情報セキュリティ白書

Information Security White Paper

2026

サイバー防御新時代：諸刃の進化に備えよ



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

「情報セキュリティ白書2026」の刊行にあたって

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

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

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

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

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

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

2026年9月

独立行政法人情報処理推進機構（IPA）

理事長 齊藤 裕

目次

序章　2025年度の情報セキュリティの概況 …… 6

第1章 国内外のサイバー脅威の動向 …… 8

1.1　2025年度に観測されたインシデント状況 …… 8

1.1.1　世界におけるサイバーセキュリティインシデント状況 …… 8
1.1.2　国内におけるサイバーセキュリティインシデント状況 …… 14

1.2　インシデント事例や脆弱性・攻撃の動向と対策 …… 19

1.2.1　ランサム攻撃 …… 19
1.2.2　標的型攻撃 …… 27
1.2.3　DDoS攻撃 …… 34
1.2.4　情報システムの脆弱性を悪用した攻撃 …… 37
1.2.5　不正アクセスや内部不正による情報漏えい …… 42
1.2.6　個人を狙う騙しの手口 …… 46
1.2.7　企業・組織を狙う騙しの手口 …… 51

第2章 サイバー空間を巡る動向 …… 62

2.1　サイバー安全保障関連施策の状況 …… 62

2.1.1　能動的サイバー防御の実現に向けた取り組み …… 62
2.1.2　経済安全保障関連施策の状況 …… 66

2.2　AIの安全性確保の取り組み …… 69

2.2.1　AIの発展と社会への普及 …… 69
2.2.2　AIのリスク …… 70
2.2.3　AIの安全性とガバナンス …… 76
2.2.4　AIのセキュリティ …… 79

2.3　偽・誤情報対策の動向 …… 88

2.3.1　偽・誤情報の定義 …… 88
2.3.2　偽・誤情報の最新情勢 …… 89
2.3.3　2025年度の注目事例 …… 91
2.3.4　偽・誤情報への対策の動向 …… 93
2.3.5　状況のまとめと今後の見通し …… 95

第3章 国内の政策及び取り組みの動向 106

3.1 国内のサイバーセキュリティ政策の状況 106

3.1.1 政府の政策動向 106
3.1.2 経済産業省の政策 114

3.2 サイバーセキュリティ人材の現状と育成 122

3.2.1 サイバーセキュリティ人材を取り巻く現状と課題 122
3.2.2 サイバーセキュリティ人材育成のための国家試験、国家資格制度 125
3.2.3 セキュリティ人材育成のための活動 126

3.3 製品・サービスの評価・認証制度、及び暗号技術の動向 133

3.3.1 セキュリティ要件適合評価及びラベリング制度（JC-STAR） 133
3.3.2 ITセキュリティ評価及び認証制度（JISEC） 138
3.3.3 政府情報システムのためのセキュリティ評価制度（ISMAP） 139
3.3.4 暗号技術の動向 141

3.4 中小企業のサイバーセキュリティ対策強化の取り組み 145

3.4.1 サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度） 145
3.4.2 中小企業のサイバーセキュリティ対策の課題とそれらに対する施策 147
3.4.3 中小企業向け支援策 151

第4章 国際的な政策及び取り組みの動向 160

4.1 国際的なサイバーセキュリティ政策の状況 160

4.1.1 国際社会と連携した日本の取り組み 160
4.1.2 米国の政策 165
4.1.3 欧州の政策 172
4.1.4 中国の政策 180
4.1.5 アジア太平洋地域でのCSIRTの動向 183

4.2 国際標準化活動 188

4.2.1 様々な標準化団体の活動 188
4.2.2 情報セキュリティ、サイバーセキュリティ、プライバシー保護関係の規格の標準化（ISO/IEC JTC 1/SC 27） 189

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

コラム

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

2026

情報セキュリティ白書

●序章　2025年度の情報セキュリティの概況

●第1章　国内外のサイバー脅威の動向

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

●第2章　サイバー空間を巡る動向

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

●第3章　国内の政策及び取り組みの動向

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

●第4章　国際的な政策及び取り組みの動向

4.1　国際的なサイバーセキュリティ政策の状況
4.2　国際標準化活動

序章

2025年度の情報セキュリティの概況

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

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

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

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

国際的には、国家を背景とするサイバー攻撃が引き続き警戒された。2025 年 8 月には APT 攻撃グループ「Salt Typhoon」によるサイバー攻撃に関する国際アドバイザリーが共同署名の形で公表された。サイバー攻撃は、機密情報の窃取にとどまらず、通信基盤や重要サービスへの影響を通じて、国家安全保障や経済安全保障にも関わる問題となっている。こうした情勢のもと、国際的な連携と情報共有の重要性は一層高まっている。

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

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

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

2025年度の主なインシデント・事件・政策・イベント

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

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

第1章
国内外のサイバー脅威の動向

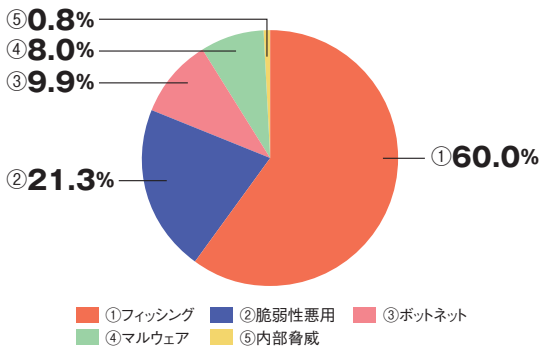
2025 年度も、地政学的な緊張の高まり、国家間の対立を背景に、社会インフラ等を標的とした国家支援型のサイバー攻撃が観測された。また、民間企業の事業継続を揺るがす侵入型ランサム攻撃も引き続き発生した。更に 2025 年度には、AI が急速に普及した一方で、攻撃者による悪用も進み、攻撃の自動化等、様々な段階で AI が用いられるようになった。SNS を悪用した巧妙な騙しの手口による金銭の詐取も横行した。本章では、国内外で観測された主なインシデント、攻撃手法、対策について解説する。

1.1 2025年度に観測されたインシデント状況

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

1.1.1 世界におけるサイバーセキュリティインシデント状況

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



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

(1) 注目すべき世界的な傾向

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

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

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

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

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

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

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

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

(2) ランサム攻撃の状況

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

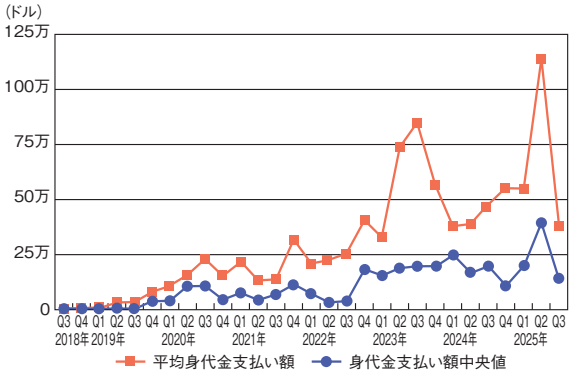
英国のサイバーセキュリティ企業である NCC Group は、傘下の Fox-IT とともに公表した「Annual Cyber Threat Intelligence Report 2025[※6]」において、2025 年の世界のランサム攻撃の件数が前年比 50% 増加し、主要な攻撃グループは「Qilin」「Akira」「ClOP」であったと分析している。また、攻撃対象の 28% を工業・産業部門が占めたこと、攻撃対象地域の 56% を北米が占めたこと等から、被害が特定の業種及び地域に集中する傾向も示されている。

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

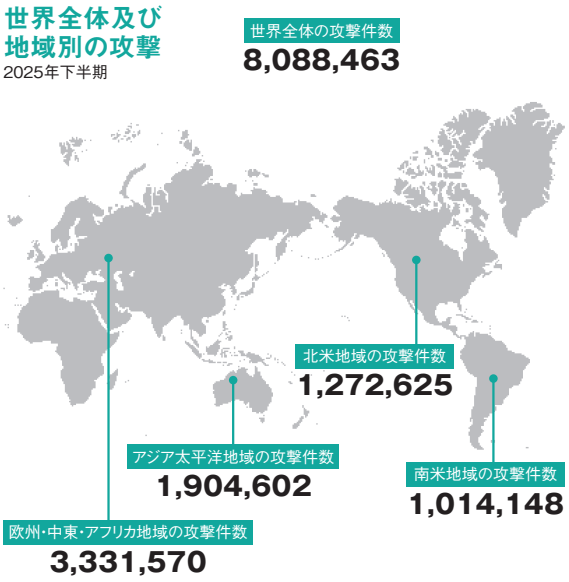
英国のサイバーセキュリティ企業である Sophos Ltd.（以下、Sophos 社）は、年次レポート「The State of Ransomware 2025[※7]」において、攻撃の 50% でデータ暗号化が発生し、暗号化被害を受けた組織の 28% ではデータ窃取も確認されたとしている。また、ランサム攻撃の被害を受けた組織の 49% がデータ復旧のため身代金を支払い、この割合は前年の 56% から 7 ポイント低下している。

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

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



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



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

(3) DDoS 攻撃の状況

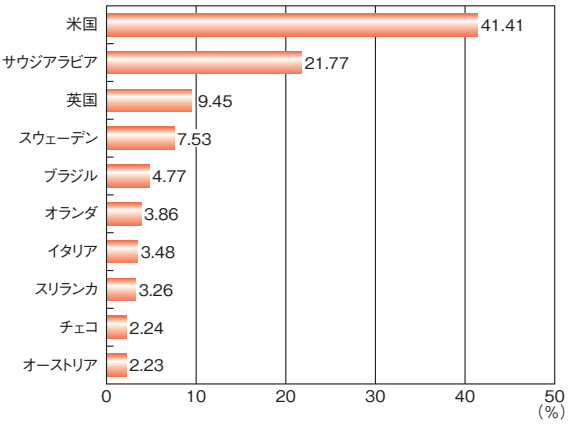
2025 年の世界における DDoS 攻撃は、件数及び規模の双方で高水準に推移し、インターネット基盤や重要サービスの可用性を脅かす主要なサイバー脅威であった。

