情報セキュリティ白書

Information Security White Paper

2024

変革の波にひそむ脅威：リスクを見直し対策を

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

「情報セキュリティ白書2024」の刊行にあたって

「情報セキュリティ白書」は、2008 年以来、サイバーセキュリティ分野における、政策や脅威の動向、インシデントや被害の実態等をまとめ、皆様のセキュリティ対策の推進、学習・研鑽等にお役立ていただくという趣旨で発刊し、産業界、学界、一般の方に広く愛読されてきました。

昨今のサイバー空間の動向を振り返ってみると、新型コロナウイルスのパンデミックは収束し、経済・社会活動の回復とともに、働き方改革、デジタル化が大きく進展し、更には生成 AI の登場により変革の兆しが見えます。他方、2022 年 2 月に始まったロシア・ウクライナ戦争の長期化等、現下の厳しい国際情勢下において、重要インフラの機能停止、国民の情報や知的財産の窃取、民主プロセスへの干渉等のサイバー攻撃が顕在化し、サイバー空間が、地政学的緊張を反映した国家間の争いの場の一部ともなってきています。今後 AI の悪用によるサイバー攻撃の激化や高度化も懸念されるところです。

国内では、ランサムウェア被害が引き続き多数発生しています。2023 年 6 月の社会保険労務士向けクラウドサービスが被害を受けた事案や、同年 7 月の港湾コンテナターミナル内のシステム停止をもたらした事案等が発生しました。また、国民情報や知的財産の窃取を目的としたサイバー攻撃も顕在化し、とりわけ、ネットワーク境界の脆弱性を突いた攻撃が多数発生する等、攻撃に一層の巧妙化・高度化が見られます。今後、人手不足解消のための自動化等、デジタルライフラインにおける AI や IoT システムの社会実装が進み、サイバーリスクが、更に増大していくことが予想されます。このようなリスクに対処していくためには、サイバー空間を巡る、変容するリスクを国際的、経済的、地政学的側面から把握・分析し、リスクへの予見性を高めていくこと、そして、サプライチェーンやサイバーやフィジカルが融合した環境を前提として、システムの設計段階から脆弱性を取り除いていく、セキュア・バイ・デザインのアプローチが重要になっています。

各国においては、こうしたサイバー空間を巡る状況変化を踏まえ、セキュリティ対策の見直しが進められています。国内では 2023 年 7 月に政府機関等のサイバーセキュリティ対策のための統一基準群が全面改定、米国でも 2024 年 2 月にサイバーセキュリティフレームワーク（CSF）が 10 年ぶりに大きく改訂され、欧州では 2024 年の期限に向けて各国が NIS 指令及び EU サイバーレジリエンス法案の実装に取り組んでいます。また、AI に関する制度化、ガイドライン等の整備、法制化も進んでいます。2023 年 12 月には G7 において広島 AI プロセス包括的政策枠組みが示されました。我が国でも、AI の安全性に対する国際的な関心の高まりを踏まえ、AI の安全性の評価手法の検討等を行う機関として、2024 年 2 月、IPA に AI セーフティ・インスティテュートを設置しました。

本白書は、2023 年に生じた事柄を中心に、サイバー空間における脅威や技術の動向、それに対応する内外の政策的対応等について、包括的に記載をしています。本白書が多くの方々に利用され、サイバーセキュリティに関わる最新状況の把握と、それに伴う脅威やリスクに対する備えを実践するための一助となることを祈念します。

2024年7月

独立行政法人情報処理推進機構（IPA）

理事長 齋藤 裕

目次

コラム

2024

情報セキュリティ白書

序章

2023年度の情報セキュリティの概況

2023 年度は、国内では新型コロナウイルス感染症の 5 類移行により、停滞していた社会活動や経済活動に活気が戻ってきた。一方で、コロナ禍を一つの契機として業務のデジタル化が進み、事業の IT 依存度やシステム・サービス障害による影響が大きくなった。

企業・組織等が受けたサイバー攻撃の件数や被害金額は世界的に増加している。特に、国家の関与が疑われるネットワーク貫通型の攻撃は巧妙かつ執拗で、長期かつ広範囲に及ぶこともあるため深刻な被害を与えている。例えば、「Volt Typhoon」と呼ばれる組織による攻撃は 2021 年ごろから継続し、2023 年 5 月、2024 年 2 月には複数の国家のセキュリティ関係機関が連名で注意喚起を行っている。また、利用者が多いシステム・サービスの脆弱性への攻撃も続いている。企業向けファイル転送ソフトウェア MOVEit Transfer の脆弱性を狙った攻撃では、2024 年 3 月の時点で、全世界の 2,768 組織が被害を受けたという。激化するランサムウェア攻撃に対しては、国際協力により摘発や攻撃用ネットワークの破壊も行われている。2024 年 2 月のランサムウェア攻撃グループ「LockBit」の摘発では、約 10 ヵ国の捜査当局が連携した。

2023 年は、生成 AI の利用が急速に進み、悪用や誤用による脅威やリスクが注目され始めた。具体的には選挙等の政治的な宣伝戦、ロシア・ウクライナ戦争やイスラエル・ハマスの武力衝突等において生成 AI による偽・誤情報が拡散しているとの報道が続いた。国内でも偽・誤情報の生成・拡散の事例が確認されている。生成 AI は真実でないコンテンツを簡単に生成できるため、偽・誤情報の拡散に注意することが大切である。

国内では、2023 年 6 月に社会保険労務士向けクラウドサービスの事業者がランサムウェア攻撃を受け、約 1 ヵ月サービスが停止し、約 3,400 ユーザーの大半に影響が出た。2023 年 7 月には、「LockBit」のランサムウェア攻撃により名古屋港のコンテナターミナル内のシステムが 2 日半停止し、コンテナの搬出・搬入作業に大きな影響があった。サイバー攻撃によるシステムやサービスの停止により、物流のような社会インフラにも影響が出ることが再認識された。一方で、国内の個人情報漏えい、紛失事故の発生件数、流出した個人情報数は増加傾向にあり、過去最多となった。2023 年は内部不正による大量の情報漏えいも報告され、大手通信事業者のグループ企業の内部不正では、2 社で合わせて 1,500 万件を超える顧客情報漏えいが報告された。内部不正は組織の社会的信用を損なう恐れがあり、経営課題として対策に取り組む必要がある。

国外のセキュリティ政策としては、2024 年 2 月、米国 NIST がサイバーセキュリティフレームワーク（CSF）2.0 版を公開した。10 年ぶりとなる大きな改訂で、重要インフラにとどまらないすべての組織におけるサイバーセキュリティ対策の枠組みを示すものとして注目されている。また、2023 年 12 月に米国は「SBOM 管理のための推奨事項」を公表した。政府調達において取引先への SBOM 整備の義務化が進められている。欧州では、重要インフラに関し「NIS 指令」及び「EU サイバーレジリエンス法案」の実装を中心に取り組んでいる。EU 加盟国は 2024 年 10 月までに、自国の規定を NIS2 指令に準拠させるよう求められており、準備が進められている。

国内のセキュリティ政策としては「サイバーセキュリティ 2023」に基づき、対策の強化を進めている。2023 年 7 月には政府機関等のサイバーセキュリティ対策のベースラインとなる統一基準群の全面的な改定がされた。また、同時に「重要インフラのサイバーセキュリティに係る安全基準等策定指針」、更に 2024 年 3 月には「重要インフラのサイバーセキュリティに係る行動計画」の改定版を公表し、重要インフラのサイバーセキュリティ確保に向けた取り組みを示した。

2023 年度は AI の利用拡大に伴い、AI の安全性に関する政策面の取り組みも各国で進んだ。米国、英国、日本等において、AI の安全性に取り組む AI セーフティ・インスティテュートが各々設置される等、各国で短期間に法制化やガイドラインの整備、体制強化が進んでいる。日本は、2023 年 5 月に開催された G7 広島サミットにおいて「広島 AI プロセス」を発表し、AI の安全な利用に関する国際ルール作りに貢献している。

2023年度の情報セキュリティの概況

	主な情報セキュリティインシデント・事件	主な情報セキュリティ政策・イベント
2023 年　4 月	Wi-Fi ルーターで任意のコード実行を可能とする脆弱性が公開され、Mirai の亜種による悪用も観測（3.5.1）	
5 月	自動車メーカー子会社のデータがクラウド環境の設定ミスにより公開されていたことを公表（3.6.2） 国家の支援が疑われる攻撃者グループによるゼロデイ脆弱性を悪用した攻撃の観測を発表（1.2.2）	G7 広島サミットで官民が連携したサイバー攻撃対策を推進（2.1.1、2.2.1） CISA を含む各国の政府機関「Volt Typhoon」に関する合同のサイバーセキュリティ勧告を発表（2.2.2）
6 月	社会保険労務士向けクラウドサービスがランサムウェアによる不正アクセスを受けサービス停止（1.2.1） ファイル転送ソフトウェアに対するゼロデイ攻撃により情報漏えいやランサムウェア被害が発生（1.2.5）	「不正競争防止法等の一部を改正する法律」成立。ビッグデータ等を念頭にした限定提供データと、営業秘密の一体的な情報管理が可能に（2.1.3）
7 月	名古屋港のコンテナターミナルで利用しているシステムがランサムウェア攻撃を受けて停止（1.2.1） 顧客情報約 596 万件の不正持ち出しを大手通信会社が公表（1.2.8） 国家が支援する攻撃者グループによる、ネットワーク貫通型攻撃による不正アクセスを公表（1.2.2）	NISC「サイバーセキュリティ 2023」、「政府機関等のサイバーセキュリティ対策のための統一基準群」改定版、「重要インフラのサイバーセキュリティに係る安全基準等策定指針」改定版公開（2.1.1）
8 月	福島第一原発処理水放出に関する偽・誤情報拡散（4.1.3）	総務省「ICT サイバーセキュリティ総合対策 2023」公表（2.1.4） EU「デジタルサービス法（Digital Services Act）」発効（2.2.3）
9 月	米国フロリダ州の市が、建設業者を装ったビジネスメール詐欺に遭い約 120 万ドルを送金（1.2.3）	警察庁、NISC、米国諸機関は中国を背景とする攻撃グループ「BlackTech」に関する注意喚起を発出（1.2.2、2.1.5）
10 月	元派遣社員による顧客情報約 928 万件の不正持ち出しを大手通信会社グループ企業が公表（1.2.8） イスラエル・ハマス間の武力衝突勃発、フェイク画像拡散（2.2.1、4.1.3）	経済産業省、IPA「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク」開催（2.2.1） 米国、AI に関する大統領令 14110 発布（2.2.2）
11 月	生成 AI を使用した岸田首相の偽動画拡散（3.1.2）	英国「AI 安全性サミット（AI Safety Summit）」開催（2.2.1）
12 月	総合 IT 企業、約 94 万件の個人情報を含むファイルが閲覧可能な状態にあったと公表（1.2.8、3.6.2） 国際刑事警察機構、2023 年 7 月から 12 月にかけて 34 ヵ国が参加した国際的な取り締りを主導（1.2.3）	「広島 AI プロセス包括的政策枠組み」G7 首脳承認（2.2.1） EU サイバーレジリエンス法承認（2.2.3） 米国「SBOM 管理のための推奨事項」公表（2.2.2）
2024 年　1 月	能登半島地震が発生、SNS で偽･誤情報拡散（3.1.2、4.1.3） 台湾総統選挙に関連する偽・誤情報拡散（2.2.2、4.1.3） 米国大統領選挙の予備選において、Biden 大統領のディープフェイク音声拡散（4.1.3）	デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」改訂（2.1.2）
2 月	約 10 ヵ国の捜査当局、LockBit テイクダウンを実施（2.1.5、2.2.3）	AISI Japan 設立（4.1.4）。USAISI 設立（2.2.2） 「Volt Typhoon」に関する再度の合同のサイバーセキュリティ勧告を発表（2.2.2） NIST「サイバーセキュリティフレームワーク（CSF）2.0 版」公開（2.2.2）
3 月		NISC「重要インフラのサイバーセキュリティに係る行動計画」改定（2.1.1） IoT 製品のセキュリティラベリング最終取りまとめ公表（2.1.3、3.2.1、3.5.5） 欧州議会「AI 法」承認（2.2.3）

※ 2023 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。ランサムウェア被害、標的型攻撃、ビジネスメール詐欺、DDoS 攻撃、Web 改ざん、フィッシング等の攻撃や被害は通年で発生している。表中の数字は本白書中に掲載している項目番号である。特に注目されたもののみを挙げた。他のインシデントや手口と対策、及び政策・イベント等については本文を参照していただきたい。

第1章
情報セキュリティインシデント・脆弱性の現状と対策

2023年は、重要インフラを狙った攻撃や、ランサムウェアによる港湾施設やクラウドサービスへの被害が発生、ディープフェイクを用いたビジネスメール詐欺が出現したほか、フィッシングによる不正送金の被害額が過去最悪を記録した。情報漏えいでは、クラウドの設定不備等により、大規模なインシデントが複数発生した。本章では、国内外で発生した主なインシデントの概要、手口、対策、脆弱性の動向等について解説する。

1.1 2023年度に観測されたインシデント状況

本節では2023年度に観測された世界と日本における情報セキュリティインシデントの発生状況について概説する。

1.1.1 世界における情報セキュリティインシデント状況

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

(1) 国家の関与が疑われるサイバー攻撃の常態化

米国CSIS(Center for Strategic and International Studies)は防衛、安全保障、国際戦略等を専門とする非営利の政策研究機関である。CSISは、2006年以降に発生した、政府機関や国防・ハイテク関連企業を狙ったサイバー攻撃や、多額の被害をもたらした重大インシデントの一覧※1を公開している。この一覧には毎年100件程度の世界的に注目された事例が含まれ、その中には特定の国家の支援や関与が疑われるものが多い。ロシア・ウクライナ戦争に関連すると見られる事例以外にも、中国、北朝鮮、イラン、インド、パキスタン、ベトナム等の名前が攻撃関与国として取り上げられており、国家を背後とするサイバー攻撃は今や全世界で常態化していると言える。

国家の関与が疑われる具体例の一つは、2023年7月11日に公表された、Microsoft Corporation（以下、Microsoft社）の電子メールクラウドサービスに対する攻撃である※2。この攻撃にはアクセス元の検証に用いられる署名用秘密鍵が悪用されていたこと、及びクラウドサービス側の署名検証処理に欠落があったことが早期に特定されていた※3。後日、厳重に隔離された環境でのみ扱われる署名用秘密鍵が流出した原因についても調査結果が公表された。調査結果によると、隔離環境内で発生したシステムクラッシュの解析情報が、管理水準のより低い検証部門へと引き渡され、そこが攻撃を受け流出の起点となったことが判明したという※4。また、この攻撃により、同クラウドメールサービスを利用していた米国政府高官のメールアカウントが不正アクセスされた※5。技術水準の高さ、攻撃の行われた時間帯、目標等に鑑み、中国を拠点とする、国家の関与が疑われるグループによる攻撃であるとMicrosoft社では推定している。

中国による関与が疑われる重大なサイバー攻撃例としては、「Volt Typhoon」と呼ばれる集団による攻撃も引き続き警戒対象となっている※6。この攻撃は2021年頃から継続しており、SOHO(Small Office Home Office)向けのインターネットアクセス環境に多く見られる脆弱性を用い、米国の重要インフラ関連の情報システムに侵入することが判明している※7。2023年の1月末には、裁判所の許可を得て、この攻撃でマルウェアに感染した数百台のSOHO機器からなる攻撃用ネットワークを米国連邦捜査局(FBI：Federal Bureau of Investigation)が破壊した。本件に関する連邦議会・行政府委員会への報告の場において、FBIのChristopher Asher Wray長官は中国を名指ししている※8。しかしながらFBIによるこの作戦だけでは事態が収束せず、中国の活発な動きが続いていることを指摘しつつ各所への注意を喚起するアドバイザリーが、米国、英国、カナダ、オーストラリア、ニュージーランドのセキュリティ関係機関の連名で2023年5月24日と2024年2月7日に公開されている※9(「2.2.2

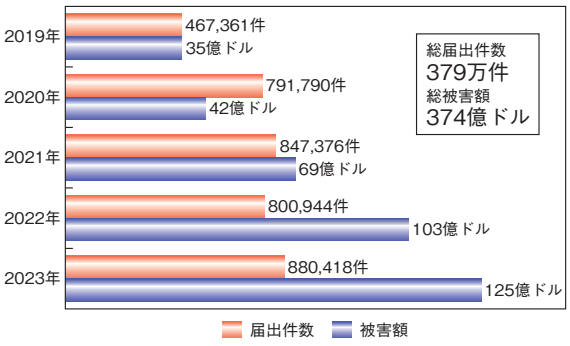
(2)(c)(ウ) Volt Typhoon に関するサイバーセキュリティ勧告」参照)。

Microsoft 社が実施した調査※10では、国家の関与が疑われる攻撃が広がっていることを、ロシア、イラン、中国、北朝鮮の動向を例示しながら指摘している。同調査の示唆の中で特に注目されるのは、この種の攻撃でいわゆる偽情報等を用いて他国の世論に影響を及ぼす工作を伴う傾向が強まっていることである。過去1年から2年で劇的な発達を見せている AI(Artificial Intelligence:人工知能)が既にこの種の攻撃に使用されているとの分析は、英国サイバーセキュリティセンター(NCSC:National Cyber Security Centre)による、当面のサイバーセキュリティ情勢に対する AI の影響の分析結果※11とも整合している。

公知されない数多くの隠れた事例があることも考慮すれば、国家の関与が疑われるサイバー攻撃の常態化と、AI を含む新たな技術によるその高度化という傾向は、今後も継続するものと推察される(標的型攻撃の事例については「1.2.2(2)標的型攻撃の事例」参照)。

(2)米国のサイバー犯罪の推移

FBI のインターネット犯罪苦情センター(IC3:Internet Crime Complaint Center)が公開している「Internet Crime Report 2023※12」によると、IC3 に届け出されたサイバー犯罪の被害額は増加が続いている(図 1-1-1)。

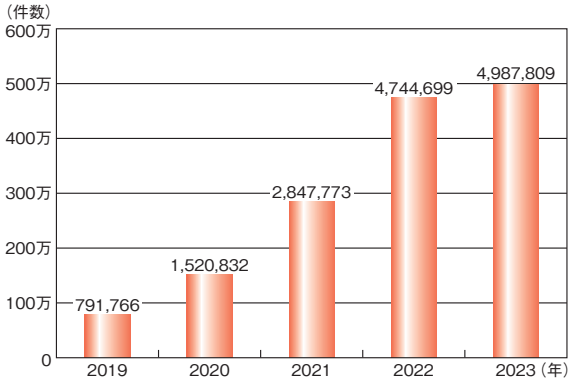


■図 1-1-1 サイバー犯罪の届出件数と被害額の推移(2019~2023年)
(出典)IC3「Internet Crime Report 2023」を基に IPA が編集

届出件数が 2020 年以降横ばいの推移を見せる一方で、2023 年の被害額は 125 億ドルに達した。このうち、約 29 億 4,700 万ドル分がビジネスメール詐欺(BEC:Business Email Compromise)となっている(ビジネスメール詐欺の被害総額の推移については「1.2.3 (1) ビジネスメール詐欺の被害状況」参照)。

(3)フィッシングの状況

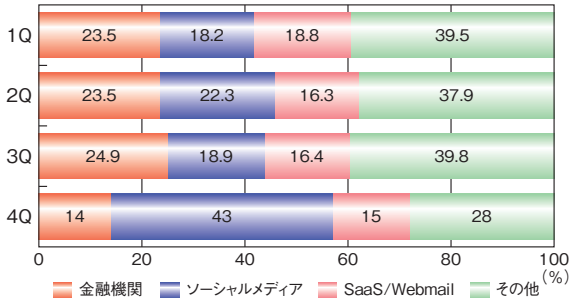
Anti-Phishing Working Group, Inc.(APWG)によると、2023 年に報告されたフィッシングメールに基づき特定された固有のフィッシングサイトの総数は約 499 万件であり、過去最大だった 2022 年の約 474 万件を上回った(図 1-1-2)。



■図 1-1-2 世界で報告されたフィッシングサイト件数(2019~2023年)
(出典)APWG「PHISHING ACTIVITY TRENDS REPORTS※13」を基に IPA が作成

2021 年から 2022 年にかけて見られた 66.6% もの大幅増加に比べ、勢いが鈍化した理由の一つは、フィッシングサイトのドメイン取得に多用されていた Freenom という無料ドメイン取得サービスが新規受付を停止したことにあるという※14。同サービスは Meta Platforms, Inc. から商標侵害で提訴され、2023 年1月にドメイン登録の新規受付を停止し、同年2月には事業撤退を表明した。これと同期してフィッシングサイト数も 2023 年中盤にかけて激減した。しかし、2023 年の後半には 2022 年以前と同様のフィッシングサイト数の増加傾向が確認されており、状況は改善していない※15。

フィッシングサイトによる偽装の対象となった業種の構成の変化を四半期ごとに見ていくと、第4四半期に「ソーシャルメディア」の割合が倍増し、全体の4割以上を占めるようになった(図 1-1-3)。

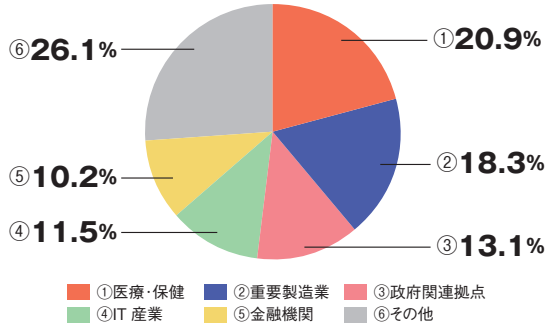


■図 1-1-3 業種別・四半期ごとのフィッシングサイト構成比(2023年)
(出典)APWG「PHISHING ACTIVITY TRENDS REPORTS」を基に IPA が作成

APWG の報告書では、SMS や電話等の音声案内を使ったフィッシングも増大しているとして、注意を喚起している[※15]。

(4) ランサムウェアの状況

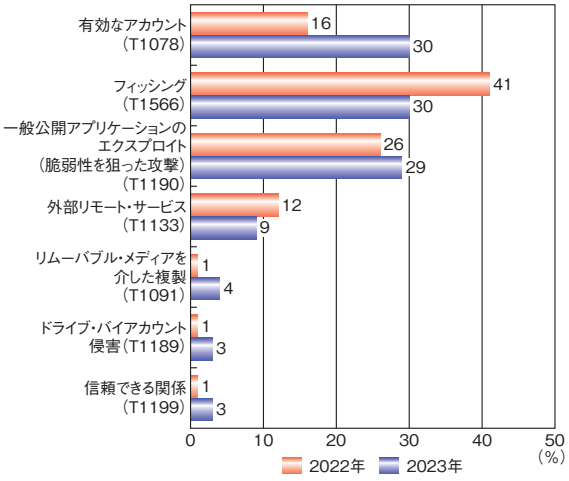
IC3 の「Internet Crime Report 2023」によれば、ランサムウェアの被害件数は対 2022 年比で 18% 増、被害額は 74% 増となった。被害件数よりも被害額の伸びの方が大きいことから分かるように、1 件あたりの被害額は 46% 増大しており、1 件あたりの被害の影響が大きくなっていることが読み取れる。また、図 1-1-4 に示すとおり、被害を受けた上位 5 業種に目を向けると、人命や経済に大きな影響を与える業種が並んでおり、これらの分野における警戒を高める必要があると言える。なお、この上位 5 業種の順位は 2022 年と同じである[※16]。



■図 1-1-4　ランサムウェア被害の業種別構成比（2023 年）
（出典）IC3「Internet Crime Report 2023」を基に IPA が作成

近年のランサムウェア被害は外部からネットワークに侵入した攻撃者によって引き起こされる。日本アイ・ビー・エム株式会社（以下、IBM 社）の「X-Force 脅威インテリジェンス・インデックス 2024[※17]」によれば、2023 年における侵入の開始段階の初期アクセス経路の割合は、「有効なアカウント」「フィッシング」「一般公開アプリケーションのエクスプロイト（脆弱性を狙った攻撃）」がそれぞれ約 30% と横並びであり、この三つで 89% を占めた（図 1-1-5）。

ランサムウェア攻撃を成立させるためには、ランサムウェアであるウイルス[※18]を被害対象組織内のコンピューターに感染させる必要があり、前述の三つの初期アクセス経路はいずれもその手段になり得る。また、同調査の分析によれば、ネットワークに侵入した攻撃者のうちの 43% がウイルスのインストールを試み、その半分近い 20% がランサムウェアのインストールであるという。特によく観測されたランサムウェア攻撃は、BlackCat、Clop（Cl0p とも表記される）、LockBit、Black Basta、Royal によるものであったという。



■図 1-1-5　上位の初期アクセス経路（2022 年と 2023 年の比較）
（出典）IBM 社「X-Force 脅威インテリジェンス・インデックス 2024」を基に IPA が編集

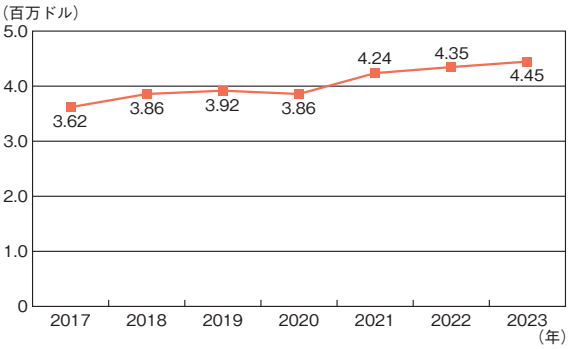
2023 年度中の事例では、Clop を用いた犯行が特に目立った。とりわけ、企業向けファイル転送ソフトウェアである MOVEit Transfer を対象に 2023 年 5 月ごろから広がった攻撃の被害が大きく、2024 年 3 月 19 日時点で、全世界で 2,768 組織が被害を受けたとの調査結果[※19]が示されている（「1.2.5 (3) (a) MOVEit Transfer の脆弱性を狙った攻撃事例」参照）。Fortra, LLC の GoAnywhere MFT という別のファイル転送ソフトウェアを対象にした 2023 年 1 月の攻撃でも Clop が用いられ、やはり 100 以上の組織で被害が発生している。Clop を用いた攻撃が始まったのは少なくとも 2019 年にさかのぼると見られる[※19]。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）では、背後にいる攻撃グループが、米国を拠点とする 3,000 以上の組織に加え、全世界で 8,000 組織に被害を与えたと推定している[※20]。

2023 年 2 月に発生した、VMware, Inc. の製品 ESXi を対象としたランサムウェア攻撃も多大な被害をもたらした。この攻撃で用いられたランサムウェアは「ESXiArgs」と呼ばれ、全世界で 3,800 台以上のサーバーが被害を受けたと見られる[※21]。ESXiArgs が悪用する脆弱性は、2023 年 2 月時点で最新版の ESXi にはなく、旧版だけに含まれる。そのため、ESXi の更新等の対策が VMware, Inc. から攻撃発生直後に示されている。しかし、ESXi を対象にした攻撃は 2023 年 5 月時点でもむしろ悪化傾向にあるとして、サイバーセキュリティの専門企業によって注意喚起がなされた[※22]。

近年のランサムウェア攻撃では、不特定多数の対象に攻撃を仕掛けるのではなく、事前に偵察等を行った対象のネットワークに侵入して着実に被害をもたらす傾向があるとされ※23、犯罪として悪質度や影響度が増していると言える。また、必ずしもデータの暗号化を行わずに窃取し、公開されたくなければ身代金を払うようにと脅迫する「ノーウェアランサム」という攻撃形態も現れ※24、手口も多様化している。その一方で、世界的に大きな被害をもたらしているランサムウェア攻撃グループ「LockBit」が、日本の警察庁を含む全世界10ヵ国の捜査当局の連携により2024年2月に摘発された※25。LockBitによる被害は数十億ドルにも上る可能性があるという※26（ランサムウェア攻撃については「1.2.1 ランサムウェア攻撃」参照）。

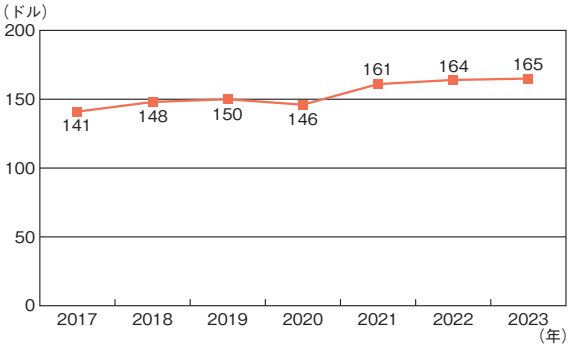
(5) 情報漏えいインシデントの状況

IBM社の「データ侵害のコストに関する調査 2023年※27」によれば、データ侵害を受けた組織において被害者への対応や機会損失等により生じる平均総コストは図1-1-6のとおり増加の一途をたどっている。



■図1-1-6　データ侵害の平均総コスト（2017～2023年）
（出典）IBM社「データ侵害のコストに関する調査 2023年」を基にIPAが編集

漏えいしたデータ1件あたりのコストも図1-1-7のとおりに増加し続けている。



■図1-1-7　データ侵害のレコード1件あたりのコスト（2017～2023年）
（出典）IBM社「データ侵害のコストに関する調査 2023年」を基にIPAが編集

以下では、規模が大きな漏えい事例二つと、ランサムウェア攻撃との関連が懸念される事例一つを示す。

- 2024年3月、米国通信キャリア大手のAT&T Inc.は同社の顧客・元顧客の情報の漏えいを確認したと発表した※28。漏えいデータはダークウェブ上で販売されており、同社によれば2019年以前に取得したものと見られるという。漏えいデータには氏名・電話番号等に加え、社会保障番号やアカウントのパスコードが含まれ、現在の顧客約760万人と元顧客約6,540万人が影響を受けることとなった。特に、現顧客760万人に対してはパスコードの強制リセットを実施した※29。同社のシステムに対する不正アクセスは発表時点で確認されておらず、引き続き調査中である。他方、漏えいしたパスコードに施されていた暗号化が不十分との指摘※30もあり、個々の顧客に対する派生的な被害が今後広がる恐れがある。
- 2023年8月8日、英国の選挙委員会は同委員会の情報システムに対するサイバー攻撃によって、選挙人名簿に含まれる個人情報が漏えいした可能性があると発表した※31。当該情報は住所・氏名等であって投票内容は含まれず、対象となった個人に大きな影響を与えるものではないとされる。技術的にはファイル共有サーバーやメールサーバーを狙った高度な攻撃であり、2022年10月ごろに発覚するまで1年以上にわたって続き、4,000万人分以上の情報が漏えいした恐れがあるとされた※32。2024年3月には、英国政府が本件の背後に中国政府の関与があると名指しした上で、他のサイバー攻撃事案も背景としつつ、関連企業と容疑者らに対する制裁を課した※33。この動きは米国・英国の共同の取り組みとなっており、関連する制裁が米国においても同時に発表されている※34。
- 2023年9月11日、米国MGM Resorts International（以下、MGM Resorts社）がランサムウェア攻撃を受けたことが報道された※35。同社はアイデンティティプロバイダーサービスを提供する米国Okta Inc.（以下、Okta社）の顧客であり、MGM Resorts社への攻撃に際してはソーシャルエンジニアリングを用いてOkta社のサービスの多要素認証を無効化する手法※36が用いられたと見られている。この攻撃ではVMware, Inc.のESXiの脆弱性も突かれており、複数の脆弱性と攻撃手法が融合した複合的な攻撃が展開されたと言える。なお、9月28日にはOkta社のカスタマーサポートシステムもサイバー攻撃を受け、同社の顧客の氏名とメールアドレスが漏えいした※37。Okta社か

ら漏えいした情報はソーシャルエンジニアリングの材料として活用でき、MGM Resorts 社の類例となる攻撃の発生が懸念される。

AT&T Inc. 及び Okta 社の事例は、セキュリティの基盤となる事業者が標的になっている実例としても示唆的である。情報漏えいによる直接的被害だけでなく、漏えいした情報を用いた攻撃の可能性があり、MGM Resorts 社への攻撃は、これが現実のものであることを示している。

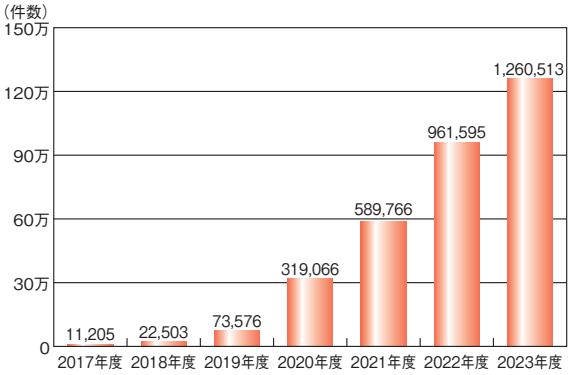
1.1.2 国内における情報セキュリティインシデント状況

国内における情報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※38」
- 警察庁：「令和 5 年におけるサイバー空間をめぐる脅威の情勢等について※24」「令和 4 年におけるサイバー空間をめぐる脅威の情勢等について※39」「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について※40-1」（以下、2021 ～ 2023 年の警察庁資料）
- 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）：「JPCERT/CC インシデント報告対応レポート 2024 年 1 月 1 日～2024 年 3 月 31 日※40-2」

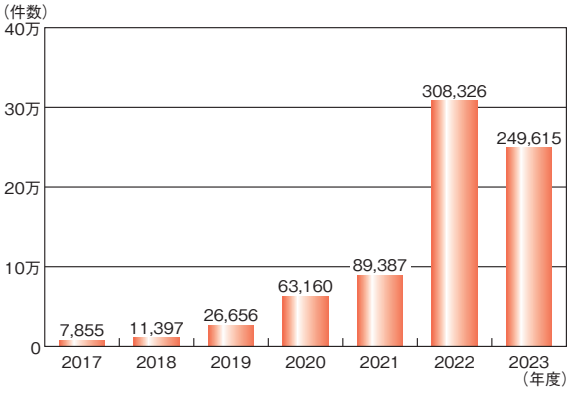
(1) フィッシングによる被害

フィッシング対策協議会への 2023 年度のフィッシング報告件数は 126 万 513 件で、2022 年度（96 万 1,595 件）から 31.1% 増となり、報告件数としては初めて 100 万件を超える結果となった（図 1-1-8）。



■図 1-1-8　年度別フィッシング報告件数（2017～2023 年度）
（出典）フィッシング対策協議会「月次報告書」（2017 年 4 月～ 2024 年 3 月）を基に IPA が作成

重複を除いて集計したフィッシングサイトの URL 件数では、2022 年度まで増加傾向だったものの、2023 年度は 24 万 9,615 件と減少に転じた（図 1-1-9）。



■図 1-1-9　年度別フィッシングサイトの URL 件数（2017～2023 年度）
（出典）フィッシング対策協議会「月次報告書」（2017 年 4 月～ 2024 年 3 月）を基に IPA が作成

フィッシングに悪用されたブランド数を表 1-1-1 に示す。2023 年度は 1,035 件となり、2 年連続で 1,000 ブランドを超える結果となった。5 年前と比較すると 2 倍以上になっており、フィッシングにおいて多くのブランドがかたられていることがうかがえる。

	2017 年度	2018 年度	2019 年度	2020 年度	2021 年度	2022 年度	2023 年度
ブランド数	274	423	641	704	985	1,105	1,035

■表 1-1-1　年度別悪用されたブランド数（2017～2023 年度）
（出典）フィッシング対策協議会「月次報告書」（2017 年 4 月～ 2024 年 3 月）を基に IPA が作成

報告件数の多かったブランドを見ると、月によって全体に占める割合の順位は入れ替わるが、「Amazon」をかたるフィッシングは 12 ヵ月連続で上位 3 位以内に入っている。ほかにも多くのクレジットカードブランドが上位にランクインしている。また、1 ヵ月に 1,000 件以上の大量の報告を受けたブランドは、2023 年度は月平均約 15 ブランドで、いずれの月でも報告件数全体の 9 割を占める。

フィッシング対策協議会から、2023 年 10 月に「URL に飾り文字などが含まれたフィッシング※40-3」、同年 11 月に「URL に特殊な IP アドレス表記を用いたフィッシング※40-4」が緊急情報として発出されている。これらの緊急情報では、フィッシングサイトの URL に飾り文字や 8/10/16 進数等の IP アドレス表記を用いることでフィルター回避を試みる※40-5 手口について注意喚起している。

また、スマートフォンの SMS（ショートメッセージ）から

フィッシングサイトに誘導するスミッシングの手口も報告され、2023年4～5月には4件の緊急情報[※40-6]が発出されている（SMSを悪用した手口については「1.2.6（1）SMSを悪用した手口」参照）。

ほかにも、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）は、2023年11月に公開した運用状況のレポート[※40-7]で、メールの受信者にフィッシングサイトのURLを変換したQRコードを読み取らせようとするフィッシング攻撃の事例を公開している。このようなQRコードをフィッシングに用いる手口は「クイッシング」と呼ばれており、フィッシング報告件数の増加とともに手口の巧妙化もうかがえる。フィッシング被害に遭わないためにも、手口等の最新情報を知ることや、メール、SMS等に記載されるURLやQRコードにはより慎重になることが求められる。

（2）内部不正による被害

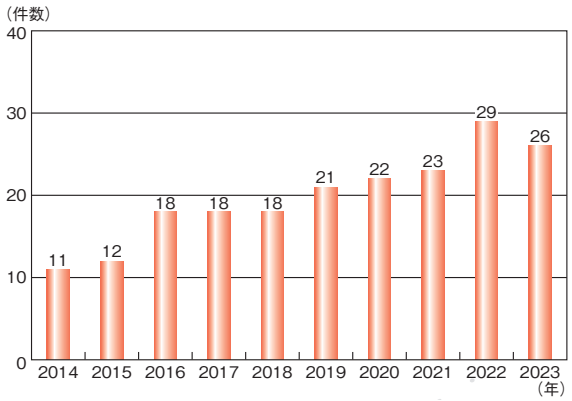
株式会社東京商工リサーチが2024年1月に公開した「2023年『上場企業の個人情報漏えい・紛失事故』調査[※40-8]」の結果によると、2023年に上場企業とその子会社から公表された個人情報の漏えい・紛失事故の件数は175件で、そのうち、「不正持ち出し・盗難」が原因で個人情報が漏えい・紛失した件数は24件であった。また、2023年に漏えいした個人情報は4,090万8,718人分であり、前年比690.2%と大幅に増え、最多を更新した。

同調査によると、個人情報が漏えいした可能性のある事案別の人数では、最多は、NTTグループの内部不正による持ち出し事案[※40-9]の928万人分であり、3番目も株式会社NTTドコモの業務委託先の元派遣社員によって596万人分が持ち出された事案[※40-10]であった（事案の詳細については「1.2.8（4）（a）内部不正による情報漏えい事例」参照）。上位3件のうち2件が内部不正による事案であり、2件合わせて1,524万人分（全体の37.3%）の情報が漏えいした。

2024年2月にIPAから公開された「情報セキュリティ10大脅威2024[※40-11]」においても、組織向けの脅威として「内部不正による情報漏えい等の被害」は3位となり、2016年以降9年連続の選出となっている。

また、内部不正には情報漏えいだけでなく、不正競争防止法違反（知的財産権審判事犯の一部）の事例も含まれる。警察庁によれば、2023年の営業秘密侵害事犯の検挙事件数は26件で2022年の29件に次ぐ件数であり、依然として高い水準で推移している（図1-1-10）。

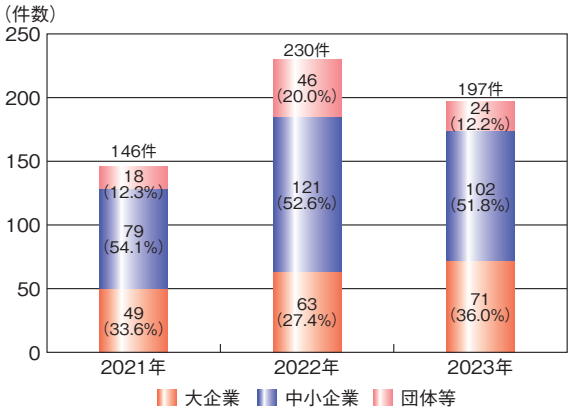
組織としては、情報管理を徹底するほか、情報の取り扱いに関するポリシーの整備や秘密保持誓約書の締結、内部不正者の処分等に関する規則の整備等のガバナンスの強化、見直しに取り組む必要がある。



■図1-1-10　営業秘密侵害の検挙事件数（2014～2023年）
（出典）警察庁「令和5年における生活経済事犯の検挙状況等について[※40-12]」を基にIPAが編集

（3）ランサムウェアによる被害

2023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197件で前年比14.3%減となったものの、前々年比では34.9%増と依然として高い水準で推移している（図1-1-11）。件数の内訳を企業（大企業・中小企業）・団体の種別で見ると、大企業については、年々被害件数が増加している。



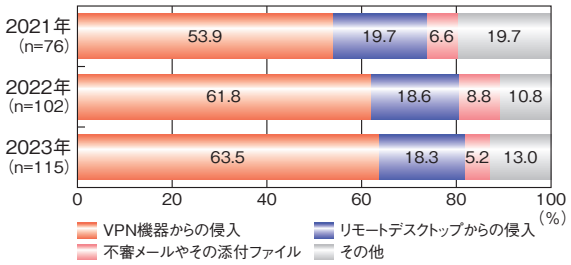
■図1-1-11　国内のランサムウェアによる被害件数（2021～2023年）
（出典）2021～2023年の警察庁資料を基にIPAが作成

2023年の被害件数を業種別で見ると、「製造業」の割合が最も大きく34.0%（67件）で、次いで「卸売・小売業」16.8%（33件）、「サービス業」13.7%（27件）と続く。それ以降は「情報通信業」「建設業」「医療・福祉」「金融業・保険業」がそれぞれ10%未満で続いている。「製造業」は3年連続で最も被害が多い結果となったが、業

種を問わず被害が発生している傾向は変わっていない。

また 2023 年に被害の報告があった 197 件のうち手口を確認できたのは 175 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」が 74.3%（130 件）を占めた。ここ 3 年間では過半数以上の割合を占める手口となっている。一方、最近の手口として、197 件とは別に、データの暗号化はせずに窃取したデータに対して対価を要求する「ノーウェアランサム」と呼ばれる攻撃の被害が 30 件確認されたという（ノーウェアランサムについては「1.2.1（1）（d）暗号化を伴わない攻撃手口」参照）。

警察庁では、ランサムウェア被害の実態を把握するために、ランサムウェアによる被害のあった企業・団体等に対して、アンケート調査を実施している。2023 年のランサムウェアの感染経路としては、アンケート調査の有効回答 115 件のうち、「VPN 機器からの侵入」が 63.5%（73 件）、「リモートデスクトップからの侵入」が 18.3%（21 件）を占めており、2022 年に引き続きこれらテレワーク時に利用される機器等からの侵入が 80% を超えている（図 1-1-12）。



