

経済産業省 御中

令和3年度サイバー・フィジカル・セキュリティ対策促進事業 (サイバーセキュリティ法制度の国際動向等に関する調査)

報告書

MRI 三菱総合研究所

2022年3月31日

デジタル・イノベーション本部

目次

1. はじめに.....	4
1.1 調査背景・目的	4
1.2 調査実施概要	4
2. サイバーセキュリティに関する諸外国の法制度や官民の取組等に関する調査.....	5
2.1 ランサムウェアに関する法制度や取組.....	5
2.1.1 2021 年 4 月以降のランサムウェア関連調査.....	5
2.1.2 サイバーインシデントに関する報告.....	7
2.2 諸外国におけるサイバーセキュリティに関する取組.....	10
2.2.1 諸外国における中小企業向けのガイドライン・ツール・認証制度等の比較.....	10
2.2.2 諸外国における政府(国)のサイバー保険普及策の有無.....	14
2.2.3 EU 諸国におけるソフトウェアのセキュリティ確保に向けた取組(SBOM 等)に関する調査	18
3. サプライチェーンを支える基盤インフラ技術に関する調査	19
3.1 基盤インフラ技術の最新動向.....	19
3.1.1 基盤インフラ技術の全体像.....	19
3.1.2 基盤インフラ実現に向けた政策動向.....	22
3.1.3 基盤インフラを構成する基盤ソフトウェアの課題	24
3.2 基盤インフラ技術に関して求められる政策の検討	24
3.2.1 有識者会合(持ち回り会合)の実施.....	24
4. 総括	26

別紙 1 現代のサイバーセキュリティの法的課題についての国際的な研究に関する調査

図 目次

図 3-1 基盤インフラの概念(昨年度報告書より)	19
図 3-2 スーパーシティ(電力)のアーキテクチャ例(昨年度報告書より).....	20
図 3-3 スーパーシティ(スマートファクトリー)のアーキテクチャ例(昨年度報告書より).....	21
図 3-4 スーパーシティ(自動車)のアーキテクチャ例(昨年度報告書より)	21
図 3-5 基盤インフラ技術研究開発のスコープ(昨年度報告書より)	22
図 3-6 分散処理技術を用いたデータ活用基盤のイメージ(半導体・デジタル産業戦略検討会議資料より)	23

表 目次

表 2-1 諸外国の中小企業向けガイドラインの比較	10
表 2-2 諸外国の中小企業向け認証制度の比較.....	12
表 2-3 諸外国の中小企業向け補助／支援制度の比較.....	12
表 2-4 諸外国の規制や報告制度の比較	13
表 2-5 諸外国のツール類の比較	14

1. はじめに

1.1 調査背景・目的

我が国では、サイバー空間とフィジカル空間を高度に融合させることにより、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的发展と社会的課題の解決を両立する超スマート社会「Society5.0」の実現を提唱している。「Society5.0」では、データの流通・活用を含む、より柔軟で動的なサプライチェーンを構成することが可能となるが、他方で、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という新たなリスクへの対応が必要である。

実際に、世界中でサプライチェーンの弱点を狙った攻撃や重要インフラ事業者のランサムウェア被害による操業停止などが発生しており、上述のような新たなリスクが顕在化している。こうした状況を踏まえ、各国は対応を急いでおり、例えば、2021年5月には米国においてサイバーセキュリティに関する大統領令が発出され、政府関係機関等による取組が加速化しているほか、2020年12月にはEUにおいてネットワーク・情報セキュリティ指令の改定(NIS2)が提案されるなど、サプライチェーン全体のサイバーセキュリティ強化に向けた取組は世界中で加速している。こうした中、日本の産業におけるサプライチェーン・サイバーセキュリティの確保、及び、世界でビジネスを行う日本企業の市場確保の観点からも、最新技術動向や主要関係国における新たなサイバーセキュリティ関連の制度・取組の動向を把握した上で、最新技術や国際的な制度調和を意識した産業サイバーセキュリティ政策を立案する必要がある。

このような状況を踏まえ、本事業では、サイバーセキュリティに関する諸外国の法制度や官民の取組、及び、サプライチェーンを支える基盤インフラ技術についての調査を実施した。

1.2 調査実施概要

調査目的を達成するために、以下の項目に関して調査・検討を行った。

1. サイバーセキュリティに関する諸外国の法制度や官民の取組等に関する調査
 - (1) ランサムウェアに関する法制度や取組
 - (2) 諸外国におけるサイバーセキュリティに関する取組
2. サプライチェーンを支える基盤インフラ技術に関する調査
 - (1) 基盤インフラ技術の最新動向
 - (2) 基盤インフラ技術に関して求められる政策の検討

2. サイバーセキュリティに関する諸外国の法制度や官民の取組等に関する調査

サイバーセキュリティに関連し、諸外国で検討・実施されている法制度や官民の各種取組（法令、認証制度、フレームワーク、ガイドライン、その他官民の取組等）について、当該取組の背景、検討経緯、主要関係機関、関連する法制度、今後の見通し、ステークホルダーの反応等について調査・分析の上、とりまとめた。

2.1 ランサムウェアに関する法制度や取組

2.1.1 2021 年 4 月以降のランサムウェア関連調査

(1) アメリカにおけるランサムウェア対応の進展

2021 年 4 月以降のランサムウェア事案に対する米国における対応について、法的な観点から考察する。

a. コロニアルパイプライン事件の概要

2021 年、米国のコロニアルパイプライン社は、標的型ランサムウェア（身代金要求ウイルス）攻撃を受け、操業停止に陥った。このランサムウェア攻撃を受け、同社は暗号資産により犯罪集団に身代金を支払っている。本件の事実関係については、連邦議会上下院で行われた 3 回の公聴会における証言が参考となる。

コロニアルパイプライン社の最高経営責任者は、身代金を支払う理由として、①ガソリンの供給が滞れば、救急車等の緊急車両が動かなくなるといった緊急事態が生じることから早期の復旧が最重要であり、②IT ネットワークシステムのバックアップに基づく復旧は時間を要することから、最も早期に復旧できる身代金の支払いを選択したと述べている。また、同最高経営責任者は、身代金の支払いを「個人の判断」で行ったことを強調している。その理由は、第三者（セキュリティ会社や顧問弁護士事務所等）が身代金の支払いを勧めた等の事実があると、財務省外国資産管理局（OFAC）の勧告に基づき、これらの第三者にも責任が及ぶ可能性があるためである。

コロニアルパイプライン社が、身代金を支払った事実を最初に報告した連邦行政機関は FBI であり、その報告は、支払いが行われた日から約 48 時間以内に行われたと証言されている。また、具体的な支払いに関する報告がなされる以前に、Digital Wallet に関する情報を FBI と共有したと証言されている。その後、すべてのパイプラインを稼働させることができた。また、同氏自身は、パイプラインを早期に復旧させることを最優先に考えていたことから、サイバー保険の保険金が支払われる点については考慮の対象としていなかったと証言している。

b. 連邦運輸保安庁によるサイバーセキュリティ対策に関する法的規制

これまで、連邦文民行政機関（国防総省とインテリジェンス機関を除いた連邦行政機関）が発行する

サイバーセキュリティ指針等には、規制対象となる重要インフラを運営する民間企業に対して法的拘束力がなかった。主務官庁は、セクターごとにサイバーセキュリティに関する指針等を定めて推奨してきたものの、これを遵守するか否かは、民間企業の自主的な判断に委ねられていた。

連邦監査院が行った TSA によるパイプラインに関するセキュリティプログラムマネジメントの問題点に関する証言では、①TSA は、パイプラインに関するサイバーセキュリティ指針に、国立標準技術研究所(NIST)が定めた重要インフラに関するサイバーセキュリティの向上における全ての要素を導入しておらず、これは同指針が定期的に見直されていないことが原因となっており、②TSA のパイプライン監査チームには、サイバーセキュリティに関する専門知識がない等の人員に関する問題があり、さらには、③パイプラインの保全審査に関するリスク評価方法も 2014 年から改訂されていない等の問題があると指摘されている。さらに、連邦監査院は、2018 年及び 2019 年に指摘した問題点のうち、2021 年 6 月の時点で、①TSA はパイプライン事業者に関する脅威、脆弱性等についてリスク評価を行うために必要となる十分な関連データを所持しておらず、②パイプライン事業者のセキュリティインシデントに対応する手順書が 10 年以上も改訂されていない等の問題について、いまだ十分な対応ができていないとの指摘がなされている。

ア) 法的拘束力のある指令の発出

連邦議会からの批判や、連邦監査院からの指摘を受け、国土安全保障省(DHS)は、パイプライン事業者に対して、2 段階で、TSA が指定した重要なパイプライン企業に対して、法的拘束力をもつ指令を発出した。DHS は、まず、2021 年 5 月 28 日に、民間のパイプライン事業者に対して、サイバーインシデント等に関して法的拘束力を持つ指令「パイプライン事業者のサイバーセキュリティの向上」(Dep't of Homeland Sec., Enhancing Pipeline Cybersecurity, Security Directive Pipeline-2021-01 (May 28, 2021))を発出した。その主たる内容は、以下のとおりである。

- 該当する事業の所有者・運営者は、本指令の施行日から 7 日以内(2021 年 6 月 4 日まで)に、TSA に対して、サイバーセキュリティ調整担当者(cybersecurity coordinator)及び少なくとも 1 名の代行者を任命し、その氏名、役職、電話番号及びメールアドレスを TSA に報告すること。
- 該当する事業の所有者・運営者は、自らが運営するシステムにおけるサイバーセキュリティインシデントが特定されてから可能な限り速やかに(少なくとも 12 時間以内に)、CISA のウェブサイト上の報告システム又は CISA の緊急連絡電話を用いて CISA に報告する義務を負う。もしも、求められているすべての情報が指定されている時間内に報告できない場合には、まず指定時間内に判明している情報のみを報告し、他の情報が判明した場合には補足的に報告を行うものとする。報告されるすべての情報は、その機微性及び重要性に応じて保護され、かつ、公開されることはない。なお、ここに言うサイバーセキュリティインシデントとは、①情報システム又は制御技術システムへの不正アクセス、②情報システム又は制御技術システムにマルウェアが見つかったこと、③情報システム又は制御技術システムへの DoS 攻撃、④所有者・運営者のネットワーク・インフラに対する物理的攻撃、⑤その他のサイバーセキュリティインシデントで、システム若しくは施設の運営を妨げるもの、又は、多数の顧客、政府の中核的機能、国家安全保障、経済安全保障等に影響をもたらし、安全で効率的な輸送に支障を引き起こす可能性のある運営を妨げるもの等を意味している。
- 「パイプラインに関するサイバーセキュリティ指針(Transp. Sec. Admin., Pipeline Security Guidelines (Mar. 2018 with Change 1 (April 2021)))」第 7 条に基づいて当該パイプラ

インのセキュリティ対策の現状を評価し、あるべき状態とのギャップがあれば特定し、その改善方法と改善計画とを策定して、TSA の定めた評価書式に記載した上で、TSA と CISA に本指令の施行日から 30 日以内(2021 年 6 月 27 日まで)に提出すること。

イ) 第 2 の法的拘束力を持つ指令

DHS は、2021 年 7 月 20 日に、第 2 の法的拘束力を持つ指令(Dep't of Homeland Sec., Security Directive Pipeline-2021-02)を発出したとの発表を行った。ただし、この指令そのものは機密指定がなされているため、その内容は公表されていない

なお、バイデン大統領が発した「重要インフラの制御システムのサイバーセキュリティ向上に関する国家安全保障覚書」の概況報告書では、この第 2 指令においては、①ランサムウェア攻撃等の脅威から情報技術システムと制御技術システムを保護するために、所定の期限以内に特定された緩和策を実施すること、②サイバーセキュリティ緊急対策及び復旧計画を策定・実施すること、及び、③サイバーセキュリティアーキテクチャデザイン年次審査(annual cybersecurity architecture design review)を実施すること等が規定されているとしている。

2.1.2 サイバーインシデントに関する報告

(1) 連邦行政機関に対してサイバーインシデントに関する通知義務を定めたもの

2002 年連邦情報セキュリティ・マネジメント法(Federal Information Security Management Act of 2002: FISMA)において、連邦行政機関でサイバーインシデントが起きた場合には、当該行政機関は、連邦法執行機関、監察総監室及び指定された連邦行政機関に通知する義務を定めている。そして、FISMA の委任に基づいて CISA が発出した「連邦インシデント通知ガイドライン」(US-CERT Federal Incident Notification Guidelines, Apr.1, 2017)に具体的な規定が置かれ、連邦文民行政機関の連邦情報システムにおける機密性・完全性・可用性に危殆化が生じた場合には、当該情報セキュリティインシデントについて、必要な報告要件とともに、CISA/US コンピュータ緊急対応チームに1時間以内に報告しなければならないこと等を定めている。

また、FISMA では、連邦行政機関が「重大なインシデント(major incidents)」に遭遇した場合には、当該インシデントが起きたと合理的に結論付けられるようになった日から 7 日以内に、又、当該インシデントに関するより詳細な内容を合理的な期間内に、連邦議会の関連する委員会に報告しなければならないと規定されている。

(2) 民間企業に対してサイバーインシデントに関する通知義務を定めたもの

まず、大規模電力システムについては、連邦エネルギー規制委員会の定める規則「サイバーセキュリティインシデント報告信頼性基準」に基づき、重大なインシデントについては、電力 ISAC(Electricity Information Sharing and Analysis Center)に 1 時間以内に報告しなければならないとの規制が課されている。

また、原子力発電システムに関するサイバーセキュリティ事案については、原子力規制委員会規則に基づき、緊急通知システム(Emergency Notification System)を通じて原子力規制委員会本部オ

ペレーションセンター(NRC Headquarters Operations Center)に、①重大な損害をもたらす攻撃が起きた場合には、1 時間以内に、②重大な損害をもたらす可能性のあった攻撃又はその未遂が判明した場合には、4 時間以内に、③サイバー攻撃の準備行為が判明した場合には、8 時間以内に報告する義務が課されている

次に、国防総省における請負人(下請負人含む)については、国防総省調達規則補遺(DFARS)に基づき、サイバーインシデントの発見から 72 時間以内に「迅速な報告」を行わなければならないと定められている

最後に、銀行業については、2021 年 11 月 23 日に、通貨監督庁(Office of the Comptroller of the Currency)、連邦準備制度理事会(Federal Reserve Board of Governors)及び連邦預金保険公社(Federal Deposit Insurance Corporation)は、共同で、連邦法上の規制を受ける銀行に対して、コンピュータセキュリティに関するインシデント(情報システム又は情報システム内の情報に実際の損害をもたらす可能性のあるもの)のうち、銀行の組織的運営又は基幹業務に実質的な支障をもたらすインシデントに該当する「通知インシデント(notification incident)」が起きたと判断した場合には、主務官庁に対して、迅速に(少なくとも 36 時間以内に)通知を行う義務を課す規則を制定した。なお、本規則の施行日は 2022 年 4 月 1 日であり、上記のサイバーインシデントに関する報告義務については、2022 年 5 月 1 日から適用される。

(3) 2021 年サイバーインシデント通知法案の概要

1) 本法案の概要

連邦行政機関、連邦政府の請負人及び重要インフラの所有者・運営者がサイバーインシデントを発見した場合には、CISA に 24 時間以内に報告を行う義務等を定めた 2021 年サイバーインシデント通知法(Cyber Incident Notification Act of 2021, 117 S. 2407)案が提出された。

本法案を含め、後で紹介する諸法案も、2002 年国土安全保障法(Homeland Security Act of 2002)の第 22 編(Cybersecurity and Infrastructure Security Agency Act of 2015 により同法に追加されたもの)を改正する形式をとっている。

また、本法案では、民間企業による連邦政府との情報共有を促進するために、①被害を受けた企業等が報告を行ったことで不利益を被らないように、当該企業に一定の情報秘匿特権を認めるとともに、②CISA が、個人を特定しうる情報を匿名化し、かつ、プライバシーを保護するためのデータ保護手続を採用する規定を置いている。

2) 本法案の規制対象者とその通知義務

本法案における「規制対象者(covered entities)」とは、①連邦行政機関、②連邦政府の請負人、③サイバーセキュリティ・インフラ保全庁(CISA)長官が、当該重要インフラの運営がセキュリティ侵害を受けた場合に想定されるリスク評価に基づいて、規制対象とすることが適切であると決定した重要インフラの所有者・運営者、及び、④サイバーセキュリティインシデント対応サービスを提供する非政府主体を意味している。

連邦行政機関又は規制対象者は、サイバーセキュリティ侵害又は潜在的サイバーセキュリティ侵害を

年の総売上高(gross revenue)の 0.5 パーセントを超えない額を、当該違反が継続した期間又は今後も継続する期間における1日当たりの民事上の罰金として評価することができるが、②当該違反の性質、状況、程度及び重大性、規制対象者の支払能力、有責性及び過去の違反歴等の情状を酌量して、上記の罰金を減額若しくは変更することができる。また、同長官は、③この罰金に関する不服申立手続を制定しなければならないと規定されている。

4) バイデン大統領による「重要インフラの制御システムのサイバーセキュリティ向上に関する国家安全保障覚書」

バイデン大統領は、2021 年 7 月 28 日に、「重要インフラの制御システムのサイバーセキュリティ向上に関する国家安全保障覚書 (National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems)」に署名した。

本覚書と同時に出された概況報告書(FACT SHEET)「バイデン政権による米国の重要インフラを保護するための追加的施策の公表」(White House, FACT SHEET: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure, July 28, 2021)では、①コロニアルパイプライン社及び JBS フードに対するランサムウェア攻撃に見られるように、民間部門が主体となって運営されている米国の重要インフラには、重大なサイバー上の脆弱性が存在しており、②このような重要インフラを制御しているシステムの劣化、機能不全等により、米国の国家安全保障、経済安全保障及び米国市民の公衆衛生・安全が弱体化する恐れがあることから、③重要インフラに対する現在の規制がセクター別になされていることに起因する問題を克服するために、最低限の共通基準を定めるとともに、④重要インフラの所有者と運営者に、自主的なガイダンスと法的拘束力を持った規制に従ってもらうことが必要になるとしている。

2.2 諸外国におけるサイバーセキュリティに関する取組

諸外国におけるサイバーセキュリティへの官民の取組について調査や比較を実施した。具体的には中小企業対策の取組、サイバー保険の普及に向けた取組、SBOM 等によるソフトウェアセキュリティ対策への取組、各国のサイバーセキュリティに係る規制等について調査を実施した。その詳細を以下に取りまとめる。

2.2.1 諸外国における中小企業向けのガイドライン・ツール・認証制度等の比較

米国、EU、英国、豪州を対象に、中小企業向けのサイバーセキュリティ施策の推進状況として、ガイドライン、認証制度、補助金／支援制度、規制や報告制度、ツール類等についての調査を実施した。

(1) ガイドライン

表 2-1 諸外国の中小企業向けガイドラインの比較

国	制度概要
米国	(1) CYBER ESSENTIALS: 中小企業のリーダーや地方自治体機関のリーダーが、組織のサイバーセキュリティの

	実践をどこから始めればよいのか、実行可能な理解を深めるための手引書。 (2) Cybersecurity Resources Road Map (A Guide for Critical Infrastructure SMBs): 4つの階層と各階層における2つの質問で構成され、重要インフラの中堅・中小企業が、自社のニーズに合った有用なサイバーセキュリティ・リソースを特定できるように設計されたロードマップ。 (3) 10 Cyber Security Tips for Small Business: 中小企業を保護するためのサイバーセキュリティに関する10の重要なヒントの解説。 (4) CYBERSECURITY FOR SMALL BUSINESS: FTC の公表するスモールビジネス向けのサイバーセキュリティ検討ポイント紹介資料。
欧州	(1) Cybersecurity guide for SMEs - 12 steps to securing your business: 中小企業が自社のシステムとビジネスの安全性を高めるための、12の実践的なハイレベルのステップを紹介したガイド。 (2) Essential Guide to Cyber-risk Management: 企業のリスク管理プロセスについての解説書。 (3) 10 steps for a Cybersecurity-beginner SME: 10のステップに従って中小企業がデジタル資産を保護するための解説書。 (4) ETSI TR 103 787-1 Cybersecurity Standardization Essentials: 中小企業が規格やフレームワークを導入してサイバーセキュリティを確立するために、何から手をつければよいのか、必要な情報を提供するために、主要な5つのフレームワークを分析し、5つのステップに展開しなおしたガイド。
英国	(1) Small Business Guide: Cyber Security: 中小企業向けのサイバー攻撃を遠ざけるための5ポイント(バックアップ対策、マルウェア対策、スマートフォン対策、パスワード管理対策、フィッシング対策)を紹介したガイド。
豪州	(1) Small Business Cyber Security Guide: 一般的なサイバーセキュリティの事故を防ぐために、中小企業でも導入できる簡単な対策について解説したガイド。 (2) Step-by-step guides: PCの起動、特定アプリの起動や認証、マルウェア防御等の29の特定のテーマについて、具体的な設定方法等を画面コピーで示した初心者向けマニュアル。 (3) Cyber Security: The Small Business Best Practice Guide: 中小企業がサイバーセキュリティ対策を考えるために必要なポイントを網羅的に解説したガイド。 (4) Quick wins: サイバーセキュリティに影響を与える技術的な問題について、その概要をユーザーに伝えるための資料で、モバイル機器、ウェブサイト、ソフトウェアのサポート終了について

	て解説したもの。

(2) 認証制度

表 2-2 諸外国の中小企業向け認証制度の比較

国	制度概要
米国	－
欧州	(1) Cybersecurity Label: 簡単なオンライン診断により中小企業のサイバーセキュリティ対策レベルを評価する認定ラベル制度。 (2) CYBERSECURITY MADE IN EUROPE label: 欧州のサイバーセキュリティ企業のプロモーションを行い、欧州およびグローバル市場での認知度を高めるためのマーケティングツールとしてのラベル認定制度。
英国	(1) Cyber Essentials: オンラインによる自己診断アンケートに回答することで、最も一般的なサイバー攻撃からの幅広い保護レベルを証明する認証制度。自己診断に加えて実地検証を含む Cyber Essentials Plus もある。
豪州	－

(3) 補助金／支援制度

表 2-3 諸外国の中小企業向け補助／支援制度の比較

国	制度概要
米国	(1) Resources for Small and Midsize Businesses (SMB): CISA が提供する SMB 向けの情報提供ポータル。 (2) SMALL BUSINESS CYBERSECURITY CORNER: NIST の展開するスモールビジネス向けのサイバーセキュリティ情報提供ポータル (3) SBA will Award \$3M in Grants to Help States, Entrepreneurs Combat Rise in Cyber Attacks and Threats: 2022 年 1 月、中小企業庁(SBA)が、新興中小企業がサイバーセキュリティ・インフラを開発するのを支援するために、300 万ドルの新たな助成金制度を発表。
欧州	(1) MARKETPLACE: ヨーロッパ全体のサイバーセキュリティ関連情報、製品、サービスについて、互いの情報を検索、交換することができるプロモーションスペース。 (2) European Cybersecurity STARtup Award: 欧州のサイバーセキュリティスタートアップに対するコンペティション形式の表彰制度。

英国	(1) Cyber Exchange: サイバーセキュリティ関連企業へのマッチングや情報提供を行うサービスで、各種コンサルティングや補助金等の情報を提供。
豪州	(1) "Small & medium businesses" page of ACSC: 中小企業向けのサイバーセキュリティ関連情報を一括して取り扱うポータルサイト。 (2) 様々な案件採択型の助成金制度を実施:

(4) 規制や報告制度

表 2-4 諸外国の規制や報告制度の比較

国	制度概要
米国	(1) Executive Order on Improving the Nation's Cybersecurity: 2021 年 5 月 12 日に署名された、政府と契約する情報通信サービス企業との間で、サイバーセキュリティ分野での官民連携を深め、同分野の発展を目指すとして、複数の施策の方向性を示した大統領令。情報通信サービス企業の報告義務について触れている。 (2) Ransom Disclosure Act: 2021 年 10 月上院に提出されたランサムに感染した企業に対する情報公開を義務付ける制度を盛り込んだ法案。米国企業や組織がランサムウェアに感染し身代金の要求を受けた際、要求された通貨の種別(米ドル・仮想通貨など)や要求金額、支払いの意思や金額などの情報提供を義務付けるというもの。 (3) Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers : 財務省通貨監督庁(OCC)、連邦準備制度理事会(Board of Governors of the Federal Reserve System)、および連邦預金保険公社(Federal Deposit Insurance Corp)によって発出された規則。銀行が「重大な」サイバーセキュリティ事案を発見した場合、発見から 36 時間以内に報告することを義務付けるもの。
欧州	(1) Cybersecurity Incident Reporting and Analysis System (CIRAS): 電気通信事業者、トラストサービス、重要インフラ事業者はそれぞれの規則によりサイバーインシデントの報告義務が課せられており、その報告を受けるシステム、報告結果の年次の分析結果の可視化情報提供するシステム。
英国	(1) The Cyber Security Information Sharing Partnership (CiSP): 英国の産業界及び政府等の組織が安全かつ機密性の高い環境でサイバー脅威情報を共有できるようにした仕組み。 (2) 重要インフラ事業者向け規則: NIS 指令に基づき、英国でサイバーセキュリティ法令を発行、重要インフラ事業者は、サイバーセキュリティ対策の実施、セキュリティ事故や IT 障害が発生した場合に規制当局への報告を義務化、サイバーセキュリティ対策を怠った場合の罰則などを発表。

豪州	(1) 重要インフラに関するインシデント報告: Security of Critical Infrastructure Act 2018 により、重要インフラ事業者はサイバー攻撃を受けた際の報告義務があるとされている。
----	--

(5) ツール類

表 2-5 諸外国のツール類の比較

国	制度概要
米国	(1) CISA CYBERSECURITY AWARENESS PROGRAM TOOLKIT: CISA の提供するあらゆる層を対象としたサイバーセキュリティ啓蒙プログラム・ツールキット。
欧州	(1) Cybersecurity for SMEs - Challenges and Recommendations: コロナ禍における中小企業のサイバーセキュリティの状況を調査し、中小企業自身の必要な対策や政府の政策について提言を行う報告書。 (2) GEIGER: Horizon2020 のプロジェクトで、中小企業が自社のリスクレベルを動的に測定できるダッシュボード的ツール開発を目指しているもの。
英国	(1) Cyber Aware: 個人または小事業者向けに、いくつかの基本的な質問に答えると、必要な対策のアクションプランを提示してくれるサービス。
豪州	—

2.2.2 諸外国における政府(国)のサイバー保険普及策の有無

米国、EU、英国、OECD を対象に、各国のサイバー保険普及策についての調査を実施した。

(1) サイバー保険の市場動向

経済協力開発機構(OECD)の推計によると、世界のサイバー保険市場の保険料規模は 2019 年時点でおおよそ 40 億ドル～50 億ドルとされている。また、保険監督者国際機構(IAIS)は、2025 年には約 200 億ドル規模に拡大すると予測している。

なお、日本損害保険協会の 2020 年の調査によると、わが国の企業のサイバー保険加入率は 7.8%にとどまっている。それに対し欧米主要国ではサイバー保険の活用が進んでおり、特に米国においては企業の加入率は 50%以上となっている。

(2) 米国の状況

- 米国企業全体におけるサイバー保険の加入率は 20～35%。
- ヘルスケア、教育分野の企業の加入率が 40～50%で高率となっており、金融、小売業界がそれ

に続く。今後は、製造、エネルギー業界においてもサイバー保険への加入が大幅に増加するとの見通し。2020 年までに年間保険料収入ベースで 56 億ドル規模に成長すると予測されている。



- 2020 年 2 月に開催された EU-US Insurance Dialogue Project の Cyber Insurance WG では、以下の議論が行われた。
 - サイバー保険の市場はまだ発展中であり、提供されているサイバー保険の種類も多様である。サイバー保険市場の発展のためには、ダイナミックに変化するサイバーリスクに対処できる商品設計が必要である。そのためには、以下の取組みが必要である。一方、保険会社としては、AI の活用等による契約文書のチェック・更新等をおこない、カバー範囲の明確化に取り組んでいる。
 - ◇ サイバーリスクおよび損失に関する認識の向上
 - ◇ 業界、保険会社、規制当局を含むステークホルダー間でサイバーリスク管理のベストプラクティスの共有
 - ◇ リスクベースの適切な保険料の算出のため、定量的モデルの使用の支援
 - ◇ 保険契約者によるサイバーインシデントへの対応と回復の促進
- EIOPA(European Insurance and Occupational Pensions Authority)のレポートによると、2018 年の保険会社の報告では総収入保険料が 72%増加し 2 億 9500 万ユーロに達している。そのフォローアップとして、EIOPA は 2019 年に、サイバーリスクに対する EIOPA の監督・規制上の優先事項を強調した「サイバーアンダーライティング戦略(Cyber Underwriting Strategy)」を策定。
- OECD レポートでは、保険契約においてサイバーがカバーされている範囲の明確化の必要性が示唆される。なお、米国では非確定的リスクが保守的な保険引き受け内容となる要因となっている。
- なお、サイバーリスクの定量化が困難であること、リスクが蓄積される可能性があること等の課題は、再保険会社も同様である。
- EU においても、米国と同様に、サイバーリスク専用の報告テンプレートを持っている。ここでは、典型的な保険データ(保険料、技術規程など)に加え、確定的または非確定的(affirmative and non-affirmative)なサイバーリスクに分けて、詳細なデータを要求している。
- 本 WG では、さらに掘り下げていくべきテーマとして以下を提案した。
 - 潜在的な蓄積リスクを含むサイバーリスクのより洗練された評価を可能にするデータ収集や技術開発
 - サイバーインシデント報告と対応のベストプラクティスへのアプローチの共有可能性
 - サイバーリスクの体系的性質に取り組むためのリスク・プールの役割と利用方法
- 2018 年 5 月に施行された欧州の「一般データ保護規則(GDPR)」により、規制当局は、組織に対して年間売上高の 4%もの罰金を科すことができることになったことから、欧州連合を主要な顧客基盤とする企業においては、プライバシーやデータ保護に関する法律違反に伴う罰則や罰金をカバーする GDPR サイバー保険の需要が高まっている。

