

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

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」を使わなければならないの？	166
セキュリティは「コスト」か「投資」か？	176



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。

(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

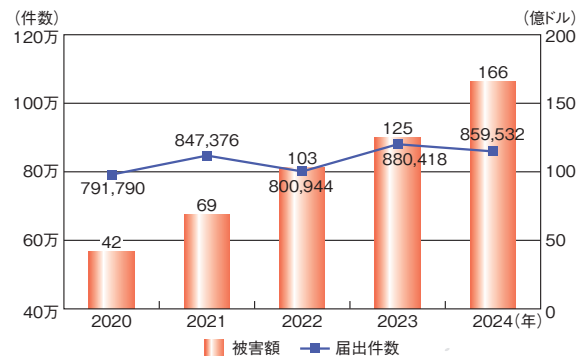


図 1-1-1 サイバー犯罪の届出件数と被害額の推移（2020～2024 年）
（出典）FBI「Internet Crime Report 2024」を基に IPA が作成

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、選挙運動の一つを標的と

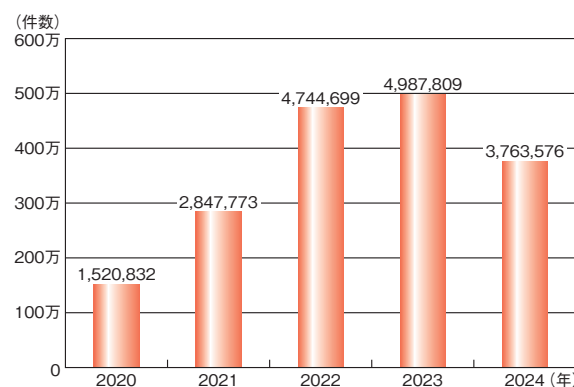
した DDoS 攻撃が数日にわたって発生し、ピーク時には 1 秒あたり 70 万件のリクエストが発生していた。同年 6 月の欧州議会選挙においても、投票日前後に複数の政治関連 Web サイトがサイバー攻撃の標的となった。特に 6 月 5 日から投票日の 6 月 6 日にかけては、オランダの二つの政治関連 Web サイトを標的とした大規模な DDoS 攻撃があり、ピーク時には 1 秒あたり 7 万 3,000 リクエストがあった。そのほか、フランス、英国、ルーマニア、南アフリカ、ポルトガルといった国でも選挙に関連して政党を標的とした DDoS 攻撃が観測された^{*12}。各国の選挙においては、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

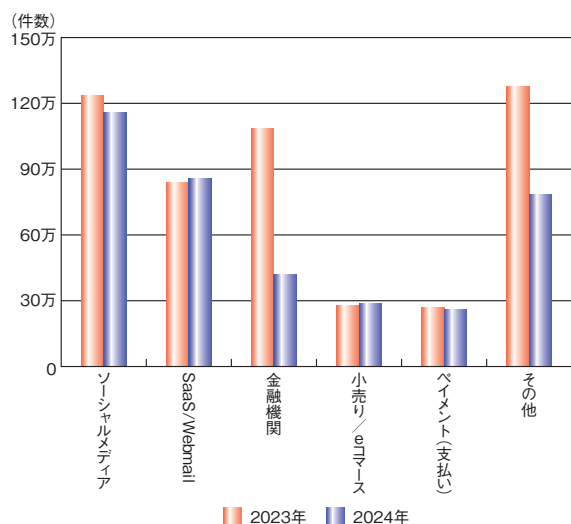
フィッシング対策の国際的な非営利団体である Anti-Phishing Working Group, Inc.（APWG）によると、2024 年に報告されたフィッシングメールに基づき特定された固有のフィッシングサイトの総数は約 376 万件であった。2018 年以降増加傾向だったが、過去最多だった 2023 年の約 499 万件から減少となった（図 1-1-2）。

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 万件的減少となった(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

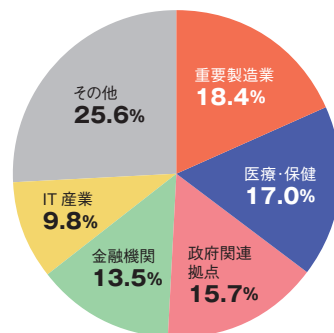
そのほか APWG の報告書では、年間をとおして、SMS を使った「スミッシング (Smishing)」や電話等の音声案内を使った「ヴィッシング (Vishing)」「(ボイスフィッシング)」ともいうといったフィッシングの増加に言及している^{*16}。APWG では、これらの手口の増加には、メールを使ったフィッシングは、高度なフィルタリング技術等によって困難になっている点や、SMS・電話ではフィルタリングはほとんど行われずユーザーに届くという、直接性の高い接触方法である点が影響していると推測している。

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}。



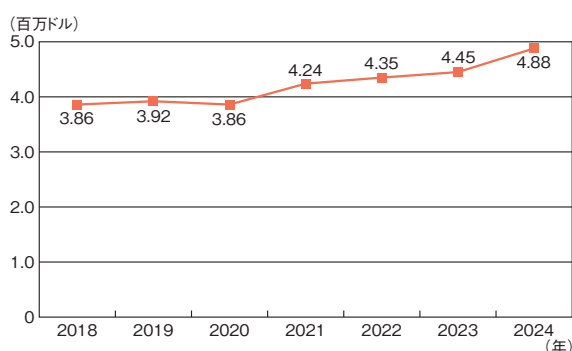
■ 図 1-1-4 ランサムウェア被害を受けた重要インフラの業種別構成比
(2024 年、n=1,403)
(出典) FBI「Internet Crime Report 2024」を基に IPA が作成

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 カ国中には欧州の国が 5 カ国含まれている。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、イタリアが続いている。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考えられた。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}。

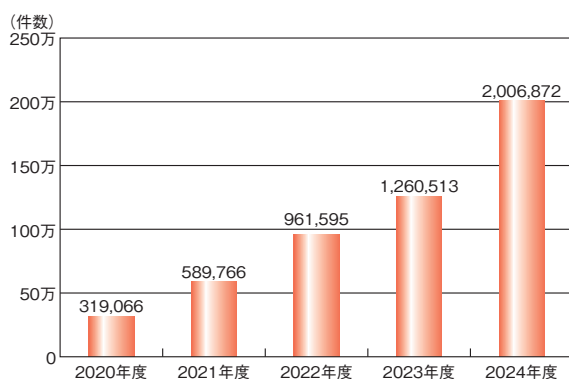
1.1.2 国内における情報セキュリティインシデント状況

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）。

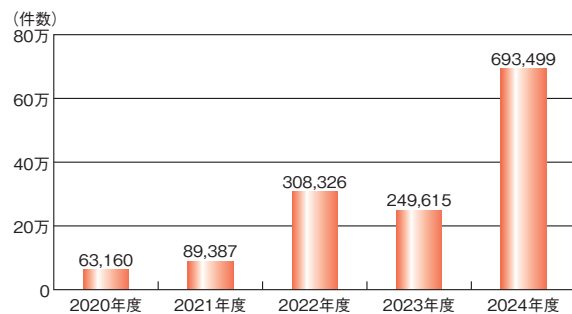


■ 図1-1-6 フィッシング報告件数(2020～2024年度)
(出典)フィッシング対策協議会「月次報告書」(2020年4月～2025年3月)を基にIPAが作成

