ISSN 2432-6089

法と情報雑誌

The Law and Information Magazine

第 6 巻第 6 号（通巻第 46 号・2021 年 12 月）

法と情報研究会　編

（第 3 分冊）

本 号 目 次

NIS 指令(EU) 2016/1148
［参考訳・再訂版］

2021 年 12 月 10 日
明治大学法学部教授
夏 井 高 人

＊＊＊

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union（OJ L 194, 19.7.2016, p. 1–30）のテキスト（英語版）に基づいて和訳を試み，2016 年 7 月，法と情報雑誌 1 巻 2 号 34～73 頁にその参考訳を掲載して公表した。

この指令(EU) 2016/1148 の参考訳は，大急ぎで作成したものであったため，誤記や誤訳等が含まれていた。そこで，この参考訳の改訂版を作成し，2017 年 8 月，法と情報雑誌 2 巻 8 号 120～163 頁に掲載して公表した。

その後の研究成果及び関連法令の改正等を踏まえ，NIS 指令の参考訳・改訂版の中で後に発見された誤記及び誤訳等を訂正し，また，その後における研究成果の進展に伴う訳語の統一等も併せ，NIS 指令の参考訳の再訂版を作成することにした。

NIS 指令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/dir/2016/1148/oj
[2021 年 12 月 7 日確認]

NIS 指令は，EU の現行法である。

－解　説－

1．指令(EU) 2016/1148（NIS 指令）

指令(EU) 2016/1148（以下「NIS 指令」という。）は，情報ネットワークのセキュリティを確保するための EU の基本的法令として 2016 年に採択され，同指令を実装する構成国の国内法は，2018 年 5 月 10 日から適用（施行）された。

NIS 指令においては，「基礎サービスの運営者（operators of essential services）」と，「デジタルサービスプロバイダ（digital service providers）」という区分により，レベルの異なる要件及び義務が設定されていた。

しかし，NIS 指令が適用されてからわずか 2 年しか経過していないのに，NIS 指令の有効性に対して疑問が生じた。その疑問の中心は，NIS 指令の実装における各構成国の国内法及び国内措置の実装に一貫性がなく，そのことが，情報社会サービス及びデジタル域内市場の断片化（fragmentation）及び EU の域内国境を越える取引を阻害する障壁をつくり出す

原因となり得るという問題意識である。これらの問題意識は，NIS 指令の第 23 条に基づく評価結果等を基礎としている。

その結果として，NIS 指令を全面改正する NIS2 指令が提案され（COM(2020) 823 final），現在，審議中である（2020/0359(COD)）。

NIS2 指令案においては，上述の基礎サービスの運営者とデジタルサービスプロバイダという区分が廃止され，原則として，当該サービスを提供する法主体の規模の大小に対応して異なる要件及び義務が定められている。NIS 指令の提案（COM/2013/048 final）では，「network and information system」に関して責任を負う法主体として「public administrations」と「market operator」という区分が採用されおり，更に，「market operator」の中には「provider of information society services」と「operator of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health」が含まれるという立法構造を採用していた。

これら，COM/2013/048 final～NIS 指令～NIS2 指令案に至る変遷を考察すると，情報ネットワークのセキュリティに関し，公的部門と民間部門を区別しないという方向で更に一元化が進められているように思われる。

NIS2 指令案の審議と並行して，重要な関連法令の提案も審議されている。例えば，デジタルサービス規則案（COM/2020/825 final），重要な法主体の回復力に関する指令案（COM(2020) 829 final），金融部門におけるデジタル業務遂行の回復力に関する規則案（COM/2020/595 final）及び分散台帳技術を基礎とする市場インフラの実験制度に関する規則案（COM/2020/594 final）がその例である。

NIS 指令に定める条項中に示されている中間介在サービス（intermediation services）のプロバイダに関しては，法的責任（liability）の責任免除原則を定める電子商取引指令 2000/31/EC（OJ L 178, 17.7.2000, p. 1-16）が適用される。デジタルサービス規則案（COM/2020/825 final）は，この電子商取引指令 2000/31/EC の一部改正を含む規則案である。

また，NIS 指令の適用のない法務当局（裁判所，検察庁及び関連行政機関）の間の通信の安全性確保に関しては，e-CODEX 規則案（COM/2020/712 final）が審議されている。

これらの NIS2 指令案と関連する規則及び指令の提案は，相互に密接な関連性をもっている。そのため，それらの法令（案）の全部を総合的に観察し，その機能と構造を理解する必要性がある。

NIS 指令の中で参照されている ENISA 規則(EU) No 526/2013（OJ L 165, 18.6.2013, p. 41-58）は，規則(EU) 2019/881（OJ L 151, 7.6.2019, p. 15-69）の第 68 条第 1 項により，2019 年 6 月 29 日をもって廃止された。ENISA 規則(EU) No 526/2013 への参照は，規則(EU) 2019/881 への参照として読み替えられる。

NIS 指令の中で参照されている個人データ保護指令 95/46/EC（OJ L 281, 23.11.1995, p. 31-50）は，GDPR と略称される一般データ保護規則(EU) 2016/679（OJ L 119, 4.5.2016, p. 1-88）

の第 94 条により，2018 年 5 月 24 日の経過をもって廃止された。個人データ保護指令 95/46/EC への参照は，一般データ保護規則(EU) 2016/679 への参照として読み替えられる。

NIS 指令の中で参照されている規則(EC) No 45/2001（OJ L 8, 12.1.2001, p.1-22）は，規則(EU) 2018/1725（OJ L 295, 21.11.2018, p.39-98）の第 99 条により，2018 年 12 月 10 日の経過をもって廃止された。規則(EC) No 45/2001 への参照は，規則(EU) 2018/1725 への参照として読み替えられる。

NIS 指令の中で参照されている枠組み指令 2002/21/EC（OJ L 108, 24.4.2002, p. 33-50）は，欧州電子通信法指令(EU) 2018/1972（OJ L 321, 17.12.2018, p. 36-214）の第 125 条により，2020 年 12 月 20 日の経過をもって廃止された。枠組み指令 2002/21/EC への参照は，欧州電子通信法指令(EU) 2018/1972 への参照として読み替えられる。

NIS 指令の別紙 II にある指令 2009/72/EC（OJ L 211, 14.8.2009, p. 55-93）は，指令(EU) 2019/944（OJ L 158, 14.6.2019, p. 125-199）の第 72 条により，2020 年 12 月 31 日の経過をもって廃止された。指令 2009/72/EC への参照は，指令(EU) 2019/944 への参照として読み替えられる。

2. 参考訳作成における基本方針

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

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

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

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

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

この参考訳に訳注はない。参考訳中にある脚注は，全て原注である。

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

この参考訳は，Eur-lex のデータ二次利用条件を遵守して作成した。

3. 参考訳作成において留意した事項

NIS 指令の前文(45)の第 1 文である「This Directive applies only to those public administrations which are identified as operators of essential services」は，立法上のミスによる誤りを含む不完全な文である可能性が高い。しかし，この参考訳においては，原文のまま訳出することにした。

NIS 指令の第 15 条第 2 項（特に(b)）は，立法上のミスによる誤りを含む不完全な文である可能性が高い。同項は，下記のような文であるのが正しいのではないかと考えられる。
しかし，この参考訳においては，原文のまま訳出することにした。

> Member States shall ensure that the competent authorities have the powers and means to require operators of essential services to:
> (a) provide the information necessary to assess the security of their network and information systems, including documented security policies;
> (b) provide evidence of the effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified auditor; and
> (c) in the latter case of point (b) of this paragraph, make the results of that security audit, including the underlying evidence, available to the competent authority.

NIS 指令の別紙 I（ANNEX I）の第 1 号(c)の(i)及び(ii)の文末は，いずれも「ピリオド（.）」となっている。これらは，いずれも立法上のミスによるもので，「セミコロン（;）」とするのが正しい。この参考訳においては，そのように解した上で，訳文を作成することにした。

NIS 指令の別紙 II（ANNEX II）の中にある「3. Banking」「5.Health sector」及び「6. Drinking water supply and distribution」の各行の「Type of entity」の列の冒頭には，いずれも「インデント（－）」がない。これは，立法の際のミスによるものであり，本来は「インデント（－）」が付されるべきものと解される。この参考訳においては，そのように解した上で，訳文を作成することにした。

4. 訳語に関する補足的説明

Operators of essential services

NIS 指令の参考訳・初版及び参考訳・改訂版においては，「operators of essential services」を「重要サービスの運営者」または「重要サービス運営者」と訳した。ところが，NIS2 指令の提案（COM(2020) 823 final）の中では，「essential services」と併せて「important services」という概念も用いられており，これらを識別可能な訳語に修正する必要性が生じた。

そこで，この参考訳においては，「operators of essential services」を「基礎サービスの運営者」と訳すことにし，関連する語も同様に修正することにした。

以上に述べたほかは，後掲規則(EU) 2020/ 1783 の参考訳，後掲規則(EU) 2020/1784 の参考訳，後掲規則(EU) 2021/693 の参考訳，後掲規則(EU) 2021/694 の参考訳，後掲理事会決議(2020/C 342 I/01)の参考訳，後掲 e-Justice 決議 2008/2125 の参考訳，後掲電子識別規則(EU) No 910/2014 の参考訳，後掲人工知能規則案（COM/2021/206 final）の参考訳，後掲デジタルサービス規則案（COM/2020/825 final）の参考訳及び後掲 e-CODEX 規則案の参考訳の各冒頭部分で述べたとおりである。

5. 関連参考訳及び参考文献

指令 2013/40/EU の参考訳・改訂版は，法と情報雑誌 2 巻 8 号 164～184 頁にある。指令(EU) 2017/541 の参考訳は，法と情報雑誌 2 巻 8 号 1～29 頁にある。規則(EU) 2018/1241 による改正後の Europol 規則(EU) 2016/794 の参考訳は，法と情報雑誌 4 巻 4 号 8～68 頁にある。規則(EU) 2019/881（Cybersecurity Act）の参考訳・改訂版は，法と情報雑誌 4 巻 8 号 16-86 頁にある。ENISA 規則(EU) No 526/2013 の参考訳は，法と情報雑誌 3 巻 7 号 263～292 頁にある。指令(EU) 2015/1535 の参考訳は，法と情報雑誌 3 巻 7 号 1-20 頁にある。ADR 指令 2013/11/EU の参考訳は，法と情報雑誌 3 巻 6 号 84～113 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。規則(EC) No 45/2001 の参考訳・改訂版は，法と情報雑誌 2 巻 5 号 111～146 頁にある。決定 No 1247/2002/EC の参考訳は，法と情報雑誌 2 巻 4 号 355～360 頁にある。指令 2002/58/EC の参考訳・改訂版は，法と情報雑誌 2 巻 5 号 158～187 頁にある。指令 97/66/EC の参考訳・改訂版は，法と情報雑誌 3 巻 7 号 109～123 頁にある。個人データ保護指令 95/46/EC の参考訳・改訂版は，法と情報雑誌 2 巻 5 号 332～365 頁にある。規則(EU) 2016/679（一般データ保護規則）の参考訳・再訂版は，法と情報雑誌 3 巻 5 号 1～114 頁にある。理事会枠組み決定 2008/977/JHA の参考訳は，法と情報雑誌 2 巻 1 号 141～169 頁にある。e-Justice 個人データ保護決定 2014/333/EU の参考訳は，法と情報雑誌 2 巻 10 号 197～206 頁にある。

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

デジタルサービス規則案（COM/2020/825 final）の参考訳は，法と情報雑誌 6 巻 6 号 1～217 頁にある。規則(EU) 2021/1232 の参考訳は，法と情報雑誌 6 巻 6 号 219～255 頁にある。欧州電子通信法指令(EU) 2018/1972 の参考訳は，法と情報雑誌 4 巻 2 号 1～212 頁にある。指令 2002/21/EC（枠組み指令）の参考訳は，法と情報雑誌 3 巻 7 号 76～108 頁にある。指令 2009/140/EC による改正後の指令 2002/21/EC の参考訳は，法と情報雑誌 3 巻 9 号 31～58 頁にある。電子商取引指令 2000/31/EC の参考訳は，法と情報雑誌 3 巻 1 号 110～141 頁にある。視聴覚メディアサービス指令 2010/13/EU の参考訳は，法と情報雑誌 2 巻 12 号 24～72 頁にある。規則(EU) 2020/1783 の参考訳は，法と情報雑誌 6 巻 5 号 1～81 頁にある。規則(EU) 2020/1784 の参考訳は，法と情報雑誌 6 巻 5 号 82～159 頁にある。規則(EU) 2021/693 の参考訳は，法と情報雑誌 6 巻 4 号 440～486 頁にある。規則(EU) 2021/694 の参考訳は，

法と情報雑誌 6 巻 1 号 1～104 頁にある。理事会決議(2020/C 342 I/01)の参考訳は，法と情報雑誌 6 巻 4 号 513～537 頁にある。e-Justice 決議 2008/2125 の参考訳は，法と情報雑誌 6 巻 4 号 487～512 頁にある。人工知能規則案（COM/2021/206 final）の参考訳は，法と情報雑誌 6 巻 5 号 320～562 頁にある。e-CODEX 規則案の参考訳は，法と情報雑誌 6 巻 5 号 233～319 頁にある。デジタルサービス規則案（COM/2020/825 final）の参考訳は，法と情報雑誌 6 巻 6 号 1～128 頁にある。電子識別規則(EU) No 910/2014 の参考訳は，法と情報雑誌 2 巻 10 号 147～196 頁にある。

ハイブリッドな脅威報告書（JOIN (2017) 30）の参考訳は，法と情報雑誌 2 巻 8 号 91～119 頁にある。サイバー犯罪条約（ETS No.185）の説明書の参考訳は，法と情報雑誌 1 巻 6 号 1～132 頁にある。

この参考訳を作成するに際しては，上記の各参考訳の冒頭部分に掲記した文献等のほか，島村智子「ネットワーク・情報システムの安全に関する指令（NIS 指令）－EU のサイバーセキュリティ対策立法－」外国の立法 277 号 1～32 頁を参考にした。

この参考訳は，科学研究費補助金基盤研究(B)（19KT0014）及び科学研究費補助金基盤研究(A)（15H01928）による研究成果の一部である。

＊＊＊

欧州連合内におけるネットワーク及び情報システムの共通の高いレベルの安全性のための措置に関する欧州議会及び理事会の 2016 年 7 月 6 日の指令 (EU) 2016/1148

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

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

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

Whereas:

(1) ネットワーク及び情報のシステム及びサービスは, 社会において非常に重要な役割を果たしている。その信頼性と安全性は, 経済活動及び社会活動にとって必須であり, とりわけ, 域内市場の稼働にとって必須である。

Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market.

(2) セキュリティ上のインシデントの大きさ, 頻度及び影響は, 増大しており, そして, ネットワーク及び情報システムの稼働に対する重大な脅威を表している。これらのシステムは, そのシス

[1] OJ C 271, 19.9.2013, p. 133.
[2] 2014 年 3 月 13 日の欧州議会の意見書（官報未登載）, 2016 年 5 月 17 日の第 1 読会における理事会の意見書（官報未登載）, 2016 年 7 月 6 日の欧州議会の意見書（官報未登載）.

テムの運用に対して害を加えまたはそれを妨害しようとする意図的で危険な行為の標的ともなりつつある。そのようなインシデントは，経済活動の遂行を阻害し，重要な資産の喪失をもたらし，利用者の秘密を損ない，そして，欧州連合の経済に対して重大な損害をもたらし得る。

The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.

(3) ネットワーク及び情報システム，そして，基本的にはインターネットは，物品，サービス及び人々の国境を越える移動を容易にする上で重要な役割を果たしている。そのような多国籍的な性質のゆえに，それらのシステムに大きな混乱が生ずると，それが意図的なものであるか偶発的なものであるかを問わず，また，どこでその混乱が発生したかとは無関係に，個々の構成国及び欧州連合全体に影響を及ぼし得る。ネットワーク及び情報システムの安全性は，それゆえ，域内市場の円滑な稼働にとって必須である。

Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market.

(4) 欧州のサイバー危機の協力のための基本原則の確立を含め，討議及びグッドプラクティスの交換を容易にする構成国の欧州フォーラム内における大きな発展を基礎として，ネットワーク及び情報システムの安全性に関する構成国間の戦略的な協力を支援し，容易にするため，構成国の代表，欧州委員会及び欧州連合ネットワーク及び情報セキュリティ局（「ENISA」）によって構成される協力グループが設けられるべきである。このグループが実効的かつ包括的なものであるために，全ての構成国が，その構成国の領土内にあるネットワーク及び情報システムの高いレベルの安全性を確保するためのミニマムの実現能力と戦略をもつことが必須である。加えて，リスク管理の文化を促進し，かつ，重大なインシデントが報告されることを確保するために，基礎サービスの運営者及びデジタルサービスプロバイダに対し，安全要件及び通知要件が適用されるべきである。

Building upon the significant progress within the European Forum of Member States in fostering discussions and exchanges on good policy practices, including the development of principles for European cyber-crisis cooperation, a Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security

('ENISA'), should be established to support and facilitate strategic cooperation between the Member States regarding the security of network and information systems. For that group to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of security of network and information systems in their territory. In addition, security and notification requirements should apply to operators of essential services and to digital service providers to promote a culture of risk management and ensure that the most serious incidents are reported.

(5) 欧州連合内のネットワーク及び情報システムの高いレベルの安全性を確保するために，既存の実現能力では不十分である。構成国は，非常に異なるレベルの準備態勢をもっており，それは，欧州連合内全体における断片化されたアプローチを導いた。このことは，消費者と企業の不均一なレベルの保護をもたらし，また，欧州連合内におけるネットワーク及び情報システムの安全性のレベル全体を損ねる。基礎サービスの運営者とデジタルサービスプロバイダの共通の義務が欠落していることは，結果として，欧州連合レベルの協力のためのグローバルで実効的な仕組みの設置を不可能にしてしまう。大学及び研究拠点は，それらの分野における先端的な調査研究，開発及び技術革新において果たすべき決定的な役割をもつ。

The existing capabilities are not sufficient to ensure a high level of security of network and information systems within the Union. Member States have very different levels of preparedness, which has led to fragmented approaches across the Union. This results in an unequal level of protection of consumers and businesses, and undermines the overall level of security of network and information systems within the Union. Lack of common requirements on operators of essential services and digital service providers in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level. Universities and research centres have a decisive role to play in spurring research, development and innovation in those areas.

(6) それゆえ，ネットワーク及び情報システムの安全性という検討課題に対して実効的に対応するためには，要件を構築及び計画する共通のミニマムの実現能力，情報の交換，協力，並びに，基礎サービスの運営者とデジタルサービスプロバイダに対する共通の安全要件を包摂する欧州連合レベルのグローバルなアプローチを要する。ただし，基礎サービスの運営者とデジタルサービスプロバイダは，この指令に基づいて定められる措置よりも強固なセキュリティ上の措置を実装することを排除しない。

Responding effectively to the challenges of the security of network and information systems therefore requires a global approach at Union level covering common minimum capacity building and planning requirements, exchange of information, cooperation and common security requirements for operators of essential services and digital service providers. However, operators of essential services and digital service providers are not precluded from implementing security

measures that are stricter than those provided for under this Directive.

(7) 関連する全てのインシデント及びリスクを包摂するため，この指令は，基礎サービスの運営者及びデジタルサービスプロバイダの両者に対して適用されるべきである。ただし，基礎サービスの運営者及びデジタルサービスプロバイダの義務は，欧州議会及び理事会の指令 2002/21/EC[3]の意味における公衆通信ネットワークまたは公衆が利用可能電子通信サービスを提供する事業者に対しては適用してはならない。それらは，同指令に定める安全性及び完全性に関する特別の要件に服する。また，基礎サービスの運営者及びデジタルサービスプロバイダの要件は，欧州議会及び理事会の規則(EU) No 910/2014[4]の意味における信頼サービスプロバイダに対しても適用してはならない。これらは，同規則に定める安全要件に服する。

To cover all relevant incidents and risks, this Directive should apply to both operators of essential services and digital service providers. However, the obligations on operators of essential services and digital service providers should not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC of the European Parliament and of the Council(3), which are subject to the specific security and integrity requirements laid down in that Directive, nor should they apply to trust service providers within the meaning of Regulation (EU) No 910/2014 of the European Parliament and of the Council(4), which are subject to the security requirements laid down in that Regulation.