(4) 英国の状況

- 英国では 2020 年 8 月に、サイバー保険の導入を検討する企業向けにサイバーセキュリティに係る注意事項のガイダンスを公表。概要は以下の通り。
 - サイバー保険は、サイバーセキュリティの問題をすべて即座に解決するものではなく、サイ

バー攻撃を防ぐものではない。サイバー保険を検討する前に、サイバーエッセンシャルやサイバーエッセンシャルプラスの認定を受けたサイバーセキュリティ対策を確実に実施することで、組織を保護することができる。

- サイバー保険加入にあたっての注意事項(カバー範囲、付帯するサービス内容)や実施する必要のある事項(サイバーインシデントによる影響範囲の理解、セキュリティ診断等)
- サイバー保険のカバー範囲
- 多くの保険会社は、ポリシーを取り出した後、サイバーセキュリティコンサルタントサービスとリスク管理サポートを提供する。これには、財務保護に加えて、回復性の計画を提供することが含まれている。
- 英国政府が 2018 年実施した調査によると、大企業の 61% 及び中小企業の 31% がサイバー攻撃を受け、平均損害額は大企業で 22,700 ポンド、中小企業で 3,650 ポンドであった。2014 年、英国政府は一般的なサイバー攻撃から組織を守るための基本的なサイバーセキュリティの衛生基準である Cyber Essentials(一般的なサイバー攻撃に対して組織を保護するのに役立つ政府支援スキーム)を発表している。

(5) OECD の状況

- OECD では、2018 年に行政へのレコメンデーションとして以下の内容を提案している。
 - 政府は、デジタルセキュリティリスクに対処するための国家戦略におけるリスク管理に対して、保険の貢献可能性を認識すべきである。
 - 政府は、サイバー脅威及び事故に関する情報共有に取り組むべきである。入手可能な脅威情報の共有、影響を受けた企業によるインシデント情報の開示及び／又は情報共有の拡大を行うべきである(情報共有に対するあらゆる法的障害への対処を含む)。
 - 政府は、サイバー保険市場が提供する商品の明確性が高まり、複雑性が低減していることを確認すべきである。必要であれば、提供されている補償についてより明確にすることを促進するために、管理上のガイダンスを策定することも考えられる(国際協調による潜在的な利点も考慮)。
 - 各国政府は、保険(または再保険)会社に対して、過度に厳しい規制や監督上の要件を課すべきではない。
- OECD では、OECD 加盟国・非加盟国当局から提供されたアンケートへの回答、および 2019 年 9 月と 10 月に実施された(再)保険業界の代表者との非公式な協議に基づいて 2020 年にとりまとめた報告書の概要は以下のとおり。
 - 保険会社にとって最も重要なアクションは、サイバーリスクに対する補償内容をより明確にすることである。米国の商業保険ブローカーを対象に実施した定期調査では、ブローカーの大多数がサイバー保険の補償内容や除外事項が十分に明確化されていないと回答している。また、既存の損害保険や賠償責任保険にサイバーインシデントに起因する損害がカバーされている場合があるが、これらには免責事項が含まれている場合があり、免責事項がどの程度適用されるかについては不確実性がある。
- 政府の役割の可能性
 - いくつかの保険管轄当局は、それぞれの種類の保険におけるサイバーリスクの補償範囲に

3. サプライチェーンを支える基盤インフラ技術に関する調査

社会のあらゆる場面においてデジタル技術を活用した DX 化が検討され、その取組が進んでいる。それに伴い、今までは考えられていなかったような者同士が接続され、新たな使い方、アプリケーションを提案していくことになるが、これを効率的に実現するため、それぞれが同じシステム基盤の上に実装されることが重要である。

同時にシステム基盤側の技術的取組としても、昨今の仮想化、クラウド化技術の進歩とともに、従来は専用システムで構築されていたようなサービスが、汎用的なハードウェアの上で動くソフトウェアによって実現されるようになってきている。モバイル通信なども従来は専用のシステムで構成されていたが、5G の時代では仮想化された汎用コンピュータシステムによりネットワークが実現するに至っている。

この流れはますます進展し、様々な社会サービスが仮想化ソフトウェアシステムとして実現する時代が間近に迫っており、これらを支える基盤インフラを我が国として戦略的に構築し、維持することが重要となっている。

3.1 基盤インフラ技術の最新動向

本調査では、ポスト5G技術や次世代クラウド基盤技術、ゼロトラストなど、サプライチェーンを下支えする基盤インフラ技術の構成要素、アーキテクチャ、セキュリティ等について調査を実施した。

3.1.1 基盤インフラ技術の全体像

まず基盤インフラの概念イメージを示す。様々な社会インフラを実現する各分野のシステムがソフトウェアとして実現されることによって、同じ基盤上で動作することを想定している。

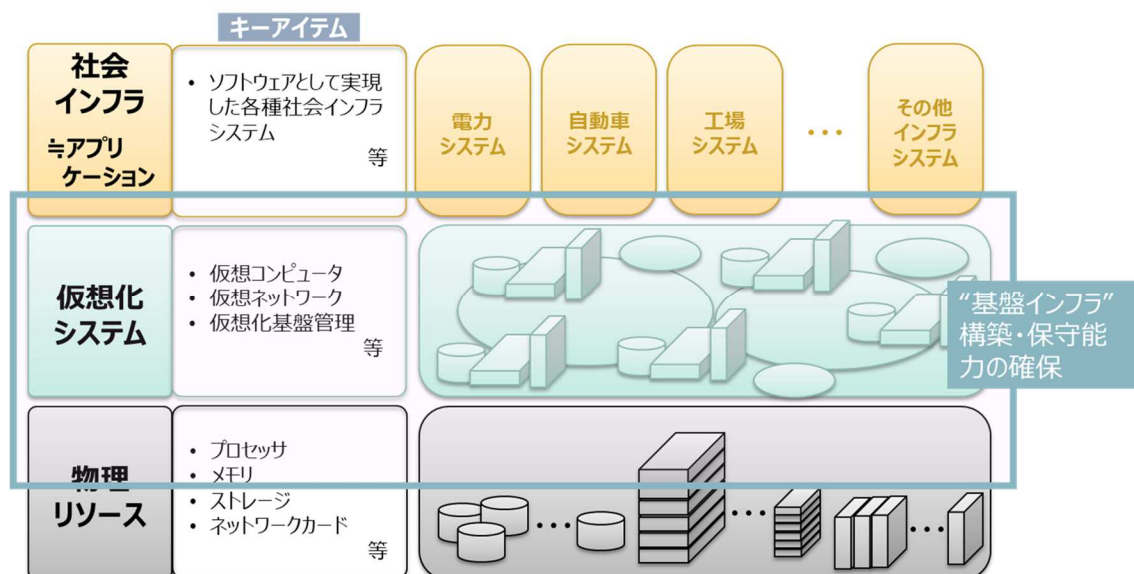


図 3-1 基盤インフラの概念(昨年度報告書より)

例えば1台のパソコン(共通のインフラ)に様々なソフトウェアを載せることによって、オフィス処理に使

うこともできれば、インターネット端末として使うことも、さらには専門の CAD システムとして使うこともできる。さらにウェブアプリケーションとして実装すれば、パソコンの種類を問わず、スマートフォンなどでも同じサービスが利用可能である。このような考え方を更に拡張していくと、あらゆるサービスアプリケーションをソフトウェア化し、汎用物理リソースと仮想化システムからなる巨大な仮想コンピュータ上で動かす姿を描くことが可能である。

これは社会システムとして、更に大きな枠組みで捉えることも可能であり、社会生活を実現する様々な社会インフラサービスがデジタルシステムとして融合的に機能し利便性を提供するスーパーシティを題材に考えると、次図のようなアーキテクチャとして捉えることが可能である。

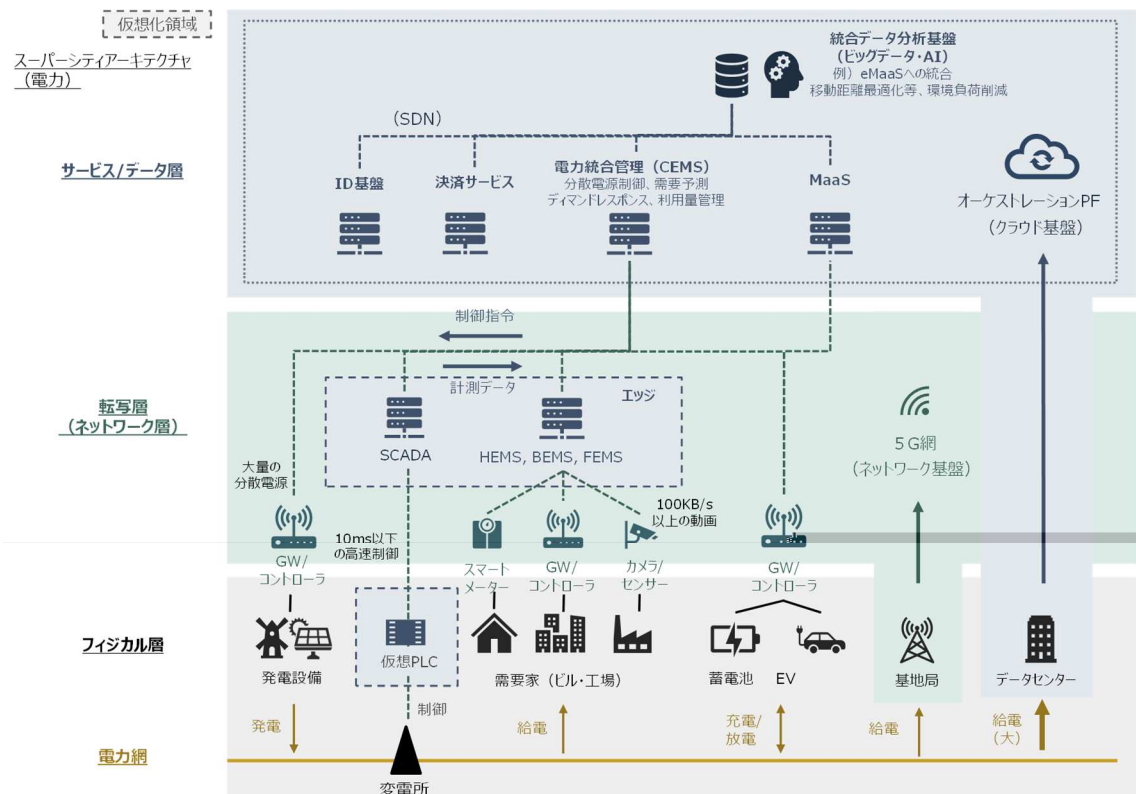


図 3-2 スーパーシティ(電力)のアーキテクチャ例(昨年度報告書より)

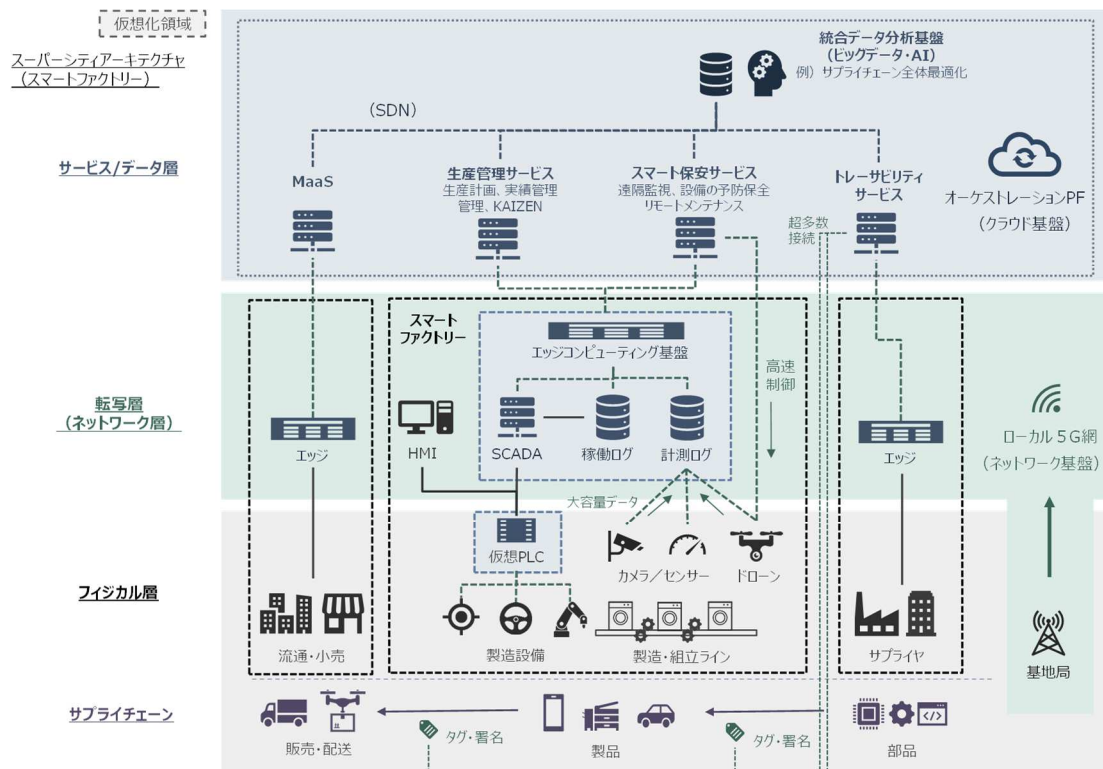


図 3-3 スーパーシティ(スマートファクトリー)のアーキテクチャ例(昨年度報告書より)

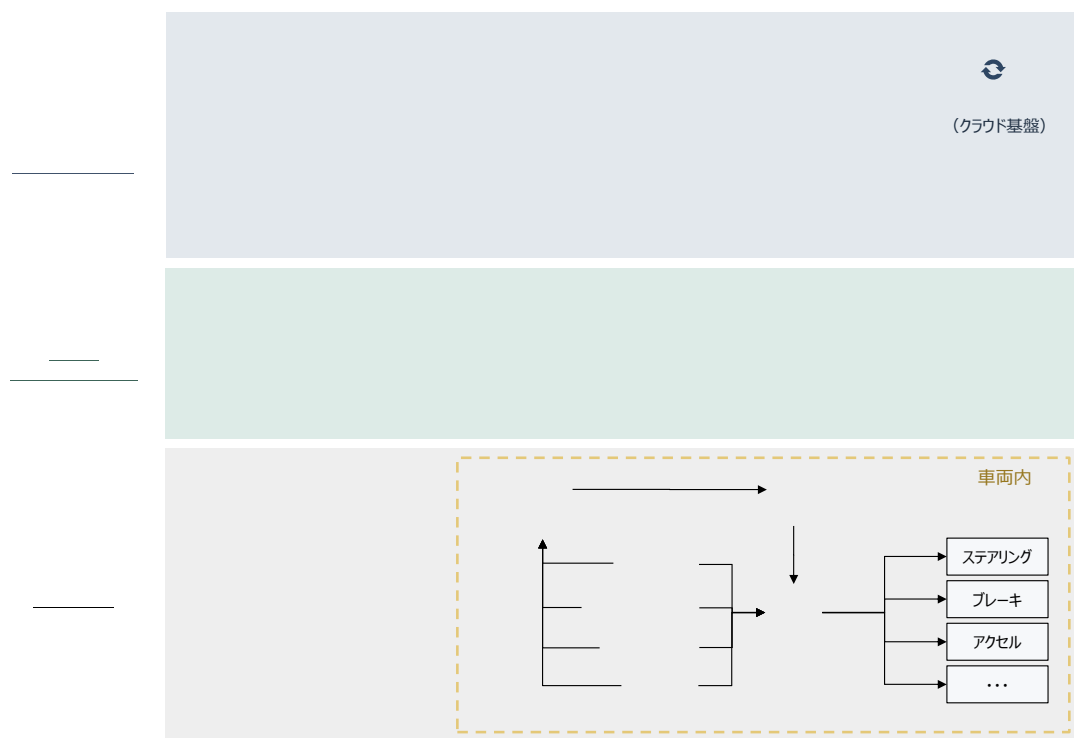


図 3-4 スーパーシティ(自動車)のアーキテクチャ例(昨年度報告書より)

サービスやデータはそれぞれの用途によって異なり、物理的なセンサーや機器もまたそれぞれの用途に応じた機能を持ったものが必要である。ただし、高度に相互連携したサービスを考えるためには、システムやシステムインフラの観点でみて、例えばデータをやり取りするためのプロトコルをあわせる、同じ

処理を分散されたリソースの中で同じように処理できるようにする（極短時間での反応が必要な場合はなるべく近くで処理をし、巨大な処理が必要な場合は多くのリソースをつなぎあわせて処理をする等）、自動車など物理的な移動にあわせて処理も移動出来るようにするなどにも要求に答えなければならない。

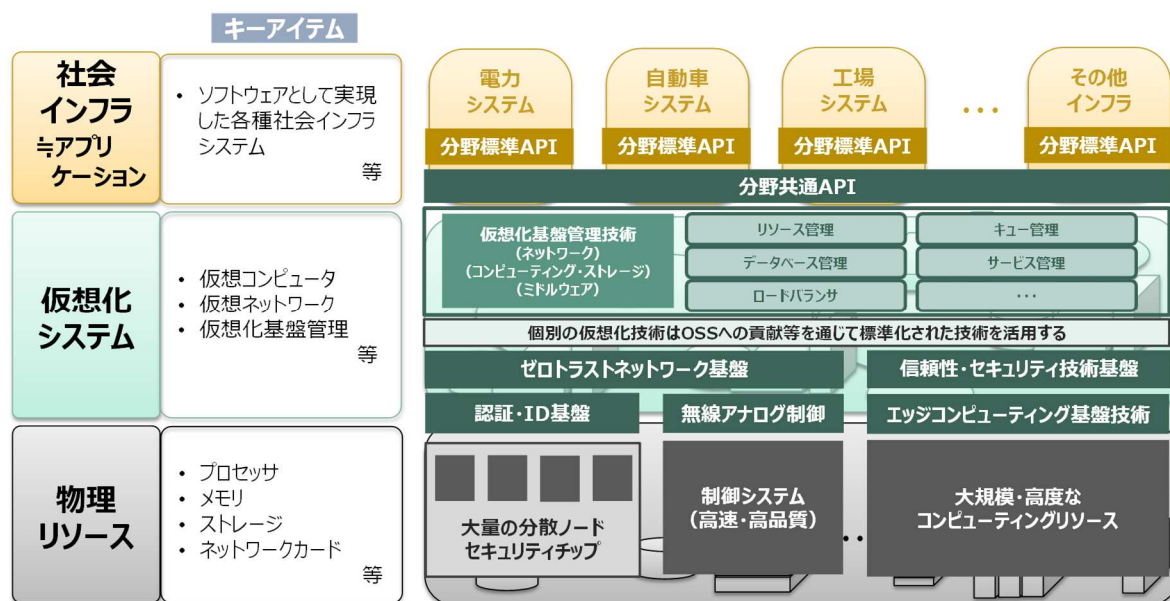


図 3-5 基盤インフラ技術研究開発のスコープ(昨年度報告書より)

上図のようなシステムアーキテクチャの観点で捉えれば、様々なアプリケーションからの要求に答えるには、この中間層の仮想化システムの部分が重要であり、この部分を実現する各要素技術、要素ミドルウェアを世界的な技術の開発傾向を踏まえつつ、我が国として如何に要点部分を確保していくかが大きな課題となっている。

3.1.2 基盤インフラ実現に向けた政策動向

前節で述べたアーキテクチャ上の重要要素技術を押さえるという観点で、我が国として必要な基盤インフラ技術を確保するために求められる国内政策についての検討を実施した。

これらはデジタルアーキテクチャ、基盤ソフトウェア、デジタル産業基盤、ガバメントクラウド等の形で既にいくつかの国のプロジェクトとして取組が始まっている。半導体産業の活性化やグローバルファウンドリ企業の誘致などもその1つと言えるが、経済産業省でも「分散処理技術を用いたデータ活用基盤」として、検討課題に示すなどしている。

分散処理技術等を核とするデータ活用促進基盤構築の方向性

- **低遅延性・低消費電力を実現し、多様性を確保しつつデータ相互利活用を円滑にするデータ活用促進基盤について、これを利用する具体的なサービスの開発主体を巻き込みながら、2020年代半ばの社会実装を目指し、技術開発の支援やルール・標準の整備を行っていく。**

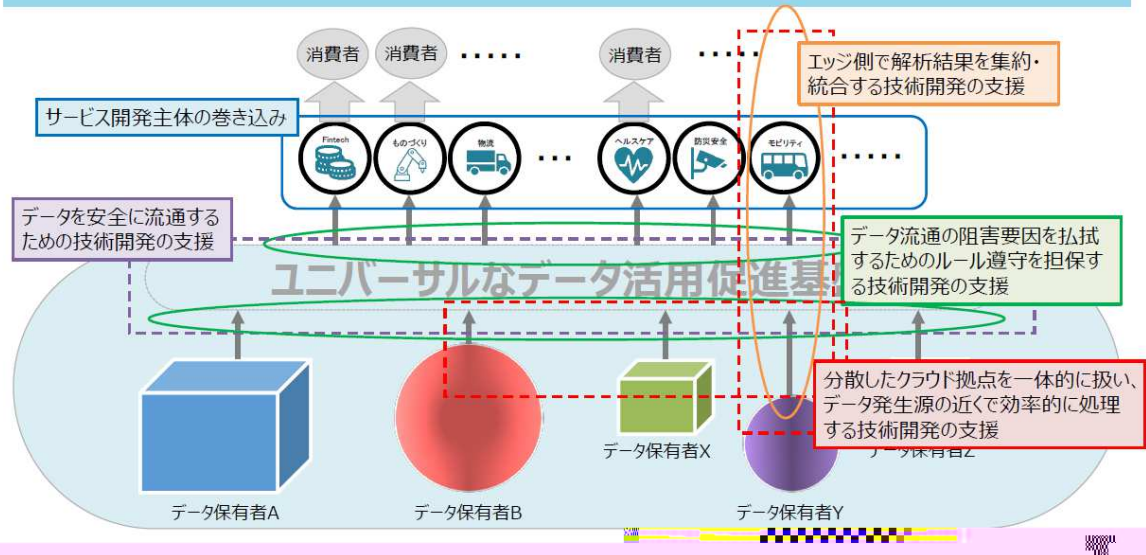


図 3-6 分散処理技術を用いたデータ活用基盤のイメージ(半導体・デジタル産業戦略検討会議資料より)

さらにこの課題設定の背景として、「超分散処理による低遅延化・低消費電力化」、「データ相互利活用ルールの実装」、「エッジ側におけるデータ連携促進」、「ユニバーサルなデータ活用促進」というサブテーマも掲げられており、従来基盤インフラとして必要であると検討してきた要素を巧みに盛り込んでおり、政策として具体的な検討に向かうことを示している。

ただし、あくまで概念のレベルであり、具体的に日本として何処までを確保するのか、要素技術としての確保なのか、実際に基盤を構築し、信頼性の高い社会インフラの基盤としての利用を目指すのか、その辺は今後とも各国動向、社会情勢、有識者等の知見をもとに見極めていくことが大事である。

(参考 1) 超分散処理による低遅延化・低消費電力化

- キャリアネットワークと計算リソースの協調動作により、分散したデータセンターを一体的に扱い、各リソースの負荷状態を踏まえつつ、データ発生源の場所に近いコンピュータで効率的に処理（超分散処理）を行うよう制御することで、低遅延化の実現と低消費電力化を図る。

従来の集中型クラウドアーキテクチャ

✓ 中央のクラウド拠点に通信が集中
✓ 秒単位の実現性の実現に限定

超分散クラウドアーキテクチャ

○ DC
● エッジサーバー等
○ 一休運用可能な範囲

✓ 分散したクラウド拠点を一体的に扱い、データ発生源の近くで処理を行うよう制御
✓ 通信距離は最小限に抑制
✓ より低遅延性が要求されるサービスへの適用が可能

38

(参考 2) データ相互利活用ルールの実装

- デジタル庁においては、データ流通の阻害要因の分析とそれを払拭するためのルールの検討が行われている。こうしたルールの遵守を担保する技術を開発し、社会実装していくことで、データ相互利活用が更に進展していくことが期待される。

データ流通の阻害要因

1. 提供先での目的外利用（流用）
2. 知見等の漏えいへの懸念
3. パーソナルデータの適切な取り扱いへの不安
4. 提供データについての関係者の利害・関心が不明
5. 対価還元機会への関心の低下
6. 取引の相手方のデータ管理への不安
7. 公正な取引市場の不在
8. 自身のデータが買収されることによる影響

データ流通の促進と阻害要因の払拭のためのルール	対応可能な阻害要因	ルールの対象者	
	提供側	利用側	両方
a 提供データについて関係者の利害・関心の把握	4,6		
b 提供データについて関係者の利害・関心の把握の導入	1,2,3,5,6		
c データに関するリスクの軽減	1~8		
d 公正なデータ取引の確保	7		
e データの不正な取得や転売の防止	8		

(出典) 第4回デジタル庁・デジタル庁におけるデータ流通の促進に関する検討会事務局説明資料
2021年10月21日、デジタル庁（資料提供）事務局（事務局）

39

(参考)背景として説明されている各要素(半導体・デジタル産業戦略検討会議資料より)

3.1.3 基盤インフラを構成する基盤ソフトウェアの課題

国として基盤環境を多方面の視点からとらえてその推進を目指すことの他に、ソフトウェア部分に着目し、基盤ソフトウェアとして課題を整理し、その解決を目指す動きも存在している。(独)情報処理推進機構は現在、基盤ソフトウェアの技術動向を整理しようと始めている。その定義では、システム及びソフトウェアの設計、開発、運用、検証等のプロセスにおいて、汎用的に用いられるソフトウェアとして、3つの要件を挙げている。

- システム及びソフトウェア(サービス)の設計、開発、運用、検証等のエンジニアリングプロセスを支援するプラットフォームであり、高度なエンジニアリング手法またはプログラミング手法を適用することを可能とするもの
-

いう形で、有識者の意見収集が行われることになった。その概要は以下の通りです。

開催方式： 持ち回り会合（メールによる資料配布と意見収集）

開催時期： 2022 年 3 月

委員構成： 前回同様の委員構成で開催

主な議案：

- 前回の議論を踏まえ、半年を経て、さらに現状の世の中の動向を踏まえ、どの部分の検討や開発に注力するべきか。

4. 総括

諸外国の法制度の調査に関しては、昨今のランサムウェア攻撃の増加にともなって、各国とも身代金への対策など制度的な対策を強化している状況がわかった。また、中小企業向けのサイバーセキュリティ対策や支援策も体系的な取り組みを行っている状況が明らかになった。一方でサイバー保険は民間の取組が中心で、一部では業界団体が基準作りをするなどの動きもみられるが、国レベルでの支援はほとんど見つけることができなかった。

基盤インフラについては、様々なアプリケーションがソフトウェア化していく中で、基盤インフラ部分が重要であるとして、国を中心にいくつかの取組が進みつつある状況がわかった。一方で全体的な戦略を踏まえた中での強弱をつけた対策も必要であり、有識者等からの意見収集を実施し、次の検討に生かすこととしている。

令和3年度サイバー・フィジカル・セキュリティ対策促進事業
(サイバーセキュリティ法制度の国際動向等に関する調査) 報告書

2022 年 3 月

株式会社三菱総合研究所
デジタル・イノベーション本部
TEL (03)6858-3637

別紙 1

現代のサイバーセキュリティの法的課題についての国際的な研究に関する調査

第 1 部 2021 年度におけるランサムウェア対応の進展

1 アメリカにおけるランサムウェア対応の進展

2021 年 4 月以降のランサムウェア事案に対する米国における対応¹について、以下では、①コロニアルパイプライン事件の概要、②同事件に関するクラスアクション、③連邦運輸保安庁によるサイバーセキュリティ対策に関する法的規制、④サイバーインシデント通知法に関する問題と進展、⑤バイデン大統領による「重要インフラの制御システムのサイバーセキュリティ向上に関する国家安全保障覚書」、⑥サイバー防衛を担う共同サイバー防衛連携の創設、⑦ホワイトハウス Ongoing Public U.S. Efforts to Counter Ransomware、⑧2022 会計年度国防授權法におけるランサムウェアに関する直接規定、⑨StopRansomware.gov の構築と注目すべき内容、⑩OAFIC の新ガイドライン、⑪その他の米国の動向、の順に説明する。

1.1 コロニアルパイプライン事件を契機としたランサムウェア対応の動き

1.1.1 コロニアルパイプライン事件の概要

(1) はじめに

2021 年 5 月 7 日、米国のコロニアルパイプライン社は、標的型ランサムウェア（身代金要求ウイルス）攻撃を受け、その操業が停止する事態に陥った。同社は、米国の東海岸で消費されるディーゼル、ガソリン及びジェット燃料の 45%を供給してきたことから、ガソリンの供給が滞ったり、価格が上昇したりするなどの被害が生じた。この事件は、ランサムウェア攻撃の結果、情報システムのみならず産業制御システムが停止したことで、大きな社会的影響が生じた点に特徴がある。なお、後の連邦捜査局（FBI）の捜査により、この標的型ランサムウェア攻撃を行った犯罪集団は、ロシアのダークサイド(Darkside)が提供する RaaS (Ransomware as a Service)（後述）を用いて攻撃を行ったことが判明している。

このランサムウェア攻撃を受け、同社のジョセフ・ブラウント最高経営責任者は、ガソリン供給等の再開を最優先させる決断を下し、暗号資産のビットコインにより 440 万ドルを犯罪集団に支払っている。なお、同社の過去 5 年間ににおける IT 投資額は 2 億ドルを超えていることから、サイバーセキュリティに関する投資がないがしろにされていたわけではない。

コロニアルパイプライン社に対するランサムウェア攻撃に関する事実関係については、報道された事実よりも、連邦議会上下院で行われた 3 回にわたる公聴会における証言の方

¹ 本報告書では、刑事関連の法令や判例については検討の対象外とした。このため、代表的なランサムウェア事案であるコロニアルパイプライン事件に関しても扱わない。See Department of Justice, Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 7, 2021).