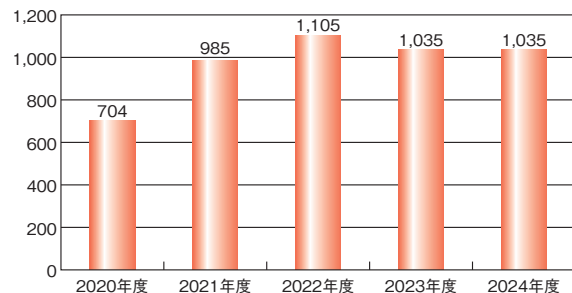
フィッシングサイトのURL件数では、2022年度をピークに2023年度は減少傾向だったものの、2024年度は再度69万3,499件と大幅な増加に転じた（図1-1-7）。

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}。

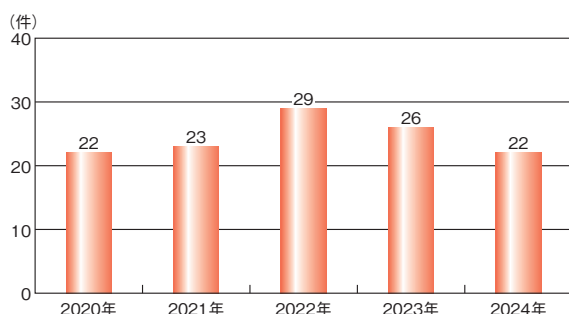
一般社団法人JPCERTコーディネーションセンター(JPCERT/CC: Japan Computer Emergency Response Team Coordination Center)の「フィッシング詐欺の現状^{※42}」では、フィッシング犯罪の特徴の一つとして「PhaaS(Phishing as a Service)」という、サービスとしてフィッシング攻撃を提供するビジネスモデルが存在していることが挙げられており、このような攻撃側の分業化も背景となり、攻撃者が特定しにくくなっていることが指摘されている。

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。

内部不正に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）。

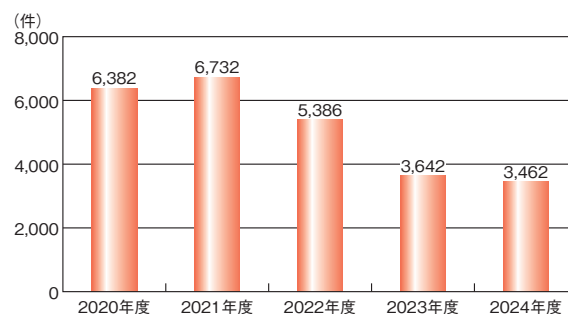


■図1-1-9 営業秘密侵害の検挙事件数(2020～2024年)
(出典)警察庁「令和6年における生活経済事犯の検挙状況等について^{*45}」を基にIPAが編集

(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での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。

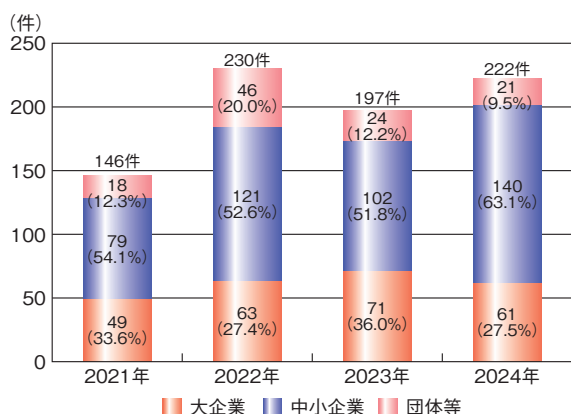
DDoS攻撃の検出数には増加が見られないものの、2024年12月末から2025年年始にかけては、日本国内において航空事業者や金融機関を狙ったDDoS攻撃が相次ぎ、多数の被害が発生した。このことを受けて、2025年2月には、内閣サイバーセキュリティセンター(NISC: National center of Incident readiness and Strategy for Cybersecurity)(現、国家サイバー統括室(NCO: National Cybersecurity Office))から、DDoS攻撃に関する注意喚起が発出された^{*48}。DDoS攻撃への対策については、平時の対策、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。

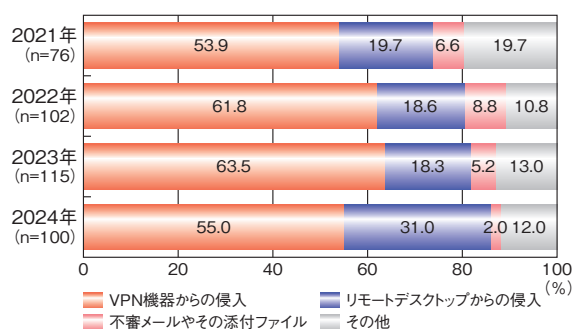
また、2024年に被害の報告があった222件のうち手



■ 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)。

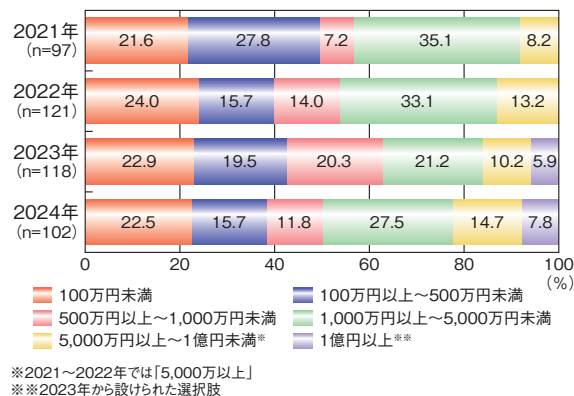


■ 図 1-1-12 ランサムウェアの感染経路(2021～2024年)
(出典)2021～2024年の警察庁資料を基に IPA が作成

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)。



■ 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 (サブ

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)。



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、データを人質にす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。

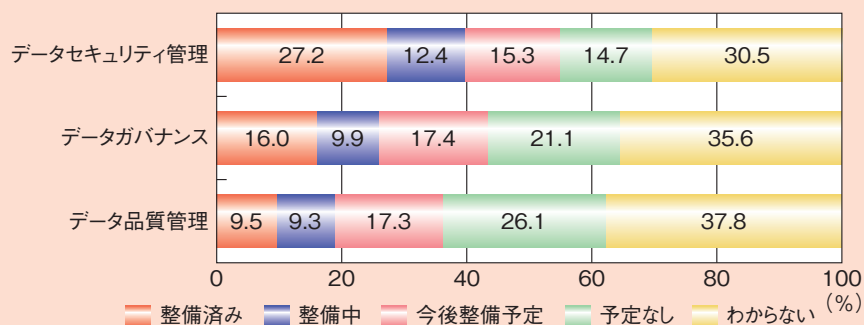


図 データマネジメントの状況(抜粋、n=798)

