【2024年度】海外サイバーセキュリティ・プライバシー政策動向の解説

2025年5月

JCIC客員研究員　古澤一憲

【2024年度】海外サイバーセキュリティ・プライバシー政策動向の解説 について

JCICでは、サイバーセキュリティとプライバシー政策に関連した最新の海外動向をまとめ、メールマガジン形式で全会員とオブザーバー組織などに「JCIC海外ニュース」を毎週配信している。

配信したニュースは翌月にJCICのウェブサイトに掲載し、広く閲覧できるようにしている。この海外ニュース配信は、基本的にセキュリティ事故や脆弱性情報、技術情報は取り扱うことはせず、海外の政策動向を中心に配信することで、日本企業のビジネス視点での施策検討の一助となることを目的とするものである。

今回のコラムでは、2024年度（2024年4月～2025年3月）に配信した146件のJCIC海外ニュースを分析し、2025年度の政策動向を占う重要な出来事を解説する[1]。

まず、2023年度の海外サイバーセキュリティ・プライバシー政策動向のまとめとして全体を俯瞰した解説を行い、次に各トレンド別に代表的なニュースの振り返りを行う。

1.　2024年度の主要なサイバー政策動向のまとめ

2024年度も、安全保障問題としてのサイバーセキュリティ対策、国際化する組織的サイバー犯罪といった潮流は基軸として維持されたといえる。一方で、25年1月に誕生した第二期トランプ政権の影響はいまだ先を見通せない状況にあり、25年度には米国のみならず世界のサイバーセキュリティ環境にこれまでと異なる変化をもたらす可能性がある。

JCICでは2024年度の主要トレンドとして、第二期トランプ政権のサイバー政策見通し、生成AI法制とセキュリティの指針、耐量子暗号移行の目途、セキュリティ開示と司法判断の傾向の4点に着目する。

第二期トランプ政権のサイバー政策見通し

2025年1月20日に米国でドナルド・トランプ大統領による第二期政権がスタートし、一週間での30を超える大統領令への署名を皮切りに多くの変化が急速にもたらされている。2025年5月現在では、特に関税政策や政府効率化省（DOGE）などの動向が最も関心を集める事項となっているが、本稿ではサイバーセキュリティ政策への影響に着目する。

[1] 2022年度以前のまとめはこちらから：https://www.j-cic.com/reports.html#org_ovrvw1c

これまで、米国のサイバーセキュリティ政策はその根幹部分は、政権を跨ぎながらも一貫している。2010年、オバマ政権においてサイバースペースが「陸・海・空・宇宙に次ぐ第五の戦場」と位置づけられ、現在のサイバー安全保障の枠組みの基本が形作られると、その後の第一期トランプ政権、バイデン政権もこの路線を発展的に継承してきた。主に中露イラン北朝鮮などを主要な脅威アクターとして識別し、政府および重要インフラをサイバー攻撃から防護することを目標とする。この10年間で、より破壊的攻撃への対処、当局による重要インフラ監督強化、輸出入規制によるサプライチェーンリスク対応など様々なアジェンダへの広がりはあったが、根本の部分は変わらない。

第二期トランプ政権においても、最も基本的なレベルでの米国自身の重要インフラを敵対国から防護するというサイバー安全保障の方針は保持されるだろう。バイデン前大統領と比較した際に、ウクライナとの関係から対ロシア政策の違いを指摘することは可能だが、ことサイバー脅威に関しては米国自体をターゲットとするものであり、この点でロシアへの警戒を緩める合理的な理由は特段ないだろう。

一方で、これまでの動きから、行政のコスト削減および反トランプ勢力の排除、米国中心路線のかじ取りといった基本路線は、サイバーセキュリティ政策においても第二期トランプ政権の特徴として顕在化がすることが予想される。

2025年5月時点で、CIAやNSAの職員を大幅削減する案が各メディアから報道されているが、特にサイバーセキュリティを専門に管轄するサイバーセキュリティ・社会基盤安全保障庁（CISA）でも大規模な予算削減と人員整理の予定が報じられている。2025年5月2日に公開された2026年度予算要求では、CISAの年間予算は4億9100万ドル（約700億円）の削減となっており、これは前年度予算のおよそ17%にあたる。具体的な内訳等は明らかにされていないが、最も大きくリソースが削減される領域のひとつは偽情報対策であるとされている。本ニュースクリップでもバイデン前大統領政権におけるCISAの偽情報対策は度々取り上げてきたが、トランプ大統領は兼ねてからこれに否定的であり、選挙インフラ情報共有分析センターは国土安全保障省による資金供与が終了したことによる活動終了のアナウンスをサイトへ掲示している[2]。2025年1月にはMeta社がファクトチェック部門を閉鎖し、2025年2月にもミュンヘン安全保障会議でもヴァンス副大統領が選挙におけるオンライン情報発信への介入を否定するスピーチを行うなど、米国においてセキュリティ文脈での偽情報対策は縮小される見通しとなるだろう。

また、25年度に入ってからの話題だが、MITRE社が中心となって運用している共通脆弱性識別子（CVE）が予算問題により継続を危ぶまれる事態となった事案も注目を集めた。結果的に本件に関しては2025年度末までの予算が直ちに延長される対応がとられたが、CVE理事会は世界各国のサイバー防御の基礎となるCVEプログラムが一国の予算措置に依存する現状に警鐘を鳴らし、CVE財団を設立した。これは米国に留まらない国際的なサイバーセキュリティ能力に影響を及ぼす問題となりえる。既に米国の国際協力関係予算には大きな見直しが入っていることから、サイバーの分野においても同様の整理が行われる可能性は高いだろう。CVE以外にも米政府は脅威情報の分析共有や海外政府のインシデント対応支援等でも重要な役割を果たしており、米国依存の見直しの議論が様々に広がる可能性がある。

[2] https://www.cisecurity.org/ei-isac

生成AI法制とAIセキュリティ対策の指針

2024年度も、前年度に引き続き生成AI関連の法整備が大きく進展した。最も印象的であったのは、EUにおけるAI法の正式な採択と米国におけるAIの安全に関する大統領令の撤回だろう。これまでもAIに対して、ハードロー路線の欧州とソフトロー路線の米国という基本方針の違いは指摘されていたが、今回のトランプ大統領の方針により一層対照性が明確になったといえる。

バイデン前大統領の署名した米国のAIの安全に関する大統領令は、リスク抑制の観点からAIシステム開発者に対して一般公開の前に安全性テストの結果を米国政府と共有するよう要求するものだった。これが、民間企業のイノベーションを阻害するという理由からトランプ大統領に撤回されたという経緯がある。EU AI法は、ハイリスクAIシステムに対して、市場投入前に適合性評価の取得を要求する構成であることから、今後の具体的な制度実装や実務面の調整において注目すべきポイントのひとつとなるだろう。

その他の国においても、基本法の制定を早期に行っていた中国ではAI合成コンテンツの標示に係る規則を制定するなど、より具体的な運用の整理を進めている。この他にも、台湾での人工知能基本法の草案公開、スペインにおけるEU AI法に準拠した国内法の制定、カナダ政府によるAI戦略の発表といった動きがあった。

