情報セキュリティ白書

Information Security White Paper

2025

一変する日常：支える仕組みを共に築こう



独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

「情報セキュリティ白書2025」の刊行にあたって

「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分野における、政策や脅威の動向、インシデントや被害の実態等をまとめ、皆様のセキュリティ対策の推進、学習・研鑽等にお役立ていただくという趣旨で発刊し、産業界、学界、一般の方に広く愛読されてきました。

サイバー空間を巡る脅威は年を追うごとに質・量ともに増大しております。2024 年も国内国外を問わず、ランサムウェア攻撃、標的型攻撃、DDoS 攻撃等、様々なサイバー攻撃による脅威に晒されました。また、今般の厳しい国際情勢下において、影響工作を始めとした地政学的背景に起因するサイバー空間のリスクも顕在化しております。サイバー攻撃の手口も、取引先や委託先等のサプライチェーン上でセキュリティ対策が不十分な部分を入口とするものや、複雑なソフトウェアのサプライチェーンの脆弱性を狙ったもの、更には、生成 AI を悪用したもの等、一層高度化・巧妙化しております。

他方、データ駆動型の便利で豊かな社会、Society 5.0 の実現を目指し、サイバー空間とフィジカル空間が融合していく中で、セキュリティ面でのリスクが顕在化してきております。これまでのフィジカル空間での経済社会行動が IoT 機器やロボット等、様々なデバイスとつながることによりデータ化され、ネット上のサイバー空間に集積し、そのビッグデータが生成 AI により解析、最適化されるサイクルの中で、サイバー攻撃を許す隙が増えるとともに、一度インシデントが起きるとその影響が瞬時に広範に伝播し、大規模な情報漏えいやインフラの機能不全をもたらすリスクがますます高まってきております。

こうした中で、国内では、2022 年 12 月に閣議決定された国家安全保障戦略において「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」との目標が掲げられ、2025 年 5 月にはサイバー対処能力強化法及び同整備法が成立し、「国民生活や経済活動の基盤」と「国家及び国民の安全」をサイバー攻撃から守るための能動的なサイバー防御を実施する体制の整備が進められています。

また、経済社会インフラが直面するサイバーリスクへの耐性を確保する観点から、システムの設計段階、すなわち、アーキテクチャーレベルでセキュリティを組み込んでいく、「セキュア・バイ・デザイン」の視点に立った様々な制度整備や取り組み、これらを推進していくための人材や技術等、サイバーセキュリティ供給能力の強化に向けた取り組み等も新たに動き出しております。

本白書が、2024 年度の情勢を踏まえた脅威分析と政策動向の総括を通じ、関係者の皆さまの日々の対策検討や実践に資するものであること、そしてより安全で信頼されるデジタル社会の確立に寄与する一助となることを、心より願っております。

2025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　2024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　2024年度に観測されたインシデント状況 …… 8

1.1.1　世界における情報セキュリティインシデント状況 …… 8
1.1.2　国内における情報セキュリティインシデント状況 …… 12

1.2　インシデント事例や脆弱性・攻撃の動向と対策 …… 17

1.2.1　ランサムウェア攻撃 …… 17
1.2.2　標的型攻撃 …… 23
1.2.3　DDoS攻撃 …… 31
1.2.4　情報システムの脆弱性に関する動向 …… 34
1.2.5　重要インフラ・制御システムに対する脅威 …… 39
1.2.6　IoTに対する脅威 …… 47
1.2.7　内部不正による情報漏えい …… 54
1.2.8　個人を狙う騙しの手口 …… 57

第2章 最近のサイバー空間を巡る注目事象 …… 76

2.1　AIセーフティ実現に向けた取り組み …… 76

2.1.1　AIの急速な発展 …… 76
2.1.2　AIリスクとは何か …… 77
2.1.3　AIセーフティに関する取り組み …… 81
2.1.4　AIセキュリティの現状 …… 85

2.2　偽・誤情報の脅威の動向 …… 91

2.2.1　虚偽情報の定義 …… 91
2.2.2　偽・誤情報の情勢 …… 92
2.2.3　2024年度の注目事象 …… 94
2.2.4　2024年度以前からの継続事象 …… 101
2.2.5　状況のまとめと今後の見通し …… 102

第3章 国内の政策及び取り組みの動向 …… 110

3.1 国内のサイバーセキュリティ政策の状況 …… 110

3.1.1 政府全体の政策動向 …… 110
3.1.2 デジタル庁の政策 …… 121
3.1.3 経済産業省の政策 …… 124
3.1.4 総務省の政策 …… 131
3.1.5 警察によるサイバー空間の安全確保の取り組み …… 134

3.2 サイバーセキュリティ人材の現状と育成 …… 141

3.2.1 サイバーセキュリティ人材の現状と育成状況 …… 141
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 …… 144
3.2.3 セキュリティ人材育成のための活動 …… 145

3.3 製品・サービスの評価・認証制度・暗号技術の動向 …… 151

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） …… 151
～ IoT製品のセキュリティレベルの見える化 ～
3.3.2 ITセキュリティ評価及び認証制度（JISEC） …… 158
～ IT製品がセキュリティ確保されていることの確認手段 ～
3.3.3 サプライチェーン強化に向けた対策評価制度構築に向けた検討 …… 161
～ サプライチェーン構成企業のセキュリティ向上に向けた取り組み ～
3.3.4 政府情報システムのためのセキュリティ評価制度（ISMAP） …… 162
～ クラウドサービスの安全性評価の取り組み ～
3.3.5 CRYPTREC …… 164
～ 安全な暗号アルゴリズムの選定と安全な利活用への取り組み ～

3.4 組織・個人に向けたサイバーセキュリティ対策の普及活動 …… 168

3.4.1 組織におけるサイバーセキュリティの取り組みと支援策 …… 168
3.4.2 サイバーセキュリティ及びネットリテラシーの普及活動 …… 173

第4章 国際的な政策及び取り組みの動向 …… 184

4.1 国際的なサイバーセキュリティ政策の状況 …… 184

4.1.1 国際社会と連携した日本の取り組み …… 184
4.1.2 米国の政策 …… 189
4.1.3 欧州の政策 …… 193
4.1.4 中国の政策 …… 199
4.1.5 アジア太平洋地域でのCSIRTの動向 …… 201

4.2 国際標準化活動 …… 206

4.2.1 様々な標準化団体の活動 …… 206
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） …… 207
4.2.3 制御システム関連のセキュリティ規格の標準化（IEC TC 65/WG 10） …… 210

付録 ····· 217
第20回IPA「ひろげよう情報セキュリティコンクール」2024受賞作品 ····· 218
IPAの便利なツールとコンテンツ ····· 220
索引 ····· 225

コラム

トラブルを招かないためのデータマネジメント ～データ品質管理の勧め～ ····· 16
情報セキュリティ10大脅威 2025 ～変わらない脅威、新たに選出された脅威～ ····· 63
サイバーセキュリティとデジタルトランスフォーメーション
～WISDOM-DXと生成AIによる「情報セキュリティ白書」の分析～ ····· 89
「クラウドサービスのリスク」をどうやって把握する? ····· 150
これからは「量子コンピューターに対して安全な暗号」を使わなければいけないの? ····· 166
セキュリティは「コスト」か「投資」か? ····· 176

2025

情報セキュリティ白書

●序章　2024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　2024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　最近のサイバー空間を巡る注目事象

2.1　AIセーフティ実現に向けた取り組み
2.2　偽・誤情報の脅威の動向

●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・暗号技術の動向
3.4　組織・個人に向けたサイバーセキュリティ対策の普及活動

●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

2024年度の情報セキュリティの概況

近年、情報セキュリティの脅威は一層深刻化しており、サイバー攻撃の手法も高度化している。2024 年においては、ランサムウェア攻撃や、DDoS 攻撃等のインシデントが相次ぎ、重要インフラや企業の運営に影響を与えた。国内では 2024 年 6 月に、総合エンターテインメント企業がランサムウェア攻撃を受け、動画配信サービスやオンラインショップの障害、出荷遅延等の被害が生じた。また印刷会社に対するランサムウェア攻撃では、約 60 の委託元に影響が及んだ。これらのインシデントは、サービス停止や情報漏えいにより多数の企業・組織及び利用者に被害をもたらし、情報セキュリティ対策の重要性を改めて認識させた。国外では、鉄道、空港、水処理施設等の重要インフラに対してランサムウェア攻撃被害が発生し、安全保障の観点からも対策が急務となっている。

2024 年には、政治的なイベントに関連した DDoS 攻撃が増加し、公共の安全や秩序が脅かされる事態も発生した。2024 年 7 月、8 月にはオリンピック関連のスポンサー、パートナーの Web サイトを標的とした DDoS 攻撃が観測された。また 2024 年は世界各国で重要な選挙が行われ、選挙運動、政党、選挙インフラを対象とした DDoS 攻撃が観測された。米国では、大統領選挙を狙った DDoS 攻撃が 11 月に発生した。日本でも、2024 年 7 月と 10 月に安全保障イベントに関連した DDoS 攻撃が発生した。また、2024 年末から 2025 年初頭にかけて、航空会社、金融機関、携帯通信会社が相次いで DDoS 攻撃を受け被害が発生した。これらの攻撃には IoT ボットネットが利用されている。

2025 年 1 月、警察庁と NISC（現 NCO）は、2019 年ごろから継続していた複数の攻撃キャンペーンについて、国家に支援されたサイバー攻撃グループによるものとして注意喚起を行った。これらの攻撃は、日本の安全保障の棄損や先端技術情報の窃取を目的としており、攻撃手法の公表を通じて被害の拡大防止が呼びかけられた。

国際的には、国家を背景としたサイバー攻撃の激化による被害が発生した。「Salt Typhoon」と呼ばれる攻撃グループによる攻撃では、米国通信事業者 9 社を含む世界中の企業数十社のシステムへの侵入が観測され、広範なスパイ活動及び情報収集が行われたことが確認された。国家を背景とした攻撃グループに対しては複数の国、組織が連携し、情報共有や摘発を行っている。

2024 年は AI の悪用による被害も報告された。前述の選挙妨害においては生成 AI が偽情報の生成に多用されたという。偽情報の流布を利用した情報操作型サイバー攻撃は、社会の混乱や分断、政府機関の信頼失墜等、サイバー領域と認知領域の双方にわたる攻撃手段として，国家の安全保障上の脅威ともとらえられる。今後も警戒が必要である。

このような状況を踏まえ、日本国内においてもサイバーセキュリティ政策の強化が進められた。ランサムウェア攻撃の被害拡大や DDoS 攻撃における IoT 機器の悪用に対して、政府は 2024 年度のサイバーセキュリティ戦略において、サプライチェーン・リスクへの対応と DX 推進・支援の強化を掲げた。経済産業省は「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引」「セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス」の発行等で、設計段階からセキュリティを考慮するセキュア・バイ・デザインの施策を推進した。また、2025 年 3 月には IoT 製品のセキュリティ評価認証制度として「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」の運用が開始された。更に、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の検討等にも取り組んでいる。

サイバー安全保障分野では、「外部からのサイバー攻撃について、被害が発生する前の段階から、その兆候に係る情報その他の情報の収集を通じて探知し、その主体を特定するとともに、その排除のための措置を講ずることにより、国家及び国民の安全を損なうおそれのあるサイバー攻撃の発生並びにこれによる被害の発生及び拡大の防止」を図る「能動的サイバー防御」の実現に向けた検討が進められた。その結果、2025 年 5 月には「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」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」が成立した。今後、官民連携の強化、通信情報の利用、攻撃サーバーの無害化等の実践を通じ、サイバー安全保障分野での対応能力向上が期待される。

	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
2024年 4月	● 米国のセキュリティベンダーが提供するファイアウォール用OSに対するゼロデイ攻撃を確認（1.2.4） ● 米国のマルチクラウドデータウェアハウスプラットフォームを利用している複数の組織を標的としたデータ侵害が発生（1.1.1）	● 米国「外国敵対勢力が管理するアプリから米国人を保護する法」成立（4.1.1）
5月	● 国家の支援が疑われるサイバー攻撃グループが、国内の暗号資産関連事業者から約482億円相当の暗号資産を窃取（1.2.2） ● 行政機関等から通知書等の印刷と発送を請け負っていた印刷会社でランサムウェア被害が発生（1.2.1）	● 「重要経済安保情報保護活用法」成立（3.1.1） ● NISCと警察庁が、米国CISAの作成したサイバー脅威緩和に関する国際ガイダンスに共同署名（4.1.1） ● 「AIソウル・サミット」開催（2.1.3）
6月	● 総合エンタメ企業が展開する動画共有サービス等がランサムウェア攻撃を受け、サービス停止（1.2.1）	● 「G7プーリア・サミット」開催（3.1.1）
7月	● 日本・NATOの活動に抗議するDDoS攻撃が発生（1.2.3） ● 米国サイバーセキュリティ会社のシステム障害により世界約850万台のWindowsデバイスに影響が発生（1.1.1） ● パリオリンピック関連のスポンサー、パートナーを標的としたDDoS攻撃が発生（1.1.1）	● NISCと警察庁は、オーストラリアのACSCが作成したAPT40に関する国際アドバイザリーに共同署名（4.1.1） ● NISC「サイバーセキュリティ2024」公表（3.1.1） ● NISTは、生成AIのセキュア開発のためのプロファイルである「SP 800-218A」公開（4.1.2）
8月	● 不動産仲介業の従業員が同業他社に転職する際、不動産登記簿に基づく社内資料を不正に持ち出し（1.2.7） ● 米国の国際空港がランサムウェア攻撃を受け、フライト情報表示等の重要な機能に影響が発生（1.2.5）	● EU「AI Act」発効（2.1.1、2.1.3） ● 経済産業省「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver 2.0」公表（3.1.3）
9月	● 米国司法省は、国家の支援が疑われる攻撃グループに侵害された20万台超の消費者向け機器からなるボットネットを無害化したと発表（1.2.2） ● 米国の水処理施設にランサムウェア攻撃（1.2.5）	
10月	● ランサムウェア開発者らを欧州刑事警察機構等による共同捜査により逮捕（4.1.1） ● 日米共同統合演習に抗議するDDoS攻撃が発生（1.2.3）	● オーストラリアのACSCは、重要インフラ事業者に向けて策定した「OTサイバーセキュリティの原則」公開（4.1.5）
11月	● 米国大統領選挙で、複数の国家が関与すると見られる影響工作を確認（2.2.3） ● 米国大統領選挙期間中に大規模なDDoS攻撃が数日にわたって発生（1.1.1） ● 国家の支援が疑われる攻撃グループが9社の米国通信事業者、及び世界中の企業数十社を侵害していたことをFBI等が公表（1.1.1、1.2.5）	● IPAとAJCCBCは、オランダのNCSCと協働し、タイで重要情報インフラ保護に関する人材育成プログラムを提供（4.1.1） ● 経済産業省とIPAは、米国政府・EU政府と連携し、「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」開催（4.1.1）
12月	● 米国の地域交通局がランサムウェア攻撃を受け、鉄道の遅延等の一時的な混乱が発生（1.2.5） ● 年末から年始にかけて国内の重要インフラ企業等へ大規模なDDoS攻撃が発生（1.2.3）	● EU「サイバーレジリエンス法」発効（4.1.3） ● 国連総会にて、サイバー犯罪に関する包括的な国際条約である「国連サイバー犯罪条約」採択（4.1.1） ● EUのサイバーセキュリティ能力を強化する「サイバー連帯法」及び「改正サイバーセキュリティ法（CSA）」が成立（4.1.3）
2025年 1月	● 警察庁及びNISCは、安全保障や先端技術に係る情報窃取を目的とした攻撃キャンペーンについて、国家の関与が疑われる組織的なサイバー攻撃活動であるとして注意喚起（1.2.2）	● 「U.S. Cyber Trust Mark」運用開始（4.1.2） ● 米国大統領令14144、ソフトウェアサプライチェーンセキュリティ強化策等を指示（4.1.2） ● EU「デジタルオペレーショナルレジリエンス法」全面適用開始（4.1.3） ● 米国大統領令14179、Biden政権のAI統制施策を棄却（4.1.2）
2月	● 営業秘密にあたる研究データを外国企業に漏えいしたとして国立研究開発法人の元研究員に有罪判決（1.2.7）	● 「AIアクションサミット」開催（2.1.3） ● 「サイバー対処能力強化法案」及び「同整備法案」が閣議決定（3.1.1） ● 米国DHS、CISA等所管機関の活動縮小（4.1.2）
3月	● 地方銀行をかたる自動音声を含む電話による大規模なボイスフィッシング被害が発生（1.1.2）	● 経済産業省「セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス案（中間整理）」公開（3.1.3） ● IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」運用開始（3.3.1）

※表には、2024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

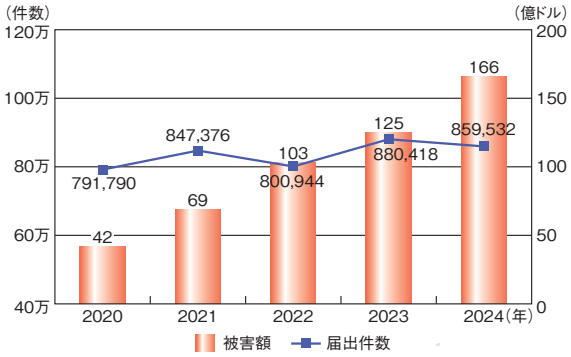
2024年は世界各地で紛争や対立が発生、再燃し、地政学的な緊張の高まりが顕著であった。これに伴い、サイバー空間では国家の関与が疑われる攻撃、世界的な大規模イベントや各国の選挙を標的とした攻撃等が確認され、サイバー空間における脅威の深刻化が実社会に及ぼす影響の大きさを浮き彫りにした。本章では、国内外で発生した主なインシデントの概要、手口、対策の動向等について解説する。

1.1 2024年度に観測されたインシデント状況

本節では、2024年度に観測された世界と日本における情報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 世界における情報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・分析している報告書等を参照し、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　サイバー犯罪の届出件数と被害額の推移(2020～2024年)
(出典)FBI「Internet Crime Report 2024」を基にIPAが作成

(1) 世界で観測された重大インシデント状況

英国国家サイバーセキュリティセンター(NCSC:National Cyber Security Centre)では、2024年にNCSCの支援を必要とするインシデント報告を430件受け、前年比約16%増となった。430件のインシデントのうち、89件は「国家的に重大なもの」であり、更にそのうち「より深刻なもの」は、前年比3倍の12件であった※1。

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)が公開している「Internet Crime Report 2024※2」によると、2024年のIC3に届け出されたサイバー犯罪の件数は2023年から減少し85万9,532件となった。このうち個人情報漏えいの届出件数については6万4,882件で2023年の届出件数から約9,000件の増加となった。推移を見ると届出件数は増減しているが、被害額は増加が続いている(図1-1-1)。

米国の防衛、安全保障、国際戦略等を専門とする非営利の政策研究機関であるCSIS(Center for Strategic and International Studies)では、2006年以降に発生した政府機関や国防・ハイテク関連企業を狙ったサイバー攻撃や、100万ドル(約1億5,000万円※3)以上の被害をもたらした重大インシデントの一覧※4を公開しており、2024年の事例件数は65件であった。記録された65件のうち、攻撃者側にロシア・中国が記された事例は34件で半数以上を占めており、そのほかにイラン、米国、ベラルーシ、ウクライナ、パキスタン等が攻撃関与国として取り上げられている。

ここではCSISの重大インシデントの一覧のうち、2024年に注目された事例を二つ紹介する。

一つ目は、国家の関与が疑われる事例として、中国の支援を受けているとされる「Salt Typhoon」と呼ばれる攻撃グループによる事例を紹介する。2024年12月、Salt Typhoonにより、9社の米国通信事業者に加え、世界中の企業数十社への侵入が行われたことが明らかとなった※5。広範なスパイ活動及び情報収集活動の一環として、顧客の通話データや政府または政治活動に関与する個人のプライベートな通信、裁判所の命令に

基づく法執行機関の要請の対象となった特定のデータを窃取したとされる※6。本件は、近年に国家の関与が疑われるサイバー攻撃が常態化している中でも、大規模な事例であり、この攻撃に関して、米国の上院特別情報委員会の委員長である Mark R. Warner 上院議員は、「我が国史上最悪の通信ハッキング」だと評している※7（「1.2.5(1)(d)通信事業者が標的となった事例」参照）。

二つ目に、サイバーセキュリティ企業 CrowdStrike Holdings, Inc.（以下、CrowdStrike 社）が引き起こした世界規模の IT 障害の事例を紹介する。2024 年 7 月、CrowdStrike 社では、自社のセキュリティ製品に関するアップデートを Windows ホストに対して公開したところ、アップデート内容に欠陥があり、公開後約 1 時間の間にオンラインだったシステムで Windows がクラッシュする障害が発生した※8。これにより世界規模の IT 障害が発生し、航空、医療、金融等、様々な業界で深刻な影響が出ることとなり、特に、航空業界では、世界中で 5,078 便が欠航となった※9。Microsoft Corporation（以下、Microsoft 社）によると、今回の障害で約 850 万台の Windows デバイスが影響を受けたという※10。このインシデントはサイバー攻撃ではないものの、世界に広く普及しているソフトウェアの問題がどれ程広範囲に及ぶかを示した。

(2) 世界的なイベントと DDoS 攻撃

2024 年は、世界各国で選挙が行われたほか、同年 7 月末にはパリ 2024 オリンピック・パラリンピック競技大会が開催される等、世界的に重要なイベントがあった年となった。Cloudflare, Inc.（以下、Cloudflare 社）の観測結果によると、2024 年 7 月にはオリンピック関連のスポンサー、パートナーの Web サイトを標的とした DDoS 攻撃のリクエストが 2 億件以上観測され、同年 8 月には 11 日間で 9,000 万件以上のリクエストが観測されたという。特に、大会期間中の 7 月 29 日には、三つのオリンピックスポンサーの Web サイトに対して 8,400 万件のリクエストがあり、大会最終日の 8 月 11 日には、フランスの交通機関の Web サイトを標的として、1 秒あたり 50 万件以上のリクエストに達する DDoS 攻撃が発生していた※11。

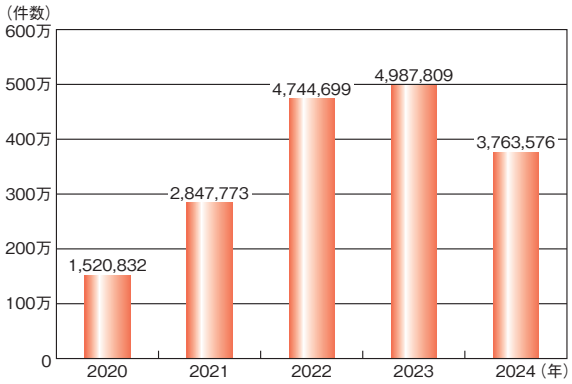
また、世界各国で行われた選挙に関しても、政治キャンペーン、政党、選挙インフラを標的とした DDoS 攻撃の増加が観測された。Cloudflare 社によると、米国では大統領選挙期間の 2024 年 11 月 1 日から 6 日の間に、60 億件を超える悪意あるリクエストがブロックされたという。11 月 5 日の投票日までに、選挙運動の一つを標的とした DDoS 攻撃が数日にわたって発生し、ピーク時には 1 秒あたり 70 万件のリクエストが発生していた。同年 6 月の欧州議会選挙においても、投票日前後に複数の政治関連 Web サイトがサイバー攻撃の標的となった。特に 6 月 5 日から投票日の 6 月 6 日にかけては、オランダの二つの政治関連 Web サイトを標的とした大規模な DDoS 攻撃があり、ピーク時には 1 秒あたり 7 万 3,000 リクエストがあった。そのほか、フランス、英国、ルーマニア、南アフリカ、ポルトガルといった国でも選挙に関連して政党を標的とした DDoS 攻撃が観測された※12。各国の選挙においては、虚偽を含んだ情報（偽・誤情報）の拡散も大きな問題となった。これについては「2.2.3 2024 年度の注目事象」を参照されたい。

そのほか、世界で観測された DDoS 攻撃の傾向としては、G-Core Labs S.A. の調査レポートによると、2024 年第 3 四半期から第 4 四半期では、2023 年の同時期と比べ DDoS 攻撃の件数は 56% 増加しており、四半期ごとの攻撃件数も 2023 年の第 1 四半期から右肩上がりとなっている※13。更に、Vercara LLC が行った調査においても、2024 年は前年比約 160% 増の 27 万 405 件の DDoS 攻撃を検出したと報告されており※14、両調査から2024 年における DDoS 攻撃の増加傾向がうかがえる。

(3) フィッシングの状況

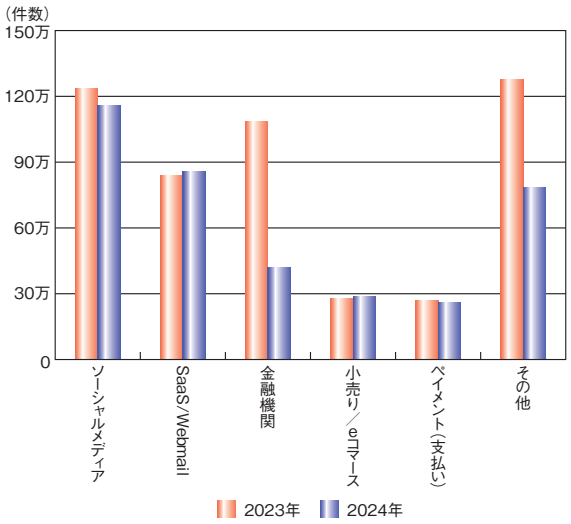
フィッシング対策の国際的な非営利団体である Anti-Phishing Working Group, Inc.（APWG）によると、2024 年に報告されたフィッシングメールに基づき特定された固有のフィッシングサイトの総数は約 376 万件であった。2018 年以降増加傾向だったが、過去最多だった 2023 年の約 499 万件から減少となった（図 1-1-2）。

偽装の対象となった業種別のフィッシングサイト件数では、2024 年は「ソーシャルメディア」が約 116 万件と最多



■図 1-1-2　世界で報告されたフィッシングサイト件数（2020～2024 年）
（出典）APWG「PHISHING ACTIVITY TRENDS REPORTS※15」を基に IPA が作成

であり、その後「SaaS ／ Webmail」が約 85 万件、「金融機関」が約 42 万件と続いている。2023 年の件数と比較すると、「金融機関」を装ったフィッシングサイトは約 66 万件の減少となった（図 1-1-3）。



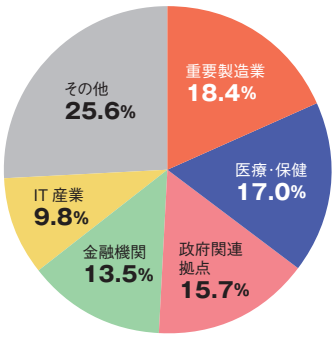
■図 1-1-3　業種別のフィッシングサイト件数（2023年と2024年の比較）
（出典）APWG「PHISHING ACTIVITY TRENDS REPORTS」を基に IPA が作成

そのほか APWG の報告書では、年間をとおして、SMS を使った「スミッシング（Smishing）」や電話等の音声案内を使った「ヴィッシング（Vishing）」（「ボイスフィッシング」ともいう）といったフィッシングの増加に言及している※16。APWG では、これらの手口の増加には、メールを使ったフィッシングは、高度なフィルタリング技術等によって困難になっている点や、SMS・電話ではフィルタリングはほとんど行われずユーザーに届くという、直接性の高い接触方法である点が影響していると推測している。

また、近年は生成 AI の登場をきっかけに、AI を活用したフィッシングの危険性についても懸念されている。SlashNext, Inc. の調査では、ChatGPT のリリース以来、悪意のあるメールが 4,151% 増加していると述べられている※17。そのほか、KnowBe4, Inc. の調査によると、フィッシングメールの 82.6% が AI を活用しているとされ、これは、前年比 53.5% 増となっており※18、AI を活用したフィッシングメールの増加がうかがえる（AI を活用したフィッシングについては「2.1.4 (2) (c) AI を用いた認知領域への攻撃」参照）。

(4) ランサムウェアの状況

「Internet Crime Report 2024」によれば、IC3 に届け出された 2024 年のランサムウェアの被害件数は 3,156 件で、2023 年の 2,825 件から約 12% 増となった。重要インフラで被害を受けた上位 5 業種については、2021 年以降 3 年連続で「医療・保健」の被害件数が最も多かったが、2024 年は「重要製造業」が最も被害を受けた業種となった（図 1-1-4）。これら上位 5 業種は 2021 年から変わらず、今後も警戒を高める必要があると言える※19。



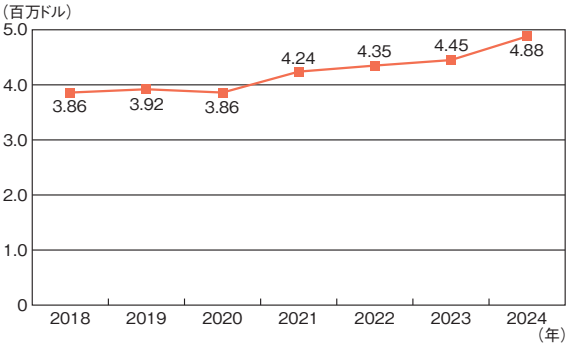
■図 1-1-4　ランサムウェア被害を受けた重要インフラの業種別構成比（2024 年、n=1,403）
（出典）FBI「Internet Crime Report 2024」を基に IPA が作成

また、Check Point Software Technologies Ltd. 傘下の Cyberint Technologies の調査報告書によると、2024 年は、世界中で 5,414 件の組織に対するランサムウェア攻撃が公表され、2023 年と比較すると 11% 増となったという※20。攻撃を受けた国を見ると、最も攻撃を受けたのが米国で 2,713 件と全体の約半数を占めており、次いで、カナダが 283 件、英国が 268 件と続き、上位 10 ヵ国中には欧州の国が 5 ヵ国含まれている。活動のあったランサムウェアの攻撃グループは、2023 年の 68 グループから 2024 年は 95 グループに増えており、2024 年 2 月から活動を開始した「RansomHub」という攻撃グループによる被害が 531 件と最も多く、攻撃全体の 9.8% を占めた（国際的なランサムウェアの事例及び攻撃グループについては「1.2.5 (1) 重要インフラを狙った攻撃の発生状況と動向」参照）。また、近年は同攻撃グループや「LockBit 3.0」といった攻撃グループで、ランサムウェアを RaaS（Ransomware as a Service）の運営者が開発し、サービスとして攻撃者が利用するビジネスモデルが採用されており、RaaS はランサムウェアの世界的な蔓延と持続化に大きな影響を及ぼしているという（ランサムウェア攻撃については「1.2.1 ランサムウェア攻撃」参照）。

(5) 情報漏えいインシデントの状況

日本アイ・ビー・エム株式会社（以下、IBM 社）の「データ侵害のコストに関する調査 2024 年※21」によれば、データ侵害を受けた組織において被害者への対応や事業機会損失等により生じるインシデント 1 件あたりの総被害コ

ストは世界平均で 488 万ドル（約 7 億 3,200 万円）であり、前年比約 9.7% 増となった（図 1-1-5）。調査対象となった 16 の国または地域別で見ると、米国が 936 万ドル（約 14 億 400 万円）と最も高く、次いで中東が 875 万ドル（約 13 億 1,250 万円）、600 万ドル（約 9 億円）以下でベネルクス三国（ベルギー、オランダ、ルクセンブルク）、ドイツ、イタリアと続いている。また、業種別で見ると、2024 年は医療が 977 万ドル（約 14 億 6,550 万円）で、2011 年以降連続でデータ侵害のコストが最も大きい業界となっており、次点の金融業 608 万ドル（約 9 億 1,200 万円）と 300 万ドル（約 4 億 5,000 万円）以上も離れている。



■図 1-1-5　データ侵害の世界平均コスト（2018 ～ 2024 年）
（出典）IBM 社「データ侵害のコストに関する調査 2024 年」を基に IPA が作成

以下では、2024 年に発生した情報漏えいインシデントのうち、大規模な漏えい事例を三つ示す。

- 身元調査事業者における情報漏えい

  2024 年 8 月、米国の Jerico Pictures, Inc. の子会社であり、身元調査事業を行っている National Public Data（以下、NPD 社）は、2023 年 12 月に悪意ある第三者による不正アクセスを受け、その後 2024 年 4 月から同年の夏にかけて、個人情報や社会保障番号等のデータが漏えいした可能性があることを公表した※22。漏えいしたデータは 29 億行ものレコードであり、その中には米国、カナダ、英国の国民に関する氏名、住所、電話番号等のデータ、2 億 7,200 万件の米国社会保障番号、1 億 3,700 万件のメールアドレスが含まれていたことが判明した。2024 年 4 月には、「USDoD」というサイバー犯罪グループによって、ダークウェブ上で窃取されたデータの販売が開始され、その後、同年の夏にも、何者かによって窃取された情報がダークウェブ上で販売されていた※23。当件を受けて NPD 社は、漏えい被害を受けた人々から複数の集団訴訟を提起され、更に同年 10 月には侵害への対応に伴う経済的負担により破産申請を行う事態となった※24。

- マルチクラウドデータウェアハウスプラットフォームに対する侵害

  2024 年 6 月、Google LLC は、Snowflake Inc. が運営するマルチクラウドデータウェアハウスプラットフォームである Snowflake を利用している複数の組織を標的としたデータ侵害が、同年 4 月以降に行われていたことを公表した※25。同社の調査によると、今回の Snowflake の顧客データベースを標的としたデータ窃盗の活動は、脅威アクター「UNC5537」によるものだという。今回の一連の事例では Snowflake 自体は侵害されていないものの、Snowflake を使用している 165 の組織が潜在的に危険に晒されている可能性があるとされた。UNC5537 は、本事例以前に情報窃取型マルウェアによって漏えいしていた Snowflake の顧客認証情報を用いて、多要素認証が有効になっていない Snowflake アカウントに不正アクセスを行っており、実際に Snowflake を介した大規模なデータ侵害も発生している。同年 4 月には通信大手の AT&T Inc. で 1 億 900 万人の顧客の通話等のデータが漏えいする事例が発生しており※26、同年 5 月には、大手銀行である Santander Bank, N. A. から 3,000 万件の顧客情報が漏えいしたと報道された※27。また同年 5 月に Ticketmaster LLC が運営するチケット販売プラットフォームである Ticketmaster の顧客記録が最大 5 億 6,000 万件漏えいしたと報道された※28。この一連の侵害によって数億単位の人が影響を受けることとなった。Snowflake Inc. では、この一連の侵害を受けて、同年 7 月には、全顧客にアカウントログイン時の多要素認証の使用を促すため、セキュリティポリシー及び多要素認証の設定誘導機能の導入を行った※29。

- 英国国防省の給与計算システムにおける情報漏えい

  2024 年 5 月、請負業者が運営する英国国防省の給与計算システムに対して大規模なサイバー攻撃があり、現役軍人、予備役軍人、退役軍人約 27 万人の氏名や銀行口座情報等の個人データが漏えいした※30。Grant Shapps 国防相は、今回の攻撃は悪意ある攻撃者によって仕組まれた疑いがあり、国家の関与の可能性についても排除できないと述べた※31。政府は公式には特定の国による攻撃とは発表していないものの、複数のメディアでは中国の関与を疑う報道が行われている。なお、中国側ではこの件に関して関与を否定している※32。

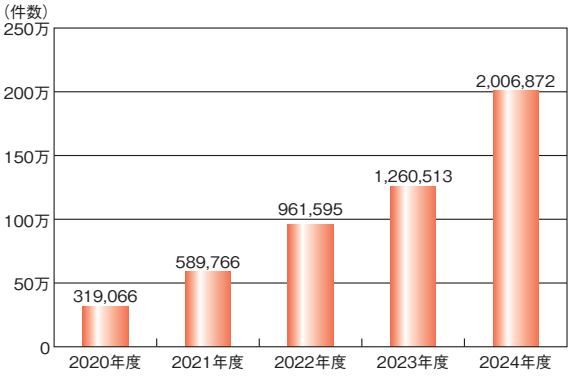
1.1.2 国内における情報セキュリティインシデント状況

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※33」
- 警察庁：「令和6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※34」「令和5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※35」「令和4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※36」「令和3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※37」（以下、2021～2024年の警察庁資料）
- 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※38」

(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2024年度のフィッシング報告件数は200万6,872件で、2023年度（126万513件）から59.2%増となり、初めて200万件を超える結果となった（図1-1-6）。

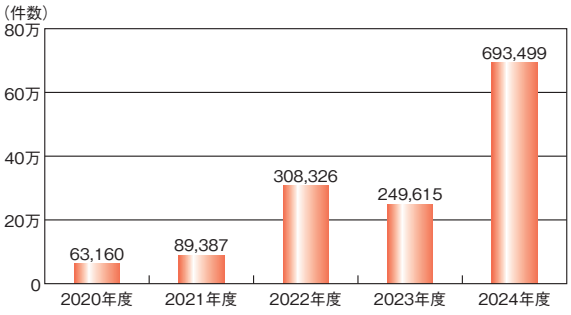


■図1-1-6　フィッシング報告件数（2020～2024年度）
（出典）フィッシング対策協議会「月次報告書」（2020年4月～2025年3月）を基にIPAが作成

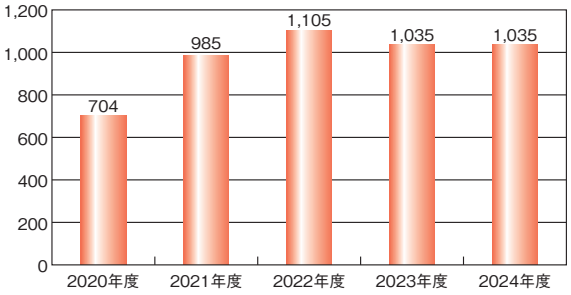
フィッシングサイトのURL件数では、2022年度をピークに2023年度は減少傾向だったものの、2024年度は再度69万3,499件と大幅な増加に転じた（図1-1-7）。

フィッシングに悪用されたブランド数を図1-1-8に示す。2024年度は1,035件となり、3年連続で1,000ブランドを超え、フィッシングにおいて多くのブランドが詐称されていることがうかがえる。

報告件数の多かったブランドを見ると、「Amazon」をかたるフィッシングは1年間のうち10ヵ月で最多となっており、そのほかクレジットカード会社をかたるフィッシングも多数報告されている。1ヵ月に1,000件以上の大量の報告を受けたブランドについては、2024年度は月平均約



■図1-1-7　フィッシングサイトのURL件数（2020～2024年度）
（出典）フィッシング対策協議会「月次報告書」（2020年4月～2025年3月）を基にIPAが作成



■図1-1-8　悪用されたブランド数（2020～2024年度）
（出典）フィッシング対策協議会「月次報告書」（2020年4月～2025年3月）を基にIPAが作成

20ブランドで、いずれの月でも報告件数全体の約9割を占める結果となった。

フィッシング対策協議会からは、2024年8月にQRコードから誘導するフィッシングについて緊急情報が発出された※39。

また警察庁から2024年12月には、金融機関をかたり法人口座を狙うボイスフィッシングによる不正送金被害に関して注意喚起が行われた※40。2025年3月には、実際に山形銀行をかたる自動音声を含む電話による大規模なボイスフィッシング被害が発生している※41。

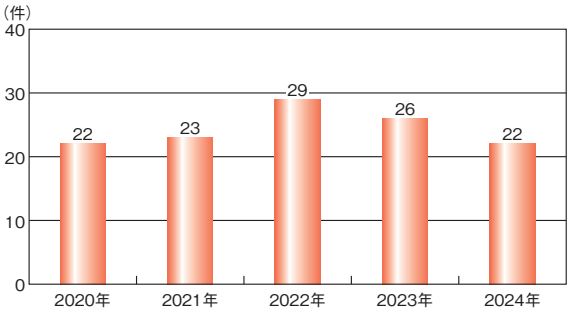
一般社団法人JPCERTコーディネーションセンター（JPCERT/CC：Japan Computer Emergency Response Team Coordination Center）の「フィッシング詐欺の現状※42」では、フィッシング犯罪の特徴の一つとして「PhaaS（Phishing as a Service）」という、サービスとしてフィッシング攻撃を提供するビジネスモデルが存在していることが挙げられており、このような攻撃側の分業化も背景となり、攻撃者が特定しにくくなっていることが指摘されている。

フィッシング被害に遭わないためにも、手口等の最新情報を知ることや、メール等に記載されているURL、QRコード、知らない番号からの着信にはより慎重になることが求められる（メールを悪用した手口と対策の詳細については「1.2.8(3)メールを悪用した手口」参照）。

(2) 情報漏えいと内部不正による被害

株式会社東京商工リサーチが2025年1月に公開した「2024年『上場企業の個人情報漏えい・紛失事故』調査※43」によると、2024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189件だった。漏えいした個人情報は1,586万5,611人分であり、大規模な漏えい事故が相次いだ2023年に比べ38.8%に減少した。

内部不正と関連するものとして、「不正持ち出し・盗難」による情報漏えいと、不正競争防止法違反（営業秘密の領得）が挙げられる。前者の「不正持ち出し・盗難」が原因で個人情報が漏えい・紛失した件数は、同調査では2024年は14件となり、2023年の24件※44より減少した。後者に関しては、警察庁によれば、2024年の営業秘密侵害事犯の検挙事件数は22件で、2022年の29件をピークに減少傾向にある（図1-1-9）。一方、営業秘密侵害事犯に関する相談受理件数は2023年の78件を上回り、2024年は79件と過去最多となった※45（内部不正については「1.2.7 内部不正による情報漏えい」参照）。

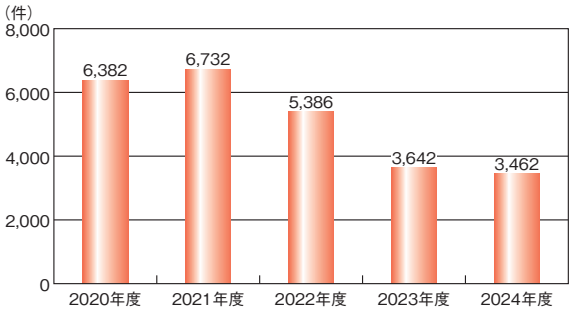


■図1-1-9　営業秘密侵害の検挙事件数（2020～2024年）
（出典）警察庁「令和6年における生活経済事犯の検挙状況等について※45」を基にIPAが編集

(3) 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、月次の観測レポートとして、IIJ社のサービスから検出されたDDoS攻撃の観測情報を取りまとめている。同レポートによると、2024年度は合計3,462件のDDoS攻撃を検出しており、年度別の検出件数で見ると2021年度を境に減少傾向にある（図1-1-10）。

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）



■図1-1-10　DDoS攻撃の検出件数（2020～2024年）
（出典）IIJ社「wizSafe Security Signal観測レポート※46」を基にIPAが作成

攻撃を定点観測している。CYNEXが公開した「NICTER観測レポート2024※47」によると、2024年に観測された日本宛てのDRDoS攻撃は累計約17万件で、2022年の約61万件、2023年の約896万件より減少している。

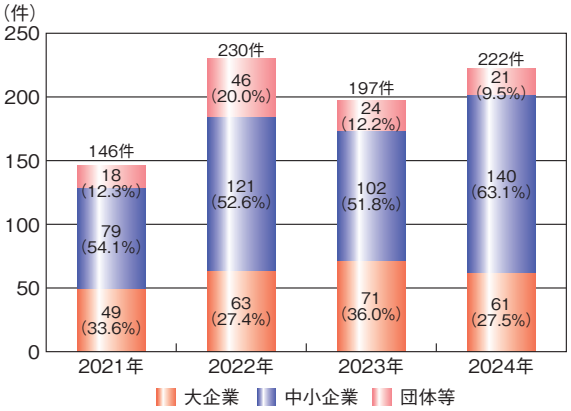
DDoS攻撃の検出数には増加が見られないものの、2024年12月末から2025年年始にかけては、日本国内において航空事業者や金融機関を狙ったDDoS攻撃が相次ぎ、多数の被害が発生した。このことを受けて、2025年2月には、内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）（現、国家サイバー統括室（NCO：National Cybersecurity Office））から、DDoS攻撃に関する注意喚起が発出された※48。DDoS攻撃への対策については、平時の対策、被害に遭った時の対策のほかに、DDoS攻撃への悪用が懸念されるネットワーク機器、IoT機器に関する対策についても講じる必要がある（事例の詳細及び対策については「1.2.3 DDoS攻撃」参照）。

(4) ランサムウェアによる被害

2024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222件で前年比12.7%増となり、依然として被害が多いことがうかがえる（次ページ図1-1-11）。件数の内訳を企業・団体等の規模別で見ると、2024年は中小企業の被害件数が増加していることが分かる。

2024年の被害件数を業種別で見ると、「製造業」の割合が最も大きく29.3%（65件）で、次いで「卸売・小売業」が19.4%（43件）、「サービス業」が14.9%（33件）と続く。それ以降は「建設業」「運輸・郵便業」「情報通信業」「医療・福祉」がそれぞれ10%未満で続いている。「製造業」は2021年に調査を開始して以降4年連続で被害件数が最も多いという結果となったが、業種を問わず被害が発生している傾向は変わっていない。

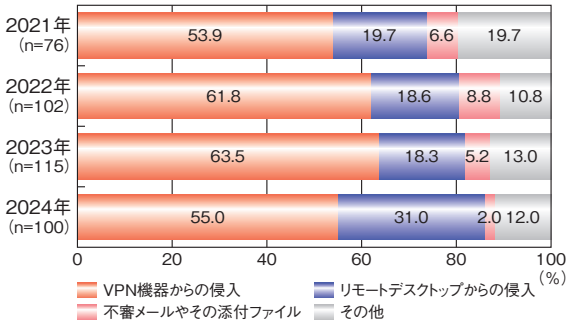
また、2024年に被害の報告があった222件のうち手



■図 1-1-11　国内のランサムウェアによる被害件数（2021 ～ 2024 年）
（出典）2021 ～ 2024 年の警察庁資料を基に IPA が作成

口を確認できたのは 134 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 82.8%（111 件）を占めた。2021 年に調査を開始して以降 4 年連続で半数以上の割合を占める手口となっている。一方、最近の手口として、222 件とは別に、データの暗号化はせずに窃盗したデータに対して対価を要求する「ノーウェアランサム」の被害が 22 件確認されたという（ノーウェアランサムについては「1.2.1 (1) (d) 暗号化を伴わない攻撃手口」参照）。

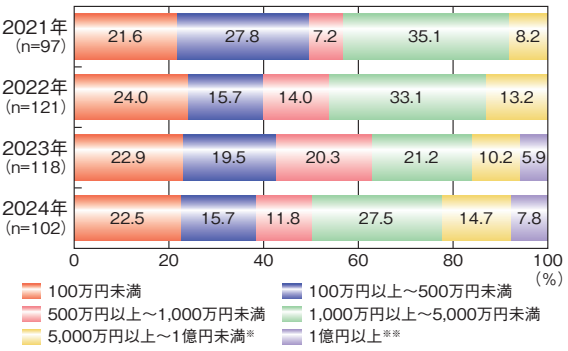
2024 年のランサムウェアの感染経路としては、有効回答 100 件のうち、「VPN 機器からの侵入」が 55.0%（55 件）、「リモートデスクトップからの侵入」が 31.0%（31 件）を占めており、2022 年に引き続きこれらテレワーク等で利用される機器からの侵入が 8 割を超えている（図 1-1-12）。



■図 1-1-12　ランサムウェアの感染経路（2021 ～ 2024 年）
（出典）2021 ～ 2024 年の警察庁資料を基に 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 87 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 41 件（47.1%）と半数未満で、未適用のセキュリティパッチがあったのは 46 件であった。この結果から、基本的なセキュリティ対策の実施が重要であることがうかがえる。

調査・復旧に要した費用の割合では、2024 年は「5,000 万円以上」の割合が 22.5% と、2021 年に調査を開始して以降最も大きくなった。また、2023 年から「1 億円以上」の項目が設けられており 2024 年は 7.8%（8 件）が該当した（図 1-1-13）。



※2021～2022年では「5,000万以上」
※※2023年から設けられた選択肢

■図 1-1-13　調査・復旧に要した費用（2021 ～ 2024 年）
（出典）2021 ～ 2024 年の警察庁資料を基に IPA が作成

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 136 件のうち、バックアップを取得していたのは 122 件（89.7%）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 110 件のうち、29 件（26.4%）にとどまった。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 74 件のうち、「バックアップも暗号化されたため」が 54 件（73.0%）、「運用の不備」が 14 件（18.9%）となっている。

2024 年の被害報告（有効回答 140 件）のうち、すべての業務が停止に追い込まれたのは 14 件（10.0%）であり、一部の業務に影響のあった割合と合わせると 91.4% にもなる。ランサムウェアによる被害は 2024 年も高止まりしており、今後もランサムウェアに対する対策の強化が求められる（「1.2.1 ランサムウェア攻撃」参照）。

(5) 中小企業におけるインシデント発生状況

2025 年に IPA が実施した「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」によると、2023 年度にサイバーインシデントが発生した、もしくは発生があった可能性が高い経験をした中小企業は、975 件（23.3%）であった。具体的な被害としては、データの破壊が 348 件（35.7%）、個人情報の漏えいが 342 件（35.1%）と多く、次いでウイルスメール等の発信が 210 件（21.5%）、業務情報（営業秘密を除く）の漏えいが 208 件（21.3%）となった。更に、サイバーインシデントが発生もしくは発生があった可能性が高い経験をした中小企業のうち、約 7 割がサイバーインシデントにより取引先（サプ

ライチェーン）に影響があったと回答している。その内容としてはサービスの障害や遅延、停止による逸失利益が352件（36.1%）、個人顧客への賠償や法人取引先への補償負担が316件（32.4%）とされている。

しかしながら、サイバーインシデントの経験を踏まえて情報セキュリティ対策を強化したと回答した企業は1割強にとどまり、8割以上の企業は対策を強化していないと回答している。この結果は、インシデントの経験が生かされず、一時的な対応にとどまっている実態を示している。

以上の調査結果は、中小企業においてもサイバーインシデントは無関係な問題ではなく、被害が取引先を含むサプライチェーン全体に広がるおそれがあることを示している。従って、サプライチェーン上のパートナーがそれぞれ対策を講じるだけでなく、パートナーが連携して対策を検討・実施することが望ましい（中小企業のセキュリティ対策強化の取り組みについては「3.4.1 組織におけるサイバーセキュリティの取り組みと支援策」参照）。

COLUMN

トラブルを招かないためのデータマネジメント ～データ品質管理の勧め～

安定的かつ高い信頼性を保ってシステムやサービスを運用するためには、ハードウェアやソフトウェアの障害対策やサイバー攻撃対策等が重視され、実施されてきました。しかし、近年はデータを大量に活用するシステムが増えたことで、データの信頼性の確保がセキュリティの確保と同様に重要な課題となっています。更に、最近の AI の台頭はその傾向を加速させています。データセキュリティの分野では、悪意ある変更や挿入が行われるデータポイズニングや、データを人質に取るランサムウェアの脅威が注目されています。これらの脅威に対抗する必要があるのはもちろんですが、サイバー攻撃を受けていなくても、データ欠損等のデータ品質の問題によってトラブルが発生するケースが増えています。

IPA の「2024 年度ソフトウェア動向調査[i]」によれば、「データセキュリティ管理」の施策については半数以上の企業で整備や検討が進んでいますが、「データガバナンス」や「データ品質管理」については整備がまだ進んでおらず、整備予定がない企業も 2 割を超えています。

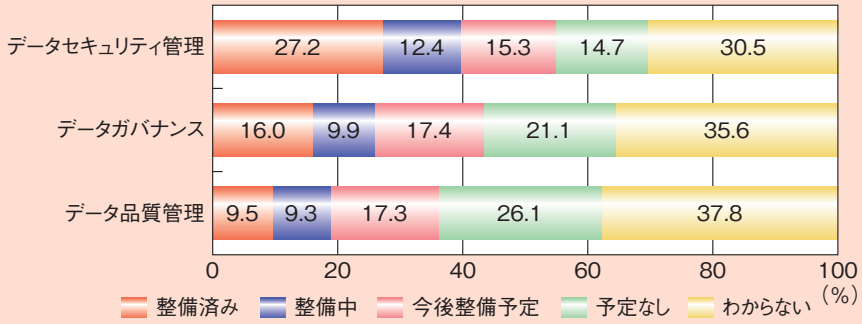


図　データマネジメントの状況（抜粋、n=798）

データマネジメントの中でも、データ品質管理は特に重要な取り組みであり、「データのライフサイクル・プロセスの視点」「データ特性の視点（正確性・完全性等）」及び「データガバナンスの視点（体制や計画等）」で管理する必要があります。これらを体系的に行うための手引きとして、AI セーフティ・インスティテュートが「データ品質マネジメントガイドブック[ii]」を公開しています。データを扱う各場面で必要とされる活動やチェックポイントが整理されており、AI を使用しない一般的なシステムでも応用できる内容になっています。

更に、データ品質管理では、データの信頼性という観点も欠かせません。保存や転送の過程で改ざんされていないことはもちろん、データそのものがそもそも高品質であり、そのデータを誰が収集・作成したのかが分からなければ安心して利用することはできません。このため、データの来歴情報（プロビナンス情報）の管理がますます重要になってきています。

i　IPA：「2024 年度ソフトウェア動向調査」調査結果データの公開と分析レポートの募集　https://www.ipa.go.jp/digital/software-survey/software-engineering/result-software2024.html〔2025/7/10 確認〕
ii　https://aisi.go.jp/effort/effort_information/250331_2/〔2025/7/10 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、2024 年度に確認されたインシデントの発生状況と、具体的な事例について述べる。また、脆弱性やサイバー攻撃の動向、その対策を解説する。

1.2.1 ランサムウェア攻撃

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。本項では、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復旧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を「ランサムウェア攻撃」と呼ぶ。

従来のランサムウェア攻撃は、メールに添付されたランサムウェアを開かせる、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ランサムウェアに感染させようとするばらまき型の攻撃が主流であった。しかし、近年のランサムウェア攻撃は、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、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ウェア攻撃を「侵入型ランサムウェア攻撃」と呼ぶ。

このような侵入型ランサムウェア攻撃では、データの復旧と引き換えに身代金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、更なる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※49。

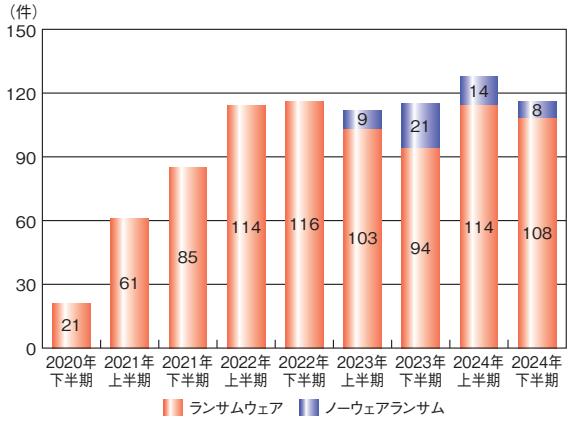
なお、昨今ではデータの暗号化を伴わない手口が確認されている。警察庁は、データを暗号化する（ランサムウェアを用いる）ことなくデータを窃取し対価を要求する手口を「ノーウェアランサム」と名付けている※50。

(1) ランサムウェア攻撃の傾向

2024 年度における日本国内のランサムウェア攻撃の傾向について説明する。

(a) 被害件数

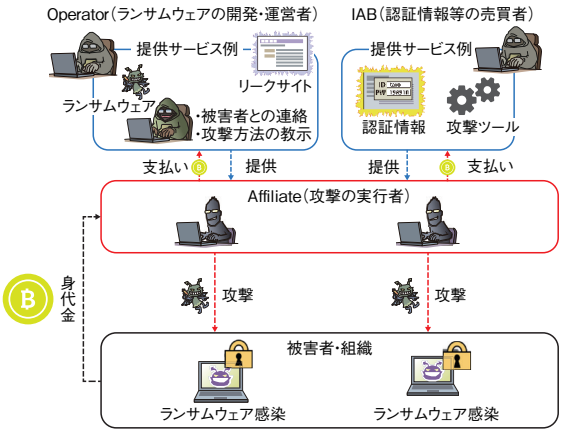
警察庁が公表した「令和 6 年におけるサイバー空間をめぐる脅威の情勢等について」（以下、警察庁資料）によると、企業・団体等におけるランサムウェア被害の報告件数は、2024 年上期が 114 件、下期が 108 件で、2022 年上期以降は継続して高い水準で推移している（図 1-2-1）。また、ノーウェアランサム被害の報告件数は、2024 年上期が 14 件、下期が 8 件である。ランサムウェア被害の報告件数と比較すると少ないが、ノーウェアランサムの統計が開始された 2023 年以降継続して被害が発生している。



■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 6 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、攻撃をより容易に行えるようになったことが影響していると考えられる。例えば、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等を提供し、攻撃の実行者が標的の組織に攻撃を仕掛け、身代金を窃取する（次ページ図

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っている。



■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※51」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。また、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、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いる。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の被害を発生させるという事例もある。なお、海外子会社等のサプライチェーンに属する組織にランサムウェア攻撃が行われた場合、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るおそれがある※52。

(c)ネットワークへの侵入手口

警察庁資料によると、2024 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 機器やリモートデスクトップからの侵入が多く、被害を受けた企業・団体から得られた有効回答中の 86% 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続いている。

(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せず、攻撃者からの脅迫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の一つは、データの暗号化を行わなくとも、データを持ち出すことができれば攻撃が成功するため、効率的に攻撃を仕掛けられることである※53。また、もう一つの理由としては、2020 年ごろから各国で犯罪組織であるランサムウェア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がある。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ない可能性があるため、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うおそれがある。また、攻撃者としても注目を浴びるほど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、攻撃者がリスクヘッジを行うための手段として浸透しつつあるという意見もある※54。

(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※55、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※56、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※56、等があるとされる。また、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、攻撃国に国家支援団体による攻撃ではないと否認する機会を与えるおそれがあることも危惧されている※57。なお、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、調査対象が暗号化されてしまうため、攻撃者の目的の把握や被害後の調査が困難となるおそれがある。

(2)ランサムウェア攻撃の被害事例

2024 年度に公表された国内における侵入型ランサムウェア攻撃の主な被害事例を紹介する。

(a)総合エンターテインメント企業における被害事例

株式会社 KADOKAWA（以下、KADOKAWA）は、2024 年 6 月 9 日、前日の 6 月 8 日未明より複数の Web サイトが利用できない事象が発生し、サイバー攻撃を受けた可能性が高いと公表した※58。その後、同年 6 月 14 日、第 2 報として動画共有サービス「ニコニコ」を中心としたサービス群を標的として、データセンター内のサー

バーがランサムウェアの攻撃を受けたことを公表した※59。事業及び業務への影響として、国内における紙書籍の受注システムの停止、「ニコニコ動画」等のサービス全般の停止及びオンラインショップの商品の受注不能や出荷の一部遅延等が発生した。また同社は、同年8月5日、情報漏えい対象や原因、対策等をまとめた調査結果を公表した※60。

この調査結果によると、ランサムウェア攻撃により、株式会社ドワンゴの従業員等の個人情報（氏名、生年月日、住所及び口座情報等）の社内情報に加え、社外情報である、一部取引先の個人情報（氏名、生年月日、住所及び口座情報等）及びN中等部、N高等学校、S高等学校の在校生及び卒業生等の個人情報（氏名、生年月日、住所及び学歴等）を含む、合計25万4,241人分の情報漏えいが確認された。また、株式会社ドワンゴの一部取引先との契約書及び法務関連の社内文書等の機微情報の漏えいも確認されている。なお、「ニコニコ」等に登録された顧客のクレジットカード情報については、社内でデータを保有していないとし、情報漏えいは起こらない仕組みになっているという。

ランサムウェアに感染した経路及び方法については、不明としているが、フィッシング等の攻撃により従業員のアカウント情報が窃取されてしまったことが根本原因であると推測されている。その窃取されたアカウント情報を悪用され、社内ネットワークに侵入、ランサムウェアに感染させられたという。

一方、同社がランサムウェア被害への対応を行っている中で、一部メディアによると、同年6月27日、「BlackSuit」を名乗る攻撃グループがダークウェブ上でKADOKAWAグループから1.5TBのデータを窃取したとの声明を発表し、同年7月1日までに身代金を支払わなければすべてのデータを公開すると予告したという（「二重の脅迫」）※61。その後、同年7月1日夜から2日未明、ダークウェブ上で、窃取した情報のダウンロード先と見られるリンクが公開され、ダウンロードできる状態となった。なお、このとき公開された情報は窃取された情報全体の50%程度とされている※62。

攻撃グループにより窃取された情報がダークウェブ上で公開された後、匿名掲示板やSNS等で、その情報を拡散する行為が確認された※63。それを受けて、KADOKAWA、株式会社ドワンゴ及び学校法人角川ドワンゴ学園の横断対策チームは、SNS、匿名掲示板、まとめサイトを巡回監視し、悪質な情報拡散行為の特定や削除要請、情報開示請求等を進め、それらの悪質な情報拡散者に対しての刑事告訴も含めた法的措置に向けた作業を進行中であるとしている※60。

なお、ランサムウェアに感染後、同社は順次関連するサービスの復旧を行っている。主なサービスの復旧状況は表1-2-1のとおりで、KADOKAWAが提供するサービスを共通で利用できるIDである「KADOKAWA-ID」について、復旧まで約6ヵ月の期間を要した。また、「ニコニコ」の「プレミアム会員」等のサービスについて、利用できなかった期間に対して返金対応等の補償を実施している※64。

復旧日	復旧したサービス
2024年6月10日	N予備校（ニコニコアカウント連携以外）※65
8月5日	ニコニコ生放送（公式番組）※66
8月5日	N予備校（ニコニコアカウント連携）※65
8月9日	KADOKAWA オフィシャルサイト※67
10月10日	PC版ニコニコ動画※68
10月17日	スマホブラウザ版ニコニコ動画※69
11月20日	KADOKAWA アプリ※70
12月11日	KADOKAWA-ID※71

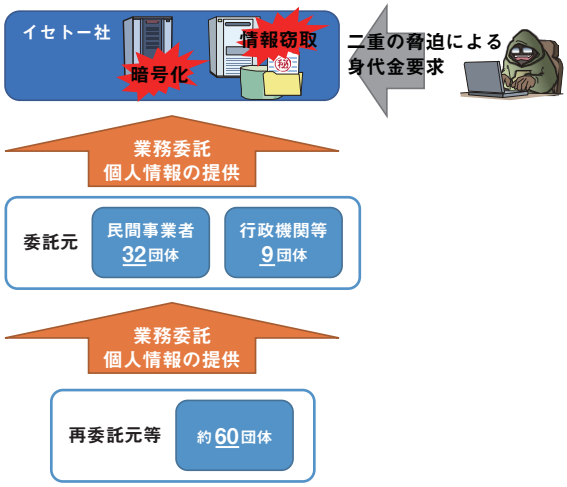
■表1-2-1　ランサムウェア被害後の主なサービスの復旧状況
（出典）公表情報を基にIPAが作成

(b) 印刷企業における被害事例

株式会社イセトー（以下、イセトー社）は、2024年5月26日にランサムウェア攻撃を受け、複数のサーバーやパソコンが暗号化される被害が発生していると同年5月29日に公表した※72。更に同年7月3日の続報においては、攻撃者グループのリークサイト（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）にて、同社から窃取したと思われる情報が公開されていたことを公表した。外部専門家が調査を行った結果、公開された情報は同社から流出したものであること、また、流出した情報の中には一部の取引先の顧客の個人情報が含まれていることが判明したと報告している※73。なお、同年7月3日時点で、公開されたファイルは消失し、ダウンロードできない状態であることが確認されている。

同社は通知書等の印刷と発送の業務を請け負っており、委託元の行政機関や企業等から個人情報を預かっていた。本事案では、委託元である各行政機関や企業等が、委託先で発生した事案の影響により情報漏えいが発生したことを公表している※74。なお、個人情報保護委員会から公開された報告書によると、今回のイセトー社へのランサムウェア攻撃により、委託元の民間事

業者 32 団体、行政機関等 9 団体、及び委託元に委託していた再委託元等約 60 団体が影響を受けたという（図 1-2-3）。また、漏えいした本人数は、民間事業者委託分が約 250 万人、行政機関等委託分が約 56.6 万人とされる※75。



■図 1-2-3　イセトー社へのランサムウェア攻撃で情報漏えいが発生した団体数
（出典）個人情報保護委員会「株式会社イセトーに対する個人情報の保護に関する法律に基づく行政上の対応について※75」を基に IPA が作成

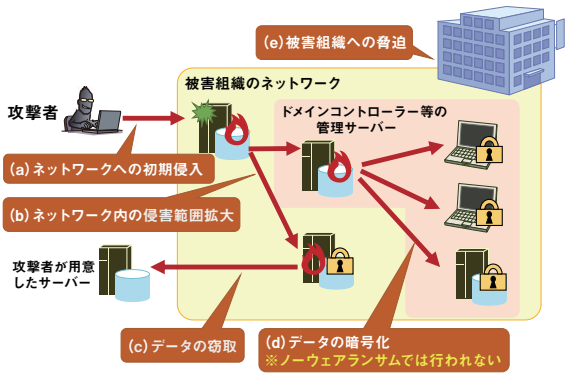
同社の報告によると、本事案は、VPN 機器へ不正アクセスされ、同社ネットワークに侵入されたことが原因としている。情報漏えいの原因は、本来個人情報を取り扱ってはならないサーバーに作業を効率化するために当該情報を保管し、業務終了後に削除できていなかったためとしている。本事案を受け同社では、VPN 機器を使用しない体制とし、認証強化を図るとしている。また、データの取り扱いについてはルールを定め、ルールが遵守されるよう監査を徹底するとしている※76。

影響は更に拡大し、本事案を受け、ISMS 審査機関である BSI グループジャパン株式会社の特別審査が行われ、イセトー社は取得済みの情報セキュリティマネジメントシステム認証（ISO 27001 認証）及びクラウドセキュリティ認証（ISO 27017 認証）を一時停止する旨の通知を受けている※77。更に、一般財団法人日本情報経済社会推進協会（JIPDEC）より、プライバシーマーク付与を一時停止する旨の通知を受けたという※78。なお、後に ISO 27001 認証及び ISO 27017 認証の一時停止は解除されている※79。

本事案は「8Base」と呼ばれる攻撃グループによるものと判明している※80。同グループは、侵入したターゲットのデータを暗号化するとともに、リークサイト上でデータを公開し、身代金を要求する「二重の脅迫」を行うとされている。また、同グループによる、他の日本企業への攻撃も確認されているという※81。2025 年 2 月 12 日、警察庁は欧州刑事警察機構（Europol：European Union Agency for Law Enforcement Cooperation）が、同グループのメンバー 4 名の逮捕とインフラのテイクダウンを行った旨のプレスリリースを公表している※82。

(3) 侵入型ランサムウェア攻撃の手口

ここでは、侵入型ランサムウェア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）。



■図 1-2-4　侵入型ランサムウェア攻撃の手口のイメージ

(a) ネットワークへの初期侵入

侵入型ランサムウェア攻撃は、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、設定不備、強度の弱いパスワードや過去に漏えいした認証情報等を悪用し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 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、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が初期侵入に使われることもある。

(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の把握や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できるドメインコント

ローラーが侵害されると、管理下のすべてのコンピューターに侵害範囲が拡大するおそれがある。更に、近年のランサムウェアには仮想化基盤（VMware や Hyper-V）を攻撃する機能を持つものが複数発見されており、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のサーバーやクラウドストレージへアップロードする。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

侵入型ランサムウェア攻撃では、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、身代金の取得を狙うとともに、事業継続に関わる重要なシステムの停止も行う。バックアップデータによる復旧を妨害するため、バックアップデータも狙って暗号化する可能性がある。

なお、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、システムの停止が発生しないだけでなく、EDR（Endpoint Detection and Response）等による攻撃検知がされにくくなり※54、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を復旧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ことがある。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が挙げられる。攻撃者との身代金の交渉には電子メールや特定のチャットサイト等が使用され、時には直接電話がかかってくるケースもあるという。

更に、被害組織が提供するサービスへの DDoS 攻撃を仕掛ける「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) 侵入型ランサムウェア攻撃への対策

ここでは、侵入型ランサムウェア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) インシデント対応力の強化」の四つに分けて説明する。なお、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。また、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）が公開している「#StopRansomware Guide※83」も併せて参考にしていただきたい。なお、「三重の脅迫」の際に行われる DDoS 攻撃への対策については「1.2.3 (3) DDoS 攻撃への対策」にて解説しているため、そちらを参照いただきたい。

(a) ネットワーク侵入への対策

侵入型ランサムウェア攻撃は、攻撃者が企業・組織内のネットワークへ侵入するところから始まるため、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ウェア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をできる限り少なくすること、不要なプロトコルやサービスを制限することで、攻撃対象となる領域を最小化することが重要である。特に、製品を初期設定のままにしていること等により、公開すべきではない情報が、意図せず外部からアクセス可能な状態になっていないかも確認いただきたい。

  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、VPN ゲートウェイを含む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。脆弱性情報は様々な組織や機関から公表されているため、そこから情報を日々収集することで、リスクの早期発見や迅速な対応につなげることができる。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していても、既に攻撃者によってアップデート前に脆弱

性が悪用され、設定情報や認証情報等が窃取されている可能性があるため、脆弱性を悪用した攻撃のIoC（Indicator of Compromise：侵害指標）等の情報を収集し、攻撃された痕跡がないか、過去のログを含め調査することが求められる。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整備しておくことも重要といえる。

- 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し、認証の試行回数に制限を設け、多要素認証等、強固な認証方式を使用することにより、認証を強化することが重要である。また、特定のIPアドレスからのアクセスを許可または拒否する等、適切なアクセス制御も有効な対策である。なお、インシデント発生時に備え、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。

- ネットワーク接続点のセキュリティ強化
  組織内の複数拠点や他組織とのネットワーク間接続において、十分なセキュリティ対策が実施されていないネットワークがあると、攻撃者によって、脆弱な箇所からまずそのネットワークに侵入される。そして、ネットワーク間接続を経由して、他のネットワークに存在する自拠点の中枢が侵害されるおそれがある。そのため、組織内の拠点間、海外拠点との接続、他組織とのネットワーク接続点において、アクセス制限や不正通信の監視等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
  ネットワーク接続点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[※84]、攻撃対象領域の縮小による攻撃リスクの低減、組織内に侵入後の侵害範囲の拡大（「水平展開（ラテラルムーブメント）」）への対策として有効である。

被害拡大防止に有効なその他のセキュリティ対策を以下に示す。

- 必要最小限の権限付与
- パスワードの管理
- ドメインコントローラーのセキュリティ強化
- セキュリティソフトの導入
- 正規プログラム・ツールの悪用への対策
- データの窃取と公開への対策

各項目の詳細は、「情報セキュリティ白書2023[※85]」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、そちらを参照いただきたい。

(c) 暗号化によるシステム停止への対策

侵入型ランサムウェア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
  バックアップからの復旧に備え、バックアップを適切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システムに接続されている場合、バックアップ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が重要である。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配置することが望ましい。それに加えて、バックアップからの復旧が可能なことを確認しておくことが重要である。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、組織のネットワークから切り離したクラウド上に保存する方法も有効である。
  注意事項として、クラウドサービスを利用する場合には、ユーザーデータのバックアップ機能の有無や責任

分界点を確認していただきたい。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、ランサムウェア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。

- 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ている場合がある※86。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、ファイルを復号できる可能性がある。

(d) インシデント対応力の強化

侵入型ランサムウェア攻撃によるインシデントでは、業務の停止や顧客・取引先の情報漏えい等が発生し、自組織内に閉じたインシデントで終わらない傾向がある。そのため、日頃から、経営層を含む顧客や取引先、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作りが必要である。

- ランサムウェア攻撃を想定した BCP の策定
  自然災害の発生を想定した事業継続計画（BCP：Business Continuity Plan）を策定している企業・組織であっても、侵入型ランサムウェア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業務継続に大きな影響を与えるため、BCP の策定時には、地震等の自然災害について考慮することに加え、侵入型ランサムウェア攻撃についても考慮する必要がある。
  例えば、実際に被害に遭った場合に備えて、迅速で適切なインシデント対応を行う能力や応用力を高めるため、被害時の報告、状況把握、対応方針決定等の手順について整理し、マニュアル化等を行っておく必要がある。
- データ暗号化と身代金要求への対応
  JPCERT/CC が「侵入型ランサムウェア攻撃を受けたら読む FAQ※87」を公開している。被害への具体的対応について詳細に紹介しているため、ぜひ参照いただきたい。
  また、経営層を含めたインシデント対応の訓練を定期的に実施することが望ましい。

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 NISC 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5年度版）※88」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

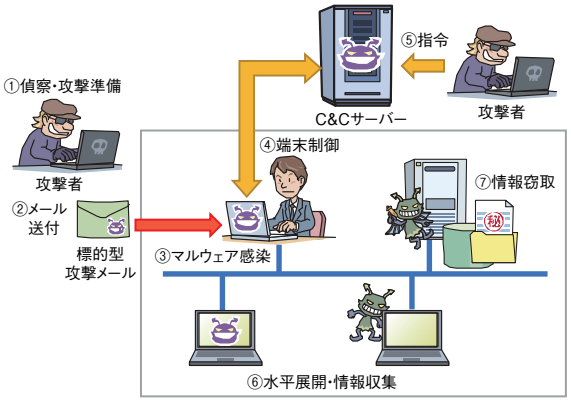
標的型攻撃における標的組織内への侵入の手口として、特定の対象をピンポイントで狙った、スピアフィッシングによる標的型攻撃メールに加え、インターネット境界に設置された機器の脆弱性の悪用等によるネットワーク貫通型攻撃も多数観測されている。以下に、それぞれの手口について述べる。

なお、ここで述べるもののほかにも、2024 年に確認された標的型攻撃の手口として、エアギャップ越しの攻撃※89 や水飲み場型攻撃※90 等がある。

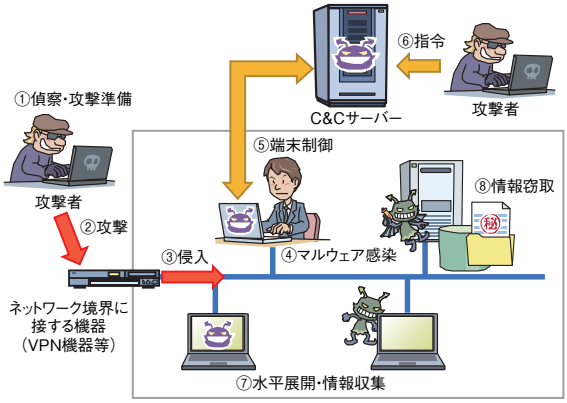
(a) 標的型攻撃メールを用いた攻撃の手口

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※91。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（次ページ図 1-2-5）。

①偵察・攻撃準備：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：標的組織宛てにメールを送付する。
③マルウェア感染：メールの添付ファイルや URL リンクを開くことでマルウェアがインストールされる。
④端末制御：パソコンと C&C（Command and Control）サーバー※92 で通信が行われる。
⑤指令：C&C サーバーを経由し、遠隔操作が可能になる。
⑥水平展開・情報収集：侵害範囲拡大や目的に関連する情報の収集を行う。



■図 1-2-5　標的型攻撃メールを用いた攻撃の流れ



■図 1-2-6　ネットワーク貫通型攻撃の流れの一例

⑦情報窃取：目的の情報等を窃取する。

(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※93。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（図 1-2-6）。

①偵察・攻撃準備：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：VPN 機器等の脆弱性を悪用し不正アクセスを行う。
③侵入：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：パソコン等に侵入しマルウェアをインストールする。
⑤端末制御：パソコンと C&C サーバーで通信が行われる。
⑥指令：C&C サーバーを経由し、遠隔操作が可能になる。
⑦水平展開・情報収集：侵害範囲拡大や目的に関連する情報の収集を行う。
⑧情報窃取：目的の情報等を窃取する。

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、他組織への踏み台としての機能が機器に仕組まれることがある。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）※94 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※95。

また、中国の国家支援型攻撃グループとされる「Volt Typhoon※96」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※97 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※98。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) 標的型攻撃メールを用いた攻撃の事例」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※99。

(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者グループによる、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※100APT 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※101。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、2024 年度に確認された、国家支援型 APT 攻撃であることが疑われる事例を紹介する。

(a) 標的型攻撃メールを用いた攻撃の事例

警察庁及び NISC は 2025 年 1 月、MirrorFace（別名「Earth Kasha」）と呼ばれる攻撃グループによる攻撃キャンペーンについて、「我が国の安全保障や先端技術に係る情報窃取を目的とした、中国の関与が疑われる組織的なサイバー攻撃活動である」として注意喚起を行った[※102]。この注意喚起で言及されている複数の攻撃キャンペーンのうち、「攻撃キャンペーン C」は、2024 年 6 月ごろから行われた標的型攻撃メールを用いた攻撃とされている。

この攻撃キャンペーンでは、国内の学術、シンクタンク、政治家、メディアに関係する個人や組織等に対し、ファイルをダウンロードさせるリンクが記載されたメールが送信された。受信者が当該リンクからダウンロードした Zip ファイルを展開後に、Microsoft Office 文書を開いてマクロを有効化すること、また、Microsoft Office 文書に偽装された拡張子が .lnk のファイルを開くことにより、「ANEL」と呼ばれるマルウェアに感染させる手口が確認されている。メールの送信者名としては、マスコミ関係者や、受信者が関心のある専門分野の有識者を詐称したものや、第三者の正規アドレスを悪用して当該正規アドレスの使用者名が用いられたものがあった。また、メールの件名の例としては、「取材のご依頼」「所蔵資料のおすすめ」「国際情勢と日本外交」といったものが確認されており、メールの本文は、詐称された送信者が過去に第三者と実際にやり取りをしていたメールを一部改変した違和感のないものであった。また、前述の注意喚起によれば、ANEL の感染のほかに「NOOPDOOR」と呼ばれるマルウェアに感染させた事例や、Windows Sandbox を悪用したマルウェア実行[※103]、Microsoft 社が提供する Visual Studio Code の開発トンネル機能（Microsoft dev tunnels）を遠隔操作ツールとして悪用した事例[※104]も確認されている。

なお、前述の注意喚起には、IPA の J-CRAT（Cyber Rescue and Advice Team against targeted attack of Japan：サイバーレスキュー隊）及びサイバーセキュリティ専門企業の協力への謝辞が含まれている。このような官を中心とした官民連携による取り組みは、国家間の課題である国家支援型 APT 攻撃への対応として、新たな進め方を示すモデルケースといえる。

(b) ネットワーク貫通型攻撃の事例

前述の MirrorFace に関する注意喚起[※102]における「攻撃キャンペーン B」は、VPN 機器の脆弱性や外部公開サーバーの SQL インジェクションの脆弱性を悪用した、ネットワーク貫通型攻撃とされている。この攻撃キャンペーンでは、2023 年 2 月ごろから 10 月ごろにかけて、国内の半導体、製造、情報通信、学術、航空宇宙の各分野の組織の VPN 機器等の脆弱性を悪用した侵入とともに、それが原因と見られる侵害活動が 2024 年 6 月ごろまで継続していた事例が確認された。侵入後の VPN 機器には、Neo-reGeorg トンネリングツールやオープンソースの WebShell[※105]が設置された事例が確認されており、また、侵入後に Active Directory サーバーへの侵害や Microsoft 365 への不正アクセスの事例のほか、Cobalt Strike Beacon[※106]の悪用、NOOPDOOR 及び「LODEINFO」と呼ばれるマルウェアへの感染の事例が確認されている。この攻撃キャンペーンで悪用されたと見られる脆弱性として、前述の注意喚起では、Array Networks Array AG 及び vxAG の脆弱性（CVE-2023-28461）、FortiOS 及び FortiProxy の脆弱性（CVE-2023-27997）、並びに NetScaler ADC（旧 Citrix ADC）及び NetScaler Gateway（旧 Citrix Gateway）の脆弱性（CVE-2023-3519）が挙げられている。

国外における事例として、中国の攻撃グループ Salt Typhoon による米国のインターネットサービスプロバイダー（ISP：Internet Service Provider、以下 ISP 事業者）等への侵害が観測され、通話記録データの窃取や政府・政治活動に関わる個人のプライベート通信の侵害が 2024 年 11 月に公表された[※107]。この攻撃において、少なくとも Cisco IOS 及び Cisco IOS XE Software の脆弱性（CVE-2018-0171）の悪用が指摘されている[※108]。

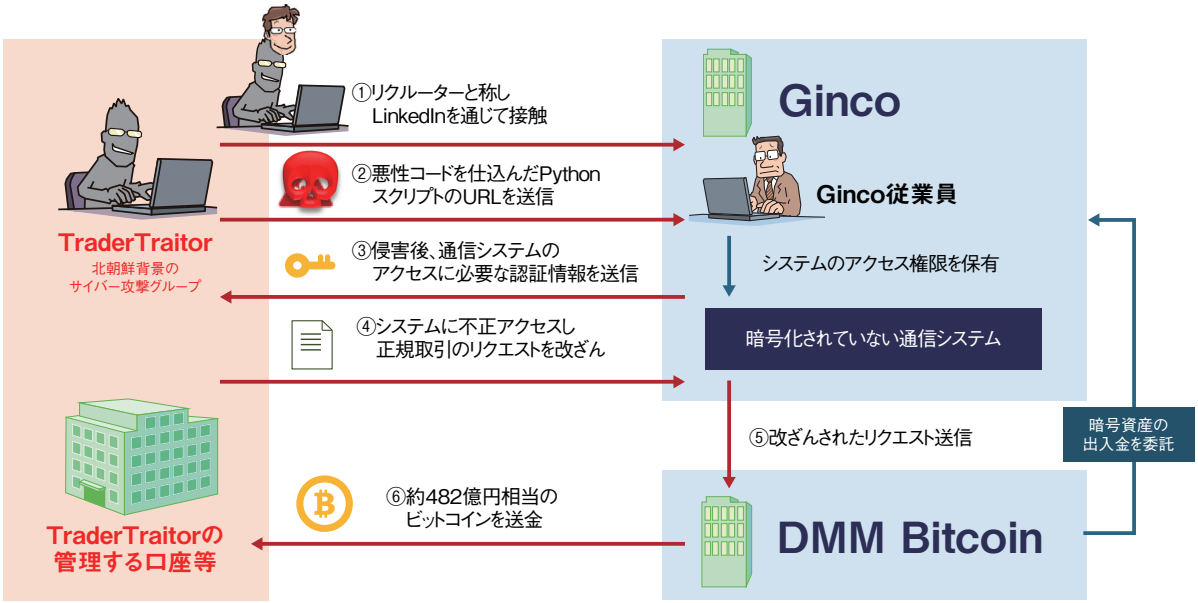
また、同年 9 月、米国司法省は、中国の国家が支援する「Flax Typhoon」と呼ばれる攻撃グループによって侵害された 20 万台超の消費者向け機器からなるボットネットを無害化したと発表した[※109]。同日、FBI 等は、Flax Typhoon が、SOHO（Small Office Home Office）ルーターや IoT 機器を含むインターネットに接続された機器の既知の脆弱性[※110]を悪用して 26 万台超の機器からなるボットネットを構築し、マルウェアの配信や DDoS 攻撃に利用しているとするセキュリティアドバイザリーを公表した[※111]。これらに関連し、2025 年 2 月、NISC は、エッジデバイスへの攻撃のリスク緩和のための七つの戦略[※112]を取りまとめた「エッジデバイスのための緩和戦略[※113]」の共同署名に参加した[※114]。IPA も、家庭用・SOHO 向けルーター等に関する注意喚起等を発出している[※115]。

(c) その他の特徴的な標的型攻撃の事例

2024 年度に国内で確認されたその他の特徴的な事例として、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」による暗号資産関連事業者を標的としたサイバー攻撃が挙げられる。2024 年 12 月、警察庁、FBI 及び米国国防省サイバー犯罪センター（DC3：Department of Defense Cyber Crime Center）は、2024 年 5 月に TraderTraitor が、日本国内の暗号資産関連事業者から約 482 億円相当（攻撃当時）の暗号資産を窃取したことを特定し、合同で文書を公表した※116。当該文書によれば、同年 3 月、攻撃者は、ビジネス向けの SNS である LinkedIn 上でリクルーターになりすまし、日本に所在する企業向け暗号資産ウォレットソフトウェア会社である株式会社 Ginco のウォレット管理システムへのアクセス権を保有する従業員に接触した。攻撃者は、採用前の試験を装って従業員に GitHub 上に保管された悪意ある Python スクリプトへの URL を送付し、従業員は、この Python コードを自身の GitHub ページにコピーした後、侵害された。その後、同年 5 月、攻撃者は、侵害された従業員になりすますためにセッションクッキーの情報を悪用し、同社の暗号化されていない通信システムへのアクセスに成功し、それを利用して暗号資産関連事業者である株式会社 DMM Bitcoin の従業員による正規取引のリクエストを改ざんした。その結果、4,502.9 BTC（攻撃当時約 482 億円相当）が喪失し、窃取された資産は最終的に TraderTraitor が管理するウォレットに移動された（図 1-2-7）。

上記文書と同日に警察庁、NISC 及び金融庁が公表した注意喚起※118 によれば、TraderTraitor は、北朝鮮当局の下部組織とされる「Lazarus Group」の一部とされる攻撃者であり、ソーシャルエンジニアリングの手法により標的組織に接近したとされている。捜査・分析で判明した具体的な手法は、まず、攻撃者は、企業幹部を装う等して、国内外に居住する暗号資産関連事業者の役職員（標的対象者）に対し、SNS で、標的対象者のプロフィールを基に、関心を引くようなメッセージを送信する。次に、標的対象者のパソコンをマルウェアに感染させるために、悪意のあるプログラムを実行させようとする。例えば、攻撃者は、C&C サーバーと通信可能なプログラムを GitHub 上にコミット（保存）し、このプログラムに不具合があると主張して、標的対象者にその特定のためにプログラムを実行させることにより、標的対象者のパソコンをマルウェアに感染させる。その後、攻撃者は、感染したパソコンに保存された認証情報やセッションクッキー等を窃取して、標的対象者になりすまして暗号資産関連のシステムにアクセスし、暗号資産を窃取する。

また、2024 年 3 月、警察庁、外務省、財務省、及び経済産業省は、北朝鮮の IT 労働者が身分を偽って業務を受注して収入を得たり、情報窃取等のサイバー活動に関与したりする懸念について注意喚起を発出している※119。北朝鮮の IT 労働者の多くは、身分証明書の偽造等によって日本人になりすまして業務の受発注のためのオンラインプラットフォームに登録して、Web ページ、アプリケーション、ソフトウェアの制作等の業務を受注し



■図 1-2-7　TraderTraitor による暗号資産関連事業者へのサイバー攻撃の概要
（出典）piyolog「TraderTraitor による DMM Bitcoin のビットコイン不正流出についてまとめてみた※117」を基に IPA が編集

ているとされ、プラットフォーム運営企業、業務発注者それぞれの注意が必要である。

更に、2025年1月、日米韓3ヵ国政府は共同で「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※120」を発出し、北朝鮮のサイバーアクターによる暗号資産窃取や、民間部門に対するインサイダー脅威となる北朝鮮IT労働者について注意喚起を行った。

(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、今まで講じていた対策が新たな攻撃手口に対して有効ではなくなる場合があるので、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※121。

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った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

  攻撃者グループが、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※122。

- 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、攻撃者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、社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や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※123。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※124。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※125」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セキュリティへ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※126」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※127」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※128。

- 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報告されている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より組織の重要情報が広範囲に分散化する傾向にあり、内部不正防止の観点から、自組織の保有する重要技術情報等の重要情報の適切な特定と漏えい対策の重要性が増している※129。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※130。内部不正を含む重要情報漏えいのリスクに対しては、自組織の重要情報の適切な特定に加え、内部不正防止のための体制として、経営層による基本方針の策定、基本方針に基づく組織横断的な計画の承認・実施統制、適切な権限移譲による具体的な対策の実施の実効性確保等、全社的に対応できる体制の整備が必要である。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※131。

(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※132。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※133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※134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、業務情報を自社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※135。
- 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※136。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※137。
- 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※138。Attack Surface（アタックサーフェス：攻撃対象領域）とは、ネットワーク機器やWebサービス等、外部（インターネット）との境界にあり、組織の外部からアクセス可能な資産を指し、これらは外部からの攻撃が行われる可能性がある。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、ツールにより資産を一元管理し、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※139、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など、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※140、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※141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、Web サーバー等の攻撃対象に対して、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、サービス運用を妨害する攻撃である。

近年では、紛争相手国や政治的に対立する周辺国に対し、社会的な混乱を引き起こすことを目的とした各種のサイバー攻撃が行われ、特に外交・安全保障上の対立をきっかけとした嫌がらせや報復の手段として DDoS 攻撃が行われることがある※142。2024 年 12 月末から 2025 年年始には、国内の重要インフラ企業等が大規模な 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、2024 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 攻撃の動向

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、2024 年上半期に全世界の同社ユーザーで観測された DDoS 攻撃は約 796 万件であり、前半期比で 12.8% 増加したという※143。DDoS 攻撃が増加している背景として、地政学上の緊張やそれに伴う、国家の活動に同調したハクティビストの抗議活動が挙げられる。ロシア・ウクライナ戦争等の世界的な出来事に関連した DDoS 攻撃は 2024 年も継続しており、2024 年 3 月のスウェーデンの北大西洋条約機構（NATO：North Atlantic Treaty Organization）加盟や、同年 6 月の G7 プーリア・サミットに伴う親ロシア派のハクティビストによる DDoS 攻撃が観測されている※144。日本国内に対しても、7 月の日・NATO 間のパートナーシップを強化していくとの NATO 事務総長による宣言に対する抗議活動※145 や、10 月の自衛隊と米軍による日米共同統合演習に対する抗議活動として攻撃が行われたと見られる。

また、CDN（Contents Delivery Network）ベンダーである Cloudflare 社のレポートによると、2024 年第 4 四半期にはランサム DDoS 攻撃の急増が観察されたという※146。ランサム DDoS 攻撃とは、攻撃者が企業や組織に対して DDoS 攻撃を行わないことや停止することと引き換えに、金銭を要求する行為のことである。同レポートによると、DDoS 攻撃の標的となった同社ユーザーの組織の 12% が脅迫されたことを報告している。脅迫された組織数は、前四半期比 78%増、前年同期比 25% 増であったという。

(2) DDoS 攻撃の事例と手口

ここでは、2024 年度における、国内の DDoS 攻撃に関する主だった事例と手口を紹介する。

(a) 国内事業者向け攻撃の事例と手口

2024 年の年末から 2025 年の年始にかけて、国内の航空会社や金融機関、携帯通信会社等に対して DDoS 攻撃と見られるサイバー攻撃が相次ぎ、被害が発生したとされる（表 1-2-2）。

発生日	対象組織名	影響
2024 年 12 月 26 日	日本航空 株式会社	国内線、国際線の航空券販売や一部のサービスが停止
12 月 26 日	株式会社 三菱UFJ銀行	オンラインバンキング等の一部のサービスが利用しづらい事象
12 月 29 日	株式会社 りそな銀行	オンラインバンキング等の一部のサービスが利用しづらい事象
12 月 31 日	株式会社 みずほ銀行	オンラインバンキング等の一部のサービスが利用しづらい事象
2025 年 1 月 2 日	株式会社 NTTドコモ	ポータルサイトのトップページへのアクセスや一部サービスが利用しづらい事象
1 月 5 日	一般財団法人 日本気象協会	Web サイト及びアプリの一部のサービスが利用しづらい事象
1 月 6 日	三井住友カード 株式会社	会員向け Web サービスが利用しづらい事象

■表 1-2-2　2024 年の年末から 2025 年の年始にかけて発生した DDoS 攻撃と見られる主なサイバー攻撃
（出典）piyolog「日本航空で発生した大量データ送付起因のネットワーク障害についてまとめてみた※147」を基に IPA が編集

これらの攻撃と関連するものとして、トレンドマイクロ社は、2024 年の年末から大規模に活動を行っている IoT ボットネットを発見し、その C&C サーバー※148 から送信される DDoS 攻撃コマンドを観測したと報告した※149。この IoT ボットネットは、Mirai と Bashlite（別名 Gafgyt、Lizkebab 等）に由来するマルウェアにより構成されていると考えられる。また、2024 年 12 月 27 日～ 2025 年 1 月 4 日の期間に収集・集計したデータについて、攻撃コマンド中に含まれる攻撃対象の IP アドレスを分析した結果、日本だけではなくアジア、北米、南米、欧州を対象とした広域に攻撃が発生していたとのことである。

ボットネットとは、攻撃者の制御下にあり、マルウェアに感染したコンピューターや IoT 機器（ボットと呼ばれる）で構成されたネットワークであり、規模が大きいもので数百

万台のボットにより構成されていることもある。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1-2-8)。

①ボットネットの構築

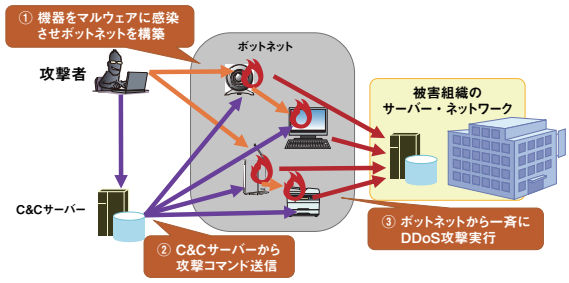
コンピューターや、家庭用ルーター、ネットワークカメラ等のインターネットに接続されているIoT機器にマルウェアを感染させ、攻撃インフラ(ボットネット)を構築する。

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。

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。



■図1-2-8　ボットネットによるDDoS攻撃の手口のイメージ

IoT機器がボットネットに組み込まれることで、サイバー攻撃の踏み台として悪用されてしまう危険性がある。これらの機器は安価で、導入が比較的容易であることから、脆弱な設定のまま安易に設置されてしまうことが多く、特に以下の三つの要因により、ボットネットに組み込まれやすいと考えられる。

①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。

②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、攻撃に対して無防備となってしまう。

③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。

(b)攻撃代行サービスによる企業攻撃の事例と手口

警察庁のサイバー特別捜査部は、外国捜査機関から提供を受けた情報を分析し、2024年8月に海外のDDoS攻撃代行サービスを利用したDDoS攻撃事案の被疑者を特定・逮捕したという※150。被疑者は、2022年3月にDDoS攻撃代行サービスを利用し、攻撃対象のWebサイトを閲覧不可能な状態にし、業務を妨害した。本件で用いられたDDoS攻撃代行サービスは、月額1,000円程度の料金であり、攻撃先を指定すれば、専門的な知見を有することのない者でも容易にDDoS攻撃を実行することが可能なものであったという。DDoS攻撃代行サービスは、安価な利用料で簡単に攻撃ができてしまうものである一方、それを利用することは、攻撃を受けた組織が経済的に打撃を受けたり、銀行や政府機関等が提供する必要不可欠なインフラが必要なときに機能しなくなったりするおそれがある悪質な犯罪であるとして、警察庁は攻撃に関与しないよう注意を促している。

また、警察庁によると、2024年10月、IPストレッサー※151という海外のネットサービスを使用し、国内の企業や自分が通っている学校に関係するWebサイトにDDoS攻撃を仕掛けたとして国内に住む中学生が書類送検されたという※152。また、別の中学生1人も、IPストレッサーを使用し、国内の企業や外国の政府機関のWebサイトにDDoS攻撃を仕掛けたとして、警察が児童相談所に通告したという。

(3)DDoS攻撃への対策

DDoS攻撃に対しては、まず自組織が提供しているサービスや業務に関する重要なシステムへの攻撃に対し、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、自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、DDoS攻撃への対策については、2025年2月に、NISCが注意喚起を行っているため、そちらも参照いただきたい※48。

(a)DDoS攻撃への平時の対策

DDoS攻撃の被害に遭う前に、平時から攻撃を想定した対策をしておくことを推奨する。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、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。

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処方法を挙げる。

- 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、対策を取る。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対応方針を策定する。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し構成する。
- 取引先や顧客等に対して、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 サーバーにソーリーページを準備しておく。
- サービスの重要性によっては、ISP 事業者等が提供する 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。
- ランダムサブドメイン攻撃のように根本的な対策が難しい 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 アドレスは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。
- WAF（Web Application Firewall）、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。
- 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。

(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してくる場合があるため、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 事業者との対策協議等の連携や警察等への通報を実施する。

(c) DDoS 攻撃に加担しないための対策

自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。
- ネットワーク機器や IoT 機器について、それらの機器上で稼働しているソフトウェアや各サービスが適切に運用されていることを確認する。具体的には、OS を始めとするソフトウェアや各サービスについて、脆弱性を含むバージョンで運用されていないか確認し、常に最新のバージョンを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し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、自組織の機器を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。組織内からインターネットに出る通信を監視し、異常な通信を確認した場合は、自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がある。異常な通信を行っている機器が確認された場合、ネットワーク切断等により通信を停止させた後、マルウェア感染等が生じていないか調査し、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に関する動向

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版がリリースされている。しかし、利用者が脆弱性を放置した場合は、情報システムにおける脅威となり、サイバー攻撃の格好の標的となる。その中でも昨今のサイバー攻撃で目立つものが、インターネットからアクセス可能なIT機器に潜む脆弱性を狙う攻撃である。テレワーク等、働き方が多様化した現在、インターネットを通じて自組織の様々な機器にアクセスすることが可能となった。しかし、それらはインターネットから攻撃可能な攻撃対象領域（アタックサーフェス）でもあり、脆弱性や機器の設定ミス等、何らかの要因によって攻撃者による攻撃を受けるおそれがある。本項では、情報システムの脆弱性に関する動向や攻撃事例、対策等を解説する。

(1) 情報システムの脆弱性の動向

IPAでは、国内外の脆弱性対策情報を収集・蓄積する脆弱性対策情報データベース「JVN iPedia※153」、及びソフトウェア製品やWebアプリケーションの脆弱性に関する情報の円滑な流通、対策の普及を図る「情報セキュリティ早期警戒パートナーシップ制度」を運用している。これらに加え、多くの利用者に影響を及ぼす脆弱性に関する注意喚起を行っている。

以下ではこれらの活動の実績から脆弱性の動向について述べる。

(a) JVN iPediaの登録状況

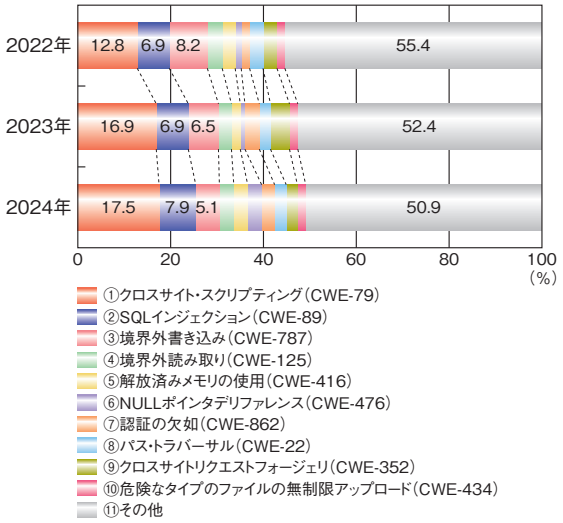
JVN iPediaは、国内外で利用されているソフトウェア製品の脆弱性対策情報を、以下の三つの公開情報から収集・蓄積している。2007年4月25日から公開しており、2024年12月末時点における登録件数の累計は22万3,690件であった。

- 脆弱性対策情報ポータルサイトJVN※154で公表した脆弱性対策情報
- 国内のソフトウェア開発者が公開した脆弱性対策情報
- 米国国立標準技術研究所（NIST：National Institute of Standards and Technology）の脆弱性データベース「NVD※155」で公開された脆弱性対策情報

JVN iPediaに登録されている脆弱性対策情報には脆弱性の種類を識別するための共通脆弱性タイプ一覧CWE（Common Weakness Enumeration）※156が含まれている。

2024年に登録された脆弱性対策情報に付与されたCWEの内訳の割合は、「クロスサイト・スクリプティング」が17.5%と最も高く、「SQLインジェクション」が7.9%、「境界外書き込み」が5.1%と続いた（図1-2-9）。最も件数の多かった「クロスサイト・スクリプティング」に分類される脆弱性を悪用されると、偽のWebページが表示されたり、情報が漏えいしたりするおそれがある。

2022年以降の経年で比較すると、2024年に1位となった「クロスサイト・スクリプティング」は増加傾向で、2024年は2023年から0.6ポイントの増加となった。2位の「SQL



■図1-2-9 JVN iPediaにおける脆弱性対策情報のCWE別割合（2022～2024年）
（出典）JVN iPediaの登録情報を基にIPAが作成

インジェクション」も 6.9% から 7.9% に 1 ポイント増加した一方、3 位の「境界外書き込み」は 6.5% から 5.1% に 1.4 ポイント減少した。

また、JVN iPedia に登録されている脆弱性対策情報には、脆弱性の深刻度として、オープンで汎用的な脆弱性評価手法である共通脆弱性評価システム CVSS（Common Vulnerability Scoring System）※157 のスコアも含まれている。なお、JVN iPedia では CVSS v2 及び CVSS v3 の二つのバージョンの情報を公開しているが、2025 年 3 月末現在では JVN iPedia の情報収集元が CVSS v2 を公開しないことが多く、本項ではすべて CVSS v3 を基に統計処理を行っている。

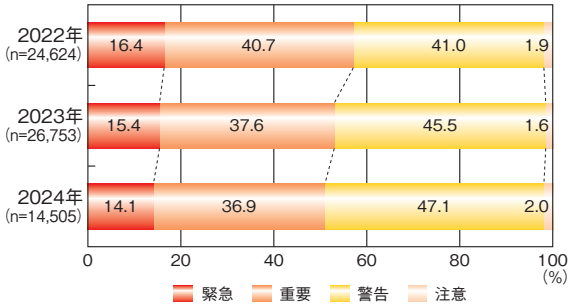
CVSS のスコアは数値が大きい程、深刻度が高くなる。CVSS v3 では基本評価基準（BM：Base Metrics）を基に評価した基本値によって、深刻度が「緊急」「重要」「警告」「注意」「なし」の 5 段階に分けられる。

深刻度のレベルごとに想定される影響は以下である。

- 深刻度 緊急：基本値 9.0 ～ 10.0
  複雑な条件なしに、リモートからシステムを完全に制御されたり、大部分の情報が漏えいしたりする等の複数の影響が想定される。
- 深刻度 重要：基本値 7.0 ～ 8.9
  リモートからシステムを完全に制御されたり、大部分の情報が漏えいしたりする等の影響が想定される。
- 深刻度 警告：基本値 4.0 ～ 6.9
  一部の情報が漏えいしたり、サービス停止につながったりする等の影響が想定される。
- 深刻度 注意：基本値 0.1 ～ 3.9
  「警告」相当の影響があるが、攻撃するには複雑な条件を必要とする。
- 深刻度 なし：基本値 0
  影響は発生しないと考えられる。

2022 年以降の深刻度のレベル別割合を年別に見ると、「緊急」及び「重要」に分類される脆弱性の割合は、2024 年は 51.0% であり、2022 年から 3 年連続で減少した。一方で、「警告」に分類される脆弱性の割合は、2024 年は 47.1% と 2023 年から 1.6 ポイント増加した（図 1-2-10）。

なお、IPA では、JVN iPedia におけるソフトウェア製品に関する脆弱性対策情報の登録状況を四半期ごとに IPA の Web サイト※158 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。



■図 1-2-10　JVN iPedia における脆弱性対策情報の深刻度のレベル別割合（2022 ～ 2024 年）
（出典）JVN iPedia の登録情報を基に IPA が作成

(b) 早期警戒パートナーシップにおける脆弱性の届出状況

ソフトウェア製品や Web アプリケーション（以下、Web サイト※159）の脆弱性は、2000 年ごろから攻撃に悪用されることが増え、重大な被害が生じるようになった。そこで、脆弱性関連情報の円滑な流通、及び対策の普及を図るため、2004 年 7 月、「情報セキュリティ早期警戒パートナーシップ※160」（以下、パートナーシップ）制度が整備された。

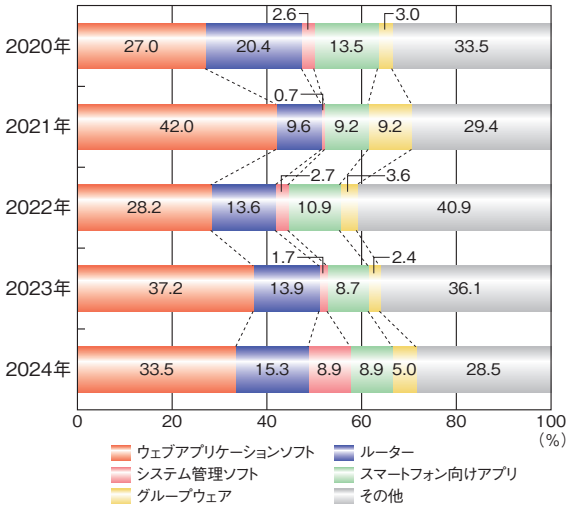
2024 年にパートナーシップへ届け出された脆弱性の件数、及び届出受付開始（2004 年 7 月 8 日）からの累計は、ソフトウェア製品が 296 件（累計 5,960 件）、Web サイトが 336 件（累計 1 万 3,326 件）、合計 632 件（累計 1 万 9,286 件）であった（表 1-2-3）。

	ソフトウェア製品	Web サイト	合計
2024 年届出件数	296 件	336 件	632 件
累計届出件数	5,960 件	1 万 3,326 件	1 万 9,286 件

■表 1-2-3　2024 年の届出件数と累計届出件数

2020 年から 2024 年までにパートナーシップに届出されたソフトウェア製品の脆弱性のうち、受け付けた届出（不受理を除いた届出）について、各年の製品種類別の割合を図 1-2-11（次ページ）に示す。2024 年は、2023 年同様、「ウェブアプリケーションソフト※161」が 3 分の 1 を占めている。依然として、ウェブアプリケーションソフトに分類される、CMS（Contents Management System）や、CMS の機能拡張プラグインに関する届出が多い傾向にあった。

続いて、2020 年から 2024 年までにパートナーシップに届出された Web サイトの脆弱性の届出のうち、受け



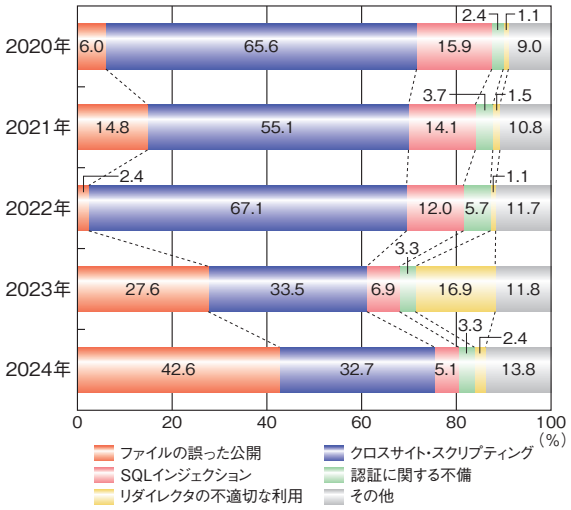
■図 1-2-11　ソフトウェア製品における脆弱性の届出の製品種類別割合（2020 ～ 2024 年）
（出典）パートナーシップへの届出状況を基に IPA が作成

付けた届出（不受理を除いた届出）について、各年の種類別の割合を図 1-2-12 に示す。

2023 年までは、「クロスサイト・スクリプティング」の脆弱性の割合が最も多かった。しかし、2024 年は、「ファイルの誤った公開」が 42.6% を占め、「クロスサイト・スクリプティング」の 32.7% を大きく超えることとなった。

「ファイルの誤った公開」は、Web サイトにおいてアクセス制限をすべきファイルが意図せず公開状態になっていることを問題とする脆弱性である。アプリケーションの機能や仕組み上の問題に由来するものだけではなく、Web サイト管理者の確認不足等により、誤って機微なファイルを Web サイトにアップロードしてしまうような場合も含まれる。

一方、2023 年には例年と比べ割合が大きかった「リダイレクタの不適切な利用」について、2024 年には 2.4% まで割合が減っていることが分かる。



■図 1-2-12　Web サイトにおける脆弱性の届出の種類別割合（2020 ～ 2024 年）
（出典）パートナーシップへの届出状況を基に IPA が作成

「リダイレクタの不適切な利用」は、Web サイトに設置されたリダイレクタ（他の Web ページに遷移するための仕組み）が悪意あるリンクの踏み台にされ、利用者が意図せずに悪意ある Web ページを表示させられる問題である。「オープンリダイレクト（Open Redirect）」とも呼ばれ、これを悪用することで、正しいリンクだと誤認した利用者に悪意あるページを表示させることができるため、フィッシング攻撃に用いられることがある。

なお、IPA では、パートナーシップへのソフトウェア等の脆弱性関連情報に関する届出状況を四半期ごとに IPA の Web サイト※162 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。

(2) 脆弱性を悪用した攻撃とその手口

2024 年度も、前年から継続して VPN 機器の脆弱性を狙った攻撃が多く発生した。また、太陽光発電設備に用いる遠隔監視機器の脆弱性を狙った攻撃のように第三者への攻撃の踏み台に利用された例も報告された。本項では、これらの脆弱性を悪用した攻撃とその手口について、事例を基に紹介する。

(a) VPN 機器の脆弱性を狙った攻撃事例

VPN は、専用のネットワーク回線を仮想的に構築することで、物理的に離れている拠点のネットワーク間を、あたかも同一のネットワークであるかのように接続する技術であり、拠点のネットワークと離れた場所にあるパソコン等を安全に接続するために使用される。

VPN 機器は、インターネットから直接アクセスできる箇所に設置されるという性質上、攻撃の対象とされやすい。攻撃が成功した場合、ネットワーク内部に侵入した攻撃者は、更なる攻撃活動に用いるための WebShell 等のツールを設置する。更に、ネットワーク内部に水平展開を行い、機密情報等の窃取を行う。場合によっては、利用者に悟られぬよう潜伏し続け、ネットワーク内部の機器を踏み台とした不正送金や第三者への攻撃に悪用したり、情報窃取後にランサムウェアに感染させ、その後の業務を妨害したりすることもある（ランサムウェア攻撃については「1.2.1 ランサムウェア攻撃」参照）。IPA は、このような攻撃に関する注意喚起を行い、対策を促している。

2024 年も引き続き、脆弱性が解消されていない VPN 機器を起点として、組織内部に設置しているサーバーが侵害され、個人情報を含むデータが窃取される事例が

確認されている※163。

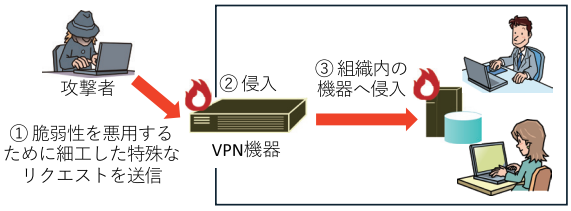
2024年4月12日、Palo Alto Networks, Inc.（以下、Palo Alto社）は、同社のファイアウォール用オペレーティングシステムPAN-OSのGlobalProtect機能に関する脆弱性（CVE-2024-3400※164）を公開した。同脆弱性が悪用された場合、認証されていない遠隔の第三者によって、root権限（管理者権限）で任意のコードが実行されるおそれがある。脆弱性の深刻度を示すCVSS v3基本値は10.0で、最も深刻度が高い「緊急」と評価された※165。

脆弱性の公開日と同日、CISAのKEV（Known Exploited Vulnerabilities Catalog：既知の悪用された脆弱性カタログ）に同脆弱性が登録された※166。また、IPA及びJPCERT/CCから注意喚起が行われた※167。

同脆弱性は、セキュリティベンダーによって、ゼロデイ攻撃が確認されており、攻撃の具体的な内容としては、リバースシェル※168の作成、各種ツールのダウンロード、設定ファイルの奪取、水平展開、バックドアの展開等が挙げられている。そして、これらの攻撃によって、Active Directoryデータベース（ntds.dit）や、Windowsイベントログ等の窃取が行われたとされている※169。

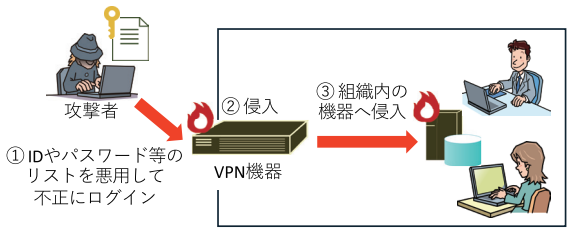
Palo Alto社は、同年4月14日から同年4月18日にかけて、順次、本脆弱性を修正するためのHot Fix（緊急の修正プログラム）を公開し、ワークアラウンド（応急措置）や緩和策が適用されている場合であっても、ソフトウェアのアップデートを早急に行うことを強く推奨している※164。

VPN機器の脆弱性を狙った攻撃の具体的な手口としては、前述したような脆弱性を悪用することによってVPN機器に侵入する方法がある（図1-2-13）。



■図1-2-13　脆弱性を悪用することによって侵入する方法

ほかにも、インターネットやダークウェブにおいて、公開または販売されている情報（IPアドレス、ID及びパスワード等の一覧）を悪用し、VPN機器に侵入する方法がある（図1-2-14）。この侵入方法への対策としては、VPN機器にログインするためのパスワードは推測されにくいものを設定し、漏えいさせないように適切に管理していくことが肝要と言える。その他の対策については、「1.2.4（3）脆弱性対策」を参照いただきたい。

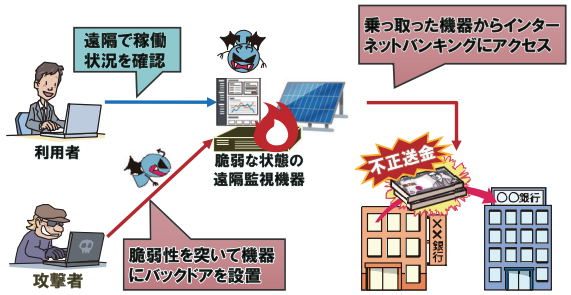


■図1-2-14　インターネットやダークウェブから入手した情報を悪用することによって侵入する方法

（b）太陽光発電設備に用いる遠隔監視機器の脆弱性を狙いネットバンキングへの踏み台として利用した攻撃事例

太陽光発電設備の遠隔監視機器は、離れた場所にある太陽光発電設備の発電量や設備の状況等の稼働状況を計測・記録し、利用者が組織内ネットワークやインターネットを経由して確認するために用いる機器である。この遠隔監視機器にも脆弱性が存在することがある。2024年には、脆弱性を解消していない遠隔監視機器を狙った攻撃が発生し、更にそれを踏み台とした第三者への攻撃（ネットバンキングでの不正送金）が起こっていたことが判明した。

2024年5月1日、株式会社コンテック（以下、コンテック社）製の遠隔監視機器、約800台に脆弱性があり、中国のハッカー集団によるものと見られるサイバー攻撃によってその一部が乗っ取られ、インターネットバンキングによる不正送金に悪用されたと報道された※170。S2W INC.のレポートでは、「軍火庫」というハッカー集団がサイバー攻撃に関わったとされていた※171。同年5月7日、コンテック社は、同社製「SolarView Compact」に存在する脆弱性に対して、対策が十分でない一部の機器に不正中継を実施できるバックドアを設置され、機器を悪用できる状況にあったと公表した※172。同製品は、太陽光発電設備の稼働状況のモニタリングに加え、Webサーバー機能を有しており、利用者のパソコンからWebブラウザーを通じて稼働状況を確認することが可能な製品である。この攻撃では、既に修正されている複数の脆弱性が悪用されたとされる。トレンドマイクロ社のレポートによると、本事例における不正送金の手口は、今回侵害されたとされる監視機器の機能で送金が行われたというわけではなく、監視技術を提供する機器の母体となるコンピューター部分を攻撃者が不正操作し、インターネットバンキングにアクセスの上、送金を行ったとされる。今回の攻撃では、製品開発者が修正済みの複数の脆弱性のうち、OSコマンドインジェクションの脆弱性を攻撃者が悪用したとされ、修正済みバージョンへのアップデート等の対策が



■図 1-2-15　SolarView Compact の脆弱性を悪用した攻撃イメージ

取られていない同製品にバックドアを設置の上、遠隔で操作を行ったと見られる※173（図 1-2-15）。

なお、今回の報道では、不正送金にのみ言及されているが、同レポートによると、不正送金だけではなく、DDoS 攻撃の攻撃元（踏み台）として悪用される場合や情報の窃取、システムの破壊等の被害に遭うおそれがあると解説している。踏み台として悪用されるケースでは、DDoS 攻撃だけでなく、ランサムウェア攻撃や標的型攻撃等において、送信元や送信先を隠蔽して攻撃を中継する ORB※174 として悪用され、意図せずに他組織への攻撃活動に加担してしまうこともあり得る。

コンテック社の Web サイトでは、2023 年 7 月時点で、不正アクセス対策のため、最新のソフトウェアを利用する等の対策を取るようにとの注意喚起をしていた※175 ものの、本事例では未対策の機器が狙われたと見られる。この件は、電力分野のサイバーセキュリティについて検討する国の研究会でも取り上げられた※176。

なお、JVN iPedia には、同製品の脆弱性が 2021 年以降に複数件登録されている。その中でも特に、CVE-2022-29303 及び CVE-2023-23333 はリモートで任意のコマンドを実行されるおそれのある脆弱性であり、脆弱性の実証コード（PoC※177）もインターネット上に公開されている。加えて、CVE-2022-29303 は、CISA の KEV にも、2023 年 7 月 13 日に掲載された※178。

本事例におけるサイバー攻撃においては、公表済みの脆弱性の対策を取っていなかったことが要因の一つに挙げられる。脆弱性を狙った攻撃による被害を防ぐため、利用するソフトウェアは常に最新のバージョンにアップデートしておくことが望ましい。アップデートによる対応が難しい場合は、脆弱性による影響を低減させる回避策がベンダーから提示されている場合があり、必要に応じて対策を実施することが推奨される。その他の対策については、「1.2.4(3)脆弱性対策」を参照いただきたい。

また、本事例のように、公表済みの脆弱性の対策を取っていなかった背景として、いわゆる IoT 機器の多くは、ライフサイクルが長いことや、IoT 機器に対する監視が行き届きにくいという性質も持ち合わせていることが挙げられる。具体的には、機器を設置する際はセキュリティ対策を施していても、月日が経過するとともに脆弱な状態となるおそれもある。また、太陽光発電設備に設置されている遠隔監視機器は、機器そのものが利用者から離れた位置にあることから、物理的にも監視の目が届かず、手元にあるパソコンやスマートフォン等の機器とは違い、セキュリティ意識が希薄になりがちである。そのため、セキュリティ対策が疎かになってしまうおそれがあることに加え、サイバー攻撃による機器への侵害にも気付きにくく、継続して侵害されたままとなってしまうおそれがあることにも注意する必要がある※179。

(3) 脆弱性対策

情報システムの脆弱性を悪用した攻撃への対策は、情報システム運用者が行う対策と、ソフトウェア製品開発者が行う対策に分けることができる。これらの対策について解説する。

(a) 情報システム運用者が行う対策

情報システム運用者は、自組織が保有するすべてのシステムを漏れなく把握した上で、各システムに対して適切な対策を実施していくことが肝要である。以下に、具体的な対処方法を挙げる。

- 脆弱性対策の実施手順を整備し、脆弱性が確認された場合、遅延なく着実に対応を実施する。併せて、攻撃を受けてしまった場合の対応についても定めておくことを推奨する。脆弱性対策の実施手順としては、以下に示す内容を定めておくことを推奨する。
  - 脆弱性対策情報の収集方法
  - 脆弱性が確認された場合の対応方法
  - 脆弱性の緊急度や深刻度に応じた対応の優先順位
  - 他部署やベンダー等への連絡の要否基準
- 自組織が保有するシステムについて、構成管理を適切に行い、利用しているソフトウェアの脆弱性対策情報を日々収集する。脆弱性対策情報は、日々、非常に多くの情報が公開されることから、自組織に必要な脆弱性対策情報を機械的に収集する仕組みを活用することで効率良く収集することができる。仕組みの具体例としては、IPA が提供する「MyJVN API※180」や「MyJVN 脆弱性対策情報フィルタリング収集ツール（mjcheck4）※181」が挙げられる。

  なお、自組織のシステムが遠隔監視装置等の IoT 機

器を構成機器として保有している場合、前項の例に挙げたような IoT 機器の特質に留意して管理しておく必要がある。

- 利用するソフトウェアは、常に最新のバージョンにアップデートしておく。アップデートによる対応が難しい場合、脆弱性による影響を低減させる回避策がベンダーから提供されている場合があるため、適宜利用することを推奨する。
- システムを構成する各種機器（サーバーやネットワーク機器、VPN 機器等）や、組織内の役職員が利用する端末に設定するパスワードについて、推測されにくいものを使用することを自組織のセキュリティ規程等で定める。なお、パスワードの桁数は、できる限り長くすることを推奨する。
- 日頃からログや通信の監視等を実施する。脆弱性の存在が明らかとなっていない状況への対策として、攻撃及びその予兆をいち早く察知できるよう備えておくことを推奨する。
- 自組織で Web サイトを運用している場合、定期的に脆弱性診断を実施し、脆弱性の有無を確認する。自組織のみで実施することが難しい場合、外部のセキュリティベンダーに依頼して実施することを推奨する。

(b)ソフトウェア製品開発者が行う対策

ソフトウェア製品開発者は、自組織が開発するソフトウェアや、開発したソフトウェアについて、ソフトウェアの企画から廃棄に至るまでのソフトウェアライフサイクルの各工程でセキュリティを考慮していくことが肝要である。以下に、具体的な対処方法を挙げる。

