【2025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

2026年4月

JCIC 客員研究員　古澤一憲

【2025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することを目的とするものである。

今回のコラムでは、2025年度（2025年4月～2026年3月、一部2026年4月配信分を含む）に配信した174件のJCIC海外ニュースを分析し、2026年度の政策動向を占う重要な出来事を解説する。まず、2025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.　2025年度の主要なサイバー政策動向のまとめ ―激動期の前夜―

2025年度のサイバー政策動向は、エージェントAI（自律的に行動を計画・実行するAIシステム）の台頭を主題として整理することができる。前半期には生成AI全般を対象としたガバナンス議論（安全性評価、透明性要件、著作権、合成コンテンツ表示など）が各国で精力的に進められた。しかし後半期に入ると、エージェントAIの自律性が既存の認証・権限・監査の前提を揺るがす構造的要因として認識されるようになり、議論すべき論点の緊急性の構図に変化が見られた。生成AIの適正利用に関する諸論点は本来的に重要な議論であり、特にロボティクス・フィジカルAI応用領域での社会的議論などが求められ続ける。一方で、エージェントAIに関する論点への対応は、より短い時間軸での行動が要請される状況となってきている。

この主題に加え、25年度は米国のサイバー政策が大きな再編の局面を迎えた年でもある。第二期トランプ政権下で米国サイバーセキュリティ・社会基盤安全保障庁（CISA）の人員・予算の大幅な縮小、国際サイバー協力組織からの相次ぐ離脱、規制実装の延期などが相次ぎ、2026年3月には新たなサイバー戦略が公表された。また、国家背景サイバー攻撃における手法・標的の両面での質的変化の兆候、ポスト量子暗号（PQC）移行をめぐる議論の加速も継続しており、これらは相互に影響し合いながらエージェントAI時代の着岸を迎えようとしている。

JCICでは、2025年度の主要トレンドとして、エージェントAIのガバナンスと悪用の現実化、トランプ政権サイバー政策の再編、国家背景サイバー攻撃の水面下での緊張拡大、耐量子暗号（PQC）移行をめぐる議論の加速という4つのトレンドの視点から分析する。なお、各トレンドに関連するニューストピックの解説と詳細については、2章の「各トレンドの代表的なニュースの振り返り」を参照されたい。

1) エージェントAIのガバナンスと悪用の現実化

エージェントAIの自律性は、25年度のサイバーセキュリティ論議における最大の主題となった。前半期の議論は生成AI全般のガバナンス枠組みに軸足があったが、後半期には各国の政策文書・標準化文書の焦点がエージェント固有のセキュリティ論点へと移行する様子がみられた。この認識転換の射程は、AI領域内にとどまらない。米国NISTが2026年4月に公表した国家脆弱性データベース（NVD）のエンリッチメント運用の大幅見直しは、集中型・人手依存の管理手法というサイバーセキュリティの暗黙の前提が、AI時代の量的・速度的圧力の下で再設計を迫られつつあることを示している。類似の前提の揺らぎが認証・権限管理・インシデント対応・監査等の領域でも顕在化するかは、2026年度を見通す上での最も注目すべき点となるだろう。

2) トランプ政権サイバー政策の再編

第二期トランプ政権下における米国サイバー政策は、単純な縮退ではなく選別的な再編として進行した年度であった。CISAの人員・予算縮小、国際サイバー協力組織からの離脱、CIRCIA最終規則の公布延期といった制度基盤が縮小される一方で、EO 14144等の選別的継承、AI規制の連邦レベルでの統合という新たな輪郭が見え始めてきた。2026年3月に公表された新サイバー戦略は、これらの実装と整合する方向性を示した。再編によって生じた国際協力の空白に対しては、EU・英国・豪州・日本等が独自連携を模索する動きが見られるが、これが補完にとどまるか代替機能を担うかは未定である。エージェントAI時代の着岸と、米国主導のサイバー協調体制の不安定な局面が重なる現状は、各国の戦略設計にも影響を与えるだろう。

3) 国家背景サイバー攻撃の水面下での緊張拡大

従前より主要トレンドとして観測されてきた中国・ロシア・イラン・北朝鮮等による国家背景のAPT攻撃において、25年度は、質と量の両面で攻撃手法が進化する様子が水面下で観察された。新たな手法としては、AIおよびエージェント的手法の活用が仮説的懸念から具体的観察事例へと移行している。また、「事前配置（pre-positioning）」と呼称される重要インフラへの持続的侵入が、規模・範囲の両面で拡大した。中国背景アクターによる単一キャンペーンでの大規模侵害、法執行機関の通信傍受システム自体への侵入、中東の地政学的緊張を背景としたイラン関連アクターによる米重要インフラのOT環境への実害を伴う攻撃等が、25年度の代表的観察事例である。APT攻撃グループ側のAI活用と標的組織側の防御側の実装における速度差が2026年度以降どのように推移するかが重要な観点となる。

4) 耐量子暗号（PQC）移行をめぐる議論の加速

ポスト量子暗号をめぐる議論は、24年度の全体的な移行計画の発表の段階から、25年度はセクター別ガイダンスの具体化と民間実装ギャップの議論へと進展した。ユーロポールによる金融機関向け移行フレームワーク、米NSA・豪ASD等による衛星通信ガイダンス、NIST SP 800-56改訂方針といった具体化が進んだ。一方、2025年5月時点で量子安全暗号の導入済み企業は5%に留まるとされ、認識と行動のギャップが25年度を通じて論点化された。現状は、移行目標時期が具体化される中で、実装のための技術や手順については決定的なものを見通せていない段階にある。企業においては、移行タイムラインを認識しつつ、自社に適した対応を具体化するに資する情報の収集が重要になるだろう。

まとめと2026年度の展望

2025年度は、サイバーセキュリティに関する政策・制度・脅威の各領域において、AIエージェントの台頭が共通の論点として浮上した年度として整理できる。1点目で述べたエージェントAIを主題とする認識転換は、2点目の米国サイバー政策の再編、3点目の国家背景サイバー攻撃における手法・標的の質的変化の兆候、4点目の耐量子暗号移行をめぐる議論の加速と、それぞれ異なる論点のいずれに対しても転換期を示唆する形で連関している。

エージェントAIがもたらす「これまでの前提の揺らぎ」が、脆弱性管理以外の領域、たとえば認証、権限管理、インシデント検知と応答、監査といった領域においても顕在化するか、するとすればどのような形で現れるか。これらは長年にわたってサイバーセキュリティ実務の前提として機能してきた領域であり、エージェントAIの自律性と量的・速度的圧力が同様の再設計を迫る可能性が指摘されている。脆弱性管理領域におけるNVD運用の見直しに続き、どのような影響が観察されるかは、2026年度の重要な観察点となる。攻撃側のAI活用は仮説から具体事例へと移行しつつあり、この動向に対する防御側の対応能力が2026年度の脅威評価および対応態勢の設計において試される。

また、米国のサイバー協調体制の不安定化を受けて、他国間の連携が、既存枠組みの補完にとどまるのか代替機能を担うようになるのかである。特にAIおよび耐量子暗号の分野における国際標準形成において、米国以外のアクターの主導性がどの程度発揮されるかは、国際的な標準の整備環境にも影響する可能性がある。

日本企業の視点からは、これらの動向を踏まえた上で、次のような実務的論点への対応が求められると考えられる。エージェントAI時代への対応は、単なるAI技術の導入・管理の問題にとどまらず、組織のセキュリティアーキテクチャ全体の再検討を要する論点として認識することが望ましい。エージェントAIの登場を「新たな技術の追加」として捉えるのではなく、「既存のセキュリティ前提に対する構造的影響」として捉える視点が有用となるだろう。

国際的規制の情報収集においては、従前のように米国および欧州を中心とした国際的な枠組みに加えて、個別の国・地域間の連携や民間主導のイニシアティブの進展にも目を配ることが望ましい。米国主導の枠組みの不安定化に伴い、実質的な議論がこれらの場で進む局面が増える可能性がある。

耐量子暗号移行は、2030年前後の技術的必要性から逆算した計画策定が求められる長期課題であるが、影響資産の棚卸しやアセスメントといった初期段階の作業は開始可能である。英国NCSCなどが示した段階的アプローチ（アセスメ

ント、移行計画策定、優先度設計、段階的実装）は技術中立な枠組みであり、早期の着手を試みるうえでの参考となるだろう。

2026年度は、エージェントAIの普及による大きな地殻変動が本格化する一方、これまでサイバーセキュリティが抱えてきた長期の課題にも継続して取り組む必要があるという複雑な盤面を迎えることになるだろう。「前提のゆらぎ」を見極めながら、目標を見失わず道筋を修正するという難しい舵取りが要求されることになる。JCICでは、引き続き海外サイバーセキュリティ・プライバシー政策に関する動向の収集と発信を通じて、日本企業および政策関係者の皆様のビジネス戦略検討および施策立案の一助となるよう努めてまいりたい。

2. 各トレンドの代表的なニュースの振り返り

本章では、1章で解説した全体トレンドに基づき、各トレンド別の詳細解説と代表的なニュースの振り返りを行う。

1) エージェントAIのガバナンスと悪用の現実化

2025年度は、AIに関する政策・標準化の議論において、生成AI全般を対象とした基本的枠組の整備から、エージェントAIの自律性がもたらす構造的課題への対応へと、議論の重心が移動した年度として位置付けることができる。前半期のニュースには生成AIの適正利用に関する各国の制度整備が多く、後半期には個別技術領域としてのエージェントAIのセキュリティ、サプライチェーン、標準化に関する文書が増加する傾向が見られた。

