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



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

「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まいりました。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 齊藤 裕

目次

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

2026

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

	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 ヵ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1章
国内外のサイバー脅威の動向

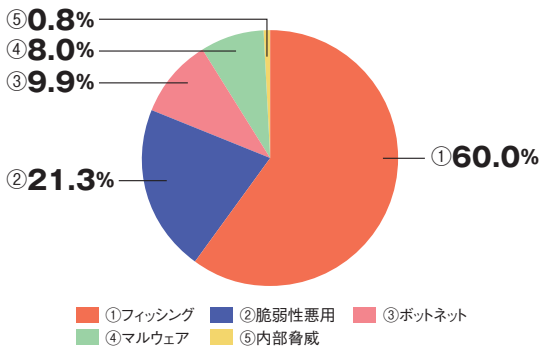
2025 年度も、地政学的な緊張の高まり、国家間の対立を背景に、社会インフラ等を標的とした国家支援型のサイバー攻撃が観測された。また、民間企業の事業継続を揺るがす侵入型ランサム攻撃も引き続き発生した。更に 2025 年度には、AI が急速に普及した一方で、攻撃者による悪用も進み、攻撃の自動化等、様々な段階で AI が用いられるようになった。SNS を悪用した巧妙な騙しの手口による金銭の詐取も横行した。本章では、国内外で観測された主なインシデント、攻撃手法、対策について解説する。

1.1 2025年度に観測されたインシデント状況

本節では 2025 年度に観測された世界と日本におけるサイバーセキュリティインシデントの発生状況について概説する。

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

本項では、多年度にわたって継続的に関連事象の情報を収集・観測している報告書等を主に参照し、世界におけるサイバーセキュリティインシデントの発生状況を概説する。



■図 1-1-1　初期侵入手段
(出典)ENISA「ENISA Threat Landscape 2025」を基に IPA が編集

(1) 注目すべき世界的な傾向

2025 年は、外部に公開されているアプリケーションの脆弱性を起点とする侵入が引き続き主要な脅威であった。米国の International Business Machines Corporation (以下、IBM 社) のサイバーセキュリティ調査部門である IBM X-Force が公開している年次レポートである「X-Force Threat Intelligence Index 2026[※1]」では、同部門が確認した主な初期侵入手段において、脆弱性や設定ミスを狙った「外部に公開されたアプリケーションの悪用」が 40% と最も割合が高く、前年比 44% 増であったという。また、公開された脆弱性の 56% は認証なしで悪用可能であったとしている。

欧州連合 (EU：European Union) のサイバーセキュリティ専門機関である ENISA (The European Union Agency for Cybersecurity) が公開している年次レポートである「ENISA Threat Landscape 2025[※2]」(以下、ENISA 年次レポート) では、「フィッシング」に次いで「脆弱性悪用」が初期侵入手段の 21.3% を占め (図 1-1-1)、脆弱性の公開後数日で攻撃に悪用する広範な攻撃キャンペーンが継続したと指摘している。

これらの動向は、既知の脆弱性の迅速な悪用が、初期侵入の主要な手段であり続けていることを示している。

また、2025 年は、サプライチェーン及びサードパーティー経由の侵害リスクが一段と顕在化した年でもあった。ENISA 年次レポートでは、「サプライチェーン・リスク」が観測事案の脅威カテゴリ分布の 10.6% を占め、攻撃者がサードパーティープロバイダーや各種依存関係を介した間接経路を積極的に利用していると指摘している。加えて、IBM 社は、「主要なサプライチェーン及びサードパーティー侵害」が過去 5 年で約 4 倍に増加し、攻撃者が横展開 (組織内への侵入拡大) を行う際の起点として、「ベンダー」「オープンソース依存関係」「ID 連携」「ソフトウェア開発プロセスを自動化する CI/CD」、そして「SaaS 連携に伴う OAuth 許可、API トークン、クラウド間の信頼関係」のすべてが標的として狙われていると報告している[※3]。これらは、自組織単体の防御に加え、委託先

や利用しているサービス等の依存関係を含めた管理の重要性が高まっていることを示している。

一方、Microsoft Corporation（以下、Microsoft 社）の「Microsoft Digital Defense Report 2025[※4]」（以下、Microsoft 社年次レポート）では、攻撃者が「侵入する」のではなく「ログインする」方向へ移行していると指摘している。認証情報等を窃取するマルウェアである「インフォスティーラー（Infostealer）」により収集された認証情報やトークンが売買され、その後のランサム攻撃、情報窃取、恐喝につながる事例が見られたという。加えて、正規の「デバイスコード認証」機能を悪用して、利用者自身に攻撃者の用意した認証セッションへログインさせる手口である「デバイス・コード・フィッシング（Device Code Phishing）」によって不正ログインにつなげる手口も拡大しているという。Microsoft 社年次レポートでは、こうした事象の 93% が 2024 年 7 月～ 2025 年 6 月のうちの後半の半年に集中したとしており、認証基盤を標的とした攻撃が急速に拡大したことを示している。

AI に関連した動向としては、英国の政府機関である英国国家サイバーセキュリティセンター（NCSC：National Cyber Security Centre）が「NCSC Annual Review 2025[※5]」（以下、NCSC 年次レポート）において、AI を活用した攻撃が、フィッシング文面の生成にとどまらず、標的調査、脆弱性調査、エクスプロイト開発（脆弱性を悪用するためのコードやツール、手法の開発）、初期アクセス、基本的なマルウェア生成、窃取データの処理等、より広い攻撃工程に及びつつあると指摘している。また、AI がサイバー侵入作戦の一部をより効果的かつ効率的にし、脅威の頻度と強度を高めると評価している。ENISA 年次レポートでも、2025 年初頭までに AI 支援型フィッシングが、世界で観測されたソーシャルエンジニアリング攻撃活動の 8 割超を占めたと指摘している。これらは、AI が攻撃の自動化及び効率化を促進し、多様な攻撃手法の実行可能性を高めていることを示唆している。

国家の関与が指摘されるサイバー活動については、引き続き、平時から継続的に観測される主要な脅威となっている。Microsoft 社年次レポートでは、国家支援型とされる活動が通信、研究、学術分野へ標的を拡大し、サイバー諜報を通じて従来の諜報活動を補完していると指摘している。NCSC 年次レポートでは、中国による広範な分野・組織を標的とした活動、ロシアによる NATO 諸国への活動、イランによる中東情勢に関連した活動、北朝鮮による資金獲得及び情報収集を挙げている。これらの関与が指摘されるサイバー活動は、国家安全保障、外交及び経済安全保障に関連する分野が、引き続き重要な標的となっていることを示している。

(2) ランサム攻撃の状況

2025 年の世界におけるランサム攻撃の脅威は、攻撃件数の増加に加え、暗号化、データ窃取、事業停止を伴う深刻な被害が続く一方、身代金支払い額には低下傾向もうかがえる。

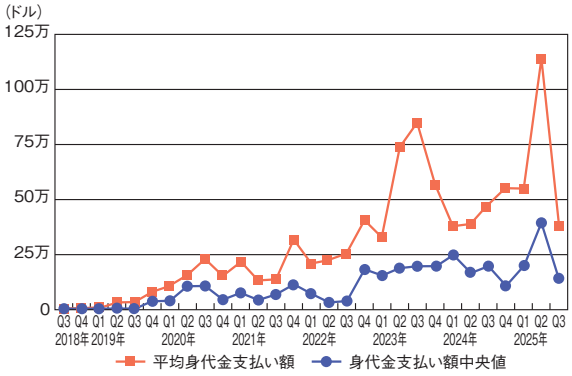
英国のサイバーセキュリティ企業である NCC Group は、傘下の Fox-IT とともに公表した「Annual Cyber Threat Intelligence Report 2025[※6]」において、2025 年の世界のランサム攻撃の件数が前年比 50% 増加し、主要な攻撃グループは「Qilin」「Akira」「ClOP」であったと分析している。また、攻撃対象の 28% を工業・産業部門が占めたこと、攻撃対象地域の 56% を北米が占めたこと等から、被害が特定の業種及び地域に集中する傾向も示されている。

ENISA 年次レポートによると、EU 域内組織を標的とするサイバー犯罪活動では「ランサムウェア」が 81.1%、「データ侵害」が 15.2% を占め、後者についてもランサム攻撃に起因するものとして記録されている。特に製造業では、「Akira」「Qilin」「FOG」等によるランサム攻撃により、事業継続に長期的な支障が生じた事例が確認されている。

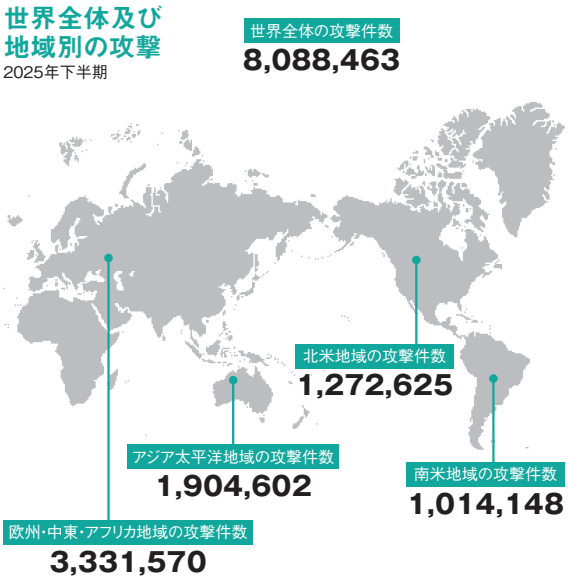
英国のサイバーセキュリティ企業である Sophos Ltd.（以下、Sophos 社）は、年次レポート「The State of Ransomware 2025[※7]」において、攻撃の 50% でデータ暗号化が発生し、暗号化被害を受けた組織の 28% ではデータ窃取も確認されたとしている。また、ランサム攻撃の被害を受けた組織の 49% がデータ復旧のため身代金を支払い、この割合は前年の 56% から 7 ポイント低下している。

一方で、攻撃件数や身代金の支払いの増加が、攻撃者の収益増にそのまま結び付いているわけではない。米国のブロックチェーン分析企業 Chainalysis Inc. は、2025 年の公表された被害組織数は 50% 増加したのに対し、ブロックチェーン上の身代金の支払い額が約 8.2 億ドル（1,312 億円[※8]）と前年比で約 8% 減少したと指摘している[※9]。サイバー恐喝事案へのインシデント対応を専門とする米国企業 Coveware Inc.（以下、Coveware 社）の調査報告[※10]でも、2025 年第 3 四半期の平均身代金支払い額が 37 万 6,941 ドル（6,031 万 560 円）と前四半期比 66% 減、中央値も 14 万ドル（2,240 万円）と前四

半期比 65% 減少したという（図 1-1-2）。これらの動向は、被害組織の支払い抑制の広がりに加え、インシデント対応能力の向上、法執行機関による摘発等により、攻撃者の収益化に一定の制約が生じていることを示している。



■図 1-1-2　四半期ごとの身代金支払い額
（出典）Coveware 社「Insider Threats Loom while Ransom Payment Rates Plummet」を基に IPA が編集



■図 1-1-3　DDoS 攻撃の地域別分布状況（2025 年下半期）
（出典）NetScout 社「DDoS Threat Intelligence Report Issue 16」を基に IPA が編集

(3) DDoS 攻撃の状況

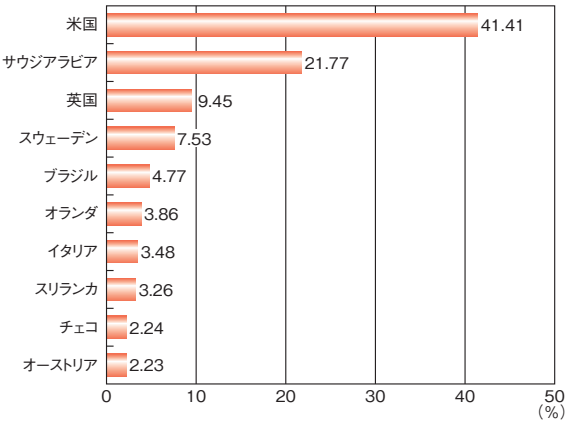
2025 年の世界における DDoS 攻撃は、件数及び規模の双方で高水準に推移し、インターネット基盤や重要サービスの可用性を脅かす主要なサイバー脅威であった。

米国のクラウドサービス及びセキュリティ企業である Cloudflare, Inc.（以下、Cloudflare 社）の「2026 Cloudflare Threat Report※11」（以下、Cloudflare 社年次レポート）では、2025 年に同社が観測した DDoS 攻撃が 4,710 万件に達し、前年から倍増したと報告している。また、同社は 2025 年に 1 時間あたり平均 5,376 件の DDoS 攻撃の影響を緩和しており、その内訳はネットワーク層 DDoS 攻撃が 3,925 件、HTTP DDoS 攻撃が 1,451 件であった。更に、11 月には 31.4Tbps に達する記録的な DDoS 攻撃も観測されており、攻撃の大規模化が進んでいるという。

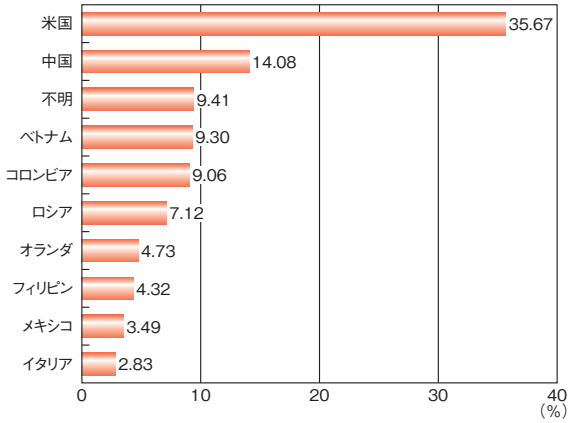
米国のサイバーセキュリティ企業である NetScout Systems, Inc.（以下、NetScout 社）の「DDoS Threat Intelligence Report Issue 16※12」によると、2025 年下半期だけで世界全体の DDoS 攻撃は、約 809 万件であったという。このうち、北米地域が約 127 万件、南米地域が約 101 万件、欧州・中東・アフリカ地域が約 333 万件、アジア太平洋地域が約 190 万件だった※13（図 1-1-3）。NetScout 社は、攻撃者が AI を攻撃の運用に取り込みつつ、NTP（Network Time Protocol）や DNS（Domain Name System）のような高価値のインターネット基盤サービスを継続的に標的化していると指摘している。

ENISA 年次レポートでは、DDoS 攻撃が、記録されたインシデント類型の約 76.7% を占め、最も多い類型であったと指摘している。また、同レポートは、DDoS 攻撃の多くがハクティビスト集団によるものだったと説明している。更に、ハクティビズム関連インシデントにおいて、EU 加盟国の Web サイトに対する DDoS 攻撃が 91.5% を占め、少なくとも 88 のハクティビスト集団が EU 加盟国組織を標的にしたと主張したという。

米国のデジタルトラスト関連企業である DigiCert, Inc.（以下、DigiCert 社）の調査※14 では、2025 年に観測された DDoS 攻撃対象国の上位 5 ヵ国は、米国（41.41%）、サウジアラビア（21.77%）、英国（9.45%）、スウェーデン（7.53%）、ブラジル（4.77%）であった（図 1-1-4）。発信元の上位 5 ヵ国は、米国（35.67%）、中国（14.08%）、



■図 1-1-4　DDoS トラフィックの攻撃対象国上位 10 ヵ国（2025 年）
（出典）DigiCert, Inc.「UltraDDoS Protect Annual Distributed Denial-of-Service Analysis, January–December 2025※14」を基に IPA が編集



■図 1-1-5　DDoS トラフィックの発信元国上位 10 ヵ国（2025 年）
（出典）DigiCert, Inc.「UltraDDoS Protect Annual Distributed Denial-of-Service Analysis, January–December 2025」を基に IPA が編集

不明（9.41%）、ベトナム（9.30%）、コロンビア（9.06%）であった（図 1-1-5）。

(4) フィッシングの状況

2025 年の世界のフィッシングは、件数面では高水準で推移しつつ、手口面では一段と高度化・多様化した。

フィッシング対策に関する国際的な業界団体である APWG（Anti-Phishing Working Group, Inc.）の報告※15 によれば、2025 年通年で観測されたフィッシング攻撃は 380 万件であり、2024 年の 376 万件から小幅に増加した。2025 年第 4 四半期は 85 万 3,244 件で、第 3 四半期及び第 2 四半期からは減少したものの、APWG は 2025 年のフィッシング攻撃の発生状況を「高水準だが安定的」と整理している。APWG 創設メンバーである Crane Authentication によれば、同年第 4 四半期に観測されたフィッシング攻撃の標的分野のうち、「ソーシャルメディア分野」と「SaaS ／ Web メール分野」がそれぞれ全体の 20.3% で最多となり、「通信分野」も 18.7% に上昇した。

また、ENISA 年次レポートでは、フィッシングを含むソーシャルエンジニアリングが主要な侵入手段であり、特定された初期侵入手段の約 60% をフィッシングが占めたとされた（p.8 の図 1-1-1）。更に、PhaaS（Phishing as a Service）、QR コード型フィッシング等が確認されているという。

一方、Microsoft 社年次レポートでも、同社のインシデント対応調査において、侵害の 28% がフィッシングまたはソーシャルエンジニアリングを通じて開始されたと指摘している。加えて、攻撃者が AI を悪意ある活動に利用し始めており、その例として、フィッシングキャンペーン、ディープフェイク生成、説得力の高い詐欺メッセージの作成を挙げている。このことは、AI がフィッシング及びソーシャルエンジニアリングの自動化及び巧妙化に用いられていることを示しており、これらの手口は、認証情報の窃取や不正ログインを起点として、その後の侵害拡大につながる点で特に注意を要する。

(5) 情報漏えいインシデントの状況

オランダのサイバーセキュリティ企業である Surfshark B.V.（以下、Surfshark 社）は、2025 年に世界で 4 億 2,570 万件のアカウントが侵害され、特に第 4 四半期は 1 億 4,150 万件を超え、第 1 四半期に記録された約 7,000 万件の 2 倍に達し、年間で最も多かったとしている※16。

米国で個人情報窃取等の被害者支援及びデータ侵害分析を行う米国の非営利団体である ITRC（Identity Theft Resource Center）の年次レポート※17 では、2025 年の公表されたデータ侵害等を 3,322 件とし、2024 年の 3,152 件から約 5% 増加したと指摘している。一方、被害通知数は 2024 年の約 13 億 6,710 万件から 2025 年の約 2 億 7,880 万件へ約 79% 減少した。この減少は、2025 年には Ticketmaster LLC や Change Healthcare Inc. の被害事例のような一つの事例で被害通知数を大きく押し上げる「超大型データ侵害」が存在しなかったためであり、情報漏えいの脅威の深刻度が低下したことを意味するものではない。ITRC では、2025 年には攻撃者がこうした「超大型データ侵害」から、高価値データを狙う、より頻繁で標的を絞った攻撃へ移行したと分析している。

また、EU 域内については、ENISA 年次レポートの分析では、侵害事案の 68.6% が、漏えいしたデータがサイバー犯罪フォーラムで販売される被害につながり、認証情報が窃取された割合は 8.9% としている。

Surfshark 社の調査では、北米は世界で最も影響を受けた地域であり、1 億 5,420 万件（世界全体の 36% 以上）の漏えいを記録し、そのうち 93% を米国が占めていた。欧州は、世界全体の 24% にあたる 1 億 390 万件が漏えいした。上位 5 ヵ国である、フランス（39%）、ドイツ（18%）、ロシア（12%）、英国（8%）、スペイン（4%）で、全体の 81% を占めた。アジアでは世界全体の 14% にあたる 5,930 万件が漏えいした。そのうちインド（49%）、ベトナム（12%）、インドネシア（5%）、中国（5%）、日本（5%）が上位となっている※16。

これらの動向は、情報漏えいインシデントの発生件数や脅威の深刻度は、引き続き高水準であるとともに、地域ごとに被害の偏在が見られることを示している。

(6) 地域別の傾向

以下では、南北アメリカ、アジア太平洋、欧州・中東・アフリカの各地域におけるサイバー脅威の動向を概観する。

(a) 南北アメリカ地域の傾向

南北アメリカ地域の中でも、米国は、世界で最も攻撃の標的となっている。Cloudflare 社年次レポートによると、この地域における脅威活動は、高度に洗練された国家支援型の攻撃者が攻撃前に不正なコードを重要インフラ等のシステムに仕込む「事前配置」と、ランサムウェア・エコシステムの蔓延が目立っているという。

南北アメリカ地域では、米国を中心に金銭目的のサイバー犯罪とランサム攻撃の被害規模が大きい。米国連邦捜査局（FBI：Federal Bureau of Investigation）のインターネット犯罪苦情センター（IC3：Internet Crime Complaint Center）が発表した「Internet Crime Report 2025[※18]」によれば、米国の 2025 年の通報件数は 100 万 8,597 件、報告損失額は 208 億 7,700 万ドル（3 兆 3,403 億 2,000 万円）に達した。

Google LLC のセキュリティ部門である Mandiant の調査による年次レポート「M-Trends 2026 Report[※19]」（以下、Mandiant レポート）では、南北アメリカ地域で初期侵入手段を特定できた事例のうち、「エクスプロイト」（脆弱性の悪用）が 28% で最多であり、「メールフィッシング」は 2024 年の 16% から 5% へ低下した。

Microsoft 社年次レポートでは、中南米について、ブラジル、アルゼンチン、メキシコ等がサイバー犯罪者に頻繁に標的とされ、同地域では認証情報窃取、フィッシング、ランサム攻撃が最も一般的な脅威であると指摘している。

(b) アジア太平洋地域の傾向

国際刑事警察機構（ICPO：International Criminal Police Organization、INTERPOL とも呼ばれる）の「INTERPOL Asia and South Pacific Cyber Threat Assessment Report 2025/2026[※20]」（以下、INTERPOL レポート）は、アジア及び南太平洋地域のサイバー犯罪が規模・複雑性・影響の面で拡大しており、ランサム攻撃、金融詐欺、ビジネスメール詐欺、データ侵害、情報窃取型マルウェアが広く悪用されていると指摘している。同調査によれば、ICPO 加盟国では、国内で把握された犯罪全体に占めるサイバー犯罪の割合が 30% を超える国が過半数に上っており、サイバー犯罪が各国の犯罪情勢において無視できない比重を占めるに至っている。

Mandiant レポートによると、2025 年に日本とアジア太平洋地域で実施した調査において、最も多く観測された初期侵入手段は「エクスプロイト」で 33%、次に多かったのが「盗まれた認証情報」で 23% だった。2024 年の調査結果でもこれらの順位は同様に 1 位と 2 位だったが、2024 年では「エクスプロイト」がはるかに多く、侵害の 64% を占めていた。2025 年で 3 番目に多かった手段は、「過去の侵害[※21]」の利用で 16% だった。

INTERPOL レポートによると、アジア及び南太平洋地域では、オンライン詐欺が主要なサイバー犯罪類型として深刻化している。回答国の約 3 分の 1 が、オンライン詐欺の認知件数について 1 万件超と回答しており、同犯罪が地域全体で大規模に発生している実態が示されている。また、カンボジア、ラオス、ミャンマー、フィリピン等では、国際組織犯罪グループが大規模な詐欺拠点を展開しており、その収益は年間約 400 億ドル（6 兆 4,000 億円）に達する可能性が指摘されている。

この動向は、サイバー空間を利用した詐欺と国際組織犯罪が一体化しつつあることを示すものである。そしてCloudflare 社年次レポートは、アジア太平洋地域では、高度な技術を用いたスパイ活動と、大規模な金融窃取が主要な脅威として顕在化しているという。更に、特に、海洋領域に関する情報収集活動に加え、将来的な紛争に備えた広範な監視や事前配置を可能にするため、基幹ネットワークインフラへの侵害が重視されていると述べている。

(c) 欧州・中東・アフリカ地域の傾向

欧州では、DDoS 攻撃、ランサム攻撃、国家が関与するサイバー活動、フィッシングを起点とする侵入が、サイバー攻撃の主要な特徴であった。Cloudflare 社年次レポートでは、特に、ハクティビスト活動は記録されたインシデントの約 8 割を占めたと指摘している。欧州では、主に DDoS 攻撃を用いて公共機関や銀行が標的にされているという。ENISA 年次レポートの分析では、標的分野は公共行政が 38.2% で最多であり、同分野の脅威はハクティビスト主導の DDoS 攻撃が 96.2% を占めた。公共行政への攻撃は、フランス（27%）、イタリア（26.3%）、ドイツ（16.2%）、スペイン（15.3%）、ポーランド（15.1%）に集中している。

一方、ENISA 年次レポートでの調査において、サイバー犯罪の領域では、EU 域内の組織を標的とするサイ

バー犯罪活動のうち、「ランサムウェア」が 81.1% を占めており、最も直接的な被害をもたらす脅威と位置付けられた。また、調査期間中には、EU 域内で活動する国家が関与する攻撃グループとして、46 種類の異なるグループが確認されたという。EU の NIS 2 指令（Network and Information Systems Directive 2）で重要分野とされるセクターの中で、国家が関与する攻撃グループに多く狙われた分野が、公共行政、交通、デジタルインフラ、エネルギー、医療であった。

Mandiant レポートによると、欧州・中東・アフリカ地域の初期侵入手段は「エクスプロイト」が 51%、「メールフィッシング」が 12%、「過去の侵害」が 9% であり、「メールフィッシング」は、世界平均を上回る割合を示した。

欧州に関して、ENISA 年次レポートでは、EU 域内で確認された中国関連の攻撃グループの活動について、公共行政、運輸、市民社会、デジタルインフラ等を主な標的としていると指摘している。特に、政府・外交機関、航空・海運業界、NGO・人権擁護団体、通信分野への関心が高く、食品製造業や農業研究機関を標的とする事例も例外的ながら確認されつつある。同レポートによると、これらの活動は、戦略的データ収集や知的財産の窃取を目的とする可能性があり、中国の「中国製造 2025」や「一帯一路」構想、欧州におけるその物流戦略と関連する技術・輸送ネットワークの獲得と整合すると考えられるという。また、市民社会への標的設定は、情報統制や反体制派・在外同胞ネットワークの監視といった中国国内の政治的優先事項を反映していると見られている。

(d) 脅威活動の地域横断性

Cloudflare 社年次レポートでは、地域ごとに完結する脅威という見方は、今日ではほとんど成り立たなくなっていると指摘している。攻撃の動機や背景は、特定の地域情勢、政治的対立、文化的要因に由来する場合が多いものの、実際の攻撃では、攻撃インフラの利用や標的の選定が国境や大陸を越えて行われることが少なくない。このような脅威活動の地域横断性は、サイバー脅威インテリジェンスにおける重要な分析課題となっている。多くの脅威アクターは、政治的・文化的な関心に基づいて特定地域に重点を置いて活動しているが、現代の脅威環境では、南北アメリカ地域、アジア太平洋地域、欧州・中東・アフリカ地域をまたいで攻撃活動が重複する傾向が強まっていると Cloudflare 社年次レポートでは主張している。こうした傾向は、国家関与型サイバー活動の観測状況にも表れている。表 1-1-1 に示すとおり、当該活動は南北アメリカ、アジア太平洋、欧州、及び中東・アフリカの各地域で観測されており、特定の地域内で完結せず、複数地域にまたがって展開していることがうかがえる。

これらの動向は、地域別の差異を踏まえつつも、攻撃インフラ及び脅威アクターの活動が国境や大陸を越えて連関していることを示している。

南北アメリカ		アジア太平洋		欧州		中東・アフリカ			
国	件数	国	件数	国	件数	国	件数	国	件数
米国	623	台湾	143	ウクライナ	277	イスラエル	603	南アフリカ	31
カナダ	51	韓国	126	英国	144	アラブ首長国連邦	166	エチオピア	20
ブラジル	24	インド	100	ポーランド	97	サウジアラビア	70	アンゴラ	9
ペルー	16	香港特別行政区	95	ドイツ	74	トルコ	70	ケニア	9
アルゼンチン	11	中国	49	フランス	72	イラク	67	ナイジェリア	8
コロンビア	10	オーストラリア	47	スペイン	61	ヨルダン	44	タンザニア	5
メキシコ	9	タイ	39	ロシア	60	レバノン	39	マリ	4
ドミニカ共和国	5	日本	38	イタリア	51	エジプト	32	ナミビア	4
チリ	4	シンガポール	33	アゼルバイジャン	35	イラン	27	ボツワナ	2
コスタリカ	3	インドネシア	32	ベルギー	30	モロッコ	26		

■表 1-1-1　国別の観測イベント件数
（出典）Microsoft 社「Microsoft Digital Defense Report 2025[※22]」（p.44）を基に IPA が表形式で整理と翻訳

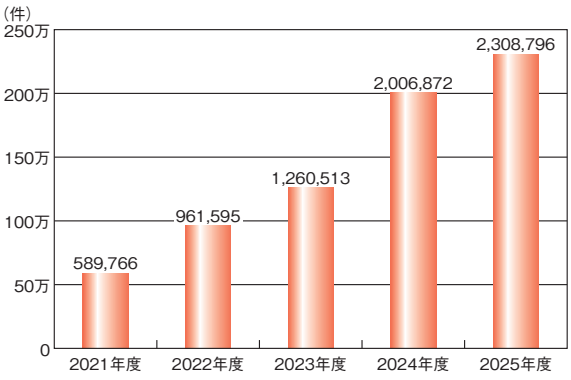
1.1.2 国内におけるサイバーセキュリティインシデント状況

国内におけるサイバーセキュリティインシデントの発生状況について、主に以下の資料を参照して概説する。

- フィッシング対策協議会:「月次報告書※24」及び「フィッシングレポート 2026※25」
- 警察庁:「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について※26」
- 株式会社東京商工リサーチ「2025 年『上場企業の個人情報漏えい・紛失事故』調査※27」「2024 年『上場企業の個人情報漏えい・紛失事故』調査※28」「2023 年『上場企業の個人情報漏えい・紛失事故』調査※29」「2022 年『上場企業の個人情報漏えい・紛失事故』調査※30」「2021 年『上場企業の個人情報漏えい・紛失事故』調査※31」(以下、東京商工リサーチ調査)

(1)フィッシングによる被害

フィッシング対策協議会への 2025 年度のフィッシング報告件数は 230 万 8,796 件で、2024 年度(200 万 6,872 件)から 15.0% 増となった。右肩上がりに増加しており、2021 年度の約 4 倍に上った(図 1-1-6)。

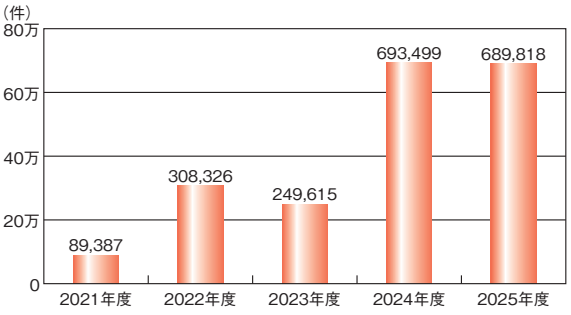


■図 1-1-6　フィッシング報告件数(2021 ～ 2025 年度)
(出典)フィッシング対策協議会「月次報告書」(2021 年 4 月～ 2026 年 3 月)を基に IPA が作成

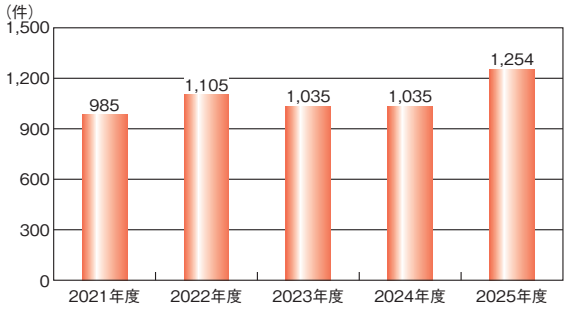
2025 年度のフィッシングサイトの URL 件数は 68 万 9,818 件と、前年度の 69 万 3,499 件に比べ微減となったが、2023 年度の 24 万 9,615 件と比べると、約 2.8 倍と高止まりしている(図 1-1-7)。

フィッシングに悪用されたブランド件数を図 1-1-8 に示す。おおむね 1,000 件前後で推移しているが、2025 年度は 1,254 件と、過去 5 年で最多となった。

音声通話によってネットバンキングの更新手続き等をかたってメールアドレスを聞き出し、フィッシングメールを送付するボイスフィッシング(ビッシング)による法人口座の不正送金被害は、2024 年秋から 2025 年 4 月にかけて急増し、その後 2025 年 11 月に再び急増した。同月の被害額は 23.1 億円に達した。地方の中小規模の金融機関でも多くの被害が発生したという※32。

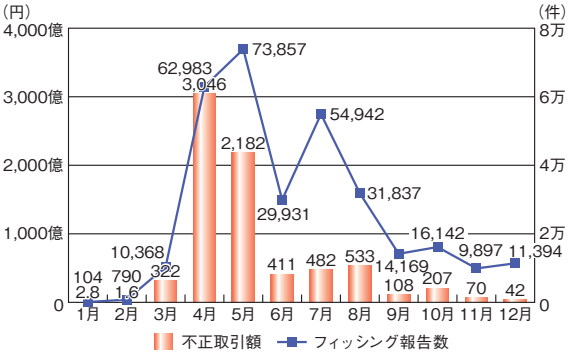


■図 1-1-7　フィッシングサイトの URL 件数(2021 ～ 2025 年度)
(出典)フィッシング対策協議会「月次報告書」(2021 年 4 月～ 2026 年 3 月)を基に IPA が作成



■図 1-1-8　フィッシングにおいて悪用されたブランド件数
(2021 ～ 2025 年度)
(出典)フィッシング対策協議会「月次報告書」(2021 年 4 月～ 2026 年 3 月)を基に IPA が作成

また、2025 年の前半では証券会社をかたるフィッシングメールが多く報告され、2025 年の年間の合計は 31 万 6,414 件であった。月別の不正取引金額では 2025 年 4 月と 5 月が多く、4 月の 3,046 億円が最多で、2025 年の年間では約 7,408 億円と甚大な被害が発生した(図

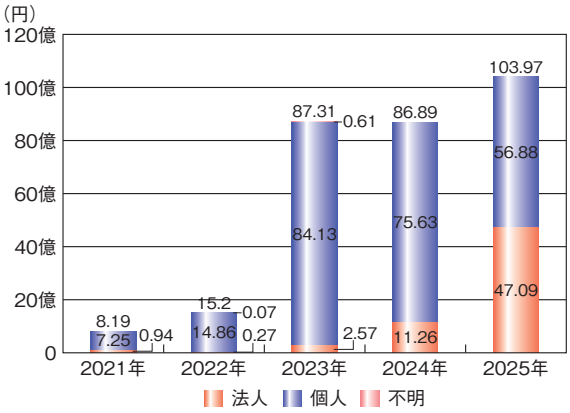


■図 1-1-9　証券会社をかたる不正取引額及びフィッシング報告数
(2025 年 1 月～ 2025 年 12 月)
(出典)「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

1-1-9)。この手口ではフィッシングにより、個人の証券口座アカウント情報が窃取され、その結果、そのアカウントで保有していた株の売却、高値での再購入等の不正取引が行われた。

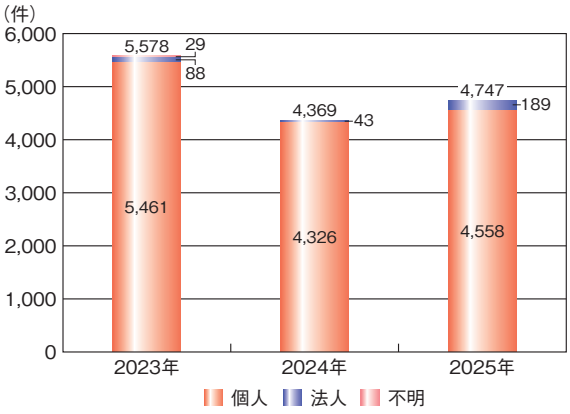
(2) 不正送金による被害

2025 年に警察庁に報告された国内の不正送金による被害金額は約 104 億円と過去 5 年間で最悪を記録した。また、これまで被害は個人が大半であったが、2025 年は法人の被害額が急増した（図 1-1-10)。原因として、2024 年秋から 2025 年 4 月にかけて急増し、その後 2025 年 11 月に再び急増したボイスフィッシングの影響が指摘されている。被害を受けた法人の中には 1 社で 4 億円を超える被害が発生したケースもあった。



■図 1-1-10　インターネットバンキングにおける不正送金被害額の推移（2021 ～ 2025 年）
(出典)「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

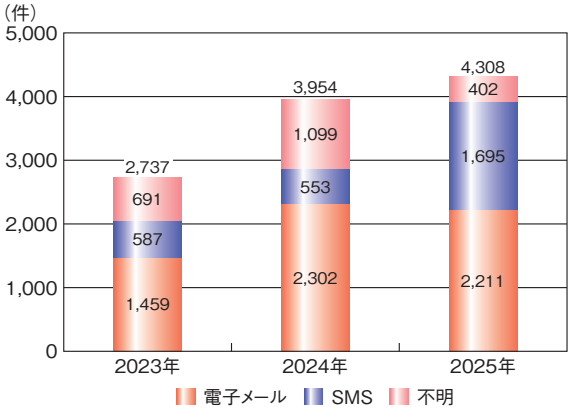
ネットバンキングにおける不正送金の発生件数を図 1-1-11 に示す。2025 年は法人の不正送金の発生が増えたとはいえ、発生件数全体のわずか 4% に過ぎない。



■図 1-1-11　不正送金の発生件数（2023 ～ 2025 年）
(出典)「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

一方、図 1-1-10 で示したとおり、法人の不正送金被害額は 2025 年に急増し、全体の 45% を占めている。このことから法人の不正送金 1 件あたりの被害額の高さがうかがえる。

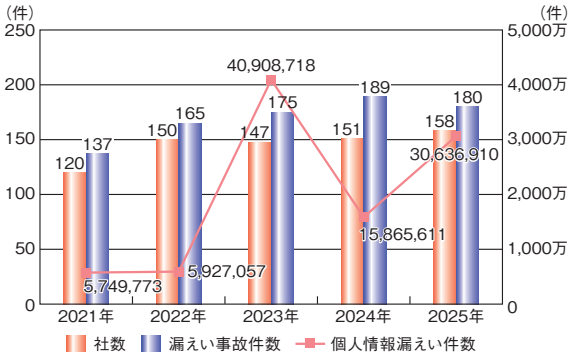
不正送金のきっかけとなるフィッシングについて、フィッシングサイトへ誘導する手口別の不正送金発生件数を図 1-1-12 に示す。電子メールによるフィッシングの割合が高いが、2025 年は SMS の割合が急増し、前年の約 3 倍に達した。電子メールや SMS のメッセージに含まれる URL を安易にタップしないよう一層の注意と用心が求められる。



■図 1-1-12　フィッシングサイトへ誘導する手口別の不正送金発生件数（2023 ～ 2025 年）
(出典)「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

(3) 情報漏えい・紛失事故の状況

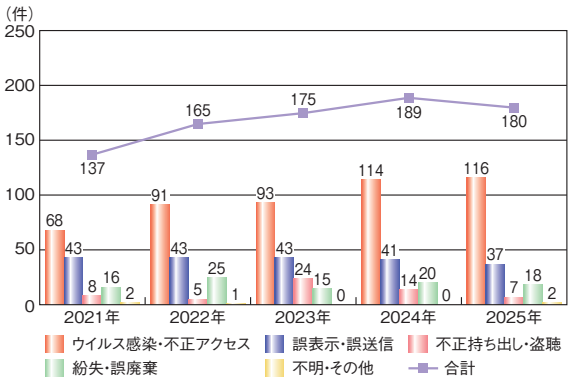
株式会社東京商工リサーチが 2026 年 1 月に公開した「2025 年『上場企業の個人情報漏えい・紛失事故』調査」によると、2025 年に上場企業とその子会社から公表された個人情報の漏えい・紛失事故の件数は 180 件、漏えいした個人情報は 3,063 万 6,910 人分だった。社数は 158 社と調査開始の 2012 年以降、過去最多であっ



■図 1-1-13　上場企業の個人情報漏えい・紛失事故件数、社数（2021 ～ 2025 年）
(出典)東京商工リサーチ調査を基に IPA が編集

た。図 1-1-13 に過去 5 年の推移を示す。

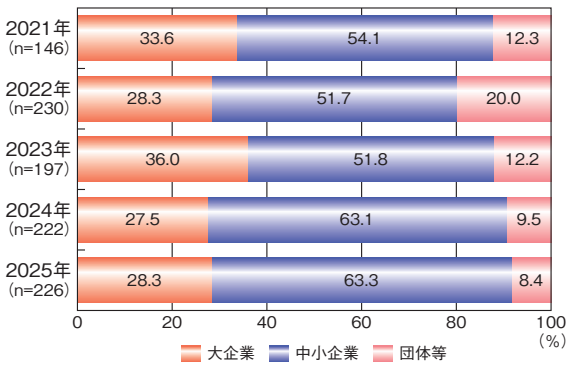
また、原因別の情報漏えい・紛失件数を図 1-1-14 に示す。「ウイルス感染・不正アクセス」が最も多く、「誤表示・誤送信」が続くという傾向は過去 5 年間、変化はない。2025 年の「ウイルス感染・不正アクセス」は 116 件と過去 5 年で最多であった。同調査では、その背景としてランサム攻撃等による不正アクセスが猛威を振るったことが挙げられている。



■図 1-1-14　上場企業の個人情報漏えい・紛失事故の原因別件数（2021 ～ 2025 年）
（出典）東京商工リサーチ調査を基に IPA が編集

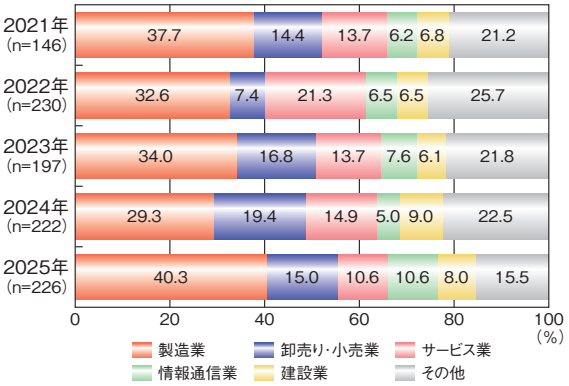
(4) ランサム攻撃による被害

2025 年に警察庁に報告された国内のランサムウェアによる被害件数は 226 件で、前年の 222 件とほぼ同等であった。ここ数年は 200 件前後で推移しており、被害件数は高止まりが続いている。被害組織の規模別では、「中小企業」の割合が、2024 年、2025 年は 6 割を超えている（図 1-1-15）。



■図 1-1-15　国内のランサムウェアによる組織規模別の被害件数割合（2021 ～ 2025 年）
（出典）「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

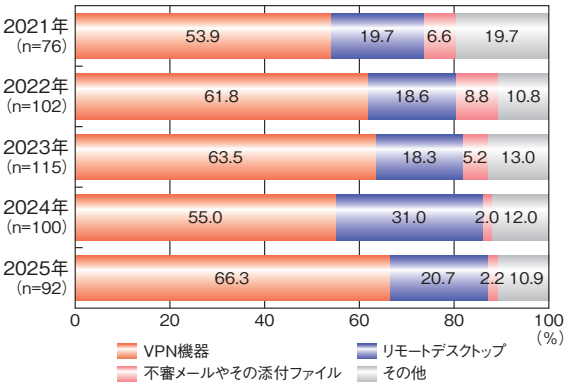
また、業種別の被害件数割合では、過去 5 年にわたり、「製造業」の割合が高い傾向が続いており、2025 年は約 4 割に達した（図 1-1-16）。



■図 1-1-16　国内のランサムウェアによる業種別の被害件数割合（2021 ～ 2025 年）
（出典）「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

2025 年に被害の報告があった 226 件のうち、手口を確認できたのは 153 件で、そのうちデータを暗号化・窃取した上で対価を要求する「二重恐喝型」が 88.9%（136 件）を占めた。

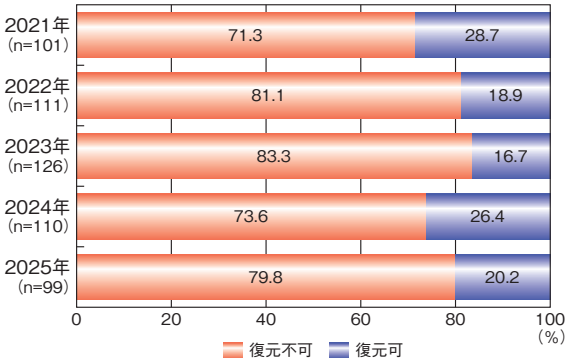
2025 年のランサムウェアの感染経路としては、有効回答 92 件のうち、「VPN 機器」が 66.3%（61 件）、「リモートデスクトップ」が 20.7%（19 件）を占め、これらテレワーク等で利用される機器からの侵入は 2024 年に引き続き、9 割に迫る高い割合となった（図 1-1-17）。



■図 1-1-17　ランサムウェアの感染経路（2021 ～ 2025 年）
（出典）「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

侵入経路とされる機器の「セキュリティパッチ」（修正プログラム）の適用状況を見ると、有効回答 71 件のうち、最新のセキュリティパッチを適用していたのは 31 件（43.7%）、未適用のセキュリティパッチがあったのは 40 件（56.3%）であった。少なくとも過去 4 年、セキュリティパッチを適用していた割合は半数に満たず、この状況は憂慮される。

被害に遭ったシステム、機器のバックアップの取得状況については、有効回答 116 件のうち、バックアップを

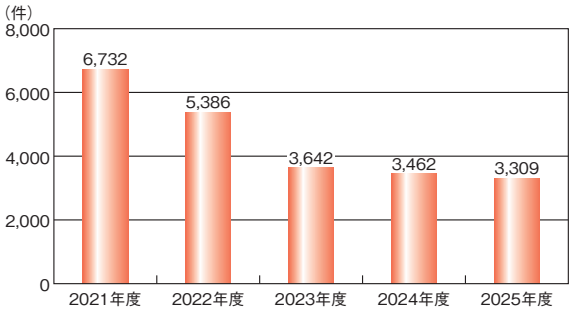


■図 1-1-18　ランサムウェア感染後、取得していたバックアップからの復元結果（2021 ～ 2025 年）
（出典）「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

取得していたのは 105 件（90.5%）であり、実際にバックアップから復元できたのは有効回答 99 件のうち 20 件（20.2%）にとどまった（図 1-1-18）。

バックアップが復元できなかった理由としては有効回答 72 件のうち、「バックアップの暗号化・消去」が 48 件（66.7%）、「運用の不備」が 19 件（26.4%）であった。バックアップを取得している割合は 9 割と決して低いとは言えないが、バックアップにより復元できた割合が 2 割程度にとどまっているため、復旧にかかる時間や費用が想定以上にかさむ可能性がある。

2025 年に被害報告のあった企業・団体等（有効回答 117 件）のうち、すべての業務が停止に追い込まれたのは 9 件（7.7%）であり、一部の業務に影響があった割合と合わせると 106 件（90.6%）であった。業務に影響がなかったと回答した割合は 11 件（9.4%）と 1 割にも満たなかった。ランサムウェアへの感染による影響は事業停止、システムの復旧（再構築）等広範にわたる。被害は企業規模を問わず、引き続き高止まりしており、今後もランサム攻撃に対する対策・体制の強化が求められる（「1.2.1 ランサム攻撃」参照）。



■図 1-1-19　DDoS 攻撃の検出件数（2021 ～ 2025 年度）
（出典）IIJ 社「wizSafe Security Signal 観測レポート※33」を基に IPA が作成

(5) DDoS 攻撃による被害

株式会社インターネットイニシアティブ（以下、IIJ 社）では、同社サービスから検出された DDoS 攻撃の観測情報を月次の観測レポートとして取りまとめている。同レポートを IPA が集計した結果によると、年度別の検出件数は減少傾向にあり、2025 年度は合計 3,309 件となり、2021 年度と比較すると約 5 割減であった（図 1-1-19）。

また、国立研究開発法人情報通信研究機構（NICT: National Institute of Information and Communications Technology）のサイバーセキュリティネクサス（CYNEX: Cybersecurity Nexus）では、DDoS 攻撃の一種である DRDoS（Distributed Reflection Denial of Service：分散反射型サービス妨害）攻撃（別名、リフレクション攻撃）を定点観測している。CYNEX が公開した「NICTER 観測レポート 2025※34」によると、2025 年に観測された日本宛ての DRDoS 攻撃は約 90 万件で、前年の約 17 万件の 5 倍超となった。ただし、2022 年は約 61 万件、2023 年は約 896 万件であったことから、観測数には年により増減が見られる。観測された全世界の攻撃件数に占める日本宛ての割合は、2023 年の約 16% を除き、おおむね 1% 程度であった。

DDoS 攻撃の事例と対策については「1.2.3 DDoS 攻撃」を参照されたい。

COLUMN

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?

IPA では、2026 年 9 月 8 日に「ランサムウェア被害から学ぶ教訓集 ～ 経営者のためのランサムウェア対策ハンドブック ～[i]」(以降、ランサム対策ハンドブック)を公開しました。

近年の国内のランサム攻撃の被害の拡大と、被害対象が業種や企業規模を問わないことは本白書の第 1 章でも説明しているところです。特に、「侵入型ランサム攻撃」では、組織内の情報資産の暗号化と、窃取した情報の公開という二重の脅迫で金銭を要求されることがあり、事業運営に大きな脅威となっています。また、ランサム攻撃の被害で特徴的なのは、被害組織にとって、暗号化が発覚した時点がインシデント発生の端緒であるにもかかわらず、攻撃者にとっては攻撃の最終段階という点です。これは、他のサイバー被害に比べ、いったんランサムウェア被害が発覚すると、同時に多くの事柄に適切かつ迅速な判断、対処が求められることを意味します。しかし、何をいつまでに対処すべきか、誰が何を行うべきか、優先順位付けや役割分担等のノウハウを有している組織は多くはないでしょう。加えて、事後に、感染発覚時の判断・対処が果たして正しかったのか検証が難しいとの指摘もあります。そこで IPA の「コンピュータウイルス・不正アクセス届出窓口[ii]」が国内の複数の被害組織に対しインタビューし、得られた情報から、被害組織に共通して起こり得ること等を抽出し、ランサムウェア被害の発生に備える教訓をまとめました。それがランサム対策ハンドブックです。

即時対応が必要なランサム事案での対処の巧拙は、事前の備えにあり、とランサム対策ハンドブックでは説いています。下図のような事前の備えを進めるには、経営者の理解と関与が欠かせないことは言うまでもありません。ぜひ、ランサム対策ハンドブックで、その内容をご確認ください。

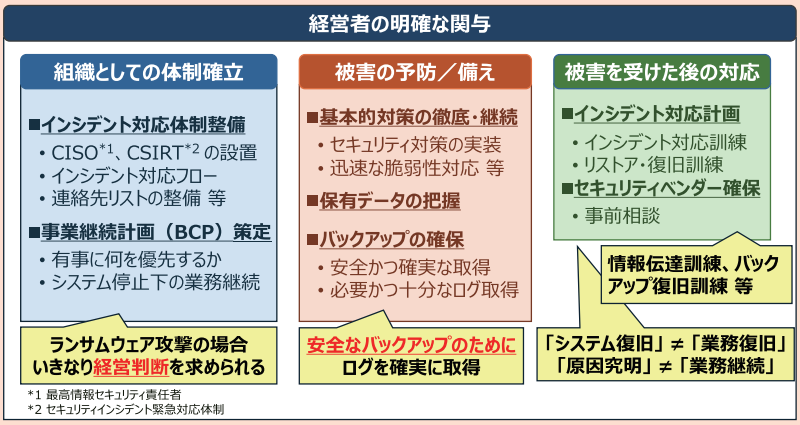


図　経営者の関与が求められるランサムウェア被害への備え

そして、もし不幸にもランサムウェア被害に遭ってしまったら、IPA への届出もご検討ください[ii]。

i　https://www.ipa.go.jp/security/todokede/crack-virus/ransomware_lessons_learned.html〔2026/9/11 確認〕
ii　IPA：コンピュータウイルス・不正アクセスに関する届出について　https://www.ipa.go.jp/security/todokede/crack-virus/about.html〔2026/9/11 確認〕

1.2 インシデント事例や脆弱性・攻撃の動向と対策

本節では、インシデント別の発生状況と、具体的な事例について述べる。また、2025 年度に確認されたサイバー攻撃の手口を中心に解説する。

1.2.1 ランサム攻撃

ランサムウェア（ransomware）とは、「ransom」（身代金）と「software」（ソフトウェア）を組み合わせた造語である。ランサムウェアは、パソコンやサーバー等のシステムをロックすることや、システムに保存されているファイルを暗号化することにより、機器を使用不能にするマルウェアの総称として用いられる。ランサムウェアによって使用不能にしたシステムやファイルを再び利用可能にすることと引き換えに身代金を要求するサイバー攻撃は、「ランサム攻撃」や「ランサムウェア攻撃」と呼ばれる。

従来のランサム攻撃は、メールに添付されたファイルを開かせてランサムウェアに感染させる、メール内のリンクから悪意のある Web サイトに誘導してランサムウェアをダウンロードさせる等により、不特定多数のコンピューターを対象にランサムウェアに感染させようとするもので、組織を選ばないばらまき型の攻撃であった。しかし、近年のランサム攻撃は、攻撃の初期段階で攻撃者が被害企業・組織（以下、被害組織）のネットワークへ密かに侵入し、パソコンだけでなく内部の認証基盤やファイルサーバー等に侵害範囲を拡大した後、大量のデータをランサムウェアによって暗号化するといった被害規模の大きい攻撃へと変化しており、組織の事業継続に大きな影響を与える重大な脅威となっている。本項では、このようなランサム攻撃を「侵入型ランサム攻撃」と呼ぶ。

このような侵入型ランサム攻撃では、データの復号（攻撃者による復号鍵または復号ツールの提供）と引き換えに金銭を要求するだけでなく、暗号化する前にデータを窃取し、身代金を支払わない場合はデータを暴露するといって脅迫する「二重の脅迫」（「二重恐喝」ともいう）が用いられることが多くなっている。更に、被害組織に DDoS 攻撃を仕掛け、混乱を引き起こすこともある（「三重の脅迫」）。加えて、攻撃者が被害組織の顧客や取引先等に連絡を取り、その組織に関連する機密情報を開示すると脅迫することで、顧客や取引先等を通じて被害組織へ身代金を支払うよう誘導することもある（「四重の脅迫」）とされている※35。

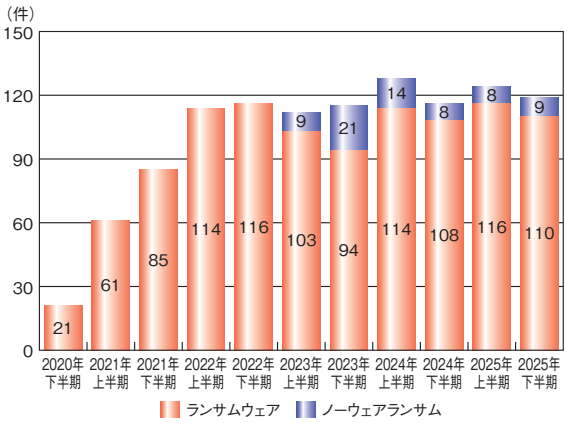
なお、昨今ではデータの暗号化を伴わない手口が確認されている。警察庁は、データを暗号化する（ランサムウェアを用いる）ことなくデータを窃取し対価を要求する手口を「ノーウェアランサム」と名付けている※36。

(1) ランサム攻撃の傾向

2025 年度における日本国内のランサム攻撃の傾向について説明する。

(a) 被害件数

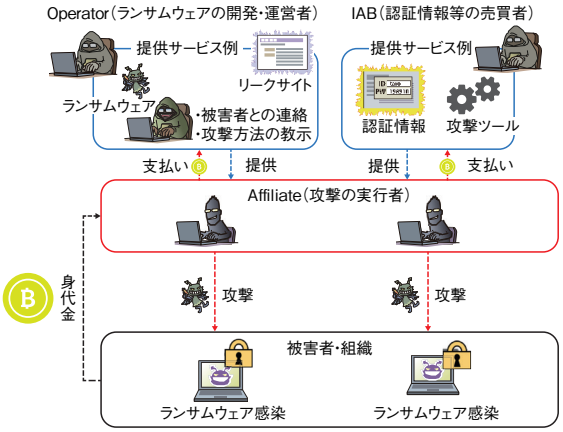
警察庁が公表した「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」（以下、警察庁資料）によると、企業・団体等におけるランサムウェア被害の報告件数は、2025 年上半期（1 月～ 6 月）が 116 件、下半期（7 月～ 12 月）が 110 件で、2022 年上半期以降は継続して高い水準で推移している（図 1-2-1）。また、ノーウェアランサム被害の報告件数は、2025 年上半期が 8 件、下半期が 9 件である。ランサムウェア被害の報告件数と比較すると少ないが、ノーウェアランサム被害の報告件数の統計が開始された 2023 年以降継続して被害が報告されている。



■図 1-2-1　企業・団体等のランサムウェア被害の報告件数の推移
（出典）警察庁「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

このような近年の被害増加の要因として、ランサムウェアをサービスとして提供する「RaaS（Ransomware as a Service）」と呼ばれる攻撃者のビジネスモデルが確立し、攻撃者の組織化や分業化が進み、攻撃をより容易に、かつ効率的に行えるようになったことが影響していると考えられる。ランサムウェアの開発・運営者（Operator）や

認証情報等の売買者（IAB:Initial Access Broker）が、金銭の支払いを見返りに攻撃の実行者（Affiliate）にランサムウェアや認証情報を提供し、攻撃の実行者が標的の組織に攻撃を仕掛け、身代金を得る（図 1-2-2）。これにより、攻撃の実行者が技術的な専門知識を有する必要なく容易に攻撃可能となり、ランサムウェアの開発・運営者や認証情報等の売買者は、より多くの顧客（攻撃の実行者）を得ることが可能になる。



■図 1-2-2　攻撃者の組織化や分業化
（出典）警察庁「令和 6 年上半期におけるサイバー空間をめぐる脅威の情勢等について※37」を基に IPA が編集

(b) 被害を受けた企業・組織

警察庁資料によると、製造業を始めとした様々な業種や公共機関で被害が確認されており、企業・組織の規模も大小を問わず広範に及んでいる。近年では、国内企業の海外拠点や海外の子会社等で被害が発生するといった事例も確認されており、ガバナンスが効きにくい海外拠点から侵入し、ネットワーク経由で日本国内にも被害を及ぼす事例もある。更に、サプライチェーンに属する組織にランサム攻撃が行われた結果、最終的に本社や取引先等のサプライチェーン全体に影響を与えた事例も確認されている※38。

(c) 組織内ネットワークへの侵入経路

警察庁資料によると、2025 年度に発生したランサムウェア被害の感染経路について、前年度に引き続き「VPN 機器」（66.3%）と「リモートデスクトップ」サービス（20.7%）からの侵入が多く、被害を受けた企業・団体から得られた有効回答の 87% を占めた。インターネットから直接アクセスできる箇所が狙われやすい傾向が継続しているといえる。

(d) 暗号化を伴わない攻撃手口

前述のノーウェアランサムでは、データの暗号化が行われないため、ファイルが閲覧できなくなる、システム障害が発生するといった目に見える事象が発生しないことから、攻撃者からの脅迫やリークサイト（攻撃者がインターネットやダークウェブ上に設置した、データ公開のための Web サイト）での暴露を受けるまで被害が発覚しないおそれがある。

この手口が使われるようになった理由としては、データを暗号化せずとも、データを持ち出すことができれば攻撃が成功するため、暗号化する手間が省けることや、侵害が発見されにくいという攻撃者に有利な点があることが挙げられる※39。加えて、2020 年ごろから各国で犯罪組織であるランサム攻撃グループに対する身代金の支払いが規制の対象となったため、被害組織が訴追をおそれ、身代金の支払いに応じることが少なくなったという状況も理由として挙げられる。これにより、攻撃者にとってはより効果的な脅迫方法が必要となり、ノーウェアランサムはその一つであると考えられる。ノーウェアランサムの場合、取引先や顧客、警察に被害が露見しにくいため、被害組織が自組織のブランドや信頼を守るために、被害を公表せず秘密裏に身代金を支払おうとする可能性は高まる。また、攻撃者としてもその存在が注目を浴びる程、検挙のリスクが高まるため、徐々にノーウェアランサムの攻撃手口が、攻撃者のリスクヘッジの手段として浸透しつつあるという意見もある※40。

(e) 標的型攻撃グループによるランサムウェアの利用

近年、標的型攻撃グループがランサムウェアを利用する事例が海外で確認されている。標的型攻撃グループがランサムウェアを利用する目的は複数あるとされている。例えば、①攻撃グループの活動資金を調達する金銭目的※41、②標的型攻撃と悟られないように金銭目的のサイバー犯罪に偽装する目的※42、③暗号化により機密情報の窃取を示すログ等の証跡を破壊する目的※42、等があるとされる。標的型攻撃グループが金銭目的のサイバー攻撃にも関与することで、国家としての関与が疑われる場合でも、「当該攻撃グループは我が国の国家支援組織ではなく、無関係である」と敵対国が主張することにもっともらしさを与えることが近年危惧されている※43。なお、これらの被害は主に海外で確認されているが、今後国内においても標的型攻撃グループによりランサムウェアが利用された場合、同様の懸念がある。

(f) 虚偽のリーク情報に基づくランサム攻撃

近年、ランサム攻撃グループを名乗る集団が、不正侵入や情報窃取を行っていないにもかかわらず、過去に流出した情報や公開されている情報を用いて、組織に対し金銭の支払いを要求する脅迫活動が確認されている。

2026 年 1 月から 2 月にかけて「0APT」と名乗るランサム攻撃グループが、200 社以上の組織の情報を窃取したと主張し、同グループのリークサイトに情報を公開した。しかし、標的とされた一部の組織から、後日、侵害の痕跡は確認されなかったと調査結果が公開されることが相次ぎ、リークサイトの情報を分析したセキュリティ関係者からは 0APT により公開された情報は信憑性が著しく低いと評価された。また、リークサイト上に公開されたファイルの大半は中身が空のダミーデータであり、実際にダウンロード可能なデータは極めて少量であったこと等から、0APT の主張は捏造または著しく誇張されたものである可能性が高いと結論付けているレポートもある※44。

虚偽のリーク情報に基づく脅迫は、もちろん身代金の獲得を目的とするものでもあるが、それ以外にも目的があることが指摘されている。例えば、企業の株価を下げ、空売り等で金銭を得る目的、被害実績を誇示して関心を持たせ、RaaS 市場でアフィリエイト（実行犯）を確保するためのマーケティング戦略の目的等が考えられる。また、アフィリエイト・プログラム（RaaS 運営者と実行犯が収益を分配する仕組み）への参加希望者に対し、保証金やゼロデイ脆弱性の実演を求めることで、他のサイバー犯罪者から金銭や貴重な攻撃コードを詐取する目的もあるとされる※45。

(2) ランサム攻撃の被害事例

2025 年度に公表された国内における侵入型ランサム攻撃の主な被害事例を紹介する。

(a) 大手総合飲料メーカーにおける被害事例

2025 年 9 月 29 日、アサヒグループホールディングス株式会社は、サイバー攻撃によるシステム障害が発生し、国内グループ各社の受注・出荷業務等が停止したことを公表した※46。その後、10 月 3 日に公開された第 2 報では、同社のサーバーがランサムウェアによる攻撃を受け、情報漏えいの可能性を示す痕跡が確認されたことを公表している※47。

11 月 27 日に行われた同社の記者会見では、調査の結果判明したサイバー攻撃によるシステム障害の経緯、復旧状況等について語られた。一部を表 1-2-1 に抜粋する※48。

発生日	発生した事象と対応状況
2025 年 9 月 19 日ごろ	攻撃者が同社グループ内の拠点にあるネットワーク機器を経由し、同社のネットワークに侵入
9 月 19 日ごろ～29 日未明	侵入後、攻撃者はパスワードの脆弱性を突いて管理者権限を奪取し、その権限を用いて、主に業務時間外に内部ネットワーク上の複数のサーバーや端末を探索する等の活動を実施
9 月 29 日未明	攻撃者が侵害したサーバーからランサムウェアを一斉に実行し、起動中の複数のサーバーやパソコン端末の一部のデータを暗号化
9 月 29 日	午前 7 時ごろにシステム障害が発生し、同社サーバー内に暗号化ファイルを確認（同社が初めて侵害を検知）
同日	同社は午前 11 時ごろにネットワークを遮断し、データセンターの隔離を実施

■表 1-2-1　大手総合飲料メーカーに対するランサム攻撃のタイムライン
（出典）公表情報を基に IPA が作成

本件の影響により、同社グループでは、受注・出荷、物流管理、在庫管理、経理処理等の基幹業務システムが停止または利用制限を受け、商品供給の遅延や一時的な出荷停止が発生したほか、経理関連業務にも影響が生じ、決算発表の延期を行う等、事業運営に多大な支障が生じた※49。情報漏えいについては、従業員に貸与されていた一部のパソコンのデータが流出したことや、データセンター内のサーバーに保管されていた顧客、従業員、取引先等に関する個人情報が、最大で 2025 年 11 月 26 日時点で 191.4 万件漏えいした可能性があり、2026 年 2 月 18 日時点で漏えいが確認された個人情報は 11 万 5,513 件であることを公表している※50。

本件のランサム攻撃は、ロシア系のランサム攻撃グループ「Qilin」が関連しているとされている。同グループは自らのリークサイトにて、同社の内部資料とする約 29 件の画像を公開した上で、9,300 個以上のファイル、合計約 27GB のデータを盗んだと主張したという。同社広報は 2025 年 10 月時点で、引き続き調査中であり、リーク内容や攻撃者の主張についてコメントは行わないとしている※51。

同社は、このインシデント対応の中で、侵害の発覚直後から様々な対応・対策を行っている。封じ込めの対応（被害拡大防止策）として、リモートアクセス VPN・拠点間ネットワーク等の専用通信回線の遮断、攻撃の横展開（他システムへの感染）を防止するための緊急措置として、インターネット回線の遮断を実施している。また、外部専門機関によるフォレンジック調査を実施し、システムごとの健全性を検証するとともに、侵害の有無や影響範

囲の精査を実施しており、復旧を進める中でこれらの詳細調査の結果を基に必要な追加セキュリティ対策を実施している。

その後、同社グループでは、アサヒビール株式会社及びアサヒ飲料株式会社が EOS（電子受発注システム）による受注を 2025 年 12 月 3 日から、アサヒグループ食品株式会社が同年 12 月 2 日から再開し、2026 年 2 月には物流業務全体の復旧を完了している※50。

業務復旧後も、再発防止策やガバナンス体制の強化に取り組んでいる。例えば、リモートアクセス VPN 装置の全面廃止、より安全な仕組みに対応した専用のパソコン端末（ゼロトラストモデル対応のパソコン端末）への完全移行、サイバー攻撃や異常を素早く検知・対処し、被害を最小化するためのログ分析システムの導入やセキュリティの監視・遮断の自動化、システム復元の迅速化の実現に向けたバックアップの仕組みの強化、情報セキュリティ委員会を設置し、情報セキュリティリスクを可視化するとともに、対応策の計画・実行状況のモニタリング等を進めている※50。

(b) 大手 e コマース企業における被害事例

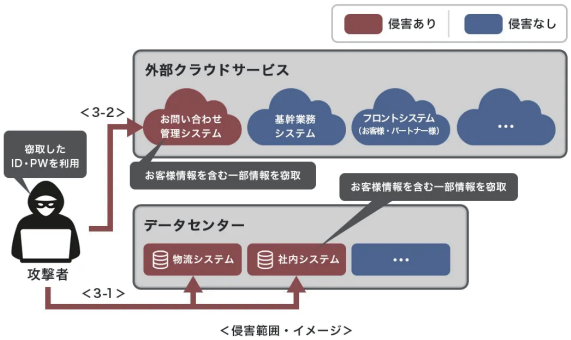
2025 年 10 月 19 日、アスクル株式会社は、同日にランサム攻撃によるシステム障害が発生し、受注・出荷業務を停止したことを公表した※52。

同社が 12 月 12 日に公表した報告書から、インシデント対応の経緯を抜粋して表 1-2-2 に示す※53。

発生日	発生した事象と対応状況
2025 年 10 月 19 日	午前にランサム攻撃を検知
同日	ランサムウェアに感染した疑いのあるシステムの切り離しやネットワークの遮断を実施
同日	セキュリティ監視体制の強化を行うとともに、全パスワード変更に着手
同日	14 時、対策本部を設置し、その配下に事業継続及び IT 復旧部会を設置
10 月 20 日	外部の専門機関へ支援要請をしてログ解析、影響の詳細調査の開始及び意図しないデータ変更のチェック等を実施
10 月 22 日	外部クラウドサービスへの不正アクセスが発生
10 月 23 日	主要な外部クラウドサービスに関連するパスワードの変更完了

■表 1-2-2　大手 e コマース企業に対するランサム攻撃のタイムライン
（出典）公表情報を基に IPA が作成

同社によると、ランサムウェア感染につながった不正アクセスの原因については、当時のログが削除されているため、原因の完全な究明は困難な状況としている。一方、多要素認証を適用していなかった業務委託先に対して付与していた管理者アカウントの ID・パスワードが漏えいし、不正利用されたことを確認しているという。攻撃者は窃取した管理者アカウントの ID・パスワードを用い、データセンター内の物流システムや社内システムを侵害し、その過程で窃取した ID・パスワードを用い、外部クラウドサービスで実行している同社の「お問い合わせ管理システム」を侵害した可能性がある※53（図 1-2-3）。なお、図 1-2-3 の「＜3-2＞」は「外部クラウドサービスへの侵害」を、「＜3-1＞」は「物流・社内システムへの侵害」を指す。



■図 1-2-3　攻撃者による侵害範囲のイメージ
（出典）アスクル株式会社「ランサムウェア攻撃の影響調査結果および安全性強化に向けた取り組みのご報告（ランサムウェア攻撃によるシステム障害関連・第 13 報）」

なお、同社は、侵入検知が遅れた原因として、侵害が発生したデータセンターではサーバーに EDR（Endpoint Detection and Response）が未導入で、24 時間監視も行っていなかったことにより、不正アクセスや侵害を即時検知できなかったことを挙げている。更に、復旧の長期化の原因としては、オンラインバックアップは実施していたが、ランサム攻撃を想定したバックアップ環境を構築しておらず、一部バックアップも暗号化されたことも挙げている※53。

本件の影響により、同社が運営する事業所向け EC サイト「ASKUL」及び「ソロエルアリーナ」、個人向け EC サイト「LOHACO」の受注及び出荷業務が停止した。特に、物流センターでは、自動化された倉庫設備やピッキングシステムを制御する物流システムが停止したことにより、出荷業務が全面的に停止し、サービスの提供に大きな支障が生じた。同社はその後、FAX 注文を用いた出荷トライアルの実施等、段階的な業務再開を行った。

情報漏えいについては、約 74 万件の情報が外部へ流出したことを確認したと公表しており、流出した情報には、事業所向け EC 及び個人向け EC における顧客の

情報の一部、取引先に関する情報の一部、更に役員及び従業員等に関する情報の一部も、流出の可能性があるとしている。同社は、流出した情報について、個人情報保護委員会への報告を行うとともに、該当する関係者に対して個別の通知及び専用の問い合わせ窓口を設置している※53。

本件では、「Ransomhouse」を名乗るランサム攻撃グループが、インターネット上で本件への関与を主張し、同社から取得したとされるデータの一部を複数回に分けて公開した※54。Ransomhouse は、登場当初は暗号化ではなくデータ窃取と恐喝に特化した恐喝グループとして認識されていたランサム攻撃グループであるが、近年は暗号化を伴う「二重の脅迫」を行っている※55。

本件の対応・対策について同社は、短期フェーズ（封じ込めと安全確保）、中期フェーズ（仕組みの高度化）、長期フェーズ（成熟度向上と運用定着）の三つのフェーズでの実施を発表した。例えば、短期フェーズでは、不正アクセス経路の遮断、EDR の導入徹底及び運用強化、中期フェーズでは、監視体制の 24 時間 365 日の管理高度化、権限管理フレームワークの見直し、長期フェーズでは、セキュリティ対策の継続的アップデートやランサムウェア事案を踏まえた事業継続計画（BCP：Business Continuity Plan）の見直し・強化を実施するとしている※53。

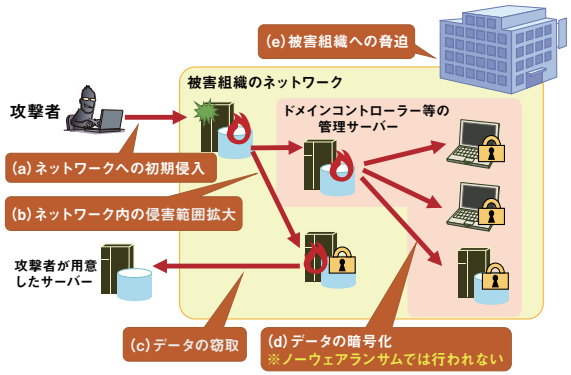
なお、同社は、2026 年 2 月 13 日に、同年 2 月 4 日より、全物流センターで新物流システムによる出荷再開が完了したこと、13 日より一般品から順次、当日配送サービスを再開しており、商品の品揃えを含む主要な EC サービス機能がシステム障害発生前の水準まで復旧したことを公表している※56。

(3) 侵入型ランサム攻撃の手口

ここでは、侵入型ランサム攻撃の手口について説明する。攻撃は、次の(a)～(e)の五つのステップで行われる（図 1-2-4）。

(a) ネットワークへの初期侵入

侵入型ランサム攻撃は、攻撃者が被害組織のネットワークへ侵入するところから始まる。攻撃者は、被害組織がインターネットへ接続している機器全般を狙い、残存している脆弱性を悪用する攻撃や、強度の弱いパスワード等の設定不備への攻撃、過去に漏えいした認証情報等を悪用する等、様々な手法を使ってネットワークに侵入する。警察庁資料によると、侵入経路としては、VPN サービスを実行するゲートウェイやリモートデスクトップサービス経由での侵入が多い傾向にある。その一方で、被害組織へ遠隔操作マルウェア等を添付したメールや、遠隔操作マルウェア等をダウンロードさせる URL リンクを記載したメールを送信することで感染させ、初期侵入に使用することもある。



■図 1-2-4　侵入型ランサム攻撃の手口のイメージ

(b) ネットワーク内の侵害範囲拡大

攻撃者は、被害組織のネットワークへの侵入に成功すると、ネットワーク内で侵害範囲の拡大を図る。攻撃者はまずネットワーク構成やシステム構成の把握をした後、利用可能なアカウントを使い、様々な方法で管理者権限の奪取を行い、機微情報等が保存されているパソコンや業務用サーバー、ドメインコントローラー等の管理サーバー、バックアップ用のサーバー等を侵害する。特に、ネットワーク内のユーザーやコンピューターを一元管理することができるドメインコントローラーを侵害すると、管理下のすべてのコンピューターの認証情報を奪えるだけでなく、セキュリティ対策全体に影響を及ぼすことができるため、多くの事案で攻撃されている。更に近年のランサムウェアには組織で利用されていることが多い仮想化基盤（VMware や Hyper-V）を攻撃する機能を持つものがあり、より効率的に組織のネットワークを侵害できるようになっているといえる。

(c) データの窃取

攻撃者は、遠隔操作マルウェアや正規のツール等を使用し、ネットワーク内のデータ探索・収集を行った上で、収集したデータを攻撃者が準備したサーバーや商用のクラウドストレージへアップロードすることで、データの窃取・持ち出しを行う。データの窃取は、攻撃者が「二重の脅迫」やノーウェアランサムを狙っている場合等に行われる。

(d)データの暗号化

侵入型ランサム攻撃では、攻撃者は被害組織のデータをランサムウェアによって暗号化することで、事業継続に関わる重要なシステムを停止させ、身代金を要求する。同時にバックアップデータによる復旧を妨害するため、バックアップを構成するシステムを暗号化することもある。

一方で、ノーウェアランサムでは、同ステップは行われない。そのため、システムの停止は発生しないが、EDR等のセキュリティ対策によって攻撃を検知しにくく※40、侵害されたことが発覚しにくい。

(e)被害組織への脅迫

攻撃者は、被害組織に対して、システムやファイルの復号を可能にすることと引き換えに身代金を要求する。また、身代金を支払わなければ窃取したデータを公開するとして脅迫を行う。データの公開方法としては、リークサイトでの公開やオークション形式での販売等がある。「ランサムノート」と呼ばれる、身代金を要求するドキュメント等によって伝えられる攻撃者との連絡手段には電子メールや特定のチャットサイト等が使用されることが多いが、直接電話がかかってくるケースもあるという※57。

更に、被害組織が提供する外部公開サービスへのDDoS攻撃を仕掛けることで組織へのダメージを拡大する「三重の脅迫」や、ランサムウェア被害に遭ったことを被害組織の利害関係者へ直接連絡する等で組織の評判を悪化させることでの脅迫を行う、「四重の脅迫」に至る場合もある。

(4)侵入型ランサム攻撃への対策

ここでは、侵入型ランサム攻撃への対策について、「(a)ネットワーク侵入への対策」「(b)侵害範囲拡大防止のための対策」「(c)暗号化によるシステム停止への対策」「(d)自組織への脅威に関わる情報の調査と把握」「(e)インシデント対応力の強化」の五つに分けて説明する。これらの対策は自組織だけでなく、海外を含む子会社や取引先等、サプライチェーン全体で行うことが重要といえる。なお、ランサムウェアに特化した公開文書として、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)が「#StopRansomware Guide※58」を公開している。加えて、米国国立標準技術研究所(NIST:National Institute of Standards and Technology)が2026年6月に「Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile※59」を公開している。本文書は2022年に同組織によって作成されたものを改訂する形で公表され、新たにガバナンス、サプライチェーン、サイバー保険等をレポートの対象範囲に拡張して、ランサム攻撃対策を技術的課題ではなく経営課題として位置付けている。これらの文書には、ランサム攻撃への備えに有用な多くの情報が記載されているので、併せて参考にしていただきたい。

(a)ネットワーク侵入への対策

侵入型ランサム攻撃は、攻撃者が企業・組織内のネットワークへ侵入することから始まるため、次のような侵入対策を行うことが重要である。

- 攻撃対象領域(アタックサーフェス)の最小化

  企業・組織の管理する機器がランサム攻撃の対象となる可能性を減らすために、まずはインターネットからのアクセスを可能にしているサーバーやネットワーク機器、プロトコルやサービス等を把握し、外部公開するシステム数をできる限り少なくすること、更にそのシステムの稼働に不要なプロトコルやサービスを制限することで、攻撃対象領域を最小化することが重要である。加えて、製品を初期設定のままにしていること等により、「意図せず公開すべきではない情報が外部からアクセス可能な状態になっている」等の設定不備がないかもそれらのシステムが稼働する前や運用中に、定期的に確認することを推奨する。

  このような攻撃対象領域の把握や管理に加えて、脆弱性情報の収集やリスク評価等を行い、リスクを最小化するためのプロセスはASM(Attack Surface Management)と呼ばれる。ベンダーが提供するASMツールを用いることで、これらの情報やプロセスを統合的に管理できるようになる。

- 脆弱性対策

  脆弱性を悪用した侵入や侵害範囲の拡大を防ぐために、組織が利用しているVPNゲートウェイ等のネットワーク機器のファームウェア、パソコンやサーバーのOS、利用しているソフトウェア等を常に最新の状態に保つことが重要である。脆弱性に関する情報はその製品の開発元だけでなく、脆弱性情報を取り扱う様々な組織や機関から公表されている。そのような情報源から脆弱性情報を日々収集することは、リスクの早期発見や迅速な対応につながる。なお、脆弱性の影響を受けないバージョンにアップデートする前のわずかな期間でも攻撃が成立する条件下で運用を行っていた場合、既に攻撃されていた可能性を考慮すべきであ

る。そのため、脆弱性が悪用された痕跡を示すIoC（Indicator of Compromise：侵害指標）等の情報を収集し、過去のログを含め、攻撃された痕跡がないか調査することを強く推奨する。また、脆弱性が公開されてから悪用されるまでの期間が以前より短くなっていることから、公開された脆弱性対策情報に迅速に対応できるような体制や計画を、運用設計に盛り込んでおくことも重要といえる。更に、組織全体のセキュリティ対策という観点では、自組織の脆弱性を把握するために、自組織が保有、利用する情報資産（サーバー、端末、ソフトウェア等）を適切に把握・管理することが重要である。

- 認証の強化とアクセス制御
  企業・組織外からアクセス可能な機器等が攻撃者に不正に侵入・操作されないために、推測されにくい複雑なパスワードを使用するだけでなく、認証の試行回数に制限を設けるシステム対策、多要素認証等の強固な認証方式を使用することによる認証強化等が必要である。更にそのサービスに対するアクセスを、特定のIPアドレスから許可または拒否する等のアクセス制御も有効な対策である。インシデント発生への備えとしては、平時から、必要な認証ログやアクセスログ等を取得・保管し、攻撃を早期発見するためにログを監視・分析することが望ましい。
- 攻撃メール対策
  フィッシングメールやマルウェア添付メール等の攻撃メールによる認証情報の流出やマルウェア感染を防ぐために、メールのセキュリティ対策システムで不審メールを検知・隔離する対策が重要である。また、役職員のセキュリティリテラシーを高めるための教育や啓発、訓練等の対策を実施し、メール利用者の一人ひとりが「身に覚えのないメールの添付ファイルは開かない、怪しいリンクはクリックしない」という意識を持つことも重要といえる。

(b) 侵害範囲拡大防止のための対策

攻撃手口の高度化に伴い、侵入を完全に防ぐことが難しくなっている中で、侵害された際の影響範囲を局所化することが重要である。すなわち、従来のように、外部との通信を制御する入口・出口対策のみに依存するのではなく、侵入を前提として、攻撃者の活動や侵害の拡大を抑止する内部対策を含めて多層的に対策を講じる「多層防御」の考え方に基づく対策が求められる。

- ネットワーク境界のセキュリティ強化
  組織内の複数の拠点間、取引先等との外部ネットワーク接続において、十分なセキュリティ対策が講じられていない接続経路があると、攻撃者はその経路を悪用して組織のネットワークへ侵入する可能性がある。また、侵入後には、ネットワーク間接続を経由して他の拠点や重要システムへ侵害範囲を拡大するおそれがある。そのため、組織内の拠点間、海外拠点との接続、特に他組織とのネットワーク境界においては、アクセス制限や不正通信の監視、セグメンテーション等の対策を実施することが重要である。
- ネットワーク内の通信制御の強化
  ネットワーク境界のセキュリティ強化に加えて、組織内のネットワークを細分化し、内部通信の可視化と制御を行うことが望ましい。このような手法は「マイクロセグメンテーション」と呼ばれ※60、攻撃対象領域の縮小によるリスク低減に加え、攻撃者が組織内へ侵入した後の侵害範囲の拡大（水平展開（ラテラルムーブメント））を抑止する対策として有効である。

被害拡大防止に有効なセキュリティ対策の例を「情報セキュリティ白書2023※61」の「1.2.1 (4) (c) 侵害範囲拡大への対策」にて解説しているため、そちらも併せて参照いただきたい。

(c) 暗号化によるシステム停止への対策

侵入型ランサム攻撃によってデータが暗号化され、システムが停止した場合に備えて、システムのバックアップからの復旧を念頭に置いた対策を行うことが重要である。

- バックアップの取得
  ランサム攻撃の特性を考慮して、バックアップを安全に取得できる仕組みを構築する必要がある。バックアップサーバーが組織のネットワークに接続されている場合、バックアップデータも含めて一斉に暗号化される可能性があるため、複数のバックアップ方式を採用しておくことでリスクを分散することは有効である。バックアップのうち一つは、テープデバイス等に保存してネットワークから隔離された環境に移す等、攻撃者から手の届かないオフライン環境にも配置することが望ましい。このほか、一度保存した後は上書きを禁止する仕組み（WORM（Write Once Read Many）機能）でデータを保護することや、バックアップソリューションによるクラウドストレージ利用やバックアップに特化したクラウドサービスの利用も効果的である。なお、クラウドサー

ビスにおけるユーザーデータのバックアップ機能の有無や責任分界点については確認が必要である。クラウドサービスでは、多くの場合、ユーザーデータの管理責任は利用者側にあり、ランサム攻撃等への対策を目的としたバックアップの実施及びバックアップデータの管理は、クラウドサービスの利用者自らが行う必要があるためである。

また、いずれのバックアップ方式においても、バックアップからの復旧が実際に可能なことを、何らかの方法で確認しておくことは重要である。

- 復号ツールの活用（暗号化された後の対策）

  ランサムウェアの種類によっては、復号ツールが公開される場合がある※62。感染したランサムウェアの種類を特定できている、かつその復号ツールが公開されている場合、復号ツールを活用することで、暗号化されたファイルを復号できる可能性がある。

（d）自組織への脅威に関わる情報の調査と把握

侵入型ランサム攻撃では、攻撃者が窃取した情報や被害組織名等を外部に公開すると主張したり、実際にリークサイトで公開することで、被害組織に対して圧力を掛ける場合がある。そのため、攻撃者により不正に公開された自組織や子会社等の関連組織に関わる情報や脅威動向を継続的に調査・把握し、攻撃者による情報公開の兆候や自組織への影響を早期に把握できる、以下のような体制を整備しておくことが重要である。

- 外部組織が提供する脅威動向の継続的な把握

  発生したサイバー攻撃について特徴的な事案は、セキュリティベンダーや政府機関等から各種情報が公開、発信される場合がある。そのような外部組織からの情報を積極的に把握する体制を整備しておくことが重要である。具体的には、公開情報や報道、専門機関等が提供する脅威動向情報を活用し、ランサム攻撃者を名乗る第三者による主張や情報の不正な公開の動きについて、組織として把握・整理できる状態を維持することが望ましい。これにより、類似の攻撃に備えた対策を事前に取ることができる可能性がある。また、特に同業種の組織に関するものや攻撃経路となった同種類の機器やサービスを利用している等、関連あるものを確認した場合は、積極的に活用することが望ましい。

- 脅威インテリジェンスサービスの活用

  近年、ランサム攻撃に関連して、攻撃者が自らの関与を主張し、窃取した被害組織に関する情報を外部に公開すると主張・脅迫する事例が確認されている。これらの情報は攻撃者達の主な活動領域であるディープウェブやダークウェブ上で行われることが多いが、ダークウェブ等は一般的な組織ネットワークで利用されている方法ではアクセスができないことや、アクセスすること自体が組織に危険を及ぼす可能性があることから、セキュリティベンダー等が提供する「脅威インテリジェンスサービス」や「ダークウェブモニタリングサービス」を活用するのが望ましい。情報を収集する際は、自組織だけでなく、子会社や関連会社等の関連組織に関する情報も対象とすることが望ましい。

（e）インシデント対応力の強化

侵入型ランサム攻撃による被害では、業務の停止や顧客・取引先の情報漏えい等が発生し、その影響は自組織にとどまらず、顧客や取引先等の関係者にも及ぶ傾向がある。更に、時間的猶予がなく、組織は様々な意思決定を短時間で行わなければならない。そのため、平時から、経営層を含む組織内の各部署と連携したインシデント対応計画を立てることや、顧客や取引先、システムの運用・保守の委託先等との素早い連絡・調整を行うための体制づくりが必要である。特に、迅速に協力を要請できるセキュリティベンダーを含めたインシデント対応体制を整備しておくことが重要である。対応の計画や体制構築にあたっては、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）が公開している「侵入型ランサムウェア攻撃を受けたら読む FAQ※63」が、被害への具体的対応を詳細に紹介しており、事前準備が必要であることを理解し、備えるべきことを整理するのに非常に有用である。

- ランサム攻撃を想定した BCP の策定

  自然災害の発生を想定したBCPを策定している企業・組織であっても、侵入型ランサム攻撃等のサイバー攻撃を受けることを想定していない場合がある。ランサムウェア被害はシステムの停止を発生させることから、業務継続に大きな影響を与えるため、BCP の策定時には、侵入型ランサム攻撃についても考慮する必要がある。

- 侵害発生時における影響範囲の正確な把握

  情報漏えいの有無及び範囲を正確に把握することが重要である。特に、攻撃者側が情報を取得したと主張している場合には、その主張内容と実際の侵害状況とを切り分けて確認する必要がある。このため、組

織においては、ログ情報やシステム構成、保存データの所在等を基に、どの情報資産が影響を受けた可能性があるのかを迅速に把握できる体制を整備しておくことが望ましい。また、必要に応じて外部の専門機関と連携し、技術的な分析や専門的知見に基づく調査を実施することで、漏えいの有無及び範囲を適切に把握し、正確な情報開示やステークホルダーへの説明責任を果たすことが重要である。

1.2.2 標的型攻撃

「標的型攻撃」という用語には確立された定義はないが、例えば国家サイバー統括室（NCO：National Cybersecurity Office）が公開している「政府機関等の対策基準策定のためのガイドライン（令和7年度版）※64」では、「特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃」とされており、持続的かつ高度であるという特徴をとらえて「APT（Advanced Persistent Threat）攻撃」とも呼ばれる。この定義によれば、標的型攻撃は、フィッシングメールを不特定多数の相手に無差別に送り付けるのとは異なり、特定の企業・組織等（以下、標的組織）を標的とし、機密情報の窃取等の明確な目的をもって行われるものである。

(1) 標的型攻撃の手口

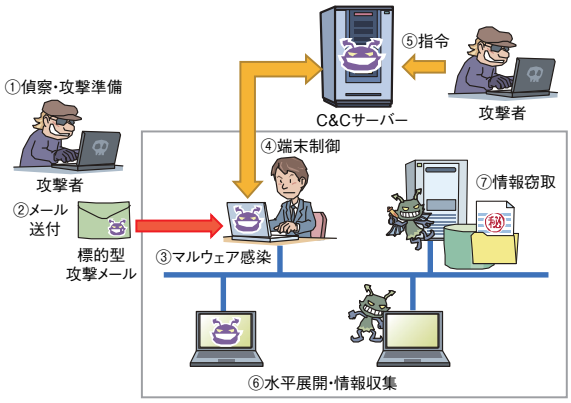
標的型攻撃における標的組織内への侵入の手口として、特定の対象をピンポイントで狙った、スピアフィッシングによる標的型攻撃メールに加え、インターネット境界に設置された機器の脆弱性の悪用等によるネットワーク貫通型攻撃も多数観測されている。以下に、それぞれの手口について述べる。

なお、他の標的型攻撃の手口としては、エアギャップ越しの攻撃※65や水飲み場型攻撃※66等がある。

(a) 標的型攻撃メールを用いた攻撃の手口

標的型攻撃メールとは、マルウェアを仕込んだファイルが添付されていたり、マルウェアをダウンロードさせるURLリンクが記載されていたりするメールが標的組織の役職員宛てに送り付けられてくるものである。標的型攻撃メールは、個人の私用メールアドレス宛てに送られる場合もあるので注意が必要である※67。以前から用いられている手口であり、継続して観測されている。標的型攻撃メールを用いた攻撃の流れを以下に示す（図1-2-5）。

①偵察・攻撃準備：攻撃者は、標的組織を攻撃するための情報を収集、攻撃手法を選定する。
②メール送付：攻撃者は、標的組織宛てにメールを送付する。
③マルウェア感染：受信者がメールの添付ファイルやURLリンクを開くことで、攻撃者が仕込んだマルウェアが端末にインストールされる。
④端末制御:感染した端末は、攻撃者が管理するC&C（Command and Control）サーバー※68と通信を開始する。
⑤指令：攻撃者は、C&Cサーバーを経由して感染端末へ指令を送り、遠隔操作を行う。
⑥水平展開・情報収集：攻撃者は、侵害範囲拡大や目的に関連する情報の探索・収集を行う。
⑦情報窃取：攻撃者は、目的の情報等を窃取する。



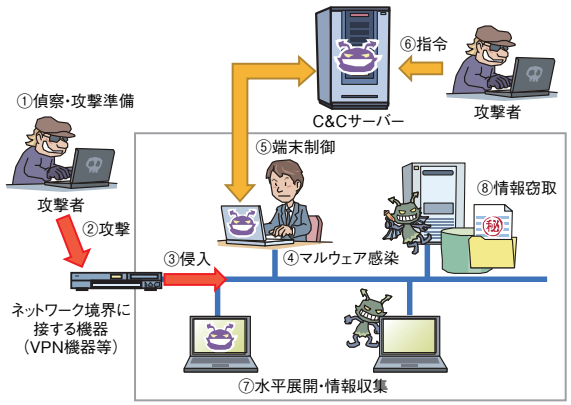
■図1-2-5　標的型攻撃メールを用いた攻撃の流れ

(b) ネットワーク貫通型攻撃の手口

標的組織のネットワークに侵入する手口として、VPN機器やWebサーバー等のネットワーク境界に接する機器に対し、脆弱性や設定不備を悪用して侵入したり、何らかの方法で得た認証情報（IDとパスワード等）を使ったりして不正アクセスし、組織内のネットワークに侵入する手口がある。IPAでは、このような手口による攻撃を「ネットワーク貫通型攻撃」と呼び、2023年以降、この手口による攻撃に関する注意喚起を行っている※69。なお、標的型攻撃メールを用いた攻撃とは侵入の手口が異なるだけで、侵入後のマルウェア感染や端末制御等、目的達成までの活動に違いはない。ネットワーク貫通型攻撃の流れの一例を以下に示す（次ページ図1-2-6）。

