ISSN 2432-6089

法と情報雑誌

The Law and Information Magazine

第 11 巻第 2 号（通巻第 73 号・2026 年 2 月）

法と情報研究会　編

本 号 目 次

規則(EU, Euratom) 2023/2841
[参考訳]

2026 年 2 月 1 日
明治大学法学部教授
夏 井 高 人

Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union（OJ L, 2023/2841, 18.12.2023）のテキスト（英語版）に基づき，その和訳を試みた。

規則(EU, Euratom) 2023/2841 の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/reg/2023/2841/oj
[2026 年 1 月 7 日確認]

規則(EU, Euratom) 2023/2841 の参考訳は，あくまでも原文を読む際の参考として提供しているものであり，個人的な見解としての法解釈の結果を「日本語以外の言語で書かれた文書の日本語による翻訳文」というスタイルを用いて表現した文書の一種である。

＊＊＊

この規則(EU, Euratom) 2023/2841 の参考訳の中には，NIS 指令(EU) 2016/1148（OJ L 194, 19.7.2016, p. 1）の参考訳・再訂版（法と情報雑誌 6 巻 6 号 467～548 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳・再訂版を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU, Euratom) 2023/2841 の参考訳の中には，NIS 指令(EU) 2016/1148 の参考訳・再訂版における訳文とは異なっている箇所がある。

この規則(EU, Euratom) 2023/2841 の参考訳の中には，指令(EU) 2022/2555（NIS2 指令）（OJ L 333, 27.12.2022, p. 80-152）の参考訳（法と情報雑誌 8 巻 4 号 1～206 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU, Euratom) 2023/2841 の参考訳の中には，指令(EU) 2022/2555（NIS2 指令）の参考訳における訳文とは異なっている箇所がある。

この規則(EU, Euratom) 2023/2841 の参考訳の中には，指令(EU) 2022/2557（OJ L 333, 27.12.2022, p. 164-198）の参考訳（法と情報雑誌 8 巻 4 号 207～303 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU, Euratom) 2023/2841 の参考訳の中には，指令(EU) 2022/2557 の参考訳における訳文とは異なっている箇所がある。

この規則(EU, Euratom) 2023/2841 の参考訳の中には，規則(EU) 2024/2847（サイバー回復力法）（OJ L, 2024/2847, 20.11.2024, p. 1–81）の参考訳（法と情報雑誌 10 巻 2 号 1～246 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳・改訂版を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU, Euratom) 2023/2841 の参考訳の中には，規則(EU) 2024/2847（サイバー回復力法）の参考訳における訳文とは異なっている箇所がある。

この規則(EU, Euratom) 2023/2841 の参考訳の中には，規則(EU) 2019/881（サイバーセキュリティ法）（OJ L 151, 7.6.2019, p.15-69）の参考訳・改訂版（法と情報雑誌 4 巻 8 号 16～86 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳・改訂版を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU, Euratom) 2023/2841 の参考訳の中には，規則(EU) 2019/881（サイバーセキュリティ法）の参考訳・改訂版における訳文とは異なっている箇所がある。

この規則(EU, Euratom) 2023/2841 の参考訳の中には，規則(EU) 2022/2554（OJ L 333, 27.12.2022, p. 1–79）の参考訳（法と情報雑誌 10 巻 5 号 1～234 頁）を踏まえて作成されている部分が含まれている。
ただし，同参考訳・改訂版を公表した後の研究の進展により，現時点では見解を改めた点もある。そのため，この規則(EU, Euratom) 2023/2841 の参考訳の中には，規則(EU) 2022/2554 の参考訳における訳文とは異なっている箇所がある。

―解 説―

1. 規則(EU, Euratom) 2023/2841 について

規則(EU, Euratom) 2023/2841 は，欧州連合の機関，組織，事務局及び部局におけるサイバー危機管理（情報交換，大きなインシデントに対するインシデント対応，大きなインシデントの取扱いの調整，それらのためのサイバー危機管理計画を事前に設けることなど）の基本的な部分を定めるEUの現行法令である。

ただし，規則(EU,Euratom)2023/2841 は，EU 機密情報（EUCI）を取扱うネットワーク及び情報システムに対しては適用されない。
その結果，規則(EU, Euratom) 2023/2841 は，特に軍事等に関する機密情報と関連するサイバー危機管理以外の欧州連合の統治組織の常務に属するサイバー危機管理（cyber crisis management）を定める基本法令であることになる。
ただし，EUCI を現行の規則(EU, Euratom) 2023/2841 の適用範囲外としている点に関しては，今後の見直しが予定されている（第 25 条第 3 項第 2 文参照）。
一般に，政府機関の情報システムがクラウドコンピューティングシステム上で統合される場合，仮想的または論理的には機密情報と非機密情報とが明確に区分されて処理され得るとしても，サイバー攻撃によって当該システムが物理的に機能しなくなると，仮装的または論理的な区分とは無関係に，システム全体が機能不全に陥ることになる。
一般論としては，機密情報に関しては，処理システム，記録保存及びバックアップ，通信経路，認証システムの全てに関し，常務のために使用される情報システムとは物理的に切り離された存在であることが望ましいと言える。
このようなタイプの問題は，本質的に，暗号技術等の適用によっては解決できない。

規則(EU, Euratom) 2023/2841 は，機関間サイバーセキュリティ委員会（the Interinstitutional Cybersecurity Board）（IICB）及び同規則第 1 条(c)による改称前の欧州連合の機関，組織及び部局のためのコンピュータ緊急対応チーム（the EU institutions, bodies and agencies ）（CERT-EU）の名称を「欧州連合の機関，組織，事務局及び部局のためのサイバーセキュリティサービス（the Cybersecurity Service for the Union institutions, bodies, offices and agencies）（CERT-EU）」と改称し，同改称後の CERT-EU の組織，権限及び予算等を定める基本法令である。

規則(EU, Euratom) 2023/2841 において使用されている「欧州連合の法主体」（Union entities）とは，「欧州連合条約，欧州連合の機能に関する条約（TFEU）または欧州原子力共同体条約によって設置された欧州連合の機関，組織，事務局及び部局」のことを意味している（規則(EU, Euratom) 2023/2841 の第 3 条第 1 号参照）。
IICB は，そのような意味における欧州連合の法主体の代表によって組織されており，それらの法主体の中で IICB としての意思決定における議決権をもつ代表を指定する法主体は，第 10 条第 3 項に列挙されている。この列挙を読むことによって，サイバーセキュリティの文脈において欧州連合の骨格を形成している機関，組織，事務局及び部局の内訳を知ることができる。

なお，同条同項に列挙されていない欧州連合の法主体に関しては，その法主体の議決権のない代表が IICB の会合に出席し得るための方途も定められている。

CERT は，欧州連合の統治組織のための CERT-EU だけではなく，欧州連合の構成国の各政府の組織としての CERT も存在するので，CERT-EU と各構成国の CERT との間の相互関係及び情報交換等を正確に理解することも重要なことである。

CERT-EU は，欧州連合のサイバーセキュリティとの関係における情報交換及び調整の活動において極めて重要な役割を果たすことが期待されており，その統治組織上の位置づけも特別に高いものとなっている。

IICB 及び CERT-EU は，欧州連合のサイバーセキュリティ全体の中で，ENISA と共に極めて重要な役割を果たすことになる。それゆえ，EU の他のサイバーセキュリティ関連法令を読解する際においても，規則(EU, Euratom) 2023/2841 の中で定められている内容を正確に踏まえることは，必須である。

規則(EU, Euratom) 2023/2841 に基づく IICB 及び CERT-EU による個人データの処理には，規則(EU) 2018/1725（OJ L 295, 21.11.2018, p. 39）が適用される。

2. 参考訳作成における基本方針

この参考訳においては，規則(EU, Euratom) 2023/2841 の前文及び条文の全文を訳出した。

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，あくまでも規則(EU, Euratom) 2023/2841 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。

この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。

原文中にある誤記と疑われる箇所に関しては，赤色字で示すことにした。この原文中の誤記と疑われる箇所は，形式的なミスという意味で誤記であるものと意味的な誤りを含むことになるために誤記であるもの両者を含む。
ただし，原文中に存在する誤記と疑われる箇所の全てが赤色字で表示されているという趣旨ではない。判断を保留した箇所が存在する。
原文中に誤りがあると判断した場合，原則として，そのまま直訳とした。しかし，そのまま直訳にしたのでは正しく法解釈された法規範を適正に示したことにならない場合，合理的に法解釈した結果を反映した訳文とすることにし，その箇所を灰色字で示すことにした。

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。

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。

3. 参考訳作成において留意した事項

European External Action Service

「the European External Action Service」は，一般に，「欧州対外行動庁」または「欧州対外行動局」と訳されている。

しかし，「the European External Action Service」は，（日本国における「庁」や「局」のように）行政上の職務に関する総括的な機関（日本国では内閣，EU では欧州委員会）の指揮命令下にある下位の行政機関ではない（2010/427/EU: Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service（OJ L 201, 3.8.2010, pp. 30–40）参照）。

一般に，EU の統治構造及びそれを組成する官庁の構造は，日本国の統治組織とはかなり異なっている。
一般に，相互に異なる性質と機能をもつ構造体（structures）であるものを類似のものであるかのように錯覚してしまう翻訳は，避けなければならない。
それゆえ，欧州委員会の下部組織であるような誤解または印象を与えることが避けられない「庁」や「局」といった語によって「the European External Action Service」を日本語表現することは，明白な誤りとなるので，厳に避けるべきである。

以上の諸点を踏まえた上で，この規則(EU, Euratom) 2023/2841 の参考訳においては，従前の参考訳の中における理解と訳を基本的に改め，「the European External Action Service」を「欧州対外行動サービス」と訳すことにした。
ここでいう「サービス」とは，行政上の役務のことを指し，「EU 全体の行政上の特定の役務に関する意思決定の任務をもつ EU 法上の構造体」という趣旨で「サービス」という語を用いている。

4. 関連参考訳等

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(EU) 2022/2555（NIS2 指令）の参考訳は，法と情報雑誌 8 巻 4 号 1～206 頁にある。委員会勧告(EU) 2017/1584 の参考訳は，法と情報雑誌 3 巻 7 号 293～327 頁にある。規則(EC) No 1049/2001 の参考訳は，法と情報雑誌 2 巻 3 号 102～118 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。

この参考訳には，丸橋透氏（明治大学法学部教授）との意見交換の結果が反映されている。

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。心から感謝する。

＊＊＊

欧州連合の機関，組織，事務局及び部局における
共通の高いレベルのサイバーセキュリティ上の措置を定める
欧州議会及び理事会の 2023 年 12 月 13 日の規則(EU, Euratom) 2023/2841

Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023
laying down measures for a high common level of cybersecurity
at the institutions, bodies, offices and agencies of the Union

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，同条約の第 298 条に鑑み，
欧州原子力共同体設立条約，とりわけ，同条約の第 106 条 a 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，
通常の立法手続に従って審議し[1]，

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 298 thereof,
Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106a thereof,
Having regard to the proposal from the European Commission,
After transmission of the draft legislative act to the national parliaments,
Acting in accordance with the ordinary legislative procedure[(1)],

Whereas:

(1) デジタル時代において，情報通信技術は，オープンであり，効率的でありかつ独立の欧州行政の礎石である。進化しつつある技術及びデジタルシステムの複雑性と相互接続されることの増加は，サイバーな脅威とインシデントに対して欧州連合の法主体をより脆弱にし，欧州連合の法主体の事業継続性とその法主体のデータを安全にする能力に対する脅威を呈するサイバーセキュリティ上のリスクを増幅している。クラウドサービスの利用増加は，情報通信技術（ICT）のユビキタスな利用，高いレベルのデジタル化，リモートワーク及び進化しつつある技術と接続性は，欧州連合の法主体の全ての活動のコアな特徴となっているが，デジタルの回復力は，まだ十分には構築されていない。

In the digital age, information and communication technology is a cornerstone of an open, efficient and independent European administration. Evolving technology and the increased complexity and interconnectedness of digital systems amplify cybersecurity risks, making Union entities more vulnerable to cyber threats and incidents, which poses a threat to their business continuity and capacity to secure their data. While the increased use of cloud services, the ubiquitous use of

[1] 欧州議会の 2023 年 11 月 21 日付けの意見書（官報未搭載）及び理事会の 2023 年 12 月 8 日付け決定。
Position of the European Parliament of 21 November 2023 (not yet published in the Official Journal) and decision of the Council of 8 December 2023.

information and communication technology (ICT), the high level of digitalisation, remote work and evolving technology and connectivity are core features of all activities of Union entities, digital resilience is not yet sufficiently built in.

(2) 欧州連合の法主体が直面しているサイバーな脅威の様相は，常に進化の状態にある。そのような攻撃の主要な動機が金銭を得るための価値ある非開示情報の盗取，公衆の意見の操作またはデジタルインフラの毀損からほとんど変化していないのに，脅威行為者によって用いられる戦術，技法及び手順は，常に進化している。脅威行為者のキャンペーンが次第に巧妙で自動化されたものとなり，脆弱性を拡大しながら迅速に悪用する攻撃に晒される場面を絞りつつ，脅威行為者が当該の者のサイバー攻撃を実行する際のペースは，増加することを維持している。

The cyber threat landscape faced by Union entities is in constant evolution. The tactics, techniques and procedures employed by threat actors are constantly evolving, while the prominent motives for such attacks change little, from stealing valuable undisclosed information to making money, manipulating public opinion or undermining digital infrastructure. The pace at which threat actors conduct their cyberattacks keeps increasing, while their campaigns are increasingly sophisticated and automated, targeting exposed attack surfaces that keep expanding and quickly exploiting vulnerabilities.

(3) 欧州連合の法主体の ICT 環境は，相互依存性と統合されたデータの流れをもち，また，その ICT 環境のユーザは，緊密に共働している。それらの ICT 環境が相互接続されているということは，何らかの崩壊が，当初は単一の EU 組織に限定されていたとしても，潜在的には欧州連合の他の法主体に対して遠くまで及びかつ長期にわたる負の影響を帰結し得る連鎖的な影響を，より広範にもち得るということを意味している。加えて，欧州連合の法主体の一定の ICT 環境は，構成国の ICT 環境と接続されており，構成国の ICT 環境に対してサイバーセキュリティ上のリスクを呈する欧州連合の法主体内のインシデント及びその逆のインシデントを生じさせている。インシデント特化情報を共有することは，類似のサイバーな脅威または構成国に影響を与えるインシデントの検出を容易にし得る。

Union entities' ICT environments have interdependencies and integrated data flows, and their users collaborate closely. That interconnection means that any disruption, even when initially confined to a single Union entity, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts on other Union entities. In addition, certain Union entities' ICT environments are connected with Member States' ICT environments, causing an incident in a Union entity to pose a cybersecurity risk to the Member States' ICT environments and vice versa. The sharing of incident-specific information may facilitate the detection of similar cyber threats or incidents affecting Member States.

(4) 欧州連合の法主体は，恰好の標的であり，高度な技能と十分な資源をもつ脅威行為者及びそれ以外の脅威に直面している。それと同時に，サイバー回復力のレベルと成熟度並びに悪意あるサイバー活動を検出し及びそれに対応する能力は，それらの法主体の間において大きく異なっている。そのことから，欧州連合の法主体の稼動にとって，特定されたサイバーセキュリティ上のリスクと見合ったサイバーセキュリティ上の措置，情報交換及び共働の実装を介して，それらの法主体が，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が必要である。

Union entities are attractive targets that face highly skilled and well-resourced threat actors as well as other threats. At the same time, the level and maturity of cyber resilience and the ability to detect and respond to malicious cyber activities vary significantly across those entities. It is thus necessary for the functioning of the Union entities that they achieve a high common level of cybersecurity through the implementation of cybersecurity measures commensurate with identified cybersecurity risks, information exchange and collaboration.

(5) 欧州議会及び理事会の指令(EU) 2022/2555[2]は，公的な法主体と民間の法主体，職務権限のある当局と組織及び全体としての欧州連合のサイバー回復力及びインシデント対応能力を更に向上させることを狙いとしている。それゆえ，指令(EU) 2022/2555 と一貫性があり，かつ，同指令のレベルの待望を反映する規定を定めることによって，欧州連合の法主体が同指令に従うことを確保する必要がある。

Directive (EU) 2022/2555 of the European Parliament and of the Council(2) aims to further improve the cyber resilience and incident response capacities of public and private entities, competent authorities and bodies as well as the Union as a whole. It is therefore necessary to ensure that Union entities follow suit by providing for rules that are consistent with Directive (EU) 2022/2555 and mirror its level of ambition.

(6) 共通の高いレベルのサイバーセキュリティに到達するため，欧州連合の各法主体が全てのサイバーセキュリティ上のリスクの実効的かつ誠実なマネジメントを確保し，かつ，事業継続性及び危機管理を考慮に入れるサイバーセキュリティ上の内部的なリスクマネジメント，統治及び管理の枠組み（「枠組み」）を設ける必要がある。枠組みは，目的及び優先事項を含め，機密ではない ICT 環境全体を包含するネットワーク及び情報システムの防護のためのサイバーセキュリティ基本方針を定めるべきである。枠組みは，窃盗，火災，洪水，通信と電力の喪失のような出来事または欧州連合の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とそれらに対する毀損及び妨害であって，ネットワーク及び情報システムを介して記録保存され，送信され，処理されまたはアクセス可能なデータの可用性，真正性，完全性または機密性を侵害し得るものに抗して，ネットワーク及び情報システム並びに同システムの物理環境を防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。

To reach a high common level of cybersecurity, it is necessary that each Union entity establish an internal cybersecurity risk-management, governance and control framework (the 'Framework'), which ensures an effective and prudent management of all cybersecurity risks, and takes account of business continuity and crisis management. The Framework should establish cybersecurity policies, including objectives and priorities, for the security of network and information

---

[2] 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）(OJ L 333, 27.12.2022, p. 80).
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).

systems encompassing the entirety of the unclassified ICT environment. The Framework 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, flooding, telecommunication or power failures, or unauthorised physical access and damage to, and interference with, a Union entity's information and information-processing facilities, which could compromise the availability, authenticity, integrity or confidentiality of data stored, transmitted, processed or accessible via network and information systems.

(7) 枠組みの下において特定されたサイバーセキュリティ上のリスクを管理するため，欧州連合の各法主体は，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べきである。それらの措置は，欧州連合の各法主体のサイバーセキュリティを強化するためにこの規則の中で定められた部門のサイバーセキュリティ上のリスクマネジメントの措置に対処すべきである。

To manage the cybersecurity risks identified under the Framework, each Union entity should take appropriate and proportionate technical, operational and organisational measures. Those measures should address the domains and cybersecurity risk-management measures provided for in this Regulation to strengthen the cybersecurity of each Union entity.

(8) 枠組みの中で特定された資産及びサイバーセキュリティ上のリスク並びに定期的なサイバーセキュリティの成熟度評価から得られた判定は，欧州連合の各法主体によって設けられるサイバーセキュリティ計画の中に反映されるべきである。サイバーセキュリティ計画は，採択されたサイバーセキュリティ上のリスクマネジメント措置を含めるべきである。

The assets and cybersecurity risks identified in the Framework as well as conclusions derived from regular cybersecurity maturity assessments should be reflected in a cybersecurity plan established by each Union entity. The cybersecurity plan should include the adopted cybersecurity risk-management measures.

(9) サイバーセキュリティを確保することは継続的な過程なので，この規則によって講じられる措置の適切性及び実効性は，欧州連合の法主体のサイバーセキュリティ上のリスク，資産及びサイバーセキュリティの成熟度の変化に照らし，定期的に改訂されるべきである。サイバーセキュリティ計画は，2 年毎に，または，それが必要なときは，サイバーセキュリティ成熟度評価または枠組みの大きな見直しの後，より頻回に改訂されるべきであるが，枠組みは，定期的に，かつ，少なくとも 4 年毎に，見直されるべきである。

As ensuring cybersecurity is a continuous process, the suitability and effectiveness of the measures taken pursuant to this Regulation should be regularly revised in light of the changing cybersecurity risks, assets and cybersecurity maturity of the Union entities. The Framework should be reviewed on a regular basis and at least every four years, while the cybersecurity plan should be revised every two years, or more frequently where necessary, following the cybersecurity maturity assessments or any substantial review of the Framework.

(10) 欧州連合の法主体によって設けられるサイバーセキュリティ上のリスクマネジメント措置は，それが可

能なときは，サードパーティまたは欧州連合の法主体の権利のための安全確保を考慮に入れた上で，ソースコードに透明性をもたせることを狙いとする基本方針を含めるべきである。その基本方針は，適用可能な契約条件を超えてサードパーティのコードを開示する義務またはそのコードにアクセスする権利を創設することなく，サイバーセキュリティ上のリスクと比例的であり，かつ，サイバーな脅威の分析を容易にすることを意図すべきである。

The cybersecurity risk-management measures put in place by Union entities should include policies aiming, where possible, to render the source code transparent, taking into account safeguards for the rights of third parties or Union entities. Those policies should be proportionate to the cybersecurity risk and are intended to facilitate the analysis of cyber threats, while not creating obligations to disclose or rights to access third-party code beyond the applicable contractual terms.

(11) オープンソースのサイバーセキュリティ上のツール及びアプリケーションは，より高いレベルのオープンさに貢献し得る。オープンな技術標準は，セキュリティツール間の相互運用性を促進し，利害関係者のセキュリティに利益を与える。オープンソースのサイバーセキュリティ上のツール及びアプリケーションは，より広範な開発者コミュニティを梃入れし得るのであり，供給者の多様化を実現可能にする。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のプロセスとコミュニティ駆動型の脆弱性発見のプロセスを導き得る。それゆえ，欧州連合の法主体は，透明性によるセキュリティの一部として，オープンデータ及びオープンソースの利用と関連する基本政策を追求することによって，オープンソースソフトウェア及びオープンな技術標準の利用を促進できるべきである。

Open-source cybersecurity tools and applications can contribute to a higher degree of openness. Open standards facilitate interoperability between security tools, benefitting the security of 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. Union entities 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.