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

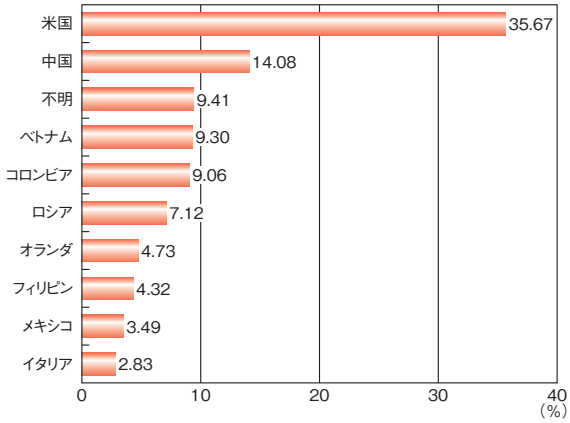
米国のサイバーセキュリティ企業である NetScout Systems, Inc.（以下、NetScout 社）の「DDoS Threat Intelligence Report Issue 16※12」によると、2025 年下半期だけで世界全体の DDoS 攻撃は、約 809 万件であったという。このうち、北米地域が約 127 万件、南米地域が約 101 万件、欧州・中東・アフリカ地域が約 333 万件、アジア太平洋地域が約 190 万件だった※13（図 1-1-3）。NetScout 社は、攻撃者が AI を攻撃の運用に取り込みつつ、NTP（Network Time Protocol）や DNS（Domain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

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

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



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



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

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

(4) フィッシングの状況

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

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

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

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

(5) 情報漏えいインシデントの状況

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

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

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

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

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

(6) 地域別の傾向

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

(a) 南北アメリカ地域の傾向

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

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

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

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

(b) アジア太平洋地域の傾向

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

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

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

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

(c) 欧州・中東・アフリカ地域の傾向

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

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

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

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

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

(d) 脅威活動の地域横断性

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

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

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

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

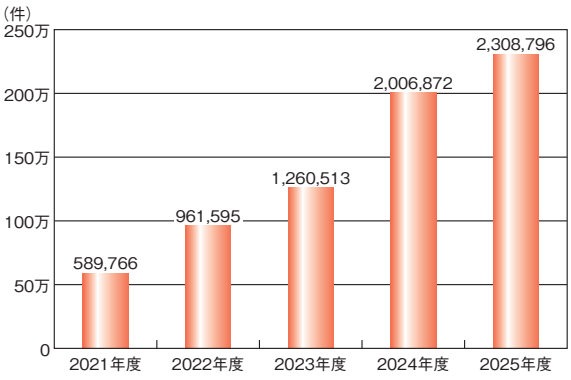
1.1.2 国内におけるサイバーセキュリティインシデント状況

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

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

(1)フィッシングによる被害

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

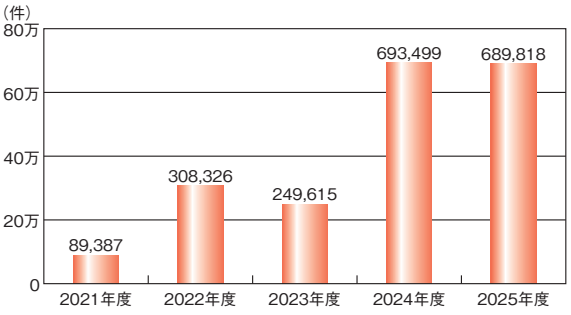


■図 1-1-6　フィッシング報告件数(2021 ～ 2025 年度)
(出典)フィッシング対策協議会「月次報告書」(2021 年 4 月～ 2026 年 3 月)を基に IPA が作成

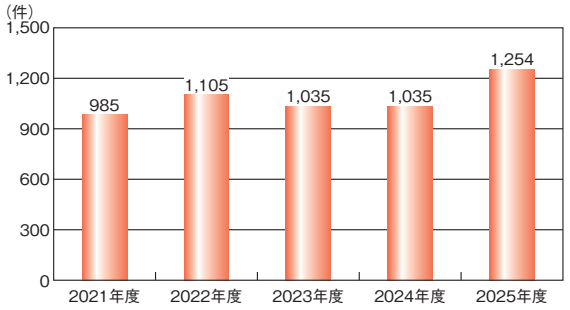
2025 年度のフィッシングサイトの URL 件数は 68 万 9,818 件と、前年度の 69 万 3,499 件に比べ微減となったが、2023 年度の 24 万 9,615 件と比べると、約 2.8 倍と高止まりしている(図 1-1-7)。

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

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

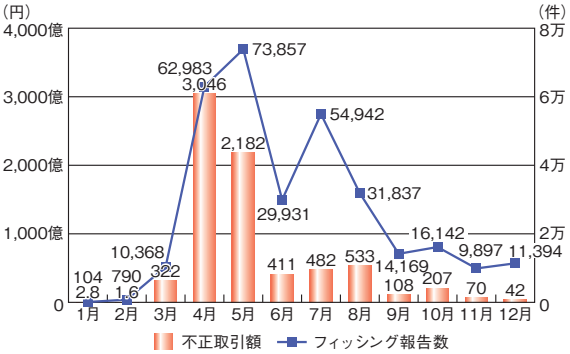


■図 1-1-7　フィッシングサイトの URL 件数(2021 ～ 2025 年度)
(出典)フィッシング対策協議会「月次報告書」(2021 年 4 月～ 2026 年 3 月)を基に IPA が作成



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

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

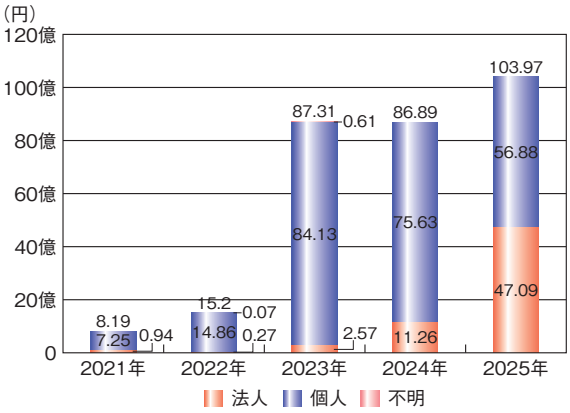


■図 1-1-9　証券会社をかたる不正取引額及びフィッシング報告数
(2025 年 1 月～ 2025 年 12 月)
(出典)「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

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

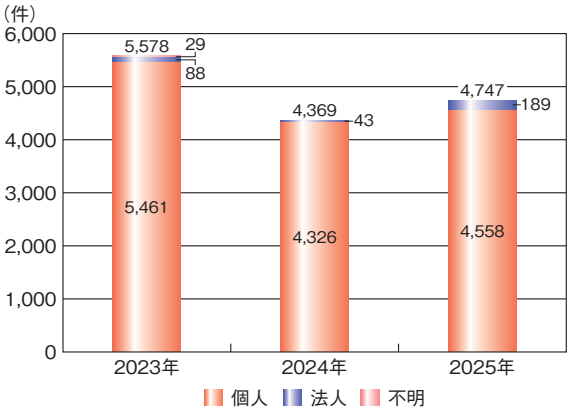
(2) 不正送金による被害

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



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

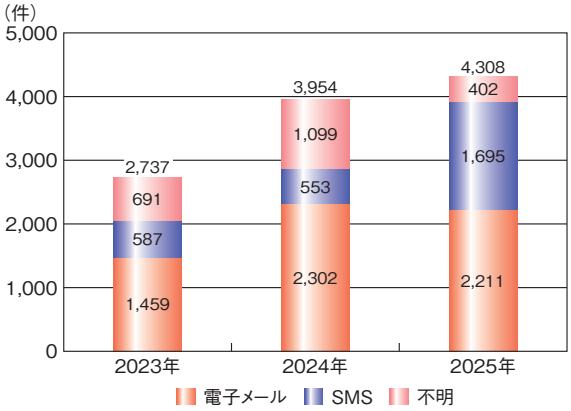
ネットバンキングにおける不正送金の発生件数を図 1-1-11 に示す。2025 年は法人の不正送金の発生が増えたとはいえ、発生件数全体のわずか 4% に過ぎない。



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

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

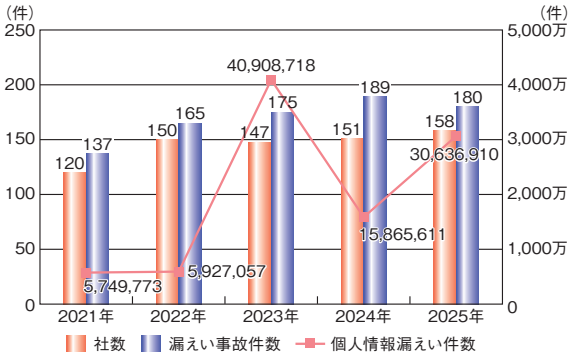
不正送金のきっかけとなるフィッシングについて、フィッシングサイトへ誘導する手口別の不正送金発生件数を図 1-1-12 に示す。電子メールによるフィッシングの割合が高いが、2025 年は SMS の割合が急増し、前年の約 3 倍に達した。電子メールや SMS のメッセージに含まれる URL を安易にタップしないよう一層の注意と用心が求められる。



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

(3) 情報漏えい・紛失事故の状況

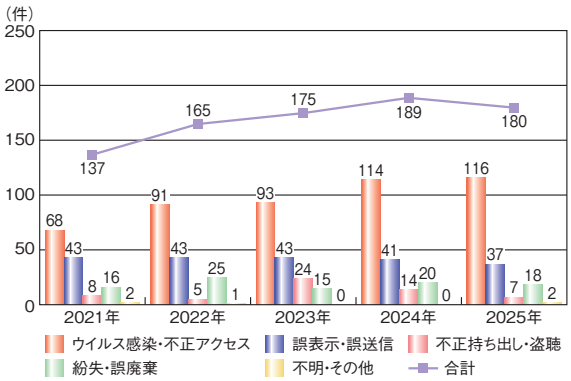
株式会社東京商工リサーチが 2026 年 1 月に公開した「2025 年『上場企業の個人情報漏えい・紛失事故』調査」によると、2025 年に上場企業とその子会社から公表された個人情報の漏えい・紛失事故の件数は 180 件、漏えいした個人情報は 3,063 万 6,910 人分だった。社数は 158 社と調査開始の 2012 年以降、過去最多であっ