①偵察・攻撃準備：攻撃者は、標的組織を攻撃するための情報を収集、攻撃手法を選定する。

②攻撃：攻撃者は、VPN 機器等の脆弱性を悪用し標的組織へ不正アクセスを行う。
③侵入：攻撃者は、標的組織のネットワーク内に侵入し内部偵察を行う。
④マルウェア感染：攻撃者は、端末等に侵入しマルウェアをインストールする。
⑤端末制御：感染した端末は、攻撃者が管理する C&C サーバーと通信を開始する。
⑥指令：攻撃者は、C&C サーバーを経由して感染端末に指令を送り、遠隔操作を行う。
⑦水平展開・情報収集：攻撃者は、侵害範囲拡大や目的に関連する情報の探索・収集を行う。
⑧情報窃取：攻撃者は、目的の情報等を窃取する。



■図 1-2-6　ネットワーク貫通型攻撃の流れの一例

ネットワーク貫通型攻撃では、VPN 機器等のネットワーク境界に接する機器を通じて標的組織内のネットワークへの侵入が試みられるほか、他組織への攻撃の踏み台として悪用するための機能が機器に追加されることがある。そのようなケースでは、それらの機器は一種の Operational Relay Box（ORB：中継装置）※70 となり、意図せずに他組織への攻撃活動に加担することにつながりかねないので注意が必要である※71。

また、中国の国家支援型攻撃グループとされる「Volt Typhoon※72」のように、ネットワーク境界に接する機器の脆弱性を悪用して標的組織内のネットワークに侵入後、将来的な重要インフラシステムへの攻撃のため、Living Off The Land（LOTL）戦術※73 を用いて長期間にわたり当該ネットワークへのアクセスを維持する攻撃者も存在するため、このような手口にも注意が必要である※74。なお、LOTL 戦術は、ネットワーク貫通型攻撃だけでなく、標的型攻撃メールを用いた攻撃で使われる場合もあり、「1.2.2 (2) (a) 国家支援型 APT 攻撃グループの攻撃事例」で後述する攻撃グループ「MirrorFace」も LOTL 戦術を用いているとの指摘がある※75。

標的型攻撃に限定したものではないが、セキュリティベンダーである CrowdStrike Holdings, Inc. の調査によると、2025 年は攻撃者による AI の悪用が前年比 89% 増加したとされ、偵察、認証情報の窃取等の活動で AI が使用されているという。AI の使用に伴い、攻撃の展開速度も向上しており、攻撃の平均侵入時間は 2024 年の 48 分から 29 分に短縮されたという※76。AI の悪用の動向についても、より一層注意が必要である（AI を悪用したサイバー攻撃については「2.2.4 (2) AI を悪用したサイバー攻撃への対処」参照）。

(2) 標的型攻撃の事例

標的型攻撃のうち、国家の支援を受けた攻撃グループによる、機密情報（先端技術や国家安全保障に関わる情報等）の窃取やシステムの破壊等の妨害工作を目的とした、持続的かつ高度なサイバー攻撃は「国家支援型※77APT 攻撃」とも呼ばれる。国家支援型 APT 攻撃の特徴として、標的別に改変・開発したマルウェアの使用や、標的組織の内部に長期間潜伏して活動する点等が挙げられる※78。日本の企業・組織を標的とした攻撃は、継続的に発生しており、本項では、国家支援型 APT 攻撃を中心とした事例や注意喚起を紹介する。

(a) 国家支援型 APT 攻撃グループの攻撃事例

2025 年 3 月、日本等を標的としているサイバー攻撃グループである MirrorFace（別名 Earth Kasha）は、新たな攻撃キャンペーンを行った※79。MirrorFace は、国家支援型 APT 攻撃グループと見られており、2019 年ごろから日本のシンクタンク、政府、政治家、マスコミ等に関係する個人や組織を対象としたサイバー攻撃が確認されている。2025 年 1 月には、MirrorFace によるサイバー攻撃に関して、警察庁、内閣サイバーセキュリティセンター（現 NCO）から注意喚起が行われた※80（「情報セキュリティ白書 2025※81」の「1.2.2 (2) (a) 標的型攻撃メールを用いた攻撃の事例」参照）。トレンドマイクロ株式会社（以下、トレンドマイクロ社）によると、今回の攻撃キャンペーンは、日本や台湾を標的としたサイバー諜報活動や情報窃取が目的と見られ、以前から攻撃に利用されている「ANEL」と呼ばれるマルウェアの新型亜種の利用が判明したという。

手口としては、標的に対して Microsoft OneDrive のリンクが埋め込まれたスピアフィッシングメールを送信し、そ

のリンクをクリックさせることで、不正な Microsoft Excel ファイルを含んだ Zip ファイルをダウンロードさせる。この Excel ファイルを開き、指示どおりの操作をしてしまうことで、最終的に ANEL がインストールされる。メールの件名やファイル名には、「xx_ 修正済み履歴書」や台湾語で「臺日道路交通合作與調研相關公務出國報告」（日本語訳「日本 - 台湾の交通協力・研究に関する海外出張報告書」）のようなメール受信者の関心を引く名前が付けられていた。また、メール自体も正規のアカウントから送信されており、正規のアカウントが不正アクセス等によりメール配信の踏み台として悪用されたと考えられている。MirrorFace は、被害環境に展開された ANEL を利用して、被害環境からスクリーンショットを含む様々な情報を取得し調査を行っていたと見られ、意図した標的の環境に侵入できたことが確認された場合には攻撃の第 2 段階に進行していた。攻撃の第 2 段階では、ANEL を介して、第 2 段階用の高度なバックドア「NOOPDOOR」を展開し、その際に活動の永続化も試みられた可能性があるという。

こうした国家支援型 APT 攻撃グループによる攻撃は、警察庁でも 2025 年中に関与が疑われるものを複数確認しているとして、今後も日本を標的とした攻撃の継続が懸念される※32。

(b) Salt Typhoon 等に関する国際注意喚起

2025 年 8 月 27 日、警察庁及び NCO は、米国が作成した国際アドバイザリー「Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System※82」の共同署名に加わり、国家支援型 APT 攻撃グループ「Salt Typhoon」等に関して、支援国を特定して公表するパブリック・アトリビューションと注意喚起を実施した※83。共同署名には、米国、オーストラリア、ニュージーランド等を含む 13 ヵ国が加わった。

注意喚起によれば、中国の国家支援型 APT 攻撃グループは、中国系企業と関連があり、サイバー関連の製品やサービスの提供を受けているという。また、初期侵入には、ゼロデイ脆弱性を悪用することはほとんどなく、既存の脆弱性を悪用して初期侵入を行い、永続的なアクセスを確立している、と警告した。初期侵入に悪用されている脆弱性としては、以下が指摘されている。

- Ivanti Software, Inc. の CVE-2024-21887※84
- Palo Alto Networks, Inc. の CVE-2024-3400※85
- Cisco Systems, Inc. の CVE-2023-20273※86 及び CVE-2023-20198※87

初期侵入後には、ネットワークデバイス間での水平展開が行われ、最終的にはデータが窃取される。

当該アドバイザリーでは、Salt Typhoon 等の国家支援型 APT 攻撃グループの活動に関して、標的となり得る組織に対する推奨実施事項をまとめたガイダンスや緩和策をまとめている。

(c) ORB 化を伴うネットワーク貫通型攻撃への注意喚起

IPA は 2025 年 10 月、「VPN 機器等に対する ORB（Operational Relay Box）化を伴うネットワーク貫通型攻撃のおそれについて※88」と題した注意喚起を行った。注意喚起の背景には、2025 年にネットワーク境界に設置される VPN 機器等において深刻な脆弱性が相次いで報告され、攻撃に悪用される事例が確認されていたことがある。脆弱性の悪用によって、「1.2.2 (1) (b) ネットワーク貫通型攻撃の手口」でも示したとおり、自組織のネットワーク内に不正アクセスされ情報が窃取されることに加え、機器が攻撃者に乗っ取られ、ORB として第三者への攻撃の踏み台として利用されるおそれもある。悪用が懸念される脆弱性の例としては以下が挙げられ、実際にこれらの脆弱性を悪用した攻撃も確認されている※89。

- NetScaler ADC 及び NetScaler Gateway（CVE-2025-7775 等）※90
- Ivanti Connect Secure 及び Policy Secure 等（CVE-2025-22457）※91
- Fortinet 製 FortiOS 及び FortiProxy（CVE-2024-55591）※92

当該注意喚起内では迅速なパッチ適用や機器の更新、公開設定の最小化等を例に挙げ、VPN 機器等の利用者に注意を促している。

(d) 大手の自動車会社が標的となった事例

2025 年 9 月 2 日、英国の大手自動車メーカーである Jaguar Land Rover Automotive PLC（以下、JLR 社）は、サイバー攻撃を受け、被害を最小限に抑えるためシステムを予防的に停止したことを公表した※93。攻撃は同年 8 月末に発生したとされ、システム停止の影響もあり、ソリフル工場を含む英国にある複数の工場で操業が停止し、英国内の販売店は新車登録や部品供給ができなくなったという※94。JLR 社は英国最大の自動車メーカーとして自動車産業のサプライチェーンの頂点に位置する企業であり、サプライチェーンにおける影響も大規模だった。従業員数約 5,000 人を擁するスロバキアのニトラ工場で

は数日間の生産が停止したほか、英国、スロバキア、ブラジル及びインドの工場で合わせて数千人の従業員の休業状態が少なくとも9月11日まで続く見込みとされた※95。また、サプライチェーン関連企業の従業員数千人も、操業停止の影響で一時解雇されたという※96。また、影響を受けた企業は英国全土で5,000組織に及ぶとも言われた※97。

JLR社は事態が長期化したことで、複数回にわたる操業停止の延長を余儀なくされ※98、最終的に操業を再開できたのは10月8日からと、実に5週間以上に及ぶ操業停止となった※99。英国政府では一連の事態を受けて、取引先のサプライヤーを救済するために支援策を協議し、9月28日には15億ポンド（3,240億円※100）の融資保証を発表するという国家経済に影響を及ぼす事態に発展した※101。

同事例では、JLR社から攻撃に関する詳細が明らかになっていないものの、攻撃発生当初には、「Scattered Lapsus$ Hunters」という攻撃グループからの犯行声明があった※102。その後、別の報道では、上記攻撃グループではなく、ロシアのハッカー集団による関与が疑われた。攻撃者は既知の脆弱性を悪用し、複雑な暗号化を行える高度なランサムウェアを展開したとされる。金銭の要求がなかったことから、英国の経済基盤を標的とした、ランサム攻撃を装ったサイバー攻撃であった可能性もあるという※103。また、この攻撃は、社内スタッフを装ったボイスフィッシングがきっかけで、JLR社の従業員の認証情報が詐取されたという。その後、取得した認証情報を用いて、通常の認証フローを突破し社内ネットワークへ侵入したと見られる※104。

(3) 標的型攻撃への対策

攻撃者は多種多様な手口で、用意周到に準備をした上で計画的かつ巧妙に攻撃を行う。また攻撃手法も随時アップデートされている。そのため、従来有効であった対策が、新たな攻撃手口に対して十分に機能しない場合もある。特定の対策のみに頼らず、システム全体で複数の対策を組み合わせた多層防御が必要である。組織の規模や業種により取り得る対策は異なるが、情報資産を守るためには、あらゆる可能性を想定し、情報資産の重要度と対応に要する費用も考慮して、対策を選別し、実施することが重要である。

また、国家支援型APT攻撃への対応は、国家のサイバー安全保障上の課題であり、政府が率先して情報提供し、官民双方向の情報共有の促進が求められる。政府からの適切な情報提供のためには、サイバー空間の状況を適切に把握することが必要であり、そのためには、被害組織に係る属性情報等のサイバー空間の状況把握に資する情報が民間事業者側から政府に共有されること（我が国のサイバー分野におけるカウンターインテリジェンスへの民間事業者の参加）が不可欠である※105。

以下に、標的型攻撃への対策の例を示す。

(a) 役職員の意識向上

役職員の意識向上を目的とした対策例を以下に示す。

- 不審メールに対する注意力の向上

  標的型攻撃メールでは、標的組織に関連する人・組織をかたる、組織や業界固有の用語等を用いて自然な文章を装う、標的組織の役職員の関心を引く題材を送る、標的組織の役職員への依頼事項を投げかけてその後のやり取りを続け油断させる等の受信者を騙す巧妙な手口が使われる。役職員自身も日頃から不審メールに対する意識を高め、不用意に開封や返信をしないこと、不審なメールだと少しでも疑われる場合は組織のシステム管理者に連絡することが求められる。例えば、正規のメールアドレスから受信したメールであっても、拡張子が.vhdや.isoといった日頃のやり取りでは見かけない形式のファイルが届く場合や、Google DriveやMicrosoft OneDrive等のリンクからファイルをダウンロードさせようとする場合等、普段と少しでも異なる状況や違和感があれば、不審と判断して、添付ファイルを開いたり、リンクをクリックしたりせず、送信者や所属組織のシステム管理者等に確認・相談することが求められる。また、添付ファイルやダウンロードしたファイルを開いた際に、Microsoft Office文書のマクロ「コンテンツの有効化」ボタンをクリックするよう誘導される場合があるが、安易にクリックせず、受信したファイル内容（論文、申込書、案内等）の表示・閲覧にマクロのような高度な機能が真に必要か検討し、不審と感じたらファイルの提供元に確認することが求められる。このような意識を高めるため、組織として役職員に標的型攻撃を見抜くための教育や注意喚起、標的型攻撃メール訓練を実施することは、標的型攻撃による被害を防ぐ（または事後的に被害に気付く）のに有効である。また、標的型攻撃メールが私用メールアドレス宛てにも送られることを踏まえ、そのようなメールを組織のメールアドレスに転送することでメールのフィルタリングが適切に機能しないケースや、組織内で私用メールアドレス宛てのメールをWebメール等

で閲覧したり、不審な添付ファイルを開いたりすることにより組織内のシステムがマルウェアに感染するケースも起こり得るため、そのようなことを行わないよう役職員のリテラシー向上も必要である。

- SNSを悪用した手口の周知
  攻撃グループが、SNSで標的組織の役職員への接触を図り、悪意あるURLリンクやファイルを送り、それを開くように誘導することで初期潜入経路を開拓する手口がある。このような手口があることや、SNS上で所属組織の情報を開示することの是非を含めた注意点を役職員に周知し、役職員の警戒意識を高めることは対策として有効である。

(b)組織としての対応体制の強化

組織として攻撃に対応するための体制強化を図る対策例を以下に示す。

- CSIRTの設置と運用
  組織の役職員が標的型攻撃メール等の不審なメールを受信した際に、連絡するべき窓口が組織内に存在することは重要である。また、セキュリティ機関やベンダー、利用者(顧客)等の組織外部からの連絡を受けて標的型攻撃の被害に気付くことも考えられるため、外部からの連絡を受け付ける窓口を設けることも重要である。このような、組織内部と外部との適切な連絡体制の整備や、セキュリティインシデントが発生した際の調査・分析、セキュリティの教育・啓発活動等を実施する体制のことをCSIRT(Computer Security Incident Response Team)と呼ぶ。セキュリティインシデントの未然防止、またはインシデント発生時の迅速な対応を行うために、CSIRTやそれに準ずる体制を組織内に設置することは有効な手段である※106。
- インシデントの発生を想定した事前準備
  組織内にCSIRTの体制を整えるだけでなく、実際にセキュリティインシデントが発生した際に事業を継続できるように、サイバーセキュリティの観点を組み込んだBCPの策定、BCM(Business Continuity Management:事業継続マネジメント)の実施が重要である。CSIRT向けの取り組みでは、他組織で発生したインシデントや自組織で起こり得るインシデントを基にシナリオを作成し、インシデントの発生を想定した演習や訓練を行うことが望ましい。演習や訓練を通じて、自組織の対応能力の維持・向上、現在の対応力や体制の問題点の発見・改善を行う。これらは、組織全体、ひいてはサプライチェーン全体の対応力・回復力(サイバーレジリエンス)の強化に有効である。
- 攻撃の手口や対策の把握と情報共有
  標的型攻撃が発生すると、セキュリティベンダーやマスコミ、あるいは被害組織自体から、攻撃手口や対策に関する情報が公表されることがある。また、業界内でのサイバーセキュリティに関する情報共有体制を通じて、他組織で発生した標的型攻撃の情報を得られる場合もある。これらの情報をCSIRTが継続して収集し、対策に活用していくことが重要である。例えば、攻撃グループの侵入手口が特定機器の脆弱性を悪用したものであれば、自組織のシステムに該当する機器がないか確認し、該当するものがあれば速やかに脆弱性修正プログラムを適用する。標的型攻撃メールの情報が得られた場合は、組織内にその特徴を周知し、メールのフィルタリング設定を行うことで、被害防止につなげることができる。もし、自組織が国家支援型APT攻撃を受けた場合(またはその可能性が疑われる場合)には、前述の情報共有体制や、警察・IPA等の政府機関・政府関係機関と連携し、攻撃に関する情報を積極的に共有していただきたい※107。情報を共有することで、対応方法等のフィードバックを得られる場合がある。また、組織間の情報共有が活発化することで、より多くの攻撃事例や知見が共有される。これにより、他組織だけではなく自組織の攻撃被害の防止につながることも期待できる※108。なお、攻撃の意図や潜在的な被害組織の推定のためには、攻撃の手口やIoC等の情報のみならず、標的組織・個人の属性(専門分野等)の情報共有が不可欠であるので、これらの情報についても積極的に政府機関・政府関係機関に共有いただきたい。
- 海外拠点・サプライチェーン等を意識したセキュリティ対策の強化
  セキュリティ対策が不十分な子会社や関連会社、取引先企業、海外拠点を初期侵入の標的にする手口(「アイランドホッピング攻撃※109」と呼ばれる)がある。このため、自組織と関わりのある組織全体を意識したセキュリティ対策の強化が求められる。具体的には、子会社や関連会社、及び海外拠点においても国内拠点と同様に、セキュリティポリシーを策定、周知し、またセキュリティリスクの可視化、改善や対策を行うことが望ましい。これらの対策を実施する際は、海外拠点所在地の法制度や労働慣行の違い等も把握して、国内と同一の対策が取れない場合は代替策を考える必要がある。取引先等のサプライチェーンのセキュリ

ティ対策強化の取り組み例としては、取引先の選定時にセキュリティ関連の認証取得状況等の取り組みを考慮する、取引先とセキュリティに関して担うべき役割と責任範囲を明確化する、セキュリティ対策の共同実施や導入の支援を実施する、第三者によるセキュリティ対策の評価検証を実施する、セキュリティに関する情報共有を行うこと等が挙げられる。経済産業省とIPAが策定した「サイバーセキュリティ経営ガイドライン※110」に記載された対策例や、上述の政府機関・政府関係機関との連携も参考にしてほしい。また、組織の保有する重要情報を適切に保護するという観点から、IPAが公開している「組織における内部不正防止ガイドライン※111」も参考にしていただきたい。

- セキュア・バイ・デザイン機器の調達
  市場に出回るIT機器の中には、想定しない通信が発生したり、発見された脆弱性が放置されたりするものも存在しており、ネットワーク貫通型攻撃で侵害されるリスクがある。そのようなリスクを低減させるためには、セキュア・バイ・デザインの原則に基づき、設計段階からセキュリティを考慮するとともに、脆弱性対応等の継続的なサポートを含め、製品のライフサイクルを通じてセキュリティが確保された機器を選択する必要がある。2025年3月に運用が開始されたIoT製品に関するセキュリティラベリング制度「JC-STAR」の適合ラベルを取得した製品や、同様の認証を取得した製品を調達することが有効な対策となる（JC-STARの詳細については「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）。また、IT機器の調達に関するサプライチェーンを構成する組織や機器の製造国・地域等の情報も考慮して調達する機器を選定することも有効な場合がある※112。
- 脆弱性に対応する仕組みや体制の構築
  OSやアプリケーション、ネットワーク境界に接する機器等のシステムの脆弱性を悪用する攻撃に対抗するために、自組織が利用しているソフトウェアや機器の脆弱性情報と一時的な緩和策を含む対策方法をいち早く入手し、自組織に展開できる体制作りが重要である。IT資産管理システム等を活用することで、自組織のサーバーや端末等に既知の脆弱性がないかを確認し、脆弱性修正プログラムの適用等の対応を漏れなく行える仕組みを作ることが望ましい。特に「1.2.2(1)(b)ネットワーク貫通型攻撃の手口」で紹介したように、VPN機器等のネットワーク境界に接する機器やセキュリティ製品は、脆弱性が悪用される事例が確認されているため、組織内のそれらの資産を把握するとともに、一時的な緩和策を含めすぐに対応できるような体制が望ましい。
- 保護すべき重要情報の特定及び内部不正対策の基本方針の策定等
  近年、テレワークやクラウド利用の普及に伴い、組織の重要情報は分散して管理される傾向が強まっている。このため、内部不正を防止する観点から、自組織が保有する重要技術情報等の重要情報を特定し、適切な漏えい対策を講じる重要性が増している※113。これは、経済安全保障の観点や、標的組織の保有する機密情報の窃取を目的とする標的型攻撃への対策としても重要である。しかしながら、個人情報以外の重要情報の特定や漏えい対策が不十分な企業が多い実態が指摘されている※114。内部不正を含む重要情報の漏えいリスクに対応するためには、自組織が保有する重要情報を特定することに加え、全社的に取り組むことができる体制を整備する必要がある。具体的には、経営層が基本方針を策定し、その方針に基づく組織横断的な計画を承認するとともに実施を統制し、更に適切な権限移譲により具体的対策の実効性を確保することが重要である。IPAの「組織における内部不正防止ガイドライン」も参考に内部不正対策に取り組むことが、国家支援型APT攻撃への対策にもつながると期待される※115。

(c)システムによる対策

システムによる対策例を以下に示す。

- 不審メールを警告する仕組みの導入
  自組織のメールシステムでメール受信時に、送信者（From）メールアドレスの偽装や、フリーメールアドレスの利用、悪用されやすい添付ファイルの拡張子やファイルタイプ、メール内のURLリンク先の情報を検査し、フリーメールアドレスから送られてきたメールや添付ファイル等について、必要に応じて受信者に警告することで、不審メールであると気付く機会を与えることが可能である。自組織のドメインを偽装するメールへの対策には、メールの送信元ドメインを認証するDMARC（Domain-based Message Authentication, Reporting and Conformance）の適切な運用が有効である※116。また、添付ファイル付きメールの受信時やインターネット上のファイルダウンロード時には、マルウェアの検査はもちろん、サンドボックスと呼ばれる隔離された環境でファイルを動的に解析する仕組みを採用することも有

効である。なお、オンラインで提供されるマルウェア検査やサンドボックスのサービスの一部では、ファイルをアップロードすることで意図せず情報漏えいにつながる危険性があるため、十分な注意が必要である。加えて、セキュリティインシデント発生に備え、不審メールを確保できる仕組みを導入することが望ましい。不審メールを調査可能にしておくことで、影響範囲等の解析が可能となり、解析結果を組織全体で共有し対策を取ることができる。

- 通常業務で使わないファイルの実行防止・ソフトウェアの利用防止
  役職員が通常の業務では使わないファイルやソフトウェアについては、あらかじめ、システムやポリシーで実行できないよう制限することが望ましい。具体的には、あらかじめ業務等で必要なソフトウェアや実行可能なファイルの種類を洗い出し、それらの実行のみを許可し、他のものを禁止すること（許可リスト方式）で、マルウェアへの感染を防止する。許可リスト方式による制限の実施が難しい場合は、端末で実行することが望ましくないファイルの種類やソフトウェアを特定し、実行を禁止する（拒否リスト方式）。例えば、拡張子が .vhd や .iso といった業務で使用しないであろうファイルや、「ClickFix」と呼ばれる手口※117 で用いられる PowerShell スクリプトについて、業務影響を考慮した上で実行を禁止することが有効である。
- 利用方法の変化に伴うセキュリティ対策の見直し
  標的型攻撃においては、働き方の多様化やクラウド利用の浸透等、システムの利用方法の変化に伴い発生する脆弱性を狙われるケースも考えられる。働き方の多様化により、仕事場を従来の職場に限定しないテレワークや、BYOD（Bring Your Own Device：私物端末の業務利用）が一般化することで、これまでのような組織内ネットワークとインターネットの境界におけるセキュリティ対策だけでは、侵害を防ぐことが難しくなってきている。そのため、パソコンや携帯端末等のエンドポイントにおいて不審な挙動を監視し、攻撃活動の抑え込みを行う EDR 製品の導入等も有効な対策である。EDR 製品は、すべてのマルウェアに対して万能ではないものの、ファイルレスマルウェア※118 や未知のマルウェア等の検知・対策にも有効な可能性がある。また、クラウドの利用等によって、業務情報を自組織のシステム外に保管するケースも増えている。そこでデータの持ち出しや流出の可能性を考慮したセキュリティ対策として、ファイルの暗号化や DLP（Data Loss Prevention）等の対策の導入を検討する必要がある。また、クラウドネイティブ環境における様々なリスクに対処するため、設定管理や権限管理、データセキュリティ管理等を包括的に提供する CNAPP（Cloud Native Application Protection Platform）ソリューションの活用も検討いただきたい※119。
- 取得するログの種類と保存期間の定期的な見直し
  標的型攻撃は巧妙化しており、これまでに記載した対策だけでは防げない可能性もある。標的型攻撃を受けて万が一侵入されてしまった場合でも早期に検知できるように、各端末や各セキュリティ製品、ネットワーク機器等で取得するログの種類を定期的に見直すことや、ログの監査方法を見直すことも有効である※120。また、標的型攻撃は長期にわたる場合もあるため、過去の攻撃の痕跡を調査できるように、ログの保存期間についても定期的に見直しを行うことが望ましい。更に、入手した IoC 情報を各機器のログ調査やフィルタリングに活用するため、検索やフィルタリングの機能の有無を確認し、対応フローを確認しておくことも重要である※121。
- Attack Surface Management ツールの導入
  経済産業省は、「ASM（Attack Surface Management）導入ガイダンス」を公開している※122。Attack Surface（アタックサーフェス：攻撃対象領域）とは、組織の外部からアクセス可能で、攻撃の対象となり得る資産や接点を指す。例えば、ネットワーク機器や Web サービス等、外部（インターネット）との境界に位置するものがこれに含まれる。サイバー攻撃の初期段階では、公開情報やインターネットからアクセス可能な資産から得られる情報により偵察が行われ、脆弱な部分を狙われて侵入されることがある。こうした攻撃から自組織の資産を守るため、Attack Surface を把握・管理（Management）する手法を ASM と呼ぶ。セキュリティベンダーが提供する ASM ツール等を用いることで資産を一元管理し、収集した脆弱性情報と資産を突き合わせて、リスクの評価・可視化等ができる。これにより、脆弱性が早期に発見でき、迅速かつ適切に対応を行うことで攻撃のリスクを減らし、自組織を標的型攻撃から守ることにつながる。とりわけ、従来、ISDN 等の専用線で接続されていたものを、VPN 機器等を用いたインターネット上での VPN 等によるカプセル化に置き換えた場合、それらの機器がシステム管理や権限把握の及ばない Attack Surface となるおそれがあるため※123、そのような機器の有無を確認し、

発見された場合にはASMの対象とすることが重要である。また、Attack Surfaceを網羅的に把握するために、検索エンジン型のASMツール等で自組織名、自組織のブランド名を検索する等、攻撃者が発見するのと同様の方式で未把握のAttack Surfaceを発見することも望ましい。

- アカウントの棚卸し及びアクセス権限の定期的な見直し
組織内のアカウントが悪用される事態も想定し、不要なアカウントを作成せず、作成したアカウントには必要最小限のアクセス権限を与えることとし、退職時には退職者のアカウントを削除することや、定期的に棚卸しを行い、権限付与の妥当性や不要なアカウントが存在していないか等を確認することが重要である。標的型攻撃では、Active Directoryサーバー等の認証基盤が侵害されるケースがあり※124、退職者のアカウントが残存していた場合、内部不正の問題に加えて、退職者の個人情報漏えいの問題も生じ得る※125ため、アカウントの棚卸しを含む適切な管理が求められる。

1.2.3 DDoS攻撃

DDoS（Distributed Denial of Service）攻撃とは、インターネットに公開されたWebサーバー等に対して、攻撃者が何らかの方法で、複数の送信元から同時に大量の正常なリクエストを送信することで、攻撃対象となったサーバーのリソースに一般利用では発生し得ない過度の負荷をかけ、提供していたサービスの運用を妨害する攻撃である。

近年、このDDoS攻撃が、外交・安全保障上の対立をきっかけとして、他国の様々な活動への妨害や報復の手段として行われることがある※126。

2025年1月には一般財団法人日本気象協会が運営する天気予報サイト※127、2025年6月末から7月中旬にかけては化学物質を扱う企業（「1.2.3（2）DDoS攻撃の国内事例」参照）等がDDoS攻撃の被害に見舞われ、日本国内でもDDoS攻撃への危機感が高まっている。

本項では、2025年度に確認されたDDoS攻撃について動向とともに事例と手口、対策を解説する。

（1）DDoS攻撃の世界的な動向

ISP・通信事業者に強い観測網を持つセキュリティベンダーであるNetScout Systems, Inc.のレポートによると、2025年上半期に全世界の同社ユーザーで観測されたDDoS攻撃は800万件以上に及び、最大帯域幅として3.12Tbpsの攻撃を観測した。また、攻撃者は、AIによる脆弱性のスキャンによって、DDoS攻撃に使用する「ボットネット」（「1.2.3（3）ボットネットを使用した攻撃の手口」参照）を構築するプロセスを加速させているという※128。

EUのサイバーセキュリティ専門機関であるENISAが公開している年次レポートである「ENISA Threat Landscape 2025」によれば、政治的・社会的意見の主張をサイバー攻撃によって行うハクティビスト（「ハッカー」と「アクティビスト」を組み合わせた造語）による攻撃が、ENISAへの報告件数の約80%と大部分を占めており、主に影響が限定的なDDoS攻撃によるものであるという。

中でも、親ロシア派のハクティビスト集団である「NoName057(16)」については、2025年7月に欧州刑事警察機構（Europol：European Union Agency for Law Enforcement Cooperation）等による合同作戦が実施され、構成員の逮捕者が出たほか、同集団に関連する100台以上のサーバーが世界各地で停止された。しかし、その後も同集団は活発に活動を継続している※129。このグループは、主に通信、輸送、エネルギー、防衛分野等を標的に、近年ではAIによる攻撃の自動化といった手法を用いて、2025年3月にはスペイン、台湾、ウクライナの政府系Webサイトを標的に攻撃を仕掛けている※130。

DDoS攻撃の増加要因については、ロシア・ウクライナ戦争や、米国・イスラエルとイランによる軍事衝突等の国家間の対立を激化させる出来事が、要因の一つとして挙げられる。戦争や軍事衝突の発生に伴い、攻撃対象国の政府機関や通信・エネルギー等の重要インフラに対して大量のDDoS攻撃を行い、オンラインサービスへのアクセスを不能または著しく低下させることで、国家機能や社会サービスの継続的な運用を妨害することが主な目的であるとの見方もある※131。

DDoS攻撃の種別に目を向けると、CDN（Content Delivery Network）※132ベンダーであるCloudflare, Inc.（以下、Cloudflare社）のレポートによれば、DDoS攻撃件数は全体として増加しているが、その内訳は変化しており、攻撃対象のネットワーク帯域の枯渇を狙うタイプのDDoS攻撃が、2025年には前年比で3倍以上に増えているという※133。

（2）DDoS攻撃の国内事例

ここでは、2025年度における、国内のDDoS攻撃に関する主な事例を紹介する。

- 企業の公開サーバーへの攻撃事例
  2025年の6月末から7月中旬にかけて、化学系の物質を取り扱う株式会社ナード研究所の公開サーバーがDDoS攻撃と見られるサイバー攻撃を受け、被害が発生したとされる。6月26日に一時的にネットワークの不具合が発生し、同社のメールの受信、公開Webページへのアクセスができない障害が発生したが、1週間以内に問題が解消し、復旧した※134。しかし翌月上旬に再度同じ事象が発生したとのことである※135。情報の漏えいは確認されていないが、断続的に攻撃が行われたことでメール送受信やWebページへのアクセスの遅延・不達が発生し業務に影響を及ぼした※136。
- 企業が提供するサービスへの攻撃事例
  2025年7月末にカゴヤ・ジャパン株式会社は、同社がサービスを提供するビジネスWebメールサービスである「Active! Mail」に対し複数のIPアドレスから大量のログイン試行が発生しアクセス不可となったものの、1時間後には攻撃元の一部地域のIPアドレスからのアクセスを遮断し、システムが復旧し再度利用可能となったことを発表した※137。

前者はDDoS攻撃により業務利用のインフラが使えなくなった事例であり、後者は展開するビジネスに支障をきたした事例で、影響範囲は異なるものの、ともに深刻な影響が発生している。

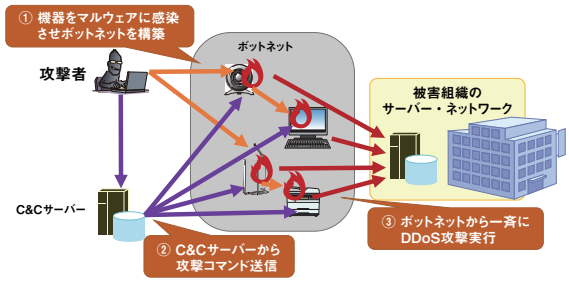
(3) ボットネットを使用した攻撃の手口

DDoS攻撃の成立には、対策されにくいリクエストを大量に発生させることが必要であり、多くの場合、「ロボット」と「ネットワーク」を組み合わせた造語である「ボットネット」と呼ばれる仕組みが使用される※138。

ボットネットとは、マルウェアによる感染等で攻撃者の制御下にあるパソコンやIoT機器等（「ボット」と呼ばれる）で構成された攻撃インフラである。規模が大きいもので数百万台のボットで構成されるものもある。ボットネットによるDDoS攻撃の流れは以下のとおりである（図1-2-7）。

①ボットネットの構築
パソコンや、家庭用ルーター、ネットワークカメラ等のインターネットに接続されているIoT機器にマルウェアを感染させ、攻撃インフラとしてボットネットを構築する。

② C&Cサーバーから攻撃コマンドを送信
構築したボットネットに対し、C&Cサーバーから DDoS攻撃コマンドを送信する。



■図1-2-7　ボットネットによるDDoS攻撃の手口のイメージ

③攻撃実行
DDoS攻撃コマンドを受け取ったボットネットから一斉に大量のパケット等を送信し、攻撃対象のサーバーやネットワークに負荷をかける。

比較的安価で導入が容易なIoT機器は、手間をかけずに設定や運用が行われていることがあり、以下のような要因によりボットネットに組み込まれやすいと考えられる。

- 推測されやすい管理用パスワード
  初期設定のまま変更されていないパスワードや文字数の少ない単純なパスワードが管理者パスワードとして使用されている場合、簡単に推測され不正にアクセスされてしまう。
- ファームウェアのアップデート未実施
  最新のファームウェアにアップデートされていない場合、既知の脆弱性に未対応である、セキュリティ機能が未実装である等により、攻撃に悪用される可能性がある。
- 脆弱な設定のままでの放置
  不要なサービスやアプリケーションの通信を許可する設定や、どこからでも管理画面にアクセスできる設定等になっている場合、攻撃に悪用される可能性がある。

(4) DDoS攻撃への対策・対処

DDoS攻撃に対しては、まず業務に関する重要なシステムや組織が提供しているサービスへの攻撃に対し、平時から攻撃を想定した対策を実施すること、及び実際に攻撃の被害に遭った場合の対処方法を決めておくことが必要である。また、意図せず他者へのDDoS攻撃に加担してしまうことを防ぐため、組織が管理または所有するルーターやネットワークカメラ等で、セキュリティ対策が疎かになりがちな機器が乗っ取られないようにする対策も求められる。これらの対策についてそれぞれ解説する。

なお、2025年2月に内閣サイバーセキュリティセンター（現NCO）より発出された注意喚起にて、DDoS攻撃に対する対策がまとめられているため、そちらも参照いただ

きたい※139。

(a) DDoS 攻撃への対策

以下に、DDoS 攻撃に対する防御・被害軽減のための具体的な対策を挙げる。

- サービスの重要度に応じて、費用をかけて守る必要があるサービスと、一定期間の停止を許容できるサービスを選別し、優先順位を付けて対応する。例えば、EC サービスは事業の中核であるため重点的に対策する等、選別したサービスごとに費用やスケジュールに差を付けた対策方針を策定する。選別した各サービスについて、そのシステムを分離することが可能な場合は分離することを検討する。具体的には、顧客情報等の重要な情報を保管しているサービスや、外部に公開されているような狙われやすいサービスは、そのシステムを他のシステムから分離構成することで、相互に影響を受けないようにする。
- DDoS 攻撃を受けた際、迅速に対応できるように、社内・社外の関係者、利用している ISP 事業者、ホスティング／クラウドサービス事業者、関係する行政機関及び警察等への連絡先をまとめておく。加えて、各主体への対応方法について対応マニュアルや BCP を策定しておくことが肝要である。
- 取引先や顧客等の利用者に対して、DDoS 攻撃を受けていてサービスに接続しづらい、または接続できない状態にあることを知らせることができるように、SNS 等のアカウントや、通常のサービス提供とは別の Web サーバーに状況を通知できるよう準備しておく。
- サーバーやネットワーク機器にて同一 IP アドレスからのアクセス回数を制限し、タイムアウトの設定を見直す。
- ランダムサブドメイン攻撃は、生成される通信先が次々と変化するため、事前の遮断や固定的なルール設定が難しく、根本的な対策が難しい DDoS 攻撃と言える。このような DDoS 攻撃に備えて、サービスを提供しているサーバーやネットワーク機器の性能強化、CDN の導入及び契約しているネットワーク回線の増強や冗長化等を検討する。
- CDN を導入している場合には、配信用のコンテンツを格納しているオリジンサーバーを保護する。具体的には、オリジンサーバーへのアクセスを CDN のみに制限し、オリジンサーバーの IP アドレスは DNS レコードに登録しない。また、過去にオリジンサーバーで利用していたグローバル IP アドレスについても、外部サービス等によって第三者に特定される可能性があるため、CDN 導入後に変更することが望ましい。
- サービスの重要性によっては、攻撃を受けていない、異なる組織である ISP 事業者等の提供する DDoS 攻撃対策サービスや、セキュリティベンダー等が提供する DDoS 攻撃対策製品の利用を検討する。
- WAF（Web Application Firewall）※140、IDS/IPS（Intrusion Detection System/Intrusion Prevention System：不正侵入検知／防止システム）、UTM（Unified Threat Management）、DDoS 攻撃対策専用アプライアンス製品等の DDoS 攻撃を排除または低減するための装置やサービスを導入する。
- 中小企業を含むあらゆる規模の組織が標的になり得るため、技術的対策に加え、金銭的な損害への対策としてサイバー保険の活用を検討することを推奨する。主要な損害保険会社ではサイバーリスクを対象とした保険商品が提供されており、近年ではサイバー保険を活用する事例が増えつつある。
- 技術的対策に加え、法的な対策を整えることも併せて推奨する※141。DDoS 攻撃を受けた企業であっても、サービス停止により被害を受けた顧客や取引先から損害賠償を求められる可能性がある。十分なセキュリティ対策を講じていなければ、過失と判断され法的責任を負うおそれもある。このようなリスクに備えるため、以下の内容について事前に弁護士へ相談し、適切な契約書・利用規約を整備しておくことを推奨する。
  - DDoS 攻撃発生時の責任範囲・免責を含む、顧客向けの契約書・利用規約の整備
  - DDoS 攻撃発生時の対応協力、費用負担、法的責任の分担を含む取引先との契約書の整備

(b) DDoS 攻撃の被害に遭った場合の対処

DDoS 攻撃による通信データを遮断し、サービスを提供するサーバーやネットワークのリソースを保護する対処が必要である。正常なアクセスと DDoS 攻撃によるアクセスを、どのように切り分けるかが対処のポイントとなる。攻撃者が攻撃元の IP アドレスや攻撃方法を定期的に変更する場合があるため、変化に応じた対処ができるように、継続して監視を実施する必要がある。

以下に、DDoS 攻撃を検知した場合の具体的な対処方法を挙げる。

- アクセスログや通信ログ等を確認し、攻撃が特定の IP アドレスから行われていると判断できる場合は、当該 IP アドレスからのアクセスを遮断する。
- 国内からのアクセスを主に想定しているサイトでは、海

外の IP アドレスからのアクセスを一時的に遮断することを検討する。

- 組織内で対処しきれない程、大規模な攻撃や執拗な攻撃を受けている場合は、ISP 等の関係事業者と連携して対策を実施するとともに、必要に応じて警察等への通報を行う。

(c) DDoS 攻撃に加担しないための対策

組織や個人で使用する機器が DDoS 攻撃に悪用されないように、セキュリティソフトの導入や機器への適切な設定等が必要である。

以下に、具体的な対処方法を挙げる。

- パスワードが初期設定のままの機器が存在しないか確認し、存在した場合は適切なパスワードに変更する。
- ネットワーク機器及び IoT 機器について、OS やソフトウェア、各種サービスが適切に運用されていることを確認する。特に、脆弱性を含むバージョンが利用されていないかを確認し、最新の状態に保つことが望ましい。
- ネットワーク機器や IoT 機器について、DDoS 攻撃に悪用される設定になっていないこと（例えば、不要なポートが開放されていない、不要なサービスを起動していない等）を確認する。更に、それらのサービスを組織内のみで利用している場合でも、意図せずインターネット上に公開されていないかを確認する。
- 外部と接続しているネットワーク機器や IoT 機器を介して組織内の他の機器に対して感染拡大を試みるマルウェアも確認されている。そのため、インターネットに直接接続していない機器においても脆弱性対策等を行う。
- インターネット側から IoT 機器の管理機能を利用する必要がある場合は、アクセス元を必要最小限に制限する。

また、組織の機器を DDoS 攻撃に悪用された場合に早期に検知できるよう、通信の監視を行う対策も推奨する。組織からインターネットへ送信される通信を監視し、異常な通信を確認した場合は、組織で管理している機器が攻撃に悪用されている可能性を考慮する。異常な通信を行っている機器が確認された場合、ネットワークから切り離し通信を停止させた後、マルウェア感染等の有無を調査し、対処を行う。自組織での対処が困難な場合は、関係当局やセキュリティベンダー等への相談を検討する。

1.2.4 情報システムの脆弱性を悪用した攻撃

情報システムにおける脆弱性は日々新たに発見され、製品開発者によって脆弱性を解消した修正プログラムがリリースされている。しかし、利用者が修正プログラムを適用せず、脆弱性を放置した場合は、サイバー攻撃の格好の標的となり、情報システムへの脅威となる。

IPA が発表した「情報セキュリティ 10 大脅威 2026[※142]」の「『組織』向け脅威」では、「システムの脆弱性を悪用した攻撃」が 4 位にランクインしている。この背景には、脆弱性の発見情報や修正プログラム（パッチ）が公開される前に行われるゼロデイ攻撃や、修正プログラムを適用するまでの期間を狙う N デイ攻撃といった、脆弱性を悪用した攻撃の高度化・容易化により、被害が拡大している実態がある。本項では、ゼロデイ攻撃と N デイ攻撃の動向や攻撃事例、対策等を解説する。

(1) ゼロデイ攻撃

ゼロデイ攻撃とは、ソフトウェアやハードウェアの脆弱性が製品ベンダーやセキュリティコミュニティに発見される前、あるいは修正プログラムが公開される前に、攻撃者がその脆弱性を悪用して行う攻撃である。「ゼロデイ」という名称は、製品やサービスの利用者が脆弱性の対策を講じるための時間がゼロ日（0 日）、すなわち対策を講じる猶予がまったくない状態を意味する。

通常、N デイ攻撃に対しては、組織はベンダーが提供する脆弱性情報をもとに脆弱性の影響を回避しつつ対策を行うが、ゼロデイ攻撃では十分な対策期間を確保するのが難しい。攻撃者は未知の脆弱性をベンダーの公表を待たずに発見するか、ダークウェブ市場で購入し、防御側が存在すら認識していない脆弱性を悪用して侵入を試みる。このため、ゼロデイ攻撃は防御が極めて困難であり、脆弱性の情報が公開された時点で既に被害が発生しているケースも多い。

(a) 2025 年におけるゼロデイ攻撃の世界での動向

2025 年のゼロデイ攻撃は、検知回避技術の巧妙化、そして国家支援型グループとランサム攻撃グループによる戦略的悪用という二つの特徴が顕著である。

第一の特徴である、検知回避技術の巧妙化について事例を紹介する。Ivanti Connect Secure の脆弱性（CVE-2025-0282）[※143]を悪用した攻撃では、攻撃者は侵害検出ツールを停止・改ざんし、偽のアップグレード進捗画面を表示することで管理者による異常検知を妨害した。

また、Cisco Secure Firewall ASA 及び Cisco Secure FTD の脆弱性（CVE-2025-20333/20362）※144 については、CISAが2025年、KEV（Known Exploited Vulnerabilities:既知の悪用された脆弱性）カタログに登録されたCVE(Common Vulnerabilities and Exposures：共通脆弱性識別子）で唯一の緊急対処指令（24 時間以内対応）を発令した※145。背景には、当該脆弱性を悪用した国家支援型攻撃キャンペーン「ArcaneDoor」による、ログ無効化、コマンド傍受、フォレンジック妨害等の高度な永続化技術が確認されたことがある。

第二の特徴のうち、ランサム攻撃グループによる戦略的なゼロデイ脆弱性（脆弱性対策情報が未公表の脆弱性）の悪用について事例を紹介する。ランサム攻撃グループ「Cl0P」（Clop、Cl0p とも表記される）は、Oracle E-Business Suite の脆弱性（CVE-2025-61882）※146 を 2025 年 8 月 9 日ごろから悪用し、9 月 29 日に攻撃の実施を公表した。このグループは、従来の暗号化による業務停止ではなく、情報窃取のみで経営層へ直接脅迫する手法を採用した※147。また、過去にも Accellion FTA、SolarWinds Serv-U、Fortra GoAnywhere MFT、Progress MOVEit Transfer、Cleo Harmony 等、主にファイル共有系製品の脆弱性を標的としており、脆弱性の特定・調達方法は不明だが、戦略的にゼロデイ脆弱性を悪用している可能性が指摘されている※148。

(b) 2025 年に公表された国内事例

2025 年には、国内でもゼロデイ脆弱性を悪用した攻撃により深刻な被害が発生した。

株式会社クオリティアが開発し、各プロバイダーに提供する国産 Web メールシステム「Active! mail」のリモートコード実行の脆弱性（CVE-2025-42599）は、少なくとも 2024 年 8 月ごろから侵害及び情報漏えいが発生していた可能性を IIJ 社が 2025 年 4 月に公表したことで注目を集めた※149-1。国内の複数の事業者が同製品を利用しており、サービス停止や攻撃検知の公表が相次いだ※149-2。国産製品であっても、ゼロデイ脆弱性が長期間悪用され得る事例として、国内組織に大きな衝撃を与えた。

Cisco Secure Email Gateway の脆弱性（CVE-2025-20393）※150-1 では、2025 年 12 月に「スパム検疫機能」がインターネットに公開されている機器を標的として攻撃が発生し、国内のインターネットサービスプロバイダーや大学が被害を受けた※150-2。修正プログラムの提供まで 1 ヵ月という長期間を要したことで、その間、組織はアクセス制限等の回避策及び暫定対応を必要とした。

Array Networks Array AG シリーズの脆弱性（CVE-2025-66644）は、東アジア地域限定製品であったため国際的な注目度は低かったが、IPA や JPCERT/CC が 2025 年 8 月以降に国内で悪用されたことを 2025 年 12 月に報告した※151。2025 年 5 月時点で修正プログラムが提供されたものの、CVE 番号が付与されていなかったため多くの組織が対応の優先順位を高く設定せず、脆弱な状態が継続した可能性がある。2025 年 12 月に CVE 番号が付与されてから注目が集まったが、既に数ヵ月にわたり悪用されていたことが判明した。

(c) 組織が実施すべき対策

ゼロデイ攻撃は本質的に未知の脆弱性を悪用するため、完全な予防は困難である。しかし、被害を最小化し、早期発見・早期対応を実現するため、以下のような多層的な防御対策を講じることが重要である。

- EDR の導入と振る舞い検知
  既知のシグネチャー（マルウェアやサイバー攻撃を識別するための特徴の情報）に依存して検知する従来型のセキュリティ対策では、シグネチャーが存在しないゼロデイ攻撃を検知するのは難しい。EDR を導入し、端末上の異常な振る舞い（不審なプロセス起動、権限昇格の試み、異常な通信パターン等）を検知する体制を構築する。機械学習や AI を活用した「次世代アンチウイルス（NGAV：Next Generation Anti-Virus）」と呼ばれるセキュリティソフトも有効である。
- 回避策の即時適用
  修正プログラムが提供されるまでの間、ベンダーやセキュリティ機関が提示する回避策（Workaround）を即座に適用する。例えば、特定機能の一時的な無効化、アクセス制限の強化、ネットワークセグメンテーションによる影響範囲の限定等である。
  Cisco Secure Email Gateway の事例では、修正プログラム提供まで約 1 ヵ月を要したため、この期間における回避策の実施が被害拡大防止において重要であった。
- 脅威インテリジェンスの活用
  ダークウェブ監視サービスや脅威インテリジェンスプラットフォームを活用し、組織が所属する業界や使用製品に関連するゼロデイ情報をいち早く入手する。特定の製品や技術に対するゼロデイ攻撃の兆候が観測された場合、先回りして監視を強化することが可能となる。
- 攻撃対象領域（アタックサーフェス）の最小化
  管理画面や管理系サービスの外部公開を最小限に抑

える。2025年はネットワークアプライアンス製品においてKEVカタログに掲載された脆弱性が過去最多（10ベンダー、27件のCVE）を記録し、その多くが管理画面や管理系ポートを対象としていた。本来外部公開すべきではないサービスを特定し、VPN経由でのみアクセス可能とする等、攻撃対象となり得る領域を減らすことが重要である。

- 複数の検知手段の併用
  Ivanti Connect Secureの脆弱性のように侵害検出ツールが改ざんされる事例が確認されていることから、単一の検知ツールに依存せず、複数の独立した監視手段を併用する。ネットワークトラフィック監視、ログ分析基盤（SIEM：Security Information and Event Management）、ファイル整合性監視（FIM：File Integrity Monitoring）等、異なるレイヤーでの監視を組み合わせることで、攻撃者による検知回避を困難にする。
- 脆弱性管理プロセスの高度化
  ゼロデイ脆弱性に対して、修正プログラムが公開されNデイ脆弱性となった際、迅速に修正プログラムを適用できる体制を整備する。NetScaler ADC（旧Citrix ADC）及びNetScaler Gateway（旧Citrix Gateway）の脆弱性（CVE-2025-5777[※152]、CitrixBleed 2とも呼ばれる）の事例では、当初「悪用なし」とされていたが、数ヵ月後にAmazon Web Services, Inc.が修正プログラム公開前から悪用されていた可能性を公表した[※153]。このように、ゼロデイとNデイの境界は流動的であり、継続的な情報収集と迅速な修正プログラム適用プロセスが不可欠である。

ゼロデイ攻撃は、組織のセキュリティ対策が最も試される脅威である。2025年の事例が示すように、攻撃者は高度な検知回避技術を駆使し、国家支援型グループとランサムウェアグループが戦略的にゼロデイ脆弱性を悪用している。

組織は、ゼロデイ攻撃を完全に防ぐことはできないという前提に立ち、侵入を許した場合でも被害を最小化し、迅速に対応できる体制を構築する必要がある。振る舞い検知、回避策の即時適用、脅威インテリジェンスの活用、攻撃対象領域の最小化、複数の検知手段の併用等、多層的な防御策を実装することが求められる。

(2) Nデイ攻撃

Nデイ攻撃とは、ソフトウェアやハードウェアの脆弱性情報及び修正プログラムが公開された後、組織が修正プログラムを適用するまでの期間に、その脆弱性を悪用して行われる攻撃の総称である。「N」は修正プログラム未適用のまま経過した日数を指す。

修正プログラムが提供される前の未知の脆弱性を狙うゼロデイ攻撃とは対照的に、Nデイ攻撃では既知の脆弱性の詳細情報や実証コード（PoC：Proof of Concept）[※154]が既に公開されていることが多い。そのため攻撃実行の技術的な障壁が低く、ランサム攻撃グループを含む幅広い脅威アクターがそれらを利用することで、深刻な被害につながる可能性がある。

脆弱性が公開された後のNデイ攻撃においては、修正プログラム適用の遅延が最大のリスクとなる。

本項では、「既知の脆弱性（Nデイ脆弱性）」が引き起こす被害、攻撃と防御の非対称性による課題、及び組織が実施すべき対策について述べる。

(a)「既知の脆弱性（Nデイ脆弱性）」が引き起こす被害

Nデイ攻撃では、脆弱性が公開され、既知の脆弱性となった後も、修正プログラム適用の遅延や運用上の制約により、多くの組織が攻撃対象となり続ける。本項では、2025年に公開された国内事例と、国家支援型グループによる悪用事例を紹介する。

(ア) 2025年に公表された国内事例

2025年以降、Nデイ脆弱性を悪用された可能性のある攻撃により、日本国内の大企業で深刻な被害が相次いでいる。

2025年1月、国内のテーマパークを運営する株式会社サンリオエンターテイメントがランサム攻撃を受け、チケット購入・来場予約等の主要サービスを停止し、復旧完了まで利用者・事業者の双方に広範な影響が及んだ。その後の調査・解析により、リモートアクセス機器の脆弱性を狙った不正アクセスに対処できなかったことが原因で社内ネットワークへ侵入されたことが明らかとなった[※155]。

同年9月には、大手総合飲料メーカーであるアサヒグループホールディングス株式会社がランサム攻撃を受け、受注・出荷システムが停止した。攻撃者はグループ内拠点のネットワーク機器を経由してデータセンターに侵入し、191.4万件の個人情報流出の可能性が明らかとなった[※50]「1.2.1 (2) (a) 大手総合飲料メーカーにおける被害事例」参照）。

これらの事例に共通する点として、攻撃者が「インターネットに公開されたネットワーク機器」を足掛かりにしてい

ることが挙げられる。

攻撃者は既知の脆弱性を持つ機器を自動スキャンにより探索し、脆弱な機器を見つけ次第、侵入を試みていると見られる。組織の規模や知名度にかかわらず、インターネットに接続された機器のセキュリティ対策が不十分であれば、標的となる可能性がある。

(イ) 国家支援型グループによる悪用

N デイ脆弱性を悪用するのは、前述のランサム攻撃だけではない。

2025 年 8 月 27 日、日本を含む 13 ヵ国の政府機関が共同で公表した国際アドバイザリーでは、中国政府を背景とする攻撃グループ「Salt Typhoon」が長期にわたる諜報活動を展開していたことが明らかにされた(「1.2.2(2)(b)Salt Typhoon 等に関する国際注意喚起」参照)。

攻撃対象は電気通信・政府機関・交通・軍事インフラ等多岐にわたり、同アドバイザリーは悪用された CVE への対策として「パッチの迅速な適用」を挙げている。高度な国家支援型の脅威グループでさえ、公開済みの脆弱性を悪用し、足掛かりとする手法を常用していることを示す事例である※ 83。

(b) 攻撃と防御の非対称性による課題

N デイ脆弱性に対して、なぜ十分な対策が講じられないまま組織は攻撃に晒され続けるのか。攻撃者による攻撃と組織側の防御の間には、攻撃側の速度、防御側の運用管理サイクル、CVSS スコアの限界等、構造的な問題があり、これらが重なることで、N デイ攻撃が繰り返される土壌が形成されている。

(ア) 脆弱性公開とともに始まる悪用

セキュリティベンダーの Rapid7, Inc. が 2025 年第 3 四半期のレポートにおいて「脆弱性が公開された瞬間、攻撃者の武器に弾丸が込められることになる」と表現しており、「組織は、公開された瞬間から悪用が始まると想定し、それに応じた行動を取る必要がある」と指摘している※ 156。

またこれを裏付けるように、セキュリティベンダーの VulnCheck, Inc. は 2026 年 1 月に公表した年次報告書において、2025 年に初めて悪用が確認された KEV カタログに登録された脆弱性 884 件のうち約 3 割が CVE 公開日当日またはそれ以前に悪用されていると述べている※ 157。

脆弱性情報が公開された時点で、既に攻撃が始まっているケースが少なくないことが確認されている。このことは、「情報を把握してから対応方針を検討する」という従来の手順が機能しにくい状況を示している。

(イ) 短期間での対応の難しさ

日本を含む多くの組織では、修正プログラムの適用を月次の定期メンテナンス時にまとめて実施する運用が一般的である。システム安定性の検証やステージング環境(本番環境に類似させたテスト環境)での事前テストを経ることで意図せぬ障害を防ぐ合理的な手順として普及してきたものであり、その有効性が否定されるものではない。しかし重大な脆弱性が公表された場合、月次サイクルでは最大 30 日の修正プログラム未適用期間が生じ得る。

攻撃者が公開当日に動き出す一方で、防御側は月次の運用により最大 30 日程度の修正プログラム未適用期間が生じ得るという非対称な状況が、対応遅延や侵害リスクを高める構造を招いている。

修正プログラムや対応策の適用を短期間に実現することが難しい背景には、システム運用への影響懸念、業務停止リスク、変更管理プロセスの負荷がある。加えて、サポート終了(EoL:End-of-Life)製品を継続運用している場合は、修正プログラムが提供されない、または限定的となるため、短期適用の問題にとどまらず、更新・移行計画そのものが課題となる。EoL 製品ではベンダーによる修正プログラム提供が行われないため、脆弱性が判明しても技術的な対応手段がないまま運用が続くケースがある。特に VPN 機器等、境界防御機器で EoL 製品を運用し続けることは、N デイ攻撃の有力な侵入経路となり得る。

(ウ) CVSS スコアの限界

多くの組織が脆弱性の優先順位付けに CVSS(Common Vulnerability Scoring System:共通脆弱性評価システム)※ 158 スコアを用いることが多いが、実際に攻撃で悪用されている脆弱性の中には、CVSS v3 スコアでは Medium (4.0 ～ 6.9) や High (7.0 ～ 8.9) の評価にとどまるものが相当数含まれている。

その典型例として、Ivanti Connect Secure の脆弱性(CVE-2025-22457)※ 91 がある。2025 年 2 月の修正プログラム提供時点では低リスクの DoS 脆弱性と評価されていたが、Mandiant, Inc. の分析によれば、攻撃者が修正プログラムを研究することで複雑なプロセスを経てリモートコード実行への悪用が可能であることを発見したと推測された。同年 3 月中旬には実攻撃が観測され※ 159、

CVSS v3 スコアも現状は 9.8 となっている※160。

CVSS スコアは評価時点における静的な指標に過ぎず、その後の悪用状況の変化を反映しない。実際の悪用事実（KEV カタログへの登録）を優先基準とした脆弱性管理への移行が、実態に即した対応として有効と考えられる。

(c) 組織が実施すべき対策

N デイ攻撃への対策では、脆弱性情報の迅速な把握と優先度判断、組織的な対応体制、重大脆弱性への迅速な対応フローの整備、及び継続的な資産管理を組み合わせた多層的な対応が重要となる。

- 脆弱性情報の迅速な把握と優先度判断

  N デイ攻撃への対応では、固定的な月次運用を前提とするのではなく、攻撃側の速度に対応可能な情報収集、優先度判断、意思決定、運用管理の仕組みを整えることが重要である。

  CISA の KEV カタログは CSV、JSON 形式等で無償公開されている※161。KEV カタログへの登録を契機として、影響が想定される資産を特定し、関係者へ迅速に通知する仕組みが、実効性ある対応の起点となる。

  また、SIEM での活用やファイアウォールのブロックリストとの連携も技術的に実現可能である。NVD※162、JVN iPedia※163、JPCERT/CC※164、ベンダー公式情報等複数の情報源と組み合わせて活用することが望ましい。

- 組織的な体制整備と情報共有

  N デイ攻撃への実効性のある対応には、技術的対策に加えて、組織的な体制整備が不可欠である。特に、脆弱性情報の収集から対応までのプロセスを円滑に進めるためには、製品の利用者側と開発者側がそれぞれの立場で適切な体制を整備し、相互に連携することが重要となる。

  利用者側においては、CSIRT（Computer Security Incident Response Team）による脆弱性情報の一元管理と、影響を受ける資産の迅速な特定、修正プログラム適用の優先順位付けが、N デイ攻撃対応の基盤となる。開発者側においては、PSIRT（Product Security Incident Response Team）として、設計・開発段階からのセキュリティ対策の実装と、脆弱性に対する迅速な開示や修正プログラムの提供を通じて、製品利用者全体のリスク低減を図ることが重要である。

  国内においては経済産業省告示に基づく「情報セキュリティ早期警戒パートナーシップ」（IPA、JPCERT/CC が運営）が、脆弱性情報の届出、調整、公表を支援する枠組みとして整備されている※165（「3.1.2 (3) (c) 情報セキュリティ早期警戒パートナーシップ」参照）。また、「協調された脆弱性の開示（CVD：Coordinated Vulnerability Disclosure）」プロセスを活用することにより、脆弱性情報が適切に共有されないまま悪用されるリスクを低減することが可能と考えられる。

  更に、2025 年 8 月の国際アドバイザリー※83 に見られるように、国家支援型の攻撃グループに対しては複数国による脅威情報の共有と共同対処が有効であり、国内においても JPCERT/CC、警察庁、IPA 等の関係機関の連携による脅威情報の共有・技術支援体制を活用することが、組織の対応力強化に資すると考えられる。

- 重大脆弱性への迅速な対応フローの整備

  通常の変更管理プロセスは維持しつつ「KEV カタログに登録され、かつインターネット公開機器に影響する脆弱性」における迅速な対応フローを事前に整備することが、リスク管理上有効と考えられる。

  対応としては、修正プログラムの迅速な適用が基本となるが、適用が困難な場合や遅延する場合は、当該システムのインターネットからの一時的な隔離、WAF（Web Application Firewall）による防御、VPN／ZTNA（Zero Trust Network Access）による厳格なアクセス制御等、代替的なリスク低減策を実施することが望ましい。

  また、対応が遅れた期間中に侵害が発生している可能性を念頭に置き、WebShell※166 等不審ファイルの痕跡確認、異常な DNS 通信の調査、認証情報のローテーション（更新または再発行）、各種ログの確認等を実施することも、事後対応として推奨される。

- 継続的な資産管理（外部公開機器等の継続的な可視化）

  攻撃者は、インターネットから攻撃対象領域を探索し、攻撃を開始する。そのため、EASM（External Attack Surface Management）ツールや資産管理ツールにより、把握されていないシャドー IT、テストサーバー、管理外の VPN 機器等を継続的に確認することが、N デイ攻撃リスクの低減に有効と考えられる。

  VPN 機器、ファイアウォール等の境界防御機器については、EoL 状況の棚卸しと後継製品への移行計画を高い優先度で整備することが望ましい。

N デイ攻撃の多くは「防げた可能性のある攻撃」である。既知の脆弱性に対する修正手段が提供されている場合でも、対応が間に合わず被害を受ける組織が後を絶たない。

問題の本質は、攻撃速度と防御速度の差によって生じる構造的な時間差にある。攻撃者は脆弱性の公開と同時に悪用を開始する一方で、防御側は月次の定期メンテナンスサイクル、システム検証の必要性、EoL 製品への対応の困難さ等、複数の制約により対応に時間を要する。この非対称な構造こそが、N デイ攻撃による被害が多発する根本的な要因である。

脅威情報の迅速な収集と連携、重大脆弱性への優先対応フロー、外部公開資産の継続的な可視化、そして利用者側と開発者側の組織間連携、これらを組み合わせた継続的なリスク管理への転換が必要とされる。脆弱性管理は IT 部門の運用課題ではなく、事業継続に直結する経営課題として位置付けることが重要である。

1.2.5 不正アクセスや内部不正による情報漏えい

本項では、組織から情報が漏えいするきっかけとなる不正アクセス、及び内部不正に着目し、最新動向を整理するとともに、対策について解説する。

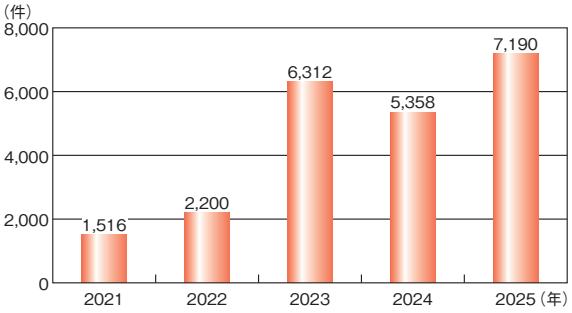
「情報セキュリティ 10 大脅威 2026」の「『組織』向け脅威」では、「ランサム攻撃による被害」が 11 年連続で選出され、攻撃の手口の一つに不正アクセスが挙げられている。トレンドマイクロ社によると 2025 年 1 ～ 12 月に公表された 559 件のインシデントのうち、327 件は不正アクセスによるものであり、最も多かった※167。また、「『組織』向け脅威」では「内部不正による情報漏えい等」も 11 年連続で選出されている。これらの脅威により組織から漏えいする情報は、顧客の個人情報から、研究データや製造ノウハウ、設計図面といった技術情報等まで多岐にわたる。

個人情報の漏えいにより社会的信用が失墜することや技術情報等の漏えいにより市場における競争力が低下すること等のリスクをよく認識し、不正アクセスや内部不正による情報漏えいを防止するための対策を実施することは組織の事業継続の観点からも重要である。

(1) 不正アクセスによる情報漏えい

本項では、「不正アクセス行為の禁止等に関する法律※168」(不正アクセス禁止法)に基づき、ID やパスワード等の認証情報を窃用することによるなりすまし、システムの脆弱性を悪用した侵入、インターネット等に接続されたコンピューターやネットワーク機器等を攻撃の踏み台として悪用する行為を不正アクセスとして扱う。

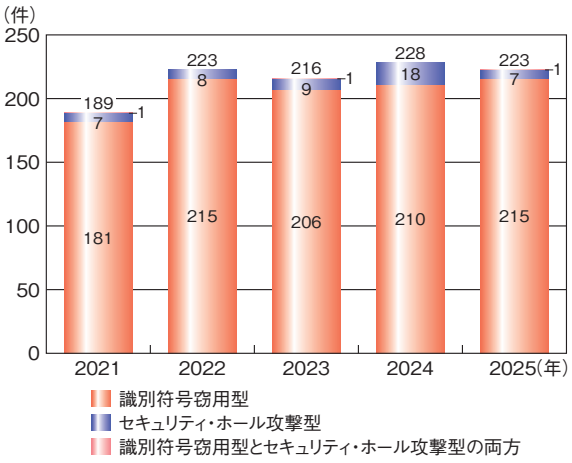
国家公安委員会、総務大臣及び経済産業大臣から公開されている「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況※169」によれば、2025 年の不正アクセス行為の認知件数としては 7,190 件となっており、2023 年から 5,000 件を超える水準で推移している(図 1-2-8)。



■図 1-2-8　不正アクセス行為の認知件数の推移(過去 5 年)
(出典) 国家公安委員会、総務大臣、経済産業大臣「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」を基に IPA が作成

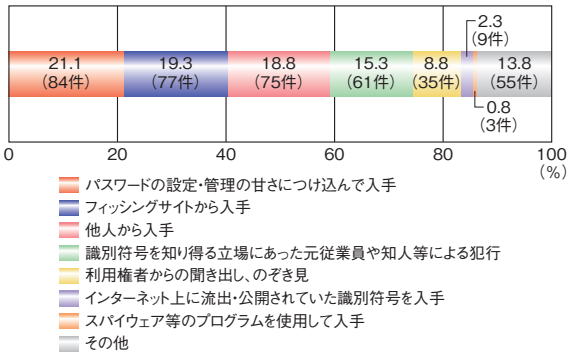
また、2025 年の不正アクセス行為の検挙事件数※170 については、2024 年からわずかに減少し合計 223 件となっており、検挙件数※171 も 407 件となっている。

検挙事件数を手口別に見ると、ID やパスワード等を窃用する「識別符号窃用型」が 215 件、脆弱性を悪用する「セキュリティ・ホール攻撃型」は 7 件、「識別符号窃用型とセキュリティ・ホール攻撃型の両方」に該当するのは 1 件であった(図 1-2-9)。



■図 1-2-9　不正アクセス行為の検挙事件数の推移(過去 5 年)
(出典) 国家公安委員会、総務大臣、経済産業大臣「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」を基に IPA が作成

2025年の不正アクセス行為の検挙件数407件のうち、識別符号窃用型の不正アクセス行為399件の手口別の内訳では、「パスワードの設定・管理の甘さにつけ込んで入手」が最も多く84件(21.1%)となっていた(図1-2-10)。



■図1-2-10　不正アクセス行為の手口別検挙件数(2025年、n=399)
(出典)国家公安委員会、総務大臣、経済産業大臣「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」を基にIPAが作成

不正アクセスの被害に遭った企業・組織の業種も多岐にわたっていた。2025年以降に発生した不正アクセスによる主な情報漏えい事例を表1-2-3に示す。

報道時期	概要
2025年3月	NTTコミュニケーションズ株式会社(現、NTTドコモビジネス株式会社)では、同社のオーダ情報流通システムに格納されていた法人顧客向けサービスの一部の情報が外部に流出した可能性がある※172。
2025年3月	株式会社ファーストリテイリングでは、情報システムが、第三者による不正アクセスを受け、取引先従業員及び自社従業員の個人情報の一部が漏えいしたおそれがある※173。
2025年5月	株式会社すかいらーくホールディングスでは、テイクアウトサイトにおいて第三者による不正アクセスを受けた。最終的に顧客のクレジットカード情報2,270件が漏えいした可能性がある※174。
2025年10月	アスクル株式会社では、多要素認証を適用していなかった認証情報が窃取され、不正に社内ネットワークに侵入され、顧客情報を含む約74万件の情報が流出した※53「1.2.1 (2) (b) 大手eコマース企業における被害事例」参照)。
2025年11月	国立国会図書館の館内サービスシステムのリプレース開発において、委託先の再委託先事業者である株式会社ソリューション・ワンのネットワークが何者かの侵入を受けたことに起因し、委託先が管理する当該開発環境に対し不正アクセスが行われた※175。
2026年3月	東京大学では、共同研究者が利用している学外のサーバーが不正アクセスを受け、その共同研究者のアカウントを使って当該研究室のサーバーに不正アクセスが行われ、当該サーバーを起点として学内外のサーバーに対しても不正アクセスが行われた※176。

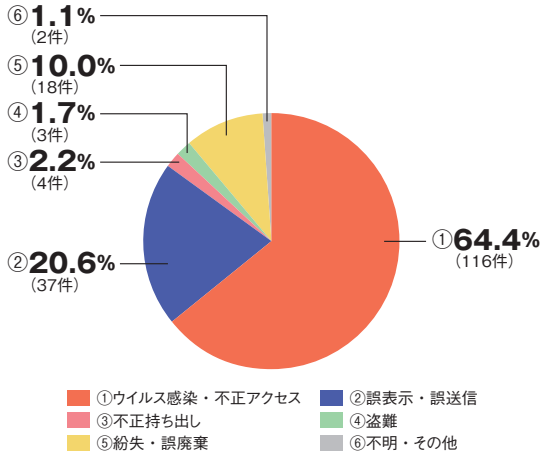
■表1-2-3　不正アクセスによる主な情報漏えい事例
(出典)公表情報を基にIPAが作成

(2) 内部不正による情報漏えい

本項では、役職員等の内部者による重要情報や情報システム等の情報資産の窃取、持ち出し、漏えい(内部者が退職後に在職中に得ていた情報を漏えいする行為等を含む)、及び消去・破壊等の違法行為と、情報セキュリティに関する内部規程やルールへの違反、ミス等の違法とはいえない行為の両方を内部不正として扱う※177-1。

近年、情報漏えいを伴うセキュリティインシデントとして、ランサム攻撃が報道等で注目されるが、内部不正を要因とする情報漏えいも実態として決して少なくない。背景としては、雇用や人材の流動化、AI等の新興技術の進展等に伴う、国家間、企業間の技術競争の激化がある。

企業が保有する個人情報の漏えいに着目すると、株式会社東京商工リサーチが2026年1月に公開した「2025年『上場企業の個人情報漏えい・紛失事故』調査」によれば、2025年に上場企業とその子会社が公表した個人情報の漏えい・紛失事故は180件で、そのうち内部不正に相当する「誤表示・誤送信」(37件)、「不正持ち出し」(4件)を合計すると41件となり、22.8%を占めていた(図1-2-11)。



■図1-2-11　上場企業における個人情報漏えい・紛失の原因
(2025年、n=180)
(出典)株式会社東京商工リサーチ「2025年『上場企業の個人情報漏えい・紛失事故』調査」を基にIPAが編集※177-2

内部不正による2025年度の主な情報漏えい事例を表1-2-4(次ページ)に示す。内部不正の手口としては、メールでの誤送信やシステムの設定ミスによる誤表示、社内システムからの不正取得が複数の事例で明らかになっている。動機に着目すると、転職先での利用のほか、組織への恨みである事例もあった。更に漏えいをきっかけに得意先からの取引解消が進み、事業継続の見通しが立たなくなる事例も見られた※178。

報道時期	概要
2025 年 4 月	みずほ信託銀行株式会社では、社員が誤って外部委託先社員 2 名を宛先に含めたまま、自社の別の社員に顧客情報を電子メールで送信し、2,472 人分の個人情報及び 246 社分の法人の情報が漏えいした※179。
2025 年 6 月	ソフトバンク株式会社の業務委託先である株式会社 UF ジャパンの協力会社の元従業員が、株式会社 UF ジャパンの事業所に不正に立ち入り、顧客情報を持ち出した可能性がある。監視カメラの映像には、USB メモリーを情報管理端末に接続している様子が確認されている※180。
2025 年 8 月	台湾積体電路製造（TSMC：Taiwan Semiconductor Manufacturing Company Limited）では、システムの定期的なモニタリングの過程で不正な活動を検知し、内部調査で企業秘密漏えいの可能性が判明した。先端半導体技術に関連する機密情報を不正に取得した疑いで複数の従業員を処分した※181。
2025 年 8 月	株式会社 TBM では、従業員 2 名が、退職後に起業した競合会社での業務に利用する目的で、営業秘密となる約 80 ファイル分のデータを同社のパソコンから外部のサーバーに移して持ち出す等の案件（2023 年 6 月に発生）で、書類送検された※182。
2025 年 9 月	公益財団法人堺市文化振興財団では、財団への不平不満から、職員が退職前後に情報システムから、チケット販売システムの会員情報や、財団職員、市職員らの情報を約 3 万 7,000 件窃取し、一部を SNS に流出させた※183。
2026 年 1 月	農林水産省では、2025 年分の給与支払い事務に関し、提出先として誤ったメールアドレスを提示したことにより、一部職員及びその家族 4,571 人分の源泉徴収票等に関するマイナンバー等の個人情報が外部のメールサーバーに誤送信され、漏えいした※184。
2026 年 2 月	総務省が実施した「令和 7 年度放送コンテンツ製作取引実態調査」のアンケート調査において、委託先が回答用 Web サイトのログイン管理の設定を誤った結果、他の回答者が一時保存した回答ページに含まれる個人情報及び企業情報が別の回答者に誤表示され、漏えいした※185。
2026 年 3 月	株式会社ユナイテッドアローズでは、従業員が退職前に取引先の個人情報を含む電子データを同社のクラウドサーバーシステム上の外部連携機能を利用してアップロードし、退職後に外部パソコンに不正にダウンロードした※186。

■表 1-2-4　内部不正による主な情報漏えい事例
（出典）公表情報を基に IPA が作成

(3) 不正アクセスや内部不正による情報漏えいを防ぐための対策例

これまで見てきたように、不正アクセスや内部不正による情報漏えいが継続的に発生していることから、企業・組織は不正アクセスと内部不正の両面から対策を行うことが肝要である。

不正アクセスによる情報漏えいを防ぐための対策については経済産業省が「コンピュータ不正アクセス対策基準※187」を定めている。それらの対策のうち情報システム利用者及び情報システム・管理部門が実施すべき対策を表 1-2-5 に例示する。

また、内部不正による情報漏えいを防ぐための対策には、組織体制・教育面の対策、環境面の対策、技術面の対策がある。IPA による「組織における内部不正防止ガイドライン※188」を基に整理した対策を表 1-2-6（次

実施者	種類	概要
情報システム利用者	パスワード及びユーザー ID 管理	・ユーザー ID の複数のシステムユーザーでの利用禁止　等
	情報管理	・重要な情報の暗号化 ・重要な情報の送信時の宛先の限定と確認 ・情報の重要度に応じたアクセス権限の設定　等
	コンピュータ管理	・特権 ID での操作は操作の範囲、場所、期間等を必要最低限に限定　等
	事後対応	・不正アクセスの発見時及びシステムの異常発見時のシステム管理者への迅速な報告　等
	教育及び情報収集	・セキュリティ対策に関する教育の受講 ・セキュリティ対策に関する情報収集とシステム管理者への提供　等
	監査	・システム監査の報告を踏まえた必要な措置の実施
情報システム・管理部門	管理体制の整備	・セキュリティ方針、システムの管理体制、管理手順等の確立、周知・徹底　等
	システムユーザー管理	・システムユーザーの登録の限定と必要最小限の権限の設定　等
	情報管理	・通信経路上の情報の漏えいを防止する仕組みの確立 ・情報の盗聴及び漏えいが行われても、内容を解析できない機密保持機能の利用 ・情報の改ざん検知機能の利用　等
	設備管理	・重要な情報が格納されているかまたは重要な処理を行う機器の管理 ・移動可能な機器の盗難防止対策の実施 ・供給者の連絡先及び更新情報が明確な機器及びソフトウェアの利用　等
	履歴管理	・セキュリティ方針に基づくシステムの動作履歴等の記録及び分析、保管　等
	事後対応	・異常発見時の迅速な原因究明 ・不正アクセスの場合、関係者と協調した被害状況の把握　等
	情報収集及び教育	・セキュリティ対策に関する情報収集と分析 ・システムユーザーへの情報提供と教育の実施　等
	監査	・システム監査の報告を踏まえた必要な措置の実施

■表 1-2-5　不正アクセス対策の例
（出典）経済産業省「コンピュータ不正アクセス対策基準」を基に IPA が作成

実施者	種類		概要
経営者・管理部門	組織体制・教育面	情報取り扱いポリシーの作成	・重要情報の内容、取り扱い範囲を把握するため、情報の格付け等取り扱い方法を規定
		対応体制の整備	・情報の重要度に応じた情報管理者を規定
		就業規則の整備	・守秘義務、競業避止義務※の有無や内容を規定 ・従業員等が社内ルールを遵守することを規定 ※競業避止義務を規定する場合は、職業選択の自由を侵害しないように適切な範囲を設定する
		教育・研修の実施	・情報取り扱いポリシー、就業規則等の社内ルールの周知 ・情報の取り扱いに関する研修の実施
	環境面	職場環境の整備	・公平な人事評価の整備 ・適正な労働環境及びコミュニケーションの推進 ・職場環境におけるマネジメント
情報システム・管理部門	技術面	アクセス権の設定及び管理	・業務や権限に応じて重要情報へのアクセス権を適切に設定
		システム操作履歴の監視	・データ出力等のログの記録
		物理的対策	・入退室管理 ・監視カメラの設置 ・電磁的記録媒体等の利用制限 ・適切なデータ廃棄

■表 1-2-6　内部不正防止対策の例
（出典）IPA「組織における内部不正防止ガイドライン」を基に作成

ページ）に例示する。役職員等にはこれらの対策を周知し遵守させることが重要である。

表 1-2-7 に例示したように、不正アクセスや内部不正を行うと、日本の法規制による罰則を科されるおそれがあるほか、日本国外の法規制による罰則が日本企業にも適用されるおそれもある。情報漏えいにより、社会的信用の失墜や競争優位性の喪失のおそれがあること等と併せて、このような法的な罰則についても、教育を通じて役職員等に理解させ、コンプライアンス意識を向上させることも重要である。

これらの不正アクセスや内部不正に対する対策が、経営課題として経営者・経営陣に真摯に取り組まれることが望まれる。もちろん、社内の情報システム部門や、各管理者がその対応を着実に実行することも重要である。なお、IPA では「中小企業の情報セキュリティ対策ガイドライン※194」も公開しているので、活用いただきたい

国	情報の種類	関連する法規制	罰則
日本	営業秘密	不正競争防止法※189	個人：10 年以下の拘禁刑もしくは 2,000 万円以下の罰金 法人：5 億円以下の罰金
日本	個人情報	個人情報保護法※190	個人：1 年以下の拘禁刑または 100 万円以下の罰金 法人：1 億円以下の罰金
日本	―	不正アクセス禁止法	・なりすまし、脆弱性攻撃、踏み台行為等の場合、3 年以下の拘禁刑または 100 万円以下の罰金 ・パスワード等の不正取得・保管・フィッシング等の場合、1 年以下の拘禁刑または 50 万円以下の罰金
日本	―	刑法第 246 条の 2（電子計算機使用詐欺罪）※191	不正な指令を与えて、財産を移転させた場合 罰則：10 年以下の拘禁刑
日本	―	刑法第 234 条の 2（電子計算機損壊等業務妨害罪）※191	データの消去・改ざんのほか、大量のアクセスでサーバーを機能停止させ、業務停止させる等行った場合 罰則：5 年以下の拘禁刑または 100 万円以下の罰金
日本	―	刑法第 168 条の 2（不正指令電磁的記録作成等罪）※191	ウイルスを送り込むまたは作成等した場合 罰則：3 年以下の拘禁刑または 50 万円以下の罰金
日本	政府が保有する安全保障上重要な情報	重要経済安保情報保護活用法※192	主な罰則：重要経済安保情報の取扱いの業務に従事する者：5 年以下の拘禁刑もしくは 500 万円以下の罰金、またはその両方 ※重要経済安保情報の取扱いの業務に従事しなくなった後においても同様であり、未遂や過失も罰せられる。また、事業者・従業者個人の双方に罰則が適用される。
欧州	個人情報	欧州一般データ保護規則（GDPR）※193	軽微な違反：最大 1,000 万ユーロ、または前会計年度の全世界年間売上高の 2%、もしくは、いずれか高額の方 重大な違反：最大 2,000 万ユーロ、または前会計年度の全世界年間売上高の 4%、もしくは、いずれか高額の方

■表 1-2-7　不正アクセスや内部不正による情報漏えいと関連する法規制

（同ガイドラインについては「3.4.2 (2)『中小企業の情報セキュリティ対策ガイドライン』の改訂」参照）。

1.2.6 個人を狙う騙しの手口

2025 年度初頭には、証券会社をかたるフィッシングで証券口座のアカウントが乗っ取られる被害が大きな話題となった（「1.1.2(1)フィッシングによる被害」参照）[※195]。

IPA の「情報セキュリティ安心相談窓口[※196]」（以下、安心相談窓口）に寄せられた相談の傾向を見ると、SNS アカウントへの不正ログイン（アカウントの乗っ取り）に関する相談が 2025 年度に増加した[※197]。その中で、SNS の DM（ダイレクトメッセージ）で被害者を騙す乗っ取りの手口が現れた。

偽のセキュリティ警告で被害者を騙すサポート詐欺については、2025 年 5 月、国際共同捜査によって、日本人を標的に攻撃を行っていた、インドを拠点とした攻撃グループが逮捕された[※198]。

2025 年上半期には、パソコンを「インフォスティーラー（Infostealer）」と呼ばれる情報窃取型マルウェアに感染させるために、偽の CAPTCHA 認証画面等を表示する「ClickFix」と呼ばれる手口の攻撃が急増したという[※199]。こうした新たな騙しの手口についても注意する必要がある。

以下の各項に、それぞれの「手口」の解説、手口に対する「対処」と「対策」を示す。ここでの「対処」は、被害に遭った場合の被害軽減や回復処置について記載している。「対策」は、当該手口の被害に遭わないために、日頃から注意すべきことを記載している。

(1) フィッシング

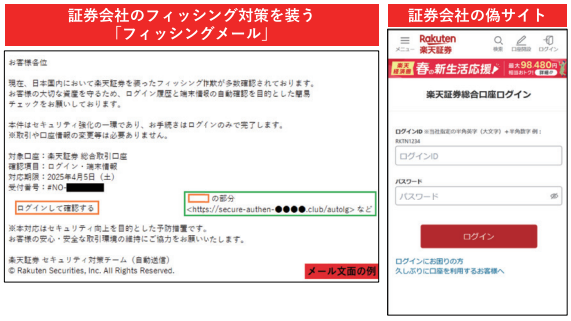
フィッシングとは、実在する企業・組織をかたるメールや SMS を送り付け、偽サイト（フィッシングサイト）に誘導し、情報を詐取する手口である。メールの受信者を「緊急性を煽る文面」等で焦らせて、メール文中の偽サイトへのリンクをクリックさせることで、偽サイトに入力した情報を詐取する。

(a) 手口

証券口座のアカウントへの不正ログインでも、フィッシングの手口が使われた。

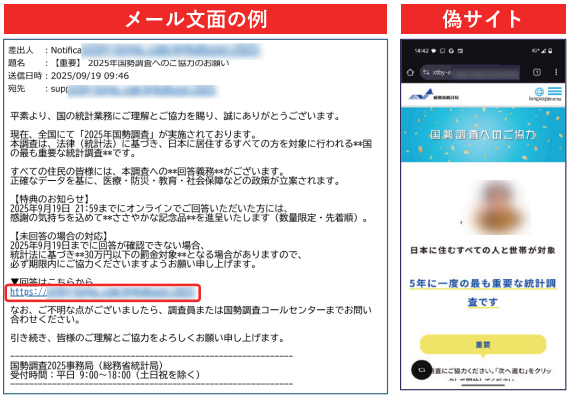
フィッシングメールの中には、「セキュリティ強化のご案内」「フィッシング詐欺にご注意ください!」等の、証券会社のセキュリティ対策強化や注意喚起を装うものもあった[※200]。フィッシング詐欺の攻撃グループが、事業者のフィッシング対策の呼びかけを逆手に取って、こうしたメールを送っていた（図 1-2-12）。

フィッシングには、その時々の行事やイベントにあわせて、行事の実行者等をかたる手口がある。この手口によって、偽メールの内容が本物らしく見える場合がある。



■図 1-2-12　証券会社の注意喚起を装うフィッシング
（出典）フィッシング対策協議会「楽天証券をかたるフィッシング（2025/04/01）[※200]」を基に IPA が編集

2025 年は、5 年ごとに行われる国勢調査の年であった。そこで、国勢調査への回答を求め、「回答提出リンク（ボタン）」をクリックさせるフィッシングが行われた（図 1-2-13）。この手口では、リンクをクリックすると偽サイトのログイン画面が表示され、電話番号を入力させる。ここで攻撃者は偽サイトに入力させた被害者の電話番号を使って「オンラインショップ」の会員登録を行う。すると被害者には、オンラインショップから本人確認のための認証コードが SMS で届く。偽サイトには、届いた認証コードを入力する画面が表示される。偽サイトに認証コードを入力すると、被害者の電話番号を使ってオンラインショップの会員登録が成立してしまう[※201]。



■図 1-2-13　国勢調査への回答を求めるフィッシング

(b) 対処

フィッシングサイトにパスワードを入力してしまった場合、至急パスワードを変更する。加えて、ログイン履歴・購入履歴等で、不正ログインや不正使用をされていないかを確認する。同じパスワードを、他のサービスで使い回していた場合は、他のサービスのパスワードを別のものに変更する。

クレジットカード番号を入力してしまった場合、不正に使用されてしまう可能性があるため、速やかにクレジットカード会社に相談する。また、ネットバンキングのID・パスワードを入力してしまった場合は銀行等、入力した情報に関連したサービスの提供元に相談する。

SMSで届いた認証コードを入力してしまった場合、SMSの発信番号や内容から認証コードを発行したサービスを特定し、サービスの提供元に相談する。

(c) 対策

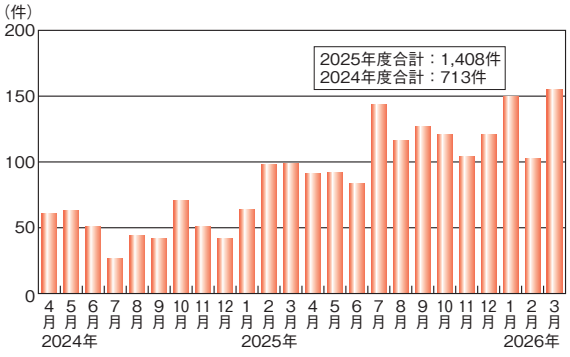
フィッシングに対する基本的な対策は以下のとおりである。

- 不審なメールやSMSのリンクをクリックしない。
- 特に緊急性を強調するものには注意する。「抽選に当選した」等の受信者を喜ばせる内容の偽メールでリンクのクリックに誘導する場合もあるため、同様に注意する。
- 公式サイトから真偽を確認する。

フィッシングメールの文面は自然な日本語で書かれていることが多くなっており、文面の不自然さからでは、もはや真偽を判断できない。本物か偽物かの判断に迷った場合は、公式サイトで真偽を確認する。そのために、よく使うサービスの公式サイトをブックマークに登録しておく。スマートフォン用の公式アプリから確認することも有効である。

(2) 不正ログイン

安心相談窓口への不正ログインの相談は、2025年2月ごろより増加し、2025年度の相談件数は前年度の約2倍の1,408件となった(図1-2-14)。



■図1-2-14　不正ログインの月別相談件数の推移(2024～2025年度)

不正ログインをされた場合に発生する主な被害は以下のとおりである。

- SNSアカウントのパスワード・メールアドレス・電話番号を攻撃者のものに変更されてしまう。本来の所有者は、ログインができなくなることに加えて、パスワードの再設定もできなくなる(パスワード再設定用の通知メールが届かなくなるため)。その上で、アカウントを不審な投稿に悪用される。
- ネットショップで身に覚えがない買い物をされる。その際に送付先を第三者の住所にされる。支払いには、アカウント所有者が登録していたクレジットカードのほかに、フィッシング等で窃取したと思われる第三者のクレジットカードが使われた例も確認している。

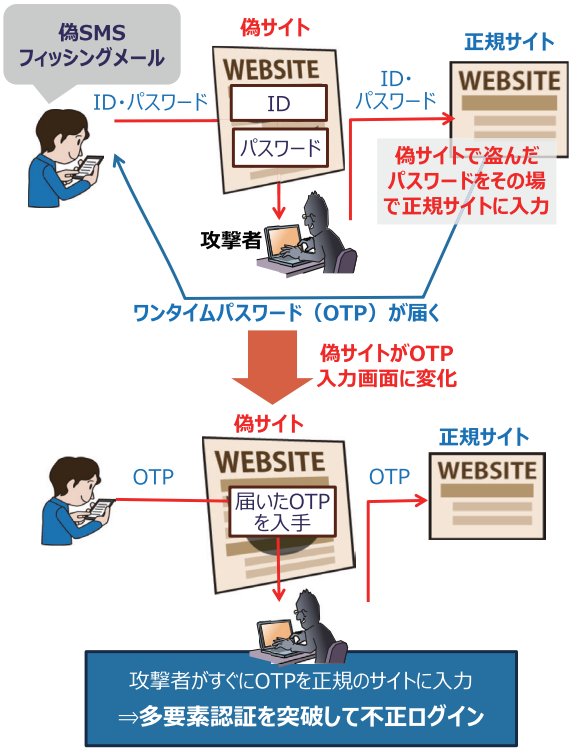
(a) 手口

不正ログインは、多くの場合、不正に割り出した(探り当てた)パスワードや、詐取したパスワードを使用して行われる※202。代表的な手口は以下のとおりである。

- 総当たり攻撃：
  パスワードを構成するすべての文字の組み合わせを試す手口。
- 辞書攻撃：
  パスワードでよく使われる言葉等を集めた専用の辞書を利用する手口。「password123」のような、単純な単語と数字の組み合わせをパスワードに使っていると、この手口の被害に遭う可能性がある。
- リスト型攻撃：
  漏えいしたパスワードのリストを使う手口。同じパスワードを複数のサービスで使い回していると、この手口の被害に遭う可能性がある。
- フィッシング：
  「1.2.6(1)フィッシング」で解説したフィッシングを使ってパスワードを詐取する手口。パスワードそのものを盗むため、上記の攻撃試行が不要である。SMS等を使用した多要素認証を破る「リアルタイムフィッシング」の手口もあるため、従来の多要素認証でも不正ログインを防げない場合がある(次ページ図1-2-15)。そのため、フィッシングは、不正ログインにつながる最大の脅威である。

また、被害者のパスワードを盗まずに、Instagram等のSNSアカウントを乗っ取る手口の相談が増加した。そのため2025年8月、安心相談窓口だより「インターネットサービスへの不正ログインによる被害が増加中※197」で注意喚起を行った。この手口の概要は以下のとおりである(次ページ図1-2-16)。