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う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た脅迫する「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

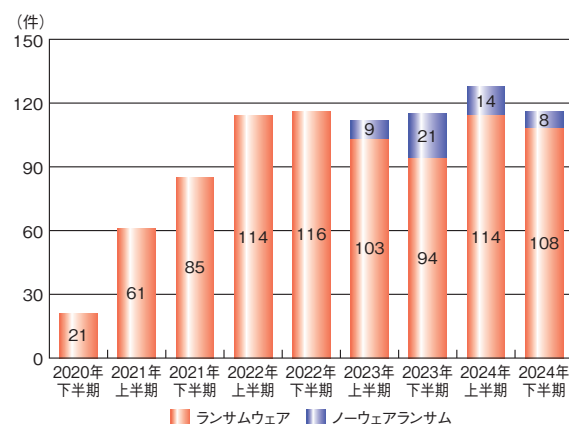
口を「ノーウェアランサム」と名付けている^{*50}。

(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

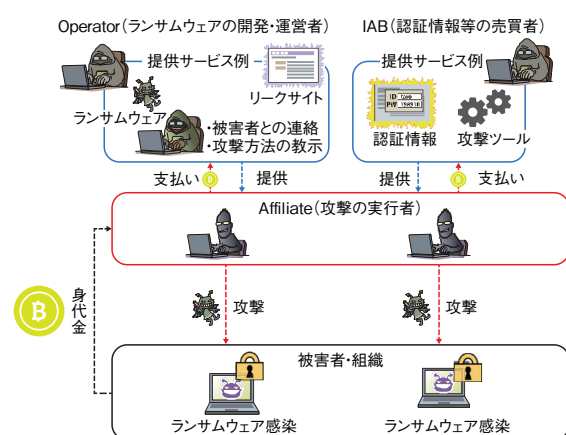
警察庁が公表した「令和 6 年におけるサイバー空間をめぐる脅威の情勢等について」(以下、警察庁資料)によると、企業・団体等におけるランサムウェア被害の報告件数は、2024 年上期が 114 件、下期が 108 件で、2022 年上期以降は継続して高い水準で推移している(図 1-2-1)。また、ノーウェアランサム被害の報告件数は、2024 年上期が 14 件、下期が 8 件である。ランサムウェア被害の報告件数と比較すると少ないが、ノーウェアランサムの統計が開始された 2023 年以降継続して被害が発生している。



■ 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、身代金の支払いにに応じてい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、社内ですべて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}

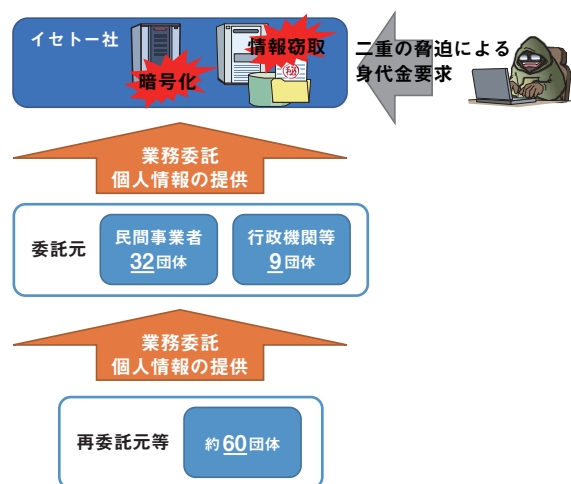
■表 1-2-1 ランサムウェア被害後の主なサービスの復旧状況
(出典)公表情報を基に IPA が作成

(b)印刷企業における被害事例

株式会社イセト (以下、イセト社) 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}。

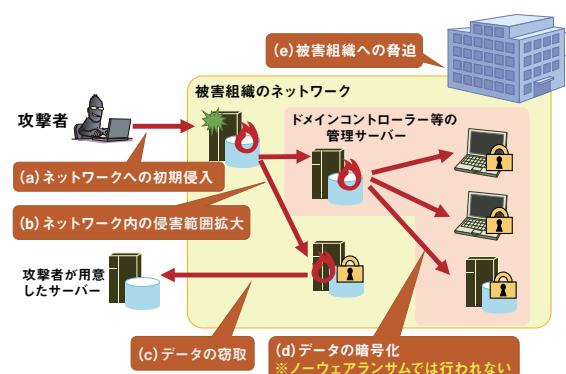
影響は更に拡大し、本事案を受け、ISMS 審査機関である BSI グループジャパン株式会社の特別審査が行われ、イセト社は取得済みの情報セキュリティマネジメントシステム認証（ISO 27001 認証）及びクラウドセキュリティ認証（ISO 27017 認証）を一時停止する旨の通知を受けている^{*77}。更に、一般財団法人日本情報経済社会推進協会（JIPDEC）より、プライバシーマーク付与を一時停止する旨の通知を受けたという^{*78}。なお、後に ISO 27001 認証及び ISO 27017 認証の一時停止は解除されている^{*79}。

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えない。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核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れ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。被害への具体的な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。

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、スパイ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。

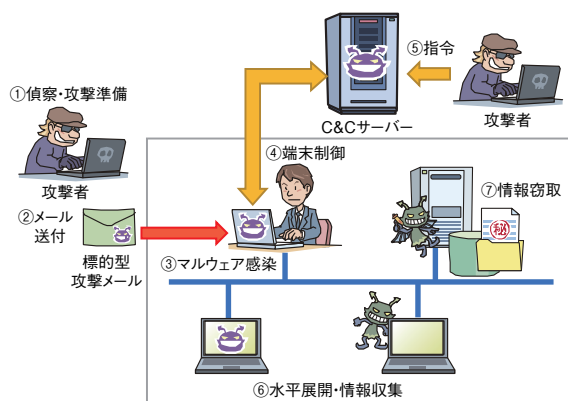
(a) 標的型攻撃メールを用いた攻撃の手口

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。

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



■ 図 1-2-5 標的型攻撃メールを用いた攻撃の流れ

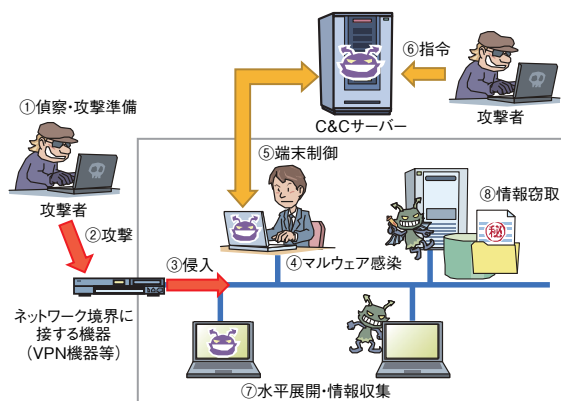
⑦情報窃取：目的の情報等を窃取する。

(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



■ 図 1-2-6 ネットワーク貫通型攻撃の流れの一例

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^{※100} APT 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}。

