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―

国立国会図書館　調査及び立法考査局
海外立法情報課　島村　智子

目　次

はじめに
Ⅰ　背景と経緯
　1　サイバーセキュリティに関する EU の取組
　2　NIS 指令の目的及び制定
Ⅱ　NIS 指令の概要
　1　構成及び法的根拠
　2　主な規定内容
Ⅲ　NIS 指令制定後の動向
　1　NIS 指令の実施に向けた取組
　2　加盟国に対する財政支援
おわりに
翻訳：ネットワーク・情報システムに係る欧州連合共通の高度な安全水準のための措置に関する 2016 年 7 月 6 日の欧州議会及び理事会の指令（EU）2016/1148

キーワード：サイバーセキュリティ、EU、NIS 指令、NIS Directive

要　旨

近年、サイバー攻撃の脅威が急速に拡大・複雑化し、サイバーセキュリティ対策は世界各国において重要な政策課題となっている。EU でも、これまでに、政策方針の策定、対応組織の設置、サイバー犯罪対策立法、研究事業等に対する資金提供などが行われている。2016 年 7 月に初のサイバーセキュリティ立法として制定された「ネットワーク・情報システムの安全に関する指令」（NIS 指令）は、各加盟国のリスク対策やインシデントへの対処能力に関し一定の基準を定め、また、EU 域内での情報収集と共有の仕組みを整備することを目指している。NIS 指令は、今後の EU のサイバーセキュリティ対策における柱と位置付けられ、実施に向けた様々な取組が進められている。

EU におけるサイバーセキュリティ関連政策の背景と経緯を紹介した上で、NIS 指令の概要と同指令の実施に向けた動向を概説し、併せて、同指令を訳出する。

はじめに

社会全体において情報通信技術への依存度が高まり続ける中で、サイバー攻撃などデジタル空間における脅威は急速に拡大・複雑化しており、サイバーセキュリティ対策は世界各国で重要な政策課題となっている(1)。被害の一例として、2015 年頃から急増したランサムウェア(2)によるサイバー攻撃は、2016 年以降世界で毎日 4,000 件以上発生しており、EU では企業の約 8 割がその影響を受けたとされる(3)。また、EU が行った世論調査では、回答者の 9 割近くがサイバー犯罪を EU 域内の安全にとって重要な課題と認識し、その中でも、マルウェア（悪意あるソフトウェア）(4)、個人情報の盗難、銀行のカードやインターネットバンキングに係る詐欺な

＊　本稿におけるインターネット情報の最終アクセス日は、2018 年 5 月 23 日である。

(1)「サイバーセキュリティ」について、我が国の「サイバーセキュリティ基本法」（平成 26 年法律第 104 号）では、「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式…（中略）…により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置…（中略）…が講じられ、その状態が適切に維持管理されていること」とされており、本稿ではこの定義を踏襲する。なお、国際標準においてもほぼ同様の定義がなされている。『情報通信技術の進展とサイバーセキュリティ―科学技術に関する調査プロジェクト調査報告書―』（調査資料 2014-3）国立国会図書館調査及び立法考査局, 2015, p.1. <http://dl.ndl.go.jp/view/download/digidepo_9104276_po_20140301.pdf?contentNo=1> を参照。

(2)　ランサムウェアは、「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。感染したパソコンに特定の制限をかけ、その制限の解除と引換えに金銭を要求する挙動から、このような不正プログラムをランサムウェアと呼ぶ。「ランサムウェア対策特設ページ」情報処理推進機構（IPA）ウェブサイト <https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html> 2017 年 5 月には、WannaCry と呼ばれるランサムウェアの感染により、150 か国で 23 万台のコンピュータが被害を受けたとされる。European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, “Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU,” JOIN(2017) 450 final, 2017.9.13, p.2. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN>

(3)　European Commission, “State of the Union 2017: The Commission scales up its response to cyber-attacks,” 2017.9.19. <http://europa.eu/rapid/press-release_MEMO-17-3194_en.htm>

(4)　マルウェアは、「malicious software（悪意あるソフトウェア）」が短縮された語で、不正かつ有害な動作を行う、悪意を持ったソフトウェアのことをいう。サイバーセキュリティ戦略本部『サイバーセキュリティ 2017』2017.8.25, p.36. 内閣サイバーセキュリティセンターウェブサイト <https://www.nisc.go.jp/active/kihon/pdf/cs2017.pdf>

どの被害に対する懸念が高いという結果が見られた[5]。

このようなサイバー犯罪の脅威に対応するため、EU は、サイバーセキュリティ対策に関する初めての共通立法として、「ネットワーク・情報システムの安全に関する指令」（以下「NIS 指令」）[6]を 2016 年 7 月に制定した。NIS 指令では、各加盟国のサイバーセキュリティ関連のリスクやインシデント[7]に対する対処能力を向上し、情報共有など EU 域内の協力を強化し、エネルギー、輸送、金融、医療等の重要インフラを保有する企業等に対してリスク管理・インシデント届出を義務付けることなどによって、EU 全体のネットワーク・情報システムの安全性を向上させることが目指されている。

本稿では、EU のサイバーセキュリティ関連政策の背景と経緯を紹介した上で、NIS 指令の概要及び同指令の実施に向けた動向を概説し、併せて、同指令を訳出する。

Ⅰ　背景と経緯

1　サイバーセキュリティに関する EU の取組

サイバーセキュリティ対策に関し、EU は、2000 年代初頭から、全般的な政策方針の策定、対応組織の設置、サイバー犯罪対策立法[8]、研究事業やデジタルインフラ整備に対する資金提供などを実施してきた。ここでは、NIS 指令の制定に至るまでの EU の政策方針の経緯と、政策の展開に伴い実際の対応組織として整備された EU の主要機関を紹介する。

(1) 政策方針の経緯

経済、産業、行政、市民生活などあらゆる分野で情報通信技術の役割が急速に拡大したことを踏まえ、欧州委員会は、2001 年の政策文書[9]において、EU レベルで、ネットワーク・情報システムの安全性向上のために対策を講じる必要性を提起した。その方法として、知識普及活動や教育による意識向上、サイバー攻撃に係る情報共有制度の構築、関連技術に関する安全基準や認証手続の検討などが提案された。同文書に続き、2006 年には政策文書「安全な情報社会の

(5)　European Commission, *op.cit*.(3)

(6)　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, *Official Journal of the European Union*, L194, 2016.7.19. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148> EU の文書等では、指令の名称を略して「Directive on the Security of Network and Information Systems (NIS Directive)」とすることが多いため、本稿では、この省略形の日本語訳「ネットワーク・情報システムの安全に関する指令（NIS 指令）」を使用する。なお、指令（Directive）は、EU の法令行為の一類型で、達成すべき結果について加盟国を拘束するが、そのための形式及び手段の選択は加盟国に委ねられている。

(7)　NIS 指令第 4 条第 1 項第 7 号において、インシデントは、「ネットワーク・情報システムの安全に実際上の有害効果を及ぼす全ての事象」と定義されている。情報セキュリティインシデントとは、「望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの」を指す。サイバーセキュリティ戦略本部　前掲注(4), p.34.

(8)　主な例として、加盟各国の刑法におけるサイバー犯罪の定義の調和や罰則強化を目的とした指令（Directive 2013/40/EU）、インターネットを利用した児童の性的搾取及び児童ポルノに関する対策強化を目的とした指令（Directive 2011/93/EU）などがある。後者については、植月献二「【EU】児童の性的搾取・児童ポルノ等の対策強化指令」『外国の立法』No.250-1, 2012.1, pp.6-7. <http://dl.ndl.go.jp/view/download/digidepo_3382152_po_02500103.pdf?contentNo=1&alternativeNo=> を参照。

(9)　Commission of the European Communities, “Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for A European Policy Approach,” COM(2001) 298 final, 2001.6.6. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52001DC0298>

ための戦略」[10]が採択され、2009年には、情報通信基盤をサイバー攻撃から保護するための対応措置を提案した政策文書[11]が採択された。

その後、経済・金融危機からの脱却を目指し、10か年の成長戦略を定めた、2010年の政策文書「欧州2020」[12]では、経済成長に向けた7施策の1つとして、インターネット高速化や情報技術を利用したサービスの促進などによる、デジタル経済の拡大が掲げられた。この実現に向けた具体的な取組を示した政策文書「欧州のためのデジタルアジェンダ」[13]では、デジタル経済拡大の阻害要因となっているサイバー犯罪の増加に対処し、ネットワークの安全と信頼を確保するため、EU諸機関及び加盟国国内でインシデントの防止・対応を担う組織を整備し、各国の法執行機関との連携を構築することなどが提案された。

2013年2月には、「EUサイバーセキュリティ戦略」[14]と題する政策文書が発表され、サイバー攻撃を含むインシデントへの対処能力の向上、サイバーセキュリティ対策に関する産業・技術開発など5つの優先項目における、EU諸機関、加盟国及び産業界それぞれの今後の取組が示された。同戦略と併せて提案されたのが、NIS指令案（2で後述）である。

さらに、域内の治安上の脅威とそれに対する政策・立法措置をまとめた2015年の行動計画[15]では、テロ及び組織犯罪と並び、サイバー犯罪が当面の優先課題と位置付けられた。

また、国家あるいは非国家主体が、重要インフラに対するサイバー攻撃や、ソーシャルメディアを利用した偽情報の拡散による世論又は意思決定過程への干渉・妨害などを、様々に組み合わせて行う「ハイブリッド脅威」に対するEUの方針を示した2016年4月の政策文書[16]においても、サイバーセキュリティ対策の強化が盛り込まれた。この中では、NIS指令の制定と確実な実施、官民の協働による技術開発、エネルギー・金融・輸送分野における対処能力強化の必要性が示された。また、加盟28か国中22か国が加盟し、サイバー防衛に関する対策を進めている北大西洋条約機構（NATO）との協力強化を重視することが強調された。

---

(10) Commission of the European Communities, “Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: A strategy for a Secure Information Society—“Dialogue, partnership and empowerment,”” COM(2006) 251 final, 2006.5.31. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52006DC0251>

(11) Commission of the European Communities, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection: “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience,”” COM(2009) 149 final, 2009.3.30. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52009DC0149>

(12) European Commission, “Communication from the Commission: Europe 2020: A strategy for smart, sustainable and inclusive growth,” COM(2010)2020 final, 2010.3.3. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010DC2020>

(13) European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe,” COM(2010)245 final/2, 2010.8.26. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010DC0245R(01)>

(14) European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, “Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,” JOIN(2013) 1 final, 2013.2.7. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001> 同戦略の優先5分野については、「EUの成長を支えるサイバーセキュリティ構築への取り組み」『EU MAG』Vol. 23, 2013.12.24. <http://eumag.jp/feature/b1213/> を参照。

(15) European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security,” COM(2015) 185 final, 2015.4.28. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015DC0185>

(16) European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, “Joint Communication to the European Parliament and the Council: Joint Framework on countering hybrid threats a European Union response,” JOIN(2016) 18 final, 2016.4.6. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018>

このように、サイバーセキュリティ対策は、デジタル経済発展に向けた安全と信頼の確保、詐欺やその他の犯罪行為の手段として行われるサイバー攻撃からの保護、さらに、国家等による干渉・攻撃の脅威からの防衛の一環として、対応が進められるようになっている。