1-a) 生成AI時代のガバナンス枠組み整備

2025年度前半期は、EU AI法の本格施行を受けた各国・地域の制度整備が続いた時期である。欧州委員会は2025年7月に汎用AI（GPAI）提供者向けガイドラインを公表し、透明性・著作権・安全評価に関する具体的な義務を明確化した。アジア地域では、韓国が2026年1月にAI基本法を施行し、中国は同月にAIガバナンスの規定を取り込んだ改正サイバーセキュリティ法を施行している。中国では同時期に、AI合成コンテンツの標示弁法が既に施行段階にある。シンガポールは2025年5月に「シンガポールコンセンサス」として11カ国・100名規模のAI研究者によるAI安全研究の国際的指針を整理し、AIガバナンスに関する多国間議論の場としての役割を強めている。

一方、米国ではトランプ政権下で2025年7月に「米国AI行動計画」が公表され、産業奨励を軸とするソフトロー路線が明示的に示された。2025年5月可決の「One Big Beautiful法案」および2025年12月のAI規制連邦統一に向けた大統領令は、州レベルでの独自AI規制を制限する方向性を示している。欧州のハードロー路線との対比は、24年度に既に顕在化していた構図の継続・拡大として位置付けられる。

[参照ニュース]

2025年5月8日　シンガポール、AI安全研究の国際的指針「シンガポールコンセンサス」を発表

シンガポール情報通信メディア開発庁（IMDA）は、AIの安全性に関する国際的な技術的優先課題を定義する文書「シンガポールコンセンサス」を発表した。これは、同日に開催されたシンガポール人工知能会議（SCAI）において取りまとめられたものであり、11カ国から100名のAI研究者が参加した。参加国には、中国、米国、欧州諸国、日本などが含まれる。

本コンセンサスは、政策的議論は除外し「より信頼できる汎用AI」の実現を目的とした技術的課題に焦点を当てている。内容は国際AI安全報告書（IAISR）を参照し、多層防御モデルを基本構造として採用している。AI安全性の研究テーマは以下の3領域に分類された。

第1の領域「リスク評価課題」AIが引き起こし得る潜在的危害の深刻度と発生確率を評価し、対策の優先順位と対応閾値の判断を行うための基盤とされる。

第2の領域「開発課題」古典的な安全工学の枠組みに従い、望ましいAI行動の仕様定義、設計、検証プロセスが対象となる。

第3の領域「展開後の制御課題」AIシステムに対する監視・介入メカニズムの開発、AIエコシステム全体への監視の拡張、社会的・経済的インフラのレジリエンス強化に関する研究が含まれる。

https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/top-scientific-minds-gathered-in-sg-to-advance-ai

https://www.scai.gov.sg/2025/scai2025-report

2025年7月18日　欧州委、汎用AIモデル提供者のためのガイドラインを発表

欧州委員会は、汎用AIモデルの提供者に向けた新たなガイドラインを発表した。2025年8月2日より適用されるEU AI規則を補完する措置として位置付けられる。

本ガイドラインでは、「汎用AIモデル」の定義を「10の23乗の浮動小数点演算を超える計算リソースを使用してトレーニングされ、言語の生成（テキストまたは音声形式）、テキストから画像への変換、またはテキストからビデオへの変換が可能であることとしている。

また、提供者とみなされる条件と遵守すべき義務の範囲、オープンソース開発者に対する適用免除条件も明確化された。具体的には、AIモデルに対して軽微な変更が行われた場合には、義務の遵守が不要となる一方で、システミックリスクをもたらす高度なモデルについては、提供者がリスク評価を実施し、その結果を欧州AI事務局に通知する法的義務が課される。また、透明性、情報公開、セキュリティに関する責任についても、モデルの特性に応じた要件が段階的に定められている。

https://digital-strategy.ec.europa.eu/en/policies/guidelines-gpai-providers

https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act

2025年7月23日　米国ホワイトハウス、米国AI行動計画を発表

米国ホワイトハウスは、米国AI行動計画を発表した。2025年1月に発令された大統領令EO14179に基づき、米国がAI分野における優位性を確立し、国際的な競争環境において勝利するために、連邦政府が短期的に実施すべき優先政策目標を示したもの。

この行動計画は、（1）イノベーションの加速 （2）AIインフラの構築 （3）国際外交および安全保障の主導 という3本柱から構成されている。具体的施策として、AIに関する既存規制の撤廃、オープンソースAIの積極的推進、政府・防衛・医療・教育など各分野におけるAIの導入促進が含まれている。また、AI駆動型科学研究や高品質なデータ基盤への投資の強化、同盟国・パートナー諸国へのAI技

術輸出支援も明記された。さらに、国際的AI統治体制における中国の影響力拡大への対抗措置、およびAIを活用したバイオセキュリティ分野への戦略的投資が政策目標として盛り込まれている。

https://www.whitehouse.gov/articles/2025/07/white-house-unveils-americas-ai-action-plan/

https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

https://www.ai.gov/action-plan

2025年5月13日　米国下院、州自治体によるAI規制の制限を含む「The One Big Beautiful」法案を可決

米国下院予算委員会は、州自治体によるAI規制の制限を含む「The One Big Beautiful法案」を可決した。同法案は、減税措置や国境警備の強化といったトランプ大統領の主要政策を包含する広範な立法案であるが、中でも「州および自治体が独自のAI規制を実施することを10年間禁止する」条項が注目を集めている。

このAI条項は、技術革新の阻害を防止する意図のもと導入されたとされ、各州自治体はAIモデルやAIシステムに関する規制を定めることを10年間禁じられることになる。これにより、AIガバナンスの権限は連邦政府に一元化される見通しである。

同条項には批判も多く、40名の州司法長官から成る超党派連合は、企業による未完成で責任のないAI開発を懸念し、上院に対し本法案の否決を強く求めている。

https://docs.house.gov/meetings/IF/IF00/20250513/118261/HMKP-119-IF00-20250513-SD003.pdf

https://waysandmeans.house.gov/wp-content/uploads/2025/05/The-One-Big-Beautiful-Bill-Section-by-Section.pdf

https://coag.gov/press-releases/attorney-general-phil-weiser-bipartisan-ag-letter-congress-artificial-intelligence-regulations-5-16-25/

2025年12月11日　米国ホワイトハウス、AI規制の連邦統一に向けた大統領令に署名

米国トランプ大統領は、AIに関する規制を連邦全域で統一し、州ごとの異なる規制を排除するための大統領令に署名した。州法による規制の断片化が米国のイノベーションを阻害しているとの懸念を解消する狙いがある。

本大統領令に基づき、司法省には「AI訴訟タスクフォース」が設置され、過度に制限的な州法や違憲の疑いがある規制への法的対抗措置を主導する。また、商務省に対しては、連邦のAI政策と矛盾する規制を導入する州への連邦資金提供を制限するよう求めた。さらに、連邦取引委員会および連邦通信委員会に対し、州がAI企業に対して特定のイデオロギーや多様性・公平性・包括性（DEI）要件を強制することを防ぐための基準策定を指示している。

全米では1,000件以上のAI関連法案が提出されており、企業にとって対応コストの増大が課題となっていた。政権はこれを「常識的なAI政策（Common Sense AI Policy）」の一環と位置づけ、5月に成立したディープフェイク対策法「Take It Down Act」などの既存施策と同様に、統一された連邦基準の確立により国際的な競争力を維持する目論見。

https://www.whitehouse.gov/fact-sheets/2025/12/fact-sheet-president-donald-j-trump-ensures-a-national-policy-framework-for-artificial-intelligence/

2026年1月1日　中国当局、AIガバナンス等を盛り込んだ「改正サイバーセキュリティ法」を施行

中国国家インターネット情報弁公室（CAC）は、AIガバナンスの強化等を盛り込んだ「改正サイバーセキュリティ法」を施行した。

まず、基本理念として国家安全と中国共産党の指導が明確化された。また、米国のガイドライン方式やEUのリスク規制モデルとは異なり、発展支援と安全確保を並行して追求する独自の中庸型ガバナンスモデルを採用したとしている。

新設された第20条では、AIの健全な発展と安全管理が制度的に位置づけられ、国家による研究開発支援、訓練データの品質向上、倫理・監督体制の強化など、包括的な規律枠組みが提示された。第42条では、個人情報保護に関して、ネットワーク運営者が「個人情報保護法」や「民法典」などの関連法と整合的に法的義務を負うことが明記された。

また、罰則体系も刷新され、従来の二段階から四段階に拡張されるとともに、最高額が1000万元（約2億円）に引き上げられた。法的措置では、ウェブサイトの閉鎖に加え、モバイルアプリケーションの閉鎖も可能となり、モバイル規制が強化された。

さらに、法の域外適用範囲も拡大された。従来は「重要インフラへの重大な危害」に限られていた追及対象が、中国のネットワークの安全を危害するすべての海外行為に及ぶこととなり、クロスボーダーなサイバー攻撃やデータ窃取への対処能力が強化されている。

https://www.cac.gov.cn/2025-12/29/c_1768735112911946.htm

https://www.cac.gov.cn/2026-01/02/c_1769093523928606.htm

2026年1月22日　韓国、AI基本法を施行

韓国政府は、人工知能産業の育成と信頼性の確保を目的とした「人工知能発展と信頼基盤造成基本法（AI基本法）」を施行した。2020年の発議から4年以上の議論を経て成立した本法は、包括的なAI規制・振興法として全面適用される。

本法の施行により、大統領を委員長とする「国家AI委員会」および「AI安全研究所」が新設され、政府には3年ごとの「AIマスタープラン」の策定が義務付けられた。産業支援策としては、AIデータセンターの設立支援や人材育成、中小企業・スタートアップへの技術援助などが盛り込まれている。また、施行に合わせて「AIフレームワーク支援デスク」が稼働を開始。中小企業に対し、法務・技術面でのコンサルティングを提供し、法制度の定着を支援する。