- 組織の製品セキュリティに関する方針や考え方を製品セキュリティポリシーとして策定する。また、新規に発見される自組織のソフトウェアの脆弱性のサポート期間を含むセキュリティサポート方針を策定する。これらは、自組織の経営層の承認を得て、組織内に周知する。なお、セキュリティサポート方針については、安心して使用できる期間を製品利用者に示すため組織外に公開することを推奨する。
- 製品セキュリティポリシーに基づき、組織として実施すると定めた内容に対応するために必要な体制を整備する。
- 製品の用途等を想定したリスク分析を行う。この結果を踏まえて、製品の設計段階からセキュリティ機能を検討する。
- 設計・開発の各段階で脆弱性検査を実施し、検知された脆弱性について対応を行う。
- 製品の構成要素（例えば、コンポーネントやライブラリ等）について、構成管理を実施し、構成要素の脆弱性に関する情報を収集する。収集した情報を基に、深刻度の高い脆弱性から対応を行う。
- セキュリティを考慮したコーディングルールを策定し、実装する。コーディングに関するルールの具体例としては、重要情報（パスワードや IP アドレス、暗号鍵等）をソースコードに埋め込まないことが挙げられる。
- 第三者によって発見された自組織のソフトウェアの脆弱性について、報告受付、分析と対策策定、情報開示を行う必要がある。そのための体制の準備、及び運用を行う。
- 利用者による適切なセキュリティ機能の利用を促すため、利用開始時のパスワードの初期設定、利用中のアップデート、利用終了時のデータ消去等、利用者がソフトウェアの利用開始時、利用中及び利用終了時のそれぞれに実施すべき事項をまとめ、利用者に開示する。ソフトウェアのセキュリティレベルを維持するためには、利用者において、セキュリティ機能が適切に利用されることが肝要である。

1.2.5 重要インフラ・制御システムに対する脅威

重要インフラは、我々の生活及び社会経済活動の基盤であり、その機能が停止、低下または利用不能な状態に陥った場合に多大なる影響を及ぼす。我が国では、電力、ガス、水道等、15 分野が重要インフラに指定されている。なお、重要インフラの定義や対象範囲（分野）は、国によって異なる。日本・米国・英国の重要インフラ分野の比較を表 1-2-4（次ページ）に示す。

攻撃者にとって重要インフラは価値の高い標的であること、地政学的緊張の高まり等から、重要インフラのセキュリティインシデントは年々増加している。

重要インフラで施設、機器やシステムを管理し、制御するためのシステムが制御システム（ICS：Industrial Control System）である。従来、制御システムの多くは、独立したネットワーク、固有のプロトコル、事業者ごとに異なる仕様で構築・運用されており、外部からサイバー攻撃を行うことは困難と考えられていた。しかし、近年、ネットワーク化やオープン化（標準プロトコル・汎用製品の利用）が進んだこと、10 ～ 20 年に及ぶライフサイクルの長さ故に、外部との接続やサイバー攻撃を想定していない制御システムが今なお多数稼働していること等から、制

	日本	米国	英国
定義した組織	内閣サイバーセキュリティセンター（NISC）※182	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）※183	国家保護安全保障局（NPSA）※184 英国国家サイバーセキュリティセンター（NCSC）
重要インフラの定義	他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもの。	重要インフラ（Critical Infrastructure）米国にとって極めて重要であり、その無効化や破壊がセキュリティ、国家安全保障、国民の健康や安全、またはそれらの組み合わせに深刻な影響を及ぼすと考えられる資産、システム、ネットワーク（物理的または仮想的なもの）。	国家重要インフラ（CNI：Critical National Infrastructure） その国の機能と日常生活に不可欠な施設、システム、場所、情報、人々、ネットワーク、プロセスを指す。また、本質的なサービスの維持には重要ではないものの、公衆に対する潜在的危険性があるため防御が必要な機能、場所、組織（例えば、民間原子力施設や化学施設）も含まれる。
分野数	15	16	13
分野	情報通信	情報技術（Information Technology）	―
		通信（Communications）	通信（Communications）
	金融	金融サービス（Financial Services）	金融（Finance）
	クレジット		
	航空	輸送システム（Transportation Systems）	輸送（Transport）
	空港		
	港湾		
	鉄道		
	物流		
	電力	エネルギー（Energy）	エネルギー（Energy）
	ガス		
	石油		
	政府・行政サービス（地方公共団体を含む）	政府サービス・施設（Government Services and Facilities）	政府（Government）
	医療	医療・公衆衛生（Healthcare and Public Health）	保健福祉（Health）
	水道	上下水道システム（Water and Wastewater Systems）	水道（Water）
	化学	化学（Chemical）	化学（Chemicals）
	―	商業施設（Commercial Facilities）	―
		重要製造業（Critical Manufacturing）	
		ダム（Dams）	
		防衛産業基盤（Defense Industrial Base）	防衛（Defence）
		緊急サービス（Emergency Services）	緊急サービス（Emergency Services）
		食料・農業（Food and Agriculture）	食品（Food）
		原子炉・材料・廃棄物（Nuclear Reactors, Materials, and Waste）	原子力（Civil Nuclear）
		―	宇宙（Space）

■表 1-2-4　日本・米国・英国の重要インフラ分野

御システムに対するサイバー脅威は年々高まっている。

本項では、重要インフラ分野を狙った攻撃と制御システムのセキュリティについて述べる。

(1) 重要インフラを狙った攻撃の発生状況と動向

2024 年も重要インフラを狙った攻撃は多数発生し、調査会社によるアンケート調査においても明らかになっている。

例えば、英国のエネルギー、製造、石油・ガス分野の従業員 1,000 人以上の大企業の役員レベルの意思決定者 406 人を対象に 2024 年 8 月に実施された調査によると、89.66% の組織が過去 12 ヵ月間にサイバーセキュリティインシデントを経験したと回答している※185。また、複数の重要インフラ分野の専門家 530 名以上を対象に

した調査では、回答者の19%が過去12ヵ月間に少なくとも1回のセキュリティインシデント（ランサムウェアを除く）を経験したと回答している※186。

サイバーセキュリティ企業のデータによると、米国のユーティリティ（電力・ガス・水道等の公共サービス提供会社）に対するサイバー攻撃は、2024年1月から8月までの週間平均で前年の同期間と比較して70%近く増加した※187。

本項では、2024年に公になった重要インフラ分野のインシデントのうち、具体的な事例をいくつか述べる。

(a) 水処理施設が標的となった事例

2024年9月22日、米国カンザス州カウリー郡のアーカンソーシティ（人口約1万2千人）の水処理施設が、ランサムウェア攻撃グループ「BlackSuit」による攻撃を受けた。同市は攻撃を検知してすぐに、CISA及びFBIに支援を要請し、更に退職者や外部オペレーターにも支援を仰ぎ、24時間体制でインシデントに対応した。予防措置のため、施設を手動運用に切り替えたが、住民への水道サービスの提供には影響はなかった。約3ヵ月後の12月18日にようやく通常運用に復旧し、フォレンジック調査の結果、機密データへの不正アクセスや漏えいはなかったことが確認された。同市は、サーバーの交換、ソフトウェア、ライセンス、技術支援といったインフラの修理とアップグレードに10万5,201ドル（約1,578万円）、フォレンジック分析、法的指導、脅威アクターとのコミュニケーション等の法的費用及び調査費用に5万8,550ドル（約878万円）の費用を負担した※188。

米国環境保護庁とCISAは、水処理施設や下水処理施設に対して、インターネットに露出しているすべてのデバイスのリストを作成し、HMI（Human Machine Interface）やその他の保護されていないシステムをインターネットから切断するか、強力なユーザー名とパスワードでセキュア化し、HMIとOTネットワーク全体に多要素認証（MFA：Multi-Factor Authentication）を使用すること等を推奨している※189。

(b) 石油精製会社が標的となった事例

2024年11月、コスタリカの国営石油精製企業Refinadora Costarricense de Petróleo（RECOPE）が、ランサムウェア攻撃を受けた。同社は、化石燃料の輸入、精製、国内流通を手掛けるほか、カリブ海から太平洋沿岸に伸びるパイプラインの運営も行っている。11月27日朝、同社はランサムウェアによるインシデントを発見し、調査を開始した。攻撃によって、支払い処理に使用されていたすべてのシステムがダウンしたため、燃料販売を手動で行わざるを得なくなった。そのため、タンカーターミナルでの業務は11月27日夜遅くまで延長され、28日も引き続き延長された。同社は、同国の科学技術通信省と協力して事態の解決に取り組み、国民に対してはソーシャルメディアを通じて燃料不足は発生していないことを繰り返し発信した。11月29日には米国からサイバーセキュリティの専門家が到着し、徐々にいくつかのシステムを復旧させることができたが、プロセスが完全に安全であることが保証されるまでは手動でシステムを運用し続けた※190。この米国による支援では、米国国務省（DOS：U.S. Department of State）が、同盟国を強化し、世界的なデジタル規範に米国の価値観を浸透させるために策定された取り組みの一つである「FALCON（Foreign Assistance Leveraged for Cybersecurity Operational Needs）」が初めて活用された。DOS職員と二つの民間企業から派遣された契約社員で構成された小規模のチームが首都サンホセに派遣され、現地で約10日間活動し、その後12月中旬までオンラインでサポートを行った。同チームは、インシデントを調査し、ランサムウェア攻撃者をシステムから排除し、バックアップからデータを復元し、システムをオンラインに戻し、今後のサイバー攻撃に対する耐性強化を支援した。この作業全体にかかった費用は約50万ドル（約7,500万円）だった※191。

(c) 輸送分野が標的となった事例

2024年8月、米国ワシントン州のシアトル・タコマ国際空港が、ランサムウェア攻撃グループ「Rhysida」による攻撃を受けた。8月24日早朝、システムに悪意のある人物が侵入した可能性があることを確認し、被害の拡大を防ぐためにシステム全体の電源を落とした。これにより、空港内のフライト情報ディスプレイや手荷物を追跡するシステムを含む重要なシステムが影響を受けた。8月26日には177便のフライトが遅延し、7便がキャンセルされた。同空港は、必要なシステムを復旧し、乗客への影響を軽減するために24時間体制で取り組み、空港当局、米国運輸保安庁、FBIが協力して調査した。同空港の多くのスタッフは、通常のデスク業務を行うことができず、自らターミナルに出向いて旅行者を搭乗ゲートや目的の場所まで案内した。また、退職した従業員や常勤のボランティアも駆け付けて支援を行った。彼らはペン、紙、手書きのサイン、サードパーティーのアプリ、

Google 検索、テキストメッセージ等を駆使して、フライト、搭乗ゲート、手荷物に関する情報を提供した。インシデント発生から 10 日間で、約 500 人のボランティアが 3,600 時間以上を費やして旅行者のサポートにあたった。攻撃グループは、データを窃取したと主張し、600 万ドル（約 9 億円）の身代金を要求したが、同空港は税金の有効な使い方ではない、として支払いを拒否した。復旧作業には時間がかかり、Web サイトは 11 月 22 日にようやく復旧した※192。

2024 年 10 月、メキシコの空港運営会社 Grupo Aeroportuario del Centro Norte（OMA）が、ランサムウェア攻撃グループ「RansomHub」による攻撃を受けた。同社 IT チームは、管理する 13 の国内空港の運営を継続するために、バックアップシステムに切り替えた。OMA は、運営している空港内のスクリーンがすべてダウンしていることを 10 月 15 日に確認した。10 月 24 日時点で、フライトのターミナル位置を示すスクリーンはまだダウンしていたが、OMA は空港周辺に乗客を支援するスタッフを配置し、乗客が搭乗ゲートを見つけることができる QR コードも用意した。また、乗客に対して、各航空会社のソーシャルメディアアカウントをフォローするよう呼びかけた。攻撃グループは、10 月 24 日にこの攻撃を主張し、身代金を支払わなければ窃取した 3TB のデータを公開すると脅迫した※193。

（d）通信事業者が標的となった事例

2024 年 11 月、中国政府が支援しているとされる APT 攻撃グループ「Salt Typhoon」が、システムの脆弱性を悪用して数十ヵ国の通信事業者を侵害していたことが FBI と CISA の共同声明で明らかとなった※194。被害者には、T-Mobile USA, Inc.、Verizon Communications Inc.、AT&T Inc.、Lumen Technologies, Inc. 等の合計 9 社の米国の通信事業者が含まれていた。攻撃グループは、被害企業のネットワークに侵入した後、通信事業者が「法執行機関の要請に応じて国内データを共有するために使用するシステム」にアクセスした可能性がある。FBI 及びその他の法執行機関は、裁判所の命令を得て、データが犯罪の解決や国家安全保障問題の調査に使用される場合に限り、電子通信の傍受を許可されている。また、ネットワークプロバイダーやその他の企業が、令状なしでこのレベルののぞき見アクセスを提供することもある。同攻撃グループは米国内の個人や企業からの一般的なインターネットトラフィックも傍受した可能性がある。連邦政府と民間のセキュリティアナリストは、同グループが窃取したデータの量や種類を含め、侵害について調査を継続している。12 月 3 日、FBI と CISA は、中国のハッカーによる通信傍受の可能性を最小限に抑えるために、米国市民に対して、暗号化メッセージングアプリに切り替えるよう勧告した※195。

（e）政府や自治体が標的となった事例

政府や自治体といった行政機関を標的としたサイバー攻撃も、世界中で相次いでいる。

2024 年 6 月 9 日、米国オハイオ州クリーブランド市の自治体がランサムウェア攻撃を受けた。同市のセキュリティチームは、被害の拡大を防ぐため、IT システムをシャットダウンした。市庁舎は 6 月 10 日、11 日の 2 日間閉鎖され、6 月 12 日に職員のみを対象に閉鎖が解除された。911 コールセンター、警察、消防署、救急医療サービスを含むすべての緊急サービスに影響はなく、通常どおり運営された※196。

2024 年 12 月 26 日、米国ノースカロライナ州ウィンストン・セーラム市の自治体がサイバー攻撃を受けた。同市は、デジタルプラットフォームの問題を発見し、万全を期すため、一部のコンピューターシステムを停止した。また、州及び連邦政府機関の協力のもと、インシデント調査及び復旧作業を実施した。水道や電気等の公共料金のオンライン支払いができなくなり、住民は現金または小切手で支払うことを余儀なくされた。しかし、公共サービスの中断はなく、消防や警察の通報への対応能力に支障はなかった。約 2 ヵ月後の 2025 年 2 月 11 日、ようやく公共料金、手数料、駐車違反切符のオンライン決済が可能になった※197。

（f）医療機関が標的となった事例

医療機関等を標的としたサイバー攻撃も、世界中で相次いでいる。

104 ヵ国の IT プロフェッショナル 1,309 名を対象に実施した調査結果によると、医療分野の組織の 84% が、過去 12 ヵ月以内に医療システムへのサイバー攻撃を検知した、と回答している。サイバー攻撃を受けた医療分野の組織の 69% が金銭的な損害を被っており、これは他の業界の 60% と比べると高い割合となっている※198。攻撃を受けて閉鎖した近隣の医療施設から患者を受け入れている病院では、脳卒中や心停止の症例が増加し、治療に影響を与えている。2023 年に発表された調査結果では、病院に対するランサムウェア攻撃が波及効果をもたらし、攻撃を受けていない病院での受け入れ患者

数が急増し、脳卒中患者は113%増加、心停止患者は81%増加した。また、その心停止患者の生存率は低下していた[※199-1]。

2024年2月21日、米国の医療サービス大手Change Healthcare[※199-2]が、ランサムウェア攻撃グループ「BlackCat/ALPHV」による攻撃を受けた。攻撃を検知した後、システムをオフラインにしたため、全米の数千の薬局や医療提供者に影響を与えた。医療提供者は保険金の支払いを適切に申請・受領することができず、特に大規模な医療提供者には、医療費請求の支払いを受領できないことによるキャッシュフローの問題が生じた。同社は、米国の医療システム全体を通じて、医療提供者、病院、開業医、患者間の決済及び取り引きを管理しており、米国の決済代行会社の中でも最多の件数となる年間150億件の取り引きを処理している。米国病院協会によると、ランサムウェア攻撃を受けたことで、翌3月には、94%もの病院に財務上の影響が生じた。また、データ侵害によって、1億人以上が影響を受けた。侵害されたデータには、名前、住所、生年月日、電話番号、運転免許証または身分証明書番号、社会保障番号、診断及び治療情報、医療記録番号、請求コード、保険加入者ID等が含まれている。この攻撃による損失総額は29億ドル(約4,350億円)近くに上ると見込まれている。攻撃者は、侵害した認証情報を使用して、多要素認証で防御されていないリモートアクセスポータルに侵入した。9日間アクセスし、その間に水平移動を行い、患者の機密データを窃取した後、ファイル暗号化マルウェアを展開した。親会社UnitedHealth Group Incorporated(以下、UnitedHealth)が、身代金2,200万ドル(約33億円)を支払ったが、同社は復旧に苦戦した。3月第2週に、一部のシステムを復旧させることができたが、決済サービスは攻撃から9ヵ月後の11月にようやく復旧した。BlackCat/ALPHVは、RaaS(Ransomware as a Service)モデルを使用しており、攻撃はアフィリエイトと呼ばれる提携ハッカーが実行した。攻撃の後、BlackCat/ALPHVは、Change Healthcareの親会社UnitedHealthから身代金が支払われたにもかかわらず、アフィリエイトに手数料を支払わず、3月初旬に姿を消した。そのアフィリエイトと関係があると考えられている、別の大手ランサムウェア攻撃グループ「RansomHub」が、2月の攻撃の際に窃取した数百万人の患者の個人情報を含む複数のファイルをダークウェブのリークサイトで4月15日に公開した。RansomHubは、身代金が支払われないとデータを最高額入札者に売却する、と同社を脅迫した。

RansomHubは、「BlackCat/ALPHVはChange Healthcareから窃取したデータを所持しておらず、我々が所持している」と主張していた[※200]。

2024年5月8日、米国の医療大手Ascensionが、ランサムウェア攻撃グループ「Black Basta」による攻撃を受けた。同グループは、2023年11月3日ごろから偵察活動を開始し、約6ヵ月間、攻撃計画と多数の試行を繰り返していた。最終的に、従業員が会社のデバイスに、正規のファイルをダウンロードしたつもりで悪意のあるファイルをダウンロードしてしまったことで、同社システムへの不正なアクセスが開始された。この攻撃は、Ascentionの電子健康記録(EHR:Electronic Health Record)システム「Mychart」、検査や処置、投薬等を指示する際に使用するシステム、電話に影響を与え、同社は一部のデバイスをオフラインにして、復旧に努めた。従業員は患者記録にアクセスできなくなったため、手続きや投薬内容を紙で管理しなければならなくなった。また、緊急性の低い選択的処置、検査、予約の一時停止や、トリアージの遅れを避けるためにその他の医療施設へ救急医療サービスの振り分けも行った。米国に136ある同社の病院の大部分が影響を受け、EHRシステムへのアクセスを復旧し、通常業務を再開するまでに約6週間を要した。また、インシデント調査の結果、攻撃者がネットワーク全体でおよそ2万5千台あるサーバーのうち7台のみにアクセスし、そこから約560万人分の患者と従業員の個人情報及び医療データを窃取していたことが分かった。これには、医療情報(医療記録番号、サービス提供日、検査の種類、または処置コード等)、支払い情報(クレジットカード情報または銀行口座番号等)、保険情報(メディケイド/メディケアID、保険請求等)、政府発行の身分証明書情報(社会保障番号、納税者番号、運転免許証番号、パスポート番号等)、及びその他の個人情報(生年月日や住所等)が含まれている。しかし、患者の全記録が保管されているEHRシステムやその他の臨床システムからデータが窃取された証拠は一切なかった。同社は2024年12月19日から個人情報が窃取された可能性のある個人への通知を開始し、24ヵ月間無料の信用監視及びアイデンティティ保護サービスを提供している。2025年2月に流出した攻撃グループのチャットメッセージによると、攻撃を実施した後、誰かが死亡してしまうかもしれないリスク、身代金の獲得、法執行機関や諜報機関からのハッキングや制裁等の懸念等、グループのメンバー間で議論があった。最終的に、攻撃グループは復号化ツー

ルを無料で提供し、窃取したデータを削除した※201。

海外と比較すると、公表されている国内の事例は少ないが、2024年には重大なインシデントが発生した。2024年5月19日、岡山県岡山市の地方独立行政法人岡山県精神科医療センター（病床数255、精神科・児童精神科・心療内科を診療科目として持つ医療機関）の電子カルテを含む総合情報システムがランサムウェア攻撃を受けた。5月19日16時ごろに電子カルテが使用できなくなり、システム担当者が速やかに対応し、電子カルテのベンダーもリモート及び現地で復旧・調査にあたった。調査の結果、翌20日6時15分ごろに、ランサムウェア攻撃による障害であることが確認され、直ちに病院ネットワークを停止し、厚生労働省、岡山県、岡山市、岡山県警察本部に報告した。20日の診療は急遽紙カルテを運用して継続した。同センターは、攻撃者との連絡、交渉及び身代金の支払いは行わず、自力で復旧する方針を固め、専門家の助言を仰ぎ、復旧を目指したが、完全復旧には約3ヵ月を要した。また、6月7日に、岡山県警察から、同センターからの個人情報の漏えいを確認したとの連絡があった。確認したところ、サーバーの共有フォルダーに保存された、氏名、住所、生年月日、病名等を含む最大4万人分の個人情報を含む文書であることが推定された。確認された攻撃者の初期侵入は2024年5月13日2時41分で、その後、病院内のネットワークのスキャン、バックアップデータの探索と破壊、Active Directoryに登録されたサーバー・端末ユーザー、コンピューター等の情報の窃取、ウイルス対策ソフトの停止と削除等を周到に実施した上で、5月19日13時10分ごろから電子カルテシステム等の暗号化が行われた。被害は、電子カルテシステム等の仮想サーバー23台と仮想用共有ストレージ1台、仮想基盤用物理サーバー3台、その他の物理サーバー6台、病院情報システム端末244台の暗号化によるシステム稼働障害と仮想用共有ストレージのデータ全喪失だった。侵入の原因は複数が考えられるが、保守用VPN装置の脆弱性の放置、推測可能なID・パスワードの使用が考えられ、水平展開及び暗号化の原因は、推測可能なID・パスワードが使いまわされ、病院内のコンピューターにすべて共通の値が設定されていたことに加え、一般ユーザーにも管理者権限を付与していたことによるウイルス対策ソフトの無効化と考えられる。また、保守用VPN装置への接続元のIPアドレスに制限がなく、インターネット上から誰でも攻撃が可能であった※202。

(g) 生産や重要サービスに影響を与えたサイバー攻撃の事例

2024年も、制御システムにおいて最も重要視される「可用性（Availability）」に影響を与えたインシデントが、世界中で相次いだ。制御システムに攻撃が及んでいなくても、停止に至った事例が多く、これはITとOT（制御・運用技術）の連携が緊密化しているためと考えられる。

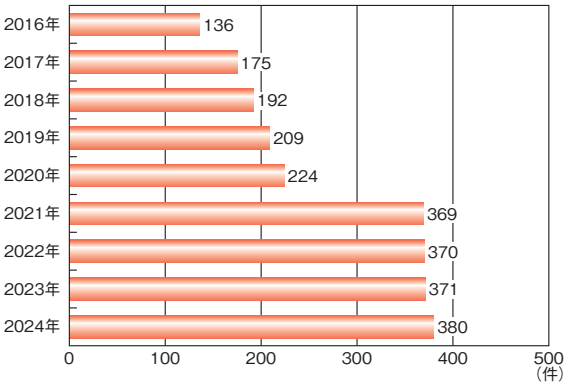
表1-2-5（次ページ）に、2024年に公にされた、生産や重要サービスに影響を与えたサイバー攻撃のインシデント事例を示す。

(2) 制御システムの脆弱性・脅威の動向

本項では、2024年に見られた、制御システムの脆弱性及び脅威の動向について述べる。

(a) 脆弱性の動向

2024年も、制御システムの脆弱性が多く公開された。制御システムの脆弱性を収集・公開している代表的な組織である米国国土安全保障省（DHS：Department of Homeland Security）のCISAが、2024年に公開した制御システムの脆弱性に関するアドバイザリー（ICS Advisory）は380件で、2023年の371件からほぼ横ばいであった（図1-2-16）。



■図1-2-16　CISAが公開した脆弱性アドバイザリーの件数（2016～2024年）
（出典）CISAの公開情報※213を基にIPAが作成

(b) 脅威の動向

2024年の脅威の動向としては、2023年に引き続き、ランサムウェア攻撃の増加が挙げられる。

米国のOTセキュリティベンダーであるDragos, Inc.によると、2024年に産業組織に対するランサムウェア攻撃は87%増加し、ランサムウェア攻撃グループのリークサイト上で機密データが公開された産業組織は1,693に上ったという※214。また、米国のForescout Technologies,

被害企業の分類	発生国	発生年月（報道年月）	内容・影響・被害
水道サービス	米国	2024 年 1 月	都市水道サービスを提供する Veolia North America, LLC が、ランサムウェア攻撃を受け、オンラインの支払いサービスが停止した※203。
電池メーカー	ドイツ	2024 年 2 月	Varta AG がサイバー攻撃を受け、封じ込めのために IT システムをシャットダウンしたため、五つの生産工場の生産が停止した※204。
鉄鋼メーカー	ドイツ	2024 年 2 月	ThyssenKrupp AG がサイバー攻撃を受け、特定のアプリケーションやシステムが一時的にオフラインになった。鉄鋼の生産及び研究開発に関与しているザールラントの工場で生産が停止した※205。
ビール醸造メーカー	ベルギー	2024 年 3 月	Duvel Moortgat がランサムウェア攻撃を受けた。3 月 6 日午前 1 時半に、ランサムウェアを検知し、すぐに醸造所の生産を停止した※206。
プリント基板組み立てメーカー	米国	2024 年 5 月	Key Tronic Corporation が、ランサムウェア攻撃グループ「Black Basta」による攻撃を受け、メキシコと米国での業務を 2 週間停止した。1,700 万ドル（約 25 億 5,000 万円）以上の損害を被った※207。
フォークリフトメーカー	米国	2024 年 6 月	Crown Equipment Corporation がサイバー攻撃を受け、IT システムをシャットダウンしたため、工場での製造が停止した。機械の配送もできない状態となり、従業員は出勤時間の記録やサービスマニュアルへのアクセスができなくなった※208。
家具製造・販売会社	米国	2024 年 7 月	Bassett Furniture Industries, Inc. がランサムウェア攻撃を受けた。一部のシステムの停止を含む封じ込め対策の結果、製造施設の操業が停止した※209。
電機メーカー	日本	2024 年 10 月	カシオ計算機株式会社がサイバー攻撃を受け、システム障害が発生し、一部のサービスが提供できなくなった。修理依頼商品の配送に大幅な遅れが生じ、多くの滞留が発生した。個人向け製品の修理品受付を一時的に停止した※210。
上下水道ユーティリティ	米国	2024 年 10 月	American Water Works Company, Inc. がサイバー攻撃を受け、一部のシステムをシャットダウンした。顧客データを保護するために顧客ポータルサービスをオフラインにした※211。
地域交通サービス	米国	2024 年 12 月	ピッツバーグ地域交通局がランサムウェアによる攻撃を受け、19 日朝に鉄道サービスが一時的に混乱（報道によると 20 分以上遅延）した※212。

■表 1-2-5　2024 年に公にされた、生産や重要サービスに影響を与えたサイバー攻撃のインシデント事例

Inc. によると、OT/ICS を標的とした攻撃の 20% 以上がエンジニアリングワークステーション（EWS：アプリケーション開発やシステム及び機器の構成、保守、診断のために産業分野でよく使用されている高性能コンピューター）を標的としていたという。多くの EWS は、ICS ベンダーが提供する特殊なソフトウェアツールだけでなく、サポートが終了した古い OS を実行しているオンプレミス機器であるため、サイバー攻撃の格好の標的となっている※215。

2024 年 4 月には、制御システムを標的とする新たな二つのマルウェアが、ロシア・ウクライナ戦争に関連して確認された。また 12 月には、IoT 及び OT デバイスを標的とするようカスタマイズされたマルウェアが確認された。それらの概要を以下に示す。

（ア）Fuxnet

イスラエルのサイバーセキュリティ企業 Claroty Ltd. によると、ウクライナ保安庁が関与しているとされるハッキンググループ「Blackjack」が 2024 年 4 月第 2 週に実施した、ロシアの下水道ネットワークの通信システムを管理する地方自治体組織 Moscollector への攻撃で、破壊的な制御システムマルウェア「Fuxnet」が使用された。このマルウェアは、センサーが収集した産業用データにインターネットアクセスを提供するセンサーゲートウェイの破壊コンポーネント、及びセンサーへ M-Bus（Meter-Bus）※216 リクエストを大量送信する DoS 攻撃コンポーネントの二つの主要コンポーネントから構成されている。同攻撃グループの主張によると、センサーゲートウェイ 2,659 台を攻撃し、そのうち約 1,700 台の攻撃に成功した。そして、空港、地下鉄システム、ガスパイプライン等の重要インフラに関連するものを含むロシア企業 AO SBK 製のセンサーやコントローラーをファジング（意図的に例外的な動作を発生させ、バグや脆弱性を発見する手法）し、機能を停止させた。このマルウェアはデバイスに侵入すると、重要なファイルやディレクトリの削除、リモートからの復旧を妨げるためのリモートアクセスサービスのシャットダウン、他のデバイスとの通信を妨げるためのルーティングテーブル情報の削除を開始する。その後、ファイルシステムを削除し、デバイスのフラッシュメモリーを書き換え、NAND 型メモリーチップを物理的に破壊し、再起動を阻止しようとする。また、マルウェアの実行中、M-Bus のチャネルに任意のデータを繰り返し書き込む。これにより、センサーとセンサーゲートウェイはデータの送受信ができなくなる※217。

（イ）FrostyGoop

Dragos Inc. が、ウクライナのサイバーセキュリティ状況センターによって提供された 2024 年 1 月のウクライナ西部の都市リヴィウの地域エネルギー企業に対するサイバー攻撃の詳細を分析した結果、ICS を標的とするマルウェア「FrostyGoop」が使用されていたことを同年 4 月に発見した。このマルウェアは、OT の運用に影響を与えるために、Modbus TCP 通信を利用する初めてのマルウェアである。Modbus TCP は、PLC（Programmable Logic Controller）向けの通信プロトコル Modbus を TCP/IP に拡張した、インターネット環境でのメッセージのやり取りが可能なプロトコルである。

攻撃を受けたエネルギー企業のネットワーク資産は、ルーター、管理サーバー、地域暖房システムコントローラーで構成されていたが、ネットワーク内で適切にセグメント化されておらず、攻撃を容易にしてしまった。攻撃者は、攻撃者のホストから地域暖房システムコントローラーに Modbus コマンドを直接送信し、コントローラーのファームウェアをダウングレードし、監視機能のないバージョンを展開した。コントローラーを破壊しようとはせず、間違った測定値をコントローラーに報告させ、システムの誤作動と顧客への暖房供給の停止を引き起こした。このエネルギー企業の施設は、リヴィウ都市圏の 600 棟以上のアパートに電力を供給し、顧客にセントラルヒーティングを提供していたが、インシデントの復旧にはほぼ 2 日間を要したため、その間、居住者は氷点下の気温に耐えなければならなかった。Modbus は、ほぼすべての産業分野のレガシーシステムや最新システムに組み込まれているため、Modbus TCP プロトコルを介して ICS と通信し、これらのデバイス上のデータを読み取ったり変更したりするコマンドを送信できるこのマルウェアの能力は、重要なサービスやシステムを混乱させ、侵害する潜在的リスクが広く存在することを示している。現在、世界中で 4 万 6,000 以上のインターネットに公開された ICS デバイスが Modbus TCP を介して通信を行っている[※220]。

（ウ）IOCONTROL

イランのイスラム革命防衛隊サイバー電子司令部と関連があるとされるサイバー攻撃グループ「CyberAv3ngers」が、イスラエルと米国の重要インフラで使用されている IoT デバイスや OT/SCADA[※219] システムを侵害するために、新たなカスタムビルドのマルウェア「IOCONTROL」を使用していたことをイスラエルのサイバーセキュリティ企業 Claroty Ltd. が 2024 年 12 月に発見した。このマルウェアは、ルーター、PLC、HMI、IP カメラ、ファイアウォール、燃料管理システム等、様々なベンダーやデバイスタイプに適応するためにモジュール構成を使用しており、幅広いシステムアーキテクチャを標的にしている。IOCONTROL は、IoT 及び OT デバイスの脆弱性を悪用し、ポート 8883 を介した MQTT プロトコルを使って攻撃者の C&C サーバーと通信する。また、感染したデバイスの詳細情報の収集、リモートコード実行、自己削除、ポートスキャン等の機能を持つ。CyberAv3ngers の攻撃活動は、イスラエルとイランの間の地政学的な対立の延長線上にあるもので、研究者らは、このマルウェアは国家によるサイバー兵器であり、重要インフラに深刻な混乱を引き起こす可能性があると報告している[※220]。

(3) 対策

情報セキュリティには、「機密性（Confidentiality）」「完全性（Integrity）」「可用性（Availability）」の三つの基本要素があり、情報システムのセキュリティにおいては機密性（=許可された人だけが情報にアクセスできること）が最も優先度が高く、その後に完全性、可用性が続く。しかし、制御システムのセキュリティにおいては可用性（=システムを停止しないこと）が最優先され、次に完全性、そして機密性が続く。従って、できる限り可用性を損なわないまま、完全性、機密性を保つことが求められる。また、「健康（Health）」「安全性（Safety）」「環境への影響（Environment）」を考慮することも重要である。

実効的なセキュリティ対策を実施するためには、保護する資産の明確化とそれらに対する脅威や脆弱性の評価によってリスクを算定するリスク分析が、非常に重要で不可欠である。IPA では、セキュリティリスク分析の全体像の理解を深め、その取り組みを促すこと及びセキュリティリスク分析を具体的に実施するための手順や手引きを示すことを目的に「制御システムのセキュリティリスク分析ガイド[※221]」を公開しているので、参考にされたい。

ICS や OT のセキュリティ対策では、以下のようなポイントが重要である。

- ネットワーク分離とトラフィック制限
  - IT と OT のネットワークを適切に分離する。
  - VLAN やファイアウォールを活用し、不要なトラフィックを制限する。
- 資産管理と脆弱性管理
  - OT ネットワーク内のすべての資産を可視化（アセットマネジメント）する。
  - ICS/OT 機器の脆弱性を定期的に評価し、パッチ

（修正プログラム）管理を適切に実施する（ただし、OT 環境ではパッチ適用が難しい場合があるため、仮想パッチ（ソフトウェアへパッチを適用するのではなく、脆弱性の悪用をネットワークレベルで防止する）等の代替策を検討する）。

- 侵入検知と監視
  - OT 専用の IDS/IPS を導入し、異常検知を実施する。
  - ログ管理と SIEM（Security Information and Event Management：ログデータを収集し、監視・分析・通知する技術）を活用し、異常な挙動を監視する。
- アクセス制御と認証強化
  - リモートアクセスを制限（必要最小限のユーザーにのみ許可）する。
  - 多要素認証を導入する。
  - デバイスごとのアクセス権限を最小化し、不要な管理者権限を排除する。
  - デバイスのデフォルトパスワードの使用を禁止する。
- 物理的セキュリティ
  - 制御室やサーバールームの物理的アクセス制御を導入する。
  - 監視カメラや入退室管理システムを導入する。
- インシデント対応計画
  - インシデント対応の手順を事前に策定する。
  - ICS/OT セキュリティに対応できる CSIRT を設置する。
- サプライチェーンのリスク管理
  - ベンダーやサードパーティーのセキュリティ評価を実施する。
  - ICS/OT 機器・ソフトウェアの導入前評価と安全性確認を実施する。
- セキュリティ教育とトレーニング
  - セキュリティトレーニングを実施する。
  - ICS/OT 向けのサイバー演習や攻撃シミュレーションを実施する。

1.2.6 IoTに対する脅威

IoT（Internet of Things）は、様々な「モノ」をインターネットに接続する技術である。セキュリティ設定が不十分なまま、あるいは脆弱性を有したままインターネットに接続されたコンピューター以外の機器（IoT 機器）に対するサイバー攻撃が継続して観測されている。また、マルウェアに感染した IoT 機器がボットネットを形成し、DDoS 攻撃を行うことでインフラが機能停止する被害も発生している。

本項では、IoT に対する脅威の動向を、マルウェア感染と感染機器悪用の実態、IoT 機器に対する脅威、IoT を狙うマルウェア、サプライチェーンリスクと EOL（End-of-life）のリスクの四つの観点から紹介する。また、それらの脅威への対策について述べる。なお、紙面の都合で、セキュリティ機器（セキュリティ機能を提供するためにネットワークへ接続する機器）及び産業用 IoT（IIoT：Industrial IoT）機器については、原則として対象外とする。

(1) 脆弱な IoT 機器のマルウェア感染と感染機器悪用の実態

IoT に対する脅威動向の概説として、脆弱な IoT 機器とマルウェア感染の実態、サイバー攻撃による感染機器悪用の実態について、官民連携によるセキュリティ対策強化の取り組みやセキュリティベンダーによる公開情報から考察する。

(a) 国内における実態調査と注意喚起

総務省、NICT 及び一般社団法人 ICT-ISAC は、ISP 事業者、IoT 機器メーカー、SIer（System Integrator）等と連携し、IoT 機器のセキュリティ対策向上を推進することにより、サイバー攻撃の発生や、その被害を未然に防ぐためのプロジェクト「NOTICE（National Operation Towards IoT Clean Environment）※222」を継続中である。

2024 年 4 月以降、活動を拡大し、「ID・パスワードに脆弱性がある IoT 機器の調査（特定アクセス行為）」と「既にマルウェアに感染している IoT 機器の情報提供」に加えて、「ファームウェアに脆弱性がある IoT 機器の調査」や IoT 機器のメーカーやその他セキュリティ関係機関等との連携強化に取り組んでおり、IoT 機器の観測状況として、以下に示す統計情報を公開している。

①容易に推測可能な ID やパスワードを使用しているため、攻撃者による管理者権限の乗っ取りやサイバー攻撃への加担の危険性がある IoT 機器（1 ヵ月の合計件数）

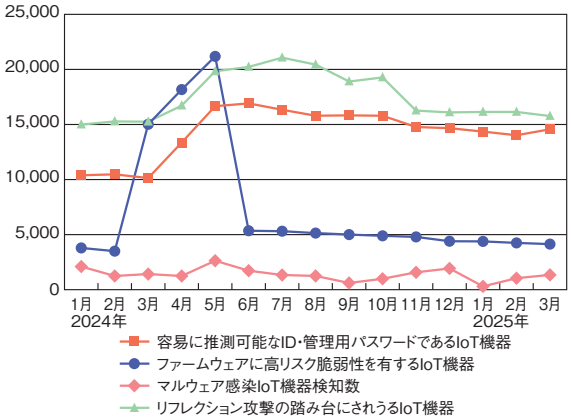
②ファームウェアにおいて第三者に不正利用される危険性がある高リスクの脆弱性を有する IoT 機器（1 ヵ月の合計件数）

③マルウェアに既に感染していると推定され、サイバー攻撃に加担させられているおそれがある IoT 機器の

検知数（1日あたりの合計件数の当月内最大値、IPアドレスが変動している場合は重複して計上）

④リフレクション攻撃の踏み台にされうるおそれがあるIoT機器の検知数（1ヵ月の合計件数）

2025年3月の時点で月1.25億件のIoT機器に対して観測を実施しており、2024年1月から2025年3月までの観測結果※223を図1-2-17に示す。



■図1-2-17　NOTICEプロジェクトの観測状況の推移
（出典）NOTICEサポートセンター「最近の観測状況※224」を基にIPAが作成

観測で発覚した危険性の高いIoT機器の管理者・利用者に対しては、ISP経由での電子メールまたは郵便を用いた通知により、注意喚起を実施している。

（b）国内における攻撃の観測

IIJ社が国内における攻撃の観測情報及び分析結果による月次観測レポートを公開している※225。IoT機器に対する攻撃として、以下に示す攻撃の検出が報告されている。

- Realtek Jungle SDKにおけるコマンドインジェクションの脆弱性（CVE-2021-35394）※226、TP-Link Technologies Co., Ltd.（普联技术有限公司。以下、TP-Link社）製ルーターArcher AX21における非認証コマンドインジェクションの脆弱性（CVE-2023-1389）※227を狙った攻撃が、ほぼ1年間をとおして観測された。
- Netis Technology Co., Ltd.（网是科技股份有限公司）製Netis/Netcoreルーターにおける Default Credentialリモートコード実行の脆弱性※228を狙った攻撃が、2024年1～4月、7月に観測された。
- Zyxel Networks Corporation（合勤科技股份有限公司。以下、Zyxel社）製ルーター等のファームウェアで使用されている、UNIX IFS Shellにおけるリモートコード実行の脆弱性※229を狙った攻撃が2024年1～2月に観測された。

（c）感染機器のサイバー攻撃への悪用の実態

サイバー攻撃者がマルウェア感染させたIoT機器の主な悪用方法は、DDoS攻撃である。DDoS攻撃対策サービス（保護・軽減）を提供するCloudflare社がマルウェア感染したIoT機器を悪用した攻撃の実態を報告している。

- 2024年第1四半期（1～3月）には、450万件（2023年合計の32%）の攻撃を軽減した。最大の攻撃はアジアのホスティング事業者を狙ったMirai亜種ボットネットによる2Tbpsに達した攻撃であった。HTTP DDoS攻撃（アプリケーション層のHTTPプロトコルを標的とした攻撃）の100件に4件、L3/4 DDoS攻撃（ネットワーク層／トランスポート層を標的とした攻撃）の100件に2件はMirai亜種ボットネットによるものであった※230。
- 2024年第2四半期（4～6月）には、400万件の攻撃を軽減したが、Mirai亜種ボットネットによる数値は公開されていない※231。
- 2024年第3四半期（7～9月）には、攻撃数が急増して600万件近くの攻撃を軽減した※232。9月初旬から発生したL3/4 DDoS攻撃では最大3.8Tbpsを65秒間防御した。この高パケットレート攻撃はMikroTik製IoT機器やDVR（Digital Video Recorder）等、高ビットレート攻撃はASUSTeK Computer Inc.（華碩電腦股份有限公司）製ルーターが発生源と考えられている※233。
- 2024年第4四半期（10～12月）には、690万件の攻撃を軽減した。Mirai亜種ボットネットによる攻撃がL3/4 DDoS攻撃全体の6%を占めた。10月29日には、1万3,000台以上のIoT機器から過去最大となる5.6TbpsのUDP DDoS攻撃が80秒間発生した※234。

また、DDoS攻撃対策サービスを提供するGSL Networks Pty Ltdは、2024年8月にピーク時3.15Gパケット／秒のDDoS攻撃を軽減した。Korea Telecomネットワークに属するMAXTECH MAX-G866acルーター等5,253台のほか、DrayTek Vigorルーターや Hikvision IPカメラ等のIoT機器がボットとして検出されている※235。

2024年10月29日、DDoS攻撃等への悪用のため

に構築されるボットネットにおいて、VPN 技術と、マルウェアに感染した IoT 機器（ルーター、産業用制御システム、医療機器、冷蔵庫等）で構成されるボットを組み合わせて、攻撃者のネットワークをメッシュ化、難読化した ORB ネットワークの調査結果が報告された※236。2024 年 9 月 18 日、FBI、Cyber National Mission Force（CNMF）と米国国家安全保障局（NSA：National Security Agency）は、中国を拠点とするサイバー攻撃者による ORB ネットワークの活動に関するアドバイザリーを共同で公開した※111。

(2) IoT 機器に対するセキュリティ脅威の動向

サイバー攻撃の対象となる IoT 機器の観点から、2024 年に観測されたセキュリティ脅威の動向を紹介する。

(a) ルーターに対する脅威

マルウェアを感染させて機器を乗っ取り、第三者への攻撃に悪用する目的に合致するルーターにおいて、多数の脆弱性が報告されている。2024 年に発生したルーターに対する主な脅威を表 1-2-6 に示す。なお、表 1-2-6 ～表 1-2-8 において「EOL」列のチェックマークは、製品ライフサイクルが終了して脆弱性対応が行われない EOL 製品の脆弱性であることを示す。

(b) NAS に対する脅威

機器の乗っ取りに加えて、ランサムウェア感染による身

ベンダー	脅威の概要	EOL
D-Link Corporation（友讯科技股份有限公司）	2024 年 1 月 20 日、DIR-859 の脆弱性（CVE-2024-0769）が公開※237。前日の 19 日、D-Link Corporation（以下、D-Link 社）は使用中止を呼びかけていた※238。6 月 25 日、同脆弱性の積極的な悪用の観測が報告※239。	√
	2024 年 1 月 16 日、DIR-822 の脆弱性が発見者から D-Link 社へ開示。同月 30 日、D-Link 社は使用中止を呼びかけた※240。2 月 6 日、脆弱性（CVE-2024-25331）の詳細が公開※241。	√
	2024 年 5 月 14 日、DIR-X4860 のゼロデイ脆弱性が公開※242。D-Link 社が応答しないため、PoC（Proof of Concept）エクスプロイト※243 も合わせて公開。	
	2024 年 5 月 16 日、CISA は DIR-600 の脆弱性（CVE-2014-100005）及び DIR-605 の脆弱性（CVE-2021-40655）を KEV※244 に追加※245。	√
	2024 年 6 月 17 日、TWCERT/CC（Taiwan Computer Emergency Response Team/Coordination Center：台灣電腦網路危機處理暨協調中心）は複数の Wi-Fi ルーター機種（E15、E30、G403、G415、G416、M15、M18、M30、M32、M60、R03、R04、R12、R15、R18、R32）における非公開の工場テスト用バックドアの存在を、深刻な脆弱性（CVE-2024-6045）としてアドバイザリーを公開※246。	
	2024 年 7 月 7 日、DIR-823X の脆弱性（CVE-2024-39202）が PoC エクスプロイトとともに公開※247。同月 19 日、D-Link 社は Hot-Fix（β版ファームウェア）を公開※248。	
	2024 年 9 月 1 日、D-Link 社は 4 件の脆弱性（CVE-2024-41622、CVE-2024-44340～44342）が公開された DIR-846W の使用中止を呼びかけた※249。	√
	2024 年 9 月 16 日、TWCERT/CC は DIR-X5460、DIR-X4860 及び COVR-X1870 の 5 件の深刻な脆弱性（CVE-2024-45694 ～ 45698）を公開※250。同日、D-Link 社は更新ファームウェアを公開※251。	
	2024 年 9 月 30 日、CISA は DIR-820 の脆弱性（CVE-2023-25280）を KEV に追加※252。	√
TP-Link Technologies Co., Ltd.（普联技术有限公司）	2024 年 1 月 31 日、Archer AX3000、Archer AX5400、Archer AXE75、Deco X50、Deco XE200 等の深刻な脆弱性（CVE-2024-21833、同月 9 日 JPCERT/CC から公開※253）について、詳細な分析結果が公開※254。	
	2024 年 5 月 26 日、Archer C5400X の深刻な脆弱性（CVE-2024-5035）が公開※255。	
	2024 年 11 月 25 日、Archer AXE75 の深刻な脆弱性（CVE-2024-53375）が PoC エクスプロイトとともに公開※256。	
NETGEAR, Inc.	2024 年 4 月 15 日、NETGEAR, Inc.（以下、NETGEAR 社）は Nighthawk RAX35/RAX38/RAX40 の脆弱性（CVE-2023-27368）を更新ファームウェアとともに公開※257。	
	2024 年 6 月 6 日、WNR614 の 6 件の深刻な脆弱性（CVE-2024-36787～36790、CVE-2024-36792、CVE-2024-36795）が公開※258。	√
	2024 年 7 月 11 日、NETGEAR 社は Nighthawk XR1000 の脆弱性（PSV-2023-0122）及び Nighthawk AX6（Wi-Fi ケーブルモデムルーター CAX30）の脆弱性（PSV-2023-0138）を更新ファームウェアとともに公開※259。	
Linksys Holdings, Inc.	2024 年 5 月 3 日及び 6 日、E5600 の 2 件の脆弱性（CVE-2024-33788 ～ 33789）が PoC エクスプロイトとともに公開※260。	

■表 1-2-6　2024 年に発生したルーターに対する主な脅威（次ページに続く）
（出典）各参考文献を基に IPA が作成

ベンダー	脅威の概要	EOL
Linksys Holdings, Inc.	2024 年 5 月 7 日、EA7500 の深刻な脆弱性（CVE-2023-46012）が PoC エクスプロイトとともに公開※261。	
DrayTek Corporation（居易科技中国分公司）	2024 年 9 月 3 日、CISA は VigorConnect の 2 件（CVE-2021-20123 ～ 20124）の脆弱性を KEV に追加※262。	
	2024 年 9 月 30 日、CISA は Vigor3900、Vigor2960 及び Vigor300B の脆弱性（CVE-2020-15415）を KEV に追加※252。	
	2024 年 10 月 28 日、Vigor2960 の脆弱性（CVE-2024-48074）が PoC エクスプロイトとともに公開※263。	
	2024 年 12 月 27 日、Vigor2960 及び Vigor300B の脆弱性（CVE-2024-12987）が PoC エクスプロイトとともに公開※264。インターネット上の 66,000 台の機器が影響を受けると指摘。	
ASUSTeK Computer Inc.（華碩電脳股份有限公司）	2024 年 6 月 14 日、TWCERT/CC は ZenWiFi XT8、ZenWiFi XT8 V2、RT-AX88U、RT-AX58U、RT-AX57、RT-AC86U、RT-AC68U の 2 件の脆弱性（CVE-2024-3079 ～ 3080）を公開※265。	
	2024 年 6 月 14 日、TWCERT/CC は複数のルーター機種（一部は EOL）の脆弱性（CVE-2024-3912）を公開※266。	√
GL Technologies (Hong Kong) Limited	2024 年 8 月 1 日、GL Technologies (Hong Kong) Limited は複数の Wi-Fi ルーターの 6 件の脆弱性（CVE-2024-39225 ～ 39229、CVE-2024-3661）に対するアドバイザリーを公開※267。	
LevelOne（Digital Data Communications GmbH）	2024 年 7 月 8 日、WBR-6013 の 2 種類の脆弱性（CVE-2023-46685、CVE-2023-49593）が公開※268。前者は、説明書に記載のない telnetd※269 のパスワードがハードコーディングされているという致命的な脆弱性だが、LevelOne はファームウェアの修正を拒否。	√
QNAP Systems, Inc.（威聯通科技股份有限公司）	2024 年 11 月 23 日、QNAP Systems, Inc.（以下、QNAP 社）は同社製ルーター用 OS QuRouter の 2 種類の脆弱性（CVE-2024-48860 ～ 48861）と更新ファームウェアを公開※270	
Telesquare（(주) 텔레스퀘어）	2024 年 4 月 10 日、TLR-2005KSH の脆弱性（CVE-2024-29269）が公開※271。同年 5 月 20 日、同脆弱性の PoC エクスプロイトが公開※272。	
株式会社アイ・オー・データ機器	2024 年 11 月 13 日、UD-LT1 及び UD-LT1/EX の 3 件の脆弱性を公開※273。うち 1 件の脆弱性（CVE-2024-52564）に対応する更新ファームウェアを同時公開。同年 12 月 18 日、残り 2 件の脆弱性（CVE-2024-45841、CVE-2024-47133）に対応する更新ファームウェアを公開。	
セイコーソリューションズ株式会社	2024 年 5 月 13 日、SkyBridge MB-A100/110 及び SkyBridge BASIC MB-A130 の脆弱性（CVE-2024-32850）を更新ファームウェアとともに公開※274。	
センチュリー・システムズ株式会社	2024 年 10 月 31 日、FutureNet NXR-G110、NXR-G060 及び NXR-G050 の各シリーズの脆弱性（CVE-2024-50357）を更新ファームウェアとともに公開※275。	

■表 1-2-6　2024 年に発生したルーターに対する主な脅威（前ページからの続き）
（出典）各参考文献を基に IPA が作成

ベンダー	脅威の概要	EOL
QNAP Systems, Inc.（威聯通科技股份有限公司）	2024 年 1 月 6 日、QNAP 社は NAS 用 OS である QTS 及び QuTS hero の既知の脆弱性（CVE-2023-39296、2023 年 12 月 7 日に技術的詳細と PoC エクスプロイト公開済み※276）のアドバイザリーを更新ファームウェアとともに公開※277。	
	2024 年 2 月 3 日、QNAP 社は NAS 用 OS である QTS、QuTS hero 及び QuTScloud の 4 件の脆弱性（CVE-2023-45025、CVE-2023-39297、CVE-2024-47567 ～ 47568）のアドバイザリーを更新ファームウェアとともに公開※278。同日、NAS 用ファイル同期アプリケーション Qsync Central の脆弱性（CVE-2023-47564）を更新ソフトウェアとともに公開※279。	
	2024 年 2 月 13 日、QNAP 社は NAS 用 OS である QTS、QuTS hero 及び QuTScloud の 2 件の脆弱性（CVE-2023-47218、CVE-2023-50358）のアドバイザリーを更新ファームウェアとともに公開※280。同日、各脆弱性の詳細な解析結果が公開※281。CVE-2023-50358 については、1 月中旬の時点で 289,665 個の異なる IP アドレスを有する脆弱な機器を検出。	
	2024 年 3 月 9 日、QNAP 社は NAS 用 OS である QTS、QuTS hero の 5 件の脆弱性（CVE-2024-21899 ～ 21901、CVE-2024-27124、CVE-2024-32766）を更新ファームウェアとともに公開※282。同年 4 月 27 日、NAS 用リモートアクセスアプリケーション myQNAPcloud、リモートアクセスサービス myQNAPcloud Link の脆弱性（CVE-2024-32764）が更新ソフトウェアとともに追加公開。	

■表 1-2-7　2024 年に発生した NAS に対する主な脅威（次ページに続く）
（出典）各参考文献を基に IPA が作成

ベンダー	脅威の概要	EOL
QNAP Systems, Inc.（威聯通科技股份有限公司）	2024 年 5 月 17 日、NAS 用 OS である QuTS hero 及び QuTScloud における最も深刻な脆弱性（CVE-2024-27130）の PoC エクスプロイトを含む 15 件の脆弱性の詳細が公開※283。同年 4 月 25 日の時点で、QNAP 社はうち 4 件の脆弱性（CVE-2023-50361 ～ 50364）に対する更新ファームウェアを公開済み※284。同年 5 月 21 日、うち 5 件の脆弱性（CVE-2023-21902、CVE-2024-27127 ～ 27130）に対する更新ファームウェアを公開※285。同年 9 月 7 日、新たな 1 件の脆弱性（CVE-2024-21904）に対応することを追記。	
	2024 年 10 月 29 日、QNAP 社は NAS 上で動作するバックアップソリューション HBS 3 Hybrid Backup Sync の脆弱性（CVE-2024-50388）を更新ファームウェアとともに公開※286	
	2024 年 12 月 7 日、QNAP 社は NAS 用 OS である QTS 及び QuTS hero の 8 件の脆弱性（CVE-2024-48859、CVE-2024-48865～48868、CVE-2024-50393、CVE-2024-50402～50403）を更新ファームウェアとともに公開※287。同日、NAS 用ラインセス管理ソフトウェア License Center の脆弱性（CVE-2024-48863）を更新ソフトウェアとともに公開※288。	
D-Link Corporation（友讯科技股份有限公司）	2024 年 4 月 3 日、DNS-340L、DNS-320L、DNS-327L 及び DNS-325 を含む複数の EOL 機種の脆弱性（CVE-2024-3273）が公開※289。インターネット上の 92,000 台以上に影響すると指摘。同年 4 月 4 日、D-Link 社は使用中止を呼びかけた※290。同年 5 月 29 日、攻撃者による積極的な悪用の観測が報告※291。	√
	2024 年 11 月 6 日、DNS-320、DNS-320LW、DNS-325 及び DNS-340L を含む複数の EOL 機種の脆弱性（CVE-2024-10914）が公開※292。インターネット上の 61,000 台以上の機器に影響すると指摘。	√
Zyxel Networks Corporation（合勤科技股份有限公司）	2024 年 6 月 3 日、NAS326 及び NAS542 の 5 件の深刻な脆弱性（CVE-2024-29972～29976）が公開※293。同月 4 日、Zyxel 社は 2023 年 12 月末に脆弱性サポートを終了した製品に対して更新ソフトウェアを公開※294。同年 6 月 21 日、Mirai 亜種のボットネットによる積極的な悪用の観測が報告※295。	√
	2024 年 9 月 9 日、NAS326 及び NAS542 の深刻な脆弱性（CVE-2024-6342）が公開※296。同月 10 日、Zyxel 社は 2023 年 12 月末に脆弱性サポートを終了した製品に対して更新ソフトウェアを公開※297。	√
Synology Inc.（群暉科技股份有限公司）	2024 年 10 月 25 日、Synology Inc.（以下、Synology 社）は NAS 用写真管理アプリケーション Synology Photos の脆弱性（CVE-2024-10443 ／ ZDI-CAN-25623）を更新ソフトウェアとともに公開※298。	
Western Digital Corporation	2024 年 9 月 26 日、Western Digital Corporation は My Cloud シリーズの脆弱性（CVE-2024-22170）を更新ファームウェアとともに公開※299	

■表 1-2-7　2024 年に発生した NAS に対する主な脅威（前ページからの続き）
（出典）各参考文献を基に IPA が作成

ベンダー	脅威の概要	EOL
HPE Aruba Networking（Hewlett Packard Enterprise Company）	2024 年 5 月 14 日、HPE Aruba Networking は Wi-Fi アクセスポイント Aruba Access Points の 18 件の脆弱性（CVE-2024-31466 ～ 31483）のアドバイザリーを更新ファームウェアのバージョン情報とともに公開※300。	
Zyxel Networks Corporation（合勤科技股份有限公司）	2024 年 9 月 3 日、Zyxel 社は複数の Wi-Fi アクセスポイント製品の脆弱性（CVE-2024-7261）のアドバイザリーを更新ファームウェアとともに公開※301。	
TP-Link Technologies Co., Ltd.（普联技术有限公司）	2024 年 8 月 19 日、Wi-Fi 中継器 RE365 V1（ファームウェアバージョン V1_180213）の深刻な脆弱性（CVE-2024-42815）が PoC エクスプロイトとともに公開※302。	
GeoVision Inc.（奇偶科技股份有限公司）	2024 年 6 月 17 日、TWCERT/CC は GeoVision Inc. 製 EOL 機器（IP カメラ、ビデオサーバー、DVR 等）の深刻な脆弱性（CVE-2024-6047）のアドバイザリーを公開※303。	√
	2024 年 11 月 15 日、TWCERT/CC は GeoVision Inc. 製 EOL 機器（ビデオサーバー、DVR 等）の深刻な脆弱性（CVE-2024-11120）のアドバイザリーを公開※304。	√
Synology Inc.（群暉科技股份有限公司）	2024 年 6 月 28 日、Synology 社はネットワークカメラ BC500 及び TC500 の 6 件の脆弱性（CVE-2024-39349 ～ 39352、CVE-2023-47802 ～ 47803）のアドバイザリーを更新、詳細情報を更新ファームウェアとともに公開※305。	

■表 1-2-8　2024 年に発生したその他の IoT 機器に対する主な脅威（次ページに続く）
（出典）各参考文献を基に IPA が作成

ベンダー	脅威の概要	EOL
Shenzhen TVT Digital Technology Co., Ltd.（深圳市同為数碼科技股分有限公司）、Provision-ISR、AVISION（虹光精密工業股分有限公司）	2024 年 8 月 1 日、Shenzhen TVT Digital Technology Co., Ltd. 製 TD-2104TS-CL 及び TD-2108TS-HP、Provision-ISR 製 SH-4050A5-5L(MM)、AVISION 製 AV108T 等の各社 DVR 製品の脆弱性（CVE-2024-7339）が公開※306。インターネット上の 408,035 台の機器に影響すると指摘。	√
AVTECH SECURITY Corporation（陞泰科技股份有限公司）	2024 年 8 月 1 日、CISA は AVTECH SECURITY Corporation（以下、AVTECH 社）のネットワークカメラ AVM1203 の脆弱性（CVE-2024-7029）に関するアドバイザリーを、AVTECH 社が CISA の協力要請に応じないこととともに公開※307。同月 28 日、同脆弱性を悪用する Mirai 亜種「Corona」の感染拡大活動が報告※308。後日、AVTECH 社は更新ファームウェア V1024 を提供していること及び CISA と協力予定であることを声明※309。	
Cisco Systems, Inc.	2024 年 5 月 1 日、Cisco Systems, Inc.（以下、Cisco 社）は IP 電話機 Cisco IP Phone 6800/7800/8800 の各シリーズ及びビデオ電話機 Cisco Video Phone 8875 の 3 件の脆弱性（CVE-2024-20376、CVE-2024-20378、CVE-2024-20357）のアドバイザリーを更新ファームウェアとともに公開※310。	
	2024 年 8 月 7 日、Cisco 社は IP 電話機 Cisco Small Business SPA300/SPA500 シリーズの Web ベース管理インターフェースの 5 件の脆弱性（CVE-2024-20450 ～ 20454）を公開し、EOL 製品のため更新ソフトウェアを提供しないと声明※311。	√
Avaya Inc.	2024 年 6 月 11 日、Avaya Inc. は Avaya IP 電話機の 2 件の脆弱性（CVE-2024-4196 ～ 4197）を公開し、ファームウェアの更新を呼びかけた※312。	
LG Electronics Inc.（LG 전자 주식회사）	2024 年 4 月 9 日、スマートテレビ LG43UM7000PLA、OLED55CXPUA、OLED48C1PUB 及び OLED55A23LA に搭載された webOS の 4 件の脆弱性（CVE-2023-6317 ～ 6320）が公開※313。インターネット上に 91,000 台以上の機器が接続されていることを確認。	
キヤノン株式会社	2024 年 2 月 5 日、SOHO 向け多機能プリンター及びレーザープリンターの 7 件の脆弱性（CVE-2023-6229 ～ 6234、CVE-2024-0244）を公開※314。	
	2024 年 3 月 8 日、SOHO 向け多機能プリンター及びレーザープリンターの脆弱性（CVE-2024-2184）を公開し、ファームウェアの更新を呼びかけた※315。	
シャープ株式会社、東芝テック株式会社	2024 年 10 月 25 日、両社の複合機（東芝テック株式会社は北米市場向けのみ）の 9 件の脆弱性（CVE-2024-42420、CVE-2024-43424、CVE-2024-45829、CVE-2024-45842、CVE-2024-47005、CVE-2024-47406、CVE-2024-47549、CVE-2024-47801、CVE-2024-48870）を公開し、提供可能な機種（シャープ製品の一部は EOL）はファームウェアの更新を呼びかけた※316。	√
株式会社リコー	2024 年 2 月 5 日、複合機 P C200SFL 及びレーザープリンター P C200L の 4 件の脆弱性（CVE-2023-50734 ～ 50737）を公開し、ファームウェアの更新を呼びかけた※317。	
	2024 年 4 月 19 日、複合機 P C200SFL 及びレーザープリンター P C200L の 3 件の脆弱性（CVE-2023-50733、CVE-2023-50738 ～ 50739）を公開し、ファームウェアの更新を呼びかけた※318。	
	2024 年 5 月 28 日、複合機及びレーザープリンターの複数機種の脆弱性（CVE-2022-37406）を公開し、ファームウェアの更新を呼びかけた※319。	
	2024 年 7 月 9 日、複合機及びレーザープリンターの複数機種の脆弱性（CVE-2024-39927）を公開し、ファームウェアの更新を呼びかけた※320。	
	2024 年 10 月 31 日、複合機及びレーザープリンターの複数機種における組み込み Web サーバーの脆弱性（CVE-2024-47939）を公開し、ファームウェアの更新を呼びかけた※321。	
セイコーエプソン株式会社	2024 年 9 月 30 日、インクジェットプリンター、レーザープリンター及びスキャナー等の複数機種におけるブラウザー経由の管理ツール（組み込み Web サーバー）Web Config における脆弱性（CVE-2024-47295）を公開し、緩和策の適用を呼びかけた※322。	
マツダ株式会社	2024 年 11 月 7 日、2014 ～ 2021 年モデルの Mazda 3 等に搭載された車載インフォテインメントシステム MAZDA CONNECT の CMU（Connectivity Master Unit）における 6 件の脆弱性（CVE-2024-8355 ～ CVE-2024-8360）が公開※323。	

■表 1-2-8　2024 年に発生したその他の IoT 機器に対する主な脅威（前ページからの続き）
（出典）各参考文献を基に IPA が作成

代金要求の脅威が存在する NAS（Network Attached Storage）の脆弱性も引き続き報告されている。2024 年に発生した NAS に対する主な脅威を表 1-2-7（前々ページ）に示す。

(c) その他の IoT 機器に対する脅威

Wi-Fi アクセスポイント／中継器、DVR/NVR（Digital Video Recorder/Network Video Recorder）、ネットワークカメラ、ネットワークプリンター／複合機、コネクテッ

ドカー等の脆弱性が報告されている。2024 年に発生したその他の IoT 機器に対する主な脅威を表 1-2-8（前々ページ）に示す。

(3) IoT を狙うマルウェアの動向

IoT を狙ったマルウェアの観点から、2024 年に観測された脅威の動向を紹介する。

(a) Mirai とその亜種

2016 年 9 月の出現以降、「Mirai」とその亜種の感染活動が継続している。主な観測結果を以下に示す。

- 2024 年 4 月 16 日、Mirai とその亜種、その他のマルウェアによる TP-Link 社製ルーターの脆弱性※227 の悪用が報告された※324。
- 2024 年 5 月 30 日、Mirai 及び Xor.DDoS のソースコードを流用したトロイの木馬（RAT：Remote Access Trojan）型マルウェア Chalubo（ChaCha-Lua-bot）の活動が報告された※325。2023 年 10 月 25 ～ 27 日の 72 時間、単一のインターネット接続事業者の管理下にある SOHO ルーターを攻撃し、約 179,000 台の Actiontec Electronics, Inc. 製ルーター T3200s 及び T3260s のファームウェアを破壊して使用不能とした。
- 2024 年 12 月 17 日、Juniper Networks, Inc. は、複数の顧客において、デフォルトパスワードのままネットワークに接続された同社製 Session Smart Router の Mirai 感染が観測されたため、パスワードの変更等を呼びかけるアドバイザリーを公開した※326。
- 2024 年 12 月 26 日、同年 10 月から 11 月にかけて Mirai の亜種「FICORA」による D-Link 社製ルーターの約 10 年前に発見された脆弱性を悪用する感染拡大攻撃が報告された※327。

(b) 7777-Botnet

2024 年 1 月 18 日、7777-Botnet が TP-Link 社製ルーター、Hangzhou Xiongmai Technology Co., Ltd.（杭州雄迈信息技术有限公司）製ファームウェアを用いた NVR や IP カメラ、Hangzhou Hikvision Digital Technology Co., Ltd.（杭州海康威视数字技术股份有限公司）製ネットワークカメラとその OEM 製品の脆弱性を感染拡大に悪用していることが報告された※328。

(c) Mirai の脆弱性／活動妨害

2024 年 8 月 20 日、Mirai 及びその亜種で発見された脆弱性（CVE-2024-45163）が PoC エクスプロイトとともに公開された※329。マルウェア感染等により乗っ取った IoT 機器を制御する C&C サーバーに対して DoS（Denial of Service）攻撃を実行し、その活動を妨害することが可能であるという。

(4) サプライチェーンリスクと EOL のリスク

IoT 機器の開発に用いられる共通コンポーネントや標準プロトコルに起因する脆弱性から生じるリスク（IoT 機器のサプライチェーンリスク）や、サポートが終了して EOL ステータスにある IoT 機器における脆弱性の発見から生じるリスク（EOL のリスク）が引き続き発生している。

(a) 共通コンポーネントの脆弱性

複数の IoT 機器の開発に用いられているハードウェアやソフトウェアにおける脆弱性の発見は、広範囲にわたる影響やセキュリティ対策の困難性を生じさせている。

- スマートフォンや IoT 機器において無線通信機能を実装するために採用されている MediaTek Inc.（聯發科技股份有限公司。以下、MediaTek 社）製チップセットにおいて、繰り返し脆弱性が発見、公開されている※330。2024 年 3 月 4 日、MediaTek 社は 1 件の脆弱性（CVE-2024-20017）を公開した※331。同年 8 月 30 日、その技術的詳細と PoC エクスプロイトが公開された※332。
- 2024 年 9 月 3 日、Arm Holdings plc は、スマートフォン等においてグラフィックス処理機能を実装するために採用されている同社製 IP コア Mali GPU の脆弱性（CVE-2024-3655）を公開した※333。
- 2024 年 10 月 8 日、CISA は Qualcomm Technologies, Inc. 製 Android 機器用チップセットの脆弱性※334（CVE-2024-43047）を KEV に追加した※335。
- 2024 年 11 月 28 日、リソースが制限された IoT 機器向けリアルタイム OS（RTOS：Real Time OS）であるオープンソース Contiki-NG の 3 件の脆弱性が修正パッチ（修正プログラム）とともに公開された※336。
- 2024 年 4 月 17 日、Linux の主要ディストリビューションで用いられている Gnu C ライブラリ（glibc）の脆弱性（CVE-2024-2961）が公開された。同年 5 月 27 日、6 月 17 日、9 月 30 日に脆弱性の詳細や PHP と組み合わせた悪用方法及び PoC エクスプロイトが公開された※337。
- 2024 年 6 月 24 日、IoT 機器向けリアルタイム OS FreeRTOS 用の TCP/IP スタックであるオープンソース FreeRTOS-Plus-TCP の脆弱性（CVE-2024-38373）が公開された※338。

- 2024 年 12 月 6 日、組み込み機器向け Linux ディストリビューションのオープンソースプロジェクト OpenWrt において、ファームウェア更新（SysUpgrade）サーバーの脆弱性（CVE-2024-54143）が公開された※339。
- 2024 年 8 月 13 日、ビデオ監視システム※340 用オープンソース ZoneMinder の脆弱性（CVE-2024-43360）が PoC エクスプロイトとともに公開された※341。同年 11 月 1 日、別の脆弱性（CVE-2024-51482）が PoC エクスプロイトとともに公開された※342。

(b) 標準プロトコルの脆弱性

2024 年 5 月 14 日、無線 LAN 規格 Wi-Fi の設計上の欠陥に起因する脆弱性（CVE-2023-52424）が公開され、「SSID Confusion Attack」と名付けられた※343。

(c) EOL のリスク

サポートが終了して更新ソフトウェアが提供されない IoT 機器において、新たな脆弱性が数多く発見された（表 1-2-6（49 ページ）～表 1-2-8 参照）。

(5) IoT のセキュリティ対策

マルウェア感染した IoT 機器で構成されるボットネットは驚異的なサイバー攻撃力を備えており（「1.2.6 (1) (c) 感染機器のサイバー攻撃への悪用の実態」参照）、我々が日々利用しているインフラに深刻な障害をもたらすおそれがある。

ここでは IoT 製品・サービスの開発者及び利用者の立場で実施すべき対策を示す。なお、IoT 機器を用いてシステムやサービスを構築して顧客に提供する事業者は、両方の立場での対策実施が必要となる。

(a) 開発者が実施すべき対策

IoT 製品・サービスの開発においては、設計段階からセキュリティを考慮した設計（セキュア・バイ・デザイン）を行うことが重要である※344。想定される脅威に対するセキュリティ機能を実装する際には、リスクアセスメントを実施し、脅威の発生頻度や想定被害からリスクを算定して対応の必要性を判断することが望ましい。

IPA が公開している「脆弱性対処に向けた製品開発者向けガイド※345」では、一般消費者が利用する IoT 機器の開発を行う事業者を対象として、製品開発者が実施すべき脆弱性対処とその開示方法を解説している。また、「IoT 製品・サービス脆弱性対応ガイド※346」では、経営者・管理者を対象として、企業のセキュリティ対応責任の考え方や脆弱性対策が必要な理由等を解説している。

製品を出荷する国・地域によっては、法制度で定められた基準の適合を求められる可能性がある。IPA では、「セキュリティ要件適合評価及びラベリング制度（JC-STAR）※347」の運用を担当しており、2025 年 3 月 25 日から「★ 1 適合ラベル」の申請受付を開始した（「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) 利用者が実施すべき対策

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 –※348」では、IoT 機器（ネット接続製品）の購入（選定）時及び利用時のポイントを紹介している。

- 購入時、安全な IoT 機器を選ぶためのポイント
  - アップデート機能があること
  - 製品のセキュリティに関する最新情報が Web サイトに掲載されていること
  - 問い合わせ先が明記されていること
  - 製品のセキュリティ方針が記載されていること
  - 製品のセキュリティ機能や設定の具体的な記載があること
  - サポート情報（サポート終了期限等）の記載があること
  - 初期化機能（廃棄時の情報消去）があること
- 購入した IoT 機器を安全に利用するためのポイント
  ①購入直後のセキュリティ設定（パスワード変更等）
  ②製品メーカーの Web サイト確認とアップデート
  ③製品のセキュリティ機能（パスワード以外）の使用
  ④不慮の事故に備えたバックアップや設定内容記録
  ⑤使わなくなった製品のネットワークからの遮断
  ⑥サポート終了製品の利用中止・買い換え
  ⑦製品廃棄時の初期化

購入後のルーターやネットワークカメラに関しては、NOTICE プロジェクトの Web サイト※349 に設置時及び利用中に定期的に実施すべき具体的なチェック項目が紹介されている。

1.2.7 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

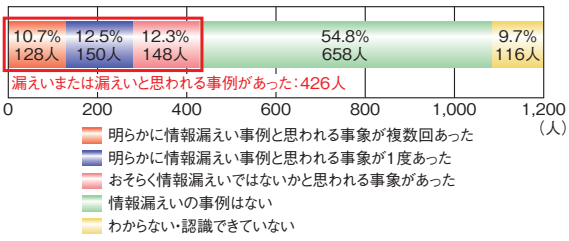
者が退職後に在職中に得ていた情報を漏えいする行為等を含む)、及び消去・破壊等の違法行為と、情報セキュリティに関する内部規程やルールへの違反、ミス等の違法とはいえない行為の両方を内部不正として扱う※350。

内部不正により組織の保有する顧客の個人情報が漏えいして社会的信用が失墜することや、顧客情報や技術ノウハウ等の営業秘密が漏えいして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、内部不正による情報漏えいや毀損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) 内部不正による情報漏えいの状況

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、ランサムウェアによるサイバー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。

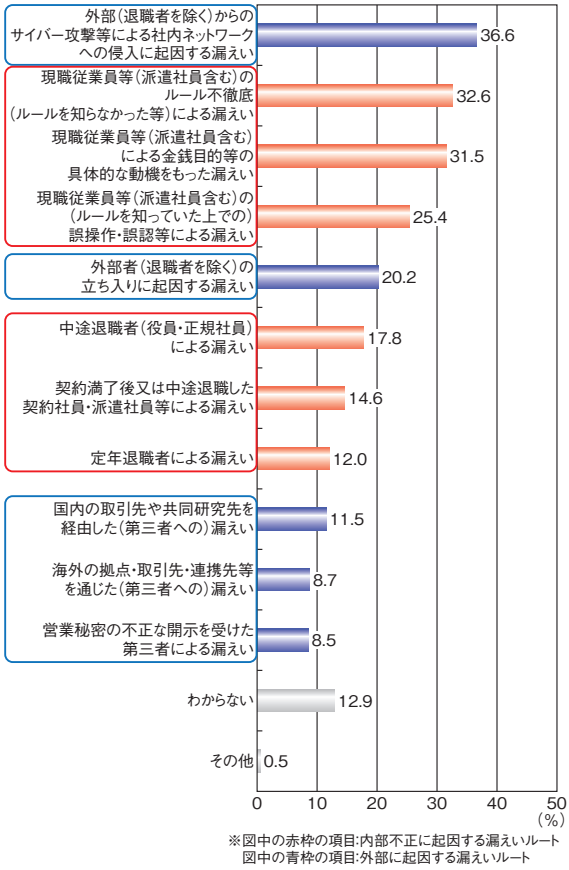
IPA が実施した「企業における営業秘密管理に関する実態調査 2024※351」では、図 1-2-18 に示すように、回答者 1,200 人のうち 426 人 (35.5%) が過去 5 年間の間に営業秘密の漏えいまたは漏えいと思われる事例があったと回答した。



■図 1-2-18　過去 5 年以内の営業秘密漏えいの発生有無
(回答者 1,200 人)
(出典)IPA「企業における営業秘密管理に関する実態調査 2024」を基に編集

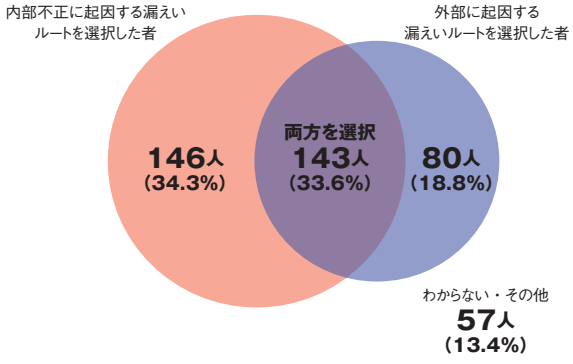
営業秘密の漏えいまたは漏えいと思われる事例があったと回答した 426 人に、複数回答を可として、漏えいのルートを尋ねた結果を図 1-2-19 に示す。図 1-2-19 では、内部不正に起因する漏えいルートを赤枠で、外部に起因する漏えいルートを青枠で示している。

外部からのサイバー攻撃等によるネットワーク侵入に起因する漏えいに次いで、内部不正に起因する漏えいルートである現職従業員等(派遣社員含む)による漏えいが多く、「外部者 (退職者を除く) の立ち入りに起因する漏えい」をはさんで、中途退職者 (役員・正規社員)、契約満了後または中途退職した契約社員・派遣社員等、及び定年退職者による漏えいが多かった。



■図 1-2-19　営業秘密の漏えいのルートの内訳
(回答者 426 人、複数回答)
(出典)IPA「企業における営業秘密管理に関する実態調査 2024」を基に作成

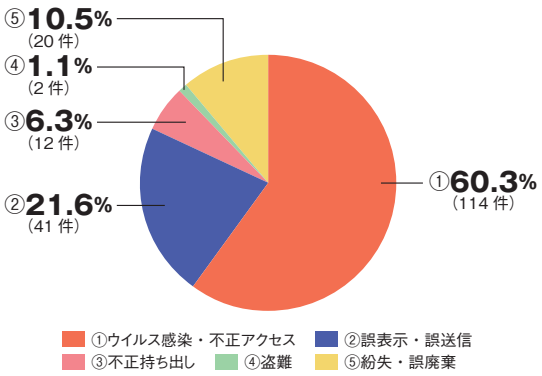
図 1-2-19 の設問への回答を基に回答者を、内部不正に起因する漏えいルートのみを選択した者、外部に起因する漏えいルートのみを選択した者、両方を選択した者、「わからない」「その他」を選択した者に分類した結果を図 1-2-20 に示す。内部不正に起因する漏えいルートのみを選択した者は 146 人 (34.3%)、外部に起因する漏えいルートのみを選択した者は 80 人 (18.8%)、両方



■図 1-2-20　営業秘密漏えい事例回答者のルートによる分類
(回答者 426 人)
(出典)IPA「企業における営業秘密管理に関する実態調査 2024」を基に作成

を選択した者は 143 人（33.6%）だった。

また、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 2025 年 1 月に公開した「2024 年『上場企業の個人情報漏えい・紛失事故』調査」によれば、2024 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 189 件で、そのうち内部不正に相当する「誤表示・誤送信」（41 件）及び「不正持ち出し」（12 件）を合計すると 53 件となり、28.0% を占めていた（図 1-2-21）。



■図 1-2-21　上場企業における個人情報漏えい・紛失の原因（2024 年、n=189）※352

（出典）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』調査」を基に IPA が編集

これらの調査結果は、ランサムウェア等のサイバー攻撃への対策だけでなく、内部不正対策を行うことも、情報漏えいを防ぐために重要であることを示唆している。

(2) 内部不正による情報漏えいの事例と手口

報道等では個人情報漏えいが注目されるが、技術情報を含む営業秘密の漏えいも起きている。中には、外国籍の内部者による日本国外への情報漏えいの事例もある。営業秘密を中心とした内部不正による情報漏えい事例を表 1-2-9 に示す。

内部不正による情報漏えいの手口としては、社用メールアドレスから私用メールアドレスへの送信や、社内のパソコンから記録媒体へのコピー、個人アカウントのクラウドにアップロードする方法等が用いられていることが明らかになっている。

(3) 内部不正による情報漏えいの対策

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。表 1-2-10（次ページ）に対策例を示す※361。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。

報道時期	不正の内容	情報の種別	数	手口	概要
2024 年 3 月	従業員による盗難	営業秘密（技術情報）	500 ファイル超	個人アカウントのクラウドにアップロード	米国で、Google LLC の中国籍元従業員が起訴された。当該従業員が在職時に AI に関する機密情報を盗み、中国企業に横流した等の疑いがある※353。
2024 年 6 月	教員による誤転送	個人情報	約 1 万件	校務用のメールアドレスから私用のメールアドレスに転送する際、宛先を誤指定	筑波大学の教員が転送先を入力する際、アドレスを誤って入力し第三者のメールアドレスを指定していたことにより、1 年超にわたり約 1 万件（このうち、個人情報等が記載されていたものは約 1,200 件）のメールを転送し続けていた※354。
2024 年 8 月	従業員による不正持ち出し	個人情報及び営業秘密（顧客情報）	2万5,000人超分	公開情報なし	東急リバブル株式会社の従業員が退職し同業他社へ転職するにあたり、退職の際に機密保持に関する誓約書を提出させていたにもかかわらず、不動産登記簿に基づく社内資料を不正に持ち出し、その一部を転職先でダイレクトメールの送付に使用した※355。
2024 年 10 月	従業員による不正持ち出し	営業秘密（技術情報）	—	社用のメールアドレスから私用のメールアドレスに送信	TDK 株式会社の従業員が営業秘密にあたる電子部品の開発や材料等に関する情報を不正に持ち出していたことが、同社が当該従業員の退職後に実施した社内調査で発覚した※356。
2025 年 2 月	従業員による不正持ち出し	営業秘密（技術情報）	約6,500件	社内のパソコンから業務用サーバーにアクセスし、記録媒体にコピー	金属加工会社である伊福精密株式会社の従業員が退職する前に、自動車や航空機の部品、主要取引先の品質管理等に関する情報を不正に持ち出した※357。退職後、同業他社に転職していた※358。
2025 年 2 月	研究員による不正持ち出し	営業秘密（技術情報）	—	職場のメールアドレスから送信	国立研究開発法人産業技術総合研究所の元研究員が 2023 年 6 月に逮捕され、2025 年 2 月に有罪判決が下された※359。当該研究員が在職時に、営業秘密にあたるフッ素化合物に関する研究データを、自身の妻が代表を務める中国企業に漏えいした事実による※360。

■表 1-2-9　内部不正の主な事例

担当／主管部署	種類	対策例	内容
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 ※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 ・従業員等が社内ルールを遵守することを規定
		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 1-2-10　内部不正による情報漏えいを防ぐための対策例

また、表 1-2-9（前ページ）に示したように退職時に機密保持契約を締結していても不正な持ち出しを防げていない事例がある。内部不正による情報漏えいは表 1-2-11 に例示した日本の法規制による罰則を科せら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。このような法的な罰則についても、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、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。こういった点について解説した「組織における内部不正防止ガイドライン※367」を IPA から公開しているので、活用いただきたい。

1.2.8 個人を狙う騙しの手口

本項では、個人を狙う騙しの手口について述べる。騙しの手口の代表例としては、サポート詐欺（偽のウイルス感染警告）とフィッシング（メールや SMS の悪用）が挙げられる。

サポート詐欺については、基本的な手口に変化はない一方で、遠隔操作を悪用しネットバンキングを通じて多額の金銭を不正送金されたという相談事例が増加した。これらについて「1.2.8（1）サポート詐欺（偽のウイルス感染警告）」と「1.2.8（2）ブラウザーの通知機能を悪用した偽の警告」で紹介する。

フィッシングについては、メールを悪用した手口（フィッシングメール）の相談が多く、「暗号資産を要求する脅迫メール」に代表される不審メールの相談が続いている。

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※362	個人：10 年以下の拘禁刑若しくは 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※363	個人：1 年以下の懲役または 100 万円以下の罰金 法人：1 億円以下の罰金
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※364	（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 年以下の拘禁刑若しくは 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）※365	軽微な違反：最大 1,000 万ユーロ、または、直前の会計年度における全世界年間売上高の 2% まで、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、直前の会計年度における全世界年間売上高の 4% まで、もしくは、いずれか高額の方

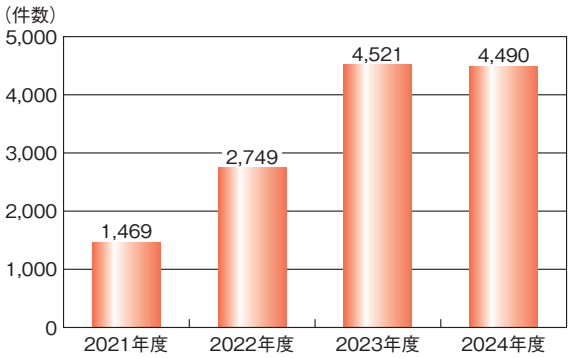
■表 1-2-11　内部不正による情報漏えいに関連する法規制の例※366

また、被害に遭ってはいないが、不審メールの受信そのものを不快と感じて対策を相談することが増えている。これらについて「1.2.8 (3) メールを悪用した手口」で紹介する。また、SMS を悪用した手口も多く、「宅配便業者等をかたる偽 SMS」について「1.2.8 (4) SMS を悪用した手口」で紹介し、最後にこれらの騙しの手口全般への対策を述べる。

なお、これら事例の分類を再整理し、IPA「情報セキュリティ安心相談窓口※368」（以下、安心相談窓口）の活動状況（四半期レポート）として公開している※369。

(1) サポート詐欺（偽のウイルス感染警告）

2024 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 4,490 件となり、過去最高を記録した 2023 年度と同レベルで推移した（図 1-2-22）。サポート詐欺の活動は依然として衰えていない。



■図 1-2-22　サポート詐欺の相談件数の推移（2021 ～ 2024 年度）

サポート詐欺の「手口」、「対処」と「対策」は以下のとおりである。ここで、「対処」は、偽の警告が突然表示された際に行っていただきたいパソコンの操作を記載している。また、被害に遭ってしまった場合の回復措置等についても記載している。「対策」は、この手口の被害に遭わないために、日頃から注意していただきたいことを記載している。

(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 1-2-23）。

②偽の警告で被害者の恐怖心をあおり、「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）。

サポート詐欺の手口の詳細は、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※370」を参照されたい。また、安心相談窓口では、主にサイバーセキュリティ関連の業務に従事されている方向けに、サポート詐欺のより詳細な手口や被害の実態を解説した「IPA『サポート詐欺レポート』2024※371」を公開した。こちらも参照いただきたい。



■図 1-2-23　パソコンに表示された偽のウイルス感染警告の例

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、代表的な方法として、Web サイトの広告を悪用する事例を確認している※372。サポート詐欺グループは、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「次のページに進むためのボタンと誤認させる広告」や「思わずクリックしたくなる広告」等を配信する。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させる（図 1-2-24）。



■図 1-2-24　Web サイトに表示された罠の広告の例

2024 年度に多くの相談が寄せられた、遠隔操作を悪用して、ネットバンキングから不正送金を行った例として、安心相談窓口には 1,000 万円以上の金銭を不正送金された被害の相談が寄せられた※373。更に、4,250 万円もの金銭を不正送金された事例も報じられている※374。

このように、1回の不正送金で多額の金銭を奪う悪質な事例が増加している。

不正送金の手口は以下のとおりである。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。その上で遠隔操作を悪用した不正送金を行う。

そのため、サポート詐欺で行われている不正送金は、フィッシングやマルウェアを使った不正送金とは異なる手口と言える。フィッシングやマルウェアを使った不正送金は、窃取したIDとログインパスワードを使って、攻撃者がネットバンキングに不正ログインした上で送金を行う。一方で、サポート詐欺では、被害者自身にログインをさせた上で、攻撃者が遠隔操作を悪用し、以下のような介入を行う。

- 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。
- 被害者のスマートフォンに遠隔操作ソフトをインストールさせた上で送金をさせる。攻撃者は、遠隔操作ソフトの画面共有機能を使い、被害者のスマートフォンに届いたワンタイムパスワードを窃取していると考えられる※375。

(b)対処

Webサイトを閲覧中に突然出現する偽の警告はブラウザーの画面上に表示される。そのため、対処はブラウザーを閉じるだけである。しかし、偽の警告は、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っている（前ページ図1-2-23）。画面が容易に閉じられない場合でも、落ち着いて画面を閉じる操作を行う必要がある。具体的には、ESC(エスケープ)キーを押下してブラウザーのフルスクリーン表示を解除した上でブラウザーを閉じる※376。安心相談窓口では、こうした操作を練習するために、パソコンに疑似的な偽の警告を表示できる「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※377。2023年12月の公開以来、本体験サイトには多くの反響があり、警察の普及啓発の場でも活用されている。また、こうした体験型コンテンツの有用性が評価され、「サイバーセキュリティアワード2025 Web・コンテンツ部門」の最優秀賞を受賞した※378。

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」機能を使用し、遠隔操作ソフトウェアをインストールする前の状態にシステムを戻すことを推奨する。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サイトに掲載している手順書を参照されたい※379。「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※380」を参照いただきたい。

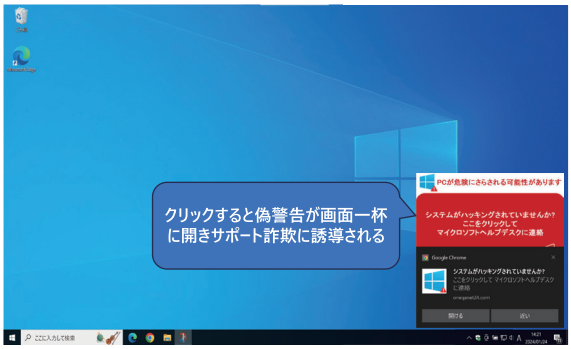
(c)対策

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が表示されるが、サポートセンターに電話を求めることは基本的にない。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の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。

パソコンがウイルス感染したのではないかという恐怖心に駆られて偽のサポートセンターに電話すると、相手の言葉に騙されやすくなる。このようにサポート詐欺は、一般利用者が持つ、パソコンのウイルス感染に対する漠然とした恐怖心に付け込んでいると言える。このウイルス感染の恐怖心に付け込む手口に騙されないための対策として、「1.2.8(5)騙しの手口への対策」が有効である。

(2)ブラウザーの通知機能を悪用した偽の警告

パソコンの画面右下からウイルス感染警告が表示され続け、ブラウザーを閉じても通知が止まらない場合がある。この警告も偽物であり、クリックすると「1.2.8(1)サポート詐欺（偽のウイルス感染警告）」に記載したサポート詐欺に誘導されることがある。加えて、偽の警告をクリックすると、様々な不審なサイトに誘導されることを確認している(次ページ図1-2-25)。



■図 1-2-25　パソコンの画面右下から出現する偽の警告

(a) 手口

閲覧中の Web サイトで突然、「ロボットでない場合は『許可』をクリック」等の表示とともに、許可ボタンが表示される場合がある。「許可」をクリックすると、このサイトからの通知の受け取りを許可したことになる(図 1-2-26)。

この通知の本来の目的は、Web サイトが更新された際の知らせを受け取るためのもので、「ブラウザーの通知機能」と呼ばれる。攻撃者は、自らが作った悪意の Web サイトに被害者を誘導し、通知を許可させる。その結果表示される悪意のサイトからの通知が、図 1-2-25 に示した偽の警告の正体である。



■図 1-2-26　悪意のサイトからの通知を許可させる手口

(b) 対処

偽の警告は、ブラウザーに意図しない悪意のサイトからの通知の許可設定が加わることで発生する。そのため、ブラウザーの設定画面から、普段利用していないサイトからの通知の許可を削除することで、偽の警告の表示を止めることができる。詳細は、安心相談窓口だより「ブラウザの通知機能から不審サイトに誘導する手口に注意※381」を参照いただきたい。

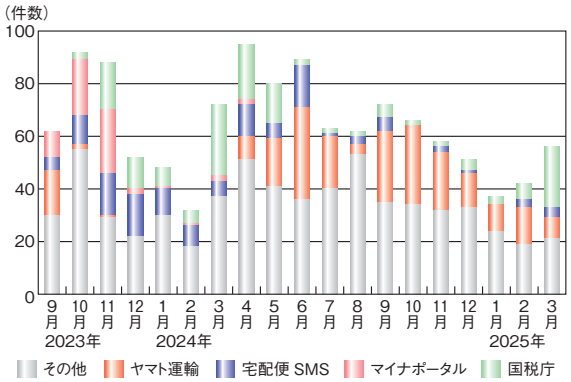
(c) 対策

検索で見つけたサイトや広告から誘導されたサイト等の、通常利用していないサイトで「通知の許可」が求められた場合は安易に許可しないことが、この手口に騙されないための対策である。

通知を許可してしまった場合、サポート詐欺等の被害に遭わないために、表示された偽の警告(通知)を鵜呑みにしないように日頃から注意していただきたい。

(3) メールを悪用した手口

2024 年度に入ってメールを悪用した手口の相談では、ヤマト運輸株式会社をかたるフィッシングメールに関するものが増加し(図 1-2-27)、確定申告の時期や年度末になると、国税庁をかたるフィッシングメールについての相談が増加した。また、2024 年末から 2025 年 2 月にかけて暗号資産を要求する脅迫メールが増加した。



■図 1-2-27　フィッシングメールに関する月別相談件数推移

(a) 宅配便業者をかたるフィッシングメールの手口とその対処

「宛先不明で配送できなかった」「不在のため持ち帰った」という偽の内容のメール(図 1-2-28)を送り、身元の確認や、再配達料の名目でクレジットカードの情報を入力させ詐取する。

受信したメールや、メールに記載された「再配達を依頼する」等のリンクをクリックすると、送り状番号が表示さ



■図 1-2-28　ヤマト運輸をかたるフィッシングメールの例

れる（図 1-2-29）ことが多く確認されており、信じて偽サイトに個人情報等を入力した後で、配達状況を確認するために改めて本物のサイトで送り状番号を入力し、フィッシングメールだったことに気が付いたという相談もあった。メールに記載されていた QR コードから偽サイトに誘導される場合もある。



■図 1-2-29　ヤマト運輸をかたるサイトの例

対処方法としては、電話番号やメールアドレス、氏名や住所等を入力した場合は、不審な内容のメール・SMS や電話が来ることが考えられるが、無視すれば問題ない。

クレジットカードの情報を入力した場合は、速やかにクレジットカード会社に連絡し対応を相談する。

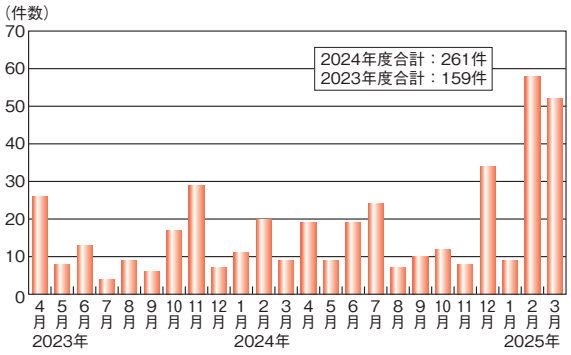
国税庁をかたるものについては、2024 年も引き続き「税金が納められていない」「国税還付金の電子発行を開始しました。」という内容が続いている。手口の変化は少ないため、「情報セキュリティ白書 2024」の「1.2.6 (2) (a) 国税庁をかたるメール」を参照いただきたい。

Amazon をかたるフィッシング等、その他の手口についてはフィッシング対策協議会のページ※382 を参照いただきたい。

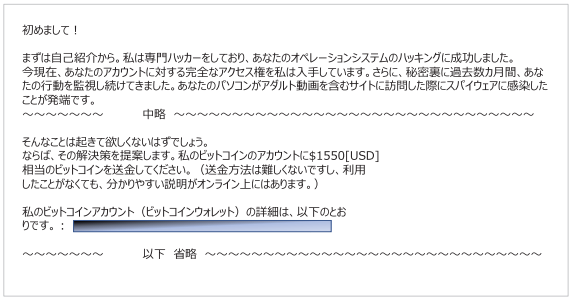
(b) 暗号資産を要求する脅迫メールの手口とその対処

フィッシングの次にメールの手口で相談が多いのが、脅迫メールにより暗号資産を要求する手口である。2018 年ごろより出現しているが、相談件数の増減を繰り返しながら続いている。2024 年末から 2025 年 2 月にかけて増加した（図 1-2-30）。

この手口のメールでは、盗んだ情報や盗撮したという動画を知人や動画サイトにばらまかれたくなければ、制限時間内にビットコイン等の暗号資産を送金するよう要求してくる（図 1-2-31）。



■図 1-2-30　暗号資産を要求する脅迫メールによる手口の相談件数推移


初めまして！

まずは自己紹介から。私は専門ハッカーをしており、あなたのオペレーションシステムのハッキングに成功しました。
今現在、あなたのアカウントに対する完全なアクセス権を私は入手しています。さらに、秘密裏に過去数カ月間、あなたの行動を監視し続けてきました。あなたのパソコンがアダルト動画を含むサイトに訪問した際にスパイウェアに感染したことが発端です。
～～～～～～～～　中略　～～～～～～～～

ターでその多くが検知、分別、削除できる。ほとんどのメールサービスでは迷惑メールフィルターが利用できるが、標準では設定が無効となっていることが多いため、設定を確認し、有効にする。メールアプリやセキュリティソフトの迷惑メールフィルター機能も併用すると効果的である。

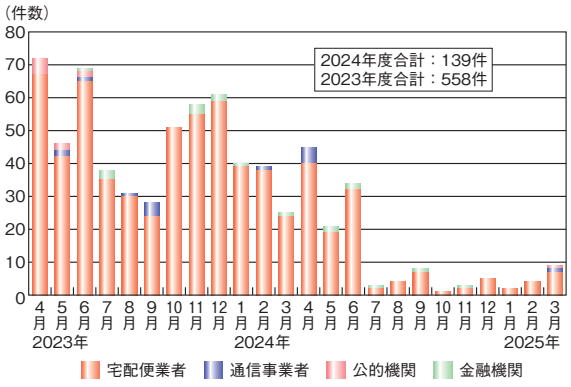
メールサービスやメールアプリが、迷惑メールと振り分けているにもかかわらず、内容を確認して心配になり、相談されることがある。無用な心配をしないことが対策となる。

以下に注意をして内容を確認しても、真偽がはっきりしないメールは無視して削除する。

- 添付ファイルを開かない。
- 記載の URL から Web サイトにアクセスしない。
- 記載の電話番号に電話をしない。
- 返信しない。

(4) SMS を悪用した手口

2024 年度に安心相談窓口に寄せられた SMS（携帯電話番号を宛先としたショートメッセージ）を悪用した手口の相談件数は、宅配便業者をかたる偽 SMS の手口が 7 月から減ってきたことから、2023 年度に比べ大幅に減少した（図 1-2-32）。



■図 1-2-32　偽 SMS に関する月別相談件数推移（2023～2024 年度）

宅配便業者をかたる偽 SMS の手口は、Android 端末の場合は URL をタップさせ不正なアプリをインストールさせる手口、iPhone の場合はフィッシングサイトに誘導する手口であることが多い。手口が出現した 2017 年から 7 年が経過し、各通信会社によって様々な対策が取られてきた。

株式会社 NTT ドコモは、「意図せぬ迷惑メッセージ送信に関するお知らせ」の提供を 2024 年 7 月から開始し、スマートフォンに不正なアプリをインストールしてしまった可能性を利用者に通知している※ 383。

SMS を送信するマルウェア感染端末の台数を報告する「リアルタイム詐欺 SMS モニター※ 384」を運営しているトビラシステムズ株式会社によると 2024 年 2 月初旬は感染端末が 1 万 4,000 台以上確認されていたが、2 月中旬にかけて 1 万 2,000 台前後まで減少し、2024 年 3 月上旬まで横ばいで推移していたという※ 385。その約 1 年後の 2025 年 3 月 22 日時点では 3,340 台となり、大幅な減少が見られた。

(a) 金融機関をかたる偽 SMS

SMS を悪用した手口の相談全体は、大幅に減少したが、その中でも、2023 年 6 月ごろから出現した、金融機関をかたり「取引制限」等の文面が記載された偽 SMS を送り付け、URL をタップさせようとする手口（図 1-2-33）は 2024 年も継続しているため引き続き注意が必要である。



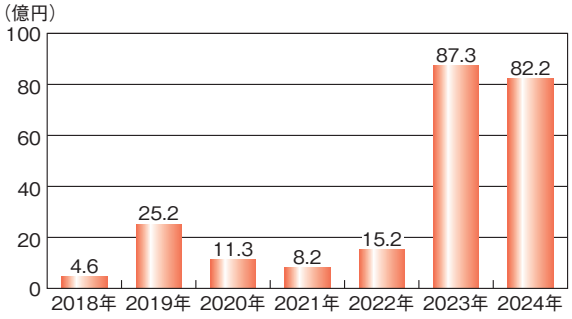
■図 1-2-33　金融機関をかたるフィッシングサイトに口座情報を入力させる例

SMS を悪用した手口だけではないが、インターネットバンキングに係る不正送金被害は、2023 年に急増し、警察庁等から注意喚起が行われたが、2024 年に入っても被害が継続しており、不正送金金額も横ばいである（次ページ図 1-2-34）。

手口の詳細や対処については「情報セキュリティ白書 2024」の「1.2.6 (1) (a) 金融機関をかたる偽 SMS」を参照いただきたい。

(b) SMS を悪用した手口への対策

送信側の企業の対策としては、0005 から始まる通信事業者共通の審査済み送信元番号を表示できる「共通ショートコード」を利用できるようになってきている※ 387。端



■図 1-2-34　インターネットバンキングに係る不正送金の金額推移（2018 ～ 2024 年）
（出典）警察庁「令和 6 年の犯罪情勢※386」を基に IPA が編集

末の利用者は、送信元番号での確認が可能である。

通信会社によっては、迷惑 SMS をブロック※388 したり、メールのように専用のフォルダに振り分けたりするアプリの提供が行われている※389 ので、利用している通信会社のサービスを確認していただきたい。

上記の対策を取っても、すべての迷惑 SMS の受信を防ぐことはできないため、メールの手口と同様に、不審と感じた SMS の真偽は、公式サイト等の確かな情報源で確かめ、真偽がはっきりしない SMS については、下記の対応をしていただきたい。

- 記載の URL から Web サイトにアクセスしない。
- 記載の電話番号に電話をしない。

(5) 騙しの手口への対策

サイバーセキュリティの脅威や被害が認知され始めていることを攻撃者に利用され、「ウイルス感染」や「トロイの木馬」「ハッキングした」等という文言を信じてしまい、被害に遭っていることが多いと考えられる。日頃からしっかりとセキュリティ対策を行うことによって、不審な通知がパソコンやスマートフォンの画面に表示されたり、不審なメールや SMS を受信したりしても、いったん立ち止まり、対応を確認できるため、過剰な心配をせず攻撃者に付け込まれないようにすることができると考える。以下に対策の例を示す。使用している端末の OS やアプリのアップデートを常日頃行い、ウイルス感染のリスクを低減することで、偽の警告に騙されないようにする。

- サービスの利用にあたって、可能な場合は多要素認証を設定する。
- 不審なメールや SMS、Web サイト等で目にした情報の真偽は、確かな情報源で確かめる。
- 判断に迷ったら、身に覚えのない内容のメールや画面に表示された電話番号の相手ではなく、信頼できる相手に相談する。

以上に加えて、日頃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であると考える。

COLUMN

情報セキュリティ10大脅威 2025 ～変わらない脅威、新たに選出された脅威～

IPA では毎年、「情報セキュリティ 10 大脅威」（以下、10 大脅威）を発表しています。前年に発生した社会的に影響が大きかったと考えられる情報セキュリティ事案から、IPA が脅威候補を選定し、情報セキュリティ分野の研究者、企業の実務担当者等、約 200 名のメンバーで構成する「10 大脅威選考会」の投票を経て、組織向けと個人向けに、それぞれ上位 10 項目を決定しています。

「10 大脅威 2025『組織』向け」では次ページの表の脅威が選出され、5 年以上連続で変わらず選出されている脅威が多い中で、7 位に新たに「地政学的リスクに起因するサイバー攻撃」が選出されました。また、8 位には 2024 年 12 月末から 2025 年 1 月初めにかけて相次いで見られた「分散型サービス妨害攻撃（DDoS 攻撃）」が、5 年ぶりにランクインしました。

（次ページに続く）

表　情報セキュリティ 10 大脅威 2025「組織」向け脅威

順位	「組織」向け脅威	初選出年	選出状況
1	ランサム攻撃による被害	2016 年	10 年連続 10 回目
2	サプライチェーンや委託先を狙った攻撃	2019 年	7 年連続 7 回目
3	システムの脆弱性を突いた攻撃※	2016 年	5 年連続 8 回目
4	内部不正による情報漏えい等	2016 年	10 年連続 10 回目
5	機密情報等を狙った標的型攻撃	2016 年	10 年連続 10 回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021 年	5 年連続 5 回目
7	地政学的リスクに起因するサイバー攻撃	2025 年	初選出
8	分散型サービス妨害攻撃（DDoS 攻撃）	2016 年	5 年ぶり 6 回目
9	ビジネスメール詐欺	2018 年	8 年連続 8 回目
10	不注意による情報漏えい等	2016 年	7 年連続 8 回目

※「システムの脆弱性を突いた攻撃」は、「10 大脅威 2024『組織』向け」の 5 位「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」と 7 位「脆弱性対策情報の公開に伴う悪用増加」を統合したもの

今回新たに脅威候補として選定され、7 位に初選出された「地政学的リスクに起因するサイバー攻撃」は、国家の関与が疑われる国際的な攻撃に関する脅威です。「地政学的リスク」とは、地理的条件に基づいた国や地域の政治や軍事等に関わるリスクのことを指し、近年の国際的な政治情勢の緊張の高まりも背景に、政治的に対立する周辺国に対して、国家の関与が疑われるグループによるサイバー攻撃が発生しています。こうした状況も踏まえて、今回初選出されました。攻撃者の支援を行う国家にとって有用な機密情報を持つ政府機関等の組織や、攻撃成功時の社会的なインパクトが大きい重要インフラ企業等が狙われており、政府機関からも注意喚起[i]が発出される等、懸念が広がっています。攻撃の目的には、機密情報の窃取だけでなく、社会的な混乱を引き起こすことや、嫌がらせや報復、更には自国の産業の競争優位性の確保、政治体制維持のための外貨獲得等が挙げられます。攻撃の手口としては、標的型攻撃、フィッシング、DDoS 攻撃、偽情報の流布による影響工作、ランサムウェア攻撃等、様々な手口が用いられています。近年では、このような国家を背景とする攻撃にも備えて、セキュリティ対策情報を継続的に収集し、組織として常にサイバー攻撃への対策を強化していくことが求められています。このような脅威に関する 2024 年の事例や対策については、「情報セキュリティ 10 大脅威 2025 解説書（組織編）[ii]」で取り上げているので参照してみてください。

そのほか、繰り返し選出されているその他の脅威についても、自組織だけでなく取引先等といった利害関係者とともに継続して対策を検討する必要があります。また、10 大脅威では個人向けの脅威も取り上げており、組織の役職員は「組織」に属するのと同時に「個人」でもあるため、「組織」としてセキュリティ対策を行う際は「個人」向け脅威も理解しておく必要があります。「情報セキュリティ 10 大脅威 2025[iii]」では、組織向け、個人向けの解説書のほかに、社内教育に使える資料等も公開していますのでぜひご活用ください。

i　警察庁、NISC：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〔2025/7/31 確認〕
ii　https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/kaisetsu_2025_soshiki.pdf〔2025/7/31 確認〕
iii　https://www.ipa.go.jp/security/10threats/10threats2025.html〔2025/7/31 確認〕

※1 NCSC：Annual Review 2024 https://www.ncsc.gov.uk/files/NCSC_Annual_Review_2024.pdf〔2025/6/18 確認〕
※2 https://www.ic3.gov/AnnualReport/Reports/2024_ic3report.pdf〔2025/6/18 確認〕
※3 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150円として換算している。
※4 CSIS：Significant Cyber Incidents https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents〔2025/6/18 確認〕
※5 Reuters：US senators vow action after briefing on Chinese Salt Typhoon telecom hacking https://www.reuters.com/world/us/us-agencies-brief-senators-chinese-salt-typhoon-telecom-hacking-2024-12-04/〔2025/6/18 確認〕
Reuters：US adds 9th telcom to list of companies hacked by Chinese-backed Salt Typhoon cyberespionage https://www.reuters.com/technology/cybersecurity/us-adds-9th-telcom-list-companies-hacked-by-chinese-backed-salt-typhoon-2024-12-27/〔2025/6/18 確認〕
※6 Bleeping Computer：US says Chinese hackers breached multiple telecom providers https://www.bleepingcomputer.com/news/security/us-says-chinese-hackers-breached-multiple-telecom-providers/〔2025/6/18 確認〕
CISA：Joint Statement from FBI and CISA on the People's Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure https://content.govdelivery.com/accounts/USDHSCISA/bulletins/3c1b400〔2025/6/18 確認〕
※7 The Washington Post:Top senator calls Salt Typhoon 'worst telecom hack in our nation's history' https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/〔2025/6/18 確認〕
※8 CrowdStrike 社：CrowdStrike PIR Executive Summary https://www.crowdstrike.com/content/dam/crowdstrike/www/en-us/wp/2024/07/CrowdStrike-PIR-Executive-Summary.pdf〔2025/6/18 確認〕
※9 Bitsight Technologies, Inc.：CrowdStrike Outage Timeline, Analysis, & Impact https://www.bitsight.com/blog/crowdstrike-outage-timeline-and-analysis〔2025/6/18 確認〕
※10 Microsoft 社：Helping our customers through the CrowdStrike outage https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/〔2025/6/18 確認〕
※11 Cloudflare 社：Paris 2024 Olympics recap: Internet trends, cyber threats, and popular moments https://blog.cloudflare.com/paris-2024-olympics-recap/〔2025/6/18 確認〕
※12 Cloudflare 社：Global elections in 2024: Internet traffic and cyber threat trends https://blog.cloudflare.com/elections-2024-internet/〔2025/6/18 確認〕
※13 G-Core Labs S.A.：Gcore Radar report reveals 56% year-on-year increase in DDoS attacks https://gcore.com/press-releases/gcore-radar-ddos-attack-trends-q3-q4-2024〔2025/6/18 確認〕
※14 Vercara LLC：UltraDDoS Protect Annual Distributed Denial-of-Service Analysis January – December 2024 https://vercara.digicert.com/resources/ultraddos-protect-annual-distributed-denial-of-service-analysis-january-december-2024〔2025/6/18 確認〕
※15 https://apwg.org/trendsreports/〔2025/6/18 確認〕
※16 APWG：apwg_trends_report_q1_2024_PRODUCTION https://docs.apwg.org/reports/apwg_trends_report_q1_2024.pdf〔2025/6/18 確認〕
APWG：apwg_trends_report_q2_2024 https://docs.apwg.org/reports/apwg_trends_report_q2_2024.pdf〔2025/6/18 確認〕
APWG：apwg_trends_report_q3_2024 https://docs.apwg.org/reports/apwg_trends_report_q3_2024.pdf〔2025/6/18 確認〕
APWG：apwg_trends_report_q4_2024 https://docs.apwg.org/reports/apwg_trends_report_q4_2024.pdf〔2025/6/18 確認〕
※17 SlashNext, Inc.：The State of Phishing 2024 https://slashnext.com/the-state-of-phishing-2024/〔2025/6/18 確認〕
※18 KnowBe4, Inc.：Phishing Threat Trends Report https://www.knowbe4.com/hubfs/Phishing-Threat-Trends-2025_Report.pdf〔2025/6/18 確認〕
※19 FBI：Internet Crime Report 2023 https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf〔2025/6/18 確認〕
FBI：Internet Crime Report 2022 https://www.ic3.gov/AnnualReport/Reports/2022_ic3report.pdf〔2025/6/18 確認〕
FBI：Internet Crime Report 2021 https://www.ic3.gov/AnnualReport/Reports/2021_ic3report.pdf〔2025/6/18 確認〕
※20 Cyberint Technologies：Ransomware Annual Report 2024 https://cyberint.com/blog/research/ransomware-annual-report-2024/〔2025/6/18 確認〕
※21 IBM 社：2024 年「データ侵害のコストに関する調査」 https://www.ibm.com/jp-ja/reports/data-breach〔2025/6/18 確認〕
※22 Microsoft 社：National Public Data breach: What you need to know https://support.microsoft.com/en-us/topic/national-public-data-breach-what-you-need-to-know-843686f7-06e2-4e91-8a3f-ae30b7213535〔2025/6/18 確認〕
※23 Krebs on Security：NationalPublicData.com Hack Exposes a Nation's Data https://krebsonsecurity.com/2024/08/national publicdata-com-hack-exposes-a-nations-data/〔2025/6/18 確認〕
※24 StrongDM, Inc.：National Public Data Breach: What Happened and How to Prevent It https://www.strongdm.com/what-is/national-public-data-breach〔2025/6/18 確認〕
※25 Google LLC：UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion?hl=en〔2025/6/18 確認〕
※26 Bleeping Computer：Massive AT&T data breach exposes call logs of 109 million customers https://www.bleepingcomputer.com/news/security/massive-atandt-data-breach-exposes-call-logs-of-109-million-customers/〔2025/6/18 確認〕
※27 BBC：Santander staff and '30 million' customers hacked https://www.bbc.com/news/articles/c6ppv06e3n8o〔2025/6/18 確認〕
※28 BBC：Ticketmaster confirms hack which could affect 560m https://www.bbc.com/news/articles/cw99ql0239wo〔2025/6/18 確認〕
※29 Snowflake Inc.：Snowflake Admins Can Now Enforce Mandatory MFA https://www.snowflake.com/en/blog/snowflake-admins-enforce-mandatory-mfa/〔2025/6/18 確認〕
※30 Cyber Management Alliance Ltd：UK Armed Forces Data Exposed: MoD Cyber Attack Timeline https://www.cm-alliance.com/cybersecurity-blog/uk-armed-forces-data-exposed-mod-cyber-attack-timeline#:~:text=information%20shared%20herein.-,The%20UK%20MoD%20Cyber%20Attack,personnel%2C%20reservists%2C%20and%20veterans.〔2025/6/18 確認〕
※31 GOV.UK：Defence Secretary Oral Statement to provide a Defence Personnel Update - 07 May 2024 https://www.gov.uk/government/speeches/defence-secretary-oral-statement-to-provide-a-defence-personnel-update-07-may-2024〔2025/6/18 確認〕
※32 Sky News：China hacked Ministry of Defence, Sky News learns https://news.sky.com/story/china-hacked-ministry-of-defence-sky-news-learns-13130757〔2025/6/18 確認〕
The Guardian：About 270,000 UK forces records exposed to Chinese hackers https://www.theguardian.com/uk-news/article/2024/may/07/270000-uk-forces-records-thought-to-have-been-exposed-to-chinese-hackers〔2025/6/18 確認〕
※33 https://www.antiphishing.jp/report/monthly/〔2025/6/18 確認〕
※34 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf〔2025/6/18 確認〕
※35 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf〔2025/6/18 確認〕
※36 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf〔2025/6/18 確認〕
※37 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf〔2025/6/18 確認〕
※38 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〔2025/6/18 確認〕
※39 フィッシング対策協議会：QR コードから誘導するフィッシング（2024/08/28） https://www.antiphishing.jp/news/alert/qr_20240828.html〔2025/6/18 確認〕
※40 警察庁：サイバー警察局便り R6Vol.15「今、企業の資産（法人口座）がねらわれている!!電話に注意!「ボイスフィッシング」による不正送金被害が急増」 https://www.npa.go.jp/bureau/cyber/pdf/R6_Vol.15cpal.pdf〔2025/6/18 確認〕
※41 株式会社山形銀行：山形銀行を騙る不審な電話（ボイスフィッシング）にご注意ください https://www.yamagatabank.co.jp/attention/vishing/〔2025/6/18 確認〕
山形放送：被害額は十数億円 山形銀行かたる不審な自動音声電話 複数の企業がだまし取られたか https://news.ntv.co.jp/n/ybc/category/society/yb37bbf9bc397d4882a291d56a7c74ee7d〔2025/6/18 確認〕