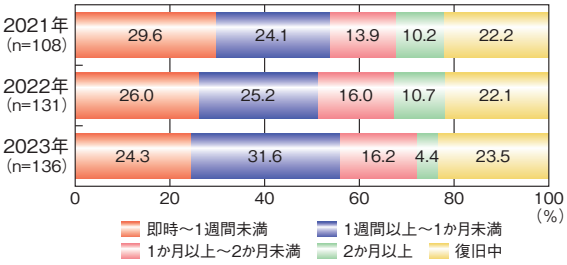
■図 1-1-12　ランサムウェアの感染経路（2021～2023 年）
（出典）2021～2023 年の警察庁資料を基に IPA が作成

侵入経路とされる機器の「セキュリティパッチ」（修正プログラム）の適用状況では、有効回答 86 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 34 件（40%）と半数未満で、未適用のセキュリティパッチがあったのは 52 件（60%）であった。

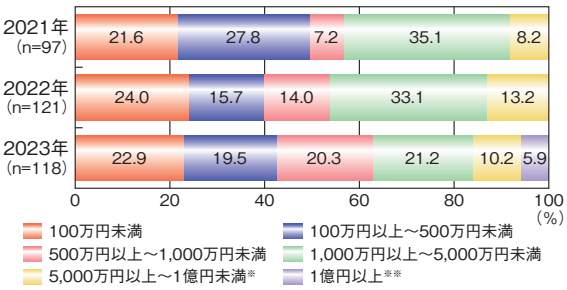
被害に遭った企業・団体等の復旧等に要した期間・費用について 3 年間の推移を図 1-1-13 と図 1-1-14 に示す。

復旧に要した期間では、2022 年と比較すると、2023 年は復旧に「2 か月以上」要した割合が 10.7% から 4.4% と減少し、「1 週間以上～ 1 か月未満」であった割合が 25.2% から 31.6% と増加しており、復旧に要する期間が短縮されている傾向が見て取れる。

調査・復旧に要した費用の割合では、2023 年は「5,000 万円以上」の割合が過去 3 年間で最も大きい。また、2023 年から「1 億円以上」の項目が設けられており 5.9%（7 件）が該当した。



■図 1-1-13　復旧に要した期間（2021～2023 年）
（出典）2021～2023 年の警察庁資料を基に IPA が作成



※「令和4年におけるサイバー空間をめぐる脅威の情勢等について」「令和3年におけるサイバー空間をめぐる脅威の情勢等について」では「5,000万円以上」
※※「令和5年におけるサイバー空間をめぐる脅威の情勢等について」から設けられた

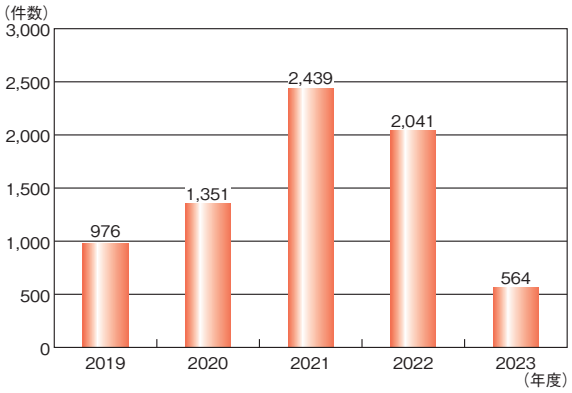
■図 1-1-14　調査・復旧に要した費用（2021～2023 年）
（出典）2021～2023 年の警察庁資料を基に IPA が作成

被害に遭ったシステム、機器のバックアップの取得状況については有効回答 140 件のうち、バックアップを取得していたのは 132 件（94.3%）であり、2022 年の 83.5% から 10.8 ポイント増えていた。取得していなかったのは 8 件（5.7%）であった。また、バックアップからの復元結果については有効回答 126 件のうち、復元できたのは 21 件（16.7%）で、被害直前の水準まで復元できなかったのは 105 件（83.3%）となった。バックアップが復元できなかった理由としては有効回答 104 件のうち、「バックアップも暗号化されたため」が 72 件（69.2%）、「運用の不備」が 16 件（15.4%）となっている。

2023 年に被害に遭った企業・団体等（有効回答 145 件）のうち、すべての業務が停止に追い込まれたのは 13 件（9.0%）であり、一部の業務に影響のあった 126 件（86.9%）と合わせると 139 件（95.9%）にもなる。ランサムウェアによる被害は 2023 年も高止まりしており、今後もランサムウェアに対する対策の強化が求められる（「1.2.1 ランサムウェア攻撃」参照）。

(4) Web サイト改ざんによる被害

2023 年 4 月 1 日から 2024 年 3 月 31 日までに JPCERT/CC に報告された Web サイト改ざん件数は 564 件で、2022 年度 (2,041 件)※40-13 の 27.6% であり、過去 5 年間では最小となった(図 1-1-15)。



■図 1-1-15　Web サイト改ざん年度別件数推移(2019～2023 年度)
(出典)JPCERT/CC「インシデント報告対応レポート」(2019 年 4 月 1 日～2024 年 3 月 31 日)を基に IPA が作成

COLUMN

守るだけではない、被害を最小限にするためのセキュリティ対策を

新型コロナウイルス等のウイルスの感染を防止するには、ワクチン接種や換気、マスク着用、手洗い、消毒等の感染対策がありますが、絶対に感染しないという保証はありません。感染してしまった場合は、周囲に感染させない対策をして、早く治療することが大切です。

実は、セキュリティ対策も同じで、「守る」ことに加えて、サイバー攻撃を受けた場合に被害を拡大させず、いかに早く復旧するかについて計画と準備をしておくことが大切です。では、どのように守り、復旧の計画と準備をしていくべきでしょうか。米国では、業種や企業規模等に依存しないサイバーセキュリティ対策のフレームワークとして「Cyber Security Framework(CSF)[i]」が定められており、その Version 2.0 が 2024 年 2 月に公開されました。

CSF は、「識別(Identify)」「防御(Protect)」「検知(Detect)」「対応(Respond)」「復旧(Recover)」「統治(Govern)」の六つのカテゴリーで構成されています。「識別」はサイバー攻撃から守るべき情報を特定しておくこと、「防御」は守るべき情報を保護する対策を実施すること、「検知」はサイバー攻撃の兆候や発生を把握すること、「対応」はサイバー攻撃を受けた場合の報告や被害拡大防止の手順をあらかじめ計画しておき実行すること、「復旧」は被害を受けた機能やサービスの復旧の計画や手順をあらかじめ計画しておき実行すること、そして「統治」は識別、防御、検知、対応、復旧に対して包括的に管理していくことです。

これら六つのカテゴリーの対策を実施することで、サイバー攻撃から守るだけでなく、攻撃された場合の影響を最小限にとどめ、早期の復旧につなげることができます。更に、いざというときの対応と復旧が計画どおり行えるよう訓練を行い、訓練の中での気付きを計画や手順にフィードバックしておくことも重要です。

CSF は、サイバーセキュリティ対策の効果を数値で評価するための基準も含む、体系的なガイドラインとなっており、日本でも多くの企業・組織が参考にしています。CSF を参考にして、被害を最小限にするため、攻撃を受ける前提で対策を行いましょう。

i　https://www.nist.gov/cyberframework〔2024/5/30 確認〕

COLUMN

情報セキュリティ10大脅威 2024
～脅威に呑まれる前に十分なセキュリティ対策を～

IPA では毎年、ランキング形式で「情報セキュリティ 10 大脅威」を発表してきましたが、下位の脅威への対策が疎かになることを懸念して 2024 年版からは「個人」向け脅威について順位の掲載を取り止めました。「組織」向け脅威については引き続き順位を掲載していますが、本コラムでは順位ではなく、2016 年以降における 10 大脅威の選出状況に着目してみます。

表　情報セキュリティ 10 大脅威 2024「組織」向け脅威

順位	「組織」向け脅威	初選出年	選出状況
1	◆ランサムウェアによる被害	2016 年	9 年連続 9 回目
2	◆サプライチェーンの弱点を悪用した攻撃	2019 年	6 年連続 6 回目
3	◆内部不正による情報漏えい等の被害	2016 年	9 年連続 9 回目
4	◆標的型攻撃による機密情報の窃取	2016 年	9 年連続 9 回目
5	◆修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022 年	3 年連続 3 回目
6	不注意による情報漏えい等の被害	2016 年	6 年連続 7 回目
7	脆弱性対策情報の公開に伴う悪用増加	2016 年	4 年連続 7 回目
8	◆ビジネスメール詐欺による金銭被害	2018 年	7 年連続 7 回目
9	◆テレワーク等のニューノーマルな働き方を狙った攻撃	2021 年	4 年連続 4 回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017 年	2 年連続 4 回目

上記の表の◆が付いた脅威は、初めて 10 大脅威に選出された年から、2024 年まで選出され続けている脅威で、全体の 7 割を占めています。そのため、「毎年状況は変わっていない」と感じられるかもしれません。しかし、これは「毎年話題になっているのに、対策しきれていない組織があるため、被害が続いてしまっている」ともとらえられるのではないでしょうか？「ランサムウェアによる被害」で脅迫の種類が増えていたり、「サプライチェーンの弱点を悪用した攻撃」では組織のつながりだけでなく、ソフトウェアやサービスのつながりを悪用する事例も発生したりと、攻撃手口の変化が見られるケースも発生しています。また、「内部不正による情報漏えい等の被害」では元従業員による機密情報の漏えいが毎年ニュースで報道されています。

「組織」のセキュリティ対策では、自組織だけでなく取引先等、自組織と関係する組織も意識することが必要ですが、それだけでなく自組織の役職員「個人」も意識した対策が必要です。役職員は「組織」に所属していても同時に「個人」でもあるため、「組織」としてセキュリティ対策を行う際は「個人」向け脅威も理解しておく必要があります。ぜひ、以下の URL から「情報セキュリティ 10 大脅威 2024」や解説書をダウンロードし、チェックしてみてください。社内教育に使える資料等も公開していますのでご活用ください。

https://www.ipa.go.jp/security/10threats/10threats2024.html

1.2 情報セキュリティインシデント別の手口と対策

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、2023 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 ランサムウェア攻撃

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

従来のランサムウェア攻撃は、メールや悪意のあるWeb サイトからのダウンロード等により、不特定多数のコンピューターをランサムウェアに感染させようとするばらまき型の攻撃であった。しかし、近年のランサムウェア攻撃は、攻撃者が被害企業・組織（以下、被害組織）のネットワークへ密かに侵入し、侵害範囲を拡大しつつ、大量のデータをランサムウェアによって暗号化するといった攻撃へと変化しており、事業継続に大きな影響を与える重大な脅威となっている。本項では、このようなランサムウェア攻撃を「侵入型ランサムウェア攻撃」と呼ぶ。

侵入型ランサムウェア攻撃では、データの復旧と引き換えに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。

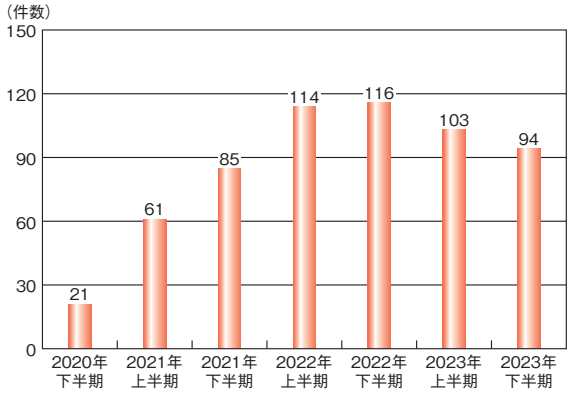
また、データの暗号化は行わずに、窃取したデータを公開すると脅迫して対価を要求する手口も確認されている。警察庁は、このようなデータの暗号化が伴わない攻撃を、ランサムウェアを使わず（暗号化せず）に身代金を要求することから「ノーウェアランサム攻撃」と名付け、注意喚起を行った※41。本項では、ノーウェアランサム攻撃についても解説する。

(1) ランサムウェア攻撃の傾向

2023 年度におけるランサムウェア攻撃の傾向について説明する。

(a) 被害件数

警察庁が公表した「令和 5 年におけるサイバー空間をめぐる脅威の情勢等について」（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、2023 年上期が 103 件、下期が 94 件である。図 1-2-1 のとおり、2022 年上期以降は継続して高い水準で推移している。なお、ノーウェアランサム攻撃による被害件数（30 件）は、図 1-2-1 の報告件数には含まれない。また、その他の警察庁によるランサムウェア被害の調査結果については「1.1.2(3)ランサムウェアによる被害」を参照いただきたい。



■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 5 年におけるサイバー空間をめぐる脅威の情勢等について※42」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）」と呼ばれる攻撃モデルの普及に見られるように、攻撃者の組織化や分業化が進んだことが影響していると考えられる。

(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※42。また、近年では、サプライチェーンに残存するセキュリティの脆弱な箇所として国内企業の海外拠点が狙われるといった事例も確認されており、その被害はサプライチェーン全体に波及する恐れがある※43。これらのことから、企業の業種や規模を問わずサプライチェーン全体でのセキュリティ対策が重要といえる。

(c)ネットワークへの侵入手口

警察庁資料によると、2023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製品やリモートデスクトップからの侵入が多く、被害を受けた企業・団体から得られた有効回答中の約82%を占めた[※42]。侵入された原因は、それらの機器やソフトウェアの脆弱性、弱い認証情報の悪用と考えられるものであった。このように、VPN製品やリモートデスクトップサービスが攻撃者に狙われていることを認識し、企業・組織は対策を講じる必要がある。

(d)暗号化を伴わない攻撃手口

警察庁資料によると、データを暗号化することなく窃取した上で、被害組織に金銭を要求する攻撃（ノーウェアランサム攻撃）による被害が、2023年に30件確認された[※42]。

この手口では、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ったり、システム障害といった目に見える事象が発生せず、攻撃者からの脅迫を受けるまで被害が発覚しない可能性がある。

この手口が使われるようになった理由の一つとして、データの暗号化を行わないため、攻撃者は管理者権限を奪取する必要がなく、従来よりも少ない労力で効率的に攻撃を仕掛けられることが挙げられる[※44]。また、被害組織は、自組織のブランドや信頼を守るために、被害を公表せず身代金を支払うことで、穏便に解決することができると考えてしまう恐れもあるという[※45]。

このような傾向から、ノーウェアランサム攻撃は、今後の攻撃手口の一つとして拡大することが考えられるため、注意が必要である。

(2)ランサムウェア攻撃の被害事例

2023年度に公表された国内における侵入型ランサムウェア攻撃及びノーウェアランサム攻撃の主な被害事例を紹介する。その他の被害事例については、IPAが公開している「コンピュータウイルス・不正アクセスの届出事例[※46]」の「身代金を要求するサイバー攻撃の被害」の記載を参照いただきたい。

(a)港湾事務所における被害事例

名古屋港運協会は、2023年7月5日、侵入型ランサムウェア攻撃を受けたことから、名古屋港すべてのコンテナターミナル内で利用している統一ターミナルシステムを停止したと発表した[※47]。

その後、7月26日に経緯報告として、被害の内容や原因等を公表した[※48]。被害内容としては、データセンター内にある同システムのすべてのサーバーが暗号化されたというものであった。調査の結果、情報漏えいの形跡は確認されていないという。また、攻撃者への連絡も行っていないとしている。

攻撃者の侵入経路は三つの可能性が考えられており、そのうちの一つであるシステム保守用のVPN機器から侵入された可能性が高いと見られている。その理由は、VPN機器に送信元のIPアドレス制限や多要素認証を設定しておらず、IDとパスワードのみでログインできる状態であったためである。また、VPN機器及び物理サーバーに関して脆弱性が公表されていたものの、未対応な状態であったことも判明している。なお、その他二つの侵入経路としては、USBメモリー経由や、港運事業者間のネットワーク接続箇所が考えられているが、ログが暗号化されているため調査は困難であるという[※49]。

続いて、復旧対応の時系列を表1-2-1に示す。同事例では、システム停止の発生から約2時間半後に愛知県警察本部サイバー攻撃対策隊に連絡を行い、約4時間後には復旧を最優先する判断が行われる等、早期に対応が進められた。その後、バックアップデータから復元した仮想サーバーからもウイルスが検知される等の困難もあったが、迅速な初動により約2日半で復旧した

日時	対応の内容
7月4日（火）	
6:30頃	システムの動作停止を確認
7:15頃	システム保守会社、開発会社へ調査を依頼
9:00頃	愛知県警察本部サイバー攻撃対策隊に連絡 ランサムウェア感染の可能性があるとの見解
10:30頃	復旧優先の判断を行い、復旧作業を開始
7月5日（水）	
2:00頃	物理サーバー基盤全8台を復旧 仮想サーバー45台の復元作業を開始
12:00頃	ランサムウェア感染のプレスリリース公表
21:00頃	復元した仮想サーバーからウイルス検知
7月6日（木）	
7:15頃	ウイルス駆除終了 システム間の連携に障害が発生
14:15頃	連携障害を解消
15:00～18:15	順次、各ターミナルで作業を再開

■表1-2-1　ランサムウェア攻撃の対応時系列（抜粋）
（出典）コンテナターミナルにおける情報セキュリティ対策等検討委員会「名古屋港のコンテナターミナルにおけるシステム障害を踏まえ緊急に実施すべき対応策及び情報セキュリティ対策等の推進のための制度的措置について[※49]」を基にIPAが編集

という。

同事例は「LockBit」と呼ばれる攻撃グループによるものと判明している。同グループについては、2022年第4四半期に世界と日本で最も活発な活動が確認されており、2023年上半期に日本で確認された二重の脅迫を行うランサムウェア攻撃の中でも、最も検出台数が多いとされている※50。2024年2月20日、日米欧等約10ヵ国が参加する共同捜査にて同グループが摘発され、サーバーの停止、メンバー2名の逮捕、資産の凍結等が行われたと公表された※51。一方で、同月24日、同グループは活動再開の声明を発表した※52-1。

なお、同事例を受けて2024年3月8日、政府のサイバーセキュリティ戦略本部は、「重要インフラのサイバーセキュリティに係る行動計画」を改定し、「重要インフラ」に「港湾」を追加した※52-2。また、コンテナターミナルシステムにおける情報セキュリティ対策の確保状況に関して、国が審査する制度も導入された※52-3。

(b)クラウドサービス事業者における被害事例

社会保険労務士（以下、社労士）向けクラウドサービス等を提供する株式会社エムケイシステム（以下、エムケイシステム社）は、2023年6月5日、障害により同社の複数サービスが停止していることを発表した※53。翌6日、障害の原因がランサムウェア被害によるものと公表した※54。

その後、7月19日まで、エムケイシステム社は継続的に調査結果を報告した。同社が報告した資料によると、今回のランサムウェア攻撃により、データセンターにあるサーバーのデータが暗号化され、約3,400ユーザーの大半に対してサービスを提供できなくなったとしている。また、外部専門機関のフォレンジック調査によってランサムウェア攻撃の侵入経路や被害を受けたサーバーは特定しているという。なお、攻撃者によって何らかのデータが窃取された可能性は完全には否定できないが、調査の結果、情報窃取及びデータの外部転送等に関する痕跡は確認されておらず、エムケイシステム社の情報がダークウェブ等に掲載されていないことを確認したとしている※55。

9月7日のユーザー向けのオンライン説明会での説明によると、原因は、攻撃者にIDとパスワードを窃取され、外部から不正アクセスを受けたものだという※56。

同社は、各サービスのバックアップデータはいずれも暗号化被害に遭っていないとしているが※57、バックアップからの全面的な復旧には時間がかかるとして※58、Amazon Web Services（AWS）上で開発中だった新バージョンへの移行を実施し、6月30日より順次サービスを再開した※59。

なお、同社が提供する社労士向けクラウドサービスにおいては、同社と契約している社労士が長期にわたりサービスの利用やデータの閲覧ができなくなることで、社労士に業務を委託していた組織の社会保険手続きや給与計算等に影響を及ぼす可能性が懸念されたという※60。

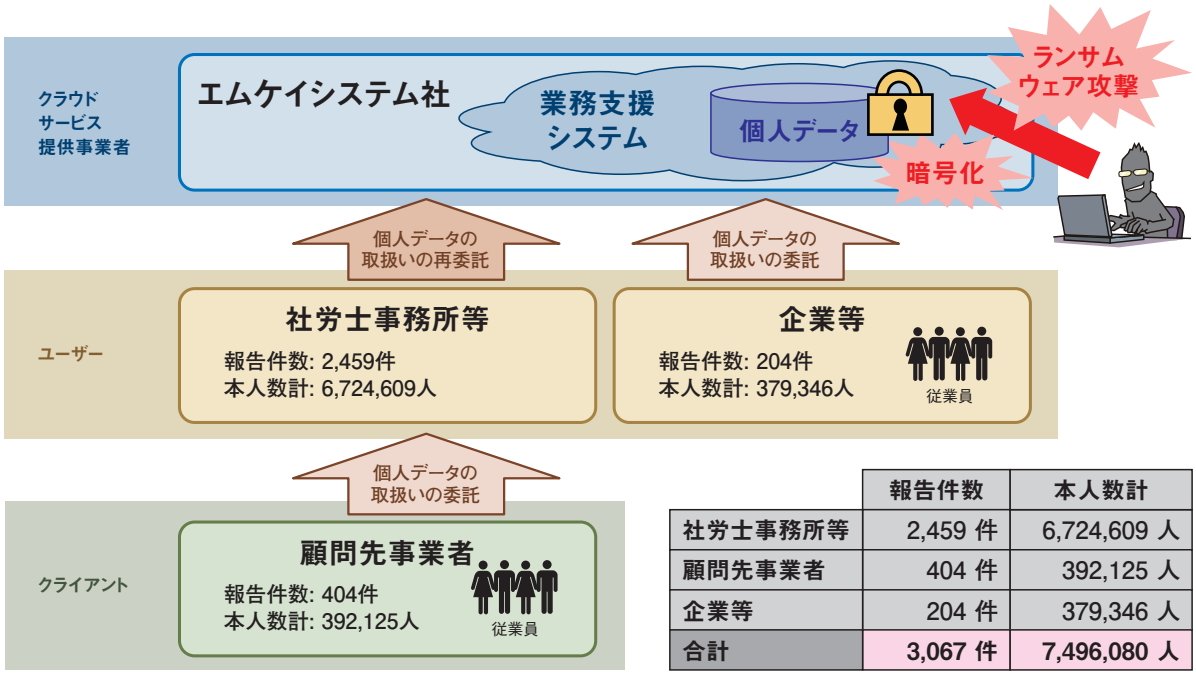
同事例について、2024年3月25日、個人情報保護委員会は、エムケイシステム社に対して個人情報の保護に関する指導を行ったことを公表した※61。公表された資料によると、管理者権限のパスワードが脆弱であり類推可能であったこと等、同社の技術的安全管理措置に不備が認められたという。なお、同事例に関連して、同委員会が同社以外から受領した漏えい等の恐れがあった報告件数は3,067件であり、対象人数は749万6,080人とのことである。その内訳は、社労士事務所等が2,459件（672万4,609人）、顧問先事業者が404件（39万2,125人）、企業等が204件（37万9,346人）であった（次ページ図1-2-2）。

同事例を受けて、同委員会は、各事業者においてクラウドサービスを利用して個人データを取り扱う場合や、個人データを取り扱う業務の委託先がクラウドサービスを利用している場合、委託元は委託先に対する監督義務があるという理解が不足していると考え、注意喚起を実施した※62。

(c)サービス提供事業者における被害事例

2023年12月18日、千葉市や伊丹市からウェアラブル端末を活用した特定保健指導の業務を委託されている株式会社Y4.com（以下、Y4.com社）は、利用する一部のサービスに対して、12月10日にノーウェアランサム攻撃が発生したことを公表した※63。その後、2024年1月22日に同社が報告した資料によると、第三者からの不正アクセスによりデータの窃取及び削除が行われており、合計1,014人の個人情報が漏えいした可能性があるという。なお、そのうちの738人は漏えいした情報に氏名が含まれないとしている※64。この事態を受けて、委託元の千葉市（対象者25人）や伊丹市（対象者20人）でも、同攻撃による被害を公表した※65。

不正アクセスの原因は、Y4.com社が過去に委託した開発会社により発行されたアクセスキー（プログラムからサービスにアクセスするための認証情報）が納品時に削除されておらず、外部に漏えいして悪用されたためとしている。Y4.com社では納品時にアカウント情報をすべ



	報告件数	本人数計
社労士事務所等	2,459 件	6,724,609 人
顧問先事業者	404 件	392,125 人
企業等	204 件	379,346 人
合計	3,067 件	7,496,080 人

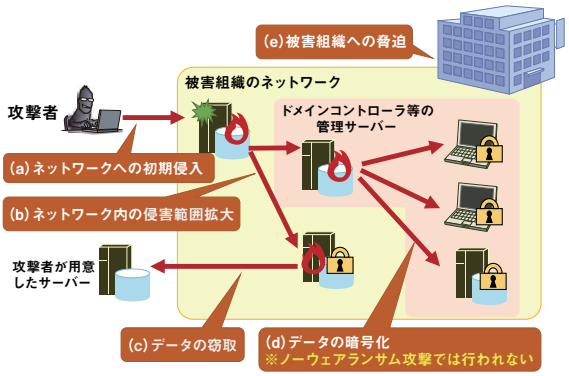
※図中の本人数計は、個人情報保護委員会に提出された漏えい等報告のうち、2024 年 3 月 8 日時点のものである（本人数不明として報告されているものを除く）。また、本人数は、社労士事務所等と顧問先事業者とで重複して報告している可能性がある。
※エムケイシステム社からの情報によると、本件システムで管理する本人数は、2023 年 6 月 5 日時点で、最大約 2,242 万人とのことである。

■図 1-2-2　事案の概要
（出典）個人情報保護委員会「株式会社エムケイシステムに対する個人情報の保護に関する法律に基づく行政上の対応について[※61]」を基に IPA が編集

て変更していたが、このアクセスキーの存在は認知していなかったという。

同社は同事例を受け、アクセスキーの管理を強化した。また、仮名加工情報と呼ばれる、他の情報と照合することで個人を識別できる情報の取り扱いルールの再整備を実施した。

なお、同社が公表した資料の中では、攻撃者名や脅迫の有無については触れられていないが、同攻撃がデータを暗号化せず身代金を要求するノーウェアランサム攻撃であることを鑑みて調査対応を行ったとしている。



■図 1-2-3　侵入型ランサムウェア攻撃の手口のイメージ

(3) 侵入型ランサムウェア攻撃の手口

ここでは、侵入型ランサムウェア攻撃の手口について説明する。なお、ノーウェアランサム攻撃については、データの暗号化は伴わないが、攻撃の手口や対策に関しては、おおむね同じである。攻撃は、次の (a) ～ (e) の五つのステップで行われる（図 1-2-3）。

(a) ネットワークへの初期侵入

侵入型ランサムウェア攻撃は、攻撃者が被害組織のネットワークへ侵入するところから始まる。攻撃者は、被害組織がインターネットへ接続している機器全般を狙い、強度の弱いパスワードや過去に漏えいした認証情報、残存している脆弱性、設定不備等を悪用してネットワークに侵入する。その中でも、VPN 製品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[※42]。また、被害組織のパソコンを乗っ取りネットワークへの侵入の足掛かりを作るために、被害組織へ遠隔操作ウイルス等を添付したメールや、遠隔操作ウイルス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り付けることもある。

(b) ネットワーク内の侵害範囲拡大

攻撃者は、被害組織のネットワークへの侵入に成功すると、ネットワーク内で侵害範囲の拡大を図る。攻撃者は、まずネットワーク構成の把握や管理者権限の奪取を行

い、機微情報等が保存されているパソコンや業務用サーバー、ドメインコントローラー等の管理サーバー、バックアップ用のサーバー等を侵害する。特に、ネットワーク内のユーザーやコンピューターを一元管理することができるドメインコントローラーが侵害されると、管理下のすべてのコンピューターに侵害範囲が拡大する恐れがある。

(c) データの窃取

データの窃取は、攻撃者が侵入型ランサムウェア攻撃で「二重の脅迫」を狙っている場合において行われる。攻撃者は遠隔操作ウイルスや正規のツール等を使用し、ネットワーク内のデータ探索・収集を行った上で、収集したデータを攻撃者のサーバーやクラウドストレージへアップロードする。

(d) データの暗号化

侵入型ランサムウェア攻撃では、被害組織のデータをランサムウェアによって暗号化し、身代金の取得を狙うとともに、事業継続に関わる重要なシステムの停止を狙っていると考えられる。バックアップデータによる復旧を妨害するため、バックアップデータも狙って暗号化する可能性がある。

なお、ノーウェアランサム攻撃では、同ステップは行われない。そのため、システムの停止が発生しないだけでなく、EDR (Endpoint Detection and Response) 等による攻撃検知がされにくくなり※45、侵害されたことが発覚しにくい。

(e) 被害組織への脅迫

攻撃者は、被害組織に対して、システムやファイルを復旧可能にすることと引き換えに身代金を要求する。また、身代金を支払わなければ窃取したデータを公開するとして脅迫を行うことがある。データの公開方法としては、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（以下、リークサイト※66）での公開やオークション形式での販売が挙げられる。攻撃者との身代金の交渉には電子メールや特定のチャットサイト等が使用される。

更に、被害組織が提供するサービスへの DDoS 攻撃や、ランサムウェア被害に遭ったことを被害組織の利害関係者へ直接連絡する等の脅迫を行う場合もある。

(4) 侵入型ランサムウェア攻撃への対策

ここでは、侵入型ランサムウェア攻撃への対策について、「(a) ネットワーク侵入への対策」「(b) 侵害範囲拡大防止のための対策」「(c) 暗号化によるシステム停止への対策」「(d) インシデント対応力の強化」の四つに分けて説明する。なお、これらの対策は自組織だけでなく、海外を含む子会社や取引先等、サプライチェーン全体で行うことが重要といえる。

(a) ネットワーク侵入への対策

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

- 攻撃対象領域 (アタックサーフェス) の最小化
  企業・組織の管理する機器が攻撃の対象となる可能性を減らすために、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、最小化することが重要である。特に、製品を初期設定のままにしていること等により、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ないかも確認いただきたい。
- 脆弱性対策
  脆弱性を悪用した侵入や侵害範囲の拡大を防ぐために、VPN 製品を含むネットワーク機器のファームウェア、パソコンやサーバーの OS、利用しているソフトウェア等を常に最新の状態に保つことが重要である。なお、脆弱性の影響を受けないバージョンにバージョンアップした状態であっても、既に攻撃者によって脆弱性が悪用され、設定情報や認証情報等が窃取されている可能性があるため、脆弱性を悪用した攻撃の IoC (Indicator of Compromise：侵害指標) 等の情報を収集し、攻撃が行われた痕跡がないか、過去のログを含め調査を怠らないようにしていただきたい。また、脆弱性が公開されてから悪用されるまでの期間が短くなっていることから、公開された脆弱性対策情報に迅速に対応できるような体制や計画を整備しておくことも重要といえる。
- アクセス制御と認証の強化
  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、特定の IP アドレスからのアクセスを許可または拒否する等、適切なアクセス制御を行うことが重要である。また、推測されにくい複雑なパスワードを使用することや、認証の試行回数に制限を設けること、多要素認証のような強固な認証方式を使用すること等により、認証を強化することも重要といえる。なお、インシデント発生時に備えて、

平時から、必要なアクセスログや認証ログ等を取得・保管することに加え、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ウイルスメール等の攻撃メールによる認証情報の流出やウイルス感染を防ぐために、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、訓練等の対策を行うことにより、メール利用者の一人ひとりが「身に覚えのないメールの添付ファイルは開かない、怪しいリンクはクリックしない」という意識を持つことも重要といえる。

(b) 侵害範囲拡大防止のための対策

攻撃手口の高度化に伴い、侵入を完全に防ぐことが難しくなっている中で、侵害された際の影響範囲を局所化することが重要である。

- ネットワーク接続点のセキュリティ強化

  組織内の複数拠点におけるネットワーク間接続や他組織とのネットワーク間接続において、セキュリティ対策が十分に実施されていないネットワークがある場合、攻撃者によって、脆弱な箇所からまずそのネットワークに侵入される。そして、ネットワーク間接続を経由して、他のネットワークに存在する自拠点の中枢が侵害される恐れがある。そのため、組織内の拠点間や他組織とのネットワーク接続点において、アクセス制限や不正通信の監視等を実施することが重要である。
- ネットワーク内の通信制御の強化

  ネットワーク接続点のセキュリティ強化に加えて、組織内のネットワークを細分化し、内部通信の可視化と制御を行うことが望ましい。このような手法は「マイクロセグメンテーション」と呼ばれる。

被害拡大防止に有効なその他のセキュリティ対策を以下に示す。

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

各項目の詳細は、「情報セキュリティ白書 2023[※67]」の「1.2.1 (4) (c) 侵害範囲拡大への対策」にて解説しているため、そちらを参照いただきたい。

(c) 暗号化によるシステム停止への対策

侵入型ランサムウェア攻撃によってデータが暗号化され、システムが停止した場合に備えて、システムの再構築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

  システム再構築に備え、バックアップを取得する。それに加えて、バックアップからの復旧が可能なことを確認しておくことが重要である。バックアップサーバーがシステムに接続されている場合、バックアップも含めて一斉に暗号化される可能性がある。このため、複数のバックアップ方式を採用しておくことも重要である。バックアップのうち一つは、テープデバイス等に保存してネットワークから隔離された環境に移す等、攻撃者から手の届かないオフライン環境に配置することが望ましい。このほか、一度保存した後は上書きを禁止する仕組み（WORM（Write Once Read Many）機能）でデータを保護することや、組織のネットワークから切り離したクラウド上に保存する方法も有効である。その他の注意事項として、クラウドサービスを利用する場合には、ユーザーデータのバックアップ機能の有無や責任分界点を確認していただきたい。多くの場合、ユーザーデータの管理責任は利用者側にあり、ランサムウェア攻撃等への対策を目的としたバックアップの実施及びバックアップデータの管理は、クラウドサービスの利用者自らが行う必要がある。
- ランサムウェア攻撃を想定した BCP の策定

  自然災害の発生を想定した事業継続計画（BCP：Business Continuity Plan）を策定している企業・組織であっても、侵入型ランサムウェア攻撃等のサイバー攻撃を受けることを想定していない場合がある。BCP の策定時には、地震等の自然災害について考慮することに加え、侵入型ランサムウェア攻撃についても必ず考慮していただきたい。

(d) インシデント対応力の強化

実際に被害に遭った場合に備えて、迅速で適切なインシデント対応を行う能力や応用力を高めるため、経営層を含めたインシデント対応の訓練を定期的に実施することが望ましい。

データ暗号化と身代金要求への対応については JPCERT/CC が侵入型ランサムウェア攻撃を受けた際の FAQ[※66] を公開しているため、こちらも参照いただき

たい。

侵入型ランサムウェア攻撃によるインシデントでは、業務の停止や顧客・取引先の情報漏えい等が発生し、自組織内に閉じたインシデントで終わらない傾向がある。そのため、日頃から、経営層を含む顧客や取引先、システムの運用・保守の委託先等との素早い連絡・調整を行うための体制作りが必要である。

1.2.2 標的型攻撃

標的型攻撃とは、ある特定の企業・組織や業界等を狙って行われるサイバー攻撃の一種である。フィッシングメールやウイルスメールを不特定多数の相手に無差別に送り付ける攻撃とは異なり、標的型攻撃は、標的とする特定の企業・組織（以下、標的組織）や業界が持つ機密情報の窃取等明確な目的をもって行われる。

(1) 標的型攻撃の手口

標的型攻撃における侵入の手口として、これまで標的型攻撃メールが用いられていたが、ネットワーク貫通型攻撃と呼ばれる手口が確認されるようになってきている。以下に、それぞれの手口について述べる。

(a) 標的型攻撃メールを用いた攻撃の手口

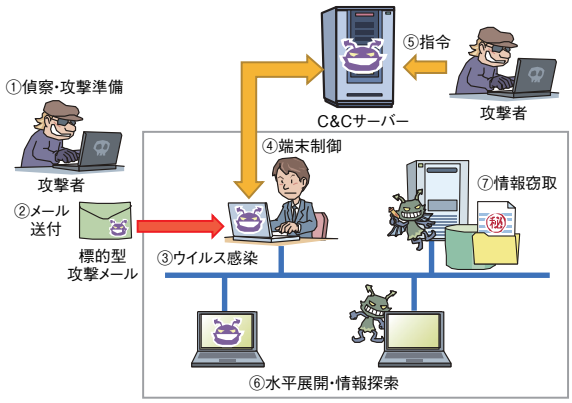
標的型攻撃メールとは、ウイルスを仕込んだファイルが添付されていたり、ウイルスをダウンロードさせるURLリンクが記載されていたりするメールが標的組織の役職員宛てに送り付けられてくるものである。以前から用いられている手口であり、継続して観測されている。標的型攻撃メールを用いた攻撃の流れを以下に示す（図1-2-4）。

①偵察・攻撃準備：標的組織を攻撃するための情報を収集、攻撃手法を選定する。
②メール送付：標的組織宛てにメールを送付する。
③ウイルス感染：メールの添付ファイルやURLリンクを開くことでウイルスがインストールされる。
④端末制御：パソコンとC&C（Command and Control）サーバー※68で通信が行われる。
⑤指令：C&Cサーバーを経由し、遠隔操作が可能になる。
⑥水平展開・情報探索：侵害範囲拡大や情報探索を行う。
⑦情報窃取：目的の情報等を窃取する。

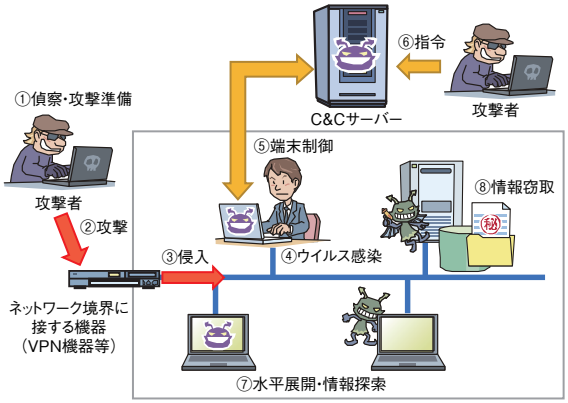
(b) ネットワーク貫通型攻撃の手口

標的組織のネットワークに侵入する手口として、VPN製品や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のJ-CRAT（Cyber Rescue and Advice Team against targeted attack of Japan：サイバーレスキュー隊）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」と呼んでいる※69。2023年には、この手口による攻撃の被害が複数確認されたことから、IPAにおいても注意喚起を行っている※70。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、侵入後のウイルス感染や端末制御等、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を以下に示す（図1-2-5）。

①偵察・攻撃準備：標的組織を攻撃するための情報を収集、攻撃手法を選定する。
②攻撃：VPN機器等の脆弱性を悪用し不正アクセスを行う。
③侵入：標的組織のネットワーク内に侵入し内部偵察を行う。



■図1-2-4　標的型攻撃メールを用いた攻撃の流れ



■図1-2-5　ネットワーク貫通型攻撃の流れ

④ウイルス感染：パソコン等に侵入しウイルスをインストールする。
⑤端末制御:パソコンとC&Cサーバーで通信が行われる。
⑥指令:C&Cサーバーを経由し、遠隔操作が可能になる。
⑦水平展開・情報探索：侵害範囲拡大や情報探索を行う。
⑧情報窃取：目的の情報等を窃取する。

(2) 標的型攻撃の事例

標的型攻撃のうち、国家の支援を受けた攻撃者グループによる、機密情報（先端技術や国家安全保障に関わる情報等）の窃取やシステムの破壊等の妨害工作を目的とした、持続的かつ高度なサイバー攻撃は「APT（Advanced Persistent Threat）攻撃」とも呼ばれる。APT攻撃の特徴として、標的別に改変・開発したウイルスの使用※71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。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、2023年度に確認された、APT攻撃であることが疑われる標的型攻撃の事例を紹介する。

(a) 標的型攻撃メールを用いた攻撃の事例

伊藤忠サイバー＆インテリジェンス株式会社は、「Tropic Trooper」（別名、Pirate Panda、KeyBoy）と呼ばれる攻撃者グループによる標的型攻撃メールを用いた攻撃があったとしている※72。

この攻撃では、中国企業で働く従業員のための公的制度に関する内容を装ったメールを標的組織へ送付し、添付ファイルを開くよう促していた。添付ファイルはZIP形式で圧縮されており、展開するとExcelファイルに偽装したショートカットファイルが一つだけ表示されるが、実際には隠しフォルダも生成される。この隠しフォルダ内には、ウイルスに感染させるための複数のファイルが格納されている。また、この隠しフォルダは、ゴミ箱のフォルダ名に似せた名称になっており、隠しフォルダが表示される設定になっていても、不審なフォルダではないと、誤認させることを狙っていると考えられる。こうした細工で、ユーザーにウイルスと気付かせずにファイルを実行するよう仕向けていると見られる。Excelファイルに偽装されたショートカットファイルを実行すると、McAfee, LLCの正規プログラムと思われる実行ファイルを呼び出す。この実行ファイルには脆弱性が存在しており、実行するとDLL Side-Loading※73と呼ばれる手法により、攻撃者が用意した悪意あるDLLファイルが読み込まれる。最終的に正規のセキュリティツールであるCobalt Strike Beacon※74が実行されるようになっていた。攻撃者はCobalt Strike Beaconを悪用し、C&Cサーバーと通信を行うことで端末を遠隔操作し、侵害範囲の拡大、情報探索や情報窃取を行おうとしたと考えられる。

(b) ネットワーク貫通型攻撃の事例

IPAは、日本の組織を標的とした標的型攻撃として、VPN製品のArray Networks Array AGシリーズ（以下、Array AG）、FortiOS/FortiProxy、オンラインストレージアプリケーションのProselfの脆弱性を狙ったネットワーク貫通型攻撃について、注意喚起を行っている※70。

JPCERT/CCが公表※75した情報によると、2022年5月以降にArray AGの「リモートコード実行の脆弱性（CVE-2023-28461）」「コマンドインジェクションの脆弱性（CVE-2022-42897）」を悪用した攻撃が観測されている。また、2023年3月以降にFortiOS/FortiProxyの「SSL-VPN事前認証におけるヒープベースのバッファオーバーフローの脆弱性（CVE-2023-27997）」を悪用した攻撃が観測されている。更に、2023年7月以降には、Proselfの「管理者権限での認証バイパス（CVE-2023-39415）の脆弱性」及び「OSコマンドインジェクション（CVE-2023-39416）の脆弱性」、2023年8月以降に「XML外部実体参照（XXE）（CVE-2023-45727）に関する脆弱性」を悪用した攻撃が観測されている。

2023年10月には、実際に攻撃を受けた組織が被害を公表している※76。これによると、アカウントのリストやパスワードハッシュが窃取され、その情報を利用して不正アクセスが行われ、一部のファイルへアクセスされたとしている。攻撃を受けた国内組織では、サーバー内に保管していた個人情報を含むデータの一部が外部に漏えいした可能性があるとしている。