(12) 欧州連合の法主体間の相違は，この規則の実装における柔軟性を要求する。この規則の中で定められた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は，欧州連合の法主体の任務の実行を直接に妨げる義務またはそれらの法主体の機関としての自律性を侵害する義務を包摂してはならない。それゆえ，それらの法主体は，当該法主体自身の枠組みを設けるべきであり，また，当該法主体自身のサイバーセキュリティ上のリスクマネジメントの措置及びサイバーセキュリティ計画を採択すべきである。そのような措置を実装する際，資源の適正な管理及び費用の最適化を狙いとして，欧州連合の法主体間における既存の相乗効果が適正に考慮に入れられるべきである。当該措置が，欧州連合の法主体間及び欧州連合の法主体と構成国の相手方との間の効率的な情報交換及び協力に対して負の影響を与えないことも適正に考慮に入れられるべきである。

The differences between Union entities require flexibility in the implementation of this Regulation. The measures for a high common level of cybersecurity provided for in this Regulation should not include any obligations directly interfering with the exercise of the missions of Union entities or encroaching on their institutional autonomy. Therefore, those entities

should establish their own Frameworks and should adopt their own cybersecurity risk-management measures and cybersecurity plans. When implementing such measures, due account should be taken of existing synergies between Union entities, with the aim of proper management of resources and cost optimisation. Due account should also be taken that the measures do not negatively affect efficient information exchange and cooperation among Union entities and between Union entities and Member State counterparts.

(13) 資源の利用を最適化するという利益において，この規則は，類似の構造をもつ欧州連合の複数の法主体が，当該複数の法主体の各法主体に関するサイバーセキュリティの成熟度評価を実施する上で協力できることを定めるべきである。

In the interest of optimising the use of resources, this Regulation should provide for the possibility for two or more Union entities with similar structures to cooperate in carrying out the cybersecurity maturity assessments for their respective entities.

(14) 欧州連合の法主体に対して不適切な財務上及び行政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上のリスクマネジメントの要件は，最先端のそのような措置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呈されているサイバーセキュリティリスクと比例するものであるべきである。欧州連合の各法主体は，当該法主体のサイバーセキュリティのレベルを向上させるために，当該法主体の適正な割合の ICT 予算を割当てることを狙いとすべきである。長期的には，少なくとも 10%のオーダーの指標的な目標が追求されるべきである。サイバーセキュリティの成熟度評価は，欧州連合の法主体のサイバーセキュリティ上の支出が当該法主体が直面するサイバーセキュリティリスクに対して比例しているか否かを評価すべきである。諸条約の下における欧州連合の年次予算と関連する諸原則を妨げることなく，この規則の発効後に採択される最初の欧州委員会の年次予算案の中で，欧州委員会は，当該法主体の予想される支出から帰結する欧州連合の法主体の予算の需要及び職員の需要を評価する際，この規則から生ずる義務を考慮に入れるべきである。

In order to avoid imposing a disproportionate financial and administrative burden on Union entities, the cybersecurity risk-management requirements should be proportionate to the cybersecurity risk posed to the network and information systems concerned, taking into account the state of the art of such measures. Each Union entity should aim to allocate an adequate percentage of its ICT budget to improve its level of cybersecurity. In the longer term an indicative target in the order of at least 10 % should be pursued. The cybersecurity maturity assessment should evaluate whether the Union entity's cybersecurity spending is proportionate to the cybersecurity risks that it faces. Without prejudice to the rules relating to the Union's annual budget under the Treaties, in its proposal for the first annual budget to be adopted after the entry into force of this Regulation the Commission should take into account the obligations arising from this Regulation when assessing the budgeting and staffing needs of the Union entities as resulting from their estimates of expenditures.

(15) 共通の高いレベルのサイバーセキュリティは，サイバーセキュリティが，欧州連合の各法主体の最上位レベルの運営主体の監督の下に入ることを要求する。欧州連合の法主体の最上位レベルの運営主体は，枠組みの設置，サイバーセキュリティ上のリスク管理の措置を講ずること及びサイバーセキュリティ計画の承認を含め，この規則の実装に関する職責を負うべきである。サイバーセキュリティの

文化，すなわち，日々のサイバーセキュリティの実務に対応することは，欧州連合の全ての法主体における枠組み及び対応するサイバーセキュリティ上のリスクマネジメントの措置の不可欠な部分である。

A high common level of cybersecurity requires cybersecurity to come under the oversight of the highest level of management of each Union entity. The Union entity's highest level of management should be responsible for the implementation of this Regulation, including for the establishment of the Framework, the taking of the cybersecurity risk-management measures and the approval of the cybersecurity plan. Addressing the cybersecurity culture, namely the daily practice of cybersecurity, is an integral part of the Framework and the corresponding cybersecurity risk-management measures in all Union entities.

(16) EU 機密情報（EUCI）を取扱うネットワーク及び情報システムの防護は，必須である。EUCI を取扱う欧州連合の法主体は，特別の統治，基本政策及びリスクマネジメントの手続を含め，そのような情報を保護するために設けられた包括的な法令上の枠組みを適用することが要求される。EUCI を取扱うネットワーク及び情報システムに関しては，機密ではないネットワーク及び情報システムよりも厳格なセキュリティ基準を遵守する必要がある。それゆえ，EUCI を取扱うネットワーク及び情報システムは，サイバーな脅威及びインシデントに対するより大きな回復力がある。その結果，この点に関する共通の枠組みの必要性を認識しているが，この規則は，EUCI を取扱うネットワーク及び情報システムに対しては適用されてはならない。ただし，欧州連合の法主体によってそのようにすべきことが明示で要求されるときは，EU 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）は，機密の ICT 環境内のインシデントとの関係において，当該欧州連合の法主体に対し，補助を提供できるべきである。

The security of network and information systems handling EU classified information (EUCI) is essential. Union entities that handle EUCI are required to apply the comprehensive regulatory frameworks in place for protecting such information, including specific governance, policies and risk-management procedures. It is necessary for network and information systems handling EUCI to comply with more stringent security standards than unclassified network and information systems. Therefore, network and information systems handling EUCI are more resilient to cyber threats and incidents. Consequently, while recognising the need for a common framework in this regard, this Regulation should not apply to network and information systems handling EUCI. However, if explicitly requested to do so by a Union entity, the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) should be able to provide assistance to that Union entity in relation to incidents in classified ICT environments.

(17) 欧州連合の法主体は，データ記録保存のサービスプロバイダとデータ処理のサービスプロバイダまたはマネージドセキュリティサービスのプロバイダを含め，サプライヤ及びサービスプロバイダとの間の関係と関連するサイバーセキュリティ上のリスクを評価すべきであり，かつ，そのリスクに対処するための適切な措置を講ずるべきである。サイバーセキュリティ上の措置は，CERT-EU から発される運用指針または勧告の中で別途細目が定められるべきである。措置及び運用指針を設ける際，最新技術，並びに，それが適用可能なときは，適格な欧州連合の技術標準と国際的な技術標準，及び，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 EU の 5G サイバーセキュリ

ティに関するツールボックスのような，指令(EU) 2022/2555 の第 14 条によって設置された協力グループから発されたサイバーセキュリティリスクの評価及び勧告を含め，適格な欧州連合法及び基本方針が適正に考慮に入れられるべきである。加えて，サイバーな脅威の様相及び欧州連合の法主体のサイバー回復力を構築することの重要性を考慮に入れた上で，欧州議会及び理事会の規則(EU) 2019/881[3]の第 49 条によって採択される個別の欧州サイバーセキュリティ認証制度の下において，適格な ICT 製品，ICT サービス及び ICT プロセスの認証が要求され得る。

Union entities should assess cybersecurity risks related to relationships with suppliers and service providers, including providers of data storage and processing services or managed security services, and take appropriate measures to address them. Cybersecurity measures should be further specified in guidelines or recommendations issued by CERT-EU. When establishing measures and guidelines, due account should be taken of the state of the art and, where applicable, relevant European and international standards, as well as relevant Union law and policies, including cybersecurity risk assessments and recommendations issued by the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555, such as the EU coordinated risk assessment of the cybersecurity of 5G networks and the EU toolbox on 5G cybersecurity. In addition, taking into account the cyber threat landscape and the importance of building up cyber resilience for the Union entities, the certification of relevant ICT products, ICT services and ICT processes could be required under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881 of the European Parliament and of the Council(3).

(18) 2011 年 5 月，欧州連合の機関及び組織の事務局長らは，機関間運営委員会によって監督される CERT-EU のための事前準備チームを設置することを決定した。2012 年 7 月，事務局長らは，実務覚書を承認し，かつ，サイバーセキュリティにおける目に見える機関間協力の例として，欧州連合の機関，組織及び部局の情報技術のセキュリティのレベル全体の向上を助けることを継続するための恒久的な部局として CERT-EU を維持することに合意した。2012 年 9 月，CERT-EU は，機関間の任務をもつ欧州委員会のタスクフォースとして設置された。2017 年 12 月，欧州連合の機関及び組織は，CERT-EU の組織及び業務運営に関する機関間覚書[4]を締結した。この規則は，CERT-EU の組織，稼

[3] 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).

[4] 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）の組織及び業務運営に関する欧州議会，欧州理事会，欧州連合の理事会，欧州委員会，欧州連合司法裁判所，欧州中央銀行，欧州会計検査院，欧州対外行動サービス，欧州経済社会委員会，欧州地域委員会及び欧州投資銀行の間の覚書(OJ C 12, 13.1.2018, p. 1).

Arrangement between the European Parliament, the European Council, the Council of the European Union, the European Commission, the Court of Justice of the European Union, the European Central Bank, the European Court of Auditors, the European External Action Service, the European Economic and Social Committee, the European Committee of the Regions and the European Investment Bank on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) (OJ C 12, 13.1.2018, p. 1).

動及び業務運営に関する包括的なセットの規定を定めるべきである。この規則の条項は，2017 年 12 月に締結された CERT-EU の組織及び業務運営に関する機関間覚書の条項よりも優先する。

In May 2011, the Secretaries-General of the Union institutions and bodies decided to establish a pre-configuration team for CERT-EU, supervised by an inter-institutional Steering Board. In July 2012, the Secretaries-General confirmed the practical arrangements and agreed to maintain CERT-EU as a permanent entity to continue to help improve the overall level of information technology security of the Union's institutions, bodies and agencies as an example of visible inter-institutional cooperation in cybersecurity. In September 2012, CERT-EU was established as a Commission Taskforce with an interinstitutional mandate. In December 2017, the Union institutions and bodies concluded an Interinstitutional arrangement on the organisation and operation of CERT-EU[4]. This Regulation should provide for a comprehensive set of rules on the organisation, functioning and operation of CERT-EU. The provisions of this Regulation prevail over the provisions of the Interinstitutional arrangement on the organisation and operation of CERT-EU that was concluded in December 2017.

(19) CERT-EU は，欧州連合の機関，組織，事務局及び部局のためのサイバーセキュリティサービスと改称されるべきであるが，その知名度のゆえに，CERT-EU という略称は維持されるべきである。

CERT-EU should be renamed Cybersecurity Service for the Union institutions, bodies, offices and agencies, but it should keep the short name CERT-EU because of name recognition.

(20) CERT-EU に対してより多くの職務と拡大された役割を与えることに加え，この規則は，欧州連合の法主体間の共通の高いレベルのサイバーセキュリティを促進するため，機関間サイバーセキュリティ委員会（IICB）を設置する。IICB は，欧州連合の法主体によるこの規則の実装を監視すること及び支援することにおいて，並びに，CERT-EU の一般的な優先事項と目的の実装を監視すること及び CERT-EU に対して戦略上の指示を提供することにおいて，専属的な役割を担うべきである。それゆえ，IICB は，欧州連合の機関が代表されることを確保すべきであり，また，EU 部局ネットワーク（EUAN）を介して，欧州連合の組織，事務局及び部局の代表を含めるべきである。IICB の組織及び稼働は，内部的な手続規則によって別途規律されるべきである。その手続規則は，IICB の各構成者の最上位レベルの運営主体の代表が，IICB が戦略上の討議をもつことを可能にし，かつ，IICB に対して戦略上のガイダンスを提供し得る政治レベルの年次総会を含め，IICB の定例会合の別途の細目を含め得る。更に，IICB は，IICB の仕事を補助するため，並びに，とりわけ，例えば，サービスカタログの承認とその後におけるそのカタログのアップデート，サービスレベル合意のための手配，この規則によって IICB に対して欧州連合の法主体から提出される文書及び報告書の評価または IICB から発される遵守措置に関する決定の準備と関連する職務の評価のような，執行委員会の構成者の特別の専門知識を要する職務の面において，IICB の職務と権限の幾つかを執行委員会に対して委任するため，並びに，欧州連合の法主体の実装を監視するため，執行委員会を設置できるべきである。IICB は，執行委員会の職務及び権限を含め，執行委員会の手続規則を定めるべきである。

In addition to giving CERT-EU more tasks and an expanded role, this Regulation establishes the Interinstitutional Cybersecurity Board (IICB) in order to facilitate a high common level of cybersecurity among Union entities. The IICB

should have an exclusive role in monitoring and supporting the implementation of this Regulation by the Union entities and in supervising the implementation of general priorities and objectives of, and providing strategic direction to, CERT-EU. The IICB should therefore ensure representation of the Union institutions and should include representatives of bodies, offices and agencies of the Union through the EU Agencies Network (EUAN). The organisation and functioning of the IICB should be further regulated by means of internal rules of procedure, which may include further specification of regular meetings of the IICB, including annual gatherings of the political level where representatives of the highest level of management of each member of the IICB would allow the IICB to have strategic discussion and provide strategic guidance to the IICB. Furthermore, the IICB should be able to establish an executive committee to assist in its work and to delegate some of its tasks and powers to it, in particular in terms of tasks that require specific expertise of its members, for instance the approval of the service catalogue and any subsequent updates to it, arrangements for service level agreements, assessments of documents and reports submitted by the Union entities to the IICB pursuant to this Regulation or tasks related to the preparation of decisions on compliance measures issued by the IICB and to monitoring their implementation. The IICB should lay down the rules of procedure of the executive committee, including its tasks and powers.

(21) IICB は，この規則の実装を通じて，欧州連合の法主体それぞれのサイバーセキュリティポスチャーを引き上げることにおいて，欧州連合の法主体を支援することを狙いとする。欧州連合の法主体を支援するため，IICB は，CERT-EU の長に対してガイダンスを提供し，欧州連合の法主体におけるサイバーセキュリティのレベルを上げることに関する多年度戦略を採択し，任意のピアレヴューのための手法及びその他の諸側面を定め，並びに，この規則の実装と関連するベストプラクティスと情報を交換することを狙いとして，欧州連合サイバーセキュリティ局（ENISA）の支援を受ける地方サイバーセキュリティ吏員の非公式グループの設置を促進すべきである。

The IICB aims to support Union entities in elevating their respective cybersecurity postures through the implementation of this Regulation. In order to support Union entities, the IICB should provide guidance to the Head of CERT-EU, adopt a multiannual strategy on raising the level of cybersecurity in the Union entities, establish the methodology for and other aspects of voluntary peer reviews, and facilitate the establishment of an informal group of local cybersecurity officers, supported by the European Union Agency for Cybersecurity (ENISA), with the aim of exchanging best practices and information in relation to the implementation of this Regulation.

(22) 欧州連合の全ての法主体におけ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，当該法主体自身の ICT 環境上で走っている欧州連合の組織，事務局及び部局の利益は，EUAN から指名される 3 名の代表者によって IICB において代表されるべきである。個人データ処理のセキュリティは，そして，それゆえに，個人データ処理のサイバーセキュリティは，データ保護の礎石である。データ保護とサイバーセキュリティとの間の相乗効果に照らし，欧州データ保護監督官は，電子通信ネットワークのセキュリティを含め，データ保護の分野における特別の専門知識をもつこの規則に服する欧州連合の法主体の一つとして，その能力において IICB において代表されるべきである。サイバーセキュリティにおける技術革新及び競争力の重要性を考慮し，欧州サイバーセキュリティ産業，技術及び調査研究能力拠点は，IICB において代表されるべきである。サイバーセキュリティにおける専門知識の拠点としての ENISA の役割と ENISA が提供する支援を考慮し，また，欧州連合の宇宙イ

ンフラと宇宙サービスのサイバーセキュリティの重要性を考慮し，ENISA 及び宇宙計画に関する欧州連合局は，IICB において代表されるべきである。この規則の下において CERT-EU に割当てられた役割に照らし，CERT-EU の長は，IICB が，CERT-EU の長と直接的に関連する事柄を討議する場合を除き，IICB の議長によって，IICB の全ての会合に招請されるべきである。

In order to achieve a high level of cybersecurity in all Union entities, the interests of the bodies, offices and agencies of the Union that run their own ICT environment should be represented on the IICB by three representatives designated by the EUAN. The security of personal data processing, and therefore also the cybersecurity thereof, is a cornerstone of data protection. In light of the synergies between data protection and cybersecurity, the European Data Protection Supervisor should be represented on the IICB in its capacity as a Union entity subject to this Regulation, with specific expertise in the area of data protection, including security of electronic communications networks. Considering the importance of innovation and competitiveness in cybersecurity, the European Cybersecurity Industrial, Technology and Research Competence Centre should be represented on the IICB. In view of ENISA's role as a centre of expertise in cybersecurity, and the support that ENISA provides, and in view of the importance of cybersecurity of Union space infrastructure and services, ENISA and the European Union Agency for the Space Programme should be represented on the IICB. In light of the role assigned to CERT-EU under this Regulation, the Head of CERT-EU should be invited by the Chair of the IICB to all of the IICB's meetings, except when the IICB discusses matters relating directly to the Head of CERT-EU.

(23) IICB は，この規則及びの運用指針と勧告の実装の遵守並びに行動要求の遵守を監視すべきである。IICB は，技術上の事柄に関し，IICB が適合していると判断するように構成される技術諮問グループによって支援されるべきである。それらの技術諮問グループは，CERT-EU，欧州連合の法主体及び必要に応じてそれら以外の利害関係者と緊密に協力して，仕事をすべきである。

The IICB should monitor compliance with this Regulation as well as the implementation of guidelines and recommendations, and calls for action. The IICB should be supported on technical matters by technical advisory groups composed as the IICB sees fit. Those technical advisory groups should work in close cooperation with CERT-EU, the Union entities and other stakeholders as necessary.

(24) この規則または IICB から発された運用指針，勧告もしくは行動要求を欧州連合の法主体が実効的に実装していないと IICB が判断するときは，IICB は，関係する欧州連合の法主体の内部手続を妨げることなく，遵守の措置を開始できるべきである。IICB は，遵守の措置を段階的に適用すべきである－換言すると，IICB は，最小の厳しさの措置，すなわち，理由を付した意見をまず採択すべきであり，次第により厳しい措置が必要となったときに限り，最も厳しい措置，すなわち，関係する欧州連合の法主体に対するデータの流れの一時的な停止の勧告を採択すべきである。そのような勧告は，関係する欧州連合の法主体によるこの規則の長期にわたる，意図的な，反復的なまたは重大な違反行為という例外的な場合に限り，適用されるべきである。

Where the IICB finds that a Union entity has not effectively implemented this Regulation or the guidelines, recommendations or calls for action issued pursuant thereto, the IICB should be able, without prejudice to the internal procedures of the Union entity concerned, to proceed with compliance measures. The IICB should apply compliance

measures progressively – in other words, the IICB should first adopt the least severe measure, namely a reasoned opinion, and only if necessary increasingly severe measures, culminating in the most severe measure, namely a recommendation of a temporary suspension of data flows to the Union entity concerned. Such a recommendation should be applied only in exceptional cases of long-term, deliberate, repetitive or serious infringements of this Regulation by the Union entity concerned.

(25) 理由を付した意見は，この規則の実装において見出された格差に対処する最小の厳しさの遵守措置を示すものである。IICB は，当該法主体の枠組み，サイバーセキュリティ上のリスクマネジメント措置，サイバーセキュリティ計画及び報告がこの規則を遵守することを確保する上で欧州連合の法主体を補助するためのガイダンスによって，そして，欧州連合の法主体の発見された欠点に対して指定された期間内に対処することの警告によって，理由を付した意見を補足し得るべきである。警告の中で特定された欠点が十分に対処されなかったときは，IICB は，理由を付した通知を発し得るべきである。

The reasoned opinion represents the least severe compliance measure addressing observed gaps in the implementation of this Regulation. The IICB should be able to follow up a reasoned opinion with guidance to assist the Union entity in ensuring that its Framework, cybersecurity risk-management measures, cybersecurity plan and reporting comply with this Regulation, and then by a warning to address identified shortcomings of the Union entity within a specified period. If the shortcomings identified in the warning have not been sufficiently addressed, the IICB should be able to issue a reasoned notification.

(26) IICB は，欧州連合の法主体の監査が実施されることを勧告できるべきである。欧州連合の法主体は，監査の目的のために，当該法主体の内部監査機能を利用できるべきである。IICB は，相互に合意された民間部門のサービスプロバイダを含め，サードパーティの監査サービスによって監査が遂行されることも要求できるべきである。

The IICB should be able to recommend that an audit of a Union entity be carried out. The Union entity should be able to use its internal audit function for that purpose. The IICB should also be able to request that an audit be performed by a third-party audit service, including from a mutually agreed private-sector service provider.

(27) 関係する欧州連合の法主体によるこの規則の長期にわたる，意図的な，反復的なまたは重大な違反行為という例外的な場合においては，IICB は，最後の手段として，全ての構成国及び欧州連合の法主体に対し，その欧州連合の法主体が違反行為を終わらせるまで有効な，その欧州連合の法主体に対するデータの流れの一時的な停止を勧告できるべきである。そのような勧告は，適切かつ安全な通信経路によって伝達されるべきである。

In exceptional cases of long-term, deliberate, repetitive or serious infringements of this Regulation by a Union entity, the IICB should be able to recommend, as a last resort, to all Member States and Union entities, a temporary suspension of data flows to the Union entity, to be effective until the Union entity has brought the infringement to an end. Such a recommendation should be communicated by means of appropriate and secure communication channels.

