【EU】高度な共通水準のサイバーセキュリティ指令（NIS2 指令）の制定

海外立法情報課　田村　祐子

＊2022 年 12 月、ネットワーク及び情報指令（NIS 指令）を廃止し、その内容を引き継ぐとともに対象を拡げ、インシデント報告記載事項等の明確化、協力体制強化等を定める指令が制定された。

1　背景・経緯

これまで EU では、2016 年制定の「ネットワーク及び情報指令」（以下「NIS 指令」）[1]に従い、サイバーセキュリティ対策を行ってきた。サイバー攻撃によるインシデントが増加・複雑化する中で、NIS 指令の対象が限定的であること[2]、NIS 指令制定後も EU で事業を行う企業のサイバーレジリエンス（サイバー攻撃への耐性）のレベルが低いこと、EU 加盟国間での共同の危機対応が不足している状況にあること[3]等の問題点が指摘されるようになり、それらを改善するために、2020 年 12 月 16 日、NIS 指令を廃止し、内容を引き継ぐとともに新たな規定を盛り込んだ指令案（COM(2020) 823 final）が提出された。同指令案は、2022 年 5 月 13 日に欧州議会、EU 理事会及び欧州委員会の間で非公式の合意に至り、同年 12 月 14 日、「高度な共通水準のサイバーセキュリティ指令」（以下「NIS2 指令」）[4]として制定された。施行日は、2023 年 1 月 16 日である。加盟国は、2024 年 10 月 17 日までに NIS2 指令を国内法化することが求められる（第 41 条）。

2　NIS2 指令の概要

全 9 章 46 か条及び別表 3 部から成り、第 1 章：一般規定（第 1 条～第 6 条）、第 2 章：協調的なサイバーセキュリティ枠組み（第 7 条～第 13 条）、第 3 章：EU・国際レベルの協力（第 14 条～第 19 条）、第 4 章：サイバーセキュリティリスク管理措置及び報告義務（第 20 条～第 25 条）、第 5 章：管轄権及び登録（第 26 条～第 28 条）、第 6 章：情報共有（第 29 条、第 30 条）、第 7 章：監督及び執行（第 31 条～第 37 条）、第 8 章：委任法及び実施法（第 38 条、第 39 条）、第 9 章：末尾規定（第 40 条～第 46 条）で構成される。

（1）対象拡大

NIS 指令の対象であった 7 分野[5]の団体（entity）に加えて、エネルギー（水素）、デジタルインフラ（公共電子通信ネットワーク等）、行政機関、宇宙、郵便・宅配、製造業（医療機器、自動車等）、研究、デジタルプロバイダ（オンラインマーケットプレイス、オンライン検索エ

＊　本稿におけるインターネット情報の最終アクセス日は、2023 年 9 月 7 日である。

1 Directive (EU) 2016/1148 [2016] OJ L 194/1. <http://data.europa.eu/eli/dir/2016/1148/oj>; 翻訳及び解説は、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』No.277, 2018.9, pp.1-32. <https://doi.org/10.11501/11152345> を参照。

2 2(1)にて後述のとおり、NIS 指令の対象は 7 分野（後掲注(5)）のみであったため、対象範囲拡大の必要性が指摘されていた。European Parliament, "The NIS2 Directive A high common level of cybersecurity in the EU," 2023.2.8, p.3. <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf>

3 European Commission. "Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148," COM(2020) 823 final, 16.12.2020, p.1. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A0823%3AFIN>

4 Directive (EU) 2022/2555 [2022] OJ L 333/80. <http://data.europa.eu/eli/dir/2022/2555/oj>

5 ①エネルギー（電力・石油・ガス）、②輸送、③銀行、④金融市場インフラ、⑤保健部門、⑥飲料水の供給及び分配、⑦デジタルインフラ（インターネット相互接続点（IXP）、ドメインネームシステム（DNS）サービス提供者、トップレベルドメイン（TLD）名レジストリ）。各分野の説明も含め、島村　前掲注(1), pp.30-31.参照。

