

情報セキュリティ白書

Information Security White Paper

2026

サイバー防御新時代：諸刃の進化に備えよ



独立行政法人
情報処理推進機構
Innovation Platform Agency, Japan

Beyond Digital

「情報セキュリティ白書2026」の刊行にあたって

デジタルトランスフォーメーション(DX)やAIの活用が急速に広がり、サイバー空間とフィジカル空間の融合は新たな段階を迎えています。デジタル技術は、人々の暮らしや企業活動、社会基盤の在り方を大きく変え、新たな価値や成長の機会を生み出しています。更に、量子コンピューティングを始めとする先端技術の発展は、イノベーションの可能性を一層広げつつあります。

一方で、デジタル社会の発展に伴い、サイバー空間を取り巻くリスクも複雑化・深刻化しています。ランサムウェアによる被害は依然として高水準にあり、サプライチェーンや委託先を狙った攻撃、システムの脆弱性を悪用した攻撃はますます高度化・巧妙化しています。また、AIの利活用の拡大に伴う新たなサイバーリスクも顕在化しています。加えて、社会や産業のデジタル化が進む中で攻撃対象領域は拡大し、ひとたび重大なインシデントが発生した場合には、その影響が広範囲に波及する可能性も高まっています。

更に、先端技術の実用化は大きな可能性をもたらす反面、既存の暗号や認証による安全性の前提を揺るがし、セキュリティの在り方そのものに変革を迫っています。技術の進化による恩恵を最大限に生かしながら、安全・安心をいかに確保していくかが、これまで以上に重要な課題となっています。

私達が目指すのは、脅威の存在を前提としながらも、人々や組織が安心して挑戦を続けられる社会です。攻撃を受けても止まらず、回復し、更にレジリエンスを社会全体で高めていくことが、挑戦と成長を支えるセキュリティの本質です。サイバー空間は持続的な経済社会の発展を支える不可欠な基盤であり、その安全・安心はもはや個々の組織だけで守れるものではありません。社会全体で支えるべき公共的な基盤として、セキュリティをとらえることが求められています。

こうした社会的要請の高まりを受け、政府はサイバーセキュリティを危機管理と成長戦略の両面を支える重要な投資分野として位置付け、産学官が連携して人材・技術・制度の強化を進めています。IPAもまた、技術・人材・制度・信頼を結び付けるハブとして、デジタル化の進展とセキュリティ確保の両立を図り、攻撃や障害に直面しても止まらず、回復する、更なるレジリエントな社会の実現に向けて、その役割を果たしてまいります。

「情報セキュリティ白書」は、2008年以来、サイバーセキュリティを巡る政策や脅威動向、被害の実態等を取りまとめ、多くの皆様に活用いただいております。本白書が、2025年度の情勢への理解を深め、それぞれの立場で取り組まれる対策や実践の一助となり、より安全で信頼されるデジタル社会の実現につながることを心より願っております。

2026年9月

独立行政法人情報処理推進機構(IPA)

理事長

齋藤 裕

序章 2025年度の情報セキュリティの概況	6
第1章 国内外のサイバー脅威の動向	8
1.1 2025年度に観測されたインシデント状況	8
1.1.1 世界におけるサイバーセキュリティインシデント状況	8
1.1.2 国内におけるサイバーセキュリティインシデント状況	14
1.2 インシデント事例や脆弱性・攻撃の動向と対策	19
1.2.1 ランサム攻撃	19
1.2.2 標的型攻撃	27
1.2.3 DDoS攻撃	34
1.2.4 情報システムの脆弱性を悪用した攻撃	37
1.2.5 不正アクセスや内部不正による情報漏えい	42
1.2.6 個人を狙う騙しの手口	46
1.2.7 企業・組織を狙う騙しの手口	51
第2章 サイバー空間を巡る動向	62
2.1 サイバー安全保障関連施策の状況	62
2.1.1 能動的サイバー防御の実現に向けた取り組み	62
2.1.2 経済安全保障関連施策の状況	66
2.2 AIの安全性確保の取り組み	69
2.2.1 AIの発展と社会への普及	69
2.2.2 AIのリスク	70
2.2.3 AIの安全性とガバナンス	76
2.2.4 AIのセキュリティ	79
2.3 偽・誤情報対策の動向	88
2.3.1 偽・誤情報の定義	88
2.3.2 偽・誤情報の最新情勢	89
2.3.3 2025年度の注目事例	91
2.3.4 偽・誤情報への対策の動向	93
2.3.5 状況のまとめと今後の見通し	95

第3章 国内の政策及び取り組みの動向 106

3.1 国内のサイバーセキュリティ政策の状況 106

3.1.1 政府の政策動向 106

3.1.2 経済産業省の政策 114

3.2 サイバーセキュリティ人材の現状と育成 122

3.2.1 サイバーセキュリティ人材を取り巻く現状と課題 122

3.2.2 サイバーセキュリティ人材育成のための国家試験、国家資格制度 125

3.2.3 セキュリティ人材育成のための活動 126

3.3 製品・サービスの評価・認証制度、及び暗号技術の動向 133

3.3.1 セキュリティ要件適合評価及びラベリング制度(JC-STAR) 133

3.3.2 ITセキュリティ評価及び認証制度(JISEC) 138

3.3.3 政府情報システムのためのセキュリティ評価制度(ISMAP) 139

3.3.4 暗号技術の動向 141

3.4 中小企業のサイバーセキュリティ対策強化の取り組み 145

3.4.1 サプライチェーン強化に向けたセキュリティ対策評価制度(SCS評価制度) 145

3.4.2 中小企業のサイバーセキュリティ対策の課題とそれらに対する施策 147

3.4.3 中小企業向け支援策 151

第4章 国際的な政策及び取り組みの動向 160

4.1 国際的なサイバーセキュリティ政策の状況 160

4.1.1 国際社会と連携した日本の取り組み 160

4.1.2 米国の政策 165

4.1.3 欧州の政策 172

4.1.4 中国の政策 180

4.1.5 アジア太平洋地域でのCSIRTの動向 183

4.2 国際標準化活動 188

4.2.1 様々な標準化団体の活動 188

4.2.2 情報セキュリティ、サイバーセキュリティ、プライバシー保護関係の規格の標準化 (ISO/IEC JTC 1/SC 27) 189

付録・索引	199
第21回IPA「ひろげよう情報セキュリティコンクール」2025受賞作品	200
索引	201

コラム

ランサムウェア被害から学ぶ、経営者に求められる実践的な対処・対応とは？	18
IoT機器は輸入禁止になるくらい危険なのでしょうか？	54
AI時代のデジタル・シティズンシップと責任	87
「AIの利用をめぐるサイバーリスク」が「情報セキュリティ10大脅威」に初登場	97
データを守ることは、事業を守り強化すること	131
サプライチェーンのセキュリティ管理のための五つのポイント	154
セキュリティを「脅威」ではなく「我々」を主語に語り直す	193



情報セキュリティ白書

●序章 2025年度の情報セキュリティの概況

●第1章 国内外のサイバー脅威の動向

- 1.1 2025年度に観測されたインシデント状況
- 1.2 インシデント事例や脆弱性・攻撃の動向と対策

●第2章 サイバー空間を巡る動向

- 2.1 サイバー安全保障関連施策の状況
- 2.2 AIの安全性確保の取り組み
- 2.3 偽・誤情報対策の動向

●第3章 国内の政策及び取り組みの動向

- 3.1 国内のサイバーセキュリティ政策の状況
- 3.2 サイバーセキュリティ人材の現状と育成
- 3.3 製品・サービスの評価・認証制度、及び暗号技術の動向
- 3.4 中小企業のサイバーセキュリティ対策強化の取り組み

●第4章 国際的な政策及び取り組みの動向

- 4.1 国際的なサイバーセキュリティ政策の状況
- 4.2 国際標準化活動

序章

2025年度の情報セキュリティの概況

2025年度の情報セキュリティを巡る状況は、生成AIや量子コンピューター関連技術の進展、社会全体のデジタル化の加速を背景として、大きな変化の中にあった。これらの技術は、業務の高度化や効率化、新たな価値の創出をもたらす一方で、攻撃の巧妙化・効率化、偽情報の拡散、将来的な暗号基盤への懸念等、新たなリスクも生み出している。技術の進化がもたらす恩恵と脅威の双方を見据え、情報セキュリティを経営、事業継続、社会基盤、安全保障にまたがる課題としてとらえる必要性は、これまで以上に高まった。

国内外ではランサム攻撃、不正アクセス、DDoS攻撃等が継続して発生し、機密性、完全性、可用性のいずれに対しても深刻な影響を及ぼした。

2025年5月には、外食事業者のテイクアウトサイトに対する不正アクセスにより、クレジットカード情報等2,270件が漏えいした可能性があることが公表された。同年6月には研究開発支援事業者、同年7月にはホスティング事業者に対するDDoS攻撃が確認され、サービス提供の継続そのものを脅かす事案が続いた。2026年1月には農林水産省でのメール誤送信、同年2月には総務省が実施したアンケート調査における委託先の設定ミスにより個人情報漏えいが発生しており、従来型の漏えい事案も引き続き発生している。

2025年度は、企業活動の中核を担う基幹システムが攻撃を受けた場合の影響の大きさも改めて浮き彫りとなった。2025年8月には海外自動車メーカーが認証情報の悪用をきっかけにランサム攻撃を受け、生産、販売、物流に影響が及び、長期間の操業停止を招いた。国内では、同年9月に大手飲料メーカーがランサム攻撃を受け、約2ヵ月間のシステム停止が発生した。同年10月には大手eコマース企業に対するランサム攻撃により、約74万件の情報漏えいが発生した。こうした事案は、業務のデジタル化が進展する中で、一部のシステムの停止による影響が、受発注、物流、顧客対応等サプライチェーンの広範囲に及び得ることを示している。

国際的には、国家を背景とするサイバー攻撃が引き続き警戒された。2025年8月にはAPT攻撃グループ「Salt Typhoon」によるサイバー攻撃に関する国際アドバイザリーが共同署名の形で公表された。サイバー攻撃は、

機密情報の窃取にとどまらず、通信基盤や重要サービスへの影響を通じて、国家安全保障や経済安全保障にも関わる問題となっている。こうした情勢のもと、国際的な連携と情報共有の重要性は一層高まっている。

新技術を巡っては、AIの利活用拡大に伴う課題も顕在化した。2025年5月には、米国の新聞でAIのハルシネーションによる存在しない書籍の書評の掲載が発生した。AIは生産性向上や高度な分析を可能にする一方で、誤情報の生成・拡散による社会的信頼の毀損といったリスクも抱えている。サイバーセキュリティ上の課題は、システムやデータの保護にとどまらず、人の認知活動や社会的信頼の維持にも及ぶものとなっている。

こうした状況を受け、国内では防御側の体制整備も進展した。2025年5月には、サイバー対処能力強化法及び同整備法が公布された。同年7月には国家サイバー統括室(NCO)が発足し、サイバーセキュリティ戦略本部が改組された。更に12月には「サイバーセキュリティ戦略」が閣議決定され、平時からの探知、分析、対処を重視する方向へ、我が国の体制整備は一段と進んだ。2026年3月には、経済産業省が「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針」(SCS評価制度の構築方針)を公表した。SCS評価制度が活用されることにより、サプライチェーン全体でのサイバーセキュリティ対策が強化されることが期待される。

制度面では、新技術への対応も着実に進められた。2025年7月には欧州で「General-Purpose AI Code of Practice (汎用AIの行動規範)」が、米国では「America's AI Action Plan」が公表された。日本でも同年6月に「人工知能関連技術の研究開発及び活用の推進に関する法律」(AI法)が公布・一部施行され、同年9月には全面施行された。同年12月には同法に基づき、「人工知能基本計画」が閣議決定され、政府の具体的な方針が示された。また、同年10月にはIoTラベリング制度の推進を図る国際的な枠組みとして「グローバル・サイバーセキュリティ・ラベリング・イニシアティブ(GCLI)」が発足した。同年11月には内閣官房が「政府機関等における耐量子計算機暗号(PQC)への移行について(中間とりまとめ)」を公表し、2035年を目途にPQCへの移行を行うことが示された。

2025年度の主なインシデント・事件・政策・イベント

序章

2025年度の情報セキュリティの概況

	● 主な情報セキュリティインシデント・事件	□ 主な情報セキュリティ政策・イベント
2025年 4月	● 証券会社をかたるフィッシングメールにより甚大な被害が発生(1.1.2)	● 「情報流通プラットフォーム対処法」の施行(2.3.4) ● IPA「企業組織向けサイバーセキュリティ相談窓口」開設(1.2.7、3.1.2)
5月	● 外食事業者のテイクアウトサイトへの不正アクセスにより、クレジットカード情報等 2,270 件の漏えいが発生した可能性(1.2.5) ● 米国の新聞において、AI のハルシネーションによる存在しない書籍の書評の掲載が発生(2.2.2)	● 重要電子計算機に対する不正な行為による被害の防止に関する法律（サイバー対処能力強化法）、及び重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（サイバー対処能力強化法整備法）の公布(2.1.1)
6月	● 研究開発支援事業者への DDoS 攻撃を確認(1.2.3)	● 第 10 回日米サイバー対話の開催(4.1.1)
7月	● ホスティング事業者が DDoS 攻撃を確認(1.2.3)	● 国家サイバー統括室（NCO）の発足と、サイバーセキュリティ戦略本部の改組(2.1.1、3.1.1) ● 欧州「General-Purpose AI Code of Practice（汎用 AI の行動規範）」を公表(2.2.3) ● 米国「America's AI Action Plan」を公表(2.2.3)
8月	● 英国自動車メーカーへの認証情報悪用による不正アクセスとランサム攻撃により、生産活動、販売、物流業務への影響及び長期間の操業停止が発生(1.2.2)	● 「Salt Typhoon」によるサイバー攻撃に関する国際アドバイザリーの共同署名を行い、パブリック・アトリビューションとして、本件アドバイザリーを公表(1.2.2、4.1.1)
9月	● 大手総合飲料メーカーへのランサム攻撃により、約 2 ヶ月間のシステム停止が発生(1.2.1)	● 「人工知能関連技術の研究開発及び活用の推進に関する法律」（AI 法）の全面施行(2.2.3)
10月	● 大手 e コマース企業へのランサム攻撃により、約 74 万件の情報漏えいが発生(1.2.1)	● 「グローバル・サイバーセキュリティ・ラベリング・イニシアティブ(GCLI)」の発足(3.3.1)
11月	● 国立国会図書館のシステム更新で委託先が管理する開発環境への不正アクセスを確認(1.2.5)	● 内閣官房「政府機関等における耐量子計算機暗号（PQC）への移行について（中間とりまとめ）」を公表(3.3.4)
12月		● 「人工知能基本計画」の閣議決定(2.2.3) ● 「サイバーセキュリティ戦略」の閣議決定(3.1.1)
2026年 1月	● 農林水産省でのメール誤送信により、マイナンバー等を含む個人情報漏えいが発生(1.2.5)	● 経済産業省「経済安全保障経営ガイドライン」を公表(2.1.2)
2月	● 総務省が実施したアンケート調査での委託先の設定ミスにより、回答者の個人情報漏えいが発生(1.2.5)	● 「International AI Safety Report 2026」の公開(4.1.1)
3月		● 「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針」の公表(3.1.2、3.4.1)

※表には、2025 年度の主な情報セキュリティインシデント・事件、及び主な情報セキュリティ政策・イベントを示している。表中の数字は本白書中に掲載している項目番号である。他のインシデント・事件や、政策・イベント等については本文を参照いただきたい。

第4章

国際的な政策及び取り組みの動向

2025年度は地政学リスクの高まりを背景に、日米韓による共同対処の取り組みや、国際協調による対応が強化された。また、米国の戦略転換、欧州でのデジタルオムニバス規則案の提案等の包括的法整備、中国での

サイバーセキュリティ法改正等、海外におけるサイバー関連政策も大きく変化した。本章では、こうした国際情勢や国際連携の取り組み、サイバーセキュリティに関する各国の政策動向、及び国際標準化活動を解説する。

4.1 国際的なサイバーセキュリティ政策の状況

サイバー攻撃は国境を問わず、あらゆる国・地域の脆弱なシステムに対して仕掛けられる。また、社会・経済活動に不可欠となった IT サービスや、IT に支えられたサプライチェーンは国境を越えてつながり合い、他国におけるサイバー脅威が自国に深刻な影響を与える可能性がある。更に近年、国家の支援を受けた攻撃者による他国へのサイバー攻撃や AI を悪用した攻撃等の脅威が現実になっている。こうした状況に国や地域が単独で対処することは難しく、国際連携が不可欠である。本節では、国際連携に向けた我が国の取り組みと、各国・各地域における情報セキュリティ政策について述べる。

4.1.1 国際社会と連携した日本の取り組み

2025年度を中心に国際社会の概況、国際的な脅威への対応、及び我が国と各国の首脳・外相等の連携協議について日本の取り組みを中心に述べる。また、国際的なサイバーセキュリティ連携の基盤となる安全保障に関する協議・連携状況にも言及する。

(1) サイバー空間における国際情勢の概況

2025年度は、長期化する紛争や新たな紛争が重なり、国際秩序が大きく変動した年となった。具体的な新たな紛争としては、2025年4月にカシミール地方で発生した観光客襲撃テロを契機としたインドとパキスタンとの軍事衝突^{*1}や、同年5月に激化したタイとカンボジアの国境未画定地帯の領有権争いを背景とした国境衝突^{*2}、2026年2月に開始されたイスラエル・米国とイラン間の軍事衝突^{*3}が挙げられる。それらは物理的な軍事衝突だけでなく、いずれも激しいサイバー攻撃を伴った。

同時に2025年度のサイバー空間では、「AIによる攻撃の自動化」や「地政学リスクと直結した重要インフラへの攻撃」等、従前より懸念されていた脅威が顕在化した年であった。また、ハイブリッド戦、サプライチェーン攻撃、ディープフェイク詐欺も勢いを増している。ここではまずそれらに関連し2025年度に発生した新たな事象を二つ挙げ、その影響を整理する。

一つ目に挙げるのは、相次いで発見された「AI駆動型マルウェア」である。2025年8月、ローカル環境で実行可能な生成 AI を悪用して、リアルタイムで悪意あるスクリプトを生成して攻撃する、新たなタイプのランサムウェア「PromptLock」が発見され、大きな注目を浴びた^{*4}。このランサムウェアは、後に研究者による概念実証のためのプログラムであることが報じられた^{*5}が、今後、類似した機能を持つマルウェアが登場することが懸念される。また、情報窃取活動を目的とした「LAMEHUG」と呼ばれるマルウェアも発見された。これはウクライナの国防・安全保障分野の組織や人物を標的型メールで狙うもので、同国の CERT (Computer Emergency Response Team) である CERT-UA が2025年7月に報告している。AI駆動型マルウェアは、通常のマルウェアが行う動作のいくつかを自身のプログラム内に保有せず、プロンプトを生成 AI に送信することで、データの収集、データの窃取、データの暗号化等を実行するため、セキュリティソフトによる悪意あるコードの静的な検知を逃れることが懸念されている^{*6}。

二つ目に挙げるのは、国家を背景に持つ「IT労働者の潜入」問題で、具体的には北朝鮮の IT 労働者が身分を偽り、欧米や日本の IT 企業にリモートワーカーとして潜り込んでいた実態が次々と判明したことである^{*7}。

生成 AI が求人応募や面接のあらゆる段階で魅力的な候補者をかたるために使用されており、面接中にリアルタイムのディープフェイク映像を使用していた事例も確認されているという^{*8}。このことは、開発中のソフトウェアにバックドアを仕掛けられるリスクを浮き彫りにし、企業の採用プロセスやサプライチェーンの信頼性が根本から問われ、2025 年 8 月、日米韓が共同声明を発表し、偽装工作への注意を喚起する事態に発展した^{*9}。

一方、従前から継続している国家の関与が疑われる攻撃も複数見られた。2021 年ごろから活動を開始している中国の国家支援型攻撃グループとされる Volt Typhoon は、米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA: Cybersecurity and Infrastructure Security Agency）等によると、Living Off The Land (LOTL: 環境寄生型) 戦術によって、サプライチェーンの脆弱性から侵入し、米国の重要インフラへ長期間潜伏し、有事の際の破壊工作を狙っているとされ^{*10}、Volt Typhoon による同国組織への侵入行為を 2025 年 1 月までに 100 件以上発見していると報じられた^{*11}。同じく中国の国家支援型攻撃グループとされる Salt Typhoon に関しては、2025 年 8 月に米国から Salt Typhoon の攻撃手法に関する技術的な説明や攻撃に対する緩和策が記された国際アドバイザリーが公表された^{*12}。同アドバイザリーによって、Salt Typhoon は 2021 年から活動していること、米国、オーストラリア、英国等を始めとする世界各地で活動していることが示された。また、ロシアからウクライナ支援国を標的としたサイバー攻撃も引き続き確認され、英国外務省は 2025 年 7 月、欧州各国の政府機関やエネルギーインフラを標的としたサイバー攻撃に関与したとして、ロシア軍参謀本部情報総局（GRU: Glavnoye Razvedyvatelnoye Upravleniye）の 3 部隊と職員 18 人を制裁対象に指定した^{*13}。

そして、サイバー空間における 2026 年に入ってからの特筆すべき動きとして Anthropic PBC が開発した最先端の AI モデル Claude Mythos が挙げられる。2026 年 4 月にプレビュー版が発表された同モデルはソフトウェアの脆弱性を自律的に発見・攻撃コードを構築する能力が極めて高いといわれており、提供先の選定には米国政府が介入する事態となっている^{*14}。

(2) 国際的な脅威に対する対応

前述の国際社会やサイバー空間における様々な環境変化のもとで生じている脅威に対して、国際的に実施さ

れている具体的な取り組みを 3 件紹介する。

(a) 国連サイバー犯罪条約の採択と署名

これまでサイバー犯罪に関する唯一の多国間条約は、2001 年に採択された「ブダベスト条約」だった^{*15}。

しかし、この条約は欧米を中心とした有志国によるもので、中国やロシアといった主要国が参加していないこと、また近年の AI の悪用や高度なサイバー戦に対応しきれていないことが課題となり、同条約による既存の枠組みに限界がきていた。

2019 年、ロシアが提案した「新たな包括的な国際条約」の策定に関する決議が国際連合（United Nations 以下、国連）で採択されたことを機に、全加盟国を巻き込んだ交渉が始まったが、交渉の過程で「人権・表現の自由」と「主権と監視」の 2 点で対立軸が生じた。

しかし、2024 年中盤の最終会合で、犯罪対象を「ランサムウェア、児童ポルノ、不正アクセス」等の重大犯罪に絞り込み、人権保護の文言を盛り込むことで妥協が成立した。2024 年 8 月に全会一致で採択され、2025 年 10 月にベトナム・ハノイで開催された閣僚級会合にて、「国連サイバー犯罪防止条約（UNCC: United Nations Convention against Cybercrime）」^{*16}の正式な署名式典が行われた。

2026 年 4 月現在、国連加盟 193 ヶ国のうち、英国、フランス等の欧州連合（EU: European Union）加盟国、並びにブラジル、ベトナムを含む 70 ヶ国以上が署名を済ませているだけでなく、交渉を主導した経緯からロシアや中国も署名している。その一方、日本、米国は署名していない。現状、一部の国が未署名ではあるものの、この条約が発効されると、以下のような具体的な効果が見込まれる。

- 証拠収集の迅速化：サーバーが海外にある場合でも、条約に基づく統一された手続きで電子証拠の保全・提供を要請できるようになる。
- 途上国の捜査能力向上：条約には技術支援の規定が含まれており、サイバー犯罪の「抜け穴（セーフヘイブン）」となっていた国々の法整備と、警察官のトレーニングが急速に進む。
- 国際協力の定着：2025 年末に実施された多国間共同捜査により、アジアとアフリカにまたがる特殊詐欺グループが摘発されたが、同条約が発効されると、この事例のような締約国による相互の法的援助や共同調査といった国際協力・支援が更に促進されることが見込まれる。

同条約では、「サイバー犯罪」と「政治的表現」の境界線については、依然として各国の国内法に委ねられている部分があるため、現在、同条約の運用状況を監視する「モニタリング・メカニズム」の構築について、更なる議論が続けられている。

(b) 対ランサムウェア・イニシアチブ(CRI)の強化と共同演習

ランサムウェア攻撃は、単なる金銭奪取にとどまらず、病院、送電網、物流ネットワークといった重要インフラを停止させ、国家の安全保障を直接脅かす存在となっている。これに対し、米国 Joe Biden 政権(当時)が提唱し、2021 年に発足したのが対ランサムウェア・イニシアチブ(CRI: Counter Ransomware Initiative)^{*17}である。

その後、攻撃側が AI を駆使して「攻撃の自動化・高速化」を進めたことで、防御側もより即応性の高い国際協力が不可欠となった。

2025 年 10 月、シンガポールで開催された第 5 回 CRI サミット^{*18}では、国際協力を強化し、ランサムウェアの脅威に対する集団的なレジリエンスを高めることを目的とした議論が行われた。また概要文書では、ランサムウェア攻撃を受けた CRI メンバーの支援を行うことや攻撃者とその協力者を追及し活動できる安全な場所を作らせないこと、攻撃実行者がランサムウェアのビジネスモデルを支える各種アクターを活用できないように対抗すること等の共同のコミットメントについて再確認した^{*19}。

現在、日本を含む米国、英国、カナダ、オーストラリア、シンガポール、EU 諸国、インド、韓国等、50 カ国以上と多数の国際機関、更には Microsoft Corporation や Palo Alto Networks, Inc. 等の IT 企業が参画しており、この「官民連携」の広がり方が CRI の最大の特徴といえる。

同サミットでは、ランサムウェア攻撃に対するサプライチェーンのセキュリティ体制を改善することを支援する「ランサムウェアに対するサプライチェーンレジリエンス構築のための組織ガイダンス^{*20}」をシンガポールと英国が主導して策定した。

(c) 「International AI Safety Report 2026」の公開

AI の急速な発展に対し、当初は「人類を滅ぼす」といった過度な懸念や、逆に「まったく問題ない」とする楽観論が混在していた。

こうした状況を受け、各国の政府や研究者が合意できる「科学的かつ客観的なリスク評価の共通基盤」が必要であるとの認識が広まり、2023 年 11 月の「AI セーフ

ティサミット(AI Safety Summit)」で、Yoshua Bengio 教授を委員長とする報告書の作成が決定され、2025 年 1 月に「International AI Safety Report 2025^{*21}」として公開された。

2026 年 2 月には、第 2 版として「International AI Safety Report 2026^{*22}」が公開された。同報告書は、30 カ国以上の国と、EU、OECD (Organisation for Economic Co-operation and Development: 経済協力開発機構)、国連等の国際機関から指名された代表者を含む、100 名以上の専門家の助言を得て作成されたものである。同報告書は、AI システムの機能とリスクに関する既知の情報を可能な限り具体的にまとめ、同時に未解明な点を明らかにすることで、科学的証拠(エビデンス)がそろった時点では介入が手遅れになるという「エビデンスのジレンマ」を、政策立案者が乗り越えるための支援を提供することを目的としている。

(3) 我が国における国際連携・協力

我が国では、これまで取り組んできた国際連携・協力に加え、2025 年も新たな取り組みを開始した。それぞれの国際連携・協力について紹介する。

(a) 新たな国際連携に関する取り組み

サイバーセキュリティへの対応に関し、我が国は従前より様々な国際連携を進めている。中でも、更なる連携強化を行うべく 2025 年に開始した新たな取り組みを以下に示す。

(ア) 日米韓による北朝鮮サイバー脅威への共同対処

日本・米国・韓国は、北朝鮮のサイバーアクターによる暗号資産の窃取を阻止するため、2025 年 1 月、3 カ国で「北朝鮮による暗号資産窃取及び官民連携に関する共同声明^{*23}」を発出した。