※ 42 https://www.mcpc-jp.org/pdf/security_seminars_20250212.pdf〔2025/6/18 確認〕
※ 43 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〔2025/6/18 確認〕
※ 44 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〔2025/6/18 確認〕
※ 45 警察庁：令和 6 年における生活経済事犯の検挙状況等について　https://www.npa.go.jp/publications/statistics/safetylife/R06_nennpou_teisei.pdf〔2025/6/18 確認〕
※ 46 IIJ 社：観測レポート　https://wizsafe.iij.ad.jp/category/report/〔2025/6/18 確認〕
※ 47 https://csl.nict.go.jp/report/NICTER_report_2024.pdf〔2025/6/18 確認〕
※ 48 NISC：DDoS 攻撃への対策について（注意喚起）　https://www.nisc.go.jp/pdf/news/press/20250204_ddos.pdf〔2025/6/18 確認〕
※ 49 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〔2025/6/12 確認〕
※ 50 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〔2025/6/12 確認〕
※ 51 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〔2025/6/12 確認〕
※ 52 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〔2025/6/12 確認〕
※ 53 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/〔2025/6/12 確認〕
※ 54 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〔2025/6/12 確認〕
※ 55 CyberSRC Consultancy Pvt. Ltd.：Chinese Nation-State Hackers APT41 Hit Gambling Sector for Financial Gain　https://cybersrcc.com/2024/10/22/chinese-nation-state-hackers-apt41-hit-gambling-sector-for-financial-gain/〔2025/6/12 確認〕
※ 56 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〔2025/6/12 確認〕
※ 57 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〔2025/6/12 確認〕
※ 58 KADOKAWA：KADOKAWA グループの複数ウェブサイトにおける障害の発生について　https://group.kadokawa.co.jp/information/media-download/1335/5e7b26d5ab9b4086/〔2025/6/12 確認〕
※ 59 KADOKAWA：【第2報】KADOKAWA グループにおけるシステム障害について　https://group.kadokawa.co.jp/information/media-download/1338/fa5deb642248bb65/〔2025/6/12 確認〕
※ 60 KADOKAWA：ランサムウェア攻撃による情報漏洩に関するお知らせ　https://group.kadokawa.co.jp/information/media-download/1356/d3f77b589c58d083/〔2025/6/12 確認〕
※ 61 朝日新聞：新たなデータ流出か　サイバー攻撃を受けた KADOKAWA が発表　https://www.asahi.com/articles/ASS720H3RS72UTIL003M.html〔2025/6/12 確認〕
※ 62 読売新聞オンライン：ハッカー集団、KADOKAWA内部情報を公開…闇サイト上に給与明細など　https://www.yomiuri.co.jp/national/20240702-OYT1T50064/〔2025/6/12 確認〕
※ 63 KADOKAWA：情報漏洩に関するお詫びならびに漏洩情報の拡散行為に対する警告と法的措置について　https://group.kadokawa.co.jp/information/media-download/1351/d405b664b0f9d545/〔2025/6/12 確認〕
※ 64 株式会社ドワンゴ：ニコニコサービスの利用停止にともなう補償のご案内　https://blog.nicovideo.jp/niconews/225420.html〔2025/6/12 確認〕
※ 65 N 高等学校・S 高等学校・R 高等学校：N 予備校の復旧状況について　https://nnn.ed.jp/news/1ltnwdyjsaqi/〔2025/7/29 確認〕
※ 66 株式会社ドワンゴ：2/25 更新【ニコニコ生放送】サービス再開状況のお知らせ　https://blog.nicovideo.jp/niconews/225372.html〔2025/6/12 確認〕
※ 67 KADOKAWA：KADOKAWA オフィシャルサイト閲覧障害のお詫びと復旧についてのお知らせ　https://www.kadokawa.co.jp/topics/12109/〔2025/6/12 確認〕
※ 68 株式会社ドワンゴ：（12/18 追記）【PC 版ニコニコ動画】再開状況のお知らせ　https://blog.nicovideo.jp/niconews/225240.html〔2025/6/12 確認〕
※ 69 株式会社ドワンゴ：（12/8 追記）【スマホブラウザ版ニコニコ動画】再開状況のお知らせ　https://blog.nicovideo.jp/niconews/225242.html〔2025/6/12 確認〕
※ 70 KADOKAWA：［復旧報告］KADOKAWA アプリ復旧のお知らせ（11/20）　https://kapp-help.kadokawa.co.jp/hc/ja/articles/33472100898073-- 復旧報告 -KADOKAWA アプリ復旧のお知らせ-11-20〔2025/6/12 確認〕
※ 71 KADOKAWA：［復旧報告］KADOKAWA-ID 復旧のお知らせ（12/11）　https://members-help.kadokawa.co.jp/hc/ja/articles/33471996607257-- 復旧報告 -KADOKAWA-ID 復旧のお知らせ-12-11〔2025/6/12 確認〕
※ 72 イセトー社：ランサムウェア被害の発生について　https://www.iseto.co.jp/news/news_202405-3.html〔2025/6/12 確認〕
※ 73 イセトー社：ランサムウェア被害の発生について（続報 2）　https://www.iseto.co.jp/news/news_202407.html〔2025/6/12 確認〕
※ 74 piyolog：イセトーのランサムウエア感染についてまとめてみた https://piyolog.hatenadiary.jp/entry/2024/06/15/011339〔2025/6/12 確認〕
※ 75 個人情報保護委員会：株式会社イセトーに対する個人情報の保護に関する法律に基づく行政上の対応について　https://www.ppc.go.jp/files/pdf/250319_houdou.pdf〔2025/6/12 確認〕
※ 76 イセトー社：不正アクセスによる個人情報漏えいに関するお詫びとご報告　https://www.iseto.co.jp/news/news_202410.html〔2025/3/14 確認〕
※ 77 イセトー社：ISO27001 認証及び ISO27017 認証の一時停止について　https://www.iseto.co.jp/news/news_202409.html〔2025/6/12 確認〕
※ 78 イセトー社：プライバシーマーク付与の一時停止について　https://www.iseto.co.jp/news/news_202412.html〔2025/6/12 確認〕
※ 79 イセトー社：ISO27001 認証及び ISO27017 認証の一時停止解除について　https://www.iseto.co.jp/news/news_202502.html〔2025/6/12 確認〕
※ 80 日本経済新聞：ランサム集団「8Base」、ロシア人逮捕　イセトーも被害　https://www.nikkei.com/article/DGXZQOUE108SD0Q5A210C2000000/〔2025/6/24 確認〕
※ 81 トレンドマイクロ社：事例にみる国内に被害をもたらす 2 大ランサムウェア攻撃者グループ　https://www.trendmicro.com/ja_jp/jp-security/24/f/expertview-20240617-01.html〔2025/6/12 確認〕
※ 82 警察庁：ロシア人ランサムウェア被疑者4名の検挙に関するユーロポールのプレスリリースについて　https://www.npa.go.jp/news/release/2025/250212release.pdf〔2025/6/12 確認〕
※ 83 https://www.cisa.gov/stopransomware/ransomware-guide〔2025/6/12 確認〕
※ 84 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〔2025/6/12 確認〕
※ 85 https://www.ipa.go.jp/publish/wp-security/2023.html〔2025/6/12 確認〕
※ 86 No More Ransom：https://www.nomoreransom.org/ja/index.html〔2025/6/12 確認〕
※ 87 https://www.jpcert.or.jp/magazine/security/ransom-faq.html〔2025/6/12 確認〕
※ 88 https://www.nisc.go.jp/pdf/policy/general/guider5.pdf〔2025/6/19 確認〕
※ 89 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/〔2025/6/19 確認〕
※ 90 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/〔2025/6/19 確認〕
※ 91 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〔2025/6/19 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〔2025/6/19 確認〕
※ 92 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させるサーバー。
※ 93 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/security/security-alert/2023/alert20230801.html〔2025/6/19 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/security/security-alert/2023/alert20231019.html〔2025/6/19 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〔2025/6/19 確認〕
※ 94 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。
※ 95 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〔2025/6/19 確認〕
※ 96 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〔2025/6/19 確認〕
※ 97 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。
※ 98 NISC：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.nisc.go.jp/pdf/news/press/240625NISC_press.pdf〔2025/6/19 確認〕
※ 99 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〔2025/6/19 確認〕
※ 100 「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〔2025/6/19 確認〕
※ 101 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〔2025/6/19 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）
※ 102 警察庁、NISC：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〔2025/6/19 確認〕
※ 103 警察庁：Windows Sandbox を悪用した手口及び 痕跡・検知策 https://www.npa.go.jp/bureau/cyber/pdf/20250108_windowssandbox.pdf〔2025/6/19 確認〕
※ 104 警察庁：VS Code を悪用した手口及び痕跡・検知策 https://www.npa.go.jp/bureau/cyber/pdf/20250108_vscode.pdf〔2025/6/19 確認〕
※ 105 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。
※ 106 Cobalt Strike Beacon：ペネトレーションテストのための正規のセキュリティツールである Cobalt Strike 内の遠隔操作ツール。ペネトレーションテストのための有益な機能が、多くの攻撃者グループによりバックドアとして悪用されている。
トレンドマイクロ社：ランサムウェア攻撃で悪用された正規ツールを解説 https://www.trendmicro.com/ja_jp/research/21/i/describing-legitimate-tools-exploited-for-ransomware-attacks.html〔2025/6/19 確認〕
※ 107 CISA：Joint Statement from FBI and CISA on the People's Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure https://content.govdelivery.com/accounts/USDHSCISA/bulletins/3c1b400〔2025/6/19 確認〕
※ 108 Cisco Systems, Inc.：Weathering the storm: In the midst of a Typhoon https://blog.talosintelligence.com/salt-typhoon-analysis/〔2025/6/19 確認〕
※ 109 U.S. Department of Justice：Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers https://www.justice.gov/archives/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state〔2025/6/19 確認〕
※ 110 悪用された脆弱性は多数にわたるため、対象の脆弱性については下記のセキュリティアドバイザリーを参照されたい。
※ 111 FBI 等：People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations https://media.defense.gov/2024/Sep/18/2003547016/-1/-1/0/CSA-PRC-LINKED-ACTORS-BOTNET.PDF〔2025/6/19 確認〕
※ 112 ①エッジを知る、②セキュア・バイ・デザイン機器を調達する、③セキュリティ強化のガイダンス、更新及びパッチを適用する、④強力な認証を実装する、⑤不要な機能とポートを無効にする、⑥管理インターフェイスを安全にする、⑦脅威検出のための監視を一元化するの七つ。詳細は「エッジデバイスのための緩和戦略」本文を参照されたい。
※ 113 NISC:（仮訳）エッジデバイスのための緩和戦略：幹部向けガイド https://www.nisc.go.jp/pdf/policy/kokusai/Provisional_Translation_Edgedevice_Guidance_executive_guidance.pdf〔2025/6/19 確認〕
NISC:（仮訳）エッジデバイスのための緩和戦略：実務者向けガイド https://www.nisc.go.jp/pdf/policy/kokusai/Provisional_Translation_Edgedevice_Guidance_practitioner_guidance.pdf〔2025/6/19 確認〕
※ 114 NISC：国際文書「エッジデバイスのための緩和戦略」への共同署名について https://www.nisc.go.jp/pdf/press/press_Edgedevice_Mitigation_Guidance.pdf〔2025/6/19 確認〕
※ 115 「IPA NEWS Vol. 70（2025 年 1 月号）」（https://www.ipa.go.jp/about/ipanews/ipanews202501.html〔2025/6/19 確認〕）の「家庭用ルーターの乗っ取りも! 8 つのセキュリティ対策で防御」及び「ルーター選定のポイントは 7 つ。セキュリティ要件の評価制度も参考に」等。
※ 116 警察庁：北朝鮮を背景とするサイバー攻撃グループ TraderTraitor による暗号資産関連事業者を標的としたサイバー攻撃について https://www.npa.go.jp/bureau/cyber/pdf/020241224_pa.pdf〔2025/6/19 確認〕
警察庁：（仮訳）FBI、DC3 及び警察庁は、Bitcoin.DMM.Com から 3 億 800 万ドルを窃取したとして、北朝鮮のサイバーアクター TraderTraitor を特定 https://www.npa.go.jp/bureau/cyber/pdf/20241224_jp.pdf〔2025/6/19 確認〕
※ 117 https://piyolog.hatenadiary.jp/entry/2024/12/25/180139〔2025/6/19 確認〕
※ 118 警察庁、NISC、金融庁:北朝鮮を背景とするサイバー攻撃グループ TraderTraitor 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/20241224_caution.pdf〔2025/6/19 確認〕
※ 119 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/NK_it.pdf〔2025/6/19 確認〕
※ 120 警察庁：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（仮訳） https://www.npa.go.jp/bureau/cyber/pdf/20250114jp.pdf〔2025/6/19 確認〕
※ 121 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〔2025/6/19 確認〕
※ 122 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。
※ 123 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〔2025/6/19 確認〕
※ 124 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.meti.go.jp/press/2022/03/20230308006/20230308006-2.pdf〔2025/6/19 確認〕
※ 125 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〔2025/6/19 確認〕
※ 126 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〔2025/6/19 確認〕
※ 127 https://www.ipa.go.jp/security/guide/hjuojm00000055l0-

att/ps6vr7000000jvcb.pdf〔2025/6/19 確認〕
※ 128 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7年5月1日時点）」（https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/pamphlet_dounyu.pdf〔2025/6/19 確認〕）参照。
※ 129 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/hjuojm000000055l0-att/Ver5gaiyo.pdf〔2025/6/19 確認〕
※ 130 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〔2025/6/19 確認〕
※ 131 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〔2025/6/19 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。
※ 132 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〔2025/6/19 確認〕
※ 133 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〔2025/6/19 確認〕
※ 134 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。
※ 135 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〔2025/6/19 確認〕
※ 136 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〔2025/6/19 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〔2025/6/19 確認〕
※ 137 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〔2025/6/19 確認〕
※ 138 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〔2025/6/19 確認〕
※ 139 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〔2025/6/19 確認〕
※ 140 @ 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〔2025/6/19 確認〕
※ 141 「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/〔2025/6/19 確認〕
※ 142 NetScout Systems, Inc.：Why Do Hackers Use DDoS Attacks? https://www.netscout.com/blog/why-do-hackers-use-ddos-attacks〔2025/6/23 確認〕
※ 143 NetScout Systems, Inc.：An Era of DDoS Hacktivism https://www.netscout.com/blog/era-ddos-hacktivism〔2025/6/13 確認〕
※ 144 Cloudflare 社：2024 年第 1 四半期 DDoS 脅威レポート https://blog.cloudflare.com/ja-jp/ddos-threat-report-for-2024-q1/〔2025/6/13 確認〕
公益財団法人笹川平和財団：外交・安全保障と連動するサイバー攻撃・偽情報――G7 サミット期間に発生した DDoS 攻撃 https://www.spf.org/iina/articles/osawa_06.html〔2025/6/13 確認〕
※ 145 SOMPOリスクマネジメント株式会社：【ブログ】親ロシア・ハクティビストが日本の金融機関・政党・鉄道会社等 Web サイトを攻撃（2024 年 7 月） https://www.sompocybersecurity.com/column/column/pro-russia-hacktivists-ddos-japan-2024-jul〔2025/6/13 確認〕
※ 146 Cloudflare 社：2024 年第 4 四半期、記録的な 5.6Tbps の DDoS 攻撃およびグローバルな DDoS の傾向 https://blog.cloudflare.com/ja-jp/ddos-threat-report-for-2024-q4/〔2025/6/13 確認〕
※ 147 https://piyolog.hatenadiary.jp/entry/2024/12/30/154109〔2025/6/13 確認〕
※ 148 C&C サーバー：Command and Control サーバーの略。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。
※ 149 トレンドマイクロ社：2024 年末からの DDoS 攻撃被害と関連性が疑われる IoT ボットネットの大規模な活動を観測 https://www.trendmicro.com/ja_jp/research/24/l/iot-botnet-activity-ddos-attacks.html〔2025/6/13 確認〕
※ 150 警察庁：DDoS 攻撃は犯罪です! https://www.npa.go.jp/bureau/cyber/countermeasures/ddos_campaign.html〔2025/6/13 確認〕
読売新聞オンライン：出版社にDDoS攻撃容疑、25歳の配管工「ストレス発散だった」…海外の代行業者を利用 https://www.yomiuri.co.jp/national/20240806-OYT1T50213/〔2025/6/13 確認〕
※ 151 IP ストレッサー：IP ストレッサーは、セキュリティテストや負荷テストを実行することを目的としたサービスであり、サービス利用者に対し、特定の Web サイトや機器に対する DDoS 攻撃を実行させることができる。
※ 152 NHK：サイバー攻撃の代行サービス使い企業攻撃か 中学生が書類送検 https://www3.nhk.or.jp/news/html/20241212/k10014665381000.html〔2025/6/13 確認〕
※ 153 IPA：JVN iPedia 脆弱性対策情報データベース https://jvndb.jvn.jp〔2025/6/13 確認〕
※ 154 JPCERT/CC、IPA：Japan Vulnerability Notes（JVN） https://jvn.jp/〔2025/6/13 確認〕
※ 155 NIST：National Vulnerability Database（NVD） https://nvd.nist.gov/〔2025/6/13 確認〕
※ 156 IPA：共通脆弱性タイプ一覧 CWE 概説 https://www.ipa.go.jp/security/vuln/scap/cwe.html〔2025/6/13 確認〕
※ 157 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〔2025/6/13 確認〕
※ 158 IPA：脆弱性対策情報データベース JVN iPedia の登録状況 https://www.ipa.go.jp/security/reports/vuln/jvn/index.html〔2025/6/13 確認〕
※ 159 「1.2.4（1）（b）早期警戒パートナーシップにおける脆弱性の届出状況」では、「ソフトウェア製品」と「Web アプリケーション」は、早期警戒パートナーシップにおける対象の区分を意味するものであり、特に断りのない限り、または文献引用上の正確性を期す必要のない限り、「Web アプリケーション」については、「Web サイト」と記載する。
※ 160 IPA：情報セキュリティ早期警戒パートナーシップの紹介 https://www.ipa.go.jp/security/guide/vuln/ug65p90000019by0-att/partnership_guideline_overview_jp.pdf〔2025/6/13 確認〕
※ 161 「1.2.4（1）（b）早期警戒パートナーシップにおける脆弱性の届出状況」では、「ウェブアプリケーションソフト」は、Web サイト構築関係のソフトウェアを指す。これは、四半期ごとの脆弱性関連情報の届出状況のレポート（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〔2025/6/13 確認〕）で使用している製品種類の「ウェブアプリケーションソフト」と同じである。
※ 162 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〔2025/6/13 確認〕
※ 163 警察庁：令和6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/R6/R06_cyber_jousei.pdf〔2025/6/13 確認〕

※ 164 Palo Alto 社：CVE-2024-3400 PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect https://security.paloaltonetworks.com/CVE-2024-3400〔2025/6/13 確認〕
※ 165 NVD：CVE-2024-3400 https://nvd.nist.gov/vuln/detail/cve-2024-3400〔2025/6/13 確認〕
※ 166 CISA：Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2024-3400〔2025/6/13 確認〕
※ 167 IPA：Palo Alto Networks 製 PAN-OS の脆弱性対策について（CVE-2024-3400） https://www.ipa.go.jp/security/security-alert/2024/alert20240415.html〔2025/6/13 確認〕
JPCERT/CC：Palo Alto Networks 社 製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起 https://www.jpcert.or.jp/at/2024/at240009.html〔2025/6/13 確認〕
※ 168 リバースシェル：攻撃者が侵害した機器から攻撃者が用意するサーバーにアクセスさせることにより、ファイアウォール等の制限を回避して、侵害した機器の遠隔操作を試みるための仕組み。
※ 169 Volexity：Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400) https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/〔2025/6/13 確認〕
※ 170 共同通信：太陽光発電施設にサイバー攻撃 身元隠し不正送金に悪用 https://www.47news.jp/10864212.html〔2025/4/23 確認〕
※ 171 S2W INC.：Detailed Analysis of 'Operation Japan' Campaign https://medium.com/s2wblog/detailed-analysis-of-operation-japan-campaign-14834a14a684〔2025/6/13 確認〕
※ 172 株式会社コンテック：太陽光発電施設向け当社遠隔監視機器へのサイバー攻撃報道について https://www.contec.com/jp/info/2024/2024050700/〔2025/6/13 確認〕
※ 173 トレンドマイクロ社：太陽光発電監視機器に対するサイバー攻撃を考察 https://www.trendmicro.com/ja_jp/jp-security/24/f/security-strategy-20240606-01.html〔2025/6/13 確認〕
※ 174 Operational Relay Box（ORB）とは、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のこと。ORB は、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。
※ 175 株式会社コンテック：インターネットからの SolarView Compact への不正アクセスの影響について https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_solarview_230718_jp.pdf〔2025/6/13 確認〕
※ 176 経済産業省：資料 5-1 小規模太陽光発電設備のサイバーセキュリティ対策の課題について https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/017_05_01.pdf〔2025/6/13 確認〕
※ 177 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。
※ 178 CISA：Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2022-29303〔2025/6/13 確認〕
※ 179 IoT 推進コンソーシアム、総務省、経済産業省：IoT セキュリティガイドライン ver 1.0 http://www.iotac.jp/wp-content/uploads/2016/01/03-IoT セキュリティガイドライン ver1.0 別紙 1.pdf〔2025/6/13 確認〕
※ 180 https://jvndb.jvn.jp/apis/index.html〔2025/6/13 確認〕
※ 181 https://jvndb.jvn.jp/apis/myjvn/mjcheck4.html〔2025/6/13 確認〕
※ 182 NISC：重要インフラ対策関連 https://www.nisc.go.jp/policy/group/infra/policy.html〔2025/6/19 確認〕
※ 183 CISA：Critical Infrastructure Sectors https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors〔2025/6/19 確認〕
※ 184 NPSA：Critical National Infrastructure https://www.npsa.gov.uk/about-npsa/critical-national-infrastructure〔2025/6/19 確認〕
※ 185 Kaspersky Lab：The State of Industrial Cybersecurity https://media.kasperskydaily.com/wp-content/uploads/sites/87/2024/11/20074452/Kaspersky-speaks-the-Language-of-Industrial-Cybersecurity.pdf〔2025/6/19 確認〕
※ 186 SANS Institute：SANS 2024 ICS/OT Survey: The State of ICS/OT Cybersecurity https://www.sans.org/white-papers/sans-2024-state-ics-ot-cybersecurity/〔2025/6/19 確認〕
※ 187 Reuters：Cyberattacks on US utilities surged 70% this year, says Check Point https://www.reuters.com/technology/cybersecurity/cyberattacks-us-utilities-surged-70-this-year-says-check-point-2024-09-11/〔2025/6/19 確認〕
※ 188 Arkansas City：City of Arkansas City Faces Cybersecurity Incident https://www.arkcity.org/environmental-services/page/city-arkansas-city-faces-cybersecurity-incident〔2025/6/19 確認〕
Arkansas City：Arkansas City Water Treatement Facility Treturns to Regular Operations https://www.arkcity.org/city-manager/page/arkansas-city-water-treatement-facility-treturns-regular-operations〔2025/6/19 確認〕
Security Affairs：Arkansas City water treatment facility switched to manual operations following a cyberattack https://securityaffairs.com/168871/hacking/arkansas-city-water-treatment-facility-cyberattack.html〔2025/6/19 確認〕
Dragos, Inc.：Dragos Industrial Ransomware Analysis: Q3 2024 https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q3-2024/〔2025/6/19 確認〕
※ 189 CISA：ALERT - CISA and EPA Release Joint Fact Sheet Detailing Risks Internet-Exposed HMIs Pose to WWS Sector https://www.cisa.gov/news-events/alerts/2024/12/13/cisa-and-epa-release-joint-fact-sheet-detailing-risks-internet-exposed-hmis-pose-wws-sector〔2025/6/19 確認〕
CISA：FACT SHEET - Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems https://www.cisa.gov/resources-tools/resources/internet-exposed-hmis-pose-cybersecurity-risks-water-and-wastewater-systems〔2025/6/19 確認〕
※ 190 The Record：Costa Rica state energy company calls in US experts to help with ransomware attack https://therecord.media/costa-rica-state-energy-company-ransomware〔2025/6/19 確認〕
The Tico Times：Major Cyberattack Disrupts Costa Rica RECOPE Digital Systems https://ticotimes.net/2024/11/29/major-cyberattack-disrupts-costa-rica-recope-digital-systems〔2025/6/19 確認〕
Daily Security Review：Costa Rica Ransomware Attack Cripples State Energy Company RECOPE https://dailysecurityreview.com/security-spotlight/costa-rica-ransomware-attack-cripples-state-energy-company-recope/〔2025/6/19 確認〕
※ 191 The Record：Costa Rica refinery cyberattack was first deployment for new US response program, ambassador says https://therecord.media/state-department-falcon-cyber-response-costa-rica-recope〔2025/6/19 確認〕
※ 192 TheStreet：Cyberattack throws airport into chaos for fourth day in a row https://www.thestreet.com/travel/is-seatac-airport-still-shut-down〔2025/6/19 確認〕
Port of Seattle：Employees Pitched in during the SEA Cyberattack https://www.portseattle.org/blog/employees-pitched-during-sea-cyberattack〔2025/6/19 確認〕
AP：Hackers demand $6 million for files stolen from Seattle airport operator in cyberattack https://apnews.com/article/seattle-airport-cyberattack-ransomware-rhysida-95cd980a9f45112f0fdce488233eec9c〔2025/6/19 確認〕
Port of Seattle：Port Website is Back Online https://www.portseattle.org/blog/port-website-back-online〔2025/6/19 確認〕
Port of Seattle：Port Cyberattack Archive https://www.portseattle.org/news/port-cyberattack-archive〔2025/6/19 確認〕
※ 193 The Record：RansomHub gang allegedly behind attack on Mexican airport operator https://therecord.media/ransomhub-gang-behind-attack-mexican-airport-operator〔2025/6/19 確認〕
※ 194 CISA：Joint Statement from FBI and CISA on the People's Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure https://content.govdelivery.com/accounts/USDHSCISA/bulletins/3c1b400〔2025/6/19 確認〕
※ 195 Bleeping Computer：US govt officials' communications compromised in recent telecom hack https://www.bleepingcomputer.com/news/security/chinese-hackers-compromised-us-government-officials-private-communications-in-recent-telecom-breach/〔2025/6/19 確認〕
Bleeping Computer：White House: Salt Typhoon hacked telcos in dozens of countries https://www.bleepingcomputer.com/news/security/white-house-salt-typhoon-hacked-telcos-in-dozens-of-countries/〔2025/6/19 確認〕
CISA：CISA and Partners Release Joint Guidance on PRC-Affiliated Threat Actor Compromising Networks of Global Telecommunications Providers https://www.cisa.gov/news-events/alerts/2024/12/03/cisa-and-partners-release

-joint-guidance-prc-affiliated-threat-actor-compromising-networks-global〔2025/6/19 確認〕
Reuters:US adds 9th telcom to list of companies hacked by Chinese-backed Salt Typhoon cyberespionage https://www.reuters.com/technology/cybersecurity/us-adds-9th-telcom-list-companies-hacked-by-chinese-backed-salt-typhoon-2024-12-27/〔2025/6/19 確認〕
※ 196 Cybernews：Cleveland cyberattack forces city officials to cut network access https://cybernews.com/news/cleveland-cyberattack-forces-government-to-cut-network-access/〔2025/6/19 確認〕
※ 197 The Record：Some Winston-Salem city services knocked offline by cyberattack https://therecord.media/winston-salem-north-carolina-services-offline-cyberattack〔2025/6/19 確認〕
City of Winston-Salem：Informational Statement on Cyber Event https://www.cityofws.org/CivicAlerts.aspx?AID=1682〔2025/6/19 確認〕
WXII NEWS：Winston-Salem makes progress restoring computer systems following cyberattack https://www.wxii12.com/article/north-carolina-winston-salem-progress-restoring-computer-systems-cyberattack/63533907〔2025/6/19 確認〕
WXII NEWS：City of Winston-Salem announces restoration of online payment system https://www.wxii12.com/article/city-of-winston-salem-restoration-online-payment-system/63759632〔2025/6/19 確認〕
※ 198 Dark Reading：84% of Healthcare Organizations Spotted a Cyberattack in the Late Year https://www.darkreading.com/threat-intelligence/84-of-healthcare-organizations-spotted-a-cyberattack-in-the-late-year〔2025/6/19 確認〕
※ 199-1 CYBERSCOOP：Ransomware attacks on health care sector are driving increase in emergency patient care https://cyberscoop.com/ransomware-attacks-health-care-emergency-visits-microsoft/〔2025/6/19 確認〕
※ 199-2 Change Healthcare は、Optum, Inc. の一部門。
※ 200 The Record：HHS to investigate UnitedHealth and ransomware attack on Change Healthcare https://therecord.media/hhs-investigating-unitedhealth-after-ransomware-attack〔2025/6/19 確認〕
TechCrunch：Change Healthcare stolen patient data leaked by ransomware gang https://techcrunch.com/2024/04/15/change-healthcare-stolen-patient-data-ransomhub-leak/〔2025/6/19 確認〕
Security Affairs：Change Healthcare data breach impacted over 100 million people https://securityaffairs.com/170258/data-breach/change-healthcare-data-breach.html〔2025/6/19 確認〕
The Register：Mega US healthcare payments network restores system 9 months after ransomware attack https://www.theregister.com/2024/11/20/change_healthcares_clearinghouse_services/〔2025/6/19 確認〕
Securityweek：Change Healthcare Data Breach Impact Grows to 190 Million Individuals https://www.securityweek.com/change-healthcare-data-breach-impact-grows-to-190-million-individuals/〔2025/7/23 確認〕
※ 201 Bleeping Computer：Ascension hacked after employee downloaded malicious file https://www.bleepingcomputer.com/news/security/ascension-hacked-after-employee-downloaded-malicious-file/〔2025/6/19 確認〕
Bleeping Computer：Ascension: Health data of 5.6 million stolen in ransomware attack https://www.bleepingcomputer.com/news/security/ascension-health-data-of-56-million-stolen-in-ransomware-attack/〔2025/6/19 確認〕
BushidoToken：BlackBasta Leaks: Lessons from the Ascension Health attack https://blog.bushidotoken.net/2025/02/blackbasta-leaks-lessons-from-ascension.html〔2025/6/19 確認〕
※ 202 地方独立行政法人岡山県精神科医療センター：地方独立行政法人 岡山県精神科医療センター ランサムウェア事案調査報告書について https://www.okayama-pmc.jp/home/consultation/er9dkox7/lromw3x9/〔2025/6/19 確認〕
※ 203 Bleeping Computer：Water services giant Veolia North America hit by ransomware attack https://www.bleepingcomputer.com/news/security/water-services-giant-veolia-north-america-hit-by-ransomware-attack/〔2025/6/19 確認〕
※ 204 The Record：Plant production still on hold for German battery manufacturer after cyberattack https://therecord.media/varta-battery-plant-production-on-hold-after-cyberattack〔2025/6/19 確認〕
※ 205 Bleeping Computer：Steel giant ThyssenKrupp confirms cyberattack on automotive division https://www.bleepingcomputer.com/news/security/steel-giant-thyssenkrupp-confirms-cyberattack-on-automotive-division/〔2025/6/19 確認〕
※ 206 Bleeping Computer：Duvel says it has "more than enough" beer after ransomware attack https://www.bleepingcomputer.com/news/security/duvel-says-it-has-more-than-enough-beer-after-ransomware-attack/〔2025/6/19 確認〕
※ 207 Security Affairs：Keytronic confirms data breach after ransomware attack https://securityaffairs.com/164642/data-breach/keytronic-blackbasta-ransomware.html〔2025/6/19 確認〕
The Record：Cyberattack cost more than $17 million, Key Tronic tells regulators https://therecord.media/key-tronic-cyberattack-cost-17-million-sec〔2025/6/19 確認〕
※ 208 Bleeping Computer：Crown Equipment confirms a cyberattack disrupted manufacturing https://www.bleepingcomputer.com/news/security/crown-equipment-confirms-a-cyberattack-disrupted-manufacturing/〔2025/6/19 確認〕
※ 209 The Record：Furniture giant shuts down manufacturing facilities after ransomware attack https://therecord.media/furniture-giant-manufacturing-shut-down-cyberattack〔2025/6/19 確認〕
※ 210 Bleeping Computer：Underground ransomware claims attack on Casio, leaks stolen data https://www.bleepingcomputer.com/news/security/underground-ransomware-claims-attack-on-casio-leaks-stolen-data/〔2025/6/19 確認〕
The Record：Japanese watchmaker Casio warns of delivery delays after ransomware attack https://therecord.media/japan-casio-delays-watchmaker-ransomware〔2025/6/19 確認〕
カシオ計算機株式会社：当社ネットワークへの不正アクセスによるシステム障害について https://www.casio.co.jp/release/2024/1008-incident/〔2025/6/19 確認〕
カシオ計算機株式会社：【重要なお知らせ】システム障害による修理品受付停止について https://www.casio.com/jp/support/info/2024/1021/〔2025/6/19 確認〕
※ 211 Help Net Security：American Water shuts down systems after cyberattack https://www.helpnetsecurity.com/2024/10/08/american-water-cyberattack/〔2025/6/19 確認〕
※ 212 The Record：Pittsburgh Regional Transit attributes recent service disruptions to ransomware attack https://therecord.media/pittsburgh-regional-transit-attributes-disruptions-to-ransomware-attack〔2025/6/19 確認〕
※ 213 2016 ～ 2023 年は、CISA の Web サイトで暦年（1/1 ～ 12/31）ごとに公開された ICS Advisory の件数をカウントした。ただし、ICS Medical Advisory（医療機器の脆弱性）は除く。カウントは、アドバイザリーベース（各アドバイザリー内の CVE の数ベースではない）及び公表日ベースとした（公表日が 2023 年なら、採番年度が 2022（ICSA-2022-xxx-x）でも 2023 年でカウント）。
CISA：Cybersecurity Alerts & Advisories https://www.cisa.gov/news-events/cybersecurity-advisories〔2025/6/19 確認〕
※ 214 Dragos, Inc.：OT/ICS CYBERSECURITY REPORT https://hub.dragos.com/hubfs/312-Year-in-Review/2025/Dragos-2025-OT-Cybersecurity-Report-A-Year-in-Review.pdf?hsLang=en〔2025/6/19 確認〕
※ 215 Industrial Cyber：New Forescout research details persistent malware threats to OT/ICS engineering workstations https://industrialcyber.co/control-device-security/new-forescout-research-details-persistent-malware-threats-to-ot-ics-engineering-workstations/〔2025/6/19 確認〕
Forescout Technologies, Inc.：ICS Threat Analysis: New, Experimental Malware Can Kill Engineering Processes https://www.forescout.com/blog/ics-threat-analysis-new-experimental-malware-can-kill-engineering-processes/〔2025/6/19 確認〕
Dark Reading：OT/ICS Engineering Workstations Face Barrage of Fresh Malware https://www.darkreading.com/vulnerabilities-threats/ot-ics-engineering-workstations-malware〔2025/6/19 確認〕
※ 216 M-Bus（Meter-Bus）：水道、ガス、電気メーターから特定のセンサーデータを読み取るための欧州標準プロトコル。
※ 217 Security Week：Destructive ICS Malware 'Fuxnet' Used by Ukraine Against Russian Infrastructure https://www.securityweek.com/destructive-ics-malware-fuxnet-used-by-ukraine-against-russian-infrastructure/〔2025/6/19 確認〕
Claroty Ltd.：Unpacking the Blackjack Group's Fuxnet Malware https://claroty.com/team82/research/unpacking-the-blackjack-groups-fuxnet-malware〔2025/6/19 確認〕

※ 218 Industrial Cyber：Dragos details novel FrostyGoop ICS malware using Modbus TCP to disrupt OT operations worldwide https://industrialcyber.co/news/dragos-details-novel-frostygoop-ics-malware-using-modbus-tcp-to-disrupt-ot-operations-worldwide/〔2025/6/19 確認〕
Dragos, Inc.：Impact of FrostyGoop ICS Malware on Connected OT Systems https://hub.dragos.com/hubfs/Reports/Dragos-FrostyGoop-ICS-Malware-Intel-Brief-0724_.pdf〔2025/6/19 確認〕
※ 219 SCADA（Supervisory Control and Data Acquisition）：産業制御システムの一種であり、コンピューターによるシステム監視とプロセス制御を行う。
※ 220 Bleeping Computer：New IOCONTROL malware used in critical infrastructure attacks https://www.bleepingcomputer.com/news/security/new-iocontrol-malware-used-in-critical-infrastructure-attacks/〔2025/6/19 確認〕
Claroty Ltd.：Inside a New OT/IoT Cyberweapon: IOCONTROL https://claroty.com/team82/research/inside-a-new-ot-iot-cyber-weapon-iocontrol〔2025/6/19 確認〕
packet-pilot.net：イランが支援する攻撃グループが IoT/OT デバイスを標的とした新しいマルウェア「IOCONTROL」を使い重要インフラを攻撃 https://packet-pilot.net/packet-news/iran-attack-infrastructure-by-iocontrol/〔2025/6/19 確認〕
※ 221 IPA：制御システムのセキュリティリスク分析ガイド 第 2 版 https://www.ipa.go.jp/security/controlsystem/riskanalysis.html〔2025/6/19 確認〕
※ 222 https://www.notice.go.jp〔2025/6/18 確認〕
※ 223 活動拡大に伴い、2024 年 3 月までに公開していた観測状況における統計データとは異なることに注意。従来のデータ（2024 年 1 ～ 3 月分にて公開終了）については、「情報セキュリティ白書 2024」（https://www.ipa.go.jp/publish/wp-security/2024.html〔2025/6/18 確認〕）の「3.5.4（1）国内における実態調査と注意喚起」（p.187）を参照。
※ 224 https://www.notice.go.jp/status〔2025/6/18 確認〕
統計情報の CSV ファイルは、以下からダウンロードできる。
NOTICE サポートセンター：CSV データ（NOTICE 注意喚起） https://www.notice.go.jp/docs/status_notice.csv〔2025/6/18 確認〕
※ 225 IIJ 社：wizSafe Security Signal https://wizsafe.iij.ad.jp/〔2025/6/18 確認〕
※ 226 詳細は、「情報セキュリティ白書 2022」（https://www.ipa.go.jp/publish/wp-security/sec-2022.html〔2025/6/18 確認〕）の「3.2.2（1）（h）Realtek 社製の無線機器向け SDK の脆弱性」（p.180）を参照。
※ 227 詳細は、「情報セキュリティ白書 2024」の「3.5.1（1）（b）TP-Link 社製ルーターに対する脅威」（p.179）を参照。
※ 228 2014 年 8 月に報告された脆弱性であり、同年 9 月に更新ファームウェアが公開されたものの、10 年間以上にわたって攻撃が継続している。
トレンドマイクロ社：UDP ポートを開放した状態にする Netis 製ルータに存在する不具合を確認 https://blog.trendmicro.co.jp/archives/9725〔2025/6/18 確認〕
トレンドマイクロ社：Netis 製ルータに存在する不具合を修正する更新プログラムを検証 https://blog.trendmicro.co.jp/archives/10050〔2025/6/18 確認〕
※ 229 Zyxel Networks Corporation：Zyxel security advisory for remote code execution and denial-of-service vulnerabilities of CPE https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-remote-code-execution-and-denial-of-service-vulnerabilities-of-cpe〔2025/6/18 確認〕
※ 230 Cloudflare 社：DDoS threat report for 2024 Q1 https://blog.cloudflare.com/ddos-threat-report-for-2024-q1/〔2025/6/18 確認〕
Cloudflare 社：2024 年第 1 四半期 DDoS 脅威レポート https://blog.cloudflare.com/ja-jp/ddos-threat-report-for-2024-q1/〔2025/6/18 確認〕
※ 231 Cloudflare 社：DDoS threat report for 2024 Q2 https://blog.cloudflare.com/ddos-threat-report-for-2024-q2/〔2025/6/18 確認〕
Cloudflare 社：2024 年第 2 四半期 DDoS 脅威レポート https://blog.cloudflare.com/ja-jp/ddos-threat-report-for-2024-q2/〔2025/6/18 確認〕
※ 232 Cloudflare 社：4.2 Tbps of bad packets and a whole lot more: Cloudflare's Q3 DDoS report https://blog.cloudflare.com/ddos-threat-report-for-2024-q3/〔2025/6/18 確認〕
Cloudflare 社：4.2 Tbps の悪性パケットとそれを超えるパケット：Cloudflare の第 3 四半期 DDoS レポート https://blog.cloudflare.com/ja-jp/ddos-threat-report-for-2024-q3/〔2025/6/18 確認〕
※ 233 Cloudflare 社：How Cloudflare auto-mitigated world record 3.8 Tbps DDoS attack https://blog.cloudflare.com/how-cloudflare-auto-mitigated-world-record-3-8-tbps-ddos-attack/〔2025/6/18 確認〕
Cloudflare 社：Cloudflare が世界記録となる 3.8Tbps の DDoS 攻撃をどのように自動軽減したか https://blog.cloudflare.com/ja-jp/how-cloudflare-auto-mitigated-world-record-3-8-tbps-ddos-attack/〔2025/6/18 確認〕
※ 234 Cloudflare 社：Record-breaking 5.6 Tbps DDoS attack and global DDoS trends for 2024 Q4 https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/〔2025/6/18 確認〕
Cloudflare 社：2024 年第 4 四半期、記録的な 5.6Tbps の DDoS 攻撃およびグローバルな DDoS の傾向 https://blog.cloudflare.com/ja-jp/ddos-threat-report-for-2024-q4/〔2025/6/18 確認〕
※ 235 GSL Networks Pty Ltd：Unprecedented 3.15 Billion Packet Rate DDoS Attack Mitigated by Global Secure Layer https://globalsecurelayer.com/blog/unprecedented-3-15-billion-packet-rate-ddos-attack〔2025/6/18 確認〕
※ 236 Team Cymru：An Introduction to Operational Relay Box (ORB) Networks - Unpatched, Forgotten, and Obscured https://www.team-cymru.com/post/an-introduction-to-operational-relay-box-orb-networks-unpatched-forgotten-and-obscured〔2025/6/18 確認〕
※ 237 Lab-C2DC - Laboratory of Command and Control and Cyber-security：D-Link DIR-859 Firmware RevA_FW_Patch_v1.06B01, an unauthenticated Path Traversal vulnerability was discovered in the "fatlady.php" file. This vulnerability allows for the leakage of session data, leading to Full Privilege Escalation and potential unauthorized control of the device via the admin panel. https://github.com/c2dc/cve-reported/blob/main/CVE-2024-0769/CVE-2024-0769.md〔2025/6/18 確認〕
※ 238 D-Link 社：DIR-859 :: All Revisions :: All Firmware :: End-of-Life / End-of-Service :: Multiple Reported Vulnerabilities https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10371〔2025/6/18 確認〕
※ 239 GreyNoise, Inc.：Perma-Vuln: D-Link DIR-859, CVE-2024-0769 https://www.labs.greynoise.io/grimoire/2024-06-25-dlink-again/〔2025/6/18 確認〕
※ 240 D-Link 社：(Non-US) DIR-822 :: H/W Rev. Ax/Bx/Cx :: All Models :: End of Life :: End of Service :: Reported Security Vulnerability https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10372〔2025/6/18 確認〕
※ 241 Ensign InfoSecurity Pte. Ltd.：LAN-Side Unauthenticated Remote Code Execution (RCE) in D-Link DIR-822 routers due to Stack-Based Buffer Overflow in HNAP https://www.ensigninfosecurity.com/advisories/vulnerability-advisories/2〔2025/6/18 確認〕
※ 242 SSD Secure Disclosure：SSD Advisory -D-Link DIR-X4860 Security Vulnerabilities https://ssd-disclosure.com/ssd-advisory-d-link-dir-x4860-security-vulnerabilities/〔2025/6/18 確認〕
※ 243 PoC エクスプロイト：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。別名「PoC コード」「PoC エクスプロイトコード」。
※ 244 KEV（Known Exploited Vulnerabilities Catalog）：CISA の運用指令「Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities」によって確立された、米国連邦政府機関に重大なリスクをもたらす既知の脆弱性のカタログ。
※ 245 CISA：CISA Adds Three Known Exploited Vulnerabilities to Catalog https://www.cisa.gov/news-events/alerts/2024/05/16/cisa-adds-three-known-exploited-vulnerabilities-catalog〔2025/6/18 確認〕
※ 246 TWCERT/CC：D-Link router - Hidden Backdoor https://www.twcert.org.tw/en/cp-139-7880-629f5-2.html〔2025/6/18 確認〕
※ 247 Swind1er：D-Link DIR-823X AX3000 Dual-Band Gigabit Wireless Router Remote Command Execution POC https://gist.github.com/Swind1er/40c33f1b1549028677cb4e2e5ef69109#file-d-link-dir-823x-ax3000-dual-band-gigabit-wireless-router-remote-command-execution-poc-md〔2025/6/18 確認〕
※ 248 D-Link 社：(non-US) DIR-823X :: Rev. Ax :: F/W 固件 - 240126 :: LAN-Side Authenticated Remote Command Execution https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10404〔2025/6/18 確認〕
※ 249 D-Link 社：(Non-US) DIR-846W：All H/W Revs. & All F/W Vers.：End-of-Life (EOL) / End-of-Service (EOS)：CVE-2024-41622/44340/44341/44342 Vulnerability Reports https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10411〔2025/6/18 確認〕
※ 250 TWCERT/CC：D-Link WiFi router - Stack-based Buffer

Overflow https://www.twcert.org.tw/en/cp-139-8081-3fb39-2.html〔2025/6/18 確認〕
TWCERT/CC：D-Link WiFi router - Stack-based Buffer Overflow https://www.twcert.org.tw/en/cp-139-8083-a299e-2.html〔2025/6/18 確認〕
TWCERT/CC：D-Link WiFi router - Hidden Functionality https://www.twcert.org.tw/en/cp-139-8087-c3e70-2.html〔2025/6/18 確認〕
TWCERT/CC：D-Link WiFi router - Hidden Functionality https://www.twcert.org.tw/en/cp-139-8089-32df6-2.html〔2025/6/18 確認〕
TWCERT/CC：D-Link WiFi router - OS Command Injection https://www.twcert.org.tw/en/cp-139-8091-bcd52-2.html〔2025/6/18 確認〕
※ 251 D-Link 社：DIR-X4860 / DIR-X5460 / COVR-X1870 :: TWCERT - TVN-202409021 / TVN-202409022 / TVN-202409023 / TVN-202409024 / TVN-202429025 Vulnerabilities reports https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10412〔2025/6/18 確認〕
※ 252 CISA：CISA Adds Four Known Exploited Vulnerabilities to Catalog https://www.cisa.gov/news-events/alerts/2024/09/30/cisa-adds-four-known-exploited-vulnerabilities-catalog〔2025/6/18 確認〕
※ 253 JVN：JVNVU#91401812, Multiple TP-Link products vulnerable to OS command injection https://jvn.jp/en/vu/JVNVU91401812/〔2025/6/18 確認〕
※ 254 サイファーマ株式会社：Comprehensive Analysis of CVE-2024-21833 Vulnerability in TP-Link Routers : Threat Landscape, Exploitation Risks, and Mitigation Strategies https://www.cyfirma.com/research/comprehensive-analysis-of-cve-2024-21833-vulnerability-in-tp-link-routers-threat-landscape-exploitation-risks-and-mitigation-strategies/〔2025/6/18 確認〕
※ 255 ONEKEY：Security Advisory: Arbitrary Command Execution on TP-Link Archer C5400X https://www.onekey.com/resource/security-advisory-remote-command-execution-on-tp-link-archer-c5400x〔2025/6/18 確認〕
※ 256 Thottysploity：CVE-2024-53375 TP-Link Archer router series Authenticated RCE https://thottysploity.github.io/posts/cve-2024-53375/〔2025/6/18 確認〕
※ 257 NETGEAR 社：Security Advisory for Authentication Bypass on Some Routers, PSV-2023-0166 https://kb.netgear.com/000066096/Security-Advisory-for-Authentication-Bypass-on-Some-Routers-PSV-2023-0166〔2025/6/18 確認〕
※ 258 Redfox Cyber Security Inc.：Security Advisory - Multiple Vulnerabilities in Netgear WNR614 Router https://redfoxsec.com/blog/security-advisory-multiple-vulnerabilities-in-netgear-wnr614-router/〔2025/6/18 確認〕
※ 259 NETGEAR 社：Security Advisory for Stored Cross Site Scripting on Some Routers, PSV-2023-0122 https://kb.netgear.com/000066264/Security-Advisory-for-Stored-Cross-Site-Scripting-on-Some-Routers-PSV-2023-0122〔2025/6/18 確認〕
NETGEAR 社：Security Advisory for Authentication Bypass on Some Cable Modem Routers, PSV-2023-0138 https://kb.netgear.com/000066265/Security-Advisory-for-Authentication-Bypass-on-Some-Cable-Modem-Routers-PSV-2023-0138〔2025/6/18 確認〕
※ 260 CoreSecurity OT/ICS Research Team：CVE-2024-33788 https://github.com/ymkyu/CVE/tree/main/CVE-2024-33788〔2025/6/18 確認〕
CoreSecurity OT/ICS Research Team：CVE-2024-33789 https://github.com/ymkyu/CVE/tree/main/CVE-2024-33789〔2025/6/18 確認〕
※ 261 Mike：LINKSYS AC1900 EA7500v3 IGD UPnP Stack Buffer Overflow Remote Code Execution Vulnerability https://github.com/dest-3/CVE-2023-46012〔2025/6/18 確認〕
※ 262 CISA：CISA Adds Three Known Exploited Vulnerabilities to Catalog https://www.cisa.gov/news-events/alerts/2024/09/03/cisa-adds-three-known-exploited-vulnerabilities-catalog〔2025/6/18 確認〕
※ 263 Giles-one：Vigor2960Crack https://github.com/Giles-one/Vigor2960Crack〔2025/6/18 確認〕
※ 264 Netsecfish：Command Injection in `apmcfgupload` endpoint for DrayTek Gateway Devices https://netsecfish.notion.site/〔2025/6/18 確認〕
※ 265 TWCERT/CC：ASUS Router - Improper Authentication https://www.twcert.org.tw/en/cp-139-7860-760b1-2.html〔2025/6/18 確認〕
TWCERT/CC：ASUS Router - Stack-based Buffer Overflow https://www.twcert.org.tw/en/cp-139-7858-3c978-2.html〔2025/6/18 確認〕
※ 266 TWCERT/CC：ASUS Router - Upload arbitrary firmware https://www.twcert.org.tw/en/cp-139-7876-396bd-2.html〔2025/6/18 確認〕
※ 267 GL Technologies (Hong Kong) Limited：Security Advisories (Vulnerabilities and CVEs) August 1 2024 https://www.gl-inet.com/security-updates/security-advisories-vulnerabilities-and-cves-aug-1-2024/〔2025/6/18 確認〕
※ 268 Cisco 社：TALOS-2023-1871, LevelOne WBR-6013 telnetd hard-coded password vulnerability https://talosintelligence.com/vulnerability_reports/TALOS-2023-1871〔2025/6/18 確認〕
Cisco 社：TALOS-2023-1873, LevelOne WBR-6013 boa formSysCmd leftover debug code vulnerability https://talosintelligence.com/vulnerability_reports/TALOS-2023-1873〔2025/6/18 確認〕
※ 269 telnetd：Telnet プロトコルを用いた遠隔操作に対応するための常駐プログラム。
※ 270 QNAP 社：QSA-24-44, Multiple Vulnerabilities in QuRouter https://www.qnap.com/en-au/security-advisory/qsa-24-44〔2025/6/18 確認〕
※ 271 无名草 talent：CVE-2024-29269 / index.md https://github.com/wutalent/CVE-2024-29269/blob/main/index.md〔2025/6/18 確認〕
※ 272 Valentin Lobstein：CVE-2024-29269 Exploit https://github.com/Chocapikk/CVE-2024-29269〔2025/6/18 確認〕
※ 273 株式会社アイ・オー・データ機器：「UD-LT1」「UD-LT1/EX」ファームウェア更新およびセキュリティ対策のお願い https://www.iodata.jp/support/information/2024/11_ud-lt1/index.htm〔2025/6/18 確認〕
※ 274 セイコーソリューションズ株式会社：SkyBridge MB-A100/110・SkyBridge BASIC MB-A130 の脆弱性と対応について https://www.seiko-sol.co.jp/archives/82992/〔2025/6/18 確認〕
※ 275 センチュリー・システムズ株式会社：センチュリー・システムズ製 FutureNet NXR シリーズにおける REST-API 機能が意図せず有効化される問題について https://www.centurysys.co.jp/backnumber/nxr_common/20241031-01.html〔2025/6/18 確認〕
※ 276 SSD Secure Disclosure：SSD Advisory - QNAP QTS5 – /usr/lib/libqcloud.so JSON parsing leads to RCE https://ssd-disclosure.com/ssd-advisory-qnap-qts5-usr-lib-libqcloud-so-json-parsing-leads-to-rce/〔2025/6/18 確認〕
※ 277 QNAP 社：QSA-23-64, Vulnerability in QTS and QuTS hero https://www.qnap.com/en/security-advisory/qsa-23-64〔2025/6/18 確認〕
※ 278 QNAP 社：QSA-23-47, Vulnerability in QTS, QuTS hero and QuTScloud https://www.qnap.com/en/security-advisory/qsa-23-47〔2025/6/18 確認〕
QNAP 社：QSA-23-30, Vulnerability in QTS, QuTS hero and QuTScloud https://www.qnap.com/en/security-advisory/qsa-23-30〔2025/6/18 確認〕
QNAP 社：QSA-24-05, Multiple Vulnerabilities in QTS, QuTS hero and QuTScloud https://www.qnap.com/en/security-advisory/qsa-24-05〔2025/6/18 確認〕
※ 279 QNAP 社：QSA-24-03, Vulnerability in Qsync Central https://www.qnap.com/en/security-advisory/qsa-24-03〔2025/6/18 確認〕
※ 280 QNAP 社：QSA-23-57, Multiple Vulnerabilities in QTS, QuTS hero and QuTScloud https://www.qnap.com/en/security-advisory/qsa-23-57〔2025/6/18 確認〕
※ 281 Rapid7 Inc.：CVE-2023-47218: QNAP QTS and QuTS Hero Unauthenticated Command Injection (FIXED) https://www.rapid7.com/blog/post/2024/02/13/cve-2023-47218-qnap-qts-and-quts-hero-unauthenticated-command-injection-fixed/〔2025/6/18 確認〕
Palo Alto Networks 社：New Vulnerability in QNAP QTS Firmware: CVE-2023-50358 https://unit42.paloaltonetworks.com/qnap-qts-firmware-cve-2023-50358/〔2025/6/18 確認〕
パロアルトネットワークス株式会社：QNAP QTS ファームウェアに新たな脆弱 性：CVE-2023-50358 https://unit42.paloaltonetworks.com/ja/qnap-qts-firmware-cve-2023-50358/〔2025/6/18 確認〕
※ 282 QNAP 社：QSA-24-09, Multiple Vulnerabilities in QTS, QuTS hero, QuTScloud, myQNAPcloud, and myQNAPcloud Link (PWN2OWN 2023) https://www.qnap.com/en/security-advisory/qsa-24-09〔2025/6/18 確認〕
※ 283 watchTowr Labs：QNAP QTS - QNAPping At The Wheel (CVE-2024-27130 and friends) https://labs.watchtowr.com/

qnap-qts-qnapping-at-the-wheel-cve-2024-27130-and-friends/〔2025/6/18 確認〕
watchTowr Labs：CVE-2024-27130 https://github.com/watchtowrlabs/CVE-2024-27130〔2025/6/18 確認〕
※ 284 QNAP 社：QSA-24-20, Multiple Vulnerabilities in QTS and QuTS hero https://www.qnap.com/en/security-advisory/qsa-24-20〔2025/6/18 確認〕
※ 285 QNAP 社：QSA-24-23, Multiple Vulnerabilities in QTS and QuTS hero https://www.qnap.com/en/security-advisory/qsa-24-23〔2025/6/18 確認〕
QNAP 社：QNAP PSIRT からの最近の セキュリティ レポートに関する公式回答（WatchTowr Labs） https://www.qnap.com/ja-jp/news/2024/qnap-psirt- からの最近の - セキュリティ - レポートに関する公式回答 watchtowr-labs〔2025/6/18 確認〕
※ 286 QNAP 社：QSA-24-41, Vulnerability in HBS 3 Hybrid Backup Sync (PWN2OWN 2024) https://www.qnap.com/en/security-advisory/qsa-24-41〔2025/6/18 確認〕
※ 287 QNAP 社：QSA-24-49, Multiple Vulnerabilities in QTS and QuTS hero (PWN2OWN 2024) https://www.qnap.com/en/security-advisory/qsa-24-49〔2025/6/18 確認〕
※ 288 QNAP 社：QSA-24-50, Vulnerability in License Center https://www.qnap.com/en/security-advisory/qsa-24-50〔2025/6/18 確認〕
※ 289 NetworkSecurityFish：Command Injection and Backdoor Account in D-Link NAS Devices https://github.com/netsecfish/dlink〔2025/6/18 確認〕
※ 290 D-Link 社：DNS-320L / DNS-325 / DNS-327 / DNS-340L and All D-Link NAS Storage :: All Models and All Revison :: End of Service Life :: CVE-2024-3273 & CVE-2024-3272: Vulnerabilities Reported https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383〔2025/6/18 確認〕
※ 291 サイファーマ株式会社：Threat Actors Actively Exploiting CVE-2024-3273：Underground Forums Share IP Addresses of Vulnerable D-Link NAS Devices https://www.cyfirma.com/research/threat-actors-actively-exploiting-cve-2024-3273-underground-forums-share-ip-addresses-of-vulnerable-d-link-nas-devices/〔2025/6/18 確認〕
※ 292 NetworkSecurityFish：Command Injection Vulnerability in `name` parameter for D-Link NAS https://netsecfish.notion.site/Command-Injection-Vulnerability-in-name-parameter-for-D-Link-NAS-12d6b683e67c80c49ffcc9214c239a07〔2025/6/18 確認〕
※ 293 Outpost24 AB：Five new vulnerabilities found in Zyxel NAS devices (including code execution and privilege escalation) https://outpost24.com/blog/zyxel-nas-critical-vulnerabilities/〔2025/6/18 確認〕
※ 294 Zyxel 社：Zyxel security advisory for multiple vulnerabilities in NAS products https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-nas-products-06-04-2024〔2025/6/18 確認〕
※ 295 The Shadowserver Foundation：https://x.com/Shadowserver/status/1804131462163108137〔2025/6/18 確認〕
※ 296 NVD：CVE-2024-6342 Detail https://nvd.nist.gov/vuln/detail/cve-2024-6342〔2025/6/18 確認〕
※ 297 Zyxel 社：Zyxel security advisory for OS command injection vulnerability in NAS products https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-nas-products-09-10-2024〔2025/6/18 確認〕
※ 298 Synology 社：Synology-SA-24:19 Synology Photos (PWN2OWN 2024) https://www.synology.com/en-global/security/advisory/Synology_SA_24_19〔2025/6/18 確認〕
※ 299 Western Digital Corporation：Western Digital My Cloud OS 5 Firmware 5.29.102 https://www.westerndigital.com/support/product-security/wdc-24005-western-digital-my-cloud-os-5-firmware-5-29-102〔2025/6/18 確認〕
※ 300 HP Aruba Networking：Aruba Access Points Multiple Vulnerabilities https://csaf.arubanetworks.com/2024/hpe_aruba_networking_-_2024-006.txt〔2025/6/18 確認〕
HPE 社：HPESBNW04647 rev.2 - HPE Aruba Access Points, Multiple Vulnerabilities https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04647en_us〔2025/6/18 確認〕
※ 301 Zyxel 社：Zyxel security advisory for OS command injection vulnerability in APs and security router devices https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024〔2025/6/18 確認〕
※ 302 CurryXiao：CVE_TP-Link_report https://gist.github.com/XiaoCurry/14d46e0becd79d9bb9907f2fbe147cfe〔2025/6/18 確認〕
※ 303 TWCERT/CC：GeoVision EOL device - OS Command Injection https://www.twcert.org.tw/en/cp-139-7884-c5a8b-2.html〔2025/6/18 確認〕
※ 304 TWCERT/CC：GeoVision EOL devices - OS Command Injection https://www.twcert.org.tw/en/cp-139-8237-26d7a-2.html〔2025/6/18 確認〕
※ 305 Synology 社：Synology-SA-23:15 Synology Camera (PWN2OWN 2023) https://www.synology.com/en-global/security/advisory/Synology_SA_23_15〔2025/6/18 確認〕
※ 306 NetworkSecurityFish：Sensitive Device Information Disclosure in TVT DVR https://netsecfish.notion.site/Sensitive-Device-Information-Disclosure-in-TVT-DVR-fad1cce703d946969be5130bf3aaac0d〔2025/6/18 確認〕
※ 307 CISA：ICS Advisary - AVTECH IP Camera https://www.cisa.gov/news-events/ics-advisories/icsa-24-214-07〔2025/6/18 確認〕
※ 308 Akamai Technologies：Beware the Unpatchable: Corona Mirai Botnet Spreads via Zero-Day https://www.akamai.com/blog/security-research/2024-corona-mirai-botnet-infects-zero-day-sirt〔2025/6/18 確認〕
※ 309 AVTECH 社：陞泰安控聲明 https://www.avtech.com.tw/img/CISA_announcement_tw.pdf〔2025/6/18 確認〕
※ 310 Cisco 社：Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware Vulnerabilities https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-multi-vulns-cXAhCvS〔2025/6/18 確認〕
※ 311 Cisco 社：Cisco Small Business SPA300 Series and SPA500 Series IP Phones Web UI Vulnerabilities https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-http-vulns-RJZmX2Xz〔2025/6/18 確認〕
※ 312 Avaya Inc.：Avaya IP Office Vulnerability (CVE-2024-4196) / (CVE-2024-4197) https://support.avaya.com/css/public/documents/101090768〔2025/6/18 確認〕
※ 313 Bitdefender：Vulnerabilities Identified in LG WebOS https://www.bitdefender.com/en-us/blog/labs/vulnerabilities-identified-in-lg-webos〔2025/6/18 確認〕
※ 314 キヤノン株式会社：CP2024-001 Vulnerabilities Mitigation/Remediation for Small Office Multifunction Printers and Laser Printers https://psirt.canon/advisory-information/cp2024-001/〔2025/6/18 確認〕
※ 315 キヤノン株式会社：CP2024-002 Vulnerability Mitigation/Remediation for Small Office Multifunction Printers and Laser Printers https://psirt.canon/advisory-information/cp2024-002/〔2025/6/18 確認〕
※ 316 シャープ株式会社：About Plural Security Vulnerabilities in SHARP Multifunctional Products (MFP) https://global.sharp/products/copier/info/info_security_2024-10.html〔2025/6/18 確認〕
シャープ株式会社：弊社複合機におけるセキュリティ脆弱性について https://jp.sharp/business/print/information/info_security_2024-10.html〔2025/6/18 確認〕
東芝テック株式会社：Response to vulnerabilities in Toshiba Tec's digital multi-function peripherals https://www.toshibatec.com/information/20241025_01.html〔2025/6/18 確認〕
東芝テック株式会社：東芝テック製デジタル複合機の脆弱性対応について https://www.toshibatec.co.jp/information/20241025_01.html〔2025/6/18 確認〕
※ 317 株式会社リコー：「PostScript インタープリタに於ける脆弱性」(CVE-2023-50734~50736)、「SE メニューの入力検証に於ける脆弱性」(CVE-2023-50737) によるリコー製品への影響について https://jp.ricoh.com/security/products/vulnerabilities/vul?id=ricoh-2024-000001〔2025/6/18 確認〕
※ 318 株式会社リコー：「Server-Side Request Forgery(SSRF) 攻撃に対する脆弱性」(CVE-2023-50733)、「ファームウェアダウングレード保護における脆弱性」(CVE-2023-50738)、「IPP におけるバッファオーバーフローの脆弱性」(CVE-2023-50739) によるリコー製品への影響について https://jp.ricoh.com/security/products/vulnerabilities/vul?id=ricoh-2024-000003〔2025/6/18 確認〕
※ 319 株式会社リコー：「クロスサイトスクリプティングの脆弱性」(CVE-2022-37406) によるリコー製品への影響について https://jp.ricoh.com/security/products/vulnerabilities/vul?id=ricoh-2023-000006〔2025/6/18 確認〕

※ 320 株式会社リコー：リコー製品へのバッファオーバーフローの脆弱性（CVE-2024-39927）の影響について　https://jp.ricoh.com/security/products/vulnerabilities/vul?id=ricoh-2024-000008〔2025/6/18 確認〕
※ 321 株式会社リコー：WebImageMonitor におけるバッファオーバーフローの脆弱性（CVE-2024-47939）　https://jp.ricoh.com/security/products/vulnerabilities/vul?id=ricoh-2024-000011〔2025/6/18 確認〕
※ 322 セイコーエプソン株式会社、エプソン販売株式会社：プリンター、スキャナーおよびネットワークインターフェイス製品の Web Config における脆弱性について　https://www.epson.jp/support/misc_t/240930_03_oshirase.htm〔2025/6/18 確認〕
セイコーエプソン株式会社：Insecure Initial Password Configuration in Epson WebConfig Vulnerability　https://epson.com/Support/wa00958〔2025/6/18 確認〕
※ 323 Zero Day Initiative（トレンドマイクロ社）：Multiple Vulnerabilities in the Mazda In-Vehicle Infotainment (IVI) System　https://www.zerodayinitiative.com/blog/2024/11/7/multiple-vulnerabilities-in-the-mazda-in-vehicle-infotainment-ivi-system〔2025/6/18 確認〕
※ 324 Fortinet, Inc.：Botnets Continue Exploiting CVE-2023-1389 for Wide-Scale Spread　https://www.fortinet.com/blog/threat-research/botnets-continue-exploiting-cve-2023-1389-for-wide-scale-spread〔2025/6/18 確認〕
※ 325 Lumen Technologies, Inc.：The Pumpkin Eclipse　https://blog.lumen.com/the-pumpkin-eclipse/〔2025/6/18 確認〕
※ 326 Juniper Networks, Inc.：2024-12 Reference Advisory: Session Smart Router: Mirai malware found on systems when the default password remains unchanged　https://supportportal.juniper.net/s/article/2024-12-Reference-Advisory-Session-Smart-Router-Mirai-malware-found-on-systems-when-the-default-password-remains-unchanged〔2025/6/18 確認〕
※ 327 Fortinet, Inc.：Botnets Continue to Target Aging D-Link Vulnerabilities　https://www.fortinet.com/blog/threat-research/botnets-continue-to-target-aging-d-link-vulnerabilities〔2025/6/18 確認〕
※ 328 VulnCheck Inc.：7777-Botnet Infection Vectors　https://vulncheck.com/blog/ip-intel-7777-botnet〔2025/6/18 確認〕
VulnCheck Inc.：Xiongmai IoT Exploitation　https://vulncheck.com/blog/xiongmai-iot-exploitation〔2025/6/18 確認〕
※ 329 Jacob Masse：CVE-2024–45163: Remote DoS Exploit in Mirai Botnet　https://jacobmasse.medium.com/remote-dos-exploit-found-in-mirai-botnet-source-code-27a1aad284f1〔2025/6/18確認〕
※ 330 MediaTek 社：Product Security Bulletin　https://corp.mediatek.com/product-security-bulletin〔2025/6/18 確認〕
※ 331 MediaTek 社：March 2024 Product Security Bulletin　https://corp.mediatek.com/product-security-bulletin/March-2024〔2025/6/18 確認〕
※ 332 hyper：4 exploits, 1 bug: exploiting cve-2024-20017 4 different ways　https://blog.coffinsec.com/0day/2024/08/30/exploiting-CVE-2024-20017-four-different-ways.html〔2025/6/18 確認〕
※ 333 Arm Holdings plc：Mali GPU Driver Security Bulletin: 2024 Disclosures　https://developer.arm.com/documentation/110355/1-0/〔2025/6/18 確認〕
※ 334 Qualcomm Technologies, Inc.：October 2024 Security Bulletin　https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html〔2025/6/18 確認〕
※ 335 CISA：CISA Adds Three Known Exploited Vulnerabilities to Catalog　https://www.cisa.gov/news-events/alerts/2024/10/08/cisa-adds-three-known-exploited-vulnerabilities-catalog〔2025/6/18 確認〕
※ 336 Contiki-NG：https://www.contiki-ng.org/〔2025/6/18 確認〕
Contiki-NG：Out-of-bounds read in SNMP when decoding a string　https://github.com/contiki-ng/contiki-ng/security/advisories/GHSA-qjj3-gqx7-438w〔2025/6/18 確認〕
Contiki-NG：Out-of-bounds read in SNMP when decoding a message　https://github.com/contiki-ng/contiki-ng/security/advisories/GHSA-444j-93j3-5gj4〔2025/6/18 確認〕
Contiki-NG：Unaligned memory access in RPL option processing　https://github.com/contiki-ng/contiki-ng/security/advisories/GHSA-crjw-x84h-h6x3〔2025/6/18 確認〕
※ 337 Ambionics Security by LEXFO：Iconv, set the charset to RCE: Exploiting the glibc to hack the PHP engine (part 1)　https://blog.lexfo.fr/iconv-cve-2024-2961-p1.html〔2025/6/18 確認〕
Ambionics Security by LEXFO：CNEXT exploits　https://github.com/ambionics/cnext-exploits/〔2025/6/18 確認〕
Ambionics Security by LEXFO：Iconv, set the charset to RCE: Exploiting the glibc to hack the PHP engine (part 2)　https://blog.lexfo.fr/iconv-cve-2024-2961-p2.html〔2025/6/18 確認〕
Ambionics Security by LEXFO：Iconv, set the charset to RCE: Exploiting the glibc to hack the PHP engine (part 3)　https://blog.lexfo.fr/iconv-cve-2024-2961-p3.html〔2025/6/18 確認〕
※ 338 FreeRTOS：Buffer Over-Read (CWE-126) in DNS Response Parser　https://github.com/FreeRTOS/FreeRTOS-Plus-TCP/security/advisories/GHSA-ppcp-rg65-58mv〔2025/6/18 確認〕
※ 339 OpenWrt Project：Security Advisory 2024-12-06-1 - OpenWrt Attended SysUpgrade server: Build artifact poisoning via truncated SHA-256 hash and command injection (CVE-2024-54143)　https://lists.openwrt.org/pipermail/openwrt-announce/2024-December/000062.html〔2025/6/18 確認〕
※ 340 ビデオ監視システム（video surveillance software system）：Linux または FreeBSD のパソコン上で実行して DVR（Digital Video Recorder）相当の機能を提供するソフトウェア。
※ 341 ZoneMinder：Time-based SQL Injection　https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-9cmr-7437-v9fj〔2025/6/18 確認〕
※ 342 ZoneMinder：Boolean-based SQL Injection in ZoneMinder v1.37.* <= 1.37.64　https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-qm8h-3xvf-m7j3〔2025/6/18 確認〕
※ 343 Top10VPN.com（PrivacyCo Ltd.）：CVE-2023-52424 WiFi Vulnerability: The SSID Confusion Attack　https://www.top10vpn.com/research/wifi-vulnerability-ssid/〔2025/6/18 確認〕
Héloïse Gollier and Mathy Vanhoef：SSID Confusion: Making Wi-Fi Clients Connect to the Wrong Network　https://www.top10vpn.com/assets/2024/05/Top10VPN-x-Vanhoef-SSID-Confusion.pdf〔2025/6/18 確認〕
※ 344 IPA：「IoT 開発におけるセキュリティ設計の手引き」を公開　https://www.ipa.go.jp/security/iot/iotguide.html〔2025/6/18 確認〕
※ 345 IPA：脆弱性対処に向けた製品開発者向けガイド　https://www.ipa.go.jp/security/guide/vuln/forvendor.html〔2025/6/18 確認〕
IPA：脆弱性対処に向けた製品開発者向けガイド　https://www.ipa.go.jp/security/guide/vuln/ug65p90000019bum-att/000085024.pdf〔2025/6/18 確認〕
※ 346 https://www.ipa.go.jp/security/guide/vuln/ug65p90000019bum-att/000065095.pdf〔2025/6/18 確認〕
※ 347 https://www.ipa.go.jp/security/jc-star/index.html〔2025/6/18 確認〕
※ 348 IPA：ネット接続製品の安全な選定・利用ガイド - 詳細版 - https://www.ipa.go.jp/security/guide/vuln/forconsumer.html〔2025/6/18 確認〕
IPA：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 - https://www.ipa.go.jp/security/guide/vuln/ug65p90000019br8-att/000085153.pdf〔2025/6/18 確認〕
※ 349 NOTICE：ルーター / ネットワークカメラの安全な管理方法　https://www.notice.go.jp/safety〔2025/6/18 確認〕
※ 350 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〔2025/6/12 確認〕
※ 351 IPA：「企業における営業秘密管理に関する実態調査 2024」報告書　https://www.ipa.go.jp/security/reports/economics/ts-kanri/tradesecret2024.html〔2025/8/29 確認〕
※ 352 図 1-2-21 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。
※ 353 日本経済新聞：米司法省、Google の中国籍元社員起訴　AI 機密窃取疑い　https://www.nikkei.com/article/DGXZQOGN072U20X00C24A3000000/〔2025/6/12 確認〕
日テレ NEWS NNN：中国企業と協力し AI 技術盗んだグーグル元エンジニアを起訴　米司法省　https://news.ntv.co.jp/category/international/6fdb17c50c294c58a83b8dade736aecc〔2025/6/12 確認〕
※ 354 筑波大学：電子メールの転送先設定ミスによる情報漏えい事案について　https://www.tsukuba.ac.jp/news/20240603140000.html〔2025/6/12 確認〕
※ 355 東急リバブル株式会社：弊社元従業員による個人情報の不正な持ち出しに関するご報告とお詫び　https://www.livable.co.jp/assets/files/3972〔2025/6/12 確認〕
※ 356 TDK 株式会社：当社元従業員の書類送検について　https://www.tdk.com/ja/information/202410_01.html〔2025/6/12 確認〕
読売新聞オンライン：TDKの研究データを不正持ち出し容疑、元研究員を

書類送検…転職に利用計画か　https://www.yomiuri.co.jp/national/20241004-OYT1T50078/〔2025/6/12 確認〕
※ 357 伊福精密株式会社：2025.02.24【会社情報】重要なお知らせとお詫び　https://www.ifukuseimitsu.com/information/20250224/2521/〔2025/6/12 確認〕
※ 358 産経ニュース：「単なる思い出に」同業他社へデータ 6500 件持ち出しか　容疑で金属加工元社員を逮捕　https://www.sankei.com/article/20250220-NGI4ZBY3KRN3JEYUGMF6VZSCWY/〔2025/3/21 確認〕
株式会社サイエンスインパクト：先週の知財ニュースト ピックス（2 月 17 日～2 月 23 日）　https://ipforce.jp/News/ip-news/summary/2025-02-25-7295〔2025/6/12 確認〕
※ 359 国立研究開発法人産業技術総合研究所：職員の逮捕について　https://www.aist.go.jp/aist_j/news/announce/au20230615.html〔2025/6/12 確認〕
※ 360 読売新聞オンライン：産総研の中国人元研究員に有罪判決、中国企業に研究データ漏えい「信頼裏切った」…東京地裁　https://www.yomiuri.co.jp/national/20250225-OYT1T50178/〔2025/6/12 確認〕
※ 361 表 1-2-10 に示した対策は「組織における内部不正防止ガイドライン」の記載内容に沿ってまとめたものである。
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〔2025/6/12 確認〕
※ 362 警視庁：営業秘密漏えい防止　https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/trade_secrets.html#:~:text= 営 業 秘密に関する罪 , に重い犯罪となります。〔2025/6/12 確認〕
※ 363 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/#:~:text= また、個人情報保護委員 ,（法第 178 条）。〔2025/6/12 確認〕
※ 364 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〔2025/6/12 確認〕
※ 365 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）【条文】第 84 条　https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf〔2025/6/12 確認〕
※ 366 ほかにも刑法（窃盗罪、横領罪、背任罪等）や民法（契約責任、不法行為責任等）、労働法（例えば秘密保持義務違反、競業避止義務違反等）、公益通報者保護法も関連する。
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〔2025/6/12 確認〕
※ 367 https://www.ipa.go.jp/security/guide/insider.html〔2025/6/12 確認〕
※ 368 https://www.ipa.go.jp/security/anshin/index.html〔2025/6/12 確認〕
※ 369 IPA：情報セキュリティ安心相談窓口の相談状況［2025 年第 1 四半期（1 月～ 3 月）］　https://www.ipa.go.jp/security/anshin/reports/2025q1outline.html〔2025/6/12 確認〕
※ 370 https://www.ipa.go.jp/security/anshin/attention/2024/mgdayori20241119.html〔2025/6/12 確認〕
※ 371 https://www.ipa.go.jp/security/anshin/measures/f55m8k00000047km-att/supportscam_report2024.pdf〔2025/6/12 確認〕
※ 372 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? - 事例を学び落ち着いて対処できるようにしましょう -　https://www.ipa.go.jp/security/anshin/attention/2023/mgdayori20240227.html〔2025/6/12 確認〕
※ 373 下記 Web ページの「3-2. 個人からの相談事例」参照。
IPA:情報セキュリティ安心相談窓口の相談状況［2024 年第 4 四半期（10 月～ 12 月）］　https://www.ipa.go.jp/security/anshin/reports/2024q4outline.html〔2025/6/12 確認〕
※ 374 ABC ニュース：「パソコンがウイルスに感染」「口座を守るために口座情報教えて」　76歳男性が約4250万円だまし取られる　大津市　https://www.asahi.co.jp/webnews/pages/abc_28658.html〔2025/6/12 確認〕
※ 375 下記 Web ページの「3-2. 個人からの相談事例」の「相談事例 2：サポート詐欺に電話をしてスマートフォンの遠隔操作で不正送金をされた」参照。
IPA：情報セキュリティ安心相談窓口の相談状況［2025 年 1 四半期（1 月～ 3 月）］　https://www.ipa.go.jp/security/anshin/reports/2025q1outline.html#section4〔2025/6/12 確認〕
※ 376 IPA：サポート詐欺で表示される偽のセキュリティ警告画面の閉じ方　https://www.ipa.go.jp/security/anshin/doe3um0000005cag-att/20231115173500.pdf〔2025/6/12 確認〕
※ 377 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〔2025/6/12 確認〕
※ 378 デジタル政策フォーラム：サイバーセキュリティアワード 2025　https://csa.digitalpolicyforum.jp/〔2025/6/12 確認〕
※ 379 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〔2025/6/12 確認〕
※ 380 https://www.zenginkyo.or.jp/hanzai/information/〔2025/6/12 確認〕
※ 381 https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210309.html〔2025/6/12 確認〕
※ 382 フィッシング対策協議会：緊急情報　https://www.antiphishing.jp/news/alert/〔2025/6/12 確認〕
※ 383 株式会社 NTT ドコモ：フィッシング詐欺被害の拡大を防ぐ「意図せぬ迷惑メッセージ送信に関するお知らせ」の提供を開始　https://www.docomo.ne.jp/info/news_release/2024/03/28_00.html〔2025/6/12 確認〕
※ 384 https://smon.tobila.com/〔2025/6/12 確認〕
※ 385 トビラシステムズ株式会社：トビラシステムズ、フィッシング詐欺のリアルタイム観測サイト「詐欺 SMS モニター」の公開継続を決定　https://tobila.com/news/release/p1792/〔2025/6/12 確認〕
※ 386 https://www.npa.go.jp/publications/statistics/kikakubunseki/r6_jyosei.pdf〔2025/6/12 確認〕
※ 387 株式会社 NTT ドコモ：共通ショートコード　https://www.docomo.ne.jp/service/sms/displayname/〔2025/6/12 確認〕
※ 388 KDDI 株式会社：迷惑 SMS ブロック　https://www.au.com/mobile/service/sms/filter/〔2025/6/12 確認〕
※ 389 株式会社 NTT ドコモ：あんしんセキュリティ（迷惑 SMS 対策）　https://anshin-security.docomo.ne.jp/sms/index.html〔2025/6/12 確認〕

第2章
最近のサイバー空間を巡る注目事象

最近のサイバー空間には AI の普及により急速な変化がもたらされている一方、その AI を悪用した偽情報の拡散が公共への大きな脅威となっている。

そこで本章では注目事象として、AI セーフティ実現に向けた取り組みと、偽情報・誤情報の脅威を取り上げる。

2.1 AIセーフティ実現に向けた取り組み

2025 年現在、AI（Artificial Intelligence:人工知能）という言葉は連日のようにニュース等で取り上げられている。その大きな契機となったのは、2022 年 11 月に登場した米国 OpenAI, Inc.（以下、OpenAI 社）の対話形式（チャット形式）で利用できる ChatGPT と、その後に続く、高度な汎用性を備えた AI の急速な発展と普及であろう。最先端の汎用的 AI（General-purpose AI）は、あたかも人間の知能を再現あるいは凌駕するような振る舞いを見せるが、実際にそれらの AI が何を実現するのか、その利用にどのような危険性があり、具体的な対策として何が講じられているのかについて、様々な議論が展開されている。本節では、AI の技術的概要、想定されているリスク、AI の安全な利用に関わる取り組み、AI とサイバーセキュリティにまたがる議論を概観する。

2.1.1 AIの急速な発展

AI 技術の研究史はコンピューターの登場から間もない 1950 年代にまでさかのぼり、代表的な技術も度々変化を重ねている。技術の発展とともに AI のできることが広がる一方で、AI の詳細な動作に対する理解は困難なものとなり、最先端の AI は事実上のブラックボックスと化している。本項では、AI 技術の発展を大まかに振り返る。

(1) 20 世紀中の AI 技術

1950 年代からインターネットの本格普及期となる 2000 年ごろにかけて、AI 技術や関連技術が数多く開発された。チェスや将棋を指すプログラムも最初期のころから存在している。自動計画や論理型プログラミングといった分野の研究も広がった。人間の脳の神経網にヒントを得て考案されたニューラルネットワークも古くより研究されている。例えば、1989 年に米国では、ニューラルネットワークを用いた文字認識により、手書きの郵便番号を機械に判読させる技術が実用化された※1。

(2) 機械学習とディープラーニングで発展した AI

2000 年ごろを境に世界中でインターネットの利用が爆発的に広まり、デジタル化されたデータの量も飛躍的に増大した。しかもこれらのデータはインターネットを通じて全世界に公開され、AI の技術開発にも利用できるデータが多く含まれていた。更に、コンピューター自身の高性能化によって、膨大な量のデータを高速に処理できる環境が整った。特に、AI が必要とする種類の計算処理に有効な、GPU（Graphics Processing Unit）と呼ばれる半導体の開発と普及が進んだ。GPU は当初はゲーム用の描画処理高速化のために開発されたものだが、その計算能力が AI 分野でも有益であると広く認識されるようになり、AI の計算処理に使用されるようになった。このような背景のもとに、「機械学習（machine learning）※2」と呼ばれる技術が 2000 年代に急速に発達した。機械学習の発達によって、従来の AI では難しいとされていた水準の性能が、様々な用途において実現された。例えば、電子メールのスパムフィルターの高性能化※3 や、EC サイトにおける高精度なレコメンデーション等※4 である。

更に機械学習の発達には、ニューラルネットワーク技術の大幅な進歩があった。大きな転換点となったのは、ディープラーニング（深層学習）※5 の登場である。ニューラルネットワークは人間の神経細胞を模した基本部品（人工ニューロン）が連なってできるネットワークであるが、これを大規模化する技術を実用化したものがディープニューラルネットワークである。ディープニューラルネットワークの

関連技術を総称してディープラーニングと呼ぶ。

写真を見てその写真に写っているものが何かを高精度に判定できるAIは、ディープラーニングによって2012年ごろに実現した。ディープラーニングはその後長足の進歩を遂げ、人間の発話を聞き取って文字に変換したり、テキストで与えた指示に基づいて絵を描いたり、自然言語のクイズに答えたり等、従来であれば困難であった様々な機能を、しばしば人間よりも優れた正答率で実現する水準に達した※6。他方で、ディープニューラルネットワークが人間をも凌駕する程の性能をどのように発揮するのか、動作メカニズムの詳細を明確に説明することは困難になっていった。

(3)汎用的AIの登場・発展

「文章、画像、プログラム等を生成できるAI」を総称して「生成AI(Generative AI)」と呼ぶ※7。生成AIの特徴は、自然言語文での入力が可能である等、入力データの自由度が非常に高く、それらの入力に対して適切に見える結果を生成することである。生成AIサービスの代名詞となったOpenAI社のChatGPTは2022年11月に登場した※8。ChatGPTは、対話形式(チャット形式)で、人間が入力した自然言語文に対し、人間のような自然な応答を返す。自由度の高い入力を受け付けるという性質は、入力内容を変えるだけで、一つのAIを多種多様な用途に転用できる可能性を示唆する。欧州連合(EU:European Union)の「AI Act※9」では、著しい汎用性を示し、異なるタスクを広範囲にわたって適切に実行でき、多種多様なシステムやアプリケーションに統合可能なAIを「汎用的AI(General-purpose AI)」と呼んでいる。生成AIは汎用的AIの中核的実装技術となっている。

汎用的AIの開発にあたっては、従来とは桁違いに大規模なディープニューラルネットワークを対象に、膨大な量の機械学習を実行する必要がある。そのためには、高度な技術・知見を有する専門家を集め、学習に必要な大量のデータを収集し、膨大な計算を実行するための大規模なコンピューター資源を確保することが必要とされる※10。代表的な汎用的AIとしては、OpenAI社のGPT、Meta Platforms, Inc.(以下、Meta社)のLLaMA、Google LLC(以下、Google社)のGemini、Anthropic PBCのClaude等がよく知られている。これらの開発元企業はいずれも高度な技術力と莫大な資金を有するグローバル企業である。経済的体力が必要な汎用的AI開発競争には高い参入障壁が築かれている現状があり※11、この状況は経済的・技術的な「AI軍拡競争(AI arms race)」とも呼ばれる※12。

汎用的AIの技術の発達の勢いは衰えを見せず、去年できなかったことが今年はでき、今できないことが来年あるいは3ヵ月後にも可能になるかもしれないというスピード感で開発競争は進んでいる。この背景には、ディープニューラルネットワークの規模や駆動計算量を拡大すればそれに応じてAIの性能が向上し、この傾向に上限がないという経験則(スケーリング則)※13が発見されたことがある。実際、汎用的AIの性能を測るベンチマークテストにおいて、汎用的AIの正答率は人間を超える水準に順次到達している※14。遠くない将来には、あらゆる面で人間と伍する「AGI(Artificial General Intelligence:汎用人工知能)」や人間を超える「ASI(Artificial Super Intelligence:人工超知能)」と呼ばれるAIが登場するという議論もあるが、実現可能性は定かでない。その反面、汎用的AIの動作メカニズムは解明されておらず、AIの研究開発者の間でもブラックボックスとなっている。AIのブラックボックス性は、後述するAIセーフティをどう保証するかという課題にも密接に関わっている。

AIの発展を振り返ってみると、機能の多様化、性能の向上と引き換えに、AIの内部動作はブラックボックス化が進んできたと言える。ブラックボックスであるということは、AIが何かの拍子に人間の期待に反する危険な挙動を見せるおそれがあることも意味する。高度な機能・性能による利益を求めてブラックボックス化した汎用的AIを利用するのか、リスクを回避し、汎用性には乏しいが振る舞いがよく解明されている従来のAIを利用するのか、あるいは、リスク対策を徹底した上で汎用的AIを積極的に採用するのかという、リスクを意識したトレードオフ判断がAI利活用に求められている。

2.1.2 AIリスクとは何か

AIの利用の拡大や社会への浸透に伴って何らかの危害が人間や社会に生じるリスクをAIリスクと呼ぶ。2025年1月末に英国科学技術イノベーション省(DSIT:Department for Science, Innovation & Technology)が発表した「International AI Safety Report 2025※15」は、AIリスクに関する議論を進める調査報告書であり、その中では、汎用的AIを念頭に置きつつ、AIリスクを次のように整理している。

- AIの悪用がもたらすリスク
- AIの不適切動作によるリスク

- システミックリスク

次項ではこれらのリスクについて、関連する実事例等を紹介しながらより詳細な説明を行う。

(1) AI の悪用がもたらすリスク

サイバー犯罪者等が AI を悪用することで生じるリスクである。生成 AI によって作られた合成ポルノ画像の流布による個人攻撃や人権侵害、架空のニュース画像等による世論操作、サイバー攻撃の半自動化、化学兵器・生物兵器開発の支援等がこれに該当する。

(a) フェイク画像等がもたらす個人への被害

生成 AI が生み出す、本物と見分けがつかない偽の画像や動画、音声、及びその生成技術を「ディープフェイク※16」と呼ぶ。人物の写真を与えてその顔を入れ替えたり表情を変えたりといった加工が行えるだけでなく、まったく架空の画像を作り出すこともできる。ディープフェイクはディープラーニングの登場から程なくして発達し、ディープフェイクを悪用した詐欺や恐喝、個人や組織の評判を傷つけるための偽情報の拡散、心理的な虐待といった悪用が FBI により警告されている※17。特に、女性や子供が被害者となるケースが多く、深刻な人権侵害となる可能性がある※18。英国の調査※19 では、女性は男性よりもディープフェイクによる被害をより恐れているという。日本においても、子供達が性的虐待コンテンツを AI で生成した・生成された事例が報道※20 されており、問題は深刻化の一途をたどっている。

(b) 世論操作

ディープフェイクの増加は、偽情報による世論操作のリスクも深刻化させている。悪意のある人物や団体が AI で生成された偽情報を用いることで、大規模かつ巧妙な世論操作が可能になるのではないかという議論があり、懸念が高まっている。近年は、国家を背景とする脅威アクターがこのような活動を試みる場合、これを「影響工作（Influence Operations）」と呼ぶことが多い※21。

ロシアによるウクライナ侵攻が起きた 2022 年にはウクライナのゼレンスキー大統領が降伏を宣言するディープフェイク動画が流布された※22。報道によれば、ロシアの関与があるとされる「Doppelgänger（ドッペルゲンガー）」という脅威アクターは、偽ニュースやディープフェイク動画を駆使して、ウクライナや西側諸国を否定的に、ロシアを肯定的に描いたコンテンツを広めようと試みたとされる※23。更に、2024 年の米国大統領選挙においても偽情報の拡散活動を行ったとされ、米国司法省による取り締りが行われている※24。日本に対しても、東京電力ホールディングス株式会社福島第一原子力発電所の処理水の海洋放出に合わせるように、「処理水ではなく核汚染水だ」という言説とともに不安を煽る偽情報が SNS を中心に広がった事例を OpenAI 社が報告している※25。ディープフェイク等の偽情報の脅威については「2.2 偽・誤情報の脅威の動向」を参照されたい。

(c) AI を悪用したサイバー攻撃

標的型攻撃のような高度なサイバー攻撃が汎用的 AI によって完全に自動化されるのではないかという懸念がある。幸いなことに、2024 年夏の時点では AI の能力はその水準に達していないと評価されている※26。他方で、ChatGPT のような AI サービスを活用することで、手動で行うサイバー攻撃を効率化する試みが、OpenAI 社と Microsoft Corporation（以下、Microsoft 社）によって確認・摘発されている※27。汎用的 AI を利用することで、高度な技能を持たない人物であってもサイバー攻撃を実践できると指摘されており、サイバー犯罪ビジネスへの参入障壁を引き下げてしまうことが、目下の大きな懸念となっている※28。日本においても、中高生 3 人が汎用的 AI を悪用してハッキング行為を行い、携帯電話会社の契約システムに不正ログインを繰り返し、利益を上げていたという事例が 2025 年 2 月に報道された※29。

(d) CBRN 兵器の開発支援

化学兵器や核兵器等の大量殺戮のおそれのある兵器は、化学（Chemical）、生物（Biological）、放射性物質（Radiological）、核（Nuclear）それぞれの頭文字を取って CBRN 兵器と呼ばれる。開発に必要な知見の多くは国家機密として管理され、材料となる物資の流通が厳格に規制されているため、国家以外のアクターが CBRN 兵器を開発することは容易ではない。しかし、インターネット上に存在する膨大な知識を学習している汎用的 AI や、化学物質や合成生物学に特化した AI であれば、少なくとも知見については十分に補えるのではないかという懸念がある。本項執筆時点で、これが机上の空論ではないことを示す研究※30 や事例※31 の報告がある。報告された事例では、汎用的 AI に生物兵器の開発に関する助言を求め、その助言に基づき民間サービスを駆使して合成した DNA をホワイトハウスに持ち込むというデモンストレーションが行われた。2025 年 1 月時

点※32で、汎用的AIは仮想的なエキスパートとして振る舞える可能性があるとの指摘や、チャットを通じて利用できる汎用的AIよりも合成生物学等に特化したAIの方が有力であるとの指摘もあり、議論は定まっていない。

(2) AIの不適切動作によるリスク

AIによる利用者の意図しない動作によって生じるリスクである。事業管理を任せていたAIが誤作動を起こし損失を被る、AIに履歴書の審査を任せていたところ特定の集団を差別するような偏った審査結果が発覚する、AIが人間の意図と大きく異なる振る舞いを示しAIを含むITシステムが暴走する等が該当する。

悪用は、誰かに危害を与えるような結果を意図して招く行為であるのに対し、不適切動作は、その背後に誰かの悪意がなくても、利用者の意図に沿わない振る舞いをAIが示した結果として事故が起こり、危害が生じる可能性のある動作を指す。以下に示すのはこの種の不適切動作に由来するリスクである。

(a) 信頼性の問題

OpenAI社は、同社のAIであるGPT-4が模擬的な司法試験※33で受験者の上位10%に入る成績を収める性能を発揮したと2023年3月に報告した※34。同時期に、当時のChatGPTが米国の医師国家試験に対して合格水準の成績を獲得できたとの報告もあった※35。このような結果は、汎用的AIが高度な専門家を凌駕する知性を獲得したかのような印象を与える。しかし、前者の模擬司法試験の成績は、最終的な司法試験合格者の中位以下の成績に相当し、必ずしも優れた結果とは言えないことが判明した※36。更に、医療における汎用的AIの性能評価を行った結果、ChatGPTも含め、人種間で答えに差異のない医療上の質問に対して、あたかも人種間で違いがあるような示唆を含む返答が得られた※37。

これらの事例は、AIの振る舞いの信頼性は限られた尺度や切り口だけでは十分に評価できない可能性を示しており、AIに何かの仕事を任せる際には、その結果を任せた人間がしっかりとチェックする必要があると言える。2023年には、米国ニューヨーク州の民事訴訟に必要な資料を作成するのに弁護士が生成AIを利用したところ、実在しない判例6件が参照されていたことが発覚している※38。2025年3月には、日本のこども家庭庁において、虐待が疑われる子供を児童相談所で一時保護するかどうかの判定を支援するAIを開発しようとしたところ、AIによる判定の正確性が疑われるケースが全体の約6割を占め、システムの導入が見送られた※39。

(b) バイアス

与えられた情報を適切に分類することはAIに期待される重要な機能の一つである。例えば、人事部門に寄せられた就職希望者の履歴書を見てAIに採用の適否を判定させることが考えられる。この取り組みは汎用的AIが登場する前の2014年ごろに実際にAmazon.com, Inc.（以下、Amazon社）において試みられたが、技術職への応募履歴書を評価する際に、対象者が女性であるというだけで評価が下がるという偏り（バイアス）が生じることが判明し、当該プロジェクトは中止となった※40。これは過去に採用されていた技術職が男性ばかりであり、機械学習のデータとしてそれらの偏りのある履歴書を用いた結果とされる。同様のバイアスは、顔認識※41や再犯予測※42の傾向に人種別で偏りが出る等の、人権侵害につながる事例が報告されている。また、汎用的AIにおいても、特定職業の従事者の画像を描かせると性別に関するバイアスが生じること※43や、テキストの出力であっても類似するバイアスが生じること※44が知られている。

バイアスを生じさせる要因の中で代表的なものは、学習データ自身の偏りである。上記のAmazon社の事例のように、AIが参考にするデータ自身に偏りがある場合に、これをAI自身が是正することは基本的にできない。このため、学習データの準備の際に入念な配慮を行う必要があるが、学習データの母体となる実社会自体に偏りがある場合には、もはやデータ自体の問題とは言えず、容易には解決できない問題となっている。

(c) コントロールの喪失

例えば、工場内の機器に対するAI制御が人間の手を離れてしまい、非常停止等の介入ができなくなる事態は、コントロールの喪失と見なされる。AIの動作が人間の期待から逸脱した状態でコントロールの喪失が発生すると、大きな被害がもたらされるおそれがある。

Sakana AI株式会社は、学術論文の執筆をアイデアの考案から検証、結果のまとめに至るまで自動化するAI Scientistという研究プロジェクトを2024年8月に発表し注目された※45。この発表は学術研究の自動化を試みておおむね成功したという点だけでなく、自動化された研究プロセスの中で、研究の際の実験時間制限を不正に書き換える等のAIの不適切動作が確認されたという点

でも議論を呼んだ。同社は2025年2月にも、AIの動作の高速化をAI自身に行わせるAI CUDA Engineerという手法を発表し、大幅な高速化を達成したとうたった[※46]。しかし、AIがシステム内の評価コードの抜け穴を見つけ、精度の検証等のチェックを回避していることが判明した。同社は後日、見かけの高速化を行う抜け道をAI自身が発見し悪用したことと、修正に取り組むことを発表した[※47]。AIがいわば人間を出し抜くような振る舞いを見せる傾向は、高度な推論能力を持つとされる最先端の汎用的AIでも見られたとの実験結果が報告されている[※48]。

(3) システミックリスク

AI自体は正常に動作していても、社会にAIが浸透する過程で社会の中の様々なバランスが崩れて、何らかの被害を生じるリスクがある。例えば、労働者の業務がAIに置き換えられることで失業者が増える、一部の大企業や先進国にAIの研究開発能力等が集中し格差が広がる、一部の大手AIベンダーがAI市場を独占することでそれらのAIの不具合が世界に影響する、AIの動作に必要な電力や水資源の多大な消費が著しい環境負荷となる、分散している断片的な個人情報をAIが統合・分析することでプライバシーが侵害される、AIの生成した画像や音声が著作権を侵害する等が該当する。AIが組み込まれた社会システムにおいて発現するこれらのリスクは、AIシステムが社会全体に対して広範かつ深刻な影響を及ぼす可能性を持つものであり、単一の不具合や誤作動が連鎖的に波及し、社会的・経済的に大規模な影響を引き起こすリスクを指してシステミックリスクと呼ばれ、以下のように既に複数の懸念が指摘されている。

(a) 労働市場リスク

汎用的AIは多種多様な業務の効率化を支援する。例えば、プログラミング支援AIツールであるGitHub Copilotを使用したプログラマーの生産性が向上した事例[※49]、中程度の専門的なライティングを主体とする業務において4割の時間短縮と質の向上が達成できた事例[※50]等が報告されている。このような生産性の向上は省力化につながり、結果として、労働市場における求人数の減少が起こると考えられる。世界有数のフリーランス事業者向けマッチングサイトである米国Upworkでは、ChatGPTが登場した2022年11月から2024年2月にかけて、ライティング、カスタマーサービス、翻訳といった、汎用的AIによる支援が有効な職種において16～33%の求人数の減少が確認された[※51]。依頼に伴う時給も下落しており、翻訳業務については20%以上の賃下げが見られた。これらの事象は失業率の上昇を示すものではないが、汎用的AIの浸透がもたらす社会的な負の側面を示す事例である。米国において生じた1980年から2016年にかけての賃金格差の拡大の半分以上は、高度な技術による自動化の影響を受けて、定型業務に特化した労働者の賃金が低下したことで説明されるとの指摘[※52]もあり、AIによる更なる自動化が労働市場に小さくない影響を及ぼす可能性が懸念されている。

(b) 世界的なAI研究開発格差

2024年を起点に過去8年を振り返ると、最先端のAIによる学習にかかるコストは毎年2～3倍のペースで増加しており、2027年までに10億ドルを超える可能性があるとされる[※53]。Google社は2022年に米国ネブラスカ州に6億ドルをかけてデータセンターを建設[※54]し、2024年にはミズーリ州に10億ドル規模のデータセンターを建設する計画を発表した[※55]。2024年12月にMeta社は、AIの進歩を支えるためとして、100億ドル以上を投資して米国ルイジアナ州に新たなデータセンターを建設することを発表した[※56]。これらの費用を負担できる一部の企業と、そうした企業が所在する一部の国はAIの技術革新・サービスについて更に優位な立場に立ち、そうでない国や企業は相対的にその地位を低下させることになる。結果として、AIにまつわる経済格差が世界規模で拡大し、それに伴う社会不安等の問題をもたらすことが懸念される。

(c) 市場における一部企業への集中と単一障害点

上記で指摘した一部の企業によるAI投資の突出は、限られた企業に社会が強く依存するという集中と表裏一体である。2024年第4四半期の時点で、Amazon社、Microsoft社、Google社3社によるクラウドコンピューティング市場の寡占率は3分の2を超えている[※57]。AIを活用するITシステムの構築や運用には大規模なクラウドデータセンターが欠かせないため、クラウド基盤の集中はAI基盤の集中と実質的に同義である。このことに伴う問題として、これらAI基盤及びその上で稼働するAIの故障や動作不良が、全世界に影響を及ぼし得る点が挙げられる。システム全体の安全性が一部の構成要素に左右されるときに、その構成要素を単一障害点[※58]と呼ぶ。特定企業への世界中の利用者からの依存は、そ

れらの企業を社会的な単一障害点にしてしまうおそれがある。

(d)環境へのリスク

データセンターとデータ送受信で消費されるエネルギーは、汎用的 AI 登場前の 2020 年の時点で、世界のエネルギー使用に関連する温室効果ガス排出量の約 0.7%を占めた[※59]。国際エネルギー機関(IEA:International Energy Agency)の推定によれば、2024 年から 2026 年にかけて世界の電力需要は 3.4% の増大が見込まれ、データセンターの急拡大の影響が大きいと指摘されている[※60]。同様に IEA では、2023 年から 2030 年にかけて、データセンターは世界の電力需要の増加の 10% 弱を占める可能性があると予測している[※61]。データセンターにおける電力消費のすべてが AI に由来するわけではないが、例えば Google 社においては、同社のデータセンターの 2023 年の電力消費量が前年と比較して 17% 増加し、同社が購入・使用した電力等による温室効果ガス排出量も 37% 増加した[※62]。同社では AI が全製品に深く結び付いているため AI の環境負荷だけを切り分けることは無意味かもしれないとしているが、近年の積極的なデータセンターへの投資の状況は既に述べたとおりである。同社は必要な電力を賄うために、次世代原子炉の開発企業と契約を締結した[※63]。Microsoft 社も、米国ペンシルベニア州のスリーマイル島原子力発電所を再開する契約を 2024 年に結び、20 年間、同発電所の発電能力をすべて購入することに合意した[※64]。これは約 80 万世帯の消費電力に相当する。日本においても、2025 年 2 月に決定されたエネルギー基本計画において、電力需要が今後増えていくことを念頭に置きつつ、再生可能エネルギーに加え原発の活用がうたわれることとなった[※65]。AI 利用の増大については地球環境への負荷というリスクも無視できなくなりつつある。

(e)プライバシーへのリスク

生成 AI は学習した内容に基づき何らかの応答を返す。学習データにプライバシー情報が含まれる場合には、AI の利用時に応答を通じてプライバシー情報の漏えいが生じる可能性がある[※66]。また、インターネット等に分散しているデータと、他のプライバシー情報を AI によりまとめて処理することで、予期せぬ目的で利用されてしまうことが懸念されている[※67]。進歩した AI の能力によって、膨大なデータの中から、それまでは見つけることが難しかった個人情報を特定したり推論したりできるのではないかとの指摘もある。その一方で、例えばヘルスケア産業[※68]や監視カメラ[※69]への AI 導入を通じて、今まで以上にプライバシー情報が IT システムに引き渡される機会が増している。AI を活用するネットサービス企業においてプライバシー保護が不十分であった事例[※70]や、家庭用防犯カメラのサイバーセキュリティ対策が不十分であった事例[※71]等が報告されている。リスクの度合いは判然としないものの、汎用的 AI の関わりによってプライバシー保護に問題が生じる可能性はあると見られている。

(f)著作権侵害のリスク

生成 AI は学習データに基づき様々な応答を合成するが、結果的に、学習データに含まれる著作物とほとんど変わらない内容を再現したり、あるいは、酷似する表現を用いた応答を合成したりする場合がある。学習データが原著者の許諾を得ていない著作物を含んでいれば、生成 AI による著作権侵害が起こる可能性がある。生成 AI の学習に用いられるデータセットの中に実際に著作者の許諾がないデータを含むものがあるとして、著作権者が権利侵害を訴える事例も既にある。2023 年 2 月に米国 Getty Images Holdings, Inc. は画像生成 AI Stable Diffusion の開発元である英国 Stability AI Ltd を訴え[※72]、同年の暮れには New York Times 紙が Microsoft 社を提訴した[※73]。世界中の Web サイトは学習データの重要な供給源であるが、この流れを受けて、それらの運営元において、AI 学習用途での閲覧やデータ取得を制限する動きもある[※74]。高性能な AI の開発に必要な学習データの量はますます増大しており、著作権侵害へのリスク対応と AI の発展がもたらす利益の間で適切に平衡を保つ議論の重要性が高まっている。

2.1.3 AIセーフティに関する取り組み

2023 年 11 月に、英国の公的機関として AI セーフティ・インスティテュート(AISI:AI Safety Institute)が設立され、日本を含む各国でも AISI あるいは相当する機関を設置する動きが広がった。英国 AISI の設立趣意書では AI セーフティ(AI 安全性)を「AI に由来する危害を理解し、予防し、緩和すること」と定義している[※75]。AI セーフティを具体化するための取り組みは多岐に渡るが、その中でも中心となっているのは、AI ガバナンスの実践である。以下では AI セーフティと AI ガバナンスの基本的な考え方を概観する。

(1) AI セーフティとは何か

冒頭の英国 AISI による定義は一つの例に過ぎず、我が国においては「人間中心の考え方をもとに、AI 活用に伴う社会的リスクを低減させるための安全性・公平性、個人情報の不適正な利用等を防止するためのプライバシー保護、AI システムの脆弱性等や外部からの攻撃等のリスクに対応するためのセキュリティ確保、システムの検証可能性を確保し適切な情報提供を行うための透明性が保たれた状態」を AI セーフティとしている※76。各国の AISI や、AI 開発を手掛ける民間企業におけるとらえ方は、次のように整理できる。

- 狭義の AI セーフティ：AI リスクを抑制する上で個々の AI 及び AI を内包する IT システムが満たすべき性質、及び実際にそれを満たしていること。具体的には、AI 出力のバイアスが十分に小さく公平であること、AI の判定の過程が事後的に精査可能・説明可能であること、サイバー攻撃に対して適切に防御されていること等。
- 広義の AI セーフティ：AI リスクを抑制・制御し、社会に対する害悪を低減するあらゆる取り組み及びその実践を通じて AI リスクが受け入れ可能な水準に抑制されていること。後述する AI ガバナンスの浸透、高いリスクを伴う用途への AI の導入に対する規制、AI リスクに対抗するための防御における AI 利用の推進等。

狭義の AI セーフティは主に技術的対策で担保されるのに対し、広義の AI セーフティはマネジメントやガバナンスといった社会的対策で担保される。技術的対策には、AI の動作を混乱させる入力を学習段階で取り入れて耐性を付ける敵対的学習※77 の実施や、学習データの品質の十分な精査、AI の応答を別の AI で監視すること等が含まれる。本項では技術的な議論には立ち入らず、後者の社会的対策に焦点を当てる。

(2) AI ガバナンスの概要

AI の利用にあたってはリスクベースアプローチが国際的に広く共有されている。AI の利用におけるリスクベースアプローチとは、「予め事前に当該利用分野における利用形態に伴って生じうるリスクの大きさ（危害の大きさ及びその蓋然性）を把握したうえで、その対策の程度をリスクの大きさに対応させる」方法を指す※7。言い換えれば、リスクマネジメントの一種として AI の利用を管理することにほかならない※78。リスクマネジメントを大きな柱として AI 利用を進める取り組みは「AI ガバナンス」と呼ばれている。以下では組織的なプロセスである AI ガバナンスと、AI ガバナンスの基礎となる AI セーフティ評価について概説する。

(a) AI ガバナンス

前述のとおり、AI ガバナンスの大きな柱は AI 利活用を対象領域としたリスクマネジメントである。リスクマネジメントとは次の四つのステップの反復を中核的プロセスとする PDCA 型のマネジメント手法であり、リスクを抑制しつつメリットを最大化することを目的とする※79。

- リスク特定：組織の目的達成に影響し得るリスク事象を洗い出す。マネジメントの対象範囲内で生じる可能性のある事件や事故を書き出すことに相当する。
- リスク分析：個々のリスク事象について、その発生や進展のメカニズム、発生の見込み・改善性、影響の度合い・詳細（インパクト）等を明らかにする。
- リスク評価：リスク分析の結果に基づき、現在のリスク水準が受け入れ可能なものかどうかを判断する。
- リスク対応：受け入れ不可能な水準のリスクに対し、事件・事故の予防策や影響の低減策等の対策を講じる。

AI ガバナンスのプロセスには、AI 利活用に関連したリスクの把握が欠かせない。リスク特定・分析・評価にわたる 3 ステップをまとめてリスクアセスメントとも呼ぶ。リスクアセスメントは、AI 利活用に伴うリスクを認識し、対応を決定するための準備作業にあたる。

代表的なリスクアセスメント手法の多くは IEC/ISO 31010※80 で紹介されているが、AI システムの利用を念頭に置いたリスクアセスメント手法には定番と言えるものがまだ存在しない。AI システムを対象とした数少ないリスクアセスメントの手引きとしては、一般社団法人日本品質管理学会がまとめた「AI リスクアセスメントガイドブック※81」がある。現状では、リスクアセスメント手法として実績のあるものを用いつつ、AI に特有の事情を勘案しながら、各自で工夫して取り組みを進めていくケースが多いと考えられる。

AI ガバナンスの全体像を整理した手引きとしては、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）のまとめた「AI Risk Management Framework※82」（以下、AI RMF）が著名である。AI RMF は多様な AI 全般を対象としているが、生成 AI に特化した注意事項をまとめた追加文書「生成 AI プロファイル※83」もよく知られる。AI RMF に相当する日本の手引きとしては、経済産業省・総務省によ

る「AI 事業者ガイドライン※84」がある。EU で AI 利用を規制する法律として制定された「AI Act」も、AI ガバナンスの手引きとしての側面を持つ。なお、日本 AISI と米国 NIST は、AI 事業者ガイドラインと AI RMF の比較を行い、相互運用性を確認するクロスウォーク活動※85を 2024 年度に実施している。

(b) AI セーフティ評価

AI を内包する IT システムを「AI システム」と呼び、AI システムの心臓部にあたる AI は「AI モデル※86」と呼ぶことが多い。AI モデル単体がソフトウェア部品として提供されることも多いため、両者の区別は重要である。

AI モデルと AI システムの区別は AI セーフティの観点でも重要である。狭義の AI セーフティにおいて満たされるべき性質は、それが AI モデルにおいて満たされるべきなのか、AI システムにおいて満たされるべきなのかという観点の違いにより、検証方法や安全性確保の方法が異なってくる。

AI システムが AI セーフティの観点で適切であるかどうか見定めることを「AI セーフティ評価」という。AI セーフティ評価は基本的には狭義の AI セーフティに関する評価であり、AI システムとその内部の AI モデルが評価対象となる。AI セーフティ評価の切り口を整理した資料としては、日本 AISI がまとめた「AI セーフティに関する評価観点ガイド※87」がある。

「2.1.1 AI の急速な発展」で述べたように、AI の実装技術には複数のアプローチがあり、評価手法はそれぞれに異なる。昨今注目を集めているのは汎用的 AI として提供されることも多い LLM（Large Language Model：大規模言語モデル）※88であるが、LLM を対象としたセーフティ評価の基本は、一般的には機械的なベンチマークテストの実施である※89。具体的には、用意した膨大な量の問題を解かせ、正答率を調べるというものである。クイズの回答により、民族や人種に対する差別的なバイアスの有無や、マルウェア作成依頼を拒否するといった安全対策が機能しているかどうかの確認を行うものであり、自動的に実行できる特徴と相まって、ベンチマークテストは AI セーフティ評価の主流となっている。

ベンチマークテストは主に AI モデルの評価手法であって、AI システム全体の評価とは異なる。例えば、内包する AI モデルには問題がないが、AI システム内で動くデータベース部分にサイバー攻撃に対する脆弱性がある場合、AI モデルのセーフティ評価だけではこれを見落とすことになる※90。また、大半のベンチマークテストは一問一答形式であり、複数回の応答を経た後に AI の動作がおかしくなるようなケースの特定にも適さない。

AI セーフティ評価の焦点を AI モデルから AI システムや利用者等に広げ、実利用に近い状況下でのテストを攻撃者の目線で個別に組み上げて実施する手法は、「レッドチーミングテスト」と呼ばれる。この呼び名は、サイバーセキュリティ分野で行われるサイバー攻撃模擬演習において攻撃側をレッドチーム、防御側をブルーチームと呼ぶ慣習にならったものである。レッドチームは AI システムや利用業務、サイバーセキュリティ等のエキスパートで編成し、それらエキスパートの専門的知見を活用することで、状況に則した高度な攻撃シナリオを組み立てる。そのシナリオに沿って模擬的に AI システムのセーフティが損なわれる攻撃を行い、リスク要因や改善点を洗い出す。レッドチーミング※91 テストの進め方については、日本 AISI のまとめた「AI セーフティに関するレッドチーミング手法ガイド※92」が詳細な手引きとなっている。

AI セーフティ評価を通じて問題が見つかった場合には、何らかの対処を施すことになる。技術的な対処については、NIST や日本の AI プロダクト品質保証コンソーシアム、国立研究開発法人産業技術総合研究所が、AI モデルへの攻撃と防御の手法を文書にまとめている※93。加えて、AI の動作を大きく左右する学習データの品質確保の手引きとして、日本 AISI から「データ品質マネジメントガイドブック※94」が公開されている。

現行の AI セーフティ評価の手法は万全ではなく、今知られている手法の範囲で問題が見つからなかったとしても、未知のリスクが残る可能性がある。また、汎用的 AI の動作が解明されていないことや、応答が状況に依存することに加え、AI セーフティの評価観点を決定する際に、多様なステークホルダーが関与できておらず、観点の洗い出しが行き届いていないという批判もある※95。多様なステークホルダーをどのように参加させるかというプロセスにも定まった議論はまだない。AI の技術が毎月のように進歩し続けていることも念頭に置き、今後の AI セーフティ評価手法の進展を注視しつつ、今できることを疎かにしない姿勢が重要と言える。

(3) AI セーフティに関する国際連携

汎用的 AI は、大手ベンダーによりクラウドサービスの一種として提供されることが多い。AI サービスは国境を越え、一つのサービスに複数の国のルールや事情が関わってくる。このため、AI セーフティに関しても国際的な連携や協調が望まれ、各国の AISI も深く関わる形で取

り組みが進みつつある。以下では AISI を含む国際会議である AI セーフティサミットについて述べる。

(a) AI セーフティ・インスティテュート

前述のとおり、2023 年 11 月に英国において設立された、AI セーフティを担う公的機関が AI Safety Institute（AISI）[※96] である。発足当時、英国 AISI は以下の任務にあたるものとされた[※75]。

- 先進的な AI システムに関する評価手法の開発・実施：AI セーフティに関連する AI の能力の特徴付け、システムのセーフティとセキュリティの理解、社会的影響の評価を目指す。
- AI セーフティに関する基礎研究の推進：様々な探索的研究プロジェクトを立ち上げ、外部の研究者を招集する。
- 情報交換の促進：任意参加と既存のプライバシー及びデータ規制遵守を前提として、政策立案者、国際パートナー、民間企業、学術界、市民社会等との明確な情報共有チャネルを確立する。

上記の内容からは、科学的な裏付けを重視しつつ AI セーフティ評価を基盤として内外の連携を図るという全体像が見える。英国 AISI は、AI モデルのセーフティ評価ツールである Inspect[※97] の開発・公開、Inspect を用いた AI セーフティ評価の結果報告[※98] 等、技術的な道具の整備と知見の展開に取り組んでいる。

他方で、AI セーフティへの関心を持つのは AISI だけではなく、考え方も一つではない。EU の「AI Act」は人命への危害や人権侵害につながる特定用途の AI 導入を禁止し、また、ハイリスク AI システムという区分による規制強化等、リスクベースアプローチの徹底を求めている。人権侵害を問題視する点は、2021 年に UNESCO（United Nations Educational, Scientific and Cultural Organization：国際連合教育科学文化機関）で採択された「Recommendation on the Ethics of Artificial Intelligence（人工知能の倫理に関する勧告）[※99]」、2023 年に発表された米国「AI 権利章典[※100]」も同様である。また Biden 政権下で 2023 年 10 月にまとめられた大統領令 EO 14110[※101] は、サイバー攻撃や CBRN 兵器開発支援への悪用等の国家安全保障上のリスク対応に言及している。加えて、国際連合（United Nations 以下、国連）がまとめた提言[※102] においては、AI の利用が先進国に集中することに伴うグローバル格差の拡大を懸念してもいる。英国 AISI が示した、技術的な観点を主とする AI セーフティ評価がこれらの基礎になることは確かであるが、議論の裾野は幅広く、AI セーフティ確保のために必要な取り組みも現時点で定まったものはない。

英国に続き、各国において AISI またはそれに相当する公的機関を設立する動きが見られる。米国は英国とほぼ同時に、NIST 内に AISI を設立した[※103]。2024 年 2 月には日本 AISI が設置された[※104]。その他、シンガポール[※105]、カナダ[※106]、韓国[※107] 等が AISI を設けている。フランスは AISI に相当する機関として INESIA（Institut national pour l'évaluation et la sécurité de l'intelligence artificielle）を 2025 年 2 月に設置した[※108]。EU には「AI Act」に関連する実務機関として European AI Office[※109] が設置され、各国の AISI のカウンターパートとして活動している。

これら AISI の動きに対しては大手 AI ベンダーらも協調姿勢を示している。米国では、AI 関係の民間企業等を集めた AISI コンソーシアムを招集し、大手 AI ベンダーを含む 200 以上の関係組織が参加している[※110]。米国政府は自発的コミットメント[※111] という形で AI ベンダーらの協力姿勢を取り付けている。各国の AISI を含む国際会議である AI セーフティサミットにはこれらの企業も参加し、歩調を合わせている（「2.1.3 (3) (b) AI セーフティサミット」参照）。

AI セーフティに関するこれら公的機関及び AI ベンダーらが国際的な交流・連携を深め、世界で調和の取れた AI セーフティの取り組みが進展することが期待される。

(b) AI セーフティサミット

英国 AISI の設立は、2023 年 11 月初頭に英国 Bletchley Park で開催された AI セーフティサミット（AI Safety Summit）[※112] にて発表された。当時の Rishi Sunak 政権の主導によるこの国際会議には、米国、イタリアをはじめとした G7、EU 等が参加したほか、OpenAI 社 CEO、DeepMind 社共同創立者、米国の Elon Musk 氏等、AI 産業における世界的なキーパーソンも集まった。同 AI セーフティサミットでは締めくくりに、AI リスクに対応するための国際連携を呼びかける「ブレッチリー宣言[※113]」を参加 28 ヵ国と EU が採択した。

AI セーフティサミットはおおむね半年ごとに開催する予定となっており、2024 年 5 月下旬には第 2 回にあたる AI ソウル・サミット[※114] が韓国にて開催された。初回同様に G7 に EU、韓国、オーストラリアを加えて採択されたソウル宣言[※115] では、① 2023 年の広島 AI プロセス

の流れを汲む形で国際的に相互運用可能な AI ガバナンスの枠組みを整備すること、② AISI 及びそれに相当する機関の各国における設立を支援すること、③多種多様な利害関係者を包括していくこと等がうたわれた。更に、民間企業が誓約主体となる「フロンティア AI のセーフティに関するコミットメント※116」も採択され、OpenAI 社や Google 社のような AI 分野を率いる IT 企業自身がソウル宣言の趣旨に賛同し、積極的に AI セーフティ及び AI ガバナンスに取り組むことが示された。広島 AI プロセスから AI ソウル・サミットに至る討議の中で浮上した AI セーフティに関する論点については、日本 AISI が「AI セーフティに関する活動マップ（AMAIS）※117」として整理している。

(c) 2025 年冒頭の国際動向

2024 年 11 月、米国大統領選挙において当時の現職副大統領であった民主党の Kamala Devi Harris 候補を破り、共和党の Donald Trump 大統領が誕生した。共和党は同時実施となった上下院選挙のマニフェスト※118 において、AI のイノベーションを阻害するものであるとして、Biden 政権下でまとめられた EO 14110 を廃止することを確約しており、実際に 2025 年 1 月に同大統領令は廃止となった※119。これに代わるものとして「AI における米国のリーダーシップへの障壁を除く」大統領令 EO 14179※120 が署名されたが、詳細な行動計画は 180 日以内に決定するとしており、米国の AI 政策の動向には今後大きな変化が生じるものと見られる。

政権交代に伴う AI 政策の変化の兆候は英国にも見られる。2024 年 7 月の英国総選挙で保守党は敗北し、党首である Sunak 首相に代わって労働党の Keir Starmer 首相が誕生した。2025 年 1 月には Starmer 政権における AI 政策にあたる「AI 機会行動計画※121」が発表され、社会における AI 利活用を積極的に推進することがうたわれた。更に、2025 年 2 月に、英国 AISI は AI Safety Institute から AI Security Institute へと改称し、国家安全保障や犯罪に関連する AI セキュリティに取り組むことが発表された※122。AI セーフティの分野では重要視されるバイアスや言論の自由といったテーマについては、今後の取り組みの対象外になるとしている。プレスリリースにおいては、国家安全保障はもとより重要なテーマであり、英国 AISI の活動が変化するものではなく明確化するに過ぎないとしつつも、英国のサイバーセキュリティ当局である NCSC（National Cyber Security Centre）や治安当局である内務省（Home Office）との連携強化が盛り込まれる等、重点課題の絞り込みはあったものと見られる※123。

AI ソウル・サミットに続く第 3 回の AI アクションサミット※124 は 2025 年 2 月にパリにて開催された。名前が変化したことからも察せられるように、サミット全体としては、AI の利活用に力点を置きつつ、100 ヵ国超から 1,000 名以上が参加した。国連の António Guterres 事務総長やインドの Narendra Modi 首相も参加する等、AI に関する国際政治の舞台にもなったと言える。他方で、同サミットでは「人類と地球にとって包摂的で持続的な AI※125」と題する共同宣言に対し、世界の AI リーダー国であるはずの英国と米国は署名しなかった。英国政府は国家安全保障とグローバル・ガバナンスに関する懸念から署名できなかったとし、サミットに出席した米国の James David Vance 副大統領は、成長を促進する AI 政策がセーフティよりも優先されるべきだと述べた※126。

これらの動きが AI セーフティに関する取り組みの変化であり、それが他国にも波及するのかはまだ定かでない。その中でもある程度、議論の収れんが見られるのは、AI リスクの議論における、想定リスクとその大まかな特徴の整理である。これを示す成果物が、過去 3 回の AI サミットで公開された、独立した学術調査グループによる 3 編の報告書※127 である。これらの報告書は汎用的 AI を念頭に置き、最先端の AI の能力、学術的な解明状況、AI リスクの現状を整理している。「2.1.2 (1) AI の悪用がもたらすリスク」では、2025 年版の同報告書で取り上げられている AI リスクを紹介した。一方、整理された AI リスクがどのような規模・メカニズム・影響・確度で実現するかは依然として不透明であり、警戒を怠ることはできないと言える。

2.1.4 AIセキュリティの現状

AI セキュリティという言葉には、未だ明確な定義がないのが現状である。しかし、AI の開発や利活用において、サイバーセキュリティに関わる多くの懸念や課題があることは明らかである。以下では、AI が関わるサイバーセキュリティの動向を論じる。

(1) AI セキュリティとは何か

英国 AISI は当初の設立趣意書の中で AI セキュリティを定義し、AI モデルや AI システムを悪意ある攻撃者による攻撃から保護すること、としている※75。AI システムのサイバーセキュリティについては同様の考え方が「AI

Act」の中で説明されており、AIシステムのサイバーセキュリティ対策は、広く受け入れられている狭義のAIセキュリティであると言える。

上記に言うAIセキュリティには、AIの悪用で社会に生じるサイバーセキュリティリスクが含まれない。しかし、既に事例があるように、サイバー攻撃の手間を汎用的AIによって軽減し、攻撃者が優位性を高めることができる。ChatGPTの登場直後からフィッシングメールの劇的な増大も確認されており[※128]、サイバー犯罪の増加の背後に汎用的AIが関わっていることも推認される。悪用目的で安全対策をあらかじめ排除したAIをサイバー犯罪者らが独自に開発することも技術力があれば可能である[※129]。

AIガバナンスは、AIシステムを守ろうとする人々にとって有益であるが、悪意あるアクターがAIを悪用することは防げない[※130]。AIシステムをサイバー攻撃から守るという狭義のAIセキュリティでは網羅されない課題があると言える。Biden政権（当時）で導入されたEO 14110のセクション4ではまさにAIの悪用に対する対策に焦点が当てられ、AI開発に用いられるクラウド環境の利用状況監視や、脆弱性の特定と緩和にAIを活用する取り組みが盛り込まれていた。

本項では、AIシステムのサイバー保護を狭義のAIセキュリティとし、サイバー空間におけるAIの悪用がもたらすリスクから社会を保護する取り組みも加えたものを広義のAIセキュリティとする。

(2) AIセキュリティ脅威の動向

サイバーセキュリティリスクの発現の起点となり得る出来事や状況を「サイバー脅威[※131]」と呼ぶ。本項ではAIセキュリティにまつわるサイバー脅威を「AIセキュリティ脅威」とし、これを大きく三つに分類し、その全体傾向を以下にまとめる。なお、以下のまとめは、ENISA（European Network and Information Security Agency）の年次報告書[※132]や、AIセキュリティに関連する調査を活発に実施している英国Alan Turing Instituteの調査結果[※133]を総合したものである。

(a) AIシステムへのサイバー攻撃

大手ITベンダーAIチャットサービスに脆弱性が発見されたとする事例[※134]はあるが、社会に大きく被害を及ぼす大規模なサイバー攻撃事例は2025年3月末時点ではない。しかし、AIモデルの実行や学習基盤として広く利用されるPyTorchというライブラリにサプライチェーン攻撃を可能にする脆弱性が見つかった事例[※135]や、様々なオープンソースAIモデルの共有サイトHugging Faceに侵入可能な脆弱性が見つかった事例[※136]、中国発の高性能AIとして話題を呼んだDeepSeekのセキュリティに問題があり、背後のデータベースに侵入できることが判明した事例[※137]等がある。これらの事例は、AIシステムへのサイバー攻撃の被害は顕在化していないが机上の空論ではなく、AIに特化した攻撃手法よりも従来のサイバー攻撃手法に対して防御が不十分であるという現状を示している。