が、法的争点にかかわる事実がよく分かる。このため、以下では、これらの公聴会における証言を再構成して、事実関係を説明する。

この3回にわたる公聴会とは、①最初のものが、2021年6月8日に連邦議会上院国土安全保障政府問題委員会で行われた「重要インフラに対する脅威—コロニアルパイプライン社に対するサイバー攻撃の検証」公聴会であり、コロニアルパイプライン社のジョセフ・ブラウント最高経営責任者が証人となって行われたものであり²、②第2の公聴会は、2021年6月9日に連邦議会下院国土安全保障委員会で行われた「パイプラインにおけるサイバー脅威—コロニアルパイプライン社へのランサムウェア攻撃の教訓に基づく重要インフラの今後の防御」であり、コロニアルパイプライン社のジョセフ・ブラウント最高経営責任者とファイアアイ・マンディアント社（以下、「マンディアント社」）のチャールズ・カーマカル上級副社長兼最高技術責任者が証人となって行われたもので³、③第3の公聴会は、2021年6月15日に連邦議会下院国土安全保障委員会・サイバーセキュリティ重要インフラ保護改革小委員会・運輸海上安全保障小委員会による合同公聴会で行われた「パイプライン事業におけるサイバー脅威—コロニアルパイプライン社に対するランサムウェア攻撃に関する連邦行政機関による対応に基づく教訓」であり、ソニア・プロクター連邦運輸庁石油施設操業担当補佐官とエリック・ゴールドステインサイバーセキュリティ・インフラ保全庁（CISA）サイバーセキュリティ担当長官上級補佐官が証人となって実施されたものである⁴。

（2）ランサムウェア攻撃と捜査上の問題点

ここでは、コロニアルパイプライン社事件の説明に入る前に、ランサムウェア攻撃とは何かについて、簡単に説明することにする。なお、この説明は、米国司法省のリチャード・ダウニング刑事局担当司法副次官補が、2021年7月27日に連邦議会上院司法委員会による公聴会に提出した証言書に基づいている⁵。

まず、ランサムウェアとは、サイバー犯罪者が、コンピュータシステムの所有者を脅迫するために用いる悪意のあるソフトウェア（マルウェア）のことである。犯罪者は、このマルウェアにより、被害者のコンピュータ上のファイルを暗号化してアクセスができないようにした上で、もしもファイルを元に戻す復号化のためのキーが欲しければ、身代金を支払うように画面上の表示を掲示するという方法をとっている。また、一部の犯罪者は、もしも身

² *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs* (June 8, 2021) (Statement of Joseph A. Blount, JR., President and Chief Executive Officer, Colonial Pipeline).

³ *Cyber Threats in the Pipeline: Using Lessons from the Colonial Ransomware Attack to Defend Critical Infrastructure: Hearing Before the H. Comm. on Homeland Sec.* (June 9, 2021) (Statement of Joseph Blount, CEO, Colonial Pipeline & Charles Carmakal, SVP & CTO, FireEye Mandiant).

⁴ *Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack: Before the H. Comm. on Homeland Sec., Subcomm. on Cybersecurity, Infrastructure Protection & Innovation, & Subcomm. on Transportation & Maritime Security* (June 15, 2021) (Statement of Sonya Proctor, Assistant Adm' for Surface Operations, Transp. Sec. Admin. (TSA), U.S. Dep't of Homeland Sec. & Eric Goldstein, Exec. Assistant Dir. for Cybersecurity, Cybersecurity and Infrastructure Sec. Agency (CISA), U.S. Dep't of Homeland Sec.).

⁵ *See America Under Cyber Siege: Preventing and Responding to Ransomware Attacks: Before the S. Comm. on Judiciary* (July 27, 2021) (Statement of Richard Downing, Deputy Assistant Attorney Gen., Criminal Div., Dep't of Justice).

代金を支払わなければ、被害者のコンピュータから盗んだ機微な情報をインターネット上に公開するという脅迫方法を合わせて用いることがある。

サイバー犯罪者は、法執行機関による捜査を困難にするために、①ネットワークトラフィックを暗号化して個人が特定されない Tor ネットワークを用いて、ランサムウェア攻撃を受けた企業と連絡をとったり、盗んだ情報を公開したりする一方で、②ビットコインやモネロといった暗号通貨を身代金の支払いに用い、さらに、一部の犯罪者は、秘匿されたブロックチェーンを用いた暗号通貨、通称「匿名性強化通貨 (anonymity enhanced currencies)」を利用して、追跡困難性と秘匿性を高めている。

また、ランサムウェアを用いたビジネスモデルも進化を遂げ、①多くのランサムウェア開発者は、自らが開発したランサムウェアを提携する攻撃者にライセンス供与して、その利用料金を取るという RaaS (ransomware-as-a-service) という手法を採用するとともに、②攻撃者は、事前に適切な攻撃対象者を選別するために、攻撃対象となる企業の資産、攻撃により事業が停止した場合に被る被害予想額、サイバー保険契約の填補限度額等を調査した上で攻撃を行うようになっている。

捜査機関にとって、ウェア攻撃の捜査が困難であるのは、①米国以外から行われる国際犯罪であり、しかも、利用されるサーバーが多数の国家に分散されていることから、多くの外国捜査機関の協力が必要であり、②攻撃者が、ロシアのような犯罪人引渡しに協力的でない国家の場合には、被疑者が国外に旅行したときに逮捕するといった手間を要することになり、③攻撃者が、米国内でメールアカウント等の管理が杜撰な企業を意図的に利用していることから、アカウントが違法に保存されていない等の事情により、捜査令状や保全命令が意味をなさない事態が生じるためである。

(3) コロニアルパイプライン社に対するランサムウェア攻撃

コロニアルパイプライン社に対するランサムウェアによる攻撃は、2021 年 5 月 7 日の米国東部標準時間の午前 5 時前に、同社の従業員が、IT ネットワーク上に身代金要求の表示を発見したことから判明した。その後、コントロールセンターの制御責任者 (Operations Supervisor) が、全パイプラインの稼働を停止するための業務停止命令を発令した。この措置は、制御技術ネットワークへの攻撃を止めるためのものであった。これに続いて、同社の従業員が、同日午前 5 時 55 分頃から、シャットダウンプロセスを開始し、午前 6 時 10 分までに全長 5,500 マイルのパイプラインが停止している。

その後、全パイプラインに対して常時地上監視 (constant ground surveillance) を実施し、いかなる物理的ダメージもないことを確認している。また、手動による操作ができる高齢の従業員により、いくつかの地域のパイプラインを復旧させた。

この事故対応手続は、訓練どおりにうまく機能したと評価されている。ただし、この手続には、ランサムウェア攻撃への対応が含まれていなかったことが問題点として指摘されている。

(4) マンディアント社への対応を依頼

サイバーセキュリティ企業として著名なマンディアント社は、コロニアルパイプライン社の顧問弁護士事務所である Hunton Andrews Kurth LLP から、2021 年 5 月 7 日の早朝に依頼を受け、本件への対応に参画することになった。なお、マンディアント社は、本件依頼を受けるまで、コロニアルパイプライン社に、サイバーセキュリティに関するコンサルティングサービスを提供したことはない。

コロニアルパイプライン社は、その後、マンディアント社に加え、Dragos 社（OT システム関連）と Black Hills 社（全体のプロセス関連）にも、コンサルタントとしての対処を依頼している。

(5) ランサムウェア攻撃を許した原因

マンディアント社によると、攻撃者による最初のシステムへの侵入は、2021 年 4 月 29 日に起きている。攻撃者は、コロニアルパイプライン社のバーチャルプライベートネットワーク（VPN）に、現在は使用されていない VPN プロファイルと、従業員のユーザーネーム及びパスワード（簡易なものではない）を使ってログインしている。この VPN プロファイルでは、ワンタイムパスワードの使用が要求されていなかった（多要素認証なし）。攻撃者は、おそらく、これらの認証情報を、他の HP 等で入手したものと推定されている。その後、同 VPN プロファイルは、コロニアルパイプライン社の復旧過程で、マンディアント社により無効化されている。

なお、コロニアルパイプライン社は、これまで定期的にペネトレーションテストや監査を行ってきたものの、今回問題となった VPN については、これまでの pin testing では発見できなかったと証言している。

(6) FBI 等の連邦政府機関への連絡

コロニアルパイプライン社は、本ランサムウェア攻撃のあった 5 月 7 日の朝に、連邦捜査局（FBI）アトランタ事務所に対して、本件攻撃の発生から数時間以内に連絡をしている。

今回の事件で明らかになったことは、報告しなければならない行政機関が非常に多いということである。コロニアルパイプライン社は、ランサムウェア攻撃を受けてからホワイトハウス、国家安全保障会議（NSC）、エネルギー省（主務官庁）、国土安全保障省、FBI、サイバーセキュリティ・インフラ保全庁（CISA）等の合計 10 の連邦行政機関等に連絡をとっている。ブラウント最高経営責任者は、公聴会において、将来的には、1 つのコンタクトポイントで連邦行政機関への連絡が済むような制度ができればありがたいとの見解を述べている。

また、コロニアルパイプライン社は、同社が加入している米国石油協会（American Petroleum Institute）と石油パイプライン協会（Association of Oil Pipe Lines）に対しても連絡をとって情報共有を行い、ランサムウェア攻撃についての注意喚起を行っている。

(7) 攻撃者への身代金の支払いについて

コロニアルパイプライン社は、攻撃者からの身代金の要求に対して、2021 年 5 月 7 日に、

交渉の上で支払うことを決定している。ブラウント最高経営責任者は、この身代金を支払う理由として、①ガソリンの供給が滞れば、救急車等の緊急車両が動かなくなるといった緊急事態が生じることから早期の復旧が最重要であり、②IT ネットワークシステムのバックアップに基づく復旧は時間を要することから、最も早期に復旧できる身代金の支払いを選択したと述べている。

また、同最高経営責任者は、身代金の支払いを「個人の判断」で行ったことを強調している。その理由は、第三者（マンディアント社や顧問弁護士事務所等）が身代金の支払いを勧めた等の事実があると、後述するように、財務省外国資産管理局（OFAC）の勧告に基づき、これらの第三者にも責任が及ぶ可能性があるためである。なお、コロニアルパイプライン社の法務部門は、5月7日に、財務省外国資産管理局に連絡をとり、ダークサイドが同局の規制対象リストに含まれていないことを確認している。

コロニアルパイプライン社が、身代金を支払った事実を最初に報告した連邦行政機関はFBIであり、その報告は、支払いが行われた5月8日から約48時間以内に行われたと証言されている。また、具体的な支払いに関する報告がなされる以前の5月9日に、身代金の支払いに利用されるDigital Walletに関する情報をFBIと共有したと証言されている。

コロニアルパイプライン社による身代金の支払いがなされたのは5月8日であるが、制御技術ネットワークが完全に復旧し、すべてのパイプラインを稼働させることができたのは、5月12日の夕方であった。

（8）サイバー保険による担保と身代金の支払いに関する連邦租税控除

ブラウント最高経営責任者は、公聴会において議員から身代金の支払いにあたって、同社が加入しているサイバー保険による保険金の支払いを考慮したか否かを問われている。同氏は、この質問に対して、社内の最高財務責任者が、加入しているサイバー保険により身代金の支払いがカバーされるかどうかを検討したことはあったかもしれないが、同氏自身は、パイプラインを早期に復旧させることを最優先に考えていたことから、保険金については考慮の対象としていなかったと証言している。

また、公聴会で、身代金の支払いに関して連邦租税控除が可能であるが、その申請をする予定があるのかどうかを問われ、その控除については全く気がついていなかったと答えている。なお、内国歳入庁（IRS）は、この点について何の指針も出していないものの、2017年に、この問題に関する論文⁶が発表されてから、「通常必要な経費（ordinary and necessary expenses）」（26 U.S.C. § 162(a)）としての控除が認められているという。

1.1.2 コロニアルパイプライン事件に関するクラスアクション

ここでは、最初に、IT ネットワークシステムへのランサムウェア攻撃により生じた個人情報漏えい事件について提起されたクラスアクションに関する判例法理を概説する。この類型の判例においては、個人情報の漏えいに伴って事実上の損害（injury in fact）が生じたか

⁶ Donald T. Williamson & A. Blair Staley, *Ransomware: Tax Compliance Issues for a New Reality*, 58-12 TAX MGMT MEM. 281 (2017).

否かが、原告適格の有無を判断する上で主たる争点になる。

これに対して、コロニアルパイプライン社事件に関して提起された2つのクラスアクションでは、パイプラインの機能をコントロールしている制御技術ネットワークが停止したことにより、ガソリンの供給が滞ったり、価格が上昇したりするなどの事実上の損害が生じている。これが、ここに紹介する2つのクラスアクションが注目されている理由である。

(1) ランサムウェア攻撃により提起されたクラスアクションにおいて原告適格を満たすための事実上の損害の有無

ランサムウェア攻撃に関係して提起されたクラスアクションの多くは、通常のサイバーインシデントにより個人情報情報が漏えいした事件と同様に、複数の被害者代表が、①過失 (negligence)、②法律上当然の過失 (negligence per se)、③契約違反 (breach of contract) 又は黙示的契約違反 (breach of implied contract)、④信任義務違反 (breach of fiduciary duty)、⑤不当利得 (unjust enrichment)、⑥プライバシー関連の州法等に基づいて提起する訴訟である。また、これらの訴訟において争点になるのは、原告は、主張している情報漏えい等により、果たして具体的な損害を被ったのか否か、又は、そのような損害を被る高い蓋然性 (急迫する損害) があるのか否かである。原告は、この民事訴訟法上の原告適格の要件を満たすために、(1)なりすまし (identity theft) 被害に関するリスクの増加、(2)自らの個人情報になりすましにより悪用されていないかどうかをチェックするサービス (credit monitoring service) の利用費用、(3)自らの個人情報の価値の低下 (医療機関に対するランサムウェア攻撃で自らの健康情報が漏出したことで、犯人がこれを闇市場で 50 ドル以上の金額で販売する事例があることから、その分、自分の個人情報の価値が低下したと主張する理論であるが、どの法域でも認められていない)、(4)ランサムウェア攻撃により被害を受けた企業に対して、元々支払った対価の中にデータセキュリティのための費用が含まれていたにもかかわらず、これが有効に機能しなかったことから、対価の過払い分を損害として主張する理論に基づく損害 (どの法域でも認められていない)、(5)精神的損害等が主張されるものの、ほとんどの事件においては、事実上の損害 (injury in fact) が立証されていないとして、その訴えが却下されている⁷。多くの法域では、原告による原告適格要件を満たすための損害に関する個別の主張について、先例に基づいて、それぞれの主張を否定していく判例が多い。

(2) コロニアルパイプライン社事案に関する最初のクラスアクション

コロニアルパイプライン社事件に関する最初のクラスアクションは、コロニアルパイプライン社の所有者が合理的なセキュリティ手段等を取らなかったという過失により、ランサムウェアによる被害を受けたことに起因して、ガソリン価格が高騰し、消費者が高額のガソリンを購入しなければならなかったことによる損害を被ったとして、2021 年 5 月 18 日に提起されたものである⁸。

⁷ See e.g., *Travis v. Assured Imaging LLC*, 2021 U.S. Dist. LEXIS 89129 (May 10, 2021); *Abernathy v. Brandywine Urology Consultants, P.A.*, 2021 Del. Super. LEXIS 46 (Jan. 21, 2021).

⁸ *Dickerson v. CDCP Colonial Partners, L.P.*, Case No. 1:21-cv-02098 (N.D. Ga.).

本件の訴状は公開されているものの、2022 年 2 月末時点で判決は下されていない。この訴訟の争点としては、①コロニアルパイプライン社は、通常のシステム監査等を受けていたものの、マンディアント社でなければ発見できなかった未使用の VPN に、多要素認証を使っていなかったことを過失と評価できるのか否か、②同社は、コンピュータシステム上の問題が生じた状態においても、手動で通常通り操業できなかったことについて、過失があると評価されるのか否か、③同社は、契約上、最終的な消費者に対して責任を負っているのか、④原告が求めているクラス認定（2021 年 5 月 7 日以降に、被告の行為により高いガソリン価格を支払ったすべての法人及び自然人）につき、自ら高値でガソリンを買いだめした消費者も相当いたことなどから、十分な因果関係が認められるかどうか等が問題になると考えられている。

(3) コロニアルパイプライン社事案に関する第 2 のクラスアクション

第 2 のクラスアクションは、コロニアルパイプライン社の所有者が合理的なセキュリティ手段等を取らなかったという過失により、1 万 1000 件を超えるガソリンスタンド所有者等が、ガソリン供給の不足から、高値のガソリンを購入する等の費用や、販売額が減った等の営業損失を被ったとして、2021 年 6 月 21 日にクラスアクションを提起したものである⁹。

このクラスアクションも、訴状が公開されているだけで、2022 年 2 月末時点で判決は下されていない。本件では、事業者が原告であることから、最初のクラスアクションよりも、損害や因果関係の立証が認められる可能性がある。争点は、①最初のクラスアクションと同様に過失の評価等と、②おそらくガソリンの供給契約には不可抗力条項が入っているので、その適用があるかどうか等であると思われる。

1.1.3 連邦運輸保安庁によるサイバーセキュリティ対策に関する法的規制

(1) パイプライン業界に対するサイバーセキュリティ規制

ア 強制力のない指針と審査

これまで、連邦文民行政機関（国防総省とインテリジェンス機関を除いた連邦行政機関）が発行するサイバーセキュリティ指針等には、規制対象となる重要インフラを運営する民間企業に対して法的拘束力がなかった¹⁰。主務官庁は、セクターごとにサイバーセキュリティに関する指針等を定めて推奨してきたものの、これを遵守するか否かは、民間企業の自主的な判断に委ねられていたのである。

この点については、パイプライン事業者を管轄する連邦運輸保安庁（Transportation Security Administration: TSA）が発行するパイプラインに関するサイバーセキュリティ指針（Transp. Sec. Admin., Pipeline Security Guidelines (Mar. 2018 with Change 1 (April 2021))）についても同様であった。また、TSA が主催するサイバー審査や演習も、民間企業による自主的な参加を促すものであった。

⁹ EZ Mart 1, LLC v. Colonial Pipeline Company, Case No. 1:21-cv-02522 (N.D. Ga.).

¹⁰ See e.g., CISA, Pipeline Cybersecurity Initiative, available at <https://www.cisa.gov/pipeline-cybersecurity-initiative>.

イ 連邦監査院による問題点の指摘

連邦監査院のウィリアム・ラッセル（William Russell）氏が、2019年5月1日に、連邦議会下院エネルギー商業委員会エネルギー小委員会で行った TSA によるパイプラインに関するセキュリティプログラムマネジメントの問題点に関する証言¹¹では、①TSA は、パイプラインに関するサイバーセキュリティ指針に、国立標準技術研究所（NIST）が定めた重要インフラに関するサイバーセキュリティの向上における全ての要素を導入しておらず、これは同指針が定期的に見直されていないことが原因となっており、②TSA のパイプライン監査チームには、サイバーセキュリティに関する専門知識がない等の人員に関する問題があり、さらには、③パイプラインの保全審査に関するリスク評価方法も 2014 年から改訂されていない等の問題があると指摘されている。

また、2021年6月15日に行われた上記の第3回公聴会において、①2018年 TSA 現代化法に基づき、地上オペレーション室が設置されたこと、②2020会計年度に 20 名からなるパイプラインセキュリティ評価チームができ、そのうちの 8 名がサイバーセキュリティの訓練を終えたこと、③サイバーセキュリティ・オペレーション・サポート部門を創設したので、今後 11 名のサイバーセキュリティ専門家を雇用していくこと、④政策室の TSA 地上政策部が、サイバーセキュリティ関連の指針の開発に集中して取り組む予定であり、2021 会計年度が終わるまでに、そのサイバーセキュリティセクションの人員を 9 名に増員すること等の後手後手の実態が明らかにされた。

さらに、連邦監査院のレスリー・ゴードン（Leslie V. Gordon）氏が、連邦議会上院通商科学運輸委員会において、2021年7月27日に行った TSA によるパイプラインセキュリティプログラムにおける問題点に対する対処についての証言¹²では、連邦監査院が、2018 年及び 2019 年に指摘した 15 の問題点のうち、2021 年 6 月の時点で、①TSA はパイプライン事業者に関する脅威、脆弱性等についてリスク評価を行うために必要となる十分な関連データを所持しておらず、②パイプライン事業者のセキュリティインシデントに対応する手順書が 10 年以上も改訂されていない等の問題について、いまだ十分な対応ができていないとの指摘がなされている。

ウ 法的拘束力のある指令の発出

連邦議会からの批判や、連邦監査院からの指摘を受け、TSA の上級行政機関である国土安全保障省（DHS）は、パイプライン事業者に対して、2 段階で、TSA が指定した重要なパイプライン企業に対して、法的拘束力をもつ指令を発出した。この規則制定の根拠は、2007 年 9 月 11 日委員会の勧告実施法（Implementing Recommendations of the 9/11 Commission Act of 2007）第 1557 条「パイプラインの保安検査及び執行（Pipeline Security Inspections and Enforcement）」第(b)項「審査と検査（Review and Inspection）」であり、同項の下で重要であ

¹¹ U.S. Gov't. Accountability Office, GAO-19-542T, Critical Infrastructure Protection: Actions Needed to Address Weaknesses in TSA's Pipeline Security Program Management (May 1, 2019).

¹² Gov't. Accountability Office, GAO-21-105263, Critical Infrastructure Protection: TSA Is Taking Steps to Address Some Pipeline Security Program Weaknesses (July 27, 2021).

る（critical）とみなされた 100 社のパイプラインの所有者・運営者が規制対象とされた。

エ 最初の法的拘束力を持つ指令

DHS は、まず、2021 年 5 月 28 日に、民間のパイプライン事業者に対して、サイバーインシデント等に関して法的拘束力を持つ指令「パイプライン事業者のサイバーセキュリティの向上」（Dep't of Homeland Sec., Enhancing Pipeline Cybersecurity, Security Directive Pipeline-2021-01 (May 28, 2021)）を発出した。その主たる内容は、以下のとおりである。

- 該当する事業の所有者・運営者は、本指令の施行日から7日以内（2021年6月4日まで）に、TSAに対して、サイバーセキュリティ調整担当者（cybersecurity coordinator）及び少なくとも1名の代行者を任命し、その氏名、役職、電話番号及びメールアドレスをTSAに報告すること。なお、サイバーセキュリティ調整担当者は、①セキュリティクリアランスをもつ米国市民でなければならない、②同担当者は、TSAとCISAとの間で、サイバー関連のインテリジェンス情報、サイバーセキュリティ関連の活動及び連絡を主として担う業務を行い、③TSAとCISAに対して週7日・24時間連絡可能でなければならない、④社内におけるサイバー及び関連するセキュリティプラクティスと手続を調整する職務を担い、かつ、⑤適切な法執行機関及び緊急対応を担当する行政機関とともに業務を遂行すると規定されている。
- 該当する事業の所有者・運営者は、自らが運営するシステムにおけるサイバーセキュリティインシデントが特定されてから可能な限り速やかに（少なくとも12時間以内に）、CISAのウェブサイト上の報告システム又はCISAの緊急連絡電話を用いてCISAに報告する義務を負う。もしも、求められているすべての情報が指定されている時間内に報告できない場合には、まず指定時間内に判明している情報のみを報告し、他の情報が判明した場合には補足的に報告を行うものとする。報告されるすべての情報は、その機微性及び重要性に応じて保護され、かつ、公開されることはない。なお、ここに言うサイバーセキュリティインシデントとは、①情報システム又は制御技術システムへの不正アクセス、②情報システム又は制御技術システムにマルウェアが見つかったこと、③情報システム又は制御技術システムへのDoS攻撃、④所有者・運営者のネットワーク・インフラに対する物理的攻撃、⑤その他のサイバーセキュリティインシデントで、システム若しくは施設の運営を妨げるもの、又は、多数の顧客、政府の中核的機能、国家安全保障、経済安全保障等に影響をもたらし、安全で効率的な輸送に支障を引き起こす可能性のある運営を妨げるもの等を意味している。
- 「パイプラインに関するサイバーセキュリティ指針（Transp. Sec. Admin., Pipeline Security Guidelines (Mar. 2018 with Change 1 (April 2021)）」第7条に基づいて当該パイプラインのセキュリティ対策の現状を評価し、あるべき状態とのギャップがあれば特定し、その改善方法と改善計画とを策定して、TSAの定めた評価書式に記載した上で、TSAとCISAに本指令の施行日から30日以内（2021年6月27日まで）に提出すること。

オ 第2の法的拘束力を持つ指令

これに続いて、DHS は、2021 年 7 月 20 日に、第 2 の法的拘束力を持つ指令（Dep't of Homeland Sec., Security Directive Pipeline-2021-02）を発出したとの発表を行った¹³。ただし、この指令そのものは機密指定がなされているため、その内容は公表されていない。

この点につき、コロニアルパイプライン社事件に関する上記の第 3 回公聴会に出席した TSA のソニア・プロクター氏によると、この第 2 指令には、ランサムウェア攻撃等に対する特定の緩和策（specific mitigating measures）等が含まれていることから機密指定されていると証言している。また、2021 年 7 月 27 日に連邦議会上院通商科学運輸委員会で行われた「パイプラインのサイバーセキュリティ重要インフラの保護」に関する公聴会で証言したデイビッド・ペコスキー連邦運輸保安長官によると、この第 2 指令は法的拘束力を持つことから、個々の違反を評価した上で民事罰を課す規定が含まれているという¹⁴。報道によれば、この民事罰は、最新の TSA 執行指針¹⁵に基づき、1 日における 1 項目の違反につき最大で 11,904 ドルが課されることになるという¹⁶。

なお、以下で紹介するバイデン大統領が 2021 年 7 月 28 日に発した「重要インフラの制御システムのサイバーセキュリティ向上に関する国家安全保障覚書」の概況報告書では、この第 2 指令においては、①ランサムウェア攻撃等の脅威から情報技術システムと制御技術システムを保護するために、所定の期限以内に特定された緩和策を実施すること、②サイバーセキュリティ緊急対策及び復旧計画を策定・実施すること、及び、③サイバーセキュリティアーキテクチャデザイン年次審査（annual cybersecurity architecture design review）を実施すること等が規定されているとしている。

（2）鉄道事業者に対するサイバーセキュリティ規制

TSA は、2021 年 12 月 2 日に、①民間の貨物鉄道事業者に対して、サイバーインシデント等に関して法的拘束力を持つ指令「鉄道サイバーセキュリティの向上」（Transp. Sec. Agency, Enhancing Rail Cybersecurity, Security Directive 1580-21-01 (Dec. 2, 2021)）と、②民間の旅客列車事業者に対して、サイバーインシデント等に関して法的拘束力を持つ指令「公共交通及び旅客列車のサイバーセキュリティの向上」（Transp. Sec. Agency, Enhancing Public Transportation and Passenger Railroad Cybersecurity, 1582-21-01 (Dec. 31, 2021)）を発出した（施行は、同年 12 月 31 日）。

その主たる内容は、既に述べた民間のパイプライン事業者に対する最初の指令と類似するものであり、①サイバーセキュリティ調整担当者の任命と届け出、②サイバーセキュリティインシデントが特定されてから 24 時間以内に、所定の事項を CISA に報告すること、③

¹³ Dep't of Homeland Sec., DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (July 20, 2021).

¹⁴ Pipeline Cybersecurity: Protecting Critical Infrastructure: Before S. Comm. on Commerce, Sci., and Transp. (July 27, 2021) (Statement of David Pekoske, Adm'r, Transp. Sec. Admin).

¹⁵ Transp. Sec. Admin., Enforcement Sanction Guidance Policy (updated on Feb. 8, 2021), available at https://www.tsa.gov/sites/default/files/enforcement_sanction_guidance_policy.pdf.