前年度のまとめでの予見通り、AIのセキュリティ面の検証に焦点をあてたAIセキュリティ対策の指針についての議論にも進展がみられた。特徴として挙げられるのが、AIのセキュリティ検証にレッドチーム手法を用いるアプローチが提案されている点だ。レッドチーム手法とは、テスト対象システムに対して実際に悪性のリクエストを送信して成否をみることで、脆弱性の有無を明らかにする手法である。従来のプログラムのIf-Thenルールや繰り返しループのような決定論的なロジックと比較し、大規模なパラメーター行列による確率的な動作に特徴のあるAIシステムに対してはホワイトボックス型の静的検証の相性が悪いことは要因のひとつに挙げられるだろう。脅威の高度化を受け、従来型のシステムにおいてもレッドチーム試験の注目度は徐々に増している傾向にあったが、AIシステムにおいてはより標準的なアプローチとして採用が広がることが想定される。

耐量子暗号移行の目途

量子コンピューティングは実用化に向けて徐々に研究が進んでいる最中であるが、様々なユースケースと共に既存の暗号アルゴリズムの危殆化がリスクとして指摘されている。

これまで、耐量子暗号アルゴリズムの研究開発や標準化のための議論が進められてきた。2024年度に新しく見られた傾向は、耐量子暗号への移行目標時期や政府機関等における切り替え計画に関する具体的な言及が複数みられたことである。JCICニュースクリップでは、米国・英国・豪州政府による計画を取り上げたが、いずれも2030年から2035年前後を切り替えの時期として見据えている。

暗号アルゴリズムの切り替えは旧式の暗号の利用停止を伴う、ITエコシステム全体に影響する刷新である。暗号技術の性質上、耐量子暗号への移行は量子コンピューティングの本格的普及に先立って検討が進むものと考えられる。

民間企業においても、動向を注視することで時機を捉えた対応が可能となるだろう。一般に想定される移行プロセスは、影響を受ける情報資産の棚卸し、移行計画の策定、移行の実施というような形になるだろう。自組織において、独自実装や手動メンテナンスの度合いが高いシステムにおいては特に移行コストが大きくなることが想定される。英国NCSCのガイダンスでは、まず自組織のアセスメントを早期に実施したうえで、システムの重要度や移行難度等に応じた優先度設計を策定することを推奨しており、参考になる現実的なアプローチであるといえる。

セキュリティ開示と司法判断の傾向

米国では2023年12月に米国証券取引委員会（SEC）が、年次報告書におけるサイバーリスク管理等の開示を義務付けられたが、2024年10月に不適切な開示を理由とする告発が4社を対象に行われた。サイバーセキュリティインシデントの発生を把握していながら、その影響の範囲や性質について適切に開示せず、情報公表を最小限に抑えたことは、投資家がリスクを過小評価することにつながるとされた。

SECによる告発以外にも、各国当局によるデータ侵害事案に対する裁判事例が多く報じられた。これらを分析すると、近年の裁定において、セキュリティガバンスへの取り組みやその時点において通常実装されていることが期待されるセキュリティ対策の有無などが、個々の事例で具体的に検証されているという傾向がみられる。例えば、6月に判決が確定したカリフォルニア州のソフトウェア企業に対する訴訟では多要素認証の実装が行われていなかったことが問題視され、10月のT-mobile社への判決では制裁金に加えてサイバーハイジーンの向上やゼロトラストアーキテクチャの構築にセキュリティ予算を振り向けることが是正勧告されるといった裁定が見られた。

サイバー侵害事案には攻撃者のみならず被害企業の責任が厳しく追及されやすいという特徴があるが、ずさんな運用や単純なミスが原因のものから極めて高度な手法による組織的攻撃によるものまで原因は様々である。企業が、サイバー攻撃被害を防ぐための努力や被害発生後の正しい情報開示と迅速な対応などの努力を十分に行っていた場合とそうでなかった場合に瑕疵の程度の裁定が区別されるのは望ましい姿といえる。JCICでも、サイバーセキュリティ開示がもたらすメリットについてのコラム[3]を掲載しているが、こうした傾向が、企業がサイバーセキュリティ対策に取り組むうえでのインセンティブとして正しく機能することが望まれる。

2. 各トレンドの代表的なニュースの振り返り

1） 第二期トランプ政権のサイバー政策見通し（バイデン前政権からの変遷）

1-a）第二期トランプ政権前（バイデン前大統領時代）の主なニュース

2024年4月11日 米国CISA、連邦政府機関に対してロシアの国家主導型サイバー脅威へ直ちに対処するよう指示

米国サイバーセキュリティ・社会基盤安全保障庁（CISA）は、ロシアの国家支援型サイバー攻撃グループが実施した一連の攻撃キャンペーンに対応するための緊急指令24-02を発令した。MicrosoftがMidnight Blizzardと呼称するこの攻

[3] https://www.j-cic.com/column/Mandatory-cybersecurity-disclosure.html

撃グループは、Microsoft電子メールアカウントの侵害に成功し、連邦政府文民機関（FCEB）機関とMicrosoftの間の電子メール通信を窃取したとされる。Microsoftの報告によると、2024年2月はパスワードスプレーなどの攻撃キャンペーンの量が前月と比較して10倍程度増加したという。

この緊急指令は4月2日に発行され、連邦政府機関に対し、流出した電子メールの内容の分析、侵害された資格情報のリセット、Microsoft Azureの特権アカウントの認証方式が安全であることを確認するための追加の措置を講じることなどを義務付けている。各政府機関は、4月8日までに必要なすべての対策の実施状況をCISAに報告し、5月1日までに追加の進捗を報告する。さらに、必要に応じて対応完了まで週次で最新の状況報告を実施する必要がある。

https://www.cisa.gov/news-events/news/cisa-directs-federal-agencies-immediately-mitigate-significant-risk-russian-state-sponsored-cyber

https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system

2024年5月16日 米国司法省、北朝鮮の違法収益創出スキームへの関与で米国籍の容疑者などを起訴

米国司法省は、北朝鮮による違法収益創出スキームへの関与し、機密情報窃取・詐欺・マネーロンダリングなどを行ったとして、アリゾナ州在住の米国籍の女とその共犯者を起訴した。

被告グループは、国外のIT労働者が身元を詐称する手助けをし、米国民や米国居住者を装って不正にリモート就労できるようにしていた。米国内からのアクセスに見せかけるための中間ホストの提供なども手がけていたという。フォーチュン500企業を含む米国企業300社以上が被害にあっていたとみられている。このスキームを利用して就労していたIT技術者の多くは北朝鮮国籍であり、被告らは偽名による金融取引やマネーロンダリングにも関与していた疑いがかけられている。被告には最高97.5年の懲役が求刑され、共犯者の情報にも最大500万ドル（約7.8億円）の報奨金が設けられた。

また、同時期に米国人のデジタルアカウントを販売し、国外のIT技術者のリモート就労を支援していたウクライナ国籍の男が同様に起訴され、最高67.5年の懲役が求刑されている。