(b) AIを悪用したサイバー攻撃

ChatGPTをサイバー攻撃のアシスタントとして悪用した事例について、OpenAI社とMicrosoft社は2024年2月に詳細な調査報告[※27]を公開した。悪用に関わったアクターの数は300を超え、そのうちの160は国家支援型アクターで、50はランサムウェア攻撃を行うグループであったとされる。これらのアクターは、攻撃対象に関する下調べや、攻撃工程を効率化するプログラムの実装、侵入経路になる脆弱性に関する技術情報の収集等にChatGPTを活用した。ChatGPTは言わばプログラマーとしてのサイバー攻撃者の日常業務を効率化した。AIによるサイバー攻撃の効率化は、低スキルの人員にも攻撃能力を与えてしまうという点で、サイバー犯罪市場への参入障壁を引き下げていることが懸念されている[※28]。

The MITRE Corporation（以下、MITRE）はAIによるサイバー攻撃の自動化能力を測定するベンチマークテストを開発し、状況の継続的な観測に取り組んでいる。MITREの評価[※26]によれば、現時点では、汎用的AIの能力はサイバー攻撃を全面自動化するには不足している。他方で、サイバー防御の自動化については一部限定的な用途における実証試験が始まるという。サイバー攻撃も含め、技術の進展次第で状況が急激に変化する可能性がある。

(c) AIを用いた認知領域への攻撃

サイバー犯罪の領域では汎用的AIの悪用と見られる状況が広く確認されている。ChatGPTの登場以後、フィッシングメールは爆発的な増大を示した[※138]。ディープフェイク画像・音声等を用いた詐欺の事例も複数確認されており、ある会社でCFO（最高財務責任者）になりすまして約40億円を不正送金させ詐取した標的型ソーシャルエンジニアリングとも言うべき事例[※139]がある。更に新たな悪用例として、チャット越しにLLMが詐欺師として

振る舞った国内の事例※140 等が報道されている。

選挙を攪乱させる影響工作が世界中で見られたことは既に「2.1.2 (1) (b) 世論操作」で述べたとおりである。影響工作の背後には国家支援型アクターがいると見られており、中国、ロシア、イラン、イスラエル等が調査報告書※25 において支援国とされている。影響工作の手段としては AI が生成したテキスト、ディープフェイク画像・動画等が用いられ、SNS がフェイク情報の拡散手段になることが多い。現状では SNS 上でのフェイク情報の拡散が進まず、大きな影響を及ぼすには至っていないと評価されている。この原因は明確になっていないが、攻撃側の展開した情報に不備がありフェイクとすぐに分かるようなものになっているといった稚拙さがあったほか、SNS 上で生身の人間が展開するコンテンツとの競合に打ち勝つ必要がある中で、関心の獲得に失敗したという構図が指摘されている。

影響工作の今後を示唆する事例としては、2024 年 11 月に実施されたルーマニア大統領選挙がある。同選挙では、親ロシア極右で無名の Călin Georgescu 候補が第一回投票で首位となったが、未申告の選挙運動資金の提供や影響工作があったとして、憲法裁判所により選挙は無効であるとされた※141。ルーマニアの諜報機関から公開された機密文書※142 によれば、ロシアによる影響工作が続いており、AI も駆使されてきたと指摘されている。ただし、この選挙における影響工作では動画投稿・共有サービス TikTok 上での世論形成が大きな役割を果たしており※143、この種の SNS において広範な影響力を持ついわゆるインフルエンサーの買収も行われている※144。影響工作の中で AI の果たした役割が選挙をどの程度左右したのかは不明だが、影響工作が複数の手段を複合して展開され、全体として一国の民主主義を操作する直前にまで至った現実の事例であると言える（事例の詳細については「2.2.3 (2) (d) ルーマニア大統領選挙」参照）。

(3) AI セキュリティリスクに関する予測

英国 NCSC は 2024 年 1 月に「サイバー脅威に対する AI の短期的影響」と題する報告を公開した※28。要点は次のとおりである。

- AI の影響でほぼ確実に今後 2 年間でサイバー攻撃の量が増加し被害内容も悪化する。
- 国家、非国家、熟練者、そうでない者、あらゆるタイプのアクターが、程度の差こそあれ、既に AI を利用している。
- 偵察とソーシャルエンジニアリングにおいて、AI は両者をより効果的、効率的、かつ発見されにくいものにしている。
- AI は、サイバー犯罪初心者、雇われハッカー、ハクティビストが効果的なアクセスや情報収集活動を行う際の障壁を引き下げる。結果として、今後 2 年間のランサムウェア脅威は助長される可能性が高い。
- 2025 年までに限れば、新しいサイバー脅威が生まれるのではなく、従来のサイバー脅威が悪化する。
- サイバー作戦における AI のより高度な利用は、高度な能力とリソースを有する一部の脅威アクターに限定される可能性が高く、かつ、2025 年までに実現する可能性は低い。
- 2025 年以降、サイバー犯罪市場や犯罪ビジネスにおいて AI を活用した能力が一般化し、より高度な能力が利用可能になることはほぼ間違いない。

その他、Alan Turing Institute 配下の CETaS（Centre for Emerging Technology and Security）が 2024 年 7 月に公表した「悪用時の生成 AI の能力評価※145」では、マルウェア作成の自動化、影響工作による世論の先鋭化、テロにおける兵器開発支援と計画立案という 3 領域について評価を行い、報告時点では危険性は限定的であるとしている。その一方で、AI の進歩がこれらの脅威に及ぼす影響について、技術的及び社会技術的な変曲点を見極めることが重要であるとしている。急激な AI の発展がより一層高速化するようなことがあれば、対策が手遅れにならないようその機をとらえるべきとの趣旨である。

(4) AI セキュリティの具体的な対策

AI システムをサイバー攻撃から保護するという狭義の AI セキュリティは AI セーフティに包括される。このため、NIST の AI RMF や我が国の「AI 事業者ガイドライン」に沿った AI ガバナンスの推進を枠組みとして、その中でレッドチーミングテストを含む AI セーフティ評価を行い、適宜対策を講じることが基本となる。加えて、セキュアシステム開発のガイドラインである NIST の「Secure Software Development Framework（SSDF）※146」には生成 AI 利用を想定した追加文書※147 があるほか、英国 NCSC が中心となって発行された「機械学習の原則※148」、更に英国、米国、カナダ、オーストラリア、ニュージーランドのサイバーセキュリティ当局が共同でまとめた「AI システムのセキュア配備※149」、そして「2.1.3 (2) (b)

AI セーフティ評価」で取り上げた手引き類がある。AI モデルの学習工程で考慮すべき対策を除けば、内容の大部分は、一般的なサイバーセキュリティ対策の強度を高めたものとなっている。

狭義の AI セキュリティの確立にあたっては、AI ガバナンスとセキュリティガバナンスの関係をどう整理するかという問題がある。AI ガバナンスの観点からは AI セーフティの一部に狭義の AI セキュリティが含まれる一方で、IT システムの一種でもある AI システムの保護はサイバーセキュリティ上の取り組みでもある。このため、AI システムの保護の主たる責任が AI ガバナンスとセキュリティガバナンスのどちらに置かれるのかという点に何らかの整理を行う必要がある。しかし、それぞれの分野で個別のガイドラインの整備等が進む一方で、両者の統合に関する議論が未成熟であることが指摘されている※150。

AI の悪用を視野に入れた広義の AI セキュリティの対策については、本節の執筆時点では標準的と言えるものがない。AI の開発に必要な基礎的情報や学習データの多くは公開されているため、悪用目的での AI モデル・AI システム開発を防ぐ方法は根本的にない。この点では、AI をセキュリティ強化の目的で積極活用する AI for Security の考え方が有望であると期待される。加えて、狭義の AI セキュリティ対策を徹底することが、通常の目的で利用される AI システムの乗っ取りと犯罪等への転用を防ぐという意味でも不可欠と言える。全体として広義の AI セキュリティの議論は煮詰まっておらず、今後の推移を注視していく必要がある。

COLUMN

サイバーセキュリティとデジタルトランスフォーメーション ～WISDOM-DXと生成AIによる「情報セキュリティ白書」の分析～

福岡伸一氏は、著書「世界は分けてもわからない[i]」の中で、鼻の移植手術のために鼻を取り出すとしたらどこまで深くえぐりとればよいかという思考実験を紹介しています。鼻と呼ばれる突起物だけでなく、鼻の奥の嗅上皮、嗅上皮のレセプターと神経線維、脳の嗅球、神経細胞群、連動する筋肉や骨や関節の仕組みというように嗅覚という機能を切り出すためには、結局、身体全体を取り出すしかない。「部分とは部分という名の幻想である」と述べています。同じように、セキュリティをデジタルトランスフォーメーション（DX）の「部分」として切り出すのも幻想でしょう。

例えば、医療 DX を例に挙げると、システムとして、給食等の供給系、電子カルテ等の基幹系、放射線等の医療機器系、診療予約等の患者サービス系が連携しており、利用者は、供給事業者、医療従事者、病院利用者、それぞれのシステムの保守要員等と多岐にわたります。そこでは利用者によるミスや不正、外部からの攻撃といった様々なインシデントが報告され、一部門のインシデントがシステム全体に影響を及ぼす結果となっています。医療以外の多くの分野においても同様です。そのため、安全管理ガイドラインの策定やサイバーセキュリティ対策の注意喚起、最高情報セキュリティ責任者（CISO）等の任命、ならびに緊急対応体制（CSIRT 等）の整備が進められていますが、担当部門や専門家に任せておけばよいというものではありません。利用者すべてが IT やサイバーセキュリティの基本知識を学ぶ必要があります。例えば、標的型攻撃の手口を知らない利用者が電子メールを利用することは大きなリスクです。

基本的な IT 知識を身につける手段として国家試験[ii]「IT パスポート試験」が注目されています。2024 年度、事務職・営業職等幅広い職種の社会人や学生から 30 万人以上の応募がありました。サイバーセキュリティの基本知識の習得には「情報セキュリティマネジメント試験」も有効です。業務で個人情報を扱う担当者、業務部門・管理部門の情報管理担当者、外部委託先に対する情報セキュリティ評価・確認を行う担当者すべてが、知っておくべき内容です。CISO には、「情報処理安全確保支援士」（登録セキスペ）の資格が望ましいです。少なくとも、登録セキスペの助言を理解し実践できる能力は必須です。DX 推進のためには、各人が業務に関連するセキュリティ対策を実践する能力、いわゆる「プラス・セキュリティ」が求められています。

経済産業省は、DX の促進を図るために、DX を推進する仕組みを社内に構築し、優れたデジタル活用の実績が表れている企業を銘柄や注目企業として選定しています[iii]。2015 年から 2024 年までに DX 銘柄、DX 注目企業、攻めの IT 経営銘柄、IT 経営注目企業等 453 社を「DX 優良企業」として選定しました。また IPA と NICT は、Web 情報を用いて企業の DX 活動を自動評価する「WISDOM-DX[iv]」を開発しています。今回、WISDOM-DX を用いて東京証券取引所の上場企業 1,984 社の DX 活動内容を抽出してベクトル化し、更に「情報セキュリティ白書 2024[v]」の各節の記載内容を生成 AI によってベクトル化しました。これらのベクトル間の距離を算出することによって、白書に記載された事項と各企業の DX 活動の内容の関連性を可視化することができます。横軸を東証上場企業 1,984 社、

縦軸を「情報セキュリティ白書 2024」の「1.1 2023 年度に観測されたインシデント状況」から「4.2 AI のセキュリティ」の各節として図 1 のような関連性ヒートマップを作成しました。

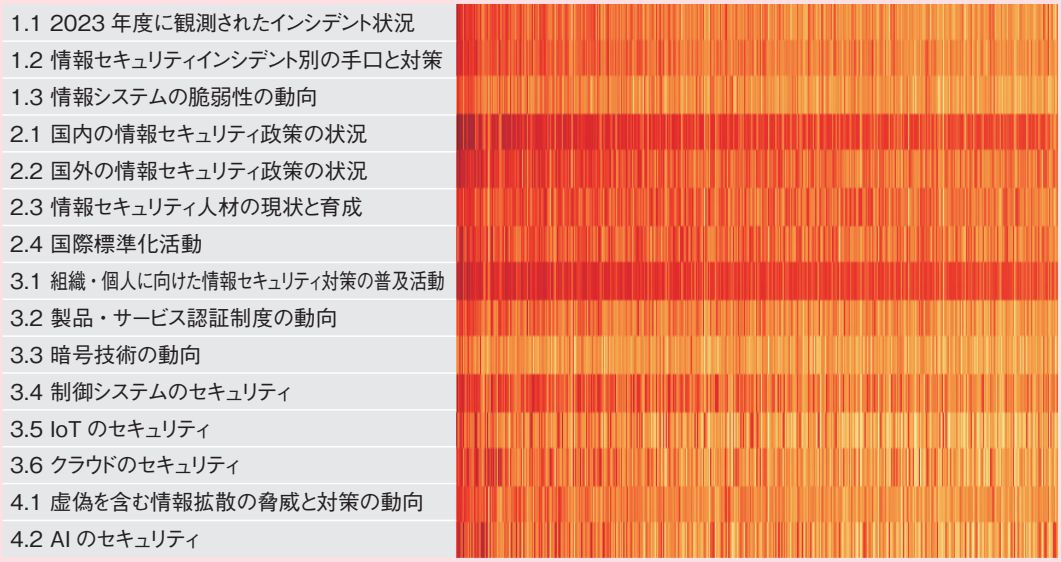


図 1　「情報セキュリティ白書 2024」の内容と企業の DX 活動との関連性

濃い色は、関連性が高いこと、つまり各企業が DX 活動として「情報セキュリティ白書 2024」の記載内容に関連する活動を行っていることを示します[vi]。多くの企業が、「2.1 国内の情報セキュリティ政策の状況」と「3.1 組織・個人に向けた情報セキュリティ対策の普及活動」に記載された内容に関連性のある活動を行っていることが分かります。次に、東証上場企業 1,984 社を「情報セキュリティ白書 2024」の内容と関連性の高い順に左から並べ、DX 優良企業 453 社を縦線としてプロットした分布図を図 2 に示します。

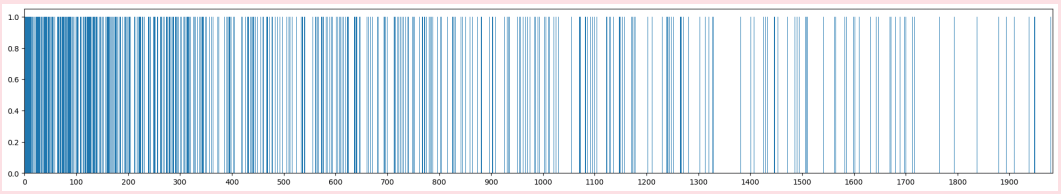


図 2　東証上場企業における DX 優良企業の分布

DX 優良企業の多くが左側に分布している、つまり、DX 優良企業は、「情報セキュリティ白書 2024」の記載内容に関連性の高い活動を行っていることが分かります。DX 優良企業の半数以上が、「情報セキュリティ白書」との関連性上位 20% に含まれています。この「情報セキュリティ白書 2025」も、企業の DX 活動を推進するために積極的にご活用いただければ幸いです。

i　福岡伸一「世界は分けてもわからない」講談社、2009 年
ii　IPA：試験区分一覧　https://www.ipa.go.jp/shiken/kubun/list.html〔2025/7/18 確認〕
iii　経済産業省：デジタルトランスフォーメーション銘柄（DX 銘柄）　https://www.meti.go.jp/policy/it_policy/investment/keiei_meigara/dx_meigara.html〔2025/7/18 確認〕
iv　IPA：WEB データに基づく企業の DX 活動の自動分析・評価システム「WISDOM-DX」を開発　https://www.ipa.go.jp/digital/dx/wisdom-dx/wisdom-dx.html〔2025/7/18 確認〕
奥村明俊、市瀬規善、久寿居大、石川開、鳥澤健太郎、大竹清敬：Web データに基づく企業のデジタルトランスフォーメーション活動評価システム WISDOM-DX の検証　https://proceedings-of-deim.github.io/DEIM2023/4b-8-2.pdf〔2025/7/18 確認〕
v　https://www.ipa.go.jp/publish/wp-security/2024.html〔2025/7/18 確認〕
vi　薄い色は「情報セキュリティ白書 2024」に記載の内容に関連する DX 活動が WEB データから読み取れないことを意味する。

2.2 偽・誤情報の脅威の動向

本節では、虚偽を含んだ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。

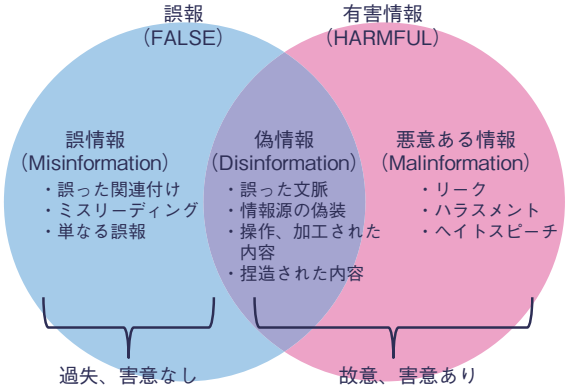
国家が関与するサイバー攻撃は、その手法等から分類すると表 2-2-1 のように整理できる。近年の情報戦・認知戦においては、虚偽を含んだ情報を流布する「情報操作型サイバー攻撃」と、それを含む様々な類型のサイバー攻撃を組み合わせた「ハイブリッド型サイバー攻撃」が大きな脅威となっている。本節では、表 2-2-1 の攻撃類型を使用して以降の解説を行う。なお、誤情報（ミスインフォメーション）と偽情報（ディスインフォメーション）を組み合わせた政府の用法※151 に従い、合わせて「偽・誤情報」と表記する。

2.2.1 虚偽情報の定義

虚偽を含んだ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 2-2-1）。

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（Misinformation、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（Disinformation、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（Malinformation、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



■図 2-2-1　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※153」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)

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

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）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 2-2-1　国家が関与するサイバー攻撃の類型と主な実行主体
（出典）大澤淳「サイバー領域の安全保障政策の方向性※152」を基に IPA が加筆・編集

定的かつ共通した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。日本国内の 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※154。また、欧州対外行動庁（EEAS：European External Action Service）の 2023 年のレポート※155 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、公共に損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。公共の損害とは、「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、その目的の一つとして経済的利益に言及するとともに、その意図として公共への害意を明示している。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はなく、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。

2.2.2 偽・誤情報の情勢

本項においては、偽・誤情報をめぐる世界的な情勢を概観し、2024 年度以前の調査等も踏まえつつ、近年の全体動向を解説する。

(1) 偽・誤情報の現在

偽情報（ディスインフォメーション）及び誤情報（ミスインフォメーション）の問題は、2024 年度も引き続き世界的な懸念事項として認識されている。

世界経済フォーラム（WEF：World Economic Forum）が毎年発表しているグローバルリスク報告書の 2024 年版では、偽・誤情報は「今後 2 年間で世界に最も大きなリスクをもたらし得る要因」として、異常気象や武力紛争といったその他の脅威を抑えてトップに記載された（表 2-2-2）。

2024 年に国政選挙が行われる 16 ヵ国を調査対象とした UNESCO による 2023 年の調査※157 では、85% の回答者が「オンライン上の偽情報の影響を懸念している」と答えた。また、87% が「既に偽情報が自国の政治に大きな影響を与えている」と回答しており、偽情報（ディスインフォメーション）はグローバルな民主主義の根幹に対する脅威として浮上している。

順位	グローバルリスク	分類
1	誤報と偽情報	テクノロジー
2	異常気象	環境
3	社会の二極化	社会
4	サイバー犯罪やサイバーセキュリティ対策の低下	テクノロジー
5	国家間武力紛争	地政学
6	不平等または経済的機会の欠如	社会
7	インフレーション	経済
8	非自発的移住	社会
9	景気後退（不況、停滞）	経済
10	汚染（大気、土壌、水）	環境

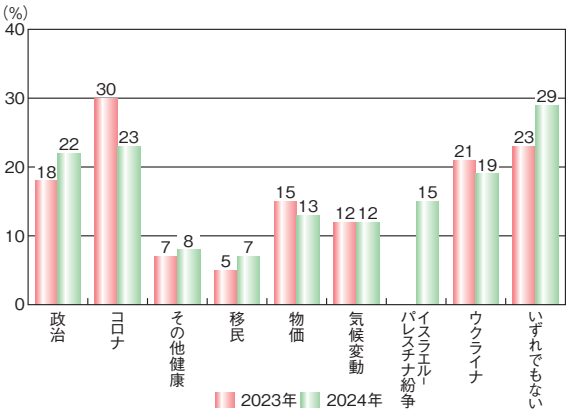
■表 2-2-2　今後 2 年間に想定されるグローバルリスク
（出典）WEF「第 19 回グローバルリスク報告書　2024 年版※156」を基に IPA が編集

SNS が情報源として機能している現代社会では、事実確認されていない情報の SNS 上の拡散が特に深刻である。同調査によると、提供される情報に対する信頼度は、「テレビ」が 66%、「ラジオ」が 63%、「Web メディアやメディアアプリ」が 57% だったのに対し、「SNS」は 50% と比較的低かった。フェイクニュースが最も広まっている場所を尋ねた結果では、回答者の 68% が「SNS」であると答え、「メッセージングアプリ」（38%）を上回り 1 位となった。一方で、ニュースや情報の主要な情報源を尋ねた結果では、「SNS」が 56% と最も高く、「テレビ」（44%）を上回っており、多くの国で 1 位となっていた。

メディアに関する国際比較調査※158 においても、日本を対象とした調査結果では、回答者の 58% が偽・誤情報の拡散に不安を抱いていると回答し、政治問題や新型コロナウイルス感染症（以下、新型コロナウイルス）、ロシア・ウクライナ戦争等に関連した偽・誤情報を日常的に目にしていることが分かっている。2023 年と 2024 年の調査結果を比較すると、政治問題や移民問題のトピックにおいて、偽・誤情報を見かける機会が増えているようである（次ページ図 2-2-2）。

更に生成 AI 技術の発展と一般市民への浸透によって、ディープフェイク等の技術を悪用した偽情報の拡散も、WEF の報告書では主要なリスクとして指摘されている。

G7 諸国、ブラジル、中国、インド、南アフリカで実施された世論調査である「ミュンヘン・セキュリティ・インデックス 2024」でも、「敵国による偽情報作戦」と「AI」に対するリスク認識が急上昇していることが示された※159。ミュンヘン安全保障会議の報告では、特に選挙における AI



■図 2-2-2　虚偽または誤解を招く情報を目にしたことのある話題（日本）
（出典）NHK 放送文化研究所「シリーズ「ロイター・デジタルニュースリポート 2024」（3）～偽情報・誤情報に対する意識は～【研究員の視点】#552[※158]」を基に IPA が編集

悪用の脅威が指摘され、警戒を呼びかけていた[※160]。後述のとおり、主要な各国選挙で AI の悪用も含めた偽情報の拡散が見られたところであり、2024 年は偽・誤情報の脅威が増大するとともに、一般市民にも脅威認識が拡大したといえよう。

(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、サイバー攻撃や情報戦等あらゆる手段を、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[※161]。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[※162]。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が、現在の IoT 社会では個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ことにより、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[※163]。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。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[※164]、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目標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[※165]。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や台湾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 による外国からの情報操作に関する報告書では、第 1 版において 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（両国の重なりがみられる事例が 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[※166]、続く第 2、第 3 版でも中露を主要アクターに挙げている。

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 Platforms, Inc.（以下、Meta 社）は 2024 年に 20 件の隠れた世論操作ネットワークを削除したと発表し、ロシア、イラン、中国が主要な発信元であると公表した[※167]。これらのネットワークは、偽の SNS アカウントや偽装ニュースサイトを用いて世論を誘導しようとするものであり、同社はその行動を「協調的不正行為（Coordinated Inauthentic Behavior）」と規定している。一方、Google LLC の Threat Analysis Group は、2024 年第 2 四半期だけで、中国関連の影響工作に関して最大で 3,931 件の YouTube チャンネルを停止し、1,177 件のブログのアカウントを削除したと報告している[※168]。また、同時期にロシア関連の 2,357 件の YouTube チャンネルも削除され

ており、プラットフォーム上での工作の拡大が続いていることがうかがえる。OpenAI, Inc.（以下、OpenAI 社）もまた、ChatGPT 等の自社モデルがロシア・中国・イラン等の国家アクターに利用されていたことを明らかにし、関連アカウントを停止したとする調査報告を公表している※169。2024 年、2025 年に連続して公表された報告書では、イランの「International Union of Virtual Media（IUVM）」に関連する影響工作を行っていた Storm-2035 という ChatGPT のアカウント群の存在を突き止め、その活動の一端として AI を用いた偽情報生成が確認されたことを明らかにした※170。一方で、米国大統領選挙後に大幅な方針転換を行った X（旧 Twitter）では、偽情報対策のラベル付与が縮小され、虚偽投稿の拡散が懸念された。英国サウスポートの暴動時※171（「2.2.3 (2) (e) 英国サウスポート暴動」参照）には、X Corp. のオーナーである Elon Musk 氏自身が偽・誤情報を助長する投稿に反応・拡散する場面も見られ、専門家から「最大のディスインフルエンサー」と批判される事態に至っている※172。一方、X では AI サービスである Grok を利用できるようになっており、それを使って、特定の投稿に対するファクトチェックを指示してリプライすることもできるため、ユーザーの AI 活用時の自主的な偽・誤情報対策の環境を提供している側面もある。

2.2.3 2024年度の注目事象

本項においては、各国における具体的な事例のうち、注目すべき事例を取り上げて解説する。

(1) 米国大統領選挙

2024 年の米国大統領選挙では、ロシア・中国・イランが関与すると見られる影響工作が確認された。米国の主要な情報機関で構成される IC（Intelligence Community）によれば、ロシアは偽のニュースサイト網や米国内の協力者を利用して世論を分断し、自国に有利な主張を広めたという※173。具体的には、ハイチ移民を装って違法投票を示唆する偽動画を作成する等のロシアの一連の情報工作は、選挙の公正さに疑念を生じさせ、信頼性を揺るがす狙いがあったと、米国国家情報長官室（ODNI：Office of the Director of National Intelligence）は FBI 及び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）との共同声明※174 で指摘している。更にロシアの関連組織はディープフェイク等の生成 AI 技術を駆使し、候補者に関する偽の映像や記事を大量生産して配信していた。「オペレーション・オーバーロード」という作戦では、偽情報の生成や拡散において生成 AI の使用が指摘されている※175。この作戦の特徴は、あえてファクトチェッカーやメディア、ジャーナリストに偽情報のファクトチェック依頼を送ることで彼らの能力に過負荷を与えることに加え、そのファクトチェック過程で偽情報と暴露されたとしても、偽情報や関連するナラティブの露出を高め、結果的に拡散を狙うという手法である。また米国財務省は 2024 年 12 月、ロシア連邦軍参謀本部情報総局と関係する地政学専門センター（CGE：Center for Geopolitical Expertise）が AI を用いて大統領候補者に関するディープフェイク動画を作成し、大規模な偽ニュースサイト網で拡散していたことを明らかにしている※176。CGE は AI 生成コンテンツを保管・配信する独自サーバーを構築し、少なくとも 100 以上の偽装ニュースサイトで偽情報を拡散していた。米国政府はこうした活動に関与したロシア人や組織に対し大統領令 13848 に基づく制裁措置を発動し、関係者を特定・資産凍結する対応を取った。

一方、中国は米国大統領選挙の結果自体には直接介入しない姿勢であると情報機関当局からは評価されているが、SNS を通じて米国社会の対立を煽り、民主主義は混乱していると印象付ける工作が報告された※173。ODNI によれば、中国当局は自国の技術企業と連携して米国向けの偽情報発信能力を強化し、X や TikTok を通じて米国内の左右両陣営に偽装アカウントを使って愛国心を装った分断情報を流していたという※177。例えば、中国発の影響工作「Spamouflage（スパムフラージュ）」では、米国有権者になりすました偽アカウント群を動員し、中絶や人種問題等論争になりやすい論点で相反する主張を大量投稿する手口が確認された。これら偽アカウントは与野党双方の政治家を批判し、特定の党派よりも「米国の愛国者」を名乗ることで信憑性を装っていた。米国当局は 2022 年の中間選挙でも超党派の反中政治家を標的に中国が中傷キャンペーンを行ったと指摘しており、この動向は 2024 年も継続した※173。もっとも、中国の狙いは米国世論の根本的な転向ではなく、米国内に潜む分断を拡大して民主主義の弱点を宣伝することにあったと分析されている。中国政府系の偽情報ネットワークでは、米国の選挙制度そのものよりも、「米国は内部分裂しており、国際的なリーダーシップやガバナンスを失ってグローバルパワーとして衰退しつつある」とのイメージ醸成に注力していた※177。

イランもまた米国大統領選挙に対する攻勢を強めた国の一つである。2024年夏、イランのイスラム革命防衛隊（IRGC：Islamic Revolutionary Guard Corps）系の組織が米国大統領選挙の両陣営関係者へのサイバー攻撃を試み、機密情報の窃取や漏えいによって選挙プロセスに不信を生じさせようとしたことを米国政府は明らかにした※176。実際に2024年9月には、ある大統領候補陣営の幹部らのアカウントがイランのハッカー集団により侵害され、選挙戦略に関わる内部資料が漏えいする事件が起きている※178。米国財務省はこの攻撃に関与したIRGC隊員や民間企業社員を特定し、選挙介入を理由に制裁リストに追加した。またイラン発の偽情報キャンペーンは米国の社会不安を煽る内容が多く、特に2023年10月以降のイスラエル・ハマス紛争に乗じた反イスラエル・反政府デマが米国内の分断拡大に利用された※173。米国情報当局は、イラン指導部が対イラン強硬派である特定候補の当選阻止を意図していた可能性を示唆しており、実際2024年米国大統領選挙でDonald Trump候補の陣営から機密文書が流出した背後にもイランの関与が疑われている※179。選挙後、米国司法省はイランがTrump氏暗殺を企図していたとする告発も行っており※180、イランはサイバー攻撃のみならず物理的脅威も含めたハイブリッド戦術で米国政局に影響を及ぼそうとしたと見られる。

こうした外国勢力の干渉に対し、米国政府とプラットフォーム各社は防御策を講じた。2016年以降の継続する選挙干渉に対し、2024年選挙を見据えて、ODNIに「外国からの悪意ある影響工作対策センター（Foreign Malign Influence Center）」を2022年に設立している。政府側では国土安全保障省（DHS：Department of Homeland Security）傘下のCISAやFBIが候補者や州政府に対し外国の偽情報活動に関する警告を発し、選挙インフラの監視を強化した※181。財務省外国資産管理室（OFAC：Office of Foreign Assets Control）による制裁発動のほか、主要IT企業も偽情報アカウントの削除やディープフェイク検知技術の導入を進めた。現時点では、2024年米国大統領選挙全体を決定的に左右したと考えられるような工作は確認されておらず、外国からの影響工作の影響は大きなものではなかったと分析されている※175。しかし選挙期間中に行われた爆破予告（ロシア発のドメインから発信）※179や大量の偽情報投稿は有権者の不安を煽り、一部投票所の混乱を招いた。

このように、米国大統領選では複数の国からの影響工作を受けており、外国勢力による選挙干渉は引き続き大きな脅威である。そして、これは同盟国を含む民主主義諸国にとっても、深刻な脅威をもたらす情勢となっている。

(2) 欧州での偽情報流布の影響（ロシアを中心とした影響工作と極右台頭）

2024年は欧州各国で重要な選挙が相次ぎ、ロシアを始めとする権威主義国による組織的な偽情報攻勢が各国で顕在化した年でもあった。6月には欧州議会選挙が27ヵ国で実施され、続いて英国やフランス、オーストリア等主要各国でそれぞれの国政選挙が行われた。その結果として、一部では極右政党が一定の勢力伸長を見せたものの、政治的中道勢力が踏みとどまり、外国からの影響工作や選挙干渉が直接選挙結果を左右する事態には至らなかったと当初評価されていた※182。しかしEEASや安全保障専門家らは、外形的に明確なインシデントというべき事案が発生していなくても、ロシアや中国による長年の偽情報攻勢が社会の結束を損ない、政治的分裂を悪化させようとして欧州民主主義に与えた影響を看過すべきでないとして、持続的な脅威として引き続き警戒を強めている※183。

(a) 欧州議会選挙

欧州議会選挙の前後には、ロシアを中心とする外国勢力による選挙干渉疑惑が相次いで浮上した。例えば、2024年3月にチェコ当局はプラハに本部を置くニュースサイト「Voice of Europe」を閉鎖した。このサイトは名称に反し親露派オリガルヒでウクライナ人のViktor Medvedchuk氏が立ち上げた偽装メディアであり、欧州各国の政治家に報酬を支払って親露的な政治宣伝をニュースを装って紛れ込ませていたと報じられた※182。更に5月には、ベルギーとフランスの捜査当局がオランダの極右派欧州議会議員Marcel de Graaff氏の議会補佐官の自宅や事務所を捜索し、ロシアから欧州議会議員への賄賂工作に関与した容疑で捜査を進めた。当局はこの補佐官が「Voice of Europe」を通じてロシア資金を各国の極右議員に仲介し、見返りに親露的発言を欧州議会で行わせていた可能性をつかんだとしている。同補佐官はフランスの「国民連合（RN：Rassemblement National）」（旧、国民戦線）や「ドイツのための選択肢（AfD：Alternative für Deutschland）」の欧州議員にも協力していた過去が判明している。加えて同5月、ドイツ連邦議会議員Peter Bystron氏（AfD所属）がロシア人オリガルヒから2万ユーロの資金提供を受けていた

音声記録が暴露され、議員特権剥奪に至る事案も発生している。このように、ロシア政府は長年かけて欧州各国の極右勢力との間に資金・情報の影響ネットワークを構築しており、その一端が2024年に相次ぎ表面化した形である。欧州議会内では国民連合やAfD、オーストリア自由党（FPÖ：Freiheitliche Partei Österreichs）等親ロシア色の強い右派会派が勢力を増しており、ハンガリーのViktor Orbán首相が組織する欧州右派連合「欧州のための愛国者達（Patriots for Europe）」の旗のもとで第3会派を形成するに至っている。

また中国も、欧州でロシアに倣った影響工作を行っている実態が明らかとなっている。2023年末、ベルギー極右政治家が2019～2022年に中国情報機関と通じて「米欧分断」を図り、香港や新疆ウイグル問題で中国の主張を広めていたとの報道がなされた※182。更に2024年4月にはドイツ当局が欧州議会議員Maximilian Krah氏（AfD所属）の議員補佐官を逮捕した※184。この補佐官は中国の対外工作部門に欧州議会内部情報を繰り返し流し、在独中国人活動家の監視にも協力したスパイ容疑を掛けられている。同氏自身も2024年欧州議会選挙におけるAfDのトップ候補であり、ロシア及び中国から資金提供を受けていた疑惑でドイツ検察当局の捜査下に置かれた。更に欧州議会選挙の直前、オランダでは新党「オランダ計画党（Nederland met een plan）」が中国の統一戦線工作部に関連する団体から寄付を受けていたと報じられた。この新党はEUと中国の関係強化を掲げており、親中的な政策主張の背後に中国当局の影響が指摘されている。

欧州委員会や各国政府もロシア・中国発の情報操作に対抗すべく対策を講じている。EUは2024年2月に発効した「デジタルサービス法（DSA：Digital Services Act）」に基づき、大規模オンラインプラットフォーム等に対し組織的な偽情報操作の迅速な発見・除去を義務付けた。しかし規制の実効性確保には時間を要し、直前の欧州議会選挙期間中もロシア寄りの広告がFacebook上で拡散されたり、TikTokが虚偽広告の承認を許していたりしたとの指摘があった※182。ロシアの偽情報キャンペーングループ「Doppelgänger（ドッペルゲンガー）」により、2023年8月から2024年3月までの間に、3,800万人のフランスとドイツのFacebookユーザーが、影響工作の標的にされた。5月だけでも、275件の反EU・反ウクライナの政治広告が、フランス、ドイツ、ポーランド、イタリアの300万人以上のFacebookユーザーに届いた。また同月、ロシア国営メディアRT（旧Russia Today）のコンテンツをミラーサイトや地方ニュースに偽装して再配信する「マトリョーシカ型」情報操作も欧州各地で確認された。EUはRTやSputnikの公式配信を禁じているが、ロシア側はこのような巧妙な迂回戦術で制裁網を潜り抜け、欧州市民への影響力を維持しようとしている。EEASのEast StratComタスクフォース等は定期的に偽情報のファクトチェックを公開しているものの、プラットフォームの対応には差異がある。例えば、Xでは国家支援型のメディアや政治広告に対するラベル表示を削除してしまっていたり、TikTokでは偽情報を含む広告掲載を承認してしまっていたりする等※182、ある程度ボットネットワークに対処をしていたとしても、RT系記事拡散が可能なプラットフォームとして、EUの規制対応にも関わらず依然として利用されてしまった事例も出ている※185。

（b）フランス総選挙

2024年6月、フランスではEmmanuel Macron大統領が下院を解散し、6月下旬から7月にかけて国民議会下院選挙が実施された。フランスでは極右政党の国民連合がロシアと歴史的に近く、2014年にロシア系銀行から融資を受けた事実も知られる。前述の欧州議会議員補佐官による賄賂工作では、国民連合所属の欧州議員が標的となっており※182、2024年選挙戦でも、ロシアの情報工作ネットワークが国民連合を後押しして、対抗する人民戦線を分断するような偽情報を利用したキャンペーンを行っていたとされる※186。フランス政府は2021年に偽情報対策専門機関VIGINUMを設立しており、2024年2月にはロシア発の工作ネットワークである「Portal Kombat」を摘発・公表した※187。この工作ネットワークはクリミア拠点のIT企業TigerWebが運営に関与し、オリジナルコンテンツを一切作成せず、ロシアまたは親露的なアクターが運営するSNSアカウントやロシアのニュースメディアをリポストして拡散する、ロシア情報工作に典型的な手口であると判断された※188。更に、別のロシアの影響工作ネットワークである「CopyCop」も、特にウクライナ支援に関してMacron政権を誹謗中傷するために、選挙前からその活動を活発化していたことが明らかになっている※189。CopyCopは生成AIも活用した偽サイトとそのネットワークによる情報拡散を特徴とし、一例では、CopyCopのなりすましによる共和国連合（Ensemble pour la République）関連サイトに見せかけた偽サイトで、「現職大統領陣営に投票する代わりに100ユーロの『マクロン・ボーナス』をフランス国民に約束した」といった偽情報を拡散していた。選挙後には、フラ

ンス政府は同じく生成 AI を活用するロシアのネットワークである Storm-1516 の影響工作活動についても明らかにして非難を表明した※190。VIGINUM は 2021 年からロシアを中心とした偽情報の脅威を国民に周知してきており、今回の総選挙の前にも、前述のような報告書発出等により警鐘を鳴らしてきた。その甲斐もあってか、フランス総選挙では極右国民連合が一定議席を維持したものの左派・中道・極右の 3 勢力が拮抗し、ロシアが望むような急進的変化は生じなかった。

(c)オーストリア総選挙

オーストリアでは 2024 年 9 月の国民議会総選挙で、親ロシア志向の強い極右政党 FPÖ が躍進し第 1 党となった。この背景には、ロシアの長年にわたる浸透工作が関係している。2019 年に明るみに出た「イビザゲート事件」※191（FPÖ 党首がロシア富豪の姪と称する女性に便宜供与を約束した録画が公開された事件）以来、ロシアと FPÖ の癒着が長年懸念されていた。選挙後の 2025 年 3 月、オーストリア国内情報局はあるブルガリア人女性スパイの捜査から、ロシアがドイツ語圏向けに大規模な偽情報キャンペーンを展開していた事実を突き止めた※192。この女性は 2024 年末に逮捕されモスクワのために働いていたことを自白したが、最終的に釈放されている。押収された電子機器の分析で、ロシアがウクライナ侵攻後、オーストリアやドイツ等ドイツ語圏諸国を標的にウクライナに関する偽情報を流布し、国内の極右・反政府運動を扇動する工作を行っていたことが明らかになった。キャンペーンの一環として、偽情報の拡散と並行してウクライナ難民を中傷するステッカーの配布やグラフィティ活動を行い、極右のシンボルや民族主義的なメッセージを宣伝していた。こうした事例から、オーストリアがロシア情報工作の欧州拠点の一つとなっていることがうかがえる※193。2024 年選挙で FPÖ が政権入りしたことで、オーストリアの対露姿勢は軟化に向かったが、これにより欧米の対露強硬路線に一定の楔が打たれ、ロシアの欧州分断戦略はオーストリアでは一定の成果を上げたと見ることもできる。

(d)ルーマニア大統領選挙

ルーマニアでは 2024 年 11 月の大統領選挙が、ロシアの情報工作により深刻な混乱に陥った。2024 年の大統領選挙では第 1 回投票で極右ポピュリスト候補 Calin Georgescu 氏が予想外の首位となったが、この結果を受け情報機関当局が「外国勢力の介入による不正の可能性が高い」と指摘する機密解除文書が Klaus Werner Iohannis 大統領（当時）から発表された※194。最終的に憲法裁判所は、11 月に実施された大統領選挙を無効とする判断を示した※195。調査の結果、SNS アルゴリズムの特定候補者への悪用、不透明な生成 AI の利用や不当な資金源による選挙活動等が確認され※196、更に情報機関の調査ではその背後にロシアの存在があり、TikTok 等、SNS 上で Georgescu 候補を支援する大量の偽情報キャンペーンを展開していたことが明らかにされた※197。具体的には、同候補の露出が上がると他の候補者の露出は下がるようなアルゴリズムの適用や、ロシアに紐付くボットネットの活用、TikToker の買収等があったと考えられている※198。この事態を受け、EU 欧州委員会は TikTok Inc. に対し DSA 違反の正式調査を開始し、プラットフォームとしての対応不備を追及した※199。翌 2025 年 5 月に再選挙が実施されることとなった。ロシア政府はこれらの介入疑惑を公式には否定し、「Georgescu 氏は不当に選挙から排除された」と主張し、選挙の正当性に疑問を投げかける発信を行った。また、国営メディアや親露派アカウントを通じてその主張を拡散する宣伝を展開した※200-1。しかしその否定とは裏腹に、TikTok 以外にも、ルーマニア語の Telegram チャンネルのメッセージの 4 分の 1 は、ロシア国営メディアやその他の親露の情報源からの情報を宣伝するものであったことも確認されている※200-2。ルーマニアの事例は、ロシアが東欧でも巧妙に民主主義的プロセス攪乱を図った典型といえる。SNS 利用率の高い若年層を狙い TikTok を主戦場とした点では新しい世代に向けたハイブリッド戦の戦術であり、欧州各国が警戒を強めている。

(e)英国サウスポート暴動

2024 年 7 月 29 日、英国のサウスポートで 3 人の少女が刺殺され、同時に 8 人の子供と 2 人の大人も負傷する事件が起こった。警察は、17 歳のルワンダ系英国人（ルワンダ出身の両親のもとに英国国内で生まれており、移民ではない）の犯行として彼を逮捕した。ところが同日、犯人は 17 歳のイスラム系の亡命希望者である Ali al-Shakati なる人物だとする偽・誤情報がインターネット上に出回った。この「ニュース」を最初に投稿したのは、オンライン・インフルエンサーで陰謀論者の Bernadette Spofforth とされている※201。その数分後、米国の通信社を名乗る Web サイト「Channel3 Now」がこの偽情報をニュース記事のような形で拡散させた。X では、「Channel3 Now」の当該投稿は 2,700 万ビューを超え、

極右系インフルエンサーを中心に移民犯人説が拡散されていった。このような情報拡散で移民への憎悪が高まり、翌7月30日、サウスポートでの追悼集会に乗じて、極右系グループを中心とした暴動が発生した。

英国紙 The Telegraph によると※202、YouTube チャンネル「Channel3 Now」は2012年に開設され、当初はロシアの都市イジェフスクでのカーレースに関するロシア語動画を公開していた。その後しばらくはアカウントが利用されていなかったが、2019年、パキスタンに関する英語の動画を公開し、2023年には「Channel3 Now」の Web サイトがリトアニアのドメインで作成され、同 YouTube チャンネルにリンクされた。英国調査報道局は、「Channel3 Now」が前述のような経緯でロシアのチャンネルとして作られたことを確認し※203、Steven McPartland 元安全保障相も、この暴動を引き起こした SNS 上の偽情報拡散キャンペーンの背後にロシアがいる可能性を示唆している※204。一方で捜査当局は、抗議行動を引き起こしたディスインフォメーションへのロシアの関与を証明するには、まだ十分な証拠がないとしている※201。

この暴動について、「Channel3 Now」のルートにおけるロシア関与の証拠は不十分ではあるものの、移民憎悪の扇動や移民に関係する陰謀論の利用という点でこれまでロシアが英国に行ってきた影響力工作のアプローチやそのナラティブとの類似がある点には注意が必要である。

これまで、ロシアの影響力工作は常に北大西洋条約機構（NATO：North Atlantic Treaty Organization）諸国の内部対立を悪化させようとしてきた。だが英国ではそれらに加えて、ロシアは英国人と移民の間に存在する対立を利用し、民族的・宗教的憎悪を煽って英国社会を弱体化させようとしている。一部の英国人が、移民に対する政府のリベラルすぎる公共政策に不満を抱いているという指摘もあり※201、そのためロシアは対英工作において「なぜ移民が必要なのか？　彼らのホテルや避難所、モスクを破壊する必要がある」と繰り返し扇動している。

RT の宣伝担当者である Vladimir Kornilov 氏は、自身の Telegram チャンネルを使って、この暴動に際し「今こそ英国の国内問題を解決すべきであり、世界のあらゆる紛争に干渉すべき時ではない」という主張を広めていた※201。

更には、国際メディアプラットフォームである openDemocracy によれば※205、こうした移民憎悪の言説を支えるものとして、「グレート・リプレイスメント（大置換）陰謀論」のナラティブが利用されていると考えられるという。この理論では、北半球の白人が南半球からの移民に計画的に「取って代わられ」ており、フェミニスト達が中絶や避妊によって出生率を抑制していると考えられている。このような陰謀論をロシアが利用して相手国の分断を扇動し、社会を不安定化させようとしていることは既に先行研究で指摘されており※206、この暴動でもそのナラティブの背景にあるロシアの影響は看過できない。

なお暴動後、英国政府は「オンライン安全法（Online Safety Act）」の早期施行を表明し※207、SNS 企業に対し有害コンテンツ拡散防止の法的責務を課す姿勢を示した※208。

(3) 太平洋地域での偽情報流布の影響

インド太平洋地域でも、中国とロシアによる偽情報・影響工作が活発化している。とりわけ台湾や南太平洋の小国の政治に干渉する動き、及び地域の安全保障イベントに絡めた情報戦が顕在化している。各国・地域の政府は警戒を強めているものの、偽情報キャンペーンの巧妙化と拡散力の強大化が課題となっている。

(a) 台湾

台湾では2024年1月の総統選挙で与党候補の頼清徳氏が当選（5月に就任）し、これに対し中国が一層の圧力を強めた。中国は軍事演習や外交的威圧に加え、オンライン上での情報戦・認知戦をも仕掛けている。台湾国家安全局の報告によれば、2024年に中国が台湾向けに流布した「物議を醸す情報」は前年比60%増の約216万件に上った※209。その主要テーマは台湾、軍、そして頼清徳総統に対する米国の支援に対する懐疑的な見方を広めることで、「政府に対する国民の信頼を損ない、社会的分裂を高めようとした」と報告書は述べている。拡散の主要なプラットフォームは Facebook であったが、Facebook での件数が前年比40%増なのに対し、X は244%増、PTT や Dcard といった台湾の掲示板フォーラムは644%増と、標的とする SNS の件数増加に偏りが見られる。また、調査対象のプラットフォーム全体で2024年には合計2万8,216件の不正アカウントが確認され、2023年から1万1,661件増加した。主要なプラットフォームはやはり Facebook であり全体の77.85%（2万1,967アカウント）を占めていたが、一方で TikTok の不正アカウント数は1,614%増の4,371に達した。これは、若者世代を対象とした SNS をターゲットとしたものと考えられる。拡散されている偽情報の主要なナラティブは、

「毎年恒例の漢江訓練を含む軍事演習は台湾の指導部が脱走するためのリハーサルである」※210といった政府要人が国を見捨てる類型のものや、「米国はウクライナと同様、台湾にも武器を売って利益を得ようとしている」※211といった「疑米論（米国懐疑論）」が主流であり、毎年の演習や関連する外交イベントの度に繰り返し拡散されている。しかし、2024年7月ごろから、台湾の親日性を攻撃し日台離反を扇動する偽情報の拡散も増えてきている※212。具体的には、「日本人の子孫が台湾に住み、台湾独立を主張している」「台湾の地方政府が、第二次世界大戦中に日本軍によって強制連行された台湾人慰安婦像を撤去し、台湾政府は、台湾人慰安婦は強制連行されたのではなく、自発的に日本軍のために働いたと主張している」「頼清徳・台湾総統が金門島を訪問した際、日本式の旭日旗の前で演説を行った」といった内容である。頼総統の演説については、バックに掲示されていた国防省の紋章が旭日旗に似たデザインだったにすぎないが、演説画像に誤ったキャプションが付されて拡散された※213。これらは微博（Weibo）等中国のSNSにも輸入され、むしろ台湾国内よりも中国で反日感情、反台感情が高まった。台湾有事の懸念が高まる中では、対台湾だけでなく、このように日本を含めた有事に関わる可能性の高い国が関係する偽情報の流布も憂慮されるところである。日本関連の偽情報については、海外の事例であっても政府が鋭敏に把握して反論する体制が今後は求められるだろう。

(b)ツバル総選挙

台湾と公式な外交関係を持つ国の一つであるツバルでは、総選挙前後に中国が偽情報を用いた情報戦を展開し、台湾との外交関係を揺るがそうとする動きが確認されたと報じられた※214。選挙の前日、ある地元メディアは、中国の国営メディアである中国国際電視台（CGTN: China Global Television Network）のドメインcgtn.comを使用したアカウントから電子メールを受け取った。そのメールは、「ツバル放送局の幹部がツバルの選挙と台湾との関係断絶の可能性に焦点を当てた800字のオピニオン記事の執筆依頼に協力を求めるもの」で、記事執筆と執筆依頼の仲介協力に対する謝礼として合計450米ドルを支払うとの記載もあった。このほかにも、選挙直前には「選挙後にツバルが台湾との関係を断つ」との噂が流され、中国が背後で流布した可能性が指摘された。また、直前に隣国ナウルが台湾と断交し中国と国交を樹立したことから、ツバルも追随するとの噂も広まった※215。選挙後に誕生したFeleti Teo新首相は台湾との「揺るぎない」関係継続を表明したが、その後も中国の影響工作は続いた。2024年末には、中国のCGTNがツバル住民に「台湾は中国の一部」と語らせたり、「中国と国交を樹立すればインフラ整備や気候変動対策で利益が得られる」と示唆する複数の映像を放映し、台湾側はこれを両国関係の弱体化を狙った偽情報キャンペーンだとして強く非難し、台湾のツバル駐在大使館も声明で、言論の自由を尊重しつつも中国による世論操作や認知戦を容認しない姿勢を明確にしている※216。

このように、中国は自国の利益のために太平洋島しょ国まで、情報戦・認知戦の戦場を拡大していることがうかがえる。

(c)ソロモン諸島国政選挙における中露の連携

2024年のソロモン諸島総選挙では、ロシアと中国が偽情報を用いた選挙干渉工作を共謀して行ったとみられると報告されている※217。両国の国営メディアは、米国が同国への援助や現地ネットワークを利用して選挙に介入し、都合の悪い結果の場合には暴動を扇動して政権転覆を企図しているとする根拠なき言説を発信したと、オーストラリア戦略政策研究所は指摘している。

具体的には、選挙の約2週間前に匿名寄稿の米国陰謀告発記事がKGB主導で創刊されたとする雑誌CovertAction Magazineに掲載され、程なくロシアのSputnikも匿名情報源に基づき米国による選挙クーデター計画説を報じた※218。中国共産党系紙「環球時報」もこれを引用して米国の介入を糾弾した※219。更に「米国が必要なら暴力的手段による民主的移行を図る」と記された偽造書簡が国際選挙制度財団（IFES：The International Foundation for Electoral Systems）関係者を装って出回り、その内容はSputnik報道で情報源とされる匿名の証言者の言葉遣いと酷似していた。こうした偽情報は一般有権者にはほとんど浸透せず、現地世論を大きく動かすには至らなかったと分析されている。

しかし当時のManasseh Damukana Sogavare首相の与党O.U.R.は問題のSputnik記事をFacebookで共有し、首相自身も外国勢力が選挙に介入し暴動を企図していると公に主張した。この事例は、中国とロシアの制限なき戦略的協力関係が情報戦にも及ぶことを示している。両国の宣伝当局は、報道分野でメディア協力協定を結ぶ等の協力関係構築を進めており※220、欧州や南米でも中露が偽情報の増幅のために連携する事例が増えている※221。国家としては関係を深めつつも情報空

間での連携は機会主義的とみられるという指摘もあり、本件はそうした連携の機会が太平洋地域でも現れた事例であるといえる。今回ロシアが長年唱えてきた「米国国際開発局（USAID：United States Agency for International Development）は政権転覆の道具」とのナラティブが初めて中国の対米プロパガンダに援用された点が特徴的である。このように安全保障上の懸念国同士が連携すると、偽情報の拡散効果は倍増してしまうため、更なる警戒が必要である。

(4) ハイブリッド型サイバー攻撃の事例

2024 年度には、偽情報拡散による「情報操作型サイバー攻撃」と「機能妨害型サイバー攻撃」を組み合わせた「ハイブリッド型サイバー攻撃」が顕在化した。特にウクライナ支援に絡む国際会議や西側諸国が関与する首脳会議の周辺で、安全保障上の懸念国が情報操作とDDoS 攻撃等のサイバー攻撃を同時に仕掛ける事案が発生している。以下、日本が関連する主要な二つの事例を取り上げる。

(a) ウクライナ復興支援会議

日本政府は 2024 年 2 月 19 日、東京で「日・ウクライナ経済復興推進会議」を開催し、官民合わせて約 350 名が参加してウクライナ復興支援策を協議した※222。この重要な国際会議を標的に、親ロシア勢力がサイバー攻撃キャンペーンを実行している。ちょうど会議当日の 2024 年 2 月 19 日、ロシア寄りのハクティビスト集団「NoName057(16)」が「日本を標的にする」と犯行を予告する声明を Telegram 上に発出した※223。声明では、日本が「ロシアと戦闘中のウクライナを支援していること」が標的化の理由に挙げられており、日本のウクライナ支援策への報復としてサイバー攻撃を開始する旨が示された。実際、NoName057(16) は他の親露グループ（Cyber Army of Russia や UserSec 等）とも連携し、日本国内の政府・民間の Web サイトに対する大規模 DDoS 攻撃を仕掛けた。彼らが公開した標的リストには、日本の自動車関連団体や大手エネルギー企業、国際経済団体等のサイトが含まれており、これらに対しアクセス不能にする攻撃を行ったと主張している。更に NoName057(16) 自身は日本の国会の公式サイトや特定政党のサイト、日本税関当局、通信大手、証券業協会サイト等をダウンさせたと主張した。これら一連の攻撃は典型的なハクティビスト型 DDoS 攻撃で人的被害はないが、日本社会に不安を与える心理戦の側面を持つ。併せて、X では岸田首相（当時）が米国政府高官に睨みつけられているように見えるディープフェイク画像※224 や、「ウクライナ復興支援の予算が 50 兆円くらいになる」※225 といったような偽情報が拡散された。こうした影響工作に対しては、外国からの関与があったと外交筋が明らかにしている※226。これはロシアがウクライナ支援国に対し報復的ハイブリッド戦を仕掛けている一例であり、日本のみならず各国で類似の手口が警戒されている。偽情報と「機能妨害型（もしくは機能破壊型）サイバー攻撃」の組み合わせは相乗効果で標的国の混乱を狙うものであり、同様の攻撃に警戒が必要である。

(b) NATO サミットにおけるディスインフォメーションと DDoS 攻撃

ロシアはウクライナ支援の要となる NATO サミットに対しても、サイバー攻撃と偽情報を駆使した情報戦・認知戦を仕掛けている。2024 年 7 月にワシントン D.C. で開催された NATO サミットでは開幕前後の期間を通じて、ロシア系ハッカー集団「People's Cyber Army」や NoName057(16) が、NATO の危機管理・災害対応センター、連合軍特殊作戦部隊司令部、軍需品安全情報分析センターの Web サイトや各加盟国政府及び重要インフラ等の Web サイトに DDoS 攻撃を仕掛けている※227。更に同サミットに合わせ、少なくとも二つのロシア系グループが偽情報キャンペーンを展開していたことが Graphika Technologies, Inc. の調査で明らかになっている※228。一つは NATO 公式サイトを模倣したドメインから偽のプレスリリースを流布する手口で、例えば「NATO が防衛予算を倍増することを決定」「NATO がウクライナ軍をフランスに派遣し、同年夏に発生したフランス国内暴動に投入することを検討」といった偽情報が発信された。もう一つのグループはリトアニア政府から入手したと称する NATO サミットの内部警備資料を公開し、「NATO の機密が漏えいした」と騒ぎ立て拡散した。これらは手口や文体から過去に欧州で活動したロシアのキャンペーングループである、Doppelgänger や「Secondary Infektion」との類似性が指摘されている。また、単純な偽情報だけでなく、軍服を着たキャラクターや食糧とともに武器を配給しているようなイメージを用いて、NATO が戦争を起こしていると思わせるナラティブをベースに、反ユダヤ陰謀論や各国政府高官やセレブリティが小児性愛犯罪に加担しているといったディープステート（闇の政府）陰謀論と関連性が見られる偽情報、その他の様々な陰謀論と組み合わせて誇張したイメージをミュージックビデオにした動

画等も生成 AI によって量産され、拡散されている※229。

更には、日本でも次のような複合的な攻撃が見られた。7 月に「日本・NATO による合同軍事演習の機会を拡大し、パートナーシップを強化していく」との NATO 事務総長による宣言が発表された後、政党や鉄道会社等の Web サイトに対し NoName057(16) 等による DDoS 攻撃が発生した※230。そして同時期に SNS 上で、「NATO や NATO サミットは戦争拡大を目的としている」※231、「NATO はウクライナの加盟を保証していない」※232、「NATO によって日本が戦争に巻き込まれる」※233、「日本は軍需産業発展のため NATO に迎合している」※234、といったロシア寄りの戦略的なナラティブや偽情報が Sputnik を中心に親露派アカウントも利用しつつ拡散された。

こうした一連の行動は、異なるハッカー集団が協調してハードな「機能妨害型サイバー攻撃」とソフトな「情報操作型サイバー攻撃」を並行実行するという、「ハイブリッド型サイバー攻撃」として新たなサイバー攻撃動向として注視すべきである。政府機関や重要インフラ系の Web サイトが機能不全に陥ることで、ウクライナ支援継続に対する嫌がらせと政府への信頼を毀損することを企図し、更にこれらに対する社会の不安感を煽るような偽情報を拡散することで相乗効果を狙うものである。これはまさにハイブリッド戦の典型であり、今後も G7 や NATO といった外交イベントの度に類似の攻撃が試みられると予想される。各国政府と国際機関はこの教訓を踏まえ、技術的防御と戦略的なコミュニケーション、情報発信を組み合わせた包括的な対策を講じていく必要がある。

2.2.4 2024年度以前からの継続事象

本項においては、2024 年度以前から継続している、偽・誤情報の主要な拡散事象を解説する。

(1) 新型コロナウイルス

新型コロナウイルスをめぐっては、パンデミック初期からの偽・誤情報が 2024 年度も根強く残っている。代表的なものはワクチンに関する陰謀論であり、「ワクチン接種を強制される」といった内容が国内では引き続き拡散されたが、実際には WHO（World Health Organization：世界保健機関）主導の「パンデミック条約」草案に強制接種の規定はなく、WHO も何度も否定している※235。また、日本で 2023 年秋に導入された新型コロナウイルスの「レプリコンワクチン」についても、「従来のファイザー製より死亡率が 75 倍」とする誤った情報が 2024 年度に流布された※236。厚生労働省の資料を誤読したもので、ワクチン接種との因果関係が証明されていない数字を用いた主張であり、実際には死亡報告例も取り下げられている。このほか「コロナワクチンで 50 万人が死亡」「日本で人体実験が行われている」等極端な反ワクチン説も散見され、その多くは科学的根拠に欠けることが専門家の検証で明らかになっている※237。こうした新型コロナウイルス関連の偽情報は、度重なる否定やファクトチェックにもかかわらず一部で信じ続けられている。

更に 2024 年 11 月には、日本政府が mRNA ワクチンを「史上最も危険な薬」と分類したと主張するニュースが中国の SNS で拡散されたという事例も発生した※238。このニュース自体は、親露派の偽情報サイトと判明している The People's Voice というサイトから発信されたもので、そのスクリーンショットが Weibo で拡散され X でも広まったものである。2021 年 7 月に中露間でメディア協力に関する二国間協定が締結されて以来、新型コロナウイルスの「バイオラボ陰謀論」等を始めとして両国の偽情報拡散、ナラティブ形成の連携が強まった※220 ことを鑑みると、こうしたワクチンに関する偽情報が日本と関連付けて拡散された事例は中露連携による偽情報拡散の射程が日本に至っているとして警戒すべき一例といえるだろう。

(2) ロシア・ウクライナ戦争

ロシアは 2022 年 2 月のウクライナ侵攻に際し、開戦当初から偽情報を戦略的に利用して情報戦・認知戦を交戦国であるウクライナだけでなく国際世論に対しても展開し、2024 年度においてもその戦闘様相を継続させている。侵略を正当化するため「ウクライナの非ナチ化」や「NATO による脅威」といったナラティブが用いられ※239、ウクライナ政府をネオナチ国家、NATO を陰で操る侵略者、と虚偽の位置付けで描いている。そして国際世論を分断する戦略を有しているため、対ウクライナ支援や NATO 拡大への反対論を煽る影響工作も続いている。

2024 年には米国大統領選挙や NATO サミットにおけるロシア勢力による偽情報の拡散が見られたが、国際または内政上重要なイベント時以外にも多くの偽情報の発信が続いた。一例としては、米国国務省（DOS：U.S. Department of State）報道官がロシア内地への無差別攻撃を容認していることを示唆するかのようなディープフェイク動画がロシアの Telegram 上に出回り、ロシアの国営メディアや政府関係者によって拡散された※240。こうした事例に見られるように、ボットアカウント生成や AI 合

成映像等のデジタル手法が駆使され、国家ぐるみの巨大な宣伝網（SNS、RT や Sputnik 等の国営メディア、偽装ニュースサイト、サイバー工作部隊）によって偽情報が大量生産・拡散されている。サイバー空間での影響工作は、これまで Internet Research Agency という企業がロシア政府機関と協働していたが、これは Yevgeny Viktorovich Prigozhin 氏による創設であったため、同氏が率いていた軍事組織ワグネルの反乱により解体された。その後、現在の工作活動は、ソーシャル・デザイン・エージェンシー（SDA：The Social Design Agency）、インターネット開発研究所（The Institute for Internet Development）、そしてストラクチュラ（Structura）といった三つのロシア企業に帰属するとされており、これらの企業は、「雇われ影響工作企業（influence-for-hire firms）」と呼ばれている※241。

更に、ロシアの偽情報は中国とも連動しており、例えば「ウクライナに米国の生物兵器研究所がある」という根拠なき陰謀論は、後追いで中国政府高官や国営メディアによって増幅された※220。こうした偽情報キャンペーンは単発の誤報ではなく、自国に有利なナラティブを形成するように国家戦略の一環として継続的に構築・流通している点に特徴がある※242。また、紛争が長期化する中で、西側諸国がウクライナに供与した武器の行方をめぐる偽情報も続いている。ロシア発のプロパガンダでは「ウクライナが受け取った武器を第三国やテロ組織に横流ししている」といった主張が度々現れ、2023 年 10 月には「ウクライナ経由の武器がハマスに渡った」との情報が SNS で拡散された※243-1。しかしこれは BBC のニュース映像を装った偽動画によるもので、BBC や調査報道機関がすぐに否定し、実際にはウクライナ当局も供与兵器の管理徹底を強調している。このように、ロシア・ウクライナ戦争に関する偽情報は、ロシアの侵攻を正当化するナラティブをベースに、生物兵器開発の陰謀論※243-2 から新たな情勢を絡めた武器横流し説まで形を変え、ウクライナ支援国に対するハラスメント目的の偽情報も派生して、日本を含む国際社会で流布し続けている。

(3) イスラエル・ハマス紛争

2023 年 10 月に始まったイスラエルとハマスの武力紛争に関する偽情報は、その後も 2024 年度を通じて拡散し続けた。戦場がガザから情報空間へと移る中、戦略的レベルでは「誰が被害者で誰が加害者か」という認識をめぐる物語の争奪となり、偽情報が構築する戦略的ナラティブが重要な役割を果たした※244。両陣営とも自らの正当性を訴える被害者としてのナラティブを掲げ、大量の映像や情報を発信して国際世論の支持獲得を試みている。

この過程で SNS 上には偽・誤情報が氾濫し、過去の映像やゲーム画面があたかも現在の戦闘映像であるかのように使い回されたほか※245、AI で生成・加工された偽の画像・動画が本物として共有される例も相次いだ※246。

開戦時には大量の偽情報が飛び交うこととなり、イスラエルの SNS 分析企業である Cyabra によれば、攻撃開始後の 1 ヵ月で、少なくとも約 4 万件以上の Bot アカウント及び不正なアカウントを確認したという。また、Facebook、Instagram、TikTok、X でこの武力衝突について投稿したアカウントのおよそ 4 個に 1 個が偽のアカウントであることが攻撃後 1 日で判明している。更には、アル・アハリ病院での爆発から 24 時間以内に、X に本件を投稿したアカウントの 3 個に 1 個以上が偽のアカウントであった。2024 年の事例としては、米国で起きた橋梁崩落事故を「イスラエルの仕業」とする荒唐無稽な陰謀論が X 上で拡散される等、紛争と無関係な出来事まで情報戦に利用されている混乱ぶりである。国際的にも、ロシアや中国、イランの国家メディアや偽アカウントがオンライン上でイスラエル・米国を貶めハマスを擁護する情報戦を展開している※247。これらの偽情報も単発の情報発信による社会の混乱（情報騒乱）にとどまらず、各主体の戦略的ナラティブに基づいた情報戦・認知戦の様相を呈している。

2.2.5 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

本節で取り上げた情勢や事例が示すとおり、2024 年も各分野で偽・誤情報が猛威を振るった。そのうち、主要な傾向として以下の 2 点が挙げられる。第 1 に、生成 AI が偽・誤情報拡散を加速・巧妙化させている点である。2022 年ごろから ChatGPT や Midjourney、Stable Diffusion といった生成 AI がリリースラッシュとなり、おおよそ 1 ～ 2 年かけて一般への浸透が進んできた。また、X では、SNS に付随した AI サービスとして Grok が 2024 年に提供され始め、AI を使った SNS 投稿を格段に容易にした。ユーザーが容易に生成 AI でフェイク

画像・音声・動画を作成できるようになり、災害時に偽の被害写真が出回ったり政治家になりすました偽映像が登場したりする等、ディープフェイクによる新たな混乱が顕在化した。更に、「2.2.2 偽・誤情報の情勢」及び「2.2.3 2024 年度の注目事象」で触れたとおり、国家アクターが情報操作のために戦略的に生成 AI を利用する事態にも至っている。第 2 に、旧来のナラティブが延命し続けている点が挙げられる。新型コロナウイルスやウクライナ戦争に端を発する陰謀論や反権威的なナラティブは、一度否定されても形を変えて生き残り、別の文脈で再利用されている。例えば反ワクチン運動やディープステート陰謀論は、パンデミック後も国際機関の新条約や新たな有事を標的に置き換えながら、その主張が広がり続けている。こうした拡散状況は自然発生的な現象だけではなく、中国やロシアといった安全保障上の懸念国が戦略的なナラティブを拡散することで、自国に有利な認知形成を目指す認知戦の広がりが背景にあることは留意すべきである。総じて 2024 年は、AI と SNS が生み出す拡散構造の中で戦略的ナラティブが延命することで、偽・誤情報が根強く社会に拡散し続けた一年だったともいえよう。

(2) 今後の見通し

2025 年は 2024 年に続き、世界各国で重要な選挙や国際政治行事が実施される予定となっており、それらに絡んだ偽情報の更なる増加が懸念される。具体的には、ノルウェー議会選挙（2025 年 9 月実施予定）、チェコ議会選挙（2025 年 10 月実施予定）、アイルランド大統領選挙（2025 年 10 月実施予定）、シンガポール総選挙（2025 年 11 月実施予定）等、主要各国の国政選挙や、太平洋戦争終結 80 年に伴う各国記念日、G20 サミット等の民主主義プロセスや外交イベントへの介入を狙った情報工作が警戒される。ドイツでは、既に 2025 年 2 月の選挙直前にロシア系グループが関与したと見られる「極右政党への投票用紙が紛失・破棄された」という偽動画が出回り当局が注意喚起する事態が起きた※248。ロシアはこれまでも紛争や国際会議の度に新たな偽情報を投入してきており（「2.2.4 (2) ロシア・ウクライナ戦争」で紹介した武器横流し説等）、ウクライナ復興会議でも「ハイブリッド型サイバー攻撃」による攻勢が懸念される。また、新たな国際情勢の火種として、インド・パキスタン関係が不安定化しており、両国に関連した偽情報の流布が増えていくことが想定される。翻って日本では、国政選挙等で、候補者に関するデマや国外勢力による情報操作が懸念されるところであり、十分な警戒が必要だろう。国際的な場においても日本国内においても、外国からの情報操作と国内の適正な情報環境の維持の双方に注意を払い、適切な対策が求められる。

※1 Y. LeCun et al.：Backpropagation Applied to Handwritten Zip Code Recognition https://doi.org/10.1162/neco.1989.1.4.541〔2025/6/18 確認〕
ニューラルネットを用いない方法での郵便番号の機械認識はもっと早い段階で実用化されている。例えば日本では 1967 年に世界初の手書き文字読み取り試作機（TR-2 型）が完成している。
郵政博物館：最初の郵便番号自動読取区分機 https://www.postalmuseum.jp/column/collection/post_27.html〔2025/6/18 確認〕
※2 電子情報通信学会：「知識ベース」S3 群―3 編―3 章 機械学習 https://ieice-hbkb.org/files/ad_base/view_pdf.html?p=/files/S3/S3gun_03hen_03.pdf#page=1〔2025/6/18 確認〕
※3 Paul Graham：「スパムへの対策 --- A Plan for Spam」（和訳）https://web.archive.org/web/20110724020751/http://practical-scheme.net/trans/spam-j.html〔2025/6/18 確認〕
※4 岡本 一志・藤井 流華：「協調フィルタリング入門」知能と情報（日本知能情報ファジィ学会誌）Vol.31, No.1, pp.5－9（2019） https://www.jstage.jst.go.jp/article/jsoft/31/1/31_5/_pdf〔2025/6/18 確認〕
※5 人工知能学会監修：「深層学習 — Deep Learning」 https://jsai-deeplearning.github.io/support/dlspecial.html〔2025/6/18 確認〕
※6 Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun：Deep Residual Learning for Image Recognition https://arxiv.org/abs/1512.03385〔2025/6/18 確認〕
WIRED：黒 37 手と白 78 手：AlphaGo とイ・セドルが再定義した「未来」 https://wired.jp/special/2016/alphago-vs-sedol/〔2025/6/18 確認〕
※7 総務省、経済産業省：AI 事業者ガイドライン（第 1.1 版） https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20250328_1.pdf〔2025/6/18 確認〕
※8 CNBC：On ChatGPT's one-year anniversary, it has more than 1.7 billion users—here's what it may do next(2023/11/30) https://www.cnbc.com/2023/11/30/chatgpts-one-year-anniversary-how-the-viral-ai-chatbot-has-changed.html〔2025/6/18 確認〕
※9 European Commission：AI Act https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai〔2025/6/18 確認〕
※10 GOV.UK：Frontier AI: capabilities and risks – discussion paper https://www.gov.uk/government/publications/frontier-ai-capabilities-and-risks-discussion-paper/frontier-ai-capabilities-and-risks-discussion-paper〔2025/6/18 確認〕
※11 TIME：The Billion-Dollar Price Tag of Building AI https://time.com/6984292/cost-artificial-intelligence-compute-epoch-report/〔2025/6/18 確認〕
※12 TIME：The AI Arms Race Is Changing Everything https://time.com/6255952/ai-impact-chatgpt-microsoft-google/〔2025/6/18 確認〕
※13 Jared Kaplan et al.：Scaling Laws for Neural Language Models https://doi.org/10.48550/arXiv.2001.08361〔2025/6/18 確認〕
Tom Henighan et al.：Scaling Laws for Autoregressive Generative Modeling https://doi.org/10.48550/arXiv.2010.14701〔2025/6/18 確認〕
※14 GOV.UK：International Scientific Report on the Safety of Advanced AI: interim report https://www.gov.uk/government/publications/international-scientific-report-on-the-safety-of-advanced-ai〔2025/6/18 確認〕
※15 GOV.UK：International AI Safety Report 2025 https://www.gov.uk/government/publications/international-ai-safety-report-2025〔2025/6/18 確認〕

※ 16 GAO：GAO-20-379SP Science & Tech Spotlight: Deepfakes https://www.gao.gov/products/gao-20-379sp〔2025/6/18 確認〕
※ 17 FBI：Alert Number I-060523-PSA Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes https://www.ic3.gov/PSA/2023/PSA230605〔2025/6/18 確認〕
※ 18 Ofcom：A deep dive into deepfakes that demean, defraud and disinform https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/deepfakes-demean-defraud-disinform/?language=en〔2025/6/18 確認〕
※ 19 Tvesha Sippy et al.：Behind the Deepfake: 8% Create; 90% Concerned. Surveying public exposure to and perceptions of deepfakes in the UK https://doi.org/10.48550/arXiv.2407.05529〔2025/6/18 確認〕
※ 20 NHK：卒業アルバムの同級生を裸に 子どもも加害者?画像加工の実態 https://www3.nhk.or.jp/news/html/20241218/k10014666221000.html〔2025/6/18 確認〕
※ 21 Takamichi Saito：影響力工作についての簡単な整理を通して、「Industrialized Disinformation ー 2020 Global Inventory of Organized Social Media Manipulation」を読み解く https://saitolab-org.medium.com/影響力工作についての簡単な整理を通して-industrialized-disinformation- ー -2020-global-inventory-of-organized-social-319d30d5f377〔2025/6/18 確認〕
※ 22 FNN プライムオンライン：ディープフェイク悪用“ゼレンスキー大統領”が国民に降伏呼びかけるニセ動画 見分ける自信ありますか? https://www.fnn.jp/articles/-/333829〔2025/6/18 確認〕
※ 23 NHK：オープン AI “ロシアなど拠点のグループ 生成 AI で世論操作” https://www3.nhk.or.jp/news/html/20240531/k10014466761000.html〔2025/3/11 確認〕
※ 24 U.S. Department of Justice：Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence〔2025/6/18 確認〕
※ 25 OpenAI 社：Disrupting deceptive uses of AI by covert influence operations https://web.archive.org/web/20240530173817/https://openai.com/index/disrupting-deceptive-uses-of-ai-by-covert-influence-operations/〔2025/6/18 確認〕
※ 26 Michael Kouremetis et al：What Lies Beneath the Surface? Evaluating LLMs for Offensive Cyber Capabilities through Prompting, Simulation & Emulation https://www.blackhat.com/us-24/briefings/schedule/#what-lies-beneath-the-surface-evaluating-llms-for-offensive-cyber-capabilities-through-prompting-simulation-38-emulation-40685〔2025/6/18 確認〕
※ 27 Microsoft Threat Intelligence：Staying ahead of threat actors in the age of AI https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/〔2025/6/18 確認〕
OpenAI 社：Disrupting malicious uses of AI by state-affiliated threat actors https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors/〔2025/6/18 確認〕
※ 28 NCSC：The near-term impact of AI on the cyber threat https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat〔2025/6/18 確認〕
※ 29 読売新聞オンライン：中高生の生成AI悪用事件、「指示役」中3男子「本人確認が甘い楽天狙った」…カード不正利用も判明 https://www.yomiuri.co.jp/national/20250227-OYT1T50322/〔2025/6/18 確認〕
※ 30 The Verge：AI suggested 40,000 new possible chemical weapons in just six hours https://www.theverge.com/2022/3/17/22983197/ai-new-possible-chemical-weapons-generative-models-vx〔2025/6/18 確認〕
※ 31 Bloomberg：AI-Made Bioweapons Are Washington's Latest Security Obsession https://www.bloomberg.com/news/features/2024-08-02/national-security-threat-from-ai-made-bioweapons-grips-us-government〔2025/6/18 確認〕
※ 32 Harvard Sussex Program：Artificial Intelligence Technologies and Chemical and Biological Weapons: A Chronology of Events (2000-Present) http://hsp.sussex.ac.uk/new/_uploads/publications/AI_and_CBW_Chronology_January_2025.pdf〔2025/6/18 確認〕
※ 33 原文では a simulated version of the Uniform Bar Examination と表記。
※ 34 OpenAI 社：GPT-4 Technical Report https://doi.org/10.48550/arXiv.2303.08774〔2025/6/18 確認〕
※ 35 Tiffany H. Kung et al.：Performance of ChatGPT on USMLE: Potential for AI-assisted medical education using large language models https://doi.org/10.1371/journal.pdig.0000198〔2025/6/18 確認〕
※ 36 Eric Martínez：Re-evaluating GPT-4's bar exam performance https://doi.org/10.1007/s10506-024-09396-9〔2025/6/18 確認〕
※ 37 Jesutofunmi A. Omiye et al：Large language models propagate race-based medicine https://doi.org/10.1038/s41746-023-00939-z〔2025/6/18 確認〕
※ 38 日本経済新聞：ChatGPT で資料作成、実在しない判例引用 米国の弁護士 https://www.nikkei.com/article/DGXZQOGN30E450Q3A530C2000000/〔2025/6/18 確認〕
※ 39 NHK：虐待疑われる子どもの保護判定 AI の導入見送りに こども家庭庁 https://www3.nhk.or.jp/news/html/20250303/k10014738301000.html〔2025/6/18 確認〕
※ 40 Reuters：焦点：アマゾンがAI採用打ち切り、「女性差別」の欠陥露呈で https://jp.reuters.com/article/amazon-jobs-ai-analysis-idJPKCN1ML0DN/〔2025/6/18 確認〕
※ 41 Joy Buolamwini & Timnit Gebru：Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification https://proceedings.mlr.press/v81/buolamwini18a.html〔2025/6/18 確認〕
※ 42 Julia Dressel & Hany Farid：The accuracy, fairness, and limits of predicting recidivism https://doi.org/10.1126/sciadv.aao5580〔2025/6/18 確認〕
※ 43 Marc Cheong et al：Investigating Gender and Racial Biases in DALL-E Mini Images https://doi.org/10.1145/3649883〔2025/6/18 確認〕
※ 44 UNESCO：CI/DIT/2024/GP/01 Challenging systematic prejudices: an investigation into bias against women and girls in large language models https://unesdoc.unesco.org/ark:/48223/pf0000388971〔2025/6/18 確認〕
※ 45 Chris Lu et al.：The AI Scientist: Towards Fully Automated Open-Ended Scientific Discovery https://doi.org/10.48550/arXiv.2408.06292〔2025/6/18 確認〕
※ 46 Sakana AI 株式会社：AI CUDA Engineer：エージェントによる CUDA カーネルの発見、最適化、生成 https://sakana.ai/ai-cuda-engineer-jp/〔2025/6/18 確認〕
※ 47 TechCrunch：Sakana walks back claims that its AI can dramatically speed up model training https://techcrunch.com/2025/02/21/sakana-walks-back-claims-that-its-ai-can-dramatically-speed-up-model-training/〔2025/6/18 確認〕
※ 48 ITmedia：OpenAI と Apollo Research、「o1」は自分の目的のために嘘をつくと報告 https://www.itmedia.co.jp/news/articles/2412/06/news169.html〔2025/6/18 確認〕
※ 49 Kevin Zheyuan Cui et al.：The Productivity Effects of Generative AI: Evidence from a Field Experiment with GitHub Copilot https://doi.org/10.21428/e4baedd9.3ad85f1c〔2025/6/18 確認〕
※ 50 Shakked Noy & Whitney Zhang：Experimental evidence on the productivity effects of generative artificial intelligence https://doi.org/10.1126/science.adh2586〔2025/6/18 確認〕
※ 51 bloomberry：The jobs being replaced by AI – an analysis of 5M freelancing jobs https://bloomberry.com/i-analyzed-5m-freelancing-jobs-to-see-what-jobs-are-being-replaced-by-ai/〔2025/6/18 確認〕
※ 52 The Econometric Society：Tasks, Automation, and the Rise in U.S. Wage Inequality https://www.econometricsociety.org/publications/econometrica/2022/09/01/Tasks-Automation-and-the-Rise-in-US-Wage-Inequality〔2025/6/18 確認〕
※ 53 Epoch AI：How Much Does It Cost to Train Frontier AI Models? https://epoch.ai/blog/how-much-does-it-cost-to-train-frontier-ai-models〔2025/6/18 確認〕
※ 54 Google 社：Nebraska, USA – Google Data Center Location https://datacenters.google/locations/nebraska/〔2025/6/18 確認〕
※ 55 Governor of Missouri：Governor Parson Announces Google's Selection of Kansas City for New Data Center https://web.archive.org/web/20240330150938/https://governor.mo.gov/press-releases/archive/governor-parson-announces-googles-selection-kansas-city-new-data-center〔2025/6/18 確認〕
※ 56 Post by Richland Parish Data Center https://www.facebook.com/RichlandParishDataCenter/posts/pfbid0u2WXqnJgziQZFEvZbz1qg1Pgbw3xLSkaFGJ26xgNqaLp4YojFWsJqHbvTy8fKJDn〔2025/3/11 確認〕
※ 57 Statista：Amazon and Microsoft Stay Ahead in Global Cloud

Market https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/〔2025/6/18 確認〕
※ 58 JPNIC：SPOF とは https://www.nic.ad.jp/ja/basics/terms/spof.html〔2025/6/18 確認〕
※ 59 Jens Malmodin et al.：ICT Sector Electricity Consumption and Greenhouse Gas Emissions – 2020 Outcome https://dx.doi.org/10.2139/ssrn.4424264〔2025/6/18 確認〕
※ 60 IEA:Electricity 2024 https://www.iea.org/reports/electricity-2024〔2025/6/18 確認〕
※ 61 IEA：World Energy Outlook 2024 https://www.iea.org/reports/world-energy-outlook-2024〔2025/6/18 確認〕
※ 62 Google 社：2024 Environmental Report https://sustainability.google/reports/google-2024-environmental-report/〔2025/6/18 確認〕
※ 63 NHK：グーグル 原発から電力調達へ AI 活用で電力需要高まる https://www3.nhk.or.jp/news/html/20241015/k10014610011000.html〔2025/6/18 確認〕
※ 64 Constellation：Constellation to Launch Crane Clean Energy Center, Restoring Jobs and Carbon-Free Power to The Grid https://www.constellationenergy.com/newsroom/2024/Constellation-to-Launch-Crane-Clean-Energy-Center-Restoring-Jobs-and-Carbon-Free-Power-to-The-Grid.html〔2025/6/18 確認〕
※ 65 NHK:エネルギー基本計画決定 “再エネ最大電源に 原子力も活用” https://www3.nhk.or.jp/news/html/20250218/k10014725571000.html〔2025/6/18 確認〕
※ 66 Nicholas Carlini et al.：Extracting Training Data from Large Language Models https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting〔2025/6/18 確認〕
※ 67 Office of the Privacy Commissioner of Canada：Joint statement on data scraping and the protection of privacy https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2023/js-dc_20230824/〔2025/6/18 確認〕
※ 68 McKinsey&Company：Generative AI in healthcare: Adoption trends and what's next https://www.mckinsey.com/industries/healthcare/our-insights/generative-ai-in-healthcare-adoption-trends-and-whats-next〔2025/6/18 確認〕
※ 69 Global Market Insights：AI In Video Surveillance Market Size https://www.gminsights.com/industry-analysis/ai-in-video-surveillance-market〔2025/6/18 確認〕
※ 70 Federal Trade Commission：FTC Staff Report Finds Large Social Media and Video Streaming Companies Have Engaged in Vast Surveillance of Users with Lax Privacy Controls and Inadequate Safeguards for Kids and Teens https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance〔2025/6/18 確認〕
※ 71 Federal Trade Commission：FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users〔2025/6/18 確認〕
※ 72 PC Watch：写真素材サイト大手が Stable Diffusion を提訴。「1,200 万枚以上の写真を無断で複製」 https://pc.watch.impress.co.jp/docs/news/1476475.html〔2025/6/18 確認〕
※ 73 BBC NEWS JAPAN：米紙ニューヨーク・タイムズがオープン AI とマイクロソフトを提訴 著作権侵害で https://www.bbc.com/japanese/67831445〔2025/6/18 確認〕
※ 74 Richard Fletcher：How many news websites block AI crawlers? https://reutersinstitute.politics.ox.ac.uk/how-many-news-websites-block-ai-crawlers〔2025/6/18 確認〕
※ 75 GOV.UK：AI Safety Institute: overview https://www.gov.uk/government/publications/ai-safety-institute-overview〔2025/6/18 確認〕
※ 76 日本 AISI：AI セーフティ年次レポート 2024 https://aisi.go.jp/assets/pdf/j-aisi_report_2024_ja.pdf〔2025/7/15 確認〕
※ 77 足立浩規他：［サーベイ論文］Adversarial Training http://mprg.jp/data/MPRG/F_group/F20220310_adachi.pdf〔2025/6/18 確認〕
※ 78 リスクマネジメントの考え方は EU AI Act の Article 9: Risk Management System で簡潔に整理されている。
EU Artificial Intelligence Act：Article 9: Risk Management System https://artificialintelligenceact.eu/article/9/〔2025/6/18 確認〕
※ 79 JIS Q 31000:2019 等を念頭に説明を翻案している。
※ 80 JIS Q 31010 が同規格の邦訳となっている。
※ 81 一般社団法人日本品質管理学会 AI 品質アジャイルガバナンス研究会著 編「AI リスクアセスメント ガイドブック」
※ 82 NIST：AI Risk Management Framework https://airc.nist.gov/airmf-resources/airmf/〔2025/6/18 確認〕
上記の Web サイトは関連資料へのリンクも集約したポータルサイトとなっている。AI RMF 1.0 版へのリンクは次のとおり。NIST：Artificial Intelligence Risk Management Framework (AI RMF 1.0) https://doi.org/10.6028/NIST.AI.100-1〔2025/6/18 確認〕
※ 83 NIST：NIST AI 600-1 Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile https://doi.org/10.6028/NIST.AI.600-1〔2025/6/18 確認〕
※ 84 経済産業省：AI 事業者ガイドライン https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20240419_report.html〔2025/6/18 確認〕
※ 85 日本 AISI：AI 事業者ガイドラインと米国 NIST AI リスクマネジメントフレームワーク（RMF）のクロスウォーク2 https://aisi.go.jp/output/output_information/240918_1/〔2025/6/18 確認〕
※ 86 AI モデル：ディープニューラルネット（DNN）を前提にした場合、DNN は線形写像と非線形写像（活性化関数）の組を 1 層としてこれを多層化した構造となっており、各層を定義するパラメーター式と、層と層の間のつながりを記述したデータをまとめたものを一般に AI モデルと呼ぶ。なお、AI 事業者ガイドライン1. 1版では、AI システムを「活用の過程を通じて様々なレベルの自律性をもって動作し学習する機能を有するソフトウェアを要素として含むシステム」、AI モデルを「AI システムに含まれ、学習データを用いた機械学習によって得られるモデルで、入力データに応じた予測結果を生成する」ものと定義している。
※ 87 日本 AISI：AI セーフティに関する評価観点ガイド（第 1.01 版） https://aisi.go.jp/effort/effort_framework/guide_to_evaluation_perspective_on_ai_safety/〔2025/6/18 確認〕
※ 88 GAO：GAO-24-106946 Artificial Intelligence: Generative AI Technologies and Their Commercial Applications https://www.gao.gov/products/gao-24-106946〔2025/6/18 確認〕
※ 89 Yupeng Chang et al.：A Survey on Evaluation of Large Language Models https://doi.org/10.48550/arXiv.2307.03109〔2025/6/18 確認〕
※ 90 Richard Harang：Practical LLM Security: Takeaways From a Year in the Trenches https://www.blackhat.com/us-24/briefings/schedule/#practical-llm-security-takeaways-from-a-year-in-the-trenches-39468〔2025/6/18 確認〕
※ 91 「AI セーフティに関するレッドチーミング手法ガイド」ではレッドチーミングを「攻撃者がどのように AI システムを攻撃するかの観点で、AI セーフティへの対応体制及び対策の有効性を確認する評価手法」と定義している。
※ 92 https://aisi.go.jp/effort/effort_framework/guide_to_red_teaming_methodology_on_ai_safety/〔2025/6/18 確認〕
※ 93 NIST：NIST AI 100-2 e2023 Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations https://doi.org/10.6028/NIST.AI.100-2e2023〔2025/6/18 確認〕
AI プロダクト品質保証コンソーシアム：AI プロダクト品質保証ガイドライン (QA4AI Guidelines) https://www.qa4ai.jp/download〔2025/6/18 確認〕
国立研究開発法人産業技術総合研究所：機械学習品質マネジメントガイドライン 第 4 版 https://www.digiarc.aist.go.jp/publication/aiqm/guideline-rev4.html〔2025/6/18 確認〕
※ 94 日本 AISI：データ品質マネジメントガイドブック（ドラフト版） https://aisi.go.jp/effort/effort_information/250207_2/〔2025/6/18 確認〕
※ 95 Ada Lovelace Institute：Under the radar? https://www.adalovelaceinstitute.org/report/under-the-radar/〔2025/6/18 確認〕
※ 96 2025 年 2 月に AI Security Institute へと改称した。
※ 97 英国 AISI：Inspect https://inspect.ai-safety-institute.org.uk/〔2025/6/18 確認〕
※ 98 英国 AISI：Advanced AI evaluations at AISI: May update https://www.aisi.gov.uk/work/advanced-ai-evaluations-may-update〔2025/6/18 確認〕
英国 AISI：Early Insights from Developing Question-Answer Evaluations for Frontier AI https://www.aisi.gov.uk/work/early-insights-from-developing-question-answer-evaluations-for-frontier-ai〔2025/6/18 確認〕
英国 AISI：Early lessons from evaluating frontier AI systems https://www.aisi.gov.uk/work/early-lessons-from-evaluating-frontier-ai-systems〔2025/6/18 確認〕
英国 AISI：Pre-Deployment Evaluation of Anthropic's Upgraded Claude 3.5 Sonnet https://www.aisi.gov.uk/work/pre-deployment-evaluation-of-anthropics-upgraded-claude-3-5-sonnet〔2025/6/18 確認〕

英国 AISI：Pre-Deployment Evaluation of OpenAI's o1 Model https://www.aisi.gov.uk/work/pre-deployment-evaluation-of-openais-o1-model〔2025/6/18 確認〕
※ 99 UNESCO：Recommendation on the Ethics of Artificial Intelligence https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence〔2025/6/18 確認〕
※ 100 内閣府 科学技術・イノベーション推進事務局：「米国の AI 権利章典（AI Bill of Rights）について https://www8.cao.go.jp/cstp/ai/ningen/r4_2kai/siryo3.pdf〔2025/6/18 確認〕
※ 101 Federal Register：Executive Order 14110 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〔2025/6/18 確認〕
※ 102 国連：Governing AI for Humanity https://doi.org/10.18356/9789211067873〔2025/6/18 確認〕
※ 103 The White House：FACT SHEET: Vice President Harris Announces New U.S. Initiatives to Advance the Safe and Responsible Use of Artificial Intelligence https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/11/01/fact-sheet-vice-president-harris-announces-new-u-s-initiatives-to-advance-the-safe-and-responsible-use-of-artificial-intelligence/〔2025/6/18 確認〕
※ 104 経済産業省：AI セーフティ・インスティテュートを設立しました https://www.meti.go.jp/press/2023/02/20240214002/20240214002.html〔2025/6/18 確認〕
※ 105 Singapore AI Safety Institute:https://sgaisi.sg/〔2025/6/18 確認〕
※ 106 Canadian Artificial Intelligence Safety Institute：https://ised-isde.canada.ca/site/ised/en/canadian-artificial-intelligence-safety-institute〔2025/6/18 確認〕
※ 107 韓国 AISI：AI Safety Institute https://www.aisi.re.kr/eng〔2025/6/18 確認〕
※ 108 Ministère de l'Économie des Finances et de la Souveraineté industrielle et numérique：La France se dote d'un Institut national pour l'évaluation et la sécurité de l'intelligence artificielle (INESIA) https://www.economie.gouv.fr/actualites/la-france-se-dote-dun-institut-national-pour-levaluation-et-la-securite-de-lintelligence〔2025/6/18 確認〕
※ 109 European Commission：European AI Office https://digital-strategy.ec.europa.eu/en/policies/ai-office〔2025/6/18 確認〕
※ 110 JETRO：米商務省、AI 安全研究所コンソーシアムの設置発表 https://www.jetro.go.jp/biznews/2024/02/eb4c5eff3da218bd.html〔2025/6/18 確認〕
※ 111 The White House：FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/〔2025/6/18 確認〕
※ 112 GOV.UK：AI Safety Summit 2023 https://www.gov.uk/government/topical-events/ai-safety-summit-2023〔2025/6/18 確認〕
※ 113 GOV.UK：AI Safety Summit 2023: The Bletchley Declaration https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration〔2025/6/18 確認〕
※ 114 GOV.UK：AI Seoul Summit 2024 https://www.gov.uk/government/topical-events/ai-seoul-summit-2024〔2025/6/18 確認〕
※ 115 GOV.UK：Seoul Declaration for safe, innovative and inclusive AI: AI Seoul Summit 2024 https://www.gov.uk/government/publications/seoul-declaration-for-safe-innovative-and-inclusive-ai-ai-seoul-summit-2024〔2025/6/18 確認〕
※ 116 GOV.UK：Frontier AI Safety Commitments, AI Seoul Summit 2024 https://www.gov.uk/government/publications/frontier-ai-safety-commitments-ai-seoul-summit-2024〔2025/6/18 確認〕
※ 117 https://aisi.go.jp/effort/effort_information/250207_1/〔2025/6/18 確認〕
※ 118 The American Presidency Project Republican Party：2024 Republican Party Platform https://www.presidency.ucsb.edu/documents/2024-republican-party-platform〔2025/6/18 確認〕
※ 119 Federal Register：Executive Order 14148 Initial Rescissions of Harmful Executive Orders and Actions https://www.federalregister.gov/documents/2025/01/28/2025-01901/initial-rescissions-of-harmful-executive-orders-and-actions〔2025/6/18 確認〕
※ 120 Federal Register：Executive Order 14179 Removing Barriers to American Leadership in Artificial Intelligence https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence〔2025/6/18 確認〕
※ 121 GOV.UK：AI Opportunities Action Plan https://www.gov.uk/government/publications/ai-opportunities-action-plan〔2025/6/18 確認〕
※ 122 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〔2025/6/18 確認〕
※ 123 この動きの直前に、AI が生成した子供の性的虐待画像を取り締まる法案が国会に提出されている。
BBC NEWS JAPAN：イギリス、AI 生成の子ども性虐待画像を取り締まる法案を発表 https://www.bbc.com/japanese/articles/ceve7dk8e38o〔2025/6/18 確認〕
※ 124 Artificial Intelligence Action Summit：https://www.elysee.fr/en/sommet-pour-l-action-sur-l-ia〔2025/6/18 確認〕
※ 125 elysee.fr：Statement on Inclusive and Sustainable Artificial Intelligence for People and the Planet https://www.elysee.fr/en/emmanuel-macron/2025/02/11/statement-on-inclusive-and-sustainable-artificial-intelligence-for-people-and-the-planet〔2025/6/18 確認〕
※ 126 BBC NEWS JAPAN：AI アクションサミット、英米は共同声明に署名せず https://www.bbc.com/japanese/articles/czx8ze7lx9no〔2025/6/18 確認〕
※ 127 GOV.UK：Frontier AI: capabilities and risks – discussion paper https://www.gov.uk/government/publications/frontier-ai-capabilities-and-risks-discussion-paper〔2025/6/18 確認〕
GOV.UK：International Scientific Report on the Safety of Advanced AI: interim report https://www.gov.uk/government/publications/international-scientific-report-on-the-safety-of-advanced-ai〔2025/6/18 確認〕
GOV.UK：International AI Safety Report 2025 https://www.gov.uk/government/publications/international-ai-safety-report-2025〔2025/6/18 確認〕
※ 128 SlashNext, Inc.：SlashNext's 2023 State of Phishing Report Reveals a 1,265% Increase in Phishing Emails Since the Launch of ChatGPT in November 2022, Signaling a New Era of Cybercrime Fueled by Generative AI https://slashnext.com/press-release/slashnexts-2023-state-of-phishing-report-reveals-a-1265-increase-in-phishing-emails-since-the-launch-of-chatgpt-in-november-2022-signaling-a-new-era-of-cybercrime-fueled-by-generative-ai/〔2025/6/18 確認〕
※ 129 日経クロステック：ガードレールなしの生成 AI が相次ぎ出現、サイバー犯罪者「御用達」の使い道とは https://xtech.nikkei.com/atcl/nxt/column/18/00676/080600141/〔2025/6/18 確認〕
※ 130 善意の開発・運用者が作った AI システムの狭義の AI セキュリティを高めるという意味ではこの限りではないが、最初から悪意を持ってそのための AI を開発することを AI ガバナンスで防ぐことはできない。
※ 131 NIST Glossary：Cyber Threat https://csrc.nist.gov/glossary/term/cyber_threat〔2025/6/18 確認〕
※ 132 ENISA は Threat Landscape という脅威サーベイ報告を毎年発刊している。また、中長期の脅威傾向の予測も行っている。詳しくは次の Web サイトを参照。
ENISA：Threat Landscape https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape〔2025/6/18 確認〕
※ 133 Centre for Emerging Technology and Security：Research and Publications https://cetas.turing.ac.uk/research-and-publications〔2025/6/18 確認〕
※ 134 ITmedia：生成 AI の弱点が相次ぎ発覚 ChatGPT や Gemini がサイバー攻撃の標的に 情報流出や不正操作の恐れも https://www.itmedia.co.jp/news/articles/2403/22/news069.html〔2025/6/18 確認〕
※ 135 Security NEXT：機械学習フレームワーク「PyTorch」に不正プログラム混入のおそれ https://www.security-next.com/142623〔2025/6/18 確認〕
※ 136 Wiz：Wiz Research finds architecture risks that may compromise AI-as-a-Service providers and consequently risk customer data; works with Hugging Face on mitigations https://www.wiz.io/blog/wiz-and-hugging-face-address-risks-to-ai-infrastructure〔2025/6/18 確認〕
※ 137 ITmedia：DeepSeek、チャット履歴含む 100 万件超のログが外

部から閲覧できた可能性　米セキュリティ企業が指摘　https://www.itmedia.co.jp/news/articles/2501/30/news173.html〔2025/6/18確認〕
※ 138 SlashNext, Inc.：The State of Phishing 2024 Report　https://slashnext.com/the-state-of-phishing-2024/〔2025/6/18確認〕
※ 139 日本経済新聞：［FT］テレビ会議、AI技術でなりすまし　英企業40億円被害　https://www.nikkei.com/article/DGXZQOCB056460V00C24A6000000/〔2025/6/18確認〕
※ 140 NHK：AIが詐欺師に!? チャットサービス悪用の新手口 被害も　https://www3.nhk.or.jp/news/special/tag-digital_deceive/article/33_01.html〔2025/6/18確認〕
※ 141 BBC NEWS JAPAN：ルーマニアの憲法裁判所、大統領選第1回投票を無効と判断　勝利候補への影響工作が明るみに　https://www.bbc.com/japanese/articles/cg4zzk1d1nxo〔2025/6/18確認〕
※ 142 JETRO：ルーマニア大統領選、ロシア介入やSNS不正操作で憲法裁判所が無効判断　https://www.jetro.go.jp/biznews/2024/12/5539b706af134586.html〔2025/6/18確認〕
Președintele României：Analiza unor riscuri la adresa securității nationale generate de actiunile unor actori cibernetici statali si non-statali asupra unor infrastructuri IT&C, suport pentrú procesul electoral　https://www.presidency.ro/files/userfiles/Documente%20CSAT/Document%20CSAT%20SIE.pdf〔2025/6/18確認〕
※ 143 Reuters：アングル：ルーマニア大統領選、親ロ極右候補躍進でTikTokに疑惑の目　https://jp.reuters.com/economy/2RCUJT3UGRLBFFP62GUM4KCQFE-2024-12-04/〔2025/6/18確認〕
※ 144 読売新聞オンライン：フォロワー5万人のインフルエンサー「報酬もらった」…ルーマニア大統領選巡り「関与を後悔」　https://www.yomiuri.co.jp/world/20241209-OYT1T50188/〔2025/6/18確認〕
※ 145 Centre for Emerging Technology and Security：Evaluating Malicious Generative AI Capabilities　https://cetas.turing.ac.uk/publications/evaluating-malicious-generative-ai-capabilities〔2025/6/18確認〕
※ 146 NIST SP 800-218：Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities　https://doi.org/10.6028/NIST.SP.800-218〔2025/6/18確認〕
※ 147 NIST SP 800-218A：Secure Software Development Practices for Generative AI and Dual-Use Foundation Models: An SSDF Community Profile　https://doi.org/10.6028/NIST.SP.800-218A〔2025/6/18確認〕
※ 148 NCSC：Machine learning principles　https://www.ncsc.gov.uk/collection/machine-learning-principles〔2025/6/18確認〕
※ 149 Joint Cybersecurity Information（U/OO/143395-24）：Deploying AI Systems Security　https://media.defense.gov/2024/apr/15/2003439257/-1/-1/0/csi-deploying-ai-systems-securely.pdf〔2025/6/18確認〕
※ 150 CSET：Securing Critical Infrastructure in the Age of AI　https://cset.georgetown.edu/publication/securing-critical-infrastructure-in-the-age-of-ai/〔2025/6/18確認〕
※ 151 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〔2025/7/16確認〕
※ 152 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、「新領域安全保障」、p.185
※ 153 https://rm.coe.int/information-disorder-toward-an-interdisciplinaryframework-for-researc/168076277c〔2025/7/16確認〕
※ 154 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〔2025/7/16確認〕
※ 155 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〔2025/7/16確認〕
※ 156 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_JP_2024.pdf〔2025/7/16確認〕
※ 157 UNESCO：Survey on the impact of online disinformation and hate speech　https://www.unesco.org/sites/default/files/medias/fichiers/2023/11/unesco_ipsos_survey.pdf〔2025/7/16確認〕
※ 158 NHK放送文化研究所：シリーズ「ロイター・デジタルニュースリポート2024」(3)～偽情報・誤情報に対する意識は～【研究員の視点】#552　https://www.nhk.or.jp/bunken-blog/200/671694.html〔2025/7/16確認〕
※ 159 Tobias Bunde, Sophie Eisentraut, and Leonard Schütte, “Munich Security Index 2024,” in: Tobias Bunde/Sophie Eisentraut/Leonard Schütte (eds.), Munich Security Report 2024: Lose-Lose?, Munich: Munich Security Conference, February 2024, 26–45, doi.org/10.47342/BMQK9457, 32–33.
※ 160 Munich Security Conference：AI-pocalypse Now?　https://securityconference.org/en/publications/analyses/ai-pocalypse-disinformation-super-election-year/#:~:text=AI,a%20global%20scale%E2%80%9D%20in%202024〔2025/7/16確認〕
※ 161 U.S. NAVAL INSTITUTE：Future Warfare: The Rise of Hybrid Wars　https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars〔2025/7/16確認〕
※ 162 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
※ 163 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〔2025/7/16確認〕
※ 164 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〔2025/7/16確認〕
※ 165 Hybrid CoE：Hybrid threats as a concept　https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/〔2025/7/16確認〕
※ 166 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
※ 167 Meta社「Q3 2024 ADVERSARIAL THREAT REPORT『Integrity Reports, Third Quarter 2024』（https://transparency.meta.com/ja-jp/integrity-reports-q3-2024/〔2025/7/16確認〕）において「Adversarial Threat Report」の「You can read the full report here.」の「here」をクリックすると表示される。
※ 168 Google LLC：TAG Bulletin: Q2 2024　https://blog.google/threat-analysis-group/tag-bulletin-q2-2024〔2025/7/16確認〕
※ 169 OpenAI社：Influence and cyber operations: an update　https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf〔2025/7/16確認〕
※ 170 OpenAI社：Disrupting a Covert Iranian Influence Operation.　https://openai.com/index/disrupting-a-covert-iranian-influence-operation/〔2025/7/16確認〕
OpenAI社：Disrupting malicious uses of our models: an update February 2025　https://cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf〔2025/7/16確認〕
※ 171 BBC NEWS JAPAN：【解説】イギリスの騒乱はなぜ起きたのか　https://www.bbc.com/japanese/articles/cp8nl49lpypo〔2025/7/16確認〕
※ 172 NPR：UK's worst riots in years were incited by online disinformation about asylum seekers　https://www.npr.org/2024/08/10/nx-s1-5066896/uks-worst-riots-in-years-were-incited-by-online-disinformation-about-asylum-seekers〔2025/7/16確認〕
※ 173 ODNI：100 Days Until Election 2024　https://www.dni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240729.pdf〔2025/7/16確認〕
※ 174 ODNI：Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts　https://www.odni.gov/index.php/newsroom/press-releases/press-releases-2024/4014-pr-28-24〔2025/7/16確認〕
※ 175 FDD：America Resilient in the Face of Aggressive Foreign Malign Influence Targeting the 2024 U.S. Elections　https://www.fdd.org/analysis/2024/12/18/america-resilient-in-the-face-of-aggressive-foreign-malign-influence-targeting-the-2024-u-s-elections/〔2025/7/16確認〕
※ 176 U.S. Department of the Treasury：Treasury Sanctions Entities in Iran and Russia That Attempted to Interfere in the U.S. 2024 Election　https://home.treasury.gov/news/press-releases/jy2766〔2025/7/16確認〕
※ 177 NPR：China is pushing divisive political messages online using fake U.S. voters　https://www.npr.org/2024/09/03/nx-s1-5096151/china-tiktok-x-fake-voters-influence-campaign〔2025/7/16確認〕

※ 178 U.S. Department of Justice：Three IRGC Cyber Actors Indicted for 'Hack-and-Leak' Operation Designed to Influence the 2024 U.S. Presidential Election https://www.justice.gov/archives/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us〔2025/7/16 確認〕
※ 179 NPR：Foreign influence efforts reached a fever pitch during the 2024 elections https://www.npr.org/2024/11/09/nx-s1-5181965/2024-election-foreign-influence-russia-china-iranp〔2025/7/16 確認〕
※ 180 US Department of Justice：Justice Department Announces Murder-For-Hire and Related Charges Against IRGC Asset and Two Local Operatives https://www.justice.gov/archives/opa/pr/justice-department-announces-murder-hire-and-related-charges-against-irgc-asset-and-two〔2025/7/16 確認〕
※ 181 U.S. Government Publishing Office：118th Congress 2nd Session：S. 5365 To require the President to notify Congress and take certain actions in response to any attempt by a country of concern to affect United States elections. https://www.congress.gov/118/bills/s5365/BILLS-118s5365is.htm#:~:text=,intelligence%20agencies%20stated%20the〔2025/7/16 確認〕
※ 182 GMF：Bribes and Lies: Foreign Interference in Europe in 2024 https://securingdemocracy.gmfus.org/bribes-and-lies-foreign-interference-in-europe-in-2024/〔2025/7/16 確認〕
※ 183 EEAS：3rd EEAS Report on Foreign Information Manipulation and Interference Threats https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en〔2025/7/16 確認〕
GMF：Bribes and Lies: Foreign Interference in Europe in 2024 https://securingdemocracy.gmfus.org/bribes-and-lies-foreign-interference-in-europe-in-2024/〔2025/7/16 確認〕
※ 184 Spiegel：Alternative gegen Deutschland https://www.spiegel.de/politik/deutschland/afd-spionageaffaere-russland-und-china-im-fokus-neue-enthuellungen-belasten-die-partei-a-46042b96-2d61-4bb4-ac25-ead57d7d6285〔2025/7/16 確認〕
※ 185 U.S. Department of Justice：Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm https://www.justice.gov/archives/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners〔2025/7/16 確認〕
※ 186 EURACTIV：Russia targets social media during French legislative campaign https://www.euractiv.com/section/politics/news/russia-targets-social-media-during-french-legislative-campaign/〔2025/7/16 確認〕
※ 187 France Diplomacy：Foreign digital interference – Result of investigations into the Russian propaganda network Portal Kombat (15 February 2024) https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/2024/article/foreign-digital-interference-result-of-investigations-into-the-russian〔2025/7/16 確認〕
※ 188 Secrétariat général de la défense et de la sécurité nationale：PORTAL KOMBAT A structured and coordinated pro-Russian propaganda network https://www.sgdsn.gouv.fr/files/files/Publications/20240214_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_PART2_ENG_VF.pdf〔2025/7/16 確認〕
※ 189 Recorded Future：Sombres Influences：Russian and Iranian Influence Networks Target French Elections https://go.recordedfuture.com/hubfs/reports/TA-2024-0628.pdf〔2025/7/16 確認〕
※ 190 France Diplomacy：France strongly condemns Russian actors and their intermediaries implicated in the Storm-1516 manoeuvres (6 May 2025) https://www.diplomatie.gouv.fr/en/country-files/russia/news/2025/article/france-strongly-condemns-russian-actors-and-their-intermediaries-implicated-in〔2025/7/16 確認〕
※ 191 BBC NEWS JAPAN：オーストリア下院、首相不信任案を可決 スキャンダルで https://www.bbc.com/japanese/48428991〔2025/7/16 確認〕
※ 192 The Record：Austria uncovers alleged Russian disinformation campaign spreading lies about Ukraine https://therecord.media/austria-uncovers-russian-disinfo-campaign〔2025/7/16 確認〕
※ 193 The Wall Street Journal：A Den of Spies: Vienna Emerges as Hub for Russian Espionage https://www.wsj.com/world/a-den-of-spies-vienna-emerges-as-hub-for-russian-espionage-9dda8b4d?st=2fd7fnlb9sgbnqs〔2025/7/16 確認〕
※ 194 BBC：Romania hit by major election influence campaign and Russian cyber-attacks https://www.bbc.com/news/articles/cgq18w507dko〔2025/7/16 確認〕
※ 195 Curtea Constituțională a României：COMUNICAT DE PRESĂ, 6 decembrie 2024 https://www.ccr.ro/comunicat-de-presa-6-decembrie-2024/〔2025/7/16 確認〕
※ 196 Curtea Constituțională a României：privind anularea procesului electoral cu privire la alegerea Președintelui României din anul 2024 https://web.archive.org/web/20241206195537/https://www.ccr.ro/wp-content/uploads/2024/12/HCC-32-2024.pdf〔2025/7/16 確認〕
※ 197 Președintele României：Analiza unor riscuri la adresa securității nationale generate de actiunile unor actori cibernetici statali si non-statali asupra unor infrastructuri IT&C, suport pentrú procesul electoral https://www.presidency.ro/files/userfiles/Documente%20CSAT/Document%20CSAT%20SIE.pdf〔2025/7/16 確認〕
※ 198 Democratic Erosion Consortium：Russia fueling Democratic Struggles in Romania through the Media https://democratic-erosion.org/2025/04/24/russia-fueling-democratic-struggles-in-romania-through-the-media/〔2025/7/16 確認〕
※ 199 Reuters：EU opens investigation into TikTok over election interference https://www.reuters.com/business/eu-opens-investigation-into-tiktok-over-election-interference-2024-12-17/〔2025/7/16 確認〕
※ 200-1 Reuters：Romania braces for wave of disinformation ahead of election second round https://www.reuters.com/world/europe/romania-braces-wave-disinformation-ahead-election-second-round-2025-05-05〔2025/7/16 確認〕
※ 200-2 OpenMinds：End of Democracy: How Pro-Russian Telegram Channels Influence Romanian Elections https://www.openminds.ltd/reports/end-of-democracy-how-pro-russian-telegram-channels-influence-romanian-elections〔2025/7/25 確認〕
※ 201 Svidomi：One fake news story fuelled riots across the country. How Russian propaganda affects the UK https://svidomi.in.ua/en/page/one-fake-news-story-fuelled-riots-across-the-country-how-russian-propaganda-affects-the-uk〔2025/5/19 確認〕
※ 202 The Telegraph：The obscure Russian-linked 'news' outlet fuelling violence on Britain's streets https://www.telegraph.co.uk/news/2024/08/03/obscure-russian-linked-news-outlet-fuelling-violence/〔2025/7/16 確認〕
※ 203 The Bureau of Investigative Journalism：Did Russian disinformation fuel the Southport protests? https://www.thebureauinvestigates.com/stories/2024-08-02/did-russian-disinformation-fuel-the-southport-protests/〔2025/7/16 確認〕
※ 204 Independent：Former security minister raises concerns Putin behind Southport far-right disinformation https://www.independent.co.uk/news/uk/politics/southport-far-right-disinformation-russia-b2589041.html〔2025/7/16 確認〕
※ 205 openDemocracy：Great Replacement & boogaloo: The ideology driving the modern far right https://www.opendemocracy.net/en/far-right-riots-great-replacement-boogaloo/〔2025/7/16 確認〕
※ 206 The Soufan Center：QUANTIFYING THE Q CONSPIRACY: A Data-Driven Approach to Understanding the Threat Posed by Qanon https://thesoufancenter.org/wp-content/uploads/2021/04/TSC-White-Paper_QAnon_16April2021-final-1.pdf〔2025/7/16 確認〕
※ 207 GOV.UK：UK children and adults to be safer online as world-leading bill becomes law https://www.gov.uk/government/news/uk-children-and-adults-to-be-safer-online-as-world-leading-bill-becomes-law〔2025/7/16 確認〕
※ 208 UK Parliament：Social media, misinformation and harmful algorithms https://committees.parliament.uk/work/8641/social-media-misinformation-and-harmful-algorithms/news/〔2025/7/16 確認〕
※ 209 FOCUS TAIWAN：China steps up disinformation campaign in 2024: NSB report https://focustaiwan.tw/politics/202501030012〔2025/7/16 確認〕
※ 210 Reuters：Chinese state media stoked allegation Taiwan's president would flee war https://www.reuters.com/world/asia-pacific/chinese-state-media-stoked-allegation-taiwans-president-would-flee-war-2024-04-01/〔2025/7/16 確認〕
※ 211 産経新聞：台湾・頼清徳政権に偽情報攻撃 「日米と組んで『独立』図る」 認知戦拡大を専門家ら警戒 https://www.sankei.com/

article/20240922-J42HRMJH7ZKUZDICHKXPDCHKPM/〔2025/7/16 確認〕
※ 212 Taiwan Factcheck Center：Who are Japanese Taiwanese? The Chinese disinformation that fixated on the ties between Taiwan and Japan https://en.tfc-taiwan.org.tw/who-are-japanese-taiwanese-the-chinese-disinformation-that-fixated-on-the-ties-between-taiwan-and-japan/〔2025/7/16 確認〕
※ 213 Taiwan Factcheck Center：【錯誤】網傳照片「總統賴清德在金門致詞，講台背板出現日本軍旗」？ https://tfc-taiwan.org.tw/fact-check-reports/migration-10958/〔2025/7/16 確認〕
※ 214 FORMOSA NEWS：China reportedly offered payment for propaganda piece on Taiwan-Tuvalu relations https://english.ftvnews.com.tw/news/2024128W06EA〔2025/7/16 確認〕
※ 215 Islands Business：Taiwan envoy says Tuvalu ties 'rock solid' post-election https://islandsbusiness.com/news-break/taiwan-envoy-says-tuvalu-ties-rock-solid-post-election/〔2025/7/16 確認〕
※ 216 FOCUS TAIWAN：Taiwan's embassy in Tuvalu blasts Beijing over 'disinformation' https://focustaiwan.tw/politics/202501150004〔2025/7/16 確認〕
※ 217 オーストラリア戦略政策研究所（Australian Strategic Policy Institute）：Russia and China co-ordinate on disinformation in Solomon Islands elections https://www.aspistrategist.org.au/russia-and-china-co-ordinate-on-disinformation-in-solomon-islands-elections/〔2025/7/16 確認〕
※ 218 Sputnik：Is US Plotting Electoral Coup in Solomon Islands? https://sputnikglobe.com/20240409/is-us-plotting-electoral-coup-in-solomon-islands-1117758198.html〔2025/7/16 確認〕
※ 219 Global Times：Allegations of US interference emerge ahead of pivotal election in Solomon Islands https://www.globaltimes.cn/page/202404/1310521.shtml〔2025/7/16 確認〕
※ 220 The Intercept：Hacked Russian Files Reveal Propaganda Agreement With China https://theintercept.com/2022/12/30/russia-china-news-media-agreement/〔2025/7/16 確認〕
※ 221 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〔2025/7/16 確認〕
International Republican Institute：The Authoritarian Nexus – How Russia and China Undermine Democracy Worldwide https://www.iri.org/wp-content/uploads/2024/04/The-Authoritarian-Nexus.pdf〔2025/7/16 確認〕
※ 222 外務省：日・ウクライナ経済復興推進会議 https://www.mofa.go.jp/mofaj/erp/c_see/ua/pageit_000001_00299.html〔2025/7/16 確認〕
※ 223 SOMPO CYBER SECURITY：親ロシア・グループの日本への攻撃（2024 年 2 月） https://www.sompocybersecurity.com/column/column/pro-russia-hacktivists-ddos-japan-2024-feb〔2025/7/16 確認〕
※ 224 NHK：岸田首相の偽画像などが SNS で相次ぎ拡散 注意を呼びかけ https://www3.nhk.or.jp/news/special/article/society20240218-01.html〔2025/7/16 確認〕
※ 225 NHK：軍事侵攻 2 年 ロシア支持サイトなどの記事 拡散割合増える https://www3.nhk.or.jp/news/html/20240222/k10014368131000.html〔2025/7/16 確認〕
※ 226 読売新聞オンライン：選挙イヤー2024で強まるインフルエンスオペレーション（影響力工作）への警戒感 https://www.yomiuri.co.jp/column/matsurigoto/20240313-OYT8T50001/3/〔2025/7/16 確認〕
※ 227 CYBLE：NATO's 75th Anniversary Washington Summit Draws Ire of Hacktivist Groups https://cyble.com/blog/natos-75th-anniversary-washington-summit-draws-ire-of-hacktivist-groups/〔2025/7/16 確認〕
※ 228 Graphika Technologies, Inc.：Summit Old, Summit New https://22006778.fs1.hubspotusercontent-na1.net/hubfs/22006778/Report%20PDFs/graphika_report_summit_old_summit_new.pdf?utm_campaign=Report%20Demand%20Gen&utm_medium=email&_hsenc=p2ANqtz-_FHUKYRyaYcED9iUc17fp8Gh48e6z62SV8y4yiyhXuFDoqvvVWRxRF-9oVdtVRIcwAPSrF4WvklrBc-kYuDhWnjyM7Wqb-H5-uBVBG_e3r9W19RpU&_hsmi=315775437&utm_content=315775437&utm_source=hs_automation〔2025/7/16 確認〕
※ 229 VOA：Russia-tailed AI-generated deepfake videos target US presidential elections, NATO https://www.voanews.com/a/7633946.html〔2025/7/16 確認〕
※ 230 SOMPO CYBER SECURITY：【ブログ】親ロシア・ハクティビストが日本の金融機関・政党・鉄道会社等 Web サイトを攻撃（2024 年 7 月） https://www.sompocybersecurity.com/column/column/pro-russia-hacktivists-ddos-japan-2024-jul〔2025/7/16 確認〕
※ 231 EEAS：Paint It Black – Pro-Kremlin take on the NATO Summit https://euvsdisinfo.eu/paint-it-black-pro-kremlin-take-on-the-nato-summit/〔2025/7/16 確認〕
※ 232 Sputnik:ウクライナが 10 年以内に NATO に加盟するとは誰も言っていない＝NATO 事務総長 https://x.com/sputnik_jp/status/1810143279754977488〔2025/7/16 確認〕
※ 233 Sputnik：NATO 諸国が警戒する、「対ロシア」で越えてはならないデッドライン＝元自衛官、矢野義昭氏 https://sputniknews.jp/20240628/nato-18723847.html〔2025/7/16 確認〕
※ 234 Sputnik：高まる NATO 東京事務所開設の可能性 岸田氏の NATO サミット出席 https://sputniknews.jp/20240706/natonato-18768338.html〔2025/7/16 確認〕
※ 235 日本ファクトチェックセンター：パンデミック条約でワクチン強制接種？ 繰り返し否定されている誤情報【ファクトチェック】 https://www.factcheckcenter.jp/fact-check/health/false-pandemic-treaty-vaccine-mandate/〔2025/7/16 確認〕
※ 236 日本ファクトチェックセンター：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/〔2025/7/16 確認〕
※ 237 PRESIDENT Online：「コロナワクチンで 50 万人が死亡」「日本で人体実験している」…反ワク派の主張を専門家と徹底検証した結果 https://president.jp/articles/-/90457?page=1〔2025/7/16 確認〕
※ 238 Radio Free Asia：Did Japan classify mRNA vaccines 'deadliest drug' in history? https://www.rfa.org/english/factcheck/2024/12/09/afcl-japan-mrna-vaccine-covid/〔2025/7/16 確認〕
※ 239 U.S. Embassy & Consulates in Italy：Fact vs. Fiction: Russian Disinformation on Ukraine https://it.usembassy.gov/fact-vs-fiction-russian-disinformation-on-ukraine/〔2025/7/25 確認〕
※ 240 The New York Times：Deepfake of U.S. Official Appears After Shift on Ukraine Attacks in Russia https://www.nytimes.com/2024/05/31/us/politics/deepfake-us-official-russia.html〔2025/7/16 確認〕
※ 241 National Security Archive：The Kremlin's Efforts to Covertly Spread Disinformation in Latin America https://nsarchive.gwu.edu/document/32130-25-state-dept-kremlin-covert-disinformation-latin-america〔2025/7/16 確認〕
※ 242 Prosperity Institute：Information at War: From China's Three Warfares to NATO's Narratives https://www.prosperity.com/media-publications/information-at-war-from-chinas-three-warfares-to-natos-narratives/〔2025/7/16 確認〕
※ 243-1 The Associated Press：Misinformation about the Israel-Hamas war is flooding social media. Here are the facts https://apnews.com/article/israel-hamas-gaza-misinformation-fact-check-e58f9ab8696309305c3ea2bfb269258e?utm_source=Email&utm_medium=share〔2025/7/16 確認〕
※ 243-2 BBC NEWS JAPAN：【解説】「ウクライナは生物兵器を開発している」 ロシアの主張をファクトチェック https://www.bbc.com/japanese/features-and-analysis-60733307〔2025/7/25 確認〕
※ 244 RAND Corporation：Lies, Misinformation Play Key Role in Israel-Hamas Fight https://www.rand.org/pubs/commentary/2023/10/lies-misinformation-play-key-role-in-israel-hamas-fight.html〔2025/7/16 確認〕
※ 245 PBS NEWS：How misinformation about Israel and Gaza has evolved in the yearlong war https://www.pbs.org/newshour/world/how-misinformation-about-israel-and-gaza-has-evolved-in-the-yearlong-war〔2025/7/16 確認〕
※ 246 日本ファクトチェックセンター：イスラエル・パレスチナ情勢をめぐり大量の誤情報 / 偽情報 検証方法を解説【ファクトチェックまとめ】 https://www.factcheckcenter.jp/fact-check/international/israel-palestine-conflict-fact-check-summary/〔2025/7/16 確認〕
※ 247 The New York Times：In a Worldwide War of Words, Russia, China and Iran Back Hamas https://www.nytimes.com/2023/11/03/technology/israel-hamas-information-war.html〔2025/7/16 確認〕
※ 248 POLITICO：Russia-linked fake videos spread German election fraud claims, authorities warn https://www.politico.eu/article/russia-linked-fake-videos-spread-german-election-fraud-claims-authorities-warn/〔2025/7/16 確認〕