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

た。図 1-1-13 に過去 5 年の推移を示す。

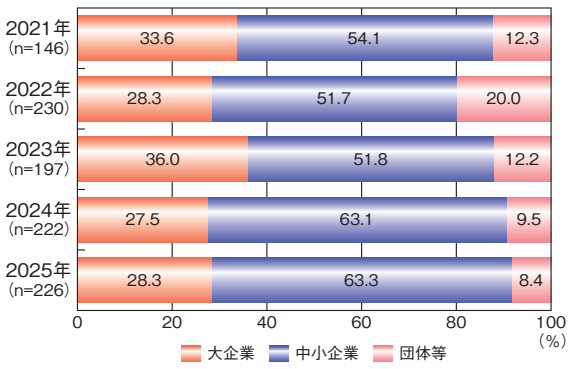
また、原因別の情報漏えい・紛失件数を図 1-1-14 に示す。「ウイルス感染・不正アクセス」が最も多く、「誤表示・誤送信」が続くという傾向は過去 5 年間、変化はない。2025 年の「ウイルス感染・不正アクセス」は 116 件と過去 5 年で最多であった。同調査では、その背景としてランサム攻撃等による不正アクセスが猛威を振るったことが挙げられている。



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

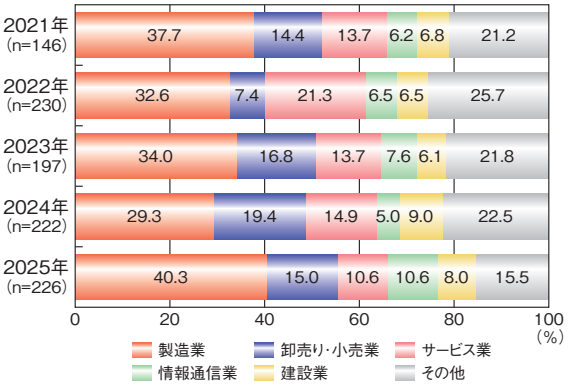
(4) ランサム攻撃による被害

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



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

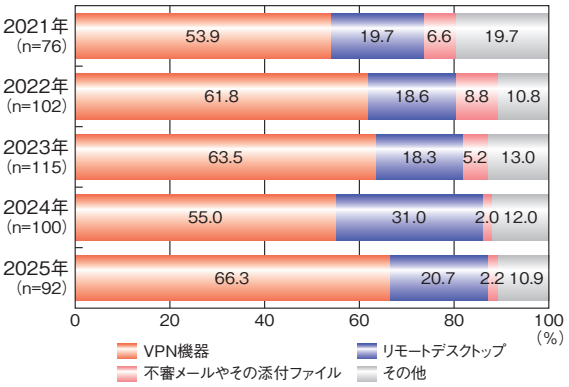
また、業種別の被害件数割合では、過去 5 年にわたり、「製造業」の割合が高い傾向が続いており、2025 年は約 4 割に達した（図 1-1-16）。



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

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

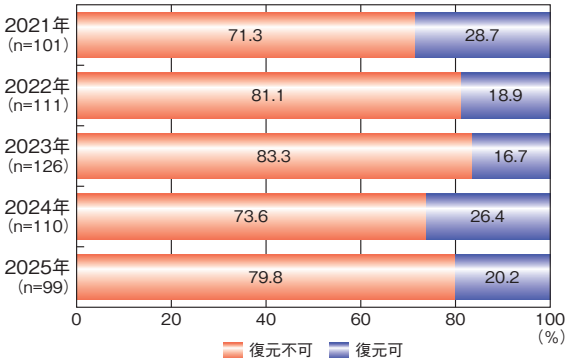
2025 年のランサムウェアの感染経路としては、有効回答 92 件のうち、「VPN 機器」が 66.3%（61 件）、「リモートデスクトップ」が 20.7%（19 件）を占め、これらテレワーク等で利用される機器からの侵入は 2024 年に引き続き、9 割に迫る高い割合となった（図 1-1-17）。



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

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

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

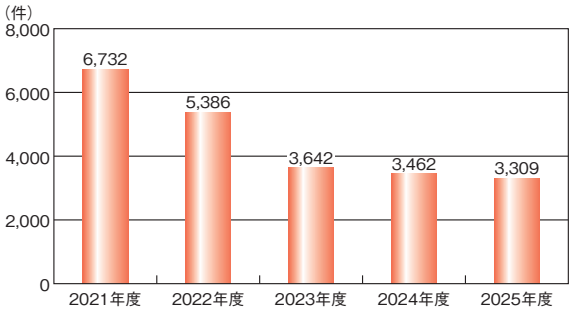


■図 1-1-18　ランサムウェア感染後、取得していたバックアップからの復元結果（2021 ～ 2025 年）
（出典）「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

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

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

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



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

(5) DDoS 攻撃による被害

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

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

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

COLUMN

ランサムウェア被害から学ぶ、経営者に求められる実践的な対処・対応とは?

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

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

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

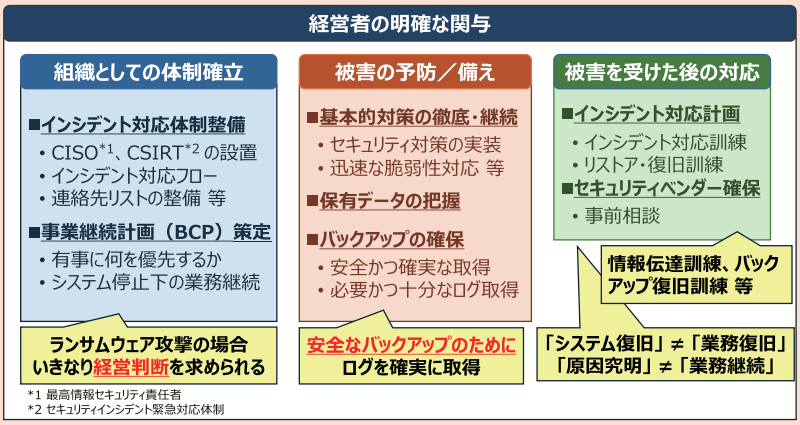


図　経営者の関与が求められるランサムウェア被害への備え

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

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

1.2 インシデント事例や脆弱性・攻撃の動向と対策

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

1.2.1 ランサム攻撃

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

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

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

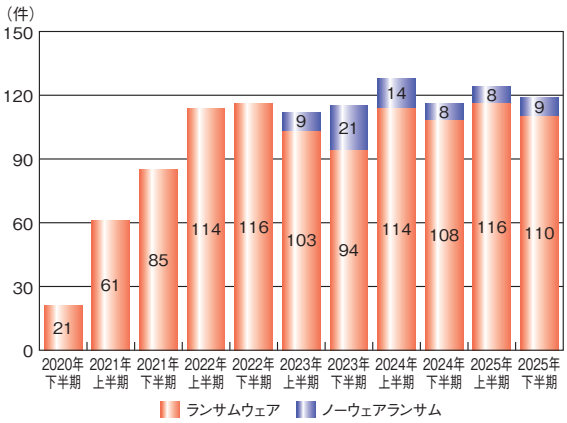
なお、昨今ではデータの暗号化を伴わない手口が確認されている。警察庁は、データを暗号化する（ランサムウェアを用いる）ことなくデータを窃取し対価を要求する手口を「ノーウェアランサム」と名付けている※36。

(1) ランサム攻撃の傾向

2025 年度における日本国内のランサム攻撃の傾向について説明する。

(a) 被害件数

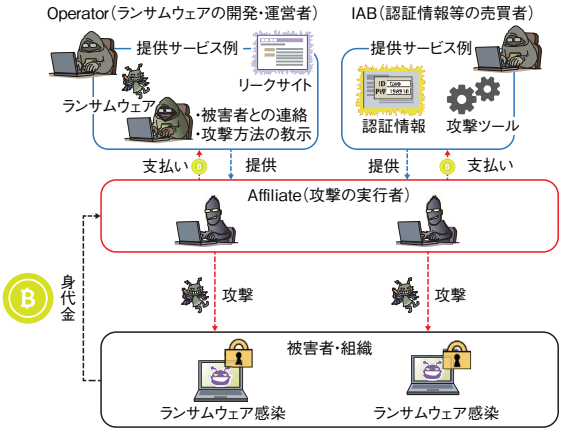
警察庁が公表した「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」（以下、警察庁資料）によると、企業・団体等におけるランサムウェア被害の報告件数は、2025 年上半期（1 月～ 6 月）が 116 件、下半期（7 月～ 12 月）が 110 件で、2022 年上半期以降は継続して高い水準で推移している（図 1-2-1）。また、ノーウェアランサム被害の報告件数は、2025 年上半期が 8 件、下半期が 9 件である。ランサムウェア被害の報告件数と比較すると少ないが、ノーウェアランサム被害の報告件数の統計が開始された 2023 年以降継続して被害が報告されている。



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

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

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



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

(b) 被害を受けた企業・組織

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

(c) 組織内ネットワークへの侵入経路

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

(d) 暗号化を伴わない攻撃手口

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

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

(e) 標的型攻撃グループによるランサムウェアの利用

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

(f) 虚偽のリーク情報に基づくランサム攻撃

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

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

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

(2) ランサム攻撃の被害事例

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

(a) 大手総合飲料メーカーにおける被害事例

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

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

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

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

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

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

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

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

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

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

(b) 大手 e コマース企業における被害事例

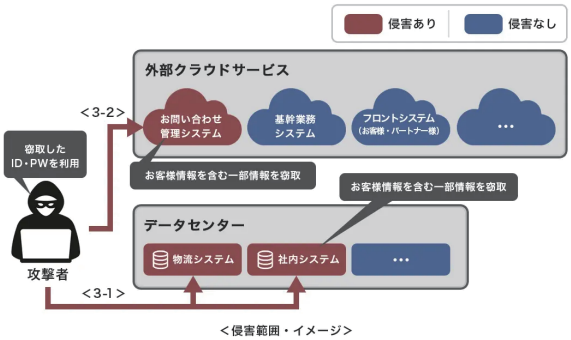
2025 年 10 月 19 日、アスクル株式会社は、同日にランサム攻撃によるシステム障害が発生し、受注・出荷業務を停止したことを公表した※52。