(8) この指令は，各構成国が，その構成国の安全保障上の必須の利益の防護を確保し，公共政策及び公共の保安を防護し，犯罪行為の捜査，検知及び訴追ができるようにするために必要となる措置を講ずることを妨げてはならない。欧州連合の機能に関する条約（「TFEU」）の第 346 条に従い，いかなる構成国も，その情報を開示することがその構成国の国家安全保障上の必須の利益に反するとその構成国が判断する情報の提供を強いられてはならない。この文脈においては，理事会決定 2013/488/EU[5]及び非開示協定，または，トラフィックライトプロトコルのような非公式の非開示協定が関係する。

This Directive should be without prejudice to the possibility for each Member State to take the necessary measures to ensure the protection of the essential interests of its security, to safeguard

[3] 電子通信ネットワーク及びサービスに関する共通の法令上の枠組みに関する欧州議会及び理事会の 2002 年 3 月 7 日の指令 2002/21/EC（枠組み指令）（OJ L 108, 24.4.2002, p.33）.

[4] 域内市場における電子的な識別及び電子的な送信のための信頼サービスに関する，並びに，指令 1999/93/EC を廃止する欧州議会及び理事会の 2014 年 7 月 23 日の規則(EU) No 910/2014（OJ L 257, 28.8.2014, p.73）.

[5] EU の機密情報の保護のための安全性規則に関する 2013 年 9 月 23 日の理事会決定 2013/488/EU（OJ L 274, 15.10.2013, p. 1）.

public policy and public security, and to allow for the investigation, detection and prosecution of criminal offences. In accordance with Article 346 of the Treaty on the Functioning of the European Union (TFEU), no Member State is to be obliged to supply information the disclosure of which it considers to be contrary to the essential interests of its security. In this context, Council Decision 2013/488/EU [5] and non-disclosure agreements, or informal non-disclosure agreements such as the Traffic Light Protocol, are of relevance.

(9) 一定の経済部門は，ネットワーク及び情報システムの安全性と関する規定を含む欧州連合の部門別の法行為によって既に規律されており，または，将来において規律され得る。それらの欧州連合の法行為がネットワーク及び情報システムの安全性またはインシデント通知に関する要件を課す条項を含む場合，その条項がこの指令に含まれる義務と少なくとも本質的に均等な要件を含むときは，それらの条項が適用されるべきである。その場合，構成国は，裁判管轄権と関連する条項を含め，そのような欧州連合の部門別の法行為の条項を適用すべきであり，かつ，この指令に定義する基礎サービスの運営者の指定過程を遂行してはならない。この過程において，構成国は，欧州委員会に対し，そのような特別法の条項の適用に関し，情報を提供すべきである。欧州連合の部門別の法行為に含まれるネットワーク及び情報システムの安全性及びインシデント通知に関する要件がこの指令に含まれている要件と均等であるか否かを判断する際，関連する欧州連合の法行為の条項及びその構成国におけるその条項の適用のみが考慮の対象とされるべきである。

Certain sectors of the economy are already regulated or may be regulated in the future by sector-specific Union legal acts that include rules related to the security of network and information systems. Whenever those Union legal acts contain provisions imposing requirements concerning the security of network and information systems or notifications of incidents, those provisions should apply if they contain requirements which are at least equivalent in effect to the obligations contained in this Directive. Member States should then apply the provisions of such sector-specific Union legal acts, including those relating to jurisdiction, and should not carry out the identification process for operators of essential services as defined by this Directive. In this context, Member States should provide information to the Commission on the application of such *lex specialis* provisions. In determining whether the requirements on the security of network and information systems and the notification of incidents contained in sector-specific Union legal acts are equivalent to those contained in this Directive, regard should only be had to the provisions of relevant Union legal acts and their application in the Member States.

(10) 水上輸送分野においては，欧州連合の法行為に基づく企業，船舶，港湾施設，港湾及び船舶交通業務に関する安全要件は，無線システム及び通信システム，コンピュータシステム及びネットワークを含む全ての運用を包摂する。従うべき義務的な手続の一部は，全てのインシデントの報告を含めていることから，それらの要件がこの指令の対応する条項と少なくとも均等である限り，特別法として判断されるべきである。

In the water transport sector, security requirements for companies, ships, port facilities, ports and vessel traffic services under Union legal acts cover all operations, including radio and telecommunication systems, computer systems and networks. Part of the mandatory procedures to be followed includes the reporting of all incidents and should therefore be considered as *lex specialis*, in so far as those requirements are at least equivalent to the corresponding provisions of this Directive.

(11) 水上輸送分野において運営者を指定する際，構成国は，個々の海事管理者に対して一貫性のあるアプローチを提供するという観点から，とりわけ，国際海事機関によって策定された現行のまたは将来の国際的準則及び運用指針を考慮に入れるべきである。

When identifying operators in the water transport sector, Member States should take into account existing and future international codes and guidelines developed in particular by the International Maritime Organisation, with a view to providing individual maritime operators with a coherent approach.

(12) 銀行部門及び金融市場インフラ部門における規制及び監督は，欧州の監督機関と共に発展してきた欧州連合の一次法及び二次法並びに標準の利用を通じて，欧州連合レベルで高度に整合化されている。欧州銀行同盟内において，それらの要件の適用及び監督は，単一の監督仕組みによって確保される。欧州銀行同盟に参加していない構成国に関しては，構成国の関連する銀行規制当局によって，それが確保されている。金融部門の他の分野の規制において，欧州金融監督制度もまた，監督実務における高度の共通性及び収斂性を確保している。欧州証券市場監督局もまた，一定の法主体，すなわち，信用格付機関及び取引情報蓄積機関に対して，直接的な監督上の役割を果たしている。

Regulation and supervision in the sectors of banking and financial market infrastructures is highly harmonised at Union level, through the use of primary and secondary Union law and standards developed together with the European supervisory authorities. Within the banking union, the application and the supervision of those requirements are ensured by the single supervisory mechanism. For Member States that are not part of the banking union, this is ensured by the relevant banking regulators of Member States. In other areas of financial sector regulation, the European System of Financial Supervision also ensures a high degree of commonality and convergence in supervisory practices. The European Securities Markets Authority also plays a direct supervision role for certain entities, namely credit-rating agencies and trade repositories.

(13) 業務遂行上のリスクは，銀行部門及び金融市場インフラ部門における健全性の規制と監督の極めて重要な部分となっている。それは，ネットワーク及び情報システムの安全性，完全性及び回復力を含め，全ての業務遂行を包摂する。それらのシステムと関連する要件は，この指令に基づいて定められる要件をしばしば上回るものであり，欧州連合の多数の法行為によって定められている。それらの法行為は，以下のものを含む：すなわち，信用機関の活

動へのアクセス及び信用機関及び投資企業の健全性監督に関する規定並びに信用機関及び投資企業の健全性要件に関する規定であって，業務遂行上のリスクと関連する要件を含むもの；金融商品の市場に関する規定であって，投資企業のリスク評価及び規制を受ける市場のリスク評価と関連する要件を含んでいるもの；OTC デリバティブ，中央清算機関及び取引情報蓄積機関に関する規定であって，中央清算機関及び取引情報蓄積機関の業務遂行上のリスク評価と関連する要件を含んでいるもの；そして，欧州連合内における証券決済の向上に関する規定及び中央証券決済機関に関する規定であって，業務遂行上のリスクと関連する要件を含んでいるものである。更に，インシデント通知の要件は，金融部門における通常の監督実務の一部分となっており，しばしば監督業務マニュアルの中に収録されている。構成国は，構成国による特別法の適用において，これらの規定及び要件を判断すべきである。

Operational risk is a crucial part of prudential regulation and supervision in the sectors of banking and financial market infrastructures. It covers all operations including the security, integrity and resilience of network and information systems. The requirements in respect of those systems, which often exceed the requirements provided for under this Directive, are set out in a number of Union legal acts, including: rules on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, and rules on prudential requirements for credit institutions and investment firms, which include requirements concerning operational risk; rules on markets in financial instruments, which include requirements concerning risk assessment for investment firms and for regulated markets; rules on OTC derivatives, central counterparties and trade repositories, which include requirements concerning operational risk for central counterparties and trade repositories; and rules on improving securities settlement in the Union and on central securities depositories, which include requirements concerning operational risk. Furthermore, requirements for notification of incidents are part of normal supervisory practice in the financial sector and are often included in supervisory manuals. Member States should consider those rules and requirements in their application of *lex specialis*.

(14) 欧州中央銀行が 2014 年 7 月 25 日付の意見書[6]の中で指摘するとおり，この指令は，決済システム及び清算システムに対する欧州中央銀行制度の監督に関する欧州連合法に基づく体制に影響を与えない。そのような監督に関して職責を負う機関が，この指令に基づく職務権限のある機関との間で，ネットワーク及び情報システムの安全性と関連する事項に関する経験を交換することは，適切なことであろう。国内法及び国内規制に基づいて決済システム及び清算システムのそのような監督を実施する欧州中央銀行制度の非ユーロ圏構成員に対しても同じ判断が適用される。

As noted by the European Central Bank in its opinion of 25 July 2014(6), this Directive does not

6 OJ C 352, 7.10.2014, p.4.

affect the regime under Union law for the Eurosystem's oversight of payment and settlement systems. It would be appropriate for the authorities responsible for such oversight to exchange experiences on matters concerning security of network and information systems with the competent authorities under this Directive. The same consideration applies to non-euro area members of the European System of Central Banks exercising such oversight of payment and settlement systems on the basis of national laws and regulations.

(15) オンライン市場は，消費者及び取引業者が，取引業者との間でオンラインの売買契約またはサービス提供契約を締結できるようにし，かつ，それらの契約の締結を完結させる場である。オンライン市場は，中間介在者としてのみ，それを介して契約が最終的に締結されるサービスを第三者に対して提供するオンラインサービスを含めてはならない。それゆえ，オンライン市場は，特定の製品またはサービスの価格と別の取引業者の価格と比較し，そして，その製品を購入するために好みの取引業者へと利用者をリダイレクトするオンラインサービスを包摂してはならない。オンライン市場によって提供されるコンピュータ処理サービスは，やりとり，データの集約または利用者のプロファイリングの処理を含み得る。第三者からのアプリケーションまたはソフトウェアプログラムのデジタル配信を実現可能にするオンライン販売店として業務遂行するアプリケーション販売店は，オンライン市場の 1 つのタイプとして理解されなければならない。

An online marketplace allows consumers and traders to conclude online sales or service contracts with traders, and is the final destination for the conclusion of those contracts. It should not cover online services that serve only as an intermediary to third-party services through which a contract can ultimately be concluded. It should therefore not cover online services that compare the price of particular products or services from different traders, and then redirect the user to the preferred trader to purchase the product. Computing services provided by the online marketplace may include processing of transactions, aggregations of data or profiling of users. Application stores, which operate as online stores enabling the digital distribution of applications or software programmes from third parties, are to be understood as being a type of online marketplace.

(16) オンライン検索エンジンは，原則として，何らかの事柄に関するクエリーを基礎として利用者が全ての Web サイトの検索を実行できるようにする。検索エンジンは，選択的に，特定の言語による Web サイトに的を絞るものであり得る。この指令に定めるオンライン検索エンジンの定義は，その検索機能が外部の検索エンジンによって提供されるか否かを問わず，特定の Web サイトのコンテントに限定される検索機能を含めてはならない。のみならず，その定義は，特定の製品またはサービスの価格と別の取引業者の価格と比較し，そして，その製品を購入するために好みの取引業者へと利用者をリダイレクトするオンラインサービスを包摂してはならない。

An online search engine allows the user to perform searches of, in principle, all websites on the basis

of a query on any subject. It may alternatively be focused on websites in a particular language. The definition of an online search engine provided in this Directive should not cover search functions that are limited to the content of a specific website, irrespective of whether the search function is provided by an external search engine. Neither should it cover online services that compare the price of particular products or services from different traders, and then redirect the user to the preferred trader to purchase the product.

(17) クラウドコンピューティングサービスは，異なるモデルに従って提供され得る広範な活動の範囲をもつ。この指令の目的のために，「クラウドコンピューティングサービス」という用語は，共有可能なコンピュータ処理資源の拡張可能で伸縮可能なプールへのアクセスをできるようにするサービスに適用され得る。それらのコンピュータ処理資源は，ネットワーク，サービスまたはそれ以外のインフラ，記録保存場所，アプリケーション及びサービスのような資源を含める。「拡張可能」という用語は，要求の変動を取扱うために，その資源の地理的な所在地とは無関係に，クラウドサービスプロバイダによって柔軟に割当てられるコンピュータ資源のことを指す。「伸縮可能なプール」という用語は，利用可能な資源を仕事量に応じて迅速に増減するため，要求に応じて，提供及び解放されるそれらのコンピュータ処理の資源と表現するのが通例である。「共有可能な」という用語は，そのサービスに対する共通のアクセスを共有する複数の利用者のために提供されるが，同一の電子機器からそのサービスが提供される場合でも個々の利用者毎に区分された処理が遂行されるコンピュータ処理の資源と表現されるのが通例である。

Cloud computing services span a wide range of activities that can be delivered according to different models. For the purposes of this Directive, the term ‘cloud computing services’ covers services that allow access to a scalable and elastic pool of shareable computing resources. Those computing resources include resources such as networks, servers or other infrastructure, storage, applications and services. The term ‘scalable’ refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term ‘elastic pool’ is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term ‘shareable’ is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment.

(18) インターネット相互接続点（IXP）の機能は，ネットワークを相互接続することである。IXP は，ネットワークのアクセスを提供することはなく，かつ，中継プロバイダまたはキャリアとして機能することもない。IXP は，相互接続とは無関係の他のサービスを提供することもないが，このことは，IXP の運営者が無関係のサービスを提供することを排除しない。IXP は，技術上または組織上で区分されたネットワークを相互接続するために存在する。「自律システム」とい

う用語は，技術上独立したネットワークと表現されるのが通例である。

The function of an internet exchange point (IXP) is to interconnect networks. An IXP does not provide network access or act as a transit provider or carrier. Nor does an IXP provide other services unrelated to interconnection, although this does not preclude an IXP operator from providing unrelated services. An IXP exists to interconnect networks that are technically and organisationally separate. The term 'autonomous system' is used to describe a technically stand-alone network.

(19) 構成国は，どの法主体が基礎サービスの運営者の判定基準に適合するかを判定することに関する職責を負うべきである。一貫性のあるアプローチを確保するため，基礎サービスの運営者の判定は，全ての構成国間において一貫性をもって適用されるべきである。その目的のために，この指令は，特定の部門及び副部門において能動的な法主体の評価，基礎サービスのリストの作成，潜在的なインシデントが大きな破壊的影響をもち得るか否かを判定するための部門横断的な共通の要素リストの検討，複数の構成国においてサービスを提供する法主体の場合における関連構成国を含む協議プロセス，並びに，識別過程における協力グループの支援を定める。市場において生じ得る変化が正確に反映されることを確保するため，識別された運営者のリストは，構成国によって定期的に見直され，かつ，必要があるときはアップデートされるべきである。それらの後，構成国は，欧州委員会に対し，この共通の手法が構成国による判定の一貫性のある適用をできるようにした範囲を評価するために必要となる情報を提出すべきである。

Member States should be responsible for determining which entities meet the criteria of the definition of operator of essential services. In order to ensure a consistent approach, the definition of operator of essential services should be coherently applied by all Member States. To that end, this Directive provides for the assessment of the entities active in specific sectors and subsectors, the establishment of a list of essential services, the consideration of a common list of cross-sectoral factors to determine whether a potential incident would have a significant disruptive effect, a consultation process involving relevant Member States in the case of entities providing services in more than one Member State, and the support of the Cooperation Group in the identification process. In order to ensure that possible changes in the market are accurately reflected, the list of identified operators should be reviewed regularly by Member States and updated when necessary. Finally, Member States should submit to the Commission the information necessary to assess the extent to which this common methodology has allowed a consistent application of the definition by Member States.

(20) 基礎サービスの運営者の識別の過程において，構成国は，少なくともこの指令が示す副部門毎に，どのサービスが，重要な社会活動及び経済活動を維持するために必須と判断されなければならないか，並びに，この指令のリストに示す部門及び副部門に列挙された法主体及びそれらのサービスの提供が運営者の識別基準に適合するか否かを評価すべきである。

ある法主体が重要な社会活動及び経済活動を維持するために必須のサービスを提供するか否かを評価する際，当該法主体が基礎サービスのリストに含められているサービスを提供する否かを吟味することで足りる。更に，その基礎サービスがネットワーク及び情報システムに依拠していることが証明されるべきである。それらの後，インシデントが，そのサービスの提供に対して大きな破壊的影響をもつか否かを評価する際，構成国は，部門横断的な要素の数，並びに，それが適切なときは，部門別の要素を考慮すべきである。

In the process of identification of operators of essential services, Member States should assess, at least for each subsector referred to in this Directive, which services have to be considered as essential for the maintenance of critical societal and economic activities, and whether the entities listed in the sectors and subsectors referred to in this Directive and providing those services meet the criteria for the identification of operators. When assessing whether an entity provides a service which is essential for the maintenance of critical societal or economic activities, it is sufficient to examine whether that entity provides a service that is included in the list of essential services. Furthermore, it should be demonstrated that provision of the essential service is dependent on network and information systems. Finally, when assessing whether an incident would have a significant disruptive effect on the provision of the service, Member States should take into account a number of cross-sectoral factors, as well as, where appropriate, sector-specific factors.

(21) 基礎サービスの運営者を識別する目的のために，構成国内の拠点とは，確実な手立てによる実効的かつ現実の活動の実行を含意する。そのような手立ての法律上の方式，法人格をもつ支店または子会社によるか否かは，この点に関する決定的な要素ではない。

For the purposes of identifying operators of essential services, establishment in a Member State implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary possessing legal personality, is not the determining factor in this respect.

(22) この指令に示す部門及び副部門において業務遂行する法主体が基礎サービスと非基礎サービスの両方を提供することがあり得る。例えば，航空輸送部門において，空港は，滑走路の運営管理のように，構成国によって必須と判断され得るサービスを提供するが，ショッピングエリアの提供のように，必須ではないと判断され得る多数のサービスも提供する。基礎サービスの運営者は，必須とみなされる当該サービスとの関係に限り，個別の安全要件に服するべきである。それゆえ，運営者の識別の目的のために，構成国は，必須と判断するサービスのリストを作成すべきである。

It is possible that entities operating in the sectors and subsectors referred to in this Directive provide both essential and non-essential services. For example, in the air transport sector, airports provide services which might be considered by a Member State to be essential, such as the management of

the runways, but also a number of services which might be considered as non-essential, such as the provision of shopping areas. Operators of essential services should be subject to the specific security requirements only with respect to those services which are deemed to be essential. For the purpose of identifying operators, Member States should therefore establish a list of the services which are considered as essential.

(23) サービスのリストは，当の構成国の領土内で提供され，この指令に基づく要件を満たす全てのサービスを含めるべきである。構成国は，既存のリストに新たなサービスを含めることによって補遺できるべきである。サービスのリストは，基礎サービスの運営者を識別できるようにする，構成国のための基準点を提供すべきである。その目的は，この指令に示す当の部門内にあるタイプの基礎サービスを識別し，そして，それによって当の部門において能動的な法主体が職責を負い得るようにするために，基礎サービスを必須ではない活動と区別することにある。構成国によって作成されるサービスのリストは，構成国間における識別過程での一貫性の全体的なレベルを確保するという観点から，各構成国の法定の業務の評価において，更なる入力を提供し得る。

The list of services should contain all services provided in the territory of a given Member State that fulfil the requirements under this Directive. Member States should be able to supplement the existing list by including new services. The list of services should serve as a reference point for Member States, allowing for identification of operators of essential services. Its purpose is to identify the types of essential services in any given sector referred to in this Directive, thus distinguishing them from non-essential activities for which an entity active in any given sector might be responsible. The list of services established by each Member State would serve as further input in the assessment of the regulatory practice of each Member State with a view to ensuring the overall level of consistency of the identification process amongst Member States.