この共同対処の取り組みの目的は、北朝鮮のサイバーアクターが、暗号資産業界を標的にしている現状に対し、官民一体となった防御網を構築することにより、具体的な施策は以下の 3 点である。

- 注意喚起の共同実施: 北朝鮮による、身分を偽って IT 業務を受注する「IT 労働者」の手口や、ソーシャルエンジニアリング(なりすまし等)の具体例を民間セクターへ周知
- 実務レベルの連携: 「日米韓サイバー・ワーキンググループ」を通じて、脅威情報のリアルタイム共有や、制裁回避を防ぐための技術的対策を協議^{*24}

- ・エコシステムの保護：暗号資産の不正流出を検知・阻止するため、暗号資産業界と連携し、攻撃の初期段階での対処能力を向上

なお、これらの施策は、2023年の「キャンプ・デービッド合意^{*25}」に基づく協力を更に具体化したものであり、北朝鮮の資金源を断つための「経済安全保障」の一環としても位置付けられている。

(イ) セキュリティ・ラベリングの国際相互承認

この取り組みは、国ごとに異なる IoT 製品（スマート家電や監視カメラ等）のセキュリティ基準（セキュリティラベル）を共通化し、他国でも認められる仕組みを構築するもの^{*26}で、二重の検査コスト等によるメーカーの負担を軽減することを目的としている。

相互承認に向けた国際連携としては、2025年11月、日本(JC-STAR)と英国(PSTI法)^{*27}の間で相互承認に関する覚書の署名が行われ、2026年1月に同覚書が発効し、JC-STARとPSTI法(Product Security and Telecommunications Infrastructure Act)との間での相互承認が開始した。また、同年3月、日本(JC-STAR)とシンガポール(Cybersecurity Labelling Scheme)^{*28}の間で相互認証に関する覚書の署名が行われ、同年6月1日、相互承認を開始した^{*29}。そのほか、米国(U.S. Cyber Trust Mark)やEU(Cyber Resilience Act)との間でも相互認証に向けた取り組みが進んでいる。

セキュリティ・ラベリングの国際相互承認の取り組みは、消費者の安全確保と、企業のグローバル展開におけるコスト削減の両立を図ることを目的としている(JC-STARについては「3.3.1 セキュリティ要件適合評価及びラベリング制度(JC-STAR)」参照)。

(b) 各国との継続的な連携強化の取り組み

これまで培ってきたサイバーセキュリティに関する各国との国際連携についても、継続的にその取り組みを進めている。以下にそれらの取り組みの事例を示す。

(ア) 日米サイバー対話(第10回)

2025年6月18日、東京において、第10回日米サイバー対話が開催された^{*30}。この対話では、両国におけるサイバー政策、二国間協力、国際場裡における能力構築支援を含む協力及び悪質なサイバー活動への対応等、サイバーに関する日米協力について議論が行われた。

日本側から斉田幸雄外務省総合外交政策局参事官兼サイバー政策担当大使を筆頭に、外務省、内閣サイバーセキュリティセンター、内閣官房サイバー安全保障体制整備準備室、国家安全保障局、警察庁、総務省、公安調査庁、経済産業省、防衛省等からの幅広い政府関係者が、米国側から、Liesyl Franz 国務省サイバー空間・デジタル政策局次官補代理を筆頭に国務省、米国立標準技術研究所(NIST: National Institute of Standards and Technology)、国防省、連邦捜査局(FBI: Federal Bureau of Investigation)を含む幅広い政府関係者がそれぞれ出席した。

(イ) 北朝鮮サイバー脅威に関する日米韓外交当局間作業部会(第4回)

北朝鮮による悪意あるサイバー活動への対抗策を協議する枠組みである日米韓外交当局間作業部会の第4回が2025年8月27日及び28日の2日間、東京において開催された^{*31}。北朝鮮の不法な大量破壊兵器及び弾道ミサイル開発の資金源となっている暗号資産の窃取を含む悪意あるサイバー活動や北朝鮮IT労働者による不正な収益活動に対して深刻な懸念を表明し、共同声明を発出した^{*32}。三宅史人外務省サイバー政策担当大使兼総合外交政策局参事官、Jonathan Fritz 米国国務省筆頭国務次官補代理(東アジア・太平洋担当)、白琬静(ベク・ユンジョン)韓国外交部国際安保局次長が共同議長を務め、日米韓の幅広い関係省庁が出席した。

(ウ) 日英サイバー対話(第9回)

2026年2月27日、東京において第9回日英サイバー対話が開催された^{*33}。2025年の日本のサイバー対処能力強化法及び同整備法の成立や新たなサイバーセキュリティ戦略の策定も踏まえ、日英両国のサイバーセキュリティ戦略や政策等の幅広い論点について意見交換を行った。三宅史人外務省総合外交政策局審議官兼サイバー政策担当大使とAndrew Whittaker 外務・英連邦・開発省サイバー政策部長が共同議長を務め、日本側からは、外務省、国家サイバー統括室(NCO: National Cybersecurity Office)、警察庁、総務省、経済産業省、防衛省及び一般社団法人JPCERTコーディネーションセンター(JPCERT/CC: Japan Computer Emergency Response Team Coordination Center)の関係者が、英国側からは、外務・英連邦・開発省、ビジネス・貿易省、科学・イノベーション・技術省及び

英国国家サイバーセキュリティセンター（NCSC：National Cyber Security Centre）の関係者がそれぞれ出席した。

（エ）日 ASEAN サイバーセキュリティ政策会議（第 18 回）

日本と ASEAN 諸国間の国際的な連携を深め、地域全体のサイバーセキュリティ能力を向上させることを目的とした実務者級の枠組みとして、日 ASEAN サイバーセキュリティ政策会議の第 18 回が 2025 年 10 月 8 日及び 9 日の 2 日間、東京において開催された^{*34}。同会議では、ASEAN 加盟国、ASEAN 事務局及び日本のサイバーセキュリティ政策推進省庁（NCO、総務省、外務省、経済産業省）の間で、今後の取り組み方針を共有した。また、2024 年の政策会議において合意された日 ASEAN サイバーセキュリティ政策便覧の策定、重要インフラ防護ワークショップ、産官学連携、共同相互通知、日 ASEAN サイバー演習、共同意識啓発、能力構築、ワーキンググループ運営について、協力活動の成果を共有し、今後の協力活動の更なる推進を確認するとともに、官民含めて今後の日 ASEAN 間の連携を一層強化することについて合意した。

なお同会議の議長国として、日本の高見澤将林笹川平和財団上席フェロー・東京大学客員教授及びラオスのカムラ・ソーナラット技術通信省サイバーセキュリティ局セキュリティ庁長官が共同議長を務めた。

（オ）日・EU サイバー対話（第 7 回）

2026 年 1 月 28 日、ベルギーの首都ブリュッセルにおいて、第 7 回日・EU サイバー対話が開催された^{*35}。同対話では、2025 年の日本のサイバー対処能力強化法及び同整備法の成立や新たなサイバーセキュリティ戦略の決定も踏まえ、日・EU 双方のサイバーセキュリティ戦略・政策、サイバー分野における諸課題、日・EU 間及び国連等の多国間での協力、能力構築支援等の幅広い論点について意見交換を行った。山本武臣外務省総合外交政策局安全保障政策課長と Barbara GALLO 欧州対外活動庁平和・安全保障・防衛総局ハイブリッド脅威・サイバー課長及び Christiane Kirketerp de Viron 欧州委員会通信ネットワーク・コンテンツ・デジタル総局サイバーセキュリティ・信頼局長代理が共同議長を務め日本側からは、外務省、NCO、警察庁、総務省、経済産業省、防衛省及び JPCERT/CC の関係者が、EU 側からは、欧州対外活動庁、欧州委員会及び欧州刑事警察機構（Europol：European Union Agency for Law Enforcement Cooperation）等の関係者がそ

れぞれ出席した。

また、「悪意あるサイバー活動に対する外交的反応についての日・EU ラウンドテーブル」を開催し、双方のサイバー分野での外交についても意見交換を行った。

（カ）インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク

2025 年 11 月、経済産業省と IPA は米国政府・EU 政府と連携し、産業制御システムのサイバーセキュリティ対策に関するキャパシティビルディングプログラム「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク」を日米 EU 共催で開催した^{*36}。同イベントは、インド太平洋地域の重要インフラ事業者、製造業者等のほか、OT（Operational Technology：制御技術）・IT に関連する政府機関におけるサイバーセキュリティ担当者や政策担当者等を対象としており、2018 年から毎年実施している。

2025 年は、日米欧のサプライチェーンレジリエンス強化及びインド太平洋地域のサイバーセキュリティ対策に関する能力構築を最大限に実現するため、演習規模を拡大して実施した。プログラムでは IPA 産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）による各業界特有のリスクや事例等を盛り込んだ仮想企業のシナリオを用いた業界別ワークショップや、産業制御分野における AI を活用したサイバー攻撃に対するハンズオン演習を実施した。また、新規のプログラムとして欧州連合サイバーセキュリティ機関（ENISA：The European Union Agency for Cybersecurity）によるワークショップを実施した。更に、日米欧の政府高官や重要インフラ企業等によるセミナーも実施し、参加者の知見の取得・能力向上の機会を提供した。

（キ）日 ASEAN サイバーセキュリティ能力構築センターと ICSCoE の連携

2025 年 7 月、ICSCoE は日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC：ASEAN-Japan Cybersecurity Capacity Building Centre）、タイ国家サイバーセキュリティ庁（NCSA：National Cyber Security Agency）及びマヒドン大学と協働し、タイのバンコクで OT セキュリティ人材育成プログラムを提供した^{*37}。同プログラムはサイバーセキュリティ能力の向上と各国との連携強化を目的として実施された。研修プログラムでは、ICSCoE による仮想企業のシナリオを用い

た参加国・業界ごとの課題やベストプラクティスを参加者同士が共有し合うワークショップのほか、実際の OT 環境を模したツールやシナリオを用いたハンズオン演習等、受講者へ実践的なスキル向上の機会を提供した。

(ク)キングモンクット工科大学 KOSEN-KMITL(タイ高専)における産業サイバーセキュリティ教育支援

ICSCoEとタイのキングモンクット工科大学 KOSEN-KMITL は、日本企業の海外における一大拠点であるタイでの産業サイバーセキュリティ人材の高度化促進及び産業制御システムのサイバーセキュリティの確保を目指し、産業サイバーセキュリティ教育支援に関する覚書を2024年7月に締結している^{*38}。同覚書に基づき、同校のコンピューター工学科のタイ人教員に対して、講義を提供(2025年度に全24回中12回実施)し、産業サイバーセキュリティに関する指導者育成及び教材開発の支援を行った。

(ケ)サイバーセキュリティとデジタルトラストサービスに関する日ASEAN能力向上プログラム強化プロジェクト^{*39}

国際協力機構(JICA:Japan International Cooperation Agency)が中心となって進める同プロジェクトは、2025年、第2フェーズ(2023～2027年)の一環として、以下のような施設拡充や訓練の高度化等、多くの具体的な活動を実施した。

- ・バンコクの新研修施設(AJCCBC)の開所^{*40}:2025年8月12日、タイ・バンコクにあるAJCCBCの新施設が正式に開所した。この施設は、ASEAN全域からの研修生を受け入れ、より実践的な演習^{*41}を行うためのスペースであり、最新の産業制御システムの演習環境や、AIを活用した脅威検知トレーニングのためのインフラが整備されている。
- ・「デジタルトラスト」分野のトレーニング拡充:同プロジェクト名にも含まれる「デジタルトラスト(電子署名や認証等の信頼性確保)」に関する活動が本格化した。トレーニング内容として、サイバー攻撃への防御だけでなく、経済活動の基盤となる「信頼性」を確保するための制度設計や技術的支援に関するワークショップが実施された。
- ・若年層向けプログラムの展開:ASEAN諸国の若手専門家や学生を対象とした人材育成プログラムが提供され、地域全体の底上げを図る取り組みが強化された。

(コ)大洋州島しょ国・地域向けサイバーセキュリティ能力構築演習

総務省の主催により、2025年9月27日～10月2日に「大洋州島しょ国・地域向けサイバーセキュリティ能力構築演習(令和7年度第1回演習)」がフィジーで実施された^{*42}。大洋州14の国・地域から計31名が参加し、日本の「実践的サイバー防御演習(CYDER: Cyber Defense Exercise with Recurrence)」を用いたトレーニングにより、基礎知識の習得から、サイバー攻撃を受けた際の一連のインシデントハンドリングまでを体験した。

2026年2月2～6日には、総務省とJICAの共催で、「大洋州島しょ国・地域向けサイバーセキュリティ能力構築演習(令和7年度第2回)」が実施された^{*43}。大洋州12の国・地域から計24名が参加し、CYDERを用いたトレーニングが実施された。

4.1.2 米国の政策

第二次 Donald Trump 政権は2026年3月に同政権のサイバーセキュリティ戦略を発表した。前 Biden 政権のサイバーセキュリティ戦略が39ページにわたり、具体的な施策や役割分担にも踏み込んだ政策文書であったのに対し、新たに提示された戦略は7ページにまとめられ、優先順位と基本方針の提示に重点を置く内容となっている。「アメリカ・ファースト」の理念のもと、米国が有する高度な技術力及び軍事的優位性をサイバー空間においても積極的に活用する方針を明確化した上で、従来の防御中心の枠組みから、攻勢的要素を含む総合的なサイバー戦略へと軸足を移している。以下では、こうした政策転換の全体像について、前政権との比較及び継続・変化の観点から整理する。

(1)2023年戦略から2026年戦略への転換

以下では、Biden 政権の2023年国家サイバーセキュリティ戦略と、第二次 Trump 政権の2026年米国サイバー戦略を比較し、それぞれの特徴について概観する。

(a)Biden 政権下のサイバーセキュリティ戦略

2023年3月1日に Biden 政権(以下、前政権)下のホワイトハウスが公表した「国家サイバーセキュリティ戦略(National Cybersecurity Strategy^{*44})」(以下、2023年戦略)は、「従来の個人や中小企業に過度に依存した防御モデルから、最も能力を有する主体が相応の責任を担う公平なエコシステムへの転換」及び「長期的な

投資を促進するためのインセンティブ構造の再設計」を重視し、①重要インフラの防御 (Defend Critical Infrastructure)、②脅威主体の妨害と解体 (Disrupt and Dismantle Threat Actors)、③セキュリティとレジリエンスを推進するための市場原理の形成 (Shape Market Forces to Drive Security and Resilience)、④レジリエントな未来への投資 (Invest in a Resilient Future)、⑤共通の目標を追求するための国際パートナーシップの構築 (Forge International Partnerships to Pursue Shared Goals)の五つの柱から構成されている。具体的には、データ管理主体及びシステムの所有者・運用者、ソフトウェア・ハードウェア開発事業者、並びに連邦政府を、能力及び責任の観点から中核的主体として位置付け、これら主体に対するサイバーリスク低減責任の再配分を通じて、防御可能性及び回復力 (レジリエンス) を備えたデジタルエコシステムの構築と信頼性の確保を目指すものである。

(b) 第二次 Trump 政権下のサイバーセキュリティ戦略

2026 年 3 月 6 日に、第二次 Trump 政権 (以下、現政権) が提示した「Trump 大統領の米国サイバー戦略 (President Trump's Cyber Strategy for America^{※45)}」 (以下、2026 年戦略) は、サイバー空間を米国の軍事力及び経済力の延長として位置付け、「アメリカ・ファースト」の理念のもとで技術的優位性の確保を最優先とする等、戦略の大幅な方向転換を示している。2026 年戦略は、①敵対者の行動の形成・抑止 (Shape Adversary Behavior)、②常識的な規制の推進 (Promote Common Sense Regulation)、③連邦政府ネットワークの近代化とセキュリティ確保 (Modernize and Secure Federal Government Networks)、④重要インフラ防護 (Secure Critical Infrastructure)、⑤重要・新興技術における優位性の維持 (Sustain Superiority in Critical and Emerging Technologies)、⑥サイバー人材の育成と対応能力の強化 (Build Talent and Capacity) の六つの柱で構成されている。

国家安全保障に直結する実務的・技術的領域においては、2023 年戦略と一定の連続性が認められる。敵対者の活動を早期に把握し、その基盤インフラを能動的に無力化する方針は両政権に共通しており、2026 年戦略ではこれがより積極的な攻勢的サイバー作戦として具体化されている。更に、連邦政府ネットワークにおけるゼロトラスト・アーキテクチャの導入、耐量子計算機暗号 (PQC: Post-Quantum Cryptography) への移行、ク

ラウドサービスの活用推進、並びにサイバー人材の確保・育成の加速は、両政権を通じて継続的に最優先課題として位置付けられている。

一方で、2026 年戦略は、敵対者に対して高度かつ非対称的な能力により重大なコストを負わせるという能動的抑止の姿勢を明確化するとともに、サイバー領域に限定することなく国家のあらゆる手段を用いて攻撃に対する代償を負わせるとしている。また、従来の過度に負担の大きいチェックリスト型規制を見直し、民間企業の機動性及びイノベーションを阻害しない合理的な制度設計への転換を志向している。更に、サプライチェーンセキュリティにおいては、前政権が多国間協調を基軸としたのに対し、2026 年戦略では敵対国ベンダーの排除及び国産技術の優先的採用を重視する等、より保護主義的なアプローチが採用されている。

(2) 戦略間で継続する重要課題

ここでは、現政権が掲げるサイバーセキュリティ政策のうち、前政権の基本路線を継承し、継続して推進される重要課題について記述する。具体的には、脅威アクターの能動的な無力化と連邦政府の運用能力強化、重要インフラ保護、並びに将来的な量子脅威を見据えた PQC への移行とデジタル認証を含む通信インフラの近代化に向けた具体的な施策について概説する。

(a) 敵対者の積極的無力化とサイバー運用能力の強化

現政権は、サイバー空間における抑止力を、能動的な無力化措置を通じて確保する方針を明確にしている。2026 年戦略の方針においては、米国の高度な技術基盤及び軍事的優位性を背景として、司法省 (DOJ: Department of Justice) 及び連邦捜査局 (FBI: Federal Bureau of Investigation) による法執行活動と、国防総省 (DoD: Department of Defense) が推進する「前方防御 (Defend Forward)」の概念を統合・拡張し、サイバー空間を含む複合領域において実効的な抑止力を確立するとともに、戦略的主導権の確保を目指すものとしている。

また、2026 年 3 月 6 日に発令された大統領令第 14390 号においては、国際犯罪組織及びこれを黙認または支援する外国政府に対し、従来の法執行及び外交手段に加え、潜在的な攻勢的措置を含む包括的な対抗手段を講じる方針が示された。これに基づき、国務長官、財務長官、陸軍長官、司法長官及び国土安全保障長官は、国家サイバー局長室 (ONCD: Office

of the National Cyber Director)並びに大統領補佐官と緊密に連携し、発令後60日以内に既存の政策・運用枠組みの再評価を実施するとともに、120日以内に国際犯罪組織の特定・解体及び詐欺拠点の無力化を目的とする具体的な行動計画を策定し、大統領に提出することが求められている^{*46}。更に、運用面の実効性向上を目的として、国家調整センター(NCC: National Coordination Center)内に新たな運用セル(部署)を設置する計画が示されている。NCCは、大統領令第14159号に基づき設立された組織であり、米国の市民、企業及び重要インフラ等を標的とする外国の国際犯罪組織によるサイバー犯罪に対し、検知、妨害、解体及び抑止を目的として連邦政府の取り組みを調整する役割を担っている。当該セルが民間部門の保有するインテリジェンスを戦略的に活用して敵対者のインフラ遮断を図るとともに、司法長官が90日以内に没収資産の被害者還元を目的とした「被害者回復プログラム」の創設を勧告する等、法的措置と実効的な被害回復を組み合わせた多層的な対応枠組みの構築が見込まれている。

更に、現政権の2026年戦略においては、民間企業による敵対者への対抗活動に対して、より広い裁量を認める姿勢が示されている。ただし、この点については、2026年4月時点において、民間企業に対して積極的なハックバック(攻撃者への逆ハッキング)等の行為を推奨または指示する行政命令、規制、あるいはガイダンスは少なくとも公表されていない。

(b) 重要インフラ保護政策の見直しとリスクベースアプローチ

米国においては、2001年10月に制定された合衆国法典第42編第5195c条において、重要インフラの定義は「物理的か仮想的かを問わず、米国にとって極めて重要であり、その機能停止または破壊が、安全保障、国家経済安全保障、国民の公衆衛生または安全、あるいはこれらの事項のいかなる組み合わせに対しても壊滅的な影響を及ぼすようなシステム及び資産」とされている^{*47}。この定義を踏まえ、重要インフラ防護の分野においては、従来の画一的なセキュリティ基準への準拠を重視したアプローチから、脅威の優先度に応じてリスクを特定・分析し、定量的に評価する「リスクベースアプローチ」への転換が進展している。

2025年3月18日に発令された大統領令第14239号^{*48}では、サイバー攻撃を含む動的かつ複合的な脅威から国家の安全及び経済基盤を保護する観点から、

連邦政府における重要インフラ政策の包括的見直しについて、国家安全保障担当大統領補佐官に対し、科学技術政策局長及び関係機関の長と連携の上で対応するよう指示がなされた。これを受け、同補佐官が関係機関との調整を主導し、2025年6月に「国家レジリエンス戦略^{*49}」を策定した。同戦略は、従来の気候変動等を重視する「全災害対応」から、敵対国や脅威から米国の国益を守り抜く「アメリカ・ファースト」の包括的なビジョンを提示するものへと転換し、「優先順位付け(Prioritize)」「近代化(Modernize)」「連邦主義による責任の分散(Distribute)」「簡素化(Simplify)」の四つの指針に基づき、以下の四つの主要領域における強化により構成される。

- 国家安全保障(National Security): 通信やインフラを近代化して指揮統制能力を分散・確保し、同盟国との連携強化を図り、米国の優位性を維持する。
- 経済(Economy): サプライチェーンを強化して米国の産業や技術を外国の支配から保護し、外部ショックに耐え得る経済システムを推進する。
- 公衆衛生と安全(Public Health and Safety): 連邦政府への過度な依存から脱却し、州や地方自治体が自立して緊急事態に対応できるよう、財政的・運用的な対応能力の構築を促進する。
- 国家インフラ(National Infrastructure): 過度な規制を削減しつつ、産業界自らがレジリエンスを標準として組み込むことを促し、物理的及びサイバー環境の信頼性を向上させる。

特にサイバー分野においては、設計段階から専門的知見を統合するサイバーインフォームド・エンジニアリングの適用、政府資金を用いる事業におけるリスク評価の義務化、並びにインフラ運営者及び労働者に対するセキュリティ訓練の提供が明確に求められている。また、同大統領令においては、同戦略を4年ごとに見直すことが義務付けられているほか、発令後180日以内に「国家安全保障覚書第22号(NSM-22)」を含む既存の重要インフラ関連政策の再評価を実施し、必要に応じて改定及び統合を行うことが求められている。更に、発令後240日以内には、同補佐官の主導のもと、国家インフラ及び関連システムに対する自然起因リスク及び悪意ある脅威を網羅的に特定・可視化し、定量的に評価するための「国家リスク登録簿(National Risk Register)」の整備に向けた調整を実施することが指示されている。

(c)耐量子計算機暗号(PQC)への移行と通信・認証基盤の高度化

将来的な量子コンピューターによる暗号解読リスクへの対応として、推奨されている耐量子計算機暗号(PQC:Post-Quantum Cryptography)^{*50}への移行及び通信基盤の高度化は、前政権から継続する最重要課題の一つとして位置付けられており、その取り組みは加速している。

2025年6月6日に発令された大統領令第14306号に基づき、国土安全保障省(DHS:Department of Homeland Security)及びCISAは、国家安全保障局(NSA:National Security Agency)と連携し、2025年12月1日までにPQCをサポートする製品カテゴリの一覧を公表することが求められていた^{*51}。

これを受けてCISAは2026年1月、「Product Categories for Technologies That Use Post-Quantum Cryptography Standards^{*52}」を公表し、クラウドサービス、Webソフトウェア、ネットワーク機器、エンドポイントセキュリティ等、PQCをサポートする主要なハードウェア及びソフトウェア製品カテゴリを整理したリストを公開した。

また、同大統領令では、通信の機密性及び完全性を確保する観点から、2030年1月2日までに、すべての連邦機関に対してTLS 1.3またはその後継プロトコルの実装のための要件の発行が義務付けられている。

更に、これらの施策に加え、行政管理予算局(OMB:Office of Management and Budget)が策定した指針「M-25-34 (Fiscal Year (FY) 2027 Administration Research and Development Budget Priorities and Cross-Cutting Actions)^{*53}」に基づき、2027年度の研究開発予算においては、PQCの導入促進を始め、AI、量子科学、半導体、並びに5G/6Gを含む次世代通信技術が重点分野として位置付けられており、技術的優位性の確保及び国家安全保障の強化に資する分野へ重点的な資源配分を行う方針とされている。

こうした技術基盤の高度化と並行して、前政権期から継続するデジタル・アイデンティティ分野の整備も進展している。具体的には、NISTが中心となり、モバイル運転免許証(mDL:Mobile Driver's License)を始めとする、安全性の確保とプライバシー保護の両立を志向したデジタル認証基盤の標準化及び社会実装が推進されている。2025年7月には、NISTより「デジタルアイデンティティガイドライン第4版(SP 800-63 Revision 4^{*54})」が公表され、フィッシング耐性を有する認証方式の導入や

自動化された攻撃への対策強化等、認証基盤の信頼性向上に向けた要件が拡充された。

加えて、2025年5月には米国自動車管理者協会(AAMVA:American Association of Motor Vehicle Administrators)による「mDL実装ガイドライン第1.5版^{*55}」が、2026年3月には「金融機関向けmDL実装ガイドライン」のドラフト版^{*56}がそれぞれ公表されている。これらは、前政権下で提唱された「セキュアかつプライバシー保護に配慮したデジタル・アイデンティティ」の理念を継承しつつ、現政権における「政府情報システムの近代化」の一環として実装を推進するものである。これらの技術は、サイバー空間における本人確認の信頼性を向上させることで、不正アクセスやオンライン詐欺の防止、及び行政サービスの利便性向上に資する基盤技術として重要な役割を担うものと位置付けられている。

(3)戦略間で転換される政策方針

ここでは、現政権が掲げるサイバーセキュリティ政策のうち、前政権の方針から大きな転換や見直しが図られた新たな政策方針について記述する。具体的には、形式的なコンプライアンスの緩和に伴う民間部門の規制負担軽減、保護主義的な米国製品優先の徹底、無人航空機システムや体現型AIを対象とする厳格なセキュリティ基準の確立、連邦政府ネットワーク防御体制の再編、外国の影響下にある製品への対策、及びサイバー人材確保に伴う多様性の排除と能力・実績を最優先する実利主義的なサイバー人材育成への移行について概説する。

(a)常識的なサイバー規制の推進と負担軽減

現政権は、前政権において推進されてきた「コンプライアンスを重視した法的責任の付与」という枠組みを見直し、イノベーションへの影響を最小限に抑えつつ実効性を確保する「合理的な規制アプローチ」の確立を志向することで、民間部門の負担軽減を図っている。

その具体的施策として、2026年1月23日に発出されたOMBメモランダム「M-26-05^{*57}」では、前政権下のソフトウェア・サプライチェーンセキュリティ強化指針(M-22-18^{*58}及びM-23-16^{*59})が見直しの対象とされ、撤回された。これらの指針は、実質的なセキュリティ向上よりも形式的なコンプライアンスを優先し、政府に製品を納入するソフトウェアベンダー等の民間企業に過度な負担を課していたほか、「実効的なセキュリティ投資よりもコンプライアンス対応を優先させる、検証が十分でなく負担の大きいプロセス」であるとされた。これを受け、各行政

機関の長は、画一的なコンプライアンス要件への一律適合を求める従来の手法から転換し、各機関のミッション及びリスク特性に応じたリスクベースアプローチに基づき、ハードウェア及びソフトウェアの安全性評価・検証を実施する方針へ移行している。