規制面では、社会に大きな影響を及ぼす「高リスクAI」および「生成AI」を対象に、安全性と透明性の確保が義務化された。具体的な規定は以下の通り。

・透明性の確保： 利用者への事前通知および生成物へのラベル（ウォーターマーク）表示の義務付け

・高影響分野の監督： 原子力安全、医療、交通、飲料水、金融（与信審査等）の5分野において、人間による監督および国内責任者の選任を必須化

・リスク評価： 企業による自主的なリスク評価と、安全管理体制の構築

https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=1071&searchOpt=ALL

1-b）エージェントAI時代への認識転換

2025年度後半期に入ると、AIに関する政策文書・標準化文書の主題として、エージェントAI固有のセキュリティ論点を扱うものが増加した。シンガポールは2026年1月に「エージェント型AI向けガバナンスフレームワーク」を公表し、自律的意思決定への責任帰属や人間による監督要件を整理している。英国科学イノベーション技術省の「国際AI安全報告書2026」（2026年2月）は、エージェントAIの制御問題と評価手法の標準化を重点課題に位置付けた。米国NISTは2025年12月に「AIサイバーセキュリティプロファイル」（NISTIR 8596）の草案を公表し、サイバーセキュリティフレームワーク（CSF 2.0）との統合を想定した枠組みの検討を進めている。2026年3月には、米英豪日等8カ国によるAI/MLサプライチェーンセキュリティに関する共同ガイダンスも公表された。

悪用事例も後半期には具体化している。商用生成AIを悪用した大規模侵害に関するAmazonからの注意喚起（2026年3月）や、AI生成マルウェアによる国家背景攻撃の観察事例（詳細は③で述べる）が報告された。英国NCSCが2026年4

月に公表したAI脅威評価レポートは、エージェントAIを最大の新興脅威として特定している。エージェント固有のリスクープロンプトインジェクション、ツール権限の昇格、メモリポイズニング等ーーは、従来のセキュリティ対策が前提としていたシステム境界や権限管理の考え方に再検討を促す要素として認識されつつある。

[参照ニュース]

2025年12月16日　米国NIST、AIサイバーセキュリティプロファイル「NISTIR 8596」草案を公表

米国国立標準技術研究所（NIST）は、組織がAIを安全に導入するための指針として「サイバーAIプロファイル草案（NISTIR 8596）」を公表した。本草案は、NISTのサイバーセキュリティフレームワーク（CSF 2.0）をAI分野に適用し、AI導入に伴うサイバーリスクへの対応策を整理したものである。組織がAI活用とサイバーセキュリティ目標を整合させ、リスクを理解した上で戦略的に導入することを支援する狙いがある。

同ガイドラインは、以下の3つの重点領域を中心に構成されている。

（1）AIシステムの保護（Secure）：AI導入に伴う技術的なセキュリティ課題への対応

（2）AIを活用した防御（Defend）：AIを用いてサイバー防御を強化する方法

（3）AIを悪用した攻撃への対策（Thwart）：AIに起因する新たな脅威への備え

草案に対するパブリックコメントは45日間受け付けられ、寄せられた意見をもとに2026年に改訂版が公開される予定である。最終版では、AIリスク管理フレームワークなど他のNISTリソースとの整合性も強化される見通しとなっている。

https://www.nist.gov/news-events/news/2025/12/draft-nist-guidelines-rethink-cybersecurity-ai-era

2026年1月22日　シンガポール、エージェント型AI向けガバナンスフレームワークを公表

シンガポール情報通信メディア開発庁（IMDA）は22日、自律的に思考・行動するエージェント型AIの安全な導入と活用の支援を目的とする包括的なガバナンスフレームワークを発表した。本指針は、同国が2020年に策定した「AIガバナンスモデルフレームワーク」を高度化させたもので、イノベーションの促進とリスク管理の両立を目的としている。

エージェント型AIは、自律的な計画立案や外部システムとの連携により企業の生産性を飛躍的に高める一方、機微データへのアクセス権限を持つことによる誤操作や未承認行動、さらには「自動化バイアス（人間による過度の信頼）」といった新たなリスクを内包している。

IMDAが提示したフレームワークは、以下の「4つの柱」に基づき、企業が技術・運用の両面からリスクを制御することを推奨している。

（1）リスク評価と権限の境界設定： 利用ケースごとにリスクを評価し、AIエージェントの自律性やアクセス権限を設計段階で制限する。

（2）意味のある人間の関与： 重要なアクションに対する人間の最終承認プロセスを組み込み、責任の所在を明確化する。

（3）技術的コントロールとプロセス： ライフサイクル全体を通じた継続的なモニタリング、ベースラインテスト、アクセス管理を徹底する。

（4）エンドユーザーの責任と透明性： ユーザー教育を実施し、AIが実行可能な権限の範囲を明確に開示する。

https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2026/new-model-ai-governance-framework-for-agentic-ai

2026年2月3日　英国科学イノベーション技術省、「国際AI安全報告書2026」を公表

英国科学イノベーション技術省（DSIT）は3日、汎用AI（GPAI）がもたらすリスクと管理策をまとめた「国際AI安全報告書2026」を公表した。インドでのAIサミットに先立ち公開された同報告書は、政策立案者や意思決定者を対象に、汎用AIシステムの能力がもたらす新たなリスク評価とその管理アプローチを提案している。内容は、EU、OECD、国連を含む30カ国以上から推薦された100名超の専門家により監督されている。

急速に進化する汎用AIについては、高度な推論が可能である一方、単純なタスクで失敗するなど、能力に不均一性が見られる点を指摘している。さらに、詐欺やディープフェイク、サイバー攻撃、兵器関連情報の提供といったリスクに加え、人間の思考力低下や孤独感の増加などの社会的影響が確認されていると述べている。技術的な安全策は進展しているものの、完全な防止には不十分であることや、オープンモデルのリスクが大きい点も強調、多層的な防御と社会全体のレジリエンス強化が不可欠であると結論づけた。

https://internationalaisafetyreport.org/publication/international-ai-safety-report-2026

https://internationalaisafetyreport.org/

2026年3月13日　8カ国がAI/MLサプライチェーンのセキュリティに関する共同ガイダンスを公表

カナダ・サイバーセキュリティセンター（CCCS）を主導機関として、豪州、日本、ニュージーランド、韓国、シンガポール、英国、米国の8カ国のサイバーセキュリティ機関が、AI（人工知能）およびML（機械学習）のサプライチェーンに関する共同ガイダンスを公表した。同ガイダンスは、組織がAI技術を導入する際にサプライチェーン上で生じうる脆弱性を理解し、適切なリスク軽減策を講じるための指針を示すものである。

ガイダンスでは、訓練データ、モデル、ソフトウェアライブラリなどのサードパーティ由来のコンポーネントに潜むリスクを重点的に取り上げている。具体的には、データポイズニング（可用性・標的型・バックドア型）によるモデルの汚染、悪意あるモデルの混入、依存ライブラリの脆弱性などが挙げられている。AIツールは業務効率の向上に寄与する一方、管理が不十分なサプライチェーンは深刻なセキュリティリスクをもたらすと警告している。日本を含む8カ国の共同署名は、AI/MLセキュリティが国際的な政策課題として認識されていることを示すものである。

https://www.cyber.gc.ca/en/news-events/joint-guidance-supply-chain-risks-mitigations-artificial-intelligence-machine-learning

https://www.cyber.gov.au/business-government/secure-design/artificial-intelligence/artificial-intelligence-and-machine-learning-supply-chain-risks-and-mitigations

2026年4月8日　英国NCSC、2027年に向けたAI脅威評価レポートを公表

英国国家サイバーセキュリティセンター（NCSC）は「AI to 2027」と題した脅威評価を公表し、AIを活用したサイバー攻撃が向こう2年間で英国の重要システムへのリスクを著しく高めると警告した。

評価では、脅威アクターがAIを用いて攻撃の自動化・高度化・低コスト化を実現しつつある一方、防御側組織のAI活用能力には大きな格差（デジタルデバイド）が生まれており、この非対称性が重要インフラの脆弱性を拡大させると指摘している。国家支援型アクターやランサムウェアグループが偵察・フィッシング・マルウェア開発にAIをすでに活用していること、またAIエージェントの自律的なサイバー攻撃への応用が現実的な脅威になりつつあることも示された。NCSCは組織に対し、AIセキュリティへの投資加速と、AI活用の防御能力格差を埋めるための具体的対策を講じるよう促している。

https://www.ncsc.gov.uk/news/ai-to-2027-threat-assessment

1-c) エージェントAI時代における前提の揺らぎ

エージェントAI時代の到来は、既存のサイバーセキュリティが長年依拠してきた慣習的な前提にも変化を迫り始めている。象徴的な事例は、米国NISTが2026年4月に公表した国家脆弱性データベース（NVD）のエンリッチメント運用の大幅見直しである。CVE提出件数は2020年から2025年の5年間で263%増加し、2026年第1四半期時点でも前年同期比で約3割増のペースで推移している。NISTは全件自動エンリッチメントを断念し、CISAのKEVカタログ掲載、連邦政府使用ソフトウェア、EO 14028が定義する重要ソフトウェアのいずれかに該当するCVEを優先する方式へと運用を転換した。

量的圧力に加え、より構造的な変化として注目すべきは、大規模言語モデル（LLM）を用いた脆弱性発見の本格化である。2026年4月、Anthropic社はサイバーセキュリティ用途に特化した次期モデル「Claude Mythos」をセキュリティ研究者・組織向けに限定公開し、OpenAI社も同時期に「GPT-5.4-Cyber」の限定提供を開始した。これらの高度AIモデルは、防御側の脆弱性発見を大幅に加速させる一方、攻撃側による同種の能力活用の可能性も示唆するものであり、CVE提出件数の今後の増加要因としても指摘されている。25年度までの量的増加は主に研究コミュニティと自動化ツールの拡充によるものであったが、LLMによる脆弱性発見の本格化は、発見速度そのものの桁を変える可能性がある。