(2) 主な対応組織

サイバーセキュリティ対策を EU レベルで担当する専門機関[17]として、2004 年に、欧州ネットワーク・情報セキュリティ機関（ENISA）が設立された[18]。この機関名は、2004 年の設置規則では「European Network and Information Security Agency」と表記され、後継の 2013 年の設置規則[19]で「European Union Agency for Network and Information Security」となっているが、略称は同じ ENISA である。ENISA は、サイバーセキュリティに関する情報収集、助言の提供、関係機関の連携促進などを任務としており、2010 年以降、大規模なインシデントの発生を想定し、加盟国等から関係者が参加するサイバー演習を隔年で実施している[20]。2016 年の予算は約 1100 万ユーロ[21]、同年末現在のスタッフ数は 69 名であった[22]。ENISA は、2013 年から 7 年間の期限付きの設置とされているが、これを EU サイバーセキュリティ機関（EU Cybersecurity Agency）として常設し、権限・機能を強化するための規則案が 2017 年 9 月 13 日に提出された[23]。同規則案は、人員・予算の拡大も目指している。

また、2012 年には、EU 諸機関の情報セキュリティ担当者から成る、コンピュータ緊急対応チーム（Computer Emergency Response Team for the EU institutions, agencies and bodies: CERT-EU）が設置された[24]。このほか、2013 年には、域内の重大犯罪に関する情報の収集、分析及び共有、各国警察機関の支援や相互協力の強化などを行うユーロポール（欧州警察機関）内に、欧州サイバー犯罪センター（European Cybercrime Centre: EC3）が設置されている[25]。

---

(17) 専門機関（補助機関ともいわれる）は、特定の任務を遂行するために EU の立法に基づいて設置されるもので、欧州環境庁、欧州医薬品庁、EU 基本権庁など多数存在する。辰巳浅嗣編著『EU―欧州統合の現在―　第 3 版』創元社, 2012, pp.89-92; 藤井良広『EU の知識　第 16 版』日本経済新聞出版社, 2013, pp.108-117.

(18) Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, *Official Journal of the European Union*, L77, 2004.3.13. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004R0460>

(19) Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, *Official Journal of the European Union*, L165, 2013.6.18. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0526>

(20) "Cyber Europe." ENISA website <https: //www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme> 2016 年 10 月 13～14 日に実施されたサイバー演習には、EU 加盟 28 か国と、欧州自由貿易連合（EFTA）加盟国のうちノルウェー及びスイスから、約 1,000 名の官民関係者が参加した。ENISA, *Cyber Europe 2016: After Action Report*, 2017. <https://www.enisa.europa.eu/publications/ce2016-after-action-report/at_download/fullReport>; "Cyber Europe 2016 – Questions and Answers," 2016.9. ENISA website <https://www.enisa.europa.eu/media/media-press-kits/press-kits/cyber-security-exercises-kit/ce2016/cyber-europe-2016-questions-and-answers>

(21) 1 ユーロは約 130 円（平成 30 年 5 月分報告省令レート）。

(22) ENISA, *Annual Activity Report 2016*, 2017. pp.53-55. <https://www.enisa.europa.eu/publications/corporate/enisa-annual-report-2016>

(23) Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM(2017) 477 final, 2017.9.13. <https: //eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0477> 同規則案では、ENISA の予算を 2019 年分から毎年拡大し、2022 年には年間 2300 万ユーロとすることが見込まれている。

(24) "About Us." Computer Emergency Response Team for the EU institutions, agencies and bodies (CERT-EU) website <https://cert.europa.eu/cert/plainedition/en/cert_about.html>

(25) "European Cybercrime Centre – EC3." Europol website <https://www.europol.europa.eu/about-europol/european-cyber crime-centre-ec3>

2　NIS 指令の目的及び制定

前述したサイバーセキュリティ戦略とともに、NIS 指令案は、2013 年 2 月 7 日に公表された[26]。提案に際し、欧州委員会は、域内でネットワーク・情報システムが相互に接続されているにもかかわらず、サイバーセキュリティに関するリスク対策やインシデントへの対処能力が加盟国によって大きく異なっていること、このため、対応が不十分な国の影響により、EU 全体のネットワーク・情報システムが脆弱化することを問題として指摘した。また、こうした状況は、対処のための相互協力・情報共有の前提となる信頼醸成の障害となっており、高い対処能力を持つ一部の加盟国間の協力に留まっていることも指摘した。[27]

このような問題点を踏まえ、NIS 指令案は、一定の基準を規定し、EU のネットワーク・情報システムの安全水準を向上させることを目指している。特に、指令案の目的として、次の 3 つが挙げられた。①各国において、ネットワーク・情報システムを管轄する官庁とインシデントの防止・対応を担うコンピュータ緊急対応チーム（Computer Emergency Response Team: CERT）を設置し、国家戦略及び国内における協力計画を策定することで、全ての加盟国が最低限の対処能力を備えること、②情報共有やインシデントの発見・対応に関する各国の管轄官庁間の協力ネットワークを構築すること、③従来、通信会社に対してのみ定められていたリスク管理手続及び重大インシデントの届出義務を、社会経済活動に不可欠な他の重要インフラにも拡大すること。[28]

NIS 指令は、2016 年 7 月 6 日に成立、同年 7 月 19 日に公布され、公布日から 20 日後の 8 月 8 日に施行された。加盟国には、2018 年 5 月 9 日までに指令を国内法制化することを義務付けている。

Ⅱ　NIS 指令の概要

1　構成及び法的根拠

NIS 指令は、第 1 章「総則」（第 1 条～第 6 条）、第 2 章「ネットワーク・情報システムの安全に関する国家枠組み」（第 7 条～第 10 条）、第 3 章「協力」（第 11 条～第 13 条）、第 4 章「基幹サービス運営者のネットワーク・情報システムの安全」（第 14 条～第 15 条）、第 5 章「デジタルサービス提供者のネットワーク・情報システムの安全」（第 16 条～第 18 条）、第 6 章「標準化及び任意の届出」（第 19 条～第 20 条）、第 7 章「最終規定」（第 21 条～第 27 条）の全 7 章 27 か条と、3 つの附属書から成る。

NIS 指令の立法上の根拠は、EU 運営条約第 114 条に置かれている[29]。同条は、EU 域内市場の設置・機能を目的として、加盟国の法令又は行政措置を調和させるため、EU の立法手続に従って措置を定めることを規定したものである。これに基づき、NIS 指令の第 1 条第 1 項は、

(26) Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final, 2013.2.7. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN>

(27) *ibid*., p.3.

(28) *ibid*., p.4.

(29) EU 運営条約（Treaty on the Functioning of the European Union）は、EU 条約（Treaty on European Union）と並ぶ EU の基本条約である。その第 114 条では、域内市場の設立及び機能を目的として、加盟国が定める法令等の規定を近似（approximation）させるための措置を、欧州議会及び EU 理事会が通常立法手続に従って採択することが定められている。

域内市場の機能を改善すべく、ネットワーク・情報システムに関し高度な共通安全水準の達成を目的とした措置を定めることとしている。ただし、これは最低基準を調和させるものであり、第 3 条では、加盟国が、より高度な安全水準達成のための措置を定めることも可能と規定されている。なお、この場合、加盟国は、デジタルサービス提供者に対しては更なる要件を課してはならず（2（4）で後述）、また、EU 法に基づく加盟国の義務には影響を与えない。

2　主な規定内容

NIS 指令の主な規定内容として、加盟国に義務付けられている、国家戦略の策定及び管轄官庁等の指定（(1) ～ (2)）、重要インフラを保有する基幹サービス運営者・デジタルサービス提供者の義務及びその他の企業等による任意のインシデント届出（(3) ～ (5)）、加盟国と EU 諸機関の協働のために設置される協力グループ及び CSIRT ネットワーク（(6) ～ (7)）、並びに罰則（(8)）について紹介する。

(1) ネットワーク・情報システムの安全に関する国家戦略

加盟国には、ネットワーク・情報システムの安全に関する国家戦略を採択し、欧州委員会に通知することが義務付けられている[(30)]。この国家戦略には、①国家戦略の目標及び優先事項、②政府機関、関係者等の役割及び責任を含む管理体制、③準備、対応及び復旧に関する措置、④教育、啓発及び訓練プログラム、⑤研究・開発計画、⑥リスク評価計画、⑦実施関係機関を記載しなければならない。（第 7 条）

(2) 加盟国国内の管轄官庁、CSIRT 及び単一窓口

加盟国は、基幹サービス運営者及びデジタルサービス提供者（(3) 及び（4）で後述）の事業分野を所掌する、1 又は 2 以上の管轄官庁を指定しなければならない。管轄官庁は、国内における NIS 指令の適用の監視を担う。（第 8 条）

さらに、加盟国は、コンピュータセキュリティインシデント対応チーム（Computer Security Incident Response Team: CSIRT）[(31)] を指定しなければならない。CSIRT は、リスク対応及びインシデント対応に責任を負う組織で、管轄官庁内に設置することも可能である。その任務は、①国内におけるインシデントの監視、②利害関係者に対するリスク及びインシデントに関する情報提供、③インシデント対応、④リスク及びインシデントの分析、⑤ CSIRT ネットワーク（(7) で後述）への参加である。CSIRT の要件として、その施設及びシステムの安全性、常時の連絡体制、及び十分な人員の配置を含む、業務継続性を確保することなどが定められている。（第 9 条及び附属書 1）

また、加盟国は、ネットワーク・情報システムの安全に関する連絡窓口となる単一窓口（single

(30) NIS 指令の制定以前に、ほぼ全ての加盟国において同分野に関する国家戦略が策定されている。これらの加盟国には、自国の既存の国家戦略が、NIS 指令が規定する国家戦略の要件に適合しているかどうかを確認し、必要に応じて指令の国内法化の期限である 2018 年 5 月 9 日までに改正することが求められている。European Commission, “Communication from the Commission to the European Parliament and the Council: Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union,” COM(2017) 476 final/2, 2017.10.4, Annex 1, pp.5-9. <https://eur-lex.europa.eu/resource.html?uri=cellar:d829f91d-9859-11e7-b92d-01aa75ed71a1.0001.02/DOC_4&format=PDF>

(31) コンピュータセキュリティインシデント対応チーム（CSIRT. シーサート）とは、企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万一問題が発生した場合にはその原因解析や影響範囲の調査等を行う体制をいう。サイバーセキュリティ戦略本部　前掲注(4), p.29.

point of contact）を指定しなければならない。単一窓口は、各国官庁間の協力や、協力グループ（(6) で後述）及び CSIRT ネットワークの協力において連絡機能を担うもので、管轄官庁が 1 つのみの場合には、その官庁が単一窓口となる。加盟国には、管轄官庁と単一窓口がそれぞれの任務を遂行するために十分な資源を確保するよう、義務付けられている。（第 8 条）

(3) 基幹サービス運営者

加盟国は、自国で設立された基幹サービス運営者（operator of essential services）を 2018 年 11 月 9 日までに特定しなければならない（第 5 条第 1 項）。基幹サービス運営者には、セキュリティ要件とインシデント届出の義務が課される（第 14 条）。対象となる事業分野と特定基準は、次のとおり定められている。