¹⁶ See Christian Vasquez & Blake Sobczak, China hacking threat prompts rare U.S. pipeline warning, E & E News, Energy Wire (June 21, 2021).

サイバーセキュリティインシデント対応計画を、他に指定がない限り、当該指令の施行から 180 日以内に策定し、TSA に承認を得ること、及び、④サイバーセキュリティ脆弱性評価と対策を当該指令の施行から 90 日以内に所定の書式に基づいて策定し、TSA に承認を得ること等の義務が課されている。

1.2 2021 年におけるランサムウェア対応の法と政策

1.2.1 サイバーインシデント通知法に関する問題と進展

これまで、民間企業に対して、ランサムウェア攻撃等によるサイバーインシデントについて、連邦行政機関に報告義務を課す一般法は存在していなかった。しかしながら、連邦議会において、コロニアルパイプライン事件等を受けて、重要インフラを運営する企業を中心に、民間企業に対してランサムウェア被害等について、広く一般的な通知義務を課すべきだという考えが広まり、複数の法案が提出された。これは、民間企業によるサイバーインシデントに関する通知がなければ、 は対応できず、また、 等の捜査機関も刑事捜査を開始することができないためである。

以下では、①連邦行政機関や、重要インフラを運営する民間企業等がランサムウェア攻撃等を受けた場合に、その通知義務を定めた既存のサイバーインシデント通知法、②コロニアルパイプライン事件を受けて、最初に本格的に民間企業によるサイバーインシデントに関する通知義務を課すことを目指した「2021年サイバーインシデント通知法案」の概要、③民間企業によるサイバーインシデント通知に関するその後の立法動向の順に概説する。

(1) 既存のサイバーインシデント通知法

ここでは、サイバーインシデントが起きた場合に、連邦行政機関に対して通知義務を課している既存の代表的な立法等につき、①連邦行政機関に対してサイバーインシデントの通知義務を定めたもの、②重要インフラ運営事業者に対してサイバーインシデントの通知義務を定めたもの、という順番で概説する。なお、②については、既に説明したパイプライン事業者と鉄道事業者に対する通知義務を定めた規則は割愛することにする。

ア 連邦行政機関に対してサイバーインシデントに関する通知義務を定めたもの

まず、2002 年連邦情報セキュリティ・マネジメント法（Federal Information Security Management Act of 2002: FISMA）¹⁷において、連邦行政機関でサイバーインシデントが起きた場合には、当該行政機関は、連邦法執行機関、監察総監室及び指定された連邦行政機関に通知する義務を定めている¹⁸。そして、FISMA の委任に基づいて CISA が発出した「連邦インシデント通知ガイドライン」（US-CERT Federal Incident Notification Guidelines, Apr.1, 2017）に具体的な規定が置かれ、連邦文民行政機関の連邦情報システムにおける機密性・完全性・可用性に危殆化が生じた場合には、当該情報セキュリティインシデントについて、必要な報

¹⁷ Federal Information Security Management Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (2002) (codified as amended in scattered sections of 44 U.S.C., 40 U.S.C., and 15 U.S.C.).

¹⁸ See 44 U.S.C. § 3554(b).

告要件とともに、CISA/US コンピュータ緊急対応チームに1時間以内に報告しなければならないこと等を定めている。

また、FISMAでは、連邦行政機関が「重大なインシデント (major incidents)」¹⁹に遭遇した場合には、当該インシデントが起きたと合理的に結論付けられるようになった日から7日以内に、又、当該インシデントに関するより詳細な内容を合理的な期間内に、連邦議会の関連する委員会に報告しなければならないと規定されている²⁰。

イ 民間企業に対してサイバーインシデントに関する通知義務を定めたもの

まず、大規模電力システムについては、連邦エネルギー規制委員会の定める規則「サイバーセキュリティインシデント報告信頼性基準」に基づき、重大なインシデントについては、電力 ISAC (Electricity Information Sharing and Analysis Center) に1時間以内に報告しなければならないとの規制が課されている²¹。

また、原子力発電システムに関するサイバーセキュリティ事案については、原子力規制委員会規則に基づき、緊急通知システム (Emergency Notification System) を通じて原子力規制委員会本部オペレーションセンター (NRC Headquarters Operations Center) に、①重大な損害をもたらす攻撃が起きた場合には、1時間以内に、②重大な損害をもたらす可能性のあった攻撃又はその未遂が判明した場合には、4時間以内に、③サイバー攻撃の準備行為が判明した場合には、8時間以内に報告する義務が課されている²²。なお、原子力規制委員会は、2022年3月4日に公聴会を開催して、原子炉サイバーセキュリティプログラム (Cyber Security Programs for Nuclear Power Reactors) 案を公表し²³、同年5月2日を期限としてパブリックコメントを募集するとの決定を下しているが、上述した通知義務と報告内容に関する変更はない²⁴。

次に、国防総省における請負人 (下請負人含む) については、国防総省調達規則補遺 (DFARS) に基づき、サイバーインシデントの発見から72時間以内に「迅速な報告」を行わなければならないと定められている²⁵。国防総省に物やサービスを提供する企業の類型は広く (我が国で、在日米軍基地をサポートする業務を行っている企業も含む)、かつ、下請負人も含むことから、72時間という時間設定がされていると考えられる。

そして、最後に、コロニアルパイプライン事件が盛んに議論された後に成立した連邦法上の規制を受ける銀行業に関するサイバーインシデントの通知についての規則を見ておき

¹⁹ ここでいう重大なインシデント (major incident) とは、国家安全保障上の利益、外交関係若しくは米国の経済、又は、米国市民の公的信頼、市民的自由若しくは公共の安全に対して、明白な損害 (demonstrable harm) がもたらされうる損害であると定義されている。See Off. of Mgmt. & Budget, Exec. Off. of the President, M-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements 5 (Oct. 16, 2017).

²⁰ 44 U.S.C. § 3554(b)(7)(C)(iii)(III).

²¹ See Cyber Security Incident Reporting Reliability Standards, 83 Fed. Reg. 36,727, 36,727 (July 31, 2018) (to be codified at 18 C.F.R. pt. 40).

²² NRC Cyber Security Event Notifications, 10 C.F.R. § 73.77(a)(3) (2016).

²³ U.S. Nuclear Reg. Comm'n, Cyber Security Programs for Nuclear Power Reactors, Draft Reg. Guide DG-5061, Rev.1, Proposed Rev. 1 to Reg. Guide 5.71 (Feb. 2022).

²⁴ See *id.* at C.3.3.2.6 Incident Response at 34.

²⁵ DFARS 252-204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting (Aug. 2015).

連邦行政機関又は規制対象者は、サイバーセキュリティ侵害又は潜在的サイバーセキュリティ侵害を確認してから 24 時間が経過する前に、「サイバー侵害報告受付組織 (Cyber Intrusion Reporting Capabilities)」(後述)を通じて、CISA に対し、サイバーセキュリティ通知を提出しなければならない。但し、連邦行政機関又は規制対象者が、他の連邦法、規則、指針又は連邦政府契約において、連邦行政機関にサイバーセキュリティ侵害又は潜在的サイバーセキュリティ侵害を 24 時間未満の期限で通知する義務を負う場合には、当該通知期限の要件は、本法においても適用される。

連邦行政機関又は規制対象者は、上記のサイバーセキュリティ通知を提出した後、サイバーセキュリティインシデントが緩和される以前、又は、追加調査が完了する以前の段階で、新たな情報が発見されてから 72 時間が経過するまでに、更新されたサイバーセキュリティ脅威情報を、サイバー侵害報告受付組織を通じて CISA に提出しなければならない。

サイバーセキュリティ通知に含まれる「サイバーセキュリティ脅威情報」の内容は、CISA 長官(国土安全保障長官を代理)が、国家情報長官、連邦行政管理予算局(OMB)長、国防長官及び国家サイバー責任者(National Cyber Director)と協力して策定し、本法が施行されてから 270 日が経過するまでに制定される暫定最終規則において規定されなければならない。

なお、この暫定最終規則におけるサイバーセキュリティ脅威情報には、少なくとも、①サイバーセキュリティ侵害に関する記述、②サイバー行為者が当該侵害を行ったときに利用した脆弱性、用いた戦術、技術及び手段(procedure)に関する記述、③当該サイバー行為者を合理的に特定するために寄与しうる情報(IPアドレス、DNS情報又はマルウェアのサンプル等)、④規制対象者の連絡先に関する情報(電話番号、メールアドレス等)、並びに、⑤当該侵害を緩和するために取られた措置が含まれていなければならない。

ウ サイバーセキュリティ通知に関する機密保全、当該情報の利用制限、訴訟における責任の免除及びプライバシーの保護

(ア) サイバー侵害報告受付組織における機密指定された通知の受領

サイバー侵害報告受付組織は、①CISA が、同組織において機密指定された提出物や通知を受領できる体制を整えるとともに、②サイバーセキュリティ通知の提出者が、規制対象者であるか否かにかかわらず、これを受領できるようにしなければならないと規定されている。

(イ) 情報の利用に関する制限

本法において、サイバー侵害報告受付組織を通じて CISA に提出されたサイバーセキュリティ通知は、情報自由法(5 U.S.C. 552)第 552 条第(b)項第(3)号(B)(注:「2009 年開かれた情報自由法」の施行日(2009 年 10 月 28 日)以後に制定された情報自由法以外の連邦法において、情報自由法における情報開示が特別に免除され、かつ、その不開示が、この情報自由法の第 3 不開示事由に該当する旨が同法で明記されている場合のこと)又は州法、インディアン部族法若しくは地方自治体の定める情報又は記録の開示を求める法令に基づき、情報開示が免除される。

また、①上記のサイバーセキュリティ通知は、本法により 2002 年国土安全保障法に追加される第 2233 条第(h)項において、CISA 長官により、規制対象者が本法に違反したと決定した場合にお

ける民事罰の執行手続(後述)を除き、サイバーセキュリティインシデントの被害者に対して提起された民事訴訟又は刑事訴訟における証拠として許容されず、また、②連邦議会が、議会による監視目的のために必要であるとして罰則付召喚令状(subpoena)を発する場合を除き、サイバーセキュリティ通知の提出者は、その他の罰則付召喚令状に服することはないと規定されている。

a. 訴訟における責任の免除

規制対象者が、本法及び今後制定される規則にしたがって、サイバー侵害報告受付組織を通じて CISA にサイバーセキュリティ通知を提出したことにより、本法により 2002 年国土安全保障法に追加される第 2233 条第(h)項において、CISA 長官により規制対象者が本法に違反したと決定した場合における民事罰に関する執行手続(後述)を除き、裁判におけるいかなる訴訟原因も生ぜず、そのような訴訟は即座に却下されなければならないと規定されている。

b. プライバシーの保護

CISA は、サイバー侵害報告受付組織を通じて CISA に提出された共有情報において、サイバーセキュリティ脅威と直接に関係のない特定の個人に関する個人情報又は個人を特定する情報を保護するためのプライバシーとデータ保護手続を、「2015 年サイバーセキュリティ情報共有法(Cybersecurity Information Sharing Act of 2015)」におけるプライバシーとデータ保護手続を参考にして策定しなければならないと規定されている。

(ウ) 罰則

CISA 長官は、①規制対象者が本法又はその要件に違反したと決定した場合、当該規制対象者の昨年の総売上高(gross revenue)の 0.5 パーセントを超えない額を、当該違反が継続した期間又は今後も継続する期間における1日当たりの民事上の罰金として評価することができるが、②当該違反の性質、状況、程度及び重大性、規制対象者の支払能力、有責性及び過去の違反歴等の情状を酌量して、上記の罰金を減額若しくは変更することができる。また、同長官は、③この罰金に関する不服申立手続を制定しなければならないと規定されている。

また、規制対象者である連邦政府の請負人が本法に違反した場合には、共通役務庁長官(Administrator of the General Services Administration)は、上記の罰金に加え、当該請負人を連邦政府調達スケジュール(Federal Contracting Schedule)から除外する等の追加の処分を課することができる。

連邦行政機関が、本法の要件に違反した場合には、当該違反を当該行政機関の監察総監(Inspector General)に付託する。なお、当該監察総監は、当該行政機関による違反を、緊急の懸念事項をして対処しなければならないと規定されている。

(エ) サイバーセキュリティ通知の分析

本法案では、提出されたサイバーセキュリティ通知に関する分析について、以下のように定めている。

まず、国土安全保障長官(CISA 長官が代理)、司法長官及び国家情報長官が共同して、提出されたサイバーセキュリティ通知を分析する手続を制定する。同手続においては、迅速かつ適切に、

①サイバーセキュリティ侵害又は侵入により、国家経済及び国家安全保障にもたらされる影響の決定、②当該サイバーセキュリティ侵害又は侵入の潜在的な原因 (potential source or sources) の特定、③当該サイバーセキュリティ侵害又は侵入による影響を緩和させるための推奨策、及び、④将来のサイバーセキュリティ侵害又は侵入に対してシステムを保護するための方法に関する情報提供につき、分析が行われる。なお、この手続においては、迅速な分析、通知又は一般公開が必要となる場合の基準が含まれていなければならないとされている。

次に、国土安全保障長官 (CISA 長官が代理)、司法長官及び国家情報長官は、各行政機関において、サイバー侵害報告受付組織を通じて CISA に提出されたサイバーセキュリティ通知に基づき、サイバー脅威インテリジェンス情報を、上記の手続に従って、国家安全保障又は公共の安全確保のために、インテリジェンス及び法執行情報を調査することができる各行政機関の被用者を指名することができる」と規定されている。

最後に、分析成果の公表について規定されている。まず、30 日に1回よりも多い頻度で、国土安全保障長官 (CISA 長官が代理)、司法長官及び国家情報長官は、連邦行政機関及び規制対象者が直面しているサイバー脅威に関する現状の特徴を記した共同サイバー脅威インテリジェンス報告を作成しなければならないと規定されている。本報告は、①公開する形式で作成されなければならないが、②必要な場合には、機密指定された添付文書 (classified annex) を含むことができる。また、③本報告書では、サイバー侵害報告受付組織を通じて CISA に提出されたサイバーセキュリティ通知における提出主体の帰属性情報 (attribution information) を現実的に最大限可能な限り匿名化しなければならないとされている。なお、国家情報長官は、ここに定められている分析結果又はその一部で機密指定されているものにつき、米国が直面しているサイバー脅威を緩和するために必要がある場合には、当該機密指定を解除することができる」と規定されている。

エ 民間企業によるサイバーインシデント通知に関するその後の立法動向

ここでは、これまで説明してきた連邦議会上院の情報特別委員会に提出された「2021 年サイバーインシデント通知法 (Cyber Incident Notification Act of 2021, 117 S. 2407) 案」(24 時間以内の報告義務等)のほかにも、民間企業にサイバーインシデント通知を求める複数の法案が提出されているので、その後の立法動向を簡単に紹介しておきたい。

その最初のものが、連邦議会上院の国土安全保障政府問題委員会 (CISA に対する管轄権あり) の主力メンバーが超党派でまとめて 2021 年 9 月 28 日に提出された「2021 年サイバーインシデント報告法 (Cyber Incident Reporting Act of 2021, 117 S.2875) 案」である。同法案では、①重要インフラの所有者・運営者に対して、CISA に 72 時間以内に報告する義務を課し、②一般企業 (50 名未満の中小企業を除く)、非営利団体、州、地方公共団体等がランサムペイメントを支払った場合には、24 時間以内に CISA に報告する義務を課するとともに、③これらの報告義務を怠った者に対して、CISA に罰則付召喚令状 (subpoena) を発する権限を付与するとともに、④この罰則付召喚令状に応じない者については、連邦司法省に対して当該令状を執行するための民事訴訟を連邦地方裁判所において提起してもらうための送付手続をとること等が規定されている。この法案は、同委員会で可決されたものの、上院で可決されるまでには至らなかった。

次のものが、連邦議会下院の国土安全保障委員会(CISA に対する管轄権あり)に 2021 年 8 月 27 日に提出された「2021 年重要インフラに関するサイバーインシデント報告法 (Cyber Incident Reporting for Critical Infrastructure Act of 2021, 117 H.R. 5440) 案」である。そして、この法案では、重要インフラを運営する民間企業にサイバーインシデントを 72 時間以内に報告する義務を課し、CISA にサイバーインシデント審査室 (Cyber Incident Review Office) を設ける等の規定を含んでいた。同法案は、下院の 2022 会計年度国防授權法案 (National Defense Authorization Act for Fiscal Year 2022, 117 H.R.4350) の一部として 2021 年 9 月 23 日に下院で可決された。しかしながら、この下院の 2022 会計年度国防授權法案におけるサイバーインシデント通知に関する規定は、上下院の軍事委員会の話し合いの中で削除されてしまった。そして、2021 年 12 月 23 日、2022 会計年度国防授權法は、連邦議会により可決され、同年 12 月 27 日にバイデン大統領に署名されて成立した。なぜ、下院の法案にあったサイバーインシデント通知に関する規定が削除されたのかについては、同法の立法者意思を示す 2022 会計年度国防授權法に関する両院合同付帯説明書 (Joint Explanatory Statement to Accompany the National Defense Authorization Act for Fiscal Year 2022) に、その理由についての記載がない。このため、重要インフラを所有・運営する民間企業に対してサイバーインシデントの通知を義務付ける立法については、新たな法案による審議が必要となった。

その後、2022 年 2 月に、ロシアによるウクライナ侵略が発生したことから、米国をはじめとした西側諸国が、ロシアに重い経済制裁を課した。このため、連邦議会上院は、ロシアが西側諸国へのサイバーエスピアナージをエスカレートさせる可能性があると考えて、3 月 1 日に「米国サイバーセキュリティ強化法 (Strengthening American Cybersecurity Act of 2022, 117 S. 3600)」案を可決²⁷、3 月 2 日に下院に送付している。同法案は、3 つの法案をまとめたものであり、第 1 編が「2022 年連邦情報セキュリティ現代化法 (Federal Information Security Modernization Act of 2022)」、第 2 編が「2022 年重要インフラに関するサイバーインシデント報告法 (Cyber Incident Reporting for Critical Infrastructure Act of 2022)」及び第 3 編が「2022 年連邦政府におけるセキュアなクラウドの向上及び労働力法 (Federal Secure Cloud Improvement and Jobs Act of 2022) から構成されている。これらのうち、第 2 編が、民間企業にサイバーインシデント通知を求めるものとなっているが、その内容については後述する。

一方、下院では、3月9日に2022年包括歳出法 (Consolidated Appropriations Act, 2022) 案が可決されたが、この中には、3月1日に上院で成立した「米国サイバーセキュリティ強化法」の第2編にあたる「2022年重要インフラに関するサイバーインシデント報告法」とほぼ同じ文言の法案が第Y編として含まれていた。そして、2022年包括歳出法案は上院に送付され、3月9日に修正を経た後に、3月10日に上院で可決され、3月15日に大統領により署名されて成立した。このような対応が取られたのは、本来は翌年の9月末までの連邦政府支出を決める包括歳出法の成立が既に5か月近く遅れており、議決によるつなぎ予算が3月15日に切れてしまうと連邦政府が閉鎖される恐れがあ

²⁷ See Jeff Burt, *Russia's invasion kicks Senate into cybersecurity law mode: Critical infrastructure, federal agencies must report intrusions, ransomware payments within hours, draft rules state*, THE REGISTER, available at <https://www.theregister.com/2022/03/05/senate-cyber-bill/>.

ったためである。以下では、2022年包括歳出法第Y編として成立した「2022年重要インフラに関するサイバーインシデント報告法」(以下、「本法」という。)の内容を概説しておきたい。

オ 民間企業によるサイバーインシデント通知に関するその後の立法動向

まず、本法においてサイバーインシデントに関する報告義務を負う「規制対象者(Covered entities)」とは、大統領政策指令第 21 号「重要インフラの保全及び耐障害性(Presidential Policy Directive (PPD) 21 - Critical Infrastructure Security and Resilience)」で定められた 16 分野の重要インフラ²⁸に含まれる事業者で、CISA 長官が、2002 年国土安全保障法第 22 編第 2242 条第(b)項に基づいて発する最終規則における定義を満たすものを意味すると規定されている。この最終規則において、CISA 長官が規制対象者を定義するにあたっては、①当該規制対象者で生じた事故又は危殆化により、国家安全保障、経済安全保障又は公衆衛生・安全にもたらされる結果、②当該規制対象者が、外国政府を含む悪意のあるサイバー行為者により攻撃目標とされる可能性、及び、③当該重要インフラにおける正常な稼働が、損害、事故又は不正アクセスにより阻害されうる程度について明確に記述しなければならないと規定されている。

第2に、規制対象者は、①サイバーインシデントが発生したことを認識してから72時間が経過するまでに、CISA に報告しなければならない、また、②ランサムウェア攻撃の結果として身代金を支払う場合には、その支払いがなされてから24時間が経過するまでに CISA に報告する義務を負う。なお、この身代金支払いに関する報告義務は、規制対象となるサイバーインシデント(covered cyber incident) (後述)に該当しない場合であっても、その報告が義務付けられている。ただし、規制対象者が、規制対象となるサイバーインシデントによる身代金を72時間が経過する前に支払った場合には、上記①及び②の報告義務を、1つの報告で満たすことができるとの注意規定が置かれている。また、規制対象者は、上記の報告を行った後に、新たな情報や実質的に異なる情報を得た場合には、CISA に追加報告を行なうとともに、関連するデータを最終規則により定められた手続に基づいて保管する義務を負っている。なお、最終規則の施行後であれば、同規則の定める手続に基づき、規制対象者は、上記の報告を、第三者(インシデント対応企業、保険会社、サービス・プロバイダ、情報分析共有機関(ISAO)、法律事務所(law firm)等)を用いて提出することができると規定されている。なお、これらの CISA に対する報告義務は、CISA が他の連邦行政機関との間で行政契約を締結し、かつ、規制対象者による当該行政機関に対する同様の報告義務が定めら

²⁸ 本指令では、重要インフラとして16のセクターと、各セクターにセクター主務官庁(Sector-Specific Agencies)が定められている。具体的には、①化学(国土安全保障省)、②商業施設(同)、③通信(同)、④重要な製造業(同)、⑤ダム(同)、⑥国防産業基盤(国防総省)、⑦救急サービス(国土安全保障省)、⑧エネルギー(エネルギー省)、⑨金融サービス(財務省)、⑩食料・農業(農務省・保健福祉省)、⑪政府施設(国土安全保障省・連邦調達庁)、⑫健康・公衆衛生(保健福祉省)、⑬情報テクノロジー(国土安全保障省)、⑭原子炉・核物質・核廃棄物(同)、⑮交通システム(国土安全保障省・運輸省)、⑯水道・下水システム(連邦環境保護庁)との指定がなされている。なお、本法における「セクターリスク管理行政機関(Sector risk management agencies)」という用語は、2021会計年度ウィリアム・M. (Mac)・ソーンベリ国防授權法第9002条「セクターリスク管理行政機関(Sector risk management agencies)」第(a)項第(7)号において、2002年国土安全保障法第2201条第(5)項(6 U.S.C. 651(5))における「セクター主務官庁(Sector-Specific Agencies)」を意味すると定義されているとされていることから、同じことを意味している。

れている場合には、当該規制対象者による CISA への報告義務は免除される。

第 3 に、規制対象となるサイバーインシデント(covered cyber incident)とは、規制対象者が経験した重大なサイバーインシデントで、CISA 長官が、2002 年国土安全保障法第 22 編第 2242 条第 (b)項に基づいて発する最終規則における定義を満たすものを意味すると規定されている。この最終規則において、CISA 長官が定義を行うにあたっては、重大なサイバーインシデントの要素として、少なくとも、①情報システム又はネットワークの機密性・完全性・可用性が実質的に損なわれるサイバーインシデントの発生又は運用システム及びプロセスの安全性・レジリエンスに重大な影響をもたらすサイバーインシデントの発生、②業務遂行又は生産工程に混乱を発生させるもので、これには、情報システム若しくはネットワーク又は運用システム若しくはプロセスに対する Dos 攻撃、ランサムウェア攻撃、ゼロデイ攻撃等に起因するものが含まれ、又は、③不正アクセスの発生、又は、クラウドサービスプロバイダ、マネージドサービスプロバイダ若しくはその他の第三者によるデータホスティングプロバイダにおける危殆化又はサプライチェーンにおける危殆化に起因してサービスの提供が失われたことによる業務遂行又は生産工程の混乱の発生が必要であり、これらについて明確に記述することが必要とされている。さらに、CISA 長官は、本定義を明確に記述するために、①サイバーインシデントの実行にあたり用いられた戦術のレベルの高さ又は新規性、及び、対象となったデータの種類、量及び機微性、②当該サイバーインシデントにより直接的、間接的又は潜在的に影響が及ぶ人数、③産業制御システム(監視制御・データ収集システム(SCADA)、分散制御システム、プログラマブルロジックコントローラ等)に対する潜在的影響を考慮しなければならないと規定されている。ただし、本定義においては、①当該情報システムの所有者又は運営者の特別な要請に善意で対応した結果として発生したサイバーインシデント、及び、②本法第 2240 条第 (14)項(注:ランサムウェア攻撃の定義)第(A)号で規定された恐喝(extortion)は含まれないと規定されている。

第 4 に、規制対象者からの報告を受領するのは、CISA 内部の国家サイバーセキュリティ・通信統合センター(National Cybersecurity and Communications Integration Center)である。同センターは、①受領した報告書を分析し、②大統領政策指令第 21 号「重要インフラの保全及び耐障害性」で定められた 16 分野の重要インフラをそれぞれ主管するセクターリスク管理行政機関と情報を共有し、③重要インフラの所有者・運営者とサイバーインシデントに関する情報共有を行い、④サイバーセキュリティ上の脅威を克服するためのセキュリティ管理や戦術・技術の有効性評価の実施等についての責任を負っている。

第 5 に、国土安全保障長官は、連邦行政管理予算局長、司法長官、国家サイバー責任者(National Cyber Director)、セクターリスク管理行政機関及びその他の適切な連邦行政機関と協議した上で、連邦政府におけるインシデント報告要件を調和させるために、連邦行政機関相互の調整機関としてのサイバーインシデント報告協議会(Cyber Incident Reporting Council)を運営する責任を負うと規定されている。

第 6 に、規制対象者が報告要件を遵守しない場合には、CISA 長官は、当該規制対象者に

対して、当該サイバーインシデント又は身代金の支払いに関する情報の提出を直接に請求し、もしも当該情報を得られない場合には、規制対象となるサイバーインシデント(covered cyber incident)又は身代金の支払いがあったか否かを決定するのに必要な情報を取得する目的で、当該規制対象者に対して罰則付召喚令状(subpoena)を発することができると規定されている。具体的には、CISA 長官は、公開されている報告書や連邦政府が取得した情報から、当該規制対象者が規制対象となるサイバーインシデントを経験し、又は、身代金の支払いを行ったものの報告義務を懈怠していると信じるに値する理由がある場合には、当該規制対象者から、追加の情報を得るための情報を請求することができる。当該規制対象者が、CISA 長官が当該情報請求を行った日から 72 時間が経過した日を過ぎても、当該請求になんらの回答も行わなかった場合、又は、不適切な回答を行った場合には、CISA 長官は、当該規制対象者に対して、規制対象となるサイバーインシデント又は身代金の支払いがあったか否かを決定するのに必要であると考えた情報を開示させるために、当該規制対象者に対して罰則付召喚令状を発することができる。この罰則付召喚令状に応じない者については、CISA 長官は、連邦司法省に対して当該令状を執行するための民事訴訟を連邦地方裁判所において提起してもらうための送付手続をとることができる。当該連邦地方裁判所は、罰則付召喚令状に違反した者に対して、裁判所侮辱罪に処することができる。なお、CISA 長官が、罰則付召喚令状に基づいて取得した情報に基づき、当該サイバーインシデント又は身代金の支払いに関連する事実が、行政上の強制執行又は刑事訴追の要件を満たすものであると判断した場合には、司法長官又は適切な連邦行政機関の長と協議した上で、当該事実を、司法長官又は適切な連邦行政機関の長に提供することができる」と規定されている。

第 7 に、本法に基づいて CISA に提出された規制対象となるサイバーインシデント若しくは身代金の支払い又は自主的に提出されたサイバーインシデント報告書は、①規制対象者により商業的、金融的かつ私的情報であると指定された場合には、そのようにみなされ、②情報自由法(5 U.S.C. 552) 第 552 条第(b)項第(3)号又は州法、インディアン部族法若しくは地方自治体の定める情報又は記録の開示を求める法令に基づく情報開示が免除され、③営業秘密の保護を定める立法を含め、法により規定され適用を受ける特権又は保護を放棄するものとみなされてはならず、かつ、④裁量上の行政決定をなしうる行政職員との意思疎通(一方的(ex parte) コミュニケーション)に関する連邦行政機関の規則又は司法上の原則に服することはないと規定されている。また、規制対象となるサイバーインシデント又は身代金の支払いに関して CISA に提出された報告について提起された民事訴訟又は刑事訴訟は、CISA 長官が罰則付召喚令状に応じない者につき連邦司法省に提起してもらった上記の民事訴訟を除き、即座に却下されなければならないと規定されている。

1.2.2 バイデン大統領による「重要インフラの制御システムのサイバーセキュリティ向上に関する国家安全保障覚書」

バイデン大統領は、2021 年 7 月 28 日に、「重要インフラの制御システムのサイバーセキュリティ向上に関する国家安全保障覚書(National Security Memorandum on Improving Cybersecurity for

Critical Infrastructure Control Systems)」に署名した。本覚書は、コロニアルパイプライン社及び JBS フード社におけるランサムウェア攻撃についての経験から、制御システムに焦点を当てているところに特徴がある。

本覚書と同時に出された概況報告書(FACT SHEET)「バイデン政権による米国の重要インフラを保護するための追加的施策の公表」(White House, FACT SHEET: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure, July 28, 2021)では、①コロニアルパイプライン社及びJBSフードに対するランサムウェア攻撃に見られるように、民間部門が主体となって運営されている米国の重要インフラには、重大なサイバー上の脆弱性が存在しており、②このような重要インフラを制御しているシステムの劣化、機能不全等により、米国の国家安全保障、経済安全保障及び米国市民の公衆衛生・安全が弱体化する恐れがあることから、③重要インフラに対する現在の規制がセクター別になされていることに起因する問題を克服するために、最低限の共通基準を定めるとともに、④重要インフラの所有者と運営者に、自主的なガイダンスと法的拘束力を持った規制に従ってもらうことが必要になるとしている。

1.2.3 サイバー防衛を担う共同サイバー防衛連携の創設

2021年8月5日、ジェン・イースタリー(Jen Easterly) CISA 長官は、世界的に大きな影響力があるサイバーセキュリティイベントである Black Hat USA 2021 において、サイバー防衛を担う共同サイバー防衛連携(Joint Cyber Defense Collaborative: JCDC)の創設を発表した²⁹。

この共同サイバー防衛連携(JCDC)は、2021会計年度国防授權法(2021NDAA)において規定されている共同サイバー計画室(Joint Cyber Planning Office: JCPO)を、その一部として取り込んだ組織である。同法第1715条においては、①共同サイバー計画室(JCPO)を創設し、同室に公的部門と民間部門との間のサイバー防衛作戦に関する計画立案と実施の役割を担わせており、また、②同室は、計画策定を担うスタッフと、国土安全保障省、米国サイバー軍、国家安全保障局(NSA)、連邦捜査局(FBI)、司法省、国家情報長官官房(ODNI)等からの代表者により構成されることになっている。

また、CISAのウェブサイトにあるように、この計画立案には、上記②の行政機関に加えて、米国の重要インフラに対するサイバー関連の脅威に対応するため、各セクターの重要インフラを管轄するセクターリスク管理行政機関も参加すると共に、民間部門からの協力も得て計画立案がなされることになる。

イースタリーCISA長官は、Black Hatにおけるスピーチにおいて、JCDCでは、①従来の国家的なサイバー脅威に共同して対処するという事後的な対応ではなく、事前に協働して積極的な計画を策定し、②民間企業から主要なパートナーとして、Amazon Web Services、CrowdStrike、AT&T、Google Cloud、FireEye Mandiant、Lumen、Microsoft、Palo Alto Networks及びVerizonに計画策定に参加して頂き、③最初に集中して対応するのは、(1)ランサムウェアへの対応と、(2)クラウドサービスプロバイダに影響を与える事案に備えるフレームワー

²⁹ Jen Easterly, Director for CISA, *Keynote: Hacking the Cybersecurity Puzzle*, BLACK HAT 2021 (Aug.5, 2021).