また、ソフトウェアの透明性向上及び脆弱性管理の高度化に資する、ソフトウェアを構成するコンポーネントや相互依存関係、ライセンスデータ等を一覧化した「SBOM (Software Bill of Materials: ソフトウェア部品表)」の提供要件についても見直しが行われている。旧指針である M-22-18 のもとでは、各機関はソフトウェアの重要度や独自の判断に基づき、調達要件において SBOM を要求することができる (may be required) とされていた。更に、提出される SBOM は、電気通信情報局 (NTIA: National Telecommunications and Information Administration) が定義した「最小要素」または CISA が公表する後継ガイダンスに従って作成されなければならない (must be generated) とされ、厳格なデータフォーマットへの準拠が義務付けられていた。これに対し、現政権下の M-26-05 では、「各機関は、要求に応じて最新の SBOM を提供しようソフトウェア生産者に求める契約条項を採用することを選択してもよい (may also choose to adopt)」とされ、各機関が個別の調達要件や契約条件に応じて導入の要否を判断する「選択的適用」として位置付けられている。

(b) AI 特有のサイバー脅威への対応と懸念国製 AI の排除

「懸念国」による技術的浸透の抑止及び国産製品の優先的採用を基軸とした保護主義的なサイバーセキュリティ政策の方向性が明確化されている^{*60-1}。同方針の具体化に向け、2027 年度予算編成においては、AI セキュリティの確保が最重要課題の一つとして位置付けられているほか、行政に加え、立法主導による法制化の動きも進展している。

その象徴的な事例として、2025 年 12 月 18 日に制定された公法 119-60 号第 1512 条において、DoD における AI 及び機械学習の安全保障に関する法的枠組みの整備が指示された^{*60-2}。同法では国防長官は法施行から 180 日以内に、国家防衛に用いられる AI・機械学習システム及びモデルに関するサイバーセキュリティ方針

を策定し、これを実施することが義務付けられている。これは大統領令による指示を超え、連邦法としての強制力を伴うものであり、当該方針には以下の事項を含めることが規定されている。

- AI・機械学習特有の脅威（モデルシリアライズ攻撃、モデル改ざん、データ漏えい、敵対的プロンプトインジェクション、モデル抽出、ジェイルブレイク、サプライチェーン攻撃等）への防護
- システムのライフサイクル全体にわたるサイバーセキュリティ対策の実施
- 業界標準フレームワークの採用によるベストプラクティスの確立
- 完全性及び耐性確保のためのガバナンス、試験、監査、監視に関する基準の整備
- AI 特有の脆弱性に対応可能な人材の育成に向けた教育・訓練要件の整備

更に、AI セキュリティの高度化に向けた産学官連携も進展している。大統領令第 14306 号に基づき、商務省 (DOC: Department of Commerce)、エネルギー省 (DOE: Department of Energy)、DHS 及び国立科学財団 (NSF: National Science Foundation) の 4 機関が連携し、2025 年 11 月までにサイバー防御研究に資するデータセットを学術機関へ提供するための基盤整備を実施することが求められている^{*51}。同施策は、産学官連携を通じた防御的 AI 技術の高度化を目的とするものである。同大統領令の進捗として、2026 年に入り、商務省傘下の NIST において、サイバー防御研究用データセットの学術コミュニティへの提供に向けた具体的な成果検証やプロジェクトへの組み込みが順次開始されている^{*60-3}。

また、OMB 覚書「M-25-22^{*61}」においては、米国製 AI 製品の採用を最大化する「Buy American」方針が示されている。加えて、AI 特有の脅威及び情報漏えいリスクへの対応として、政府の非公開データがベンダーの商用 AI の学習に無断で利用されることを契約上恒久的に禁止する措置が講じられている。更に、特定ベンダーへの過度な依存を回避する観点から、導入後においても継続的なリスクモニタリング及び独立した検証・評価の実施が求められており、安全性及びレジリエンスを備えた AI の調達・運用体制の確立が志向されている。

(c) 無人航空機システム(UAS)及び体现型 AI におけるセキュリティ基準の確立

前述のサプライチェーン保護の方針を技術的観点から具体化するものとして、連邦政府はドローンを含む無人航空機システム(UAS: Unmanned Aircraft Systems)及び関連する AI 技術に対し、厳格なサイバーセキュリティ要件を規定している。

OMB 覚書「M-26-02」^{*62}においては、UAS の調達に先立ち、FIPS 199 に基づくセキュリティ影響評価の実施が義務付けられている。具体的な技術要件としては、NIST SP 800-63 に準拠した多要素認証の導入、通信データ及び保存データの暗号化、並びに遠隔消去機能の実装が不可欠とされている。

更に、「M-25-34」^{*53}及び「M-25-21」^{*63}において、ドローン等の自律型ロボットは「体现型 AI (Embodied AI)」かつ「高インパクト AI」として位置付けられている。これにより、物理的損害を引き起こすリスクへの対応として、運用開始前の脆弱性試験の実施、運用中の継続的な監視、並びに人間による介入を可能とするフェイルセーフ機能の実装が強く求められている。加えて、AI モデルの構成を可視化する「AI SBOM」の提出を義務付ける等、ソフトウェア及び AI の透明性を確保することにより、システムのライフサイクル全体にわたるサイバーレジリエンスの向上が図られている。

(d) サプライチェーンの信頼性確保と米国製品優先の徹底

テクノロジー調達におけるサプライチェーンの自律性及び安全性の確保については、2025 年 6 月 6 日の大統領令第 14307 号^{*64}に基づき、外国製機器に起因するデータ漏えい及び監視リスクの排除に向けた取り組みが進められている。同大統領令では、サプライチェーン上のリスクを有する企業を特定する「対象外国実体リスト」の策定が指示されており、外国勢力による不当な関与から国内の重要インフラを防護するための枠組みが整備されている。これに伴い、連邦機関に対しては、外国製品への依存度の低減を図るとともに、技術的主権及びセキュリティが確保された米国製品の採用を最大限優先することが求められている。

また、大統領令第 14306 号^{*51}に基づき、消費者向け IoT 製品についても、2027 年 1 月までに「U.S. Cyber Trust Mark」^{*65}の取得を政府調達の要件とする等、ハードウェアの信頼性を調達基準の中核に位置付ける方針が示されている。同認証マークは、対象となる IoT 製

品が連邦通信委員会(FCC: Federal Communications Commission)の定める最低限のサイバーセキュリティ基準を満たしていることを消費者に示すものであり、製品のセキュリティ評価は、NIST が作成した IoT 製品のコアベースライン(NIST IR 8425)に基づき、データ保護、アクセス制御、ソフトウェアのアップデート機能等が評価されるとしている^{*66}。経済産業省の施策であり IPA が運営する「セキュリティ要件適合評価及びラベリング制度(JC-STAR: Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements)」は、同認証制度との相互認証を目指している^{*67}(「3.3.1 (3) (c) 他国制度との相互承認」参照)。

(e) 連邦政府ネットワークの防御高度化と組織の合理化

連邦政府は、CISA を中核として、連邦文民政府機関(FCEB: Federal Civilian Executive Branch)ネットワークの防御能力の向上を推進している。具体的には、CDM (Continuous Diagnostics and Mitigation: 継続的診断・緩和) プログラムのもとで、54 の政府機関が「Dashboard-as-a-Service (DaaS)」モデルへの移行を完了した^{*68}。これにより、CISA が 2022 年より提供を開始し、すべての連邦文民政府機関に義務付けられている「Protective Domain Name System (DNS) Resolver」サービス^{*69}等を通じて、各機関のセキュリティ状況を CISA がリアルタイムかつ一元的に可視化・管理する体制が整備された。こうした取り組みの成果として、2025 年には連邦ネットワークへの悪意ある接続を約 26.2 億件、重要インフラへの攻撃を約 3.7 億件阻止する等の実績が報告されている^{*68}。また、脆弱性管理の高度化を目的として、既知の悪用された脆弱性(KEV: Known Exploited Vulnerabilities)カタログに 238 件を追加するとともに、4 万 3,000 件超の脆弱性に対して、意思決定を重視した「SSVC (Stakeholder-Specific Vulnerability Categorization)」方式によるスコアリングを実施し、脆弱性対応の優先順位付けの最適化が図られている。更に、2025 年 12 月 11 日には「サイバーセキュリティパフォーマンス目標 2.0(Cybersecurity Performance Goals 2.0」^{*70})を公表し、基礎的なセキュリティ目標が更新された。この更新では、新たに組織統治に重点を置く「The NIST Cybersecurity Framework (CSF) 2.0」^{*71}に準拠し、新たな機能である統治機能に基づく「Govern」の項目が追加されたほか、IT、IoT、OT 等の分野別目標が統合されたことにより、中小企業においても分野に固有の目標について混乱することなく適用でき

ようになった。なお、同目標はおおむね24～36ヵ月ごとに更新される。

これと並行して、2022年に成立した「重要インフラサイバーインシデント報告法（CIRCIA^{*72}）」に基づく実施規則の策定が、最重要課題の一つとされている。同実施規則は、政府サービスや交通システム等、定められた重要インフラ16分野^{*73-1}の対象事業者に対し、重大なインシデント発生から72時間以内、ランサム攻撃に対する身代金の支払いから24時間以内の報告を義務付けるものである。CISAによって、2024年4月4日に公表された実施規則案^{*73-2}に対しては、広範なパブリックコメントが寄せられ、具体的には産業団体から報告範囲の広さ^{*74}や報告期限の厳しさに対する批判^{*75}が示されたほか、議会からは最終規則が「議会の意図（立法趣旨）」と一致していないとの指摘^{*76}もなされた。これを踏まえ、2026年2月から4月にかけて、適用範囲及び負担軽減に関する議論を目的とした仮想タウンホール（対話集会）が開催される予定であったが^{*77}、政府閉鎖の影響により同年6月に延期された。これに伴い、当初同年5月を予定していた最終規則の公表時期も遅れる見通しとなっている。

一方で、政権交代に伴う政府全体の効率化方針を背景として、2026年度予算案においては、CISAの予算が前年度比で約4億9,500万ドル削減される方針が示された^{*78}。加えて、政府効率化省（DOGE：Department of Government Efficiency）の主導により、人員の約3分の1の削減が進められる等、大規模な組織再編が実施されており、現場の運用体制への影響が指摘されている^{*79}。こうした組織的変化は、CISAの戦略的取り組みにも影響を及ぼしている。国境を越えた重要インフラの相互依存に伴うリスクへの対応を目的とし、2024年10月29日に同庁として初めて、同盟国及びパートナー国との情報共有や技術支援の強化を掲げた「CISA 2025-2026 国際戦略計画^{*80}」が公表されていたが、同計画において国際業務の中核的な調整機能を担っていたCISA ステークホルダーエンゲージメント部門（SED：Stakeholder Engagement Division^{*81}）内の国際関係のオフィスが、2025年の新政権発足以降に実施された大規模な人員削減及び予算の圧縮により廃止された結果、国際連携や情報共有を含む計画の実行体制に対して、実質的な制約が生じると指摘されている^{*82}。

(f) 外国由来アプリケーションに係る安全保障措置の推進

米国においては従来、TikTokが外国の敵対勢力の

影響下にあるとの安全保障上の懸念を背景として、議会において「Protecting Americans from Foreign Adversary Controlled Applications Act^{*83}」が成立しているが、同法に基づく利用禁止措置の施行はこれまで複数回にわたり延期されてきた。

2025年9月25日に発令された大統領令第14352号においては、同法に基づくTikTokの米国内における利用禁止措置を回避しつつ、国家安全保障の確保と事業継続の両立を図るための法的枠組みが示された。当該枠組みにおいては、事業継続の要件として、運営主体となる共同事業体における中国のByteDance Ltd.の出資比率を20%未満に制限するとともに、米国資本による過半数の所有及び支配権の確立が不可欠とされている^{*84}。更に、新たな共同事業体によるソースコードの完全な米国内管理の実施、及び米国の信頼に足るセキュリティパートナーの監督下における、アルゴリズムの米国内での再構築（再トレーニング）が、事業継続の必須要件として位置付けられている。これらの措置により、データプライバシーの保護と国家安全保障の強化の両立が図られることが企図されている。

その後、2026年1月には、TikTokの米国でのサービスについて、米国主体の新たな共同事業体を設立することで最終合意に至り、米国投資家が約80%を保有し、ByteDance Ltd.は約20%未満の少数出資にとどまる形となった。これにより、米国内におけるデータ及びアルゴリズムの管理は当該事業体が担うこととなり、利用禁止措置は回避され、米国内でのサービス継続が可能となった^{*85}。

(g) サイバー人材の育成とスキルベース採用への転換

サイバー空間を支える人材育成の在り方についても政策指針の転換が進展している。2023年戦略と2026年戦略を比較すると、国家のレジリエンス強化に向けた人的資本投資の重要性については共通の認識が示されている一方で、その推進理念やアプローチについては変化が認められる。

まず、実務面においては、両政権の取り組みに一定の継続性が確認できる。具体的には、学位に過度に依存しない職業訓練機関や技術教育機関、登録見習い制度等を活用した実践的な人材育成パイプラインの構築、並びに産学官軍の連携を阻害する要因の解消やスキルベース採用の推進といった即応力を重視した施策は、政権を超えて共通の優先課題として継承されている。

その一方で、人材育成の根本的な理念については、

以下のとおり大幅な方針転換が図られている。2023 年戦略においては、多様性・公平性・包括性（DEI: Diversity, Equity and Inclusion）の観点から、女性や有色人種、LGBTQI+ 等の過小評価されている層への対応を「道義的かつ戦略的に不可欠な要素」と位置付け、構造的な不平等の是正を重視していた。また、移民を重要な人材供給源の一部として位置付ける方針を採用していた。これに対し、2026 年戦略は「アメリカ・ファースト」の理念のもとで DEI に関する施策を排除し、人材を「米国の経済的繁栄及び国家安全保障を支える戦略的資源」として再定義している。これにより、属性に基づく配慮よりも能力及び実績を重視する「実利的な人材確保」の方針が明確化された。更に、国内労働市場の保護を優先し、低コストな海外人材の流入抑制を志向する等、前政権とは対照的なスタンスを示している。加えて、現政権は AI 時代の到来に対応した人材基盤の強化を加速させている。2025 年 4 月 23 日に発令された大統領令第 14277 号^{*86}に基づき、教育省及び労働省等の関係機関が連携し、初等・中等教育段階からの AI 教育の導入や、AI 分野における登録見習い制度の拡充を推進している。

4.1.3 欧州の政策

2025 年度のサイバー空間は、ランサムウェアの高度化や国家支援型攻撃、AI を悪用した攻撃等により、更なる脅威に直面した。これに対し EU は、欧州全体の防衛能力とレジリエンスを強化するべく、包括的な法整備による統一的な防御体制の確立に注力している。以下では欧州におけるサイバー脅威の全体動向と今後の見通しを紹介し、2025 年から 2026 年 1 月にかけて検討・実施された主要なサイバーセキュリティ政策について述べる。

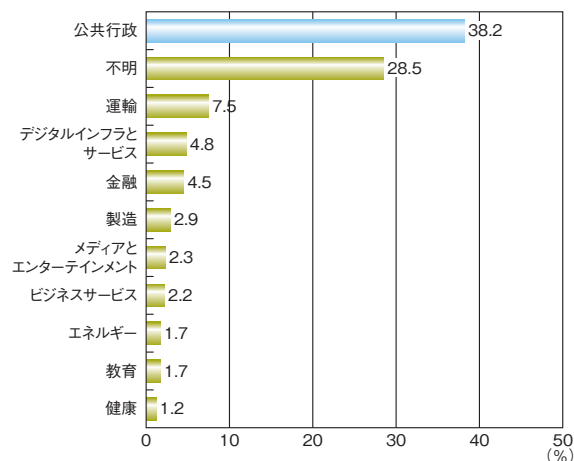
(1) EU 圏におけるサイバー脅威の全体動向

欧州連合サイバーセキュリティ機関（ENISA: The European Union Agency for Cybersecurity）の「ENISA Threat Landscape 2025^{*87}」を基に、2024 年 7 月から 2025 年 6 月にかけての EU 圏の主要なサイバー脅威について述べる。

(a) セクター別の脅威動向

ENISA への報告期間（2024 年 7 月～ 2025 年 6 月）中に発生したインシデントにおいて、標的となったセクター

の上位五つ（「不明」を除く）は、「公共行政」「運輸」「デジタルインフラとサービス」「金融」「製造」であった（図 4-1-1）。



■ 図 4-1-1 セクター別のインシデント発生割合
 （出典）ENISA「ENISA Threat Landscape 2025」（Booklet^{*88}）を基に IPA が編集

「公共行政」セクターは最も標的とされ、インシデント全体の 38.2% を占めた。その多くはハクティビストによる DDos 攻撃であった。特にフランス、イタリア、ドイツ等の公的機関への攻撃が目立ち、選挙や外交政策の発表等に合わせて攻撃が急増する傾向が見られた。

(b) フィッシングの脅威

フィッシングは依然として初期侵入の主要な手段であり、観測事例の初期侵入の手段の約 60% を占めた。Phishing as a Service (PhaaS) プラットフォームの悪用、メール添付ファイルへの悪意コード埋め込み、モバイルデバイスを通じた認証情報の窃取等の詐欺が確認された。

(c) 脆弱性の悪用

脆弱性の悪用は依然としてシステム侵害の中核をなしている。脆弱性が悪用されたインシデントでは、68% が悪意コードの展開に至っている。特に VPN 機器やネットワーク管理ソフトウェアの脆弱性は、境界防御を突破するための格好の標的となっている。

(d) サイバー犯罪の脅威

EU において深刻なサイバー犯罪はランサム攻撃（81.1%）とデータ侵害（15.2%）であり、これらで EU の組織に対する犯罪全体の 96.3% を占める。

ランサム攻撃グループの細分化による犯罪組織のエコシステムの変化により、「Akira」「SafePay」「Qilin」といっ

た新たなランサム攻撃グループが出現した。また攻撃グループは機密データを公開すると脅す二重恐喝に加え、法的圧力や欧州一般データ保護規則（GDPR：General Data Protection Regulation）違反等への懸念を逆手に取った交渉も行っている。

(e) 国家支援型脅威グループによる活動

国家支援型脅威グループは、主にポーランド、フランス、ドイツ、ベルギー、ギリシャ等のウクライナを支援する北大西洋条約機構（NATO：North Atlantic Treaty Organization）加盟国に対して攻撃を集中させている。中でも「APT29」は、欧州宇宙機関（ESA：European Space Agency）や NATO に関わる個人や組織へのフィッシング攻撃を実施した。この攻撃では Amazon や Microsoft 365 等のサービスへのなりすまし、政府機関、軍事、IT セクターの組織を装ったドメインの悪用が見られた。

(f) ハクティビストによる脅威

ハクティビストの活動は、記録されたインシデント全体のほぼ 8 割を占め、その多くは影響が限定的な DDoS 攻撃であり、主に政府の Web サイトや自治体、インフラ機関のポータルサイトが標的となった。攻撃による実質的な被害は限定的だが、SNS 上での宣伝活動を通じて自らの主張を拡散させ、政府に対する市民の信頼を心理的に損なうことを目的としている。

(2) EU 圏におけるサイバー脅威の今後の見通し

「ENISA Threat Landscape 2025」では、EU 圏のサイバー脅威環境の今後の見通しについても論じている。以下に、ENISA によるサイバー脅威の主要な見通しを述べる。

(a) パッチ適用遅延による脆弱性を狙った攻撃の増加

パッチ（修正プログラム）適用の遅延は、引き続き広範かつ迅速な攻撃を受ける対象となる。脆弱性が公開された後、数日あるいは数時間以内に当該脆弱性を悪用した攻撃が発生する可能性があり、インターネットに接続された脆弱性を有する公開資産等は攻撃の標的となり得る。

(b) ハクティビズムによる世論や政策論争への影響

ハクティビストの活動は単なる嫌がらせにとどまらず、情報操作と密接に結び付いている。社会の不安を煽り、

特定の政策に対する論争を激化させる手段としての DDoS 攻撃や、ランサムウェアを利用した攻撃、エネルギーや水道等の制御システムを標的とする攻撃等、心理的影響を最大化する戦術が強化される見通しである。

(c) AI による攻撃サイクルの加速と技術の進化

攻撃専用の AI システムの出現により、これまでは高度な技術が必要だった攻撃が容易になり、攻撃サイクルの劇的な加速が進む見通しである。

(3) デジタルオムニバス規則案

2024 年に発表された「ドラギ報告書（Draghi report）^{*89}」では、欧州経済の競争力強化のための包括的な戦略を提示するとともに、デジタル分野の企業規模拡大における障壁として、企業の法令遵守のための負担の重さと規制の不整合について言及している。特に中小企業にとっては、複数の法律にまたがる重複した要件や、法律ごとに異なる報告義務に対応するための法令遵守コストが極めて高く、法的な不確実性も生じているとされる。

この状況を改善するため、欧州委員会（European Commission）は 2025 年 11 月にデジタルルールの簡素化と統合を柱とする「デジタルオムニバス規則案（Digital Omnibus）^{*90}」を提案した。同規則案は、GDPR、AI 法（EU AI Act）、データ法（Data Act）等の既存法制の複雑な規則を簡素化し、企業の負担を軽減することを主眼とする。

(a) デジタルオムニバス規則案の対象法制

デジタルオムニバス規則案は、以下に示す複数の既存法制の廃止、統合、または改正により、デジタル経済における単一のルールブックとして機能することを目指している^{*91}。

(ア) 改正対象の法制

以下の法制に他の関連法制の規定を吸収・統合することで、その機能を整理・強化する。

- データ法（Data Act ^{*92}）：
規則ごとにばらばらだったデータ利用ルールを一本化する枠組みを構築する。
- GDPR ^{*93}：

「e プライバシー指令」から、クッキー等の端末機器に関するデータ処理や同意の要件を移行することにより、ブラウザ設定等を通じたユーザーによる一括の同意

管理等、利便性と透明性の向上を図る。

- EU 機関データ保護規則 (EUDPR: European Union Data Protection Regulation ^{*94}):
EU の機関、諮問機関、及び事務所における個人データ保護を規定する本規則を、GDPR の改正内容と整合させる形で調整・統合する。
- 単一デジタルゲートウェイ規則 (Single Digital Gateway Regulation ^{*95}):
データ法改正で一本化される新たなデータ利用ルールの枠組みの導入に伴い、登録手続き等の要件を更新し、行政手続きの簡素化を図る。
- AI 法 (AI Act ^{*96}):
AI の安全で信頼できる開発・利用を促進するため、複数の改正を加える。

(イ) 廃止及び他法制に統合する法制

重複を排除し法的明確性を高めるため、以下の法制を廃止する。

- データガバナンス法 (DGA: Data Governance Act):
法制自体は廃止し、データ仲介サービス、データ利他主義 (公益のための自発的なデータ提供)、及び保護されたデータの再利用に関するルールは、簡素化した上で、再構築するデータ法 (「4.1.3 (3) (b) (ア) データ・サイバーセキュリティ・プライバシーに関するデジタルオムニバス」参照) に統合する。
- オープンデータ指令:
公共部門が保有するデータの再利用に関するルールはデータ法に統合する。
- 非個人データ自由移動規則:
EU 域内でのデータローカリゼーション要求の禁止に関する規定等をデータ法に統合する。
- P2B (Platform to Business) 規則:
P2B 規則の大部分は、デジタルサービス法 (DSA: Digital Services Act) ^{*97} やデジタル市場法 (DMA: Digital Markets Act) ^{*98} によりカバーされているため、重複を避け完全に廃止する。
- e プライバシー指令:
端末から取得する個人データ処理や同意要件に関する規定を GDPR に移行することに伴い、重複する規定を整理・廃止する。

(ウ) 報告を一本化する法制

デジタルオムニバス規則案では、NIS 2 指令 (Network and Information Systems Directive 2)、サイバー

レジリエンス法 (CRA: Cyber Resilience Act)、デジタルオペレーショナルレジリエンス法 (DORA: Digital Operational Resilience Act)、重要エンティティレジリエンス法 (CER 指令: Critical Entities Resilience Directive)、GDPR 等で義務付けられている報告形式及び報告先を単一のプラットフォームに統合する。

(b) デジタルオムニバス規則案の概要

デジタルオムニバス規則案は、主に二つの独立した規則案と、それらを補完する追加提案 (デジタルパッケージ) で構成される ^{*99}。

(ア) データ・サイバーセキュリティ・プライバシーに関するデジタルオムニバス

この規則案は、デジタル空間における安全とプライバシー、データの利活用を統合管理するものである。主な提案内容は以下のとおりである。

- インシデント報告の単一窓口設立:
サイバーセキュリティインシデントやデータ侵害の報告を一つの窓口で受け付ける体制を構築する。
- データ法の再構築:
DGA、オープンデータと公共セクター情報の再利用指令 (通称、オープンデータ指令)、非個人データ自由移動規則を統合し、法的明確性を高めた単一のデータ法を制定する。
- P2B 規則の廃止:
DSA 等との重複を解消するため、P2B 規則を廃止し、プラットフォーム事業者と利用企業の取引関係を公正・透明化するための規制を簡素化する。
- GDPR の限定的修正:
中核となる個人データ保護のレベルを維持しつつ、イノベーションを支援するために特定のルールの整合・明確化・簡素化を行う。

(イ) AI に関するデジタルオムニバス (AI 法改正案)

AI 法の効果的な実施を支援し、特に中小企業の負担を軽減するための改正案である ^{*100}。主な内容は以下のとおりである。

- 高リスク AI に対する義務の適用期限調整:
高リスク AI システムに課される義務の適用開始時期を、対応する規格や支援ツールの利用可能性と整合させる。具体的には、規格等が利用可能であることを欧州委員会が確認してから最大 16 ヶ月の猶予を設けるよう調整する。

- 簡素化措置の対象拡大：
中小企業に認められている技術文書の簡素化等の措置を、小規模中堅企業（SMCs：Small Mid-Caps）にも拡大する。
- 規制サンドボックスの拡充：
2028年からのEUレベルの規制サンドボックス^{*101}設置や、自動車等の主要産業における実世界テストの拡充により、イノベーションを促進する。
- ガバナンスの合理化：
EUにおけるAI法執行の中核となるAIオフィスに更なる監督権限を与え、汎用AIモデルに基づくAIシステムの監視を一元化し、ガバナンスの断片化による非効率を解消する。

（ウ）デジタルオムニバスを補完する追加提案（デジタルパッケージ）

規則案を実効的にするため、以下の戦略及びツールが併せて提案されている。

- データ統合戦略：
AI向けの高品質なデータへのアクセスを改善する戦略である。データラボの設置や、データ法に関する法的ヘルプデスクの設置を含む。機密性の高い非個人データの保護や、海外でのEUデータの適正な取り扱いを評価するガイドライン作成等、欧州のデータ主権を強化する措置も講じられる。
- EU ビジネスウォレット：
欧州の企業や公的機関に統一されたデジタルツールを提供する提案である。対面で行っていた書類手続きをデジタル化し、デジタル署名や検証済み書類の交換を安全に行えるようにすることで加盟国間のビジネスを容易にする。

同規則案は今後、欧州議会及び欧州理事会で審議され、欧州委員会では累積的な規制の影響の検証及び継続的な簡素化が進められる。

なお、2026年1月20日に提案されたNIS 2指令の改正案（「4.1.3(5)NIS 2指令の改正案」参照）を含む新しいサイバーセキュリティパッケージには、同規則案のインシデント報告の単一窓口の設立を補完するENISAの役割拡大も含まれており、次項にて述べる。

（4）EU サイバーセキュリティ法（CSA）の改正案

2019年にENISAを恒久的なサイバーセキュリティ機関へと改組・強化し、ICT製品やサービスの共通的な

認証の枠組みを確立した「EU サイバーセキュリティ法（CSA：Cybersecurity Act）^{*102}」は、これまで欧州のデジタル市場における信頼性と安全性の基盤として機能してきた。