第3章
国内の政策及び取り組みの動向

2024 年度以降、我が国のサイバー安全保障分野での対応能力向上を目的とした各種法整備が進み、政府機関等により、これに関連した様々な取り組みが開始された。また、網羅的なセキュリティ対策強化のため、中小企業を含む人材育成の取り組みや機会創出、評価・認証制度の運営、普及啓発活動も進んでいる。本章ではサイバーセキュリティに関する国内の政策、取り組みについて解説する。

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 政府全体の政策動向

本項では、政府が特に注力している取り組みについて取り上げる。具体的には、サイバー安全保障に関する取り組み、「サイバーセキュリティ 2024（2023 年度年次報告・2024 年度年次計画）※1」において特に強力に取り組むとされた施策を紹介する。また、経済安全保障に関する取り組みを紹介する。

(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）

2022 年に閣議決定された「国家安全保障戦略※2」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、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・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、これらの実現に向けた検討を行うために開催された有識者会議の提言、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※3」（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※4」（以下、整備法）の概要を紹介する。

(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

「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※5」が立ち上げられ、4 回の全体会議、及び以下をテーマとした計 9 回のテーマ別会合で検討を行った。

①官民連携の強化
②通信情報の利用
③アクセス・無害化

その結果、実現すべき具体的な方向性について、上記 3 テーマ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横断的課題について「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※6」を取りまとめた。各テーマについての提言の概要は以下のとおりである。

①官民連携の強化
- 官民双方向の情報共有を促進すべき。
- 技術情報に加え、経営層が判断を下す際に必要な、攻撃の背景や目的等も共有されるべき。
- 特に漏えいにより我が国の安全保障に支障を与えるおそれがある情報等を扱う場合にはセキュリティ・クリアランス制度を活用する等、適切な情報管理と情報共有を両立する仕組みを構築すべき。
- ベンダーとの連携を深めるべき。ベンダーが利用者とリスクコミュニケーションを行うべき旨を法的責務として位置付けるべき。

- 基幹インフラ事業者によるインシデント報告の義務化のほか、その保有重要機器の機種名等の届出を求め、攻撃関連情報の迅速な提供等ができる仕組みを整えるべき。被害組織の負担軽減等のため、報告先や様式の一元化、簡素化等を進めるべき。

②通信情報の利用

- 先進主要国は国家安全保障の観点からサイバー攻撃対策のため事前に対象を特定せず通信情報を収集して分析しており、我が国でも一定の条件下での通信情報の利用を検討すべき。
- 外外通信（国内を経由し伝送される国外から国外への通信）は先進主要国と同等の方法の分析が必要。加えて、外内通信（国外から国内への通信）及び内外通信（国内から国外への通信）についても必要な分析をできるようにしておくべき。
- コミュニケーションの本質的内容に関わる部分は分析の必要があるとは言えない。機械的にデータを選別し検索条件等で絞る等の工夫が必要。
- 通信の秘密であっても公共の福祉のために必要かつ合理的な制限を受ける。取得及び情報処理のプロセスについて独立機関の監督が重要。
- 通信当事者の有効な同意がある場合の通信情報の利用は、同意がない場合とは異なる内容の制度により実施することも可能。
- 性質上非公開とすべき範囲はあるが、適切な情報公開は行われるべき。公開困難な部分を独立機関の監督で補うべき。

③アクセス・無害化

- サイバー攻撃の特徴を踏まえ、被害防止を目的としたアクセス・無害化を行う権限は、緊急性を意識し、事象や状況の変化に応じて臨機応変かつ即時に対処可能な制度にすべき。比例原則を遵守し、必要な範囲で実施されるものとするため、警察官職務執行法を参考としつつ、適正な実施を確保するための検討を行うべき。
- 武力攻撃事態に至らない段階から我が国を全方位でシームレスに守るための制度とすべき。
- 権限の執行主体は、警察や防衛省・自衛隊とし、共同で実効的に措置を実施可能な制度とすべき。
- 措置の対象は、国、重要インフラ、事態発生時等に自衛隊等の活動が依存するインフラ等へのサイバー攻撃に重点を置く一方、必要性が認められる場合には、適切にアクセス・無害化が実施できるような仕組みとすべき。
- 国際法上許容される範囲でアクセス・無害化が行われるような仕組みを検討すべき。

④横断的課題

- サイバーセキュリティ戦略本部の構成等を見直すとともに、NISC の発展的改組にあたり、政府の司令塔として強力な情報収集・分析、対処調整機能を有する組織とすべき。
- 重要インフラに求められるサイバーセキュリティ対策の水準を示し、常に見直しを図る制度とすべき。
- 政府主導での高品質な国産セキュリティ製品、サービス供給の強化を支援すべき。
- 官民の人材交流を強化すべき。
- 中小企業等のセキュリティ対策についての支援拡充やサプライチェーン企業の対策水準を検討すべき。

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。

- 新たな司令塔機能の確立
  - NISC を我が国におけるサイバーセキュリティの司令塔機能を担う新組織へ発展的に改組する。
  - サイバー脅威に関するすべての利用可能な情報による付加価値の高い分析に基づき、国際連携・官民連携により、政府全体で被害の未然防止・拡大防止を含めた対応を行うため、新組織を中心に、高度な情報収集・分析能力を担う体制・基盤・人材等を総合的に整備する。
- 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
  - 新組織を中心に官民連携基盤を整備し、適切な情報保全・管理に基づく政府からの積極的な情報提供及び報告等に係る民間の負担軽減を進め、官民双方向の情報共有を求心力とした、認識共有・信頼醸成に基づく新たな官民連携エコシステムの実現を図る。
  - 政府機関等について、横断的な監視体制を強化・高度化し、セキュリティ対策水準の向上及び実効

性の確保を図る。また、IoT 製品のセキュリティ評価制度である「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、政府機関等の調達の選定基準に含める。

- 単独での対策が困難な小規模自治体も念頭に置いた人材確保等の支援や、診療等への影響を最小限にするため、医療機関等に対する初動対応等の支援を推進する。
- 政府機関・重要インフラ等を通じ、官民横断的な対策の強化を図るため、脅威ハンティングの実施拡大や、実践的対応力の強化を推進する。また、重要インフラについては、分野特性を踏まえつつ、分野横断的な新たな基準を策定する。
- 社会全体のセキュリティ確保の強化に向け、セキュアバイデザイン原則等に基づき、IoT 製品等のセキュリティ対策やソフトウェアの透明性確保等に係る取り組みを推進し、普及・浸透を図る。
- 中小企業等を含めたサプライチェーン全体のレジリエンス強化に向け、リスクに応じた対策水準の提示、対策サービスに係る支援、関係法令の適用関係の明確化等、対応力に応じたサイバーセキュリティ対策の実装拡大に向けた取り組みを推進する。

- サイバーセキュリティを支える人的・技術的基盤の整備
  - 官民を通じた人材の育成・確保のため、関係政府機関等における高度人材の確保・育成に向けた民間人材の活用や演習環境の構築の推進とともに、官民共通の「人材フレームワーク」を策定し、官民を通じた実態把握やキャリアパス設計等を進める。
  - サイバーセキュリティ関連技術について、官のニーズを踏まえた研究開発・実証等を通じた技術情報等の提供や、政府機関等による積極的な活用等により、国内産業の育成及び早期の社会実装による新たな技術・サービスを生み出すエコシステムの形成を図るとともに、先端技術について、国際的な動向を踏まえ、AI に係る安全性の確保や耐量子計算機暗号（PQC：Post-Quantum Cryptography）への移行等に関して対応を進める。
- 国際連携を通じた我が国のプレゼンス強化
  - 国際的なルール整備に関し、二国間・多国間関係を強化・進展させるとともに、ASEAN・太平洋島しょ国等に対する能力構築プログラムを提供し、協力関係を強化する。

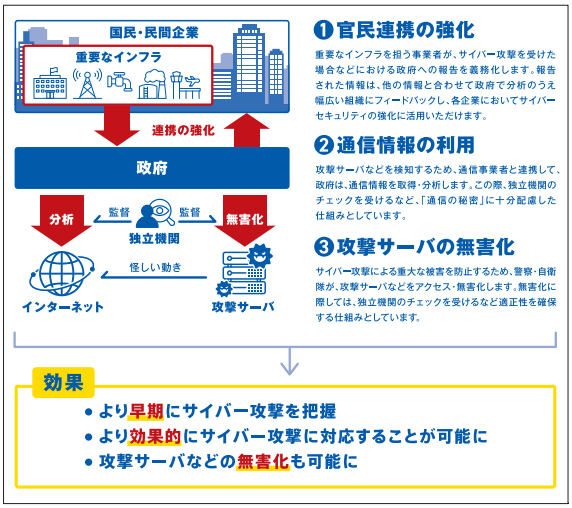
2025 年 7 月 1 日には、NISC が発展的に改組され、サイバー安全保障も含め、官民を通じたサイバーセキュリティの確保に関する司令塔として、内閣サイバー官を長とする国家サイバー統括室（NCO：National Cybersecurity Office）が発足した[※8]。

(b) サイバー対処能力強化法及び整備法

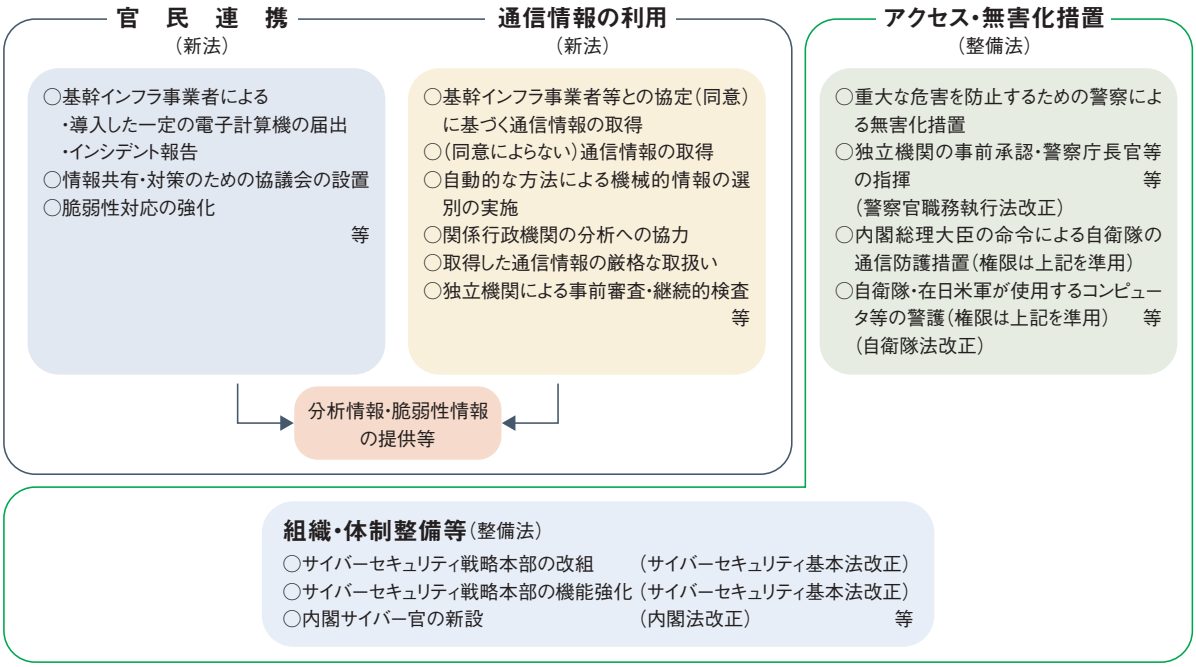
「国家安全保障戦略」及び前述の提言を踏まえて 2025 年 2 月、サイバー対処能力強化法案及び整備法案が閣議決定され、同年 5 月に成立し[※9]、同月、サイバー対処能力強化法及び整備法として公布された[※10]。

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[※10]。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ため、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、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 3-1-1 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。また、図 3-1-2（次ページ）は、両法律の概



■図 3-1-1　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。[※11]」



■図 3-1-2　サイバー対処能力強化法（図中の「新法」）及び整備法の概要
（出典）内閣官房「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 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案 概要※12」を基に IPA が編集

要である。

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を参照されたい※13。

①官民連携の強化

- 基幹インフラ事業者によるインシデント報告等
  - 基幹インフラ事業者※14が特定重要電子計算機（サイバーセキュリティが害された場合に、特定重要設備の機能が停止し、または低下するおそれがある一定の電子計算機）を導入した際の事業所管大臣への届出
  - 基幹インフラ事業者が特定重要電子計算機のインシデント情報等を認知した際の事業所管大臣・内閣総理大臣への報告
- 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
  - 内閣総理大臣・電子計算機等供給事業所管大臣（電子計算機やそれに組み込まれるプログラムの供給を行う事業を所管する大臣。経済産業大臣等※15）が重要電子計算機として用いられる電子計算機やプログラムにおける脆弱性を認知した際の当該電子計算機等の供給者に対する情報提供
  - 脆弱性が基幹インフラ事業者が使用する特定重要電子計算機に用いられる電子計算機等に関連する場合、電子計算機等供給事業所管大臣が、当該電子計算機等の供給者に対し、サイバー攻撃による被害を防止するために必要な措置を講ずるよう要請
- 罰則の整備
  - 行政職員・協議会構成員等による秘密の不正な利用・漏えいの行為に対する罰則
  - 基幹インフラ事業者が、インシデント報告等を行わず、是正命令を受けてもなお対応しない場合、または、インシデント報告等に関連し、資料提出等を求められても対応しない場合の罰則

②通信情報の利用

- 基幹インフラ事業者等との協定（同意）に基づく通信情報の取得
  内閣総理大臣は、基幹インフラ事業者等との協定に基づき、通信情報を取得し、取得した通信情報のうち、外内通信に係るものを用いて分析を実施し、当該事業者に必要な分析結果を提供する。
  なお、この場合の通信情報の取得は、協定（同意）に基づくため、通信の秘密に抵触しない。
- （同意によらない）通信情報の取得
  内閣総理大臣は、国外の攻撃インフラ等の実態把握のため必要があると認める場合には、サイバー通

信情報監理委員会（いわゆる 3 条委員会）の承認を受け、外外通信の通信情報を取得することができる。また、内閣総理大臣は、国内へのサイバー攻撃の実態把握のため、特定の外国設備との通信等を分析する必要があると認める場合には、サイバー通信情報監理委員会の承認を受け、外内通信または内外通信の通信情報を取得することができる。

- 自動的な方法による機械的情報の選別の実施

  内閣総理大臣は、取得した通信情報について、人による知得を伴わない自動的な方法により、調査すべきサイバー攻撃に関係があると認めるに足りる機械的情報（IP アドレス、指令情報等のコミュニケーションの本質的な内容ではない情報（図 3-1-3））を選別し、それ以外のものを直ちに消去する措置を講ずることとされている。

コミュニケーションの本質的な内容に**当たらない例**	○ 送受信日時 2024.04.01 12:00:04 ○ IPアドレス 103.23.145.84 ○ 通信量 20kB ○ ポート番号 80 ○ コマンド POST/ A3fe e3844A7D35300734D2BA HTTP/1.1 ○ プロトコル（通信方式） HTTP / SSL / SMTP ○ ソフトウェアの種類 Mozilla/4.0(…Trident/7.0;NET4.0c;…)… ○ ドメイン名 cas.go.jp ○ メールアドレス hogehoge@example.com （個人情報保護の観点から、個人を識別することができないように加工することが必要）
コミュニケーションの本質的な内容に**当たる例**	× 電子メールの本文・件名 × 添付ファイルの内容・名称 × IP電話の通話内容 × Webサイトに掲載されている文章、画像

■図 3-1-3　コミュニケーションの本質的な内容ではない情報の例
（出典）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※9」を基に IPA が編集

- 独立機関による事前審査・継続的検査

  通信情報の利用の適正確保のため、サイバー通信情報監理委員会を設置し、内閣総理大臣による（同意によらない）国外関係通信の取得に際しての遅滞のない審査・承認、通信情報の取り扱いに対する継続的な検査、無害化措置に際しての審査・承認等の事務等を行わせることとする。

  同委員会は、承認件数等について国会に報告するとともに、その概要を公表しなければならない。

  なお、通信情報の漏えいや盗用については罰則が定められている。

- 罰則の整備
  - 通信情報を取り扱う行政職員による通信情報の不正な利用・漏えいの行為に対する罰則
  - 通信情報を保有する行政機関の管理を侵害して通信情報を取得する行為に対する罰則

③分析情報・脆弱性情報の提供等

内閣総理大臣は、基幹インフラ事業者によるインシデント報告や選別後の通信情報、協議会を通じて得た情報等の整理・分析を行い、整理・分析した情報（分析情報）を、サイバーセキュリティ確保のため、関係行政機関に提供する。必要に応じて、外国政府等にも提供できる。また、事業所管大臣は、必要に応じ、基幹インフラ事業者に対して分析情報を提供できる。

そのほか、前記①で述べたように、脆弱性対応の強化のための関係者への情報提供や、協議会における情報共有等が規定されている（次ページ図 3-1-4）。

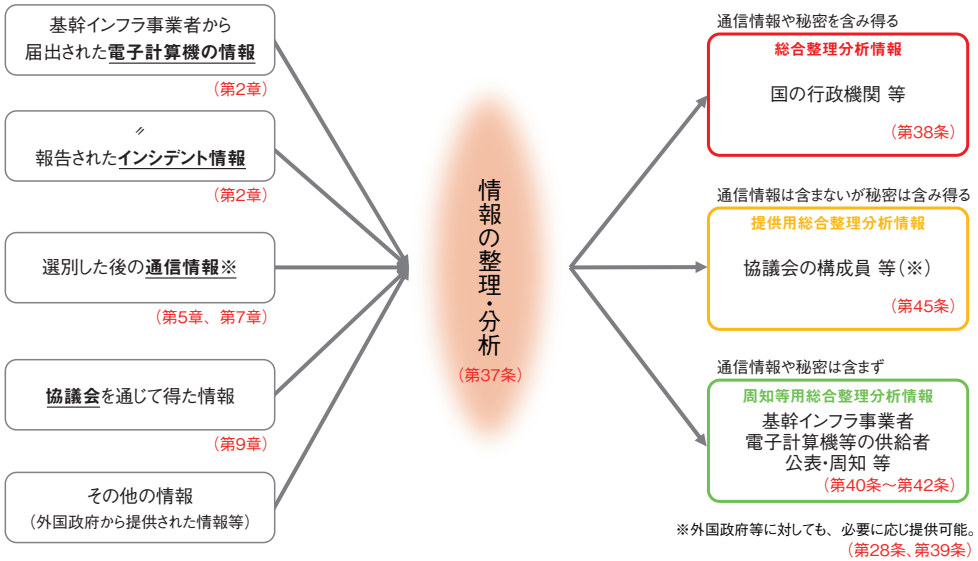
④アクセス・無害化措置

- 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）

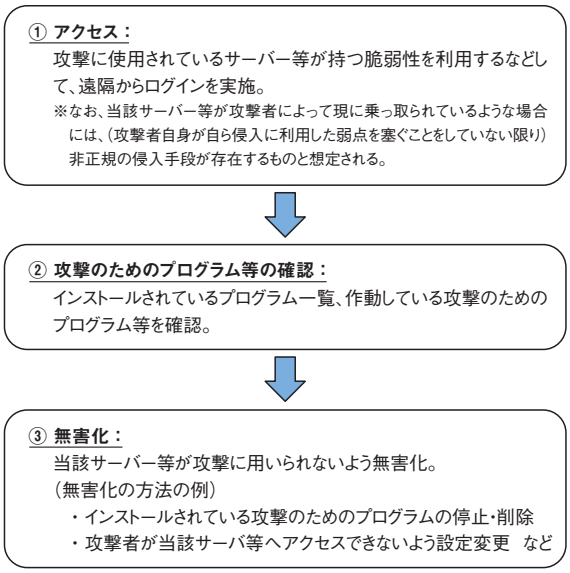
  警察庁長官が指名する警察官（サイバー危害防止措置執行官）は、サイバー攻撃に用いられる通信等を認めた場合であって、そのまま放置すれば重大な危害が発生するおそれがあるため緊急の必要があるときは、サイバー攻撃の送信元等であるサーバー等の管理者等に対し、攻撃のためのプログラムの停止・削除等の措置（当該サーバー等にアクセスし、インストールされた攻撃のためのプログラム等を確認することを含む）を命じ、または自ら当該措置を実施することができる（アクセス・無害化のステップについては、次ページ図 3-1-5 参照）。国外のサーバー等への措置に際しては、外務大臣との事前協議が必要とされている。また、措置に際しては、原則、サイバー通信情報監理委員会の事前の承認が必要である。

- 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）

  国や基幹インフラ等の重要電子計算機に対する攻撃であり、外国政府を背景とする主体による高度の攻撃と認められるものが行われ、自衛隊が対処する特別の必要があるときは、内閣総理大臣が当該重要電子計算機に対する通信防護措置をとるべき旨を命ずることができる。通信防護措置を命ぜられた部隊等は、警察と共同して当該措置を実施する。その際、改正警察官職務執行法を準用し、サイバー



■図 3-1-4　分析情報・脆弱性情報の提供等のイメージ
（出典）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」



■図 3-1-5　アクセス・無害化のステップ（イメージ）
（出典）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」を基に IPA が編集

通信情報監理委員会の事前の承認等のもとでアクセス・無害化措置を実施することができる。

また、自衛隊及び在日米軍が使用する電子計算機をサイバー攻撃から職務上警護する自衛官についても、緊急の必要があるときには、同法を準用し、アクセス・無害化措置を実施できる。

なお、アクセス・無害化については、その実施主体が警察及び自衛隊になるが、こうした措置は国家安全保障の観点から整合性の取れた形で行われる必要があり、内閣官房（新組織）が、国家安全保障局とも連携しつつ、その司令塔機能を発揮する必要がある[※10]。

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
  - サイバーセキュリティ戦略本部を、内閣総理大臣を本部長、すべての国務大臣を本部員とする組織に改組するとともに、有識者から構成されるサイバーセキュリティ推進専門家会議を新設
  - サイバーセキュリティ戦略本部の所掌事務に、重要インフラ事業者等のサイバーセキュリティ確保に関する国の施策の基準の作成及び国の行政機関等におけるサイバーセキュリティの確保の状況の評価等を追加し、機能強化
  - 内閣府の所掌事務にサイバー対処能力強化法に基づく官民連携の強化及び通信情報の利用に関する事務を追加するとともに、同府にサイバー通信情報監理委員会を設置。また、サイバー対処能力強化法に係る事務を掌理する内閣府特命担当大臣の設置
  - 内閣官房に、サイバーセキュリティの確保に関する総合調整等の事務を掌理する内閣サイバー官を新設
  - IPA の業務に、情報の整理分析及び被害防止に必要な情報の周知等の事務並びに重要インフラ事業者等のサイバーセキュリティの確保の状況の調査を追加
  - 国立研究開発法人情報通信研究機構（NICT：National Institute of Information and Communications Technology）の業務に、国

等の情報システムに対する不正な活動の監視及び分析に係る事務を追加

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の設置については公布日から 1 年以内、通信情報の利用については一部を除き 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、内閣サイバー官の設置等については、6 ヵ月以内）で政令で定める日から施行される。

今後、サイバー対処能力強化法第 3 条に基づき閣議決定される基本方針に基づき、上記の事項等が具体化される。

(2) 年次計画に基づく取り組み

政府は、「サイバーセキュリティ基本法[※16]」に基づき、3 年程度の間のサイバーセキュリティに係る諸施策の目標及び実施方針を示すサイバーセキュリティ戦略を策定するとともに、同戦略を的確に実施するために、各年度の年次計画を作成し、サイバーセキュリティ施策を推進している。

本項では、2024 年 7 月に策定された「サイバーセキュリティ 2024（2023 年度年次報告・2024 年度年次計画）」（以下、年次計画）において「特に強力に取り組む施策」として掲げられているものに関連する取り組みを中心に紹介する。

(a) 政府機関や重要インフラ等の対処能力の向上

年次計画では、国全体のリスクの低減とレジリエンスの向上を図るため、「政府機関や重要インフラ等の対処能力の向上」が必要であり、そのために政府機関におけるサイバーセキュリティ体制の抜本的強化、重要インフラ演習の強化及び個別分野におけるレジリエンス向上、IPA の機能強化及び NICT の取り組み強化を通じたサイバーセキュリティ対策の底上げ等に取り組むこととされた。

- 政府機関におけるサイバーセキュリティ体制の抜本的強化

  政府機関等が講ずるべきサイバーセキュリティ対策のベースラインとなる「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」が 2023 年に令和 5 年度版[※17]に改定されたのを受け、NISC は、2024 年 7 月に「政府機関等の対策基準策定のためのガイドライン（令和 5 年度版）」の一部改定[※18]、同年 10 月に「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」の改定[※19]を行った。また、NISC は、同年 7 月、政府機関等の情報システムを対象とした横断的アタックサーフェスマネジメント（ASM）事業を開始した[※20]。そのほか、年次計画には、デジタル庁における総合運用・監視システムによる運用監視の開始（「3.1.2 (2) 総合運用・監視システム（COSMOS）の整備」参照）や、安全性や透明性の検証が可能な国産センサーを導入し、得られた情報を集約して分析し、我が国独自にサイバーセキュリティに関する情報の生成を行うこと等が取り組みとして掲げられている。

- 重要インフラ演習の強化及び個別分野におけるレジリエンス向上

  2024 年度、NISC は、2006 年度から重要インフラ事業者等向けに実施してきた「分野横断的演習」を「全分野一斉演習」として実施するとともに、官民間の連携の実践に重点を置いた新たな「官民連携演習」も実施した。重要インフラ事業者等の障害対応体制の有効性検証を目的とする「全分野一斉演習」は、2024 年 12 月 5 日に机上演習形式で行われ、重要インフラ事業者等（情報通信、金融、電力等の 15 分野）、重要インフラ所管省庁（金融庁、総務省、厚生労働省、経済産業省、国土交通省）、セプター（15 分野 21 セプター）、サイバーセキュリティ関係機関（IPA、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））が参加した。同演習では、情報収集については速やかに対応できているものの、関係機関等への情報共有や緊急時における事業継続の対応については手順書の有無の把握や手順書の即座の参照・行動ができていない点が明らかとなった。また、他業種・他組織へ影響が及ぶ脅威を想定して官民連携（連絡体制・情報共有等）の手順を重点的に確認・検証・強化することを目的とした新たな取り組みである「官民連携演習」は、同年 10 月 16 日（予行）及び 2025 年 2 月 13 日（試行）に机上演習形式で行われた。同演習には、NISC、情報通信分野・電力分野の事業者、セプター及び所管省庁、サイバーセキュリティ関係機関が参加した（予行は 16 組織、試行は 21 組織が参加）。同演習を通じて、政府からの注意喚起等を発出する際に事業者に期待するアクションを明らかにすることや、被害組織からの攻撃に関する情報提供、それを踏まえた政府・事業者間でそれぞれ付加価値を付けて情報を回していくことの重

要性が認識された※21。

医療機関に向けた取り組みとして、厚生労働省は、医療法に基づく医療機関に対する立入検査の際に確認するサイバーセキュリティ対策の項目について、医療情報システムの安全管理に関するガイドラインから特に取り組むべき重要な項目を抽出した「令和6年度版 医療機関におけるサイバーセキュリティ対策チェックリスト※22」及びその解説である「令和6年度版 医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～※23」の公表（2024年5月）、「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表※24」の公表（同年6月）のほか、「医療機関向けセキュリティ教育支援ポータルサイト※25」を通じて研修やインシデント発生時の初動対応支援を行った。また、同月、総務省、厚生労働省及び経済産業省は、情報セキュリティインシデント予防等の観点から、医療機関及び医療情報システム・サービス事業者が医療情報システムの契約において、役割分担等の協議しておくべき事項を具体化するため「医療情報システムの契約における当事者間の役割分担等に関する確認表※26」を公表した。そのほか、2024年6月に改正された「地方自治法※27」により、地方公共団体は、サイバーセキュリティの確保の方針を定め、必要な措置を講じることとされ、総務大臣は、当該方針の策定等について指針を示すこととされた（当該部分は2026年4月施行）。

- IPAの機能強化及びNICTの取り組み強化を通じたサイバーセキュリティ対策の底上げ

IPAが事務局を務めるAIセーフティ・インスティテュート（AISI：AI Safety Institute）は、2024年9月、AIシステムの開発者や提供者がAIセーフティ評価を実施する際に参照できる基本的な考え方を提示する「AIセーフティに関する評価観点ガイド※28」及びAIセーフティ評価手法の一つであるレッドチーミング手法を解説する「AIセーフティに関するレッドチーミング手法ガイド※29」を公開した（「2.1.3 (2) (b) AIセーフティ評価」参照）。また、経済産業省及びIPAは、2025年3月、「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」の運用を開始した※30（「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は、産業分野のセキュリティ・リスク情報集約のハブとしての機能強化等を行った※31（「3.1.3 (1) (c) 政府全体でのサイバーセキュリティ対応体制の強化」参照）。総務省・NICTと厚生労働省が連携し、医療システムを想定した演習教材を作成し、医療機関向けサイバーセキュリティ演習を試行実施した※32。そのほか、年次計画では、講師人材の育成にも取り組むとされている。

(b) サプライチェーン・リスクへの対応強化とDXを推進・支援する取り組みの強化

年次計画では、「サプライチェーン・リスクへの対応強化とDXを推進・支援する取組の強化」のため、セキュアバイデザイン・セキュアバイデフォルト原則を踏まえたIoT機器・ソフトウェア製品のサイバーセキュリティ対策促進、中小企業のサイバーセキュリティ対策促進等に取り組むこととされた。

- セキュアバイデザイン・セキュアバイデフォルト原則を踏まえたIoT機器・ソフトウェア製品のサイバーセキュリティ対策促進

経済産業省は、2024年8月、「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引 ver 2.0※33」を公表したほか、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」において「セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス」の策定に向けた検討が行われている※34（「3.1.3 (1) (b) セキュア・バイ・デザインの実践」参照）。また、前述のとおり、2025年3月、JC-STARの運用が開始されたところ、経済産業省は、IoT製品の輸出時の適合性評価に係る負担を軽減するため、シンガポール（Cybersecurity Labelling Scheme）、英国（PSTI法）、米国（U.S. Cyber Trust Mark）、欧州連合（EU：European Union）（Cyber Resilience Act）との相互承認に向け、海外当局との交渉を引き続き進めるとしている※30。

NICTは、2023年に改正された「国立研究開発法人情報通信研究機構法※35」に基づき、2024年度から、「NOTICE（National Operation Towards IoT Clean Environment）」において、ID・パスワードに脆弱性があるIoT機器の調査に加えて、脆弱性があるファームウェア等を搭載しているIoT機器、既にマルウェアに感染しているIoT機器を新たに対象とするサイバーセキュリティ対策助言等業務を新設する※36とともに、IoT機器メーカー等との連携を強化した※37（「3.1.4 (1) (a) IoTボットネットに対する端末側の対策（新NOTICE）」参照）。また、総務省は、2024年度、

「電気通信事業者におけるフロー情報分析によるC&Cサーバ検知に関する調査」として、一般社団法人ICT-ISAC及び電気通信事業者とともに、平時におけるフロー情報分析によるC&Cサーバー※38の疑いがある機器の検知を行い、C&Cサーバーの検知情報等をICT-ISAC会員企業と共有する運用と対策の検討を行った※39（「3.1.4（1）（b）IoTボットネットに対するネットワーク側の対策（C&Cサーバーの検知・対処の推進）」参照）。

- 中小企業のサイバーセキュリティ対策促進
  IPAは、監視機能の強化や定期的なコンサルティングの実施等の拡充を要件としたサイバーセキュリティお助け隊サービスの新たな類型（2類）を創設し、2024年10月に2類の最初の登録を行った※40ほか、経済産業省は、政府広報の活用※41等により同サービスの認知度拡大を図った（「3.4.1（2）（b）サイバーセキュリティお助け隊サービス制度」参照）。IPAは、2024年度に実施した中小企業実態調査を踏まえ、中小企業において効果のある対策として、SECURITY ACTION二つ星の実施や第三者認証の取得・社内セキュリティ体制の整備等を示した※42（「3.4.1（2）（c）SECURITY ACTION」参照）。また、IPAは、地域のセキュリティ専門家である情報処理安全確保支援士（登録セキスペ）と中小企業のマッチングを促す場としてサイバーセキュリティ相談会を2024年度に計6回開催し、相談会を通じて、中小企業等のセキュリティ対策を支援できる登録セキスペをリスト化（中小企業向けサイバーセキュリティ対策支援者リスト）した※43（登録セキスペについては「3.2.2（2）情報処理安全確保支援士制度」参照）。

（c）欧米主要国を始めとする関係国との連携の一層の強化

年次計画では、「自由、公正かつ安全なサイバー空間」を確保するため、「海外のサイバーセキュリティ関係機関との協調・連携及びインド太平洋地域における能力構築支援の推進」「警察におけるサイバー空間の安全・安心の確保に資する取組の推進」等に取り組むこととされた。

- 海外のサイバーセキュリティ関係機関との協調・連携及びインド太平洋地域における能力構築支援の推進
  海外の関係機関との協調・連携の取り組みとして以下を実施した。
  - 2024年5月、NISC及び警察庁による人権保護や民主主義の推進に関与する組織や個人のためのサイバー脅威緩和に関する国際ガイダンスへの共同署名※44
  - 同年7月、NISC及び警察庁によるAPT40グループに関する国際アドバイザリーへの共同署名※45（「3.1.5（2）（b）（ア）国際アドバイザリーへの共同署名」参照）
  - 同年9月、米国で開催され、68ヵ国・機関が参加した「カウンターランサムウェア・イニシアティブ会合」へのNISC、警察庁及び外務省等による参加※46
  - 2025年1月、日米韓3ヵ国政府による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発出※47
  - 同月、NISCによる英国主導の「サイバーセキュリティ人材に関する国際的な連合」への参画※48

上記のほか、2024年度におけるサイバー分野の外交として、米国（6月）、英国（9月）、EU（11月）等の国・機関とのサイバー対話・協議※49や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※50等の実施により、関係国との連携を深化した（「4.1.1（3）（b）各国との連携強化」）。

2024年6月のG7プーリア・サミットでは、岸田文雄総理（当時）が、AIは人類の発展にとって大きな可能性を秘める一方、偽情報の拡散やサイバー攻撃を含むリスクも生じさせることを指摘した※51。また、G7サイバーセキュリティ作業部会が新たに設置され、2024年5月※52及び12月※53に会合が開催され、重要インフラ保護、サプライチェーンのセキュリティ確保、AIの安全な方法での活用等について議論された。

インド太平洋地域における途上国の能力構築支援の取り組みとして、NISC、総務省及び経済産業省による日ASEANサイバーセキュリティ政策会議（同年10月）※54、経済産業省及びIPA並びに米国及びEU政府による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（同年11月）※55等が実施された（「4.1.1（3）（b）各国との連携強化」参照）。

- 警察におけるサイバー空間の安全・安心の確保に資する取り組みの推進
  警察庁は、2024年度、ランサムウェア攻撃グループ「Phobos」に対する欧州刑事警察機構（Europol：European Union Agency for Law Enforcement Cooperation）や米国連邦捜査局（FBI：Federal Bureau of Investigation）との国際共同捜査や、国際刑事警察機構（ICPO：International Criminal

Police Organization、INTERPOLとも呼ばれる）が主導する西アフリカにおける組織的な金融犯罪に対するオペレーション「ジャッカル」における国際共同捜査に参画し、独自の分析結果等を関係国の捜査機関に提供することにより、被疑者の検挙に貢献した※56（「3.1.5(2)(b)(イ)その他国際連携による犯罪捜査等の取り組み」参照）。

(3)経済安全保障関連施策の状況

2024年度は、「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※57」（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※58」（以下、重要経済安保情報保護活用法）が成立し、公布され、同法の施行に向けた準備が進められた。本節では、両法に関する2024年度の主な動きを紹介する。

(a)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、2025年5月時点で12の特定重要物資について124件の供給確保計画が認定されている※59。

③に関しては、「経済安全保障重要技術育成プログラム※60」（通称、K Program）において、サイバーセキュリティに関係が深い技術の研究開発構想が策定されている。2024年度は、個別研究型の「人工知能（AI）が浸透するデータ駆動型の経済社会に必要なAIセキュリティ技術の確立※61」について4件※62、「サプライチェーンセキュリティに関する不正機能検証技術の確立（ファームウェア・ソフトウェア）※63」について4件※64、「セキュアなデータ流通を支える暗号関連技術（高機能暗号）※65」について5件※66、「偽情報分析に係る技術の開発※67」について1件※68の研究開発課題（テーマ）が新規採択された。またプロジェクト型の「先進的サイバー防御機能・分析能力強化※69」については、4件のテーマが採択された※70。

2024年5月には、②の制度の運用が開始されるとともに、④の制度が開始された。④の制度により、特許出願の明細書等に、公にすることにより外部から行われる行為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発明が記載されていた場合には、「保全指定」という手続きにより、出願公開や特許査定等の特許手続きが留保されるとともに、発明の内容の開示が原則禁止され、発明の実施も許可制となり、機微な技術の公開や情報流出が防止される。特許出願を非公開にするかどうか（保全指定をするか否か）の審査は、特許庁による第一次審査と内閣府による保全審査（第二次審査）の2段階に分けて行われる。このうち、第一次審査では、特許出願の中から、政令で定められた「特定技術分野※71」に属する発明が記載されている出願を選別して内閣総理大臣（内閣府）に出願書類を送付する。特定技術分野には、サイバーセキュリティと関係が深いものとして、耐タンパ性ハウジングにより計算機の部品等を保護する技術及び通信妨害等に関する技術が含まれている。両技術を含む特定技術分野の一部の技術に関して、2025年3月、内閣府が産業の発達への影響に関する調査結果を発表した※72。

(b)重要経済安保情報保護活用法

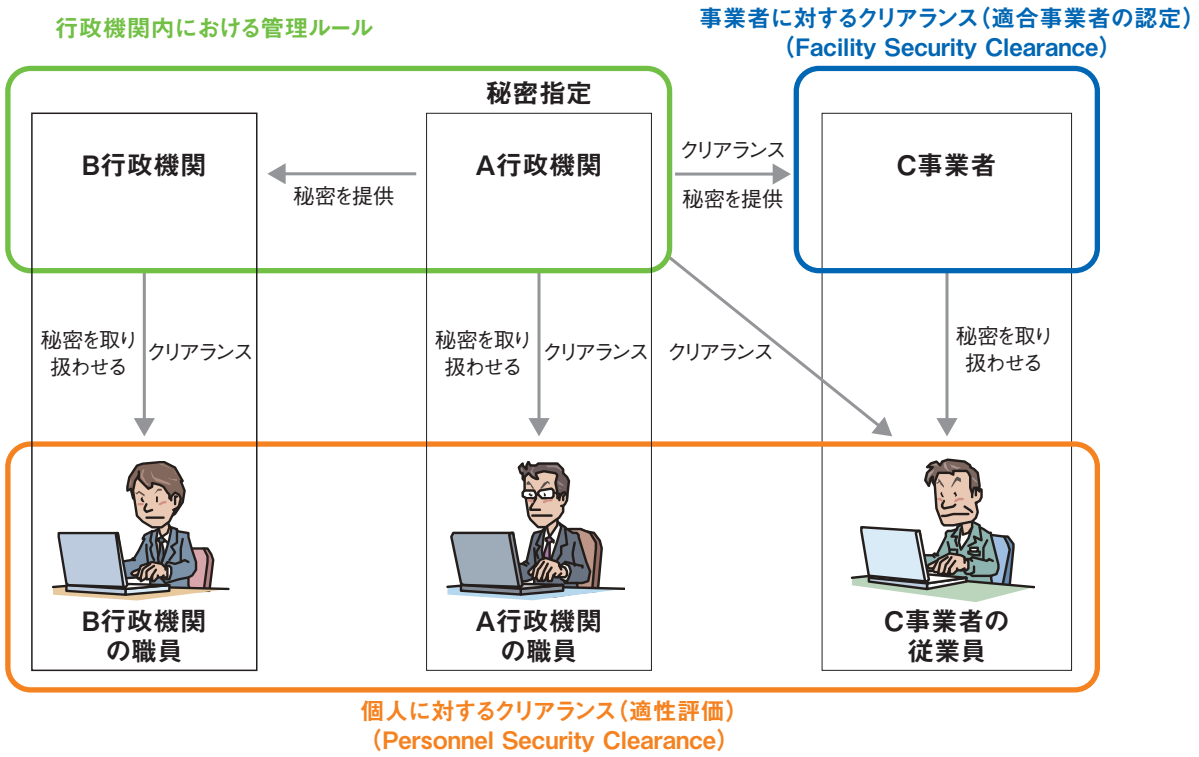
2024年1月に公表された「経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議」の「最終とりまとめ※73」により、経済安全保障分野におけるセキュリティ・クリアランス制度※74の創設が提言された。これを受けて、2024年5月に重要経済安保情報保護活用法が成立し※75、同月公布され、2025年5月に施行された。

図3-1-6（次ページ）は、同法に基づく重要経済安保情報の提供の流れの概略図である。

同法は、①重要経済安保情報の指定、②重要経済安保情報の提供、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。概要は、以下のとおりである※77。

①重要経済安保情報の指定

行政機関の長は、重要経済基盤（重要なインフラや物資のサプライチェーン）に関する一定の情報であって、公になっていないもののうち、その漏えいが我が国の安全保障に支障を与えるおそれがあるため、特に秘匿する必要があるものを、「重要経済安保情報」として指定する。重要経済安保情報の具体例としては、サイバー脅威・対策等に関する情報や、サプライチェーン上の脆弱性関連情報が想定されている。指定の有効期間は5年以内で、原則30年まで延長可能である。行政機関の長は、重要経済安保情報の取り扱い業務を行わせる職員の範囲を定める等の



■図 3-1-6　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※76」を基に IPA が編集

保護措置を講ずることとされている。

②重要経済安保情報の提供

行政機関の長は、必要に応じて他の行政機関等（外国の政府を含む）に重要経済安保情報を提供できる。我が国の安全保障に著しい支障を及ぼすおそれがないと認めるとき等は、国会や裁判所等にも提供できる。また、重要経済基盤の脆弱性の解消等我が国の安全保障の確保に資する活動を促すため、必要があると認めたときは、適合事業者（政令で定める基準に適合する事業者）との契約に基づき、重要経済安保情報を提供することも可能となっている。

③重要経済安保情報の取扱者の制限

重要経済安保情報の取り扱いの業務は、適性評価において重要経済安保情報を漏えいするおそれがないと認められた者に制限される。なお、特定秘密保護法による適性評価において特定秘密の取り扱いの業務を行った場合にこれを漏らすおそれがないと認められた者は、重要経済安保情報の取り扱いの業務を行うことができるとされている。

④適性評価

行政機関の長は、重要経済安保情報の取り扱いの業務を行うことが見込まれる行政機関の職員又は適合事業者の従業員について、本人の同意を得た上で、内閣総理大臣による調査の結果に基づき漏えいのおそれがないことについての評価（適性評価）を行う。適性評価の有効期間は 10 年である。調査内容は、重要経済基盤毀損活動との関係に関する事項、犯罪及び懲戒の経歴に関する事項、情報の取り扱いに係る非違の経歴に関する事項、薬物の濫用及び影響に関する事項、精神疾患に関する事項、飲酒についての節度に関する事項、及び信用状態その他の経済的な状況に関する事項の七つとされている。

なお、評価対象者が他の行政機関の長が直近に実施した適性評価（10 年を経過していないものに限る）において漏えいのおそれがないと認められた者である場合には、改めて調査することなく適性評価を実施可能とされている。

⑤罰則

重要経済安保情報の漏えい時に、5 年以下の拘禁刑若しくは 500 万円以下の罰金またはこれを併科する罰則等が規定されている。

2025 年 1 月、同法第 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※78」（運用基準）が閣議決定された。運用

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、法定の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。

3.1.2 デジタル庁の政策

デジタル庁では、「デジタル社会推進標準ガイドライン」群のセキュリティに関するドキュメントの策定・改訂や、政府情報システムに係るセキュリティガバナンスの構築・維持に資する情報システムの整備を行っている。

(1)「デジタル社会推進標準ガイドライン」群におけるセキュリティに関するドキュメントの策定・改訂

デジタル庁では、府省庁におけるサービス・業務改革並びにこれらに伴う政府情報システムの整備及び管理についての手続き・手順や、各種技術標準等に関する共通ルール及び参考ドキュメントである「デジタル社会推進標準ガイドライン」群をまとめている。そのうちセキュリティに関するドキュメントとしては、10 本のドキュメント（ガイドライン、適用方針、エンタープライズアーキテクチャ、技術レポート）を公開している※79。

2024 年には、猛威を振るうサプライチェーン・リスクへの対応や既存ドキュメント利用者のより一層の理解を促進し、政府情報システムのセキュリティ強化に資することを目的として、以下のドキュメントの策定・改訂を行った。

(a)「政府情報システムにおけるサイバーセキュリティに係るサプライチェーン・リスクの課題整理及びその対策のグッドプラクティス集」の策定

情報システムの構築・運用・保守では、外部事業者（サードパーティー、クラウドサービス、業務委託等）を活用することが多いが、これらはすべてサプライチェーンの一部である。昨今、クラウドサービスの利用等によりサプライチェーンが一層拡大していることもあり、サプライチェーンに起因するセキュリティインシデントも多発している。

「政府情報システムにおけるサイバーセキュリティに係るサプライチェーン・リスクの課題整理 及び その対策のグッドプラクティス集※80」では、サプライチェーン・リスクを含めた網羅的なセキュリティ対策はこれまでどおり「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群※81」（以下、政府統一基準群）をベースラインとしつつ、サプライチェーン・リスクに起因する大規模な攻撃や事故等に備えて、自組織やシステムだけでなく、サプライチェーン全体を考慮したリスクを管理し、対策するための課題整理とその対策のグッドプラクティスを示した。

同グッドプラクティス集では、政府情報システムに想定される主要なサプライチェーン・リスクを、以下のとおり定義している。

- ビジネスサプライチェーン・リスク
  政府情報システムの開発・運用・保守等の業務を請け負う委託先や再委託先（それ以降も同様）に関連する、内部不正による情報漏えいやマルウェア感染等のサイバー攻撃を受けることによる業務停止等のセキュリティリスク
- サービスサプライチェーン・リスク
  政府情報システム等で利用する事業者によって提供されるクラウドサービスに関連する情報漏えい、業務停止等のセキュリティリスク
- 機器・ソフトウェアサプライチェーン・リスク
  政府情報システムで利用するハードウェアやソフトウェアに含まれるバックドアや致命的な脆弱性が悪用され、システムへの不正アクセスやマルウェア感染等のサイバー攻撃を受けることによる、情報漏えい、業務停止等のセキュリティリスク

これらの異なる領域にまたがるサプライチェーン・リスクや、様々なセキュリティリスクを含めた政府情報システムに係るリスク全体に関する総合的なリスクアセスメントを確実に実施することが重要であること、特に、業務委託先やクラウドプロバイダー等の外部の関係者が関与する場合、その相手先でのセキュリティ対策等を適切に把握することが求められることから、委託先、サプライヤー、サービス提供者等との緊密な協力が不可欠であることを、同グッドプラクティス集のグッドプラクティスは示している。

また、サプライチェーン・リスクは動的なものであり、技術の進化や新たな脅威の発生によりリスクの性質や影響範囲が変化することがあることから、初回のリスク評価や対策実施にとどまらず、継続的な監視と再評価を行うことの重要性を示している。

更に、同グッドプラクティス集は、サプライチェーン・リ

スクが顕在化した場合の対応を適切に行うために、あらかじめインシデント対応計画を整備することとし、その対応計画の中でインシデントの検知、報告、対応、復旧の手順を明確に定め、委託先等の関係者との協力体制を整備しておく必要性を説明している。これらの取り組みにより、より堅牢なサプライチェーン・リスク管理体制を構築し、政府情報システムにおけるセキュリティ水準の向上に努めることが期待される。

(b)「CI/CD パイプラインにおけるセキュリティの留意点に関する技術レポート」の改訂

昨今のモダン技術を基に構築されたモダンアプリケーションにおいて、開発のサイクルを自動化する CI/CD パイプラインは、開発プロセスやセキュリティ対策を最適化させる上で欠かせない情報システム・コンポーネントである。「CI/CD パイプラインにおけるセキュリティの留意点に関する技術レポート[※82]」では、CI/CD パイプラインをセキュリティの観点から解説し、保護策を検討する際のポイントについて説明している。

今回、同技術レポートに「別添 . CI/CD パイプラインによる Infrastructure as Code 実装例[※83]」を追加した。同実装例では、AWS（Amazon Web Services）上で稼働する政府情報システムが、その AWS リソースを Infrastructure as Code ツール「Terraform」によって構成管理され、そして CI/CD パイプラインツール「GitHub Actions」を用いて自動適用されている状況を想定した実装例を紹介している。

同実装例では、CI/CD パイプラインのサーバーやネットワーク等のインフラ構成管理と自動化ツールの提供を担当するプラットフォームチームと、アプリケーションのコード開発とテスト、デプロイメントを担当するサービスチームのそれぞれの観点から、具体的なシナリオを基に各要素の実例を示している。

図 3-1-7 にプラットフォームチームの CI/CD パイプライン概要図を示す。

プラットフォームチームの CI/CD パイプラインでは、プラットフォームチームが一元的に管理する Terraform バイナリー及び AWS プロバイダーを、サービスチームに提供できる状態を想定している。これは、複数チームで共通利用されるソフトウェアに対する個別のセキュリティチェックをプラットフォームチームが担うことで、ルールへの準拠がより実行的になる効果を期待している。

図 3-1-8（次ページ）にサービスチームの CI/CD パイプライン概要図を示す。

サービスチームは、AWS リソースの構成を Terraform ファイルに定義し管理する。これを自動化するのがサービスチームの CI/CD パイプラインである。これは、プラットフォームチームの CI/CD パイプラインの成果物であるコンテナイメージと AWS の各種シークレット情報を用いて、Terraform ファイルの内容を AWS に反映している。

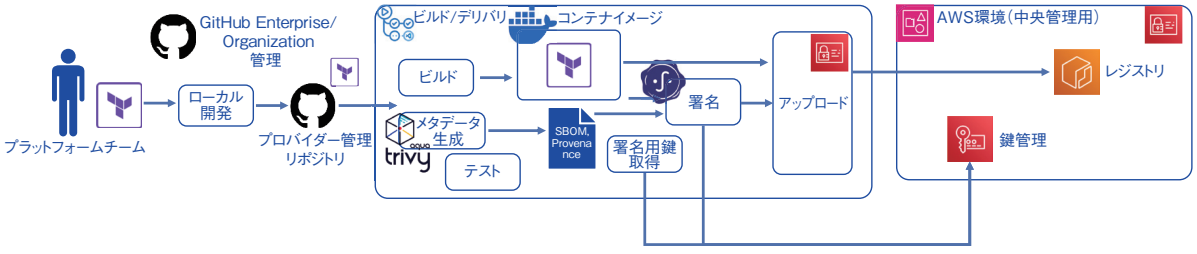
同実装例はあくまで保護策の全体的な実装例であり、実運用環境では、全体的なリスクやパフォーマンス等の機能・非機能要件を基に、保護策の要否、粒度、強度を決定し、ツールを選定することを求めている。

(2) 総合運用・監視システム（COSMOS）の整備

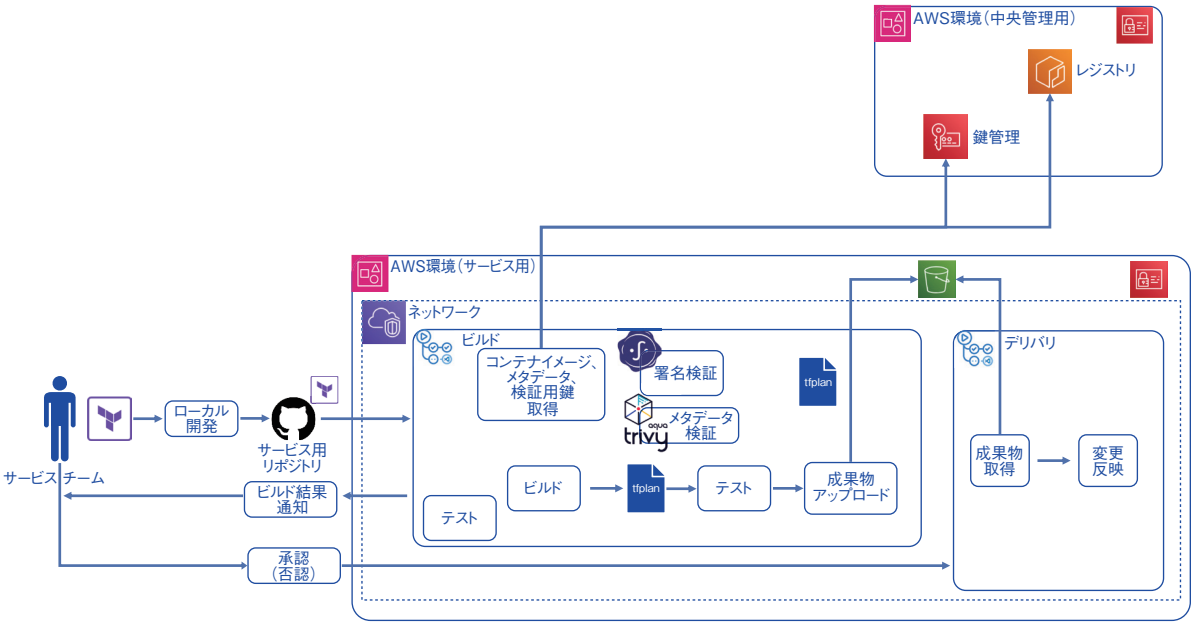
デジタル庁における総合運用監視は、デジタル庁の整備する政府情報システム全体のサービス提供状況の把握を行いつつ、内部監査人協会（IIA：The Institute of Internal Auditors）の 3 ラインモデル[※84] における第 2 ライン及び第 3 ラインの役割から各システムの IT マネジメントを支援する仕組みである。デジタル庁におけるシステム全体のサービス稼働状況を横断して一元的に把握する総合運用・監視システム（COSMOS）を構築・運用することで、デジタル庁の IT ガバナンスの実現を目指す（次ページ図 3-1-9）。

総合運用・監視システムは、デジタル庁が管理する政府情報システムを対象として各システムへの外形監視を行う。総合運用監視の目的・役割について紹介する。

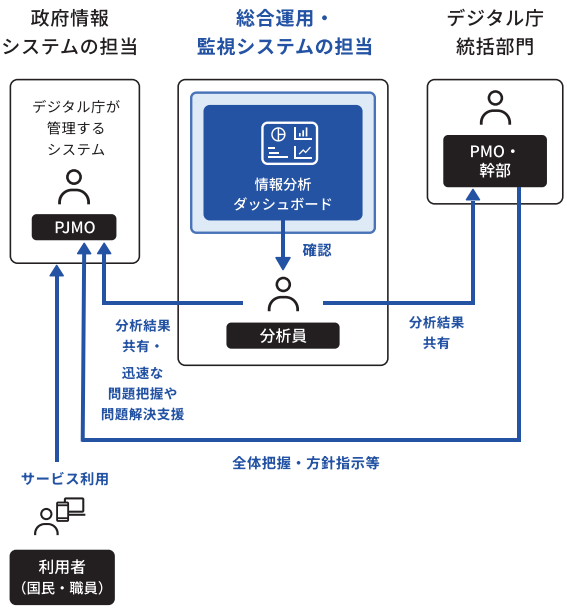
- 総合運用監視によるデジタル庁の IT ガバナンス向上



■図 3-1-7　プラットフォームチームの CI/CD パイプライン概観
（出典）デジタル庁「別添 . CI/CD パイプラインによる Infrastructure as Code 実装例」



■図 3-1-8　サービスチームの CI/CD パイプライン概観
（出典）デジタル庁「別添 . CI/CD パイプラインによる Infrastructure as Code 実装例」



■図 3-1-9　総合運用・監視システム概要図
（出典）デジタル庁「IT ガバナンスを確保するための総合運用監視※85」

政府情報システムの提供サービスが（インターネットや外部サービスを含む）複数のシステムで構成される等、各システムの運用者では提供サービスへの影響が把握しづらい場合に支援できるように、総合的な手法でデジタル庁の異なるシステムの運用状況を全体的・継続的に監視する。

- 利用者視点及び客観的なサービス提供状況の把握
  各システムの運用者は、利用者に対するサービス提供やリスク管理等を担う第 1 ラインとしてのシステム稼働の状況把握をしている。総合運用監視では、システム稼働に加え、利用者視点でのサービス提供の状況を把握する。そのため、総合運用監視は、第 1 ラインを支援する第 2 ライン／第 3 ラインとして各システムの運用者から独立的・客観的にサービス提供の状況を把握する。
- インシデント発生時のデジタル庁全体の対応支援
  インシデント発生時に影響の範囲やシステムの関連性を特定することを支援する。これにより、インシデントが発生した各システムの運用者と連携し、デジタル庁全体としてインシデント対応を迅速かつ効果的に行う。
- 各システムの運用品質のレベルの向上
  独立的・客観的にサービス提供状況を把握し、各システムの運用者に定期的にフィードバックする。サービス提供状況のフィードバックにより、各システムの運用者による運用品質レベルの向上を図る。

(3) 常時リスク診断・対処（CRSA）システムの整備

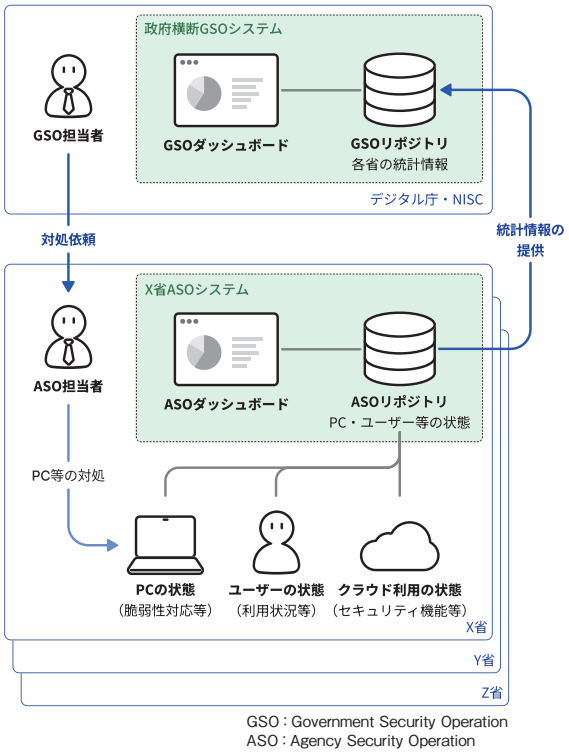
CRSA（Continuous Risk Scoring & Action：常時リスク診断・対処）とは、組織のセキュリティポリシー等に準拠するために情報システムに導入された必要なコントロール（管理策）に関して、以下を実施するものである。

- リスク診断：必要なコントロールと実際の状態とのギャップやリスクを可視化
- 対処：可視化されたギャップやリスクの是正対応

- 常時：ギャップやリスクの可視化と是正対応を継続的に実施

デジタル庁は、2024 年度に CRSA の概念に基づき、組織のネットワークとシステムのサイバーセキュリティを強化するための仕組みを提供する CRSA システムを整備した。

これにより、組織の資産に関する情報を収集し、資産の構成及びソフトウェアコンポーネントに更新を適用するといった潜在的リスクの是正活動を支援し、情報システムの運用等においてセキュリティポリシー等からの逸脱を発見し、適時適切に対処することを可能とする（図 3-1-10）。



■図 3-1-10　CRSA システム概要図
（出典）デジタル庁「常時リスク診断・対処（CRSA）※86」

CRSA システム導入の目的と効果は以下のとおりである。

- 政府統一基準群等に準拠したコントロール（管理策）からの逸脱の迅速な把握と是正対応
  サイバーセキュリティ対策に必要なコントロールの実施状況を継続的にモニタリングし、どこが不適切な状態になっているかを迅速に把握し、是正対応を実施する。
- インシデント発生時のトリアージ等の効果的な対応
  リアルタイムに自組織の資産状況、脆弱性対応状況等を把握し、インシデント発生時の資産等への影響規模や対応の優先度について迅速に判断する。
- リアルタイムデータによるセキュリティ対策実施状況の効率的な報告
  CRSA システムを導入した組織は、リアルタイムな資産状態、アカウントの利用状況、インシデントの発生状況等を把握できる。これにより、サイバーセキュリティ対策状況を客観的かつ効率的に報告可能とする。政府全体としては、各組織のサイバーセキュリティ対策状況を各組織に負担をかけることなく効率的に把握可能とする。
- 脅威やインシデントに対する政府横断的な脆弱箇所の迅速な発見と是正対応
  特定の脅威情報やインシデントに関する情報を基に、影響のある箇所やインシデントの発生する可能性のある箇所を政府横断的に特定し、迅速かつ効果的に対処可能とする。
- ゼロトラストアーキテクチャの運用環境を適切に維持
  ゼロトラストアーキテクチャの具体的な実装・運用において、CRSA システムの診断結果をポリシーエンジンのインプット情報として活用する。

3.1.3 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※87。

- WG1（実効性強化・国際連携）
  - 分野横断 SWG
  - 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

- 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2024年4月5日に第8回会合を開催し、今後の産業サイバーセキュリティ政策について議論を行った。2025年5月23日には第9回会合を開催し、施策の進捗状況が確認された※88。以下では、2024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

経済産業省は、半導体関連産業のサイバーセキュリティ対策のため、2024年11月にWG1に「半導体産業SWG」を設置し、我が国の半導体産業におけるサイバーセキュリティの在り方や守るべき対象技術等を議論するとともに、サイバーセキュリティ対策への取り組み、問題意識や事例等、相互に情報共有を行っている※89。

同SWGでは、国内の半導体産業におけるセキュリティ対策状況等を踏まえた工場セキュリティ対策の指針を示すため、「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」の策定に向け議論している。同ガイドラインは、最も高度な攻撃者（国家の支援を受けたグループ）を想定した対策レベルを実現するために、「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）※90」や「The NIST Cybersecurity Framework（CSF）2.0※91」等リスクベースのサイバーセキュリティフレームワークを活用したリスク分析、及び具体的な対策を検討する際等に活用されることが想定される。

また経済産業省は、サプライチェーンに起因するインシデントへの対策を強化するため、2024年7月、WG1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SWG※92」を設置し、対策状況を可視化し企業の対策決定を容易・適切なものにする仕組みである「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」の制定を目指し議論を行っている。同SWGは2025年4月14日に「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構築に向けた中間取りまとめ※93」を公表し、現状の構想を取りまとめた。同制度は2025年度の実証事業を踏まえた上で、2026年度の運用開始を目指す。

そのほか、WG1の「電力SWG」は、2025年2月4日に第18回会合※94を開催し、サプライチェーン・リスクへの対応、分散型電源のサイバーセキュリティ、電力システムにおけるサイバーセキュリティリスク点検ツールの活用について議論し、サプライチェーン・リスクへの対策に関する手引き文書の策定を目指している。

WG1の「工場SWG」は、2025年3月4日に第8回会合※95を開催し、2022年11月16日に第1.0版が公表された「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※96」の改訂及び、より利用しやすいAppendixの作成を目指し議論を行った（新規Appendixは2025年4月11日に公表）。

(b) セキュア・バイ・デザインの実践

経済産業省は、IoT製品やソフトウェアでのセキュア・バイ・デザインの実践を推進する観点から、以下の検討・取り組みを行っている。

WG3の「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」では、IoT製品を対象として、一定水準のセキュリティ要件に対するセキュリティ対策の適合性を評価し、その結果を調達者・利用者が分かる形で可視化する制度を策定するため議論を行ってきた。それを踏まえ、2024年8月に経済産業省は「IoT製品に対するセキュリティ適合性評価制度構築方針※97」を公表した。この方針を基にして、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）」の運用を開始した（「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）。

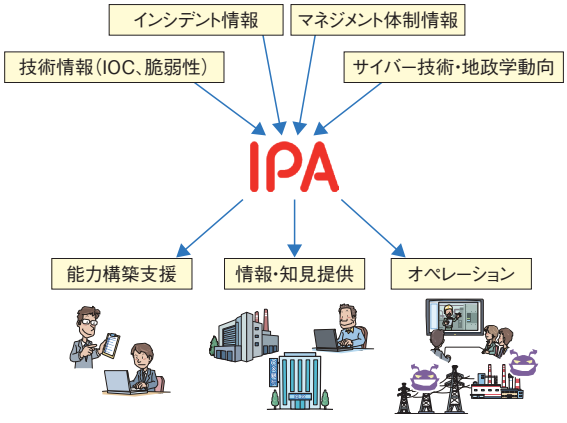
WG1の「分野横断SWG」で活動している「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース」（以下、ソフトウェアTF）では、オープンソースソフトウェア（OSS：Open Source Software）等のソフトウェアの活用・脆弱性管理手法を検討している。ソフトウェアTFは、2024年8月29日に「ソフトウェア管理に向けたSBOM（Software Bill of

Materials）の導入に関する手引 ver 2.0」を公開した※98。改訂版となる同手引は、ソフトウェアを供給する企業と調達する企業の双方を想定読者とし、中小企業も含め、あらゆる企業にとって SBOM をより効率的に活用できる方法等として、脆弱性管理プロセスの具体化、SBOM 対応モデル、SBOM 取引モデル等を新たな内容として盛り込んでいる。2025 年 3 月 4 日には第 15 回会合※99を開催し、経済産業省はそこでの議論を基に、ソフトウェアのセキュア開発のための標準である「セキュア・ソフトウェア開発フレームワーク（SSDF：Secure Software Development Framework）※100」を組織・プロジェクトの現場に導入するための具体的な方法や手順を示す「セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス案（中間整理）※101」を提示した。また WG1 は、政府機関等及び重要インフラ事業者を始め広く社会で活用される情報・通信システム、ソフトウェア製品及び ICT サービスを開発し提供する「サイバーインフラ事業者」を対象としたセキュリティガイドラインとして、「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（案）※102」を提示した。

（c）政府全体でのサイバーセキュリティ対応体制の強化

経済産業省は、「サイバー状況把握力」の強化により国家安全保障戦略に基づく対応を強化すべく、以下の取り組みを行っている。

- IPA が有する産業界とのネットワーク、セキュリティ対策制度を駆使した産業分野のセキュリティ・リスク情報（サイバーインテリジェンス）集約のハブとしての機能強化（図 3-1-11）
- 経済活動に影響を及ぼすサイバーリスクを統合的に分析することによる、産業分野に関する脅威評価のハブとしての機能を追加
- J-CRAT を活用した、防御や抑止対応に資する情報共有／対応支援活動のハブとしての活動推進（「3.1.3（3）（b）J-CRAT（サイバーレスキュー隊）」参照）
- サイバー事案の対処及びサイバー脅威情報等の共有等に関する包括的な連携（「3.1.3（4）（c）サイバー事案の対処及びサイバー脅威情報等の共有等に関する包括的な連携」参照）



■図 3-1-11　IPA におけるサイバー情報集約・情勢分析能力の強化
（出典）経済産業省「第9回 産業サイバーセキュリティ研究会 事務局説明資料※31」を基に IPA が編集

今後、経済インテリジェンス収集力の強化等によりサイバー情報の集約・情勢分析機能や対処支援能力の一層の強化を図るとともに、第 217 回通常国会で成立したサイバー対処能力強化法に基づく業務への対応により、政府全体のサイバー安全保障体制の強化に貢献していく。

（d）サイバーセキュリティ供給能力の強化

経済産業省は、国内のセキュリティ企業の強化のため、2024 年 7 月、WG3 に「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※103」を設置し、サイバーセキュリティビジネスの振興のための方策について議論を行っている。

国産のサイバーセキュリティ製品・サービスが創出される環境を作るための包括的な政策パッケージとして、同検討会での議論を踏まえ、経済産業省は 2025 年 3 月 5 日に「サイバーセキュリティ産業振興戦略※104」を発表した。サイバーセキュリティ産業のマーケットには、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現状や、導入実績が重視される商慣習、十分に開発投資が行われにくい事業環境といった課題が存在している。「サイバーセキュリティ産業振興戦略」では、政府機関等がスタートアップの製品・サービスを試行的に活用することで製品開発の出口を確保し、技術力・競争力強化の支援やベンダー・SIer 間の共同のための枠組みの構築を行うことにより、国内マーケットを拡大し、安全保障の確保やデジタル赤字の解消を目指す。経済産業省では、今後、予算編成等を踏まえ取り組みの具体化を図る。

また経済産業省は、産業界のサイバーセキュリティ対策の強化のため、2024 年 7 月、WG2 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※105」を設置し、セキュリティ人材のすそ野を拡大するための施策について議論を行っている。

同検討会ではサイバーセキュリティ人材不足への対応として、特に以下の 3 点について重点的に検討をしてい

る（「3.2.1 サイバーセキュリティ人材の現状と育成状況」参照）。

- セキュリティ・キャンプの拡充
- 情報処理安全確保支援士（登録セキスペ）の活用及び制度の見直し
- 中堅・中小企業等の内部でセキュリティ対策を推進する者の確保に向けた新たな施策

(2) 技術情報管理認証制度

経済産業省は「産業競争力強化法等の一部を改正する法律」に基づき、2018 年 9 月から「技術情報管理認証制度」を開始している※106。これは、事業者の技術等の情報管理について、国が示す認証基準に適合していることを、事業所管大臣及び経済産業大臣が認定した認証機関が認証を付与する制度である。2024 年 8 月 16 日に「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※107」が改正され、認証の基準が更新された。この改正により、企業が取り組むべき内容を更新・明確化した。引き続き機密性の高い技術情報等を保持する中小企業や業界団体等による同制度の活用が期待される。

(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※108）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（次ページ図 3-1-12）。

2025 年 3 月には、新たに半導体業界 SIG、同年 4 月には、暗号資産交換業界情報連携体制が発足し、2025 年 7 月 1 日現在、IPA を情報の中継・集約点（情報ハブ）として 17 の業界から 320 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。

2024 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。

これらの情報共有の中には、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、以前から観測されている、特定の業界や組織を標的としたメールによる攻撃も含まれている。

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。

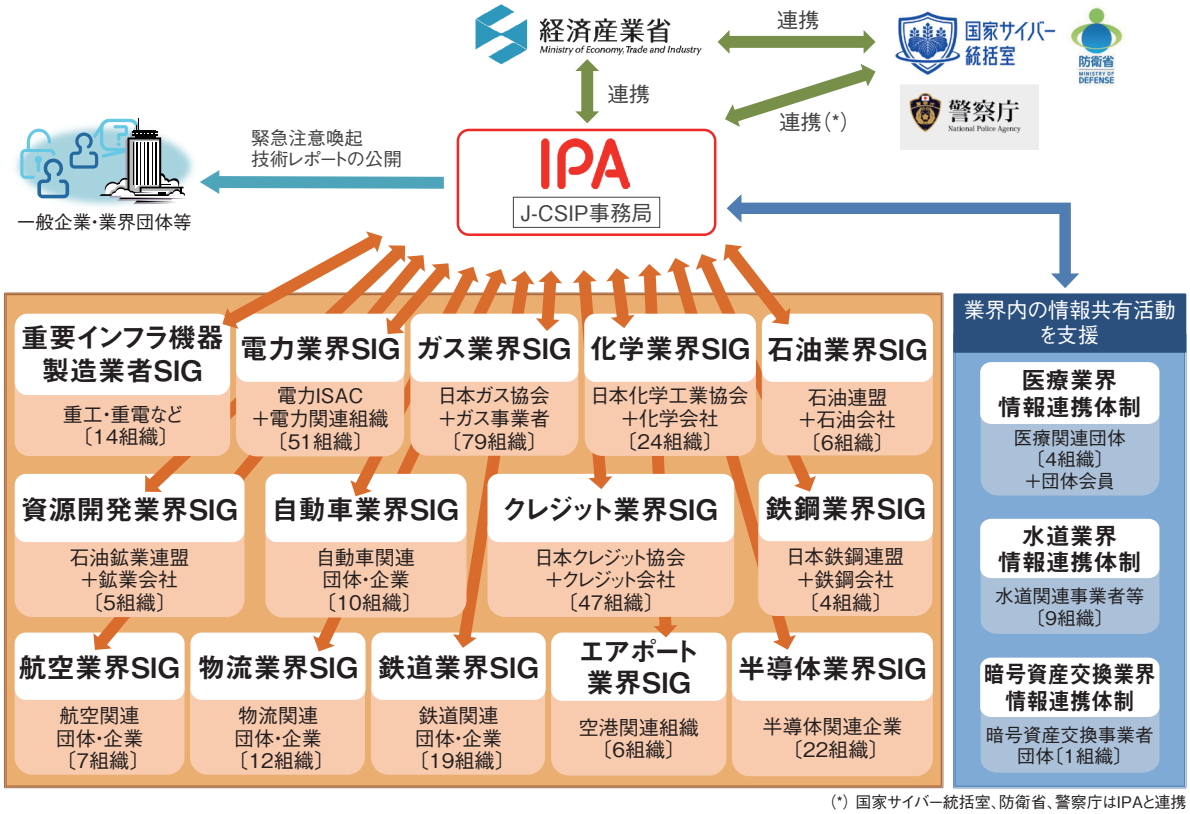
(b) J-CRAT（サイバーレスキュー隊）

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）※110」を発足させた。J-CRAT の目的を以下に示す。

- 攻撃に気付いた組織における被害拡大と再発の抑止・低減
- 標的型攻撃による諜報活動等の連鎖の遮断

J-CRAT では、常時「標的型サイバー攻撃特別相談窓口※111」（以下、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。

窓口では、主に公的機関等の組織から、標的型攻撃メールに関する情報提供や相談を受け付けている。「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、各種マルウェア情報等を収集している。これまでの活動実績から、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



(*) 国家サイバー統括室、防衛省、警察庁はIPAと連携

■図 3-1-12　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[※109]」を基に編集

なっているため、それらの情報収集を幅広く行っている。

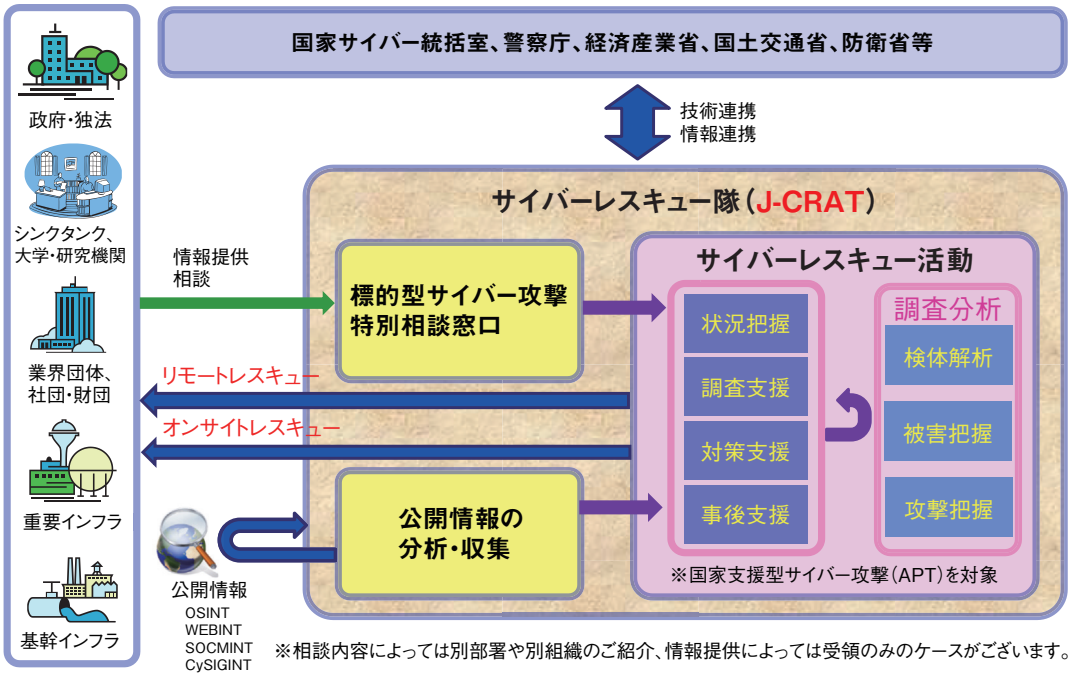
標的型攻撃の被害に遭っている、または遭っている可能性が高い組織のうち、特に公的機関や業界団体、重要インフラ関連企業や取引先等サプライチェーンを構成する組織に対しては、被害実態の確認と認知の支援、被害緩和の暫定対応に関する助言を「サイバーレスキュー活動」として実施している。また、窓口における対応の結果、必要があると判断した組織に対して、攻撃の期間・内容、感染範囲、想定被害等をヒアリングし、早急な対策着手が行えるよう、「リモートレスキュー」や「オンサイトレスキュー」等によって、民間セキュリティ事業者への移行を前提とした助言を行っている（次ページ図3-1-13)。

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、注意喚起情報等を随時公開している。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、平時における標的型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、標的型攻撃の連鎖の解明、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 7 月に整備された脆弱性関連情報の届出受付制度である。後述する経済産業省の告示のもと、IPA が受付機関、JPCERT/CC が調整機関の役割を担い、運営している。

不正アクセス、マルウェア等による被害発生を抑制するため、脆弱性関連情報が発見された場合に、それらをどのように取り扱うべきかを示した経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」が 2004 年に制定されたことを踏まえ、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」の第 1 版が 2004 年 7 月に制定された。同告示は、2017 年に経済産業省告示「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[※112]」となり、2024 年 6 月に改正された。この改正と「情報システム等の脆弱性情報の取扱いに関する研究会」での検討結果を踏まえ、同ガイドラインについても改訂を行い、2024 年 6



■図 3-1-13　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※110」

月に第 13 版が発行されている※113。

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（例えば、主に日本語で記述された Web サイトや、URL のトップレベルドメインが「jp」の Web サイト等）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 3-1-1 に示す。

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 3-1-1　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※114」を基に編集

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含む）は、製品に関する脆弱性情報を把握し、対策を行い、その製品に対する攻撃のリスクを低減できるようになる。また、システムの企画や開発・設計等で使用する製品の選定に際して、公表情報を参考として活用できるようになる。

パートナーシップの活動の全体像を図 3-1-14（次ページ）に示す。

2024 年にパートナーシップへ届出された脆弱性の届出状況については、「1.2.4（1）（b）早期警戒パートナーシップにおける脆弱性の届出状況」を参照されたい。

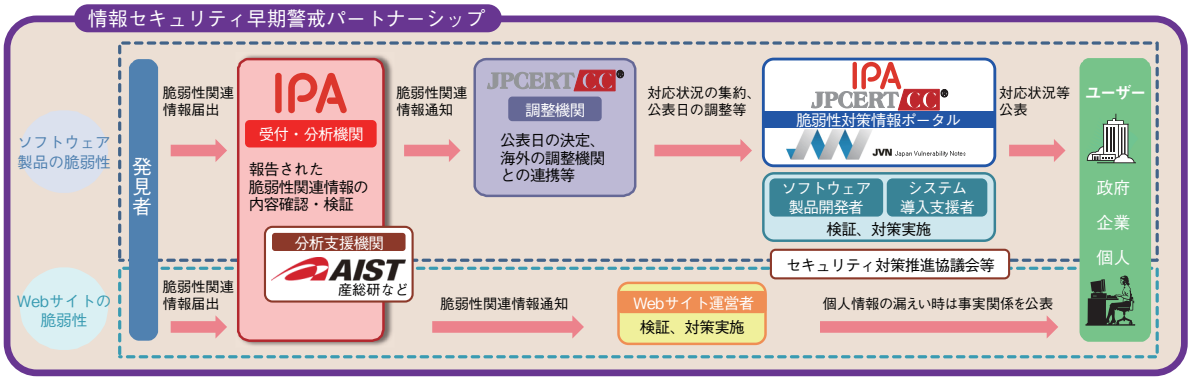
今後も、脆弱性関連情報が関係者の協力のもと、適切に流通、対応、公表されることで、製品利用者や Web サイト運営者が脆弱性を攻撃される可能性を低減することが期待される。

（4）その他の検討会等における活動

他の検討会等における活動について述べる。

（a）AI 事業者ガイドライン検討会

2023 年 10 月、経済産業省は「人間中心の AI 社会原則※115」の実装に向けて、統一的で分かりやすい事業者向けガイドラインを検討するため「AI 事業者ガイドライン検討会※116」を設置した。2024 年 10 月より、経済産業省と IPA AI セーフティ・インスティテュートが同検



※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 3-1-14　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

討会の共同事務局となり運営している。

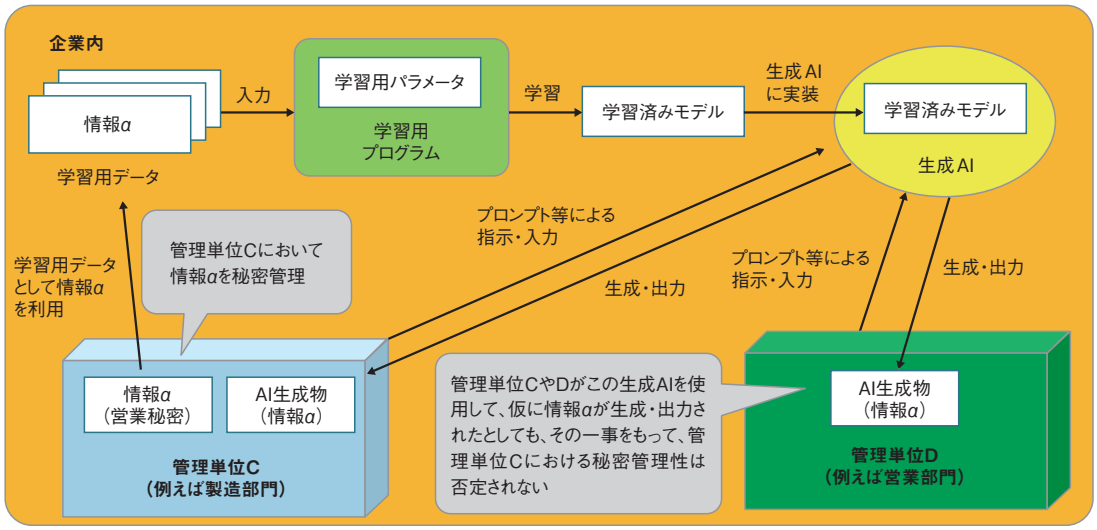
同検討会は、2024 年 4 月に公開された「AI 事業者ガイドライン（第 1.0 版）※117」について、AI をめぐる動向が国際的な議論の進展等目まぐるしく変化する中、AI の安全安心な活用が促進されるよう、改訂を行った。改訂版は、2025 年 3 月に「AI 事業者ガイドライン（第 1.1 版）※118」として総務省と経済産業省から発行された。

(b) 不正競争防止小委員会

経済産業省は、不正競争防止法に関する事項を審議する場として、2017 年 7 月に「産業構造審議会 知的財産分科会 不正競争防止小委員会」を設置し、定期的に議論を行っている※119。

同小委員会は 2025 年 3 月 25 日に第 28 回を開催し、2025 年 3 月 31 日に「営業秘密管理指針※120」を改訂した。営業秘密管理指針は、不正競争防止法により営業秘密として法的保護を受けるために必要となる「最低限の水準の対策」を示すものとして策定された。同指針は、前回改訂である 2019 年 1 月以降の営業秘密を取り巻く環境の変化、及び関連する法制度の見直し、裁判の動向を踏まえて、改訂が行われた。これらの改訂により、クラウド・AI の活用等における営業秘密の要件の解釈が明確化された。以下、営業秘密の 3 要件（秘密管理性、有用性、非公知性）における主な改訂内容を示す。

- 秘密管理性について
  企業における管理実態を踏まえ、秘密管理性及び秘密管理措置について具体化を行った。例えば、営業秘密と他の情報との分別管理を含めた考え方について、「秘密管理措置の程度」の考慮要素の一つに位置付けるとともに、秘密管理措置においては情報セキュリティで求められる措置の程度に達していなくとも、秘密管理措置が認められ得る旨の記載を追記した。また、外部クラウドや生成 AI を利用した具体例についても追記を行った。例えば、企業内で、秘密管理されている情報を生成 AI に利用し、当該情報が同一部門及び別部門において AI 生成物として生成・出力されることがあったとしても、当該情報が秘密管理されているのであれば、そのことの一事をもって秘密管理性が否定されることはないことを明確化した（次ページ図 3-1-15）。
- 有用性の考え方について
  昨今の裁判例を踏まえ、営業秘密の有用性の要件として、当該情報を取得した者がそれを有効に活用できるかどうかに関わらず、事業者の事業活動に使用・利用されているのであれば、有用性の要件が充足されるものであると考えられる旨等を明確化した。
- 非公知性の考え方について
  非公知性の有無の判断についての考え方を明確化した。例えば、第三者からのハッキング等により不正取得された営業秘密が、その後ダークウェブ上に公表されたとしても、その一事をもって直ちに非公知性が喪失するわけではない旨を明確化した。また、AI 学習用データを想定した公知情報を組み合わせたものについて、その組み合わせが知られていなかったり容易に知り得ないため、財産的価値が失われていない場合や、その組み合わせが知られていたり容易であったりしたとしても、取得に要する時間や資金的コストがかかるため財産的価値があるという場合には、非公知と言い得る旨を明確化した。リバースエンジニアリングについては、特殊な技術をもって相当な期間が必要であり、誰でも容易に当該営業秘密を知ることができない場合には、当該製品を市販したことをもって非公知性



■図 3-1-15　生成 AI 利用における秘密管理の参考例
（出典）経済産業省「『営業秘密管理指針』の主な改訂内容一覧※121」

を喪失するとはならないが、誰でもごく簡単に製品を解析することによって営業秘密を取得できるような場合には、当該製品を市販したことによって営業秘密自体を公開したに等しいと考えられることから、非公知性を喪失すると考えられる旨を明確化した。

(c) サイバー事案の対処及びサイバー脅威情報等の共有等に関する包括的な連携

防衛省、経済産業省及び IPA は、2024 年 12 月 27 日に、防衛省・自衛隊を含む我が国のサイバー状況把握力、及びサイバー事案への対処能力の強化、並びにサイバー安全保障の確保に資することを目的として、3 者間での連携を強化すべく、包括的な連携協定を締結した※122。同協定に基づき 3 者間がそれぞれに保有する技術的・専門的な知識を相互に共有し、「自衛隊による IPA の取り組みへの参画等を通じた産業界向けセキュリティ支援」「情報提供等を通じた防衛産業との連携強化」「3 者間の新たな協議体（枠組み）の設置」※123 を進めていく。

(d) クレジット取引セキュリティ対策協議会

同協議会は、クレジットカード取引に関わる事業者が実施すべきセキュリティ対策を定めたガイドラインを改訂し、「クレジットカード・セキュリティガイドライン【6.0 版】※124」を 2025 年 3 月 5 日に公開した。改訂内容として、EC 加盟店における、システムや Web サイトの脆弱性対策や、不正利用対策として EMV 3-D セキュア（カード決済時に本人認証を強化するサービス）の導入、及び不正ログイン対策等のセキュリティ対策の実施が盛り込まれた。

3.1.4 総務省の政策

総務省は「ICT サイバーセキュリティ政策の中期重点方針」（以下、中期重点方針）を 2024 年 7 月 31 日に公表した※125。中期重点方針は、2024 年 2 月にサイバーセキュリティタスクフォースのもとに設置された「ICT サイバーセキュリティ政策分科会」により取りまとめられた。同分科会は我が国のサイバーセキュリティをめぐる環境が今後大きく変化していくことが見込まれることを踏まえ、総務省が中長期的に取り組むべきサイバーセキュリティ施策の方向性について集中的に検討を行うために設置された。「重要インフラ分野におけるサイバーセキュリティ対策強化」「サイバーセキュリティの基盤となる人材育成及び研究開発」「サイバーセキュリティの確保に向けた国際連携及び普及啓発」に関し、総務省が中長期的に取り組むべき施策の方向性が検討され、中期重点方針として「重要インフラ分野等におけるサイバーセキュリティの確保」「サイバー攻撃対処能力の向上と新技術への対応」「地域をはじめとするサイバーセキュリティの底上げに向けた取組」「国際連携の更なる推進」が示された。

以下では、中期重点方針の内容も踏まえつつ、総務省の施策を紹介する。なお、総務省における人材育成に関する施策については、「3.2.3 (2) サイバーセキュリティ人材育成のための活動」を参照いただきたい。

(1) 情報通信ネットワーク・サービスにおけるサイバーセキュリティ確保の取り組み

情報通信ネットワークに大きな影響を及ぼすIoTボットネット対策、安全・安心な通信サービスの利用に向けたスマートフォンアプリのセキュリティ対策、データの改ざんや送信元のなりすまし等を防止する仕組みであるトラストサービス等について2024年度の取り組みを紹介する。

(a) IoTボットネットに対する端末側の対策（新NOTICE）

NOTICE（National Operation Towards IoT Clean Environment）※126は総務省所管のNICTが推進するIoTボットネット対策の一つである。「国立研究開発法人情報通信研究機構法（NICT法）」が2023年12月に改正され※127、新NOTICEでは、従来のIoT機器のパスワードの設定不備を検知、注意喚起する取り組みに加え、ファームウェアに脆弱性を有する機器の調査、感染端末の探索も調査対象となった（「情報セキュリティ白書2024※128」の「2.1.4(1)(a)NOTICEにおける端末（IoT機器）側の調査」参照）。新NOTICEの活動の目的は「IoT機器のセキュリティ対策向上を推進することにより、ボットネットによるサイバー攻撃の発生や被害を未然に防ぐ」ことである。「脆弱なIoT機器の観測能力強化」「IoT機器へのリスクと対策への意識啓発」「メーカーやSIerとの連携強化」の活動を行い、総合的な対処を推進していくという。

2024年度のIoT機器の観測状況を表3-1-2に示す。

種類	件数
容易に推測可能なID・パスワードである機器	18万3,066件
ファームウェアに高リスク脆弱性を有するIoT機器	8万7,005件
マルウェア感染IoT機器検知数	1万5,965件
リフレクション攻撃の踏み台にされうるIoT機器	21万6,852件

■表3-1-2　IoT機器の観測状況（2024年4月～2025年3月）
（出典）NOTICE Webサイト※129を基にIPAが作成

今後は、NOTICEで得られたNICTの知見、ノウハウを活用し、高度な分析情報の提供や重要インフラを対象としたアタックサーフェス（攻撃対象領域）調査に取り組む。

(b) IoTボットネットに対するネットワーク側の対策（C&Cサーバーの検知・対処の推進）

2022～2023年度の2年間のプロジェクトとして、電気通信事業者におけるフロー情報※130の分析によるC&Cサーバー検知技術の有効性検証、及び事業者間の情報共有における課題整理のための実証事業を行った（「情報セキュリティ白書2024」の「2.1.4(1)(b)ネットワーク側やその他における対策」参照）。その結果、分析機能の強化、能動的分析等の新たな手法の導入による、技術的に信頼度の極めて高いC&Cサーバーリストの作成、C&Cサーバーの挙動状況、国別、マルウェアファミリー等の属性の把握等に成功したという。

今後、C&Cサーバーの検出網羅性の向上を目指すためには「迅速かつ精緻なC&Cサーバーリストの作成」「分析事業者の拡大」「統合的な分析」といった取り組みが必要であり、ボットネット縮小を目指すためには、「IoTボットネットの全体像の可視化」「各ボットネットの特性に応じた効果的な対処の実現」が必要であるという。

(c) スマートフォンアプリのセキュリティ対策の推進

スマートフォンに搭載されているアプリについて、利用者の意図しない利用者情報の取り扱いが生じ得る懸念等に対し、2023年度より人気アプリ等を対象に利用者の意図に反したスマートフォンアプリによる情報送信等について技術的な解析を実施し、国内のアプリ解析能力水準に係る課題等の整理が行われた。

また、「スマートフォン利用者情報取扱指針」等を含む「スマートフォン プライバシー イニシアティブ（SPI）」は、2024年11月、セキュリティの確保に係る取り組みの追記等が行われ、「スマートフォン プライバシー セキュリティイニシアティブ（SPSI）」として公表された※131。

(d) データ流通基盤のトラストサービス（eシール）の推進

2024年4月に「eシールに係る指針（第2版）※132」が公表された。同指針ではeシールを以下のように説明している。

- 電子データの出所または起源を示すためのもの
- 電子データについて改変が行われていないかどうかを確認することができるもの

eシールは電子文書等が改ざんされていないことの確認ができ、発行元を証明する。電子署名も電子文書等への暗号化等の措置が行われて以降、当該電子文書等が改ざんされていないことを確認できるという点では同じである。一方、電子署名は自然人※133が電子文書を作成したこと、電子文書に示された意思表示が本人によるものであることを証明するという点で違いがある。テレワーク等の働き方が定着し、官民を問わずあらゆる手

続きを電子的にスムーズに完結させるニーズが増大した。オンライン取引・手続き等において、発行元に関する証明のニーズが高まること等が想定されるため、e シールに係る認証業務の民間サービスの信頼性を評価する基準策定及び適合性評価の実現に向けた検討を行い、2025 年 3 月に「e シールに係る認証業務の認定に関する規程※134」（令和 7 年総務省告示第 113 号）により国（総務大臣）による認定制度を創設した。

(2) サイバー攻撃対処能力の向上の取り組み

サイバー攻撃対処能力の向上を目指す実証事業、体制強化の取り組みを紹介する。

(a) CYXROSS

「CYXROSS」はサイバーセキュリティ情報の収集、分析等を行う実証事業である。安全性、透明性の検証が可能な NICT 開発のセンサー「CYXROSS Agent」を各省庁の端末に導入し、得られたマルウェア情報等を NICT の「CYNEX」（「3.2.3 (2) (b) CYNEX」参照）で組織横断的な情報分析を行い、デジタル庁、NISC、各省庁等に情報共有する※135（図 3-1-16）。CYXROSS の取り組みの意義は、「自国の健康診断は自国の技術で」行うことにあり、国産技術による政府端末情報収集、複数省庁が連携する横断分析環境の確立、日本の情勢分析能力強化を挙げている。2024 年までに CYXROSS Agent Ver1.0 の実装が完了し、オペレーションルーム「CYXROSS CORE」の運用を開始した。また、総務省の端末への導入を開始し、今後政府全体の端末への導入を拡大する。更に、CYXROSS を GSOC※136 と連携させ、NICT の継続的な実務として取り組むことで、エンドポイントを含む政府システムの一元的な監視体制の構築に貢献する予定である。

(b) 研究開発等を担う NICT の体制強化の取り組み

サイバーセキュリティ分野における研究開発能力の強化に向けて、大きな影響力を有する米国との連携を深化させるため、NICT 内に米国の政府機関や研究組織とのサイバーセキュリティ技術に関する国際的な結節点を形成し、共同研究や人材交流、情報の共有や発信等を戦略的に活性化させる必要があるという。

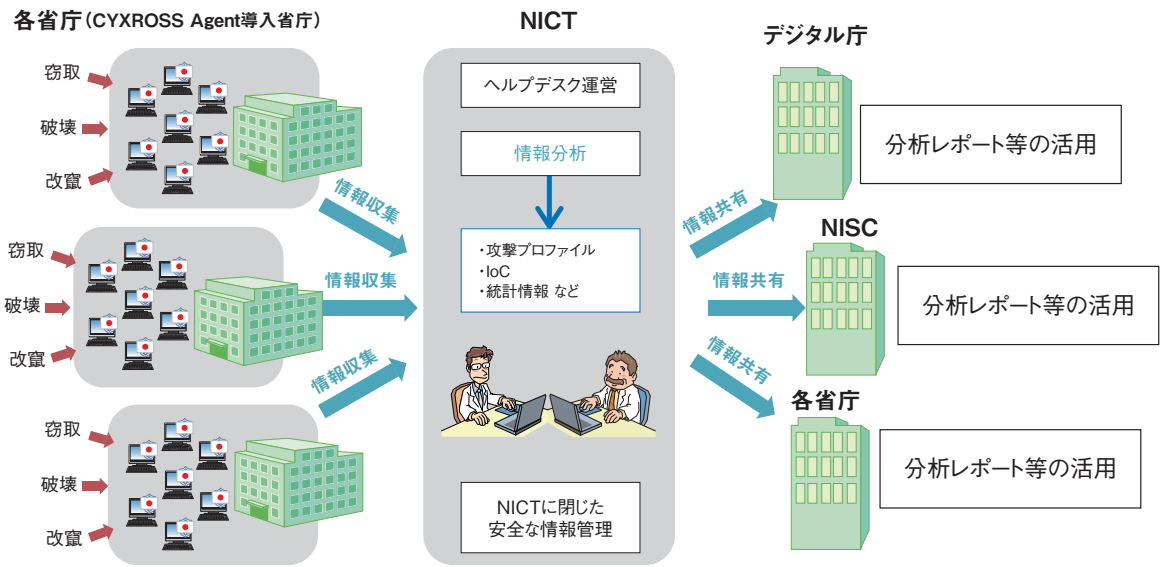
(3) ガイドライン改訂の取り組み

総務省では、日常生活にネットサービスの利用が不可欠な現代社会において、安全にサービスが利用できるよう各種ガイドラインの整備とその普及に努めている。ここでは 2024 年度に改定されたセキュリティに関するガイドラインを紹介する。

(a) スマートシティセキュリティガイドラインの改訂

2024 年 6 月 28 日、「スマートシティセキュリティガイドライン（第 3.0 版）」が公表された※137。同ガイドラインは地域 DX や地域活性化にもつながるスマートシティのセキュリティ確保のため策定されている。目的は以下のとおりである。

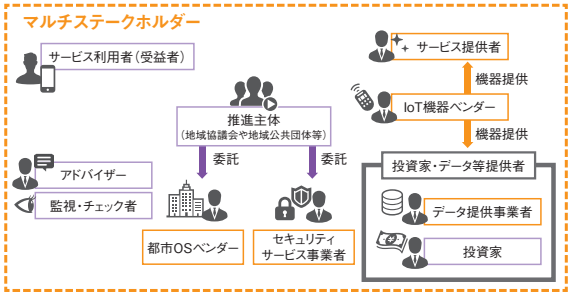
- スマートシティの推進に関わるあらゆる主体において、セキュリティの観点でスマートシティの構造を把握する。



■図 3-1-16　CYXROSS 実証事業の全体イメージ
（出典）NICT「NICT サイバーセキュリティ研究所の取り組み※135」を基に IPA が編集

- 各関係主体が、スマートシティを構成する各要素のセキュリティ上のリスク及び実施すべきセキュリティ対策を把握する。
- 各関係主体が、スマートシティの特徴を踏まえたスマートシティ横断的なセキュリティ上のリスク及び実施すべきセキュリティ対策を把握する。

なお、同ガイドラインでは関係主体を以下の図 3-1-17 のとおり定義し、想定読者を地域協議会、地域公共団体等の推進主体、推進主体と連携しセキュリティ対策の実施が求められるサービス提供者、及び都市 OS ベンダー等としている。



■図 3-1-17　ガイドラインで定義する関係主体のイメージ
（出典）総務省「スマートシティセキュリティガイドライン（第 3.0 版）※138」を基に IPA が編集

(b) 地方公共団体におけるサイバーセキュリティ対策

総務省は、地方公共団体に対し「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」を示している。直近では、以下のポイントについて改定を行い、「令和 7 年 3 月版」として 2025 年 3 月 28 日に公表した※139。

- マイナンバー利用事務系に係る画面転送の方式について
- 無線 LAN 利用の要件について
- 機器等の調達について
- インシデントの対応について

また、2024 年 6 月に改正された地方自治法において、地方公共団体は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指針を示すこととされている（2026 年 4 月 1 日施行）。

総務大臣の指針案については、2024 年 4 月 1 日に通知され、各地方公共団体は当該指針案を十分に参照して、方針の策定を改正法施行日に行うことになる。更なるサイバーセキュリティの確保・充実が目指される。

3.1.5 警察によるサイバー空間の安全確保の取り組み

2021 年 9 月に閣議決定されたサイバーセキュリティ戦略に基づき、警察庁が 2022 年 4 月に改定した「警察におけるサイバー戦略※140」では、2025 年までの 3 年間の警察の取り組みとして、サイバー空間の安全・安心を確保するため、深刻化する脅威に対処できる態勢の整備、国内外の多様な主体との連携強化、社会全体でのサイバーセキュリティ向上に向けた取り組みの推進強化が掲げられた。

同戦略に基づき「警察におけるサイバー重点施策※141」も併せて改定された。そこでは、「①体制及び人的・物的基盤の強化」としてサイバー空間の脅威に対処するための警察庁及び都道府県警察における体制構築や優秀な人材の確保及び育成、警察における情報セキュリティの確保等が挙げられている。また、「②実態把握と社会変化への適応力の強化」として通報・相談への対応強化による実態把握の推進や実態解明と実効的な対策の推進等が挙げられている。そのほか「③部門間連携の推進」「④国際連携の推進」「⑤官民連携の推進」も併せた五つが重点施策として推進されてきた。

本項では、これらのサイバー空間に対する警察の基本施策のもと、2024 年度を中心とした取り組み状況とサイバー攻撃、犯罪の情勢等について、主に「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※142」「令和 6 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※56」及び「令和 6 年版 警察白書※143」等に基づいて述べる。

(1) 警察における主な取り組み

2024 年度の警察における主な取り組みとして、組織基盤強化、実態把握と社会変化への適応力の強化、官民連携の推進の三つについて述べる。

(a) 警察における組織基盤の更なる強化

警察では、深刻化する重大サイバー事案の対処を担う国の捜査機関として、関東管区警察局に「サイバー特別捜査隊」を 2022 年 4 月に新設した。2024 年 4 月には、同隊を発展的に改組し、新たに「サイバー特別捜査部※144」が設置されるとともに、そのもとに企画分析課と特別捜査課が置かれた。企画分析課は、重大サイバー事案に関する情報の収集と分析、特別捜査課は、重大サイバー事案に関係した犯罪の捜査を主に担う。

サイバー特別捜査部は、情報技術解析部門の解析

担当職員等の併任者も合わせると総勢約 300 人強の体制となり、犯罪捜査のほかに、重大サイバー事案の対処に必要な情報の収集や整理及び事案横断的な分析等を行う。

これにより、サイバー特別捜査部は、都道府県警察が捜査により得た膨大な情報を集約し、外国捜査機関等との情報交換や独自の捜査で得た情報と併せて高度な分析・解析を行い、犯罪グループの中枢被疑者の特定や実態解明等を一層推進することができるようになった。

(b) 実態把握と社会変化への対応力の強化

日本国内の治安をめぐる情勢は近年目まぐるしく変化を続けており、その中でサイバー空間は社会経済活動が営まれる重要かつ公共性の高い空間へと変貌を遂げ、特に SNS は目覚ましい普及が見られている。

このように我々を取り巻く環境が激変する中において、ますます深刻化するサイバー犯罪の検挙と抑止に向けた警察による実態把握と対応力の強化について述べる。

(ア) 不正アクセスへの対応

警察では、サイバー犯罪の上位を占める不正アクセス行為の犯行手口の分析に基づき、関係機関等とも連携し、広報・啓発等により被害を防止するとともに、毎年、民間企業や行政機関等に対する「不正アクセス行為対策等の実態調査※145」及び「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状況等に関する調査※146」等を実施し、公表している。

前者は市販のデータベースに掲載された企業、教育機関（国公立、私立の大学等）、医療機関、地方公共団体（県・市区町村等）、独立行政法人及び特殊法人、後者は市販のデータベースに掲載された企業のうち業種分類が「情報・通信」「サービス」「電気機器」または「金融」であるもの、及び国公立・私立大学のうち理工系学部またはこれに準ずるものを設置するものから無作為に抽出し、調査票を郵送で配布し、電子メールまたは郵送により回答を得た結果を取りまとめたものであり、産官学の広い範囲のデータが集約されているといえる。

(イ) インターネットバンキングに係る不正送金への対応

警察では、2023 年から被害が急増しているインターネットバンキングに係る不正送金事犯に対し、関係機関と連携したフィッシング被害の実態把握や、フィッシングサイトに関する分析及び関係事業者への照会等、早期の実態解明と必要な取り締りを推進している。併せて、フィッシング対策に関する Web サイト※147 を開設し、被害防止策や被害に遭った際の対応について周知している。

また、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）※148 等との官民連携の枠組みを通じて、把握したフィッシングサイトの情報をセキュリティソフト事業者等に提供する等の被害防止対策も推進している。

(ウ) インターネット上の違法情報・有害情報への対応

警察庁は、一般財団法人インターネット協会へ業務委託する形で、違法・有害情報の発信に関する情報収集と対処を目的とする団体であるインターネット・ホットラインセンター（IHC：Internet Hotline Center）※149 を 2006 年に開設した。具体的には「児童ポルノ」「覚醒剤等の規制薬物の販売」「犯罪実行者の募集」「集団自殺の呼び掛け」に関する通報を一般のインターネット利用者等から受理して、警察への情報提供、サイト管理者への削除依頼等を行っている。

また、インターネット上の重要犯罪密接関連情報等を収集し、IHC に通報するサイバーパトロールセンター（CPC）も運用している。

(エ) 国際情勢を踏まえた注意喚起

ここ数年、情報窃取を目的としたサイバー攻撃、国家を背景とする暗号資産獲得を目的としたサイバー攻撃事案等が相次ぎ発生していることから、警察庁も積極的に注意喚起情報を発出している。

2019 年から現在に至るまで、警察庁は NISC とともに、「MirrorFace」というサイバー攻撃グループが、日本国内の組織、事業者及び個人に対して、マルウェアを添付したメールの送信等により、情報窃取を目的としたサイバー攻撃を行っていることを確認している。2025 年 1 月、これらのサイバー攻撃が、中国の関与が疑われる組織的なサイバー攻撃活動である可能性があることから、サイバー攻撃の手口や未然防止対策等に関する注意喚起を実施した※150。

(c) 官民連携の推進

警察では、各都道府県警察及び重要インフラ事業者等で構成される「サイバーテロ対策協議会※151」をすべての都道府県に設置しており、重要インフラ事業者等とのサイバー攻撃事案の発生を想定した共同対処訓練等の官民連携による取り組みを実施している。同協議会との連携については、警察庁の Web サイトにサイバー事

案に関する通報・相談・情報提供の統一窓口を設置して、通報・相談の負担軽減も図っている。

その他の取り組みとして、警察及び全国約 8,700 の事業者等からなるサイバーインテリジェンス情報共有ネットワーク（CCI ネットワーク）の枠組みを構築している。ここでは、情報窃取を目的としたと見られるサイバー攻撃に関する各種情報を集約するとともに、これら情報及びその他の情報を総合的に分析し、事業者等に対し注意喚起を実施している。

(2) 2024 年のサイバー攻撃の情勢と警察の対応

2024 年におけるサイバー空間の脅威の情勢と、その脅威に対し、世の中の安心・安全を確保するための警察の主な対応について述べる。

(a) サイバー空間の脅威の情勢と検挙状況

2024 年におけるサイバー空間の脅威の情勢について述べる。

(ア) センサーにおいて検知した不審なアクセスの概況

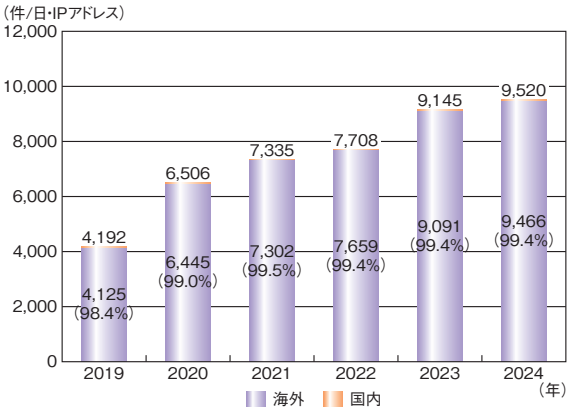
警察では、セキュリティ上の脆弱性に関する情報や標的型攻撃等の犯行手口に関する情報等を把握・分析し、被害を未然防止、拡大防止するための施策の一環として、都道府県警察のサイバー事案対策部門に技術的な面から支援を行う部隊であるサイバーフォース※152 を、警察庁及び全国の情報通信部にそれぞれ設置している。

全国のサイバーフォースの司令塔を担う警察庁のサイバーフォースセンターは、サイバー事案の予兆・実態等を把握することを目的とし、2002 年よりインターネット上にセンサーを設置し、リアルタイム検知ネットワークシステムを通じて、不特定多数の IP アドレスに対して無差別に送られてくる通信パケットを収集し、分析している。これにより、インターネットに接続された各種機器の脆弱性の探索行為等を観測し、脆弱性を悪用した攻撃、マルウェアに感染したコンピューターの振る舞い等、インターネット上で発生している各種事象を把握することができる。

2024 年に同センサーが検知した不審なアクセス件数は、1 日・1IP アドレスあたり 9,520 件と前年を 4.1% 上回り、2011 年以降、増加の一途をたどっているが、その大部分は海外を発信元とするアクセスが占めている（図 3-1-18）。

(イ) サイバー犯罪・サイバー事案の概況

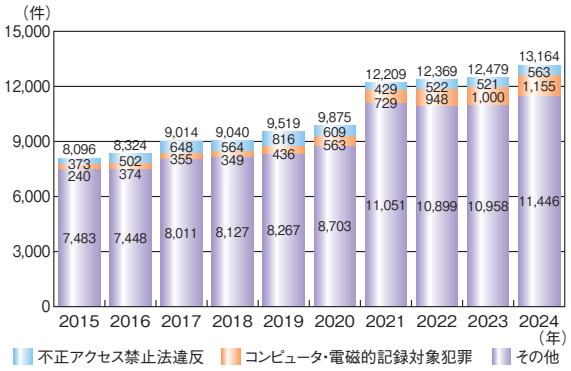
インターネット空間を悪用したサイバー犯罪※153 の検



■図 3-1-18　警察庁が検知した不審なアクセス件数（1 日・1IP アドレスあたり、2019 ～ 2024 年）
（出典）警察庁「令和 6 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

挙件数は 2020 年までは 1 万件／年以下で推移していたが、2021 年に一気に 2 割以上増加の 1 万 2,209 件に跳ね上がって以来、高水準で推移している。2024 年におけるサイバー犯罪の検挙件数は、前年から 5.5% 増の 1 万 3,164 件に上った。

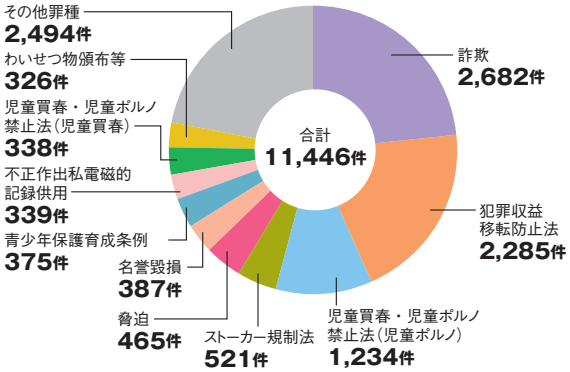
1 万 3,164 件のサイバー犯罪の内訳では、「コンピュータ・電磁的記録対象犯罪」が 1,155 件、「不正アクセス禁止法違反」が 563 件を占める（図 3-1-19）。



■図 3-1-19　サイバー犯罪の検挙件数の推移（2015 ～ 2024 年）
（出典）警察庁「令和 6 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

1 万 1,446 件を占める「その他」の内訳（次ページ図 3-1-20）については、最多を占めているのが「詐欺」であることに変わりはないが、第 2 位の「犯罪収益移転防止法違反」と第 3 位の「児童買春・児童ポルノ禁止法違反」は前年※154 と順位が逆転しているとともに、これら上位の事案全体が占める割合が増加していることは注目される。

2024 年に検挙された不正アクセス禁止法違反 563 件のうち約 9 割を占める 511 件が、認証情報を悪用する手口である識別符号窃用型となっている。同手口を不

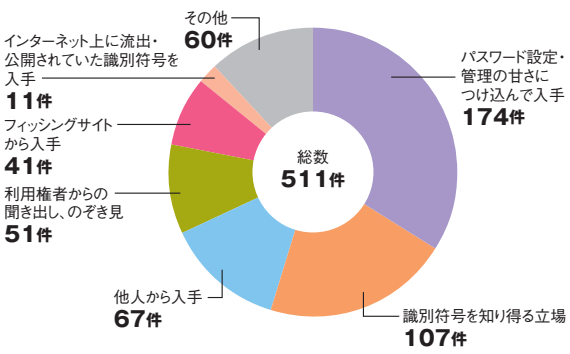


■図 3-1-20　その他の検挙状況(2024 年)
(出典)警察庁「令和 6 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

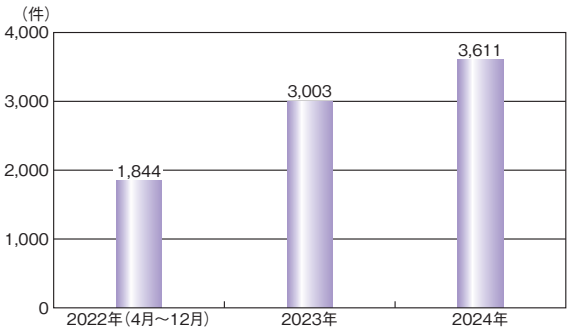
正に利用されたサービス別に見ると、「パスワードの設定・管理の甘さに付け込んで入手」が最多の 174 件、「識別符号を知り得る立場」が 2 番目の 107 件を占め、ユーザー側とサービス提供側双方に起因する事案が半分以上を占めていることが分かる(図 3-1-21)。

サイバー事案※155 の検挙件数は前年より 2 割程度増え 3,611 件に達している(図 3-1-22)。

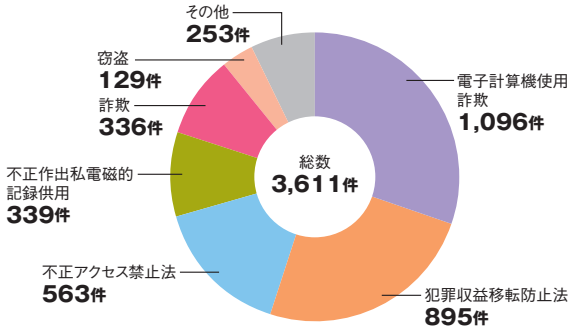
サイバー事案のうち、従業員による着服等の「電子計算機使用詐欺」と、金融機関の口座やキャッシュカードの譲渡・売買等の「犯罪収益移転防止法」に違反した案件が過半を占め(図 3-1-23)、直接的な金銭窃取を目的とした犯罪の多さが浮き彫りになっている。



■図 3-1-21　不正アクセス行為(識別符号窃用型)に係る手口別検挙件数(2024 年)
(出典)警察庁「令和 6 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



■図 3-1-22　サイバー事案の検挙件数の推移(2022 ～ 2024 年)
(出典)警察庁「令和 6 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



■図 3-1-23　サイバー事案の検挙状況(2024 年)
(出典)警察庁「令和 6 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

(ウ)インターネット空間を悪用した犯罪の概況

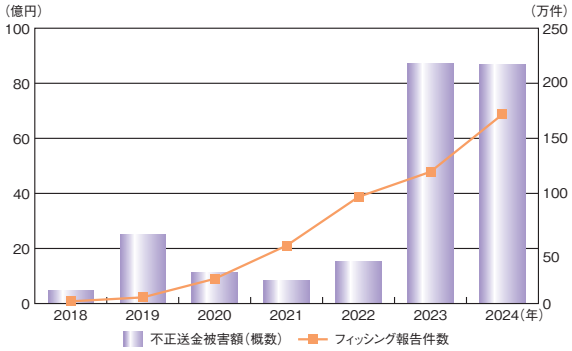
以下、インターネット空間を悪用した主な犯罪の概況を述べる。

- フィッシング

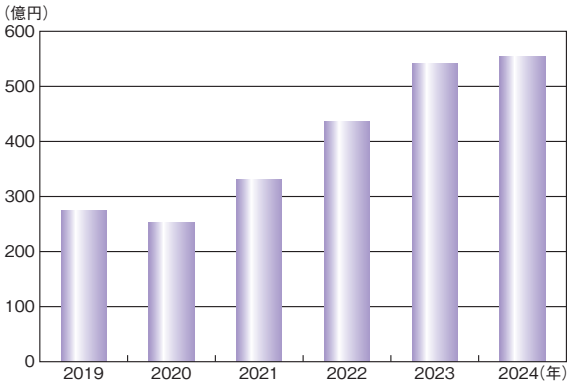
  フィッシング対策協議会によると、2024 年におけるフィッシング報告件数は 171 万 8,036 件であり、前年の 119 万 6,390 件から大きく増加した一方、不正送金の被害額は 86 億 9,000 万円と微減となった(図 3-1-24)。また、一般社団法人日本クレジット協会によると 2024 年のクレジットカードの不正利用被害額は約 555 億円と前年比で 2.6% 増え、過去最多となった(次ページ図 3-1-25)。

- 特殊詐欺

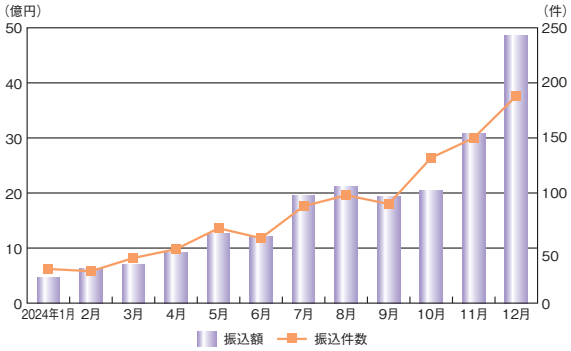
  2024 年の特殊詐欺(被害額 500 万円以上の振り込み型の事案)の被害件数・振込額は、年末に向け、ともに右肩上がりになっている(次ページ図 3-1-26)。2024 年の被害額は約 314 億円であり、そのうちインター



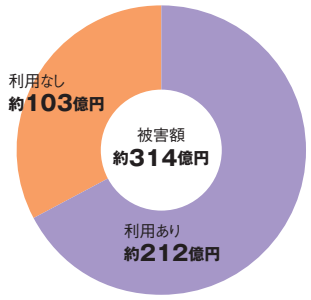
■図 3-1-24　フィッシング報告件数及び不正送金被害額の推移(2018 ～ 2024 年)
(出典)警察庁「令和 6 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集



■図 3-1-25　クレジットカード不正利用被害額の推移(2019～2024 年)
(出典)警察庁「令和 6 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



■図 3-1-26　特殊詐欺におけるインターネットバンキングを利用した振込被害の推移(2024 年 1 ～ 12 月)
(出典)警察庁「令和 6 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



■図 3-1-27　特殊詐欺の被害額に関するインターネットバンキングの利用の有無(2024 年)
(出典)警察庁「令和 6 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