クの計画であり、また、(3)州・地方公共団体等や情報共有組織（ISAOs/ISACs）とサイバー関連のリスク情報を共有することになるという。

なお、その後、IBM、Broadcom、Splunk 等の企業も共同サイバー防衛連携のパートナーとして参画している。

1.2.4 概況報告書「Factsheet: Ongoing Public U.S. Efforts to Counter Ransomware」

(1) 概要

この「Factsheet: Ongoing Public U.S. Efforts to Counter Ransomware（米国政府による進行中の対ランサムウェア政策に関する概況報告書）」³⁰は、2021 年 10 月にホワイトハウスから公表されたもので、米国政府が現在行っている対ランサムウェア対策の概要を示す。

その政策の方針は大きく 4 つに分かれ、以下の通りである。

- ① ランサムウェアにかかるインフラ及びアクター（行為者）の壊滅
- ② ランサムウェア攻撃に耐えられるレジリエンスの強化
- ③ 身代金の洗浄に仮想通貨が濫用されることに対する対応
- ④ ランサムウェアのエコシステムを壊滅し、ランサムウェア加害者に逃亡先を提供している国等に対応するための国際協力を強化

具体的な政策は以下の通りである。

(2) ランサムウェアにかかるインフラ及びアクターの壊滅

ア 司法省のランサムウェア・タスクフォース

司法省は、国家サイバー捜査合同タスクフォース（NCIJTF: National Cyber Investigative Joint Task Force）を中心に、対ランサムウェアのための法執行・起訴を政府機関間で協調して実施することを目的としたタスクフォースを立ち上げた。

イ 財務省による仮想通貨取引所に対する初の制裁

米国財務省外国資産管理室（OFAC : Office of Foreign Assets Control）は、2021 年 9 月、仮想通貨取引所である SUEX OTC, S.R.O.（以下「SUEX」）に対し、同取引所がランサムウェアを使用する犯罪者による脅威に重大なサポートを提供しているとして、大統領令第 13694 号³¹に基づき、仮想通貨取引所に対する初の経済制裁措置を課した³²。同取引所は、これまでの総取引の 40%以上が違法行為者の関与するものであり、少なくとも 8 つの亜種のランサムウェアの支払いに使用されたとされる。

この措置により、米国の管轄内に所在する同取引所の資産は凍結され、同取引所が 50%以上の支配権を有する法人の資産も凍結される。米国人や米国の機関（特に金融機関）は原

³⁰ <https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/>

³¹ 同大統領令は、2015 年 4 月 2 日にオバマ大統領が発出したものであり、「Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities（著しく悪意のあるサイバー活動に関与する特定の者の資産を凍結する）」という標題のものである

（<https://www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities>）。同大統領令により、財務省が指定したサイバー犯罪者の資産を凍結するという方法で金融制裁を課することができる。

³² <https://home.treasury.gov/news/press-releases/jy0364>

則として同取引所との取引を禁じられ、それに違反すると自らも制裁を課されるおそれがある。

ウ 財務省 OFAC による最新勧告

OFAC は、ランサムウェア攻撃及びそれに対する支払いを米国政府に報告することの重要性を強調する、制裁に関する最新勧告を公表した（後述）。

エ 米国サイバー軍及び国家安全保障局（National Security Agency）

米国サイバー軍及び国家安全保障局（National Security Agency）は、ランサムウェア対策のために人材、技術、知見を総動員している。

オ 国務省「正義への報酬」

国務省は、「正義への報酬」（Rewards for Justice）プログラムに基づき、2021 年 7 月、米国の重要インフラを標的としたサイバー攻撃（ランサムウェア攻撃を含む。）に関する情報について、最大 1000 万ドルの報奨金を支払うと発表した。情報提供者を守るために通報先はダークウェブに用意されている。

(3) ランサムウェア攻撃に耐えられるレジリエンスの強化

ア 産業制御システム・サイバーセキュリティ・イニシアチブ

大統領は、2021 年 4 月、産業制御システム（ICS: Industrial Control System）イニシアチブを立ち上げた。これは、連邦政府と重要インフラ産業間の任意の協力を促すものである。同イニシアチブにより、150 の電力事業において制御システムにサイバーセキュリティ技術が実装されることとなり、当該施設のセキュリティ及びレジリエンスの強化が図られた。同イニシアチブは電力だけでなく、天然ガスパイプラインにも拡張され、水道事業にも拡張されるという（本ファクトシート公表時点）。

イ StopRansomware.gov の構築

国土安全保障省及び司法省は、2021 年 7 月、ランサムウェア対策のためのワンストップ・ウェブサイトである StopRansomware.gov を構築した（後述）。

ウ TSA によるセキュリティ指令

国土安全保障省運輸保安庁（TSA: Transportation Security Administration）は、パイプラインを所有又は運営する事業者に対してサイバー防御を強化するようセキュリティ指令を発行した。

エ 副国家安全保障補佐官（サイバー・新技術担当）によるレター

副国家安全保障補佐官（サイバー・新技術担当）は、2021 年 6 月、ビジネスリーダーに対し、データのバックアップ、多要素認証、インシデントレスポンスプランの検証等、ランサムウェア攻撃に対しての防御を強化するための優先度の高いベストプラクティスを列挙したレターを送付した³³。そのベストプラクティスは具体的には、①バイデン大統領が 2021

³³ [Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf \(whitehouse.gov\)](#)

年 5 月に発付した大統領令第 14028 号「国家のサイバーセキュリティの向上」³⁴における 5 つのベストプラクティス (i)多要素認証、(ii)エンドポイントにおける検知及びレスポンス、(iii)暗号化、(iv)優秀なセキュリティチームの設置) を実施すること、②データ・システムイメージ・コンフィギュレーションのオフラインでのバックアップ・定期チェック、③システムを速やかにアップデートしパッチを当てること、④インシデントレスポンスプランを検証すること、⑤セキュリティチームの作業確認、⑥ネットワーク・セグメンテーションの実施、である。

オ 大統領とビジネスリーダーによるイニシアチブ

2021 年 8 月、バイデン大統領と民間部門・教育部門のリーダーは、米国のサイバーセキュリティを強化するためのイニシアチブを発表した³⁶。このイニシアチブには以下のプログラムが含まれる。

- ・NIST は、マイクロソフト、Google、IBM などの産業界と協力して、技術サプライチェーンのセキュリティと完全性を向上する新たなフレームワークを策定する (後述「ランサムウェア・リスクマネジメントのためのサイバーセキュリティ・フレームワーク・プロフィール」)。

- ・バイデン政権による産業制御システムサイバーセキュリティ・イニシアチブを電気業界のみならず天然ガスパイプラインに正式に拡大する。

- ・Apple は、米国における 9000 のサプライヤーを含むサプライチェーンを通じて、多要素認証、セキュリティ研修、脆弱性修復、イベントログ、インシデントレスポンスを採用してセキュリティの向上を図る新しいプログラムを構築する。

- ・Google は、今後 5 年間で 100 億ドルを投じて、ゼロトラストプログラムを拡張し、ソフトウェアサプライチェーンのセキュリティ改善を支援し、オープンソースセキュリティの向上に努めると発表した。

- ・IBM は、今後 3 年間で 15 万人にサイバーセキュリティ技能に関する研修を施すと発表した。

- ・マイクロソフトは、今後 5 年間で 200 億ドルを投じて、セキュリティ・バイ・デザインを組み入れ、高度なセキュリティソリューションを提供できるように努めると公表した。

³⁴ <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

³⁵ 同大統領令は、コロナルパイプライン事件を受けて発出されたもので、サイバーインシデントの防止、検知、評価、修復が国家安全保障、経済安全保障に不可欠であるとの方針のもと、脅威情報の共有の促進 (第 2 条)、ゼロトラストアーキテクチャの採用を始めとするベストプラクティスによる連邦政府におけるサイバーセキュリティの現代化 (第 3 条)、ソフトウェアサプライチェーンの向上 (第 4 条)、DHS によるサイバー安全審査理事会の設置 (第 5 条)、サイバーセキュリティ脆弱性・インシデント対応に関する連邦政府のための実践集 (プレイブック) の標準化 (第 6 条)、連邦政府のネットワークにおけるサイバーセキュリティ脆弱性・インシデントの検知の向上 (第 7 条)、連邦政府における調査能力・修復能力の向上 (第 8 条)、国家セキュリティシステム (第 9 条) に関する規定を定める。

³⁶ [FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity | The White House](#)

・Amazon は、従業員に施しているセキュリティ・アウェアネス研修を無償で公に提供すると公表した。

カ NIST によるランサムウェア対策の標準の策定

国立標準技術研究所 (NIST) は、2022 年 2 月、NIST サイバーセキュリティ・フレームワークの一環として、産業界と協力して、ランサムウェア攻撃に対する防御、レスポンス、リカバリに関するガイダンスを提供する「ランサムウェア・リスクマネジメントのためのサイバーセキュリティ・フレームワーク・プロフィール」を策定した (後述)。

キ 財務省及び CISA によるサイバー保険部門への働きかけ

財務省及び CISA は、サイバー保険事業者に働きかけ、同事業者らがサイバーセキュリティを強化し、ランサムウェアの行動の可視化を向上させるインセンティブを探索している。

1.2.5 2022 会計年度国防授權法におけるランサムウェアに関する直接規定

2021 年 12 月 23 日、2022 会計年度国防授權法 (National Defense Authorization Act for Fiscal Year 2022: 2022 NDAA) は、連邦議会により可決され、同年 12 月 27 日にバイデン大統領に署名されて成立した。同法は、ランサムウェアやサイバーインシデントへの対応、さらには、サイバー関連の官民協力、重要インフラ防御といったサイバーセキュリティに関する規定を多く含んだものになっているが、ここでは、ランサムウェアに直接関係した第 1510 条に限って紹介したい。なお、非常に重要な条文であるので、全訳を行った。

第 1510 条「敵のランサムウェアの利用、能力及びインフラに対抗するための能力評価 (Assessing capabilities to counter adversary use of ransomware, capabilities, and infrastructure)」
(仮訳)

第(a)項「求められる包括的な評価と提言」 国防長官は、本法が施行されてから 180 日が経過するまでに、以下の各項が定める義務を遂行しなければならない。

第(1)号 米国をランサムウェア攻撃の脅威から守り、かつ、その影響を減らすために必要となる国防総省の政策、機能 (capacity) 及び能力 (capabilities) に関して、以下の事項を含む包括的な評価を行うこと。

(A) 以下の 2 つの項目により課される国家経済安全保障に対する現在の又は潜在的な脅威とリスクに対する評価。

(i) 大規模で洗練されたサイバー攻撃能力をもち、かつ、ランサムウェア攻撃を行うために用いるインフラを有する大規模で洗練された犯罪サイバー組織、及び、

(ii)米国の重要資産及びシステム (重要インフラを含む) に対して、大規模な上記(i)に記述した能力とインフラを用いてランサムウェア又はその他の攻撃を行うことのできる組織、又は、過去に行うことができた組織。

(B) 以下の 2 つの項目に関する評価。

(i) 国防総省の情報ネットワーク及び米国に対して、上記第(a)項第(1)号 (A)で記述した大規模で洗練された犯罪組織で、その能力及びインフラに

より課される脅威、及び、

(ii) 上記(i)で述べた脅威に対する米国サイバー軍の現在又は潜在的な役割で、以下の2つの項目を含むもの。

(I) 米国サイバー軍が当該脅威に対処すべき閾値 (threshold)、及び、

(II) 米国サイバー軍が、その他の本来任務を遂行する上で負の影響をもたらさずに当該脅威に対応しうる適応能力。

(C)本条第(a)項第(1)号(B) (i)において述べた脅威を阻止し対処するための国防総省の取り組み、手続及び能力（これには、攻撃的サイバー効果を持つ作戦も含まれる）の特定。

(D)米国へのランサムウェア攻撃に対する脅威を阻止し、かつ、対処するために、国防総省の前方防衛及び持続的対処という作戦概念と能力とを適用した場合の評価。

(E)ランサムウェア攻撃の実行や、他の目的のために攻撃を行いうる大規模で洗練された犯罪組織による増大する脅威に対処するために、国防総省が取れる他の連邦行政機関との間の協力、及び、米国の同盟国及び同志国との相互協力に関する取り組みについての記述。

(F)大規模で洗練されたサイバー犯罪組織が主として活動している国家の政府は、どの程度、当該犯罪組織の活動を許容しているのか、意思の疎通があるのか、当該犯罪組織による作戦を命じている可能性があるのか、及び、当該犯罪組織を制圧することができるのかに関する決定。

(G) 本条第(a)項第(1)号(F)において述べられた大規模で洗練されたサイバー犯罪組織は、当該犯罪組織が主に所在している国家において提供されているサービスに加入でき、攻撃技術の能力を訓練し、かつ、向上させているのかに関する評価。

(H) ランサムウェア攻撃による脅威により効果的に対応するために必要となる立法上又は行政上の措置の特定。

第(2)号 ランサムウェア攻撃が開始される前に、同攻撃による脅威を阻止・対応する革新的な手法を開発・執行するのに必要となる能力構築を行うための提言を国防総省に対して行うこと。

第(b)項「概況説明」 国防長官は、本法が施行されてから 210 日が経過するまでに、連邦議会上下院の軍事委員会に対して、本条第(a)項第(1)号に基づいて行われた包括的評価、及び、本条第(a)項第(2)号に基づいて行われた提言に関する概況説明を行わなければならない。

第(c)項「定義」 本条における「重要インフラ (critical infrastructure)」という用語は、連邦公法第 107-56 号第 1016 条第(e)項 (42 U.S.C. 5195c(e)) に定められた意味を有するものとする。

1.3 アメリカにおけるランサムウェア対応の実際

1.3.1 StopRansomware.gov の構築と注目すべき内容及び関係するガイドライン

(1) StopRansomware.gov とは

StopRansomware.gov³⁷とは、国土安全保障省（DHS）及び司法省が構築したランサムウェア対策のためのワンストップ・ウェブサイトである。これは、2021 年 1 月にサイバーセキュリティ及びインフラストラクチャセキュリティ庁（CISA: Cybersecurity Infrastructure Security Agency）が発表した「Reduce the Risk of Ransomware Campaign（ランサムウェアのリスクを低減するキャンペーン）」の一環として 2021 年 7 月に構築された³⁸。

同サイトでは、ランサムウェアに対する防御、検知、レスポンスに関する各省庁のリソースやアラートが提供され、例えば、CISA や FBI、NIST、シークレットサービスによる報告書やガイダンスが掲載されている。

(2) 提供される内容

ア 注目されるサービス

同サイトで提供されているサービスの中でも注目すべきものとしては、CISA から提供される無償のスキャン・テストサービスがある。これは、個人、組織が、ランサムウェアを含む脅威を評価、特定、緩和するために提供されるもので、同サービスには、脆弱性スキャン、ウェブアプリケーション・スキャン、フィッシング査定、リモートペネトレーションテストが含まれる³⁹。

また、ネットワーク上の行動についてサイバーセキュリティ上問題がないかを自己査定するためのデスクトップソフトウェアツールであるサイバーセキュリティ査定ツール（CSET）も無償で提供されており、2021 年 6 月には同ツールに対ランサムウェアモジュールである Ransomware Readiness Assessment（RRA）も加えられた⁴⁰。

イ 提供されるガイドライン等

ランサムウェアに対する事前対応に関するガイドラインとしては、シークレットサービスによるガイダンス「サイバーインシデント対応（Preparing for a Cyber Incident）」⁴¹や、CISA 及び MS-ISAC が提供する「Ransomware Guide」⁴²（2020 年 9 月発行）がある。「Ransomware Guide」の第 1 章では、ランサムウェア対策のベストプラクティスが列挙されている。概要は以下の通りである

[準備段階]

- ・定期的にオフラインで最新の暗号化バックアップをとっておくこと。
- ・基本的なインシデントレスポンスプランを策定・維持・訓練しておくこと。その

³⁷ <https://www.cisa.gov/stopransomware>

³⁸ <https://www.cisa.gov/news/2021/01/21/cisa-launches-campaign-reduce-risk-ransomware>

³⁹ <https://www.cisa.gov/stopransomware/services>

⁴⁰ <https://www.cisa.gov/uscrt/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat>

⁴¹

際、「Public Power Cyber Incident Response Playbook⁴³」や「Ransomware Guide」第2章のランサムウェア・レスポンス・チェックリスト（後述）が参考となる。

[脆弱性、コンフィギュレーションの過誤について]

- ・定期的に脆弱性をチェックすること。
- ・ソフトウェアやOSについて定期的にパッチを当て最新の状態にアップデートしておくこと。
- ・デバイスのコンフィギュレーションを適切に維持し、セキュリティ機能をオンにしておくこと。
- ・リモート・デスクトップ・サービスを使用する際はそのベストプラクティスを参照すること。
- ・外部からのサーバー・メッセージ・ブロック（SMB）プロトコルをオフにする又はブロックすること。

[フィッシングについて]

- ・サイバーセキュリティ意識・訓練プログラムを導入すること。
- ・電子メールゲートウェイにフィルタリングを施すこと。
- ・DMARC（電子メール認証プロトコル）のポリシーと認証を実装すること。
- ・電子メールで送付されるマイクロソフトの Office ファイルのマクロスクリプトをオフにすることの検討。

[ウイルス・マルウェア対策]

- ・アンチウイルス・アンチマルウェアの機能を実装し最新の状態に保つこと。
- ・承認したソフトウェアのみが動くように、すべてのアセットについてアプリケーション・ディレクトリ許可リストを使用すること。
- ・侵入検知システム（IDS）の導入を検討すること。

[サードパーティデバイスについて]

- ・サードパーティデバイスのリスク管理と健全なプラクティスについて考慮に入れて使用すること。

[一般的なベストプラクティス]

- ・すべてのサービスにおいて多要素認証を採用すること。
- ・最小権限の原則（アクセス権限の制限）を採用すること。
- ・クラウド環境においては特にベストプラクティスを重視すること。
- ・ネットワークの全体図を策定し、最新の状態であるか定期的に確認すること。
- ・論理的又は物理的なネットワーク・セグメンテーションを実装すること。
- ・包括的なアセット管理アプローチを採用すること。
- ・PowerShell の使用を一定の者に制限すること。
- ・ドメイン・コントローラのセキュリティを維持すること。

⁴³ <https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf>

- ・ネットワークデバイス及びローカルホストのログを十分かつ安全に保持すること。

- ・数か月単位でのネットワーク上のアクティビティを把握すること（異常なイベントを検知しやすいように）。

反対に、CISA は、とりわけ重要インフラや国家重要機能（National Critical Functions）においてとってはならないバッドプラクティス（①サポートされていない（製品寿命が終了した）ソフトウェアを使用すること、②既知のパスワード、固定のパスワード、初期設定時のパスワードを使用すること、③重要インフラの稼働をサポートするシステムにリモートでアクセスする際及び管理者権限でアクセスする際に多要素認証ではなく単一要素認証を採用すること）を掲載している⁴⁴。このリストは今後も追加されるという。

また、同サイトは、事前対策として、各種研修素材（動画）やウェビナーを提供している⁴⁵。

ランサムウェアに攻撃された可能性がある場合にとるべき行動については、ランサムウェア・レスポンス・チェックリストとして前掲「Ransomware Guide」第2章に列挙されており、CISA はこのチェックリストに準じて対応することを強く推奨している⁴⁶。同チェックリストは具体的には以下の通りである。

[検知・分析段階]

1. 影響を受けたシステムを識別し、直ちに隔離する。
2. デバイスをネットワークから切断できない場合は、電源を切ってマルウェアの感染拡大を防ぐ。
3. 復旧・回復のために影響を受けたシステムの優先度を選別（トリアージ）する。
4. 初期の分析に基づきチーム内で初期段階での理解をまとめ書面化する。
5. 社内チームや CISA などの外部チームに協力を仰ぐ。

[封じ込め及び除去]

6. 影響を受けたデバイスのシステムイメージやメモリを取得。関係するログを収集する。
7. 連邦法執行機関に連絡し、解読方法がないか確認する。
8. 当該ランサムウェアについて推奨される措置がないか信頼できるガイダンスを参照する。
9. 当初のデータ漏洩に関与したシステムやアカウントを特定する。
10. 特定されたシステム等の情報に基づき、さらなる不正アクセスがないか確認し、封じ込める。
11. サーバーサイドデータが暗号化されているかを確認する。
12. アンチウイルスや侵入検知システムなどの社内の既存の検知・防止システムに

⁴⁴ <https://www.cisa.gov/stopransomware/bad-practices>

⁴⁵ <https://www.cisa.gov/stopransomware/training>

⁴⁶ <https://www.cisa.gov/stopransomware/ive-been-hit-ransomware>

よるテスト及びログのテストを実施する。

13. 外側からの侵入及び内側からの漏えいのメカニズムがないか広範な分析を実施する。
14. 重要サービスの優先度にしたがってシステムを再構築する。
15. すべての環境がクリーンになった段階で、影響を受けたシステム及びアドレスについてリセットされたパスワードを発行する。
16. IT チームにおいてインシデントの終了を宣言する。

[回復・事故後の対応]

17. サービスの優先度・重要度に従って、システムを再接続し、オフラインの暗号化されたバックアップからデータを回復させる。
18. インシデントから学んだことを書面化し、会社のポリシー・手順に反映させる。
19. インシデントから学んだことを CISA 等と共有することを検討する。

ランサムウェアを検知した場合、被害者は報告することが強く推奨されているところ⁴⁷、報告先が FBI や CISA、シークレットサービスなど複数存在する。StopRansomware.gov では FBI や CISA の電子報告サイト並びに FBI 及びシークレットサービスのローカルオフィスの連絡先情報を一つのサイトにまとめ、いずれか一つに報告すればすべての機関に情報共有されることとして、報告者の便宜を図っている⁴⁸。

また、NIST は、2022 年 2 月、ランサムウェアに関する事前対策、レスポンス、リカバリについて、セキュリティ・プライバシー管理策である NIST SP800-53 Rev.5⁴⁹⁵⁰や ISO/IEC 27001:2013 に対応した形で、各段階においてどのような対応をとるべきかを示した NIST 所内及び省庁間報告書「ランサムウェア・リスクマネジメントのためのサイバーセキュリティ・フレームワーク・プロフィール」（NISTIR 8374 Ransomware Risk Management: A Cybersecurity Framework Profile）を発表している⁵¹。

1.3.2 OAFC の最新勧告（Updated Advisory）

（1）概要

2021 年 9 月、財務省外国資産管理局（OFAC）は、「Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments（ランサムウェアに対する支払いを促進することにおける制裁の可能性に関する最新勧告）」⁵²を公表した。これは、2020 年 10 月に OFAC から公表された「Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments（ラ

⁴⁷ 前掲 Ransomware Guide・11 頁、後掲 OAFC 最新勧告・5 頁。

⁴⁸ <https://www.cisa.gov/stopransomware/report-ransomware-0>

⁴⁹ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>

⁵⁰ 2020 年 9 月に公表。タイトルは、「情報システム及び組織のためのセキュリティ管理策とプライバシー管理策」。Rev.4 では「連邦政府情報システム及び連邦組織のためのセキュリティ管理策とプライバシー管理策」であったところ、Rev.5 では「連邦政府情報システム及び連邦組織のための」が消去され、一般的に組織で採用されるべき管理策のカタログとなった。連邦政府がとるべき最低限のセキュリティ管理策は NIST SP800-53B に記載されている。

⁵¹ <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf>

⁵² https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

ンサムウェアに対する支払いを促進することにおける制裁の可能性に関する勧告)」の内容⁵³をアップデートさせたものであり、本最新勧告は従前の勧告に優先する⁵⁴。

OFAC は、国際緊急経済権限法（IEEPA: International Emergency Economic Powers Act）⁵⁵に定める経済制裁違反、その未遂、共謀、教唆・幫助に対して、民事上の制裁金を課す役割を担うところ⁵⁶、本最新勧告は、(1) OFAC がランサムウェア加害者等を経済制裁対象者に指定してきたこと、(2) 米国政府は身代金の支払いをしないよう強く推奨していること、(3) ランサムウェアについて身代金を支払うこと及びその支払いを促進すること（金融機関、サイバー保険会社、デジタルフォレンジックやインシデントレスポンスに関与する会社等による行為）が制裁対象者との取引を禁じる OFAC 規制に違反する可能性があること、(4) 支払先が制裁対象者又は制裁関連者（sanctions nexus）の可能性がある場合は直ちに OFAC を含む関係機関に通報すべきこと、(5) OFAC による制裁可能性を緩和する積極的な措置について論じる。

以下で本最新勧告の内容を紹介するが、ほとんどの部分は 2020 年 10 月の勧告と重なり、下線を引いた部分が最新勧告において新しく加えられた内容である。

(2) ランサムウェア攻撃者への制裁措置の事例

OFAC は、サイバー関連の制裁プログラム等に基づき、以下に対してランサムウェア攻撃に関連したとして制裁措置をとってきた。

- ・Cryptolocker の開発者 Evgeniy Mikhailovich Bogachev（2016 年 12 月）
- ・SamSam ランサムウェアの拡散に重要な支援を行ったイラン人 2 名及び同ランサムウェアに対する支払いに使用された仮想通貨の送付先⁵⁷2 つ（2018 年 11 月）
- ・WannaCry 2.0 に関与した北朝鮮の支援する Lazarus Group とその下部組織 2 つ（2019 年 9 月）
- ・Dridex マルウェアを開発し拡散したロシアを拠点とする Evil Corp 及びそのリーダー Maksim Yakubets（2019 年 12 月）
- ・これまでの総取引の 40%以上が違法行為者の関与するものであり、少なくとも 8 つの亜種のランサムウェアの支払いに使用されたとされる仮想通貨取引所である SUEX OTC, S.R.O.（本社はチェコ）（2021 年 9 月）

⁵³ 「現代のサイバーセキュリティの法的課題についての国際的な研究」に関する調査報告書（2021 年）第 1 章において詳述（<https://www.jnsa.org/result/compliance/2021/index.html>）。