事業分野は、①エネルギー（電力、石油、ガス）、②輸送（航空、鉄道、水上、道路）、③銀行、④金融市場インフラ（証券取引所等）、⑤保健医療、⑥飲料水、⑦デジタルインフラの 7 種類であり、その定義等を含め附属書 2 に規定されている。前述のとおり、NIS 指令は最低限の基準の調和を定めたものであり、各国が事業分野の範囲を拡大することも可能である。これについては、複数の加盟国において、郵便、食品製造、化学・原子力産業、環境保護、市民保護（災害支援）といった分野を含めることが決定され又は検討されていると、欧州委員会の文書で報告されている(32)。

また、特定基準は、①重要な社会経済活動の維持に不可欠なサービスを提供する団体であること、②ネットワーク・情報システムに依存して①のサービスを提供していること、③①のサービス提供にとって、インシデントが重大な破壊的影響を及ぼすであろうことの 3 つである（第 5 条第 2 項）。なお、破壊的影響の重大性は加盟国が決定するが、その決定に当たっては、運営者が提供するサービスの利用者数、程度・期間の面で社会経済活動に又は公共の安全に及ぼす影響、運営者の市場占有率、影響の地理的分布などを考慮することが義務付けられている（第 6 条）。加盟国は、①のサービスのリスト、特定された基幹サービス運営者の数及び当該運営者の重要性を示す情報などを、欧州委員会に提出しなければならない（第 5 条第 7 項）。

基幹サービス運営者のセキュリティ要件として、加盟国は、サービスに使用されているネットワーク・情報システムのリスク管理や、インシデントによる影響の防止・最小化のため、運営者が適切な措置を講じるようにしなければならない。また、サービスの継続に重大な影響を及ぼすインシデントについて、基幹サービス運営者が管轄官庁又は CSIRT に届け出るようにしなければならない。他の加盟国でのサービスの継続に重大な影響を及ぼす場合には、管轄官庁又は CSIRT は、当該加盟国に対して通知するよう義務付けられている。インシデントの防止又はインシデントへの対処のため、個別のインシデントについて公衆に知らせる必要がある場合には、管轄官庁又は CSIRT は、届出を行った運営者と協議した上で、公衆に周知することができる。（第 14 条）

(4) デジタルサービス提供者

各加盟国が特定する基幹サービス運営者とは異なり、デジタルサービス提供者については、NIS 指令が規定するデジタルサービスを提供する、全ての法人が対象となる(33)。該当するデジ

(32) European Commission, *op.cit.*(30), pp.23-24.

タルサービスは、①ウェブサイト上で商品の販売やオンラインサービスに係る契約を行うためのオンラインマーケット、②オンライン検索エンジン、③クラウドコンピューティングサービスの 3 種類である。（第 4 条第 5 号及び第 6 号、附属書 3）。ただし、小規模企業及び零細企業[34]は、適用が除外される（第 16 条第 11 項）。

デジタルサービス提供者にも、基幹サービス運営者と同様に、EU 域内で提供するサービスに使用するネットワーク・情報システムの安全のための措置の確保、インシデントの影響を防止・最小化するための措置の確保、サービス提供に重大な影響があるインシデント発生時の届出と他の加盟国への通知、必要な場合の公衆への通知などが定められている（第 16 条第 1 項～第 3 項、第 6 項及び第 7 項）。ただし、加盟国の本質的な国家機能の保護（国家安全保障等）及び法と秩序の維持のために行う行為を除き、デジタルサービス提供者に対しては、加盟国が更なるセキュリティ要件･インシデント届出要件を課すことは禁止されている（第 16 条第 10 項）。

デジタルサービス提供者は、主たる事業所が置かれた加盟国の管轄権の下にあるとみなされる。EU 域外で設立され、域内で①から③のサービスを提供する事業者は、サービスを提供する加盟国のうちの 1 つに、代表者を置かなければならない。（第 18 条）

(5) 任意の届出

基幹サービス運営者と特定されず、デジタルサービス提供者でもない団体は、提供するサービスの継続性に重大な影響を及ぼすインシデントを、任意で届け出ることができる。届出とその処理の手続の流れは、基幹サービス運営者と同様だが、加盟国は、任意の届出の処理よりも義務に基づく届出の処理を優先することができると定められている。（第 20 条）

(6) 協力グループ

加盟国間の戦略的協力及び情報共有の支援・促進等を目的として、加盟国、欧州委員会及び ENISA の代表者から成る、協力グループが設置される。協力グループの任務は、CSIRT ネットワーク（(7) で後述）の活動に対する戦略的指導、基幹サービス運営者及びデジタルサービス提供者によるインシデントの届出に関するベストプラクティス（最良の事例）の共有、ネットワーク・情報システムの安全確保に向けた加盟国の取組の共有、加盟国の能力構築支援、啓発・訓練及び研究・開発に関する情報共有などである。協力グループは、2018 年 2 月 9 日までに、かつそれ以降 2 年ごとに、その目的・任務の遂行に関する作業プログラムを定めなければならない。（第 11 条）

---

(33) 基幹サービス運営者は各国の物的インフラが対象であるのに対し、デジタルサービス提供者は複数の国をまたいだサービス提供を行うという特質を持つ。このような違いを踏まえ、基準の調和に関して両者には異なる手続が設けられた。デジタルサービス提供者に対しては、域内でより均一的な規制となるよう目指されている。（NIS 指令前文（57））

(34) 以下の委員会勧告に基づき、小規模企業は、従業員数 50 人未満で、年間売上高又は年次貸借対照表の合計が 1000 万ユーロ以下の企業を指し、零細企業は、従業員数 10 人未満で、年間売上高又は年次貸借対照表の合計が 200 万ユーロ以下の企業を指す。Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, *Official Journal of the European Union*, L124, 2003.5.20. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361> なお、適用対象外となっている小規模企業等がサイバー攻撃の入口となる可能性もあることから、この範囲については今後見直しが必要であろうといった課題も指摘されている。Annegret Bendiek et al., “The EU’s Revised Cybersecurity Strategy: Half-Hearted Progress on Far-Reaching Challenges,” *SWP Comments*, 47, 2017.11, p.4. German Institute for International and Security Affairs website <https: //www.swp-berlin.org/fileadmin/contents/products/comments/2017C47_bdk_etal.pdf>

(7) CSIRT ネットワーク

リスク対策及びインシデント対応の実施組織として各国で指定された CSIRT と、CERT-EU（Ⅰ 1(2)を参照）の代表者から成る、CSIRT ネットワークが設置される。CSIRT ネットワークでは、ENISA が事務局の提供と各国 CSIRT 間協力の支援を行い、また、欧州委員会がオブザーバーとして参加する。CSIRT ネットワークの任務は、各国 CSIRT に係る情報の共有、確認されたインシデントに係る検討、インシデント及び関連リスクに関する情報共有、国境を越えるインシデント対応の際の加盟国支援、更なる実施協力形態の検討などである。（第 12 条）

なお、協力グループと CSIRT ネットワークは、NIS 指令の国内法制化期限（2018 年 5 月 9 日）までの期間に協力活動を行うため、それぞれ規定の任務を 2017 年 2 月 9 日までに開始する（第 24 条）。

(8) 罰則

加盟国は、NIS 指令に基づき採択された国内規定への違反があった場合に適用可能な罰則規定を定め、その実施を確保するための措置を講じなければならない（第 21 条）。

Ⅲ　NIS 指令制定後の動向

NIS 指令の制定以降、欧州委員会及び ENISA を中心として、加盟国による実施を支援するための取組が進められている[35]。

1　NIS 指令の実施に向けた取組

欧州委員会及び外務・安全保障政策上級代表は 2017 年 9 月 13 日、EU のサイバーセキュリティ対策に関する新たな政策文書の中で、今後の対策においては、NIS 指令を確実に実施することが不可欠だとあらためて確認した[36]。この政策文書発表と同日に、欧州委員会は、NIS 指令の主な規定の趣旨や実施方法をまとめた文書を公表した[37]。同文書では特に、ネットワーク・情報システムの安全に関する国家戦略の採択、国内の管轄官庁・単一窓口・CSIRT の設置、基幹サービス運営者の特定、デジタルサービス提供者の類型などについて、解説や手順が整理されている。

なお、加盟国、欧州委員会及び ENISA の代表者から成る協力グループについては、2017 年 2 月 1 日の欧州委員会実施決定[38]でその運営の詳細が定められた。協力グループは、EU 理事

(35) 各国における国内法制化の状況及び指定された単一窓口等の情報については、欧州委員会のウェブサイトを参照。“State-of-play of the transposition of the NIS Directive.” European Commission website <https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive>

(36) European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, *op.cit*.(2), pp.6-7.

(37) European Commission, “Communication from the Commission to the European Parliament and the Council: Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union,” COM(2017) 476 final/2, 2017.10.4. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC0476>

(38) Commission Implementing Decision (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, *Official Journal of the European Union*, L28, 2017.2.2. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017D0179>

会[39]の議長国（加盟国による輪番制）が議長を担当し、会合等の議論の内容や文書は原則として非公開とされる。2017 年 2 月から 2018 年 5 月までの間に 6 回の会合が開催され、基幹サービス運営者によるセキュリティ対策措置及びインシデント届出に関するガイドラインが策定された[40]。

デジタルサービス提供者については、2018 年 1 月 30 日の欧州委員会実施規則[41]で、セキュリティ対策措置に当たって考慮すべき要素（NIS 指令第 16 条第 1 項で規定）と、インシデントの影響の重大性を確定するために考慮すべき条件（NIS 指令第 16 条第 4 項で規定）の詳細が定められた。この実施規則では、次の 4 条件のいずれかに該当する場合には、インシデントは重大な影響を有するものとみなされ、届出義務の対象となることが定められた。①域内で 1 時間に延べ 500 万人を超える利用者が、デジタルサービス提供者のサービスを使用できなかった、② 10 万人を超える利用者に、インシデントによるデータ損失やサービス障害の影響が及んでいる、③インシデントが、公共の安全に対する危険や人命損失の危険をもたらしている、④インシデントが、100 万ユーロを超える物質的損害をもたらしている。

２　加盟国に対する財政支援

このほか、インフラ構築に対する EU の財政支援の枠組みである、コネクティング・ヨーロッパ・ファシリティ（Connecting Europe Facility: CEF）[42]のプログラムを通じた資金提供も実施されている。欧州委員会によれば、各国 CSIRT 間における情報共有の円滑化を目的としたプログラムに対して 630 万ユーロが提供され、また、ソフトウェア購入、人材育成、演習の実施など各国 CSIRT の能力向上を目的としたプログラムに対し、2017 年から 2020 年の間に 1870 万ユーロが配分されるほか、今後、NIS 指令の対象となる関係者に対し、さらに 1300 万ユーロの提供の用意があるとされる[43]。

おわりに

NIS 指令では、エネルギー、輸送、金融、医療等の重要インフラを保有する企業に対して、十分なセキュリティ対策と重大インシデントの届出が義務化された。これは原則として EU 域内の企業活動に適用されるが、NIS 指令の制定に当たっては、米国系のグローバル企業に対してどのような義務が課されるかが注目されていた[44]。これについて、NIS 指令では、主要なイン

(39) EU 理事会（Council of the European Union）は、加盟国の閣僚級代表により構成される機関で、閣僚理事会とも呼ばれる。

(40) 各会合の議題及び両ガイドラインについては、欧州委員会ウェブサイトを参照。“NIS Cooperation Group.” European Commission website <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group>

(41) Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, *Official Journal of the European Union*, L26, 2018.1.31. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0151>

(42) コネクティング・ヨーロッパ・ファシリティ（Connecting Europe Facility: CEF）は、エネルギー、通信、輸送の 3 分野のインフラ構築に対して EU が財政的支援を提供する枠組み。“Connecting Europe Facility.” European Commission website <https://ec.europa.eu/inea/en/connecting-europe-facility>

(43) European Commission, “Questions and Answers: Directive on Security of Network and Information systems, the first EU-wide legislation on cybersecurity,” 2018.5.4. <http://europa.eu/rapid/press-release_MEMO-18-3651_en.htm>

(44) 情報処理推進機構（IPA）『情報セキュリティ白書　2016』2016, p.85.