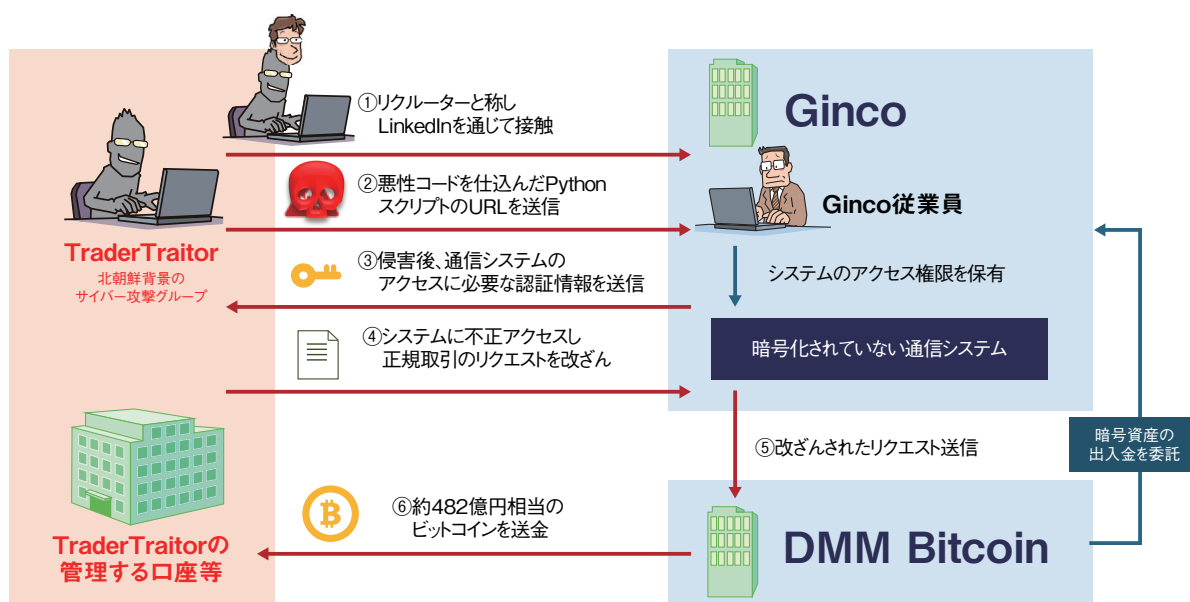
また、同年9月、米国司法省は、中国の国家が支援する「Flax Typhoon」と呼ばれる攻撃グループによって侵害された20万台超の消費者向け機器からなるボットネットを無害化したと発表した^{*109}。同日、FBI等は、Flax Typhoonが、SOHO(Small Office Home Office)ルーターやIoT機器を含むインターネットに接続された機器の既知の脆弱性^{*110}を悪用して26万台超の機器からなるボットネットを構築し、マルウェアの配信やDDoS攻撃に利用しているとするセキュリティアドバイザリーを公表した^{*111}。これらに関連し、2025年2月、NISCは、エッジ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 Gincó 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なか検討し、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、仕事を従来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 Manage-

ment）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 年年初には、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 月の日本・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 1-28)。

①ボットネットの構築

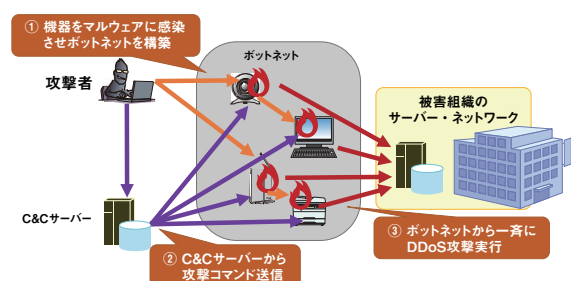
コンピューターや、家庭用ルーター、ネットワークカメラ等のインターネットに接続されている IoT 機器にマルウェアを感染させ、攻撃インフラ(ボットネット)を構築する。

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となる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

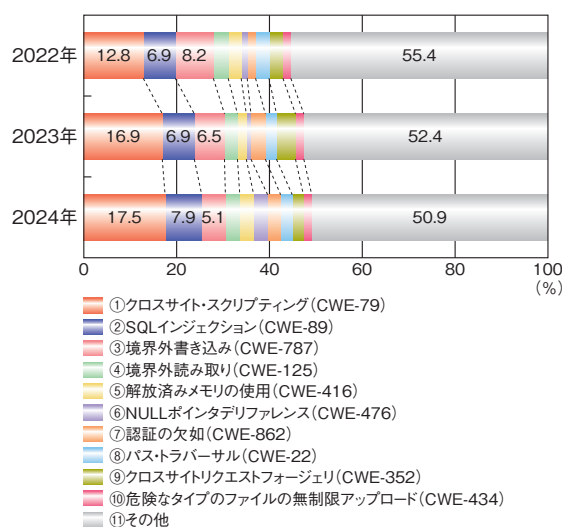


図 1-2-9 JVN iPedia における脆弱性対策情報の CWE 別割合 (2022 ~ 2024 年)

(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。

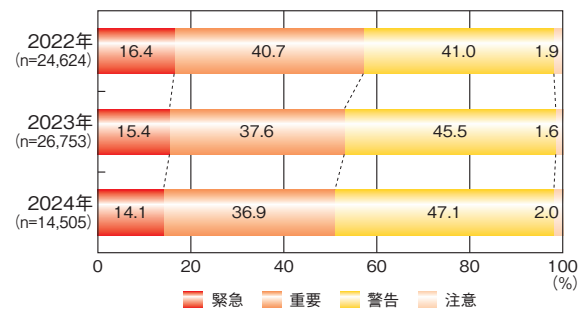
CVSS のスコアは数値が大きい程、深刻度が高くなる。CVSS v3 では基本評価基準(BM:Base Metrics)を基に評価した基本値によって、深刻度が「緊急」「重要」「警告」「注意」「なし」の 5 段階に分けられる。

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。

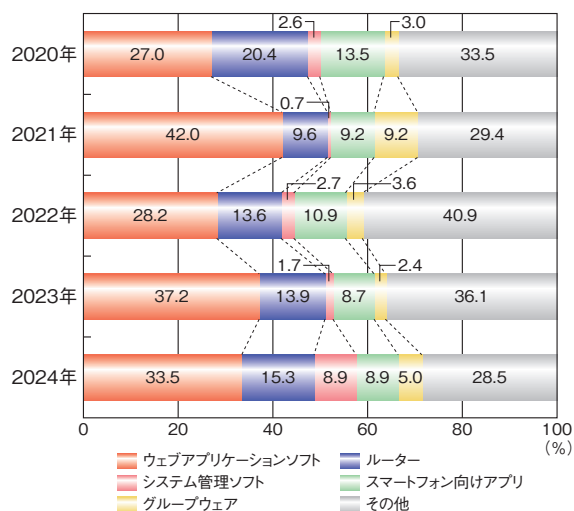
2024 年にパートナーシップへ届け出された脆弱性の件数、及び届出受付開始(2004 年 7 月 8 日)からの累計は、ソフトウェア製品が 296 件 (累計 5,960 件)、Web サイトが 336 件 (累計 1 万 3,326 件)、合計 632 件 (累計 1 万 9,286 件) であった(表 1-2-3)。