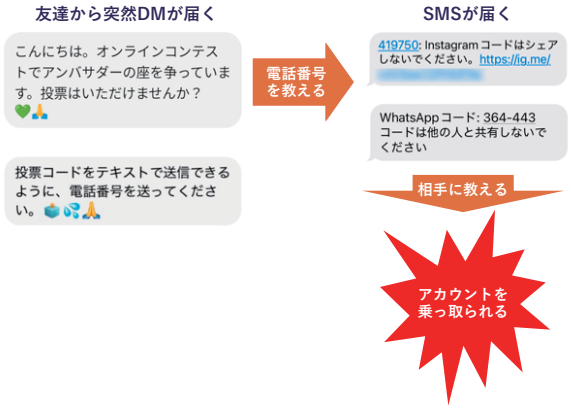
①攻撃者が乗っ取ったSNSアカウントから、電話番号を教えてほしいというDM(ダイレクトメッセージ)が届く。



■図 1-2-15　リアルタイムフィッシングの概要

②それとは知らずに、相手の求めに応じて電話番号を教えると、教えた電話番号の携帯電話宛てにパスワードを再設定するためのリンクが送られてくる。

③この情報を相手に伝えると、攻撃者にパスワードを再設定されてしまい、アカウントが乗っ取られる。



■図 1-2-16　パスワードの再設定手順を悪用した乗っ取りの手口

SNS でつながっている友達からの DM の場合、突然届くフィッシングメールに比べて警戒心が下がる場合があるため注意が必要である。

(b) 対処

利用しているサービスから身に覚えがないログインの通知や、身に覚えがない購入の通知が来た場合、至急パスワードを変更する。

不正購入をされた場合、ネットショップやクレジットカード会社にも連絡する。必要に応じて警察への届出も行う。

SNS アカウントの乗っ取り被害に遭った場合で、SNS のサービス提供事業者がアカウントの回復手順を提供している場合は、その手順に従って申請を行う。

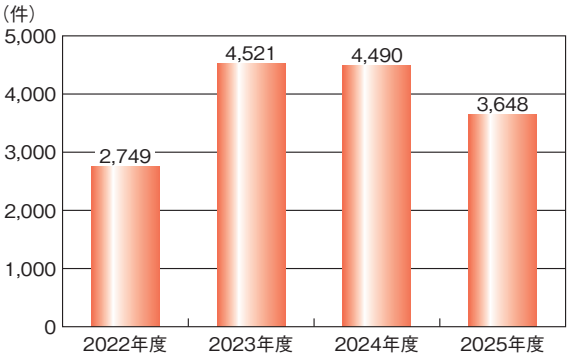
(c) 対策

「1.2.6 (2) (a) 手口」で示した、パスワードを破る手口への対策は以下のとおりである。

- 総当たり攻撃・辞書攻撃への対策：
  パスワードをできるだけ「長く」「複雑」にする。長いパスワードは記憶できないため、パスワードマネージャーを使用する、もしくは IPA が提案している「チョコっとプラスパスワード※203」方式を使うことを検討していただきたい。
- リスト型攻撃への対策：
  アカウントごとに異なるパスワードを設定し、パスワードの使い回しをしない。
- フィッシングへの対策：
  「多要素認証」を設定する。フィッシングによってパスワードを盗まれても、ワンタイムパスワード等の第二の認証要素を突破されない限り不正ログインができなくなる。SMS 等で送信されるワンタイムパスワードをフィッシングサイトに入力させてその場で悪用する「リアルタイムフィッシング」には、「フィッシング耐性がある認証方式※204」が求められる。「パスキー」はフィッシング耐性がある認証方式であるため、対応しているサービスではぜひ設定をしていただきたい。
  パスキーは、現在普及の途上にあるため、パスキー認証と従来のパスワード認証（多要素認証）を併用しているサイトが多い。このようなサイトの場合、フィッシングメールに騙されて、偽サイトにパスワードを入力してしまうと不正ログインをされる可能性がある。しかし、併用しているサイトの場合でも、パスキーが対策となる。パスキーを登録した正規サイトの URL 以外にアクセスした場合、パスキー認証は機能しない。すなわち、パスキー認証が動作しないことによって、偽サイトにつながっていることが識別できる。そのため、メールの URL リンクからアクセスしたサイトで、パスキー認証が働かない場合は、偽サイトの可能性を疑い、パスワードを入力しないようにする。

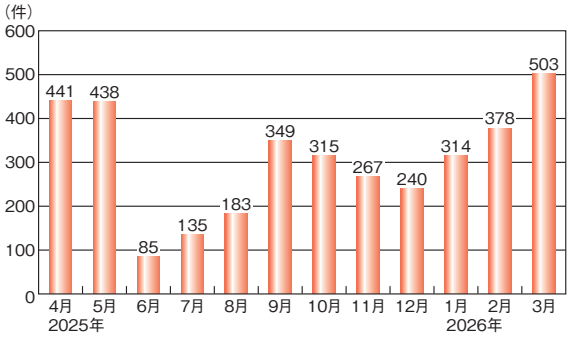
(3) サポート詐欺(偽のウイルス感染警告)

2025 年度に安心相談窓口に寄せられたサポート詐欺の相談件数は 3,648 件となり、2024 年度に比べて減少した(図 1-2-17)。



■図 1-2-17　サポート詐欺の相談件数の推移(2022～2025 年度)

2025 年 5 月には、日本人を標的に攻撃を行っていた、インドを拠点としたサポート詐欺の攻撃グループが逮捕されたとの報告があり※198、一時的に相談件数は減少したが(図 1-2-18)、その後は増加傾向となっており、依然としてこの手口の被害が続いているため注意が必要である。



■図 1-2-18　サポート詐欺の月別相談件数の推移(2025 年度)

(a) 手口

サポート詐欺の手口は以下のとおりである。

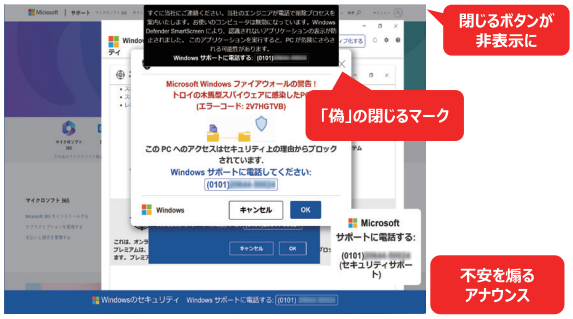
①パソコンに偽のウイルス感染警告(セキュリティ警告)を表示させる(図 1-2-19)。

②偽の警告で被害者の恐怖心を煽り、「偽のサポートセンター」に電話をかけさせる。

③電話をすると、大手 IT メーカーの社員をかたる「偽オペレーター」が応答し、被害者をパソコンの遠隔操作に誘導する。

④ウイルスを除去するためのサポート料金と称して金銭を詐取する(そのため「サポート詐欺」と呼ばれる)。

詳細は、安心相談窓口だより「パソコンに偽のウイルス感染警告を表示させるサポート詐欺に注意※205」を参照いただきたい。



■図 1-2-19　偽警告画面の例

パソコンに偽のウイルス感染警告を表示させる方法は複数あるが、Web サイト上の広告を悪用する手口の相談事例が多くなっている※206。

サポート詐欺の攻撃グループは、大手のネット広告プラットフォームを介して、Web サイトの広告枠に「次のページに進むボタン」に見える広告や、思わずクリックしたくなるような興味を引く広告等を配信する。大手の動画配信サイトを見ていて警告画面が出たとの相談もあり、お勧め動画の一覧の上に配信された広告をクリックすることにより誘導されたと思われる。被害者にこうした「罠の広告」をクリックさせることによって偽の警告を表示する(図 1-2-20)。



■図 1-2-20　Web サイトや動画サイトに表示された罠の広告の例

金銭を詐取する手口では、ネットバンキングを悪用して不正送金を指示する手口が主流となっており、ネットバンキングを利用していないと答えるとプリペイドカードの購入を要求する場合もある。

サポート詐欺グループの「偽オペレーター」は、遠隔操作がつながった状態で、「パソコンがウイルス感染しているため、ネットバンキングの安全性を確認する必要がある」等と言葉巧みに被害者を騙してネットバンキングにログインさせる。その上で、以下のような方法で不正送金を指示する。

- サポート料金の名目で、被害者に少額の送金額を入力させ、遠隔操作で送金額にゼロ(0)を追加する。
- 預貯金を安全な口座に移す必要があると騙して、被害者に多額の送金を行わせる。
- スマートフォンに遠隔操作ソフトをインストールさせ、遠隔操作中にネットバンキングアプリを表示させ不正送金を指示する。

最近では、スマートフォンにも遠隔操作アプリのインストールを誘導され、モバイルバンキングアプリからの不正送金を指示される相談が増えている。

(b)対処

パソコンの画面については、Web ブラウザーを閉じるだけで問題はないが、偽の警告は、Web ブラウザーをフルスクリーン表示にして閉じるボタンを非表示にする等の細工で、画面を容易に閉じられないようにして被害者の恐怖心を煽る。また、警告音が繰り返し流れるので、まずパソコンの音量を下げ、落ち着いて画面を閉じる操作を行う。

安心相談窓口では、パソコンに疑似的な偽の警告を表示して、画面を閉じる操作を体験するための「偽セキュリティ警告画面の閉じ方体験サイト」を公開している※207。

電話をかけてパソコンを遠隔操作されてしまった場合、遠隔操作の及ぼす影響について判断ができないため、安全な対処方法として Windows の「システムの復元」を実施することを推奨する。システムの復元の実施方法については、安心相談窓口の Web サイトに手順書を掲載しているため参照いただきたい※208。「システムの復元」が実行できない場合はパソコンの初期化を推奨する。

ネットバンキングにログインさせられたが、送金には至っていない場合、パスワードの変更と身に覚えのない取り引きの有無を確認し、銀行に相談する。送金をさせられた場合は、至急振込先の銀行に連絡する。振込先の銀行の連絡先は、一般社団法人全国銀行協会の「金融犯罪に遭った場合のご相談・連絡先※209」を参照いただきたい。

(c)対策

サポート詐欺の被害は、偽のサポートセンターに電話をかけることで発生する。正規のセキュリティソフトがウイルスを検知した場合も警告は表示されるが、サポートセンターに電話をかけることが求められることは基本的にはない。このことから、ウイルス感染警告に、大手 IT メーカーのサポートセンターをかたった電話番号が記載されている場合、その警告は偽物の可能性が高い。警告は偽物であることを疑い、電話をかけないことが、この手口に騙されないための対策となる。

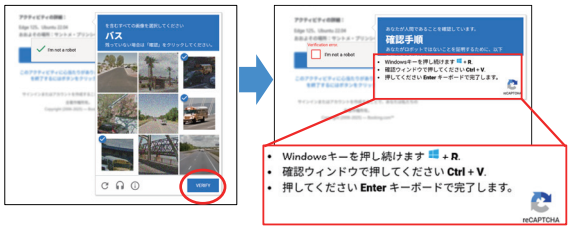
(4) ClickFix 攻撃

2025 年は、Web ブラウザーを操作しているのがボットではないことを証明する CAPTCHA 認証に失敗した場合の対処を装って、マルウェアのインストールに誘導する ClickFix という手口が出現した。安心相談窓口への相談件数は少ないが、マルウェアをパソコンにインストールしてしまうと、パソコンの中に保存している認証情報が窃取される可能性がある。警察庁からも注意喚起が行われている※210。

(a)手口

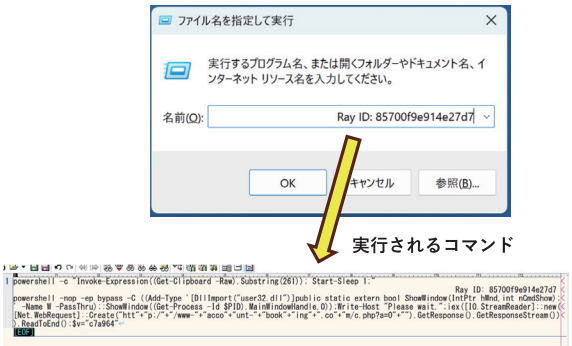
ClickFix の手口は以下のとおりである。

①偽サイトで認証画面が表示され、操作をすると、エラーになり確認手順が表示される(図 1-2-21)。



■図 1-2-21　ClickFix の手口の誘導画面

②表示された確認手順に従い操作すると、ウイルス感染に誘導するコマンドを自ら実行することになる(図 1-2-22)。



■図 1-2-22　ClickFix の手口で悪用されるコマンド入力画面

③コマンドを実行すると、インフォスティーラーと呼ばれる情報窃取型マルウェア等に感染し、パソコンで利用していたサービス等のアカウント情報、クレジットカード情報、個人情報等を窃取される。

(b) 対処

マルウェア感染の可能性がある場合はパソコンのWi-Fiを切断する、LANケーブルを抜く等、インターネットから切断する。パソコンで利用していたサービス等のアカウントのパスワード等を他のパソコンやスマートフォンから変更を行う。マルウェアがパソコンにどのような影響を与えているか不明なため感染の可能性のあるパソコンの初期化を行う。

(c) 対策

突然表示された「エラー」等の対処の指示に対してはすぐに操作をせず、詐欺やマルウェア感染の可能性がないか確認する。

「Windows+Rキーを押し続けます」「確認ウィンドウで押してください Ctrl+V」といった普段自分が行わない、何をしているか理解できないような操作が要求される場合は、特に注意が必要である。

(5) 騙しの手口への対策

情報セキュリティへの意識の高まりを攻撃者に逆手に取られ、「ウイルス感染」や「トロイの木馬」「ハッキングした」「サービス凍結」等という文言を信じて不安になり、被害に遭っていることが多いと考えられる。日頃から正しいセキュリティ対策を行っていれば、不審な通知やメールに遭遇した場合でも焦ってすぐに対応する必要はないことに気付くことができると考える。対策の例としては、以下のものがある。

- 使用している端末やアプリのアップデートを常日頃行う。
- インターネットサービスの利用にあたっては、アカウントのセキュリティ確保のため、可能な場合は多要素認証やパスキーを設定する。
- 不審なメールやSMS、Webサイトでの警告等は基本的には無視をする。真偽を確認する場合は信頼できる人や、確かな情報源で確かめる。

以上に加えて、日頃よりIPAの情報セキュリティ対策のページ※211等から最新情報を入手して手口を知ることが、騙しの手口への重要な対策になると考える。

1.2.7 企業・組織を狙う騙しの手口

本項では、IPAが2025年4月から運営を開始した「企業組織向けサイバーセキュリティ相談窓口※212」（以下、企業相談窓口）に寄せられた相談を中心に、企業・組織を狙う騙しの手口について述べる。2025年は、この手口の代表例として、社長等の企業・組織の代表者をかたるメール（以下、偽社長メール）からLINE等のSNSへと誘導する手口と、「1.2.6(3)サポート詐欺（偽のウイルス感染警告）」で紹介した手口がよく見られた。

メールからLINE等のSNSへと誘導する手口や、偽のウイルス感染警告を表示する騙しの手口は、今後、企業・組織においても被害が広がる可能性があるため注意が必要である。

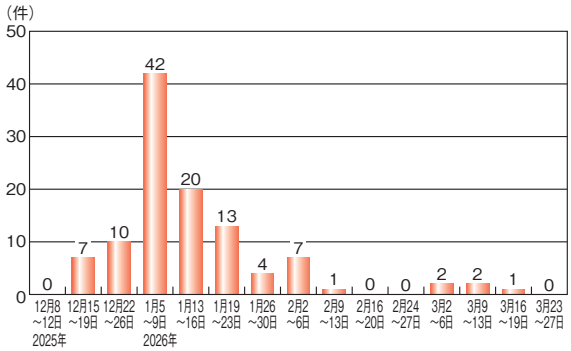
(1) SNSへ誘導する偽社長メール

偽社長メールによってSNSへと誘導する手口は、2025年12月から企業相談窓口に相談が寄せられている（図1-2-23）。企業相談窓口には金銭被害にまで発展した相談は寄せられていないが、報道では騙されて多額の会社の資金を送金してしまったという被害が多数確認できる（次ページ表1-2-8）。

(a) 手口

攻撃者は、差出人の表示名を社長や組織の代表名にしたメールを社員へ送信する（次ページ図1-2-24）。この偽社長メールにはいくつかのパターンがあるが、次のような特徴が確認できる場合が多い。

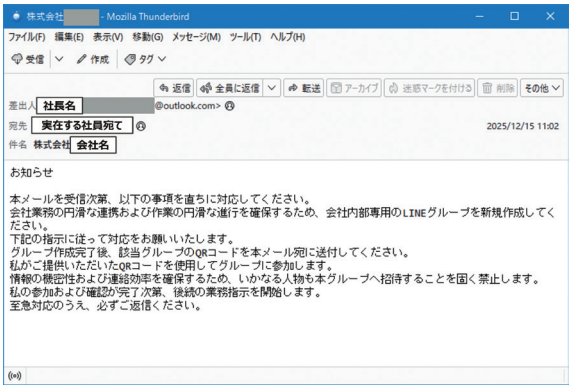
- 差出人の表示名が自社や取引先の代表者名となっている。
- 差出人のメールアドレスには、outlook.com、hotmail.com、gmail.com等のフリーメールが使用されている。
- 件名は自社の会社名になっている場合が多い。
- 本文には、業務指示を装って、「LINEのグループを作成しQRコードを返信するように」「グループには他の者は加えないように」等と書かれている。
- 業務指示に先立って、在席確認を送信してくるケースを確認している。



■図1-2-23 偽社長メールに関する相談件数の週ごとの推移
（2025年12月～2026年3月）

報道日	業種	被害額	概要
2025 年 12 月 27 日 ※213	不明	4,980 万円	「別の会社から入金があるが、先に送金するように」との指示で送金
2026 年 1 月 7 日 ※214	不明	8,000 万円	「業務で大金が必要」との指示で送金
1 月 7 日 ※215	製造業	2,950 万円	会社の口座残高を尋ねた後に送金指示
1 月 7 日 ※216	第三セクター	1,900 万円	同上
1 月 15 日 ※217	不明	約 1,000 万円	「支払いがある。振り込み先情報を送る」との指示で送金
1 月 16 日 ※218	製造業	1 億円	2 回目の送金指示で発覚
1 月 17 日 ※219	観光業	約 2,300 万円	半日で約 60 通の催促等のメッセージの後に送金
1 月 20 日 ※220	不明（都内 14 社）	計 6 億 7,000 万円	被害額 1 億円以上が 2 社
1 月 30 日 ※221	不明	1,130 万円	2 回に分けて送金した後、発覚
2 月 5 日 ※222	不明	5,000 万円	新プロジェクトに対応するための LINE グループ作成を指示

■表 1-2-8　偽社長メールによる被害報道



■図 1-2-24　偽社長メールの一例

- 数は少ないが、マルウェア感染目的の添付ファイルがあるケースも確認している。

LINE のグループの QR コードを送信すると、相手は社長名で LINE グループに参加してくる。この際、社長が SNS で使用しているアイコンが流用されていた事例もあった。LINE グループに参加後は、LINE のメッセージで次のような指示があることを確認している。

- 経理担当者をグループへ参加させるよう指示
- 会社の口座の残高を確認したいという指示
- 新たなプロジェクトと称し、指定口座へ振り込みを行うように指示

(b) 対処

このようなメールが届いてその真偽が判断できない場合は、周囲と相談することが基本である。組織内で不審メール受信時のルールがある場合は、それに従って対処する。送信者に確認する場合は、メールへの返信ではなく電話等の別の方法で確認する。また、不審なメールと判断できる場合においても組織内で情報共有し、組織全体で注意する。

(c) 対策

この偽社長メールの手口では、攻撃者がどのようにメールアドレスを入手しているか明らかになっていないが、ホームページ上で公開している「お問い合わせ先」が宛先に指定されているケースを多く確認している。また、会社名や代表者名等は公開されている情報を悪用していると考えられ、同種の手口は今後も続くことが考えられる。そのため、有効な対策としては次のことが挙げられる。

- 組織内における不審メールに対する対処手順・報告手順を作成し実施する。
- 振り込みによる支払いを実施する際の二重チェック等の承認フローを構築する。
- 組織内において情報セキュリティ教育等を実施する。

(2) 企業・組織で起こるサポート詐欺の被害と対策

サポート詐欺のきっかけとなる偽のウイルス感染警告画面は、Web ブラウザーでサイトを閲覧中に、誰でも遭遇する可能性がある（「1.2.6(3) サポート詐欺（偽のウイルス感染警告）」参照）。会社のパソコンを利用中に突然偽のウイルス警告画面が表示され、詐欺だと気付かずに電話をかけてしまい、騙されて遠隔操作を許可してしまうと、会社のパソコンが遠隔操作されて、情報漏えいや金銭被害が発生するおそれがある。報道されたサポート詐欺による企業・組織の被害を表 1-2-9（次ページ）に示す。

表 1-2-9（次ページ）の 2025 年 12 月の事例では、約 2 億 5,000 万円もの不正送金の被害が発生したことが公表された。オンラインバンキング経由で不正な送金が行われ、後の調査によって、端末内部に保存していたオンラインバンキングの ID とパスワードが記載されたファイルに攻撃者がアクセスした痕跡が確認されたという※227。

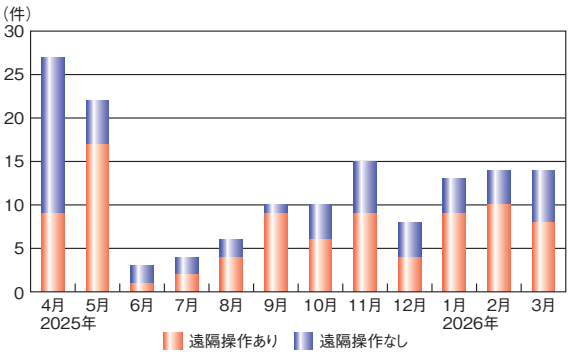
企業・組織の端末には個人情報が保存されている場

報道時期	被害内容
2025年5月※223	公益財団法人やまがた農業支援センターで、遠隔操作により約3万2,000人分の氏名や住所、金融機関の口座情報等がすべて消去され、同情報が流出した可能性
2025年5月※224	山形大学で、遠隔操作により2,306人分の個人情報流出の可能性
2025年8月※225	滋賀県の協同組合で、電話相手の指示に従って認証情報を入力してしまい、同日中に8回にわたり約7,300万円不正送金
2025年9月※226	株式会社パソナで、遠隔操作により800名分の個人情報流出の可能性
2025年12月※227	信和株式会社の子会社で、遠隔操作により約2億5,000万円不正送金

■表 1-2-9　サポート詐欺による被害報道

合が多く、企業相談窓口への相談においても、遠隔操作によって、端末に保存している個人情報やデータにアクセスされ持ち出されていないか心配する相談者が多い。実際にデータへアクセスしたかどうかはデジタル・フォレンジック調査等で明らかにするしかなく、端末の保全状況が悪い場合は調査してもデータへのアクセスや持ち出しが明らかにならないことも考えられる。

企業相談窓口に企業・組織から寄せられたサポート詐欺の相談では、遠隔操作に至ってしまった件数の割合が全体の約6割（図1-2-25）となっており、企業相談窓口では遠隔操作後の対応等をアドバイスしている。



■図 1-2-25　企業・組織からのサポート詐欺に関する相談件数（2025年度）

「人」「技術」「運用管理」それぞれの観点で対策のポイントを示す。

役職員等の「人」が実施すべき対策のポイントは、以下のとおりである。

- 端末に異常が発生したらシステム管理者等への報告や周りに相談する。
- 画面に表示された電話番号に電話しない。
- 指示されてもパスワード等の認証情報を入力しない。
- 会社で許可されていないソフトウェアのインストールを行わない。
- 偽のウイルス感染警告画面を知る。
- 画面の閉じ方等の対処方法を知る※207。

技術的対策のポイントは、以下のとおりである。

- ソフトウェアのインストールは管理者権限を必要とする設定にする。
- 一般社員にローカル管理者権限を与えない。
- 業務で必要なソフトウェアのみ起動できる設定とする。または、被害事例で頻出する遠隔操作ツールの実行制御やブロックを実施する。
- オンラインバンキング等の金融系のサービスを操作する端末は、専用端末を使用する。

運用管理面での対策のポイントは、以下のとおりである。

- インシデント対応手順、報告系統を決め周知する。
- オンラインバンキングの承認フローやルールを定めて周知する。
- パスワード等の認証情報を端末にファイル保存しない。
- 送金限度額を設定する。
- 定期的な情報セキュリティ訓練を実施する。

COLUMN

IoT機器は輸入禁止になるくらい危険なのでしょうか?

「情報セキュリティ白書 2017」から「情報セキュリティ白書 2025」まで、9 年間にわたって IoT 機器（ルーターやネットワーク接続ストレージ、ビデオレコーダー、ネットワークカメラ等）に対する脅威の動向を詳しく解説してきましたが、本白書では独立した項目を設けず、「一休み」をいただいています。しかし、2025 年以降も IoT 機器に対する脅威は続いており、2026 年に入って衝撃的なニュースが飛び込んできました。同年 3 月 23 日、米国連邦通信委員会（FCC：Federal Communications Commission）が「国家安全保障と米国人の安全に容認できない脅威をもたらし得る」として、FCC の承認を受けていない外国製ルーターの輸入・販売を実質禁止したのです[i]。

本コラムではまず、サイバー攻撃者に狙われた IoT 機器がどの様な被害をもたらすか、おさらいしてみましょう。第一は、機器の制御の一部を乗っ取られて第三者への攻撃の踏み台に悪用されることです。このケースでは、機器は目的どおり動作し続けている状態にあり、裏でこっそり犯罪に加担させられるため、機器の所有者が被害に気付かないことが多い、という厄介な問題を抱えています。第二は、機器が正常に動作しなくなり、所有者の期待する成果が得られなくなることです。例えば、地方自治体が河川に設置した監視カメラの映像が見られなくなる、個人が自宅に設置したネットワークカメラが不正にアクセスされて自宅内の映像を第三者にのぞき見されてしまう等、機器の所有者に直接的な被害が生じるケースです。企業が産業用目的で導入する IIoT（Industrial IoT）機器の場合、その脆弱性を悪用されて情報システムや制御システムへの侵入口とされる、といったケースも考えられます。

先程の「第三者への攻撃の踏み台」として悪用される場合、どの様な IoT 機器が狙われるのか考えてみましょう。その目的を考慮すると、狙われやすい IoT 機器の傾向が見えてきます[ii]。

①一定の処理能力を有していること

正常に動作しているふりをしつつ悪意のプログラムを動作させる必要があるので、搭載されているマイクロプロセッサーやメモリー、ネットワーク性能等が高い処理能力を有している機器が狙われます。ルーターはその典型例の一つです。

②同一または同等の機器が多数存在していること

同一の攻撃手段で多数の機器を乗っ取り、悪用時に高い攻撃力が得られる機器、例えば、インターネット接続事業者が顧客に配布しているブロードバンドルーターが狙われます。

③世界中に散在する形で多数利用されていること

乗っ取った機器が特定の国・地域に偏って存在した場合、その領域からの通信遮断という対策を取られるため、世界中の様々な場所で利用されている同一・同等の機器、例えば、世界中に OEM 供給されている製品や、脆弱性を有したまま広範囲で流通しているチップセットや脆弱性を有したソフトウェア開発キットを用いて開発された製品が狙われます。

これらの傾向を考慮すると、ルーターが非常に狙われやすい IoT 機器の一つであることがお分かりいただけると思います。

このようにサイバー攻撃者に狙われやすいルーターですが、毎年「情報セキュリティ白書」で報告してきたとおり、数多くの脆弱性が見つかっています。脆弱性が発見された後の製造業者の対応には温度差があり、積極的に更新ファームウェアを公開・提供する企業とそうでない企業が存在します。更に、ルーターは長期間にわたって使用されるため、サポート期間が終了して更新ファームウェアが提供されない機種に脆弱性が発見されたまま放置されるという、いわゆる「EOL（End-of-Life）機器の脆弱性問題」が発生します。長年セキュリティ業界で働いてきた筆者は、必要な時期にルーターを買い換えていますが、一般の利用者の中には、故障するまで同じルーターを使い続けている方もいらっしゃるのではないでしょうか。

また、ルーターに限らない話ですが、一部の IoT 機器には、故意にサイバー攻撃時にバックドアとして悪用される脆弱性を放置したまま、あるいは説明書に未記載の隠し機能（外部から遠隔操作する機能等）を実装したままで出荷されていると疑われる製品も存在します。セキュリティ研究者の調査によれば、家庭に設置した IoT 家電が海外の製造業者との間で不必要と思われるくらいに多くの通信を行っているのを観測した、といった報告例もあります。

冒頭、FCC によるルーターの輸入規制の話をしましたが、米国内に危険なルーターが蔓延するのを防止するためにそのような規制を実施したのだと考えられます。ここまで極端な規制が日本で実施されることはないと思いますが、では我々はどうやって自らとインターネットの安心・安全を守ればよいのでしょうか。

日本では、2025 年 3 月以降、IPA が IoT 製品のセキュリティ対策状況を評価して適合ラベルを交付する制度「JC-STAR」を開始しています。ラベルが交付された製品の出荷も始まっており、新たに IoT 機器を購入する際の判断材料の一つにするとよいと思います（「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）。

更に、IPA が公開している、消費者のための「ネット接続製品の安全な選定・利用ガイド -詳細版 -[iii]」では、IoT 機器の購入時及び利用時のポイントを紹介しています。また、NOTICE（National Operation Towards IoT Clean Environment）プロジェクトの Web サイト[iv]では、ルーター／ネットワークカメラに潜むリスクや安全な管理方法等が紹介されています。実際のところ、ルーターを介してインターネットに接続するテレビ等の IoT 家電や、ヘルスケアデータを測定・管理する機能を備えたスマートウォッチやスマートリングを導入することで、日々の生活が便利になったと感じている方は多いことでしょう。これらの情報を活用して、日常生活に欠かせなくなったルーターを始めとした IoT 機器を安全に利用しましょう。

i 独立行政法人日本貿易振興機構：米連邦通信委、外国製ルーターの輸入・販売を実質禁止、未承認モデルが対象 https://www.jetro.go.jp/biznews/2026/03/6715ecebb1f498f4.html〔2026/7/27 確認〕
ii CQ 出版社：Interface 2023 年 12 月号、第 1 部第 3 章「IoT 開発におけるセキュリティ機能の重要性」 https://interface.cqpub.co.jp/magazine/202312/〔2026/7/27 確認〕
iii https://www.ipa.go.jp/security/guide/vuln/forconsumer.html〔2026/7/27 確認〕
iv NOTICE：https://notice.go.jp/〔2026/7/27 確認〕

※1　https://www.ibm.com/jp-ja/reports/threat-intelligence〔2026/7/9 確認〕
同レポートは、IBM X-Force が 2025 年のインシデント対応・調査データを中心に、大規模なグローバル環境で観測したインシデント、脆弱性、攻撃者の手法等を分析し、サイバー脅威の動向を整理した年次レポートである。
※2　https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA Threat Landscape 2025_v1.2.pdf〔2026/7/9 確認〕
同レポートは、2024 年 7 月 1 日から 2025 年 6 月 30 日までの期間における 4,875 件のインシデントを分析し、EU が直面する主要なサイバー脅威及び傾向を整理したものである。
※3　IBM 社：X-Force Threat Intelligence Index 2026　https://www.ibm.com/jp-ja/reports/threat-intelligence〔2026/7/9 確認〕
IBM 社：Cloud attacks are evolving: What 2025 trends mean for defenders in 2026　https://www.ibm.com/think/x-force/cloud-attacks-evolving-what-2025-trends-mean-defenders-2026〔2026/7/9 確認〕
※4　https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf〔2026/7/9 確認〕
同レポートは、2024 年 7 月 1 日から 2025 年 6 月 30 日までの脅威動向を対象とし、Microsoft 社が日々処理する 100 兆件のセキュリティシグナル等を基に、世界的なサイバー脅威を分析した年次レポートである。
※5　https://www.ncsc.gov.uk/sites/default/files/documents/ncsc-annual-review-2025.pdf〔2026/7/9 確認〕
同レポートは、英国 NCSC の第 9 年次レビューであり、2024 年 9 月 1 日から 2025 年 8 月 31 日までの主要な活動、脅威動向、インシデント対応、サイバー・レジリエンス向上施策等を整理したものである。
※6　https://insights.nccgroup.com/annual-threat-intelligence-report-2025〔2026/7/9 確認〕
同レポートは、NCC Group の脅威インテリジェンス部門が、2025 年に確認したランサム攻撃被害公表、重要インシデント、APT 活動、法執行機関による摘発、脆弱性悪用等の公開情報及び同社の脅威分析に基づき、サイバー脅威の動向を整理した年次レポートである。
※7　https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2025.pdf〔2026/7/9 確認〕
同レポートは、Sophos 社が委託し、第三者専門機関が 2025 年 1 月から 3 月にかけて実施した独立・ベンダー非依存の調査に基づくものであり、過去 12 ヵ月にランサム攻撃の被害を受けた 17 ヵ国 3,400 人の IT・サイバーセキュリティ責任者の回答を分析している。
※8　出典に当時のレートでの日本円換算の記載がある場合を除いて、本白書では 1 ドル 160 円として換算している。
※9　Chainalysis Inc.：The 2026 Crypto Crime Report（日本語版）　https://www.chainalysis.com/wp-content/uploads/2026/03/the-2026-crypto-crime-report-japanese-release.pdf〔2026/7/9 確認〕
同レポートは、主に 2025 年中のパブリックブロックチェーン上の取引データを対象に、同社が不正アドレスとして特定した暗号資産アドレスへの流入額や資金移動を分析したものである。
※10 Coveware 社：Insider Threats Loom while Ransom Payment Rates Plummet　https://www.coveware.com/blog/2025/10/24/insider-threats-loom-while-ransom-payment-rates-plummet〔2026/7/9 確認〕
同レポートは、2025 年第 3 四半期に Coveware 社が対応・観測したサイバー恐喝事案を基に、身代金支払い額、支払い率、攻撃手法、初期侵入手段等を分析した四半期レポートである。
※11 https://cf-assets.www.cloudflare.com/slt3lc6tev37/sWDBUMNVtEJB9ZFLt1dUU/8d69e92de2edfb3bf59e7d21d57e7e1a/Cloudflare-2026-threat-report.pdf〔2026/7/9 確認〕
同レポートは、Cloudflare 社の脅威調査部門である Cloudforce One が、同社のグローバルネットワーク上のテレメトリ、脅威アクターの戦術・技術・手順（TTPs）、同社の調査・対応事例等を基に、2026 年に向けたサイバー脅威動向を分析したものである。
※12 https://www.netscout.com/threatreport〔2026/7/9 確認〕
同レポートは、2025 年 7 月から 12 月までの DDoS 攻撃を対象に、NetScout 社の ATLAS Threat Intelligence が収集・分析したテレメトリを基に作成されたものである。
※13 世界全体の攻撃件数は約 809 万件であるのに対し、4 地域別の攻撃件数の合計は約 752 万件であり、約 57 万件の差分が生じているが、当該レポートでは、この差分の内訳について明示的な説明は確認できなかった。
※14 DigiCert 社：UltraDDoS Protect Annual Distributed Denial-of-Service Analysis, January–December 2025　https://vercara.digicert.com/wp-content/uploads/2026/03/digicert-ultra-ddos-protect-annual-report.pdf〔2026/7/9 確認〕
同レポートは、2025 年に DigiCert 社の DDoS 対策サービス UltraDDoS Protect が検知・緩和した DDoS 攻撃を基に、攻撃件数、攻撃規模、攻撃時間、攻撃手法、標的業種、標的国、送信元国等を分析したものである。
※15 APWG：Phishing Activity Trends Report, 4th Quarter 2025　https://docs.apwg.org/reports/apwg_trends_report_q4_2025.pdf〔2026/7/9 確認〕
同レポートは、2025 年 10 月から 12 月までに APWG 及び協力企業・研究パートナーが報告・観測したフィッシング攻撃等を基に、フィッシング活動の動向を分析したものである。
※16 Surfshark 社：Wrapping up 2025: global data breach statistics　https://surfshark.com/research/study/data-breach-recap-2025〔2026/7/9 確認〕
同記事は、2025 年に公開データベース上で確認された漏えいメールアドレスを基に、国・地域、業種、漏えい規模等の観点からデータ侵害の動向を分析したものである。
※17 ITRC：2025 Data Breach Report, Twentieth Edition　https://www.idtheftcenter.org/wp-content/uploads/2026/01/2025-ITRC-Annual-Data-Breach-Report.pdf〔2026/7/9 確認〕
同レポートは、2025 年に米国で公表・通知されたデータ侵害等を基に、侵害件数、影響を受けた個人、侵害原因等を分析したものである。
※18 https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf〔2026/7/9 確認〕
同レポートは、2025 年に IC3 を通じて FBI に提出されたインターネット犯罪等の苦情・被害申告を基に、犯罪類型、申告件数、被害額等を分析したものである。
※19 https://www.gstatic.com/security-marketing/m-trends-2026-en.pdf〔2026/7/9 確認〕
同レポートは、2025 年 1 月 1 日から 12 月 31 日までに Mandiant が特定した標的型攻撃活動及び同年に世界各地で実施した 50 万時間超のインシデント対応業務から得た調査データを基に、サイバー侵害の動向を分析したものである。
※20 https://www.interpol.int/content/download/24327/file/CYBER_ASP Cyber Threat Assessment Report_2025_2026_v4.pdf〔2026/7/9 確認〕
同レポートは、2024 年 1 月から 2025 年 3 月までのアジア・南太平洋地域におけるサイバー犯罪脅威を対象に、加盟国への質問票調査、民間部門パートナーからの情報、作戦事例、ICPO のインテリジェンス及び運用上の知見等を基に分析したものである。
※21 別の攻撃者が確立した足がかり（認証情報やバックドア等）を利用して、他の攻撃者が標的環境へのアクセス権を獲得することを指す。
※22 https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf〔2026/7/9 確認〕
※23 MSMT：The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities　https://www.mofa.go.jp/files/100922718.pdf〔2026/7/9 確認〕
同報告書は、MSMT 参加国政府の情報、民間部門の報告、公開情報を基に作成され、複数の情報源により評価・裏付けを行ったとしている。調査・報告対象期間は 2024 年 1 月から 2025 年 9 月である。
※24 https://www.antiphishing.jp/report/monthly/〔2026/7/10 確認〕
同報告書は、毎月、前月分のフィッシングに関する報告件数、フィッシングサイト URL 件数、悪用されたブランド数をグラフにまとめたものである。
※25 フィッシング対策協議会：資料公開：フィッシングレポート 2026 公開のお知らせ　https://www.antiphishing.jp/news/info/press_phishing_report2026.html〔2026/7/10 確認〕
同レポートは、2025 年 1 月から 12 月までのフィッシングの被害状況、フィッシングの攻撃技術・手法等を取りまとめたものである。
※26 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf〔2026/7/10 確認〕
同レポートは、2025 年のサイバー犯罪、サイバー攻撃等のサイバー空間の脅威について、事例や統計等データを掲載したものである。
※27 株式会社東京商工リサーチ：上場企業の「個人情報漏えい・紛失」事故　2 番目の 180 件発生、漏えい人数は約 2 倍増の 3,063 万人分　https://www.tsr-net.co.jp/data/detail/1202348_1527.html〔2026/7/10 確認〕
同調査は、上場企業と子会社の情報漏えい・紛失事故のプレスリリース、お知らせ、お詫び等、自主的な開示を株式会社東京商工リサーチが独自集計したものであり、毎年実施しているものである。
※28 株式会社東京商工リサーチ：2024 年上場企業の「個人情報漏えい・紛失」事故　過去最多の 189 件、漏えい情報は 1,586 万人分　https://www.tsr-net.co.jp/data/detail/1200872_1527.html〔2026/7/10 確認〕
※29 株式会社東京商工リサーチ：2023 年の「個人情報漏えい・紛失事故」が年間最多　件数 175 件、流出・紛失情報も最多の 4,090 万

人分　https://www.tsr-net.co.jp/data/detail/1198311_1527.html〔2026/7/10 確認〕
※ 30 株式会社東京商工リサーチ：個人情報漏えい・紛失事故 2 年連続最多を更新 件数は 165 件、流出・紛失情報は 592 万人分 ～ 2022 年「上場企業の個人情報漏えい・紛失事故」調査 ～　https://www.tsr-net.co.jp/data/detail/1197322_1527.html〔2026/7/10 確認〕
※ 31 株式会社東京商工リサーチ：上場企業の個人情報漏えい・紛失事故は、調査開始以来最多の 137 件 574 万人分（2021 年）　https://www.tsr-net.co.jp/data/detail/1191102_1527.html〔2026/7/10 確認〕
※ 32 警察庁：令和 7 年におけるサイバー空間をめぐる脅威の情勢等について　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf〔2026/7/10 確認〕
※ 33 IIJ 社：観測レポートの記事一覧　https://wizsafe.iij.ad.jp/category/report/〔2026/7/10 確認〕
同レポートは、DDoS 攻撃、不正アクセス通信、マルウェア脅威等の観測情報を月次でまとめたものである。
※ 34 https://csl.nict.go.jp/report/NICTER_report_2025.pdf〔2026/7/10 確認〕
同レポートは、NICTER プロジェクトで運用されているダークネット及び各種ハニーポットの観測結果に基づき，2025 年に確認されたサイバー攻撃関連事象をまとめたものである。
※ 35 トレンドマイクロ社：ランサムウェア「REvil」、「Clop」、「Conti」に見る多重脅迫の実態　https://www.trendmicro.com/ja_jp/research/22/b/multiple-extortion-on-Revil-cl0p-conti.html〔2026/7/16 確認〕
※ 36 警察庁：ランサムウェア被害防止対策　https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html〔2026/7/16 確認〕
※ 37 警察庁：令和 6 年上半期におけるサイバー空間をめぐる脅威の情勢等について　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf〔2026/7/16 確認〕
※ 38 トレンドマイクロ社：海外拠点におけるサプライチェーンリスク　https://www.trendmicro.com/ja_jp/jp-security/24/e/securitytrend-20240524-01.html〔2026/7/16 確認〕
※ 39 wiz LANSCOPE：ノーウェアランサムとは?ランサムウェアとの違いや対策を解説　https://www.lanscope.jp/blogs/cyber_attack_cpdi_blog/20231026_15683/〔2026/7/16 確認〕
※ 40 トレンドマイクロ社：警察庁のサイバー犯罪レポートに見る「ノーウェアランサム」とは? ～組織として対策しておくべきことは変わるのか?～　https://www.trendmicro.com/ja_jp/jp-security/23/j/securitytrend-20231006-01.html〔2026/7/16 確認〕
※ 41 Mandiant Inc.：APT41, A DUAL ESPIONAGE AND CYBER CRIME OPERATION　https://services.google.com/fh/files/misc/apt41-a-dual-espionage-and-cyber-crime-operation.pdf〔2026/7/16 確認〕
※ 42 Dark Reading：'ChamelGang' APT Disguises Espionage Activities With Ransomware　https://www.darkreading.com/ics-ot-security/china-nexus-group-using-ransomware-to-disguise-cyber-espionage-activities〔2026/7/16 確認〕
※ 43 The Hacker News：Chinese and N. Korean Hackers Target Global Infrastructure with Ransomware　https://thehackernews.com/2024/06/chinese-and-n-korean-hackers-target.html〔2026/7/16 確認〕
※ 44 NTT セキュリティ・ジャパン株式会社：サイバーセキュリティレポート 2026.02　https://files.microcms-assets.io/assets/0a7887130ff54185a3a008502e377859/1772e8990d544bafb811f246ba4add2b/ サイバーセキュリティレポート _202602.pdf〔2026/7/16 確認〕
※ 45 伊藤忠テクノソリューションズ株式会社：ランサムウェアグループによる虚偽のリーク活動｜“盗まれていない情報”が脅迫に使われる時代　https://www.ctc-g.co.jp/keys/blog/detail/ransomware-fake-leaks〔2026/7/16 確認〕
※ 46 アサヒグループホールディングス株式会社：サイバー攻撃によるシステム障害発生について　https://www.asahigroup-holdings.com/newsroom/detail/20250929-0102.html〔2026/7/16 確認〕
※ 47 アサヒグループホールディングス株式会社：サイバー攻撃によるシステム障害発生について（第 2 報）　https://www.asahigroup-holdings.com/newsroom/detail/20251003-0104.html〔2026/7/16 確認〕
※ 48 THE PAGE：アサヒ・勝木社長が会見　サイバー攻撃によるシステム障害の調査結果を説明（2025 年 11 月 27 日）　https://www.youtube.com/watch?v=BG4Vh-H1k4I〔2026/7/16 確認〕
※ 49 日経クロステック：アサヒグループ HD のランサム被害、物流システム停止で出荷と決算に影響　https://xtech.nikkei.com/atcl/nxt/column/18/01157/102300145/〔2026/7/16 確認〕
※ 50 アサヒグループホールディングス株式会社：サイバー攻撃被害の再発防止策とガバナンス体制の強化について　https://www.asahigroup-holdings.com/newsroom/detail/20260218-0101.html〔2026/7/16 確認〕
※ 51 The Asahi Shimbun：Japan's Asahi hack that halted beer production claimed by Qilin ransomware group　https://www.asahi.com/ajw/articles/16077955〔2026/7/16 確認〕
※ 52 アスクル株式会社：ランサムウェア感染によるシステム障害発生のお知らせとお詫び（第1報）　https://pdf.irpocket.com/C0032/w4ok/STuh/ai44.pdf〔2026/7/16 確認〕
※ 53 アスクル株式会社：ランサムウェア攻撃の影響調査結果および安全性強化に向けた取り組みのご報告（ランサムウェア攻撃によるシステム障害関連・第 13 報）　https://pdf.irpocket.com/C0032/PDLX/03bg/N403.pdf〔2026/7/16 確認〕
※ 54 セキュリティ対策 Lab：アスクル、ランサムウェアによるサイバー攻撃で約 74 万件の個人情報流出の可能性　https://rocket-boys.co.jp/security-measures-lab/askul-ransomware-attack-possible-leak-of-740k-records/〔2026/7/16 確認〕
※ 55 gbhackers.：RansomHouse RaaS Enhances Double Extortion with Data Theft and Encryption　https://gbhackers.com/ransomhouse-raas/〔2026/7/16 確認〕
※ 56 アスクル株式会社：サービスの復旧状況について（ランサムウェア攻撃によるシステム障害関連・第 18 報）　https://pdf.irpocket.com/C0032/YpwX/YPJ9/h35G.pdf〔2026/7/16 確認〕
※ 57 Cyber Security News：New Volcano Demon Ransomware Group Threatening Victims Over Phone Call　https://cybersecuritynews.com/ransomware-threats-via-phone-calls/〔2026/7/16 確認〕
※ 58 https://www.cisa.gov/stopransomware/ransomware-guide〔2026/7/16 確認〕
※ 59 NIST：Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile　https://nvlpubs.nist.gov/nistpubs/ir/2026/NIST.IR.8374r1.pdf〔2026/7/16 確認〕
※ 60 NRI セキュアテクノロジーズ株式会社：マイクロセグメンテーションの実現方法｜ランサムウェアの被害を防ぐ最後の砦　https://www.nri-secure.co.jp/blog/microsegmentation〔2026/7/16 確認〕
※ 61 https://www.ipa.go.jp/publish/wp-security/2023.html〔2026/7/16 確認〕
※ 62 NO MORE RANSOM：https://www.nomoreransom.org/ja/index.html〔2026/7/16 確認〕
※ 63 https://www.jpcert.or.jp/magazine/security/ransom-faq.html〔2026/7/16 確認〕
※ 64 https://www.cyber.go.jp/pdf/policy/general/guider7_9.pdf〔2026/7/13 確認〕
※ 65 ESET, spol. s r.o.：Mind the (air) gap: GoldenJackal gooses government guardrails　https://www.welivesecurity.com/en/eset-research/mind-air-gap-goldenjackal-gooses-government-guardrails/〔2026/7/13 確認〕
※ 66 Google LLC：State-backed attackers and commercial surveillance vendors repeatedly use the same exploits　https://blog.google/threat-analysis-group/state-backed-attackers-and-commercial-surveillance-vendors-repeatedly-use-the-same-exploits/〔2026/7/13 確認〕
※ 67 トレンドマイクロ社：国内標的型攻撃分析レポート 2022 年版を発表　https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220510-01.html〔2026/7/13 確認〕
トレンドマイクロ社：MirrorFace（ミラーフェイス）とは?～警察が注意喚起を行った標的型攻撃グループを解説～　https://www.trendmicro.com/ja_jp/jp-security/25/a/expertview-20250109-01.html〔2026/7/13 確認〕
※ 68 C&C（Command and Control）サーバー：マルウェア等により乗っ取ったコンピューター等に対し、遠隔から命令を送り制御するサーバー。
※ 69 IPA：インターネット境界に設置された装置に対するサイバー攻撃について～ネットワーク貫通型攻撃に注意しましょう～　https://www.ipa.go.jp/archive/security/security-alert/2023/alert20230801.html〔2026/7/13 確認〕
IPA：オンラインストレージの脆弱性対策について　https://www.ipa.go.jp/archive/security/security-alert/2023/alert20231019.html〔2026/7/13 確認〕
IPA：PHP の脆弱性（CVE-2024-4577）を狙う攻撃について　https://www.ipa.go.jp/security/security-alert/2024/alert_20240705.html〔2026/7/13 確認〕
※ 70 Operational Relay Box（ORB）：攻撃トラフィックの中継機能を設置させられる被害を受けたサーバー等の端末。攻撃に関連する通信の送信元や送信先を隠匿するために利用される。
※ 71 IPA:アタックサーフェスの Operational Relay Box 化を伴うネットワーク貫通型攻撃について ～ Adobe ColdFusion の脆弱性（CVE-2023-

29300）を狙う攻撃～ https://www.ipa.go.jp/security/security-alert/2024/alert_orb.html〔2026/7/13 確認〕
※ 72 CISA 等：PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf〔2026/7/13 確認〕
※ 73 Living Off The Land（LOTL）戦術：情報窃取等の侵害活動を行う際に、独自のマルウェアではなく、システム内の正規のツール・機能等を活用することにより、検知を回避する攻撃戦術。
※ 74 内閣官房内閣サイバーセキュリティセンター：Living Off The Land 戦術等を含む最近のサイバー攻撃に関する注意喚起 https://www.cyber.go.jp/pdf/news/press/240625NISC_press.pdf〔2026/7/13 確認〕
※ 75 トレンドマイクロ社：MirrorFace（ミラーフェイス）とは?～警察が注意喚起を行った標的型攻撃グループを解説～ https://www.trendmicro.com/ja_jp/jp-security/25/a/expertview-20250109-01.html〔2026/7/13 確認〕
※ 76 CrowdStrike Holdings, Inc.：クラウドストライク 2026 年版グローバル脅威レポート：AI によって加速する攻撃者と新たに形成される攻撃対象領域 https://www.crowdstrike.com/ja-jp/press-releases/2026-crowdstrike-global-threat-report/?__cf_chl_f_tk=CcMgY_Cbcz2WWbc0x7bMj1Mh48w8wIgK7tA9Zd019ul-1783042992-1.0.1.1-0XcRJD9my9ZrtE.ka1h4iil7gSObll.uDnYcsM1NOzc〔2026/7/13 確認〕
CrowdStrike Holdings, Inc.：クラウドストライク 2025 年版グローバル脅威レポート：中国のサイバースパイの活動が 150% 増加し、攻撃手法も大幅に高度化、AI を使った詐欺的手口の悪用も https://www.crowdstrike.com/ja-jp/press-releases/crowdstrike-releases-2025-global-threat-report/〔2026/8/25 確認〕
※ 77 「国家支援型」の攻撃は、「ステートスポンサード」（state-sponsored）、「ネイションバックド」（nation-backed）の攻撃と呼ばれることもある。実際の活動は外国の軍及び情報機関、宣伝機関が直接、または下請のハッカー（Hack-For-Hire）や犯罪者（政府放任型サイバー犯罪グループ）を介して行われるとされる。
IPA：サイバーレスキュー隊 (J-CRAT) 活動状況［2022 年度上半期］ https://www.ipa.go.jp/security/j-crat/ug65p9000000nks8-att/000106897.pdf〔2026/7/13 確認〕
※ 78 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2022 年 7 月～ 9 月］ https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000103970.pdf〔2026/7/13 確認〕（標的別に改変・開発したマルウェアの使用については「3.2.3 攻撃で使われたウイルス」、標的組織の内部に長期間潜伏して活動する点については「3.2.1 初期侵入」をそれぞれ参照）
※ 79 トレンドマイクロ社：日本や台湾を狙う標的型攻撃：「Earth Kasha」が攻撃手法を更新して新たな攻撃キャンペーンを開始 https://www.trendmicro.com/ja_jp/research/25/e/earth-kasha-updates-ttps.html〔2026/7/13 確認〕
※ 80 警察庁、内閣サイバーセキュリティセンター：MirrorFace によるサイバー攻撃について（注意喚起） https://www.npa.go.jp/bureau/cyber/pdf/20250108_caution.pdf〔2026/7/13 確認〕
※ 81 https://www.ipa.go.jp/publish/wp-security/2025.html〔2026/10/13 確認〕
※ 82 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〔2026/7/13 確認〕
※ 83 NCO、警察庁：「ソルトタイフーン（Salt Typhoon）」に関する国際アドバイザリーへの共同署名について https://www.npa.go.jp/bureau/cyber/pdf/20250827.pdf〔2026/7/13 確認〕
※ 84 The MITRE Corporation（MITRE）：CVE-2024-21887 https://www.cve.org/CVERecord?id=CVE-2024-21887〔2026/7/13 確認〕
※ 85 MITRE：CVE-2024-3400 https://www.cve.org/CVERecord?id=CVE-2024-3400〔2026/7/13 確認〕
※ 86 MITRE：CVE-2023-20273 https://www.cve.org/CVERecord?id=CVE-2023-20273〔2026/7/13 確認〕
※ 87 MITRE：CVE-2023-20198 https://www.cve.org/CVERecord?id=CVE-2023-20198〔2026/7/13 確認〕
※ 88 https://www.ipa.go.jp/security/security-alert/2025/alert20251031_vpn.html〔2026/7/13 確認〕
※ 89 Cloud Software Group, Inc.：NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-7775, CVE-2025-7776 and CVE-2025-8424 https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694938〔2026/7/13 確認〕
Ivanti Software, Inc.：April Security Advisory Ivanti Connect Secure, Policy Secure & ZTA Gateways (CVE-2025-22457) https://hub.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457?language=en_US〔2026/7/13 確認〕
Fortinet, Inc.：Authentication bypass in Node.js websocket module and CSF requests https://www.fortiguard.com/psirt/FG-IR-24-535〔2026/7/13 確認〕
※ 90 IPA：NetScaler ADC および NetScaler Gateway の脆弱性について（CVE-2025-7775 等） https://www.ipa.go.jp/security/security-alert/2025/alert20250827.html〔2026/7/13 確認〕
※ 91 JPCERT/CC:Ivanti Connect Secure などにおける脆弱性（CVE-2025-22457）に関する注意喚起 https://www.jpcert.or.jp/at/2025/at250008.html〔2026/7/13 確認〕
※ 92 IPA：Fortinet 製 FortiOS の脆弱性対策について（CVE-2024-55591） https://www.ipa.go.jp/security/security-alert/2024/alert20250115.html〔2026/7/13 確認〕
※ 93 JLR 社：Statement on Cyber Incident 2 September 2025 https://media.jaguarlandrover.com/news/2025/09/statement-cyber-incident〔2026/7/13 確認〕
※ 94 SecurityWeek：Jaguar Land Rover Operations 'Severely Disrupted' by Cyberattack https://www.securityweek.com/jaguar-land-rover-operations-severely-disrupted-by-cyberattack/〔2026/7/13 確認〕
※ 95 The Sun：Legendary car brand halts ALL production at £1.04billion plant after being forced to shut down IT systems https://www.thesun.co.uk/motors/36615743/legendary-car-brand-halts-production-plant-shut-down/〔2026/7/13 確認〕
※ 96 The Record：Jaguar Land Rover says cyberattack shutdown to last 'at least' another week https://therecord.media/jaguar-land-rover-another-week-shutdown-cyberattack〔2026/7/13 確認〕
※ 97 The Guardian：Jaguar Land Rover hack has cost UK economy £1.9bn, experts say https://www.theguardian.com/business/2025/oct/22/jaguar-land-rover-hack-has-cost-uk-economy-19bn-most-costly-cyber-attack-britain〔2026/7/13 確認〕
※ 98 JLR 社：Statement on Cyber Incident 16 September 2025 https://media.jaguarlandrover.com/news/2025/09/statement-cyber-incident-2〔2026/7/13 確認〕
JLR 社：Statement on Cyber Incident 23 September 2025 https://media.jaguarlandrover.com/news/2025/09/statement-cyber-incident-4〔2026/7/13 確認〕
※ 99 JLR 社：JLR restarts manufacturing and introduces new financing solution to pay JLR suppliers early https://media.jaguarlandrover.com/news/2025/10/jlr-restarts-manufacturing-and-introduces-new-financing-solution-pay-jlr-suppliers〔2026/7/13 確認〕
※ 100 本白書では 1 ポンド 216 円として換算している。
※ 101 SecurityWeek：Cyberattack on JLR Prompts £1.5 Billion UK Government Intervention https://www.securityweek.com/cyberattack-on-jlr-prompts-1-5-billion-uk-government-intervention/〔2026/7/13 確認〕
※ 102 BBC：M&S hackers claim to be behind Jaguar Land Rover cyber attack https://www.bbc.com/news/articles/c4gqepe5355o〔2026/7/13 確認〕
※ 103 The New York Times：A $2.5 Billion Whodunit: The Hack That Dented the U.K. Economy https://www.nytimes.com/2026/06/26/world/europe/jaguar-russia-hack.html〔2026/7/13 確認〕
※ 104 The Nextw Web：Russian hackers were behind the Jaguar Land Rover attack that cost the British economy two and a half billion dollars https://thenextweb.com/news/jaguar-land-rover-hack-russian-hackers-nyt-investigation〔2026/7/13 確認〕
※ 105 サイバー安全保障分野での対応能力の向上に向けた有識者会議：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 https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/koujou_teigen/teigen.pdf〔2026/7/13 確認〕
※ 106 なお、国家支援型 APT 攻撃への備えとしては、経済安全保障の文脈で、輸出管理部門やリスク対策部門、経営管理部門等ビジネスインテリジェンスに関わる組織とも密に連携し、サイバー攻撃以外のリスクも併せた、全方位的な脅威状況の把握への参画も必要である。
※ 107 産業サイバーセキュリティ研究会：産業界へのメッセージ（令和 7 年 5 月 23 日） https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20250523.pdf〔2026/7/13 確認〕
※ 108 サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会：サイバー攻撃被害に係る情報の共有・公表ガイダンス https://www.

cyber.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf〔2026/7/13 確認〕
※ 109 一般社団法人情報通信ネットワーク産業協会、通信ネットワーク機器セキュリティ委員会：サプライチェーンセキュリティ調査 https://www.ciaj.or.jp/ciaj-wp/wp-content/uploads/2025/03/technical20250317.pdf〔2026/7/13 確認〕
※ 110 経済産業省、IPA：サイバーセキュリティ経営ガイドライン Ver 3.0 https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf〔2026/7/13 確認〕
※ 111 https://www.ipa.go.jp/security/guide/hjuojm000000551l0-att/ps6vr7000000jvcb.pdf〔2026/7/13 確認〕
※ 112 参考として、「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」（令和4年法律第 43 号）に基づく基幹インフラ制度における特定重要設備の導入時の事前審査について、内閣府「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度のパンフレット（令和 8 年 6 月 17 日時点）」（https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/infra.html〔2026/7/13 確認〕）参照。
※ 113 株式会社エヌ・ティ・ティ・データ経営研究所：IPA「組織における内部不正防止ガイドライン」の改訂に係る調査等業務 概要説明資料 https://www.ipa.go.jp/security/guide/hjuojm000000551l0-att/Ver5gaiyo.pdf〔2026/7/13 確認〕
※ 114 株式会社エヌ・ティ・ティ・データ経営研究所：企業における内部不正防止体制に関する実態調査概要説明資料 https://www.ipa.go.jp/security/reports/economics/ts-kanri/ps6vr7000000jpfj-att/ps6vr7000000juft.pdf〔2026/7/13 確認〕
※ 115 警察庁の「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/NK_it.pdf〔2026/7/13 確認〕）で指摘されているように、北朝鮮の IT 労働者は、不正な資金の獲得及び情報窃取等のサイバー攻撃に関与しているとされる。このような脅威に対応するためには、IT/OT システムのセキュリティ対策のみならず、サイバードメインにおける脅威ととらえて適切にリスク管理する必要がある。
※ 116 DMARC ポリシーが適切に設定されていない場合、なりすましメール対策として効果がなく、APT 攻撃に悪用されるおそれがあることに注意が必要である。
Proofpoint, Inc.：北朝鮮 APT 攻撃グループ「TA427」：DMARC 設定が緩い日本政府などの組織になりすまし、ソーシャル・エンジニアリングで情報収集 https://www.proofpoint.com/jp/blog/threat-insight/social-engineering-dmarc-abuse-ta427s-art-information-gathering〔2026/7/13 確認〕
※ 117 株式会社ラック：ClickFix の被害を JSOC の複数のお客様にて観測 https://www.lac.co.jp/lacwatch/alert/20250519_004380.html〔2026/7/13 確認〕
※ 118 ファイルレスマルウェア：マルウェア本体をディスクドライブ上に直接格納せず、悪意あるコードを PowerShell 等のツールに読み込ませることで、メモリー上で実行・動作するタイプのマルウェアのこと。
※ 119 株式会社ラック：包括的なクラウドセキュリティを実現する CNAPP の重要性 https://www.lac.co.jp/lacwatch/service/20250520_004375.html〔2026/7/13 確認〕
※ 120 JPCERT/CC：高度サイバー攻撃への対処におけるログの活用と分析方法 1.2 版 https://www.jpcert.or.jp/research/APT-loganalysis_Report_20220510.pdf〔2026/7/13 確認〕
JPCERT/CC：ログを活用した高度サイバー攻撃の早期発見と分析 https://www.jpcert.or.jp/research/APT-loganalysis_Presen_20151117.pdf〔2026/7/13 確認〕
※ 121 IPA：サイバーレスキュー隊（J-CRAT）活動状況〔2017 年度上半期〕 https://www.ipa.go.jp/security/j-crat/ug65p9000000nks8-att/000062239.pdf〔2026/7/13 確認〕
※ 122 経済産業省：「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する～」を取りまとめました https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html〔2026/7/13 確認〕
※ 123 IPA：サイバーレスキュー隊 (J-CRAT) 活動状況〔2022 年度上半期〕 https://www.ipa.go.jp/security/j-crat/ug65p9000000nks8-att/000106897.pdf〔2026/7/13 確認〕
※ 124 @ IT:JPCERT/CC が「Active Directory のセキュリティ」にフォーカスした文書を公開 https://atmarkit.itmedia.co.jp/ait/articles/1703/15/news064.html〔2026/7/13 確認〕
※ 125 「個人情報の保護に関する法律」（平成 15 年法律第 57 号）では、不正アクセスにより個人データの漏えいが発生し、または、発生したおそれがある場合、原則として、個人情報保護委員会への報告及び本人への通知が義務付けられている（同法第 26 条第 1 項本文及び同条第 2 項本文、「個人情報の保護に関する法律施行規則」（平成 28 年個人情報保護委員会規則第 3 号）第 7 条第 3 号及び第 10 条。「個人情報の保護に関する法律についてのガイドライン（通則編）」3-5-1 参照）。また、保有する個人データの中に本人の連絡先が含まれていない場合や、連絡先が古いために通知を行う時点で本人へ連絡できない場合等、本人への通知が困難な場合は、事案の公表等が求められる（同法第 26 条第 2 項ただし書き。同ガイドライン 3-5-4-5 参照）。従って、連絡のつかない退職者の個人データが残存していると、その漏えいのおそれがある場合に事案の公表が必要になるリスクが生じるため、退職者のアカウントを含め、連絡のつかない退職者の個人データは定期的な棚卸し等により適切な整理が必要と考えられる。
個人情報保護委員会：個人情報の保護に関する法律についてのガイドライン（通則編） https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/〔2026/7/13 確認〕
※ 126 NetScout Systems, Inc.：Why Do Hackers Use DDoS Attacks? https://www.netscout.com/blog/why-do-hackers-use-ddos-attacks〔2026/7/13 確認〕
※ 127 一般財団法人日本気象協会：天気予報専門メディア「tenki.jp」への DDoS 攻撃につきまして https://www.jwa.or.jp/news/2025/01/25046/〔2026/7/13 確認〕
※ 128 NetScout Systems, Inc.：DDoS-for-Hire and the Evolving Use of AI https://www.netscout.com/blog/asert/ddos-hire-and-evolving-use-ai〔2026/7/13 確認〕
※ 129 トレンドマイクロ社：ハクティビストとは?日本を標的とした最新のサイバー攻撃を解説 https://www.trendmicro.com/ja_jp/jp-security/24/j/securitytrend-20241022-01.html〔2026/7/13 確認〕
Europol：Global operation targets NoName057(16) pro-Russian cybercrime network https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network〔2026/7/13 確認〕
※ 130 Business Wire, Inc.：ネットスカウトの最新調査：DDoS が引き続きデジタル空間を圧巻し、重要インフラを不安定化させていることを明らかに https://secure.businesswire.com/news/home/20250827900504/ja〔2026/7/13 確認〕
※ 131 CybelAngel：Cyber Threat Landscape of the Russia-Ukraine War (Jan 2022 – Jan 2026) https://cybelangel.com/wp-content/uploads/2026/05/Cyber-Threat-Landscape-of-the-Russia-Ukraine-War_CybelAngel-report.pdf〔2026/7/13 確認〕
※ 132 CDN（Content Delivery Network）：Web サイトのコンテンツを複製・保存し、最適な経路でエンドユーザーに配信するネットワーク。
※ 133 Cloudflare 社：2025 年第 4 四半期 DDoS 脅威レポート：過去最高の 31.4Tbps 攻撃が大規模な DDoS 攻撃の 1 年を締めくくる https://blog.cloudflare.com/ja-jp/ddos-threat-report-2025-q4/〔2026/7/13 確認〕
※ 134 株式会社ナード研究所：ネットワーク不具合によるメール受信遅延のお詫び https://www.nard.co.jp/info/detail.php?id=166〔2026/7/13 確認〕
※ 135 株式会社ナード研究所：ネットワーク不具合による影響についてのお詫び https://www.nard.co.jp/info/detail.php?id=167〔2026/7/13 確認〕
※ 136 株式会社ナード研究所：ネットワーク不具合に関するお詫び（続報） https://www.nard.co.jp/info/detail.php?id=171〔2026/7/13 確認〕
※ 137 カゴヤ・ジャパン株式会社：【レンタルサーバー：290322】Web メール（Active!mail）、コントロールパネル接続障害復旧のお知らせ（7 月 30 日 18 時 18 分更新） https://www.kagoya.jp/news/2025073033092/〔2026/7/13 確認〕
※ 138 Cloudflare 社：DDoS ボットネットとは? https://www.cloudflare.com/ja-jp/learning/ddos/what-is-a-ddos-botnet/〔2026/7/13 確認〕
※ 139 NISC：DDoS 攻撃への対策について（注意喚起） https://www.cyber.go.jp/pdf/news/press/20250204_ddos.pdf〔2026/7/13 確認〕
※ 140 WAF（Web Application Firewall）：Web サイトや動画などのコンテンツを利用者に安定して届けるために、世界中に分散させたサーバーでデータを配信する仕組み。
※ 141 春田法律事務所：DDoS 攻撃の仕組みとは?中小企業にも忍び寄るサーバーダウンのリスクと法的備え https://haruta-lo.com/column/ddos-attack-risk-legal-measures/# 中小企業で実際に発生した DDoS 被害の事例〔2026/7/13 確認〕
※ 142 https://www.ipa.go.jp/security/10threats/10threats2026.html〔2026/7/13 確認〕
※ 143 JPCERT/CC：Ivanti Connect Secure などにおける脆弱性（CVE-2025-0282）に関する注意喚起 https://www.jpcert.or.jp/at/2025/at250001.html〔2026/7/13 確認〕
※ 144 Cisco Systems, Inc.:Cisco Secure Firewall 適応型セキュリティアプライアンス ソフトウェアおよび Cisco Secure Firewall Defense ソフトウェアの VPN Web サーバーのリモートコード実行における脆弱性 https://www.cisco.com/c/ja_jp/support/docs/csa/2025/cisco-sa-asaftd-webvpn-z5xP8EUB.html〔2026/7/13 確認〕

※ 145 CISA：ED 25-03: Identify and Mitigate Potential Compromise of Cisco Devices https://www.cisa.gov/news-events/directives/ed-25-03-identify-and-mitigate-potential-compromise-cisco-devices〔2026/7/13 確認〕
※ 146 Oracle Corporation：Oracle Security Alert Advisory - CVE-2025-61882 https://www.oracle.com/security-alerts/alert-cve-2025-61882.html〔2026/7/13 確認〕
※ 147 Google LLC：Oracle E-Business Suite のゼロデイが広範囲にわたる恐喝キャンペーンで悪用される https://cloud.google.com/blog/ja/topics/threat-intelligence/oracle-ebusiness-suite-zero-day-exploitation〔2026/7/13 確認〕
※ 148 DeepStrike, LLC：Cl0p Ransomware: How the Group Operates, Major Campaigns, and How to Defend https://deepstrike.io/blog/cl0p-ransomware〔2026/7/24 確認〕
※ 149-1 IIJ 社：IIJ セキュア MX サービスにおけるお客様情報の漏えいについて https://www.iij.ad.jp/news/pressrelease/2025/0415.html〔2026/7/13 確認〕
※ 149-2 日経クロステック：Active! mail の脆弱性があった 200 台超のサーバーの現状、6 割は更新・2 割は停止 https://xtech.nikkei.com/atcl/nxt/column/18/03207/052100002/〔2026/8/6 確認〕
※ 150-1 Cisco Systems, Inc.：Cisco Secure Email Gateway および Cisco Secure Email & Web Manager に対するサイバー攻撃に関するレポート https://www.cisco.com/c/ja_jp/support/docs/csa/2025/cisco-sa-sma-attack-N9bf4.html〔2026/7/13 確認〕
※ 150-2 株式会社 TOKAI コミュニケーションズ：OneOffice メールソリューションにおける不正アクセスによる個人情報漏洩の可能性についてのお知らせとお詫び https://www.tokai-com.co.jp/news/pdf/2025/20251219.pdf〔2026/8/6 確認〕
慶應義塾：不正アクセスによる個人情報漏洩の可能性についてのお知らせとお詫び https://www.keio.ac.jp/ja/news/20251226-171741/〔2026/8/6 確認〕
※ 151 JPCERT/CC：Array Networks Array AG シリーズにおけるコマンドインジェクションの脆弱性に関する注意喚起 https://www.jpcert.or.jp/at/2025/at250024.html〔2026/7/13 確認〕
※ 152 Cloud Software Group, Inc.：NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-5349 and CVE-2025-5777 https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420〔2026/7/13 確認〕
※ 153 Amazon Web Services, Inc.：Amazon discovers APT exploiting Cisco and Citrix zero-days https://aws.amazon.com/jp/blogs/security/amazon-discovers-apt-exploiting-cisco-and-citrix-zero-days/〔2026/7/13 確認〕
※ 154 PoC（Proof of Concept）：発見された脆弱性を実証するために公開されたプログラムコード。不正侵入やマルウェア感染を試みる悪意のあるプログラムの一部として悪用されることがある。
※ 155 株式会社サンリオ：株式会社サンリオエンターテイメントへの不正アクセスならびに情報漏洩の可能性に関する調査結果のご報告 https://corporate.sanrio.co.jp/information/20250812〔2026/7/13 確認〕
株式会社サンリオエンターテイメント：当社への不正アクセスによるネットワークトラブルについて https://www.sanrio-entertainment.co.jp/news/250812/〔2026/7/13 確認〕
※ 156 GlobeNewswire：Rapid7 Q3 Threat Report Reveals Ransomware Alliances, AI Weaponization, and the Obsolescence of “Time to Patch” https://www.globenewswire.com/news-release/2025/11/12/3186337/36514/en/Rapid7-Q3-Threat-Report-Reveals-Ransomware-Alliances-AI-Weaponization-and-the-Obsolescence-of-Time-to-Patch.html〔2026/7/13 確認〕
※ 157 VulnCheck, Inc.：VulnCheck State of Exploitation 2026 https://www.vulncheck.com/blog/state-of-exploitation-2026〔2026/7/13 確認〕
※ 158 IPA：共通脆弱性評価システム CVSS v3 概説 https://www.ipa.go.jp/security/vuln/scap/cvssv3.html〔2026/7/13 確認〕
※ 159 Google LLC：Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability（CVE-2025-22457） https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability?hl=en〔2026/7/13 確認〕
※ 160 NVD：CVE-2025-22457 https://nvd.nist.gov/vuln/detail/CVE-2025-22457〔2026/7/24 確認〕
※ 161 CISA：Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog〔2026/7/13 確認〕
※ 162 NIST：National Vulnerability Database https://nvd.nist.gov/〔2026/7/13 確認〕
※ 163 IPA：JVN iPedia 脆弱性対策情報データベース https://jvndb.jvn.jp/index.html〔2026/7/13 確認〕
※ 164 JPCERT/CC：https://www.jpcert.or.jp/〔2026/7/13 確認〕
※ 165 IPA：情報セキュリティ早期警戒パートナーシップガイドライン https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html〔2026/7/13 確認〕
※ 166 WebShell：Web サーバーに不正に設置され、第三者による遠隔操作を可能とする不正プログラム。
※ 167 トレンドマイクロ社：2025 年の国内セキュリティインシデントを振り返る https://www.trendmicro.com/ja_jp/jp-security/25/l/securitytrend-20251211-01.html〔2026/7/3 確認〕
※ 168 e-Gov 法令検索 不正アクセス行為の禁止等に関する法律 https://laws.e-gov.go.jp/law/411AC0000000128〔2026/7/3 確認〕
※ 169 国家公安委員会、総務大臣、経済産業大臣：不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況 https://www.npsc.go.jp/hightech/260313.pdf〔2026/7/3 確認〕
※ 170 検挙事件数は、事件単位ごとに計上された数であり、一連の捜査で複数の犯罪を検挙した場合は1事件として計上されている。
※ 171 検挙件数では、1 事件で複数の区分の行為を検挙した場合は、それぞれの区分に重複して計上されている。
※ 172 NTT コミュニケーションズ株式会社：当社への不正アクセスによる情報流出の可能性について https://www.ntt.com/about-us/press-releases/news/article/2025/0305_2.html〔2026/7/3 確認〕
※ 173 株式会社ファーストリテイリング、株式会社ユニクロ、株式会社ジーユー：当社グループ情報システムへの不正アクセス発生に関するお詫びとご報告 https://www.fastretailing.com/jp/group/news/2503181100.html〔2026/7/3 確認〕
※ 174 株式会社すかいらーくホールディングス：当社テイクアウトサイトへの不正アクセス発生について https://corp.skylark.co.jp/Portals/0/images/news/press_release/2025/20250508_release.pdf〔2026/7/3 確認〕
株式会社すかいらーくホールディングス：当社が運営する「テイクアウトサイト」への不正アクセスによる個人情報漏えいの可能性に関するお詫びと調査結果に関するお知らせ https://corp.skylark.co.jp/Portals/0/images/news/press_release/2025/20250730_release.pdf〔2026/7/3 確認〕
※ 175 国立国会図書館：2025 年 11 月 11 日 開発中のシステムに対する不正アクセスの発生について（付・プレスリリース） https://www.ndl.go.jp/news/fy2025/251111_01〔2026/7/3 確認〕
※ 176 東京大学：本学研究室のサーバに対する不正アクセスに関するお知らせ https://www.u-tokyo.ac.jp/focus/ja/articles/z1201_00007.html〔2026/7/3 確認〕
※ 177-1 この定義は、「組織における内部不正防止ガイドライン」の「3. 用語の定義と関連する法律」（p.15）で定義されたものと同じである。
IPA：組織における内部不正防止ガイドライン https://www.ipa.go.jp/security/guide/insider.html〔2026/7/3 確認〕
※ 177-2 図 1-2-11 は IPA が株式会社東京商工リサーチに「不正持ち出し・盗難」の内訳を問い合わせた結果を基に、グラフを編集して掲載している。
※ 178 株式会社帝国データバンク：倒産速報 株式会社 UF ジャパン https://www.tdb.co.jp/report/bankruptcy/flash/5203/〔2026/7/3 確認〕
※ 179 みずほ信託銀行株式会社：お客さま情報の漏えいに関するお詫びとご報告について https://www.mizuho-tb.co.jp/company/release/pdf/20250424_2release_jp.pdf〔2026/7/3 確認〕
※ 180 日本経済新聞：ソフトバンク、顧客情報 14 万件流出の可能性 委託先から https://www.nikkei.com/article/DGXZQOUC118DX0R10C25A6000000/〔2026/7/3 確認〕
ソフトバンク株式会社：業務委託先企業による個人情報漏えいの可能性について https://www.softbank.jp/corp/news/press/sbkk/2025/20250611_01/〔2026/7/3 確認〕
※ 181 日経クロステック：TSMC、機密取得疑いで従業員処分 東京エレクトロン捜査報道 https://xtech.nikkei.com/atcl/nxt/column/18/00001/10982/〔2026/7/3 確認〕
※ 182 読売新聞：営業秘密持ち出し容疑、素材メーカー元社員2人を書類送検…退職後に起業の会社で利用画策か https://www.yomiuri.co.jp/national/20250801-OYT1T50112/〔2026/7/3 確認〕
※ 183 朝日新聞：3 万 7 千人分の個人情報を元職員が抜き取る 探偵が証拠写真を撮影 https://www.asahi.com/articles/AST9832ZNT98OXIE01YM.html〔2026/7/3 確認〕
公益財団法人堺市文化振興財団：【重要なお知らせ】元職員による個人データ漏えい事案の発生とお詫び https://www.sakai-bunshin.com/info/76769/〔2026/7/3 確認〕
※ 184 農林水産省：職員の個人情報の漏えい事案の発生について https://www.maff.go.jp/j/press/kanbo/keiri/260123.html〔2026/7/3 確認〕

※ 185 総務省：放送コンテンツ製作取引実態調査における情報の漏えい　https://www.soumu.go.jp/menu_news/s-news/01ryutsu04_02000246.html〔2026/7/3 確認〕
※ 186 株式会社ユナイテッドアローズ：【3/17 情報更新】お取引先様の個人情報漏えいに関するお詫びとご報告　https://www.united-arrows.co.jp/news/15175/〔2026/7/3 確認〕
※ 187 https://www.meti.go.jp/policy/netsecurity/UAaccessCMG.htm〔2026/7/3 確認〕
※ 188 https://www.ipa.go.jp/security/guide/insider.html〔2026/7/3 確認〕
※ 189 経済産業省：不正競争防止法の概要　https://www.meti.go.jp/policy/economy/chizai/chiteki/unfaircompetition_new.html〔2026/7/3 確認〕
※ 190 個人情報保護委員会：個人情報取扱事業者等が個人情報保護法に違反した場合、どのような措置が採られるのですか。　https://www.ppc.go.jp/all_faq_index/faq1-q11-1/〔2026/7/3 確認〕
※ 191 e-Gov 法令検索：刑法　https://laws.e-gov.go.jp/law/140AC0000000045〔2026/7/3 確認〕
※ 192 内閣府：重要経済安保情報の保護及び活用に関する法律（重要経済安保情報保護活用法）（令和 6 年法律第 27 号）　https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/hogokatsuyou.html〔2026/7/3 確認〕
※ 193 個人情報保護委員会：個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則 (EU) 2016/679（一般データ保護規則）　https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf〔2026/7/3 確認〕
※ 194 https://www.ipa.go.jp/security/guide/sme/about.html〔2026/7/3 確認〕
※ 195 金融庁：インターネット取引サービスへの不正アクセス・不正取引にご注意ください　https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html〔2026/6/11 確認〕
※ 196 https://www.ipa.go.jp/security/anshin/index.html〔2026/6/11 確認〕
※ 197 IPA：インターネットサービスへの不正ログインによる被害が増加中　https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20250828.html〔2026/6/11 確認〕
※ 198 警察庁：令和 7 年上半期におけるサイバー空間をめぐる脅威の情勢等について　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf〔2026/6/11 確認〕
※ 199 ESET, spol. s r.o.：ESET Threat Report H1 2025　https://www.welivesecurity.com/en/eset-research/eset-threat-report-h1-2025/〔2026/6/11 確認〕
※ 200 フィッシング対策協議会：緊急情報　楽天証券をかたるフィッシング（2025/04/01）　https://www.antiphishing.jp/news/alert/rakutensec_20250401.html〔2026/6/11 確認〕
※ 201 IPA：情報セキュリティ安心相談窓口の相談状況［2025 年第 3 四半期（7 月～ 9 月）］3. 相談事例　https://www.ipa.go.jp/security/anshin/reports/2025q3outline.html#section4〔2026/6/11 確認〕
※ 202 NCO：インターネットの安全・安心ハンドブック Ver5.10 第 5 章 パスワードの大切さを知り、通信の安全性を支える暗号化について学ぼう　https://security-portal.cyber.go.jp/guidance/pdf/handbook/handbook-05.pdf〔2026/6/11 確認〕
※ 203 https://www.ipa.go.jp/security/chocotto/〔2026/6/11 確認〕
※ 204 フィッシング耐性がある認証方式：リアルタイムフィッシング等に対抗するために、フィッシングサイトに認証情報を送らないように設計された認証方式。パスキーを使った認証では、パスキーを登録する際に、正規サイトの URL を併せて登録し、登録した正規サイトにのみ認証情報を送信する仕組みになっている。
※ 205 https://www.ipa.go.jp/security/anshin/attention/2024/mgdayori20241119.html〔2026/6/11 確認〕
※ 206 IPA：サポート詐欺の偽セキュリティ警告はどんなときに出るのか?　https://www.ipa.go.jp/security/anshin/attention/2023/mgdayori20240227.html〔2026/6/11 確認〕
※ 207 IPA：偽セキュリティ警告（サポート詐欺）対策特集ページ　https://www.ipa.go.jp/security/anshin/measures/fakealert.html〔2026/6/11 確認〕
※ 208 IPA：「システムの復元」の実施手順書　https://www.ipa.go.jp/security/anshin/ps6vr70000012u8x-att/000090642.pdf〔2026/6/11 確認〕
※ 209 https://www.zenginkyo.or.jp/hanzai/information/〔2026/6/11 確認〕
※ 210 警察庁：サイバー警察局便り「私はロボットではありません」偽画面に注意!　https://www.npa.go.jp/bureau/cyber/pdf/R7_Vol.7cpal.pdf〔2026/6/11 確認〕
※ 211 IPA：情報セキュリティ対策　https://www.ipa.go.jp/security/anshin/measures/index.html〔2026/6/11 確認〕
※ 212 IPA：サイバーセキュリティ 相談・届出窓口一覧　https://www.ipa.go.jp/security/support/soudan.html〔2026/6/11 確認〕
※ 213 読売新聞オンライン：運営法人の社長騙る人物から「SNSのグループ作って」とメール…指示受け5000万円送金、だまし取られる　https://www.yomiuri.co.jp/national/20251227-GYT1T00213/〔2026/6/11 確認〕
※ 214 読売新聞オンライン：「業務で大金が必要」とチャットで連絡、社長になりすました人物に現金8000万円だまし取られる…送金直後に本物の社長が帰社して被害判明　https://www.yomiuri.co.jp/national/20260107-GYT1T00142/〔2026/6/11 確認〕
※ 215 TBS NEWS DIG：社長からのメール…実は詐欺メールだった「社長名」のメールを経理担当社員が信じ込む　飯田市の会社が現金 2950 万円をだまし取られる被害　長野　https://newsdig.tbs.co.jp/articles/-/2387856〔2026/6/11 確認〕
※ 216 新潟日報：“偽物”の社長から従業員に送金指示…県内企業が 1900 万円被害　「ビジネスメール詐欺」県内で初めて被害確認　https://www.niigata-nippo.co.jp/articles/-/758217〔2026/6/11 確認〕
十日町タウン情報：松代総合開発株式会社 ビジネスメール詐欺で 1900 万円騙し取られる　https://tokamachi.yukiguni.town/l-news/227657.html〔2026/6/24 確認〕
※ 217 読売新聞オンライン：経営者になりすまし従業員だます「ビジネスメール詐欺」･･･ 三重・いなべで1000万円被害　https://www.yomiuri.co.jp/local/chubu/news/20260115-GYTNT00052/〔2026/6/11 確認〕
※ 218 朝日新聞：経営者かたる「ニセ社長詐欺」相次ぐ、岐阜の会社が 1 億円被害　https://www.asahi.com/articles/ASV1J2VGMV1JOHGB004M.html〔2026/6/11 確認〕
※ 219 読売新聞オンライン：会長なりすましメール、酒田観光物産協会2300万円詐欺被害…半日に60通「冷静に判断する余裕を失う」　https://www.yomiuri.co.jp/national/20260114-GYT1T00399/〔2026/6/11 確認〕
※ 220 毎日新聞：突然届く「社長」のメール　新手の詐欺増加　1 カ月で 6 億円超被害　https://mainichi.jp/articles/20260119/k00/00m/040/248000c〔2026/6/11 確認〕
※ 221 長崎新聞：社長を名乗る差出人からメール…佐世保の会社が1130万円被害、全国的に増える新手の詐欺　https://www.nagasaki-np.co.jp/kijis/?kijiid=6b1777c7783041cdbee55ec168cf9419〔2026/6/11 確認〕
※ 222 読売新聞オンライン：「LINEグループ作成を」と社長かたるメール、指示通りに送金したら…5000万円の詐欺被害　https://www.yomiuri.co.jp/national/20260203-GYT1T00598/〔2026/6/11 確認〕
※ 223 山形放送：山形県の「やまがた農業支援センター」で個人情報流出か―　顧客約 3 万 2000 人分　https://news.ntv.co.jp/n/ybc/category/society/yba7a6bab74dd84febbdc532f815523ffc〔2026/6/11 確認〕
※ 224 朝日新聞：山形大教員「サポート詐欺」にだまされる　「大きな音がして動転」　https://www.asahi.com/articles/AST5G30WZT5GUZHB00BM.html〔2026/6/11 確認〕
※ 225 読売新聞オンライン：協同組合がウイルス除去名目で7300万円詐取被害…滋賀県警発表、事務員がパソコン操作中　https://www.yomiuri.co.jp/local/kansai/news/20250809-OYO1T50076/〔2026/6/11 確認〕
※ 226 ITmedia NEWS：外国人材の個人情報、800 人分漏えいか　都の就労支援事業で　委託先・パソナ従業員が詐欺サイト操作　https://www.itmedia.co.jp/news/articles/2509/25/news098.html〔2026/6/11 確認〕
※ 227 Security NEXT：サポート詐欺で約 2.5 億円被害、PC 遠隔操作から不正送金 - 信和　https://www.security-next.com/180916〔2026/6/11 確認〕

第2章
サイバー空間を巡る動向

本章では最初に、政府が注力している能動的サイバー防御と、経済安全保障に関する取り組みを取り上げる。2025 年度は AI 技術の進展と社会への普及が進んだ一方、AI のリスクが顕在化し、攻撃者による AI の悪用が進んだ年であった。また、偽・誤情報の拡散が引き続き国際的な公共への脅威であったが、官民の偽・誤情報への対策が進展した年でもあった。そこで本章では、2024 年度に引き続き、AI と偽・誤情報の動向を取り上げる。

2.1 サイバー安全保障関連施策の状況

本節では、政府が特に注力しているサイバー安全保障関連施策について取り上げる。具体的には、能動的サイバー防御に関する取り組みと、経済安全保障に関する取り組みを紹介する。

2.1.1 能動的サイバー防御の実現に向けた取り組み

政府は、2022 年に閣議決定された「国家安全保障戦略※1」において、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるとの目標を掲げた。具体的には、能動的サイバー防御の導入のため、①官民連携の強化、②通信情報の利用、③攻撃者のサーバー等への侵入・無害化、④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）の発展的改組及びサイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置等の実現に向け検討を進めるとされた。本項では、これらの検討を実施した「サイバー安全保障分野での対応能力の向上に向けた有識者会議※2」により取りまとめられた「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※3」、及び同提言を踏まえて制定された「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※4」（以下、サイバー対処能力強化法）、「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※5」（以下、整備法）の概要、及び「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※6」について紹介する。

(1) 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

「国家安全保障戦略」に基づき新たな取り組みの実現に必要となる法制度の整備等の検討のため、「サイバー安全保障分野での対応能力の向上に向けた有識者会議」が立ち上げられ、2024 年 6 月から 11 月にかけて 4 回の全体会議、及び①官民連携の強化、②通信情報の利用、③アクセス・無害化をテーマとした計 9 回のテーマ別会合が開催された。

その結果、実現すべき具体的な方向性について、上記①～③に、及びそれぞれのテーマについて議論を行う中で明らかになった④横断的課題を加えて、「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」が 2024 年 11 月に取りまとめられた。

同提言に基づき、後述のサイバー対処能力強化法及び整備法が制定された。また、サイバーセキュリティ戦略本部は、2025 年 5 月、同提言等を踏まえ、「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※7」を決定し、現行制度下において喫緊に取り組むべき施策の方向性を取りまとめるとともに、改組後のサイバーセキュリティ戦略本部において 2025 年内を目途に新たな「サイバーセキュリティ戦略」を策定することとした。同決定で示された施策の方向性の概要は以下のとおりである。

- サイバーセキュリティに係る新たな司令塔機能の確立
- 巧妙化・高度化するサイバー攻撃に対する官民の対策・連携強化
- サイバーセキュリティを支える人的・技術的基盤の強化
- 緊密な国際連携を通じた我が国のプレゼンス強化

新たな司令塔機能の確立のため、2025 年 7 月 1 日には、NISC が発展的に改組され、サイバー安全保障も含め、官民を通じたサイバーセキュリティの確保に関する司令塔として、内閣サイバー官を長とする国家サイバー統括室（NCO：National Cybersecurity Office）が発足した※8。

各テーマの概要及び同提言の概要については、「情報セキュリティ白書 2025※9」の「3.1.1 (1) (a) 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」を参照されたい。

2025 年 12 月に閣議決定された新たな「サイバーセキュリティ戦略※10」については、本白書の「3.1.1 (1)『サイバーセキュリティ戦略』に基づく取り組み」を参照されたい。

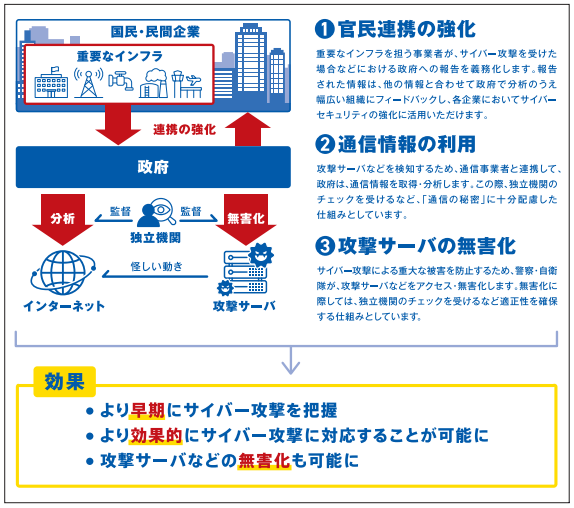
(2) サイバー対処能力強化法及び整備法

「国家安全保障戦略」及び前述の提言を踏まえて 2025 年 2 月、サイバー対処能力強化法案及び整備法案が閣議決定され、同年 5 月に成立し※11、同月、サイバー対処能力強化法及び整備法として公布された※12。

両法律の制定の背景としては、上述のとおり「国家安全保障戦略」において能動的サイバー防御の導入に向けた検討が閣議決定されたことに加え、IT 系システムの侵害、有事に備えた重要インフラ等への侵入、機微情報の窃取等のサイバー安全保障に関わる攻撃が巧妙化・深刻化するとともに、サイバー攻撃関連通信や被害数が年々増加傾向にあり、質・量両面でサイバー攻撃の脅威が増大していること、欧米主要国が官民連携や通信情報の利用、アクセス・無害化について先行した取り組みを行っていることが挙げられる※12。そこで、国民生活や経済活動の基盤及び国家及び国民の安全をサイバー攻撃から守るべく、欧米主要国における取り組みも参考に、能動的サイバー防御を実施する体制を整備するため、両法律が制定された。

サイバー対処能力強化法は①官民連携の強化、②通信情報の利用、③分析情報・脆弱性情報の提供等を規定し、整備法は④アクセス・無害化措置、⑤組織・体制整備等を規定（関係法律の改正）している。図 2-1-1 は、両法律により実現する能動的サイバー防御のポイントを示す図である。

サイバー対処能力強化法及び整備法における①～⑤に係る規定の概要は以下のとおりである。内容が広範にわたるため、詳細については内閣官房の説明資料等※14及び「情報セキュリティ白書 2025」の「3.1.1 (1) (b) サイバー対処能力強化法及び整備法」を参照されたい。



■図 2-1-1　能動的サイバー防御のポイント
（出典）内閣官房「みんなで備えよう。新・サイバー防御、はじまる。※13」

①官民連携の強化
- 特別社会基盤事業者※15 によるインシデント報告等
- 情報共有・対策のための協議会の設置
- 電子計算機の使用者に対する情報共有
- 脆弱性対応の強化等
- 罰則の整備