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

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

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

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



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

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

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

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

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

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

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

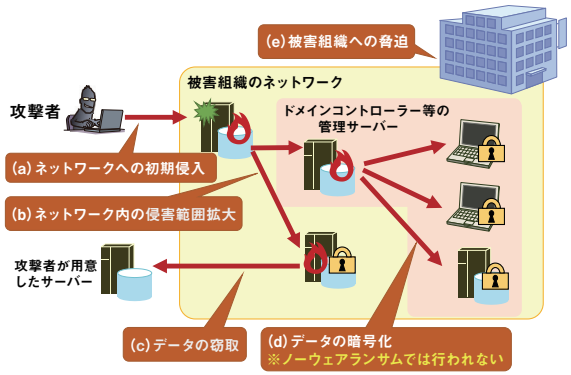
なお、同社は、2026 年 2 月 13 日に、同年 2 月 4 日より、全物流センターで新物流システムによる出荷再開が完了したこと、13 日より一般品から順次、当日配送サービスを再開しており、商品の品揃えを含む主要な EC サービス機能がシステム障害発生前の水準まで復旧したことを公表している※56。

(3) 侵入型ランサム攻撃の手口

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

(a) ネットワークへの初期侵入

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



■図 1-2-4　侵入型ランサム攻撃の手口のイメージ

(b) ネットワーク内の侵害範囲拡大

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

(c) データの窃取

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

(d)データの暗号化

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

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

(e)被害組織への脅迫

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

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

(4)侵入型ランサム攻撃への対策

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

(a)ネットワーク侵入への対策

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

- 攻撃対象領域(アタックサーフェス)の最小化

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

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

- 脆弱性対策

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

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

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

(b) 侵害範囲拡大防止のための対策

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

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

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

(c) 暗号化によるシステム停止への対策

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

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

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

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

- 復号ツールの活用（暗号化された後の対策）

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

（d）自組織への脅威に関わる情報の調査と把握

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

- 外部組織が提供する脅威動向の継続的な把握

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

- 脅威インテリジェンスサービスの活用

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

（e）インシデント対応力の強化

侵入型ランサム攻撃による被害では、業務の停止や顧客・取引先の情報漏えい等が発生し、その影響は自組織にとどまらず、顧客や取引先等の関係者にも及ぶ傾向がある。更に、時間的猶予がなく、組織は様々な意思決定を短時間で行わなければならない。そのため、平時から、経営層を含む組織内の各部署と連携したインシデント対応計画を立てることや、顧客や取引先、システムの運用・保守の委託先等との素早い連絡・調整を行うための体制づくりが必要である。特に、迅速に協力を要請できるセキュリティベンダーを含めたインシデント対応体制を整備しておくことが重要である。対応の計画や体制構築にあたっては、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC：Japan Computer Emergency Response Team Coordination Center）が公開している「侵入型ランサムウェア攻撃を受けたら読む FAQ※63」が、被害への具体的対応を詳細に紹介しており、事前準備が必要であることを理解し、備えるべきことを整理するのに非常に有用である。

- ランサム攻撃を想定した BCP の策定

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

- 侵害発生時における影響範囲の正確な把握

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

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

1.2.2 標的型攻撃

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

(1) 標的型攻撃の手口

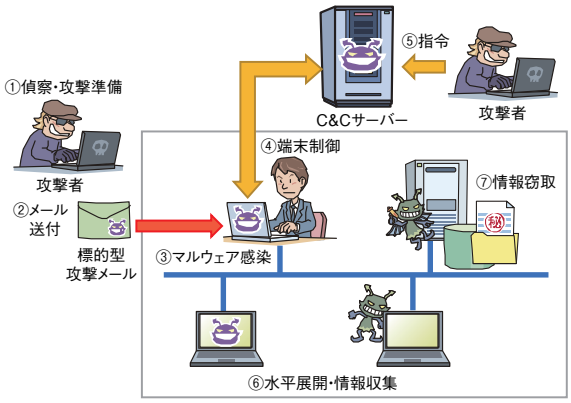
標的型攻撃における標的組織内への侵入の手口として、特定の対象をピンポイントで狙った、スピアフィッシングによる標的型攻撃メールに加え、インターネット境界に設置された機器の脆弱性の悪用等によるネットワーク貫通型攻撃も多数観測されている。以下に、それぞれの手口について述べる。

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

(a) 標的型攻撃メールを用いた攻撃の手口

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

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



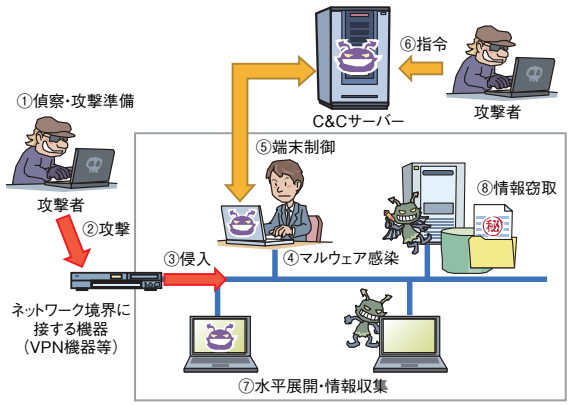
■図1-2-5　標的型攻撃メールを用いた攻撃の流れ

(b) ネットワーク貫通型攻撃の手口

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

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

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



■図 1-2-6　ネットワーク貫通型攻撃の流れの一例

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

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

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

(2) 標的型攻撃の事例

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

(a) 国家支援型 APT 攻撃グループの攻撃事例

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

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

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

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

(b) Salt Typhoon 等に関する国際注意喚起

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

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

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

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

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

(c) ORB 化を伴うネットワーク貫通型攻撃への注意喚起

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

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

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

(d) 大手の自動車会社が標的となった事例

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

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

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

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

(3) 標的型攻撃への対策

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

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

以下に、標的型攻撃への対策の例を示す。

(a) 役職員の意識向上

役職員の意識向上を目的とした対策例を以下に示す。

- 不審メールに対する注意力の向上

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

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

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

(b)組織としての対応体制の強化

組織として攻撃に対応するための体制強化を図る対策例を以下に示す。

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

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

- セキュア・バイ・デザイン機器の調達
  市場に出回るIT機器の中には、想定しない通信が発生したり、発見された脆弱性が放置されたりするものも存在しており、ネットワーク貫通型攻撃で侵害されるリスクがある。そのようなリスクを低減させるためには、セキュア・バイ・デザインの原則に基づき、設計段階からセキュリティを考慮するとともに、脆弱性対応等の継続的なサポートを含め、製品のライフサイクルを通じてセキュリティが確保された機器を選択する必要がある。2025年3月に運用が開始されたIoT製品に関するセキュリティラベリング制度「JC-STAR」の適合ラベルを取得した製品や、同様の認証を取得した製品を調達することが有効な対策となる（JC-STARの詳細については「3.3.1 セキュリティ要件適合評価及びラベリング制度（JC-STAR）」参照）。また、IT機器の調達に関するサプライチェーンを構成する組織や機器の製造国・地域等の情報も考慮して調達する機器を選定することも有効な場合がある※112。
- 脆弱性に対応する仕組みや体制の構築
  OSやアプリケーション、ネットワーク境界に接する機器等のシステムの脆弱性を悪用する攻撃に対抗するために、自組織が利用しているソフトウェアや機器の脆弱性情報と一時的な緩和策を含む対策方法をいち早く入手し、自組織に展開できる体制作りが重要である。IT資産管理システム等を活用することで、自組織のサーバーや端末等に既知の脆弱性がないかを確認し、脆弱性修正プログラムの適用等の対応を漏れなく行える仕組みを作ることが望ましい。特に「1.2.2(1)(b)ネットワーク貫通型攻撃の手口」で紹介したように、VPN機器等のネットワーク境界に接する機器やセキュリティ製品は、脆弱性が悪用される事例が確認されているため、組織内のそれらの資産を把握するとともに、一時的な緩和策を含めすぐに対応できるような体制が望ましい。
- 保護すべき重要情報の特定及び内部不正対策の基本方針の策定等
  近年、テレワークやクラウド利用の普及に伴い、組織の重要情報は分散して管理される傾向が強まっている。このため、内部不正を防止する観点から、自組織が保有する重要技術情報等の重要情報を特定し、適切な漏えい対策を講じる重要性が増している※113。これは、経済安全保障の観点や、標的組織の保有する機密情報の窃取を目的とする標的型攻撃への対策としても重要である。しかしながら、個人情報以外の重要情報の特定や漏えい対策が不十分な企業が多い実態が指摘されている※114。内部不正を含む重要情報の漏えいリスクに対応するためには、自組織が保有する重要情報を特定することに加え、全社的に取り組むことができる体制を整備する必要がある。具体的には、経営層が基本方針を策定し、その方針に基づく組織横断的な計画を承認するとともに実施を統制し、更に適切な権限移譲により具体的対策の実効性を確保することが重要である。IPAの「組織における内部不正防止ガイドライン」も参考に内部不正対策に取り組むことが、国家支援型APT攻撃への対策にもつながると期待される※115。