	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



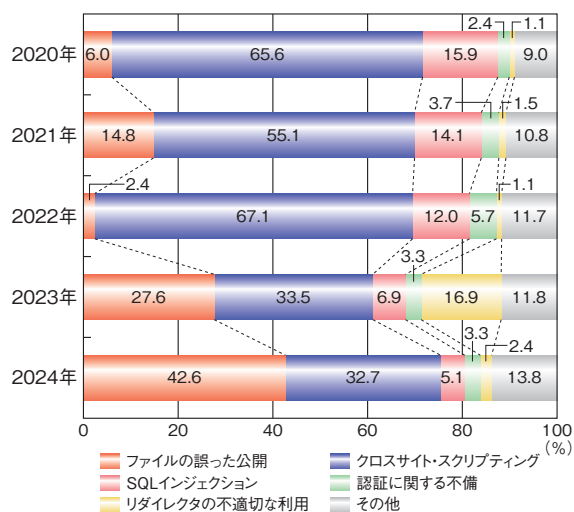
■ 図 1-2-11 ソフトウェア製品における脆弱性の届出の製品種類別割合 (2020～2024 年)
(出典) パートナシップへの届出状況を基に IPA が作成

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



■ 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) パートナシップへの届出状況を基に IPA が作成

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。

「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}。

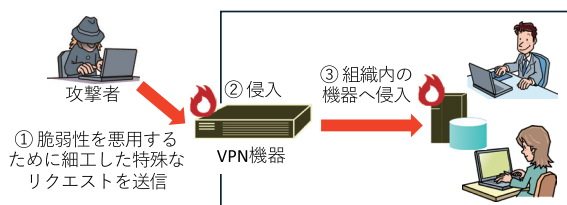
2024年4月12日、Palo Alto Networks, Inc. (以下、Palo Alto 社) は、同社のファイアウォール用オペレーティングシステム PAN-OS の GlobalProtect 機能に関する脆弱性 (CVE-2024-3400^{*164}) を公開した。同脆弱性が悪用された場合、認証されていない遠隔の第三者によって、root 権限 (管理者権限) で任意のコードが実行されるおそれがある。脆弱性の深刻度を示す CVSS v3 基本値は 10.0 で、最も深刻度が高い「緊急」と評価された^{*165}。

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}。

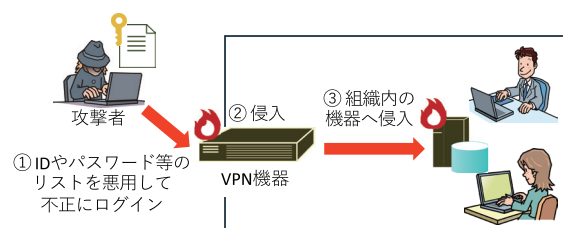
Palo Alto 社は、同年4月14日から同年4月18日にかけて、順次、本脆弱性を修正するための Hot Fix (緊急の修正プログラム) を公開し、ワークアラウンド (応急措置) や緩和策が適用されている場合であっても、ソフトウェアのアップデートを早急に行うことを強く推奨している^{*164}。

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。

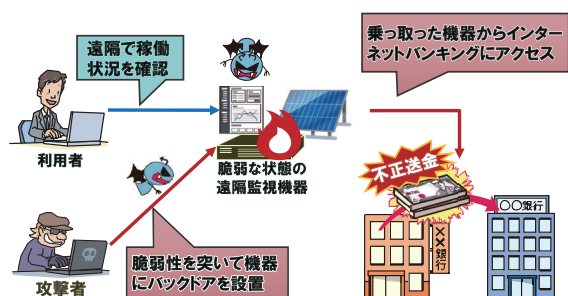


■ 図 1-2-14 インターネットやダークウェブから入手した情報を悪用することによって侵入する方法

(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 ヶ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カ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カ国の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月によりやく復旧した。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、Ascension 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、法執行機関や課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

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より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。侵入の原因は複数と考えられるが、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。

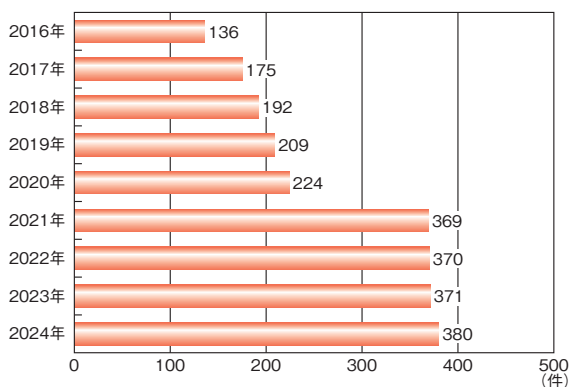
表1-2-5（次ページ）に、2024年に公にされた、生産や重要サービスに影響を与えたサイバー攻撃のインシデント事例を示す。

(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	発生日	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の生産が停止した ^{*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のチャン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^{*218}。

(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^{*220}と報告している。

(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^{*221}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のまま、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。

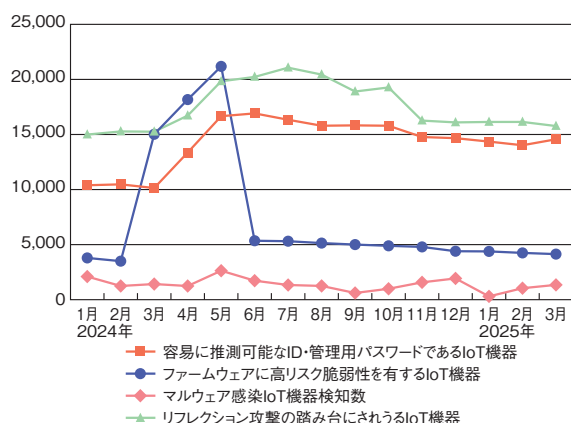
2024 年 4 月以降、活動を拡大し、「ID・パスワードに脆弱性がある IoT 機器の調査 (特定アクセス行為)」と「既にマルウェアに感染している IoT 機器の情報提供」に加えて、「ファームウェアに脆弱性がある IoT 機器の調査」や IoT 機器のメーカーやその他セキュリティ関係機関等との連携強化に取り組んでおり、IoT 機器の観測状況として、以下に示す統計情報を公開している。

