【アメリカ】サイバーセキュリティに関する連邦法の制定

専門調査員　海外立法情報調査室主任　ローラー　ミカ

＊2022 年 3 月 15 日に重要インフラのサイバーインシデントについて連邦政府 CISA への報告を義務付ける法律が、6 月にもサイバーセキュリティ関連の 3 つの法律が制定された。

1　重要インフラのサイバーインシデント報告法

2022 年 3 月 15 日、重要インフラでのサイバーインシデントの報告を義務付ける法律が制定された[1]。同法第 103 条により 2002 年国土安全保障法[2]第 22 編に第 2240 条から第 2246 条が追加され、重要インフラ事業者に対し、一定のサイバーインシデント及び身代金を要求するランサムウェア攻撃への支払について、国土安全保障省傘下のサイバーセキュリティ・インフラセキュリティ庁（CISA）への報告が義務付けられることになった。

（1）報告義務と期限（第 2242 条(a) (1) (2)）

報告義務を課される対象事業体（covered entity）は、対象サイバーインシデント（covered cyber incident）が発生したと同事業体が合理的に考えた時点から 72 時間以内にそのインシデントを CISA に報告しなくてはならない。ランサムウェア攻撃の結果身代金を支払った対象事業体は、支払後 24 時間以内にその支払を CISA に報告しなくてはならない。

（2）対象事業体と対象サイバーインシデント（第 2240 条(4) (5)）

2013 年の大統領政策指令第 21 号に規定された重要インフラ部門の事業体であり[3]、本法律に基づき制定される最終規則（後述）において CISA 長官が定める定義を満たすものが対象事業体となる。また、対象サイバーインシデントは、対象事業体が経験する重大な（substantial）サイバーインシデントであり、最終規則で CISA 長官が定める定義及び基準を満たすものである。

（3）報告義務に従わない場合の措置（第 2244 条）

対象事業体が報告義務を遵守していないと信ずべき理由がある場合、CISA 長官は直接、当該事業体に情報を要求することができる。72 時間以内に十分な応答が得られない場合、同長官は情報開示を命じる召喚状（subpoena）を発出することができ、事業体が召喚状に応じない場合、連邦政府（司法長官）は召喚状を強制するため民事訴訟を起こすことができる。

（4）対象事業体の保護（第 2245 条）

CISA に提出された報告書は、情報自由法[4] その他の法律による開示を免除される。また、報告を提出することは、企業秘密等に関する法律上の保護の放棄とは見なされない（同条(b) (2) (3)）。事業者は報告提出に起因する法的責任から保護され、これを訴因とする訴訟は却下され

＊　本稿におけるインターネット情報の最終アクセス日は、2022 年 7 月 8 日である。

[1] Cyber Incident Reporting for Critical Infrastructure Act of 2022. 2022 年 3 月 15 日に成立した 2022 会計年度の包括的歳出法（本予算）（Consolidated Appropriations Act, 2022, P.L.117-103）に第 Y 部として含まれている。

[2] Homeland Security Act of 2002, P.L.107-296, November 25, 2002.

[3] Critical Infrastructure Security and Resilience (Presidential Policy Directive), PPD-21, February 12, 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> 同指令では重要インフラ部門として、化学、商業施設、通信、重要製造業、ダム、防衛産業基盤、緊急対応機関、エネルギー、金融、食料・農業、政府施設、ヘルスケア・公衆衛生、情報技術、原子炉・核物質・核廃棄物、輸送システム、水・排水システムの 16 部門を挙げている。

[4] Freedom of Information Act (5 U.S.C. § 552).