(28) この規則の正確な実装を確保するため，IICB は，欧州連合の法主体によるこの規則の恒常的な違反行為が，最上位レベルの運営主体を含め，その法主体の職員の一員の作為または不作為によって直接に生じたものであると IICB が判断するときは，関係する欧州連合の法主体に対し，理事会規則(EEC, Euratom, ECSC) No 259/68[5]の中で定められた欧州連合の官吏の就業規則及び欧州連合のその他の公務員の雇用条件（「職員規則」）の中で定められた規定及び手続並びにそれ以外の適用可能な規定及び手続に従い，懲戒の性質をもつ行動をとることを検討することを当該法主体に対して要求することを含め，適切な行動をとることを要求すべきである。

To ensure the correct implementation of this Regulation, the IICB should, if it considers that a persistent infringement of this Regulation by a Union entity has been caused directly by the actions or omissions of a member of its staff, including at the highest level of management, request the Union entity concerned to take appropriate action, including requesting it to consider taking action of a disciplinary nature, in accordance with the rules and procedures laid down in the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the Union, laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68[(5)] (the 'Staff Regulations') and any other applicable rules and procedures.

(29) CERT-EU は，欧州連合の全ての法主体の ICT 環境のセキュリティに貢献すべきである。欧州連合の法主体の要請を受けた後，適格な政策上の事項に関し，技術上の助言または入力を提供すべきか否かを判断する際，CERT-EU は，そのことが，この規則によって CERT-EU に対して与えられた他の職務を遂行することの妨げとはならないことを確保すべきである。CERT-EU は，指令(EU) 2022/2555 の第 12 条第 1 項による調整された脆弱性開示の目的のために指定された調整官と均等な者として欧州連合の法主体の側に立って行動する。

CERT-EU should contribute to the security of the ICT environment of all Union entities. When considering whether to provide technical advice or input on relevant policy matters upon the request of a Union entity, CERT-EU should ensure that this is no obstacle to carrying out the other tasks conferred on it pursuant to this Regulation. CERT-EU should act on the part of Union entities as the equivalent of the coordinator designated for the purposes of coordinated vulnerability disclosure pursuant to Article 12(1) of Directive (EU) 2022/2555.

(30) CERT-EU は，IICB に対する運用指針及び勧告の提案によって，または，行動要求を発することによって，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の実装を支えるべきである。そのような運用指針及び勧告は，IICB によって承認されるべきである。それが必要なときは，CERT-EU は，欧州連合の法主体が定められた時間枠内でとることが督促される緊急防護措置を記述している行動要

---

[5] 欧州共同体の官吏の職員規則及びその他の公務人の雇用条件を定め並びに欧州委員会の官吏に対して一時的に適用可能な特別措置を定める 1968 年 2 月 29 日の理事会の規則(EEC, Euratom, ECSC) No 259/68 (OJ L 56, 4.3.1968, p. 1).
Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (OJ L 56, 4.3.1968, p. 1).

求を発すべきである。IICB は，CERT-EU に対し，運用指針もしくは勧告の提案または行動要求を発すること，撤回することまたは修正することを指示すべきである。

CERT-EU should support the implementation of measures for a high common level of cybersecurity by means of proposals for guidelines and recommendations to the IICB or by issuing calls for action. Such guidelines and recommendations should be approved by the IICB. When needed, CERT-EU should issue calls for action describing urgent security measures which Union entities are urged to take within a set timeframe. The IICB should instruct CERT-EU to issue, withdraw or modify a proposal for guidelines or for a recommendation, or a call for action.

(31) CERT-EU は，指令(EU) 2022/2555 の第 15 条によって設置されたコンピュータセキュリティインシデント対応チーム（CSIRTs）ネットワークとの協力及び情報交換と関係して同指令の中で定められた役割も満たすべきである。更に，委員会勧告(EU) 2017/1584[6]に沿って，CERT-EU は，適格な利害関係者と協力しかつ対応を調整すべきである。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に貢献するため，CERT-EU は，構成国内の相手方との間でインシデント特化情報を共有すべきである。CERT-EU は，IICB の事前の承認に服して，北大西洋条約機構を含め，その他の公的な相手方及び民間の相手方とも，共働すべきである。

CERT-EU should also fulfil the role provided for it in Directive (EU) 2022/2555 concerning cooperation and information exchange with the computer security incident response teams (CSIRTs) network established pursuant to Article 15 of that Directive. Moreover, in line with Commission Recommendation (EU) 2017/1584[6], CERT-EU should cooperate and coordinate a response with the relevant stakeholders. In order to contribute to a high level of cybersecurity across the Union, CERT-EU should share incident-specific information with Member State counterparts. CERT-EU should also collaborate with other public as well as private counterparts, including the North Atlantic Treaty Organization, subject to prior approval by the IICB.

(32) 業務運営上のサイバーセキュリティの支援において，CERT-EU は，規則(EU) 2019/881 の中で定められた構造化された協力を介して ENISA の利用可能な専門知識を活用すべきである。必要に応じて，そのような協力の実務上の実装を定義するため及び活動の重複を避けるため，2 つの法主体間の専用の手立てが設けられるべきである。CERT-EU は，サイバーな脅威の分析に関して ENISA と協力すべきであり，また，ENISA と定期的に CERT-EU の脅威様相報告を共有すべきである。

In supporting operational cybersecurity, CERT-EU should make use of the available expertise of ENISA through structured cooperation as provided for in Regulation (EU) 2019/881. Where appropriate, dedicated arrangements between the two entities should be established to define the practical implementation of such cooperation and to avoid the duplication of activities. CERT-EU should cooperate with ENISA on cyber threat analysis and share its threat landscape

---

[6] 大規模なサイバーセキュリティインシデント及び危機に対する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).

report with ENISA on a regular basis.

(33) CERT-EU は，欧州連合の防護におけるサイバーセキュリティコミュニティの全ての潜在力を現実化することにおいて，業務運営上の協力を育成しかつ既存のネットワークを利用できるようにするため，欧州連合及びその構成国内の適格なサイバーセキュリティコミュニティと協力し及び情報交換できるべきである。

CERT-EU should be able to cooperate and exchange information with relevant cybersecurity communities within the Union and its Member States to foster operational cooperation and to enable the existing networks in realising their full potential in protecting the Union.

(34) CERT-EU のサービス及び職務は，欧州連合の法主体と利害関係があるので，ICT 予算支出をもつ欧州連合の各法主体は，CERT-EU のサービス及び職務に対する公正な分担金を拠出すべきである。その拠出は，欧州連合の法主体の予算上の自律性を妨げない。

As the services and tasks of CERT-EU are in the interest of Union entities, each Union entity with ICT expenditure should contribute a fair share to those services and tasks. Those contributions are without prejudice to the budgetary autonomy of the Union entities.

(35) サイバー攻撃の多くは，欧州連合の法主体のグループまたは欧州連合の法主体を含む利害関係のあるコミュニティを狙いとするより広範なキャンペーンの一部である。事前の検出，インシデント対応または緩和措置及びインシデントからの復旧を実現可能にするため，欧州連合の法主体は，CERT-EU に対し，インシデント，サイバーな脅威，脆弱性及びニアミスを通知できるべきであり，また，欧州連合の他の法主体内の類似のインシデント，サイバーな脅威，脆弱性及びニアミスの検出または緩和及びそれらへの対応を実現可能にする適切な技術上の詳細情報を共有できるべきである。指令(EU) 2022/2555 と同じアプローチに従い，欧州連合の法主体は，大きなインシデントに気づいた後 24 時間以内に，CERT-EU に対し，早期警戒を提出することを要求されるべきである。そのような情報交換は，CERT-EU が，類似のインシデントに抗して欧州連合の法主体の ICT 環境及び欧州連合の法主体の相手方の ICT 環境の防護を助けるため，欧州連合の他の法主体及び適切な相手方に対してその情報を伝達できるようにすべきである。

Many cyberattacks are part of wider campaigns that target groups of Union entities or communities of interest that include Union entities. To enable proactive detection, incident response or mitigating measures and recovery from incidents, Union entities should be able to notify CERT-EU of incidents, cyber threats, vulnerabilities and near misses and share appropriate technical details that enable detection or mitigation of, as well as response to, similar incidents, cyber threats, vulnerabilities and near misses in other Union entities. Following the same approach as in Directive (EU) 2022/2555, Union entities should be required to submit an early warning to CERT-EU within 24 hours of becoming aware of a significant incident. Such information exchange should enable CERT-EU to disseminate the information to other Union entities, as well as to appropriate counterparts, to help protect the Union entities' ICT environments and the Union entities' counterparts' ICT environments against similar incidents.

(36) この規則は，一方における，大きなインシデントの潜在的な拡大の緩和を助け，かつ，欧州連合の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，かつ，欧州連合の個々の法主体のサイバー回復力を徐々に向上させ，かつ，欧州連合の法主体の全体的なサイバーセキュリティポスチャーを向上させることに貢献する詳細な報告とのとの間における正しいバランスをとるため，大きなインシデントの報告に向けた多段階のアプローチを定める。その点に関し，この規則は，関係する欧州連合の法主体によって実施された当初評価を基礎として，関係する欧州連合の法主体の稼動に対して業務運営上の重大な支障もしくは金銭的な損失を生じさせ得るインシデント，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，影響を受けるネットワーク及び情報システム，とりわけ，欧州連合の法主体の稼動のためのその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と技術上の特性及び根底にある悪用されている脆弱性並びに欧州連合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。欧州連合の法主体の稼動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自然人もしくは法人の数のような指標は，業務運営上の混乱が重大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 Regulation 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 Union 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 Union entities and contributes to increasing their overall cybersecurity posture. In that regard, this Regulation should include the reporting of incidents that, on the basis of an initial assessment carried out by the Union entity concerned, could cause severe operational disruption to the functioning of, or financial loss to, the Union entity concerned, 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 network and information systems affected, in particular their importance for the functioning of the Union entity, the severity and technical characteristics of a cyber threat and any underlying vulnerabilities that are being exploited as well as the Union entity's experience with similar incidents. Indicators such as the extent to which the functioning of the Union entity is affected, the duration of an incident or the number of affected natural or legal persons could play an important role in identifying whether the operational disruption is severe.

(37) 適格な欧州連合の法主体のインフラ及びネットワーク及び情報システムと当該欧州連合の法主体が所在している構成国とは相互接続されているので，当該構成国にとって，当該欧州連合の法主体内の大きなインシデントが不適切な遅滞なく連絡されることは，非常に重要なことである。その目的のために，影響を受けた欧州連合の法主体は，指令(EU) 2022/2555 の第 8 条及び第 10 条によって指定されまたは設置された適格な構成国の相手方に対し，CERT-EU に報告されている大きなインシデントの発生を連絡すべきである。構成国内において発生している大きなインシデントに CERT-EU が気付いたときは，CERT-EU は，当該構成国内の適格な相手方に対して通知すべきである。

As the infrastructure and network and information systems of the relevant Union entity and the Member State where that Union entity is located are interconnected, it is crucial for that Member State to be informed without undue delay of a

significant incident within that Union entity. To that end, the Union entity affected should inform any relevant Member State counterparts designated or established pursuant to Articles 8 and 10 of Directive (EU) 2022/2555 of the occurrence of a significant incident about which it is reporting to CERT-EU. Where CERT-EU becomes aware of a significant incident occurring within a Member State, it should notify any relevant counterpart in that Member State.

(38) 大きなインシデントの場合において欧州連合の法主体の実効的な情報交換，調整及び協力を確保するための仕組みは，関与する欧州連合の法主体の役割及び職責の明確な特定を含めて実装されるべきである。IICB 内における欧州委員会の代表は，共有される状況認識への貢献として，サイバー危機管理計画に服して，欧州サイバー危機連絡組織ネットワーク（EU-CyCLONe）との間において，大きなインシデントとの関係における適格な情報の IICB の共有を容易にするための連絡部局であるべきである。IICB 内における欧州委員会の代表の連絡部局としての役割は，指令(EU) 2022/2555 の第 16 条第 2 項による EU-CyCLONe 内における欧州委員会の区別されかつ区分された役割を妨げてはならない。

A mechanism to ensure effective exchange of information, coordination, and cooperation of the Union entities in the case of major incidents should be implemented, including a clear identification of the roles and responsibilities of the Union entities involved. The Commission representative in the IICB should, subject to the cyber crisis management plan, be the point of contact to facilitate the IICB's sharing of relevant information in relation to major incidents with the European cyber crisis liaison organisation network (EU-CyCLONe), as a contribution to the shared situational awareness. The role of the Commission representative in the IICB as the point of contact should be without prejudice to the Commission's separate and distinct role in EU-CyCLONe pursuant to Article 16(2) of Directive (EU) 2022/2555.

(39) この規則による個人データの処理に対しては，欧州議会及び理事会の規則(EU) 2018/1725[7]が適用される。個人データの処理は，サイバーセキュリティリスク管理，脆弱性とインシデントの取扱い，インシデント，サイバーな脅威及び脆弱性に関する情報共有並びにインシデント対応の調整及び協力の過程において採択された措置との関係において起き得る。そのような措置は，IP アドレス，統一資源位置指定子（URLs），ドメイン名，電子メールアドレス，データ主体の組織上の役割，タイムスタンプ，電子メールの件名またはファイル名のような，一定の類型の個人データの処理を要求し得る。この規則によって講じられる全ての措置は，データ保護及びプライバシーの枠組みを遵守すべきであり，また，欧州連合の法主体，CERT-EU，及び，それが適格なときは，IICB は，説明責任を果たす態様でそのような遵守を確保するための全ての適格な技術上の安全確保及び組織上の安全確保を講ずるべきである。

[7] 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).

Regulation (EU) 2018/1725 of the European Parliament and of the Council [7] applies to any processing of personal data pursuant to this Regulation. The processing of personal data could take place in relation to measures adopted in the context of cybersecurity risk management, vulnerability and incident handling, information sharing about incidents, cyber threats and vulnerabilities, and incident response coordination and cooperation. Such measures could require the processing of certain categories of personal data, such as IP addresses, uniform resources locators (URLs), domain names, email addresses, organisational roles of the data subject, time stamps, email subjects or file names. All measures taken pursuant to this Regulation should comply with the data protection and privacy framework, and the Union entities, CERT-EU and, where relevant, the IICB, should take all relevant technical and organisational safeguards to ensure such compliance in an accountable manner.

(40) この規則は，規則(EU) 2018/1725 の第 5 条第 1 項(b)に従い，この規則の下における当該法主体の職務を遂行すること及び当該法主体の義務を履行することという目的のための欧州連合の法主体，CERT-EU，及び，それが適格なときは，IICB による個人データの処理のための法律上の根拠を定める。CERT-EU は，規則(EU) 2018/1725 によって CERT-EU が遂行する職務の別により，処理者または管理者として行動し得る。

This Regulation establishes the legal basis for the processing of personal data by Union entities, CERT-EU and, where relevant, the IICB, for the purpose of performing their tasks and fulfilling their obligations under this Regulation, in accordance with Article 5(1), point (b), of Regulation (EU) 2018/1725. CERT-EU may act as processor or controller depending on the task it performs pursuant to Regulation (EU) 2018/1725.

(41) 一定の場合において，高いレベルのサイバーセキュリティを確保すべきこの規則の下における当該法主体の義務を遵守する目的のために，及び，とりわけ脆弱性とインシデントの取扱いの過程において，欧州連合の法主体及び CERT-EU に関し，規則(EU) 2018/1725 の第 10 条第 1 項に示す特別類型の個人データを処理することが必要となり得る。この規則は，規則(EU) 2018/1725 の第 10 条第 2 項(g)に従い，欧州連合の法主体及び CERT-EU による特別類型の個人データの処理のための法律上の根拠を定める。この規則の下における特別類型の個人データの処理は，求められる狙いに対して厳格に比例的であるべきである。規則(EU) 2018/1725 の第 10 条第 2 項(g)の中で定められた条件に服して，欧州連合の法主体及び CERT-EU は，それが必要な範囲内に限り，かつ，この規則の中で明示で定められている場合に限り，そのようなデータを処理できるべきである。特別類型の個人データを処理する際，欧州連合の法主体及び CERT-EU は，データ保護の権利の本質を尊重すべきであり，かつ，基本的な権利及びデータ主体の利益を守るための適切かつ個別の措置を定めるべきである。

In certain cases, for the purpose of complying with their obligations under this Regulation to ensure a high level of cybersecurity and in particular in the context of vulnerability and incident handling, it may be necessary for Union entities and CERT-EU to process special categories of personal data as referred to in Article 10(1) of Regulation (EU) 2018/1725. This Regulation establishes the legal basis for the processing of special categories of personal data by Union entities and CERT-EU in accordance with Article 10(2), point (g), of Regulation (EU) 2018/1725. The processing of special categories of personal data under this Regulation should be strictly proportionate to the aim pursued. Subject to the

conditions set out in Article 10(2), point (g), of that Regulation, the Union entities and CERT-EU should be able to process such data only to the extent necessary and where explicitly provided for in this Regulation. When processing special categories of personal data, the Union entities and CERT-EU should respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subjects.

(42) 規則(EU) 2018/1725 の第 33 条により，欧州連合の法主体及び CERT-EU は，最新技術，実装の費用及び処理の性質，範囲，過程と目的，並びに，自然人の権利及び自由に関する多様な蓋然性と深刻度のリスクを考慮に入れた上で，知る必要性ベースで制限されたアクセスの権利の提供，監査証跡の諸原則の適用，証跡の保全の採択，管理下にありかつ監査可能な環境内におけるデータの記録保存，標準化された業務運営手続，並びに，仮名化または暗号のようなプライバシー保護措置のような，適切なレベルの個人データの安全性を確保するための適切な技術上の措置及び組織上の措置を実装すべきである。それらの措置は，インシデントの取扱い及び証拠の完全性の目的に対して影響を与える態様で実装されてはならない。欧州連合の法主体または CERT-EU が，この規則の目的のために，相手方またはパートナーに対し，特別類型の個人データを含め，インシデントと関連する個人データを移転するときは，そのような移転は，規則(EU) 2018/1725 を遵守すべきである。特別類型の個人データが第三者に対して移転されるときは，欧州連合の法主体及び CERT-EU は，当該第三者が，規則(EU) 2018/1725 と均等なレベルの個人データの保護に関する措置を適用することを確保すべきである。

Pursuant to Article 33 of Regulation (EU) 2018/1725, Union entities and CERT-EU should, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure an appropriate level of security of personal data, such as the provision of restricted access rights on a need-to-know basis, the application of audit trail principles, the adoption of chain of custody, the storage of data at rest in a controlled and auditable environment, standardised operational procedures and privacy preserving measures such as pseudonymisation or encryption. Those measures should not be implemented in a manner affecting the purposes of incident handling and integrity of evidence. Where a Union entity or CERT-EU transfers personal data related to an incident, including special categories of personal data, to a counterpart or partner for the purposes of this Regulation, such transfers should comply with Regulation (EU) 2018/1725. Where special categories of personal data are transferred to a third party, the Union entities and CERT-EU should ensure that the third party applies measures concerning the protection of personal data at a level equivalent to Regulation (EU) 2018/1725.

(43) この規則の目的のために処理される個人データは，規則(EU) 2018/1725 に従って必要な期間内に限り，保持されるものとしなければならない。欧州連合の法主体，及び，それが適用可能なときは，管理者として行動する CERT-EU は，個々の目的を達成するために必要なところに制限される保持期間を定めるべきである。とりわけ，インシデントの取扱いのための個人データの収集との関係において，欧州連合の法主体及び CERT-EU は，インシデントを防止するために，当該法主体の ICT 環境中のサイバーな脅威の検出のために収集される個人データと，インシデントの緩和，それへの対応及びそれからの復旧のために収集される個人データとを区別すべきである。サイバーな脅威の検出のためには，脅威行動者がシステム中では未検出のままであり得る時間を考慮に入れることが重要であ

る。インシデントの緩和，それへの対応及びそれからの復旧のためには，反復的なインシデントまたは当該インシデントに関して相関関係が示され得る類似の性質のインシデントの追跡及び取扱いのためのその個人データが必要であるか否かを判断することが重要である。

Personal data processed for the purposes of this Regulation should be retained only for as long as necessary in accordance with Regulation (EU) 2018/1725. Union entities and, where applicable, CERT-EU acting as a controller, should set retention periods which are limited to what is necessary to achieve the specified purposes. In particular in relation to personal data collected for incident handling, Union entities and CERT-EU should differentiate between personal data that are collected for the detection of a cyber threat in their ICT environments to prevent an incident and personal data that are collected for the mitigation of, response to and recovery from an incident. For the detection of a cyber threat, it is important to take into account the time that a threat actor can remain undetected in a system. For the mitigation of, response to and recovery from an incident, it is important to consider whether the personal data are necessary to trace and handle a recurrent incident or an incident of similar nature for which a correlation could be demonstrated.

(44) 欧州連合の法主体及び CERT-EU による情報の取扱いは，情報セキュリティに関する適用可能な規定を遵守すべきである。サイバーセキュリティ上のリスクマネジメント措置としての人的資源の防護の包摂もまた，適用可能な規定を遵守すべきである。

The handling of information by Union entities and CERT-EU should comply with the applicable rules on information security. The inclusion of human resources security as a cybersecurity risk-management measure should also comply with the applicable rules.