- 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 ヶ月の合計件数)
- 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 ヶ月の合計件数)
- 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 年間をととして観測された。
- 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、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 (友訊科技股份有限公司)	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 : 台湾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} 。	
TP-Link Technologies Co., Ltd. (普联技术有限公司)	2024 年 9 月 30 日、CISA は DIR-820 の脆弱性 (CVE-2023-25280) を KEV に追加 ^{*252} 。	✓
	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} 。	
NETGEAR, Inc.	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} 。	
	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} 。	✓
Linksys Holdings, Inc.	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} 。	
	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. (華碩電腦股份有限公司)	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用ライセン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 (友訊科技股份有限公司)	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垂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 (陸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

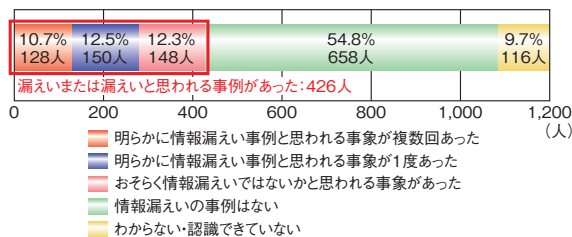
者が退職後に在職中に得ていた情報を漏えいする行為等を含む）、及び消去・破壊等の違法行為と、情報セキュリティに関する内部規程やルールへの違反、ミス等の違法とはいえない行為の両方を内部不正として扱う^{※350}。

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。

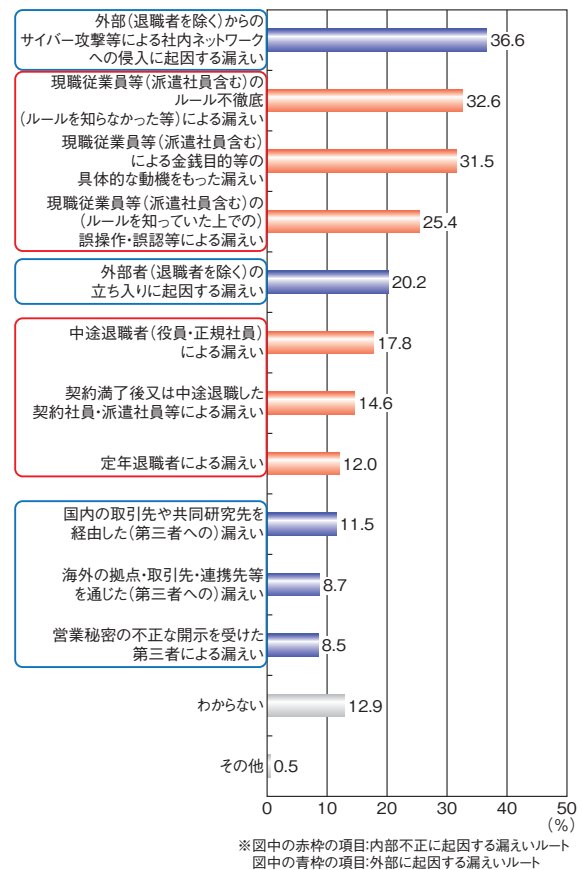
IPAが実施した「企業における営業秘密管理に関する実態調査2024」^{※351}では、図1-2-18に示すように、回答者1,200人のうち426人（35.5%）が過去5年間に営業秘密の漏えいまたは漏えいと思われる事例があったと回答した。



■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。

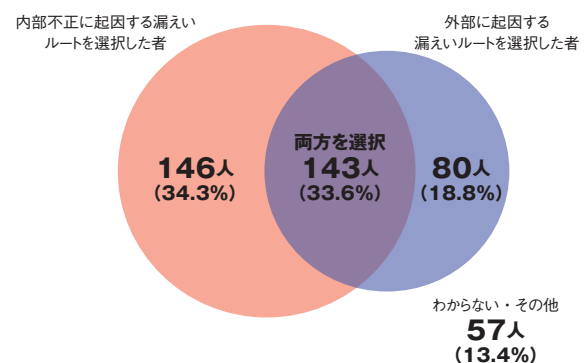
外部からのサイバー攻撃等によるネットワーク侵入に起因する漏えいに次いで、内部不正に起因する漏えいルートである現職従業員等（派遣社員含む）による漏えいが多く、「外部者（退職者を除く）の立ち入り」に起因する漏えい」をはさんで、中途退職者（役員・正規社員）、契約満了後または中途退職した契約社員・派遣社員等、及



■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

び定年退職者による漏えいが多かった。

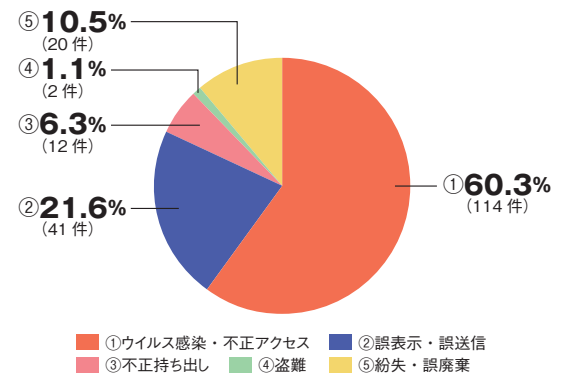
図1-2-19の設問への回答を基に回答者を、内部不正に起因する漏えいルートのみを選択した者、外部に起因する漏えいルートのみを選択した者、両方を選択した者、「わからない」「その他」を選択した者に分類した結果を図1-2-20に示す。内部不正に起因する漏えいルートのみを選択した者は146人（34.3%）、外部に起因する漏えいルートのみを選択した者は80人（18.8%）、両方



■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、競業禁止義務の有無や内容を規定 ※競業禁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
情報システム・ 管理部門	技術面	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
		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

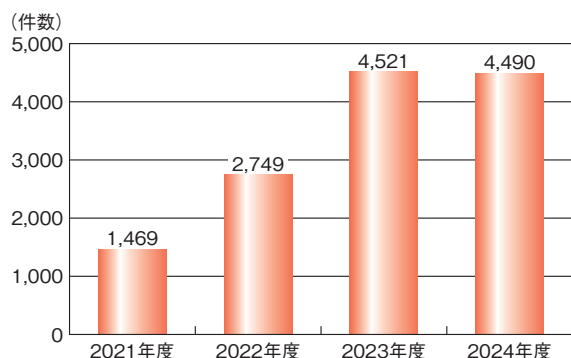
■表 1-2-11 内部不正による情報漏えいに関連する法規制の例^{※366}

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。

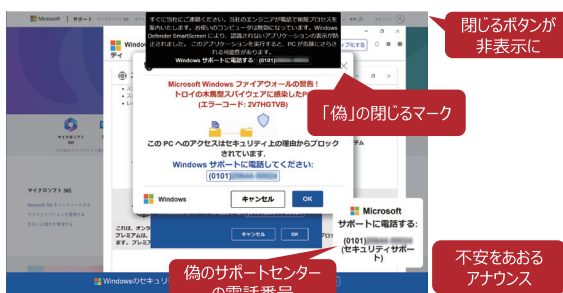
(a) 手口

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の画面上に表示される。そのため、対処はブラウザを閉じるだけである。しかし、偽の警告は、ブラウザ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のフルスクリーン表示を解除した上でブラウザを閉じる^{*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引の有无を確認し、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。