⁵⁴ 本最新勧告注 2。

⁵⁵ IEEPA は、1977 年に施行された法律である。対敵貿易法（Trading with Enemy Act）が大統領に戦時に限り対外的な経済制裁の権限を認めるのに対し、IEEPA は、戦時のみならず平時においても、米国外において、米国の国家安全保障、外交政策、経済に対し、異例かつ重大な脅威がある場合に、大統領が国家緊急事態宣言を発付して、指定国・国民が関与する取引又は指定国等が利害関係を有する財産の使用、譲渡、輸出入等を調査、規制、禁じる制裁を行うことを認めるものである。

⁵⁶ なお、IEEPA では同法に定める経済制裁違反等について刑事罰も科すが、この刑事訴追を所管するのは司法省の国家安全保障部（National Security Division）である。

⁵⁷ 従前は SDN リストに掲載されるのは個人又は法人であったところ、OFAC は、2018 年 3 月、デジタル通貨の送付先（digital currency address）も掲載対象とし、それに関与する取引を制裁対象とした（OFAC の FAQ 参照。<https://home.treasury.gov/policy-issues/financial-sanctions/faqs/647>）。

(3) ランサムウェアに対する米国政府の方針

米国政府は、身代金の支払いをしないよう強く推奨している。その理由として、制裁関連者に利益を供与し、その違法な目的に資すること、それによって合衆国の国家安全保障や外交政策目的に反する活動の資金として使用される可能性があること、さらなるランサムウェア攻撃を誘発すること、身代金を支払ってもデータが戻ってこないリスクがあることを挙げる。

(4) ランサムウェア攻撃に対する支払いへの関与が制裁対象となりうること

米国人は、国際緊急経済権限法（IEEPA）又は対敵貿易法（TWEA）⁵⁸のもと、OFAC の特別指定国民・凍結者リスト（SDN（Specially Designated Nationals）リスト）、その他の凍結者、及び包括的な国や地域の禁輸措置の対象となっている者（キューバ、ウクライナのクリミア地域、イラン、北朝鮮、シリアなど）の個人又は事業体との間で、直接又は間接的に取引に関与することが一般的に禁止されている。また、IEEPA に基づく違反を引き起こすあらゆる取引（米国人による違反を生じさせる非米国人による取引を含む。）も禁止されている。

これらの違反に対しては厳格責任が適用される。すなわち、当事者は、取引の相手方が経済制裁の対象となっていることを知らなかったとしても、また、知り得なかったとしても責任を問われうる。

違反に対する制裁としては、非公開措置であるノーアクションレターや警告レター（Cautionary Letter）の交付、公開措置である制裁金の賦課がある。

OFAC は経済制裁執行ガイドライン（Enforcement Guidelines）⁵⁹において経済制裁違反に対してどのような場合に執行措置が加えられるかを示すところ、適切な制裁コンプライアンス・プログラムが存在するか、それが適切に運営されているかが斟酌され、適切な場合には制裁が課されない又は軽減される、としている⁶⁰。これに基づき、OFAC は、ランサムウェア攻撃の被害者のみならず、それに関与するサイバー保険会社、デジタルフォレンジック会社、インシデントレスポンス会社、金融サービス会社がそれぞれリスクベースのコンプライアンス・プログラムを実装することを推奨する。また、身代金の支払いに関与する事業者に対しては、2020 年 10 月に発表された財務省の金融犯罪取締ネットワーク（FinCEN: Financial Crimes Enforcement Network）のガイダンス「Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments（ランサムウェア及び支払いを促進する金融機関の利用についての助言）」も遵守するよう呼びかけている⁶¹。

また、ランサムウェア攻撃を受けるリスクを軽減するために普段から CISA の前掲「Ransomware Guide」を遵守している場合は、制裁緩和の大きな要素になるとする。具体的

⁵⁸ 50 U.S.C. §§ 4301–41; 50 U.S.C. §§ 1701–06。

⁵⁹ 31 C.F.R. part 501、別紙 A。

⁶⁰ 「A Framework for OFAC Compliance Commitments（OFAC コンプライアンス取組みのための枠組み）」
(https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf) 1 頁。

⁶¹ FinCEN のガイダンスについては、前掲脚注 53 報告書第 1 章をご参照のこと。

には、データをオフラインでバックアップしておくこと、インシデントレスポンスプランを策定しておくこと、サイバーセキュリティ訓練を実施していること、定期的にウイルス・マルウェア対策ソフトをアップデートしていること、認証プロトコルを採用していること、が重視されている。

さらに、OFAC による Enforcement Guidelines（執行ガイドライン）では、ランサムウェア攻撃の自主的で完全かつタイムリーな通報は OFAC による制裁を大幅に緩和する要素であるとされるところ、ランサムウェア攻撃を発見後可及的速やかに CISA や財務省サイバーセキュリティ・重要インフラ保護室（OCCIP: Office of Cybersecurity and Critical Infrastructure Protection）等の適切な政府機関にランサムウェア攻撃を通報した場合がそれにあたりとする。そして、技術情報や身代金の支払要求、支払指示等の関連情報をできる限り早く提供する等、ランサムウェア攻撃の最中及びその後において法執行機関に全面的に協力した場合も大幅な緩和要素となる、とする。このような通報・協力を実施した場合、仮に支払先が制裁関連者であったとしても、事情によっては、非公開型の執行（ノーアクションレターや警告レター）で済む、とされる。

(5) OFAC による許認可方針

ランサムウェアに対する支払いは合衆国の安全保障に関わるため、身代金の支払いに関する許可申請については原則不許可として扱われる。

(6) 通報先

ランサムウェア攻撃を受けた場合、CISA、FBI 地方局、FBI インターネット犯罪苦情センター（IC3）、シークレットサービス地方局にできる限り早期に通報することが強く奨励される。さらに、身代金の支払いについて制裁関連者が関与している疑いがある場合は、財務省の OCCIP 及び OFAC に通報すべきである。

このような通報をした場合、復号ツールによってデータへのアクセスを復旧できる可能性があり、支払った身代金を取り戻せる可能性があり、加害者を追跡し、その責任を追及し、将来的な犯罪を防止することにつながる、として通報した場合のメリットが強調されている。

1.3.3 身代金の洗浄に仮想通貨が濫用されることに対する対応

(1) 自国の仮想通貨ビジネスに対するマネーロンダリング対策規制

米国は、自国の仮想通貨取引所に対してマネーロンダリング・テロ対策（AML/CFT: anti-money laundering/countering the financing of terrorism）規制を適用しており、財務省の金融犯罪取締ネットワーク（FinCEN: Financial Crimes Enforcement Network）の交換プログラム（FinCEN Exchange）等を通じて仮想通貨の不正使用の指標や類型を金融機関と共有している。なお、FinCEN Exchange とは、2021 年 1 月に制定された 2020 年アンチマネーロンダリング法（AML 法）に基づき設立された⁶²、法執行・国家安全保障にかかわる政府機関と金融機関との間の任意の情報共有パートナーシップであり、情報共有によって金融機関がより

⁶² AML 法第 6103 条。

リスクを特定できるようにし、金融機関から行政機関に対してマネーロンダリング、テロリストによる資金調達、その他の金融犯罪を摘発するにあたり重要な情報が提供されるようにすることを目的とする⁶³。

(2) 海外の仮想通貨資産に対する規制強化の働きかけ

米財務省は、OECD に事務局を置く金融活動作業部会（FATF: Financial Action Task Force）において暗号資産の金融的透明性を高めるための国際標準を実装するよう働きかけている⁶⁴。また、二国間パートナーシップを構築して、海外の仮想通貨取引所に対して AML/CFT 規制を強化すべく動いている。

(3) FBI による IVAN 情報共有パートナーシップの構築

米政府は、FBI の主導のもと、違法暗号資産通知（IVAN: Illicit Virtual Asset Notification）情報共有パートナーシップを構築し、ランサムウェアに対する支払いその他の違法な暗号資産による支払いの流れを検知し妨害する行動計画を改善することを試みている。

1.3.4 国際協力の強化

(1) 国際組織への働きかけ

米政府は国際社会にランサムウェア脅威への対応強化を働きかけ、その成果が、G7 サミットにおける共同声明、北大西洋条約機構（NATO）の共同声明⁶⁵、FATF の動きにつながっていると。また、バイデン政権は、サイバー犯罪条約の加盟国の拡大を支持している。

(2) 二国間外交による働きかけ

ロシアに対してランサムウェア攻撃犯罪者に対して避難地を提供することのないよう外交的な交渉に努めている。

2 英国におけるランサムウェア対応の進展

2.1 2021 年調査について

2021 年 3 月段階の調査において英国においては、ランサムウェア対応についての政府関係のコメントはあまり多くはなく、国家サイバーセキュリティセンター（NCSC）の「マルウェアとランサムウェア攻撃を緩和するーマルウェアとランサムウェア攻撃から組織をどのようにして防御するか（Mitigating malware and ransomware attacksーHow to defend organisations against malware or ransomware attacks）」というページでのガイダンス⁶⁶が見つかる程度であり、資金洗浄及びテロリスト金融犯罪の対象となりうることも、金融規制機関からの助言等⁶⁷については、現時点においては見つからなかった。

⁶³ <https://www.fincen.gov/resources/financial-crime-enforcement-network-exchange>

⁶⁴ FATF は、2019 年 6 月、基準を改訂し、すべての国に対し、取引所を含む暗号資産取引業者（VASP）を規制・監督し、暗号資産取引に従事する際のリスクを軽減することを求め、VASP 全体に顧客管理（CDD）要件を課し、疑わしい取引の報告義務を課すこととした（<https://home.treasury.gov/news/press-releases/jy0364>）。

⁶⁵ 2021 年 7 月、NATO は共同声明を発表し、その中で、包括的サイバー防衛政策を提唱し、著しく悪意のある度重なるサイバー活動は、一定の事情のもとでは、武力攻撃とみなされ、国連憲章 5 条（集団的自衛権）の発動につながるとの見解を示した（https://www.nato.int/cps/en/natohq/news_185000.htm）。

⁶⁶ <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>

⁶⁷ なお、英国財務省及び内務省「資金洗浄及びテロリスト資金供与についての国家リスク評価

2.2 NCSC の動向

2.2.1 ランサムウェアのポータルサイト

NCSC は、ランサムウェアについての総合的なポータルのページを展開しており⁶⁸、上記の「マルウェアとランサムウェア攻撃を緩和する—マルウェアとランサムウェア攻撃から組織をどのようにして防御するか」のページは、その一部となっている。このガイダンスのページのマルウェアの概念、4つのアクション、既に感染してしまった場合へのアドバイスの項目という基本的な情報の構成については、変わっていない。そこでは、米国の CISA との合同でのアドバイザリが紹介されているとともに、No More Ransome プロジェクトへのリンクが貼られている。

ポータルのページからは、データバックアップのガイダンス⁶⁹、報告書の提出⁷⁰、サイバーインシデント対応⁷¹、CiSP（サイバーセキュリティ情報共有パートナーシップ）⁷²、サイバーエッセンシャルズ⁷³などへのリンクが記載されている。

2.2.2 Ransomware Taskforce (RTF)

NCSC は、2021 年 4 月に、ランサムウェア・タスクフォース（RTF）の活動に貢献したというアナウンスをしている⁷⁴。RTF は、世界的なランサムウェアの脅威に対処する強固な計画を策定することにより、攻撃者を抑止し、混乱させるとともに、組織が準備と対応を行えるように支援することを目的として 2021 年初めに米国が主導し、世界中の政府、ソフトウェア企業、サイバーセキュリティベンダー、非営利団体、学術機関から参加者を集めて招集されたものである。RTF は、主に米国政府を対象とした最終報告書を発表した。この報告書には、ランサムウェア攻撃による被害を世界的に軽減する可能性のある行動の枠組みが盛り込まれている。このアナウンスでは、英国では、教育機関がオンライン学習、入学、試験手続の管理に懸命に取り組んでいた時期に、教育分野に影響を及ぼすランサムウェア攻撃

(National risk assessment of money laundering and terrorist financing 2020

(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf)) においては、サイバー犯罪が、資金洗浄やテロリスト資金と関連の深いものであり、ランサムウェアもそのひとつであるという記述がある (3.22)。

⁶⁸ <https://www.ncsc.gov.uk/ransomware/home>

⁶⁹ <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/always-back-up-your-most-important-data>

⁷⁰ NCSC への報告 (<https://report.ncsc.gov.uk/>)、不正及びサイバー犯罪報告 (Action Fraud) への報告 (<https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime>)

⁷¹ サイバーインシデントレスポンス (Cyber Incident Response (CIR)) という認定企業の一覧がある

([https://www.ncsc.gov.uk/section/products-services/all-products-services-categories?productType=Cyber%20Incident%20Response%20\(CIR\)](https://www.ncsc.gov.uk/section/products-services/all-products-services-categories?productType=Cyber%20Incident%20Response%20(CIR)))。また、そのための標準が公開されている ([https://www.ncsc.gov.uk/files/NCSC%20CIR%20Standard%20\(Level%201\).pdf](https://www.ncsc.gov.uk/files/NCSC%20CIR%20Standard%20(Level%201).pdf))。

⁷² 英国内の組織に、コミュニティを支援し、英国のサイバー耐性を高めることができる情報を議論し、共有するための安全なポータルを提供している (<https://www.ncsc.gov.uk/section/keep-up-to-date/cisp>)。特にランサムウェアなどの新しいマルウェアの影響を軽減できるよう、技術情報や侵害の指標を共有するよう会員に呼びかけている。

⁷³ サイバーエッセンシャルズは、最も一般的なサイバー攻撃から組織を保護することを政府が支援する制度である。サイバーエッセンシャルズ (自己診断オプションからなる認証) とサイバーエッセンシャルズプラス (技術検証が実施される) という 2 つのレベルがある。

⁷⁴ “Ransomware Taskforce (RTF) announce framework to combat ransomware” <https://www.ncsc.gov.uk/blog-post/ransomware-taskforce-rtf-announce-framework-to-combat-ransomware>

が急増したこと、また、2020 年に NCSC は、早期警告サービス、悪質な指標の共有、アクティブ・サイバー・ディフェンス対策などにより、防御と脅威の検知能力を強化するため、取組みを強化したことが明らかにされている。

そして、官民の広範なコラボレーションのモデルは、NCSC が設立当初から受け入れているアプローチであるとしている。具体的には、NCSC は、Industry 100 スキームを含む産業界との緊密なパートナーシップを確立しており、専門知識の共有、能力の共有、緩和のための共同戦略の策定を可能にしている。また、法執行機関（インシデントを分類するための単一のマトリクスを開発し、重要インシデントへの効果的な共同対応を実現）や政策部門とも密接に連携し、タスクフォースの報告書で取り上げられている多くの点について、すでに積極的に検討を進めている。

2.3 英国のサイバーセキュリティ政策とランサムウェア対応など

2.3.1 国家サイバーセキュリティ戦略 2022⁷⁵

新しい国家サイバー戦略 2022 は、英国がこの動きの速いデジタル世界で自信と能力、回復力を維持し、サイバースペースでの利益を保護・促進するために適応、革新、投資を続けることを確実にするための計画で、2021 年 12 月 15 日に公表された。

この戦略の中でも、ランサムウェア戦略は、重要なものとして対応が図られている。

この戦略は、「国家目標をサポートするサイバーパワー」というビジョンを立てている。そして、「柱 1：英国のサイバーエコシステムの強化」、「柱 2：弾力性のある豊かなデジタル英国の構築」、「柱 3：サイバーパワーに不可欠な技術で主導権を握る」、「柱 4：より安全で豊かな、そして開かれた国際秩序のために、英国のグローバルなリーダーシップと影響力を強化する」、柱 5：サイバースペースにおける英国の安全保障を強化するための、敵対者の検知、混乱、抑止」という 5 項目を戦略の柱としている。

この戦略において、ランサムウェアは、敵対者の検知、混乱、抑止の柱において、重大な脅威とされ、具体的なケーススタディがなされている。具体的な案件としては、Hackney Council の案件、アイルランド・ヘルスサービス・エグゼクティブの案件が紹介されている。また、そこでは、法執行機関は、犯人への身代金の支払を推奨していないことが記載されている。

2.3.2 NIS 法改正

米国のコロニアルパイプライン事件で重要インフラに対するランサムウェアの攻撃やそれに伴う緊急対応が議論されたが、英国において、水、健康、エネルギー、輸送、デジタルインフラ分野の必須サービスの事業者と、厳選されたデジタルサービスプロバイダに対して、サービスを支えるネットワークのセキュリティを確保するための適切な措置を講じるよう求めているのは、「ネットワーク及び情報システム規則 2018（以下、「NIS 規則」）⁷⁶」である。これは、欧州連合の「ネットワーク及び情報システム」指令（NIS 指令）に応じて

⁷⁵ <https://www.gov.uk/government/publications/national-cyber-strategy-2022>

⁷⁶ <https://www.legislation.gov.uk/ukxi/2018/506>

制定されたものであるが、現在、施行後のレビューがなされている。2020 年 5 月に発表されたレビュー⁷⁷では、規制がポジティブな影響を与え、規制の適用範囲である必須サービスの事業者と関連するデジタルサービス事業者のサイバーセキュリティへの投資を促進しており、また、規制によって、それらの必須サービス事業者のサイバーセキュリティレベルを大規模に把握する能力が向上し、どこに改善の必要性があるのかの根拠を示すのに役立ったとされた。また、NIS 規則の監視・執行権限、罰則制度、所轄官庁が発行するガイダンスによって上級管理職レベルでのセキュリティの優先順位が高まったと結論づけられた。もっとも、レビューでは、NIS 規則はセキュリティの改善につながるものの、組織はこれらの改善を加速させる必要があることが示唆された。また、サプライチェーンの脆弱性への対応、施行体制のさらなる整備と改善、新たな不服申立てメカニズム、所轄官庁へのサポートとガイダンスの改善など、改善可能な点が数多く提言された。その結果、2020 年に政府は、レビューの勧告の一部を実施するために、NIS 規則の改正を打ち出した⁷⁸。

この NIS 規則の改正案⁷⁹は、「柱 1：デジタルサービスプロバイダに関する条項の改正案」と、「柱 2：UK 将来に耐えうる NIS 規則の提案」からなる。

柱 1 の内容として、「デジタルサービス」の範囲を拡大し、「マネージドサービス」を含むようにすること、すべてのデジタルサービス事業者に対して、2 段階の監督体制を適用する（最も重要な事業者に対しては新たにプロアクティブな監督層を設け、それ以外の事業者に対しては既存のリアクティブな監督層を設ける）が提案されている。

柱 2 の内容としては、政府が適切な保護措置を講じた上で、規制の枠組みや範囲を更新できるよう、新たな権限委譲を行うこと、既に規制の対象となっている事業者が決定的に依存している特定の組織を NIS 規則の対象とするための新たな権限を創設すること、現在はサービスに影響を与えるインシデントに限定されている既存のインシデント報告義務を、その他の重要なインシデントも含むように強化すること、規制当局（例えば、Ofcom、Ofgem、ICO）が合理的な実施コストの全額を規制対象企業から回収できるように、既存のコスト回収規定を拡張すること、が提案されている。

2.4 その他英国におけるサイバーセキュリティに関する法的進展

その他の注目される動向としては、2021 年電気通信（安全保障）法の提案がある。これは、2003 年通信法を改正し、国務長官に国家安全保障の観点から、公共通信事業者に対して、その指示で指定された指定業者が供給、提供又は利用可能とする商品、サービス又は設

⁷⁷ 「2018 年 NIS 規則実施後のレビュー」（Post-Implementation Review of the Network and Information Systems Regulations 2018）

(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/960574/CCS207_CCS0320329850-001_Network_and_Information_Systems_Regulations_Post-Implementation_Review_Web_V2.pdf)

⁷⁸ このレビューに対してパブリックコメントがなされており(Call for views on amending the NIS regulations 2018 (<https://www.gov.uk/government/publications/call-for-views-on-proposed-amendments-to-the-network-and-information-systems-regulations/call-for-views-on-amending-the-nis-regulations-2018>)), 政令の改正もなされている(SI2020/1245)。

⁷⁹ <https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience>

備の利用を規制する指示を出すこと（指定業者指示）、国家安全保障の観点から、指定業者指示の発行のために人を指定する通知を発行すること（指定通知）の権限を与えるものである。現在、パブリックコメント募集が終了した段階⁸⁰である。

3 ドイツにおけるランサムウェア対応の進展

ここでは、ドイツにおけるランサムウェアについての事象報告、及び判例の動向を追う。

3.1 BSI ランサムウェア報告書（Ransomware Bedrohungslage, Prävention & Reaktion 2021）⁸¹

（1）概要

2020 年度の調査において、IT セキュリティ庁（BSI (Bundesamt für Sicherheit in der Informationstechnik)）が継続的に発行している Ransomware Bedrohungslage, Prävention & Reaktion 2019 に依拠しつつ、ランサムウェア対策の一般論を次の通り述べた。一般論については Ransomware Bedrohungslage, Prävention & Reaktion 2021（以下、「Ransomware 2021」）においても変わりはない。

ランサムウェアの被害として、会社の営業が害されること等によるコストという意味での固有の損害、レピュテーション侵害、さらに契約の相手方等の第三者への損害の 3 つがあると整理される（Ransomware 2021, 8）。ランサムウェアを用いる攻撃者の動機は金銭的な利益、（政治的、経済目的）破壊的活動、憂さ晴らし等がある（Ransomware 2021, 11）。

ランサムウェアについては、その再販により、2016 年以降、以前から知られていた方法がさらに広まった。潜在的な被害者の環境等への適応に向けて、ランサムウェアのサービスが（攻撃者により購入される仕組みの中で）提供されており、こうしたモデルは RaaS (Ransomware-as-a-Service) と呼ばれる（Ransomware 2021, 28）。さらに、ソフトウェア各機能（コンポーネント）のモジュール化が進み、脅威が増している（Ransomware 2021, 29）。BSI によれば、マルウェアや攻撃方法は攻撃者間で拡散し、成功事例がすぐに他の攻撃者に採用される、という。データを公開して被害者を脅迫する手法も 2019 年末には少数の攻撃者によって導入されたものであるが、2020 年の途中で標準的な手法になった（Ransomware 2021, 30）。

（2）具体的なインシデント

出版社である Funke Mediengruppe がランサムウェア「DoppelPaymer」の攻撃を受け、6,000 を超えるコンピュータシステムが感染し、配信障害が発生した事例があるが、さらにデュッセルドルフ大学病院事件⁸²等の計 3 件のインシデントが、死亡事故につながったとみることもできる点で重大である（Ransomware 2021, 13-14）。

⁸⁰ <https://www.gov.uk/government/publications/targeted-consultations-on-proposed-designated-vendor-direction-and-designation-notice/telecommunications-security-act-2021-draft-designated-vendor-direction-consultation>

⁸¹ <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf>

⁸² 以下の事案紹介は、次のサイトにもよった。<https://www.heise.de/amp/news/Hackerangriff-auf-Uniklinik-Duesseldorf-Ermittlungen-wegen-fahrtaessiger-Toetung-4904134.html?fbclid=IwAR0Hn3Xne99dgUOVK-6WUetYcFykPHgR0J5K52AEqAwDptSvLVgYgJVzEds>

デュッセルドルフ大学病院事件は、ハッカーの攻撃によって大学病院での IT 機器の停止が起きてしまった事件である。当該病院の 30 のサーバー上のデータが暗号化され、サーバー上に攻撃者の恐喝のメッセージが残されていた。攻撃者は、当該メッセージで、自身に連絡をとるように求めている。警察が実際に攻撃者にコンタクトをとり、同人に、あなたの犯罪的なハッカー攻撃によって大学ではなく病院が被害を被った、それにより、病院の患者が重症化してしまったと通知した。すると攻撃者は恐喝を撤回し、(サーバー上の) データをもう一度復号可能なデジタル鍵を交付した。本件においては、攻撃者のメインの標的は大学病院ではなく、大学病院は偶然に被害を受けてしまったただだと推測されている。この攻撃の後に、治療が遅れてしまった患者が死亡した。VPN 製品の脆弱性を突いた攻撃であり、攻撃の 8 か月前からパッチが提供されてはいたが、既に攻撃者によりバックドアが組み込まれていたため、数か月経っても攻撃が可能な状態にあったと分析されている。鍵の提供を受けたにもかかわらず、病院側でのシステムの復旧には数週間かかった。

(3) ランサムウェア対策

ランサムウェア対策は、Ransomware 2021, 16 以下において、予防、対応に分けて論じられる。予防においては、感染を予防する方策（迅速なソフトウェア・アップデート、不要なプログラムのアンインストール等による攻撃範囲の最小化、スパムメールの取扱い、管理者アカウントの安全な取扱い（同アカウントで不要なことはしない）、ウイルス対策等）、バックアップ、従業員の意識改革、といった観点から論じられる。技術的な推奨事項だけでなく、従業員への啓蒙も重要だとされている。例えば、意識向上キャンペーンや従業員のトレーニングにおいては、悪意のあるプログラムの感染方法について、電子メールの添付ファイルを誤って開くことによる侵入や、信頼されていないウェブサイトへのアクセス（ドライブバイエクスプロイト）という 2 つの重大な感染方法が常に問題とされる。特に、被害者側の誤った行動は、ソーシャルエンジニアリングによる場合もある。私的な関係を装ったり、利益を約束したりするソーシャルエンジニアリングに対しては、レポートやニュースを盲目的に信頼しないということが何よりも重要である。どんなに魅力的であっても、当該ニュース等を信頼して、求めに応じてクリックなどしてはならない。例えば Ransomware 2021, 20 では、怪しい事象に遭遇した場合には、クリックではなく、そこに書いてある連絡先に電話をしてみることを推奨している。

対応については、身代金の要求に対し十分な準備をし、毅然とした態度をとり、攻撃者に動機付けを与えないためにも支払いをしないこと、警察に刑事事件としての申立てを行うこと、インシデント対応、外部のエキスパートの支援があげられている（Ransomware 2021, 23）。

3.2 コンピュータ・サボタージュ罪の動向等

(1) 刑法の規定

ドイツにおいては、データの変更やこれに基づくデータ処理の妨害を直接処罰する規定

群（刑法第 303 条 a、第 303 条 b）がある⁸³。

刑法第 303 条 b は、コンピュータ・サボタージュという刑法第 303 条 a よりも重い犯罪類型を規定している。刑法第 303 条 b 第 1 項第 1 号で、刑法第 303 条 a が参照されていることに着目してほしい。刑法第 303 条 a の行為により、「他人にとって重要な意味をもつデータ処理を、」「著しく妨害」した場合に刑法第 303 条 a よりも厳しく罰せられる。日本の刑法では妨害とでいう場合、現実には妨害がなされる必要はない、と理解されることが多いが（業務妨害罪ではそのような理解がなされている⁸⁴）、ドイツでは、現実の妨害が要求される。

既に、以前の報告書において、ランサムウェアの使用は、データ変更罪（刑法第 303 条 a 「隠匿」（処分権者のアクセスを排除して利用できなくさせること（BT-Drs.10/5058, 34））の類型にあたる、とされていること⁸⁵、コンピュータ・サボタージュ罪（刑法第 303 条 b）に該当し得ること⁸⁶も紹介していた。

（2）ランサム使用事案への適用

そのような中で、ドイツの連邦通常裁判所（Bundesgerichtshof, BGH。我が国でいうところの最高裁判所）は 2021 年 4 月 8 日、ランサムウェアの使用事案において刑法 303 条 b を適用できる旨の決定を下したので（BGH, Beschluss vom 8.4.2021 – 1 StR 78/21）、以下に要約的に紹介する。

事案の概要は次の通りである。被告人が属する犯罪グループは、ウェブサイト上の広告

⁸³ 刑法第 303 条 a（データの変更）

(1) 違法にデータ（第 202 条 a 第 2 項）を、消去、隠匿、利用不能化、又は変更する者は、2 年以下の自由刑又は罰金に処する。

(2) 未遂は罰する。

(3) 第 1 項に定める犯罪行為の予備について、第 202 条 c を準用する。

刑法第 303 条 b（コンピュータ・サボタージュ）

(1) 他人にとって重要な意味をもつデータ処理を、次のいずれかの方法で、著しく妨害する者は、3 年以下の自由刑又は罰金に処す。

1. 刑法第 303 条 a 第 1 項の行為をする

2. 他人に不利益を与える目的で、データ（刑法第 202 条 a 第 2 項）を入力又は送信する、

3. データ処理装置又はデータ媒体を破壊、損壊、利用不能化、隠滅又は変更する

(2) 他人の営業、他人の会社、又は官庁にとって重要な意味をもつデータ処理が問題になる場合には、刑は 5 年以下の自由刑又は罰金である。

(3) 未遂は罰する。

(4) 第 2 項のうち特に重大な事案においては、刑は 6 月以上 10 年以下の懲役である。特に重大な事案は、通例、次の場合である。

1. 行為者が大規模な財産的損害を惹起する場合

2. 業として、又はコンピュータ・サボタージュを継続的に実行するために結成された集団の構成員として行為する場合

3. 行為により、全住民の生活上重要な物若しくは役務の供給又はドイツ連邦の安全を害する場合

(5) 第 1 項に基づく犯罪行為の予備について、第 202 条 c を準用する。

⁸⁴ 西貝吉晃「サイバー・フィジカル・セキュリティの維持に関する政策的議論及び罰則の現況」千葉大学法学論集 36 巻 1 号 160 頁、130 頁（2021）(<https://opac.ll.chiba-u.jp/da/curator/900119534/>)

⁸⁵ Tobias Singelstein/Louisa Zech in Hornung/Schallbruch, IT-Sicherheitsrecht, Rn 66.