ネットバンキングを利用したものは約 212 億円と約 3 分の 2 を占める(図 3-1-27)。

近年は、匿名・流動型犯罪グループによるものと見られる特殊詐欺が広域的に行われており、同グループはSNSでいわゆる闇バイト等で高額な報酬を示唆して「受け子」等を募集し、犯行に加担させている。また、首謀者、指示役、実行役の間の連絡手段には、匿名性が高く、メッセージが自動的に消去される仕組みを備えた通信手段を使用する等、犯罪の証拠を隠滅しようとする手口が多く見られる。

なお、特殊詐欺の被害拡大防止を目的として、警察庁では 2025 年 1 月にゆうちょ銀行との間で情報連携協定書を締結した※156。

- SNS 型投資・ロマンス詐欺

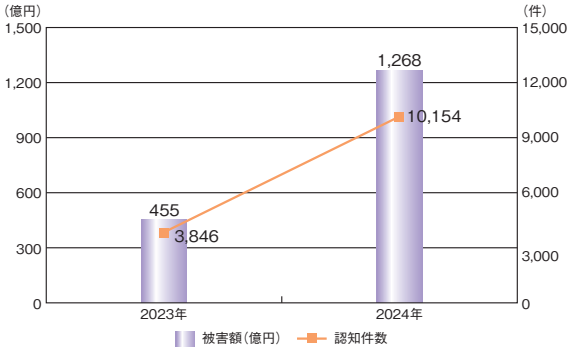
SNS 型投資・ロマンス詐欺は、SNS を通じて対面することなく、交信を重ねる等して関係を深めて信用させ、投資金名目やその利益の出金手数料名目等で金銭を騙し取る、または恋愛感情や親近感を抱かせて金銭を騙し取る等の犯罪である。

SNS の利用が進む中、同詐欺の認知件数、被害額ともに前年比で急増し、被害額が約 1,268 億円と特殊詐欺を大きく上回っていることは注目に値する※157(図 3-1-28)。

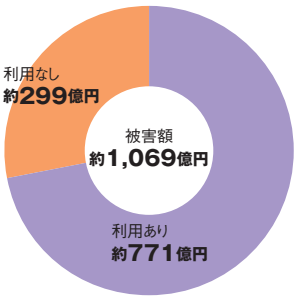
また、同詐欺でも振込が主に使用された事案では、インターネットバンキングが利用された事案の被害額が約 771 億円と 7 割以上の高い比率を占める(図 3-1-29)。

- ランサムウェア

2024 年のランサムウェアの被害報告件数は 222 件、ノーウェアランサムは 22 件であった。ノーウェアランサムの件数は前年比で 8 件減っているものの、ランサム



■図 3-1-28　SNS 型投資・ロマンス詐欺の認知件数・被害額の推移(2023 ～ 2024 年)
(出典)警察庁「令和 6 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



■図 3-1-29　SNS 型投資・ロマンス詐欺(振込が主に使用された事案)の被害額に関するインターネットバンキングの利用の有無(2024 年)
(出典)警察庁「令和 6 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

ウェアは 25 件増えていることから、合算では 17 件増えており、2022 年から高止まりが続いている。なお、最近拡大しつつある手口であるノーウェアランサムとは、データを暗号化することなくデータを窃取した上で対価を要求する手口の呼称である。ランサムウェアについては「1.2.1 ランサムウェア攻撃」を参照されたい。

(b) サイバー攻撃に対する警察の取り組み事例

2024 年に実施した、主なサイバー攻撃に対する具体的な取り組み事例を挙げる。

(ア) 国際アドバイザリーへの共同署名

中国政府を背景とするサイバー攻撃グループといわれている「APT40」は、北米、欧州、豪州等を標的としており、我が国の企業も攻撃の標的になっていたことが確認されている。

2024 年 7 月、警察庁及び NISC は、米国、英国、カナダ、ニュージーランド、ドイツ及び韓国の関係機関とともに、オーストラリア通信情報局（ASD：Australian Signals Directorate）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）が作成した国際アドバイザリー「APT40 Advisory PRC MSS tradecraft in action[※158]」の共同署名に加わり、アドバイザリーを公表した。これには、APT40 による過去の攻撃事例に基づく攻撃手法、攻撃の検知や緩和策が示されている。

(イ) その他国際連携による犯罪捜査等の取り組み

ICPO が主導して、西アフリカにおける組織的な金融犯罪を国際共同捜査するオペレーション「ジャッカル」に、日本警察も 2024 年 4 月から参画した。警察庁のサイバー特別捜査部は、SNS 型投資・ロマンス詐欺事案について、関係都道府県警察の横断的な捜査情報の分析や暗号資産追跡を実施し、ナイジェリア人名義の暗号資産アカウントに送金されている事実を突き止めた。同情報をナイジェリア警察に提供したところ、同国内の被疑者の検挙が行われた[※159]。

これを受け、2024 年 7 月、国際的な詐欺の拠点となっているナイジェリアで、ICPO と独立行政法人国際協力機構（JICA：Japan International Cooperation Agency）が開催した、ロマンス詐欺等の捜査力向上を目的とした研修会において、警察庁担当者が資金回収等に使われる暗号資産に関する捜査手法の説明等を行った[※160]。

2024 年にも深刻な被害が発生した DDoS 攻撃への対応については、国際共同捜査を通じ、外国捜査機関から提供を受けた情報を緻密に精査することによって、DDoS 攻撃 Web サービスを利用した者を 3 名検挙した。2024 年 12 月には警察庁 Web サイトにおいて DDoS 攻撃に関する注意を促すメッセージを掲載するとともに、公式 X アカウントや Google の広告機能を活用して周知する取り組みを行った[※161]。

OT（Operational Technology）のサイバーセキュリティ対策に関する国際連携としては、警察庁は NISC とともに、ACSC が策定した文書「OT サイバーセキュリティの原則（Principles of OT Cyber Security）」の共同署名に加わった[※162]。

(ウ) 生成 AI を悪用した事件被疑者の検挙

生成 AI に関する具体的な事案としては、2023 年 3 月、生成 AI を利用し、人が電子計算機で実行した際、ファイルのデータを上書きして破壊する機能を有する不正プログラムを作成したことにより、警視庁は 2024 年 5 月に不正指令電磁的記録作成容疑で無職の男（25 歳）を逮捕した[※163]。

(エ) 合同捜査本部による不正送金事件の捜査

2022 年から 2023 年にかけて発生したインターネットバンキングに関する不正送金事件で、関係都道府県警察により得られた情報をサイバー特別捜査部が集約・分析するとともに、暗号資産の追跡捜査や関係被疑者の SNS アカウントに関する捜査を実施した。

その結果、サイバー特別捜査部や関東管区警察局及び 16 都道府県警察（警視庁、広島、北海道、宮城、茨城、群馬、千葉、静岡、大阪、兵庫、奈良、岡山、愛媛、福岡、長崎、熊本）の合同捜査本部は、同一の犯行グループが SIM スワップという手口を駆使し、組織的に不正送金を実行している実態を解明した。そして最終的に 2024 年 7 月、犯行グループの指示役と見られる男（44 歳）を不正アクセス禁止法違反（不正アクセス行為）で逮捕した[※164]。

合同捜査本部の捜査により、同グループによる被害件数及び被害額は、少なくとも 20 件、1 億 2,000 万円に上ることが明らかになっている。

(オ) 偽情報投稿事案被疑者の検挙等、能登半島地震に関する対応

2024 年 1 月 1 日に発生した能登半島地震においては、被災地の警察が捜索活動等に全力を挙げる中、SNS

上において過去の災害時の画像や虚偽の救助要請が拡散されたこと等により、捜索活動等が妨害される事態が生じていた。そうした状況の中、サイバー特別捜査隊（当時）は、各種情報収集を通じて、被災地の警察と連携しながら、関連アカウントに関する捜査を実施した。

石川県警察は、サイバー特別捜査隊との連携による捜査の結果、地震当日に被災者を装ってSNS上に救助を求める虚偽の内容を投稿し、本来不要な捜索活動等を警察に実施させてその業務を妨害した会社員の男（25歳）を特定し、2024年7月に偽計業務妨害容疑で逮捕した※165。

なお、同地震発生時には、SNS上において、QRコードを利用した義援金を募る送金詐欺も、警察によって確認された。

（カ）警察におけるその他の取り組み

警察庁はSIMスワップによる不正送金対策として、2024年5月、総務省と連携し、携帯電話事業者に対して本人確認の強化を要請した（2022年以降2度目）。SIMスワップは、実在する人物になりすまして店舗に来店し、本人確認資料として偽造した運転免許証等を用い、MNP（携帯電話番号ポータビリティ）またはSIMカードの再発行を行うことで携帯電話番号を乗っ取り、乗っ取った携帯電話番号のスマホを悪用して2段階認証やパスワードの再発行を行うことでインターネットバンキング等のアカウントを乗っ取り、不正送金を行う手口である※166。この手口による被害は、2022年に爆発的に発生した。

国内におけるサイバー保険を名目とした架空料金請求詐欺事件に係る捜査においては、サイバー特別捜査隊（当時）による暗号資産追跡と、その結果の事案横断的な分析により、従来明らかになっていなかった事案相互の関連性が明らかになり、関係警察による関連被疑者の逮捕に貢献した。

このほか、「国民を詐欺から守るための総合対策※167」（2024年6月18日、犯罪対策閣僚会議決定）に基づき、関係機関・団体・民間事業者等の協力を得ながら、各種施策を強力に推進している。

3.2 サイバーセキュリティ人材の現状と育成

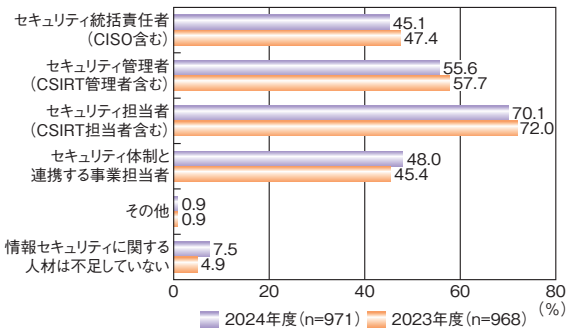
日本におけるサイバーセキュリティ人材は、様々な人材育成施策が行われているものの、不足状態が続き、深刻な問題となっている。官民挙げての新たな育成施策では、多くの課題が浮き彫りになっており、これらに対応する取り組みが行われている。本節では、官民における、サイバーセキュリティ人材育成の取り組みについて述べる。

3.2.1 サイバーセキュリティ人材の現状と育成状況

ISC2, Inc. が発表した「2024 ISC2 Cybersecurity Workforce Study※168」によると、日本のサイバーセキュリティ人材の不足は過去最大に達しており、セキュリティ確保には 16 万 9,603 人の専門家が追加で必要であるとされた。一方、セキュリティ人材の労働力については、堅調に増加しており、前年より 4% 増加しているものの、供給が需要に追い付いていない状況である※169。

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）の東証一部上場企業とそれに準じる企業を対象とした「企業 IT 動向調査報告書 2025※170」によると、不足しているセキュリティ人材の職種は、「セキュリティ担当者（CSIRT 担当者含む）」の割合が 70.1% と最も高く、続いて「セキュリティ管理者（CSIRT 管理者含む）」が 55.6% と高い（図 3-2-1）。「セキュリティ体制と連携する事業担当者」を除いて、2023 年度に比べて、すべての職種の人材で不足と回答した割合が若干減少しており、「情報セキュリティに関する人材は不足していない」割合が若干増加しているものの、情報セキュリティ人材の不足の状況に大きな改善は見られない。

また、民間の IT 転職サービス企業であるレバテック株式会社の調査※171 によれば、2024 年 12 月のセキュリティ人材の転職求人倍率が 54 倍と IT 業界における順位が 1 位となっており、深刻な人材不足が浮き彫りとなっている。



■図 3-2-1　情報セキュリティ人材不足の状況
（出典）JUAS「企業 IT 動向調査報告書 2025」を基に IPA が編集

需要の背景には様々なものがあるが、主な要因として AI の普及やデジタル化の急速な拡大や、これに伴うサイバーセキュリティインシデントの増加が考えられる。例えば、IPA が発行した「DX 動向 2024※172」によれば、DX に取り組んでいる日本企業の割合は年々増加しており、2023 年度は 7 割を超えている。また、IDC Japan 株式会社によれば、日本国内における 2024 年の国内エッジインフラ市場の支出額は前年比 12.3% 増の 1 兆 6,000 億円になると推計しており、2024 年以降も年々増加すると予想している※173。一方、警察庁によると、サイバー攻撃の前兆となることもある脆弱性探索行為等の不審なアクセス件数や、ランサムウェアの被害報告件数が前年から増加する等、極めて深刻な情勢が継続しているという※56。

日本政府においては、2024 年 11 月に東京都内で開かれた国際会議「サイバーイニシアチブ東京 2024※174」において、平将明デジタル大臣が、国家及び国民の安全を守る「能動的サイバー防衛」の検討を進めるべく、「自由、公正かつ安全なサイバー空間を確保するために官民が連携し、日本全体で対策を強化することが不可欠だ」と述べ、中谷元防衛大臣は、「サイバー人材の育成・確保こそがサイバー能力の抜本的強化の基盤であり中枢だ」と述べている※175。更に、武藤容治経済産業大臣は、産業界に「サイバーセキュリティを将来の事業活動や成長に不可欠な取り組みとして対策の強化を図ってほしい」と呼びかけている※176。

経済産業省においては、2024 年 7 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 2（経営・人材・国際）サイバーセキュリティ人材の育成促進に向けた検討会」（以下、人材育成促進に向けた検討会）を発足し、有識者及び IPA とともに、サイバーセキュリティ人材育成を更に加速し、セキュリティ人材を増加させるための検討を行い、2025 年 5 月に施策の方向性を取りまとめた。人材育成促進に向けた検討会では、「①民間企業の 99% 以上を占める中小企業におけるセキュリティ人材」「②企業や IT ベンダー等でセキュリティをリードする登録セキスペ人材」「③未来のサイバーセキュリティを担う学

生等の若年層人材」を対象として検討が進められた。

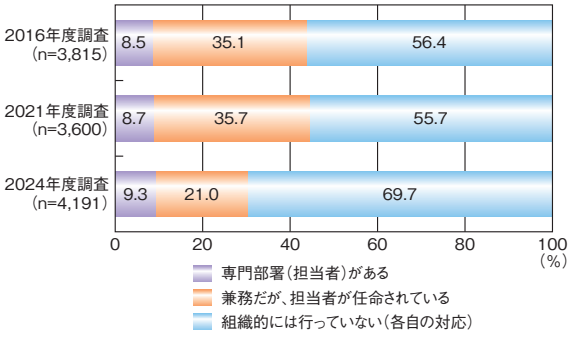
本項では、人材育成促進に向けた検討会での検討対象となっているこれら三つの活動に焦点を当て、それぞれの現状や課題と、今後のセキュリティ人材育成の方向性について述べる。

(1) セキュリティ人材不足の現状

セキュリティ人材不足については、サイバーセキュリティ対策の必要性が十分認知されていないことやコストの問題等、様々な要因により生じているものと考えられる。以下では、人材育成促進に向けた検討会で取り上げられたセキュリティ人材不足の現状を紹介する。

(a) 中小企業のサイバーセキュリティ

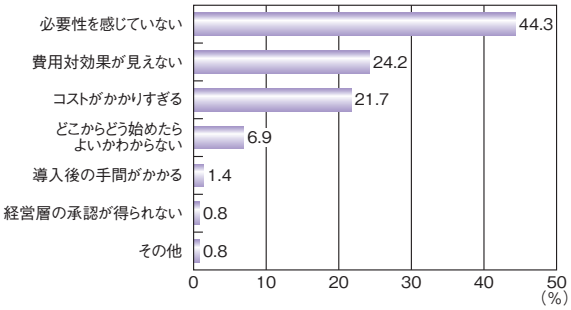
IPA が実施した「2024 年度 中小企業における情報セキュリティ対策に関する実態調査※177」によると、セキュリティの「専門部署（担当者）がある」企業の割合は、2021 年度に行った同様の調査時と比較して、0.6% 増の 9.3% にとどまっている。また、「兼務だが、担当者が任命されている」企業は21.0%に減少、「組織的には行っていない（各自の対応）」企業が 69.7% と大幅に増加している（図 3-2-2）。



■図 3-2-2　中小企業における情報セキュリティ体制
（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」を基に編集

パロアルトネットワークス株式会社の調査※178 においても、セキュリティの対策に関与する担当者を「非 IT 担当が兼務」している中小企業が 34%、「担当者不在」の中小企業が 9% であるとの結果が示されている。

更に、「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」によると、情報セキュリティに関する教育を含む過去 3 期の情報セキュリティ投資について、投資していないと回答した中小企業の割合が 2024 年度は 62.6% に上っている。投資していない 1 番の理由として「必要性を感じていない」が 44.3% と最も多く、次いで「費用対効果が見えない」が 24.2%、「コストがかかりすぎる」が 21.7% となっている（図 3-2-3）。



■図 3-2-3　情報セキュリティ対策投資を行わなかった理由（n=2,623）
（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」を基に編集

以上のことから、中小企業ではセキュリティ人材による組織的な体制の構築が進んでおらず、その背景として情報セキュリティ投資の必要性の認識の不足やコストの問題があることがうかがえる。

(b) 情報処理安全確保支援士（登録セキスペ）の推移

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に係る専門人材の国家資格である（「3.2.2 (2) 情報処理安全確保支援士制度」参照）。登録セキスペの登録者数は、2020 年 5 月に情報処理の促進に関する法律が改正され、登録セキスペの登録更新制度が導入されて以降、2 万人前後と横ばいで推移していた。2024 年には増加に転じたものの、2020 年 4 月の登録者数である 20,413 人と比較すると、2025 年 4 月は 16% 増の 23,751 人にとどまっている。このような登録者数の伸び悩みから、特に中小企業では、登録セキスペの確保が難しくなっている可能性がある。

更に、情報処理安全確保支援士試験合格者のうち 6 割以上は登録セキスペへの登録がされていない。また、登録消除者のアンケート結果によると、「メリットがない」「金銭的な負担が大きい」「転職・異動・業務上不要」というコメントが目立っている。課題として、セキュリティ業務がベンダー側に偏っており、ユーザー企業での活用が進んでいないこと、専業化がされておらず活躍の場が限られていること、資格維持のためのコストが大きいこと（3 年間で 10 万円以上）等が挙げられており※179、維持コストを低減するとともに、登録セキスペの活躍の場とユーザー企業での活用促進が望まれている。

(c)若年層への教育

一般社団法人セキュリティ・キャンプ協議会とIPAにより運営されているセキュリティ・キャンプ事業※180では、2004年度から2024年度までに「セキュリティ・キャンプ全国大会」を始めとして「セキュリティ・キャンプ　ネクスト」「セキュリティ・キャンプ　ジュニア」「セキュリティ・ミニキャンプ」を実施し、累計3,012名が修了した(「3.2.3(2)(a)セキュリティ・キャンプ」参照)。若年層の優秀なセキュリティ人材の早期発掘と育成という目的に沿って、これまで数多くの将来有望な人材を輩出してきており、情報セキュリティの業界にとどまらず各方面から、高度なIT人材育成の有益なイベントとして認知されている。その一方で、1年間に育成できる人数が限定的であること、また、同全国大会を修了した後の状況を把握できていないのが現状の課題である※181。

(2)セキュリティ人材不足への対応

前項では、セキュリティ人材不足における現状や課題等について取り上げた。本項では、人材育成促進に向けた検討会の検討内容を基に、人材不足への対応の方向性について紹介する。

(a)中小企業へのセキュリティ人材育成

IPAでは、中小企業の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「中小企業の情報セキュリティ対策ガイドライン※182」を公開している。同ガイドラインは、経営者が認識すべき「3原則」、経営者がやらなければならない「重要7項目の取組」を始め、情報セキュリティ対策の具体的な進め方を分かりやすく説明している。対策は、「情報セキュリティ5か条」等、できるところから始めて段階的にステップアップできる構成としている。同ガイドラインを活用することで、サイバーセキュリティ人材が不足している中小企業においても、対策の必要性を理解した上で組織的対策を行うことが可能になる。

また、人材育成促進に向けた検討会においては、中堅・中小企業等の組織内でセキュリティ対策を推進する者の育成・確保を行うための取り組みとして「実践的方策ガイド」の作成を進めている※183。同ガイドの案には、セキュリティ対策を実施するための最初のステップとして、セキュリティ担当者を配置転換等により兼務であっても1名は確保すること、内部だけで実施が難しい対策については付き合いのあるITベンダーや商工会・商工会議所等の支援機関を活用すること等が盛り込まれている。

(b)登録セキスペの登録者数の拡大

人材育成促進に向けた検討会では、登録セキスペを増やすための施策が検討されている。まず、登録セキスペの活用促進・活躍の場の拡大については、サイバーセキュリティ人材が特に不足している中小企業等(需要側)と登録セキスペ(供給側)をつなぐマッチングの枠組みの整備、スキル強化の機会や講習の拡大等、登録セキスペへの働きかけ、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やIoT製品に対するセキュリティ適合性評価制度である「セキュリティ要件適合評価及びラベリング制度(JC-STAR)」等の活用についての企業側への働きかけ等、多面的な施策が検討されている。例えば、「中小企業向けサイバーセキュリティ対策支援者リスト」の整備が挙げられている。同リストは登録セキスペの得意分野、専門領域等を可視化するものである。中小企業が同リストを活用することにより、登録セキスペによる中小企業のニーズに合ったセキュリティ対策の実装支援、適切なセキュリティ商材の導入支援を可能にすることが期待される。

次に、資格更新コストの低減に関しては、実際に企業等においてサイバーセキュリティ関連業務に従事している等、所定の実務にあたっている登録セキスペについて、資格更新のために同様の内容の講習を受ける負担を軽減すべく、更新講習(一部)のみなし受講制度や、更新講習の一部である「オンライン講習」の一部簡素化が検討されている※184。これらの施策を通じて、現在の登録セキスペ登録人数を2030年までに5万人まで増加させることを目指している。

(c)若年層への教育

前述のセキュリティ・キャンプでの育成人数が限定的であるという課題に関しては、既存事業を修了する人数を増やすのではなく、セキュリティの裾野を広げる観点から、AI等の特定領域の専門性と高度なセキュリティの知見の双方を兼ね備えた人材の育成を目的とする新たなセキュリティ・キャンプ事業を2025年度から実施することで、育成人数を増やす。また、修了生の継続的な知見研鑽、社会還元、活躍状況の共有等を目的としたコミュニティを整備していくことで、修了後の実績等を把握できるようにすることが今後の方向性として示された。

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や国家資格制度に関する動向を紹介する。

(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。2020 年度から CBT（Computer Based Testing）方式[※185]に移行した同試験は、2023 年 4 月からは年間を通じて随時[※186] CBT 方式により実施され、2024 年度は応募者数 4 万 5,481 人（前年比約 1.14 倍）、合格者数 2 万 8,731 人（前年比約 1.09 倍）であった[※187]。

(2) 情報処理安全確保支援士制度

サイバーセキュリティ分野初の国家資格である「情報処理安全確保支援士[※188]」（以下、登録セキスペ）は、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、2024 年度は応募者数 4 万 3,597 人（前年比約 1.16 倍）、合格者数 5,384 人（前年比約 0.95 倍）であった[※187]。登録セキスペは 2025 年 4 月 1 日時点で 2 万 3,751 人となった[※189]。

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 3-2-4 に示す。



■図 3-2-4　登録証のカラーパターン（2025 年 4 月 1 日時点）

また、登録更新には計 4 回の講習の受講が必要である[※190]。講習の種類とその概要を表 3-2-1 に示す。

「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。

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
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 3-2-1　講習の全体像

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」のうち、主に登録後 3 年目までの登録セキスペを対象とした「実践講習 A」は、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、2024 年度は 1,209 名が受講した。主に登録後 4 年目以降の登録セキスペを対象とした「実践講習 B」は、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、2024 年度は 2,506 名が受講した。また、主に登録後 7 年目以降の登録セキスペを対象とした「実践講習 C」を 2025 年 7 月に開始した。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 IPA が行う「業界別サイバーレジリエンス強化演習（CyberREX）[※191]」と「制御システム向けサイバーセキュリティ演習（CyberSTIX）[※192]」という「実践講習」の選択も可能となっている（「3.2.3 (1) 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」[※193]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。2024 年度には 14 実施機関 48 講習であったものが、2025 年度には 16 実施機関 56 講習と増加した。

サイバーセキュリティ対策の現場で活躍している登録セキスペからは「本資格の取得が会社の信用の大きな裏付けになり、その結果数多くの企業に脆弱性診断を実施できた。」（IT ベンダー企業経営者）[※194]、「本資格が専門性や倫理観の高い人材の証になっていて、また、質の高い学びを継続する取り組み姿勢も評価できることから資格取得を内部表彰の対象としている。」（警察関係者）[※195]との声が聞かれた。今後も、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。

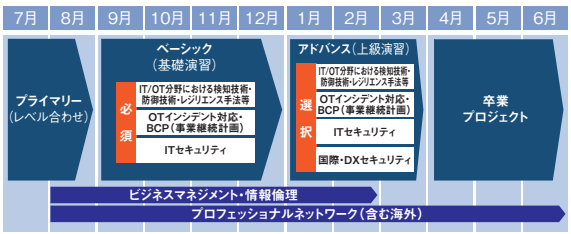
(1) 産業システムセキュリティ人材育成のための活動

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 2024 年度に実施した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（図 3-2-5）。第 1 期から第 7 期までに 435 名の修了者を輩出し、2024 年 7 月に開講した第 8 期では、電力・鉄鋼・化学・自動車・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 57 名が参加した。



■図 3-2-5　第 8 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等も行っている。

海外派遣演習として、2025 年 4 月には、第 8 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、英国科学・イノベーション・技術省にて英国におけるサイバーセキュリティ政策の紹介を受けた後、Imperial College London 内の Institute for Security Science and Technology（ISST）によって運営されている産学官共同研究機関 Research Institute in Trustworthy Industrial Control 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てグループワークを通じて成果物を作成する。第 7 期では 20 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 15 件を Web サイトで公開した※196。

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※197」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。

2024 年 11 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 7 回叶会総会を開催した。

叶会には第 1 期から第 7 期までの修了者に加え、2025 年 6 月に修了した第 8 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。

また ICSCoE では、修了者の修了後の知識・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。2024 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。

(b) 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）」「サイバー危機対応机上演習（CyberCREST）」の三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）※191 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。
  2024 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）※198 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 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。
- サイバー危機対応机上演習（CyberCREST）
  CyberCREST（Cyber Crisis RESponse Table top exercise）※199 は、制御システムを有する企業・団体においてサイバーセキュリティ対策を統括する責任者（CISO）や SOC（Security Operation Center）の責任者、サイバーセキュリティ対策部門の管理職を対象としたプログラムである。
  2024 年度の同演習は、DX 化による OT 領域のリスクと海外拠点のセキュリティ強化に焦点を当て、具体的な軽減策の検討や国際的な OT セキュリティ戦略を強化するために必要な実践的な知識やスキルの習得を目指し、2024 年 12 月から 2025 年 1 月にオンデマンド講習、2 月に講義及び机上演習を東京で実施した。

(c) 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）※192 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。
  2024 年 5 月に大阪、9 月に東京、2025 年 2 月に札幌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※200 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。
  同演習は、経済産業省の「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 Ver2.0※201」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いる。2024 年 11 月から 12 月にオンデマンド講習、同 12 月に最新動向の講義、グループワーク、実機を用いた実演（デモ）を中心とした演習を東京で実施した。

(2) 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関係機関の活動について述べる。

(a) セキュリティ・キャンプ

「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、並びに将来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（以下、セキュリ

ティ・キャンプ協議会）とIPAにより運営されている。セキュリティ・キャンプ協議会とIPAが開催しているプログラム、イベントについて以下で紹介する。

- セキュリティ・キャンプ　全国大会
  年1回、主に夏休み期間中に合宿形式の勉強会としてセキュリティ・キャンプのメインイベントである「セキュリティ・キャンプ　全国大会」（以下、全国大会）を開催してきた。21回目となる2024年度の全国大会は8月12日から17日の6日間で開催した。497名の応募があり、選考を通過した80名が参加した※202。
- セキュリティ・キャンプ　ネクスト
  過去の全国大会を修了、または同等以上のスキルを持つ25歳以下の学生等を対象に、更なる育成の場として「セキュリティ・キャンプ2024　ネクスト」を全国大会と同時に開催した。6回目の開催※203となる本プログラムでは144名の応募があり、選考を通過した10名が参加した※204。
- セキュリティ・キャンプ　ジュニア
  小中学生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歳以下の生徒を対象に「セキュリティ・キャンプ2024ジュニア」を全国大会と同時に開催した。2回目の開催となる本プログラムでは25名の応募があり、選考を通過した6名が参加した※205。
- セキュリティ・ミニキャンプ
  25歳以下の学生、生徒、児童を対象に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のほか、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開催している※206。
  セキュリティ・キャンプ協議会等と地域の組織・団体との共催により1日または2日にわたり行われるプログラムで、2024年度は全国12ヵ所の地域で開催した※207。東京（2024年4月）、宮城（2024年6月）、三重（2024年7月）、沖縄、岩手（2024年10月）、北海道、熊本（2024年11月）では専門講座のみ開催した。広島（2024年8月）、愛知（2024年9月）、山梨（2024年9月）、大阪（2025年3月）では公開講座と専門講座が開催された。石川（2024年12月）ではワークショップと称し、専門講座に加えてCTF（Capture The Flag）も開催した。
- 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超えた交流、及び修了後の活動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開催している。2024年度は2025年3月15日に開催し、特別講演と修了生の活動状況の発表、セキュリティ・キャンプ関係者によるブース展示を実施した※208。
- Global Cybersecurity Camp
  「Global Cybersecurity Camp（GCC）」は「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25歳以下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の韓国、台湾、シンガポールの4地域で開始した。7回目となる2024年度は台湾で「GCC 2025」として、11の国と地域の関連団体・大学により開催された。日本からは選考を通過した4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※209。

(b) CYNEX

「サイバーセキュリティネクサス（CYNEX：Cybersecurity Nexus）※210」は、NICTが運営するサイバーセキュリティ研究所で運営されている。産官学連携の結節点（ネクサス）となる先端的基盤の構築のため、2021年4月に組織され、2025年度までが第1期CYNEXとされている※135。ナショナルサイバートレーニングセンターとサイバーセキュリティ研究室の活動から得られるサイバー攻撃の膨大なデータと人材育成ノウハウを活用し、社会全体でサイバーセキュリティ人材を育成するための共通基盤を共有することで、日本のサイバーセキュリティの対応能力向上を目指している。

2023年10月に発足が発表された「CYNEXアライアンス」は、2024年には本格稼働フェーズに進んだ。CYNEXアライアンスは日本のサイバーセキュリティの産学官中核拠点確立を目指し、2024年12月末時点で既に90組織が参加している。CYNEXアライアンスには四つのサブプロジェクト「Co-Nexus」があり、そのうち人材育成に関係するのはCo-Nexus S（Security Operation & Sharing）、Co-Nexus C（CYROP：Cyber Range Open Platform）である。Co-Nexus Sは高度な解析者の育成とCYNEX独自の脅威情報の生成・発信を行っており、2024年12月末時点で参加組織は18組織であった。Co-Nexus Cはサイバーセキュリティ演習基盤CYROPを民間等に開放し、セキュリティ人材育成のハー

ドルを下げることで、国内のセキュリティ人材育成事業を活性化させる取り組みである。2024 年 12 月末時点の参加組織は 65 組織であった※211。いずれも前年の参加組織数から増加している。

(c) CYDER

「実践的サイバー防御演習（CYDER：Cyber Defense Exercise with Recurrence）」は、2013 年に総務省の実証実験としてスタートし、現在は NICT のナショナルサイバートレーニングセンターによって開発・実施されている。CYDER では、標的型攻撃、踏み台攻撃、ランサムウェア攻撃等、最近のサイバー攻撃事例に基づいた、リアリティのあるシナリオを使った演習が実施されており、自治体等のネットワーク環境を忠実に再現した仮想空間上で、受講者は実機を操作し、実際に手を動かしながら、ロールプレイ形式でインシデントハンドリングを体験できる。

2024 年度は初級（A コース）69 回、中級（B コース）32 回、準上級（C コース）5 回の集合演習を実施した。また 2023 年度下期より、オンラインによる、個人向け独習型の演習「プレ CYDER」を開講しており、「地方公立病院を襲うランサムウェア編」を 2024 年 5 月 21 日～ 7 月 19 日に※212、「たったひとつの冴えないパスワード編」を 2024 年 10 月 17 日～ 2025 年 1 月 31 日に開講した※213。基礎の基礎から学べ、最短 3 時間で受講が可能なこと、複数回に分けての受講が可能なことが特徴である。

(d) CIDLE

ナショナルサイバートレーニングセンターでは、2023 年度から 2024 年度にかけて、万博向けサイバー防御講習「CIDLE（Cyber Incident Defense Learning for EXPO）」を実施した※214。CIDLE は CYDER や東京 2020 オリンピック・パラリンピック競技大会の関連組織のセキュリティ担当者等を対象とした実践的サイバー演習「サイバーコロッセオ」の知見も活用して構成されたプログラムである※215。2025 年日本国際博覧会（大阪・関西万博）に向け、サイバーセキュリティを強化し安全な開催に資するよう、2023 年 9 月から関連組織の情報システム担当者等を対象として総務省・NICT により実施された。

(e) SecHack365

NICT が主催する「SecHack365」は、25 歳以下を対象に長期にわたるハッカソンによるモノづくりの機会を提供し、「セキュリティイノベーター」としてセキュリティの様々な課題にアイデアで切り込める人材の育成を目指すプログラムである。次の四つの能力を身に付けた人材の育成を目指し 2017 年度から実施している※216。

- サイバーセキュリティの課題に関する分析力
- 新たな発想で課題解決に挑むアイデアを多産し研究やシステムなどに形作る力
- サービスやプロダクト、システムを安全なものにする能力
- サイバーセキュリティの課題を解消するストーリーを作り、それを分かりやすく表現できる力

年 6 回のイベントと通年のオンライン指導で参加者の研究・開発を支援する仕組みで、「表現駆動」「学習駆動」「開発駆動」「思索駆動」「研究駆動」の 5 種類のコースが用意されている。2024 年度はキックオフを 6 月にオンラインで行った後、7 月に東京、9 月に広島、11 月に大阪で 2 泊 3 日のオフラインイベントが行われた※217。その後、2025 年 3 月 9 日にオフラインで成果発表会が行われ、6 作品が優秀作品として表彰された※218。

(f) SECCON

「SECCON（SECURITY CONTEST）」は、年間を通じ情報セキュリティをテーマにした多様な競技を開催する情報セキュリティコンテストイベントである。2012 年より特定非営利活動法人日本ネットワークセキュリティ協会（JNSA：Japan Network Security Association）内に設置された SECCON 実行委員会が運営している※219。目的は実践的情報セキュリティの人材発掘・育成、技術の実践の場の提供である※220。なお、SECCON の呼称がそれまでの西暦（例：SECCON2023）から連番になることが 2024 年 4 月に発表され※221、2024 年度の呼称は「SECCON 13」となった※222。「SECCON 13」の各プログラムの実施内容について紹介する。

- SECCON CTF
  CTF は攻撃・防御両者の視点を含むセキュリティの総合力を競うハッキングコンテストである。予選大会「SECCON CTF 13 Quals」は 2024 年 11 月 23 ～ 24 日にオンラインで実施された。その後、国際部門と国内部門の 2 部門で構成される決勝大会「SECCON CTF 13 Finals」が、東京で開催された「SECCON 13 電脳会議※223」の会場において 2025 年 3 月 1 ～ 2 日に行われた。国際部門の出場条件は予選大会の上位 8 チーム、国内部門は日本在住のメンバーで構成されるチームのうち、上位 8 位（ただし、国際部門に出場できるチームを除く）であること等が定められて

いる※224。

- SECCON Beginners
  「SECCON Beginners」は日本国内のCTFプレイヤーを増やし、人材育成とセキュリティ技術の底上げを目的としたCTF未経験者向けの勉強会である。2024年度は初・中級者向けのオンラインCTFが2024年6月15～16日に開催されたほか、国内5ヵ所でワークショップが行われた※225。
- CTF for GIRLS
  「CTF for GIRLS」は、情報セキュリティ技術に興味がある女性を対象に情報セキュリティ技術について学ぶワークショップやCTFイベントを開催しているコミュニティである。2024年は8月にフォレンジック分野、12月にペネトレーション分野のワークショップを行ったほか、「SECCON 13電脳会議」の会場において、CTFのワークショップ、ハンズオン、交流会等を行った※226。
- SECCONCON
  「SECCONCON（SECCON Contests）」は、応募された競技やコンテストの企画案や設計案を実際に行うイベントである。2024年は4回目の開催となり11月にオンラインで行われた※227。

(g) 産学情報セキュリティ人材育成交流会

産学情報セキュリティ人材育成交流会は、JNSAが情報セキュリティ分野の人材不足の状況を踏まえ、JNSA産学情報セキュリティ人材育成検討会を2012年に発足し、「教育機関における産学連携の支援」と「会員企業における採用を支援する取り組み」の実行を宣言したことに始まる※228。同交流会はインターンシップに興味を持つ学生に対し、受け入れ企業と交流できる場を提供し、長期インターンシップに関わる不安等を解消する目的で実施している。2024年度の同交流会は6月15日に定員60名で、東京大学本郷キャンパスで開催された※229。

COLUMN

「クラウドサービスのリスク」をどうやって把握する?

最近は、クラウドサービスを利用することが当たり前になってきました。一般的なオンプレミスの情報システムと比較すると、クラウドサービスを活用した場合のほうが、セキュリティ対策が十分行われていることも多い。とは言うものの、クラウドサービスにおいて、セキュリティインシデントや障害は発生していないのでしょうか? また、クラウドサービスのセキュリティ対策は十分であると断言できるでしょうか?

実際、グローバルなクラウドサービスの長時間のサービス停止や、広域での障害は、近年でも発生しています。また、国内や小規模クラウドサービスにおけるセキュリティインシデントも同様に発生しています。こうした現実がある中、クラウドサービスのセキュリティ対策状況を、利用者である我々はどうやって知ることができるのでしょう?

オンプレミスで情報システムを構築する場合のセキュリティ対策状況は、設置場所、建屋、設備、ハードウェア、仮想環境、OS、ミドルウェア、アプリのすべてを対象とし、それらを直接確認する情報セキュリティ監査により把握することができました。一方、クラウドサービス上に情報システムを構築した場合、一般的には、サービスの内部を直接確認することはできません。つまりは、クラウドサービスの中のセキュリティ対策状況は、「ブラックボックス」になっているわけです。

ブラックボックスに対しては、セキュリティ的観点から十分なリスクの判断ができません。これを解消するために、クラウドサービス事業者によっては、自らの情報セキュリティ対策状況を、米国公認会計士協会(AICPA)の標準であるSOC(Service Organization Control)2に基づいたレポートとして提供している場合があります。また、ISMAP(政府情報システムのためのセキュリティ評価制度)で認証されたクラウドサービスにおいては、対応するセキュリティ管理策、リスク評価を行うために必要な情報等が公開されています。

クラウドサービスを活用したシステム構築では、自ら設定・構築するOS、ミドルウェア、アプリは直接確認し、クラウドサービスについてはSOC2レポートやISMAP認証制度の公開情報等を確認して、クラウドサービスを含むセキュリティ対策の状況全体を把握する必要があります。情報セキュリティ監査だけでは、セキュリティインシデントや障害等を防ぐことはできませんが、情報セキュリティ監査を通じて情報システムのリスクを把握することにより、自らのリスクを適切に管理することができます。クラウドサービスの活用にあたっては、クラウドサービスのリスクを把握することが重要です。

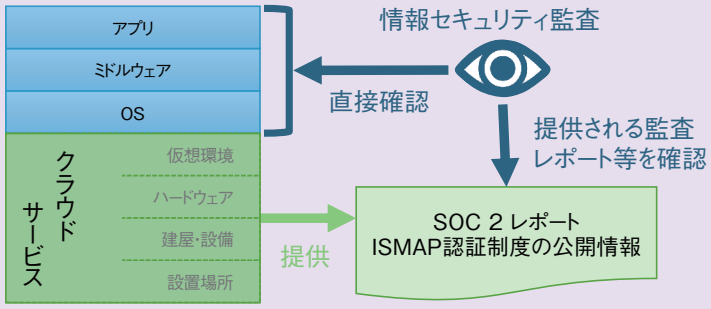


図　クラウドサービスを活用したシステム構築における情報セキュリティ監査

3.3 製品・サービスの評価・認証制度・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、新たに開始した 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）」、サプライチェーン強化に向けた対策評価制度構築に向けた検討、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、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安全性の評価・監視等を目的とし、デジタル庁、総務省、経済産業省、NICT、及び IPA が組織する CRYPTREC 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）※230」の運用を新たに開始した。JC-STAR は、IPA が運営する製品のセキュリティ機能等に対する評価制度としては、「IT セキュリティ評価及び認証制度（JISEC）」「暗号モジュール試験及び認証制度（JCMVP）」に次ぐ、三つ目の評価制度となる。なお、JC-STAR という名称及び同制度のロゴ（図 3-3-1）は、それぞれ第 6839291 号及び第 6910025 号として商標登録されている。



■図 3-3-1　JC-STAR ロゴ

本項では、JC-STAR が発足することとなった背景や制度概要、今後の取り組み等について解説する。

(1) JC-STAR 発足の背景

様々な IoT 製品がインターネットにつながることで便利なサービスが提供されるデジタル社会が実現している。実際、「情報通信白書令和 6 年版※231」に掲載された調査会社の予測によれば、世界の IoT 機器数は 2025 年に 462.9 億台に達すると見込まれている。

一方、IoT 製品を狙ったサイバー攻撃が増加しており、NICT が観測している NICTER（Network Incident analysis Center for Tactical Emergency Response）の観測レポート※232 によれば不審な通信のうち 3 分の 1 以上が IoT 機器を狙った攻撃に分類されている。これらの攻撃の結果として、マルウェアに感染した多くの IoT 機器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停止させるといった被害が現実化している。

初期の事例では、2016 年 10 月、米国で Twitter（現 X）や Spotify 等の著名なインターネットサービスへのアクセスに大規模な障害を生じさせた DDoS 攻撃が発生し、Mirai というマルウェアに感染した多数の IoT 機器によって構成されたボットネットが使用された攻撃であることが判明した※233。1 台の IoT 機器の攻撃能力はごく限られたものだが、IoT 製品が普及したことにより、多数の IoT 機器がボットネット化されると 500Gbps から 1Tbps に達するトラフィックを発生させ、社会インフラをダウンさせることができると証明された。その後も DDoS 攻撃にはボット化した IoT 機器が使われ続けており、日本でも 2024 年の年末から 2025 年の年始にかけて、航空業界や金融機関等に DDoS 攻撃の被害が出て、社会的な混乱を招いた（「1.2.3 (2) (a) 国内事業者向け攻撃の事例と手口」参照）。IPA の「情報セキュリティ 10 大脅威 2025※234」では、5 年ぶりに DDoS 攻撃がランクインしている。

ここでの問題は、「ボット化した IoT 機器」には、ホームルーター、ビデオレコーダー、ネットワークカメラ、ネット家電等を始めとして、身近で使われている IoT 機器が多く含まれていることである。このことは、IoT 製品の利用者はサイバー攻撃の「被害者」になるだけではなく、知らないうちに利用者自らが社会システムを停止させるサイバー攻撃の「加害者」の片棒を担ぐことになるかもしれない、ということを意味している。実際、マルウェアに感染し、

サイバー攻撃に加担してしまう危険性があるような、セキュリティ対策が十分に行われていない IoT 機器を観測し、注意喚起を行う「NOTICE※235」プロジェクトによれば、容易に推測可能な ID ／パスワードを使っている IoT 機器約 1 万 5,000 台、脆弱性が放置されたままの IoT 機器約 4,000 台、マルウェアに感染していると推定される IoT 機器約 1,000 ～ 1,500 台が発見されている。

本来、IoT 製品の利用者も IoT 製品のセキュリティ確保の役割の一翼を担っており、購入前に「十分なセキュリティ機能があるか」や「購入後のアップデートファイルの提供等のサポート体制がどのようになっているのか」を自ら確認し、利便性や価格だけでなく、セキュリティ対策も施されているかを考慮して IoT 製品を購入することが期待される。更に、購入後もその製品に脆弱性があれば、セキュリティアップデートの適用等への対処が求められる。

しかしこれまでは、IoT 製品の利用者がそのような情報を自ら確認することは難しく、どの IoT 製品のセキュリティ対策が適切なのか判断できなかった。また、セキュリティ対策を行った IoT 製品をベンダーが販売しても、セキュリティ対策の取り組みについて利用者にアピールすることが難しいという課題があった。加えて、最近では、IoT 製品のセキュリティ機能のみならず、サプライチェーン・リスク※236 管理の必要性も高まっている。

このような背景のもと、IoT 製品へのセキュリティ対策を進めるべく、米国、EU、シンガポール、英国等が IoT 製品のセキュリティ対策に関する評価制度の導入を進めており、日本でも経済産業省が 2022 年 11 月から「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※237」を発足させた。この検討会では、共通の物差しで IoT 製品のセキュリティ機能を評価・可視化し、適切なセキュリティ対策が講じられている IoT 製品が広まる仕組みの構築に向けた報告書を取りまとめた。その後、パブリックコメントの結果を踏まえ、2024 年 8 月に「IoT 製品に対するセキュリティ適合性評価制度構築方針※238」が公表された。

IPA では、上記の制度構築方針に基づき、JC-STAR の発足準備を進め、2025 年 3 月 25 日に「★ 1 適合ラベル」取得の申請受付※239 を開始した。その後、「★ 1 適合ラベル」の交付を開始し、同年 5 月 21 日に最初の「適合ラベル取得製品リスト※240」を公開した。なお、「★ 1 適合ラベル」は、IoT 製品共通の最低限の脅威に対応するための基準として設けられた適合基準を満たすことを、ベンダーが自己宣言した IoT 製品に対して交付されるものである。

(2) IoT 製品のセキュリティリスクが放置される理由と対処

インターネットに接続する以上、IoT 製品も IT 製品と同様のセキュリティリスクがある。しかし、以下のような IoT 製品特有の要因によって、セキュリティリスクが放置されたままになってしまうことが考えられる。

- IT 製品と異なり、IoT 製品に備わっているセキュリティ機能とは別のセキュリティ機能を独自に追加して利用することができない。
- IoT 製品が持つリソースが少なく、十分なセキュリティ機能を実装することができない。
- インターネットに簡単につながらないことのほうが利用者の不満に直結しやすいため、簡単にインターネット接続できるように初期設定では簡易なアクセス制御／ログイン管理機能しか提供していない。
- もともとはインターネットに接続することが想定されずに設計・製造されていた製品に対して、オプションとして、あるいは新機能としてインターネットに接続できるようにしたケースでは、インターネットに接続する際のセキュリティリスクに関する検討が不十分な攻撃対象領域（アタックサーフェス）が残ったまま発売されてしまうことがある。
- 利用者が想定しない機能（場合によってはベンダー自身も把握していない機能）が初期設定で有効になっており、想定外のデータのやり取りがあっても分からない。
- 設定ミスやマルウェア感染、不正アクセスといった問題が発生していても、IoT 製品の基本機能（例えば、エアコンなら空調機能、カメラなら撮影機能、テレビなら受信機能）としては正常に動作し、物理的な異常が見られない場合には、そもそも問題が発生していることに気が付きにくい。
- IoT 製品の明確な管理担当者等はおらず、一度設置されると、故障等が生じない限り、長期間メンテナンスされることなく使われ続け、発見された脆弱性に対する修正プログラムさえも適用されない。
- ベンダーがいつまでサポートするのかがはっきりせず、発見された脆弱性に対してアップデートファイルがそもそも作られないことがある。
- サポート期間が終了し、発見された脆弱性に対するアップデートファイルが提供されなくなってもそのまま使われ続ける。
- IoT 製品に記録されたデータの廃棄手順がはっきりしない。

こういったセキュリティリスクに対処するために、ベン

ダーにはIoT製品の設計段階からセキュリティを考慮（セキュア・バイ・デザイン）し、運用・保守フェーズを含むIoT製品のライフサイクルを通じた対策が求められる。例えば、IoT機器を開発する企業向けの「IoT機器を開発する中小企業向け製品セキュリティ対策ガイド※241」が参考になる。

IoT製品のセキュリティがほぼ評価されずに調達されることが多い現状を踏まえ、JC-STARに期待されることは、適切なセキュリティ対策が講じられたIoT製品を適合ラベルの交付により可視化し、それを目印に調達してもらうことでIoT製品のセキュリティ向上を図ることである。

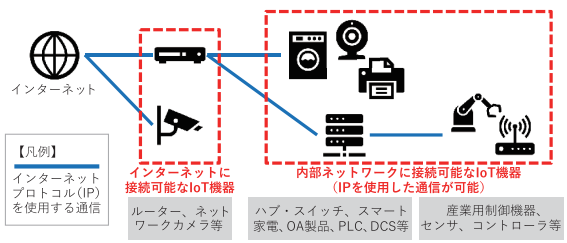
(3) JC-STARの概要

JC-STARは、インターネットと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の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。

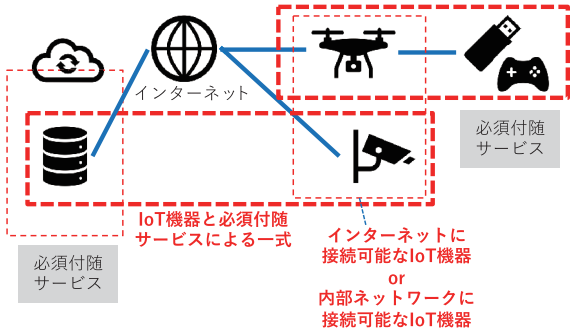
具体的な対象範囲は、以下の4条件を満たすIoT製品である。簡単に言えば、「インターネットの世界とつながり、インターネット側からの通信を受けるIoT製品のうち、その製品のベンダーが提供するセキュリティ機能のみが利用できるIoT製品」ということである（図3-3-2）。

①機器が含まれている（クラウドサービスやソフトウェアといったものは単体では対象外）。
②インターネットプロトコルを使用したデータ送受信（IP通信）ができる機能を有する。
③直接・間接を問わず、インターネットにつながる（可能性がある／否定できない場合を含む）。
④購入時にその IoT 製品に搭載されているセキュリティ機能を利用し、アップデート以外で（調達者・利用者が自らの意志で）後から別のセキュリティ機能を追加することが困難である。

また、IoT製品が意図した目的を提供するために、IoT機器と一体で提供することが必須となるデジタルサービスを「必須付随サービス」と呼び、これも適合ラベルの



■図3-3-2　JC-STARの対象製品例
（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※242」



■図3-3-3　JC-STARの対象製品例（必須付随サービスを有するもの）
（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」

対象となる（図3-3-3）。

パソコン等のように後からセキュリティソフトを入れる等、セキュリティ対策を後から追加できるものについては別途セキュリティ対策を検討してもらえばよいのに対して、IoT製品ではあらかじめその製品が備えるセキュリティ機能を使うしか利用者には選択肢がない以上、必要なセキュリティ機能はベンダーの責任において提供すべきというのが、このような対象範囲を定めた理由である。

一方、セキュリティ機能の提供には相応のコストがかかり、最終的にはベンダーだけでなく購入者にも一定の負担をしてもらう以上、むやみに高いコストをかけられない。そこで、JC-STARでは求められるセキュリティ水準に応じた4段階（「★1」（レベル1）～「★4」（レベル4））の適合基準を設定している。

適合基準を満たしたIoT製品は、その基準に応じた適合ラベルを取得することができる。この適合ラベルは、機器本体やパッケージ、ホームページ等に表示することができ、IoT製品のセキュリティ対策のアピールに利用できる。

(a) 適合基準について

JC-STARでは、適合ラベルを取得するために求められるセキュリティ水準に応じたセキュリティ要件として、以下の合計4段階の適合基準を設けており、レベルが上がる程、高度なセキュリティ要件となる。

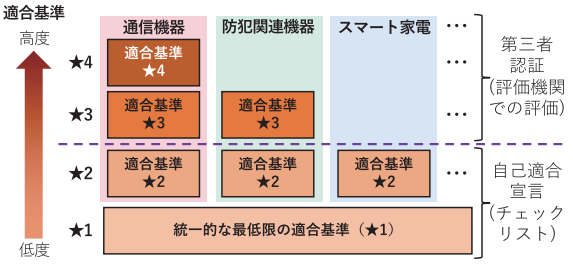
- 最低限の脅威に対抗するための製品共通の適合基準である「★1」
- IoT製品類型ごとの特徴に応じた適合基準である「★2」「★3」「★4」

これらの適合基準は、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、将来的な相互承認の実現を見据えてETSI EN 303 645※243、NIST IR

8425※244、EU CRA（Cyber Resilience Act※245）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。

具体的には、各レベル・製品類型ごとに想定される脅威や保護すべき情報資産等を考慮し、その脅威に対抗するためにIoT製品のセキュリティ機能として具備すべきセキュリティ要件を設定している。製品類型、想定されるセキュリティ脅威や保護すべき情報資産等の違いにより、求められるセキュリティ要件が異なり、適合基準のレベルが高くなる程、求められるセキュリティ要件のレベルが高くなる。

「★1」と「★2」の適合基準は主に民間の利用を想定しており、「★3」と「★4」の適合基準は主に政府機関や重要インフラ、地方自治体等の高いセキュリティが必要なシステムでの利用を想定している。購入者は、自身が求めるセキュリティ水準に適した適合基準のラベルが交付された製品を優先的に選択することが期待される。なお、高い適合基準を選ぶことが必要、あるいは、最良であるということは必ずしもなく、利用環境や利用目的に応じて、想定すべき脅威が考慮された適切な水準の適合基準を選択することが重要である（図3-3-4、表3-3-1）。



■図3-3-4　適合基準
（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」

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

「★1」では、最低限の脅威に対抗するために、主に以下の事項を実現することを目指している。

- マルウェアに感染してボット化するのを防ぐ。とりわけ、感染した機器からの感染拡大を防止する。
- インターネット経由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。

また、「★1」の適合基準への評価はチェックリストや評価ガイドを用いてベンダーが低コストで自己評価可能なレベルとする一方、海外制度と国際連携可能な要件とすることを踏まえ、表3-3-2（次ページ）に示す16個の適合基準（(1)～(16)）が定められた。

(b) 適合ラベルについて

適合ラベルは、IoT製品があらかじめ備えるセキュリティ機能が定められたセキュリティ要件（適合基準）に適合していることを示す目印として交付される。適合ラベルを取得したIoT製品には、製品本体（筐体）、パッケージ、マニュアル、パンフレット、ホームページ等に適合ラベルを記載・貼付・使用することで、セキュリティ対策の取り組みを購入者にアピールすることができる。

なお、適合ラベルの有効期間は2年を基本とし、延長申請が可能である。また、適合ラベルの有効期間内はアップデートファイルの提供等のサポートが義務付けられている。

適合ラベルには、IoT製品が取得した適合基準のレベルと登録番号のほか、そのIoT製品情報を確認するため、IPAが管理する「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（次ページ図3-3-5）。この製品情報ページは登録番号ごとに用意されており、「適合ラベル取得製品リスト」から表示できる。

製品情報ページでは、適合ラベルが交付されたIoT製品に対して、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を最新の状態に維持しながら、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、いつまでその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

★1で考慮する主な脅威			脅威に対抗するために★1で求める適合基準			
			IoT製品に対する適合基準		IoT製品ベンダーに対する適合基準	
			カテゴリ	適合基準の概要	カテゴリ	適合基準の概要
1.	①弱い認証機能により、	外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	識別・認証、アクセス制御	(1)適切な認証に基づくアクセス制御 (2)容易に推測可能なデフォルトパスワードの禁止 (3)パスワード等の認証値の変更機能 (4)ネットワーク経由のユーザ認証に対する総当たり攻撃からの保護	情報提供	(16)ユーザへのセキュアな利用・廃棄方法に関する情報提供(初期設定手順、セキュリティ更新、サポート期限、安全な廃棄手順等)
	②脆弱性の放置により、		脆弱性対策、ソフトウェア更新	(6)ソフトウェアコンポーネントのアップデート機能 (7)容易かつ分かりやすいアップデート手順 (8)アップデート前のソフトウェアの完全性の確認機能 (10)ユーザが製品型番を認識可能とする記載・機能	情報・問合せの受付、情報提供	(5)連絡先・手続き等の脆弱性開示ポリシーの公開 (9)セキュリティアップデートの優先度決定方針の文書化
	③未使用インタフェースの有効化により、		インタフェースへの論理アクセス	(13)不要かつリスクの高いインタフェースの無効化(物理的・論理的な通信ポート等)	―	―
	①～③共通		データ保護	(11)製品に保存される守るべき情報の保護(保存データの暗号化、物理的保護による保存、OSセキュア管理等)	―	―
2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威			データ保護	(12)ネットワーク経由で伝送される守るべき情報の保護(通信の暗号化、保護された通信環境の利用等)	―	―
3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威			データ保護	(15)製品内に保存される守るべき情報の削除機能 ※(11)も含む	情報提供	※(16)に含む
4. ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威			レジリエンス向上	(14)停電・ネットワーク停止等からの復旧時の認証情報やソフトウェア設定の維持(初期状態に戻らないこと)	―	―

■表3-3-2 ★1の適合基準
(出典)IPA「IoT製品のセキュリティ確保に向けて※246」



■図3-3-5 適合ラベルの例

対策やトラブル発生時等の対処がしやすくなることが期待される。

更に、製品情報ページの「適合ラベル情報」の「適合ラベルステータス」では、市場に長期間流通しているIoT製品についても、その時点の適合ラベルの状態をリアルタイムで確認できる(次ページ表3-3-3)。

(c)適合ラベルの取得スキーム

JC-STARでは、適合基準で定めた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)が用意されている。適合基準と評価手順は1対1の関係にあり、この評価手順に従って適合基準への適合性を確認する必要がある。

この評価手順を使って、「★1」と「★2」では、ベンダーが自己適合宣言、すなわち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、適合ラベルの申請を行うことができる。その申請がIPAに受理されると、そのIoT製品に対して適合ラベルが交付される。これにより、評価の信頼性はベンダーの信

ステータス	説明
有効	適合ラベルが有効期間内にあり、失効・取り消しに該当する事由がない状態
失効猶予（延長申請中）	適合ラベルの有効期間が満了しているが、有効期間の延長申請手続きが行われている状態
失効（有効期限切れ）	適合ラベルの有効期間が満了した後、有効期間の延長が行われていない状態
失効（自主取下げ）	適合ラベルの有効期間内に、IoT 製品ベンダーからの申し出により、適合ラベルの効力を失効させた状態
取消し	適合ラベルの有効期間内に、適合ラベルの取り消し事由に該当する事象が発生し、定められた期間内にその事由を解消するための是正がなされなかった場合に、IPA が強制的に適合ラベルの効力を停止させた状態

■表 3-3-3　適合ラベルのステータス

頼性に依存することになるが、低コストかつ短期間で適合ラベルを取得することができる。

なお、適合ラベルの交付にあたり、IPA はチェックリストの評価結果の根拠となる証跡の提出は求めておらず、評価結果の内容が正しいかどうかを IPA が自ら確認するものではないことに留意する必要がある。その代わり、適合ラベルの有効期間中は証跡の保管をベンダーに課しており、疑義が生じた場合に、事後的に IPA がサーベイランス（検査）を実施し、証跡等の提出を要求できる。その結果次第で適合ラベルの取り消しもあり得る仕組みを導入することで信頼性のバランスを取っている。

一方、高い信頼性が求められる「★ 3」と「★ 4」では、独立した評価機関が評価手順に従って適合性を評価し、その結果を IPA が認証するという第三者評価・認証方式により、適合ラベルが交付される（図 3-3-6）。「IT セキュリティ評価及び認証制度（JISEC）」に基づくコモンクライテリア認証とほぼ同様の考え方で運営される。

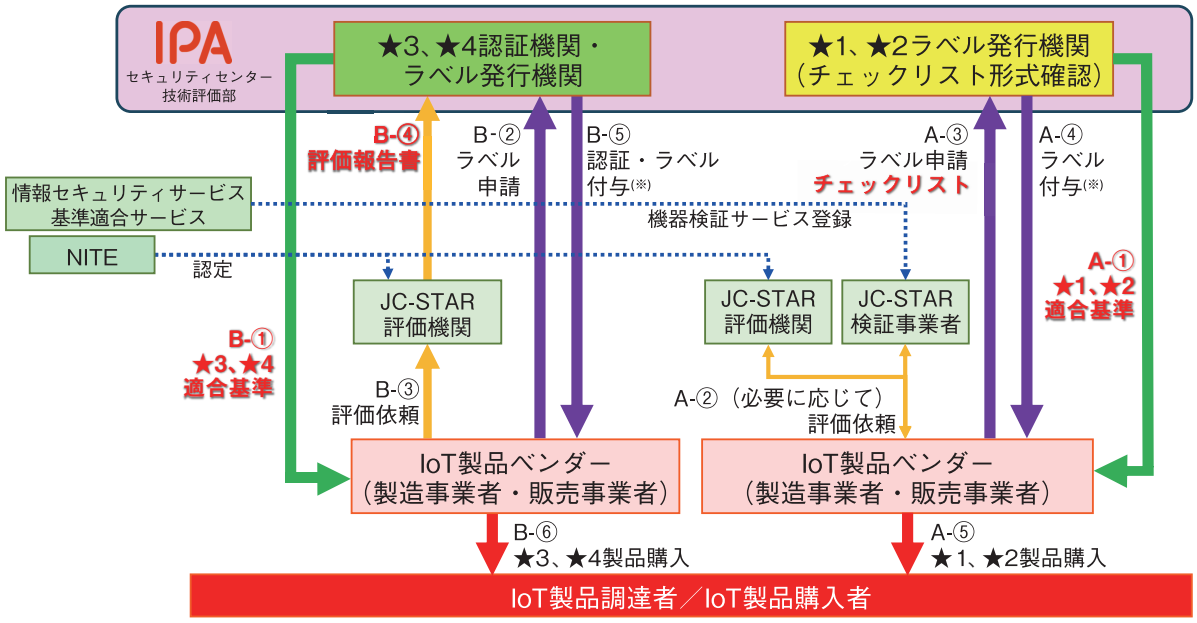
(4) JC-STAR 活用に向けた今後の取り組み

「★ 1 適合ラベル」の交付が始まり、今後もラベルを取得した IoT 製品が「適合ラベル取得製品リスト」に順次追加される。これにより、IoT 製品に求められる「★ 1」のセキュリティ要件を満たしていることを示す「★ 1 適合ラベル」が貼付された IoT 製品が実際に市場投入されることになる。

今後もベンダーが多くの IoT 製品で適合ラベルの取得を望むような環境を整備していくことと併せて、調達者や利用者に対してパンフレット、ポスター等で JC-STAR の意義を分かりやすく伝え、IoT 製品を購入する際は少なくとも「★ 1 適合ラベル」を取得した製品を購入してもらうように賛同団体等とともにプロモーション活動をしていく予定である。

(a) 調達要件での活用に関する調整

政府機関、重要インフラ事業者、地方公共団体等の社会的にセキュリティリスクが高いシステムを扱う組織における IoT 製品の調達要件に、JC-STAR の適合ラベ



(※) 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 3-3-6　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

ル取得製品の選定を含めるよう経済産業省等が働きかけている。2025 年 5 月時点で、以下の文書に JC-STAR 活用に関する記載がある。

- 「政府機関等の対策基準策定のためのガイドライン（令和 5 年度版）」の一部改定（2024 年 7 月）※18 の「4.3.1 機器等の調達」
- 「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 7 年 3 月版）※247」の第 2 章「6.3. システム開発、導入、保守等」
- 「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※248」の「3.4. ERAB システムが維持すべきサービスレベル」「3.6. ERAB システムにおけるサイバーセキュリティ対策」

経済産業省はまた、重要インフラ事業者に対する施策として、「重要インフラのサイバーセキュリティに係る行動計画」に基づく「重要インフラのサイバーセキュリティに係る安全基準等策定指針」に、調達製品への要求事項の策定及び調達時の確認を明示した上で、「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書※249」に詳細な記載を追加する方向で調整を進める予定である。

(b) 適合基準の拡張

IoT 製品類型ごとの特徴に応じたより高度な適合基準（「★ 2」以上）については、政府調達での活用が見込まれるネットワークカメラと通信機器の二つの製品類型を対象に、IPA に設置された適合基準検討ワーキンググループにより整備が進められており、2026 年 1 月以降に当該製品分野の「★ 2」以上の受付を開始する予定である。また、スマートホーム関連機器に対する「★ 2」等、その他の製品類型の「★ 2」以上の適合基準も順次整備し、制度を拡張していく計画である。

(c) 諸外国制度との相互承認に向けた調整

諸外国における IoT 製品の適合性評価制度の動向（表 3-3-4）も踏まえ、各国の制度との連携を図り、相互承認に向けた交渉を経済産業省と IPA は行っている。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軽減が期待される。

現在、シンガポール（Cybersecurity Labelling Scheme※250）、英国（PSTI 法※251）、米国（U.S. Cyber

国・地域	シンガポール	英国	米国	EU
制度名	Cybersecurity Labelling Scheme (CLS)	Product Security & Telecommunication 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	2025 年より基準策定開始（制度開始時期調整中）	・報告義務 :2026 年 9 月 ・その他 :2027 年 12 月
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：ETSI EN 303 645 のすべての必須要件に基づく基準 ・＊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）	NISTIR 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	・「重要なデジタル製品」以外の製品：自己適合宣言 ・「重要なデジタル製品」のクラスⅠ（EUCC や EN 規格の対象外の製品を除く）及びクラスⅡの製品：第三者認証

■表 3-3-4　諸外国の IoT 適合性評価制度
（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

Trust Mark[※252])、EU(CRA)等の各国担当機関との間で交渉を行っている。また、日米(首脳級)、日EU(閣僚級)、G7(首脳級)等において、相互承認に向けて取り組む旨を合意している。

進捗状況としては、英国とは具体的な相互承認のやり方を含めた交渉を行っている段階である。それ以外の国・地域についても、基準策定の方針に関する認識合わせなど、相互認証に向けた前向きな協議を進めている。

(d)業界団体・賛同団体との連携

経済産業省は2025年3月、「特定分野システムのIoT製品におけるJC-STAR制度活用ガイド(1.1版)[※253]」を公開した。同ガイドは、特定分野システム(特定の分野や業界において類似の汎用的な構成で利用されるシステム)にて調達・利用されるIoT製品に対して、実質的な業界標準としてのセキュリティ要件を定め、それをJC-STARにおける適合基準として整備することで、適合ラベル取得製品の供給と調達のエコシステム構築を促し、当該分野でのセキュリティの確保に貢献することを目的としている。特定分野システムの例として、スマートホームシステム、工場システム、ビルシステムが挙げられている。

このほかにも、各業界団体やIoT製品ベンダーも参画し、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「賛同団体」が5団体ある(五十音順)。

- 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)
- 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)

例えば、JBMIAが運営しているBMSec(事務機セキュリティプログラム)については、2025年10月以降JC-STARへ制度統合することが発表されている[※254]。

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)[※255]」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の動向や認証制度の国際連携について解説する。

(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5年度版)[※17]」(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[※256]」(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が遵守事項として定められた。

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。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。

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等のスマートカードの調達でJISECの認証制度は活用されている。

(2)認証制度の国際連携

JISECでも採用しているセキュリティ評価基準であるISO/IEC 15408は、欧米6ヵ国によるコモンクライテリア(共通基準)プロジェクトの成果をベースに開発された。

また、これらの国々を代表する公的機関が運営する制度でコモンクライテリアを用いて評価された結果については相互に認め合うという相互承認協定が締結された。これによりIT製品のベンダーは、調達国ごとに重複したセキュリティ評価や認証を受けることなく、製品を国際的に展開できるようになっている。

相互承認協定は、その後、多くの国が加盟し、現在ではCCRA（Common Criteria Recognition Arrangement）と呼ばれている※257。CCRAでは、自国で認証制度を運営している「認証国」と、認証制度を有しないが政府調達要件として認証結果を受け入れる「受入国」がある。2024年にベルギーとヨルダンが受入国としてCCRAに加盟し、2025年3月末現在、CCRA加盟国は認証国18ヵ国、受入国15ヵ国の計33ヵ国に上る（図3-3-7）。

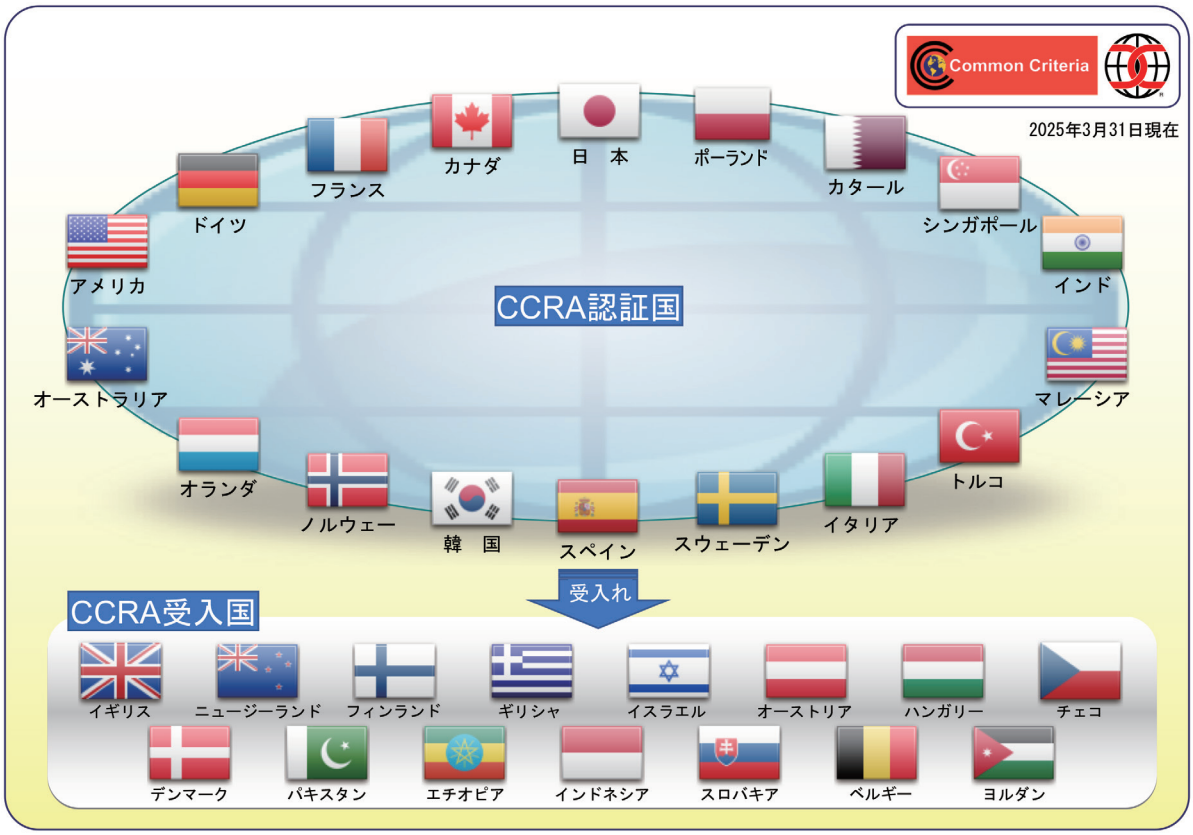
JISECを運営する日本も2003年にCCRAに認証国として加盟している。これにより、日本のベンダーはJISECを活用することで、日本語の開発資料をそのまま使用してIT製品の認証を取得することができ、かつそのIT製品がCCRA加盟国の調達対象として認められるようになっている。

また日本は2025年3月現在、CCRAの管理運営上の重要事項を議論する意思決定機関である運営委員会（MC：Management Committee）の議長国となっており、認証制度の国際連携の推進に努めている。

(3) セキュリティ要件の共通化

コモンクライテリアでは、IT製品が具備すべきセキュリティ要件を、規定された形式に従って記述することを定めている。中でも、アクセス制御機能や監査機能等、必要なセキュリティ機能の要件をテンプレート化して表現することにより、調達者が必要としているIT製品のセキュリティ要件仕様を、あいまいさを排除して製品開発者に伝えることが可能になる。このコモンクライテリア形式で表された調達要件仕様書は「プロテクションプロファイル（PP：Protection Profile）」と呼ばれている。

プロテクションプロファイルはCCRA加盟国でIT製品の政府調達要件として利用されている。プロテクションプロファイルのうち汎用的なものは、CCRAのポータルサイト※258にも掲載され、政府機関以外の機関でも同様の分野の製品を調達する際に調達要件として指定することができる。日本においても、調達要件リストでは製品分野ごとにこれらのプロテクションプロファイルを指定している。また、調達要件リストに含まれていない独自の製品



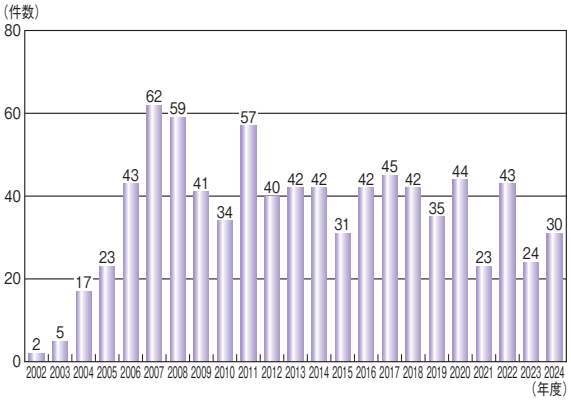
■図3-3-7　CCRA加盟国

を調達する機関は、プロテクションプロファイルを自ら作成し※259、調達を実施することもある。

同じ製品分野のIT製品調達で、複数の調達者から似ているが完全には一致していないプロテクションプロファイルが調達要件として指定されることは、別の認証として取り直す必要があることを意味し、ベンダーにとっては大きな負担となる。また、重複した評価や認証を繰り返す労力を省くというCCRAの目的にも合致しない。そこでCCRAでは、いくつかの製品分野で、加盟国の認証機関が中心となり、対象製品分野のベンダーや有識者を含む国際的な技術コミュニティを組織し、世界共通のプロテクションプロファイル「cPP（collaborative Protection Profile）」の策定を行っている。既にファイアウォール、ドライブ全体暗号化システム、ネットワークデバイス、バイオメトリクス認証、データベース管理システムやデジタル複合機等の製品分野についてcPPが策定され、CCRAポータルサイトで公開されている。

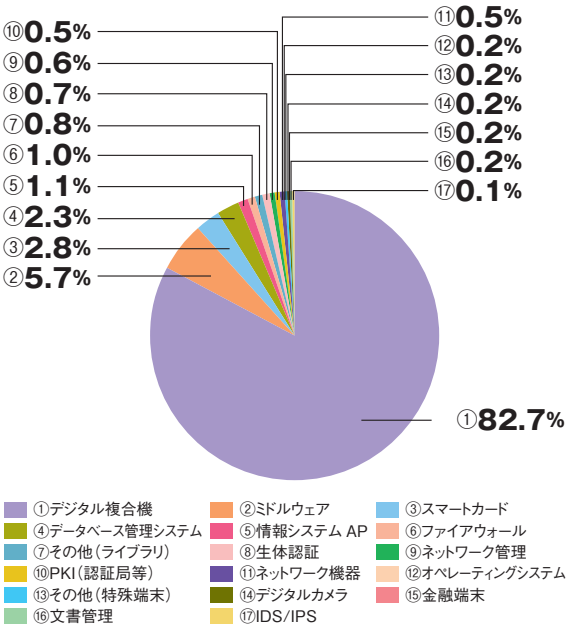
(4) 認証の状況

2024年度までのJISECにおける認証発行件数の推移を図3-3-8に示す。2024年度の認証発行件数は30件であり、2020年以降の年度別の認証発行件数は40件以上または30件以下と、年度によって大きな差がある。2019年以前は認証発行までに1年以上要する製品もあり、年度別で見ると認証発行件数は平準化されていた。近年は短期間での認証発行が実現していることもあり、製品開発サイクルの影響が認証発行件数に表れるようになってきており、年度の違いで認証発行件数が大きく増減する状況が生じている。



■図3-3-8　JISECの認証発行件数の推移

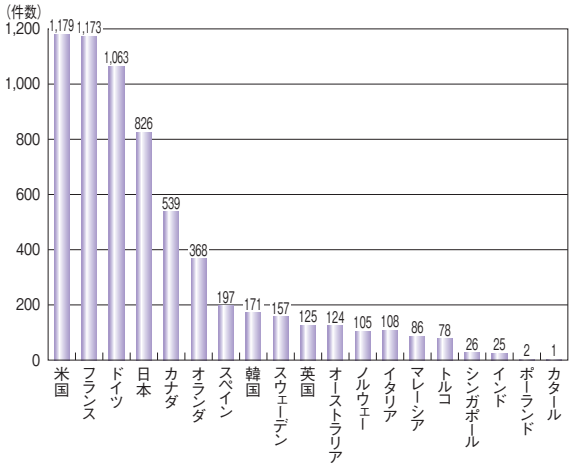
JISECにおける累計の認証発行件数の製品分野別の割合を図3-3-9に示す。認証製品分野としては、デジタル複合機が認証発行件数の8割以上を占め圧倒的に多い。これは日本のデジタル複合機ベンダーが国際的にも高いシェアを有し、CCRA加盟国においても政府調達の対象となっているからである。また、それ以外の製品分野の認証発行件数がJISECで少ないのは、セキュリティ製品全般において日本のベンダーの国際的な競争力が弱いこと、ファイアウォールやネットワーク管理製品等はシステム構築の中で組み込まれてテストされ納入されることが多いため、製品単品での調達要件の対象とならないこと等が理由である。JISECが毎年発行している認証のほとんどはデジタル複合機の新機種リリースによるものである。



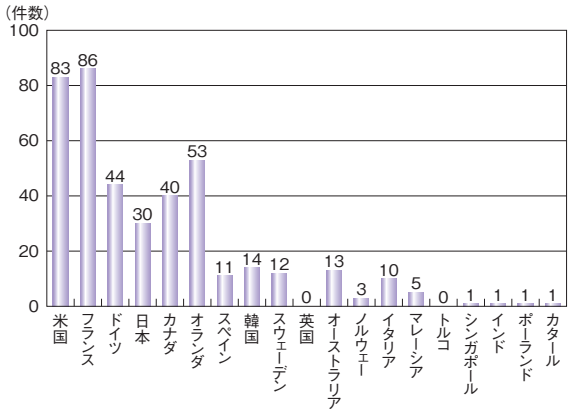
■図3-3-9　JISECの認証発行件数の製品分野別割合

CCRA加盟各国の認証機関が公開している認証発行件数の2024年度までの累計を図3-3-10（次ページ）に示す。日本の累計認証発行件数は、米国、フランス、ドイツに次いで4番目に多い。これら4ヵ国は、政府調達に認証製品を活用しているのに加えて、国内にIT製品の製造ベンダーを多く持つ国々である。近年は、新しい認証機関が設立されたオランダの認証発行件数が大きく増加しており、2024年度のオランダの認証発行件数は、フランス（86件）、米国（83件）に次ぐ3番目の53件となっている（次ページ図3-3-11）。

一方、英国のように、セキュリティ評価の歴史が長い国でも、国内の製造ベンダーの減少による制度維持コストの削減を理由に認証国から受入国に移行している国もある。韓国では、国際的に大きな市場を持つ製造ベンダーが、製品仕向地によりモバイル製品は米国で、スマー



■図 3-3-10　CCRA 各国の累計認証発行件数



■図 3-3-11　CCRA 各国の認証発行件数（2024 年度）

トカード関連製品はヨーロッパで認証を取得しているため、国内制度での認証発行件数は少ない。

(5) 2024 年度のトピック（CCRA 定期審査の受審）

JISEC に対する CCRA の定期審査が 2024 年 12 月 16 日から 12 月 20 日にわたり IPA にて行われた。CCRA では、加盟国の認証機関が CCRA の要求事項を満たしているかを確認するため、各国の認証機関が互いに審査員を派遣し、定期審査が行われることになっている。前回の JISEC に対する定期審査は 2015 年であり、新型コロナウイルスの流行により審査が延期となったこともあり 9 年ぶり 3 回目の定期審査となった。

今回の定期審査は、審査員として米国、マレーシアの認証機関から各 2 名、オブザーバーとしてインド、シンガポールの認証機関から各 2 名、合計 8 名が来日して実施され、認証制度の規程、認証員の技術的能力、運営状況等が CCRA の要求事項に適合していることが確認された。2025 年 3 月の CCRA 会合を経て、CCRA 加盟各国より認証国として継続承認を得た。

3.3.3 サプライチェーン強化に向けた対策評価制度構築に向けた検討

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対策評価制度について、中間取りまとめ※260 及び経済産業省及び NISC のプレスリリース※261 を基に紹介する。

(1) 制度構築の背景

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、事業継続に大きな影響が及ぶ事案が発生している※262。IPA による「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」では、2023 年度にサイバーインシデントの被害に遭ったと回答した企業のうち、約 7 割がサイバーインシデントにより取引先に影響があったと回答した。大企業のみならず中小企業においても、商流において多くの取引先を持ち、サプライチェーンを形成している。そのうちの 1 社がサイバー攻撃を受けた場合、前述のような被害を他社に及ぼす可能性がある。しかし、業務委託先が適切なセキュリティ対策を講じているのかを委託元が確認することは容易ではない。また、業務委託先では、各社から様々なセキュリティ対策を要求されることが、特にリソースが限られる中小企業では過度な負担となっており、サプライチェーン全体でのセキュリティ向上につながっていないことが課題となっている。

経済産業省及び NISC では、前述の課題解決に向け、産業サイバーセキュリティ研究会において、「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」を設置、2024 年 7 月に第 1 回を開催し、2025 年 4 月開催の第 5 回まで議論を重ね、検討を行った※263。この検討の結果は 2025 年 4 月 14 日に「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構築に向けた中間取りまとめ※260」として公表された。

(2) 制度の目的

こうした状況の中、前記の中間取りまとめでは、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、サプライチェーン強化に向けた対策評価制度で提示することで、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。特にサプライチェーンを構成する中小企業が自力でセキュリティ対策強化に取り組むには限界があるため、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、サプライチェーンのみならず、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。

(3) 基準の考え方

同制度では、求められるセキュリティ対策を「三つ星(★3)」「四つ星(★4)」「五つ星(★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[※264]が参考にされた[※265]。

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[※266]という先行する仕組みにおいて、一つ星、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「3.4.1 (2) (c) SECURITY ACTION」参照)。

それぞれの段階で目指す対策としては、三つ星が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、四つ星はサプライチェーン企業が標準的に目指すべきセキュリティ対策、五つ星が未知の攻撃も含めた高度なサイバー攻撃を想定する等サプライチェーン企業が到達点として目指すべき対策としている。

なお、各区分の評価スキームは三つ星が社内等の専門家による自己評価、四つ星、五つ星については、評価機関による第三者評価を想定している。

(4) 今後のスケジュール

2024年度の検討を踏まえ、2025年度には制度案の実証及び、制度構築方針の公表を予定しており、経済産業省は2026年度での制度運用開始を目指している。

3.3.4 政府情報システムのためのセキュリティ評価制度(ISMAP)

2020年6月3日、内閣官房、総務省、経済産業省は「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))」の開始をアナウンスした[※267]。本項では、ISMAPの概要や運用等について紹介する。

(1) ISMAPの概要及び制度改善の経緯

ISMAP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。政府調達において、ISMAP導入前は、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。

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[※268]」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[※269]」を発足、ISMAP管理基準を制定し、2020年6月に制度の運用を開始した。

また主に「機密性2情報[※270]」を扱うSaaSサービスに関し、リスクの小さい業務に特化した「ISMAP-LIU(ISMAP for Low-Impact Use)」を設け、2022年11月1日から運用を開始した。なお、一定のセキュリティ水準を維持しつつ、登録に必要な提出物や外部監査の対象を一部免除することでISMAP-LIUへの登録を促進することを目的とした「ISMAP-LIU登録促進のための特別措置」は、2023年5月19日に開始され、2025年3月31日に終了した。

ISMAPは2020年6月の運用開始から5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。その一方で、運用を通じた課題も明らかになってきていることから、ISMAPの信頼性・安定性の保持を前提としつつ、制度運用を合理化・明確化するため、2022年10月より「ISMAP制度改善の取組み」を継続して実施している。

2023年10月からは、「外部監査の負担軽減」や「審査の迅速化・効率化」等の諸課題を改善した運用が開始された[※271]。更に、管理基準の解釈を明確化するための「ISMAP管理基準ガイドブック」が2024年5月に作成・公開された[※272]。今後も国際規格の改訂に伴うISMAP管理基準の改定と併せて、ISMAPが担保している安全性・信頼性を保持しつつ、過剰なセキュリティレベルを求めない(合理化)、重複監査の排除、外部監査機関に競争性を持たせる等により、制度運用の合理化・明確化、クラウドサービス事業者の負荷軽減、審査の迅速化・効率化等の改善といった制度の継続的な見

直しを進めていく※273。

また、ISMAP-LIU についても、2025 年 4 月に事前申請及び事前申請に伴う影響度評価の廃止や、対象業務の拡大といった制度改善が実施された※271。

(2) ISMAP 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、ISMAP クラウドサービスリスト（以下、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 3-3-12 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。

(3) ISMAP の運用

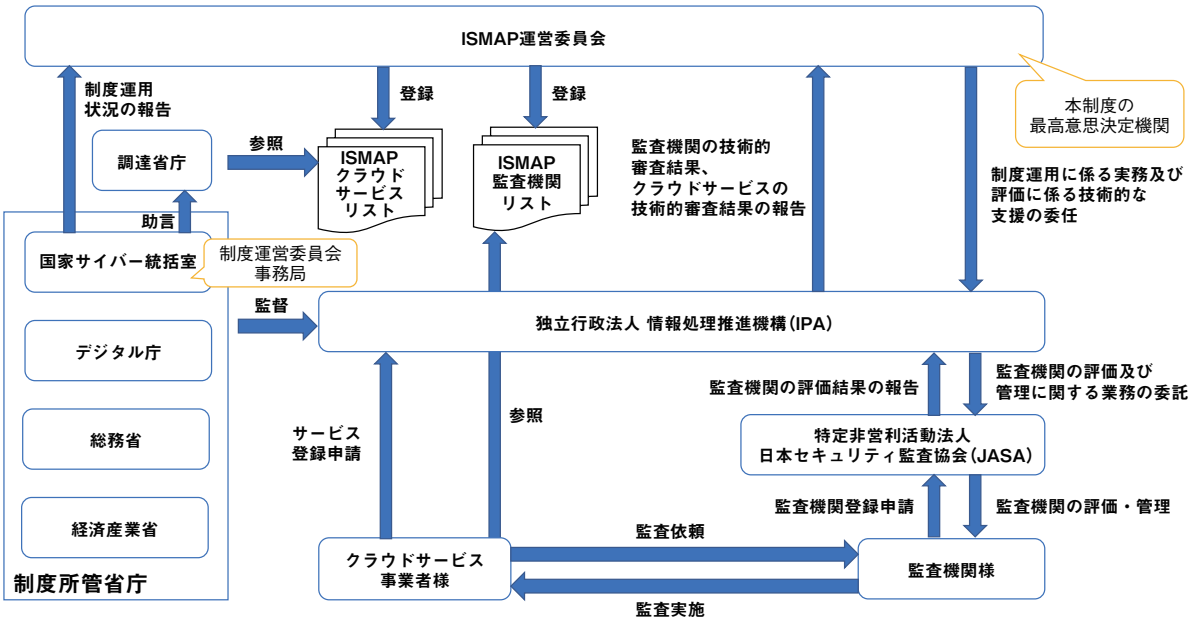
同制度は、2020 年 6 月に内閣官房（NISC、情報通信技術（IT）総合戦略室）、総務省、経済産業省の所管で運用が開始され、2021 年 9 月以降は、NISC（現 NCO）、デジタル庁、総務省、経済産業省の所管で運営されている。最高意思決定機関として ISMAP 運営委員会を設置し、事務局を NCO に置き、運用支援は IPA が担当している。

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※275 で公開されており、2025 年 4 月末日時点で、登録されている監査機関は 5 機関、クラウドサービスは 78 サービス（うち 1 件は ISMAP-LIU）である。

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※276」にも記載されている。同制度に登録されたクラウドサービスを利用したとしても、それだけでは情報システム全体のセキュリティが十分に確保されることにはならない。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分析し、適切な対策を行うことが求められる。

(4) セキュアなクラウド利用に向けて

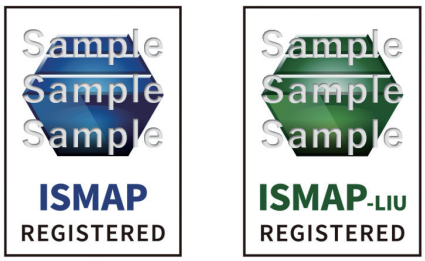
ISMAP の更なる理解促進と普及に向けて、ISMAP を象徴するロゴマーク（次ページ図 3-3-13）と、ISMAP に登録されているクラウドサービスが使用可能なロゴマーク（次ページ図 3-3-14）を作成し、公開した。また、同制度と類似する海外の制度との比較調査を実施し、調査結果について 2024 年 8 月 27 日に、IPA ホームページ



■図 3-3-12　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※274」



■図 3-3-13　ISMAP 制度のロゴマーク（サンプル）



■図 3-3-14　ISMAP に登録されているクラウドサービスが使用可能なロゴマーク（サンプル）

で公開している※277。

そのほかにも、ISMAP に係る各種主体（登録クラウドサービス事業者、クラウドサービス登録申請者、監査機関、制度所管省庁、及び ISMAP 運用支援機関等）の間で、双方向のコミュニケーションを実施・促進している。これに関連した情報発信の一環として、同制度の制度概要を分かりやすくまとめたパンフレット「はじめての ISMAP※278」を 2024 年 4 月に作成・公開した。2025 年 3 月 26 日には、2025 年度以降の ISMAP 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※273。

更に、ISMAP 制度運営側と、登録クラウドサービス事業者及びクラウドサービス登録申請者（以下、登録事業者・申請者）側の双方向でコミュニケーションを図るため、制度運営側から制度改善の取り組み状況について説明会を実施し、改善内容を説明するとともに、登録事業者・申請者側から意見を聴取している。併せて、ISMAP における情報セキュリティインシデントに関する報告について、制度運営側と登録クラウドサービス事業者側双方において速やかな情報連携・共有を図ることを目的に、報告の枠組みを設け、コミュニケーション方法を明確化した※279。

引き続き、制度運営側からの ISMAP に関する情報発信強化、及び ISMAP に係る各種主体間の双方向のコミュニケーション深化によって、同制度が担保している安全性・信頼性を確保しつつ、変化の速いクラウド分野に対応できる制度であるよう変革を進めていく。

3.3.5 CRYPTREC

電子政府のサイバーセキュリティを確保するため、デジタル庁、総務省、経済産業省、NICT、及び IPA は、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（CRYPTREC 暗号リスト※280）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、CRYPTREC（Cryptography Research and Evaluation Committees）を組織している。CRYPTREC の体制では、暗号技術検討会のもとに、暗号技術評価委員会と暗号技術活用委員会が設置されている。体制の詳細については CRYPTREC のサイト※281 を参照されたい。ここでは、2024 年度の主な活動内容及び成果をまとめる。

(1) 暗号技術検討会

暗号技術検討会は、CRYPTREC 活動計画の承認、委員会が作成する各種成果物の承認等、政策的な判断を含む総合的な観点から電子政府の安全性及び信頼性を確保する活動を推進している。2024 年度には、各委員会で作成した「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）2024 年度版※282」（以下、耐量子計算機暗号ガイドライン）及び「暗号鍵管理ガイダンス Part 2※283」について審議が行われ、承認された。また、2025 年度の活動として、耐量子計算機暗号（PQC：Post-Quantum Cryptography）に関する対応を速やかに進めることが決定された。

(2) 暗号技術評価委員会

暗号技術評価委員会は、暗号技術に対する攻撃技術の動向調査や安全性評価等、暗号技術の技術的信頼性を検討している。CRYPTREC 暗号リストに掲載されている暗号技術の安全性に関わる監視活動※284 を継続的に実施しているほか、2024 年度の主な活動内容及び成果は以下のとおりである。

- 耐量子計算機暗号ガイドライン及び調査報告書の作成
  暗号技術評価委員会の傘下に設置した WG（Working Group）において、2024 年度版の耐量子計算機暗号ガイドライン及び「CRYPTREC 耐量子計算機暗号の研究動向調査報告書※285」（以下、調査報告書）を作成した。2022 年度に作成した同様のガイドライン及び調査報告書を基に、米国政府標準暗号として規格化された ML-KEM※286、ML-DSA※287、SLH-DSA※288 の各方式や、NIST PQC 標準化プロジェクト※289 において 2022 年から追加募集が行われた PQC 署名方式の評価状況を踏まえて、安全性の根拠とする数学的問題のカテゴリーである格子、符号、多変数多項式、同種写像、ハッシュ関数のそれぞれ

に基づく方式に分類した解説を更新した。

- 量子コンピューターが共通鍵暗号の安全性に及ぼす影響の調査及び評価
  耐量子計算機暗号ガイドライン及び調査報告書において対象としているのは公開鍵暗号や署名方式であり、共通鍵暗号は含まれていない。2019 年度の技術調査報告書「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」を基に、技術の進展を反映した 2024 年度版※290 を作成した。
  2019 年度版からの結論の差異は、量子コンピューターによる攻撃では、ハッシュ関数 SHA-2 及び SHA-3 において衝突攻撃に対する安全性マージンが従来よりも下がることが明らかになったことである。このため、重要な用途に利用するハッシュ関数は、可能であれば、より安全性のマージンが確保できる出力長 384 ビットか 512 ビットのアルゴリズムを採用するのが望ましいとされた。

(3) 暗号技術活用委員会

暗号技術活用委員会は、暗号技術の普及促進、及び安全な利用等に寄与する運用ガイドラインの整備を中心に、暗号利活用に関する課題を検討している。2024 年度の主な活動内容及び成果は以下のとおりである。

- 「暗号鍵管理ガイダンス Part 2」の作成
  暗号技術活用委員会の傘下に設置した WG では、「暗号鍵管理ガイダンス Part 2」を作成した。
  情報を安全に取り扱うためには、暗号鍵の管理を適切に行うことが要求される。2023 年に公開した「暗号鍵管理ガイダンス Part 1※291」及び今回の「暗号鍵管理ガイダンス Part 2」は、暗号鍵管理機能を備えたシステムにおいて検討すべき要求項目を網羅的に解説した「暗号鍵管理システム設計指針（基本編）※292」の理解を促進することを目的として、暗号鍵管理システムのシンプルなモデル（トイモデル）を用いた各要求項目への対応例の提示等をしながら、より詳細に要求項目について解説した。これら二つのガイダンスにより、同設計指針の全要求項目をカバーした。
  「暗号鍵管理ガイダンス Part 2」で解説した内容は、「暗号鍵管理システムの概要設計に関わる項目」「暗号鍵管理デバイスの管理に関わる項目」「暗号鍵管理システムのオペレーション管理に関わる項目」である。このうち、二つ目の項目は暗号鍵管理デバイスを使って暗号鍵の管理及び保管を行うシステムの場合に、三つ目の項目は多層防御や災害・障害復旧対策等を組込むシステムの場合に特に検討が必要となる項目である。
- クラウドサービスにおける鍵管理ガイダンスの検討
  近年は、クラウドサービスを活用して情報システムを構築し、運用することも増えている。しかし、設定不備等によりクラウドサービスに預けた情報が漏えいするリスクも存在する。そこで、クラウドサービスにおける暗号鍵管理システムを適切に選択、構築、運用することを目的として、クラウドサービスにおける暗号鍵管理の仕組みや注意事項を解説したガイダンスを作成すべく、2024 年度から検討を開始した。
  2024 年度は趣旨（目的、想定読者、スコープ）、検討体制、スケジュール等のガイダンス作成方針を議論した。2025 年度から新たな WG を設置して、本格的にガイダンスの作成に着手する予定である。

(4) CRYPTREC シンポジウム 2024 の開催

CRYPTREC の活動成果を周知し、暗号技術に関する最新動向を紹介することで、社会全体のセキュリティ向上に寄与するため、CRYPTREC シンポジウムを開催している。2024 年度は 9 月 2 日に「CRYPTREC シンポジウム 2024※293」を開催し、CRYPTREC の活動報告に加え、第一人者を招いて三つの招待講演（軽量暗号と標準化動向、軽量暗号に対するサイドチャネル攻撃、暗号資産の鍵管理）を行った。

COLUMN

これからは「量子コンピューターに対して安全な暗号」を使わなければいけないの？

量子コンピューター関連技術の発達は目覚ましく、将来的には、現在使っている暗号が量子コンピューターによって解読されてしまう、と聞いたことはありませんか？　他方で、そのような事態に対応するための「量子コンピューターに対して安全な暗号」というものについても聞いたことがあるかもしれません。正式には、「耐量子計算機暗号」や「PQC（Post-Quantum Cryptography）」と呼ばれるものです。このコラムでは、このような話をどれだけ深刻に受け止める必要があるのかをお話しします。

まずは安心できる点から見ていきましょう。幸いにも、現在広く利用されている暗号が、近い将来に量子コンピューターにより解読される可能性は低いと考えられています[i]。これは、現在実現している量子コンピューターと、暗号解読に利用できる水準の量子コンピューターでは、性能に大きな隔たりがあるためです。その隔たりを埋めるためにどのくらいの期間が必要かという議論には、大きな余地があり、誰も確かなことは言えません。10 年で実現すると予想する人もいれば、永遠に実現しないと予想する人もいます。確実なのは、今、暗号解読をするのであれば、量子コンピューターよりもスーパーコンピューターを使う方が圧倒的に確実だということです。

一方で、以下に挙げるようないくつかの懸念点もあります。

一つ目の懸念点は、暗号解読できる量子コンピューターの実現時期について、確かなことは誰にも分からないということは、前述したようにかなり長い期間実現しないとの予想とは反対に、かなり短期間で実現する可能性もゼロだとは言い切れないという点です。

二つ目の懸念点は、現時点では暗号解読ができない情報であっても、遠い将来においては量子コンピューターを利用してその情報が解読されてしまうかもしれないという点です。例えば、患者を特定可能な情報を含む遺伝子疾患に関する医療情報を暗号化して保管してあったとしましょう。その情報の保護期間が 100 年と設定されていたとすると、量子コンピューターによる暗号解読が 100 年以内に実現した場合、このような情報は量子コンピューターによって解読される脅威に晒されることとなります。

三つ目の懸念点は、情報システムで使用されている暗号を変更するためには、様々な作業が発生し、それらを完了するには多くの人が想像する以上に時間がかかる点です。例えば、情報システムで使用される製品の製造事業者が PQC を搭載した製品を開発・供給する、情報システムの構築事業者が PQC を利用できるよう情報システムを更新する（ハードウェア、ソフトウェア、システムの再設計や交換が必要な場合もある）、品質保証・認定基準・監査等の手続きを更新する、更新された基準に基づいて認証を再度取得する等の一連の作業が完了してやっと暗号の変更ができるという場合もあります。これらの作業は、多くの人々が協力して行う必要があるものですが、共通の目標意識を持てなかった場合は、より長い時間がかかることになりかねません。

これらの懸念点があることから、現時点では「暗号解読される可能性が低い」のにもかかわらず、「量子コンピューターに対して安全な暗号に移行すべきだ」といった話が出てきているのです。

COLUMN

以上の背景のもと、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）は PQC の標準化を行い[ii]、それらの暗号をいつごろまでに利用するべきかの計画案を公表しました[iii]。この計画案の中では、PQC への切り替えのタイミングを 2035 年としています。また、産業界においても、これらの標準化された PQC に対応する製品が急ピッチで開発されつつあります。今後は、それらの製品が、徐々に利用されるようになると予想されています。

もっとも、情報システムで使用しているすべての暗号を PQC に置き換えるには、相当なコスト（費用及び期間）が必要となります。そもそも現実的なコストではすべての暗号を一斉に PQC に置き換えることは不可能かもしれません。そのような事情を踏まえると、保護しなければいけない期間が長く、また漏えいした場合のリスクが高い情報から優先して、PQC への置き換えを行うアプローチが効果的だと考えられます。例えば、数十年にわたって秘密裡に保管しなければならないデータは早急に対応しつつ、短期間の保護しか要求されていないデータに対しては今までどおり既存の暗号技術で対応し、長期的には徐々に PQC を利用する割合を増やすといったアプローチです。

ただし、このようなアプローチを実施するためには、対象とする情報システムが、どのようなデータに対して、どのような暗号を利用しているかということを把握していないといけません。つまり、情報システムの管理者が最初に行うべきことは、その情報システムが保護しているデータと、利用する暗号にどのようなものがあるのかを確認することなのです。

i　CRYPTREC：現在の量子コンピュータによる暗号技術の安全性への影響　https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2019.html〔2025/7/10 確認〕
ii　NIST：FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard　https://csrc.nist.gov/pubs/fips/203/final〔2025/7/10 確認〕
NIST:FIPS 204, Module-Lattice-Based Digital Signature Standard　https://csrc.nist.gov/pubs/fips/204/final〔2025/7/10 確認〕
NIST:FIPS 205, Stateless Hash-Based Digital Signature Standard　https://csrc.nist.gov/pubs/fips/205/final〔2025/7/10 確認〕
iii　NIST：IR 8547, Transition to Post-Quantum Cryptography Standards　https://csrc.nist.gov/pubs/ir/8547/ipd〔2025/7/10 確認〕　注：この計画案は、あくまでドラフト段階であり、最終稿ではありません。

3.4 組織・個人に向けたサイバーセキュリティ対策の普及活動

組織や個人に向けたサイバーセキュリティ対策の普及活動について述べる。

3.4.1 組織におけるサイバーセキュリティの取り組みと支援策

組織におけるサイバーセキュリティの実態と対策状況、普及活動及び組織に向けたサイバーセキュリティ支援策と支援ツールについて述べる。

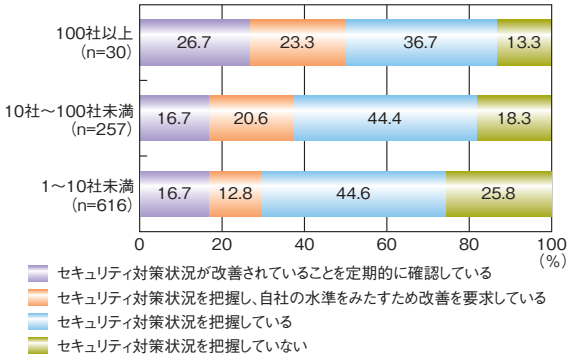
(1) 中小企業におけるセキュリティ管理体制の構築状況

中小企業における企業のセキュリティ対策・統制状況について、以下の資料を基に述べる。

- NRI セキュアテクノロジーズ株式会社（以下、NRI セキュア社）:「NRI Secure Insight 2024[※294]」（日本 1,481 社、米国 507 社、オーストラリア 503 社の企業を対象に調査。以下、NRI セキュア社調査）
- 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」（全国の中小企業の経営層及び情報システム／情報セキュリティの担当マネージャー 4,191 人を対象に調査。以下、IPA 調査）

(a) サプライチェーンのセキュリティ対策把握状況

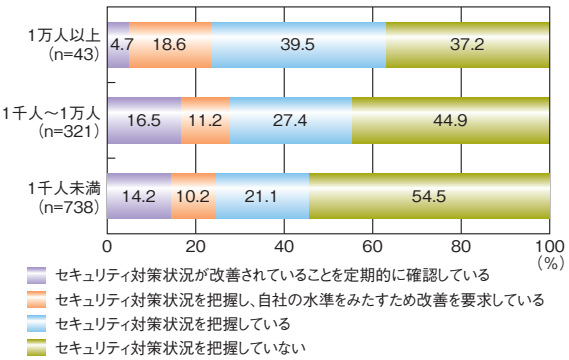
NRI セキュア社調査によると、国内関係会社／グループ会社の統制状況についてグループ会社数別で見た場合の、グループ会社数が 10 社未満である日本企業における、「セキュリティ対策状況を把握していない」の割合は 25.8% であるのに対し、グループ会社数が 100 社以上の企業における「セキュリティ対策状況を把握していない」の割合は 13.3% であった（図 3-4-1）。



■図 3-4-1　グループ会社数別で見た国内関係会社／グループ会社の統制状況
（出典）NRI セキュア社「NRI Secure Insight 2024」を基に IPA が編集

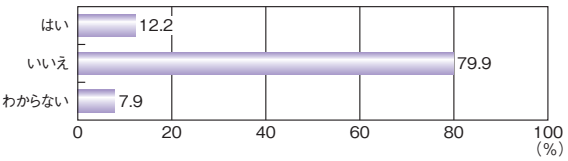
また、国内パートナー／委託先の対策状況について従業員数別で見ると、従業員数が 1 千人未満である企業では「セキュリティ対策を把握していない」の割合は 54.5% であるのに対し、従業員数が 1 万人以上の企業では 37.2% であった（図 3-4-2）。

これらにより、企業規模が大きい程、サプライチェーンにおけるセキュリティ対策状況の把握が進んでいること、また、グループ会社への統制と比較して、委託先への統制は進んでいないことが分かる。



■図 3-4-2　従業員数別で見た国内パートナー／委託先の統制状況
（出典）NRI セキュア社「NRI Secure Insight 2024」を基に IPA が編集

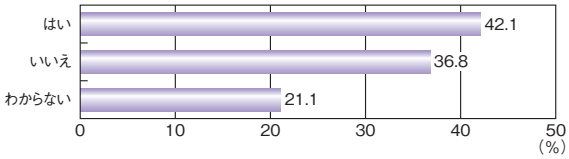
一方、中小企業を対象とした IPA 調査で「発注元企業から情報セキュリティに関する要請を受けた経験はあるか」を尋ねたところ、「はい」が 12.2%、「いいえ」が 79.9%、「わからない」が 7.9% となり、全体の 1 割強が発注元企業から情報セキュリティに関する要請を受けた経験があると回答した（図 3-4-3）。



■図 3-4-3　販売先（発注元企業）から情報セキュリティに関する要請を受けた経験（n=4,191）
（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」を基に編集

また、このうちの「はい」と答えた企業に「発注元企業から要請された情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因だと思うか」を尋ねたところ、「はい」が 42.1% となり、全体の 4 割強となることが分かった。ここから、発注元企業の求めるセキュリティ

対策に応じる、あるいはそういった対策を行っているということは、発注元企業との取り引きにつながる大きな要因になり得るということが分かる（図 3-4-4）。

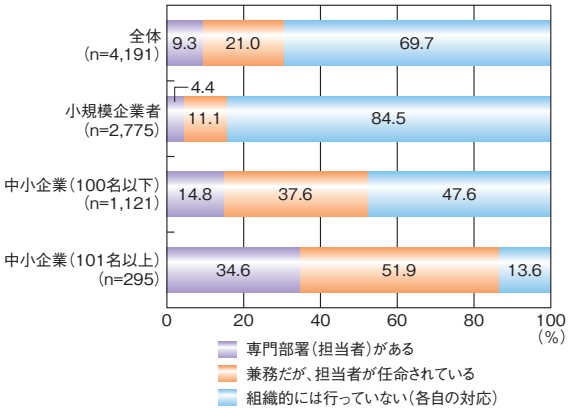


■図 3-4-4　情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因か（n=511）
（出典）IPA「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」を基に編集

(b) 中小企業の情報セキュリティ体制の整備状況

IPA 調査によると、中小企業に情報セキュリティ対策はどのような体制で行われているか、整備状況を尋ねた結果、「組織的には行っていない（各自の対応）」と回答した割合が 69.7% と最も高く、ほぼ 7 割の中小企業において情報セキュリティ体制が整備されていないことが分かる。

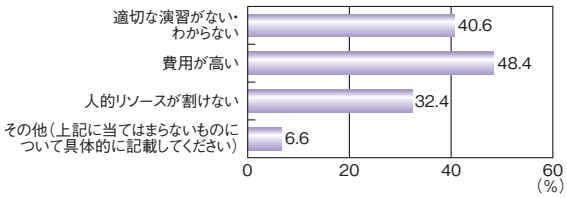
企業規模別に見ると、「小規模企業者」（5 名以下）では「組織的には行っていない（各自の対応）」割合が 84.5% であるのに対し、「中小企業（100 名以下）」では 47.6%、「中小企業（101 名以上）」では 13.6% となっており、企業規模が大きくなるにつれ、セキュリティ体制の整備がなされていることが分かる（図 3-4-5）。



■図 3-4-5　セキュリティ体制の整備状況
（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」を基に編集

(c) 中小企業の情報セキュリティ人材の教育状況

IPA 調査では、中小企業のセキュリティ人材の教育に関する調査を行っている。「セキュリティ人材を育成するために外部研修を活用している、または活用する意向があるか」を尋ねた結果、19.8% が「はい」、80.2% が「いいえ」と答えた。「いいえ」と答えた理由について尋ねた結果、「費用が高い」が 48.4%、「適切な演習がない・わからない」が 40.6% との回答があり、コストや適切な演習が分からないといったことが外部研修の活用の障壁になっていることが分かる。また、「人的リソースが割けない」が 32.4% であり、セキュリティ担当として育てる人員を確保する余裕がないことが読み取れる（図 3-4-6）。

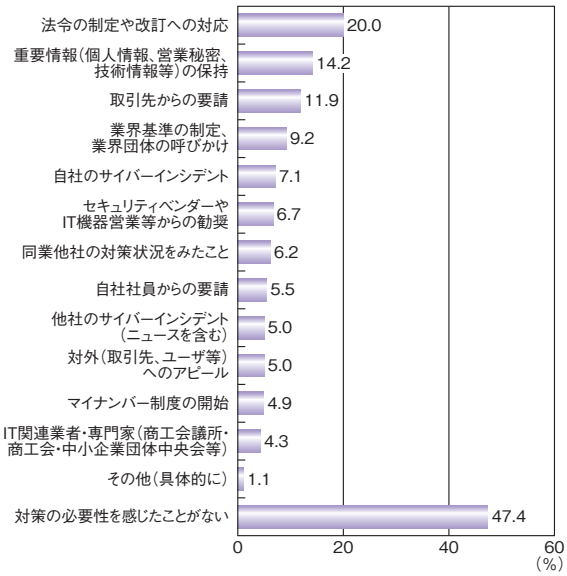


■図 3-4-6　外部研修を活用していないまたは活用する意向がない理由（n=3,361）
（出典）IPA「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」を基に編集

(d) 中小企業の情報セキュリティの技術的対策実施状況

IPA 調査によると、中小企業が情報セキュリティ対策を実施（強化）するきっかけとなった理由について、「法令の制定や改訂への対応」が 20.0% と最も多く、「重要情報（個人情報、営業秘密、技術情報等）の保持」が 14.2%、「取引先からの要請」が 11.9%、「業界基準の制定、業界団体の呼びかけ」が 9.2% と続いている（図 3-4-7）。

自ら重要情報を保持しているとの認識を持って対策を強化するケースも見られるが、外的要因（外部の基準や規程の制定や取引先からの要請）をきっかけとするケー

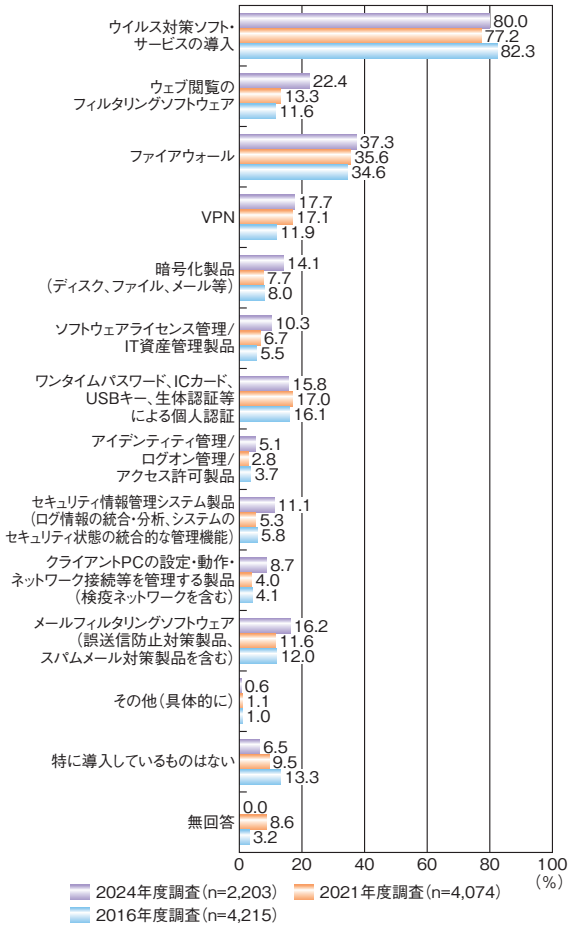


■図 3-4-7　情報セキュリティ対策を実施（強化）するきっかけとなった理由（n=4,191）
（出典）IPA「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」を基に編集

スも多いことがうかがえる。

また、図 3-4-7（前ページ）の設問に「対策の必要性を感じたことがない」以外の回答をした中小企業に対して、導入している情報セキュリティ関連製品やソフトウェアについて尋ねた結果を図 3-4-8 に示す。「ウイルス対策ソフト・サービスの導入」が 80.0% と最も高く、幅広く利用されており、基本的なセキュリティ対策は進んでいることが読み取れる。次いで、「ファイアウォール」が 37.3%、「ウェブ閲覧のフィルタリングソフトウェア」が 22.4% となった。過去 2 回の調査と比較すると、ウイルス対策ソフト・サービスの導入率は 2021 年度の 77.2% と比較して微増している。また、フィルタリングや資産管理製品の導入は拡大しており、これは新たなセキュリティニーズを反映したものであると思われる。クライアント PC の設定等を管理する製品の導入も増えており、2021 年度の 4.0% から 8.7% に増加していることから、ネットワーク管理の重要性が認識されてきていると思われる。

これらのことから、不正アクセスやデータ保護への関心と投資が高まっており、それに伴い様々なセキュリティ製品が導入されつつあることがうかがえる。



■図 3-4-8　情報セキュリティ関連製品やソフトウェアの導入状況
（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」を基に編集

(2) 組織に向けたサイバーセキュリティ支援組織・支援策と支援ツール

IPA に関連したサイバーセキュリティ支援組織・支援策と支援ツールについて紹介する。

(a) CRIC SC3

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）※295 は、産業界が一体となって中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策の推進運動を進めていくことを目的として、2020 年に設立された。設立当初は、IPA が事務局となり、取り組みを進めてきたが、更なる体制強化を行うため、2025 年 1 月に一般社団法人サイバーリスク情報センター（CRIC：Cyber Risk Intelligence Center）※296 と一体的連携を行う形式で法人化を行い、一般社団法人サイバーリスク情報センター 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（CRIC SC3）※297 として活動を開始した。

SC3 は 2020 年の設立当初からサプライチェーン対策の重要性を業界に広め、経営層への情報提供や中小企業向けの対策強化、セキュリティ人材の育成を推進し、「業界連携のプラットフォーム」としての位置付けを確立してきた。しかし、サイバー攻撃の高度化やパンデミックによるリモートワークの普及、DX の進展、生成 AI 等の環境変化に伴い、産業界のサイバーセキュリティへの意識も急速に向上、変化しており、個々の企業による対応に加えて、業種・業態を越えたサプライチェーン全体での課題対応や、産業界と政府間の連携強化の必要性が高まってきた。このような背景から、設立当初からの理念である「産業界主導による業界連携のプラットフォーム」としてサプライチェーン上のステークホルダーとの対話や政策提言を主導し、施策の実効性を高めるために、2024 年 4 月からは企画運営機能の強化、WG の再編を進めた。

業界連携、国際連携、人材育成を推進する方針が 2024 年 6 月の総会で承認されたことから、業界連携 WG、国際 WG、人材教育・育成 WG が設置され、更に WG のもとでよりターゲットを限定した SWG が活動している。業界連携 WG にはサプライチェーンサイバーセキュリティ成熟度モデル検討 SWG や工場セキュリティ共創 SWG が存在する。前者は中小企業を含めたサプライチェーン全体のセキュリティ対策の底上げを目的として、

取引先から対策状況が確認可能になるよう企業ごとに対策レベルを可視化する制度の運用を検討する（「3.3.3 サプライチェーン強化に向けた対策評価制度構築に向けた検討」参照）。後者は工場システムにおけるセキュリティの普及啓発を行うことを目的としている。

一体的連携を行っている CRIC は、セキュリティ産業の供給側であるセキュリティベンダーが活動をする CRIC SQC（セキュリティ品質検討委員会：Security Quality Committee）と、需要側のユーザー企業団体である CRIC CSF（産業横断サイバーセキュリティ検討会：Cross Sectors Forum）を有している。CRIC に、需要側の中小企業を含む団体の SC3 が加わることで、産業界におけるサイバーセキュリティ対策を包括的に議論する組織が CRIC に集約される。これにより、議論が活性化し、産業界のサイバーセキュリティ対策を推進するための様々な取り組みの実現につながることが期待される。

(b) 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を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※298」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※299」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※300」に定められている。これらを満たした民間のセキュリティ事業者のサービスが「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※301。2025 年 4 月 1 日時点で 46 事業者、78 サービスが登録されており、2025 年 3 月時点で約 8,400 の企業に導入されている。同サービスの導入に際しては、IT 導入補助金（セキュリティ対策推進枠）を申請することが可能である。2025 年度は補助の上限金額が 100 万円から 150 万円に、補助率は 2 分の 1 以内から小規模事業者限定で 3 分の 2 以内にそれぞれ引き上げられた。このように、中小企業が導入しやすいサービスとなっている。

2024 年度には、中規模以上の中小企業のセキュリティ対策のニーズに応える、お助け隊サービス 2 類制度が開始された。同制度は、従来のお助け隊サービスのコンセプトを維持しながら、価格要件を緩和したものであり、監視上限台数の拡大、監視機能の強化、定期的なコンサルティング実施等のサービス拡充を行うことが可能となった。

(c) SECURITY ACTION

「SECURITY ACTION※302」は IPA が運営する中小企業向けの情報セキュリティ対策の自己宣言制度であり、2025 年 4 月時点で、40 万件超の宣言が行われている。この制度では「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（図 3-4-10）。



■図 3-4-10 「SECURITY ACTION」ロゴマーク

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 5 か条」に取り組むことが求められる。二つ星は、「5 分でできる! 情報セキュリティ自社診断※303」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。自己宣言をすることが、経済産業省が実施する IT 導入補助金等の申請要件となっており、都道府県や市町村が提供する補助金や助成金の申請要件としても活用されている。この制度により、中小企業は情報セキュリティ対策を強化しつつ、経済的

な支援を受けることが可能になる。

(d) セキュリティインシデント対応机上演習教材

中小企業においても、サイバー攻撃によってセキュリティインシデントが発生した場合、被害とその影響範囲を最小限に抑えて事業継続を確保する必要がある。そのためには、あらかじめ対応手順の整備をしておくほか、実際にセキュリティインシデントが発生した際の対応を体験しておくことが重要である。こうしたことを踏まえ、IPAは、初動対応や再発防止策の検討を行う「セキュリティインシデント対応机上演習」を組織内で行うための教材とマニュアルを2025年4月に公開した※304。

同演習は、最初にインシデント対応のポイントを学習した後、付与されたインシデント発生状況を踏まえた対応についてディスカッションを実施し、最後に振り返りを行う流れとなっている（表3-4-1）。演習を通じ、組織の意思決定プロセスを体験する内容となっているため、セキュリティの担当者だけではなく経営層も参加することを推奨している。

演習教材は、一般企業及び医療機関においてランサムウェアに感染した場合を想定したシナリオとなっており、必要に応じて企業の設定やシステム構成等、内容をカスタマイズできる。マニュアルには、実施手順やシナリオの解説等が記載されており、中小企業のセキュリティ担当者等が演習を企画・実施しやすいようになっている。

演習を通じ、組織におけるインシデント対応の課題を発見し、体制や対応ルール等の改善を行うことで、組織のインシデント対応能力を向上させることが可能となる。

時間	内容
0:00～0:05 （5分）	オープニング（主催者挨拶、講師紹介、目的説明等）
0:05～0:25 （20分）	**講習（座学）** 「中小企業のためのセキュリティインシデント対応の手引き」をベースにインシデント対応のポイントを学ぶ。
0:25～1:25 （60分） ※説明、発表時間を含む	**演習1** 発生した事案の初動対応について、グループディスカッションにより対応方針等を検討する。
1:25～1:35 （10分）	（休憩）
1:35～2:35 （60分） ※説明、発表時間を含む	**演習2** 業務・システムの復旧や再発防止、公表等について、グループディスカッションにより対応方針等を検討する。
2:35～2:50 （15分）	振り返り
2:50～3:00 （10分）	質疑応答・クロージング

■表3-4-1　セキュリティインシデント対応机上演習のタイムスケジュール
（出典）IPA「セキュリティインシデント対応机上演習教材※304」

(e) 制御システムのセキュリティリスク分析ガイド

IPAは、制御システムのセキュリティ向上を目的として2017年10月、「制御システムのセキュリティリスク分析ガイド」の第1版を公開し、2018年10月には第2版を公開した。2023年3月に記載誤り等を訂正した最新版を公開している※305。同ガイドは、既存の規格やガイドラインで要求されているリスク分析の手順について事業者が実施できるように解説したガイドブック（手引き書）である。同ガイドの第1版公開後、同ガイドや付随する別冊資料や補足資料の拡充を行っており、2024年は以下の追加公開を行った。

- 2024年3月、同ガイドの補足資料である「制御システム関連のサイバーインシデント事例」シリーズにおいて、「【事例10】2022年 衛星通信網へのサイバー攻撃の事例」「【事例11】2022年 電力網への攻撃の事例」を公開した※306。同シリーズでは、インシデント事例の概要と攻撃の流れ（攻撃ツリー）を紹介しており、制御システム保有事業者が、同ガイドに提唱された「事業被害ベースのリスク分析」を実施する際に活用できる。
- 2024年12月、同ガイドの別冊として「制御システムに対するリスク分析の実施例 第2版 事例2：社外サービスと接続した制御システムに対するリスク分析※307」を公開した。同文書では、外部サービスと接続した制御システムのリスク分析を行い、「外部ネットワークから攻撃者が侵入する脅威」を新たに想定している。
- 2024年12月、同ガイドの補足資料として「『制御システムのセキュリティリスク分析ガイド』と国際規格との比較※308」を公開した。同資料では、リスクアセスメントに言及する国際規格ISO/IEC 27000シリーズ、IEC 62443シリーズやNIST SP 800-30等と同ガイドを比較し、評価項目の類似性や違いを明確にしている。

また2024年10月には「『スマート工場のセキュリティリスク分析調査』調査報告書 第2版※309」を公開した。第2版には、スマート工場化に伴う制御システムの新たな課題を調査する目的で実施された「高度制御を実現する新たな制御システムのスマート化モデル類型細分化と対策の調査」の調査結果が追加された。同調査では、実装モデルに対するリスク分析手法として「制御システムのセキュリティリスク分析ガイド」を用いている。

IPA では、同ガイドや事例シリーズの提供だけなく、効果的なリスク分析を実施するためのセミナーを開催し、セキュリティ対策としてのリスク分析の有効性及びリスク分析手法の理解を深める活動に取り組んでいる※310。

3.4.2 サイバーセキュリティ及びネットリテラシーの普及活動

本項では、インターネットにまつわる不適切な利用事例の紹介と、その解決に向けたネットリテラシー向上のための啓発活動について述べる。

(1) 生成 AI の安全利用に関する啓発活動

近年、高精度な文章や画像等を生成する生成 AI が、急速に発展しており、個人でも生成 AI を簡単に利用できるようになってきている。それに伴い、生成 AI を悪用した犯罪や、情報の漏えい等が問題となっている。

2024 年 5 月、インターネット上で公開されている対話型生成 AI を悪用してマルウェアを作成したとして、川崎市在住の 25 歳の無職の男性が不正指令電磁的記録作成容疑で逮捕された※163。複数の対話型生成 AI に指示を出してマルウェアの設計情報を回答させ、回答内容を組み合わせてマルウェアを作成したという。

また、2025 年 3 月にミャンマーで大地震が発生した際には、AI で作成されたフェイク画像や動画が出回り、各国のメディアが誤って引用してしまう等、混乱を招く事態に陥った※311。

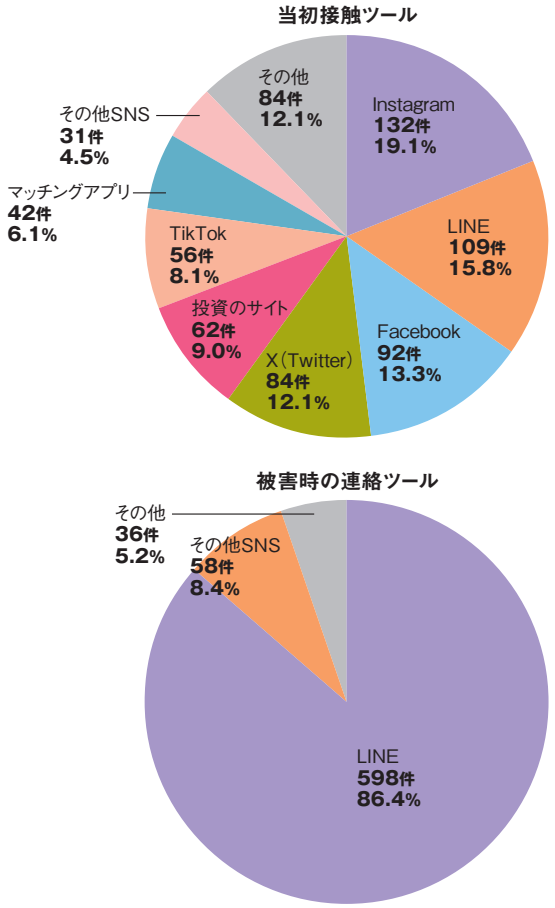
総務省は、生成 AI を活用する上で注意すべきことをクイズ形式で学べる啓発教材「生成 AI はじめの一歩～生成 AI の入門的な使い方と注意点～※312」を公開した。同教材では、生成 AI の活用にあたって注意すべきポイントとして「情報の正確性」「情報流出」「知的財産権の侵害」「活用者としてのモラル」の四つを挙げている。

なお、生成 AI については、「2.1 AI セーフティ実現に向けた取り組み」も参照いただきたい。

(2) SNS を使った詐欺防止に向けた啓発活動

近年、SNS を悪用した詐欺の被害が急増している。2025 年 2 月、60 代の女性が、SNS を通じて嘘の投資話を持ちかけられ、現金 2,200 万円を騙し取られる事件があった※313。

警察庁は「警察庁・SOS47 特殊詐欺対策ページ※314」で、このような SNS 型投資詐欺について、手口と被害の実態や、実際の事例を丁寧に解説している※315。被害の実態については、SNS 等の様々なチャネルから接触を図った後、被害時の連絡ツールとして LINE が使用されるケースが多いことが示されている（図 3-4-11）。事例の紹介では、被害者の年齢や被害金額に加え、「必ず儲かります」「投資用アプリをインストールしてください」といった、詐欺に用いられるキーワードを挙げながら解説している。最後に、気を付けるべきポイントとして「投資先が実在しているか・国の登録業者かどうか」「振込先の口座に不審な点がないか」等を挙げ、注意を促している。



■図 3-4-11　SNS 型投資詐欺の被害の実態（2025 年 1 ～ 2 月、総数 692 件）
（出典）警察庁「SNS 型投資詐欺※315」を基に IPA が編集

また、金融庁では、「詐欺的な投資に関する相談ダイヤル」を開設し、SNS 型投資詐欺による損害を被った場合に限らず、詐欺的な投資勧誘を受けて不審に思った場合や、投資について悩んでいる場合の相談等を受け付けている※316。

2025 年 1 月、50 代の無職の男性が、マッチングアプリで知り合った人物から、SNS を通じたやり取りで「会うためには会員カードを作る必要がある」等と言われ、現金 125 万円を騙し取られる SNS 型ロマンス詐欺の被害に遭った※317。

警察庁はSNS型ロマンス詐欺についても対策ページを公開しており、「実際に会ったことがない人からお金の話をされたら要注意」と呼びかけている※318。

また、2024年12月に岩手県警察はNTT東日本岩手支店、セコム株式会社岩手統括支社と「地域の安全・安心の実現に向けた連携協定」を締結し、特殊詐欺被害防止のための広報啓発活動や、特殊詐欺を認知した際の積極的な通報等に連携して取り組むことを発表した※319。

(3)闇バイト防止のための啓発活動

2024年8月から11月にかけて、1都3県でいわゆる闇バイト※320との関連が疑われる強盗事件が19件発生した※321。これらの事件により逮捕された47人のうち37人が20代以下であり、若年層が闇バイトに応募し犯罪の実行者となるケースが目立っている。2024年9月、さいたま市で起きた事件では、住宅に20代の男らが押し入り、住人女性2人が粘着テープのようなもので拘束され、現金約10万円とキャッシュカード等が奪われた※322。2024年10月には横浜市内で男性高齢者が殺害され、現金や貴金属等が奪われるといった凶悪な事件も起きた※323。

文部科学省は、YouTubeの「文部科学省／mextchannel※324」で、闇バイトの危険性をドラマ形式で説明した「教材㉗情報の真偽を確かめよう! SNS闇バイト編(高校生)※325」を公開した。

警視庁では、闇バイトに申し込んでしまった場合、警視庁総合相談センターまたはヤング・テレホン・コーナー(警視庁少年相談係)に相談するよう呼びかけている※326。

また、LINEヤフー株式会社と国立大学法人静岡大学は、闇バイトの加担リスクを学ぶことを目的とした中学生・高校生向けの情報モラル教材「『闇バイト』を自分ごととして考えてみよう～闇バイトに注意!あなたを犯罪に巻き込む手口～」を公開した※327。同教材では、実際に闇バイトを募集する側に立ち、募集コメントを考える経験を通じて、闇バイトの可能性がある募集の見極め方を学ぶことができる。

(4)誹謗中傷防止のための啓発活動

インターネット上での誹謗中傷は、2024年夏に開催されたパリ2024オリンピック・パラリンピック競技大会でも問題となった。競歩の日本代表2人が混合リレーに専念するため、個人種目を辞退したことをめぐり、誹謗中傷が相次ぎ、選手が自身のSNSで「たくさんの方からの厳しい言葉に傷ついた。このようなことが少しでも減ってほしい」と投稿した※328。公益財団法人日本オリンピック委員会も異例の声明を出し、行き過ぎた内容に対しては警察への通報や法的措置も検討する姿勢を示す事態となった※329。

相次ぐ誹謗中傷に対して、開示請求を行う動きが増えている。芸能事務所の株式会社セント・フォースは2025年2月26日、公式サイトを更新し、所属タレントに対するネット上の誹謗中傷や虚偽の情報の拡散について「弊社はタレントの安全と尊厳を守るため、悪質な誹謗中傷・デマの拡散について、法的措置を含めた厳正な対応を進めてまいります。具体的には、弁護士と連携のもと、発信者情報開示請求を行い、悪質な投稿の発信者に対する適切な措置を講じます」と声明を発表した※330。

総務省では、一般社団法人ソーシャルメディア利用環境整備機構、一般社団法人セーファーインターネット協会及び法務省と共同して、特設サイト「#NoHeartNoSNS※331」を開設し、誹謗中傷に対する相談窓口を紹介している(図3-4-12)。



■図3-4-12　#NoHeartNoSNS
(出典)一般社団法人ソーシャルメディア利用環境整備機構「#NoHeartNoSNS」

法務省はYouTubeの「MOJchannel※332」で、「人権啓発動画『インターネットはヒトを傷つけるモノじゃない。』※333」を公開し、インターネット上の誹謗中傷等の根絶を呼びかけている※334。

(5)ネットリテラシー向上のための啓発活動

NISCは毎年2月1日から3月18日を「サイバーセキュリティ月間」と定め、「#サイバーセキュリティは全員参加」というキャッチフレーズのもと、中央省庁のほか、民間企業でも様々な啓発イベントやコンテンツの公開を実施している※335。

2024 年度の「サイバーセキュリティ月間」にあわせて NISC は、「インターネットの安全・安心ハンドブック Ver 5.10[※336]」を公開した。

内閣府大臣官房政府広報室は、「スマートフォンのセキュリティ対策できていますか? 4 つのポイント[※337]」を公開し、電子メールや SMS 内のリンクは安易にタップせず、携帯電話会社等が提供するセキュリティ設定を活用する等の対策を徹底するよう呼びかけている。

総務省は、インターネットや SNS における利用者の ICT リテラシー向上を目指し、プラットフォーム事業者や通信事業者、IT 企業・団体等とともに官民連携プロジェクト「DIGITAL POSITIVE ACTION[※338]」を開始した。

また、総務省では Web サイト「上手にネットと付き合おう! 安心・安全なインターネット利用ガイド[※339]」を運営しており、2024 年度は、青少年、保護者、シニアを対象に、ICT リテラシーを身に付けるための教材「5 つの分野の ICT リテラシーを学ぼう ～つくろう!守ろう!安心できる情報社会～[※340]」を公開した(図 3-4-13)。



■図 3-4-13　青少年向け啓発教育教材
(出典)総務省「5 つの分野の ICT リテラシーを学ぼう ～つくろう!守ろう!安心できる情報社会～」

COLUMN

セキュリティは「コスト」か「投資」か?