FBIは、これらは単なる詐欺やマネーロンダリングではなく、米国の制裁措置を回避するハイテク犯罪であるとして、全力で対応していく方針だと説明している。

https://www.justice.gov/opa/pr/charges-and-seizures-brought-fraud-scheme-aimed-denying-revenue-workers-associated-north

https://rewardsforjustice.net/rewards/north-korean-information-technology-it-workers/

https://www.38north.org/2024/04/what-we-learned-inside-a-north-korean-internet-server-how-well-do-you-know-your-partners/

2024年5月22日 米国CNMF、サイバー防衛チームをザンビアに初派遣

米国国防省ミッションフォース（CNMF）は、サイバー防衛チームを初めてザンビアに派遣し、パートナーとしての協力関係の強化を報告した。

派遣期間は約3か月で、米国のサイバー部隊はザンビア情報通信技術庁のネットワーク防衛担当者と協力しながら脆弱性を特定、悪意あるサイバー活動を捜索した。

米国サイバー軍の永続的な関与戦略の重要要素であるディフェンスフォワード作戦は、米国と同盟国の国防を強化し、悪意のあるサイバー活動を防御および妨害することを目的としている。CNMFは、海外でのミッションを通じて獲得した洞察を米国の民間業界や政府機関間のパートナーと共有しており、同種の脅威が米国のネットワークに到達する前に防御を強化することを可能とするため米国の国益にも還元されているという。

https://www.cybercom.mil/Media/News/Article/3783991/cnmf-deploys-first-defensive-cyber-team-to-zambia/

2024年9月23日 米国商務省、コネクテッドカーへの中国・ロシア製部品搭載を禁止する規則案

米国商務省は、国家安全保障上の懸念から、コネクテッドカーへの中国製およびロシア製部品の搭載を禁止する規則案を発表した。敵対勢力が車両接続システムへの不正アクセスを通じて機密データを収集したり、米国の道路を走行する車両を遠隔操作するリスクを防止することを目的としている。農業用車両や採掘用車両などの公道で使用されない車両を除き、車輪のついたすべての路上走行車両に適用される。

特にコネクテッドカーの外部接続機能および自律走行機能を可能にする車両接続システム（VCS）や自動運転システム（ADS）に統合されるハードウェアおよびソフトウェアに焦点を当てており、国内外の主要自動車メーカーに対して、中国製およびロシア製のソフトウェアやハードウェアの使用を禁止する。VCSは、テレマティクス制御ユニット・Bluetooth/モバイル/衛星/Wi-Fi通信モジュールなど、車両が外部と通信することを可能にする一連のシステムを意味し、ADSには、高度に自律化された車両が運転手なしで運転できるようにするコンポーネントが含まれる。該当するコンポーネントが搭載された車両は輸入および販売が全面的に禁止される予定。

https://www.bis.gov/press-release/commerce-announces-proposed-rule-secure-connected-vehicle-supply-chains-foreign

https://www.federalregister.gov/

2024年10月18日 米当局、米国総選挙で国外の脅威主体が偽情報の拡散のため使用する戦術に警告

米国連邦捜査局（FBI）と米国サイバーセキュリティ・社会基盤安全保障庁（CISA）は、2024年の米国総選挙で外国の脅威アクターが偽情報を拡散するために使用する戦術を警告する共同公共広告を発表した。

2024年の米国総選挙に向けて、民主的プロセスの完全性に疑問を投げかけ、党派間の不和を植え付けることを目的に偽情報を拡散する外国のアクターの取り組みに焦点を当てている。様々な偽情報キャンペーンにおいてAIなどの新しいツールを活用し、誤解を招くコンテンツを作成・拡散する傾向がみられるとのこと。

両機関は、州や地方の選挙当局からの信頼できる情報を参考にすることを推奨し、ソーシャルメディア等に情報を共有する際は、事前に複数の信頼できる情報源を通じて主張を検証するよう促している。

https://www.cisa.gov/news-events/news/fbi-and-cisa-issue-public-service-announcement-warning-tactics-foreign-threat-actors-are-using

2024年10月24日 米国ホワイトハウス、AIに関する初の国家安全保障覚書と関連するフレームワークを発表

米国ホワイトハウスは、AIの進歩が国家安全保障と外交政策に及ぼす影響を重視し、AIに関して初となる国家安全保障覚書（AI NSM）とこれに関連するフレームワークを発表した。

AI NSMには、米国が安心・安全で信頼性のあるAI開発をリードすること、国家安全保障上の任務遂行にAI技術を最大限活用すること、そして国際的なAIガバナンスの形成を推進することが盛り込まれている。さらに、敵対的なAI技術の開発および使用の監視と対抗措置をとることが指示されている。この取り組みの一環として、新たに設立されるAI安全研究所が、情報機関や国防総省、エネルギー省などの国家安全保障機関と連携し、AIリスクに対処していく予定。

また、同時に発表された「国家安全保障におけるAIガバナンスとリスク管理を推進するためのフレームワーク」は、AI NSM セクション4.2の要件に基づき、国家安全保障システム（NSS）におけるAI活用のガバナンスとリスク管理の指針を示している。各機関の部門長は、本指針に従い自部門でのAIリスク管理体制の整備とガバナンスの強化を推進する役割を担う。

https://www.whitehouse.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security/

https://www.whitehouse.gov/briefing-room/statements-releases/2024/10/24/fact-sheet-biden-harris-administration-outlines-coordinated-approach-to-harness-power-of-ai-for-u-s-national-security/

https://www.whitehouse.gov/briefing-room/statements-releases/2024/10/24/statement-from-national-economic-advisor-lael-brainard-on-national-security-memorandum-nsm-on-artificial-intelligence-ai/

2024年10月29日 米国CISA、重要インフラのセキュリティとレジリエンスに関連する国際戦略計画を発表

米国サイバーセキュリティ・社会基盤安全保障庁（CISA）は、2025～2026年国際戦略計画を発表し、同庁初となる包括的な国際戦略の枠組みを示した。

この計画は、重要インフラのセキュリティとレジリエンスに関する国家安全保障覚書に基づいており、米国および国際パートナーが直面する脅威や課題に対応するための具体的目標が設定されている。計画には、CISAが目指すべき3つの主な目標が掲げられている。まず、米国が依存する海外インフラのレジリエンスを強化し、対外依存の安全性を高めること。次に、国際的なサイバー防衛の統合を強化し、脅威の早期探知と効果的な対策を講じる能力を向上させること。そして、国際活動における機関調整を統一し、協力の一貫性と効率性を確保することである。CISAはこの計画を通じて、国際的なサイバーセキュリティの強化と持続可能なインフラ防衛の基盤作りを目指すとしている。

https://www.cisa.gov/news-events/news/cisa-releases-its-first-ever-international-strategic-plan

https://www.cisa.gov/2025-2026-cisa-international-strategic-plan

2025年1月16日 米国バイデン大統領、退任直前に国家サイバーセキュリティを強化する2度目の大統領令に署名

米国バイデン元大統領は、任期最終週に「国家のサイバーセキュリティにおけるイノベーションの強化と促進に関する大統領令（EO 14144）」への署名を行った。2021年に署名された EO 14028に続き、敵対国からのサイバー脅威へ対処するため国家サイバーセキュリティを強化することを目的としたもの。トランプ新大統領は就任直後に複数の大統領令の撤回を行っているが、現在のところ本件は撤回リストには含まれていない。