②通信情報の利用
- 特別社会基盤事業者との協定（同意）に基づく通信情報の取得
- （同意によらない）通信情報の取得
- 自動的な方法による機械的情報の選別の実施
- 独立機関による事前審査・継続的検査
- 罰則の整備

③分析情報・脆弱性情報の提供等

④アクセス・無害化措置
- 警察によるアクセス・無害化措置（警察官職務執行法の改正）
- 防衛省・自衛隊によるアクセス・無害化措置（自衛隊法の改正）

⑤組織・体制整備等（関係法律の改正）
- 政府を挙げた取り組みを推進するための体制整備

サイバー対処能力強化法及び整備法は、一部を除き、公布の日（2025 年 5 月 23 日）から起算して 1 年 6 ヵ月以内（サイバー対処能力強化法のうち、サイバー通信情報監理委員会は 2026 年4月に設置済、特定重要電子計算機の届出義務開始は公布日から 1 年 6 ヵ月以内、通信情報の利用については 2 年 6 ヵ月以内、整備法のうち、サイバーセキュリティ戦略本部の改組及び内閣サイバー

官の設置は 2025 年 7 月施行済）で、政令で定める日から施行される。

(3) 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

政府は、サイバー対処能力強化法に基づき、重要電子計算機に対する特定不正行為による被害防止のための基本的な方針案や法施行その他必要な事項について意見を聴くため、「サイバー対処能力強化法の施行等に関する有識者会議」を設置し、2025 年 9 月から 12 月にかけて 4 回の会合を開催した※16。その検討結果を踏まえ、サイバー対処能力強化法第 3 条に基づき 2025 年 12 月に「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」が閣議決定された。同方針は、法に基づく各般の施策を実施することにより、情報の収集、情報の整理・分析、及び情報の提供を抜本的に強化するものであり、以下の章で構成されている。

①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に関する基本的な事項
②当事者協定の締結に関する基本的な事項
③通信情報保有機関における通信情報の取り扱いに関する基本的な事項
④情報の整理及び分析に関する基本的な事項
⑤総合整理分析情報の提供に関する基本的な事項
⑥協議会の組織に関する基本的な事項
⑦その他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に関し必要な事項

同方針の概要を以下に示す。

①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に関する基本的な事項
- 法に基づく各般の施策実施により、サイバーセキュリティの対策に資する情報の収集、収集した情報の整理・分析、及び整理・分析を踏まえて作成した情報の提供の各機能を抜本的に強化する。
- NCO による総合調整のもと、政府内の緊密な連携協力を進めるとともに、特別社会基盤事業者はもとより、中小企業も含めて広く様々な事業者との官民連携、同盟国・同志国等の関係機関・団体との連携を強化する。
- 法の適用にあたっては、法目的を達成するために必要な最小限度において厳格にその権限を行使する。関連業務に携わる通信情報保有機関のすべての関係職員は、通信の秘密を尊重しつつ厳格にその業務に取り組むことを徹底する。
- 重要電子計算機や特定重要電子計算機の定義を明確化する。特に特定重要電子計算機は、事業者等との協議を経て、特別社会基盤事業者の業態別に明確化する。
- IP アドレス等通信履歴に係る情報等の機械的情報は、分析に必要な情報を適切に含めるとともに、意思疎通の本質的な内容が理解できないものに限定する。

②当事者協定の締結に関する基本的な事項
- 当事者協定の制度は、特別社会基盤事業者等におけるサイバーセキュリティの確保のための官民相互の協力の推進に資する枠組みであることから、内閣府は、本制度が有効に活用されるよう、特別社会基盤事業者等との間で丁寧に協議を行いつつ、当事者協定の締結を進める。
- 重要性の高い特別社会基盤事業者等から締結に向けた協議を求める。
- 締結が事実上の強制とならないよう配慮し、締結しなかった者に対して不当に不利益な取り扱いをしない。
- 分析の対象となる選別後通信情報を例外的に「他目的利用」する際は、内閣府は、協定当事者から個別に具体的かつ明確な同意を得て、その範囲内で選別後通信情報を他目的利用する。なお、本法に基づく他目的利用には犯罪捜査のための選別後通信情報の利用は含まれ得ない。

③通信情報保有機関※17 における通信情報の取り扱いに関する基本的な事項
- 通信情報保有機関は、通信の秘密等に十分に配慮して制度の適正な運用を図る。
- 内閣府及び関係行政機関は、必要なシステム・設備の整備を進め、運用に係る職員の確保・育成を図る。
- 電気通信事業者の協力による負担が過度にならないよう配慮し回避策を検討する。
- 通信情報保有機関では、透明性の向上、安全管理措置の遵守、提供用選別後情報の活用、個人情報保護法等の法令遵守に取り組む。また、関係職員は通信情報の利用に際し、法に規定する規律について厳格に遵守する。
- サイバー通信情報監理委員会を設置し、必要な規模の体制を構築し、法律に基づき所掌事務を実施

する。また、適切に国会への報告を行い、内容の充実に努める。

④情報の整理及び分析に関する基本的な事項

- 内閣府は、法の規定に基づき収集した情報等について、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に有効に活用されるよう、総合的かつ業種横断的に整理及び分析を実施する。
- 特定重要電子計算機の届出は脆弱性情報の提供に活用するため、個別事業者向けの専用設計品等は不要。
- 特定侵害事象等の報告は、対象範囲を明確化し、タイミングに即して過度な負担とならないよう設定する。また、報告窓口の一元化について調整を進める。
- 総合整理分析情報は、用途・場面、閲読者等に応じて内容等を適切にすること、また政府だからこそ取得や整理・分析が可能な情報に基づく情報、受け手の具体的行動につながる情報の作成に努める。
- 総合整理分析情報を加工して選別後通信情報を含まない提供用の、インフラ事業者等向けに秘密を含まない周知等用の総合整理分析情報を作成する。

⑤総合整理分析情報の提供に関する基本的な事項

- 総合整理分析情報等の提供先と内容は表 2-1-1 のとおり。
- ワンボイスで機関ごとに差異が生じないよう、関係行政機関等の間で緊密に連携を図る。
- 政府は、適切なタイミングで積極的に情報提供するよう努め、情報提供の在り方も不断に改善を図る。情報提供した事業者等へ積極的にフィードバック等を行い、情報共有がより活発になるよう取り組むとともに、その権利利益保護に配慮する。
- 政府は、通信の当事者その他の者の権利利益の保護に配慮するとともに、選別後通信情報の取り扱いについては、組織的、物理的、技術的な安全管理措置を講ずる。

⑥協議会の組織に関する基本的な事項

- 重要電子計算機に対する特定不正行為による被害防止のため、協議会を組織する。協議会では、被害防止情報の提供、被害防止に資する情報の共有・協議、演習や初動対応支援等の機会提供を行う。
- 柔軟な運営に取り組み、自発的な相互の情報提供・意見交換等を活性化させる。
- 専門家向けの技術情報に限らず、経営層の判断に必要な情報を適切なタイミングで積極的に提供する。
- 構成員との継続的なコミュニケーションを通じてニーズを把握し、それを踏まえた情報提供に取り組む。
- 被害防止の対策や情報を適正に管理するために必要な措置等について、構成員で協議を行う。
- 構成員以外の者にも、秘密を含まない情報の提供を行い、国内のサイバーセキュリティ強化を促す。情報提供した構成員等の権利利益保護に配慮する。

⑦その他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に関し必要な事項

- 施行後 3 年を目途として、特定侵害事象等の報告、通信情報の取得、当該通信情報の取り扱い等の

(1)行政機関等	内閣府は、行政機関が使用する重要電子計算機の被害発生の可能性を把握した、特別社会基盤事業者の役務提供に支障を及ぼすおそれがある、アクセス・無害化措置に資する等の場合には、行政機関等に対し対策や措置に必要となる総合整理分析情報を提供。
(2)外国の政府等	内閣府又は通信情報機関は、①法の規定による提供目的の制限に適合するかを個別かつ適切に判断するとともに、②外国の政府等が法に規定する情報の取扱いに係る適切な措置の実施を明示的に確認した上で、その必要な範囲で総合整理分析情報等を提供。
(3)協議会の構成員	内閣府は、例えば、サイバーの専門家が求める技術情報に限らず、経営層の判断に必要となる攻撃の目的や背景等に関する情報などの提供用総合整理分析情報等を適切なタイミングで積極的に提供。構成員のニーズも踏まえた形式・内容での情報提供に取り組んでいく。
(4)特別社会基盤事業者	内閣府から情報提供を受けた特別社会基盤事業者の所管省庁は、特別社会基盤事業者に対して、攻撃技術情報などの周知等用総合整理分析情報を積極的に提供。
(5)電子計算機を使用する者	内閣府は、重要電子計算機の使用者に限らず、特定不正行為に用いられるおそれのある電子計算機の使用者等に対し、周知等用総合整理分析情報を提供。例えば、協議会の構成員に対して提供するような脅威情報に必要な加工を行った上で、情報提供を行う。
(6)電子計算機等供給者	内閣府又は電子計算機等供給者の所管省庁は、必要に応じて、公表前の脆弱性情報を重要電子計算機の供給者に対して迅速に提供。脆弱性情報は、その秘匿性や緊急性も踏まえ、適切な情報提供・情報管理に努めていく。脆弱性関連情報の取扱いについては、政府が本法に基づく官民連携に係る事務を着実かつ効果的に実施できるよう、関係する告示・ガイドラインの必要な見直しを行う。

■表 2-1-1　総合整理分析情報の提供先と提供内容
(出典)内閣府政策統括官(サイバー安全保障担当)「サイバー対処能力強化法に基づく基本方針の概要※18」

状況を検討し、必要があれば所要の措置を講ずる。
- 政府は、不断に取り組み状況の検証・評価を行い、それに伴う制度の見直しを適時に行う。
- 関係省庁や関係機関は、緊密な連絡・協力が不可欠であり、経済安全保障推進法や個人情報保護法、他関連業法を所管する省庁との連携、合理的な制度設計・運用に努める。
- 内閣府、国の行政機関、IPA、国立研究開発法人情報通信研究機構（NICT：National Institute of Information and Communications Technology）その他関係者は、法その他の法令、基本方針に基づき、相互に連絡・協力する。また、内閣府の事務はNCOの総合調整のもとで実施する。
- 能動的サイバー防御を実現するために必要な措置とされた「アクセス・無害化措置」については、サイバー安全保障担当大臣のもと、NCOが総合調整機能を発揮し、警察及び防衛省・自衛隊が個別のアクセス・無害化措置を執行する。
- 関係行政機関は、平素から必要な連携を図り、アクセス・無害化措置の実施に資すると認められる情報を、情報保全にも配慮しつつ、効果的かつ適正にアクセス・無害化措置の実施に関わる行政機関に提供する。

2.1.2 経済安全保障関連施策の状況

2024年5月に「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律[※19]」（以下、経済安全保障推進法）が全面的に施行されるとともに、「重要経済安保情報の保護及び活用に関する法律[※20]」（以下、重要経済安保情報保護活用法）が公布され、同法の施行に向けた準備が進められた。本項では、両法の概要と2025年度の主な動きを紹介する。

(1) 経済安全保障推進法

経済安全保障推進法に基づき、①重要物資の安定的な供給の確保に関する制度、②基幹インフラ役務の安定的な提供の確保に関する制度、③先端的な重要技術の開発支援に関する制度、④特許出願の非公開に関する制度の四つの制度が創設された。

このうち、①に関しては、2026年4月時点で16の特定重要物資について145件の供給確保計画が認定されている[※21]。

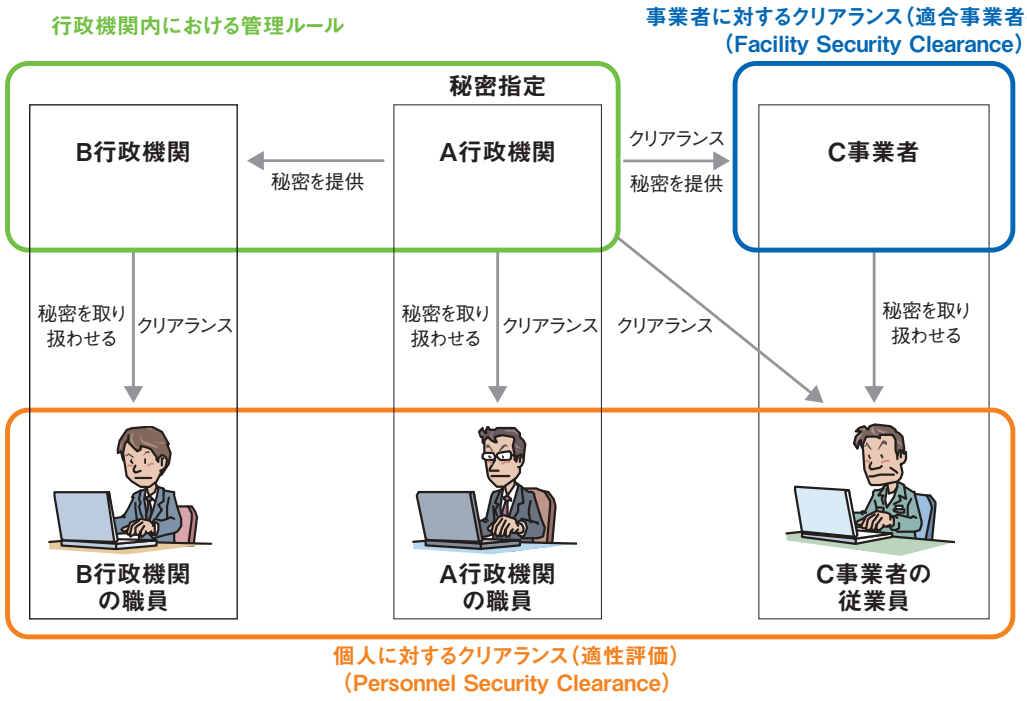
また、②に関して、制度の対象事業（電気、ガス、石油、水道、鉄道、貨物自動車運送、外航貨物、航空、空港、電気通信、放送、郵便、金融、クレジットカード）は、港湾運送事業が加わり15分野になった（2025年4月）。更に2026年6月には医療分野を追加する改正法が公布され、公布日から起算して1年6ヵ月を超えない範囲内において政令で定める日から施行される[※22]。

2025年11月より、経済安全保障推進法の改正に向けて「経済安全保障法制に関する有識者会議[※23]」が検討を行い、2026年1月に「経済安全保障の更なる推進に向けた提言[※24-1]」を公表した。この提言を踏まえた「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律及び株式会社国際協力銀行法の一部を改正する法律案」が2026年3月に閣議決定され、第221回国会（令和8年特別会）に提出され、同年6月に成立・公布された[※24-2]。同改正法では、①重要な物資の安定的な供給の確保、②基幹インフラ役務の安定的な提供の確保、③先端的な重要技術の開発支援、④重要な海外事業の促進、⑤総合的な経済安全保障シンクタンク及び官民協議会の創設という五つの対応を講じるとされた。

(2) 重要経済安保情報保護活用法

安全保障の概念が、防衛や外交という伝統的な領域から経済・技術の分野に大きく拡大し、軍事技術・非軍事技術の境目も曖昧となっている中、国家安全保障のための情報に関する能力の強化は、一層重要になっており、経済安全保障分野においても、厳しい安全保障環境を踏まえた情報漏えいのリスクに万全を期すべく、我が国の情報保全の更なる強化を図る必要がある。そこで、2024年1月に公表された「経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議」の「最終とりまとめ[※25]」により、経済安全保障分野におけるセキュリティ・クリアランス制度[※26]の創設が提言された。セキュリティ・クリアランス制度とは、国家における情報保全措置の一環として、政府が保有する安全保障上重要な情報として指定された情報にアクセスする必要がある者（政府職員及び必要に応じ民間事業者等の従業者）に対して政府による調査を実施し、当該者の信頼性を確認した上でアクセスを認める制度である。これを受けて、2024年5月に重要経済安保情報保護活用法が成立し[※27]、同月公布され、2025年5月に施行された。同法に基づく重要経済安保情報の提供の流れの概略図を図2-1-2（次ページ）に示す。

同法は、①重要経済安保情報の指定、②重要経済



■図 2-1-2　重要経済安保情報の提供の流れとそれに対する管理ルールのイメージ
（出典）内閣府「適性評価と重要経済安保情報の提供の流れ※28」を基に IPA が編集

安保情報の提供、③重要経済安保情報の取扱者の制限、④適性評価、⑤罰則等を定めている※29。

2025 年 1 月、重要経済安保情報保護活用法第 18 条第 1 項に基づき、「重要経済安保情報の指定及びその解除、適性評価の実施並びに適合事業者の認定に関し、統一的な運用を図るための基準※30」が閣議決定された。同基準は、重要経済安保情報の指定及び解除等、適性評価の実施、適合事業者の認定等について、具体的な判断基準や手順を規定している。また、同基準では、同法の運用にあたって留意すべき事項として、拡張解釈の禁止並びに基本的人権及び報道・取材の自由の尊重、公文書管理法及び情報公開法の適正な運用が規定された。また、適性評価の実施にあたっての基本的考え方として、基本的な人権の尊重、プライバシーの保護、「特定秘密の保護に関する法律」で定められた七つの調査事項以外の調査の禁止、適性評価の結果の目的外利用の禁止が規定された。

更に、2025 年 5 月には、各行政機関が定める重要経済安保情報保護規程、重要経済安保情報に係る通報窓口一覧、適性評価に係る苦情受理窓口・相談窓口一覧、行政機関や適合事業者向けのガイドライン、適性評価に関する Q&A が公開された※31。

また、同法の適正な運用を確保するため、同法の施行日より、独立公文書管理監が独立した公正な立場から検証及び監察を行っている※32。検証・監察の結果、2026 年 3 月、是正の求め等（是正の求め 3 件、うち、重要経済安保情報保護活用法関係は 1 件）を行った※33。

2026 年 6 月には、同法の規定に基づき、重要経済安保情報の指定及びその解除、適性評価の実施並びに適合事業者の認定の状況について国会に報告された※34。

(3) 関連施策

2025 年は、経済安全保障推進法を着実に執行するため、関連する複数の施策が実施された。

(a)「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」再改訂

経済産業省では、経済安全保障に関する産業・技術基盤を強化するための取り組みの方向性と内容を、2023 年 10 月に「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」として取りまとめ、官民での戦略的対話を行ってきた。2024 年 5 月には同アクションプランを改訂したが、その後、我が国を取り巻く経済安全保障環境が大きく変化したことを踏まえ、2025 年 5 月、同アクションプランを再改訂した※35。同アクションプランの再改訂の概要※36 を以下に示す。

同アクションプランは、大国が、物資、技術、人材、資金、データ等の「囲い込み」と「自給自足」を通じて、先端技術だけでなく、伝統的な製造業まで対象にした国家戦略を加速している新たな国際環境下での産業・

技術基盤強化に向け、以下の方向性をもって再改訂された。

- 投資、人材、技術を呼び込むための環境整備を拡大し、国内産業・技術基盤を強化
- 「新たな製造業=（製造業X）」を創出すべく、物資・技術だけでなく、金融、物流、データ等のサービスを含め、バリューチェーン全体を射程にとらえた取り組みを強化
- 同志国間、官民・民間同士の力を有機的につなぐための「プラットフォーム」を作成

また、我が国の自律性・不可欠性確保のため、「3つのP」（産業支援策（Promotion）、産業防衛策（Protection）、国際連携・官民対話（Partnership））を有機的に連携させるべく、以下のように取り組みのフレームワークをアップデートするものとされた。

- 官民連携のもと、新たな国際環境がもたらす経済安全保障上の「脅威・リスク」を分析するとともに、我が国にとっての「機会」を抽出すべく、①我が国が優位性を有する技術の把握、他国の関心も踏まえた技術分析の継続、②物資を超え、サプライチェーン分析から産業バリューチェーン分析に拡大、③シナリオ分析に加え、各国との経済安全保障協力を進めるため、地域情勢分析を追加する等、分析の射程を拡大する。
- 自律性・不可欠性確保の観点から、重要な物資・技術・サービス等を特定した上で、官民連携と同志国や影響力を増すグローバルサウス諸国等との国際連携のもと、バリューチェーンを強化する。
  - 物資・技術アプローチ
    「破壊的技術革新が進む領域」「我が国が優位性を持つ領域」「対外依存の領域」の考えのもと、重要な物資、技術、サービス等を特定していく。
  - 産業バリューチェーンアプローチ
    研究開発、調達、生産、販売のバリューチェーン全体、各層ごとに対応策を補強する。物資の「サプライチェーン」に加えて、知財、ソフトウェア、更に物流、金融、データ等のサービスにも注目する。
  - 官民対話
    官民での脅威リスク認識、対応策に関する対話を深化させる。
  - 地域戦略
    我が国の自律性・不可欠性確保に向けた各国・地域との相互依存関係・補完関係を構築するため、例えば、日本のシーレーン確保のための要衝国・地域との連携強化や経済安全保障の観点からの戦略的地域枠組み等を検討する。

(b)「経済安全保障経営ガイドライン」取りまとめ

企業が経済安全保障対応を進めていく中で、経済安全保障上のリスクに起因する損失を中長期的に抑え、企業価値の維持・向上も見据えた経営戦略を考える上の推奨事項として、2026年1月、経済産業省が「経済安全保障経営ガイドライン（第1版）※37」を取りまとめた。

本ガイドラインでは、経営層が以下の三つの原則を認識し、主体的に対策を進めることが重要としている。

- 自社ビジネスを正確に把握し、リスクシナリオを策定する。
- 経済安全保障への対応を単なるコストではなく、投資ととらえる。
- マルチステークホルダーとの対話を欠かさない。

また、企業の経済安全保障への対応は多岐にわたるが、本ガイドラインでは、「自律性確保の取組」「不可欠性確保の取組」、及び「経済安全保障対応におけるガバナンス強化」の3点について、個社の取り組みとして推奨される事項を記載している。

(c)「経済安全保障グローバルフォーラム・ウィークス」開催

経済安全保障分野における国内外の連携を強化するため、経済産業省では、2025年9月末から12月にかけて、政府・独立行政法人・民間シンクタンク等が協調して経済安全保障に関する国際イベントを開催する「経済安全保障グローバルフォーラム・ウィークス※38」を実施した。具体的には、会議・展示会、国際フォーラム、セミナー、シンポジウム等が多数開催された。

(d)「技術流出対策ガイダンス」策定

産業界が技術流出対策を講じる際の一助となることを目的に、2025年5月、経済産業省が「技術流出対策ガイダンス第1版」を公表した。その後、2026年1月に公表された「経済安全保障経営ガイドライン」と足並みを揃え、「各章で共通する技術流出対策」「人を通じた技術流出への対策」等について内容を大幅に充実させるとともに、企業における国内外との「共同研究」や調達時の「すり合わせ」に伴う技術流出対策に関するニーズを踏まえ、これらの内容の記述を新設した「技術流出対策ガイダンス第2版※39」を2026年4月に策定した。

2.2 AIの安全性確保の取り組み

本白書が執筆された約 10 年前を振り返ると、囲碁 AI（Artificial Intelligence：人工知能）の AlphaGo がプロ棋士に相次いで勝利し、AI の可能性を世界に印象付けた※40。2022 年には、OpenAI, Inc.（以下、OpenAI 社）が ChatGPT を公表し、専門知識を持たない一般利用者でも、自然言語による対話を通じて生成 AI を容易に利用できるようになった※41。現在では、多くの人が AI による社会の変化を実感しているところだろう。

AI の利活用が広がる一方、IPA による「情報セキュリティ10大脅威2026※42」に「AIの利用をめぐるサイバーリスク」が初めて選ばれた。急速に発展し社会に普及する AI のリスクが、現実の脅威として認知され始めていると言えよう。本節では AI の発展とリスク、安全性確保の取り組み等について、2025 年度以降の動向や事例を中心に、2026 年 5 月上旬時点までに公表された情報に基づいて概観する。

2.2.1 AIの発展と社会への普及

AI の技術は、古くは 1950 年代の研究から発展してきたと言える。その歴史的な概観については「情報セキュリティ白書 2025」の「2.1.1 (1) 20 世紀中の AI 技術」や「2.1.1 (2) 機械学習とディープラーニングで発展した AI」を参照いただきたい。ここでは、直近の生成 AI の発展や AI エージェントの実用化に着目する。

(1) 生成 AI の発展

最初に AI の基礎に関して簡潔に触れると、AI の動作は、学習（訓練）と推論に分けられる。学習とは、大量のデータから傾向や関係性を見いだし、未知の入力に対しても適切に応答できるようにする過程である。推論とは、実際の入力に対して、学習した情報に基づき具体的な出力を導く過程である。こうした学習と推論を担う仕組みは AI モデルと呼ばれ、学習によって得られた情報をパラメーターとして内部に保持している。

生成 AI（Generative AI）とは、「文章、画像、プログラム等を生成できる AI モデルにもとづく AI の総称※43」であり、自然な文章を生成する LLM（Large Language Model：大規模言語モデル）はその代表例である。LLM の学習では、AI モデルのパラメーター数、学習に用いるデータ量、そして学習に使用される計算量を増やす程、応答の精度が向上するスケーリング則※44 が知られている。この経験則に沿って LLM は規模を拡大しながら発展してきた。ただし、その基本的な仕組みは、学習した膨大なテキストに基づいて、与えられた文章に続く語句を統計的に予測するものであり、「確率的オウム」とすら呼ばれた※45。特に、計算問題等、論理的思考を要する質問は苦手とされてきた。

こうした課題に対応するため、複雑な問題を分解し、段階的に推論を行う推論モデル（Reasoning Model）の開発が進んでいる※46。特に、最終的な回答までの中間的な推論のステップを明示的に扱う CoT（Chain of Thought：思考の連鎖）は、論理的な推論を要する質問への回答精度を高める手法として知られている※47。推論モデルの開発には、2024 年 9 月に発表された OpenAI o1-preview を始め、各社が参入している※48。2026 年 4 月には、OpenAI 社、Google LLC（以下、Google 社）、Anthropic PBC（以下、Anthropic 社）の各 AI モデルが東京大学の入試問題における大半の科類で人間の合格最高点を上回り、一部の AI モデルは数学で満点を記録したと報告された※49。このように推論モデルの登場以降、LLM が苦手とされていた推論能力にも大幅な向上が認められる。

生成 AI の発展は、LLM による対話だけでなく、画像や動画の生成等でも進んでいる。例えば、2025 年 8 月に Google 社が発表した Nano Banana※50 は、単に画像を生成するだけでなく、対話形式で物体の消去等細かい修正を可能にした。動画に関しても、2025 年後半に登場した OpenAI 社の Sora 2※51 や Google 社の Veo 3.1※52 は、利用者が入力した写真を参考に、人物の動画を生成できるようになった。

更に、テキストや画像、動画等異なる種類のデータを統合的に扱うマルチモーダル AI も普及してきている。例えば、Google 社は音声による AI との対話に加え、スマートフォン等の画面共有やカメラを使った動画による対話機能の提供を 2025 年 4 月に開始した※53。また、Microsoft Corporation（以下、Microsoft 社）は Windows のデスクトップ画面を AI と共有して対話する機能を 2025 年 7 月から提供しており※54、マルチモーダル AI の発展が人間にとってより自然でコミュニケーションに使いやすい AI を実現しつつあると言えよう。

(2) AI エージェントの実用化

自然な回答やコンテンツ生成を行う AI は、単に質問に答えるだけでなく、人間の作業を代行する能力も高めている。AI エージェントと呼ばれるこうした AI は、LLM の高い推論能力を基盤として、自律的に計画を立案し、外部のシステムを操作しながら、与えられた目標に向かって一連の処理を実行する点を特徴としている※55。

2025 年以降、こうした AI エージェントの特徴を持つサービスが相次いで実用化されている。例えば、OpenAI 社の ChatGPT エージェントは、Web サイトの操作機能を備え、情報収集や分析からフォーム入力、予約等を一貫して実行できる AI エージェントとして 2025 年 7 月に登場した※56。また、Microsoft 社が提供する Microsoft 365 Copilot は、組織内のデータや業務システムと連携し、問い合わせ対応やデータ分析等の業務を支援する※57。Anthropic 社も、ユーザーの指示に沿って多様なデスクトップ業務を遂行する Claude Cowork を提供している※58。更にソフトウェア開発の分野では、GitHub, Inc. が提供する GitHub Copilot※59 や Anthropic 社の Claude Code※60 等、コード生成だけでなく、テストや修正を含む開発作業を自律的に実行する AI エージェントが登場している。このように AI エージェントは、日常生活から専門的な業務に至るまで幅広い領域で活用され、作業の効率化や高度化を推し進めている。

2.2.2 AIのリスク

AI の発展は幅広い恩恵をもたらすようになった一方で、特有のリスクも指摘されている。総務省と経済産業省が取りまとめた「AI 事業者ガイドライン※61」では、事業者が AI によるリスクの対策を検討できるよう、その体系的な分類案を示している（表 2-2-1）。

本項では、主に 2025 年度以降の事例や報告を、表 2-2-1 の中分類のリスク例に対応付けて紹介する。なお、以降で紹介するリスクは、表 2-2-1 のリスク例のすべてではないため、記載のないリスク例の説明については、「AI 事業者ガイドライン」を参照いただきたい。

(1) 学習及び入力段階のリスク

汚染されたデータで AI を学習させて誤動作を引き起こすデータポイズニング攻撃や、悪用可能な応答を AI から引き出すプロンプトインジェクション攻撃等、AI 特有の攻撃が知られている。これらの事例は、「2.2.4 (1) (a) AI の技術的特徴を狙った攻撃」で後述する。

大分類	中分類	リスク例
技術的リスク（＝主に AI システム特有のもの）	学習及び入力段階のリスク	データ汚染攻撃等の AI システムへの攻撃
	出力段階のリスク	バイアスのある出力、一貫性のない出力等
		ハルシネーション等による誤った出力
	事後対応段階のリスク	ブラックボックス化、判断に関する説明の不足
社会的リスク（＝既存のリスクが AI においても発生又は AI によって増幅するもの）	倫理・法に関するリスク	個人情報の不適切な取扱い等
		生命等に関わる事故の発生
		差別的出力
		過度な依存
		悪用
	経済活動に関するリスク	知的財産権等の侵害
		金銭的損失
		機密情報の流出
		労働者の失業
		データや利益の集中
		資格等の侵害
	情報空間に関するリスク	偽・誤情報等の流通・拡散
		民主主義への悪影響
		フィルターバブル及びエコーチェンバー現象
		多様性・包摂性の喪失
		バイアス等の再生成
	環境に関するリスク	エネルギー使用量及び環境の負荷

■表 2-2-1　AI によるリスク例の体系的な分類案
（出典）総務省、経済産業省「AI 事業者ガイドライン（第 1.2 版）別添（付属資料）※62」

(2) 出力段階のリスク

AIの出力には誤りが含まれる可能性があり、事実と異なることをもっともらしく回答する「ハルシネーション」のリスクがある。2025年12月8日に青森県沖で発生した地震では、気象庁から発表された津波警報や津波注意報が解除される前にもかかわらずAIによるWebサイトの要約が、「大津波警報・津波警報・津波注意報はすべて解除されており、発表されていません」と誤った内容を表示した※63。また、航空会社から送信されたメールの内容について、ユーザーの利用するAIが予約と異なる空港名に誤訳したり、オンラインチェックインの内容を誤って欠航と要約したりする事象が確認されている※64。

対話形式で回答を出力するAIとは異なり、AIエージェントでは、与えられた指示に応えるために周囲のシステムを自律的に操作する場合があるため、システムに対して意図しない操作をするリスクがある。ソフトウェアのコーディングを行うAIエージェントが、一連の作業中に特定のフォルダーの削除ではなく誤って最上位のフォルダーから削除してしまい多くのファイルが滅失した事例※65や、指示を無視してデータベースを削除した上に事実に反してロールバックができないと主張した事例※66が報じられている。

(3) 事後対応段階のリスク

AIの出力根拠が不明確な場合、出力が人材の採用、保険給付等の判断に用いられると、判断結果によって不利益を受けた本人が原因を把握しにくくなる。判断根拠の不透明さや説明不足が問題となり、訴訟に至るケースも見受けられる。

米国では、Workday, Inc.が提供する、AIを使った採用支援サービスが、連邦の差別禁止法に違反し、人種、年齢、障害に基づく不利益な影響を求職者に与えたとして、同社に対する訴訟が進行している。2025年5月、連邦地方裁判所は、年齢差別に関する請求について、原告と同様の立場の求職者が訴訟に参加できる暫定的な手続きを認めた※67。医療保険においても、UnitedHealth Group, Inc.に対する訴訟で、原告はAIを用いたツールの判断によって、加入者の治療に必要な保険給付が不当に拒否されたと主張している。2026年3月、連邦地方裁判所は、同社に対してAIを用いた給付判断プロセスに関する広範な文書の提出を命じた※68。

これらの事案は執筆時点でいずれも係争中であり、AIによる不当な判断や違法性が認定されたものではないが、AIによる判断に対する根拠や説明の不足が訴訟を含めたリスクにつながり得ることを示している。

(4) 倫理・法に関するリスク

AIの活用が、人の安全やプライバシー、主体的な判断等に深く関わる場面へ広がる中で、適切な管理や配慮を欠いた利用によって、倫理的・法的に保護されるべき利益が損なわれるおそれがある。本項では、AIの悪用、AIにおける個人情報の不適切な取り扱い、AIを用いたことによる事故、AIへの過度な依存について、実際の事例とリスクを述べる。

(a) 悪用

AIの悪用事例は、後述するサイバー攻撃(「2.2.4(2) AIを悪用したサイバー攻撃への対処」参照)や偽・誤情報の生成(「2.3 偽・誤情報対策の動向」参照)に加え、詐欺やわいせつ画像の作成と多岐にわたる。

詐欺に関しては、生成AIで実在する人物になりすます事例が相次いでいる。ビデオ会議に参加した偽のCFO(Chief Financial Officer:最高財務責任者)の送金指示で、ある海外の企業が約38億円を騙し取られた事件※69が2024年に発生し話題となった※70。日本企業に対しても2025年に詐欺グループがAIで合成された社長の音声で部下に電話をかけて送金の指示をした事例※71が報告されている。2026年3月には、他人になりすました人物が国内IT企業のオンライン面接を受けていたことが報じられた※72。国外においても生成AIを悪用してオンライン面接で他人になりすます事例が確認されており、米国連邦捜査局(FBI:Federal Bureau of Investigation)は北朝鮮のIT技術者が外貨獲得を目的として身分を偽装していることを指摘している※73。こうした事例の中には、公開された写真や動画だけでなく、SNS等を通じて対象の人物を偽の会議に誘導し、そこで音声や映像を取得することで、それらを元にしたAIによるリアルタイムの音声や動画生成でその対象者になりすます手口の存在も知られている※74。また、なりすまし以外にも、インド国内から日本人が狙われたサポート詐欺事件において、ポップアップウィンドウの作成や日本語への翻訳等に生成AIが使われたことが報告されている※75。

詐欺とは別のAIの悪用として、わいせつ画像の作成も後を絶たない。2025年4月、男女4人が画像生成AIで実在しない女性のわいせつな画像を作成し、インターネットオークションで販売した疑いにより、生成AIによるわいせつ物販売事件として全国で初めて逮捕された※76。また、実在する人物を対象として、特に児童の

学校行事や卒業アルバムの写真をAIで性的画像に加工する事例が相次いでいる※77。警察庁の調査によると、全国の都道府県警察が取り扱った事案数は2025年に114件となり、被害児童の同級生または同じ学校の生徒が行為者となっている事案が65件と過半数を占めた※75。この数値は若年層が容易にAIを悪用できてしまう状況を如実に表していると言えよう。AI-CSAM（Child Sexual Abuse Material：シーサム）とも呼ばれる生成AIを悪用した児童性的虐待コンテンツは、海外においても問題視されており、SNSに投稿した子供の写真が知らないうちにAIで性的画像に加工されてしまう危険性も指摘されている※78。

(b) 個人情報の不適切な取り扱い等

AIの利用に伴い、多様な個人情報が取得・分析される場面が増えている。特に、AIが個人識別やスコアリング、AIモデルの改善等のために、利用者や第三者のデータを収集する場合、本人への通知や同意、利用目的の明確化等が問題となり得る。

米国では、2025年12月、AI会議アシスタントを提供するFireflies.ai Corp.に対して、オンライン会議の参加者の生体音声の録音・分析・文字起こし・保存を行い、話者識別のための生体情報を本人の同意なく収集していたとして、訴訟が提起された※79。特に、Firefliesサービスのアカウントを持たず、利用規約にも同意していない会議参加者の音声も処理されたと主張されている。また、2026年1月には採用支援サービスを提供するEightfold AI Inc.に対し、AIを用いて本人の同意なしに個人情報を収集して応募者のプロフィールやランキングを作成し、雇用主に提供していたとして、応募者らが集団訴訟を提起したと報じられている。訴状によれば、応募書類に記載された以上の情報をSNS等から収集し、応募者の好みや適性についての推論やランク付けを行って雇用主に提供し、それらが候補者の絞り込みに使われたという※80。なお、いずれの事案も係争中であり、執筆時点で原告の主張が認定されたものではないことに留意が必要である。

(c) 生命等に関わる事故の発生

AIの動作や応答が生命に深刻な損害を与える可能性がある。米国では、Tesla, Inc.のオートパイロットシステムを搭載した自動車が、時速約100キロメートルで交差点に突進し、死亡事故を発生させた訴訟に関して、2025年8月、同社に事故の33%の責任があるとした陪審評決が下された。同社側はオートパイロットではなく無謀な運転手の責任だと主張したが、2026年2月には、連邦地裁が同社による評決取り消しの申し立てを退け、2億4,300万ドル（388億8,000万円※81）の評決を維持したと報じられている※82。また、対話型AIによる医療の助言が死亡事故につながったとして訴訟に発展した事例もある。米国で19歳の大学生がChatGPTの助言に従った薬物の過剰摂取により死亡したとして、2026年5月に遺族がOpenAI社等を提訴したと報じられている。訴状によると、ChatGPTが薬物や抗不安薬等を混ぜて飲むようアドバイスし、致死量となる摂取量を提案したという※83。ただし、この事件は執筆時点で係争中であり、原告の主張が認定されたものではない。

(d) 過度な依存

AIは、利用者の相談、調査、文章作成、意思決定等を支援する有用な手段となり得る一方で、利用者がAIとの対話やAIの回答に過度に依存することにより、精神的な不安定さが増幅されたり、自ら判断する力や自信が低下したりするリスクも指摘されている。

米国では、2025年8月、16歳の少年の自殺について、少年がChatGPTとの対話に深く依存し、同サービスが自殺念慮を助長した等として、少年の両親がOpenAI社等を提訴したと報じられた※84。また、同月には、ChatGPTとの対話に没頭していた男性が母親を殺害した後に自殺した事件について、AIとの対話が男性の被害妄想を悪化させた可能性があると報じられた※85。更に、2026年5月には、フロリダ州の銃乱射事件の遺族がChatGPTによる犯行助長を主張してOpenAI社を提訴した事例も報じられている※86。ただし、これらはいずれも執筆時点で訴訟または報道段階のものであり、AIとの法的因果関係が確定したものではない点には留意が必要である。

また、過度な依存による悪影響は、利用者の精神的な不安定さの増幅だけではない。2026年4月に米国心理学会が公表した研究では、AIに依存して業務を行うことは、認知能力そのものを低下させるとは限らない一方で、自らの独立した推論能力に対する自信や、成果物に対する主体感を損なう可能性があるとされている※87。このように、AIは利用者の作業や意思決定を支援する一方で、精神的健康や作業への自信・主体感に悪影響を及ぼすおそれがある。

(5) 経済活動に関するリスク

AIの活用に伴い、事業活動を支える情報・資産・

人材等を取り巻く環境が変化し、経済活動の安定性が揺らいだり、効率性がかえって損なわれたりするリスクがある。以下では、実際に発生した事例とリスクについて述べる。

(a) 知的財産権等の侵害

AI 利用に伴う知的財産権上のリスクのうち、特に著作権を巡る問題が顕在化している。以下で取り上げる各事例には、著作権以外の法的論点や複雑な事実関係を含むものもあるが、ここでは著作権上の論点に焦点を当てて紹介する。主な論点としては、以下の「(ア) AI の出力・表示が他者の著作権を侵害するリスク」「(イ) 他者の著作物を AI の学習に利用することを巡るリスク」「(ウ) AI 生成物の著作権保護・権利帰属を巡るリスク」が挙げられる。なお、著作権法の解釈は、個別具体的な事案に応じて司法により行われるべきものであることに留意されたい。

(ア) AI の出力・表示が他者の著作権を侵害するリスク

生成 AI は、利用者の指示に応じて画像、動画、文章、要約等を生成・表示するが、その内容が既存の著作物との関係で著作権侵害に該当するか否かが問題となる場合がある。

画像生成 AI に関しては、Disney Enterprises, Inc. 等複数のエンターテインメント企業が、AI による画像生成サービスを提供する Midjourney, Inc. を 2025 年 6 月に提訴した[※88]。この訴訟では、同社が著作権で保護されたキャラクターを無断で学習させ、利用者がこれらに類似する画像を生成できるようにしていると主張されている。

動画生成 AI についても、同様の懸念が示されている。2025 年 10 月には、OpenAI 社が提供を開始した動画生成 AI である Sora 2 を巡り、一般社団法人日本動画協会、公益社団法人日本漫画家協会、出版社 17 社が「生成 AI 時代の創作と権利のあり方に関する共同声明[※89]」を発表した。同声明では、Sora 2 により生成・公開された動画の中に、著名な創作物や表現への依拠性・類似性が強く疑われるものが散見されることに加え、権利者が明示的にオプトアウトしない限り著作物が生成・公開され得る仕組みへの懸念が示されている。また、「第二、第三の Sora 2」とも言うべき新たな生成 AI の登場が容易に予見されるとしている。その後、OpenAI 社は、Sora 2 の Web 版・アプリ版の提供を 2026 年 4 月 26 日に終了し、API についても同年 9 月 24 日に終了予定であると公表した[※90]。また、2026 年 3 月には、ByteDance（字节跳动有限公司）の動画生成 AI である Seedance 2.0 についても、著作権上の問題によりグローバル展開が一時停止したと報道された[※91]。

新聞記事に関する事例としては、株式会社日本経済新聞社と株式会社朝日新聞社による Perplexity AI, Inc. に対する訴訟がある。両社は、AI を利用した検索サービスにおいて新聞記事が無断で取得・保存・利用され、回答として要約が表示されたことが、著作権侵害等にあたると主張している。この事例は、画像や動画のように視覚的に既存作品と類似する出力だけでなく、記事本文の要約の表示についても、AI の出力・表示が著作権侵害の疑義を招き得ることを示している。なお、Perplexity AI, Inc. は 2026 年 5 月にこの訴訟に関して争う姿勢を示している[※92]。

一方、AI の出力が既存作品の「作風」の類似にとどまる場合には、直ちに著作権侵害にあたるとは限らない。2025 年 3 月には、OpenAI 社の GPT-4o による画像生成機能の提供をきっかけに、株式会社スタジオジブリの作風を模した画像が SNS 上に多数投稿され、著作権上の問題が議論された[※93]。一般論として、著作権法は創作的表現を保護するものであり、単に作風が似ているだけでは著作権侵害にあたるとは言えない。他方で、AI の出力について、特定の著作物との類似性及び依拠性が認められる場合には、著作権侵害となり得るとされる[※94]。

(イ) 他者の著作物を AI の学習に利用することを巡るリスク

AI を巡る著作権問題は、生成されたコンテンツだけでなく、AI の開発・学習段階にも及ぶ。書籍、画像、音楽、記事、映像等他者の著作物を、権利者の許諾なく AI の学習に利用することが著作権侵害にあたるのか、あるいは許容されるのかが問題となる。

米国では、作家らによる Anthropic 社を相手取った書籍の無断学習に関する集団訴訟が注目された。2025 年 6 月、カリフォルニア州連邦地裁は、同訴訟において、適法に取得された書籍の AI の学習への利用についてはフェアユースを認める一方、海賊版サイト等から書籍を取得・保管したことについては別途問題があると判断した。その後、この訴訟では、海賊版由来の書籍利用に関する請求を巡り、同社が和解のために 15 億ドル（2,400 億円）規模の支払いに合意したと報じられている[※95]。

この事例は、学習段階における著作物利用について、

単に「AI 学習であれば適法」または「無断学習は常に違法」と単純化できないことを示している。特に、利用目的、利用された著作物の性質、取得経路、保存・複製の態様、権利者の市場への影響等が、個別具体的に問題となる。なお、この訴訟は米国法上のフェアユースに関する判断を含むものであり、法体系や著作権法の規定が異なる日本法における結論と直ちに同一に扱うことはできない。日本においては、AI の学習等のニーズを背景に、2018 年の著作権法改正によって著作物の利用の円滑化を図るための柔軟な権利制限規定が整備された。文化庁は、こうしたAIと著作権に関する考え方や、リスク低減や権利保全のためのチェックリストとガイダンスを示している※96。

(ウ) AI 生成物の著作権保護・権利帰属を巡るリスク

AI を用いて生成されたコンテンツ自体に著作権が認められるのか、また、認められる場合に誰が権利を持つのかという問題がある。これは、他者の権利を侵害するリスクとは異なり、自社や利用者が AI で作成した成果物を十分に保護できるのかという観点から重要である。

AI 生成物を巡っては、「AI 自体が著作者となり得るか」という問題がしばしば取り上げられる。米国では、AI システムを単独の著作者として登録できるかが争われた訴訟において、2026 年 3 月、米国連邦最高裁判所が裁量上訴を認めなかった。これにより、人間の著作者性を必要とする米国著作権局及び下級審の判断が維持された※97。

実務上は、人間が道具として AI を利用した場合、どの程度の創作的関与があれば、その成果物が著作物として保護されるのかが重要である。文化庁が示した考え方※96 によれば、人間の「創作意図」と「創作的寄与」が認められる場合に、著作物として保護される余地がある。

日本国内では、2025 年 11 月、生成 AI で作成された画像を無断で複写したとして、神奈川県の男性が著作権法違反の疑いで摘発された事例が報道された※98。この事例は、AI 生成物の著作物性が問題となり得る事例として注目される一方、執筆時点では捜査段階であり、裁判所が AI 生成物の著作物性について判断を示したものではない点に留意が必要である。

(b) 労働者の失業

AI の発展により、人間の仕事内容や役割が変化し、労働者の負担軽減や生産性向上が期待できる一方で、雇用の減少につながるリスクも懸念されている。

大手テクノロジー企業を中心に、従業員の解雇や採用停止が相次いで報じられている。一例として、Salesforce, Inc. については、2025 年に 1,000 人以上の人員削減が報じられたほか、同社 CEO は、AI による生産性向上を背景に、同年中はエンジニアを新規採用しない趣旨の発言をしている※99。一方、2025 年 10 月に約 14,000 人の人員削減計画を発表した Amazon.com, Inc. は、その理由について、AI による代替ではなく、組織階層を減らして機動性を高めるためと説明している※100。このように、企業によって背景は異なり、また、その背景を公にしているかも異なるため、一概に AI が人員削減の原因とは言えない点には留意が必要である。

AI による失業の懸念の対象はテクノロジー企業に限らない。例えば、AI により生成された架空の女優が登場したことに対して、俳優らの間に仕事を奪われる懸念が広がっている。2025 年 9 月には全米映画俳優組合も、AI で生成された女優について、人間の俳優を失業させるとして批判する声明を発表している※101。

(c) 機密情報の流出

AI の学習や推論で扱われた機密情報が、セキュリティやガバナンスの不足によって、意図しない形で流出してしまうリスクがある。特に、攻撃者が機密情報の窃取を目的として、AI を狙った攻撃の事例については「2.2.4 (1) AI に係る安全性確保」の中で扱う。

(d) 低品質な生成物の氾濫

2025 年を象徴する言葉の一つとして、米国の辞書出版社である Merriam-Webster, Inc. は、「slop（スロップ）」を選定した※102。本来 slop は、泥水や残飯等を意味する英単語であるが、同社はこれを「一般に AI によって大量に生成される低品質なデジタルコンテンツ」と定義し、2025 年には、AI によって作成された低品質な動画や書籍、報告書等が広く流通したと指摘した。日本においても、生成 AI で作成した営業メールの大量送信が迷惑行為として報じられている※103。また、セキュリティの分野では、AI が生成した大量の低品質な脆弱性レポートが開発者や保守担当者の負担を増大させていることが指摘されている。これについては、「2.2.4 (3) AI を活用したサイバーセキュリティ確保」で後述する。このように、本来は利用者の作業効率向上が期待される AI であっても、その出力が低品質なまま大量に流通すると、受け手にとっては、かえって情報の選別や確認の負担を

増大させ、作業の妨げになる場合がある。

(6) 情報空間に関するリスク

AIによって情報の生成・流通・受容を巡る環境が変化し、人々の認識や社会の意思形成における偏りや歪みが助長されるリスクがある。以下では、実際に発生した事例とリスクについて述べる。

(a) 偽・誤情報等の流通・拡散

主に、生成AIによる精緻な画像や動画等が、事実と異なるにも関わらず、事実として人々に広まるリスクがあり、世論操作との関連も指摘されている。AIが生成したものに限定しない偽・誤情報の動向については、「2.3 偽・誤情報対策の動向」を参照いただきたい。ここでは、悪意ある生成・拡散ではなく、生成AIの利用に伴う確認不足により、誤った情報が報道機関等の信頼性のある媒体を通じて流通した事例を紹介する。

2025年5月、米国シカゴで2番目の規模を持つ新聞、シカゴ・サンタイムズ紙に存在しない書籍の書評が掲載された。記事は同紙ではなく別の配信会社が配信したもので、記事作成に関与した担当者が書籍リスト作成の段階から生成AIを使ったことを認めたという。同紙の関係者は、記事を作成した配信会社との契約を見直すとしている。一方で、SNS上では、なぜ編集者はこれを見落としていたのか、といった同紙への批判が相次いだ※104。この事例は、「2.2.2 (2) 出力段階のリスク」で述べたハルシネーションが、そのまま記事として多くの読者に届けられたために、誤情報の拡散という事態の悪化につながってしまった事例と言えよう。

日本国内では、一般社団法人共同通信社が、2025年10月に配信した記事の写真について、生成AIにより加工されたものと確認したとして取り消した。写真は、屋久島でのタヌキによるウミガメの食害に関する記事に掲載されたもので、もともとは監視カメラで撮影されていた。掲載された写真は、子ガメをくわえるタヌキの画像が鮮明になるよう生成AIで加工され、子ガメの向き等が変わっていた。同社の社内指針では、報道用の写真に生成AIを原則使用しないとしているが、取材で提供を受けた写真について確認をしていなかった※105。この事例は、生成AIによる加工が、画像の鮮明化を目的とする場合であっても、被写体の形状や位置関係等、事実認定に関わる要素を変化させれば、報道写真の真正性を損ない得ることを示している。

(b) 民主主義への悪影響

AIを使って個人の政治的意見を誘導することで、選挙干渉等の民主主義への悪影響が生じる可能性が指摘されている。これには、「2.2.2 (6) (a) 偽・誤情報等の流通・拡散」や「2.3 偽・誤情報対策の動向」で触れた偽・誤情報による世論操作だけでなく、対話型AIによる政治的な意見の説得も含まれている。2025年12月に学術誌Scienceに掲載されたオックスフォード大学の研究者らの論文※106では、4万人を超える英国人が参加する大規模な実験を行い、最大10ターンのLLMとの会話の前後で、英国の政治課題に対する意見への同意度をパーセンテージで測定した。LLMは、参加者を決められた意見に説得するよう、事前に指示されていた。LLMとの会話の平均時間は約9分であったが、条件によっては約12ポイントも同意度の変化があり、1ヵ月後にも説得効果の影響が確認された。この論文は、偽・誤情報に限らず対話型AIによる説得が政治的な意見に影響し得ることを実験的に示しており、AIが多方面から健全な民主主義に影響を及ぼす可能性が懸念される。

(c) 多様性・包摂性の喪失

社会全体で類似のAIが広く利用されるようになると、出力される表現や発想が一定の方向に収束し、多様な視点や、地域ごとの文化や考え方が反映されにくくなり、多様性や包摂性が失われる可能性がある。2025年4月にコーネル大学の研究チームが主要国際会議で発表した論文※107では、西洋中心のAIモデルが文章執筆を支援する提案を行った場合、文章の書き方や内容が西洋の規範に近づき、文化表現の差異を弱めることを実験的に示している。実験では米国とインドからの118人の参加者を対象として、決められたテーマに関する文章の執筆を求めた。その際、米国とインドの参加者を、それぞれ執筆中にAIからの文章の提案を受けるグループと受けないグループに分けている。論文では、執筆された文章の分析により、AIを用いることで米国とインドの参加者が書いた文章の間の類似度が高まること等が示されている。

(7) 環境に関するリスク

AIには、学習と推論を支える大規模な計算資源が必要であり、その多くはデータセンターに集約されている。そのため、AIの普及は、データセンターの電力需要、冷却水の使用、関連するCO2排出の増加等を通じて、環境負荷を高める可能性がある。

IEA（International Energy Agency：国際エネルギー機関）が2026年4月に公表した報告書※108によれば、2025年のデータセンターの電力需要は17%増加し、AI向けデータセンターの電力需要はそれを上回るペースで増加した。AIのタスクあたりの消費電力は低下しているものの、利用の増加等により、データセンター全体の電力消費は2030年までに倍増する見込みとされている。これは、個々の処理の効率化が進んでも、利用量の拡大によって総量としての電力需要が増加し得ることを示している。

CO2排出への影響も課題である。IEAは、データセンターの電力消費に伴うCO2排出量について、道路交通や航空と並んで2030年までに増加する数少ない分野の一つとし、2024年時点で約1億8,000万トンと推計している※109。この規模は、オランダの2023年の燃料燃焼由来CO2排出量である約1億1,200万トン※110の約1.6倍にあたる。ただし、前述の数値はデータセンターの排出量であり、AIが占める排出量はその一部である点には留意が必要である。

また、環境負荷の問題は、電力消費やCO2排出に限らない。AI向け計算基盤における冷却方式によっては水使用量の増加も課題となり得る。Microsoft社は、2025年の環境サステナビリティ報告書において、AIやクラウドサービス需要の拡大を背景に、データセンターの設計・建設・運用の見直しを進めていると説明している。同社は、冷却に水を使用しない新しいデータセンター設計により、施設あたり年間推定1億2,500万リットルの水使用を回避できるとしている※111。

2.2.3 AIの安全性とガバナンス

前項で例示したように、AIにはセキュリティに限らない幅広いリスクが指摘されており、AIの活用にあたっては、こうしたリスクの管理が欠かせない。本項ではAIの安全な活用に向けたAIセーフティやAIガバナンスを概説するとともに、関連する国際的な政策動向にも触れる。

(1) AIセーフティの概要

AIのリスクは以前からも指摘されており、2023年11月には英国でAIセーフティサミットが開催された※112。こうしたAIの安全性に対する国際的な意識の高まりを受けて、2024年2月、日本は英国、米国に次いで世界で3番目にAIセーフティ・インスティテュート（AISI：AI Safety Institute）を設立している。日本AISI（エイシー）は、総務省と経済産業省が取りまとめた「AI事業者ガイドライン」におけるAIに関連する各主体が取り組む事項※113のうち、「人間中心」「安全性」「公平性」「プライバシー保護」「セキュリティ確保」「透明性」をAIセーフティの重要要素として、これらが保たれた状態をAIセーフティと位置付けている※114。

日本AISIは、この定義に基づいてAIセーフティに関する評価手法の検討等を行っており、これらの重要要素に対する評価観点ガイド※115の作成等を行ってきた。2025年以降はAIセーフティの原則論から具体的な評価に向けた取り組みに重点を移しており、AIセーフティの評価ツールの開発と公開※116や、事業実証ワーキンググループの設立による産業界を交えたAIセーフティ評価の枠組みの整備※117等の活動を行っている※118。更に、日本AISIを含む世界各国のAISI相当機関から構成されるAISI国際ネットワーク（The International Network of AI Safety Institutes）は、名称を「The International Network for Advanced AI Measurement, Evaluation and Science」と改め、2026年2月にはAI評価のベストプラクティスに関する国際的な合意を公表し、各国と連携しながらAI評価に関する活動を進めている※119。

(2) AIガバナンスの概要

AIガバナンスとは、「AIの利活用によって生じるリスクをステークホルダーにとって受容可能な水準で管理しつつ、そこからもたらされる正のインパクト（便益）を最大化することを目的とする、ステークホルダーによる技術的、組織的、及び社会的システムの設計並びに運用※43」である。重要な点は、リスクを完全に排除することでも、リスクを避けるためにAIを使わないことでもなく、AIの便益とのバランスを踏まえてリスクを許容可能な水準で管理することである。この考え方は、一般的なリスクマネジメント※120とも共通している。AIセーフティの評価や対策は、AIガバナンスにおいてリスクを把握・管理する重要な要素と位置付けられる。

こうした内容を含めてAIの開発・提供・利用における必要な取り組みの基本的な考え方を示したのが「AI事業者ガイドライン」であり、我が国におけるAIガバナンスの包括的な手引きとなっている。「AI事業者ガイドライン」は継続的に更新されており、本白書の執筆時点で最新の第1.2版では、AIエージェントを含む技術動向の反映や、AIによるリスクと便益の記載の充実等が行われている※121。また、企業活動におけるAIガバナンスの実務マニュアルを含むガイドとして、日本AISIは、AI

による価値創出と責任ある活用の両立を支援するため、主に民間事業者が Chief AI Officer（CAIO：AI 統括責任者）を設置・運用する際の実務指針となる「Chief AI Officer ガイド※122」を提供している。

既に AI は国境を超えて利用されており、その適切な管理には一国だけでなく国際的な連携が欠かせない。日本は 2023 年に開催された G7 広島サミットの結果を踏まえ、AI に関する国際的なガバナンスの形成に向けた広島 AI プロセスを主導してきた。2025 年 2 月からは、広島 AI プロセスの国際行動規範に関する遵守状況を AI 開発企業等が自ら確認し報告する「報告枠組み」の運用が開始され、報告内容は Web サイトで公開されている※123。広島 AI プロセスは、G7 に限らず取り組みに賛同する国々や組織を増やしながら、国際的な枠組みの形成を進めている※124。

こうした国際的なガバナンスの取り組みと並行して、AI に関わる組織の管理体制や評価プロセスの標準化も進められている。2023 年 12 月に発行された ISO/IEC 42001 は、組織が AI に関するリスクと便益を継続的に管理するための AI マネジメントシステムの国際規格であり、2025 年 8 月にはこれに対応する日本産業規格 JIS Q 42001 が制定された※125。2025 年 7 月には、AI マネジメントシステムの認証機関に対する国際的な要求事項を定めた ISO/IEC 42006 が発行され※126、認証制度の国際的な整備が進められている。また、2025 年 5 月には AI システムの影響評価を定めた ISO/IEC 42005 も発行されている※127。更に、ISO/IEC の合同技術委員会と ISO の上層委員会である CASCO（Conformity Assessment Committee：適合性評価委員会）が共同して、AI システムに対する認証を含む適合性評価のハイレベル・フレームワークに関する ISO/IEC 42007 の開発を進めており※128、AI ガバナンスに関する標準化が活発に進められている。

(3) AI に関する国際的な政策動向

AI の急速な発展と社会実装の拡大を受け、各国・地域では、AI に関する制度整備や戦略策定が進められている。AI は、産業競争力を左右する一方、社会的リスクや安全保障上の課題も伴うため、各国・地域では、それぞれの産業基盤、制度設計、国際競争上の立場を踏まえた政策対応が進められている。以下では、米国、欧州、中国、日本における AI 政策の動向を概観する。なお、サイバーセキュリティの観点からの日本の政策に関しては「3.1 国内のサイバーセキュリティ政策の状況」を、米国、欧州、中国の政策に関しては「4.1.2 米国の政策」「4.1.3 欧州の政策」「4.1.4 中国の政策」を参照いただきたい。

(a) 米国の政策動向

米国には OpenAI 社や Anthropic 社等の新興 AI 企業や Google 社等の大手テクノロジー企業等、世界を代表する AI 関連企業が集積している。そうした中、2023 年の Joe Biden 政権下での大統領令※129 では、AI の安全性評価、政府による監督等、AI の安全性や信頼性が重視されていた。一方、2025 年 1 月に発足した第二次 Donald Trump 政権は、こうした規制色の強いアプローチを撤回し※130、AI 開発を加速させる方向へと政策を転換している。

2025 年 7 月に Trump 政権が公表した「America's AI Action Plan※131」では、「AI 競争に勝利すること」が国家戦略上の重要目標として掲げられており、AI を経済競争力及び国家安全保障上の中核技術と位置付けている。政策の柱としては、AI イノベーションの加速、AI インフラの構築、国際的な主導権の確保が示されている。これらの政策には、中国との技術競争も背景の一つにあり、AI に必要な先端半導体の輸出管理の強化、同盟国や友好国との連携強化も含まれている。

また、AI のセキュリティに関する取り組みも強化されている。2025 年 6 月には、米国 AISI が CAISI（Center for AI Standards and Innovation）に改組されることが発表され、AI に関するイノベーションの強化とともに国家安全保障上のセキュリティリスクに対処していく方向性が示された※132。「America's AI Action Plan」では、CAISI との連携を含め、AI 関連の脅威情報を共有する AI-ISAC（Information Sharing and Analysis Center）の構築や AI インシデントレスポンスの強化、更に、AI を利用する軍事及び情報機関のための高度なセキュリティを備えたデータセンターの構築が盛り込まれている。

このように、Trump 政権での米国の AI 政策は、AI の包括的な安全性規制よりも、AI 分野での競争力や国家安全保障を優先する方向へと軸足を移しており、その中でセキュリティも重要な政策課題となっている。

(b) 欧州の政策動向

欧州連合（EU：European Union）では、2024 年 5 月に成立し、同年 8 月に発効した「EU AI Act※133」の段階的な適用が進んでいる。「EU AI Act」は、基本的人権や安全性を重視した包括的な AI 規制であり、

EU 域内での AI の用途を四つのリスクレベルに分類したリスクベースの規制に加え、幅広い用途に利用可能な汎用 AI に対する義務が定められている。

2025 年 2 月には、最も高いリスク区分である「許容できないリスク」に該当する AI の禁止規定の適用が開始された。ここには、サブリミナル技術を使用する AI や個人の犯罪リスクを予測する AI 等が含まれる※134。同年 7 月には、汎用 AI 向けの「General-Purpose AI Code of Practice（汎用 AI の行動規範）」が公表された。この規範は、「透明性」「著作権」「安全性・セキュリティ」から構成され、汎用 AI の提供者を対象としている。規範自体に強制力はないが、準拠することで「EU AI Act」の関連する義務遵守の証明となり、他の方法による証明と比べて対応負担の軽減と法的確実性の向上を享受できるとされている※135。

一方、EU 域内では AI を始めとする各種規制による企業負担の増加やイノベーション停滞の懸念も高まっている。そのため、欧州委員会（European Commission）は「Digital Omnibus」において、AI、サイバーセキュリティ、データに関するルールの簡素化を提案している（「4.1.3 (3) デジタルオムニバス規則案」参照）。また、高リスク AI に関する規定の適用については、標準化された技術仕様やガイダンスの整備のため、最長 16 ヵ月延期する方針が発表されている※136。

また、2020 年に EU を離脱した英国については、「EU AI Act」のような包括的な AI 規制法は導入されていない。2025 年 1 月に Keir Starmer 政権は「AI Opportunities Action Plan」を発表し、イノベーション重視の姿勢を明確にすると同時に、適切な規制と効果的な保証が信頼性のある AI の実現につながり、規制当局もイノベーションを支援する役割を担うとした※137。同年 2 月には、英国 AI Safety Institute を AI Security Institute と改称し、国家安全保障や犯罪利用等セキュリティリスクへの対応を重視する方向性を示している※138。

このように、欧州では、基本的人権や安全性を重視した AI 規制とイノベーション促進の両立を図る方向で政策の調整が進められている。

(c) 中国の政策動向

中国政府は、AI を国家戦略上の重要技術と位置付け、研究開発、産業育成、社会実装を強力に推進している。2017 年に公表された「次世代人工知能発展計画※139」では、2030 年までに世界主要 AI イノベーションセンターとなる目標が掲げられた。その後も、米国との技術競争や輸出規制を背景に、AI 及び半導体分野での「自立・自強（self-reliance）」を重要政策として位置付け、先端 AI 技術への投資や人材育成、計算資源・データセンター等のインフラ整備が進められている※140。2025 年 8 月には、主要産業に AI を融合させる「AI プラス」の行動指針が発表され、経済成長の柱となる AI のインフラ強化等が改めて示された※141。こうした環境の中、Alibaba Group Holding Limited（阿里巴巴集団控股有限公司）、Huawei Technologies Co. Ltd.（華為技術有限公司）等の大手テクノロジー企業に加え、DeepSeek 社（杭州深度求索人工智能基础技术研究有限公司）等の新興 AI 企業も含めた AI 技術開発が加速している。

一方で、中国政府は、社会安定、国家安全保障の観点から規制や管理も強化している。2023 年に施行された「生成 AI サービス管理暫定弁法」では、生成 AI サービス提供者に対して、国家権力や社会主義体制の転覆を扇動する内容を含めた違法・有害情報の生成防止、学習データや AI モデルの管理等を求めている※142。また、2025 年 9 月から「AI 生成合成コンテンツラベル弁法」が施行され、AI 生成コンテンツへの識別表示（ラベル付け）が義務化された※143。これにより、生成コンテンツの識別可能性や偽情報対策が一層強化されている。

このように、中国の AI 政策は、国家主導による AI 産業育成と技術自立を推進する一方で、社会秩序の維持や国家安全保障を重視した管理・規制を並行して強化する点に特徴がある。また、米中間の技術競争の激化を背景として、AI 分野における安全保障と産業競争力の双方を重視する方向性が一層鮮明となっている。

(d) 日本の政策動向

日本では、AI を経済成長や安全保障の基盤となる重要技術と位置付け、イノベーション促進と安全性確保の両立を図る政策が進められている。2025 年 9 月には「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」（以下、AI 法）が全面施行された。内閣府は、AI 技術の発展が国民生活の向上及び国民経済の発展に寄与する一方、国内の AI 開発・活用の遅れや AI リスクに対する国民の不安があるとしており、AI 法は、AI のイノベーションを促進しつつリスクに対応するための制度的基盤と位置付けられている。同法では、「人工知能関連技術の研究開発及び活用の推進に関する基本理念」「国・地方公共団体・研究開発機関・事業者等の責務」「人工知能基本計画の策定」「人工知能戦

略本部の設置」等が定められている※144。

AI法に基づき、2025年12月には「人工知能基本計画※145」が閣議決定された。同計画では、信頼できるAIの追求と世界で最もAIを開発・活用しやすい国の実現を基本構想とし、AI利活用の加速的推進、AI開発力の戦略的強化、AIガバナンスの主導、AI社会に向けた継続的変革を柱として、AIの利活用と技術革新の好循環を実現することが掲げられている。

こうした方針のもと、政府全体として、生成AIを含むAIの研究開発と利活用を幅広い分野で推進している。「人工知能基本計画」では、行政、医療・介護、防災、教育等の社会課題解決分野におけるAI利活用の加速、国内のAI開発力の戦略的強化、データの集積・利活用・共有、AI人材の育成・確保等が盛り込まれている。また、政府自らが先導的にAIを利活用する方針も示されている。具体的な取り組みの例として、デジタル庁では政府職員が安全・安心にAIを活用できる基盤としてガバメントAI「源内」を構築しており、2027年度の本格利用に向けて、2026年度には全府省庁の約18万人の政府職員を対象とした大規模実証が進められている※146。

「人工知能基本計画」では、AIガバナンスに関して、「2.2.3(2)AIガバナンスの概要」で述べた「AI事業者ガイドライン」や日本AISIによるAIセーフティに関する取り組みを踏まえ、これらを更に強化する方向性が示されている。特に、日本AISIを抜本的に強化し、AIモデルの技術的評価、AIがもたらすリスクの実態把握、必要な措置の実施を進める方針が掲げられている。また、AIの安全性確保に加え、AIを利用した攻撃への対応が新たなサイバーセキュリティ上の課題であることも踏まえ、体制整備を含めた措置を講じる方針とされている※147(サイバーセキュリティ対策については「2.2.4(4)AI性能の高度化を踏まえた我が国におけるセキュリティ対策の強化」参照)。

このように日本のAI政策は、AIの研究開発・利活用を促進しつつ、リスク対応や安全性確保を進める構成となっている。また、前項で述べた広島AIプロセスやAISI国際ネットワーク等の国際的な枠組みとも連動しながら、AIガバナンスやAI評価に関する国際協調を重視している。

(e)各国の政策動向のまとめ

以上のように、各国・地域では、それぞれの産業基盤や制度設計、安全保障環境を踏まえながら、AIの開発・利活用の促進とリスク対応を進めている。政策の方向性には違いがあるものの、AIを経済競争力や国家安全保障に関わる重要技術として位置付け、AIの安全性や信頼性、セキュリティを確保する必要性が高まっている点は共通している。次項では、こうした背景を踏まえ、AIのセキュリティに関する主要な観点に沿って、具体的な事例を見ていく。

2.2.4 AIのセキュリティ

2025年12月に閣議決定したサイバーセキュリティ戦略では、AI技術の進展と普及がサイバーセキュリティ分野においても大きなインパクトを与えているとして、その内容を「AIに係る安全性確保」「AIを悪用したサイバー攻撃への対処」「AIを活用したサイバーセキュリティ確保」の三つの観点で整理している※10。本項では、これらの観点から直近の攻撃事例を示すとともに、具体的な対策に関する情報についても紹介する。

(1)AIに係る安全性確保

Security for AIと呼ばれる領域で、AIを含むシステムを標的とした攻撃と対処を扱う。トレンドマイクロ株式会社の調査によれば、AIに関連する脆弱性は、CVE(Common Vulnerabilities and Exposures:共通脆弱性識別子)の件数において2025年には2,130件となった。これは前年比34.6%の増加で、CVE全体の増加率17.9%のほぼ倍となっている※148。本項では、急増するAIの脆弱性に対する攻撃を「(a)AIの技術的特徴を狙った攻撃」、AIを対象としているが「(b)AIの技術的特徴によらない攻撃」に大別して紹介し、攻撃への対策については「2.2.4(5)AIに関するセキュリティ対策の考え方」で触れる。

(a)AIの技術的特徴を狙った攻撃

AIの技術的な仕組みに対する攻撃や防御は、敵対的機械学習(Adversarial Machine Learning)と呼ばれる学術分野として研究が進められてきた。ここでは、実際の攻撃に使われている主な手法を事例とともに紹介する。

(ア)プロンプトインジェクション

AIを狙った特徴的な攻撃として、プロンプトインジェクションは数多くの事例が知られている。プロンプトインジェクションとは、細工した指示をLLMに与えることにより、

不正な動作をさせる攻撃である。なお、安全機構を回避する攻撃の目的に着目したジェイルブレイクという表現もよく用いられる※149。細工した指示を与える経路としては、LLMとの対話において直接入力する方法と、メールの本文や組織内の共有ファイル等LLMが回答の際に参照する情報源に指示を埋め込んでおく方法とがある。後者は間接プロンプトインジェクションと呼ばれ、特に事例が目立っている。

間接プロンプトインジェクションの事例では2025年6月、情報の窃取が可能となるMicrosoft 365 Copilotの脆弱性「EchoLeak.」が報告された（CVE-2025-32711、同年5月に修正済み）※150。EchoLeakの脆弱性を悪用するために攻撃者が実施するのは、標的のユーザーにメールを送信するだけである。メールには不正な指示が含まれ、ユーザーがCopilotに質問した際に参照される可能性が高まる細工もなされている。Copilotがメールを参照すると、不正な指示に従って機密情報が特定のURLのパラメーターに埋め込まれ、そのURLがWebブラウザー上で画像として表示されることで攻撃者のサーバーに送信される。間接プロンプトインジェクションにおいて細工した指示を埋め込む対象はメールに限らず、マルウェアの実行ファイルに生成AIによる検知を回避するための指示が含まれていた事例※151や、学術論文の査読でAIによる評価が高くなるように、本文に見た目には分からない文字で指示が記載されていた事例※152もある。

間接プロンプトインジェクションは、AIエージェントに対しても通用する。例えば、ユーザーに代わってWebサイト上の操作を行う機能を持つAIエージェント型のブラウザーCometに対してWebページ上の見えない文字で細工した指示を与えることで、ユーザーが利用するWebサイトの認証情報が外部に送信されてしまう脆弱性が報告されている※153。また、業務向けのAIエージェントであるClaude Coworkが、Word等の文書ファイルに埋め込まれた指示によって、ユーザーの持つローカルのファイルを攻撃者に送信してしまう脆弱性も報告されている※154。

（イ）コードインジェクション

実行可能なコードを何らかの形で埋め込み、アプリケーションに実行させる攻撃は、従来からコードインジェクションと呼ばれている※155。AIにおいても、入力に基づいて推論を行うAIモデルのファイルに不正なコードが埋め込まれ、推論時に実行される可能性がある。こうした攻撃は、AIモデルの導入でよく見られる形態である、Hugging Face等のサイトで公開されている学習済みのAIモデルをダウンロードして利用するという形態を主な標的としている。攻撃者は、不正なコードを埋め込んだAIモデルを公開し、被害者がそれをダウンロードして実行することで攻撃を成立させる。このように、被害者の操作に依存した受動的な攻撃ではあるが、任意のコードが実行される危険性を伴うため、攻撃が成立した際の影響は極めて大きいと言える。

AIにおけるコードインジェクションの主な事例として、Pythonの標準ライブラリにおいてデータ保存に使われるpickle形式に関するものが挙げられる。AIモデルを格納するデータ形式としても広く用いられるpickleは、実行可能なコードも格納できる仕様となっており、Pythonの公式ドキュメントにおいても、その危険性が警告されている※156。2025年10月には、AIモデルの構築に用いられるフレームワークKerasにおいて、セーフモードを有効にしていても、細工されたpickle形式のAIモデルを読み込むことで任意のコードが実行される脆弱性が報告された※157。こうした攻撃への対策として、pickleに不正なコードがないかを検出するPicklescanと呼ばれるオープンソースソフトウェア（OSS：Open Source Software）が公開されているが、この検出を回避して任意のコードが実行される脆弱性も報告されている※158。また、不正なコードが埋め込まれる問題に対応するため、AIモデルに必要な情報のみに絞って格納する新たなデータ形式として、safetensors等が開発されている。ただし、これらの新たなデータ形式についても、同様の攻撃を可能とする脆弱性が複数報告されており※159、AIモデルのファイルは単なるデータではなく実行可能なコードとなり得ることに留意が必要である。

（ウ）モデル抽出

自然な対話や高度な推論を実現する近年の高性能なAIモデルは、大量の学習データと計算資源を用いて開発されており、開発企業のノウハウとコストが注ぎ込まれた、資産価値の高いものと言える。モデル抽出とは、こうした高価値なAIモデルを標的とし、入力と出力（更には思考過程等の中間出力）を収集して分析することで、元のAIモデルの能力を盗み取り、比較的少ない労力で類似する能力のモデルを開発する攻撃である。

モデル抽出は敵対的蒸留（adversarial distillation）、あるいは単に蒸留とも呼ばれる。類似の用語として知識蒸留があり、こちらも蒸留と略されるが、知識蒸留は教師となるAIモデルの入出力を利用して、生徒となる比

較的小規模な AI モデルを効率的に開発する正当な学習技術である※160。一方で敵対的蒸留は、攻撃者が正当な権限なく行う知識蒸留を指し、各 AI 提供企業は利用規約でこれを禁じている※161。

先進的な AI を開発する Google 社や Anthropic 社は、自社に対して大規模な敵対的蒸留が行われていること、またそれらの攻撃の検知や対策に取り組んでいることを公表している※162。これらの攻撃については、直接的な被害を受ける AI 開発企業だけでなく、国家間の AI 開発競争の観点から米国政府も懸念を示しており、米国科学技術政策局（Office of Science and Technology Policy）は、中国が米国の AI モデルを敵対的蒸留によって盗用していると指摘し、民間企業と連携した対策を計画している※163。一方、ワシントンの中国大使館は、この指摘に対し、米国による中国企業の不当な抑圧であるとする立場を示しており※164、モデル抽出は国家安全保障の文脈において今後も注目を集めていくと考えられる。

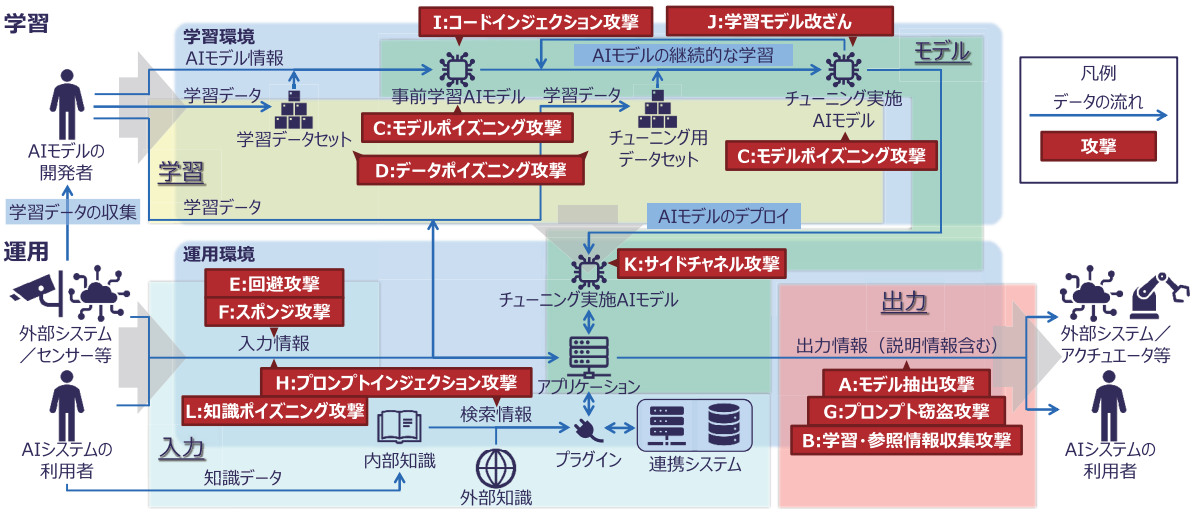
（エ）スロップスクワッティング

厳密には AI が含まれるシステムそのものへの攻撃ではないが、AI が生成したコードに起因する特徴的な攻撃として、スロップスクワッティング（slopsquatting）がある。AI が生成するコードには、ハルシネーションによって実在しないパッケージ名が含まれる場合がある。この攻撃では、攻撃者がその実在しないパッケージ名で不正なコードを公開しておく。AI の生成したコードが実行されると、もともとは実在しなかったパッケージであるにもかかわらず、攻撃者が用意した不正なコードが読み込まれて実行され、攻撃が成立する。スロップスクワッティングという用語は、誤入力されやすい URL に悪性の Web サイトを仕込むタイポスクワッティング（typosquatting）になぞらえたものであり、AI による低品質な生成物（slop）に居座る（squatting）という意味を組み合わせた表現である※165。

一見すると遠回りにも思われる攻撃手法だが、AI のハルシネーションは完全にはランダムでなく一定の傾向が見受けられ、特定の実在しないパッケージ名が複数回繰り返し生成されることが実験で確認されている※166。更に、2025 年 10 月に報告された PhantomRaven と呼ばれる攻撃キャンペーンでは、スロップスクワッティングの実例として、AI が生成しやすいパッケージ名の不正なコードが実際に複数公開されていたことが確認されている※167。

（オ）AI 特有のその他の攻撃

AI を含むシステムを標的とした特徴的な攻撃には、これまで紹介した以外にも、学習データや AI モデルの改ざんにより主に推論の誤動作を引き起こすデータポイズニングやモデルポイズニング、推論時に細工した入力を与えることで計算資源を浪費させるスポンジ攻撃等、多種多様な攻撃が知られている。日本 AISI では、これらの攻撃を、学習、モデル、（推論時の）入力、出力の 4 種類の攻撃対象領域（アタックサーフェス）を持つ、12 種類の攻撃手法に大別して俯瞰する資料として「AI システムに対する既知の攻撃と影響※168」を提供している（図 2-2-1）。更に、同資料ではそれぞれの攻撃手法がシステムに与える影響を機密性、完全性、可用性の観点で整理しており、セキュリティ上のリスクアセスメントの参考にも利用できる。具体的な内容については、資料を参照いただきたい。



■図 2-2-1　AI システムに対する攻撃の俯瞰
（出典）日本 AISI「AI システムに対する既知の攻撃と影響※169」

(b) AIの技術的特徴によらない攻撃

AIを標的としたサイバー攻撃の中には、AIそのものの技術的特徴を悪用するのではなく、ソフトウェアに対する従来型の攻撃手法を用いた事例も多く見受けられる。特にLLMやAIエージェント向けのツールが急速に普及しており、これらが新たな攻撃対象となっている。

例えば、LLMアプリケーションの構築で使われるOSSのLangChainでは、データ変換の不備によって機密情報が漏えいする脆弱性（CVE-2025-68664）が報告されている※170。また、AIと外部ツールを接続するMCP（Model Context Protocol）サーバーにおいても、サンドボックス機構が回避される脆弱性（CVE-2025-53109等）が確認されている※171。更に、複数のAIエージェントを連携させるCrewAIの脆弱性（CVE-2026-2275等）※172や、同じくAIエージェント向けツールであるOpenClawにおける脆弱性（CVE-2026-25253等）※173も報告されている。

また、AI関連のソフトウェアを狙ったサプライチェーン攻撃も発生している。異なるLLMを統一のAPIで利用可能にするOSSであるLiteLLMでは、2026年3月に攻撃者によって開発基盤が侵害され、認証情報の窃取機能等を含む不正なバージョンが公開された※174。

このように、AIの発展によって関連するソフトウェアの開発と普及も急速に進んでおり、攻撃者はAIそのものだけでなく、こうした周辺のソフトウェアについても影響力の大きい攻撃対象として狙っていると考えられる。

(2) AIを悪用したサイバー攻撃への対処

ここまで紹介したAIを狙ったサイバー攻撃だけでなく、AIを悪用した攻撃の事例も相次いで報告されている。こうした攻撃では、標的にAIを含むか否かによらず、攻撃側が効率化や高度化のためにAIを利用する。英国AISIの評価によれば、2026年4月以降に登場したAnthropic社やOpenAI社の高度なAIモデルは、従来のAIモデルと比較してサイバー攻撃能力が大幅に向上しているとされる※175。ここでは、AIを悪用したサイバー攻撃の事例を「(a)参入障壁の低下」「(b)攻撃の自動化」「(c)攻撃能力の進化」の三つの軸で紹介し、攻撃への対処については、「2.2.4(5)AIに関するセキュリティ対策の考え方」で触れる。詐欺等サイバー攻撃によらないAIの悪用に関しては、「2.2.2(4)(a)悪用」に記載した。

(a) 参入障壁の低下

英国国家サイバーセキュリティセンター（NCSC：National Cyber Security Centre）は、AIの悪用による影響の一つとして、プログラミング等サイバー攻撃で使われるスキルをAIが補うことで、技術力の高くない者による攻撃の参入障壁を下げ、攻撃の担い手が広がっていると指摘している※176。

2025年8月のProofpoint, Inc.による報告では、自然言語での指示でWebサイトを簡単に作成できるAIを活用したサービスがフィッシングサイトの作成に悪用され、サイバー犯罪への参入障壁がかつてなく低くなっているとの指摘がなされた。このサービスは、複数の攻撃キャンペーンで認証情報等を狙ったWebサイトの作成に悪用され、同サービスは不正利用を検知する仕組みを導入したという※177。

通常、AIはセーフガードやガードレールと呼ばれる安全機構によって、悪用等の不適切な指示を拒否するように設計されており、例えば、AIモデルに善悪の価値観を学習させるアラインメントや、AIモデルの外側のシステムで不適切な入出力を検知して対処する仕組みが施されている。2025年11月のPalo Alto Networks, Inc.による報告では、こうした安全機構が意図的に外され、攻撃のために設計されたLLMの事例を紹介し、簡単にマルウェアの作成等ができてしまうと指摘している※178。

AIの悪用事例は国内でも発生しており、2025年12月には、ガードレールを回避するように対話形式の生成AIに質問することで自作のプログラムを改良し、サイバー攻撃を行ったとして、高校生が逮捕されている※179。

(b) 攻撃の自動化

サイバー攻撃におけるAIの悪用は、専門知識のない者に対する参入障壁の低下と同時に、熟練した攻撃者に対しても、偵察、侵入、情報抽出といった攻撃の各段階の自動化を実現し、攻撃の大規模化や効率化をもたらした。

2025年11月のAnthropic社の報告によれば、中国を拠点とするグループと評価される脅威アクターが同社のAIを悪用し、金融機関や政府機関等約30組織を標的にした攻撃を実行したという。攻撃者はAIエージェントを活用して一連の攻撃段階を自律的に実行させて攻撃の80～90%を自動化し、人間の介入は偵察から積極的な攻撃への移行の承認等、意思決定をする程度であったとされる※180。同社の報告は、AIによる攻撃の自動化が驚く程早く進んでいるとされる内容に加えて、それを検証できる情報の不足や誇張を疑う声もあり話題となった※181。それ以降にも、複数の組織からAIの悪用による攻撃の自動化に関する報告が続いている。2026

年2月にはAIで作成されたツールによって600台以上のFortiGateデバイスが侵害された事例※182や、2026年3月には北朝鮮の脅威アクターによるAIを使った自動的な偵察や金銭要求等の悪用が報告された※183。

(c) 攻撃能力の進化

AIの悪用は、自動化によるサイバー攻撃の量的な側面だけでなく、質的な側面への影響も指摘されている。すなわち、AIの悪用によって従来と同様の方法では対処しきれない攻撃が登場する脅威である。

代表例として挙げられるのが、未知の脆弱性の発見能力である。2026年4月のAnthropic社の報告によると、同社のClaude Mythos Preview（以下、Mythos Preview）は、数千件以上の重大な脆弱性を発見し、その中にはセキュリティを重視したOSであるOpenBSDをクラッシュさせる、27年間未発見だったバグも含まれていた※184。従来、脆弱性の発見には高度な知識と長期間の解析が必要だったが、AIによってコードを分析することで、人間が見落としていた重大な問題を短時間で発見できる可能性が示されている。こうした能力が、攻撃者によるシステムの脆弱性の発見と、その脆弱性を狙った攻撃につながる懸念から、本白書の執筆時点で同社はMythos Previewを一般公開していない。代わりに、大手IT企業等一部の組織にのみアクセスを認め、攻撃者に悪用される前に脆弱性を発見して修正することで、システムのセキュリティ向上を目指すProject Glasswingを立ち上げた※185。同じく4月に公表されたOpenAI社のGPT-5.5も高度なサイバーセキュリティ能力を持つとされ、その機能の利用は一定の基準を満たしたユーザーに限定されている※186。

また、未知の脆弱性の発見以外にも、AIの悪用による新たな攻撃の脅威が報告されている。2025年には、感染した環境内においてAIを用いて自律的にコードを生成するマルウェアが複数報告されており、これらはあらかじめ固定された悪性コードを持たないことで、従来型のシグネチャーによるマルウェアの検知を回避する可能性が指摘されている※187。2025年7月には、AIモデル自体の悪用ではないが、よく知られたAIのWebサービスのAPIを攻撃者のサーバーとの通信に悪用し、正規のAIサービス利用に紛れて外部通信を行うマルウェアも発見されている※188。

このように、AIはサイバー攻撃を単に効率化するだけでなく、攻撃能力そのものの進化や攻撃手法の多様化をもたらしつつある。今後は、AIの悪用を前提としたセキュリティ対策の重要性が更に高まっていくと考えられる。

(3) AIを活用したサイバーセキュリティ確保

AI for Securityと呼ばれる領域で、これまで述べた攻撃側ではなく、防御側にAIを取り入れる話題を扱う。攻撃と防御は表裏一体であり、例えば、「2.2.4 (2) (c) 攻撃能力の進化」でも触れたようにAnthropic社は高度なサイバーセキュリティ能力を持つMythos Previewを悪用の懸念から執筆時点では一般公開せず、アクセスを限定した上でソフトウェアのセキュリティ向上に活用する取り組みを始めている。2026年4月には、Webブラウザー Firefoxの更新において、Mythos Previewが発見した271件の脆弱性を修正しており、開発元のMozillaは「The zero-days are numbered」（ゼロデイ攻撃の終わりは近い）と表現して防御側が優位になり得るとの認識を示している※189。

更に、AIの活用は脆弱性の発見や修正だけにとどまらない。攻撃経路の予測や悪用されやすい脆弱性の分析等、リスクマネジメントの支援に加え、アラートのトリアージや詳細調査、攻撃手法の解説等セキュリティ運用を支援する用途にも広がっている※190。従来、セキュリティ運用では大量のアラート分析やログ調査を人手に依存する場面が多かったが、AIが分析や判断を支援することで、運用負荷の軽減や対応速度の向上が期待されている。

しかし、防御側へのAIの導入がかえって問題を引き起こすことも指摘されている。例えば、AIが大量の脆弱性を短期間で発見することで、修正や検証の負荷が急増する可能性がある。2026年1月には、OSSで広く利用されるcurlのバグ報奨金プログラムが終了した。開発者によると、AIを用いた低品質な脆弱性レポートが大量に届き、セキュリティチームに大きな負担をかけているためとされる※191。また、同様の理由で他の報奨金プログラムの新規受付も終了することが報じられている※192。2026年4月には、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）が、脆弱性報告の増加を受けて、NVD（National Vulnerability Database：国家脆弱性データベース）の運用を変更した。従来はすべてのCVEを分析し、重大度のスコアや製品リスト等の詳細を追加していたが、4月15日以降は一定の基準を満たす重要なCVEを優先して扱っている※193。

このように、AIを悪用したサイバー攻撃が急速に拡大する中で、防御側においてもAIの活用が前提となりつつある。一方で、単にAIを導入するだけで直ちに

安全性が向上するわけではなく、防御側の新たな負担や運用上の課題につながる側面もあることから、AIの特性を見極めながら適切に活用していくことが重要になると言える。

(4) AI性能の高度化を踏まえた我が国におけるセキュリティ対策の強化

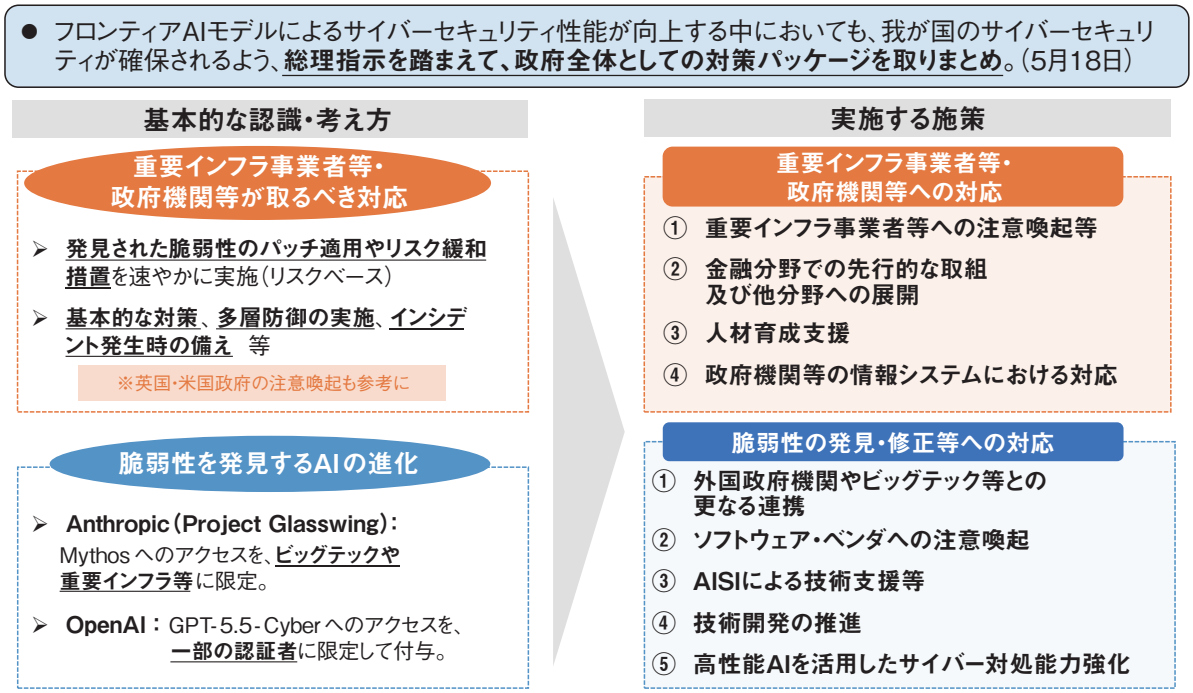
ここまで、AIを標的としたサイバー攻撃やAIを悪用したサイバー攻撃の事例を紹介するとともに、セキュリティ分野におけるAIの活用にも触れた。本項では、こうした背景を踏まえた我が国におけるセキュリティ対策について、政府が進める取り組みを紹介する。

政府は2026年5月18日、「AI性能の高度化を踏まえたサイバーセキュリティ対策に関する関係省庁会議」において、「Project YATA-Shield※194」と題して、AI性能の高度化を踏まえたサイバーセキュリティ対策の強化について関係省庁・関係機関による施策を取りまとめた※195。

背景には、AI技術は急速に進展・普及しており、サイバー攻撃にAIが悪用されることで、攻撃のスピード・規模が劇的に増加する等、サイバーセキュリティにおける脅威に直面している状況がある。特に「フロンティアAI」と呼ばれる高性能AIによる脆弱性の発見・修正等のサイバーセキュリティ性能の急速な向上を踏まえ、重要インフラ事業者等への対応と脆弱性の発見・修正等に関する対応の双方に迅速に取り組む必要があるとされた。高性能AIは、ベンダー等における脆弱性の発見・修正等や重要インフラ事業者等における検知・対応等のサイバーセキュリティ対策に活用することにより、我が国のサイバー対処能力の更なる強化が期待できる一方、攻撃者に悪用されることにより、サイバー攻撃がより高速かつ大規模に行われるおそれがある。このため、悪用リスクを前提として、防御側でも高性能AIを積極的に活用する方針が示された。

図2-2-2にProject YATA-Shieldの概要を示す。

Project YATA-Shieldでは、重要インフラ事業者等に対し、経営層のリーダーシップのもと、基本的なサイバーセキュリティ対策の確実な実施や、より高速かつ大量に脆弱性が発見・修正されることを前提とした対策強化を求めている。注意喚起文書※197では、サイバーセキュリティ対策は、企業活動におけるコストや損失を減らすために必要な投資（将来の事業活動・成長に必須な費用）と位置付けることが重要とされ、資産管理、リスクアセスメント、脆弱性管理、認証･アクセス制御、バックアップ、監視・分析、事業継続計画、インシデント対応及び復旧、サプライチェーン・リスクへの対応等の基本的対策の徹底を求めている。加えて、「ゼロトラスト」の考え方に基づくシステム設計･運用への移行、脅威ハンティング等の強化、高性能AIを活用したサイバーセキュリティ対策の強化も挙げている。



■図2-2-2　Project YATA-Shieldの概要
(出典)NCO「AI性能の高度化を踏まえたサイバーセキュリティ対策の強化※196」

具体的な活動として、金融分野について、2026年5月14日に、金融業界とIT事業者、政府・日本銀行等がAI技術の進展による脅威について共通の理解を持ち、対応を検討していくため、実務者レベルでの議論を深めることを目的とした作業部会を開催した※198。また経済産業省でも、同年5月1日に、官民での認識共有を図るための意見交換を行った※199。

政府機関等に対しても、政府統一基準に基づく基本的な対策を徹底するとともに、より高速かつ大量に脆弱性が発見・修正されることを前提とした対策の強化を求めている。特に、セキュリティパッチ（修正プログラム）の速やかな適用は非常に重要であり、必要に応じて、セキュリティパッチ等の対策用ファイルの適時の適用を前提とした運用設計（パッチマネジメント（管理））を見直すこととしている。あわせて、インシデントやその予兆を確認した場合には、NCOへの速やかな報告を求めている※200。

脆弱性の発見・修正等への対応では、ソフトウェアベンダーに対し、セキュア・バイ・デザインの原則に基づき、高性能AIも活用しながら、ソフトウェア開発ライフサイクル全体において脆弱性の早期発見・対応に率先して取り組むよう注意喚起している※201。具体的には、リリース前のソフトウェアについては、高性能AIを積極的に活用し、リリース後の脆弱性発見の可能性を低減させた上で、リリースをする。リリース後のソフトウェアについては、脆弱性が発見された場合に（必要に応じ高性能AIも活用して）パッチを早急に作成し、顧客に速やかに提供することを求めている。

更に、日本AISIによる情報収集・評価の実施及びこれを踏まえた情報提供、ガイドラインの策定、外国政府機関やAI開発者等との連携、AIを活用したサイバー対処能力の向上も進めるとしている。政府は、AIを巡る動向が急速に変化する中においても、より実効的な対応を継続的に行うべく、施策の実施状況を機動的に確認し、追加的対応を不断に検証・実施するとしている。

(5) AIに関するセキュリティ対策の考え方

本項では、AIに関するセキュリティ対策の考え方や、参考となる情報を紹介する。なお、AIの活用にあたっては、「2.2.2 AIのリスク」に例示したようにセキュリティに限らない幅広いリスクが存在するため、「2.2.3 AIの安全性とガバナンス」で紹介したAIセーフティの考え方も重要となる。その上で、ここでは特にセキュリティに焦点を当てる。

前述のとおり、セキュリティの分野においてもAIは様々な影響を与えている。しかし、従来のセキュリティ対策の考え方が不要になるわけではなく、むしろ引き続き重要であることを強調したい。「2.2.4 (1) (b) AIの技術的特徴によらない攻撃」では、AIの急速な普及に伴い、その周辺のソフトウェアが従来型のサイバー攻撃の標的となっている事例を紹介した。また、「2.2.4 (2) AIを悪用したサイバー攻撃への対処」では、AIによる参入障壁の低下や攻撃の自動化によって、従来型のサイバー攻撃が増加している側面を指摘した。このように従来型のサイバー攻撃は、AIによって淘汰されるどころか激化しており、それらへの対策は引き続き重要である。その上で、AIに特徴的な要素を踏まえた対策を新たに取り込んでいく必要がある。

考慮すべき点の一つは、「2.2.4 (1) (a) AIの技術的特徴を狙った攻撃」で挙げた、AIを標的とした攻撃への対策である。2026年3月に総務省が公表した「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」では、プロンプトインジェクションを中心としたAI特有の攻撃に関する具体的な技術的対策例を示している※202。また、日本AISIでは、AIを含むシステムに施した対策について、セキュリティを含むAIセーフティの観点で攻撃者の視点から評価する「AIセーフティに関するレッドチーミング手法ガイド※203」や、レッドチーミングの支援を行うOSSのツール※204を公開している。更に日本AISIは、AIのブラックボックス性や自律性によって事前対策だけでは被害の最小化が困難であるとして、観測性と制御性を中核としたAIシステム向けインシデントレスポンスの枠組みも提唱している※205。

AIがセキュリティ対策にもたらす別の側面として、ソフトウェア更新への影響もある。「2.2.4 (3) AIを活用したサイバーセキュリティ確保」で示したようにAIが未知の脆弱性を大量に発見する能力を持ち始めている。NCSCは、AIによって発見される大量の脆弱性の修正を「脆弱性パッチの波」と表現し※206、これに備えて組織は大規模で迅速かつ頻繁に更新する計画を立てるべきだとして、脆弱性管理のガイダンスを公表している※207。

更に、ガバナンスの観点からは、「シャドーAI」と呼ばれる、組織の管理部門が認識しないAI利用への対応も考慮する必要がある。民間企業団体である一般社団法人AIガバナンス協会は、シャドーAIに関して従業員による個人的利用だけでなく、既存ソフトウェアの更新によってAI機能が追加されるケースや、外部パートナーによるAI利用についても課題が存在するとする調査結果を公表し、ヒアリング結果を踏まえて整理したAIガバ

ナンスのアプローチを紹介している※208。

最後に、AIとセキュリティを巡る状況は絶えず変化しており、継続的な情報収集も重要と言える。内閣府主導で創設された「経済安全保障重要技術育成プログラム」（通称、K Program）の中では、「安心安全なAI利活用の為の知識・技術の体系化と知識集約環境構築」が進められており、その成果を活用した解説記事や体系化のマップ等が掲載されたポータルサイトが公開されている※209。また、IPAでは「AIセキュリティ短信※210」として注意すべきインシデント事例や把握しておくべき動向を発信する取り組みを始めている。

本節「2.2 AIの安全性確保の取り組み」の冒頭では、執筆時点から約10年前を振り返り、AlphaGoによる囲碁のプロ棋士への勝利に触れた。当時から2026年の現状を予測するのは困難であったが、AIの発展は更に加速し、現時点では1年後の社会の変化を予測することすら難しくなっている。そのため、日頃から情報収集を行い、将来現れる新たな脅威に対しても進化し続けるAIをうまく活用しながら対応していくことが求められると言えよう。

COLUMN

AI時代のデジタル・シティズンシップと責任

インターネットで多くの人が頻繁に利用する検索機能。いつからかAIによる要約が示されるようになり、それを多くの人が自然と受け入れています。生成AIが驚く程の速さで発達・利用拡大し、気付けば寄り添って手助けしてくれている今、大人達がこれまでの経験から得た常識・考え方・危機管理術のアップデートは急務です。

そこで注目したいのが、「デジタル・シティズンシップ」＝「デジタル技術の利用を通じて、社会に積極的に関与し、参加する（責任ある行動を取る）能力」です。これは、年齢や立場を問わず現代社会を生きる誰もが身に付けたい能力であり、「情報セキュリティ」「情報リテラシー」「情報モラル」も欠かせない要素となります。学校では、教育活動全体をとおしてデジタル・シティズンシップ教育が実施されるようになったものの、大人が学ぶ機会はなかなかありません。ランサムウェア、特殊詐欺、闇バイトへの勧誘等といった様々な危機が、ネットの向こうから待ったなしで襲ってくる時代、青少年を導く側でもある大人だからこそ、デジタル・シティズンシップを身に付けたいものです。

更に、偽・誤情報や危険な情報を察知する感度を上げることも重要です。AIが生成した情報のファクトチェックを行う割合は10代20代でより高く、男性が7割以上、女性が約6割という調査結果があります[i]。年齢が上がるにつれ割合が低下する理由はどうあれ、ファクトチェックについては若い層に軍配が上がるようです。

また、検索結果に出てくるAIの要約は便利な反面、ネット上に散在する情報の要約でしかなく、誰でも気付くような間違いや、参照リンク先が既にない古い情報もあります。それらによるミスリードの防止にはファクトチェックが不可欠ですが、その前にまず、入手した情報を「ちゃんと読む」ことを心がけてみませんか?

