または，犯罪行為の捜査，検知及び訴追を含め，法執行の分野において当該法主体の活動を遂行する行政機関である法主体に対しては，適用されない。

This Directive does not apply to public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences.

7. 構成国は，国家安全保障，公共の保安，国防の分野，もしくは，犯罪行為の捜査，検知及び訴追を含め，法執行の分野における活動を遂行する特定の必須法主体に対し，または，専ら本条の第 6 項に示す行政機関である法主体に対してサービスを提供する特定の必須法主体に対し，第 11 条並びに第Ⅲ章，第Ⅳ章及び第Ⅵ章の全部または一部が適用されないことを決定できる。

Member States may decide that Article 11 and Chapters III, IV and VI, in whole or in part, do not apply to specific critical entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in paragraph 6 of this Article.

8. この指令に定める義務は，その情報の開示が構成国の国家安全保障，公共の保安または国防という必須の利益に反するような情報の供給を伴ってはならない。

The obligations laid down in this Directive shall not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence.

9. この指令は，個人データの保護に関する欧州連合法，とりわけ，欧州議会及び理事会の規則(EU) 2016/679[28]並びに欧州議会及び理事会の指令 2002/58/EC[29]を妨げない。

---

[28] 個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する，並びに，指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679（一般データ保護規則）(OJ L 119, 4.5.2016, p. 1).
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[29] 電子通信部門における個人データ処理及びプライバシー保護に関する欧州議会及び理事会の 2002 年 7 月 12 日の指令 2002/58/EC（プライバシー及び電子通信に関する指令）(OJ L 201, 31.7.2002, p. 37).

This Directive is without prejudice to Union law on the protection of personal data, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council[28] and Directive 2002/58/EC of the European Parliament and of the Council[29].

第 2 条 定義

Article 2 **Definitions**

この指令の目的のために，以下の定義が適用される：

(1) 「必須法主体」とは，別紙の表の第 3 列に定める類型のいずれかに属し，第 6 条に従って構成国によって指定された公的法主体または民間法主体のことを意味し；

(2) 「回復力」とは，インシデントを防止し，インシデントから保護し，インシデントに対応し，インシデントに抗し，インシデントを緩和し，インシデントを吸収し，インシデントを封じ込め，そして，インシデントから復旧するための必須法主体の能力のことを意味し；

(3) 「インシデント」とは，それが法の支配を守る国内システムに対して影響を及ぼす場合を含め，必須サービスの提供を大きく混乱させる可能性をもつ出来事または混乱させる出来事のことを意味し；

(4) 「重要インフラ」とは，必須サービスの提供のために必要な資産，施設，装置，ネットワークもしくはシステム，または，資産，施設，装置，ネットワークもしくはシステムの一部のことを意味し；

(5) 「必須サービス」とは，重要な社会的機能，経済活動，公衆衛生及び公衆の安全または環境の維持のために不可欠なサービスのことを意味し；

(6) 「リスク」とは，インシデントによって生ずる損失または混乱の可能性のことを意味し，そのような損失または混乱の大きさとそのインシデントの発生の蓋然性の組み合わせとして表現されるべきであり；

(7) 「リスク評価」とは，インシデントを導き得る関連する潜在的な脅威，脆弱性及び危険を識別及び分析することにより，並びに，当該インシデントによって生ずる必須サービスの提供の潜在的な喪失または混乱を評価することにより，リスクの性質及び範囲を判定するための全体的なプロセスのことを意味し；

(8) 「技術標準」とは，欧州議会及び理事会の規則(EU) No 1025/2012[30]の第 2 条第 1 号に定義

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

[30] 欧州の標準化に関する，理事会決定 89/686/EEC 及び理事会決定 93/15/EEC，欧州議会及び理事会の指令 94/9/EC，指令 94/25/EC，指令 95/16/EC，指令 97/23/EC，指令 98/34/EC，指令 2004/22/EC，指令 2007/23/EC，指令 2009/23/EC 及び指令 2009/105/EC を改正する，並びに，理事会決定 87/95/EEC 及び欧州議会及び理事会の決定 No 1673/2006/EC を廃止する欧州議会及び理事会の 2012 年 10 月 25 日の規則(EU) No 1025/2012 (OJ L 316, 14.11.2012, p. 12).

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC,

する技術標準のことを意味し；

(9) 「技術仕様」とは，規則(EU) No 1025/2012 の第 2 条第 4 号に定義する技術仕様のことを意味し；

(10) 「行政機関である法主体」とは，国内法に従い，構成国においてそのようなものとして承認された法主体であって，法務当局，議会または中央銀行を含まず，以下の基準を満たすもののことを意味する：

(a) その法主体は，一般的な利益における必要性に適合する目的のために設けられており，かつ，産業上の性質または商業上の性質をもたない；

(b) その法主体は，法人格をもち，または，法人格をもつ別の法主体の代わりに行動するための法律上の資格をもつ；

(c) その法主体は，その資金の大部分において，国の機関またはそれ以外の公法によって規律される中央レベルの組織から提供されており，当該機関または組織による運営管理上の監督に服しており，または，その構成員の半数以上が国の機関またはそれ以外の公法によって規律される中央レベルの組織から指名された者である業務運営，運営管理または監督の委員会をもつ；

(d) その法主体は，自然人または法人に対し，人，物品，サービスまたは資本の国境を越える移動に際し，当該自然人または法人の権利に影響を与える行政上の決定または規制上の決定を発令する権限をもつ。

For the purposes of this Directive, the following definitions apply:

(1) ‘critical entity’ means a public or private entity which has been identified by a Member State in accordance with Article 6 as belonging to one of the categories set out in the third column of the table in the Annex;

(2) ‘resilience’ means a critical entity’s ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident;

(3) ‘incident’ means an event which has the potential to significantly disrupt, or that disrupts, the provision of an essential service, including when it affects the national systems that safeguard the rule of law;

(4) ‘critical infrastructure’ means an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service;

(5) ‘essential service’ means a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment;

(6) ‘risk’ means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;

95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

(7) ‘risk assessment ’ means the overall process for determining the nature and extent of a risk by identifying and analysing potential relevant threats, vulnerabilities and hazards which could lead to an incident and by evaluating the potential loss or disruption of the provision of an essential service caused by that incident;

(8) ‘standard’ means a standard as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council[30];

(9) ‘technical specification’ means a technical specification as defined in Article 2, point (4), of Regulation (EU) No 1025/2012;

(10) ‘public administration entity’ means an entity recognised as such in a Member State in accordance with national law, not including the judiciary, parliaments or central banks, which complies with the following criteria:

(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;

(b) it has legal personality or is entitled by law to act on behalf of another entity with legal personality;

(c) it is financed, for the most part, by the State authorities or by other central-level bodies governed by public law, is subject to management supervision by those authorities or bodies, or has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State authorities or by other central-level bodies governed by public law;

(d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital.

第 3 条 ミニマムの整合化

Article 3 **Minimum harmonisation**

この指令は，そのような条項が欧州連合法に定める構成国の義務と一貫性があることを条件として，構成国が，必須法主体のより高いレベルの回復力を達成するための国内法の条項を採択または維持することを排除してはならない。

This Directive shall not preclude Member States from adopting or maintaining provisions of national law with a view to achieving a higher level of resilience of critical entities, provided that such provisions are consistent with Member States’ obligations laid down in Union law.

第Ⅱ章 必須法主体の回復力に関する国内枠組み

Chapter II National Frameworks on the Resilience of Critical Entities

第 4 条 必須法主体の回復力に関する戦略

Article 4 **Strategy on the resilience of critical entities**

1. 実務上可能な範囲内で関連する利害関係者に対して開かれる意見聴取を経た後，各構成国は，2026 年 1 月 17 日までに，必須法主体の回復力を拡大するための戦略（「戦略」）を採択する。戦略は，必須法主体の側における高いレベルの回復力を達成及び維持し，少なくとも別紙に定める部門を包摂するという観点から，関連する既存の国内戦略及び部門別戦略，計画または類似の文書を基礎として，戦略上の目標及び政策上の措置を定める。

   Following a consultation that is, to the extent practically possible, open to relevant stakeholders, each Member State shall adopt by 17 January 2026 a strategy for enhancing the resilience of critical entities (the 'strategy'). The strategy shall set out strategic objectives and policy measures, building upon relevant existing national and sectoral strategies, plans or similar documents, with a view to achieving and maintaining a high level of resilience on the part of critical entities and covering at least the sectors set out in the Annex.

2. 各戦略は，少なくとも以下の要素を含める：
   (a) 国境を越える及び部門横断の依存性及び相互依存性を考慮に入れた上で，必須法主体の全体的な回復力を拡大する目的のための戦略上の目標及び優先順序；
   (b) 戦略の実装に関与する異なる機関，必須法主体及びそれ以外の者の役割と責任の記述を含め，戦略上の目標と優先順序を達成するための統治枠組み；
   (c) 第 5 条に示すリスク評価の記述を含め，必須法主体の全体的な回復力を拡大するために必要となる措置の記述；
   (d) それによって必須法主体が識別されるプロセスの記述；
   (e) 一方における公的部門と，他方における民間部門並びに公的法主体及び民間の法主体との間の協力を拡大するための措置を含め，本章に従って必須法主体を支援するプロセスの記述：
   (f) 必須法主体以外の，戦略の実装に関与する主要な機関と関連利害関係者のリスト；
   (g) サイバーセキュリティ上のリスク，サイバーな脅威及びサイバーなインシデント，並びに，非サイバーなリスク，脅威及びインシデントに関する情報交換の目的のための，そして，監督の職務の執行に関する情報交換の目的のための，この指令の下にある職務権限のある機関（「職務権限のある機関」）と指令(EU) 2022/2555 の下にある職務権限のある機関との間の調整のための政策枠組み；
   (h) 当の構成国が必須法主体として識別した委員会勧告 2003/361/EC[31] の別紙の意味における小企業及び中規模企業によるこの指令の第Ⅲ章の下にある義務の実装を容易にすることを狙いとして既に設けられた措置の記述。

Each strategy shall contain at least the following elements:

(a) strategic objectives and priorities for the purposes of enhancing the overall resilience of critical entities, taking into account cross-border and cross-sectoral dependencies and interdependencies;

(b) a governance framework to achieve the strategic objectives and priorities, including a description of the roles and responsibilities of the different authorities, critical entities and other parties involved in the implementation of the strategy;

(c) a description of measures necessary to enhance the overall resilience of critical entities, including a description of the risk assessment referred to in Article 5;

(d) a description of the process by which critical entities are identified;

(e) a description of the process supporting critical entities in accordance with this Chapter, including measures to enhance cooperation between the public sector, on the one hand, and the private sector and public and private entities, on the other hand;

(f) a list of the main authorities and relevant stakeholders, other than critical entities, involved in the implementation of the strategy;

(g) a policy framework for coordination between the competent authorities under this Directive ('competent authorities') and the competent authorities under Directive (EU) 2022/2555 for the purposes of information sharing on cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents and the exercise of supervisory tasks;

(h) a description of measures already in place which aim to facilitate the implementation of obligations under Chapter III of this Directive by small and medium-sized enterprises within the meaning of the Annex to Commission Recommendation 2003/361/EC [31] that the Member State in question has identified as critical entities.

実務上可能な範囲内で関連する利害関係者に対して開かれる意見聴取を経た後，各構成国は，少なくとも 4 年毎に，当該構成国の戦略をアップデートする。

Following a consultation that is, to the extent practically possible, open to relevant stakeholders, Member States shall update their strategies at least every four years.

3. 構成国は，欧州委員会に対し，当該構成国の戦略及び同戦略の実質的に意味のあるアップデートの採択から 3 か月以内に，同戦略及び同戦略の実質的に意味のあるアップデートを通知する。

Member States shall communicate their strategies, and substantial updates thereto, to the Commission within three months of their adoption.

---

31 マイクロ企業，小企業及び中規模企業の定義に関する 2003 年 5 月 6 日の委員会勧告 2003/361/EC (OJ L 124, 20.5.2003, p. 36).

Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

第 5 条 構成国によるリスク評価

Article 5 **Risk assessment by Member States**

1. 欧州委員会は，2023 年 11 月 17 日まで，別紙に定める部門及び副部門の中にある必須サービスの非網羅的なリストを作成することによってこの指令を補遺するため，第 23 条に従って委任される行為を採択する権限を与えられる。職務権限のある機関は，2026 年 1 月 17 日までに，その後は，必要があるときはいつでも，かつ，少なくとも 4 年毎に，リスク評価（「構成国リスク評価」）を遂行する目的のために当該必須サービスのリストを使用する。職務権限のある機関は，第 6 条に従って必須法主体を識別する目的のために，及び，第 13 条による措置を講ずるために当該必須法主体を補助する目的のために，構成国リスク評価を使用する。

The Commission is empowered to adopt a delegated act, in accordance with Article 23, by 17 November 2023 to supplement this Directive by establishing a non-exhaustive list of essential services in the sectors and subsectors set out in the Annex. The competent authorities shall use that list of essential services for the purpose of carrying out a risk assessment ('Member State risk assessment') by 17 January 2026, whenever necessary subsequently, and at least every four years. The competent authorities shall use Member State risk assessments for the purpose of identifying critical entities in accordance with Article 6 and assisting those critical entities to take measures pursuant to Article 13.

構成国リスク評価は，部門横断の性質または国境を越える性質をもつリスクを含め，関連する自然のリスク及び人為的なリスク，事故，自然災害，公衆衛生上の緊急事態，欧州議会及び理事会の指令(EU) 2017/541[32]に定めるテロリスト行為を含め，ハイブリッドな脅威またはそれ以外の敵対的な脅威を考慮する。

Member State risk assessments shall account for the relevant natural and man-made risks, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid threats or other antagonistic threats, including terrorist offences as provided for in Directive (EU) 2017/541 of the European Parliament and of the Council [(32)].

2. 構成国リスク評価を遂行する際，構成国は，少なくとも以下の事項を考慮に入れる：
   (a) 決定 No 1313/2013/EU の第 6 条第 1 項によって遂行される一般的なリスク評価；
   (b) 欧州議会及び理事会の規則(EU) 2017/1938[33]及び規則(EU) 2019/941[34]，並びに，欧州議会

---

32 テロリズムとの闘いに関する，並びに，理事会枠組み決定 2002/475/JHA を置き換え，及び，理事会決定 2005/671/JHA を改正する欧州議会及び理事会の 2017 年 3 月 15 日の指令(EU)2017/541(OJ L 88, 31.3.2017, p. 6).
Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

33 ガス供給の防護を守る措置に関する，及び，規則(EU) No 994/2010 を廃止する欧州議会及び理事会の 2017 年 10 月 25 日の規則(EU) 2017/1938 (OJ L 280, 28.10.2017, p. 1).

及び理事会の指令 2007/60/EC[35] 及び指令 2012/18/EU[36] を含め，関連する欧州連合の部門別の法行為の要件に従って遂行される，他の関連するリスク評価；

(c) 別の構成国及び第三国に所在する法主体に別紙に定める諸部門が依存する程度から生ずる関連リスクを含め，別紙に定める諸部門が相互に依存する程度から生ずる関連リスク，並びに，市民及び域内市場に対する重大なリスクを含め，ある部門における重大な混乱が他の部門に対してもち得る影響；

(d) 第 15 条に従って通知されるインシデントに関する情報。

In carrying out Member State risk assessments, Member States shall take into account at least the following:

(a) the general risk assessment carried out pursuant to Article 6(1) of Decision No 1313/2013/EU;

(b) other relevant risk assessments, carried out in accordance with the requirements of the relevant sector-specific Union legal acts, including Regulations (EU) 2017/1938 [33] and (EU) 2019/941 [34] of the European Parliament and of the Council and Directives 2007/60/EC [35] and 2012/18/EU [36] of the European Parliament and of the Council;

(c) the relevant risks arising from the extent to which the sectors set out in the Annex depend on one another, including from the extent to which they depend on entities located within other Member States and third countries, and the impact that a significant disruption in one sector may have on other sectors, including any significant risks to citizens and the internal market;

(d) any information on incidents notified in accordance with Article 15.

第 1 副項(c)の目的のために，構成国は，他の構成国の職務権限のある機関及び第三国の職務権限のある機関と，しかるべく協力する。

For the purposes of the first subparagraph, point (c), Member States shall cooperate with the competent

---

Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010 (OJ L 280, 28.10.2017, p. 1).

34 電気部門におけるリスク準備態勢に関する，及び，指令 2005/89/EC を廃止する欧州議会及び理事会の 2019 年 6 月 5 日の規則(EU) 2019/941(OJ L 158, 14.6.2019, p. 1).

Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC (OJ L 158, 14.6.2019, p. 1).

35 洪水のリスクの評価及び管理に関する欧州議会及び理事会の 2007 年 10 月 23 日の指令 2007/60/EC (OJ L 288, 6.11.2007, p. 27).

Directive 2007/60/EC of the European Parliament and of the Council of 23 October 2007 on the assessment and management of flood risks (OJ L 288, 6.11.2007, p. 27).

36 危険な物質と関係する重大事故の危険の管理に関する，理事会指令 96/82/EC を改正し，その後に廃止する欧州議会及び理事会の 2012 年 7 月 4 日の指令 2012/18/EU (OJ L 197, 24.7.2012, p. 1).

Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC (OJ L 197, 24.7.2012, p. 1).

authorities of other Member States and the competent authorities of third countries, as appropriate.

3. 構成国は，当該構成国の単一連絡部局を介して関係をもつときは，第 6 条に従って当該構成国が識別した必須法主体に対し，構成国リスク評価の関連する構成要素を利用できるようにする。構成国は，必須法主体に対して提供される情報が，第 12 条による当該必須法主体のリスク評価を遂行する上で，及び，第 13 条による当該必須法主体の回復力を確保するための措置を講ずる上で，当該必須法主体を補助することを確保する。

Member States shall make the relevant elements of Member State risk assessments available, where relevant through their single points of contact, to the critical entities that they have identified in accordance with Article 6. Member States shall ensure that the information provided to critical entities assists them in carrying out their risk assessments pursuant to Article 12 and in taking measures to ensure their resilience pursuant to Article 13.

4. 構成国リスク評価の実施から 3 か月以内に，構成国は，欧州委員会に対し，別紙に定める部門及び副部門毎に，当該構成国リスク評価によって識別されたリスクのタイプ及び当該構成国リスク評価の結果に関する関連情報を提供する。

Within three months of carrying out a Member State risk assessment, a Member State shall provide the Commission with relevant information on the types of risks identified following, and the outcomes of, that Member State risk assessment, per sector and subsector set out in the Annex.