本大統領令EO 14144の各条項は、ソフトウェアプロバイダーなどの説明責任向上、連邦政府のネットワークとシステムの管理強化、新技術の利用奨励、サプライチェーンの透明性と安全性確保などの方針を定めている。具体的な施策としては、政府システムおよび重要インフラシステムを対象に次のような規則を盛り込んでいる。

1.機械読み取り可能なサイバーセキュリティ認証の義務化とCISAによる検証一元化

2.重要インフラとしての宇宙システム目録作成と通信セキュリティ担保

3.2030年までに量子耐性暗号へ移行

4.アイデンティティとアクセス管理の強化

5.AI主導のサイバー防衛パイロットプログラムの作成と研究資金の提供

https://www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity

https://www.reuters.com/technology/artificial-intelligence/biden-issue-executive-order-ensure-power-ai-data-centers-2025-01-14/

https://www.cnbc.com/2025/01/16/biden-administration-launches-cybersecurity-executive-order.html

1-b) 第二期トランプ政権移行後の米国サイバー政策に関するニュース

2025年1月20日 米国ホワイトハウス、バイデン元大統領署名の「AIの安全に関する大統領令」を撤回

トランプ新大統領は、バイデン元大統領が2023年に署名した「AIの安全でセキュアな信頼性の高い開発と利用に関する大統領（EO 14110）」を撤回した。

EO 14110は、AI産業における米国の競争力の確保・AIによる市民の自由や国家安全保障に対する脅威の防止・国家的なAI統制アプローチの構築を目的としたもの。この中で、リスク抑制の観点から、AIシステム開発者に対して一般公開の前に安全性テストの結果を米国政府と共有するよう要求していた。この要求事項が民間セクターのAIイノベーションを妨げているとして、2024年共和党綱領ではEO 14110を撤回する方針を掲げられていた。

一方、同じくバイデン大統領によって署名されたAI関係の大統領令のうち、AIデータセンターとクリーン電力設備増設のために政府用地を貸与する大統領令は撤回されなかった。

https://www.whitehouse.gov/presidential-actions/2025/01/initial-rescissions-of-harmful-executive-orders-and-actions/

https://www.reuters.com/technology/artificial-intelligence/trump-revokes-biden-executive-order-addressing-ai-risks-2025-01-21/

2025年2月14日 ミュンヘン安全保障会議におけるヴァンス副大統領の演説 （ニュースクリップ収録外）

米国ヴァンス副大統領は、ミュンヘン安全保障会議において基調演説を行い、欧州と米国の安全保障観に対する根本的な見解を示した。

ヴァンス副大統領は、欧州が直面する最大の脅威は外部勢力であるロシアや中国ではなく、民主主義の原則や言論の自由からの逸脱といった内部的要因であると強調した。具体例として、ルーマニアにおける選挙結果の無効化や、欧州各国における選挙制度の正当性に対する不信感を挙げ、制度的信頼の低下を憂慮した。

さらに、各国政府による「偽情報」対策が反対意見の封殺手段として機能していると現状を批判し、言論の自由の尊重を訴えた。

https://www.cisa.gov/news-events/news/cisa-and-uk-ncsc-hold-inaugural-meeting-strategic-dialogue-cybersecurity-civil-society-under-threat

2025年2月11日 米豪英当局、ランサムウェア攻撃に使用された防弾ホスティングサービスへ共同制裁

米国財務省外国資産管理室（OFAC）、豪州外務貿易省、英国外務英連邦開発省は、ロシアを拠点とする防弾ホスティングサービスプロバイダー「Zservers」を制裁対象に指定した。

Zserversは、ロシア・バルナウルに本社を構え、法執行機関の監視を回避するための防弾ホスティングサービスをサイバー犯罪フォーラム上で宣伝していた。特に、同社が実際にLockBitランサムウェアグループに対して多数のIPアドレスの貸出しを含む防弾ホスティングサービスを提供してきたとし、制裁の主な根拠としている。

今回の制裁措置により、米国内に存在する、または米国人が所有・管理するZserversのすべての財産および財産権益は凍結され、OFACへの報告が義務付けられる。

https://home.treasury.gov/news/press-releases/sb0018

2025年3月5日 米国司法省、中国の標的型攻撃グループAPT27のメンバーおよび請負業者職員など計12名を起訴

米国司法省（DOJ）は、中国を背景とする高度標的型攻撃グループAPT27のメンバーとみられる中国人2名を起訴した。両名は、2011年から現在に至るまで、米国の多数の企業、自治体、政府機関を標的としたサイバースパイ活動に関与していたとみられている。起訴状の公開とともに財務省による制裁を発表し、両名の逮捕に役立つ情報に最大200万ドルの報奨金が設定された。また、司法省は起訴された2人が悪意ある活動に用いていたとみられる複数のドメインと仮想プライベートサーバー（VPS）を押収し、分析を行っている。容疑者らの活動は、APT27（別名：Silk Typhoon、

Emissary Panda、UNC5221）と関連する脅威グループに技術基盤を提供するものであったとみられ、2024年の米国財務省への不正アクセス事案での利用も含まれている。

続けて同日、司法省は中国の政府系請負業者であるi-Soon社の幹部および従業員8名と政府職員2名を起訴したと発表した。少なくとも2016年頃から2023年頃まで米国へのサイバースパイ活動に従事したとされ、こちらもAPT27の活動との関連があるとみられている。捜査の背景には、2024年2月にi-Soon社の内部文書が流出し、中国政府とのサイバー攻撃業務請負に関係する情報が明らかになっていたことがある。司法省は、本件の10名の逮捕に有益な情報に対しても最高1,000万ドルの報奨金を設定した。

https://www.justice.gov/usao-dc/pr/chinese-nationals-ties-prc-government-and-apt27-charged-computer-hacking-campaign-profit

https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global

2025年4月4日 CISA職員1,300人以上の削減に関するニュース（ニュースクリップ収録外）

関係者への取材から、CISA職員のうち最大1,300人に解雇もしくは退職勧告がなされる見通しとの報道。

https://www.cbsnews.com/news/cisa-cybersecurity-election-infrastructure-face-significant-cuts-sources-say/

2025年5月2日 2026年度予算においてCISA予算が4億9100万ドルの削減（ニュースクリップ収録外）

ホワイトハウスの公表した2026年度予算資料において、CISAの予算は約4億9100万ドル（約700億円）の削減とする計画が示された。

https://www.whitehouse.gov/wp-content/uploads/2025/05/Fiscal-Year-2026-Discretionary-Budget-Request.pdf