(24) 識別過程の目的のために，ある法主体が複数の構成国において基礎サービスを提供する場合，それらの構成国は，相互に，2 国間または多国間の協議に入るべきである。この協議過程は，国境を越える影響の面における運営者の必須性を評価するために，構成国を助けること，それによって，関与する各構成国が，提供されるサービスと関連するリスクに関するその構成国の見解を提示できるようにすることを意図している。関係する構成国は，この過程の中で，他の構成国の見解を考慮に入れるべきであり，また，これに関する協力グループの補助を要請できるべきである。

For the purposes of the identification process, where an entity provides an essential service in two or more Member States, those Member States should engage in bilateral or multilateral discussions with each other. This consultation process is intended to help them to assess the critical nature of the operator in terms of cross-border impact, thereby allowing each Member State involved to present its views regarding the risks associated with the services provided. The Member States concerned

should take into account each other's views in this process, and should be able to request the assistance of the Cooperation Group in this regard.

(25) 識別過程の結果として，構成国は，どの法主体がネットワーク及び情報システムの安全性に関する義務に服するかを判定するための国内措置を採択すべきである。この結果は，全ての基礎サービスの運営者を反映するリストを採択することによって，または，運営者の出力や利用者数のような客観的で定量的な基準を含め，どの法主体がネットワーク及び情報システムの安全性に関する義務に服するかを判定できるようにする国内措置を採択することによって到達され得る。その国内措置は，既存のものであるか，この指令の文脈において採択されるものであるかを問わず，この指令に基づく基礎サービスの運営者の識別をできるようにする全ての法律上の措置，行政上の措置及び政策上の措置を含めるべきである。

As a result of the identification process, Member States should adopt national measures to determine which entities are subject to obligations regarding the security of network and information systems. This result could be achieved by adopting a list enumerating all operators of essential services or by adopting national measures including objective quantifiable criteria, such as the output of the operator or the number of users, which make it possible to determine which entities are subject to obligations regarding the security of network and information systems. The national measures, whether already existing or adopted in the context of this Directive, should include all legal measures, administrative measures and policies allowing for the identification of operators of essential services under this Directive.

(26) 関係部門との関係において，識別された基礎サービスの運営者の重要性の表示を提供するため，構成国は，どの運営者が識別されたかを明らかにし得る情報を漏らすことを強いられることなく，例えば，市場占有率または製造もしくは運搬される分量の面におけるそれらの運営者の数及び規模を考慮に入れるべきである。

In order to give an indication of the importance, in relation to the sector concerned, of the identified operators of essential services, Member States should take into account the number and the size of those operators, for example in terms of market share or of the quantity produced or carried, without being obliged to divulge information which would reveal which operators have been identified.

(27) 基礎サービスの提供に対してどのインシデントが大きな破壊的な影響をもち得るかを判定するため，構成国は，私的な目的または職業上の目的で当該サービスに依拠する利用者の数のような，異なる要素の数を考慮に入れるべきである。当該サービスの利用は，直接的なもの，間接的なもの，または，中間介在されるものであり得る。程度及び持続期間の面において，経済活動，社会活動または公共の保安に対してインシデントがもち得る影響を評価する際，構成国は，継続不能状態が負の影響をもち始めるまでに要する可能性のある時間も評価すべきである。

In order to determine whether an incident would have a significant disruptive effect on the provision of an essential service, Member States should take into account a number of different factors, such as the number of users relying on that service for private or professional purposes. The use of that service can be direct, indirect or by intermediation. When assessing the impact that an incident could have, in terms of its degree and duration, on economic and societal activities or public safety, Member States should also assess the time likely to elapse before the discontinuity would start to have a negative impact.

(28) 部門横断的な要素に加え，インシデントが基礎サービスの提供に対して大きな破壊的影響をもち得るか否かを判定するため，部門別の要素も判断されるべきである。エネルギーの供給者に関しては，そのような要素は，国内で生産されるエネルギーの量及び割合を；石油の供給者に関しては，1 日当たりの量；空港及び航空会社を含め，航空輸送，鉄道輸送及び港湾に関しては，国内輸送量の割合及び 1 年当たりの旅客数または貨物輸送業務数；銀行インフラ及び金融市場インフラに関しては，総資産または GDP に対する総資産の割合を基礎とするそれらのインフラのシステミックな重要性；医療部門に関しては，そのサービスの下で診療を受けた 1 年当たりの患者数；水道に関しては，浄水処理と供給，例えば，病院，公共機関または個人を含め，水の供給を受ける利用者の数と種類，並びに，同一の地理的範囲を包摂する代替的な水資源の存在を含め得る。

In addition to the cross-sectoral factors, sector-specific factors should also be considered in order to determine whether an incident would have a significant disruptive effect on the provision of an essential service. With regard to energy suppliers, such factors could include the volume or proportion of national power generated; for oil suppliers, the volume per day; for air transport, including airports and air carriers, rail transport and maritime ports, the proportion of national traffic volume and the number of passengers or cargo operations per year; for banking or financial market infrastructures, their systemic importance based on total assets or the ratio of those total assets to GDP; for the health sector, the number of patients under the provider's care per year; for water production, processing and supply, the volume and number and types of users supplied, including, for example, hospitals, public service organisations, or individuals, and the existence of alternative sources of water to cover the same geographical area.

(29) ネットワーク及び情報システムの高いレベルの安全性を達成し，維持するために，各構成国は，実装されるべき戦略上の目標及び政策上の具体的な活動を定める，ネットワーク及び情報システムの安全性に関する国内戦略をもつべきである。

To achieve and maintain a high level of security of network and information systems, each Member State should have a national strategy on the security of network and information systems defining

the strategic objectives and concrete policy actions to be implemented.

(30) 国内統治構造の相違を考慮し，また，既に存在する部門別の手立てまたは欧州連合の監督機関または規制組織を防護するため，及び，重複を避けるため，構成国は，この指令に基づく基礎サービスの運営者及びデジタルサービスプロバイダのネットワーク及び情報システムの安全性と結びつけられた職務を満たすことに関して職責を負う複数の職務権限のある国内機関を指定できるべきである。

In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, and to avoid duplication, Member States should be able to designate more than one national competent authority responsible for fulfilling the tasks linked to the security of the network and information systems of operators of essential services and digital service providers under this Directive.

(31) 国境を越える協力及び通信を容易にするため，また，この指令が実効的に実装され得るようにするため，部門別の法令上の手立てを妨げることなく，欧州連合レベルのネットワーク及び情報システムの高いレベルの安全性及び国境を越える協力と関連する検討課題の調整に関して職責を負う国内単一連絡部局を，各構成国が指定する必要がある。職務権限のある機関及び単一連絡部局は，それらに割り当てられた職務を実効的かつ効率的な態様で遂行し，そして，この指令の目的を達成することを確保するための十分な技術上，資金上及び人的な資源をもつべきである。この指令は，信頼と信任をつくり出すことによって域内市場の稼働を向上させることを目的としているので，構成国の組織は，経済取引主体と実効的に連携することができ，かつ，しかるべく組織化される必要がある。

In order to facilitate cross-border cooperation and communication and to enable this Directive to be implemented effectively, it is necessary for each Member State, without prejudice to sectoral regulatory arrangements, to designate a national single point of contact responsible for coordinating issues related to the security of network and information systems and cross-border cooperation at Union level. Competent authorities and single points of contact should have the adequate technical, financial and human resources to ensure that they can carry out the tasks assigned to them in an effective and efficient manner and thus achieve the objectives of this Directive. As this Directive aims to improve the functioning of the internal market by creating trust and confidence, Member State bodies need to be able to cooperate effectively with economic actors and to be structured accordingly.

(32) 職務権限のある機関またはコンピュータセキュリティインシデント対応チーム（「CSIRT」）は，インシデント通知を受けるべきである。単一連絡部局は，その単一連絡部局が職務権限のある機関または CSIRT としても活動するのでない限り，インシデント通知を直接に受けてはならない。ただし，職務権限のある機関または CSIRT は，影響を受ける別の構成国の単一連

絡部局に対してインシデント通知を転送する職務を単一連絡部局に与え得るべきである。

Competent authorities or the computer security incident response teams (‘CSIRTs’) should receive notifications of incidents. The single points of contact should not receive directly any notifications of incidents unless they also act as a competent authority or a CSIRT. A competent authority or a CSIRT should however be able to task the single point of contact with forwarding incident notifications to the single points of contact of other affected Member States.

(33) 構成国及び欧州委員会に対する実効的な情報の提供を確保するため，単一連絡部局から協力グループに対して概要報告書が送付されるべきであり，かつ，通知元法主体の識別に関する情報は，協力グループにおけるベストプラクティスの交換にとって必要がないので，通知内容並びに基礎サービスの運営者及びデジタルサービスプロバイダの識別名の機密性を維持するため，概要報告書は匿名化されるべきである。概要報告書は，受けた通知の数，並びに，安全性の侵害の種類，その侵害の重大性及びその侵害の持続時間のような，通知されたインシデントの性質の表示を含めるべきである。

To ensure the effective provision of information to the Member States and to the Commission, a summary report should be submitted by the single point of contact to the Cooperation Group, and should be anonymised in order to preserve the confidentiality of the notifications and the identity of operators of essential services and digital service providers, as information on the identity of the notifying entities is not required for the exchange of best practice in the Cooperation Group. The summary report should include information on the number of notifications received, as well as an indication of the nature of the notified incidents, such as the types of security breaches, their seriousness or their duration.

(34) 構成国は，ネットワーク及び情報システムのインシデント及びリスクを防止し，検出し，対応し，そして，緩和するための技術上及び組織上の実現能力の両者の面において，適切な手段を具備すべきである。それゆえ，構成国は，コンピュータ緊急対応チーム（「CERT」）としても知られ，インシデント及びリスクを取り扱うための実効的かつ互換性のある実現能力を保障し，かつ，欧州連合レベルの効率的な協力を確保するための必須の要件を遵守し，良好に機能する CSIRT をもつべきである。全てのタイプの基礎サービスの運営者及びデジタルサービスプロバイダがそのような実現能力及び協力からの利益を享受するため，構成国は，指定された CSIRT によって全てのタイプが包摂されることを確保すべきである。サイバーセキュリティに関する国際協力の重要性に鑑み，CSIRT は，この指令によって設けられる CSIRT ネットワークに加え，国際協力ネットワークにも参加できるべきである。

Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information system incidents and risks. Member States should therefore ensure that they have well-functioning CSIRTs, also

known as computer emergency response teams (‘CERTs’), complying with essential requirements to guarantee effective and compatible capabilities to deal with incidents and risks and ensure efficient cooperation at Union level. In order for all types of operators of essential services and digital service providers to benefit from such capabilities and cooperation, Member States should ensure that all types are covered by a designated CSIRT. Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive.

(35) ネットワーク及び情報システムの大部分が民間で運営されているので，民間部門と公的部門との間の協力が必須である。基礎サービスの運営者及びデジタルサービスプロバイダは，ネットワーク及び情報システムの安全性を確保するため，それら自身の非公式な協力の仕組みを求めることが推進されるべきである。協力グループは，それが適切な場合には，関連する利害関係者を討議のために招請できるべきである。情報及びベストプラクティスの共有を効率的に推進するため，そのような交換に参加する基礎サービスの運営者及びデジタルサービスプロバイダが，それらの協力の結果として不利益を受けないことを確保することが必須である。

As most network and information systems are privately operated, cooperation between the public and private sectors is essential. Operators of essential services and digital service providers should be encouraged to pursue their own informal cooperation mechanisms to ensure the security of network and information systems. The Cooperation Group should be able to invite relevant stakeholders to the discussions where appropriate. To encourage effectively the sharing of information and of best practice, it is essential to ensure that operators of essential services and digital service providers who participate in such exchanges are not disadvantaged as a result of their cooperation.

(36) ENISA は，その専門知識及び助言を提供することによって，そして，ベストプラクティスの交換を容易にすることによって，構成国及び欧州委員会を補助すべきである。とりわけ，この指令の適用において，欧州委員会は，ENISA と協議すべきであり，かつ，構成国は，ENISA と協議できるべきである。構成国間における実現能力と知識を構築するため，協力グループは，ベストプラクティスの交換，構成国の実現能力及び準備態勢に関する討議のための道具として，並びに，任意で，ネットワーク及び情報システムの安全性に関する国内戦略を評価する際，構成国の実現能力を構築する際，そして，ネットワーク及び情報システムの安全性と関連する演習を評価する際，その協力グループの構成員を支援するための道具としても役立つべきである。

ENISA should assist the Member States and the Commission by providing expertise and advice and by facilitating the exchange of best practice. In particular, in the application of this Directive, the Commission should, and Member States should be able to, consult ENISA. To build capacity and

knowledge among Member States, the Cooperation Group should also serve as an instrument for the exchange of best practice, discussion of capabilities and preparedness of the Member States and, on a voluntary basis, to assist its members in evaluating national strategies on the security of network and information systems, building capacity and evaluating exercises relating to the security of network and information systems.

(37) それが適切なときは，構成国は，この指令を適用する際，既存の組織構造または戦略を使用または修正できるべきである。

Where appropriate, Member States should be able to use or adapt existing organisational structures or strategies when applying this Directive.

(38) 協力グループ及び ENISA のそれぞれの職務は，相互依存し，補完するものである。一般に，ENISA は，その職務を実行する際，欧州議会及び理事会の規則(EU) No 526/2013[7]に定める ENISA の目的に沿って，すなわち，欧州連合の現行の法行為または将来の法行為に基づき，ネットワーク及び情報システムの安全性に関する法律上の及び法令上の要件に適合するために必要となる政策の実装において，欧州連合の機関，組織，事務局及び部局並びに構成国を支援するために協力グループを支援すべきであり，とりわけ，ENISA は，規則(EU) No 526/2013 に定める ENISA 自身の職務と対応する部門において，すなわち，ネットワーク及び情報システムの安全性戦略を分析すること，ネットワーク及び情報システムの安全性と関連する欧州連合の演習の組織化及びその実施を支援すること，そして，認識向上及び訓練に関する情報及びベストプラクティスを交換することにおいて，補助を提供すべきである。ENISA は，インシデントの影響力の大きさを判定するための部門別基準に関する運用指針の策定にも関与すべきである。

The respective tasks of the Cooperation Group and of ENISA are interdependent and complementary. In general, ENISA should assist the Cooperation Group in the execution of its tasks, in line with the objective of ENISA set out in Regulation (EU) No 526/2013 of the European Parliament and the Council (7), namely to assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information system security under existing and future legal acts of the Union. In particular, ENISA should provide assistance in those areas that correspond to its own tasks, as set out in Regulation (EU) No 526/2013, namely analysing network and information system security strategies, supporting the organisation and running of Union exercises relating to the security of network and information systems, and exchanging information and best practice on awareness-raising and training. ENISA should also be involved in the development of guidelines for sector-

[7] 欧州連合ネットワーク及び情報セキュリティ局（ENISA）に関する，並びに，規則(EC) No 460/2004 を廃止する欧州議会及び理事会の 2013 年 5 月 21 日の規則(EU) No 526/2013（OJ L 165, 18.6.2013, p.41）.

specific criteria for determining the significance of the impact of an incident.

(39) ネットワーク及び情報システムの高度な安全性を促進するため，協力グループは，それが適切なときは，制限のある情報の交換に関する既存の手立てを尊重しつつ，ノウハウ及びベストプラクティスを交換するため，そして，それらの機関等の仕事に対して影響をもち得るネットワーク及び情報システムの安全性の側面に関して助言を提供するため，関連する欧州連合の機関，組織，事務局及び部局と協力すべきである。法執行機関の仕事に対して影響をもち得るネットワーク及び情報システムの安全性の側面に関する法執行機関との間の協力において，協力グループは，既存の情報伝達経路及び設けられたネットワークを尊重すべきである。

In order to promote advanced security of network and information systems, the Cooperation Group should, where appropriate, cooperate with relevant Union institutions, bodies, offices and agencies, to exchange know-how and best practice, and to provide advice on security aspects of network and information systems that might have an impact on their work, while respecting existing arrangements for the exchange of restricted information. In cooperating with law enforcement authorities regarding the security aspects of network and information systems that might have an impact on their work, the Cooperation Group should respect existing channels of information and established networks.

(40) インシデントに関する情報は，一般公衆及び企業にとって，とりわけ，中小規模の企業にとって，その重要性を増加させている。幾つかの事例において，そのような情報は，構成国レベルで，Web サイトを介して，特定の国の言語を用いて，すなわち，国内の局面をもつインシデント及びその発生に主に焦点を当てて，既に提供されている。企業が次第に国境を越えて業務遂行し，また，市民がオンラインサービスを利用していることに鑑み，インシデントに関する情報は，欧州連合レベルで，集約された方式で提供されるべきである。CSIRT ネットワークの事務局は，企業の利益と必要性に特に的を絞って，欧州連合を横断して発生した大きなインシデントに関する一般的な情報を一般公衆が利用できるようにする場合，Web サイトを維持管理し，または，既存の Web サイト上に専用ページをホストすることが推奨される。CSIRT ネットワークに参加する CSIRT は，機密情報または機微の情報が含まれることなく，任意に，当該 Web サイト上で公表されるインシデント情報を提供することが推奨される。

Information about incidents is increasingly valuable to the general public and businesses, particularly small and medium-sized enterprises. In some cases, such information is already provided via websites at the national level, in the language of a specific country and focusing mainly on incidents and occurrences with a national dimension. Given that businesses increasingly operate across borders and citizens use online services, information on incidents should be provided in an aggregated form at Union level. The secretariat of the CSIRTs network is encouraged to maintain a website or to host a dedicated page on an existing website, where general information on major

incidents that have occurred across the Union is made available to the general public, with a specific focus on the interests and needs of businesses. CSIRTs participating in the CSIRTs network are encouraged to provide on a voluntary basis the information to be published on that website, without including confidential or sensitive information.

(41) 企業秘密に関する欧州連合の規定及び国内規定に従って情報が機密のものと判断される場合，そのような機密性は，この指令に定める活動を遂行し，義務を満たす際，確保されるべきである。

Where information is considered to be confidential in accordance with Union and national rules on business confidentiality, such confidentiality should be ensured when carrying out the activities and fulfilling the objectives set by this Directive.

(42) リアルタイムでインシデントのシナリオをシミュレートする演習は，ネットワーク及び情報システムの安全性と関連する構成国の準備態勢及び協力を試験するために必須である。ENISA によって調整され，構成国が参加して実施される CyberEurope の演習サイクルは，試験のため，そして，欧州連合レベルのインシデント対応をどのようにして次第に向上させるべきかに関する勧告の策定のための有用な道具の 1 つである。現在のところ，演習の計画及びその実施への参加のいずれにも構成国が義務を負っていないことを考慮し，この指令に基づく CSIRT ネットワークの創設は，正確な計画と戦略上の選択を基礎として構成国が演習に参加することを実現可能にすべきである。この指令に基づいて設けられる協力グループは，とりわけ，演習と関連する戦略上の決定を討議すべきであるが，演習の定期的な実施，及び，シナリオの設計に関することのみとしてはならない。ENISA は，その任務に従い，協力グループ及び CSIRT ネットワークに対して専門知識と助言を提供することによって，欧州連合全域の演習の組織化及びその実施を支援すべきである。

Exercises which simulate real-time incident scenarios are essential for testing Member States' preparedness and cooperation regarding the security of network and information systems. The CyberEurope cycle of exercises coordinated by ENISA with the participation of the Member States is a useful tool for testing and drawing up recommendations on how incident-handling at Union level should improve over time. Considering that the Member States are not currently under any obligation to either plan or participate in exercises, the creation of the CSIRTs network under this Directive should enable Member States to participate in exercises on the basis of accurate planning and strategic choices. The Cooperation Group set up under this Directive should discuss the strategic decisions regarding exercises, in particular but not exclusively as regards the regularity of the exercises and the design of the scenarios. ENISA should, in accordance with its mandate, support the organisation and running of Union-wide exercises by providing its expertise and advice to the Cooperation Group and the CSIRTs network.