これら一連の攻撃に関連して、トレンドマイクロ株式会社（以下、トレンドマイクロ社）では「Earth Kasha」（別名、MirrorFace）と呼ばれる攻撃者グループの活動について報告している。この攻撃者グループは、以前は標的型攻撃メールを用いた攻撃を行っていたが、2023年5月以降、Array AG、FortiOS/FortiProxy、Proselfの脆弱性を悪用した新たな攻撃キャンペーンを行うようになったという※77。同攻撃キャンペーンでは、日本の政府機関やハイテク関連団体等を対象とした情報窃取を目的に活動しているとされる。

インターネットとの境界に設置されるネットワーク機器に

対する攻撃として、Cisco Systems, Inc. 製ルーターのファームウェアを不正なファームウェアに入れ替えることで、標的組織ネットワークへの長期的な侵入を維持しようとする攻撃が確認されている。この攻撃は中国を背景とする「BlackTech」と呼ばれる攻撃者グループによるものとされ、不正に入手した管理者の認証情報を用いて、管理者レベルの設定等を行っていたという※78。2023年9月には、警察庁及び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）が、米国国家安全保障局（NSA：National Security Agency）、FBI及びCISAと合同で注意喚起を行っている※79。

このほかにもメールゲートウェイ製品が対象となったケースもあり、Mandiant, Inc. によると、Barracuda Networks, Inc. のBarracuda ESG（Barracuda Email Security Gateway）のゼロデイ脆弱性（CVE-2023-2868）を悪用した攻撃が、2022年10月から観測されていると、2023年5月に発表された。これには中国からの支援が疑われる「UNC4841」と呼ばれる攻撃者グループが関わっているとされている※80。UNC4841は、Barracuda ESGがメールの添付ファイルの中身を検査しウイルスを検出する機能における、コマンドインジェクションの脆弱性を悪用することで、同製品内にバックドアを設置したものと推定される。その後、標的組織内に侵入し、情報窃取や侵害範囲拡大等の活動を行ったと見られる。この攻撃では、日本を含む世界中の政府機関やハイテク関連を始め、多数の業種が標的になっているという※81。

海外で発生したネットワーク貫通型攻撃として、Microsoft社は、中国で活動する「Storm-0558」と呼ばれる攻撃者グループによる、Outlook Web Access及びOutlook.comへの不正アクセスについて公表した※82。この攻撃により、米国の政府機関等、複数組織が被害を受けたという。

(c) その他の特徴的な標的型攻撃の事例

2023年度に確認されているその他の特徴的な事例として、USBメモリーを用いた攻撃が観測されている。「Mustang Panda」（別名、TEMP.HEX）と呼ばれる攻撃者グループによる、感染したUSB機器を経由してウイルスを拡散する標的型攻撃が、日本を含む東アジアや欧州、北米等の複数の業界で観測されているという※83。報告された事例では、ヨーロッパの医療機関において感染したUSBメモリーを通じて「WispRider」と呼ばれるウイルスがシステムに侵入し、他のコンピューターに感染が拡大する被害を受けたとしている。きっかけは医療カンファレンスに参加した医療従事者がUSBメモリーを他者と共有した際に、その中にウイルスに感染したコンピューターがあったことから、USBメモリーにウイルスが感染したとされている。

(3) 標的型攻撃への対策

「1.2.2 (1) 標的型攻撃の手口」に記載したとおり、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、攻撃手口の変化により対策が有効でなくなる場合があるので、特定の対策のみに頼るのではなく、システム全体で多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、対策の選別をした上で実施することが重要である。以下に、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用いる、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。しかし、すべての標的型攻撃メールが見抜けない程完成度の高いものではない。役職員自身も日頃から不審メールに対する意識を高め、不用意に開封や返信をしないこと、不審なメールだと少しでも疑った場合は組織のシステム管理者に連絡することが求められる。そのため、組織として役職員に標的型攻撃メール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のに有効である。
- SNSを悪用した手口の周知

  攻撃者グループが、SNSで標的組織の役職員への接触を図り、悪意あるURLリンクやファイルを送り、それを開くように誘導することで初期潜入経路を開拓する手口がある。このような手口があることや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が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・啓発活動の実施等を行う組織体制のことを 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。

- 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はなく、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、事業継続計画に情報セキュリティの観点を組み込むことは重要である。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、組織全体の対応力・回復力(サイバーレジリエンス)の強化に有効である。

- 攻撃の手口や対策の把握と情報共有

  標的型攻撃が発生すると、セキュリティベンダーやマスコミ、あるいは被害組織自体から、攻撃手口や対策に関する情報が公表されることがある。また、業界内でのサイバーセキュリティに関する情報共有体制を通じて、他組織で発生した標的型攻撃の情報を得られる場合もある。これらの情報を CSIRT が継続して収集し、対策に活用していくことが重要である。例えば、攻撃者グループの侵入手口が特定機器の脆弱性を悪用したものであれば、自組織のシステムに該当する機器がないか確認し、該当するものがあれば、脆弱性の有無を確認し必要に応じて修正プログラムを適用する。標的型攻撃メールの情報が得られた場合は、社内にその特徴を周知し、メールのフィルタリング設定を行うことで、被害防止につなげることができる。もし、自組織が標的型攻撃を受けた場合には、前述の情報共有体制や IPA 等の組織と連携し、攻撃の手口や IoC 等の情報を積極的に共有していただきたい。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※84。

- 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、海外拠点においても国内拠点と同様に、セキュリティポリシーを策定、周知し、またセキュリティリスクの可視化、改善や対策を行うことが望ましい。これらの対策を実施する際は、海外拠点所在地の法制度や労働慣行の違い等も把握して、国内と同一の対策が取れない場合は代替策を考える必要がある。取引先等のサプライチェーンのセキュリティ対策強化の取り組み例としては、取引先の選定時にセキュリティ関連の認証取得状況等のセキュリティへの取り組みを考慮する、取引先とセキュリティに関して担うべき役割と責任範囲を明確化する、セキュリティ対策の共同実施や導入の支援を実施する、第三者によるセキュリティ対策の評価検証を実施する、セキュリティに関する情報共有を行うこと等が挙げられる。「サイバーセキュリティ経営ガイドライン※85」にも対策例が記載されているので参考にしていただきたい。

- 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、ネットワーク境界装置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ような体制作りが重要である。IT 資産管理システム等を活用することで、自組織のサーバーや端末等に報告されている脆弱性がないかを確認し、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、企業・組織のネットワークとインターネットとの境界に設置されるネットワーク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、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。

(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。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、ウイルスの検査はもちろん、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ウイルス検査やサンドボックスのサービスの一部には、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、ウイルス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、悪用されることの多いPowerShellやJavaScript等のスクリプトファイル(拡張子が.ps1や.js等のファイル)のような、業務で使用しないであろうファイルの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せず、職場外での勤務を可能にする勤務形態や、BYOD(Bring Your Own Device:私物端末の業務利用)により、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、すべてのウイルス等に対して万能ではないものの、ファイルレスマルウェア※86や未知のウイルス等の検知・対策にも有効である可能性がある。また、クラウドの利用等によって、業務情報を自社システム外に保管するケースも増えている。そこでデータの持ち出しや流出の可能性を考慮したセキュリティ対策としてファイルの暗号化やDLP(Data Loss Prevention)等の対策の導入を検討する必要がある。
- 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※87。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、ログの保管期間についても定期的に見直しを行うことが望ましい。
- Attack Surface Management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※88。Attack Surface(アタックサーフェス)とは、ネットワーク機器やWebサービス等、外部(インターネット)との境界にあり、組織の外部からアクセス可能な資産を指し、これらは外部からの攻撃を受ける可能性がある。サイバー攻撃の初期段階では、公開情報やインターネットからアクセス可能な資産から得られる情報により偵察が行われ、脆弱な部分を狙われて侵入されることがある。こうした攻撃から自組織の資産を守るため、Attack Surfaceを把握・管理(Management)する手法をASMと呼ぶ。セキュリティベンダーが提供するASMツール等を用いることで、ツールにより資産を一元管理し、収集した脆弱性情報と資産を突き合わせて、リスクの評価・可

視化等ができる。これにより、脆弱性が早期発見でき、迅速かつ適切に対応を行うことで、攻撃のリスクを減らし、自組織を標的型攻撃から守ることにつながる。

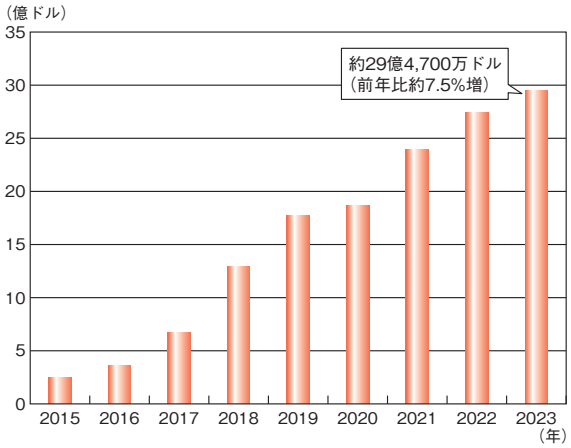
1.2.3 ビジネスメール詐欺（BEC）

ビジネスメール詐欺（BEC：Business Email Compromise）は、巧妙な騙しの手口を駆使した偽のメールを企業・組織に送り付け、役職員を騙して送金取引に関わる資金を詐取する等の金銭被害をもたらすサイバー攻撃の一種である。偽のメールを送るための前段階として、企業の役職員や取引先のメールアカウント情報を狙うケースもあり、フィッシング攻撃や情報を窃取するウイルスを使用することもある。

本項では、2023 年度に公表されたビジネスメール詐欺の被害状況、事例を紹介し、その巧妙な手口と対策について解説する。

(1) ビジネスメール詐欺の被害状況

FBI のインターネット犯罪苦情センター（IC3：Internet Crime Complaint Center）が 2024 年 3 月に公開した年次報告書※89 によると、2023 年に IC3 に報告されたビジネスメール詐欺の被害総額は、前年比約 7.5% 増の約 29 億 4,700 万ドルとなっている。IC3 が公開した 2015 年から 2023 年までの年次被害総額の推移を図 1-2-6 に示す。



■図 1-2-6　ビジネスメール詐欺の被害総額推移（2015～2023 年）
（出典）IC3 年次報告書※89 を基に IPA が作成

この図から、被害総額が年々継続して増加しており、ビジネスメール詐欺の脅威がより深刻なものとなっていることが見て取れる。

なお、当該報告書によると、被害件数は 2022 年が 21,832 件、2023 年が 21,489 件とわずかながら減少しており、ここから 1 件あたりの被害金額が増加傾向にあることも推測される。

(2) ビジネスメール詐欺検挙の事例

脅威がより深刻となる一方で、世界の法執行機関がビジネスメール詐欺の容疑者を検挙する事例も前年度に引き続き多数公開された。国際刑事警察機構（ICPO：International Criminal Police Organization、INTERPOL とも呼ばれる）は、2023 年 7 月から 12 月にかけて「HAECHI IV」と呼ぶ国際的な取り締りを主導し、34 ヵ国が参加した。その成果として、ビジネスメール詐欺を含むサイバー犯罪に関わっていた約 3,500 人を逮捕し、悪用されていた 82,112 件の銀行口座や仮想通貨口座を凍結させ、約 3 億ドルの資産を押収したという※90。

また、地域の法執行機関と民間企業の協力によって容疑者の逮捕につながった事例も公開されている。一例としては、INTERPOL とアフリカ警察協力機構（AFRIPOL：African Union Mechanism for Police Cooperation）が、パートナーである民間企業数社の協力を得て、アフリカ 25 ヵ国で共同の捜査を行い、ビジネスメール詐欺の容疑者の逮捕に至った事例が挙げられる※91。

(3) 2023 年度に報道された事例

2023 年度においても国内外で金銭被害に遭った事例の報道が確認されている。

国内で発生した事例では、イベント事業を展開する株式会社 NHK プロモーションが、虚偽のメールによる送金指示により詐欺被害を受けたという事例※92 や、医療製品事業を展開する株式会社スリー・ディー・マトリックスが、取引先を装った虚偽のメールによる送金指示により約 2 億円の被害を受けた事例※93 が挙げられる。

国外で発生した事例では、米国のフロリダ州フォートローダーデール市が、建設業者を装った攻撃者による虚偽のメール及び巧妙な請求書の偽造によって約 120 万ドルを送金させられたものの、市警察が資金を追跡し全額を回収した事例※94 が挙げられる。また、手口としてディープフェイクが悪用された事例の報道も複数あり、ビデオ会議に参加していた数人すべてがディープフェイクにより生成されたものであったという事例※95 の報道もある。

(4) IPA が情報提供を受けた事例

IPA では、2022 年 9 月から Web サイト上で「ビジネ

スメール詐欺（BEC）対策特設ページ※96」（以下、特設ページ）と題して、情報提供を受けた事例や対策等を紹介しているほか、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）の運用状況レポートでも事例を公開している（J-CSIPの活動については「2.1.3 (5) J-CSIP（サイバー情報共有イニシアティブ）」参照）。

IPAが情報提供を受け、2023年度に公開したビジネスメール詐欺事例3件の概要を表1-2-2に示す。

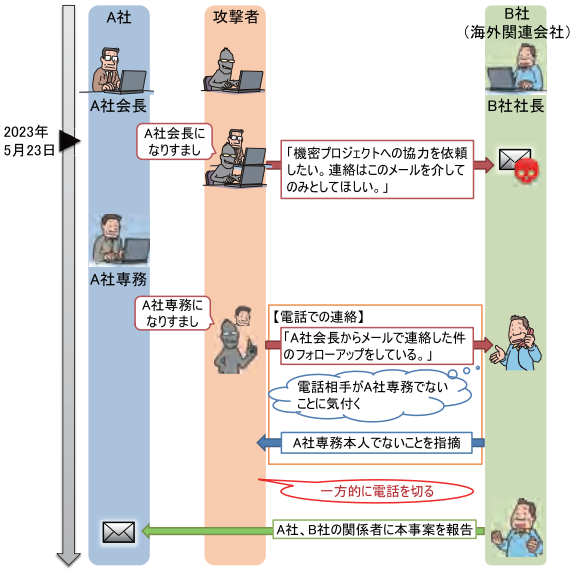
IPAではビジネスメール詐欺を「経営者等へのなりすまし」と「取引先との請求書の偽装」の二つのパターン※99に分類している。ここでは各パターンで使用される代表的な手口について、表1-2-2の項番1及び2の事例を用いて、「(a) 海外関連企業を狙った電話を併用した攻撃事例」「(b) 偽造文書を使い海外取引先を狙った攻撃事例」で紹介する。

また、「経営者等へのなりすまし」分類の代表的なビジネスメール詐欺である「CEO（Chief Executive Officer：最高経営責任者）を詐称するビジネスメール詐欺」（以下、CEO詐欺）について、継続して情報提供を受けたため、概要を「(c) CEOを詐称する一連の攻撃の特徴」で紹介する。

(a) 海外関連企業を狙った電話を併用した攻撃事例（表1-2-2の項番1）

同事例は、2023年5月、J-CSIPの参加組織（A社：請求側）の海外関連企業（B社：支払側）の社長に対し、A社の会長及び専務になりすました攻撃者から、偽のメールと発信者電話番号を偽装した電話が着信したものである。この電話ではA社専務の声が模倣されていた。昨今では、ディープフェイクで生成された音声による電話がビジネスメール詐欺に用いられたとの報道があり、同事例でもディープフェイクが使用されていた可能性もある。なお、同事例では、攻撃者からの電話を受けたB社社長がなりすましに気付いたことで、金銭的な被害は発生しなかった。

攻撃に関連したメール及び電話のやり取りを図1-2-7に示す。



■図1-2-7　攻撃者とのやり取り
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2023年4月～6月］」

この攻撃は、前述のビジネスメール詐欺の二つのパターンのうち、「経営者等へのなりすまし」に該当する。同事例では詐欺の過程で次の手口が使われた。

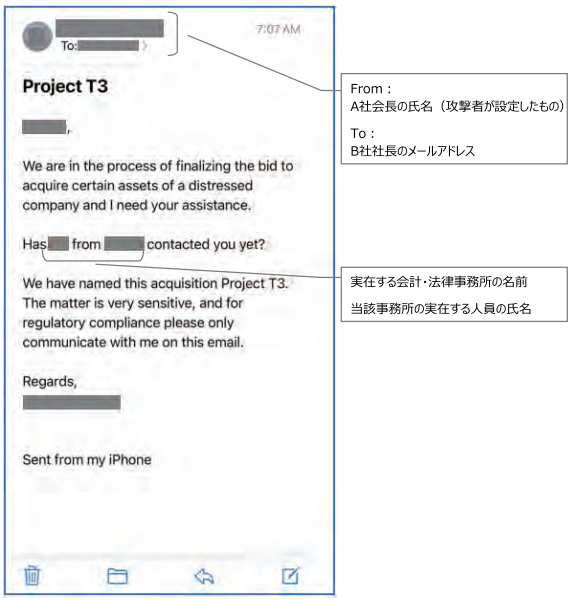
(ア) 実在する経営者をかたるメール

同事例は、A社の会長を装いB社の社長に対して機密プロジェクトへの協力を依頼するもので、メール本文には、実在する会計・法律事務所の実在する人員の

項番	事例概要	被害の有無	備考
1	2023年5月、国内企業（請求側）と海外グループ企業（支払側）の間で、請求側の国内企業の会長及び専務になりすました攻撃者から、偽のメールと電話が発信されて海外グループ企業の社長に着信したが、詐欺であると気付き、金銭的な被害は発生しなかった。	なし	「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2023年4月～6月］※97」に記載
2	2023年5月、国内企業（請求側）と海外企業（支払側）との取り引きにおいて、請求側の国内企業の担当者になりすました攻撃者から正規のメールを流用した偽のメールが発信されて海外企業の経理担当者に着信したが、経理担当者が不審に思い、信頼できる別の経路で事実確認を行い、金銭的な被害は発生しなかった。	なし	「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2023年4月～6月］」に記載
3	2022年8月、国内企業（請求側）と海外グループ企業（支払側）の間で、請求側の国内企業の社長になりすました攻撃者から支払い要求をするメールが発信されて海外グループ企業の役員に着信したが、詐欺であると気付き、金銭的な被害は発生しなかった。	なし	「ビジネスメール詐欺（BEC）の詳細事例6※98」に記載

■表1-2-2　IPAが情報提供を受け2023年度に公開したビジネスメール詐欺事例の概要

氏名が挙げられていた。攻撃者が送付したメールを図1-2-8に示す。



■図 1-2-8　攻撃者が送付したメール
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2023 年 4 月～ 6 月］」

（イ）正規のメールアドレスに似せたメールアドレス

同事例では、攻撃者がメールの差出人を A 社会長であるかのように偽装するため、差出人（From）に表示される表示名（スクリーンネーム）には A 社会長の氏名（英語表記）を、メールアドレスには A 社会長のメールアドレスに似た、実在しないメールアドレスを設定していた。このメールアドレスは、ドメイン部を A 社で使用している正規のドメインに偽装しており、@ より前のローカル部は A 社会長の氏名を含むものであった。攻撃者が設定したメールアドレスの偽装パターンを図 1-2-9 に示す。

■なりすまされた人物の名前を「山田 太郎（Yamada Taro）」さんとした場合の例

本物のメールアドレス表示：Taro Yamada < t.yamada @ [A社の正規ドメイン] >
偽のメールアドレス表示　：Taro Yamada < **taro**_yamada @ [A社の正規ドメイン] >
→ 氏名からローカル部への変換規則が実際のA社のものと異なる

■図 1-2-9　攻撃者によるメールアドレスの偽装パターン
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2023 年 4 月～ 6 月］」

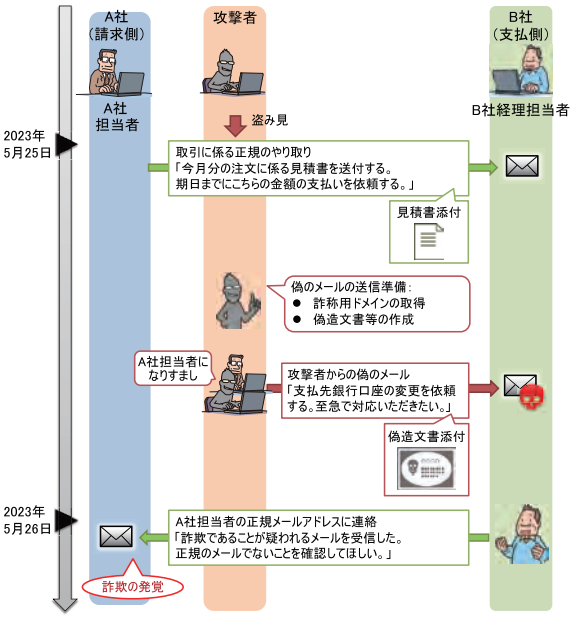
（ウ）発信者電話番号を偽装した電話

同事例では、A 社会長を詐称したメールを受信した当日中に、A 社専務になりすました攻撃者から、「A 社会長からメールで連絡した件のフォローアップをしている」と称した電話が B 社社長に着信した。発信者電話番号は A 社の代表番号に偽装されていたという。また、この電話では、攻撃者は A 社専務の声を模倣していたとのことであった。こうした詐欺に、ディープフェイクで生成した音声が利用されているとの情報※100もあるため、発信者電話番号や声色のみで判断しないよう注意が必要である。

（b）偽造文書を使い海外取引先を狙った攻撃事例（表 1-2-2 の項番 2）

同事例は、2023 年 5 月、J-CSIP の参加組織（A 社：請求側）が、海外取引先企業（B 社：支払側）との取り引きを行っている中、A 社の担当者になりすました攻撃者から B 社経理担当者に、偽の口座への振込先の変更を要求するメールが送られたものである。B 社経理担当者が連絡内容を不審に思い A 社担当者に連絡を行ったため、金銭的な被害は発生しなかった。

攻撃に関係したメールのやり取りを図 1-2-10 に示す。



■図 1-2-10　攻撃者とのやり取り
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2023 年 4 月～ 6 月］」

この攻撃は、前述のビジネスメール詐欺の二つのパターンのうち、「取引先との請求書の偽装」に該当する。

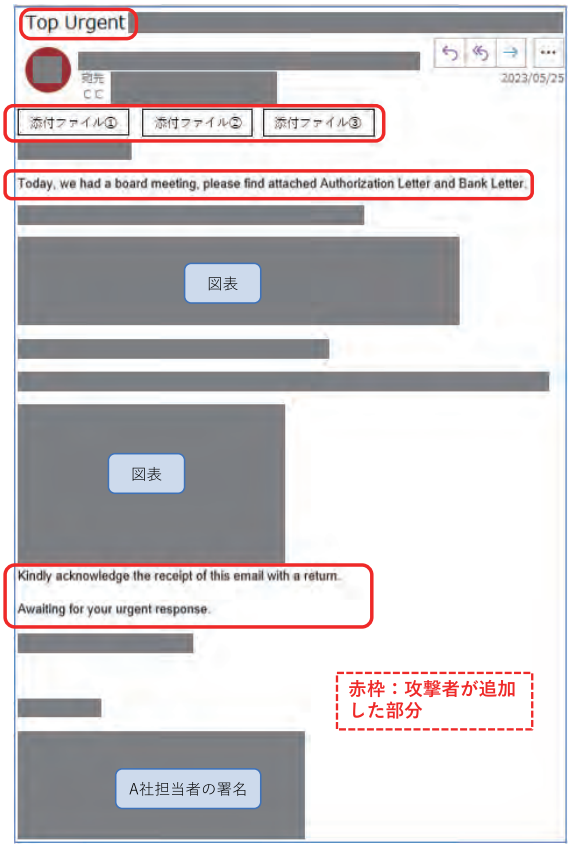
同事例では、A 社担当者から送信されたメールが攻撃者により不正に盗み見られ、その情報を悪用して偽メールの送信が行われたと推測される。詐欺の過程では次の手口が使われた。

（ア）正規のやり取りへ介入するメール

A 社と B 社の間で取り引きに関するメールのやり取りを

している中で、A 社担当者になりすました攻撃者から、支払い先の銀行口座の変更を依頼する偽のメールが B 社経理担当者へ送られた。このメールには、過去にやり取りされた正規のメールの内容が流用されており、攻撃者が何らかの方法で正規のメールを盗み見ていたことが推測される。

同事例で攻撃者から送られたメールを図 1-2-11 に示す。前述のとおり、正規のメールを流用しており、図内の赤枠部分のみを追加したメールとなっていた。



■図 1-2-11　攻撃者が送付したメール
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2023 年 4 月～ 6 月］」

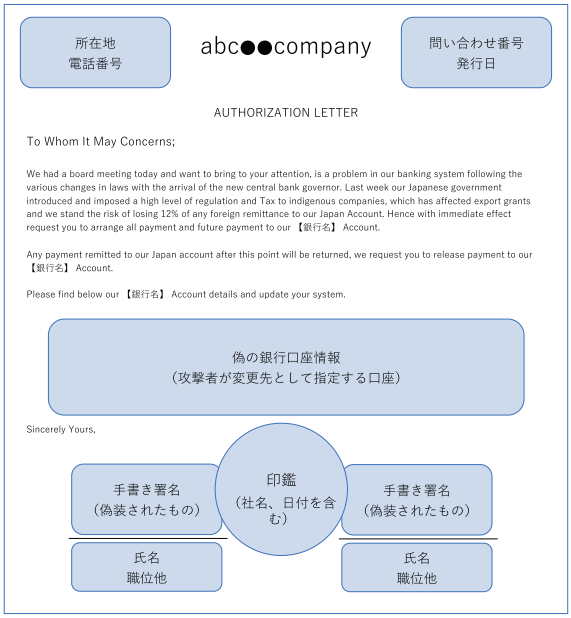
メールを受信した B 社経理担当者が不審に思い、A 社担当者に連絡したところ、詐欺であることが発覚した。

（イ）偽造文書をメールに添付

同事例で送信された偽メールには、3 点のファイル（2 点の PDF ファイルと 1 点の ZIP ファイル）が添付されており、2 点の PDF ファイルは攻撃者が偽造したファイルであった。添付ファイルの内容を以下に示す。

- PDF ファイル 1：A 社の正規の文書を模倣したと推測される、振込先口座の変更を依頼する偽造された文書ファイル
- PDF ファイル 2：A 社の依頼を元に変更先口座の銀行が発行したように見せかけた、A 社の口座が開設したことの証明書類を装った文書ファイル
- ZIP ファイル：ZIP ファイルの拡張子を「zip」から一文字違いに変更したファイル。メールシステムの制限を回避するための A 社の習慣に沿うメールに見せかけて、B 社経理担当者に正規のメールであると誤認させるために添付されたと推測される

攻撃者が作成した文書ファイルは、A 社担当者が正規のメールを送信した 4 ～ 5 時間後に作成されたと推測される。PDF ファイル 1 のイメージを、図 1-2-12 に示す。

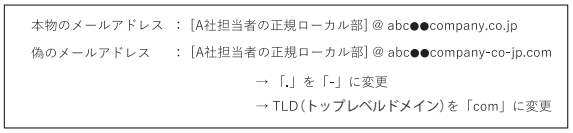


■図 1-2-12　攻撃者が作成した PDF ファイル 1 のイメージ
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2023 年 4 月～ 6 月］」

（ウ）正規ドメインと類似した詐称用ドメインの利用

同事例の攻撃メールでは、差出人（From）及び同報先（CC）のメールアドレスには、A 社のメールアドレスに似せた偽のメールアドレスが使用されていた。攻撃者が同報先にも偽のメールアドレスを設定していたのは、A 社関係者が同報でメールを確認できる状況にあると錯覚させることや、実際には A 社関係者にメールが届かないようにすることで詐欺の発覚を避けることが目的であったと推測される。攻撃者が設定したメールアドレスの偽装パターンを図 1-2-13（次ページ）に示す。

偽のメールアドレスのローカル部は本物のメールアドレスと同一であり、ドメイン部には A 社の正規ドメインに似せた詐称用ドメインが使用されていた。



■図 1-2-13　攻撃者によるメールアドレスの偽装パターン
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2023 年 4 月～ 6 月］」を基に編集

同事例の詐称用ドメインは、偽のメールに流用された正規メールの送信から 5 時間後、攻撃者が偽造文書を作成したと推測される時刻とほぼ同時刻に取得されていた。

（c）CEO を詐称する一連の攻撃の特徴

2023 年においても、CEO 詐欺について継続して情報提供があった。更に IPA で J-CSIP 外の情報を含め独自に調査を行ったところ、複数の類似するメール検体を入手した。

ここでは、攻撃メールの特徴から同一の攻撃者による攻撃と推測される二つの CEO 詐欺について説明する。いずれも企業の極秘買収をテーマとして CEO や会長等の役員をかたり、偽の弁護士とやり取りさせることで多額の金銭を詐取しようとするものである。また、メールに加えて電話や WhatsApp 等を併用しようとする手口を 2020 年 4 月以降、継続して観測している。

（ア）複数組織に行われた CEO を詐称する一連の攻撃

IPA では「複数組織へ行われた CEO を詐称する一連の攻撃」について、2023 年に 9 件（2022 年は 11 件）、2022 年以前も含めると合計約 260 件のメール情報を入手した。同攻撃は、2019 年 7 月以降継続して観測しており※101、中には 1 億円程度の大きな金額を要求するメールも確認している。メールの件名や内容は時期によって変化が見られるが、メールのヘッダー情報に類似する点があり、一連の攻撃は同一の攻撃者によるものと IPA では推測している（表 1-2-2（p.29）の項番 1 も同攻撃の一つであると推測している）。また、同攻撃メールについては、米国のセキュリティベンダーが公開したレポート※102 と同様の手口であることを確認している。

（イ）「日本語化」された CEO 詐欺の攻撃

IPA では「『日本語化』された CEO 詐欺の攻撃」について、2023 年に 82 件（2022 年は 27 件）、2022 年以前も含めると合計約 190 件のメール情報を入手した。同攻撃は、2019 年 11 月以降継続して観測しており、中には数千万円から 1 億円程度を送金するよう要求するメールも確認している。メールの件名や内容は一部に変化が見られるが、ほぼ同じ内容のメールであり、メールのヘッダー情報や、「SendGrid」「SMTP2GO」「Sendinblue（現、Brevo）」「Fastmail」「Mailgun」「Mailhostbox」というメールサービスを使用する場合がある等、類似する点があり、一連の攻撃は同一の攻撃者によるものと推測している（表 1-2-2（p.29）の項番 3 も同攻撃の一つであると推測している）。

これら二つの CEO 詐欺は、特定の組織や業種を狙うものではなく、多くの業種に対して試みられたことが確認されている。このため、業種に関わらず、今後も継続して国内外の組織に対して多額の金銭を詐取しようとする攻撃が行われる可能性があり、注意が必要である。

（5）ビジネスメール詐欺への対策

攻撃者は被害者から金銭を詐取するために、手口を多様に組み合わせて巧妙に攻撃を仕掛ける場合があることや、時流に沿った口実で相手を騙そうとする等、手口を新しくしながら攻撃を行っていることを認識しておく必要がある。日頃からビジネスメール詐欺への意識を高め、組織内の送金チェック体制や監視体制、被害に遭ったときの迅速な対応体制を整えておくことが重要である。

また、JPCERT/CC や株式会社マクニカ、PwC の報告書※103 等に加え、IPA の特設ページにも対策や被害に遭ってしまった際の対応について公開しているため、そちらも活用いただきたい。

今後、AI 等を悪用し手口は更に巧妙になることが想定されるものの、ビジネスメール詐欺への対策は変わらず、以下を徹底することが重要である（AI の悪用については「4.2 AI のセキュリティ」参照）。

（a）ビジネスメール詐欺の周知徹底と情報共有

ビジネスメール詐欺は、企業間のビジネス活動がメールに依存している点を悪用した巧妙な騙しの手口であり、その手口を知らなければ、被害を防止することは困難である。代表的な手口については、前述の特設ページにて公開しているレポート「ビジネスメール詐欺（BEC）の特徴と対策※104」の「3 ビジネスメール詐欺の代表的な手口の紹介」に掲載しているため参照いただきたい。

ビジネスメール詐欺におけるなりすましは外部企業との取り引きだけでなく、グループ企業同士の取り引きにおいても発生している。このため、海外関連企業を含む全グループ企業の全役職員に対して詐欺の手口について周

知徹底し、ビジネスメール詐欺への意識を高めておくことが重要である。特に、最高財務責任者（CFO：Chief Financial Officer）や経理部門等の金銭を取り扱う担当者が、ビジネスメール詐欺の脅威についてよく理解し、送金前に攻撃に気付くことができれば、金銭的な被害を未然に防ぐ可能性が高まる。

また、メールに普段とは異なる言い回しや表現の誤りがあった、返信したメールが送信エラーになった等、不審な兆候が見られた場合に、CSIRT 等の社内の適切な部門に報告できる体制をあらかじめ整えておき、その情報を組織内外で共有することも重要である。ビジネスメール詐欺は、自組織だけではなく、取引先にも被害が及ぶことがあり、取引先と情報を共有することにより、サプライチェーン全体でビジネスメール詐欺への耐性を高めることができる。自組織を詐称したビジネスメール詐欺を確認した場合や自組織が被害に遭った場合に、警察や金融機関に相談するとともに、取引先への注意喚起、IPA への報告等を迅速に行うことができる体制をあらかじめ整えておくことで、更なる被害拡大を防ぐことが可能となる。

(b) 送金処理のチェック体制強化

ビジネスメール詐欺の被害を防止するためには、送金時のチェック体制を強化することが最も重要である。金銭を取り扱う担当者は、通常と異なる対応（役員等からの通常の手順とは異なる支払い依頼や、企業間取引において別の口座への突然の変更依頼、見積価格の修正、支払方法の変更、急なメールアドレス変更等）を求められた場合はビジネスメール詐欺を疑い、別の担当者とダブルチェックを行うことや、信頼できる方法で入手した連絡先に、電話や FAX 等メール以外の手段で事実を確認するといった、二重三重のチェックを行う体制とすることが必要である。

(c) 攻撃に使われるメールアドレスへの対策

ビジネスメール詐欺において、攻撃者がメールを偽装する方法は様々であるが、返信先に設定されたメールアドレスに注意していれば偽メールであると見破れる可能性があったにも関わらず、返信してしまった事例が多く見られるため、送信前にメールアドレスが正しいかどうか、落ち着いて確認していただきたい。

ビジネスメール詐欺で使われるメール偽装の手口として、フリーメールを悪用する場合や、自組織のドメイン名に似せた詐称用のドメインを取得し、そのドメインのメールアドレスを用いて攻撃を行う場合がある。フリーメールや自組織外のメールアドレスから着信したメールについて、件名や本文にその旨の警告を表示するメールシステムを採用すれば、役職員がそれらのメールを見分けやすくなる。なお、このようなメールシステムを利用していても、取引先がフリーメールをビジネスに使っている場合や、攻撃者が取引先等のドメイン名に似せた詐称用のドメインを取得し、そのドメインのメールアドレスを用いる場合等、正しいメールと偽のメールの区別がつきにくい場合があるため、注意が必要である。また、送信元（From）を正しい送信者のメールアドレスに偽装し、返信先（Reply-To）を攻撃者のメールアドレスにする手口もあり、送信元（From）と返信先（Reply-To）が異なる際に警告を表示する機能があるメールシステムを導入することも対策として有効である。

(d) フィッシング・ウイルス・不正アクセス対策

ビジネスメール詐欺を行う攻撃者は、攻撃に至る前に、何らかの方法でメールのやり取りを盗み見ている場合がある。その方法として、フィッシング攻撃によるメールアカウント情報の詐取、ウイルス感染等によるメールの内容やメールアカウント情報の窃取、メールサーバーへの不正アクセス等がある。そのため、基本的なフィッシング対策・ウイルス対策・不正アクセス対策を徹底していただきたい。

特に、Microsoft 365 や Google Workspace 等のクラウドサービスを利用している場合は、多要素認証等を活用し、第三者による不正ログインを防ぐことが重要である。ただし、多要素認証を設定している場合でも、「AiTM（adversary-in-the-middle）」と呼ばれるフィッシング攻撃により認証を突破される被害が確認されている※105。多要素認証を設定しても対策は万全ではないことを認識の上、不審なメール内の URL にはアクセスしない等、基本的なフィッシング対策も同時に実施していただきたい。

また、利用者本人が行っていない転送設定やフォルダの振り分け設定がされている等、攻撃者によってメールアカウントが乗っ取られている兆候があった場合には、Microsoft 社等より該当アカウントへの対処方法※106 が公開されているため、そちらを参照いただきたい。

1.2.4 DDoS攻撃

DDoS（Distributed Denial of Service）攻撃とは、Web サーバー等の攻撃対象に対して、複数の送信元から同時に大量のパケットや問い合わせを送信すること

で、攻撃対象のリソースに負荷をかけ、サービス運用を妨害する攻撃である。

本項では、2023年度に確認されたDDoS攻撃について手口と事例、対策を解説する。

(1) DDoS攻撃の動向

セキュリティベンダーによると、2023年上半期に全世界で確認されたDDoS攻撃は、過去最多となる約790万回で、前年同期と比較して30.5%増加した※107。ロシア・ウクライナ戦争や、フィンランドの北大西洋条約機構（NATO：North Atlantic Treaty Organization）加盟等の世界的な出来事が、DDoS攻撃の増加要因とされる。戦争の発生に伴い、攻撃対象国の政府機関や重要インフラ事業者のサイトを使用不能にし、経済活動を麻痺させることを狙い、DDoS攻撃が増加したと考えられる。DDoS攻撃によりインターネットに接続しづらい状態にし、国民に不便を強いることで、国民がその国の政府に不満を持つように仕向けることも目的として考えられるという※108。

また、アジア太平洋地域の無線通信プロバイダーに対するDDoS攻撃が増加しており、これは、多くのオンラインゲーム利用者が、5G固定無線アクセスに移行していることと相関しているという※109。オンラインゲーム業界はDDoS攻撃の対象とされやすく、オンラインゲーム利用者のインターネット接続方式の移行に合わせて、攻撃対象が変化していることが考えられる。

(2) DDoS攻撃の手口と事例

ここでは、2023年度における、DDoS攻撃に関する主だった手口と事例を紹介する。

(a) リフレクション攻撃の手口と事例

通信プロトコルの中には、リクエスト（要求）よりもレスポンス（応答）のデータサイズの方が大きくなるものがある。

攻撃者がそのような仕様を悪用し、送信元を攻撃対象のIPアドレスに偽装した要求パケットをインターネット上の機器へ大量に送信することで、増幅された応答パケットが攻撃対象のIPアドレス宛てに送信される。攻撃対象はデータサイズの大きいパケットを受信することとなり、パケットの受信が継続すると、やがて処理能力が限界に達し、パフォーマンスの低下や動作の停止に至る。このようなDDoS攻撃を「リフレクション攻撃」と呼ぶ。

リフレクション攻撃では、外部に公開されているUDP（User Datagram Protocol）※110を用いて通信を行うサービス（以下、UDPサービス）を悪用した攻撃が、2022年度に引き続き、2023年度においても多く観測されている※111。UDPサービスを悪用した攻撃では、UDPの以下の三つの特徴が悪用される。

① UDPの仕様上、要求パケットの送信元IPアドレスを確認しないことから、送信元を偽装してパケットを送信することができる。

②応答パケットの方が、要求パケットよりもサイズが大きくなる増幅効果（Amplification）がある。

③ UDPサービスを提供するサーバー（以下、UDPサーバー）に要求パケットを送信することで、要求パケットに指定した送信元IPアドレスへ応答パケットが返される。リフレクション攻撃においては、送信元の機器として偽装された攻撃対象の機器に対し、増幅された応答パケットが反射（Reflection）される。

UDPサービスがDDoS攻撃に悪用されると、①の特徴により、攻撃元の特定が困難となり、②③の特徴を悪用することで、送信するデータサイズを数十倍から数百倍に増幅させた攻撃が可能となる。また、攻撃元とインターネット上からアクセス可能なUDPサーバーとの間の通信自体は正常であるため、攻撃の兆候を検出して対応を行うには、後述の「1.2.4(3)(c) DDoS攻撃に加担しないための対策」が必要となる。

UDPサービスを悪用したリフレクション攻撃の事例としては、2023年4月に、BitSight Technologies, Inc.及びcuresec GmbHによって公表された、SLP（Service Location Protocol）の脆弱性（CVE-2023-29552※112）を悪用したものが挙げられる。LAN内のプリンターやファイルサーバーを見つけるためのプロトコルであるSLPが単なるリフレクション攻撃に悪用された場合、増幅率は最大で12倍程度であるが、SLPへサービスを登録することにより、29バイトのリクエストに対して約6万5,000バイトを応答させることも可能であり、その場合の増幅率は約2,200倍もの高さになるという※113。SLPの脆弱性（CVE-2023-29552）は、悪用が確認されているとして、2023年11月に、CISAのKEV（Known Exploited Vulnerabilities Catalog：既知の悪用された脆弱性カタログ）にも登録された※114。

(b) ランダムサブドメイン攻撃の手口と事例

DNS（Domain Name System）の仕組みを悪用した「ランダムサブドメイン攻撃」（別名、DNS水責め攻撃）と呼ばれるDDoS攻撃が、2023年初めより急増している

という。セキュリティベンダーによると、2023年初めは、1日あたり平均144件であったところ、同年6月末には611件まで増加したとされる※115。ここでは、その手口について紹介する※116。

ランダムサブドメイン攻撃は、次の①～④の四つのステップで行われる。

①ボットネット※117の作成

攻撃者が、以下の二つから構成されるボットネットを作成する。

- 攻撃者が、ソフトウェアの脆弱性を悪用したりウイルスを感染させたりすることによって乗っ取った多数のコンピューター、ネットワーク機器及びIoT機器等
- 乗っ取った機器に対して、遠隔で命令を送信するためのC&Cサーバー

②オープンリゾルバー※118への問い合わせ

攻撃者は、①で作成したボットネットに対して、インターネット上に存在するオープンリゾルバーに、攻撃対象ドメイン名のランダムなサブドメインをDNS問い合わせするように命令する。この際、規制を回避するため、ボットネットからのDNS問い合わせは低い頻度で行われる。しかし、ボットネットに属する機器は多数であるため、オープンリゾルバーには大量の問い合わせが到達する。

③権威DNSサーバー※119への問い合わせ

ボットネットからのDNS問い合わせについては、ランダムに作成される文字列がサブドメインとして設定されている。そのため、オープンリゾルバーのキャッシュには情報が存在せず、攻撃対象である権威DNSサーバーへの問い合わせが毎回発生することとなる。

④権威DNSサーバー停止

攻撃対象の権威DNSサーバーに問い合わせが集中することで負荷がかかり、やがてサービス不能の状態となる。

ランダムサブドメイン攻撃は、DNSの仕組みそのものを悪用することから、根本的な対策が難しいと考えられる。対策としては、権威DNSサーバーの性能強化や、外部から不正使用できるオープンリゾルバーを減らす等が挙げられる※120。

2023年5月に開催されたG7広島サミットの期間中、地方公共団体を含む複数の官公庁に対して、DNSやHTTP（Hyper Text Transfer Protocol）を悪用したDDoS攻撃が行われ、広島市のWebサイトにおいても一時的に接続しづらい状態となったという※121。