2） 生成AI法制とAIセキュリティ対策の指針

2-a) セキュリティに限らない生成AI全般に関する法制・ガバナンス

2024年5月21日 欧州連合理事会、EU AI法を正式採択

欧州連合理事会（EC）は、EU AI法を最終承認し、正式に採択した。EU官報への掲載から20日後に発効となる予定。

「AIに関する規則の調和を目指す画期的な法律（EU AI法）」の目的は、EU市民の基本的権利の尊重を確保しながらEUにおけるAI技術の革新と投資を促し、安全で信頼できるAIシステムを開発・導入することと位置付けられている。

AIをリスクレベルで分類したうえで規制する方式を採用しており、企業がEU市場にAIシステム製品やサービスを提供するためには該当するリスクレベルに対応する要件を満たす必要がある。ただし、最も深刻なリスクが認められるカテゴリ（人間の認知行動の操作、ソーシャルスコアリング、犯罪予測に基づく予防的取締り、生体データを利用した人種や宗教などの特定の属性分類など）は、容認できないリスクとしてAIの利用が禁止される（「禁止AI」に分類）。それ以

外のAIについては、想定されるリスクの大きさに応じて「高リスクAI」や「低リスクAI」などに分類され、それぞれ異なる水準の要件が設定される。

要件の適用はAI法の発効から2年間をかけて段階的に行われる予定。一部の規定は先行して適用されることが決まっており、禁止AIの規定がまず6ヵ月後に適用され、汎用AI（GPAI）に関する規定も1年後に適用される。一方で、軍事・防衛、研究目的のAIシステムは適用対象外となる。

AI法の違反に対しては罰金規定が設けられ、EU域外にも適用される。罰金の基準額は、1500万ユーロまたは前会計年度の全世界売上高の3%のいずれか高い方（禁止AI規定への違反は3500万ユーロまたは全世界売上高の7%のいずれか高い方）とされる。中小企業と新興企業は、基準に比例した行政罰の対象となる。

https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/

https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/en/pdf

2024年6月5日 米国商務省およびシンガポール通信情報省、AIガバナンスに関するパートナーシップを深化

米国商務省とシンガポール通信情報省はそれぞれ、AIガバナンスに関する両国のパートナーシップを深める方針について発表した。

現在シンガポールでは約6千社の米国企業が事業展開しており、両国間の貿易は米国全土で約25万人の雇用を支えている。また、米国はシンガポールの投資家にとって最大の技術投資先であり、その額は年間約184億米ドル（約2.9兆円）に及ぶ。これを受け、米国企業は、シンガポールの国家AI戦略2.0に沿ったAICoEを設立するなど、今後数年間で370億米ドル（約5.8兆円）以上をシンガポールのAIエコシステムに投資する予定だという。

両国はこの取り組みの中でAIの安全な利用を共通の関心事項としており、AIガバナンス領域におけるパートナーシップ強化のための施策を発表した。

米国商務部とシンガポール通信情報省は、米国NISTが開発した「AIリスク管理フレームワーク」とシンガポール情報通信メディア開発庁が開発した「AIベリファイ」という2つのフレームワークをマッピング作業を完了している。今後も生成のAIガバナンスフレームワークのマッピング、テスト、ガイドライン、ベンチマークに関して協力を続ける。また、両国のAI安全研究機関の協力やビジネス機会の推進、国際標準の開発、人材育成など様々な分野での共同活動に取り組んでいく方針を示した。

https://www.commerce.gov/news/fact-sheets/2024/06/fact-sheet-us-singapore-shared-principles-and-collaboration-artificial

https://www.mci.gov.sg/us-singapore-shared-principles-and-collaboration-on-artificial-intelligence/

2024年7月15日 台湾国家科学技術委員会、「人工知能基本法（草案）」への意見募集を開始

台湾国家科学技術委員会は、「人工知能基本法（草案）」を公開し、9月13日を期限とする意見募集を開始した。AIの開発と応用を促進するための指標と指導原則を備えた法律の制定を目的としている。

全18条からなる草案は、データ保護とガバナンス、セキュリティと安全性、透明性と説明可能性、公平性と無差別など7つの原則を規定している。また、イノベーションと人材育成、リスク管理と責任、権益の保護とデータ利用、規制の適応と事業の見直しの4点を優先して推進する事項と位置付けた。

特徴的な点として、AIリスクの分類に分野別の指標を導入している。一方で、AIモデルの訓練に向けた個人データの収集や利用の監督については、国家科学技術委員会が統括する。また、法制定手続きの完了に先立ち、関連事項が規定に適合することを確保するために中央政府の目的事業の所轄官庁と科学技術担当官庁が協力の上で規定を解釈・適用することとされた。

https://www.nstc.gov.tw/folksonomy/detail/87e76bcd-a19f-4aa3-9707-ca8927dcb663?l=ch

https://law.nstc.gov.tw/index.aspx?LawType=12

https://join.gov.tw/policies/detail/4c714d85-ab9f-4b17-8335-f13b31148dc4

2024年9月3日 米国カリフォルニア州、AI開発者に安全義務を課す法案を可決

米国カリフォルニア州は、AI開発者に対して安全義務を課す法案（SB1047 SB-1047 Safe and Secure Innovation for Frontier Artificial Intelligence Models Act.）の可決を最終承認した。

本法案は、技術の販売前に壊滅的なリスク（サイバー攻撃や生物兵器製造方法の教授能力など）を評価し、AIモデルの緊急停止機能の実装を義務付けるものである。加えて、有害な結果（5億ドル以上の損害をもたらす重要インフラへのサイバー攻撃など）に対してAI開発者が責任を負うことを求める。開発および訓練のコストが1億ドル（約142億円）以上、または一定の計算能力を超えるAIモデルを開発する企業が適用対象となる。

今回の法案は他州のAI規制のモデルにもなる可能性があり、これまで産官学で激しい議論が交わされてきた。カリフォルニア州の学術コミュニティやペロシ前下院議長が反対し、AI Alliance（Meta社やIBM社などが加盟）や商工会議所も経済や産業への悪影響を理由に反対を表明している。AIスタートアップ各社も州知事に対して慎重な考慮を求める書簡を送り、OpenAI社は連邦レベルでの規制を検討することが適切であると主張している。

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB1047

https://www.documentcloud.org/documents/25056617-ca-sb-1047-openai-opposition-letter

https://advocacy.calchamber.com/2024/08/21/ai-models-bill-will-hurt-economy-industry-study-concludes/

https://pelosi.house.gov/news/press-releases/pelosi-statement-opposition-california-senate-bill-1047

2025年1月20日 米国ホワイトハウス、バイデン元大統領署名の「AIの安全に関する大統領令」を撤回（再掲）

トランプ新大統領は、バイデン元大統領が2023年に署名した「AIの安全でセキュアな信頼性の高い開発と利用に関する大統領（EO 14110）」を撤回した。

EO 14110は、AI産業における米国の競争力の確保・AIによる市民の自由や国家安全保障に対する脅威の防止・国家的なAI統制アプローチの構築を目的としたもの。この中で、リスク抑制の観点から、AIシステム開発者に対して一般公開