(43) ネットワーク及び情報システムに影響を及ぼすセキュリティ上の諸問題がグローバルな性質に鑑み，安全性基準及び情報交換を向上させ，かつ，セキュリティ上の検討課題に対する共通のグローバルなアプローチを促進するために，緊密な国際協力の必要性がある。

Given the global nature of security problems affecting network and information systems, there is a need for closer international cooperation to improve security standards and information exchange, and to promote a common global approach to security issues.

(44) ネットワーク及び情報システムの安全性を確保すべき責任は，大きな範囲で，基礎サービスの運営者及びデジタルサービスプロバイダの上にある。リスク評価及び直面しているリスクとって適切なセキュリティ上の措置の実装を含め，リスク管理の文化は，法令上の適切な要件及び産業界の任意の実務によって促進され，開発されるべきである。信頼できるレベルの活動の場を構築することは，全ての構成国からの実効的な協力を確保するための協力グループ及び CSIRT ネットワークの実効的な稼働にとって必須である。

Responsibilities in ensuring the security of network and information systems lie, to a great extent, with operators of essential services and digital service providers. A culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced, should be promoted and developed through appropriate regulatory requirements and voluntary industry practices. Establishing a trustworthy level playing field is also essential to the effective functioning of the Cooperation Group and the CSIRTs network, to ensure effective cooperation from all Member States.

(45) この指令は，基礎サービスの運営者として識別されるその構成国の行政に対してのみ適用される。それゆえ，この指令の適用範囲外にある行政組織のネットワーク及び情報システムの安全性を確保するのは，構成国の責任である。

This Directive applies only to those public administrations which are identified as operators of essential services. Therefore, it is the responsibility of Member States to ensure the security of network and information systems of public administrations not falling within the scope of this Directive.

(46) リスク管理の措置は，インシデントのリスクを特定し，インシデントを防止し，検出し及び対処し，そして，その影響を緩和するための措置を含む。ネットワーク及び情報システムの安全性は，記録保存され，送信され及び処理されるデータの安全性を含む。

Risk-management measures include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact. The security of network and information systems comprises the security of stored, transmitted and processed data.

(47) 職務権限のある機関は，基礎サービスの運営者がインシデント通知を要求される場合に関する国内運用指針を採択する能力を保持すべきである。

Competent authorities should retain the ability to adopt national guidelines concerning the circumstances in which operators of essential services are required to notify incidents.

(48) 欧州連合内の企業の多くは，その企業のサービス提供のためにデジタルサービスプロバイダに依拠している。幾つかのデジタルサービスは，基礎サービスの運営者を含め，そのデジタルサービスの利用者の重要な資源となり得るので，また，そのような利用者が利用可能な代替手段を常にもっているとは限らないので，この指令は，そのようなサービスのプロバイダに対しても適用されるべきである。この指令に示すタイプのデジタルサービスの安全性，継続性及び信頼性は，多数の企業の円滑な稼働にとって必須である。そのようなデジタルサービスが混乱すると，それに依拠している他のサービスの提供が妨げられることとなり得るのであり，そして，欧州連合内における重要な経済活動及び社会活動に対して影響をもつこととなり得る。それゆえ，そのようなデジタルサービスは，それに依拠する企業の円滑な稼働のために，更には，そのような企業が域内市場や欧州連合内を横断する国境を越える取引に参加するために，決定的な重要性をもち得る。この指令が対象とするそれらのデジタルサービスプロバイダは，欧州連合内の多数の企業が次第に依拠するようになっているデジタルサービスを提供すると考えられるプロバイダである。

Many businesses in the Union rely on digital service providers for the provision of their services. As some digital services could be an important resource for their users, including operators of essential services, and as such users might not always have alternatives available, this Directive should also apply to providers of such services. The security, continuity and reliability of the type of digital services referred to in this Directive are of the essence for the smooth functioning of many businesses. A disruption of such a digital service could prevent the provision of other services which rely on it and could thus have an impact on key economic and societal activities in the Union. Such digital services might therefore be of crucial importance for the smooth functioning of businesses that depend on them and, moreover, for the participation of such businesses in the internal market and cross-border trade across the Union. Those digital service providers that are subject to this Directive are those that are considered to offer digital services on which many businesses in the Union increasingly rely.

(49) 欧州連合内における他の企業の業務遂行に対するそのサービスの重要性に鑑み，デジタルサービスプロバイダは，そのプロバイダが提供するデジタルサービスの安全性に対して示されたリスクの程度に見合ったレベルの安全性を確保すべきである。実際のところ，非常に重要な社会活動及び経済活動の維持のためにしばしば必須である基礎サービスの運営者のリスクの程度は，デジタルサービスプロバイダよりも高い。それゆえ，デジタルサービスプロバイダの安全要件は，より軽くすべきである。デジタルサービスプロバイダは，そのプロ

バイダのネットワーク及び情報システムの安全性に対して示されたリスクを管理するために適切であるとそのプロバイダが判断する措置を講ずる自由を維持すべきである。その国境を越える性質のゆえに，デジタルサービスプロバイダは，欧州連合レベルで，より整合化されたアプローチに服すべきである。実装行為は，そのような措置の指定及び実装を促進すべきである。

Digital service providers should ensure a level of security commensurate with the degree of risk posed to the security of the digital services they provide, given the importance of their services to the operations of other businesses within the Union. In practice, the degree of risk for operators of essential services, which are often essential for the maintenance of critical societal and economic activities, is higher than for digital service providers. Therefore, the security requirements for digital service providers should be lighter. Digital service providers should remain free to take measures they consider appropriate to manage the risks posed to the security of their network and information systems. Because of their cross-border nature, digital service providers should be subject to a more harmonised approach at Union level. Implementing acts should facilitate the specification and implementation of such measures.

(50) ハードウェア製造業者及びソフトウェア開発者は，基礎サービスの運営者ではなく，デジタルサービスプロバイダでもないが，それらの者の製品は，ネットワーク及び情報システムの安全性を拡大する。それゆえ，それらの者は，基礎サービスの運営者及びデジタルサービスプロバイダがそのネットワーク及び情報システムを安全なものとする上で，重要な役割を演じている。そのようなハードウェア製品及びソフトウェア製品は，既に，製造物責任に関する既存の規定の適用対象となっている。

While hardware manufacturers and software developers are not operators of essential services, nor are they digital service providers, their products enhance the security of network and information systems. Therefore, they play an important role in enabling operators of essential services and digital service providers to secure their network and information systems. Such hardware and software products are already subject to existing rules on product liability.

(51) 基礎サービスの運営者及びデジタルサービスプロバイダに課される技術上及び組織上の措置は，特別の商業情報及び通信技術製品が，特別な態様で設計，開発または製造されることを要求してはならない。

Technical and organisational measures imposed on operators of essential services and digital service providers should not require a particular commercial information and communications technology product to be designed, developed or manufactured in a particular manner.

(52) 基礎サービスの運営者及びデジタルサービスプロバイダは，それらの者が使用するネットワ

ーク及び情報システムの安全性を確保すべきである。それらは，そのプロバイダの内部ITスタッフによって管理され，または，そのセキュリティがアウトソースされている，基本的には民間のネットワーク及び情報システムである。それらのプロバイダが，そのネットワーク及び情報システムの維持管理を内部者によって遂行しているか，または，それをアウトソースしているかに拘りなく，関連する基礎サービスの運営者及びデジタルサービスプロバイダに対し，安全要件及び通知要件が適用されるべきである。

Operators of essential services and digital service providers should ensure the security of the network and information systems which they use. These are primarily private network and information systems managed by their internal IT staff or the security of which has been outsourced. The security and notification requirements should apply to the relevant operators of essential services and digital service providers regardless of whether they perform the maintenance of their network and information systems internally or outsource it.

(53) 基礎サービスの運営者及びデジタルサービスプロバイダに対して資金上及び管理運営上の過大な負担を課すことを避けるため，それらの要件は，そのような措置に要する最新技術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よって示されているリスクの程度と比例すべきである。デジタルサービスプロバイダの場合においては，それらの要件は，中小規模の企業に対して適用してはならない。

To avoid imposing a disproportionate financial and administrative burden on operators of essential services and digital service providers, the requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the state of the art of such measures. In the case of digital service providers, those requirements should not apply to micro- and small enterprises.

(54) 構成国の行政機関がデジタルサービスプロバイダから提供されるサービスを利用する場合，とりわけ，クラウドコンピューティングサービスを利用する場合，その行政機関は，そのようなサービスの提供者に対し，デジタルサービスプロバイダがこの指令の義務を遵守して通常提供するようなものより以上の付加的な防護措置を要求しようと望むことがあり得る。それらの行政機関は，契約上の義務によって，そのようにできるべきである。

Where public administrations in Member States use services offered by digital service providers, in particular cloud computing services, they might wish to require from the providers of such services additional security measures beyond what digital service providers would normally offer in compliance with the requirements of this Directive. They should be able to do so by means of contractual obligations.

(55) この指令におけるオンライン市場，オンライン検索エンジン及びクラウドコンピューティング

サービスの定義は，この指令における個別の目的のための定義であり，かつ，他の法律文書を妨げない。

The definitions of online marketplaces, online search engines and cloud computing services in this Directive are for the specific purpose of this Directive, and without prejudice to any other instruments.

(56) この指令は，構成国の公的部門の組織がクラウドコンピューティングサービスと契約を締結する場合，その公的部門の組織に対して特別の安全要件を確保すべきことを要求する国内措置を，構成国が採択することを排除してはならない。そのような国内措置は，関係する公的部門の組織に対して適用されるべきであり，かつ，そのクラウドコンピューティングサービスプロバイダに対して適用してはならない。

This Directive should not preclude Member States from adopting national measures requiring public-sector bodies to ensure specific security requirements when they contract cloud computing services. Any such national measures should apply to the public-sector body concerned and not to the cloud computing service provider.

(57) 基礎サービスの運営者，とりわけ，その運営者の物理インフラとの直接の結びつきと，デジタルサービスプロバイダ，とりわけ，そのプロバイダの国境を越える性質との間の基本的な相違に鑑み，この指令は，それら2つのグループの法主体と関連する整合性のレベルに関し，区分されたアプローチをとるべきである。基礎サービスの運営者に関し，構成国は，関連する運営者を識別し，この指令に定める要件よりも厳格な要件を課し得るべきである。その適用範囲内にある全てのデジタルサービスプロバイダに対してこの指令が適用されるべきであるので，構成国は，デジタルサービスプロバイダを識別してはならない。加えて，この指令及びそれに基づいて採択される実装行為は，安全要件及び通知要件に関し，デジタルサービスプロバイダの高いレベルの整合性を確保すべきである。このことは，デジタルサービスプロバイダが，それらのプロバイダが直面し得るリスクの性質及び程度と比例的な態様で，欧州連合全域にわたり統一的な方法で取り扱われることを可能とすべきである。

Given the fundamental differences between operators of essential services, in particular their direct link with physical infrastructure, and digital service providers, in particular their cross-border nature, this Directive should take a differentiated approach with respect to the level of harmonisation in relation to those two groups of entities. For operators of essential services, Member States should be able to identify the relevant operators and impose stricter requirements than those laid down in this Directive. Member States should not identify digital service providers, as this Directive should apply to all digital service providers within its scope. In addition, this Directive and the implementing acts adopted under it should ensure a high level of harmonisation for digital service providers with respect to security and notification requirements. This should enable digital service providers to be treated in a uniform way across the Union, in a manner proportionate to their nature and the degree of risk

which they might face.

(58) この指令は，欧州連合法に基づく構成国の義務を妨げることなく，構成国が，この指令の適用範囲内にあるデジタルサービスプロバイダではない法主体に対して安全要件及び通知要件を課すことを排除してはならない。

This Directive should not preclude Member States from imposing security and notification requirements on entities that are not digital service providers within the scope of this Directive, without prejudice to Member States' obligations under Union law.

(59) 職務権限のある機関は，非公式で信頼できる情報共有の経路を維持することに適正に注意を払うべきである。職務権限のある機関に対して報告されるインシデントの公表は，脅威に関する情報提供を受ける公衆の利益と，インシデントを通知する基礎サービスの運営者及びデジタルサービスプロバイダにとってあり得る評判上または商業上の損失との適正なバランスをとるべきである。通知義務の実装において，職務権限のある機関及び CSIRT は，セキュリティ上の適切な修正が公表される前においては，その製品の脆弱性に関する情報を厳格に機密に保つ必要性に特に注意を払うべきである。

Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing. Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats against possible reputational and commercial damage for the operators of essential services and digital service providers reporting incidents. In the implementation of the notification obligations, competent authorities and the CSIRTs should pay particular attention to the need to keep information about product vulnerabilities strictly confidential, prior to the release of appropriate security fixes.

(60) デジタルサービスプロバイダは，そのプロバイダのサービス及び業務遂行の性質によって正当化される軽いタッチの事後的な監督活動に服するべきである。関係する職務権限のある機関は，それゆえ，例えば，そのデジタルサービスプロバイダ自身から，他の構成国の職務権限のある機関を含め他の職務権限のある機関から，または，そのサービスの利用者から，デジタルサービスプロバイダがこの指令の要件を遵守していないことの証拠が提供された場合に限り，とりわけ，インシデントが発生した後に限り，行動をとるべきである。それゆえ，職務権限のある機関は，デジタルサービスプロバイダを監督すべき一般的義務を負わない。

Digital service providers should be subject to light-touch and reactive *ex post* supervisory activities justified by the nature of their services and operations. The competent authority concerned should therefore only take action when provided with evidence, for example by the digital service provider itself, by another competent authority, including a competent authority of another Member State, or by a user of the service, that a digital service provider is not complying with the requirements of this

Directive, in particular following the occurrence of an incident. The competent authority should therefore have no general obligation to supervise digital service providers.

(61) 職務権限のある機関は，ネットワーク及び情報システムの安全性のレベルを評価するための十分な情報を入手する権限を含め，その機関の職務を遂行するために必要となる手段をもつべきである。

Competent authorities should have the necessary means to perform their duties, including powers to obtain sufficient information in order to assess the level of security of network and information systems.

(62) インシデントは，犯罪活動の結果かもしれず，その防止，捜査及び訴追は，基礎サービスの運営者，デジタルサービスプロバイダ，職務権限のある機関及び法執行機関の間の調整及び協力によって支えられる。あるインシデントが，欧州連合法または国内法に基づく重大な犯罪活動と関連している疑いがある場合，構成国は，基礎サービスの運営者及びデジタルサービスプロバイダが，関連する法執行機関に対し，重大犯罪の性質をもつ疑いのあるインシデントを報告することを推奨すべきである。それが適切なときは，欧州サイバー犯罪センター（EC3）及び ENISA によって，職務権限のある機関と別の構成国の法執行機関との間の調整が容易にされることが望ましい。

Incidents may be the result of criminal activities the prevention, investigation and prosecution of which is supported by coordination and cooperation between operators of essential services, digital service providers, competent authorities and law enforcement authorities. Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage operators of essential services and digital service providers to report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. Where appropriate, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the European Cybercrime Centre (EC3) and ENISA.

(63) 多くの場合において，インシデントの結果として個人データが被害を受ける。この文脈において，職務権限のある機関及びデータ保護機関は，インシデントから生ずる個人データの侵害と闘うため，全ての関連事柄に関して協力し，かつ，情報交換すべきである。

Personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents.

(64) デジタルサービスプロバイダとの関係における裁判管轄権は，関係するデジタルサービスプロバイダが欧州連合内における主たる拠点をもつ構成国に割当てられるべきである。その

構成国は，原則として，そのプロバイダが欧州連合内における本店をもつ場所と一致する。拠点とは，確実な手立てによる実効的かつ現実的な活動の実行を含意する。そのような手立ての法律上の方式，法人格をもつ支店または子会社によるか否かは，この点に関する決定的な要素ではない。この基準は，ネットワーク及び情報システムが当の場所に物理的に存在しているか否かに依拠してはならない；すなわち，そのようなシステムの存在及び利用は，それ自体としては，そのような主たる拠点を構成するものではなく，それゆえ，主たる拠点を判定するための基準ではない。

Jurisdiction in respect of digital service providers should be attributed to the Member State in which the digital service provider concerned has its main establishment in the Union, which in principle corresponds to the place where the provider has its head office in the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect. This criterion should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not criteria for determining the main establishment.

(65) 欧州連合内に拠点のないデジタルサービスプロバイダが欧州連合内でサービスを提供する場合，そのプロバイダは，代理者を指定すべきである。そのようなデジタルサービスプロバイダが欧州連合内でサービスを提供しているか否かを判定するため，そのサービスプロバイダが 1 または複数の構成国内の者に対してサービスを提供することを予定していることが明確か否かを確認すべきである。そのデジタルサービスプロバイダの Web サイトもしくはその中間介在者の Web サイトもしくは電子メールアドレスまたはそれ以外の連絡場所への欧州連合内におけるアクセスが困難であること，あるいは，そのデジタルサービスプロバイダが拠点をもつ第三国において一般的に使用されている言語が使用されていることだけでは，そのような意図の確認のためには不十分である。ただし，当該別の言語によるサービスの申込みのできる 1 または複数の構成国において一般的に使用されている言語もしくは通貨の使用，または，欧州連合内の消費者もしくは利用者の言及のような要素は，そのデジタルサービスプロバイダが欧州連合内でサービスを提供することを予定していることを明確にし得る。代理者は，そのデジタルサービスプロバイダの代わりに行動すべきであり，かつ，職務権限のある機関または CSIRT がその代理者と連絡をとれるようにすべきである。代理者は，インシデント報告を含め，この指令に基づくデジタルサービスプロバイダの義務に関してそのプロバイダの代わりに行動することのデジタルサービスプロバイダの書面による委任によって明示で指定されるべきである。

Where a digital service provider not established in the Union offers services within the Union, it should designate a representative. In order to determine whether such a digital service provider is offering services within the Union, it should be ascertained whether it is apparent that the digital

service provider is planning to offer services to persons in one or more Member States. The mere accessibility in the Union of the digital service provider's or an intermediary's website or of an email address and of other contact details, or the use of a language generally used in the third country where the digital service provider is established, is insufficient to ascertain such an intention. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the digital service provider is planning to offer services within the Union. The representative should act on behalf of the digital service provider and it should be possible for competent authorities or the CSIRTs to contact the representative. The representative should be explicitly designated by a written mandate of the digital service provider to act on the latter's behalf with regard to the latter's obligations under this Directive, including incident reporting.

(66) 安全要件を標準化することは，市場主導の過程の 1 つである。セキュリティ標準の確実な適用を確保するため，構成国は，欧州連合レベルのネットワーク及び情報システムの高いレベルの安全性を確保するための指定された標準の遵守または適合を推進すべきである。ENISA は，助言及び運用指針を通じて構成国を補助すべきである。この目的のために，欧州議会及び理事会の規則(EU) No 1025/2012[8]に従って行われるべき整合化された標準案が助けとなり得る。

Standardisation of security requirements is a market-driven process. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards so as to ensure a high level of security of network and information systems at Union level. ENISA should assist Member States through advice and guidelines. To this end, it might be helpful to draft harmonised standards, which should be done in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council [(8)].

(67) この指令の適用範囲外にある法主体は，その法主体が提供するサービスに対して大きな影響をもつインシデントを経験し得る。そのようなインシデントの発生を通知することが公共の利益に適うとそれらの法主体が判断する場合，それらの法主体は，任意で，そのようにできるべきである。そのような処理が構成国に対して不適切または不適正な負担を負わせるものではないときは，そのような通知は，職務権限のある機関または CSIRT によって処理されるべきである。

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

Entities falling outside the scope of this Directive may experience incidents having a significant impact on the services they provide. Where those entities consider that it is in the public interest to notify the occurrence of such incidents, they should be able to do so on a voluntary basis. Such notifications should be processed by the competent authority or the CSIRT where such processing does not constitute a disproportionate or undue burden on the Member States concerned.