NISTがエンリッチメント運用の見直しを余儀なくされた直接の背景には人員・予算の制約もあるが、より本質的には、集中型の人手による脆弱性情報の品質管理という、サイバーセキュリティが長年にわたって暗黙の前提としてきた慣習が、AI時代の量的・速度的圧力によって成立しなくなりつつあると捉えることができるだろう。同様の前提の揺らぎは、認証、権限管理、インシデント検知と応答、監査といった領域においても今後顕在化するか、どのようなで影響をするかは2026年度以降の重要な観点となるだろう。

[参照ニュース]

2026年4月15日　米国NIST、CVE提出数の急増を受けNVDの脆弱性エンリッチメント運用を大幅見直し

米国国立標準技術研究所（NIST）は、国家脆弱性データベース（NVD：National Vulnerability Database）の運用方針を大幅に変更し、リスクベースのトリアージモデルへ移行することを発表した。CVE（共通脆弱性識別子）の提出件数が2020年から2025年の間に263%増加し、NISTが2025年に処理したCVEは4万2,000件にのぼるが、増加速度への対応が限界に達したことが背景にある。

新方針では、CISAの既知悪用脆弱性（KEV：Known Exploited Vulnerabilities Catalog）に掲載されたCVEを受領から1営業日以内に最優先でエンリッチメント（CVSSスコア付与・CPE情報追加等）する。次に連邦政府使用ソフトウェアおよび大統領令14028が定義する重要ソフトウェアのCVEを優先する。これらの基準を満たさないCVEは「最低優先度」に分類され、即座の処理は行われない。また2026年3月1日以前のバックログCVEは「未スケジュール」カテゴリに移行する。

本変更は組織のパッチ優先順位付けプロセスに直接影響する。NVDのエンリッチメントに依存して脆弱性管理ツールを運用している場合、KEVおよびCVE採番機関（CNA）が提供するスコアリングの参照に移行することが推奨される。優先対象外のCVEについては申請でエンリッチメントを要求できる。

https://www.nist.gov/news-events/news/2026/04/nist-updates-nvd-operations-address-record-cve-growth

https://www.securityweek.com/nist-prioritizes-nvd-enrichment-for-cves-in-cisa-kev-critical-software/

2026年4月7日　Anthropic、次期AIモデル「Claude Mythos」をサイバーセキュリティ用途に限定公開

米国のAI企業Anthropicは、同社の主力モデルClaudeの次期モデル「Mythos」のプレビュー版を発表した。同モデルは主要なオペレーティングシステム・ウェブブラウザ・ソフトウェアを対象に、事前に未知の重大ゼロデイ脆弱性を数千件規模で自律的に発見する能力を持ち、その中には27年前に遡る脆弱性も含まれる。Anthropicは悪用リスクを考慮し、一般公開を見送り、Amazon、Apple、Cisco、CrowdStrike、Microsoft、Palo Alto Networks、Linux財団等のテクノロジー・サイバーセキュリティ企業40社超を含む限定パートナーのみに提供する方針を採った。

同時に「Project Glasswing」を始動し、Mythos Previewを活用して世界の重要ソフトウェアインフラのセキュリティ強化に取り組む方針を示した。Anthropicは同プロジェクトに最大1億ドル（約155億円）相当の利用クレジットと400万ドル（約6億2,000万円）のオープンソースセキュリティ組織への寄付を拠出する。本件の社会的インパクトは大きく、米財務長官や米連邦準備制度理事会（FRB）議長が大手銀行CEOとAIモデルがもたらすサイバーリスクを協議する場が設けられたとも報じられている。

https://red.anthropic.com/2026/mythos-preview/

https://www.anthropic.com/glasswing

https://techcrunch.com/2026/04/07/anthropic-mythos-ai-model-preview-security/

2) トランプ政権サイバー政策の再編

2026年3月、第二期トランプ政権下での新たなサイバー戦略が公表された。中露・イラン・北朝鮮への強硬姿勢の維持、国際協力の選別的縮小、国内産業優先、規制コストの削減という方向性が示されたが、個別施策の具体性については限定的であるとの評価もある。一方、同戦略が示す方向性と、25年度を通じて段階的に実装されてきた諸施策との整合性は高い。本節では、25年度の米国サイバー政策の動向を、制度基盤の縮小、選別的継承、新たな輪郭という3つの観点から整理する。

2-a）制度基盤の縮小

25年度は、これまで米国のサイバーセキュリティ政策基盤を担ってきた制度・組織の大幅な縮小が続いた。

米国サイバーセキュリティ・社会基盤安全保障庁（CISA）については、2026年度予算要求で約4億9,500万ドル（前年度比約17%）の削減が示され、1,300人規模の人員削減または早期退職が実施される見通しとなった。2025年10月には、州・地方政府、民間企業、外国パートナーとの重要インフラ調整を担ってきたステークホルダー連携部門（Stakeholder Engagement Division）約95人のほぼ全員が解雇された。同部門は、国内の情報共有と同盟国との実務連携の両面で重要な機能を果たしてきたものであり、これら連携の継続性への懸念が指摘されている。

米国務省においては、2022年に設立されたサイバー空間・デジタル政策局（Bureau of Cyberspace and Digital Policy）が解体された。国際サイバー協力の枠組みとしては、サイバー専門知識グローバルフォーラム（Global Forum on Cyber Expertise、GFCE）、オンライン自由連合（Online Freedom Coalition）、欧州ハイブリッド脅威対策センター（European Centre of Excellence for Countering Hybrid Threats）等からの相次ぐ離脱が発表されている。

規制面では、「重要インフラのためのサイバーインシデント報告法」（CIRCIA）に基づく最終規則の公布が、2026年5月以降に再度延期された（2026年3月発表）。重要インフラ事業者のインシデント報告義務化は、24年度時点で実装が期待されていた主要施策のひとつであり、その遅延は民間セクターのコンプライアンス計画における不確実性として継続している。

[参照ニュース]

2025年6月6日　米国ホワイトハウス、国家サイバーセキュリティ戦略を一部修正する大統領令を公表

米国ホワイトハウスは、トランプ大統領が新たな大統領令に署名し、国家サイバーセキュリティの強化を目的とする厳選された施策の維持と過去の大統領令の一部修正を行うと発表した。外国からのサイバー脅威からの保護を国家サイバー安全保障政策の主眼とし、安全な技術慣行の徹底と制度改革を通じた防衛力の向上を目指す。加えて、過去の大統領令13694号（オバマ政権）および14144号（バイデン政権）に含まれるサイバー政策の見直しと修正を行い、イノベーション促進のメッセージを強化している。

具体的には、不法移民が政府発行の身分証明書を用いることで公的サービスの不正受給が可能となる懸念から、当該IDの対象から不法移民を除外する規定を導入している。また、AI利用に関する定義を「検閲」から「脆弱性管理」へと再定義し、コンテンツ統制による言論の自由の侵害や技術革新の阻害を回避する観点が強調された。さらに、次世代型のコンピュートアーキテクチャに基づく高度なサイバー脅威への備えとして、ポスト量子暗号（Post-Quantum Cryptography：PQC）の導入を各省庁に対して指示した。これにより、量子計算時代における暗号脆弱性の克服を目指すとしている。

この他にも、サイバーセキュリティ政策の普及を目的とした技術的措置の推進も盛り込んでおり、国内のセキュリティ基準の見直しおよび法制度との整合性の強化を図る内容となっている。

https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/

https://www.whitehouse.gov/fact-sheets/2025/06/fact-sheet-president-donald-j-trump-reprioritizes-cybersecurity-efforts-to-protect-america/

2026年3月3日　米国CISA、CIRCIA最終規則の公布を2026年5月以降に延期

米国サイバーセキュリティ・社会基盤安全保障庁（CISA）は、重要インフラ事業者にサイバーインシデントの報告を義務付ける「サイバーインシデント報告法」（Cyber Incident Reporting for Critical Infrastructure Act: CIRCIA）の最終規則について、当初2025年9月を予定していた公布時期を2026年5月以降に延期した。提案規則に対して数百件の意見が寄せられ、「対象事業者」の定義の広さと「対象サイバーインシデント」の範囲に関する業界からの反発が主な要因である。

最終規則では、対象事業者はサイバーインシデント発見から72時間以内にCISAへ報告し、身代金の支払いについては24時間以内に通知することが求められる。報告には技術的詳細、不正アクセスの内容、タイムライン、業務への影響、悪用された脆弱性、攻撃者の戦術・技術・手順（TTPs）、侵害指標（IoC）、および対処措置の記載が必要となる。CISAの分析によれば、規模基準のみで約3万の事業者が対象に含まれる見込みであり、業界からはその広範さに懸念が示されている。なお、政府シャットダウンの影響で2026年3～4月に予定されていた意見聴取会（タウンホール）も延期されている。

https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

https://www.dwt.com/blogs/privacy--security-law-blog/2026/02/cisa-seeks-input-cybersecurity-reporting-rules

2-b) 選別的継承

一方で、トランプ政権が発足後も撤回・廃止を選択しなかった施策や、新政権下でも維持された枠組みも存在する。

バイデン前大統領が退任直前（2025年1月）に署名したEO 14144「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」は、2026年4月時点も撤回されていない。同EOは、2030年までの耐量子暗号への移行、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、AI主導のサイバー防衛パイロットプログラム等を規定するものであり、その内容は後述のポスト量子暗号移行やAI防衛の議論とも連関する。