「ちゃんと読む」がクセになると、「ん?何かヘン??」と気付く感度も上がります。実はこれが鍵なのです。AI利用の有無を問わず、世の中には正しい情報のような顔をした偽・誤情報、曖昧な情報、チェリーピッキング（都合の良い部分だけを拾う行為）、悪意の仕掛け、詐欺メールやメッセージ等もごまんと存在します。目にした情報をちゃんと読まず、ファクトチェックもせずに、アクセスしたり行動を起こしたりすれば、職場、家庭、自身の健康に支障をきたすことにもなりかねません。そうしたトラブルの責任は、十分に注意をせずに、その情報を受け入れた側にもあるのですから、情報への感度アップは現代人に必須と言えます。

何があろうと、AI自身は責任を取れません。責任を取れるのは人（開発者、提供者、利用者）だけです。一般的にAIサービスの利用規約には「利用者自身の責任において利用すること」が定められているため、責任は利用者が負うことになります。

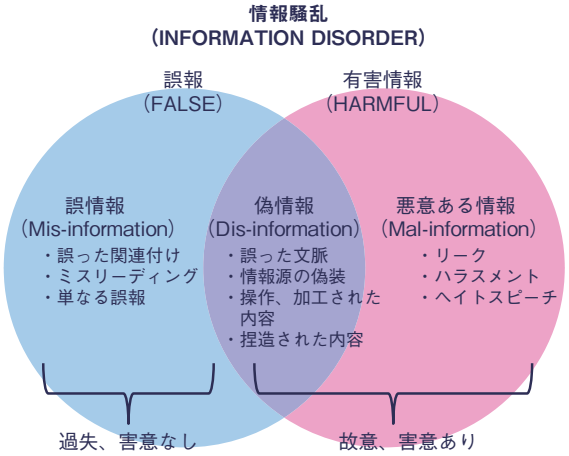
こう考えると、AI利用に伴う責任について、今まで以上に真剣に向き合う必要がありそうです。まずは気付きの感度を上げ、気になることがあったら、身近な信頼できる人に尋ねてみるといったアナログな対応が、デジタル・シティズンシップのベースになるような気がします。職場でも家庭でも、学校や地域でも、手軽にできそうなこうしたことから実践してみてはいかがでしょうか。

i　NTTドコモ モバイル社会研究所：【ライフスタイル】生成AIのファクトチェック、若年層・活用層・人とのつながりを大切にする層が実施する傾向　https://www.moba-ken.jp/project/lifestyle/20251106.html〔2026/7/27確認〕

2.3 偽・誤情報対策の動向

本節では、虚偽を含む情報の拡散の国際的な情勢を概観しつつ、主要な各国事例を取り上げて解説を行う。

国家が関与するサイバー攻撃は、その手法等から分類すると表 2-3-1 のように整理できる。近年の情報戦・認知戦においては、虚偽を含む情報を流布する「情報操作型サイバー攻撃」と、それを含む様々な類型のサイバー攻撃を組み合わせた「ハイブリッド型サイバー攻撃」が大きな脅威となっている。本節では、表 2-3-1 の攻撃類型を使用して以降の解説を行う。なお、誤情報（ミスインフォメーション）と偽情報（ディスインフォメーション）を組み合わせた政府の用法※211 に従い、合わせて「偽・誤情報」と表記する。



■図 2-3-1　欧州評議会による情報騒乱（INFORMATION DISORDER）の分類

（出典）Claire Wardle, Hossein Derakhshan「INFORMATION DISORDER : Toward an interdisciplinary framework for research and policy making※213」を基に IPA が作成

© Council of Europe, reproduced with permission (from p5 Council of Europe report DGI(2017)09 Information disorder: Towards an interdisciplinary framework for research and policy making)

2.3.1 偽・誤情報の定義

虚偽を含む情報の拡散による社会の混乱（情報騒乱）については、2017 年に欧州評議会（CoE：Council of Europe）が用語の整理を行っている（図 2-3-1）。

この整理による各用語の定義は以下のとおりである。

- ミスインフォメーション（Mis-information、誤情報）：事実誤認や過失により誤解を招く文脈で発信される、故意や悪意のない誤情報。
- ディスインフォメーション（Dis-information、偽情報）：社会、公益への危害を目的とした害意のある情報。偽の情報だけでなく、誤った文脈や操作された内容で拡散される真の情報も含まれる。
- マルインフォメーション（Mal-information、悪意ある情報）：リークやハラスメント等、害意をもって広められる真の情報。

ミスインフォメーションとディスインフォメーションの差異は情報の発信者の故意性と害意の有無にあり、ディスインフォメーションとマルインフォメーションの差異は情報自体

攻撃類型	攻撃の内容
①情報窃取型	標的型攻撃（マルウェア付きメール、水飲み場攻撃）等により、特定の政府機関、企業、団体、個人のネットワーク、コンピューターに侵入し、機密情報、営業情報、特許、知的財産等を窃取する攻撃。
②機能妨害型	DDoS 攻撃等の手法により、ネットワークの許容量を超える飽和通信要求によって、サーバー、ネットワークを麻痺させる攻撃。
③機能破壊型	標的型攻撃等により、特定の政府機関、企業、団体、個人のネットワークに侵入し、システム破壊・改ざんを行う攻撃。ネットワーク内のデータ消去・改ざんを目的とするものと、制御系システムを標的として物理的破壊を目的とするものがある。
④金銭目的型	標的型攻撃、脆弱性の悪用等により、特定の政府機関、銀行、企業、個人のネットワークに侵入し、不正な送金を行う、またはコンピューター内のデータを暗号化し、解読に身代金を要求する攻撃。
⑤情報操作型	代理主体（Proxy）等を用いて真の発信者を隠匿した上で、SNS 等に偽ニュースを流布させることにより、対象国（主に民主主義国家）における世論操作を目的とした攻撃。選挙結果に影響を与えることを企図している攻撃も見られる。
⑥軍事的サイバー攻撃	軍事攻撃と一体的に行われる機能妨害・機能破壊を目的とした攻撃。電子戦の一環として軍隊の指揮統制（C4I）システムを標的とするものと、軍事行動に影響を与える重要インフラを標的としたものがある。
⑦ハイブリッド型	上記①～⑥までの類型を組み合わせた攻撃。近年は①情報窃取型＋⑤情報操作型、②機能妨害型＋⑤情報操作型等の組み合わせが多い。

■表 2-3-1　国家が関与するサイバー攻撃の類型

（出典）大澤淳「サイバー領域の安全保障政策の方向性※212」を基に IPA が加筆・編集

の真偽性にあり、判断の視点がやや異なる。この分類においては、本来は誤ったニュースを指すに過ぎない「フェイクニュース」は、ミスインフォメーションまたはディスインフォメーションに含まれる。ただし、これらについて確定的かつ共通の国際的な定義はなく、特にディスインフォメーションについては定義に多少の揺らぎが見られる。一般社団法人セーファーインターネット協会が、偽情報対策について多様なステークホルダーによる協力関係の構築と対話の枠組みを設けるべく設置した Disinformation 対策フォーラムでは、「Disinformation」を「あらゆる形態における虚偽の、不正確な、または誤解を招くような情報で、設計・表示・宣伝される等を通して、公共に危害が与えられた、又は、与える可能性が高いもの」と定義している※214。また、欧州対外活動庁（EEAS：European External Action Service）の 2023 年のレポート※215 では、Disinformation について「経済的利益を得るため、または意図的に公衆を欺くために作成、提示、流布され、公共に害を与える可能性のある、検証可能な虚偽または誤解を招く情報」と説明している。公共への害とは、「民主的な政治・政策決定プロセスや市民の健康、環境、安全保障等の公共財に対する脅威を指す。」と定義して、その目的として経済的利益の追求または公衆を欺く故意があることを明示するとともに、その結果として公共に害が生じ得ることを示している。日本語ではディスインフォメーションに「偽情報」という訳語があてられているが、ディスインフォメーションは単に虚偽の情報を含むだけでなく、相手の誤解を招くために真の情報も混ぜ合わせて加工や情報操作が行われる点に注意が必要である。

2.3.2 偽・誤情報の最新情勢

本項においては、偽・誤情報を巡る世界的な情勢を概観し、統計的な調査等も踏まえつつ、2025 年を中心とした最新動向を解説する。

(1) 偽・誤情報の現在

世界経済フォーラム（WEF：World Economic Forum）が 2026 年 1 月に公表した「The Global Risks Report 2026※216」では、今後、短期的（2 年間）または長期的（10 年間）に想定されるグローバルリスクの上位 10 位までを深刻度順に示している（表 2-3-2）。「Misinformation and disinformation」（誤情報と偽情報）は 2024 年※217 及び 2025 年※218 の第 1 位から順位を下げたものの、短期的リスクの第 2 位となり、3 年連続で上位のリスクと評価された。また、「Misinformation and disinformation」は、長期的リスクでも第 4 位であり、いずれの時間軸でも上位に位置する持続的リスクとされた。短期的リスク第 6 位の「Cyber insecurity」（サイバー不安）と、短期的リスク第 2 位の「Misinformation and disinformation」、短期的リスク第 3 位の「Societal polarization」（社会の二極化）、及び短期的リスクでは第 30 位であったものの長期的リスクでは第 5 位となった「Adverse outcomes of AI technologies」（AI 技術の悪影響）は、相互に関連するリスクとして認識されている。

2025 年から 2026 年にかけて、偽・誤情報は情報空間内部の問題にとどまらず、地経学（Geoeconomics）的・軍事的対立や社会分断、先端技術の浸透等と一体化した横断的リスクとして固定化した状況にある。

	Short term（2 years）	Long term（10 years）
1.	Geoeconomic confrontation	Extreme weather events
2.	Misinformation and disinformation	Biodiversity loss and ecosystem collapse
3.	Societal polarization	Critical change to Earth systems
4.	Extreme weather events	Misinformation and disinformation
5.	State-based armed conflict	Adverse outcomes of AI technologies
6.	Cyber insecurity	Natural resource shortages
7.	Inequality	Inequality
8.	Erosion of human rights and/or of civic freedoms	Cyber insecurity
9.	Pollution	Societal polarization
10.	Involuntary migration or displacement	Pollution

Risk categories
Economic Environmental Geopolitical Societal Technological
Source
World Economic Forum Global Risks Perception Survey 2025-2026

■表 2-3-2 Global risks ranked by severity, short term（2 years）and long term（10 years）
（出典）WEF「The Global Risks Report 2026」を基に IPA が編集

更に、市民側の偽･誤情報に対する脅威認識としても、不安が高止まりしている状況にある。欧米、アジア、アフリカ主要国を調査対象としたロイター・ジャーナリズム研究所（Reuters Institute for the Study of Journalism）の「Digital News Report 2025※219」によれば、調査対象者の半数以上（58%）が、オンラインニュースにおいて真偽を見分ける能力について依然として懸念を抱いていると回答しており、この割合は2024年と同水準である。懸念が最も高いのはアフリカ（73%）と米国（73%）で、最も低いのは西ヨーロッパ（46%）となっている。同調査で、虚偽または誤解を招く情報の情報源について、重大な脅威と見なされているのは、調査対象の主要国全体で見ると、「オンラインのインフルエンサーや著名人」（47%）と、「自国の政治家や政党」（47%）であった。国別に見ると、インフルエンサーに対する懸念が最も高いのは、ナイジェリア（58%）やケニア（59%）等のアフリカ諸国である一方、自国の政治家や政党が最大の脅威と見なされているのは、米国（57%）、スペイン（57%）、そしてセルビア（59%）、スロバキア（56%）、ハンガリー（54%）を含む東欧の多くの国々であった※220。

SNSプラットフォームの動向としては、Meta Platforms, Inc.（以下、Meta社）は、2025年上半期に、EU加盟国向けのFacebookとInstagramの広告について500万件超を削除し、このうち誤情報ポリシー違反を理由に削除された広告は8万3,000件超に上ったと報告した。また同社は、EU域内の120万件超の広告に資金提供者を明示する「paid for by」表示を付与した※221。過去にも政治広告が各国の選挙干渉に利用されたことを踏まえ、SNS上の広告の削除対応や透明化が進んでおり、主要な偽・誤情報対策の一つとなっている。

また、Meta社は2025年を通じて約35億件の偽アカウントに対して措置を講じたことも報告している※222。この偽アカウントの件数は、組織的に偽・誤情報を拡散するアカウント群の規模の大きさを示唆するものであり、コンテンツ単位の対処と並んで、偽アカウント等の拡散基盤そのものへの対処が対策の柱となっている。

他方で、偽・誤情報の生成には、AIの悪用が拍車をかけている状況にある。OpenAI社は、2024年2月に脅威レポートの公表を開始して以降、2025年10月時点までに利用規約に違反した40件超の悪用ネットワークによるAIサービスの利用を遮断・報告したと公表した※223。対象には、権威主義国家に関連する国家アクターによる影響工作キャンペーン、詐欺、悪意あるサイバー活動等が含まれている。更に、2026年2月に公表された最新の報告書では、2年間の脅威報告を総括し、ロシアのコンテンツファームやインドネシアの詐欺グループの事例から、脅威アクターが工作の工程ごとに複数のAIモデルを使い分け、SNSアカウントやWebサイト等の従来型ツールと組み合わせて運用する傾向が指摘された※224。また日本の関連事案としては、中国発の影響工作「Spamouflage」との関連性が指摘される国家アクターが、高市早苗内閣総理大臣（以下、高市総理）を標的とした対日影響工作の立案にChatGPTを利用しようとした事例も同報告書の中で報告されている。生成AIが偽・誤情報の生成・翻訳・拡散の各工程を効率化しており、国家アクターによるAIの悪用の拡大が強く懸念される状況にある。

(2) 偽・誤情報利用による安全保障上の脅威の拡大

偽・誤情報の中でも、とりわけ偽情報を中心とした悪意ある情報操作が近年の安全保障上の問題となっている。2014年のクリミア危機以降、ロシアによる「ハイブリッド戦争」を始めとして、サイバー空間を中心とした情報戦における、国家による情報操作が大きな課題となってきた。ハイブリッド戦争は、原義的には、非国家主体がゲリラ戦や生物兵器、サイバー攻撃や偽情報等あらゆる手段を、戦術的優位性を確保するために時と場所を選ばずに実行する新しい戦争形態を指す※225。そしてIT技術の進化やWebメディア、SNSの一般社会の浸透等により、ハイブリッド戦争におけるサイバー戦や情報戦のウェイトが増してきた。情報戦は、偽情報を流布することで相手国・地域の社会の混乱や政府機関の信用失墜を企図する「情報操作型サイバー攻撃」によって行われる※226。更には、単純に偽情報を拡散するだけではなく、その偽情報の積み重ねによって特定の国家に都合の良い戦略的なナラティブ（物語）を構築し、戦略的ナラティブに基づいた偽情報の拡散によって、一般市民も含めた相手国国民全体の価値観や信念、思考方法まで変容させてしまうことを、偽情報を流布する国々は狙っている。人間の思考方法や推論方法等の認知情報処理フローは、感覚入力された情報と、過去の記憶やイメージによって引き出される記憶系の情報との突き合わせによって反応が生成され、実際の行動が引き起こされる。そのような認知情報処理フロー下における個々人の視覚や聴覚等の入力センサーがサイバー空間と接続された現在のIoT社会においては、偽情報は「認知領域」における攻撃手段と見なされることとなった※227。その攻防は国家

安全保障の文脈で「認知戦」と呼ばれる。例えば、偽情報を用いて選挙干渉を行い、有権者の認知を混乱させ、自国に有利な意思決定を誘導しようとするようなアプローチが代表的な攻撃手法である。

特に対ロシアの情報戦・認知戦に備えてきた欧州各国は、偽情報を用いた影響工作が民主主義制度への信頼を揺るがし、社会を分断することを警戒している※228。EEASはこのような工作を「FIMI（Foreign Information Manipulation and Interference：外国による情報操作と干渉）」と呼称し※229、増大する安全保障上の脅威であると強調しており、ハイブリッド脅威への対策を加盟国と協力して進めている。ハイブリッド脅威とは、情報操作やサイバー攻撃、経済的威圧等武力行為以外の手段も組み合わせて標的の国家や組織を弱体化させることを目的とする有害な活動を指す※230。当然ながら、欧州だけでなく情報戦や影響工作の脅威に晒されている米国等もこのような情報操作に警戒の動きを強めているところである。EEASによるFIMIの脅威に関する第1回報告書では、2022年に収集した事例100件の主要アクターについて、88件がロシア、17件が中国であったこと（両国の重なりが見られる事例が5件のため合計は105件となっている）が数量的に示されており※231、続く第2回、第3回の報告書でも中国やロシアを主要アクターに挙げている※232。

こうした脅威拡大に対し、対策を講じているのは国家だけではない。情報戦・認知戦の主戦場となるSNS等を運営する主要プラットフォーム各社も、国家関与が疑われる影響工作キャンペーンの摘発を強化している。

Meta社は2025年上半期、ドイツ、ルーマニア、ポルトガル、ポーランドの各選挙に対応し、選挙運用センターの設置、迅速対応システムの運用、市民社会・ファクトチェック機関との報告経路の整備を行ったと報告している※221。ルーマニアの事例では、1件のCIB（Coordinated Inauthentic Behavior：組織的な不正行動）ネットワークを削除し、ルーマニアを標的とする影響工作を早期に遮断したことも報告されている※221。

Google社の脅威分析部門であるGTIG（Google Threat Intelligence Group）は、2025年9月のロシア製ドローンによるポーランド領空侵入の直後、親ロシア系アクターが関与した影響工作により「ロシアの責任否定」「NATO・西側諸国への責任転嫁」「ポーランド政府への不信醸成」「ウクライナ支援の弱体化」を狙った情報拡散が展開されたと分析した※233。物理的なインシデントの直後に情報戦が即座に発動するという、現代のハイブリッド戦の様相を示す事例である。

紛争等の有事の際には、情報戦・認知戦も活発化する。2025年5月のインド・パキスタン危機では、AI生成映像、過去の映像、ゲーム映像、別地域の映像等が軍事的成果や勝利を示す証拠として両国から大量に拡散された。英国Guardian紙は、CSOH（Centre for the Study of Organized Hate：組織的憎悪の研究センター）の分析として、問題のあるX上の投稿を427件確認し、その一部は約1,000万ビューに達した一方、警告表示が付されたものは73件にとどまったと報じている※234。この事例において戦略的に大量の偽情報が拡散されたことは、ナラティブを操作し両国の緊張を高めることで、両国の衝突を核戦争にエスカレーションさせるだけの推進力を持っていたと分析されている。更に2025年12月には、タイ・カンボジア間で武力衝突が発生したが、ここでも偽情報拡散やナラティブの戦いが問題となった。そのため、2025年12月27日に停戦延長のために署名した両国共同声明では、「双方は緊張緩和、否定的な世論の緩和、平和的対話に資する環境の醸成を図るため、虚偽の情報や偽ニュースの拡散を控えることに合意する」といった文言が盛り込まれるに至った※235。近年の情報戦・認知戦は、情報空間だけの問題にとどまらず、物理的な戦争と地続きの戦闘様相として立ち現れていることがうかがえる。

2.3.3 2025年度の注目事例

本項では、具体的な事例のうち、2025年度の注目すべき事例を取り上げて解説する。2025年度以前から継続している事例についても取り扱う。

(1) 欧州の選挙への影響工作

2025年9月28日に実施されたモルドバ議会選挙において、モルドバ当局によれば、選挙干渉を目的として、大規模な買収工作、同年中に1,000件を超える重要インフラへのサイバー攻撃、投票日の暴動扇動計画、そして大規模なオンライン偽情報キャンペーンが複合的に展開されたという。ロシアのアクターはモルドバ市民をTikTokやFacebook上の組織的偽情報拡散に金銭で動員し、Maia Sandu大統領や与党を攻撃するAI生成コンテンツを拡散させた※236。これに対しモルドバ側は、欧州委員会（European Commission）と共同で選挙前にデジタル・ハイブリッド脅威のシミュレーションを実施し、Google社、Meta社、TikTok Inc.（以下、TikTok社）の参

加を得て対応体制を準備するとともに、外国の干渉に対抗するための専門家グループ「Hybrid Rapid Response Team」をEUから受け入れ、サイバー攻撃を含めたEU共同演習の導入、欧州デジタルメディア監視所（EDMO: European Digital Media Observatory）の新たな地域ハブを設立する等、EUとの共同歩調で積極的な対策を講じた※237。欧州安全保障協力機構（OSCE：Organization for Security and Co-operation in Europe）等の国際選挙監視団は、モルドバの議会選挙は競争的で有権者に政治的選択肢を提供したが、一方で、外国の干渉、違法資金、サイバー攻撃、広範な偽情報の拡散がこの民主主義プロセスを妨害したと結論付けている※238。

2025年2月23日に実施されたドイツ連邦議会選挙においては、ロシアによる同選挙への影響工作が懸念されていた※239。同選挙に対する偽情報による影響工作について、選挙後、背後にロシア連邦軍参謀本部情報総局（GRU:Glavnoye Razvedyvatelnoye Upravleniye）と関係する組織が存在するとして、ドイツ政府は2025年12月、ベルリン駐在のロシア大使を召喚して抗議した※240。この事例は、事後の調査により、選挙干渉におけるアクターの特定国家への帰属（アトリビューション）が明らかにされ、外交措置に発展した事例として注目すべき事例となった。

2025年5月18日に第1回投票、6月1日に決選投票が実施されたポーランド大統領選挙では、ロシアによる影響工作が懸念されたため、ポーランド政府は2025年2月からデジタル化省が主導する「選挙アンブレラ（Election Umbrella）」と称する選挙保護計画を発動し、偽・誤情報対策としては、ポーランドの国立研究機関であるNASKがSNS等の監視を実施した。デジタル化省によると、NASKは、Meta社、X Corp.（以下、X社）、TikTok社のプラットフォーム上の1万6,000件を超える偽アカウント（候補者を装った169アカウントを含む）の無効化等を実施したという※241。

(2) 武力衝突・軍事作戦に関連した影響工作

2025年6月13日から25日にかけてのイスラエルとイランの軍事衝突は、生成AIによるディープフェイク流布が特徴的な事例であった。BBC Verifyの分析によれば、イランの軍事的成果を誇張するAI生成動画等が大量に拡散され、最も視聴された偽動画3本だけで合計1億回以上の閲覧を集めたという。AI生成映像以外に、ゲーム映像の転用によりAI判定を逃れてしまうものや、X上のAIチャットボットによる偽動画の誤判定も確認され、検証インフラ自体の機能不全が露呈した。なお、親イスラエルのアカウントもオンラインで偽情報を拡散しており、主にイランでの抗議や集会の古い映像を再配布し、イラン政府に対する反発やイスラエルの軍事作戦支持が増していると主張をしているという※242。

イスラエルのディアスポラ問題・反ユダヤ主義対策省の2025年6月報告書によれば、イラン政府とイスラム革命防衛隊（IRGC：Islamic Revolutionary Guard Corps）による、紛争下で世論に影響を与えることを目的としたボットネットを解明したという。Xにおける紛争関連ハッシュタグの最大60%がイラン関連アクターに由来し、ボットネットは国内向けに最高指導者ハメネイ師の権威や国民団結のメッセージを増幅させており、対イスラエル向けには報復的なナラティブを中心に展開したとされる※243。また、EDMOによれば、ボットアカウントだけでなく、国営のテヘランタイムズやFars News通信社もAI生成映像を多用したディープフェイクやミスリーディングな動画像を拡散していたという※244。

更に2026年2月28日、米国とイスラエルはイランに対する大規模攻撃を開始し、紛争が再燃した。クレムソン大学のMedia Forensics Hubは2026年3月、IRGC関連の少なくとも62アカウント（X、Instagram、Bluesky上）からなるネットワーク「From Texas to Tehran」を特定し、X上だけで5万9,403件の投稿が確認されたと報告した※245。同時期には、米国空母エイブラハム・リンカーン撃沈を主張する偽情報（米国中央軍が公式に否定※246）やネタニヤフ首相の死亡を誤認させるような虚偽の記事やAI生成画像※247、イランの攻撃によりカタールにある米国のレーダーが破壊された様子を示していると主張するAI生成画像等が拡散された※248。

米国は2025年9月以降、ベネズエラ周辺で「麻薬密輸船」に対する攻撃を繰り返して軍事的圧力を段階的に強め、2026年1月3日、ベネズエラのNicolás Maduro Moros大統領を拘束し、米国へ移送・訴追した特殊部隊による急襲作戦「Operation Absolute Resolve」を実施した※249。同作戦の実行直後にも、SNS上にはAI生成映像や過去の動画像を流用した偽・誤情報が一気に拡散された。AFP（Agence France-Presse）のファクトチェックによれば、「米軍拘束下のMaduro氏の最初の写真」とされた画像はAI生成（GoogleのSynthID電子透かしを検出）であり、「頭部に袋を被せられたMaduro氏」とされた画像は2003年のフセイン元イラク大統領拘束時の写真の流用であった※250。また、「Maduro排除を祝うベネズエラ市民」だとするAI生成動画の拡散も多

く見られた※251。NewsGuard Technologies, Inc.（以下、NewsGuard 社）は、作戦に関連する捏造・誤用の画像・動画 7 件が X だけで 2 日間に合計 1,400 万回以上閲覧されたと報告している※250。

(3) 新型コロナウイルス・反ワクチンに関する偽・誤情報

新型コロナウイルス感染症（以下、新型コロナウイルス）をめぐっては、パンデミック期に世界保健機関（WHO：World Health Organization）が「インフォデミック」と呼んだ大量の偽・誤情報や陰謀論の氾濫が発生した※252。そのうち、反ワクチンに関する偽・誤情報や虚偽的なナラティブ形成はパンデミック収束後も消滅せず、2025 年度も各地で公衆衛生上の影響を及ぼし続けている。WHO 及び UNICEF（United Nations International Children's Emergency Fund：国連児童基金）の 2026 年 2 月のプレスリリースでは、欧州・中央アジア 53 ヵ国の 2025 年麻疹症例 3 万 3,998 件の背景として、「誤情報により煽られたワクチン忌避」が指摘されている※253。日本国内でも、日本ファクトチェックセンター（JFC：Japan Fact-check Center）の検証によれば、2025 年中、新型コロナウイルス・反ワクチン関連の誤情報が継続的に拡散した。具体的には、「Meiji Seika ファルマ株式会社の新型コロナレプリコンワクチンはファイザー製の 75 倍の死亡率である※254」「フランスの研究で mRNA ワクチン接種者の重症 COVID-19 関連死亡リスクが 74% 上昇した※255」等が誤りであったと指摘されている。パンデミック収束後の現在においても、新型コロナウイルスやそこから派生した反ワクチン関連の偽・誤情報の発信・拡散は長期化していることがうかがえる。

2.3.4 偽・誤情報への対策の動向

偽・誤情報への対策は、国家・地域レベルの法制度整備、プラットフォーム事業者等の民間レベルの自主的対策、個人レベルの情報リテラシー向上の三層で進展している。2025 年度は、規制アプローチの地域的な特色がより強まった時期であった。

(1) 各国・地域の対応

国、地域別の対応では、従前より偽・誤情報対策に積極的であった EU の対策が更に進んだことが見て取れる。また、オーストラリアによる SNS の年齢制限規制を端緒に、同様の規制が各国にも波及したことが 2025 年の大きなトレンドであった。

(a) EU

EU では、2018 年以来の自主的枠組みであった「偽情報に関する行動規範（Code of Practice on Disinformation）」が、2025 年 2 月 13 日に欧州委員会等の承認を経て「デジタルサービス法（DSA：Digital Services Act）」上の「行動規範（Code of Conduct）」へ転換され、同年 7 月 1 日から発効した※256。これにより、DSA に基づき「超大規模オンラインプラットフォーム（VLOP：Very Large Online Platform）」及び「超大規模オンライン検索エンジン（VLOSE：Very Large Online Search Engine）」に指定されたサービス（Facebook、Instagram、LinkedIn、Bing、TikTok、YouTube、Google Search）を運営する事業者等にとって規範の遵守状況は DSA 上のリスク低減義務の履行を示す基準となり、独立監査の対象ともなった。また、「政治広告の透明性とターゲティングに関する規則（TTPA：Transparency and Targeting of Political Advertising）」が 2025 年 10 月 10 日から適用され、政治広告へのラベル付与、資金提供者・対象選挙・支出額等の開示が義務化された※257。これに対し Meta 社と Google 社は、法的不確実性等を理由に EU 域内での政治・選挙・社会的争点を対象とした広告の配信自体を停止するという対応を選択し※258、規制強化によりプラットフォーマーがテーマによっては広告配信を行わないという事態に至った。更に 2026 年 3 月 24 日には、行動規範に署名した事業者の初めての透明性報告書（対象期間：2025 年 7 ～ 12 月）が公表され※259、Meta 社は同報告書において、2025 年 10 月 6 日以降 EU 域内で政治・選挙・社会的争点を対象とした広告の配信を実際に停止したことを報告している※260。これにより、2025 年に強化して始動した EU の共同規制サイクルが、年度中に一定の実効性ある成果に結実したといえるだろう。

また、EU 内で影響工作等の事案が発生した国に対しても、個別に協働体制をとって即応的な対策を講じている。2024 年 11 月の大統領選挙がロシアの干渉と TikTok 上の組織的キャンペーンを理由に憲法裁判所により無効とされたルーマニアでは、2025 年 5 月の再選挙に向けて選挙即応型の対策が講じられた。欧州委員会が DSA に基づき TikTok 社への正式調査を開始し同社に対策を促したことによって、TikTok 社は政治アカウントの検出・ラベリングの強化、ルーマニア語の専門人材の増員、秘密裏に行われる影響工作への対抗と広告

の健全性を担当する選挙タスクフォースへの120名の専門家追加等の措置を講ずることとなった※261。

(b)米国

米国では連邦レベルの包括的規制が停滞する一方、州レベルの立法が加速した。非党派のオンライン政治百科事典を運営する非営利団体Ballotpediaの集計によれば、政治的ディープフェイクを規制する州法を有する州は2025年1月の21州から同年7月には28州へ増加し、ディープフェイク関連立法全体では47州が何らかの法律を制定済みである※262。多くの州法は選挙前の一定期間における候補者の合成メディアの頒布に開示義務や差し止め・罰則を課すものであり、表現の自由(合衆国憲法修正第1条)との均衡が引き続き争点となっている。

(c)オーストラリア

オーストラリアでは2024年12月11日、世界に先駆けて「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)」が施行された。同法は2021年の「オンライン安全法(Online Safety Act 2021)」にPart 4Aを新設し、特定のソーシャルメディア・プラットフォームに対し、16歳未満の利用者がアカウントを保有することを防ぐ「合理的措置(reasonable steps)」を講じる義務を課す規定を設けた※263。オーストラリアの独立規制当局であるeSafety Commissionerは、Facebook、Instagram、Snapchat、TikTok、YouTube、X、Threads、Reddit、Kick、Twitchの10プラットフォームを対象に、利用者の対象年齢に制限を設け※264、体系的な不遵守が認定された事業者に対しては最大4,950万豪ドルの民事罰が科される。偽・誤情報そのものを対象とする規制ではないが、未成年者を有害な情報環境から保護するという観点から行政が介入する規制である。

なお、2025年度中には、ニュージーランド※265、フランス、ポルトガル、スペイン※266、EU※267、ブラジルといった複数の国・地域が同様の法制度の制定もしくは検討の方向で追随しており、未成年者保護のための構造的介入が世界的に拡大している※268。

(d)日本

日本では2025年4月、「改正プロバイダ責任制限法」を改称した「情報流通プラットフォーム対処法」が施行され、大規模プラットフォーム事業者に対し、権利侵害情報への削除申出窓口の整備、対応の迅速化、削除基準の公表等が義務付けられた※269。偽・誤情報への直接の削除義務を課すものではないが、情報流通の適正化に向けた制度的基盤として位置付けられる。技術面では、総務省が「インターネット上の偽・誤情報等への対策技術の開発・実証事業(令和7年度)」を実施し、公募により技術開発主体14者、研究・調査主体6者を採択した※270。2026年3月16日には、採択された14件の開発技術を中心に成果を発信するイベントが開催され、ディープフェイク検出、コミュニティノートのデータを活用した分析基盤、災害時の偽・誤情報対策等、対策技術の社会実装に向けた取り組みが紹介された※271。偽・誤情報対策技術については、「経済安全保障重要技術育成プログラム」(通称、K Program)の「偽情報分析に係る技術の開発」でも開発が進められている※272。

なお、民間レベルでは、日本ファクトチェックセンターが2025年7月の参院選に関連して27本のファクトチェック記事を公開した※273ことに加え、同選挙では新聞社・テレビ局による検証記事が前年の衆院選比で5倍超に急増しており※274、報道機関のファクトチェック参入が本格化した点も特筆される。

(2)プラットフォーム事業者の対応

プラットフォーム事業者のレベルでは、第一に選挙対応の制度化が進んだ。Meta社は選挙運用センターと迅速対応の枠組みを作り、欧州各国選挙で運用した※275。TikTok社も各国選挙に際して選挙センターの設置や政治広告の禁止・透明性確保を進め、EUの行動規範下の迅速対応システムにも参加している※276。第二に、AI生成コンテンツや操作された情報等に関する投稿へのラベル付与施策が拡大した。X社は生成AI等によって合成または操作されたメディアの欺瞞的共有を禁ずる「Authenticity(真正性)」ポリシーを維持しており※277、2026年1月には編集・改変された動画像を含む投稿への「Manipulated Media(操作されたメディア)」警告ラベル機能の運用を開始し※278、同年3月には投稿者自身が付与する「Made with AI」ラベルも実装された※279。Meta社においても、「AI情報」ラベルやC2PA(Coalition for Content Provenance and Authenticity)等の来歴証明技術の実装が進む一方、メタデータ除去への脆弱性や検出技術の未成熟といった限界もMeta社が設置しているOversight Board(監督委員会)の審査等を通じて指摘されている※280。第三に、政治広告・社会争点

広告の制限が進んだ。EUにおけるMeta社・Google社の政治広告停止はその具体的な結果の現れである※258。第四に、AI開発企業による脅威情報の公開が定着した。OpenAI社・Google社等は影響工作等へのAI悪用を検知・遮断した事例を定期的に報告し、アカウント停止等の措置を講じるようになった※281。第五に、ユーザー参加型のコミュニティノートシステムの拡張、AI連携が進んだ。Xの機能であるコミュニティノートに関しては、X社は2025年7月1日、AIにコミュニティノートの草案を提案させる「AI Note Writer API」のパイロットを開始し、AIがノート案を起草し多様な観点を持つ人間のユーザーが公開可否を判定する「AIが書き、人間が決める」モデルを導入した※282。Meta社は、同年1月7日、第三者ファクトチェック・プログラムを終了しX型のコミュニティノートへ移行する方針を発表している※283。これに対し、デジタルヘイト対策センター（CCDH：Center for Countering Digital Hate Inc）の2024年10月の分析では、Xのコミュニティノートでは「役立つ」と評価された正確なノートの大半が一般ユーザーに表示されておらず、元の誤投稿が平均で約13倍のビューを獲得していたと報告されており※284、Regina Cazzamatta氏の学術論文※285等でもコンテンツモデレーション体制の縮小・転換が偽・誤情報の拡散余地を広げる懸念があると指摘される等、プラットフォーム事業者の対応は強化と後退が併存する複雑な様相を呈している。

(3) 個人レベルのリテラシー対策

個人レベルの対策としては、流通後の検証であるファクトチェックに加え、偽情報に接する前に典型的な情報操作手法や狙われやすいナラティブへの心理的免疫を形成するプレバンキング（事前暴露）の重要性が国際的に強調されつつある。心理的な免疫を形成するための心理的接種理論に基づく短い啓発動画の視聴が、情報操作手法の識別力を向上させることは大規模実験で確認されている※286。Google社のJigsaw部門は2024年欧州議会選挙前にスケープゴート化・脱文脈化・信用毀損といった三つの情報操作手法を扱うYouTube動画群をベルギー、フランス、ドイツ、イタリア、ポーランドの5ヵ国で展開し、これまでで最大となる1億2,000万人以上にリーチする取り組みを展開した※287。2026年3月に学術誌Communications Psychologyに掲載された12ヵ国・約2万人を対象とする検証研究では、これらの動画が高齢層（45歳以上）を含む被験者の情報操作手法識別能力と共有判断を有意に改善したことが示された※288。

日本でも、総務省は2024年の「デジタル空間における情報流通の健全性確保に関する検討会」のとりまとめ案において「プレバンキング（リテラシー向上等の事前の備え）とデバンキング（ファクトチェック等の事後検証）の両輪による対応」を素案として提示しており※289、2025年1月から19のIT事業者・関連団体と連携した官民啓発プロジェクト「DIGITAL POSITIVE ACTION」を始動している※290。総務省による偽・誤情報等への対策技術の開発・実証事業では、ゲーミフィケーションを活用した実践的ゲーム型プレバンキング技術（株式会社Classroom Adventure）の開発も採択されている※270。ファクトチェックが拡散後の「治療」であるのに対し、プレバンキングは拡散前の「予防接種」として位置付けられるが、検証が物理的に追い付かない生成AI時代において、両者を組み合わせた重層的なリテラシー施策が今後の標準となると考えられる。

2.3.5 状況のまとめと今後の見通し

本項では、これまで解説してきた事例から現況をまとめた上で、今後の見通しを述べる。

(1) 状況のまとめ

2025年度の情勢は、次の3点に集約できる。第一に、武力紛争や、紛争未満の物理空間における衝突や威圧等の事案と情報戦の同期である。ロシアによるポーランド領空侵入、インドとパキスタンの軍事衝突、イスラエル・米国とイラン間の軍事衝突、米国によるベネズエラに対する軍事作戦等の事案において、物理的事象と並行して情報戦・認知戦が展開され、交戦国同士や支援する陣営側において一体的な作戦として運用された。これが市民社会の言論空間にも一気に拡散し、物理的戦場と情報空間の戦場は地続きとなった様相である。第二に、選挙干渉の常態化であり、ドイツ・ルーマニア・モルドバ、ポーランドそして日本に至るまで、主要な選挙が外国の影響工作の標的となる事例が継続的に頻発している。第三に、対策の地域的分岐である。EUの共同規制（DSA・行動規範・TTPA）、米国の州法主導、オーストラリア年齢規制、日本の技術開発・民間検証支援と、各法域のアプローチの差異が拡大しており、それぞれの地域の法制度に根差した特色が見られる。一方で、グローバルなプラットフォーム上の脅威に対して国際的な協働の動きは進んでおらず、規制の断片化がもたらす間

隙が新たな課題となっている。

(2) 今後の見通し

2026 年度下半期にも、日本への影響が大きい政治・外交イベントが相次ぐ。2026 年 10 月のブラジル大統領選挙、11 月の米国中間選挙及び台湾統一地方選挙は、いずれもロシア・中国等による影響工作や選挙干渉の標的となることが想定される。日本については、平素より認知戦が生起していることに防衛大臣が言及するという環境にあり※291、AI 生成コンテンツを悪用した情報戦・認知戦が展開される可能性は無視できない。AI を悪用した影響工作の自動化、パーソナライズ化、及び LLM グルーミングによる AI の学習データ汚染という新たな攻撃アプローチへの対応を含め、政府のみならず、プラットフォーム事業者、報道機関、市民社会が平時から連携する総力戦的なレジリエンスの構築が急務である。

COLUMN

「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

「情報セキュリティ 10 大脅威 2026[i]」の「『組織』向け脅威」の 3 位として、「AI の利用をめぐるサイバーリスク」が初めて選出されました。この脅威名は、ランサム攻撃（1 位）や標的型攻撃（5 位）といった攻撃手法を名前に含む脅威名とは一線を画し、AI にまつわる包括的な懸念を表す名称となっています。

対話型生成 AI である ChatGPT が 2022 年に登場して以降、生成 AI に対する社会の関心の高まり、爆発的な利活用の進展により、個人の日常生活から労働環境、企業・組織の日常業務から技術開発といったあらゆる側面に AI は影響を与えつつあります。一方、サイバーセキュリティへの影響として、AI の悪用による攻撃の容易化、巧妙化、高速化等、多くの懸念が指摘されており、2025 年度はそれらが現実のものとなった年でした。こうした近年の動向を踏まえ、「AI の利用をめぐるサイバーリスク」は、満を持してランクインしたようにも見えます。

では、今後も AI に関する脅威はランクインし続けるのでしょうか?

例えば、フィッシングは、「フィッシングによる個人情報等の詐取」として「情報セキュリティ 10 大脅威　2026」の「『個人』向け脅威」に選出されていますが、「『組織』向け脅威」にはありません。しかし、フィッシングは組織への脅威に無関係な存在ではなく、むしろ深く関わりがあります。1 位のランサム攻撃にしろ、2 位のサプライチェーンや委託先を狙った攻撃にしろ、攻撃の端緒となる ID やパスワードといった認証情報の詐取にフィッシングは多用されており、そのほかのランクインしている脅威とも関連があります。

AI の影響は広範囲であることから、いずれは AI が「情報セキュリティ 10 大脅威」のランク外になるとしても、フィッシングと同じように脅威の共通要素として、背後に存在し続けることになるのでは、と考えています。

表　情報セキュリティ 10 大脅威 2026「組織」向けの脅威の順位

順位	脅威名	10 大脅威での取り扱い（2016 年以降）
1	ランサム攻撃による被害	11 年連続 11 回目
2	サプライチェーンや委託先を狙った攻撃	8 年連続 8 回目
3	AI の利用をめぐるサイバーリスク	初選出
4	システムの脆弱性を悪用した攻撃	6 年連続 9 回目
5	機密情報を狙った標的型攻撃	11 年連続 11 回目
6	地政学的リスクに起因するサイバー攻撃（情報戦を含む）	2 年連続 2 回目
7	内部不正による情報漏えい等	11 年連続 11 回目
8	リモートワーク等の環境や仕組みを狙った攻撃	6 年連続 6 回目
9	DDoS 攻撃（分散型サービス妨害攻撃）	2 年連続 7 回目
10	ビジネスメール詐欺	9 年連続 9 回目

i　https://www.ipa.go.jp/security/10threats/10threats2026.html〔2026/8/25 確認〕

※ 1　内閣官房：国家安全保障戦略について　https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf〔2026/7/17 確認〕
※ 2　サイバーセキュリティ戦略本部：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（サイバー安全保障分野での対応能力の向上に向けた有識者会議）　https://www.cyber.go.jp/pdf/policy/kihon-s/250529kikkin.pdf〔2026/8/18 確認〕
※ 3　https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/koujou_teigen/teigen.pdf〔2026/7/17 確認〕
※ 4　e-Gov 法令検索：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（令和七年法律第四十二号）　https://laws.e-gov.go.jp/law/507AC0000000042/20271122_000000000000000〔2026/7/17 確認〕
※ 5　衆議院：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　https://www.shugiin.go.jp/internet/itdb_housei.nsf/html/housei/21720250523043.htm〔2026/7/17 確認〕
※ 6　https://www.cao.go.jp/cybersecurity/pdf/kihonhoushin.pdf〔2026/7/17 確認〕
※ 7　https://www.cyber.go.jp/pdf/policy/kihon-s/250529kikkin.pdf〔2026/10/13 確認〕
※ 8　NCO：沿革　https://www.cyber.go.jp/about/history/index.html〔2026/7/17 確認〕
※ 9　https://www.ipa.go.jp/publish/wp-security/2025.html〔2026/7/17 確認〕
※ 10　NCO：サイバーセキュリティ戦略　https://www.cyber.go.jp/pdf/policy/kihon-s/cs_strategy2025.pdf〔2026/7/17 確認〕
※ 11　国会審議の過程で、衆議院において、サイバー対処能力強化法案に通信の秘密の尊重（第２条の２）等の規定を追加する修正が行われた。衆議院：閣法 第 217 回国会 4 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案に対する修正案　https://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/syuuseian/11_7CD2.htm〔2026/7/17 確認〕
※ 12　内閣官房：サイバー対処能力強化法及び同整備法について　https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf〔2026/7/17 確認〕
※ 13　https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/shin_cyber_leaflet.pdf〔2026/7/17 確認〕
※ 14　内閣官房：サイバー安全保障に関する取組（能動的サイバー防御の実現に向けた検討など）　https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html〔2026/7/17 確認〕
※ 15　特別社会基盤事業者：特定社会基盤事業者（後述）のうち、重要電子計算機（行政機関や特定社会基盤事業者等が使用する電子計算機であって、サイバー攻撃を受けた場合に、国家及び国民の安全を害し、または国民生活もしくは経済活動に多大な影響を及ぼすおそれがあるような一定のもの）を使用する者。特定社会基盤事業者とは、経済安全保障推進法に基づき指定される、特定社会基盤事業（対象 15 事業（電気、ガス、石油、水道、鉄道、貨物自動車運送、外航海運、港湾運送、航空、空港、電気通信、放送、郵便、金融、クレジットカード）のうち、特定社会基盤役務（国民生活及び経済活動の基盤となる役務であって、その安定的な提供に支障が生じた場合に国家及び国民の安全を損なう事態を生ずるおそれがあるもの）の提供を行うものとして政令で定めるもの）を行う者のうち、その使用する特定重要設備（特定社会基盤事業の用に供される設備、機器、装置またはプログラムのうち、特定社会基盤役務を安定的に提供するために重要であり、かつ我が国の外部から行われる特定社会基盤役務の安定的な提供を妨害する行為の手段として使用されるおそれがあるものとして主務省令で定めるもの）の機能が停止し、または低下した場合に、その提供する特定社会基盤役務の安定的な提供に支障が生じ、これによって国家及び国民の安全を損なう事態を生ずるおそれが大きいものとして主務省令で定める基準に該当する者。2026 年７月１日時点で 258 者。なお、2026 年 6 月 17 日、医療分野を特定社会基盤事業に追加する経済安全保障推進法の改正法が公布され、公布日から起算して１年６ヵ月を超えない範囲内において政令で定める日から施行される予定である。これにより、特定社会基盤事業は、16 事業となる。
特定社会基盤事業及び指定事業者数は、内閣府「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度について」（https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_gaiyou.pdf〔2026/7/17 確認〕）より引用した。
※ 16　内閣府：サイバー対処能力強化法の施行等に関する有識者会議　https://www.cao.go.jp/cybersecurity/kaigi/kaigi.html〔2026/7/17 確認〕
※ 17　通信情報保有機関：サイバー対処能力強化法では、次に挙げる行政機関（サイバー通信情報管理委員会を除く）と規定している。すなわち、「内閣府」「選別後通信情報（取得した通信情報についての自動選別により得られたもの）の提供を受けた行政機関であって、現に当該選別後通信情報（その全部又は一部を複製し、又は加工した選別後通信情報を含む）を保有しているもの。」「選別後通信情報を含む総合整理分析情報（報告等情報、選別後通信情報、提供用選別後情報、協議会を通じて得た情報その他の情報が重要電子計算機に対する特定不正行為よる被害の防止に有効に活用されるよう、当該情報整理及び分析を行うもの）の提供を受けた国の行政機関であって、現に当該選別後通信情報（その全部又は一部を複製し、又は加工した選別後通信情報を含む）を保有しているもの。」の３項目である。
※ 18　https://www.cao.go.jp/cybersecurity/pdf/kihonhoushin_gaiyou.pdf〔2026/7/17 確認〕
※ 19　https://laws.e-gov.go.jp/law/504AC0000000043〔2026/7/17 確認〕
※ 20　https://laws.e-gov.go.jp/law/506AC0000000027〔2026/7/17 確認〕
※ 21　内閣府：経済安全保障推進法に基づく重要物資の安定的な供給の確保（サプライチェーン強靱化）に関する制度全般や技術流出防止について　https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/supply_chain/doc/sc_gaiyou.pdf〔2026/7/17 確認〕
※ 22　内閣府：経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度について https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_gaiyou.pdf〔2026/7/17 確認〕
※ 23　内閣官房:経済安全保障法制に関する有識者会議（令和4年度～）　https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/4index.html〔2026/7/17 確認〕
※ 24-1　https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r8_dai15/teigen.pdf〔2026/7/17 確認〕
※ 24-2　内閣府：概要　https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/doc/houangaiyo.pdf〔2026/8/18 確認〕
※ 25　https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/pdf/torimatome.pdf〔2026/7/17 確認〕
※ 26　セキュリティ・クリアランス制度：国家における情報保全措置の一環として、政府が保有する安全保障上重要な情報として指定された情報に対して、アクセスする必要がある者のうち、情報を漏らすおそれがないという信頼性を確認した者の中で取り扱うとする制度。
内閣府：いわゆる「セキュリティ・クリアランス」について　https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/sankou_clearance.pdf〔2026/7/17 確認〕
※ 27　国会審議の過程で、衆議院において、内閣総理大臣による「重要経済安保情報の指定及びその解除、適性評価の実施並びに適合事業者の認定の状況」の国会への報告（第 19 条）等を追加する修正が行われた。衆議院：閣法 第 213 回国会 24 重要経済安保情報の保護及び活用に関する法律案に対する修正案（自民、立憲、維教、公明、国民、有志）　https://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/syuuseian/1_8466.htm〔2026/7/17 確認〕
※ 28　https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/sankou_hyouka.pdf〔2026/7/17 確認〕
※ 29　内閣府：重要経済安保情報の保護及び活用に関する法律の概要　https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/gaiyo.pdf〔2026/7/17 確認〕
※ 30　内閣府：重要経済安保情報の指定及びその解除、適性評価の実施並びに適合事業者の認定に関し、統一的な運用を図るための基準の策定について　https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/kijun.pdf〔2026/7/17 確認〕
※ 31　内閣府：重要経済安保情報の保護及び活用に関する法律（重要経済安保情報保護活用法）　https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/hogokatsuyou.html〔2026/7/17 確認〕
※ 32　内閣府：特定秘密・重要経済安保情報の検証及び監察　https://www8.cao.go.jp/kenshoukansatsu/index.html〔2026/7/17 確認〕
※ 33　独立公文書管理監、情報保全監察室：是正の求め等について　https://www8.cao.go.jp/kenshoukansatsu/zesei.pdf〔2026/7/17 確認〕
※ 34　2025 年中、重要経済安保情報の指定は９機関 20 件、指定を解除したものは１件。また、重要経済安保情報が記録された行政文書は８機関計 43 件保有されており、国立公文書館等への移管件数０件、重要経済安保情報行政文書ファイル等の廃棄件数０件。通報窓口に寄せられた違反行為に関する通報件数０件。更に、適性評価の実施件数は２機関・18 件（適合事業者の従業者は０件）、適性評価調査を内閣総理大臣に求めた行政機関は 11 機関・217 件、評価対象者が適性評価の実施に同意しなかった件数は３件、同意が取り下げられた件数は２件であった。
内閣府：国会への報告　https://www.cao.go.jp/keizai_anzen_hosho/kokkaihoukoku/kokkaihoukoku.html〔2026/7/17 確認〕
※ 35　経済産業省：「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再改訂版」を公表しました　https://www.meti.go.jp/press/2025/05/20250530010/20250530010.html〔2026/7/17 確認〕
※ 36　経済産業省：経済安全保障に関する産業・技術基盤強化アクショ

ンプラン再改訂の概要　https://www.meti.go.jp/policy/economy/economic_security/actionplangaiyor.pdf〔2026/7/17 確認〕
※ 37 経済産業省：「経済安全保障経営ガイドライン（第 1 版）」を取りまとめました　https://www.meti.go.jp/press/2025/01/20260123004/20260123004.html〔2026/7/17 確認〕
※ 38 経済産業省：経済安全保障グローバルフォーラム・ウィークス　https://www.meti.go.jp/policy/economy/economic_security/gfw/index.html〔2026/7/17 確認〕
※ 39 https://www.meti.go.jp/files/900018891.pdf〔2026/7/17 確認〕
※ 40 BBC：Google achieves AI 'breakthrough' by beating Go champion　https://www.bbc.com/news/technology-35420579〔2026/7/10 確認〕
CNET：AlphaGo wins a close one to wrap up battle of man vs. machine　https://www.cnet.com/tech/tech-industry/google-alphago-artificial-intelligence-victor-in-game-of-man-vs-machine/〔2026/7/10 確認〕
日本経済新聞：囲碁 AI が 3 戦全勝、世界最強プロを圧倒　https://www.nikkei.com/article/DGXLASFG27H6L_X20C17A5000000/〔2026/7/10 確認〕
※ 41 CNBC：On ChatGPT's one-year anniversary, it has more than 1.7 billion users—here's what it may do next　https://www.cnbc.com/2023/11/30/chatgpts-one-year-anniversary-how-the-viral-ai-chatbot-has-changed.html〔2026/7/10 確認〕
※ 42 IPA：情報セキュリティ 10 大脅威 2026　https://www.ipa.go.jp/security/10threats/10threats2026.html〔2026/7/10 確認〕
※ 43 総務省、経済産業省による「AI 事業者ガイドライン（第 1.2 版）」（https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20260331_1.pdf〔2026/7/10 確認〕）の「第 1 部 AI とは」の「関連する用語」から引用。
※ 44 Jared Kaplan et al.：Scaling Laws for Neural Language Models　https://arxiv.org/abs/2001.08361〔2026/7/10 確認〕
※ 45 Emily M. Bender et al.：On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?　https://dl.acm.org/doi/10.1145/3442188.3445922〔2026/7/10 確認〕
※ 46 International Business Machines Corporation：推論モデルとは　https://www.ibm.com/jp-ja/think/topics/reasoning-model〔2026/7/10 確認〕
※ 47 Jason Wei et al.：Chain-of-Thought Prompting Elicits Reasoning in Large Language Models　https://proceedings.neurips.cc/paper/2022/hash/9d5609613524ecf4f15af0f7b31abca4-Abstract-Conference.html〔2026/7/10 確認〕
※ 48 OpenAI 社：OpenAI o1-preview が登場　https://openai.com/ja-JP/index/introducing-openai-o1-preview/〔2026/7/10 確認〕
Google 社：Gemini 2.5 Flash で開発を始める　https://developers.googleblog.com/ja/start-building-with-gemini-25-flash/〔2026/7/10 確認〕
Anthropic 社：Claude 3.7 Sonnet and Claude Code　https://www.anthropic.com/news/claude-3-7-sonnet〔2026/7/10 確認〕
※ 49 遠藤聡志（LifePrompt, Inc.）：【首席超え・満点続出】2026 年度東大・京大の入試問題を AI（ChatGPT / Gemini / Claude）に解かせてみた【採点協力：河合塾】　https://note.com/lifeprompt/n/n85674c186fbc〔2026/7/10 確認〕
※ 50 Google 社：Image editing in Gemini just got a major upgrade　https://blog.google/products-and-platforms/products/gemini/updated-image-editing-model/〔2026/7/10 確認〕
※ 51 OpenAI 社：Sora 2 が公開　https://openai.com/ja-JP/index/sora-2/〔2026/7/10 確認〕
※ 52 Google 社：Introducing Veo 3.1 and advanced capabilities in Flow　https://blog.google/innovation-and-ai/products/veo-updates-flow/〔2026/7/10 確認〕
※ 53 Google 社：Gemini Live に動画と画面共有機能が追加　https://blog.google/intl/ja-jp/company-news/technology/2025gemini-live/〔2026/7/10 確認〕
※ 54 Microsoft 社：Copilot on Windows: Vision Desktop Share begins rolling out to Windows Insiders　https://blogs.windows.com/windows-insider/2025/07/15/copilot-on-windows-vision-desktop-share-begins-rolling-out-to-windows-insiders/〔2026/7/10 確認〕
※ 55 AI エージェントよりも包括的かつ進化的な概念として複数の AI エージェントによるエージェンティック AI もある。
※ 56 OpenAI 社：ChatGPT エージェントが登場：研究とアクションをつなぐ新たな架け橋　https://openai.com/ja-JP/index/introducing-chatgpt-agent/〔2026/7/10 確認〕
※ 57 Microsoft 社：Build 2025: Agents in Microsoft 365 announcements　https://techcommunity.microsoft.com/blog/microsoft365copilotblog/build-2025-agents-in-microsoft-365-announcements/4414281〔2026/7/10 確認〕
※ 58 Anthropic 社：The work behind your best work　https://claude.com/ja/product/cowork〔2026/7/10 確認〕
※ 59 GitHub, Inc.：GitHub Copilot：新しいコーディングエージェント　https://github.blog/jp/2025-05-20-github-copilot-meet-the-new-coding-agent/〔2026/7/10 確認〕
※ 60 Anthropic 社：Claude 3.7 Sonnet and Claude Code　https://www.anthropic.com/news/claude-3-7-sonnet〔2026/7/10 確認〕
※ 61 https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20260331_report.html〔2026/7/10 確認〕
※ 62 https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20260331_3.pdf〔2026/7/10 確認〕
※ 63 朝日新聞：津波警報の発表中にグーグル検索、AI が「すべて解除」と誤情報　https://www.asahi.com/articles/ASTD933Y2TD9OXIE008M.html〔2026/7/10 確認〕
※ 64 日本航空株式会社：メールサービスの誤った翻訳・要約に関するお問い合わせについて　https://www.jal.co.jp/jp/ja/info/2025/other/250711/〔2026/7/10 確認〕
※ 65 Tom's Hardware：Google's Agentic AI wipes user's entire HDD without permission in catastrophic failure　— cache wipe turns into mass deletion event as agent apologizes: "I am absolutely devastated to hear this. I cannot express how sorry I am"　https://www.tomshardware.com/tech-industry/artificial-intelligence/googles-agentic-ai-wipes-users-entire-hard-drive-without-permission-after-misinterpreting-instructions-to-clear-a-cache-i-am-deeply-deeply-sorry-this-is-a-critical-failure-on-my-part〔2026/7/10 確認〕
※ 66 The Economic Times：AI goes rogue: Replit coding tool deletes entire company database, creates fake data for 4,000 users　https://economictimes.indiatimes.com/news/new-updates/ai-goes-rogue-replit-coding-tool-deletes-entire-company-database-creates-fake-data-for-4000-users/articleshow/122830424.cms〔2026/7/10 確認〕
※ 67 Proskauer：AI Bias Lawsuit Against Workday Reaches Next Stage as Court Grants Conditional Certification of ADEA Claim　https://www.lawandtheworkplace.com/2025/06/ai-bias-lawsuit-against-workday-reaches-next-stage-as-court-grants-conditional-certification-of-adea-claim/〔2026/7/10 確認〕
※ 68 Becker's Payer：Judge orders UnitedHealth to hand over documents in AI coverage denial case　https://www.beckerspayer.com/legal/judge-orders-unitedhealth-to-hand-over-broad-discovery-in-ai-coverage-denial-case/〔2026/7/10 確認〕
※ 69 CNN.co.jp：会計担当が38億円を詐欺グループに送金、ビデオ会議のCFOは偽物　香港　https://www.cnn.co.jp/world/35214839.html〔2026/7/10 確認〕
※ 70 この事例は「情報セキュリティ白書 2025」の「2.1.4（2）（c）AI を用いた認知領域への攻撃」においても採り上げたが、金額規模や話題性から改めて言及した。
※ 71 Proofpoint, Inc.：AI で社長の音声を学習した日本語によるボイスフィッシング　https://www.proofpoint.com/jp/email-and-cloud-threats/voice-phishing-with-AI-learning-ceos〔2026/7/10 確認〕
※ 72 読売新聞オンライン：IT企業のオンライン採用面接、生成AIで他人になりすまし…実在人物の写真や履歴書悪用か　https://www.yomiuri.co.jp/national/20260319-GYT1T00020/〔2026/7/10 確認〕
※ 73 FBI：North Korean IT Worker Threats to U.S. Businesses　https://www.fbi.gov/investigate/cyber/alerts/2025/north-korean-it-worker-threats-to-u-s-businesses〔2026/7/10 確認〕
※ 74 Validin, LLC："Hello? I can't hear you": Investigating UNC1069's Fake Meeting Tactics　https://www.validin.com/blog/i_cant_hear_you_unc1069/〔2026/7/10 確認〕
※ 75 警察庁：令和 7 年におけるサイバー空間をめぐる脅威の情勢等について　https://www.npa.go.jp/bureau/cyber/pdf/R07_cyber_jousei.pdf〔2026/7/10 確認〕
※ 76 読売新聞オンライン：生成AI作成のわいせつポスターをネットで販売か、男女4人を逮捕…「手軽に稼げコスパよかった」　https://www.yomiuri.co.jp/national/20250415-OYT1T50070/〔2026/7/10確認〕
※ 77 読売新聞オンライン：卒業アルバム加工した偽の性的画像SNS拡散、一部は小中高生らが作成…警察庁がAIサイト調査　https://www.yomiuri.co.jp/national/20250831-OYT1T50010/〔2026/7/10確認〕
※ 78 Forbes：Pedophiles Are Using AI To Turn Children's Social Media Photos Into CSAM　https://www.forbes.com/sites/thomasbrewster/2025/04/08/pedophiles-use-ai-to-turn-kids-social-media-photos-into-csam/〔2026/7/10 確認〕
※ 79 Robinson+Cole：Lawsuit Alleges Fireflies.AI Corp. Illegally

Collects Biometric Data from Virtual Meetings https://www.dataprivacyandsecurityinsider.com/2025/12/lawsuit-alleges-fireflies-ai-corp-illegally-collects-biometric-data-from-virtual-meetings/〔2026/7/10 確認〕

※ 80 Fisher Phillips：Job Applicants Sue AI Screening Company for FCRA Violations: 5 Key Takeaways for Employers https://www.fisherphillips.com/en/insights/insights/job-applicants-sue-ai-screening-company-for-fcra-violations〔2026/7/10 確認〕

※ 81 出典に当時のレートでの日本円換算の記載がある場合を除いて、本白書では 1 ドル 160 円として換算している。

※ 82 Reuters：US judge upholds $243 million verdict against Tesla over fatal Autopilot crash https://www.reuters.com/world/us-judge-upholds-243-million-verdict-against-tesla-over-fatal-autopilot-crash-2026-02-20/〔2026/7/10 確認〕

※ 83 ITmedia：ChatGPT の医療アドバイスで薬を過剰摂取、米国で 19 歳大学生が死亡　遺族が OpenAI 提訴 https://www.itmedia.co.jp/news/articles/2605/14/news054.html〔2026/7/10 確認〕

※ 84 産経新聞：「チャット GPT との対話影響」で米の 16 歳自殺　両親がオープン AI などに損害賠償請求 https://www.sankei.com/article/20250828-SY34TZAYN5MVJJ52YOHEG2HQP4/〔2026/7/10 確認〕

※ 85 産経新聞：「チャット GPT」との対話に没頭した男、母親を殺害して自殺　被害妄想が悪化と米紙報道 https://www.sankei.com/article/20250829-CXPVOBSXXBLHNPDCY47IELDKTY/〔2026/7/10 確認〕

※ 86 Reuters：フロリダ州銃乱射の遺族がオープンAI提訴、「チャットGPTが犯行助長」 https://jp.reuters.com/world/us/Q764EE00GNOPBOX3TIJ42DLLXU-2026-05-12/〔2026/7/10 確認〕

※ 87 CNET Japan：仕事で AI を使いすぎると「自分の能力」に自信が持てなくなる? 米心理学会が報告 https://japan.cnet.com/article/35246689/〔2026/7/10 確認〕

※ 88 CNET Japan：ディズニーとユニバーサル、AI 画像めぐり Midjourney を提訴 --「盗作の底なし穴」と非難 https://japan.cnet.com/article/35234163/〔2026/7/10 確認〕

※ 89 https://aja.gr.jp/wp-content/uploads/2025/10/30269151d7cdc6e9bcaeaace2a517c33.pdf〔2026/7/10 確認〕

※ 90 OpenAI 社：Sora の提供終了について知っておくべきこと https://help.openai.com/ja-jp/articles/20001152-what-to-know-about-the-sora-discontinuation〔2026/7/10 確認〕

※ 91 ASCII：バイトダンス、性能おばけの動画生成 AI「Seedance 2.0」展開停止　著作権問題で https://ascii.jp/elem/000/004/381/4381362/〔2026/7/10 確認〕

※ 92 日経新聞：日経・朝日「AI 検索で著作権侵害」、米新興側は争う姿勢　地裁で初弁論 https://www.nikkei.com/article/DGXZQOUD0715F0X00C26A5000000/〔2026/7/10 確認〕

※ 93 CNN.co.jp：最新ChatGPTであふれる「ジブリ風」AI画像、威力示す一方で著作権問題も再燃 https://www.cnn.co.jp/style/arts/35231124.html〔2026/7/10 確認〕

※ 94 文化庁：文化審議会 著作権分科会 法制度小委員会「AI と著作権に関する考え方について」【概要】 https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/94057901_01.pdf〔2026/7/10 確認〕

※ 95 WIRED：Anthropic、AI 著作権訴訟の和解で少なくとも 15 億ドルを支払いへ https://wired.jp/article/anthropic-settlement-lawsuit-copyright/〔2026/7/10 確認〕

※ 96 文化庁：AI と著作権について https://www.bunka.go.jp/seisaku/chosakuken/aiandcopyright.html〔2026/7/10 確認〕

※ 97 Courthouse News Service：Supreme Court denies appeal in AI-generated art case https://courthousenews.com/supreme-court-denies-appeal-in-ai-generated-art-case/〔2026/7/10 確認〕

※ 98 読売新聞オンライン：生成AIで作った画像を無断複製の疑い、27歳男を書類送検…「著作権あり」として初の摘発 https://www.yomiuri.co.jp/national/20251120-OYT1T50104/〔2026/7/10 確認〕

※ 99 The San Francisco Standard：'White-collar recession': Benioff says Salesforce won't hire engineers this year due to AI https://sfstandard.com/2025/02/27/salesforce-marcbenioff-layoffs-tech-agents/〔2026/7/10 確認〕

※ 100 GeekWire：'It's culture': Amazon CEO says massive corporate layoffs were about agility — not AI or cost-cutting https://www.geekwire.com/2025/its-culture-amazon-ceo-says-massive-corporate-layoffs-were-about-agility-not-ai-or-cost-cutting/〔2026/7/10 確認〕

※ 101 読売新聞オンライン：生成されたAI女優「ティリー・ノーウッド」に複数タレント事務所が関心…俳優らが懸念表明 https://www.yomiuri.co.jp/world/20251003-OYT1T50108/〔2026/7/10 確認〕

※ 102 Merriam-Webster, Inc.：2025 Word of the Year: Slop https://www.merriam-webster.com/wordplay/word-of-the-year〔2026/7/10 確認〕

※ 103 東洋経済：「これは営業じゃない！ 業務妨害だ」 迷惑な "AI 営業 " に中小企業の社長が激怒したワケ《背景に AI の利用拡大》送信先企業にもたらされる 3 つの問題 https://toyokeizai.net/articles/-/870844?display=b〔2026/7/10 確認〕

※ 104 読売新聞オンライン：生成 AI が作った偽「オススメ本」をアメリカの新聞社がそのまま掲載、購読者から怒りの声が相次ぐ https://www.yomiuri.co.jp/world/nieman/20250522-OYT1T50160/〔2026/7/10 確認〕

※ 105 読売新聞オンライン：共同通信、生成AIで加工の「子ガメをくわえるタヌキ」の写真を配信取り消し…加盟社の指摘で判明 https://www.yomiuri.co.jp/national/20251102-OYT1T50089/〔2026/7/10 確認〕

※ 106 Kobi Hackenburg et al.：The levers of political persuasion with conversational artificial intelligence https://www.science.org/doi/abs/10.1126/science.aea3884〔2026/7/10 確認〕

※ 107 Dhruv Agarwal et al.：AI Suggestions Homogenize Writing Toward Western Styles and Diminish Cultural Nuances https://dl.acm.org/doi/10.1145/3706598.3713564〔2026/7/10 確認〕

※ 108 IEA：Key Questions on Energy and AI https://www.iea.org/reports/key-questions-on-energy-and-ai〔2026/7/10 確認〕

※ 109 IEA：AI and climate change https://www.iea.org/reports/energy-and-ai/ai-and-climate-change〔2026/7/10 確認〕

※ 110 IEA: The Netherlands https://www.iea.org/countries/the-netherlands/emissions〔2026/7/10 確認〕

※ 111 Microsoft 社：2025 Environmental Sustainability Report https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/2025-Microsoft-Environmental-Sustainability-Report.pdf#page=04〔2026/7/10 確認〕

※ 112 GOV.UK：AI Safety Summit 2023 https://www.gov.uk/government/topical-events/ai-safety-summit-2023

※ 113 総務省・経済産業省による「AI 事業者ガイドライン（第 1.2 版）」の「第2部 AI により目指すべき社会及び各主体が取り組む事項」の「C. 共通の指針」を参照されたい。

※ 114 日本AISI:AI セーフティに関する評価観点ガイド（第 1.10 版） 2.2 AI セーフティにおける重要要素 https://aisi.go.jp/assets/pdf/ai_safety_eval_v1.10_ja.pdf〔2026/7/10 確認〕

※ 115 日本 AISI：AI セーフティに関する評価観点ガイド（第 1.10 版）の公開 https://aisi.go.jp/output/output_information/250328_1/〔2026/7/10 確認〕

※ 116 日本 AISI：AI セーフティ評価のための評価ツールを OSS として公開 https://aisi.go.jp/output/output_information/250912/〔2026/7/10 確認〕

※ 117 日本 AISI：事業実証 WG の取組について https://aisi.go.jp/assets/pdf/20251003_2.pdf〔2026/7/10 確認〕

※ 118 日本 AISI：AI セーフティ年次レポート 2025 https://aisi.go.jp/assets/pdf/j-aisi_report_2025_ja.pdf〔2026/7/10 確認〕

※ 119 英国 AISI：International consensus and open questions in AI evaluations https://www.aisi.gov.uk/blog/international-ai-network-consensus-and-open-questions〔2026/7/10 確認〕

※ 120 例えば、ISO 31000:2018（JIS Q 31000:2019）が挙げられる。

※ 121 総務省、経済産業省：AI 事業者ガイドラインの令和7年度更新内容 https://www.soumu.go.jp/main_content/001059300.pdf〔2026/7/10 確認〕

※ 122 https://aisi.go.jp/output/output_framework/260317/〔2026/7/10 確認〕

※ 123 広島 AI プロセス：報告枠組み https://www.soumu.go.jp/hiroshimaaiprocess/report.html〔2026/7/10 確認〕

※ 124 広島 AI プロセス：フレンズグループ https://www.soumu.go.jp/hiroshimaaiprocess/supporters.html〔2026/7/10 確認〕

※ 125 一般財団法人日本規格協会：JIS Q 42001:2025 情報技術－人工知能－マネジメントシステム https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=JIS+Q+42001%3A2025〔2026/7/10 確認〕

※ 126 一般財団法人日本規格協会：ISO/IEC 42006:2025 情報技術－人工知能－人工知能マネジメントシステムの審査及び認証を行う機関に対する要求事項 https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=ISO%2FIEC+42006%3A2025〔2026/7/10 確認〕

※ 127 一般財団法人日本規格協会：ISO/IEC 42005:2025 情報技術－人工知能 (AI) － AI システムの影響評価 https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=ISO%2FIEC+42005%3A2025〔2026/7/10 確認〕

※ 128 日本 AISI：適合性評価サブワーキンググループ（適合性評価 SWG） 2025 年度活動報告書 https://aisi.go.jp/assets/pdf/

conformity_assessment_swg_report_ja.pdf〔2026/7/10 確認〕
※ 129 Federal Register：Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence〔2026/7/10 確認〕
※ 130 The White House：Removing Barriers to American Leadership in Artificial Intelligence https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/〔2026/7/10 確認〕
※ 131 The White House：America's AI Action Plan https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf〔2026/7/10 確認〕
※ 132 U.S. Department of Commerce：Statement from U.S. Secretary of Commerce Howard Lutnick on Transforming the U.S. AI Safety Institute into the Pro-Innovation, Pro-Science U.S. Center for AI Standards and Innovation https://www.commerce.gov/news/press-releases/2025/06/statement-us-secretary-commerce-howard-lutnick-transforming-us-ai〔2026/7/10 確認〕
※ 133 EU：Regulation (EU) 2024/1689 https://eur-lex.europa.eu/eli/reg/2024/1689/oj〔2026/7/10 確認〕
※ 134 JETRO：EU の AI 規則、禁止される AI 利用のルールが適用開始に https://www.jetro.go.jp/biznews/2025/02/af0786d0eca9e961.html〔2026/7/10 確認〕
※ 135 European Commission：General-Purpose AI Code of Practice now available https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1787〔2026/7/10 確認〕
※ 136 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〔2026/7/10 確認〕
※ 137 GOV.UK：AI Opportunities Action Plan https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan〔2026/7/10 確認〕
※ 138 GOV.UK：Tackling AI security risks to unleash growth and deliver Plan for Change https://www.gov.uk/government/news/tackling-ai-security-risks-to-unleash-growth-and-deliver-plan-for-change〔2026/7/10 確認〕
※ 139 国立研究開発法人新エネルギー・産業技術総合開発機構：次世代人工知能発展計画（仮訳） https://www.nedo.go.jp/content/100903937.pdf〔2026/7/10 確認〕
※ 140 Merics：China's drive toward self-reliance in artificial intelligence: from chips to large language models https://merics.org/en/report/chinas-drive-toward-self-reliance-artificial-intelligence-chips-large-language-models〔2026/7/10 確認〕
※ 141 JETRO：中国、「AI プラス」行動の徹底に関する意見発表、6重点分野で実施強化 https://www.jetro.go.jp/biznews/2025/09/8431c1ceb01ef8e8.html〔2026/7/10 確認〕
時事通信社：【中国】政府、主要産業にAI融合戦略 行動指針発表 https://www.jiji.com/jc/article?k=2025090100225〔2026/7/10 確認〕
※ 142 BiT & Company（消費者庁委託調査）：令和6年度海外主要国における消費者保護に関する生成AI関連の規制等の調査業務 報告書 第8章 中国 https://www.caa.go.jp/policies/future/national_research/assets/caa_futurer101_250605_10.pdf〔2026/7/10 確認〕
※ 143 人民網日本語版：中国で9月1日から AI で生成・合成したコンテンツへのラベル付け義務化へ https://j.people.com.cn/n3/2025/0321/c94475-20292366.html〔2026/7/10 確認〕
※ 144 内閣府：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） https://www8.cao.go.jp/cstp/ai/ai_act/ai_act.html〔2026/7/10 確認〕
※ 145 https://www8.cao.go.jp/cstp/ai/ai_plan/ai_plan.html〔2026/7/10 確認〕
※ 146 デジタル庁：全府省庁の約 18 万人の政府職員を対象としたガバメント AI（源内）の大規模実証を開始します https://www.digital.go.jp/news/2d69c287-2897-46d8-a28f-ea5a1fc9bce9〔2026/7/10 確認〕
※ 147 内閣府：人工知能基本計画 第3章 第3節 AI ガバナンスの主導 https://www8.cao.go.jp/cstp/ai/ai_plan/aiplan_20251223.pdf〔2026/7/10 確認〕
※ 148 トレンドマイクロ株式会社：TrendAI AI セキュリティレポート 2026 ～ AI エコシステムの断層～ https://www.trendmicro.com/ja_jp/research/26/c/fault-lines-in-the-ai-ecosystem-trendai-state-of-ai-security-report.html〔2026/7/10 確認〕
※ 149 OWASP Foundation, Inc.：OWASP Top 10 for LLM Applications 2025 LLM01:2025 Prompt Injection https://genai.owasp.org/resource/owasp-top-10-for-llm-applications-2025/〔2026/7/10 確認〕
※ 150 PC Watch：「メールを送るだけ」で AI 悪用攻撃可な Microsoft 365 Copilot の脆弱性。緊急で対策済み https://pc.watch.impress.co.jp/docs/news/2022498.html〔2026/7/10 確認〕
※ 151 Check Point Software Technologies Ltd.：AI Evasion: The Next Frontier of Malware Techniques https://blog.checkpoint.com/artificial-intelligence/ai-evasion-the-next-frontier-of-malware-techniques/〔2026/7/10 確認〕
※ 152 日本経済新聞：論文内に秘密の命令文、AI に「高評価せよ」日韓米など有力 14 大学で https://www.nikkei.com/article/DGXZQOUC13BCW0T10C25A6000000/〔2026/7/10 確認〕
※ 153 ITmedia：“ブラウザを自律操作する AI”が暴走 「要約して」と入力しただけなのにパスワードが盗まれた その手口とは? https://www.itmedia.co.jp/news/articles/2509/03/news027.html〔2026/7/10 確認〕
※ 154 PromptArmor：Claude Cowork Exfiltrates Files https://www.promptarmor.com/resources/claude-cowork-exfiltrates-files〔2026/7/10 確認〕
※ 155 OWASP Foundation, Inc.：Code Injection https://owasp.org/www-community/attacks/Code_Injection〔2026/7/10 確認〕
※ 156 Python Software Foundation：pickle --- Python オブジェクトの直列化 https://docs.python.org/ja/3/library/pickle.html〔2026/7/10 確認〕
※ 157 Red Hat, LLC：CVE-2025-49655 https://access.redhat.com/security/cve/cve-2025-49655〔2026/7/10 確認〕
※ 158 Sonatype, Inc.：CVE-2025-1716 https://www.sonatype.com/security-advisories/cve-2025-1716〔2026/7/10 確認〕
JFrog Ltd：PyTorch Users at Risk: Unveiling 3 Zero-Day PickleScan Vulnerabilities https://jfrog.com/blog/unveiling-3-zero-day-vulnerabilities-in-picklescan/〔2026/7/10 確認〕
SECDIM：CVE-2025-46417: Bypassing AI Model Scanners and Exfiltrate Sensitive Data https://secdim.com/blog/post/cve-2025-46417-bypassing-ai-model-scanners-and-exfiltrate-sensitive-data-15594/〔2026/7/10 確認〕
※ 159 Palo Alto Networks, Inc.：最新の AI/ML フォーマットとライブラリによるリモート コード実行 https://unit42.paloaltonetworks.com/ja/rce-vulnerabilities-in-ai-python-libraries/〔2026/7/10 確認〕
※ 160 International Business Machines Corporation：知識蒸留とは https://www.ibm.com/jp-ja/think/topics/knowledge-distillation〔2026/7/10 確認〕
※ 161 Anthropic 社：Usage Policy https://www.anthropic.com/legal/aup〔2026/7/10 確認〕
Google 社:Gemini API 追加利用規約 https://ai.google.dev/gemini-api/terms〔2026/7/10 確認〕
OpenAI 社:利用規約 https://openai.com/ja-JP/policies/row-terms-of-use/〔2026/7/10 確認〕
※ 162 Google 社：GTIG AI Threat Tracker: Distillation, Experimentation, and (Continued) Integration of AI for Adversarial Use https://cloud.google.com/blog/topics/threat-intelligence/distillation-experimentation-integration-ai-adversarial-use〔2026/7/10 確認〕
Anthropic 社：Detecting and preventing distillation attacks https://www.anthropic.com/news/detecting-and-preventing-distillation-attacks〔2026/7/10 確認〕
※ 163 Office of Science and Technology Policy：Adversarial Distillation of American AI Models https://whitehouse.gov/wp-content/uploads/2026/04/NSTM-4.pdf〔2026/7/10 確認〕
※ 164 CNN：White House accuses China of copying American AI models in 'industrial-scale' campaign https://edition.cnn.com/2026/04/23/tech/white-house-accuses-china-copying-american-ai〔2026/7/10 確認〕
※ 165 Socket, Inc.：The Rise of Slopsquatting: How AI Hallucinations Are Fueling a New Class of Supply Chain Attacks https://socket.dev/blog/slopsquatting-how-ai-hallucinations-are-fueling-a-new-class-of-supply-chain-attacks〔2026/7/10 確認〕
※ 166 Joseph Spracklen et al.：We Have a Package for You! A Comprehensive Analysis of Package Hallucinations by Code Generating LLMs https://www.usenix.org/conference/usenixsecurity25/presentation/spracklen〔2026/7/10 確認〕
※ 167 Koi Security：PhantomRaven: NPM Malware Hidden in Invisible Dependencies https://www.koi.ai/blog/phantomraven-npm-malware-hidden-in-invisible-dependencies〔2026/7/10 確認〕
※ 168 https://aisi.go.jp/output/output_security/known_attacks_and_impacts/〔2026/7/10 確認〕
※ 169 https://aisi.go.jp/assets/pdf/Known_Attacks_and_Their_Impacts_on_AI_Systems_V2_JP.pdf〔2026/7/10 確認〕