ターネット関連企業には、サービスを提供する域内の加盟国の 1 つに代表者を指定することが定められ、域内の企業と同様に、重大インシデントが発生した際の届出が義務付けられることとなった。違反の場合には、罰則を課すことも可能である。

加盟国における NIS 指令の実施に向けた取組と並行して、2017 年 9 月 13 日には、加盟国支援を担う ENISA の強化や、情報通信技術関連の製品・サービスの安全性に関する認証制度の創設を目的とする新たな規則案(45)が提出され、審議が行われている。国際社会共通の課題として、対策の動向を引き続き注視する必要があるだろう。

（しまむら　ともこ）

(45) *op.cit.*(23)

ネットワーク・情報システムに係る欧州連合共通の高度な安全水準のための措置に関する2016年7月6日の欧州議会及び理事会の指令（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

国立国会図書館　調査及び立法考査局
海外立法情報課　島村　智子訳

【目次】

第1章　総則（第1条～第6条）
第2章　ネットワーク・情報システムの安全に関する国家枠組み（第7条～第10条）
第3章　協力（第11条～第13条）
第4章　基幹サービス運営者のネットワーク・情報システムの安全（第14条～第15条）
第5章　デジタルサービス提供者のネットワーク・情報システムの安全（第16条～第18条）
第6章　標準化及び任意の届出（第19条～第20条）
第7章　最終規定（第21条～第27条）
附属書1　コンピュータセキュリティインシデント対応チーム（CSIRT）の要件及び任務
附属書2　第4条第4号［基幹サービス運営者］の目的における団体の類型
附属書3　第4条第5号［デジタルサービス］の目的におけるデジタルサービスの類型

欧州議会及び欧州連合理事会は、欧州連合運営条約、特にその第114条(1)に鑑み、［…中略…］この指令を採択した。

第1章　総則

第1条　主題及び範囲

1. この指令は、域内市場の機能を改善するため、ネットワーク・情報システムに係る欧州連合共通の高度な安全水準の達成を目的として、措置を定めるものである。
2. この目的のため、この指令は、次の各号に掲げる事項を規定する。
   (a) 全ての加盟国がネットワーク・情報システムの安全に関する国家戦略を採択する義務を定めること。

＊　注は全て訳者によるものであり、規則、指令等の詳細を示した原注は、本稿のフォーマットに合わせて脚注に取り込んだ。訳文中の［ ］内の語句は、訳者による補記である。また、訳文の「理事会」は全てEU理事会（Council of the European Union）を、補記のない「委員会」は全て欧州委員会（European Commission）を指す。なお、本稿におけるインターネット情報の最終アクセス日は、2018年5月23日である。

(1)　EU運営条約（Treaty on the Functioning of the European Union）は、EU条約（Treaty on European Union）と並ぶEUの基本条約である。その第114条では、域内市場の設立及び機能を目的として、加盟国が定める法令等の規定を近似（approximation）させるための措置を、欧州議会及びEU理事会が通常立法手続に従って採択することが定められている。

(b)　加盟国間の戦略的協力及び情報交換を支援し及び促進し、並びに加盟国間の信頼及び信任を構築することを目的として、協力グループを創設すること。

(c)　加盟国間の信頼及び信任の構築、並びに迅速かつ実効性ある実施協力の促進に資することを目的として、コンピュータセキュリティインシデント対応チームネットワーク（「CSIRT ネットワーク」）(2) を創設すること。

(d)　基幹サービス運営者［原語は operators of essential services］(3) 及びデジタルサービス提供者 (4) のセキュリティ要件及び届出要件を定めること。

(e)　加盟国が、ネットワーク・情報システムの安全に関する任務を負う国内の管轄官庁、単一窓口及び CSIRT を指定する義務を定めること。

3.　この指令が規定するセキュリティ要件及び届出要件は、指令 2002/21/EC (5) の第 13a 条及び第 13b 条の要件の対象である［電子通信］事業者又は規則（EU）No 910/2014 (6) の第 19 条の要件の対象である認証サービス提供者には適用されないものとする。

4.　この指令は、理事会指令 2008/114/EC (7) 並びに欧州議会及び理事会の指令 2011/93/EU (8) 及び 2013/40/EU (9) に影響を及ぼすことなく適用される。

5.　商業上の秘密保持に関する規定を含む、欧州連合及び各国の規定に基づく機密情報は、この指令の適用に必要な場合に限り、欧州連合運営条約の第 346 条 (10) に影響を及ぼすことなく、委員会及びその他の関係官庁と交換されるものとする。交換される情報は、当該交換の目的に照らし妥当、かつ、均衡の取れた範囲に限られなければならない。このような情報交換に際しては、当該情報の機密性が保持されなければならず、基幹サービス運営者及びデジタルサービス提供者の安全及び商業的利益が保護されなければならない。

6.　この指令は、加盟国の本質的な国家機能を保護するため、特に、国家の安全を保護するため、公開が自国の安全上の本質的な利益に反すると加盟国がみなす情報を保護する行為を含む加盟国がなす行為、並びに法と秩序を維持するため、特に、犯罪行為の捜査、発見及び訴追を可能とするために加盟国がなす行為に影響を与えない。

---

(2)　コンピュータセキュリティインシデント対応チーム（computer security incident response team: CSIRT）については第 9 条を参照。CSIRT ネットワークについては第 12 条を参照。

(3)　第 4 条第 4 号を参照。

(4)　第 4 条第 5 号及び第 6 号を参照。

(5)　Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), *Official Journal of the European Union*, L108, 2002.4.24. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002L0021-20091219>

(6)　Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, *Official Journal of the European Union*, L257, 2014.8.28. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910>

(7)　Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *Official Journal of the European Union*, L345, 2008.12.23. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114>

(8)　Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, *Official Journal of the European Union*, L335, 2011.12.17. <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1518574358205&uri=CELEX:02011L0093-20111217>

(9)　Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, *Official Journal of the European Union*, L218, 2013.8.14. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0040>

(10)　EU 運営条約の第 346 条では、加盟国がその開示を自国の安全保障上の重大な利益に反するとみなす情報について提供を義務付けられないという原則の適用を、EU 条約及び EU 運営条約の規定が妨げてはならないと規定している。

7. 特定部門のための欧州連合の法行為が、基幹サービス運営者又はデジタルサービス提供者に対し、ネットワーク・情報システムの安全確保又はインシデント届出のいずれかを義務付けており、その要件が、この指令が規定する義務と、効果において少なくとも同等である場合には、当該の特定部門のための欧州連合の法行為の規定が適用されるものとする。

第 2 条　個人データの取扱い

1. この指令に基づく個人データの取扱いは、指令 95/46/EC(11) に従って、行わなければならない。

2. この指令に基づく欧州連合諸機関による個人データの取扱いは、規則（EC）No 45/2001(12) に従って、行わなければならない。

第 3 条　最低限の調和

加盟国は、第 16 条第 10 項及び欧州連合の法に基づく加盟国の義務に影響を及ぼすことなく、ネットワーク・情報システムのより高度な安全水準の達成を目的とした規定を採択し又は維持することができる。

第 4 条　定義

この指令の目的のため、次の各号に掲げる定義を適用する。

(1) 「ネットワーク・情報システム」とは、次のいずれかに該当するものをいう。
  (a) 指令 2002/21/EC(13) の第 2 条第 a 号が意味するところの電子通信ネットワーク
  (b) 機器又は相互に接続された若しくは関連する機器の集まりであり、そのうち 1 又は 2 以上が、プログラムに基づきデジタルデータの自動処理を行うもの
  (c) 第 a 号及び第 b 号に該当する要素が、その操作、使用、保護及び保全を目的として、保存し、処理し、検索し又は送信するデジタルデータ

(2) 「ネットワーク・情報システムの安全」とは、当該ネットワーク・情報システムが提供する又は当該ネットワーク・情報システムを通じてアクセス可能な、保存され、送信され若しくは処理されたデータ又は関連サービスについて、その可用性、真正性、完全性又は機密性(14) を危険にさらす全ての行為を、ネットワーク・情報システムが、一定水準の確実性をもって、阻止し得ることをいう。

(3) 「ネットワーク・情報システムの安全に関する国家戦略」とは、国家レベルでネットワーク・情報システムの安全に関する戦略目標及び優先事項を規定する枠組みをいう。

(4) 「基幹サービス運営者」とは、第 5 条第 2 項が規定する基準を満たす、附属書 2 に掲げる類

---

(11) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Union*, L281, 1995.11.23. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046> この指令は、2016 年制定の一般データ保護規則（Regulation (EU) 2016/679）（General Data Protection Regulation: GDPR）により 2018 年 5 月 24 日をもって廃止され、翌 25 日からは、同規則のことを指す。

(12) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, *Official Journal of the European Union*, L8, 2001.1.12. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001R0045>

(13) *op.cit*.(5)

(14) 可用性（availability）とは、情報に関して正当な権限を持った者が、必要時に中断することなく、情報にアクセスできることをいう。完全性（integrity）とは、情報に関して破壊、改ざん又は消去されていないことをいう。機密性（confidentiality）とは、情報に関して正当な権限を持った者だけが、情報にアクセスできることをいう。これら 3 つは、情報セキュリティの 3 大要素と呼ばれる。サイバーセキュリティ戦略本部『サイバーセキュリティ 2017』2017.8.25, p.32. 内閣サイバーセキュリティセンターウェブサイト <https://www.nisc.go.jp/active/kihon/pdf/cs2017.pdf>

型の、公共又は民間の団体をいう。

(5) 「デジタルサービス」とは、附属書 3 に掲げる類型の、欧州議会及び理事会の指令（EU）2015/1535[15]の第 1 条第 1 項第 b 号が意味するところのサービスをいう。

(6) 「デジタルサービス提供者」とは、デジタルサービスを提供する全ての法人をいう。

(7) 「インシデント」とは、ネットワーク・情報システムの安全に実際上の有害効果を及ぼす全ての事象をいう。

(8) 「インシデント対応」とは、インシデントの調査、分析及び抑制並びにインシデントへの対応を支援する全ての手続をいう。

(9) 「リスク」とは、ネットワーク・情報システムの安全に有害効果を及ぼす可能性がある、全ての合理的に特定可能な状況又は事象をいう。

(10) 「代表者」とは、欧州連合域内に置かれた自然人又は法人であって、欧州連合域外で設置されたデジタルサービス提供者を代行するよう明示的に指定された者をいい、各国の管轄官庁又は CSIRT が、この指令に基づくデジタルサービス提供者の義務に関し、当該デジタルサービス提供者の代わりに名宛人とすることができる者をいう。