MITRE社が運用するCVEプログラムについては、2025年4月にCISAが連邦資金の継続を発表した。同時に、米国一国の予算措置に依存する現行の運用体制を脱することを目的としたCVE財団の設立も発表された。脆弱性識別子プログラムという国際的サイバー防御の基礎機能については、形式的な米国資金の継続と、米国依存からの段階的脱却の準備が並行する形となっている。なお、米国立標準技術研究所（NIST）によるNVDのエンリッチメント運用の見直しについては既に「エージェントAI時代における前提の揺らぎ」の節で述べたとおりである。

脅威評価の観点では、2026年3月に米国家情報長官室（ODNI）が公表した「2026年次脅威評価」において、中国・ロシア・イラン・北朝鮮が引き続き主要サイバー脅威アクターとして指定された。CISA、米連邦捜査局（FBI）、米国家安全保障局（NSA）による中国系脅威アクター（Volt Typhoon、Salt Typhoon等）への警戒情報発信や、2026年4月のイラン系APTによる重要インフラPLC攻撃に関する合同勧告など、特定国家に対する強硬姿勢の発信は継続している。これらは、2026年3月のトランプ戦略における中露強硬姿勢の継承と整合する動向である。

[参照ニュース]

2025年4月16日　米CISA、CVEプログラムへの資金継続を発表　CVE財団設立により独立運用の検討も

米国サイバーセキュリティ・社会基盤安全保障庁（CISA）は、MITRE社が運営する脆弱性情報データベース「CVE（Common Vulnerabilities and Exposures）」プログラムに関して、11か月間の契約延長を決定した。これにより、CVEプログラムの継続的な運用が確保され、サービスの中断が回避される見通しとなった。背景として、前日の4月15日にMITRE副社長バルスーム氏が、CVEプログラムへの資金が期限切れとなり、連邦政府に契約を更新する意向がみられないと警告する書簡をCVE理事会へ提出したことで、サイバーセキュリティ関係者の多くが懸念を表明していた。

CISA広報担当者は声明の中で「CVEプログラムはCISAの優先事項であり、サイバーコミュニティにとって極めて重要である」と強調し、MITRE社との取り組みを再確認したという。延長期限後の運営に関しては不確定要素が残るが、CISAはその点についての明言を避けている。

CISAの発表と平行し、CVE理事会の有志メンバーらによって非営利団体「CVE財団（CVE Foundation）」の設立が発表された。CVE理事会は、CVEプログラムの運営が単一政府の資金に依存していることは長年の懸念点であったと述べ、CVE財団の設立によって中立的かつ持続可能なガバナンス体制を確立することを目指すとしている。財団の共同設立者でありCVE理事のランドフィールド氏は、CVEプログラムの重要性を強調し、国際的に信頼されるコミュニティ主導の取り組みであり続けることための取り組みだと説明した。財団の体制等の詳細は今後明らかにされる予定。

両者の発表をうけ、MITRE社は、引き続き政府・CVE委員会・セキュリティコミュニティと連携していく予定であるとコメントしている。

https://x.com/CISAgov/status/1912522040935850445

https://www.thecvefoundation.org/

https://therecord.media/cisa-extends-cve-program-contract-with-mitre

https://www.nextgov.com/cybersecurity/2025/04/mitre-backed-cyber-vulnerability-program-lose-funding-wednesday/404585/

2026年3月26日　米国家情報長官室、2026年次脅威評価を公表

米国家情報長官室（ODNI）は3月26日、米情報コミュニティによる「2026年次脅威評価（Annual Threat Assessment）」を公表した。移民、麻薬、テロ、ミサイル、サイバー、AIといった幅広い分野を対象に、米国が直面する主要な安全保障上の脅威を整理。国土防衛を最優先課題と位置づけた。

サイバー領域では、中国とロシアを最も持続的かつ深刻な脅威と評価し、両国が米政府機関だけでなく、民間や重要インフラを標的とした攻撃能力の強化を進めていると指摘。中国は有事の際、特にインド太平洋地域の危機において戦略的優位を確保する目的で重要インフラを破壊・妨害する能力をすでに実証済みであるとしている。ロシアもサイバー作戦のR&Dを継続しており、依然として高度な持続的脅威（APT）と位置づけられた。北朝鮮については、2025年だけで約20億ドル（約3,100億円）相当の暗号資産を窃取し、その資金が核・弾道ミサイル開発に充当されている可能性が高いと分析された。イランも重要インフラを標的とした攻撃を継続しているとされる。

また、AIの急速な進展がサイバー攻撃の高度化・効率化を促し、脅威をさらに拡大させるとして警告。中国は2030年までにAI分野で米国を追い越すことを目標に掲げており、量子コンピュータや宇宙領域の軍事化も含め、技術競争の激化が国際的な安全保障環境を不安定化させると分析した。国家主体に加え、ランサムウェア集団などの非国家主体も深刻な脅威であり続けるとした。これらの勢力は、情報窃取や資金獲得といった利益を背景に、米国の政府ネットワークや重要インフラを継続的に狙っているという。

ODNIは「情報は米国の最も鋭い防衛手段である」と強調し、政権や議会に対して迅速かつ客観的な情報提供を今後も続ける姿勢を示した。

https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2026/4141-2026-annual-threat-assessment

https://industrialcyber.co/reports/odni-report-us-critical-infrastructure-faces-escalating-cyber-risks-from-china-russia-iran-and-north-korea/

2-c) 新たな輪郭

新規に導入された政策的方向性としては、AI規制の連邦レベルへの統合が挙げられる。2025年5月に米国下院で可決された「One Big Beautiful法案」は、州独自のAI規制を連邦レベルで制限する条項を含むものであった。続く2025年12月には、AI規制の連邦統一に向けた大統領令が署名され、州規制との整合性を強制する方向性が明確化された。これらは、①で述べた米国のソフトロー路線を、規制主体の統一という別軸から強化する動きとも位置付けられる。欧州のハードロー型AI規制との方向性の対称性は、24年度から指摘されてきた構図が一層鮮明化したものと捉えられる。

トランプ政権のサイバー政策の輪郭は、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根幹を維持しつつ、国際協力や民間規制の実装コストを大幅に圧縮し、AI等の新興技術領域では連邦レベルでの規制統一によって産業活動を優先する構成へと再編されつつあると評価できる。

米国サイバー政策の再編によって生じた国際協力の空白に対し、EU・英国・豪州・日本等が二国間・多国間の独自連携を強化する動きが見られる。これらの連携が米国主導の既存枠組みを補完するものとなるか、あるいは代替する性格のものとなっていくかは、2026年度の重要な観察点となるだろう。また、AIエージェント時代における前提の揺らぎという転換期を迎える局面において、米国のサイバー協調体制が最も不安定な状況にあるという点は、各国のサイバー戦略設計においても考慮すべき構造的要因となると考えられる。

[参照ニュース]

2026年3月6日　米ホワイトハウス、「トランプ大統領のサイバー戦略」を公表

米ホワイトハウスは6日、国家サイバー戦略文書「President Trump's Cyber Strategy for America」を公表した。本戦略は、サイバー空間を地政学的競争の主要領域と位置付け、攻撃的サイバー作戦の強化を明確に打ち出した点が特徴である。

戦略は6つの柱で構成される。（1）「敵対者の行動を抑止・変容させる」では、攻撃・防御の両面から国家・犯罪系サイバー脅威アクターに対するコスト賦課と抑止を推進する。（2）「合理的な規制の推進」では、サイバー・データ規制を簡素化し、民間部門の迅速な対応を可能にする方針を示した。（3）「連邦ネットワークの近代化」では、ゼロトラスト・クラウド移行・AI駆動型セキュリティ・ポスト量子暗号の導入を掲げる。（4）「重要インフラの防護」では、エネルギー・金融・通信・水道・医療の各分野における官民協力とサプライチェーンの強靭化を目指す。（5）「技術的優位性の維持」では、AI・量子コンピューティング・暗号技術における米国の主導的地位の確保を明記した。（6）「サイバー人材の育成」では、政府・学界・産業界の連携による人材基盤の拡充を推進する。

同日、トランプ大統領はサイバー犯罪・詐欺対策に関する大統領令にも署名し、国際犯罪組織によるサイバー犯罪への対策強化と専門作戦セルの設置を指示した。

https://www.whitehouse.gov/articles/2026/03/white-house-unveils-president-trumps-cyber-strategy-for-america/

https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf

3) 国家背景サイバー攻撃の水面下での緊張拡大

国家背景のサイバー攻撃は、JCICニュースクリップで従前より主要トレンドとして扱ってきたテーマであり、25年度も中国・ロシア・イラン・北朝鮮等の脅威アクターによる活動が引き続き主要な脅威として観測されている。23年度には中国Volt Typhoonによる米国重要インフラへの破壊的サイバー攻撃への焦点化、24年度には各国の脅威評価と告発・制裁の蓄積を整理してきたが、25年度はこれら継続的観測に加え、攻撃の手法および標的の両面におけるエスカレーションの兆候が水面下で観察され始めた年度として位置付けることができる。

本節では、25年度に観察された手法面の変化と、標的面の変化について整理する。攻撃側の手法におけるAI活用の先行と標的側における重要インフラへの持続的侵食の拡大は、防御側の対応時間の実質的な圧縮として顕在化しつつあ

る。攻撃側の手法進化の速度に対し、防御側の対策実装速度の差が2026年度以降どのように推移するかは、各国の脅威評価および防御態勢の設計において重要な視点となるだろう。