(68) この指令の実装のための統一的な条件を確保するため，協力グループの稼働のため，並びに，デジタルサービスプロバイダに対して適用可能な安全要件及び通知要件のために必要な手続上の手立てを定めるための実装権限は，欧州委員会に対して与えられるべきである。それらの実装権限は，欧州議会及び理事会の規則（EU） No 182/2011[9]に従って行使されるべきである。協力グループの稼働のために必要な手続上の手立てに関する実装行為を採択する際，欧州委員会は，ENISA の意見を最大限考慮に入れるべきである。

In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission to lay down the procedural arrangements necessary for the functioning of the Cooperation Group and the security and notification requirements applicable to digital service providers. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council(9). When adopting implementing acts related to the procedural arrangements necessary for the functioning of the Cooperation Group, the Commission should take the utmost account of the opinion of ENISA.

(69) デジタルサービスプロバイダに対する安全要件に関する実装行為を採択する際，欧州委員会は，ENISA の意見を最大限考慮に入れるべきであり，かつ，関連する利害関係者と協議すべきである。更に，欧州委員会は，以下の例示を考慮に入れることが推奨される：システムと施設の安全性に関するものとして：物理的及び周辺環境上の安全性，用品の安全性，ネットワーク及び情報システムのアクセス管理，並びに，ネットワーク及び情報システムの完全性；インシデント対応に関するものとして：インシデント対応手順，インシデント検出能力，インシデント報告及びインシデント通知；事業継続性管理に関するものとして：サービス提供継続性戦略及び危機管理計画，災害復旧能力；並びに，監視，監査及試験に関するものとして：監視及び履歴管理の基本方針，演習危機管理計画，ネットワーク及び情報システムの試験，安全性評価及び法令遵守の監視。

When adopting implementing acts on the security requirements for digital service providers, the Commission should take the utmost account of the opinion of ENISA and should consult interested stakeholders. Moreover, the Commission is encouraged to take into account the following examples: as regards security of systems and facilities: physical and environmental security, security of supplies,

9 欧州委員会による実装権限の行使の構成国による管理の仕組みに関する規定及び基本原則を定める欧州議会及び理事会の 2011 年 2 月 16 日の規則(EU) No 182/2011（OJ L 55, 28.2.2011, p.13）.

access control to network and information systems and integrity of network and information systems; as regards incident handling: incident-handling procedures, incident detection capability, incident reporting and communication; as regards business continuity management: service continuity strategy and contingency plans, disaster recovery capabilities; and as regards monitoring, auditing and testing: monitoring and logging policies, exercise contingency plans, network and information systems testing, security assessments and compliance monitoring.

(70) この指令の実装において，欧州委員会は，この指令の適用のある分野において欧州連合レベルで設けられている関連部門の委員会及び関連組織との間で適切に連絡すべきである。

In the implementation of this Directive, the Commission should liaise as appropriate with relevant sectoral committees and relevant bodies set up at Union level in the fields covered by this Directive.

(71) 欧州委員会は，とりわけ，社会，政治，技術または市場の条件の変化に照らして修正の要否を判断するという観点から，関連する利害関係者と協議した上で，定期的に，この指令を見直すべきである。

The Commission should periodically review this Directive, in consultation with interested stakeholders, in particular with a view to determining the need for modification in the light of changes to societal, political, technological or market conditions.

(72) リスク及びインシデントに関する情報の協力グループ内及び CSIRT ネットワーク内における共有，並びに，職務権限のある国内機関または CSIRT に対するインシデント通知の要件の遵守は，個人データの処理を要し得る。そのような処理は，欧州議会及び理事会の指令 95/46/EC[10]及び欧州議会及び理事会の規則(EC) No45/2001[11]を遵守すべきである。この指令を適用する際，欧州議会及び理事会の規則(EC) No1049/2001[12]が適切に適用されるべきである。

Such processing should comply with Directive 95/46/EC of the European Parliament and the Council (10) and Regulation (EC) No 45/2001 of the European Parliament and of the Council (11). In the application of this Directive, Regulation (EC) No 1049/2001 of the European Parliament and of

10 個人データの処理と関連する個人の保護及びそのデータの支障のない移動に関する欧州議会及び理事会の 1995 年 10 月 24 日の指令 95/46/EC（OJ L 281, 23.11.1995, p.31）.

11 欧州連合の機関及び組織による個人データの処理と関連する個人の保護及びそのデータの支障のない移動に関する欧州議会及び理事会の 2000 年 12 月 18 日の規則(EC) No 45/2001（OJ L 8, 12.1.2001, p.1）.

12 欧州議会，理事会及び欧州委員会の文書への公衆のアクセス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）.

the Council [12] should apply as appropriate.

(73) 欧州データ保護監督官は，規則(EC) No 45/2001 の第 28 条第 2 項に従って協議し，2013 年 6 月 14 日に意見書[13]を提出した。

The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 14 June 2013 [13].

(74) この指令の目的，すなわち，ネットワーク及び情報システムの共通の高いレベルの安全性を達成することは，構成国によっては十分に達成され得ず，その活動の効果のゆえに，欧州連合レベルにおいてより良く達成され得るので，欧州連合は，欧州連合条約の第 5 条に定める補完性の原則に従い，措置を採択できる。同条に定める比例性の原則に従い，この指令は，その目的を達成するために必要なところを超えることがない。

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

(75) この指令は，基本的な権利を尊重し，欧州連合の基本権憲章によって認められた基本原則，とりわけ，私生活の尊重及び情報伝達の権利，個人データの保護，事業活動の自由，財産権，裁判所における実効的な救済の権利及び聴聞を受ける権利を尊重する。この指令は，これらの権利及び基本原則に従って実装されるべきである，

This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive should be implemented in accordance with those rights and principles,

以上のとおりであるので，この指令を採択する：

HAVE ADOPTED THIS DIRECTIVE:

13 OJ C 32, 4.2.2014, p. 19.

第 I 章 総則的な規定
Chapter I General Provisions

第 1 条 対象事項及び適用範囲
Article 1 Subject matter and scope

1. この指令は，域内市場の稼働を向上させるための欧州連合内におけるネットワーク及び情報システムの共通の高いレベルの安全性を達成するための措置を定める。

   This Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market.

2. その目的のために，この指令は：
   (a) ネットワーク及び情報システムの安全性に関する国内戦略を採択すべき全ての構成国の義務を定め；
   (b) 構成国間における戦略上の協力と情報交換を支援及び容易にし，かつ，構成国間における信頼と信任を発展させるための協力グループを創設し；
   (c) 構成国間における信頼と信任の発展に寄与し，かつ，迅速かつ実効的な業務遂行上の協力を促進するためのコンピュータセキュリティインシデント対応チームのネットワーク（「CSIRT ネットワーク」）を創設し；
   (d) 基礎サービスの運営者及びデジタルサービスプロバイダの安全要件及び通知要件を設け；
   (e) ネットワーク及び情報システムの安全性と関連する職務をもつ職務権限のある国内機関，単一連絡部局及び CSIRT を設置すべき構成国の義務を定める。

   To that end, this Directive:
   (a) lays down obligations for all Member States to adopt a national strategy on the security of network and information systems;
   (b) creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them;
   (c) creates a computer security incident response teams network (‘CSIRTs network’) in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation;
   (d) establishes security and notification requirements for operators of essential services and for digital service providers;
   (e) lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information

systems.

3. この指令に定める安全要件及び通知要件は，指令 2002/21/EC の第 13 条 a 及び第 13 条 b の要件に服する事業者に対して，または，規則(EU) No 910/2014 の第 19 条の要件に服する信頼サービスプロバイダに対して適用してはならない。

The security and notification requirements provided for in this Directive shall not apply to undertakings which are subject to the requirements of Articles 13a and 13b of Directive 2002/21/EC, or to trust service providers which are subject to the requirements of Article 19 of Regulation (EU) No 910/2014.

4. この指令は，理事会指令 2008/114/EC[14]並びに欧州議会及び理事会の指令 2011/93/EU[15]及び指令 2013/40/EU[16]を妨げることなく適用される。

This Directive applies without prejudice to Council Directive 2008/114/EC[(14)] and Directives 2011/93/EU[(15)] and 2013/40/EU[(16)] of the European Parliament and of the Council.

5. TFEU の第 346 条を妨げることなく，営業秘密に関する規定のような欧州連合及び構成国の規定により秘密である情報は，この指令の適用のためにそのような交換が必要となる場合に限り，欧州委員会及びそれ以外の関連機関との間で交換される。交換される情報は，そのような交換の目的と関連性があり，かつ，比例するものに限定される。そのような情報交換は，当該情報の機密性を維持し，かつ，基礎サービスの運営者及びデジタルサービスプロバイダの安全及び商業的利益を保護するものとする。

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

---

[14] 欧州の重要インフラの識別及び設計並びにそれらの保護の向上の必要性評価に関する 2008 年 12 月 8 日の理事会指令 2008/114/EC（OJ L 345, 23.12.2008, p.75）.

[15] 児童の性的虐待と性的搾取及び児童ポルノとの闘いに関する，並びに，理事会枠組み決定 2004/68/JHA を廃止する 2011 年 12 月 13 日の欧州議会及び理事会の指令 2011/93/EU（OJ L 335, 17.12.2011, p.1）.

[16] 情報システムに対する攻撃に関する，及び，理事会枠組み指令 2005/222/JHA を廃止する 2013 年 8 月 12 日の欧州議会及び理事会の指令 2013/40/EU（OJ L 218, 14.8.2013, p.8）.

6. この指令は，その情報の開示が構成国の保安の必須の利益に反するとその構成国が判断する情報を防護する活動，法と秩序を維持するための活動，とりわけ，犯罪行為の捜査，検知及び訴追をできるようにするための活動を含め，その構成国の必須の国家機能を防護するため，とりわけ，国家安全保障を防護するために行われる活動を妨げない。

This Directive is without prejudice to the actions taken by Member States to safeguard their essential State functions, in particular to safeguard national security, including actions protecting information the disclosure of which Member States consider contrary to the essential interests of their security, and to maintain law and order, in particular to allow for the investigation, detection and prosecution of criminal offences.

7. 基礎サービスの運営者もしくはデジタルサービスプロバイダに対してそのネットワーク及び情報システムの安全を確保すること及びインシデントを通知することを欧州連合の部門別の法行為が要求する場合，そのような要件がこの指令に定める義務と少なくとも均等であることを条件として，当該欧州連合の部門別の法行為の当該条項が適用される。

Where a sector-specific Union legal act requires operators of essential services or digital service providers either to ensure the security of their network and information systems or to notify incidents, provided that such requirements are at least equivalent in effect to the obligations laid down in this Directive, those provisions of that sector-specific Union legal act shall apply.

第 2 条 個人データの処理

Article 2 Processing of personal data

1. この指令による個人データの処理は，指令 95/46/EC に従って遂行される。

Processing of personal data pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC.

2. この指令による欧州連合の機関及び組織による個人データの処理は，規則(EC) No 45/2001 に従って遂行される。

Processing of personal data by Union institutions and bodies pursuant to this Directive shall be carried out in accordance with Regulation (EC) No 45/2001.

第 3 条 ミニマムの整合性

Article 3 Minimum harmonisation

第 16 条第 10 項及び欧州連合法に基づく構成国の義務を妨げることなく，構成国は，ネットワーク及び情報システムのより高いレベルの安全性を達成するための条項を採択または維持し得る。

Without prejudice to Article 16(10) and to their obligations under Union law, Member States may adopt or maintain provisions with a view to achieving a higher level of security of network and information systems.

第 4 条 定義

Article 4 Definitions

この指令の目的のために，以下の定義が適用される：

(1) 「ネットワーク及び情報システム」とは，以下のもののことを意味し：
   (a) 指令 2002/21/EC 第 2 条(a)の意味における電子通信ネットワーク；
   (b) 機器または相互接続されもしくは関連する機器のグループであって，その中の 1 もしくは複数のものがプログラムによってデジタルデータの自動処理を実行するもの；または
   (c) (a)及び(b)に含まれる構成要素の運用，使用，保護及び維持管理のために，それらの構成要素によって記録保存され，処理され，検索されまたは送信されるデジタルデータ；

(2) 「ネットワーク及び情報システムの安全性」とは，当該ネットワーク及び情報システムによって提供されまたはそれを介してアクセス可能な，記録保存されもしくは送信されもしくは処理されるデータまたはその関連サービスの可用性，真正性，完全性及び機密性を損なう全ての行為に対し，所定の機密性の程度に応じて抗するためのネットワーク及び情報システムの能力のことを意味し；

(3) 「ネットワーク及び情報システムの安全性に関する国内戦略」とは，ネットワーク及び情報システムの安全性に関する戦略上の目標及び優先事項を定める構成国レベルの枠組みのことを意味し；

(4) 「基礎サービスの運営者」とは，別紙 II に示すタイプの公的部門または民間部門の法主体であって，第 5 条第 2 項に定める基準に適合するもののことを意味し；

(5) 「デジタルサービス」とは，欧州議会及び理事会の指令(EU) 2015/1535[17]の第 1 条第 1 項(b)の意味におけるサービスであって，別紙 III に列挙するタイプのサービスのことを意味し；

(6) 「デジタルサービスプロバイダ」とは，デジタルサービスを提供する法人のことを意味し；

(7) 「インシデント」とは，ネットワーク及び情報システムの安全性に対して現実の負の影響

[17] 情報社会サービスに関する技術の法令及び規定の分野における情報提供の手続を定める 2015 年 9 月 9 日の欧州議会及び理事会指令 (EU) 2015/1535（OJ L 241, 17.9.2015, p.1）.

をもつ出来事のことを意味し；

(8) 「インシデント対応」とは，インシデントの検出，分析及び抑止を支援する全ての手順，並びに，そのインシデントへの対応のことを意味し；

(9) 「リスク」とは，ネットワーク及び情報システムの安全性に対して潜在的な負の影響をもつと合理的に識別可能な状況または出来事のことを意味し；

(10) 「代理者」とは，欧州連合内に拠点をもたないデジタルサービスプロバイダの代わりに行動するために明示で指定された欧州連合内に拠点のある自然人または法人であって，職務権限のある国内機関または CSIRT によって，この指令に基づく当該デジタルサービスプロバイダの義務に関してそのデジタルサービスプロバイダに代わりに名宛人とされ得る者のことを意味し；

(11) 「標準」とは，規則(EU) No.1025/2012 の第 2 条第 1 号の意味における標準のことを意味し；

(12) 「仕様」とは，規則(EU) No.1025/2012 の第 2 条第 4 号の意味における技術仕様のことを意味し；

(13) 「インターネット相互接続点（IXP）」とは，主としてインターネットトラフィックの交換を容易にする目的のために，複数の独立した自律システムの相互接続を実現可能にするネットワーク機能のことを意味し；IXP は，自律システムのために限って相互接続を提供し；IXP は，参加するどのペアの自律システムを通過するインターネットトラフィックに対しても，第三の自律システムを通過することを要求せず，かつ，そのようなトラフィックの修正またはそれ以外の干渉をせず；

(14) 「ドメイン名システム（DNS）」とは，ネットワーク内の階層化された分散的な命名システムであって，ドメイン名のクエリーを参照するもののことを意味し；

(15) 「DNS サービスのプロバイダ」とは，インターネット上において DNS サービスを提供する法主体のことを意味し；

(16) 「トップレベルドメイン名レジストリ」とは，特定のトップレベルドメイン（TLD）の下にあるインターネットドメイン名の登録を管理及び運営する法主体のことを意味し；

(17) 「オンライン市場」とは，欧州議会及び理事会の指令 2013/11/EU[18]の第 4 条第 1 項の(a)及び(b)にそれぞれ定める消費者及びまたは取引業者が，オンライン市場の Web サイト上において，または，オンライン市場から提供されるコンピュータ処理サービスを使用する取引業者の Web サイト上において，当該取引業者との間のオンライン売買契約または役務提供契約を締結できるようにするデジタルサービスのことを意味し；

(18) 「オンライン検索エンジン」とは，キーワード，語句もしくはそれ以外の入力の方式による事項のクエリーを基礎として，原則として，全ての Web サイトまたは特定の言語で書かれた Web サイトの検索を利用者が実行できるようにし，かつ，要求されたコンテントに関する情報を見つけ得るリンクを返すデジタルサービスのことを意味し；

[18] 消費者紛争のための裁判外紛争解決手続に関する，並びに，規則(EC) No 2006/2004 及び指令 2009/22/EC を改正する欧州議会及び理事会の 2013 年 5 月 21 日の指令 2013/11/EU（消費者 ADR に関する指令）(OJ L 165, 18.6.2013, p.63).

(19) 「クラウドコンピューティングサービス」とは，共有可能なコンピュータ資源の拡張可能で伸縮可能なプールへのアクセスをできるようにするデジタルサービスのことを意味する。

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

(1) ‘network and information system’ means:
   (a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC;
   (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or
   (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

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

(3) ‘national strategy on the security of network and information systems’ means a framework providing strategic objectives and priorities on the security of network and information systems at national level;

(4) ‘operator of essential services’ means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2);

(5) ‘digital service’ means a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council[17] which is of a type listed in Annex III;

(6) ‘digital service provider’ means any legal person that provides a digital service;

(7) ‘incident’ means any event having an actual adverse effect on the security of network and information systems;

(8) ‘incident handling’ means all procedures supporting the detection, analysis and containment of an incident and the response thereto;

(9) ‘risk’ means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems;

(10) ‘representative’ means any natural or legal person established in the Union explicitly designated to act on behalf of a digital service provider not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the digital service provider with regard to the obligations of that digital service provider under this Directive;

(11) ‘standard’ means a standard within the meaning of point (1) of Article 2 of Regulation (EU) No 1025/2012;

(12) ‘specification’ means a technical specification within the meaning of point (4) of Article 2 of Regulation (EU) No 1025/2012;

(13) ‘internet exchange point (IXP)’ means a network facility which enables the interconnection of

more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;

(14) ‘domain name system (DNS)’ means a hierarchical distributed naming system in a network which refers queries for domain names;

(15) ‘DNS service provider’ means an entity which provides DNS services on the internet;

(16) ‘top-level domain name registry’ means an entity which administers and operates the registration of internet domain names under a specific top-level domain (TLD);

(17) ‘online marketplace’ means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council[18] to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace;

(18) ‘online search engine’ means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found;

(19) ‘cloud computing service’ means a digital service that enables access to a scalable and elastic pool of shareable computing resources.

第 5 条 基礎サービスの運営者の識別

Article 5 Identification of operators of essential services

1. 2018 年 11 月 9 日までに，別紙 II に示す部門毎及び副部門毎に，構成国は，その領土上に拠点のある基礎サービスの運営者を識別する。

By 9 November 2018, for each sector and subsector referred to in Annex II, Member States shall identify the operators of essential services with an establishment on their territory.

2. 第 4 条第 4 号に示す基礎サービスの運営者の識別のための基準は，以下のとおりとする：
   (a) 法主体が，重要な社会的活動及びまたは重要な経済的活動の維持にとって必須のサービスを提供していること；
   (b) 当該サービスの提供が，ネットワーク及び情報システムに依拠していること；並びに
   (c) 当該サービスの提供に対して，インシデントが大きな破壊的影響をもち得ること。

The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, shall be as follows:

(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
(b) the provision of that service depends on network and information systems; and
(c) an incident would have significant disruptive effects on the provision of that service.

3. 第 1 項の目的のために，各構成国は，第 2 項(a)に示すサービスのリストを作成する。

For the purposes of paragraph 1, each Member State shall establish a list of the services referred to in point (a) of paragraph 2.

4. 第 1 項の目的のために，複数の構成国において法主体が第 2 項(a)に示すサービスを提供する場合，それらの構成国は，相互に，協議に入る。この協議は，識別に関する決定が行われる前に行われる。

For the purposes of paragraph 1, where an entity provides a service as referred to in point (a) of paragraph 2 in two or more Member States, those Member States shall engage in consultation with each other. That consultation shall take place before a decision on identification is taken.

5. 構成国は，定期的に，2018 年 5 月 9 日以降は少なくとも 2 年毎に，識別された基礎サービスの運営者のリストを見直し，また，それが適切なときは，そのリストをアップデートする。

Member States shall, on a regular basis, and at least every two years after 9 May 2018, review and, where appropriate, update the list of identified operators of essential services.