(11) 「標準」とは、規則（EU）No 1025/2012[16]の第 2 条第 1 号が意味するところの標準をいう。

(12) 「仕様」とは、規則（EU）No 1025/2012 の第 2 条第 4 号が意味するところの技術仕様をいう。

(13) 「インターネット相互接続点（IXP）」とは、インターネット通信の交換促進を主な目的として、2 以上の独立した自律システムの相互接続を可能とする、ネットワーク設備をいう。IXP は、自律システムに限り相互接続を提供する。IXP は、関係する 2 つの自律システム間で伝達されるインターネット通信が、いかなる第 3 の自律システムを通過することも要さず、また、当該通信を変更又は妨害しない。

(14) 「ドメインネームシステム（DNS）」[17]とは、ドメイン名の問合せを照会するネットワーク上の階層的な分散型ネーミングシステムをいう。

(15) 「DNS サービス提供者」とは、インターネット上で DNS サービスを提供する全ての団体をいう。

(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）[18]に

---

(15) Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, *Official Journal of the European Union*, L241, 2015.9.17. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L1535>

(16) Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council, *Official Journal of the European Union*, L316, 2012.11.14. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02012R1025-20151007>

(17) ドメインネームシステム（Domain Name System: DNS）は、ドメイン名（国、組織、サービス等の単位で割り当てられたインターネット上の名前であり、英数字等を用いて表したもの）と IP アドレス（インターネットやイントラネットなど、IP ネットワークに接続されたコンピュータや通信機器等に割り振られた識別番号）を対応付けて管理するシステムを指す。サイバーセキュリティ戦略本部『サイバーセキュリティ政策に係る年次報告　2016 年度』2017.7.13, pp.217-218, 224. 内閣サイバーセキュリティセンターウェブサイト <https://www.nisc.go.jp/active/kihon/pdf/jseval_2016.pdf>

(18) トップレベルドメイン（TLD）は、ドメイン名において、ドットで区切られた文字列の一番右の部分（ラベル）で、「com」「jp」「us」などの部分を指す。「解説：TLD（トップレベルドメイン）」日本レジストリサービス（JPRS）ウェブサイト <https://jprs.jp/glossary/index.php?ID=0058>

ついて、インターネットのドメイン名の登録を管理し及び運営する全ての団体をいう。

(17) 「オンラインマーケット」とは、欧州議会及び理事会の指令2013/11/EU[19]の第4条第1項第a号及び第b号がそれぞれ定義する消費者、取引業者又はその両方が、オンラインマーケットのウェブサイト又はオンラインマーケットが提供するコンピューティングサービスを使用した取引業者のウェブサイトにおいて、オンライン販売又はオンラインサービスに係る契約を締結することを可能とするデジタルサービスをいう。

(18) 「オンライン検索エンジン」とは、利用者が、キーワード、フレーズ又はその他の入力データの形式によるあらゆる主題に関する問合せに基づき、原則として、全てのウェブサイト又は特定言語のウェブサイトの検索を行うことを可能とし、かつ、要求内容に関する情報を得られるリンクを返答するデジタルサービスをいう。

(19) 「クラウドコンピューティングサービス」[20]とは、共用可能なコンピュータ資源の、拡張性及び柔軟性のある蓄積へのアクセスを可能とするデジタルサービスをいう。

第5条　基幹サービス運営者の特定

1. 加盟国は、2018年11月9日までに、附属書2に掲げる部門及び下位部門について、自国の領域に事業所を持つ基幹サービス運営者を特定しなければならない。
2. 第4条第4号に掲げる基幹サービス運営者の特定基準は、次の各号に掲げるとおりとする。
   (a) 重要な社会活動、経済活動又はその両方の維持に不可欠なサービスを提供する団体であること。
   (b) 当該サービスの提供をネットワーク・情報システムに依存していること。
   (c) インシデントが、当該サービスの提供にとって重大な破壊的影響を及ぼすであろうこと。
3. 第1項の目的のため、各加盟国は、第2項第a号に掲げるサービスの一覧表を作成しなければならない。
4. 第1項の目的のため、ある団体が第2項第a号に掲げるサービスを2以上の加盟国で提供する場合には、当該加盟国は相互協議を行わなければならない。当該協議は、特定に係る決定がなされる前に行われなければならない。
5. 加盟国は、定期的に、かつ、2018年5月9日以後少なくとも2年ごとに、特定された基幹サービス運営者の一覧表を再審査し、必要に応じて、更新しなければならない。
6. 協力グループの役割は、第11条に掲げる任務に基づき、加盟国が基幹サービス運営者の特定過程において、整合性のとれた取組を行うよう支援することとする。
7. 加盟国は、第23条に掲げる再審査の目的のため、2018年11月9日までに、かつ、それ以降2年ごとに、委員会がこの指令の実施、特に、加盟国による基幹サービス運営者の特定方法の整合性を評価するために、必要な情報を委員会に提出しなければならない。当該情報には、少なくとも次の各号に掲げる事項を含めなければならない。

---

(19) Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR), *Official Journal of the European Union*, L165, 2013.6.18. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0011>

(20) クラウドは、インターネット等のブロードバンド回線を経由して、データセンタに蓄積されたコンピュータ資源を役務（サービス）として、第三者（利用者）に対して遠隔地から提供するものを指す。サイバーセキュリティ戦略本部　前掲注(14), p.33.

(a)　基幹サービス運営者を特定するための国内措置
(b)　第 3 項に掲げるサービスの一覧表
(c)　附属書 2 に掲げる各部門において特定された基幹サービス運営者の数、及び当該部門における特定された運営者の重要性の概要
(d)　第 6 条第 1 項第 a 号に掲げるサービスを利用する利用者の数又は第 6 条第 1 項第 f 号に掲げる特定された基幹サービス運営者の重要性を参照して、適切な供給水準を決定するための最低基準が存在する場合には、その値

委員会は、比較可能な情報の提供に資することを目的として、ENISA［欧州ネットワーク・情報セキュリティ機関］(21)の意見を最大限考慮し、この項に掲げる情報の範囲に関する適切な技術的指針を採択することができる。

第 6 条　重大な破壊的影響

1. 加盟国は、第 5 条第 2 項第 c 号に掲げる破壊的影響の重大性の決定に際し、少なくとも次の各号に掲げる分野横断的要素を考慮しなければならない。
(a)　関係する団体が提供するサービスを利用する利用者の数
(b)　当該団体が提供するサービスに対する、附属書 2 に掲げる他の部門の依存度
(c)　インシデントが、程度及び期間の観点において、社会経済活動又は公共の安全に及ぼす影響
(d)　当該団体の市場占有率
(e)　インシデントによって影響を受ける可能性がある地域の地理的範囲
(f)　当該サービス提供の代替手段の利用可能性を考慮した上で、十分なサービスを維持するための当該団体の重要性
2. 加盟国は、インシデントが重大な破壊的影響を及ぼすかどうかを決定するため、必要に応じて、部門特有の要素も考慮しなければならない。

第 2 章　ネットワーク・情報システムの安全に関する国家枠組み

第 7 条　ネットワーク・情報システムの安全に関する国家戦略

1. 各加盟国は、ネットワーク・情報システムの高度な安全水準の達成及び維持を目的とした戦略目標並びに適切な政策及び規制措置を定義し、かつ、少なくとも附属書 2 に掲げる部門及び附属書 3 に掲げるサービスを対象とする、ネットワーク・情報システムの安全に関する国家戦略を採択しなければならない。ネットワーク・情報システムの安全に関する国家戦略は、特に、次の各号に掲げる事項が記載されたものでなければならない。
(a)　ネットワーク・情報システムの安全に関する国家戦略の目標及び優先事項
(b)　政府機関及び他の関係者の役割及び責任を含む、ネットワーク・情報システムの安全に関する国家戦略の目標及び優先事項を達成するための管理体制
(c)　官民の協力を含む、準備、対応及び復旧に関する措置の特定

(21) 欧州ネットワーク・情報セキュリティ機関（European Union Agency for Network and Information Security: ENISA）は、2004 年に設置された、ネットワーク・情報セキュリティに関する対応能力の促進を任務とする EU の機関。“About ENISA.” European Union Agency for Network and Information Security (ENISA) website <https://www.enisa.europa.eu/about-enisa>

(d)　ネットワーク・情報システムの安全に関する国家戦略についての教育、啓発及び訓練プログラムの概要

(e)　ネットワーク・情報システムの安全に関する国家戦略についての研究及び開発計画の概要

(f)　リスク特定のためのリスク評価計画

(g)　ネットワーク・情報システムの安全に関する国家戦略の実施に関与する様々な主体の一覧表

2.　加盟国は、ネットワーク・情報システムの安全に関する国家戦略の策定に際し、ENISA からの支援を要請することができる。

3.　加盟国は、ネットワーク・情報システムの安全に関する国家戦略の採択から 3 か月以内に、当該戦略を委員会に通知しなければならない。その際、加盟国は、当該戦略のうち国家安全保障に関する要素を除外することができる。

第 8 条　国内の管轄官庁及び単一窓口

1.　各加盟国は、少なくとも附属書 2 に掲げる部門及び附属書 3 に掲げるサービスを所掌する、ネットワーク・情報システムの安全に関する国内管轄官庁（「管轄官庁」）を、1 又は 2 以上指定しなければならない。加盟国は、この役割を既存の 1 又は 2 以上の官庁に課すことができる。

2.　管轄官庁は、国家レベルにおいてこの指令の適用を監視しなければならない。

3.　各加盟国は、ネットワーク・情報システムの安全に関する国内の単一の窓口（「単一窓口」）を指定しなければならない。加盟国は、この役割を既存の官庁に課すことができる。加盟国が管轄官庁を 1 つのみ指定する場合には、当該管轄官庁が単一窓口とならなければならない。

4.　単一窓口は、加盟国官庁間及び他の加盟国の関係官庁との国境を越える協力、並びに第 11 条に掲げる協力グループ及び第 12 条に掲げる CSIRT ネットワークとの協力を確保するため、連絡機能を遂行しなければならない。

5.　加盟国は、管轄官庁及び単一窓口が課された任務を効果的かつ効率的に遂行し、それによってこの指令の目的を達成するため、両者に十分な資源を確保しなければならない。加盟国は、協力グループにおいて、指定された代表者による効果的で、効率的かつ安定した協力を確保しなければならない。

6.　管轄官庁及び単一窓口は、必要に応じ、国内法に基づき、関連する国内の法執行官庁及び国内のデータ保護官庁と協議し及び協力しなければならない。

7.　各加盟国は、管轄官庁及び単一窓口の指定、その任務並びに後日の変更について、委員会に遅滞なく通知しなければならない。各加盟国は、指定した管轄官庁及び単一窓口を公表しなければならない。委員会は、指定された単一窓口の一覧表を公表しなければならない。

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）

1.　各加盟国は、明確に定義された手順に基づくリスク対応及びインシデント対応に責任を有し、少なくとも附属書 2 に掲げる分野及び附属書 3 に掲げるサービスを対象とし、附属書 1 の（1）が規定する要件を遵守した、1 又は 2 以上の CSIRT を指定しなければならない。管轄官庁内に、CSIRT を設置することもできる。