欧州委員会は、近年の急激な環境変化に即応し、欧州のサイバーレジリエンスと防衛能力を抜本的に強化するため、2026年1月20日に新サイバーセキュリティパッケージを提案した。このパッケージは、現行の枠組みの欠陥を修正し、EU全体のサイバーセキュリティ・エコシステムをより機敏で統合されたものへ進化させるための包括的な改革案であり、CSA改正案^{*103}とNIS 2指令改正案が含まれる。以下ではCSA改正案を述べ、NIS 2指令改正案については「4.1.3(5)NIS 2指令の改正案」にて述べる。

CSA改正案が解決を目指す主要課題は以下の四つに集約できる。

- 政策の枠組みと現実のニーズの不一致による政策面の乖離の解消
- 相次ぐ法制導入による企業のコンプライアンス負荷の軽減
- 「欧州サイバーセキュリティ認証フレームワーク（ECCF：European Cybersecurity Certification Framework）^{*104}」の実施停滞の改善
- セキュリティ懸念のある第三国へのICTサプライチェーン依存に対する法的対応

以下にCSA改正案の主な措置について述べる。

（a）ENISAの役割拡大

CSA改正案及びENISAが策定した2026～2028年の「単一計画文書（SPD：Single Programming Document）^{*105}」に基づき、ENISAの役割はこれまでの助言的な立場から、より実務的かつ運用の中核を担う専門センターへと大幅に拡大される。これは、EU全体のサイバー防衛能力の底上げを図る措置であり、加盟国及びEU機関に対する運用的・技術的な支援機能が大幅に強化される。拡大された主な役割は以下のとおりである。

（ア）インシデント報告の単一窓口の設立・運営

CSA改正案では、デジタルオムニバス規則案を補完するものとして、ENISAに対しインシデント報告の単一窓口（SEP：Single Entry Point）の設立及びその運営を担わせる、としている。

NIS 2 指令に基づき注視すべき産業セクターに分類される重大エンティティ (essential entity) または重要エンティティ (important entity) の企業等は重大なインシデントが発生した際、この窓口を通じて、共通のテンプレートをを用いて一度通知を行えばよい。通知された情報は、関連する加盟国の CSIRT (Computer Security Incident Response Team) や管轄当局、データ保護当局等へ自動的に配信される。報告対象となる事象には、NIS 2 指令に基づく重大インシデントや、製造業者が CRA に基づき報告する深刻な脆弱性、GDPR が規定する個人データ侵害、DORA が定める金融セクターの ICT 障害、CER 指令や eIDAS (electronic Identification, Authentication and Trust Services: 電子識別、認証、及び信頼サービス) 規則に関連する事象等が含まれる。

(イ) EUVD の運営及び脆弱性管理サービスの提供

ENISA は NIS 2 指令第 12 条に基づく義務として、欧州共通の脆弱性データベース「EUVD (European Vulnerability Database)」を設置し、2025 年 5 月 13 日から正式に運用を開始した^{*106}。EUVD の開発は、障害リスク軽減において、米国等への過度な依存を避け、正確かつタイムリーな脆弱性情報の把握により市場の安全を確保する、欧州独自の脆弱性管理能力の獲得が目的である。

EUVD の運用において、ENISA は ICT 製品・サービスのサプライヤー、研究者、CSIRT 等に対し、公知の脆弱性を自発的に開示・登録できる仕組みを提供する。利害関係者のアクセスのために透明性とアクセシビリティが重視され、幅広い脆弱性管理サービスを提供する。具体的には、脆弱性の早期警告、CVSS (Common Vulnerability Scoring System: 共通脆弱性評価システム) 等を用いた深刻度のスコアリング、脆弱性管理を支援する対策カタログの提供、悪用が確認されている脆弱性の特定等が含まれる。このように、ENISA は EUVD により、EU 全体のサイバー衛生の向上と状況把握の強化を主導する。

(ウ) EU 機関及び CSIRTs との運用協力

ENISA は EU 加盟各国の CSIRT が連携する「CSIRTs ネットワーク」や、国家間の危機管理調整を司る「EU-CyCLONe (European Cyber Crisis Liaison Organisation Network)」の事務局機能を担ってきたが、今回の改正により運用支援の内容がより具体的か

つ強力なものとなった。

具体的には、複数国にまたがり、かつ大規模なサイバー攻撃が発生した際の調整業務や、インシデント発生時の EU 各機関及び各国 CSIRT との協力による復旧支援が、ENISA の職務として明文化されている。特に、Europol との連携を強化し、ランサム攻撃等の被害に対し、早期警告や技術的な復旧支援を行う体制が整備される^{*107}。これにより、加盟国単独で対処が困難な事案に対し、ENISA が高度な専門知識を提供し、EU 全体のレジリエンス向上を目指す。

2025 年 11 月 20 日、ENISA は NIS 2 指令に基づく EUVD の設置・運営により、CVE (Common Vulnerabilities and Exposures: 共通脆弱性識別子) のルート機関に権限が昇格した^{*108}。

CVE ルート機関としての ENISA は、自身の CNA (CVE Numbering Authority) としての機能のほか、管轄する EU 域内の他の CNA を特定し、ENISA 管理下へのスムーズな移行支援を統括する。また各 CNA による CVE ID の割り当てや管理手順、運用ルールを標準化し、情報の品質を改善する責務も負う。こうした活動は CSA 改正案に先立ち強化されている。

(b) 新たな「欧州サイバーセキュリティ認証フレームワーク (ECCF)」の構築

2019 年の CSA 導入以降、複雑な手続き及び法令遵守の整合性の不明瞭による個々の認証スキームの開発遅延や地政学的なサプライチェーン課題により、「欧州サイバーセキュリティ認証フレームワーク (ECCF: European Cybersecurity Certification Framework)」の実施が大幅に停滞していた^{*103}ことから、より機敏で実効性の高い認証制度を確立するために新たな ECCF の構築が提案された^{*104}。

新たな ECCF では、従来の ICT 製品、ICT サービス、ICT プロセスという枠組みに加え、マネージドセキュリティサービス (MSS: Managed Security Service) と、組織のサイバーセキュリティ態勢を客観的に評価、証明する「サイバーポスチャー (Cyber Posture)」が加えられた。これにより、個別の製品に加え、企業の運用体制の信頼性を証明することが可能になる。この新たな認証の枠組みが、NIS 2 指令等他の EU 法への準拠証明に利用されることにより、企業の監査負担や管理コストの軽減が期待される(「4.1.3 (5) (b) コンプライアンスの負担軽減と簡素化」参照)。

また、欧州委員会から ENISA への新しい認証制度

の開発の要請後原則 12 ヶ月以内の認証制度候補の提出、及び正式に法制化されるまでの承認プロセスの明確な期限が設定された。

(c) 信頼できる ICT サプライチェーンフレームワークの導入

CSA 改正案では、サイバーセキュリティ上の懸念がある第三国サプライヤーによる、ICT サプライチェーン・リスクを軽減する法的枠組みとして、新たに「Trusted ICT supply chain framework (信頼できる ICT サプライチェーンフレームワーク)」を導入するとしている。

EU は 5G ネットワークのサプライチェーン・リスクに対応するために「5G Toolbox」というリスク緩和策を運用してきた。しかし、加盟国間で実施状況にばらつきがあり、域内市場の断片化が課題となっていた。また近年では第三国の関与等による非技術的なリスクの顕在化もあり、技術やセクターを問わず EU 全域で適用されるフレームワークの確立が求められた。

同フレームワークでは、EU レベルの協調的なセキュリティリスク評価が義務化される。NIS 協力グループ (NIS Cooperation Group^{*109}) または欧州委員会がリスク評価を主導し、保護すべき重要 ICT 資産、及びサイバーセキュリティ上の懸念がある第三国を特定し、その国の管理下にある企業等を高リスクサプライヤーとして指定する仕組みが新設された。

これにより、EU の重要 ICT サプライチェーンから高リスクサプライヤーに指定された企業を排除することが可能になる。一方 EU 内の企業には、高リスクサプライヤーが提供する ICT コンポーネントの使用や統合の禁止、第三国へのデータ転送制限、マルチベンダー化、オンデバイス処理の採用やネットワークセグメンテーション等の技術的措置が義務付けられる。また、重大な脅威が存在し直ちに行動が必要な場合には、欧州委員会が例外的に迅速なリスク評価と介入を行う手順も整備される。

5G Toolbox からの主な変更点としては、自主的なガイドラインから、法的拘束力を持つ規制への転換がある。これにより、加盟国ごとの判断に委ねられていたリスク緩和措置が、EU 全体の共通義務となる。また、対象範囲の飛躍的な拡大も特筆すべき点であり、対象は 5G ネットワークにとどまらず、NIS 2 指令が定める高度に重要なセクターの ICT サプライチェーン全般、固定通信網や衛星通信網の重要資産にまで及ぶ。ほかにも、非技術的リスクを排除の直接的な根拠とすることや、排除措置の導入における経済的な影響評価や市場供給の継続

性、代替品の有無等の確認プロセスが同フレームワークに組み込まれている。

(5) NIS 2 指令の改正案

NIS 2 指令改正案^{*110} は、AI を悪用したサイバー攻撃の高度化や、地政学的リスクに伴う重要インフラへの脅威増大を背景に、既存の NIS 2 指令が抱える運用の複雑さを解消し、法的明確性を高めるために 2026 年 1 月に提案された。同改正案は、法的明確化及びコンプライアンスの仕組みを簡素化し、CSA 改正案による認証等の枠組みや手段の整備を支援し、より強固で一貫したサイバーセキュリティ体制の構築を目指している。以下では、同改正案の主な改正内容について述べる。

(a) 対象スコープの主な変更

同改正案の適用範囲をより明確化し、不釣り合いな負担を避けるための調整が行われる。対象スコープの主な変更は以下のとおりである。

- 電力セクター及び DNS プロバイダーの制限：
電力セクターにおいては、合計発電容量が 1 メガワットを超える電力生産者に対象を限定し、小規模な事業者に対する過度な管理負担を防止する。DNS プロバイダーについては、従来の無条件な適用に代わり一般的な企業規模の上限ルールが適用され、従業員数が 10 人未満であるマイクロ企業や 50 人未満である小規模企業は対象外となる。
- 航空運送及び化学セクターの明確化：
航空会社の管轄権は、運航免許を付与した加盟国に属することが明記された。また、ヘルスケア、水素、化学セクターの定義を明確にし、解釈の食い違いによる混乱を防止した。
- 新たな重要インフラの追加：
デジタル社会の基盤となる技術を提供する企業については、規模にかかわらず対象に含まれる。新たに追加される主要な重要インフラとしては、欧州デジタル ID ウォレット^{*111}・欧州ビジネスウォレット^{*112}、海底データ伝送インフラ、軍民両用インフラ等の提供者または運用者が追加される。

(b) コンプライアンスの負担軽減と簡素化

企業によるサイバーセキュリティ基準の準拠証明プロセスが合理化される。主な措置は以下のとおりである。

- ECCF の活用：
企業は、ECCF に基づく特定の認証スキーム (EUCC

等)を取得することで、NIS 2 指令が求めるリスク管理義務の一部または全部を遵守していると見なされる。認証を受けた項目については、各加盟国の管轄当局による追加的な監督措置や検査が原則として免除される。

- サプライチェーン評価の標準化:
異なる形式でのセキュリティ調査によるサプライヤーの負担を解消するために、欧州委員会は情報の詳細度、構造、形式に関する一貫性のあるセキュリティ評価ガイドラインを策定する。
- 「SMCs」カテゴリーの導入:
2025 年の欧州委員会勧告に基づき、新たに「小規模中堅企業 (SMCs: Small Mid-Caps)」という企業カテゴリーを導入する。これらの企業は、原則として重要エンティティとして指定されることにより、規模の大きい重大エンティティに比べて監督やコンプライアンス負担が緩和される。

(c) 報告義務と技術的要件の強化

主にランサム攻撃の報告義務と、深刻な脅威や将来の技術変化に対する要件が具体化・強化される。

- ランサム攻撃の報告標準化:
ランサム攻撃を検出した際、被害報告だけでなく、攻撃の侵入経路の特定、緩和策の実施状況、身代金の要求内容及び支払いの有無等の情報の共有が求められる。これらの情報は、規則の遵守により報告を行った当該企業に新たに法的責任が生じないように、加盟国の攻撃の実態把握と法的執行機関の捜査に役立てられる。
- PQC への移行:
量子コンピューターによる将来的な暗号解読の脅威に備え、加盟国は国家サイバーセキュリティ戦略の中に「ポスト量子暗号 (PQC) への移行ポリシー」を含めることが義務付けられる。

(d) 監督体制の強化

複数国にまたがり活動する企業に対する監督を効率化するため、ENISA の役割が拡大される。拡大される主な役割は以下のとおりである。

- ENISA による複数国にまたがる監督の支援:
複数の加盟国でサービスを提供する企業に対し、各国の規制当局による監督を効率化するため、複数国にまたがる事業主体に関する情報を集約した中央レジストリーを維持・管理する。また、ENISA は毎年、

複数国にまたがったリスク分析を実施し、重要度の高いリスクが特定された場合には、関係国の当局に対し共同検査チームの設置を勧告する。当局の要請があれば、ENISA は共同監督アクションに参加し、技術支援を提供する。

- 相互支援の効率化:
ある加盟国が別の加盟国に対して監督の支援を求めた場合、そのプロセスを ENISA が支援する。支援が行われた事実はベストプラクティスの共有や一貫した監督体制の構築に役立てられる。
- 最大限の調和:
リスク管理措置の具体的な技術的・方法論的要件について、欧州委員会が NIS 2 指令に基づく二次的な実施令を採択した場合、加盟国はそれ以上の独自要件を企業に課すことができなくなる。これにより、EU 全域で統一された基準が適用され、国ごとに異なるルールに対応する必要がなくなる。

(6) サイバーレジリエンス法

「サイバーレジリエンス法 (CRA: Cyber Resilience Act)^{*113}」は、デジタル要素を含む製品のセキュリティを強化し、消費者及び企業ユーザーをサイバー脅威から保護することを目的とした EU 規則である。同規則の対象は、ネットワークに接続可能なすべてのソフトウェア及びハードウェア製品に及ぶ。

CRA は製造業者に対し、企画から設計、開発、保守に至る、製品のライフサイクル全体に対する必須のセキュリティ要件の遵守を義務付けている。

サイバーセキュリティ上の重要度が高い製品については、EU 市場での販売前に専門機関による第三者評価を受けることも求められる。CRA の適合性評価の手段として EUCC (「4.1.3 (8) EUCC 枠組みの運用開始と改正」参照) 等の認証制度も活用する。要件を遵守している製品には、その適合性を示す CE マーク^{*114} が付与され、ユーザーはどの製品が適切なセキュリティ機能を備えているかを容易に識別できる。

CRA は 2024 年 12 月 10 日に施行され、2027 年 12 月 11 日から全面的に適用される予定である^{*115}。

製造業者が遵守すべき要件は主に以下のとおりである。

- 設計・開発段階のセキュリティ確保:
製品の設計段階からセキュリティ要件を組み込み、既知の脆弱性がない状態で出荷する。

- 脆弱性管理：

製品の想定される耐用期間、または少なくとも5年間にわたり、脆弱性を効果的に処理し、修正プログラムを提供し続ける。

- 透明性の確保：

ユーザーに対し、製品のセキュリティ機能やサポート期間に関する明確な情報を提供する。

全面適用に先立ち、製造業者等による脆弱性及びインシデントの報告義務について、2026年9月11日から先行して適用が開始される。製造業者は製品に関して「能動的に悪用されている脆弱性」及び「セキュリティに影響を及ぼす重大なインシデント^{*116}」を検知した場合、速やかに報告する必要がある。EU域外の製造業者がEU域内に製品を輸出する場合も同様の義務が課される。

これらの報告は、CSA改正案にてENISAに設置・運営を規定した単一窓口を通じて行われるよう整備が進められている。報告された脆弱性情報は、修正プログラムが利用可能になった後、製造業者の同意のもとEUVDに開示される。NIS 2指令の対象となる重大または重要エンティティや製造業者は、自社が使用する製品の脆弱性情報を適時に取得し、リスク管理に役立てることが可能となる。

(7) サイバー連帯法(CSoA)

デジタル技術の深化によるEU加盟諸国の経済相互依存、及び地政学的緊張の高まりの状況下において、サイバー脅威のEU全体への拡大が懸念されている。

「サイバー連帯法(CSoA: Cyber Solidarity Act)^{*117}」は、EU全体での重大かつ大規模なサイバー脅威及び攻撃に対する備え、検知、対応能力を強化するために2025年2月4日に施行された。以下では、CSoAに関連して実施された主な措置について取り上げる^{*118}。

(a) EU サイバーセキュリティリザーブの設立

CSoAの主な施策の一つとして、「EU サイバーセキュリティリザーブ(EU Cybersecurity Reserve)^{*119}」が設立された。これは、大規模なサイバー攻撃を受けた際、即座に展開可能な信頼できる民間プロバイダーの支援を確保するものである。

運営と管理はENISAが担当し、公共調達を通じて、信頼できる民間プロバイダーであるマネージドセキュリティサービスプロバイダー(MSSP: Managed Security Service Provider)と契約し、サービスの可用性を確保

する。

支援要請の主体は、EU加盟国、EU機関・団体、及び特定の条件を満たす「デジタル・ヨーロッパ・プログラム」関連の第三国であり、支援の対象は、NIS 2指令で規定されたヘルスケア、エネルギー等の重大エンティティの活動団体となる。提供されるサービスは、インシデントの直接対応、回復支援、インシデント予防に関わる準備支援を含む。

支援サービスの質を保証するため、ENISAはMSSに対する欧州サイバーセキュリティ認証制度の開発にも取り組んでおり、MSSPは制度導入後2年以内に自社のサービスについて認証を受けることが求められる予定である。

(b) 「サイバーブループリント」の更新

「サイバーブループリント(Cyber Blueprint)^{*120}」は、一連の対応責任者であるEU加盟国や調整を担う欧州理事会、運用を支援するEU-CyCLONe、脅威の検知や技術的な情報共有を担うCSIRTs等のEU関係者が危機管理ライフサイクル全体を通じて、どのように連携し利用可能な危機管理メカニズムを活用するかを説明した文書である。2025年2月24日、大規模サイバー危機の危機管理ライフサイクル全体における役割と責任を明確化・簡素化したサイバーブループリント更新案が公表され、同年6月6日に欧州理事会により採択された。

インシデント対応の主な責務は加盟国にあるが、国境を越える影響がある場合には、EU加盟国間での協力が不可欠となる。

同ブループリントは、危機管理ライフサイクル全体を通じて以下の三つのレベルでの連携を規定している。

- 技術レベル：

CSIRTsネットワークが中心となり、インシデントの分析や情報の共有、技術的な影響評価を行う。CERT-EUも重要な役割を果たす。

- 政治レベル：

欧州理事会が統合的政治危機対応の枠組みを使用し、戦略的な意思決定等を行う。

- 運用レベル：

危機管理プロセスの運用はEU-CyCLONeが担当し、技術レベルと政治レベルの橋渡しを行う。大規模インシデントの影響を評価し、緩和策を提案する。

また、同ブループリントでは民間セクターとの情報共有、軍事主体(MICNET(Military Computer Emergency

Response Teams Operational Network) 等) との連携、及び NATO 等の国際的なパートナーとの調整についてもガイドラインが示され、サイバー空間における軍民の境界を越えた危機管理体制が強化された。

(c) BlueOLEx 2025

2025 年 11 月 4 日、キプロスにおいて「BlueOLEx 2025^{*121}」が実施された。これは更新されたサイバースループプリントに基づき、危機の際の関係者の役割と責任を検証する初の演習で、ENISA の支援を受けてキプロス当局が主催した。

同演習には、加盟国のサイバー危機管理当局幹部や欧州委員会の関係者が参加し、重要セクターに影響を及ぼす大規模なサイバーインシデントシナリオが検証された。

シナリオの準備と運用は主に EU-CyCLONe が行い、EU と国家の危機管理手続きがどのように足並みを揃えて機能すべきかが演習の焦点となった。また、戦略的パートナーシップやインシデント対応手法の洗練、共有された状況把握の構築についても議論が行われた。

得られた教訓は、EU の広範な「準備連合戦略 (Preparedness Union Strategy)^{*122}」に反映される。同演習は、多元的かつ複数セクターにまたがる脅威の調整能力を高め、EU 市民のための安全なデジタル環境を維持するための実効的なステップとなった。

(8) EUCC 枠組みの運用開始と改正

ECCF の枠組みにおいて最初に採用された具体的な認証制度が、ICT 製品の共通基準である「EUCC (European Common Criteria-based cybersecurity certification scheme)」である (ECCF については「4.1.3 (4) (b) 新たな『欧州サイバーセキュリティ認証フレームワーク (ECCF)』の構築」参照)。

EUCC の実施規則^{*123} は 2024 年初頭に採択され、移行期間を経て 2025 年 2 月 27 日から本格的な運用が開始された。この間、従来の SOG-IS (Senior Officials Group Information Systems Security) による相互承認協定に基づく認証からの円滑な移行が進められている。

認証対象には IC カードや IC チップ、バイオメトリックシステム、ファイアウォール、ルーター・スイッチ、データダイオード、暗号化ストレージ・データベース等の製品群が含まれる。これらの製品に対し、セキュリティリスクに応じた保証レベルが設定される。CSA では、「基本 (basic)」「重要 (substantial)」「高度 (high)」の 3 段階のレベル

が定義されるが、EUCC は主に「重要」及び「高度」レベルに焦点を当てている。高い保証レベルの認証を得るためには、最先端のセキュリティテストが要求される。

EUCC の証明書はすべての EU 加盟国で認められるため、企業は加盟国ごとの認証を取得する必要がない。また製品購入者は共通の基準に基づいて製品のセキュリティ機能を理解できるようになる。

EUCC は運用開始後も、技術の進展や法規制の変化に対応するため、段階的な改正が行われている。2024 年に採択された第一次改正^{*124} は、主に軽微な文言修正や運用の整合性確保であったが、2025 年 12 月 8 日に採択された第二次改正^{*125} は、実務的な効率化と維持管理の強化を目的とした重要な変更を含んでいる。

第二次改正では、定義の見直しに加え、特に以下の 3 点について新たな規定が導入された。

- ICT 製品シリーズ認証：
個別の製品単位の認証に代わり、同一の設計思想や共通のセキュリティ機能を有する製品群をシリーズとしてまとめ、一つの認証でカバーすることが可能になった。
- 保証継続性：
認証取得後の製品に軽微な変更や修正プログラム適用が行われた際、評価をやり直すのではなく、既存の認証を維持しながら変更を管理するプロセスが明確化された。
- 最新技術文書に関する規定：
サイバー脅威の変化に対応するため、評価基準となる技術文書を常に最新の状態に保つメカニズムが強化された。

欧州サイバーセキュリティ認証に関する「EU ローリング・ワークプログラム (URWP: Union Rolling Work Programme)^{*126}」に基づき、MSS、ID ウォレット等の分野における新しい認証制度 (「4.1.3 (4) (b) 新たな『欧州サイバーセキュリティ認証フレームワーク (ECCF)』の構築」参照) の導入や検討が進められており、EUCC は今後も改正が行われる予定である。

4.1.4 中国の政策

中華人民共和国 (以下、中国) では、2021 年から 2025 年までを対象期間とする「第 14 次 5 年計画」のもと、サイバーセキュリティ、データ安全及び個人情報保護に関する制度整備が進められてきた。これらの制度は、ネットワークの保護に加え、デジタル経済の発展や国家

安全保障とも関係する政策領域として位置付けられている。本項では、中国のサイバーセキュリティに関する計画、法律、行政法規及び関連規則等について概説する。

(1) 中国におけるサイバーセキュリティ政策の位置付け

中国のサイバーセキュリティ政策は、単にネットワークの保護のみを対象とするものではない。デジタル経済政策、データ安全、個人情報保護、重要情報インフラ保護等を含む、広範な政策領域として展開されている。「第14次5ヵ年計画」及び「第14次5ヵ年デジタル経済発展計画」では、デジタル中国建設、ネットワーク強国建設、データ要素の活用、発展と安全の両立を基本方針として掲げており^{*127}、中国のサイバー・データ関連制度が、経済発展と安全保障の双方を政策目的としていることがうかがえる。

法制度面では、2015年の「中華人民共和国国家安全法^{*128}」が「ネットワーク・情報安全保障体系」の構築を国家安全上の任務として位置付けたほか、2015年の「中華人民共和国反テロリズム法」、2017年の「中華人民共和国国家情報法」、2019年の「中華人民共和国暗号法」も、それぞれ、電信・インターネット事業者等の本人確認・技術支援義務^{*129}、組織・公民の国家情報活動への援助・協力義務^{*130}、暗号の分類管理^{*131}を制度化している。2017年施行の「中華人民共和国サイバーセキュリティ法^{*132}」（以下、中国サイバーセキュリティ法）に加え、2021年に「中華人民共和国データ安全法^{*133}」（以下、中国データ安全法）及び「中華人民共和国個人情報保護法^{*134}」（以下、中国個人情報保護法）が施行され、ネットワーク安全、データ安全、個人情報保護を支える基本的な枠組みが整えられた。以下、これら三つの法律を便宜上「データ三法」と総称する^{*135}。更に、「重要情報インフラ安全保護条例」及び「等級保護制度（ネットワーク安全等級保護制度）」が、重要分野の保護責任と情報システム管理の実務上の基盤を構成している^{*136}。

こうした中国の経済安全保障・データ保護法制について、独立行政法人日本貿易振興機構（JETRO: Japan External Trade Organization）は、中国の経済安全保障関連制度を、サイバー、データ、重要インフラ、対外規制が相互に結び付く体系として整理している^{*137}。また国際法律事務所 DLA Piper も、中国のデータ保護法制を、複数の法令が重層的に構成する制度領域として説明している^{*138}。

こうした制度的背景を踏まえると、2025年は、既存制度の具体的な運用の進展を示す動きが相次いだ年であった^{*139}。これらの動向を見ると、2025年は、「第14次5ヵ年計画期」に整備された制度を実務運用へと移行させるとともに、次期の「第15次5ヵ年計画期」を見据えた運用基盤の整備が進んだ時期として位置付けることができる。

(2) ネットワークデータ安全管理条例

2025年における中国のデータ制度運用を把握する上で、その中核に位置付けられる行政法規が「ネットワークデータ安全管理条例」である。同条例は2024年9月に公表され、2025年1月1日に施行された。条文上は、データ三法等が上位法（根拠法）として明示されており、ネットワークデータ処理活動の規範化、ネットワークデータ安全の確保、データの適法かつ有効な利用の促進、国家安全、公共利益、個人・組織の適法な権益の保護を目的としている^{*140}。

同条例の意義は、ネットワークデータ処理に関する具体的ルールを、データ三法を前提として定めた点にある。中国サイバーセキュリティ法は主にネットワーク運営者及び重要情報インフラの保護を、中国データ安全法はデータ分類・分級管理や重要データ保護を、中国個人情報保護法は個人情報処理及び越境移転の規律をそれぞれ定めている。これらを踏まえ、JETROや欧米主要法律事務所による実務解説では、同条例はこれらの規律を企業のネットワークデータ処理実務に即して具体化する制度として整理されている^{*141}。

そのため、中国に拠点や現地法人を有する企業においては、顧客情報、従業員情報、取引情報、製造・物流データ等の管理体制を、法務、情報システム、コンプライアンスの各観点から改めて点検することが求められる。特に、中国国内で収集・生成されたデータの取り扱い、データ処理の委託先管理、データ分類・分級の社内運用の構築、更にはデータ越境移転（出境）の有無の確認及び必要性の判断を、相互に関連する実務課題としてとらえる必要がある。企業がこれらを網羅的なガバナンス体制として再構築することが迫られる点に、同条例の極めて高い実務的影響力がある^{*142}。