(c)システムによる対策

システムによる対策例を以下に示す。

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

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

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

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

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

1.2.3 DDoS攻撃

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

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

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

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

（1）DDoS攻撃の世界的な動向

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

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

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

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

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

（2）DDoS攻撃の国内事例

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

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

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

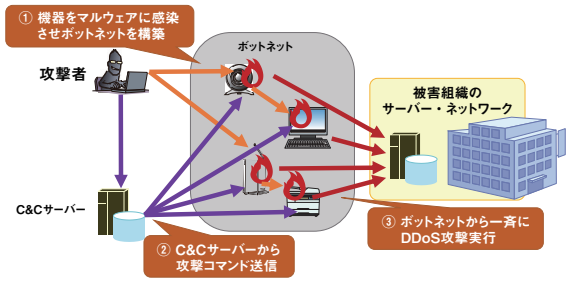
(3) ボットネットを使用した攻撃の手口

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

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

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

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



■図1-2-7　ボットネットによるDDoS攻撃の手口のイメージ

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

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

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

(4) DDoS攻撃への対策・対処

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

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

きたい※139。

(a) DDoS 攻撃への対策

以下に、DDoS 攻撃に対する防御・被害軽減のための具体的な対策を挙げる。

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

(b) DDoS 攻撃の被害に遭った場合の対処

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

以下に、DDoS 攻撃を検知した場合の具体的な対処方法を挙げる。

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

外の IP アドレスからのアクセスを一時的に遮断することを検討する。

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

(c) DDoS 攻撃に加担しないための対策

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

以下に、具体的な対処方法を挙げる。

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

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

1.2.4 情報システムの脆弱性を悪用した攻撃

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

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

(1) ゼロデイ攻撃

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

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

(a) 2025 年におけるゼロデイ攻撃の世界での動向

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

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

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

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

(b) 2025 年に公表された国内事例

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

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

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

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

(c) 組織が実施すべき対策

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

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

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

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

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

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

(2) Nデイ攻撃

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

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

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

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

(a)「既知の脆弱性（Nデイ脆弱性）」が引き起こす被害

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

(ア) 2025年に公表された国内事例

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

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

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

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

ることが挙げられる。

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

(イ) 国家支援型グループによる悪用

N デイ脆弱性を悪用するのは、前述のランサム攻撃だけではない。

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

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

(b) 攻撃と防御の非対称性による課題

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

(ア) 脆弱性公開とともに始まる悪用

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

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

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

(イ) 短期間での対応の難しさ

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

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

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

(ウ) CVSS スコアの限界

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

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

CVSS v3 スコアも現状は 9.8 となっている※160。

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

(c) 組織が実施すべき対策

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

- 脆弱性情報の迅速な把握と優先度判断

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

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

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

- 組織的な体制整備と情報共有

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

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

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

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

- 重大脆弱性への迅速な対応フローの整備

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

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

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

- 継続的な資産管理（外部公開機器等の継続的な可視化）

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

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

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

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

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

1.2.5 不正アクセスや内部不正による情報漏えい

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

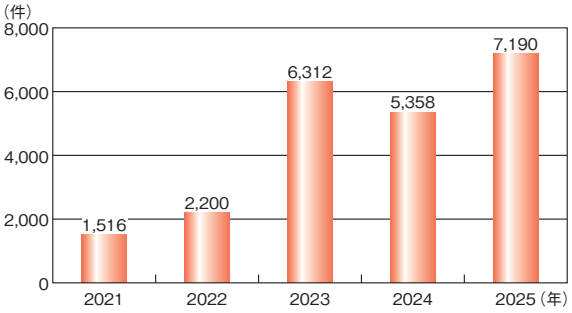
「情報セキュリティ 10 大脅威 2026」の「『組織』向け脅威」では、「ランサム攻撃による被害」が 11 年連続で選出され、攻撃の手口の一つに不正アクセスが挙げられている。トレンドマイクロ社によると 2025 年 1 ～ 12 月に公表された 559 件のインシデントのうち、327 件は不正アクセスによるものであり、最も多かった※167。また、「『組織』向け脅威」では「内部不正による情報漏えい等」も 11 年連続で選出されている。これらの脅威により組織から漏えいする情報は、顧客の個人情報から、研究データや製造ノウハウ、設計図面といった技術情報等まで多岐にわたる。

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

(1) 不正アクセスによる情報漏えい

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

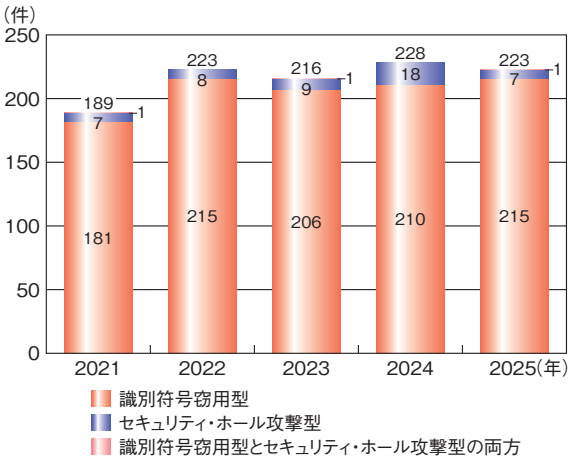
国家公安委員会、総務大臣及び経済産業大臣から公開されている「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況※169」によれば、2025 年の不正アクセス行為の認知件数としては 7,190 件となっており、2023 年から 5,000 件を超える水準で推移している(図 1-2-8)。



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

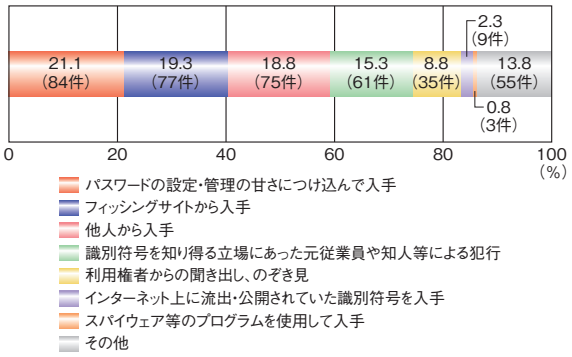
また、2025 年の不正アクセス行為の検挙事件数※170 については、2024 年からわずかに減少し合計 223 件となっており、検挙件数※171 も 407 件となっている。

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



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

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



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

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

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

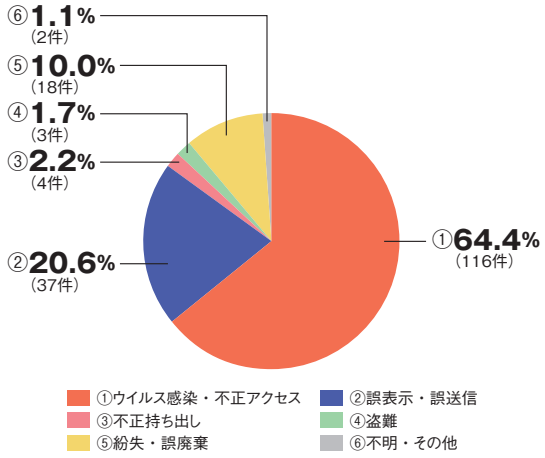
■表1-2-3 不正アクセスによる主な情報漏えい事例
(出典)公表情報を基にIPAが作成

(2) 内部不正による情報漏えい

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

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

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



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

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

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

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

(3) 不正アクセスや内部不正による情報漏えいを防ぐための対策例

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

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

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

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

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

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

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

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

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

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

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

■表 1-2-7　不正アクセスや内部不正による情報漏えいと関連する法規制

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

1.2.6 個人を狙う騙しの手口

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

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

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

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

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

(1) フィッシング

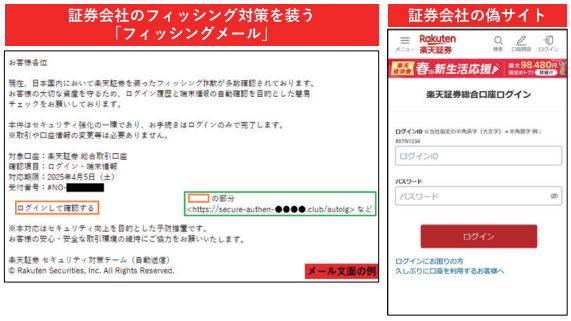
フィッシングとは、実在する企業・組織をかたるメールや SMS を送り付け、偽サイト（フィッシングサイト）に誘導し、情報を詐取する手口である。メールの受信者を「緊急性を煽る文面」等で焦らせて、メール文中の偽サイトへのリンクをクリックさせることで、偽サイトに入力した情報を詐取する。

(a) 手口

証券口座のアカウントへの不正ログインでも、フィッシングの手口が使われた。

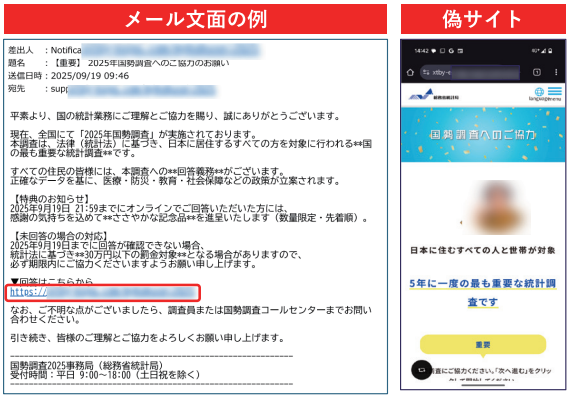
フィッシングメールの中には、「セキュリティ強化のご案内」「フィッシング詐欺にご注意ください!」等の、証券会社のセキュリティ対策強化や注意喚起を装うものもあった[※200]。フィッシング詐欺の攻撃グループが、事業者のフィッシング対策の呼びかけを逆手に取って、こうしたメールを送っていた（図 1-2-12）。

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



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

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



■図 1-2-13　国勢調査への回答を求めるフィッシング

(b) 対処

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

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

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

(c) 対策

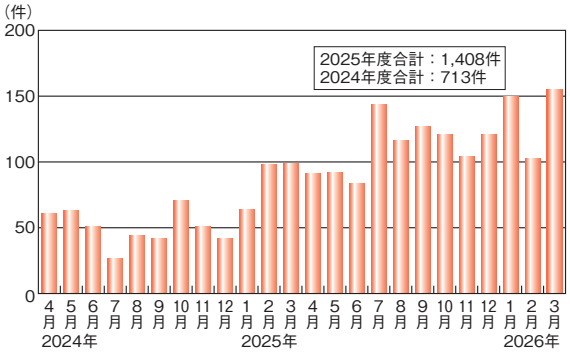
フィッシングに対する基本的な対策は以下のとおりである。

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

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

(2) 不正ログイン

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



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

不正ログインをされた場合に発生する主な被害は以下のとおりである。

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

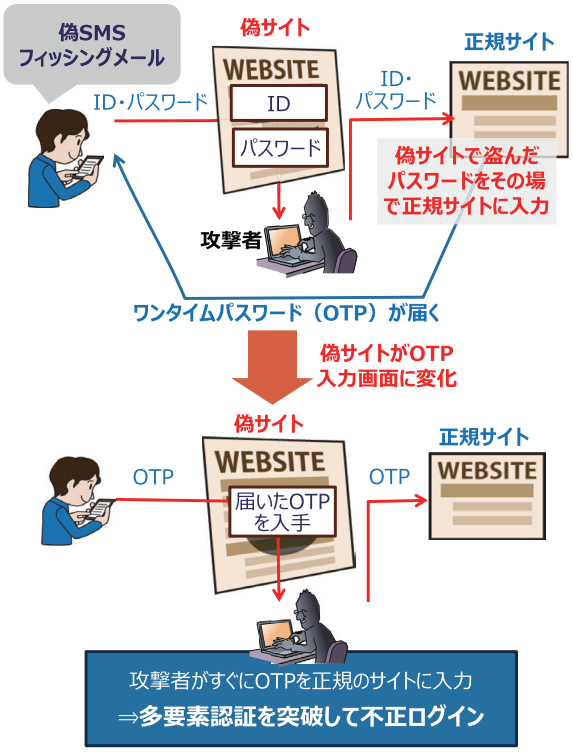
(a) 手口

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

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

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

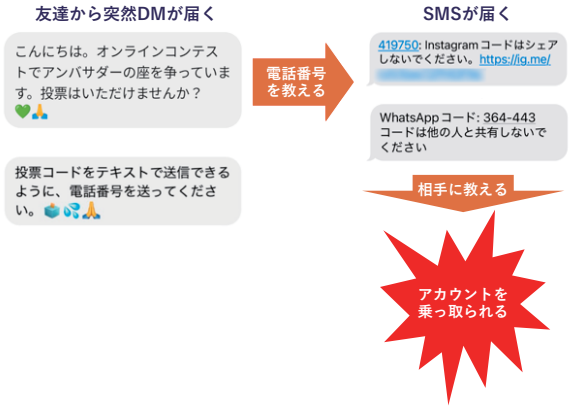
①攻撃者が乗っ取ったSNSアカウントから、電話番号を教えてほしいというDM(ダイレクトメッセージ)が届く。