このケースでは、Webサイトの一時的に接続しづらい状態が確認されたものの、警察庁によると、関係施設の事業者や重要インフラ事業者等との共同対処訓練等の取り組みの結果として、サミット等の進行に影響を及ぼすようなサイバー攻撃は発生しなかったとされている※122。

(3) DDoS攻撃への対策

DDoS攻撃への対策では、平時からの対策や、DDoS攻撃の被害に遭った場合の対策に加えて、管理または所有する機器が乗っ取られDDoS攻撃に加担してしまうことを防ぐための対策が求められる。これらの対策について解説する。

また、DDoS攻撃への対策については、2023年5月に、警察庁とNISCが連名で注意喚起を行っているため、そちらも参照いただきたい※123。

(a) DDoS攻撃への平時の対策

DDoS攻撃の被害に遭う前に、平時から攻撃を想定した対策をしておくことを推奨する。以下に、具体的な対処方法を挙げる。

- サービスの重要度に応じて、費用をかけて守る必要があるサービスと、一定期間の停止を許容できるサービスを選別する。選別したサービスごとに対応方針を策定する。選別した各サービスについて、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システムと、外部に公開されているような狙われやすいシステムを分離する。
- DDoS攻撃を受けた際、迅速に対応できるように、社内・社外の関係者、関係する行政機関及び警察等への連絡先をまとめておく。加えて、各主体がどのように対応を行うか等を記載した対応マニュアルやBCPを策定しておく。
- 取引先や顧客等に対して、DDoS攻撃を受けていてサービスに接続しづらい、または接続できない状態にあることを知らせることができるように、SNS等のアカウントや、通常のサービス提供とは別のWebサーバーにソーリーページを準備しておく。
- サービスの重要性によっては、インターネットサービスプロバイダー（ISP：Internet Service Provider、以下ISP事業者）等が提供するDDoS攻撃対策サービスや、セキュリティベンダー等が提供するDDoS攻撃対策製品の利用を検討する。
- ランダムサブドメイン攻撃のように根本的な対策が難し

い DDoS 攻撃に備えて、サービスを提供しているサーバーやネットワーク機器の性能強化、CDN（Contents Delivery Network）の導入及び契約しているネットワーク回線の増強等を検討する。

(b) DDoS 攻撃の被害に遭った場合の対策

DDoS 攻撃によって送られてく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策が必要である。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策のポイントとなる。以下に、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。
- 攻撃者が攻撃元の IP アドレスや攻撃方法を定期的に変更してくる場合がある。変化に応じた対策ができるように、継続して監視を実施する。
- 組織内で対処しきれない程、大規模な攻撃や執拗な攻撃を受けている場合は、ISP 事業者との対策協議等の連携や警察等への通報を実施する。

(c) DDoS 攻撃に加担しないための対策

自組織や個人で使用する機器が DDoS 攻撃に悪用されないように、セキュリティソフトの導入や機器への適切な設定等の対策が必要である。また、自組織の機器を悪用された場合に、それを早期に検知できるように通信の監視を行うような対策も推奨する。以下に、具体的な対処方法を挙げる。

- ネットワーク機器や IoT 機器の OS やファームウェアを最新の状態に保ち、脆弱性の悪用により制御を奪われることを防ぐ。
- 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。パスワードが初期設定のままの機器は、攻撃者により容易に侵入され、制御を奪われてしまう可能性がある。
- 外部と接続しているネットワーク機器や IoT 機器をとおして組織内の他の機器に対して感染拡大を試みるウイルスも確認されているため、インターネットに直接接続していない機器においても脆弱性対策等を行う。
- 組織内で運用している機器（例えば、プリンターや屋外に設置してリモートで管理している Web カメラ・センサー等）について、それらの機器上で稼働しているソフトウェアや各サービスが適切に運用されていることを確認する。具体的には、OS を始めとするソフトウェアや各サービスについて、脆弱性を含むバージョンで運用されていないかどうかや、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ことや、不要なサービスが起動していないこと等）を確認する。また、それらのサービスを組織内のみで利用している場合でも、意図せずインターネット上に公開していないかを確認する。
- 組織内の機器の外向きの通信を監視し、異常な通信を確認した場合は、自組織で管理している機器が攻撃に悪用されている可能性がある。異常な通信を行っている機器が確認された場合、ウイルス感染等が生じていないか調査し、対処を行う。自組織での対処が困難な場合は関係当局やセキュリティベンダー等への相談を検討する。

1.2.5 ソフトウェアの脆弱性を悪用した攻撃

2023 年度も、前年から継続して VPN 製品の脆弱性を狙った攻撃が多く報告された。また、多くの利用者がいる Microsoft 製品や、政府機関や企業等において利用者の多いファイル転送ソフトウェアに関する脆弱性を狙った攻撃も報告された。本項では、これらの脆弱性を悪用した攻撃の状況と対策について解説する。

(1) VPN 製品の脆弱性を対象とした攻撃

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

新たな脆弱性の発見と、脆弱性が解消されていない VPN 製品を狙った攻撃は 2023 年度も続いた。

本項では、VPN 製品の脆弱性を狙った攻撃事例と対策について解説する。

(a) Citrix Bleed を悪用した攻撃事例

2023 年 10 月 10 日、Citrix Systems, Inc.（以下、Citrix 社）は、自社製 Citrix NetScaler ADC（旧 Citrix ADC）及び NetScaler Gateway（旧 Citrix Gateway）に関して、複数の脆弱性（CVE-2023-4966 及び CVE-2023-4967[※124]）を公開し、脆弱性が解消されているバー

ジョンへ、ソフトウェアをバージョンアップすることを求めた。このうち CVE-2023-4966 は「Citrix Bleed」と呼ばれ、当該製品がゲートウェイ、または AAA※125 仮想サーバーとして構成されている場合において、攻撃者が細工した HTTP あるいは HTTPS リクエストを送信することで、Web 管理インターフェースの認証をバイパスすることが可能となる。結果として、攻撃者により任意の操作が行われる恐れのある脆弱性である（脆弱性対策情報の登録状況については「1.3.1 (3) Citrix Bleed に関する脆弱性を悪用した攻撃について」参照）。

同年 10 月 17 日、米国のセキュリティベンダーは、この脆弱性が同年 8 月下旬からゼロデイ脆弱性として存在していたとし、修正プログラムを適用する以前に、攻撃者がこの脆弱性を悪用して正規ユーザーのセッション情報を取得していた場合、修正プログラムを適用した後でも、セッションハイジャック攻撃により認証をバイパスされることを確認したと公表した※126。これを受けて Citrix 社は、ソフトウェアのバージョンアップに加え、アクティブなセッションや永続的なセッションの削除を推奨している※127。なお、セキュリティベンダーは、同年 10 月 31 日、この脆弱性における攻撃コード（PoC※128）を公開した※129。

この脆弱性は、LockBit や BlackCat 等の攻撃グループによるランサムウェア攻撃にも悪用され※130、これを受けて、同年 11 月 21 日、米国の CISA は FBI 等と共同でセキュリティアドバイザリーを公開した※131。

(b) VPN 製品の脆弱性を狙った攻撃への対策

新型コロナウイルス感染症の影響や働き方改革によるテレワークの普及等により VPN 製品の必要性が高まっているが、様々な理由により古い製品を利用せざるを得ないことも考えられる。その際は、ベンダーから継続的にサポートを受けられる状態であることを確認し、必要な修正プログラムを適用して既知の脆弱性を解消してから利用を継続することが望ましい。

利用しているソフトウェア等に脆弱性が発見されると攻撃者に狙われ、被害が発生してしまう可能性がある。新たな脆弱性が公開された際は、VPN 製品に限らず、迅速な対応が求められる。そのためには、事前の準備が重要である。自らが保有または利用するシステムについて、構成管理を適切に行い、システムを構成するソフトウェア等の脆弱性に関する情報収集を日々行う必要がある。また、事前に対策の実施手順を整えておき、脆弱性の対応を遅延なく着実に実施することが重要である。対策の実施手順として、以下に示す内容をあらかじめ定めておくことを推奨する。

- 利用しているソフトウェア等の脆弱性情報の収集方法
- 脆弱性が確認された場合の対応方法
- 脆弱性の緊急度や深刻度に応じた対応の優先順位
- 他部署やベンダー等への連絡の要否基準

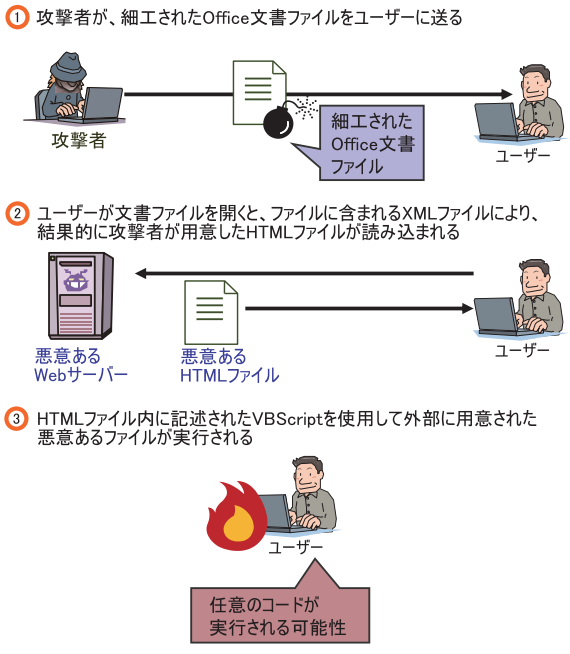
このような実施手順の準備に加え、侵害されている痕跡の有無の確認や、攻撃を受けてしまった場合の対応を定めておくことを推奨する。VPN 製品に対する攻撃は、組織内部への更なる攻撃の起点となる可能性があるため、包括的な対策が必要となる。

(2) Microsoft 製品の脆弱性を対象とした攻撃

2023 年度も、Microsoft 製品の脆弱性を狙った攻撃が多数報告されている。本項では、Microsoft Office が関係する脆弱性を狙った攻撃事例と対策を紹介する。

(a) Microsoft Office が関係する脆弱性を狙った攻撃事例

2023 年 7 月 11 日、Microsoft 社は、月例セキュリティ更新の際に、Microsoft Office が関係するリモートコード実行の脆弱性（CVE-2023-36884※132）の存在を公表した。この脆弱性は、攻撃者が細工した悪意のある Microsoft Office 文書ファイルをユーザーに送り付け、これをユーザーが開くことで、スクリプトを含むファイルがダウンロードされ、結果的に任意のコードが実行されるものである（図 1-2-14）。本来であれば、Mark of the



■図 1-2-14　CVE-2023-36884 の脆弱性を悪用した攻撃イメージ

Web（MOTW）と呼ばれるセキュリティ機能により、文書ファイルは保護ビューで開かれるはずであるが、ここではこの機能を回避する脆弱性（CVE-2023-36584[※133]）が悪用されていることが、後の調査で判明した[※134]。

これらの脆弱性を「Storm-0978」（別名、RomCom）と呼ばれる攻撃グループが悪用し、欧米の防衛機関及び政府機関を標的として攻撃を行ったとされている[※135]。

また、同攻撃グループが攻撃に使用したと見られるWordファイルが2023年7月3日にVirusTotalへアップロードされていたことが確認されている。Palo Alto Networks, Inc.の調査チームがこのファイルを確認したところ、ウクライナのNATO加盟を議論する2023年7月のNATO首脳会議における参加者を狙ったものだったと報告している[※134]。

(b) Microsoft製品の脆弱性を狙った攻撃への対策

脆弱性を狙った攻撃による被害を防ぐため、Microsoft社から修正プログラムが公開された際は、利用者は速やかにアップデートを実施することが求められる。修正プログラムが公表される前であっても、回避策が存在する場合は、悪用される可能性を踏まえた上で、回避策の実施を検討することが望ましい。

また、事前に対策の実施手順を整えておくことを推奨する（「1.2.5 (1) (b) VPN製品の脆弱性を狙った攻撃への対策」参照）。

(3) ファイル転送ソフトウェアの脆弱性を悪用した攻撃

2023年度は、ファイル転送ソフトウェアの脆弱性を悪用した攻撃が相次いだ。電子メールの添付ファイルによる送信よりも安全なファイル転送方法として、ファイル転送ソフトウェアを利用する企業が増えているが、そのソフトウェアに脆弱性が見つかり、悪用された場合、重要なデータを窃取されるだけでなく、暗号化された上、脅迫されることもある。

本項では、実際に発生した攻撃事例として、MOVEit Transfer及びProselfの脆弱性を悪用した攻撃とファイル転送ソフトウェアの脆弱性を狙った攻撃への対策について解説する。

(a) MOVEit Transferの脆弱性を狙った攻撃事例

MOVEit Transferは、Progress Software Corporation（以下、Progress Software社）が提供する高い安全性をうたったファイル転送ソフトウェアであり、米国においては幅広い政府系組織をユーザーに持つソフトウェアである。2023年5月31日、同社は、このソフトウェアにSQLインジェクションの脆弱性（CVE-2023-34362[※136]）があると公表した（脆弱性対策情報の登録状況については「1.3.1 (2) MOVEit Transferのゼロデイ脆弱性について」参照）。

同年6月2日、米国のセキュリティベンダーは、攻撃グループ「Clop」（「Cl0p」とも表記される）によるゼロデイ攻撃が同年5月27日から発生し、情報漏えいやランサムウェア攻撃が行われていたと公表している[※137]。

この脆弱性は、認証されていないリモートの攻撃者によるMOVEit Transferのデータベースへの不正なアクセスを可能とするもので、これを悪用されると不正アクセスによって、データの窃取や改ざん、権限の昇格を実行される恐れがある[※138]。このソフトウェアが広く使われている欧米を中心に被害が拡大し、海外拠点を持つ日本企業もその対象となり、トヨタ紡織株式会社の欧州子会社も被害に遭った可能性がある[※139]。また、2024年3月19日時点で、全世界で2,768組織及び約9,494万人の個人が被害を受けたことが明らかとなっている[※140]。

Progress Software社は、MOVEit Transferについて、2023年5月31日にCVE-2023-34362を公開して以降、同年6月中にCVE-2023-35036[※141]及びCVE-2023-35708[※142]を立て続けに公開した。これらもSQLインジェクションの脆弱性であり、なおかつ、CVSS v3.1基本値がそれぞれ9.1、9.8と最も深刻度が高い「緊急」に分類される脆弱性であったため、広く注目を集めることとなった。

(b) Proselfの脆弱性を狙った攻撃事例

Proselfは、株式会社ノースグリッドが提供するオンラインストレージ構築パッケージソフトウェアであり、ファイルの受け渡し等の機能を有している。2023年7月20日、同社は、Proselfにおける、認証バイパス及びOSコマンドインジェクションのゼロデイ脆弱性（CVE-2023-39415、CVE-2023-39416[※143]）を公開し、更に同年10月10日、XML外部実体参照（XXE：XML External Entity）のゼロデイ脆弱性（CVE-2023-45727[※144]）を公表した。これらの脆弱性が悪用された結果、独立行政法人日本学術振興会が不正アクセスされ、個人情報が漏えいする等の被害を受けた[※145]。

(c) ファイル転送ソフトウェアの脆弱性を狙った攻撃への対策

脆弱性を狙った攻撃による被害を防ぐため、利用するソフトウェアは常に最新のバージョンにアップデートしておくことが望ましい。アップデートによる対応が難しい場合は、脆弱性による影響を低減させる回避策がベンダーから提示されている場合があり、必要に応じて対応を実施することが推奨される。ただし、ここで紹介したゼロデイ脆弱性等、脆弱性の存在が明らかとなっていない状況では、日頃からログや通信の監視等を実施し、攻撃及びその予兆をいち早く察知できるよう備えておくことが肝要である。なお、IPA では、ファイル転送ソフトウェア等オンラインストレージを利用する際の脆弱性対策として、2023 年 10 月 19 日に「オンラインストレージの脆弱性対策について※146」と題した注意喚起を実施しているので、併せて確認していただきたい。

また、事前に対策の実施手順を整えておくことを推奨する(「1.2.5 (1) (b) VPN 製品の脆弱性を狙った攻撃への対策」参照)。

1.2.6 個人を狙うSMS・メールを悪用した手口

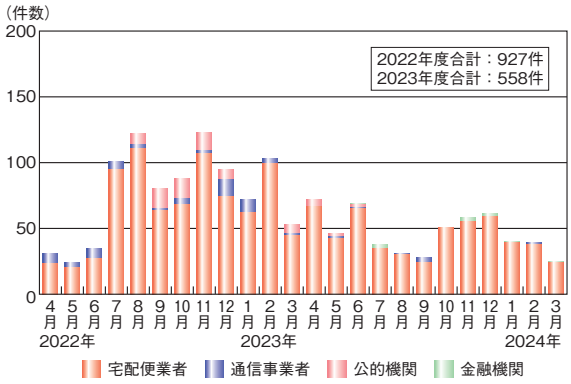
従来フィッシングサイトへの誘導は、主にメールで行われてきたが、SMS (ショートメッセージ) を悪用したものが増えてきている。個人がインターネットを利用する際の端末は、スマートフォンが約 7 割となっていることも背景として考えられる※147。

2023 年度に IPA の「情報セキュリティ安心相談窓口」(以下、安心相談窓口) に寄せられた SMS を悪用した手口の相談件数は、国税庁等公的機関をかたるものがメールに移行したこともあり、2022 年度に比べ減少したが、金融機関をかたる偽の内容の SMS (以下、偽 SMS) の手口が出現した。宅配便業者をかたる偽 SMS の手口は相談が継続して寄せられている(図 1-2-15)。

メールを悪用した手口では、ETC 利用照会サービスをかたるフィッシングのフィッシング対策協議会への報告が増加している※148。また、世の中の関心に乗じる手口としてマイナポイントに関連した手口が出現している。

(1) SMS を悪用した手口

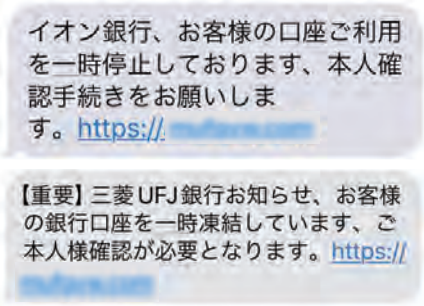
2023 年度も、偽 SMS の手口に関する相談は継続して寄せられている。国税庁等公的機関をかたる偽 SMS は減少する一方、宅配便業者をかたる偽 SMS の手口が継続して多い状況である(図 1-2-15)。



■図 1-2-15　偽 SMS に関する月別相談件数推移(2022～2023 年度)

(a) 金融機関をかたる偽 SMS

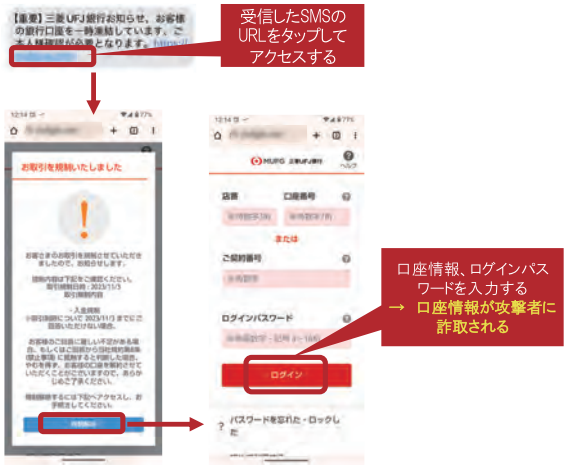
2023 年 6 月ごろより、金融機関をかたる「口座一時停止」等の文面が記載された偽 SMS (図 1-2-16) を送り付け、URL をタップさせようとする手口が出現し、IPA に相談が寄せられるようになった。2023 年 12 月には金融庁※149 や警察庁※150 から、被害額が過去最多になったと注意喚起が行われている。



■図 1-2-16　金融機関をかたる偽 SMS の例

この手口では、「口座一時凍結」「一時利用停止」という金融機関をかたった偽 SMS を送り付け、SMS 内のリンクからフィッシングサイトへ誘導する。iPhone や iPad 等の iOS 端末(以下、iPhone)と Android 端末(以下、Android) に共通して、偽 SMS の URL をタップさせ、銀行口座の情報を入力させるフィッシングサイトに誘導する手口が確認されている。URL をタップさせ、金融機関になりすましたフィッシングサイトへ誘導し、口座情報やログインパスワードを入力させる(次ページ図 1-2-17)。

この事例の金融機関のシステムでは、ログイン時に普段と異なる環境からインターネットバンキングにアクセスしていると判断されると、利用者本人にメールでワンタイムパスワードを送信し、第三者が不正ログインできないように対策を取っている※151。しかし、被害者が偽サイトに ID とパスワードを入力し、攻撃者がその情報を使って不正ログインを試みると、普段と異なる端末からのアクセス



■図 1-2-17　金融機関をかたるフィッシングサイトにログイン情報を入力させる例

であるため、被害者宛てにワンタイムパスワードが送信される。被害者が受信したワンタイムパスワードを偽サイトに入力してしまうと、攻撃者にワンタイムパスワードが伝わり、不正ログインが成功すると考えられる。

攻撃者は、他にも各インターネットバンキングの認証システムに合わせて偽の入力画面を表示し、情報を詐取していると考えられる。

安心相談窓口では、以下の被害を確認している。

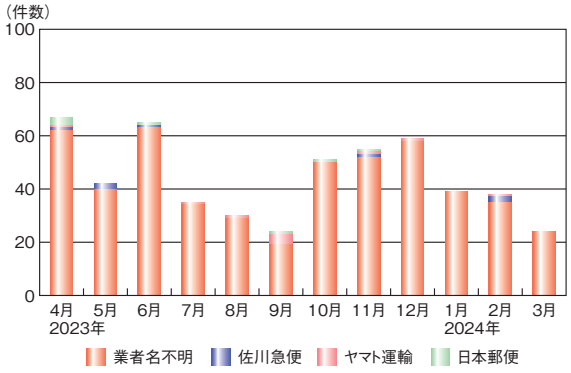
- フィッシングサイトで入力した銀行口座情報、メールアドレス、電話番号、氏名等の個人情報が詐取された。
- インターネットバンキングの口座に不正ログインされ、偽サイトでワンタイムパスワードを入力してしまい、攻撃者の口座へ不正に送金された。

金融機関をかたったフィッシングサイトにアクセスして口座情報やログインパスワード等の情報を入力した場合や金銭被害に遭った場合は、金融機関や警察に相談する必要がある。

(b) 宅配便業者をかたる偽 SMS

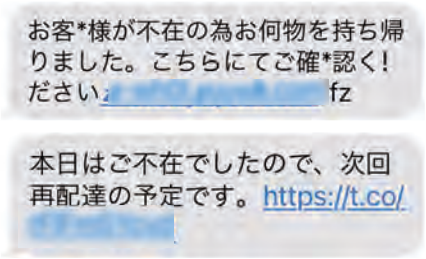
本件に関する相談は、2017 年から確認されている。この手口は、当初、佐川急便株式会社をかたるものであった。その後、ヤマト運輸株式会社や日本郵便株式会社といった実在する複数の宅配便業者名もかたられることがあったが、業者名がない偽 SMS も出現するようになった。2022 年 7 月からは、業者名のない偽 SMS の相談が増加し、ほとんどの相談が、業者名のないものとなっており、2023 年度も同様な手口が続いている（図 1-2-18）。

従来、通信事業者の迷惑 SMS ブロックサービスで止



■図 1-2-18　宅配便業者をかたる SMS の相談件数推移（2023 年度）

められないよう、偽 SMS の URL 表記として数学用英字等の特殊な文字が使われるケースがあったが、2023 年 10 月ごろからは、特殊な文字の使用はなくなり、X（旧 Twitter）が提供する短縮 URL 表記となった（図 1-2-19）。短縮 URL をタップすると攻撃者のサイトに転送される手口が出現してきている。



■図 1-2-19　偽宅配便 SMS の例

URL をタップさせ、Android に不正なアプリをインストールさせる手口や、iPhone でフィッシングサイトに誘導する手口については変化が少ないため、「情報セキュリティ白書 2021 [※152]」の「1.2.7 (3) (a) 宅配便の不在通知を装う SMS」を参照いただきたい。

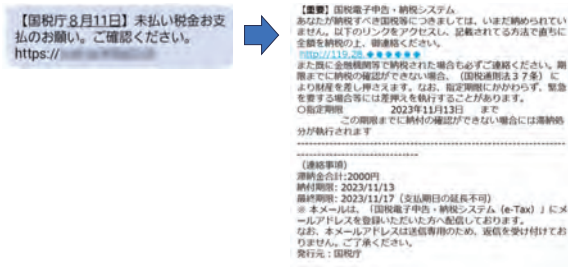
(2) メールを悪用したフィッシングの手口

SMS を悪用したフィッシングが増加しているが、メールを悪用したフィッシングの手口でも、様々な組織、企業をかたったり、世の中の動向に合わせた内容のメールが継続的に送られている。

(a) 国税庁をかたるメール

国税庁をかたるフィッシングの手口は、2022 年度は偽 SMS を送信する手口であったが、2023 年度には偽メールを送信する手口へと変化している（次ページ図 1-2-20）。

メールの文面の変化が続いており、当初は、「税金が納められていない」という内容がほとんどであったが、



■図 1-2-20　国税庁フィッシングの手口が SMS 送信からメール送信に変化

「国税還付金の電子発行を開始しました。」という、e-TAX への登録と思わせる文面が増えてきている。

「税金が納められていない」という内容の場合は、メールの URL をクリックすると、個人情報を入力させる画面が表示され、プリペイドカードでの支払いに誘導される（図 1-2-21）。

■図 1-2-21　プリペイドカードでの支払いに誘導する例

「国税還付金の電子発行を開始しました。」という内容の場合は、メールの URL をクリックすると、e-Tax への登録とかたる画面が表示され、クレジットカード情報の入力に誘導される（図 1-2-22）。

■図 1-2-22　e-Tax への登録とかたる例

(b) 世の中の関心に乗じる手口

2023 年は、マイナンバーカード取得によるポイント給付の締め切りが 9 月末であった※153 こともあり、マイナポイントの給付やマイナポータルサイトから給付金が支払われるといったフィッシングメールの手口が出現した。

2023 年 9 月末以降もポイント給付期限が延長されたと偽った内容のメールが送信されている（次ページ図 1-2-23）。

URL をタップすると、フィッシングサイトに誘導され、個人情報を入力させる。更に、マイナポイントの受け取りにキャッシュレスサービスの登録が必要とかたり、クレジットカード情報を入力させ、詐取する（次ページ図 1-2-24）。

また、物価高騰に伴う、給付金の受給がマイナポータルサイトから申請できるとかたる偽メールが、「電力・ガス・食料品等価格高騰緊急支援給付金」という内容で送信

■件名：マイナポイント第2弾で2万円のマイナポイントを獲得しました

■本文

マイナポイント第2弾で2万円のマイナポイントを獲得しましたが、
まもなく無効になります。
期限内に請求するように注意してください。

マイナポイントとは？
マイナポイントは、マイナンバーカードの普及や活用を促進するとともに、消費を活性化させるため、QRコード決済や電子マネーなどのキャッシュレス決済サービスで利用できるマイナポイント（1人2万円分）を付与する事業です。

ポイントをもらえますか？
はい、1回目のキャンペーンに参加してポイントを受け取っていても、
キャンペーンに参加できます。

マイナポイントの申し込み方法です
下記の手順でお申し込みください,最短3分でお申し込み完了です

★STEP1
応募専用サイトにアクセスし、応募書類を記入
★STEP2
マイナポイントの申込みをしよう
★STEP3
20,000円分のマイナポイントを取得し、ご活用ください

下記リンクよりお申し込みください！

https://[redacted]

※マイナポイント第2弾のポイント申込期限は、2024年1月末まで延長されました。

毎月更新している

なお、[redacted]信専用」ですので、
返信してお問い合わせいただくことはできません。

© マイナポイント第2弾

■図 1-2-23　マイナポイント第二弾をかたるフィッシングメール

■図 1-2-24　クレジットカード情報の登録に誘導する例

されている（図1-2-25）。フィッシングサイトに誘導し、クレジットカード情報を入力させ、詐取する。

(3) SMS・メールを悪用した手口への対策

金融機関によっては、取り引きに関するお知らせ等をSMSで送ることはないと注意喚起している。また金融庁は、金融機関がID・パスワード等をSMS等で問い合わせることはないと注意喚起している※149。特にSMS

住民税課税世帯等の皆さまへ

電力・ガス・食料品等価格高騰緊急支援給付金
（１世帯あたり５万円）

給付金の支給額？
１世帯あたり５万円

給付金の支給時期？

市区町村により異なります。
※市区町村が確認書を受理した後、
記載漏れがないか等の確認に、一定期間が必要です

支給対象と申請の有無？

令和４年度 現在で住民基本台帳に記録されている方
給付金を受給するためには、手続きが必要です。
マイナポータルサイトからオンラインで申請できます

下記リンクよりお申し込みください！

https://[redacted]

なお、本メールの送信アドレスは「送信専用」ですので、
返信してお問い合わせいただくことはできません。

© マイナポータル

■図 1-2-25　電力・ガス・食料品等価格高騰緊急支援給付金をかたるフィッシングメール

に記載されているURLには注意が必要である。

また、SMS、メールともに送信元の情報表示は偽装されている場合もあることに注意する。

不審と感じたメールやSMSの真偽は、公式サイト等の確かな情報源で確かめ、真偽がはっきりしないメールやSMSについては、下記の対応をする。

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

SMSを悪用した手口では、不正なアプリをインストールしてしまうと、他人に同様な偽SMSが送られることがある。SMSを悪用された場合は、不審なメッセージを受信した本人が被害を受けるだけでなく、他人に被害の連鎖を広げてしまう可能性があることに注意が必要である。

1.2.7 個人を狙う様々な騙しと悪用の手口

本項では、「1.2.6 個人を狙うSMS・メールを悪用した手口」に続いて、その他の個人を狙う騙しの手口と対策について述べる。

インターネットサービスやアプリを悪用して個人から金銭を奪うネット詐欺の被害が拡大している。中でも、2022年に引き続き、偽のセキュリティ警告（サポート詐欺）の被

害が拡大した。また、2022 年から IPA の安心相談窓口に相談が寄せられるようになった、副業詐欺、偽 EC サイトの被害も増加している。

副業詐欺は比較的新しい手口である。偽 EC サイトは以前から存在するが、2021 年に検索サイトを悪用して被害者を誘い込む手口の報告件数が増加し、現在も続いている※154。

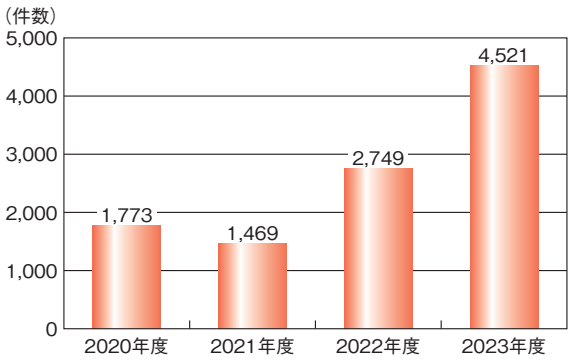
一方で、サポート詐欺は 2015 年ごろに出現して以来その手口に大きな変化はない。その反面、こうした従来の手口で騙されてしまう被害者も後を絶たない状況である。

(1) 偽のセキュリティ警告（サポート詐欺）

この手口では、パソコンに偽のセキュリティ警告を表示させ、それを見て慌てた被害者に偽のサポート窓口まで電話をかけさせる。その上で、サポート料金と称して高額の金銭を騙し取る。そのため、「サポート詐欺」とも呼ばれている※155。

2023 年度に IPA の安心相談窓口に寄せられた相談件数は、過去最高の 4,521 件となった（図 1-2-26）。2023 年は、金銭を騙し取る際に、パソコンの遠隔操作ソフトウェアを悪用してネットバンキングの不正送金に誘導する新たな手口が出現した。IPA の安心相談窓口に寄せられた相談では、攻撃者が遠隔操作を悪用して送金額に 0（ゼロ）を加えたため、その結果として被害者がネットバンクから 198 万円を送金させられた事例が発生した（「1.2.7 (1) (a) 手口」の「⑥サポートプランを示して支払いを求める」参照）。また警察の発表によると、サポート詐欺の被害に遭い、複数回にわたり不正送金をされた結果、1,690 万円もの被害に遭った事例が発生している※156。

サポート詐欺の 1 年間の被害額も年々増加しており、独立行政法人国民生活センター（以下、国民生活センター）によると、2022 年度の被害額は過去最高の約 5 億 9,000 万円であった※157。



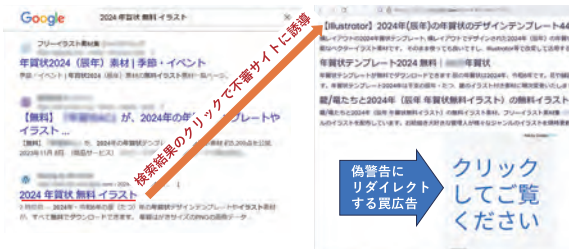
■図 1-2-26　偽のセキュリティ警告（サポート詐欺）に関する相談件数の推移（2020～2023 年度）

(a) 手口

具体的な手口について順を追って解説する。

①ネットに偽の警告を表示させる罠を仕掛ける

パソコンでインターネットを閲覧中に、突然偽のセキュリティ警告を表示させる罠の仕掛け方として、広告や検索サイトの悪用がある。例えば、2023 年の 11 月中旬から 12 月にかけて、検索サイトで「2024 年賀状 無料 イラスト」といったキーワードを入力して検索を行うと、結果に不審なサイトが表示され、そのリンクをクリックすると不審なサイトに誘導された（図 1-2-27）。誘導先の不審なサイトには、無料イラストのコンテンツはなかった。代わりに「クリックしてご覧ください」と記載した広告が表示され、この広告をクリックすると偽のセキュリティ警告サイトにリダイレクトされた。アダルトサイトの動画再生リンク等から誘導される場合もある。このような形でネット上には、クリックすると偽の警告に誘導される罠が仕掛けられている。

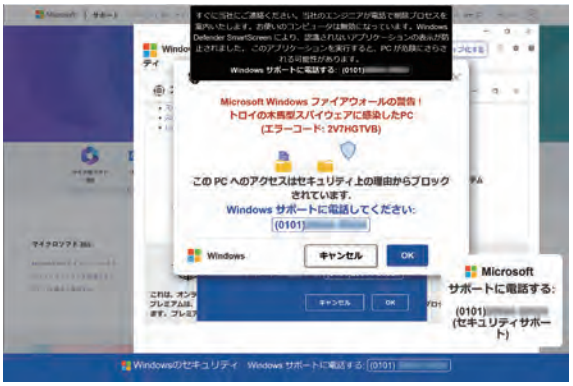


■図 1-2-27　検索結果と広告から偽のセキュリティ警告に誘導する例

②偽のセキュリティ警告で恐怖を煽る

偽のセキュリティ警告は、図 1-2-28 に示すような形で、Web サイトを閲覧中の Web ブラウザーによって表示される。

画面を埋め尽くすように次々と表示される警告の中に



■図 1-2-28　画面を埋め尽くすように表示される警告画面の例

は、「トロイの木馬スパイウェアに感染したPC」「PCへのアクセスがセキュリティ上の理由からブロックされた」等の警告文が書かれている。これらはすべて根拠のない偽の内容である。

③巧妙な細工で焦らせる

偽のセキュリティ警告が表示された際に、警告を消そうとしてキャンセルボタン等をクリックすると、Webブラウザーがフルスクリーン表示に変わり、「×」(閉じる)ボタンが非表示になってしまう。画面上に見えている偽の「×」(閉じる)マークをクリックしても反応はない。加えてスピーカーからは、「今すぐお電話ください、パソコンを再起動するとデータや個人情報の損失につながります」といった警告アナウンスが流れる。

このような細工によって、被害者に、パソコンが正常に操作できないという焦りや、ウイルスに感染してしまったのではないかとう恐怖心をいだかせて、正常な判断力を奪おうとしていると考えられる。

④実在する企業の名前をかたり信用させる

偽のセキュリティ警告画面には、Microsoft社等の実在する企業のサポートセンターと称する電話番号が表示される。被害者を焦らせた上で、著名な企業名をかたることによって、「ここに電話すれば解決してもらえる」と思わせようとしていると考えられる。

偽のセキュリティ警告に表示される電話番号では、国内の通信事業者が提供するIP電話番号(050番号)が悪用されていたが、2023年10月ごろから、0101で始まる電話番号への変化が見られた。この番号は、国番号1の北米(主に米国)に国際電話をかけさせるものである。この変化は、犯罪防止を目的として050番号契約時に本人確認の厳格化を求める法令改正[※158]に攻撃者側が対応した動きであると思われる。

⑤遠隔操作ソフトウェアを悪用して虚偽の説明を行う

被害者が偽のサポートセンターに電話をしてしまうと、片言の日本語を話す外国人のオペレーターにつながる。オペレーターは、キー操作等を指示して、遠隔操作ソフトウェアのダウンロードを行わせる。このソフトウェアは市販のもので、AnyDesk、LogMeIn Rescue、TeamViewer、UltraViewer等を悪用している。遠隔操作が可能になると、オペレーターは、被害者のパソコンを遠隔操作して様々な画面を開き、「これらはパソコンがウイルス感染している証拠である」という虚偽の説明を行う。例えば、テキストエディターでWindowsフォルダ内のバイナリーファイルを開いて文字化けした画面を見せ、「これは犯罪者の危険なファイルである」

■図1-2-29　文字化けしたファイルを危険なファイルであると主張

と主張する(図1-2-29)。

2023年は、企業・組織の役職員が同手口の被害に遭うケースも目立った。その際に、業務用のパソコンを遠隔操作されたことによる情報漏えいの懸念から、個人情報保護委員会への報告や、関係者への謝罪に至る事例があった。そのためIPAは、「安心相談窓口だより」で、業務で使用しているパソコンに偽の警告が突然表示された場合は、慌てずにシステム管理者に連絡を行うよう注意喚起を行った[※159]。

⑥サポートプランを示して支払いを求める

被害者に虚偽の説明を信じさせると、3～10万円のサポートプランを示す。料金の支払いには、Google Playギフトカード、Appleギフトカード等のプリペイドカードを近くのコンビニで買うように指示してギフトコードを詐取する。金銭の詐取は現在もこのようなプリペイドカードを悪用した手口が多くを占めるが、安心相談窓口で相談を受けた事例[※160]において、遠隔操作を悪用してネットバンキングで不正送金を行う手口を確認した。この事例では、攻撃者からネットバンクで料金を振り込むように求められた被害者が、遠隔操作が可能な状態のままネットバンキングサービスにログインして指示された口座に送金を行った。この際に、被害者が料金として19,800円を送金画面に入力した後で、攻撃者が遠隔操作を悪用して送金額に0(ゼロ)を2桁加えて、1,980,000円を送金させられた可能性がある。

ネットバンキングサービスでは、ログイン認証に加えて、送金時のワンタイムパスワード等で不正送金に対する多重のセキュリティ対策を行っているが、遠隔操作を悪用されると画面を見られたり、勝手に操作されることでセキュリティ対策を無力化されてしまう危険がある。

(b)対処

パソコンの警告画面については、Webブラウザーを閉

じるだけでよい。画面を閉じるには、「ESC」キーを長押しして Web ブラウザーのフルスクリーン表示を解除した上で画面右上に現れた「×」(閉じる) ボタンをクリック、または「Ctrl」「Alt」「Delete」キーを同時に押してからパソコンの再起動を行う※161。

上記の対処方法は、パソコンの操作に不慣れな初心者はうまく実施できない場合が多い。そのため IPA では、東京都の消費者月間イベント「見て、聞いて、話そう!交流フェスタ 2023※162」に偽警告の体験コーナーを出展し、偽警告画面の閉じ方を多くの来場者が体験した。加えて、IPA の Web サイトに「偽セキュリティ警告 (サポート詐欺) 画面の閉じ方体験サイト」を公開してこの操作を練習できるようにした※163。

パソコンに遠隔操作ソフトウェアをインストールさせられた場合は、Windows の「システムの復元」機能を使用して、当該ソフトウェアをインストールする前の状態にシステムを戻すことを推奨する。遠隔操作の及ぼす影響について判断できないため、システムの復元ができない場合は、パソコンの初期化を推奨する。

(2) スマートフォンの Web ブラウザーに表示される偽のセキュリティ警告

同手口は、スマートフォンで Web サイトを閲覧中に「ウイルスに感染している」等の根拠のない警告画面を表示して、偽のセキュリティ警告から iPhone や Android の公式アプリストアに誘導して、有償アプリの自動継続課金※164 に誘導するものである※165。

相談件数は減少しているものの、依然として不審な警告からアプリをインストールさせられたという相談が IPA の安心相談窓口に寄せられている。

(a) 手口

この手口では、インターネット閲覧中に偽のセキュリティ警告から誘導されることが多い。例えば 2024 年 1 月初頭に発生した攻撃では、箱根駅伝の動画配信を装った罠の動画が、検索サイトの検索結果に表示された。それをクリックすると、偽のセキュリティ警告が表示され、アプリのインストールに誘導された (図 1-2-30)。

以下では、iPhone の場合の手口と対処を中心に説明する。この手口では、「iPhone がウイルスにより深刻なダメージを受けています」「今すぐウイルスを除去」というような、偽のセキュリティ警告を表示して公式ストア上のアプリをインストールするよう誘導する (図 1-2-30)。

アプリのインストール時、または起動時に出る「1 週間無料トライアル」等の承認を行うと自動継続課金が登録されてしまう。当初は無料であっても、トライアル期間が過ぎると自動的に課金が始まる。この手口の目的は、偽のセキュリティ警告によってインストールさせたアプリの自動継続課金に相手を誘導することであると考えられる。

■図 1-2-30　偽警告 (図の中央) からアプリのインストールに誘導する例

(b) 対処

偽のセキュリティ警告が表示された場合は、Web ブラウザーのタブを閉じることで対処できる。

アプリをインストールしてしまった場合は、アンインストールする。アンインストールだけでは自動継続課金は解約されないので、自動継続課金が登録されてしまった場合は取り消す必要がある。iPhone の場合はサブスクリプションの解約、Android の場合は定期購入の解約を実施する。

(3) Web ブラウザー通知機能の悪用

パソコンやスマートフォンで、「システムエラー」「スマホをきれいにする!壊れる前に」等の警告が Web サイトを閲覧していない状態においても繰り返し表示されることがある。この表示は、攻撃者が Web ブラウザーの通知機能を悪用して偽の警告として表示したもので、表示された警告のリンクやボタンをクリックすると、セキュリティソフトの購入ページや、不審なスマートフォンアプリのインストールに誘導される場合がある※166。パソコンの場合は、「1.2.7 (1) 偽のセキュリティ警告 (サポート詐欺)」で解説した、サポート詐欺に誘導される場合もある (次ページ図 1-2-32)。IPA の安心相談窓口への相談件数は横ばいであるが、その中では電話をしてしまいサポート詐欺の被害に遭ったという相談が多い。