(45) 情報共有の目的のために，とりわけ，非公開の合意もしくはトラフィックライトプロトコルのような非公開の非公式合意またはそれら以外の情報源からの明確な表示を基礎として，情報の受領者によって適用されるべき共有の限界を表示するために，視認可能なマーキングが使用される。トラフィックライトプロトコルは，情報の別の目的による拡散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。トラフィックライトプロトコルは，ほぼ全ての CSIRTs において及び幾つかの情報分析共有拠点において使用されている。

For the purpose of sharing information, visible markings are used to indicate that sharing boundaries are to be applied by the recipients of information on the basis of, in particular, non-disclosure agreements, or informal non-disclosure agreements such as the traffic light protocol or other clear indications by the source. 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 CSIRTs and in some information analysis and sharing centres.

(46) この規則は，欧州連合の事務局としての CERT-EU の設置の可能性を含め，CERT-EU の稼動及び組織上の役割に関して別の決定が行われることを許容する多年度財政枠組みの将来の交渉に照らし，定期的に評価されるべきである。

This Regulation should be evaluated on a regular basis in light of future negotiations of multiannual financial frameworks,

allowing for further decisions to be made with respect to the functioning and institutional role of CERT-EU, including the possible establishment of CERT-EU as a Union office.

(47) IICB は，CERT-EU の補助を得て，この規則の実装を見直しし及び評価すべきであり，また，欧州委員会に対し，IICB の判断結果を報告すべきである。この入力を基礎として，欧州委員会は，欧州議会，理事会，欧州経済社会委員会及び地域委員会に対し，報告すべきである。その報告は，IICB の入力と共に，とりわけ，欧州連合の法主体にとって共通の情報セキュリティ規定がない場合において，この規則の適用範囲内で EUCI を取扱うネットワーク及び情報システムを包摂することの適切性を評価すべきである。

The IICB, with the assistance of CERT-EU, should review and evaluate the implementation of this Regulation and should report its findings to the Commission. Building on this input, the Commission should report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. That report, with the input of the IICB, should evaluate the appropriateness of including network and information systems handling EUCI within the scope of this Regulation, in particular in the absence of information security rules common to Union entities.

(48) 比例性の原則に従い，欧州連合の法主体のためのサイバーセキュリティに関する規定を定めることは，欧州連合の法主体内の共通の高いレベルのサイバーセキュリティを達成するという基本的な目的の達成のために必要かつ適切である。この規則は，欧州連合条約の第 5 条第 4 項に従い，求める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。

In accordance with the principle of proportionality, it is necessary and appropriate for the achievement of the basic objective of achieving a high common level of cybersecurity within Union entities to lay down rules on cybersecurity for Union entities. This Regulation does not go beyond what is necessary in order to achieve the objective pursued, in accordance with Article 5(4) of the Treaty on European Union.

(49) この規則は，欧州連合の法主体が，資金面及び人的資源の面を含め，規模及び能力において異なっているという事実を反映している。

This Regulation reflects the fact that Union entities differ in size and capacity, including in terms of financial and human resources.

(50) 欧州データ保護監督官は，規則(EU) 2018/1725 の第 42 条第 1 項に従って意見聴取を受け，2022 年 5 月 17 日に意見書[8]を伝達した，

The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on 17 May 2022[8],

[8] OJ C 258, 5.7.2022, p. 10.

以上のとおりであるので, この規則を採択する:

HAVE ADOPTED THIS REGULATION:

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

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

この規則は，以下の事柄に関し，欧州連合の法主体内の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狙いとする措置を定める：

This Regulation lays down measures that aim to achieve a high common level of cybersecurity within Union entities with regard to:

(a) 第 6 条によるサイバーセキュリティ上の内部的なリスクマネジメント，統治及び管理の枠組みの欧州連合の各法主体による設置；

the establishment by each Union entity of an internal cybersecurity risk-management, governance and control framework pursuant to Article 6;

(b) サイバーセキュリティ上のリスクマネジメント，報告及び情報共有；

cybersecurity risk management, reporting and information sharing;

(c) 第 10 条によって設置される機関間サイバーセキュリティ委員会の組織，稼動及び業務運営，並びに，欧州連合の機関，組織，事務局及び部局のためのサイバーセキュリティサービス（CERT-EU）の組織，稼動及び業務運営；

the organisation, functioning and operation of the Interinstitutional Cybersecurity Board established pursuant to Article 10, as well as the organisation, functioning and operation of the Cybersecurity Service for the Union institutions, bodies, offices and agencies (CERT-EU);

(d) この規則の実装の監視。

the monitoring of the implementation of this Regulation.

第 2 条 適用範囲
Article 2 **Scope**

1. この規則は，欧州連合の法主体に対し，第 10 条によって設置される機関間サイバーセキュリティ委員会に対し及び CERT-EU に対し，適用される。

This Regulation applies to Union entities, to the Interinstitutional Cybersecurity Board established pursuant to Article 10 and to CERT-EU.

2. この規則は，諸条約による諸機関の自律性を妨げることなく適用される。

This Regulation applies without prejudice to the institutional autonomy pursuant to the Treaties.

3. 第 13 条第 8 項の場合を除き，この規則は，EU機密情報（EUCI）を取扱うネットワーク及び情報システムに対しては，適用されない。

With the exception of Article 13(8), this Regulation does not apply to network and information systems handling EU classified information (EUCI).

第 3 条 定義

Article 3 **Definitions**

この規則の目的のために，以下の定義が適用される：

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

(1) 「欧州連合の法主体」とは，欧州連合条約，欧州連合の機能に関する条約（TFEU）または欧州原子力共同体条約によって設置された欧州連合の機関，組織，事務局及び部局のことを意味し；

‘Union entities’ means the Union institutions, bodies, offices and agencies set up by or pursuant to the Treaty on European Union, the Treaty on the Functioning of European Union (TFEU) or the Treaty establishing the European Atomic Energy Community;

(2) 「ネットワーク及び情報システム」とは，指令(EU) 2022/2555 の第 6 条第 1 号の中で定義されたネットワーク及び情報システムのことを意味し；

‘network and information system’ means a network and information system as defined in Article 6, point (1), of Directive (EU) 2022/2555;

(3) 「ネットワーク及び情報システムの防護」とは，指令(EU) 2022/2555 の第 6 条第 2 号の中で定義されたネットワーク及び情報システムの防護のことを意味し；

‘security of network and information systems’ means security of network and information systems as defined in Article 6, point (2), of Directive (EU) 2022/2555;

(4) 「サイバーセキュリティ」とは，規則(EU) 2019/881 の第 2 条第 1 号の中で定義されたサイバーセキュリティのことを意味し；

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

(5) 「最上位レベルの運営主体」とは，遵守及びサイバーセキュリティ上のリスクマネジメントに関する他のレベルの運営主体の当該運営主体のそれぞれの職責分野における公式の職責を妨げることなく，欧州連合の法主体の稼動に関して最上位の行政レベルで職責を負い，当該欧州連合の法主体の高いレベルの統治の手立てに沿って決定を採択しまたは許可することの委任を受けた運営者，運営組織または調整と監視の組織のことを意味し；

‘highest level of management’ means a manager, management body or coordination and oversight body that is responsible for the functioning of a Union entity, at the most senior administrative level, with a mandate to adopt or authorise decisions in line with the high-level governance arrangements of that Union entity, without prejudice to the formal responsibilities of other levels of management for compliance and cybersecurity risk management in their respective areas of responsibility;

(6) 「ニアミス」とは，指令(EU) 2022/2555 の第 6 条第 5 号の中で定義されたニアミスのことを意味し；

‘near miss’ means a near miss as defined in Article 6, point (5), of Directive (EU) 2022/2555;

(7) 「インシデント」とは，指令(EU) 2022/2555 の第 6 条第 6 号の中で定義されたインシデントのことを意味し；

‘incident’ means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555;

(8) 「大きなインシデント」とは，そのインシデントに対して対応するための欧州連合の法主体及び CERT-EU 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 つの欧州連合の法主体に対して大きな影響をもつインシデントのことを意味し；

‘major incident’ means an incident which causes a level of disruption that exceeds a Union entity’s and CERT-EU’s capacity to respond to it or which has a significant impact on at least two Union entities;

(9) 「大規模なサイバーセキュリティインシデント」とは，指令(EU) 2022/2555 の第 6 条第 7 号の中で定義された大規模なサイバーセキュリティインシデントのことを意味し；

‘large-scale cybersecurity incident’ means a large-scale cybersecurity incident as defined in Article 6, point (7), of Directive (EU) 2022/2555;

(10) 「インシデントの取扱い」とは，指令(EU) 2022/2555 の第 6 条第 8 号の中で定義されたインシデン

トの取扱い のことを意味し；

‘incident handling’ means incident handling as defined in Article 6, point (8), of Directive (EU) 2022/2555;

(11) 「サイバーな脅威」とは，規則(EU) 2019/881 の第 2 条第 8 号の中で定義されたサイバーな脅威のことを意味し；

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

(12) 「大きなサイバーな脅威」とは，指令(EU)2022/2555 の第 6 条第 11 号の中で定義された大きなサイバーな脅威のことを意味し；

‘significant cyber threat’ means a significant cyber threat as defined in Article 6, point (11), of Directive (EU) 2022/2555;

(13) 「脆弱性」とは，指令(EU) 2022/2555 の第 6 条第 15 号の中で定義された脆弱性のことを意味し；

‘vulnerability’ means a vulnerability as defined in Article 6, point (15), of Directive (EU) 2022/2555;

(14) 「サイバーセキュリティ上のリスク」とは，指令(EU) 2022/2555 の第 6 条第 9 号の中で定義されたリスクのことを意味し；

‘cybersecurity risk’ means a risk as defined in Article 6, point (9), of Directive (EU) 2022/2555;

(15) 「クラウドコンピューティングサービス」とは，指令(EU) 2022/2555 の第 6 条第 30 号の中で定義されたクラウドコンピューティングサービスのことを意味する。

‘cloud computing service’ means a cloud computing service as defined in Article 6, point (30), of Directive (EU) 2022/2555.

第 4 条 個人データの処理

Article 4 **Processing of personal data**

1. CERT-EU，第 10 条によって設置される機関間サイバーセキュリティ委員会及び欧州連合の法主体によるこの規則の下における個人データの処理は，規則(EU) 2018/1725 に従って実行される。

The processing of personal data under this Regulation by CERT-EU, the Interinstitutional Cybersecurity Board established pursuant to Article 10 and Union entities shall be carried out in accordance with Regulation (EU) 2018/1725.

2. CERT-EU, 第 10 条によって設置される機関間サイバーセキュリティ委員会及び欧州連合の法主体がこの規則によって職務を遂行しまたは義務を履行するときは, それらの法主体は, 必要な範囲内に限り, かつ, 当該職務を遂行することまたは当該義務を履行することという目的のためにのみ, 個人データを処理し及び交換する。

Where they perform tasks or fulfil obligations pursuant to this Regulation, CERT-EU, the Interinstitutional Cybersecurity Board established pursuant to Article 10 and Union entities shall process and exchange personal data only to the extent necessary and for the sole purpose of performing those tasks or fulfilling those obligations.

3. 規則(EU) 2018/1725 の第 10 条第 1 項に示す特別類型の個人データの処理は, 同規則の第 10 条第 2 項(g)による重要な公共の利益を理由として必要であると判断される。そのようなデータは, この規則の第 6 条及び第 8 条に示すサイバーセキュリティ上のリスクマネジメント措置の実装のため, 第 13 条による CERT-EU からのサービスの提供のため, 第 17 条第 3 項及び第 18 条第 3 項によるインシデント特化情報の共有のため, 第 20 条による情報の共有のため, 第 21 条による報告義務のため, 第 22 条によるインシデント対応の調整及び協力のため, 並びに, 第 23 条による大きなインシデントの取扱いのために必要な範囲内に限り, 処理され得る。欧州連合の法主体及びデータ管理者として行動する場合の CERT-EU は, 別の目的のための特別類型の個人データの処理を防止するための技術上の措置を適用し, かつ, 基本的な権利及びデータ主体の利益を守るための適切かつ個別の措置を定める。

The processing of special categories of personal data as referred to in Article 10(1) of Regulation (EU) 2018/1725 shall be considered to be necessary for reasons of substantial public interest pursuant to Article 10(2), point (g), of that Regulation. Such data may be processed only to the extent necessary for the implementation of cybersecurity risk-management measures referred to in Articles 6 and 8, for the provision of services by CERT-EU pursuant to Article 13, for the sharing of incident-specific information pursuant to Article 17(3) and Article 18(3), for the sharing of information pursuant Article 20, for the reporting obligations pursuant to Article 21, for incident response coordination and cooperation pursuant to Article 22 and for the management of major incidents pursuant to Article 23 of this Regulation. The Union entities and CERT-EU, when acting as data controllers, shall apply technical measures to prevent the processing of special categories of personal data for other purposes and shall provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subjects.

第 II 章 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
Chapter II Measures for a High Common Level of Cybersecurity

第 5 条 措置の実装
Article 5 **Implementation of measures**

1. 2024 年 9 月 8 日までに，第 10 条によって設置される機関間サイバーセキュリティ委員会は，欧州連合サイバーセキュリティ局（ENISA）からの意見聴取を経た上で，かつ，CERT-EU からのガイダンスを受けた後，最初のサイバーセキュリティの見直しを実行し，並びに，第 6 条によるサイバーセキュリティ上の内部的なリスクマネジメント，統治及び管理の枠組みを設け，第 7 条によるサイバーセキュリティの成熟度評価を実施し，第 8 条によるサイバーセキュリティ上のリスクマネジメント措置をとり，並びに，第 9 条によりサイバーセキュリティ計画を採択するという目的のために，欧州連合の法主体宛に運用指針を発行する。

   By 8 September 2024, the Interinstitutional Cybersecurity Board established pursuant to Article 10 shall, after consulting the European Union Agency for Cybersecurity (ENISA) and after receiving guidance from CERT-EU, issue guidelines to Union entities for the purpose of carrying out an initial cybersecurity review and establishing an internal cybersecurity risk-management, governance and control framework pursuant to Article 6, carrying out cybersecurity maturity assessments pursuant to Article 7, taking cybersecurity risk-management measures pursuant to Article 8, and adopting the cybersecurity plan pursuant to Article 9.

2. 第 6 条ないし第 9 条を実装する際，欧州連合の法主体は，本条第 1 項に示す運用指針並びに第 11 条及び第 14 条によって採択される適格な運用指針及び勧告を考慮に入れる。

   When implementing Articles 6 to 9, Union entities shall take into account the guidelines referred to in paragraph 1 of this Article, as well as relevant guidelines and recommendations adopted pursuant to Articles 11 and 14.

第 6 条 サイバーセキュリティ上のリスクマネジメント，統治及び管理の枠組み
Article 6 **Cybersecurity risk-management, governance and control framework**

1. 2025 年 4 月 8 日までに，欧州連合の各法主体は，監査のような最初のサイバーセキュリティ上の見直しを実行した後，サイバーセキュリティ上の内部的なリスクマネジメント，統治及び管理の枠組み（「枠組み」）を設ける。枠組みの構築は，その欧州連合の法主体の最上位レベルの運営主体による監督を受け，かつ，その職責の下にある。

   By 8 April 2025, each Union entity shall, after carrying out an initial cybersecurity review, such as an audit, establish an internal cybersecurity risk-management, governance and control framework (the 'Framework'). The establishment of the Framework shall be overseen by and under the responsibility of the Union entity's highest level of management.

2. 枠組みは，オンプレミスICT環境，運用技術ネットワーク，アウトソースされた資産及びクラウドコンピューティング環境内のサービスもしくはサードパーティによってホストされるサービス，モバイル機器，社内ネットワーク，インターネットに接続されていない企業ネットワーク及びそれらの環境（ICT 環境）に接続されている機器を含め，関係する欧州連合の法主体の機密ではない ICT 環境全部を包摂する。枠組みは，オールハザードアプローチを基礎とする。

The Framework shall cover the entirety of the unclassified ICT environment of the Union entity concerned, including any on-premises ICT environment, operational technology network, outsourced assets and services in cloud computing environments or hosted by third parties, mobile devices, corporate networks, business networks not connected to the internet and any devices connected to those environments (ICT environment). The Framework shall be based on an all-hazards approach.

3. 枠組みは，高いレベルのサイバーセキュリティを確保する。枠組みは，目的及び優先事項を含め，ネットワーク及び情報システムの防護並びにこの規則の実効的な実装を確保することを職務とする欧州連合の法主体職員の役割及び職責に関する内部的なサイバーセキュリティ基本方針を定める。枠組みは，実装の実効性を測定するための仕組みも含める。

The Framework shall ensure a high level of cybersecurity. The Framework shall establish internal cybersecurity policies, including objectives and priorities, for the security of network and information systems, and the roles and responsibilities of the Union entity's staff tasked with ensuring the effective implementation of this Regulation. The Framework shall also include mechanisms to measure the effectiveness of the implementation.

4. 枠組みは，サイバーセキュリティ上のリスクが変化していることに照らし，定期的に，かつ，少なくとも 4 年毎に，見直される。必要に応じて，かつ，第 10 条によって設置される機関間サイバーセキュリティ委員会から要求を受けた後，欧州連合の法主体の枠組みは，この規則の実装の中で発見されたインシデント及び観察された格差の可能性に関する CERT-EU からのガイダンスを基礎としてアップデートされ得る。

The Framework shall be reviewed on a regular basis, in light of the changing cybersecurity risks, and at least every four years. Where appropriate and following a request from the Interinstitutional Cybersecurity Board established pursuant to Article 10, a Union entity's Framework may be updated on the basis of guidance from CERT-EU on incidents identified or possible gaps observed in the implementation of this Regulation.

5. 欧州連合の各法主体の最上位レベルの運営主体は，この規則の実装に関する職責を負い，かつ，当該法主体の組織による枠組みと関連する義務の遵守を監督する。

The highest level of management of each Union entity shall be responsible for the implementation of this Regulation and shall oversee the compliance of its organisation with the obligations related to the Framework.

6. 必要に応じて，かつ，この規則の実装に関する当該最上位レベルの運営主体の職責を妨げること

なく，欧州連合の各法主体の最上位レベルの運営主体は，この規則の下にある特定の義務を，関係する欧州連合の法主体内の職員規則の第 29 条第 2 項の意味における上級官吏またはそれ以外の均等なレベルの官吏に対して委任できる。そのような委任に拘わらず，その最上位レベルの運営主体は，関係する欧州連合の法主体によるこの規則の違反行為に関し，法的責任を負い得る。

Where appropriate and without prejudice to its responsibility for the implementation of this Regulation, the highest level of management of each Union entity may delegate specific obligations under this Regulation to senior officials within the meaning of Article 29(2) of the Staff Regulations or other officials at equivalent level, within the Union entity concerned. Regardless of any such delegation, the highest level of management may be held liable for infringements of this Regulation by the Union entity concerned.

7. 欧州連合の各法主体は，サイバーセキュリティに対して適切な割合の ICT 予算が支出されることを確保するための実効的な仕組みを設ける。その割合を定める際，枠組みが適正に考慮に入れられる。

Each Union entity shall have effective mechanisms in place to ensure that an adequate percentage of the ICT budget is spent on cybersecurity. Due account shall be taken of the Framework when establishing that percentage.

8. 欧州連合の各法主体は，地方サイバーセキュリティ吏員，または，その吏員と均等な機能をもつサイバーセキュリティの全ての側面と関係する当該法主体の単一連絡部局として行動する者を任命する。地方サイバーセキュリティ吏員は，この規則の実装を促進し，かつ，定期的に，その実装の状態に関し，最上位レベルの運営主体に対して直接に報告する。欧州連合の各法主体の単一連絡部局である地方サイバーセキュリティ吏員を妨げることなく，欧州連合の法主体は，当該欧州連合の法主体と CERT-EU との間で締結されるサービスレベルの合意を基礎として，この規則の実装と関連する地方サイバーセキュリティ吏員の一定の職務を，CERT-EU に対して委任することができ，または，当該職務は，複数の欧州連合の法主体によって共有され得る。それらの職務が CERT-EU に対して委任されるときは，第 10 条によって設置される機関間サイバーセキュリティ委員会は，関係する欧州連合の法主体の人的資源及び資金を考慮に入れた上で，当該サービスの提供が CERT-EU のベースラインのサービスの一部であるべきか否かを判定する。欧州連合の各法主体は，不適切な遅滞なく，CERT-EU に対し，任命された地方サイバーセキュリティ吏員及びその任命のその後の変更を通知する。

Each Union entity shall appoint a local cybersecurity officer or an equivalent function who shall act as its single point of contact regarding all aspects of cybersecurity. The local cybersecurity officer shall facilitate the implementation of this Regulation and report directly to the highest level of management on a regular basis on the state of the implementation. Without prejudice to the local cybersecurity officer being the single point of contact in each Union entity, a Union entity may delegate certain tasks of the local cybersecurity officer with regard to the implementation of this Regulation to CERT-EU on the basis of a service level agreement concluded between that Union entity and CERT-EU, or those tasks may be shared by several Union entities. Where those tasks are delegated to CERT-EU, the Interinstitutional Cybersecurity Board established pursuant to Article 10 shall decide whether the provision of that service is to be part of the baseline services of

CERT-EU, taking into account the human and financial resources of the Union entity concerned. Each Union entity shall, without undue delay, notify CERT-EU of the local cybersecurity officer appointed and any subsequent change thereto.

CERT-EU は，任命された地方サイバーセキュリティ吏員のリストを作成し，かつ，最新のものに保つ。

CERT-EU shall establish and keep updated a list of appointed local cybersecurity officers.

9. 欧州連合の各法主体の職員規則の第 29 条第 2 項の意味における上級官吏またはそれ以外の均等なレベルの官吏，並びに，サイバーセキュリティ上のリスクマネジメント措置を実装し，かつ，この規則の中で定められた義務を履行する職務をもつ適格な全ての職員である者は，サイバーセキュリティ上のリスクマネジメント及びマネジメント実務並びに欧州連合の法主体に対するそのマネジメントの運用の影響を理解しかつ評価するための十分な知識と技能を獲得するという観点から，定期的に，特別の訓練を受ける。

The senior officials within the meaning of Article 29(2) of the Staff Regulations or other officials at equivalent level of each Union entity, as well as all relevant members of staff tasked with implementing the cybersecurity risk-management measures and with fulfilling obligations laid down in this Regulation, shall follow specific training on a regular basis with a view to gaining sufficient knowledge and skills in order to apprehend and assess cybersecurity risk- and management practices and their impact on the operations of the Union entity.