■図 1-2-15　リアルタイムフィッシングの概要

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

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



■図 1-2-16　パスワードの再設定手順を悪用した乗っ取りの手口

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

(b) 対処

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

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

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

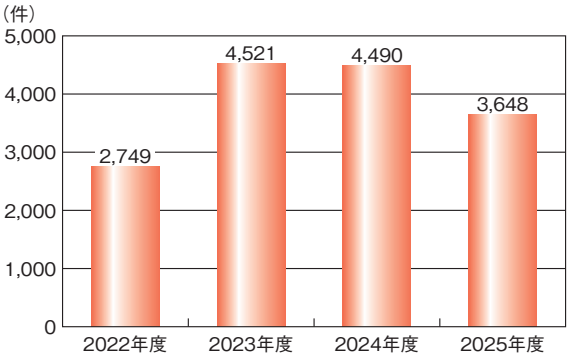
(c) 対策

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

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

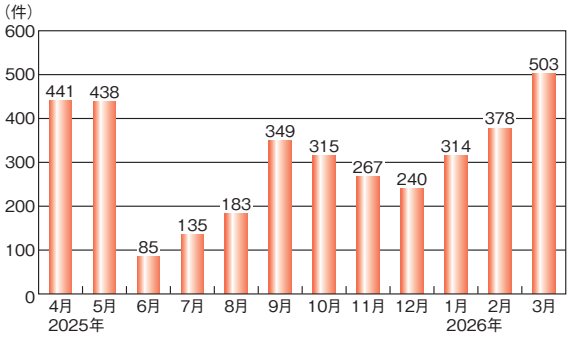
(3) サポート詐欺(偽のウイルス感染警告)

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



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

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



■図 1-2-18　サポート詐欺の月別相談件数の推移(2025 年度)

(a) 手口

サポート詐欺の手口は以下のとおりである。

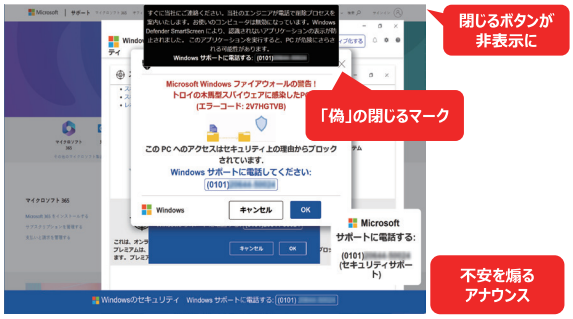
①パソコンに偽のウイルス感染警告(セキュリティ警告)を表示させる(図 1-2-19)。

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

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

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

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



■図 1-2-19　偽警告画面の例

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

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



■図 1-2-20　Web サイトや動画サイトに表示された罠の広告の例

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

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

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

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

(b)対処

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

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

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

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

(c)対策

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

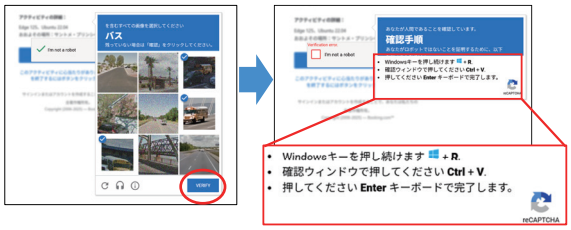
(4) ClickFix 攻撃

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

(a)手口

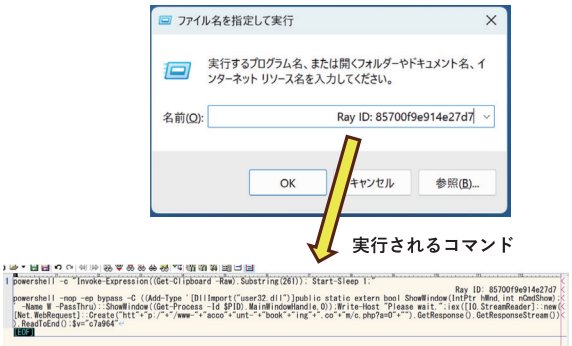
ClickFix の手口は以下のとおりである。

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



■図 1-2-21　ClickFix の手口の誘導画面

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



■図 1-2-22　ClickFix の手口で悪用されるコマンド入力画面

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

(b) 対処

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

(c) 対策

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

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

(5) 騙しの手口への対策

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

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

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

1.2.7 企業・組織を狙う騙しの手口

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

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

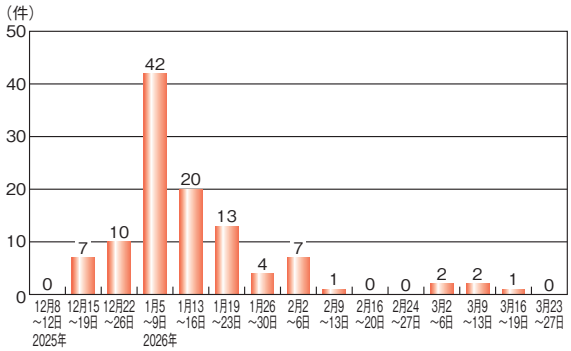
(1) SNSへ誘導する偽社長メール

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

(a) 手口

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

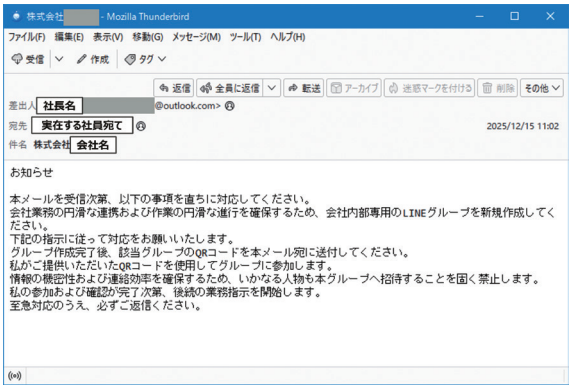
- 差出人の表示名が自社や取引先の代表者名となっている。
- 差出人のメールアドレスには、outlook.com、hotmail.com、gmail.com等のフリーメールが使用されている。
- 件名は自社の会社名になっている場合が多い。
- 本文には、業務指示を装って、「LINEのグループを作成しQRコードを返信するように」「グループには他の者は加えないように」等と書かれている。
- 業務指示に先立って、在席確認を送信してくるケースを確認している。



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

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

■表 1-2-8　偽社長メールによる被害報道



■図 1-2-24　偽社長メールの一例

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

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

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

(b) 対処

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

(c) 対策

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

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

(2) 企業・組織で起こるサポート詐欺の被害と対策

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

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

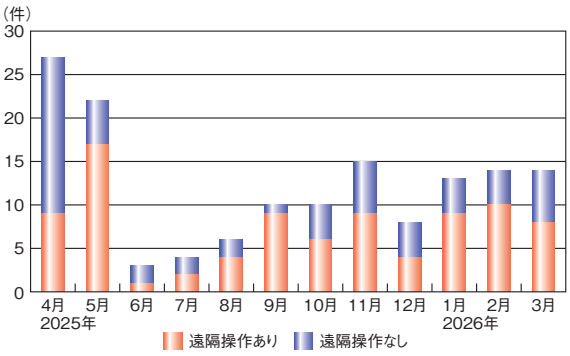
企業・組織の端末には個人情報が保存されている場

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

■表 1-2-9　サポート詐欺による被害報道

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

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



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

「人」「技術」「運用管理」それぞれの観点で対策のポイントを示す。

役職員等の「人」が実施すべき対策のポイントは、以下のとおりである。

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

技術的対策のポイントは、以下のとおりである。

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

運用管理面での対策のポイントは、以下のとおりである。

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

COLUMN

IoT機器は輸入禁止になるくらい危険なのでしょうか?

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

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

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

①一定の処理能力を有していること

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

②同一または同等の機器が多数存在していること

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

③世界中に散在する形で多数利用されていること

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

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

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

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

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

日本では、2025 年 3 月以降、IPA が IoT 製品のセキュリティ対策状況を評価して適合ラベルを交付する制度「JC-STAR」を開始しています。ラベルが交付された製品の出荷も始まっており、新たに IoT 機器を購入する際の判断材料の一つにするとよいと思います（「3.3.1 セキュリティ要件適合評価及びラベリング制度（JC-STAR）」参照）。

