【EU】サイバー連帯法の制定

海外立法情報課長　芦田　淳

＊2024 年 12 月、欧州サイバーセキュリティ警報システム、サイバーセキュリティ緊急メカニズム及び欧州サイバーセキュリティインシデント審査メカニズムを設ける規則が制定された。

1　概要

2024 年 12 月、「サイバー脅威及びインシデントに対する検知、準備及び対応のための［欧州］連合における連帯及び能力の強化措置を設け、規則（EU）2021/694[1]の改正を行う 2024 年 12 月 19 日の欧州議会及び理事会規則（EU）2025/38（サイバー連帯法）」[2]が制定された。サイバー連帯法は、欧州連合（EU）におけるサイバー脅威及びインシデントの検知、準備及び対応に関する能力を強化するための措置を定めることを目的とする（第 1 条[3]）。同法は、全 5 章 26 か条及び附属書から成り、2025 年 2 月 4 日から施行された（第 26 条）。

2　主な規定

（1）欧州サイバーセキュリティ警報システム（第 2 章：第 3 条～第 9 条）

サイバー脅威に関する検知、分析及びデータ処理に係る能力強化を目的とした EU の高度な能力の開発並びに EU 内でのインシデントの予防を支援するため、自主的に参加する加盟各国のサイバーハブ及び国境を越えたサイバーハブから構成される「欧州サイバーセキュリティ警報システム」を設ける（第 3 条）。加盟各国のサイバーハブは、当該国の権限の下で活動する単一の組織であり、各加盟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）[4]又はサイバー危機管理当局等をもって充てることができる（第 4 条）。また、国境を越えたサイバーハブとは、3 か国以上のサイバーハブを協定により統合したものを指す（第 5 条）。

（2）サイバーセキュリティ緊急メカニズム（第 3 章：第 10 条～第 20 条）

サイバー脅威に対する EU の回復力（resilience）向上に加え、(a) 重大なサイバーセキュリティインシデント、(b) 大規模なサイバーセキュリティインシデント及び(c) 大規模に相当するサイバーセキュリティインシデントの短期的な影響に対する準備及びその緩和を支援するために、「サイバーセキュリティ緊急メカニズム」を設ける（第 10 条）。(a)は、①関係する法主体に関し、そのサービスの業務運営上の深刻な混乱又は金銭的な損失を生じさせたインシデント又は生じさせ得るインシデント及び②有形又は無形の甚大な損害を生じさせることによって、他の自然人

＊　本稿におけるインターネット情報の最終アクセス日は、2025 年 6 月 11 日、［ ］は筆者による補記である。

1 デジタルヨーロッパプログラムを制定し、決定（EU）2015/2240 を廃止する 2021 年 4 月 29 日の欧州議会及び理事会規則（EU）2021/694（EEA 関連文書）（Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (Text with EEA relevance), OJ L 166, 11.5.2021, pp.1-34. <https://eur-lex.europa.eu/eli/reg/2021/694/oj>）

2 Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act), OJ L, 2025/38, 15.1.2025. <https://eur-lex.europa.eu/eli/reg/2025/38/oj>

3 同条を含む第 1 章は、サイバー連帯法の主題及び目的並びに用語の定義を定める一般規定である。

4 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。加盟国内におけるサイバー脅威、脆（ぜい）弱性、インシデントの監視及び分析等を任務とする。田村祐子「【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」『外国の立法』No.297-1，2023.10，p.13. <https://doi.org/10.11501/13013008>

又は法人に対して影響を与えたインシデント又は影響を与え得るインシデントを指す（第 2 条）[5]。(b)は、当該インシデントに対応するための加盟国の能力を超過するレベルの混乱を生じさせるインシデント又は 2 以上の加盟国に対して重大な影響を持つインシデントを指す（同条）[6]。(c)は、EU の機関等の場合には重大なインシデントを意味し、デジタルヨーロッパプログラム[7]関連第三国（同プログラムへの参加を認める EU との協定の当事国である第三国）の場合には、当該国の対応能力を超過するレベルの混乱を生じさせるインシデントを指す（同条）。