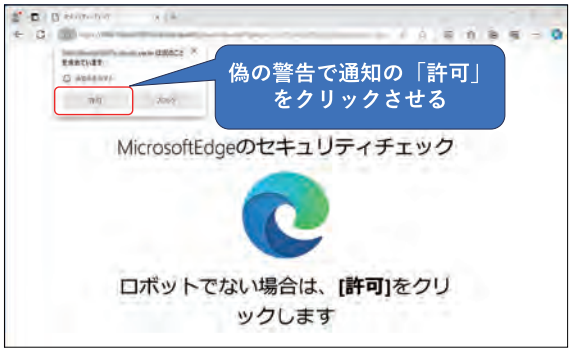
(a) 手口

Web ブラウザーの通知機能は、よく訪問するサイトから更新情報の通知等を受け取る機能である。この機能

を悪用して偽のセキュリティ警告のプッシュ通知を表示させ、不審サイトに誘導する。この手口は、以下の流れとなる場合が多い。

① Web ブラウザーの通知を許可するように誘導する

通知を受け取るためには、被害者が Web サイトからの通知を「許可」する必要がある。そのため、悪意のある Web サイトを訪れた被害者を騙して通知を「許可」させようとする。パソコンの場合は、Web ブラウザーに reCAPTCHA v2[※167] 認証を装った画面を表示して、「許可」ボタンを押させようとする（図 1-2-31）。スマートフォンの場合、通知を許可するか否かを求めるポップアップが表示される。



■図 1-2-31　reCAPTCHAv2 認証を装った「許可」ボタンへの誘導事例（パソコンの場合）

②偽の通知が表示される

通知を「許可」してしまうと、「システムエラー」「ウイルスを除去」等の偽のセキュリティ警告がデスクトップの右下から現れるようになる（図 1-2-32）。スマートフォンの場合は、「スマホをきれいにする!壊れる前に」等の通知が表示される。これらの表示は、アプリやパソコン、スマートフォンを再起動しても出続ける。

■図 1-2-32　Web ブラウザーの通知機能を悪用した偽警告の例

なお iPhone では Web ブラウザーの通知機能を提供していないため、この手口による被害が発生することはない。

(b) 対処

Web ブラウザーに登録した通知許可を削除することで、通知表示を止めることができる。各ブラウザーの操作方法の詳細は、IPA の「安心相談窓口だより[※166]」や、パソコン・スマートフォンメーカーのサポート情報、各 Web ブラウザーのヘルプページを参照いただきたい。

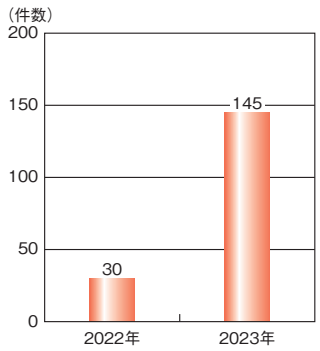
偽の通知に従って操作を行ってしまった場合は、行った操作や誘導された不審サイトの手口に応じて、以下の対処を行う。

- 偽の警告が画面一杯に広がり記載された番号に電話をしてしまった場合は、「1.2.7 (1) 偽のセキュリティ警告（サポート詐欺）」に記載した対処を行う。
- スマートフォンで不審なアプリのインストールに誘導された場合は、「1.2.7 (2) スマートフォンの Web ブラウザーに表示される偽のセキュリティ警告」に記載した対処を行う。

(4) 副業詐欺

副業詐欺では、通常は考えられない好条件の副業を SNS 等で宣伝して被害者を誘い込み、遠隔操作アプリを悪用して高額な副業マニュアルの購入やサポート契約を行わせる。

この手口は 2022 年から IPA の安心相談窓口に相談が寄せられるようになり、2023 年度は相談件数が大幅に増加した（図 1-2-33）。国民生活センターにも多くの相談が寄せられている[※168]。悪用される遠隔操作アプリは、2022 年に続いて、AnyDesk である場合が多い。副業詐欺に加えて、有利な投資を持ちかける投資詐欺においても遠隔操作アプリを悪用する事例が発生している。



■図 1-2-33　副業詐欺に関する相談件数の推移（2022～2023 年度）

(a) 手口

具体的な手口について順を追って解説する。

① SNS を使用した宣伝で誘導

SNS の広告やダイレクトメッセージを使用して副業紹介業者の URL に誘導する。

②高額なサポートプランに勧誘

副業紹介業者は、宣伝に興味を持った被害者を、業者の LINE アカウントに友達登録するように誘導する。そして、友達登録した被害者に、副業マニュアル購入等の高額なサポートプランの契約を強引に勧誘する。

③消費者金融からの借り入れを指示

被害者が契約に必要な現金を持っていない場合、消費者金融から借り入れを行うように指示する。その際に副業紹介業者は、遠隔操作アプリを公式アプリストアからインストールさせ、遠隔操作アプリを使用して被害者のスマートフォンの画面を見ながら借り入れの方法等を指示する。

(b)対処

遠隔操作が始まった後で、業者の行為に不審な点を感じた場合は、ネットワークを切断して遠隔操作接続を強制的に切断する。スマートフォンの場合、機内モードにすることでネットワークを切断する。遠隔操作を切断した後は、遠隔操作を受ける側が再度承認しない限り再接続されることはできない。

スマートフォンに遠隔操作アプリをインストールさせられた場合は、他のアプリと同様にアンインストールが可能である。ただし、副業紹介業者からの返金等を求めたい場合は、アンインストールは行わずに消費生活センターや警察に相談することを推奨する。

(5)偽 EC サイト

ネット検索で見つけた商品を EC サイトで購入したが商品が届かない等、偽 EC サイトの被害に関する相談が IPA の安心相談窓口に引き続き寄せられている。

2023 年は、業者に返金を求めた際に更に金銭を騙し取られる手口が現れた。この手口では、返金を装い LINE の通話機能等で被害者に接触し、キャッシュレス決済アプリ（PayPay 等）の送金機能を悪用して、被害者から業者に送金をさせてしまう。国民生活センターが注意喚起[※169]を行っており、IPA の安心相談窓口でも同様の相談を受けている。

(a)手口

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）によると、悪質なショッピングサイト等に関する通報の際に「どのようにそのサイトを知りましたか」と質問したところ、「インターネット検索結果」との回答が継続して最も多くなっているという。特に 2023 年上半期は、「インターネット検索結果」の割合が約 75% となっている[※154]。攻撃者は、インターネットの検索サイトを積極的に悪用して被害者を悪質な偽 EC サイトに誘い込んでいると思われる。

ここでは、検索サイトの検索結果から、改ざんされた Web サイトを経由して、被害者を偽 EC サイトに誘導する手口について紹介する。偽 EC 業者は、脆弱性の対処が行われていない WordPress 等の CMS（Contents Management System）で構築された Web サイトを改ざんし、偽 EC サイトの商品情報を仕込む。この情報を検索サイトの検索エンジンにクローリング（自動収集）させる。その結果、改ざんされた Web サイトのドメイン名に紐付く形で偽 EC サイトの商品情報の検索インデックスが生成され、検索サイトの検索結果にこの情報が表示される（図 1-2-34）。このとき、商品名に加えて「激安」等のキーワードを入れて検索を行うと、偽 EC サイトが検索結果の上位に表示される可能性が高まる。

■図 1-2-34　改ざんされた Web サイトに仕込まれた偽 EC サイトの商品情報

被害者が検索結果をクリックすると、改ざんされた Web サイトに HTTP リクエストが発行されるが、改ざんされた Web サイトは偽 EC サイトにリダイレクトする応答を行う。この結果、改ざんされた Web サイトを経由して、被害者が偽 EC サイトに誘導される[※170]。検索サイトの検索結果に目当ての商品が安い価格で表示されたとしても、安易に飛びつかないことが重要である。

(b)対処

偽 EC サイトに、他のサイトでも使用しているパスワードを入力してしまった場合は、当該パスワードを変更する。

また、配送先として入力した住所・氏名等の情報を悪用した不審メールや SMS に注意する。

支払いや返金に関する問題が発生した際は、最寄りの警察または、消費生活センターに相談していただきたい。

(6) ネット詐欺の被害に遭わないために手口を知る

本項のまとめとして、個人を狙う手口に対する対策を示す。個人を狙う手口に共通する点は、ネットに様々な罠を仕掛け、罠にかかった被害者を騙して金銭を詐取することである。こうした手口は、個人を狙う「サイバー攻撃」というよりは、人の心理的な弱点に付け込み、被害者を騙すための道具として既存のインターネットサービスやアプリを悪用する「ネット詐欺」と呼ぶ方がふさわしい。これらのネット詐欺への対策として最も重要なのは、手口を知り、騙されないことである。

正規のセキュリティソフトが、「1.2.7(1)偽のセキュリティ警告（サポート詐欺）」で解説したサポート詐欺の手口のように、セキュリティ警告を画面一杯に表示して今すぐサポートセンターに電話するように警告することはない。そのため、こうした偽警告の不自然さを知ることが騙されないために有効である。

サポート詐欺や副業詐欺で行われる遠隔操作アプリの悪用の被害に遭わないためには、遠隔操作のリスクや悪用の手口を知り、安易に遠隔操作を許可しないことが重要である。IPA では遠隔操作アプリの悪用に関する注意喚起を行っているため参照いただきたい※171。

偽 EC サイトは、価格の安さや限定商品であることを訴求している一方で、雑多な商品が乱雑に並んでいることが多い。また、個人が撮影してフリーマーケットサイトに掲載した商品画像と思われる写真を盗用して掲載している等の不自然な点も見受けられる。

こうした騙しの手口に対する知識を持つことによって、不審な状況に初めて遭遇した際も、慌てずに適切な対処が可能となる。

1.2.8 情報漏えいによる被害

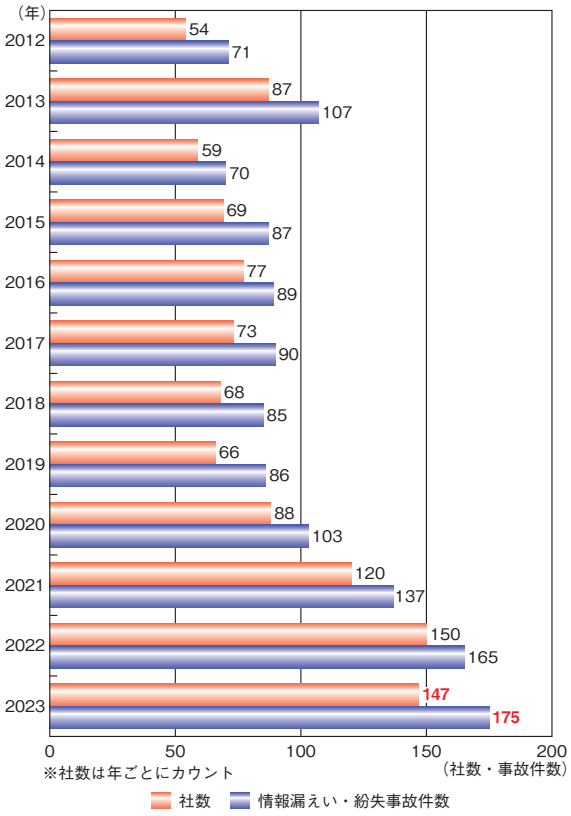
2023 年度も多数の情報漏えい被害が発生している。

本項では、外部からの不正アクセス、操作ミス等の過失、内部者の故意による持ち出し等の内部不正、不適切な情報の取り扱い等を主な要因とする情報漏えい被害について述べる。

(1) 2023 年度の情報漏えい件数

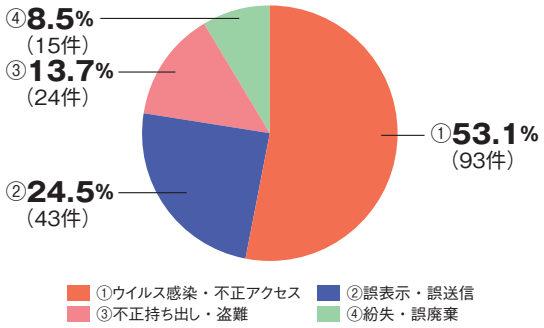
2024 年 1 月に株式会社東京商工リサーチ（以下、東京商工リサーチ社）が公開した上場企業とその子会社の個人情報漏えい・紛失事故の調査結果※172 によると、2023 年に漏えいした個人情報は 4,090 万 8,718 人分（2022 年は 592 万 7,057 人分）に達し、過去最多（2014 年の 3,615 万 1,467 人分）を大幅に更新した。

2023 年に個人情報の漏えい・紛失事故を公表した社数は 147 社（2022 年※173 は 150 社）、事故件数は 175 件（2022 年は 165 件）であった。漏えい・紛失事故を公表した社数は、2014 年から 2019 年までは 50 ～ 70 社台で推移していたが、2020 年から増加傾向にあり、2023 年も 147 社と高止まりしている。事故件数は、3 年連続で過去最多を更新した（図 1-2-35）。



■図 1-2-35　漏えい・紛失事故　年次推移
（出典）東京商工リサーチ社「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※172」を基に IPA が編集

2023 年の情報漏えい・紛失事故 175 件のうち、原因として最も多かったのは「ウイルス感染・不正アクセス」の 93 件で 53.1% を占め、次いで「誤表示・誤送信」が 43 件で 24.5%、「不正持ち出し・盗難」が 24 件で 13.7% であった。「不正持ち出し・盗難」は、2022 年の 5 件から約 5 倍の 24 件となった（次ページ図 1-2-36）。「不正



■図 1-2-36　情報漏えい・紛失　原因別
(出典) 東京商工リサーチ社「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」を基に IPA が編集

持ち出し・盗難」による大きな事故が相次いだことが、漏えいした個人情報の件数が過去最多となる要因となった。

(2) 不正アクセスによる情報漏えい

不正アクセスの手口は年々巧妙化しており、システムの脆弱性を悪用したものや、サプライチェーンを含む対策が不十分な取引先や委託先、システムへの侵入等、様々な原因から不正アクセスが発生している。

(a) 不正アクセスによる情報流出事例

2023 年 11 月に公表された JCOM 株式会社の事例※174 では、提携先のサーバーが不正アクセスを受け、顧客の個人情報（氏名または氏名とメールアドレス）合計約 23 万件が漏えいしたという。

LINE ヤフー株式会社の事例※175 では、委託先企業への第三者による不正アクセスを受け、ユーザー・取引先・従業者等に関する約 52 万件の個人情報が漏えいした可能性があることが 2024 年 2 月に公表された。2023 年 9 月、委託先企業の従業員が所有するパソコンがウイルスに感染したことを契機に、同社のシステムへ第三者による不正アクセスが行われたという（「3.6.2 (2) (c) 業務委託先経由のサイバー攻撃の事例」参照）。

(b) 不正アクセスによる情報流出への対策・対処

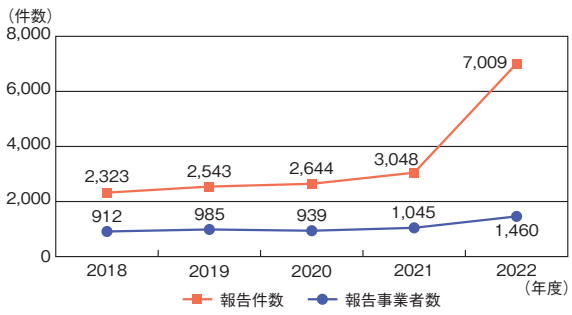
不正アクセスへの事前対策については、「1.2.2 (3) 標的型攻撃への対策」を参照いただきたい。不正アクセスが発生した場合、情報流出の有無の調査に時間を要することが多い。情報漏えいは企業・組織の信頼を失墜させる可能性があり、流出の事実が確認できるまでは公表を避けたいと考える企業もある。しかし、不正アクセスが検知された段階で公表することにより、類似の攻撃によるインシデントの未然防止や早期検知に貢献できる。また流出が確認された場合は、情報の悪用による二次被害を防げる可能性がある。そのため、企業・組織は早期に公表、あるいは関連機関への報告を行い、調査を継続して経過を伝えることが重要である。調査しても情報流出の有無が判明しない場合は、不正アクセス対策を強化するとともに、流出した情報が悪用されていないかを定期的に確認することが必要である。

複数の企業・組織が利用するシステムやサービスに対する不正アクセスは、影響範囲が広く、システムやサービスの提供事業者は、不正アクセス対策と流出した情報を特定する調査に更に時間を要することが多い。利用各社は当該事業者から情報流出の可能性について報告を受けた場合、すぐに二次被害を防ぐための対応と当該システムやサービスの利用継続の可否を検討しなければならない。情報流出被害がなかった委託元企業・組織も、システムやサービスの運用停止、改修等の影響を受ける可能性がある。システムやサービスの委託にあたっては日頃から委託している情報の種類、量、保管状態等を確認し、この情報が流出あるいは利用できない状態となった場合の対応策についても検討しておくことが望ましい。

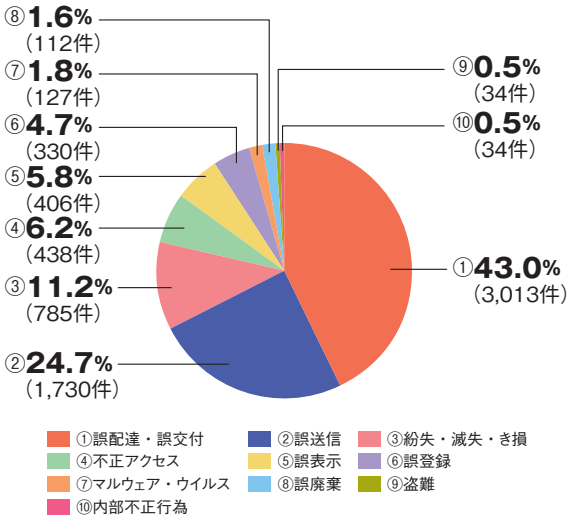
(3) 過失による情報漏えい

認定個人情報保護団体である一般財団法人日本情報経済社会推進協会（JIPDEC）が 2023 年 7 月 24 日に公表した「2022 年度　個人情報の取扱いにおける事故報告集計結果※176」によると、個人情報の取り扱いにおける事故等について、2022 年度は 1,460 社のプライバシーマーク取得事業者から 7,009 件の事故報告があった。2021 年度と比較すると、事故の報告件数、報告事業者数ともに大幅に増加している（図 1-2-37）。

事故分類は、「誤配達・誤交付」が最多の 3,013 件で 43.0% を占め、「誤送信」が 1,730 件で 24.7%、「紛失・



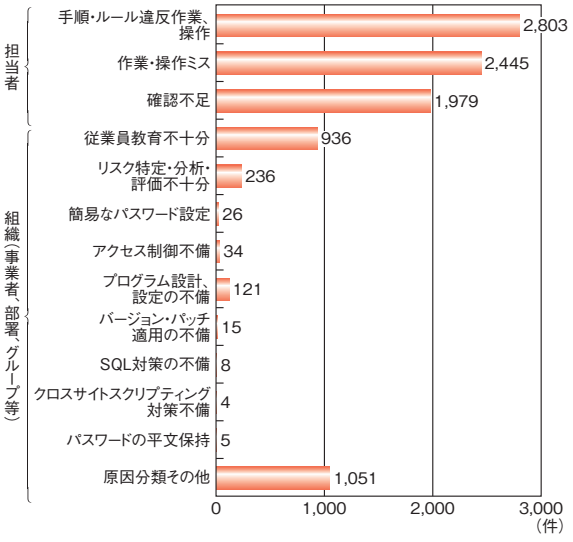
■図 1-2-37　事故報告の状況（2018～2022 年度）
(出典) JIPDEC「2021 年度『個人情報の取扱いにおける事故報告集計結果』※177」「2022 年度　個人情報の取扱いにおける事故報告集計結果」を基に IPA が作成



■図 1-2-38　事象分類別の事故報告件数(n=7,009 件)
(出典)JIPDEC「2022 年度『個人情報の取扱いにおける事故報告集計結果』」を基に IPA が編集

滅失・き損」が 785 件で 11.2% と続いた(図 1-2-38)。

事故原因は、「手順・ルール違反作業、操作」が最も多く 2,803 件、次いで「作業・操作ミス」が 2,445 件、「確認不足」が 1,979 件であった。組織(事業者、部署、グループ等)の対策不備に起因するものは少ない一方で、担当者の不適切な作業に起因するものが多かった(図 1-2-39)。



■図 1-2-39　事故原因別集計(n=9,663 件※178)
(出典)JIPDEC「2022 年度『個人情報の取扱いにおける事故報告集計結果』」を基に IPA が編集

(a)過失による情報漏えい事例

ひまわりネットワーク株式会社の事例※179 では、システムの機能停止によって、顧客へ同時送信した電子メールのアドレス 652 件が受信者に見える状態となっていたことが 2023 年 4 月に公表された。宛先アドレスを強制的に「BCC」へ変換するシステムに必要なソフトウェアライセンスの更新手続きを失念していたという。

株式会社出前館の事例※180 では、924 万 4,553 件のアカウント情報を第三者が閲覧できる状態にあったことが 2023 年 6 月に公表された。LINE アカウント等との連携システムに不備があり、同じパソコンやスマートフォンを複数人で共有している状態で、アカウント連携サービスにログインすると、直前に利用していたユーザーのログイン情報を閲覧できる状態であった。

2023 年 11 月に公表された九州電力株式会社の事例※181 では、帳票システムへのアクセス権限設定の誤りにより、約 290 万件の顧客情報が子会社の送配電会社で閲覧できる状態であった。閲覧可能だったのは、契約する顧客の名前や料金プラン、電気料金等の電子データであり、子会社の送配電会社からの指摘で発覚した。

(b)過失による情報漏えいへの対策

情報の取り扱いに人が介在する状況においては、過失による情報漏えい被害を完全に防ぐことは難しい。事故事例に基づく教育等で担当者の意識向上を図ることに加え、重要な情報の取り扱いルールを設け、運用を徹底する、適宜見直す等で、過失の発生機会をできる限りなくす体制作りが望まれる。うっかりミスを減らすために、ダブルチェック等の対策が取られることも多いが、テレワークや省人化・自動化のため、1 人で業務することも増えており、業務フローの見直しも含めたリスク低減策が必要である。また、業務を委託している場合は、ルール順守状況の点検や成果物の確認等を委託元の責任として実施することも大切である。

(c)クラウドの設定不備による情報流出事例

トヨタ自動車株式会社の事例※182 では、顧客の車台番号や位置情報等の一部が外部から閲覧できる状態になっていたことが 2023 年 5 月に公表された。漏えいした可能性があるのは、同社のコネクテッドサービス等の車載通信サービスに契約した顧客のデータ約 215 万人分であり、約 10 年間にわたり、外部からアクセスできる状態だった。同社の子会社トヨタコネクティッド株式会社が顧客のデータを誤ってクラウド上で公開設定にしていたことが、クラウド上のデータ取り扱いを点検する過程で判明したという(「3.6.2(1)(b)IaaS/PaaS 利用時の設定ミス」参照)。

2023年12月に公表された株式会社エイチームの事例※183では、クラウドサービス上で作成した個人情報約94万件を含むファイルがインターネット上で閲覧可能な状態にあったと判明した。クラウドサービスで管理する閲覧範囲を誤って「このリンクを知っているインターネット上の全員が閲覧できます」と設定していた。グループ全体で導入を検討しているセキュリティ製品の精度を検証したレポートにより、リスクのあるファイルとして検知されたことで発覚したという。

(d) クラウドの設定不備による情報流出への対策・対処

ここ数年、クラウドサービスを利用する事業者において、設定不備による情報漏えいが増加している。外部に公開すべきでない情報を設定不備で公開してしまい情報漏えいにつながるケースや、不正アクセスの原因となるケースが多く、社会的影響が無視できなくなっている。その他のクラウドサービスの課題と対策については「3.6 クラウドのセキュリティ」を参照いただきたい。

(4) 内部不正による情報漏えい

2023年も引き続き元社員等による営業秘密を不正に持ち出す事例が発生している。国の研究機関でも、元職員が中国企業に営業秘密を漏えいさせたとして逮捕された事例が発生している。

(a) 内部不正による情報漏えい事例

国立研究開発法人産業技術総合研究所の事例※184では、元研究所職員が不正競争防止法違反の容疑で逮捕されたことが2023年6月に公表された。元研究所職員は、2018年4月に研究内容を中国の民間企業にメールで送り、営業秘密を漏えいした疑いが持たれている※185。

日本山村硝子株式会社の事例※186では、元社員が不正競争防止法違反の容疑で逮捕されたことが2023年10月に公表された。元社員は同社固有の製造技術に関する機密情報を無断で社外に持ち出したとして、2022年11月に懲戒解雇処分となっていた。

2023年7月に公表された株式会社NTTドコモの事例※187では、顧客の情報約596万件が不正に持ち出されたという。委託先の株式会社NTTネクシアの元派遣社員が業務に使用しているパソコンから個人として契約する外部ストレージへアクセスし、顧客情報を含む業務情報を不正に持ち出したという。

2023年10月に公表された株式会社NTTマーケティングアクトProCX（以下、ProCX社）とNTTビジネスソリューションズ株式会社（以下、BS社）の事例では、BS社の元派遣社員により、ProCX社の顧客情報約928万件が不正に持ち出されたという。ProCX社は企業よりテレマーケティング業務を受託し、その遂行に必要なコールセンターシステムをクラウドサービスとしてBS社がProCX社に提供する関係にあった。BS社の元派遣社員は、顧客情報を預かるシステム運営企業の内部関係者にあたる。本件については、グループ親会社である西日本電信電話株式会社（以下、NTT西日本）により招集された社内調査委員会による詳細な報告書がまとめられている※188。報告書によれば不正な持ち出しは9年以上に及び、2022年には顧客企業より不正の疑いありとの訴えがあったにも関わらず、その時点での発覚とはならなかった。報告書では、2022年時点で行われた調査は「『調査』と表現することも憚られるほどの極めて杜撰な『作業』」と批判しつつ、直接的なセキュリティ対策上の問題としては、データ持ち出しを防ぐ技術的対策が導入されていなかったことや、十分な監視が行われていなかったことがある一方で、業務上の便宜を優先する空気が蔓延し、セキュリティがそもそもないがしろにされる組織となっていたことを厳しく指摘している。この事件を受け、NTT西日本の森林正彰社長は、2024年3月末をもって引責辞任することを表明した※189。

(b) 内部不正による情報漏えいへの対策

IPAでは、2022年4月に「組織における内部不正防止ガイドライン※190」第5版を公開している。内部不正による情報セキュリティ事故を防止するための幅広い対策を掲載しているため、参照いただきたい。

2024年4月に施行された不正競争防止法の改正では、内部不正に対する営業秘密の保護が強化された。被告が不正取得した「営業秘密」を使用したと推定する規定の適用対象が、元々営業秘密にアクセス権限のある者（元従業員、業務委託先等）にも拡充された（「2.1.3 (2) (b) 不正競争防止法の改正」参照）。

(5) 不適切な情報の取り扱い

誤送信等の情報の不適切な取り扱いによる漏えいも継続している。

(a) 不適切な情報の取り扱い事例

2023年11月に公表された株式会社プラスワン教育の事例※191では、3,732名分の個人情報が含まれるCSV

データを添付した電子メールを、自社が運営するWebサイト会員登録者約2,000名へ誤送信したという。誤送信されたCSVデータにはパスワードがかかっておらず、子供や保護者の氏名、生年月日、住所等が含まれていた。

三井住友カード株式会社の事例[※192]では、2023年4月18日と20日にダイレクトメールの表面宛先部に、誤ってクレジットカード番号を印字した状態で顧客へ送付していた。ダイレクトメールにはクレジットカード番号以外の情報（有効期限やセキュリティコード等）は記載していなかった。顧客が申告した住所宛てに発送していることから第三者がクレジットカード番号を知り得た可能性は極めて低いという。

(b) 不適切な情報の取り扱いへの対策

個人情報や営業秘密情報等の取り扱いについては、法改正やガイドラインの整備が進んでおり、組織内ルールへの取り込みや周知徹底のために役職員への教育等を継続して行う必要がある。

また図1-2-38（前々ページ）で見たとおり、電子メールには誤送信による情報漏えいの恐れがある。誤って重要情報が関係者以外に渡ってしまう可能性も考慮して、重要情報については暗号化等で保護することが必要である。

COLUMN

サポート詐欺で人が騙されてしまう心理的要因とその対策

サポート詐欺の手口で、被害者がどのように騙されてしまうのか、順番に心理的要因について考察していきたいと思います。

①偽の警告画面との接触時

インターネット検索や広告が悪用されて、Web ブラウザーに偽のセキュリティ警告画面が表示されると、被害者は次のような心理的な要因で騙されやすくなると考えます。

信頼感：Microsoft 等の社名やロゴマークが使われているため本物だと信じてしまう。

焦りや恐怖心：偽の警告画面は警報音とともに全画面に突然表示され、通常の操作では閉じにくいように細工されているため、異常が発生して操作できなくなったと思ってしまう。

②電話や遠隔操作による偽オペレーターの説明時

冷静な判断ができなくなり、表示された番号へ電話をかけてしまうと、次のような心理的な要因で詐欺の話術にはまってしまうと考えます。相手を信じて、言われるまま操作するとパソコンが遠隔操作されることになります。

信頼感：片言の日本語に違和感があっても、Microsoft 等の社名を名乗っているため信用してしまう。また、遠隔操作では偽の社員証を画面上に映され、安心してしまう。

焦りや恐怖心：パソコン内のシステムファイルを開かれ、ウイルスやハッカーの影響であるという嘘の説明や、すぐに処置をしないと更に情報が流出する等の嘘の説明を信じてしまう。カメラアプリを起動され、自身や室内の様子を画面上に表示され、映像が流出していると等の嘘の説明にパニックに陥った事例もある。

③偽オペレーターによる解決策の説明と支払い要求時

問題の解決策として料金の支払いを求められると、次のような心理的な要因で支払ってしまうと考えます。

信頼感：警告画面が消え、Microsoft 等のサポートを受けたと認識してしまっている。

安心感：嘘であるにもかかわらず、説明により恐怖や不安がなくなり、料金を支払えば安心だと考えてしまう。保証期間に応じた料金を選択できることで、支払いに対する不安も低減する。

以上のような心理的要因で騙されてしまうとすれば、手口を詳しく知らない場合でも、次のような心構えで対処することで被害に遭う可能性を減らせると考えます。

冷静に考える：焦りや恐怖心を抑え、落ち着いて判断や対処することが重要。

警戒心を持ち、真実を確かめる：初めて遭遇した出来事や不明なことは、周りの人に相談したりネットで検索したりして、真偽を確認する。

違和感を見逃さない：偽オペレーターは緊急性を訴えたり、矛盾した回答や高圧的な言葉遣いをしてくる特徴がある。電話をかけてしまった場合でも、違和感を持ったらすぐに電話を切る。

不審に思ったらどの段階でも、IPA の「情報セキュリティ安心相談窓口[i]」等の信頼できる機関へ相談されることをお勧めします。

i　https://www.ipa.go.jp/security/anshin/about.html〔2024/5/30 確認〕

1.3 情報システムの脆弱性の動向

本節では、ソフトウェア製品の脆弱性の動向や、ソフトウェア製品及び Web アプリケーションの脆弱性対策について概説する。

1.3.1 JVN iPediaの登録情報から見る脆弱性の傾向

IPA は、脆弱性対策情報データベース「JVN iPedia※193」に、国内外のソフトウェア製品の脆弱性対策情報を収集し、蓄積している。このデータベースに登録されている脆弱性対策情報から、ソフトウェア製品に関する脆弱性の特徴を統計的に分析することができる。本項では、主に 2023 年 12 月までに登録された JVN iPedia の脆弱性対策情報の傾向を分析する。

(1) JVN iPedia への登録状況

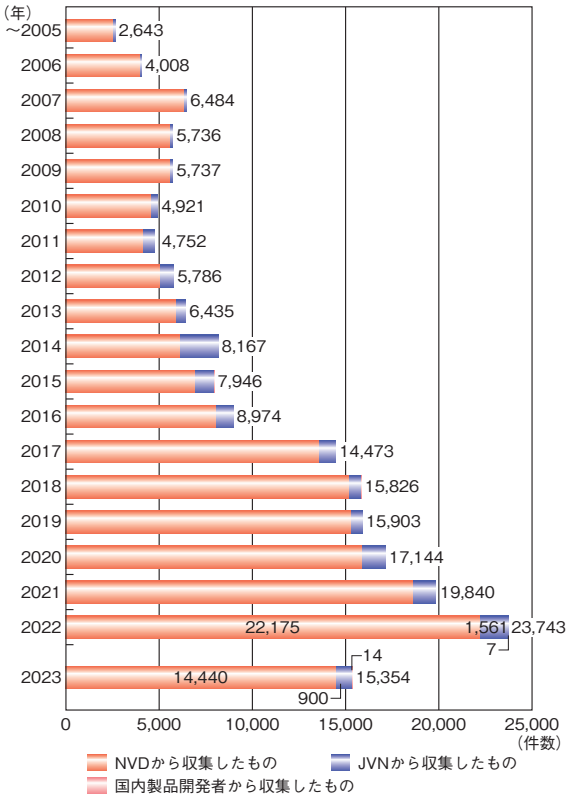
JVN iPedia は、国内外で利用されているソフトウェア製品の脆弱性対策情報を、以下の三つの公開情報から収集・蓄積しており、2007 年 4 月 25 日から公開している。

- 脆弱性対策情報ポータルサイト JVN※194 で公表した脆弱性対策情報
- 国内のソフトウェア開発者が公開した脆弱性対策情報
- 米国国立標準技術研究所（NIST：National Institute of Standards and Technology）の脆弱性データベース「NVD※195」で公開された脆弱性対策情報

(a) JVN iPedia の登録件数の推移

JVN iPedia に登録されている脆弱性対策情報の件数を、製品ベンダーやセキュリティ関連企業が情報を公表した年別※196 にまとめると、2011 年を境にして NVD から収集した情報の登録件数がおおむね増加傾向となっており、2022 年は 2 万件を超えた。なお、2023 年の登録件数は 12 月末時点で 1 万 5,354 件であるが、脆弱性対策情報の公開から JVN iPedia への登録までタイムラグがあるため、2023 年の登録件数も最終的には 2022 年と同程度になる見込みである（図 1-3-1）。2017 年以降、NVD に公開される脆弱性対策情報の件数が大幅に増加した理由としては、脆弱性を登録するための共通識別子である CVE（Common Vulnerabilities and Exposures）※197 の採番機関（CNA：CVE Numbering Authority）※198 が増加したことが一因として挙げられる。The MITRE Corporation※199（以下、MITRE 社）によると、2016 年 12 月に 47 組織※200 だった CNA は、2023 年 12 月には 345 組織※201 と約 7.3 倍となった。2023 年だけでも 82 組織が新たに CNA となっている。この増加した CNA によって、多くの脆弱性に CVE が付与され、NVD に公開される脆弱性対策情報の件数増加につながった可能性がある。

一方、JVN から収集した脆弱性対策情報のうち、JVN が 2023 年に公表したものは 900 件で、2022 年の 1,561 件から大幅な減少となっている。ただし、NVD から収集した脆弱性対策情報と同様に情報の公開から JVN iPedia への登録までのタイムラグが生じる場合があるため、最終的には 2022 年と同程度になる見込みである。また、国内製品開発者から公表された脆弱性対策情報は、近年十数件から 20 件の登録が続いた中で 2022 年は 7 件と減少していたが、2023 年は 14 件と例年と同程度の件数となった。



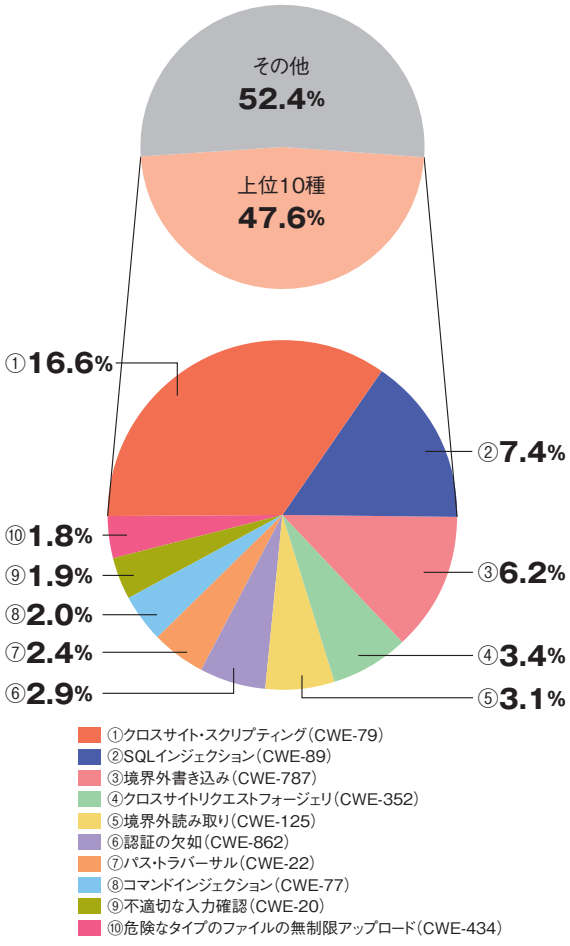
■図 1-3-1　JVN iPedia 登録状況（公表年別）
（出典）JVN iPedia の登録情報を基に IPA が作成

JVN iPedia は、発見された脆弱性の種類を識別するための共通脆弱性タイプ一覧 CWE（Common

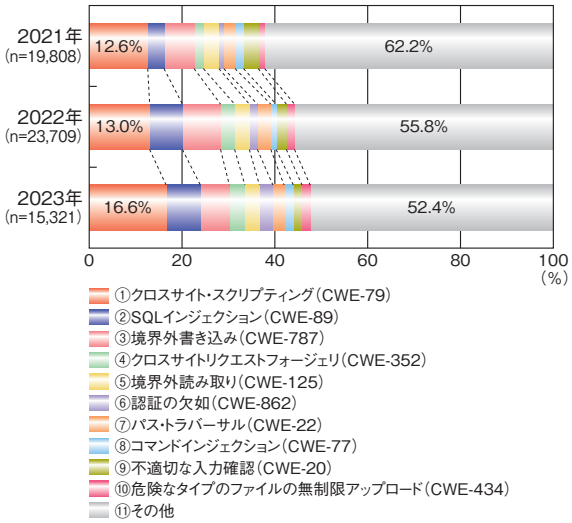
Weakness Enumeration)※202-1を脆弱性対策情報に付与して登録を行っている。2023年に登録されたCWEの割合は上位10種が全体の47.6%を占めており、その内訳を見ると「クロスサイト・スクリプティング」が16.6%と最も高く、「SQLインジェクション」が7.4%、「境界外書き込み」が6.2%、「クロスサイトリクエストフォージェリ」が3.4%と続いている(図1-3-2)。

最も件数の多かった「クロスサイト・スクリプティング」に分類される脆弱性を悪用されると、偽のWebページが表示されたり、情報が漏えいしたりする恐れがある。

2021年以降のCWE別割合を年別に見ると、今回1位となった「クロスサイト・スクリプティング」は増加傾向で、2023年は2022年から3.6%の増加となった。それ以外に2022年から2023年にかけて1%以上の増減が見られたのは、8.2%から6.2%に減少した3位の「境界外書き込み」及び、1.7%から2.9%に増加した6位の「認証の欠如」であった(図1-3-3)。



■図1-3-2 JVN iPediaにおける脆弱性対策情報のCWE別割合(2023年、n=15,321※202-2)
(出典)JVN iPediaの登録情報を基にIPAが作成



■図1-3-3 JVN iPediaにおける脆弱性対策情報のCWE別割合(2021～2023年)
(出典)JVN iPediaの登録情報を基にIPAが作成

(b) JVN iPediaの登録情報における脆弱性の深刻度

JVN iPediaは、オープンで汎用的な脆弱性評価手法であるCVSS(Common Vulnerability Scoring System:共通脆弱性評価システム)※203-1を用いて、脆弱性の深刻度を公開している。なお、JVN iPediaではCVSS v2及びCVSS v3の二つのバージョンの情報を公開しているが、昨今ではJVN iPediaの情報収集元がCVSS v2を公開しないことが多いため、本項ではすべてCVSS v3を基に統計処理を行っている。

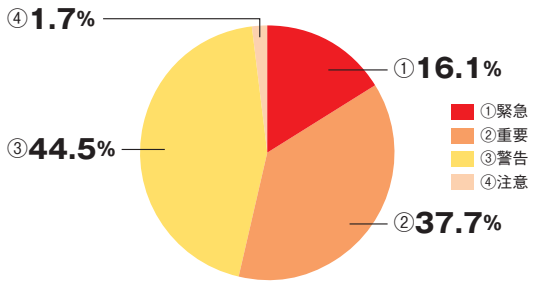
CVSSのスコアは数値が大きい程、深刻度が高くなる。CVSS v3では基本評価基準(BM:Base Metrics)を基に評価した基本値によって、深刻度が「緊急」「重要」「警告」「注意」「なし」の5段階に分けられる。

深刻度のレベルごとに想定される影響は以下である。

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

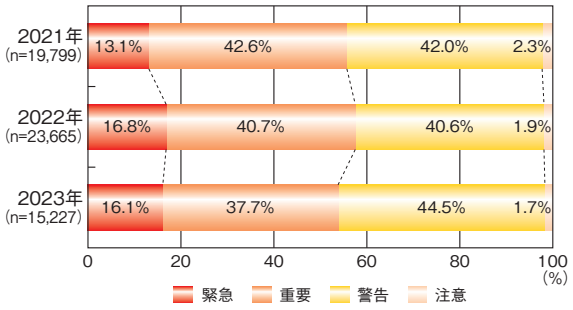
影響は発生しないと考えられる。

2023 年に登録された脆弱性対策情報を深刻度のレベルで分類すると、「緊急」が 16.1%、「重要」が 37.7%、「警告」が 44.5%、「注意」が 1.7% となっており、脆弱性を悪用された場合の影響が大きい「緊急」及び「重要」が過半数を占めている（図 1-3-4）。



■図 1-3-4　JVN iPedia における脆弱性対策情報のレベル別割合（2023 年、n=15,227[※203-2]）
（出典）JVN iPedia の登録情報を基に IPA が作成

2021 年以降の深刻度のレベル別割合を年別に見ると、「緊急」及び「重要」に分類される脆弱性の割合が 2022 年は 57.5% と 2021 年の 55.7% から増加していたが、2023 年は減少に転じ 53.8% となった。一方で、「警告」に分類される脆弱性の割合が、2023 年は 44.5% と 2022 年から 3.9% 増加している（図 1-3-5）。これは、比較的「警告」に分類されることが多い「クロスサイト・スクリプティング」の脆弱性の割合が増加したことが一因と考えられる。



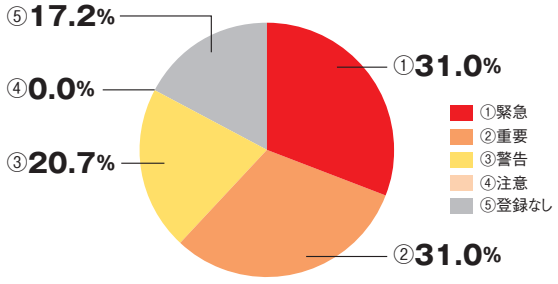
■図 1-3-5　JVN iPedia における脆弱性対策情報のレベル別割合（2021～2023 年）
（出典）JVN iPedia の登録情報を基に IPA が作成