⁸⁶ Salomon, Cybercrime und Lösegeld - Strafbarkeit der Zahlung von Lösegeld als Reaktion auf Erpressungstrojaner, MMR 2016, 575, 576.

をクリックすると、ユーザーの意思によらずにマルウェアがダウンロードされて被害者のコンピュータにインストールされるようにした。これに感染すると、感染したコンピュータに、国家機関のロゴを表示することであたかも公式に遮断しているような印象を与えるロック画面が送信されて、コンピュータはロックされてしまい、電子決済システム用いた100ユーロ相当の支払いを要求された。このグループは多くのサーバーを利用してランサム攻撃をしかけ、結局、2013年から2016年の間に全世界で2億ものコンピュータシステムが感染し、900万ユーロ以上の金銭が送金された。被告人は、このグループにおいて、システム管理者及び技術コンサルタントの仕事をしていた者であった。ここでは、(被告人の共犯としての責任の問題ではなく、) グループとして起きた被害を刑法第303条bで捕捉できるか、ということについての判断が示された。

BGHは、まず、刑法第303条aの適用に関し(上記の通り、刑法303条b第1項1号で刑法303条aが参照されている)、被害を受けたコンピュータシステムのレジストリファイルへの干渉(エントリの追加)により、ユーザーが気づかないうちに、画面全体と他の全てのウィンドウがロック画面で覆われ、タスクマネージャへの全ての呼出しが悪意のソフトウェアによって終了させられる程度にデータが変更されたと評価した。

その上で、刑法第303条bに固有の要件のうち、まず、妨害対象となる「他人にとって『重要な意味をもつ』データ処理」について、機器上のデータの利用が不可能になり、データの完全な喪失を伴うOSの再インストールによってのみコンピュータを使えるようになったことに加え、さらに、多くの場合にコンピュータのユーザーが(ランサムウェアの恐喝に対して)支払いを行ったことで恐喝が成功したという間接事実も用いて、この要件に該当すると説示した。

次に、結果要件である「著しい妨害」について、当該ロック画面がハードディスク(内のデータ)の削除、及びOSの再インストールによってしか解除できなかったがゆえに、コンピュータへの感染は、同コンピュータ上に保存された全てのデータの不可逆的喪失に結びついており、これも充たすと説示した。

以上により、刑法第303条bの罪が成立するとされた。

ドイツ刑法第303条aは我が国の電磁的記録毀棄罪(刑法第258条、第259条)に、ドイツ刑法第303条bは我が国の電子計算機損壊等業務妨害罪(刑法第234条の2)に対応しているとみることが不可能ではないものの、ドイツ刑法の方が、データやデータ処理システムのセキュリティを直接保護している犯罪類型だといえる。これらの犯罪類型を用いた処罰が行われていることは、規定のポテンシャルを活かせるか、という観点からして示唆的である⁸⁷。

4 ランサムウェア対応について国際的な動向

ランサムウェア対応は、国際的な問題としても注目を集めている。Revilの構成員の逮捕、

⁸⁷ 刑法第303条bについて、詳しくは西貝吉晃「コンピュータ・サボタージュ罪刑法303条b—ドイツ刑法典の改正(2)」刑事法ジャーナル71号97頁(2022)を参考にされたい。

G7 の動向、国際的な法執行機関の動向などを以下にまとめる。

4.1 コロニアルパイプラインの犯人グループの逮捕について⁸⁸

ロシア連邦保安庁（FSB）安全保障局は犯罪グループ「REvil」のメンバーを逮捕起訴している。具体的には、2022 年 1 月 14 日に、14 名が逮捕され⁸⁹、その後、1 月 15 日に 3 名⁹⁰が逮捕されたと発表されている⁹¹。1 月 14 日の報道によると、メンバーの居住地で、4 億 2600 万ルーブル、60 万ドル相当の暗号通貨、PC、暗号通貨ウォレット、20 台の高級車等を押収した。容疑は、ロシア連邦法第 187 条 2 項の決済手段の違法流通である。

その後、拘留に対しての異議がなされるものの、異議は認められず、また、容疑者は容疑を認めている⁹²。

また、2021 年 10 月 8 日にポーランドで逮捕された Yaroslav Vasinskyi 容疑者は、2022 年 3 月 3 日にアメリカに犯罪人引渡しがなされている⁹³。

4.2 G7 等の動向

G7 の「G7 コーンウォール・サミット首脳コミュニケ（骨子）」⁹⁴においては、将来的な先端領域の課題として、「身代金目的のサイバー攻撃（ランサムウェア）の犯罪ネットワークによる脅威の高まりに緊急に対処」するとされている。

国際的には、国際ランサムウェア対抗イニシアチブ⁹⁵が結成されており、2021 年 10 月 13、14 日に会議が開催されている⁹⁶。その共同声明によると、各国政府は、ランサムウェアのリスクを低減するために、緊急の行動、共通の優先事項、及び相互補完的な取り組みが必要であることを認識していることが明らかにされた。具体的な取り組みとして、可能な限りインシデントを防止し、インシデント発生時に効果的に対応するためのネットワーク回復力の向上、身代金の支払いを洗浄するための金融メカニズムの乱用やランサムウェアを収益化するその他の活動への対処、ランサムウェアの行為者を捜査・起訴する法執行機関の協力、ランサムウェア犯罪者の隠れ家への対処、継続した外交関与によるランサムウェアのエコ

⁸⁸ 以下は、この案件についてのタス通信の報道をまとめたものである。

⁸⁹ <https://tass.ru/proisshestviya/13431243>。2 名の逮捕については、<https://tass.ru/proisshestviya/13434909>。この逮捕されたメンバーについては、コロニアルパイプラインの犯人であると報道されている。日本語の記事では、「ロシア当局、REvil ランサムウェア攻撃集団を逮捕したと発表」

(<https://www.itmedia.co.jp/news/articles/2201/17/news075.html>)

⁹⁰ <https://tass.ru/proisshestviya/13437117>

⁹¹ 「ロシア当局、REvil ランサムウェア攻撃集団を逮捕したと発表」

(<https://www.itmedia.co.jp/news/articles/2201/17/news075.html>)

⁹² <https://tass.ru/obschestvo/13598921>

⁹³ Sodinokibi/REvil Ransomware Defendant Extradited to United States and Arraigned in Texas”

(<https://www.justice.gov/opa/pr/sodinokibirevil-ransomware-defendant-extradited-united-states-and-arraigned-texas>)

⁹⁴ <https://www.mofa.go.jp/mofaj/files/100200458.pdf>

⁹⁵ 構成国は、オーストラリア、ブラジル、ブルガリア、カナダ、チェコ、ドミニカ、エストニア、欧州連合、フランス、ドイツ、インド、アイルランド、イスラエル、イタリア、日本、ケニア、リトアニア、メキシコ、オランダ、ニュージーランド、ナイジェリア、ポーランド、韓国、ルーマニア、シンガポール、南アフリカ、スウェーデン、スイス、ウクライナ、アラブ首長国連邦、英国、米国である。

⁹⁶ その内容については、「ランサムウェア対策イニシアチブ会合 2021 年 10 月閣僚・代表者共同声明」

(<https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/>)

システムの撲滅、などに今後取り組んでいくことが明らかにされている。

その後、2021 年 12 月 15 日、16 日に G7 の内務担当、安全保障担当高官によるランサムウェアに関する臨時フォーラムが開催されている⁹⁷。この会議は、オンラインで開催されたもので、G7 の高官に加えて、欧州評議会、欧州委員会、欧州連合サイバーセキュリティ機関、欧州警察、金融活動作業部会、G7 サイバー専門家グループ、サイバー専門家グローバルフォーラム、インターポール、国連薬物犯罪事務所からの代表者が参加した。

この議長要約が公表されている⁹⁸。それによると、脅威、政策によるアプローチ、暗号通貨、レジリエンスとコミュニケーションについて、次のステップの項目で議論がされている。

脅威においては、ランサムウェアは、最も重要かつ拡大している脅威の一つであること、また、ランサムウェアは複雑な犯罪形態であること、ランサムウェアグループは、Ransomware as a Service (RaaS)モデルを運用していることなどが議論されている。

政策的アプローチにおいては、国境を越えた問題であるため、いかなる解決策も G7 メンバーと国際的なパートナーとの間で緊密に調整される必要があること、解決策を迅速に進め、多面的かつ多部門にまたがるアプローチをとる必要性があること、受け取った情報の共有について協力する必要性を認識していることが論じられている。

暗号通貨については、ランサムウェアの攻撃者は、暗号資産のエコシステムからロンダリングして「現金化しようとしており、G7 が民間セクターと協力して、ランサムウェア攻撃による金銭的報酬の可能性を最小限に抑えることができれば、犯罪者がランサムウェア攻撃を行うインセンティブを減らすことができることが明らかにされている。

レジリエンスとコミュニケーションにおいては、サイバーインシデントは、シンプルで実行可能なステップを踏むことで相当程度防ぐことができること、セクターや組織がより安全で、サイバー脅威に対する回復力を持つように取り組むことが優先事項であること、そのために、官民一体となった投資が必要であること、が達成さるべきであるとされている。そして、そのために、効果的なコミュニケーションが重要なツールとなるとされる。

これらの認識のもとに、次のステップとして、G7 と参加国際機関は、ランサムウェアのリスクを低減するための集団的な取り組みを引き続き優先させる必要性を認識し、ランサムウェア対策イニシアチブなどの既存のイニシアチブの継続的な活動を補完し、集団的に脅威に対処し、我々の協力を深めるために、さらなる作業の優先分野を共に特定したとされている。

4.3 法執行機関の動向

ランサムウェア対応のためのユーロポール（Europol、欧州刑事警察機構）の活動を見ていく。とくに、ユーロポールでは、対応のために欧州サイバー犯罪センター（EC3）を

⁹⁷ 日本語の記事だと「G7 内務担当、安全保障担当高官によるランサムウェアに関する臨時フォーラム」(<http://maruyama-mitsuhiko.cocolog-nifty.com/security/2021/12/post-9a4f85.html>)

⁹⁸ <https://www.gov.uk/government/publications/g7-interior-and-security-senior-officials-meeting-on-ransomware/chairs-summary-from-the-g7-interior-and-security-senior-officials-extraordinary-forum-on-ransomware-on-15-and-16-december-2021>

2013年に創設しており、共同サイバー犯罪行動タスクフォース（J-CAT）を運営している。

EC3とJ-CATの共同のプロジェクトによるボットネット対応の執行事件としてはOperation TALPA、Operation FIFTH ELEMENT、Operation GOLD DUST/ QUICK SAND等がある。

EC3は、「インターネット組織犯罪脅威評価」（Internet Organised Crime Threat Assessment）を発表している⁹⁹。2021年の報告書においては、COVID-19のパンデミックによる影響がまだ認められること、ランサムウェアのアフィリエイトプログラムにより、より多くの犯罪者グループが、DDoS攻撃などの多層的な恐喝手法で大企業や公共機関を脅し、攻撃することが可能になっていること、モバイル端末向けマルウェアは、2要素認証などの追加的なセキュリティ対策を回避しようとするものに進化していること、オンラインショッピングによるオンライン詐欺が急増していること、また、露骨な自作自演はますます懸念され、営利目的の配信も行われていること、VPN、暗号化通信サービス、暗号通貨など、合法的なサービスを悪用する犯罪が後を絶たないこと、などが報告されている。

また、「ランサムウェア—知っておきべきこと」（“Ransomware: What you need to know A joint report by Check point and Europol”）¹⁰⁰は、ランサムウェアの状況とその種類に関する報告書である。

同報告書は、ランサムウェアとその初期の主要なタイプ（CryptoLocker、CryptoWall、TelaCrypt、CTB-Locker）を挙げたあと、現在の主たるタイプ（Locky、CryptXXX、TorrentLocker、Jigsaw、Cerber、Crysis）について説明している。近時の発展としては、「内部者のリクルートのために脅迫する—Deliah」、「指令・コントロールなしの暗号化—SamSam」、「完全なハードドライブの暗号化—Petya」、「同期化された攻撃—Cerber」、「オープンソースランサムウェア—LockLock」、「スパイフィッシング攻撃—RAA」、「ルーマニアからの脅威—NoobCrypt」、「Cerber そっくり—Razy5.0」、「EDA2の変種—Fantom」、「アンドロイド用のランサム—Dogspectus」、「Shade またの名を Encoder.858,Troldesh」、「Popcorn Time」が紹介されている。

同報告では、2016年には、その種類が増大していることについての統計を紹介した後、「ノーモアランサムプロジェクト」がなされていることが報告されている。また、ランサムウェア対応のためにすべきこと、してはならないこと（DOSとDON'TS）のインフォグラフィックが紹介されている。

4.4 WEFにおけるランサムウェアの報告

世界経済フォーラム（World Economic Forum）は、「グローバル・サイバーセキュリティ・

⁹⁹ <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021>

¹⁰⁰ <https://www.europol.europa.eu/publications-events/publications/ransomware-what-you-need-to-know>

アウトLOOK 2022」という報告書を公表している¹⁰¹。

同報告書は、「1 現状の調査」、「2 ギャップを埋める・サイバーとビジネス（Bridging the Gap）」、「3 エコシステムの確保」、「4 結論」から成り立っている。

「1 現状の調査」において、最も重大な脅威はランサムウェアの脅威であると特定している（同報告書 13 頁）。ランサムウェアの脅威は拡大の一途をたどっていることがデータで説明されている。2021 年の上半期において、151%の増加であるとしており、また、サイバーリーダーの 8 割が、ランサムウェアは公共の安全に対する危険な脅威であり、進化していると強調している。そして、今回の調査では、サイバーリーダーの 5 割がランサムウェアを最大の懸念事項として挙げ、ランサムウェア攻撃がサイバーリーダーにとって最重要課題であることが確認されている。

「2 ギャップを埋める・サイバーとビジネス（Bridging the Gap）」においては、サプライチェーン全体に影響を及ぼす攻撃の例として、2021 年にランサムウェアグループ「REvil」が遠隔監視・管理ソフトウェアプラットフォームの脆弱性を悪用し、実行したことが挙げられている。ランサムウェアが、サプライチェーン全体への悪影響が懸念されていることが強調されている。

「3 エコシステムの確保」においては、サイバーレジリエンスを確保することが重要であるということが強調されるとともに、ランサムウェアやゼロデイ悪用のような問題に対するイノベーションの重要性が強調されている。

¹⁰¹ <https://www.weforum.org/reports/global-cybersecurity-outlook-2022>

第2部 データの保存場所リスクの内容と評価

経済安全保障が意識される中、データの保存場所をめぐるリスク管理の観点から、個人データ保護以外の根拠である安全保障、自国産業保護・育成などの観点からの規制についての国際的な議論動向及び概観を調査する。

1 概念に関する国際的な議論動向

1.1 データのローカル化の概念

データのローカル化（Data Localization）というのは、「国境を越えた重要なデータの移転を制限する一連の動向」と定義することができる¹⁰²。我が国においては、2021 年国際的な議論動向について、データのローカル化については、データナショナリズム、スプリンターネットなどの概念とも関連して議論されている。

詳細を見ていくと、以下のような種々の仕組み¹⁰³があり、いずれもデータのローカル化とされる。

(1) 明示的なローカルデータ保存

企業はデータが発信された国に物理的にデータを置かなければならない、というものである。ただし、外国でデータを取り扱うことが可能な場合もある。

(2) ローカルデータのミラーリング

これは、企業が国外にデータのコピーを移転する前に、まずローカルにデータのコピーを保存しなければならない、というものである。

(3) 事実上の現地保存と処理

厳しいデータ移転要件（移転の事前承認や明示的な同意の取得など）やデータ移転に関する法的不確実性は、高額な罰金や恣意的な執行と相まって、企業にとっては受け入れがたいリスクとなるため、企業はデータを現地で保存する。

(4) 明確なローカルでのデータ保存・処理

これは、明文で各国が他国への移転を禁止している場合である。

(5) 現地での明示的かつ差別的なデータ処理、ルーティング、保管

これは一部の国で行われている措置であり、差別的なライセンス、認証、及びその他の規制制限を用いて、ローカルでのデータ保存を要求するものである。実質的に、外国企業が現地データの管理及び処理から完全に排除されることになる。

このデータのローカル化の正当化根拠としては、外国からの監視の回避、セキュリティ強化、プライバシーの保護、経済発展の促進、国内法執行の円滑化などが挙げられる（注の Chander 他 (2014)による）。詳細は、2.2.3 で述べる。

データのローカル化については、上述の Chander 他 (2014)以外にも、Drake (2016)¹⁰⁴、

¹⁰² Anupam Chander, Uyen P. Le 「ウェブを裂く・データのローカル化対グローバル・インターネット」 (Breaking the Web: Data Localization vs. the Global Internet) (以下、「Chander 他 (2014)」)。なお、Chander 他 “Data Nationalism” (2015) も同一の内容である。

¹⁰³ これは、後述の ITIF の報告書による。

¹⁰⁴ William J. Drake, “BACKGROUND PAPER for the workshop on Data Localization” and Barriers to Transborder Data Flows” (https://www3.weforum.org/docs/Background_Paper_Forum_workshop%2009.2016.pdf) (以下、

Sargsyan (2016)¹⁰⁵、Selby (2017)¹⁰⁶、Chander (2020)¹⁰⁷、Wu (2021)¹⁰⁸などの論文がある¹⁰⁹。

Chander 他 (2014)の論文は、各国の具体的な動きを挙げるとともに、結局、データのローカル化の根拠が実現されることはなく、むしろ、実際には、経済全体から見れば大きな損害をもたらすと分析する。これらの考察をもとに上記 Chander 他 (2014)は、データのローカル化を強制する努力は、個人をよりよく保護する努力から目をそらすことになり、より良い、より安全なインターネットをすべての人に提供するためにはデータをバラバラにする必要はない、という結論を導いている。また、Chander (2020)も、論旨は同様である。

Drake (2016)は、2016年9月14日及び15日に開催された世界経済フォーラムでの「データローカライゼーションと越境データフローへのバリア」ワークショップのために準備されたペーパーである。構成は、「1 歴史的背景・国家主権と越境データフロー」、「2 データローカライゼーションと越境データフローへのバリア」、「3 国際貿易協定及びその他の政府枠組み」から成り立っている。この報告書は、準備されたペーパーという性格もあり、ローカライゼーションと障壁の問題—その原因、形態、発生率など—と、影響を受ける当事者にある程度の秩序と救済を与えるための貿易と他のガバナンス環境における関連する取組みについての調査を提唱するものとなっている。また、理想的には、インターネット関係者、貿易関係者、学識経験者、政府関係者が参加するマルチステークホルダー・タスクフォースは、出発点が異なるステークホルダーグループのオピニオンリーダーを集め、対話を通じて、実質的・手続的な問題についての共通点を見出すことにより、創造的で効果的な提言を行うべきとしている。

Sargsyan (2016)は、データのローカル化を政府が、その政治的・経済的目的を追求する動きと中間媒体者の技術的・政策的インフラとしての動向との近況と競争利益と捉えている。

同論文は、国家、データのローカル化、監視・プライバシー・セキュリティを拡張するためのインフラの環境構築として、国家は、民間のプロバイダを通じて、データを収集するように努めていること、アメリカのNSAの監視プログラムが暴露されたスノーデン事件の後、対外の情報活動に対して国内でのインフラでの保存は、プライバシー・セキュリティの保護措置となっているという合意があることを述べている。これらをもとに中国、ロシア、フランス、ドイツのそれぞれのデータのローカル化の動きを概観している。これらの考察のもと、

「Drake (2016)」

¹⁰⁵Tatevik Sargsyan, “Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security,” *International Journal of Communication* 10 (2016) (<https://ijoc.org/index.php/ijoc/article/view/3854>) (以下、「Sargsyan (2016)」)

¹⁰⁶ John Selby “Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?” (<https://doi.org/10.1093/ijlit/eax010>) (以下、「Selby (2017)」)

¹⁰⁷ Chander, Anupam, “Is Data Localization a Solution for Schrems II?” (July 27, 2020). *Journal of International Economic Law*, Forthcoming, (<https://ssrn.com/abstract=3662626>, <http://dx.doi.org/10.2139/ssrn.3662626>) (以下、「Chander (2020)」)

¹⁰⁸ Emily Wu “Sovereignty and Data Localization” (<https://www.belfercenter.org/sites/default/files/2021-07/SovereigntyLocalization.pdf>) (以下、「Wu (2021)」)

¹⁰⁹ その他にも、個別の法域について、データのローカル化の実際について分析する論考もあり、また、ここ数年で、この分野に関する論考の数も増大している。その中で、引用等の多い論文をあげて分析している。

国内での処理が、外国の情報活動から免れて安全となるとは限らないこと、また、中間伝達者による技術の利用、セキュリティ・プライバシーポリシー、産業標準の確立等が望ましいこと、が提言されている。

Selby (2017)は、一般的な議論である Castro (2013)¹¹⁰と国別の規制にフォーカスする Chander 他 (2014)との間のギャップを埋めようとするものである。そこでは、「データローカライゼーションの概念」を簡単に説明した後、米国政府を含む米国の利害関係者がデータのローカライズに反対する根拠を探り、また、次世代地域貿易協定 (TPP、TTIP、TISA、RCEP、FRAAP) のうち、米国が推進するデータローカライゼーション禁止 (中国を除く) 協定 3 つと、中国が推進するデータローカライゼーション禁止協定 2 つでデータローカライゼーションがどのように争われたかを解説している。さらに、BRICs (ブラジル、ロシア、インド、中国) の国内法の枠組みの中でデータローカライゼーション政策を導入しようとする試みの成功と失敗を検証し、4 つの政策論争を分析している。

Wu (2021)は、新興技術 (クラウド、5G、AI) の局面からデータ主権とその重要性に注目し、データ主権の主張にデータのローカル化が用いられてきたことを論じている。それぞれのデータのローカル化のタイプを分析している。これには、①国内のみでの保存、通信、取扱 (ロシア、中国)、②国内への複製保存の必要 (インド)、③条件付制限 (EU、ブラジル) などがある。データのローカライゼーション政策は、益というより害を及ぼしているとい主張をしている。これらの政策は、技術的懸念 (セキュリティ、国内経済の保護、国内法執行の単純化、外国からの干渉の低下) などからなされる。しかしながら、セキュリティの向上には効果がなく、規制の簡素化にはほとんど寄与せず、それが課される市場に経済的な損害を与えていると分析する。もっとも、他国依存への懸念、外国政府への不信、コントロール喪失の懸念も挙げられる。結局、同論文は、技術的な懸念と価値の懸念の両方に焦点を当てる方策をとるべきであるとする。

1.2 類似の概念

(1) データナショナリズム

また、同様の概念がデータナショナリズムという概念のもとに語られることもある¹¹¹¹²。また、Kuner (2015)¹¹³は、データローカライゼーションとデータナショナリズムを同義として論じている。同書によると、データナショナリズムのほとんどは、2010 年以降に論じられるようになったものであって、特に、アメリカのスノーデンによる暴露以来のものであるとされる。もっとも歴史的には、1976 年にブラジルが、政府関係者に外国のコンピュータネットワークの利用の許可を求めたことがある。その後、カナダ、フランス、スウェーデン

¹¹⁰ DANIEL CASTRO, "How Much Will PRISM Cost the US Cloud Computing Industry?" (2013), Information and Technology Foundation (<http://www2.itif.org/2013-cloud-computing-costs.pdf>)

¹¹¹ Daniel Castro, "The False Promise of Data Nationalism", INFO. TECH. & INNOVATION FOUND. 1 (Dec. 2013). (<http://www2.itif.org/2013-false-promise-data-nationalism.pdf>)

¹¹² Anupam Chander, "Is Data Localization a Solution for Schrems II?" Journal of International Economic Law, Volume 23, Issue 3 (2020 年 9 月) 771-784 頁 (<https://doi.org/10.1093/jiel/jgaa024>)

¹¹³ Christopher Kuner, "Data Nationalism and Its Discontents," 64 Emory L. J. Online 2089 (2015) (<https://scholarlycommons.law.emory.edu/elj-online/25>)

は、個人データの越境フローについて懸念を示していた。同氏は、これらの動きを「情報主権 (informational sovereignty)」と呼んでいる。同氏は、また、データ保護に基づく規定を保護主義とみるアメリカの見解に異を唱えて、基本権の保護と保護主義を同視しないようにと主張している。また、経済的効率性を指摘する他の見解に対して「もしある国が、データナショナリズムによって促進されると信じる他の正当な価値を促進する代わりに、ある程度の経済効率を犠牲にしたいと決めたとしたらどうでしょうか？」という疑問を投げかけている。つまり、データのローカライズの欠点と同様に、データの自由な流れを可能にすることの利点に集中し、経済的・実地的な考慮だけでなく、基本的な価値観に基づいて議論することが重要であるとして、バランスのとれた議論を強調するという特徴がある。

(2) スプリンターネット

また、スプリンターネットは、別個の、私的な、自律的な空間として運営されている並列化したインターネットをさす概念である¹¹⁴。この概念は、2001年に Clyde Wayne Crews の “On My Mind” で明らかにされた。そこでは、古典派経済学での「コモンズの悲劇」と呼ばれる現象に対する対応策としてインターネットを私有化し分割することを意味した。「プライバシーやその他のガバナンスの問題に関して事前に規定された基本ルールが、規制や中央計画に取って代わる、独自の『スプリンターネット』への道を開く」とされていた¹¹⁵。

その後、スプリンターネットという用語は、より地勢学的な動きにより分断化されたインターネットを示す意味で使われるようになる。

そのような用法を示す代表的なものは、Malcomson (2016) である。同書は、現代戦争の仮想現実として、戦争の歴史において、デジタル信号が重要な役割を果たすに至るまでの経緯を概観している。その上で、コンピュータネットワークの発展、国家情報インフラなどのインターネットの利用の開始・増大を概観する。それらをもとに国際化とアメリカの力が、2000年代になって、変化していくこととなり、ロシアや中国の出現などを契機として、多極化していった姿を、スプリンターネットと呼んでいる。

Lemely (2021) は、インターネットは、バルカン半島化しているという。これは、悪いもので、止めなければならないとする。この具体的な状況として、ソフトウェアの国産化及び規制、ハードウェアネットワークの国産化、ネットワーク各国化 (Nationalizing) の観点ごとに分析している。同論文によれば、私たちは、インターネットを失いつつあり、「スプリンターネット」すなわち、会社によって国によって異なるバルカン半島化したコンピュータプロトコルのセットがそれにとり代わっているという。これは、国際化というプロジェクト

¹¹⁴ この用語を使うものとして Scott Malcomson, “Splinternet: How Geopolitics and Commerce Are Fragmenting the World Wide Web (English Edition)” (2016) (以下、「Malcomson (2016)」)、Mark A. Lemley, “The Splinternet,” 70 Duke Law Journal (2021) 1397-1427 頁 (<https://scholarship.law.duke.edu/dlj/vol70/iss6/3>) (以下、「Lemely (2021)」) がある。

¹¹⁵ Crews (2001) は、デジタル・コモンズに対する戦争は、さらなる規制を招き、劣化し時代遅れになったインターネットに拍車をかけることになる、分断化 (splintering) は、私たちの選択肢と富を増やす、また、私有財産の制度に決定的に依存している私たちの権利を保護することにもなるとしている。

を失いつつあることを意味しており、結末は破局的となりうるとしている。このような認識のもと、政府の検閲に耐えうる技術を促進すること、個人は、私的市場における高度な個人化に抵抗しなければならないこと、法はウォールドガーデン間の相互流用性を促進しなければならないこと、インターネットプラットフォームの競争を促進させるメカニズムを探さなければならないこと、を推奨している。この論文は、国家ごとによる分断のみならず、プラットフォームごとの分断をも検討の範囲としている点に特徴があるといえる。

2 具体的な法規制

2.1 ITIF 調査による各国の規制

データのローカル化について、各国の規制を広く検討したものとして、ITIF（Information Technology and Innovation Foundation）による報告書がある。ITIF は、米国ワシントン DC に本拠をもつシンクタンクである。その使命は、イノベーションを加速し、生産性を向上させ、成長、機会、進歩に拍車をかける政策ソリューションを策定し、評価し、推進することである。ITIF は、データのローカル化について、積極的な研究報告書を公表している。研究報告書には、2017 年¹¹⁶と 2021 年¹¹⁷のものがあって、それらを比較することが可能である。2021 年の研究報告書は、各国ごとにその規制の根拠を、①会計・税・金融、②個人データ、③電気通信、④緊急デジタルサービス、⑤政府及び公共、⑥その他、に分けて論じている。

この報告書やその他の国際的な論考をもとに、②以外の根拠による規制の状況を分けて洗い出している。

これらの根拠のうち、個人データの保護の根拠に関する各国の情勢については、我が国においても調査がなされている。その一方で、それ以外の事実を根拠とする規制については、依然として紹介・分析が十分であるとは思えないというのが報告者の見解である。そこで、上記二つの報告書のうち、2021 年における 62 国の分析（規制のべ 144）のうち、個人データ保護を除いた部分（のべ 80）をまとめることとする。