5. 欧州委員会は，構成国と協力して，第 4 項の遵守の目的のための任意で共通の報告書雛型を策定する。

The Commission shall, in cooperation with the Member States, develop a voluntary common reporting template for the purpose of complying with paragraph 4.

第 6 条 必須法主体の識別

Article 6 **Identification of critical entities**

1. 2026 年 7 月 17 日までに，各構成国は，別紙に定める部門及び副部門毎に，必須法主体を識別する。

By 17 July 2026, each Member State shall identify the critical entities for the sectors and subsectors set out in the Annex.

2. 第 1 項により構成国が必須法主体を識別するときは，その構成国の構成国リスク評価及びその構成国の戦略を考慮に入れ，かつ，以下の基準の全てを適用する：

(a) その法主体は，1 または複数の必須サービスを提供している；
(b) その法主体は，当該構成国の領土上で業務運営しており，かつ，当該構成国の領土上にその法主体の重要インフラが所在している；
(c) インシデントは，1 もしくは複数の必須サービスのその法主体からの提供に対し，または，当該1または複数の必須サービスに依存し，別紙に定める部門の中にある別の必須サービスの提供に対し，第 7 条第 1 項に従って決定される重大な混乱の影響をもち得る。

When a Member State identifies critical entities pursuant to paragraph 1, it shall take into account the outcomes of its Member State risk assessment and its strategy and shall apply all of the following criteria:
(a) the entity provides one or more essential services;
(b) the entity operates, and its critical infrastructure is located, on the territory of that Member State; and
(c) an incident would have significant disruptive effects, as determined in accordance with Article 7(1), on the provision by the entity of one or more essential services or on the provision of other essential services in the sectors set out in the Annex that depend on that or those essential services.

3. 各構成国は，第 2 項により識別された必須法主体のリストを作成し，かつ，当該識別から 1 か月以内に，当該必須法主体が必須法主体として識別された旨を当該必須法主体が通知されることを確保する。構成国は，第 8 条を妨げることなく，当該必須法主体に対し，第Ⅲ章及び第Ⅳ章に基づく当該必須法主体の義務並びに当該義務が当該必須法主体に対して適用開始となる日を連絡する。構成国は，別紙の表の第 3 号，第 4 号及び第 8 号に定める部門の必須法主体に対し，国内措置が別異に定めていない限り，当該必須法主体が第Ⅲ章及び第Ⅳ章に基づく義務を負わないことを連絡する。

Each Member State shall establish a list of the critical entities identified pursuant to paragraph 2 and ensure that those critical entities are notified that they have been identified as critical entities within one month of that identification. Member States shall inform those critical entities of their obligations under Chapters III and IV and the date from which those obligations apply to them, without prejudice to Article 8. Member States shall inform critical entities in the sectors set out in points 3, 4 and 8 of the table in the Annex that they have no obligations under Chapters III and IV, unless national measures provide otherwise.

関係する必須法主体に関しては，第Ⅲ章は，本項の第 1 副項に示す通知の日の 10 か月後から適用される。

For the critical entities concerned, Chapter III shall apply from 10 months after the date of the notification referred to in the first subparagraph of this paragraph.

4. 構成国は，この指令の下にある当該構成国の職務権限のある機関が，当該識別から 1 か月以内に，指令(EU) 2022/2555 の下にある職務権限のある機関に対し，本条に基づいて当該構成国が

識別した必須法主体の識別名を通知することを確保する。当該通知は，それが適用可能なときは，関係する必須法主体がこの指令の別紙の表の第 3 号，第 4 号及び第 8 号に定める部門の法主体であること，及び，同指令の第Ⅲ章及び第Ⅳ章に基づく義務を負わないことを指示する。

Member States shall ensure that their competent authorities under this Directive notify the competent authorities under Directive (EU) 2022/2555 of the identity of the critical entities that they have identified under this Article within one month of that identification. That notification shall specify, where applicable, that the critical entities concerned are entities in the sectors set out in points 3, 4 and 8 of the table in the Annex to this Directive and have no obligations under Chapters III and IV thereof.

5. 構成国は，それが必要なときは，かつ，いかなる場合においても少なくとも 4 年毎に，第 3 項に示す識別された必須法主体のリストを見直し，また，それが適切なときは，アップデートする。当該アップデートが追加的な必須法主体の識別を導くときは，当該追加的な必須法主体に対し，第 3 項及び第 4 項が適用される。加えて，構成国は，そのようなアップデート後に必須法主体として識別されなくなった法主体が，そのこと，及び，当該法主体が当該通知の受領の日から第Ⅲ章に基づく義務に服さなくなったことの通知を，適時に受けることを確保する。

Member States shall, where necessary and in any event at least every four years, review and, where appropriate, update the list of identified critical entities referred to in paragraph 3. Where those updates lead to the identification of additional critical entities, paragraphs 3 and 4 shall apply to those additional critical entities. In addition, Member States shall ensure that entities that are no longer identified as critical entities following any such update are notified in due time of that fact and the fact that they are no longer subject to the obligations under Chapter III from the date of receipt of that notification.

6. 欧州委員会は，構成国と協力して，必須法主体の識別において構成国を支援するための推奨事項及び拘束力のない指針を策定する。

The Commission shall, in cooperation with the Member States, develop recommendations and non-binding guidelines to support Member States in identifying critical entities.

第 7 条 重大な混乱の影響

Article 7 **Significant disruptive effect**

1. 第 6 条第 2 項(c)に示す混乱の影響の大きさを判定する際，構成国は，以下の基準を考慮に入れる：
   (a) 関係する法主体から提供される必須サービスに依拠している利用者の数；
   (b) 別紙に定める別の部門及び副部門が当の必須サービスに依存する程度；
   (c) 程度及び持続期間の面において，経済活動及び社会的活動，環境，公共の治安及び公衆衛生または人々の健康に対してインシデントがもち得る影響；

(d) 必須サービスまたは関係する必須サービスのための市場における法主体の市場占有率;
(e) 島嶼部, 遠隔地, 山間部のような, あるタイプの地理的領域の孤立の程度と関係する脆弱性を考慮に入れた, 国境を越える影響を含め, インシデントの影響を受け得る地理的領域;
(f) 当該必須サービスの提供のための代替的手段の可用性を考慮に入れ, 十分なレベルの必須サービスを維持する上での法主体の重要性。

When determining the significance of a disruptive effect as referred to in Article 6(2), point (c), Member States shall take into account the following criteria:
(a) the number of users relying on the essential service provided by the entity concerned;
(b) the extent to which other sectors and subsectors as set out in the Annex depend on the essential service in question;
(c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities, the environment, public safety and security, or the health of the population;
(d) the entity's market share in the market for the essential service or essential services concerned;
(e) the geographic area that could be affected by an incident, including any cross-border impact, taking into account the vulnerability associated with the degree of isolation of certain types of geographic areas, such as insular regions, remote regions or mountainous areas;
(f) the importance of the entity in maintaining a sufficient level of the essential service, taking into account the availability of alternative means for the provision of that essential service.

2. 第 6 条第 1 項に基づく必須法主体の識別の後, 各構成国は, 欧州委員会に対し, 不適切な遅滞なく, 以下の情報を提出する:
(a) 第 5 条第 1 項に示す必須サービスのリストと比較して追加的な必須サービスが存在する場合, 当該構成国における必須サービスのリスト;
(b) 別紙に定めるそれぞれの部門及び副部門毎に及びそれぞれの必須サービス毎に識別された必須法主体の数;
(c) 第 1 項における 1 または複数の基準を示すために適用された閾値。

After the identification of the critical entities under Article 6(1), each Member State shall submit the following information to the Commission without undue delay:
(a) a list of essential services in that Member State where there are any additional essential services as compared to the list of essential services referred to in Article 5(1);
(b) the number of critical entities identified for each sector and subsector set out in the Annex and for each essential service;
(c) any thresholds applied to specify one or more of the criteria in paragraph 1.

第 1 副項(c)に示す閾値は, そのようなものとして, または, 集約された形態で提示され得る。

Thresholds as referred to in the first subparagraph, point (c), may be presented as such or in aggregated form.

構成国は，必要があるときはいつでも，かつ，少なくとも 4 年毎に，第 1 副項に示す情報を事後に提出する。

Member States shall subsequently submit information referred to in the first subparagraph whenever necessary and at least every four years.

3. 欧州委員会は，第 19 条に示す必須法主体回復力グループの意見聴取を経た上で，本条の第 2 項に示す情報を考慮に入れ，本条の第 1 項に示す基準の適用を容易にするため，拘束力のない指針を採択する。

The Commission shall, after consulting the Critical Entities Resilience Group referred to in Article 19, adopt non-binding guidelines to facilitate the application of the criteria referred to in paragraph 1 of this Article, taking into account the information referred to in paragraph 2 of this Article.

第 8 条 銀行部門，金融市場インフラ部門及びデジタルインフラ部門の必須法主体

Article 8 **Critical entities in the banking, financial market infrastructure and digital infrastructure sectors**

構成国は，別紙の表の第 3 号，第 4 号及び第 8 号に定める部門内にあると当該構成国が識別した必須法主体に対して第 11 条並びに第III章，第IV章及び第VI章を適用しないことを確保する。構成国は，当該条項が，適用可能な欧州連合法と一貫性があることを条件として，当該必須法主体に関し，より高いレベルの回復力を達成するための国内法の条項を採択または維持できる。

Member States shall ensure that Article 11 and Chapters III, IV and VI do not apply to critical entities that they have identified in the sectors set out in points 3, 4 and 8 of the table in the Annex. Member States may adopt or maintain provisions of national law to achieve a higher level of resilience for those critical entities, provided that those provisions are consistent with applicable Union law.

第 9 条 職務権限のある機関及び単一連絡部局

Article 9 **Competent authorities and single point of contact**

1. 各構成国は，国内レベルにおいて，この指令に定める規定の正確な適用に関して，及び，それが必要なときは，その執行に関して職責を負う 1 または複数の職務権限のある機関を指定または設置する。

Each Member State shall designate or establish one or more competent authorities responsible for the correct application and, where necessary, enforcement of the rules set out in this Directive at national level.

この指令の別紙の表の第 3 号及び第 4 号に定める部門の中にある必須法主体に関しては，職務権限のある機関は，原則として，規則(EU) 2022/2554 の第 46 条に示す職務権限のある機関とする。この指令の別紙の表の第 8 号に定める部門の中にある必須法主体に関しては，職務権限のある機関は，原則として，規則(EU) 2022/2555 の下にある職務権限のある機関とする。構成国は，現行の国内枠組みに従い，この指令の別紙の表の第 3 号，第 4 号及び第 8 号に定める部門に関し，異なる職務権限のある機関を指定できる。

As regards the critical entities in the sectors set out in points 3 and 4 of the table in the Annex to this Directive, the competent authorities shall, in principle, be the competent authorities referred to in Article 46 of Regulation (EU) 2022/2554. As regards the critical entities in the sector set out in point 8 of the table in the Annex to this Directive, the competent authorities shall, in principle, be the competent authorities under Directive (EU) 2022/2555. Member States may designate a different competent authority for the sectors set out in points 3, 4 and 8 of the table in the Annex to this Directive in accordance with existing national frameworks.

構成国が複数の職務権限のある機関を指定または設置するときは，当該構成国は，関係する機関それぞれの職務を明確に定め，かつ，第 2 項に示す単一連絡部局の指定及び活動と関連する協力を含め，当該職務権限のある機関が，この指令に基づく当該職務権限のある機関の職務を満たすために実効的に協力することを確保する。

Where Member States designate or establish more than one competent authority, they shall clearly set out the tasks of each of the authorities concerned and ensure that they cooperate effectively to fulfil their tasks under this Directive, including with regard to the designation and activities of the single point of contact referred to in paragraph 2.

2. 各構成国は，別の構成国の単一連絡部局及び第 19 条に示す必須法主体回復力グループとの間の国境を越える協力を確保する目的のために連絡官の権限を行使するための 1 つの単一連絡部局（「単一連絡部局」）を指定または設置する。それが適切なときは，構成国は，その構成国の単一連絡部局を，職務権限のある機関の中で指定できる。それが適切なときは，構成国は，その構成国の単一連絡部局が，欧州委員会との間においても連絡官の権限を行使し，第三国との間の協力を確保することを定め得る。

Each Member State shall designate or establish one single point of contact to exercise a liaison function for the purpose of ensuring cross-border cooperation with the single points of contact of other Member States and the Critical Entities Resilience Group referred to in Article 19 (‘single point of contact’). Where relevant, a Member State shall designate its single point of contact within a competent authority. Where relevant, a Member State may provide that its single point of contact also exercise a liaison function with the Commission and ensure cooperation with third countries.

3. 2028 年 7 月 17 日までに，その後は 2 年毎に，単一連絡部局は，欧州委員会及び第 19 条に示

す必須法主体回復力グループに対し，通知の数，通知されたインシデントの性質及び第 15 条第 3 項に従って行われた活動を含め，当該単一連絡部局が受領した通知に関する要旨報告書を提出する。

By 17 July 2028, and every two years thereafter, the single points of contact shall submit a summary report to the Commission and to the Critical Entities Resilience Group referred to in Article 19 on the notifications they have received, including the number of notifications, the nature of notified incidents and the actions taken in accordance with Article 15(3).

欧州委員会は，必須法主体回復力グループと協力して，共通の報告書雛型を策定する。職務権限のある機関は，第 1 副項に示す要旨報告書を提出する目的のために，任意に，同共通の報告書雛型を使用できる。

The Commission shall, in cooperation with the Critical Entities Resilience Group, develop a common reporting template. The competent authorities may use, on a voluntary basis, that common reporting template for the purpose of submitting summary reports as referred to in the first subparagraph.

4. 各構成国は，その構成国の職務権限のある機関及び単一連絡部局が，当該職務権限のある機関及び単一連絡部局に割当てられた職務を実効的かつ効率的な態様で遂行するための権限並びに十分な資金，人的資源及び技術上の資源をもつことを確保する。

Each Member State shall ensure that its competent authority and single point of contact have the powers and the adequate financial, human and technical resources to carry out, in an effective and efficient manner, the tasks assigned to them.

5. 各構成国は，その構成国の職務権限のある機関が，それが適切なときは，かつ，欧州連合法及び国内法に従って，市民保護，法執行及び個人データの保護の職務に従事する機関を含め，他の関連する国内機関との間で，並びに，必須法主体及び関連する利害関係者との間で，意見聴取し，かつ，協力することを確保する。

Each Member State shall ensure that its competent authority, whenever appropriate, and in accordance with Union and national law, consults and cooperates with other relevant national authorities, including those in charge of civil protection, law enforcement and the protection of personal data, and with critical entities and relevant interested parties.

6. 各構成国は，その構成国のこの指令の下にある職務権限のある機関が，指令(EU) 2022/2555 の下にある職務権限のある機関との間で，その構成国の職務権限のある機関及び指令(EU) 2022/2555 の下にある職務権限のある機関が講じた関連措置との関連を含め，必須法主体に対して影響を与えるサイバーセキュリティ上のリスク，サイバーな脅威及びサイバーなインシデント，並びに，非サイバーなリスク，脅威及びインシデントに関し，協力し，かつ，情報交換することを確

保する。

Each Member State shall ensure that its competent authority under this Directive cooperates and exchanges information with competent authorities under Directive (EU) 2022/2555 on cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents affecting critical entities, including with regard to relevant measures its competent authority and competent authorities under Directive (EU) 2022/2555 have taken.

7. 職務権限のある機関及び単一連絡部局の指定または設置から 3 か月以内に，各構成国は，欧州委員会に対し，当該職務権限のある機関及び単一連絡部局の識別名及びこの指令に基づくその職務及び職責，その連絡先を通知し，かつ，その後の変更を通知する。構成国は，当該構成国が第 1 項第 2 副項に示す職務権限のある機関以外の機関を，別紙の表の第 3 号，第 4 号及び第 8 号に定める部門内の必須法主体と関係する職務権限のある機関として指定することを決定したときは，欧州委員会に対し，連絡する。各構成国は，その構成国の職務権限のある機関及び単一連絡部局の識別名を公表する。

Within three months of the designation or establishment of the competent authority and the single point of contact, each Member State shall notify the Commission of their identity and their tasks and responsibilities under this Directive, their contact details and any subsequent change thereto. Member States shall inform the Commission where they decide to designate an authority other than the competent authorities referred to in paragraph 1, second subparagraph, as the competent authorities in respect of the critical entities in the sectors set out in points 3, 4 and 8 of the table in the Annex. Each Member State shall make public the identity of its competent authority and single point of contact.

8. 欧州委員会は，単一連絡部局のリストを公表する。

The Commission shall make a list of the single points of contact publicly available.

第 10 条　必須法主体に対する構成国の支援

Article 10 **Member States' support to critical entities**

1. 構成国は，当該必須法主体の回復力の拡大において，必須法主体を支援する。当該支援は，ガイド資料及び手法を作成すること，当該必須法主体の回復力を試すための演習の計画を支援すること，並びに，必須法主体の要員に対して助言と訓練を提供することを含み得る。国家補助に関する適用可能な規定を妨げることなく，構成国は，それが必要であり，かつ，公共の利益の目的によって正当化されるときは，必須法主体に対し，資金を提供し得る。

Member States shall support critical entities in enhancing their resilience. That support may include developing guidance materials and methodologies, supporting the organisation of exercises to test their

resilience and providing advice and training to the personnel of critical entities. Without prejudice to applicable rules on State aid, Member States may provide financial resources to critical entities, where necessary and justified by public interest objectives.

2. 各構成国は，その構成国の職務権限のある機関が，別紙に定める諸部門の必須法主体との間で，協力し，かつ，情報及びグッドプラクティスを交換することを確保する。

Each Member State shall ensure that its competent authority cooperates and exchanges information and good practices with critical entities of the sectors set out in the Annex.

3. 構成国は，この指令によって包摂される事項に関し，とりわけ，機密情報及び機微の情報，競争並びに個人データの保護に関する欧州連合法及び国内法に従い，必須法主体間の任意の情報共有を促進する。

Member States shall facilitate voluntary information sharing between critical entities in relation to matters covered by this Directive, in accordance with Union and national law on, in particular, classified and sensitive information, competition and protection of personal data.