第 7 条 サイバーセキュリティの成熟度評価

Article 7 **Cybersecurity maturity assessments**

1. 2025 年 7 月 8 日までに，かつ，その後は少なくとも 2 年毎に，欧州連合の各法主体は，当該法主体の ICT 環境の全ての要素を盛り込むサイバーセキュリティの成熟度評価を実施する。

By 8 July 2025 and at least every two years thereafter, each Union entity shall carry out a cybersecurity maturity assessment incorporating all the elements of its ICT environment.

2. サイバーセキュリティの成熟度評価は，必要に応じて，特化されたサードパーティの補助を得て実施される。

The cybersecurity maturity assessments shall, where appropriate, be carried out with the assistance of a specialised third party.

3. 類似の構造をもつ欧州連合の法主体は，それらそれぞれの法主体のサイバーセキュリティの成熟度評価を実施する上で，協力し得る。

Union entities with similar structures may cooperate in carrying out cybersecurity maturity assessments for their respective

entities.

4. 第 10 条によって設置される機関間サイバーセキュリティ委員会の要請を基礎として，かつ，関係する欧州連合の法主体の明示の同意を得た上で，サイバーセキュリティの成熟度評価の結果は，経験から学習し及びベストプラクティスを共有するという観点から，同委員会の中において，または，地方サイバーセキュリティ吏員の非公式グループの中において討議され得る。

On the basis of a request of the Interinstitutional Cybersecurity Board established pursuant to Article 10 and with the explicit consent of the Union entity concerned, the results of a cybersecurity maturity assessment may be discussed within that Board or within the informal group of local cybersecurity officers with a view to learning from experience and sharing best practices.

第 8 条 サイバーセキュリティ上のリスクマネジメント措置

Article 8 **Cybersecurity risk-management measures**

1. 不適切な遅滞なく，かつ，いかなる場合においても 2025 年 9 月 8 日までに，欧州連合の各法主体は，当該法主体の最上位レベルの運営主体の監督の下において，枠組みの下において特定されたサイバーセキュリティ上のリスクを管理するため，及び，インシデントの影響を防止またはミニマム化するため，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。最新技術を考慮に入れた上で，かつ，それが適用可能なときは，適格な欧州の技術標準と国際的な技術標準を考慮に入れた上で，それらの措置は，呈されているサイバーセキュリティ上のリスクに見合った ICT 環境全体にわたるネットワーク及び情報システムの防護のレベルを確保する。それらの措置の比例性を評価する際には，欧州連合の法主体のサイバーセキュリティ上のリスクへのエクスポージャーの程度，そのエクスポージャーの大きさ及びインシデント発生の蓋然性，並びに，当該インシデントの社会的影響，経済的影響及び機関間の影響を含め，インシデントの深刻度が適正に考慮に入れられる。

Without undue delay and in any event by 8 September 2025, each Union entity shall, under the oversight of its highest level of management, take appropriate and proportionate technical, operational and organisational measures to manage the cybersecurity risks identified under the Framework, and to prevent or minimise the impact of incidents. Taking into account the state of the art and, where applicable, relevant European and international standards, those measures shall ensure a level of security of network and information systems across the entirety of the ICT environment commensurate to the cybersecurity risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the Union entity's exposure to cybersecurity risks, its size and the likelihood of occurrence of incidents and their severity, including their societal, economic and interinstitutional impact.

2. 欧州連合の法主体は，サイバーセキュリティ上のリスクマネジメント措置の実装において，少なくとも以下の諸部門に対処する:

Union entities shall address at least the following domains in the implementation of the cybersecurity risk-management measures:

(a) 第 6 条及び本条第 3 項に示す目的及び優先事項に到達するために要する措置を含め，サイバーセキュリティの基本方針；

cybersecurity policy, including measures needed to reach objectives and priorities referred to in Article 6 and paragraph 3 of this Article;

(b) セイバーセキュリティ上のリスク分析及び情報システムの防護に関する基本方針；

policies on cybersecurity risk analysis and information system security;

(c) クラウドコンピューティングサービスの利用と関連する基本政策上の目的；

policy objectives regarding the use of cloud computing services;

(d) サイバーセキュリティ監査，必要に応じて，その監査は，信頼できる民間プロバイダによって定期的に実施されるサイバーセキュリティ上のリスク，脆弱性及びサイバーな脅威の評価並びにペネトレーションテストを含み得る；

cybersecurity audit, where appropriate, which may include a cybersecurity risk, vulnerability and cyber threat assessment, and penetration testing carried out by a trusted private provider on a regular basis;

(e) サイバーセキュリティ及び基本方針のアップデートを介する，(d)に示すサイバーセキュリティ監査から帰結する推奨事項の実装；

implementation of recommendations resulting from cybersecurity audits referred to in point (d) through cybersecurity and policy updates;

(f) 役割及び職責の設定を含め，サイバーセキュリティの組織；

organisation of cybersecurity, including establishment of roles and responsibilities;

(g) ICT 資産目録及び ICT ネットワーク構成図を含め，資産管理；

asset management, including ICT asset inventory and ICT network cartography;

(h) 人的資源の防護及びアクセス管理；

human resources security and access control;

(i) 業務運営の防護;

operations security;

(j) 通信の防護;

communications security;

(k) 脆弱性の取扱い及び開示に関する基本方針を含め，システムの獲得，開発及び維持管理;

system acquisition, development and maintenance, including policies on vulnerability handling and disclosure;

(l) それが可能なときは，ソースコードの透明性に関する基本方針;

where possible, policies on the transparency of the source code;

(m) 欧州連合の各法主体とその直接の供給者またはサービスプロバイダとの間の関係に関する防護関連の諸側面を含め，サプライチェーンの防護;

supply chain security, including security-related aspects concerning the relationships between each Union entity and its direct suppliers or service providers;

(n) セキュリティ監視及び履歴記録の維持管理のような，インシデントの取扱い及び CERT-EU との協力;

incident handling and cooperation with CERT-EU, such as the maintenance of security monitoring and logging;

(o) バックアップ管理と災害からの復旧及び危機管理のような，事業継続性の管理;並びに

business continuity management, such as backup management and disaster recovery, and crisis management; and

(p) サイバーセキュリティ上の教育，技能，認識向上，演習及び訓練の計画の促進と開発。

promotion and development of cybersecurity education, skills, awareness-raising, exercise and training programmes.

第 1 副項(m)の目的のために，欧州連合の法主体は，個々の直接の供給者とサービスプロバイダの脆弱性の特性，並びに，製品の全体的な品質，及び，当該供給者とサービスプロバイダの安全な開

発手順を含め，当該供給者とサービスプロバイダのサイバーセキュリティ上の実務を考慮に入れる。

For the purposes of the first subparagraph, point (m), Union entities shall 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.

3. 欧州連合の法主体は，少なくとも以下のとおりのサイバーセキュリティ上の細目的なリスクマネジメント措置を講ずる：

Union entities shall take at least the following specific cybersecurity risk-management measures:

(a) テレワーキングを実現可能にしかつ支持する技術上の手配；

technical arrangements to enable and sustain teleworking;

(b) ゼロトラスト原則に向けて移行するための具体的な手立て；

concrete steps for moving towards zero-trust principles;

(c) ネットワーク及び情報システム全体にわたる規範としての多要素認証の利用；

the use of multifactor authentication as a norm across network and information systems;

(d) 暗号学及び暗号化の利用，とりわけ，エンドツーエンドの暗号化及び安全なデジタル署名の利用；

the use of cryptography and encryption, in particular end-to-end encryption, as well as secure digital signing;

(e) 必要に応じて，欧州連合の法主体内における安全な音声通信，映像通信及びテキスト通信並びに安全な緊急通信システム；

where appropriate, secured voice, video and text communications, and secured emergency communications systems within the Union entity;

(f) マルウェア及びスパイウェアの検出及び除去のための事前の措置；

proactive measures for detection and removal of malware and spyware;

(g) 安全なソフトウェア開発と評価のための基準を介するソフトウェアサプライチェーンの防護の構築；

the establishment of software supply chain security through criteria for secure software development and evaluation;

(h) この規則の実効的な実装を確保する職務をもつ欧州連合の法主体の最上位レベルの運営主体と職員である者の定められた職務及び期待される能力に応じたサイバーセキュリティに関する訓練計画の策定と採択；

the establishment and adoption of training programmes on cybersecurity commensurate to the prescribed tasks and expected capabilities for the highest level of management and members of staff of the Union entity tasked with ensuring the effective implementation of this Regulation;

(i) 職員である者の定期的なサイバーセキュリティ訓練；

regular cybersecurity training of staff members;

(j) それが適格なときは，欧州連合の法主体間の相互接続性リスク分析への参加；

where relevant, participation in interconnectivity risk analyses between the Union entities;

(k) 以下のことを介する共通の高いレベルのサイバーセキュリティを促進するための調達原則の拡大：

the enhancement of procurement rules to facilitate a high common level of cybersecurity through:

(i) インシデント，脆弱性及びサイバーな脅威に関する ICT サービスプロバイダからの情報を CERT-EU と共有することを制限している契約上の障壁の除去；

the removal of contractual barriers that limit information sharing from ICT service providers about incidents, vulnerabilities and cyber threats with CERT-EU;

(ii) インシデント，脆弱性及びサイバーな脅威を報告すべき契約上の義務，並びに，適切なインシデント対応及び監視の仕組みを設けるべき契約上の義務。

contractual obligations to report incidents, vulnerabilities and cyber threats as well as to have appropriate incident response and monitoring mechanisms in place.

第 9 条 サイバーセキュリティ計画

Article 9 **Cybersecurity plans**

1. 第 7 条によって実施されるサイバーセキュリティの成熟度評価の結了の後，かつ，枠組みの中で特定された資産及びサイバーセキュリティ上のリスク並びに第 8 条によって講じられるサイバーセキュリティ上のリスク管理措置を考慮に入れた上で，欧州連合の各法主体の最上位レベルの運営主体は，不適正な遅滞なく，かつ，いかなる場合においても 2026 年 1 月 8 日までに，サイバーセキュリティ計画を承認する。サイバーセキュリティ計画は，欧州連合の法主体のサイバーセキュリティ全体を向上させることを狙いとし，かつ，それによって，欧州連合の法主体内の共通の高いレベルのサイバーセキュリティの拡大に貢献する。サイバーセキュリティ計画は，少なくとも，第 8 条によって講じられるサイバーセキュリティ上のリスク管理措置を含める。サイバーセキュリティ計画は，2 年毎に改訂され，または，第 7 条によって実施されるサイバーセキュリティの成熟度評価の後，または，枠組みの大きな見直しの後，それが必要なときは，より頻回に改訂される。

   Following the conclusion of the cybersecurity maturity assessment carried out pursuant to Article 7 and taking into account the assets and cybersecurity risks identified in the Framework as well as the cybersecurity risk-management measures taken pursuant to Article 8, the highest level of management of each Union entity shall approve a cybersecurity plan without undue delay and in any event by 8 January 2026. The cybersecurity plan shall aim at increasing the overall cybersecurity of the Union entity and shall thereby contribute to the enhancement of a high common level of cybersecurity within the Union entities. The cybersecurity plan shall include at least the cybersecurity risk-management measures taken pursuant to Article 8. The cybersecurity plan shall be revised every two years, or more frequently where necessary, following the cybersecurity maturity assessments carried out pursuant to Article 7 or any substantial review of the Framework.

2. サイバーセキュリティ計画は，大きなインシデントに対する欧州連合の法主体のサイバー危機管理計画を含める。

   The cybersecurity plan shall include the Union entity's cyber crisis management plan for major incidents.

3. 欧州連合の法主体は，第 10 条によって設置される機関間サイバーセキュリティ委員会に対し，完成したサイバーセキュリティ計画を提出する。

   The Union entity shall submit the completed cybersecurity plan to the Interinstitutional Cybersecurity Board established pursuant to Article 10.

第 III 章 機関間サイバーセキュリティ委員会
Chapter III Interinstitutional Cybersecurity Board

第 10 条 機関間サイバーセキュリティ委員会
Article 10 Interinstitutional Cybersecurity Board

1. ここに, 機関間サイバーセキュリティ委員会（IICB）が設置される。

   An Interinstitutional Cybersecurity Board (IICB) is hereby established.

2. IICB は, 以下の事柄に関して職責を負う:

   The IICB shall be responsible for:

   (a) 欧州連合の法主体によるこの規則の実装を監視すること及び支援すること;

   monitoring and supporting the implementation of this Regulation by the Union entities;

   (b) CERT-EU による一般的な優先事項と目的の実装を監視すること及び CERT-EU に対して戦略上の指示を提供すること。

   supervising the implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU.

3. IICB は, 以下の法主体によって構成される:

   The IICB shall consist of:

   (a) 以下の各法主体から指名された 1 名の代表:

   one representative designated by each of the following:

   (i) 欧州議会;

   the European Parliament;

   (ii) 欧州理事会;

   the European Council;

(iii) 欧州連合の理事会；

the Council of the European Union;

(iv) 欧州委員会；

the Commission;

(v) 欧州連合司法裁判所；

the Court of Justice of the European Union;

(vi) 欧州中央銀行；

the European Central Bank;

(vii) 会計検査院；

the Court of Auditors;

(viii) 欧州対外行動サービス；

the European External Action Service;

(ix) 欧州経済社会委員会；

the European Economic and Social Committee;

(x) 欧州地域委員会；

the European Committee of the Regions;

(xi) 欧州投資銀行；

the European Investment Bank;

(xii) 欧州サイバーセキュリティ産業，技術及び調査研究能力拠点；

the European Cybersecurity Industrial, Technology and Research Competence Centre;

(xiii) ENISA；

ENISA;

(xiv) 欧州データ保護監督官（EDPS）；

the European Data Protection Supervisor (EDPS);

(xv) 宇宙計画に関する欧州連合局。

the European Union Agency for the Space Programme.

(b) (a)に示す者以外の，当該法主体自身の ICT 環境上で走っている欧州連合の組織，事務局及び部局の利益を代表するための当該法主体の ICT 諮問委員会からの提案を基礎として EU 部局ネットワーク（EUAN）によって指名された 3 名の代表者。

three representatives designated by the EU Agencies Network (EUAN) on the basis of a proposal by its ICT Advisory Committee to represent the interests of the bodies, offices and agencies of the Union that run their own ICT environment, other than those referred to in point (a).

IICB 上において代表される欧州連合の法主体は，指名された代表者間のジェンダーバランスを達成することを狙いとする。

The Union entities represented on the IICB shall aim to achieve gender balance among the designated representatives.

4. IICB の構成員は，代替者による補助を受け得る。第 3 項に示す欧州連合の法主体の代表以外の者または第 3 項に示す欧州連合の法主体以外の欧州連合の法主体の者は，議長から，投票の権利なく IICB の会合に出席することを招請され得る。

Members of the IICB may be assisted by an alternate. Other representatives of the Union entities referred to in paragraph 3 or of other Union entities may be invited by the Chair to attend IICB meetings without voting power.

5. CERT-EU の長，並びに，指令(EU) 2022/2555 の第 14 条，第 15 条及び第 16 条によってそれぞれ設置された協力グループ，CSIRTs ネットワーク及び EU-CyCLONe の各議長またはそれらの各議長の代替者は，オブザーバーとして IICB の会合に参加し得る。例外的な場合において，IICB の内部的な手続規則に従い，IICB は，別異に決定し得る。

The Head of CERT-EU and the Chairs of the Cooperation Group, the CSIRTs network and EU-CyCLONe established, respectively, pursuant to Articles 14, 15 and 16 of Directive (EU) 2022/2555, or their alternates, may participate in IICB meetings as observers. In exceptional cases, the IICB may, in accordance with its internal rules of procedure, decide

otherwise.

6. IICB は，IICB の内部的な手続規則を採択する。

The IICB shall adopt its internal rules of procedure.

7. IICB は，IICB の内部的な手続規則に従い，その構成員の中から，3 年の任期で，議長を指名する。議長の代替者は，同じ任期で IICB の完全な資格をもつ構成員となる。

The IICB shall designate a Chair in accordance with its internal rules of procedure, from among its members for a period of three years. The Chair's alternate shall become a full member of the IICB for the same duration.

8. IICB は，IICB の議長の発意によるとき，CERT-EU の要請があるときまたは IICB の構成員の要請があるときは，少なくとも年 3 回，会合する。

The IICB shall meet at least three times a year at the initiative of its Chair, at the request of CERT-EU or at the request of any of its members.

9. IICB の各構成員は，1 票をもつ。IICB の決定は，この規則の中で別異に定められている場合を除き，単純多数決によって行われる。IICB の議長は，可否同数の場合を除き，票をもってはならない。可否同数の場合においては，議長は，投票を決する役割を行い得る。

Each member of the IICB shall have one vote. The IICB's decisions shall be taken by simple majority except where otherwise provided for in this Regulation. The Chair of the IICB shall not have a vote except in the event of a tied vote, in which case the Chair may cast a deciding vote.

10. IICB は，IICB の内部的な手続規則に従って開始される簡易な書面手続によって審議し得る。同手続の下において，適格な決定は，構成員が異議を唱える場合を除き，議長によって定められる時間枠内において承認されたものとみなされる。

The IICB may act by means of a simplified written procedure initiated in accordance with its internal rules of procedure. Under that procedure, the relevant decision shall be deemed to be approved within the timeframe set by the Chair, except where a member objects.

11. IICB の事務局は，欧州委員会から提供され，かつ，IICB の議長に対して責任を負う。

The secretariat of the IICB shall be provided by the Commission and shall be accountable to the Chair of the IICB.

12. EUAN によって指名された代表は，EUAN の構成員に対して IICB の決定を伝達する。EUAN の構成員は，その構成員が IICB の注意を向けさせるべきだと判断する事柄を，EUAN の代表または IICB

の議長に対して提起する資格をもつ。

The representatives nominated by the EUAN shall relay the IICB's decisions to the members of the EUAN. Any member of the EUAN shall be entitled to raise with those representatives or the Chair of the IICB any matter which it considers should be brought to the IICB's attention.

13. IICB は，IICB の仕事を補佐するための執行委員会を設置し，かつ，IICB の職務及び権限中の幾つかをその執行部に対して委任し得る。IICB は，執行委員会の職務及び権限並びにその構成員の任期を含め，執行委員会の手続規則を定める。

The IICB may establish an executive committee to assist it in its work, and delegate some of its tasks and powers to it. The IICB shall lay down the rules of procedure of the executive committee, including its tasks and powers, and the terms of office of its members.

14. 2025 年 1 月 8 日までに，かつ，その後は年次で，IICB は，欧州議会及び理事会に対し，この規則の実装について行われた進捗状況の詳細を述べ，かつ，とりわけ，個々の構成国における CERT-EU と構成国の相手方との間の協力の範囲の細目を述べる報告書を提出する。その報告書は，指令(EU) 2022/2555 の第 18 条によって採択される欧州連合のサイバーセキュリティの状態に関する隔年報告書への入力となる。

By 8 January 2025 and on an annual basis thereafter, the IICB shall submit a report to the European Parliament and to the Council detailing progress made with the implementation of this Regulation and specifying in particular the extent of cooperation of CERT-EU with Member State counterparts in each of the Member States. The report shall constitute an input to the biennial report on the state of cybersecurity in the Union adopted pursuant to Article 18 of Directive (EU) 2022/2555.