3-a）攻撃者によるエージェントAI利用の兆候

25年度後半期は、国家背景サイバー攻撃におけるAI活用が、仮説的な懸念から具体的な観察事例へと移行した時期であった。

2026年3月、パキスタン系APT36がAI生成マルウェア「Vibeware」を用いてインド政府を標的とする攻撃が報告された。AI生成による国家背景の攻撃マルウェアが実例として確認された初期の事案のひとつである。米国家情報長官室（ODNI）が2026年3月に公表した「2026年次脅威評価」においても、AIを活用した攻撃の高度化が主要な傾向として指摘されている。

イランAPTについては、中東情勢の緊張を背景とした活動の活性化が報告されるとともに、AIを用いたソーシャルエンジニアリングの高度化が観察されている（英国NCSCによる2026年3月の警戒情報等）。

これら個別事例は、攻撃側がAIおよびエージェント的手法の活用を先行させている可能性を示唆している。①で述べた防御側の枠組み整備（NIST AIサイバーセキュリティプロファイル、NCSC AI脅威評価、8カ国共同のAI/MLサプライチェーンセキュリティガイダンス等）は、こうした観察事例に対する防御側の対応整備としても読むことができるが、対策の実装におけるタイムラグは、2026年度以降の対応能力の試金石となるだろう。

[参照ニュース]

2026年3月5日　パキスタン系APT36、AI生成マルウェア「Vibeware」でインド政府を標的

ルーマニアのセキュリティ企業Bitdefenderは、パキスタン系のAPTグループ「APT36」（別名：Transparent Tribe）が、AIを活用して大量のマルウェアを生成し、インド政府機関や在外大使館を標的とする攻撃キャンペーンを展開していると報告した。

APT36は従来の既製マルウェアから方針を転換し、生成AIを用いてNim、Zig、Crystalなどのニッチなプログラミング言語でマルウェアを量産する手法を採用した。Bitdefenderはこれを「Vibeware」と命名している。個々のマルウェアの品質は低いものの、大量に生成して投入することで従来型のウイルス対策ソフトの検知を回避し、防御側のリソースを圧倒する戦術である。さらに、指令通信にはGoogle SheetsやSlack、Discordなど正規のクラウドサービスを利用し、通常の業務通信に紛れ込ませることで検出を困難にしている。

https://www.bitdefender.com/en-us/blog/businessinsights/apt36-nightmare-vibeware

2026年3月2日　英国NCSC、中東紛争の激化を受けイラン関連サイバー脅威への警戒を呼びかけ

英国国家サイバーセキュリティセンター（NCSC）は、中東情勢の緊迫化を受け、英国組織に対しサイバーセキュリティ態勢の点検を求める警告を発出した。2月28日の米国・イスラエルによるイラン攻撃の後、イラン系のサイバー報復リスクが高まっていることが背景にある。

NCSCは、現時点でイランから英国への直接的なサイバー脅威に大きな変化は確認されていないとしつつも、中東地域に拠点やサプライチェーンを有する組織にとっては、間接的なサイバー脅威が「ほぼ確実に高まっている」と評価した。具体的な対策として、外部攻撃面の点検、ネットワーク監視の強化、インシデント対応計画の確認を推奨している。
https://www.ncsc.gov.uk/news/ncsc-advises-uk-organisations-take-action-following-conflict-in-middle-east

2026年3月26日　米国家情報長官室、2026年次脅威評価を公表

米国家情報長官室（ODNI）は3月26日、米情報コミュニティによる「2026年次脅威評価（Annual Threat Assessment）」を公表した。移民、麻薬、テロ、ミサイル、サイバー、AIといった幅広い分野を対象に、米国が直面する主要な安全保障上の脅威を整理。国土防衛を最優先課題と位置づけた。
サイバー領域では、中国とロシアを最も持続的かつ深刻な脅威と評価し、両国が米政府機関だけでなく、民間や重要インフラを標的とした攻撃能力の強化を進めていると指摘。中国は有事の際、特にインド太平洋地域の危機において戦略的優位を確保する目的で重要インフラを破壊・妨害する能力をすでに実証済みであるとしている。ロシアもサイバー作戦のR&Dを継続しており、依然として高度な持続的脅威（APT）と位置づけられた。北朝鮮については、2025年だけで約20億ドル（約3,100億円）相当の暗号資産を窃取し、その資金が核・弾道ミサイル開発に充当されている可能性が高いと分析された。イランも重要インフラを標的とした攻撃を継続しているとされる。
また、AIの急速な進展がサイバー攻撃の高度化・効率化を促し、脅威をさらに拡大させるとして警告。中国は2030年までにAI分野で米国を追い越すことを目標に掲げており、量子コンピュータや宇宙領域の軍事化も含め、技術競争の激化が国際的な安全保障環境を不安定化させると分析した。国家主体に加え、ランサムウェア集団などの非国家主体も深刻な脅威であり続けるとした。これらの勢力は、情報窃取や資金獲得といった利益を背景に、米国の政府ネットワークや重要インフラを継続的に狙っているという。
ODNIは「情報は米国の最も鋭い防衛手段である」と強調し、政権や議会に対して迅速かつ客観的な情報提供を今後も続ける姿勢を示した。
https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2026/4141-2026-annual-threat-assessment
https://industrialcyber.co/reports/odni-report-us-critical-infrastructure-faces-escalating-cyber-risks-from-china-russia-iran-and-north-korea/

3-b）事前配置の規模と範囲の拡大

23年度に中国Volt Typhoonによる米国重要インフラへの侵入事案が焦点化されて以降、国家背景アクターによる「事前配置（pre-positioning）」は、継続的な警戒対象であり続けている。事前配置とは、将来の地政学的危機に備えて攻撃者が予め重要インフラに潜伏・アクセス経路を確保しておく攻撃の準備行動のことを指す。25年度の動向からは、この事前配置の規模および範囲の両面において拡大がみられた。

中国背景の脅威アクターによる活動では、2025年7月に中国背景の3グループがマイクロソフトSharePointの脆弱性を通じて米国エネルギー省、国土安全保障省、厚生省を含む400以上の組織を侵害した事案が報告された。単一の攻撃キャンペーンで400組織以上に及ぶ侵害は、事前配置の規模としても顕著である。2025年9月には、米英豪カナダ四カ国が共同署名する形で、中国政府支援の脅威アクターに対するアドバイザリが公開され、通信インフラへの侵入が指摘

された。2025年12月には英国政府が中国拠点企業2社をサイバー攻撃への関与で制裁し、民間企業が国家支援型活動に関与する構造への対応が見られた。2026年1月、台湾国家安全局は重要インフラに対する中国背景の攻撃が一日平均263万件に達するとの分析を公表している。2026年4月には、米連邦捜査局（FBI）が中国背景の脅威アクターによる米国内の通信傍受システムに対する侵害を「重大インシデント」として認定した（Salt Typhoonの関与が指摘されている）。特に通信傍受システムという、法執行機関がサイバー攻撃捜査の基盤としている機能自体への侵害は、事前配置の対象領域としても従前には見られなかった範囲の拡大を示唆する。

ロシア背景のグループの活動としては、2025年6月に英米政府等が、ロシアによる西側諸国の物流・輸送組織を標的とした諜報活動への警戒情報を発出し、2025年7月には英国NCSCが軍情報機関(GRU)関連グループによるスパイツール「LOSTKEYS」の使用を公式に非難した。2026年1月には親ロシア系ハクティビストによる欧州インフラへのDDoS攻撃リスクへの警戒が英国NCSCから発信されている。

2026年4月には、米連邦捜査局（FBI）、米国サイバーセキュリティ・社会基盤安全保障庁（CISA）、米国家安全保障局（NSA）、米国環境保護庁（EPA）、米国エネルギー省（DOE）、米国サイバー軍サイバーナショナルミッションフォース（CNMF）の6省庁共同による合同勧告が発出され、イラン関連APTによる米重要インフラの産業用制御システム（PLC）への侵害が報告された。イラン関連アクターによる米国OT環境への攻撃自体は2023年のCyberAv3ngersキャンペーン（水道事業者等を標的とした75デバイス規模の侵害）から継続的に観測されてきた現象であるが、今回の合同勧告は、現在進行中のイラン・イスラエル・米国間の地政学的緊張を背景として、PLCへの攻撃が実際の運用停止および財務的損失を伴う被害を生じさせていることを公式に確認する内容となっている。また、6省庁共同での合同勧告という発表形式自体が、当該脅威に対する米国政府の強度を示す要素として指摘できる。

[参照ニュース]

2026年4月1日　FBI、中国系ハッカーによる国内監視システム侵害を「重大インシデント」認定

米連邦捜査局（FBI）は4月1日、同局の未分類の法執行監視システムが中国系ハッカーに侵害された事案を、連邦情報セキュリティ近代化法（FISMA）に基づく「重大インシデント（Major Incident）」に認定し、議会に正式通知した。異常なログ活動として最初に検知されたのは2026年2月17日。

侵害されたのはFBIのデジタル収集システムネットワーク（DCSNet）内のペンレジスタ・トラップ＆トレース監視業務を担うシステム「DCS-3000（通称：Red Hook）」とされる。法的令状に基づく通話・通信の監視に用いられる未分類インフラであり、流出した電話番号や個人情報から米国の諜報監視対象者が特定されるリスクがある。攻撃は商用インターネットサービスプロバイダのインフラを悪用したサプライチェーン型の手法が用いられ、過去に米国の主要通信事業者8社を侵害した「Salt Typhoon」と同様の戦術・技術・手順（TTPs）が確認されたとウォール・ストリート・ジャーナルが報じている。

本件は調査継続中。政府職員の大幅削減が進む中、専門家は連邦政府の攻撃対象領域が拡大していると指摘しており、中国系アクターがこの状況を認識しているとみている。

https://www.nbcnews.com/news/us-news/fbi-labels-suspected-china-hack-law-enforcement-data-major-cyber-incid-rcna266495

https://www.nextgov.com/cybersecurity/2026/04/suspected-chinese-breach-fbi-system-exposed-surveillance-targets-phone-numbers/412612/