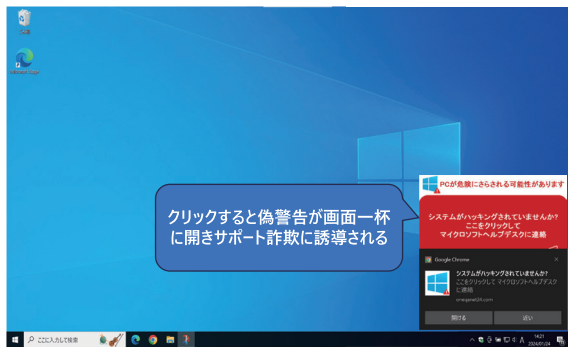
(c) 対策

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。

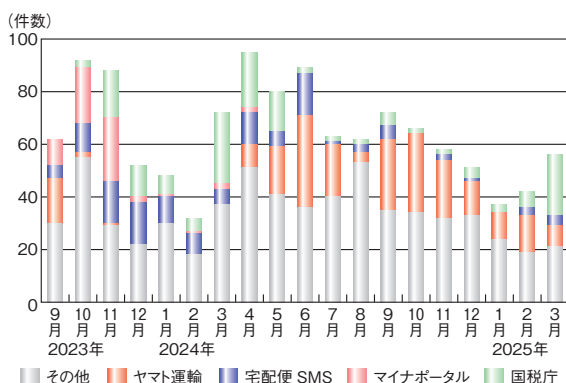
(c) 対策

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。

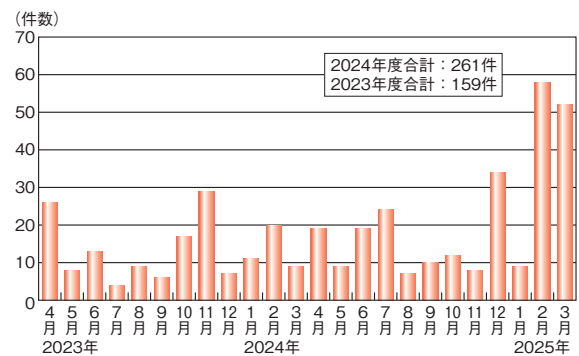
国税庁をかたるものについては、2024 年も引き続き「税金が納められていない」「国税還付金の電子発行を開始しました。」という内容が続いている。手口の変化は少ないため、「情報セキュリティ白書 2024」の「1.2.6 (2) (a) 国税庁をかたるメール」を参照いただきたい。

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。

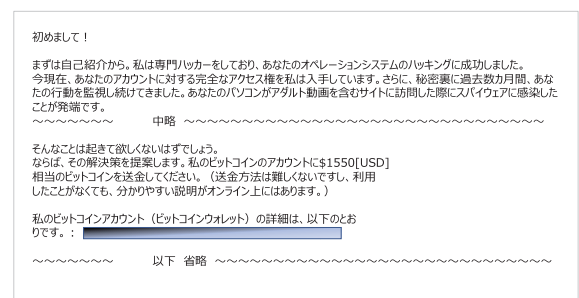
(b) 暗号資産を要求する脅迫メールの手口とその対処

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



■図 1-2-31 脅迫メールの例

メールに書かれている内容はすべて根拠のない嘘の情報である。

実際にビットコインを送金してしまったという被害相談の事例はほとんどないが、文章が自然な日本語で書かれており、メールの送信元が、メール受信者自身のアドレスから送信されているように詐称されていることもあるので、本当に起こっているのではないかと心配して相談される場合が多い。

送信元アドレスは技術的に詐称が可能であり、送信元アドレスを詐称することで迷惑メールのフィルタリングを回避することや、あたかもメールアカウントをハッキングしたと信じさせることが目的と考えられる。対処としては、無視して削除すれば問題ない。また、現在使用しているパスワードが書かれていた場合は、すぐにパスワードを変更し、併せて、そのパスワードを使っていたサービスへの不正ログインがないか確認することを推奨する。パスワードは登録していた他のサービスから漏えいした可能性があるが、メールに書かれているような、自分のパソコンから盗まれたというものではない。

(c) メールを悪用した手口への対策

フィッシングメールや脅迫メールは目に触れないようにすることが対策になる。

フィッシングメールや脅迫メールは、迷惑メールフィル

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）。

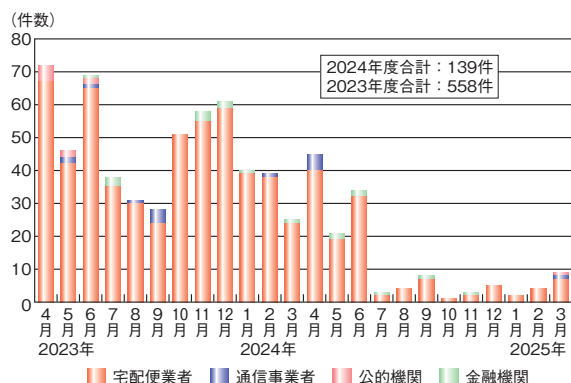


図 1-2-32 偽 SMS に関する月別相談件数推移 (2023 ~ 2024 年度)

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}」を運営しているトピラス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。



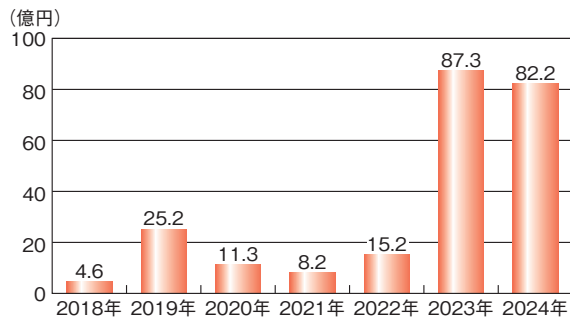
図 1-2-33 金融機関をかたるフィッシングサイトに口座情報を入力させる例

SMS を悪用した手口だけではなく、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られる。



C O L U M N

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 2025 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]

※ 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 IJ 社：観測レポート <https://wizsafe.ij.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rend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-clOp-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rend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rend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://cybersrc.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：イセトのランサムウェ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 イセトも被害 <https://www.nikkei.com/article/DGXZQQUE108SD0Q5A210C2000000/> [2025/6/24 確認]

※ 81 トrend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ボ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.jpccert.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 goes 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rend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rend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ponsored」(state-sponsored)、「ネーションバックド」(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/ug65p9000000nkvmm-att/000103970.pdf> [2025/6/19 確認] (標的に改変・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_window_ssandbox.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/technical_20250317.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/hjuojm0000005510->

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/hjuojm00000055i0-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/ps6vr7000000jft.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.jpccert.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.jpccert.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)導入ガイドンス～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/jina/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-hacktivism-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/24/1/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.jpccert.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://jvnadb.jvn.jp/apis/index.html> [2025/6/13 確認]