6. 協力グループの役割は，第 11 条に示す職務に従い，基礎サービスの運営者の識別過程において一貫性のあるアプローチをとる上で，構成国を支援することである。

The role of the Cooperation Group shall be, in accordance with the tasks referred to in Article 11, to support Member States in taking a consistent approach in the process of identification of operators of essential services.

7. 第 23 条に示す見直しの目的のために，かつ，2018 年 11 月 9 日までに，及び，その後は 2 年毎に，構成国は，欧州委員会に対し，この指令の実装，とりわけ，基礎サービスの運営者の指定のための構成国のアプローチの一貫性を欧州委員会が評価できるようにするために必要となる情報を提出する。その情報は，少なくとも，以下のものを含める：
(a) 基礎サービスの運営者の識別をできるようにする国内措置；
(b) 第 3 項に示すサービスのリスト；
(c) 別紙 II に示す部門別別に識別された基礎サービスの運営者の数及び当該部門との関係におけるその重要性の表示；

(d) それが存在するときは，第 6 条第 1 項(a)に示す当該サービスに依拠する利用者の数を示し，または，第 6 条第 1 項(f)に示す当該特定の基礎サービスの運営者の重要性を示すことによって，関連する供給レベルを判定するための閾値。

For the purpose of the review referred to in Article 23 and by 9 November 2018, and every two years thereafter, Member States shall submit to the Commission the information necessary to enable the Commission to assess the implementation of this Directive, in particular the consistency of Member States' approaches to the identification of operators of essential services. That information shall include at least:

(a) national measures allowing for the identification of operators of essential services;
(b) the list of services referred to in paragraph 3;
(c) the number of operators of essential services identified for each sector referred to in Annex II and an indication of their importance in relation to that sector;
(d) thresholds, where they exist, to determine the relevant supply level by reference to the number of users relying on that service as referred to in point (a) of Article 6(1) or to the importance of that particular operator of essential services as referred to in point (f) of Article 6(1).

同等の情報提供に貢献するため，欧州委員会は，ENISA の意見を最大限考慮に入れた上で，本項に示す情報のためのパラメータに関する適切な技術上の運用指針を採択できる。

In order to contribute to the provision of comparable information, the Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical guidelines on parameters for the information referred to in this paragraph.

第 6 条 大きな破壊的影響

Article 6 Significant disruptive effect

1. 第 5 条第 2 項(c)に示す破壊的影響の大きさを判定する際，構成国は，少なくとも，以下の部門横断的な要素を考慮に入れる：
   (a) 関係する法主体によって提供されるサービスに依存する利用者の数；
   (b) 当該法主体によって提供されるサービスに対する別紙 II に示す別の部門の依存関係；
   (c) 経済活動及び社会活動または公共の安全に対してインシデントがもち得る程度及び持続時間の面における影響；
   (d) 当該法主体の市場占有率；
   (e) インシデントによって影響を受ける可能性のある地域に関する地理的な広がり；
   (f) 当該サービス提供の代替手段の利用可能性を考慮に入れた上で，十分なレベルでそのサービス提供を維持するためのその法主体の重要性。

When determining the significance of a disruptive effect as referred to in point (c) of Article 5(2),

Member States shall take into account at least the following cross-sectoral factors:

(a) the number of users relying on the service provided by the entity concerned;
(b) the dependency of other sectors referred to in Annex II on the service provided by that entity;
(c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;
(d) the market share of that entity;
(e) the geographic spread with regard to the area that could be affected by an incident;
(f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

2. インシデントが大きな破壊的影響をもつか否かを判断するため，構成国は，それが適切なときは，部門別の要素も考慮に入れる。

In order to determine whether an incident would have a significant disruptive effect, Member States shall also, where appropriate, take into account sector-specific factors.

第Ⅱ章 ネットワーク及び情報システムの安全性に関する国内枠組み

Chapter II National Frameworks on the Security of Network and Information Systems

第 7 条 ネットワーク及び情報システムの安全性に関する国内戦略

Article 7 National strategy on the security of network and information systems

1. 各構成国は，ネットワーク及び情報システムの高いレベルの安全性を達成及び維持し，かつ，少なくとも，別紙 II に示す部門及び別紙 III に示すサービスを包摂するという観点から戦略目標並びに適切な基本方針及び法令上の措置を定めるネットワーク及び情報システムの安全性に関する国内戦略を採択する。ネットワーク及び情報システムの安全性に関する国内戦略は，とりわけ，下記の検討課題に対処するものとする：
   (a) ネットワーク及び情報システムの安全性に関する国内戦略上の目標及び優先事項；
   (b) 政府機関及びそれ以外の関係者の役割及び責務を含め，ネットワーク及び情報システムの安全性に関する国内戦略上の目標及び優先事項を達成するための統治枠組み；
   (c) 公的部門と民間部門の間の協力を含め，準備態勢，対応及び復旧と関連する措置の指示；
   (d) ネットワーク及び情報システムの安全性に関する国内戦略と関連する教育，認識向上及び訓練計画の表示；
   (e) ネットワーク及び情報システムの安全性に関する国内戦略と関連する調査研究計画及び開発計画の表示；
   (f) リスクを特定するためのリスク評価計画；
   (g) ネットワーク及び情報システムの安全性に関する国内戦略の実装に関与する様々な関係者のリスト。

Each Member State shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems and covering at least the sectors referred to in Annex II and the services referred to in Annex III. The national strategy on the security of network and information systems shall address, in particular, the following issues:

(a) the objectives and priorities of the national strategy on the security of network and information systems;
(b) a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors;
(c) the identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors;
(d) an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems;
(e) an indication of the research and development plans relating to the national strategy on the security of network and information systems;
(f) a risk assessment plan to identify risks;
(g) a list of the various actors involved in the implementation of the national strategy on the security of network and information systems.

2. 構成国は，ネットワーク及び情報システムの安全性に関する国内戦略の策定に際し，ENISA の補助を要請できる。

Member States may request the assistance of ENISA in developing national strategies on the security of network and information systems.

3. 構成国は，欧州委員会に対し，その採択から 3 か月以内に，ネットワーク及び情報システムの安全性に関する国内戦略を送付する。そのようにする際，構成国は，国家安全保障と関連する戦略の要素を除外できる。

Member States shall communicate their national strategies on the security of network and information systems to the Commission within three months from their adoption. In so doing, Member States may exclude elements of the strategy which relate to national security.

第 8 条　職務権限のある国内機関及び単一連絡部局

Article 8 National competent authorities and single point of contact

1. 各構成国は，少なくとも別紙 II に示す部門及び別紙 III に示すサービスを包摂し，ネットワー

ク及び情報システムの安全性に関する 1 または複数の職務権限のある機関（「職務権限のある機関」）を指定する。構成国は，既存の機関または複数の機関に対してその役割を割当て得る。

Each Member State shall designate one or more national competent authorities on the security of network and information systems (‘competent authority’), covering at least the sectors referred to in Annex II and the services referred to in Annex III. Member States may assign this role to an existing authority or authorities.

2. 職務権限のある機関は，国内レベルでこの指令の適用を監視する。

The competent authorities shall monitor the application of this Directive at national level.

3. 各構成国は，ネットワーク及び情報システムの安全性に関する単一の国内連絡部局（「単一連絡部局」）を指定する。構成国は，既存の機関にこの役割を割当て得る。構成国が 1 の職務権限のある機関のみを指定する場合，当該職務権限のある機関は，単一連絡部局ともなる。

Each Member State shall designate a national single point of contact on the security of network and information systems (‘single point of contact’). Member States may assign this role to an existing authority. Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact.

4. 単一連絡部局は，構成国の機関の国境を越える協力を確保するための連絡機能，他の構成国の関連機関との間の連絡機能並びに第 11 条に示す協力グループ及び第 12 条に示す CSIRT ネットワークとの間の連絡機能を遂行する。

The single point of contact shall exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group referred to in Article 11 and the CSIRTs network referred to in Article 12.

5. 構成国は，それらの機関に割当てられた職務を実効的かつ効率的な態様で遂行し，それによって，この指令の目的を満たすため，職務権限のある機関及び単一連絡部局が十分な資源をもつことを確保する。構成国は，協力グループ内における任命された代表の実効的，効率的かつ安全な協力を確保する。

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

secure cooperation of the designated representatives in the Cooperation Group.

6. 職務権限のある機関及び単一連絡部局は，それが適切なときは，かつ，国内法に従い，国内の関連法執行機関及び国内個人データ保護機関と協議し，かつ，協力する。

The competent authorities and single point of contact shall, whenever appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities and national data protection authorities.

7. 各構成国は，欧州委員会に対し，遅滞なく，職務権限のある機関及び単一連絡部局の指定，それらの職務，並びに，その後の変更を通知する。各構成国は，職務権限のある機関及び単一連絡部局の指定を公表する。欧州委員会は，指定された単一連絡部局のリストを公表する。

Each Member State shall notify to the Commission without delay the designation of the competent authority and single point of contact, their tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authority and single point of contact. The Commission shall publish the list of designated single points of contacts.

第 9 条 コンピュータセキュリティインシデント対応チーム（CSIRT）

Article 9 Computer security incident response teams (CSIRTs)

1. 各構成国は，別紙 I の第 1 号に定める要件を遵守し，少なくとも，別紙 II に示す部門及び別紙 III に示すサービスを包摂し，良好に定義された手順に従ったリスク及びインシデント対応に関して職責を負う 1 または複数の CSIRT を指定する。CSIRT は，職務権限のある機関内に設けられ得る。

Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority.

2. 構成国は，CSIRT が，別紙 I の第 2 号に定めるその職務を実効的に遂行するための十分な資源をもつことを確保する。

Member States shall ensure that the CSIRTs have adequate resources to effectively carry out their tasks as set out in point (2) of Annex I.

構成国は，第 12 条に示す CSIRT ネットワーク内におけるその構成国の CSIRT の実効的，

効率的かつ安全な協力を確保する。

Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 12.

3. 構成国は，その構成国の CSIRT が，国内レベルで，適切，安全かつ回復力のある通信インフラ及び情報インフラへのアクセスをもつことを確保する。

Member States shall ensure that their CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level.

4. 構成国は，欧州委員会に対し，その構成国の CSIRT の権限及びインシデント対応プロセスの主要な構成要素を通知する。

Member States shall inform the Commission about the remit, as well as the main elements of the incident-handling process, of their CSIRTs.

5. 構成国は，国内 CSIRT の発展において，ENISA の補助を要請できる。

Member States may request the assistance of ENISA in developing national CSIRTs.

第 10 条 国内レベルの協力

Article 10 Cooperation at national level

1. それらが区分されている場合，同一の構成国の職務権限のある機関，単一連絡部局及び CSIRT は，この指令に定める義務の履行に関し，協力する。

Where they are separate, the competent authority, the single point of contact and the CSIRT of the same Member State shall cooperate with regard to the fulfilment of the obligations laid down in this Directive.

2. 構成国は，職務権限のある機関または CSIRT のいずれかが，この指令によって提出されるインシデント通知を受けることを確保する。CSIRT がその通知を受けてはならないことを構成国が定める場合，その CSIRT は，その職務を満たすために必要な範囲内で，第 14 条第 3 項及び第 5 項により基礎サービスの運営者から通知され，または，第 16 条第 3 項及び第 6 項によりデジタルサービスプロバイダから通知されるインシデントに関するデータへのアクセスが認められる。

Member States shall ensure that either the competent authorities or the CSIRTs receive incident

notifications submitted pursuant to this Directive. Where a Member State decides that CSIRTs shall not receive notifications, the CSIRTs shall, to the extent necessary to fulfil their tasks, be granted access to data on incidents notified by operators of essential services, pursuant to Article 14(3) and (5), or by digital service providers, pursuant to Article 16(3) and (6).

3. 構成国は，職務権限のある機関または CSIRT が，この指令によって提出されるインシデント通知に関し，単一連絡部局に連絡することを確保する。

Member States shall ensure that the competent authorities or the CSIRTs inform the single points of contact about incident notifications submitted pursuant to this Directive.

単一連絡部局は，2018 年 8 月 9 日までに，及び，その後は毎年，協力グループに対し，通知の数及び通知されたインシデントの性質，第 14 条第 3 項及び第 5 項並びに第 16 条第 3 項及び第 6 項に従って行われた活動を含め，受けた通知に関する概要報告書を提出する。

By 9 August 2018, and every year thereafter, the single point of contact shall submit a summary report to the Cooperation Group on the notifications received, including the number of notifications and the nature of notified incidents, and the actions taken in accordance with Article 14(3) and (5) and Article 16(3) and (6).

第Ⅲ章 協力

Chapter III Cooperation

第 11 条 協力グループ

Article 11 Cooperation Group

1. 構成国間における戦略的な協力及び情報の交換を支援し容易にするため，信頼と信任を発展させるため，そして，欧州連合内におけるネットワーク及び情報システムの共通で高いレベルの安全性を達成するという観点から，ここに，協力グループが設置される。

In order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence, and with a view to achieving a high common level of security of network and information systems in the Union, a Cooperation Group is hereby established.

協力グループは，第 3 項第 2 副項に示す 2 年毎の業務計画に基づき，その職務を遂行する。

The Cooperation Group shall carry out its tasks on the basis of biennial work programmes as referred

to in the second subparagraph of paragraph 3.

2. 協力グループは，構成国の代表，欧州委員会及び ENISA によって構成される。

The Cooperation Group shall be composed of representatives of the Member States, the Commission and ENISA.

それが適切なときは，協力グループは，関連する利害関係者の代表に対し，協力グループの作業への参加を招請できる。

Where appropriate, the Cooperation Group may invite representatives of the relevant stakeholders to participate in its work.

欧州委員会は，事務局を提供する。

The Commission shall provide the secretariat.

3. 協力グループは，以下の職務をもつ：
   (a) 第 12 条に基づいて設置される CSIRT ネットワークの活動のための戦略上の運用指針を提供すること；
   (b) 第 14 条第 3 項及び第 5 項並びに第 16 条第 3 項及び第 6 項に示すインシデント通知と関連する情報の交換に関するベストプラクティスを交換すること；
   (c) 構成国間においてベストプラクティスを交換すること，並びに，ENISA と共働して，ネットワーク及び情報システムの安全性を確保する能力の構築において構成国を補助すること；
   (d) 構成国の実現能力及び準備態勢に関して討議すること，任意で，ネットワーク及び情報システムの安全性に関する国内戦略及び CSIRT の実効性を評価すること，並びに，ベストプラクティスを指示すること；
   (e) 意識向上及び訓練に関する情報及びベストプラクティスを交換すること；
   (f) ネットワーク及び情報システムの安全性と関連する調査研究及び開発に関する情報及びベストプラクティスを交換すること；
   (g) それが関連するときは，関連する欧州連合の機関，組織，事務局及び部局との間で，ネットワーク及び情報システムの安全性と関連する事項に関し，経験を交換すること；
   (h) 関連する欧州標準機関の代表との間で，第 19 条に示す標準及び仕様に関し，討議すること；
   (i) リスク及びインシデントに関するベストプラクティス情報を収集すること；
   (j) 年次で，第 10 条第 3 項第 2 副項に示す概要報告書を検討すること；
   (k) ENISA によって行われる作業を含め，ネットワーク及び情報システムの安全性と関連する演習，教育計画及び訓練と関連して実施される作業に関し，討議すること；

(l) ENISA の補助を得て，リスク及びインシデントと関連する国境を越える依存関係と関係するものを含め，構成国による基礎サービスの運営者の識別と関連するベストプラクティスを交換すること；
(m) 第 14 条及び第 16 条に示す通知を報告するための様式に関して討議すること。

The Cooperation Group shall have the following tasks:
(a) providing strategic guidance for the activities of the CSIRTs network established under Article 12;
(b) exchanging best practice on the exchange of information related to incident notification as referred to in Article 14(3) and (5) and Article 16(3) and (6);
(c) exchanging best practice between Member States and, in collaboration with ENISA, assisting Member States in building capacity to ensure the security of network and information systems;
(d) discussing capabilities and preparedness of the Member States, and, on a voluntary basis, evaluating national strategies on the security of network and information systems and the effectiveness of CSIRTs, and identifying best practice;
(e) exchanging information and best practice on awareness-raising and training;
(f) exchanging information and best practice on research and development relating to the security of network and information systems;
(g) where relevant, exchanging experiences on matters concerning the security of network and information systems with relevant Union institutions, bodies, offices and agencies;
(h) discussing the standards and specifications referred to in Article 19 with representatives from the relevant European standardisation organisations;
(i) collecting best practice information on risks and incidents;
(j) examining, on an annual basis, the summary reports referred to in the second subparagraph of Article 10(3);
(k) discussing the work undertaken with regard to exercises relating to the security of network and information systems, education programmes and training, including the work done by ENISA;
(l) with ENISA's assistance, exchanging best practice with regard to the identification of operators of essential services by the Member States, including in relation to cross-border dependencies, regarding risks and incidents;

2018 年 2 月 9 日までに，及び，その後は 2 年毎に，協力グループは，協力グループの目的及び職務の実装のために実施されるべき活動に関する業務計画を策定する。その業務計画は，この指令の目的と一貫性のあるものとする。

By 9 February 2018 and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks, which shall be consistent with the objectives of this Directive.

4. 第 23 条に示す見直しの目的のために，かつ，2018 年 8 月 9 日までに，及び，その後は 1 年半毎に，協力グループは，本条に基づいて求められる戦略上の協力から得られた経験を評価する報告書を準備する。

For the purpose of the review referred to in Article 23 and by 9 August 2018, and every year and a half thereafter, the Cooperation Group shall prepare a report assessing the experience gained with the strategic cooperation pursued under this Article.

5. 欧州委員会は，協力グループの稼働のために必要となる手続上の手立てを定める実装行為を採択する。それらの実装行為は，第 22 条第 2 項に示す審議手続に従って採択される。

The Commission shall adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).

第 1 副項の目的のために，欧州委員会は，2017 年 2 月 9 日までに，第 22 条第 1 項に示す委員会に対し，最初の実装行為案を提出する。

For the purposes of the first subparagraph, the Commission shall submit the first draft implementing act to the committee referred to in Article 22(1) by 9 February 2017.

第 12 条 CSIRT ネットワーク

Article 12 CSIRTs network

1. 構成国間における信任と信頼を発展させるため，及び，迅速かつ実効的な業務遂行上の協力を促進するため，ここに，国内 CSIRT のネットワークが設置される。

In order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation, a network of the national CSIRTs is hereby established.

2. CSIRT ネットワークは，構成国の CSIRT の代表及び CERT-EU によって構成される。欧州委員会は，CSIRT ネットワークにオブザーバーとして参加する。ENISA は，事務局を提供し，かつ，CSIRT の間における協力を積極的に支援する。

The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support the cooperation among the CSIRTs.