2025年8月27日　米国CISA、中国政府支援の脅威アクターに対する共同署名アドバイザリを公開

米国サイバーセキュリティ・社会基盤安全保障庁（CISA）は、諜報活動として世界中のネットワークに侵入する中国政府支援の脅威アクターに関し、世界各国の機関が共同署名したサイバーセキュリティアドバイザリ（CSA）を公開した。今回共同署名し協力機関として組織名を列記した国は、米国の他に、豪州、カナダ、ニュージーランド、英国、チェコ、フィンランド、ドイツ、イタリア、オランダ、ポーランド、スペイン及び日本の13か国で、日本では国家サイバー統括室 (NCO)と警察庁 (NPA)の２組織が記載されている。

中華人民共和国（PRC）の国家支援を受けたサイバー脅威アクターは、通信・政府・交通・宿泊施設・軍事インフラネットワークなど、世界中のネットワークを標的にしており、一般的にSalt Typhoon、OPERATOR PANDA、RedMike、UNC5807、GhostEmperorなどの名称で追跡されている。本CSAには、政府機関および各業界における様々な調査結果が含まれており、企業の内部ネットワークのみならず、顧客向け直接サービスを供するシステムやネットワークへの攻撃を解析している。

https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a

https://www.npa.go.jp/bureau/cyber/pdf/20250827.pdf

2025年12月9日　英国政府、中国拠点企業2社をサイバー攻撃への関与で制裁

英国政府は、世界80カ国以上の政府および民間ITシステムを標的とした無差別なサイバー攻撃に関与したとして、中国に拠点を置く技術企業「i-Soon」および「Integrity Tech」の2社に対する制裁措置を発表した。

発表によると、i-Soonは各国のネットワークへの直接的な攻撃に加え、第三者の悪意ある活動を支援していたとみられる。一方、Integrity Techは秘匿されたサイバーネットワークを運用し、攻撃活動に対する技術的な支援を行った疑いが持たれている。英国政府は、これらの企業が中国国家と連携するサイバー産業の一角を形成しており、その活動は国連の合意するサイバー空間の責任ある行動規範に違反し、国際社会の安定を脅かすものであると非難した。

今回の措置は、同年8月に明らかとなった攻撃グループ「Salt Typhoon」に関連する企業への追及に続くものである。英国は、中国企業による脅威が広範に及んでいる実態が浮き彫りになったとして、責任あるサイバー行動を求める国際的な枠組み作りを主導していく姿勢を改めて示した。

https://www.gov.uk/government/news/uk-clamps-down-on-china-based-companies-for-reckless-and-irresponsible-activity-in-cyberspace

2026年1月4日　台湾国家安全局、重要インフラに対する中国のサイバー脅威分析を公開

台湾国家安全局（NSB）は、2025年に中国が台湾の重要インフラに対して実施したサイバー攻撃を分析した報告書を公開した。

報告書によると、攻撃回数は一日平均263万件、年間で約9億6千万件に達した。これは前年比で6%の増加であり、2023年と比較すると113%の大幅な増加となる。特にエネルギー分野（石油・電力・天然ガス）への攻撃が顕著で、2024年比で約11倍に急増した。これらの攻撃は、産業制御システムのアップデートや機器メンテナンスのタイミングを狙い、脆弱性を悪用する手法が多用されたという。

攻撃の発生時期は台湾総統の演説や中国軍の戦備パトロールと重なっており、軍事圧力や偽情報の流布と組み合わせた「ハイブリッド脅威」として、台湾社会の機能を麻痺させる意図があると分析された。また、中国による技術的自立や米中技術競争での優位性確保を目的とした先端技術の窃取についても、NSBは警戒を強めている。

https://www.nsb.gov.tw/en/#/%E5%85%AC%E5%91%8A%E8%B3%87%E8%A8%8A/%E6%96%B0%E8%81%9E%E7%A8%BF%E6%9A%A8%E6%96%B0%E8%81%9E%E5%8F%83%E8%80%83%E8%B3%87%E6%96%99/2026-01-04/Analysis%20on%20China%E2%80%99s%20Cyber%20Threats%20to%20Taiwan%E2%80%99s%20Critical%20Infrastructure%20in%202025

2025年5月21日　英米政府ら、西側諸国の物流組織等を標的としたロシアの諜報活動への警戒情報

英米両政府らは、同盟国の協力のもとロシアの連邦軍参謀本部情報総局（GRU）によるサイバー諜報活動を摘発したと発表した。特に、GRUの軍事部隊26165（別名APT28）が2022年以降に展開した作戦に関する詳細な技術的分析を公表し、警戒を促している。
この作戦の標的は、ウクライナ支援に関与する西側諸国の物流企業・IT企業・政府機関に及んでおり、輸送調整機関・防衛関連企業・海事／港湾インフラ・航空交通管制機関など多岐にわたる分野が含まれている。また、これらの攻撃は主にNATO加盟国に向けられたものであるとされ、サイバー空間における軍事的・諜報的脅威の高まりが指摘されている。
公開されたレポートでは、今回APT28が用いた手口からスピアフィッシングやウェブメールの侵害などの技術的詳細を公開し、脅威の検出対応と緩和手順の実施を強く求めている。
https://www.ncsc.gov.uk/news/uk-partners-expose-russian-intelligence-campaign
https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a

2025年7月18日　英国NCSC、ロシア軍情報機関によるスパイ活動ツールの使用を非難

英国通信本部（GCHQ）傘下の国家サイバーセキュリティセンター（NCSC）は、ロシア軍参謀本部情報総局（GRU）に属するハッカー集団APT28によるスパイ活動に関連して、高度なマルウェア「AUTHENTIC ANTICS」の使用を確認したと発表した。
同マルウェアは電子メールアカウントを標的とし、感染すると被害者のログイン資格情報および認証トークンを窃取し、攻撃者が長期的に当該アカウントに不正アクセスできる状態となる。これにより、機密情報の流出リスクが高まるとされている。NCSCは、本件が国家主導のサイバー諜報活動の一環であると明言し、国家安全保障上重大な懸念を表明した。これを受け、英国政府はGRUの部隊番号26165、29155、74455に所属する18名の工作員および職員に対して制裁を発動した。
https://www.ncsc.gov.uk/news/uk-call-out-russian-military-intelligence-use-espionage-tool

2026年1月19日　英国NCSC、ロシア系ハクティビストにDDoS攻撃へ警戒呼びかけ

英国国家サイバーセキュリティセンター（NCSC）は、ロシア系ハクティビスト集団によるサイバー攻撃が継続的に英国組織を標的としているとして警告を発表した。攻撃の多くはDDoS（分散型サービス妨害）で、公共機関、地方自治体、交通、医療など市民生活に直結するオンラインサービスの停止や混乱を目的としている。これらの活動はロシア・ウクライナ情勢などの地政学的要因と結びついており、NoName057(16)を含む複数のハクティビスト集団が関与しているとされる。NCSCは、被害の多くが限定的かつ一時的である一方、今後も断続的な攻撃が続く可能性が高いと指摘し、DDoS対策、インシデント対応計画の整備、関係機関との連携強化を呼びかけている。
https://www.ncsc.gov.uk/news/ncsc-issues-warning-over-hacktivist-groups-disrupting-uk-organisations-online-services
https://www.ncsc.gov.uk/news/pro-russia-hacktivist-activity-continues-to-target-uk-organisations

2026年4月7日　CISA/FBI/NSA等、イラン系APTによる米重要インフラへのPLC攻撃に関する合同勧告を発表

米国サイバーセキュリティ・社会基盤安全保障庁（CISA）、連邦捜査局（FBI）、国家安全保障局（NSA）、環境保護庁（EPA）、エネルギー省（DOE）、米サイバー軍サイバー国家任務部隊（CNMF）は、イラン革命防衛隊のサイバー電子司令部（IRGC-CEC）と関連するAPTグループ「CyberAv3ngers」（別称：Shahid Kaveh Group、Storm-0784、UNC5691）による米重要インフラへのサイバー攻撃に関する合同勧告（AA26-097A）を公表した。

同グループは少なくとも2026年3月以降、インターネット接続状態にあるRockwell Automation/Allen-Bradley製プログラマブルロジックコントローラ（PLC）を悪用し、水道・廃水処理、エネルギー、政府施設を含む複数のインフラセクターを標的に攻撃を継続している。具体的な手口としては、海外拠点のIPアドレスを経由してPLCへの不正アクセスを行い、Dropbear SSHを利用した永続的なC2チャネルを確立。PLCプロジェクトファイルを改ざんし、SCADA/HMI画面に虚偽の計測値を表示させながら、実際の制御ロジックを攻撃者が意図した状態に書き換えるという手法が確認された。一部の被害組織では業務停止や財務的損失が生じている。

各機関は、インターネットに接続されたOT/ICSデバイスのネットワーク分離、多要素認証（MFA）の徹底、デフォルト認証情報の変更、未使用ポートの無効化、異常なアクセスのログ監視などを緊急の対策として推奨している。

https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a

https://www.ic3.gov/CSA/2026/260407.pdf

4) 耐量子暗号（PQC）移行をめぐる議論の加速

24年度には、米国・英国・豪州の政府機関による耐量子暗号への移行計画が相次いで発表され、2030年から2035年前後を切り替え時期として見据える具体的な言及が整理された時期であった。25年度は、こうした横断的な移行計画を前提としつつ、セクター別の具体的ガイダンス整備と、民間実装における認識と行動のギャップが可視化された年度として位置付けられる。