第 11 条 構成国間の協力

Article 11 **Cooperation between Member States**

1. それが適切である限り，構成国は，この指令が一貫性のある態様で適用されることを確保する目的のために，必須法主体と関連して相互に意見聴取する。そのような意見聴取は，とりわけ，以下の必須法主体に関して行われる：
   (a) 複数の構成国の間で物理的に結び付けられた重要インフラを使用する必須法主体；
   (b) 別の構成国内の必須法主体と結び付けられており，または，別の構成国内の必須法主体と連携している企業構造の一部である必須法主体；
   (c) 1 つの構成国の中で必須法主体として識別され，かつ，別の構成国に対しまたは別の構成国の中で必須サービスを提供する必須法主体。

Whenever appropriate, Member States shall consult one another regarding critical entities for the purpose of ensuring that this Directive is applied in a consistent manner. Such consultations shall take place, in particular, regarding critical entities that:
   (a) use critical infrastructure which is physically connected between two or more Member States;
   (b) are part of corporate structures that are connected with, or linked to, critical entities in other Member States;
   (c) have been identified as critical entities in one Member State and provide essential services to or in other Member States.

2. 第 1 項に示す意見聴取は，必須法主体の回復力を拡大すること，及び，それが可能なときは，必須法主体に対する管理運営上の負担を削減することを狙いとする。

The consultations referred to in paragraph 1 shall aim at enhancing the resilience of critical entities and, where possible, reducing the administrative burden on them.

第III章 必須法主体の回復力
Chapter III Resilience of Critical Entities

第 12 条 必須法主体によるリスク評価
Article 12 **Risk assessment by critical entities**

1. 第 6 条第 3 項第 2 副項に定める期限に拘わらず，構成国は，必須法主体が，当該必須法主体の必須サービスの提供を混乱させ得る全ての関連リスクを評価するため，第 6 条第 3 項に示す通知の受領から 9 か月以内に，その後は，必要があるときはいつでも，かつ，少なくとも 4 年毎に，構成国リスク評価及びそれ以外の関連する情報源を基礎として，リスク評価（「必須法主体リスク評価」）を遂行することを確保する。

   Notwithstanding the deadline set out in Article 6(3), second subparagraph, Member States shall ensure that critical entities carry out a risk assessment within nine months of receiving the notification referred to in Article 6(3), whenever necessary subsequently, and at least every four years, on the basis of Member State risk assessments and other relevant sources of information, in order to assess all relevant risks that could disrupt the provision of their essential services (‘critical entity risk assessment’).

2. 必須法主体リスク評価は，部門横断の性質または国境を越える性質をもつリスクを含め，インシデントを導き得る関連する自然のリスク及び人為的なリスク，事故，自然災害，公衆衛生上の緊急事態，並びに，指令(EU) 2017/541 に定めるテロリスト行為を含め，ハイブリッドな脅威またはそれ以外の敵対的な脅威を考慮する。必須法主体リスク評価は，それが関連するときは，近隣の構成国内及び第三国内のものを含め，別紙に定める他の諸部門が，その必須法主体から提供される必須サービスに依存する程度，及び，当該必須法主体が，そのような別の諸部門の中にある別の法主体から提供される必須サービスに依存する程度を考慮に入れる。

   Critical entity risk assessments shall account for all the relevant natural and man-made risks which could lead to an incident, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid threats and other antagonistic threats, including terrorist offences as provided for in Directive (EU) 2017/541. A critical entity risk assessment shall take into account the extent to which other sectors as set out in the Annex depend on the essential service provided by the critical entity and the extent to which that critical entity depends on essential services provided by other entities in such other sectors, including, where relevant, in neighbouring Member States and third countries.

   必須法主体が，別のリスク評価を遂行したとき，または，その必須法主体の必須法主体リスク評価と関連する別の法行為の中で定められた義務により文書を作成したときは，その必須法主体は，本条に定める要件に適合するために，当該評価及び文書を利用できる。職務権限のある機関の監督の権限を行使する際，その職務権限のある機関は，必須法主体によって遂行された，関連リスク及び依存性の程度に対処する本項の第 1 副項に示す現行のリスク評価が，その全部または

一部において，この指令に定める義務を遵守するものとして宣言できる。

Where a critical entity has carried out other risk assessments or drawn up documents pursuant to obligations laid down in other legal acts that are relevant for its critical entity risk assessment, it may use those assessments and documents to meet the requirements set out in this Article. When exercising its supervisory functions, the competent authority may declare an existing risk assessment carried out by a critical entity that addresses the risks and extent of dependence referred to in the first subparagraph of this paragraph as compliant, in whole or in part, with the obligations under this Article.

第 13 条　必須法主体の回復力の措置

Article 13 **Resilience measures of critical entities**

1. 構成国は，必須法主体が，当該必須法主体の回復力を確保するため，構成国から提供される関連情報，構成国リスク評価，及び，必須法主体リスク評価の結果を基礎として，以下のために必要な措置を含め，適切かつ比例的な技術上の措置，防護上の措置及び組織上の措置を講ずることを確保する：
   (a) 災害リスクの削減措置及び気候変動適応措置を適切に検討し，インシデントの発生を防止するため；
   (b) 例えば，フェンス，障壁，境界を監視するツール及びルーチン，検出機器及びアクセス管理を適切に検討し，当該必須法主体の施設及び重要インフラの適切な物理的保護を確保するため；
   (c) リスク管理及び危機管理の手順とプロトコル並びに警報ルーチンの実装を適切に検討し，インシデントに対応し，インシデントに抗し，及び，インシデントの結果を緩和するため；
   (d) 必須サービスの提供を再開するために事業継続の措置及び代替的なサプライチェーンの識別を適切に検討し，インシデントから復旧するため；
   (e) 必須の機能を行使する要員の類型を定めること，施設，重要インフラ及び機微の情報へのアクセスの権利を設定すること，第 14 条に従った身辺調査のための手順を定めること，及び，そのような身辺調査を実施することが求められる者の類型を指定すること，並びに，適切な訓練の要件と資格を定めることのような措置を適切に検討し，従業者の安全性の管理を十分に確保するため；
   (f) 訓練課程，情報提供資料及び演習を適切に検討し，関連する要員の中において，(a)ないし(e)に示す措置に関して認識を向上させるため。

Member States shall ensure that critical entities take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:
   (a) prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures;

(b) ensure adequate physical protection of their premises and critical infrastructure, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls;
(c) respond to, resist and mitigate the consequences of incidents, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;
(d) recover from incidents, duly considering business continuity measures and the identification of alternative supply chains, in order to resume the provision of the essential service;
(e) ensure adequate employee security management, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information, setting up procedures for background checks in accordance with Article 14 and designating the categories of persons who are required to undergo such background checks, and laying down appropriate training requirements and qualifications;
(f) raise awareness about the measures referred to in points (a) to (e) among relevant personnel, duly considering training courses, information materials and exercises.

第 1 副項(e)の目的のために，構成国は，必須法主体が，必須の機能を行使する要員の類型を定める際，外部のサービスプロバイダの要員を考慮に入れることを確保する。

For the purposes of the first subparagraph, point (e), Member States shall ensure that critical entities take into account the personnel of external service providers when setting out categories of personnel who exercise critical functions.

2. 構成国は，第 1 項によって講じられる措置を記述する回復力計画またはそれと均等な 1 もしくは複数の文書を整えかつ適用することを確保する。必須法主体が，文書を作成したとき，または，第 1 項に示す措置と関連する別の法行為の中で定められた義務により措置を講じたときは，当該必須法主体は，本条に定める要件に適合するために，当該文書及び措置を利用できる。職務権限のある機関の監督の権限を行使する際，その職務権限のある機関は，第 1 項に示す技術上の措置，防護上の措置及び組織上の措置に対処する必須法主体によって適切かつ比例的な態様で講じられた現行の回復力拡大措置が，その全部または一部において，この指令に定める義務を遵守するものとして宣言できる。

Member States shall ensure that critical entities have in place and apply a resilience plan or equivalent document or documents which describe the measures taken pursuant to paragraph 1. Where critical entities have drawn up documents or taken measures pursuant to obligations laid down in other legal acts that are relevant for the measures referred to in paragraph 1, they may use those documents and measures to meet the requirements set out in this Article. When exercising its supervisory functions, the competent authority may declare existing resilience-enhancing measures taken by a critical entity that address, in an appropriate and proportionate manner, the technical, security and organisational measures referred to in paragraph 1 as compliant, in whole or in part, with the obligations under this Article.

3. 構成国は，各必須法主体が，職務権限のある機関との間の連絡場所として，連絡担当者またはそれと均等な者を指定することを確保する。

Member States shall ensure that each critical entity designates a liaison officer or equivalent as the point of contact with the competent authorities.

4. 必須法主体を識別した構成国の要請に応じて，かつ，関係する必須法主体の同意を得て，欧州委員会は，第 18 条第 6 項，第 8 項及び第 9 項に定める手立てに従い，第Ⅲ章に基づく必須法主体の義務に適合する際に，関係する必須法主体に対して助言を提供するための諮問機関を置く。その諮問機関は，欧州委員会に対し，当該構成国に対し，及び，関係する必須法主体に対し，その諮問機関の判断を報告する。

At the request of the Member State that has identified the critical entity and with the agreement of the critical entity concerned, the Commission shall organise advisory missions, in accordance with the arrangements set out in Article 18(6), (8) and (9), to provide advice to the critical entity concerned in meeting its obligations under Chapter III. The advisory mission shall report its findings to the Commission, that Member State and the critical entity concerned.

5. 欧州委員会は，第 19 条に示す必須法主体回復力グループの意見聴取を経た上で，本条の第 1 項により講じられ得る技術上の措置，防護上の措置及び組織上の措置の細目を定める拘束力のない指針を採択する。

The Commission shall, after consulting the Critical Entities Resilience Group referred to in Article 19, adopt non-binding guidelines to further specify the technical, security and organisational measures that may be taken pursuant to paragraph 1 of this Article.

6. 欧州委員会は，本条の第 1 項に示す措置の適用と関連して必要となる技術上の仕様及び手法上の仕様を定めるため，実装行為を採択する。それらの実装行為は，第 24 条第 2 項に示す審議手続に従って採択される。

The Commission shall adopt implementing acts in order to set out the necessary technical and methodological specifications relating to the application of the measures referred to in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 24(2).

第 14 条 身辺調査

Article 14 **Background checks**

1. 構成国は，適正に根拠づけられる案件において，かつ，構成国リスク評価を考慮に入れた上で，

以下の者に関し，必須法主体が身辺調査を求める要請書を提出することが認められるための条件を定める：

(a) とりわけ，その必須法主体の回復力との関係において，その必須法主体の利益となる，または，その必須法主体の利益のための機微の役割をもつ者；
(b) その必須法主体の防護と関係するものを含め，その必須法主体の施設，情報または管理システムに直接またはリモートでアクセスする権限が与えられている者；
(c) (a)または(b)に定める基準の下にある職位への採用が検討中の者。

Member States shall specify the conditions under which a critical entity is permitted, in duly reasoned cases and taking into account the Member State risk assessment, to submit requests for background checks on persons who:

(a) hold sensitive roles in or for the benefit of the critical entity, in particular in relation to the resilience of the critical entity;
(b) are authorised to directly or remotely access its premises, information or control systems, including in connection with the security of the critical entity;
(c) are under consideration for recruitment to positions that fall under the criteria set out in point (a) or (b).

2. 本条の第 1 項に示す要請書は，合理的な時間枠内で評価され，かつ，国内法及び国内手続，並びに，欧州議会及び理事会の規則(EU) 2016/679 及び指令(EU) 2016/680[37]を含め，関連する適用可能な欧州連合法に従って処理される。身辺調査は，比例的なものとし，かつ，必要な範囲内に厳格に制限される。身辺調査は，関係する必須法主体に対する潜在的なセキュリティリスクを評価する目的のためにのみ遂行される。

Requests as referred to in paragraph 1 of this Article shall be assessed within a reasonable timeframe and processed in accordance with national law and procedures and relevant and applicable Union law, including Regulation (EU) 2016/679 and Directive (EU) 2016/680 of the European Parliament and of the Council [(37)]. Background checks shall be proportionate and strictly limited to what is necessary. They shall be carried out for the sole purpose of evaluating a potential security risk to the critical entity concerned.

---

[37] 犯罪行為の防止，捜査，検知もしくは訴追または刑罰の執行の目的のために職務権限のある機関による個人データの処理と関連する自然人の保護及びそのデータの支障のない移転に関する，並びに，理事会枠組み決定 2008/977/JHA を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の指令 (EU) 2016/680(OJ L 119, 4.5.2016, p. 89).

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

3. 第 1 項に示す身辺調査は，少なくとも：
   (a) 身辺調査の対象である者の同一性を確認し；
   (b) 特定の職位と関連するような侵害行為に関し，当該の者の犯罪記録を検査する。

A background check as referred to in paragraph 1 shall, at least:
   (a) corroborate the identity of the person who is the subject of the background check;
   (b) check the criminal records of that person with regards to offences which would be relevant for a specific position.

身辺調査を遂行する際，構成国は，他の構成国によって保有されている犯罪記録から情報を入手する目的のために，枠組み決定 2009/315/JHA に定める手続に従い，及び，それが関連しかつ適用可能なときは，規則(EU) 2019/816 に定める手続に従い，欧州犯罪記録情報システムを使用する。枠組み決定 2009/315/JHA の第「3 条第 1 項及び規則(EU) 2019/816 の第 3 条第 5 号に示す中央当局は，枠組み決定 2009/315/JHA の第 8 条第 1 項に従って要請を受領した日から 10 業務日以内に，そのような情報を求める要請に対する回答を提供する。

When carrying out background checks, Member States shall use the European Criminal Records Information System in accordance with the procedures set out in Framework Decision 2009/315/JHA and, where relevant and applicable, Regulation (EU) 2019/816 for the purpose of obtaining information from criminal records held by other Member States. The central authorities referred to in Article 3(1) of Framework Decision 2009/315/JHA and in Article 3, point (5), of Regulation (EU) 2019/816 shall provide replies to requests for such information within 10 working days from the date on which the request was received in accordance with Article 8(1) of Framework Decision 2009/315/JHA.

第 15 条 インシデント通知

Article 15 **Incident notification**

1. 構成国は，必須法主体が，職務権限のある機関に対し，不適切な遅滞なく，必須サービスの提供に対して重大な混乱を発生させるインシデント，または，重大な混乱を発生させる可能性のあるインシデントを通知することを確保する。構成国は，業務運営上そのようにすることが不可能な場合を除き，必須法主体が，インシデントに気づいてから遅くとも 24 時間以内に，最初の通知を提出すること，そして，それが適切なときは，そのインシデントから遅くとも 1 か月以内に，詳細報告書によって事後対応されることを確保する。混乱の重大性を判定するため，とりわけ，以下のパラメータが考慮に入れられる：
   (a) その混乱によって影響を受けた利用者の数及び割合；
   (b) その混乱の持続期間；
   (c) その領域が地理的に孤立しているかどうかを考慮に入れた上で，その混乱によって影響を受けた地理的領域。

Member States shall ensure that critical entities notify the competent authority, without undue delay, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. Member States shall ensure that, unless operationally unable to do so, critical entities submit an initial notification no later than 24 hours after becoming aware of an incident, followed, where relevant, by a detailed report no later than one month thereafter. In order to determine the significance of a disruption, the following parameters shall, in particular, be taken into account:

(a) the number and proportion of users affected by the disruption;
(b) the duration of the disruption;
(c) the geographical area affected by the disruption, taking into account whether the area is geographically isolated.

インシデントが，6 以上の構成国に対しまたは 6 以上の構成国内で，必須サービスの提供の継続に重大な影響をもつ場合，または，重大な影響をもつかもしれない場合，そのインシデントによって影響を受ける構成国の職務権限のある機関は，欧州委員会に対し，当該インシデントを通知する。

Where an incident has or might have a significant impact on the continuity of the provision of essential services to or in six or more Member States, the competent authorities of the Member States affected by the incident shall notify the Commission of that incident.

2. 第 1 項第 1 副項に示す通知は，職務権限のある機関が，そのインシデントの国境を越える影響を判定するために必要となる利用可能な情報を含め，そのインシデントの性質，原因及びあり得る結果を理解できるようにするために必要となる利用可能な情報を含める。そのような通知は，必須法主体を，法的責任の増加に服させてはならない。

Notifications as referred to in paragraph 1, first subparagraph, shall include any available information necessary to enable the competent authority to understand the nature, cause and possible consequences of the incident, including any available information necessary to determine any cross-border impact of the incident. Such notifications shall not subject critical entities to increased liability.

3. 第 1 項に示す通知の中で必須法主体から提供された情報を基礎として，関連する職務権限のある機関は，1 もしくは複数の構成国に対しまたは 1 もしくは複数の構成国内で，必須法主体及び必須サービスの提供の継続に重大な影響をもつ場合，または，重大な影響をもつかもしれない場合，単一連絡部局を介して，影響を受ける別の構成国の単一連絡部局に対し，連絡する。

On the basis of the information provided by a critical entity in a notification as referred to in paragraph 1, the relevant competent authority, via the single point of contact, shall inform the single point of contact of other affected Member States where the incident has or might have a significant impact on critical entities and the continuity of the provision of essential services to or in one or more other Member States.

第 1 副項により情報を送付及び受領する単一連絡部局は，欧州連合法または国内法に従い，当該情報の機密性を尊重し，かつ，関係する必須法主体の防護及び商業上の利益を保護する方法で，当該情報を取扱う。

Single points of contact sending and receiving information pursuant to the first subparagraph shall, in accordance with Union or national law, treat that information in a way that respects its confidentiality and protects the security and commercial interest of the critical entity concerned.

4. 第 1 項に示す通知の後，可能な限り速やかに，関係する職務権限のある機関は，関係する必須法主体に対し，当のインシデントに対する当該必須法主体の実効性のある対応を支援し得る情報を含め，関連する事後対応情報を提供する。構成国は，そのようにすることが公共の利益となり得ると判断したときは，公衆に対して連絡する。

As soon as possible following a notification as referred to in paragraph 1, the competent authority concerned shall provide the critical entity concerned with relevant follow-up information, including information that could support that critical entity's effective response to the incident in question. Member States shall inform the public where they determine that it would be in the public interest to do so.

第 16 条 技術標準

Article 16 **Standards**

この指令の一貫性のある実装を促進するため，構成国は，それが有用であるときは，かつ，特定のタイプの技術の利用を課すことなく，または，特定のタイプの技術の利用を有利に差別化することなく，必須法主体に適用可能な防護の措置及び回復力の措置と関連する欧州の技術標準及び国際的な技術標準並びに技術仕様の利用を推奨する。

In order to promote the convergent implementation of this Directive, Member States shall, where useful and without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security and resilience measures applicable to critical entities.