※ 181 <https://jvnadb.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/](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 Treatment Facility Returns to Regular Operations <https://www.arkcity.org/city-manager/page/arkansas-city-water-treatment-facility-returns-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-95cd980a9f45112f0dce488233eec9c> [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/Iromw3x9/> [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.com/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つであり、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]

Clarity Ltd. : Inside a New OT/IoT Cyberweapon: IOCONTROL <https://clarity.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 IJ 社 : wizSafe Security Signal <https://wizsafe.ij.ad.jp/> [2025/6/19 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越えるパケット : 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 HMAP <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-2024-14622/44340/44341/44342 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 : JVN#91401812, Multiple TP-Link products vulnerable to OS command injection <https://jvn.jp/en/vu/JVN#91401812/> [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 Thottsploity : CVE-2024-53375 TP-Link Archer router series Authenticated RCE <https://thottsploity.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/yymkyu/CVE/tree/main/CVE-2024-33788> [2025/6/18 確認]

CoreSecurity OT/ICS Research Team : CVE-2024-33789 <https://github.com/yymkyu/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 'apmcfupload' 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/qa-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/qa-23-64> [2025/6/18 確認]

※ 278 QNAP 社 : QSA-23-47, Vulnerability in QTS, QuTS hero and QuTScld <https://www.qnap.com/en/security-advisory/qa-23-47> [2025/6/18 確認]

QNAP 社 : QSA-23-30, Vulnerability in QTS, QuTS hero and QuTScld <https://www.qnap.com/en/security-advisory/qa-23-30> [2025/6/18 確認]

QNAP 社 : QSA-24-05, Multiple Vulnerabilities in QTS, QuTS hero and QuTScld <https://www.qnap.com/en/security-advisory/qa-24-05> [2025/6/18 確認]

※ 279 QNAP 社 : QSA-24-03, Vulnerability in Qsync Central <https://www.qnap.com/en/security-advisory/qa-24-03> [2025/6/18 確認]

※ 280 QNAP 社 : QSA-23-57, Multiple Vulnerabilities in QTS, QuTS hero and QuTScld <https://www.qnap.com/en/security-advisory/qa-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, QuTScld, myQNAPcloud, and myQNAPcloud Link (PWN2OWN 2023) <https://www.qnap.com/en/security-advisory/qa-24-09> [2025/6/18 確認]

※ 283 watchTower Labs : QNAP QTS - QNAPping At The Wheel (CVE-2024-27130 and friends) <https://labs.watchtower.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/qa-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/qa-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/qa-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/qa-24-49> [2025/6/18 確認]
※ 288 QNAP 社 : QSA-24-50, Vulnerability in License Center <https://www.qnap.com/en/security-advisory/qa-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 Revision :: 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 サイファーム株式会社 : 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-12d6b683e67c80c49ficc9214c239a07> [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/hpsc/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 Advisory - 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 : 陸泰安控聲明 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-iphone-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.com/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.com/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.com/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/oday/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-ajj3-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/tradeseecret2024.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 東急リパブル株式会社：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」同業他社ヘデータ 6500 件持ち出し 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バクト: 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,\(法第178条\)。](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、競業禁止義務違反等)、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/an shin/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/an shin/reports/2025q1outline.html> [2025/6/12 確認]

※ 370 <https://www.ipa.go.jp/security/an shin/attention/2024/mgdayori20241119.html> [2025/6/12 確認]

※ 371 <https://www.ipa.go.jp/security/an shin/measures/f55m8k>

00000047km-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? - 事例を学び落着いて対処できるようにしよう - <https://www.ipa.go.jp/security/an shin/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/an shin/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/an shin/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/an shin/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/an shin/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/an shin/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/an shin/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://an shin-security.docomo.ne.jp/sms/index.html> [2025/6/12 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>



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/>



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>



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/



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!」

<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

<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ー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

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>



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>



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て学べる

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～



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(AMAI) 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
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) 導入ガイド
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 Combat 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 Infection 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
ジャックカル	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方法	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	セキュア・バイ・デザイン	28, 54, 112, 117, 125
情報処理安全確保支援士(登録セキスベ)	118, 127, 142, 144	セキュリティ・キャンプ	143, 146
情報セキュリティ安心相談窓口	58	セキュリティ・クリアランス制度	110, 119
情報セキュリティ早期警戒パートナーシップ	35, 128	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
情報セキュリティマネジメント試験	144	ゼロデイ攻撃	37
情報セキュリティマネジメントシステム(ISMS : Information Security Management System)	207	ゼロトラストアーキテクチャ	124
情報戦	91, 93	総合運用・監視システム(COSMOS)	122
情報操作型サイバー攻撃	91, 93, 100	組織における内部不正防止ガイドライン	57
情報漏えい	8, 10, 13, 19, 54	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
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	た	
水平展開	22, 23, 36	ダークウェブ	11, 19, 37, 43, 130, 193
スマートカード	158	第 14 次五年計画	200
「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	耐量子計算機暗号(PQC : Post-Quantum Cryptography)	112, 164, 209
スマートシティセキュリティガイドライン	133	中核人材育成プログラム	145
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	中華人民共和国サイバーセキュリティ法	200
スミッシング(Smishing)	10	中小企業の情報セキュリティ対策ガイドライン	143, 171
制御システム(ICS : Industrial Control System)	39, 145, 172, 210	ディープフェイク	78, 86, 92, 94, 100, 189
制御システムのセキュリティリスク分析ガイド	46, 172	ディスインフォメーション(Disinformation)	91, 98, 100
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	データ三法	200
脆弱性	34, 44, 47, 82, 113, 128	データ品質マネジメントガイドブック	83
脆弱性対処に向けた製品開発者向けガイド	54	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
生成 AI(Generative AI)	77, 92, 130, 139, 173, 185	デジタルサービス法(DSA : Digital Services Act)	96
生成 AI プロファイル	82	デジタル社会推進標準ガイドライン	121
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	デジタル署名	208
政府機関等の対策基準策定のためのガイドライン	23, 116	テレワーク	14, 29, 30
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	電子署名	132
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	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
プレッチリー宣言	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 井上 佳春	沖田 孝裕 渋谷 環	小山 明美	涌田 明夫	白石 歩
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 鷺見 拓哉 銭谷 謙吾 田島 凜 辻 宏郷 豊田 亮子 長迫 智子 西尾 秀一 野村 春佳 平本 健二 富士 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 藪口 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 穰 高柳 大輔 田口 聡 田中 館 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 渡邊 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				

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のでしょうか。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版を記載しています。

例「(出典)《組織名等》『《文書名等》』を基に IPA が編集」

例「(出典)《組織名等》『《文書名等》』を基に IPA が作成」

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

例「《組織名等》『《文書名等》』」

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

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

- ・ 本白書は 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、TM または [®] マークは明記していません。
- ・ 本白書に掲載しているグラフ内の数値の合計は、小数点以下の端数処理により、100% にならない場合があります。

情報セキュリティ白書 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