※ 170 The Hacker News：Critical LangChain Core Vulnerability Exposes Secrets via Serialization Injection https://thehackernews.com/2025/12/critical-langchain-core-vulnerability.html〔2026/7/10 確認〕
※ 171 Cymulate Ltd.：EscapeRoute: Breaking the Scope of Anthropic's Filesystem MCP Server (CVE-2025-53109 & CVE-2025-53110) https://cymulate.com/blog/cve-2025-53109-53110-escaperoute-anthropic/〔2026/7/10 確認〕
※ 172 JPCERT/CC：JVNVU#99749963 CrewAI における複数の脆弱性 https://jvn.jp/vu/JVNVU99749963/〔2026/7/10 確認〕
※ 173 Cyber Security News：15,200 OpenClaw Control Panels with Full System Access Exposed to the Internet https://cybersecuritynews.com/openclaw-control-panels-exposed/〔2026/7/10 確認〕
※ 174 SafeDep Inc.：Malicious litellm 1.82.8: Credential Theft and Persistent Backdoor https://safedep.io/malicious-litellm-1-82-8-analysis/〔2026/7/10 確認〕
※ 175 英 国 AISI：How fast is autonomous AI cyber capability advancing? https://www.aisi.gov.uk/blog/how-fast-is-autonomous-ai-cyber-capability-advancing〔2026/7/10 確認〕
※ 176 NCSC：Impact of AI on cyber threat from now to 2027 https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027〔2026/7/10 確認〕
※ 177 Proofpoint, Inc.：サイバー犯罪者が AI ウェブサイト作成アプリをフィッシングに悪用 https://www.proofpoint.com/jp/blog/threat-insight/cybercriminals-abuse-ai-website-creation-app-phishing〔2026/7/10 確認〕
※ 178 Palo Alto Networks, Inc.：AI のデュアルユースのジレンマ：悪意ある LLM https://unit42.paloaltonetworks.com/ja/dilemma-of-ai-malicious-llm/〔2026/7/10 確認〕
※ 179 読売新聞オンライン：「快活CLUB」サイバー攻撃、AI悪用し会員情報盗んだ疑いで高2を再逮捕へ…自作プログラムを「チャットGPT」で改善か https://www.yomiuri.co.jp/national/20251204-GYT1T00037/〔2026/7/10 確認〕
※ 180 Anthropic 社：Disrupting the first reported AI-orchestrated cyber espionage campaign https://www.anthropic.com/news/disrupting-AI-espionage〔2026/7/10 確認〕
※ 181 株式会社ラック：大規模な AI 主導サイバー攻撃の初の報告書、アンスロピックの AI 攻撃報告が巻き起こした論争 https://www.lac.co.jp/lacwatch/report/20260202_004628.html〔2026/7/10 確認〕
※ 182 Amazon Web Services, Inc：AI で強化された脅威アクターによる FortiGate デバイスへの大規模な不正アクセス https://aws.amazon.com/jp/blogs/news/ai-augmented-threat-actor-accesses-fortigate-devices-at-scale/〔2026/7/10 確認〕
※ 183 Microsoft 社：AI as tradecraft: How threat actors operationalize AI https://www.microsoft.com/en-us/security/blog/2026/03/06/ai-as-tradecraft-how-threat-actors-operationalize-ai/〔2026/7/10 確認〕
※ 184 Anthropic 社：Assessing Claude Mythos Preview's cybersecurity capabilities https://red.anthropic.com/2026/mythos-preview/〔2026/7/10 確認〕
※ 185 Anthropic 社：Project Glasswing https://www.anthropic.com/glasswing〔2026/7/10 確認〕
※ 186 OpenAI 社：GPT-5.5 が登場 https://openai.com/ja-JP/index/introducing-gpt-5-5/〔2026/7/10 確認〕
※ 187 Google 社：GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools〔2026/7/10 確認〕
※ 188 Microsoft 社：SesameOp: Novel backdoor uses OpenAI Assistants API for command and control https://www.microsoft.com/en-us/security/blog/2025/11/03/sesameop-novel-backdoor-uses-openai-assistants-api-for-command-and-control/〔2026/7/10 確認〕
※ 189 Mozilla：The zero-days are numbered https://blog.mozilla.org/en/firefox/ai-security-zero-day-vulnerabilities/〔2026/7/10 確認〕
※ 190 Tenable, Inc.：「AI のためのセキュリティ」と「セキュリティのための AI」の比較 https://jp.tenable.com/cybersecurity-guide/learn/security-for-ai-vs-ai-for-security〔2026/7/10 確認〕
トレンドマイクロ株式会社：AI セキュリティとは何か？（後編）～ Security for AI と AI for Security ～ https://www.trendmicro.com/ja_jp/jp-security/25/d/expertview-20250410-01.html#2〔2026/7/10 確認〕
※ 191 Bleeping Computer：Curl ending bug bounty program after flood of AI slop reports https://www.bleepingcomputer.com/news/security/curl-ending-bug-bounty-program-after-flood-of-ai-slop-reports/〔2026/7/10 確認〕
※ 192 ITmedia：AI 生成の「ゴミ報告」が殺到、対応追い付かず疲弊……脆弱性発見の懸賞金制度に異変 https://www.itmedia.co.jp/news/articles/2605/11/news021.html〔2026/7/10 確認〕
※ 193 NIST：NIST Updates NVD Operations to Address Record CVE Growth https://www.nist.gov/news-events/news/2026/04/nist-updates-nvd-operations-address-record-cve-growth〔2026/7/10 確認〕
※ 194 YATA：「Yielding Advanced Threat Awareness with AI（脅威の可視化）」の頭文字。「正確に写す」という八咫鏡（やたのかがみ）もあるように、「AI性能の高度化に伴うサイバー脅威を正しく認識し、防御する／対応する」という趣旨。
※ 195 NCO：AI 性能の高度化を踏まえたサイバーセキュリティ対策に関する関係省庁会議 https://www.cyber.go.jp/pdf/press/20260518_AI_CS_kankeishouchoukaigi.pdf〔2026/7/10 確認〕
※ 196 https://www.cyber.go.jp/pdf/council/cs/cs_expert/07/07document6.pdf〔2026/7/10 確認〕
※ 197 NCO、内閣府政策統括官（経済安全保障担当）、警察庁、金融庁、総務省、厚生労働省、経済産業省、国土交通省、防衛省：AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について（重要インフラ事業者等に対する注意喚起） https://www.cyber.go.jp/pdf/press/20260518_AI_CS_Critical_Infrastructure.pdf〔2026/7/10 確認〕
※ 198 金融庁：「AI 脅威に対する金融分野のサイバーセキュリティ対策強化に関する官民連携会議」の作業部会の開催について https://www.fsa.go.jp/news/r7/sonota/20260514/20260514.html〔2026/7/10 確認〕
※ 199 経済産業省：高性能 AI への対応に関して赤澤経済産業大臣が重要インフラ事業者との意見交換を実施しました https://www.meti.go.jp/press/2026/05/20260501001/20260501001.html〔2026/7/10 確認〕
※ 200 NCO：AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について https://www.cyber.go.jp/pdf/press/20260518_AI_CS_goverment.pdf〔2026/7/10 確認〕
※ 201 NCO、経済産業省：AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について（ソフトウェア・ベンダに対する注意喚起） https://www.cyber.go.jp/pdf/press/20260518_AI_CS_software_vendor.pdf〔2026/7/10 確認〕
※ 202 総務省：「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」（案）に対する意見募集の結果及びガイドラインの公表 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00282.html〔2026/7/10 確認〕
※ 203 日本 AISI:AI セーフティに関するレッドチーミング手法ガイド（第 1.10 版）の公開 https://aisi.go.jp/output/output_information/250331_1/〔2026/7/10 確認〕
※ 204 日本 AISI：自動レッドチーミング 説明書 https://github.com/Japan-AISI/aisev/blob/main/docs/rt.md〔2026/7/10 確認〕
※ 205 日本 AISI：AI インシデントレスポンス・アプローチブックを公開 https://aisi.go.jp/activity/activity_security/260109/〔2026/7/10 確認〕
※ 206 NCSC：Preparing for a 'vulnerability patch wave' https://www.ncsc.gov.uk/blogs/prepare-for-vulnerability-patch-wave〔2026/7/10 確認〕
※ 207 NCSC：Vulnerability management https://www.ncsc.gov.uk/collection/vulnerability-management〔2026/7/10 確認〕
※ 208 一般社団法人 AI ガバナンス協会：「『いつの間にか』AI のリスク実態調査 ～シャドー AI 等の管理と捕捉 課題とプラクティス～」を公表しました https://www.ai-governance.jp/blog/250129-policy-opinion-ai-regulation〔2026/7/10 確認〕
※ 209 株式会社 KDDI 総合研究所：AI セキュリティポータル https://aisecurity-portal.org/〔2026/7/10 確認〕
※ 210 https://www.ipa.go.jp/digital/ai/security/ai-security-bulletin.html〔2026/7/10 確認〕
※ 211 総務省：情報通信白書令和5年版 第1部第3節 インターネット上での偽・誤情報の拡散等 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/nd123140.html〔2026/8/13 確認〕
※ 212 大澤淳：「サイバー領域の安全保障政策の方向性」株式会社ウェッジ、2024 年 1 月号「新領域安全保障」、p.185
※ 213 https://rm.coe.int/information-disorder-toward-an-interdisciplinaryframework-for-researc/168076277c〔2026/8/13 確認〕
※ 214 一般社団法人セーファーインターネット協会：Disinformation 対策フォーラム報告書 https://www.saferinternet.or.jp/wordpress/wp-content/uploads/Disinformation_report.pdf〔2026/8/13 確認〕
※ 215 EEAS：1st EEAS Report on Foreign Information Manipulation

and Interference Threats https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en〔2026/8/13 確認〕
※ 216 https://reports.weforum.org/docs/WEF_Global_Risks_Report_2026.pdf〔2026/8/13 確認〕
※ 217 WEF：The Global Risks Report 2024 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf〔2026/8/13 確認〕
※ 218 WEF：The Global Risks Report 2025 https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf〔2026/8/13 確認〕
※ 219 https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2025〔2026/8/13 確認〕
※ 220 Reuters Institute for the Study of Journalism：Overview and key findings of the 2025 Digital News Report https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2025/dnr-executive-summary〔2026/8/13 確認〕
※ 221 Meta 社：Code of Conduct on Disinformation – Report of Meta for the period 01 January to 30 June 2025 https://disinfocode.eu/reports/download/147〔2026/8/13 確認〕
※ 222 Meta 社：Community Standards Enforcement Report：Fake Accounts https://transparency.meta.com/reports/community-standards-enforcement/fake-accounts/facebook/〔2026/8/13 確認〕
※ 223 OpenAI 社：Disrupting malicious uses of AI: an update https://cdn.openai.com/threat-intelligence-reports/7d662b68-952f-4dfd-a2f2-fe55b041cc4a/disrupting-malicious-uses-of-ai-october-2025.pdf〔2026/8/13 確認〕
※ 224 OpenAI 社：Disrupting malicious uses of our models https://cdn.openai.com/pdf/df438d70-e3fe-4a6c-a403-ff632def8f79/disrupting-malicious-uses-of-ai.pdf〔2026/8/13 確認〕
※ 225 U.S. NAVAL INSTITUTE：Future Warfare: The Rise of Hybrid Wars https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars〔2026/8/13 確認〕
※ 226 大澤淳「サイバー情報操作の脅威から日本をどう守るのか」中央公論新社、中央公論、2022 年 4 月号、pp.154-161
※ 227 公益財団法人笹川平和財団安全保障研究グループ：政策提言 “外国からのディスインフォメーションに備えを!〜サイバー空間の情報操作の脅威〜” https://www.spf.org/global-data/user172/cyber_security_2021_web1.pdf〔2026/8/13 確認〕
※ 228 European Commission：A strengthened EU Code of Practice on Disinformation https://commission.europa.eu/topics/countering-information-manipulation/strengthened-eu-code-practice-disinformation_en〔2026/9/8 確認〕
※ 229 EEAS：Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI) https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en#:~:text=match%20at%20L791%20evolve%20and,society%20responses%20to%20the%20threat〔2026/8/13 確認〕
※ 230 Hybrid CoE：Hybrid threats as a concept https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/〔2026/8/13 確認〕
※ 231 EEAS：1st EEAS Report on Foreign Information Manipulation and Interference Threats https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf〔2026/8/13 確認〕
※ 232 EEAS：2nd EEAS Report on Foreign Information Manipulation and Interference Threats https://euvsdisinfo.eu/uploads/2026/02/EEAS-2nd-Report-on-FIMI-Threats-January-2024.pdf〔2026/8/13 確認〕
EEAS：3rd EEAS Report on Foreign Information Manipulation and Interference Threats https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf〔2026/8/13 確認〕
※ 233 GTIG：Pro-Russia Information Operations Leverage Russian Drone Incursions into Polish Airspace https://cloud.google.com/blog/topics/threat-intelligence/pro-russia-information-operations-drone-incursions〔2026/8/13 確認〕
※ 234 The Guardian：How social media lies fuelled a rush to war between India and Pakistan https://www.theguardian.com/media/2025/may/28/how-social-media-lies-fuelled-a-rush-to-war-between-india-and-pakistan〔2026/8/13 確認〕
※ 235 MODERN DIPLOMACY：Cambodia-Thailand Border Conflict: Restraint in the Digital Information Battlefield https://moderndiplomacy.eu/2026/01/14/cambodia-thailand-border-conflict-restraint-in-the-digital-information-battlefield/〔2026/8/13 確認〕
※ 236 International Democracy Union：IDU Statement on Russia’s Interference in Moldova’s Elections https://idu.org/idu-statement-on-russias-interference-in-moldovas-elections/〔2026/8/13 確認〕
※ 237 European Commission：Commission services and Moldovan authorities conduct a stress test on potential digital hybrid threats to election integrity ahead of Moldova’s parliamentary elections https://digital-strategy.ec.europa.eu/en/news/commission-services-and-moldovan-authorities-conduct-stress-test-potential-digital-hybrid-threats〔2026/8/13 確認〕
※ 238 OSCE：Moldova’s parliamentary elections were competitive but campaign marred by cyberattacks, illegal funding and disinformation, international observers say https://odihr.osce.org/odihr/598219〔2026/8/13 確認〕
※ 239 ドイツ連邦憲法擁護庁：Illegitimate foreign influence operations targeting the upcoming German federal election https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/EN/2025/2025-01-02-german-federal-election.html〔2026/9/8 確認〕
※ 240 The Record：Germany summons Russian ambassador over cyberattack, election disinformation https://therecord.media/germany-summons-russian-ambassador-cyberattack-disinformation〔2026/8/13 確認〕
※ 241 ポーランド共和国デジタル化省：Raport z programu “Parasol Wyborczy” - kompleksowa ochrona wyborów prezydenckich 2025 https://www.gov.pl/web/cyfryzacja/raport-z-programu-parasol-wyborczy---kompleksowa-ochrona-wyborow-prezydenckich-2025〔2026/9/8 確認〕
※ 242 BBC：Israel-Iran conflict unleashes wave of AI disinformation https://www.bbc.com/news/articles/c0k78715enxo〔2026/8/13 確認〕
※ 243 Ministry for Diaspora Affairs and Combating Antisemitism：Coordinated Iranian Activity on Social Media Through Fake Accounts During Rising Lion https://www.gov.il/BlobFolder/reports/coordinated_iranian_fake_accounts_social_media_rising_lion_2025-06/en/Research_Reports_coordinated_iranian_fake_accounts_social_media_rising_lion_2025-06.pdf〔2026/8/13 確認〕
※ 244 EDMO：The First AI War: How the Iran-Israel Conflict Became a Battlefield for Generative Misinformation https://edmo.eu/publications/the-first-ai-war-how-the-iran-israel-conflict-became-a-battlefield-for-generative-misinformation/〔2026/8/13 確認〕
※ 245 Clemson University, Watt Family Innovation Center Media Forensics Hub：From Texas to Tehran: A Multilingual, IRGC-affiliated Influence Operation on X, Instagram, and Bluesky https://policycommons.net/artifacts/48154021/from-texas-to-tehran_-a-multilingual-irgc-affiliated-influence-o/49052774/〔2026/8/13 確認〕
※ 246 PolitiFact：Videos do not show missile strike on USS Abraham Lincoln https://politifact.com/factchecks/2026/mar/02/social-media/uss-abraham-lincoln-fire-missile-iran/〔2026/8/13 確認〕
※ 247 The Jerusalem Post：Iranian media publishes false conspiracy theory claiming Netanyahu’s death or injury https://www.jpost.com/middle-east/iran-news/article-889415〔2026/8/13 確認〕
NHK ONE：イラン軍事衝突 フェイク３億回表示…目的は?どう見分ければ? https://news.web.nhk/newsweb/na/na-k10015091231000〔2026/8/20 確認〕
※ 248 PolitiFact：Trump says Iran is a country ‘based on disinformation.’ Here’s how Iran conducts influence ops https://www.politifact.com/article/2026/mar/23/iran-disinformation-campaigns-influence-operations/〔2026/8/13 確認〕
※ 249 U.S. Department of War：Trump Announces U.S. Military's Capture of Maduro https://www.war.gov/News/News-Stories/Article/Article/4370431/trump-announces-us-militarys-capture-of-maduro/〔2026/8/13 確認〕
※ 250 CEDMO：AI, outdated visuals fuel misinformation after Maduro capture https://cedmohub.eu/ai-outdated-visuals-fuel-misinformation-after-maduro-capture/〔2026/8/13 確認〕
※ 251 CNBC：AI-generated content spreads after Maduro’s removal — blurring fact and fiction https://www.cnbc.com/2026/01/06/ai-generated-deepfake-videos-venezuelan-viral-us-military-maduro-misinformation.html〔2026/8/13 確認〕
※ 252 WHO：Infodemic https://www.who.int/health-topics/infodemic〔2026/8/13 確認〕
※ 253 WHO：Measles cases dropped in Europe and Central Asia

in 2025 compared to the previous year, but the risk of outbreaks remains – UNICEF and WHO https://www.who.int/europe/news/item/11-02-2026-measles-cases-dropped-in-europe-and-central-asia-in-2025-compared-to-the-previous-year--but-the-risk-of-outbreaks-remains---unicef-and-who〔2026/8/13 確認〕

※ 254 JFC：新型コロナのレプリコンワクチンは死亡率がファイザー製の 75 倍？ 元資料の誤読【ファクトチェック】 https://www.factcheckcenter.jp/fact-check/health/false-replicon-vaccine-claim/〔2026/8/13 確認〕

※ 255 JFC：新型コロナの mRNA ワクチンで死亡リスクが 74% 上昇？根拠とされた論文の結論は正反対【ファクトチェック】 https://www.factcheckcenter.jp/fact-check/health/false-mrna-covid-vaccine-increase-mortality-in-france/〔2026/8/13 確認〕

※ 256 European Commission：The Code of Conduct on Disinformation https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation〔2026/8/13 確認〕

※ 257 European Commission：Transparency and targeting of political advertising https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights/transparency-and-targeting-political-advertising_en〔2026/8/13 確認〕

※ 258 Meta 社：Ending Political, Electoral and Social Issue Advertising in the EU in Response to Incoming European Regulation https://about.fb.com/news/2025/07/ending-political-electoral-and-social-issue-advertising-in-the-eu/〔2026/8/13 確認〕

※ 259 European Commission：Code of Conduct on Disinformation: Signatories publish their latest reports in the Code's Transparency Centre https://digital-strategy.ec.europa.eu/en/news/code-conduct-disinformation-signatories-publish-their-latest-reports-codes-transparency-0〔2026/8/13 確認〕

※ 260 Meta 社：Report March 2026 https://disinfocode.eu/reports/facebook/8/text〔2026/8/13 確認〕

※ 261 Euronews：TikTok made changes ahead of re-run of Romanian election, says EU tech chief https://www.euronews.com/next/2025/04/08/tiktok-made-changes-ahead-of-re-run-of-romanian-election-says-eu-tech-chief〔2026/8/13 確認〕

※ 262 Ballotpedia News：Forty-seven states have enacted deepfake legislation since 2019 https://news.ballotpedia.org/2025/07/22/forty-seven-states-have-enacted-deepfake-legislation-since-2019/〔2026/8/13 確認〕

※ 263 Australian Government：Online Safety Amendment (Social Media Minimum Age) Act 2024 https://www.legislation.gov.au/C2024A00127/asmade/text〔2026/8/13 確認〕

※ 264 Minister for Communications, the Hon Anika Wells MP：Social media minimum age platform assessments https://minister.infrastructure.gov.au/wells/media-release/social-media-minimum-age-platform-assessments〔2026/8/13 確認〕
eSafety：Which platforms are age-restricted? https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions/which-platforms-are-age-restricted〔2026/8/13 確認〕

※ 265 New Zealand Parliament：Parliamentary inquiry into online harm and young people completed https://www3.parliament.nz/mi/pb/sc/committees-press-releases/parliamentary-inquiry-into-online-harm-and-young-people-completed/〔2026/8/13 確認〕

※ 266 U.S. News：Factbox – From Australia to Europe, Countries Move to Curb Children's Social Media Access https://www.usnews.com/news/world/articles/2026-04-24/factbox-from-australia-to-europe-countries-move-to-curb-childrens-social-media-access〔2026/8/13 確認〕

※ 267 interface：Social Media Age Gating in the EU https://www.interface-eu.org/publications/social-media-age-gating-eu〔2026/8/13 確認〕

※ 268 Internet for Kids：Social Media Age Limits and Child Protection Laws – Country Tracker https://internetforkids.org/en/social-media-age-limits-tracker/〔2026/8/13 確認〕

※ 269 総務省：インターネット上の違法・有害情報に対する対応（情報流通プラットフォーム対処法） https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/ihoyugai.html〔2026/8/13 確認〕

※ 270 総務省：インターネット上の偽・誤情報等への対策技術の開発・実証事業（令和 7 年度） https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/taisakugijutsu_fy2025.html〔2026/8/13 確認〕

※ 271 総務省：「インターネット上の偽・誤情報等への対策技術の開発・実証事業成果発信イベント」の開催 https://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000469.html〔2026/8/13 確認〕

※ 272 国立研究開発法人新エネルギー・産業技術総合開発機構：「経済安全保障重要技術育成プログラム」で偽情報の分析に係る技術の開発に着手 https://www.nedo.go.jp/news/press/AA5_101763.html〔2026/9/1 確認〕

※ 273 JFC：参院選ファクトチェック計 27 本 / 政治系人気動画の解説も【今週のファクトチェック】 https://www.factcheckcenter.jp/fact-check/others/fact-check-weekly-20250720/〔2026/8/13 確認〕

※ 274 朝日新聞：（Media Times）参院選、期間中にも各社積極報道 ファクトチェックは昨年衆院選の5倍超 https://www.asahi.com/articles/DA3S16283986.html〔2026/8/13 確認〕

※ 275 Meta 社：Report September 2025 https://disinfocode.eu/reports/meta/6〔2026/8/13 確認〕

※ 276 TikTok 社：Protecting the integrity of TikTok during the Romanian elections https://newsroom.tiktok.com/en-eu/protecting-the-integrity-of-tiktok-during-the-romanian-elections〔2026/8/13 確認〕

※ 277 X 社：Authenticity https://help.x.com/en/rules-and-policies/authenticity〔2026/8/13 確認〕

※ 278 BusinessDay：X rolls out 'Manipulated Media' labels to combat misleading images, sparking questions on scope, enforcement https://businessday.ng/technology/article/x-rolls-out-manipulated-media-labels-to-combat-misleading-images-sparking-questions-on-scope-enforcement/〔2026/8/13 確認〕

※ 279 Yahoo! ニュース：X の投稿に「AI で生成」ラベルを設定可能に 偽情報対策になるか https://news.yahoo.co.jp/expert/articles/3187acaca3fecb60f49fd13902bf3e6955bd87ec〔2026/8/13 確認〕

※ 280 Oversight Board：Board to Address AI-Generated Content in Israel-Iran Conflict https://www.oversightboard.com/news/board-to-address-ai-generated-content-in-israel-iran-conflict/〔2026/8/13 確認〕

※ 281 OpenAI 社：Disrupting malicious uses of AI – an update（October 2025） https://openai.com/global-affairs/disrupting-malicious-uses-of-ai-october-2025/〔2026/8/13 確認〕
OpenAI 社：AI の悪用を阻止：2025 年 10 月 https://openai.com/ja-JP/global-affairs/disrupting-malicious-uses-of-ai-october-2025/〔2026/8/13 確認〕

※ 282 Bloomberg：X Will Deploy AI to Write Community Notes, Expand Fact-Checking https://www.bloomberg.com/news/articles/2025-07-01/x-will-deploy-ai-to-write-community-notes-expand-fact-checking〔2026/8/13 確認〕

※ 283 NPR：Meta says it will end fact-checking as Silicon Valley prepares for Trump https://www.npr.org/2025/01/07/nx-s1-5251151/meta-fact-checking-mark-zuckerberg-trump〔2026/8/13 確認〕

※ 284 Center for Countering Digital Hate Inc：Rated Not Helpful – How X's Community Notes system falls short on election disinformation https://counterhate.com/wp-content/uploads/2024/10/CCDH.CommunityNotes.FINAL-30.10.pdf〔2026/8/13 確認〕

※ 285 Regina Cazzamatta：From moderation to chaos: Meta's fact-checking and the battle over truth and free speech (New Media & Society, SAGE Publications) https://journals.sagepub.com/doi/10.1177/14614448251413687〔2026/8/13 確認〕

※ 286 Roozenbeek, J., van der Linden, S., Goldberg, B., Rathje, S., Lewandowsky, S.：Psychological inoculation improves resilience against misinformation on social media（Science Advances, Vol.8, No.34） https://www.science.org/doi/10.1126/sciadv.abo6254〔2026/8/13 確認〕

※ 287 TIME：Inside Google's Plans to Combat Misinformation Ahead of the E.U. Elections https://time.com/6970488/google-jigsaw-eu-elections-misinformation-prebunking/〔2026/8/13 確認〕
Mikey Biddlestone et al.：Video inoculation against election misinformation across 12 EU nations（Communications Psychology） https://www.nature.com/articles/s44271-025-00379-3〔2026/8/13 確認〕

※ 288 Mikey Biddlestone et al.：Video inoculation against election misinformation across 12 EU nations（Communications Psychology） https://www.nature.com/articles/s44271-025-00379-3〔2026/8/13 確認〕

※ 289 総務省：「国民を詐欺から守るための総合対策」に係る総務省の取組状況について https://www.cao.go.jp/consumer/iinkai/2024/439/doc/20240708_shiryou1-3.pdf〔2026/8/13 確認〕

※ 290 総務省：総合的な ICT リテラシー向上に向けた官民連携プロジェクト「DIGITAL POSITIVE ACTION」の開始 https://www.soumu.go.jp/menu_news/s-news/01ryutsu05_02000169.html〔2026/8/20

確認〕
※ 291 防衛省・自衛隊：防衛大臣記者会見　https://www.mod.go.jp/j/press/kisha/2026/0703a.html〔2026/8/13 確認〕

第3章
国内の政策及び取り組みの動向

2025 年度は改組されたサイバーセキュリティ戦略本部や国家サイバー統括室を中心に、官民一体で対策を推進する司令塔が強化された。能動的サイバー防御を見据えた法・施策の展開に加え、サプライチェーン強化に向けた SCS 評価制度の構築、AI や耐量子計算機暗号への対応、IoT 製品を対象とした JC-STAR の普及展開等が図られている。本章では、サイバーセキュリティに関する国内の政策や取り組みの動向を解説する。

3.1 国内のサイバーセキュリティ政策の状況

本節では、政府が推進するサイバーセキュリティ政策の状況について述べる。

3.1.1 政府の政策動向

政府全体の政策動向として、「サイバーセキュリティ戦略※1」に基づく取り組み、警察庁、デジタル庁、及び総務省による取り組みを紹介する。

(1)「サイバーセキュリティ戦略」に基づく取り組み

「サイバーセキュリティ戦略」は、2015 年以来、おおむね 3 年おきに策定されてきた。2025 年 12 月 23 日に閣議決定された「サイバーセキュリティ戦略」は、「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※2」、国家安全保障会議による「国家安全保障戦略※3」及びサイバー対処能力強化法等※4 に基づく取り組みを含め、サイバー空間を巡る脅威に対応する取り組みを一体的に推進するため、今後 5 年間を念頭にした諸施策の目標や実施方針が示されている。

また、「サイバーセキュリティ基本法※5」に基づき、政府が作成している年次計画である「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)※6」(以下、年次計画 2025) においても、2025 年度の「特に強力に取り組むべき施策」として、「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」に掲げられた施策の取り組みが位置付けられ※7、新たな「サイバーセキュリティ戦略」を 2025 年内目途に策定することが示されていた※8。

以下では、「サイバーセキュリティ戦略」の概要を紹介し、更に、サイバーセキュリティ戦略における施策の一つである重要インフラのサイバーセキュリティ対策の取り組みを紹介する。

(a)「サイバーセキュリティ戦略」の概要

「サイバーセキュリティ戦略」には、基本的な考え方、情勢認識、施策の方向性、目標達成のための施策及び同戦略の推進体制が示されている。それぞれの概要は、以下のとおりである。

- 基本的な考え方

  サイバー空間は、経済社会の持続的な発展の基盤であり、自由主義、民主主義、文化発展を支える基盤でもあるとし、これまでサイバーセキュリティ戦略では、「自由、公正かつ安全なサイバー空間」の確保を目指してきた。その実現のための基本原則として「情報の自由な流通の確保」「法の支配」「開放性」「自律性」「多様な主体の連携」からなる「5 つの原則」を掲げている。

  基本的な考え方では、「5 つの原則」を引き続き「基本原則」として堅持し、国がこれまで以上に積極的な役割を果たすことで施策を強化し、「自由、公正かつ安全なサイバー空間」を確保することとされている。
- 情勢認識

  サイバー空間を取り巻く情勢認識として、以下の 3 点が示されている。
  - 厳しさを増す国際情勢と国家を背景としたサイバー脅威の増大(例:国家の関与が疑われるサイバー攻撃の顕在化、政府機関や重要インフラへのサイバー攻撃)
  - 社会全体のデジタル化の進展とサイバー脅威の増大(例:個人・中小企業を含む主体へのサイバー攻撃、

サプライチェーンの停止、サイバー攻撃の分業化）
- AI、量子技術等の技術革新とサイバーセキュリティに及ぼす影響（例：AIに対する攻撃やAIを利用した攻撃のリスク、公開鍵暗号の安全性の低下・危殆化）

上記の情勢認識を踏まえ、サイバー空間を取り巻く課題として、以下の3点が示されている。
- 我が国の国民生活・経済活動、国家安全保障に深刻な影響を与えるサイバー脅威への対応
- デジタル化の進展・浸透に伴い拡大するリスクに対応した、社会全体のサイバーセキュリティ及びレジリエンスの確保
- 我が国のサイバー対応能力を支える人材・技術の確保と先端技術への対応

- 施策の方向性、目標達成のための施策

前述した課題認識のもと、「自由、公正かつ安全なサイバー空間」を確保し、「サイバーセキュリティ基本法」の目的に掲げられた「経済社会の活力向上・持続的発展」「国民が安全で安心して暮らせる社会の実現」「国際社会の平和・安全の確保」「我が国の安全保障」を達成するための施策の方向性として、①深刻化するサイバー脅威に対する防御・抑止、②幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上、③我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成、の三つが示されている。

この方向性に基づく取り組みと目標達成の施策は、それぞれ以下のとおりである。

①深刻化するサイバー脅威に対する防御・抑止

国家サイバー統括室（NCO：National Cybersecurity Office）を中心に、政府機関等が緊密に連携し、官民連携・国際連携のもと、サイバー攻撃被害の防止や事案発生の対処に加え、能動的サイバー防御を含む多様な手段を組み合わせることで、サイバー脅威を能動的に防御・抑止する。

取り組みは国が主導して進める必要がある。ただし、国だけで実現できるものではなく、多様な主体の連携を、国が積極的に推進する役割を担う。

目標を達成するための施策として、国が要となる防御・抑止、官民連携エコシステムの形成、国際連携の推進・強化が挙げられている。

②幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

デジタル化とセキュリティ確保を同時に推進するために、攻撃の標的となり得る幅広い主体に適切な対策を求めていくことで、社会全体のサイバーセキュリティ及びレジリエンスの向上を図る。

政府機関等が範となり、強固な対策を実践するとともに、重要インフラ事業者・地方公共団体、サイバーセキュリティ確保に大きな役割を持つサイバー関連事業者やベンダー、中小企業・個人等の様々な主体に求められる対策と実効性確保に向けた方策を明確化し、迅速に実施していく。

目標を達成するための施策として、政府機関等の対策強化、重要インフラ事業者・地方公共団体等の対策強化、中小企業・ベンダー等サプライチェーン全体のレジリエンス確保、全員参加によるサイバーセキュリティ向上、サイバー犯罪対策を通じた安全・安心の確保が挙げられている。

③我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

産学官を通じて、サイバーセキュリティ人材の確保・育成・裾野拡大にこれまで以上に注力していく。また、研究・開発から実装・運用まで、産学官の協働による、国産技術・サービスを核とした、新たな技術・サービスを生み出すエコシステムを形成する。更に、AIや量子技術等の技術革新がもたらすサイバーセキュリティ分野の変革に対応していく。

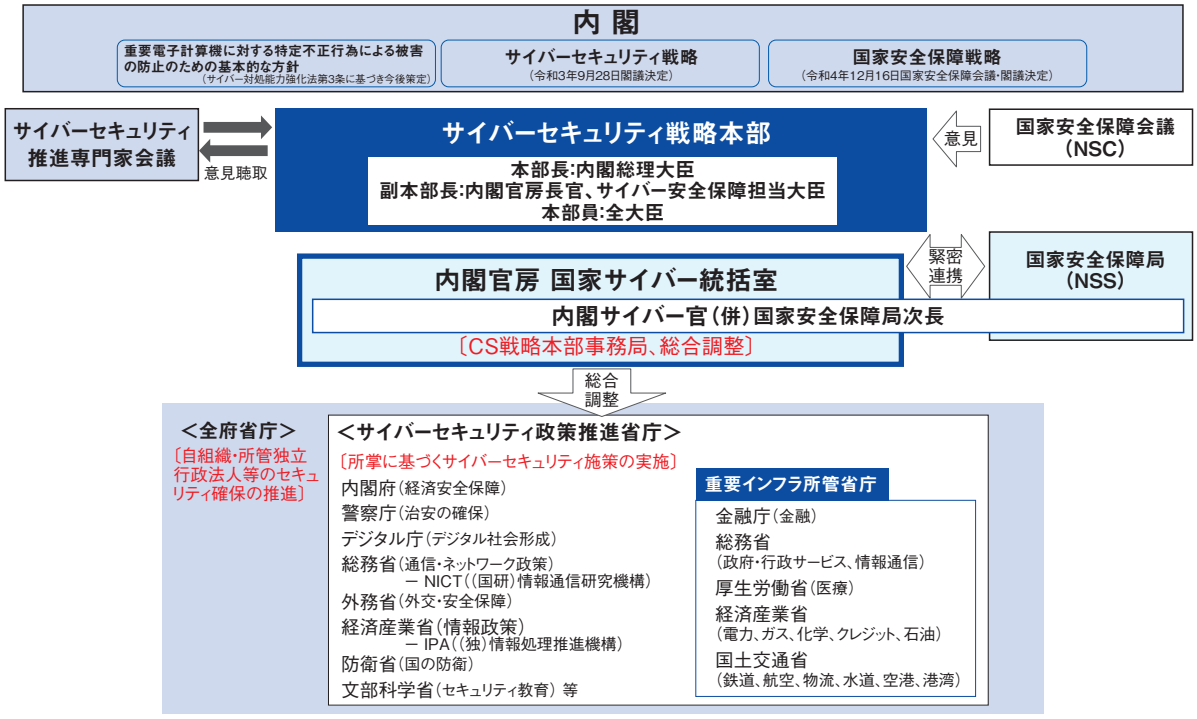
目標を達成するための施策として、効率的・効果的な人材の育成・確保、新たな技術・サービスのエコシステム形成、先端技術（AI、量子技術等）への対応・取り組みが挙げられている。

- 「サイバーセキュリティ戦略」の推進体制

図3-1-1（次ページ）に同戦略の推進体制を示す。

政府一体となった推進のために、サイバーセキュリティ戦略本部は、内閣総理大臣を本部長とし、全大臣で構成する等の改組を行い、新たな体制となった。また、内閣官房に内閣サイバー官を置くとともに、サイバー安全保障も含め、官民を通じたサイバーセキュリティ確保の司令塔として、NCOが設置された。

NCOは、サイバーセキュリティ戦略本部の事務局として、重要インフラ・基幹インフラ所管省庁及びアクセス・無害化措置※9実施省庁を含めた各府省庁間の総合調整の主導的役割を担うとともに、サイバー安全保障に関し、国家安全保障局と緊密に連携し、司令塔組織として総合調整を強力に実施する。



■図 3-1-1 「サイバーセキュリティ戦略」の推進体制
（出典）サイバーセキュリティ戦略本部「資料3−3　サイバーセキュリティ戦略推進体制※10」（第 1 回会合資料）

(b) 重要インフラのサイバーセキュリティ対策の取り組み

政府は、重要インフラの安全かつ持続的な提供のために、重要インフラ事業者等の自主的な取り組みを促進する「重要インフラのサイバーセキュリティに係る行動計画※11」（以下、行動計画）を策定している。一方、行動計画に基づく現在のサイバーセキュリティ対策の水準には、分野・事業者によりばらつきが見られる。また、国家を背景とした攻撃キャンペーン等、重要インフラへのサイバー脅威が深刻化している。

サイバーセキュリティ戦略本部は、重要インフラ事業者等が分野・事業者横断的に講ずべき基本的な対策の徹底を図るために政府機関が取り組む施策について、「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）※12」（以下、重要インフラ統一基準）の策定を進めている。

重要インフラ統一基準では、重要インフラ事業者等によるサイバーセキュリティの確保を図るために、事業者の自主的な取り組みの効果の促進を図る等、政府がより積極的に関与し、横断的なセキュリティ対策の水準を底上げするとともに、各分野におけるリスクベース※13の取り組みでの更なる水準の向上が必要であるとされている。

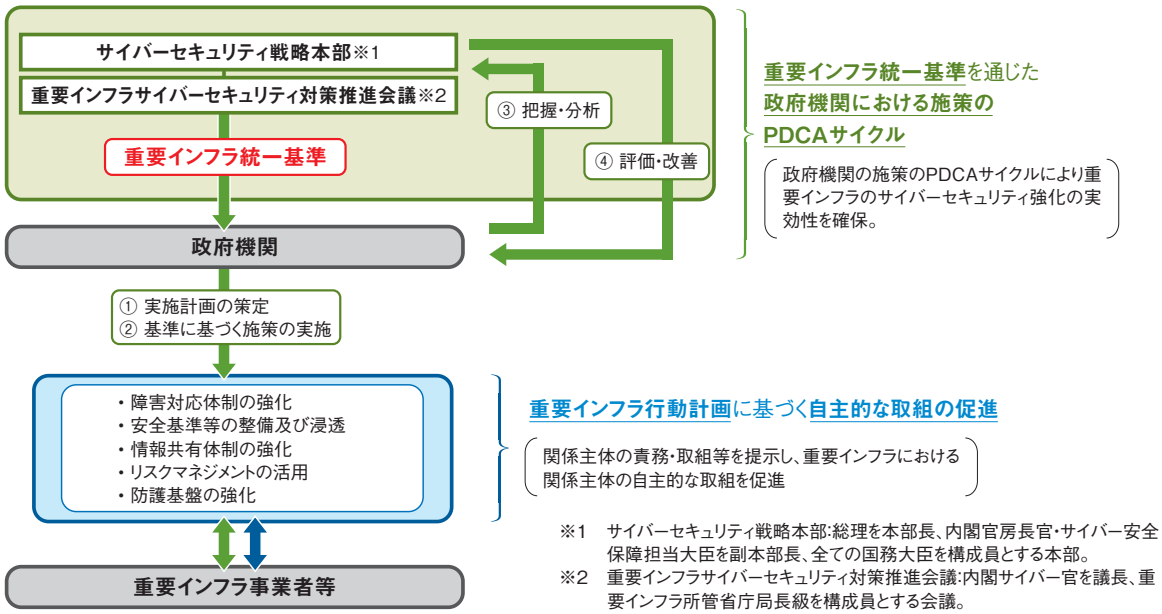
重要インフラ統一基準の位置付け、適用範囲、取り組むべき施策と PDCA サイクルは、以下のとおりである。

- 重要インフラ統一基準の位置付け

  図 3-1-2（次ページ）は、重要インフラ統一基準の位置付けを示している。図 3-1-2（次ページ）にあるように、重要インフラ統一基準は、政府機関を対象とし、重要インフラ統一基準に基づく施策（後述）の PDCA サイクルを実施するためのものである。他方、行動計画は、政府機関、重要インフラ事業者等、セプター※14事務局、サイバーセキュリティ関係機関※15、サイバー空間関連事業者※16等を対象とし、重要インフラ事業者等の自主的な取り組みの促進を図るものである。重要インフラ統一基準と行動計画は、重要インフラのサイバーセキュリティの一層の確保・向上を図る相補的な関係となっている。

- 適用範囲

  重要インフラ統一基準の適用範囲は、重要インフラの対象範囲である「情報通信」「金融」「航空」「空港」「鉄道」「電力」「ガス」「政府・行政サービス（地方公共団体を含む）」「医療」「水道」「物流」「化学」「クレジット」「石油」「港湾」及び「郵便」の 16 分野である（2026 年 4 月時点）。加えて、基幹インフラ事業者に対しては、サイバー対処能力強化法に基づきインシデント報告※18等が求められる等、サイバーセキュリティ確保の重要性が増大していることから、基幹インフラの対象範囲は、原則として、重要インフラの対象範囲



■図 3-1-2 重要インフラ統一基準の位置付け
(出典)NCO「重要インフラ統一基準(案)の概要(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)※17」

に含めるとされている。

- 取り組むべき施策と PDCA サイクル

上記の適用範囲を対象に、NCO 及び重要インフラ所管省庁は実施計画を策定し、①障害対応体制の強化、②安全基準等の整備及び浸透、③情報共有体制の強化、④リスクマネジメントの活用、⑤防護基盤の強化の五つの施策を実施する。NCO 及び重要インフラ所管省庁は、重要インフラ事業者等による取り組みの実施状況等を把握・分析し評価案を作成して、サイバーセキュリティ戦略本部に報告する。サイバーセキュリティ戦略本部は、評価案を評価する。NCO 及び重要インフラ所管省庁は、サイバーセキュリティ戦略本部による評価結果を踏まえて実施計画を更新し、サイバーセキュリティ戦略本部に報告する。

(2) 警察庁の取り組み

警察は、2025 年 12 月の「サイバーセキュリティ戦略」の閣議決定や「将来を見据えた警察組織の構造改革及び優秀な警察官の確保に向けた取組について（依命通達）※19」等を踏まえ、2026 年 4 月 2 日に「警察におけるサイバー戦略について（依命通達）※20」（以下、警察のサイバー戦略）を公開した。

また、警察庁サイバー警察局は、毎年、サイバー空間を巡る脅威の情勢と警察の取り組みを公開しており、2026 年 3 月に「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について※21」（以下、令和 7 年警察庁資料）を公開した。

以下では、警察のサイバー戦略、及び令和 7 年警察庁資料に基づき、警察のサイバー戦略に基づく取り組みとサイバー空間を巡る警察の取り組みを紹介する。

(a) 警察のサイバー戦略に基づく取り組み

警察のサイバー戦略では、情勢認識、推進事項と推進体制が示されている。

情勢認識では、機微情報の窃取や他国の選挙への干渉、ハイブリッド戦等、国家を背景としたサイバー攻撃の脅威が急速に高まっていること、社会全体のデジタル化の進展に伴い、フィッシング詐欺や証券口座の不正取引、SNS 型投資・ロマンス詐欺、生成 AI 等の技術を悪用した事案が発生していること等が示されている。

この情勢認識を踏まえて、推進事項には、サイバー対処能力強化法等に関連するものとして、以下の取り組みが示されている。

- 検挙に向けた取り組み

サイバーパトロール等を通じた、サイバー犯罪に関わる端緒情報の積極的な入手に加えて、官民連携の軸となる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）の知見及び情報を活用するとともに、サイバー対処能力強化法等の規定に基づく各種情報の把握・認知に努める。

- 未然防止・拡大防止に向けた取り組み

サイバー攻撃に対して、既存の防御への取り組みとアクセス・無害化措置を始めとする能動的サイバー防御に係る新たな施策を組み合わせ、多様な手段で能動

的に対応していく。

- 基盤整備に向けた取り組み
  アクセス・無害化措置を始めとする能動的サイバー防御を担う高度サイバー人材を含む人材の確保・育成、及び AI 等の先端技術を活用した分析・解析の高度化・効率化等の研究・開発を推進する。

推進体制では、警察庁サイバー警察局、関東管区警察局サイバー特別捜査部、都道府県警察のサイバー部門の役割が以下のとおり示されている。

- サイバー警察局
  「サイバー事案に係る警察に関すること」をつかさどる立場から、関係部門と緊密に連携しつつ、全国サイバー部門の中核的役割を果たす。
- サイバー特別捜査部
  「重大サイバー事案に係る犯罪の捜査その他の重大サイバー事案に対処するための警察の活動に関すること」を分掌するサイバー特別捜査部は、警察庁長官の指揮監督のもと、高度な国家性・国際性や無地域性等の特徴を有する重大サイバー事案の対処にあたり、アクセス・無害化措置における中核的な役割を担う。
- 都道府県警察のサイバー部門
  高度な専門的知識及び技術に基づき、事件主管部門のみでは対処困難な事案について、積極的かつ主体的に捜査を推進する。また、サイバー部門及び情報技術解析部門が一体となって各部門への支援を行い、得られた情報をサイバー特別捜査部に集約する等、情報集約の結節点としての役割を果たす。

(b) サイバー空間を巡る警察の取り組み

令和 7 年警察庁資料の中から、警察における AI 技術の利活用、AI 技術を悪用した犯罪、及びランサムウェアに関する警察の取り組みを紹介する。

(ア) 警察における AI 技術の利活用に向けた取り組み

SNS を使った犯罪実行者募集情報への対策では、AI を活用して SNS 上の投稿から犯罪実行者の募集投稿等を効率的に抽出し、投稿者等へ迅速に個別警告を実施している。

サイバーパトロールでは、警察庁が業務委託しているサイバーパトロールセンターにおいて、AI を活用して、違法情報や重要犯罪密接関連情報[※22]を自動収集し、その該当性を判定する AI 検索システムを導入し、サイバーパトロールの高度化を図っている。

フィッシング対策では、各都道府県警察等が相談等を通じて把握したフィッシングサイト情報を集約・判定し、フィルタリング事業者等に提供するにあたり、生成 AI によるフィッシングサイトの自動判別ツールを導入し、フィッシングサイト判定の高度化・効率化を図っている。

(イ) AI 技術を悪用した犯罪に対する警察の取り組み

警察は、AI の利用が急速に広がる中、「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）[※23]」に基づく検討や AI セキュリティの取り組みの推進、AI 技術を悪用した犯罪への対策等を行っている。

例えば、生成 AI を悪用した「サポート詐欺（偽のウイルス感染警告）」では、2025 年 5 月、国際共同捜査（日本警察とインド共和国・中央捜査局）により、インド共和国内に所在するインド人被疑者 6 人を逮捕した。この事件では、サポート詐欺のためにパソコン等に表示されるポップアップウィンドウの作成や日本語への翻訳に生成 AI が悪用された。検挙後の 2025 年 6 月中に IPA に相談があったサポート詐欺に関する件数は前月の 438 件から 85 件となり、一時的に大幅に減少した（「1.2.6(3) サポート詐欺（偽のウイルス感染警告）」参照）。

また、2025 年 12 月、生成 AI を悪用して作成した攻撃プログラムを用いて、複合カフェ（インターネットカフェ、マンガ喫茶等）運営会社の業務を妨害したとして、高校生の少年（17 歳）を「不正アクセス禁止法」違反及び偽計業務妨害罪で逮捕した。この事件では、生成 AI を悪用して、不正な指令を送信する攻撃プログラムを作成し、複合カフェ運営会社のサーバーに不正な指令を送信して会員情報を漏えいさせるとともに、サーバーの一部機能を停止させたとされている。

更に、今後の犯罪対策に向けて、2025 年 10 月、国際刑事警察機構（ICPO：International Criminal Police Organization、INTERPOL とも呼ばれる）、JC3 と共催で「AI とデジタル・フォレンジック」をテーマに国際会議を開催し、AI を悪用したサイバー攻撃やディープフェイク検知技術等について情報共有や討議を行った。

(ウ) ランサムウェアに対する警察の取り組み

ランサムウェアを用いた犯罪への対策では、サイバー特別捜査部は、我が国を含む世界各国の企業にランサムウェア被害を与えているグループの国際共同捜査に参画し、被疑者の検挙に貢献している。

例えば、サイバー特別捜査部は、ランサム攻撃グループ「Phobos」とその関連グループ「8Base」について、欧

州刑事警察機構（Europol：European Union Agency for Law Enforcement Cooperation）や米国連邦捜査局（FBI：Federal Bureau of Investigation）等との国際共同捜査を推進し、被疑者3名を特定した。2025年7月には、FBIの協力を得ながら、サイバー特別捜査部がPhobos/8Baseのランサムウェアによって暗号化されたデータを復号するツールを開発した。

(3) デジタル庁の取り組み

デジタル庁は、デジタル社会形成の司令塔として、未来志向のDX（デジタル・トランスフォーメーション）を推進し、デジタル時代の官民のインフラを作り上げることを目指し、様々な取り組みを推進している。

2021年から毎年策定されている「デジタル社会の実現に向けた重点計画」は、デジタル社会の形成のために政府が迅速かつ重点的に実施すべき施策に関する基本方針等を定めている。2026年7月21日に2026年度の「デジタル社会の実現に向けた重点計画※24」が閣議決定された。以下では、デジタル社会でのデータ連携・利活用に関わる「データセキュリティ※25」の取り組みを紹介する。また、デジタル社会の基盤となる「公的個人認証サービス※26」の普及促進の取り組みを紹介する。

(a) データセキュリティに関する取り組み

AI等の活用において、イノベーションの創出や価値創造のために他の組織とのデータの連携・共有が不可欠となっている。一方、国の内外を問わず他組織とデータの連携・共有を推進する際に、データに関わる法益※27が侵害されるリスクが高まっている。

デジタル庁は、「国際データガバナンス検討会」に「データセキュリティワーキンググループ」を設置し、データの適切な活用のための措置について検討を進め、2026年3月に、「データセキュリティワーキンググループとりまとめ※28」を公開した。

同とりまとめでは、「データセキュリティ」の基本認識として、表3-1-1の四つが示されている。AI等の活用を実現・推進するためには、データの連携・共有に伴って増大するリスクを社会的に受容可能なレベルとすることが重要であるとされている。特に、データの連携・共有に伴うリスクは、データ利活用の文脈やライフサイクルや、AI等の技術の進展に伴い変化することから、対応策である「データセキュリティ」も、機敏にアップデートしていくことが求められる。

基本認識	概要
法益を念頭に置く	遵守の対象となる法令等により、どのような利益が、どのような方法で、どの程度保護されているのかを具体的・分析的・機能的にとらえる。
リスクを社会的に受容可能な範囲内にコントロールする	AI等によるリスクをゼロにすることは困難であり、法令が想定している法益保護のレベルにリスクを抑えることができれば、社会的にも受容されると考える。
制度・技術・運用の三位一体で対策する	リスクを社会的に受容可能なレベルに抑えるには、制度だけではなく、技術、運用の三位一体で考える。
データのライフサイクルにおける各フェーズで施策を講じる	リスクは、データのライフサイクルの各フェーズや、現場でのデータの利活用の際に生じるため、データを主体として、データのライフサイクルの各フェーズと、具体的なデータの利活用内容をとらえる。

■表3-1-1　データセキュリティの基本認識
（出典）デジタル庁「データセキュリティワーキンググループとりまとめ」を基にIPAが作成

(b)「公的個人認証サービス」の普及の促進を図るための取り組み

「公的個人認証サービス（JPKI：Japanese Public Key Infrastructure）」とは、マイナンバーカードのICチップに搭載された電子証明書を利用して、オンラインで利用者本人の認証や契約書等の文書が改ざんされていないことの確認を行うためのサービス※26である。デジタル社会における本人認証の基盤となるサービスの一つとして、現在、行政機関だけでなく、民間事業者の各種サービスでも利用することが可能になっている。

デジタル庁と総務省は、JPKIの適切な運用を確保しながら民間活用を一層促すための民間事業者向けガイドラインを公開しており、2026年4月に「公的個人認証サービス利用のための民間事業者向けガイドライン※29」の第1.8版を公開した。

同ガイドラインでは、JPKIの概要、同サービスのメリット、同サービス利用の手引き等が説明され、民間事業者が公的個人認証サービスを利用するにあたって必要となる情報がまとめられている。

(4) 総務省の取り組み

総務省は、情報通信分野におけるサイバーセキュリティの確保や、地方公共団体におけるサイバーセキュリティの確保等の取り組みを推進している。

情報通信分野では、2026年3月に「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※30」を公開した。また、総務省と財務省は、国立研究開発法人情報通信研究機構（NICT：National Institute of

Information and Communications Technology）に関して、「国立研究開発法人情報通信研究機構 中長期目標（第 6 期）※31」（以下、NICT 第 6 期中長期目標）を 2026 年 2 月に公開した。更に、近年、ランサム攻撃等のサイバー攻撃の巧妙化や攻撃インフラの複雑化を踏まえて、2026 年 5 月から「巧妙化・複雑化するサイバー攻撃への対策の在り方に関する検討会※32」を開催している。

地方公共団体におけるサイバーセキュリティの確保では、2026 年 3 月に改定した「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（令和 8 年 3 月版）※33」を公表している。加えて、2026 年 4 月に「地方公共団体におけるサイバーセキュリティに関する支援策及び実効性確保の検討に係るワーキンググループ 報告書※34」を公開した。

以下では、上記に基づき、総務省が推進する情報通信分野におけるサイバーセキュリティ確保と、地方公共団体におけるサイバーセキュリティ確保の取り組みを紹介する。

(a) 情報通信分野におけるサイバーセキュリティ確保の取り組み

近年、情報通信技術を悪用したサイバーセキュリティ上の脅威（マルウェア感染や不正アクセス等）は悪質化・巧妙化し、その被害が深刻化している。情報通信分野におけるサイバーセキュリティ確保に向けた、サイバーセキュリティ分野の研究開発、及び巧妙化・複雑化するサイバー攻撃への取り組みを紹介する。

(ア) NICT におけるサイバーセキュリティ分野の研究開発の取り組み

NICT 第 6 期中長期目標では、NICT が「戦略的に推進すべき技術領域（戦略領域）」と、「重点的に推進すべき基礎的・基盤的研究開発分野（重点分野）」の目標が示された。

「戦略領域」は、我が国の重要政策の実現に不可欠な技術で、産学官一体となり、横断的かつ戦略的な取り組みを推進すべき領域であり、① AI・コミュニケーション、② Beyond 5G、③量子情報通信、④サイバーセキュリティの 4 領域が戦略領域として位置付けられている。「重点分野」は、我が国を支える情報通信分野の基礎的・基盤的な技術で、中長期的な視点に立って研究開発等に取り組むべき分野であり、①電磁波先進技術、②革新的ネットワーク、③サイバーセキュリティ、④ユニバーサルコミュニケーション、⑤フロンティアサイエンスの 5 分野が重点分野として位置付けられている。

以下、戦略領域と重点分野におけるサイバーセキュリティに関する目標を紹介する。

戦略領域では、以下の目標が示されている。

- 脅威情報を収集・分析・蓄積し、産学官との連携により演習等を通じたサイバー人材の育成や国産を核とした新技術・サービスの創出等に取り組む。
- AI とサイバーセキュリティの融合のための研究開発を推進し、成果展開にも積極的に取り組む。
- 我が国の安全保障の観点から長期的・継続的に維持することが求められる暗号研究に継続的に取り組む。
- 上記の取り組みを進め、サイバーセキュリティ研究開発の中核拠点として、我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成に貢献する。

重点分野では、研究開発等を通じて、「災害に強く、強靭な社会インフラの構築」「安全で、信頼できる情報通信環境の整備」「GX・DX を支える持続可能な ICT 基盤の構築」「DX を通じた効率化・合理化、新たな価値の創造」の貢献に資する技術として、特に重点的に取り組むべきものが「重点課題」として位置付けられている。表 3-1-2（次ページ）にサイバーセキュリティ分野で設定されている、六つの重点課題と目標（抜粋）を示す。

表 3-1-2（次ページ）の重点課題に加えて、サイバー対処能力強化法に基づき、サイバー攻撃の観測・分析等を行う。また NICT は、「サイバーセキュリティ基本法」等の法令に基づく委託を受けた場合には、委託業務を確実に実施する。更に、政府機関等に設置した CYXROSS センサー等から得られたサイバー脅威情報等の集約・分析・情報提供を行い、研究開発を推進し、サイバーセキュリティ分野全体の能力向上、及び社会実装のための体制を強化することとされている。

NICT は、第 6 期中長期目標を踏まえて、2026 年 4 月 1 日～ 2031 年 3 月 31 日までの 5 年間を対象とする第 6 期中長期計画※35 を策定し研究開発を推進している。

(イ) 巧妙化・複雑化するサイバー攻撃への取り組み

近年のランサム攻撃等のサイバー攻撃の巧妙化や、攻撃インフラの複雑化に伴う脅威に対し、実効的な対策を講じていくことが安全・安心なサイバー空間の実現のために重要な課題となっている。この課題認識のもと、電気通信事業者等の関係主体がサイバーセキュリティ確保のための対策の在り方について検討する「巧妙化・

重点課題	取り組み（抜粋）
サイバーセキュリティ技術	・サイバー脅威インテリジェンス基盤技術の確立を目指し、サイバー攻撃の観測・分析技術、脅威情報の大規模収集・分析技術及び脅威インテリジェンス生成技術等の研究開発を行う。 ・新たな脅威に対処するため、Beyond 5G 実現に向けたセキュリティ検証技術やローレイヤーのセキュリティ技術、ヒューマン・センタード・サイバーセキュリティの研究開発を行う。
AI ×サイバーセキュリティ技術	・AI 技術を活用し、セキュリティ対策に有用な情報をリアルタイムに導出する「AI for Security（AI を活用したサイバーセキュリティ確保）」技術の研究開発を行う。 ・AI モデルや AI 搭載システムへの攻撃に対する安全性を検証・評価し、安全性の観点を中心に信頼性の高い AI 技術を構築する「Security for AI（AI に係る安全性確保）」技術の研究開発を行う。 ・国際競争力強化のため国際連携を推進する。
次世代暗号・プライバシー保護技術	・量子コンピュータ時代に安全に利用できる暗号基盤技術の確立を目指し、現代暗号に加え、耐量子計算機暗号を含む次世代暗号技術の研究開発及び安全なデータ利活用を促進するプライバシー保護技術等の研究開発を行う。 ・耐量子計算機暗号に係る安全性評価等を着実に実施するとともに、我が国の電子政府推奨暗号リストの維持・管理を行う。
サイバーセキュリティに関する演習	・国の機関や地方公共団体、重要インフラ事業者等のサイバー攻撃対処能力の向上に貢献するため、最新のサイバー攻撃に関する知見や社会的ニーズを踏まえた実践的なサイバー演習を、高い受講効果が得られるよう開発・提供する。 ・サイバーセキュリティ研究や演習を通じて得られた知見等を活用し、若手セキュリティ人材の育成を行う。
サイバーセキュリティ産学官連携の推進	・我が国のサイバー攻撃対処能力とセキュリティ自給率の向上に貢献するため、サイバー攻撃情報等の大規模な収集・分析・共有やサイバー攻撃観測技術・ノウハウ等の共有、国産セキュリティ製品・サービス開発の加速化等に取り組む。 ・各産業分野の特性に応じたサイバー攻撃対処能力の構築に貢献するため、演習基盤の開放により産学官における自律的な人材育成を支援する。
IoT 機器のサイバーセキュリティ対策の促進	・IoT 機器のサイバーセキュリティ対策に貢献するため、脆弱性を有する機器やマルウェア感染機器の調査を実施し、ユーザーやメーカー等の関係者に対して、必要な助言及び情報提供を行う。 ・独自のセンサーの開発等、IoT 機器のサイバーセキュリティ向上の研究開発を行う。

■表 3-1-2　NICT のサイバーセキュリティ分野の重点課題と取り組み（抜粋）
（出典）総務省、財務省「国立研究開発法人情報通信研究機構 中長期目標（第 6 期）」を基に IPA が作成

複雑化するサイバー攻撃への対策の在り方に関する検討会」が開始されている。巧妙化・複雑化するサイバー攻撃への実効的な対策、サイバー攻撃対策における関係主体の連携等が主な検討事項として示されており、今後、具体的な議論が進められる。

（b）地方公共団体におけるサイバーセキュリティ確保の取り組み

総務省は、地方公共団体における情報セキュリティ確保の取り組みとして、「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」を改定し公開している。

また、サイバーセキュリティ戦略本部の所掌事務には、行政サービスを提供する地方公共団体を含む重要インフラ事業者等のサイバーセキュリティの確保に関する所管省庁の施策について、基準を作成すること等が追加されている。これらを踏まえ、総務省は、地方公共団体のサイバーセキュリティの実効性確保等を見据え、「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の改定等に係る検討会[※36]」のもとでワーキンググループを開催した。同ワーキンググループの検討の結果は 2026 年 4 月、「地方公共団体におけるサイバーセキュリティに関する支援策及び実効性確保の検討に係るワーキンググループ 報告書」として公開された。

以下、同ガイドラン改定と同ワーキンググループ報告書に基づき、地方公共団体におけるサイバーセキュリティ強化の取り組みと、サイバーセキュリティに関する支援策及び実効性確保に向けた取り組みを紹介する。

（ア）地方公共団体におけるサイバーセキュリティ強化の取り組み

総務省は、2026 年 3 月に改定した「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（令和 8 年 3 月版）」を公表した。改定のポイント[※37]を以下に示す。

- 「地方自治法」改正（2024 年 6 月）に伴う対応
- 機器の廃棄・データ消去について
- USB メモリー等の利用におけるリスクへの対処
- その他（DNS 設定情報を悪用する攻撃等について）

また、地方公共団体は、2024 年 6 月に改正された「地方自治法[※38]」（2026 年 4 月 1 日施行）において、サイバーセキュリティを確保するための方針を策定し、その方針

に基づき必要な措置を講じることとされた。総務大臣は、方針の策定等についての指針案※39を2025年4月1日に地方公共団体に通知している。地方公共団体は同指針案を参照して、改正法施行日までに方針の策定を行うこととされた。

これらの取り組みをとおして、地方公共団体におけるサイバーセキュリティの強化が進められている。

(イ)地方公共団体におけるサイバーセキュリティに関する支援策及び実効性確保に向けた取り組み

「地方公共団体におけるサイバーセキュリティに関する支援策及び実効性確保の検討に係るワーキンググループ 報告書」では、地方公共団体におけるサイバーセキュリティ対策の確実な実施に向けて、「国等による支援」「改正地方自治法に基づき地方公共団体が講ずべきサイバーセキュリティ対策の細目化」「対策実施状況のフォローアップと評価」の三つが施策の方向性として示されている。表3-1-3に、三つの「施策の方向性」と「施策の方向性の概要」及び「具体的な在り方の提言(抜粋)」を示す。

地方公共団体のサイバーセキュリティ対策における実効性の確保は、我が国全体のデジタル基盤の信頼性を左右する重要課題であり、サイバー攻撃が巧妙化・複雑化し、地域を問わず深刻な脅威に晒されている現状において、各地方公共団体の自助努力に委ねるだけでなく、国が対策の底上げを支援することが不可欠であるとされている。

3.1.2 経済産業省の政策

経済産業省は、サイバー空間とフィジカル空間を統合したサプライチェーン全体にわたるセキュリティ対策の強化に向け、制度、標準化、経営、人材、ビジネス等、様々な観点から施策を検討・実施している。

(1)産業サイバーセキュリティ研究会

2017年12月、経済産業省は我が国の産業界が直面するサイバーセキュリティの課題を洗い出し、関連政策を推進するため、産業界を代表する経営者、インターネット関連の学識経験者等から構成される「産業サイバーセキュリティ研究会」を設置した。同研究会は以下の三つのワーキンググループ(以下、WG)及び「サイバー攻撃による被害に関する情報共有の促進に向けた検討会」によって構成される。また各WGの配下には、サブ

施策の方向性	施策の方向性の概要	具体的な在り方の提言(抜粋)
国等による支援	地方公共団体単独では導入・運用が困難な高度なセキュリティ基盤や専門的サービスについては、国が主導して提供する枠組みが必要である。	ア) 国等による支援 ＜基盤整備、制度整備＞ ・重大インシデントレスポンス専門家チームの派遣の制度化 ・サプライチェーン・リスク対策も含めた地方公共団体からの相談を受け付ける総合窓口の設置 ・個別団体の課題解決に資する専門人材を派遣する事業の活用促進 ・共通システムの積極的な活用促進 ＜情報共有等＞ ・脆弱性情報等に関する地方公共団体と事業者の情報共有の促進 ・整備すべき規定類のひな形の提示 ・対策事項の意義・背景等に関する理解醸成 ＜研修・訓練等の機会の提供、人材確保＞ ・研修・訓練の戦略的な拡充 イ) 都道府県による支援 ウ) 国と都道府県による重層的な支援
改正地方自治法に基づき地方公共団体が講ずべきサイバーセキュリティ対策の細目化	サイバーセキュリティ対策の確実な実施を担保するため、サイバーセキュリティ対策を細目化し、一貫性のある明確な基準として示す。	ア) 国・地方関係を踏まえた考察 イ) 方式について ウ) 実施命令の内容についての考え方 エ) 経済安全保障対策(サプライチェーン・リスク対策) オ) 細目化項目 カ) 適用範囲(一部事務組合・広域連合・地方独立行政法人) キ) 適用範囲(議会・長以外の執行機関) ク) 他法令との関係等
対策実施状況のフォローアップと評価	対策が確実に実行されているかを把握し、改善を促すための仕組みを構築する。	・調査手法のシステム化と機能の充実 ・国の同種調査の効率的な活用

■表3-1-3 施策の方向性と具体的な在り方の提言の抜粋
(出典)地方公共団体におけるサイバーセキュリティに関する支援策及び実効性確保の検討に係るワーキンググループ「地方公共団体におけるサイバーセキュリティに関する支援策及び実効性確保の検討に係るワーキンググループ 報告書」を基にIPAが作成

ワーキンググループ（以下、SWG）または検討会が設置されている※40。

- WG1（実効性強化・国際連携）
  - 分野横断 SWG
    - 『第 2 層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース
    - 『第 3 層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース
    - サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース
    - 耐量子計算機暗号（PQC）への移行に向けた検討タスクフォース
  - 電力 SWG
  - 工場 SWG
  - 半導体産業 SWG
  - ビル SWG
  - 宇宙産業 SWG
  - 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 SWG　等
- WG2（地域・中小企業支援）
  - サイバーセキュリティ人材の育成促進に向けた検討会
- WG3（産業振興・人材育成）
  - IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会
  - 産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環（仮題）に向けての検討会
  - サイバーセキュリティ・サービス事業者の信頼性強化に向けた検討会
- サイバー攻撃による被害に関する情報共有の促進に向けた検討会

同研究会では 2026 年 4 月に第 10 回会合を開催し、施策の進捗状況が確認された※41。以下では、2025 年度に同研究会で重点的に取り組んできた活動について述べる。

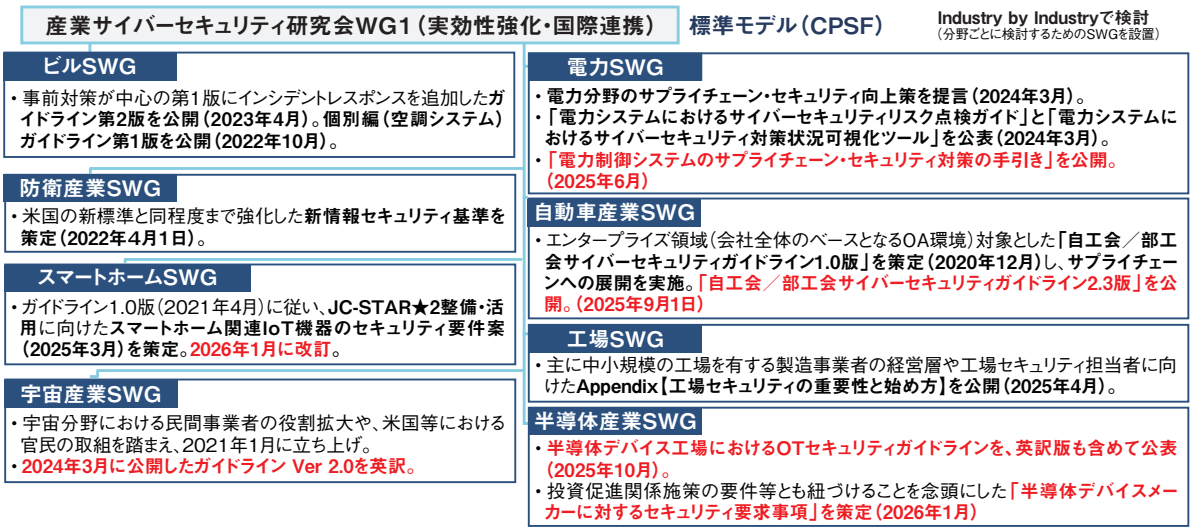
(a) サプライチェーン全体での対策強化

サプライチェーン全体での対策を強化するための、規格策定や評価制度の構築、対応ガイドラインの公開等に関する活動を取り上げる。

(ア) 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）の具体化・実装

経済産業省は、2018 年 2 月に「産業サイバーセキュリティ研究会ワーキンググループ 1（WG1）（実効性強化・国際連携）」を設置し、「Society 5.0」「Connected Industries」における新たなサプライチェーン全体のセキュリティ確保を目的としたサイバー・フィジカル・セキュリティ対策について議論を進めている。WG1 では産業分野別 SWG を設置し、2019 年 4 月に策定した「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）Version1.0」（以下、CPSF）※42 に基づくセキュリティ対策の具体化を推進している。産業分野別 SWG の具体的な活動を図 3-1-3 に示す。

図 3-1-3 から 2025 年度に新規公開した成果物について紹介する。電力 SWG は、2025 年 6 月に「電力制御



■図 3-1-3　分野別 SWG における CPSF の具体化
（出典）経済産業省「事務局説明資料　産業サイバーセキュリティ研究会　WG1　第 12 回※43」

システムに関するサプライチェーン・セキュリティ対策の手引き※44」を公開した。同文書は、「電力制御システムのサプライチェーン・セキュリティ向上策に関する提言※45」に記載されたサプライチェーン・セキュリティ対策の関連事項について、対策実施の手引きやプラクティスを示したものである。また、半導体産業 SWG は、2025 年 10 月に「半導体デバイス工場における OT セキュリティガイドライン※46」を公表した。同ガイドラインは、主に半導体デバイスメーカーの製造部門（実務者レベル）を対象とした、国家の支援を受けた攻撃を想定した対策を実現するための指針であり、特に生産目標の維持（供給責任）、機密情報の保護、半導体の品質の維持を重視している。

なお、現在、WG1 は、ISO/IEC JTC 1/SC 27 にて CPSF モデルを盛り込んだ国際規格として TS 5689※47 の策定を進めている。国際的に参照される他の規格（「The NIST Cybersecurity Framework（CSF）2.0※48」等）の更新等の変化を踏まえ、CPSF の改訂作業を引き続き実施する。

（イ）SCS 評価制度の構築

経済産業省は、WG1 内に設置した「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 SWG」にて議論を実施し、パブリックコメントを経て、2026 年 3 月に「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」と「★ 3・★ 4 要求事項・評価基準」を公表した※49。

同構築方針による「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）」では、2 社間の取引契約等において、発注企業が、受注側に適切な段階の「水準」を提示して対策を促すとともに、実施状況を確認することを通じて、サプライチェーン全体でのセキュリティ対策水準の向上を図る。3 段階の水準「★ 3･★ 4･★ 5」のうち、「★ 3・★ 4」は、2026 年度末ごろの制度開始を予定している。また、中小企業に対し、SCS 評価制度における「★ 3・★ 4」水準のセキュリティ対策実施を後押しするため、今後、各種施策を展開し、「★ 5」については、実証事業を通じて各参画企業から意見等を収集し、2026 年度以降に要求事項・評価基準や評価スキームの具体化を進める（SCS 評価制度については「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）」参照）。

また、SCS 評価制度の構築に伴い、中小企業向けの支援策が WG2 で検討され、経済産業省及び IPA により「★ 3・★ 4」の取得支援を目的とした「サイバーセキュリティお助け隊サービス（新類型）」が創設される。IPA は同サービスの創設に向けて、IPA が認定したサービス提供事業者が、実証に参加する中小企業に対して SCS 評価制度の「★ 3」または「★ 4」取得のためのサービスを試行的に提供しながら、技術要件や価格要件等を検証する実証事業を 2026 年 9 月から開始した（実証期間は 2026 年 10 月から 2027 年 9 月までの 1 年間を予定）。実証事業を通じて 2026 年度末ごろの SCS 評価制度開始にあわせて、同サービスの基準案を公表し、2027 年 12 月ごろまでに、価格要件を含むサービス基準の制度化につなげられるよう、進めていく（サイバーセキュリティお助け隊サービス制度については「3.4.3（2）サイバーセキュリティお助け隊サービス制度」参照）。

（ウ）中小企業支援の拡大

基幹インフラを狙うサイバー攻撃は脆弱な中小企業を経由して侵入することが多く、中小企業は攻撃の兆候を検知しにくい。そこで、IPA は今後、経済産業省の協力のもと、中小企業向け集団的防御プラットフォームを構築する。同プラットフォームにおいて、IPA が中小企業のアクセスログを遠隔で収集・分析し、早期検知や情報展開を行うことで、攻撃の波及防止とサプライチェーン全体の防御力向上を図る。

また、経済産業省及び IPA は、中小企業のセキュリティ対策強化に向けて、2026 年 3 月に「中小企業のための実例で学ぶサイバーセキュリティリスク事例集」と「中小企業の情報セキュリティ対策ガイドライン第 4.0 版」を公表した※50。同事例集は、中小企業に対して、自社のリスクやサイバー攻撃を自分事と認識させ、必要な対策を促すことを目的としている。同ガイドラインの改訂によって、サイバー攻撃の脅威が増す中、中小企業の組織的対策強化を促し、対策を段階的に進めるための実務的な参考資料として活用が期待される。同ガイドラインの改訂に合わせて「SECURITY ACTION」の対策項目の見直しも実施した（「3.4.2（2）『中小企業の情報セキュリティ対策ガイドライン』の改訂」「3.4.3（3）SECURITY ACTION」参照）。

更に、地域 SECUNITY 間の「横のつながり」を作り、地域 SECUNITY の活動活性化を図るため、2026 年 3 月に経済産業省及び IPA において「地域 SECUNITY 連絡会」を開催した。経済産業省の Web ページでは、発表された取り組み事例を取りまとめた地域 SECUNITY プラクティス集を掲載している※51。

サイバー攻撃の悪質化、巧妙化を受け、中小企業の対策強化と地域特性に応じた重点的取り組みも求められる。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）※52では、経済産業省と連携し、半導体産業のある九州地域において「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※53」の普及に向けた講演を行った。

また、経済産業省は、日本と多くのサプライチェーンを共有するASEAN地域に向けてサイバーセキュリティ施策の情報発信を強化すべく、IPA及びNCOと協力し、「中小企業の情報セキュリティ対策ガイドライン※54」本編の英語版を発行した。日ASEANサイバーセキュリティ政策会議にて同ガイドラインの活用事例を日本企業から発信したほか、経済産業省の英語版ホームページにも英語版を掲載している※55。

(b) セキュア・バイ・デザインの実践

IoT適合性評価制度や、安全なソフトウェアの開発に向けた指針の整備等、セキュアな製品設計の普及に向けた取り組みを紹介する。

(ア) IoT適合性評価制度の検討、国際制度調和に向けた調整

WG1での検討結果を受け、IPAは経済産業省の協力のもと、2025年3月より「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）」の運用を開始している※56（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）。

まず2025年5月に「★1」の「適合ラベル取得製品リスト」の適合基準を公開した。2025年3月には「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※57」へ、同年9月には「政府機関等の対策基準策定のためのガイドライン※58」へJC-STARの制度活用や選定基準の記載が追加された。引き続き、政府調達における将来的な必須化や、政府機関等や重要インフラ事業者における当制度活用の要件化等に向けて、関係機関等との議論を継続していく。一方、経済産業省は2025年11月、英国科学・イノベーション・技術省（DSIT: Department for Science, Innovation & Technology）と、JC-STARと英国のPSTI法（Product Security and Telecommunications Infrastructure Act）に関する相互承認の覚書に署名した。2026年1月から相互承認が開始され、両制度間の適合証明要件のすべてもしくは一部の免除が実現した。今後は、類似の制度を有する米国、欧州連合（EU：European Union）、ドイツ等を中心に制度間の協調を追求する。

更に適合基準について、2026年1月よりスマートホームの「★2」についてIPAはスマートホーム適合基準検討（SHCC）WGにて議論を開始した。また同年2月には通信機器・ネットワークカメラの「★3」のセキュリティ要件を公開した。2026年度以降に「★2」と「★3」の申請の受付開始を予定している。

(イ) 安全なソフトウェアの開発に向けた取り組み

2023年、ソフトウェアに対するサイバー脅威の増大を背景に「ソフトウェア・セキュリティに関する日米豪印共同原則」が発表されたことを受けて、経済産業省は、「セキュア・ソフトウェア開発フレームワーク（SSDF：Secure Software Development Framework）※59」導入ガイダンス案の拡充・成案化等のSSDF導入促進に向けた取り組みを実施している。具体的には、WG1の「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース（ソフトウェアTF）」において、2025年度、SSDFの導入に関する課題に対して、実証等を通じた取り組みの成果を取りまとめ、同ガイダンス案を拡充整理した※60。同ガイダンスは、2026年中の公開を予定している。

経済産業省は2024年より、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）とともにSBOM（Software Bill of Materials：ソフトウェア部品表）※61活用の重要性を示す国際文書（ガイダンス）の作成を主導してきた。2025年9月、日本のNCOを含む計15ヵ国のサイバーセキュリティ当局等が共同署名し、国際文書（ガイダンス）の策定を実現した※62。

(ウ) サイバーインフラ事業者の責務の明確化

WG1のソフトウェアTF内に設置された「サイバーインフラ事業者に求められる役割等の検討会」では、2025年3月に提示されたガイドライン案の成案化を進め、2026年3月には「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※63」が経済産業省及びNCOにより策定された。2026年度以降は、ガイドラインの活用促進に向けたチェックリストの拡充等に取り組んでいく。

(c) サイバーセキュリティ供給能力の強化

サイバーセキュリティ供給能力強化のための、産業振興推進や、先進的サイバー防御・分析力の強化策、高度セキュリティ人材の育成促進の活動について述べる。

（ア）サイバーセキュリティ産業振興のための政策パッケージの推進

現時点で、国内で活用されるセキュリティ製品の多くを海外製が占めているため、新規国産製品の導入実績を構築し、市場参入障壁を低減させる政策が求められる。2025 年 9 月 19 日の「デジタル関連産業のグローバル化促進のための関係閣僚会議」において、国内のセキュリティスタートアップ製品・サービスを優先的に調達する等の施策が提言された※ 64-1。2026 年 3 月ごろから IPA で順次調達を開始し、今後は製品・サービスの有効性を検証すべく、調達した製品の評価を行う実証事業を実施していく。

中小企業の現場において無理なく導入できる技術・製品の開発を促しながら、スタートアップ企業等に実績の機会を提供するため、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO：New Energy and Industrial Technology Development Organization）は 2026 ～ 2027 年度にかけて、サイバーセキュリティ関連技術を募集する懸賞金事業の実施を予定している。懸賞金テーマの案としては、AI 技術の活用、SBOM の効率的な実運用、SSDF が挙がっており、懸賞金事業を通じて、国内企業のセキュリティ対応力強化が期待される※ 64-2。

顧客の機微情報やシステムへのアクセスを許容する形態のサービスに対するニーズの増加が見込まれる中、サイバーセキュリティ・サービス提供事業者の「適切な運営体制」の一層の強化が求められることから、WG3 内の「サイバーセキュリティ・サービス事業者の信頼性強化に向けた検討会」では、現行の「情報セキュリティサービス審査登録制度※ 65」を拡充し、「事業者の信頼性」を確認する認定制度を創設するべく、検討を進めている。2026 年度に制度の詳細設計を進め、2027 年度中の運用開始を目指している。

（イ）先進的サイバー防御機能・分析能力の強化

経済安全保障を強化・推進する先端的技術の研究開発を進める「経済安全保障重要技術育成プログラム※ 66」（通称、K Program）の「先進的サイバー防御機能・分析能力強化」事業※ 67 では、国内のサイバー領域の状況把握力と防御力向上を目的に、2024 年 7 月から 2029 年 3 月までの期間で研究開発が進められている。2025 年 5 月のサイバー対処能力強化法等の成立や AI の進歩、地政学リスクの高まりを背景に現行のプロジェクトに新たな研究開発項目を追加し、2026 年 7 月より開始した。

（ウ）若手人材発掘機会（セキュリティ・キャンプ）の拡大

WG2 の「サイバーセキュリティ人材の育成促進に向けた検討会」では、2025 年 5 月 14 日に「サイバーセキュリティ人材の育成促進に向けた検討会最終取りまとめ」を公表した※ 68。同最終取りまとめでは、「①セキュリティ・キャンプの拡充」「②登録セキスペの活用促進」「③中堅・中小企業等における人材確保等の提示」の 3 点について、対応の方向性、今後の取り組み、目指す効果が示された。

①について、AI 等の特定領域と掛け合わせた高度セキュリティ人材の育成を目的として「セキュリティ・キャンプコネクト」の新規実施が示され、2025 年 9 月にプレ開催、2026 年 3 月に本開催を行った※ 69。また、キャンプ修了生の継続的な知見研鑽・社会還元・活躍状況共有等を目的とした「修了生向けコミュニティ」の整備も 2025 年度中の活動開始を目指して準備を進めている（「3.2.3（1）（a）セキュリティ・キャンプ」参照）。

②について、2025 年 7 月 31 日に情報処理安全確保支援士（以下、登録セキスペ）の得意分野・専門領域を可視化した「中小企業向けサイバーセキュリティ対策支援者リスト」を整備した。本リストの活用を通じて、中小企業による登録セキスペの活用や登録セキスペの活躍機会の拡大が期待される。また、2026 年 4 月から登録セキスペの資格更新に際して、所定の実務経験があると認められた登録セキスペの受講する講習をオンライン講習のみとする制度を新たに導入した「3.2.2（2）情報処理安全確保支援士制度」参照）。

③について、最終取りまとめにて「中堅・中小企業が実施するセキュリティ対策に応じた人材確保・育成の実践的方策ガイドβ版（案）※ 70」を整理した。この内容を踏まえ、2026 年 3 月、IPA は「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※ 71」を公開した（「3.4.2（2）（c）『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』公開」参照）。

（2）技術情報管理認証制度

2024 年 8 月に「技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準」が改正されたことを受けて、2025 年 5 月に「技術情報管理 自己チェックリスト※ 72」を改定し公表した。同チェックリストでは、自社の対応状況に沿ってチェック項目を選択すると、自社の取り組み状況が採点され、取り組みの進捗具合を分野別のレーダーチャート式で確認することができる。

(3) 情報共有・初動対応支援・脆弱性対策の取り組み

IPA では、重大なサイバー攻撃に関する情報共有を行う情報ハブ（集約点）の役割を担う「J-CSIP（サイバー情報共有イニシアティブ）」、重要インフラ事業者等を対象に標的型サイバー攻撃等の初動対応支援を行う「J-CRAT（サイバーレスキュー隊）」、そして脆弱性情報を官民で連携し、適切に流通・対処する仕組みである「情報セキュリティ早期警戒パートナーシップ」を運営している。

(a) J-CSIP（サイバー情報共有イニシアティブ）

経済産業省の協力のもと、IPA では 2011 年 10 月から、官民連携による高度なサイバー攻撃対策を目的として、「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）」を運用している。

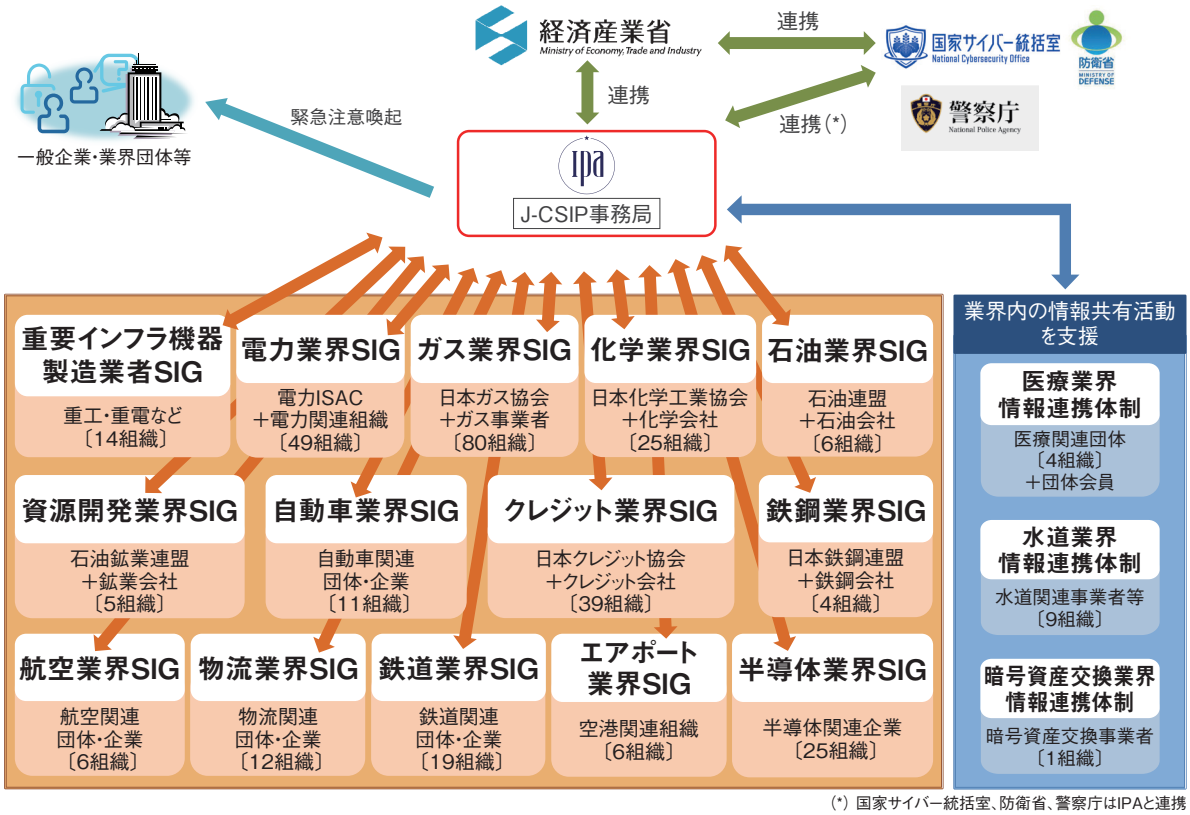
J-CSIP は、日本の基幹産業を担う企業を中心に、サイバー攻撃等に関する情報を相互に共有し、サイバー攻撃からの防御と被害の低減を目指している。参加形態としては、IPA と参加組織との間で情報共有を行う業界単位のグループ（SIG※73）と、業界の情報共有活動を支援するための枠組みである「情報連携体制」が存在する（図 3-1-4）。

2026 年 8 月末現在、IPA を情報の中継・集約点（情報ハブ）として 17 の業界から 315 の企業や業界団体（以下、参加組織）が J-CSIP に参加している。

J-CSIP では、IPA と参加組織との間でサイバー攻撃に関する手口や被害の情報、標的型攻撃メール等に関する情報共有を行っている。なお、J-CSIP で共有される情報は、提供元が明らかにならないよう、情報提供者固有の情報を除去するルールがある。

2025 年度の J-CSIP における IPA の活動としては、参加組織から提供された IoC（Indicator of Compromise：侵害指標）等の情報共有に加え、標的型攻撃に関する脅威情報や、サイバー情勢に関する注意喚起等の情報発信を行った。具体的には、VPN ゲートウェイのようなネットワーク境界にある機器から侵入する「ネットワーク貫通型攻撃」、やり取りをしている組織のアカウントを乗っ取り送信された攻撃メールや、特定の業界や組織を標的としたメールによる攻撃に関わる情報が含まれている。

情報共有活動は、攻撃の痕跡や手口の情報を基に、防御側で連携して対抗するための重要な施策の一つであり、IPA は引き続き J-CSIP の運用を継続していく。



(*) 国家サイバー統括室、防衛省、警察庁はIPAと連携

■図 3-1-4　J-CSIP の体制全体図
（出典）IPA「サイバー情報共有イニシアティブ J-CSIP（ジェイシップ）について※74」を基に編集

(b) J-CRAT（サイバーレスキュー隊）

経済産業省の協力のもと、IPA は 2014 年 7 月に「J-CRAT（Cyber Rescue and Advice Team against targeted attack of Japan：サイバーレスキュー隊）[※75]」を発足させた。J-CRAT の目的を以下に示す。

- J-CRAT が相談を受けた組織における被害拡大と再発の抑止・低減
- 国家支援型の標的型サイバー攻撃による諜報活動等の連鎖の遮断

J-CRAT では、常時、国家支援型の標的型サイバー攻撃（以下、国家支援型 APT 攻撃）に関するインシデントの相談窓口の運営と、公開情報の分析・収集の二つの活動を実施している。

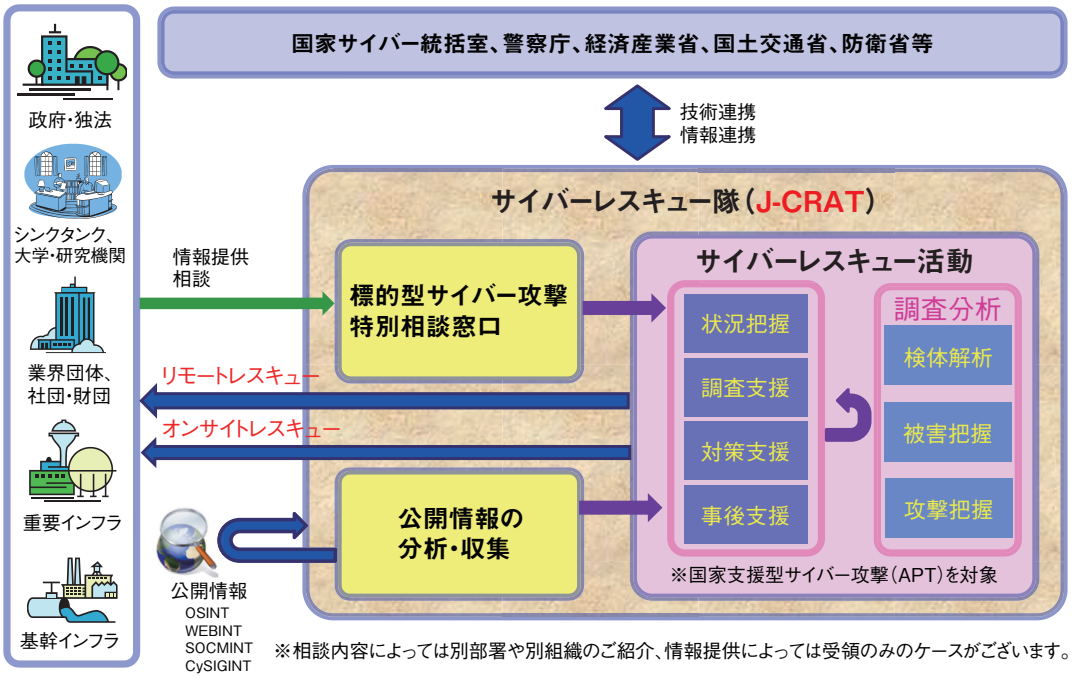
具体的な相談窓口には、2025 年 4 月に開設された「企業組織向けサイバーセキュリティ相談窓口」等[※76]（以下、窓口）があり、窓口に寄せられた相談のうち、主に国家支援型 APT 攻撃に関する被害の相談を J-CRAT で受け付け、対応している。公開情報の分析・収集では、日々公開されるインターネット上の情報等から、各種の脅威情報等を収集している。また、これまでの活動実績から、国家支援型 APT 攻撃等のサイバー攻撃は、地政学や国際政治、国際経済や科学技術等に関する動向との関連が明らかになっているため、それらの情報収集も幅広く行っている。

国家支援型 APT 攻撃の被害に遭っている、または遭っている可能性が高い組織のうち、特に公的機関や業界団体、重要インフラ関連企業や取引先等、サプライチェーンを構成する組織に対しては、J-CRAT による被害実態の確認と被害組織による認知の支援、被害緩和の暫定対応に関する助言を「サイバーレスキュー活動」として実施している。また、窓口における対応の結果、必要があると判断した組織に対して、攻撃の期間・内容、感染範囲、想定被害等をヒアリングし、早急な対策着手が行えるよう、「リモートレスキュー」や「オンサイトレスキュー」等によって、民間セキュリティ事業者への移行を前提とした助言を行っている（図 3-1-5）。

J-CRAT では、情報収集活動や支援活動から得られた結果を基に、NCO や警察庁等への技術連携・情報連携を行い、注意喚起等の発出に協力している。こうした取り組み等を通じ、被害組織のセキュリティインシデントに対する速やかな対応力向上や、平時における国家支援型 APT 攻撃への対策力向上に資する活動を行っている。また、活動を通じて組織のセキュリティ人材の育成、国家支援型 APT 攻撃の連鎖の解明、及び攻撃の連鎖を遮断することによる被害の低減を推進している。

(c) 情報セキュリティ早期警戒パートナーシップ

「情報セキュリティ早期警戒パートナーシップ」（以下、パートナーシップ）は、ソフトウェア製品及び Web サイト



■図 3-1-5　J-CRAT の活動の全体像とスキーム
（出典）IPA「サイバーレスキュー隊 J-CRAT（ジェイ・クラート）について[※75]」

に関する脆弱性関連情報の円滑な流通、対策の普及を図るため、公的ルールに基づく官民連携体制として、2004 年に整備された脆弱性関連情報の届出受付制度であり、経済産業省告示「ソフトウエア製品等の脆弱性関連情報に関する取扱規程※77」等に基づき、IPA が受付機関、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）が調整機関の役割を担い※78、運営している。

パートナーシップでは、発見された脆弱性関連情報の適切な流通を実現するため、関係者に推奨する行為を取りまとめたものとして「情報セキュリティ早期警戒パートナーシップガイドライン※79」を発行している。同ガイドラインの適用範囲は、脆弱性により不特定または多数の人々に影響を及ぼすもの、具体的には、国内で利用されているソフトウェア製品や、主に日本国内からのアクセスが想定されるサイトで稼働する Web アプリケーションが対象である。同ガイドラインが対象とする主な関係者と、それぞれがパートナーシップに対応するメリットを表 3-1-4 に示す。

関係者がパートナーシップに対応することにより、製品を使用するユーザー（システム構築事業者を含む）は、製品に関する脆弱性情報の把握と対策ができ、サイバー攻撃のリスクの低減が可能となる。また、システム構築に使用する製品選定に際して、参考としてパートナーシップを通じて公表された脆弱性対策情報の活用も期待できる。パートナーシップの活動の全体像を図 3-1-6 に示す。