直近 3 年間の登録情報の深刻度から見ても、製品開発者は、ソフトウェアの企画・設計・製造の各段階からセキュアコーディング[※204]を含めたセキュリティ対策を講じる等、脆弱性による被害を未然に防ぐための対応が必要となる。また、製品の利用者にも、日頃から新たに公開される脆弱性対策情報に注意を払い、脆弱性が公開された場合には製品を最新バージョンにアップデートする等の対応が必要となる。

(2) MOVEit Transfer のゼロデイ脆弱性について

2023 年 5 月、Progress Software 社が提供するファイル転送ソフトウェア MOVEit Transfer の脆弱性 CVE-2023-34362 が公開された[※136]。同脆弱性はデータベースを不正に操作される恐れのある SQL インジェクションの脆弱性で、認証されていないリモート攻撃者がこれを悪用すると、MOVEit Transfer に不正アクセスされ、データの窃取や改ざん、権限の昇格を実行される恐れがある。脆弱性の深刻度を示す CVSS v3 基本値は 9.8 で、最も深刻度が高い「緊急」と評価されている[※205]。同脆弱性は、脆弱性対策情報が公開される前から攻撃に悪用されていたことが確認されていた。このような脆弱性はゼロデイ脆弱性と呼ばれている。2023 年は MOVEit Transfer の脆弱性がほかにも複数公開され、深刻度が高い脆弱性も含まれていたことから広く注目を集めていた。

JVN iPedia には 2024 年 1 月末時点で累計 29 件の MOVEit 関連製品の脆弱性が登録されている。図 1-3-6 はその深刻度別割合を示したものである。脆弱性の深刻度が高い順に「緊急」が 31.0%、「重要」が 31.0%、「警告」が 20.7%、「注意」が 0.0% となっており、60% 以上が脆弱性を悪用された場合の影響が大きい「緊急」及び「重要」に分類されている。



■図 1-3-6　MOVEit 関連製品の脆弱性の深刻度別割合（n=29）
（出典）JVN iPedia の登録情報を元に IPA が作成

MOVEit Transfer のように利用者の多い製品は、脆弱性対策情報が公開されると攻撃者の注目も集め、攻撃に悪用される恐れがある。MOVEit Transfer は主に海外の企業・組織での利用が多いためか、日本における被害は限定的であった（攻撃事例については「1.2.5 (3) (a) MOVEit Transfer の脆弱性を狙った攻撃事例」参照）。しかし、国内で広く使用されている製品にも、MOVEit Transfer の脆弱性と同様の深刻な

脆弱性が発見される可能性は常にある。利用者においては、継続的に脆弱性対策情報を収集し、修正プログラムが公開された場合は速やかに対応することが求められる。また、同事例のように脆弱性を悪用した攻撃が既に確認されている場合もあるため、脆弱性対策情報と併せて攻撃に関する情報も収集し、被害の有無を確認することを推奨する。

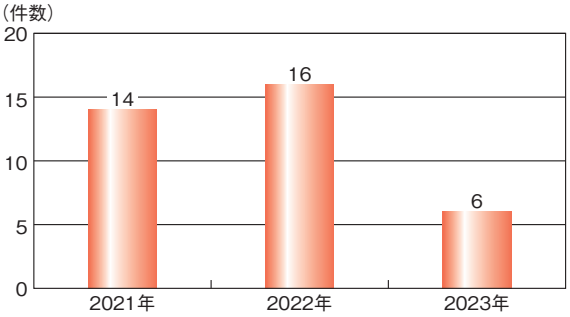
(3) Citrix Bleed に関する脆弱性を悪用した攻撃について

2023 年にも数々の脆弱性が発見されたが、10 月に公表された CVE-2023-4966[※206] は「Citrix Bleed」と呼ばれて話題になった。Citrix Bleed は Citrix 社の Citrix NetScaler ADC（旧 Citrix ADC）及び NetScaler Gateway（旧 Citrix Gateway）に存在する脆弱性で、製品がゲートウェイ、または AAA 仮想サーバーとして構成されている場合に、バッファオーバーフローが引き起こされ、情報漏えいが発生する恐れがある。また、バッファオーバーフローを発生させた際に窃取したセッション情報を悪用した攻撃も確認された。更にランサムウェアへの悪用も確認され、被害が拡大した（攻撃事例については「1.2.5(1)(a)Citrix Bleed を悪用した攻撃事例」参照）。

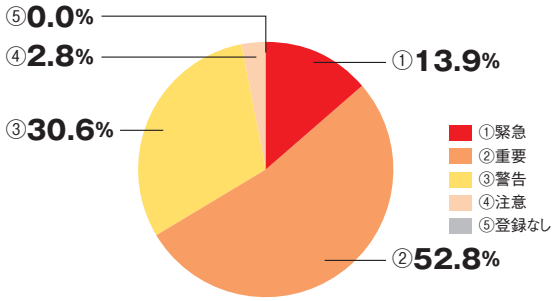
開発元である Citrix 社は、この脆弱性への対策としてソフトウェアのアップデートだけではなく、追加でコマンドを実行してアクティブなセッションや永続的なセッションを削除することを推奨した[※207]。また、同社は CVE-2023-4966 の CVSS v3 基本値を 9.4 とし、最も深刻度が高い「緊急」と評価した。

2021 年から 2023 年に公表され、JVN iPedia に登録された Citrix NetScaler ADC 及び NetScaler Gateway を含む Citrix 社製品の脆弱性対策情報件数の推移及び深刻度別割合を図 1-3-7、図 1-3-8 に示す。

JVN iPedia では 2012 年から毎年 Citrix 社製品の



■図 1-3-7　2021 年～2023 年に公表された Citrix 社製品の脆弱性対策情報件数
(出典)JVN iPedia の登録情報を元に IPA が作成



■図 1-3-8　2021 年～2023 年に公表されたシトリックス・システムズ製品の深刻度割合（CVSS v3）(n=36)
(出典)JVN iPedia の登録情報を元に IPA が作成

脆弱性が登録されている。深刻度別割合を見ると脆弱性の深刻度が高い順に「緊急」が 13.9%、「重要」が 52.8%、「警告」が 30.6%、「注意」が 2.8% となっており、全体の 66.7% が脆弱性を悪用された場合の影響が大きい「緊急」もしくは「重要」に分類されている。

ソフトウェアやハードウェアの導入当初には既存の脆弱性に対応した最新バージョンを利用していても、時間が経過するとともに新しく脆弱性が発見される恐れがある。また、脆弱性に対応した最新バージョンへのアップデートだけではなく、今回の Citrix Bleed のようにアップデート以外に追加の対応が必要になる場合もある。自組織で利用している製品の脆弱性対策情報を収集し、開発元等から最新バージョンへのアップデート以外に追加の対応が要求されている場合は速やかに実施する必要がある。

(4) 今後の展望

JVN iPedia に登録された脆弱性対策情報の登録件数は 2023 年 12 月末時点で累計約 20 万件となった。公表年単位で見ると、件数が大きく増えた 2017 年は約 1 万 4,000 件であったが、2022 年には約 2 万 4,000 件となっており、毎年脆弱性の公開件数が増えていく状況になっている。2023 年の公開件数は 2023 年 12 月末時点で約 1 万 5,000 件となっており、今後も更に増えるものと思われる。そして、2024 年に公表される脆弱性対策情報も同様の傾向になると考えられる。非常に多くの脆弱性対策情報が公開されるため、自組織に必要な脆弱性対策情報を機械的に収集する仕組みを活用することを検討いただきたい。その仕組みとしては、IPA が提供する「MyJVN API[※208]」や「MyJVN 脆弱性対策情報フィルタリング収集ツール（mjcheck4）[※209]」等が挙げられる。

また、2023 年は身近に生成 AI という言葉が使われ出した。そして、その仕組みを利用したサービスやソフトウェ

アが提供され、企業や官公庁では活用の検討や試験的な活用が始まっている。例えば、大和証券株式会社では 2023 年 4 月に対話型 AI である ChatGPT が導入され、資料作成の時間短縮や ChatGPT を利用した更なる活用のアイデアの創出を期待しているとしている※210。

一方、生成 AI の普及に伴い、生成 AI 本体の脆弱性や、生成 AI を利用したソフトウェアの脆弱性が、セキュリティの研究者や攻撃者に興味を持たれ、数多く発見されることで、脆弱性対策情報が公開される機会が増えると考えられる。既に JVN iPedia では生成 AI を利用したソフトウェアの脆弱性対策情報が登録されており、今後は更に JVN iPedia への登録も増加すると見込まれる。

それぞれの環境で使用しているソフトウェア等をきちんと把握した上で、アップデート等の情報収集を行い、適切な脆弱性対応ができるようにする必要がある。その手段の一つとして JVN iPedia を活用いただきたい。

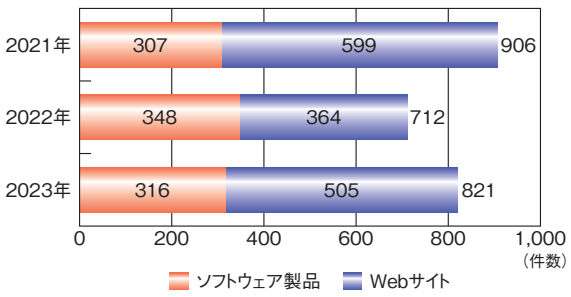
1.3.2 早期警戒パートナーシップの届出状況から見る脆弱性の動向

ソフトウェア製品や Web アプリケーション（以下、Web サイト）※211 の脆弱性を悪用した攻撃による情報漏えい、及び Web サイト改ざん等の被害は、2023 年も引き続き発生している。2000 年ごろより、ソフトウェア製品や Web サイトに脆弱性が発見されることが増え、重大な被害が生じるようになった。そこで、脆弱性関連情報の円滑な流通、及び対策の普及を図るため、「情報セキュリティ早期警戒パートナーシップ※212」（以下、パートナーシップ）制度が整備された。

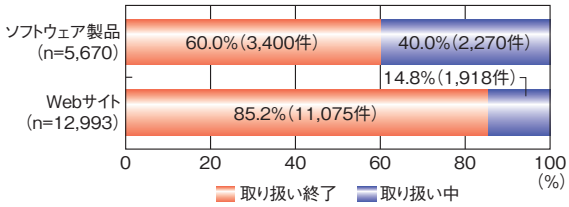
2023 年にパートナーシップへ届出された件数は、ソフトウェア製品が 316 件、Web サイトが 505 件、合計 821 件であった（図 1-3-9）。

2023 年のソフトウェア製品及び Web サイトの総届出件数（821 件）と、2022 年の件数（712 件）を比較すると、約 15% 増加している。なお、2023 年のソフトウェア製品と Web サイトそれぞれの届出件数を 2022 年の件数と比較すると、ソフトウェア製品の届出は約 9% 減少、Web サイトの届出は約 39% 増加した。

パートナーシップ開始時点（2004 年 7 月 8 日）から 2023 年 12 月末時点での届出件数を累計すると、ソフトウェア製品は 5,670 件、Web サイトは 1 万 2,993 件、合計は 1 万 8,663 件に上る。これらの届出のうち IPA での取り扱いが終了※213 した届出件数は、ソフトウェア製品 3,400 件（60.0%）、Web サイト 1 万 1,075 件（85.2%）である（図 1-3-10）。



■図 1-3-9　脆弱性関連情報の種類別届出状況（2021～2023 年）
（出典）パートナーシップの届出状況を基に IPA が作成



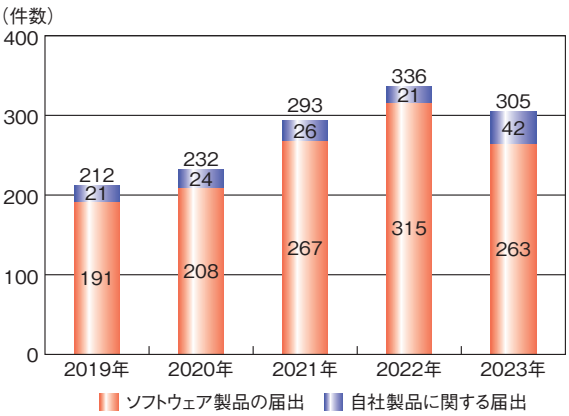
■図 1-3-10　脆弱性関連情報の種類別取り扱い終了状況
（2023 年 12 月末時点での累計）
（出典）パートナーシップの届出状況を基に IPA が作成

(1) ソフトウェア製品の脆弱性

2023 年のソフトウェア製品の脆弱性の状況を、パートナーシップへの届出件数や製品開発者による対策の取り組み状況等から解説する。

(a) 2023 年のパートナーシップの届出受付動向

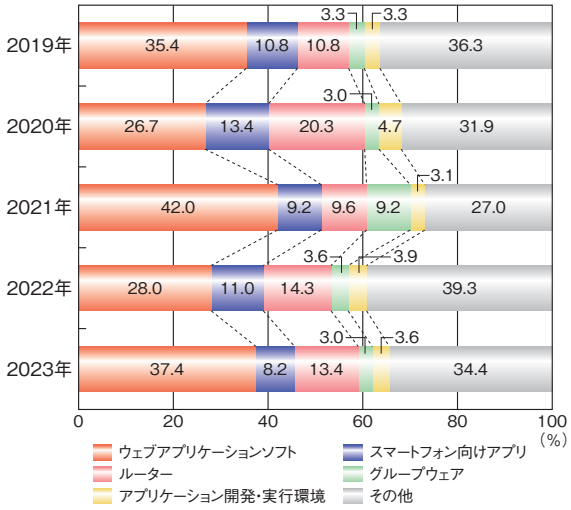
図 1-3-11 は、2019 年から 2023 年までの 5 年間のソフトウェア製品の届出受付数（不受理を除く）を示している。2023 年の届出受付数は 305 件であり、2019 年から増加傾向にあったものが減少に転じた。一方で、製品開発者自身による届出である自社製品に関する届出は 42 件となり、5 年間で最も件数が多くなった（「1.3.2 (1)



■図 1-3-11　ソフトウェア製品の不受理を除いた届出受付数
（2019～2023 年）
（出典）パートナーシップの届出状況を基に IPA が作成

(c) 製品開発者によるパートナーシップへの届出の活用」参照)。

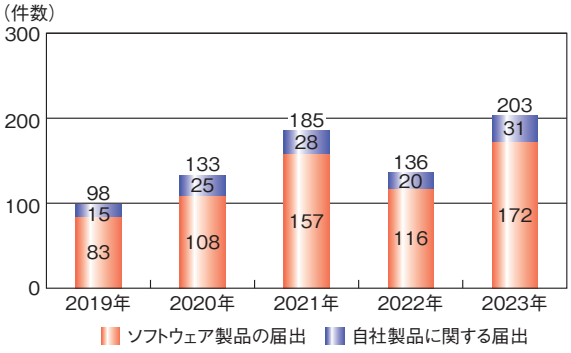
図 1-3-12 は、2019 年から 2023 年までの 5 年間の製品種類別の届出受付数の割合を示している。2022 年に比べ 2023 年に割合が増加したものは「ウェブアプリケーションソフト※214」で、28.0% から 37.4% に増加した。Web サイトを構築するためのソフトウェアである CMS (Contents Management System) や、CMS の機能拡張プラグインに関する届出が多い傾向にあった。「ウェブアプリケーションソフト」「スマートフォン向けアプリ」「ルーター」の割合は、直近 5 年間で常に上位 3 位を占めている。



■図 1-3-12 製品種類別のソフトウェア製品の届出受付数の割合 (2019～2023 年)
(出典)パートナーシップの届出状況を基に IPA が作成

(b) 2023 年の JVN 公表の動向

図 1-3-13 は、2019 年から 2023 年までの 5 年間の JVN 公表数を示している。パートナーシップへの届出のうち 2023 年に JVN 公表に至った件数は、203 件であった。2022 年の 136 件と比べて増加し、5 年間で最も件数が多くなった。また、2023 年に JVN 公表した自社製品に関する届出は 31 件であり、5 年間で最多であった。



■図 1-3-13 届出されたソフトウェア製品のうち JVN 公表した件数 (2019～2023 年)
(出典)パートナーシップの届出状況を基に IPA が作成

パートナーシップにおけるソフトウェア製品の届出については、パソコンやサーバーにインストールして使うパッケージソフトや、スマートフォンアプリといったソフトウェアだけでなく、ルーターやプリンター、IoT 製品等の組み込み機器に関する脆弱性届出も受付している。

表 1-3-1 は 2023 年に JVN 公表に至った IoT 製品の例である。2023 年の JVN 公表の事例から、データロガー機能を持つ温度計やセンサーを搭載した眼鏡等、様々な種類の製品で届出がされ、脆弱性が修正されていることが分かる。

製品ジャンル	JVN 番号	件名
カメラ	JVN#98612206	プラネックスコミュニケーションズ製 ネットワークカメラ「CS-WMV02G」における複数の脆弱性
温度計	JVN#14778242	ティアンドデイ製およびエスペックミック製データロガーにおける複数の脆弱性
住まい	JVN#19748237	Panasonic 製「AiSEG2」における複数の脆弱性
眼鏡	JVN#13306058	「JINS MEME CORE」におけるハードコードされた暗号鍵の使用の脆弱性
鍵・錠	JVN#48687031	「Qrio Lock (Q-SL2)」における Capture-replay による認証回避の脆弱性

■表 1-3-1 2023 年に JVN 公表した IoT 製品の脆弱性の例
(出典)JVN を基に IPA が作成

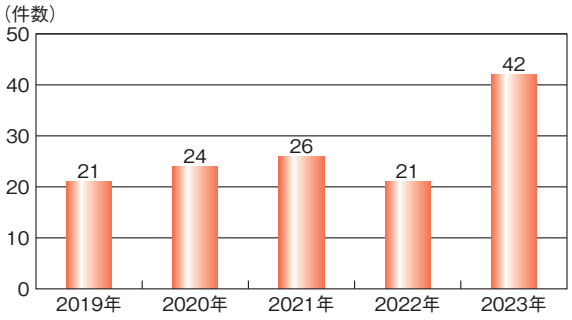
(c) 製品開発者によるパートナーシップへの届出の活用

製品開発者は、脆弱性対策された修正版の情報を広く利用者に周知し、アップデートを促すことが重要となる。しかしながら、パートナーシップの届出において、修正版が公開されているにも関わらず、利用者がアップデートせずにそのまま製品が使用されており、脆弱性が再現するという指摘が外部の人より届出されるケースがある。

利用者が製品をアップデートしていない要因として、業務へ影響が出る可能性がある、他のソフトウェア製品への影響調査に時間を要する等のケースがあるが、そもそも修正版が公開されていることを認知していないケースも考えられる。製品開発者は脆弱性対策情報を自社 Web サイトで公開するだけでなく、脆弱性対策情報を複数経路で提供し、入手しやすくすることで、利用者が認知しやすくなると考えられる。パートナーシップでは、

そのような対応の一助として、製品開発者自身による自社製品の届出（自社届出）を用意している。自社届出として受け付けた脆弱性についても、JVN 公表をしている。

図 1-3-14 は 2019 年から 2023 年までの 5 年間について、自社届出の届出受付数を示している。自社届出の年間の受付数は、2021 年の 26 件、2022 年の 21 件に対し、2023 年は 42 件と倍増している。一度自社届出をした製品開発者が、その後も継続的に自社届出をするケースが増加したことが一因と考えられる。



■図 1-3-14　自社届出の届出受付数（2019～2023 年）
（出典）パートナーシップの届出状況を基に IPA が作成

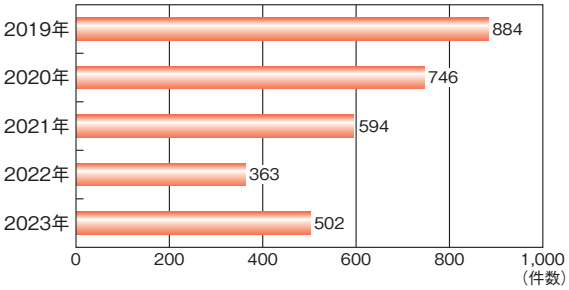
製品開発者は脆弱性対策情報の公表手段として、自社 Web サイトでの公開のほかに、自社届出の活用も検討いただき、より多くの利用者への情報周知を心がけていただきたい。情報周知にあたっては、利用者へ修正版へのアップデートを促すため、当該脆弱性を利用した攻撃の有無や、影響の大きさ等の緊急性を認識できる情報を含むことが好ましいと考える。脆弱性対策が行われていないソフトウェア製品を使い続ける利用者を少しでも減らすため、今後も自社届出を利用する製品開発者が増えることを期待したい。

(2) Web サイトの脆弱性

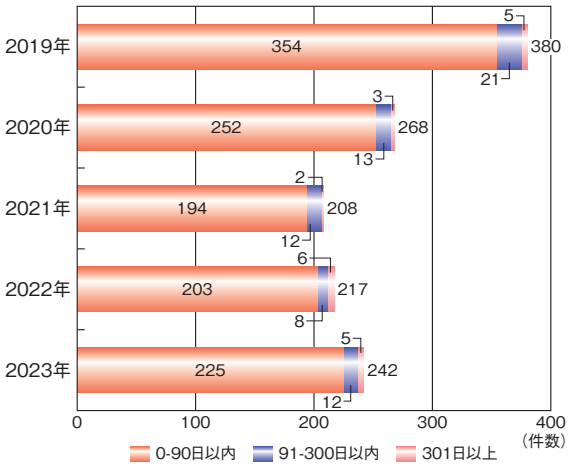
2023 年にパートナーシップで受け付けた Web サイトの届出（不受理 3 件を除く）は、502 件であった。

図 1-3-15 は、2019 年から 2023 年までの Web サイトの届出件数（不受理を除く）を示している。届出件数は 2019 年から減少傾向にあり、2022 年は 363 件であったが、2023 年は増加に転じた。

図 1-3-16 は、2019 年から 2023 年までに IPA が修正完了と判断した届出件数を、修正完了までに要した日数別に示している。なお、本件数は、当該年に届出された中で修正完了と判断した件数ではなく、届出された年は問わず、当該年において修正完了と判断した件数である。修正完了と判断した件数は、2023 年は 242 件



■図 1-3-15　Web サイトの不受理を除いた届出受付数（2019～2023 年）
（出典）パートナーシップの届出状況を基に IPA が作成

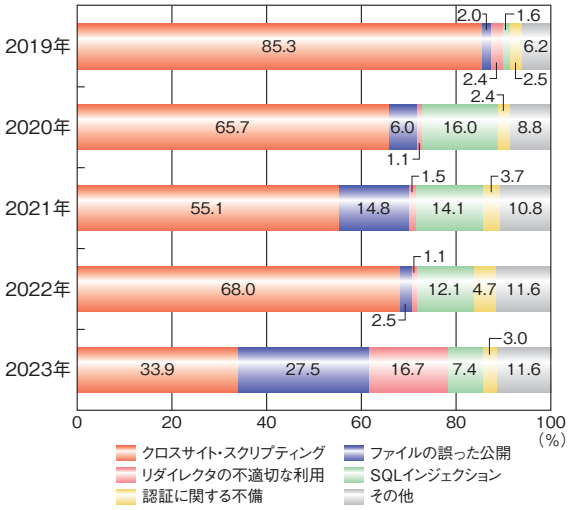


■図 1-3-16　Web サイトの修正完了に要した日数別の届出件数（2019～2023 年）
（出典）パートナーシップの届出状況を基に IPA が作成

であった。2019 年から減少傾向にあったが、2022 年に増加に転じており、2023 年も増加傾向が続いた。

(a) パートナーシップから見る 2023 年の届出の動向

図 1-3-17 は、2019 年から 2023 年までに受け付けた



■図 1-3-17　Web サイトの不受理を除いた脆弱性種類別届出件数割合（2019～2023 年）
（出典）パートナーシップの届出状況を基に IPA が作成

届出（不受理を除く）における Web サイトの脆弱性について種類別内訳の割合を示している。

例年、「クロスサイト・スクリプティング」の脆弱性が最も多く、2023 年も最多であった。ただし、2019 年以降、割合としては毎年 50% 以上を占めていたが、2023 年は 33.9% まで小さくなった。また、2022 年に「クロスサイト・スクリプティング」に次いで 12.1% を占めた「SQL インジェクション」の脆弱性は、2023 年には 7.4% となった。

一方、2023 年にその割合が大きくなったものとしては「ファイルの誤った公開」と「リダイレクタの不適切な利用」の脆弱性がある。

「ファイルの誤った公開」の脆弱性は 2023 年には 27.5% を占め、2 番目に多かった。届出件数では 138 件となり、2021 年の 88 件を超え、脆弱性種類別で見ると、パートナーシップ開始の 2004 年から最多の届出件数となった。

2023 年に 3 番目に多く届出されたのは「リダイレクタの不適切な利用」の脆弱性であった。「リダイレクタの不適切な利用」は、例年、1 ～ 2% 程度の届出割合であり、最も大きかった年でも 2019 年の 2.4% であったが、2023 年ではそれを超え、16.7% を占めた。届出件数では 84 件で、「ファイルの誤った公開」と同様に、パートナーシップ開始以来、最多の届出件数となった。

パートナーシップは、原則として、セキュリティ研究者を始めとする発見者が見つけた脆弱性を届出として受け付ける制度であり、その届出傾向は、世の中全体で発見される脆弱性や、サイバー攻撃等に悪用される脆弱性の傾向を反映するものではない。しかしながら、この届出傾向から、2023 年においても、様々な種類の脆弱性が Web サイトに存在していること、そして「クロスサイト・スクリプティング」や「SQL インジェクション」の脆弱性のような、よく発見される脆弱性以外の脆弱性についても、日々、発見されている状況にあることが分かる。

以下では、2023 年に届出が多かった「ファイルの誤った公開」と「リダイレクタの不適切な利用」について紹介する。

(b) 2023 年のファイルの誤った公開の届出

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

2023 年には、あるアプリケーションの認証に関連する設定情報ファイルが Web サイトで公開状態となっていることを指摘するものが複数届出された。このファイルはアプリケーションの構築・実装の段階で自動的に生成されるものであって、Web サイト運営者が意図してアップロードしたものではない可能性があると推定されるものであった。Web サイト運営者がそのファイルの存在を認識できていなかったために、アクセス制限の必要性を検討する機会を逸していたことが考えられる。

(c) 2023 年のリダイレクタの不適切な利用の届出

「リダイレクタの不適切な利用」は、Web サイトに設置されたリダイレクタ（他の Web ページに遷移するための仕組み）が悪意あるリンクの踏み台にされ、利用者が意図せずに悪意ある Web ページを表示させられる問題である。「オープンリダイレクト（Open Redirect）」とも呼ばれる。

この脆弱性は、悪用することで、正しいリンクだと誤認した利用者に悪意あるページを表示させることができるため、フィッシング攻撃に用いられることがある。2023 年の届出にも、フィッシングを目的に送信されたと思われるメール等で悪用されている可能性を指摘するものが複数存在した。

また、Web サイト運営者が独自に構築したアプリケーションではなく、広く頒布されているソフトウェア製品にオープンリダイレクトの脆弱性があり、その製品を Web サイトに組み込んで利用していることによって脆弱性が生じていることを指摘するものも複数あった。

(d) Web サイト運営者に求められる対策

2023 年は届出件数も増加に転じており、届出傾向からも認識できるように、Web サイトにおける脆弱性は様々な種類のものが存在している。Web サイト運営者には、自組織で運用する Web サイトについて、脆弱性診断を実施して、改めて脆弱性の有無を確認するよう努めていただきたい。自組織で実施が難しい場合には、外部のセキュリティベンダーに依頼して実施することも一案となる。

特に 2023 年に届出の多かった「ファイルの誤った公開」については、どのようなファイルが自組織で運用する Web サイト上で外部からアクセス可能な状態となっているか改めて確認することが必要となる。また、Web サイトと同一のサーバーで稼働させているアプリケーションについて、構築・運用時にどのようなファイルを生成するの

か、それらのファイルがWebサーバー上のどの領域に配置されるのかについても、情報を把握することが有用だと考えられる。

「リダイレクタの不適切な利用」については、IPAが提供している「ウェブ健康診断仕様※215」において検出方法を紹介しているので、運用しているWebサイトにおける脆弱性の有無の確認に役立てていただきたい。また、Webサイトの運用に利用しているアプリケーションがサポート対象となっているかどうか等も確認していただきたい。

前述のとおり、「クロスサイト・スクリプティング」や「SQLインジェクション」といった種類の脆弱性も継続して発見されている。IPAが提供している「安全なウェブサイトの作り方※216」等を参考としながら、構築時にこれらの脆弱性を作り込まないようにすることが基本的な対策となる。

また、ECサイトを主に扱ったものではあるが、IPAは2023年に、Webサイトの構築から運用までについて、経営者やセキュリティ対策を実践する責任者・担当者が認識すべき事項について広くまとめた「EC サイト構築・運用セキュリティガイドライン※217」を公表している。Webサイトの運用管理にあたって、参考としていただきたい。

※1 CSIS：Significant Cyber Incidents https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents〔2024/5/16 確認〕

※2 Microsoft 社：Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/〔2024/5/16 確認〕

※3 Microsoft 社：Analysis of Storm-0558 techniques for unauthorized email access https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/〔2024/5/16 確認〕

※4 Microsoft 社：Results of Major Technical Investigations for Storm-0558 Key Acquisition https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/〔2024/5/16 確認〕

※5 Reuters：中国系ハッカー、米商務長官のメールに侵入＝関係筋 https://jp.reuters.com/article/usa-china-cyber-idJPL6N38Z0GM/〔2024/5/16 確認〕

※6 Microsoft 社：Volt Typhoon targets US critical infrastructure with living-off-the-land techniques https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/〔2024/5/16 確認〕

※7 Palo Alto Networks, Inc.：[2024-02-15 JST 更新] 脅威に関する情報：Volt Typhoon（Unit 42 追跡名 Insidious Taurus）に帰属する重要インフラへの攻撃 https://unit42.paloaltonetworks.jp/volt-typhoon-threat-brief/〔2024/5/16 確認〕

※8 BBC NEWS JAPAN：米FBI、中国支援のハッキングを阻止と報告 主要インフラが標的に https://www.bbc.com/japanese/68163206〔2024/5/16 確認〕

※9 Joint Cybersecurity Advisory：People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF〔2024/5/16 確認〕
CISA：PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a〔2024/5/16 確認〕

※10 Microsoft 社：Espionage fuels global cyberattacks https://blogs.microsoft.com/on-the-issues/2023/10/05/microsoft-digital-defense-report-2023-global-cyberattacks/〔2024/5/16 確認〕

※11 NCSC：The near-term impact of AI on the cyber threat https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat〔2024/5/16 確認〕

※12 https://www.ic3.gov/media/pdf/annualreport/2023_ic3report.pdf〔2024/5/16 確認〕

※13 https://apwg.org/trendsreports/〔2024/5/16 確認〕

※14 Krebs On Security：Sued by Meta, Freenom Halts Domain Registrations https://krebsonsecurity.com/2023/03/sued-by-meta-freenom-halts-domain-registrations/〔2024/5/16 確認〕

※15 APWG：Phishing Activity Trends Report, 4th Quarter 2023 https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf〔2024/5/16 確認〕

※16 FBI：Internet Crime Report 2022 https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf〔2024/5/16 確認〕

※17 IBM 社：IBM X-Force 脅威インテリジェンス・インデックス 2024 https://www.ibm.com/jp-ja/reports/threat-intelligence〔2024/5/16 確認〕

※18 本白書では文献引用上の正確性を期す必要がない場合、表記の統一のため、悪意のあるプログラム、マルウェア等を総称して「ウイルス」と表記する。

※19 Emsisoft Ltd：Unpacking the MOVEit Breach: Statistics and Analysis https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/〔2024/3/22 確認〕

※20 CISA：#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a〔2024/5/16 確認〕

※21 CISA：ESXiArgs Ransomware Virtual Machine Recovery Guidance https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-039a〔2024/5/16 確認〕

※22 CrowdStrike Blog：Hypervisor Jackpotting, Part 3: Lack of Antivirus Support Opens the Door to Adversary Attacks https://www.crowdstrike.com/blog/hypervisor-jackpotting-lack-of-antivirus-support-opens-the-door-to-adversaries/〔2024/5/16 確認〕

※23 マクニカネットワークスブログ：急増中!今猛威を振るうランサムウェアとは? https://mnb.macnica.co.jp/2023/06/aptir/ransomware.html〔2024/5/16 確認〕

※24 警察庁：令和5年におけるサイバー空間をめぐる脅威の情勢等について https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf〔2024/5/16 確認〕

※25 Europol：Law enforcement disrupt world's biggest ransomware operation https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation〔2024/5/16 確認〕

※26 The Register：LockBit extorted $1B+ from victims over four years https://www.theregister.com/2024/02/23/lockbit_extorted_billions_of_dollars/〔2024/5/28 確認〕

※27 IBM 社：2023年「データ侵害のコストに関する調査」 https://www.ibm.com/jp-ja/reports/data-breach〔2024/5/16 確認〕

※28 AT&T Inc.：AT&T Addresses Recent Data Set Released on the Dark Web https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html〔2024/5/16 確認〕

※29 AT&T Inc.：Keeping your account secure https://www.att.

com/support/article/my-account/000101995〔2024/5/16 確認〕
※ 30 TechCrunch：AT&T resets account passcodes after millions of customer records leak online https://techcrunch.com/2024/03/30/att-reset-account-passcodes-customer-data/〔2024/5/16 確認〕
※ 31 Electoral Commission：Public notification of cyber-attack on Electoral Commission systems https://www.electoralcommission.org.uk/privacy-policy/public-notification-cyber-attack-electoral-commission-systems〔2024/5/16 確認〕
※ 32 TechCrunch：Parsing the UK electoral register cyberattack https://techcrunch.com/2023/08/09/parsing-uk-electoral-commission-cyberattack/〔2024/5/16 確認〕
※ 33 GOV.UK：UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity〔2024/5/16 確認〕
※ 34 U.S. Department of the Treasury：Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure https://home.treasury.gov/news/press-releases/jy2205〔2024/5/16 確認〕
※ 35 Bleeping Computer：MGM casino's ESXi servers allegedly encrypted in ransomware attack https://www.bleepingcomputer.com/news/security/mgm-casinos-esxi-servers-allegedly-encrypted-in-ransomware-attack/〔2024/5/16 確認〕
※ 36 Okta 社：Cross-Tenant Impersonation: Prevention and Detection https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection〔2024/5/16 確認〕
※ 37 Okta 社：Okta October 2023 Security Incident Investigation Closure https://sec.okta.com/harfiles〔2024/5/16 確認〕
※ 38 https://www.antiphishing.jp/report/monthly/〔2024/5/21 確認〕
※ 39 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf〔2024/5/21 確認〕
※ 40-1 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf〔2024/5/21 確認〕
※ 40-2 https://www.jpcert.or.jp/pr/2024/IR_Report2023Q4.pdf〔2024/5/21 確認〕
※ 40-3 フィッシング対策協議会：URL に飾り文字などが含まれたフィッシング（2023/10/17） https://www.antiphishing.jp/news/alert/decourl_20231017.html〔2024/5/21 確認〕
※ 40-4 フィッシング対策協議会：URL に特殊な IP アドレス表記を用いたフィッシング（2023/11/14） https://www.antiphishing.jp/news/alert/ipurl_20231114.html〔2024/5/21 確認〕
※ 40-5 フィッシング対策協議会：2023/10 フィッシング報告状況 https://www.antiphishing.jp/report/monthly/202310.html〔2024/5/21 確認〕
※ 40-6 フィッシング対策協議会：総務省をかたるフィッシング（2023/04/05） https://www.antiphishing.jp/news/alert/mic_20230405.html〔2024/5/21 確認〕
フィッシング対策協議会：三井住友信託銀行をかたるフィッシング（2023/04/10） https://www.antiphishing.jp/news/alert/smtb_20230410.html〔2024/5/21 確認〕
フィッシング対策協議会：国土交通省をかたるフィッシング（2023/04/25） https://www.antiphishing.jp/news/alert/mlit_20230425.html〔2024/5/21 確認〕
フィッシング対策協議会：Apple をかたるフィッシング（2023/05/02） https://www.antiphishing.jp/news/alert/apple_20230502.html〔2024/5/21 確認〕
※ 40-7 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況〔2023 年 7 月～ 9 月〕 https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q2-report.pdf〔2024/5/21 確認〕
※ 40-8 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〔2024/5/21 確認〕
※ 40-9 株式会社 NTT マーケティングアクト ProCX、NTT ビジネスソリューションズ株式会社：NTTビジネスソリューションズに派遣された元派遣社員によるお客さま情報の不正流出について（続報） https://www.nttactprocx.com/info/detail/231219.html〔2024/5/21 確認〕
ITmedia：NTT 西子会社の内部不正、追加で 28 万件の持ち出し明らかに 社内調査で 計 928 万件に https://www.itmedia.co.jp/news/articles/2312/19/news176.html〔2024/5/21 確認〕
※ 40-10 株式会社 NTT ドコモ：【お詫び】「ぷらら」および「ひかり TV」をご利用のお客さま情報流出のお知らせとお詫び https://www.docomo.ne.jp/info/notice/page/230721_00_m.html〔2024/5/21 確認〕
※ 40-11 https://www.ipa.go.jp/security/10threats/10threats2024.html〔2024/5/21 確認〕
※ 40-12 https://www.npa.go.jp/publications/statistics/safetylife/seikeikan/R05_nenpou.pdf〔2024/5/21 確認〕
※ 40-13 JPCERT/CC：JPCERT/CC インシデント報告対応レポート 2023 年 1 月 1 日～ 2023 年 3 月 31 日 https://www.jpcert.or.jp/pr/2023/IR_Report2022Q4.pdf〔2024/5/21 確認〕
※ 41 日経クロステック：警察庁命名のサイバー攻撃の新手口「ノーウエアランサム」、SNS で大喜利始まる https://xtech.nikkei.com/atcl/nxt/column/18/00001/08492/〔2024/4/12 確認〕
※ 42 警察庁：令和5年におけるサイバー空間をめぐる脅威の情勢等について https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf〔2024/4/12 確認〕
※ 43 トレンドマイクロ社：2023 年、サプライチェーンにおけるセキュリティリスク動向～被害事例にみる企業が直面するリスクとは? https://www.trendmicro.com/ja_jp/jp-security/23/k/securitytrend-20231113-01.html〔2024/4/12 確認〕
※ 44 wiz LANSCOPE：ノーウェアランサムとは?新種のランサムウェア手口と対策について最新情報を解説 https://www.lanscope.jp/blogs/cyber_attack_cpdi_blog/20231026_15683/〔2024/4/12 確認〕
※ 45 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〔2024/4/12 確認〕
※ 46 IPA：コンピュータウイルス・不正アクセスの届出事例〔2023 年上半期（1月～6月）〕 https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/2023-h1-jirei.pdf〔2024/4/12 確認〕
IPA：コンピュータウイルス・不正アクセスの届出事例〔2023 年下半期（7月～ 12 月）〕 https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/2023-h2-jirei.pdf〔2024/4/12 確認〕
※ 47 名古屋港運協会、名古屋港コンテナ委員会、ターミナル部会：名古屋港統一ターミナルシステムのシステム障害について https://meikoukyo.com/wp-content/uploads/2023/07/165c5b14bf0021d077a4852f0cb232b8.pdf〔2024/4/12 確認〕
※ 48 名古屋港運協会、名古屋港コンテナ委員会、ターミナル部会：NUTS システム障害の経緯報告 https://meikoukyo.com/wp-content/uploads/2023/07/0bb9d9907568e832da8f400e529efc99.pdf〔2024/4/12 確認〕
※ 49 コンテナターミナルにおける情報セキュリティ対策等検討委員会：名古屋港のコンテナターミナルにおけるシステム障害を踏まえ緊急に実施すべき対応策及び情報セキュリティ対策等の推進のための制度的措置について https://www.mlit.go.jp/kowan/content/001719866.pdf〔2024/4/12 確認〕
※ 50 トレンドマイクロ社：ランサムウェア「LockBit」の概要と対策～名古屋港の活動停止を引き起こした犯罪集団 https://www.trendmicro.com/ja_jp/jp-security/23/h/securitytrend-20230823-01.html〔2024/4/12 確認〕
※ 51 日経クロステック：国際サイバー犯罪集団「ロックビット」摘発、メンバー2人を逮捕 https://xtech.nikkei.com/atcl/nxt/news/24/00289/〔2024/4/12 確認〕
※ 52-1 Codebook：LockBit ランサムウェアが復活、新リークサイトに 5 つの被害組織を掲載 https://codebook.machinarecord.com/threatreport/32128/〔2024/4/12 確認〕
BleepingComputer：LockBit ransomware returns, restores servers after police disruption https://www.bleepingcomputer.com/news/security/lockbit-ransomware-returns-restores-servers-after-police-disruption/〔2024/4/12 確認〕
※ 52-2 NISC：サイバーセキュリティ戦略本部第 39 回会合の開催について https://www.nisc.go.jp/pdf/council/cs/dai39/39cs_press.pdf〔2024/6/21 確認〕
※ 52-3 国土交通省：コンテナターミナルにおける情報セキュリティ対策等について https://www.mlit.go.jp/policy/shingikai/content/001727807.pdf〔2024/4/12 確認〕
※ 53 エムケイシステム社：【お詫び】弊社製品障害に関するご報告 https://www.mks.jp/company/topics/20230605〔2024/4/12 確認〕
※ 54 エムケイシステム社：第三者によるランサムウェア感染被害のお知らせ https://contents.xj-storage.jp/xcontents/AS97180/bc464498/fb3c/479a/ad33/51ec0cd39818/140120230606596742.pdf〔2024/4/12 確認〕
※ 55 エムケイシステム社：当社サーバへの不正アクセスに関する調査結果のご報告（第3報） https://contents.xj-storage.jp/xcontents/AS97180/813d570f/5138/4bc7/a113/f4837598df38/140120230719524126.pdf〔2024/4/12 確認〕
※ 56 日本経済新聞：「社労夢」のエムケイシステム、社労士クラウド障害