4-a) 政府・規制当局の移行指針の具体化

米国国立標準技術研究所（NIST）が確定させた耐量子暗号標準（FIPS 203、204、205）の公表以降、各国・機関はこれら標準の具体的な適用領域を対象とするガイダンスの整備を進めている。

2026年2月には、欧州刑事警察機構（ユーロポール）が金融機関向けの耐量子暗号移行における優先順位付けフレームワークを公表した。中央銀行および決済インフラを最優先とする位置付けを含み、金融セクターにおける移行ロードマップの国際的な参照点となることを意図したものである。金融インフラは決済システムや長期保存が必要な取引記録を扱う性質上、移行の遅延が「収集後解読（harvest now, decrypt later）」型のリスクに直結する領域として位置付けられてきたが、セクター固有のガイダンスとして具体化された点に意味がある。

2026年3月には、米国家安全保障局（NSA）、豪州信号局（ASD）等による低軌道衛星通信のサイバーリスクに関する国際共同ガイダンスが公表された。衛星通信領域における耐量子暗号対応要件が国際的に明示化されたものであり、宇宙システムのサイバーセキュリティ基準整備の一環として位置付けることができる。

2026年4月には、NISTが暗号鍵確立推奨事項（SP 800-56）への耐量子暗号対応の改訂方針を発表した。鍵交換プロトコル全体の耐量子暗号化に向けた具体的なロードマップが示されたものであり、既存の鍵確立標準を基盤として運用されている多くのシステムの移行設計に直接的な影響を及ぼす。

なお、米国EO 14144は2030年までの耐量子暗号への移行を規定しており、第二期トランプ政権下でも撤回されていない点は、米国の耐量子暗号政策の基本路線が政権交代を挟んでも維持されている構図として確認できる。

[参照ニュース]

2026年1月21日　ユーロポール、金融機関向けにポスト量子暗号移行の優先順位付けフレームワークを発表

欧州警察機構（Europol）は、FS-ISACらと共同で、ポスト量子暗号（PQC）への移行計画を策定するための実務的なフレームワークを発表した。将来の量子コンピュータによる暗号解読リスクへの対策として、金融サービス分野がポスト量子暗号（PQC）への移行を計画的に進めるための実用的な優先順位付け手法を提示している。

本フレームワークでは、データの機密性、公開範囲、潜在的な影響などに基づく「量子リスク」と、実装に必要な時間・コスト・外部依存性などを評価する「移行時間」の2軸で優先度を決定する枠組みを示している。早期に実施可能な「ノーリグレット（後悔のない）」対策として、ハイブリッド暗号の導入や旧式暗号の排除、公開Webサービス保護の強化などが例示されている。同報告は、複数企業・団体の協力で作成され、金融エコシステム全体で意思決定や統一的な対応を促すことを目的としている。

https://www.europol.europa.eu/media-press/newsroom/news/joint-report-outlines-practical-approach-to-prioritising-post-quantum-cryptography-migration-in-financial-services

https://www.europol.europa.eu/cms/sites/default/files/documents/Post-quantum-cryptography-report.pdf

2026年3月24日　米NSA・豪ASD等、低軌道衛星通信のサイバーリスクに関する国際共同ガイダンスを発表

米国家安全保障局（NSA）と豪州信号局（ASD）のサイバーセキュリティセンター（ACSC）は3月24日、低軌道衛星通信（LEO SATCOM）システムのサイバーリスクと緩和策に関する共同サイバーセキュリティ情報シート（CSI）「Securing space: Cyber security for low earth orbit satellite communications」を公開した。カナダサイバーセキュリティセンター（CCCS）、豪州宇宙庁、ニュージーランド国家サイバーセキュリティセンター（NCSC-NZ）も共同作成に参加している。

ガイダンスはLEO SATCOMシステムを（1）衛星自体で構成される宇宙セグメント、（2）管制センター・地上局・ゲートウェイ・ユーザー端末を含む地上セグメント、（3）エンドユーザー機器・アプリケーションで構成されるユーザーセグメント、（4）通信リンク・サプライチェーンの4セグメントに分類し、それぞれの脅威と緩和策を体系的に整理している。宇宙資産への物理アクセス制限という固有の制約に加え、無線周波数リンクのジャミング・スプーフィング・傍受リスクが詳述されている。

https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4443075/nsa-and-asds-acsc-release-joint-guidance-on-leo-satcom-system-risks-and-mitigat/

https://media.defense.gov/2026/Mar/24/2003902673/-1/-1/0/SECURING%20SPACE%20CYBER%20SECURITY%20FOR%20LOW%20EARTH%20ORBIT%20SATELLITE%20COMMUNICATIONS.PDF

2026年4月17日　米国NIST、暗号鍵確立推奨事項（SP 800-56）にPQC対応の改訂方針

米国国立標準技術研究所（NIST）は、暗号鍵確立に関する推奨事項の特別刊行物（SP：Special Publication）800-56シリーズの改訂方針を発表した。2025年7月に実施したパブリックコメントの結果を踏まえ、3文書について対応方針を決定した。

SP 800-56Ar3は更新版の位置づけとし、楕円曲線暗号（ECC）におけるx座標のみの実装を承認するとともにSP 800-186との曲線要件の整合性を確保する。SP 800-56Br2は現時点では変更なしとし、他文書の更新後に参照情報を更新する予定とする。SP 800-56Cr2は改訂（Revision）とし、耐量子暗号（PQC）時代を見据えた鍵カプセル化メカニズム（KEM：Key Encapsulation Mechanism）

から得られた共有秘密の組み込みを新たに許可する。ハイブリッド鍵共有秘密のフォーマット柔軟性も向上させるほか、KMACをランダム性抽出ステップでも承認する。企業のPQC移行計画において、鍵確立プロセスの見直しが必要となる可能性がある。
https://csrc.nist.gov/News/2026/nist-to-revise-key-establishment-recommendations

4-b) 民間実装の現状と加速要因

政府・規制当局による移行指針の具体化が進む一方、民間企業における耐量子暗号実装の現状には大きな課題が残っている。2025年5月時点の調査では、量子安全暗号を実際に導入済みの企業はわずか5%に過ぎず、調査対象の69%が量子脅威を認識しているにもかかわらず「認識はしているが行動していない」という状態にあるとの結果が報告された。認識と行動の間のギャップは、耐量子暗号移行における主要な実務的課題として25年度を通じて論点化された。

このギャップの背景には、移行プロセスの複雑性があり、24年度に英国NCSCのガイダンスが指摘した通り、組織内部のアセスメントから着手する現実的なアプローチが求められる状況は継続している。NISTの試算では、大規模企業が2026年に移行を開始した場合でも完全移行は2030年代初頭まで要するとされており、移行の開始時期そのものが、将来の規制対応や取引先からの要求への応答可能性を左右する要素となりつつある。

25年度後半期には、学術研究の領域でも耐量子暗号移行の時間軸に影響を与え得る動きが見られた。2026年3月に報じられた複数の研究成果によれば、RSA暗号の解読に必要な論理量子ビット数が、従来想定されていた2,000万規模から100万以下へと引き下げられる可能性が示唆されている。量子コンピューティングの実用化時期そのものが前倒しされたわけではないが、必要とされる計算リソースの見積もりに影響する研究動向として観察に値する。

一部の大手テック企業においては、耐量子暗号の段階的な実装が先行的に進められている。これらの先行実装は、サプライチェーンにおける取引先への耐量子暗号対応の要求に結びつく可能性があり、民間企業の移行加速の実務的要因として今後影響を及ぼしていくことが想定される。

[参照ニュース]

2026年3月31日　NIST、鍵確立推奨規格の見直しを決定――学術界でもQ-Day前倒しを示唆する論文

米国立標準技術研究所（NIST）は3月、ポスト量子暗号（PQC）移行を見据え、鍵確立推奨規格SP 800-56シリーズ3本の見直しを決定した。SP 800-56Ar3（離散対数暗号を用いるペアワイズ鍵確立）は楕円曲線暗号（ECC）のx座標のみ実装を承認しSP 800-186との整合性を確保、SP 800-56Cr2（鍵導出方法）は承認済みの鍵カプセル化メカニズム（KEM）からの共有秘密の組み込みと二段階鍵導出でのKMAC（Keccakメッセージ認証コード）承認を追加する。いずれも暗号アジリティ強化を念頭に置いた対応で、NISTは2030年以降に量子脆弱アルゴリズムを非推奨化する方針をすでに示している。

こうした標準化の動きと並行して、学術・研究機関からもQ-Dayタイムラインの前倒しを示唆する論文が3本相次いで発表されている。Google Quantum AI（2025年5月）はRSA-2048解読に必要なqubit数を100万未満に、シドニーのIceberg Quantum（2026年2月）はさらに10万未満に圧縮。さらにGoogle Quantum AI（2026年3月）は楕円曲線暗号（256ビットECDLP）を50万qubit未満かつ数分以内に解読可能と示した。2019年時点の推定約2,000万qubitから10年余りで100分の1以下に圧縮されたことになる。3本目の論文は安全上の懸念から攻撃回路を非公開とし、正当性のゼロ知識証明のみを公開するという前例のない対応を取った。現時点では量子コンピュータは数千～数万qubit規模にとどまり、即座の脅威ではないとされる。しかし各論文が示す進歩は量子誤り訂正・qubit

密度・演算効率化といった独立した技術領域で同時に生じており、専門家は「残る障壁はエンジニアリング上の問題のみ」と警戒感を強めている。

https://csrc.nist.gov/News/2026/nist-to-revise-key-establishment-recommendations

https://thequantuminsider.com/2026/03/31/q-day-just-got-closer-three-papers-in-three-months-are-rewriting-the-quantum-threat-timeline/

以上