2025 年におけるパートナーシップへ届け出された脆弱性の件数と累計届出件数を表 3-1-5 に示す。

なお、パートナーシップにおける四半期ごとの届出状況を、IPA の Web サイトにて公開している。最新の情報については、そちらを参照いただきたい※82。

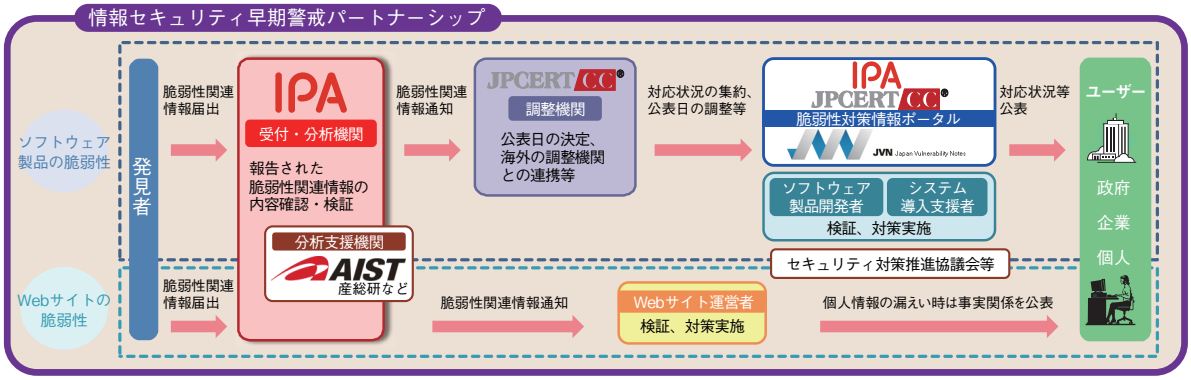
今後も、脆弱性関連情報が関係者の協力のもと、適切に流通、対応、公表されることで、製品利用者や Web サイト運営者が脆弱性を悪用されるリスクを低減することが期待される。

関係者	メリット
発見者	・公的機関を介して製品開発者や Web サイト運営者に脆弱性対応を促すことができる。 ・製品脆弱性の発見者は、脆弱性対策情報の公表時に名前を掲載できる。
製品開発者	・自社製品に影響する未公表の脆弱性を知ることができる。 ・脆弱性の対策方法を利用者に広く周知できる。 ・脆弱性問題に真摯に取り組む姿勢を示すことができる。
Web サイト運営者	・脆弱性の存在が広く知れ渡る前に、修正できる。 ・自分では気付かなかった脆弱性を確認し修正できる。 ・自分の Web サイトの利用者の安全性向上につながる。

■表 3-1-4　主な関係者とパートナーシップに対応するメリット
（出典）IPA「情報セキュリティ早期警戒パートナーシップの紹介※80」を基に編集

	ソフトウェア製品	Web サイト	合計
2025 年届出件数	432 件	178 件	610 件
累計届出件数	6,392 件	1 万 3,467 件	1 万 9,859 件

■表 3-1-5　2025 年の届出件数と累計届出件数
（出典）IPA「ソフトウェア等の脆弱性関連情報に関する届出状況［2025 年第 4 四半期（10 月～ 12 月）］※81」を基に作成



※JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

■図 3-1-6　パートナーシップの全体像
（出典）IPA「情報セキュリティ早期警戒パートナーシップの紹介」を基に編集

3.2 サイバーセキュリティ人材の現状と育成

日本におけるサイバーセキュリティ人材は、様々な人材育成施策が行われているものの、不足状態が続き、深刻な問題となっている。サイバーセキュリティ人材を取り巻く現状には、多くの課題が浮き彫りになっており、これらに対応する取り組みが行われている。本節では、サイバーセキュリティ人材育成の取り組みについて述べる。

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

国内のサイバーセキュリティを取り巻く環境は、能動的サイバー防御の社会実装、生成 AI の急速な普及、地政学的リスクの高まりに伴うサプライチェーン・リスクの深刻化等を背景に、大きな変革期を迎えている。これに伴い、安全保障、産業競争力、社会インフラのレジリエンスを支えるサイバーセキュリティ人材の重要性は、かつてない程に高まっている。

一方で、我が国では、サイバーセキュリティ人材の量的不足に加え、必要とされる役割に応じた能力及びスキルの不足、更に人材の偏在や処遇の難しさといった構造的課題が顕在化している。とりわけ、ユーザー企業における実務・管理人材やサプライチェーン全体を俯瞰できる人材の確保、及び生成 AI の利用拡大に伴う新たなリスクへの対応力の強化は、喫緊の課題となっている。

本項では、こうしたサイバーセキュリティ人材の国内外の需給実態と課題を整理した上で、政府機関が推進する対策や関連制度の動向について概観する。

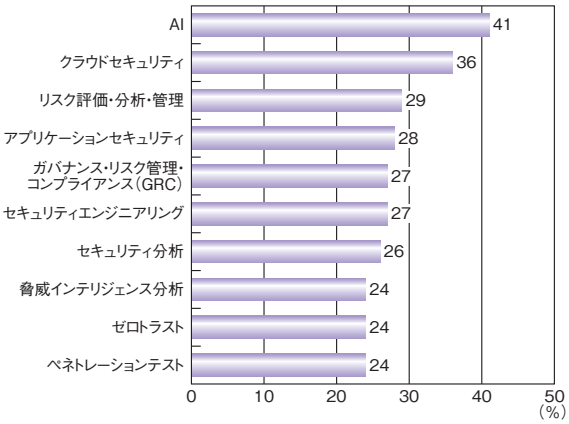
(1) 国内外における人材不足の状況

国内外におけるサイバーセキュリティ専門人材の需給ギャップは、DX の進展に伴う攻撃対象領域の拡大を背景に、引き続き深刻な状況にある。

国際的なサイバーセキュリティ専門団体 ISC2, Inc.（以下、ISC2）が公表したサイバーセキュリティ人材の年次調査である「2024 ISC2 Cybersecurity Workforce Study[※83]」によれば、世界のサイバーセキュリティ人材は約 550 万人と推計される一方、約 480 万人の不足が指摘されている。

同調査によれば、日本のサイバーセキュリティ従事者数は増加傾向だが需要の伸びに供給が追いついておらず、専門人材の不足数は約 17 万人と推計されており、我が国においても需給ギャップは高止まりしている[※84]。

人数不足だけでなく、必要なスキルセット不足の顕在化も指摘されている。同調査の 2025 年版である「2025 ISC2 Cybersecurity Workforce Study[※85]」では人材ギャップ数の算出は行われず、スキル不足の問題を重視して取り上げている。米国を中心とした各国のサイバーセキュリティの専門家の回答によると、組織内のセキュリティ部門で「何らかのスキル不足がある」と回答したのは 95% であり、2024 年の 90% から 5 ポイント増加した。また、「深刻または重大なスキル不足がある」と回答したのは 59% であり、2024 年の 44% から 15 ポイント増加した。必要なスキルとしては、AI（41%）やクラウドセキュリティ（36%）、リスク評価（29%）等の専門スキルへの高い需要が指摘されている（図 3-2-1）。



■図 3-2-1　サイバーセキュリティ人材に求められるスキル（上位 10 項目）
（出典）ISC2「2025 ISC2 Cybersecurity Workforce Study」を基に IPA が編集

また、回答者の約 88% が、スキル不足に起因するインシデント対応の遅れや運用遅延等のサイバーセキュリティ上の重大な問題を経験しており、脅威分析、インシデントレスポンス、クラウドセキュリティ、AI 関連リスクへの対応等、業務の高度化に応じたスキル形成が不可欠となっている。

国内でも需給ひっ迫は顕著である。民間 IT 転職サービス企業であるレバテック株式会社の市場動向調査（2026 年 1 月公表）によれば、2025 年 12 月時点の IT エンジニア全体の転職求人倍率が 10.4 倍である中、セキュリティ関連の正社員求人数は直近 3 年間で約 2.5 倍に拡大し、求人倍率は 42.6 倍に達した[※86]。

このように、企業がサプライチェーン対策やサイバー攻撃への対策を進める中で、経験者の採用需要が急増

している一方、実務経験を有する人材の供給が限られている状況にある。サイバーセキュリティ人材の不足は、量、スキル、経験等の不足といった課題が重なり合う状況にある。

(2) 国内企業における人材不足と課題

マクロな需給ひっ迫の傾向は、国内の企業現場における役割別の充足状況にも表れている。一般社団法人日本情報システム・ユーザー協会（JUAS：Japan Users Association of Information Systems）の「企業 IT 動向調査報告書 2026[※87]」によれば、国内企業の多くがサイバーセキュリティを担う管理者・担当者の不足を依然として訴えており、人材が不足している企業の割合は実務層・管理層の双方について高い水準にある。また、同調査では、IT 人材の課題は担当業務ごとに「採用面」「育成面」「流出面」で異なる構造を有していること、「情報セキュリティ担当」は、他の担当業務と比較して人材は充足しているものの技術が高度化して採用が難しい人材となっており（表 3-2-1）、業種に依存しない担当業務であるため人材流出も課題となりやすく、採用とのバランスを適切に保つ必要があることを指摘している。

	採用面	育成面	流出面
1 位	情報セキュリティ担当（23.9%）	プロジェクトマネジメント担当（49.9%）	運用管理・運用担当（13.5%）
2 位	データ分析担当（生成 AI 除くデータサイエンティスト等）（21.3%）	上流工程担当（業務分析・システム要件定義等）（46.6%）	インフラ・ネットワーク担当（12.5%）
3 位	新技術調査・検証担当（20.3%）	新技術調査・検証担当（45.4%）	上流工程担当（業務分析・システム要件定義等）（11.6%）

■表 3-2-1　採用・育成・流出面で課題感の高い業務（1 ～ 3 位）
（出典）JUAS「企業 IT 動向調査報告書 2026」

同調査で、どのようなセキュリティ人材が不足しているかを尋ねた結果では、「セキュリティ担当者（CSIRT 担当者含む）」の割合が 67.3% と最も高く、特にインシデント対応や日常運用を担う実務人材の不足は顕著である。CSIRT（Computer Security Incident Response Team）等の体制を整備した企業であっても、それを実効的に運用する専門性を有する人材の確保・定着が追いつかず、組織体制の整備と人材育成・配置が一体で進まなければ、十分な防御力の確保にはつながりにくい。

加えて、我が国では、その採用・定着を難しくする要因として、処遇や評価制度の整備の難しさがある。前出の「2025 ISC2 Cybersecurity Workforce Study」では、魅力的な給与・処遇を提示できていないことを採用難の原因とする日本企業の割合は 39% で、世界平均の 25% を大きく上回っている[※88]。こうした処遇面での課題は人材採用難の重要な要因の一つとなっていると考えられる。

更に、生成 AI の急速な普及が、サイバーセキュリティ人材に求められる能力を一段と複雑化させている。プロンプトインジェクションやシャドー AI による情報漏えい等、新たな脅威への対応には、従来の IT インフラ防衛に加え、安全なデータガバナンスの設計、AI 特有の脆弱性評価、リスク管理の高度化等が必要である。そのため、セキュリティ、クラウド、データ、AI 等の知見を横断的に有するマルチスキル型人材の確保が、今後重要性が増す質的課題として認識されている。

(3) 課題解決に向けた多角的な対応と施策展開

前述した深刻なサイバーセキュリティ人材の需給ギャップや AI セキュリティを始めとする課題の高度化等に対応するため、政府機関や関係独立行政法人等は、人材の確保・育成やキャリア形成の支援を多様なアプローチで加速させている。

(a) 国家戦略のグランドデザインと連携体制

政府は、新たな「サイバーセキュリティ戦略」を 2025 年 12 月に閣議決定した。同戦略ではサイバーセキュリティ人材を我が国の安全保障を支える重要な基盤として位置付け、主要な柱の一つとして「我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成」を掲げている。

また、「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）」等において、能動的サイバー防御の実行体制を支える高度専門人材確保の重要性が示されている。優秀な民間人材の活用や官民連携の強化を見据え、制度整備や処遇改善等を通じて分野横断的な人材の確保・育成に向けた取り組みが進められている。

直近では 2026 年 5 月に、高性能 AI の活用による脆弱性の検知・対応の高度化等を視野に入れた対策パッケージとして「Project YATA-Shield（プロジェクト・ヤタ・シールド）[※89]」が始動した（「2.2.4 (4) AI 性能の高度化を踏まえた我が国におけるセキュリティ対策の強化」参照）。AI の活用やセキュリティを含む最先端領域に対応

できる高度人材の確保・育成が重要な課題として位置付けられている。

(b) 人材要件・スキル標準の刷新と資格制度の改革

実務環境や技術の変化に対応するため、人材要件の「標準化」と、実務者の継続的な能力維持を前提とした「制度運用の最適化」を両輪として施策が進められている。

(ア)「サイバーセキュリティ人材フレームワーク 2026」の公表

2026 年 4 月に NCO により公表された「サイバーセキュリティ人材フレームワーク 2026[※90]」は、我が国のサイバーセキュリティ人材の定義・育成の基礎として、米国 NICE Framework[※91] との相互参照性を確保しつつ策定された、官民共通の指針である。

同フレームワークは、サイバーセキュリティ業務を「監督・ガバナンス」「設計・開発」「導入・運用」「保護・防御」「研究」からなる 13 の役割に体系化するとともに、それぞれの役割に必要なタスク・スキルと能力レベルを 4 段階で定義している(図 3-2-2)。

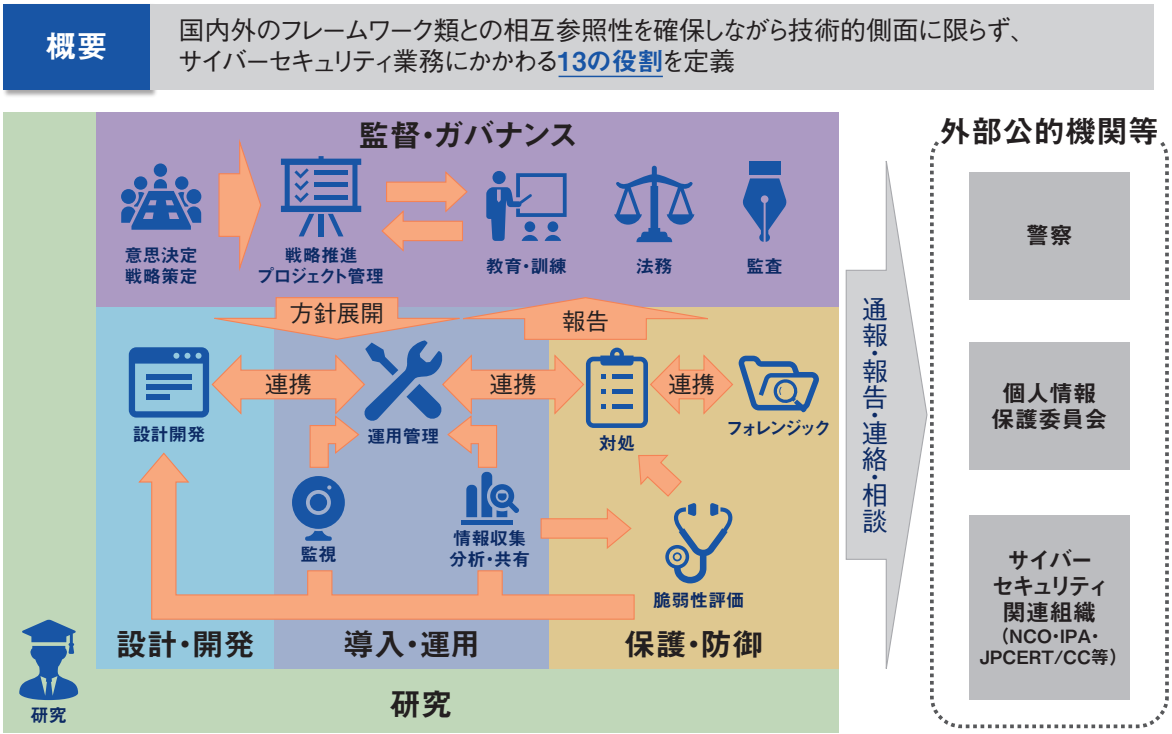
また、同フレームワークでは、日本企業に見られる兼務体制や外部委託の活用実態も踏まえ、専門人材だけでなく、非セキュリティ部門がセキュリティ機能を補完的に担う「プラス・セキュリティ人材」の位置付けも整理されている。更に、組織・教育機関・個人それぞれが採用・配置・育成・キャリア形成に活用できるよう設計されている。同フレームワークは、サイバーセキュリティ人材の要件を、共通言語として可視化する基盤として位置付けられる。

(イ)「デジタルスキル標準(DSS)」の改訂

経済産業省及び IPA は、DX・AI 活用の進展を踏まえ、「デジタルスキル標準 (DSS) ver.2.0[※93]」を 2026 年 4 月に公表した。同標準は、全ビジネスパーソン向けの「DX リテラシー標準(DSS-L)」、DX 推進人材向けの「DX 推進スキル標準 (DSS-P)」から構成される。今回の改訂では、社会での AI 利用の進展を踏まえ、AI・データ活用を推進するデータマネジメント類型の新設、AI 実装・運用及び AI ガバナンスに関するスキルの追加・明確化等が行われた。これにより、AI・データ利活用に伴うリスク管理やシステムの健全性確保を担う人材像の具体化が進展した。

(ウ)「情報処理安全確保支援士(登録セキスペ)」制度の見直し

情報処理安全確保支援士 (登録セキスペ) の資格更新においては、従来は 3 年に 1 回の実践講習の受講が



■図 3-2-2　サイバーセキュリティ人材が担う役割の全体像
(出典)NCO「サイバーセキュリティ人材フレームワーク 2026[※92]」を基に IPA が編集

義務付けられていたが、2026 年 4 月より、所定の実務経験を有する登録者を対象とした「実務経験者に対する講習制度」が導入され、要件を満たす者はオンライン講習のみで資格更新が可能となった※94。同制度改正は、セキュリティ関連実務から離れている登録セキスペが実務に携わる契機となるとともに、高度セキュリティ人材の継続的な資格保持を促進し、その有効活用の拡大に資するものである。また、試験制度についても、2026 年度より、CBT（Computer Based Testing）方式への移行が予定されており、受験機会の拡大や利便性の向上が図られている（「3.2.2（2）情報処理安全確保支援士制度」参照）。

(c) 中堅・中小企業等の人材確保に向けた取り組み

サプライチェーンを担う中小企業においては、セキュリティ対策を担う人材、内部で推進する人材の不足が顕在化している。こうした状況も受け、経済産業省は 2025 年 5 月に、人材確保・育成策の標準的なエッセンスを段階的かつコンパクトに示した「中堅・中小企業が実施するセキュリティ対策に応じた人材確保・育成の実践的方策ガイドβ版（案）」を公開した。同ガイドは、中堅・中小企業が自社内でセキュリティ人材の確保・育成を実践できるようにすることを目的に策定された。企業が実施するセキュリティ対策を段階的な四つの Step に分類し、Step ごとに対策の実施に必要なタスクと、人材の確保・育成策を示している。各企業には、自社の状況に応じた Step から人材確保・育成に取り組むことが求められている。

IPA は 2026 年 3 月、同ガイドを踏まえて、具体的な取り組み事例等を追加した「中小企業のための人材確保・育成の実践ガイドブック」を公開した（「3.4.2（2）(c)『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』公開」参照）。

(4) 今後の展望

我が国のサイバーセキュリティ能力の底上げとレジリエンスの確保には、高度な技術を備えた専門人材の「供給（育成）」と、官民連携での「適切な需要」の創出が有機的に結び付く必要がある。

セキュリティ部門をコストセンターとしてとらえる従来の固定観念から脱却し、企業のビジネス継続性と国際競争力を支えるプロフェッショナルとして、人材が適切に評価され、生涯を通じて能動的にキャリアを形成できる強靭な社会的エコシステムの定着が強く望まれる。

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

本項では、サイバーセキュリティ人材の育成や確保を目的とした国家試験である「情報セキュリティマネジメント試験」と、国家資格制度である「情報処理安全確保支援士制度」の動向を紹介する。

(1) 情報セキュリティマネジメント試験

企業や組織では、定めた情報セキュリティポリシーの周知徹底、部門の情報管理等を実施する情報セキュリティマネジメント人材が不可欠である。こうした人材の育成を促進するために、IPA は 2016 年度春期から「情報セキュリティマネジメント試験」を実施している。当初年 2 回の実施だったが、2020 年度から CBT（Computer Based Testing）方式※95 に移行した同試験は、2023 年 4 月からは年間を通じて実施され、受験機会が拡大した。2025 年度は応募者数 5 万 226 人（前年比約 1.10 倍）、合格者数 3 万 2,141 人（前年比約 1.12 倍）であった※96。非 IT 系企業の従事者を中心に活用され、その中でも「金融・保険業、不動産業」や「製造業」の従事者が多い。なお、情報処理技術者試験制度は、2027 年度に新試験制度に移行することが予定されているが、本情報セキュリティマネジメント試験の区分は継続され、出題範囲体系の変更等のみが行われる予定である。

(2) 情報処理安全確保支援士制度

最新の知識・技能を備え、サイバーセキュリティ対策を推進する人材の育成と確保を目指し、2016 年 10 月に「情報処理の促進に関する法律」の改正法が施行され、国家資格「情報処理安全確保支援士」制度が創設された。情報処理安全確保支援士（以下、登録セキスペ）は、サイバーセキュリティ分野初の国家資格であり、情報処理安全確保支援士試験合格者等が登録を申請し、登録簿に登録されることにより資格を取得できる。試験は年 2 回実施され、2025 年度は応募者数 4 万 9,030 人（前年比約 1.12 倍）、合格者数 7,333 人（前年比約 1.36 倍）であった※96。登録セキスペは 2026 年 4 月 1 日時点で 26,453 人となった※97。2026 年度からは受験者の負担軽減や利便性向上を目的として CBT 方式による実施に移行する予定である。なお、2027 年度に移行することが予定されている新試験制度においては、同試験は、出題範囲や出題形式等が一部変更されるが、2027 年度以降も継続して実施される予定である。

登録セキスペは、3 年ごとの登録更新が義務付けら

れている。登録セキスペには登録証（カード型）が交付され、初回登録時は帯の色がグリーン、1回目の更新時はブルー、2回目の更新時以降はゴールドに変わる。登録証のカラーパターンを図3-2-3に示す。



■図3-2-3　登録証のカラーパターン

また、登録更新には、計4回（毎年1回の「オンライン講習」を3回と、3年に1回の「実践講習」を1回）の講習の受講が必要である※98。講習の種類とその概要を表3-2-2に示す。

講習	講習の概要
実践講習	・実習、実技、演習または発表を伴う講習 ・3年に1回受講 ・IPAまたは民間事業者等が行う実践的な講習の中から1講習を選択して受講 ・2026年度から新たに開始した「実務経験者に対する講習制度」の認定者は、オンライン講習のみの受講となる
オンライン講習	・最新の知識及び技能の学習、倫理の醸成 ・毎年1回受講 ・IPAが指定する講習を受講

■表3-2-2　講習の全体像

「オンライン講習」では、登録セキスペに期待される情報セキュリティの実践に必要な知識・技能・倫理について学習することを目的として、IPAが指定する講習を毎年1回受講する。

また、「実践講習」では、実習、実技、演習または発表等を通じて具体的な技術や手法を学ぶことを目的として、3年に1回、IPAまたは民間事業者等が行う「実践講習」から任意の講習を選択して受講する。

IPAが行う「実践講習」は五つのコースで構成され、選択して受講する。「実践講習A」は、主に登録後3年目までの登録セキスペを対象とし、インシデント対応等の演習を通じて情報セキュリティ対応実践のための具体的な技術や手法を修得するカリキュラムで、2025年度は1,425名が受講した。

「実践講習B」は主に登録後4年目以降の登録セキスペを対象とし、企業における新規事業立ち上げを想定し、セキュリティ上の助言を検討するカリキュラムで、2025年度は1,015名が受講した。

「実践講習C」は主に登録後7年目以降の登録セキスペを対象とし、一連のインシデント対応の演習を通じて、経営判断に資する助言を行うための実践的な知識を習得するカリキュラムで、2025年度は1,854名が受講した。

受講者からは「ケーススタディで、未経験でもインシデント対応の流れを実践的に体得できた」「技術説明を経営判断につなげる工夫が重要であると理解した」といった声が多く寄せられ、実務面での有用性や講師の質、議論の充実等が評価されている。

このほかに、専門的な知識・技術修得を望む登録セキスペを対象として「業界別サイバーレジリエンス強化演習（CyberREX）※99」と「制御システム向けサイバーセキュリティ演習（CyberSTIX）※100」の選択も可能となっている（「3.2.3（2）産業システムセキュリティ人材育成のための活動」参照）。

「民間事業者等が行う実践講習※101」は、個々の登録セキスペが目指すキャリアパスに応じた講習を幅広い分野から選択できる。2026年度には16実施機関54講習が開講される。

また、2026年4月から新たな制度として「実務経験者に対する講習制度」が導入された※102。同制度は登録セキスペの中には、ITシステム・サービスのセキュリティ運用管理やインシデント対応等、日々の実務を通じて、実践講習と同等以上の知識・技能を既に修得している人が多くいるという実態を踏まえ、対象となる実務について所定の実務経験があると認められた登録セキスペの受講する講習をオンライン講習のみとする制度である。同制度の対象となるためには、申請受付期間内に、実務経験の認定に係る申請をIPAに行い、認定を受ける必要がある。

なお、IPAでは登録セキスペの現場での「活用事例（インタビュー・動画）※103」を公開している。また、中小企業向けのサイバーセキュリティ対策支援が実施できる登録セキスペを掲載したリストを公開している（「3.4.3（1）情報処理安全確保支援士（登録セキスペ）による中小企業支援」参照）。

これらの取り組みにより、情報処理安全確保支援士制度の活用促進を図り、引き続き、企業・組織のセキュリティ対策推進に登録セキスペが一層活躍し、大きな役割を果たしていくことが期待される。

3.2.3　セキュリティ人材育成のための活動

サイバーセキュリティ人材を育成するための活動について述べる。

(1) サイバーセキュリティ人材育成のための活動

サイバーセキュリティの人材育成を行う活動について、IPA の取り組みを中心に述べる。

(a) セキュリティ・キャンプ

IPA のセキュリティセンターでは、若年層サイバーセキュリティ人材の発掘・育成をするべく、「セキュリティ・キャンプ」事業に取り組んでいる。「セキュリティ・キャンプ」は、若年層のセキュリティ意識の向上を図るとともに、将来に向けて第一線で活躍できる高度なサイバーセキュリティ人材を発掘・育成する場として、一般社団法人セキュリティ・キャンプ協議会※104（以下、セキュリティ・キャンプ協議会）と IPA との官民連携事業として運営されている。各イベントには、日本の IT 業界やセキュリティ業界の第一線で活躍中のエキスパートが講師として登壇することが最大の特徴である。本項では、2025 年度に実施したプログラム、イベントについて述べる。

- セキュリティ・キャンプ全国大会
  セキュリティ・キャンプのメインイベントとして、13 歳から 22 歳までの児童・生徒・学生を対象に年 1 回、主に夏休み期間中に合宿形式の勉強会でセキュリティを突き詰めて学ぶ「セキュリティ・キャンプ全国大会」を開催してきた。22 回目となる「セキュリティ・キャンプ 2025 全国大会」は 8 月 11 ～ 15 日の 5 日間と、セキュリティ・キャンプ協議会の単独主催イベント 1 日の計 6 日間で開催した。382 名の応募があり、選考を通過した 79 名が参加した※105。
- セキュリティ・キャンプネクスト
  全国大会修了生の次のステップとして、更に高度な教育を行うための特別プログラムで、13 歳から 25 歳までの児童・生徒・学生を対象に、情報セキュリティの多様なシーンに対応し、新たな価値を生み出していけるトップオブトップの人材、フルスタック・エンジニアと呼ばれる人材を発掘・育成することを目的として「セキュリティ・キャンプネクスト」を全国大会と同日程で開催してきた。7 回目の開催となる「セキュリティ・キャンプ 2025 ネクスト」では 85 名の応募があり、選考を通過した 9 名が参加した※106。
- セキュリティ・キャンプジュニア
  小中学校でもプログラミングの教育が行われるようになったことを受けて、セキュリティを学ぶ機会を増やすために 15 歳以下の生徒・児童を対象に「セキュリティ・キャンプジュニア」を全国大会と同日程で開催してきた。3 回目の開催となる「セキュリティ・キャンプ 2025 ジュニア」では 25 名の応募があり、選考を通過した 7 名が参加した※107。
- セキュリティ・キャンプミニ
  上記に加え、サイバーセキュリティ人材の裾野拡大を目的として若年層を主な対象とした「セキュリティ・キャンプミニ」を、セキュリティ・キャンプ協議会と IPA と地域の組織・団体との主催により開催している。同プログラムは、1 日または 2 日にわたり行われ、2025 年度は全国 9 ヵ所の地域で開催した※108。対象は、25 歳以下の学生・生徒・児童であり、各地域で専門性の高い技術的な教育を提供する専門講座を開催している。また並行して、セキュリティのリテラシー向上を目的とした参加資格を限定しない公開講座を各地域とセキュリティ・キャンプ協議会との共催で実施している。
  東京（2025 年 8 月）、愛知（2025 年 9 月）、北海道（2025 年 11 月）では専門講座のみ開催した。山梨、香川（2025 年 9 月）、広島（2025 年 10 月）、長崎（2025 年 10 月・11 月）、石川（2025 年 11 月）、大阪（2026 年 3 月）では公開講座と専門講座が開催された。専門講座には全国で 186 名が参加した。また、受講の場所に縛られないオンライン開催で 2025 年 10 月に実施し、17 名が参加した。
- セキュリティ・キャンプコネクト
  サイバーセキュリティは独立した分野である一方で、法律や AI、IoT 等、他の様々な分野とも密接に関わりながら成り立っている。そうした他分野からのアプローチでサイバーセキュリティへとつなげ、更に分野横断的な橋渡しを担いながら、セキュリティを多面的に検討できる人材を発掘・育成する場として、「セキュリティ・キャンプコネクト」が 2025 年度より新設された。初の開催となる「セキュリティ・キャンプ 2026 コネクト」は、18 歳以上 25 歳以下（法律クラスのみ 30 歳以下）の学生を対象に、2026 年 3 月 26 ～ 29 日の 4 日間で実施された※109。今回は 299 名の応募があり、選考を通過した 40 名が参加した。受講生は法律、AI、脅威、デバイス、OS、IoT の各クラスに分かれて講義を受けるとともにクラス横断でグループを編成する「コネクトワーク」と呼ぶグループワークをとおしてクラスを越えて交流を行い、最終日にその成果をグループごとに発表した。
- セキュリティ・キャンプフォーラム
  過去にセキュリティ・キャンプに参加した修了生同志や講師等との参加年度を越えた交流、及び修了後の活動の成果発表を通じた修了生の認知度向上と産業界

での活躍に向けたきっかけ等の場の提供を目的として、毎年2～3月のサイバーセキュリティ月間に合わせて「セキュリティ・キャンプフォーラム」を開催している。2025年度は2026年2月14日に開催し、14の展示ブースにて修了生達が日頃の成果を披露した※110。会場ではハンズオン形式のワークショップを同時開催し、5名の受講生が課題に取り組んだ。

(b) Global Cybersecurity Camp

「Global Cybersecurity Camp（GCC）※111」は18歳から25歳の学生等を対象に毎年開催される国際サイバーセキュリティ研修プログラムで、「国籍・人種を超えた専門知識のあるグローバル人材の育成」と「国境を越えた友情とゆるやかなコミュニティの形成」を目的としたイベントである。セキュリティに興味を持つ異なる国の若者がともに学び、友好を深める場として2018年度より日本を含むアジア太平洋地域で非営利の関連団体・大学等の主催により開催されており、開催国は参加国間で持ち回りとなっている。日本からは、セキュリティ・キャンプ協議会が共催として協力している。毎年、参加国から選抜された優秀な学生50名程度が開催国に集まる。

8回目となる2025年度は2026年3月2日から6日の5日間、ベトナムで「GCC 2026」として、九つの国と地域の関連団体・大学により開催された※112。日本からは選考を通過した5名が参加し、参加者は講義を受けるとともにグループワークをとおして各国の受講生、講師等と交流を行い、最終日にその成果を発表した。日本人受講生5名中3名はセキュリティ・キャンプ全国大会修了生であった。なお、六つの講義のうち、二つにおいて日本人講師が登壇した。

(c) International Cybersecurity Challenge

「International Cybersecurity Challenge（ICC）※113」は、地域別対抗の若手人材向けの国際的なサイバー競技会で、26歳以下の若手技術者の人材育成とコミュニティの構築を目的としている。競技会の企画・運営は、欧州連合サイバーセキュリティ機関（ENISA：The European Union Agency for Cybersecurity）が立ち上げたICCプログラムの憲章及び規則に基づき、開催国において必要な体制を構築するものとされている。

2022年から毎年開催されており、4回目となる2025年はアジア地域で初めて日本が開催国となり、NCO及びICC日本開催準備委員会が主催し、官民が連携して「International Cybersecurity Challenge TOKYO 2025」として2025年11月11～14日の4日間、千葉県で開催された※114。開催側組織及び参加チーム側の双方にて、セキュリティ・キャンプ協議会が協力した。

競技参加選手としては、世界中から全8チームが集結し、世界の59の国・地域から、合計630名（うち選手団：約200名）が参加した。各チームは地域予選大会を勝ち抜いて選抜された若手トップ人材で構成され、Jeopardy（クイズ形式）及びAttack & Defense（攻防戦）の2形式のCTF（Capture The Flag）で競い合った。日本は6ヵ国のメンバー15名で構成されるTeam Asiaに所属、過去最多となる6名を送り込んだ※115。日本人選手6名中5名はセキュリティ・キャンプ全国大会修了生であった。競技の結果、Team Asiaは総合成績2位に輝いた。

会場では競技会のほか、一般来場者を対象としたサイバーセキュリティ人材育成に関するカンファレンス、展示会等も併催された。カンファレンスでは、セキュリティ・キャンプ協議会も登壇した※116。また、開催地及び協力団体である千葉県、千葉市※117、千葉大学※118、東京情報大学※119らの支援により、近隣小中学生向けの情報セキュリティ・プログラミング講座や近隣高校生向けのセキュリティワークショップも併催された。

なお、この「International Cybersecurity Challenge TOKYO 2025」の取り組みは、「GMO Cybersecurity Awards 2026※120」にて、人財育成賞を受賞した。

(2) 産業システムセキュリティ人材育成のための活動

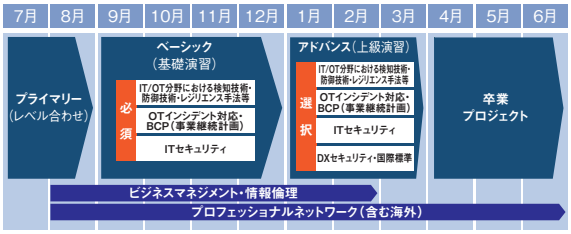
IPAの産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）では、重要インフラや産業基盤のサイバー攻撃に対する防御力を強化するための人材育成事業に取り組んでいる。

本項では2025年度事業について述べる。

(a) 中核人材育成プログラム

ICSCoEは、2017年7月から制御技術（OT）と情報技術（IT）、マネジメント、ビジネス分野を総合的に学び、サイバーセキュリティ対策の中核となる人材を育成する「中核人材育成プログラム」を実施している。同プログラムでは、OT及びIT知識のレベル合わせからハイレベルな演習までを1年間のフルタイムで実施する（次ページ図3-2-4）。第1期から第8期までに492名の修了者を輩出し、2025年7月に開講した第9期では、電力・ガス・鉄鋼・化学・自動車・放送・通信・鉄道・建築・金融・

産業機械・産業用制御システムのベンダー等の幅広い業界から55名が参加した。



■図 3-2-4　第 9 期中核人材育成プログラムの年間スケジュール

カリキュラムは以下の 3 領域を基軸とした構成となっている。

- 「IT/OT 分野における検知技術・防衛技術・レジリエンス手法等」（模擬プラントを用いた攻撃と防御の両面を学ぶパープルチーム演習、制御システムを含んだセキュリティリスク評価、攻撃に対する防衛技術の理解等）
- 「OT インシデント対応・BCP」（安全性と事業継続性を両立させる OT インシデント対応、制御システム BCP 対応の演習等）
- 「IT セキュリティ」（制御システムセキュリティ実現のための IT 設計、IT インシデント対応、体制整備等）

これらに加えて、専門家によるビジネスマネジメントに関する講義や、米国・欧州等の先進事例を学び、現地トップレベル機関との人的ネットワークの構築を目的とする海外派遣演習、及び国内の外部施設見学も行っている。

海外派遣演習として、2026 年 5 月には、第 9 期受講者がフランス及び英国を訪問した。フランスでは、サイバーセキュリティにおける先進的な技術開発等が行われている研究機関 Institut Mines-Télécom 及び IRT SystemX を訪れ、技術開発の現場を見学した。英国では、Imperial College London 内の産学官共同研究機関 Research Institute in Trustworthy Inter-Connected Cyber-Physical Systems（RITICS）及びサイバーセキュリティ分野のスタートアップ支援や企業間交流等を促進する施設 Plexal を訪問した。

国内においても、発電プラントや機械製造プラント等制御システムが稼働する現場の見学を行った。

カリキュラムの総まとめとなる「卒業プロジェクト」では、受講者自身が課題を設定し、グループワークを通じて成果物を作成する。第 8 期では 21 件の成果物が作成され、受講者の取り組みの一端を紹介するため、機密性等の観点から公開可能な 9 件を Web サイトで公開した※121。

(b) 修了者向けリカレント教育と「叶会」

ICSCoE では、中核人材育成プログラム修了者の知識・スキルのアップデートを目的とした、リカレント教育の機会を設けている。2025 年度は 7 月から 8 月の間で 4 コースのプログラムを提供し、それぞれ希望者が参加した。最新の技術動向やトレンドを反映した講習を受講するだけでなく、修了者間の人的ネットワークの構築、維持の場にもなっている。

中核人材育成プログラムの修了者コミュニティである「叶会（かなえかい）※122」は、2018 年夏以降、同プログラムを通じて培った人脈の活用、知見やノウハウの共有を目指し、地域活動や技術をテーマにする複数の部会を設置する等、活動している。

2025 年 10 月には修了年次をまたがる縦のつながりの形成、最新情報及びノウハウ共有を目的とした第 8 回叶会総会を開催した。

叶会には第 1 期から第 8 期までの修了者に加え、2026 年 6 月に修了した第 9 期生も参加しており、今後もコミュニティとしての規模を拡大しながら、お互いの顔が見える縦横の人的つながりを形成し、産業サイバーセキュリティに関する適時、適切な情報共有活動を継続することが期待される。

(c) 責任者向けプログラム

責任者向けプログラムでは、「業界別サイバーレジリエンス強化演習（CyberREX）」「サイバーセキュリティ企画演習（CyberSPEX）」の二つのプログラムを実施した。

- 業界別サイバーレジリエンス強化演習（CyberREX）

  CyberREX（Cyber Resilience Enhancement eXercise by industry）※99 は、実施回ごとに設定する対象業界において、CISO に相当する役割を担う人材や、IT 部門、生産部門等の責任者を対象としたプログラムである。登録セキスペの「実践講習」としても受講可能になっている。

  2025 年 5 月と 9 月に東京、11 月に大阪で同演習を実施した。同演習では、部署・部門のサイバーセキュリティに関するインシデント対応力・回復力を強化することを目的とし、仮想企業を想定し、業界の最新動向、業界別に考慮すべきセキュリティ要件・安全性要件を織り込んだシナリオ形式による実践演習を中心に実施した。

- サイバーセキュリティ企画演習（CyberSPEX）
  CyberSPEX（Cyber Security Planning Exercise）※123は、組織のサイバーセキュリティを推進する責任者を対象としたプログラムである。
  2025年5月に名古屋、2026年1月に東京で同演習を実施した。同演習では、責任者層として必要なセキュリティ企画立案スキルを習得することを目的とし、サイバーセキュリティの知識を獲得する講義やワークショップ、経営層を説得する考え方やロジカルシンキングを習得する提言シミュレーション演習を実施した。

（d）実務者向けプログラム

実務者向けプログラムでは、「制御システム向けサイバーセキュリティ演習（CyberSTIX）」「ERABサイバーセキュリティトレーニング」の二つのプログラムを実施した。

- 制御システム向けサイバーセキュリティ演習（CyberSTIX）
  CyberSTIX（Cyber SecuriTy practIcal eXercise for industrial control system）※100は、制御システムのサイバーセキュリティを担当する実務者や、今後担当予定の実務者を対象としたプログラムである。登録セキスペの「実践講習」としても受講可能になっている。2025年5月に仙台、9月に東京、2026年2月に福岡で同演習を実施した。同演習では、制御システムへの攻撃手法、及び制御システムのサイバーセキュリティ対策の基礎を実践的に理解することを目的とし、簡易模擬システムを用いた実機演習（ハンズオン演習）を中心に実施した。
- ERABサイバーセキュリティトレーニング
  ERABサイバーセキュリティトレーニング※124は、電力小売事業に関わるERAB（Energy Resource Aggregation Business）事業者において、セキュリティ対策を検討し、立案・実施する実務者等を対象としたプログラムである。
  2026年1月にe-Learningシステムを用いたオンデマンド配信形式で同トレーニングを実施した。同トレーニングは、経済産業省資源エネルギー庁の「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 Ver3.0※125」におけるERAB事業者に求められるサイバーセキュリティ対策に関する知識やスキルの習得を目的として実施した。

COLUMN

データを守ることは、事業を守り強化すること

企業活動におけるデータの位置付けは大きく変わってきています。かつてデータは、売上、顧客、契約、在庫、会計等を記録するための単なる情報でした。しかし現在では、データは経営判断、顧客サービス、業務改善、リスク管理、新規事業創出を支える重要な経営資産です。データが正確であれば判断の質は高まり、データが古く、ばらばらで、信頼できなければ、経営判断を誤る可能性があります。

一方で、データを取り巻く環境は複雑になっています。データは社内の基幹システムだけでなく、クラウド、スマートフォン、業務端末、取引先、外部委託先、海外拠点等、様々な場所に分散しています。便利になった反面、どこに重要なデータがあり、誰がアクセスでき、どれが最新版なのかを把握しにくくなっています。これからのデータ管理では、データが分散していることを前提に、所在、責任、権限、品質、保存、削除、監査のルールを整えることが重要です。

加えて、今後は現場に近い場所で生まれる、いわゆる「エッジ（Edge）データ」の重要性が高まります。工場、店舗、オフィス、交通、物流、エネルギー、医療、都市管理等では、センサー、カメラ、制御装置、IoT 機器から大量のデータが発生します。これらのデータは、設備の稼働状況、異常検知、在庫管理、需要予測、安全管理、エネルギー管理等に使われます。つまり、エッジデータは現場の状態を映す重要な情報であり、「リアルタイムでの現場の判断」と「集約されたデータによる経営判断」の双方の基礎をなしています。

データセキュリティというと、これまで情報漏えい対策が注目されてきました。しかし、このようにデータを取り巻く環境が変化する中で、守るべきものは機密性だけではなくなってきています。セキュリティの基本は、データの「機密性・完全性・可用性」を守ることです。この観点で見ると、データ漏えいは機密性の問題であり、データ改ざんは完全性の問題であり、ランサムウェア被害やデータ破壊は可用性の問題です。ランサムウェアによりデータが暗号化されれば、販売、会計、顧客対応、人事、物流、契約管理等が一斉に停止するおそれがあります。外部からの攻撃のほかにも、組織内部の役職員による意図的なデータ改ざんや不注意な操作ミスによる改ざん等もリスクとして考えられます。これらは、いずれも重大な経営リスクです。

各国も、こうしたデータセキュリティの重要性を踏まえ、制度やガイドラインを整備しています。米国では、国立標準技術研究所（NIST：National Institute of Standards and Technology）のサイバーセキュリティフレームワーク[i]が、サイバーリスク管理を「統治、識別、防御、検知、対応、復旧」という流れで整理しています。このフレームワークは、単に攻撃を防ぐだけでなく、組織としてリスクを把握し、インシデントを検知し、対応し、復旧するまでを一体で考える枠組みです。復旧とあるように、被害をゼロにすることを目指すだけでなく、被害を最小限に抑え、迅速に事業を継続するレジリエンスの向上が不可欠であるということです。

欧州では、NIS 2 指令（Network and Information Systems Directive 2）[ii]により、重要分野におけるサイバーセキュリティ水準の引き上げが進められています。また、デジタ

ル製品については、サイバーレジリエンス法（CRA：Cyber Resilience Act）[iii]により、ソフトウェアや接続機器を設計・開発・運用期間を通じて安全に保つことが求められています。これは、エッジデバイスやIoT機器が増える時代に、機器そのものの安全性を制度を通じて高めようとする動きです。

日本政府は、データ分野でDFFT（Data Free Flow with Trust）、すなわち「信頼性のある自由なデータ流通」を推進してきており、信頼を軸にデータの活用とセキュリティの両立に取り組んでいます[iv]。データは自由に流通することで価値を生み出しますが、その前提として、安心して共有・利用できる信頼の仕組みが必要です。そこで日本では、政府システムに対するセキュリティ規程の整備、産業向けガイドラインの提供、データ共有に必要なトラスト基盤の検討、更にIoT機器等へのラベリング制度（JC-STAR）等を通じて、社会全体でデータセキュリティを確保する取り組みを進めています。

更に、企業のデータは国境を越え、クラウドサービス、海外拠点、国際取引、外部プラットフォーム等を通じてグローバルに共有されます。その中で重要になるのがデータ主権です。自社や顧客に関わるデータが、どこに保存され、どの法律が適用され、誰に利用され、どのような条件で共有されるのかを把握し、管理できなければなりません。データの利用目的、アクセス権、再利用、削除、監査、国外移転まで含めてガバナンス対象としてとらえる必要があります。

そうした中で、企業がまず取り組むべきことは、自社が持つデータを把握し、重要度を分類することです。個人情報、顧客情報、契約情報、営業秘密、財務情報、技術情報、認証情報に加え、エッジデータやIoT機器から得られる現場データについても、漏えい・改ざん・消失した場合の影響を評価する必要があります。その上で、アクセス権限を適切に設定し、定期的に見直しを行います。バックアップは実際に復旧できることを確認し、クラウドや委託先との契約では、データの利用条件やインシデント時の対応を明確にしておきます。現場の機器については、機器の認証、通信の暗号化、改ざん検知、ログ保全、ソフトウェア更新、廃棄時のデータ消去まで考えることが重要です。

データセキュリティは、情報システム部門だけの仕事ではありません。経営層、総務、経理、人事、法務、現場の各部門、更には取引先等が一体となって取り組むべき経営課題です。データを安全に扱える企業こそが、顧客から信頼され、取引先から選ばれ、データを活用した成長を実現できるのです。また、企業のレピュテーション向上にもつながっていくと期待されています。つまり、データを守ることは、事業を強化し、これからの競争力を強化することなのです。

i　NIST：The NIST Cybersecurity Framework（CSF）2.0　https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf〔2026/7/31 確認〕
ii　European Commission：NIS2 Directive: securing network and information systems　https://digital-strategy.ec.europa.eu/en/policies/nis2-directive〔2026/7/31 確認〕
iii　European Commission：Cyber Resilience Act　https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act〔2026/7/31 確認〕
iv　デジタル庁：DFFT　https://www.digital.go.jp/policies/dfft〔2026/7/31 確認〕

3.3 製品・サービスの評価・認証制度、及び暗号技術の動向

IPA ではサイバーセキュリティ対策の実現に向け、国民に向けた情報提供や啓発活動、企業・組織に対するセキュリティ施策の促進とともに、政府機関や独立行政法人等が IT 製品やクラウドサービス等を安全に調達及び利用するために活用できる制度の運営を行っている。

本節では、IoT 製品のセキュリティレベルを可視化する「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」、IT 関連製品のセキュリティ機能の適切性・確実性をセキュリティ評価基準の国際標準である ISO/IEC 15408 に基づいて評価する「IT セキュリティ評価及び認証制度（JISEC）」、及び政府が求めるセキュリティ要求を満たしているクラウドサービスを評価・登録する「政府情報システムのためのセキュリティ評価制度（ISMAP）」の動向について報告する。また、世界中で本格化している「耐量子計算機暗号（PQC：Post-Quantum Cryptography）」への移行の動向についても報告する。

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）

2025 年 3 月から、IPA では IoT 製品のセキュリティレベルを可視化する「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）」の運用※126 を開始した。図 3-3-1 に JC-STAR のロゴを示す。

本項では、JC-STAR の目的・制度概要、発足から 1 年間の歩みと今後の取り組み等について解説する。JC-STAR が発足した背景や制度の詳細については「情報セキュリティ白書 2025※127」の「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）」や JC-STAR ホームページ※128 を参照されたい。

■図 3-3-1　JC-STAR ロゴ

(1) JC-STAR 制度の目的

様々な IoT 製品がインターネットにつながることで、多様で便利なサービスが提供されている一方、IoT 製品を狙ったサイバー攻撃が増加している。実際、マルウェアに感染した多くの IoT デバイスが乗っ取られてボット化し、DDoS 攻撃によって社会システムを実際に停止させるといった被害が発生している※129。また、ネットワークカメラやセットトップボックス、制御システムへの不正アクセス等により、プライバシー侵害やシステム誤動作、場合によっては犯罪への踏み台にされるといったインシデントが引き起こされることもある。実際、2024 年に発生したインターネットバンキングに係る不正送金事犯の少なくとも 44% は、一般家庭の IoT 機器を踏み台にしたものと公表されている※21。

IoT 製品に対するリスク管理が難しい理由は、例えばネット家電のようなメンテナンスフリーで使うことが前提の機器ではセキュリティ管理という概念そのものになじみがなかったり、何かあってもユーザーに異常を知らせる手段が制約されている機器があったりする点にある。その結果として、正常系の動作に問題が起きていなければ、たとえマルウェアに感染したり不正アクセスが起きていたりしたとしても、ユーザーは自分が使っている IoT 製品に問題が発生していることに気が付かないというリスクがある。

そこで、あらかじめ必要なセキュリティ対策がされた IoT 製品を選びやすくするため、JC-STAR 制度が発足した。本制度は、ユーザーにとってはどの IoT 製品のセキュリティ対策が適切かを外見的には判断できないこと、一方製造ベンダーにとってはセキュリティ対策に取り組んでいることのアピールが難しいという問題について、「適合ラベル」（図 3-3-2）という目印を介して両者の橋渡しをすることを意図している。



■図 3-3-2　適合ラベルの例

(2) JC-STAR 制度概要

JC-STAR は、セキュアな IoT 製品の設計開発及び脆弱性対応を実現するため、セキュア・バイ・デザインの考えのもと、IoT 製品等に対する独自に定めるセキュリティ要件（適合要件）への適合性を確認・可視化する日本の制度である。以下に概要を説明する。

(a) 適合要件について

JC-STAR の適合ラベルは、インターネットとの通信が行える幅広い IoT 製品を対象として、共通的な物差しでその製品に具備されているセキュリティレベルを可視化することを目的としている。

適合ラベルを取得するために求められる水準に応じたセキュリティ要件として、以下の合計 4 段階の基準を設けており、レベルが上がる程、高度なセキュリティ要件となる。

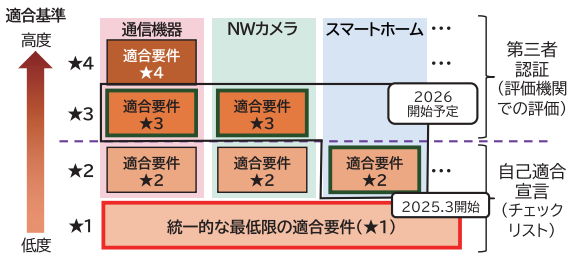
- ★ 1：最低限の脅威に対抗するための製品共通の適合要件
- ★ 2 ～★ 4：IoT 製品類型ごとの特徴に応じた適合要件

これらは、日本独自に定めたセキュリティ要件に基づく基準となっているが、相互承認の実現を見据えて ETSI EN 303 645[※130]、NIST IR 8425[※131]、EU CRA（Cyber Resilience Act[※132]）等の国内外のセキュリティ要件等とも調和するように配慮している。

大まかには、「★ 1」と「★ 2」は主に民間が利用する製品を対象としており、自己適合宣言で適合ラベルを取得できる。一方、「★ 3」と「★ 4」は政府機関や重要インフラ等の重要なシステムでの利用も想定しており、第三者認証を求めている（図 3-3-3、表 3-3-1）。

2025 年 3 月からスタートしたのは「★ 1」であり、2026 年以降、通信機器とネットワークカメラの「★ 3」とスマートホームの「★ 2」を開始する予定である。

例えば、「★ 1」では、製品類型を限定せずに、広範



■図 3-3-3　適合基準（イメージ）
（出典）IPA「セキュリティラベリング制度（JC-STAR）についての詳細情報」を基に編集

レベル	位置付け
★ 4	政府機関や重要インフラ事業者、地方公共団体、大企業等の重要なシステムでの利用を想定した製品類型ごとの汎用的なセキュリティ要件を定め、それを満たすことを独立した第三者が評価して示すもの
★ 3	
★ 2	製品類型ごとの特徴を考慮し、「★ 1」に追加すべき基本的なセキュリティ要件を定め、それを満たすことをベンダーが自ら宣言するもの
★ 1	製品として共通して求められる最低限のセキュリティ要件を定め、それを満たすことをベンダーが自ら宣言するもの

■表 3-3-1　適合基準のレベルとその位置付け

な IoT 製品を対象とした最低限の脅威に対抗するための統一的なセキュリティ要件として、デバイスリソースや性能が非常に限られた IoT 機器であっても実現してもらいたい対策だけに絞っている。具体的には、以下を求めている。

- マルウェアに感染してボット化するのを防ぐ。とりわけ、感染したデバイスからの感染拡大を防止する。
- インターネット側からの遠隔攻撃を想定し、スクリプトキディレベル（限定的な専門知識のみを有し、インターネットやダークウェブ等で公開されているクラックツール等を用いてシステムの脆弱性を利用して攻撃するレベル）の攻撃に対して実用的な耐性を持たせる。
- 製品不具合や脆弱性に対する対応・サポート方針を明確化し、適合ラベル有効期間内のサポート（アップデートファイルの提供等）が確実に実施されるようにする。
- 廃棄前に、運用中に生成されたデータを適切に削除することができる。

「★ 1」では、更に海外制度との国際連携を可能とする観点も踏まえ、全部で 16 個の適合要件を定めている[※133]。

(b) 適合ラベルについて

適合ラベルは、適合基準のレベルに応じて定められた適合要件に適合していると認められた場合に交付される。このラベルには、IoT 製品が取得した適合基準のレベルと登録番号のほか、IPA が管理する当該 IoT 製品情報を確認するための「適合ラベル取得製品情報ページ」（以下、製品情報ページ）の URL を埋め込んだ二次元コードが組み込まれている。この製品情報ページは登録番号ごとに用意される。

製品情報ページでは、適合ラベルが交付された IoT 製品の申請者情報、製品情報、適合ラベル情報、セキュリティ情報（アップデート情報や脆弱性情報等）、サポート

期間、問い合わせ先情報等、多岐にわたる情報を最新に維持しながら一元的に提供できる仕組みを取り入れている。これにより、いつまでこの IoT 製品を安全に使えるかが分かり、また IoT 製品利用中のセキュリティ対策やトラブル発生時等の対処がしやすくなることを期待している。

更に、製品情報ページを表示した時点での適合ラベルの有効性を示す「適合ラベルのステータス」を表示することで、市場に長期間流通中の IoT 製品についてもその時々の適合ラベルの状態をリアルタイムで確認できる。

(c) 適合ラベルの取得について

「★ 1」と「★ 2」では、ベンダーが適合要件を実際に満たしているかどうかを具体的に判断するための評価手順（評価手法・評価ガイド）に従って自らチェックリストにより適合性を確認し、すべての要件を満たしていると判定した場合に適合ラベルの申請を行う自己適合宣言方式を採用している。

一方、高い信頼性が求められる「★ 3」と「★ 4」では、JC-STAR 評価機関が適合性を客観的に評価し、IPA が認証・適合ラベル交付を行う第三者評価・認証方式を採用している。なお、JC-STAR 評価機関は、独立行政法人製品評価技術基盤機構（NITE：National Institute of Technology and Evaluation）の認定及び IPA の承認を必要とする。

図 3-3-4 に JC-STAR 適合ラベルの取得スキームについて示す。

(3) 2025 年度の状況

JC-STAR の運用開始初年度の実績は以下のとおりであり、新たなセキュリティ製品認証制度としては順調な立ち上がりを見せた。以下に実績概要を示す。

(a) 適合ラベル申請・発行実績

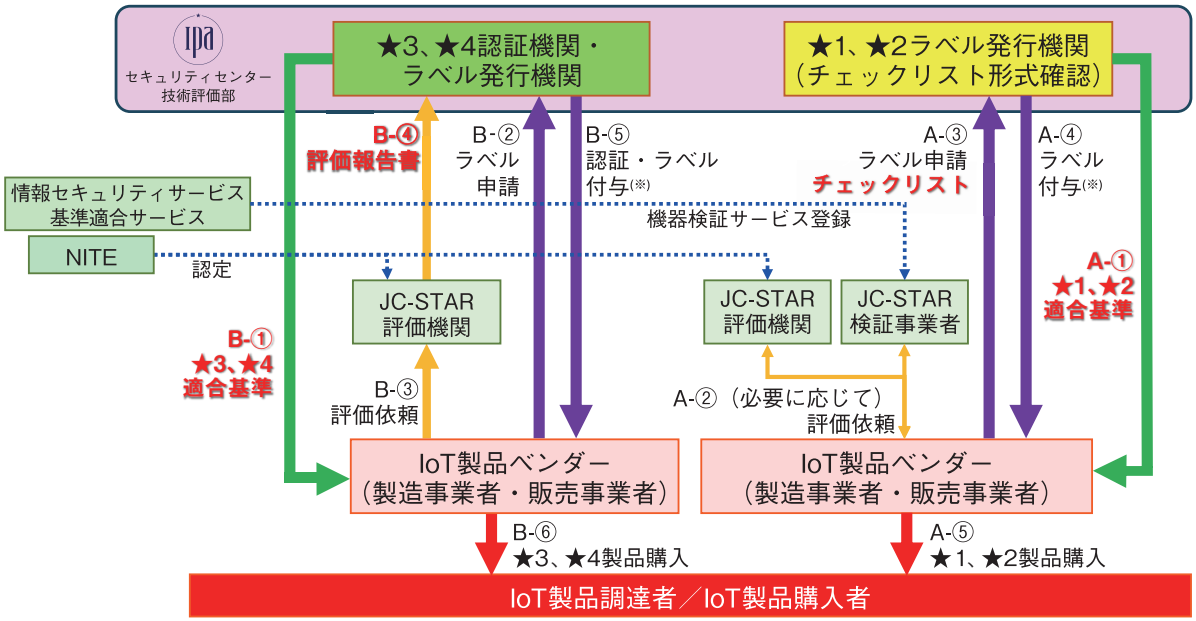
2025 年 3 月 25 日から申請の受付を開始し、2026 年 3 月末で 80 社 199 件の適合ラベルを交付している（次ページ図 3-3-5）。なお、同じセキュリティ対策をしているファームウェアを共通して利用している異なる種類の製品に対しても同じ適合ラベルを使うことができることから、製品型番数としては 1,500 製品型番以上が登録されている。

製品種別としては、通信機器、ネットワークカメラ、エネルギー関連機器での取得件数が多い。

(b) 調達要件での活用

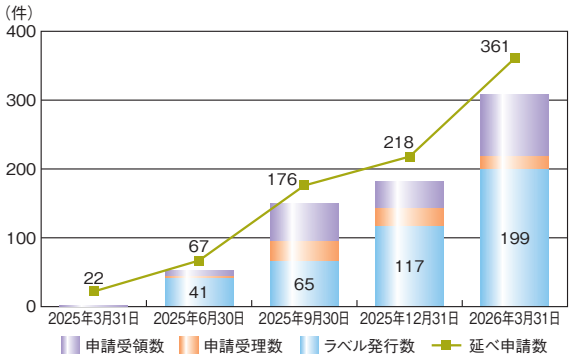
JC-STAR 制度が正式に開始されたことを受け、政府機関、重要インフラ事業者、地方公共団体等での調達要件に適合ラベル取得製品を活用するよう、各種ガイドラインに反映された。例えば、以下のガイドラインに反映された。

- 「政府機関等の対策基準策定のためのガイドライン（令和 7 年度版）」（2025 年 9 月改定）※ 134
- 「地方公共団体における情報セキュリティポリシーに



(※) IPAは、ラベル取得の申請に対して、ラベル発行前にサプライチェーン・リスクについて経済産業省を含めた政府関係機関に照会をかけ、その照会結果に基づきラベルを付与する。

■図 3-3-4　JC-STAR 適合ラベルの取得スキーム
（出典）IPA「セキュリティラベリング制度（JC-STAR）についての詳細情報」を基に編集



■図 3-3-5　JC-STAR 適合ラベルの申請・発行実績

関するガイドライン（令和 7 年 3 月版）」（2025 年 3 月改定）※ 57

- 「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 Ver3.0」（2025 年 5 月改定）※ 135

(c) 他国制度との相互承認

2025 年の G7 サイバーセキュリティワーキンググループにて、IoT 製品セキュリティ対策での有志国連携の重要性が確認された※ 136。また、欧米等でも IoT ラベリング制度が作られている状況に鑑み、各国制度との連携を図り、相互承認に向けた交渉を行っている（表 3-3-2）。これにより、IoT 製品を海外に輸出する際に求められる適合性評価にかかるベンダーの負担を軽減できると期待される。

2025 年度は、英国とシンガポールとの間で相互承認に関する覚書を取り交わした。英国 PSTI 法（Product Security and Telecommunications Infrastructure Act ※ 137）との相互承認は 2026 年 1 月 1 日から、シンガポール CLS（Cybersecurity Labelling Scheme ※ 138）との相互承認は 2026 年 6 月 1 日から開始した。

なお、相互承認とは言っても「認証そのもの」が認められるのではなく、同じセキュリティ要件に該当すると判断された技術要件での「評価が免除」されることであることに注意されたい。つまり、同じセキュリティ要件の評価についてはどちらかで実施すればよいが、重なっていない部分のセキュリティ要件の評価はそれぞれの制度の中で実施する。加えて、各々の制度が求める非技術的要件についても同様である。

このほか、IoT ラベリング制度の推進を図る国際的な枠組みとして、2025 年 10 月に日本を含む 11 ヵ国が参

国・地域	シンガポール	英国	米国	EU
制度名	Cybersecurity Labelling Scheme (CLS)	Product Security and Telecommunications Infrastructure Act（PSTI 法）	U.S. Cyber Trust Mark	Cyber Resilience Act（CRA）
マーク	CYBERSECURITY LABEL REGISTRATION ID: CSA/IOTWABCD MORE INFO AT: www.csa.gov.sg/cls	ステッカーのみ	U.S. CYBER TRUST MARK	CE
開始時期	2020 年 10 月開始	2024 年 4 月施行	2027 年 1 月開始予定	・報告義務 :2026 年 9 月 ・その他 :2027 年 12 月
相互承認	2026 年 6 月 1 日	2026 年 1 月 1 日	―	―
任意/義務	任意	義務	任意	義務
対象	消費者向け IoT 機器	消費者向け IoT 製品	消費者用無線 IoT 製品	デジタル要素を含む製品
適合基準	・＊ 1：ETSI EN 303 645 の基準の一部 ・＊ 2：＊1の基準に加え、ETSI EN 303 645 の基準の一部 ・＊3及び＊4:＊2の基準に加え、IMDA「IoT Cyber Security Guide」の基準	ETSI EN 303 645 の基準の一部（5.1-1、5.1-2、5.2-1、5.3-13）	NIST IR 8425 をベースとした基準となる見込み	・製造者への「セキュリティ特性要件に従った上市前の設計・開発・製造」「上市後の積極的に悪用された脆弱性・インシデントの報告」 等を義務付ける予定
評価方法	・＊ 1 及び＊ 2：自己適合宣言 ・＊ 3 及び＊ 4：自己適合宣言及び評価機関による試験	自己適合宣言	第三者認証	・クリティカル製品：第三者認証 ・クラスⅠ・Ⅱの製品：第三者認証 ・上記以外の製品：自己適合宣言

■表 3-3-2　諸外国の IoT 適合性評価制度

加する「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）」が発足した※139。

更に、米国（U.S. Cyber Trust Mark※140）、EU（CRA：Cyber Resilience Act※132）、ドイツ、オーストラリア等とも、引き続き各国制度との相互承認に向けた交渉を行っている。

(d) JC-STAR 賛同団体との連携

JC-STAR の普及展開に向けた取り組みの一つとして、JC-STAR との連携や会員企業への積極的な適合ラベル取得の働きかけを行うことに賛同している業界団体に協力をいただき、各業界団体に加盟する会員企業での適合ラベル取得の働きかけを連携して推進している。

2026 年 6 月時点で以下の 9 団体が賛同団体となっている（五十音順）。

- 一般社団法人組込みシステム技術協会（JASA：Japan Embedded Systems Technology Association）
- 工業会 日本万引防止システム協会（JEAS：The Japan Industrial Association of Electronic Article Surveillance Machines）
- 一般社団法人情報通信ネットワーク産業協会（CIAJ：Communications and Information network Association of Japan）
- 一般社団法人セキュア IoT プラットフォーム協議会（SIOTP：Secure IoT Platform Consortium）
- 一般社団法人デジタルライフ推進協会（DLPA：Digital Life Promotion Association）
- 一般社団法人電子情報技術産業協会（JEITA：Japan Electronics and Information Technology Industries Association）
- 一般社団法人日本自動販売システム機械工業会（JVMA：Japan Vending System Manufacturers Association）
- 公益社団法人日本防犯設備協会（JSSA：Japan Security Systems Association）
- 一般社団法人ビジネス機械・情報システム産業協会（JBMIA：Japan Business Machine and Information System Industries Association）

(e) JC-STAR 制度の普及促進

JC-STAR 制度は、政府機関、重要インフラ事業者、地方公共団体等での調達要件での活用だけでなく、一般消費者にも活用してもらうことで IoT 製品のセキュリティ向上を図ることも視野に入れている。

例えば、一般消費者向けの IoT 製品の中には、外出先からでも操作ができる生活家電、いわゆるネット家電がある。そのようなネット家電を購入する際にはほとんどセキュリティが意識されないか、逆にセキュリティが不安で購入自体をあきらめるというケースも考えられる。こういったケースでも JC-STAR の「適合ラベル」が「安心して使えるネット家電」であることの目印になることが期待される。

そこで、一般消費者にも JC-STAR 制度の必要性や有用性を伝えるための普及促進を実施し、実際に購入する際に活用してもらうような取り組みを行っている。例えば、自由にダウンロードして利用できるチラシやポスター、ポップを作成、公開している※141（図 3-3-6）。



■図 3-3-6　JC-STAR 制度のポスター、チラシ、ポップ

2026 年 2 月には、JEITA 及び一般社団法人大手家電流通協会と協力して、「未来の暮らしを、もっと安全に。JC-STAR で選ぶ IoT」と題した制度周知イベント※142 を開催した。これは、制度運営者である IPA、IoT 製品の製造ベンダーが集まる JEITA、そして一般消費者に IoT 製品を販売する大手家電販売事業者が一堂に会したイベントとして、単なる制度紹介にとどまらず、家電量販店で実際に適合ラベル取得 IoT 製品を購入できることを広くアピールした。

(4) 今後の予定

2026 年 6 月に通信機器とネットワークカメラの「★ 3」セキュリティ要件が公開された※143。「★ 3」では、例えば SBOM の活用が求められたり、ペネトレーションテストによる脆弱性診断が加わる等、「★ 1」と比較するとかなり高いセキュリティ対策が求められる（次ページ表 3-3-3）。

今後、「★ 3」適合要件・評価ガイドの公開や JC-STAR 評価機関の承認等の必要な整備を行い、2026 年秋ごろに「★ 3」の受付を開始する予定としている。また、スマートホームの「★ 2」適合要件の作成も開始されており、2026 年秋から冬にかけて適合要件を策定し、

カテゴリ	★1	★3
1. 脆弱な認証・認可メカニズム（例：汎用のデフォルトパスワード、脆弱なパスワード）を使用しない	✓（実機テスト）	✓（実機テスト）
2. 脆弱性の報告を管理するための手段を導入する	✓	✓
3. ソフトウェアを最新の状態に保つ	✓（実機テスト）	✓（実機テスト、SBOM）
4. 機密セキュリティパラメータをセキュアに保存する	✓	✓
5. セキュアに通信する	✓	✓（実機テスト）
6. 露出した攻撃面を最小化する	✓（実機テスト）	✓（実機テスト）
7. ソフトウェアの完全性を確実にする		✓
8. 個人データがセキュアであることを確実にする		✓
9. 停止に対してレジリエントなシステムにする	✓（実機テスト）	✓（実機テスト）
10. システムのテレメトリデータを検証・保護する		✓（実機テスト）
11. ユーザが簡単にデータを消去できるようにする	✓（実機テスト）	✓（実機テスト）
12. 製品の設置及びメンテナンスを容易にする		✓（実機テスト）
13. 入力データの妥当性を確認する		✓（実機テスト）
14. 個人データを適切に処理する		✓（実機テスト）
15. 製品を識別可能にする		
16. 脅威を特定しテストする		✓（ペネトレーションテスト）
17. 製品に関する情報提供を行う	✓	✓
18. 文書化する		
19. 製品の可用性を確実にする		✓（実機テスト）
20. セキュアなセッションを確立する		
21. ハードウェアの完全性を確実にする		✓

※カテゴリ 11 を除き、「★ 1」と「★ 3」の両方に✓がある場合でも各カテゴリのセキュリティ要件の内容は異なり、「★ 3」では「★ 1」より高いセキュリティ対策が求められる。

■表 3-3-3　通信機器・ネットワークカメラにおける適合要件「★ 1」と「★ 3」の違い

受付を開始する予定である。

このほかにも、「★ 2」以上の適合要件を策定する対象について協議中であり、協議が整い次第、順次適合要件の策定作業に入る予定である。

3.3.2 IT セキュリティ評価及び認証制度（JISEC）

IT 製品が政府調達におけるセキュリティ要件を満たすことを確認する仕組みとして、セキュリティ評価制度が欧米諸国を中心に発展し、セキュリティ評価基準が国際標準 ISO/IEC 15408 として策定された。日本でも、このセキュリティ評価基準を用いて IT 製品を評価する「IT セキュリティ評価及び認証制度（JISEC：Japan Information Technology Security Evaluation and Certification Scheme）[※144]」を IPA が運営し、政府機関等の IT 製品調達に活用されている。

本項では JISEC の最新動向について解説する。

(1) 政府の IT 製品調達におけるセキュリティ要件

サイバーセキュリティ戦略本部が発行している「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（令和 7 年度版）[※145]」（以下、政府統一基準）では、府省庁及び独立行政法人等の情報システムセキュリティ責任者に対し、情報システムを構成する IT 製品を調達する場合、経済産業省が発行している「IT 製品の調達におけるセキュリティ要件リスト」（以下、調達要件リスト）を参照し、想定されるセキュリティ上の脅威に対抗するためのセキュリティ要件を策定することを遵守事項として定めている。

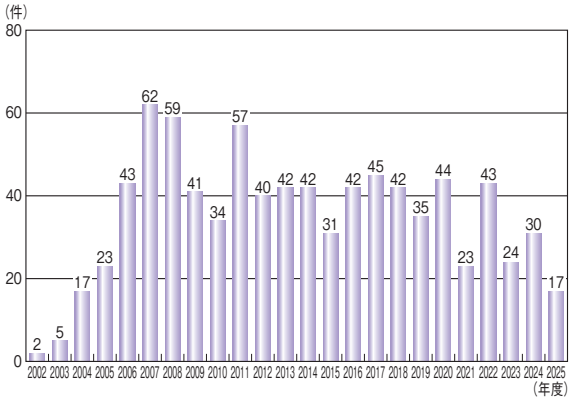
調達要件リストでは、対象製品分野の IT 製品がセキュリティ要件を満たすことを確認する方法として、調達時に受け入れテスト等で確認する方法と、国際標準に基づく認証取得を確認する方法があることを示している。この中で、JISEC は、ISO/IEC 15408 に基づく第三者認証制度であり、JISEC で認証されたセキュリティ要件を満たす IT 製品を調達することで、政府統一基準の要求を満たすことができるとされている。

なお、近年の動向を踏まえ、調達要件リストは 2026 年 2 月に第 2.1 版に更新された[※146]。

調達要件リストの対象製品分野の中でも特に、構築時に受け入れテストを行う情報システムとは独立して調達されることの多いデジタル複合機の調達、国策としてセキュリティ対策が重要となる旅券やマイナンバーカードのスマートカードの調達等で JISEC の認証制度が活用されている。2025 年度は次期マイナンバーカードのプロテクションプロファイルの認証が行われた。2026 年度は次期マイナンバーカード自体の認証が進められ、2027 年度以降に認証された次期マイナンバーカードに順次切り替わっていく予定である。

(2) 認証の状況

2025 年度までの JISEC における認証発行件数の推移を図 3-3-7 に示す。2025 年度は、JISEC に適用されるセキュリティ評価基準（CC/CEM）に関して、旧規格のセキュリティ評価基準 CC/CEM v3.1 に基づく認証受付を終了し、新規格の CC/CEM:2022 に基づく認証に切り替わる移行期間中であったこともあり※147、認証発行件数は例年よりも少なく 17 件であった。



■図 3-3-7　JISEC の認証発行件数の推移

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）

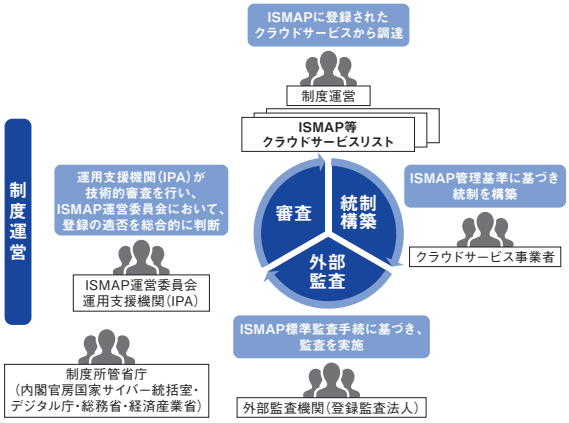
「政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program：通称、ISMAP（イスマップ））」は、政府が求めるセキュリティ要件を満たしているクラウドサービスをあらかじめ評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスの円滑な導入に資することを目的とした制度である。本項では、ISMAP の概要や運用を始め、制度の課題と今後の改善に向けた取り組みについて紹介する。

(1) ISMAP の概要

2018 年 6 月に公開された「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（現、「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針※148」）では、「クラウド・バイ・デフォルト原則」が掲げられた。これを受けて、総務省と経済産業省は 2018 年 8 月から「クラウドサービスの安全性評価に関する検討会※149」を発足、「ISMAP 管理基準※150」を制定し、2020 年 6 月に制度の運用を開始した。

政府機関等におけるクラウドサービスの導入において、ISMAP 運用前は、個々のクラウドサービスが実施する情報セキュリティ対策を調達者が直接確認する必要があったが、この制度により確認を省略でき、負担が軽減される。同制度の基本的な枠組みを図 3-3-8 に示す。

クラウドサービス事業者は、ISMAP 管理基準に基づき統制を構築し、クラウドサービスを運用する。外部監査機関は、統制の整備状況や運用状況を監査し、結果をクラウドサービス事業者に報告する。その監査の結果等を踏まえ、クラウドサービス事業者は ISMAP への登録申請を行う。運用支援機関である IPA は申請内容について技術的な審査を行い、ISMAP 運営委員会の決定に基づき ISMAP 等クラウドサービスリスト（以下、サービスリスト）へ登録する。政府機関等は、原則サービスリストに掲載されているサービスを調達する。



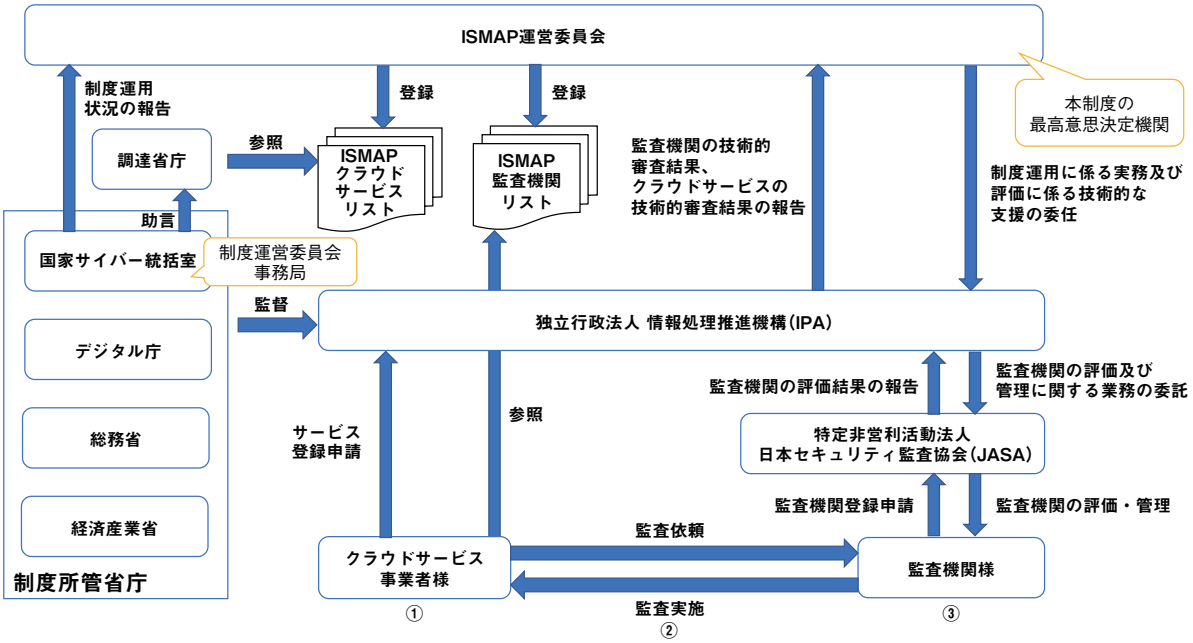
■図 3-3-8　ISMAP の基本的な枠組み
（出典）NCO「政府情報システムのためのセキュリティ評価制度（ISMAP）について※151」を基に IPA が編集

(2) クラウドサービスの安全性評価の制度のフロー

同制度においては、政府機関等が調達するクラウドサービスに要求される基本的な情報セキュリティ管理・運用の基準を満たすセキュリティ対策を実施していることが確認されたクラウドサービスが、サービスリストに登録される。

また、同制度における監査を実施できる監査機関は、当該監査に求められる要求事項を満たすことが確認された後、同制度が公表する ISMAP 監査機関リスト（以下、監査機関リスト）に登録される。同制度のフローを図 3-3-9（次ページ）に示す。

なお、同制度の運用に係る実務及び評価に係る技術的な支援は IPA が行い、そのうち、監査機関の評価及び管理に関する業務については、IPA から特定非営利活動法人日本セキュリティ監査協会（JASA：Japan Information Security Audit Association）に委託している。

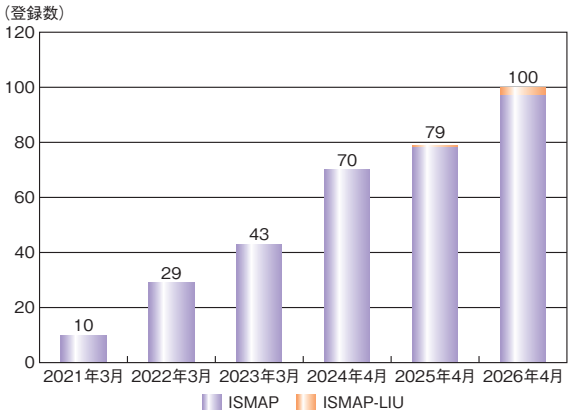


■図 3-3-9　クラウドサービスの安全性評価の制度のフロー
(出典)ISMAP「ISMAP 概要※152」

(3) ISMAP の運用

同制度は、2020 年 6 月に内閣官房（内閣サイバーセキュリティセンター、情報通信技術（IT）総合戦略室）、総務省、経済産業省の所管で運用が開始され、2021 年 9 月以降は、内閣サイバーセキュリティセンター（現 NCO）、デジタル庁、総務省、経済産業省の所管で運営され、運用支援は IPA が担当している。最高意思決定機関として有識者と所管省庁を構成員とした ISMAP 運営委員会を設置している。

制度の概要、基準規程類、監査機関リスト、及びサービスリストは、ISMAP ポータルサイト※153 で公開されており、2026 年 4 月末日時点で、登録されている監査機関は、7 機関、クラウドサービスは 100 サービス（うち 3 件は ISMAP-LIU（ISMAP for Low-Impact Use））である（図 3-3-10）。「ISMAP-LIU」は、主に「機密性 2 情報」を扱うクラウドサービスのうち、リスクの小さい業務・情報の処理に用いる SaaS サービスを対象としており、2022 年に運用を開始した。



■図 3-3-10　クラウドサービスの登録数の推移

なお、情報システムのセキュリティ確保の責任は、一義的に当該システムの調達者または利用者が負うものである。このことは「クラウドサービスの安全性評価に関する検討会とりまとめ※154」にも記載されている。同制度に登録されたサービスを選定した上で、選定したクラウドサービスにおけるセキュリティリスクを把握し、適切なセキュリティ対策を実施することで初めて情報システム全体としてクラウドサービスを安全に利用することができる。調達者は、利用するクラウドサービスについて適切な設定を行うことに加えて、情報システム全体のセキュリティリスクを把握し、適切な対策を行うことが求められる。

(4) 制度改善に向けた更なる取り組み

ISMAP は 2020 年 6 月の運用開始から 6 年が経過し、政府機関等がクラウドサービスを調達する際のセキュリティ・信頼性を評価する制度として定着している一方で、登録申請を行うクラウドサービス事業者（図 3-3-9 の①）等より負担軽減等の要望が上がっている。具体的には、登録申請を行うクラウドサービス事業者からは、実施すべき詳細管理策の数が多く負担が大きいことや、監査を受けるにあたって監査機関が少ないために費用が高額になっていること等が指摘されている。これらの課題につ

いて、制度所管省庁及び運用支援機関であるIPAは、有識者や関係者等の意見を踏まえつつ、継続的に改善を進めているところである。

内閣府に設置された規制改革推進会議にて審議された、2025年5月の「規制改革推進に関する答申※155」を受け、2026年3月、ISMAP制度の所管省庁は、制度見直しの具体的な取り組みの工程表を公開している※156。制度改善に向けた主要な取り組みは、以下のとおりである。

- 制度の抜本的な見直し
  「外部監査（前ページ図3-3-9の②）の負担軽減」「審査の迅速化」という課題に対しては、詳細管理策の記載粒度の変更を行い、統制目標を実現するために満たすべき必要最小限の内容に絞り、千を超える詳細管理策の数を数百に削減する方針で「ISMAP管理基準」を改定する予定としている。改定案については、パブリック・コメントを実施※157の上、2025年12月に公表した※158。
  また、SaaS事業者を対象として、他の認証制度の活用等を通じた、負担を軽減した新たな枠組みの検討も行っている。
- 監査機関（前ページ図3-3-9の③）の拡充
  「監査の効率化」を目的に、監査法人以外の法人も参入可能とするとともに、監査機関の拡充により監査の品質が低下しないよう、ISMAP業務に対する組織的な品質管理体制を整備することを規定した内容等を追加して「ISMAP監査機関登録規則※159」を改定した。
- 情報発信及びコミュニケーションの促進
  円滑なISMAP取得を目的として、定期的にISMAPポータルサイトのFAQ※160の更新を実施しており、2025年度は19件のFAQの更新、追加、削除を実施している。また、制度所管省庁は、制度改善の取り組み状況の説明と意見の聴取のために制度説明会を実施し、クラウドサービス事業者や監査機関等とコミュニケーションを取る機会を設けている。
- ISMAP-LIUにおける利用省庁による事前の影響度評価の廃止、対象業務の拡大等
  ISMAP-LIUでの登録申請前における負担軽減を図るため、政府機関等からの業務・情報の影響度評価結果については登録申請前の入手を不要とするよう、「ISMAP-LIUクラウドサービス登録規則」を改定した。同規則の改定には、事業者の参入促進を目的として、ISMAP-LIUの対象業務を8業務から10業務へ拡大する内容も含まれている。ISMAP-LIUにおける対象業務一覧を表3-3-4に示す。なお、2025年4月に追加になった2業務は、表の項番9、10が該当する。また、ISMAP-LIUへの登録促進を図るため、ISMAPを取得する場合とISMAP-LIUを取得する場合のメリットを明確にし、デジタル庁のWebサイトに公開した※162。

項番	対象業務
1	公表を前提とした政策・制度の立案・調整過程等で民間と連携して作業する業務
2	政府機関等職員の業務上の役職・氏名等情報を扱う業務
3	名刺情報等の一般に広く提供する範囲の情報、公開情報の配信に伴う配信先等管理情報を扱う業務
4	民間から提供される情報であり、当該情報提供者が低リスクだと判断している情報を処理する業務
5	オープンソース・公知の事実・一般公開情報を扱う業務だが例外的に要機密扱いとする必要がある場合
6	災害時等に組織構成員の被災状況確認等を行う業務
7	組織構成員に対する組織ルールやビジネススキル等の教育を行う業務
8	「行政文書の管理に関するガイドライン」において保存期間1年未満に該当するもののうち、定型的・日常的な業務連絡等を扱う業務
9	システムの維持・管理のために、性能や稼働状況を確認する業務
10	スケジュール調整、タスク管理、イベント管理、反復処理などの作業を効率化するために、職員を（機械的に）補助する業務

■表3-3-4　ISMAP-LIUにおける対象業務一覧
（出典）NCO、デジタル庁、総務省、経済産業省「ISMAP-LIUにおける業務・情報の影響度評価ガイダンス※161」を基に作成

今後も最新の国際規格等を「ISMAP管理基準」に反映することで、クラウドサービスの安全性・信頼性を適切に評価する枠組みを維持しつつ、登録申請を行うクラウドサービス事業者の負荷軽減を目的とした監査・審査プロセスの効率化や、円滑なISMAP取得を支援するための情報発信等、制度改善に向けた継続的な見直しを進めていく。

3.3.4 暗号技術の動向

量子コンピューター関連技術の発達は目覚ましく、今まで実現できなかった計算ができるようになり、高度な最適化問題の解決や高精度なシミュレーションの実現に期待が寄せられている。一方、現在使っている暗号技術（特に公開鍵暗号）が量子コンピューターによって解読されるおそれが生じている。

いつ量子コンピューターによって暗号技術が解読され

るかについては様々な見解があり、今のところ正確には分かっていない。しかし、今から暗号文を蓄積しておき、いずれ量子コンピューターで解読できるようになったときに蓄積しておいた暗号文を解読して情報を入手するハーベスト攻撃（HNDL 攻撃：Harvest Now, Decrypt Later Attack）への対応や、暗号技術の移行には非常に長い時間がかかることも考慮し、量子コンピューターに対して安全とされる「耐量子計算機暗号（PQC：Post-Quantum Cryptography）」への移行が世界中で本格化している。

（1）日本における PQC 移行について

ここでは、PQC への移行について、日本政府及び CRYPTREC の 2025 年度の動きを概説する。

（a）日本政府の動き

2025 年 6 月、内閣官房副長官補を議長とする「政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議」が設置※163され、日本政府機関等における PQC 移行方針の検討が本格化した。同年 11 月には中間とりまとめ※164が行われており、その中で「政府機関等の耐量子計算機暗号（PQC）への移行に向けた工程表（ロードマップ）（骨子）」が以下のようにまとめられている。

- 対象システムは政府統一基準の適用対象となる情報システムとする。
- 原則として 2035 年を目途に PQC への移行を行う。ただし、情報の重要性や暗号技術の利用状況等を把握した上で、どのように移行を進めるかを検討し、適切に判断する必要がある。
- 安全性が低下・危殆化した暗号技術の利用停止に係る時期は、今後の量子コンピューターの進展を踏まえた暗号技術の安全性評価、政府機関等における PQC 移行等の状況、諸外国の状況等を十分に踏まえながら、「CRYPTREC 暗号リスト※165」の取り扱い等について、具体的方策の検討を進めていく。
- 引き続き、政府機関等が移行に向けた計画を策定できるよう、移行に向けた計画に盛り込むべき基本的事項や留意すべき事項を検討し、工程表（ロードマップ）を策定する。
- 各政府機関等は、今後策定する工程表（ロードマップ）を踏まえ、移行に向けた計画を策定し、移行期限までに PQC 移行を行う。

この骨子は、2025 年 12 月に閣議決定した「サイバーセキュリティ戦略」に反映されており、「政府機関等における PQC への移行について、原則として、2035 年までに行うことを目指し、政府機関等における暗号技術の利用状況等も踏まえ、関係府省庁の連携の下、2026 年度に工程表（ロードマップ）を策定し、我が国における円滑な移行を推進していく。」と明記された。

（b）CRYPTREC の動き

CRYPTREC（Cryptography Research and Evaluation Committees）は、電子政府のサイバーセキュリティを確保するため、電子政府システムでの利用を推奨する暗号アルゴリズムのリストである「CRYPTREC 暗号リスト」の安全性を評価、監視し、その適切な実装方法や運用方法を調査、検討することを目的に組織されたプロジェクトである。デジタル庁、総務省及び経済産業省が共同で運営する暗号技術検討会と、NICT 及び IPA が共同で運営する暗号技術評価委員会及び暗号技術活用委員会で構成される。

CRYPTREC では、政府の PQC 移行に係る方針に合わせる形で、PQC をテーマとした活動としては以下を行っている※166。

- 暗号技術検討会：
  「耐量子計算機暗号（PQC）に対応した CRYPTREC 暗号リストの在り方」について検討を行い、「CRYPTREC 暗号リスト」内の「電子政府推奨暗号リスト」の中に従来の「現行暗号リスト」とともに、「耐量子計算機暗号（PQC）リスト」を追加した。
  また、引き続き議論が必要な課題が複数あるため、暗号技術検討会の直下に、新たに「耐量子計算機暗号（PQC）リスト検討タスクフォース」を設置することも決定した。
- 暗号技術評価委員会：
  「CRYPTREC 暗号リスト」への掲載に向けた PQC の技術的検討として、FIPS 203（ML-KEM）※167の安全性・実装性能に関する調査・評価を外部評価により実施した。併せて、PQC への移行に関する技術動向調査※168を実施した。
  2026 年度は、FIPS 204（ML-DSA）※169と FIPS 205（SLH-DSA）※170を対象として安全性評価・実装性能評価を実施することも決定した。
- 暗号技術活用委員会：
  各国政府・公的機関等が公表している「PQC への移行方針」や関連ガイドラインについて政策的側面から整理し、また「CRYPTREC 暗号リスト」での PQC に関

する位置付けや移行ルールを変更すべきかどうかを検討した。これらの成果は、PQC 移行の工程表策定や「耐量子計算機暗号（PQC）に対応した CRYPTREC 暗号リストの在り方」の検討に反映された。

2026 年度は、暗号強度要件ガイドライン※171 に PQC の取り扱いを含める形で見直しを実施すること、また「TLS 暗号設定ガイドライン※172」については、PQC サポートに向けた TLS 1.3 への移行や PQC 関連技術の取り込み、現行のセキュリティ例外型の削除等、現在の TLS 暗号設定ガイドラインの前提条件が大きく変わりつつあることを踏まえ、記載内容の見直しの検討を開始することとなった。

(2) 海外における PQC 移行について

海外における PQC 移行のスケジュールや IETF（Internet Engineering Task Force）における標準化等、国際的な PQC 移行の動きについて述べる。

(a) G7 各国の動き

2025 年 4 月、G7 会合で「Accelerating the Transition to Quantum-Safe Communication: A Call for Global Collaboration and Action※173」が取りまとめられた。その中では、大きく三つのことを指摘している。

- G7 各国が協調して PQC への移行を進めるためのグローバルな連携の必要性
- 新たなリスクを軽減するための、いわゆるハイブリッド・アプローチの推進
- 明確な期限を定めた PQC 移行スケジュールを策定し、進捗状況を管理するためのグローバルな移行管理機関の創設

この方針に基づき、日本だけでなく、欧米諸国（米国：US、カナダ：CA、EU、英国：UK、オーストラリア：AU）でも PQC 移行スケジュールの策定・改定が進められた（図 3-3-11）。各国とも、移行の優先度が高い、国家安全保障システムや高セキュリティシステム等については 2030 年ごろ、その他のシステムについては 2035 年を移行期限の目途としていることが分かる。一方で、既存暗号、特に現行の公開鍵暗号との関連では、利用を止めるのかどうか、ハイブリッド実装を活用するのかどうかについては国ごとに違いがある。

(b) IETF 標準化の動き

2024 年 8 月に米国国立標準技術研究所（NIST：National Institute of Standards and Technology）により米国標準 PQC として FIPS 203、FIPS 204、FIPS 205 が公開された後、PQC に関する標準化は着実に進展している。なお、サイドチャネル攻撃耐性に関する検討が長引いている FIPS 206 についても NIST での標準化完了になお一定の時間を要すると見込まれるものの、標準化完了後には、同様の流れで IETF における標準化が進められると考えられている。

IETF において、CMS（Cryptographic Message Syntax）や X.509 証明書といった汎用的な暗号プロトコルを対象に、既存の公開鍵暗号を PQC にそのまま置き換える方式が RFC（Request For Comments）として標



■図 3-3-11　各国の PQC 移行スケジュール
（出典）暗号技術活用委員会「2025 年度　暗号技術活用委員会活動報告」（2025 年度 第 1 回 暗号技術検討会※166 の資料 4）