2.　加盟国は、CSIRT が、附属書 1 の（2）が規定する任務を効果的に実施するために十分な資源を確保しなければならない。

加盟国は、第 12 条に掲げる CSIRT ネットワークにおいて、自国の CSIRT による効果的で、効率的かつ安定した協力を確保しなければならない。

3. 加盟国は、自国の CSIRT が、国家レベルにおいて、適切で、安定し、かつ強靭な情報通信インフラを利用できるようにしなければならない。
4. 加盟国は、自国の CSIRT の権限及びインシデント対応手順の主な要素について、委員会に通知しなければならない。
5. 加盟国は、国内の CSIRT の構築に際し、ENISA からの支援を要請することができる。

第 10 条　国家レベルの協力

1. 同一加盟国の管轄官庁、単一窓口及び CSIRT は、それらが異なる組織である場合には、この指令が規定する義務の履行に関し、協力しなければならない。
2. 加盟国は、管轄官庁又は CSIRT のいずれかが、この指令に基づき提出されたインシデント届出を受理するようにしなければならない。加盟国が、CSIRT は届出を受理しないと決定する場合、CSIRT は、その任務を果たすために必要な範囲において、第 14 条第 3 項及び第 5 項に基づく基幹サービス運営者からのインシデント届出又は第 16 条第 3 項及び第 6 項に基づくデジタルサービス提供者からのインシデント届出に関するデータに対し、アクセスが許可されなければならない。
3. 加盟国は、管轄官庁又は CSIRT が、この指令に基づき提出されたインシデント届出について、単一窓口に通知するようにしなければならない。

単一窓口は、2018 年 8 月 9 日までに、かつ、それ以降毎年、受理した届出、並びに第 14 条第 3 項及び第 5 項並びに第 16 条第 3 項及び第 6 項に従ってなされた行為に関する概要報告書を協力グループに提出しなければならない。受理した届出には、届出の件数及び届け出られたインシデントの特質を含めるものとする。

第 3 章　協力

第 11 条　協力グループ

1. 加盟国間の戦略的協力及び情報交換を支援し及び促進し、信頼及び信任を構築するため、並びにネットワーク・情報システムに係る欧州連合共通の高度な安全水準の達成を目的として、協力グループが設置される。

協力グループは、第 3 項の後段に掲げる隔年の作業プログラムに基づき、その任務を遂行しなければならない。

2. 協力グループは、加盟国、委員会及び ENISA の代表者から構成されるものとする。

協力グループは、必要に応じて、利害関係者の代表者をその作業に招請することができる。

委員会は、事務局を提供しなければならない。

3. 協力グループは、次の各号に掲げる任務を有するものとする。
   (a)　第 12 条に基づき設置された CSIRT ネットワークの活動に対し、戦略的指導を行うこと。
   (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 項に掲げるインシデント届出に関する情報交換について、ベストプラクティス［最良の事例］を共有すること。
   (c)　ネットワーク・情報システムの安全を確保するため、ベストプラクティスを加盟国間で共有し、ENISA と共同で、加盟国における能力構築を支援すること。

(d)　加盟国の能力及び準備状況を検討し、ネットワーク・情報システムの安全に関する国家戦略及び CSIRT の実効性を任意に評価し、並びにベストプラクティスを特定すること。
(e)　啓発及び訓練に関する情報及びベストプラクティスを共有すること。
(f)　ネットワーク・情報システムの安全に関する研究及び開発について、情報及びベストプラクティスを共有すること。
(g)　関連性がある場合には、ネットワーク・情報システムの安全に関する事項について、欧州連合の諸機関と経験を共有すること。
(h)　第 19 条に掲げる標準及び仕様について、関係する欧州の標準化組織の代表者と検討すること。
(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の情報を収集すること。
(j)　第 10 条第 3 項の後段に掲げる概要報告書を、毎年審査すること。
(k)　ENISA による作業を含め、ネットワーク・情報システムの安全、教育プログラム及び訓練に関する演習に関連して行われた作業を検討すること。
(l)　リスク及びインシデントについて、国境を越えて依存関係にあるものを含む、基幹サービス運営者の特定に関するベストプラクティスを、ENISA の支援を受けて共有すること。
(m)　第 14 条及び第 16 条に掲げるインシデント届出の様式を検討すること。

協力グループは、2018 年 2 月 9 日までに、かつ、それ以降 2 年ごとに、当該協力グループの目的及び任務の実施のために行う行為に関する作業プログラムを定めなければならず、同プログラムは、この指令の目的と整合性のとれたものでなければならない。

4.　協力グループは、第 23 条に掲げる再審査の目的のため、2018 年 8 月 9 日までに、かつ、それ以降 1 年半ごとに、この条に基づく戦略的協力から得られた経験を評価する報告書を作成しなければならない。

5.　委員会は、協力グループの機能に必要な手続上の取決めを規定する実施行為[22]を採択しなければならない。当該実施行為は、第 22 条第 2 項に掲げる審査手続に基づき採択されなければならない。

委員会は、前段の目的のため、2017 年 2 月 9 日までに、第 22 条第 1 項に掲げる実施行為の最初の草案を［ネットワーク・情報システムセキュリティ］委員会に提出しなければならない。

第 12 条　CSIRT ネットワーク

1.　加盟国間の信任及び信頼の構築に資するため、並びに迅速かつ実効性ある実施協力を促進するため、各国 CSIRT のネットワークが設置される。

2.　CSIRT ネットワークは、加盟国の CSIRT 及び CERT-EU[23]の代表者で構成されるものとする。委員会は、CSIRT ネットワークにオブザーバーとして参加しなければならない。ENISA は、事務局を提供し、CSIRT 間の協力を積極的に支援しなければならない。

---

(22) 実施行為（implementing acts）とは、法的拘束力を有する EU の行為を実施するために一律の条件が必要とされる場合に採択されるもので、実施規則（implementing regulation）、実施指令（implementing directive）、実施決定（implementing decision）が存在する。庄司克宏『新 EU 法　基礎篇』岩波書店, 2013, pp.105-108, 209-210.

(23) CERT-EU（Computer Emergency Response Team for the EU institutions, agencies and bodies）は、2012 年に設置された、EU 諸機関の情報セキュリティ担当者によるコンピュータ緊急対応チーム。“About Us.” Computer Emergency Response Team for the EU institutions, agencies and bodies (CERT-EU) website <https://cert.europa.eu/cert/plainedition/en/cert_about.html>

3. CSIRT ネットワークは、次の各号に掲げる任務を有するものとする。
(a) CSIRT のサービス、運営及び協力の能力に関する情報を交換すること。
(b) インシデントにより影響を受ける可能性がある加盟国の CSIRT の代表者からの要請に基づき、当該インシデント及び関連するリスクに関する、商業上の機密情報を除く情報を交換し及び検討すること。ただし、インシデントの調査に影響を及ぼすおそれがある場合には、全ての加盟国の CSIRT は、当該検討への協力を拒否することができる。
(c) 個別のインシデントに関する非機密情報について、任意に交換し及び公表すること。
(d) 加盟国の CSIRT の代表者からの要請に基づき、当該加盟国の管轄権内で確認されたインシデントについて検討し、可能な場合には、協調的な対応を特定すること。
(e) 自発的な相互支援に基づき、国境を越えるインシデントへの対処において、加盟国を支援すること。
(f) 次の各号に掲げる事項を含め、更なる実施協力の形態を検討し、調査し及び特定すること。
(ⅰ) リスク及びインシデントの類型
(ⅱ) 早期警戒情報
(ⅲ) 相互支援
(ⅳ) 加盟国が国境を越えるリスク及びインシデントに対応する際の、協調の原則及び様式
(g) 自身の活動及び第 f 号に基づき検討された更なる実施協力の形態を協力グループに通知し、これに関し、指導を要請すること。
(h) ENISA が組織したものを含む、ネットワーク・情報システムの安全に関する演習から得られた教訓について検討すること。
(i) 個別の CSIRT からの要請に基づき、当該 CSIRT の能力及び準備状況について検討すること。
(j) 実施協力において、この条の規定の適用に関し、一致した実施を促進するため、指針を公表すること。
4. CSIRT ネットワークは、第 23 条に掲げる再審査の目的のため、2018 年 8 月 9 日までに、かつ、それ以降 1 年半ごとに、結論及び勧告を含む、この条に基づく実施協力により得られた経験を評価する報告書を作成しなければならない。当該報告書は、協力グループにも提出されなければならない。
5. CSIRT ネットワークは、自身の手続規則を定めなければならない。

第 13 条　国際協力

欧州連合は、EU 運営条約第 218 条(24) に基づき、第三国又は国際組織との間に、協力グループの何らかの活動への参加を許可し及び組織する国際協定を締結することができる。当該協定は、十分なデータ保護の確保の必要性を考慮したものでなければならない。

第 4 章　基幹サービス運営者のネットワーク・情報システムの安全

(24) EU 運営条約第 218 条は、EU と第三国又は国際組織との間に結ばれる国際協定の交渉・締結手続を規定している。

第 14 条　セキュリティ要件及びインシデント届出

1. 加盟国は、基幹サービス運営者が、運営において使用しているネットワーク・情報システムの安全に対するリスクに対処するため、適切かつ均衡の取れた技術的及び組織的措置を講じるようにしなければならない。当該措置は、最新技術を考慮して、リスクに対して適切なネットワーク・情報システムの安全水準を確保するものでなければならない。
2. 加盟国は、基幹サービス運営者が、基幹サービスの継続性確保を目的として、当該サービスの提供に使用されているネットワーク・情報システムの安全を侵害するインシデントの影響を防止し及び最小化するため、適切な措置を講じるようにしなければならない。
3. 加盟国は、基幹サービス運営者が、提供する基幹サービスの継続性に重大な影響を及ぼすインシデントを、不当に遅滞することなく、管轄官庁又は CSIRT に届け出るようにしなければならない。届出は、管轄官庁又は CSIRT が、当該インシデントによる国境を越える影響の確定を可能とする情報を含んだものでなければならない。届出により、届け出た者の責任を加重してはならない。
4. インシデントの影響の重大性を確定するため、特に次の各号に掲げる要因が考慮されなければならない。
   (a) 基幹サービスの途絶により影響を受ける利用者の数
   (b) インシデントの継続期間
   (c) インシデントにより影響を受ける地域の地理的範囲
5. 管轄官庁又は CSIRT は、基幹サービス運営者からの届出において提供された情報に基づき、インシデントが他の加盟国における基幹サービスの継続性に重大な影響を及ぼす場合には、当該加盟国に通知しなければならない。その際、管轄官庁又は CSIRT は、欧州連合の法又は欧州連合の法を遵守した国内立法に基づき、基幹サービス運営者の安全及び商業的利益、並びに届出において提供された情報の機密性を保護しなければならない。

   管轄官庁又は CSIRT は、可能な場合、届出を行った基幹サービス運営者に対し、効果的なインシデント対応を支援する情報等、当該届出に続く措置に関する関連情報を提供しなければならない。