現代社会において、企業や組織が直面するサイバーセキュリティ上の脅威はますます深刻化していますが、脅威に対応するためのセキュリティ対策を「コスト」としてとらえるべきか、積極的な「投資」ととらえるべきかという議論が昔からされてきました。

長年にわたり、セキュリティ対策が直接的な収益を生まないことから「(やむを得ない) コスト」とみなされてきました。例えば、企業がファイアウォールやセキュリティソフトを導入する場合、それらの製品購入費、ライセンス料、保守費用等に加え、専門スタッフの雇用や教育、システムの運用監視のための人的リソースも必要です。これらは目に見える形では利益に直結しないため、「コスト」と感じられるのも無理はありません。特に予算が限られている中小企業にとっては、こうした費用を負担に感じる場合もあることから、セキュリティ対策への出費がなかなか進まなかったという側面があります。

これに対して、2015 年に経済産業省と IPA が「サイバーセキュリティ経営ガイドライン[i]」を発表して、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不可欠な「投資」であると位置付け、経営者に対してセキュリティ対策への出費を促しました。例えば、サイバー攻撃によるシステムダウンが発生すれば、業務停止による機会損失は計り知れません。特に、現代ではデジタル化が進み、オンラインでの取り引きやサービス提供が主流となっています。この環境下でシステムが脆弱であれば、顧客は安心してサービスを利用できず、競争力を失うことになります。逆に、強固なセキュリティをアピールできれば、顧客からの信頼を獲得し、長期的な収益増加につなげられるというわけです。

ところが最近、このセキュリティ対策は「投資」であるという考え方に疑問を持つ声が増えていきています。その理由の一つは、やはりセキュリティ対策の効果は事後的にしか評価できないという点にあります。例えば、新しいマーケティング戦略や設備導入といった投資では、事前に ROI (投資収益率) を予測し、その成果を数値で追跡することが可能ですが、セキュリティ対策の場合、「攻撃が防げた」「被害がゼロだった」といった成果は、実際に何かが起こらなかったことを証明するものであり、具体的な利益として計上することは難しいという特性があるからです。セキュリティ対策の ROI を定義しようという試みもされてきましたが、未だに説得力のある定義はされていません。また、セキュリティや個人情報保護に関する法規制や、サプライチェーンにおける発注元からの要求等、社会的要請への対応や社会的責任を果たすための「必要なコスト」であると考えるべきだとの意見が台頭してきています。

しかしながら、この「コスト」か「投資」という議論は、視点の違いに過ぎません。現状の課題に対応するという視点からは「コスト」と言えるでしょうし、将来起こる可能性がある課題に先んじて対応し企業競争力を高めるという視点からは「投資」と言えるでしょう。いずれにしても大切なことは、セキュリティ対策は、企業の規模や業種を問わず普遍的なものであるということです。リスク評価を行い、自組織にとって最適な対策を見極め、過少でも過度でもない適切な出費を行うことこそが重要であると考えます。

i https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf〔2025/7/10 確認〕

※ 1　https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf〔2025/6/26 確認〕
※ 2　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〔2025/6/26 確認〕
※ 3　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〔2025/6/26 確認〕
※ 4　内閣府：官報 令和７年５月23日号外第113号（p.75）　https://www.kanpo.go.jp/20250523/20250523g00113/20250523g001130075f.html〔2025/6/26 確認〕
※ 5　https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/index.html〔2025/6/26 確認〕
※ 6　https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/koujou_teigen/teigen.pdf〔2025/6/26 確認〕
※ 7　https://www.nisc.go.jp/pdf/policy/kihon-s/250529kikkin.pdf〔2025/6/26 確認〕
※ 8　NCO：国家サイバー統括室の設置について　https://www.nisc.go.jp/pdf/press/NCO0701.pdf〔2025/7/2 確認〕
NCO：概要　https://www.nisc.go.jp/about/overview/index.html〔2025/7/2 確認〕
※ 9　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〔2025/6/26 確認〕
※ 10 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〔2025/6/26 確認〕
※ 11 https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/shin_cyber_leaflet.pdf〔2025/6/26 確認〕
※ 12 https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/gaiyou.pdf〔2025/6/10 確認〕
※ 13 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〔2025/6/26 確認〕
※ 14 経済安全保障推進法に基づき指定される、基幹インフラ事業（15事業）を行う者のうち、特定重要設備（役務の安定的な提供のために重要であり、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）の機能が停止・低下した場合に、役務の安定的な提供に支障が生じ、国家・国民の安全を損なう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。2025 年５月時点で 249 者。
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〔2025/6/26 確認〕
※ 15 柿沼重志：能動的サイバー防御の導入（立法と調査 474 号）　https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/2025pdf/20250414003.pdf〔2025/6/26 確認〕
※ 16 https://laws.e-gov.go.jp/law/426AC1000000104〔2025/6/26 確認〕
※ 17 サイバーセキュリティ戦略本部：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5年度版）　https://www.nisc.go.jp/pdf/policy/general/kijyunr5.pdf〔2025/6/26 確認〕
※ 18 NISC：政府機関等の対策基準策定のためのガイドライン（令和5年度版）　https://www.nisc.go.jp/pdf/policy/general/guider6.pdf〔2025/6/26 確認〕
※ 19 NISC：「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」　https://www.nisc.go.jp/policy/group/general/sbd_sakutei.html〔2025/6/26 確認〕
※ 20 NISC：横断的アタックサーフェスマネジメント（ASM）事業の運用開始に係るプレスリリース　https://www.nisc.go.jp/pdf/press/20240719NISC_press.pdf〔2025/6/26 確認〕
※ 21 NISC：2024 年度 官民連携演習等 実施結果　https://www.nisc.go.jp/pdf/policy/infra/NISC_enshu_20250527.pdf〔2025/6/26 確認〕
※ 22 https://www.mhlw.go.jp/content/10808000/001262036.pdf〔2025/6/26 確認〕
※ 23 https://www.mhlw.go.jp/content/10808000/001262037.pdf〔2025/6/26 確認〕
※ 24 https://www.mhlw.go.jp/content/10808000/001261299.pdf〔2025/6/26 確認〕
※ 25 https://mist.mhlw.go.jp/〔2025/6/26 確認〕
※ 26 https://www.meti.go.jp/shingikai/mono_info_service/medical_information_system/checklist.html〔2025/6/26 確認〕
※ 27 e-Gov 法令検索：地方自治法（昭和二十二年法律第六十七号）　https://laws.e-gov.go.jp/law/322AC0000000067/20261225_506AC0000000065〔2025/6/26 確認〕
※ 28 AISI：AI セーフティに関する評価観点ガイド（第 1.00 版）　https://aisi.go.jp/assets/pdf/ai_safety_eval_v1.00_ja.pdf〔2025/6/26 確認〕
なお、2025 年３月に、マルチモーダル基盤モデルに対して AI セーフティ評価を行う際に重要となる評価観点及び評価項目例を追記した第 1.10 版が公開されている（AISI:AI セーフティに関する評価観点ガイド（第 1.10 版）　https://aisi.go.jp/assets/pdf/ai_safety_eval_v1.10_ja.pdf〔2025/6/26 確認〕）。
※ 29 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 1.00 版）　https://aisi.go.jp/assets/pdf/ai_safety_RT_v1.00_ja.pdf〔2025/6/26 確認〕
なお、2025 年３月に、画像等のマルチモーダル情報に関する攻撃手法等の追記に加え、新たに作成した詳細解説書やレッドチーミングの成果物例を含めた第 1.10 版が公開されている（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/effort/effort_information/250331_1/〔2025/6/26 確認〕）。
※ 30 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〔2025/6/26 確認〕
※ 31 経済産業省：第9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/009_03_00.pdf〔2025/6/26 確認〕
※ 32 総務省：令和6年度医療分野向けサイバーセキュリティ演習のご案内　https://www.jmha.or.jp/contentsdata/keiei/dx/cynex_sankousiryou.pdf〔2025/6/26 確認〕
※ 33 https://www.meti.go.jp/press/2024/08/20240829001/20240829001-1r.pdf〔2025/6/26 確認〕
※ 34 2025 年３月に開催された第 15 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において、「セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス案（中間整理）」（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/015_s01_00.pdf〔2025/6/26 確認〕）が提示された。
※ 35 e-Gov 法令検索：国立研究開発法人情報通信研究機構法（平成十一年法律第百六十二号）　https://laws.e-gov.go.jp/law/411AC0000000162〔2025/6/26 確認〕
※ 36 NICT：IoT 機器のセキュリティ向上を推進する新しい「NOTICE」を開始　https://www.nict.go.jp/press/2024/03/29-2.html〔2025/6/26 確認〕
※ 37 NOTICE：NOTICE の取り組みに、新たに IoT 機器メーカー・関連団体からも参加いただきました　https://notice.go.jp/news/topic/news20240828_2〔2025/6/26 確認〕
※ 38 C&C サーバー：Command and Control サーバーの略。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。
※ 39 一般社団法人 ICT-ISAC：電気通信事業者におけるフロー情報分析による C&C サーバ検知に関する調査について（分析事業者の拡大）　https://www.ict-isac.jp/news/news20240625.html〔2025/6/26 確認〕
※ 40 IPA：登録番号 2024-　https://www.ipa.go.jp/security/sme/otasuketai/servicelist/category2/registration-number2024.html〔2025/6/26 確認〕
※ 41 例えば、政府広報ラジオ番組「杉浦太陽・村上佳菜子 日曜まなびより」2月16日（日曜日）放送「備えて安心!中小企業のサイバーセキュリティお助け隊サービス」（https://www.gov-online.go.jp/article/202502/radio-2765.html〔2025/6/26 確認〕）、日経ビジネス広告記事「中小企業のサイバーセキュリティー対策『お助け隊サービス』で中小企業をサイバー攻撃から守る」（https://special.nikkeibp.co.jp/atclh/ONB/25/gov_online0214/〔2025/6/26 確認〕）。
※ 42 経済産業省:第11回産業サイバーセキュリティ研究会WG2（地域・中小企業支援）事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/011_03_00.pdf#page=30〔2025/6/26 確認〕
※ 43 IPA：サイバーセキュリティ相談会・マネジメント指導　https://www.ipa.go.jp/security/seminar/sme/riss-katsuyo.html〔2025/6/26 確認〕
※ 44 NISC、警察庁：人権保護や民主主義の推進に関与する組織や個人のためのサイバー脅威緩和に関する国際ガイダンスへの共同署名について　https://www.nisc.go.jp/pdf/press/press_Mitigating_Threats.pdf〔2025/6/26 確認〕
※ 45 NISC、警察庁：豪州主導の APT40 グループ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.nisc.go.jp/pdf/press/press_APT40Advisory.pdf〔2025/6/26 確認〕

※ 46 NISC、警察庁、外務省：「カウンターランサムウェア・イニシアティブ会合」への参加　https://www.nisc.go.jp/pdf/press/press_cri_statement_20241003.pdf〔2025/6/26 確認〕
※ 47 NISC：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　https://www.nisc.go.jp/pdf/news/press/250114_jointstatement_jpn.pdf〔2025/6/26 確認〕
※ 48 NISC：英国主導の「サイバーセキュリティ人材に関する国際的な連合」への参画について　https://www.nisc.go.jp/pdf/press/2025_International_Coalition_on_Cyber_Security_Workforces.pdf〔2025/6/26 確認〕
※ 49 外務省：日本のサイバー分野での外交　二国間協議・対話等 https://www.mofa.go.jp/mofaj/fp/nsp/page24_000687.html〔2025/6/26 確認〕
※ 50 外務省：第３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_01135.html〔2025/6/26 確認〕
※ 51 外務省：G7 プーリア・サミット（概要）　https://www.mofa.go.jp/mofaj/ecm/ec/pageit_000001_00752.html〔2025/6/26 確認〕
※ 52 National Cybersecurity Agency：G7 cybersecurity working group　https://www.acn.gov.it/portale/en/w/gruppo-di-lavoro-g7-sulla-cybersicurezza〔2025/6/26 確認〕
※ 53 National Cybersecurity Agency：Press statement of the President of the G7 Cybersecurity Working Group, Bruno Frattasi　https://www.acn.gov.it/portale/en/w/dichiarazione-alla-stampa-del-presidente-del-gruppo-di-lavoro-g7-sulla-cybersicurezza-bruno-frattasi〔2025/6/26 確認〕
※ 54 NISC、総務省、経済産業省：第 17 回　日 ASEAN サイバーセキュリティ政策会議の結果　https://www.nisc.go.jp/pdf/press/17thAJCPM_ja.pdf〔2025/6/26 確認〕
※ 55 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/2024/11/20241115001/20241115001.html〔2025/6/26 確認〕
※ 56 警察庁：令和6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/R6/R06_cyber_jousei.pdf〔2025/6/26 確認〕
※ 57 https://laws.e-gov.go.jp/law/504AC0000000043〔2025/6/26 確認〕
※ 58 https://laws.e-gov.go.jp/law/506AC0000000027〔2025/6/26 確認〕
※ 59 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〔2025/6/26 確認〕
※ 60 https://www8.cao.go.jp/cstp/anzen_anshin/kprogram.html〔2025/6/26 確認〕
※ 61 内閣府、文部科学省：「人工知能（AI）が浸透するデータ駆動型の経済社会に必要な AI キュリティ技術の確立」に関する研究開発構想（個別研究型）　https://www8.cao.go.jp/cstp/anzen_anshin/20221021_next_3.pdf〔2025/6/26 確認〕
※ 62 JST：経済安全保障重要技術育成プログラム（K Program）における新規採択課題の決定について（令和5年度第3回募集 AIセキュリティ）　https://www.jst.go.jp/pr/info/info1712/pdf/info1712.pdf〔2025/6/26 確認〕
※ 63 内閣府、文部科学省：「サプライチェーンセキュリティに関する不正機能検証技術の確立（ファームウェア・ソフトウェア）」に関する研究開発構想（個別研究型）　https://www8.cao.go.jp/cstp/anzen_anshin/20230310_next_2.pdf〔2025/6/26 確認〕
※ 64 JST：経済安全保障重要技術育成プログラム（K Program）における新規採択課題の決定について（令和5年度第2回募集）　https://www.jst.go.jp/pr/info/info1697/pdf/info1697.pdf〔2025/6/26 確認〕
JST：経済安全保障重要技術育成プログラム（K Program）における新規採択課題の決定について（令和5年度第4回募集、令和6年度第3回募集）　https://www.jst.go.jp/pr/info/info1749/pdf/info1749.pdf〔2025/6/26 確認〕
※ 65 内閣府、文部科学省：「セキュアなデータ流通を支える暗号関連技術（高機能暗号）」に関する研究開発構想（個別研究型）　https://www8.cao.go.jp/cstp/anzen_anshin/4_20231225_next.pdf〔2025/6/26 確認〕
※ 66 JST：経済安全保障重要技術育成プログラム（K Program）における新規採択課題の決定について（令和5年度第4回募集、令和6年度第1回募集）　https://www.jst.go.jp/pr/info/info1747/pdf/info1747.pdf〔2025/6/26 確認〕
※ 67 内閣府、経済産業省：「偽情報分析に係る技術の開発」に関する研究開発構想（個別研究型）　https://www8.cao.go.jp/cstp/anzen_anshin/02-07_20231020_meti_5.pdf〔2025/6/26 確認〕
※ 68 NEDO：「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 ―複数の根拠から真偽判定を支援する偽情報対策システムの開発を目指す―　https://www.nedo.go.jp/news/press/AA5_101763.html〔2025/6/26 確認〕
※ 69 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〔2025/6/26 確認〕
※ 70 NEDO：「経済安全保障重要技術育成プログラム」で先進的サイバー防御機能・分析能力強化に着手　―自由、公正かつ安全なサイバー空間の確保を目指す―　https://www.nedo.go.jp/news/press/AA5_101762.html〔2025/6/26 確認〕
※ 71 「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施行令（令和四年政令第三百九十四号）」（https://laws.e-gov.go.jp/law/504C00000000394〔2025/6/26 確認〕）の第 12 条第 1 項参照。
※ 72 本文に掲げた技術についての調査結果は、「令和6年度特定技術分野における産業の発達への影響に関する調査　ー耐タンパ性ハウジングにより計算機の部品等を保護する技術ー」（https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/patent/doc/patent_sangyou_r6_4.pdf〔2025/6/26 確認〕）及び「令和6年度特定技術分野における産業の発達への影響に関する調査　ー通信妨害等に関する技術ー」（https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/patent/doc/patent_sangyou_r6_5.pdf〔2025/6/26 確認〕）として公表された。
※ 73 https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/pdf/torimatome.pdf〔2025/6/26 確認〕
※ 74 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〔2025/6/26 確認〕
※ 75 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〔2025/6/26 確認〕。
※ 76 https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/sankou_hyouka.pdf〔2025/6/26 確認〕
※ 77 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〔2025/6/26 確認〕
※ 78 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〔2025/6/26 確認〕
※ 79 デジタル庁：デジタル社会推進標準ガイドライン　https://www.digital.go.jp/resources/standard_guidelines/〔2025/6/4 確認〕
※ 80 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a547f9a6/20250630_resources_standard_guidelines_technical_report_01.pdf〔2025/7/1 確認〕
※ 81 https://www.nisc.go.jp/policy/group/general/kijun.html〔2025/6/4 確認〕
※ 82 https://www.digital.go.jp/resources/standard_guidelines/#ds202〔2025/6/4 確認〕
※ 83 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/2aa40167/20250630_resources_standard_guidelines_technical_report_02.pdf〔2025/7/1〕
※ 84 IIA（一般社団法人日本内部監査協会訳）：IIA の３ラインモデル https://www.iiajapan.com/leg/pdf/data/iia/2020.07_1_Three-Lines-Model-Updated-Japanese.pdf〔2025/6/4 確認〕
※ 85 https://www.digital.go.jp/policies/security/comprehensive-operational-synthetic-monitoring-system〔2025/6/4 確認〕
※ 86 https://www.digital.go.jp/policies/security/crsa〔2025/6/4 確認〕
※ 87 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〔2025/7/1 確認〕
※ 88 経済産業省：第９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/009.

html〔2025/7/1 確認〕
※ 89 経済産業省：事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_semiconductor/pdf/002_06_00.pdf〔2025/7/1 確認〕
※ 90 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〔2025/7/1 確認〕
※ 91 NIST：The NIST Cybersecurity Framework (CSF) 2.0 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf〔2025/7/1 確認〕
※ 92 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/index.html〔2025/7/1 確認〕
※ 93 https://www.meti.go.jp/press/2025/04/20250414002/20250414002-2.pdf〔2025/7/1 確認〕
※ 94 経済産業省：第 18 回 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（制度・技術・標準化）電力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_denryoku/018.html〔2025/7/1 確認〕
※ 95 経済産業省：第 8 回 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（制度・技術・標準化）工場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_kojo/008.html〔2025/7/1 確認〕
※ 96 https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_ver1.0.pdf〔2025/7/1 確認〕
※ 97 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/20240823_1.pdf〔2025/7/1 確認〕
※ 98 経済産業省：サイバー攻撃への備えを!「SBOM」（ソフトウェア部品構成表）を活用してソフトウェアの脆弱性を管理する具体的手法についての改訂手引を策定しました　https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html〔2025/7/1 確認〕
※ 99 経済産業省：第 15 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　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/015.html〔2025/7/1 確認〕
※ 100 NIST：Secure Software Development Framework (SSDF) Version 1.1:　https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf〔2025/7/1 確認〕
※ 101 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/015_s01_00.pdf〔2025/7/1 確認〕
※ 102 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/cyber_infrastructure/pdf/202503_g2.pdf〔2025/7/1 確認〕
※ 103 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/enhanced_security/index.html〔2025/7/1 確認〕
※ 104 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/enhanced_security/pdf/20250305_2.pdf〔2025/7/1 確認〕
※ 105 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/cyber_human/index.html〔2025/7/1 確認〕
※ 106 経済産業省：技術情報管理認証制度（トップページ）　https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/〔2025/7/1 確認〕
※ 107 https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/pdf/08.pdf〔2025/7/1 確認〕
※ 108 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。
※ 109 https://www.ipa.go.jp/security/j-csip/about.html〔2025/6/4 確認〕
※ 110 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〔2025/6/4 確認〕
※ 111 IPA：J-CRAT 標的型サイバー攻撃特別相談窓口　https://www.ipa.go.jp/security/todokede/tokubetsu.html〔2025/6/4 確認〕
※ 112 https://www.meti.go.jp/policy/netsecurity/vul_notification.pdf〔2025/7/3 確認〕
※ 113 https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html〔2025/7/3 確認〕
※ 114 https://www.ipa.go.jp/security/guide/ps6vr70000011k4i-att/000059695.pdf〔2025/7/3 確認〕
※ 115 https://www8.cao.go.jp/cstp/aigensoku.pdf〔2025/7/1 確認〕
※ 116 https://www.ipa.go.jp/disc/committee/expert-group-on-aigfb.html〔2025/7/1 確認〕
※ 117 https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240419_1.pdf〔2025/7/1 確認〕
※ 118 https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20250328_1.pdf〔2025/7/1 確認〕
※ 119 経済産業省：不正競争防止小委員会　https://www.meti.go.jp/shingikai/sankoshin/chiteki_zaisan/fusei_kyoso/index.html〔2025/7/1 確認〕
※ 120 https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/r7ts.pdf〔2025/7/1 確認〕
※ 121 https://www.meti.go.jp/shingikai/sankoshin/chiteki_zaisan/fusei_kyoso/pdf/027_03_01.pdf〔2025/7/1 確認〕
※ 122 経済産業省：サイバー事案の対処及びサイバー脅威情報等の共有等に関する包括的な連携に関する協定書　https://www.meti.go.jp/press/2024/12/20241227001/20241227001-1.pdf〔2025/7/1 確認〕
※ 123 防衛省：サイバーセキュリティ分野における経済産業省との連携強化について（サイバー事案の対処及びサイバー脅威情報等の共有等に関する包括的な連携）　https://www.mod.go.jp/j/press/news/2024/12/27b_02.pdf〔2025/7/1 確認〕
※ 124 https://www.j-credit.or.jp/security/pdf/Creditcardsecurityguidelines_6.0_published.pdf〔2025/7/1 確認〕
※ 125 総務省：「ICT サイバーセキュリティ政策の中期重点方針」（案）に対する意見募集の結果及び「ICT サイバーセキュリティ政策の中期重点方針」の公表　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00219.html〔2025/6/4 確認〕
総務省：ICT サイバーセキュリティ政策の中期重点方針　https://www.soumu.go.jp/main_content/000960379.pdf〔2025/6/4 確認〕
※ 126 https://notice.go.jp〔2025/6/4 確認〕
※ 127 衆議院：国立研究開発法人情報通信研究機構法の一部を改正する等の法律　https://www.shugiin.go.jp/internet/itdb_housei.nsf/html/housei/21220231215087.htm〔2025/6/4 確認〕
※ 128 https://www.ipa.go.jp/publish/wp-security/2024.html〔2025/6/4 確認〕
※ 129 NOTICE：最近の観測状況　https://notice.go.jp/status〔2025/6/4 確認〕
※ 130 フロー情報：通信トラフィックデータのうち、IP アドレス、ポート番号等ヘッダー情報、ルーターでヘッダー情報を抽出する際に付与されるタイムスタンプ等の情報であり、通信の内容は含まれない。
ICT サイバーセキュリティ政策分科会：ICT サイバーセキュリティ政策の中期重点方針　https://www.soumu.go.jp/main_content/000960379.pdf〔2025/6/4 確認〕
※ 131 総務省：スマートフォン　プライバシー　https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/smartphone_privacy.html〔2025/6/4 確認〕
※ 132 https://www.soumu.go.jp/main_content/000942602.pdf〔2025/6/4 確認〕
※ 133 自然人：民法上、権利義務の主体となることができる人を指し、法人と自然人が含まれる。自然人は個人のこと。
図解六法：人・者・自然人・法人　https://www.zukairoppo.com/glossary-hito〔2025/6/4 確認〕
※ 134 https://www.soumu.go.jp/main_content/001000541.pdf〔2025/6/4 確認〕
※ 135 総務省：NICT サイバーセキュリティ研究所の取り組み　https://www.soumu.go.jp/main_content/000952545.pdf〔2025/6/4 確認〕
※ 136 GSOC（Government Security Operation Coordination team）：24 時間 365 日、政府横断的な情報収集、攻撃の分析、政府機関への助言等を行うため、NISC に設置された体制。
NISC：別添8 用語解説 GSOC（Government Security Operation Coordination team：ジーソック）　https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024-8.pdf〔2025/6/4 確認〕
※ 137 総務省：「スマートシティセキュリティガイドライン（第 3.0 版）」（案）に対する意見募集の結果及び「スマートシティガイドライン（第 3.0 版）」の公表　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00215.html〔2025/6/4 確認〕
※ 138 https://www.soumu.go.jp/main_content/000955126.pdf〔2025/6/4 確認〕
※ 139 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〔2025/6/4 確認〕
※ 140 警察庁：警察におけるサイバー戦略について（依命通達）　https://www.npa.go.jp/bureau/cyber/pdf/202204_senryaku.pdf〔2025/6/4 確認〕
※ 141 警察庁：サイバー重点施策について（通達）　https://www.npa.go.jp/bureau/cyber/pdf/202204_jyuten.pdf〔2025/6/4 確認〕

※ 142 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〔2025/6/4 確認〕
※ 143 国家公安委員会、警察庁：令和６年版 警察白書　https://www.npa.go.jp/hakusyo/r06/index.html〔2025/6/4 確認〕
※ 144 警察庁：サイバー特別捜査部とは　https://www.npa.go.jp/bureau/cyber/what-we-do/about_ncu.html〔2025/6/4 確認〕
※ 145 警察庁：不正アクセス行為対策等の実態調査 アクセス制御機能に関する技術の研究開発の状況等に関する調査 調査報告書　https://www.npa.go.jp/bureau/cyber/pdf/R6countermeasures.pdf〔2025/6/4 確認〕
※ 146 警察庁：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.npa.go.jp/news/release/2024/20240314.pdf〔2025/6/4 確認〕
※ 147 警察庁：フィッシング対策　https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html〔2025/6/4 確認〕
※ 148 https://www.jc3.or.jp/〔2025/6/4 確認〕
※ 149 https://www.internethotline.jp/〔2025/6/4 確認〕
※ 150 警察庁、NISC：MirrrorFace 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〔2025/6/4 確認〕
※ 151 警察庁：サイバーテロ対策協議会　https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/katsudo/cyber/index.html〔2025/6/4 確認〕
※ 152 警察庁：サイバーフォース　https://www.npa.go.jp/bureau/cyber/what-we-do/cyberforce.html〔2025/6/4 確認〕
※ 153 サイバー犯罪：警察庁による定義では「不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪、その他犯罪の実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪」を指す。
※ 154 警察庁：令和５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/R5/R05_cyber_jousei.pdf〔2025/6/4 確認〕
※ 155 サイバー事案：警察庁による定義では「サイバーセキュリティが害されることその他情報技術を用いた不正な行為により生ずる個人の生命、身体及び財産並びに公共の安全と秩序を害し、又は害するおそれのある事案」を指す。
※ 156 警察庁:特殊詐欺等の被害拡大防止を目的とした株式会社ゆうちょ銀行との「情報連携協定書」締結について　https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/jyouhourenkei250117.pdf〔2025/6/4 確認〕
※ 157 警察庁：令和６年における特殊詐欺及び SNS 型投資・ロマンス詐欺の認知・検挙状況について（暫定値版）　https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2024.pdf〔2025/6/4 確認〕
※ 158 ACSC：APT40 Advisory PRC MSS tradecraft in action　https://www.cyber.gov.au/sites/default/files/2024-07/apt40-advisory-prc-mss-tradecraft-in-action.pdf〔2025/6/4 確認〕
※ 159 警察庁：ナイジェリアとの国際共同捜査について　https://www.npa.go.jp/news/release/2025/release.pdf〔2025/6/4 確認〕
※ 160 NHK：インターポールと JICA ロマンス詐欺などの捜査力向上へ支援　https://www3.nhk.or.jp/news/html/20240728/k10014527031000.html〔2025/6/4 確認〕
※ 161 警察庁：DDoS 攻撃ウェブサービスに関する国際共同捜査について　https://www.npa.go.jp/news/release/2024/20241206001.html〔2025/6/4 確認〕
※ 162 警察庁：豪州主導国際文書「OT サイバーセキュリティの原則」への共同署名について　https://www.npa.go.jp/news/release/2024/caution20240913.html〔2025/6/4 確認〕
※ 163 読売新聞オンライン：生成AI悪用しウイルス作成、警視庁が25歳の男を容疑で逮捕…設計情報を回答させたか　https://www.yomiuri.co.jp/news/national/20240528-OYT1T50015/〔2025/6/4 確認〕
※ 164 読売新聞オンライン：大手銀行のネットバンキングに不正アクセス容疑、指示役の男逮捕…警察庁サイバー特捜部など　https://www.yomiuri.co.jp/national/20240709-OYT1T50166/〔2025/8/4 確認〕
朝日新聞：ネット不正送金の指示役逮捕　詐欺グループ全体、異例の摘発　警察庁　https://www.asahi.com/articles/ASS791S95S79UTIL01VM.html〔2025/6/4 確認〕
※ 165 日本経済新聞：災害時の SNS デマ、警察が厳格姿勢　安易な拡散は要注意　https://www.nikkei.com/article/DGXZQOUE242390U4A720C2000000/〔2025/6/4 確認〕
朝日新聞：能登半島地震で SNS にうその投稿の男性、罰金 20 万円　輪島簡裁　https://www.asahi.com/articles/ASSC11GTLSC1PJLB001M.html〔2025/6/4 確認〕
※ 166 ScanNetSecurity:警察庁、総務省それぞれの最新の取り組みは?官民連携、国際連携を通してより安全なサイバー空間の実現を ～JPAAWG 6th General Meeting レポート　https://scan.netsecurity.ne.jp/article/2024/04/02/50805.html〔2025/6/4 確認〕
※ 167 https://www.kantei.go.jp/jp/singi/hanzai/kettei/240618/honbun.pdf〔2025/6/4 確認〕
※ 168 https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study〔2025/6/4 確認〕
※ 169 ISC2, Inc.：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〔2025/6/4 確認〕
※ 170 https://juas.or.jp/cms/media/2025/04/JUAS_IT2025.pdf〔2025/6/6 確認〕
※ 171 レバテック株式会社：「セキュリティ」が転職求人倍率 1 位に、50 倍超えの高需要　https://levtech.jp/partner/guide/research/detail/303/〔2025/6/4 確認〕
※ 172 IPA：「DX 動向 2024」進む取組、求められる成果と変革　https://www.ipa.go.jp/digital/chousa/dx-trend/dx-trend-2024.html〔2025/6/4 確認〕
※ 173 IDC Japan 株式会社：国内市場におけるエッジコンピューティングへの投資は、2024 年に 1 兆 6 千億円と予測～国内エッジインフラ市場予測を発表～　https://my.idc.com/getdoc.jsp?containerId=prJPJ51979224〔2025/6/4 確認〕
※ 174 https://www.global-nikkei.com/cit/24/〔2025/6/4 確認〕
※ 175 日本経済新聞：サイバー防御の強化　防衛相「人材育成が基盤」　https://www.nikkei.com/article/DGKKZO85061580W4A121C2EP0000/〔2025/6/4 確認〕
※ 176 日本経済新聞:企業のサイバー対策、経産相「事業活動に不可欠」　https://www.nikkei.com/article/DGKKZO85085330X21C24A1EP0000/〔2025/6/4 確認〕
※ 177 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〔2025/6/4 確認〕
※ 178 パロアルトネットワークス株式会社：日本国内の中小企業のサイバーセキュリティに関する実態調査 2024 年版　https://www.paloaltonetworks.jp/content/dam/pan/ja_JP/PressRelease/2024-ecosystem-sme-press-release-supplement.pdf〔2025/6/4 確認〕
※ 179 経済産業省：第 1 回産業サイバーセキュリティ研究会ワーキンググループ 2（経営・人材・国際）サイバーセキュリティ人材の育成促進に向けた検討会事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/cyber_human/pdf/001_04_00.pdf〔2025/6/4 確認〕
※ 180 IPA：セキュリティ・キャンプ　https://www.ipa.go.jp/jinzai/security-camp/index.html〔2025/6/4 確認〕
※ 181 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これまでの議論の整理と継続的な検討事項　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/cyber_human/pdf/003_03_00.pdf〔2025/6/4 確認〕
※ 182 IPA：中小企業の情報セキュリティ対策ガイドライン第 3.1 版　https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf〔2025/6/4 確認〕
※ 183 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）最終取りまとめ　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/cyber_human/20250514_report.html〔2025/6/4 確認〕
※ 184 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における検討状況について　https://www.meti.go.jp/shingikai/mono_info_service/society_digital/digital_skill/pdf/005_02_00.pdf〔2025/6/4 確認〕
※ 185 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。
※ 186 このほかに、身体の不自由等により CBT 方式の受験ができない方を対象とした筆記試験を、春期 4 月 21 日及び秋期 10 月 13 日に実施した。
※ 187 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６年度試験 全試験区分版）　https://www.ipa.go.jp/shiken/reports/nq6ept000000i5c9-att/toukei_r06.pdf〔2025/6/4 確認〕
※ 188 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。
※ 189 IPA：国家資格「情報処理安全確保支援士」2025 年 4 月 1 日付新規登録者 1,173 名の内訳　https://www.ipa.go.jp/jinzai/riss/

reports/data/20250401newriss.html〔2025/6/4 確認〕
※ 190 IPA：講習の目的と概要 https://www.ipa.go.jp/jinzai/riss/forriss/koushu/overview.html〔2025/6/4 確認〕
※ 191 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〔2025/6/4 確認〕
※ 192 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〔2025/6/4 確認〕
※ 193 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〔2025/6/4 確認〕
※ 194 IPA：登録セキスペインタビュー https://www.ipa.go.jp/jinzai/riss/interview/riss.html〔2025/6/4 確認〕
※ 195 IPA：活用企業・組織のインタビュー https://www.ipa.go.jp/jinzai/riss/interview/soshiki/index.html〔2025/6/4 確認〕
※ 196 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〔2025/6/5 確認〕
※ 197 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〔2025/6/5 確認〕
※ 198 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〔2025/6/5 確認〕
※ 199 IPA：責任者向けプログラム サイバー危機対応机上演習（CyberCREST） https://www.ipa.go.jp/jinzai/ics/short-pgm/cybercrest/index.html〔2025/6/5 確認〕
※ 200 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〔2025/6/5 確認〕
※ 201 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/007_05_04.pdf〔2025/6/5 確認〕
※ 202 IPA：セキュリティ・キャンプ 2024 全国大会 https://www.ipa.go.jp/jinzai/security-camp/2024/camp/zenkoku/index.html〔2025/6/5 確認〕
※ 203 セキュリティ・キャンプ協議会：セキュリティ・キャンプ キャンプレポート https://www.security-camp.or.jp/camp/index.html〔2025/6/5 確認〕
※ 204 IPA：セキュリティ・キャンプ 2024 ネクスト https://www.ipa.go.jp/jinzai/security-camp/2024/camp/next/index.html〔2025/6/5 確認〕
※ 205 IPA：セキュリティ・キャンプ 2024 ジュニア https://www.ipa.go.jp/jinzai/security-camp/2024/camp/junior/index.html〔2025/6/5 確認〕
※ 206 セキュリティ・キャンプ協議会：地方大会 https://www.security-camp.or.jp/minicamp/〔2025/6/5 確認〕
※ 207 セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 東京 2024 https://www.security-camp.or.jp/minicamp/tokyo2024.html〔2025/6/5 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 宮城 2024 https://www.security-camp.or.jp/minicamp/miyagi2024.html〔2025/6/5 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 三重 2024 https://www.security-camp.or.jp/minicamp/mie2024.html〔2025/6/5 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 広島 2024 https://www.security-camp.or.jp/minicamp/hiroshima2024.html〔2025/6/5 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 愛知 2024 https://www.security-camp.or.jp/minicamp/aichi2024.html〔2025/6/5 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 山梨 2024 https://www.security-camp.or.jp/minicamp/yamanashi2024.html〔2025/6/5 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 沖縄 2024 https://www.security-camp.or.jp/minicamp/okinawa2024.html〔2025/6/5 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 岩手 2024 https://www.security-camp.or.jp/minicamp/iwate2024.html〔2025/6/5 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 北海道 2024 https://www.security-camp.or.jp/minicamp/hokkaido2024.html〔2025/6/5 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 熊本 2024 https://www.security-camp.or.jp/minicamp/kumamoto2024.html〔2025/6/5 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 石川 2024 https://www.security-camp.or.jp/minicamp/ishikawa2024.html〔2025/6/5 確認〕
セキュリティ・キャンプ協議会：セキュリティ・ミニキャンプ in 大阪 2025 https://www.security-camp.or.jp/minicamp/osaka2025.html〔2025/6/5 確認〕
※ 208 IPA：セキュリティ・キャンプフォーラム 2025 https://www.ipa.go.jp/jinzai/security-camp/2024/forum2025.html〔2025/6/5 確認〕
※ 209 セキュリティ・キャンプ協議会：GCC 2025 Taiwan - Global Cybersecurity Camp 2025 Taiwan https://www.security-camp.or.jp/event/gcc_taiwan2025.html〔2025/6/5 確認〕
※ 210 https://cynex.nict.go.jp/〔2025/6/5 確認〕
※ 211 NICT：社会実装・外部連携等に関する NICT の取組について https://www.soumu.go.jp/main_content/000987147.pdf〔2025/6/5 確認〕
※ 212 NICT：2024 年度 実践的サイバー防御演習「CYDER」の受講申込受付を開始 https://www.nict.go.jp/press/2024/05/14-1.html〔2025/6/5 確認〕
※ 213 NICT：プレ CYDER 後半が開講しました https://cyder.nict.go.jp/news/2024/post_11.html〔2025/6/5 確認〕
※ 214 NICT：ナショナルサイバートレーニングセンター https://nct.nict.go.jp/〔2025/6/5 確認〕
※ 215 総務省：2025 年日本国際博覧会に向けたサイバー防御講習「CIDLE（シードル）」の実施 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00175.html〔2025/6/5 確認〕
※ 216 NICT：SecHack365 の目的 https://sechack365.nict.go.jp/document/〔2025/6/5 確認〕
※ 217 NICT：集合イベントレポート https://sechack365.nict.go.jp/report/〔2025/6/5 確認〕
※ 218 NICT：SecHack365 2024 年度 成果発表会 https://sechack365.nict.go.jp/presentation/〔2025/6/5 確認〕
※ 219 SECCON：セキュリティコンテスト SECCON 実行委員会とは https://www.seccon.jp/13/seccon/executivecommittee.html〔2025/6/5 確認〕
※ 220 SECCON：SECCON と は https://www.seccon.jp/13/seccon/about.html〔2025/6/5 確認〕
※ 221 SECCON：本年度より、SECCON の呼称を西暦から連番といたします。 https://www.seccon.jp/13/seccon.html
※ 222 SECCON：SECCON 13 開催スケジュール https://www.seccon.jp/13/seccon/schedule.html〔2025/6/5 確認〕
※ 223 SECCON：SECCON 13 電脳会議 https://www.seccon.jp/13/ep250301.html〔2025/6/5 確認〕
※ 224 SECCON：SECCON CTF 13 予選のお知らせ https://www.seccon.jp/13/seccon_ctf/quals.html〔2025/6/5 確認〕
※ 225 SECCON：SECCON Beginners とは https://www.seccon.jp/13/beginners/about-seccon-beginners.html〔2025/6/5 確認〕
※ 226 SECCON：CTF for GIRLS とは https://www.seccon.jp/13/girls/ctf-for-girls.html〔2025/6/5 確認〕
※ 227 SECCON：SECCONCON とは https://www.seccon.jp/13/seccon/secconcon.html〔2025/6/5 確認〕
※ 228 JNSA：JNSA 産学情報セキュリティ人材育成検討会とは？ https://www.jnsa.org/internship/jinzai.html〔2025/6/5 確認〕
※ 229 JNSA：交流会に参加しよう！ー「産学情報セキュリティ人材育成交流会」 https://www.jnsa.org/internship/event.html〔2025/6/5 確認〕
※ 230 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〔2025/6/6 確認〕
※ 231 総務省：令和 6 年版 情報通信白書｜データ集 第Ⅱ部第 1 章第 5 節 41. 世界の IoT デバイス数の推移及び予測 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/html/datashu.html#f00246〔2025/6/6 確認〕
※ 232 NICT：NICTER 観測レポート 2024 の公開 https://www.nict.go.jp/press/2025/02/13-1.html〔2025/6/6 確認〕
※ 233 CNET：That massive internet outage, explained https://www.cnet.com/tech/computing/what-is-a-ddos-attack/〔2025/6/6 確認〕
※ 234 https://www.ipa.go.jp/security/10threats/10threats2025.html〔2025/6/6 確認〕
※ 235 https://notice.go.jp/〔2025/6/6 確認〕
※ 236 サプライチェーン・リスク：「サイバー空間を構成するシステムのサプライチェーンの複雑化やグローバル化を通じ、サプライチェーンの過程で製品に不正機能等が埋め込まれるリスクや政治経済情勢による機器・サービスの供給途絶など、サイバー空間自体の信頼性や供給安定性に係るリ

スク」とされる。
NISC：サイバーセキュリティ戦略（令和３年９月28日閣議決定） https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf〔2025/6/6 確認〕
※ 237 経済産業省：ワーキンググループ３（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） https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html〔2025/6/6 確認〕
※ 238 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240823.html〔2025/6/6 確認〕
※ 239 IPA：申請手続き・報告手続き https://www.ipa.go.jp/security/jc-star/shinsei/index.html〔2025/7/11 確認〕
※ 240 https://www.ipa.go.jp/security/jc-star/list/jc-star-product-list/index.html〔2025/7/11 確認〕
※ 241 https://www.meti.go.jp/policy/netsecurity/chusyosecurityguide_r6.pdf〔2025/6/6 確認〕
※ 242 https://www.ipa.go.jp/security/jc-star/detail.html〔2025/6/6 確認〕
※ 243 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〔2025/6/6 確認〕
※ 244 米国国立標準技術研究所（NIST：National Institute of Standards and Technology）：NIST IR 8425 Profile of the IoT Core Baseline for Consumer IoT Products https://csrc.nist.gov/pubs/ir/8425/final〔2025/6/6 確認〕
※ 245 European Commission:Cyber Resilience Act https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act〔2025/6/6 確認〕
※ 246 https://www.ipa.go.jp/security/jc-star/begoj9000000gg60-att/JC-STARsetumeikai_1.pdf〔2025/6/6 確認〕
※ 247 https://www.soumu.go.jp/main_content/001000932.pdf〔2025/6/6 確認〕
※ 248 https://www.enecho.meti.go.jp/category/saving_and_new/advanced_systems/vpp_dr/20250522.pdf〔2025/6/6 確認〕
※ 249 https://www.nisc.go.jp/pdf/policy/infra/rmtebiki202307.pdf〔2025/6/6 確認〕
※ 250 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/〔2025/6/6 確認〕
※ 251 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〔2025/6/6 確認〕
※ 252 FCC：U.S. Cyber Trust Mark https://www.fcc.gov/CyberTrustMark〔2025/6/6 確認〕
※ 253 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/20241106_2.pdf〔2025/6/6 確認〕
※ 254 JBMIA：BMSec は、JC-STAR と制度統合します https://bmsec.jbmia.or.jp/news/details.php?id=76〔2025/6/6 確認〕
※ 255 https://www.ipa.go.jp/security/jisec/index.html〔2025/6/6 確認〕
※ 256 https://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf〔2025/6/6 確認〕
※ 257 IPA：国際承認アレンジメント（CCRA）概要 https://www.ipa.go.jp/security/jisec/about/ccra.html〔2025/6/6 確認〕
※ 258 https://www.commoncriteriaportal.org〔2025/6/6 確認〕
※ 259 IPA：評価・認証プロテクションプロファイルリスト https://www.ipa.go.jp/security/jisec/pps/certified-pps/〔2025/6/6 確認〕
※ 260 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構築に向けた中間取りまとめ https://www.meti.go.jp/press/2025/04/20250414002/20250414002-2.pdf〔2025/6/6 確認〕
※ 261 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構築に向けた中間取りまとめ」を公表しました https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html〔2025/6/6 確認〕
NISC：「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構築に向けた中間取りまとめ」を公表しました https://www.nisc.go.jp/pdf/council/wg_supply_chain/20250414_press.pdf〔2025/6/6 確認〕
※ 262 IPA：情報セキュリティ 10 大脅威 2025 組織編 ２位「サプライチェーンや委託先を狙った攻撃」 https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/kaisetsu_2025_soshiki.pdf〔2025/6/6 確認〕
※ 263 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〔2025/6/6 確認〕
※ 264 英国の「Cyber Essentials」、米国の「Cybersecurity Maturity Model Certification 2.0 Program（CMMC 2.0）」、フランスのサイバースコア法、オーストラリアの「Essential Eight」等。
NCSC：Cyber Essentials https://www.ncsc.gov.uk/cyberessentials/overview〔2025/6/6 確認〕
CISA：Cybersecurity Maturity Model Certification 2.0 Program https://www.cisa.gov/resources-tools/resources/cybersecurity-maturity-model-certification-20-program〔2025/6/6 確認〕
legifrance.gouv.fr：LOI n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public (1) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045294275〔2025/6/6 確認〕
ACSC：Essential Eight https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight〔2025/6/6 確認〕
※ 265 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構築に向けた中間取りまとめ（概要） https://www.meti.go.jp/press/2025/04/20250414002/20250414002-1.pdf〔2025/6/6 確認〕
一般財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〔2025/6/6 確認〕
一般財団法人日本情報経済社会推進協会：情報マネジメントシステム関連文書 ISMS 認証に関するガイド類 https://www.jipdec.or.jp/library/smpo_doc.html#11〔2025/6/6 確認〕
※ 266 IPA：SECURITY ACTION セキュリティ対策自己宣言 https://www.ipa.go.jp/security/security-action/〔2025/6/6 確認〕
※ 267 内閣官房、総務省、経済産業省：「政府情報システムのためのセキュリティ評価制度 (ISMAP)」の運用開始 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00071.html〔2025/6/6 確認〕
※ 268 https://cio.go.jp/sites/default/files/uploads/documents/cloud_policy_20210330.pdf〔2025/6/6 確認〕
※ 269 総務省、経済産業省：クラウドサービスの安全性評価に関する検討会について https://www.meti.go.jp/shingikai/mono_info_service/cloud_services/pdf/001_02_00.pdf〔2025/6/6 確認〕
※ 270 機密性２情報：行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより、国民の権利が侵害されまたは行政事務の遂行に支障を及ぼすおそれがある情報を指す。
※ 271 NISC、デジタル庁、総務省、経済産業省：ISMAP 制度改善の取組み https://www.ismap.go.jp/sys_attachment.do?sys_id=be1ce75c4713b5103f0f6befe16d4355〔2025/6/6 確認〕
※ 272 ISMAP：ISMAP 管理基準の解釈や具体的な実装例を示したガイドはありますか。 https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010068〔2025/6/6 確認〕
※ 273 NISC、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=87b793a583e86a10aa68c6a8beaad3af〔2025/6/6 確認〕
※ 274 https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005〔2025/6/6 確認〕
※ 275 https://www.ismap.go.jp〔2025/6/6 確認〕
※ 276 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〔2025/6/6 確認〕
※ 277 IPA：海外のクラウドサービスのセキュリティ評価制度に関する調査 https://www.ipa.go.jp/security/reports/cloud_oversea.html〔2025/6/6 確認〕
※ 278 https://www.ismap.go.jp/sys_attachment.do?sys_id=570a04b62b606e10f0bbfd69fe91bf74〔2025/6/6 確認〕
※ 279 ISMAP：「ISMAP クラウドサービス登録規則」第９章において求められる、情報セキュリティインシデント報告を行う際の具体的な方法や基準、項目などを教えてください。 https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010898&sys_kb_id=42b3851f83889210d54cba98beaad33e&spa=1〔2025/6/6 確認〕
※ 280 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-0001-2022r1.pdf〔2025/6/4 確認〕
※ 281 CRYPTREC：CRYPTREC の体制 https://www.cryptrec.go.jp/system.html〔2025/6/4 確認〕
※ 282 https://www.cryptrec.go.jp/report/cryptrec-gl-2007-2024.pdf〔2025/6/4 確認〕

※ 283 https://www.cryptrec.go.jp/report/cryptrec-gl-3005-1.0.pdf〔2025/6/4 確認〕
※ 284 NICT、IPA：CRYPTREC Report 2024 https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2024.pdf〔2025/7/31 確認〕
※ 285 https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2024.pdf〔2025/6/4 確認〕
※ 286 NIST：Module-Lattice-Based Key-Encapsulation Mechanism Standard https://csrc.nist.gov/pubs/fips/203/final〔2025/6/4 確認〕
※ 287 NIST：Module-Lattice-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/204/final〔2025/6/4 確認〕
※ 288 NIST：Stateless Hash-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/205/final〔2025/6/4 確認〕
※ 289 NIST：Post-Quantum Cryptography https://csrc.nist.gov/projects/post-quantum-cryptography〔2025/6/4 確認〕
※ 290 CRYPTREC：量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価 2024 年度版 https://www.cryptrec.go.jp/exreport/cryptrec-ex-3401-2024.pdf〔2025/6/4 確認〕
※ 291 https://www.cryptrec.go.jp/report/cryptrec-gl-3004-1.1.pdf〔2025/6/4 確認〕
※ 292 https://www.cryptrec.go.jp/report/cryptrec-gl-3002-1.0.pdf〔2025/6/4 確認〕
※ 293 https://www.cryptrec.go.jp/events/cryptrec_symposium2024_presentation.html〔2025/6/4 確認〕
※ 294 https://www.nri-secure.co.jp/download/insight2024-report〔2025/6/6 確認〕
※ 295 https://sc3.jp/〔2025/7/31 確認〕
※ 296 https://cric.jp/guide/〔2025/6/6 確認〕
※ 297 https://sc3.jp/〔2025/6/6 確認〕
※ 298 https://www.ipa.go.jp/security/sme/otasuketai-about.html〔2025/6/6 確認〕
※ 299 https://www.ipa.go.jp/security/sme/ps6vr7000001hnrl-att/otasuketai-leaflet.pdf〔2025/6/6 確認〕
※ 300 https://www.ipa.go.jp/security/sme/otasuketai/nq6ept000000faii-att/000092713.pdf〔2025/6/6 確認〕
※ 301 https://www.ipa.go.jp/security/otasuketai-pr/〔2025/6/6 確認〕
※ 302 https://www.ipa.go.jp/security/security-action/index.html〔2025/6/6 確認〕
※ 303 https://www.ipa.go.jp/security/guide/sme/5minutes.html〔2025/6/6 確認〕
※ 304 IPA：セキュリティインシデント対応机上演習教材 https://www.ipa.go.jp/security/sec-tools/ttx.html〔2025/6/6 確認〕
※ 305 IPA：制御システムのセキュリティリスク分析ガイド 第 2 版 https://www.ipa.go.jp/security/controlsystem/riskanalysis.html〔2025/7/4 確認〕
※ 306 IPA：制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ https://www.ipa.go.jp/security/controlsystem/incident.html〔2025/7/4 確認〕
※ 307 https://www.ipa.go.jp/security/controlsystem/ug65p900000019bkg-att/begoj9000000hpvw.pdf〔2025/7/4 確認〕
※ 308 https://www.ipa.go.jp/security/controlsystem/ug65p900000019bkg-att/begoj9000000hqxn.pdf〔2025/7/4 確認〕
※ 309 https://www.ipa.go.jp/security/controlsystem/controlsystem-smartplant.html〔2025/7/4 確認〕
※ 310 IPA：制御システムのセキュリティリスク分析ガイドセミナー https://www.ipa.go.jp/security/seminar/controlsystem/controlsystem.html〔2025/7/4 確認〕
※ 311 東スポ WEB:ミャンマー地震がフェイク画像で混乱 IT事情通は「再生回数稼ぎや募金詐欺」と指摘 https://www.tokyo-sports.co.jp/articles/-/339475〔2025/6/6 確認〕
※ 312 https://www.soumu.go.jp/use_the_internet_wisely/special/generativeai/〔2025/6/6 確認〕
※ 313 KRY 山口放送：「元本が多いほど得られる利益も多くなる」下関市の 60 代女性が SNS 型投資詐欺で 2200 万円被害 https://news.ntv.co.jp/n/kry/category/society/krb301e87a451b4b33a12831f008dd6e0c〔2025/6/6 確認〕
※ 314 https://www.npa.go.jp/bureau/safetylife/sos47/〔2025/6/6 確認〕
※ 315 警察庁：SNS 型投資詐欺 https://www.npa.go.jp/bureau/safetylife/sos47/case/sns-romance/investment/〔2025/4/9 確認〕
※ 316 金融庁：「詐欺的な投資に関する相談ダイヤル」の開設について https://www.fsa.go.jp/news/r5/sonota/20240619/toshisagi.html〔2025/6/6 確認〕
※ 317 KRY 山口放送：「私と会うためには会員カード作って」…50 代男性が 125 万円の SNS 型ロマンス詐欺被害・宇部 https://news.ntv.co.jp/n/kry/category/society/krf35d63b34e704c4bad718274a53b1efc〔2025/6/6 確認〕
※ 318 警察庁：SNS 型ロマンス詐欺 https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/sns-romance/romance/〔2025/6/6 確認〕
※ 319 岩手日日新聞社：被害防止へ連携 SNS型投資・ロマンス詐欺 岩手県警 NTT、セコムと協定 https://www.iwanichi.co.jp/2024/12/07/13985771/〔2025/6/6 確認〕
※ 320 インターネット掲示板や SNS 等で、仕事内容を明示せず高額な報酬を提示して犯罪の実行者を募集するもの。
※ 321 テレ朝 news：“闇バイト”コア 19 事件で 47 人逮捕 「トクリュウ対策元年」になった一連の強盗事件を振り返る https://news.tv-asahi.co.jp/news_society/articles/900015077.html〔2025/6/6 確認〕
※ 322 埼玉新聞：母娘が恐怖…寝ていると男 3 人が襲いかかる 深夜に自宅で テープで縛り暴行した 26 歳、カードなど強奪し逮捕 母娘は自力でテープはがす カードで現金を下ろそうとした大学生も逮捕、番号が一致せず諦めた 21 歳 https://www.saitama-np.co.jp/index.php/articles/101710/postDetail〔2025/6/6 確認〕
※ 323 朝日新聞：「闇バイト」実行役 2 人を強盗殺人容疑で再逮捕 横浜市青葉区の事件 https://www.asahi.com/articles/AST2B0GWPT2BOXIE003M.html〔2025/6/6 確認〕
※ 324 https://www.youtube.com/@mextchannel〔2025/6/6 確認〕
※ 325 https://www.youtube.com/watch?v=SkdwK9PdKfI〔2025/6/6 確認〕
※ 326 警視庁：＃BAN 闇バイト https://www.keishicho.metro.tokyo.lg.jp/kurashi/drug/yami_arbeit/ban_yamiarbeit.html〔2025/6/6 確認〕
※ 327 LINE ヤフー：LINE ヤフー、闇バイト対策として新たな取り組みを開始／闇バイトへの加担リスクを学べる中学生・高校生向け 情報モラル教材を静岡大学と共同開発／さらに「LINE」を悪用した闇バイト・詐欺行為の撲滅を目指し、啓発活動を実施 https://www.lycorp.co.jp/ja/news/release/017128/〔2025/6/6 確認〕
※ 328 福井新聞：競歩柳井、中傷被害を訴え 個人種目の辞退発表後 https://www.fukuishimbun.co.jp/articles/-/2096071〔2025/6/6 確認〕
※ 329 TEAM JAPAN：第 33 回オリンピック競技大会（2024/ パリ）TEAM JAPAN からのメッセージの掲出について https://www.joc.or.jp/news/20240801035399.html〔2025/6/6 確認〕
※ 330 株式会社セント・フォース：所属タレントに対する誹謗中傷等への対応につきまして https://www.centforce.com/topics/page/12〔2025/6/23 確認〕
※ 331 https://no-heart-no-sns.smaj.or.jp/〔2025/6/6 確認〕
※ 332 https://www.youtube.com/@MOJchannel〔2025/6/6 確認〕
※ 333 https://www.youtube.com/watch?v=onA58-GRKQQ〔2025/6/6 確認〕
※ 334 法務省：人権啓発動画「インターネットはヒトを傷つけるモノじゃない。」公開中! https://www.moj.go.jp/JINKEN/jinken04_00257.html〔2025/6/6 確認〕
※ 335 NISC：NISC サイバーセキュリティ月間 2025 https://security-portal.nisc.go.jp/cybersecuritymonth/2025/〔2025/6/6 確認〕
※ 336 NISC：インターネットの安全・安心ハンドブック https://security-portal.nisc.go.jp/guidance/handbook.html〔2025/6/6 確認〕
※ 337 内閣府大臣官房政府広報室：スマートフォンのセキュリティ対策できていますか? 4 つのポイント【字幕付】 https://www.gov-online.go.jp/prg/prg26093.html〔2025/6/6 確認〕
※ 338 総務省：つくろう!守ろう!安心できる情報社会 https://www.soumu.go.jp/dpa/#initiative〔2025/6/6 確認〕
※ 339 https://www.soumu.go.jp/use_the_internet_wisely/〔2025/6/6 確認〕
※ 340 https://www.soumu.go.jp/use_the_internet_wisely/special/lctliteracy_for_yps/〔2025/6/6 確認〕

第4章
国際的な政策及び取り組みの動向

2024 年は欧米各国で国政選挙が行われたが、そこでは分断や混乱を狙った様々なサイバー攻撃や影響力工作が見られた。国際連携により国境を越えた脅威に対抗する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。

また、2024 年のセキュリティ分野での国際標準化の動きとして ISO/IEC JTC 1/SC 27 と IEC TC 65/WG 10 の活動を紹介する。

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、IT 化した社会サービスやそれを支える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虚偽情報流布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･各地域におけるサイバー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

国際社会の概況、国際的な脅威に対する対応、及び我が国と各国の首脳・外相等の連携協議を中心に取り組みを述べる。なお、国際間の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・連携状況も含める。

(1) 国際社会の概況

2024 年も国際情勢に影響を及ぼし得る出来事が多くあった。国際社会における環境変化及びその環境変化に基づくサイバー空間への影響に関する概況を以下に示す。

(a) 国際社会全般について

これまで経済のグローバル化と相互依存が進み、国際社会に一定の安定と経済成長がもたらされてきた一方で、様々な環境変化が生じている。

2022 年 2 月にロシアがウクライナに侵攻して以来 3 年以上経過するが、解決には至っていない。また、2023 年 10 月にイスラエル・パレスチナをめぐる情勢が悪化し、双方の攻撃により多数の死者・被害が生じた。停戦をめぐり協議が行われる場面もあったが、双方の合意に向けた交渉は難航している。

また 2024 年には世界各地で重要な選挙が実施された。具体的には、台湾総統選挙（1 月）、インドネシア大統領選挙（2 月）、ロシア大統領選挙（3 月）、メキシコ大統領選挙（6 月）、米国大統領選挙（11 月）といった各国首脳の選挙が実施された。また、韓国では総選挙（4 月）が、英国において下院総選挙（7 月）が、そして日本においても衆議院選挙（10 月）が行われた。G20 のうち 11 の国や地域で国政レベルの選挙が実施され、その後の政策決定及び国際情勢に影響を与え得る状況となっている。

更に 7 月から 9 月にかけ、パリ 2024 オリンピック・パラリンピック競技大会（以下、パリ大会）が開催される等、2024 年は多くの出来事があった年となった。

(b) サイバー空間における国際情勢

選挙やオリンピックといった国際的に見て大きな出来事が多くあったが、これらの出来事に関連し、サイバー空間でも様々な影響があった。

例えば米国大統領選挙について見ると、複数の国から影響工作が行われたとの報告がされている※1。また、同選挙に関連する偽情報が急増したものの、選挙結果に直接影響を及ぼすような活動の証拠は見られなかった、との報道があった※2。

パリ大会について見ると、オリンピック開催前の段階か

ら偽の Web サイトを用いて偽造チケットを販売する詐欺※3 や投資詐欺等が確認※4 されている。フランス当局からは、オリンピック開催期間中に 140 件以上のサイバー攻撃を受けたものの、競技に支障をきたすような攻撃はなかった、との発表がされている※5。

このように、実社会での出来事はサイバー空間にも影響を与え、両者は切り離せない関係にある。特に、近年急速に進化している生成 AI の利用が進み、フィッシング攻撃の準備段階等においてもその活用が進んでいる状況となっている※6。

生成 AI では、OpenAI, Inc. の GPT-4o や Google LLC の Gemini 等が登場し、テキストのみならず、画像、音声や動画といった様々な形式のデータを組み合わせた処理ができるマルチモーダル AI の進化が見られた。

2025 年 1 月、中国の DeepSeek（杭州深度求索人工智能基础技术研究有限公司）が低コストであるものの高性能な生成 AI モデルを発表すると、同社の iPhone 向けアプリが無料アプリランキングで ChatGPT を抑えて 1 位となったことのみならず、米国の株式市場におけるハイテク株の下落等、社会に様々な影響を及ぼした※7。

同社の生成 AI について、同年 1 月にはイタリアの個人情報保護保証機関がイタリアのユーザーのデータを保護すべく、そのデータ処理を制限するよう命令を行った※8。また 2 月に韓国の個人情報保護委員会において、韓国でのサービス提供を一時停止する決定※9 がなされる等、複数の国や地域において、同社のサービスに関して様々な対応が行われている。

(2) 国際的な脅威に対する対応

前述のとおり、国際社会及びサイバー空間において様々な環境変化が進む中、新たな脅威が生じている。ここでは、脅威に対して国際的に実施されている取り組みについて紹介する。

(a) 国家安全保障上のリスクに伴う規制強化

2024 年 4 月、米国において「外国敵対勢力が管理するアプリから米国人を保護する法」が成立した※10。これは、「合衆国法典」の第 10 編第 4872 条(d)(2)で指定される国に本社や主な事業所を有する企業が運営するアプリ等を対象とし、条文において具体的に TikTok Inc. と親会社の ByteDance Ltd.（以下、バイトダンス社）が明示された。これに対し、バイトダンス社は 5 月に当該法律の合憲性審査を求め米国政府を提訴した※11。2025 年 1 月米国連邦最高裁判所は、当該法律を支持する判断を示した※12。また 2024 年 11 月にカナダ政府は、「投資カナダ法※13」に基づき TikTok Technology Canada, Inc. が営むカナダ事業の清算を命じた※14。

2024 年 6 月、国家安全保障上のリスクから、米国政府はロシアの Kaspersky Lab, Inc.（以下、カスペルスキー社）の米国子会社へセキュリティソフト等の米国での販売を 7 月以降禁止する決定を行った※15。またデンマーク政府は 2024 年 6 月、カスペルスキー社が開発したセキュリティソフトを使用しないよう公的機関及び民間企業に要請を行った※16。更に 2025 年 2 月には、オーストラリア政府が政府機関に対して政府のすべてのシステムやデバイスに対するカスペルスキー社製の製品・サービスのインストールの防止・削除を義務付ける指令を発行した※17。

(b) 脅威への国際連携による対応

2024 年 10 月、ランサムウェア攻撃グループ「LockBit」のマルウェア開発者らが欧州刑事警察機構（Europol：European Union Agency for Law Enforcement Cooperation）等による共同捜査で逮捕された。LockBit は 2021 年の徳島県つるぎ町立半田病院の診療一時停止※18 や 2023 年の名古屋港コンテナターミナルの稼働停止※19 の原因となった攻撃への関与が疑われており、世界で数十億ポンドの被害があったとされている※20。LockBit に対して行われた一連の共同捜査は Operation Cronos と呼ばれ、当該作戦には日本警察庁を含む 10 ヵ国の司法機関が参加し、4 ヵ国が支援を行った※21。

また米国、英国、ドイツの司法機関が連携して捜査・摘発を行い、欧米を拠点として活動を行っていたランサムウェア攻撃グループ「Radar/Dispossessor」を解体させたと 2024 年 8 月に公表した※22。

(c) 国連サイバー犯罪条約の採択

2024 年 12 月、サイバー犯罪に関する包括的な国際条約である「国連サイバー犯罪条約」が国連総会により採択された。この条約は、国際協力の強化、開発途上国に対する技術支援と能力構築の促進等を通じてサイバー犯罪を防止しそれに対抗することを目的としており、前文と九つの章から構成されている。人権保障を含めつつ、サイバー犯罪という世界的な問題を防止し対処するための包括的なアプローチを示し、犯罪捜査における従来の手段と手法を ICT 環境に適合させ、国際協力を強化することにより技術的・法的課題を解決するものである※23。

この条約は2025年10月にベトナムのハノイで開催される式典において署名され、2026年12月31日までに国連本部で署名が行われる。そして、発効要件である40ヵ国が締約国になった後に発効する※24。

(3) 我が国における国際連携・協力

我が国では、2024年も新たな国際連携・協力を開始しながら、これまで取り組んできた国際連携・協力についても継続的に進めてきている。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への参画

我が国はこれまでも様々な国際連携を進めているが、更なる連携強化を行うべく2024年において新たな取り組みを実施した。それらの取り組みについて以下に示す。

(ア) 人権保護や民主主義の推進に関与する組織や個人のためのサイバー脅威緩和に関する国際ガイダンスへの共同署名

2024年5月、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)(現、国家サイバー統括室(NCO: National Cybersecurity Office))と警察庁は、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)が作成した国際ガイダンス「Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society※25」の共同署名に加わり、文書を公表した。これは、人権保護や民主主義の推進に関与する組織や個人が、国家を背景としたグループによる民主主義の価値を損なわせるためのサイバー攻撃の被害に遭う危険が高いとした上で、取るべきリスク緩和策を列挙したものである。同ガイダンスに共同署名し、協力機関として組織名を列記した国は、日本、米国を含む6ヵ国であった※26。

(イ) オーストラリア主導の「APT40グループに関する国際アドバイザリー」への共同署名

2024年7月、NISCと警察庁は、オーストラリア通信情報局(ASD: Australian Signals Directorate)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)が作成した国際アドバイザリー「APT40 Advisory PRC MSS tradecraft in action※27」の共同署名に加わり、このアドバイザリーを公表した。これはサイバー攻撃グループAPT40による過去の攻撃事例をケーススタディとして攻撃手法を詳述した上で、攻撃の検知や緩和策を示しているものである。同アドバイザリーに共同署名し、協力機関として組織名を列記した国は、日本、オーストラリアを含む8ヵ国であった※28。

(ウ) 英国主導の「サイバーセキュリティ人材に関する国際的な連合」への参画

2025年1月、NISCは、英国科学・イノベーション・技術省が策定した文書「サイバーセキュリティ人材に関する国際的な連合」に署名し、同連合に参画することとした。この連合に参画する協力機関として組織名を列記したのは、英国、日本を含む6ヵ国であった。この連合は、各国で取り組まれてきたサイバーセキュリティ人材に関する枠組みや基準に関し、相互参照性を高めることを目的としており、サイバーセキュリティ人材が我が国を含めグローバルに活躍できる環境の整備に資するものとなる※29。

(b) 各国との連携強化

これまで行ってきた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、連携を強化している。また新たな連携強化も実施している。以下にそれらの取り組みの状況を示す。

(ア) 日米サイバー対話(第9回)

2024年6月、米国ワシントンD.C.において、第9回日米サイバー対話が開催された。この対話では、日米両国におけるサイバー政策、二国間協力及び国際場裡における能力構築支援を含む協力等、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、熊谷直樹外務省総合外交政策局審議官兼サイバー政策担当大使(以下、熊谷審議官)、外務省、NISC、公安調査庁、総務省、経済産業省、防衛省を含む関係者が、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、国務省、国防省を含む関係者がそれぞれ出席した※30。

(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3回)

2024年9月、韓国ソウルにおいて、第3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が実施された。この作業部会において、日本、米国、韓国の3ヵ国は、北朝鮮の不法な大量破壊兵器及び弾道ミサイル計画の資金源となる、北朝鮮の不正なサイバー活動に対する懸念を改めて表明した。その上で、北朝鮮によ

る暗号資産窃取や北朝鮮 IT 労働者を含む北朝鮮のサイバー脅威に対する各国の取り組みや今後の日米韓協力等について意見交換を行った。この作業部会は、熊谷審議官、Seth Bailey 米国国務省北朝鮮担当次席特別代表、李埈一韓国外交部朝鮮半島政策局長が共同議長を務めた※31。

(ウ)日英サイバー対話(第 8 回)

2024 年 9 月、英国ロンドンにおいて、第 8 回日英サイバー対話が開催された。この対話では、サイバー分野に関し、日英両国のサイバーセキュリティ戦略や政策、国連を含む国際場裡における協力、能力構築支援等の幅広い論点について意見交換が行われた。熊谷審議官と William Middleton 外務・英連邦・開発省サイバー政策部長が共同議長を務め、日本側から外務省、NISC、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、外務・英連邦・開発省、内閣府、ビジネス・通商省、科学・イノベーション・技術省、内務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※32。

(エ)日 ASEAN サイバーセキュリティ政策会議(第 17 回)

2024 年 10 月、シンガポールにおいて、第 17 回日 ASEAN サイバーセキュリティ政策会議が開催された。この政策会議は、サイバーセキュリティ分野における我が国と ASEAN 諸国との国際的な連携・取り組みを強化することを目的としており、この 1 年間の各国のサイバーセキュリティ政策について意見交換し、より高度で洗練化された攻撃の脅威に直面している現状等を共有した。また、サイバー演習や重要インフラ防護ワークショップ等の協力活動を確認し、今後の更なる協力活動の在り方についても議論が行われた。NISC、総務省、経済産業省が主催し、髙見澤將林東京大学公共政策大学院客員教授とプア・プエイ・リー シンガポールサイバーセキュリティ庁長官補(政策・企業開発)が議長となり、日本側から内閣官房・総務省・外務省・経済産業省の関係者が、ASEAN 側から ASEAN 加盟国のサイバーセキュリティ関係省庁及び情報通信関係省庁、ASEAN 事務局の関係者がそれぞれ参加した※33。

(オ)日・EU サイバー対話(第 6 回)

2024 年 11 月、東京において、第 6 回日・EU サイバー対話が開催された。この対話では、日本と欧州連合(EU:European Union)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が行われた。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と、Maciej STADEJEK 欧州対外活動庁平和・安全保障・防衛総局次長が共同議長を務め、日本側から外務省、内閣官房、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、欧州対外活動庁、欧州委員会及び駐日欧州連合代表部の関係者がそれぞれ参加した※34。

(カ)日リトアニアサイバー協議(第 1 回)

2024 年 9 月、リトアニアのヴィリニュスにおいて、第 1 回日リトアニアサイバー協議が開催された。この協議では、日本、リトアニア両国のサイバーセキュリティ戦略や政策、二国間及び多国間での協力等の幅広い論点について意見交換が行われ、両国は、サイバー協議等も活用し、サイバー分野で引き続き緊密に連携していくことを確認した。この協議は熊谷審議官と Inga SŪNELAITIENĖ 国防省サイバーセキュリティ・IT 政策部長が共同議長を務め、日本側から外務省、NISC 及び防衛省の関係者が、リトアニア側から、国防省、外務省及び国家サイバーセキュリティセンターの関係者がそれぞれ出席した※35。

(キ)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

2024 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のほか、国の OT・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。2024 年は、企業のサプライチェーンレジリエンス強化をテーマとして、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、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、ネットワーク脅威の解析やインシデント対応等のワークショップを日米合同で実施した。また、テーマ別セミナーでは、ICSCoEが実施する中核人材育成プログラムの修了者が米国の専門家とともにパネルディスカッションに登壇して知見を共有した。

(ク)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

2024年11月、ICSCoEと日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）は、オランダ国家サイバーセキュリティセンター（NCSC：National Cyber Security Centre）と協働し、タイのバンコクでOT（Operational Technology：制御技術）セキュリティを含む重要情報インフラ保護に関する人材育成プログラムを提供した。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。5日間の研修プログラムでは、オランダNCSCからOTセキュリティの意義についての講義、重要インフラ及びサイバーセキュリティに関する基礎的な理論や認識を深める講義が提供された。その後、ICSCoEからサプライチェーンリスクマネジメントを主題とした講義及びワークショップを提供し、受講者へ実践的なスキル向上の機会を提供した。

(ケ)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

2024年7月、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締結した[※37]。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（全24回中、2024年度中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。

(コ)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

AJCCBCにおいて、国際協力機構（JICA：Japan International Cooperation Agency）は、ASEAN事務局との技術協力協定に基づく技術協力プロジェクトとして「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」を2023年3月から4年間の予定で実施している[※38]。このプロジェクトはタイのNCSA（National Cyber Security Agency）とJICAによって運営されている。主な活動は、次のとおりである[※39]。

- ハンズオンのトレーニングとセミナー
- CTF（Capture the Flag）競技のような能力構築イベント
- 企業や団体との連携
- 情報の収集と共有

2024年10月には、CTFイベントである「Cyber SEA Game 2024」、2024年8月、11月、2025年1月、3月にテクニカルトレーニング、2024年12月にCII（Critical Information Infrastructure：重要情報インフラ）等の防御のためのトレーニングが実施された[※40]。

(サ)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

2023年度から実施されている「大洋州島しょ国・地域向けサイバー能力構築演習」では、総務省を実施主体者として「実践的サイバー防御演習（CYDER：Cyber Defense Exercise with Recurrence）」を活用した演習が行われている。同演習は、世界全体のサイバーセキュリティ上のリスク低減の観点から、地理的に重要な位置を占めるインド太平洋地域を含む開発途上国に対する能力構築支援、国際的な人材育成を行うことを目指している。対象は大洋州島しょ国・地域のサイバーセキュリティ対策に従事する政府職員及び通信事業者等の重要インフラ事業者の職員である。2024年度は、CYDERを含む演習及びサイバーセキュリティに関する基礎知識の習得を目的とした研修が2回実施された。

第1回[※41]は、フィジーで2024年10月2～10日に開催され、パラオ、ミクロネシア連邦、マーシャル諸島、ナウル、キリバス、フィジー、パプアニューギニア、サモア、ソロモン諸島、バヌアツ、トンガ、ツバル、クック諸島からの29名が参加した。第2回[※42]は、グアムで2025年2月7～14日に開催され、パラオ、ミクロネシア連邦、マーシャル諸島、ナウル、キリバス、フィジー、パプアニューギニア、サモア、バヌアツ、ツバル、クック諸島、フランス領ポリネシアからの26名が参加した。

4.1.2 米国の政策

2024 年 11 月 5 日、米国大統領選挙が行われ、共和党の Donald Trump 候補が圧勝した※43。また同時に行われた上院・下院選挙でも共和党が過半数を占め、民主党の Joe Biden 前大統領が進めてきた政策が大幅に転換されることとなった。Trump 大統領は就任直後から大統領令を多数発令し、クリーンエネルギー推進・気候変動対策の転換、移民制限、多様性・公正性・包括性（DEI：Diversity, Equity and Inclusion）政策の転換、国際機関脱退、国際援助削減、関税強化等の施策を矢継ぎ早に実施※44し、世界に大きな動揺を与えている。本項では、こうした状況下で 2024 年度に実施された米国連邦政府のサイバーセキュリティ政策等を概観する。

(1) Trump 大統領の政策転換の影響

Trump 大統領の政策転換の柱は、連邦政府の権限縮小による規制緩和・減税、国内産業優先の方針である。デジタル政策においては、例えば、2025 年 1 月 23 日発令の EO（Executive Order：大統領令）14179※45にて、Biden 政権における AI のリスクガバナンスの支柱だった EO 14110※46を過度な統制であるとして棄却、「米国が AI のリーダーシップを維持するための」行動計画を 180 日以内に策定する、とした。新しい行動計画において、AI の安全の記載は盛り込まれるとしても縮小されると思われる。なお、米国を含む AI ガバナンスの動向については「2.1.3 AI セーフティに関する取り組み」を参照されたい。

また Trump 大統領は、SNS 事業者等へのフェイク情報チェック要請は政府による言論統制であると指弾しており、2025 年 1 月 20 日、EO 14149「表現の自由と連邦政府の検閲終了」を発令して政府による規制を停止させた※47。同年 5 月 19 日、Trump 大統領は Melania Trump 夫人が連邦議会に協力をよびかけていた、性的画像（リベンジポルノ、ディープフェイク画像等）の不同意生成・配布禁止法案「TAKE IT DOWN Act※48」を承認した。性的画像には法的規制が課されることとなったが、他の AI の安全性やフェイク情報の氾濫・悪用が今後どう統制されるのかは 2025 年 5 月時点では不確定である。

一方、Trump 大統領により臨時に設置され、連邦政府の業務革新を標榜する政府効率化省（DOGE：Department of Government Efficiency）※49の見直し活動により、米国国土安全保障省（DHS：Department of Homeland Security）や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）等のサイバーセキュリティ対策活動が縮小された。例えば、かねてから Trump 大統領は選挙セキュリティ※50対策が自身の選挙運動への不当な干渉であると不満を表明してきたが、2025 年 2 月に CISA のフェイク情報対策関連人員を含む 300 ～ 400 人が削減されたという。同年 3 月には官民でセキュリティ情報共有を支援する Center for Internet Security, Inc.（CIS）※51への補助金が 1,000 万ドル（15 億円※52）規模で削減され、選挙インフラ情報共有団体 EL-ISAC（Elections Infrastructure Information Sharing and Analysis Center）への支援が打ち切られた※53。官民のセキュリティ情報共有は過去 10 年にわたり DHS が力を入れて推進してきた活動だが、後退が懸念される。また CISA の活動に関して、連邦政府重要インフラの脆弱性管理と防御を担うレッドチームが解雇された、と報じられた※54が CISA はこれを否定、業務効率化は行うがレッドチームの活動は継続する、とした※55。

CISA が支援するサイバーセキュリティ研究の非営利組織 The MITRE Corporation※56（以下、MITRE 社）の活動縮小も報じられた。MITRE 社は共通脆弱性識別子 CVE（Common Vulnerabilities and Exposures）に基づく脆弱性管理を担っている※57が、CISA の支援契約が 2025 年 4 月 16 日に失効すると報じられた※58。CVE の脆弱性管理プログラムは世界的に利用されており、同プログラムの停止は各国のサイバーセキュリティ対策者に深刻な影響を及ぼす可能性がある。しかし 4 月 16 日、CVE プログラムを存続させる基金の創設が公表され※59、当面の危機は回避された。CISA は可能な限り援助を続けるとしているが、今後の運営が順調に進むかには不安が残る。同じく 2025 年 4 月、CISA は契約していた VirusTotal 等の脅威検知・ハンティング用ツールの利用を停止すると報じられた※60。

更に CISA と米国国防総省（DoD：Department of Defense）が関わるサイバー軍事行動に関して、2025 年 2 月末から 3 月上旬にかけ、Pete Hegseth 国防長官の命により※61、ロシアに対する攻撃的サイバー作戦が停止したと報道された※62が、DoD と CISA は直ちにこれを否定した※63。政府のサイバーセキュリティ関連活動縮小が対ロシア等のナショナルセキュリティにも及んでいる、との憶測を否定する意図もあると思われる。セキュリ

ティ活動縮小の行きすぎが、安全保障を含めたサイバーセキュリティの確保に影響するのではないか、との不安はしばらく継続すると思われる。

こうした懸念の一方、Trump 大統領は Biden 前大統領が辞任直前（2025 年 1 月）に発令したサイバーセキュリティに関する大統領令は撤回していない。以下ではまず、この大統領令について見ていく。

(2) Biden 前大統領の大統領令

2025 年 1 月 16 日、Biden 大統領（当時）は、2021 年 5 月発令の EO 14028[※64] の改訂版となる EO 14144[※65] を発令した。EO 14144 は EO 14028 の対策（情報共有・対策近代化・ソフトウェアサプラチェーン強化等）に追加する形で、以下の項目を含むセキュリティ施策を指示している。

- サードパーティーソフトウェアサプライチェーン強化
  - サードパーティーリスク管理（テスト・認証等）強化
  - 「セキュアソフトウェア開発フレームワーク（SSDF：Secure Software Development Framework）[※66]」の実装と改訂
  - オープンソースソフトウェアセキュリティ強化
- 連邦政府システムのセキュリティ強化
  - 耐フィッシングに向けた Web 認証等の革新的な標準の試行
  - 政府と関係企業を横断した脅威の同定と共有
  - 遠隔 EDR（Endpoint Detection and Response）ツール利用等による脅威検知強化
  - FedRAMP（Federal Risk and Authorization Management Program）[※67] に基づく政府系クラウドセキュリティ強化
  - 宇宙システムのセキュリティ強化
- ネットワークのセキュリティ強化
  - IP アドレスの管理強化
  - ボーダーゲートウェイセキュリティの強化
  - DNS のセキュリティ強化
  - ハードウェアセキュリティモジュール等のトラスト基盤の活用
  - 量子コンピューティング向け暗号の選定推進
  - メールや会議音声・映像データの暗号化推進
- サイバー犯罪・詐欺対策強化
  - 運転免許等のデジタル身分証明書の普及推進
  - 属性検証プロセスのセキュア化
  - 不正取引事前検知・防御の試行検討
- AI セキュリティの推進
  - 重要インフラの AI によるセキュリティ強化
  - サイバー防衛対応 AI モデルの開発
  - サイバー防衛研究向け大規模学習データ整備
  - AI セキュリティや AI を含むインシデント対応の研究強化
  - AI システム脆弱性の管理強化
- 各政府機関の施策実践
  - IT 基盤・開発規則・セキュリティ規則の現代化
  - サイバーセキュリティプラクティスの共有
  - 製品調達規則の見直し
- 重大な悪意のあるサイバー活動への対応
  - 海外の国家支援活動家等の重大脅威に対抗するための EO 13694[※68] の拡張

以上のように内容は多岐にわたり、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）、CISA、DHS を含む関係機関に 30 日後から 270 日後まで期限を切って指示が出ている。サイバー防衛に関する AI 活用、あるいは政府機関の IT インフラ現代化を求める等、Trump 政権の意図と重なる部分があり、その点が、EO 14144 が撤回対象とならない一因であると思われる。しかし、前掲の DOGE の政府業務見直しがどの程度影響するかは自明でなく、各機関の活動が縮小される可能性は残っている。

2025 年 6 月 6 日、Trump 大統領は上記の EO 14144、及び EO 13694 を改訂する大統領令を発令[※69]し、不法移民・海外敵対勢力への対策強化、SNS 等における政治活動や AI に関する国内規制緩和の姿勢を鮮明にした。概要説明には以下のものが含まれている。

- ポスト量子暗号の対策に関する指示
- 最新の暗号プロトコルの政府機関採用
- AI セキュリティの脆弱性対策の重点化、検閲の否定
- 外国の敵対的勢力に特化したサイバー制裁適用と国内政治・選挙活動への適用の否定
- 不法移民を利するおそれのあるデジタル ID 義務化の削除

以下の各項では、主要なセキュリティ対策実施機関の活動について述べる。

(3) NIST と関連政府組織の活動

本項では、NIST の主な活動、及び NIST が策定した規格の適用に関する政府組織の活動を紹介する。AI ガバナンスに関連する NIST の活動（AI Safety

Institute※70の活動を含む）については、「2.1 AIセーフティ実現に向けた取り組み」を参照されたい。

(a) サイバーセキュリティフレームワーク 2.0 公開のフォローアップ

2024年2月26日、セキュリティ実務層と経営層を結ぶセキュリティマネジメントの枠組みが改訂され、「The NIST Cybersecurity Framework (CSF) 2.0」（以下、CSF 2.0）として公開された※71（「情報セキュリティ白書2024※72」の「2.2.2(1)(d)NISTの施策」参照）。CSF 2.0はマネジメント機能への統治（govern）の追加、サプライチェーンリスク管理の強化、他フレームワークとの整合等大幅な改定となり、業種・規模を問わない広範な組織での利用が期待されている。

CSF 2.0のリリース後、NISTは利用者のケース提供に対する要望に応えるため、共有できるユースケースを「CSF 2.0 Community Profiles」として公開している※73。現在策定中、または策定検討中のものには以下がある。

- NIST IR 8374r1 ipd※74ドラフト版
- ランサムウェアリスク管理（2025年3月意見募集終了）
- NIST IR 8546 ipd※75ドラフト版
- 半導体製造プロセスプロファイル（2025年7月30日意見募集終了予定）
- Cybersecurity and AI Workshop Concept Paper※76
- 2025年4月3日開催のCyber AI Profile Workshop※77で提案されたCyber AI profile

上記で注目されるのはCyber AI Profileである。これはCSF 2.0に基づき、AIのサイバーセキュリティマネジメントに関する具体事例を作成する提案で、AIによるセキュリティ強化、AIに起因するセキュリティ脅威への対応がいずれも想定されている。NISTによりAIコミュニティとの官民連携のもとで策定された「AI Risk Management Framework※78」との紐付けも行われる。2025年4月のCyber AI Profile Workshop以降、ステークホルダーによる個別プロファイルの作成計画が具体化すると思われる。

(b) サプライチェーンセキュリティ規格群の整備

2024年5月14日、管理対象非機密情報（CUI：Controlled Unclassified Information）の保護規格の改訂版「NIST SP 800-171 Rev.3」及びCUIセキュリティ要件評価規格の改訂版「NIST SP 800-171A Rev.3」が公開された※79。政府調達サプライチェーン上の事業者が遵守すべきCUI保護施策の改訂であるが、親規格であるSP 800-53 Rev.5※80の公開（2020年）に合わせて改訂された第2版は適用の難しさの問題をはらんでいた。このため改訂第3版では、セキュリティ要件数や要件区分の簡易化、組織独自の統制の容易化等に配慮して改訂が行われた。

また、NISTは2024年11月1日、サプライチェーンのサイバーセキュリティリスクマネジメントプラクティス「NIST SP 800-161 Rev. 1」の事例更新※81、続けて11月13日に前記CUIの拡張セキュリティ要件規格「SP 800-172 Rev.3」のドラフトを公開した※82。後者のSP 800-172 Rev.3改訂はセキュリティ要件の具体化・更新やSP 800-171 Rev.3、SP 800-53 Rev.5等の関連規格との整合を主眼としている。

なおCUI保護に関連して、2024年10月15日、DoDが防衛調達事業者に課すサイバーセキュリティ成熟度モデル認証（CMMC：Cybersecurity Maturity Model Certification）プログラムの最終版を公開した※83。CMMC認証取得は、当該調達事業者が契約情報及び調達に関わるCUIの保護規則を遵守することが前提となる。

データ保護・リスクマネジメント系規格の整備・実装が進む一方、ソフトウェアサプライチェーンセキュリティで注目されるソフトウェア部品表（SBOM：Software Bill of Materials）※84について、NISTの目立った活動は見られない。SBOMの普及推進はCISAの担当となっていると見られる。

(c) U.S. Cyber Trust Markの運用

U.S. Cyber Trust Mark※85は、米国の一般向けIoT製品・ソフトウェア製品のサイバーセキュリティが確保されていることを示す認証ラベルである。2021年5月のEO 14028によって同ラベルを付与する認証制度の設置が指示され、満たすべきセキュリティ基準の策定がNISTに指示された。NISTは連邦取引委員会（FTC：Federal Trade Commission）と連携し、2022年2月4日、IoT製品、及びコンシューマーソフトウェア製品の推奨セキュリティ基準を公開した※86。

2022年2月以降、NIST及び連邦通信委員会（FCC：Federal Communications Commission）は同基準に基づく認証パイロットプロジェクトの試行、制度設計を行ってきたが、2025年1月7日、Biden政権は認証制度の運用開始を発表した※87。日本国内では2025年3月25

日、IoT 製品の「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が開始された※88が、いずれも強制力のない任意の制度であり、2024 年 12 月 10 日に発効し、罰則を伴う欧州連合（EU：European Union）のサイバーレジリエンス法（Cyber Resilience Act）※89とは対照的である。2025 年 4 月以降、U.S. Cyber Trust Mark を含む各国の制度間で相互承認の調整が進むと思われる。一方で、Trump 政権の政府権限縮小方針により U.S. Cyber Trust Mark 制度も廃止の懸念があるとも言われる※90。

(d) その他の NIST 規格の状況

2024 年度に公開・改訂された NIST 規格には以下のものが含まれる。

- NIST SP 800-231※91（2024 年 7 月 30 日公開）
  サイバーセキュリティの脆弱性を形式化するバグフレームワーク（Bugs Framework）の概要を示している。脆弱性に関する既存の枠組みである CWE（Common Weakness Enumeration）※92、CVE※93 は体系的なラベリングや構造化が難しいとし、バグフレームワークは構造化の形式を与えるものだとしている。
- NIST SP 800-63-4 2pd※94（2024 年 8 月 21 日公開）
  デジタルアイデンティティガイドラインの第 2 版ドラフトが公開され、2024 年 10 月まで意見募集が行われた。Biden 政権（当時）が要請した個人識別・認証におけるなりすまし・詐欺攻撃対策の一環である。AI に関する規定が含まれ、この点が拡張される可能性がある。関連するアイデンティティ検証、認証マネジメント、認証連携の各規格第 2 版も公開された※95。
- NIST SP 800-218A※96（2024 年 7 月 26 日公開）
  AI の安全に関する EO 14110 により策定された、生成 AI とデュアルユース対応基盤モデル※97 開発のセキュリティガイドラインであり、SSDF に基づく詳細なプロファイルが記載されている。前掲のとおり EO 14110 は撤回されたが、同ガイドラインは 2025 年 4 月時点で有効である。ただし、Trump 政権の政府機関活動縮小方針で NIST も影響を受けていること、EO 14110 の AI テスト要請が撤回されたこと等から、Trump 政権下で今後 AI セキュリティに関する規格が策定される可能性は小さいと思われる。

(4) CISA の活動

本項では CISA と関係機関の活動、及び Trump 政権の政策転換による影響について述べる。

(a) CISA の役割強化

2024 年 4 月 30 日、米国国家安全保障会議（NSC：National Security Council）は海外からのサイバー脅威の変化に対応するため、重要インフラセキュリティに関する覚書※98 を発行した。これに基づき、DHS は以下のように CISA の役割を強化した※99。

- 国家の重要インフラのセキュリティ・頑健性に関する調整の実施（National Coordinator）
- 重要インフラ 8 セクター及び一つのサブセクターに関するリスク管理強化（セクターリスク管理機関 SRMA（Sector Risk Management Agency）として活動）
- 連邦政府内のパートナー支援（情報共有、ガイダンス）

この役割の強化に基づき、CISA は情報提供・ガイダンス等の活動のほか、サイバー攻撃で経済・健康等に深刻な影響が発生し得る重要インフラ SIE（Systemically Important Entities）の確定を行った。

次いで同年 10 月 29 日、重要インフラやそのサプライチェーンが海外に広がり、かつ深刻なサイバー攻撃被害が世界的な影響を及ぼす状況を踏まえ、CISA は重要インフラセキュリティに関する国際戦略を発表した※100。同戦略は、①米国が依存する海外重要インフラの頑健化、②統合的なサイバー防御の強化、③国際活動に関わる政府機関の調整統一、の三つを目標とし、DHS、DoD 等と連携して海外重要インフラへの依存性の評価、及び海外企業との連携を進めるとしている。

前記の目標①について、CISA は海外パイプライン・通信・基盤サプライチェーン等の海外重要インフラの同定と優先度付け、国際パートナーとの脅威情報共有や能力強化、セキュリティに関する標準・ガイドライン策定を推進するとしている。目標②については、CISA は国際的な CSIRT（Computer Security Incident Response Team）連携によるリスク低減、セキュア開発に関する標準化・規格化、重要パートナーのリスク対応力強化を推進するとしている。また目標③については、CISA は国内政府機関の海外活動プロセスの共通化、自組織（CISA）内の情報共有・活動調整、国際業務のための人材強化を推進し、One CISA として活動するとしている。

(b) CISA の人員・予算削減の影響

Trump 政権の誕生により、CISA は業務縮小の対象となって環境は激変、大幅な人員削減、予算カットが行われた。CISA を所管する DHS は、2025 年 2 月 18 日の大統領令※101 に基づき、所管機関の業務効率化・

予算削減計画を公開した※102。同計画に基づき2025年6月4日時点でCISAは約390の連携機関・調達事業者に対する契約をカットまたは縮小し、約6億5,167万ドル（約977億5,050万円）を削減するとしている。

このうち選挙セキュリティに関して、CISAは2025年3月11日、各州の選挙セキュリティ対策支援予算を打ち切ると表明した※103。各州や自治体の選挙セキュリティ担当者は、選挙セキュリティ対策ツールキット※104やサイバー脅威の監視・情報共有等、CISAの支援に大きく依存してきた。担当者からは前述の選挙インフラ情報共有団体EL-ISACの支援打ち切りと合わせ、各州の選挙セキュリティ対策が機能しなくなるとの懸念が表明されている※105。また選挙セキュリティ専門家は、CISAの予算カットは連邦を含めた選挙のセキュリティと頑健性への脅威であると警告している※106。更に前項で述べた役割強化に対してCISAがどこまで実践できるのかも2025年4月時点では不透明であり、今後のCISAの情報開示が待たれる。

(5) OMBの活動

2025年4月3日、米国行政管理予算局（OMB：Office of Management and Budget）は、新たなAIに関するEO 14179の実施規則M-25-21を公開した※107。M-25-21は連邦政府機関に対してAIの積極導入、及びAI革新の障害となる規制の排除を求め、そのためのAI戦略をM-25-21公開後180日以内に公表するとしている。AI戦略においてはAIの成熟度強化、受容拡大のためにセキュリティ、プライバシー、機密保護、データ信頼性等の観点からアセスメントを実施することを求めている。

また各機関のAIの統制マネジメントについては、M-25-21公開後60日以内にこれを統括するChief AI Officer（CAIO）を任命し、90日以内に課題調整のためのAI統制委員会（AI Governance Board）を置く、としている。AI統制委員会はIT、サイバーセキュリティ、プライバシー、データ等に加え人権、個人の自由に関する専門家で構成するとしており、AIの安全性に関する規制排除が言われながらも一定の配慮がなされる可能性は残っている。

4.1.3 欧州の政策

欧州のサイバーセキュリティ政策は欧州連合（EU：European Union）でまとめたサイバーセキュリティ戦略に基づいており、取り組みの進捗状況やEU全体のサイバーリスクの概況を様々なレポートにより確認することができる。以下ではまずEUにおけるサイバー脅威の動向とサイバーセキュリティ戦略を紹介した上で、2024年度中に動きのあった主要なサイバーセキュリティ政策をEU法整備の観点から述べる。

(1) EUにおけるサイバー脅威の全体動向

欧州ネットワーク・情報セキュリティ機関（ENISA：The European Union Agency for Cybersecurity）は「ENISA Threat Landscape」（以下、ETL）においてEU圏全体のサイバー脅威の年次動向をまとめている。ETLは、サイバーセキュリティ関連の公開情報や関係各所からの共有情報、学術情報、ダークウェブ※108等の観測情報等を総合した、体系的な定点観測報告及びセキュリティ上の助言である。ETL作成の詳細は2022年7月に発行されたガイド※109に定められている。

2024年9月に発行されたETL 2024※110によれば、2023年7月から2024年6月にかけてのEU圏のサイバー脅威の主だった動向は次のとおりである。

- 可用性への脅威
  システムやサービスの可用性を標的とする攻撃、特にDDoS攻撃が、最も頻繁に観測される脅威となった。前年まではランサムウェアが最も多く観測されており、攻撃者の戦略や目的の変化を示唆している可能性がある。DDoS攻撃は特に金融セクターにおいてロシア・ウクライナ戦争のような地政学的な出来事と連動して増加が見られた。DDoS攻撃代行サービスの存在も攻撃の増加に寄与している。
- ランサムウェア
  観測頻度の上では「可用性への脅威」に続いて2位となったものの、ランサムウェアは依然としてEUにおける深刻な脅威である。マルウェア攻撃をサービスとして販売するMaaS（Malware as a Service）モデルの普及により、技術力の低い攻撃者でもランサムウェア攻撃を実行できるようになり、企業や公共部門を問わず多くの組織が被害を受けている。
- データに対する脅威
  データに対する侵害や漏えいといった脅威も増加傾向にある。個人情報を扱う組織が標的となりやすい。フィッシング、ランサムウェア、サプライチェーン攻撃等の組み合わせが用いられるようになってきている。
- サイバー脅威の越境
  ETL 2024で分析された1万1,079件のインシデント

のうち322件はEU加盟国2ヵ国以上を標的としていた。また、ロシア・ウクライナ戦争との関連が認められるEU各国へのDDoS攻撃の増大や、ロシアとの関係が推測されるグループによるEU加盟国の選挙への攻撃の広がりも指摘される等、国境を越えたサイバー脅威が具体化している。これらのサイバー脅威への対処にあたっては、EU加盟国間での円滑な連携が必要になる。

- その他の脅威
  ランサムウェア以外のマルウェア（情報窃取型マルウェア、モバイルバンキングを狙ったトロイの木馬等）、ソーシャルエンジニアリング（フィッシング、サプライチェーン侵害への悪用等）、サプライチェーン攻撃も引き続き重大な脅威である。広く利用されるソフトウェアやサービスを標的にしたサプライチェーン攻撃は広範囲に影響を及ぼす可能性があり、データ圧縮ソフトウェアであるXZ Utilsに仕掛けられたバックドアのように実例も観測されている※111。XZ UtilsはLinux向けのオープンソースソフトウェアとして開発・管理がなされていたが、2年以上をかけて徐々に開発者コミュニティに浸透した、中国系の名前を持つ脅威アクターによりバックドアが混入された。たまたま他の開発者が気付いたことで発覚したが、潜在的には世界中のLinuxホストが影響を被った可能性のある重大事案である。その他、AIを悪用した情報操作も、今はまだ限定的だが、将来的な脅威として注目されている。

(2) EUにおけるサイバー脅威の今後の見通し

ENISAはサイバー脅威の現状だけでなく長期の見通し※112をまとめている。この長期予測は2030年ごろまでに深刻化し得る脅威やサイバーセキュリティ課題を特定することを目的としている。長期予測で取り上げられた主なサイバー脅威・課題は以下のとおりである。

- ソフトウェア依存関係におけるサプライチェーン侵害
  オープンソースライブラリ等へのバックドア設置による広範な情報窃取や破壊活動が起こり得る。
- スキルの不足
  サイバーセキュリティ人材の不足が求人情報等を通じて組織の脆弱性を示す間接情報と見なされ、攻撃者に悪用される。
- サイバーフィジカル領域のレガシーシステムやパッチ（修正プログラム）未適用システムへの攻撃
  IoTの普及やスキル不足と相まって、管理不十分なシステムが攻撃対象となる。
- 国境を越えたICTサービスプロバイダーの単一障害点化
  重要な社会インフラを支えるICTプロバイダーが攻撃されることで広範な機能不全が引き起こされる。
- 高度な偽情報・影響工作
  AI技術を用いた偽情報の拡散、選挙介入、社会不安の醸成が更に悪化する。
- ハイブリッド脅威の高度化
  サイバー攻撃と物理的攻撃を融合した、検知や防御が困難な攻撃が広まる。
- AIの悪用
  AIの能力を利用した、生体認証データ等の収集、攻撃の自動化・高度化が進む。
- その他の脅威
  デジタル監視の強化、宇宙インフラへの攻撃、スマートデバイスデータを用いた標的型攻撃、量子コンピューティングによる暗号解読、デジタル通貨を利用したサイバー犯罪、eヘルス・遺伝子データの悪用、自然災害によるデジタルインフラへの物理的影響等が挙げられている。

これらの脅威は、AIを筆頭とする技術の進化、デジタル化した社会インフラへの依存、地政学的な緊張の高まりといった要因によって、今後の複雑化・深刻化が予測されている。この見通しのもとで、EU全体での協調的な対策と、将来を見据えた備えが不可欠になっていると言える。

(3) EUのサイバーセキュリティ戦略

EU全体での現行のサイバーセキュリティ戦略は2020年に策定された「The EU's Cybersecurity Strategy for the Digital Decade※113」（以下、EUサイバーセキュリティ戦略）にまとめられている。EUサイバーセキュリティ戦略では、デジタル化の進む社会がサイバー攻撃によって被り得る潜在的被害を重く受け止め、実効性重視の対策が多数取り上げられている。以下では同戦略を要約する。

(a) EUにおけるサイバーセキュリティ課題

EUサイバーセキュリティ戦略が着目するサイバー脅威の筆頭は、コネクテッド機器、電力網、銀行、航空機、公共機関、病院といった、生活に不可欠な要素へのサイバー攻撃である。ICT社会においてこれらのシステムは深く相互接続しており、サイバー攻撃が社会インフラを

連鎖的に損なうことが懸念されている。また、コネクテッド機器の増大とコロナ禍による働き方のデジタル化の加速により、社会の脆弱性は増している。ロシア・ウクライナ戦争に代表される地政学的な緊張の高まりや 5G 通信等をめぐる技術的な覇権争いも、サイバー空間における脅威の状況・影響を複雑化させている。

重要インフラを標的としたサイバー攻撃は、EU 圏に限定されないグローバルリスクである。DNS（Domain Name System）のようなインターネットの中核機能そのものや、基盤的サービスを提供する少数の民間企業への依存によって、サイバー脅威の潜在的影響は増している。EU 圏でサイバー犯罪は蔓延しているが、サイバー犯罪の報告率は低い。データ侵害による損失も深刻であり、その経済的コストは増大の一途をたどっている。更に、デジタルサービスや金融セクター、公共セクター、製造業等が頻繁にサイバー攻撃の標的となっているにもかかわらず、サイバーセキュリティへの意識は低く、備えも十分でない。サイバーセキュリティ人材が大幅に不足していることも、脅威への対応を遅らせる要因となっている。EU 全体としては、越境するサイバー脅威に対して、組織・国家の垣根を超えた集団的な状況認識が不十分かつ加盟国間の情報共有も限定的であるため、大規模なサイバーインシデントへの効果的な対応が困難な状況にある。

ハイブリッド型の脅威、つまり、インフラや経済プロセス、公的機関へのサイバー攻撃と偽情報キャンペーン等の融合も深刻化している。ハイブリッド型の脅威がサイバーセキュリティ上の EU の弱点に結び付くと、物理的な損害、個人データへの不正アクセス、産業・国家機密の漏えい、社会不信の増大や結束の弱体化を引き起こすおそれがある。

(b) 課題緩和・解決へのアプローチ

課題緩和や解決のために EU サイバーセキュリティ戦略で採用されたアプローチは次の三つの柱からなる。

- サイバーレジリエンスの強化と技術的主権の確立
  重要インフラやサービスのセキュリティを根本的に強化し、セキュアな技術を EU 内で自主開発・利用できる能力を確保する。
- サイバー攻撃の防止・抑止・対応能力の向上
  サイバー攻撃を未然に防ぐとともに、攻撃発生時に迅速かつ効果的に対応できる運用能力を構築する。
- グローバルでオープンかつ安全なサイバー空間の推進
  EU の価値観に基づいたグローバルなサイバー空間を維持し、国際協力と多国間主義を推進する。

この三つの柱それぞれを構成する要素として多数のイニシアティブ（提言）が EU サイバーセキュリティ戦略には盛り込まれている。これらのイニシアティブの重要な基盤となるのが、サイバーセキュリティに関連する数々の EU 法の整備である。特に 2024 年度中に整備・施行が進んだものを取り上げると、各国のサイバーセキュリティ当局や企業のセキュリティ義務を拡大する NIS2 指令（Network and Information Systems Directive 2）[※114]、EU 広域でのインシデント対応能力を高めるサイバー連帯法、金融セクター向けのレジリエンス確保を狙ったデジタルオペレーショナルレジリエンス法、デジタル要素のある製品一般のセキュア・バイ・デフォルトを徹底するサイバーレジリエンス法、ICT 製品のセキュリティ認証制度ほかを定めるサイバーセキュリティ法の改正等がある。NIS2 指令やサイバー連帯法は、各国の SOC（Security Operation Center）や CSIRT のネットワークを通じた連携強化、インシデント報告の改善、官民連携、国際協力を促すものとなっている。本項ではこれらの主なサイバーセキュリティ関連の各 EU 法について後述する。

(c) サイバーセキュリティ能力の評価

NIS2 指令の第 18 条は、2 年に一度、EU 全体のサイバーセキュリティ能力の整備状況等を評価することを求めている。この役割を担う ENISA の 2024 年度の報告書[※115]では次の評価を与えており、現状は道半ばと言える。

- EU の政策的枠組みは成熟しているが、NIS2 指令の実施は進行中であり、加盟国や事業者においてリソース面の課題が持ち上がっている。加盟国のサイバーセキュリティの成熟度の平均は 100 点満点中の 62.5 点であり、加盟国やセクター間でばらつきが見られる。
- サイバーセキュリティスキル、中小企業のセキュリティ意識・投資、サプライチェーンセキュリティ対策、包括的な状況認識の達成において、依然として目標との間に大きなギャップが存在する。インシデントは過小に報告・評価されている可能性が高い。
- 中長期の見通しとしては、新たに制定された各種 EU 法の効果的な実施、事業者支援、市民や民間企業のデジタルスキル向上、協力と状況認識の強化、サプライチェーンリスクへの対応、AI や耐量子暗号のような新技術への適応に重点が置かれる。

以後の各項では2024年度中に目立った動きのあった主要なサイバーセキュリティ法令について述べる。

(4) NIS2 指令

2016年のNIS指令[※116]に準拠する国内法制定[※117]の議論を経て、NIS指令自身に不足やあいまいさがあるため、これを置き換える必要がある[※118]としてNIS2指令が2022年に導入された。NIS2指令が取り扱う課題は多岐に及ぶが、ここでは以下の三つを大きな柱として取り上げる。

(a) 注視すべき対象セクターの拡大

サイバー脅威の共有対象とすべき産業セクターの範囲や定義にNIS指令では不足があった。NIS2指令では、注視すべき対象セクターに公共セクターや運輸、食品製造・流通等を加え、その数を7から18へと大幅に増やした。また、サプライチェーン上で重要な役割を果たす中小企業も対象とするよう改められた。

(b) 企業等のインシデント通報義務の明確化

注視すべき産業セクターに属する企業等は、重大エンティティ（essential entity）または重要エンティティ（important entity）に分類される。NIS2指令ではこれらの組織の守るべき義務を明確化した。具体的には、自らのサービスの依存するITインフラにおけるセキュリティ対策の実施と、インシデント発生時の各国当局への通報である。前者については多種多様なインシデントに統一的な枠組みで対応するオールハザード（all-hazards）アプローチをうたい、事業継続計画（BCP：Business Continuity Plan）策定やサプライチェーンセキュリティ確保を含むものとしている。後者については重大インシデントを認識してから24時間以内に各国のNational CSIRTに通報することや、72時間以内の続報、1ヵ月以内の詳細報告が求められている。報告項目の指定や通報期限の明記がNIS指令との大きな違いである。

(c) 各国のサイバーセキュリティ当局の役割と連携

各国で指名あるいは設立しなければならないNational CSIRTの満たすべき条件をNIS2指令では明記し、かつ、各国のサイバー危機管理当局がEU内で国際連携するための仕組みとして、新たにEU-CyCLONe（European Cyber Crisis Liaison Organisation Network）[※119]を立ち上げることを盛り込んだ。各国のNational CSIRTは、NIS2指令で拡大した対象セクターにおけるインシデント対応に責任を持つことが義務付けられている。EU-CyCLONeの事務局機能はEU全域でのサイバーセキュリティ政策を担うENISAが提供する。EU-CyCLONeは大規模なサイバーインシデント発生時の情報共有を支援し、加盟国間の連携と危機対応能力を強化する。また、状況認識の共有、影響評価、政治レベルでの意思決定支援も担うとされる。

NIS2指令に準拠する加盟各国における新たな国内法の制定期限は2024年10月17日とされたが、2025年3月時点で国内法の整備が終わっているのは、ベルギー、クロアチア、ギリシャ、イタリア、リトアニア、ルーマニアの6ヵ国のみであり、大部分の加盟国では法案審議中となっている[※120]。準拠法の整備と施行の遅れはNIS2指令が目指すEU内での国境を越えたサイバーセキュリティの強化の遅れと同義である。2024年11月末ごろには、その時点で対応が遅延していた23ヵ国宛に速やかな国内法化を求める通知を欧州委員会（European Commission）より送付している[※121]。

(5) サイバー連帯法（CSoA）

「サイバー連帯法（CSoA：Cyber Solidarity Act）[※122]」が解決しようとしている主な課題は、EU加盟国間で断片化されているサイバーセキュリティ対策の連携円滑化である。特に、大規模な損害の発生に先んじてサイバー脅威を検知する能力と、サイバー脅威に関わる情報交換の強化が重視されている。この背景には、ロシアによるウクライナへの軍事侵攻がサイバー作戦を伴っており、国家間の紛争にサイバー活動が広範に組み込まれているという現状がある。一国の領分を超える事態をリアルタイムで検知し集団的能力を強化して対応するために、より動的で協調的なサイバーセキュリティ環境を構築するという戦略をEUは採用した[※123]。CSoAはこの戦略を具体化する法令であり、次に示す三つの主要な仕組みの導入を定めている。

- 欧州サイバーシールド（European Cyber Shield）
  EU全域で相互接続されたSOCのネットワークである。EU横断でサイバー脅威を検知し、分析・対応を大幅に改善することを目的としている。AI等高度なテクノロジーの助力も得つつ潜在的なサイバー脅威を特定した上で、各SOCは国境を越えて警告情報を関連当局に広める。同ネットワーク参加にあたり、各加盟国はNational SOCを指定しなければならない。効果的な情報共有とSOC間の高度な相互運用性確保のための各種要件も法に含まれている。