第Ⅳ章 欧州の特別に重要な必須法主体
Chapter IV Critical Entities of Particular European Significance

第 17 条 欧州の特別に重要な必須法主体の識別
Article 17 **Identification of critical entities of particular European significance**

1. その法主体が, 以下のとおりである場合, 法主体は, 欧州の特別に重要な必須法主体と判断される:
   (a) 第 6 条第 1 項により必須法主体として識別された;
   (b) 6 以上の構成国に対しまたは 6 以上の構成国内において, 同一または類似の必須サービスを提供している;かつ
   (c) 本条の第 3 項による通知を受けた。

   An entity shall be considered a critical entity of particular European significance where it:
   (a) has been identified as a critical entity pursuant to Article 6(1);
   (b) provides the same or similar essential services to or in six or more Member States; and
   (c) has been notified pursuant to paragraph 3 of this Article.

2. 構成国は, 6 以上の構成国に対してまたは 6 以上の構成国内において必須法主体が必須サービスを提供しているときは, 必須法主体が, 第 6 条第 3 項に示す通知を受けた後, その通知をした構成国の職務権限のある機関に対し, 連絡することを確保する。そのような場合, 構成国は, その必須法主体が, その通知をした構成国の職務権限のある機関に対し, 当該必須法主体が当該 6 以上の構成国に対してまたは 6 以上の構成国内で提供している必須サービスに関し, 及び, 当該 6 以上の構成国に対しまたは当該 6 以上の構成国内で当該必須法主体がそのような必須サービスを提供している構成国に関し, 連絡することを確保する。構成国は, 欧州委員会に対し, 不適切な遅滞なく, そのような必須法主体の識別名及び本項に基づいて当該法主体が提供した情報を通知する。

   Member States shall ensure that a critical entity, following the notification referred to in Article 6(3), informs its competent authority where it provides essential services to or in six or more Member States. In such a case, Member States shall ensure that the critical entity informs its competent authority of the essential services it provides to or in those Member States and of the Member States to which or in which it provides such essential services. Member States shall notify the Commission, without undue delay, of the identity of such critical entities and of the information they provide under this paragraph.

   欧州委員会は, 第 1 副項に示す必須法主体を識別した構成国の職務権限のある機関, 関係する別の構成国の職務権限のある機関, 及び, 当の必須法主体と協議する。当該協議の間, 各構成国は, その必須法主体から当該構成国に対して提供されているサービスが必須サービスであると当該構成国が判断するときは, 欧州委員会に対し, 連絡する。

The Commission shall consult the competent authority of the Member State which identified a critical entity as referred to in the first subparagraph, the competent authority of other Member States concerned and the critical entity in question. During those consultations, each Member State shall inform the Commission where it deems that the services provided to that Member State by the critical entity are essential services.

3. 本条の第 2 項に示す意見聴取を基礎として，関係する必須法主体が 6 以上の構成国に対してまたは 6 以上の構成国内で必須サービスを提供していると欧州委員会が判断するときは，欧州委員会は，当該必須法主体に対し，その通知をした構成国の職務権限のある機関を介して，欧州の特別に重要な必須法主体であると判断される旨を通知し，かつ，当該必須法主体に対し，本章に基づく当該必須法主体の義務，及び，当該義務が当該必須法主体に対して適用される開始日を連絡する。欧州委員会が，職務権限のある機関に対し，必須法主体を欧州の特別に重要な必須法主体であると判断する欧州委員会の決定を連絡した後，その職務権限のある機関は，不適切な遅滞なく，当該通知を当該必須法主体に対して転送する。

Where the Commission establishes, on the basis of the consultations referred to in paragraph 2 of this Article, that the critical entity concerned provides essential services to or in six or more Member States, the Commission shall notify that critical entity, through its competent authority, that it is considered a critical entity of particular European significance and inform that critical entity of its obligations under this Chapter and the date from which those obligations apply to it. Once the Commission informs the competent authority of its decision to consider a critical entity as a critical entity of particular European significance, the competent authority shall forward that notification to that critical entity without undue delay.

4. 本章は，関係する欧州の特別に重要な必須法主体に対し，本条の第 3 項に示す通知を受領した日から適用される。

This Chapter shall apply to the critical entity of particular European significance concerned from the date of receipt of the notification referred to in paragraph 3 of this Article.

第 18 条 諮問機関

Article 18 **Advisory missions**

1. 欧州の特別に重要な必須法主体を第 6 条第 1 項により必須法主体として識別した構成国の要請に応じて，欧州委員会は，当該必須法主体が当該必須法主体の第Ⅲ章に基づく義務に適合するために設けた措置を評価するための諮問機関を置く。

At the request of the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1), the Commission shall organise an advisory mission to assess

the measures that that critical entity has put in place to meet its obligations under Chapter III.

2. 欧州委員会自身の発意により，または，その構成国に対してもしくはその構成国の中でその必須サービスが提供されている 1 もしくは複数の構成国の要請に応じて，かつ，欧州の特別に重要な必須法主体を第 6 条第 1 項により必須法主体として識別した構成国がそのように同意することを条件として，欧州委員会は，本条の第 1 項に示す諮問機関を置く。

On its own initiative or at the request of one or more Member States to or in which the essential service is provided, and provided that the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1) so agrees, the Commission shall organise an advisory mission as referred to in paragraph 1 of this Article.

3. 欧州委員会からの理由を付した要請に応じて，または，その構成国に対してもしくはその構成国の中でその必須サービスが提供されている 1 もしくは複数の構成国からの理由を付した要請に応じて，欧州の特別に重要な必須法主体を第 6 条第 1 項により必須法主体として識別した構成国は，欧州委員会に対し，以下のものを提供する：
   (a) 必須法主体リスク評価の関連部分；
   (b) 第 13 条に従って講じられた関連措置のリスト；
   (c) 遵守の評価書または発令された命令書を含め，当該必須法主体との関係において当該構成国の職務権限のある機関が第 21 条及び第 22 条により実施した監督活動または執行活動。

On a reasoned request from the Commission or from one or more Member States to or in which the essential service is provided, the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1) shall provide the following to the Commission:
   (a) the relevant parts of the critical entity risk assessment;
   (b) a list of relevant measures taken in accordance with Article 13;
   (c) supervisory or enforcement actions, including assessments of compliance or orders issued, that its competent authority has undertaken pursuant to Articles 21 and 22 in respect of that critical entity.

4. 諮問機関は，その諮問機関が結論を得た時から 3 か月以内に，欧州委員会，欧州の特別に重要な必須法主体を第 6 条第 1 項により必須法主体として識別した構成国，その構成国に対してまたはその構成国の中でその必須サービスが提供されている構成国，及び，関係する必須法主体に対し，その諮問機関の判断を報告する。

The advisory mission shall report its findings to the Commission, to the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1), to the Member States to or in which the essential service is provided and to the critical entity concerned within three months of the conclusion of the advisory mission.

その構成国に対してまたはその構成国の中でその必須サービスが提供されている構成国は，第 1 副項に示す報告を分析し，かつ，それが必要なときは，欧州委員会に対し，関係する欧州の特別に重要な必須法主体が第Ⅲ章に基づく当該必須法主体の義務を遵守しているかどうかに関し，及び，それが適切なときは，当該必須法主体の回復力を向上させるために講じられ得る措置に関し，助言する。

The Member States to or in which the essential service is provided shall analyse the report referred to in the first subparagraph and, where necessary, shall advise the Commission as to whether the critical entity of particular European significance concerned complies with its obligations under Chapter III and, where appropriate, as to the measures which could be taken to improve the resilience of that critical entity.

欧州委員会は，本項の第 2 副項に示す助言を基礎として，欧州の特別に重要な必須法主体を第 6 条第 1 項により必須法主体として識別した構成国，その構成国に対してまたはその構成国の中でその必須サービスが提供されている構成国，及び，その必須法主体に対し，当該必須法主体が第Ⅲ章に基づく当該必須法主体の義務を遵守しているかどうかに関し，及び，それが適切なときは，当該必須法主体の回復力を向上させるために講じられ得る措置に関し，欧州委員会の意見を通知する。

The Commission shall, based on the advice referred to in the second subparagraph of this paragraph, communicate its opinion to the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1), to the Member States to or in which the essential service is provided and to that critical entity as to whether that critical entity complies with its obligations under Chapter III and, where appropriate, as to the measures which could be taken to improve the resilience of that critical entity.

欧州の特別に重要な必須法主体を第 6 条第 1 項により必須法主体として識別した構成国は，その構成国の職務権限のある機関及び関係する必須法主体が，本項第 3 副項に示す意見を考慮に入れること，並びに，欧州委員会及びその構成国に対してまたはその構成国の中でその必須サービスが提供されている構成国に対し，当該意見により講じられた措置に関する情報を提供することを確保する。

The Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1) shall ensure that its competent authority and the critical entity concerned take into account the opinion referred to in the third subparagraph of this paragraph and provide information to the Commission and the Member States to or in which the essential service is provided on the measures it has taken pursuant to that opinion.

5. 個々の諮問機関は，欧州の特別に重要な必須法主体が所在する構成国の専門家，その構成国に対してまたはその構成国の中でその必須サービスが提供されている構成国の専門家，及び，欧州委員会の代表によって構成される。当該構成国は，諮問機関の一部となる候補者を提案で

きる。欧州委員会は，欧州の特別に重要な必須法主体を第 6 条第 1 項により必須法主体として識別した構成国の意見聴取を経た上で，当該の者の専門家としての実現能力に従って，かつ，それが可能なときは，当該全ての構成国からの地理的にバランスのとれた代表を確保して，個々の諮問機関の構成員を選抜し，任命する。必要があるときはいつでも，諮問機関の構成員は，有効かつ適切なセキュリティクリアランスをもつものとする。欧州委員会は，諮問機関への参加と関連する費用を負担する。

Each advisory mission shall consist of experts from the Member State in which the critical entity of particular European significance is located, experts from the Member States to or in which the essential service is provided, and Commission representatives. Those Member States may propose candidates to be part of an advisory mission. The Commission shall, following a consultation with the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1), select and appoint the members of each advisory mission in accordance with their professional capacity and ensuring, where possible, a geographically balanced representation from all those Member States. Whenever necessary, members of the advisory mission shall have valid and appropriate security clearance. The Commission shall bear the costs related to participation in advisory missions.

欧州委員会は，当の諮問機関の構成員との間の意見聴取を経た上で，かつ，欧州の特別に重要な必須法主体を第 6 条第 1 項により必須法主体として識別した構成国の同意を得た上で，個々の諮問機関の計画を定める。

The Commission shall organise the programme of each advisory mission, in consultation with the members of the advisory mission in question and in agreement with the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1).

6. 欧州委員会は，関係する情報の機密性及び商業上の機微性を適切に考慮に入れた上で，諮問機関を置くことの要請に関する，そのような要請の取扱いに関する，諮問機関の行動及び報告に関する，並びに，本条の第 4 項第 3 副項に示す欧州委員会の意見及び講じられた措置の通知の取扱いに関する手続覚書に関する規定を定める実装行為を採択する。同実装行為は，第 24 条第 2 項に示す審議手続に従って採択される。

The Commission shall adopt an implementing act laying down rules on the procedural arrangements for requests to organise advisory missions, for handling such requests, for the conduct and reports of advisory missions and for handling the communication of the Commission's opinion referred to in paragraph 4, third subparagraph, of this Article and of the measures taken, duly taking into account the confidentiality and commercial sensitivity of the information concerned. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 24(2).

7. 構成国は，欧州の特別に重要な必須法主体が，諮問機関に対し，関係する諮問の任務を遂行するために必要となる当該必須法主体の必須サービスの提供と関連する情報，システム及び施設

へのアクセスを提供することを確保する。

Member States shall ensure that critical entities of particular European significance provide advisory missions with access to information, systems and facilities relating to the provision of their essential services necessary for carrying out the advisory mission concerned.

8. 諮問の任務は，当該諮問の任務が生ずる構成国の適用可能な国内法に従い，国家安全保障及び保安の利益の防護に関する当該構成国の職責を尊重して，遂行される。

Advisory missions shall be carried out in compliance with the applicable national law of the Member State in which they take place, with respect for that Member State's responsibility for national security and the protection of its security interests.

9. 諮問機関を置くときは，欧州委員会は，規則(EC) No 725/2004 及び規則(EC) No 300/2008 の下で欧州委員会によって遂行される検査の報告書，並びに，関係する必須法主体と関係して指令 2005/65/EC の下で欧州委員会によって遂行される監視の報告書を考慮に入れる。

When organising advisory missions, the Commission shall take into account the reports of any inspections carried out by the Commission under Regulations (EC) No 725/2004 and (EC) No 300/2008 and the reports of any monitoring carried out by the Commission under Directive 2005/65/EC in respect of the critical entity concerned.

10. 欧州委員会は，諮問機関が置かれたときはいつでも，第 19 条に示す必須法主体回復力グループに対して連絡する。諮問の任務が生じた構成国及び欧州委員会は，必須法主体回復力グループに対し，諮問機関の主要な判断結果及び相互学習を促進する観点から学んだ教訓も連絡する。

The Commission shall inform the Critical Entities Resilience Group referred to in Article 19 whenever an advisory mission is organised. The Member State in which the advisory mission took place and the Commission shall also inform the Critical Entities Resilience Group of the main findings of the advisory mission and the lessons learned with a view to promoting mutual learning.

第Ⅴ章 協力及び報告

Chapter V Cooperation and Reporting

第 19 条 必須法主体回復力グループ

Article 19 **Critical Entities Resilience Group**

1. 必須法主体回復力グループが，ここに設置される。必須法主体回復力グループは，欧州委員会を支援し，かつ，構成国間の協力及びこの指令と関連する問題に関する情報の交換を容易にする。

   A Critical Entities Resilience Group is hereby established. The Critical Entities Resilience Group shall support the Commission and facilitate cooperation among Member States and the exchange of information on issues relating to this Directive.

2. 必須法主体回復力グループは，それが適切なときはセキュリティクリアランスをもつ構成国の代表及び欧州委員会の代表によって構成される。同グループの職務を遂行するために適切なときは，必須法主体回復力グループは，関連する利害関係者に対し，同グループの作業に参加することを招請できる。欧州議会から要請を受けたときは，欧州委員会は，欧州議会の専門家に対し，必須法主体回復力グループの会合に出席することを招請できる。

   The Critical Entities Resilience Group shall be composed of representatives of the Member States and the Commission who hold security clearance, where appropriate. Where relevant for the performance of its tasks, the Critical Entities Resilience Group may invite relevant stakeholders to participate in its work. Where requested by the European Parliament, the Commission may invite experts from the European Parliament to attend meetings of the Critical Entities Resilience Group.

   欧州委員会の代表は，必須法主体回復力グループを主宰する。

   The Commission's representative shall chair the Critical Entities Resilience Group.

3. 必須法主体回復力グループは，以下の職務をもつ：
   (a) この指令に従い，必須法主体の回復力を確保することに寄与する構成国の実現能力を強化する上で構成国を補助することにおいて，欧州委員会を支援すること；
   (b) 戦略と関係するベストプラクティスを発見するため，戦略を分析すること；
   (c) 国境を越える依存性及び部門横断の依存性との関係におけるもの，並びに，リスク及びインシデントと関連するものを含め，第 6 条第 1 項による構成国による必須法主体の識別と関連するベストプラクティスの交換を容易にすること；
   (d) それが適切なときは，この指令と関連する問題に関し，欧州連合レベルの回復力に関する文書に寄与すること；

(e) 第 7 条第 3 項及び第 13 条第 5 項に示すガイドの準備，並びに，要請に応じて，この指令により採択される委任される行為または実装行為の準備に貢献すること；
(f) 第 15 条第 3 項に従って講じられた活動に関するベストプラクティスの交換を促進するという観点から，第 9 条第 3 項に示す要旨報告書を分析すること；
(g) 第 15 条に示すインシデントの通知と関連するベストプラクティスを共有すること；
(h) 諮問機関の要旨報告書及び第 18 条第 10 項に従って学んだ教訓を討議すること；
(i) この指令に従った必須法主体の回復力と関係する技術革新，調査研究及び発展に関し，情報及びベストプラクティスを交換すること；
(j) それが適切なときは，関連する欧州連合の機関，組織，事務局及び部局との間で，必須法主体の回復力と関係する事項に関する情報を交換すること。

The Critical Entities Resilience Group shall have the following tasks:
(a) supporting the Commission in assisting Member States in reinforcing their capacity to contribute to ensuring the resilience of critical entities in accordance with this Directive;
(b) analysing the strategies in order to identify best practices in respect of the strategies;
(c) facilitating the exchange of best practices with regard to the identification of critical entities by the Member States pursuant to Article 6(1), including in relation to cross-border and cross-sectoral dependencies and regarding risks and incidents;
(d) where appropriate, contributing on issues relating to this Directive to documents concerning resilience at Union level;
(e) contributing to the preparation of the guidelines referred to in Article 7(3) and Article 13(5) and, upon request, any delegated or implementing acts adopted pursuant to this Directive;
(f) analysing the summary reports referred to in Article 9(3) with a view to promoting the sharing of best practices on the action taken in accordance with Article 15(3);
(g) exchanging best practices related to the notification of incidents referred to in Article 15;
(h) discussing the summary reports of advisory missions and the lessons learned in accordance with Article 18(10);
(i) exchanging information and best practices on innovation, research and development relating to the resilience of critical entities in accordance with this Directive;
(j) where relevant, exchanging information on matters concerning the resilience of critical entities with relevant Union institutions, bodies, offices and agencies.

4. 2025 年 1 月 17 日までに，かつ，その後は 2 年毎に，必須法主体回復力グループは，同グループの目的及び職務を実装するために実施される活動と関係する作業計画を策定する。同作業計画は，この指令の要件及び目的と一貫性のあるものとする。

By 17 January 2025 and every two years thereafter, the Critical Entities Resilience Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks. That work programme shall be consistent with the requirements and objectives of this Directive.

5. 必須法主体回復力グループは，定期的に，かつ，いかなる場合においても少なくとも年 1 回，指令(EU) 2022/2555 の下において設置された協力グループとの間で，協力及び情報交換を促進し，容易にするために会合する。

The Critical Entities Resilience Group shall meet on a regular basis and in any event at least once a year with the Cooperation Group established under Directive (EU) 2022/2555 to promote and facilitate cooperation and the exchange of information.