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

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

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

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

29300）を狙う攻撃～ https://www.ipa.go.jp/security/security-alert/2024/alert_orb.html〔2026/7/13 確認〕
※ 72 CISA 等：PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf〔2026/7/13 確認〕
※ 73 Living Off The Land（LOTL）戦術：情報窃取等の侵害活動を行う際に、独自のマルウェアではなく、システム内の正規のツール・機能等を活用することにより、検知を回避する攻撃戦術。
※ 74 内閣官房内閣サイバーセキュリティセンター：Living Off The Land 戦術等を含む最近のサイバー攻撃に関する注意喚起 https://www.cyber.go.jp/pdf/news/press/240625NISC_press.pdf〔2026/7/13 確認〕
※ 75 トレンドマイクロ社：MirrorFace（ミラーフェイス）とは?～警察が注意喚起を行った標的型攻撃グループを解説～ https://www.trendmicro.com/ja_jp/jp-security/25/a/expertview-20250109-01.html〔2026/7/13 確認〕
※ 76 CrowdStrike Holdings, Inc.：クラウドストライク 2026 年版グローバル脅威レポート：AI によって加速する攻撃者と新たに形成される攻撃対象領域 https://www.crowdstrike.com/ja-jp/press-releases/2026-crowdstrike-global-threat-report/?__cf_chl_f_tk=CcMgY_Cbcz2WWbc0x7bMj1Mh48w8wIgK7tA9Zd019ul-1783042992-1.0.1.1-0XcRJD9my9ZrtE.ka1h4iil7gSObll.uDnYcsM1NOzc〔2026/7/13 確認〕
CrowdStrike Holdings, Inc.：クラウドストライク 2025 年版グローバル脅威レポート：中国のサイバースパイの活動が 150% 増加し、攻撃手法も大幅に高度化、AI を使った詐欺的手口の悪用も https://www.crowdstrike.com/ja-jp/press-releases/crowdstrike-releases-2025-global-threat-report/〔2026/8/25 確認〕
※ 77 「国家支援型」の攻撃は、「ステートスポンサード」（state-sponsored）、「ネイションバックド」（nation-backed）の攻撃と呼ばれることもある。実際の活動は外国の軍及び情報機関、宣伝機関が直接、または下請のハッカー（Hack-For-Hire）や犯罪者（政府放任型サイバー犯罪グループ）を介して行われるとされる。
IPA：サイバーレスキュー隊 (J-CRAT) 活動状況［2022 年度上半期］ https://www.ipa.go.jp/security/j-crat/ug65p9000000nks8-att/000106897.pdf〔2026/7/13 確認〕
※ 78 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2022 年 7 月～ 9 月］ https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000103970.pdf〔2026/7/13 確認〕（標的別に改変・開発したマルウェアの使用については「3.2.3 攻撃で使われたウイルス」、標的組織の内部に長期間潜伏して活動する点については「3.2.1 初期侵入」をそれぞれ参照）
※ 79 トレンドマイクロ社：日本や台湾を狙う標的型攻撃：「Earth Kasha」が攻撃手法を更新して新たな攻撃キャンペーンを開始 https://www.trendmicro.com/ja_jp/research/25/e/earth-kasha-updates-ttps.html〔2026/7/13 確認〕
※ 80 警察庁、内閣サイバーセキュリティセンター：MirrorFace によるサイバー攻撃について（注意喚起） https://www.npa.go.jp/bureau/cyber/pdf/20250108_caution.pdf〔2026/7/13 確認〕
※ 81 https://www.ipa.go.jp/publish/wp-security/2025.html〔2026/10/13 確認〕
※ 82 CISA：Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a〔2026/7/13 確認〕
※ 83 NCO、警察庁：「ソルトタイフーン（Salt Typhoon）」に関する国際アドバイザリーへの共同署名について https://www.npa.go.jp/bureau/cyber/pdf/20250827.pdf〔2026/7/13 確認〕
※ 84 The MITRE Corporation（MITRE）：CVE-2024-21887 https://www.cve.org/CVERecord?id=CVE-2024-21887〔2026/7/13 確認〕
※ 85 MITRE：CVE-2024-3400 https://www.cve.org/CVERecord?id=CVE-2024-3400〔2026/7/13 確認〕
※ 86 MITRE：CVE-2023-20273 https://www.cve.org/CVERecord?id=CVE-2023-20273〔2026/7/13 確認〕
※ 87 MITRE：CVE-2023-20198 https://www.cve.org/CVERecord?id=CVE-2023-20198〔2026/7/13 確認〕
※ 88 https://www.ipa.go.jp/security/security-alert/2025/alert20251031_vpn.html〔2026/7/13 確認〕
※ 89 Cloud Software Group, Inc.：NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-7775, CVE-2025-7776 and CVE-2025-8424 https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694938〔2026/7/13 確認〕
Ivanti Software, Inc.：April Security Advisory Ivanti Connect Secure, Policy Secure & ZTA Gateways (CVE-2025-22457) https://hub.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457?language=en_US〔2026/7/13 確認〕
Fortinet, Inc.：Authentication bypass in Node.js websocket module and CSF requests https://www.fortiguard.com/psirt/FG-IR-24-535〔2026/7/13 確認〕
※ 90 IPA：NetScaler ADC および NetScaler Gateway の脆弱性について（CVE-2025-7775 等） https://www.ipa.go.jp/security/security-alert/2025/alert20250827.html〔2026/7/13 確認〕
※ 91 JPCERT/CC:Ivanti Connect Secure などにおける脆弱性（CVE-2025-22457）に関する注意喚起 https://www.jpcert.or.jp/at/2025/at250008.html〔2026/7/13 確認〕
※ 92 IPA：Fortinet 製 FortiOS の脆弱性対策について（CVE-2024-55591） https://www.ipa.go.jp/security/security-alert/2024/alert20250115.html〔2026/7/13 確認〕
※ 93 JLR 社：Statement on Cyber Incident 2 September 2025 https://media.jaguarlandrover.com/news/2025/09/statement-cyber-incident〔2026/7/13 確認〕
※ 94 SecurityWeek：Jaguar Land Rover Operations 'Severely Disrupted' by Cyberattack https://www.securityweek.com/jaguar-land-rover-operations-severely-disrupted-by-cyberattack/〔2026/7/13 確認〕
※ 95 The Sun：Legendary car brand halts ALL production at £1.04billion plant after being forced to shut down IT systems https://www.thesun.co.uk/motors/36615743/legendary-car-brand-halts-production-plant-shut-down/〔2026/7/13 確認〕
※ 96 The Record：Jaguar Land Rover says cyberattack shutdown to last 'at least' another week https://therecord.media/jaguar-land-rover-another-week-shutdown-cyberattack〔2026/7/13 確認〕
※ 97 The Guardian：Jaguar Land Rover hack has cost UK economy £1.9bn, experts say https://www.theguardian.com/business/2025/oct/22/jaguar-land-rover-hack-has-cost-uk-economy-19bn-most-costly-cyber-attack-britain〔2026/7/13 確認〕
※ 98 JLR 社：Statement on Cyber Incident 16 September 2025 https://media.jaguarlandrover.com/news/2025/09/statement-cyber-incident-2〔2026/7/13 確認〕
JLR 社：Statement on Cyber Incident 23 September 2025 https://media.jaguarlandrover.com/news/2025/09/statement-cyber-incident-4〔2026/7/13 確認〕
※ 99 JLR 社：JLR restarts manufacturing and introduces new financing solution to pay JLR suppliers early https://media.jaguarlandrover.com/news/2025/10/jlr-restarts-manufacturing-and-introduces-new-financing-solution-pay-jlr-suppliers〔2026/7/13 確認〕
※ 100 本白書では 1 ポンド 216 円として換算している。
※ 101 SecurityWeek：Cyberattack on JLR Prompts £1.5 Billion UK Government Intervention https://www.securityweek.com/cyberattack-on-jlr-prompts-1-5-billion-uk-government-intervention/〔2026/7/13 確認〕
※ 102 BBC：M&S hackers claim to be behind Jaguar Land Rover cyber attack https://www.bbc.com/news/articles/c4gqepe5355o〔2026/7/13 確認〕
※ 103 The New York Times：A $2.5 Billion Whodunit: The Hack That Dented the U.K. Economy https://www.nytimes.com/2026/06/26/world/europe/jaguar-russia-hack.html〔2026/7/13 確認〕
※ 104 The Nextw Web：Russian hackers were behind the Jaguar Land Rover attack that cost the British economy two and a half billion dollars https://thenextweb.com/news/jaguar-land-rover-hack-russian-hackers-nyt-investigation〔2026/7/13 確認〕
※ 105 サイバー安全保障分野での対応能力の向上に向けた有識者会議：サイバー安全保障分野での対応能力の向上に向けた提言 https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/koujou_teigen/teigen.pdf〔2026/7/13 確認〕
※ 106 なお、国家支援型 APT 攻撃への備えとしては、経済安全保障の文脈で、輸出管理部門やリスク対策部門、経営管理部門等ビジネスインテリジェンスに関わる組織とも密に連携し、サイバー攻撃以外のリスクも併せた、全方位的な脅威状況の把握への参画も必要である。
※ 107 産業サイバーセキュリティ研究会：産業界へのメッセージ（令和 7 年 5 月 23 日） https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20250523.pdf〔2026/7/13 確認〕
※ 108 サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会：サイバー攻撃被害に係る情報の共有・公表ガイダンス https://www.

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

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

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

付録・索引

第21回 IPA「ひろげよう情報セキュリティコンクール」2025 受賞作品

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

最優秀賞

油断禁物



長浜 ちひろさん
立川女子高等学校

優秀賞

そのパスワード大丈夫？



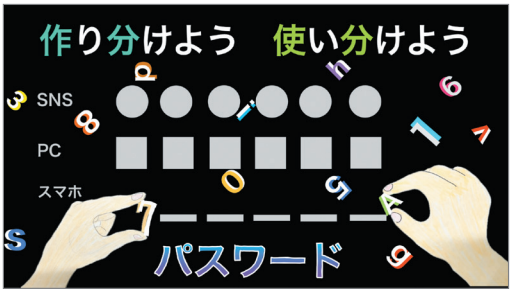
脇 玲美奈さん
静岡市立安東小学校

視線の先



小磯 凛さん
静岡県立三島南高等学校

作り分けよう
使い分けようパスワード



宮城 優佳さん
白百合学園中学校

索引

数字

0APT ····· 21
2024 年オンライン安全修正（ソーシャルメディア最低年齢）法（Online Safety Amendment (Social Media Minimum Age) Act 2024） ····· 94
8Base ····· 110

A

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

C

C&C（Command and Control）サーバー ····· 27, 35
CCRA（Common Criteria Recognition Arrangement） ····· 191
ChatGPT ····· 69, 72, 90
ClOP（ClOp、Clop） ····· 9, 38
Claude Mythos ····· 83, 161
ClickFix ····· 33, 46, 50
CRYPTREC（Cryptography Research and Evaluation Committees） ····· 142
CSIRT（Computer Security Incident Response Team） ····· 31, 41, 123, 176, 183
CVE（Common Vulnerabilities and Exposures：共通脆弱性識別子） ····· 38, 79, 176
CVSS（Common Vulnerability Scoring System：共通脆弱性評価システム） ····· 40, 176

D

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

E

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

F

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

G

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

I

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

J·K

J-CRAT（Cyber Rescue and Advice Team against targeted attack of Japan：サイバーレスキュー隊）…… 120
JTC 1（Joint Technical Committee 1：第一合同技術委員会）…… 188
KEV（Known Exploited Vulnerabilities：既知の悪用された脆弱性）カタログ…… 38, 41, 170