(3) 個人情報保護コンプライアンス監査管理弁法

個人情報保護分野では、2025年2月に「個人情報保護コンプライアンス監査管理弁法」が公布され、同年5月1日に施行された。同弁法は、中国個人情報保護

法が定める個人情報の取り扱いに関するルール、影響評価、内部管理体制等について、それらが継続的に遵守・実施されているかを点検する監査の枠組みを具体化したものである^{*143}。

この制度整備により、中国の個人情報保護制度において、取得時の同意管理だけで完結するのではなく、記録管理、内部統制、監査、説明責任を含む継続的な運用管理を企業に求める方向性が、より明確になったととらえることができる。国際法律事務所 Mayer Brown の解説でも、同制度は、コンプライアンス監査を通じて組織的なガバナンスを強化するための重要な措置として位置付けられている^{*144}。

従って、中国国内において従業員情報や顧客情報を継続的に取り扱う企業にとっては、データ処理記録の作成、委託先管理、保存期間の適正管理、個人情報保護影響評価の実施、監査体制の整備が、形式的対応ではなく、日常的な管理実務として求められる。中国における個人情報保護は、単独の「プライバシー対応」にとどまるのではなく、データ管理全体の内部統制と密接に結び付いた経営課題として理解する必要がある^{*144}。

(4) 国家ネットワーク安全事件報告管理弁法

インシデント対応の分野では、「国家ネットワーク安全事件報告管理弁法^{*145}」が2025年9月に公表され、同年11月1日に施行された。同弁法は、中国サイバーセキュリティ法や「重要情報インフラ安全保護条例」等を上位法として、インシデント(事件)報告義務を具体化し、適用範囲、報告主体、報告手順、報告期限、報告内容等を明確に定めた制度である。

同弁法の実務的な意義は、平時における安全管理体制の構築にとどまらず、インシデント発生後の初動対応と当局への報告についても、制度として具体化した点にある。付属文書である「ネットワーク安全事件分級ガイド」は、事件の重大性(深刻度)を判定するための具体的な客観的基準を示しており、報告対象となる事象を把握し、社内で判断する際の前提となる^{*146}。

国際法律事務所 Morgan Lewis の実務解説では、この制度は、企業に対して統一的なサイバーセキュリティインシデント報告の枠組みを課すものとして整理されている。従って、中国拠点でインシデントが発生した場合には、中国国内法上の報告義務の有無、報告先、報告内容、報告期限等を確認する必要がある。中国で事業を行う企業にとっては、技術面の対応と法令面の対応を切り離さず、平時から連動させて準備しておくことが重要であ

る^{*146}。

(5) AI 生成合成コンテンツラベル弁法

人工知能(AI)分野では、2025年3月に「AI生成合成コンテンツラベル弁法」が公布され、同年9月1日に施行された。同弁法は、AIによって生成・合成されたコンテンツに対する識別表示(ラベル付け)のルールを定め、一般利用者がAI生成物を容易に識別できるようにすることで、社会的な誤認の防止や健全な情報流通の管理を図る^{*147}。この制度導入に関しては、国家インターネット情報弁公室(CAC: Cyberspace Administration of China)が2025年4月に公表した「清朗・整治AI技術濫用」特別行動を併せて参照する必要がある^{*148}。AIを用いた虚偽情報、不实情報、なりすまし、ネット世論操作等への重点的な取り締まりを進めるとともに、関連規定に該当するネットワーク情報サービス提供者に対して、AI生成・合成されたコンテンツかどうかテストし、真正性を確認する能力、及びAI生成・合成コンテンツの審査体制の強化を求める流れが見られた。もともと、同弁法第9条は、提供対象情報等の関連ログを6ヵ月以上保存する等、一定の条件のもとで、識別表示を付さない生成・合成コンテンツの提供を認めており、表示義務の実効性には一定の留保があると考えられる。

また、関連規格として、強制国家標準「GB 45438-2025」が策定されており^{*149}、法令と技術標準が結び付いた形で運用が進められている^{*147}。この制度の実務上の特徴は、表示義務に加え、識別表示の具体的な付与方法が技術標準と一体化して運用されている点にある^{*150}。

国際通信社 Reuters は、この制度を、中国当局がAI生成コンテンツのラベリング要件を導入したものととして報じている^{*151}。また、国際法律事務所 Loeb & Loeb による解説では、明示的な表示、メタデータ上の暗黙的な表示、国家標準との関係を含め、企業実務への影響が整理されている^{*150}。従って、中国市場向けにAIを活用したサービス提供、広告展開、あるいはSNSの運用等を行う企業にとっては、識別表示の付与、適切な表示方法の選定、関連標準を踏まえた実装対応が実務上の重要な論点となる。

(6) データ出境安全管理政策問答

データの越境移転(出境)については、2025年にCACが「データ出境安全管理政策問答」を複数回にわたり公表し、取り扱うデータが「重要データ」に該当する

可否かの判断基準、個人情報の越境移転に関する標準契約(標準合同)の再締結義務、あるいは日常的な従業員情報の管理や海外へのサービス提供の場面における越境移転の手続き等、実務上問題となりやすい論点が整理された^{*152}。これらの政策問答は法令そのものではないものの、既存のデータ越境移転制度を具体的に適用・執行する際の対応を理解する上で重要な運用資料となっている^{*153}。

法律事務所 Grandway Law Offices やビジネスメディア China Briefing による解説においても、これらの政策問答は、データ安全評価、標準契約、個人情報保護認証等といった各種手続きに関する実務的な理解を補う資料として整理されている。従って、2025 年の越境移転政策においては、既存制度の適用関係の明確化や、煩雑な行政手続きの具体的な運用及び適正化を図る方向で実務が進展した^{*153}。そして、2025 年 10 月には「個人情報出境認証弁法」が公布され、2026 年 1 月 1 日に施行されているため^{*154}、2025 年の越境移転政策全体としては、新たな制度整備も進められたということになる。

(7) 中国サイバーセキュリティ法改正

2025 年 10 月には、全国人民代表大会(全人代)常務委員会による中国サイバーセキュリティ法の改正決定が採択され、2026 年 1 月 1 日に施行された。改正後の法文は、国家法律法規データベースにおいて公開されている^{*155}。

今回の改正では、党の指導、総体国家安全観、AI 関連条項、中国個人情報保護法との接続の明確化及び罰則体系の変更が盛り込まれた^{*156}。これにより、既存の中国サイバーセキュリティ法について、中国データ安全法、中国個人情報保護法等、近年整備が進んだ関連法制との整合を図るものととどまらず、ネットワーク安全規制の内容を拡充・強化するものと理解できる。欧米の主要法律事務所やビジネスメディアの実務解説においても、同改正は、データ関連法制や AI 規制との整合、企業に求められるコンプライアンス義務の明確化・強化、罰則体系の見直しを含む重要な節目として位置付けられている^{*157}。

従って、この改正は、2025 年に見られた既存制度間の関係の整理と運用の具体化を示す重要な動きの一つといえる。すなわち、新たな基本法制を大きく追加するというよりも、これまでに整備された複数の法体系を相互につなぎ合わせ、その適用関係をより明確にする方向で制度整備が進められたものと評価できる。

その一方で、個別分野では、2025 年 6 月に施行された顔認識技術応用安全管理弁法^{*158}、同年 7 月に施行された国家ネットワーク身分認証公共サービス管理弁法等^{*159}、新たな実施規則の整備も進展した。

4.1.5 アジア太平洋地域での CSIRT の動向

アジア太平洋地域の多くの国では、各国のインシデント対応連携の窓口となる National CSIRT(本項では CSIRT と記す)が既に設立され、運用されている。これらの CSIRT(Computer Security Incident Response Team)は、自国内の関係組織や他国のカウンターパートと連携し、サイバー攻撃による被害拡大を防ぐための対策情報の共有や、被害を受けた後の復旧支援等、インシデント対応や情報共有に日々取り組んでいる。また、インシデント対応をより迅速かつ円滑に進めるため、サイバーセキュリティ戦略や法令で CSIRT 及び所管省庁の役割や権限を明文化し、重要インフラ事業者に対してはインシデント報告を義務化する等、制度や運用枠組みの整備を進める動きも継続して見られる。

本項では、主に 2025 年度を中心としたアジア太平洋地域における CSIRT の機能強化やインシデント対応の取り組み、CSIRT 間の相互連携の実態について述べる。

(1) CSIRT の機能強化の動き

アジア太平洋地域における各国・地域の CSIRT の機能強化やインシデント対応への取り組みについて述べる。

(a) オーストラリア

2025 年 5 月 30 日、ランサム攻撃等のサイバー攻撃を背景に、情報の公開やシステム停止等を示唆した恐喝的要求に応じて行った支払いについて、「2024 年サイバーセキュリティ法(Cyber Security Act 2024)」に基づき政府への報告が義務付けられた^{*160}。オーストラリア内務省(Australian Government Department of Home Affairs)は、同報告制度の施行にあたって要点を整理したファクトシートを公開している^{*161}。

同制度で報告の義務が課されるのは、オーストラリアで年間売上 300 万豪ドル(3 億 4,200 万円^{*162})以上の事業を営む事業者及び重要インフラ事業者である。対象事業者は、恐喝者への支払いを行った場合または企業グループ内の他の事業者等の第三者が代理で支払いを行ったことを認識した場合、72 時間以内に報告を行う必要がある。報告は、オーストラリア通信情報局(ASD:

Australian Signals Directorate) 傘下で CSIRT の機能を担うオーストラリアサイバーセキュリティセンター (ACSC: Australian Cyber Security Centre) が運営する Web サイト上のフォームを通じて行う。報告内容には、支払いを行った事業者の連絡先及び事業情報に加え、インシデントの概要、恐喝者からの要求内容及び支払い内容、恐喝者との交渉の経緯等の情報を含める必要がある。報告が必要な「支払い」行為には、金銭に加え、サービスやデータ提供等の利益供与も含まれる。なお、報告義務に違反した場合には、制裁金として 60 ペナルティユニットが科される可能性がある。ペナルティユニットとは、罰金額を算定するための標準単位であり、連邦法における 1 ユニットあたりの金額は、2026 年 5 月時点で 330 豪ドル (3 万 7,620 円) と定められている^{*163}。

政府は、届けられた報告情報を攻撃主体の特定や使用されているマルウェア及び連絡手段等の情報収集、標的となっている業種や経済への影響の把握に活用するとしている。また、企業に対する具体的なサイバーセキュリティ対策の助言や、ランサム攻撃に関する問題に対処するための今後の立法及び各種プログラムの検討にも役立てるとしている。制度の運用は段階的に進められており、2025 年中は教育・周知を重視した運用を行い、2026 年以降に本格的な規制の執行を開始する方針が示され実行されている。

なお、重要インフラ事業者については、同制度とは別に、「2018 年重要インフラ保護法 (Security of Critical Infrastructure Act 2018)」に基づき、インシデント発生時の報告義務も課されている。そのため、該当事業者はインシデント報告と恐喝に対する支払い報告の双方への対応が求められる。

(b) スリランカ

Sri Lanka CERT|CC (Sri Lanka Computer Emergency Readiness Team | Coordination Centre: スリランカコンピュータ緊急対応チーム調整センター) が、デジタル経済省の支援及び世界銀行の協力を得て「国家サイバーセキュリティ戦略 2025-2029 (National Cyber Security Strategy of Sri Lanka 2025-2029^{*164})」を策定し、2025 年 7 月 22 日に内閣承認を得た。同戦略は、2019 年から 2023 年に実施された国家サイバーセキュリティ戦略の成果と教訓並びに国民のサイバーセキュリティ対策に対する意識の低さや熟練したサイバーセキュリティ専門家の不足、脅威に対応するための政府機関の体制整備の遅れ、包括的なガバナンス体制・規制枠

組みの不備等の課題を踏まえて策定された。これらの課題を解決するため、同戦略では今後 5 年間、次の四つの分野に重点的に取り組むとしている。

① 法的な規制枠組みの強化

サイバーセキュリティ監督機関の設立、国家サイバーセキュリティ戦略の実施計画の策定、重要情報インフラ保護のための法的規定の強化、サイバー犯罪の法的枠組みの強化、新興技術に対応したセキュリティ対策に関する政策の策定等

② 知識・意識の向上

多様な社会のニーズに応える包括的な意識啓発活動及び教育カリキュラムの強化、政府・民間を支える専門家人材の育成・確保・多様化の推進等

③ 備えと対応能力の強化

危機管理計画の策定、インシデント報告・対応体制の整備、政府機関の技術能力向上、重要情報インフラ保護の強化、インシデント対応・復旧能力の強化等

④ 連携の強化

APCERT (Asia Pacific Computer Emergency Response Team: アジア太平洋コンピューター緊急対応チーム)^{*165} や FIRST (Forum of Incident Response and Security Teams)^{*166} 等の国際的コミュニティ・団体への参加を通じた情報連携・協力の推進、他国 CSIRT との能力構築に関する協力推進、国内の産業界・学術機関との官民パートナーシップの構築、セクター別のサイバーセキュリティ対応能力向上支援等

同戦略は、「①法的な規制枠組みの強化」及び「③備えと対応能力の強化」の取り組みに関連して、今後中核的な役割を担う二つの新たな機関の整備計画を掲げている。一つは、戦略公開時点で審議中であったサイバーセキュリティ法に基づく「サイバーセキュリティ機関 (CSA: Cyber Security Authority)」の設立である。同機関は、国家のサイバーセキュリティ政策や規則の策定・施行において中心的な役割を果たすとされている。もう一つは、政府システムの管理・監視を担当する「国家サイバーセキュリティオペレーションセンター (NCSOC: National Cyber Security Operations Center)」の設立及び機能拡張である。同センターは 2025 年 9 月に開設され、運用が開始されており、今後は監視・管理対象を重要情報インフラ運営者及びその他の機関にまで拡大する方針を示している。CSA の設立により、NCSOC 及び Sri Lanka CERT|CC と連携し、国のサイバーセ

セキュリティインシデント管理と状況監督を一元的に担う体制が確立されるとしている。

Sri Lanka CERT|CC については、引き続きインシデント対応の調整において中心的役割を担う組織として位置付けられている。同組織は、これまでも脅威情報の共有や、政府及び民間への技術的助言等を担ってきた実績を持ち、新戦略のもとでは、ペネトレーションテストや、リスク評価、脆弱性評価等の技術的機能を更に強化していく方針が示されている。

スリランカ政府は、同戦略に基づき国家のサイバーセキュリティの基盤を整えることで、安全で信頼性の高い包括的なデジタルエコシステムの実現を目指すとしている。

(c)トンガ

2025 年 11 月、国家のサイバーセキュリティ対応能力の強化を目的とする「Cybersecurity Act 2025^{*167}」が施行された。主な内容として、サイバーセキュリティに関する政策・運用体制の整備や、CERT (Computer Emergency Response Team) の機能及び役割、重要インフラ事業者の義務等について定められている。

具体的には、サイバーセキュリティ政策・規制を担う CPR 大臣 (Minister CPR: Minister responsible for cybersecurity policy and regulation) と、現場運用を担う CO 大臣 (Minister CO: Minister responsible for cybersecurity operations) という二つの役職が設けられ、それぞれの所掌に応じて監督・管理を行うことが定められている。CPR 大臣は、主に政策立案、指針の策定、義務違反が認められた組織への是正命令の発出、国際協力等に関する権限を有する。また、重要インフラ事業者や法執行機関が情報を共有する場となる「サイバーセキュリティ諮問委員会」の議長を CPR 大臣が務めることが定められている。CO 大臣の具体的な役割については明示されているが、同時にその運用権限や機能を CERT に委任するものと定められている。

同法において CERT は、サイバーセキュリティ脅威の検出・情報共有、インシデントの監視及び早期警戒情報の発信、インシデント報告の受付等を担う中核的組織として位置付けられている。更に、法執行機関へのインシデントの分析及び捜査の支援、政府省庁のサイバーセキュリティ対策支援、市民への意識啓発・教育プログラムの実施、国内外の CERT との連携等、多岐にわたる役割を担う。また、必要に応じて CPR 大臣に対し重要インフラ事業者への是正措置を提案する権限も付与されている。トンガには、既に CERT Tonga が存在し、

条文の中では具体的な組織名は挙げられていないものの、同組織がこれらの役割を担うと見られる。

重要インフラ保護に関しては、指定事業者に対し、定期的なサイバーセキュリティ評価の実施及び結果の提出、インシデント認知後 24 時間以内の CERT への報告、脅威対応に関する方針・手順の策定等を義務付けている。これらに違反した個人には 50 万パアンガドル (3,400 万円^{*168})、法人には 100 万パアンガドル (6,800 万円) までの制裁金が科される可能性があると定められている。

(d)シンガポール

2025 年 10 月、「シンガポール国際サイバーウィーク 2025 (Singapore International Cyber Week 2025)」において、中小企業のサイバーセキュリティ対策を支援するサイバーレジリエンスセンター (CRC: Cyber Resilience Centre) を設置する計画が発表された。同計画の詳細については、シンガポールサイバーセキュリティ庁 (CSA: Cyber Security Agency of Singapore) がプレスリリースを公開している^{*169}。CSA は、シンガポールの CSIRT である SingCERT (Singapore Cyber Emergency Response Team: シンガポールサイバー緊急対応チーム) を管轄している。

同センターは、中小企業のサイバーセキュリティに関する意識向上、インシデント対応への備え、回復力 (レジリエンス) の強化、官民連携を促進する中核拠点として機能し、インシデント発生時には復旧支援も提供するとしている。運営は、CSA の支援のもと、シンガポールビジネス連盟 (SBF: Singapore Business Federation) が担う。また、シンガポール中華総商会 (SCCCI: Singapore Chinese Chamber of Commerce and Industry)、SGTech 等の業界団体とも連携して運用される予定である。

同センターの主な活動としては、インシデント対応ホットラインの開設・運用に加え、中小企業のサイバーセキュリティ体制の評価・診断等を行う「サイバーセキュリティ・ヘルスクリニック」の提供、CSA の「CISO as-a-Service」プログラムを通じたサイバーセキュリティ対策強化の支援、インシデント対応及び復旧のノウハウの習得を目的とした中小企業向けサイバー演習等が含まれる。CRC は SBF の施設内に設置され、2026 年中に稼働を開始する予定である。

(2) アジア太平洋地域の CSIRT 間連携

アジア太平洋地域全体の CSIRT からなるコミュニティ

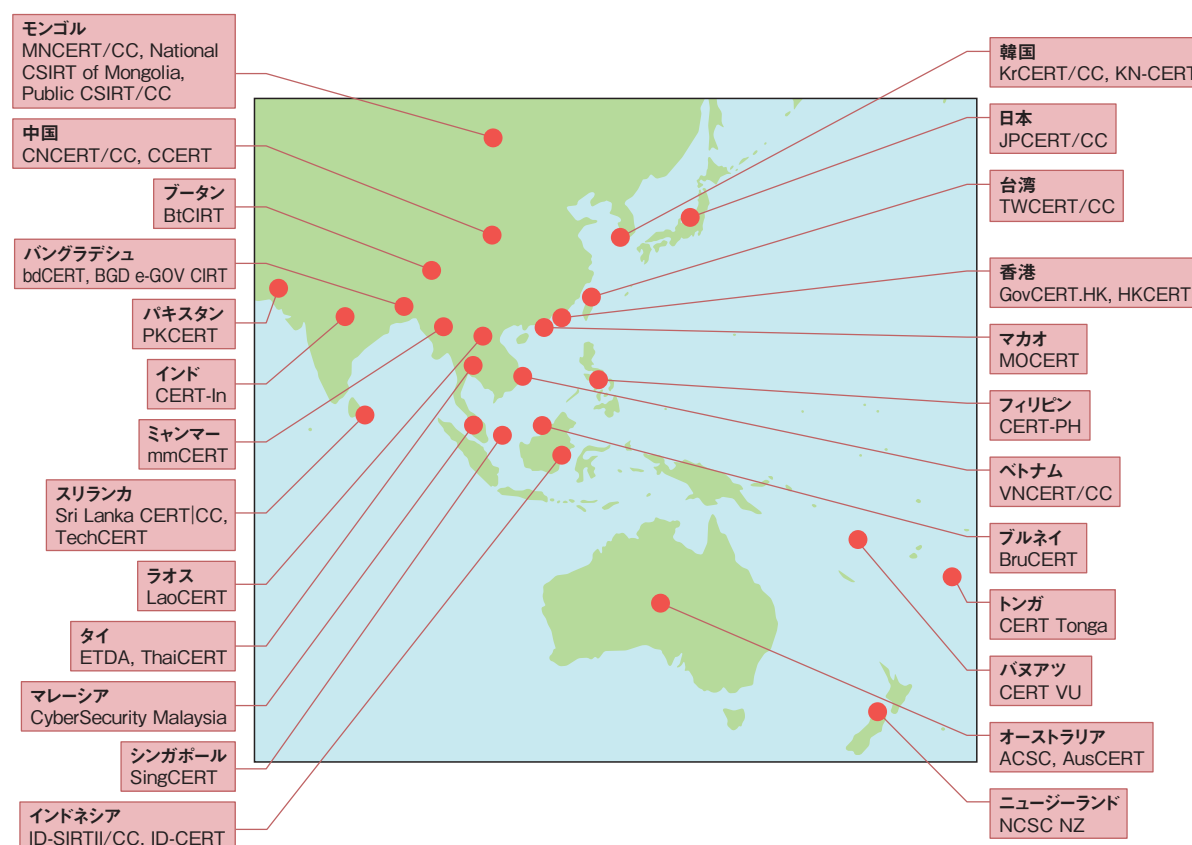
として、APCERT があり、地域内で発生したインシデント対応における連携の円滑化や、サイバー脅威等に関する情報共有・技術交流の推進を目的に活動している。2003 年の設立当初、参加メンバーは 12 の国・経済地域の 15 チームだったが、地域内で CSIRT の立ち上げが進んだことや、CSIRT コミュニティへの参加を通じた情報共有等の重要性が高まっていることから年々メンバーが増えている。2026 年 5 月末現在、25 の国・経済地域の 35 チームが、APCERT の活動に参加するオペレーショナルメンバーとなっている(図 4-1-2)。

JPCERT/CC は、2003 年の APCERT 設立当初から事務局を務め、運営委員会の一員として組織運営を支えている。APCERT の主な活動は、年次サイバー演習の実施、年次報告書の発行及び年次会合の開催である。

2025 年のサイバー演習は、「When Ransomware Meets Generative AI(ランサムウェアと生成型 AI の融合)」をテーマに実施された^{*171}。同演習には、APCERT のオペレーショナルメンバーのうち合計 18 の国・経済地域から 24 チームが参加した。年次報告書は、APCERT 全体の活動に加えて各チームの組織概要や、対応した

インシデント統計等をまとめた文書で、Web サイトで公開されている^{*172}。2025 年の APCERT 年次会合は、11 月にオーストラリアのシドニーで開催された。会合では、オーストラリアの ACSC^{*173} が議長に、韓国の KrCERT/CC^{*174} が副議長に選出された。また、JPCERT/CC が事務局に、マレーシアの CyberSecurity Malaysia^{*175}、スリランカの Sri Lanka CERT|CC^{*176}、JPCERT/CC が運営委員にそれぞれ再選された。APCERT では能力開発の取り組みとして、インシデント対応に関するノウハウを教えるオンライントレーニングを 2014 年以来継続的に実施している。こうしたオンラインで連携する取り組みを継続することで、加盟組織間の交流を深めている。

そのほか、アジア太平洋地域における CSIRT 間連携については、シンガポール主催による「ASEAN CERT インシデント演習 (ACID: ASEAN CERT Incident Drill)」が毎年開催されており、同地域におけるサイバーセキュリティ対応能力及び関係機関間の連携強化が図られている。2025 年の演習は、第 20 回の開催を記念し、10 月にシンガポールの ASCCE (ASEAN-Singapore Cybersecurity Centre of Excellence) において初めて対面形式で開催された^{*177}。演習には、ASEAN 加



■図 4-1-2 APCERT オペレーショナルメンバー(2026 年 5 月末現在)
(出典)APCERT「Member Teams^{*170}」を基に IPA が編集

盟国に加え、シンガポールが招待した日本、韓国、東ティモール、インド、オーストラリア等の CSIRT のインシデント対応担当者が参加した。なお、一部の参加者はリモートで参加した。演習では、国境を越えたサイバーインシデントへの対応を目的とした机上演習や、高度標的型攻撃に対する防御強化に関するワークショップが実施された。また、「ネットワークエッジデバイスのセキュリティ確保」をテーマに、サイバー攻撃からこれらの機器を保護するための実践的な防御技術が紹介された。

このように、APCERT や ASEAN 等の地域横断的な団体が、CSIRT の能力強化や CSIRT 間の連携促進に向けた取り組みを継続して進めている。国境を越えたサイバーインシデントへの対応を効果的に進めるためには、CSIRT 間の国際連携が重要であり、ここに挙げたような活動を通じてアジア太平洋地域の CSIRT 全体の対応能力向上や相互連携の深化につながることを期待される。

4.2 国際標準化活動

国際標準とは、製品や技術を、国境を越えて利用するために制定される国際的な共通規格であり、国際規格とも呼ばれる。本節では、日本の標準化活動への取り組み、及び国際標準化の動向として ISO、IEC のセキュリティ分野の活動を紹介する。

4.2.1 様々な標準化団体の活動

作成プロセスや作成組織の違いから見た標準の分類、及びセキュリティに関連する分野の主な標準化団体の概要を示す。

(1) 標準の分類

国際標準には、公的な標準化団体により所定の手続きを経て作成される「デジュール標準 (de jure standard)」、いくつかの企業や団体等が協力して自主的に作成する「フォーラム標準 (forum standard)」、公的な標準化団体を介さず、市場や業界において広く採用された結果として事実上標準化される「デファクト標準 (de facto standard)」がある。

デジュール標準では、幅広くステークホルダーを集めて議論をととして合意形成を行う。次項で紹介する ISO、IEC、ITU が作成する国際規格や JIS (Japanese Industrial Standards: 日本産業規格) 等の国家規格が該当し、策定プロセスが規定されており、様々な規制等に用いられることも多い。合意形成のために複数の検討段階が設定されており、正式に発行するまでに時間がかかる (ISO/IEC の場合は約 3 年)。

フォーラム標準は業界団体等、共通の関心を持つ企業等が集まって議論し、業界ルール等限定的な範囲で合意される標準である。作成スピードは速く、業界の特性が反映されていることから該当する業界内では利用が促進されやすい。次項で紹介する IEEE、IETF、TCG が発行する標準が該当する。コンソーシアム標準と呼ばれることもある。業界のフォーラム標準が、その後、国際標準化団体に提案され、時間をかけてデジュール標準となる場合もある。

電気製品や IT 製品等、開発サイクルの短い分野では、その時点の市場で一般的な規格としてデファクト標準が採用される傾向にある。

(2) 情報セキュリティ分野に関する標準化団体

情報セキュリティに関連するデジュール標準やフォーラム標準の策定を行っている主な国際標準化団体を以下に示す。

- ISO (International Organization for Standardization: 国際標準化機構) / IEC (International Electrotechnical Commission: 国際電気標準会議) JTC 1 (Joint Technical Committee 1: 第一合同技術委員会)^{*178}:

情報セキュリティを含む情報技術の国際規格を策定している。コンピューターや情報分野を扱う国際標準化団体として ISO、IEC はそれぞれ独立に存在しているが、扱う領域の競合を避けるために双方が連携し、JTC 1 が設立された。日本国内の標準化団体としては、日本産業標準調査会 (JISC: Japanese Industrial Standards Committee) が ISO、IEC 双方のメンバーであり、JTC 1 でも活動している^{*179}。

- ITU-T (International Telecommunication Union Telecommunication Standardization Sector: 国際電気通信連合 電気通信標準化部門):
電気通信技術に関わる国際規格を策定している。情報セキュリティに関しては SG (Study Group) 17 が設置され^{*180}、ISO や後述する IETF とともにネットワークや ID 管理等に関する標準化活動を行っている。策定した標準は ITU 勧告として定められる。