ンジン、SNS プラットフォーム）等が追加され、NIS2 指令の対象は計 18 分野に拡大された（第 2 条、別表 1、別表 2）。

（2）サイバーセキュリティリスク管理及び報告義務

サイバーレジリエンスを強化するため、NIS2 指令では、団体が採るべきリスク管理措置の明確化、インシデント報告に記載すべき事項・報告期限の明確化及び罰則強化が行われた。新たに定められた規定は次のとおりである。加盟国は、団体が、その運営又はサービス提供に使用するネットワーク及び情報システムのセキュリティに生じるリスクを管理するために適切な措置（サプライチェーンのセキュリティ確保、脆弱（ぜいじゃく）性情報の開示、暗号化等 10 項目）を講ずることを保証する義務を負う（第 21 条）。加盟国は、団体が、重大なインシデント[6]について、自国のコンピュータセキュリティインシデント対応チーム（CSIRT）[7]又は適当な場合には管轄当局に過度の（undue）遅滞なく通知すること（第 23 条第 1 項）、そのために重大なインシデントを認識してから①24 時間以内に早期警告[8]を、②72 時間以内にインシデント通知[9]を、③インシデント通知後 1 か月以内に最終報告書[10]を提出すること（同条第 4 項）を保証する義務を負う。加盟国は、第 21 条又は第 23 条に違反した団体に対して、最大で、1000 万ユーロ[11]又は売上高 2%のいずれか高い方を過料として科す（第 34 条）。

（3）協力体制の強化

NIS 指令でも協力体制に関する規定があったが[12]、共同の危機対応が不足しているとの指摘を踏まえ、NIS2 指令では、新たに次のとおり規定している。加盟国は、大規模なサイバーセキュリティインシデント危機の管理を担当する、サイバー危機管理当局を指定・設立する（第 9 条）。欧州ネットワーク・情報セキュリティ機関（ENISA）[13]は、脆弱性情報、影響を受ける ICT 製品・サービス等を内容とする、欧州脆弱性データベースを開発・維持する（第 12 条）。大規模なサイバーセキュリティインシデント及び危機について、運用レベルでの協調的な管理を支援し、加盟国と EU 諸機関間での定期的な情報交換を目的とする、欧州サイバー危機連絡調整ネットワーク（EU-CyCLONe）を設立する（第 16 条）。

---

6 あるインシデントが、①団体にサービス運営の深刻な中断又は経済的損失を引き起こした又は引き起こす可能性がある場合、②重大な物質的又は非物質的な損害を引き起こすことにより、他の自然人又は法人に影響を与えた又は影響を与える可能性がある場合、重大なインシデントとみなされる（第 23 条第 3 項）。

7 インシデント対応に責任を負う団体で、加盟国が指定・設置する。管轄当局内に設置することも可能である。国内におけるサイバー脅威、脆弱性、インシデントの監視及び分析等を任務とする（第 10 条、第 11 条）。

8 早期警告は、重大なインシデントが違法行為（unlawful act）若しくは悪意のある行為（malicious act）によって引き起こされた疑いがあるかどうか又は国境を越える可能性があるかどうかを示すものである（第 23 条第 4 項）。

9 インシデント通知は、早期警告の情報を更新するもので、重大度、影響及び入手可能な場合は情報漏洩（ろうえい）の兆候（indicators of compromise）を含めて、重大なインシデントの初期評価を示す（第 23 条第 4 項）。

10 最終報告書は、①重大度と影響を含むインシデントの詳細な説明、②インシデントを引き起こしたと考えられる脅威又は根本原因の種類、③適用され、継続中の緩和措置、④該当する場合、国境を越えたインシデントの影響を含むものとする（第 23 条第 4 項）。

11 1 ユーロは、約 157 円（令和 5 年 9 月分報告省令レート）である。

12 NIS 指令は、CSIRT ネットワークと協力グループについて定めており、これらの規定は NIS2 指令に引き継がれた。CSIRT ネットワークは、各加盟国の CSIRT と EU 諸機関のコンピュータ緊急対応チーム（CERT-EU）の代表者から成り、情報共有等を任務とする（第 15 条）。協力グループは、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（後掲注(13)）の代表者から成り、CSIRT ネットワークの活動に対する戦略的指導等を任務とする（第 14 条）。

13 2004 年に設立された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。島村　前掲注(1), p.5.