6. 欧州委員会は，第 1 条第 4 項を尊重し，必須法主体回復力グループの稼働のために必要となる手続覚書を定める実装行為を採択できる。同実装行為は，第 24 条第 2 項に示す審議手続に従って採択される。

The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the Critical Entities Resilience Group, respecting Article 1(4). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 24(2).

7. 欧州委員会は，2027 年 1 月 17 日までに，その後は必要があるときはいつでも，かつ，少なくとも 4 年毎に，必須法主体回復力グループに対し，第 4 条第 3 項及び第 5 条第 4 項により構成国から提供された情報の要旨報告書を提供する。

The Commission shall provide the Critical Entities Resilience Group with a summary report of the information provided by the Member States pursuant to Article 4(3) and Article 5(4) by 17 January 2027, whenever necessary subsequently, and at least every four years.

第 20 条　職務権限のある機関及び必須法主体に対する欧州委員会の支援

Article 20 **Commission support to competent authorities and critical entities**

1. 欧州委員会は，それが適切なときは，構成国及び必須法主体に対し，この指令に基づく構成国及び必須法主体の義務の遵守において支援する。欧州委員会は，必須サービスの提供を妨げる国境を越えるリスク及び部門横断のリスクの欧州連合レベルの概観を準備し，第 13 条第 4 項及び第 18 条に示す諮問機関を置き，構成国及び欧州連合全域にわたる専門家の間の情報交換を容易にする。

The Commission shall, where appropriate, support Member States and critical entities in complying with their obligations under this Directive. The Commission shall prepare a Union-level overview of cross-border and cross-sectoral risks to the provision of essential services, organise advisory missions as referred to in Article 13(4) and Article 18 and facilitate information exchange among Member States and experts across the Union.

2. 欧州委員会は，ベストプラクティス，ガイド資料及び手法を作成すること，並びに，国境を越える訓練活動及び必須法主体の回復力を試験するための演習によって，第 10 条に示す構成国の活動を補完する。

The Commission shall complement Member States' activities as referred to in Article 10 by developing best practices, guidance materials and methodologies, and cross-border training activities and exercises to test the resilience of critical entities.

3. 欧州委員会は，構成国に対し，必須法主体の回復力を拡大するために構成国にとって利用可能な欧州連合レベルの資金に関し，情報提供する。

The Commission shall inform Member States about financial resources at Union level available to Member States for enhancing the resilience of critical entities.

第VI章 監督及び執行

Chapter VI Supervision and Enforcement

第 21 条 監督及び執行

Article 21 **Supervision and enforcement**

1. 第 6 条第 1 項により構成国によって必須法主体として識別された法主体によるこの指令に定める義務の遵守を評価するため，構成国は，職務権限のある機関が，以下のための権限及び手段をもつことを確保する：
   (a) 重要インフラ及びその必須法主体がその必須法主体の必須サービスを提供するために使用している施設において，施設内における検査を実施するため，並びに，第 13 条に従って必須法主体によって講じられた措置の施設外における監督を実施するため；
   (b) 必須法主体と関係する監査を実施するためまたはそれを命ずるため。

   In order to assess the compliance of the entities identified by Member States as critical entities pursuant to Article 6(1) with the obligations laid down in this Directive, Member States shall ensure that the competent authorities have the powers and means to:
   (a) conduct on-site inspections of the critical infrastructure and the premises that the critical entity uses to provide its essential services, and off-site supervision of measures taken by critical entities in accordance with Article 13;
   (b) conduct or order audits in respect of critical entities.

2. 構成国は，職務権限のある機関が，この指令に基づく当該職務権限のある機関の職務の遂行のために必要があるときは，この指令の下において必須法主体として構成国が識別した指令(EU) 2022/2555 の下における法主体が当該職務権限のある機関によって定められた合理的な期限内に以下のものを提供することを命ずる権限及び手段をもつことを確保する：
   (a) 当該法主体の回復力を確保するために当該法主体によって講じられた措置が第 13 条に定める要件に適合しているか否かを評価するために必要となる情報；
   (b) 当該法主体によって選択され，かつ，当該法主体の費用負担で実施された独立かつ資格のある監査者によって実施された監査結果を含め，当該措置の実効的な実装の証拠。

   Member States shall ensure that the competent authorities have the powers and means to require, where necessary for the performance of their tasks under this Directive, that the entities under Directive (EU) 2022/2555 that Member States have identified as critical entities under this Directive provide, within a reasonable time limit set by those authorities:
   (a) the information necessary to assess whether the measures taken by those entities to ensure their resilience meet the requirements set out in Article 13;
   (b) evidence of the effective implementation of those measures, including the results of an audit conducted by an independent and qualified auditor selected by that entity and conducted at its

expense.

当該情報を要求する際, その職務権限のある機関は, 要求の目的を示し, かつ, 要求される情報を特定する。

When requiring that information, the competent authorities shall state the purpose of the requirement and specify the information required.

3. 第 22 条に従って罰を科すことができることを妨げることなく, 職務権限のある機関は, 本条の第 1 項に示す監督の活動または本条の第 2 項に示す情報の評価を経た上で, 関係する必須法主体に対し, 当該職務権限のある機関によって定められた合理的な期限内に, 発見されたこの指令の違反行為を是正するための必要かつ比例的な措置を講ずることを命じ, かつ, 当該職務権限のある機関に対し, 講じられた措置に関する情報を提供することを命じ得る。それらの命令は, とりわけ, その違反行為の重大性を考慮に入れる。

Without prejudice to the possibility to impose penalties in accordance with Article 22, the competent authorities may, following the supervisory actions referred to in paragraph 1 of this Article or the assessment of the information referred to in paragraph 2 of this Article, order the critical entities concerned to take the necessary and proportionate measures to remedy any identified infringement of this Directive, within a reasonable time limit set by those authorities, and to provide those authorities with information on the measures taken. Those orders shall take into account, in particular, the seriousness of the infringement.

4. 構成国は, 第 1 項, 第 2 項及び第 3 項に定める権限が, 適切な安全確保に服する場合に限り行使され得ることを確保する。当該安全確保は, とりわけ, そのような行使が客観的であり, 透明性があり, かつ, 比例的な態様で行われること, そして, 営業秘密及び企業秘密の保護のような, 影響を受ける必須法主体の権利及び正当な利益が, 聴聞を受ける権利, 防御の権利及び独立の裁判所における実効的な救済の権利を含め, 適正に安全確保されることを保証する。

Member State shall ensure that the powers provided for in paragraphs 1, 2 and 3 can only be exercised subject to appropriate safeguards. Those safeguards shall guarantee, in particular, that such exercise takes place in an objective, transparent and proportionate manner, and that the rights and legitimate interests of the critical entities affected, such as the protection of trade and business secrets, are duly safeguarded, including the right to be heard, the right of defence and the right to an effective remedy before an independent court.

5. 構成国は, この指令の下にある職務権限のある機関が本条による必須法主体の遵守を評価する場合, 当該職務権限のある機関が, 関係する構成国の指令(EU) 2022/2555 の下にある職務権限のある機関に対し, 連絡することを確保する。その目的のために, 構成国は, この指令の下にある職務権限のある機関が, 当該職務権限のある機関に対し, この指令の下において必須法主体

として識別された指令(EU) 2022/2555 の下にある職務権限のある機関との関係において，指令(EU) 2022/2555 の下にある職務権限のある機関の監督及び執行の権限を行使することを要請できることを確保する。その目的のために，構成国は，この指令の下にある職務権限のある機関が，指令(EU) 2022/2555 の下にある職務権限のある機関との間において，協力し，かつ，情報を交換することを確保する。

Member States shall ensure that, where a competent authority under this Directive assesses the compliance of a critical entity pursuant to this Article, that competent authority informs the competent authorities of the Member States concerned under Directive (EU) 2022/2555. For that purpose, Member States shall ensure that competent authorities under this Directive can request the competent authorities under Directive (EU) 2022/2555 to exercise their supervisory and enforcement powers in relation to an entity under that Directive that has been identified as a critical entity under this Directive. For that purpose, Member States shall ensure that competent authorities under this Directive cooperate and exchange information with the competent authorities under Directive (EU) 2022/2555.

第 22 条 罰則

Article 22 **Penalties**

構成国は，この指令により採択された国内措置の違反行為に対して適用可能な罰に関する規定を定め，かつ，当該規定が実装されることを確保するために必要となる全ての措置を講ずる。定められる罰は，実効的であり，比例的かつ抑止力のあるものとする。構成国は，2024 年 10 月 17 日までに，欧州委員会に対し，当該規定及び当該措置を通知し，かつ，欧州委員会に対し，遅滞なく，当該規定に影響を与えるその後の改正を通知する。

Member States shall lay down the rules on penalties applicable to infringements of the national measures adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by 17 October 2024, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

第VII章　委任される行為及び実装行為
Chapter VII Delegated and Implementing Acts

第 23 条　委任の実行
Article 23 **Exercise of the delegation**

1. 委任される行為を採択する権限は，本条に定める条件に従い，欧州委員会に対して与えられる。

   The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. 第 5 条第 1 項に示す委任される行為を採択する権限は，2023 年 1 月 16 日から 5 年間，欧州委員会に対して与えられる。

   The power to adopt delegated acts referred to in Article 5(1) shall be conferred on the Commission for a period of five years from 16 January 2023.

3. 第 5 条第 1 項に示す権限の委任は，いつでも，欧州議会または理事会によって取消され得る。取消しの決定は，同決定の中で指示される権限の委任を終了させる。その決定は，EU 官報上でその決定が公示された翌日に発効し，または，その決定の中で指定された後の日に発効する。その決定は，既に発効している委任される行為の有効性に影響を与えてはならない。

   The delegation of power referred to in Article 5(1) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. 委任される行為を採択する前に，欧州委員会は，より良い立法に関する 2016 年 4 月 13 日の機関間合意に定める基本原則に従い，各構成国から指定された専門家から意見聴取する。

   Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. 欧州委員会が委任される行為を採択したときは直ちに，欧州委員会は，欧州議会及び理事会に対し，同時に通知する。

   As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European

Parliament and to the Council.

6. 第 5 条第 1 項によって採択された委任される行為は，欧州議会及び理事会に対する当該行為の通知から 2 か月以内に欧州議会もしくは理事会のいずれからも異議が表明されないとき，または，その期間が満了する前に，欧州議会及び理事会の両者が欧州委員会に対して異議を述べない旨を連絡したときに限り発効する。その期間は，欧州議会の発意または理事会の発意により，2 か月まで延長される。

A delegated act adopted pursuant to Article 5(1) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

第 24 条 委員会の手続

Article 24 **Committee procedure**

1. 欧州委員会は，委員会による補佐をうける。同委員会は，規則(EU) No 182/2011 の意味における委員会である。

The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. 本項に対する参照があるときは，規則(EU) No 182/2011 の第 5 条が適用される。

Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

第Ⅷ章 最終規定
Chapter VIII Final Provisions

第 25 条 報告及び見直し
Article 25 **Reporting and review**

2027 年 7 月 17 日までに, 欧州委員会は, 欧州議会及び理事会に対し, 各構成国が講じた, この指令を遵守するために必要となる措置の範囲を評価する報告書を提出する。

By 17 July 2027, the Commission shall submit to the European Parliament and to the Council a report assessing the extent to which each Member State has taken the necessary measures to comply with this Directive.

欧州委員会は, 定期的に, この指令の稼働を見直し, かつ, 欧州議会及び理事会に対し, 報告する。同報告書は, とりわけ, この指令の付加価値, 必須法主体の回復力を確保することに対するこの指令の影響, 及び, この指令の別紙が修正されるべきか否かを評価する。欧州委員会は, 2029 年 6 月 17 日までに, 最初のそのような報告書を提出する。本条の報告の目的のために, 欧州委員会は, 必須法主体回復力グループの関連文書を考慮に入れる。

The Commission shall periodically review the functioning of this Directive and report to the European Parliament and to the Council. That report shall, in particular, assess the added value of this Directive, its impact on ensuring the resilience of critical entities and whether the Annex to this Directive should be modified. The Commission shall submit the first such report by 17 June 2029. For the purpose of reporting under this Article, the Commission shall take into account relevant documents of the Critical Entities Resilience Group.

第 26 条 国内法化
Article 26 **Transposition**

1. 2024 年 10 月 17 日までに, 構成国は, この指令を遵守するために必要となる措置を採択及び公示する。当該構成国は, 欧州委員会に対し, 直ちに, 当該措置を連絡する。

   By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

   当該構成国は, 2024 年 10 月 18 日から当該措置を適用する。

   They shall apply those measures from 18 October 2024.

2. 構成国が第 1 項に示す措置を採択する際, 当該措置は, この指令に対する参照を含めるものとし, または, 当該措置の公示の際にそのような参照を添えるものとする。そのような参照を行う手法は, 構成国によって定められる。

When Member States adopt the measures referred to in paragraph 1, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

第 27 条 指令 2008/114/EC の廃止

Article 27 **Repeal of Directive 2008/114/EC**

指令 2008/114/EC は, 2024 年 10 月 18 日から発効するものとして廃止される。

Directive 2008/114/EC is repealed with effect from 18 October 2024.

廃止される指令に対する参照は, この指令に対する参照として解釈される。

References to the repealed Directive shall be construed as references to this Directive.

第 28 条 発効

Article 28 **Entry into force**

この指令は, EU 官報上のその公示の 20 日後に発効する。

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

第 29 条 発出

Article 29 **Addressees**

この指令は, 構成国に対して発出される。

This Directive is addressed to the Member States.

ストラスブールにおいて, 2022 年 12 月 14 日に行われた。

Done at Strasbourg, 14 December 2022.

欧州議会として	理事会として
For the European Parliament	For the Council
議長　R. METSOLA	議長　M. BEK
The President　R. METSOLA	The President　M. BEK

別紙　法主体の部門, 副部門及び類型

ANNEX SECTORS, SUBSECTORS AND CATEGORIES OF ENTITIES

部門 Sector	副部門 Subsector	法主体の類型 Categories of entities
1.エネルギー Energy	(a)電力 Electricity	－欧州議会及び理事会の指令(EU) 2019/944[1] の第 2 条第 57 号に定義する電力事業者であって, 同指令の第 2 条第 12 号に定義する「供給」の機能を遂行する者 Electricity undertakings as defined in Article 2, point (57), of Directive (EU) 2019/944 of the European Parliament and of the Council[(1)], which carry out the function of 'supply' as defined in Article 2, point (12), of that Directive
		－指令(EU) 2019/944 の第 2 条第 29 号に定義する配電システムの運営者 Distribution system operators as defined in Article 2, point (29), of Directive (EU) 2019/944
		－指令(EU) 2019/944 の第 2 条第 35 号に定義する送電システムの運営者 Transmission system operators as defined in Article 2, point (35), of Directive (EU) 2019/944
		－指令(EU) 2019/944 の第 2 条第 38 号に定義する製造者 Producers as defined in Article 2, point (38), of Directive (EU) 2019/944
		－欧州議会及び理事会の規則(EU) 2019/943[2] の第 2 条第 8 号に定義する指定された電力市場の運営者 Nominated electricity market operators as defined in Article 2, point (8), of Regulation (EU) 2019/943 of the European Parliament and of the Council[(2)]
		－指令(EU) 2019/944 の第 2 条第 18 号, 第 20 号及び第 59 号に定義する集約サービス, 需要対応サービスまたは蓄電サービスを提供する規則(EU) 2019/943 の第 2 条第 25 号に定義する市場参加者 Market participants as defined in Article 2, point (25), of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services as defined in Article 2, points (18), (20) and (59), of Directive (EU) 2019/944
	(b) 地域冷暖房 District heating	－欧州議会及び理事会の指令(EU) 2018/2001[3] の第 2 条第 19 号に定義する地域冷暖房の運営者 Operators of district heating or district cooling as defined in Article

	and cooling	2, point (19), of Directive (EU) 2018/2001 of the European Parliament and of the Council (3)
	(c)石油 Oil	－送油パイプラインの運営者 Operators of oil transmission pipelines
		－石油の製造, 精製及び管理施設, 貯蔵及び送油の運営者 Operators of oil production, refining and treatment facilities, storage and transmission
		－理事会指令 2009/119/EC[4]の第 2 条(f)に定義する中央備蓄機関 Central stockholding entities as defined in Article 2, point (f), of Council Directive 2009/119/EC (4)
	(d)ガス Gas	－欧州議会及び理事会の指令 2009/73/EC[5] の第 2 条第 8 号に定義する供給事業者 Supply undertakings as defined in Article 2, point (8), of Directive 2009/73/EC of the European Parliament and of the Council (5)
		－指令 2009/73/EC の第 2 条第 6 号に定義する配給システムの運営者 Distribution system operators as defined in Article 2, point (6), of Directive 2009/73/EC
		－指令 2009/73/EC の第 2 条第 4 号に定義する送出システムの運営者 Transmission system operators as defined in Article 2, point (4), of Directive 2009/73/EC
		－指令 2009/73/EC の第 2 条第 10 号に定義する貯蔵システムの運営者 Storage system operators as defined in Article 2, point (10), of Directive 2009/73/EC
		－指令 2009/73/EC の第 2 条第 12 号に定義する LNG システムの運営者 LNG system operators as defined in Article 2, point (12), of Directive 2009/73/EC
		－指令 2009/73/EC の第 2 条第 1 号に定義する天然ガス事業者 Natural gas undertakings as defined in Article 2, point (1), of Directive 2009/73/EC
		－天然ガスの精製施設及び管理施設の運営者 Operators of natural gas refining and treatment facilities
	(e)水素 Hydrogen	－水素の製造, 貯蔵及び送出の運営者 Operators of hydrogen production, storage and transmission
2.輸送 Transport	(a)空 Air	－商業目的のために用いられる規則(EC) No 300/2008 の第 3 条第 4 号に定義する航空会社