3. CSIRT ネットワークは，以下の職務をもつ：
   (a) CSIRT のサービス，業務遂行及び協力の実現能力に関する情報を交換すること；
   (b) インシデントによる影響を受けている可能性のある構成国の CSIRT 代表の要請により，当該インシデント及び付帯リスクと関連する非商業的な機微の情報を交換すること及び討議すること；ただし，インシデントの調査を妨げるリスクがあるときは，構成国の CSIRT は，当該討議への貢献を拒否できる；
   (c) 個々のインシデントに関する機密ではない情報を任意で交換すること及びその情報を利用できるようにすること；
   (d) 構成国の CSIRT 代表の要請により，当該同一の構成国の裁判管轄権内で発見されたインシデントへの共同対応を討議すること，及び，それが可能なときは，その共同対応を指示すること；
   (e) 構成国間の任意の相互補助を基礎として，構成国に対し，国境を越えるインシデントに対処する支援を提供すること；
   (f) 以下と関連するものを含め，別の形態の業務遂行上の協力に関し，討議すること，検討すること及び指示すること：
      (i) リスク及びインシデントの類型；
      (ii) 早期警戒；
      (iii) 相互補助；
      (iv) 国境を越えるリスク及びインシデントに構成国が対応する場合における，協力の基本原則及び様式；
   (g) CSIRT ネットワークの活動，及び，(f)によって討議された別の形態の業務遂行上の協力，並びに，それに関する運用指針の要請を，協力グループに対して連絡すること；
   (h) ENISA によって組織された演習からの教訓を含め，ネットワーク及び情報システムの安全性と関連する演習から得られた教訓に関し，討議すること；
   (i) 個々の CSIRT の要請により，当該 CSIRT の実現能力及び準備態勢に関し，討議すること；
   (j) 業務遂行上の協力に関する本条の条項の適用と関連する業務遂行実務の収斂を促進するための運用指針を発行すること。

The CSIRTs network shall have the following tasks:
   (a) exchanging information on CSIRTs' services, operations and cooperation capabilities;
   (b) at the request of a representative of a CSIRT from a Member State potentially affected by an incident, exchanging and discussing non-commercially sensitive information related to that incident and associated risks; however, any Member State's CSIRT may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident;
   (c) exchanging and making available on a voluntary basis non-confidential information concerning individual incidents;
   (d) at the request of a representative of a Member State's CSIRT, discussing and, where possible, identifying a coordinated response to an incident that has been identified within the jurisdiction

of that same Member State;

(e) providing Member States with support in addressing cross-border incidents on the basis of their voluntary mutual assistance;

(f) discussing, exploring and identifying further forms of operational cooperation, including in relation to:

(i) categories of risks and incidents;

(ii) early warnings;

(iii) mutual assistance;

(iv) principles and modalities for coordination, when Member States respond to cross-border risks and incidents;

(g) informing the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (f), and requesting guidance in that regard;

(h) discussing lessons learnt from exercises relating to the security of network and information systems, including from those organised by ENISA;

(i) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT;

(j) issuing guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation.

4. 第 23 条に示す見直しの目的のために，かつ，2018 年 8 月 9 日まで，及び，その後は 1 年半毎に，CSIRT ネットワークは，結論及び勧告を含め，本条に基づいて求められる業務遂行上の協力から得られた経験を評価する報告書を作成する。その報告書は，協力グループに対しても提出される。

For the purpose of the review referred to in Article 23 and by 9 August 2018, and every year and a half thereafter, the CSIRTs network shall produce a report assessing the experience gained with the operational cooperation, including conclusions and recommendations, pursued under this Article. That report shall also be submitted to the Cooperation Group.

5. CSIRT ネットワークは，5. CSIRT ネットワーク自身の手続規則を定める。

The CSIRTs network shall lay down its own rules of procedure.

第 13 条 国際的な協力

Article 13 International cooperation

欧州連合は，TFEU の第 218 条に従い，第三国または国際組織との間で，協力グループの活動の中の幾つかにそれらが参加することを認め，それを組織する国際協定を締結できる。そのような協定は，個人データの十分な保護を確保する必要性を考慮に入れるものとする。

The Union may conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group. Such agreements shall take into account the need to ensure adequate protection of data.

第Ⅳ章 基礎サービスの運営者のネットワーク及び情報システムの安全性

Chapter IV Security of the Network and Information Systems of Operators of Essential Services

第 14 条 安全要件及びインシデント通知

Article 14 Security requirements and incident notification

1. 構成国は，基礎サービスの運営者が，その運営者の業務遂行に利用するネットワーク及び情報システムの安全性に対して示されたリスクを管理するための適切かつ比例的な技術上及び組織上の措置を講ずることを確保する。最新技術を考慮した上で，それらの措置は，示されたリスクに適切に対応するレベルのネットワーク及び情報システムの安全性を確保する。

   Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.

2. 構成国は，基礎サービスの運営者が，その運営者のサービスの継続性を確保するという観点から，そのような基礎サービスの提供のために利用されるネットワーク及び情報システムの安全性に影響を及ぼすインシデントの影響を防止及びミニマム化するための適切な措置を講ずることを確保する。

   Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

3. 構成国は，基礎サービスの運営者が，不適切な遅滞なく，職務権限のある機関または CSIRT に対し，その運営者が提供する基礎サービスの継続性に大な影響をもつインシデントを通知することを確保する。その通知は，そのインシデントの国境を越える影響を職務権限のある機関または CSIRT が判定できるようにするための情報を含める。その通知は，通知をする当事者を，加重された法的責任に服させてはならない。

   Member States shall ensure that operators of essential services notify, without undue delay, the

competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.

4. インシデントの影響の大きさを判定するため，とりわけ，以下のパラメータが考慮に入れられる：
   (a) 基礎サービスの混乱により影響を受ける利用者の数；
   (b) インシデントの持続時間；
   (c) インシデントによって影響を受ける地域に関する地理的な広がり。

   In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:
   (a) the number of users affected by the disruption of the essential service;
   (b) the duration of the incident;
   (c) the geographical spread with regard to the area affected by the incident.

5. 基礎サービスの運営者からの通知の中で提供される情報を基礎として，職務権限のある機関または CSIRT は，当該構成国の基礎サービスの継続性に対してそのインシデントが大きな影響をもつときは，影響を受ける他の構成国に対して連絡する。そのようにする際，職務権限のある機関または CSIRT は，欧州連合法または欧州連合法を遵守する国内法に従い，その基礎サービスの運営者の安全及び商業的利益，並びに，その運営者の通知の中で提供された情報の機密性を維持する。

   On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In so doing, the competent authority or the CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification.

   状況が許す場合，職務権限のある機関または CSIRT は，通知元である基礎サービスの運営者に対し，実効的なインシデント対応を支援し得る情報のような，その通知の事後対応と関係する関連情報を提供する。

   Where the circumstances allow, the competent authority or the CSIRT shall provide the notifying operator of essential services with relevant information regarding the follow-up of its notification, such as information that could support the effective incident handling.

職務権限のある機関または CSIRT の要請により，単一連絡部局は，影響を受ける他の構成国の単一連絡部局に対し，第 1 副項に示す通知を転送する。

At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications as referred to in the first subparagraph to single points of contact of other affected Member States.

6. インシデントを防止するため，または，進行中のインシデントに対応するため，公衆の認識が必要な場合，職務権限のある機関または CSIRT は，通知元である基礎サービスの運営者との協議を経た上で，公衆に対し，個々のインシデントに関して情報提供できる。

After consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident.

7. 協力活動ネットワーク内において共に行動する職務権限のある機関は，第 4 項に示すインシデントの影響の大きさを判定するためのパラメータに関するものを含め，基礎サービスの運営者がインシデント通知を求められる状況に関する運用指針を策定及び採択できる。

Competent authorities acting together within the Cooperation Group may develop and adopt guidelines concerning the circumstances in which operators of essential services are required to notify incidents, including on the parameters to determine the significance of the impact of an incident as referred to in paragraph 4.

第 15 条 実装及び執行

Article 15 Implementation and enforcement

1. 構成国は，職務権限のある機関が，第 14 条に基づく基礎サービスの運営者の義務を基礎サービスの運営者による遵守，並びに，そのネットワーク及び情報システムの安全性に対するその遵守の影響を評価するために必要となる権限及び手段をもつことを確保する。

Member States shall ensure that the competent authorities have the necessary powers and means to assess the compliance of operators of essential services with their obligations under Article 14 and the effects thereof on the security of network and information systems.

2. 構成国は，職務権限のある機関が，基礎サービスの運営者に対して以下のものの提供を要求する権限及び手段をもつことを確保する：
   (a) 文書化されたセキュリティ基本方針を含め，その運営者のネットワーク及び情報システムの安全性を評価するために必要な情報；

(b) 職務権限のある機関もしくは資格のある監査機関によって実施されたセキュリティ監査結果のような，セキュリティ基本方針の実効的な実装を示す証拠，並びに，後者の場合，監査証跡を含め，職務権限のある機関がその監査結果を利用できるようにすること。

Member States shall ensure that the competent authorities have the powers and means to require operators of essential services to provide:

(a) the information necessary to assess the security of their network and information systems, including documented security policies;

(b) evidence of the effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified auditor and, in the latter case, to make the results thereof, including the underlying evidence, available to the competent authority.

そのような情報または証拠を要求する場合，職務権限のある機関は，その要求の目的を説明し，かつ，要求される情報を特定する。

When requesting such information or evidence, the competent authority shall state the purpose of the request and specify what information is required.

3. 第 2 項に示す情報またはセキュリティ監査の結果に対する評価の後，その職務権限のある機関は，基礎サービスの運営者に対し，特定された不備を是正するための拘束力のある指示書を発し得る。

Following the assessment of information or results of security audits referred to in paragraph 2, the competent authority may issue binding instructions to the operators of essential services to remedy the deficiencies identified.

4. 職務権限のある機関は，インシデントへの対応が個人データの侵害をもたらす場合，データ保護機関と緊密に協力して作業する。

The competent authority shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches.

第Ⅴ章 デジタルサービスプロバイダのネットワーク及び情報システムの安全性

Chapter V Security of the Network and Information Systems of Digital Service Providers

第 16 条 安全要件及びインシデント通知

Article 16 Security requirements and incident notification

1. 構成国は，デジタルサービスプロバイダが，欧州連合内において別紙 III に示すサービスを提供する過程でそのプロバイダが利用するネットワーク及び情報システムの安全性に対して示されたリスクを特定し，管理するための適切かつ比例的な技術上及び組織上の措置を講ずることを確保する。最新技術を考慮した上で，それらの措置は，示されたリスクに適切に対応するレベルのネットワーク及び情報システムの安全性を確保し，かつ，以下の要素を考慮に入れる：
   (a) システム及び施設の安全性；
   (b) インシデント対応；
   (c) 事業継続性管理；
   (d) 監視，監査及び試験；
   (e) 国際的な標準の準拠。

   Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:
   (a) the security of systems and facilities;
   (b) incident handling;
   (c) business continuity management;
   (d) monitoring, auditing and testing;
   (e) compliance with international standards.

2. 構成国は，デジタルサービスプロバイダが，そのプロバイダのサービスの継続性を確保するため，欧州連合内において提供される別紙 III に示すサービスに対する，そのプロバイダのネットワーク及び情報システムの安全性に影響を及ぼすインシデントの影響を防止及びミニマム化するための適切な措置を講ずることを確保する。

   Member States shall ensure that digital service providers take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services referred to in Annex III that are offered within the Union, with a view to ensuring the continuity of those services.

3. 構成国は，デジタルサービスプロバイダが，職務権限のある機関または CSIRT に対し，不適切な遅滞なく，欧州連合内において提供する別紙 III に示すサービスの提供に大きな影響をもつインシデントを通知することを確保する。その通知は，そのインシデントの国境を越える影響を職務権限のある機関または CSIRT が判定できるようにするための情報を含める。その通知は，通知をする当事者を，加重された法的責任に服させてはならない。

Member States shall ensure that digital service providers notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union. Notifications shall include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact. Notification shall not make the notifying party subject to increased liability.

4. インシデントの影響の大きさを判定するため，とりわけ，以下のパラメータが考慮に入れられる：
   (a) インシデントにより影響を受ける利用者の数，とりわけ，そのサービスに利用者自身のサービスが依拠する利用者の数；
   (b) インシデントの持続時間；
   (c) インシデントによって影響を受ける地域に関する地理的な広がり；
   (d) そのサービスの機能の混乱が及ぶ範囲；
   (e) 経済活動及び社会活動に対する影響の範囲。

In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account:
   (a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services;
   (b) the duration of the incident;
   (c) the geographical spread with regard to the area affected by the incident;
   (d) the extent of the disruption of the functioning of the service;
   (e) the extent of the impact on economic and societal activities.

インシデントを通知すべき義務は，そのデジタルサービスプロバイダが，第 1 副項に示すパラメータに対応するインシデントの影響を評価するために必要な情報へのアクセスをもつ場合に限り，適用される。

The obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in the first subparagraph.

5. 重要な社会活動及び経済活動の維持のために必須のサービスの提供のために基礎サービ

スの運営者が第三者であるデジタルサービスプロバイダに依拠する場合，そのデジタルサービスプロバイダに影響を及ぼすインシデントによるその基礎サービスの継続性に対する大きな影響は，当該運営者から通知される。

Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator.

6. それが適切なときは，かつ，とりわけ，第 3 項に示すインシデントが複数の構成国と関係するときは，職務権限のある機関または CSIRT は，影響を受ける他の構成国に対して連絡する。そのようにする場合，職務権限のある機関，CSIRT 及び単一連絡部局は，欧州連合法または欧州連合法を遵守する国内法に従い，そのデジタルサービスプロバイダの安全及び商業的利益，並びに，提供された情報の機密性を維持する。

Where appropriate, and in particular if the incident referred to in paragraph 3 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law, or national legislation that complies with Union law, preserve the digital service provider's security and commercial interests as well as the confidentiality of the information provided.

7. インシデントを防止するため，または，進行中のインシデントに対応するため，公衆の認識が必要な場合，あるいは，そのインシデントの開示が公共の利用と関わる場合，職務権限のある機関及び CSIRT，関係する他の構成国の職務権限のある機関または CSIRT は，関係するデジタルサービスプロバイダとの協議を経た上で，公衆に対し，個々のインシデントに関して情報提供でき，または，そのデジタルサービスプロバイダに対し，そのようにすることを要求できる。

After consulting the digital service provider concerned, the competent authority or the CSIRT and, where appropriate, the authorities or the CSIRTs of other Member States concerned may inform the public about individual incidents or require the digital service provider to do so, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest.

8. 欧州委員会は，本条の第 1 項に示す要素及び第 4 項に列挙するパラメータを更に追加して指定するため，実装行為を採択する。それらの実装行為は，第 22 条第 2 項に示す審議手続に従い，2017 年 8 月 9 日までに，採択される。

The Commission shall adopt implementing acts in order to specify further the elements referred to in paragraph 1 and the parameters listed in paragraph 4 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2) by 9 August 2017.

9. 欧州委員会は，通知要件に適用可能なフォーマット及び手順を定める実装行為を採択できる。それらの実装行為は，第 22 条第 2 項に示す審議手続に従って採択される。

The Commission may adopt implementing acts laying down the formats and procedures applicable to notification requirements. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).

10. 第 1 条第 6 項を妨げることなく，構成国は，デジタルサービスプロバイダに対し，別の安全要件及び通知要件を課してはならない。

Without prejudice to Article 1(6), Member States shall not impose any further security or notification requirements on digital service providers.

11. 第 5 章は，委員会勧告 2003/361/EC[19]に定めるマイクロ企業及び小規模企業に対して適用してはならない。

Chapter V shall not apply to micro- and small enterprises as defined in Commission Recommendation 2003/361/EC[19].

第 17 条 実装及び執行

Article 17 Implementation and enforcement

1. 構成国は，デジタルサービスプロバイダが第 16 条に定める要件に適合するものではないとの証拠を得た場合，それが必要なときは，職務権限のある機関が，事後的の監督措置により，行動することを確保する。そのような証拠は，そのサービスが提供されている別の構成国の職務権限のある機関から提出され得る。

Member States shall ensure that the competent authorities take action, if necessary, through *ex post* supervisory measures, when provided with evidence that a digital service provider does not meet the requirements laid down in Article 16. Such evidence may be submitted by a competent authority of another Member State where the service is provided.

[19] マイクロ企業、小規模企業及び中規模企業の定義に関する 2003 年 5 月 6 日の委員会勧告 2003/361/EC (OJ L 124, 20.5.2003, p.36).

2. 第 1 項の目的のために，職務権限のある機関は，デジタルサービスプロバイダに対し，以下のことを要求するために必要な権限及び手段をもつ：
   (a) 文書化されたセキュリティ基本方針を含め，そのプロバイダのネットワーク及び情報システムの安全性を評価するために必要となる情報を提供すること；
   (b) 第 16 条に定める要件に適合していないことを是正すること。

   For the purposes of paragraph 1, the competent authorities shall have the necessary powers and means to require digital service providers to:
   (a) provide the information necessary to assess the security of their network and information systems, including documented security policies;
   (b) remedy any failure to meet the requirements laid down in Article 16.

3. デジタルサービスプロバイダが，ある構成国内にそのプロバイダの主たる拠点または代理者をもつが，そのプロバイダのネットワーク及び情報システムが 1 または複数の別の構成国内に所在しているときは，その主たる拠点もしくは代理者のある構成国の職務権限のある機関及びそれらの別の構成国の職務権限のある機関は，協力し，かつ，必要に応じて相互に補助する。そのような補助及び協力は，関係する職務権限のある機関の間の情報交換及び第 2 項に示す監督措置を講ずることの要請を包摂し得る。

   If a digital service provider has its main establishment or a representative in a Member State, but its network and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or of the representative and the competent authorities of those other Member States shall cooperate and assist each other as necessary. Such assistance and cooperation may cover information exchanges between the competent authorities concerned and requests to take the supervisory measures referred to in paragraph 2.

第 18 条 裁判管轄権及び属地主義

Article 18 Jurisdiction and territoriality

1. この指令の目的のために，デジタルサービスプロバイダは，そのプロバイダが主たる拠点をもつ構成国の裁判管轄権の下にあるとみなされる。デジタルサービスプロバイダは，そのプロバイダの本社が当該構成国に所在する場合，その構成国内に主たる拠点をもつとみなされる。

   For the purposes of this Directive, a digital service provider shall be deemed to be under the jurisdiction of the Member State in which it has its main establishment. A digital service provider shall be deemed to have its main establishment in a Member State when it has its head office in that Member State.

2. 欧州連合内に拠点をもたないが，欧州連合内で別紙 III に示すサービスを提供するデジタルサービスプロバイダは，欧州連合内における代理者を指定する。その代理者は，そのサービスが提供されている構成国中のいずれか 1 つに設けられる。そのデジタルサービスプロバイダは，代理者が設けられている構成国の裁判管轄権の下にあるとみなされる。

A digital service provider that is not established in the Union, but offers services referred to in Annex III within the Union, shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. The digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established.

3. The designation of a representative by the digital service provider shall be without prejudice to legal actions which could be initiated against the digital service provider itself.

デジタルサービスプロバイダによる代理者の指定は，そのデジタルサービスプロバイダ自身を相手方として開始され得る訴訟を妨げてはならない。

第VI章 標準化及び任意の通知
Chapter VI Standardisation and Voluntary Notification

第 19 条 標準化
Article 19 Standardisation

1. 第 14 条第 1 項及び第 2 項並びに第 16 条第 1 項及び第 2 項の収斂的な実装を促進するため，構成国は，特定のタイプの技術の利用にとって有利となるような強制や差別なく，ネットワーク及び情報システムの安全性と関連する欧州で承認され，または，国際的に承認された標準及び仕様の利用を推進する。

In order to promote convergent implementation of Article 14(1) and (2) and Article 16(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.

2. ENISA は，構成国と共働して，第 1 項と関連して考慮されるべき技術分野に関し，並びに，構成国の国内標準を含め，それらの分野に包摂され得るような既に存在している標準に関し，助言及び運用指針を作成する。

ENISA, in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing

standards, including Member States' national standards, which would allow for those areas to be covered.

第 20 条 任意の通知

Article 20 Voluntary notification

1. 第 3 条を妨げることなく，基礎サービスの運営者として識別されなかった法主体及びデジタルサービスプロバイダではない法主体は，任意に，それらの法主体が提供するサービスの継続性に大きな影響をもつインシデントを通知できる。

Without prejudice to Article 3, entities which have not been identified as operators of essential services and are not digital service providers may notify, on a voluntary basis, incidents having a significant impact on the continuity of the services which they provide.

2. 通知を処理する場合，構成国は，第 14 条に定める手続に従って行動する。構成国は，義務的な通知の処理を任意の通知よりも優先し得る。任意の通知は，その処理が，関係する構成国に対して不適切または不適正な負担を構成しない場合に限り，処理される。

When processing notifications, Member States shall act in accordance with the procedure set out in Article 14. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary notifications shall only be processed where such processing does not constitute a disproportionate or undue burden on Member States concerned.

任意の通知は，通知元である法主体に対し，もしその法主体が当該通知を与えなかったとすればその組織が服することがなかったような義務を課す結果を招いてはならない。

Voluntary notification shall not result in the imposition upon the notifying entity of any obligations to which it would not have been subject had it not given that notification.