る（同(c)）。政府は、当該事業体の活動を規制（法執行を含む。）するために、報告により取得した情報を用いてはならない（同(a) (5)）。

（5）規則制定と施行日（第 2242 条(b)、第 2242 条(a) (7)）

CISA 長官は、法制定日から 24 か月以内に規則案を連邦官報で公示し、公示から 18 か月以内に最終規則を制定する。 報告義務に関する規定の施行日は、最終規則において定められる。

2　州及び地方政府サイバーセキュリティ法

2022 年 6 月 21 日、2002 年国土安全保障法第 22 編第 2209 条に規定を追加し、州や地方政府等のサイバーセキュリティに関する連邦政府の協力について法定化する法律が制定された[5]。国家サイバーセキュリティ通信統合センター（NCCIC）[6]は、他機関（多州間情報共有分析センター（MS-ISAC）など）と連携し、州、地方政府等及びその下部組織のために、求めに応じ、サイバーセキュリティに関する訓練、戦略的・技術的研修、情報共有支援、影響が及ぶ特定インシデント情報の通知、製品・政策・ガイドライン等に関する情報提供・調整・運用支援、政策・手順策定支援、教育・啓発の推進を行う[7]。

3　連邦サイバー職員出向法

IT、サイバーセキュリティ、その他サイバー関連の機能を持つ職務ポジション（サイバー職ポジション）職員の連邦省庁間出向プログラムを創出する法律も同日制定された[8]。各省庁の長は、自組織のサイバー職ポジションの同プログラム参加を決定することができ、その決定及びポジションの情報を人事管理局（OPM）長官に提出する（第 3 条）。OPM 長官は、法制定後 270 日以内にサイバー職ポジション間の職員出向に係る指針、過程及び手続を定めた「連邦サイバー職員出向プログラム運用計画」を策定し、公表するものとする（第 4 条）[9]。本法には、法廃止期日を制定の 5 年後と定めた条項（サンセット条項）が置かれている（第 6 条）。

4　サプライチェーン・セキュリティ研修法

同月 16 日、サプライチェーン（供給網）のリスク管理業務に従事する連邦職員向け研修に関する法律も制定された[10]。共通役務庁（GSA）長官は、連邦調達研究所（FAI）を通じ、法制定後 180 日以内に、ICT の調達を含め、調達過程において生じるサプライチェーンのセキュリティリスクを識別・軽減し、業務を遂行するための研修プログラムを策定する。研修プログラム策定後 180 日以内に行政管理予算局（OMB）長官は、関連のガイダンスを公表し、連邦省庁に研修プログラムの採用･使用を義務付け､立法府と司法府にはその利用を可能とする（第 2 条）。

---

[5] State and Local Government Cybersecurity Act of 2021, P.L.117-150, June 21, 2022.

[6] CISA 長官の特定の任務実施のため国土安全保障省に設置される組織（2002 年国土安全保障法第 2209 条(b)）。

[7] 州・地方政府への連邦の支援に係る最近の立法として他に、2021 年 10 月 8 日、CISA 長官がハイスクール段階までの学校のサイバーセキュリティリスクを調査し、ガイドラインを含む勧告を策定すること、学校教職員向けオンライン研修ツールを作成することなどを定めた法律が制定されている（K-12 Cybersecurity Act of 2021, P.L.117-47）。また、同年 11 月 15 日制定の「インフラ投資雇用法」（Infrastructure Investment and Jobs Act, P.L.117–58）第 G 部第 6 編で､州と地方政府のサイバーセキュリティのための補助金プログラムに 4 年間で 10 億ドルが配分されている。2022 年 5 月 12 日にも関連の立法が行われている（P.L.117-122）（本誌 No.292-2, 2022.8, p.28 参照）。

[8] Federal Rotational Cyber Workforce Program Act of 2021, P.L.117-149, June 21, 2022.

[9] 類似のプログラムを定めた 2019 年 5 月 2 日の大統領令第 13870 号「アメリカのサイバーセキュリティ・ワークフォース」は、こうした出向について、知識移転メカニズム及び人材育成プログラムであるとしている。

[10] Supply Chain Security Training Act of 2021, P.L.117-145, June 16, 2022.