- サイバーセキュリティ緊急メカニズム（Cyber Emergency Mechanism）
  インシデント発生に備えた準備行動の支援、EU サイバーセキュリティリザーブ（EU Cybersecurity Reserve）の創設、加盟国間の相互支援の確保という 3 系統の取り組みである。準備行動の支援に関しては、金融、エネルギー、医療、輸送等の重要セクターで活動する事業体のセキュリティテストを促進し、サイバー脅威によって悪用される可能性のある潜在的な脆弱性を特定する。EU サイバーセキュリティリザーブは、「信頼できるプロバイダー」として指定された民間事業体によって提供されるインシデント対応サービスの集合体である。このリザーブに含まれるサービスは、重大または大規模なサイバーインシデントへの対処に際して、加盟国または EU 機関の要請に応じて展開できる。相互支援の確保に関しては、サイバーセキュリティインシデントの影響を受けたある加盟国に、別の加盟国から人員派遣等の支援を行う際に資金援助を行う。
- サイバーセキュリティインシデント・レビューメカニズム（Cybersecurity Incident Review Mechanism）
  重大または大規模と見なされる特定のサイバーセキュリティインシデントを事後にレビューする仕組みである。欧州委員会や、加盟各国の国内当局の要請に応じて ENISA がレビューを実施する。レビュー後、インシデントから得られた主要な教訓と、必要に応じて EU のサイバー対応能力を改善する推奨事項を含むレポートを ENISA にて作成する。同メカニズムは、サイバーセキュリティ緊急メカニズムのもとで取られた措置の有効性と、サイバーセキュリティリザーブの利用状況、EU のサイバーセキュリティ産業の競争力強化に対する CSoA の貢献についても評価する。

CSoA は既存のサイバーセキュリティ法制を補完することで、対処調整と緊急対応を担う EU 広域の仕組みを提供する。CSoA は NIS2 指令の特別法（Lex specialis）であり、NIS2 指令ではカバーされていない緊急対応のメカニズムを導入する。また、NIS2 指令が主に個々の組織におけるサイバーセキュリティリスク管理の遵守とインシデント報告の義務付けに焦点を当てているのに対し、CSoA は EU 加盟国間の連携と対応能力の確立を扱っている。後述するサイバーレジリエンス法との比較では、同法がセキュア・バイ・デフォルトによるサイバーセキュリティの予防的側面に焦点を当てているのに対し、CSoA は大規模なサイバー攻撃やその他の緊急事態における即時の対応と緩和を扱っている。

欧州委員会は 2023 年 4 月 18 日に CSoA の最初の法案を欧州議会（European Parliament）に提出し、2024 年 12 月 2 日に採択に至り、その後、2025 年 2 月 4 日には施行されている。このように迅速な立法プロセスの進行は、国境を越えてサイバー脅威への対処・連携能力を速やかに高めなければならないという EU 加盟国間の強い問題意識の現れと言える。

(6) デジタルオペレーショナルレジリエンス法（DORA）

「デジタルオペレーショナルレジリエンス法（DORA：Digital Operational Resilience Act）[※124]」は金融システムのサイバーセキュリティ上の安定性維持を狙った法令であり、金融セクターを適用対象としつつ、金融機関だけでなく、その運営に不可欠な ICT サービスを提供するサードパーティープロバイダーにも適用される特徴を持つ。

DORA が着目する主要な課題は、金融セクターの依存先 ICT サービスに由来するサプライチェーンセキュリティリスクへの対策である。金融機関は業務遂行のために高度な ICT ツールやシステム、更にはサードパーティープロバイダーに大きく依存しており、これらの依存先 ICT へのサイバー攻撃や運用事故といった新たなリスクが潜在している。しかし、重要な機能を提供するこれら ICT サードパーティープロバイダーは金融セクター固有の規制や監督の枠外にある場合が多く、これがリスク管理上のギャップとなっていた。加えて、金融システムは相互接続性が高いため、1 ヵ所での ICT インシデントが国境を越えて他の金融機関や経済全体に急速に波及し、社会システム全体のリスクが実体化するおそれもある。余裕資金の確保を中心とした従来のリスク管理では ICT 固有のこうしたリスクに十分に対応できず、加盟国間の規制の断片化も課題となっていた。

DORA は、インシデント発生の予防だけでなく、インシデント発生時の影響を最小限に抑え、迅速に回復する能力の向上に重点を置く。このアプローチは、以下の五つの柱として具体化されている。

- ICT リスク管理
  金融機関に対し、ICT リスクを特定、評価、軽減、監視、管理するための包括的なフレームワークの確立を義務付ける。経営陣は ICT リスク管理戦略を定義・承認・監督し、その実施に対して最終的な責任を負う。

また、業務ニーズに適した、信頼性が高く、技術的に回復力のある最新の ICT システム、プロトコル、ツールの利用と維持を金融機関に要求する。

- ICT サードパーティーリスク管理
  サードパーティープロバイダーに起因するリスクを継続的に監視することを義務付ける。プロバイダーとの契約にはセキュリティ・可用性・データ保護等に関する特定の重要条項を盛り込まなければならず、すべての ICT サードパーティー契約に関する詳細な情報を記録した情報登録簿を作成・維持することも求められる。更に、金融システムにとって重要（critical）と指定された ICT サードパーティープロバイダーに対しては、欧州監督機関（ESAs：European Supervisory Authorities）による直接的な監督を行う新たな枠組みを導入する。
- デジタルオペレーショナルレジリエンステスト
  金融機関に対し、ペネトレーションテストを含む定期的なテストプログラムの確立と実施を義務付ける。リスクプロファイルや事業環境に応じ、特定の金融機関に対しては、少なくとも 3 年ごとに、実際の脅威シナリオに基づいた高度なテスト（TLPT：Threat-Led Penetration Test）の実施を要求する。
- ICT 関連インシデント管理
  ICT 関連インシデントを迅速に検知し、効果的に管理・記録・分類するプロセスを確立した上で、重大な ICT 関連インシデントが発生した場合には規制当局へ速やかに報告することを金融機関に義務付ける。報告の際には、影響を受ける顧客・取引相手の数、インシデントの期間、地理的範囲、データ損失の程度等、事前に定義された基準に基づきインシデントを分類する。重大なサイバー脅威も当局への報告対象となる。
- 情報共有
  サイバー脅威に関する情報やインテリジェンスを金融機関の間で共有することを奨励する。なお、情報共有の際には、事業上の機密情報や個人データの保護、関連する競争法規の遵守に配慮する。

幅広い重要・基幹セクターに適用される NIS2 指令に対し、DORA は金融セクターに特化した特別法であり、金融システム固有のリスクを考慮した詳細かつ厳格な要件を定めている。適用対象機関においては DORA の規定が NIS2 指令の規定に優先する。EU 加盟各国の準拠国内法が必要な NIS2 指令に対し、DORA は EU 全域で直接に適用される EU 規則でもある。金融機関は自セクターに特化した一貫した規制に従うことになり、準拠法が複数ある場合に生じがちな混乱を防いでいる。

DORA は 2023 年 1 月 16 日に発効し、その規定は 2025 年 1 月 17 日から全面的に適用されている。この適用開始日に向けて、欧州委員会は DORA の要件を具体化するための多数の実施技術基準（ITS：Implementing Technical Standards）や規制技術基準（RTS：Regulatory Technical Standards）といった二次法規を 2024 年から 2025 年初頭にかけて順次採択・公表※125してきた。例えば、金融機関は、2025 年 1 月 1 日までに ICT サードパーティー契約に関する情報登録簿※126を整備しなければならず、各国の管轄当局は、これらの情報登録簿を収集し、2025 年 4 月 30 日までに ESAs へ提出しなければならない。ESAs は提出された情報に基づき重要 ICT サードパーティープロバイダーを指定し※127、2025 年 7 月までに該当プロバイダーへ通知する予定である。ESAs による重要 ICT サードパーティープロバイダーへの監督は 2025 年から開始される。また、大規模なサイバーインシデント発生時の EU レベルでの連携を目的とした EU-SCICF（EU Systemic Cyber Incident Coordination Framework）※128が 2024 年 11 月に設立された。

(7) サイバーレジリエンス法（CRA）

「サイバーレジリエンス法（CRA：Cyber Resilience Act）※129」は、多くのデジタル製品に見られるセキュリティ対策の不備を、製品の製造業者の責任において改善することを課す EU 規則である。CRA の適用対象となる「デジタル要素を含む製品（product with digital elements）」（以下、デジタル製品）とは、ソフトウェアまたはハードウェア製品とその遠隔データ処理ソリューションを意味し、ソフトウェアまたはハードウェアのコンポーネントが個別に市場に出回る場合も含むとされる。具体的には、パソコン、スマートフォン、IoT 機器、OT（Operational Technology：制御技術）機器、ファームウェアや OS、スマートフォンやパソコン向けのソフトウェア等が対象に含まれる。なお、デジタル製品と直接に結び付かない純然たる PaaS（Platform as a Service）や SaaS（Software as a Service）等は CRA の適用対象とはならない。

CRA の策定に先立ってはいくつかのセキュリティ課題が認識されていた。第一に、コネクテッド機器が大量に社会に浸透している一方で、出荷時点でのセキュリティを確保するセキュア・バイ・デフォルトが徹底されていない。第二に、中小・零細事業者等も含むデジタル製品の利

用者のセキュリティ理解には限界がある。第三に、デジタル製品に見られる様々な脆弱性を利用したインシデントは既に多発している。ETL 2024 では観測されたインシデントの過半が DDoS とランサムウェア攻撃であるとしているが、これらの攻撃ではデジタル製品の脆弱性を悪用されることが多い。このような状況から、EU 市場を流通するデジタル製品の製造業者にセキュリティ対策の義務を課すこととしたのが CRA の骨子※130 である。

例外規定はあるものの CRA が製造業者に求める義務的要件は大まかには次のとおりである。

- 製品に十分なセキュリティ対策を施した上で、出荷時の設定がセキュア・バイ・デフォルトに沿うようにする。
- セキュリティアップデートにより遅滞なく脆弱性対策が行えるようにする。可能なら自動アップデートをデフォルトで有効にする。
- 製品中のデジタル要素に含まれる脆弱性を事前に特定し文書化する。これには SBOM の参照を含む。
- システムの内部動作を監視・記録することでセキュリティ情報を提供できる仕組みを設ける。
- 当該デジタル製品の脆弱性を突いた事例を製造業者が把握した場合には、NIS2 指令における CVD（Coordinated Vulnerability Disclosure）に従い、当該事象発生国及び管轄 CSIRT、ENISA に対し、24 時間以内に早期警戒情報を通知し、72 時間以内に追加の脆弱性情報を提供する。
- デジタル製品の製造業者は CRA に対する適合性評価手続きを実施しなければならない。

想定されるリスクによって、デジタル製品は「重要なデジタル製品（クラス I・II）」「クリティカルなデジタル製品」「これら以外の製品」という四つのカテゴリに分類されており、利用できる適合性評価手続きはそれぞれに異なる。また、CRA への整合規格（harmonised standard）に準拠していることをもって CRA 準拠と見なすこともできる。なお、CRA の違反事業者に対しては、1,500 万ユーロまたはグローバル年間売上高の 2.5% のどちらか高い方が課徴金として科せられる※131。

CRA は CE マーキング※132 と統合されており、CRA への適合は CE マークによって示される。EU 圏への輸入業者等は、輸入する製品に CE マークが貼付されていることを確認する義務を負っている。このため、輸入されるデジタル製品についても、CE マークによって CRA へ適合していることが確認されることになる。最終的には、2027 年 11 月までに義務的要件を満たすよう、関係各所が取り組みを進めるスケジュールとなっている。

(8) EUCC 実施規則の修正と CSA 改正

EUCC（EU Cybersecurity Certification Scheme on Common Criteria）※133 は ICT 製品（ハードウェア・ソフトウェア・ファームウェア）のセキュリティ認証制度であり、EU 統一の制度として「EU サイバーセキュリティ法（CSA：The EU Cybersecurity Act）※134」により導入され、2024 年 1 月 31 日に採択された実施規則※135 において具体的な運用詳細が定められた。細目としては、CSA で規定された三つの保証レベル（基本・実質的・高度）のうちの実質的・高度の二つの保証レベルの詳細な定義、認定された適合性評価機関による認証プロセス、証明書の様式、認証後の脆弱性管理等を明確化した。これにより、EUCC が実際に運用可能な認証制度となった。

CRA と EUCC は相補的な関係にある。CRA が ICT 製品に限らない広範なデジタル製品のライフサイクル全般に安全要件を義務として課すのに対して、EUCC は CSA に基づく ICT 製品の認証制度であり、取得は原則として任意である。CRA が市中の製品に広く最低限の安全基準遵守を義務付けるのに対し、EUCC は製品セキュリティの高さを証明したい場合の標準的手段を提供する。

EUCC の実施規則は細部の調整を含む修正案※136 が 2024 年 12 月 18 日に改めて採択され、2025 年 1 月 18 日より修正後の内容で施行されている。2027 年 2 月には既存の加盟国内標準から EUCC への移行措置が期限を迎え、EUCC の全面運用が確立する予定である。

EUCC とは適用範囲が異なるが、2024 年 12 月 19 日には CSA の改正案※137 が採択され、マネージドセキュリティサービスが CSA で規定されているサイバーセキュリティ認証フレームワークの対象に加わることとなった。なお、EUCC はサイバーセキュリティ認証フレームワークの中で具体化された制度の一つであり、サービスではなく ICT 製品を対象としている。

CSA 改正法は 2025 年 2 月 4 日より施行されているが、認証制度の具体化に先立ち実施規則等の策定といった段階を経る必要があり、認証制度が本格的に運用開始となる日程はまだ明確になっていない。

4.1.4 中国の政策

中華人民共和国（以下、中国）では 2021 年～ 2025

年を対象期間とした「第 14 次五ヵ年計画」が 2021 年 3 月に全国人民代表大会（全人代）で承認された※138。中国は、サイバーセキュリティにおける安全保障問題、ビジネスにおいて収集・生成される膨大な電子データの価値、サイバーリスクを認識し、同計画の期間を通じてサイバーセキュリティ分野の法律及び法令の整備を着々と進めてきた。本項では、中国のサイバーセキュリティに関する計画、法令、規則等について概説する。

(1) 第 14 次五ヵ年計画

「第 14 次五ヵ年計画」は全 19 編 65 章からなり、中国の国民経済及び社会発展に必要な要素が記載されており、これに基づき各担当部局、地方行政機関が計画の実現に向け、具体的なプロジェクトの策定を進める※139。同計画における、サイバーセキュリティ分野の記述は、第 5 編「デジタル化発展の加速、デジタル中国の建設」内の第 18 章「良好なデジタル・エコシステムの創出」にある。具体的には第 3 節「ネットワークセキュリティ保護の強化」、第 4 節「サイバー空間における運命共同体の構築の推進」が該当する。第 3 節には、ネットワークセキュリティに関する法律・法規及び制度標準の整備、重要分野のデータ・ネットワーク・情報システムのセキュリティ強化、重要インフラ設備の構築、ネットワークセキュリティのリスク評価・審査の強化、ネットワークセキュリティのインフラ設備の建設、脅威の検知・監視の対応強化等、多岐にわたる要素が盛り込まれている。第 4 節では、サイバー空間における国際交流と協力の推進、データセキュリティ、デジタル通貨、デジタル税等の国際規則等の制定に積極的に関与するとある※140。

(2) データ三法

中国ではサイバーセキュリティ分野の基本法である「中華人民共和国サイバーセキュリティ法」が 2017 年 6 月 1 日に施行されて以降、「中華人民共和国データセキュリティ法」が 2021 年 9 月 1 日、「中華人民共和国個人情報保護法」が同年 11 月 1 日に施行され、同分野の関連法令の整備も 2021 年ごろまでに相次いで整備され、規制が厳格化された※141。これら三つの法律は「データ三法」と呼ばれている。中国域内でビジネスを行う事業者、個人にも影響がある。

(a) データ越境移転の促進及び規範化に関する規定

データ三法において、重要データ※142 を国外へ越境移転するには、データ取り扱い者が当局による安全評価への合格を得ることが必須であると定められている。安全評価を得るには、57 営業日かかるという。また個人情報の越境移転の場合は、当局による安全評価への合格以外にも、専門機関による認証の取得、個人情報取り扱い者と当該個人情報の受領者間の標準契約の締結・届出、これら三つのうち一つを事前に充足させておく必要があった。その上で、越境移転について、対象の個人に対し、越境移転の詳細の告知及び同意を個々に得て、更に個人情報取り扱いの目的、方法等の合法性、正当性、必要性、個人の権益への影響等、影響評価を行う必要があり、その手続きの負担は軽微とは言えないものであった。こうした状況を受け、データセキュリティ及び個人情報の権益を保護し、法に基づく秩序正しいデータの自由な流通を促進することを目的に、国家インターネット情報弁公室（Cyberspace Administration of China：CAC）が「データ越境移転の促進及び規範化に関する規定」を発布し、2024 年 3 月 22 日に施行した。一方、重要データについては取り扱うデータが重要データに該当するのか不透明であることが指摘されていたが、当局が重要データに該当する旨を公開、発表していなければ、該当しないと見なすことができることになったという※143。また、同規定の施行に合わせて「データ越境移転セキュリティ評価申告ガイドライン」と「個人情報越境移転標準契約届出ガイドライン」第二版が公表された。

(b) ネットワークデータ安全管理条例

「ネットワークデータ安全管理条例」はデータ三法に基づく行政法規レベルの規定であり、国務院から公布され、2025 年 1 月 1 日から施行された。個人情報や重要データを含むあらゆるネットワークデータの取り扱いと監督管理に関してデータ三法に対し補足、強調を行い、原則的な規定の詳細化等を図ったものである。適用の対象は中国国内におけるネットワークデータの取り扱い行為である※144。国外の取り扱いについては国家の安全、個人・組織の権益を脅かす場合において、域外適用される。

(3)「データ要素×」3 ヵ年計画

2024 年 1 月 5 日、中国国家データ局等 17 部門により「『データ要素×』3 ヵ年計画」が発表された。2026 年末までに製造、農業、商業・貿易・流通、交通輸送、金融サービス、科学技術イノベーション、文化・観光、医療・ヘルスケア、緊急対応管理、気象サービス、都市ガバナンス、グリーン・低炭素の 12 分野において、データの活用シーン、活用方法を明確にし、データ活用を拡大・

推進するとした。加えて、地方の積極的なデータ活用や新たな実証事例の創出を奨励するために、各部門、各地方が連携し、重点産業・分野においてデータリソースの所有権やデータ加工使用権、データ製品運用権等を分離させる政策の導入を検討するという※145。

(4) 産業分野におけるデータセキュリティ能力の向上に関する実施計画(2024年～2026年)

2024年2月26日、中国工業情報省が発表した「産業分野におけるデータセキュリティ能力の向上に関する実施計画(2024年～2026年)」は製造業のデータ保護、データセキュリティの規制、データセキュリティ産業の支援を向上させるために11の実施項目を指定したものである※146。また、中国工業情報省は、リスクの自己点検と自己是正を強化し、的確な管理と予防措置を取るという。予防措置として具体的には、ランサムウェア攻撃を想定した訓練等を2026年末までに産業セクターの4万5,000社以上に適用するという※147。

(a) 工業及び情報化分野データセキュリティリスク評価実施細則(試行)

工業情報化部が公布し2024年6月1日に施行された「工業及び情報化分野データセキュリティリスク評価実施細則(試行)」は工業及び情報化分野の重要データ及び中核データのデータ取り扱い者による規範的なデータセキュリティリスク評価作業について記載されたものである。具体的には、データセキュリティリスク評価の実施、評価報告書の作成と評価結果への責任を負うこと、少なくとも年1回はリスク評価を行うこと、評価は自らの実施、あるいは第三者評価機構に依頼してもよく、評価報告書は評価完了後10営業日以内に主管機関に提出し、審査を受けなければならないこと等が記載されているという※148。

(b) GB/T 43697-2024 データセキュリティ技術 データの分類と等級区分の規則

2024年10月1日に施行された「GB/T 43697-2024 データセキュリティ技術 データの分類と等級区分の規則」は重要データの該当性判断を含むデータの分類、等級に関するルールの明確化に着手したものである。事業者は以前に比べ、同規則の規定に基づいて分類、等級付けを行うことが容易になったと考えられる※149。なお、同規則は国家市場監督管理総局／国家標準化管理委員会が運営する国家標準全文公開系統で公表されている※150。

(5) 国家秘密保護法の改正

1988年に制定され、2010年に改正された国家秘密保護法は14年ぶりに再改正され、2024年5月1日に施行された。改正の背景には国内外の情勢の変化、科学技術の急速な発展等により、機密保護が新たな問題や課題に直面していることがあるという。今回の改正ではサイバー情報機密保護・管理制度が更に整備された※151。改正内容の一例を挙げると、中国の組織等が国外の組織等に国家秘密を提供する場合や国外の人員が業務上の必要性から国家秘密を知った場合には規定に基づいた手続きが必要になった。また、国家秘密に関わった職員は離任、離職後も「秘密離脱期間」管理を行い、期間内の就業、出国を制限し、同期間終了後も秘密保持義務を負うこととされた※152。その後、2024年9月1日には国家秘密保護法実施条例が施行された。条例では、政府が例外を認めない限り、国家機密を扱う組織の担当者は中国国民でなければならないとされた。また共産党中央と政府機関すべてに秘密保持事務所の設置、指定されたスタッフの配置が義務付けられた。各作業部門では国家機密リストを作成し、部門のトップが機密業務の責任を負うことになった。また、機密情報を取り扱う担当者が域外に出る場合、事前に承認と研修の受講が必要であるという※153。

4.1.5 アジア太平洋地域でのCSIRTの動向

2024年度も、ランサムウェアや不正アクセス等のサイバー攻撃による情報漏えい、システムの一時停止、取引先への影響等の被害が世界中で発生しており、アジア太平洋地域においても深刻な脅威となっている。こうした攻撃による被害を防ぐための対策情報の共有や、被害後の復旧支援等、インシデント対応連携の窓口となる各国のNational CSIRT（以下、CSIRT）が果たす役割は大きく、対応の迅速化や情報連携強化のための取り組みが進んでいる。また、法令でCSIRT及び所管省庁の役割を明文化し、権限を付与することにより、インシデント対応の円滑化に取り組む動きも継続して見られる。

本項では、主に2024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)シンガポール

シンガポールにおいて「サイバーセキュリティ法 2018」が改正され「サイバーセキュリティ法 2024(Cybersecurity (Amendment) Act 2024)」として施行された※154。

今回の改正では、サイバー脅威の高まりや、クラウドコンピューティング等の運用環境の技術的変化へ対応するため、同法の適用対象の拡大や、重要情報インフラのサイバーセキュリティ保護の強化、監督機関であるCSA(Cyber Security Agency of Singapore:シンガポールサイバーセキュリティ庁)の権限強化等を行っている。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。

まず同法では、適用対象についてコンピューター及びコンピューターシステムの定義を拡大し、従前の物理的システムに加えて、仮想コンピューター、仮想コンピューターシステムが追加された。重要情報インフラのサイバーセキュリティ保護の強化については、重要サービス提供事業者は自社のシステムだけでなく、使用している第三者所有の重要情報インフラのサイバーセキュリティの管理と保護に対しても責任を負うことが定められた。具体的には、第三者所有のシステムがサイバーセキュリティ基準を満たすよう、そのシステム所有者と契約等の法的拘束力のある公約(コミットメント)を確立することを求めている。更に、同法は重要サービス提供事業者以外に、次の三つのシステム及び事業体を規制対象とし、それぞれに対しサイバーセキュリティ基準・ルール等を定め、規制の遵守やインシデント報告義務を課すことを定めている。

- 一時的なサイバーセキュリティ配慮システム(STCC:Systems of Temporary Cybersecurity Concern):大規模イベントやパンデミック発生時等に一時的にセキュリティリスクが高まるシステムを指す。
- 特別サイバーセキュリティ関心事業体(ESCI:Entities of Special Cybersecurity Interest):機密情報を保有する等、サイバー攻撃者に関心を持たれ、標的となりやすいシステムを使用する団体を指す。
- 基盤デジタルインフラサービス提供者(FDI:Foundational Digital Infrastructure):クラウドコンピューティング及びデータセンター施設・サービスが含まれる。

CSA はこれらの規制対象に対し、サイバーセキュリティの脅威に対して講じるべき措置等について書面による指示を行う権限のほか、セキュリティ検査を行う権限等を持ち、サイバー攻撃への備えを強化するとしている。

(b)マレーシア

マレーシアでは、サイバー脅威への対処とセキュリティ管理等に関する規定を定めた「サイバーセキュリティ法 2024(Cyber Security Act 2024)」が新たに制定され施行された※155。

同法において、サイバーセキュリティの統括組織として、サイバーセキュリティ政策及び戦略を調整する役割を担うNCSC(National Cyber Security Committee:国家サイバーセキュリティ委員会)が設立され、規制と執行の主導的役割を NACSA(National Cyber Security Agency:国家サイバーセキュリティ庁)が担うことが定められた。また、重要情報インフラ分野ごとの実践的セキュリティ対策を規制・管理する NCII セクターリーダー(National Critical Information Infrastructure Sector Lead:国家重要情報インフラセクターリーダー)という役割の設置も定められた。同法の主な適用対象は、11 分野にわたる国家重要情報インフラ事業者(以下、NCII 事業者)及び SOC(Security Operation Center)やペネトレーションテスト等のサイバーセキュリティサービス提供者である。NCII 事業者に対しては、サイバーセキュリティ対策、リスク評価、監査の実施やインシデント報告等の義務を課しており、リスク評価を毎年実施し、少なくとも 2 年に 1 回は監査を実施するよう求めている。また、サイバーセキュリティインシデントが発生した際は、NACSA 及び NCII セクターリーダーに報告することを義務付け、インシデント発生時の NCII 事業者の対応の強化を図るとしている。サイバーセキュリティサービス提供者に対しては、サイバーセキュリティサービスの提供を許可する免許の取得を義務付けた。同法に違反した場合の罰則も設けており、重要情報インフラ事業者のセキュリティ対策における意識向上や、サイバーセキュリティサービスの品質と信頼性の確保を目指している。

(c)ベトナム

ベトナムでは、2024 年 3 月下旬以降、オンライン証券会社 VNDIRECT、ガソリンスタンドチェーン PVOIL 等の大手企業や、通信サービスプロバイダーを標的としたランサムウェア攻撃が相次いで発生しており、社会経済活動に深刻な影響を及ぼすリスクが高まっていることが懸念されている。こうした状況の背景には、政府が進め

てきたサイバーセキュリティ規制等の対策強化の取り組みが、一部の分野の企業で効果的に実施されていない状況や、所管省庁の指導及び管理が行き届いていない等の課題があると現地メディアが指摘している※156。

上記の状況を踏まえ、2024年4月7日、ベトナムのPhạm Minh Chính首相は、政府省庁及び地方自治体等にサイバーセキュリティ対策の強化を促す指令を発出した※157。

同指令では、情報通信省の指導のもと、各省庁、地方自治体等に対し、政府機関及び管轄組織の情報システムのサイバーセキュリティ対策状況の点検と評価を指定された期限までに行い、安全基準を厳格に遵守することを求めている。また、サイバー攻撃やサイバーセキュリティインシデントが発生した場合には、所管省庁や国の調整機関、インシデント対応専門機関に速やかに報告することや、関連機関の指示に従い、情報を収集・分析し、発生源の追跡や原因の検証を行い、インシデントへの対処に官民が連携して取り組むことを求めている。このインシデント対応専門機関は、VNCERT/CC（Vietnam Computer Emergency Response Team：ベトナムサイバーセキュリティ緊急対応チーム）を指していると推察される。更に、サイバー空間における脅威を監視、検出し、迅速に対応するためには、公安省及び国防省との連携が重要であるとして、各省庁が協力して取り組むよう指示している。

(d)オーストラリア

2024年8月22日、オーストラリアのASD及びCSIRTの機能を担うACSCが主導し、パートナー国（日本、オーストラリア、米国、英国、カナダ、ニュージーランド、シンガポール、韓国、オランダの9ヵ国）と協力して策定した文書「イベントログと脅威検知のためのベストプラクティス（Best practices for event logging and threat detection※158）」が公開された。

同文書は、昨今検出の困難なLiving off the Land戦術を用いる悪意のあるアクターが増えており、イベントログの重要性が高まっているとして、経営層のIT責任者やネットワーク運用者に向けて、イベントログと脅威検知に関するベストプラクティスを紹介している。Living off the Land戦術とは、攻撃者が標的とするシステムへの侵入に成功した後に、マルウェアを使用せず、システムに組み込まれている正規ツール等を用いて、認証情報の窃取、システム情報の収集等の不正な活動を行う攻撃手法である。イベントログのベストプラクティスでは、考慮すべき四つの要点として「イベントログポリシーの策定と実装」「ログ収集における優先順位付け」「安全性の高いストレージとイベントログの完全性の確保」「関連する脅威の検知戦略の検討」を挙げ、それぞれ対策を詳述している。

同文書の共同発行組織には、上記パートナー国のサイバーセキュリティを管轄する政府機関及び関連組織が名を連ねている。日本からは、NISCとJPCERT/CCが署名に加わった。

ACSCは同文書以外にも、重要インフラ事業者に向けて策定した文書「OTサイバーセキュリティの原則（Principles of operational technology cybersecurity※159）」をパートナー国と協力して10月に公開しており、サイバー空間における脅威に対するセキュリティ対策意識と対処能力向上を目的とした国際協調を促進している。

(e)インド

インドのMeitY（Ministry of Electronics and Information Technology：電子情報技術省）傘下のCERT-In（Indian Computer Emergency Response Team：インドコンピューター緊急対応チーム）とISAC（Information Sharing and Analysis Center：情報共有分析センター）は協力して、国家のサイバーセキュリティを保護する専門家を育成するプログラムNCSSP（National Cyber Security Scholar Program：国家サイバーセキュリティ教育プログラム）を提供している※160。

同プログラムは、サイバーセキュリティを保護する上で必要な知識や技術、管理能力、倫理観、チームビルディング等包括的なスキルを身に付けるトレーニングを、一定の基準を満たすサイバーセキュリティ従事者に提供することで、国や企業のデジタルインフラ及び資産をサイバー脅威から守る次世代リーダーを育成することを目指している。例えば、重要インフラの保護に関するカリキュラムでは、空港や発電所、データセンター等、様々な重要情報インフラ施設を訪問し、各業界が直面しているデジタル化の課題やセキュリティリスクについて現場から学ぶ機会を提供している。また、実践的なトレーニングとして参加者は、攻撃者やSOCチーム、フォレンジック担当者、CISO、CEO等、様々な関係者の役割を担い、サイバー危機を想定したインシデント対応を行う机上演習に取り組む。同演習を通じて、参加者は多様な利害関係者の視点について理解を深め、サイバーセキュリティの意思決定がもたらす経済的影響やリスク管理の重要性について貴重な洞察を得ることができるとしている。2024年は

第 6 期生のトレーニングを行った。

このように、インドでは政府と各業界のサイバーセキュリティ組織が協力し、国家のサイバーレジリエンス能力向上を主導する人材育成に力を入れて取り組んでいる。

(2) アジア太平洋地域の CSIRT 間連携

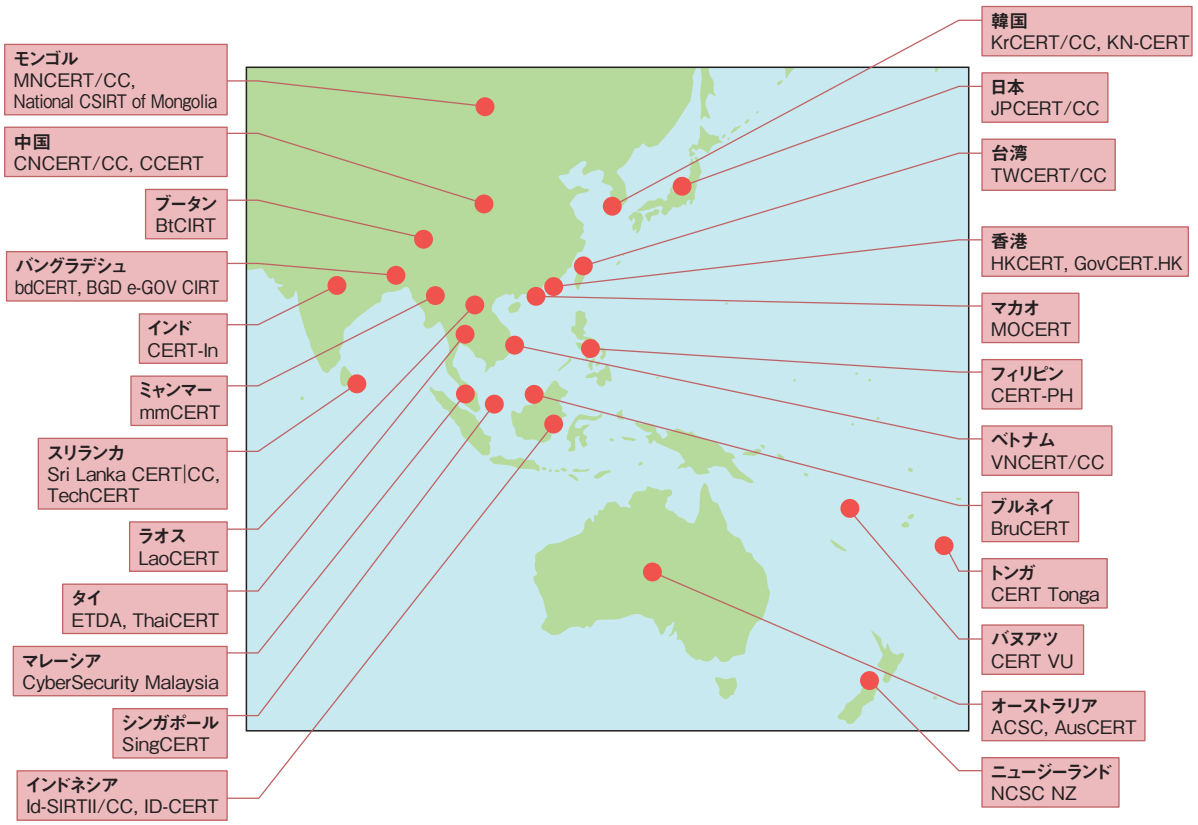
アジア太平洋地域全体の CSIRT からなるコミュニティとして、APCERT（Asia Pacific Computer Emergency Response Team：アジア太平洋コンピューター緊急対応チーム）[※161] があり、地域内で発生したインシデント対応における連携の円滑化や、サイバー脅威等に関する情報共有・技術交流の推進を目的に活動している。2003 年の設立当初、参加メンバーは 12 の国・経済地域の 15 チームだったが、地域内で CSIRT の立ち上げが進んだことや、CSIRT コミュニティへの参加を通じた情報共有等の重要性が高まったことから年々メンバーが増えている。2025 年 3 月末現在、24 の国・経済地域の 33 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 4-1-1）。

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。

2024 年のサイバー演習は、「APT Group Attack Response: Where is Wally?（APT グループ攻撃への対応）」をテーマに実施された[※163]。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 22 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[※164]。2024 年の APCERT 年次会合は、2019 年以来 5 年ぶりの対面にて 11 月に台湾の台北市で開催された。会合では、韓国の KrCERT/CC[※165] が議長に再選され、オーストラリアの ACSC が新たに副議長に選出された。また、中国の CNCERT/CC[※166] と KrCERT/CC、台湾の TWCERT/CC[※167]、ACSC 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、電話会議システムを利用して、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



■図 4-1-1　APCERT オペレーショナルメンバー（2025 年 3 月末現在）
（出典）APCERT「Member Teams[※162]」を基に IPA が編集

携については、ASEAN Regional CERT（ASEAN Regional Computer Emergency Response Team：ASEAN 地域コンピューター緊急対応チーム）の運用に関する議論が進んでいる。例えば、2024 年 8 月に、同組織のタスクフォース初会合がシンガポールで開催され、ASEAN 加盟国間の情報共有の促進や同地域におけるサイバーセキュリティ演習の実施等、ASEAN Regional CERT の運用における八つの主な目的を実行するための議論が行われた※168。また、2024 年 10 月 16 日にシンガポール国際サイバーウィーク（SICW：Singapore International Cyber Week）の一環として開催された「第 9 回 ASEAN サイバーセキュリティ閣僚会議（AMCC：ASEAN Ministerial Conference on Cybersecurity）」において、ASEAN Regional CERT の物理的施設の開所が発表された。同施設はシンガポールの ASCCE（ASEAN-Singapore Cybersecurity Centre of Excellence）に併設され、今後サイバー脅威や攻撃、オンライン詐欺に関する ASEAN 加盟国間の情報共有を大幅に前進させるとしている。また、サイバー演習、ワークショップ、CERT 間のサイバー能力構築プログラム等の対面活動のための専用スペースとして使用される予定である。

このように、アジア太平洋地域の各国個別による CSIRT 活動の機能強化に加えて、APCERT や ASEAN 等の地域横断的な団体も、CSIRT の活動を後押しする取り組みを継続して進めている。ここに挙げたようにアジア太平洋地域の CSIRT コミュニティが連携して、サイバーセキュリティ能力向上施策に継続して取り組むことにより、地域全体のサイバーセキュリティ対応能力の確保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、日本の標準化活動の取り組み、及び 2024 年のセキュリティ分野の国際標準化の動きとして ISO/IEC JTC 1/SC 27 と IEC TC 65/WG 10 の活動を紹介する。

4.2.1 様々な標準化団体の活動

国際標準の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、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 等の国家規格が該当し、これらには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、業界ルール等の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。これらは、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主な国際標準化団体の概要を述べる。

まず、デジュール標準を策定する代表的な組織としては、以下がある。

- 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)※169:
  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※170。
- 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※171、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※172。標準化した技術文書はRFC（Request For Comments）として参照できる。

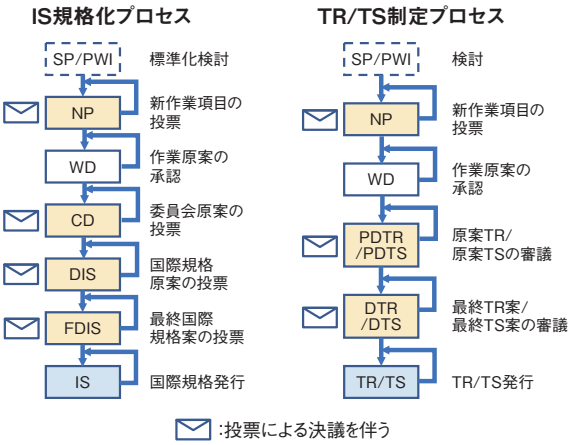
- TCG（Trusted Computing Group）：
  信頼できるコンピューティング環境（埋め込み機器、パソコン／サーバー、ネットワーク等）に関するセキュリティ技術の標準化を行う業界団体である。ハードウェア、ソフトウェア等のベンダーやシステムインテグレーターがメンバーとなり、中国、日本にRegional Forum（地域支部）がある※173。

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※174（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する。



■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※175」を基にIPAが作成

図4-2-1の各文書の段階と略号は以下のとおりである。

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：新作業項目（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。

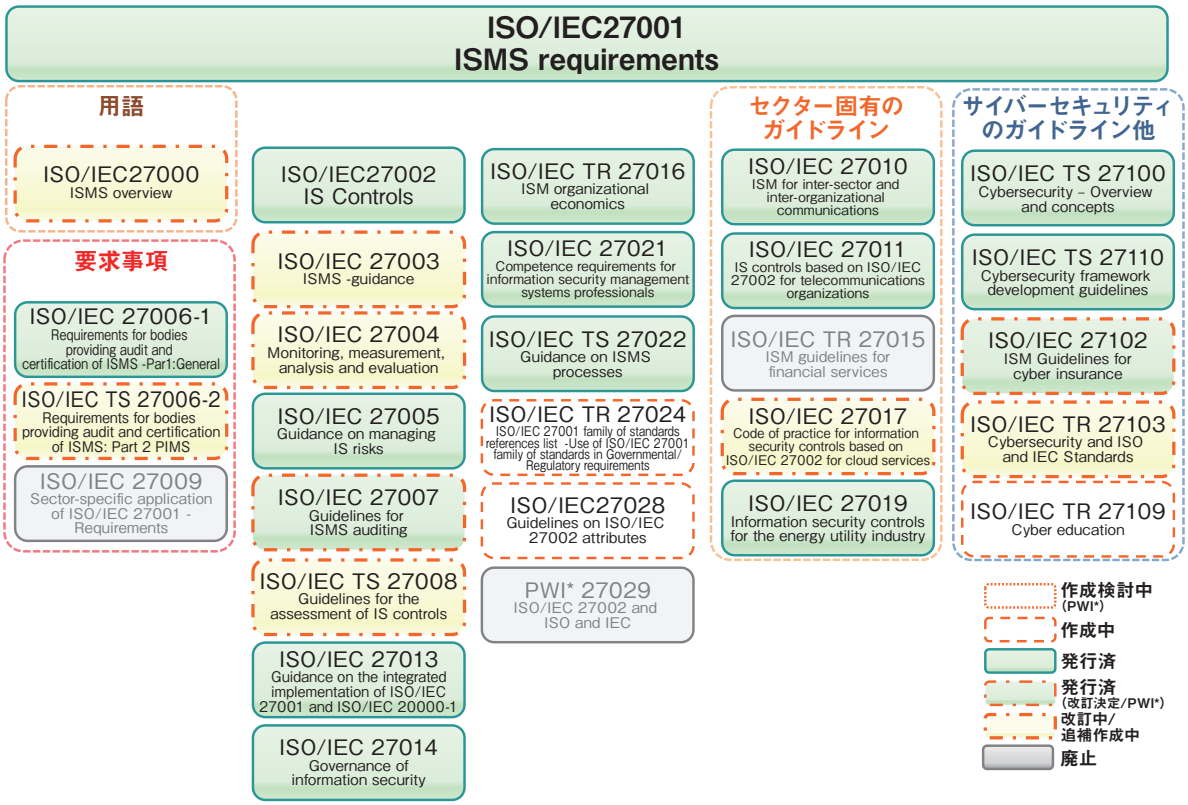
（1）WG 1（情報セキュリティマネジメントシステム）

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を特定の技術分野（例えばクラウドサービス）や特定の業界（例えば電力）に適用するための規格、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（次ページ図4-2-2）。

2022年には、ISO/IEC 27001の本文とISO/IEC 27002の構成の大きな変更を伴う改訂が行われた。この改訂に伴い、これら規格を引用、参照している規格には見直しが発生している。ISO/IEC 27001ファミリーの改訂状況は以下のとおりである。

ISO/IEC 27019（エネルギー業界のための情報セキュリティ管理策）は、2024年10月に発行された。

ISO/IEC 27013（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－ISO/IEC 27001及びISO/



* 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）。
※ISO/IEC TS 27006-2 は、SC 27/WG 5 のプロジェクトとして登録されていますが、SC 27/WG 1 と合同で策定され、ISO/IEC 27006 の第 2 部（Part 2）であるため記載している。

■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[※176]」を基に IPA が編集

IEC 20000-1 の統合的実施の手引）については、追補版が 2024 年 12 月に発行された。

サイバーセキュリティに関するガイドラインである ISO/IEC TR 27103（サイバーセキュリティと ISO 及び IEC 規格）は DTS の段階である。

また、現在 DIS として、次の二つの規格の審議が進められている。

- ISO/IEC 27000（ISMS 概要）
  今回の改訂において、ISO/IEC 27001 関連規格の用語定義を削除し、表題も「情報セキュリティマネジメントシステム－概要及び用語」から、「情報セキュリティマネジメントシステム－概要」へ変更した。ISMS 及び ISMS 規格の概要を提供する規格として改訂中である。
- 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の実践の規範）
  ISO/IEC 27002:2022 との整合を図るため、最近のクラウド動向等に対応して管理策、手引きを更新するために改訂中である。

(2) WG 2（暗号とセキュリティメカニズム）

WG 2 では、暗号プリミティブ（暗号アルゴリズム）や、デジタル署名技術、鍵共有のような汎用的かつ基本的な暗号プロトコル等の標準化を行っている。

2024 年 7 月 1 日から 2025 年 6 月 30 日の間に、発行された規格は以下のとおりである。

- ISO/IEC 23264-2:2024
  Information security — Redaction of authentic data — Part 2: Redactable signature schemes based on asymmetric mechanisms
- ISO/IEC 20008-3:2024
  Information security — Anonymous digital signatures — Part 3: Mechanisms using multiple public keys
- ISO/IEC 18031:2025
  Information technology — Security techniques — Random bit generation
- ISO/IEC 18014-1:2008/Amd 1:2025
  Information technology — Security techniques — Time-stamping services — Part 1: Framework —

Amendment 1
- ISO/IEC 18014-2:2021/Cor 1:2024
  Information security — Time-stamping services — Part 2: Mechanisms producing independent tokens — Technical Corrigendum 1
- ISO/IEC 11770-3:2021/Amd 1:2025
  Information security — Key management — Part 3: Mechanisms using asymmetric techniques — Amendment 1: TFNS identity-based key agreement
- ISO/IEC 9797-2:2021/Cor 1:2024
  Information security — Message authentication codes（MACs）— Part 2: Mechanisms using a dedicated hash-function — Technical Corrigendum 1

NP 提案として、「付随情報付きデジタル署名 - 第 5 部：格子ベースのメカニズム（ISO/IEC 14888-5）」「付随情報付きデジタル署名 - 第 6 部：ステートレスハッシュベースのメカニズム（ISO/IEC 14888-6）」「サイドチャネル攻撃からハードウェア内の対称アルゴリズムを保護するアルゴリズミックメカニズム（ISO/IEC 25888）」の三つが提出された。ISO/IEC 14888 は、デジタル署名の規格であり、量子計算機を用いた攻撃にも耐性がある格子ベースとステートレスハッシュベースのメカニズムの標準化が提案されている。

また、IEEE Computer Society（CS）から耐量子計算機暗号技術とプライバシー保護計算について、ISO/IEC JTC 1/SC 17/WG 3 から耐量子暗号技術のためのデジタル署名を ISO/IEC 標準に含めることについて、それぞれリエゾンステートメント（連絡文書）を受け取った。

（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。

「IT セキュリティ評価及び認証制度（JISEC）」でも参照している ISO/IEC 15408、ISO/IEC 18045 は 2022 年に発行されているが、改訂版の検討が進んでおり、現在 DIS 発行に向けて議論が継続している。

直近では、2025 年 2 月に以下の二つが発行された。
- ISO/IEC 19790:2025
  Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules
- ISO/IEC 24759:2025
  Information security, cybersecurity and privacy protection — Test requirements for cryptographic modules

WG 3 は SC 42[※177] と協力して AI に関する標準化活動に関する議論を実施しており、その結果を基に WG 3 において AI のセキュリティ評価を実施するための新規標準の提案を行っている。

（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。

日本が提案及び関与している ISO/IEC 27404、ISO/IEC TS 5689 の状況は以下のとおりである。
- ISO/IEC 27404
  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。DIS の段階で追加的な修正を行い、現在は FDIS に移行する段階にある。
- ISO/IEC TS 5689
  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）」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、3rd WD に対するコメントの審議結果を受けて、DTS のためのドラフト作成を完了した段階にある。DTS に関するコメントの審議は、次回の SC 27 会合（2025 年 9 月）を予定している。

（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 27562（Privacy guidelines for fintech services）を 2024 年 12 月に発行した。

ISO/IEC 24760-1, 2, 3（A Framework for identity

management: Parts 1-3）の三つについては 2025 年 5 月現在発行準備中である。

また、以下の三つのプロジェクトが FDIS の段階に進んでいる。

- ISO/IEC 27701 (ed. 2)
  Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance
- ISO/IEC 27553-2：2025
  Information security, cybersecurity and privacy protection — Security and privacy requirements for authentication using biometrics on mobile devices — Part 2: Remote modes
- ISO/IEC 27018 (ed. 3)
  Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors

また、ISO/IEC 27701 の審査及び認証を行う機関に対する要求事項を定めている ISO/IEC 27706（Requirements for bodies providing audit and certification of privacy information management systems）は、ISO/IEC 27701 の発行直後に発行予定である。

4.2.3 制御システム関連のセキュリティ規格の標準化（IEC TC 65/WG 10）

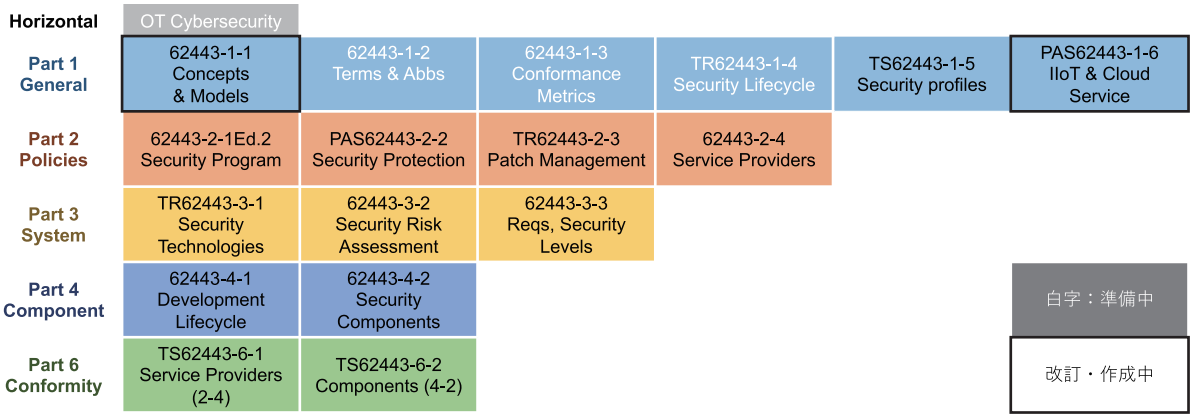
近年の制御システムは、情報システム同様にネットワーク化やオープン化（標準プロトコル・汎用製品の利用）が進んだことで、サイバー攻撃の脅威に晒されるようになった。こうした動向に伴い、制御システムにおいてもリスク分析に基づくセキュリティ対策が喫緊の課題となっており、日米欧各国の政府機関・業界団体が取り組みを進めている。本項では制御システムのセキュリティの国際標準について述べる。

(1) ISA/IEC 62443 シリーズの概要

制御システムのセキュリティを包括的に網羅した国際標準「工業通信ネットワーク－ネットワーク及びシステムセキュリティ（ISA/IEC 62443）」は、ISA（International Society of Automation：国際自動制御学会）99 Committee[※178] と IEC Technical Committee 65 Working Group 10（TC 65/WG 10）[※179] により作成されているため、ISA/IEC 62443-X-Y と記載される。

ISA/IEC 62443 は大別して五つのグループに分類され、発行済みと策定・準備中のものを合わせて 17 の規格が存在する（図 4-2-3）。

ISA/IEC 62443 は、産業制御システムをサイバー攻撃から守るために開発された。規格の議論を始めた 2002 年ごろは、市販 OS や汎用プロトコルが狙われやすいとして、それらの対策方針について検討された。しかし、2011 年になって各社独自技術を用いた制御システムやコントローラーがサイバー攻撃を受けるようになったため[※182]、制御システム全般のサイバー脅威への基本的概念から、分析と対策の手順、マネジメントや機器機能等まで、幅広い要求を扱うようになった。同規格を参照して、鉄道や機械等の分野規格の開発も進んでおり、産業システムのサイバーセキュリティの基本規格として位置付けられている。



■図 4-2-3　ISA/IEC 62443 シリーズ文書の発行・改定状況（概要）
（出典）星野浩志、藤田淳也、神余浩夫「IEC 62443 制御システムセキュリティ規格の現状[※180]」（「制御システムセキュリティカンファレンス 2023[※181]」講演資料）を基に執筆者が更新

(2) 各グループの概要と状況

ISA/IEC 62443 のグループごとの概要や 2024 年度の検討状況について紹介する。

(a) ISA/IEC 62443-1 グループ(一般)

ISA/IEC 62443 の中で用いられる用語の解説や、制御システムのセキュリティ動向、地理的に分散したフィールド機器を遠隔から集中監視制御する SCADA[※183] モデルの一般論等を規定している。このグループは、事業者やシステムインテグレーター、機器ベンダー等、すべての関係者が共通して参照する規格である。「TS 62443-1-1 概念とモデル」の国際標準(IS)化、及び「1-6 IIoT とクラウドサービス」の策定が進んでいる。

(b) ISA/IEC 62443-2 グループ(ポリシーと手順)

事業者や運用者等の組織を対象とした、主にマネジメントに関連するセキュリティ要求事項等を規定した規格であり、組織としてのセキュリティマネジメントシステムの確立や、パッチ管理等の運用に関連する事項が記載されている。「2-1 制御システム設備オーナーへの要求」の第 2 版が 2024 年 8 月に、「2-2 IACS セキュリティ保護スキーム」が 2025 年 3 月に発行された。

(c) ISA/IEC 62443-3 グループ(システム)

複数の機器や製品を組み合わせて運用する制御システムを対象とした規格である。

ISA/IEC 62443-3-3 は、ISA/IEC TS 62443-1-1 で規定される基礎的要求事項(FR:Foundational Requirement)に対応する形で、システムの技術的なセキュリティ要求事項を規定している。要求事項は、システム要件(SR:System Requirement)と強化策(RE:Requirement Enhancement)から構成され、各要求事項にセキュリティレベル(SL:Security Level)が割り当てられている。SL は、それぞれの要求事項を満たした場合に、どのような攻撃からシステムを保護できるかを示すものである。4 段階の SL が規定されており、最も高度な要求事項を満たすものをレベル 4 としている。

(d) ISA/IEC 62443-4 グループ(コンポーネント)

制御システムを構成する個別コンポーネント(機器や装置)を対象とした規格であり、主にコンポーネントのライフサイクルの各フェーズにおけるセキュリティ要求事項や、搭載されるセキュリティ機能等に関する事項が記載されている。

(e) ISA/IEC 62443-6 グループ(コンフォーミティ)

製品等の規格適合性評価の方法を開発する IECEE(IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components)[※184] のワーキンググループから IEC TC 65/WG 10 へ依頼されたことをきっかけに基準作成を行っている。IEC 62443 要件準拠の基準や基準を満たすことのエビデンスの確認方法について具体化している。「6-1 2-4 の評価手法」が 2024 年 3 月、「6-2 4-2 の評価手法」が 2025 年 1 月に発行された。

(3) ISA/IEC 62443 の活用

2024 年度も、様々な業界での ISA/IEC 62443 活用が進展し、電力、化学、石油、ビル、鉄道等におけるセキュリティ標準の開発が進んでいる。また各国での第三者評価・認証(ISASecure[※185]、IECEE の ISA/IEC 62443 関係認証)での活用を見据えての評価認証におけるセキュリティ評価手法の開発も進んでいる。重要インフラや産業システムのサイバーセキュリティ対策は、各国の緊急課題であり、法整備や制度開発が急がれる。

※ 1　日本マイクロソフト株式会社：イランがサイバー対応型影響力工作で 2024 年の米国大統領選挙に干渉　https://www.microsoft.com/ja-jp/security/security-insider/intelligence-reports/iran-steps-into-us-election-2024-with-cyber-enabled-influence-operations〔2025/5/29 確認〕
※ 2　Reuters：米選挙巡る偽情報「前例ない量」、結果に直接影響なし＝当局者　https://jp.reuters.com/world/us/AFLGHM6DAVOARHPNICOSIAZIHQ-2024-11-04/〔2025/5/29 確認〕
※ 3　BforeAI：2024 Paris Olympic Games Infrastructure Attack Report　https://bfore.ai/2024-paris-olympic-games-infrastructure-attack-report/〔2025/5/29 確認〕
※ 4　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 2024.08　https://jp.security.ntt/resources/cyber_security_report/CSR_202408.pdf〔2025/5/29 確認〕
※ 5　France 24：France reports over 140 cyberattacks linked to Olympics　https://www.france24.com/en/live-news/20240814-france-reports-over-140-cyberattacks-linked-to-olympics〔2025/5/29 確認〕
※ 6　トレンドマイクロ株式会社：2024 年パリ・オリンピックに便乗するサイバー犯罪者 ～生成 AI も利用する詐欺の手口とは?～　https://www.trendmicro.com/ja_jp/jp-security/24/g/ico-scams-leverage-2024-olympics-to-lure-victims-use-ai-for-fake.html〔2025/5/29 確認〕
※ 7　ITmedia：「DeepSeek ショック」とは何だったのか?　2025 年、AI 開発の最新事情を解説　https://www.itmedia.co.jp/aiplus/articles/2502/04/news121.html〔2025/5/29 確認〕
※ 8　GPDP：COMUNICATO STAMPA - Intelligenza artificiale: il Garante privacy blocca DeepSeek　https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10097450#english〔2025/5/29 確認〕
※ 9　Personal Information Protection Commission：DeepSeek Temporarily Suspends Its Application Service in Korea　https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2784〔2025/5/29 確認〕
※ 10　独立行政法人日本貿易振興機構（JETRO：Japan External Trade Organization）：米国で TikTok 規制法成立、規制可否は合憲性が焦点に　https://www.jetro.go.jp/biznews/2024/04/3c37773d311c994a.html〔2025/5/29 確認〕
Library of Congress:Text - H.R.815 - 118th Congress (2023-2024): Making emergency supplemental appropriations for the fiscal year ending September 30, 2024, and for other purposes.　https://www.congress.gov/bill/118th-congress/house-bill/815/text〔2025/5/29 確認〕
※ 11　JETRO：TikTok が米国規制法の合憲性審査を求めて米政府を提訴　https://www.jetro.go.jp/biznews/2024/05/43c7ac915b03f92e.html〔2025/5/29 確認〕
TikTok Inc.：Court Filing on TikTok Ban　https://newsroom.tiktok.com/en-us/court-filing-on-tiktok-ban-2024〔2025/5/29 確認〕
※ 12　Bloomberg L.P.：米最高裁が TikTok 禁止法を支持、施行巡るトランプ氏の判断に注目　https://www.bloomberg.co.jp/news/articles/2025-01-17/SQ8NADDWRGG000〔2025/5/29 確認〕
※ 13　Government of Canada：Investment Canada Act　https://ised-isde.canada.ca/site/investment-canada-act/en〔2025/5/29 確認〕
※ 14　Government of Canada：Government of Canada orders the wind up of TikTok Technology Canada, Inc. following a national security review under the Investment Canada Act　https://www.canada.ca/en/innovation-science-economic-development/news/2024/11/government-of-canada-orders-the-wind-up-of-tiktok-technology-canada-inc-following-a-national-security-review-under-the-investment-canada-act.html〔2025/5/29 確認〕
※ 15　JETRO：米商務省、ロシアのカスペルスキーに取引禁止措置、情報通信技術サービス保護規則で初　https://www.jetro.go.jp/biznews/2024/06/735a1f17c0566e90.html〔2025/5/29 確認〕
Federal Register：Final Determination: Case No. ICTS-2021-002, Kaspersky Lab, Inc.　https://public-inspection.federalregister.gov/2024-13532.pdf〔2025/5/29 確認〕
※ 16　Anadolu Agency Turkish Inc.：Denmark urges local firms not to use antivirus programs developed by Russian cybersecurity firm　https://www.aa.com.tr/en/europe/denmark-urges-local-firms-not-to-use-antivirus-programs-developed-by-russian-cybersecurity-firm/3256252#〔2025/5/29 確認〕
※ 17　Australian Government：PSPF Direction Update – Kaspersky Lab, Inc. Products and Web Services　https://www.protectivesecurity.gov.au/news/pspf-direction-update-kaspersky-lab-inc-products-and-web-services〔2025/5/29 確認〕
※ 18　徳島県つるぎ町立半田病院：コンピュータウイルス感染事案有識者会議調査報告書　https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf〔2025/5/29 確認〕
※ 19　名古屋港運協会、名古屋コンテナー委員会、ターミナル部会：NUTS システム障害の経緯報告　https://meikoukyo.com/wp-content/uploads/2023/07/0bb9d9907568e832da8f400e529efc99.pdf〔2025/5/29 確認〕
※ 20　日本経済新聞：ランサム集団、ウイルス開発者逮捕　国際連携で成果　https://www.nikkei.com/article/DGXZQOUE0136K0R01C24A0000000/〔2025/5/29 確認〕
日経クロステック：国際サイバー犯罪集団「ロックビット」摘発、メンバー 2 人を逮捕　https://xtech.nikkei.com/atcl/nxt/news/24/00289/〔2025/5/29 確認〕
※ 21　Europol：Law enforcement disrupt world's biggest ransomware operation　https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation〔2025/5/29 確認〕
※ 22　FBI：International Investigation Leads to Shutdown of Ransomware Group　https://www.fbi.gov/contact-us/field-offices/cleveland/news/international-investigation-leads-to-shutdown-of-ransomware-group〔2025/5/29 確認〕
※ 23　United Nations：United Nations Convention against Cybercrime Chapters　https://www.unodc.org/unodc/en/cybercrime/convention/convention-against-cybercrime-chapters.html〔2025/5/29 確認〕
外務省：サイバー犯罪に対する国際社会と日本の取組　https://www.mofa.go.jp/mofaj/gaiko/soshiki/cyber/index.html〔2025/5/29 確認〕
※ 24　United Nations：United Nations Convention against Cybercrime　https://www.unodc.org/unodc/en/cybercrime/convention/home.html〔2025/5/29 確認〕
※ 25　https://www.npa.go.jp/bureau/cyber/pdf/20240515_english.pdf〔2025/5/29 確認〕
※ 26　NISC、警察庁：人権保護や民主主義の推進に関与する組織や個人のためのサイバー脅威緩和に関する国際ガイダンスへの共同署名について　https://www.nisc.go.jp/pdf/press/press_Mitigating_Threats.pdf〔2025/5/29 確認〕
※ 27　https://www.cyber.gov.au/sites/default/files/2024-07/apt40-advisory-prc-mss-tradecraft-in-action.pdf〔2025/5/29 確認〕
NISC：APT40 に関するアドバイザリー　https://www.nisc.go.jp/pdf/policy/kokusai/Provisional_Translation_JP_APT40Advisory.pdf〔2025/5/29 確認〕
※ 28　NISC、警察庁：豪州主導の APT40 グループ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.nisc.go.jp/pdf/press/press_APT40Advisory.pdf〔2025/5/29 確認〕
※ 29　NISC：英国主導の「サイバーセキュリティ人材に関する国際的な連合」への参画について　https://www.nisc.go.jp/pdf/press/2025_International_Coalition_on_Cyber_Security_Workforces.pdf〔2025/5/29 確認〕
GOV.UK：International Coalition on Cyber Security Workforces　https://www.gov.uk/government/publications/international-coalition-on-cyber-security-workforces〔2025/5/29 確認〕
※ 30　外務省：第 9 回日米サイバー対話の開催　https://www.mofa.go.jp/mofaj/press/release/pressit_000001_00828.html〔2025/5/29 確認〕
※ 31　外務省：第 3 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_01135.html〔2025/5/29 確認〕
※ 32　外務省：第 8 回日英サイバー対話の開催（結果）　https://www.mofa.go.jp/mofaj/press/release/pressit_000001_01161.html〔2025/5/29 確認〕
※ 33　NISC、総務省、経済産業省：第 17 回 日 ASEAN サイバーセキュリティ政策会議の結果　https://www.nisc.go.jp/pdf/press/17thAJCPM_ja.pdf〔2025/5/29 確認〕
※ 34　外務省：第 6 回日・EU サイバー対話の開催（結果）　https://www.mofa.go.jp/mofaj/press/release/pressit_000001_01382.html〔2025/5/29 確認〕
※ 35　外務省：第 1 回日リトアニアサイバー協議の開催（結果）　https://www.mofa.go.jp/mofaj/fp/es/pagew_000001_00934.html〔2025/5/29 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/2024/11/20241115001/20241115001.html〔2025/5/29 確認〕
※ 37　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〔2025/5/29

確認〕
※ 38 JICA:日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）における第 1 回研修オープニングセレモニー:ASEAN 各国のサイバーセキュリティ専門人材の育成に貢献 https://www.jica.go.jp/information/press/2023/20230619_42.html〔2025/5/29 確認〕
※ 39 AJCCBC：ABOUT US https://ajccbc.ncsa.or.th/about-us/〔2025/5/29 確認〕
※ 40 AJCCBC：NEWS https://ajccbc.ncsa.or.th/ajccbc-news/〔2025/5/29 確認〕
※ 41 総務省：大洋州島しょ国向けサイバーセキュリティ能力構築演習（令和 6 年度第 1 回）を実施 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00221.html〔2025/5/29 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 6 年度第 2 回）の実施 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00233.html〔2025/5/29 確認〕
※ 43 The New York Times：Presidential Election Results: Trump Wins https://www.nytimes.com/interactive/2024/11/05/us/elections/results-president.html?searchResultPosition=5〔2025/6/2 確認〕
The Washington Post：Donald Trump wins presidential election, defeating Harris to retake White House https://www.washingtonpost.com/politics/2024/11/06/donald-trump-wins-presidential-election/?=undefined〔2025/6/2 確認〕
※ 44 朝日新聞：【随時更新】トランプ氏が大統領令に続々署名 一目で分かる政策一覧 https://www.asahi.com/articles/AST1L1T17T1LUHBI009M.html〔2025/6/2 確認〕
※ 45 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/〔2025/6/2 確認〕
※ 46 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〔2025/6/2 確認〕
※ 47 Federal Register：Restoring Freedom of Speech and Ending Federal Censorship https://www.federalregister.gov/documents/2025/01/28/2025-01902/restoring-freedom-of-speech-and-ending-federal-censorship〔2025/6/2 確認〕
Yahoo! ニュース：「連邦政府の検閲終了」反偽誤情報対策を掲げるトランプ大統領令の影響とは？ https://news.yahoo.co.jp/expert/articles/02dcd5b29617a688425b9b779eaa7ec2484328a9〔2025/6/2 確認〕
※ 48 CONGRESS.GOV：S.146 - TAKE IT DOWN Act https://www.congress.gov/bill/119th-congress/senate-bill/146〔2025/6/2 確認〕
※ 49 DOGE：Latest work https://doge.gov/〔2025/6/2 確認〕
BBC：What is Doge and why has Musk left? https://www.bbc.com/news/articles/c23vkd57471o〔2025/6/2 確認〕
※ 50 選挙セキュリティ：選挙インフラを標的とする攻撃に対するセキュリティの総称。ここでの「選挙インフラ」は、狭義には選挙実施に関わるシステム（電子投票等の IT システムに加え、投票箱・郵便投票等の物理システム）、選挙に関わる投票データ・個人情報、及びそれらの制度・運用である。2016 年の米国大統領選挙以降は、広義の選挙セキュリティとして候補者・支持者・選挙実施者へのサイバー攻撃、偽情報・誤情報による選挙妨害・誹謗中傷・世論操作等も対策の対象となっている。
※ 51 https://www.cisecurity.org/〔2025/6/2 確認〕
※ 52 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 150 円として換算している。
※ 53 Dark Reading：CISA Cuts $10M in ISAC Funding & 100s of Employees https://www.darkreading.com/remote-workforce/cisa-cuts-isac-funding-employees〔2025/6/2 確認〕
※ 54 The Register：CISA pen-tester says 100-strong red team binned after DOGE canceled contract https://www.theregister.com/2025/03/12/cisa_staff_layoffs/〔2025/6/2 確認〕
※ 55 CISA：Statement on CISA's Red Team https://www.cisa.gov/news-events/news/statement-cisas-red-team〔2025/6/2 確認〕
※ 56 MITRE 社：https://www.mitre.org/〔2025/6/2 確認〕
※ 57 CVE：https://www.cve.org/〔2025/6/2 確認〕
※ 58 GIGAZINE：脆弱性管理を担う CVE プログラムの運営資金が 2025 年 4 月 16 日で失効することが明らかに https://gigazine.net/news/20250416-cve-program-lose-funding/〔2025/6/2 確認〕
※ 59 HPCwire：CVE Foundation Launched to Secure the Future of the CVE Program https://www.hpcwire.com/off-the-wire/cve-foundation-launched-to-secure-the-future-of-the-cve-program/〔2025/6/2 確認〕
CVE Foundation：https://www.thecvefoundation.org/〔2025/6/2 確認〕
※ 60 Nextgov/FCW：CISA warns threat hunting staff of end to Google, Censys contracts as agency cuts set in https://www.nextgov.com/cybersecurity/2025/04/cisa-warns-threat-hunting-staff-end-google-censys-contracts-agency-cuts-set/404680/〔2025/6/2 確認〕
※ 61 The Record：Exclusive: Hegseth orders Cyber Command to stand down on Russia planning https://therecord.media/hegseth-orders-cyber-command-stand-down-russia-planning〔2025/6/2 確認〕
The Associated Press：Hegseth orders suspension of Pentagon's offensive cyberoperations against Russia https://apnews.com/article/cyber-command-russia-putin-trump-hegseth-c46ef1396e3980071cab81c27e0c0236〔2025/6/2 確認〕
※ 62 CNN：US suspends offensive cyber operations against Russia, senior US official says https://edition.cnn.com/2025/03/02/politics/us-cyber-operations-russia-suspend/index.html〔2025/6/2 確認〕
※ 63 Dark Reading：Pentagon, CISA Deny Change in US Cyber Policy on Russia https://www.darkreading.com/threat-intelligence/pentagon-cisa-deny-change-us-cyber-policy-russia〔2025/6/2 確認〕
※ 64 Federal Register：Improving the Nation's Cybersecurity https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity〔2025/6/2 確認〕
※ 65 The White House：Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2025/01/16/executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/〔2025/6/2 確認〕
※ 66 NIST：Secure Software Development Framework（SSDF）Version 1.1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf〔2025/6/2 確認〕
※ 67 FedRAMP：https://www.fedramp.gov/〔2025/6/2 確認〕
※ 68 Federal Register：Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities https://www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities〔2025/6/2 確認〕
※ 69 The White House：Fact Sheet: President Donald J. Trump Reprioritizes Cybersecurity Efforts to Protect America https://www.whitehouse.gov/fact-sheets/2025/06/fact-sheet-president-donald-j-trump-reprioritizes-cybersecurity-efforts-to-protect-america/〔2025/6/16 確認〕
The White House：Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144 https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/〔2025/6/16 確認〕
※ 70 NIST：U.S. Artificial Intelligence Safety Institute https://www.nist.gov/aisi〔2025/6/2 確認〕
※ 71 NIST：The NIST Cybersecurity Framework (CSF) 2.0 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf〔2025/6/2 確認〕
※ 72 https://www.ipa.go.jp/publish/wp-security/2024.html〔2025/6/2 確認〕
※ 73 NIST：CSF 2.0 Profiles https://www.nist.gov/cyberframework/profiles〔2025/6/2 確認〕
※ 74 NIST：NIST IR 8374r1 ipd Ransomware Risk Management https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8374r1.ipd.pdf〔2025/6/2 確認〕
※ 75 NIST：NIST IR 8546 ipd Cybersecurity Framework Version 2.0 Semiconductor Manufacturing Profile https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8546.ipd.pdf〔2025/6/2 確認〕
※ 76 NIST：Cybersecurity and AI Workshop Concept Paper https://www.nccoe.nist.gov/sites/default/files/2025-02/cyber-ai-concept-paper.pdf〔2025/6/2 確認〕
※ 77 NIST：Cyber AI Profile Workshop https://www.nccoe.nist.gov/get-involved/attend-events/cyber-ai-profile-workshop〔2025/6/2 確認〕
※ 78 NIST:Artificial Intelligence Risk Management Framework（AI RMF 1.0） https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

〔2025/6/2 確認〕
※ 79 NIST：NIST SP 800-171 Rev. 3 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations https://csrc.nist.gov/pubs/sp/800/171/r3/final〔2025/6/2 確認〕
NIST SP 800-171A Rev. 3 Assessing Security Requirements for Controlled Unclassified Information https://csrc.nist.gov/pubs/sp/800/171/a/r3/final〔2025/6/2 確認〕
※ 80 NIST：NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final〔2025/6/2 確認〕
※ 81 NIST：NIST SP 800-161r1-upd1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf〔2025/6/2 確認〕
※ 82 NIST：NIST SP 800-172 Rev. 3 Enhanced Security Requirements for Protecting Controlled Unclassified Information https://csrc.nist.gov/pubs/sp/800/172/r3/ipd〔2025/6/2 確認〕
※ 83 DoD：Cybersecurity Maturity Model Certification Program Final Rule Published https://www.defense.gov/News/Releases/Release/Article/3932947/cybersecurity-maturity-model-certification-program-final-rule-published/〔2025/6/2 確認〕
Federal Register：Cybersecurity Maturity Model Certification (CMMC) Program https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program〔2025/6/2 確認〕
※ 84 Software Bill of Materials（SBOM）：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。
※ 85 FCC：U.S. Cyber Trust Mark https://www.fcc.gov/CyberTrustMark〔2025/6/2 確認〕
※ 86 NIST：Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf〔2025/6/2 確認〕
NIST：Recommended Criteria for Cybersecurity Labeling of Consumer Software https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-1.pdf〔2025/6/2 確認〕
※ 87 The White House：White House Launches “U.S. Cyber Trust Mark”, Providing American Consumers an Easy Label to See if Connected Devices are Cybersecure https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2025/01/07/white-house-launches-u-s-cyber-trust-mark-providing-american-consumers-an-easy-label-to-see-if-connected-devices-are-cybersecure/〔2025/6/2 確認〕
※ 88 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〔2025/6/2 確認〕
※ 89 European Commission：Cyber Resilience Act (CRA) ¦ Updates, Compliance, https://www.european-cyber-resilience-act.com/〔2025/6/2 確認〕
※ 90 Questex, LLC：What’s next for the Cyber Trust Mark program under Trump? https://www.fierceelectronics.com/electronics/whats-next-cyber-trust-mark-program-under-trump〔2025/6/2 確認〕
※ 91 NIST：NIST SP 800-231 Bugs Framework (BF) Formalizing Cybersecurity Weaknesses and Vulnerabilities https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-231.pdf〔2025/6/2 確認〕
※ 92 IPA：共通脆弱性タイプ一覧 CWE 概説 https://www.ipa.go.jp/security/vuln/scap/cwe.html〔2025/6/2 確認〕
※ 93 IPA：共通脆弱性識別子 CVE 概説 https://www.ipa.go.jp/security/vuln/scap/cve.html〔2025/6/2 確認〕
※ 94 NIST：NIST SP 800-63-4 2pd Digital Identity Guidelines https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.2pd.pdf〔2025/6/2 確認〕
※ 95 NIST：NIST SP 800-63A-4 2pd Digital Identity Guidelines Identity Proofing and Enrollment https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63A-4.2pd.pdf〔2025/6/2 確認〕
NIST：NIST SP 800-63B-4 2pd Digital Identity Guidelines Authentication and Authenticator Management https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.2pd.pdf〔2025/6/2 確認〕
NIST：NIST 800-63C-4 2pd Digital Identity Guidelines Federation and Assertions https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63C-4.2pd.pdf〔2025/6/2 確認〕
※ 96 NIST：NIST SP 800-218A Secure Software Development Practices for Generative AI and Dual-Use Foundation Models An SSDF Community Profile https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218A.pdf〔2025/6/2 確認〕
※ 97 デュアルユース対応基盤モデル（Dual-use foundation model）：EO 14110 では、大量のデータで学習した AI モデルで広く応用可能であり、悪用のために改変されるとセキュリティ、安全保障、経済安全保障、公衆衛生、公衆の安全に重大なリスクをもたらすもの、としている。
※ 98 同覚書「National Security Memorandum on Critical Infrastructure Security and Resilience（NSM-22）」は Trump 政権によって撤回された。
※ 99 CISA：National Security Memorandum on Critical Infrastructure Security and Resilience https://www.cisa.gov/national-security-memorandum-critical-infrastructure-security-and-resilience〔2025/6/2 確認〕
※ 100 CISA：FY2025-2026 CISA International Strategic Plan https://www.cisa.gov/2025-2026-cisa-international-strategic-plan#:~:text=The%20CISA%20International%20Strategic%20Plan%20will%20focus%20and%20guide%20the,Americans%20rely%20on%20every%20day.〔2025/6/2 確認〕
※ 101 The White House：Radical Transparency About Wasteful Spending https://www.whitehouse.gov/presidential-actions/2025/02/radical-transparency-about-wasteful-spending/〔2025/6/2 確認〕
※ 102 DHS：Transparency of Contract Actions to Reduce Spending https://www.dhs.gov/cpo-transparency-contract-actions-reduce-spending〔2025/6/4 確認〕
※ 103 Democracy Docket：Cybersecurity Agency Ends Support to Election Security Program https://www.democracydocket.com/news-alerts/cybersecurity-agency-ends-support-to-election-security-program/〔2025/6/2 確認〕
※ 104 CISA：Cybersecurity Toolkit and Resources to Protect Elections https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections〔2025/6/2 確認〕
※ 105 GovInfoSecurity：CISA Budget Cuts Weaken US Election Security, Officials Warn https://www.govinfosecurity.com/cisa-budget-cuts-weaken-us-election-security-officials-warn-a-27858〔2025/6/2 確認〕
※ 106 Verified Voting：Election Security Experts Warn Cuts to CISA Threaten the Security and Resilience of Federal, State and Local Elections https://verifiedvoting.org/cisa-2-27-25/〔2025/6/2 確認〕
※ 107 The White House：OMB: M-25-21 MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf〔2025/6/2 確認〕
※ 108 ダークウェブ：検索エンジン等を経由する通常の経路ではアクセスできないインターネット上の一部領域を「ダークネット」と呼び、ダークネット上に構築された Web サイト群を特に「ダークウェブ」と呼ぶ。ダークウェブ上の情報交換は秘匿性が高いことを悪用し、サイバー犯罪者による交渉等に用いられることが多い。
※ 109 ENISA：ENISA Threat Landscape Methodology https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology〔2025/5/30 確認〕
※ 110 ENISA：ENISA Threat Landscape 2024 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024〔2025/5/30 確認〕
※ 111 piyolog：XZ Utils の脆弱性 CVE-2024-3094 についてまとめてみた https://piyolog.hatenadiary.jp/entry/2024/04/01/035321〔2025/5/30 確認〕
※ 112 ENISA：ENISA Foresight Cybersecurity Threats for 2030 https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030〔2025/5/30 確認〕
ENISA：Foresight Cybersecurity Threats For 2030 - Update 2024 https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024〔2025/5/30 確認〕
※ 113 European Commission：JOIN(2020) 18 final The EU's Cybersecurity Strategy for the Digital Decade https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018〔2025/5/30 確認〕
※ 114 EU：Directive (EU) 2022/2555 NIS 2 Directive https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022L2555〔2025/5/30 確認〕
※ 115 ENISA：2024 Report on the State of Cybersecurity in the Union https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union〔2025/5/30 確認〕

※ 116 EU：Directive (EU) 2016/1148 NIS Directive https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng〔2025/5/30 確認〕
※ 117 EU 指令（Directive）は EU 法の一形態であり、これに準拠する国内法を EU 加盟各国において制定することで具体化する。NIS 指令や NIS 2 指令は EU 指令の一種である。
※ 118 European Parliament：Briefing, The NIS2 Directive https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf〔2025/5/30 確認〕
※ 119 ENISA：EU CyCLONe https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cyclone〔2025/5/30 確認〕
※ 120 DNS Research Federation：NIS2 Article 28 Tracker https://dnsrf.org/nis2-transition/〔2025/5/30 確認〕
※ 121 European Commission：The Commission calls on 23 Member States to fully transpose the NIS2 Directive https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive〔2025/5/30 確認〕
※ 122 EU：Regulation (EU) 2025/38 Cyber Solidarity Act https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32025R0038〔2025/5/30 確認〕
※ 123 European Parliament：Briefing, Cyber solidarity act https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754614/EPRS_BRI(2023)754614_EN.pdf〔2025/5/30 確認〕
※ 124 EU：Regulation (EU) 2022/2554 Digital Operational Resilience Act https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng〔2025/5/30 確認〕
※ 125 EIOPA：Digital Operational Resilience Act (DORA) https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en〔2025/5/30 確認〕
※ 126 EU：Commission Implementing Regulation (EU) 2024/2956 Register of Information https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402956〔2025/5/30 確認〕
※ 127 EU：Commission Delegated Regulation (EU) 2024/1502 the criteria for the designation of ICT third-party service providers as critical for financial entities https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1502〔2025/5/30 確認〕
※ 128 EU-SCICF：Systemic Cyber Incident Coordination Framework (EU-SCICF) https://www.eu-scicf.com/〔2025/5/30 確認〕
※ 129 EU：Regulation (EU) 2024/2847 Cyber Resilience Act https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng〔2025/5/30 確認〕
※ 130 European Parliament：Briefing, EU Cyber Resilience Act https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI(2022)739259_EN.pdf〔2025/5/30 確認〕
※ 131 PwC：欧州サイバーレジリエンス法～製造業が今すぐに取るべき対策～ https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/eu-cyber-resilience-act05.html〔2025/5/30 確認〕
※ 132 JETRO：CE マーキングの概要：EU https://www.jetro.go.jp/world/qa/04S-040011.html〔2025/5/30 確認〕
※ 133 ENISA：EUCC Certification Scheme https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en〔2025/5/30 確認〕
※ 134 EU：Regulation (EU) 2019/881 Cybersecurity Act https://eur-lex.europa.eu/eli/reg/2019/881/oj〔2025/5/30 確認〕
※ 135 EU：Commission Implementing Regulation (EU) 2024/482 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R0482&qid=1707312751025〔2025/5/30 確認〕
※ 136 EU：Commission Implementing Regulation (EU) 2024/3144 https://eur-lex.europa.eu/eli/reg_impl/2024/3144/oj〔2025/5/30 確認〕
※ 137 EU：Regulation (EU) 2025/37 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32025R0037〔2025/5/30 確認〕
※ 138 国立研究開発法人科学技術振興機構：中国：中国・第 13 期全人代第 4 回会議　第 14 次五カ年計画における科学技術イノベーション政策動向概要 https://www.jst.go.jp/crds/report/CN20210325.html〔2025/6/18 確認〕
※ 139 国立研究開発法人科学技術振興機構：中国・第 13 期全人代第 4 回会議第 14 次五カ年計画における科学技術イノベーション政策動向概要 https://www.jst.go.jp/crds/pdf/2020/FU/CN20210325.pdf〔2025/6/18 確認〕
※ 140 国立研究開発法人科学技術振興機構：中華人民共和国国民経済・社会発展の第 14 次五カ年計画および 2035 年までの長期目標綱要 https://spc.jst.go.jp/policy/national_policy/downloads/r_gvm_2022.pdf〔2025/6/18 確認〕
※ 141 JETRO：サイバーセキュリティとデータ管理監督法制の体系整理 https://www.jetro.go.jp/ext_images/_Reports/01/5bfcc1481fbb2442/20210047_04.pdf〔2025/6/18 確認〕
※ 142 JETRO：重要データの識別・認定 https://www.jetro.go.jp/ext_images/_Reports/01/5a02eed2b328b63b/20220046_02.pdf〔2025/6/18 確認〕
※ 143 JETRO：中国のデータ・個人情報の域外移転規制の最新動向（2024 年 3 月時点） https://www.jetro.go.jp/ext_images/_Reports/01/690307ed2a411652/20240004_02.pdf〔2025/6/18 確認〕
※ 144 JETRO：ネットワークデータ安全管理条例 https://www.jetro.go.jp/ext_images/_Reports/01/b41ddf5b802238e1/20250007_01.pdf〔2025/6/18 確認〕
※ 145 JETRO:「『データ要素×』3 カ年行動計画」を発表、12 分野でデータの活用を推進 https://www.jetro.go.jp/biznews/2024/01/ddc4c96a55ea3f22.html〔2025/6/18 確認〕
※ 146 NISC：重要インフラを取り巻く情勢について https://www.nisc.go.jp/pdf/council/cs/ciip/dai37/37_shiryou4_jousei.pdf〔2025/6/18 確認〕
※ 147 Reuters：中国、主要産業のハッキング対策強化へ https://jp.reuters.com/world/security/UKJ32RJ205KZPL2UKTTSAEJ7UA-2024-02-26/〔2025/6/18 確認〕
※ 148 JETRO：最近法規情報 2024 年 5 月に公布された主な法規 https://www.jetro.go.jp/ext_images/world/asia/cn/kahoku/pdf/beijing_202405.pdf〔2025/6/18 確認〕
※ 149 TMI 総合法律事務所：【中国】データの越境流動の促進と規範規定について https://www.tmi.gr.jp/eyes/blog/2024/15613.html#_ftnref20〔2025/6/18 確認〕
※ 150 一般財団法人安全保障貿易情報センター：中国の推奨性国家標準《データ安全技術―データの分類と等級区分の規則》と重要データ識別ガイドラインについて https://www.cistec.or.jp/service/uschina/20240801-2.pdf〔2025/6/18 確認〕
国家市場監督管理総局 国家標準化管理委員会：国家標準全文公開系統 https://openstd.samr.gov.cn/bzgk/gb/index〔2025/6/18 確認〕
※ 151 人民網日本語版：「国家秘密保護法」が 14 年ぶりの改正、サイバー情報の機密管理を整備 https://j.people.com.cn/n3/2024/0228/c94474-20138456.html〔2025/6/18 確認〕
※ 152 JETRO：中国、国家秘密保護法を改正、党の指導と関連部門の権限を強化 https://www.jetro.go.jp/biznews/2024/03/bb18d8286956a0ad.html〔2025/6/18 確認〕
※ 153 Reuters：中国、国家機密保護法の実施条例を公表　データ保護を徹底 https://jp.reuters.com/world/security/5263TH4KFJPSBI3GSZB7TDY6BI-2024-07-24/〔2025/6/18 確認〕
※ 154 CSA：Cybersecurity Act https://www.csa.gov.sg/legislation/cybersecurity-act〔2025/5/29 確認〕
※ 155 NACSA：CYBER SECURITY ACT 2024 (ACT 854) https://www.nacsa.gov.my/act854.php〔2025/5/29 確認〕
※ 156 Viet Nam News：Prime Minister issues directive to enhance cybersecurity https://vietnamnews.vn/society/1653493/prime-minister-issues-directive-to-enhance-cybersecurity.html〔2025/5/29 確認〕
※ 157 Phạm Minh Chính：VỀ TĂNG CƯỜNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Cong-dien-33-CD-TTg-2024-tang-cuong-bao-dam-an-toan-thong-tin-mang-605594.aspx〔2025/5/29 確認〕
※ 158 https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-monitoring/best-practices-event-logging-threat-detection〔2025/5/29 確認〕
※ 159 https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/critical-infrastructure/principles-operational-technology-cybersecurity?_ga=2.71302352.1136199635.1742301373-782615522.1742301373〔2025/5/29 確認〕
※ 160 ISAC：Certified National Cyber Security Scholar https://isacfoundation.org/national-cyber-security-scholar/〔2025/5/29 確認〕
※ 161 https://www.apcert.org/〔2025/5/29 確認〕
※ 162 APCERT：Member Teams https://www.apcert.org/about/structure/members.html〔2025/5/29 確認〕
※ 163 APCERT：APCERT CYBER DRILL 2024 “APT Group Attack Response: Where is Wally?” https://www.apcert.org/documents/pdf/APCERT_Drill_2024_Press_Release_draft.pdf〔2025/5/29 確認〕
※ 164 APCERT：Documents https://www.apcert.org/documents/index.html〔2025/5/29 確認〕

※ 165 https://krcert.or.kr〔2025/5/29 確認〕
※ 166 https://www.cert.org.cn〔2025/5/29 確認〕
※ 167 https://www.twcert.org.tw〔2025/5/29 確認〕
※ 168 CSA：Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region https://www.csa.gov.sg/news-events/press-releases/singapore-and-asean-member-states-deepen-commitment-to-enhance-collective-cybersecurity-in-the-region〔2025/5/29 確認〕
※ 169 ISO：ISO/IEC JTC 1　https://www.iso.org/committee/45020.html〔2025/7/11 確認〕
※ 170 JISC：JISC について　https://www.jisc.go.jp/jisc/index.html〔2025/7/11 確認〕
※ 171 ITU：SG17: Security　https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx〔2025/7/11 確認〕
※ 172 IETF：Security Area　https://wiki.ietf.org/group/sec〔2025/7/11 確認〕
※ 173 TCG：Welcome to Trusted Computing Group　https://trustedcomputinggroup.org/work-groups/regional-forums/japan〔2025/7/11 確認〕
※ 174 ISO：ISO/IEC JTC 1/SC 27　https://committee.iso.org/home/jtc1sc27〔2025/7/11 確認〕
※ 175 https://www.jisc.go.jp/international/iso-prcs.html〔2025/7/11 確認〕
※ 176 https://www.jipdec.or.jp/project/smpo/u71kba000000jjgv-att/27000family_20250423.pdf〔2025/7/11 確認〕
※ 177 ISO：ISO/IEC JTC 1/SC 42　https://www.iso.org/committee/6794475.html〔2025/7/11 確認〕
※ 178 ISA：ISA99, Industrial Automation and Control Systems Security　https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99〔2025/7/11 確認〕
※ 179 IEC：TC 65　https://www.iec.ch/dyn/www/f?p=103:14:613850989665891::::FSP_ORG_ID,FSP_LANG_ID:2612,25〔2025/7/11 確認〕
※ 180 https://www.jpcert.or.jp/present/2023/ICSR2023_02_YOKOGAWAElectric.pdf〔2025/7/11 確認〕
※ 181 https://www.jpcert.or.jp/event/ics-conference2023.html〔2025/7/11 確認〕
※ 182 IPA：制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ　https://www.ipa.go.jp/security/controlsystem/incident.html〔2025/7/11 確認〕
※ 183 SCADA（Supervisory Control and Data Acquisition）：産業制御システムの一種であり、コンピューターによるシステム監視とプロセス制御を行う。
※ 184 https://www.iecee.org〔2025/7/11 確認〕
※ 185 https://isasecure.org〔2025/7/11 確認〕

付録

第20回 IPA「ひろげよう情報セキュリティコンクール」2024 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30,636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

〈標語部門〉

パスワード
意味ない配列
意味がある

板野 早希さん　東京都 東京都立上野高等学校

〈ポスター部門〉

多要素認証があなたを守る



岩永 陽翔さん　東京都 国際基督教大学高等学校

優秀賞

〈標語部門〉

パスワード　よりふくざつに　足すワード

佐藤 海璃さん
宮城県 南三陸町立志津川小学校

謎メール　軽いクリック　重い代償

酒井 翔琉さん
茨城県 北茨城市立中郷中学校

多要素認証　そのひと手間が　漏洩防ぐ

一ノ瀬 玲央さん
北海道 北海道旭川東高等学校

〈ポスター部門〉

タップの前に疑って!!



今岡陽菜歌さん　大阪府 大阪市立大淀小学校

覗き見に注意



井上羽南さん 茨城県 茨城県立並木中等教育学校

同じ鍵は危険です



杉本瑞季さん 愛知県 愛知県立安城南高等学校

IPAの便利なツールとコンテンツ

情報セキュリティ対策ベンチマーク
https://www.ipa.go.jp/security/sec-tools/benchmark.html

診断

用途・目的	自組織のセキュリティレベルを診断
利用対象者	情報セキュリティ担当者
特 長	• 他組織と比較した自組織のセキュリティレベルが判る • 自組織に不足しているセキュリティ対策が判る

概要

「セキュリティ対策の取り組み状況に関する評価項目」27 問と「企業プロフィールに関する評価項目」19 問、計 46 問に回答すると以下の診断結果を表示します。

■提供される診断結果
- セキュリティレベルを示したスコア（最高点 135 点、最低点 27 点）
- 企業規模、業種が自組織と近い他組織と診断項目別にスコアを比較
- 結果に応じた推奨される取り組み

脆弱性体験学習ツール「AppGoat」
https://www.ipa.go.jp/security/vuln/appgoat/

学習

用途・目的	脆弱性に関する基礎的な知識の学習
利用対象者	• アプリケーション開発者 • Web サイト管理者
特 長	脆弱性の概要や対策方法等、脆弱性に関する基礎的な知識を実習形式で体系的に学べるツール

概要

SQL インジェクション、クロスサイト・スクリプティング等 の 12 種類の Web アプリケーションに関連する脆弱性について学習できるツールです。
利用者は学習テーマ毎の演習問題に対して、埋め込まれた脆弱性の発見、プログラミング上の問題点の把握、対策手法を学べます。

■活用方法例
- Web アプリケーション用学習ツール（個人学習モード）を利用した、自宅等での個人学習
- Web アプリケーション用学習ツール（集合学習モード）を利用した、学校の講義や組織内のセミナー等、複数人での学習

脆弱性対策情報データベース「JVN iPedia」
https://jvndb.jvn.jp/

対策

用途・目的	自組織で使用しているソフトウェア製品の脆弱性の確認と対策
利用対象者	• システム管理者 • 製品・サービスの保守を担う担当者
特 長	国内外で公開されたソフトウェア製品の脆弱性対策情報が掲載された、キーワード検索可能なデータベース

概要

■掲載情報例
- 脆弱性の概要
- 脆弱性がある製品名とそのベンダー名
- 共通脆弱性識別子 CVE
- 脆弱性の深刻度 CVSS 基本値
- 本脆弱性に関わる製品ベンダー等のリンク

■活用方法例
- ネット記事等に記載された CVE 番号を JVN iPediaで検索し、脆弱性の詳細を確認
- 自組織で使用している製品名で検索し、脆弱性の詳細を確認

MyJVN バージョンチェッカ for .NET
https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html

対策

用途・目的	パソコンにインストールされたソフトウェア製品のバージョンが最新かどうかの確認
利用対象者	パソコン利用者全般
特 長	インストールされている対象製品が最新バージョンかどうかをまとめて確認できる

概要

■判定対象ソフトウェア製品

- Adobe Reader
- JRE
- Lhaplus
- Mozilla Firefox
- Mozilla Thunderbird
- iTunes
- Lunascape
- Becky! Internet Mail
- OpenOffice.org
- VMware Player
- Google Chrome
- LibreOffice

■活用方法例

毎朝、MyJVN バージョンチェッカを実行して、使用しているソフトウェアが最新かどうかをチェックし、最新でなければそのソフトウェアを更新する

注意警戒情報サービス
https://jvndb.jvn.jp/alert/

対策

用途・目的	脆弱性対策に必要な最新情報の収集
利用対象者	• システム管理者 • 製品・サービスの保守を担う担当者
特 長	国内で広く利用され、脆弱性が悪用されると影響の大きいサーバー用オープンソースソフトウェアのリリース情報と IPA が発信する「重要なセキュリティ情報」を提供

概要

■掲載情報例

- Apache HTTP Server
- Apache Struts
- Apache Tomcat
- BIND
- Joomla!
- OpenSSL
- WordPress
- 重要なセキュリティ情報

■活用方法例

定期的に自組織で使用しているオープンソースソフトウェアのリリース情報や IPA が発信する「重要なセキュリティ情報」が公表されているかどうかを確認し、公表されていれば内容の確認、必要に応じ対応を行う

サイバーセキュリティ注意喚起サービス「icat for JSON」
https://www.ipa.go.jp/security/vuln/icat.html

対策

用途・目的	IPA が発信する「重要なセキュリティ情報」のリアルタイム取得
利用対象者	• システム管理者 • サービスの保守を担う担当者 • 個人利用者
特 長	Web ページに HTML タグを埋め込むと、Web ページから IPA が発信する「重要なセキュリティ情報」を配信

概要

■「重要なセキュリティ情報」発信例

- 利用者への影響が大きい製品の脆弱性情報
- 広く使われる製品のサポート終了情報
- サイバー攻撃への注意喚起

■活用方法例

icat を自組織の従業員がよくアクセスする Web ページ（イントラページ等）に表示させ、ソフトウェア更新等の対策を促す

MyJVN 脆弱性対策情報フィルタリング収集ツール（mjcheck4）
https://jvndb.jvn.jp/apis/myjvn/mjcheck4.html

対策

用途・目的	自組織で使用しているソフトウェア製品の脆弱性の確認と対策
利用対象者	• システム管理者 • 製品・サービスの保守を担う担当者
特 長	JVN iPedia に登録されている脆弱性対策情報をフィルタリングして自社システムに関連する脆弱性情報を効率よく収集

概要

■フィルタリング例
• 製品名　　• CVSSv3　　• 公開日　等

■活用方法例
• 自組織が利用しているオープンソースソフトウェア製品の脆弱性対策情報収集
• 情報システム部門が運用しているシステムの脆弱性対策情報の収集

Web サイトの攻撃兆候検出ツール「iLogScanner」
https://www.ipa.go.jp/security/vuln/ilogscanner/

診断

用途・目的	Web サイトに対する攻撃の痕跡、攻撃の可能性を検出
利用対象者	Web サイト運営者
特 長	Web サイトのアクセスログ、エラーログ、認証ログを解析し、攻撃の痕跡や攻撃に成功した可能性があるログを解析結果レポートに表示

概要

■アクセスログ、エラーログから検出可能な項目例
• SQL インジェクション　　• OS コマンド・インジェクション
• ディレクトリ・トラバーサル　　• クロスサイト・スクリプティング

■認証ログ（Secure Shell、FTP）から検出可能な項目例
• 大量のログイン失敗　　• 短時間の集中ログイン
• 同一ファイルへの大量アクセス　　• 認証試行回数

■活用方法例
定期的に iLogScanner を実行し、自組織の Web サイトを狙った攻撃が行われているか確認する

5 分でできる！情報セキュリティ自社診断
https://www.ipa.go.jp/security/guide/sme/5minutes.html

診断

用途・目的	自社の情報セキュリティ対策状況を診断
利用対象者	中小企業・小規模事業者の経営者、管理者、従業員
特 長	• 設問に答えるだけで自社のセキュリティ対策状況を把握することができる • 診断後は、診断結果に即した対策が確認できる

概要

「5 分でできる！情報セキュリティ自社診断」は、情報セキュリティ対策のレベルを数値化し、問題点を見つけるためのツールです。
25 の質問に答えるだけで診断することができ、解説編を参照することで、自社で対応していない場合に生じる情報セキュリティ上のリスクと、今後どのような対策を設けるべきかを把握することができます。

情報セキュリティ・ポータルサイト「ここからセキュリティ！」

学習 診断 対策

https://www.ipa.go.jp/security/kokokara/

用途・目的	• 情報セキュリティや情報リテラシーに関する情報収集 • 国内の主なレポート、ガイドライン、学習・診断等のツール等の利用
利用対象者	• インターネットの一般利用者（小学生～大人） • 企業の管理者／一般利用者
特 長	情報セキュリティ関連の民間及び公的な団体が公開する無償の資料、情報、ツールを網羅的に掲載。目的別、用途別、役割別に情報を選択し利用が可能

概要

• セキュリティベンダー、公的機関、政府等から発信される注意喚起や、資料・動画・ツール等のコンテンツを網羅的に掲載したポータルサイト
• コンテンツを「被害に遭ったら」「対策する」「教育・学習」「セキュリティチェック」「データ＆レポート」に分類。必要な情報が見つけやすい
• 教育学習は対象者を細分化し、それぞれに適した教育学習コンテンツを紹介

サイバーセキュリティ経営可視化ツール

診断

https://www.ipa.go.jp/security/economics/checktool.html

用途・目的	セキュリティ対策の実施状況のセルフチェック
利用対象者	原則として、従業員 300 名以上の企業の CISO 等、サイバーセキュリティ対策の実施責任者
特 長	サイバーセキュリティ経営ガイドライン Ver3.0 に準拠したセキュリティ対策の実施状況を成熟度モデルで自己診断し、レーダーチャートで可視化

概要

経営者がサイバーセキュリティ対策を実施する上で責任者となる担当幹部（CISO 等）に指示すべき“重要 10 項目”が、適切に実施されているかどうかを 5 段階の成熟度モデルで自己診断し、その結果をレーダーチャートで可視化するツールです。
診断結果は、経営者への自社のセキュリティ対策の実施状況の説明資料として利用できます。経営者が対策状況を定量的に把握することで、サイバーセキュリティに関する方針の策定や適切なセキュリティ投資の検討、投資家等ステークホルダとのコミュニケーション等に役立てることができます。

■提供される主な機能
・重要 10 項目の実施状況の可視化
・診断結果と業種平均との比較
・対策を実施する際の参考事例
・グループ企業同士の診断結果の比較

5 分でできる！情報セキュリティポイント学習

学習

https://www.ipa.go.jp/security/sec-tools/5mins_point.html

用途・目的	自社の情報セキュリティ教育の実施
利用対象者	中小企業の経営者、管理者、従業員等
特 長	• 自社診断の質問を 1 テーマ 5 分で学べる • インストール不要、無料の学習ツール

概要

情報セキュリティについて学習できるツールです。
身近にある職場の日常の 1 コマを取り入れた親しみやすい学習テーマで、情報セキュリティに関する様々な事例を疑似体験しながら適切な対処法を学ぶことができます。

安心相談窓口だより
https://www.ipa.go.jp/security/anshin/attention/index.html

学習 対策

用途・目的	最新の「ネット詐欺」等の手口を知り被害防止につなげる
利用対象者	スマートフォン、パソコンの一般利用者
特 長	実際に相談窓口に寄せられる、よくある相談内容に関して「手口」と「被害にあった場合の対処」「被害にあわないための対策」を学べる

概要

IPA 情報セキュリティ安心相談窓口では、寄せられる相談に関して手口を実際に検証し、そこで得られた知見をその後の相談対応にフィードバックするとともに、注意喚起等、情報発信にも活かしています。
「安心相談窓口だより」では中でも多く相談が寄せられる相談内容の「手口」「対処」「対策」について、パソコンやスマートフォンの操作等にあまり詳しくない人でも理解できるように分かりやすく説明を行っています。
記事は不定期に公開されますので、「安心相談窓口だより」を定期的に確認することで、最新のネット詐欺等の手口や対策を知り、被害の未然防止に役立てることができます。
手口に関する内容以外にも、被害にあわないための日ごろから気を付けるポイントについての記事も公開しています。

映像で知る情報セキュリティ
https://www.ipa.go.jp/security/videos/list.html

学習

用途・目的	動画の視聴により、情報セキュリティの脅威、手口、対策等を学ぶ
利用対象者	スマートフォンやパソコンを使用する一般利用者 組織の経営者、対策実践者、啓発者、従業員等
特 長	組織内の研修等で利用できる10 分前後の動画を公開。情報セキュリティ上の様々な脅威・手口、対策をドラマ等の動画を通じで学べる

概要

「サイバー攻撃」「内部不正」「ワンクリック請求」「偽警告」等の脅威をテーマにした動画のほか、「中小企業向け情報セキュリティ対策」「新入社員向け」「保護者／小学生／中高生向け」といった訴求対象者別の動画を公開しています。動画の視聴により、様々な情報セキュリティ上の脅威・手口、対策を学ぶことができます。
情報セキュリティの自己研さんを目的とした個人の視聴のほか、組織内の研修用としての利用が可能です。

■動画のタイトル例
- 今そこにある脅威～組織を狙うランサムウェア攻撃～
- 今そこにある脅威～内部不正による情報流出のリスク～
- What' s BEC ？～ビジネスメール詐欺 手口と対策～
- あなたのパスワードは大丈夫？～インターネットサービスの不正ログイン対策～

索引

数字

8Base ····· 20

A

Active Directory ····· 25, 30, 37, 44
AI（Artificial Intelligence：人工知能）
····· 76, 92, 118, 189
AI Act ····· 77, 83, 84
AI Risk Management Framework（AI RMF）
····· 82, 191
AI ガバナンス ····· 82, 85
AI 事業者ガイドライン ····· 83, 87, 129
AI システム ····· 83
AI セーフティサミット ····· 84
AI セーフティ ····· 76, 81, 87
AI セーフティ・インスティテュート（AISI：AI Safety Institute） ····· 81, 84, 117, 129
AI セーフティに関する活動マップ（AMAIS） ····· 85
AI セキュリティ ····· 85, 190
AI ソウル・サミット ····· 84
AI モデル ····· 83
AI リスク ····· 77, 82, 84
ANEL ····· 25
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） ····· 204
APT40 ····· 118, 139, 186
APT（Advanced Persistent Threat）攻撃
····· 23, 24, 42
ASEAN Regional CERT（ASEAN Regional Computer Emergency Response Team：ASEAN 地域コンピューター緊急対応チーム）
····· 205
ASEAN サイバーセキュリティ閣僚会議（AMCC：ASEAN Ministerial Conference on Cybersecurity） ····· 205
ASM（Attack Surface Management）導入ガイダンス ····· 30
Attack Surface Management（ASM） ·· 21, 30, 116

B

Bashlite ····· 31
Black Basta ····· 43
BlackCat/ALPHV ····· 43
BlackSuit ····· 19, 41

C

C&C（Command and Control）サーバー
····· 23, 24, 26, 31, 118, 132
CCRA（Common Criteria Recognition Arrangement） ····· 159
ChatGPT ····· 10, 76, 86, 94, 102, 185
CI/CD パイプラインにおけるセキュリティの留意点に関する技術レポート ····· 122
CopyCop ····· 96
CRYPTREC（Cryptography Research and Evaluation Committees） ····· 164
CSIRT（Computer Security Incident Response Team） ····· 27, 141, 192, 195, 196, 201
CyberAv3ngers ····· 46
CYROP（Cyber Range Open Platform） ····· 147
CYXROSS ····· 133

D

DDoS 攻撃 ····· 9, 13, 31, 48, 100, 139
DNS（Domain Name System） ····· 33, 190, 195
Doppelgänger（ドッペルゲンガー） ····· 78, 96, 100
DRDoS（Distributed Reflection Denial of Service）攻撃 ····· 13

E

Earth Kasha ····· 25
EDR（Endpoint Detection and Response）
····· 21, 30, 190
EO 14028 ····· 190, 191
EO 14110 ····· 84, 85, 189, 192
EO 14144 ····· 190
ERAB サイバーセキュリティトレーニング ····· 146
EUCC（EU Cybersecurity Certification Scheme on Common Criteria） ····· 199
EU サイバーセキュリティ法（CSA：The EU Cybersecurity Act） ····· 199

eシール ····· 132

F

Flax Typhoon ····· 25
FrostyGoop ····· 46
Fuxnet ····· 45

G

Gafgyt ····· 31

I

IEC（International Electrotechnical Commission：国際電気標準会議） ····· 206
IEEE（The Institute of Electrical and Electronics Engineers, Inc.） ····· 206
IETF（Internet Engineering Task Force） ····· 206
IoC（Indicator of Compromise：侵害指標） ····· 22, 127
IOCONTROL ····· 46
IoT ····· 31, 47, 117, 151, 191
IoT 製品・サービス脆弱性対応ガイド ····· 54
IoT 製品に対するセキュリティ適合性評価制度 ····· 125, 143, 152
IoT ボットネット対策 ····· 132
ISA/IEC 62443 シリーズ ····· 210
ISMAP-LIU（イスマップ・エルアイユー：ISMAP for Low-Impact Use） ····· 162
ISMAP 管理基準 ····· 162
ISMAP クラウドサービスリスト ····· 163
ISO（International Organization for Standardization：国際標準化機構） ····· 206
ISO/IEC 15408 ····· 158, 209
ISO/IEC 27000 ファミリー ····· 207
ISO/IEC JTC 1/SC 27 ····· 207
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） ····· 206
IT 製品の調達におけるセキュリティ要件リスト ····· 158
IT セキュリティ評価及び認証制度（JISEC：Japan Information Technology Security Evaluation and Certification Scheme） ····· 158

J

J-CRAT（Cyber Rescue and Advice Team against targeted attack of Japan：サイバーレスキュー隊） ····· 25, 127
JTC 1（Joint Technical Committee 1：第一合同技術委員会） ····· 206
JVN iPedia ····· 34

L

Lazarus Group ····· 26
Living Off The Land（LOTL）戦術 ····· 24
Lizkebab ····· 31
LockBit ····· 10, 185
LODEINFO ····· 25

M

Microsoft Office ····· 25, 27
Mirai ····· 31, 48, 53, 151
MirrorFace ····· 25, 135

N

NICTER（Network Incident analysis Center for Tactical Emergency Response） ····· 13, 151
NIS2 指令（Network and Information Systems Directive 2） ····· 195, 196
NoName057(16) ····· 100
NOOPDOOR ····· 25
NOTICE（National Operation Towards IoT Clean Environment） ····· 47, 54, 132, 152
NVD（National Vulnerability Database） ····· 34

O

Operational Relay Box（ORB：中継装置） ····· 24, 38, 49
OT サイバーセキュリティの原則（Principles of OT Cyber Security） ····· 139, 203

P

People's Cyber Army ····· 100
PhaaS（Phishing as a Service） ····· 12
Phobos ····· 118
Portal Kombat ····· 96

R

RaaS（Ransomware as a Service） ……10, 17, 43
Radar/Dispossessor ……185
RansomHub ……10, 42, 43
Rhysida ……41

S

SaaS ……10, 162, 198
Salt Typhoon ……8, 25, 42
SBOM（Software Bill of Materials：ソフトウェア部品表） ……117, 125, 191, 199
SECCON（SECURITY CONTEST） ……148
SecHack365 ……148
Secondary Infektion ……100
Secure Software Development Framework（SSDF） ……87, 117, 126, 190
SECURITY ACTION ……118, 162, 171
SIM スワップ ……139, 140
SMS ……10, 62
SNS 型投資・ロマンス詐欺 ……138, 139, 173
Spamouflage（スパムフラージュ） ……94
SQL インジェクション ……25, 34
Storm-1516 ……97
Storm-2035 ……94

T

TCG（Trusted Computing Group） ……207
Telegram ……97, 100, 101
The NIST Cybersecurity Framework (CSF) 2.0 ……125, 191
TraderTraitor ……26

U

U.S. Cyber Trust Mark ……117, 157, 191
UNC5537 ……11

V

Volt Typhoon ……24
VPN ……14, 18, 20, 24, 36, 44

W

Windows ……9, 25, 37, 59

あ

アイデンティティ管理 ……209
アイランドホッピング攻撃 ……28
アクセス・無害化 ……110, 112, 114
暗号鍵管理ガイダンス ……164, 165
暗号鍵管理システム設計指針（基本編） ……165
暗号資産 ……26, 61, 118, 127, 139, 187
イスラエル・ハマス紛争 ……95, 102
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） ……135
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） ……12, 116, 128, 187, 204
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 ……118, 187
ヴィッシング（Vishing） ……10
営業秘密 ……13, 55, 130, 169
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 ……146, 157
遠隔操作ソフト ……59
遠隔操作マルウェア ……20
欧州刑事警察機構（Europol：European Union Agency for Law Enforcement Cooperation） ……20, 118, 185
オープンソースソフトウェア（OSS：Open Source Software） ……125, 190, 194
オープンリダイレクト（Open Redirect） ……36
お助け隊サービス 2 類 ……118, 171
オンライン安全法（Online Safety Act） ……98

か

技術情報管理認証制度 ……127
機能妨害型サイバー攻撃 ……100, 101
業界別サイバーレジリエンス強化演習（CyberREX：Cyber Resilience Enhancement eXercise by industry） ……144, 146
共通鍵暗号 ……165
共通脆弱性識別子 CVE（Common Vulnerabilities and Exposures） ……189, 192

共通脆弱性タイプ一覧 CWE（Common Weakness Enumeration）……34, 192
共通脆弱性評価システム CVSS（Common Vulnerability Scoring System）……35
虚偽情報……91
クラウドサービス……22, 121, 162, 165
クレジットカード……12, 60, 131, 137
クロスサイト・スクリプティング……34, 36
経済安全保障重要技術育成プログラム（K Program）……119
経済安全保障推進法……119
軽量暗号……165
公開鍵暗号……165
攻撃対象領域（アタックサーフェス）……21, 30, 34, 132, 152
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……125
国立研究開発法人情報通信研究機構（NICT：National Institute of Information and Communications Technology）……13, 115, 117, 132, 133, 147
国連サイバー犯罪条約……185
国家安全保障戦略……110, 112
国家サイバー統括室（NCO：National Cybersecurity Office）……13, 112, 186
国家支援型 APT 攻撃……24, 25, 27
コモンクライテリア（共通基準）……158

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……110
サイバーインテリジェンス情報共有ネットワーク……136
サイバー危機対応机上演習（CyberCREST：Cyber Crisis RESponse Table top exercise）……146
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）……127
サイバーセキュリティ 2024（2023 年度年次報告・2024 年度年次計画）……110, 116
サイバーセキュリティお助け隊サービス……118, 171
サイバーセキュリティ企画演習（CyberSPEX：Cyber Security Planning Exercise）……146
サイバーセキュリティ経営ガイドライン……28
サイバーセキュリティ月間……147, 174
サイバーセキュリティ産業振興戦略……126
サイバーセキュリティ人材……126, 141, 186, 194
サイバーセキュリティ戦略……111
サイバーセキュリティネクサス（CYNEX：Cybersecurity Nexus）……13, 147
サイバー対処能力強化法……110, 112
サイバー特別捜査部……32, 134, 139
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）……125, 209
サイバーレジリエンス法（CRA：Cyber Resilience Act）……157, 192, 198
サイバー連帯法（CSoA：Cyber Solidarity Act）……195, 196
サプライチェーン……28, 119, 125, 161, 168, 170
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……125, 161
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）……170
サプライチェーンリスク……53, 117, 121, 152, 191
サポート詐欺……58
産学情報セキュリティ人材育成交流会……149
産業サイバーセキュリティ研究会…117, 124, 141, 161
産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）……145, 187
事業継続計画（BCP：Business Continuity Plan）……23, 28, 196
実践的サイバー防御演習（CYDER：Cyber Defense Exercise with Recurrence）…148, 188
ジャッカル……119, 139
重要インフラ……10, 39, 111, 116, 135, 192
重要経済安保情報保護活用法……57, 119
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）……110
常時リスク診断・対処（CRSA：Continuous Risk Scoring & Action）……123
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 -……54
情報システムに係る政府調達におけるセキュリティ要

件策定マニュアル……116
情報処理安全確保支援士（登録セキスペ）……118, 127, 142, 144
情報セキュリティ安心相談窓口……58
情報セキュリティ早期警戒パートナーシップ……35, 128
情報セキュリティマネジメント試験……144
情報セキュリティマネジメントシステム（ISMS：Information Security Management System）……207
情報戦……91, 93
情報操作型サイバー攻撃……91, 93, 100
情報漏えい……8, 10, 13, 19, 54
新型コロナウイルス……92, 101
侵入型ランサムウェア攻撃……17, 20
水平展開……22, 23, 36
スマートカード……158
「スマート工場のセキュリティリスク分析調査」調査報告書……172
スマートシティセキュリティガイドライン……133
スマートフォン プライバシー セキュリティイニシアティブ（SPSI）……132
スミッシング（Smishing）……10
制御システム（ICS：Industrial Control System）……39, 145, 172, 210
制御システムのセキュリティリスク分析ガイド……46, 172
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）……146
脆弱性……34, 44, 47, 82, 113, 128
脆弱性対処に向けた製品開発者向けガイド……54
生成 AI（Generative AI）……77, 92, 130, 139, 173, 185
生成 AI プロファイル……82
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……116, 121, 158
政府機関等の対策基準策定のためのガイドライン……23, 116
政府情報システムにおけるサイバーセキュリティに係るサプライチェーン・リスクの課題整理及びその対策のグッドプラクティス集……121
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））……162
セキュア・バイ・デザイン……28, 54, 112, 117, 125
セキュリティ・キャンプ……143, 146
セキュリティ・クリアランス制度……110, 119
セキュリティ要件適合評価及びラベリング制度（JC-STAR）……112, 125, 151, 192, 209
ゼロデイ攻撃……37
ゼロトラストアーキテクチャ……124
総合運用・監視システム（COSMOS）……122
組織における内部不正防止ガイドライン……57
ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引……117, 125

た

ダークウェブ……11, 19, 37, 43, 130, 193
第 14 次五ヵ年計画……200
耐量子計算機暗号（PQC：Post-Quantum Cryptography）……112, 164, 209
中核人材育成プログラム……145
中華人民共和国サイバーセキュリティ法……200
中小企業の情報セキュリティ対策ガイドライン……143, 171
ディープフェイク……78, 86, 92, 94, 100, 189
ディスインフォメーション（Disinformation）……91, 98, 100
データ三法……200
データ品質マネジメントガイドブック……83
デジタルオペレーショナルレジリエンス法（DORA：Digital Operational Resilience Act）……197
デジタルサービス法（DSA：Digital Services Act）……96
デジタル社会推進標準ガイドライン……121
デジタル署名……208
テレワーク……14, 29, 30
電子署名……132
特殊詐欺……137, 173
特定分野システムの IoT 製品における JC-STAR 制度活用ガイド……158
トラストサービス……132, 188
トロイの木馬（RAT：Remote Access Trojan）……53, 63, 194

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) …… 13, 25, 110, 161, 174, 186
内部不正 …… 13, 29, 54
ナラティブ(Narrative) …… 93
なりすまし …… 26, 86, 94, 96, 103, 192
二重の脅迫(二重恐喝) …… 14, 17, 19
偽・誤情報 …… 9, 91
偽情報 …… 78, 91, 118, 139
偽のウイルス感染警告 …… 58
日 ASEAN サイバーセキュリティ政策会議 …118, 187
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) …… 188
日 ASEAN 能力向上プログラム強化プロジェクト …… 188
日英サイバー対話 …… 187
日米サイバー対話 …… 186
日リトアニアサイバー協議 …… 187
日本産業標準調査会(JISC : Japanese Industrial Standards Committee) …… 206
認知戦 …… 93
ネットリテラシー向上 …… 174
ネットワーク貫通型攻撃 …… 24, 28, 127
ノーウェアランサム …… 14, 17, 21, 138

は

バイオメトリクス …… 160, 209
ハイブリッド型サイバー攻撃 …… 91, 100, 103
バックドア …… 37, 121, 194
ばらまき型の攻撃 …… 17
万博向けサイバー防御講習(CIDLE : Cyber Incident Defense Learning for EXPO) …… 148
汎用的 AI(General-purpose AI) …… 76, 77
誹謗中傷防止 …… 174
標的型攻撃 …… 18, 23, 78, 194
標的型サイバー攻撃特別相談窓口 …… 127
広島 AI プロセス …… 84
ファクトチェック …… 94, 96, 101
フィッシング …… 9, 12, 36, 57, 60, 135, 137
フェイクニュース …… 91
不正アクセス …… 11, 20, 24, 135
不正競争防止法 …… 13, 57, 130
不正送金 …… 12, 37, 58, 62, 86, 135, 139
ブレッチリー宣言 …… 84
プロテクションプロファイル(PP : Protection Profile) …… 159
米国国立標準技術研究所(NIST : National Institute of Standards and Technology) …… 34, 82, 87, 190
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) …… 21, 37, 44, 189, 192
ボイスフィッシング …… 10, 12
ボットネット …… 25, 31, 47, 132, 151

ま

マイクロセグメンテーション …… 22
マルインフォメーション(Malinformation) …… 91
ミスインフォメーション(Misinformation) …… 91

や

闇バイト …… 138, 174

ら

ランサムウェア …… 10, 13, 17, 41, 138, 193
リークサイト …… 19, 21, 44
リフレクション攻撃 …… 48, 132
リモートデスクトップ …… 14, 18, 20
ロシア・ウクライナ戦争 …… 31, 45, 92, 101, 193

著作・製作　独立行政法人情報処理推進機構（IPA）

編集責任　高柳 大輔　沖田 孝裕　小山 明美　涌田 明夫　白石 歩
井上 佳春　渋谷 環

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　奥村 明俊　大海 健太　小川 賢一
小川 隆一　沖田 孝裕　金木 陽一　金子 成徳　加納 諒也
神谷 健司　亀山 友彦　菅野 和哉　菊池 秀一　小杉 聡志
小山 明美　小山 祐平　佐藤 栄城　渋谷 環　白石 歩
新保 淳　鷲見 拓哉　銭谷 謙吾　田島 凛　辻 宏郷
豊田 亮子　長迫 智子　西尾 秀一　野村 春佳　平本 健二
冨士 愛恵里　藤井 明宏　古居 敬大　松島 伸彰　宮本 冬美
森貞 夏樹　守屋 真人　籔口 春南　山下 恵一　吉原 正人
吉本 賢樹

三菱電機株式会社　神余 浩夫
デジタル庁 戦略・組織グループ セキュリティ危機管理チーム　中村 元洋
順天堂大学 健康データサイエンス学部　満塩 尚史
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
浅見 侑太　井上 真弓　板橋 博之　伊藤 真一　江島 将和
大澤 淳　小野塚 直人　甲斐 成樹　釜谷 誠　唐亀 侑久
神田 雅透　岸野 照明　北村 弘　桐淵 直人　黒岩 俊二
桑名 利幸　佐川 陽一　貞広 憲一　篠塚 耕一　白井 綾
瀬光 孝之　高見 穣　高柳 大輔　田口 聡　田中舘 隼
田村 智和　土屋 正　遠山 真　中島 尚樹　西原 栄太郎
西村 奏一　日向 英俊　福原 聡　松岡 光　松田 修平
宮崎 卓行　安田 進　渡邉 祥樹
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・企画チーム

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
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
総務省 サイバーセキュリティ統括官室
国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所
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

2024年度は、仕事や日々の生活での生成AIの活用が本格化し、「日常が一変」したという方も多いのではないでしょうか。 その一方で、総合エンターテインメント企業がランサムウェア攻撃で多大な被害を受けた事例のように、1回のサイバー攻撃で、いままでの「日常が一変」することも起こっています。 良くも悪くも「一変する日常」に私達は対応していかないといけない、そしてその日常を支えるのは個々人や個々の組織だけでは難しいことから、サブタイトルを「一変する日常:支える仕組みを共に築こう」としました。
IPAでは2025年3月にIoT製品のセキュリティレベルを可視化する新たな制度「セキュリティ要件適合評価及びラベリング制度(JC-STAR)」を開始し、5月には適合ラベルの交付が開始されました。サブタイトル後半の日常を「支える仕組み」の一つとして、本制度が浸透し、安全なIoT機器が積極的に選ばれることで、DDoS攻撃等のサイバー攻撃の被害を減らす一助になればと思います。

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 2024 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 2025

一変する日常 : 支える仕組みを共に築こう

2025 年 9 月 30 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 © 2025 Information-technology Promotion Agency, Japan.