第Ⅶ章 最終規定

Chapter VII Final Provisions

第 21 条 制裁

Article 21 Penalties

構成国は，この指令によって採択された国内条項の違反行為に対して適用される制裁に関する規定を定め，かつ，その規定が実装されることを確保するために必要となる全ての措置を講ずる。定められる制裁は，実効的であり，比例的であり，かつ，抑止力のあるものとする。構成国は，2018 年 5 月 9 日までに，欧州委員会に対し，それらの規定及び措置を通知し，ま

た，その後の改正がそれらの規定に影響を及ぼすときは，遅滞なく，その改正を通知する。

Member States shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by 9 May 2018, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

第 22 条 委員会の手続

Article 22 Committee procedure

1. 欧州委員会は，ネットワーク及び情報システム安全性委員会よって補佐を受ける。この委員会は，規則(EU) No 182/2011 の意味における委員会である。

The Commission shall be assisted by the Network and Information Systems Security Committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. 本項に対する参照が行われるときは，規則(EU) No 182/2011 の第 5 条が適用される。

Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

第 23 条 評価

Article 23 Review

1. 2019 年 5 月 9 日までに，欧州委員会は，欧州議会及び理事会に対し，基礎サービスの運営者の識別において構成国によって行われたアプローチの一貫性を評価する報告書を送付する。

By 9 May 2019, the Commission shall submit a report to the European Parliament and to Council, assessing the consistency of the approach taken by Member States in the identification of the operators of essential services.

2. 欧州委員会は，この指令の稼働を定期的に見直し，かつ，欧州議会及び理事会に対して報告する。この目的のために，かつ，戦略上及び業務遂行上の協力の将来の発展という観点から，欧州委員会は，戦略レベル及び運用レベルにおいて得られた経験に関する協力グループ及び CSIRT ネットワークの報告書を考慮に入れる。その見直しにおいて，欧州委員会は，別紙 II 及び別紙 III に含められているリスト，並びに，基礎サービスの運営者の識別及び別紙 II に示す部門のサービスの一貫性を評価する。最初の報告書は，2021 年 5 月 9 日までに提出される。

The Commission shall periodically review the functioning of this Directive and report to the European Parliament and to the Council. For this purpose and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. In its review, the Commission shall also assess the lists contained in Annexes II and III, and the consistency in the identification of operators of essential services and services in the sectors referred to in Annex II. The first report shall be submitted by 9 May 2021.

第 24 条 移行措置

Article 24 Transitional measures

1. 第 25 条を妨げることなく，かつ，構成国に対して国内法化の期間内における適切な協力のための付加的な可能性を提供するため，協力グループ及び CSIRT ネットワークは，2017 年 2 月 9 日までに，第 11 条第 3 項及び第 12 条第 3 項にそれぞれ定める職務の遂行を開始する。

Without prejudice to Article 25 and with a view to providing Member States with additional possibilities for appropriate cooperation during the period of transposition, the Cooperation Group and the CSIRTs network shall begin to perform the tasks set out in Articles 11(3) and 12(3) respectively by 9 February 2017.

2. 2017 年 2 月 9 日から 2018 年 11 月 9 日までの間に，かつ，基礎サービスの運営者の識別過程における一貫性のあるアプローチを行う上で構成国を支援する目的のために，協力グループは，第 5 条及び第 6 条に定める基準に従って特定の部門内にある基礎サービスの運営者を識別できるようにする国内措置の手順，内容及びタイプに関し，討議すべきである。協力グループは，構成国の要請により，第 5 条及び第 6 条に規定する基準に従って特定の部門に属する基礎サービスの運営者を識別できるようにする当該構成国の個別の国内措置案に関しても，討議する。

For the period from 9 February 2017 to 9 November 2018, and for the purposes of supporting Member States in taking a consistent approach in the process of identification of operators of essential services, the Cooperation Group shall discuss the process, substance and type of national measures allowing for the identification of operators of essential services within a specific sector in accordance with the criteria set out in Articles 5 and 6. The Cooperation Group shall also discuss, at the request of a Member State, specific draft national measures of that Member State, allowing for the identification of operators of essential services within a specific sector in accordance with the criteria set out in Articles 5 and 6.

3. 2017 年 2 月 9 日までに, かつ, 本条の目的のために, 構成国は, 協力グループ及び CSIRT ネットワーク内における適切な代表を確保する。

By 9 February 2017 and for the purposes of this Article, Member States shall ensure appropriate representation in the Cooperation Group and the CSIRTs network.

第 25 条 国内法化

Article 25 Transposition

1. 構成国は, 2018 年 5 月 9 日までに, この指令を遵守するために必要となる法律, 行政規則または行政条項を採択し, 公示すべきである。構成国は, 欧州委員会に対し, 直ちに, それらを通知する。

Member States shall adopt and publish, by 9 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof.

構成国は, 2018 年 5 月 10 日から, それらの措置を適用する。

They shall apply those measures from 10 May 2018.

構成国がそれらの措置を採択する際, それらの措置は, この指令への参照を含めるものとし, または, それらの措置の公示の際にそのような参照を添えるものとする。そのような参照を行うための手法は, 構成国によって定められる。

When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. 構成国は, 欧州委員会に対し, この指令の適用のある分野において構成国が採択する国内法の主要な条項の正文を送付する。

Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

第 26 条 発効

Article 26 Entry into force

この指令は, EU 官報上で公示された日の 20 日後に発効する。

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

第 27 条 発出
Article 27 Addressees

この指令は，構成国宛てに発出される。

This Directive is addressed to the Member States.

2016 年 7 月 6 日にストラスブールにおいて行われた。
Done at Strasbourg, 6 July 2016.

欧州議会として	理事会として
議長 M. Schulz	議長 I. Korčok

別紙 I

コンピュータセキュリティインシデント対応チーム（CSIRT）の要件及び職務

Requirements and Tasks of Computer Security Incident Response Teams (CSIRTs)

CSIRT の要件及び職務は，国内政策及びまたは法令によって十分かつ明確に定義され，かつ，支持されるものとする。それらは，以下のものを含める：

The requirements and tasks of CSIRTs shall be adequately and clearly defined and supported by national policy and/or regulation. They shall include the following:

(1) CSIRT の要件:
   (a) CSIRT は，単一障害点を避けることによって，構成国の通信サービスの高いレベルの可用性を確保し，かつ，常時，他者との間で接続されるため，及び，他者と接続するための複数の手段をもつ。更に，その通信経路は，明確に指定され，かつ，構成員及び協力者に対して周知される。
   (b) CSIRT の施設及びその支援情報システムは，安全な場所に所在する。
   (c) 事業継続性
      (i) CSIRT は，引継ぎを容易にするため，運用管理及びルーティング要求のための適切なシステムを装備する；
      (ii) CSIRT は，可用性を常時確保するため，十分な要員をもつ；
      (iii) CSIRT は，その継続性が確保されたインフラに依拠する。その目的のために，冗長システム及びバックアップ作業領域を利用できる。
   (d) CSIRT は，その CSIRI がそのように望む場合，国際的な協力ネットワークに参加する可能性をもつ。

   Requirements for CSIRTs:
   (a) CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.
   (b) CSIRTs' premises and the supporting information systems shall be located in secure sites.
   (c) Business continuity:
      (i) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers.
      (ii) CSIRTs shall be adequately staffed to ensure availability at all times.
      (iii) CSIRTs shall rely on an infrastructure the continuity of which is ensured. To that end, redundant systems and backup working space shall be available.
   (d) CSIRTs shall have the possibility to participate, where they wish to do so, in international

cooperation networks.

(2) CSIRT の職務:
  (a) CSIRT の職務は, 少なくとも, 以下のものを含める:
    (i) 国内レベルでインシデントを監視すること;
    (ii) リスク及びインシデントに関し, 早期警戒, 警報, 表明及び関連する利害関係者に対する情報の伝達を提供すること;
    (iii) インシデントに対応すること;
    (iv) 動的なリスク及びインシデントの分析並びに状況認識を提供すること;
    (v) CSIRT ネットワークに参加すること。
  (b) CSIRT は, 民間部門との間の協力関係を構築する。
  (c) 協力関係を促進するため, CSIRT は, 以下のための共通のプラクティスまたは標準的なプラクティスの導入及び利用を促進する:
    (i) インシデント及びリスク対応の手順;
    (ii) インシデント, リスク及び情報の分類手法。

CSIRTs' tasks:
(a) CSIRTs' tasks shall include at least the following:
  (i) monitoring incidents at a national level;
  (ii) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;
  (iii) responding to incidents;
  (iv) providing dynamic risk and incident analysis and situational awareness;
  (v) participating in the CSIRTs network.
(b) CSIRTs shall establish cooperation relationships with the private sector.
(c) To facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices for:
  (i) incident and risk-handling procedures;
  (ii) incident, risk and information classification schemes.

別紙Ⅱ

第 4 条第 4 号に定める法主体のタイプ

Types of Entities for the Purposes of point (4) of Article 4

部門 Sector	副部門 Subsector	法主体の種類 Type of entity
1. エネルギー Energy	(a) 電力 Electricity	― 欧州議会及び理事会の指令 2009/72/EC[1]の第 2 条第 35 号に定義する, 同指令の第 2 条第 19 号に定める「供給」の機能を遂行する電力事業者 Electricity undertakings as defined in point (35) of Article 2 of Directive 2009/72/EC of the European Parliament and of the Council (1), which carry out the function of 'supply' as defined in point (19) of Article 2 of that Directive
		― 指令 2009/72/EC の第 2 条第 6 号に定義する配電システム事業者 Distribution system operators as defined in point (6) of Article 2 of Directive 2009/72/EC
		― 指令 2009/72/EC の第 2 条第 4 号に定義する送電システム事業者 Transmission system operators as defined in point (4) of Article 2 of Directive 2009/72/EC
	(b) 石油 Oil	― 石油パイプライン事業者 Operators of oil transmission pipelines
		― 石油の生産, 精製, 施設管理, 貯蔵及び送油の事業者 Operators of oil production, refining and treatment facilities, storage and transmission
	(c) ガス Gas	― 欧州議会及び理事会の指令 2009/73/EC[2]の第 2 条第 8 号に定義する供給事業者 ― Supply undertakings as defined in point (8) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council (2)

[1] 電力における域内市場の共通規定に関する, 及び, 指令 2003/54/EC を廃止する欧州議会及び理事会の 2009 年 7 月 13 日の指令 2009/72/EC（OJ L 211, 14.8.2009, p.55）.

[2] 天然ガスにおける域内市場の共通規定に関する, 及び, 指令 2003/55/EC を廃止する欧州議会及び理事会の 2009 年 7 月 13 日の指令 2009/73/EC（OJ L 211, 14.8.2009, p.94）.

		― 指令 2009/73/EC の第 2 条第 6 号に定義する配給事業者 Distribution system operators as defined in point (6) of Article 2 of Directive 2009/73/EC
		― 指令 2009/73/EC の第 2 条第 4 号に定義する送出事業者 Transmission system operators as defined in point (4) of Article 2 of Directive 2009/73/EC
		― 指令 2009/73/EC の第 2 条第 10 号に定義する貯蔵システム事業者 Storage system operators as defined in point (10) of Article 2 of Directive 2009/73/EC
		― 指令 2009/73/EC の第 2 条第 12 号に定義する LNG システム事業者 LNG system operators as defined in point (12) of Article 2 of Directive 2009/73/EC
		― 指令 2009/73/EC の第 2 条第 1 号に定義する天然ガス事業者 Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC
		― 天然ガス精製送出施設事業者 Operators of natural gas refining and treatment facilities
2. 輸送 Transport	(a) 航空輸送 Air transport	― 欧州議会及び理事会の規則(EC) No 300/2008[3]の第 3 条第 4 号に定義する航空会社 Air carriers as defined in point (4) of Article 3 of Regulation (EC) No 300/2008 of the European Parliament and of the Council (3)
		― 欧州議会及び理事会の規則(EU) No 1315/2013[5] の別紙 II の第 2 節に列挙する中核空港を含め, 欧州議会及び理事会の指令 2009/12/EC[4] の第 2 条第 2 項に定義する空港管理組織, 同指令の第 2 条第 1 号に定める空港, 並びに, 空港内にある補助施設を

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

[4] 空港使用料金に関する欧州議会及び理事会の 2009 年 3 月 11 日の指令 2009/12/EC（OJ L 70, 14.3. 2009, p.11）.

[5] 全欧輸送網の開発のための欧州連合の運用指針に関する, 及び, 決定 No 661/2010/EU を廃止する欧州議会及び理事会の 2013 年 12 月 11 日の規則(EU) No 1315/2013（OJ L 348, 20.12.2013, p.1）.

		運用する法主体 Airport managing bodies as defined in point (2) of Article 2 of Directive 2009/12/EC of the European Parliament and of the Council(4), airports as defined in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council(5), and entities operating ancillary installations contained within airports
		― 欧州議会及び理事会の規則(EC)No 549/2004[6]の第 2 条第 1 号に定義する航空機運航管理（ATC）サービスを提供する航空管制事業者 Traffic management control operators providing air traffic control (ATC) services as defined in point (1) of Article 2 of Regulation (EC) No 549/2004 of the European Parliament and of the Council(6)
	(b) 鉄道輸送 Rail transport	― 欧州議会及び理事会の指令 2012/34/EU[7]の第 3 条第 2 号に定義するインフラ管理者 Infrastructure managers as defined in point (2) of Article 3 of Directive 2012/34/EU of the European Parliament and of the Council(7)
		― 指令 2012/34/EU の第 3 条第 12 号に定義するサービス施設管理者を含め，指令 2012/34/EU の第 3 条第 1 号に定める鉄道事業者 Railway undertakings as defined in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities as defined in point (12) of Article 3 of Directive 2012/34/EU
	(c) 水上輸送 Water transport	― それらの会社が運用する個々の船舶を除き，欧州議会及び理事会の規則(EC) No 725/2004[8]の別紙 I の中で水上運送として定義する内水面，水上及び沿岸の旅客及び貨物の水上輸送企業

6 単一欧州領空の創設のための枠組みを定める欧州議会及び理事会の 2004 年 3 月 10 日の規則(EC) No 549/2004（OJ L 96, 31.3.2004, p.1）.

7 単一欧州鉄道領域を設ける欧州議会及び理事会の 2012 年 11 月 21 日の指令 2012/34/EU（OJ L 343, 14.12.2012, p.32）.

8 船舶及び港湾施設の安全を拡大する欧州議会及び理事会の 2004 年 3 月 31 日の規則(EC) No 725/2004（OJ L 129, 29.4.2004, p.6）.

		Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council[8], not including the individual vessels operated by those companies
		― 規則(EC) No 725/2004 の第 2 条第 11 号に定義する港湾施設を含め，欧州議会及び理事会の指令 2005/65/EC[9]の第 3 条第 1 号に定義する港湾管理組織，並びに，港湾内の作業や設備を運営する法主体 Managing bodies of ports as defined in point (1) of Article 3 of Directive 2005/65/EC of the European Parliament and of the Council[9], including their port facilities as defined in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports
		― 欧州議会及び理事会の指令 2002/59/EC[10]の第 3 条(o)に定義する船舶交通業務の運営者 Operators of vessel traffic services as defined in point (o) of Article 3 of Directive 2002/59/EC of the European Parliament and of the Council [10]
	(d) 陸上輸送 Road transport	― 委員会委任規則(EU)2015/962[11]の第 2 条第 12 号に定義する交通管制の職責を負う道路管理者 Road authorities as defined in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962[11] responsible for traffic management control
		― 欧州議会及び理事会の指令 2010/40/EU[12]の第 4 条第 1 号に定義する高度輸送システムの運営者 Operators of Intelligent Transport Systems as defined in point (1) of Article 4 of Directive 2010/40/EU of the

9 港湾の安全を拡大する欧州議会及び理事会の 2005 年 10 月 26 日の指令 2005/65/EC（OJ L 310, 25. 11.2005, p.28）.

10 欧州共同体の船舶交通監視及び情報システムを設置に関する，及び，理事会指令 93/75/EC を廃止する欧州議会及び理事会の 2002 年 6 月 27 日の指令 2002/59/EC（OJ L 208, 5.8.2002, p.10）.

11 全 EU リアルタイム交通情報サービスの提供に関する欧州議会及び理事会の指令 2010/40/EU を補足する 2014 年 12 月 18 日の委員会委任規則(EU) 2015/962（OJ L 157, 23.6.2015, p.21）.

12 道路輸送の分野における高度輸送システムの配置及び他のモードの輸送とのインタフェイスの枠組みに関する欧州議会及び理事会の 2010 年 7 月 7 日の指令 2010/40/EU（OJ L 207, 6.8.2010, p.1）.

			European Parliament and of the Council [12]
3. 銀行 Banking		―	欧州議会及び理事会の規則(EU) No 575/2013[13]の第 4 条第 1 号に定義する信用機関 Credit institutions as defined in point (1) of Article 4 of Regulation (EU) No 575/2013 of the European Parliament and of the Council[13]
4. 金融市場インフラ Financial market infrastructures		―	欧州議会及び理事会の指令 2014/65/EU[14]の第 4 条第 24 号に定義する取引所の運営者 Operators of trading venues as defined in point (24) of Article 4 of Directive 2014/65/EU of the European Parliament and of the Council[14]
		―	欧州議会及び理事会の規則(EU) No 648/2012[15]の第 2 条第 1 号に定義する中央決済機関（CCPs） Central counterparties (CCPs) as defined in point (1) of Article 2 of Regulation (EU) No 648/2012 of the European Parliament and of the Council[15]
5. 医療部門 Health sector	（病院及び医院を含め）医療の設置 Health care settings (including hospitals and private clinics)	―	欧州議会及び理事会の指令 2011/24/EU[16]の第 3 条(g)に定義する医療機関 Healthcare providers as defined in point (g) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council [16]
6. 飲料水の供給及び分配 Drinking water supply and distribution		―	人間の消費の用に供する水の流通が当該事業者の一般的な業務である他の商品や物品の販売業務の一部分を構成するのに過ぎず，基礎サービスではないと判断される場合を除き，理事会指令 98/83/EC[17]の第 2 条第 1 号(a)に定義する人間の消費用の水の供給事業者及び分配業者 Suppliers and distributors of water intended for human

13 信用機関及び投資企業のための健全性要件に関する，及び，規則(EU)No 648/2012 を改正する欧州議会及び理事会の 2013 年 6 月 26 日の規則(EU) No 575/2013（OJ L 176, 27.6.2013, p.1）.

14 金融商品市場に関する，及び，指令 2002/92/EC を改正する欧州議会及び理事会の 2014 年 5 月 15 日の指令 2014/65/EU（OJ L 173, 12.6.2014, p.349）.

15 OTC デリバティブ，中央決済機関及び取引情報蓄積機関に関する欧州議会及び理事会の 2012 年 7 月 4 日の規則(EU) No 648/2012（OJ L 201, 27.7.2012, p.1）.

16 国境を越える医療における患者の権利の適用に関する欧州議会及び理事会の 2011 年 3 月 9 日の指令 2011/24/EU（OJ L 88, 4.4.2011, p.45）.

17 人間の消費の用に供する水の品質に関する 1998 年 11 月 3 日の理事会指令 98/83/EC（OJ L 330, 5.12.1998, p.32）.

		consumption as defined in point (1)(a) of Article 2 of Council Directive 98/83/EC(17) but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services
7. デジタルインフラ Digital Infrastructure		― IXPs
		― DNS サービスプロバイダ DNS service providers
		― TLD ネームレジストリ TLD name registries

別紙Ⅲ

第 4 条第 5 号に定めるデジタルサービスのタイプ
Types of Digital Services for the Purposes of point (5) of Article 4

1. オンライン市場。
   Online marketplace.

2. オンライン検索エンジン。
   Online search engine.

3. クラウドコンピューティングサービス。
   Cloud computing service.

2021 Printed in Japan
ISSN 2432-6089
法と情報雑誌　第 6 巻第 6 号（通巻第 46 号）（第 3 分冊）
The Law and Information Magazine vol.6 no.6 (consecutive no.46) part 3

2021 年 12 月 10 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）