   単一窓口は、管轄官庁又は CSIRT からの要請に基づき、前段に掲げる届出を、影響を受ける他の加盟国の単一窓口に送付しなければならない。
6. 管轄官庁又は CSIRT は、インシデントの防止又は発生中のインシデントへの対処のため、公衆の認知が必要な場合には、届出を行った基幹サービス運営者との協議後に、個別のインシデントについて公衆に通知することができる。
7. 協力グループ内で協働する管轄官庁は、基幹サービス運営者によるインシデントの届出が義務付けられる状況に関する指針を作成し及び採択することができ、これには、第 4 項に掲げるインシデントの影響の重大性を確定する要因に関するものも含まれる。

第 15 条　実施及び執行

1. 加盟国は、管轄官庁が、第 14 条に基づく基幹サービス運営者の義務の遵守［状況］及びそれによるネットワーク・情報システムの安全に対する効果を評価するために必要な権限及び手段を有するようにしなければならない。
2. 加盟国は、管轄官庁が、次の各号に掲げる事項を基幹サービス運営者に対し要請するために必要な権限及び手段を有するようにしなければならない。

(a) セキュリティポリシー文書を含む、ネットワーク・情報システムの安全を評価するために必要な情報の提供

(b) 管轄官庁又は資格のある監査人によるセキュリティ監査の結果等の、セキュリティポリシーの効果的な実施に関する証拠の提供及び、監査人によるセキュリティ監査の場合には、基礎となる証拠を含む結果の管轄官庁への提供

管轄官庁は、当該情報又は証拠を要請する場合、要請の目的を述べ、かつ、要請対象の情報を特定しなければならない。

3. 管轄官庁は、第 2 項に掲げる情報又はセキュリティ監査の結果を評価した後、特定された欠陥を除去するため、当該基幹サービス運営者に対し、拘束力のある指示を与えることができる。

4. 管轄官庁は、個人データを侵害するインシデントへの対処に際し、データ保護官庁と緊密に協力しなければならない。

第 5 章　デジタルサービス提供者のネットワーク・情報システムの安全

第 16 条　セキュリティ要件及びインシデント届出

1. 加盟国は、デジタルサービス提供者が、欧州連合内における附属書 3 に掲げるサービスのために使用しているネットワーク・情報システムについて、その安全に対するリスクに対処するため、適切かつ均衡の取れた技術的及び組織的措置を特定し及び講じるようにしなければならない。当該措置は、最新技術を考慮して、リスクに対して適切なネットワーク・情報システムの安全水準を確保するものでなければならず、次の各号に掲げる要素を考慮したものでなければならない。

(a) システム及び設備の安全

(b) インシデント対応

(c) 事業継続マネジメント

(d) 監視、監査及び検査

(e) 国際標準の遵守

2. 加盟国は、デジタルサービスの継続性確保を目的として、欧州連合内で提供される附属書 3 に掲げるサービスに対する、ネットワーク・情報システムの安全を侵害するインシデントの影響を防止し及び最小化するため、デジタルサービス提供者が措置を講じるようにしなければならない。

3. 加盟国は、デジタルサービス提供者が、欧州連合内で提供する附属書 3 に掲げるサービスの提供に重要な影響を与える全てのインシデントを、不当に遅滞することなく、管轄官庁又は CSIRT に届け出るようにしなければならない。届出は、管轄官庁又は CSIRT が、国境を越える影響の重大性を確定できる情報を含んだものでなければならない。届出により、届け出た者の責任を加重してはならない。

4. インシデントの影響の重要性を確定するため、次の各号に掲げる要因が考慮されなければならない。

(a) インシデントにより影響を受ける利用者、特に、自身のサービス提供のために当該デジタルサービスを利用する利用者の数

(b)　インシデントの継続期間
(c)　インシデントにより影響を受ける地域の地理的範囲
(d)　サービス運営の途絶範囲
(e)　社会経済活動に対する影響の範囲

インシデント届出の義務は、デジタルサービス提供者が、前段に掲げる要因に照らしてインシデントの影響を評価するために必要な情報にアクセス可能な場合にのみ適用される。

5.　基幹サービス運営者が、重要な社会経済活動の維持に不可欠なサービスの提供のために、第三者のデジタルサービス提供者に依存している場合、当該運営者は、デジタルサービス提供者に影響を及ぼすインシデントによる、基幹サービスの継続性に対する全ての重大な影響を届け出なければならない。

6.　管轄官庁又は CSIRT は、必要に応じ、特に、第 3 項に掲げるインシデントが 2 以上の加盟国に関係する場合、影響を受ける他の加盟国に通知しなければならない。その際、管轄官庁、CSIRT 及び単一窓口は、欧州連合の法又は欧州連合の法を遵守した国内立法に基づき、デジタルサービス提供者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保護しなければならない。

7.　管轄官庁又は CSIRT 及び、必要に応じ、関係する他の加盟国の官庁又は CSIRT は、インシデントの防止若しくは発生中のインシデントへの対処のために公衆の認知が必要な場合又はインシデントの公開が公共の利益となる場合、関係するデジタルサービス提供者との協議後に、個別のインシデントについて公衆に通知し又はデジタルサービス提供者に通知を要請することができる。

8.　委員会は、この条の第 1 項に掲げる要素及び第 4 項に掲げる要因の詳細を定めるため、実施行為[25]を採択しなければならない。当該実施行為は、第 22 条第 2 項に掲げる審査手続に基づき、2017 年 8 月 9 日までに採択されなければならない。

9.　委員会は、届出義務に適用可能な様式及び手続を定める実施行為を採択することができる。当該実施行為は、第 22 条第 2 項に掲げる審査手続に基づき採択されなければならない。

10.　第 1 条第 6 項に影響を及ぼすことなく、加盟国は、デジタルサービス提供者に対し、更なるセキュリティ要件又は届出要件を課してはならない。

11.　第 5 章は、委員会勧告 2003/361/EC[26]が規定する小規模企業及び零細企業に適用してはならない。

第 17 条　実施及び執行

1.　加盟国は、第 16 条が規定する要件をデジタルサービス提供者が満たさないという証拠が提供されたときは、管轄官庁が、必要な場合には事後監督措置を通じて、措置を講じるようにしなければならない。当該デジタルサービスが提供されている他の加盟国の管轄官庁は、同様の証拠を提出することができる。

2.　管轄官庁は、第 1 項の目的のため、次の各号に掲げる事項をデジタルサービス提供者に対

(25) 前掲注(22)参照。
(26) Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, *Official Journal of the European Union*, L124, 2003.5.20. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361> この委員会勧告では、小規模企業は、従業員数 50 人未満で、年間売上高又は年次貸借対照表の合計が 1000 万ユーロ以下の企業を指し、零細企業は、従業員数 10 人未満で、年間売上高又は年次貸借対照表の合計が 200 万ユーロ以下の企業を指す。

し要請するために必要な権限及び手段を有していなければならない。

(a)　セキュリティポリシー文書を含む、ネットワーク・情報システムの安全を評価するために必要な情報を提供すること。

(b)　第 16 条が規定する要件を満たすため、全ての障害を除去すること。

3.　デジタルサービス提供者がその主たる事業所又は代表者をある加盟国に有し、そのネットワーク・情報システムが 1 又は 2 以上の他の加盟国に置かれている場合、主たる事業所又は代表者がある加盟国の管轄官庁及び他の加盟国の管轄官庁は、必要に応じ、相互に協力し及び支援しなければならない。当該支援及び協力には、関係する管轄官庁間の情報交換、及び第 2 項に掲げる監督措置の要請を含めることができる。

第 18 条　管轄権及び属地主義

1.　この指令の目的のため、デジタルサービス提供者は、主たる事業所を有している加盟国の管轄権の下にあるとみなされるものとする。デジタルサービス提供者は、ある加盟国にその本社を有している場合、当該加盟国に主たる事業所を有しているとみなされるものとする。

2.　欧州連合の域外で設立され、附属書 3 に掲げるサービスを欧州連合内で提供するデジタルサービス提供者は、欧州連合内に代表者を指定しなければならない。当該代表者は、サービスが提供される加盟国のうちの 1 つに置かなければならない。デジタルサービス提供者は、当該代表者が置かれる加盟国の管轄権の下にあるとみなされるものとする。

3.　デジタルサービス提供者による代表者の指定は、当該デジタルサービス提供者自身に対する訴訟の提起に影響を与えないものとする。

第 6 章　標準化及び任意の届出

第 19 条　標準化

1.　加盟国は、第 14 条第 1 項及び第 2 項並びに第 16 条第 1 項及び第 2 項の集中的実施を促進するため、特定の技術的方式の使用に利益となるよう強要又は優遇することなく、ネットワーク・情報システムの安全に関し、欧州で又は国際的に認められた標準及び仕様の使用を奨励しなければならない。

2.　ENISA は、加盟国と共同で、第 1 項に関連して考慮されるべき技術分野に関する及び当該分野に適用が見込まれる、加盟国国内の標準を含む既存の標準に関する助言及び指針を作成しなければならない。

第 20 条　任意の届出

1.　基幹サービス運営者と特定されず、デジタルサービス提供者でもない団体は、第 3 条に影響を及ぼすことなく、その提供するサービスの継続性に重大な影響を及ぼすインシデントを、任意に届け出ることができる。

2.　加盟国は、届出の処理に際し、第 14 条が規定する手続に基づいて行わなければならない。加盟国は、任意の届出よりも、義務的届出の処理を優先することができる。任意の届出は、関係する加盟国に対して均衡を欠く又は不当な負担を与えるものでない場合にのみ、処理されるものとする。

　任意の届出により、届出を行った団体に対し、当該届出がなかった場合には課されなかったであろういかなる義務も課してはならない。

第 7 章　最終規定

第 21 条　罰則

加盟国は、この指令に基づき採択された国内規定への違反に対して適用できる罰則規定を定めなければならず、当該罰則規定の実施を確保するために必要な全ての措置を講じなければならない。規定される罰則は、実効的で、均衡の取れた、かつ、抑止的なものでなければならない。加盟国は、2018 年 5 月 9 日までに、当該罰則規定及び措置を委員会に通知しなければならず、それらに影響を及ぼす全ての事後修正を、委員会に遅滞なく通知しなければならない。

第 22 条　［ネットワーク・情報システムセキュリティ］委員会手続

1. 委員会は、ネットワーク・情報システムセキュリティ委員会の支援を受けなければならない。当該［ネットワーク・情報システムセキュリティ］委員会は、規則（EU）No 182/2011 [(27)] が意味するところの［加盟国の代表から成る］委員会とする。
2. この項に対し付託がなされた場合、規則（EU）No 182/2011 の第 5 条が適用されるものとする。

第 23 条　再審査

1. 委員会は、2019 年 5 月 9 日までに、加盟国が基幹サービス運営者の特定においてとった方法の整合性を評価した報告書を、欧州議会及び理事会に提出しなければならない。
2. 委員会は、この指令の機能を定期的に再審査し、欧州議会及び理事会に報告しなければならない。委員会は、この目的のため、並びに戦略的及び実施上の協力を一層進展させる目的のため、戦略及び実施の段階において得られた経験に関する、協力グループ及び CSIRT ネットワークからの報告を考慮しなければならない。委員会は、再審査において、附属書 2 及び 3 に含まれるリスト、並びに基幹サービス運営者の特定及び附属書 2 に掲げる分野のサービスの整合性についても、評価しなければならない。最初の報告書は、2021 年 5 月 9 日までに提出されなければならない。