第 11 条 IICB の職務

Article 11 **Tasks of the IICB**

IICB の職責を果たす際，IICB は，とりわけ：

When exercising its responsibilities, the IICB shall, in particular:

(a) CERT-EU の長に対し，ガイダンスを提供し；

provide guidance to the Head of CERT-EU;

(b) この規則の実装を実効的に監視及び監督し，かつ，必要に応じて，欧州連合の法主体及び CERT-EU に対してアドホックな報告書を要求することを含め，欧州連合の法主体のサイバーセ

キュリティを強化することにおいて欧州連合の法主体を支援し；

effectively monitor and supervise the implementation of this Regulation and support the Union entities in strengthening their cybersecurity, including, where appropriate, requesting ad-hoc reports from Union entities and CERT-EU;

(c) 戦略上の討議の後，欧州連合の法主体におけるサイバーセキュリティのレベルを向上させることに関する多年度戦略を採択し，定期的に，かつ，いかなる場合においても 5 年毎に，同戦略を評価し，かつ，それが必要なときは，同戦略を修正し；

following a strategic discussion, adopt a multiannual strategy on raising the level of cybersecurity in the Union entities, asses that strategy on a regular basis and in any event every five years and, where necessary, amend that strategy;

(d) 共有された経験から学習する，相互の信頼を強化する，共通の高いレベルのサイバーセキュリティを達成する及び欧州連合の法主体のサイバーセキュリティ上の能力を拡大するという観点から，欧州連合の法主体による任意の相互評価の実行のための手法及び組織上の側面を定め，そのような相互評価が評価を受ける欧州連合の法主体とは別の欧州連合の法主体から指名されたサイバーセキュリティ専門家によって実施されること及びそのような手法が指令(EU) 2022/2555 の第 19 条を基礎とし，かつ，必要に応じて，欧州連合の法主体に適応することを確保し；

establish the methodology and organisational aspects for the conduct of voluntary peer reviews by Union entities, with a view to learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity, as well as enhancing Union entities' cybersecurity capabilities, ensuring that such peer reviews are conducted by cybersecurity experts designated by a Union entity different from the Union entity being reviewed and that the methodology is based on Article 19 of Directive (EU) 2022/2555 and is, where appropriate, adapted to the Union entities;

(e) CERT-EU の長からの提案を基礎として，CERT-EU の年次作業計画を承認し，かつ，同計画の実装を監視し；

approve, on the basis of a proposal by the Head of CERT-EU, CERT-EU's annual work programme and monitor its implementation;

(f) CERT-EU の長からの提案を基礎として，CERT-EU のサービス目録及び同目録のアップデートを承認し；

approve, on the basis of a proposal by the Head of CERT-EU, CERT-EU's service catalogue and any updates thereof;

(g) CERT-EU の長からの提案を基礎として，人員配置を含め，CERT-EU の活動のための歳入と歳出の年次財務計画を承認し；

approve, on the basis of a proposal by the Head of CERT-EU, the annual financial planning of revenue and expenditure, including staffing, for CERT-EU activities;

(h) CERT-EU の長からの提案を基礎として，サービスレベル合意のための手配を承認し；

approve, on the basis of a proposal by the Head of CERT-EU, the arrangements for service level agreements;

(i) CERT-EU の長によって作成され，CERT-EU の活動及び CERT-EU の資金管理を包摂する年次報告書を審議しかつ承認し；

examine and approve the annual report drawn up by the Head of CERT-EU covering the activities of, and management of funds by, CERT-EU;

(j) CERT-EU の長からの提案を基礎として定められる CERT-EU のための重要業績評価指標（KPIs）を承認しかつ監視し；

approve and monitor key performance indicators (KPIs) for CERT-EU established on the basis of a proposal by the Head of CERT-EU;

(k) 第 18 条による CERT-EU とそれ以外の法主体との間の協力覚書，サービスレベル合意または契約を承認し；

approve cooperation arrangements, service level agreements or contracts between CERT-EU and other entities pursuant to Article 18;

(l) 第 14 条に従った CERT-EU の長からの提案を基礎とする運用指針及び勧告を採択し，並びに，CERT-EU に対し，運用指針もしくは勧告の提案または行動要求を発すること，取消すこともしくは修正することを指示し；

adopt guidelines and recommendations on the basis of a proposal by CERT-EU in accordance with Article 14 and instruct CERT-EU to issue, withdraw or modify a proposal for guidelines or recommendations, or a call for action;

(m) IICB の仕事を補助するための特別の職務をもつ技術上の諮問グループを設置し，同グループの付託条件を承認し，かつ，同グループそれぞれの議長を指名し；

establish technical advisory groups with specific tasks to assist the IICB's work, approve their terms of reference and designate their respective Chairs;

(n) サイバーセキュリティの成熟度評価書のような，この規則の下において欧州連合の法主体から提出される文書及び報告書を受領しかつ評価し；

receive and assess documents and reports submitted by the Union entities under this Regulation, such as cybersecurity maturity assessments;

(o) この規則の実装との関係におけるベストプラクティスと情報の交換を狙いとして，ENISA の支援を受け，欧州連合の法主体の地方サイバーセキュリティ吏員の非公式グループの設置を促進し；

facilitate the establishment of an informal group of local cybersecurity officers of Union entities, supported by ENISA, with the aim of exchanging best practices and information in relation to the implementation of this Regulation;

(p) CERT-EU から提供される識別されたサイバーセキュリティ上のリスク及び学習された教訓に関する情報を考慮に入れた上で，欧州連合の法主体の ICT 環境間の相互接続性の手配の適切性を監視し，かつ，可能な改善に関して助言し；

taking into account the information on the identified cybersecurity risks and lessons learnt provided by CERT-EU, monitor the adequacy of interconnectivity arrangements among the Union entities' ICT environments and advise on possible improvements;

(q) 欧州連合の法主体に影響を与える大きなインシデントの調整された取扱いを業務運営レベルで支援すること，並びに，とりわけ，大きなインシデントの影響と深刻度及びその影響を緩和する可能な方法に関し，適格な情報の定期的な交換に貢献することという観点から，サイバー危機管理計画を設け；

establish a cyber crisis management plan with a view to supporting, at an operational level, the coordinated management of major incidents affecting Union entities and to contributing to the regular exchange of relevant information, in particular with regard to the impacts and severity of, and the possible ways of mitigating the effects of, major incidents;

(r) 第 9 条第 2 項に示す個々の欧州連合の法主体のサイバー危機管理計画の採択を調整し；

coordinate the adoption of individual Union entities' cyber crisis management plans referred to in Article 9(2);

(s) 指令(EU) 2022/2555 の第 22 条に示す不可欠なサプライチェーンの欧州連合レベルで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た上で，実効的かつ比例的なサイバーセキュリティリスクマネジメント措置の採択において欧州連合の法主体を支援するため，第 8 条第 2 項第 1 副項(m)に示すサプライチェーンの防護と関連する勧告を採択する。

adopt recommendations relating to supply chain security referred to in Article 8(2), first subparagraph, point (m), taking into account the results of Union level coordinated security risk assessments of critical supply chains referred to in Article 22 of Directive (EU) 2022/2555 to support Union entities in adopting effective and proportionate cybersecurity risk-management measures.

第 12 条 遵守

Article 12 **Compliance**

1. IICB は，第 10 条第 2 項及び第 11 条により，この規則の実装並びに欧州連合の法主体によって採択された運用指針，勧告及び行動要求の実装を実効的に監視する。IICB は，，欧州連合の法主体に対し，その監視の目的のために必要となる情報または文書を要求し得る。本条の下における遵守措置を採択することの目的のために，関係する欧州連合の法主体が IICB 上で直接に代表されているときは，当該欧州連合の法主体は，投票の権利をもってはならない。

The IICB shall, pursuant to Article 10(2) and Article 11, effectively monitor the implementation of this Regulation and of adopted guidelines, recommendations and calls for action by the Union entities. The IICB may request information or documentation necessary for that purpose from the Union entities. For the purpose of adopting compliance measures under this Article, where the Union entity concerned is directly represented on the IICB, that Union entity shall not have voting rights.

2. この規則または IICB から発された運用指針，勧告及び行動要求を欧州連合の法主体が実効的に実装していないと IICB が判断するときは，関係する欧州連合の法主体の内部手続を妨げることなく，かつ，関係する欧州連合の法主体に対して当該法主体の見解を提出する機会を与えた後，IICB は，以下のことを行い得る：

Where the IICB finds that a Union entity has not effectively implemented this Regulation or guidelines, recommendations or calls for action issued pursuant thereto, it may, without prejudice to the internal procedures of the Union entity concerned, and after giving an opportunity to the Union entity concerned to present its observations:

(a) この規則の実装における観察された格差をもつ関係する欧州連合の法主体に対し，理由を付した意見を伝達し；

communicate a reasoned opinion to the Union entity concerned with observed gaps in the implementation of this Regulation;

(b) CERT-EU からの意見聴取を経た後，関係する欧州連合の法主体に対し，当該法主体の枠組み，サイバーセキュリティ上のリスクマネジメント措置，サイバーセキュリティ計画及び報告が指定された期間内にこの規則を遵守することを確保するための運用指針を提供し；

provide, after consulting CERT-EU, guidelines to the Union entity concerned to ensure that its Framework, cybersecurity risk-management measures, cybersecurity plan and reporting comply with this Regulation within a specified period;

(c) この規則によって関係する欧州連合の法主体によって採択された措置を修正することの勧告を含め，発見された欠点に対して指定された期間内に対処することの警告を発し；

issue a warning to address identified shortcomings within a specified period, including recommendations to amend measures adopted by the Union entity concerned pursuant to this Regulation;

(d) (c)によって発された警告の中で特定された欠点が指定された期間内に十分に対処されなかった場合，関係する欧州連合の法主体に対し，理由を付した通知を発し；

issue a reasoned notification to the Union entity concerned, in the event that shortcomings identified in a warning issued pursuant to point (c) were not sufficiently addressed within the specified period;

(e) 以下のものを発し：

issue:

(i) 監査が実行されることを求める勧告；または

a recommendation for an audit to be carried out; or

(ii) サードパーティの監査サービスによって監査が遂行されることの要求書；

a request that an audit be performed by a third-party audit service;

(f) それが適用可能なときは，会計検査院に対し，その任務の範囲内で，主張された不遵守を連絡し；

if applicable, inform the Court of Auditors, within the remit of its mandate, of the alleged non-compliance;

(g) 全ての構成国及び欧州連合の法主体が，関係する欧州連合の法主体に対するデータの流れの一時的な停止を実装することの勧告を発する。

issue a recommendation that all Member States and Union entities implement a temporary suspension of data flows to the Union entity concerned.

第 1 副項(c)の目的のために，サイバーセキュリティ上のリスクという観点から必要なときは，警告を知

る者は，しかるべく制限される。

For the purposes of the first subparagraph, point (c), the audience of a warning shall be restricted appropriately, where necessary in view of the cybersecurity risk.

第 1 副項によって発される警告及び勧告は，関係する欧州連合の法主体の最上位レベルの運営主体に対して向けられる。

Warnings and recommendations issued pursuant to the first subparagraph shall be directed to the highest level of management of the Union entity concerned.

3. IICB が第 2 項第 1 副項(a)ないし(g)の下にある措置を採択したときは，関係する欧州連合の法主体は，IICB によって特定された主張された欠点に対処するための措置及びとられた行動の詳細説明書を提供する。その欧州連合の法主体は，IICB の同意を得た合理的な期間内に，その詳細説明書を提出する。

Where the IICB has adopted measures under paragraph 2, first subparagraph, points (a) to (g), the Union entity concerned shall provide details of the measures and actions taken to address the alleged shortcomings identified by the IICB. The Union entity shall submit those details within a reasonable period to be agreed with the IICB.

4. 最上位レベルの運営主体を含め，欧州連合の官吏またはそれ以外の公務員の作為または不作為から直接に帰結する欧州連合の法主体によるこの規則の恒常的な違反行為が存在すると IICB が判断するときは，IICB は，関係する欧州連合の法主体が，職員規則の中で定められた規定及び手続並びにそれ以外の適用可能な規定及び手続に従い，懲戒の性質をもつ行動をとることを検討することを当該法主体に対して要求することを含め，適切な行動をとることを要求する。その目的のために，IICB は，関係する欧州連合の法主体に対し，必要な情報を送信する。

Where the IICB considers that there is persistent infringement of this Regulation by a Union entity resulting directly from actions or omissions of an official or other servant of the Union, including at the highest level of management, the IICB shall request that the Union entity concerned take appropriate action, including requesting it to consider taking action of a disciplinary nature, in accordance with the rules and procedures laid down in the Staff Regulations and any other applicable rules and procedures. To that end, the IICB shall transfer the necessary information to the Union entity concerned.

5. 欧州連合の法主体が，当該法主体が第 6 条第 1 項及び第 8 条第 1 項の中で定められた期限を遵守できない旨を通知するときは，IICB は，適正な根拠のある場合において，その欧州連合の法主体の規模を考慮に入れた上で，当該期限の延長を認め得る。

Where Union entities notify that they are unable to meet the deadlines set out in Article 6(1) and Article 8(1), the IICB may, in duly substantiated cases, taking into account the size of the Union entity, authorise the extension of those deadlines.

第 IV 章　CERT-EU
Chapter IV　CERT-EU

第 13 条　CERT-EU の任務及び職務
Article 13　CERT-EU mission and tasks

1. CERT-EU の任務は，欧州連合の法主体に対してサイバーセキュリティに関し助言すること，インシデントを防止し，検出し，取扱い，緩和し，それに対して対応し及びそれから復旧するために欧州連合の法主体を助けることによって，並びに，欧州連合の法主体のサイバーセキュリティ上の情報交換とインシデント対応調整のハブとして行動することによって，欧州連合の法主体の機密ではない ICT 環境の防護に貢献することにある。

   CERT-EU's mission shall be to contribute to the security of the unclassified ICT environment of Union entities by advising them on cybersecurity, by helping them to prevent, detect, handle, mitigate, respond to and recover from incidents and by acting as their cybersecurity information exchange and incident response coordination hub.

2. CERT-EU は，機密ではない ICT インフラ内のサイバーな脅威，脆弱性及びインシデントに関する情報を収集し，管理し，分析し，かつ，欧州連合の法主体と共有する。CERT-EU は，特化された運用上の補助を提供することによる場合またはその提供を調整することによる場合を含め，機関間レベル及び欧州連合の法主体レベルで，インシデントに対する対応を調整する。

   CERT-EU shall collect, manage, analyse and share information with the Union entities on cyber threats, vulnerabilities and incidents in unclassified ICT infrastructure. It shall coordinate responses to incidents at interinstitutional and Union entity level, including by providing or coordinating the provision of specialised operational assistance.

3. CERT-EU は，欧州連合の法主体を補助するため，以下のとおりの職務を遂行する：

   CERT-EU shall carry out the following tasks to assist the Union entities:

   (a) 第 14 条第 1 項の中で列挙された措置を介してまたは IICB から要求されたアドホックな報告を介して，この規則の実装について欧州連合の法主体を補助すること及びこの規則の実装の調整に貢献すること；

   support them with the implementation of this Regulation and contribute to the coordination of the implementation of this Regulation through the measures listed in Article 14(1) or through ad-hoc reports requested by the IICB;

   (b) CERT-EU のサービス目録の中で記述されたサイバーセキュリティ上のサービスのパッケージによって，欧州連合の法主体のための標準的な CSIRT サービス(ベースラインのサービス)を提示すること；

offer standard CSIRT services for Union entities by means of a package of cybersecurity services described in its service catalogue (baseline services);

(c) 第 17 条及び第 18 条の中で概要を示すサービスを支援するためのピア及びパートナーのネットワークを維持管理すること;

maintain a network of peers and partners to support the services as outlined in Articles 17 and 18;

(d) この規則の実装並びに運用指針，勧告及び行動要求の実装と関連する問題に対して，IICB の注意を向けさせること;

bring to the attention of the IICB any problems relating to the implementation of this Regulation and the implementation of guidelines, recommendations and calls for action;

(e) 第 2 項に示す情報を基礎として，ENISA と緊密に協力して，欧州連合のサイバーな状況認識に貢献すること;

on the basis of the information referred to in paragraph 2, contribute to the Union cyber situational awareness in close cooperation with ENISA;

(f) 大きなインシデントの取扱いを調整すること;

coordinate the management of major incidents;

(g) 指令(EU) 2022/2555 の第 12 条第 1 項による調整された脆弱性の開示の目的のために指定された調整官と均等な者として，欧州連合の法主体の側に立って行動すること;

act on the part of Union entities as the equivalent of the coordinator designated for the purposes of coordinated vulnerability disclosure pursuant to Article 12(1) of Directive (EU) 2022/2555;

(h) 欧州連合の法主体の要請を受けた後，当該欧州連合の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事前の非侵襲的なスキャニングを提供すること。

provide, upon the request of a Union entity, proactive non-intrusive scanning of publicly accessible network and information systems of that Union entity.

第 1 副項(e)に示す情報は，それが適用可能かつ適切なときは，かつ，適切な機密保持条件に服して，IICB，CSIRTs ネットワーク並びに欧州連合情報及び状況拠点（EU INTCEN）と共有される。

The information referred to in the first subparagraph, point (e), shall be shared with the IICB, the CSIRTs network and the

European Union Intelligence and Situation Centre (EU INTCEN), where applicable and appropriate, and subject to appropriate confidentiality conditions.

4. CERT-EU は，第 17 条または第 18 条にしかるべく従い，以下の諸分野を含め，欧州連合及びその構成国内の適格なサイバーセキュリティコミュニティと協力し得る：

CERT-EU may, in accordance with Article 17 or 18 as appropriate, cooperate with relevant cybersecurity communities within the Union and its Member States, including in the following areas:

(a) 欧州連合の法主体と関係する案件における技術レベルの対応準備，インシデント対応の調整，情報交換及び危機対応；

preparedness, incident coordination, information exchange and crisis response at the technical level on cases linked to Union entities;

(b) 相互補助に関するものを含め，CSIRTs ネットワークと関連する業務運営上の協力；

operational cooperation regarding the CSIRTs network, including with regard to mutual assistance;

(c) 状況認識を含め，サイバーな脅威の情報；

cyber threat intelligence, including situational awareness;

(d) CERT-EU のサイバーセキュリティ上の技術的な専門知識を要するトピック。

on any topic requiring CERT-EU's technical cybersecurity expertise.

5. CERT-EU の能力内において，CERT-EU は，規則(EU) 2019/881 に従った能力構築，運用上の協力及びサイバーな脅威の長期的な戦略分析に関し，ENISA との構造化された協力に従事する。CERT-EU は，Europol の欧州サイバー犯罪拠点と協力し及び情報を交換し得る。

Within its competence, CERT-EU shall engage in structured cooperation with ENISA on capacity building, operational cooperation and long-term strategic analyses of cyber threats in accordance with Regulation (EU) 2019/881. CERT-EU may cooperate and exchange information with Europol's European Cybercrime Centre.

6. CERT-EU は，CERT-EU のサービス目録の中に記述されていない以下のとおりのサービス（負担可能サービス）を提供し得る：

CERT-EU may provide the following services not described in its service catalogue (chargeable services):

(a) サービスレベル合意を基礎とし，かつ，利用可能な資源，とりわけ，広域ネットワーク監視に服して，高い深刻度のサイバーな脅威に対するファーストラインの 24 時間週 7 日間の監視を含め，第 3 項に示す ICT 環境以外の欧州連合の法主体の ICT 環境のサイバーセキュリティを支援するサービス；

services that support the cybersecurity of Union entities' ICT environment, other than those referred to in paragraph 3, on the basis of service level agreements and subject to available resources, in particular broad-spectrum network monitoring, including first-line 24/7 monitoring for high-severity cyber threats;

(b) 書面による合意を基礎として，かつ，IICB の事前の承認を受け，当該法主体の ICT 環境を防護するためのもの以外の欧州連合の法主体のサイバーセキュリティ上の業務運営またはプロジェクトを支援するサービス；

services that support cybersecurity operations or projects of Union entities, other than those to protect their ICT environment, on the basis of written agreements and with the prior approval of the IICB;

(c) 要請に応じて，潜在的な大きな影響をもつ脆弱性を検出するための，関係する欧州連合の法主体のネットワーク及び情報システムの事前スキャニング；

upon request, a proactive scanning of the network and information systems of the Union entity concerned to detect vulnerabilities with a potential significant impact;

(d) 書面による合意を基礎として，かつ，IICB の事前の承認を受け，例えば，欧州連合法の下において当該組織に対して職務または職責をもたせることによって，欧州連合の法主体と緊密に協力する欧州連合の法主体以外の組織のために，当該組織の ICT 環境の防護を支援するサービス。

services that support the security of their ICT environment to organisations other than the Union entities that cooperate closely with Union entities, for instance by having tasks or responsibilities conferred under Union law, on the basis of written agreements and with the prior approval of the IICB.

第 1 副項(d)に関し，CERT-EU は，例外ベースで，IICB の事前の承認を得て，欧州連合の法主体以外の法主体とのサービスレベル合意に入り得る。

With regard to the first subparagraph, point (d), CERT-EU may, on an exceptional basis, enter into service level agreements with entities other than the Union entities with the prior approval of the IICB.

7. ENISA と緊密に協力して申請可能なときは，CERT-EU は，欧州連合の法主体のサイバーセキュリティのレベルを試験するため，サイバーセキュリティ演習を組織し，または，サイバーセキュリティ演習に参加しもしくは既存の演習への参加を勧告し得る。

CERT-EU shall organise and may participate in cybersecurity exercises or recommend participation in existing exercises, where applicable in close cooperation with ENISA, to test the level of cybersecurity of the Union entities.

8. CERT-EU は，関係する欧州連合の法主体から，当該法主体それぞれの手続に従って，そのようにすることが明示で要求されるときは，EUCI を取扱うネットワーク及び情報システム内のインシデントに関し，欧州連合の法主体に対して補助を提供し得る。本項の下における CERT-EU からの補助の提供は，機密情報の保護と関係する適用可能な規定を妨げてはならない。

CERT-EU may provide assistance to Union entities regarding incidents in network and information systems handling EUCI where it is explicitly requested to do so by the Union entities concerned in accordance with their respective procedures. The provision of assistance by CERT-EU under this paragraph shall be without prejudice to applicable rules concerning the protection of classified information.

9. CERT-EU は，欧州連合の法主体に対し，CERT-EU のインシデントを取扱う手続及びプロセスに関して連絡する。

CERT-EU shall inform Union entities about its incident handling procedures and processes.

10. CERT-EUは，高いレベルの機密性及び信頼性をもって，適切な協力の仕組み及び報告の流れを介して，大きなインシデント及び当該インシデントが取扱われた態様に関する適格かつ匿名化された情報に寄与する。その情報は，第 10 条第 14 項に示す報告書の中に含められる。

CERT-EU shall contribute, with a high level of confidentiality and reliability, via the appropriate cooperation mechanisms and reporting lines, relevant and anonymised information about major incidents and the manner in which they were handled. That information shall be included in the report referred to in Article 10(14).

11. CERT-EU 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際，規則(EU) 2018/1725 の下における監督機関としての EDPS の職務権限及び職務を妨げることなく，EDPS と協力して，関係する欧州連合の法主体を支援する。

CERT-EU shall, in cooperation with the EDPS, support the Union entities concerned when addressing incidents resulting in personal data breaches, without prejudice to the competence and tasks of the EDPS as a supervisory authority under Regulation (EU) 2018/1725.

12. CERT-EU は，欧州連合の法主体の政策決定官署から明示で要求されるときは，適格な政策上の事項に関し，技術上の助言または入力を提供し得る。

CERT-EU may, if expressly requested by Union entities' policy departments, provide technical advice or input on relevant policy matters.

第 14 条 運用指針，勧告及び行動要求

Article 14 **Guidelines, recommendations and calls for action**

1. CERT-EU は，以下のものを発することによって，この規則の実装を支援する：

CERT-EU shall support the implementation of this Regulation by issuing:

(a) 定められた時間枠内に欧州連合の法主体がとることを促される緊急防護措置を記述している行動要求；

calls for action describing urgent security measures that Union entities are urged to take within a set timeframe;

(b) 欧州連合の法主体の全部またはサブセットを名宛人とする運用指針に関する IICB に対する提案；

proposals to the IICB for guidelines addressed to all or a subset of the Union entities;

(c) 個々の欧州連合の法主体を名宛人とする勧告に関する IICB に対する提案。

proposals to the IICB for recommendations addressed to individual Union entities.