個人データ保護以外のローカル化の一覧を、世界の地域ごとにまとめた表は、附属文書 1 のようになる。

それぞれの規制を項目ごとにまとめると、表 1 の通りである。

表 1 規制の根拠ごとの数

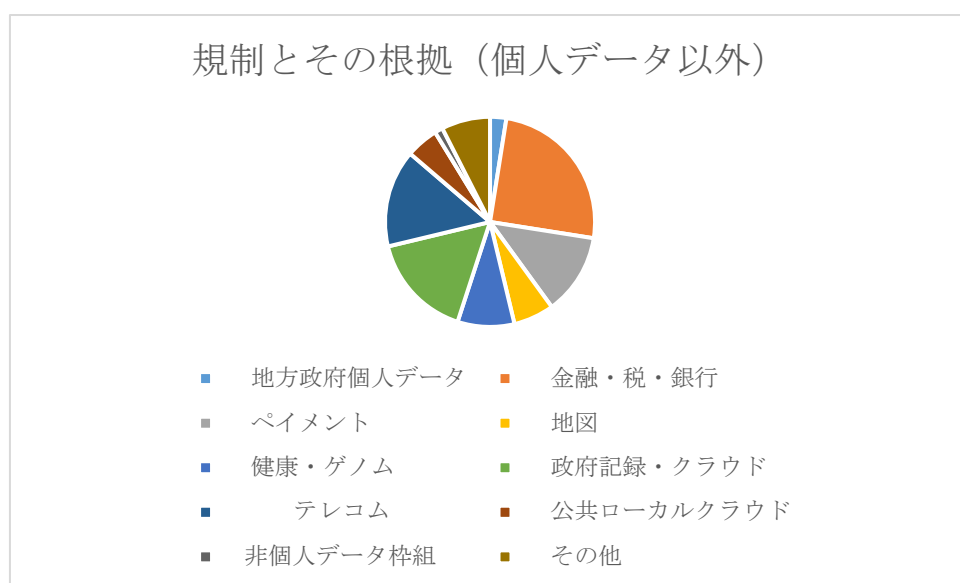
規制の根拠	規制の数 (のべ)
01 地方政府個人データ	2

¹¹⁶ “Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?” (2017)

(<https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>)

¹¹⁷ “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them” (2021) “<https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>”

02 金融・税・銀行	20
03 ペイメント	10
04 地図	5
05 健康・ゲノム	7
06 政府記録・クラウド	13
07 ICT テレコム	12
08 公共ローカルクラウド	4
09 非個人データ枠組	1
10 その他	6



なお、2017 年の 34 か国のデータを国別にまとめたものは、附属文書 2 として添付する。

2.2 比較からわかる近時の動向

ITIF の調査における 2021 年版と 2017 年版とを比較したときに、世界中で施行されているデータローカライゼーション施策の数は、4 年間で 2 倍以上に増えていること、そして、さらに数十カ国が検討中であること、が指摘されている。具体的な政策の数で行くと、多い国としては、中国（29）、インド（12）、ロシア（9）、トルコ（7）が挙げられている。

同調査において近時の傾向として指摘されている事項としては、(1) 政府によっては、特定の種類のデータの国外への移転を制限している場合が増加していること。具体的には、個人データ、健康・ゲノムデータ、地図・地理空間データ、政府データ、銀行・信用調査・金融・決済・税務・保険・会計データ、上場企業の社内データ、ソーシャルメディアやインターネットサービスプラットフォーム上のユーザー生成コンテンツに関するデータ、従来の電気通信及びインターネットベースの通信サービスの加入者データ・通信コンテンツ・メタデータ、電子商取引事業者データなどが含まれる。(2) 「機密」「重要」「中核」「国家安全保障」とみなされるデータなど、広範で曖昧なカテゴリーでデータを制限する国が増えつつあ

り、多くの場合、広範囲の商業データに影響を与えていること。(3) 事実上のローカライゼーションも進んでいること。これは、データ移転が非常に複雑で、コストが高く、不確実であるため、企業は基本的に、特に巨額の罰金に直面した場合、データをローカルに保存する以外の選択肢を持たなくなるということを意味している。この最も特徴的な例は、個人データ保護であり、一般データ保護規則（GDPR）は世界最大の事実上のローカライゼーション枠組みになっていると指摘されている。

2.3 根拠からみた具体的な法的規制

上述のように ITIF の 2021 年の報告書においては、データ保護以外の根拠として上述の 10 種類の根拠が挙げられている。これらを大きく分けたときに、プライバシーの保護、セキュリティ強化、経済発展の促進、外国からの監視の回避、国内法執行の円滑化などがある。

以下、これらの根拠ごとに当該規制を採用している国を挙げ、具体的な規制について代表的なものを 2021 年報告書に従って紹介する。

(1) 経済発展の推進

これは、サイバー主権（データ主権又はデジタル主権とも呼ばれている）という名のもとに、行われるものであって、その実質は、企業にローカルにデータを保存することを強制することで、国の機関、そして自国の企業や人々の機関を強化できるという保護主義的な主張であるということになる。このような観点からは、上の分類でいうと、「③ペイメント（決済）」に関する規制を挙げることができる。また、「⑦ICT テレコム」もこの根拠による場合も多いと考えられる。

「③ペイメント（決済）」についての規制がなされている国としては、

1	アフリカ 01	Ghana	ガーナ
3	アフリカ 03	Nigeria	ナイジェリア
8	アフリカ 06	South Africa	南アフリカ
27	ヨーロッパ 15	Russia	ロシア
33	ヨーロッパ 17	Turky	トルコ
45	南アジア 2	India	インド
60	東南アジア 4	Vietnam	ベトナム
63	南中央アメリカ 2	Chilie	チリ
66	南中央アメリカ 4	Venezuela	ベネズエラ
68	中国	China	中国

がある。

この規制の具体的な国における規制のうち、いくつかをみると、例えば、ガーナでは、2019 年にガーナ決済システム法及びガイドラインが定められ、決済システム運営ライセンス制度が導入された。そこでは、現地法人及び現地の 30%の資本、取締役には、最低でも 3 名のガーナ人、一人は CEO であることが求められている。2018 年に、ガーナは、すべての国内取引を Ghana Interbank Payment and Settlement Systems Limited（GhiPPS、ガーナ中央銀行

が 100%出資) で処理することを義務付ける規制案を発表したが、産業界からの懸念が大きかったため、最終的な実施指令はまだ出されていない。トルコは、PayPal などのインターネット決済サービスに対し、すべてのデータをトルコ国内で 10 年間保存することを義務付ける法律 (決済及びセキュリティ決済システム、決済サービス、電子マネー機関に関する法律) を制定した。インドでは、2018 年にインド準備銀行が、すべての決済をインド国内で保存することを強制する規則を制定した。もっとも、規制の根拠としては、データ侵害のリスクを減らすために決済データの「継続的監視と監督」の必要性を挙げており、規制監督とサイバーセキュリティに関する懸念であった。また、処理が海外で行われた場合、データは海外のシステムから削除され、決済処理から 1 営業日又は 24 時間のいずれか早い方までにインドに持ち帰る必要があるとされた。

また、「⑦ICT テレコム」による規制がなされている国として、

4	アフリカ 03	Nigeria	ナイジェリア
6	アフリカ 04	Rwanda	ルワンダ
19	ヨーロッパ 8	Germany	ドイツ
20	ヨーロッパ 9	Greece	ギリシア
29	ヨーロッパ 15	Russia	ロシア
35	ヨーロッパ 17	Turky	トルコ
41	中央アジア 1	Kazakhstan	カザフスタン
49	南アジア 2	India	インド
54	東南アジア 1	Indonesia	インドネシア
61	東南アジア 4	Vietnam	ベトナム
71	中国	China	中国
80	北アメリカ 3	US	アメリカ合衆国

が挙げられる。

インドは、National Telecom Machine-to-Machine (M2M) ロードマップを発表し、インドの顧客にサービスを提供する関連ゲートウェイとアプリケーションサーバーをすべて国内に設置することを要求した (2015 年)。ただし、このロードマップはまだ実施されていない。

インド国家安全保障会議は、すべてのメールプロバイダに対し、インドでの業務に必要なローカルサーバーの設置を義務付け、インド国内の 2 人のユーザー間の通信に関わるすべてのデータを国内に残すことを義務付けることにより、データのローカル化を制度化する政策を提案した (2014 年)。

ベトナムでは、2020 年インターネットサービス及びオンライン情報の管理、提供及び使用に関する政令第 72 号によって、特に、外国のソーシャルメディアプラットフォーム、アプリストア・プラットフォーム、アプリ内取引決済、その他ユーザー ID 確認技術を使用する必要のあるすべての事業者を規制すること、ベトナム国内にキャッシュサーバーを持つ国内通信会社と外国のプラットフォームの両方に新しい義務を導入し、外国のプラットフ

フォーム上の不快なコンテンツに対する責任を負わせることを提案している。

(2) 外国からの監視の回避

これは、外国においてデータが保存される場合には、その保存場所の外国国家によって検閲・監視がなされる可能性があるということを根拠としている。このような懸念に基づく規制は、ITIF 報告書の分類によると、「①地方政府個人データ」、「⑥政府記録・クラウド」、「⑧公共ローカルクラウド」がある。また、「⑤健康・ゲノム」もこの根拠によるものと考えられる。外国国家による利用のおそれという観点からは、「④地図データ」もこの分類に該当する。

「①これらの規制の具体的な国における規制をみると、地方政府個人データ」については、カナダとアメリカ合衆国がある。

カナダの2つの州、ブリティッシュコロンビア州とノバスコシア州は、2003年、学校、病院、公共機関などの公的機関が保有する個人データは、一定の条件を満たさない限り、カナダ国内でのみ保存、アクセスすることを義務付ける法律を施行した。また、63の異なる機関に対する電子メールを含む連邦政府のICTサービスを統合するプロジェクトの入札では、契約企業にカナダ国内でのデータ保存が義務付けられた。これは、国家安全保障上の理由を根拠とするものである。

アメリカでは、ロサンゼルス市が Google に米国内でのデータ保存を要求した(2009年)。

「⑥政府記録・クラウド」については、

5	アフリカ 04	Rwanda	ルワンダ
7	アフリカ 05	Senegal	セネガル
14	ヨーロッパ 4	Denmark	デンマーク
15	ヨーロッパ 5	European Union	欧州連合
17	ヨーロッパ 7	France	フランス
23	ヨーロッパ 12	Netherland	オランダ
28	ヨーロッパ 15	Russia	ロシア
43	南アジア 1	Bangladesh	バングラデシュ
48	南アジア 2	India	インド
53	東南アジア 1	Indonesia	インドネシア
58	東南アジア 3	South Korea	大韓民国
62	南中央アメリカ 1	Brazil	ブラジル
79	北アメリカ 3	US	アメリカ合衆国

がある。これらの規制については、地域的な特徴はあまりないといえよう。

フランスでは、行政機関が作成したデータは、アーカイブと考えられ、国内で保存するため、「主権」のない（つまり外国の）クラウドに保存することはできないとする大臣通達が発表された(2016年)。

インドネシア通信情報技術省は、2021年度の中央政府機関のサードパーティクラウドサ

ービス利用に関する大臣通達 No.3/2021 を発表した。同通達では、公的機関が利用できるサードパーティクラウドプロバイダについて、インドネシア国内の異なるデータセンター拠点に少なくとも 2 つの可用なゾーンを持つこと、暗号鍵をインドネシア国内に保管することなど、13 項目のセキュリティ基準を定めている。

韓国のクラウドセキュリティ保証プログラム（CSAP、公共機関向けクラウドサービスを規定）では、クラウドシステムとデータの物理的な保管場所は韓国国内のみとすること、公共機関向けクラウドサービスと民間機関向けクラウドサービスエリアを物理的に分離することなどが規定されている（2019 年）。

「⑧公共ローカルクラウド」については、

30	ヨーロッパ 15	Russia	ロシア
39	中東北アフリカ 2	Saud Arabia	サウジアラビア
65	南中央アメリカ 3	Peru	ペルー
77	北アメリカ 2	Mexico	メキシコ

がある。

ペルーの AI 国家戦略草案では、公的資金で賄われるすべてのプロジェクトに、ペルー国内にインフラを持つデータセンターやクラウドプラットフォームの利用を推奨している（2021 年）。

メキシコ中央銀行（Banxico）と国立銀行証券委員会（CNBV）は、企業にメキシコに拠点を置くクラウドプロバイダのみを選択するよう強制するフィンテック規制（電子決済基金機関に適用される規定）の草案を公表している（2020 年）。その第 50 条では、現地でのデータ保存の要件を課し、第 49 条は、決済・金融機関が利用できるクラウドコンピューティングサービスを決定するために、高度な裁量と透明性に欠ける規制承認モデルを確立するものである。

「⑤健康・ゲノム」については、

2	アフリカ 02	Kenya	ケニア
37	ヨーロッパ 18	United Kingdom	連合王国（イギリス）
40	中東北アフリカ 3	United Arab Emirates	アラブ首長国連合
47	南アジア 2	India	インド
52	東南アジア 1	Indonesia	インドネシア
70	中国	China	中国
73	オセアニア 1	Australia	オーストラリア

がある。

イギリスにおいては、National Health Service の情報ガバナンスルール（2014 年）によると、NHS のデータを海外に保存することは違法ではないが、それを行うことはリスク要因と見なされるため、推奨されないとされている。

オーストラリアの個人用電子健康記録法（2012 年）では、個人の健康記録をオーストラ

リア国内でのみ保存することを義務付けている。

(3) 国内法執行の円滑化

これは、国内外の企業に法執行機関や金融規制当局からのデータ要求に応じてもらうための唯一の方法がデータのローカル化であるという考え方を根拠とするものである。上記報告書の分類によると「②金融・税・銀行」にあたる。

10	ヨーロッパ 1	Belgium	ベルギー
13	ヨーロッパ 4	Denmark	デンマーク
16	ヨーロッパ 6	Finland	フィンランド
18	ヨーロッパ 8	Germany	ドイツ
21	ヨーロッパ 10	Italy	イタリア
22	ヨーロッパ 11	Luxemburg	ルクセンブルグ
26	ヨーロッパ 15	Russia	ロシア
31	ヨーロッパ 16	Sweden	スウェーデン
32	ヨーロッパ 17	Turky	トルコ
36	ヨーロッパ 18	United Kingdom	連合王国（イギリス）
38	中東北アフリカ 1	Algeria	アルジェリア
42	南アジア 1	Bangladesh	バングラデシュ
44	南アジア 2	India	インド
51	東南アジア 1	Indonesia	インドネシア
55	東南アジア 2	Malaysia	マレーシア
56	東南アジア 3	South Korea	大韓民国
59	東南アジア 4	Vietnam	ベトナム
67	中国	China	中国
74	オセアニア 2	New Zealand	ニュージーランド
76	北アメリカ 2	Mexico	メキシコ

これらの規制の具体的な国における規制を見ていく。

欧州の例をいくつか挙げると、ベルギーでは、1992 年付加価値税法第 60 条によって、インボイスは、ベルギー又は他の EU 加盟国で保管されなければならないとされた。2005 年会社法第 463 条によれば、株主名簿と社債明細書を事務所に保管しなければならないが、2005 年以降は、当該事務所で容易にアクセスできる限り、電子的に保管することができる定められている。また、デンマークにおいて、2007 年 監査法（第 45 条）によると、政府機関の財務記録は国内で保存しなければならない（ただし、毎月コピーを作成し、デンマークで保管する限り、海外でも保管可能である）。また、2006 年簿記法（第 12 条）によると、財務記録はデンマーク又は北欧諸国のいずれかに保存しなければならないとされている。ドイツでは、2013 年税法によると、帳簿や記録の保存が必要な個人及び企業は、ドイツ国内で保存しなければならない（多国籍企業にはいくつかの例外がある）。

ニュージーランドの内国歳入庁は、企業に対し、事業記録を現地のデータセンターに保存することを義務付けている（2010年）。

なお、「②金融・税・銀行」に関していえば、国の決済システムは国の重要なインフラの一部であり、グローバルな決済ネットワークを利用することは、その国の決済サービスではないため、システミックリスク、地政学的リスク、ソブリンリスクになるというのを根拠とする場合もある。この最も代表的な例としてはロシアがあり、2022年のロシアのウクライナ侵略に伴うSWIFTからの排除が現実化した。そのような場合に備えようとするものであった。

3 データのローカル化をめぐる議論

上記の根拠が事実によって支えられているのか、という点については、反対論も強いところである。以下、具体的に、それらの根拠ごとに議論を見ていく。

3.1 データのローカル化の根拠の有無について

（1）経済発展の推進

これについては、このようなデータのローカル化が地域の経済発展につながるのかという根本的な疑問が提起されている。

この点については、経済、ガバナンス、社会、政治的な要因が複雑に絡み合っており、デジタル問題に対する国家の立場を決定しているという点を見逃していること、データのローカル化によって得られるエージェンシーはせいぜい幻想に過ぎないこと、特に、権威主義的な国の場合、データのローカル化を支援する機関が監視や社会的・政治的統制に関与する機関であることを考えると、それは我田引水であることなどが指摘されている¹¹⁸。また、ローカルのデータセンターは、規模の経済が働かないために価格が高くなってしまいうこと、また、ローカルのデータセンターが技術的な能力やインフラを十分に提供できるとは限らないこと、も指摘されている¹¹⁹。

（2）外国からの監視の回避

外国からの監視を避けるためという根拠が挙げられているものの、これに対しては、権威主義的な動機をもとになされている場合には、「国家の安全保障、社会秩序と安全、社会倫理、コミュニティの健康を守るためという、広範かつ漠然」の根拠のもとに、むしろ、「情報を政府の管理下に置き、政府が個人を特定し脅すことを可能にすることで政治的抑圧を可能にし、プライバシー、データ保護、表現の自由に影響を与える」ものとして認識される¹²⁰という批判がなされている。また、米国の諜報活動は、米国域外においてもなされているし、また、欧州においても欧州域内に保存されているから欧州の監視から免れるわけではないとされている。マルウェアによる外国情報の取得も行われているし、秘密裏の情報収集は、当然に行われているとされる。そして、よりセキュリティの弱いローカルの企業がデータを

¹¹⁸ これらは、2021年ITIF報告書。

¹¹⁹ Shelby (2017) 229頁。

¹²⁰ 2021年ITIF報告書（「データ主権」は、デジタル保護主義に代わる主要な動機付け）。

取り扱うこともあり、従って、外国からの監視を避けるためという理由が単純に成り立つわけではないとされる¹²¹。

(3) 国内法執行の円滑化

これは、企業は単にデータを国外に転送するだけで監督やデータ要求を回避でき、どの国の法律に従うか、従わないかを選択するという点で、ある種の規制や法律の選定を追求できるという考えを根拠としており、これは誤りであると批判される。このような法執行は、誰がデータに責任を持つかという観点からなされるものであって、データの保存場所がどこになるのかということで影響を受けるものではない¹²²ということがこの批判の根拠となる。

3.2 経済的な厚生低下

産業への影響としては、データの流れを制限することは、その国の経済に統計的に大きな影響を及ぼし、貿易総量を大幅に減らし、生産性を低下させ、データにますます依存する下流産業の価格を上昇させることになること、が指摘されている。

この点を実証的に論じているのは、ITIF の報告書である。2021 年の報告書においては、データ制限指標（Data Restrictiveness Index）を提案し、さらに、データやデータ関連ツールサービスへの依存度が高い経済産業ほど、データ規制の影響が大きくなることから、データ強度修正（Data-Intensity Modifier、DIM）を経た上で、データ制限連携（Data Restrictiveness Linkage、DRL）を算出している。これをもとに、回帰分析をなした場合に、「データ規制は物価、貿易、生産性に有意な影響を与える」という結果が観察されると報告している。また、ITIF の調査によると、OECD の市場規制データに基づく尺度を用いるとき、ある国のデータ規制度が 1 ポイント上昇すると、5 年間で貿易総生産高を 7%削減し、生産性を 2.9%低下させ、川下価格を 1.5%上昇させる影響があること、世界で最もデータ規制が厳しい国は中国であり、インドネシア、ロシア、南アフリカがそれに続く。これらの国の経済は、すべてそのために苦しむことになるものと考えられるとされている。

3.3 我が国における示唆

これらの議論をもとに我が国におけるデータのローカル化の議論について検討する。

これらの論点の問題意識が我が国において問われたのは 2021 年の LINE 事件であると考えられる。しかしながら、当該事件において、この問題が、世界において、いわゆるデータのローカル化の問題の文脈で検討されているということはほとんど指摘されていなかった。その意味で、データの保存場所の問題を世界的な議論の文脈で捉えるべきというのが、本件調査の第一の示唆であるということができる。

実際に、上のデータのローカル化の根拠の妥当性について考えれば、我が国においては、

「(1) 経済発展の推進」及び「(3) 国内法執行の円滑化」という根拠については、我が国において、このような根拠は、それ自体事実としての根拠を有するものではないであろう。

「(2) 外国からの監視の回避」については、上記で挙げた批判は、権威主義的国家が、こ

¹²¹ 以上について、Chander (2020) 11 頁、Chander (2015) 717 頁。

¹²² 2021 年 ITIF 報告書（法執行と規制監督のためのデータローカル化）。

の根拠を名目に、捕食的な検閲・監視を強化しようという動きに対する批判であり、我が国にはあてはまらないであろう。しかしながら、このようなアプローチが、実質的には、経済的に厚生を阻害するという指摘は、きわめて重要である。このような指摘を考えるときには、人々、企業、政府がデータとデジタル技術から得られる膨大な社会的・経済的利益を最大化できるようにする必要があること、という観点から具体的に、当該国における外国からの監視というリスクを判断した上で、データのローカル化について検討すべきということになるものと考えられる。

また、ITIF 報告書は、オーストラリア、カナダ、チリ、日本、シンガポール、ニュージーランド、米国、英国は、オープンでルールに基づいた革新的なデジタル経済を構築するために、データのローカライゼーションに代わる建設的な選択肢を共同で検討する必要があると提唱しており、DFFT 構想等の普及・発展の観点から非常に興味深いものがあるといえる。

以上

附属文書1

ID	番号	英語国名	国名	規制根拠
1	アフリカ01	Ghana	ガーナ	03 ペイメント
2	アフリカ02	Kenya	ケニア	05 健康・ゲノム
3	アフリカ03	Nigeria	ナイジェリア	03 ペイメント
4	アフリカ03	Nigeria	ナイジェリア	07 ICTテレコム
5	アフリカ04	Rwanda	ルワンダ	06 政府記録・クラウド
6	アフリカ04	Rwanda	ルワンダ	07 ICTテレコム
7	アフリカ05	Senegal	セネガル	06 政府記録・クラウド
8	アフリカ06	South Africa	南アフリカ	03 ペイメント
9	アフリカ06	South Africa	南アフリカ	10 その他
10	ヨーロッパ1	Belgium	ベルギー	02 金融・税・銀行
11	ヨーロッパ2	Bulgaria	ブルガリア	10 その他
12	ヨーロッパ3	Cyprus	キプロス	04 地図
13	ヨーロッパ4	Denmark	デンマーク	02 金融・税・銀行
14	ヨーロッパ4	Denmark	デンマーク	06 政府記録・クラウド
15	ヨーロッパ5	European Union	欧州連合	06 政府記録・クラウド
16	ヨーロッパ6	Finland	フィンランド	02 金融・税・銀行
17	ヨーロッパ7	France	フランス	06 政府記録・クラウド
18	ヨーロッパ8	Germany	ドイツ	02 金融・税・銀行
19	ヨーロッパ8	Germany	ドイツ	07 ICTテレコム
20	ヨーロッパ9	Greece	ギリシア	07 ICTテレコム
21	ヨーロッパ10	Italy	イタリア	02 金融・税・銀行
22	ヨーロッパ11	Luxemburg	ルクセンブルグ	02 金融・税・銀行
23	ヨーロッパ12	Netherlands	オランダ	06 政府記録・クラウド
24	ヨーロッパ13	Poland	ポーランド	10 その他
25	ヨーロッパ14	Romania	ルーマニア	10 その他
26	ヨーロッパ15	Russia	ロシア	02 金融・税・銀行
27	ヨーロッパ15	Russia	ロシア	03 ペイメント
28	ヨーロッパ15	Russia	ロシア	06 政府記録・クラウド
29	ヨーロッパ15	Russia	ロシア	07 ICTテレコム
30	ヨーロッパ15	Russia	ロシア	08 公共ローカルクラウド
31	ヨーロッパ16	Sweden	スウェーデン	02 金融・税・銀行
32	ヨーロッパ17	Turkey	トルコ	02 金融・税・銀行
33	ヨーロッパ17	Turkey	トルコ	03 ペイメント
34	ヨーロッパ17	Turkey	トルコ	04 地図
35	ヨーロッパ17	Turkey	トルコ	07 ICTテレコム
36	ヨーロッパ18	United Kingdom	連合王国(イギリス)	02 金融・税・銀行
37	ヨーロッパ18	United Kingdom	連合王国(イギリス)	05 健康・ゲノム
38	中東北アフリカ1	Algeria	アルジェリア	02 金融・税・銀行
39	中東北アフリカ2	Saudi Arabia	サウジアラビア	08 公共ローカルクラウド
40	中東北アフリカ3	United Arab Emirates	アラブ首長国連合	05 健康・ゲノム
41	中央アジア1	Kazakhstan	カザフスタン	07 ICTテレコム
42	南アジア1	Bangladesh	バングラデシュ	02 金融・税・銀行
43	南アジア1	Bangladesh	バングラデシュ	06 政府記録・クラウド
44	南アジア2	India	インド	02 金融・税・銀行
45	南アジア2	India	インド	03 ペイメント
46	南アジア2	India	インド	04 地図
47	南アジア2	India	インド	05 健康・ゲノム
48	南アジア2	India	インド	06 政府記録・クラウド
49	南アジア2	India	インド	07 ICTテレコム
50	南アジア2	India	インド	09 非個人データ枠組
51	東南アジア1	Indonesia	インドネシア	02 金融・税・銀行
52	東南アジア1	Indonesia	インドネシア	05 健康・ゲノム
53	東南アジア1	Indonesia	インドネシア	06 政府記録・クラウド
54	東南アジア1	Indonesia	インドネシア	07 ICTテレコム
55	東南アジア2	Malaysia	マレーシア	02 金融・税・銀行
56	東南アジア3	South Korea	大韓民国	02 金融・税・銀行
57	東南アジア3	South Korea	大韓民国	04 地図
58	東南アジア3	South Korea	大韓民国	06 政府記録・クラウド
59	東南アジア4	Vietnam	ベトナム	02 金融・税・銀行
60	東南アジア4	Vietnam	ベトナム	03 ペイメント
61	東南アジア4	Vietnam	ベトナム	07 ICTテレコム
62	南中央アメリカ1	Brazil	ブラジル	06 政府記録・クラウド
63	南中央アメリカ2	Chile	チリ	03 ペイメント
64	南中央アメリカ2	Chile	チリ	10 その他
65	南中央アメリカ3	Peru	ペルー	08 公共ローカルクラウド
66	南中央アメリカ4	Venezuela	ベネズエラ	03 ペイメント
67	中国	China	中国	02 金融・税・銀行
68	中国	China	中国	03 ペイメント
69	中国	China	中国	04 地図
70	中国	China	中国	05 健康・ゲノム
71	中国	China	中国	07 ICTテレコム
72	中国	China	中国	10 その他

73	オセアニア1	Australia	オーストラリア	05 健康・ゲノム
74	オセアニア2	New Zealand	ニュージーランド	02 金融・税・銀行
75	北アメリカ1	Canada	カナダ	01 地方政府個人データ
76	北アメリカ2	Mexico	メキシコ	02 金融・税・銀行
77	北アメリカ2	Mexico	メキシコ	08 公共ローカルクラウド
78	北アメリカ3	US	アメリカ合衆国	01 地方政府個人データ
79	北アメリカ3	US	アメリカ合衆国	06 政府記録・クラウド
80	北アメリカ3	US	アメリカ合衆国	07 ICTテレコム

附属文書2

番号	国名	規制根拠
1	ベルギー	1 会計・税・金融
2	ブラジル	4 政府・公共
3	ブルガリア	3 新興デジタル
4	カナダ	4 政府・公共
5	中国	1 会計・税・金融
5	中国	3 新興デジタル
5	中国	4 政府・公共
6	コロンビア	4 政府・公共
7	キプロス	2 電気通信
8	デンマーク	1 会計・税・金融
9	フィンランド	1 会計・税・金融
10	フランス	1 会計・税・金融
10	フランス	5 その他
11	ドイツ	1 会計・税・金融
11	ドイツ	2 電気通信
12	ギリシア	2 電気通信
13	インド	1 会計・税・金融
13	インド	4 政府・公共
14	インドネシア	3 新興デジタル
15	イラン	3 新興デジタル
16	カザフスタン	5 その他
17	ルクセンブルグ	1 会計・税・金融
18	オランダ	4 政府・公共
19	ナイジェリア	1 会計・税・金融
20	ニュージーランド	1 会計・税・金融
21	ポーランド	3 新興デジタル
22	ルーマニア	3 新興デジタル
23	ロシア	2 電気通信
24	韓国	2 電気通信
24	韓国	4 政府・公共
25	スウェーデン	1 会計・税・金融
25	スウェーデン	4 政府・公共
26	トルコ	1 会計・税・金融
27	イギリス	1 会計・税・金融
28	アメリカ合衆国	4 政府・公共
29	ベトナム	3 新興デジタル
29	ベトナム	5 その他
30	ベネズエラ	1 会計・税・金融