		Air carriers as defined in Article 3, point (4), of Regulation (EC) No 300/2008 used for commercial purposes
		－欧州議会及び理事会の規則(EU) No 1315/2013[7]の別紙 II の第 2 節に列挙する中核空港を含め，欧州議会及び理事会の指令 2009/12/EC[6]の第 2 条第 2 号に定義する空港管理組織，同指令の第 2 条第 1 号に定義する空港，並びに，空港内に含まれている付属施設を運用する法主体 Airport managing bodies as defined in Article 2, point (2), of Directive 2009/12/EC of the European Parliament and of the Council (6), airports as defined in Article 2, point (1), of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council (7), and entities operating ancillary installations contained within airports
		－欧州議会及び理事会の規則(EC)No 549/2004[8]の第 2 条第 1 号に定義する航空機運航管理（ATC）のサービスを提供する航空管制の運営者 Traffic management control operators providing air traffic control (ATC) services as defined in Article 2, point (1), of Regulation (EC) No 549/2004 of the European Parliament and of the Council (8)
	(b)鉄道 Rail	－欧州議会及び理事会の指令 2012/34/EU[9]の第 3 条第 2 号に定義するインフラ管理者 Infrastructure managers as defined in Article 3, point (2), of Directive 2012/34/EU of the European Parliament and of the Council (9)
		－指令 2012/34/EU の第 3 条第 1 号に定める鉄道事業者及び同指令の第 3 条第 12 号に定義するサービス施設の運営者 Railway undertakings as defined in Article 3, point (1), of Directive 2012/34/EU and operators of service facilities as defined in Article 3, point (12), of that Directive
	(c)水上 Water	－当該会社によって運用される個々の船舶を含めることなく，規則(EC) No 725/2004 の別紙 I の中で水上運送に関して定義する内水面，海及び沿岸の旅客及び貨物の水上輸送会社 Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004, not including the individual vessels operated by those companies
		－規則(EC) No 725/2004 の第 2 条第 11 号に定義する当該組織の港湾施設を含め，指令 2005/65/EC の第 3 条第 1 号に定義する港湾管理組織，並びに，港湾内に含まれている作業及び

		設備を運用する法主体 Managing bodies of ports as defined in Article 3, point (1), of Directive 2005/65/EC, including their port facilities as defined in Article 2, point (11), of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports
		ー欧州議会及び理事会の指令 2002/59/EC[10] の第 3 条(o)に定義する船舶交通サービス（VTS）の運営者 Operators of vessel traffic services (VTS) as defined in Article 3, point (o), of Directive 2002/59/EC of the European Parliament and of the Council [(10)]
	(d)道路 Road	ー高度輸送システムの交通管理または運営が当該法主体の一般的な活動中の不可欠ではない部分となっている公的部門の法主体を除き，委員会委任規則(EU)2015/962[11] の第 2 条第 12 号に定義する交通管理の職責を負う道路当局 Road authorities as defined in Article 2, point (12), of Commission Delegated Regulation (EU) 2015/962 [(11)] responsible for traffic management control, excluding public entities for whom traffic-management or the operation of intelligent transport systems is a non-essential part of their general activity
		ー欧州議会及び理事会の指令 2010/40/EU[12] の第 4 条第 1 号に定義する高度輸送システムの運営者 Operators of Intelligent Transport Systems as defined in Article 4, point (1), of Directive 2010/40/EU of the European Parliament and of the Council [(12)]
	(e)公共輸送 Public transport	ー欧州議会及び理事会の規則(EC) No 1370/2007[13] の第 2 条(d)に定義する公共サービスの運営者 Public service operators as defined in Article 2, point (d), of Regulation (EC) No 1370/2007 of the European Parliament and of the Council [(13)]
3.銀行 Banking		ー規則(EU) No 575/2013 の第 4 条第 1 号に定義する与信機関 Credit institutions as defined in Article 4, point (1), of Regulation (EU) No 575/2013
4.金融市場インフラ Financial market infrastructure		ー指令 2014/65/EU の第 4 条第 24 号に定義する取引所の運営者 Operators of trading venues as defined in Article 4, point (24), of Directive 2014/65/EU
		ー規則(EU) No 648/2012 の第 2 条第 1 号に定義する中央清算機関（CCPs） Central counterparties (CCPs) as defined in Article 2, point (1), of Regulation (EU) No 648/2012

5.医療 Health		－欧州議会及び理事会の指令 2011/24/EU[14] の第 3 条(g)に定義する医療のプロバイダ Healthcare providers as defined in Article 3, point (g), of Directive 2011/24/EU of the European Parliament and of the Council (14)
		－欧州議会及び理事会の規則(EU) 2022/2371[15] の第 15 条に示す EU 参照試験所 EU reference laboratories as referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council (15)
		－欧州議会及び理事会の指令 2001/83/EC[16] の第 1 条第 2 号に定義する医療製品の調査研究及び開発を遂行する法主体 Entities carrying out research and development activities of medicinal products as defined in Article 1, point (2), of Directive 2001/83/EC of the European Parliament and of the Council (16)
		－NACE Rev. 2 の Section C division 21 に示す基礎医薬品及び医薬調合品を製造する法主体 Entities manufacturing basic pharmaceutical products and pharmaceutical preparations as referred to in Section C division 21 of NACE Rev. 2
		－欧州議会及び理事会の規則(EU) 2022/123[17] の第 22 条の意味における公的医療の緊急事態の間に重要であるとして判断された医療機器（緊急事態時公的医療重要機器リスト）を製造する法主体 Entities manufacturing medical devices considered as critical during a public health emergency ('public health emergency critical devices list') within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council (17)
		－指令 2001/83/EC の第 79 条に示す流通許可をもつ法主体 Entities holding a distribution authorisation as referred to in Article 79 of Directive 2001/83/EC
6.飲料水 Drinking water		－人間の消費のための水の流通が，他の商品及び物品の流通という当該流通業者の一般的な活動中の不可欠ではない部分となっている流通業者を除き，欧州議会及び理事会の指令(EU) 2020/ 2184[18] の第 2 条第 1 号(a)に定義する人間の消費のために準備された水の供給者及び流通業者 Suppliers and distributors of water intended for human consumption as defined in Article 2, point (1)(a), of Directive (EU) 2020/2184 of the European Parliament and of the Council (18), excluding distributors for which distribution of water for human consumption is a non-essential part of their general activity of distributing other

		commodities and goods
7.廃水 Waste water		―都市廃水, 生活廃水または産業廃水の収集, 処理または取扱いが当該事業者の一般的な活動中の不可欠ではない部分となっている事業者を除き, 理事会指令 91/271/EEC[19] の第 2 条第 1 号, 第 2 号及び第 3 号に定義する都市廃水, 生活廃水または産業廃水を収集し, 処理しまたは取り扱う事業者 Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water as defined in Article 2, points (1), (2) and (3), of Council Directive 91/271/EEC [(19)], excluding undertakings for which collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water is a non-essential part of their general activity
8.デジタルインフラ Digital infrastructure		―指令(EU) 2022/2555 の第 6 条第 18 号に定義するインターネット相互接続点のプロバイダ Providers of internet exchange points as defined in Article 6, point (18), of Directive (EU) 2022/2555
		―ルート名サーバの運営者を除き, 指令(EU) 2022/2555 の第 6 条第 20 号に定義する DNS サービスのプロバイダ DNS service providers as defined in Article 6, point (20), of Directive (EU) 2022/2555, excluding operators of root name servers
		―指令(EU) 2022/2555 の第 6 条第 21 号に定義するトップレベルドメイン名レジストリ top-level-domain name registries as defined in Article 6, point (21), of Directive (EU) 2022/2555
		―指令(EU) 2022/2555 の第 6 条第 30 号に定義するクラウドコンピューティングサービスのプロバイダ Providers of cloud computing services as defined in Article 6, point (30), of Directive (EU) 2022/2555
		―指令(EU) 2022/2555 の第 6 条第 31 号に定義するデータセンターサービスのプロバイダ Providers of data centre services as defined in Article 6, point (31), of Directive (EU) 2022/2555
		―指令(EU) 2022/2555 の第 6 条第 32 号に定義するコンテント伝達ネットワークのプロバイダ Providers of content delivery networks as defined in Article 6, point (32), of Directive (EU) 2022/2555
		―欧州議会及び理事会の規則(EU) No 910/2014[20] の第 3 条第 19 号に定義する信頼サービスのプロバイダ Trust service providers as defined in Article 3, point (19), of

		Regulation (EU) No 910/2014 of the European Parliament and of the Council [20]
		－欧州議会及び理事会の指令(EU) 2018/1972[21] の第 2 条第 8 号に定義する公共電子通信ネットワークのプロバイダ Providers of public electronic communications networks as defined in Article 2, point (8), of Directive (EU) 2018/1972 of the European Parliament and of the Council [21]
		－当該プロバイダのサービスが，公衆が利用可能なものである限り，欧州議会及び理事会の指令(EU) 2018/1972 の第 2 条第 4 号に定義する電子通信サービスのプロバイダ Providers of electronic communications services as defined in Article 2, point (4), of Directive (EU) 2018/1972 insofar as their services are publicly available
9.公行政 Public administration		－国内法に従って構成国によって定義された中央政府の行政機関である法主体 Public administration entities of central governments as defined by Member States in accordance with national law
10.宇宙 Space		－欧州議会及び理事会の指令(EU) 2018/1972 の第 2 条第 8 号に定義する公共電子通信ネットワークのプロバイダを除き，宇宙ベースのサービスの提供を支援し，構成国または民間の者によって保有，管理及び運営されている地上ベースのインフラの運営者 Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks as defined in Article 2, point (8), of Directive (EU) 2018/1972
11. 食品の製造，加工及び流通 Production, processing and distribution of food		－欧州議会及び理事会の規則(EC) No 178/2002[22] の第 3 条第 2 号に定める，専ら，物流及び卸売販売並びに大規模な工業製造及び加工に従事する食品事業者 Food businesses as defined in Article 3, point (2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council [22] which are engaged exclusively in logistics and wholesale distribution and large scale industrial production and processing

[1] 電力のための域内市場の共通規定に関する及び指令 2012/27/EU を改正する欧州議会及び理事会の 2019 年 6 月 5 日の指令(EU) 2019/944 (OJ L 158, 14.6.2019, p. 125).
Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p. 125).

[2] 電力のための域内市場に関する欧州議会及び理事会の 2019 年 6 月 5 日の規則(EU) 2019/943 (OJ L 158, 14.6.2019, p. 54).
Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).

[3] 再生可能資源からのエネルギーの利用の促進に関する欧州議会及び理事会の 2018 年 12 月 11 日の指令(EU) 2018/2001 (OJ L 328, 21.12.2018, p. 82).
Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).

[4] 原油及びまたは石油製品のミニマムの備蓄を維持する義務を構成国に負わせる 2009 年 9 月 14 日の理事会指令 2009/119/EC (OJ L 265, 9.10.2009, p. 9).
Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p. 9).

[5] 天然ガスの域内市場の共通規定に関する及び指令 2003/55/EC を廃止する欧州議会及び理事会の 2009 年 7 月 13 日の指令 2009/73/EC (OJ L 211, 14.8.2009, p. 94).
Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).

[6] 空港使用料に関する欧州議会及び理事会の 2009 年 3 月 11 日の指令 2009/12/EC (OJ L 70, 14.3.2009, p. 11).
Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p. 11).

[7] 欧州横断輸送ネットワークの開発のための欧州連合の指針に関する及び決定 No 661/2010/EU を廃止する欧州議会及び理事会の 2013 年 12 月 11 日の規則(EU) No 1315/2013 (OJ L 348, 20.12.2013, p. 1).
Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p. 1).

[8] 欧州の単一の空の創始のための枠組みを定める欧州議会及び理事会の 2004 年 3 月 10 日の規則(EC) No 549/2004（枠組み規則）(OJ L 96, 31.3.2004, p. 1).
Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p. 1).

[9] 欧州の単一鉄道領域を設ける欧州議会及び理事会の 2012 年 11 月 21 日の指令 2012/34/EU (OJ L 343, 14.12.2012, p. 32).
Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a

single European railway area (OJ L 343, 14.12.2012, p. 32).

10 欧州共同体の船舶航行監視情報システムを設置し及び理事会指令 93/75/EEC を廃止する欧州議会及び理事会の 2002 年 6 月 27 日の指令 2002/59/EC (OJ L 208, 5.8.2002, p. 10).
Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p. 10).

11 EU 全域のリアルタイム交通情報サービスの提供に関する 2014 年 12 月 18 日の欧州議会及び理事会の指令 2010/40/EU を補完する委員会委任規則(EU) 2015/962 (OJ L 157, 23.6.2015, p. 21).
Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services (OJ L 157, 23.6.2015, p. 21).

12 道路交通の分野における高度交通システムの配置及び他の態様の交通とのインタフェイスのための枠組みに関する欧州議会及び理事会の 2010 年 7 月 7 日の指令 2010/40/EU (OJ L 207, 6.8.2010, p. 1).
Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).

13 線路による及び道路による公共旅客輸送サービスに関する, 並びに, 理事会規則(EEC) No 1191/69 及び理事会規則(EEC) No 1107/70 を廃止する欧州議会及び理事会の 2007 年 10 月 23 日の規則 (EC) No 1370/2007 (OJ L 315, 3.12.2007, p. 1).
Regulation (EC) No 1370/2007 of the European Parliament and of the Council of 23 October 2007 on public passenger transport services by rail and by road and repealing Council Regulations (EEC) Nos 1191/69 and 1107/70 (OJ L 315, 3.12.2007, p. 1).

14 国境を越える医療における患者の権利の適用に関する欧州議会及び理事会の 2011 年 3 月 9 日の指令 2011/24/EU (OJ L 88, 4.4.2011, p. 45).
Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

15 医療に対する国境を越える重大な脅威に関する及び決定 No 1082/2013/EU を廃止する欧州議会及び理事会の 2022 年 11 月 23 日の規則(EU) 2022/2371 (OJ L 314, 6.12.2022, p. 26).
Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU (OJ L 314, 6.12.2022, p. 26).

16 人間の利用のための医療製品と関連する欧州共同体法に関する欧州議会及び理事会の 2001 年 11 月 6 日の指令 2001/83/EC (OJ L 311, 28.11.2001, p. 67).
Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p. 67).

17 医療製品及び医療機器の危機準備態勢及び危機管理における欧州医療局の役割の強化に関する欧州議会及び理事会の 2022 年 1 月 25 日の規則(EU) 2022/123 (OJ L 20, 31.1.2022, p. 1).
Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (OJ L 20, 31.1.2022, p. 1).

[18] 人間の消費のために準備される水の品質に関する欧州議会及び理事会の 2020 年 12 月 16 日の指令(EU) 2020/2184 (OJ L 435, 23.12.2020, p. 1).
Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the quality of water intended for human consumption (OJ L 435, 23.12.2020, p. 1).

[19] 都市の廃水処理に関する 1991 年 5 月 21 日の理事会指令 91/271/EEC (OJ L 135, 30.5.1991, p. 40).
Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991, p. 40).

[20] 域内市場における電子的なやりとりのための電子識別及び信頼サービスに関する，及び，指令 1999/93/EC を廃止する欧州議会及び理事会の 2014 年 7 月 23 日の規則(EU) No 910/2014 (OJ L 257, 28.8. 2014, p. 73).
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

[21] 欧州電子通信法を定める欧州議会及び理事会の 2018 年 12 月 11 日の指令(EU) 2018/1972 (OJ L 321, 17.12.2018, p. 36).
Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communication Code (OJ L 321, 17.12.2018, p. 36).

[22] 食品法の一般原則及び要件を定め，欧州食品安全局を設置し，食品安全事項の手続を定める欧州議会及び理事会の 2002 年 1 月 28 日の規則(EC) No 178/2002 (OJ L 31, 1.2.2002, p. 1).
Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p. 1).

理事会決定(EU) 2023/436

[参考訳]

2023 年 11 月 30 日
明治大学法学部教授
夏 井 高 人

COUNCIL DECISION (EU) 2023/436 of 14 February 2023 authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence（OJ L 63, 28.2.2023, p. 48–53）のテキスト（英語版）に基づいて和訳を試みた。

原文のテキストを入手できるサイトの URL は，下記のとおりである。

http://data.europa.eu/eli/dec/2023/436/oj
[2023 年 11 月 28 日確認]

―解 説―

1. 理事会決定(EU) 2023/436 について

理事会決定(EU) 2023/436 は，TFEU の関連条項に基づき，欧州評議会のサイバー犯罪条約の第二追加議定書に EU の構成国が批准することを認める理事会決定である。
理事会決定(EU) 2023/436 の発効によって，EU の構成国によるサイバー犯罪条約の第二追加議定書の批准が EU の基本条約の下で適法なものとなる。

理事会決定(EU) 2023/436 は，2023 年 2 月 14 日に採択され，同日，発効した（第 3 条参照）。

理事会決定(EU) 2023/436 の立法提案の経緯等に関しては，同決定の立法提案書（Proposal for a COUNCIL DECISION authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (Brussels, 25.11.2021) (COM(2021) 719 final) (2021/0383(NLE))）の中で詳しく述べられている。

1. 1 サイバー犯罪条約の第二追加議定書の批准手続

理事会決定(EU) 2023/436 は，EU の構成国が，基本条約の下において適法な行為として欧州評議会のサイバー犯罪条約の第二追加議定書に批准できるようにするということだけではなく，議定書の批准の際の留保や宣言に関しても，EU の構成国としての統一的な対応をとることを狙いとしている。

それゆえ，理事会決定(EU) 2023/436 を理解するためには，サイバー犯罪条約の第二追加議定書の提案の経緯，条約に定める内容と機能並びに国際的な影響等を総合的に理解している必要がある。

サイバー犯罪条約の第二追加議定書の原文及び関連情報は，下記のところで入手できる。

> Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)
> https://www.coe.int/en/web/cybercrime/second-additional-protocol
> [2023 年 11 月 29 日確認]

サイバー犯罪条約の第二追加議定書の公式訳は，外務省の Web サイトで公表されている。
ただし，この公式訳（2023 年 11 月 29 日の時点の版）の中には現時点における私見とは異なる訳文が含まれている。

1．2 EU の関連法令

理事会決定(EU) 2023/436 の前文(4)で示されているとおり，理事会決定(EU) 2023/436 として採択された立法提案（COM(2021) 719 final）と密接な関連をもつ法令の提案として，刑事における電子証拠の欧州提出命令及び欧州保全命令に関する欧州議会及び理事会の規則の提案書（Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters）（Strasbourg, 17.4.2018）（COM(2018) 225 final）（2018/0108(COD)）及び刑事手続における証拠収集の目的のための法律上の代理者の指定に関する整合化された規定を定める欧州議会及び理事会の指令の提案書（Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings）（Strasbourg,17.4.2018）（COM(2018) 226 final）（2018/0107(COD)）が提出され，審議されていた。
これらの提案は，2023 年 7 月 12 日，それぞれ，規則(EU) 2023/1543（OJ L 191, 28.7.2023, p. 118-180）及び指令(EU) 2023/1544（OJ L 191, 28.7.2023, p. 181-190）として採択された。

これらの法令のほか，サイバー犯罪条約の第二追加議定書の実装・運用と関連する EU の法令として指令 2014/41/EU（OJ L 130, 1.5.2014, p. 1-36）がある。