L

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

M

Microsoft Office…… 30
MirrorFace…… 28

N·O

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

P·Q

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

R

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

S

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

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

T・U

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

V

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

あ

アイデンティティ管理……191
アイランドホッピング攻撃……31
悪意ある情報……88, 90
アクセス・無害化……63, 107, 109
暗号資産……162
一般財団法人日本サイバー犯罪対策センター（JC3：Japan Cybercrime Control Center）……109
一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC：Japan Computer Emergency Response Team Coordination Center）……26, 38, 41, 121, 186
インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク……164
インフォスティーラー（Infostealer）……9, 46, 50
エクスプロイト……9, 12
エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン……130, 136
遠隔操作……27, 49, 52
遠隔操作マルウェア……23
欧州刑事警察機構（Europol：European Union Agency for Law Enforcement Cooperation）……34, 110, 164, 176
欧州サイバーセキュリティ認証フレームワーク（ECCF：European Cybersecurity Certification Framework……176, 180
オンライン安全法（Online Safety Act）……94

か

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

さ

サイバー安全保障分野での対応能力の向上に向けた提言……62
サイバーインフラ事業者に求められる役割等に関するガイドライン……117
サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項……62, 106
サイバー警察局……110
サイバー情報共有イニシアティブ（J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan）……119
サイバーセキュリティ 2025（2024 年度年次報告・2025 年度年次計画）……106, 123
サイバーセキュリティお助け隊サービス……116, 147, 151
サイバーセキュリティ企画演習（CyberSPEX：Cyber Security Planning Exercise）……129
サイバーセキュリティ基本法……106, 112
サイバーセキュリティ経営ガイドライン……32
サイバーセキュリティ人材……118, 122, 148
サイバーセキュリティ人材フレームワーク 2026…124
サイバーセキュリティ戦略……62, 106
サイバーセキュリティネクサス（CYNEX：Cybersecurity Nexus）……17
サイバー対処能力強化法……62, 106
サイバー特別捜査部……110
サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）……115, 191
サイバーブループリント（Cyber Blueprint）……179
サイバーレジリエンス法（CRA：Cyber Resilience Act）……174, 178
サイバー連帯法（CSoA：Cyber Solidarity Act）……179
サプライチェーン……8, 24, 31, 115, 145, 160
サプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度）……116, 145, 148, 150
サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3：Supply-Chain Cybersecurity Consortium）……116
サプライチェーン・リスク……8, 84, 177
サポート詐欺……49, 52, 71, 110
産業サイバーセキュリティ研究会……114
産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）……128, 164
ジェイルブレイク……80, 169
事業継続計画（BCP：Business Continuity Plan）……23, 26, 31, 36, 129
次世代アンチウイルス（NGAV：Next Generation Anti-Virus）……38
実践的サイバー防御演習（CYDER：Cyber Defense Exercise with Recurrence）……165
シャドー AI……85, 123
重要インフラ……34, 63, 84, 108, 167, 177
重要インフラのサイバーセキュリティ対策のための統一基準（案）……108
重要インフラのサイバーセキュリティに係る行動計画……108
重要経済安保情報保護活用法……66
重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針……64
重要電子計算機に対する不正な行為による被害の防止に関する法律（サイバー対処能力強化法）……62
情報処理安全確保支援士（登録セキスペ）……124, 125, 151
情報セキュリティ安心相談窓口……46
情報セキュリティ早期警戒パートナーシップ……41, 120
情報セキュリティマネジメント試験……125
情報セキュリティマネジメントシステム（ISMS：Information Security Management System）……189
情報戦……90, 95
情報操作型サイバー攻撃……88, 90
情報流通プラットフォーム対処法……94
情報漏えい……11, 15, 42
新型コロナウイルス……93
人工知能関連技術の研究開発及び活用の推進に関する法律（AI 法）……78, 110
人工知能基本計画……79
侵入型ランサム攻撃……19, 21, 23
水平展開……25, 27
スロップスクワッティング……81
制御システム……129, 164

制御システム向けサイバーセキュリティ演習（CyberSTIX：Cyber SecuriTy practIcal eXercise for industrial control system）……130
脆弱性……8, 24, 37, 121, 170, 176
生成 AI（Generative AI）……69, 92, 110
政府機関等のサイバーセキュリティ対策のための統一基準……138
政府機関等の対策基準策定のためのガイドライン……27, 117, 135
政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program：通称、ISMAP（イスマップ））……139
セキュア・ソフトウェア開発フレームワーク（SSDF：Secure Software Development Framework）……117
セキュア・バイ・デザイン……32, 117
セキュリティ・キャンプ……118, 127
セキュリティ・クリアランス制度……66
セキュリティ要件適合評価及びラベリング制度（JC-STAR）……32, 117, 133, 163
ゼロデイ攻撃……37
ゼロトラスト……84, 166
組織における内部不正防止ガイドライン……44

た

ダークウェブ……20, 26, 37
第 14 次 5 ヵ年計画……180
対ランサムウェア・イニシアチブ（CRI：Counter Ransomware Initiative）……162
耐量子計算機暗号（PQC：Post-Quantum Cryptography）……142, 168
地方公共団体における情報セキュリティポリシーに関するガイドライン……113
中核人材育成プログラム……128
中華人民共和国サイバーセキュリティ法……181, 183
中小企業の情報セキュリティ対策ガイドライン……116, 147
中小企業のためのセキュリティ人材確保・育成の実践ガイドブック……118, 150
ディープフェイク……92, 94, 110, 160
ディスインフォメーション（Dis-information）……88
データ三法……181
データ侵害……9, 11, 172
データセキュリティ……111
適合ラベル……133
デジタルオペレーショナルレジリエンス法（DORA：Digital Operational Resilience Act）……174
デジタルオムニバス規則案……173
デジタルサービス法（DSA：Digital Services Act）……93, 174
デジタル社会の実現に向けた重点計画……111
デジタル署名……175, 190
デジタルスキル標準（DSS）……124
デジタルトラスト……165
デバイス・コード・フィッシング（Device Code Phishing）……9
特別社会基盤事業者……63

な

内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）……62
内部不正……32, 42
ナラティブ……90, 95
なりすまし……42, 71, 162
二重の脅迫（二重恐喝）……16, 19, 23
偽・誤情報……75, 88
偽情報……88
偽のウイルス感染警告……49, 52, 110
日 ASEAN サイバーセキュリティ政策会議……117, 164
日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC：ASEAN-Japan Cybersecurity Capacity Building Centre）……164
日 ASEAN 能力向上プログラム強化プロジェクト……165
日・EU サイバー対話……164
日英サイバー対話……163
日米サイバー対話……163
日本 AISI……76, 79, 81, 85
日本産業標準調査会（JISC：Japanese Industrial Standards Committee）……188
認知戦……88, 91, 95
ネットワーク貫通型攻撃……27, 29, 119
ノーウェアランサム……19, 23

は

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

ま

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

ら

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

著作・製作　独立行政法人情報処理推進機構（IPA）

編集責任

大川 龍郎	清水 督史	小山 明美
涌田 明夫	白石 歩	井上 佳春

執筆者

IPA

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

（敬称略）

ネット教育アナリスト　尾花 紀子

一般社団法人日本クラウドセキュリティアライアンス　諸角 昌宏

一般社団法人 JPCERT コーディネーションセンター　米澤 詩歩乃

協力者

IPA

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

サイバーレスキュー隊 J-CRAT（ジェイ・クラート）

AISI 事務局 戦略企画グループ

（敬称略）

一般財団法人日本情報経済社会推進協会　大熊 三恵子

NRI セキュアテクノロジーズ株式会社　北原 幸彦

一般財団法人日本情報経済社会推進協会　崎村 夏彦

一般社団法人 JPCERT コーディネーションセンター　染川 夕貴

京都外国語大学 共通教育機構　土屋 貴裕

NTT 株式会社　永井 彰

国立研究開発法人情報通信研究機構　中尾 康二

デジタル庁 戦略・組織グループ セキュリティチーム　中村 元洋

総務省 サイバーセキュリティ統括官室

経済産業省 商務情報政策局 サイバーセキュリティ課

おわりに

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

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

編集子

・本白書の引用、転載については、IPA Web サイトの「書籍・刊行物等に関するよくあるご質問と回答」（https://www.ipa.go.jp/publish/faq.html）に掲載されている「2. 引用や転載に関するご質問」をご参照ください。
ただし、出典元が IPA 以外であり、かつ IPA が編集、作成を行った図表については、本白書からの転載・改変について IPA は許諾ができません。転載・改変について IPA が許諾できない図表は以下の様に出典を記載しています。
例「（出典）《組織名等》『《文書名等》』を基に IPA が編集」
例「（出典）《組織名等》『《文書名等》』を基に IPA が作成」
また、出典元が IPA 以外であり、かつ IPA が本白書で引用している図表についても、転載・改変について IPA は許諾ができません。以下の様に記載している図表の転載・改変の可否については、出典元をご確認ください。
例「《組織名等》『《文書名等》』」
上記の例にある《組織名等》《文書名等》には実際の出典元組織名、文書名が記載されます。
なお、これは、著作権法で定められた本白書からの引用を妨げるものではありません。
・本白書は 2025 年度の出来事を主な対象とし、執筆時点の情報に基づいて記載しています。
・電話によるご質問、及び本白書に記載されている内容以外のご質問には一切お答えできません。
あらかじめご了承ください。
・本白書に記載されている会社名、製品名、及びサービス名は、それぞれ各社の商標または登録商標です。本文中では、™ または ® マークは明記しておりません。
・本白書に掲載しているグラフ内の数値の合計は、小数点以下の端数処理により、100% にならない場合があります。

情報セキュリティ白書 2026

サイバー防御新時代：諸刃の進化に備えよ

2026 年 10 月 19 日　PDF 版 第 1 版発行

企画・著作・制作・発行　**独立行政法人情報処理推進機構（IPA）**

〒 113-6591
東京都文京区本駒込2丁目 28 番8号
文京グリーンコートセンターオフィス 16 階
URL　https://www.ipa.go.jp/
電話　03-5978-7503
E-Mail spd-book@ipa.go.jp

表紙デザイン／本文 DTP・編集　**伊藤 千絵、久磨 公治、涌田 明夫、北林 俊平**

Copyright © 2026 Innovation Platform Agency, Japan（IPA）