第 1 副項(a)に関し，関係する欧州連合の法主体は，行動要求の受領後不適正な遅滞なく，CERT-EU に対し，緊急防護措置がどのように適用されたかを連絡する。

With regard to the first subparagraph, point (a), the Union entity concerned shall, without undue delay after receiving the call for action, inform CERT-EU of how the urgent security measures were applied.

2. 運用指針及び勧告は，以下のものを含め得る：

Guidelines and recommendations may include:

(a) 欧州連合の法主体全体にわたる継続的なサイバーセキュリティ上の向上を支援する上での参考として奉仕し，かつ，法主体のサイバーセキュリティポスチャーを考慮に入れたサイバーセキュリティ上の部門及び措置の優先順序付けを容易にする，対応する規模及び KPIs を含め，欧州連合の法主体のサイバーセキュリティの成熟度を評価するための共通の手法とモデル，

common methodologies and a model for assessing the cybersecurity maturity of the Union entities, including the corresponding scales or KPIs, serving as reference in support of continuous cybersecurity improvement across the Union entities and facilitating the prioritisation of cybersecurity domains and measures taking into account entities' cybersecurity posture;

(b) サイバーセキュリティ上のリスクマネジメントのための手配またはそのリスクマネジメントの改善及びサイバーセキュリティ上のリスクマネジメント措置；

arrangements for or improvements to cybersecurity risk management and the cybersecurity risk-management measures;

(c) サイバーセキュリティの成熟度評価及びサイバーセキュリティ計画の手配；

arrangements for cybersecurity maturity assessments and cybersecurity plans;

(d) 必要に応じて，相互運用性の達成を狙いとする共通の技術，アーキテクチャ，オープンソース及び関連するベストプラクティスの利用，並びに，サプライチェーンの防護に向けた調整されたアプローチを含め，共通の技術標準の利用；

where appropriate, the use of common technology, architecture, open source and associated best practices with the aim of achieving interoperability and common standards, including a coordinated approach to supply chain security;

(e) 必要に応じて，サードパーティの供給者からの適格なサイバーセキュリティ上のサービス及び製品の購入のための共通の調達手段の利用を促進するための情報；

where appropriate, information to facilitate the use of common procurement instruments for the purchasing of relevant cybersecurity services and products from third-party suppliers;

(f) 第 20 条による情報共有の手立て。

information-sharing arrangements pursuant to Article 20.

第 15 条 CERT-EU の長

Article 15 **Head of CERT-EU**

1. 欧州委員会は，IICB の構成員の 3 分の 2 の多数による承認を獲得した後，CERT-EU の長を任命する。IICB は，とりわけ，その職との関係における欠員通知の作成，申込みの審査及び選考委員会の任命に関し，任命手続の全ての段階において意見聴取を受ける。その名簿の中から CERT-EU の長が選考される最終候補者名簿を含め，選考手続は，提出された申込みを考慮に入れた上で，各ジェンダーの公正な代表比率を確保する。

The Commission, after obtaining the approval of a majority of two thirds of the members of the IICB, shall appoint the Head of CERT-EU. The IICB shall be consulted at all stages of the appointment procedure, in particular with regard to

drafting vacancy notices, examining applications and appointing selection boards in relation to the post. The selection procedure, including the final shortlist of candidates from which the Head of CERT-EU is to be appointed, shall ensure fair representation of each gender, taking into account the applications submitted.

2. CERT-EU の長は，CERT-EU の適正な稼働に関する職責を負い，かつ，彼または彼女の役割の範囲内及び IICB の指示の下において行動する。CERT-EU の長は，IICB の議長に対して定期的に報告し，かつ，IICB の要請を受けた後，IICB に対し，アドホックな報告書を提出する。

The Head of CERT-EU shall be responsible for the proper functioning of CERT-EU and shall act within the remit of his or her role and under the direction of the IICB. The Head of CERT-EU shall report regularly to the Chair of the IICB and shall submit ad-hoc reports to the IICB upon its request.

3. CERT-EU の長は，欧州議会及び理事会の規則(EU, Euratom) 2018/1046[9]の第 74 条第 9 項に従って作成される監督結果を含む財務及び運営管理の情報を包摂する年次活動報告書を作成する際における委任によって，職責上の承認権限のある官吏を補助し，かつ，CERT-EU の長に対して再委任された権限との関係における諸措置の実装に関する委任によって，権限のある官吏に対し，定期的に報告する。

The Head of CERT-EU shall assist the responsible authorising officer by delegation in drafting the annual activity report containing financial and management information, including the results of controls, drawn up in accordance with Article 74(9) of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council[9], and shall report regularly to the authorising officer by delegation on the implementation of measures in respect of which powers have been sub-delegated to the Head of CERT-EU.

4. CERT-EU の長は，年次で，第 11 条に従い IICB によって承認される，CERT-EU の活動のための行政上の歳入及び歳出の財務計画，年次作業計画案，CERT-EU のサービス目録案，サービス目録の改訂案，サービスレベル合意のための覚書案及び CERT-EU のための KPIs 案を作成する。CERT-EU のサービス目録の中にあるサービスのリストを改訂する際，CERT-EU の長は，CERT-EU に対して割当てられた資源を考慮に入れる。

The Head of CERT-EU shall draw up, on an annual basis, a financial planning of administrative revenue and expenditure for its activities, a proposed annual work programme, a proposed service catalogue for CERT-EU, proposed revisions of

---

[9] 欧州連合の一般予算に対して適用可能な財務規則に関する，規則(EU) No 1296/2013，規則(EU) No 1301/2013，規則 (EU) No 1303/2013，規則(EU) No 1304/2013，規則(EU) No 1309/2013，規則(EU) No 1316/2013，規則(EU) No 223/2014，規則(EU) No 283/2014 及び決定 No 541/2014/EU を改正し，並びに，規則 (EU, Euratom) No 966/2012 を廃止する欧州議会及び理事会の 2018 年 7 月 18 日の規則(EU, Euratom) 2018/1046 (OJ L 193, 30.7.2018, p. 1).

Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).

the service catalogue, proposed arrangements for service level agreements and proposed KPIs for CERT-EU, to be approved by the IICB in accordance with Article 11. When revising the list of services in CERT-EU's service catalogue, the Head of CERT-EU shall take into account the resources allocated to CERT-EU.

5. CERT-EU の長は，少なくとも年次で，IICB 及び IICB の議長に対し，第 11 条に示す報告書を含め，予算の実装，締結されたサービスレベル合意及び書面による合意，相手方及びパートナーとの協力関係並びに職員によって実施された任務に関する報告書を含め，該当する期間内における CERT-EU の活動及び遂行能力に関する報告書を提出する。それらの報告書は，次年度の作業計画，人員配置を含め，歳入と歳出の財務計画，CERT-EU のサービス目録の計画中のアップデート，及び，そのようなアップデートが資金及び人的資源と関連してもち得る予想される影響の評価を含める。

The Head of CERT-EU shall submit reports at least annually to the IICB and the Chair of the IICB on the activities and performance of CERT-EU during the reference period, including on the implementation of the budget, service level agreements and written agreements entered into, cooperation with counterparts and partners, and missions undertaken by staff, including the reports referred to in Article 11. Those reports shall include a work programme for the following period, financial planning of revenue and expenditure, including staffing, planned updates of CERT-EU's service catalogue and an assessment of the expected impact that such updates may have with regard to financial and human resources.

第 16 条 財務及び人員の事項

Article 16 **Financial and staffing matters**

1. CERT-EUは，欧州連合の全ての法主体のための自律的な機関間サービスプロバイダとしての CERT-EU の地位を維持しつつ，欧州委員会の行政上，財務管理上及び監査支援上の構造から受益するため，欧州委員会の事務総局の行政機構の中に統合される。欧州委員会は，IICB に対し，CERT-EU の行政組織上の位置づけ及びその変更を連絡する。欧州委員会は，適切な行動がとられ得るようにするため，定期的に，かつ，いかなる場合においても TFEU の第 312 条による多年度財政枠組みの確定の前に，CERT-EU と関連する行政上の手配を見直す。その見直しは，欧州連合の事務局として CERT-EU を設置することの可否を含める。

CERT-EU shall be integrated into the administrative structure of a directorate-general of the Commission in order to benefit from the Commission's administrative, financial management and accounting support structures, while maintaining its status as an autonomous interinstitutional service provider for all Union entities. The Commission shall inform the IICB of the administrative location of CERT-EU and any changes thereto. The Commission shall review the administrative arrangements related to CERT-EU on a regular basis and in any event before the establishment of any multiannual financial framework pursuant to Article 312 TFEU, in order to allow for appropriate action to be taken. The review shall include the possibility of establishing CERT-EU as a Union office.

2. 行政上及び財務上の手続の適用に関し，CERT-EU の長は，欧州委員会の権限の下においてかつ

IICB の監督の下において行動する。

For the application of administrative and financial procedures, the Head of CERT-EU shall act under the authority of the Commission and under the supervision of the IICB.

3. 第 13 条第 3 項, 第 4 項, 第 5 項及び第 7 項並びに第 14 条第 1 項によって, CERT-EU から, 欧州行政機関専用の多年度財政枠組みの費目において資金供与を受ける欧州連合の法主体に対して提供されるサービスを含め, CERT-EU の職務及び活動は, 欧州委員会の予算とは区別された予算線によって資金供与を受ける。CERT-EU のために予定される地位は, 欧州委員会の設置計画の脚注の中で詳述される。

CERT-EU's tasks and activities, including services provided by CERT-EU pursuant to Article 13(3), (4), (5) and (7) and Article 14(1) to Union entities financed from the heading of the multiannual financial framework dedicated to European public administration, shall be funded by means of a distinct budget line of the Commission budget. The posts earmarked for CERT-EU shall be detailed in a footnote to the Commission establishment plan.

4. 本条の第 3 項に示す法主体以外の欧州連合の法主体は, 同項によって CERT-EU から提供されるサービスを賄うため, CERT-EU に対する年次資金拠出を行う。その拠出は, IICB から与えられる指針及びサービスレベル合意の中で欧州連合の各法主体と CERT-EU との間で合意される指針を基礎とする。その拠出は, 提供されるサービスの総費用中の公正かつ比例的な分担を反映するものとする。その拠出は, 規則(EU, Euratom) 2018/1046 の第 21 条第 3 項(c)の中で定められた内部割当て歳入として, 本条の第 3 項に示す区分された予算線によって受領される。

Union entities other than those referred to in paragraph 3 of this Article shall make an annual financial contribution to CERT-EU to cover the services provided by CERT-EU pursuant to that paragraph. The contributions shall be based on orientations given by the IICB and agreed between each Union entity and CERT-EU in service level agreements. The contributions shall represent a fair and proportionate share of the total costs of services provided. They shall be received by the distinct budget line referred to in paragraph 3 of this Article, as internal assigned revenue, as provided for in Article 21(3), point (c), of Regulation (EU, Euratom) 2018/1046.

5. 第 13 条第 6 項の中で定められたサービスの費用は, CERT-EU のサービスを受ける欧州連合の法主体から回収される。その歳入は, 費用を支える予算線に割当てられる。

The costs of the services provided for in Article 13(6) shall be recovered from the Union entities receiving CERT-EU services. The revenues shall be assigned to the budget lines supporting the costs.

第 17 条 CERT-EU と構成国の相手方との間の協力

Article 17 **Cooperation of CERT-EU with Member State counterparts**

1. CERT-EU は，不適切な遅滞なく，インシデント，サイバーな脅威，脆弱性，ニアミス，可能な対抗措置及びベストプラクティスに関し，並びに，欧州連合の法主体の ICT 環境の保護を向上させることにとって適格な全ての事項に関し，指令(EU) 2022/2555 の第 15 条によって設置された CSIRTs ネットワークによって行われる場合を含め，構成国の相手方との間で，とりわけ，指令(EU) 2022/2555 の第 10 条によって指定されまたは設置された CSIRTs との間で，または，それが適用可能なときは，同指令の第 8 条によって指定されまたは設置された職務権限のある当局及び単一連絡部局との間で協力し及び情報交換する。大規模なサイバーセキュリティインシデント及び危機の調整された取扱いに関し，CERT-EU は，指令(EU) 2022/2555 の第 16 条によって設置された EU-CyCLONe 内において，欧州委員会を支援する。

   CERT-EU shall, without undue delay, cooperate and exchange information with Member State counterparts, in particular the CSIRTs designated or established pursuant to Article 10 of Directive (EU) 2022/2555, or, where applicable, the competent authorities and single points of contact designated or established pursuant to Article 8 of that Directive, with regard to incidents, cyber threats, vulnerabilities, near misses, possible countermeasures as well as best practices and on all matters relevant for improving the protection of the ICT environments of Union entities, including by means of the CSIRTs network established pursuant to Article 15 of Directive (EU) 2022/2555. CERT-EU shall support the Commission in EU-CyCLONe established pursuant to Article 16 of Directive (EU) 2022/2555 on the coordinated management of large-scale cybersecurity incidents and crises.

2. CERT-EU が構成国の領土内で発生している大きなインシデントに気づいたときは，CERT-EU は，第 1 項に従い，遅滞なく，当該構成国内の適格な相手方に対し，通知する。

   Where CERT-EU becomes aware of a significant incident occurring within the territory of a Member State, it shall, without delay, notify any relevant counterpart in that Member State, in accordance with paragraph 1.

3. 適用可能な欧州連合のデータ保護法に従って個人データが保護されることを条件として，影響を受けた欧州連合の法主体の承認を受けることなく，類似のサイバーな脅威またはインシデントの検出を容易にするためまたはインシデントの分析に貢献するため，CERT-EU は，不適切な遅滞なく，構成国の相手方との間で適格なインシデント特化情報を交換する。CERT-EU は，以下のいずれかの場合に限り，当該インシデントの標的の識別名を明らかにするインシデント特化情報を交換する：

   Provided that personal data are protected in accordance with applicable Union data protection law, CERT-EU shall, without undue delay, exchange relevant incident-specific information with Member State counterparts to facilitate detection of similar cyber threats or incidents, or to contribute to the analysis of an incident, without the authorisation of the Union entity affected. CERT-EU shall exchange incident-specific information which reveals the identity of the target of the incident only in the event of one of the following:

(a) 影響を受けた欧州連合の法主体が同意している場合；

the Union entity affected consents;

(b) 影響を受けた欧州連合の法主体が(a)の中で定められた同意をしていないが，その影響を受けた欧州連合の法主体の識別名を開示することが，他の場所にあるインシデントが避けられまたは緩和されるような蓋然性を増加させ得る場合；

the Union entity affected does not consent as provided for in point (a) but the disclosure of the identity of the Union entity affected would increase the probability that incidents elsewhere would be avoided or mitigated;

(c) 影響を受けた欧州連合の法主体が，その法主体が影響を受けたということを既に公表している場合。

the Union entity affected has already made public that it was affected.

第 1 副項(b)によって当該インシデントの標的の識別名を明らかにするインシデント特化情報を交換することの決定は，CERT-EU の長の承認を受ける。そのような決定を発出する前に，CERT-EU は，その法主体の識別名を開示することが他の場所にあるインシデントを避けることまたは緩和することをどのように助け得るのかを明確に説明する書面により，当該影響を受けた欧州連合の法主体と連絡をとる。CERT-EU の長は，その説明書を提供し，かつ，当該欧州連合の法主体に対し，定められた時間枠内に当該法主体が同意するか否かを述べることを明示で要求する。CERT-EU の長は，当該欧州連合の法主体に対し，提供される説明書に照らし，同意がない場合であってもその情報を開示する権利を彼または彼女が保持していることも連絡する。影響を受けた欧州連合の法主体は，その情報が開示される前に，連絡を受ける。

Decisions to exchange incident-specific information which reveals the identity of the target of the incident pursuant to the first subparagraph, point (b), shall be endorsed by the Head of CERT-EU. Prior to issuing such a decision, CERT-EU shall contact the Union entity affected in writing, explaining clearly how the disclosure of its identity would help to avoid or mitigate incidents elsewhere. The Head of CERT-EU shall provide the explanation and explicitly request the Union entity to state whether it consents within a set timeframe. The Head of CERT-EU shall also inform the Union entity that, in light of the explanation provided, he or she reserves the right to disclose the information even in the absence of consent. The Union entity affected shall be informed before the information is disclosed.

第 18 条 CERT-EU と他の相手方との間の協力

Article 18 **Cooperation of CERT-EU with other counterparts**

1. CERT-EUは，第 17 条に示す相手方以外の欧州連合内の相手方であって，特定の産業部門の相手方を含め，技法，戦略，手順及びベストプラクティスのようなツール及び手法に関する並びにサイバ

ーな脅威及び脆弱性に関する欧州連合のサイバーセキュリティ上の要件に服する者との間で協力し得る。そのような相手方との間の全ての協力に関し，CERT-EUは，ケースバイケースで，IICBからの事前の承認を求める。CERT-EU がそのような相手方との間の協力を確立するときは，CERT-EU は，当該相手方が所在する構成国内の第 17 条第 1 項に示す適格な構成国の相手方に対し，連絡する。それが適用可能でありかつ適切なときは，サイバーセキュリティ，データ保護及び情報の取扱いと関連するものを含め，そのような協力及びその条件は，契約または行政上の協定のような個別の機密保持の手配の中で定められる。機密保持の手立ては，IICB による事前の承認を要しないが，IICB の議長は，連絡を受ける。欧州連合の法主体またはそれ以外の当事者の利益においてサイバーセキュリティ上の情報を交換すべき緊急かつ差し迫った必要性がある場合においては，CERT-EU は，CERT-EU が当該法主体との間において機密保持の手立てを設けていない場合であっても，そのような緊急かつ差し迫った必要性を補助するために，当該法主体の特別の能力，実現能力及び専門知識が正当に要求され得る法主体との間で，そのようにし得る。そのような場合においては，CERT-EU は，IICB の議長に対して直ちに連絡し，かつ，定期的な報告または会合によって，IICB に対して報告する。

CERT-EU may cooperate with counterparts in the Union other than those referred to in Article 17 which are subject to Union cybersecurity requirements, including industry sector-specific counterparts, on tools and methods, such as techniques, tactics, procedures and best practices, and on cyber threats and vulnerabilities. For all cooperation with such counterparts, CERT-EU shall seek prior approval from the IICB on a case-by-case basis. Where CERT-EU establishes cooperation with such counterparts, it shall inform any relevant Member State counterparts referred to in Article 17(1), in the Member State in which the counterpart is located. Where applicable and appropriate, such cooperation and the conditions thereof, including regarding cybersecurity, data protection and information handling, shall be established in specific confidentiality arrangements such as contracts or administrative arrangements. The confidentiality arrangements shall not require prior approval by the IICB, but the Chair of the IICB shall be informed. In the case of an urgent and imminent need to exchange cybersecurity information in the interests of Union entities or another party, CERT-EU may do so with an entity whose specific competence, capacity and expertise are justifiably required to assist with such an urgent and imminent need, even if CERT-EU does not have a confidentiality arrangement in place with that entity. In such cases, CERT-EU shall immediately inform the Chair of the IICB, and shall report to the IICB by means of regular reports or meetings.

2. CERT-EUは，一般的または個別のサイバーな脅威，ニアミス，脆弱性及び可能な対抗措置に関する情報を収集するため，特定の産業部門の法主体，国際組織，欧州連合の国内法主体ではない法主体または個人の専門家を含め，商業上の法主体のようなパートナーとの間で協力し得る。そのようなパートナーとの間におけるより広い協力のためには，CERT-EU は，ケースバイケースで，IICB からの事前の承認を求める。

CERT-EU may cooperate with partners, such as commercial entities, including industry sector-specific entities, international organisations, non-Union national entities or individual experts, to gather information on general and specific cyber threats, near misses, vulnerabilities and possible countermeasures. For wider cooperation with such partners, CERT-EU shall seek prior approval from the IICB on a case-by-case basis.

3. CERT-EU は，インシデントによる影響を受けた欧州連合の法主体の同意を得て，かつ，適格な相手方またはパートナーとの間で非開示の合意もしくは契約が置かれることを条件として，当該インシデントの分析に貢献することという目的のためにのみ，第 1 項及び第 2 項に示す相手方またはパートナーに対し特定のインシデントと関連する情報を提供し得る。

CERT-EU may, with the consent of the Union entity affected by an incident and provided that a non-disclosure arrangement or contract is in place with the relevant counterpart or partner, provide information related to the specific incident to counterparts or partners referred to in paragraphs 1 and 2 solely for the purpose of contributing to its analysis.

第 V 章 協力及び報告義務
Chapter V Cooperation and Reporting Obligations

第 19 条 情報の取扱い
Article 19 **Information handling**

1. 欧州連合の法主体及び CERT-EU は，TFEU の第 339 条に従った職業上の守秘義務またはそれと均等な適用可能な枠組みを尊重する。

   Union entities and CERT-EU shall respect the obligation of professional secrecy in accordance with Article 339 TFEU or equivalent applicable frameworks.

2. CERT-EU によって保有されている文書への公衆のアクセスを求める要求に関しては，欧州議会及び理事会の規則(EC) No 1049/2001[10]の下における要求が欧州連合の法主体の文書または構成国の文書と関係する限り，欧州連合の他の法主体から意見聴取しまたはそれが適格なときは構成国から意見聴取すべき義務を含め，同規則が適用される。

   Regulation (EC) No 1049/2001 of the European Parliament and of the Council[10] shall apply with regard to requests for public access to documents held by CERT-EU, including the obligation under that Regulation to consult other Union entities or, where relevant, Member States, whenever a request concerns their documents.