を謝罪　https://www.nikkei.com/article/DGXZQOUF074GH0X00C23A9000000/〔2024/4/12 確認〕
※ 57 Security NEXT：人事労務システム障害、給与システムを順次提供 - MK システム　https://www.security-next.com/146843〔2024/4/12 確認〕
※ 58 Security NEXT：「社労夢」の復旧、6 月末から 7 月上旬を予定 - MK システム　https://www.security-next.com/147265〔2024/4/12 確認〕
※ 59 ITmedia NEWS：ランサムウェアで約 1カ月停止の社労士向けクラウド、サービスを一部再開　開発中の AWS 版を急きょ改修　https://www.itmedia.co.jp/news/articles/2307/05/news144.html〔2024/4/12 確認〕
※ 60 日経クロステック：番外編：ランサムウエア攻撃が憎い、顧客の給与支給が間に合うか窮地に立たされる　https://xtech.nikkei.com/atcl/nxt/column/18/00084/00270〔2024/4/12 確認〕
※ 61 個人情報保護委員会：株式会社エムケイシステムに対する個人情報の保護に関する法律に基づく行政上の対応について　https://www.ppc.go.jp/files/pdf/240325_houdou.pdf〔2024/4/12 確認〕
※ 62 個人情報保護委員会：クラウドサービス提供事業者が個人情報保護法上の個人情報取扱事業者に該当する場合の留意点について（注意喚起）　https://www.ppc.go.jp/files/pdf/240325_alert_cloud_service_provider.pdf〔2024/4/12 確認〕
※ 63 株式会社 Y4.com：不正アクセスによる情報漏えいのお知らせとお詫び　https://y-4.jp/wp-content/uploads/2023/12/jyoho1218.pdf〔2024/4/12 確認〕
※ 64 株式会社 Y4.com：不正アクセスによる情報漏えいに関するお詫びとご報告（最終）　https://y-4.jp/wp-content/uploads/2024/01/jyohoroei0122.pdf〔2024/4/12 確認〕
※ 65 千葉市：委託事業者による個人情報の流出した可能性のある事案の発生について　https://www.city.chiba.jp/hokenfukushi/kenkofukushi/shien/hokensidouosirase.html〔2024/4/12 確認〕
伊丹市：委託事業者による個人情報の流出事案の発生について　https://www.city.itami.lg.jp/SOSIKI/KENKOFUKUSHI/KENKO_SEISAKU/37560.html〔2024/4/12 確認〕
※ 66 JPCERT/CC：侵入型ランサムウェア攻撃を受けたら読む FAQ　https://www.jpcert.or.jp/magazine/security/ransom-faq.html〔2024/4/12 確認〕
※ 67 https://www.ipa.go.jp/publish/wp-security/2023.html〔2024/4/12 確認〕
※ 68 C&C（Command and Control）サーバー:ウイルス等により乗っ取ったコンピューター等に対し、遠隔から命令を送り制御させるサーバー。
※ 69 IPA：サイバーレスキュー隊（J-CRAT）活動状況［2020 年度上半期］　https://www.ipa.go.jp/security/j-crat/ug65p9000000nks8-att/000086892.pdf〔2024/4/12 確認〕
※ 70 IPA：インターネット境界に設置された装置に対するサイバー攻撃について～ネットワーク貫通型攻撃に注意しましょう～　https://www.ipa.go.jp/security/security-alert/2023/alert20230801.html〔2024/4/12 確認〕
※ 71 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〔2024/4/12 確認〕
※ 72 伊藤忠サイバー&インテリジェンス株式会社：熱帯の海賊からの贈り物 - メールとマルウェアに隠された新しい危険な武器 - https://blog.itochuci.co.jp/entry/2023/09/27/105758〔2024/4/12 確認〕
※ 73 DLL Side-Loading：Windows の DLL 検索順序メカニズム (最初に実行されたプログラムと同じフォルダにある DLL を探索する仕様) を悪用し、悪意ある DLL を読み込ませる手法。このとき、プログラム側が読み込む DLL の正当性を確認する処理を行わない場合、悪意あるコードが実行されてしまう。また、DLL Side-Loading により読み込まれた悪意あるコード（ウイルス）は、正規のプログラムを介して実行されるため、セキュリティ対策ソフト等で検知されにくくなる特徴を持つ。
※ 74 Cobalt Strike Beacon：Fortra, LLC の正規のセキュリティツールである、Cobalt Strike を使用するためのエージェントプログラム（Cobalt Strike Beacon）である。本来は、セキュリティツールとして有益な機能を、多くの攻撃者グループが悪用している。
※ 75 JPCERT/CC：日本の組織を標的にした外部からアクセス可能な IT 資産を狙う複数の標的型サイバー攻撃活動に関する注意喚起　https://www.jpcert.or.jp/at/2023/at230029.html〔2024/4/12 確認〕
※ 76 国立研究開発法人国立環境研究所：国立環境研究所が運用するオンラインストレージサービス（Proself）への不正アクセスについて　https://www.nies.go.jp/whatsnew/2023/20231030-1.html〔2024/4/12 確認〕
※ 77 トレンドマイクロ社：Spot the Difference: An Analysis of the New LODEINFO Campaign by Earth Kasha　https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_2_7_hara_shoji_higashi_vickie-su_nick-dai_en.pdf〔2024/4/12 確認〕
※ 78 Cisco 社：Reports about Cyber Actors Hiding in Router Firmware https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csa-cyber-report-sept-2023〔2024/4/12 確認〕
※ 79 警察庁、NISC：中国を背景とするサイバー攻撃グループ BlackTech 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/20230927press.pdf〔2024/4/12 確認〕
※ 80 Mandiant, Inc.：中国との関連が疑われる攻撃的、かつ高度なスキルを持つ攻撃者が Barracuda ESG のゼロデイ脆弱性（CVE-2023-2868）を悪用　https://www.mandiant.jp/resources/blog/barracuda-esg-exploited-globally〔2024/4/12 確認〕
※ 81 Mandiant, Inc.：Barracuda ESG のゼロデイ修復（CVE-2023-2868）後の UNC4841 の活動についてのさらなる考察　https://www.mandiant.jp/resources/blog/unc4841-post-barracuda-zero-day-remediation〔2024/4/12 確認〕
※ 82 Microsoft 社：マイクロソフトは、顧客の電子メールを標的とした中国を拠点とする脅威アクター Storm-0558 を緩和しました。　https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email-ja/〔2024/4/12 確認〕
※ 83 Mandiant, Inc.：The Spies Who Loved You: Infected USB Drives to Steal Secrets　https://www.mandiant.com/resources/blog/infected-usb-steal-secrets〔2024/4/12 確認〕
チェック・ポイント・ソフトウェア・テクノロジーズ株式会社：チェック・ポイント・リサーチ、USB 機器を介して増殖する中国の諜報活動用マルウェアの新バージョンを発見　https://prtimes.jp/main/html/rd/p/000000218.000021207.html〔2024/4/12 確認〕
※ 84 サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会：サイバー攻撃被害に係る情報の共有・公表ガイダンス　https://www.meti.go.jp/press/2022/03/20230308006/20230308006-2.pdf〔2024/4/12 確認〕
※ 85 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〔2024/4/12 確認〕
※ 86 ファイルレスマルウェア：ウイルス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・動作するタイプのウイルスのこと。
※ 87 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〔2024/4/12 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〔2024/4/12 確認〕
※ 88 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〔2024/4/12 確認〕
※ 89 被害金額については、2015 ～ 2023 年の年次報告書（IC3：Annual Reports　https://www.ic3.gov/Home/AnnualReports〔2024/4/12 確認〕）を参照した。
※ 90 Security Affairs：Law enforcement Operation HAECHI IV led to the seizure of $300 Million　https://securityaffairs.com/156209/cyber-crime/haechi-iv-operation-interpol.html〔2024/4/12 確認〕
INTERPOL：USD 300 million seized and 3,500 suspects arrested in international financial crime operation　https://www.interpol.int/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation〔2024/4/12 確認〕
※ 91 The Register：Interpol arrests 14 who allegedly scammed $40m from victims in 'cyber surge'　https://www.theregister.com/2023/08/20/interpol_africa_arrests/〔2024/4/12 確認〕
INTERPOL：Cybercrime：14 arrests, thousands of illicit cyber networks disrupted in Africa operation　https://www.interpol.int/en/News-and-Events/News/2023/Cybercrime-14-arrests-thousands-of-illicit-cyber-networks-disrupted-in-Africa-operation〔2024/4/12 確認〕
※ 92 株式会社 NHK メディアホールディングス、株式会社 NHK プロモーション：送金詐欺被害が疑われる事案の発生について　https://www.nhk.or.jp/keiei-iinkai/giji/shiryou/1430_kaicho01.pdf〔2024/4/12 確認〕
※ 93 株式会社スリー・ディー・マトリックス：送金詐欺による資金流出被害のお知らせ　https://pdf.irpocket.com/C7777/ZoWa/awjA/EOHM.pdf〔2024/4/12 確認〕
株式会社スリー・ディー・マトリックス：営業外収益、営業外費用及び特

別損失の計上並びに役員報酬の一部自主返納に関するお知らせ https://pdf.irpocket.com/C7777/nGVW/npNB/aTkn.pdf〔2024/4/12 確認〕
※ 94 Fort Lauderdale Police Department：FLPD RECOVERS APPROXIMATELY $1.2M TAKEN IN A CONSTRUCTION FRAUD SCHEME https://www.flpd.gov/home/showpublisheddocument/6914〔2024/4/12 確認〕
WSVN 7News：City of Fort Lauderdale falls victim to $1.2 million fraud scheme https://wsvn.com/news/local/broward/city-of-fort-lauderdale-falls-victim-to-1-2-million-fraud-scheme/〔2024/4/12 確認〕
※ 95 CNN：Finance worker pays out $25 million after video call with deepfake 'chief financial officer' https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html〔2024/4/12 確認〕
※ 96 IPA：ビジネスメール詐欺（BEC）対策特設ページ https://www.ipa.go.jp/security/bec/about.html〔2024/4/12 確認〕
※ 97 https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q1-report.pdf〔2024/4/12 確認〕
※ 98 https://www.ipa.go.jp/security/bec/hjuojm0000003c8r-att/case6.pdf〔2024/4/12 確認〕
※ 99 IPA：ビジネスメール詐欺のパターンとは https://www.ipa.go.jp/security/bec/bec_pattern.html〔2024/4/12 確認〕
※ 100 ZDNET Japan：CEO になりすましたディープフェイクの音声で約2600 万円の詐欺被害か https://japan.zdnet.com/article/35142255/〔2024/4/12 確認〕
※ 101 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況〔2019年10月～12月〕 https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000080133.pdf〔2024/4/12 確認〕
※ 102 Fortra, LLC：Cosmic Lynx: A Russian Threat Hits the BEC Scene https://www.agari.com/blog/cosmic-lynx-russian-bec〔2024/4/12 確認〕
※ 103 JPCERT/CC：ビジネスメール詐欺の実態調査報告 https://www.jpcert.or.jp/research/BEC-survey.html〔2024/4/12 確認〕
株式会社マクニカ：ビジネスメール詐欺の実態と対策アプローチ 第1版 https://www.macnica.co.jp/business/security/security-reports/141698/〔2024/4/12 確認〕
PwC：Business-Email-Compromise-Guide (BEC) https://github.com/PwC-IR/Business-Email-Compromise-Guide/blob/main/PwC-Business_Email_Compromise-Guide.pdf〔2024/4/12 確認〕
※ 104 IPA：ビジネスメール詐欺（BEC）の特徴と対策 https://www.ipa.go.jp/security/bec/hjuojm00000037nn-att/000102392.pdf〔2024/4/12 確認〕
※ 105 Microsoft 社：From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/〔2024/4/12 確認〕
Microsoft 社：Detecting and mitigating a multi-stage AiTM phishing and BEC campaign https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/〔2024/4/12 確認〕
※ 106 Microsoft 社：侵害されたメールアカウントへの応答 https://learn.microsoft.com/ja-jp/defender-office-365/responding-to-a-compromised-email-account?view=o365-worldwide〔2024/4/12 確認〕
※ 107 NetScout Systems, Inc.：Internet Traffic and Slipstreamed Threats - Latest Cyber Threat Intelligence Report https://www.netscout.com/threatreport/internet-traffic-slipstreamed-threats/〔2024/4/12 確認〕
※ 108 NHK：あなたはなぜ「参戦」するのか?ウクライナ侵攻でサイバー攻撃に手を染める市民たち https://www3.nhk.or.jp/news/special/sci_cul/2022/07/special/cyber-hacker-ukraine-0728/〔2024/4/12 確認〕
※ 109 NetScout Systems, Inc.：NETSCOUT Identified Nearly 7.9 Million DDoS Attacks in 1H2023 According to Its Latest DDoS Threat Intelligence Report https://www.netscout.com/press-releases/netscout-identified-nearly-79-million-ddos-attacks-1h2023〔2024/4/12 確認〕
※ 110 UDP（User Datagram Protocol）：インターネットで標準的に使われているプロトコルの一種。接続のチェックが不要なコネクションレスなサービスに利用される。
※ 111 Cloudflare, Inc.：2023 年第 4 四半期 DDoS 脅威レポート https://blog.cloudflare.com/ja-jp/ddos-threat-report-2023-q4-ja-jp/〔2024/4/12 確認〕
※ 112 BitSight Technologies, Inc.：New high-severity vulnerability（CVE-2023-29552）discovered in the Service Location Protocol（SLP） https://www.bitsight.com/blog/new-high-severity-vulnerability-cve-2023-29552-discovered-service-location-protocol-slp〔2024/4/12 確認〕
※ 113 Security NEXT：「SLP」に反射攻撃のおそれ、早急にアクセス制限を - 最大 2200 倍に増幅 https://www.security-next.com/145722〔2024/4/12 確認〕
※ 114 CISA：Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2023-29552&field_date_added_wrapper=all&sort_by=field_date_added&items_per_page=20〔2024/4/12 確認〕
Security NEXT：米当局、「SLP」や「Atlassian Confluence」狙う脆弱性攻撃に注意喚起 https://www.security-next.com/150961〔2024/4/12 確認〕
※ 115 NetScout Systems, Inc.：Revealing Adversary Methodology - Latest Cyber Threat Intelligence Report https://www.netscout.com/threatreport/revealing-adversary-methodology/〔2024/4/12 確認〕
※ 116 株式会社日本レジストリサービス：JPRS トピックス＆コラム（No.021）Bot 経由で DNS サーバーを広く薄く攻撃～ DNS 水責め攻撃の概要と対策～ https://jprs.jp/related-info/guide/021.pdf〔2024/4/12 確認〕
株式会社日本レジストリサービス：[Interop Tokyo 2023 出展報告] 権威 DNS サーバーを狙った攻撃の影響範囲と可用性を高めるためのポイント～ランダムサブドメイン攻撃を題材として～ https://jprs.jp/related-info/event/2023/InteropTokyo-02.html〔2024/4/12 確認〕
GMO インターネットグループ株式会社：ランダムサブドメイン攻撃についてドメイン名登録者が出来ること https://dnsops.jp/event/20230623/20230623-nagai.pdf〔2024/4/12 確認〕
※ 117 ボットネット：攻撃者に乗っ取られた複数の機器から形成されるネットワーク。
※ 118 オープンリゾルバー：外部の不特定の IP アドレスからの再帰的な問い合わせを許可している DNS サーバー。
※ 119 権威 DNS サーバー：あるゾーンの情報を保持し、他のサーバーに問い合わせることなく応答を返すことができるサーバー。
※ 120 株式会社日本レジストリサービス：ランダムサブドメイン攻撃（DNS 水責め攻撃） https://jprs.jp/glossary/index.php?ID=0137〔2024/4/12 確認〕
※ 121 Akamai Technologies, Inc.：金融・公共部門における DDoS 攻撃トレンドと対策ソリューション https://www.akamai.com/ja/blog/security/ddos-attack-2023-fsipub〔2024/4/12 確認〕
※ 122 警察庁：令和5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/R05_kami_cyber_jousei.pdf〔2024/4/12 確認〕
※ 123 警察庁：DDoS 攻撃への対策について https://www.npa.go.jp/bureau/cyber/koho/caution/caution20230501.html〔2024/4/12 確認〕
警察庁、NISC：DDoS 攻撃への対策について https://www.npa.go.jp/bureau/cyber/pdf/20230501.pdf〔2024/4/12 確認〕
※ 124 Cloud Software Group, Inc.：NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967 https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967〔2024/4/12 確認〕
※ 125 AAA:Authentication（認証）、Authorization（認可）、Accounting（課金）の略。
※ 126 Mandiant, Inc.：Remediation for Citrix NetScaler ADC and Gateway Vulnerability (CVE-2023-4966) https://www.mandiant.com/resources/blog/remediation-netscaler-adc-gateway-cve-2023-4966〔2024/4/12 確認〕
※ 127 Cloud Software Group, Inc.：NetScaler investigation recommendations for CVE-2023-4966 https://www.netscaler.com/blog/news/netscaler-investigation-recommendations-for-cve-2023-4966/〔2024/4/12 確認〕
※ 128 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。不正侵入やウイルス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。
※ 129 Mandiant, Inc.：Investigation of Session Hijacking via Citrix NetScaler ADC and Gateway Vulnerability (CVE-2023-4966) https://www.mandiant.com/resources/blog/session-hijacking-citrix-cve-2023-4966〔2024/4/12 確認〕
※ 130 ITmedia エンタープライズ：CitrixBleed は消えない サイバー攻撃者に利用される悪質な脆弱性についてまとめた https://www.itmedia.co.jp/enterprise/articles/2401/20/news021.html〔2024/4/12 確認〕

※ 131 CISA：#StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a〔2024/4/12 確認〕
※ 132 Microsoft 社：Windows Search のリモートでコードが実行される脆弱性 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884〔2024/4/12 確認〕
※ 133 Microsoft 社：Windows Mark Of The Web セキュリティ機能のバイパスの脆弱性 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36584〔2024/4/12 確認〕
※ 134 Palo Alto Networks, Inc.：CVE-2023-36884、CVE-2023-36584 を悪用する 2023 年 7 月のエクスプロイトチェーンの詳解 https://unit42.paloaltonetworks.jp/new-cve-2023-36584-discovered-in-attack-chain-used-by-russian-apt/〔2024/4/12 確認〕
※ 135 サイバーリーズン合同会社：【脅威分析レポート】CVE-2023-36884 - Windows Search のゼロデイ脆弱性 https://www.cybereason.co.jp/blog/threat-analysis-report/11012/〔2024/4/12 確認〕
Security NEXT：「Office」のゼロデイ脆弱性、ロシア攻撃グループが悪用 https://www.security-next.com/147778〔2024/4/12 確認〕
※ 136 Progress Software 社：MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362) https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023〔2024/4/12 確認〕
※ 137 Mandiant, Inc.：Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft〔2024/4/12 確認〕
※ 138 Palo Alto Networks, Inc.：脅威に関する情報：MOVEit Transfer の SQL インジェクションの脆弱性 (CVE-2023-34362、CVE-2023-35036、CVE-2023-35708) https://unit42.paloaltonetworks.jp/threat-brief-moveit-cve-2023-34362/〔2024/4/12 確認〕
※ 139 日経クロステック：MOVEit の脆弱性を突いた情報窃取で英シェルなどを脅迫、日本企業への影響は https://xtech.nikkei.com/atcl/nxt/column/18/00001/08139/〔2024/4/12 確認〕
※ 140 Security NEXT：「MOVEit Transfer」にゼロデイ脆弱性 - 侵害状況も確認を https://www.security-next.com/146673.html〔2024/4/12 確認〕
Reuters：US energy department, other agencies hit in global hacking spree https://www.reuters.com/world/us/us-government-agencies-hit-global-cyber-attack-cnn-2023-06-15/〔2024/4/12 確認〕
Bleeping Computer：Sony confirms data breach impacting thousands in the U.S. https://www.bleepingcomputer.com/news/security/sony-confirms-data-breach-impacting-thousands-in-the-us/〔2024/4/12 確認〕
Emsisoft Ltd：Unpacking the MOVEit Breach: Statistics and Analysis https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/〔2024/3/22 確認〕
※ 141 Progress Software 社：MOVEit Transfer Critical Vulnerability - CVE-2023-35036 (June 9, 2023) https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-CVE-2023-35036-June-9-2023〔2024/4/12 確認〕
※ 142 Progress Software 社：MOVEit Transfer Critical Vulnerability - CVE-2023-35708（June 15, 2023） https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023〔2024/4/12 確認〕
※ 143 株式会社ノースグリッド：[至急] Proself の脆弱性（CVE-2023-39415、CVE-2023-39416）による攻撃発生について（更新） https://www.proself.jp/information/149/〔2024/4/12 確認〕
※ 144 株式会社ノースグリッド：[至急] Proself のゼロデイ脆弱性（CVE-2023-45727）による攻撃発生について（更新） https://www.proself.jp/information/153/〔2024/4/12 確認〕
※ 145 日経クロステック：日本学術振興会が 8 月に続き 11 月も個人情報漏洩を発表、Proself の脆弱性悪用される https://xtech.nikkei.com/atcl/nxt/column/18/00598/100500243/〔2024/4/12 確認〕
※ 146 https://www.ipa.go.jp/security/security-alert/2023/alert20231019.html〔2024/4/12 確認〕
※ 147 総務省：令和4年通信利用動向調査の結果 https://www.soumu.go.jp/johotsusintokei/statistics/data/230529_1.pdf〔2024/4/12 確認〕
※ 148 フィッシング対策協議会：2023/12 フィッシング報告状況 https://www.antiphishing.jp/report/monthly/202312.html〔2024/4/12 確認〕
※ 149 金融庁：フィッシングによるものとみられるインターネットバンキングによる預金の不正送金被害が急増しています。 https://www.fsa.go.jp/ordinary/internet-bank_2.html〔2024/4/12 確認〕
※ 150 警察庁、金融庁：フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起） https://www.npa.go.jp/bureau/cyber/pdf/20231225_press.pdf〔2024/4/12 確認〕
※ 151 株式会社三菱UFJ銀行：三菱UFJダイレクトのセキュリティ対策 https://direct.bk.mufg.jp/secure/index.html?link_id=direct_top_security〔2024/4/12 確認〕
※ 152 https://www.ipa.go.jp/publish/wp-security/qv6pgp0000000vcv-att/000094186.pdf〔2024/4/12 確認〕
※ 153 政府広報オンライン：マイナポイント第 2 弾! ポイント申込期限は 2023 年 9 月末まで! https://www.gov-online.go.jp/useful/article/202206/2.html〔2024/4/12 確認〕
※ 154 JC3：悪質なショッピングサイト等に関する統計情報（2023 年上半期） https://www.jc3.or.jp/threats/topics/article-515.html〔2024/4/12 確認〕
※ 155 IPA：偽のセキュリティ警告に表示された番号に電話をかけないで https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20211116.html〔2024/4/12 確認〕
※ 156 長野県警察：電話でお金詐欺（特殊詐欺）等被害の発生（飯山署） https://www.pref.nagano.lg.jp/police/news24/2312/14.html〔2024/4/12 確認〕
※ 157 国民生活センター：パソコンで警告が出たらサポート詐欺に注意! https://www.kokusen.go.jp/pdf/n-20240327_1.pdf〔2024/4/12 確認〕
※ 158 総務省：携帯電話の犯罪利用の防止 関係資料 https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/050526_1.files/Page377.html〔2024/4/12 確認〕
※ 159 IPA：会社や組織のパソコンにセキュリティ警告が出たら、管理者に連絡! https://www.ipa.go.jp/security/anshin/attention/2023/mgdayori20230711.html〔2024/4/12 確認〕
※ 160 IPA：情報セキュリティ安心相談窓口の相談状況［2023 年第 4 四半期（10 月～ 12 月）］ https://www.ipa.go.jp/security/anshin/reports/2023q4outline.html〔2024/4/12 確認〕
※ 161 IPA：サポート詐欺で表示される偽のセキュリティ警告画面の閉じ方 https://www.ipa.go.jp/security/anshin/doe3um0000005cag-att/20231115173500.pdf〔2024/4/12 確認〕
※ 162 「見て、聞いて、話そう!交流フェスタ 2023」は、消費者意識の啓発、消費者団体相互の連携強化、消費者・事業者・行政の協働の推進を目的として東京都と消費者団体が協働して行う「くらしフェスタ東京 2023」のイベントの一つとして、2023 年 10 月 22 ～ 23 日の期間に、新宿駅西口広場イベントコーナーで開催された。
東京都消費者月間実行委員会：くらしフェスタ東京 2023 https://kurashifesta-tokyo.org/2023/festa/〔2024/4/12 確認〕
※ 163 IPA：偽セキュリティ警告（サポート詐欺）画面の閉じ方体験サイト https://www.ipa.go.jp/security/anshin/measures/fakealert.html〔2024/4/12 確認〕
※ 164 自動継続課金：ここでは「一定の利用期間ごとに定額を支払う料金方式、かつ、利用契約が自動更新される方式」を指す。なお、「一定の利用期間ごとに定額を支払う料金方式」は、Android では「定期購入」、iPhone では「サブスクリプション」と呼ばれる。
※ 165 IPA：スマートフォンの偽セキュリティ警告から自動継続課金アプリのインストールへ誘導する手口にあらためて注意! https://www.ipa.go.jp/security/anshin/attention/2022/mgdayori20221025.html〔2024/4/12 確認〕
※ 166 IPA：ブラウザの通知機能から不審サイトに誘導する手口に注意 https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210309.html〔2024/4/12 確認〕
※ 167 reCAPTCHA v2：reCAPTCHA とは、アクセスしているのが機械でなく人間であることの判別をするための認証機能。reCAPTCHA v2 は Google が提供する CAPTCHA（キャプチャ）認証システムの名称。
※ 168 国民生活センター：20 歳代が狙われている!?遠隔操作アプリを悪用して借金をさせる副業や投資の勧誘に注意 https://www.kokusen.go.jp/news/data/n-20230607_1.html〔2024/4/12 確認〕
※ 169 国民生活センター：【新手の詐欺】「○○ペイで返金します」に注意! ーネットショッピング代金を返金するふりをして、送金させる手口ー https://www.kokusen.go.jp/news/data/n-20230927_2.html〔2024/4/12 確認〕
※ 170 株式会社ラック:LAC Security Insight 第2号 2022秋 ー 特集:偽ショッピングサイト誘導の調査 https://www.lac.co.jp/lacwatch/report/20221214_003222.html〔2024/4/12 確認〕
※ 171 IPA：遠隔操作ソフト（アプリ）を悪用される手口に気をつけて! https://www.ipa.go.jp/security/anshin/attention/2023/mgdayori20230411.html〔2024/4/12 確認〕
※ 172 東京商工リサーチ社：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〔2024/4/12 確認〕
※ 173 東京商工リサーチ社：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〔2024/4/12 確認〕
※ 174 JCOM 株式会社：お客さまの個人情報漏えいに関するお知らせとお詫び https://newsreleases.jcom.co.jp/news/20231122_9239.html〔2024/4/12 確認〕
※ 175 LINE ヤフー株式会社：不正アクセスによる、情報漏えいに関するお知らせとお詫び（2024/2/14 更新） https://www.lycorp.co.jp/ja/news/announcements/007712/〔2024/4/12 確認〕
※ 176 https://www.privacymark.jp/guideline/wakaru/g7ccig0000002vj1-att/2022JikoHoukoku_230802.pdf〔2024/06/19 確認〕
※ 177 https://privacymark.jp/news/2022/other/g7ccig0000001e7p-att/2021JikoHoukoku_221007.pdf〔2024/06/19 確認〕
※ 178 一つの発生事象に対して複数の原因が報告される場合があるため、事故報告件数を上回る件数になっている。
※ 179 ひまわりネットワーク株式会社：当社システムの機能停止による豊田市が送信した電子メールアドレスの流出について（完報） https://www.himawari.co.jp/corporate/company_info/ct2197/〔2024/4/12 確認〕
※ 180 株式会社出前館：【続報】アカウント連携システム不備による『出前館』アカウント情報閲覧の恐れに関するお詫びとお知らせ https://corporate.demae-can.co.jp/pr/info/20230623.html〔2024/4/12 確認〕
ITmedia NEWS：出前館で他人のログイン情報が表示されるバグ キャッシュ削除処理に不備 924 万人が対象 https://www.itmedia.co.jp/news/articles/2306/26/news178.html〔2024/4/12 確認〕
※ 181 九州電力株式会社：お客さまの個人情報の漏えいに関するお知らせとお詫びについて https://www.kyuden.co.jp/notice_231220.html〔2024/4/12 確認〕
読売新聞オンライン：九州電力の顧客情報290万件が子会社で閲覧可能な状態に…設定誤り、政府委員会に報告 https://www.yomiuri.co.jp/local/kyushu/news/20231130-OYTNT50032/〔2024/4/12 確認〕
※ 182 トヨタ自動車株式会社：クラウド環境の誤設定によるお客様情報の漏洩可能性に関するお詫びとお知らせについて https://global.toyota/jp/newsroom/corporate/39174380.html〔2024/4/12 確認〕
個人情報保護委員会：トヨタ自動車株式会社による個人データの漏えい等事案に対する個人情報の保護に関する法律に基づく行政上の対応について https://www.ppc.go.jp/files/pdf/230712_01_houdou.pdf〔2024/5/23 確認〕
※ 183 株式会社エイチーム：個人情報漏えいの可能性に関するお知らせ https://www.a-tm.co.jp/news/43858/〔2024/4/12 確認〕
株式会社エイチーム：個人情報漏えいの可能性に関するご報告とお詫び https://www.a-tm.co.jp/news/44238/〔2024/5/2 確認〕
※ 184 国立研究開発法人産業技術総合研究所：職員の逮捕について https://www.aist.go.jp/aist_j/news/announce/au20230615.html〔2024/4/12 確認〕
※ 185 読売新聞オンライン：中国企業に先端技術情報を漏えいした疑い、産総研の中国籍研究員を逮捕 https://www.yomiuri.co.jp/national/20230615-OYT1T50179/〔2024/4/12 確認〕
※ 186 日本山村硝子株式会社：当社元社員の逮捕について https://www.yamamura.co.jp/cms/wp-content/uploads/2023/10/20231005_CMS0289.pdf〔2024/4/12 確認〕
※ 187 株式会社 NTT ドコモ：【お詫び】「ぷらら」および「ひかり TV」をご利用のお客さま情報流出のお知らせとお詫び https://www.docomo.ne.jp/info/notice/page/230721_00_m.html〔2024/4/12 確認〕
※ 188 NTT 西日本、ProCX 社、BS 社：お客さま情報の不正持ち出しを踏まえた NTT 西日本グループの情報セキュリティ強化に向けた取組みについて https://www.ntt-west.co.jp/news/2402/240229a.html〔2024/4/12 確認〕
※ 189 NHK：NTT 西日本 森林社長 3 月末で退任 子会社の個人情報不正流出で https://www3.nhk.or.jp/news/html/20240229/k10014374531000.html〔2024/4/12 確認〕
※ 190 https://www.ipa.go.jp/security/guide/insider.html〔2024/4/12 確認〕
※ 191 株式会社プラスワン教育：お客様の個人情報漏えいに関するお知らせとお詫び https://riso-plus1.co.jp/ お客さまの個人情報漏えいに関するお知らせとお詫び .pdf〔2024/4/12 確認〕
※ 192 三井住友カード株式会社：ご利用代金明細書の有料化ご案内 DM に関するお詫び https://www.smbc-card.com/mem/cardinfo/cardinfo4010656.jsp〔2024/4/12 確認〕
※ 193 IPA：JVN iPedia 脆弱性対策情報データベース https://jvndb.jvn.jp/〔2024/4/12 確認〕
※ 194 JPCERT/CC、IPA：Japan Vulnerability Notes（JVN） https://jvn.jp/〔2024/4/12 確認〕
※ 195 NIST：National Vulnerability Database（NVD） https://nvd.nist.gov/〔2024/4/12 確認〕
※ 196 公表年は、ベンダーがアドバイザリーを公開した年、他組織やセキュリティポータルサイト等の登録／公開した年、発見者が一般向けに報告した年等、脆弱性対策情報が一般に公表された年を指す。なお、JVN iPedia で脆弱性対策情報を公開した年は「登録年」としている。
※ 197 IPA：共通脆弱性識別子 CVE 概説 https://www.ipa.go.jp/security/vuln/CVE.html〔2024/4/12 確認〕
※ 198 MITRE 社：CVE Numbering Authorities（CNAs） https://www.cve.org/ProgramOrganization/CNAs〔2024/4/12 確認〕
※ 199 The MITRE Corporation：米国政府向けの技術支援や研究開発を行う非営利組織。80 を超える主要な脆弱性情報サイトと連携して、脆弱性情報の収集と、重複のない CVE の採番を行っている。
※ 200 MITRE 社：CVE Adds 7 New CVE Numbering Authorities（CNAs） https://cve.mitre.org/news/archives/2016/news.html〔2024/4/12 確認〕
※ 201 MITRE 社：ARC Informatique Added as CVE Numbering Authority（CNA） https://www.cve.org/Media/News/item/news/2023/12/19/ARC-Informatique-Added-as-CNA〔2024/4/12 確認〕
※ 202-1 IPA：共通脆弱性タイプ一覧 CWE 概説 https://www.ipa.go.jp/security/vuln/CWE.html〔2024/4/12 確認〕
※ 202-2 JVN iPedia の情報収集元が CWE を付与していない脆弱性対策情報については対象外としている。
※ 203-1 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〔2024/4/12 確認〕
※ 203-2 JVN iPedia の情報収集元が CVSS v3 を付与していない脆弱性対策情報については対象外としている。
※ 204 JPCERT/CC：セキュアコーディング https://www.jpcert.or.jp/securecoding/〔2024/4/12 確認〕
※ 205 NVD：CVE-2023-34362 https://nvd.nist.gov/vuln/detail/CVE-2023-34362〔2024/4/12 確認〕
※ 206 NVD：CVE-2023-4966 https://nvd.nist.gov/vuln/detail/CVE-2023-4966〔2024/4/12 確認〕
※ 207 Citrix Systems, Inc.：CVE-2023-4966: Critical security update now available for NetScaler ADC and NetScaler Gateway https://www.netscaler.com/blog/news/cve-2023-4966-critical-security-update-now-available-for-netscaler-adc-and-netscaler-gateway/〔2024/4/12 確認〕
※ 208 https://jvndb.jvn.jp/apis/index.html〔2024/4/12 確認〕
※ 209 https://jvndb.jvn.jp/apis/myjvn/mjcheck4.html〔2024/4/12 確認〕
※ 210 株式会社大和証券グループ本社：大和証券における全社員の ChatGPT 利用開始について https://ssl4.eir-parts.net/doc/8601/tdnet/2263460/00.pdf〔2024/4/12 確認〕
※ 211 「1.3.2 早期警戒パートナーシップの届出状況から見る脆弱性の動向」では、「ソフトウェア製品」と「Web アプリケーション」は、早期警戒パートナーシップにおける対象の区分を意味するものであり、特に断りのない限り、または文献引用上の正確性を期す必要のない限り、「Web アプリケーション」の省略形として「Web サイト」を使用する。
※ 212 IPA：情報セキュリティ早期警戒パートナーシップの紹介 https://www.ipa.go.jp/security/guide/vuln/ug65p90000019by0-att/000059695.pdf〔2024/4/12 確認〕
※ 213 ソフトウェア製品の取り扱い終了は、「不受理」「脆弱性でない」「脆弱性対策情報公表済み」「公表せずに製品開発者が利用者ごとに個別で対策を実施済み」のいずれかであることを指す。Web アプリケーションの取り扱い終了は、「不受理」「脆弱性でない」「連絡不可能」「修正完了」「IPA による注意喚起実施済み」のいずれかであることを指す。
※ 214 「1.3.2 早期警戒パートナーシップの届出状況から見る脆弱性の動向」では、「ウェブアプリケーションソフト」は、Web サイト構築関係のソフトウェアを指す。これは、四半期ごとの脆弱性関連情報の届出状況のレポート（IPA：ソフトウェア等の脆弱性関連情報に関する届出状況 https://www.ipa.go.jp/security/reports/vuln/software/index.html〔2024/4/12 確認〕）で使用している製品種類の「ウェブアプリケーションソフト」と同じである。
※ 215 https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000196e2-att/000017319.pdf〔2024/4/12 確認〕
※ 216 https://www.ipa.go.jp/security/vuln/websecurity/about.html〔2024/4/12 確認〕
※ 217 https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html〔2024/4/12 確認〕

付録

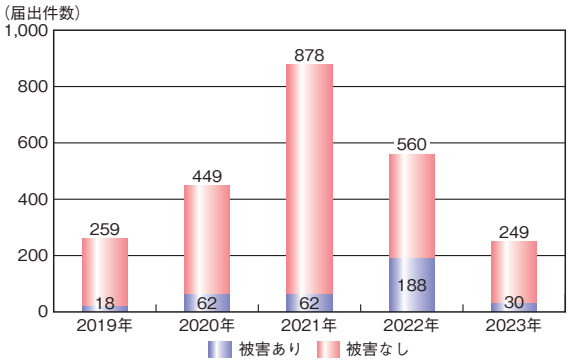
資料

資料A　2023年のコンピュータウイルス届出状況

IPA が 2023 年 1 月から 12 月の期間に受け付けたコンピュータウイルス（以下、ウイルス）届出の集計結果について述べる。

A.1　届出件数

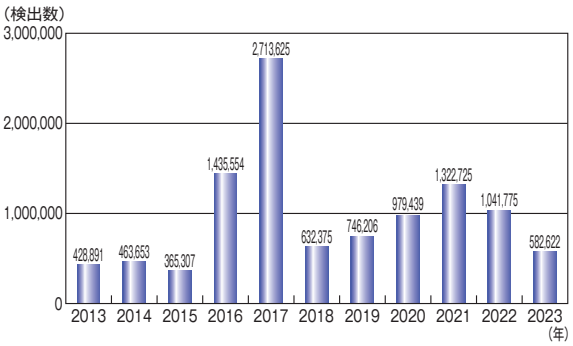
2023 年の年間届出件数は、前年の 560 件より 311 件（55.5%）少ない 249 件であった（図 A-1）。そのうち、ウイルス感染の実被害があった届出は 30 件であった。



■図 A-1　ウイルス届出件数推移（2019～2023 年）

A.2　届出のあったウイルス等検出数

2023 年に寄せられたウイルス等の検出数は、前年の 104 万 1,775 個より 45 万 9,153 個（44.1%）少ない 58 万 2,622 個であった（図 A-2）。



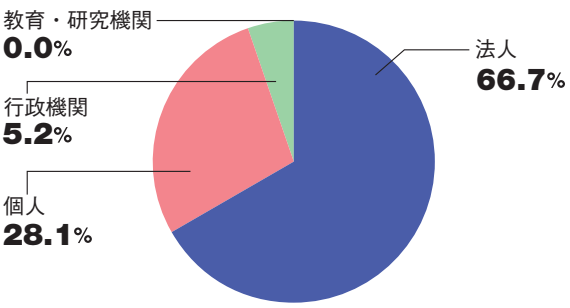
■図 A-2　ウイルス等検出数推移（2013～2023 年）

A.3　届出者の主体別届出件数

2023 年の主体別届出件数は前年と比較すると、全体的に減少した。主体別の比率では「法人」からの届出が 66.7%（166 件）と最も多かった（表 A-1、図 A-3）。

届出者の主体	2021 年	2022 年	2023 年
法人	284	388	166
個人	578	145	70
行政機関	15	18	13
教育・研究機関	1	9	0
合計（件）	878	560	249

■表 A-1　ウイルス届出者の主体別届出件数（2021～2023 年）



■図 A-3　ウイルス届出者の主体別届出件数の比率（2023 年）

A.4　傾向

2023 年でウイルス感染の実被害に遭った届出 30 件のうち、ランサムウェアの感染被害が 11 件あった。また、Emotet の感染被害も同じく 11 件あり、2022 年で実被害に遭った届出 188 件のうち、Emotet の感染被害が 145 件であったことに比べると大幅に減少したものの届出はされている。なお、Emotet に関しては不定期に休止・再開を繰り返しており、今後、再び大規模な攻撃活動が開始される可能性もあるため、引き続き警戒をしていただきたい。

これらの届出件数の詳細は、下記の資料から参照可能であり、ランサムウェアの攻撃手口や対策に関しては、本白書の「1.2.1 ランサムウェア攻撃」にて詳しく述べているので、ぜひそちらを一読いただきたい。

参照

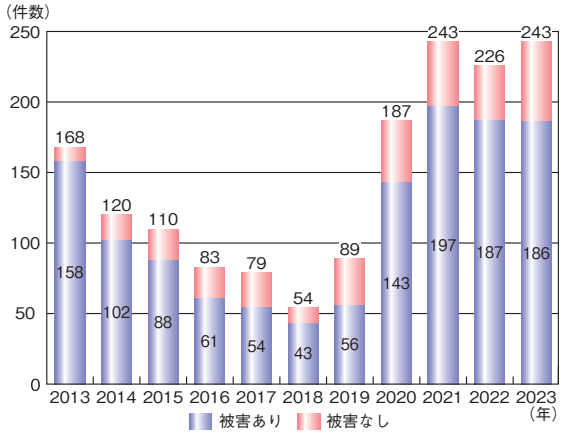
■コンピュータウイルス・不正アクセスの届出状況［2023年（1月～12月）］
https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/2023-report.pdf

資料B　2023年のコンピュータ不正アクセス届出状況

IPA が 2023 年 1 月から 12 月の期間に受け付けたコンピュータ不正アクセス（以下、不正アクセス）届出の集計結果について述べる。

B.1　届出件数

2023 年の年間届出件数は、前年の 226 件より 17 件（7.5%）多い 243 件であった（図 B-1）。そのうち、実被害があった届出は 186 件であった。



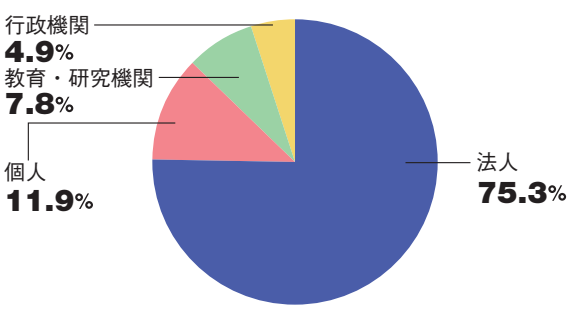
■図 B-1　不正アクセス届出件数推移（2013 年～2023 年）

B.2　届出者の主体別届出件数

2023 年は前年と比較すると、「法人」からの届出件数が増加した一方で、その他の届出件数は減少している。届出者の主体別の比率で見ると「法人」からの届出が 75.3%（183 件）と最も多かった（表 B-1、図 B-2）。

届出者の主体	2021 年	2022 年	2023 年
法人	156	137	183
個人	46	50	29
教育・研究機関	22	21	19
行政機関	19	18	12
合計（件）	243	226	243

■表 B-1　不正アクセス届出者の主体別届出件数（2021～2023 年）

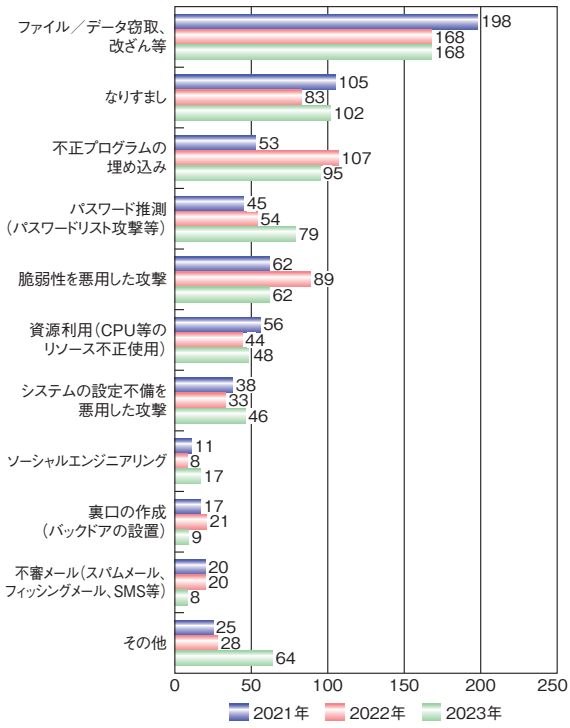


■図 B-2　不正アクセス届出者の主体別届出件数の比率（2023 年）

B.3　手口別件数

届出を攻撃行為（手口）により分類した件数を図 B-3 に示す。なお、以降の分類も含め、届出 1 件につき、複数の分類項目が該当する場合がある。その場合は該当する項目のそれぞれにカウントした。