サイバーセキュリティ緊急メカニズムは、(a) EU 全域で高度に重要な部門（エネルギー、輸送、銀行、医療等）において活動する法主体の準備状況に係る共通化されたテスト（例えば、システムに対する侵入テスト）（第 12 条）等の準備行動、(b) EU サイバーセキュリティリザーブ[8]に参加する信頼できるマネージドセキュリティサービスプロバイダ[9]が提供する、重大なサイバーセキュリティインシデント等への対応を支援する行動（第 14 条）、(c) 重大なサイバーセキュリティインシデント等の影響を受けた加盟国に対する他の加盟国からの技術的支援（第 18 条）に対する支援を行う（第 11 条）。

（3）欧州サイバーセキュリティインシデント審査メカニズム（第 4 章：第 21 条）

欧州ネットワーク・情報セキュリティ機関（ENISA）[10]に対して、欧州委員会等の要請に基づき、CSIRT ネットワーク[11]の支援を受け、関係加盟国の承認を得て、特定の重大なサイバーセキュリティインシデント又は大規模なサイバーセキュリティインシデントに関するサイバー脅威、既知の悪用可能な脆（ぜい）弱性及び緩和措置について審査及び評価を行うことを義務付ける。インシデントに関する審査及び評価の完了後、将来のインシデントを回避し、又は緩和するための教訓を得ることを目的として、ENISA は、欧州委員会等に対し、インシデント審査報告書を提出するものとする。

（4）末尾規定（第 5 章：第 22 条～第 26 条）

デジタルヨーロッパプログラムに関する規則（EU）2021/694 に対して、サイバー連帯法制定に伴う改正を加える（第 22 条）ほか、欧州委員会に対して 2027 年 2 月 5 日までに、その後は少なくとも 4 年ごとに、サイバー連帯法に定められた措置の機能を評価し、欧州議会及び理事会に報告書を提出する義務を課す規定（第 25 条）などが置かれている。

---

5 この定義は、指令（EU）2022/2555 第 23 条第 3 項による定義を参照するものとなっており、当該指令の翻訳については、夏井高人「指令（EU）2022/2555（NIS2 指令）[参考訳]」『法と情報雑誌』8(4), 2023, p.153. <http://cyberlaw.la.coocan.jp/Documents/LawandInformationMag_No54.pdf> を参照した。

6 この定義も、指令（EU）2022/2555 第 6 条第 7 号を参照するものとなっており、夏井　同上, p.110 を参照した。

7 DX を加速するため、デジタル革新のための必要なインフラ構築、競争力強化、技術主権確保を目的として、企業、市民及び行政へのデジタル技術の提供に焦点を当てるものとされる。大磯輝将「AI 人材をめぐる状況と政策課題―EU の取組を参考に―」『調査と情報』No.1310, 2025.3, p.9. <https://doi.org/10.11501/14058052>

8 EU サイバーセキュリティリザーブは、サイバー連帯法第 14 条によって設けられ、CSIRT 等の要請に基づき、重大なサイバーセキュリティインシデント等への対応及びその支援を行うことを目的としている。

9 サイバーセキュリティのリスク管理と関連する活動のための補助を遂行し、又は提供するマネージドサービスプロバイダを指す。また、マネージドサービスプロバイダとは、顧客の施設において実施され、又はリモートで実施される補助又は能動的な管理運営を介して、ICT 製品、ネットワーク、インフラ、アプリケーション又はそれ以外のネットワーク及び情報システムの設置、管理、運営又は維持と関連するサービスを提供する法主体を指す。夏井前掲注(5), p.113.

10 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である。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, p.5. <https://doi.org/10.11501/11152345>

11 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。田村　前掲注(4)