の前に安全性テストの結果を米国政府と共有するよう要求していた。この要求事項が民間セクターのAIイノベーションを妨げているとして、2024年共和党綱領ではEO 14110を撤回する方針を掲げられていた。

一方、同じくバイデン大統領によって署名されたAI関係の大統領令のうち、AIデータセンターとクリーン電力設備増設のために政府用地を貸与する大統領令は撤回されなかった。

https://www.whitehouse.gov/presidential-actions/2025/01/initial-rescissions-of-harmful-executive-orders-and-actions/

https://www.reuters.com/technology/artificial-intelligence/trump-revokes-biden-executive-order-addressing-ai-risks-2025-01-21/

2025年3月4日 カナダ政府、連邦公共サービスにおけるAI政府戦略を発表

カナダ政府は、連邦公共サービスにおけるAIの安全かつ倫理的で信頼性の高い提供および責任ある利用を促進するためのAI戦略を発表した。

本戦略は、科学技術の発展と労働力の生産性向上、国民へのデジタルサービスの改善を目的とし、4つの主要分野を柱としている。それぞれの柱の目標は（1）AI専門センターの設立、（2）AIの安全かつ責任ある利用の確保、（3）トレーニングと人材開発の強化、（4）透明性を通じた信頼の構築、である。政府は本戦略を2年ごとに更新し、継続的な改善を図る方針を示している。

なお、カナダ政府は本戦略の策定にあたり、2024年5月から10月にかけて国民からの意見を収集し、2025年1月にはその結果をまとめた報告書「What We Heard」を公表していた。また、公務員による生成AIの責任ある活用とリスク評価のためのガイダンスも発表するなど、行政機関におけるAI利用の適正管理を推進する施策を強化している。

https://www.canada.ca/en/treasury-board-secretariat/news/2025/03/canada-launches-first-ever-artificial-intelligence-strategy-for-the-federal-public-service.html

2025年3月11日 スペイン、EU AI法に準拠した国内AIガバナンス法を起草

スペインのデジタル変革公共サービス省は、EU AI法の規定を適用した国内AIガバナンス法を起草した。本法案は、倫理的かつ包括的で、人々にとって有益なAIの開発・使用を保証することを目的とし、EU AI法により禁止されているAIの行為や高リスクAIの開発規制を国内法に適合させる内容となっている。

今回、AIシステムが人間の死亡や重大な事故を引き起こした場合、監督当局がスペイン市場から当該システムを暫定的に撤退させる権限を有することが明記された。また、禁止システムの監視を担当する当局は、スペインデータ保護庁（生体認証システムと国境管理）、司法総評議会（司法分野のAIシステム）、中央選挙管理委員会（民主的プロセスに影響を与えるAIシステム）、スペイン人工知能監督庁（その他の場合）とされた。

罰則規定として、2025年8月2日以降に禁止行為が発覚した場合、違反企業には750万～3,500万ユーロ、または前年の全世界売上高の2%～7%のいずれか高い金額の罰金が科される。中小企業の場合はそのいずれか低い金額となる。本法案は緊急処理が予定されており、閣僚理事会で最終承認を受けた後、スペイン議会で正式に承認される予定。

https://digital.gob.es/en/comunicacion/sala-de-prensa/comunicacion_ministro/2025/03/2025-03-11.html

2025年3月14日 中国CAC、「AI合成コンテンツ標示弁法」を交付 9月1日より施行

中国国家インターネット情報弁公室（CAC）は、工業情報化省、公安省、国家ラジオテレビ総局と共同で「AI合成コンテンツ標示弁法」を公布し、2025年9月1日より施行すると発表した。本弁法は、生成AIによって作成されたコンテンツの識別と標示の明確化を図り、社会公益の保護を目的としたもの。

規定によれば、AI合成コンテンツには「明示的な標示」または「暗黙の標示」のいずれかの形式で識別情報を付すことが義務付けられる。明示的な標示とは、テキスト・音声・画像などを用いたユーザーが視認可能な標示を指し、暗黙の標示は、技術的手段によりコンテンツファイル内に埋め込まれる識別情報（例：隠しロゴ）を意味する。

また、サービス提供者には、関連する深層合成技術やアルゴリズム推薦の管理規定に適合した技術的対策を講じる義務が課される。さらに、いかなる組織または個人も、これらの表示を削除・改ざん・偽造・隠蔽する行為や、それを可能にするツール・サービスの提供が禁止される。

また、同日に国家サイバーセキュリティ標準化技術委員会が「AI合成コンテンツロゴサービスプロバイダーコーディングルール」に関するサイバーセキュリティ標準実務ガイドラインを正式承認しており、国内の技術基盤整備が進められている。

https://www.cac.gov.cn/2025-03/14/c_1743654685899683.htm

2-b）生成AIの安全性/セキュリティに着目した議論の動向

2024年4月29日 米国DHSら、重要インフラに対するAIリスクを防ぐためのガイドラインを発表

米国国土安全保障省（DHS）は、サイバーセキュリティ・社会基盤安全保障庁（CISA）および大量破壊兵器対策局（CWMD）と連携し、重要インフラに対するAIリスクの防止を目的とした2つの資料「重要インフラに対するAIリスクを軽減するためのガイドライン」および「化学・生物・放射線・核（CBRN）の開発と生産におけるAIの悪用に関する報告書」を公開した。これらは、米国の重要インフラを保護するとともに利害関係者によるAIの活用を支援する取り組みに基づいており、人工知能安全セキュリティ委員会も参加している。

重要インフラに対するAIリスクを軽減するためのガイドラインでは、3つのリスク（1.AIを使用した攻撃 2.AIシステムを標的とした攻撃 3.AIの設計と実装の失敗）を軸に分析をまとめ、米国国立標準技術研究所（NIST）のAIリスク管理フレームワークに基づく4つの緩和戦略（ガバナンス・マッピング・測定・管理）の概要を示している。

https://www.dhs.gov/news/2024/04/29/dhs-publishes-guidelines-and-report-secure-critical-infrastructure-and-weapons-mass

2024年5月28日 米国NIST、AIの社会的リスク評価を推進する新プログラム「ARIA」を開始

米国国立標準技術研究所（NIST）は、AIの社会的リスクと影響を評価するための新しいプログラム「ARIA（Assessing Risks and Impacts of AI）」を開始した。

組織や個人が特定のAI技術を導入する際に、技術の有効性・信頼性・安全性・セキュリティ・プライバシー保護・公正性などの担保性を判断できるような手法を開発することを目的としている。