第 24 条　経過措置

1. 協力グループ及び CSIRT ネットワークは、第 25 条に影響を及ぼすことなく、［国内法への］置換の期間において、追加的に適切な協力を可能とすることを目的として、2017 年 2 月 9 日までに、第 11 条第 3 項及び第 12 条第 3 項がそれぞれ規定する任務の実施を開始しなければならない。
2. 協力グループは、2017 年 2 月 9 日から 2018 年 11 月 9 日までの間、加盟国が基幹サービス運営者の特定の過程で整合性のとれた取組を行うよう支援する目的のため、第 5 条及び第 6 条が規定する基準に基づく特定部門における基幹サービス運営者の特定を可能とする国内措置の手順、内容及び類型を検討しなければならない。協力グループは、加盟国の要請に基づき、第 5 条及び第 6 条が規定する基準に基づく特定部門における、基幹サービス運営者の特

(27) "Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers," *Official Journal of the European Union*, L55, 2011.2.28. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011R0182> この規則は「コミトロジー規則」と呼ばれ、欧州委員会が法令実施のために「実施行為」を定める際に、その草案を加盟国の代表から成る委員会（committee）に提出し、諮問手続（advisory procedure）又は審査手続（examination procedure）に付すことを規定している。同規則の第 5 条は、審査手続について定めている。

定を可能とする当該加盟国の国内措置の草案についても検討しなければならない。

3. 加盟国は、この条の目的のため、2017 年 2 月 9 日までに、協力グループ及び CSIRT ネットワークに適切な代表者を確保しなければならない。

第 25 条 ［国内法への］置換

1. 加盟国は、この指令を遵守するために必要な法律、規則及び行政規定を、2018 年 5 月 9 日までに採択し及び公表しなければならない。加盟国は、それらを委員会に直ちに通知しなければならない。

加盟国は、当該措置を、2018 年 5 月 10 日から適用しなければならない。

加盟国が当該措置を採択する際、この指令への言及を含めなければならず又は公布時にこの指令への言及を添付しなければならない。言及の方法は、加盟国がこれを定めなければならない。

2. 加盟国は、この指令が該当する範囲において採択する国内法の主要な規定の本文を委員会に通知しなければならない。

第 26 条 施行

この指令は、『欧州連合官報［*Official Journal of the European Union*］』における公布日から 20 日後に施行するものとする。

第 27 条 名宛人

この指令は、加盟国を名宛人とする。

2016 年 7 月 6 日、ストラスブールにて採択。

欧州議会議長 M. SCHULZ
理事会議長 I. KORČOK

附属書１　コンピュータセキュリティインシデント対応チーム（CSIRT）の要件及び任務

CSIRTの要件及び任務は、国内の政策、規則又はその両方により、十分かつ明確に定義されなければならない。CSIRTの要件及び任務には、次に掲げる事項を含めなければならない。

(1)　CSIRTの要件

(a)　CSIRTは、単一障害点[28]を回避することによって、通信サービスの高水準な利用可能性を確保し、かつ、常時連絡を受け付け及び他者に連絡するための複数の手段を有していなければならない。さらに、当該通信手段は、明確に指定され、サービス対象［原語はconstituency］及び協力パートナーに周知されなければならない。

(b)　CSIRTの施設及び支援情報システムは、安全な場所に置かなければならない。

(c)　業務継続性

(ⅰ)　CSIRTは、円滑な処理の引継ぎのため、要求の管理及び経路制御に適したシステムを備えたものでなければならない。

(ⅱ)　CSIRTには、常時利用可能性を確保するため、十分な人員が配置されなければならない。

(ⅲ)　CSIRTは、継続性が確保されたインフラを利用しなければならない。この目的のため、冗長[29]システム及びバックアップ作業領域が利用可能とされなければならない。

(d)　CSIRTは、希望する場合、国際的な協力ネットワークへの参加可能性を有していなければならない。

(2)　CSIRTの任務

(a)　CSIRTの任務には、少なくとも次に掲げる事項を含めなければならない。

(ⅰ)　国家レベルにおけるインシデントの監視

(ⅱ)　リスク及びインシデントに関する、利害関係者への早期警戒情報、警告、情報の公表及び普及

(ⅲ)　インシデントへの対応

(ⅳ)　リスク及びインシデントの動態分析並びに状況認識の提供

(ⅴ)　CSIRTネットワークへの参加

(b)　CSIRTは、民間部門と協力的関係を確立しなければならない。

(c)　CSIRTは、協力促進のため、次に掲げる事項に関する共通の又は標準化された方法の採用及び利用を促進しなければならない。

(ⅰ)　インシデント及びリスク対応手続

(ⅱ)　インシデント、リスク及び情報の分類体系

(28)　単一障害点（single point of failure: SPOF）とは、コンピュータやネットワークシステムにおいて、その部分が故障するとシステム全体が動作しなくなる要素を指す（『デジタル大辞泉』JapanKnowledge）。

(29)　コンピュータシステムにおける機器やネットワークの障害に備え、システムの予備を追加して多重化を図ることを、冗長化（redundancy）という。同上

附属書２　第４条第４号［基幹サービス運営者］の目的における団体の類型

部門	下位部門	団体の種類
1　エネルギー	(a)　電力	欧州議会及び理事会の指令 2009/72/EC[30] の第 2 条第 35 項が規定する電力事業者であり、当該指令の第 2 条第 19 項が規定する「供給」の機能を遂行するもの
		指令 2009/72/EC の第 2 条第 6 項が規定する流通システム運営者
		指令 2009/72/EC の第 2 条第 4 項が規定する輸送システム運営者
	(b)　石油	石油輸送パイプラインの運営者
		石油の生産、精製及び処理設備、並びに保管及び輸送の運営者
	(c)　ガス	欧州議会及び理事会の指令 2009/73/EC[31] の第 2 条第 8 号が規定する供給事業者
		指令 2009/73/EC の第 2 条第 6 号が規定する流通システム運営者
		指令 2009/73/EC の第 2 条第 4 号が規定する輸送システム運営者
		指令 2009/73/EC の第 2 条第 10 号が規定する保管システム運営者
		指令 2009/73/EC の第 2 条第 12 号が規定する LNG システム運営者
		指令 2009/73/EC の第 2 条第 1 号が規定する天然ガス事業者
		天然ガスの精製及び処理設備の運営者
2　輸送	(a)　航空輸送	欧州議会及び理事会の規則（EC）No 300/2008[32] の第 3 条第 4 項が規定する航空会社
		欧州議会及び理事会の指令 2009/12/EC[33] の第 2 条第 2 項が規定する空港管理組織、欧州議会及び理事会の規則（EU）No 1315/2013[34] の附属書 2 の項目 2［中核的及び総合的ネットワークにおける空港、海港、内陸港、鉄道ターミナル］に掲げる中核的空港を含む、当該指令［2009/12/EC］の第 2 条第 1 項が規定する空港、並びに空港内に含まれる附属設備運営者
		欧州議会及び理事会の規則（EC）No 549/2004[35] の第 2 条第 1 項が規定する航空交通管制（ATC）サービスを提供する航空管理管制運営者
	(b)　鉄道輸送	欧州議会及び理事会の指令 2012/34/EU[36] の第 3 条第 2 号が規定する［鉄道］インフラ管理者
		指令 2012/34/EU の第 3 条第 12 号が規定するサービス設備運営者を含む、指令 2012/34/EU の第 3 条第 1 号が規定する鉄道事業者
	(c)　水上輸送	欧州議会及び理事会の規則（EC）No 725/2004[37] の附属書 1 の海上輸送が規定する、内水、海洋及び沿岸の水上貨客輸送会社（当該会社が操業する個別の船舶を除く）

(30) Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC, OJ L211, 2009.8.14. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0072>

(31) Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC, OJ L211, 2009.8.14. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0073>

(32) Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002, OJ L97, 2008.4.9. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02008R0300-20100201>

(33) Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges, OJ L70, 2009.3.14. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0012>

(34) Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU, OJ L348, 2013.12.20. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02013R1315-20170608>

(35) Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation), OJ L96, 2004.3.31. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02004R0549-20091204>

(36) Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area, OJ L343, 2012.12.14. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02012L0034-20171204>

(37) Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security, OJ L129, 2004.4.29. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02004R0725-20090420>

		規則（EC）No 725/2004 の第 2 条第 11 項が規定する港湾設備を含む、欧州議会及び理事会の指令 2005/65/EC[38] の第 3 条第 1 項が規定する港の管理組織、並びに港において作業及び設備を稼働する団体
		欧州議会及び理事会の指令 2002/59/EC[39] の第 3 条第 o 号が規定する船舶通航サービスの運営者
	(d)　道路輸送	交通管理に責任を有する、委員会委任規則（EU）2015/962[40] の第 2 条第 12 号が規定する道路管理官庁
		欧州議会及び理事会の指令 2010/40/EU[41] の第 4 条第 1 号が規定する高度道路交通システムの運営者
3　銀行		欧州議会及び理事会の規則（EU）No 575/2013[42] の第 4 条第 1 項第 1 号が規定する金融機関
4　金融市場インフラ		欧州議会及び理事会の指令 2014/65/EU[43] の第 4 条第 1 項第 24 号が規定する取引所の運営者
		欧州議会及び理事会の規則（EU）No 648/2012[44] の第 2 条第 1 号が規定する中央清算機関（CCPs）
5　保健部門	保健医療機関（病院及び民間診療所を含む）	欧州議会及び理事会の指令 2011/24/EU[45] の第 3 条第 g 号が規定する保健医療サービス提供者
6　飲料水の供給及び分配		理事会指令 98/83/EC[46] の第 2 条第 1 項第 a 号が規定する人間向けの飲料水の供給者及び分配者（人間向けの飲料水の分配が、基幹サービスとはみなされない他の商品及び財を流通させる一般的活動の一部に限られる場合の分配者を除く）
7　デジタルインフラ		IXP［インターネット相互接続点］[47]
		DNS［ドメインネームシステム］サービス提供者[48]
		TLD［トップレベルドメイン］名レジストリ[49]

(38) Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security, OJ L310, 2005.11.25. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02005L0065-20090420>

(39) Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC, OJ L208, 2002.8.5. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002L0059-20141118>

(40) Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services, OJ L157, 2015.6.23. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R0962>

(41) Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, OJ L207, 2010.8.6. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02010L0040-20180109>

(42) Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012, OJ L 176, 2013.6.27. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02013R0575-20180101>

(43) Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, OJ L173, 2014.6.12. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02014L0065-20160701>

(44) Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories, OJ L201, 2012.7.27. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02012R0648-20170630>

(45) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, OJ L88, 2011.4.4. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02011L0024-20140101>

(46) Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption, OJ L330, 1998.12.5. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:01998L0083-20151027>

(47) 第 4 条第 13 号を参照。

(48) 第 4 条第 14 号及び第 15 号を参照。

(49) 第 4 条第 16 号を参照。

附属書３　第４条第５号［デジタルサービス］の目的におけるデジタルサービスの類型

1　オンラインマーケット
2　オンライン検索エンジン
3　クラウドコンピューティングサービス

（しまむら　ともこ）