3. 欧州連合の法主体及び CERT-EU による情報の取扱いは，情報の防護に関する適用可能な規定を遵守する。

   The handling of information by Union entities and CERT-EU shall comply with the applicable rules on information security.

第 20 条 サイバーセキュリティ上の情報共有の手立て
Article 20 **Cybersecurity information-sharing arrangements**

1. 欧州連合の法主体は，任意に，CERT-EU に対し，当該法主体に対して影響を与えるインシデント，サイバーな脅威，ニアミス及び脆弱性に関する情報を通知し及びその情報を提供し得る。CERT-EU は，欧州連合の法主体との間の情報共有を促進することという目的のために利用可能な高いレベルの追跡可能性，機密性及び信頼性をもつ効率的な通信手段を確保する。通知を処理する際，

---

[10] 欧州議会，理事会及び欧州委員会の文書に対する公衆のアクセスに関する欧州議会及び理事会の 2001 年 5 月 30 日の規則(EC) No 1049/2001 (OJ L 145, 31.5.2001, p. 43).
Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

CERT-EU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。第12条を妨げることなく，任意の通知は，報告元である欧州連合の法主体に対し，もし当該法主体がその通知を提出しなかったとすれば当該法主体が服することがなかったような付加的な義務を課す結果となってはならない。

Union entities may, on a voluntary basis, notify CERT-EU of, and provide it with information on, incidents, cyber threats, near misses and vulnerabilities that affect them. CERT-EU shall ensure that efficient means of communication, with a high level of traceability, confidentiality and reliability, are available for the purpose of facilitating information sharing with the Union entities. When processing notifications, CERT-EU may prioritise the processing of mandatory notifications over voluntary notifications. Without prejudice to Article 12, voluntary notification shall not result in the imposition of any additional obligations upon the reporting Union entity to which it would not have been subject had it not submitted the notification.

2. 第13条によって与えられたその任務及び職務を遂行するため，CERT-EUは，欧州連合の法主体に対し，サイバーな脅威，ニアミス，脆弱性，侵害の兆候，サイバーセキュリティ警報及びインシデント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，欧州連合の法主体それぞれのICTシステムの資産目録からの情報をCERT-EUに対して提供することを要求し得る。要求先である欧州連合の法主体は，不適切な遅滞なく，要求された情報及びその情報の後のアップデートを送信する。

To perform its mission and tasks conferred pursuant to Article 13, CERT-EU may request Union entities to provide it with information from their respective ICT system inventories, including information relating to cyber threats, near misses, vulnerabilities, indicators of compromise, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect incidents. The requested Union entity shall transmit the requested information, and any subsequent updates thereto, without undue delay.

3. CERT-EUは，欧州連合の法主体との間で，当該影響を受けた欧州連合の法主体が同意を与えることを条件として，当該インシデントによって影響を受けた欧州連合の法主体の識別名を明らかにするインシデント特化情報を交換し得る。欧州連合の法主体がその法主体の同意を撤回するときは，当該法主体は，CERT-EUに対し，当該決定を正当化する理由を提供する。

CERT-EU may exchange incident-specific information with Union entities which reveals the identity of the Union entity affected by the incident, provided that the Union entity affected consents. Where a Union entity withholds its consent, it shall provide CERT-EU with reasons substantiating that decision.

4. 欧州連合の法主体は，要請に応じて，欧州議会及び理事会との間で，サイバーセキュリティ計画の完成に関する情報を共有する。

Union entities shall, upon request, share information with the European Parliament and the Council on the completion of cybersecurity plans.

5. IICB または CERT-EU は，適用可能なときは，要請に応じて，欧州議会及び理事会との間で，運用指針，勧告及び行動要求を共有する。

The IICB or CERT-EU, as applicable, shall, upon request, share guidelines, recommendations and calls for action with the European Parliament and the Council.

6. 本条の中で定められた共有義務は、以下の情報に対しては拡張してはならない：

The sharing obligations laid down in this Article shall not extend to:

(a) EUCI；

EUCI;

(b) 当該情報の CERT-EU との間における共有が明示で認められている場合を除き，視認可能なマークによって，当該情報を更に配布することが禁止されている情報。

information the further distribution of which has been excluded by means of a visible marking, unless the sharing thereof with CERT-EU has been explicitly allowed.

第 21 条 報告義務

Article 21 **Reporting obligations**

1. 以下の場合においては，インシデントは，大きいと判断される：

An incident shall be considered to be significant if:

(a) そのインシデントが，関係する欧州連合の法主体の稼動に対する業務運営上の重大な支障または関係する欧州連合の法主体に対する金銭的な損失を生じさせた場合または生じさせ得る場合；

it has caused or is capable of causing severe operational disruption to the functioning of, or financial loss to, the Union entity concerned;

(b) そのインシデントが，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。

it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

2. 欧州連合の法主体は，CERT-EU に対し，以下のとおり提出する:

Union entities shall submit to CERT-EU:

(a) 不適切な遅滞なく，かつ，いかなる場合においても大きなインシデントに気づいてから 24 時間以内に，それが適用可能なときは，その大きなインシデントが違法行為もしくは悪意ある行為によって発生させられつつあると疑われることまたは法主体を越える影響もしくは国境を越える影響をもち得ることを示す早期警戒;

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 that the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-entity or a cross-border impact;

(b) 不適切な遅滞なく，かつ，いかなる場合においても大きなインシデントに気づいてから 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するインシデント通知，並びに，そのインシデントの深刻度と影響，及び，それが利用可能なときは，侵害の兆候を含め，大きなインシデントの当初評価を示すインシデント通知;

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) CERT-EU の要求に応じて，適格な事態の進展に関する中間報告;

upon the request of CERT-EU, an intermediate report on relevant status updates;

(d) 以下の事項を含め，(b)の下におけるインシデント通知の提出後 1 か月以内に，最終報告:

a final report not later than one month after the submission of the incident notification under point (b), including the following:

(i) 深刻度及び影響を含め，インシデントの詳細な記述;

a detailed description of the incident, including its severity and impact;

(ii) そのインシデントの引金となった可能性のある脅威または主たる要因のタイプ;

the type of threat or root cause that is likely to have triggered the incident;

(iii) 適用された及び進行中の緩和措置；

applied and ongoing mitigation measures;

(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または法主体を越える影響；

where applicable, the cross-border or cross-entity impact of the incident;

(e) (d)に示す最終報告の提出の時点ではインシデントが進行中の場合においては，当該時点における進捗状況報告書及びそのインシデントの当該法主体の取扱いから 1 か月以内に最終報告。

in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), a progress report at that time and a final report within one month of their handling of the incident.

3. 欧州連合の法主体は，不適切な遅滞なく，かつ，いかなる場合においても大きなインシデントに気づいてから 24 時間以内に，大きなインシデントが発生した場所である構成国内の第 17 条第 1 項に示す適格な構成国の相手方に対し，連絡する。

A Union entity shall, without undue delay and in any event within 24 hours of becoming aware of a significant incident, inform any relevant Member State counterparts referred to in Article 17(1) in the Member State where it is located that a significant incident has occurred.

4. 欧州連合の法主体は，就中，大きなインシデント後の法主体を越える影響，法主体をホストしている構成国に対す影響または国境を越える影響を CERT-EU が判定できるようにする情報を通知する。第 12 条を妨げることなく，通知行為そのものは，欧州連合の法主体を加重された法的責任に服させてはならない。

The Union entities shall notify, inter alia, any information enabling CERT-EU to determine any cross-entity impact, impact on the hosting Member State or cross-border impact following a significant incident. Without prejudice to Article 12, the mere act of notification shall not subject the Union entity to increased liability.

5. それが適用可能なときは，欧州連合の法主体は，不適切な遅滞なく，影響を受けたネットワーク及び情報システムのユーザまたはそれ以外の ICT 環境のコンポーネントのユーザであって，大きなインシデントまたは大きなサイバーな脅威によって潜在的に影響を受けており，かつ，必要に応じて，緩和の方策をとることを要する者に対し，当該インシデントまたは当該脅威に対する対応において当該ユーザがとり得る方策または解消策を伝達する。必要に応じて，欧州連合の法主体は，当該ユーザに対し，その大きなサイバーな脅威それ自体を連絡する。

Where applicable, Union entities shall communicate, without undue delay, to the users of the network and information

systems affected, or of other components of the ICT environment, that are potentially affected by a significant incident or a significant cyber threat, and, where appropriate, need to take mitigating measures, any measures or remedies that they can take in response to that incident or that threat. Where appropriate, Union entities shall inform those users of the significant cyber threat itself.

6. 大きなインシデントまたは大きなサイバーな脅威が，ネットワーク及び情報システムに対して影響を与え，または，欧州連合の法主体の ICT 環境のコンポーネントであって，別の欧州連合の法主体の ICT 環境と接続されていることが知られているものに対して影響を与えるときは，CERT-EU は，適格なサイバーセキュリティ警報を発する。

Where a significant incident or significant cyber threat affects a network and information system, or a component of a Union entity's ICT environment that is knowingly connected with another Union entity's ICT environment, CERT-EU shall issue a relevant cybersecurity alert.

7. 欧州連合の法主体は，CERT-EU の要請に応じて，不適切な遅滞なく，CERT-EU に対し，当該法主体それぞれのインシデントに含まれている電子機器の利用によってつくられたデジタル情報を提供する。CERT-EU は，状況認識及びインシデント対応のために CERT-EU が必要とする情報のタイプのより詳細な情報を提供し得る。

The Union entities, upon the request of CERT-EU, shall, without undue delay, provide CERT-EU with digital information created by the use of electronic devices involved in their respective incidents. CERT-EU may provide further details of the types of information that it requires for situational awareness and incident response.

8. CERT-EU は，IICB，ENISA，EU INTCEN 及び CSIRTs ネットワークに対し，3 か月毎に，第 20 条による大きなインシデント，インシデント，サイバーな脅威，ニアミス及び脆弱性並びに本条第 2 項によって通知された大きなインシデントに関する匿名化されかつ集約化されたデータを含む要旨報告書を提出する。その要旨報告書は，指令(EU) 2022/2555 の第 18 条によって採択される欧州連合におけるサイバーセキュリティの状態に関する隔年報告書への入力を組成する。

CERT-EU shall submit to the IICB, ENISA, the EU INTCEN and the CSIRTs network, every three months, a summary report including anonymised and aggregated data on significant incidents, incidents, cyber threats, near misses and vulnerabilities pursuant to Article 20 and significant incidents notified pursuant to paragraph 2 of this Article. The summary report shall constitute an input to the biennial report on the state of cybersecurity in the Union adopted pursuant to Article 18 of Directive (EU) 2022/2555.

9. 2024 年 7 月 8 日までに，IICB は，本条による報告のための手立て並びにそのための書式及び内容の細目を別途定める運用指針または勧告を発する。そのような運用指針または勧告を準備する際，IICB は，指令(EU) 2022/2555 の第 23 条第 11 項によって採択され，情報のタイプ，書式及び通知手続の細目を定めている実装行為を考慮に入れる。CERT-EU は，欧州連合の法主体による事前の検出，インシデント対応または緩和措置を実現可能にするための適切な技術上の詳細情報を配布する。

By 8 July 2024, the IICB shall issue guidelines or recommendations further specifying the arrangements for, and format and content of, the reporting pursuant to this Article. When preparing such guidelines or recommendations, the IICB shall take into account any implementing acts adopted pursuant to Article 23(11) of Directive (EU) 2022/2555 specifying the type of information, the format and the procedure of notifications. CERT-EU shall disseminate the appropriate technical details to enable proactive detection, incident response or mitigating measures by Union entities.

10. 本条の中で定められた報告義務は、以下の情報に対しては拡張してはならない：

The reporting obligations laid down in this Article shall not extend to:

(a) EUCI；

EUCI;

(b) 当該情報の CERT-EU との間における共有が明示で認められている場合を除き，視認可能なマークによって，当該情報を更に配布することが禁止されている情報。

information the further distribution of which has been excluded by means of a visible marking, unless the sharing thereof with CERT-EU has been explicitly allowed.

第 22 条 インシデント対応の調整及び協力

Article 22 **Incident response coordination and cooperation**

1. サイバーセキュリティ上の情報交換及びインシデント対応調整のハブとして行動する際，CERT-EU は，以下の法主体の間におけるインシデント，サイバーな脅威，脆弱性及びニアミスと関連する情報交換を促進する：

In acting as a cybersecurity information exchange and incident response coordination hub, CERT-EU shall facilitate information exchange with regards to incidents, cyber threats, vulnerabilities and near misses among:

(a) 欧州連合の法主体；

Union entities;

(b) 第 17 条及び第 18 条に示す相手方。

the counterparts referred to in Articles 17 and 18.

2. CERT-EU は，それが ENISA との間の緊密な協力において適格なときは，以下のことを含め，インシ

デント対応に関する欧州連合の法主体間の調整を促進する：

CERT-EU, where relevant in close cooperation with ENISA, shall facilitate coordination among Union entities on incident response, including:

(a) 一貫性のある外部との通信への貢献；

contribution to consistent external communication;

(b) 欧州連合の法主体にとって適格な情報を共有すること，または，それが適格なときは現場において直接に，補助を提供することのような，相互支援；

mutual support, such as sharing information relevant to Union entities, or providing assistance, where relevant directly on site;

(c) 業務運営上の資源の最適化された利用；

optimal use of operational resources;

(d) 欧州連合レベルの他の危機対応の仕組みとの間の調整。

coordination with other crisis response mechanisms at Union level.

3. CERT-EU は，ENISA と緊密に協力して，インシデント，サイバーな脅威，脆弱性及びニアミスの状況認識に関し並びにサイバーセキュリティの分野における適格な発展の共有に関し，欧州連合の法主体を支援する。

CERT-EU, in close cooperation with ENISA, shall support Union entities regarding situational awareness of incidents, cyber threats, vulnerabilities and near misses as well as sharing relevant developments in the field of cybersecurity.

4. 2025 年 1 月 8 日までに，IICB は，CERT-EU からの提案を基礎として，大きなインシデントのインシデント対応の調整及び協力に関する運用指針または勧告を採択する。インシデントの犯罪性が疑われるときは，CERT-EU は，不適切な遅滞なく，法執行機関に対し，そのインシデントをどのように報告するかに関して助言する。

By 8 January 2025, the IICB shall, on the basis of a proposal by CERT-EU, adopt guidelines or recommendations on incident response coordination and cooperation for significant incidents. Where the criminal nature of an incident is suspected, CERT-EU shall advise on how to report the incident to law enforcement authorities, without undue delay.

5. 構成国からの個別の要請の後，かつ，関係する欧州連合の法主体の承認を得て，CERT-EU は，当

該構成国内において影響をもつ大きなインシデントに対する対応または指令(EU) 2022/2555 の第 15 条第 3 項(g)に従った大規模なサイバーセキュリティインシデントに対する対応への貢献のため，第 23 条第 4 項に示すリストの中から，専門家を招請できる。欧州連合の法主体からの技術専門家へのアクセス及びその利用に関する特別規定は，CERT-EU からの提案を基礎として，IICB によって承認される。

Following a specific request from a Member State and with the approval of the Union entities concerned, CERT-EU may call on experts from the list referred to in Article 23(4), for contributing to the response to a major incident which has an impact in that Member State, or a large-scale cybersecurity incident in accordance with Article 15(3), point (g), of Directive (EU) 2022/2555. Specific rules on access to and the use of technical experts from Union entities shall be approved by the IICB on the basis of a proposal by CERT-EU.

第 23 条 大きなインシデントの取扱い

Article 23 **Management of major incidents**

1. 欧州連合の法主体に対して影響を与える大きなインシデントの調整された取扱いを業務運営レベルで支援するため並びに欧州連合の法主体間の及び構成国との間の適格な情報の定期的な交換に貢献するため，IICB は，第 11 条(q)により，CERT-EU 及び ENISA との間で緊密に協力して，第 22 条第 2 項に示す活動を基礎とするサイバー危機管理計画を設ける。サイバー危機管理計画は，少なくとも，以下の諸要素を含める：

   In order to support at operational level the coordinated management of major incidents affecting Union entities and to contribute to the regular exchange of relevant information among Union entities and with Member States, the IICB shall, pursuant to Article 11, point (q), establish a cyber crisis management plan based on the activities referred to in Article 22(2), in close cooperation with CERT-EU and ENISA. The cyber crisis management plan shall include at least the following elements:

   (a) 大きなインシデントの業務運営レベルの管理のために欧州連合の法主体間における調整及び情報の流れに関する手立て；

   arrangements concerning coordination and information flow among Union entities for the management of major incidents at operational level;

   (b) 共通の標準運用手順（SOPs）；

   common standard operating procedures (SOPs);

   (c) 大きなインシデントの深刻度及び危機引金ポイントの共通分類法；

a common taxonomy of major incident severity and crisis triggering points;

(d) 定期的な演習；

regular exercises;

(e) 使用されるべき安全な通信経路。

secure communication channels that are to be used.

2. IICB 内における欧州委員会の代表は，本条第 1 項によって設けられるサイバー危機管理計画に服して，かつ，指令(EU) 2022/2555 の第 16 条第 2 項第 1 副項を妨げることなく，大きなインシデントとの関係における適格な情報の EU-CyCLONe との間の共有のための連絡部局であるものとする。

The Commission representative in the IICB shall, subject to the cyber crisis management plan established pursuant to paragraph 1 of this Article and without prejudice to Article 16(2), first subparagraph, of Directive (EU) 2022/2555, be the point of contact for the sharing of relevant information in relation to major incidents with EU-CyCLONe.

3. CERT-EU は，欧州連合の法主体間において，大きなインシデントの取扱いを調整する。CERT-EU は，大きなインシデントの場合におけるインシデント対応のために必要となり得る利用可能な技術上の専門知識の目録を維持管理し，かつ，第 9 条第 2 項に示す大きなインシデントに関する欧州連合の法主体のサイバー危機管理計画の調整において，IICB を補佐する。

CERT-EU shall coordinate among the Union entities the management of major incidents. It shall maintain an inventory of the available technical expertise that would be needed for incident response in the event of major incidents and assist the IICB in coordinating Union entities' cyber crisis management plans for major incidents referred to in Article 9(2).

4. 欧州連合の法主体は，欧州連合の法主体それぞれの組織内において利用可能な専門家の，当該法主体の特定の技術上の技能の詳細を示す，年次で更新されるリストを提供することによって，技術上の専門知識の目録に貢献する。

The Union entities shall contribute to the inventory of technical expertise by providing an annually updated list of experts available within their respective organisations detailing their specific technical skills.

第 VI 章 最終規定
Chapter VI Final Provisions

第 24 条 当初予算の再配分
Article 24 **Initial budgetary reallocation**

CERT-EU の適正かつ安定した稼動を確保するため，欧州委員会は，CERT-EU の業務運営における使用のために欧州委員会の予算に対する人員及び資金の再配分を提案し得る。その再配分は，この規則の発効後に採択される欧州連合の最初の年次予算と同時に発効する。

In order to ensure the proper and stable functioning of CERT-EU, the Commission may propose the reallocation of staff and financial resources to the Commission budget for use in CERT-EU operations. The reallocation shall be effective at the same time as the first Union annual budget adopted following the entry into force of this Regulation.

第 25 条 見直し
Article 25 **Review**

1. 2025 年 1 月 8 日までに，かつ，その後は年次で，IICB は，CERT-EU の補佐を得て，欧州委員会に対し，この規則の実装に関して報告する。IICB は，欧州委員会に対し，この規則を見直すことの勧告を行い得る。

   By 8 January 2025 and on an annual basis thereafter, the IICB, with the assistance of CERT-EU, shall report to the Commission on the implementation of this Regulation. The IICB may make recommendations to the Commission to review this Regulation.

2. 2027 年 1 月 8 日までに，かつ，その後は 2 年毎に，欧州委員会は，この規則の実装に関し並びに戦略及び業務運営レベルで獲得された経験に関して評価し，かつ，欧州議会及び理事会に対して報告する。

   By 8 January 2027 and every two years thereafter, the Commission shall assess and report on the implementation of this Regulation and on the experience gained at a strategic and operational level to the European Parliament and to the Council.

   本項第 1 副項に示す報告は，欧州連合の事務局としての CERT-EU の設置の可否に関する第 16 条第 1 項に示す見直しを含める。

   The report referred to in the first subparagraph of this paragraph shall include the review referred to in Article 16(1), on the possibility of establishing CERT-EU as a Union office.

3. 2029 年 1 月 8 日までに，欧州委員会は，この規則の稼動を評価し，かつ，欧州議会，理事会，欧州

経済社会委員会及び理域委員会に対し，報告書を提出する。欧州委員会は，当該システムに対して適用可能な欧州連合の他の立法を考慮に入れた上で，EUCI を取扱うネットワーク及び情報システムをこの規則の適用範囲内に包摂することの適切性も評価する。その報告書は，それが必要なときは，立法提案が添付される。

By 8 January 2029, the Commission shall evaluate the functioning of this Regulation and submit a report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The Commission shall also evaluate the appropriateness of including network and information systems handling EUCI within the scope of this Regulation, taking into account other Union legislative acts applicable to those systems. The report shall be accompanied, where necessary, by a legislative proposal.

第 26 条 発効

Article 26 **Entry into force**

この規則は，EU 官報上におけるその公示の 20 日後に発効する。

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

この規則は，その全体について拘束力があり，かつ，全ての構成国において直接に適用される。

This Regulation shall be binding in its entirety and directly applicable in all Member States.

2023 年 12 月 13 日にストラスブールにおいて行われた。

Done at Strasbourg, 13 December 2023.

欧州議会として	理事会として
For the European Parliament	For the Council
長　R. METSOLA	長　P. NAVARRO RÍOS
The President　R. METSOLA	The President　P. NAVARRO RÍOS

2026 Printed in Japan
ISSN 2432-6089
法と情報雑誌　第 11 巻第 2 号（通巻第 73 号）
The Law and Information Magazine vol.11 no.2 (consecutive no.73)

2026 年 2 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）