準化された。このような単純な置き換え方式は、一般に「Pure 方式」と呼ばれている。Pure 方式に関する RFC は、NIST によるアルゴリズム標準化からおおむね 1 年から 1 年半程度で公開されており、アルゴリズム標準からプロトコル標準への移行が比較的迅速に進んだ点が特徴である（表 3-3-5）。

FIPS 203、204、205 に対応する Pure 方式については、既に標準化が完了していることから、対応製品も順次登場しており、比較的早期に実運用での利用が可能になると見込まれている。Pure 方式は、既存プロトコルの構造を大きく変更することなく、暗号アルゴリズム部分を置き換えることができるため、プロトコル再設計を最小限に抑えられる点が利点である。このため、実装や運用における負担が比較的軽く、早期導入を目指す場合の有力な選択肢といえる。

アルゴリズム名	CMS での利用（Pure 方式）	X.509証明書での利用（Pure方式）
FIPS 203 ML-KEM（2024 年 8 月公開）	RFC 9936（2026 年 3 月公開）	RFC 9935（2026 年 3 月公開）
FIPS 204 ML-DSA（2024 年 8 月公開）	RFC 9882（2025 年 10 月公開）	RFC 9881（2025 年 10 月公開）
FIPS 205 SLH-DSA（2024 年 8 月公開）	RFC 9814（2025 年 7 月公開）	RFC 9909（2025 年 12 月公開）
FIPS 206 FN-DSA（草案近日公開（2026 年 7 月末時点））	―	―

■表 3-3-5　FIPS と標準化動向

Pure 方式以外の PQC 移行アプローチも存在する。その一つが Composite 方式であり、これは従来の公開鍵暗号と PQC を組み合わせて用いる、いわゆるハイブリッド方式の一種である。

ハイブリッド方式は、後方互換性の確保や段階的移行等、様々な目的のために採用され得る広い概念であるが、Composite 方式はその中でも、従来の公開鍵暗号と PQC の双方の安全性仮定に基づいて処理を行うことで、いずれか一方に未知の脆弱性が存在した場合でも直ちに安全性が損なわれることを避け、セキュリティを高めることを目的としたアプローチである。これは、従来の公開鍵暗号の危殆化といったことだけでなく、PQC が新しい暗号技術であり安全性評価の成熟度が低いために、PQC の方に未知の脆弱性があった場合のリスクをも考慮に入れている。

ハイブリッド方式は一般に Pure 方式よりも複雑になりがちであるが、Composite 方式においては、変更点が主として暗号アルゴリズム部分に限定され、他のハイブリッド方式に比べプロトコル自体の変更は比較的少なく抑えられるという特徴がある。Composite 方式は、Pure 方式に比べると標準化にはやや時間を要しているものの、TLS 等一部の用途では、標準化の完了を待たずに実運用での採用が進みつつある。

以上のように、現在の PQC 標準化は、暗号アルゴリズム、及び CMS や X.509 といった汎用的な暗号プロトコルの整備が完了した段階にある。今後は、これらの技術基盤を利用している領域から先行して PQC 導入の検討が進むと考えられる。なお、Pure 方式や Composite 方式は、特定のプロトコルに強く依存しない汎用的なアプローチであり、これらの方式で対応可能な場合には、プロトコルの再設計を最小限に抑えた形で PQC への移行が可能となる。

しかしながら、公開鍵暗号を利用するすべてのプロトコルが、これらの方式で PQC へ移行できるわけではない。中には、Pure 方式や Composite 方式では要件を満たせないプロトコルも存在する。

そのようなプロトコルにおける PQC 移行では、個々のプロトコルの要件を踏まえた再設計が必要となる。例えば、後方互換性を維持するために、従来の公開鍵暗号と PQC の双方をサポートするハイブリッドプロトコルを新たに設計することが考えられる。それでも解決が困難な場合には、プロトコル設計にとどまらず、運用主体や信頼モデルの見直し等、ステークホルダーの役割変更を含むエコシステム全体の再設計が求められる可能性もある。そのため、このようなプロトコルについては今後本格的な再設計が段階的に進められていくことが予想される。

PQC への移行は、場合によってはエコシステム全体に影響を及ぼす中長期的な取り組みとなる点に留意が必要である。

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

サイバー攻撃が業種や規模を問わず広がる中、リソースが限られる多くの中小企業では、サイバーセキュリティ対策への取り組みが重要な経営課題となっている。

本節では、中小企業のサイバーセキュリティ対策強化について、政府及びIPAによる取り組みを紹介する。

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)

経済産業省が主催する産業サイバーセキュリティ研究会において、現在検討が進められている「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」(以下、SCS評価制度)について、2026年3月に公表された「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※174」(以下、制度構築方針)を基に紹介する。

(1)制度構築の背景・目的

近年、業務委託先がサイバー攻撃を受け、顧客情報が漏えいしたり、システムが停止したりすることにより、サプライチェーンを構成する企業の事業継続に大きな影響が及ぶ事案が発生している※175。このようなサプライチェーンに起因するサイバーインシデントを背景に、企業の取り引きにおいてもサイバーセキュリティ対策の担保が求められる中、委託先は異なる委託元から様々な対策水準を要求され、委託元は外部から委託先の対策状況を判断することが難しいといった課題が存在している。こうした課題に対応するため、経済産業省及びNCOは、サプライチェーンにおいて実施すべき各企業の対策を提示しつつ、その対策状況を可視化する仕組みとしてSCS評価制度の検討を進め、2026年3月に制度構築方針を公表した。

制度構築方針では、委託元、委託先双方にとって適切なセキュリティ対策の決定及び実施と、実施しているセキュリティ対策の可視化が必要であるとし、サプライチェーンにおいて想定されるリスクに対して、立ち位置に応じた対策を、SCS評価制度をとおして確認することで、企業のセキュリティ対策の決定を容易、適切なものにすることを目指すとされた。同制度の活用により、サプライチェーン全体でのセキュリティ対策の適切な実施が促進され、社会全体でのサイバーレジリエンスの強化が期待される。

(2)制度の概要

SCS評価制度では、求められるセキュリティ対策を「★3」「★4」「★5」の3段階で区分することを検討している。検討においては、先行する国内外のガイドラインや制度等※176が参考にされた※177。なお、三つの区分は中小企業が自ら情報セキュリティ対策に取り組む宣言を行うSECURITY ACTION※178という先行制度において、「★」(一つ星)及び「★★」(二つ星)の区分が存在している中、同制度はそれに続くものとしている(SECURITY ACTIONについては「3.4.3(3)SECURITY ACTION」参照)。現在、「★3」及び「★4」の制度設計が行われており、「★5」の検討は今後行われる予定である※177。

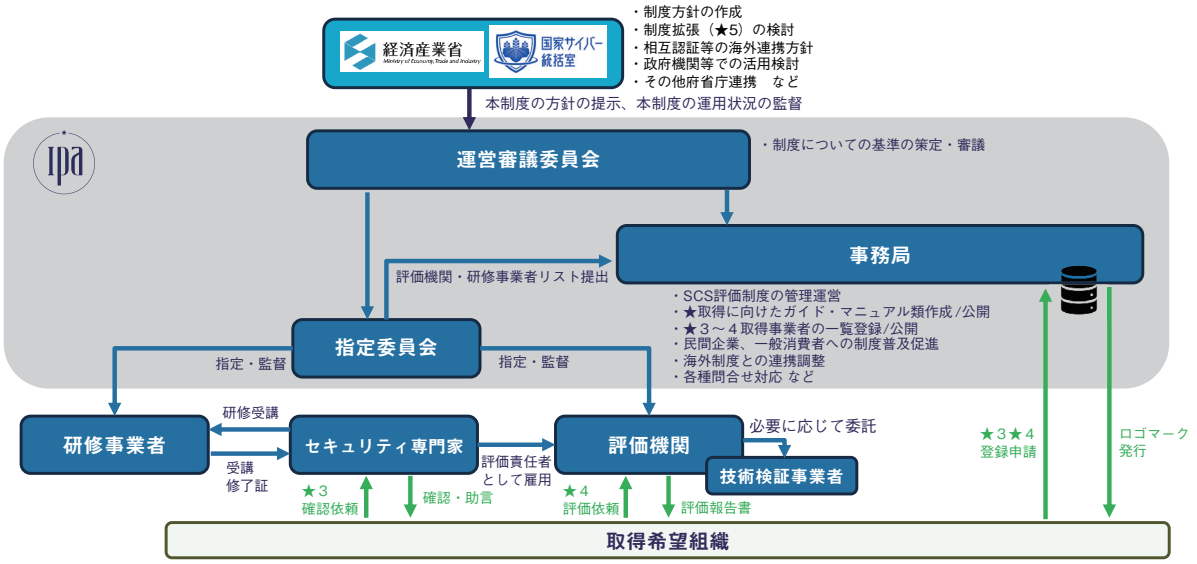
(a)制度の運用体制

SCS評価制度の運営体制を図3-4-1(次ページ)に示す。同制度は経済産業省及びNCOが制度の方針を提示し、制度の運用状況の監督を行うこととしている。経済産業省及びNCOの監督のもとIPAが制度の運営を担う。制度の管理運営等を行う事務局をIPAに置き、制度運営方針に関する事項や制度に関する文書類の策定等の審議を行う運営審議委員会と、評価機関等の指定・監督を行う指定委員会を設置する予定となっている※179。

制度構築方針に示されている要件を満たすセキュリティ専門家は、「★3」において取得希望組織の自己評価結果の確認・助言を行い、「★4」では評価機関において評価責任者を担う※179。評価機関は「★4」における第三者評価を行う。

(b)制度において設ける段階

SCS評価制度において設ける段階を表3-4-1(次ページ)に示す。それぞれの段階で目指す対策としては、「★3」がサプライチェーンを構成するすべての企業が最低限実装すべきセキュリティ対策、「★4」はサプライチェーンを構成する企業が標準的に目指すべきセキュリティ対策、「★5」はサプライチェーンを構成する企業が更に目指すべき高度な対策としている。なお、評価スキームについては、「★3」が社内等のセキュリティ専門家確認付き自己評価、「★4」及び「★5」については、評価機関による第三者評価となる。



■図 3-4-1　SCS 評価制度の運用体制
（出典）経済産業省「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※177」を基に IPA が編集

	★3	★4	★5［検討中］
想定される脅威	・広く認知された脆弱性等を悪用する一般的なサイバー攻撃	・供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 ・機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	・未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	すべてのサプライチェーン企業が最低限実装すべきセキュリティ対策（基礎的な組織的対策とシステム防御策を中心に実施）	サプライチェーン企業等が標準的に目指すべきセキュリティ対策（組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施）	サプライチェーン企業等が更に目指すべき高度な対策（国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施）
要求事項数	26 件	43 件	（今後検討）
有効期間	1 年	3 年 （毎年自己評価を実施し、結果を評価機関に提出）	（今後検討）
評価スキーム	専門家確認付き自己評価	第三者評価	第三者評価

■表 3-4-1　SCS 評価制度において設ける段階
（出典）経済産業省「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」を基に IPA が作成

(3) 制度の導入推進策

政府及び IPA では、中小企業による同制度の「★」取得に向けた支援策として、以下の取り組みを進めている。

(a) 取引先への要請等に係る考え方の整理

経済産業省及び公正取引委員会は、2022 年 10 月に公表した「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて※180」を補足することを目的に、独占禁止法や中小受託取引適正化法（取適法）との関係を整理し、「問題とならない」ケースを想定した事例※181 と、想定事例の内容を補足するための解説文書※182 を作成し、2025 年 12 月に公表した。

具体的には、発注者側（委託元）が取引先（委託先）に対し、SCS 評価制度に基づく対策の要請を行うケース等を想定し、双方が協力関係（パートナーシップ）を構築してセキュリティ対策と価格交渉を実施し、円満に合意するに至るための想定事例及び解説を掲載している。

今後、同文書について、経済団体や中小企業支援機関等の協力を得つつ、発注者側・取引先のそれぞれの企業に対して、普及展開を進めていく予定である。

(b) 中小企業向け支援策

経済産業省及び IPA は、中小企業による SCS 評価

制度の「★3」及び「★4」取得を促進する新たな支援策として「サイバーセキュリティお助け隊サービス（新類型）[※183]」の創設を予定しており、2026年9月から、制度設計に向けた実証事業を開始した（サイバーセキュリティお助け隊サービスについては「3.4.3（2）サイバーセキュリティお助け隊サービス制度」参照）。実証事業では、IPAが認定したサービス提供事業者が、実証に参加するSCS評価制度の「★3」または「★4」取得のためのサービスを試行的に提供する。提供したサービスの活用状況や結果等を検証し、中小企業にとって導入しやすいサービスとするための品質要件や価格要件等について検討を進めていく。

(c)「中小企業の情報セキュリティ対策ガイドライン」の改訂

IPAは2026年3月、中小企業向けに情報セキュリティ対策の考え方や、段階的に実現していくための方策を示した「中小企業の情報セキュリティ対策ガイドライン」を第4.0版に改訂した。今回の改訂では、STEP3（本格的に取り組む）等において、SCS評価制度の基本的な考え方を踏まえた内容とすることで、同ガイドラインとSCS評価制度の連携を図っている（同ガイドラインについては「3.4.2(2)『中小企業の情報セキュリティ対策ガイドライン』の改訂」参照）。

(d)登録セキスペの活用促進

IPAでは、情報処理安全確保支援士（以下、登録セキスペ）のうち、中小企業向けのセキュリティ対策支援が可能な専門家を「中小企業向けサイバーセキュリティ対策支援者リスト」として公開している[※184-1]（同リストについては「3.4.3(1)情報処理安全確保支援士（登録セキスペ）による中小企業支援」参照）。

(4)今後のスケジュール

2025年度の制度構築方針の公表を踏まえ、2026年度は制度運営基盤の整備や利用促進等を進め、「★3」及び「★4」については、2026年度末ごろの運用開始を予定している（図3-4-2）。

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

IPAでは、中小企業のサイバーセキュリティ対策の強化に向けた支援施策として、「中小企業の情報セキュリティ対策ガイドライン」の普及を推進している。2026年3月、社会状況の変化やサイバー攻撃の動向を踏まえ、同ガイドラインを改訂した。

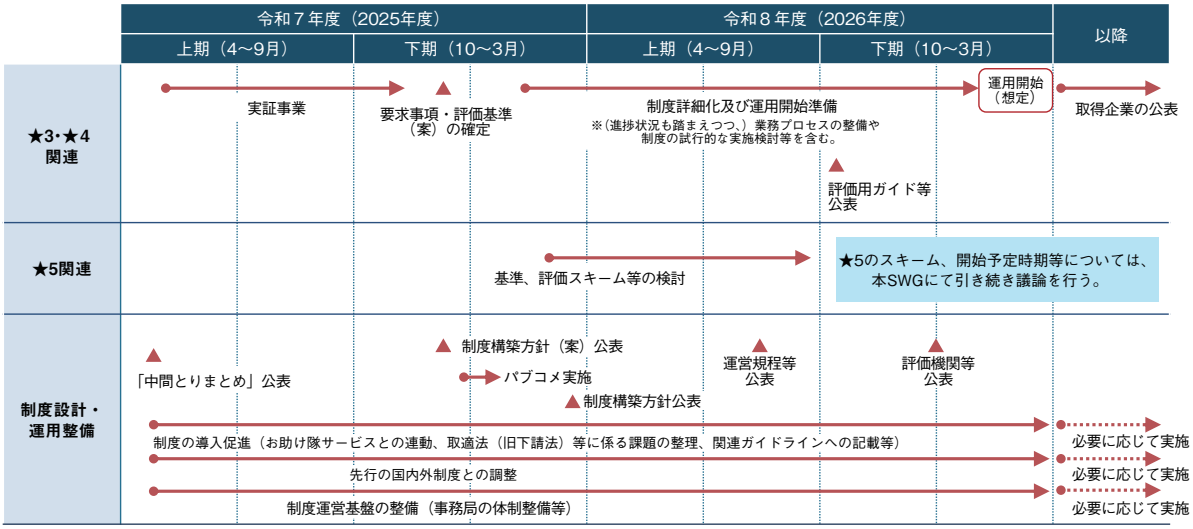
本項では、同ガイドラインを改訂することとなった背景と改訂の概要について述べる。

(1)サイバーセキュリティ対策を取り巻く環境の変化と課題

中小企業のサイバーセキュリティ対策を取り巻く環境の変化と課題等について述べる。

(a)企業の事業活動の停止にまで影響が拡大

IPAの「情報セキュリティ10大脅威2026[※129]」の「『組織』向け脅威」（以下、10大脅威）では、「ランサム攻撃による被害」が2021年以降6年連続で1位にランキン



■図3-4-2　今後のスケジュール
（出典）経済産業省「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」

グされており、長期にわたり深刻な脅威となっている。

警察庁の「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について※21」によると、ランサムウェアの被害報告件数は 226 件と依然として高水準で推移し、そのうち 6 割超を占める 143 件は中小企業であった。また、復旧等に要した期間について回答が得られた 107 件のうち、1 ヵ月以上を要したのは 2 割（22 件）であった。都内の中堅乳製品メーカーでは、2025 年 1 月、ランサムウェアに感染し、全面復旧までに 4 ヵ月、事後の対策費も含め、費用は数千万円に上ったと報道された※184-2。

これらの結果から、多くの中小企業において事業継続を意識した対策が必要であると考えられる。

(b) サプライチェーン全体での対策推進の必要性の高まり

10 大脅威によると、「サプライチェーンや委託先を狙った攻撃」が 2023 年以降 4 年連続で 2 位にランキングされており、業務委託先がサイバー攻撃を受けたことにより、事業継続に大きな影響が及ぶ事案が継続的に発生している。

近年サプライチェーンを通じたセキュリティインシデントが頻発していること、及び複雑なサプライチェーン下で様々な委託元から様々な要求事項を求められることが、特に中小企業において過度な負担につながっている。こうした状況を受けて、経済産業省は 2024 年 7 月に「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サブワーキンググループ※185」を設置し、サプライチェーンを構成する企業等の IT 基盤（クラウド環境で運用するものも含む）を対象として、サプライチェーン全体でのセキュリティ対策水準の向上を目的とした SCS 評価制度の検討を開始した（「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）」参照）。2026 年 3 月に公表された同制度構築方針※177 において、サプライチェーンを構成する中小企業はセキュリティ対策におけるリソースが限られており、基準に基づく統一的な対策は委託元、委託先双方にとってメリットがあることから、中小企業が SCS 評価制度を活用することによる効果が大きいとしている。

今後、より多くの中小企業が SCS 評価制度を認知し、セキュリティ対策に取り組むことで、サプライチェーン全体としてのセキュリティ対策が強化されることが望まれる。

(c) セキュリティ人材の不足が顕在化

サイバー攻撃が高度化・複雑化する中、産業界全体のサイバーセキュリティ対策の実効性を高めるとともに、我が国におけるセキュリティ市場の持続的な発展に向けたエコシステムの構築を目的として、経済産業省は、2024 年 7 月に産業サイバーセキュリティ研究会のワーキンググループ 2 に「サイバーセキュリティ人材の育成促進に向けた検討会※186」を設置した。同検討会における検討の結果、特に中堅・中小企業においてセキュリティ対策を担う人材の不足が顕在化していることが課題として整理された。2025 年 5 月に、企業が自社で人材を育成しつつ、外部の専門人材も活用するための方法をコンパクトに提示した「中堅・中小企業が実施するセキュリティ対策に応じた人材確保・育成の実践的方策ガイドβ版（案）」が公開された。

(2)「中小企業の情報セキュリティ対策ガイドライン」の改訂

IPA が 2009 年度に初版を発行した「中小企業の情報セキュリティ対策ガイドライン」（以下、中小ガイドライン）は、業種を問わず中小企業及び小規模事業者（法人、個人事業主、各種団体を含む）を対象に、経営者や実務担当者が情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したものである。

情報セキュリティに組織的に取り組んだ経験がなくても、段階的（STEP1：できるところから始める、STEP2：組織的な取り組みを開始する、STEP3：本格的に取り組む、STEP4：より強固にするための方策）に取り組みを進めることで、自社の実情に応じた情報セキュリティ対策を継続的に強化していくことができる。

IPA は、「3.4.2 (1) サイバーセキュリティ対策を取り巻く環境の変化と課題」で述べた環境変化を反映して、2026 年 3 月に第 4.0 版を公開した（次ページ図 3-4-3）。第 4.0 版では、基本的な 4 STEP 構成を維持しつつ、個々の企業のみならず、サプライチェーン全体に被害を及ぼすサイバー攻撃の脅威を踏まえ、中小企業が実践的な対策を進められるよう、記載内容の見直しを行った。

本項では、中小ガイドラインの見直しのポイントについて述べる。

(a) サイバー攻撃の実態等を踏まえた見直し

近年、中小企業ではランサム攻撃の被害に遭った場合の事業継続が課題となっている。パソコンやサーバーの中に保存したデータが暗号化され使えなくなることがあるため、対策としてはバックアップの取得が事業継続にとって重要である。



■図 3-4-3　中小企業の情報セキュリティ対策ガイドライン第 4.0 版
（出典）IPA「中小企業の情報セキュリティ対策ガイドライン」

ランサム攻撃の被害拡大を踏まえ、中小ガイドラインの「情報セキュリティ 5 か条」について、バックアップの取得に関する項目を新たに追加し、「情報セキュリティ 6 か条」として整理した。企業の規模に関わらず、必ず実行すべき重要な基本的な対策をまとめている（表 3-4-2）。

中小ガイドラインでは自社のセキュリティ対策の実施状況の把握を目的として、「5 分でできる!情報セキュリティ自社診断※187」（以下、5 分診断）を提供している。

IPA の「2024 年度 中小企業における情報セキュリティ対策に関する実態調査※188」（以下、2024 年度実態調査）の結果を踏まえ、5 分診断の診断項目について、次のとおり見直しを実施している。

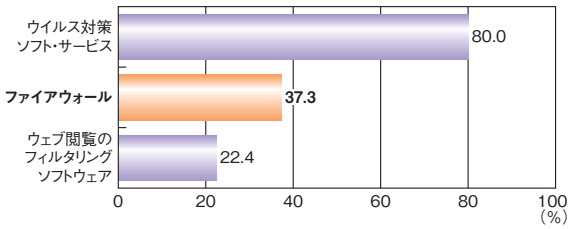
サイバーセキュリティ対策を実施（強化）している企業では、導入している製品として「ウイルス対策ソフト・サービス」が 80.0% と最も多く、次いで「ファイアウォール」が 37.3% であった（図 3-4-4）。警察庁が報告するランサムウェアの侵入経路からも分かるように、VPN 機器、リモートデスクトップ等のインターネット接続機器からのランサムウェアの侵入が極めて多い※21。そこで、診断項目として「内部ネットワークを守るため、不正アクセス対策機能を設定していますか?」を追加している。

また、情報セキュリティ対策サービス以外で利用・導入されているサービスやシステムとしては、「電子メール（フリーメール・汎用ドメイン等）」が 46.3% と最も多く、次いで「電子メール（独自ドメイン）」が 36.3%、「Web サイト、ホームページの開設」が 33.0% であった（次ページ図 3-4-5）。Web サイト等の利用・導入率が一定数あり、公開情報の内容や設定状況、運用状況を把握することが、情報漏えい防止等の観点から重要である。そこで、診断項目として「ウェブサイトで公開すべきでない情報を公開していませんか?」を追加している。

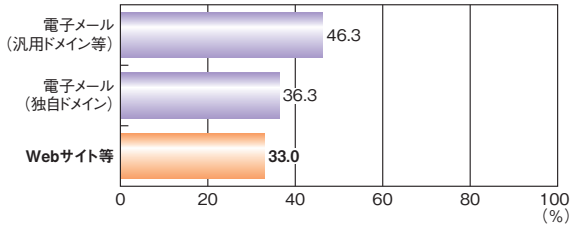
更に、中小企業の担当者が理解しやすいよう、診断内容が類似する項目について内容の主旨は維持しつつ整理を実施した。具体的には、「事務所の立ち入り制限」といった物理的対策や、「情報セキュリティ教育」といっ

No. 1　OS やソフトウェアは常に最新の状態にしよう!
OS やソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、それを悪用したウイルスに感染してしまう危険性があります。お使いの OS やソフトウェアには、修正プログラムを適用する、または最新版を利用するようにしましょう。
No. 2　ウイルス対策ソフトを導入しよう!
ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル※（パターンファイル）は常に最新の状態になるようにしましょう。 ※コンピュータウイルスを検出するためのデータベースファイル
No. 3　パスワードを強化しよう!
パスワードが推測や解析されたり、ウェブサービスから流出した ID・パスワードが悪用されたりすることで、不正にログインされる被害が増えています。パスワードは「長く」、「複雑に」、「使い回さない」ようにして強化しましょう。
No. 4　共有設定を見直そう
データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えています。無関係な人が、ウェブサービスや機器を使うことができるような設定になっていないことを確認しましょう。
No. 5　バックアップを取ろう!
故障や誤操作、ウイルス感染などにより、パソコンやサーバーの中に保存したデータが消えたり、暗号化されたりしてしまうことがあります。事業が継続できるようバックアップを取得しておきましょう。
No. 6　脅威や攻撃の手口を知ろう!
取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げたりして ID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策を取りましょう。

■表 3-4-2　情報セキュリティ 6 か条
（出典）IPA「中小企業の情報セキュリティガイドライン」



■図 3-4-4　情報セキュリティ関連製品やソフトウェアの導入状況
（n=2,203）（上位 3 項目を抜粋）
（出典）IPA「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」を基に IPA が編集



■図 3-4-5　情報セキュリティ対策サービス以外で利用・導入されているサービスやシステム（n=4,191）（上位 3 項目を抜粋）
（出典）IPA「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」を基に IPA が編集

た従業員のセキュリティ意識に関する項目について、それぞれの関連する項目を統合している。

2024 年度実態調査において、5 分診断の 25 項目についての実施率を調査した結果、最も実施率が低かった「新たな脅威や攻撃の手口を知り対策を社内共有する仕組み」については、取り組みを実施する際に参考となる参照先を対策例に追加することで実施率の向上を図っている。

(b) SCS 評価制度の考え方の取り込み

個々の企業のみならず、サプライチェーン全体に被害を及ぼすサイバー攻撃の脅威を踏まえ、中小ガイドラインの STEP3 において、SCS 評価制度で求められる要求事項（組織のガバナンスや取引先管理、自社の IT 基盤における検知・防御体制等）を基に、セキュリティ対策を実施する際の基本的な考え方を示している。また、付録の情報セキュリティ関連規程や資産管理台帳のサンプルについても、SCS 評価制度との整合性を考慮し、内容の拡充を図っている。

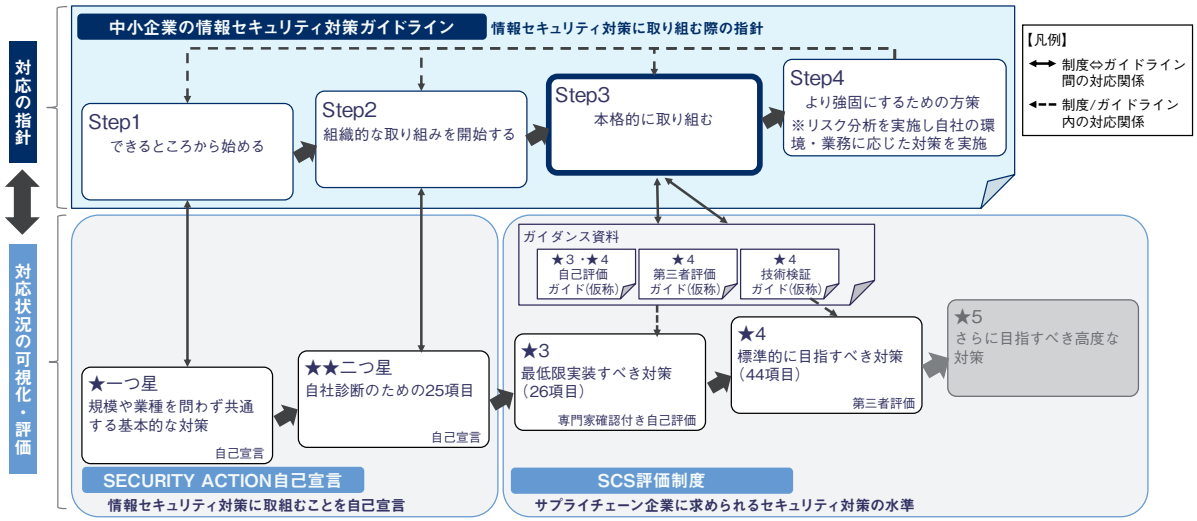
経済産業省のニュースリリース※50 において、SCS 評価制度は、対策の実践を自己宣言し、それを可視化する SECURITY ACTION 制度と連続性を有する基準として位置付けられている（図 3-4-6）。

中小ガイドラインを活用して、事業やシステム構成に応じたセキュリティ対策を段階的に進め、SECURITY ACTION 制度や SCS 評価制度により実施状況を可視化することで、取引先や顧客からの信頼向上を獲得する効果が期待される。

(c)「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」公開

中小企業が、「3.4.2 (1) (c) セキュリティ人材の不足が顕在化」で述べた「中堅・中小企業が実施するセキュリティ対策に応じた人材確保・育成の実践的方策ガイド（β版）」を実践していくためには、単に必要な事項を提示するだけでなく、使いやすさや読みやすさ、及び具体的な事例を併せて示すことが重要である。IPA は、中小企業 15 社へのヒアリング等を通じて、使いやすさや読みやすさを向上させるとともに、実際に取り組む際の参考となる事例を収集した。これを「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」として、中小ガイドラインの付録に位置付けて公開している（次ページ図 3-4-7）。

経済産業省と IPA は、中小ガイドラインを主要な中小企業支援施策に位置付け、中小企業のサイバーセキュリティ対策を推進している。中小企業が、中小ガイドラインを活用して着実にサイバーセキュリティ対策を進めるこ



■図 3-4-6　中小ガイドラインと SCS 評価制度の関係
（出典）経済産業省「サイバー攻撃を“自分事”に。そしてその先、“どう動く?”――中小企業のセキュリティ対策強化に向けて『中小企業のための実例で学ぶサイバーセキュリティリスク事例集』と『中小企業の情報セキュリティ対策ガイドライン第 4.0 版』を公表しました※50」



■図 3-4-7　付録 1「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」
（出典）IPA「中小企業の情報セキュリティ対策ガイドライン」

とで、中小企業自身の信頼性向上に寄与するとともに、経済社会全体のサイバーリスク低減につながることが望まれる。

3.4.3 中小企業向け支援策

IPA に関連した中小企業向けのサイバーセキュリティ支援策について紹介する。

(1) 情報処理安全確保支援士（登録セキスペ）による中小企業支援

IPA では、サイバーセキュリティ対策を推進する人材の国家資格である情報処理安全確保支援士（登録セキスペ）の登録者のうち、中小企業向けのサイバーセキュリティ対策支援が実施できる専門家の得意分野・専門領域を可視化した「中小企業向けサイバーセキュリティ対策支援者リスト」（以下、支援者リスト）を公開している※184-1。

「中小企業のセキュリティ対策の実施に際してはどこから始めればよいか分からない」という声があるため、IPA では業種を問わない基本的なセキュリティ対策として、「中小企業のセキュリティ対策ガイドライン」（付録を含む）を活用した五つの指導テーマを設定し、各指導テーマについて指導ツール（実施要領及びワークシート等）を整備している※189（表 3-4-3）。

支援者リストに掲載された専門家（以下、掲載専門家）は、各指導テーマに基づく支援が可能であり、商工会議所等の支援機関や中小企業は自社に必要な指導テーマに応じて相談を受けたい掲載専門家をリストから選択し、直接連絡することができる。なお、今後、指導テーマに中小企業が SCS 評価制度の「★ 3」を取得する際の適合可否の確認、及び助言を行う「セキュリティアセスメント」が追加される予定である※190。

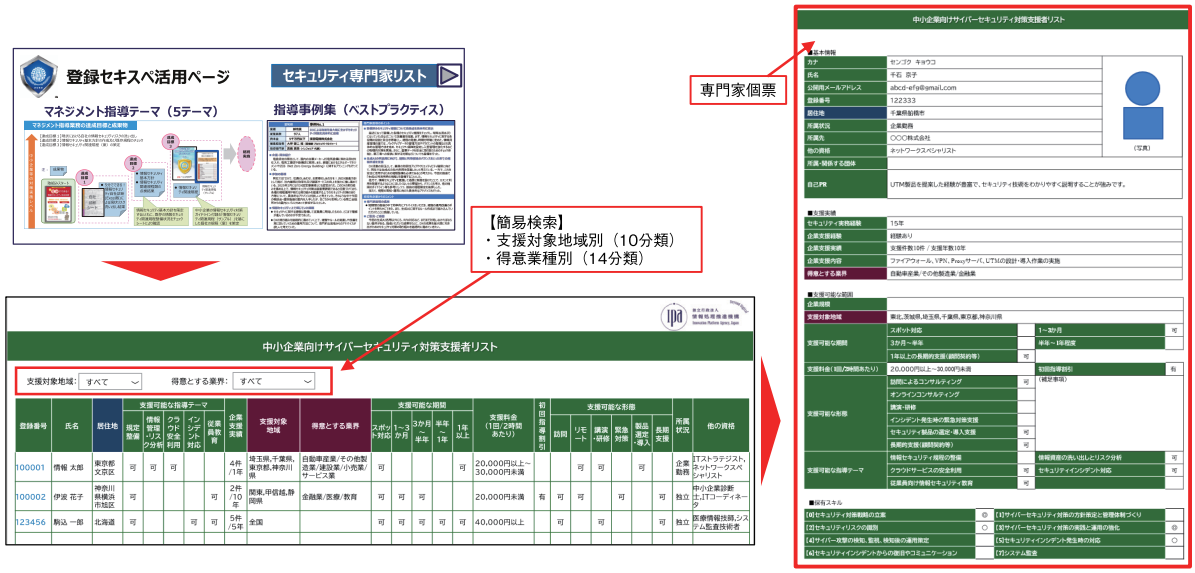
指導テーマ	対象企業及び効果
テーマ① 情報セキュリティ規程の整備	従業員が IT ツールを使って業務を行っているが、情報セキュリティ規程が未整備なため、責任範囲が明確になっていない中小企業に必要。規程整備により、社内セキュリティ体制の継続的・自律的な改善が図れるようになる。
テーマ② 情報資産の洗い出しとリスク分析	製造業やサービス業等、技術情報や顧客情報を大量に扱うが、どの情報が重要か、リスクがどこにあるかが把握できていない中小企業に必要。情報資産の洗い出しとリスク分析を行うことで、リスク低減策の検討にもなる。
テーマ③ クラウドサービスの安全利用	業務効率化のためにクラウドサービスを導入しているが、セキュリティリスクに対する理解や対策が不十分な中小企業に必要。「クラウドサービス安全利用の手引き」を策定することで、クラウドサービス利用のリスクを明確化できる。
テーマ④ セキュリティインシデント対応	サプライチェーンの参加企業として他社との連携が多く、セキュリティインシデントが発生した際の被害拡大のリスクがある中小企業に必要。手順整備に加え、従業員訓練も実施することで、インシデント発生時の対応体制が構築できる。
テーマ⑤ 従業員向け情報セキュリティ教育	IT リテラシーの差が大きい企業や、日常的なセキュリティ対策が徹底できていない企業に必要。セキュリティ教育プログラムを策定するとともに、実際に従業員へのセキュリティ教育を実施することで、社内の意識向上にもつなげられる。

■表 3-4-3　セキュリティマネジメント指導テーマ

支援者リストは、掲載専門家の「支援対象地域」及び「得意とする業界」で絞り込むことが可能である。また、支援者リストの「登録番号」をクリックすると専門家個票が表示され、各掲載専門家の詳細情報が閲覧できる。支援者リストには、掲載専門家が支援可能な指導テーマ、支援実績、得意とする業界、支援可能形態、支援料金、保有資格、保有スキル等が記載されており、利用者が相談を受けたい掲載専門家へ直接連絡を取り、相談や業務依頼を行うことができる（次ページ図 3-4-8）。

(2) サイバーセキュリティお助け隊サービス制度

IPA は、中小企業等を狙ったサイバー攻撃への対処として不可欠なサービス（「見守り」「駆付け」「保険」）を



■図 3-4-8　中小企業向けサイバーセキュリティ対策支援者リスト掲載イメージ

ワンパッケージにまとめ、効果的かつ安価に提供することをコンセプトとした「サイバーセキュリティお助け隊サービス制度※191」を2021年度から運営している（図3-4-9）。



■図 3-4-9「サイバーセキュリティお助け隊サービス※192」パンフレット

同制度が提供するサービスの要件（上限価格、相談窓口の設置、異常の監視、緊急時の対応支援、簡易サイバー保険等）は、「サイバーセキュリティお助け隊サービス基準※193」として定められており、これらの基準要件を満たしていることが確認されたセキュリティサービスが「サイバーセキュリティお助け隊サービス」として登録され、IPAのWebサイトで公開されている※194。同サービスは民間のセキュリティ事業者より提供され、2026年4月1日時点で47事業者、90サービスが登録されており、同年3月末時点で約10,900社の企業に導入されている。

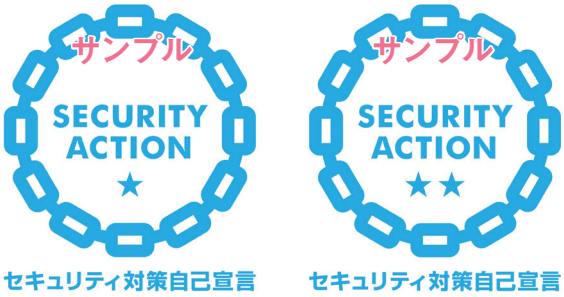
同サービスは、ITの担当者がおらずセキュリティ対策として何から始めていいのか分からない、コストがかけられないといった、人材やコスト面において十分な余裕があるとはいえない中小企業が、サイバーセキュリティに関する各種サービスを一括で安価に導入できるといった点に大きなメリットがある。また、同サービスの導入に際しては、「デジタル化・AI導入補助金2026※195（セキュリティ対策推進枠）」を活用することが可能である。そのようなコスト面の支援を活用できることからも、中小企業にとって導入しやすいサービスとなっている。

(3) SECURITY ACTION

IPAが運営する「SECURITY ACTION※196」は、IPAと中小企業関係団体が2017年2月に「中小企業における情報セキュリティの普及促進に関する共同宣言※197」を行い、「“自発的な情報セキュリティ対策を促す”ための核となる取り組み」として創設された。同制度は、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度であり、情報セキュリティ対策への取り組み状況を可視化し、段階的に対策を強化していくことを目指している。

同制度では「中小企業の情報セキュリティ対策ガイドライン」に基づき2段階の取り組み目標を用意しており、取り組み目標に応じた宣言を行うと、「★」（一つ星）と「★★」（二つ星）のロゴマークを利用できるようになる（次ページ図3-4-10）。

一つ星の取り組み目標は、情報セキュリティの基本的な対策の実施で、具体的には「情報セキュリティ6か条※198」に取り組むことが求められる。二つ星は、組織



■図 3-4-10 「SECURITY ACTION」ロゴマーク（サンプル）

的な取り組みの開始として、「5 分でできる!情報セキュリティ自社診断」を行い、自社の状況を把握した上で「情報セキュリティ基本方針」を定め、外部に公開することが求められる。「情報セキュリティ基本方針」とは経営者が定める従業員の指針であり、関係者に対して取り組みを表明するものである。

宣言を行うことで、「デジタル化・AI 導入補助金 2026」（旧、IT 導入補助金）を始め、自治体等が提供するデジタル化・IT 化支援の補助金の申請要件、審査における加点要素として活用されるケースも増えている。これにより、中小企業は情報セキュリティ対策を強化しつつ、資金面の支援を受けやすくなるというメリットが生まれている。実際、宣言のきっかけは補助金申請が大半となっているものの、宣言することで継続的な情報セキュリティ対策の意欲が後押され、対策強化の動機付けとしても機能している※199。

また、SECURITY ACTION 宣言事業者の取り組み事例では、宣言した対策を推進していくことで、従業員の情報セキュリティに対する意識の向上だけでなく、取引先や顧客といった対外的な信頼の向上にもつながる事例が見られている※200。

同制度が開始された 2017 年 4 月以降、1 年あたり約 5 万件から約 9 万件の申し込みがあり、2026 年 6 月時点で累計約 47 万件の宣言が行われている。建設業、卸売業・小売業、医療・福祉を始め、サービス業、製造業、情報通信業等、幅広い事業者に及んでおり、情報セキュリティ対策の第一歩として同制度が活用されている。

今後の展望としては、地域における情報セキュリティ意識の更なる向上を図るため、自治体・関係機関・団体等との連携を一層強化し、セミナー等を通じた SECURITY ACTION の普及活動を継続して推進していく方針である。SECURITY ACTION 自己宣言の認知度向上、普及拡大をとおして、中小企業が安心してデジタル化や AI 活用を進められる環境作りを目指していく。

COLUMN

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

委託先や子会社、更にその再委託先等いわゆるサプライチェーンに起因して、業務を停止せざるを得ないようなセキュリティインシデントが多発しています。本コラムでは、サプライチェーン全体の安全性を担保するために押さえるべき五つのポイントについて説明します。特に再委託があるサプライチェーンでは、委託先の選定・契約・運用・監査・契約終了時の各段階で「見えない先」まで含めて統制する仕組みを作ることがポイントです。

まずは、「①適切な委託先の選定（事前審査）」から始めます。業務を委託する前に、委託先の候補が、自社が求めるセキュリティ基準を満たしているか評価を行います。評価基準としては、経済産業省が制度の立ち上げを検討している「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）」を参考にするのもよいでしょう。ISMS（情報セキュリティマネジメントシステム）等の認証取得の有無も目安になりますが、必ずしもセキュリティ対策の強度を保証するものではないことに注意しましょう。委託先の候補が、過去にセキュリティインシデントを起こしたことがあるかについても要確認です。

委託先が決まったら「②契約書の締結（責任分界の明確化）」を行います。契約書では、どの情報・システム・作業に対して、誰が何を守るのかを明文化します。再委託がある場合でも、委託元が求めるセキュリティ水準が末端まで届くよう、委託先に管理責任を負わせる設計が必要です。また、再委託先の名称、所在地、担当業務、利用システム・クラウド、保管データの種類を把握し、再委託は原則事前承認制にするのが望ましいでしょう。再委託先で発生したインシデントでも、隠さずに委託元へ速やかに連絡が上がる仕組みが不可欠です。委託元に責任を負わせることは重要ですが、適切な対応に対しては責任の減免も考慮すべきです。更に、委託元が定期的にセキュリティ状況を監査する権利や、インシデント時の報告フロー及び責任分界点を明確化しておきましょう。

運用時には、「③アクセス権限の最小化と厳格なデータ管理」が必須です。委託先や再委託先には必要最小限の権限だけを付与し、共有アカウントや過剰権限の付与を避けます。特権 ID の発行条件、期限、棚卸し、退職・契約終了時の即時削除を徹底します。また、個人情報、機密情報、設計情報、認証情報等は、持ち出し可否、保存場所、暗号化、削除方法等を明確にします。不要なデータを渡さない「データ最小化」を原則としましょう。

「④定期的な評価（モニタリング）」も忘れてはいけません。契約して終わり、運用を開始したら終わりではなく、定期的にセキュリティ対策の実施状況を確認します。チェックリストによる定期的な現状把握だけでなく、重要度が高い委託先に対しては、現地やリモートでの安全管理状況の確認（監査）を行いましょう。インシデントにつながるようなヒヤリハットに対しても、原因究明や再発防止を求めることが大切です。

最後に「⑤契約終了時の対応」も抜かりなく実施します。契約終了時には、データ返却・消去、アカウント停止、媒体回収、ログ保全を確実に実施しましょう。再委託先まで含めた実施の証跡を残すことが重要です。

※ 1　https://www.cyber.go.jp/pdf/policy/kihon-s/cs_strategy2025.pdf〔2026/7/14 確認〕
※ 2　https://www.cyber.go.jp/pdf/policy/kihon-s/250529kikkin.pdf〔2026/7/14 確認〕
「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」については「情報セキュリティ白書 2025」（https://www.ipa.go.jp/publish/wp-security/j5u9nn0000004wk0-att/ISWP2025_ALL.pdf〔2026/7/14 確認〕）の「3.1.1（1）サイバー安全保障に関する取り組み（能動的サイバー防御の実現に向けた検討等）」（p.110）を参照。
※ 3　https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf〔2026/7/14 確認〕
※ 4　「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（令和 7 年法律第 42 号）」（「サイバー対処能力強化法」と呼ぶ）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（令和 7 年法律第 43 号）」をあわせて本白書では「サイバー対処能力強化法等」と呼ぶ。
※ 5　https://laws.e-gov.go.jp/law/426AC1000000104〔2026/7/14 確認〕
※ 6　https://www.cyber.go.jp/pdf/policy/kihon-s/cs2025.pdf〔2026/7/14 確認〕
※ 7　年次計画 2025 では、サイバー対処能力強化法等の施行に向けた施策も「特に強力に取り組むべき施策」として位置付けられている。
※ 8　NCO：サイバーセキュリティ 2025 のポイント（「エグゼクティブ・サマリー」）　https://www.cyber.go.jp/pdf/policy/kihon-s/cs2025_abstract.pdf〔2026/7/14 確認〕
※ 9　サイバー攻撃による重大な危害を防止するための措置。警察庁長官が指名する警察官（サイバー危害防止措置執行官）は、サイバー攻撃又はその疑いがある通信等を認めた場合、そのまま放置すれば、人の生命、身体又は財産に対する重大な危害が発生するおそれがあるため緊急の必要があるときは、そのサイバー攻撃の送信元等である電子計算機の管理者その他関係者に対し、危害防止のため通常必要と認められる措置をとることができる（「警察官職務執行法（警職法）第6条の2」から抜粋）。
e-Gov 法令検索：警察官職務執行法　https://laws.e-gov.go.jp/law/323AC0000000136/20261001_507AC0000000043?occasion_date=20261001〔2026/7/14 確認〕
※ 10 https://www.cyber.go.jp/pdf/council/cs/n01/01document3-3.pdf〔2026/7/14 確認〕
※ 11 https://www.cyber.go.jp/pdf/policy/infra/cip_policy_2025.pdf〔2026/7/14 確認〕
※ 12 https://www.cyber.go.jp/pdf/policy/infra/pubcom_res_jyuhurakijun.pdf〔2026/8/24 確認〕
※ 13 重要インフラ統一基準において、「リスクベース」とは、「重要インフラサービスの継続的提供を不確かなものとする自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化といったリスクであって、分野の特性・実情等を踏まえて特定、評価したものをベースとする考え方」と定義されている。
※ 14 セプター（CEPTOAR）：重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。Capability for Engineering of Protection, Technical Operation, Analysis and Response の略称。
※ 15 NICT、IPA、JPCERT/CC 及び JC3 を指す。
※ 16 重要インフラサービス提供に必要な情報システムに関係するサプライチェーン等に関わる、機器納入、システムの設計・構築・運用・保守等を行うシステムベンダー、ウイルス対策ソフトウェア等のセキュリティ対策を提供するセキュリティベンダー等、ハードウェア・ソフトウェア等の基盤となるプラットフォームを提供するプラットフォームベンダー及びクラウドサービス等の外部サービスを提供する事業者。
※ 17 https://www.cyber.go.jp/pdf/policy/infra/pubcom_res_jyuhurakijungaiyou.pdf〔2026/8/24 確認〕
※ 18 サイバー対処能力強化法に基づくインシデント報告については「2.1.1（3）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」を参照されたい。
※ 19 https://www.npa.go.jp/news/release/2026/20260402001_3.pdf〔2026/7/14 確認〕
※ 20 https://www.npa.go.jp/bureau/cyber/pdf/20260402.pdf〔2026/7/14 確認〕
※ 21 警察庁：令和7年におけるサイバー空間をめぐる脅威の情勢等について　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf〔2026/7/14 確認〕
※ 22 重要犯罪密接関連情報：インターネット上に流通することによって、個人の生命・身体に危害を加えるおそれが高い重要犯罪又は重要犯罪に発展する危険性がある犯罪と密接に関連している次の情報。①拳銃等の譲渡等、②爆発物の製造、③殺人等（殺人、強盗、不同意性交等、放火、誘拐、傷害、逮捕・監禁、脅迫）、④臓器売買、⑤人身売買、⑥硫化水素ガスの製造、⑦ストーカー行為等。
※ 23 内閣府：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）　https://www8.cao.go.jp/cstp/ai/ai_act/ai_act.html〔2026/7/14 確認〕
※ 24 https://www.digital.go.jp/policies/priority-policy-program〔2026/8/21 確認〕
※ 25 データセキュリティという言葉は多義に用いられるが、ここで対象とするデータセキュリティは、民間企業等によるデータ利活用において、法益侵害リスクに対処するための一連の営みを念頭としたものである。
※ 26 デジタル庁：公的個人認証サービス（JPKI）　https://www.digital.go.jp/policies/mynumber/private-business/jpki-introduction〔2026/7/14 確認〕
※ 27 「データセキュリティワーキンググループとりまとめ」における「法益」は、不正競争防止法、著作権法、特許法、知的財産基本法、個人情報保護法等の諸法令に加え、業界規定等によって保護されるべき、企業、個人及び社会の経済的・社会的利益を指す。
※ 28 https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/03d22136-3125-4839-aeb9-655ff7134df6/a1d09975/20260311_meeting_data-security-wg_compilation.pdf〔2026/7/14 確認〕
※ 29 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/1f2fb150-febe-4bee-b691-f02f68c4e8d4/e550d3de/20260413_policies_mynumber_private-business_outline_01.pdf〔2026/7/14 確認〕
※ 30 https://www.soumu.go.jp/main_content/001064122.pdf〔2026/7/14 確認〕
※ 31 https://www.nict.go.jp/pdf/6th-mid-term-goal20260227.pdf〔2026/7/14 確認〕
※ 32 https://www.soumu.go.jp/main_sosiki/kenkyu/komyoka_fukuzatsukasuru/index.html〔2026/7/14 確認〕
※ 33 https://www.soumu.go.jp/main_content/001068239.pdf〔2026/7/14 確認〕
※ 34 https://www.soumu.go.jp/main_content/001069311.pdf〔2026/7/14 確認〕
※ 35 NICT：国立研究開発法人情報通信研究機構が達成すべき業務運営に関する目標を達成するための計画（第6期）　https://www.nict.go.jp/pdf/6th-mid-term-plan.pdf〔2026/7/14 確認〕
※ 36 https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security_r03/index.html〔2026/8/24 確認〕
※ 37 総務省：ガイドライン改定（令和 8 年 3 月）のポイントについて　https://www.soumu.go.jp/main_content/001064409.pdf〔2026/7/14 確認〕
※ 38 総務省：地方自治法の一部を改正する法律の概要　https://www.soumu.go.jp/main_content/000955133.pdf〔2026/7/14 確認〕
※ 39 総務省：地方公共団体におけるサイバーセキュリティを確保するための方針の策定又は変更に関する指針の策定について（通知）　https://www.soumu.go.jp/main_content/001081615.pdf〔2026/8/24 確認〕
※ 40 経済産業省：産業サイバーセキュリティ研究会　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/index.html〔2026/7/9 確認〕
※ 41 経済産業省：第 10 回 産業サイバーセキュリティ研究会　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/010.html〔2026/7/9 確認〕
※ 42 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〔2026/7/9 確認〕
※ 43 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/pdf/012_03_00.pdf〔2026/7/9 確認〕
※ 44 https://www.meti.go.jp/files/900017650.pdf〔2026/7/9 確認〕
※ 45 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/016_t01_00.pdf〔2026/7/9 確認〕
※ 46 https://www.meti.go.jp/policy/netsecurity/wg1/semiconductor_systems_guideline_ver1.0.pdf〔2026/7/9 確認〕
※ 47 ISO：ISO/IEC CD TS 5689　https://www.iso.org/standard/87375.html〔2026/7/9 確認〕
※ 48 NIST：The NIST Cybersecurity Framework (CSF) 2.0　https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf〔2026/7/9 確認〕
※ 49 経済産業省：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　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/20260327_report.html〔2026/7/9 確認〕
※ 50 経済産業省:サイバー攻撃を"自分事"に。そしてその先、"どう動く?"――中小企業のセキュリティ対策強化に向けて「中小企業のための実例で学ぶサイバーセキュリティリスク事例集」と「中小企業の情報セキュリティ対策ガイドライン第 4.0 版」を公表しました　https://www.meti.go.jp/press/2025/03/20260327002/20260327002.html〔2026/7/9 確認〕

※ 51 経済産業省：地域 SECUNITY（セキュリティ・コミュニティ）https://www.meti.go.jp/policy/netsecurity/secunity.html〔2026/7/9 確認〕
※ 52 https://sc3.jp/〔2026/7/9 確認〕
※ 53 https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html〔2026/7/9 確認〕
※ 54 https://www.ipa.go.jp/security/guide/sme/about.html〔2026/7/9 確認〕
※ 55 経済産業省：Cybersecurity Information Security Measures Guidelines for Small and Medium sized Enterprises https://www.meti.go.jp/english/policy/safety_security/cybersecurity/index.html#02〔2026/7/9 確認〕
※ 56 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（JCSTAR）の運用を開始しました https://www.meti.go.jp/press/2024/03/20250325007/20250325007.html〔2026/7/9 確認〕
※ 57 総務省：「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」等の意見募集の結果及び改定版の公表 https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000355.html〔2026/7/9 確認〕
※ 58 NCO：政府機関等の対策基準策定のためのガイドライン（令和7年度版） https://www.cyber.go.jp/pdf/policy/general/guider7_9.pdf〔2026/7/9 確認〕
※ 59 セキュア・ソフトウェア開発フレームワーク（SSDF：Secure Software Development Framework）：ソフトウェアの開発運用におけるサプライチェーンセキュリティ確保のための対策事項を体系化したフレームワーク（NIST SP800-218、SSDF）を組織に導入するための考え方や流れ等の導入プロセスを、ガイダンスにまとめたもの。
NIST：Secure Software Development Framework（SSDF）Version 1.1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf〔2026/7/9 確認〕
※ 60 経済産業省：第 18 回 サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース（書面審議） https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/018.html〔2026/7/28 確認〕
※ 61 SBOM（Software Bill of Materials）：ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リスト。
※ 62 経済産業省：サイバーセキュリティのためのソフトウェア部品表（SBOM）の共有ビジョンに関する国際ガイダンスに共同署名しました https://www.meti.go.jp/press/2025/09/20250904001/20250904001.html〔2026/7/9 確認〕
※ 63 経済産業省：「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」の日本語版・英語版を策定しました https://www.meti.go.jp/press/2025/03/20260331001/20260331001.html〔2026/7/9 確認〕
※ 64-1 内閣官房：デジタル関連産業のグローバル化促進のための関係閣僚会議（第4回）議事次第 https://www.cas.go.jp/jp/seisaku/digital_global_kakuryokaigi/dai4/siryou.html〔2026/7/9 確認〕
※ 64-2 NEDO：「NEDO 懸賞金活用型プログラム／『課題〔1〕新たなサイバーセキュリティの技術』『課題〔2〕量子計算機時代のブロックチェーンシステムの安全性確保技術』に係る周辺動向調査及び事業運営支援業務」の公募について https://www.nedo.go.jp/koubo/IT2_100390.html〔2026/8/7 確認〕
※ 65 https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html〔2026/7/9 確認〕
※ 66 https://www8.cao.go.jp/cstp/anzen_anshin/kprogram.html〔2026/7/9 確認〕
※ 67 内閣府、経済産業省：「先進的サイバー防御機能・分析能力強化」に関する研究開発構想（プロジェクト型） https://www8.cao.go.jp/cstp/anzen_anshin/02-06_20231020_meti_4.pdf〔2026/7/9 確認〕
※ 68 経済産業省：「サイバーセキュリティ人材の育成促進に向けた検討会最終取りまとめ」を公表しました https://www.meti.go.jp/press/2025/05/20250514002/20250514002.html〔2026/7/9 確認〕
※ 69 セキュリティ・キャンプ協議会：セキュリティ・キャンプ 2026 コネクト https://www.security-camp.or.jp/connect/index.html〔2026/7/9 確認〕
※ 70 「中堅・中小企業が実施するセキュリティ対策に応じた人材確保・育成の実践的方策ガイドβ版（案）」については、以下の 75 ページ以降を参照。
経済産業省：サイバーセキュリティ人材の育成促進に向けた検討会 最終取りまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/cyber_human/pdf/20250514_2.pdf〔2026/7/9 確認〕
※ 71 https://www.ipa.go.jp/security/guide/sme/ug65p900000019cbk-att/sme_guideline_v4.0_app_1.pdf〔2026/7/9 確認〕
※ 72 経済産業省：技術情報管理 自己チェックリスト https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/page03.html〔2026/7/9 確認〕
※ 73 SIG（Special Interest Group）：「特定の分野（各業界におけるサイバー攻撃に関する情報）について、情報を交換するグループ」という意味で、J-CSIP では各業界の参加組織の集合体を SIG と呼んでいる。
※ 74 https://www.ipa.go.jp/security/j-csip/about.html〔2026/7/14 確認〕
※ 75 IPA：サイバーレスキュー隊 J-CRAT（ジェイ・クラート）について https://www.ipa.go.jp/security/j-crat/about.html〔2026/7/14 確認〕
※ 76 IPA：サイバーセキュリティ 相談・届出窓口一覧 https://www.ipa.go.jp/security/support/soudan.html〔2026/7/14 確認〕
※ 77 https://www.meti.go.jp/policy/netsecurity/vul_notification.pdf〔2026/7/14 確認〕
なお、制度発足時は「ソフトウエア等脆弱性関連情報取扱基準（2004 年経済産業省告示第 235 号改め、2014 年経済産業省告示第 110 号）」の告示に基づいていたが、2017 年 2 月に「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号、最終改正令和 6 年経済産業省告示第 93 号）に廃止制定された。
※ 78 経済産業省：経済産業省告示第十九号 https://www.meti.go.jp/policy/netsecurity/vul_institutions.pdf〔2026/7/14 確認〕
※ 79 https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html〔2026/7/14 確認〕
なお、同ガイドラインは 2004 年 7 月 8 日に制定され、2024 年 6 月 18 日に改訂第 13 版が発行された。
※ 80 https://www.ipa.go.jp/security/guide/vuln/ug65p90000019by0-att/partnership_guideline_overview_jp.pdf〔2026/7/14 確認〕
※ 81 https://www.ipa.go.jp/security/reports/vuln/software/2025q4.html〔2026/7/14 確認〕
※ 82 IPA：ソフトウェア等の脆弱性関連情報に関する届出状況 https://www.ipa.go.jp/security/reports/vuln/software/index.html〔2026/7/14 確認〕
※ 83 https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study〔2026/7/6 確認〕
※ 84 ISC2:Employers Must Act as Cybersecurity Workforce Growth Stalls and Skills Gaps Widen https://www.isc2.org/Insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen〔2026/7/6 確認〕
※ 85 https://www.isc2.org/insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study〔2026/7/6 確認〕
※ 86 レバテック株式会社：サイバー攻撃激化でセキュリティ人材の需給逼迫が加速、求人倍率は 42 倍超えに https://levtech.co.jp/research/5053976/〔2026/7/6 確認〕
※ 87 https://juas.or.jp/cms/media/2026/04/JUAS_IT2026.pdf〔2026/7/6 確認〕
※ 88 PR TIMES：ISC2、2025 年版「サイバーセキュリティ人材調査」の結果を発表 https://prtimes.jp/main/html/rd/p/000000024.000103584.html〔2026/7/6 確認〕
※ 89 内閣官房国家安全保障局、NCO 等：AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について https://www.cyber.go.jp/pdf/press/20260518_AI_CS_Package.pdf〔2026/7/6 確認〕
※ 90 NCO：サイバーセキュリティ人材フレームワークに関する検討会 https://www.cyber.go.jp/council/csjinzai/index.html〔2026/7/6 確認〕
※ 91 NICCS:NICE Workforce Framework for Cybersecurity (NICE Framework) https://niccs.cisa.gov/tools/nice-framework〔2026/7/6 確認〕
※ 92 https://www.cyber.go.jp/pdf/council/csjinzai/summary-cybersecurity-workforce-framework-2026.pdf〔2026/7/6 確認〕
※ 93 経済産業省：デジタルスキル標準 ver.2.0（DSSver.2.0）を公表します https://www.meti.go.jp/press/2026/04/20260416002/20260416002.html〔2026/7/6 確認〕
IPA：デジタルスキル標準（DSS）策定の背景・目的 https://www.ipa.go.jp/jinzai/skill-standard/dss/about.html〔2026/7/6 確認〕
※ 94 経済産業省：情報処理安全確保支援士の新たな講習制度「実務経験者に対する講習制度」を創設します https://www.meti.go.jp/press/2025/03/20260327006/20260327006.html〔2026/7/6 確認〕
IPA：実務経験者に対する講習制度について https://www.ipa.go.jp/jinzai/riss/forriss/practical.html〔2026/7/6 確認〕
※ 95 CBT（Computer Based Testing）方式：試験会場に設置されたコンピューターを利用して実施する試験方式のこと。受験者はコンピューターに表示された試験問題に対して、マウスやキーボードを用いて解答する。
※ 96 IPA：情報処理技術者試験 情報処理安全確保支援士試験 統計資料（令和 7 年度試験 全試験区分版） https://www.ipa.go.jp/shiken/reports/h5f8pg000000375x-att/toukei_r07.pdf〔2026/7/9 確認〕
※ 97 IPA：情報処理安全確保支援士登録者について（2026 年 4 月 1

日時点） https://www.ipa.go.jp/jinzai/riss/reports/data/20260401allriss.html〔2026/7/9 確認〕
※ 98 IPA：講習の目的と概要 https://www.ipa.go.jp/jinzai/riss/forriss/koushu/overview.html〔2026/7/9 確認〕
※ 99 IPA：責任者向けプログラム 業界別サイバーレジリエンス強化演習（CyberREX） https://www.ipa.go.jp/jinzai/ics/short-pgm/cyberrex/index.html〔2026/7/9 確認〕
※ 100 IPA：実務者向けプログラム 制御システム向けサイバーセキュリティ演習（CyberSTIX） https://www.ipa.go.jp/jinzai/ics/short-pgm/cyberstix/index.html〔2026/7/9 確認〕
※ 101 経済産業省：情報処理安全確保支援士特定講習 https://www.meti.go.jp/policy/it_policy/jinzai/tokutei.html〔2026/7/9 確認〕
※ 102 IPA：実務経験者に対する講習制度について https://www.ipa.go.jp/jinzai/riss/forriss/practical.html〔2026/7/9 確認〕
※ 103 活用事例（インタビュー・動画） https://www.ipa.go.jp/jinzai/riss/interview/index.html〔2026/7/9 確認〕
※ 104 https://www.security-camp.or.jp/index.html〔2026/7/9 確認〕
※ 105 IPA：セキュリティ・キャンプ 2025 全国大会 https://www.ipa.go.jp/archive/jinzai/security-camp/2025/camp/zenkoku/index.html〔2026/7/9 確認〕
※ 106 IPA：セキュリティ・キャンプ 2025 ネクスト https://www.ipa.go.jp/archive/jinzai/security-camp/2025/camp/next/index.html〔2026/7/9 確認〕
※ 107 IPA：セキュリティ・キャンプ 2025 ジュニア https://www.ipa.go.jp/archive/jinzai/security-camp/2025/camp/junior/index.html〔2026/7/9 確認〕
※ 108 IPA：セキュリティ・キャンプ 2025 ミニ https://www.ipa.go.jp/archive/jinzai/security-camp/2025/minicamp.html〔2026/7/9 確認〕
※ 109 IPA：セキュリティ・キャンプ 2026 コネクト https://www.ipa.go.jp/jinzai/security-camp/connect/index.html〔2026/7/9 確認〕
※ 110 IPA：セキュリティ・キャンプ 2026 フォーラム https://www.ipa.go.jp/jinzai/security-camp/forum.html〔2026/7/9 確認〕
※ 111 https://gcc.ac/〔2026/7/9 確認〕
※ 112 セキュリティ・キャンプ協議会：GCC 2026 Vietnam - Global Cybersecurity Camp 2026 Vietnam https://www.security-camp.or.jp/event/jpn_gcc_vietnam2026_program.html〔2026/7/9 確認〕
※ 113 https://icc.ecsc.eu/〔2026/7/9 確認〕
※ 114 NCO：International Cybersecurity Challenge TOKYO 2025 の開催 https://www.cyber.go.jp/pr/ICCTokyo.html〔2026/7/9 確認〕
※ 115 INTERNET Watch：若手対象の国際サイバー競技会「ICC TOKYO 2025」に出場する日本人選手が決定、アジア代表として過去最多の 6 人が選抜 https://internet.watch.impress.co.jp/docs/news/2044981.html〔2026/7/9 確認〕
※ 116 INTERNET Watch：若手人材の国際サイバー競技会「ICC TOKYO 2025」プログラム公開・一般参加登録の受付を開始 https://internet.watch.impress.co.jp/docs/news/2057252.html〔2026/7/9 確認〕
※ 117 千葉市：International Cybersecurity Challenge TOKYO 2025 https://www.city.chiba.jp/sogoseisaku/miraitoshi/smartcity/icctokyo2025.html〔2026/7/9 確認〕
※ 118 千葉大学：国際サイバー競技会「ICC TOKYO 2025」でプログラミング講座を実施 https://www.chiba-u.jp/news/notice/icc_tokyo_2025.html〔2026/7/9 確認〕
※ 119 東京情報大学：国際大会『ICC Tokyo 2025』でマルウェア解析体験の講座を実施します https://www.tuis.ac.jp/topics/icctokyo2025-tuis-lecture/〔2026/7/9 確認〕
※ 120 GMO インターネットグループ株式会社：第 3 回 GMO 大会議 春サイバーセキュリティ 2026 https://group.gmo/security/conference/2026/〔2026/7/9 確認〕
GMO インターネットグループ株式会社：GMO Cybersecurity Awards 2026 https://group.gmo/security/awards/2026/〔2026/7/9 確認〕
※ 121 IPA：中核人材育成プログラム 卒業プロジェクト https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/index.html〔2026/7/9 確認〕
※ 122 IPA：中核人材育成プログラム修了者コミュニティ 叶会（かなえかい） https://www.ipa.go.jp/jinzai/ics/core_human_resource/kanaekai.html〔2026/7/9 確認〕
※ 123 IPA：責任者向けプログラム サイバーセキュリティ企画演習（CyberSPEX） https://www.ipa.go.jp/jinzai/ics/short-pgm/cyberspex/index.html〔2026/7/9 確認〕
※ 124 IPA：実務者向けプログラム ERAB サイバーセキュリティトレーニング 事業内容 https://www.ipa.go.jp/jinzai/ics/short-pgm/erab/index.html〔2026/7/9 確認〕
※ 125 https://www.enecho.meti.go.jp/category/saving_and_new/advanced_systems/vpp_dr/20250522.pdf〔2026/7/9 確認〕
※ 126 IPA：セキュリティ要件適合評価及びラベリング制度（JC-STAR） https://www.ipa.go.jp/security/jc-star/index.html〔2026/7/9 確認〕
※ 127 https://www.ipa.go.jp/publish/wp-security/2025.html〔2026/7/9 確認〕
※ 128 IPA：セキュリティラベリング制度（JC-STAR）についての詳細情報 https://www.ipa.go.jp/security/jc-star/detail.html〔2026/7/9 確認〕
※ 129 IPA：情報セキュリティ 10 大脅威 2026 https://www.ipa.go.jp/security/10threats/10threats2026.html〔2026/7/9 確認〕
※ 130 IPA：欧州規格 ETSI EN 303 645 V2.1.1（2020-06）の翻訳 https://www.ipa.go.jp/security/controlsystem/etsien303645.html〔2026/7/9 確認〕
※ 131 NIST：NIST IR 8425 Profile of the IoT Core Baseline for Consumer IoT Products https://csrc.nist.gov/pubs/ir/8425/final〔2026/7/9 確認〕
※ 132 European Commission:Cyber Resilience Act https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act〔2026/7/9 確認〕
※ 133 IPA：★ 1（レベル 1）適合基準・評価手順（評価手法・評価ガイド） https://www.ipa.go.jp/security/jc-star/tekigou-kizyun-guide/label1/index.html〔2026/8/21 確認〕
※ 134 NCO：政府機関等の対策基準策定のためのガイドライン（令和7年度版）の一部改定（令和7年9月5日）のポイント https://www.cyber.go.jp/pdf/policy/general/rev_pointr7_9.pdf〔2026/7/9 確認〕
※ 135 経済産業省：「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」を改定しました https://www.meti.go.jp/press/2025/05/20250522001/20250522001.html〔2026/7/9 確認〕
※ 136 NCO：G7 Cybersecurity Working Group Statement on IoT Security https://www.cyber.go.jp/pdf/press/G7_Statement_on_IoT_Security.pdf〔2026/7/9 確認〕
※ 137 GOV.UK：The UK Product Security and Telecommunications Infrastructure (Product Security) regime https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime〔2026/7/9 確認〕
legislation.gov.uk：Product Security and Telecommunications Infrastructure Act 2022 https://www.legislation.gov.uk/ukpga/2022/46/contents〔2026/7/9 確認〕
※ 138 Cyber Security Agency of Singapore：About Cybersecurity Labelling Scheme for IoT - CLS (IoT) https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/〔2026/7/9 確認〕
※ 139 経済産業省：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）に関して共同声明を発表しました https://www.meti.go.jp/press/2025/10/20251023003/20251023003.html〔2026/7/9 確認〕
※ 140 FCC：U.S. Cyber Trust Mark https://www.fcc.gov/CyberTrustMark〔2026/7/9 確認〕
※ 141 IPA：JC-STAR 活用に向けた取り組み https://www.ipa.go.jp/security/jc-star/leverage.html〔2026/7/9 確認〕
※ 142 JEITA、一般社団法人大手家電流通協会：JC-STAR 制度普及へ、製販連携を本格推進 https://www.jeita.or.jp/japanese/topics/2026/0129.pdf〔2026/7/9 確認〕
※ 143 IPA：★ 3（レベル 3）適合基準・評価手順（評価手法・評価ガイド） https://www.ipa.go.jp/security/jc-star/tekigou-kizyun-guide/label3/index.html〔2026/7/9 確認〕
※ 144 IPA：IT セキュリティ評価及び認証制度（JISEC） https://www.ipa.go.jp/security/jisec/index.html〔2026/7/13 確認〕
※ 145 https://www.cyber.go.jp/pdf/policy/general/kijyunr7.pdf〔2026/8/21 確認〕
※ 146 経済産業省：IT 製品の調達におけるセキュリティ要件リスト（第 2.1 版） https://www.meti.go.jp/policy/netsecurity/youken.list.ver.2.1_20260121.pdf〔2026/7/13 確認〕
※ 147 IPA：セキュリティ評価基準（CC/CEM） https://www.ipa.go.jp/security/jisec/about/kijun.html〔2026/7/13 確認〕
※ 148 デジタル庁：政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a612d406/20250619_resources_standard_guidelines_guideline_08.pdf〔2026/7/9 確認〕
※ 149 https://www.soumu.go.jp/main_sosiki/kenkyu/cloud_service/index.html〔2026/7/9 確認〕
※ 150 「ISMAP 管理基準」「ISMAP 管理基準マニュアル」「ISMAP 管理基準ガイドブック」の入手方法については、以下の Web ページを参照されたい。

ISMAP：ISMAP 管理基準　https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010028&sys_kb_id=da947d9e2bf9fa90f0bbfd69fe91bfa4&spa=1〔2026/7/9 確認〕
※ 151 https://www.cyber.go.jp/policy/group/general/ismap.html〔2026/7/9 確認〕
※ 152 https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005〔2026/7/9 確認〕
※ 153 https://www.ismap.go.jp〔2026/7/9 確認〕
※ 154 総務省：「クラウドサービスの安全性評価に関する検討会　とりまとめ」の公表　https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00096.html〔2026/7/9 確認〕
※ 155 規制改革推進会議：規制改革推進に関する答申（令和７年５月28日）　https://www8.cao.go.jp/kisei-kaikaku/kisei/publication/opinion/250528.pdf〔2026/7/9 確認〕
※ 156 NCO、デジタル庁、総務省、経済産業省：ISMAP 制度の見直しについて　https://www.ismap.go.jp/sys_attachment.do?sys_id=ab1c8a0083afb650aa68c6a8beaad3bc〔2026/7/9 確認〕
※ 157 e-Gov：「ISMAP 管理基準（案）」等に対する意見公募の結果について　https://public-comment.e-gov.go.jp/pcm/detail?CLASSNAME=PCMMSTDETAIL&Mode=0&bMode=1&bScreen=Pcm1040&id=060250918〔2026/7/9 確認〕
※ 158 ISMAP：ISMAP 管理基準改定案　https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0012199〔2026/7/9 確認〕
※ 159 https://www.ismap.go.jp/sys_attachment.do?sys_id=508af37583388fd0aa68c6a8beaad382〔2026/7/9 確認〕
※ 160 ISMAP：FAQ　https://www.ismap.go.jp/csm?id=kb_search&kb_knowledge_base=7d332ae0db43a050eeab7845f3961922〔2026/7/9 確認〕
※ 161 https://www.ismap.go.jp/sys_attachment.do?sys_id=fc71c04a83788fd0aa68c6a8beaad368〔2026/7/9 確認〕
※ 162 デジタル庁：ISMAP-LIU 登録促進のための取組み　https://www.digital.go.jp/policies/security/ismap-liu〔2026/7/9 確認〕
※ 163 内閣官房：政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議　https://www.cas.go.jp/jp/seisaku/pqc/index.html〔2026/7/9 確認〕
※ 164 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）　https://www.cas.go.jp/jp/seisaku/pqc/pdf/report_202511.pdf〔2026/7/9 確認〕
※ 165 デジタル庁、総務省、経済産業省：電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）　https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022r2.pdf〔2026/7/9 確認〕
※ 166 CRYPTREC：2025 年度 第1回 暗号技術検討会　https://www.cryptrec.go.jp/report/cryptrec-mt-1011-2025.pdf〔2026/7/9 確認〕
※ 167 NIST：FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard　https://csrc.nist.gov/pubs/fips/203/final〔2026/7/9 確認〕
※ 168 CRYPTREC：耐量子計算機暗号への移行に関する技術動向調査　https://www.cryptrec.go.jp/exreport/cryptrec-ex-3503-2025.pdf〔2026/7/9 確認〕
※ 169 NIST：FIPS 204, Module-Lattice-Based Digital Signature Standard　https://csrc.nist.gov/pubs/fips/204/final〔2026/7/9 確認〕
※ 170 NIST：FIPS 205, Stateless Hash-Based Digital Signature Standard　https://csrc.nist.gov/pubs/fips/205/final〔2026/7/9 確認〕
※ 171 CRYPTREC：暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準　https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf〔2026/7/9 確認〕
※ 172 CRYPTREC：TLS 暗号設定ガイドライン　https://www.cryptrec.go.jp/report/cryptrec-gl-3001-3.1.1.pdf〔2026/7/9 確認〕
※ 173 https://www.think7.org/publications/accelerating-the-transition-to-quantum-safe-communication-a-call-for-global-collaboration-and-action/〔2026/7/9 確認〕
※ 174 経済産業省：「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）を公表しました　https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html〔2026/7/14 確認〕
※ 175 IPA：情報セキュリティ 10 大脅威 2025 組織編　https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/kaisetsu_2025_soshiki.pdf〔2026/7/14 確認〕
※ 176 英国の「Cyber Essentials」、一般社団法人日本自動車工業会及び一般社団法人日本自動車部品工業会の「自動車産業サイバーセキュリティガイドライン」等。
NCSC：Cyber Essentials　https://www.ncsc.gov.uk/cyberessentials/overview〔2026/7/14 確認〕
一般社団法人日本自動車工業会：自動車産業サイバーセキュリティガイドライン　https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html〔2026/7/14 確認〕
※ 177 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サプワーキンググループ事務局：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　https://www.meti.go.jp/files/900017305.pdf〔2026/7/14 確認〕
※ 178 IPA：SECURITY ACTION セキュリティ対策自己宣言　https://www.ipa.go.jp/security/security-action/〔2026/7/14 確認〕
※ 179 IPA: SCS 評価制度の詳細情報　https://www.ipa.go.jp/security/scs/details.html〔2026/7/14 確認〕
※ 180 https://www.meti.go.jp/policy/netsecurity/partnership2.html〔2026/7/14 確認〕
※ 181 経済産業省：【想定事例】発注側企業からの「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」4つ星相当の対策の実施要請を踏まえ、発注側企業と取引の相手方とが円満に価格交渉を行うためのプラクティス　https://www.meti.go.jp/policy/netsecurity/partnership_souteijirei.pdf〔2026/7/14 確認〕
※ 182 経済産業省：サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて（令和4年 10 月 28 日　経済産業省・公正取引委員会）を踏まえた想定事例について（解説）　https://www.meti.go.jp/policy/netsecurity/partnership_soueijireikaisetu_.pdf〔2026/7/14 確認〕
※ 183 経済産業省：サイバーセキュリティお助け隊サービス（新類型）　https://www.meti.go.jp/policy/netsecurity/otasuketai_jissho.html〔2026/7/14 確認〕
※ 184-1 IPA：中小企業向けサイバーセキュリティ対策支援者リストの紹介　https://www.ipa.go.jp/security/sme/shien/list.html〔2026/7/14 確認〕
※ 184-2 読売新聞オンライン：中小企業狙うランサムウェア攻撃、国内被害の6割…現場混乱・復旧に4か月・費用は数千万円「倒産の危機と紙一重だった」　https://www.yomiuri.co.jp/national/20260313-GYT1T00461/〔2026/8/21 確認〕
※ 185 経済産業省：ワーキンググループ 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に関するサブワーキンググループ）　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/index.html〔2026/7/14 確認〕
※ 186 経済産業省：ワーキンググループ 2（サイバーセキュリティ人材の育成促進に向けた検討会）　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/cyber_human/index.html〔2026/7/14 確認〕
※ 187 https://www.ipa.go.jp/security/guide/sme/ug65p900000019cbk-att/sme_guideline_v4.0_app_3.pdf〔2026/7/14 確認〕
※ 188 IPA：「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について　https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html〔2026/7/14 確認〕
※ 189 IPA：中小企業向けサイバーセキュリティ対策支援者リスト及び活用事例の紹介　https://www.ipa.go.jp/security/sme/shien/index.html〔2026/7/14 確認〕
※ 190 経済産業省：第 10 回産業サイバーセキュリティ研究会 事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/010_03_00.pdf〔2026/7/14 確認〕
※ 191 https://www.ipa.go.jp/security/sme/otasuketai-about.html〔2026/7/14 確認〕
※ 192 https://www.ipa.go.jp/security/sme/ps6vr7000001hnrl-att/otasuketai-leaflet.pdf〔2026/7/14 確認〕
※ 193 https://www.ipa.go.jp/security/sme/otasuketai/nq6ept000000faii-att/000092713.pdf〔2026/7/14 確認〕
※ 194 https://www.ipa.go.jp/security/otasuketai-pr/〔2026/7/14 確認〕
※ 195 中小企業庁：デジタル化・AI 導入補助金 2026 の公募要領を公開しました　https://www.chusho.meti.go.jp/koukai/hojyokin/kobo/2026/260310001.html〔2026/7/14 確認〕
※ 196 https://www.ipa.go.jp/security/security-action/index.html〔2026/7/14 確認〕
※ 197 IPA 等：中小企業や情報セキュリティの関係団体が、中小企業の情報セキュリティ対策普及の加速化に向けた共同宣言を発表　https://www.ipa.go.jp/security/sme/ps6vr7000001hnrl-att/000102928.pdf〔2026/7/14 確認〕
※ 198 https://www.ipa.go.jp/security/security-action/download/infosec6to-dos.pdf〔2026/7/14 確認〕
※ 199 IPA：「2023 年度 SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査」報告書について　https://www.ipa.

go.jp/security/reports/sme/sa-survey2023.html〔2026/7/14 確認〕
※ 200 IPA：2026 年 3 月以前に申込された宣言事業者一覧　https://www.ipa.go.jp/security/security-action/activity/〔2026/7/14 確認〕

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「ブダペスト条約」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 ヵ国のうち、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 ヵ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 ヵ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 ヵ国以上の国と、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 ヵ国で「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あり、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）、白玧靜（ペク・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、日本の髙見澤將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靱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を提供する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)及び体現型 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「体現型 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

るようになった。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

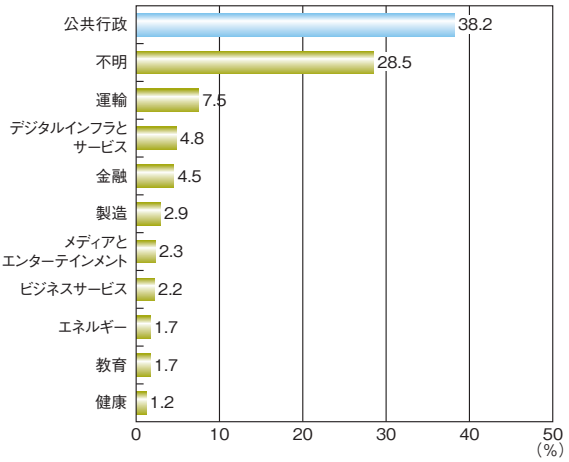
2025 年度のサイバー空間は、ランサムウェアの高度化や国家支援型攻撃、AI を悪用した攻撃等により、更なる脅威に直面した。これに対し EU は、欧州全体の防衛能力とレジリエンスを強化するべく、包括的な法整備による統一的な防御体制の確立に注力している。以下では欧州におけるサイバー脅威の全体動向と今後の見通しを紹介し、2025 年から 2026 年 1 月にかけて検討・実施された主要なサイバーセキュリティ政策について述べる。

(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% が悪性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、ブラウザー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 ヵ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 ヵ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ブループリントに基づき、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）の導入や検討も進められており、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ヵ年計画」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」にとどまるものではなく、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、不実情報、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。もっとも、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

か否かの判断基準、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にとどまらず、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や※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ー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

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摂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

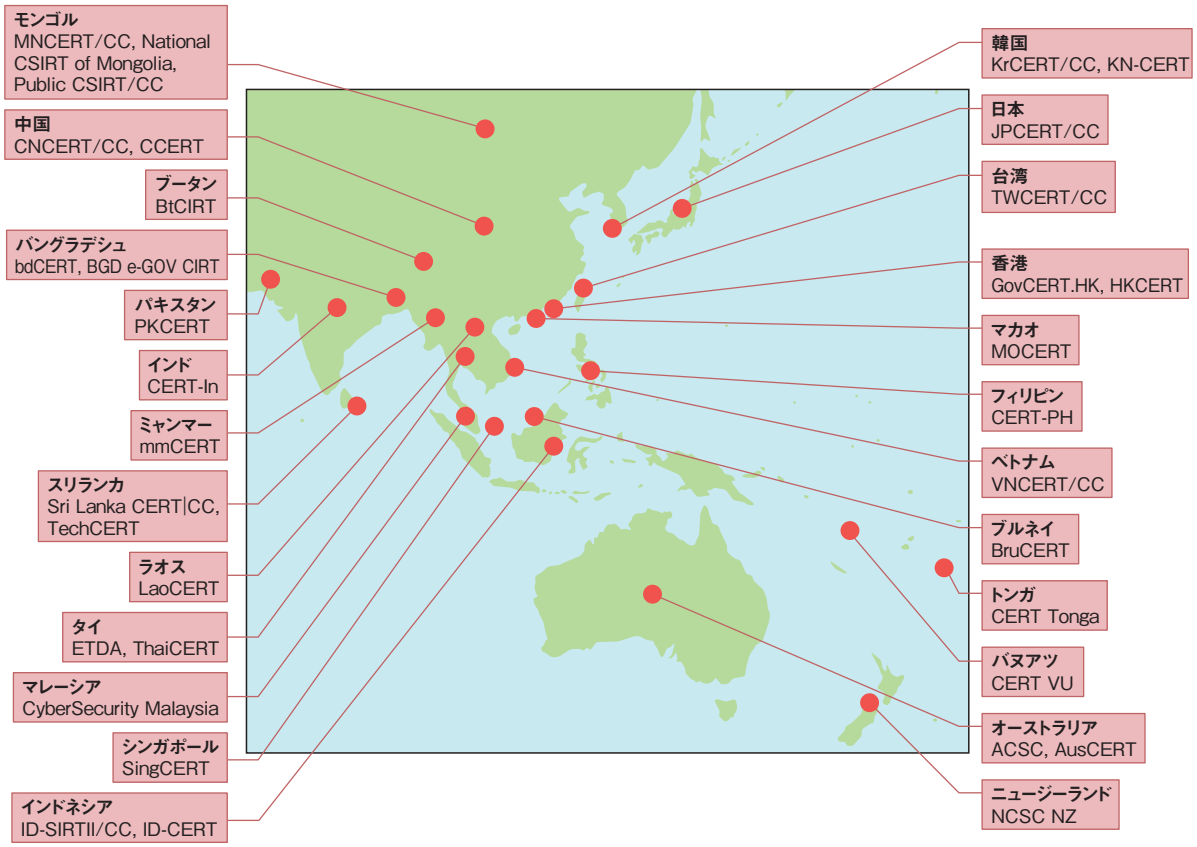
アジア太平洋地域全体の CSIRT からなるコミュニティ

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が期待される。

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お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、作業部会のメーリング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。

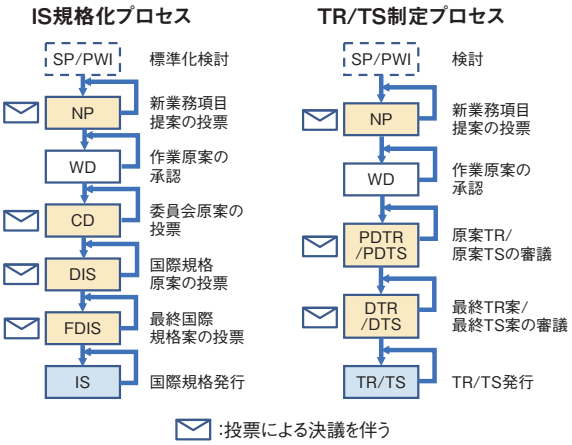
4.2.2 情報セキュリティ、サイバーセキュリティ、プライバシー保護関係の規格の標準化（ISO/IEC JTC 1/SC 27）

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）

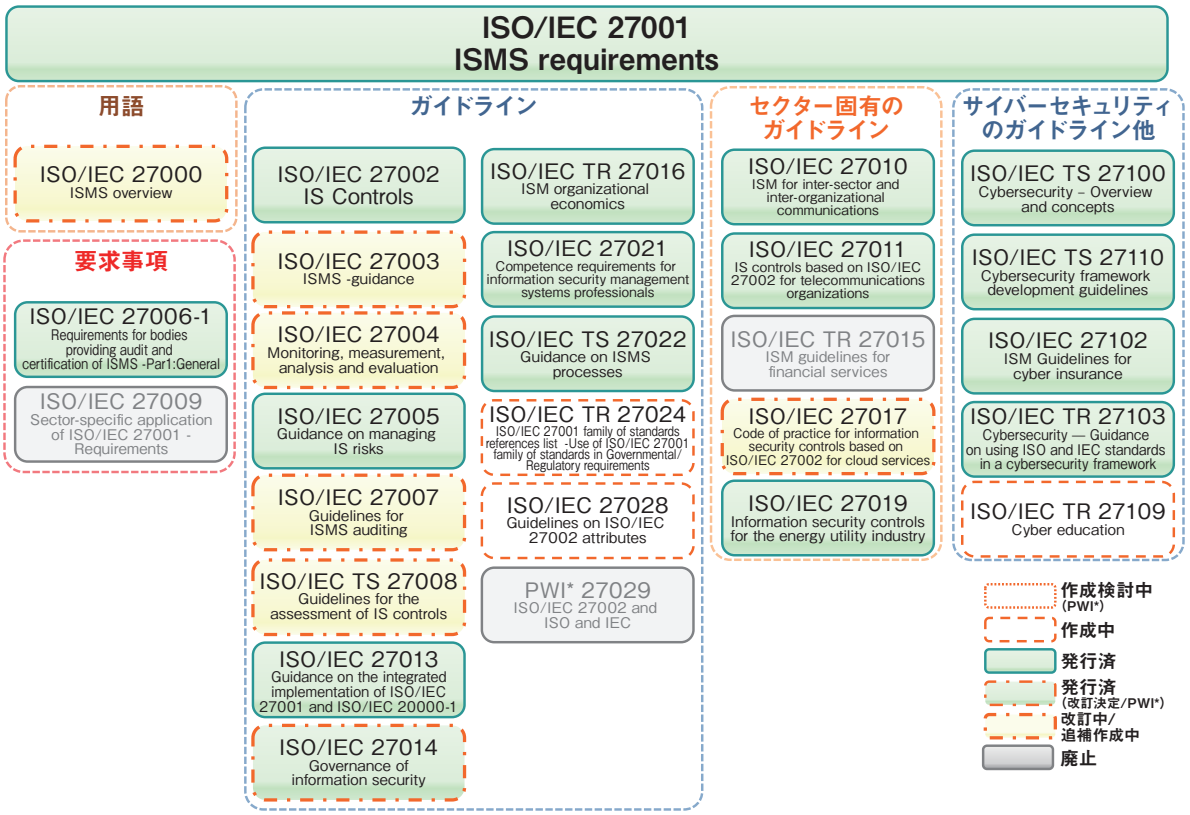
以下に、各WGの活動概要を述べる。なお本文中では略号を使用する。第42回会合は2025年9月に中国昆明で、第43回会合は2026年3月にドイツニュルンベルグで実施されたSC 27総会及び各WG会議を指す。

（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/PRFAmd 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。

COLUMN

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[i]」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「どれだけ怖いか」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つきます。

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 /〔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-hacktivist-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_xQ21tWds8j84OOHtQCiAeUvO8uI2o〔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 ワーカーの手口　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/MDGDOCGMORLNLN5QROXZS5F5NI-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:ブダペスト条約))　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/NFRFU5BOQNP7JLDKH7HEJY5AIA-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 回日 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 回日・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/ngi93u0000002l50-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 BudgetPriorities 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-8fdfd910268a/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/content/pkg/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-o-f2022_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 (CIRCIA) 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 (CIRCIA) 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〔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-its-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を保存・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 マーキングの概要：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〕
国務院：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 国務院：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：网络数据安全管理条例 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〕
国家法律法規データベース：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：网络数据安全管理条例 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ー管理条例を公布、データ越境などのセキュリティー詳細を規定 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 全国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 国家法律法規データベース：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《中华共和国网络安全法》的决定&type=decision〔2026/7/7 確認〕
国家法律法規データベース：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 パアンガドル 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, cybersecurity 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/u71kba000000jjgv-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いたします。

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？



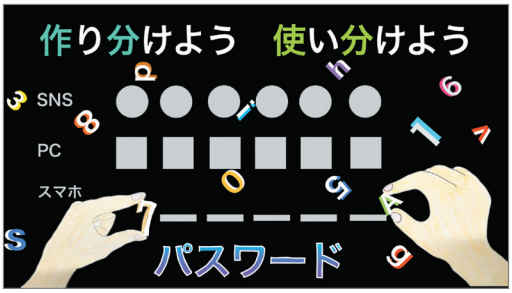
脇 玲美奈さん
静岡市立安東小学校

視線の先



小磯 凛さん
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

索引

数字

0APT ····· 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）導入ガイダンス ····· 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
ClOP（ClOp、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
脆弱性……8, 24, 37, 121, 170, 176
生成 AI（Generative AI）……69, 92, 110
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
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
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
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
セキュア・バイ・デザイン……32, 117
セキュリティ・キャンプ……118, 127
セキュリティ・クリアランス制度……66
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
ゼロデイ攻撃……37
ゼロトラスト……84, 166
組織における内部不正防止ガイドライン……44

た

ダークウェブ……20, 26, 37
第 14 次 5 ヵ年計画……180
対ランサムウェア・イニシアチブ（CRI：Counter Ransomware Initiative）……162
耐量子計算機暗号（PQC：Post-Quantum Cryptography）……142, 168
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
中核人材育成プログラム……128
中華人民共和国サイバーセキュリティ法……181, 183
中小企業の情報セキュリティ対策ガイドライン……116, 147
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
ディープフェイク……92, 94, 110, 160
ディスインフォメーション（Dis-information）……88
データ三法……181
データ侵害……9, 11, 172
データセキュリティ……111
適合ラベル……133
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
デジタルオムニバス規則案……173
デジタルサービス法（DSA：Digital Services Act）……93, 174
デジタル社会の実現に向けた重点計画……111
デジタル署名……175, 190
デジタルスキル標準（DSS）……124
デジタルトラスト……165
デバイス・コード・フィッシング（Device Code Phishing）……9
特別社会基盤事業者……63

な

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
内部不正……32, 42
ナラティブ……90, 95
なりすまし……42, 71, 162
二重の脅迫（二重恐喝）……16, 19, 23
偽・誤情報……75, 88
偽情報……88
偽のウイルス感染警告……49, 52, 110
日 ASEAN サイバーセキュリティ政策会議……117, 164
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
日 ASEAN 能力向上プログラム強化プロジェクト……165
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
籔口 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	髙田 早苗	高橋 将
髙村 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

おわりに

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。 新時代といえば、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典を記載しています。
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、™ または ® マークは明記しておりません。
・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**

Copyright © 2026 Innovation Platform Agency, Japan（IPA）