また、情報セキュリティ分野に関するフォーラム標準を策定する代表的な組織として、以下がある。

- IEEE (The Institute of Electrical and Electronics Engineers, Inc.):
電気工学・電子工学技術に関する国際学会である。標準化活動は内部組織である IEEE-SA (Standards Association) が行っている。情報セキュリティについては、サイバーセキュリティ、ネットワークセキュリティ、IoT セキュリティ等の広範な領域で標準化を行っている。
- IETF (Internet Engineering Task Force):
インターネット技術の国際標準化を行う任意団体である。非常にオープンな組織であり、作業部会のメンバーリストに登録することで誰でも議論に参加できる。情報セキュリティについては、インターネット上のセキュアなプロトコル、暗号、署名、認証、セキュリティ情

報連携（セキュリティオートメーション）等の方式の標準化を行っている^{*181}。標準化した技術文書はRFC（Request For Comments）として参照できる。

• TCG（Trusted Computing Group）：

信頼できるコンピューティング環境（埋め込み機器、パソコン／サーバー、ネットワーク等）に関するセキュリティ技術の標準化を行う業界団体である。ハードウェア、ソフトウェア等のベンダーやシステムインテグレーターがメンバーとなり、中国、日本にRegional Forum（地域支部）がある^{*182}。

4.2.2 情報セキュリティ、サイバーセキュリティ、プライバシー保護関係の規格の標準化（ISO/IEC JTC 1/SC 27）

ISO/IEC JTC 1/SC 27^{*183}（以下、SC 27）は、ISO及びIECの合同専門委員会（ISO/IEC JTC 1）において、情報セキュリティに関する国際標準化を行う分科委員会（SC）である。SC 27は、テーマ別に以下の五つの作業グループ（WG）で構成される。

WG 1：情報セキュリティマネジメントシステム

WG 2：暗号とセキュリティメカニズム

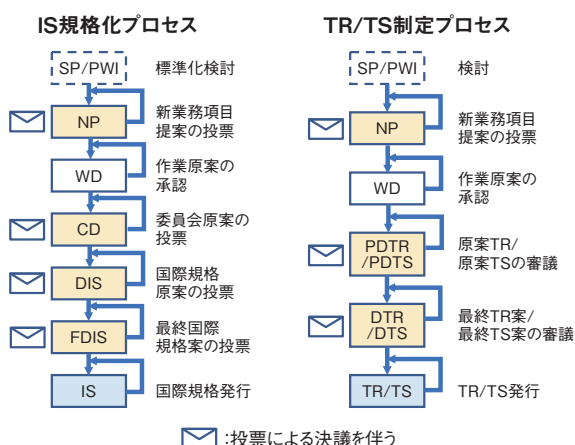
WG 3：セキュリティの評価・試験・仕様

WG 4：セキュリティコントロールとサービス

WG 5：アイデンティティ管理とプライバシー技術

ISO/IECにおける標準化作業は、策定する仕様の完成度によって図4-2-1のような段階があり、それぞれ各国の投票によって次の段階へ進む。なお、ISOにおいて、技術が未成熟である、またはガイダンス等の標準仕様ではないが重要であるとされたものは、技術報告書または技術仕様書として発行される。

図4-2-1の各文書の段階と略号は以下のとおりである。



■ 図4-2-1 ISO/IEC JTC 1/SC 27における規格作成の段階
（出典）JISC「ISO/IEC 規格の開発手順^{*184}」を基にIPAが作成

SP：研究期間（Study Period）

PWI：予備業務項目（Preliminary Work Item）

※SPとPWIのどちらを実施するかはWGによって異なる。

NP：新業務項目提案（New work item Proposal）

WD：作業原案（Working Draft）

CD：委員会原案（Committee Draft）

DIS：国際規格原案（Draft International Standard）

FDIS：最終国際規格案（Final Draft International Standard）

IS：国際規格（International Standard）

PDTR：予備技術報告原案（Preliminary Draft Technical Report）

PDTS：予備技術仕様書原案（Preliminary Draft Technical Specification）

DTR：技術報告書原案（Draft Technical Report）

DTS：技術仕様書原案（Draft Technical Specification）

TR：技術報告書（Technical Report）

TS：技術仕様書（Technical Specification）

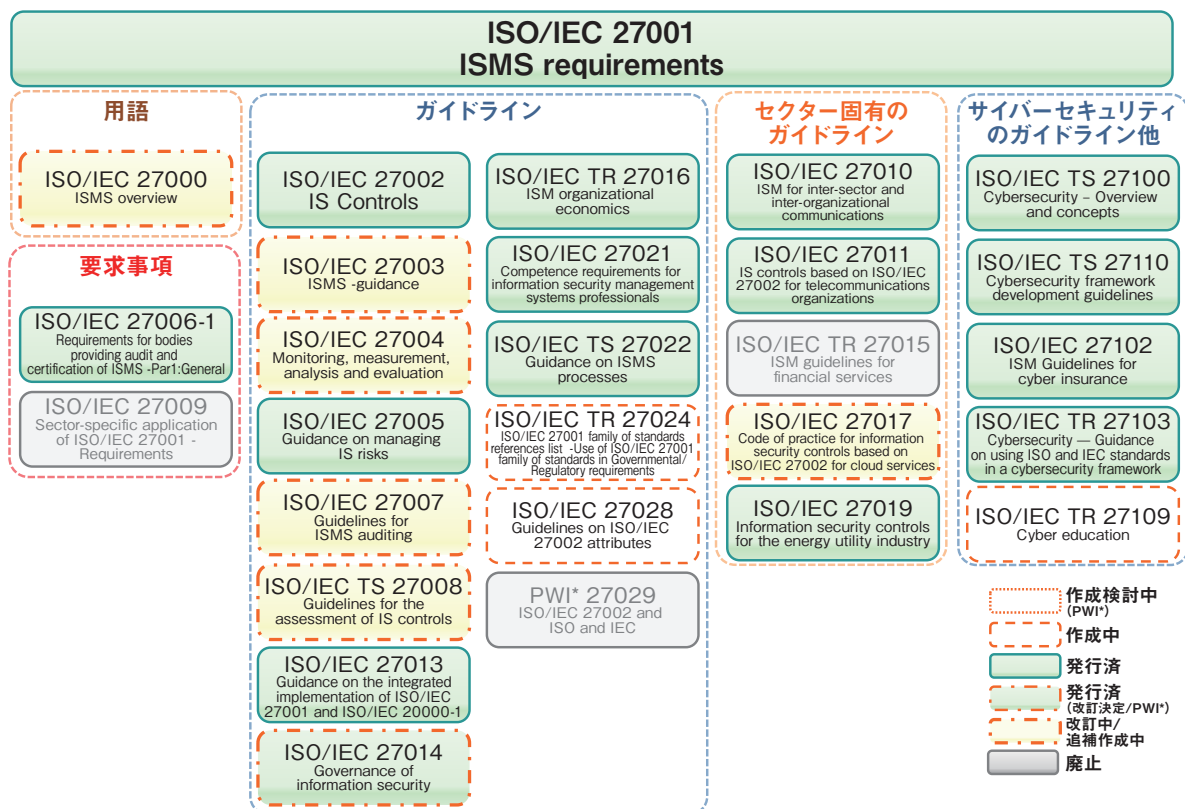
以下に、各WGの活動概要を述べる。なお本文中では略号を使用する。第42回会合は2025年9月に中国昆明で、第43回会合は2026年3月にドイツニュルンベルグで実施されたSC 27総会及び各WG会議を指す。

(1) WG 1（情報セキュリティマネジメントシステム）

WG 1では、情報セキュリティマネジメントシステム（ISMS：Information Security Management System）に関する国際規格として、ISO/IEC 27001（ISMS要求事項）及びISO/IEC 27002（情報セキュリティ管理策）を中心に、ISO/IEC 27001が示すISMS要求事項に関する手引きや指針を提供する規格、ISO/IEC 27001及びISO/IEC 27002を土台とする分野別規格、及びその他トピックスに関するISO/IEC 27000ファミリー規格の国際標準化活動を実施している。

ISO/IEC 27001ファミリーの改訂状況は図4-2-2（次ページ）のとおりである。

WG 1全体としてMSS（Management System Standard：マネジメントシステム規格）群の将来の方向に関する戦略的議論が継続された。特に、2026年第2四半期に予定されるAnnex SL（附属書SL）改訂の影響が大きく、ISO/IEC 27001を含むMSS群全体の構成や整合性に関わる重要な論点として認識された。また、ISO/IEC 27007及び27102でオンライン標準開発（OSD：Online Standards Development）を採用し、



* PWI : ISO 規格作成/改訂手続 (NP) 前に設置される予備段階で、主に規格の作成/改訂の方針等について検討している (「作成中」は手続済で作成段階にある規格)。

■ 図 4-2-2 ISO/IEC 27000 ファミリー規格の作成/改訂状況

(出典)一般財団法人日本情報経済社会推進協会(JIPDEC)「ISO/IEC 27000 ファミリー規格について^{*185}」(2026 年 5 月 18 日発行)を基に IPA が編集

今後の文書開発の進め方にも変化が見られた。

- ISO/IEC 27000 (ISMS- 概要)

2018 年発行の第 5 版からの改訂により、タイトルを「ISMS- 概要と用語」から「ISMS- 概要」に変更し、2026 年 7 月に第 6 版として発行されている。
- ISO/IEC 27007 (ISMS 監査のためのガイドライン)

第 43 回会合で CD から DIS へ進むことが決定された。第 43 回会合からは OSD 適用対象として文書開発が進められている。
- ISO/IEC 27003 (ISO/IEC 27001:2022 適用の手引き)

第 43 回会合で 3rd CD に進むことが決定された。
- ISO/IEC 27008 (情報セキュリティ管理策の評価に関するガイドライン)

第 42 回会合で 3rd CD から DTS の投票へ進むことが決定された。
- ISO/IEC 27017 (ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策)

2026 年 6 月に FDIS 投票が承認され、2015 年発行の初版の改訂版が 2026 年 7 月に発行された。

(2) WG 2 (暗号とセキュリティメカニズム)

WG 2 では、機密性、エンティティ認証、否認防止、鍵管理及びデータ完全性を実現するための暗号技術及び非暗号技術のセキュリティメカニズムを対象として、暗号アルゴリズム、デジタル署名、エンティティ認証、鍵管理、匿名認証、秘密計算及び準同型暗号等の標準化を行っている。

- ISO/IEC 29192 シリーズ (軽量暗号)

2025 年 12 月に「パート 1: 概要」の追補 1 版が発行された。また、第 43 回会合で、Ascon アルゴリズムを同シリーズへ導入する方向で検討が進められた。
- ISO/IEC FDIS 11770-8 (パスワードベース鍵導出)

第 43 回会合において、FDIS に進むことが決定された。
- ISO/IEC 14888-3:2018/FDAmd 1 (離散対数ベースのデジタル署名メカニズム追補 1 版)

第 43 回会合において、FDAmd に進むことが決定された。FDAmd は「最終規格追補原案 (Final Draft Amendment)」を表す。
- ISO/IEC FDIS 28033-4 (完全準同型暗号 (ルックアップテーブル評価に基づく算術メカニズム))

第43回会合において、FDISに進むことが決定された。

- ISO/IEC CD 9798-5 (ゼロ知識証明を用いたエンティティ認証)

第43回会合において、DISに進むことが決定された。

- ISO/IEC DIS 25330-1 (紛失通信)
第43回会合において、DISに進むことが決定された。
- ISO/IEC 20009-4:2017/PRF Amd 1 (弱い秘密に基づく匿名エンティティ認証 追補1版)

第43回会合において発行準備中であることが報告された。

(3) WG 3(セキュリティの評価・試験・仕様)

WG 3では、セキュリティ評価・テスト・仕様に関わる標準化活動として、ISO/IEC 15408 (Common Criteria) 等のセキュリティ評価基準を策定している。

- ISO/IEC 19792:2025 (生体認証システムのセキュリティ評価に関する一般原則、要件、及びガイダンス)
2025年6月に第2版を発行した。
- ISO/IEC 19896-1/2/3 (IT セキュリティ適合性評価機関職員の能力要件)
2025年11月に「パート1: 概要と概念」、2026年1月に「パート2: ISO/IEC 19790 及び ISO/IEC 24759 に基づく試験者及び検証者の知識と技能要件」、2025年11月に「パート3: ISO/IEC 15408 シリーズ 及び ISO/IEC 18045 に基づく評価者及びレビュー担当者の知識と技能要件」が発行された。
- ISO/IEC TS 20540:2025 (暗号モジュールの現場でのテスト)
2025年5月に第2版を発行した。
- ISO/IEC WD 25959 (ディープラーニングベースのテクノロジーへの攻撃可能性の適用)
AI技術のセキュリティ評価を可能にするための開発を開始した。
- ISO/IEC AWI 26160 (人工知能(AI)機能の評価に関するISO/IEC 15408 シリーズ及びISO/IEC 18045の強化)
第43回会合において新規プロジェクトとして承認された。
- ISO/IEC 15408 / ISO/IEC 18045
第43回会合において、CCRA (Common Criteria Recognition Arrangement)とISO事務局の間で著作権及びコンテンツ使用権に関する問題が継続課題として議論された。また、OSD への移行に伴う編集

上の困難も大きいことが確認された。

(4) WG 4(セキュリティコントロールとサービス)

WG 4では、WG 1が対象とするISMSを実施・運用する際に必要となる具体的なセキュリティ対策、及びセキュリティサービスの標準化を行っている。

日本が提案、関与しているISO/IEC 27404、ISO/IEC TS 5689、及び関連する規格の状況を示す。

- ISO/IEC 27404 (消費者向けIoTのサイバーセキュリティ表示フレームワーク)
消費者向けIoT製品・サービスのセキュリティ評価及びラベリングについて、各国で制定するスキームの共通化を図るフレームワークを示す規格である。経済産業省で2025年3月から運用を開始したIoT製品に対する「セキュリティ要件適合評価及びラベリング制度(JC-STAR)」について、本国際規格のAnnex (附属書)への概要記事を提案し、事例として採用された。2025年10月に第1版を発行した。
- ISO/IEC TS 5689 (サイバーフィジカルシステムのためのセキュリティフレームワークとユースケース)
経済産業省のもとで策定した「サイバー・フィジカル・セキュリティ対策フレームワーク(CPSF)^{※186}」を基礎に、日本からの提案により開始したプロジェクトである。日本はメインエディターを担当しており、2025年3月時点でDTSへの移行を進めていたが、OT(運用技術)を主として規格化する団体のIEC TC 65からOT関連について「Major」な修正提案があり、その後、数度の編集会議を繰り返し、2026年6月会議でDTSへの移行が正式に決定され、現在エディターによるDTSテキストの策定を実施しているところである。DTSテキストの完成後、DTS投票に入る予定である。
- ISO/IEC FDIS 27090 (AIシステムに対するセキュリティ上の脅威及び侵害への対応)
AIシステムに特有のセキュリティ上の脅威がライフサイクル全体を通じて及ぼす影響をより深く理解するための情報、及びそのような脅威を検知・軽減する方法に関する情報を組織に対し提供することを目的としている。2026年6月にFDIS投票が開始され、今後発行に進む予定である。

(5) WG 5(アイデンティティ管理とプライバシー技術)

WG 5では、アイデンティティ管理、プライバシー、バイオメトリクスの標準化を行っている。主な規格の制定、

改訂状況について示す。

- ISO/IEC 27701:2025 (プライバシー情報マネジメントシステム)

2025 年 10 月に第 2 版が発行された。プライバシー情報マネジメントシステムの確立、導入、維持及び継続的な改善に関する要件をまとめている。2019 年に発行された第 1 版は、ISO/IEC 27001 及び ISO/IEC 27002 を、プライバシー情報マネジメントシステムの保護のために拡張した規格であったが、第 2 版は、要求事項を含むタイプ A MSS であることから、ISO/IEC 27001 及び ISO/IEC 27002 の拡張規格ではなく、単独のマネジメントシステム規格として発行された 27002 をプライバシーに拡張した規格として位置付けられる。

- ISO/IEC 27706:2025 (プライバシー情報マネジメントシステムの監査及び認証を提供する機関に対する要件)
2025 年 10 月に第 1 版が発行された。ISO/IEC 27701

に基づいてプライバシー情報マネジメントシステムの監査及び認証を行う機関に対する要求事項を規定している。

- ISO/IEC 27091 (AI プライバシー保護)

機械学習モデルを含む AI システム及びにおけるプライバシーリスクへの対処に関する組織向けの手引きを提供している。第 56 回オンライン会合で DIS から FDIS へ進んだ。

- ISO/IEC 29151 (個人識別可能情報の保護に関する管理策、要件、及びガイダンス)

個人識別情報の保護に関連するリスク及び影響評価によって特定された要件を満たすための管理策、目的、及び管理策を実施するためのガイダンスである。2017 年に発行された第 1 版が改訂され、2026 年 7 月に第 2 版が発行された。なお、本規格は ITU-T と共同で策定しており、ITU-T X.1058 と同一の規格本文を持っている。



C O L U M N

セキュリティを「脅威」ではなく「我々」を主語に語り直す

新しい脅威が報じられる度に製品を検討し、予算を取り、導入する、それでも不安は消えない。多くの組織がこのサイクルから抜け出せずにいます。一般社団法人日本クラウドセキュリティアライアンス (CSA ジャパン) のブログ「セキュリティを脅威で語るかぎり、対策は終わらない¹⁾」は、その原因を担当者ではなく「脅威を主語にする」語り方そのものに見いだしています。本コラムでは、同ブログで示されている二つの転換に注目します。

一つ目の転換は、基本対策のとらえ直しです。資産管理も修正プログラムの適用もバックアップも、ニュース性がなくベンダーの目玉商品にもならないため、最新製品の陰で「地味な義務」として後回しにされがちです。しかし、実際のインシデントの多くは、高度な攻撃ではなく、この足元の穴から起きています。セキュリティの目的を「何が起きても、把握し、対処し、元に戻せる状態を保つこと」と言い換えると、基本対策の意味は一変します。資産管理は「把握する」能力、最小権限の設定や多要素認証は「対処する」能力、バックアップは「元に戻せる」能力、監査ログは「説明できる」能力、脆弱性管理の継続運用は「適応し続ける」能力とそれぞれ言い換えられます。これらはいずれも組織のコントロール能力を構成する「部品」そのものです。高度な製品は、その土台の上に載る追加部品にすぎません。資産台帳のない組織に EDR 等の製品を入れても、アラートの指す先が分からなければ動くことはできません。

二つ目の転換は、意思決定の起点とする「問い」の入れ替えです。担当者がやるべきことは、新しい対策を増やすことではありません。会議や報告の場で問いの主語に注意を向け、それが「脅威」や「製品」になっていたら、すかさず主語を「我々」に引き戻すことが必要です。つまり「我々は把握できているか／対処できるか／元に戻せるか／説明できるか／適応し続けられるか」という五つの能力のうち、どの能力に対する問いなのかを、その場で言葉にして確かめます。例えば、重大な脆弱性が公表されたら、「CVSS スコア (深刻度) が高いか」ではなく「自社のどの機器が影響を受けるか、すぐに洗い出せるか」、つまり我々は「把握」できているかを問うことです。EDR の導入を提案されたら、「どの脅威を防げるか」ではなく「我々の『対処』する力を高めるものか、そしてそれを活かす資産把握の土台はあるか」を問います。問いを言い換えるこの一手間こそ、担当者が日々の判断の中で実践できる、最も現実的な一歩です。

この入れ替えは、経営陣との対話でも有効です。脅威ベースの予算要求では、攻撃が起きなかったとき、それが投資の成果か単なる幸運かを区別できず、判断のよりどころが「どれだけ怖い」しか残りません。一方、能力を問えば、検知から対処までの時間や復旧目標の達成度といった形で投資効果を数値化でき、経営陣は他の事業投資と同じ物差しでセキュリティを評価できます。能力は放置すれば劣化するからこそ、継続投資の理由も自然に説明が付きまします。

完璧な対策一覧を作ることだけが、担当者の仕事なのではありません。「この脅威をどう防ぐか」ではなく、「何が起きても、我々は把握し、対処し、元に戻せるか」。この問いを起点にすることこそが、新しい脅威の度に製品を導入し続けるサイクルから抜け出す、最初の一歩になります。

i [https://cloudsecurityalliance.jp/newblog/2026/06/13/ セキュリティを脅威で語るかぎり、対策は終わらない](https://cloudsecurityalliance.jp/newblog/2026/06/13/セキュリティを脅威で語るかぎり、対策は終わらない) / [2026/7/27 確認]

※ 1 Silobreaker Limited.: Hacktivism in the India-Pakistan conflict
<https://www.silobreaker.com/blog/geopolitical/hacktivism-in-the-india-pakistan-conflict-analysis-of-recent-campaigns/>〔2026/7/3 確認〕
Codebook: インド・パキスタン軍事衝突におけるハクティビズム <https://codebook.machinarecord.com/cyber-intelligence/geopolitical-risk/39666/>〔2026/7/3 確認〕
※ 2 Group-IB: Hacktivists at War <https://go.group-ib.com/hubfs/report/protected/group-ib-hackivist-at-war-report-2025-apac-en.pdf>〔2026/7/3 確認〕
※ 3 Cybereason Inc.: LevelBlue SpiderLabs が解説する、イラン危機におけるサイバー作戦の役割 <https://www.cybereason.co.jp/blog/levelblue-spiderlabs-blog/13981/>〔2026/7/3 確認〕
※ 4 ESET, spol. s r.o.: ESET、初の AI 駆動型ランサムウェア「PromptLock」発見 ～サイバー攻撃は新たなフェーズへ突入～
https://www.eset.com/jp/about/newsroom/press-releases/2025/eset-discovers-promptlock-the-first-ai-powered-ransomware-jp/?srsltid=AfmBOorDAue63fS7DsWUXY5SRH_xQ21tWds8j840OhtQCiaEUV08ul2o〔2026/7/3 確認〕
※ 5 The Register: The crazy, true story behind the first AI-powered ransomware <https://www.theregister.com/security/2025/09/05/the-crazy-true-story-behind-the-first-ai-powered-ransomware/624795/>〔2026/7/3 確認〕
※ 6 トレンドマイクロ株式会社: AI 駆動型マルウェアとは何か?～ Vibe Coding を駆使する LAMEHUG、PromptLock を解説 https://www.trendmicro.com/ja_jp/jp-security/25/i/securitytrend-20250924-01.html〔2026/7/3 確認〕
※ 7 ITmedia NEWS: 大企業に潜り込む工作員、増加中——北朝鮮 IT ワーカーの大口 採用面接も AI で突破、実績アピールの偽装 SNS も
<https://www.itmedia.co.jp/news/articles/2507/10/news031.html>〔2026/7/3 確認〕
※ 8 Okta, Inc.: 生成 AI サービスを悪用した北朝鮮労働者のリモート勤務契約 <https://www.okta.com/ja-jp/blog/industry-insights/genaidprk/>〔2026/7/3 確認〕
※ 9 警察庁: 北朝鮮 IT 労働者に関する企業等に対する注意喚起
https://www.npa.go.jp/bureau/security/northkorea_IT/NK_IT_202508.html〔2026/7/3 確認〕
※ 10 CISA: PRC STATE-SPONSORED CYBER ACTIVITY: ACTIONS FOR CRITICAL INFRASTRUCTURE LEADERS
https://www.cisa.gov/sites/default/files/2024-03/Fact-Sheet-PRC-State-Sponsored-Cyber-Activity-Actions-for-Critical-Infrastructure-Leaders-508c_0.pdf〔2026/9/24 確認〕
※ 11 Codebook: 中国の「Typhoon」ハッカーグループ: Volt Typhoon、Flax Typhoon、Salt Typhoon の概要や注目ポイント <https://codebook.machinarecord.com/threatreport/silobreaker-cyber-alert/36791/>〔2026/7/3 確認〕
Bloomberg: Hackers Terrify US Intelligence After Infiltrating Guam
<https://www.bloomberg.com/news/features/2025-01-03/chinese-cyber-hackers-terrify-us-intelligence-after-infiltrating-guam>〔2026/7/3 確認〕
※ 12 CISA: Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a>〔2026/7/3 確認〕
※ 13 Reuters: 英、サイバー攻撃でロシアに制裁 軍情報機関部隊など対象 <https://jp.reuters.com/world/security/MDGDOCGMORLN LN5QROXZS5F5NI-2025-07-18/>〔2026/7/3 確認〕
※ 14 株式会社大和総研: 米国政府はなぜ最先端 AI を停止させたのか
https://www.dir.co.jp/report/research/economics/usa/20260617_025839.pdf〔2026/7/3 確認〕
※ 15 外務省: サイバー犯罪に関する条約(略称: サイバー犯罪条約(通称: ブダベスト条約)) https://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html〔2026/4/20 確認〕
※ 16 United Nations: United Nations Convention against Cybercrime <https://www.unodc.org/unodc/en/cybercrime/convention/home.html>〔2026/7/3 確認〕
※ 17 International Counter Ransomware Initiative: <https://counter-ransomware.org/>〔2026/7/3 確認〕
※ 18 International Counter Ransomware Initiative: Singapore Hosted the 5th Counter Ransomware Initiative Summit <https://counter-ransomware.org/briefingroom/5ebb6bfd-1a14-47d8-80e7-ffb40c0be113>〔2026/7/3 確認〕
※ 19 外務省: 「カウンターランサムウェア・イニシアティブ(CRI)会合」への参加 https://www.mofa.go.jp/mofaj/press/release/pressit_000001_02885.html〔2026/7/3 確認〕