NISTは、AIの社会的リスクを評価するためには現実的なシナリオでのテストが必要であるとの立場を示しており、ARIAプログラムでは「テスト・評価・検証・妥当性確認（TEVV）」のアプローチが採用されている。また、具体的な評価レベルとしてモデルテスト・レッドチームテスト・フィールドテストの3段階に対応するとしている。システムのパフォーマンスと精度だけを重視するのではなく、技術的な指標と社会的な指標の双方で堅牢性を測定する点に特徴があると説明している。

https://www.nist.gov/news-events/news/2024/05/nist-launches-aria-new-program-advance-sociotechnical-testing-and

https://ai-challenges.nist.gov/aria

2024年6月14日 米国CISAおよびJCDC、官民の組織とAIインシデント机上演習を実施

米国サイバーセキュリティ・社会基盤安全保障庁（CISA）は、AIセキュリティインシデントへの効果的かつ協調的な対応に焦点を当てた官民合同の机上演習をはじめて実施した。この演習には、バージニア州レストンにあるマイクロソフト社の施設で行われ、政府機関や民間企業などから50人以上のAI専門家が集まった。

演習はJoint Cyber Defense Collaborative（JCDC）が主導、AIシステムが関与するサイバーセキュリティインシデントをシミュレーションし、参加者は代表組織間でインシデント対応のための運用協力と情報共有プロトコルについて学んだ。

https://www.cisa.gov/news-events/news/cisa-jcdc-government-and-industry-partners-conduct-ai-tabletop-exercise

2024年11月26日 米国CISA、AIレッドチームの評価検証フレームワークについての考察を発表

米国サイバーセキュリティ・社会基盤安全保障庁（CISA）は、AIを対象としたレッドチーム演習のフレームワークに関する考察を発表した。同庁は、AIレッドチーム演習が既存の「テスト、評価、検証、確認（TEVV）フレームワーク」に適合する必要があると主張している。使用される具体的なソフトウェアやツールには違いがあるが、AIのTEVVは戦略的および運用的な観点からソフトウェアTEVVに基づいて処理される必要があるとした。

この主張は、TEVVが40年以上にわたってソフトウェアの安全性とセキュリティを向上させるために使用されてきたという事実に基づいているという。AI TEVVとソフトウェア TEVVでは戦術的な実装と技術的な詳細に違いはあるが、戦略的および運用的な観点から見ると2つのプロセスは非常に似ており、この主張を裏付けるすべてのソフトウェアシステムに関する事実として以下の3点を挙げている。

1. ソフトウェアシステムは常に安全上のリスクを抱えている
2. ソフトウェアシステムには妥当性と信頼性のテストが必要
3. ソフトウェアシステムは基本的に確率的である

https://www.cisa.gov/news-events/news/ai-red-teaming-applying-software-tevv-ai-evaluations

2025年1月14日 米国CISAおよびJCDC、AIサイバーセキュリティのコラボレーションプレイブックを公開

米国サイバーセキュリティ・社会基盤安全保障庁（CISA）は、官民サイバー防衛共同体（JCDC）と連携して、AIサイバーセキュリティのコラボレーションプレイブックを公開した。JCDCは、CISAが主催するサイバー防衛のアジェンダについて政府と民間が継続的な議論と対応を行うための枠組み。

この文書は、AIプロバイダー・開発者・利用者を含むAIコミュニティ向けに、インシデントや脆弱性に関する情報を自発的に共有する方法に関するガイダンスを提供している。特に積極的な情報共有によって運用コラボレーションを強化し、AIシステムの回復力を向上させる以下の事項について解説している。

・JCDCパートナーに、AIシステムに関連するインシデントや脆弱性に関する情報を自主的に共有する方法を指導する

・共有情報を受け取った後、CISAが取る可能性のあるアクションを説明する

・重要インフラ全体にわたるAIサイバーセキュリティのリスクに対する認識を高めるコラボレーションを促進し、AI技術のセキュリティとレジリエンスを強化する

https://www.cisa.gov/news-events/news/cisa-jcdc-government-and-industry-partners-publish-ai-cybersecurity-collaboration-playbook

3） 耐量子暗号移行の目途

2024年6月10日 ユーロポール、セキュリティとプライバシーのバランスに係る暗号化に関する報告書を公表

ユーロポールは関係機関と協力し、セキュリティとプライバシーのバランスに係る暗号化に関する報告書を発表した。

背景として、EncroChatやSkyECCなどの暗号化通信プラットフォームを標的とした作戦により、大規模な犯罪組織がこの技術をどの程度利用しているかが明らかになったことがある。暗号化通信の犯罪利用が急増したため、多くのEU加盟国で新たな法規定が施行され、法執行機関が犯罪捜査で暗号化通信に合法的にアクセスできるようになった。しかし、エンドツーエンドの暗号化によりテクノロジー企業が自身のプラットフォームで発生する犯罪行為を監視できないという課題があったとしている。

これを受け、2024年4月18日にロンドンで開催された非公式会議で欧州警察長官が共同宣言に合意し、業界と政府にソーシャルメディアプラットフォーム全体で公共の安全を確保するための緊急措置を講じるよう求めた。

公開された報告書の5つの主要な結論は以下の通り。

1）プライバシーとセキュリティの適切なバランスを実現するには、データへの合法的なアクセスと司法手続きにおける暗号化された通信の使用に関する法的枠組みを導入することが最も重要である

2）データへの合法的なアクセスとプライバシーの両方を確保するには、通信（5G、6Gネットワーク）・生体認証・DNS・ブロックチェーン・量子コンピューティングなどの暗号化を使用する技術の研究とキャッチアップが必要である

3）通信の全体的なセキュリティを損なうことなく、法執行機関の捜査に役立つ新しいツールを作成するには、学界や民間企業との連携が不可欠である

4）AI製品は、多面的かつ協調的なアプローチを必要とし、深刻な組織犯罪と闘う法執行機関の取り組みを支援することを妨げることもある

5）量子コンピューティングは捜査を大幅に改善できる一方で、暗号化に大きな脅威をもたらすため、ポスト量子暗号への迅速な移行が求められている

https://www.europol.europa.eu/media-press/newsroom/news/equilibrium-between-security-and-privacy-new-report-encryption

2024年12月12日 豪州信号局、暗号アルゴリズムに関するガイドラインを公開

オーストラリア信号局（ASD）は、将来の量子を利用したサイバー攻撃に備えるために暗号アルゴリズムに関するガイドラインを公開した。米国NISTは11月に、耐量子暗号標準への移行に関する最初の公開草案の中で、既存の特定の暗号化アルゴリズムは2035年に禁止され、組織には耐量子暗号アルゴリズムを実装するための約10年の猶予が与えられると述べた。一方、ASDはNISTが示した2035年は遅すぎるとし、既存の暗号化アルゴリズムに2030年という終了期限を設定する準備ができていると述べた。エディンバラ・ネイピア大学の暗号学教授ビル・ブキャナン氏はブログ投稿で、オーストラリアはSHA-256、RSA、ECDSA、ECDHなどの脆弱な暗号アルゴリズムの終了日を2030年と設定することでNISTより一歩先を進んでいると書いている。

https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cryptography

https://billatnapier.medium.com/shock-news-sha-256-ecdsa-and-rsa-not-approved-in-australia-by-2030-3d1c286cad58