2023 年の届出において最も多く見られた手口は、前年と同様に「ファイル／データ窃取、改ざん等」の 168 件であり、次いで「なりすまし」が 102 件、「不正プログラムの埋め込み」が 95 件であった。



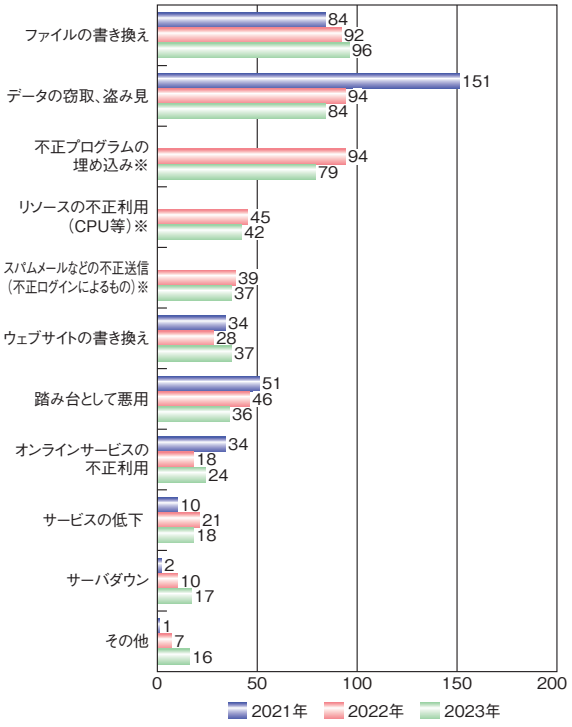
■図 B-3　不正アクセス手口別件数の推移（2021～2023 年）

B.4　被害内容別件数

届出のうち、実際に被害に遭った届出について、被害内容により分類した件数を図 B-4 に示す。2023 年の届出において最も多く見られた被害は、「ファイルの書き換え」の 96 件であった。次いで「データの窃取、盗み見」が 84 件、「不正プログラムの埋め込み」が 79 件であった。

なお、具体的な被害事例については、「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）において「コンピュータウイルス・不正アクセスの届出事例［2023 年上半期（1 月～ 6 月）］」及び「コン

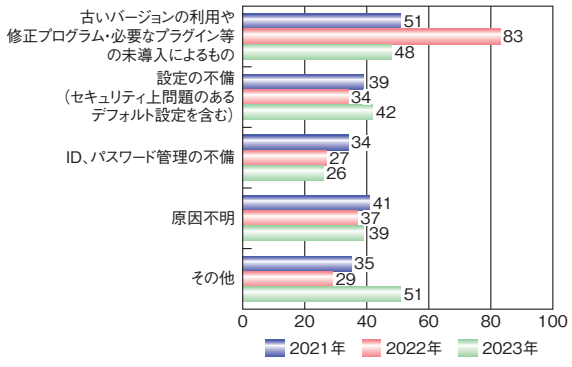
ピュータウイルス・不正アクセスの届出事例［2023 年下半期（7 月～ 12 月）］」を紹介している。そちらも、ぜひ参考にしていただきたい。



■図 B-4　不正アクセス被害内容別件数の推移（2021～2023 年）
※被害内容が多様化したため、2022 年から項目を細分化した。

B.5 原因別件数

実際に被害に遭った届出について、不正アクセスの原因となった問題点／弱点で分類した件数を図 B-5 に示す。2023 年の届出において最も多く見られた原因は、前年と同様に「古いバージョンの利用や修正プログラム・必要なプラグイン等の未導入によるもの」であり 48 件であった。次いで「設定の不備（セキュリティ上問題のあるデフォルト設定を含む）」が 42 件、「ID、パスワード管理の不備」が 26 件であった。



■図 B-5　不正アクセス原因別件数の推移（2021～2023 年）

B.6 傾向と対策

不正アクセスの傾向と対策について述べる。

(1) 傾向

図 B-1 に示した 2023 年に届出された 243 件について、不正アクセス（被害なしも含む）の傾向を分析したところ、「Web サイトの脆弱性や設定不備の悪用に関する不正アクセス」が 65 件、「VPN 装置の脆弱性やリモートデスクトップサービスの設定不備を悪用したランサムウェア攻撃に関する不正アクセス」が 52 件確認された。また、「パスワードリスト攻撃や総当たり攻撃で、認証を突破されたことによる、メールアカウント等の不正アクセス」が 44 件あった。

(2) 対策

(1)で示した脆弱性や設定不備の対策としては、利用している機器やソフトウェアに関する脆弱性情報の収集や修正プログラムの適用、設定の定期的な見直しといった、基本的なセキュリティ対策を実施することが重要である。企業・組織においては、脆弱性診断やペネトレーションテスト等を行い、確実に脆弱性や設定不備を解消することが望まれる。なお、ソフトウェア等の脆弱性対策に関しては、本白書の「1.2.5 ソフトウェアの脆弱性を悪用した攻撃」も参照していただきたい。

メールアカウント等の不正アクセスに関する対策としては、企業・組織やシステム利用者に限らず、他者に推測されにくい複雑なパスワードを設定する、パスワードの使い回しをしない等の基本的な対策を実施することに加え、利用しているシステムで多要素認証等のセキュリティオプションが用意されている場合には積極的に採用する等、今一度、アカウントが適切に管理できているか見直すことを勧める。

参照

■コンピュータウイルス・不正アクセスの届出状況［2023年（1月～12月）］
https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/2023-report.pdf

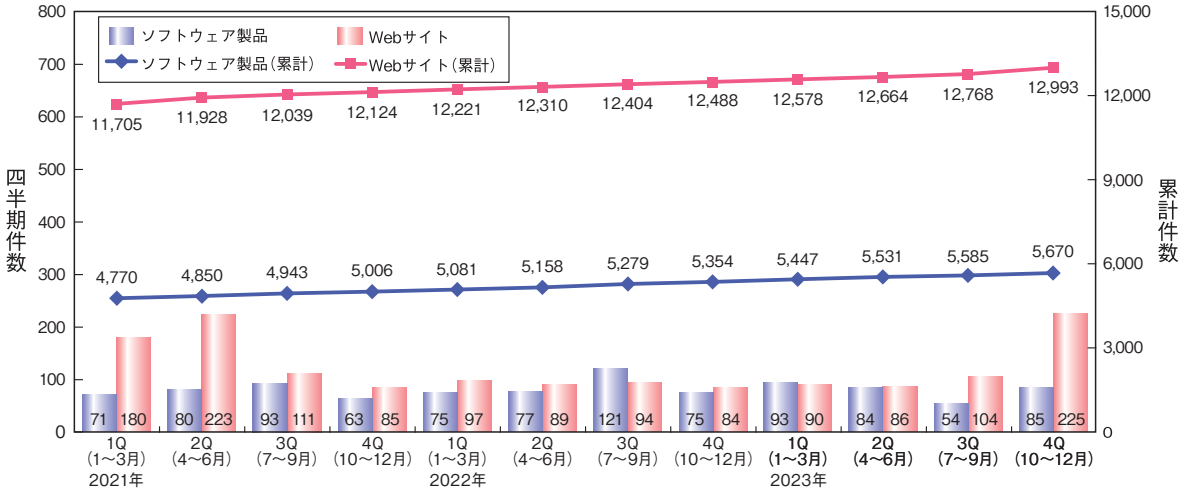
資料C　ソフトウェア等の脆弱性関連情報に関する届出状況

IPA が受け付けたソフトウェア製品や Web サイトの脆弱性の情報について、届出件数や処理の状況を述べる。

C.1　脆弱性の届出概況

2023 年末時点で、届出受付開始（2004 年 7 月 8 日）からの累計は、ソフトウェア製品に関するもの 5,670 件、Web サイトに関するもの 1 万 2,993 件、合計 1 万 8,663 件で、Web サイトに関する届出が全体の 69.6% を占めている（図 C-1）。

表 C-1 に示すように、届出受付開始から各四半期末時点までの就業日 1 日あたりの届出件数は、2023 年第 4 四半期末時点で 3.93 件となっている。



■図 C-1　脆弱性関連情報の届出件数の四半期別推移

2021年1Q（1~3月）	2021年2Q（4~6月）	2021年3Q（7~9月）	2021年4Q（10~12月）	2022年1Q（1~3月）	2022年2Q（4~6月）	2022年3Q（7~9月）	2022年4Q（10~12月）	2023年1Q（1~3月）	2023年2Q（4~6月）	2023年3Q（7~9月）	2023年4Q（10~12月）
4.04	4.06	4.05	4.02	4.01	3.99	3.98	3.97	3.95	3.94	3.92	3.93

■表 C-1　就業日 1 日あたりの届出件数（届出受付開始から各四半期末時点）

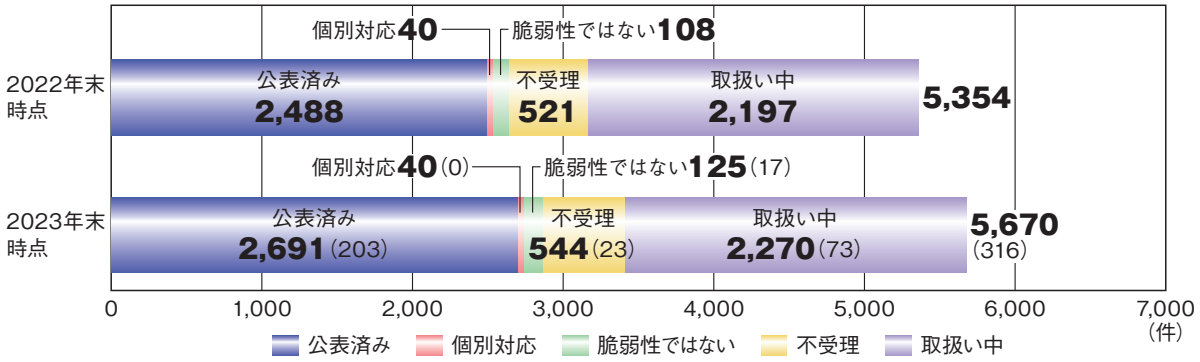
C.2　ソフトウェア製品の脆弱性届出の処理状況

ソフトウェア製品に関する脆弱性届出の 2023 年における処理件数及び 2023 年末時点での処理状況別の累計件数について図 C-2 に示す。

2023 年の届出のうち、JPCERT/CC が調整を行い、製品開発者が脆弱性の修正を完了し、JVN で対策情報を公表した「公表済み」のものは 203 件で累計 2,691 件、JVN で公表せず製品開発者が「個別対応」を行ったものは 0 件で累計 40 件、製品開発者が「脆弱性ではない」と判断したものは 17 件で累計 125 件、告示で定める届出の対象に該当せず「不受理」としたものは 23 件で累計 544 件となり、これらをまとめた「処理の終了」件数は 243 件で累計 3,400 件に達した。また、「取扱い中」の届出は 73 件増加して 2,270 件となり、ソフトウェア製品に関する届出は累計 5,670 件となった。

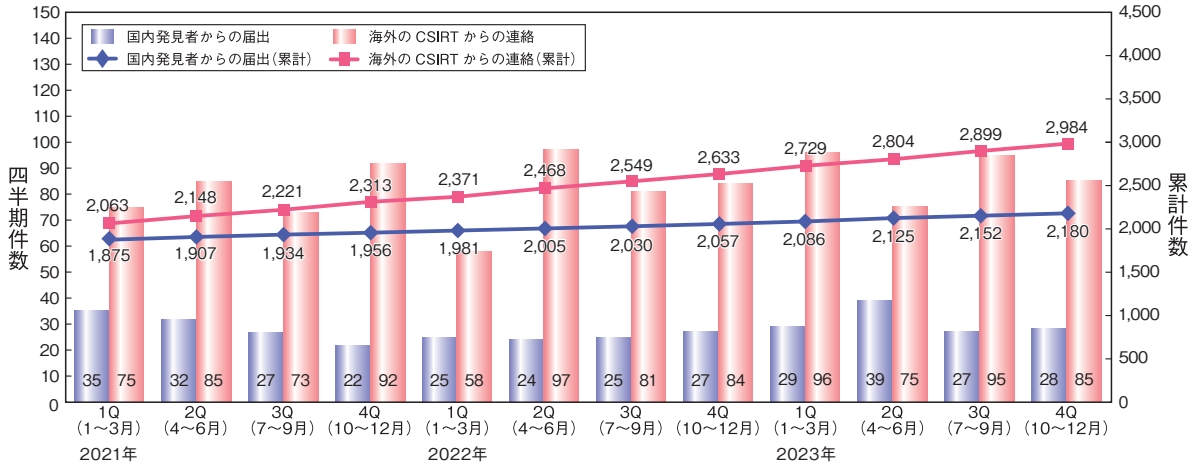
ソフトウェア製品の脆弱性対策情報の公表件数の累計は、国内発見者からの届出を公表したものが 2,180 件、海外の CSIRT から JPCERT/CC が連絡を受けたものを JVN で公表したものが 2,984 件となった。これらソフトウェア製品の脆弱性対策情報の公表件数の期別推移を図 C-3 に示す。

なお、複数の届出についてまとめて 1 件の脆弱性対策情報として公表する場合があるため、図 C-2 の「公表済み」の件数と図 C-3 の公表件数は異なっている。



※( )内の数値は 2022 年末時点と 2023 年末時点の差分

■図 C-2　ソフトウェア製品の脆弱性関連情報の届出の処理状況の推移



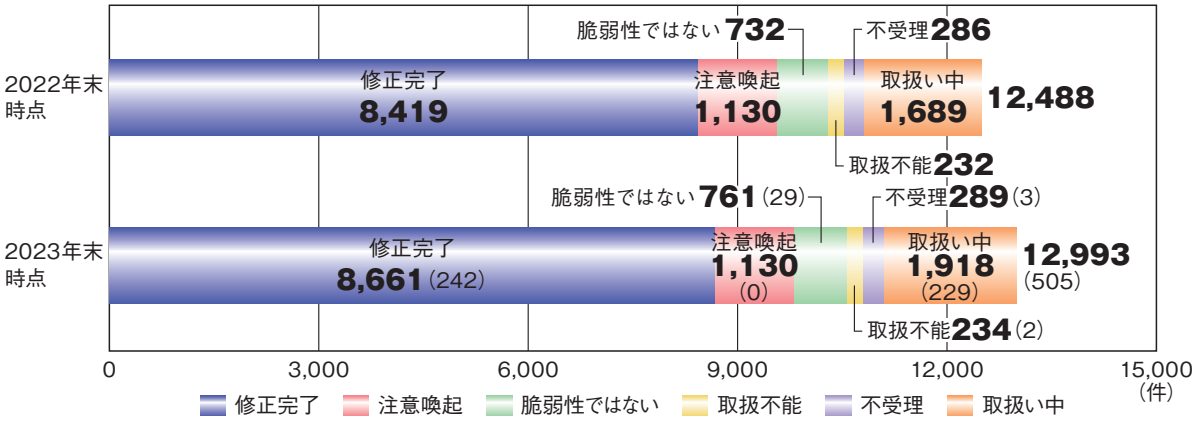
■図 C-3　ソフトウェア製品の脆弱性対策情報の公表件数

C.3 Webサイトの脆弱性届出の処理状況

Web サイトに関する脆弱性届出の 2023 年における処理件数及び 2023 年末時点での処理状況別の累計件数について図 C-4 に示す。

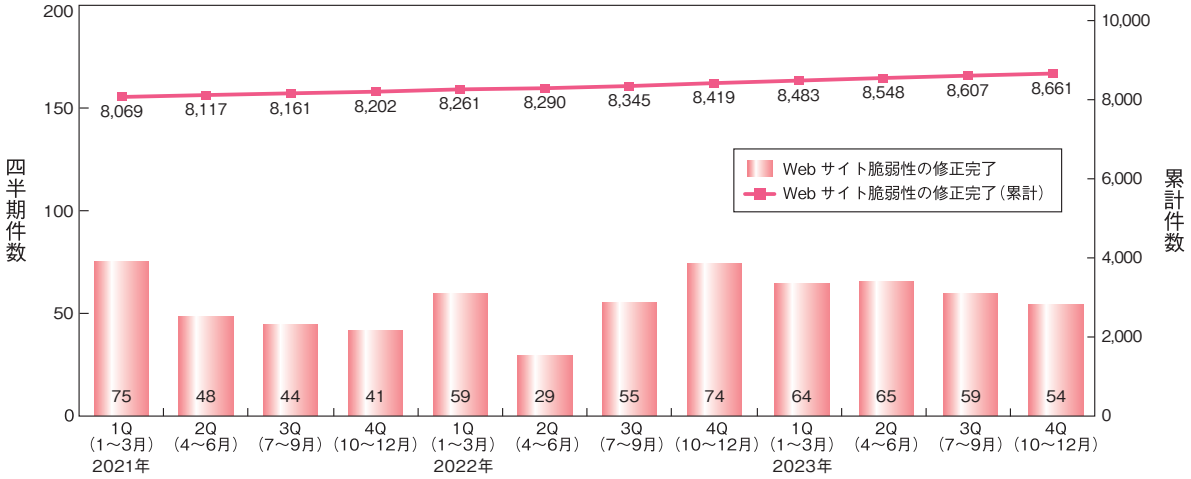
2023 年の届出のうち、IPA が通知を行い Web サイト運営者が「修正完了」としたものは 242 件で累計 8,661 件、IPA が「注意喚起」等を行った後に処理を終了したものは 0 件で累計 1,130 件、IPA 及び Web サイト運営者が「脆弱性ではない」と判断したものは 29 件で累計 761 件、Web サイト運営者と連絡が不可能なもの、または IPA が対応を促しても修正完了した旨の報告をしない、修正を拒否する等、Web サイト運営者の対応により「取扱不能」なものは 2 件で累計 234 件、告示で定める届出の対象に該当せず「不受理」としたものは 3 件で累計 289 件となり、これらをまとめた「処理の終了」件数は 276 件で累計 1 万 1,075 件に達した。また、「取扱い中」の届出は 229 件増加して 1,918 件となり、Web サイトに関する届出は累計 1 万 2,993 件となった。

これらのうち、「修正完了」件数の期別推移を図 C-5 に示す。



※( )内の数値は 2022 年末時点と 2023 年末時点の差分

■図 C-4　Web サイトの脆弱性関連情報の届出の処理状況の推移



■図 C-5　Web サイトの脆弱性の修正完了件数

参照

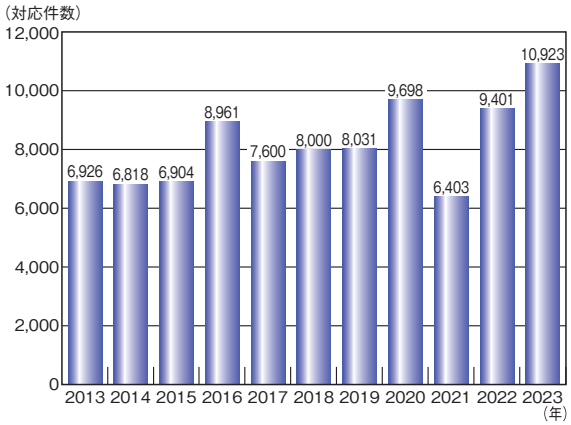
■ソフトウェア等の脆弱性関連情報に関する届出状況［2023年第4四半期（10月～12月）］
https://www.ipa.go.jp/security/reports/vuln/software/2023q4.html

資料D　2023年の情報セキュリティ安心相談窓口の相談状況

IPA が 2023 年 1 月から 12 月の期間に対応した、相談状況の集計結果について述べる。

D.1　相談対応件数

2023 年の年間相談対応件数は 10,923 件となり、2022 年の相談対応件数 9,401 件より 1,522 件（16.2%）の増加となった（図 D-1）。



■図 D-1　相談対応件数の推移（2013～2023 年）

D.2　相談者の主体別相談件数

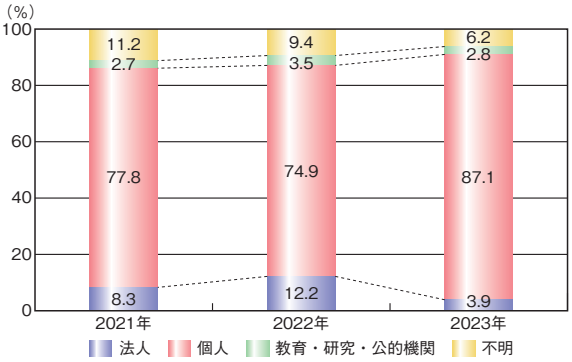
相談者の主体別では、2023 年も個人からの相談が 9,514 件（87.1%）と最も多かった。

主体別相談比率の推移では、法人からの相談比率は 2022 年と比較して 8.3% 減少した一方、個人からの相談比率は 12.2% 増加した（表 D-1、図 D-2）。

法人については、2022 年に多かった「Emotet 関連」の相談の減少が、要因の一つと考えられる。また個人については、「ウイルス警告の偽警告」についての相談の増加が要因の一つと考えられる（「D.4 手口別相談件数」参照）。

相談者の主体	2021 年	2022 年	2023 年
法人	530	1,145	427
個人	4,984	7,043	9,514
教育・研究・公的機関	170	330	308
不明	719	883	674
合計（件）	6,403	9,401	10,923

■表 D-1　情報セキュリティ安心相談窓口の主体別相談件数（2021～2023 年）



■図 D-2　情報セキュリティ安心相談窓口の主体別相談件数の比率推移（2021～2023 年）

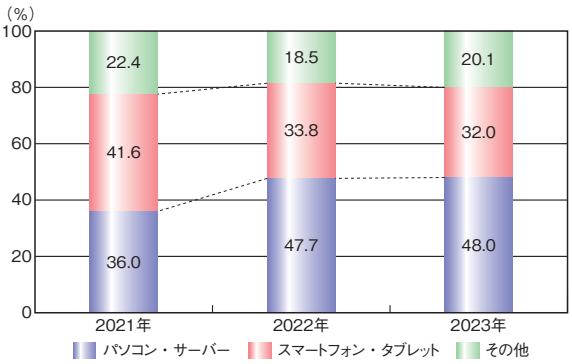
D.3　相談者の機器種別相談件数

相談機器種別では、2023 年は「パソコン・サーバー」に関する相談が 5,240 件（48.0%）と最も多かった。

相談者の機器種別相談比率は、2022 年と比較して同じ水準で推移しており、大きな変化はなかった（表 D-2、図 D-3）。

相談機器種別の主体	2021 年	2022 年	2023 年
パソコン・サーバー	2,304	4,487	5,240
スマートフォン・タブレット	2,666	3,173	3,492
その他	1,433	1,741	2,191
合計（件）	6,403	9,401	10,923

■表 D-2　情報セキュリティ安心相談窓口の機器種別相談件数（2021～2023 年）

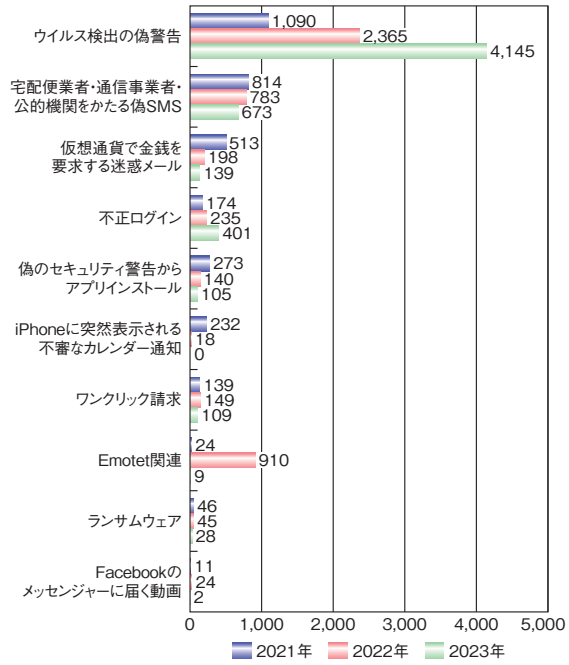


■図 D-3　情報セキュリティ安心相談窓口の機器種別相談件数の比率推移（2021～2023 年）

D.4 手口別相談件数

主な手口ごとの相談件数を図 D-4 に示す。2023 年の相談で最も多く寄せられたのは、「ウイルス検出の偽警告」に関する相談で4,145件(37.9%)であった。次いで、「宅配便業者・通信事業者・公的機関をかたる偽SMS」に関する相談が 673 件 (6.2%)、「不正ログイン」に関する相談が 401 件(3.7%)であった。上位三つの手口による相談件数の合計は 5,219 件で、全相談件数(10,923 件)の 47.8% であった。

問い合わせの多い手口については、情報セキュリティ安心相談窓口の発行する「安心相談窓口だより」や、「手口検証動画」で注意喚起を行っている。ぜひ参考にしてほしい。



■図 D-4　主な手口別相談件数の推移（2021～2023 年）

参照

■安心相談窓口だより
https://www.ipa.go.jp/security/anshin/attention/index.html
■手口検証動画シリーズ
https://www.ipa.go.jp/security/anshin/measures/verificationmov.html

第19回 IPA「ひろげよう情報セキュリティコンクール」2023 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53,312点の応募作品の中から、受賞した作品の一部をご紹介いたします。

最優秀賞

〈独立行政法人情報処理推進機構〉

〈標語部門〉

それでいい？
使いまわしの
パスワード

大阪府 大阪市立大淀小学校 5年 **今岡 陽菜歌**さん

〈ポスター部門〉

扱いに注意！君の味方は敵にもなる

神奈川県 神奈川県立神奈川工業高等学校 3年 **村石 琉音**さん

〈4コマ漫画部門〉

フィッシング

兵庫県 西宮市立鳴尾中学校 3年
奥埜 和花さん

優秀賞

〈独立行政法人情報処理推進機構〉

〈標語部門〉

信じるの　知らない人の　その言葉

大阪府　堺市立南八下小学校　4年
市ノ瀬 瑚珀さん

セキュリティ　「面倒くさい」が　命とり

大阪府　大阪教育大学附属平野中学校　1年
稲垣 敢太さん

詐欺メール「緊急」「至急」疑おう

大阪府　東大谷高等学校　1年
小倉 結子さん

〈ポスター部門〉

フィッシングに注意！

兵庫県 雲雀丘学園小学校 6年
オストハイダ 真紋さん

“Fake” Wi-Fi

愛媛県 松山市立勝山中学校 3年
渡辺 梨緒さん

兵庫県 兵庫県立姫路工業高等学校 2年
川上 心優さん

〈4コマ漫画部門〉

なぞかけ

岡山県 岡山市立御津南小学校 5年
北山 穂風さん

「まぁ、いっか。」の結末は…。

広島県 呉市立東畑中学校 3年
長尾 妃芽さん

こわ〜い話

広島県 広島県立呉商業高等学校 3年
井上 心彩さん

IPAの便利なツールとコンテンツ

情報セキュリティ対策ベンチマーク
https://www.ipa.go.jp/security/sec-tools/benchmark.html

診断

用途・目的	自組織のセキュリティレベルを診断
利用対象者	情報セキュリティ担当者
特 長	• 他組織と比較した自組織のセキュリティレベルが判る • 自組織に不足しているセキュリティ対策が判る

概要

「セキュリティ対策の取り組み状況に関する評価項目」27 問と「企業プロフィールに関する評価項目」19 問、計 46 問に回答すると以下の診断結果を表示します。

■提供される診断結果
- セキュリティレベルを示したスコア（最高点 135 点、最低点 27 点）
- 情報セキュリティリスクの指標と企業規模、業種が自組織と近い他組織について診断項目別に比較
- 結果に応じた推奨される取り組み

脆弱性体験学習ツール「AppGoat」
https://www.ipa.go.jp/security/vuln/appgoat/

学習

用途・目的	脆弱性に関する基礎的な知識の学習
利用対象者	• アプリケーション開発者 • Web サイト管理者
特 長	脆弱性の概要や対策方法等、脆弱性に関する基礎的な知識を実習形式で体系的に学べるツール

概要

SQL インジェクション、クロスサイト・スクリプティング等 の 12 種類の Web アプリケーションに関連する脆弱性について学習できるツールです。
利用者は学習テーマ毎の演習問題に対して、埋め込まれた脆弱性の発見、プログラミング上の問題点の把握、対策手法を学べます。

■活用方法例
- Web アプリケーション用学習ツール（個人学習モード）を利用した、自宅等での個人学習
- Web アプリケーション用学習ツール（集合学習モード）を利用した、学校の講義や組織内のセミナー等における複数人での学習

■動作環境・必須ソフトウェア
Windows 10、11

脆弱性対策情報データベース「JVN iPedia」
https://jvndb.jvn.jp/

対策

用途・目的	自組織で使用しているソフトウェア製品の脆弱性の確認と対策
利用対象者	• システム管理者 • 製品・サービスの保守を担う担当者
特 長	国内外で公開されたソフトウェア製品の脆弱性対策情報が掲載された、キーワード検索可能なデータベース

概要

■掲載情報例
- 脆弱性の概要
- 脆弱性がある製品名とそのベンダー名
- 共通脆弱性識別子 CVE
- 脆弱性の深刻度 CVSS 基本値
- 本脆弱性に関わる製品ベンダー等のリンク

■活用方法例
- ネット記事等に記載された CVE 番号を JVN iPediaで検索し、脆弱性の詳細を確認
- 自組織で使用している製品名で検索し、脆弱性の詳細を確認

MyJVN バージョンチェッカ for .NET
https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html

対策

用途・目的	パソコンにインストールされたソフトウェア製品のバージョンが最新かどうかの確認
利用対象者	パソコン利用者全般
特 長	インストールされている対象製品が最新バージョンかどうかをまとめて確認できる

概要

■判定対象ソフトウェア製品

- Adobe Reader
- JRE
- Lhaplus
- Mozilla Firefox
- Mozilla Thunderbird
- iTunes
- Lunascape
- Becky! Internet Mail
- OpenOffice.org
- VMware Player
- Google Chrome
- LibreOffice

■活用方法例

毎朝、MyJVN バージョンチェッカを実行して、使用しているソフトウェアが最新かどうかをチェックし、最新でなければそのソフトウェアを更新する

■動作環境・必須ソフトウェア

Windows 10、11

注意警戒情報サービス
https://jvndb.jvn.jp/alert/

対策

用途・目的	脆弱性対策に必要な最新情報の収集
利用対象者	• システム管理者 • 製品・サービスの保守を担う担当者
特 長	国内で広く利用され、脆弱性が悪用されると影響の大きいサーバー用オープンソースソフトウェアのリリース情報と IPA が発信する「重要なセキュリティ情報」を提供

概要

■掲載情報例

- Apache HTTP Server
- Apache Struts
- Apache Tomcat
- BIND
- Joomla!
- OpenSSL
- WordPress
- 重要なセキュリティ情報

■活用方法例

定期的に自組織で使用しているオープンソースソフトウェアのリリース情報やIPA が発信する「重要なセキュリティ情報」が公表されているかどうかを確認し、公表されていれば内容の確認、必要に応じ対応を行う

サイバーセキュリティ注意喚起サービス「icat for JSON」
https://www.ipa.go.jp/security/vuln/icat.html

対策

用途・目的	IPA が発信する「重要なセキュリティ情報」のリアルタイム取得
利用対象者	• システム管理者 • サービスの保守を担う担当者 • 個人利用者
特 長	Web ページに HTML タグを埋め込むと、Web ページから IPA が発信する「重要なセキュリティ情報」を配信

概要

■「重要なセキュリティ情報」発信例

- 利用者への影響が大きい製品の脆弱性情報
- 広く使われる製品のサポート終了情報
- サイバー攻撃への注意喚起

■活用方法例

icat を自組織の従業員がよくアクセスする Web ページ（イントラページ等）に表示させ、ソフトウェア更新等の対策を促す

MyJVN 脆弱性対策情報フィルタリング収集ツール（mjcheck4）
https://jvndb.jvn.jp/apis/myjvn/mjcheck4.html

対策

用途・目的	自組織で使用しているソフトウェア製品の脆弱性の確認と対策
利用対象者	• システム管理者 • 製品・サービスの保守を担う担当者
特 長	JVN iPedia に登録されている脆弱性対策情報をフィルタリングして自社システムに関連する脆弱性情報を効率よく収集

概要

■フィルタリング例
• 製品名　　• CVSSv3　　• 公開日　等

■活用方法例
• 自組織が利用しているオープンソースソフトウェア製品の脆弱性対策情報収集
• 情報システム部門が運用しているシステムの脆弱性対策情報の収集

■動作環境・必須ソフトウェア
Windows 10、11

Web サイトの攻撃兆候検出ツール「iLogScanner」
https://www.ipa.go.jp/security/vuln/ilogscanner/

診断

用途・目的	Web サイトに対する攻撃の痕跡、攻撃の可能性を検出
利用対象者	Web サイト運営者
特 長	Web サイトのアクセスログ、エラーログ、認証ログを解析し、攻撃の痕跡や攻撃に成功した可能性があるログを解析結果レポートに表示

概要

■アクセスログ、エラーログから検出可能な項目例
• SQL インジェクション　　• OS コマンド・インジェクション
• ディレクトリ・トラバーサル　　• クロスサイト・スクリプティング

■認証ログ（Secure Shell、FTP）から検出可能な項目例
• 大量のログイン失敗　　• 短時間の集中ログイン
• 同一ファイルへの大量アクセス　　• 認証試行回数

■活用方法例
定期的に iLogScanner を実行し、自組織の Web サイトを狙った攻撃が行われているか確認する

5 分でできる！情報セキュリティ自社診断
https://www.ipa.go.jp/security/guide/sme/5minutes.html

診断

用途・目的	自社の情報セキュリティ対策状況を診断
利用対象者	中小企業・小規模事業者の経営者、管理者、従業員
特 長	• 設問に答えるだけで自社のセキュリティ対策状況を把握することができる • 診断後は、診断結果に即した対策が確認できる

概要

「5 分でできる！情報セキュリティ自社診断」は、情報セキュリティ対策のレベルを数値化し、問題点を見つけるためのツールです。
25 の質問に答えるだけで診断することができ、解説編を参照することで、診断編にある設問の内容を自社で対応していない場合に生じる情報セキュリティへのリスクと、今後どのような対策を設けるべきかを把握することができます。

情報セキュリティ・ポータルサイト「ここからセキュリティ！」
https://www.ipa.go.jp/security/kokokara/

学習 診断 対策

用途・目的	• 情報セキュリティや情報リテラシーに関する情報収集 • 国内の主なレポート、ガイドライン、学習・診断等のツール等の利用
利用対象者	• インターネットの一般利用者（小学生～大人） • 企業の管理者／一般利用者
特 長	情報セキュリティ関連の民間及び公的な団体が公開する無償の資料、情報、ツールを網羅的に掲載。目的別、用途別、役割別に情報を選択し利用が可能

概要

• セキュリティベンダー、公的機関、政府等から発信される注意喚起や、資料・動画・ツール等のコンテンツを網羅的に掲載したポータルサイト
• コンテンツを「被害に遭ったら」「対策する」「教育・学習」「セキュリティチェック」「データ＆レポート」に分類。必要な情報が見つけやすい
• 教育学習は対象者を細分化し、それぞれに適した教育学習コンテンツを紹介

サイバーセキュリティ経営可視化ツール
https://www.ipa.go.jp/security/economics/checktool.html

診断

用途・目的	セキュリティ対策の実施状況のセルフチェック
利用対象者	原則として、従業員 300 名以上の企業の CISO 等、サイバーセキュリティ対策の実施責任者
特 長	サイバーセキュリティ経営ガイドライン Ver3.0 に準拠したセキュリティ対策の実施状況を成熟度モデルで自己診断し、レーダーチャートで可視化

概要

経営者がサイバーセキュリティ対策を実施する上で責任者となる担当幹部（CISO 等）に指示すべき“重要 10 項目”が、適切に実施されているかどうかを 5 段階の成熟度モデルで自己診断し、その結果をレーダーチャートで可視化するツールです。
診断結果は、経営者への自社のセキュリティ対策の実施状況の説明資料として利用できます。経営者が対策状況を定量的に把握することで、サイバーセキュリティに関する方針の策定や適切なセキュリティ投資の検討、投資家等ステークホルダとのコミュニケーション等に役立てることができます。

■提供される主な機能
・重要 10 項目の実施状況の可視化
・診断結果と業種平均との比較
・対策を実施する際の参考事例
・グループ企業同士の診断結果の比較

5 分でできる！情報セキュリティポイント学習
https://www.ipa.go.jp/security/sec-tools/5mins_point.html

学習

用途・目的	自社の情報セキュリティ教育の実施
利用対象者	中小企業の経営者、管理者、従業員等
特 長	• 自社診断の質問を 1 テーマ 5 分で学べる • インストール不要、無料の学習ツール

概要

情報セキュリティについて学習できるツールです。
身近にある職場の日常の 1 コマを取り入れた親しみやすい学習テーマで、セキュリティに関する様々な事例を疑似体験しながら適切な対処法を学ぶことができます。

安心相談窓口だより
https://www.ipa.go.jp/security/anshin/attention/index.html

学習 対策

用途・目的	最新の「ネット詐欺」等の手口を知り被害防止につなげる
利用対象者	スマートフォン、パソコンの一般利用者
特 長	実際に相談窓口に寄せられる、よくある相談内容に関して「手口」と「被害にあった場合の対処」「被害にあわないための対策」を学べる

概要

IPA 情報セキュリティ安心相談窓口では、寄せられる相談に関して手口を実際に検証し、そこで得られた知見をその後の相談対応にフィードバックするとともに、注意喚起等、情報発信にも活かしています。
「安心相談窓口だより」では中でも多く相談が寄せられる相談内容の「手口」「対処」「対策」について、パソコンやスマートフォンの操作等にあまり詳しくない人でも理解できるように分かりやすく説明を行っています。
記事は不定期に公開されますので、「安心相談窓口だより」を定期的に確認することで、最新のネット詐欺等の手口や対策を知り、被害の未然防止に役立てることができます。
手口に関する内容以外にも、被害にあわないための日ごろから気を付けるポイントについての記事も公開しています。

映像で知る情報セキュリティ　各種映像コンテンツ
https://www.ipa.go.jp/security/videos/list.html

学習

用途・目的	動画の視聴により、情報セキュリティの脅威、手口、対策等を学ぶ
利用対象者	スマートフォンやパソコンを使用する一般利用者 組織の経営者、対策実践者、啓発者、従業員等
特 長	組織内の研修等で利用できる10 分前後の動画を公開。情報セキュリティ上の様々な脅威・手口、対策をドラマ等の動画を通じで学べる

概要

「サイバー攻撃」「内部不正」「ワンクリック請求」「偽警告」等の脅威をテーマにした動画のほか、「中小企業向け情報セキュリティ対策」「新入社員向け」「保護者／小学生／中高生向け」といった訴求対象者別の動画を公開しています。動画の視聴により、スマートフォン・パソコンを使用する際に利用者に求められる振舞いや対策を身に付けることができます。
情報セキュリティの自己研さんを目的とした個人の視聴のほか、組織内の研修用としての利用が可能です。

■動画のタイトル例
- 今そこにある脅威～組織を狙うランサムウェア攻撃～
- 今そこにある脅威～内部不正による情報流出のリスク～
- What' s BEC ？～ビジネスメール詐欺 手口と対策～
- あなたのパスワードは大丈夫？～インターネットサービスの不正ログイン対策～

索引

J

L

M

N

O

P

R

S

T

U

V

W

あ

か

さ

た

な

は

ま

ら

著作・製作　独立行政法人情報処理推進機構（IPA）

編集責任　高柳 大輔　小山 明美　涌田 明夫　白石 歩　井上 佳春
小川 隆一

執筆者　IPA
浅見 侑太　板垣 寛二　伊藤 彰朗　伊東 麻子　伊藤 吉史
井上 佳春　内海 百葉　大久保 直人　大友 更紗　小川 賢一
小川 隆一　小幡 宗宏　甲斐 成樹　金山 栄一　金子 成徳
神谷 健司　唐亀 侑久　河合 真吾　神田 雅透　黒岩 俊二
小杉 聡志　小山 明美　小山 祐平　佐川 陽一　佐藤 栄城
篠塚 耕一　白石 歩　白鳥 悦正　新保 淳　銭谷 謙吾
高塚 光幸　竹内 智子　武智 洋　田島 威史　田島 凛
丹野 菜美　近澤 武　辻 宏郷　長迫 智子　中島 健児
楢原 龍史　西尾 秀一　西村 奏一　野村 春佳　橋本 徹
長谷川 智香　平尾 謙次　福岡 尊　福原 聡　冨士 愛恵里
藤井 明宏　古居 敬大　松島 伸彰　宮本 冬美　森 淳子
安田 進　山下 恵一　吉野 和博　吉原 正人　吉本 賢樹
渡邉 祥樹

株式会社日立製作所　相羽 律子
三菱電機株式会社　神余 浩夫
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 セキュリティ危機管理チーム　満塩 尚史
株式会社 KDDI 総合研究所　三宅 優
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
情報規格調査会 JTC 1 ／ SC 27 ／ WG 5 小委員会

協力者　IPA
和泉 隆平　板橋 博之　伊藤 真一　江島 将和　大澤 淳
釜谷 誠　亀山 友彦　岸野 照明　北村 弘　栗原 史泰
桑名 利幸　古明地 正俊　塩田 英二　清水 碩人　瀬光 孝之
高見 穣　高柳 大輔　田口 聡　田村 智和　土屋 正
遠山 真　中島 尚樹　中野 美夏　西原 栄太郎　日向 英俊
松田 修平　真鍋 史明　宮崎 卓行

一般社団法人 JPCERT コーディネーションセンター　石寺 桂子
Trend Micro Incorporated　木村 仁美
長崎県立大学　島 成佳
国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所
経済産業省 商務情報政策局 サイバーセキュリティ課

おわりに

ロシア・ ウクライナ戦争の収束の兆しが見えないところに、イスラエル・ ハマス間の武力衝突が勃発した2023年。 戦場での戦闘とサイバー戦に加え、生成AIの進化や台頭によって精巧に加工された虚偽情報を用いた情報戦が繰り広げられているといいます。 一方、私達の身の回りにも本物の画像を細工したフェイクニュースや詐欺目的と思われる虚偽情報がSNS等で数多く飛び交っています。 本白書では新たに設けた「第4章　注目のトピック」に、前年に引き続き、虚偽情報拡散に関する節を設け、多くの事例について解説しています。 これに加え、AIのセキュリティについても第4章に節を設けました。IPAには2024年2月、AIを安全に利用し、 利便性を享受できるよう、AIの安全性に関する評価手法や基準の検討等を行うAIセーフティ・インスティテュート（AISI）が設置されました。今後、本白書においてもAIに関する記述は欠かせないものになりそうです。

編集子

情報セキュリティ白書 2024

変革の波にひそむ脅威：リスクを見直し対策を

2024 年 7 月 30 日　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**