※ 20 GOV.UK: Guidance for organisations to build supply chain resilience against ransomware <https://www.gov.uk/government/publications/supply-chain-resilience-against-ransomware/guidance-for-organisations-to-build-supply-chain-resilience-against-ransomware>〔2026/7/3 確認〕
※ 21 Department for Science, Innovation & Technology: International AI Safety Report 2025 <https://internationalaisafetyreport.org/publication/international-ai-safety-report-2025>〔2026/7/3 確認〕
※ 22 Department for Science, Innovation & Technology: International AI Safety Report 2026 <https://internationalaisafetyreport.org/publication/international-ai-safety-report-2026>〔2026/7/3 確認〕
※ 23 金融庁、警察庁、内閣サイバーセキュリティセンター、外務省、財務省、経済産業省: 「北朝鮮による暗号資産窃取及び官民連携に関する共同声明」の公表について <https://www.fsa.go.jp/news/r6/sonota/20250114/20250114.html>〔2026/7/3 確認〕
※ 24 Reuters: 日米韓、北朝鮮のサイバー脅威巡り協議体発足へ 兵器開発の資金源 <https://jp.reuters.com/world/security/NFRFU5B OQNP7JLDKH7HEJY5AIA-2023-11-06/>〔2026/7/3 確認〕
※ 25 外務省: 日米韓首脳共同声明「キャンプ・デービッドの精神」
<https://www.mofa.go.jp/mofaj/files/100541771.pdf>〔2026/7/3 確認〕
※ 26 経済産業省: IoT 製品に対するセキュリティラベリング制度(JC-STAR)の運用を開始しました <https://www.meti.go.jp/press/2024/03/20250325007/20250325007.html>〔2026/7/3 確認〕
※ 27 経済産業省: JC-STAR と英国 PSTI 法の相互承認に関する覚書に署名しました <https://www.meti.go.jp/press/2025/11/20251106003/20251106003.html>〔2026/7/3 確認〕
※ 28 IPA: プレス発表 日本・シンガポール、IoT サイバーセキュリティ制度の相互承認に関する覚書に署名 <https://www.ipa.go.jp/pressrelease/2025/press20260318.html>〔2026/7/3 確認〕
※ 29 IPA: シンガポール CLS 適合の相互承認申請について <https://www.ipa.go.jp/security/jc-star/shinsei/cls.html>〔2026/7/3 確認〕
※ 30 外務省: 第 10 回日米サイバー対話の開催 https://www.mofa.go.jp/mofaj/press/release/pressit_000001_02292.html〔2026/7/3 確認〕
※ 31 外務省: 第 4 回北朝鮮サイバー脅威に関する日米韓外交当局間作業部会の開催 https://www.mofa.go.jp/mofaj/press/release/pressit_000001_02652.html〔2026/7/3 確認〕
※ 32 外務省: 日米韓「北朝鮮 IT 労働者に関する共同声明」及び「北朝鮮 IT 労働者に関する企業等に対する注意喚起」の公表 https://www.mofa.go.jp/mofaj/press/release/pressit_000001_02650.html〔2026/7/3 確認〕
※ 33 外務省: 第 9 回日英サイバー対話の開催(結果) https://www.mofa.go.jp/mofaj/press/release/pressit_000001_03394.html〔2026/7/3 確認〕
※ 34 経済産業省: 第 18 回 ASEAN サイバーセキュリティ政策会議を開催しました <https://www.meti.go.jp/press/2025/10/20251016001/20251016001.html>〔2026/7/3 確認〕
※ 35 外務省: 第 7 回 EU サイバー対話の開催(結果) https://www.mofa.go.jp/mofaj/press/release/pressit_000001_03261.html〔2026/7/3 確認〕
※ 36 経済産業省: 「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク」を実施しました <https://www.meti.go.jp/press/2025/11/20251125001/20251125001.html>〔2026/4/23 確認〕
※ 37 IPA: ICSCoE REPORT vol.22 ASEAN 諸国の実務者を対象に OT セキュリティトレーニングを実施 <https://www.ipa.go.jp/jinzai/ics/ngi93u0000002150-att/j5u9nn000000673l.pdf>〔2026/7/3 確認〕
※ 38 IPA: キングモンクット工科大学ラカバン校(KOSEN-KMITL)との産業サイバーセキュリティ教育支援に関する覚書の締結について <https://www.ipa.go.jp/jinzai/ics/global/news20240710.html>〔2026/7/3 確認〕
※ 39 JICA: サイバーセキュリティとデジタルトラストサービスに関する日 ASEAN 能力向上プログラム強化プロジェクト <https://www.jica.go.jp/oda/project/202210323/index.html>〔2026/7/3 確認〕
※ 40 PR TIMES: タイ・バンコクの ASEAN 向けサイバー研修施設を開所 <https://prtimes.jp/main/html/rd/p/000000031.000151049.html>〔2026/7/3 確認〕
※ 41 総務省: 日 ASEAN サイバーセキュリティ能力構築センター(AJCCBC)における官民連携による演習実施 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00278.html〔2026/7/3 確認〕
※ 42 総務省: 大洋州島しょ国・地域向けサイバーセキュリティ能力構築演習(令和 7 年度第 1 回)の実施 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00259.html〔2026/7/3 確認〕

※ 43 総務省：大洋州島しょ国・地域向けサイバーセキュリティ能力構築演習（令和7年度第2回）の実施 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00274.html [2026/7/3 確認]

※ 44 <https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf> [2026/6/10 確認]

※ 45 <https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf> [2026/6/10 確認]

※ 46 Federal Register: Executive Order 14390, Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens <https://www.federalregister.gov/documents/2026/03/11/2026-04826/combating-cybercrime-fraud-and-predatory-schemes-against-american-citizens> [2026/6/10 確認]

※ 47 U.S. Government Publishing Office: 42 U.S.C. 5195c - Critical infrastructures protection <https://www.govinfo.gov/app/details/USCODE-2024-title42/USCODE-2024-title42-chap68-subchapIV-B-sec5195c/summary> [2026/8/3 確認]

※ 48 Federal Register: Executive Order 14239, Achieving Efficiency Through State and Local Preparedness <https://www.federalregister.gov/documents/2025/03/21/2025-04973/achieving-efficiency-through-state-and-local-preparedness> [2026/6/10 確認]

※ 49 The White House: White House Unveils President Trump's America First Resilience Strategy <https://www.whitehouse.gov/releases/2026/06/white-house-unveils-president-trumps-america-first-resilience-strategy/> [2026/8/3 確認]

※ 50 NIST: Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography <https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved> [2026/6/10 確認]

※ 51 Federal Register: Executive Order 14306, Sustaining Select Efforts To Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144 <https://www.federalregister.gov/documents/2025/06/11/2025-10804/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694> [2026/6/10 確認]

※ 52 <https://www.cisa.gov/resources-tools/resources/product-categories-technologies-use-post-quantum-cryptography-standards> [2026/6/10 確認]

※ 53 OMB: Memorandum M-25-34/NSTM-2 Fiscal Year (FY) 2027 Administration Research and Development Budget Priorities and Cross-Cutting Actions <https://www.whitehouse.gov/wp-content/uploads/2025/09/M-25-34-NSTM-2-Fiscal-Year-FY-2027-Administration-Research-and-Development-Budget-Priorities-and-Cross-Cutting-Actions.pdf> [2026/6/10 確認]

※ 54 NIST: NIST SP 800-63 Digital Identity Guidelines <https://pages.nist.gov/800-63-4/> [2026/6/10 確認]

※ 55 American Association of Motor Vehicle Administrators: Mobile Driver's License (mDL) Implementation Guidelines, Version 1.5 <https://www.aamva.org/getmedia/bb4fee66-592d-4d39-813a-8fd910268a/MobileDLGuidelines1-5.pdf> [2026/6/10 確認]

※ 56 NIST: Draft NIST Guidelines on Implementing Mobile Driver's Licenses for Financial Institutions <https://csrc.nist.gov/News/2026/mdl-for-financial-institutions-draft-guidelines> [2026/6/10 確認]

※ 57 OMB: Memorandum M-26-05: Adopting a Risk-based Approach to Software and Hardware Security <https://www.whitehouse.gov/wp-content/uploads/2026/01/M-26-05-Adopting-a-Risk-based-Approach-to-Software-and-Hardware-Security.pdf> [2026/6/10 確認]

※ 58 OMB: Memorandum M-22-18: Enhancing the Security of the Software Supply Chain through Secure Software Development Practices <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/09/M-22-18.pdf> [2026/6/10 確認]

※ 59 OMB: Memorandum M-23-16: Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices <https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security.pdf> [2026/6/10 確認]

※ 60-1 United States Congress: Making consolidated appropriations for the fiscal year ending September 30, 2026, and for other purposes, Public Law 119-74 <https://www.govinfo.gov/congress/pkgs/PLAW-119publ74/pdf/PLAW-119publ74.pdf> [2026/6/10 確認]

※ 60-2 United States Congress: NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2026, Public Law 119-60 <https://www.congress.gov/119/plaws/publ60/PLAW-119publ60.pdf> [2026/6/10 確認]

※ 60-3 NIST: Executive Order 14306 -- Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144 <https://www.nist.gov/itl/executive-orders/strengthening-and-promoting-innovation-nations-cybersecurity> [2026/8/3 確認]

※ 61 OMB: Memorandum M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government <https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial-Intelligence-in-Government.pdf> [2026/6/10 確認]

※ 62 OMB: Memorandum M-26-02: Ensuring Government Use of Secure Unmanned Aircraft Systems and Supporting United States Producers <https://www.whitehouse.gov/wp-content/uploads/2025/11/M-26-02-Ensuring-Government-Use-of-Secure-Unmanned-Aircraft-Systems-and-Supporting-United-States-Producers.pdf> [2026/6/10 確認]

※ 63 OMB: Memorandum M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust <https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf> [2026/6/10 確認]

※ 64 Federal Register: Executive Order 14307: Unleashing American Drone Dominance <https://www.federalregister.gov/documents/2025/06/11/2025-10814/unleashing-american-drone-dominance> [2026/6/10 確認]

※ 65 <https://www.fcc.gov/CyberTrustMark> [2026/6/10 確認]

※ 66 FCC: FCC 24-26 A1 <https://docs.fcc.gov/public/attachments/FCC-24-26A1.pdf> [2026/6/10 確認]

※ 67 IPA: JC-STAR 活用に向けた取り組み <https://www.ipa.go.jp/security/jc-star/leverage.html> [2026/6/10 確認]

※ 68 CISA: 2025 Year in Review <https://www.cisa.gov/about/2025YIR> [2026/6/10 確認]

※ 69 CISA: Protective Domain Name System (DNS) Resolver <https://www.cisa.gov/resources-tools/services/protective-domain-name-system-dns-resolver> [2026/6/10 確認]

※ 70 CISA: Cybersecurity Performance Goals 2.0 (CPG 2.0) <https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0> [2026/6/10 確認]

※ IPA: 米 CISA 発行 Cross-Sector Cybersecurity Performance Goals Ver.2.0 (2025-12) の翻訳 <https://www.ipa.go.jp/security/controlsystem/cisacpgs.html> [2026/6/10 確認]

※ 71 <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> [2026/6/10 確認]

※ 72 CISA: Cyber Incident Reporting for Critical Infrastructure Act of 2022 https://www.cisa.gov/sites/default/files/2023-01/Cyber-Incident-Reporting-ForCriticalInfrastructure-Act-of2022_508.pdf [2026/6/10 確認]

※ 73-1 CISA: Critical Infrastructure Sectors <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors> [2026/6/10 確認]

※ 73-2 Federal Register: Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) Reporting Requirements <https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements> [2026/8/3 確認]

※ 74 Regulations.gov: Comment Submitted by American Public Media Group (APMG) <https://www.regulations.gov/comment/CISA-2022-0010-0391> [2026/6/10 確認]

※ 75 The HIPAA Journal: Industry Groups Give Feedback on CISA's Proposed Cybersecurity Reporting Requirements <https://www.hipaajournal.com/industry-groups-feedback-cisa-circia-cybersecurity-incident-reports/> [2026/6/10 確認]

※ 76 Garbarino, Andrew: RE: Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) Reporting Requirements, 89 FR 23644, CISA-2022-0010. <https://business.cch.com/cybersecurityPrivacy/circiagarbarino.pdf> [2026/6/10 確認]

※ 77 CISA: CISA Announces New Town Halls to Engage with Stakeholders on Cyber Incident Reporting for Critical Infrastructure <https://www.cisa.gov/news-events/news/>

cisa-announces-new-town-halls-engage-stakeholders-cyber-incident-reporting-critical-infrastructure[2026/6/10 確認]

※ 78 DHS : DHS Fiscal Year 2026 Budget in Brief https://www.dhs.gov/sites/default/files/2025-07/2025_07_03_ocfo_fy-2026-budget-in-brief.pdf[2026/6/10 確認]

※ 79 MeriTalk : White House Eyes 29% CISA Workforce Cut <https://www.meritalk.com/articles/white-house-eyes-29-cisa-workforce-cut/>[2026/6/10 確認]

※ 80 CISA : CISA Releases Its First Ever International Strategic Plan <https://www.cisa.gov/news-events/news/cisa-releases-its-first-ever-international-strategic-plan>[2026/6/10 確認]

※ 81 <https://www.cisa.gov/about/divisions-offices/stakeholder-engagement-division>[2026/6/10 確認]

※ 82 The Foundation for Defense of Democracies : The Cipher Brief America's Cyber Strategy Has a Budget Problem <https://www.fdd.org/analysis/2026/04/23/americas-cyber-strategy-has-a-budget-problem/>[2026/6/10 確認]

※ 83 United States Congress : DIVISION H.—Protecting Americans from Foreign Adversary Controlled Applications Act, Public Law 118-50 <https://www.congress.gov/118/plaws/publ50/PLAW-118publ50.pdf>[2026/6/10 確認]

※ 84 Federal Register : Executive Order 14352: Saving TikTok While Protecting National Security <https://www.federalregister.gov/documents/2025/09/30/2025-19139/saving-tiktok-while-protecting-national-security>[2026/6/30 確認]

※ 85 Reuters : TikTok seals deal for new US joint venture to avoid American ban <https://www.reuters.com/world/china/tiktok-reaches-deal-new-us-joint-venture-avoid-american-ban-2026-01-23/>[2026/6/10 確認]

※ 86 Federal Register : Executive Order 14277: Advancing Artificial Intelligence Education for American Youth <https://www.federalregister.gov/documents/2025/04/28/2025-07368/advancing-artificial-intelligence-education-for-american-youth>[2026/6/10 確認]

※ 87 <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>[2026/6/10 確認]

※ 88 [https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA Threat Landscape 2025 Booklet.pdf](https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%2025%20Booklet.pdf)[2026/6/10 確認]

※ 89 European Commission : The Draghi report on EU competitiveness https://commission.europa.eu/topics/competitiveness/draghi-report_en#paragraph_47059[2026/6/10 確認]

※ 90 European Commission : Simpler EU digital rules and new digital wallets to save billions for businesses and boost innovation https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718[2026/6/10 確認]

※ 91 EU : Document 52025PC0837 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837> [2026/6/10 確認]

※ 92 EU : Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 <https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng>[2026/7/2 確認]

※ 93 EU : Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>[2026/7/2 確認]

※ 94 EU : Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC <https://eur-lex.europa.eu/eli/reg/2018/1725/oj/eng>[2026/7/2 確認]

※ 95 EU : Consolidated text: Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018R1724-20260520>[2026/7/2 確認]

※ 96 EU : Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>[2026/7/2 確認]

※ 97 デジタルサービス法 (DSA : Digital Services Act) : 違法コンテンツの拡散防止や利用者の基本的人権の保護を目的として、オンラインプラットフォーム等の仲介サービス提供者に対して、安全で透明性の高いオンライン環境を確保する義務を定めた法律。
EU : Regulation (EU) 2022/2065 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=>

1780560741397[2026/6/10 確認]

※ 98 デジタル市場法 (DMA : Digital Markets Act) : 強大な影響力を持つ巨大 IT 企業の不公正な慣行を規制し、デジタル分野における公平で競争可能な市場を確保するための法律。
EU : Regulation (EU) 2022/1925 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925&qid=1780560741397>[2026/6/10 確認]

※ 99 European Commission : An agile Digital Rulebook for the EU <https://digital-strategy.ec.europa.eu/en/policies/digital-rulebook>[2026/6/10 確認]

※ 100 EU : Document 52025PC0836 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0836> [2026/6/10 確認]

※ 101 規制サンドボックス : 規制当局の監督のもとで、規制の適用を受けずに一定期間・限定された環境で新技術等の実証を行える制度。

※ 102 European Commission : EU Cybersecurity Act <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>[2026/6/10 確認]

※ 103 European Commission : Proposal for a Regulation for the EU Cybersecurity Act <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act>[2026/6/10 確認]

※ 104 European Commission : EU Cybersecurity Certification Framework <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework>[2026/6/10 確認]

※ 105 ENISA : MB Decision 2025-18 on adopting ENISA SPD 2026-2028 with Annexes.pdf <https://www.enisa.europa.eu/sites/default/files/2025-12/MB%20Decision%202025-18%20on%20adopting%20ENISA%20SPD%202026-2028%20with%20Annexes.pdf>[2026/6/10 確認]

※ 106 European Commission : EU launches a European vulnerability database to boost its digital security <https://digital-strategy.ec.europa.eu/en/news/eu-launches-european-vulnerability-database-boost-digital-security>[2026/6/10 確認]

※ 107 European Commission : Commission strengthens EU cybersecurity resilience and capabilities https://ec.europa.eu/commission/presscorner/detail/en/ip_26_105[2026/6/10 確認]

※ 108 ENISA : Stepping up our role in Vulnerability Management: ENISA Becomes CVE Root <https://www.enisa.europa.eu/news/stepping-up-our-role-in-vulnerability-management-enisa-becomes-cve-root>[2026/6/10 確認]

※ 109 <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>[2026/6/10 確認]

※ 110 European Commission : Proposal for a Directive as regards simplification measures and alignment with the Cybersecurity Act <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act>[2026/6/10 確認]

※ 111 欧州デジタル ID ウォレット : スマートフォン等のデバイスに利用者の個人情報や保存・管理し、安全な身元確認や認証、属性の電子証明を含む電子文書の交換を可能にするアプリ。
European Commission : European Digital Identity (EUDI) Regulation <https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation>[2026/6/10 確認]

※ 112 欧州ビジネスウォレット : 欧州の企業や公共機関に統一されたデジタルツールを提供し、対面で行う必要がある業務等をデジタル化することで EU 全域でのビジネスを容易にする仕組み。
European Commission : Simpler EU digital rules and new digital wallets to save billions for businesses and boost innovation https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718[2026/6/10 確認]

※ 113 EU : Regulation (EU) 2024/2847 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847> [2026/6/10 確認]

※ 114 JETRO : CE マーケティングの概要 : EU <https://www.jetro.go.jp/world/qa/04S-040011.html>[2026/6/10 確認]

※ 115 European Commission : Cyber Resilience Act <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act> [2026/6/10 確認]

※ 116 重大インシデント : 製造業者の製品ライフサイクルに影響を与え、ユーザーまたはその他のサイバーセキュリティリスクを高める可能性がある状況。

※ 117 European Commission : EU Cyber Solidarity Act <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>[2026/6/10 確認]

※ 118 European Commission : EU cybersecurity policies <https://>

digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies [2026/6/10 確認]

※ 119 ENISA: ENISA to operate the EU Cybersecurity Reserve with EUR 36 million <https://www.enisa.europa.eu/news/enisa-to-operate-the-eu-cybersecurity-reserve-with-eur-36-million> [2026/6/10 確認]

※ 120 European Commission: Cyber Blueprint - Council Recommendation <https://digital-strategy.ec.europa.eu/en/library/cyber-blueprint-council-recommendation> [2026/6/10 確認]

※ 121 European Commission: Member States and Commission test collective cybersecurity crisis response <https://digital-strategy.ec.europa.eu/en/news/member-states-and-commission-test-collective-cybersecurity-crisis-response> [2026/6/10 確認]

ENISA: BlueOLEx 2025: Testing the Capabilities of EU Crisis Management Executives <https://www.enisa.europa.eu/news/blueolex-2025-testing-the-capabilities-of-eu-crisis-management-executives> [2026/6/10 確認]

※ 122 European Commission: EU Preparedness Union Strategy to prevent and react to emerging threats and crises https://ec.europa.eu/commission/presscorner/detail/en/ip_25_856 [2026/6/10 確認]

※ 123 EU: Implementing Regulation (EU) 2024/482 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R0482> [2026/6/10 確認]

※ 124 ENISA: EUCC Certification Scheme https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en [2026/6/10 確認]

※ 125 EU: Implementing Regulation (EU) 2025/2462 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R2462> [2026/6/10 確認]

※ 126 https://certification.enisa.europa.eu/about-eu-cyber-certification/eu-regulatory-context/union-rolling-work-programme_en [2026/6/10 確認]

※ 127 中国政府網: 中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要 https://www.gov.cn/xinwen/2021-03/13/content_5592681.htm [2026/7/7 確認]

國務院: 国务院关于印发“十四五”数字经济发展规划的通知 https://www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm [2026/7/7 確認]

※ 128 中国政府網: 中华人民共和国国家安全法 (主席令第二十九号) https://www.gov.cn/zhengce/2015-07/01/content_2893902.htm [2026/7/7 確認]

※ 129 国立国会図書館: 中国の反テロリズム法 https://dl.ndl.go.jp/view/download/digidepo_10016375_po_02680005.pdf?contentNo=1 [2026/7/7 確認]

※ 130 国立国会図書館: 中国の国家情報法 https://dl.ndl.go.jp/view/download/digidepo_11000634_po_02740005.pdf?contentNo=1 [2026/7/7 確認]

※ 131 国家密码管理局: 《中华人民共和国密码法》解读 https://www.oscca.gov.cn/sca/c100236/2019-12/25/content_1057308.shtml [2026/7/7 確認]

※ 132 CAC: 中华人民共和国网络安全法 https://www.cac.gov.cn/2025-12/29/c_1768735112911946.htm [2026/7/7 確認]

※ 133 CAC: 中华人民共和国数据安全法 https://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm [2026/7/7 確認]

※ 134 CAC: 中华人民共和国个人信息保护法 https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm [2026/7/7 確認]

※ 135 データ三法が中国のデータ保護法制の基本枠組みを構成している点については、以下の分析も参照されたい。

DLA Piper: Data protection laws in China - Data Protection Laws of the World <https://www.dlapiperdataprotection.com/index.html?c=CN> [2026/7/7 確認]

※ 136 國務院: 关键信息基础设施安全保护条例 https://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm [2026/7/7 確認]

※ 137 JETRO: 中国の経済安全保障に関する制度情報 https://www.jetro.go.jp/ext_images/_Reports/01/04c339ffc1751cb1/20210042_01.pdf [2026/7/7 確認]

JETRO: ネットワークデータ安全管理条例 ～中国の安全保障貿易管理に関する制度情報 専門家による政策解説～ (2025年5月) https://www.jetro.go.jp/ext_images/_Reports/01/b41ddf5b802238e1/20250007_01.pdf [2026/7/7 確認]

※ 138 DLA Piper: Data protection laws in China - Data Protection Laws of the World <https://www.dlapiperdataprotection.com/index.html?c=CN> [2026/7/7 確認]

※ 139 CAC: 网络数据安全条例 https://www.cac.gov.cn/2024-09/30/c_1729384452307680.htm [2026/7/7 確認]

CAC: 个人信息保护合规审计管理办法 https://www.cac.gov.cn/2025-02/14/c_1741233507681519.htm [2026/7/7 確認]

CAC: 国家网络安全事件报告管理办法 https://www.cac.gov.cn/2025-09/15/c_1759583017717009.htm [2026/7/7 確認]

CAC: 关于印发《人工智能生成合成内容标识办法》的通知 https://www.cac.gov.cn/2025-03/14/c_1743654684782215.htm [2026/7/7 確認]

CAC: 数据出境安全管理政策问答 (2025年4月) https://www.cac.gov.cn/2025-04/09/c_1745906286623776.htm [2026/7/7 確認]

国家法律法规データベース: 全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定 <https://flk.npc.gov.cn/detail?id=621d029681d4457ab5fc56ec7c7464a1&title=全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定&type=decision> [2026/7/7 確認]

※ 140 CAC: 网络数据安全条例 https://www.cac.gov.cn/2024-09/30/c_1729384452307680.htm [2026/7/7 確認]

※ 141 JETRO: 中国、ネットワークデータセキュリティ管理条例を公布、データ越境などのセキュリティ詳細を規定 <https://www.jetro.go.jp/biznews/2024/10/758e74e9e1e2f718.html> [2026/7/7 確認]

JETRO: ネットワークデータ安全管理条例 ～中国の安全保障貿易管理に関する制度情報 専門家による政策解説～ (2025年5月) https://www.jetro.go.jp/ext_images/_Reports/01/b41ddf5b802238e1/20250007_01.pdf [2026/7/7 確認]

Latham & Watkins: China Clarifies Privacy and Data Security Requirements in Network Data Security Management Regulations <https://www.lw.com/admin/upload/SiteAttachments/China-Clarifies-Privacy-and-Data-Security-Requirements-in-Network-Data-Security-Management-Regulations.pdf> [2026/7/7 確認]

Mayer Brown: PRC Network Data Security Management Regulations <https://www.mayerbrown.com/en/insights/publications/2024/12/prc-network-data-security-management-regulations> [2026/7/7 確認]

※ 142 JETRO: ネットワークデータ安全管理条例 ～中国の安全保障貿易管理に関する制度情報 専門家による政策解説～ (2025年5月) https://www.jetro.go.jp/ext_images/_Reports/01/b41ddf5b802238e1/20250007_01.pdf [2026/7/7 確認]

Mayer Brown: China Finalises the Measures for Personal Information Protection Compliance Audits <https://www.mayerbrown.com/en/insights/publications/2025/04/china-finalises-the-measures-for-personal-information-protection-compliance-audits> [2026/7/7 確認]

Latham & Watkins: China Clarifies Privacy and Data Security Requirements in Network Data Security Management Regulations <https://www.lw.com/admin/upload/SiteAttachments/China-Clarifies-Privacy-and-Data-Security-Requirements-in-Network-Data-Security-Management-Regulations.pdf> [2026/7/7 確認]

Mayer Brown: PRC Network Data Security Management Regulations <https://www.mayerbrown.com/en/insights/publications/2024/12/prc-network-data-security-management-regulations> [2026/7/7 確認]

※ 143 CAC: 个人信息保护合规审计管理办法 https://www.cac.gov.cn/2025-02/14/c_1741233507681519.htm [2026/7/7 確認]

CAC: 中华人民共和国个人信息保护法 https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm [2026/7/7 確認]

※ 144 Mayer Brown: China Finalises the Measures for Personal Information Protection Compliance Audits <https://www.mayerbrown.com/en/insights/publications/2025/04/china-finalises-the-measures-for-personal-information-protection-compliance-audits> [2026/7/7 確認]

※ 145 CAC: 国家网络安全事件报告管理办法 https://www.cac.gov.cn/2025-09/15/c_1759583017717009.htm [2026/7/7 確認]

※ 146 Morgan Lewis: China Issues New Cybersecurity Incident Reporting Framework <https://www.morganlewis.com/pubs/2025/09/china-issues-new-cybersecurity-incident-reporting-framework> [2026/7/7 確認]

※ 147 CAC: 关于印发《人工智能生成合成内容标识办法》的通知 https://www.cac.gov.cn/2025-03/14/c_1743654684782215.htm [2026/7/7 確認]

※ 148 CAC: 中央网信办部署开展“清朗·整治AI技术滥用”专项行动 https://www.cac.gov.cn/2025-04/30/c_1747719097461951.htm [2026/7/7 確認]

※ 149 国家标准信息公共服务平台: 网络安全技术 人工智能生成合成

内容标识方法 <https://std.samr.gov.cn/gb/search/gbDetailed?id=301E0388CB75788DE06397BE0A0AE1B4> [2026/7/7 確認]

※ 150 Loeb & Loeb LLP : China's AI-Labeling Measures and Mandatory National Standards Take Effect September 1 <https://www.loeb.com/en/insights/publications/2025/03/chinas-ai-labeling-measures-and-mandatory-national-standards-take-effect-september-1> [2026/7/7 確認]

※ 151 Reuters : Chinese regulators issue requirements for the labeling of AI-generated content <https://www.reuters.com/world/asia-pacific/chinese-regulators-issue-requirements-labeling-ai-generated-content-2025-03-14/> [2026/7/7 確認]

※ 152 CAC : 数据出境安全管理政策问答 (2025 年 4 月) https://www.cac.gov.cn/2025-04/09/c_1745906286623776.htm [2026/7/7 確認]

CAC : 数据出境安全管理政策问答 (2025 年 5 月) https://www.cac.gov.cn/2025-05/30/c_1750315283722063.htm [2026/7/7 確認]

CAC : 数据出境安全管理政策问答 (2025 年 10 月) https://www.cac.gov.cn/2025-10/31/c_1763633376984070.htm [2026/7/7 確認]

※ 153 Grandway Law Offices : CAC Releases First Batch of Q&A on Data Cross-Border Security Management Policies <https://www.grandwaylaw.com/en/Legalupdate/4475.html> [2026/7/7 確認]

China Briefing : China Clarifies Cross-Border Data Transfer Rules: Key Takeaways from Official Q&A (I) <https://www.china-briefing.com/news/china-clarifies-cross-border-data-transfer-rules-official-qa/> [2026/7/7 確認]

※ 154 CAC : 国家互联网信息办公室、国家市场监督管理总局联合公布《个人信息出境认证办法》 https://www.cac.gov.cn/2025-10/17/c_1762449728518762.htm [2026/7/7 確認]

※ 155 国家法律法规データベース : 全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定 <https://flk.npc.gov.cn/detail?id=621d029681d4457ab5fc56ec7c7464a1&title=全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定&type=decision> [2026/7/7 確認]

国家法律法规データベース : 中华人民共和国网络安全法 (改正後法文) <https://flk.npc.gov.cn/detail?fileId=&id=2c909fdd678bf17901678bf8276f093d&title=中华人民共和国网络安全法&type=decision> [2026/7/7 確認]