1．2 個人データ保護との関係

サイバー犯罪条約の第二追加議定書は，捜査機関の権限濫用または（第三国の工作員としての諜報活動を含め）捜査機関の構成員の背任・横領・業務妨害的な行為等による関係者（被疑者・被告人・被害者）の個人データの侵害に関し，大きな懸念が示されてきたことに鑑み，議定書に基づいて締約国が国内法の中で定める電子的な証拠の収集等の際において，国際的に承認された個人データ保護の法的枠組みを遵守することを強く求めている。

この点に関し，理事会決定(EU) 2023/436 の前文(11)は，規則(EU) 2016/679(OJ L 119, 4.5.2016, p. 1)及び指令(EU) 2016/680 (OJ L 119, 4.5.2016, p. 89)を遵守すべきことを示している。

これらの個人データ保護法令のほか，理事会決定(EU) 2023/436 の中では明示されていないが，構成国の法務当局の間で電子通信回線を介して電子証拠の通信が実行される場合等には，指令 2002/58/EC(OJ L 201, 31.7.2002, p. 37)適用される。

これに対し，サイバー犯罪条約の第二追加議定書に定める事項と関連して，欧州委員会，EPPO，Europol (EC3) ，ENISA のような欧州連合の機関，組織，事務局及び部局による個人データの処理に関しては，理事会決定(EU) 2023/436 の中では明示されていないが，規則(EU) 2018/1725 (OJ L 295, 21.11.2018, p. 39)が適用される。

なお，第三国を攻撃元とするサイバー戦に該当する場合を含め，構成国の国家安全保障や国防と関係する場合及び欧州連合の対外関係と関係する場合においては，規則(EU) 2016/679（GDPR）及び規則(EU) 2018/1725 が適用されない。

1．3 指令(EU) 2022/2557 の原文中にある誤記等の問題

理事会決定(EU) 2023/436 の原文（英語版）には明らかな誤りが見られる。

それらが訂正されるべき誤記等に該当すると欧州委員会が判断する場合，所定の手続を経て EU 官報上で公表されるその正誤表（corrigendum）によっていずれ訂正されることになると予想されるが，Eur-lex 上で 2023 年 11 月 29 日の時点において確認できた範囲内では，理事会決定(EU) 2023/436 の原文（英語版）に適用される正誤表は公表されていない。

そのため，この参考訳においては，誤記等のある箇所に関し，適宜意訳し，または，意識的に原文のままで訳出することにしたが，特に留意すべき点に関しては，「参考訳作成において留意した事項」の項で個別に指摘することにした。

2. 参考訳作成における基本方針

この参考訳においては，理事会決定(EU) 2023/436 の前文（recital），条文（articles）及び別紙（Annex）の前文を訳出した。

この参考訳においては対訳方式を採用することにした。

この参考訳は，あくまでも理事会決定(EU) 2023/436 の私的な和訳である。公式訳でも確定訳でもない。

この参考訳は，現時点における研究成果を反映するものである。将来，更に研究を深めた結果として修正すべき部分を発見したときは，その時点において，改訂版等を作成すべきかどうかを検討する。

参考訳の訳出に際しては原則として直訳とすることとしたが，直訳のままでは日本語になりにくい箇所に関しては，やむを得ず意訳とした。

この参考訳に訳注はない。参考訳中にある脚注は，全て原注である。訳注等による個別の説明がなければ当該箇所の訳出の理由がわかりにくいと想定される箇所に関しては，必要に応じて，「参考訳作成において留意した事項」の中で説明を加えることにした。

読みやすさを重視し，条文中の号(point)の表記を一部省略した。例えば，「point(a)」は「第(a)号」であるが，「第」と「号」を省略し，「(a)」と表記することにした。

この参考訳は，Eur-lex のデータ二次利用条件を遵守して作成した。

3. 参考訳作成において留意した事項

この参考訳は理事会決定(EU) 2023/436 の注釈書ではないので，それらの箇所の全てを指摘することは避け，必要に応じて合理的に解釈した上で訳文を作成することにした。

ここでは，特に説明を加えないと誤訳ではないかと誤解される危険性がある箇所を中心にして，この参考訳作成において留意した事項を摘記する。

＊＊＊

理事会決定(EU) 2023/436 の前文(2)の中にある「and is envisaged to be opened for signature on 12 May 2022」との箇所は，理事会決定(EU) 2023/436 の採択の時点が 2023 年 2 月 14 日であることからすると，奇妙な文である。この理事会決定の欧州委員会による提案（COM(2021) 719 final）の時点が 2021 年 11 月 25 日であることから推測すると，提案文が訂正されることなくそのまま採択された結果だと考えられる。提案書の中にある理事会決定案の前文(2)の対応する箇所は「and is envisaged to be opened for signature in March 2022」となっているので，日付が修正されただけであり，「and is envisaged」を「and was envisaged」と修正することが失念されてしまったのであろう。
ただし，この参考訳においては，原文のまま訳出することにした。

理事会決定(EU) 2023/436 の前文(17)の末尾は「コンマ（,）」となっているが，この箇所は「ピリオド（.）」が正しいので，誤記と思われる。
この参考訳においては，そのように解した上で，合理的に訳出することにした。

理事会決定(EU) 2023/436 の中では「notification or communication」と表現されている箇所と「notifications and communications」と表現されている箇所がある。
これは，議定書の第 25 条第 1 項 e に由来するもので，同項 e が定める内容は「any other act, notification or communication relating to this Protocol」となっている。ここでは，「notification」と「communication」は「any other act」の例示であると考えられる。「communication」は，外務省の公式訳では「通報」となっており，「通牒」とも訳し得ると考えられるが，この参考訳では「連絡」と訳すことにした。
理事会決定(EU) 2023/436 の中にある「notification or communication」との表現と「notifications and communications」との表現に何らかの積極的な意味があるとは考えられず，もし議定書第 25 条第 1 項 e の表現に揃えるべきであるとすれば，「notifications and communications」との表現部分の方が誤記となると解される。
ただし，この参考訳においては，いずれも原文のまま訳出することにした。

理事会決定(EU) 2023/436 の別紙（Annex）の第 4 号の第 1 段落の中にある「established by Regulation (EU) 2017/1939」との箇所は，「established by Council Regulation (EU) 2017/1939」の誤記である。
この参考訳においては，そのように解した上で，合理的に訳出することにした。

理事会決定(EU) 2023/436 の別紙（Annex）の第 4 号の第 1 段落の中にある「as national prosecutors of those Member States Member States」の「those」は，「当該国内検察官が属する構成国」ということを指しているが，日本語文で丁寧に表現しようとすると逆にその意味をとりにくい文となってしまうという問題がある。
そこで，この参考訳においては，この箇所を「当該構成国の国内検察官と」と訳すことにした。

4. 関連参考訳

指令 2014/41/EU の参考訳は，法と情報雑誌 3 巻 7 号 199～245 頁にある。

理事会規則(EU) 2017/1939 の参考訳は，法と情報雑誌 3 巻 1 号 1～91 頁にある。

規則 (EU) 2016/679（一般データ保護規則）の参考訳・再訂版は，法と情報雑誌 3 巻 5 号 1～114 頁にある。規則(EU)2018/1725 の参考訳は，法と情報雑誌 4 巻 1 号 1～81 頁にある。指令 2002/58/EC の参考訳・改訂版は，法と情報雑誌 2 巻 5 号 158～187 頁にある。指令(EU) 2016/680 の参考訳は，法と情報雑誌 2 巻 1 号 41～140 頁にある。

この参考訳の校正等に関し，唐亀侑久氏（株式会社ラック）の助力を得た。

＊＊＊

欧州連合の利益において，拡大された協力及び電子証拠の開示に関するサイバー犯罪に関する条約の第二追加議定書に構成国が批准する権限を与える 2023 年 2 月 14 日の理事会決定(EU) 2023/436

COUNCIL DECISION (EU) 2023/436 of 14 February 2023 authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence

欧州連合の理事会は，
欧州連合の機能に関する条約，とりわけ，同条約の第 218 条第 6 項と重畳して適用される第 16 条及び第 82 条第 1 項に鑑み，
欧州委員会からの提案に鑑み，
欧州議会の同意に鑑み[1]，

THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 and Article 82(1), in conjunction with 218(6) thereof,
Having regard to the proposal from the European Commission,
Having regard to the consent of the European Parliament[(1)],

Whereas:

(1) 2019 年 6 月 6 日，理事会は，サイバー犯罪に関する欧州評議会条約（CETS No 185）（「サイバー犯罪に関する条約」）の第二追加議定書に関する交渉に，欧州委員会が欧州連合の代わりに参加する権限を与えた。

On 6 June 2019, the Council authorised the Commission to participate, on behalf of the Union, in the negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No 185) ('the Convention on Cybercrime').

(2) 拡大された協力及び電子証拠の開示に関するサイバー犯罪に関する条約の第二追加議定書（「議定書」）は，2021 年 11 月 17 日に欧州評議会の閣僚委員会によって採択され，2022 年 5 月 12 日に署名のために公開されることが予定されている。

The Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence ('the Protocol') was adopted by the Committee of Ministers of the

[1] 2023 年 1 月 17 日の同意（官報未搭載）.
Consent of 17 January 2023 (not yet published in the Official Journal).

Council of Europe on 17 November 2021 and is envisaged to be opened for signature on 12 May 2022.

(3) 議定書の諸条項は，刑事における法務上の協力を容易にする法律文書，手続上の権利のミニマムな基準を確保する法律文書，並びに，データ保護及びプライバシーの安全確保を含め，欧州連合の機能に関する条約（TFEU）の第 3 条第 2 項の意味における共通規定によって大部分が包摂される領域の範囲内にある。

The provisions of the Protocol fall within an area covered to a large extent by common rules within the meaning of Article 3(2) of the Treaty on the Functioning of the European Union (TFEU), including instruments facilitating judicial cooperation in criminal matters, ensuring minimum standards of procedural rights as well as data protection and privacy safeguards.

(4) 欧州委員会は，刑事における電子証拠の欧州提出命令及び欧州保全命令に関する規則の立法提案，並びに，別の構成国のサービスプロバイダの代理者を直接の名宛人とし，国境を越えて拘束力のある欧州提出命令及び欧州保全命令を導入し，刑事手続における証拠収集の目的のための法律上の代理者の指定に関する整合化された規定を定める指令の立法提案の立法提案書も提出した。

The Commission also submitted legislative proposals for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, introducing binding cross-border European Production and Preservation Orders to be addressed directly to a representative of a service provider in another Member State.

(5) 議定書に関する交渉への欧州委員会の参加により，欧州委員会は，関連する欧州連合の共通の規定と議定書との互換性を確保した。

With its participation in the negotiations on the Protocol, the Commission ensured its compatibility with relevant common Union rules.

(6) 議定書と欧州連合の法律及び政策との間の互換性を確保するため，議定書と関係する多数の留保，宣言，通知及び連絡が必要である。それら以外は，議定書の締約国である第三国（「第三国締約国」）と当該構成国との関係における，議定書の締約国である欧州連合の構成国（「構成国締約国」）による議定書の統一的な適用を確保すること，及び，議定書の実効的な適用を確保することと関連している。

A number of reservations, declarations, notifications and communications in relation to the Protocol are necessary to ensure compatibility of the Protocol with Union law and policies. Others are relevant to ensure the uniform application of the Protocol by Union Member States that are Parties to the Protocol (‘Member State Parties’) in their relation with third countries that are Parties to the Protocol (‘third-

country Parties'), as well as the effective application of the Protocol.

(7) 構成国に対してこの決定の別紙の中でそのガイドが与えられる留保, 宣言, 通知及び連絡は, 議定書がそのように許容している場合において当該構成国が個別に行うことを望む別の留保または宣言を妨げない。

The reservations, declarations, notifications and communications on which guidance is given to the Member States in the Annex to this Decision, are without prejudice to any other reservations or declarations that they might wish to make individually where the Protocol so permits.

(8) 署名の時点においてこの決定の別紙に従って留保, 宣言, 通知または連絡をしなかった構成国は, 議定書の当該構成国の批准書, 受諾書または承認書を当該構成国が寄託する際, そのようにすべきである。

Member States which did not make reservations, declarations, notifications and communications in accordance with the Annex to this Decision at the time of signature should do so when they deposit their instrument of ratification, acceptance or approval of the Protocol.

(9) 加えて, 議定書の批准, 受諾または承認の後, 構成国は, この決定の別紙に定める指示を尊重すべきである。

Following the ratification, acceptance or approval of the Protocol, Member States should, in addition, observe the indications set out in the Annex to this Decision.

(10) 議定書は, 電子証拠への国境を越えるアクセス及び高いレベルの安全確保を向上させる迅速な手続を定めている。それゆえ, 議定書の発効は, 構成国締約国と第三国締約国との間の協力を容易にすることによって, サイバー犯罪及びそれ以外の形態の犯罪に抗する闘いにグローバルなレベルで貢献し, 個人の高いレベルの保護を確保し, かつ, 法抵触に対処することになる。

The Protocol provides for swift procedures that improve cross-border access to electronic evidence and a high level of safeguards. Therefore, its entry into force will contribute to the fight against cybercrime and other forms of crime at global level by facilitating cooperation between Member State Parties and third-country Parties, ensure a high level of protection of individuals, and address conflicts of law.

(11) 議定書は, 欧州議会及び理事会の規則(EU) 2016/679[2]並びに欧州議会及び理事会の指令(EU)

[2] 個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する, 並びに, 指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679（一般データ保護規則）(OJ L 119, 4.5.2016, p. 1).
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of

2016/680[3]に基づく個人データの国際的な移転のための要件に沿った適切な安全確保を定めている。それゆえ，議定書の発効は，欧州連合のデータ保護の基準の普及にグローバルなレベルで貢献し，構成国締約国と第三国締約国との間のデータの流れを容易にし，かつ，欧州連合のデータ保護の規定に基づく構成国の義務の構成国締約国の遵守を確保することになる。

The Protocol provides for appropriate safeguards in line with the requirements for international transfers of personal data under Regulation (EU) 2016/679 of the European Parliament and of the Council (2) and Directive (EU) 2016/680 of the European Parliament and of the Council (3). Therefore, its entry into force will contribute to the promotion of Union data protection standards at global level, facilitate data flows between Member State Parties and third-country Parties, and ensure compliance of Member State Parties with their obligations under Union data protection rules.

(12) 議定書の迅速な発効は，サイバー犯罪に抗する闘いのための主たる多国間枠組みとしてのサイバー犯罪に関する条約の地位を更に確実なものとすることになる。

The swift entry into force of the Protocol will furthermore confirm the position of the Convention on Cybercrime as the main multilateral framework for the fight against cybercrime.

(13) 国家のみが同条約の締約国となり得るため，欧州連合は，議定書に批准できない。

The Union cannot ratify the Protocol, as only states can be parties thereto.

(14) それゆえ，構成国は，欧州連合の利益において共同し行動し，議定書に批准することが認められるべきである。

Member States should therefore be authorised to ratify the Protocol, acting jointly in the interests of the Union.

(15) 欧州データ保護監督官は，欧州議会及び理事会の規則(EU) 2018/1725[4] に従って意見聴取を受

natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[3] 犯罪行為の防止，捜査，検知もしくは訴追または刑罰の執行の目的のための職務権限のある機関による個人データの処理と関連する自然人の保護に関する，並びに，そのデータの支障のない移動に関する，並びに，理事会枠組み決定 2008/977/JHA を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の指令(EU) 2016/680 (OJ L 119, 4.5.2016, p. 89).

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

け, 2022 年 1 月 21 日にその意見を伝達した。[4]

The European Data Protection Supervisor was consulted in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council[(4)] and delivered an opinion on 21 January 2022.

(16) 欧州連合条約（TEU）及び TFEU に附属する自由, 保安及び法務の領域に関する英国及びアイルランドの地位に関する議定書第 21 号の第 1 条及び第 2 条に従い, かつ, 同議定書の第 4 条を妨げることなく, アイルランドは, この決定の採択に参加せず, この決定によって拘束されることがなく, または, この決定の適用に服さない。

In accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union (TEU) and to the TFEU, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Decision and is not bound by it or subject to its application.

(17) TEU 及び TFEU に附属するデンマークの地位に関する議定書第 22 号の第 1 条及び第 2 条に従い, デンマークは, この決定の採択に参加せず, この決定によって拘束されることがなく, または, この決定の適用に服さない。

In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Decision and is not bound by it or subject to its application,

(18) 議定書の公式の版は, 2021 年 11 月 17 日に欧州評議会の閣僚委員会によって採択された正文の英語版及びフランス語版である,

The authentic versions of the Protocol are the English and French versions of the text, adopted by the Committee of Ministers of the Council of Europe on 17 November 2021,

HAS ADOPTED THIS DECISION:

以上のとおりであるので, この決定を採択する：

---

[4] 欧州連合の機関, 組織, 事務局及び部局による個人データの処理と関連する自然人の保護に関する並びにそのデータの支障のない移動に関する, 並びに, 規則(EC) No 45/2001 及び決定 No 1247/2002/EC を廃止する欧州議会及び理事会の 2018 年 10 月 23 日の規則(EU) 2018/1725 (OJ L 295, 21.11.2018, p. 39).
Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

第 1 条
Article 1

構成国は，ここに，欧州連合の利益において，拡大された協力及び電子証拠の開示に関するサイバー犯罪に関する条約の第二追加議定書（「議定書」）[5]に批准することが認められる。

The Member States are hereby authorised to ratify, in the interest of the Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence ('the Protocol') [(5)].

第 2 条
Article 2

1. 議定書に批准する場合，署名の時点においてこの決定の別紙の第 1 項ないし第 3 項に従って留保，宣言，通知及び連絡をしなかった構成国は，議定書の当該構成国の批准書，受諾書または承認書を当該構成国が寄託する際，そのようにする。

   When ratifying the Protocol, Member States which did not, at the time of signature of the Protocol, make reservations, declarations, notifications or communications in accordance with Sections 1 to 3 of the Annex to this Decision shall do so when they deposit their instrument of ratification, acceptance or approval of the Protocol.

2. 加えて，議定書の批准，受諾または承認の後，構成国は，この決定の別紙の第 4 項に定める指示を遵守する。

   Following the ratification, acceptance or approval of the Protocol, the Member States shall, in addition, observe the indications set out in Section 4 of the Annex to this Decision.

第 3 条
Article 3

この決定は，この決定の採択の日に発効する。

This Decision shall enter into force on the date of its adoption.