2025年1月16日 米国バイデン大統領、退任直前に国家サイバーセキュリティを強化する2度目の大統領令に署名（再掲）

米国バイデン元大統領は、任期最終週に「国家のサイバーセキュリティにおけるイノベーションの強化と促進に関する大統領令（EO 14144）」への署名を行った。2021年に署名された EO 14028に続き、敵対国からのサイバー脅威へ対処するため国家サイバーセキュリティを強化することを目的としたもの。トランプ新大統領は就任直後に複数の大統領令の撤回を行っているが、現在のところ本件は撤回リストには含まれていない。

本大統領令EO 14144の各条項は、ソフトウェアプロバイダーなどの説明責任向上、連邦政府のネットワークとシステムの管理強化、新技術の利用奨励、サプライチェーンの透明性と安全性確保などの方針を定めている。具体的な施策としては、政府システムおよび重要インフラシステムを対象に次のような規則を盛り込んでいる。

1.機械読み取り可能なサイバーセキュリティ認証の義務化とCISAによる検証一元化

2.重要インフラとしての宇宙システム目録作成と通信セキュリティ担保

3.2030年までに量子耐性暗号へ移行

4.アイデンティティとアクセス管理の強化

5.AI主導のサイバー防衛パイロットプログラムの作成と研究資金の提供

https://www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity

https://www.reuters.com/technology/artificial-intelligence/biden-issue-executive-order-ensure-power-ai-data-centers-2025-01-14/

https://www.cnbc.com/2025/01/16/biden-administration-launches-cybersecurity-executive-order.html

2025年3月20日 英国NCSC、量子耐性暗号への移行に向けたガイダンスを発行

英国国家サイバーセキュリティセンター（NCSC）は、将来の量子コンピューティングの脅威を見据え、量子耐性暗号への移行に向けたガイダンスを発行した。

このガイダンスでは、主要セクターと組織（大規模組織の技術意思決定者やリスク所有者、産業用制御システムを含む重要な国家インフラシステムの運営者、特定のITシステムを持つ企業）が2035年までに量子耐性のある暗号化方式に移行するため、段階的に３つの期限を設けることを提案した。

具体的には、2028年までにITシステムの評価・移行計画を準備し、2031年までに優先度の高いシステムを量子暗号に切り替え、2035年までに全面的な移行を完了する必要があるとしている。

https://www.ncsc.gov.uk/news/pqc-migration-roadmap-unveiled

4） セキュリティ開示と司法判断の傾向

2024年6月13日 米国カリフォルニア州政府、2020年のデータ侵害事件についてソフトウェア開発企業と和解

米国カリフォルニア州政府は、2020年のデータ侵害事件に関して係争中だったソフトウェア開発企業Blackbaud社との間で、同社が和解金675万ドル（約10億円）を支払うことを条件に和解が成立したと発表した。

2020年5月にBlackbaud社のネットワークが侵害され、消費者の個人データの漏洩が発生した本件事案において、同社は攻撃者が社会保障番号や銀行口座番号を含む個人データにアクセスしたことを知りながらもデータの侵害がなかったと発表し、侵害の影響を受けたユーザーにも正確な情報を提供していなかった。

カリフォルニア州司法省の調査から、多要素認証の実装などの基本的なセキュリティ手順を実行せず、個人情報を管理するシステムで発生した不審な行動を適切に監視していなかったことが明らかになったが、同社は情報漏洩前のデータセキュリティへの取り組みや情報漏洩の程度についても虚偽の説明を行っていたことについて、その責任を問われていた。

https://oag.ca.gov/news/press-releases/attorney-general-bonta-secures-675-million-settlement-against-blackbaud-over

https://oag.ca.gov/system/files/attachments/press-docs/Complaint%5B2%5D.pdf

https://oag.ca.gov/system/files/attachments/press-docs/Blackbaud%20Judgment%20final%5B2%5D.pdf

2024年8月14日 米国対米外国投資委員会、不十分な機密データ保護を理由にT-mobile社へ制裁金

対米外国投資委員会（CFIUS）は、機密データへの不正アクセス防止と侵害時の適切な報告を怠ったとしてT-mobile社へ6千万ドル（約8.7億円）の制裁金を科した。問題の機密データへの不正アクセスは2020年8月～2021年6月に発生したが、T-mobileがインシデントを迅速に報告しなかったためにCFIUSによる米国の国家安全保障に対する潜在的な危害を調査し軽減するための取り組みが遅れたとされた。

CFIUSは財務省が主幹する組織で、国防総省・司法省・エネルギー省・商務省などの代表も参加している。国家安全保障上のリスクについて外国投資を精査する役割を担い、懸念が解消されない場合には、大統領に取引の停止を勧告する権限を有する。ドイツ資本であるT-mobileは、2018年に米国企業のSprintを買収する承認をCFIUSから得た後、同委員会と国家安全保障協定を結んでいた。

今回の制裁は、CFIUSが科した罰金としてはこれまでで最大であり、また、企業名が公表された強制措置として初の事例となった。

https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-enforcement

https://home.treasury.gov/news/press-releases/jy2537

2024年9月17日 米国連邦通信委員会、AT&T社のクラウドベンダー侵害調査について1,300万ドルで和解

米国連邦通信委員会（FCC）は、2023年1月に発生したAT&T社のクラウドベンダーにおけるセキュリティ侵害に関する調査を受け、AT&T社が1,300万ドル（約18億円）を支払うことで和解に合意したと発表した。このデータ侵害では、AT&Tの顧客情報が不正にアクセスされ、一部のデータが外部に漏洩したとされる。

AT&T社は、この和解金の支払いに加え、データセキュリティ保護策とサプライチェーンの完全性を強化することに同意する協定をFCCと締結した。同社は、請求書やマーケティング目的で使用するパーソナライズされた動画コンテンツの生成・ホスティングに外部ベンダーを利用していたが、顧客情報の保護が不十分であったことが指摘された。また、ベンダーは契約が終了した時点でAT&T社の顧客情報を破棄または返却することになっていたが、それらが実施されていなかったことも判明した。

https://www.fcc.gov/document/fcc-settles-att-vendor-cloud-breach

https://docs.fcc.gov/public/attachments/DOC-405545A1.pdf

2024年10月22日 米国SEC、サイバーセキュリティに関する重大な誤解を招く開示により4社を告発

米国証券取引委員会（SEC）は、サイバーセキュリティに関するリスクやインシデントの開示において重大な誤解を招く内容を開示したとして、Unisys・Avaya・Check Point・Mimecastの4社を告発した。2020年のSolarWinds Orion

ソフトウェア侵害事件に関する調査の一環で指摘され、4社は制裁金として少なくとも99万米ドル（約1.5億円）から最大400万米ドル（約6億円）までの支払いに合意している。

SECによれば、これらの企業はサイバーセキュリティインシデントの発生を把握していながら、その影響の範囲や性質について適切に開示せず、情報公表を最小限に抑えた。SECは連邦証券法のもとで、リスク要因の開示において誤解を招く「半真実」の提供を禁じており、重大なサイバーセキュリティ侵害を過小評価することが投資家にとってリスクとなると指摘した。

https://www.sec.gov/newsroom/press-releases/2024-174

以上