※ 156 CAC : 全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定 https://www.cac.gov.cn/2025-10/29/c_1763461514768457.htm [2026/7/7 確認]

※ 157 China Briefing : China Cybersecurity Law Amendment in Effect January 1, 2026 <https://www.china-briefing.com/news/china-cybersecurity-law-amendment/> [2026/7/7 確認]

Mayer Brown : China Finalises Amendments to the Cybersecurity Law What Businesses Need to Know Before 1 January 2026 <https://www.mayerbrown.com/en/insights/publications/2025/12/china-finalises-amendments-to-the-cybersecurity-law-what-businesses-need-to-know-before-1-january-2026> [2026/7/7 確認]

Fangda Partners : China's Cybersecurity Law Amendment - Key Changes and Compliance Recommendations https://www.fangdalaw.com/en/content/print32_17612.html [2026/7/7 確認]

※ 158 CAC : 人脸识别技术应用安全管理办法 https://www.cac.gov.cn/2025-03/21/c_1744174262156096.htm [2026/7/7 確認]

※ 159 CAC : 国家网络身份认证公共服务管理办法 https://www.cac.gov.cn/2025-05/23/c_1749711107835487.htm [2026/7/7 確認]

※ 160 Australian Government : Cyber Security (Ransomware Payment Reporting) Rules 2025 <https://www.legislation.gov.au/>

F2025L00278/asmade/text [2026/6/11 確認]

※ 161 Australian Government Department of Home Affairs : FACTSHEET: Mandatory ransomware and cyber extortion payment reporting is active from 30 May 2025 <https://www.homeaffairs.gov.au/cyber-security-subsite/files/factsheet-ransomware-payment-reporting.pdf> [2026/6/11 確認]

※ 162 本白書では 1 豪ドル 114 円として換算している。

※ 163 Australian Taxation Office : Penalty units <https://www.ato.gov.au/individuals-and-families/paying-the-ato/interest-and-penalties/penalties/penalty-units> [2026/6/11 確認]

※ 164 https://cert.gov.lk/wp-content/uploads/policies/National_Cyber_Security_Strategy_of_Sri-Lanka.pdf [2026/6/11 確認]

※ 165 <https://www.apcert.org/> [2026/6/11 確認]

※ 166 <https://www.first.org/> [2026/6/11 確認]

※ 167 https://ago.gov.to/cms/images/LEGISLATION/PRINCIPAL/2025/2025-0037/CybersecurityAct2025_1.pdf [2026/6/11 確認]

※ 168 本白書では 1 バアンガドル 68 円として換算している。

※ 169 CSA : Plans For Establishment Of Cyber Resilience Centre To Provide Support To Organisations <https://www.csa.gov.sg/news-events/press-releases/plans-for-establishment-of-cyber-resilience-centre-to-provide-support-to-organisations/> [2026/6/11 確認]

※ 170 APCERT : Member Teams <https://www.apcert.org/about/structure/members.html> [2026/6/11 確認]

※ 171 APCERT : APCERT CYBER DRILL 2025 "When Ransomware Meets Generative AI" https://www.apcert.org/documents/pdf/APCERT_Drill_2025_Press_Release.pdf [2026/6/11 確認]

※ 172 APCERT : Documents <https://www.apcert.org/documents/index.html> [2026/6/11 確認]

※ 173 <https://www.cyber.gov.au/> [2026/6/11 確認]

※ 174 <https://krcert.or.kr> [2026/6/11 確認]

※ 175 <https://www.cybersecurity.my/> [2026/6/11 確認]

※ 176 <https://cert.gov.lk/> [2026/6/11 確認]

※ 177 CSA : CERTS From ASEAN Member States Gather In Singapore For The First Time To Participate In The ASEAN CERT Incident Drill (ACID) <https://www.csa.gov.sg/news-events/press-releases/certs-from-asean-member-states-gather-in-singapore-for-the-first-time-to-participate-in-the-asean-cert-incident-drill-acid/> [2026/6/11 確認]

※ 178 ISO : ISO/IEC JTC 1 <https://www.iso.org/committee/45020.html> [2026/7/31 確認]

※ 179 JISC : JISC について <https://www.jisc.go.jp/jisc/index.html> [2026/7/31 確認]

※ 180 ITU : SG17: Security <https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx> [2026/7/31 確認]

※ 181 IETF:Security Area <https://wiki.ietf.org/group/sec> [2026/7/31 確認]

※ 182 TCG : Welcome to Trusted Computing Group <https://trustedcomputinggroup.org/work-groups/regional-forums/japan> [2026/7/31 確認]

※ 183 ISO : ISO/IEC JTC 1/SC 27 Information security, cyber-security and privacy protection <https://committee.iso.org/home/jtc1sc27> [2026/7/31 確認]

※ 184 <https://www.jisc.go.jp/international/iso-prcs.html> [2026/7/31 確認]

※ 185 https://www.jipdec.or.jp/project/smpo/u71kba000000jigv-att/27000family_20260518.pdf [2026/7/31 確認]

※ 186 経済産業省 : サイバー・フィジカル・セキュリティ対策フレームワーク <https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html> [2026/7/31 確認]

付録・索引



第21回 IPA

「ひろげよう情報セキュリティ コンクール」2025 受賞作品

「ひろげよう情報セキュリティコンクール」は、情報セキュリティをテーマとした作品制作を通じて、全国における児童・生徒等の情報セキュリティに関する意識醸成と興味喚起を図ることを目的として開催しています。ここでは、全2,184点の応募作品の中から、IPAが授与している最優秀賞と優秀賞をご紹介します。

最優秀賞

油断禁物



長浜 ちひろさん
立川女子高等学校

優秀賞

そのパスワード大丈夫？



脇 玲美奈さん
静岡市立安東小学校

視線の先



小磯 凜さん
静岡県立三島南高等学校

作り分けよう
使い分けようパスワード



宮城 優佳さん
白百合学園中学校

数字

OAPT	21
2024 年オンライン安全修正(ソーシャルメディア最低年齢)法(Online Safety Amendment (Social Media Minimum Age) Act 2024)	94
8Base	110

A

Active Directory	34
AI(Artificial Intelligence: 人工知能)	9, 69, 89, 110, 122, 160
AI エージェント	70, 80, 82
AI ガバナンス	76
AI 事業者ガイドライン	70, 76
AI システム	77, 81
AI セーフティ	76
AI セーフティ・インスティテュート(AISI: AI Safety Institute)	76, 79, 85
AI セーフティサミット	76, 162
AI の悪用	71, 82, 90
AI のセキュリティ	79, 111
AI のセキュリティ確保のための技術的対策に係るガイドライン	85, 111
AI のリスク	70
AI 法	78, 110
AI モデル	69, 80
Akira	9, 172
America's AI Action Plan	77
ANEL	28
APCERT(Asia Pacific Computer Emergency Response Team: アジア太平洋コンピュータ緊急対応チーム)	184, 186
APT29	173
APT(Advanced Persistent Threat) 攻撃	27, 120
ArcaneDoor	38
ASM(Attack Surface Management) 導入ガイド	33
Attack Surface Management(ASM)	24, 33

C

C&C(Command and Control) サーバー	27, 35
-------------------------------	--------

CCRA(Common Criteria Recognition Arrangement)	191
ChatGPT	69, 72, 90
CIOP(CIOp、Clop)	9, 38
Claude Mythos	83, 161
ClickFix	33, 46, 50
CRYPTREC(Cryptography Research and Evaluation Committees)	142
CSIRT(Computer Security Incident Response Team)	31, 41, 123, 176, 183
CVE(Common Vulnerabilities and Exposures: 共通脆弱性識別子)	38, 79, 176
CVSS(Common Vulnerability Scoring System: 共通脆弱性評価システム)	40, 176

D

DDoS 攻撃	10, 17, 34, 172
DIGITAL POSITIVE ACTION	95
DNS(Domain Name System)	10, 36, 41, 177
DRDoS(Distributed Reflection Denial of Service) 攻撃	17

E

Earth Kasha	28
EchoLeak	80
EDR(Endpoint Detection and Response)	22, 33, 38
ENISA(The European Union Agency for Cybersecurity)	8, 128, 164, 172, 175
ERAB サイバーセキュリティトレーニング	130
EU AI Act	77, 173
EUCC(European Common Criteria-based cybersecurity certification scheme)	180
EUVD(European Vulnerability Database)	176
EU サイバーセキュリティ法(CSA: Cybersecurity Act)	175

F

FIMI(Foreign Information Manipulation and Interference: 外国による情報操作と干渉)	91
FOG	9

G

General-Purpose AI Code of Practice(汎用 AI の行動規範)	78
Global Cybersecurity Camp(GCC)	128

I

IEC(International Electrotechnical Commission : 国際電気標準会議)	188
IEEE(The Institute of Electrical and Electronics Engineers, Inc.)	188
IETF(Internet Engineering Task Force)	143, 188
International AI Safety Report 2026	162
International Cybersecurity Challenge(ICC)	128
IoC(Indicator of Compromise : 侵害指標)	25, 31, 119
IoT	35, 37, 117, 133, 163
ISMAP-LIU(イスマップ・エルアイユー : ISMAP for Low-Impact Use)	140
ISMAP 管理基準	139
ISMAP 等クラウドサービスリスト	139
ISO(International Organization for Standardization : 国際標準化機構)	188
ISO/IEC 15408(Common Criteria)	138, 191
ISO/IEC 27000 ファミリー	189
ISO/IEC JTC 1/SC 27	116, 189
ITU-T(International Telecommunication Union Telecommunication Standardization Sector : 国際電気通信連合 電気通信標準化部門) ..	188
IT 製品の調達におけるセキュリティ要件リスト ..	138
IT セキュリティ評価及び認証制度(JISEC : Japan Information Technology Security Evaluation and Certification Scheme)	138

J・K

J-CRAT(Cyber Rescue and Advice Team against targeted attack of Japan : サイバーレスキュー隊)	120
JTC 1(Joint Technical Committee 1 : 第一合同技術委員会)	188

KEV(Known Exploited Vulnerabilities : 既知の悪用された脆弱性) カタログ	38, 41, 170
---	-------------

L

LAMEHUG	160
Living Off The Land(LOTL) 戦術	28, 161
LLM(Large Language Model : 大規模言語モデル)	69, 75, 79, 82

M

Microsoft Office	30
MirrorFace	28

N・O

NIS 2 指令(Network and Information Systems Directive 2)	13, 174, 177
NoName057(16)	34
NOOPDOOR	29
NVD(National Vulnerability Database : 国家脆弱性データベース)	41, 83
N デイ攻撃	39
Operational Relay Box(ORB : 中継装置) ..	28, 29

P・Q

PhaaS(Phishing as a Service)	11, 172
PhantomRaven	81
Phobos	110
Project YATA-Shield	84, 123
PromptLock	160
PSTI 法(Product Security and Telecommunications Infrastructure Act)	117, 136, 163
Qilin	9, 21, 172

R

RaaS(Ransomware as a Service)	19, 21
Ransomhouse	23

S

SaaS	11, 140
SafePay	172
Salt Typhoon	29, 40, 161

SBOM (Software Bill of Materials : ソフトウェア 部品表)	117, 137, 169
Scattered Lapsus\$ Hunters	30
SECURITY ACTION	116, 145, 150, 152
slop (スロップ)	74, 81
SMS	15, 46
Spamouflage	90

T・U

TCG (Trusted Computing Group)	189
The NIST Cybersecurity Framework (CSF) 2.0	116, 170
TS 5689	116, 191
U.S. Cyber Trust Mark	137, 163, 170

V

Volt Typhoon	28, 161
VPN	16, 20, 23, 27, 119

あ

アイデンティティ管理	191
アイランドホッピング攻撃	31
悪意ある情報	88, 90
アクセス・無害化	63, 107, 109
暗号資産	162
一般財団法人日本サイバー犯罪対策センター (JC3 : Japan Cybercrime Control Center)	109
一般社団法人 JPCERT コーディネーションセンター (JPCERT/CC : Japan Computer Emergency Response Team Coordination Center)	26, 38, 41, 121, 186
インド太平洋地域向け日米 EU 産業制御システムサ イバーセキュリティウィーク	164
インフォスティーラー (Infostealer)	9, 46, 50
エクスプロイト	9, 12
エネルギー・リソース・アグリゲーション・ビジネスに 関するサイバーセキュリティガイドライン	130, 136
遠隔操作	27, 49, 52
遠隔操作マルウェア	23
欧州刑事警察機構 (Europol : European Union Agency for Law Enforcement Cooperation)	34, 110, 164, 176

欧州サイバーセキュリティ認証フレームワーク (ECCF : European Cybersecurity Certification Framework)	176, 180
オンライン安全法 (Online Safety Act)	94

か

技術情報管理認証制度	118
技術流出対策ガイダンス	68
業界別サイバーレジリエンス強化演習 (CyberREX : Cyber Resilience Enhancement eXercise by industry)	129
クラウドサービス	22, 25, 139, 190
クレジットカード	47, 66
グローバル・サイバーセキュリティ・ラベリング・イニ シアティブ (GCLI : Global Cybersecurity Labeling Initiative)	137
経済安全保障経営ガイドライン	68
経済安全保障重要技術育成プログラム (通称、K Program)	86, 94, 118
経済安全保障推進法	66
経済安全保障に関する産業・技術基盤強化アクション プラン	67
公開鍵暗号	141, 143
攻撃対象領域 (アタックサーフェス)	24, 33, 38, 81
工場システムにおけるサイバー・フィジカル・セキュリ ティ対策ガイドライン	117
公的個人認証サービス (JPKI : Japanese Public Key Infrastructure)	111
コードインジェクション	80
国立研究開発法人情報通信研究機構 (NICT : National Institute of Information and Communications Technology)	17, 66, 111
国連サイバー犯罪防止条約 (UNCC : United Nations Convention against Cybercrime)	161
誤情報	75, 88
国家安全保障戦略	62, 106
国家サイバー統括室 (NCO : National Cybersecurity Office)	27, 63, 107
国家支援型 APT 攻撃	28, 120
コンピュータ不正アクセス対策基準	44

さ

サイバー安全保障分野での対応能力の向上に向けた提言	62
サイバーインフラ事業者に求められる役割等に関するガイドライン	117
サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項	62, 106
サイバー警察局	110
サイバー情報共有イニシアティブ(J-CSIP: Initiative for Cyber Security Information sharing Partnership of Japan)	119
サイバーセキュリティ2025(2024年度年次報告・2025年度年次計画)	106, 123
サイバーセキュリティお助け隊サービス	116, 147, 151
サイバーセキュリティ企画演習(CyberSPEX: Cyber Security Planning Exercise)	129
サイバーセキュリティ基本法	106, 112
サイバーセキュリティ経営ガイドライン	32
サイバーセキュリティ人材	118, 122, 148
サイバーセキュリティ人材フレームワーク2026	124
サイバーセキュリティ戦略	62, 106
サイバーセキュリティネクサス(CYNEX: Cybersecurity Nexus)	17
サイバー対処能力強化法	62, 106
サイバー特別捜査部	110
サイバー・フィジカル・セキュリティ対策フレームワーク(CPSF)	115, 191
サイバーブループリント(Cyber Blueprint)	179
サイバーレジリエンス法(CRA: Cyber Resilience Act)	174, 178
サイバー連帯法(CSoA: Cyber Solidarity Act)	179
サプライチェーン	8, 24, 31, 115, 145, 160
サプライチェーン強化に向けたセキュリティ対策評価制度(SCS 評価制度)	116, 145, 148, 150
サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3: Supply-Chain Cybersecurity Consortium)	116
サプライチェーン・リスク	8, 84, 177
サポート詐欺	49, 52, 71, 110
産業サイバーセキュリティ研究会	114

産業サイバーセキュリティセンター(ICSCoE: Industrial Cyber Security Center of Excellence)	128, 164
ジェイルブレイク	80, 169
事業継続計画(BCP: Business Continuity Plan)	23, 26, 31, 36, 129
次世代アンチウイルス(NGAV: Next Generation Anti-Virus)	38
実践的サイバー防御演習(CYDER: Cyber Defense Exercise with Recurrence)	165
シャドー AI	85, 123
重要インフラ	34, 63, 84, 108, 167, 177
重要インフラのサイバーセキュリティ対策のための統一基準(案)	108
重要インフラのサイバーセキュリティに係る行動計画	108
重要経済安保情報保護活用法	66
重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針	64
重要電子計算機に対する不正な行為による被害の防止に関する法律(サイバー対処能力強化法)	62
情報処理安全確保支援士(登録セキスペ)	124, 125, 151
情報セキュリティ安心相談窓口	46
情報セキュリティ早期警戒パートナーシップ	41, 120
情報セキュリティマネジメント試験	125
情報セキュリティマネジメントシステム(ISMS: Information Security Management System)	189
情報戦	90, 95
情報操作型サイバー攻撃	88, 90
情報流通プラットフォーム対処法	94
情報漏えい	11, 15, 42
新型コロナウイルス	93
人工知能関連技術の研究開発及び活用の推進に関する法律(AI 法)	78, 110
人工知能基本計画	79
侵入型ランサム攻撃	19, 21, 23
水平展開	25, 27
スロップスクワッティング	81
制御システム	129, 164

制御システム向けサイバーセキュリティ演習 (CyberSTIX : Cyber Security practical eXercise for industrial control system)	130	データ三法	181
脆弱性	8, 24, 37, 121, 170, 176	データ侵害	9, 11, 172
生成 AI (Generative AI)	69, 92, 110	データセキュリティ	111
政府機関等のサイバーセキュリティ対策のための統一基準	138	適合ラベル	133
政府機関等の対策基準策定のためのガイドライン	27, 117, 135	デジタルオペレーショナルレジリエンス法 (DORA : Digital Operational Resilience Act)	174
政府情報システムのためのセキュリティ評価制度 (Information system Security Management and Assessment Program : 通称、ISMAP (イ スマップ))	139	デジタルオムニバス規則案	173
セキュア・ソフトウェア開発フレームワーク (SSDF : Secure Software Development Framework)	117	デジタルサービス法 (DSA : Digital Services Act)	93, 174
セキュア・バイ・デザイン	32, 117	デジタル社会の実現に向けた重点計画	111
セキュリティ・キャンプ	118, 127	デジタル署名	175, 190
セキュリティ・クリアランス制度	66	デジタルスキル標準 (DSS)	124
セキュリティ要件適合評価及びラベリング制度 (JC- STAR)	32, 117, 133, 163	デジタルトラスト	165
ゼロデイ攻撃	37	デバイス・コード・フィッシング (Device Code Phishing)	9
ゼロトラスト	84, 166	特別社会基盤事業者	63
組織における内部不正防止ガイドライン	44		
		な	
た		内閣サイバーセキュリティセンター (NISC : National center of Incident readiness and Strategy for Cybersecurity)	62
ダークウェブ	20, 26, 37	内部不正	32, 42
第 14 次 5 ヵ年計画	180	ナラティブ	90, 95
対ランサムウェア・イニシアチブ (CRI : Counter Ransomware Initiative)	162	なりすまし	42, 71, 162
耐量子計算機暗号 (PQC : Post-Quantum Cryptography)	142, 168	二重の脅迫 (二重恐喝)	16, 19, 23
地方公共団体における情報セキュリティポリシーに関 するガイドライン	113	偽・誤情報	75, 88
中核人材育成プログラム	128	偽情報	88
中華人民共和国サイバーセキュリティ法	181, 183	偽のウイルス感染警告	49, 52, 110
中小企業の情報セキュリティ対策ガイドライン	116, 147	日 ASEAN サイバーセキュリティ政策会議	117, 164
中小企業のためのセキュリティ人材確保・育成の実 践ガイドブック	118, 150	日 ASEAN サイバーセキュリティ能力構築センター (AJCCBC : ASEAN-Japan Cybersecurity Capacity Building Centre)	164
ディープフェイク	92, 94, 110, 160	日 ASEAN 能力向上プログラム強化プロジェクト	165
ディスインフォメーション (Dis-information)	88	日・EU サイバー対話	164
		日英サイバー対話	163
		日米サイバー対話	163
		日本 AISI	76, 79, 81, 85
		日本産業標準調査会 (JISC : Japanese Industrial Standards Committee)	188
		認知戦	88, 91, 95
		ネットワーク貫通型攻撃	27, 29, 119
		ノーウェアランサム	19, 23

は

ハーベスト攻撃(HNDL 攻撃 : Harvest Now, Decrypt Later Attack)	142
ハイブリッド型サイバー攻撃	88
ハイブリッド脅威	91
ハイブリッド戦争	90
ハクティビスト	10, 12, 34, 173
バックドア	29, 161
ばらまき型の攻撃	19
ハルシネーション	71, 75, 81
汎用 AI (General-Purpose AI)	78, 175
標的型攻撃	20, 27, 119
広島 AI プロセス	77
ファクトチェック	91, 94
フィッシング	11, 14, 46, 110, 172
フェイクニュース	89
不正アクセス	16, 22, 27, 39, 42
不正送金	15, 49, 52, 133
不正ログイン	11, 46, 47
プロテクションプロファイル	138
フロンティア AI	84
プロンプトインジェクション	79, 85, 169
米国国立標準技術研究所 (NIST : National Institute of Standards and Technology)	24, 83, 143, 170
米国サイバーセキュリティ・インフラストラクチャセキュリティ庁 (CISA : Cybersecurity and Infrastructure Security Agency)	24, 38, 117, 168
米国連邦捜査局 (FBI : Federal Bureau of Investigation)	12, 71, 111, 166
ボイスフィッシング (ビッシング)	14, 30
ボットネット	35, 92

ま

マイクロセグメンテーション	25
マルインフォメーション (Mal-information)	88
ミスインフォメーション (Mis-information)	88
無人航空機システム (UAS : Unmanned Aircraft Systems)	170
モデル抽出	80, 169

ら

ランサムウェア	9, 16, 19, 110, 162
ランサム攻撃	9, 16, 19, 37, 110, 148, 172
リアルタイムフィッシング	47
リークサイト	20, 24, 26
リスクベースアプローチ	167
リフレクション攻撃	17
リモートデスクトップ	16, 20, 23, 149

著作・製作 独立行政法人情報処理推進機構（IPA）

編集責任 大川 龍郎 清水 督史 小山 明美
涌田 明夫 白石 歩 井上 佳春

執筆者 IPA
伊藤 彰朗 伊藤 さやか 伊藤 忠彦 伊藤 吉史 井上 佳春
入来 星衣 大久保 直人 大海 健太 小川 賢一 加賀谷 伸一郎
勝川 雅義 金山 栄一 金子 成徳 神谷 健司 亀山 友彦
川口 修司 神田 雅透 北爪 亮太郎 儀部 頼之 桐淵 直人
古閑 みなみ 小山 明美 酒井 崇行 榊原 七美 佐藤 みゆき
渋谷 環 白石 歩 関 鈴良 関根 大助 高橋 慎治
武田 泰貴 辻 初実 辻 宏郷 豊田 亮子 長迫 智子
中村 友亮 夏目 典大 新山 雄大 西尾 秀一 芳賀 政伸
平本 健二 福井 章人 松本 穂乃花 室賀 直来 安田 進
籾口 春南 山下 恵一

（敬称略）

ネット教育アナリスト 尾花 紀子

一般社団法人日本クラウドセキュリティアライアンス 諸角 昌宏

一般社団法人 JPCERT コーディネーションセンター 米澤 詩歩乃

協力者 IPA
安藤 康浩 板橋 博之 江島 将和 大川 龍郎 大澤 淳
小川 隆一 沖田 孝裕 奥村 元 小野塚 直人 甲斐 成樹
鎌田 林太郎 釜谷 誠 菊池 秀一 岸野 照明 北村 弘
桑名 利幸 白井 綾 銭谷 謙吾 高田 早苗 高橋 将
高村 博紀 高柳 大輔 土屋 正 中島 尚樹 西原 栄太郎
二村 和明 肱岡 七愛 平原 裕貴 松島 伸彰 松田 修平
宮崎 卓行 谷澤 昭紀

サイバーレスキュー隊 J-CRAT（ジェイ・クラート）

AISI 事務局 戦略企画グループ

（敬称略）

一般財団法人日本情報経済社会推進協会 大熊 三恵子

NRI セキュアテクノロジーズ株式会社 北原 幸彦

一般財団法人日本情報経済社会推進協会 崎村 夏彦

一般社団法人 JPCERT コーディネーションセンター 染川 夕貴

京都外国語大学 共通教育機構 土屋 貴裕

NTT 株式会社 永井 彰

国立研究開発法人情報通信研究機構 中尾 康二

デジタル庁 戦略・組織グループ セキュリティチーム 中村 元洋

総務省 サイバーセキュリティ統括官室

経済産業省 商務情報政策局 サイバーセキュリティ課

2025年度は、同年5月に成立した「サイバー対処能力強化法及び同整備法」により、能動的サイバー防御を実現する体制の整備が着々と進められ、日本の能動的サイバー防御が実装段階へ移行する転換点となった年であったことから、サブタイトルの前半を「サイバー防御新時代」としました。新時代といえ、その一方でAIの悪用によるサイバー攻撃の脅威が顕在化し、将来的に量子コンピューターによる暗号解読のリスクが懸念されることから、耐量子計算機暗号(PQC)への移行が世界中で本格化する等、「進化」した先端技術が「諸刃の剣」となって我々の喉元に迫ってきた年でもありました。進化を続ける先端技術は、脅威であると同時に、我々の生活を便利にしたり、従来は不可能だった問題解決を実現したりするといった二面性を持つものです。それらに積極的に対応していく必要があるとの考えから、サブタイトルの後半を「諸刃の進化に備えよ」としました。

IPAは、日本の能動的サイバー防御の取り組みの一端を担うとともに、サイバー脅威に対して組織・個人によるセキュリティ対策の一助となるよう、今後とも努めていきます。

編集子

- ・ 本白書の引用、転載については、IPA Web サイトの「書籍・刊行物等に関するよくあるご質問と回答」(<https://www.ipa.go.jp/publish/faq.html>)に掲載されている「2. 引用や転載に関するご質問」をご参照ください。ただし、出典元がIPA 以外であり、かつ IPA が編集、作成を行った図表については、本白書からの転載・改変について IPA は許諾ができません。転載・改変について IPA が許諾できない図表は以下の様に出版を記載しています。

例「(出典)《組織名等》『《文書名等》』を基に IPA が編集」

例「(出典)《組織名等》『《文書名等》』を基に IPA が作成」

また、出典元がIPA 以外であり、かつ IPA が本白書で引用している図表についても、転載・改変について IPA は許諾ができません。以下の様に記載している図表の転載・改変の可否については、出典元をご確認ください。

例「《組織名等》『《文書名等》』」

上記の例にある《組織名等》《文書名等》には実際の出典元組織名、文書名が記載されます。

なお、これは、著作権法で定められた本白書からの引用を妨げるものではありません。

- ・ 本白書は 2025 年度の出来事を主な対象とし、執筆時点の情報に基づいて記載しています。
- ・ 電話によるご質問、及び本白書に記載されている内容以外のご質問には一切お答えできません。あらかじめご了承ください。
- ・ 本白書に記載されている会社名、製品名、及びサービス名は、それぞれ各社の商標または登録商標です。本文中では、TM または [®] マークは明記していません。
- ・ 本白書に掲載しているグラフ内の数値の合計は、小数点以下の端数処理により、100% にならない場合があります。

情報セキュリティ白書 2026

サイバー防御新時代：諸刃の進化に備えよ

2026 年 10 月 19 日 PDF 版 第 1 版発行

企画・著作・制作・発行 独立行政法人情報処理推進機構 (IPA)

〒113-6591

東京都文京区本駒込2丁目28番8号

文京グリーンコートセンターオフィス 16 階

URL <https://www.ipa.go.jp/>

電話 03-5978-7503

E-Mail spd-book@ipa.go.jp

表紙デザイン／
本文DTP・編集

伊藤 千絵、久磨 公治、涌田 明夫、北林 俊平