---

[5] この官報の 28 頁参照。
See page 28 of this Official Journal.

第 4 条
Article 4

この決定は，EU 官報上で公示される。

This Decision shall be published in the *Official Journal of the European Union*.

第 5 条
Article 5

この決定は，構成国宛に発出される。

This Decision is addressed to the Member States.

ブリュッセルにおいて，2023 年 2 月 14 日に行われた。

Done at Brussels, 14 February 2023.

理事会として
For the Council

議長　E. SVANTESSON
The President E. SVANTESSON

別 紙
ANNEX

この別紙は，第 2 条に示す留保，宣言，通知，連絡及び指示を定める。

This Annex sets out the reservations, declarations, notifications, communications and indications referred to in Article 2.

1. 留保
Reservation

議定書の第 19 条第 1 項により，締約国は，議定書の幾つかの条項に定める 1 または複数の留保を利用できる。

Pursuant to Article 19, paragraph 1, of the Protocol, a Party may declare that it avails itself of one or more of the reservations provided for in certain articles of the Protocol.

議定書の第 7 条第 9 項の a により，締約国は，第 7 条(加入者情報の開示)を適用しない権利を留保できる。構成国は，そのような留保を行うことを控える。

Pursuant to Article 7, paragraph 9.a, of the Protocol, a Party may reserve the right not to apply Article 7 (Disclosure of subscriber information). Member States shall refrain from making such a reservation.

議定書の第 7 条第 9 項 b により，締約国は，同項 b に定める条件に服して，一定のタイプのアクセス番号に対して第 7 条を適用しない権利を留保できる。構成国は，そのような留保を行い得るが，利用者を識別する目的のみのために必要なアクセス番号以外のアクセス番号との関係においてのみである。

Pursuant to Article 7, paragraph 9.b, of the Protocol, a Party may, subject to the conditions therein, reserve the right not to apply Article 7 to certain types of access numbers. Member States may make such a reservation, but only in relation to access numbers other than those necessary for the sole purpose of identifying the user.

議定書の第 8 条(加入者情報及びトラフィックデータの応急開示を求める別の締約国からの命令の有効化)第 13 項により，締約国はトラフィックデータに対して第 8 条を適用しない権利を留保できる。構成国は，そのような留保を行うことを控えることが推奨される。

Pursuant to Article 8, paragraph 13, of the Protocol, a Party may reserve the right not to apply Article 8 (Giving effect to orders from another Party for expedited production of subscriber information and traffic

data) to traffic data. Member States are encouraged to refrain from making such a reservation.

第 19 条第 1 項がこれら以外の留保の根拠を提供する場合，構成国は，そのような留保を行うことを検討し，それを行うことが認められる。

Where Article 19, paragraph 1, provides a basis for other reservations, Member States are authorised to consider and make such reservations.

2. 宣言

Declarations

議定書の第 19 条第 2 項により，締約国は，議定書の一定の条項に示された宣言を行い得る。

Pursuant to Article 19, paragraph 2, of the Protocol, a Party may make the declarations identified in certain articles of the Protocol.

議定書の第 7 条第 2 項 b により，締約国は，当該締約国の領土内のサービスプロバイダに対して発令される命令に関し，以下の宣言を行い得る：
「第 7 条第 1 項に基づく命令は，検察官またはそれ以外の法務当局によって発令され，もしくは，検察官またはそれ以外の法務当局の監督の下に発令されなければならず，または，さもなければ，独立の監督の下において発令されなければならない。」。

Pursuant to Article 7, paragraph 2.b, of the Protocol, a Party may, with respect to orders issued to service providers in its territory, make the following declaration:
'The order under Article 7, paragraph 1, must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision.'.

構成国は，当該構成国の領土内のサービスプロバイダに対して発令される命令に関し，本号の第 2 段落に定める宣言を行う。

Member States shall, with respect to orders issued to service providers in its territory, make the declaration set out in the second paragraph of this point.

議定書の第 9 条（緊急時における記録保存されたコンピュータデータの応急開示）第 1 項 b により，締約国は，その締約国が，加入者情報の開示のみを求める同条第 1 項 a に基づく要請を執行しないことを宣言できる。構成国は，そのような宣言を行うことを控えることが推奨される。

Pursuant to Article 9 (Expedited disclosure of stored computer data in an emergency), paragraph 1.b, of the Protocol, a Party may declare that it will not execute requests under paragraph l.a of that Article,

seeking only the disclosure of subscriber information. Member States are encouraged to refrain from making such a declaration.

第 19 条第 2 項がこれら以外の宣言の根拠を提供する場合，構成国は，そのような宣言を行うことを検討し，それを行うことが認められる。

Where Article 19, paragraph 2, provides a basis for other declarations, Member States are authorised to consider and make such declarations.

3. 宣言，通知または連絡

Declarations, notifications or communications

議定書の第 19 条第 3 項により，締約国は，当該条項で定められた条件に従い，議定書の一定の条項に定める宣言，通知または連絡を行い得る。

Pursuant to Article 19, paragraph 3, of the Protocol, a Party is to make any declarations, notifications or communications identified in certain articles of the Protocol according to the terms specified therein.

議定書の第 7 条第 5 項 a により，締約国は，欧州評議会の事務局長に対し，その締約国の領土内のサービスプロバイダに対し同条第 1 項に基づいて命令が発令される場合においては，当該締約国が，全ての案件において，または，定められた状況下において，その命令，補充的な情報及び捜査または刑事手続と関連する事実の要旨の同時通知を要求する旨を通知できる。従って，構成国は，欧州評議会の事務局長に対し，以下の通知を行うものとする：
「[構成国]の領土内のサービスプロバイダに対して第 7 条第 1 項に基づく命令が発令される場合，[構成国]は，全ての案件において，その命令，補充的な情報及び捜査または刑事手続と関連する事実の要旨の同時通知を要求する。」。

Pursuant to Article 7, paragraph 5.a, of the Protocol, a Party may notify the Secretary General of the Council of Europe that when an order is issued under paragraph 1 of that Article to a service provider in its territory, that Party requires, in every case or in identified circumstances, simultaneous notification of the order, the supplemental information and a summary of the facts related to the investigation or proceeding. Accordingly, Member States shall make the following notification to the Secretary General of the Council of Europe:
‘When an order is issued under Article 7, paragraph 1, to a service provider in the territory of [Member State], [Member State] requires in every case simultaneous notification of the order, the supplemental information and a summary of the facts related to the investigation or proceeding.’.

議定書の第 7 条第 5 項 e に従い，構成国は，議定書の第 7 条第 5 項 a に基づく通知を受領し，議定書の第 7 条第 5 項 b，第 5 項 c 及び第 5 項 d に示す活動を遂行する単一の職務権限のある機関を指定し，かつ，議定書の第 7 条第 5 項 a に基づく欧州評議会の事務局長に対する通知が最

初に与えられる際, 欧州評議会の事務局長に対し, 当該機関の連絡先情報を連絡する。

In accordance with Article 7, paragraph 5.e, of the Protocol, Member States shall designate a single competent authority to receive the notification under Article 7, paragraph 5.a, of the Protocol, and perform the actions described in Article 7, paragraphs 5.b, 5.c and 5.d, of the Protocol, and shall, when the notification to the Secretary General of the Council of Europe under Article 7, paragraph 5.a, of the Protocol is first given, communicate to the Secretary General of the Council of Europe the contact information of that authority.

議定書の第 8 条第 4 項により, 締約国は, 同条第 1 項に基づく命令を有効にするために, 付加的な補助情報が要求される旨を宣言できる。従って, 構成国は, 以下の宣言を行うものとする:
「第 8 条第 1 項に基づく命令を有効にするために, 付加的な補助情報が要求される。要求される付加的な補助情報は, その命令の状況及び関連する捜査または刑事手続の別により, 異なる。」。

Pursuant to Article 8, paragraph 4, of the Protocol, a Party may declare that additional supporting information is required to give effect to orders under paragraph 1 of that Article. Accordingly, Member States shall make the following declaration:
'Additional supporting information is required to give effect to orders under Article 8, paragraph 1. The additional supporting information required will depend on the circumstances of the order and the related investigation or proceeding.'.

議定書の第 8 条第 10 項 a 及び第 10 項 b に従い, 構成国は, 第 8 条に基づく命令書を提出するために指定された機関及び第 8 条に基づく命令を受領するために指定された機関それぞれの連絡先情報を通知し, かつ, これを最新のものに保つ。欧州検察局（「EPPO」）の設置に関する拡大された協力を実装する理事会規則(EU) 2017/1939 によって設けられた拡大された協力に参加する構成国は, 議定書の第 8 条第 10 項 a 及び第 10 項 b の下で連絡を受ける機関の中に, 第 22 条, 第 23 条及び第 25 条に定める EPPO の職務権限の行使の制限の範囲内において, EPPO を含めるものとし, かつ, 調整された態様でそのようにする。

In accordance with Article 8, paragraphs 10.a and 10.b, of the Protocol, Member States shall communicate and keep up to date the contact information of the authorities designated to submit an order under Article 8, and of the authorities designated to receive an order under Article 8, respectively. The Member States that participate in the enhanced cooperation established by Council Regulation (EU) 2017/1939 [(1)], implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), shall include the EPPO, within the limits of the exercise of its competences as provided for

[1] 欧州検察局（「EPPO」）の設置に関する拡大された協力を実装する 2017 年 10 月 12 日の理事会規則(EU) 2017/1939 (OJ L 283, 31.10.2017, p. 1).
Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') (OJ L 283, 31.10.2017, p. 1).

in Articles 22, 23 and 25 of that Regulation, among the authorities communicated under Article 8, paragraphs 10.a and 10.b, of the Protocol, and do so in a coordinated manner.

従って，構成国は，以下の宣言を行うものとする：
「第 8 条第 10 項に従い，欧州検察局（「EPPO」）の設置に関する拡大された協力に参加する欧州連合の構成国としての[構成国]は，欧州検察局（「EPPO」）の設置に関する拡大された協力を実装する理事会規則(EU) 2017/1939 の第 22 条，第 23 条及び第 25 条に定める職務権限の行使において，EPPO を職務権限のある機関として指定する。」。

Accordingly, Member States shall make the following declaration:
‘In accordance with Article 8, paragraph 10, [Member State], as a Member State of the European Union participating in the enhanced cooperation on the establishment of the European Public Prosecutor’s Office (“the EPPO”), designates the EPPO, in the exercise of its competences, as provided for in Articles 22, 23 and 25 of Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor’s Office (“the EPPO”), as a competent authority.’.

議定書の第 14 条第 7 項 c に従い，構成国は，欧州評議会の事務局長に対し，セキュリティ上のインシデントと関係する議定書の第 II 章第 2 節の目的のために，議定書の第 14 条第 7 項 b に基づき通知を受ける 1 または複数の機関を連絡する。

In accordance with Article 14, paragraph 7.c, of the Protocol, Member States shall communicate to the Secretary General of the Council of Europe the authority or authorities to be notified under Article 14, paragraph 7.b, of the Protocol, for the purposes of Chapter II, Section 2, of the Protocol, in relation to a security incident.

議定書の第 14 条第 10 項 b に従い，構成国は，欧州評議会の事務局長に対し，議定書に基づき受領したデータの別の国または国際機関に対する転送と関係する議定書の第 II 章第 2 節の目的のための許可を与える 1 または複数の機関を連絡する。

In accordance with Article 14, paragraph 10.b, of the Protocol, Member States shall communicate to the Secretary General of the Council of Europe the authority or authorities to provide authorisation for the purposes of Chapter II, Section 2, of the Protocol, in relation to the onward transfer to another State or international organisation of data received under the Protocol.

議定書の第 19 条第 3 項がこれら以外の宣言，通知または連絡の根拠を提供する場合，構成国は，そのような宣言，通知または連絡を行うことを検討し，それを行うことが認められる。

Where Article 19, paragraph 3, of the Protocol provides a basis for other declarations, notifications or communications, Member States are authorised to consider and make such declarations, notifications or communications.

4. その他の指示
Other indications

理事会規則(EU) 2017/1939 によって設けられた拡大された協力に参加する構成国は，同規則の第 22 条，第 23 条及び第 25 条に定める EPPO の職務権限を行使する際，EPPO が，当該構成国の国内検察官と同じ方法で議定書に基づく協力を求め得ることを確保する。

Member States that participate in the enhanced cooperation established by Regulation (EU) 2017/1939 shall ensure that the EPPO can, in the exercise of its competences as provided for in Articles 22, 23 and 25 of that Regulation, seek cooperation under the Protocol in the same way as national prosecutors of those Member States.

第 7 条の適用に関し，とりわけ，一定のタイプのアクセス番号との関係において，構成国は，当該構成国の職務権限のある機関が，要求された情報のプロバイダによる開示よりも前に，その命令の同時通知を受けるときは，同条に基づく命令を，検察官またはそれ以外の法務当局の精査に服させ得る。

With regard to the application of Article 7, in particular in relation to certain types of access numbers, Member States may subject an order under that Article to the scrutiny of a prosecutor or other judicial authority when their competent authority receives a simultaneous notification of the order prior to the disclosure of the requested information by the provider.

議定書の第 14 条第 11 項 c に従い，構成国は，当該構成国が議定書の目的のためにデータを移転するときは，受領する締約国が，当該の者のデータが提供される個人に対して直接の通知を与えることを要求する当該構成国の国内的な法律上の枠組みの連絡を受けることを確保する。

In accordance with Article 14, paragraph 11.c, of the Protocol, Member States shall ensure that, when they transfer data for the purposes of the Protocol, the receiving Party is informed that their domestic legal framework requires giving personal notice to the individual whose data is provided.

犯罪行為の防止，捜査，検知及び訴追と関連する個人情報の保護に関するアメリカ合衆国と欧州連合との間の合意（「包括合意」）[2]を基礎とする国際的な移転に関し，構成国は，議定書の第 14 条第 1 項 b の目的のために，合衆国の職務権限のある機関に対し，職務権限のある機関の間における議定書に基づく個人データの相互移転に対して包括合意が適用される旨を連絡する。ただし，構成国は，議定書の下で定められている機関間以外の，サービスプロバイダによる直接の電子証拠の移転の特別の要件を考慮に入れた付加的な安全確保によって包括合意が補完されるべきであるということを考慮に入れるものとする。従って，構成国は，合衆国の職務権限のある機関に対し，以下の連絡を行うものとする：

[2] OJ L 336, 10.12.2016, p. 3.

「サイバー犯罪に関する欧州評議会条約の第二追加議定書（「議定書」）の第 14 条第 1 項 b の目的のために，[構成国]は，職務権限のある機関の間における議定書に基づく個人データの相互移転に対して犯罪行為の防止，捜査，検知及び訴追と関連する個人情報の保護に関するアメリカ合衆国と欧州連合との間の合意（「包括合意」）が適用されると判断する。議定書に基づくサービスプロバイダと機関との間の移転に関しては，機関間以外のサービスプロバイダによる直接の電子証拠の移転の特別の要件に対処する包括合意の第 3 条第 1 項の意味における別の個別協定と組み合わせる場合に限り，包括合意が適用される。そのような個別協定が存在しないときは，そのような移転は，議定書に基づいて行われ得るものとし，そのような案件においては，議定書の第 14 条第 1 項 a が，第 14 条第 2 項ないし第 15 条と重畳的に適用される。」。

With regard to international transfers on the basis of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences (2) ('the Umbrella Agreement'), Member States shall, for the purposes of Article 14, paragraph 1.b, of the Protocol, communicate to the competent authorities of the United States that the Umbrella Agreement applies to the reciprocal transfers of personal data under the Protocol between competent authorities. However, Member States shall take into account that the Umbrella Agreement should be complemented with additional safeguards that take into account the unique requirements of the transfer of electronic evidence directly by service providers rather than between authorities as provided for under the Protocol. Accordingly, Member States shall make the following communication to the competent authorities of the United States:
'For the purposes of Article 14, paragraph 1.b, of the Second Additional Protocol to the Council of Europe Convention on Cybercrime ("the Protocol"), [Member State] considers that the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences ("the Umbrella Agreement") applies to the reciprocal transfers of personal data under the Protocol between competent authorities. For transfers between service providers and authorities under the Protocol, the Umbrella Agreement applies only in combination with a further, specific agreement within the meaning of Article 3, paragraph 1, of the Umbrella Agreement that addresses the unique requirements of the transfer of electronic evidence directly by service providers rather than between authorities. In the absence of such a specific transfer agreement, such transfers may take place under the Protocol, in which case, Article 14, paragraph 1.a, in conjunction with Article 14, paragraphs 2 to 15, of the Protocol apply.'.

構成国は，当該構成国が，関連する第三国に関する欧州議会及び理事会の規則(EU) 2016/679[3]

[3] 個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する，並びに，指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679（一般データ保護規則）(OJ L 119, 4.5.2016, p. 1).
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

の第 45 条もしくは欧州議会及び理事会の指令(EU) 2016/680[4] の第 36 条によってそれぞれのデータの移転に適用される十分性の判定を欧州委員会が採択したときに限り，または，規則(EU) 2016/679 の第 46 条第 2 項 a もしくは指令(EU) 2016/680 の第 37 条第 1 項 a による，適切なデータ保護の安全確保を確保する別の合意を基礎とする場合に限り，議定書の第 14 条第 1 項 c を適用することを確保する。

Member States shall ensure that they apply Article 14, paragraph 1.c, of the Protocol, only if the European Commission has adopted an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 of the European Parliament and of the Council [(3)] or Article 36 of Directive (EU) 2016/680 of the European Parliament and of the Council [(4)] for the third country concerned that covers the respective data transfers, or on the basis of another agreement that ensures appropriate data protection safeguards pursuant to Article 46(2), point a, of Regulation (EU) 2016/679 or Article 37(1), point a, of Directive (EU) 2016/680.

[4] 犯罪行為の防止，捜査，検知もしくは訴追または刑罰の執行の目的のための職務権限のある機関による個人データの処理と関連する自然人の保護に関する，並びに，そのデータの支障のない移動に関する，並びに，理事会枠組み決定 2008/977/JHA を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の指令(EU) 2016/680 (OJ L 119, 4.5.2016, p. 89).

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

2023 Printed in Japan
ISSN 2432-6089
法と情報雑誌　第 8 巻第 4 号（通巻第 54 号）
The Law and Information Magazine vol.8 no.4 (consecutive no.54)

2023 年 12 月 1 日発行
発行者　夏井高人
発行所　法と情報研究会（代表 夏井高人）
東京都千代田区神田駿河台 1－1
学校法人明治大学研究棟
（非売品）