情報セキュリティ白書

Information Security White Paper

2023

進む技術と未知の世界：新時代の脅威に備えよ

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2023」の刊行にあたって

2022 年を振り返ると、2 月に発生したロシアのウクライナ侵攻は、近隣諸国や支援国、そして食料やエネルギー等の経済的つながりを持つ国々にまで影響を及ぼしました。この紛争は武力戦にサイバー空間を含む情報戦を加えたハイブリッド戦と呼ばれるものとなり、関係各国はランサムウェアを始めとするサイバー攻撃や、世論誘導を意図する虚偽情報拡散等の対応に追われました。米国では CISA、FBI 等によりサイバー攻撃への注意喚起が繰り返されました。日本では、9 月に政府機関や企業のホームページ等を標的とした DDoS 攻撃と思われるサービス不能攻撃により、業務継続に影響のある事案も発生したほか、国家等が背景にあると考えられる攻撃者による暗号資産取引事業者等を狙ったサイバー攻撃や、一定の集団によるものとみられる学術関係者等を標的としたサイバー攻撃も明らかとなり、国民の誰もがサイバー攻撃の懸念に直面することとなりました。政府からも関係省庁等々の合同による注意喚起が多数出されました。

この間、国内では、ランサムウェア攻撃による大きな被害が報告されました。2 月には自動車部品工場が攻撃を受け、出荷先の工場が稼働停止しました。10 月には自治体の医療センターのサーバーが取引先の給食提供業者を経由した攻撃を受け、電子カルテシステムが利用できなくなりました。サプライチェーン全体のセキュリティ対策、事業継続計画、インシデント対応等の重要性が再認識されました。

一方政策面では、「サイバーセキュリティ 2022」「重要インフラのサイバーセキュリティに係る行動計画」「国家安全保障戦略」 等が公表され、サイバー警察局、サイバー特別捜査隊等の設置等が実施されました。6 月に閣議決定された「デジタル社会の実現に向けた重点計画」では、利便性の向上とサイバーセキュリティ確保の両立に向け、官民の緊密な連携を進めていくことが示されました。

そして、2022 年は AI への注目が集まった年でもありました。特に生成系 AI の技術的な発展は目覚ましく、ビジネスにおける業務革新等への期待が高まる一方、AI の利用による人権、プライバシー、知的財産権等の保護が課題として顕在化しました。更にウクライナ侵攻では、虚偽情報生成に AI が利用され、情報の信頼性に対する課題が深刻化しました。このような AI の課題に対して EU では、AI の安全で遵法的な利用に関する規則が策定されました。また米国も「AI 権利章典」を公開して人権や安全に配慮した AI の利用を宣言しました。

AI 利用を起点とする IT 環境の革新は、確かに大きな可能性があるようですが、セキュリティやプライバシーの脅威も大きくなると思われます。では、私達はどうすればよいのでしょうか。

まずはリスクを正しく知ることから始めましょう。何が重大なリスクなのかを特定した上で、変化に対応してセキュリティ対策の基本を継続的に実践していくとともに、未知の脅威に対しては情報共有し、適切な利用について議論を重ね、安全、安心なデジタル社会の実現を目指していくことが重要です。

本白書が、多くの方々に広く利用され、技術の進展とそれに伴う未知の脅威、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。

2023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

2023

情報セキュリティ白書

序章

2022年度の情報セキュリティの概況

2022 年はウクライナ侵攻による安全面や経済面の不安が継続する一方、生成系 AI の急激な普及等で IT 環境の革新を予感させる年となった。国内では、企業・団体におけるランサムウェア被害が増え続けた。攻撃の手口では、窃取したデータを暴露する「二重の脅迫」に加え、被害組織への DDoS 攻撃や、被害の事実を被害組織の顧客や利害関係者に連絡する等の脅迫手法も確認されている。ここ数年で被害が急増している要因として、ランサムウェア攻撃をサービスとして提供する「RaaS（Ransomware as a Service）」の普及や、攻撃者の組織化・分業化が挙げられる。2022 年 2 月の自動車部品会社へのランサムウェア攻撃では、部品供給先である自動車工場の稼働が 1 日停止した。同年 10 月の大阪市の医療センターへのランサムウェア攻撃では、VPN でつながる給食提供業者から侵入され、サーバーを介して医療センターの電子カルテシステムに障害が及んだ。同システムはバックアップが保管されていたが復旧に 2 ヵ月を要した。これらの事案から、サプライチェーン全体での脆弱性対策、データ保護、復旧計画の必要性等が再認識された。

情報漏えいの被害について、調査会社の調査によれば、漏えい・紛失事故を公表した社数、事故件数はともに 2 年連続で最多となった。2022 年 6 月には、地方自治体の業務委託先の従業員が、46 万人余りの個人情報を含む USB メモリーを紛失した。USB メモリーは回収され、漏えいの痕跡はないとされたが、記録媒体管理の重要性を再認識させられる事案であった。

個人を狙ったフィッシング等の被害については、2022 年度は通信事業者をかたる偽 SMS が減少した一方、宅配便業者や公的機関をかたる偽 SMS が増加、または新たに出現した。また、パソコン利用者に対する偽のセキュリティ警告について IPA に寄せられた相談件数は過去 4 年間で最多となった。

海外においても、様々なサイバー攻撃の脅威がより深刻になっている。米国連邦捜査局（FBI）の年次報告書によると、2022 年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 15% 増の約 27 億 4,200 万ドルであった。セキュリティベンダーが 2022 年上半期に全世界で確認した DDoS 攻撃は、過去最多となる約 602 万回で、前年同期比で 205% であった。ランサムウェア攻撃も世界中で起きており、イタリアでは地方行政機関の通信インフラのサービスが全面中断し、フランスでは病院が被害を受け手術の中止や入院患者の移送等、生活や治療に影響を及ぼす被害が報告されている。

セキュリティ政策面では、国内ではサイバー警察局、サイバー特別捜査隊等の体制面の強化、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の公開、業界ごとのサイバー・フィジカル・セキュリティ対策ガイドラインの公開等で、より実践的な対策を推進した。また、経済安全保障推進法や安全保障関連 3 文書の中でもサイバーセキュリティ対策強化の方向性が示された。

世界的には、2022 年 2 月のウクライナ侵攻以降、安全保障面の緊張、エネルギー・食料不足等で予断を許さない状況が続いている。ウクライナでの戦いは、国家間の武力攻撃とサイバー攻撃のハイブリッド戦、及びサイバー空間での情報宣伝戦が特徴となっている。サイバー攻撃について、米国はサイバー軍による諜報面のウクライナ支援、国内におけるサイバー攻撃注意喚起、大統領令 14028 に基づくサプライチェーン防御強化等を継続した。また EU は、重要インフラの統一セキュリティ規格である「NIS 2」を 2022 年 11 月に成立させた。

情報宣伝戦について、ロシアは虚偽情報を多用したが、ウクライナも SNS 等で情報を発信して対抗した。技術面では、生成系 AI の急速な発展や広告配信等の IT 基盤の普及により、虚偽情報の容易な生成・配信が可能となった。虚偽情報の識別は難しく、拡散にどう対応するかは今後の課題である。AI の関連政策として、EU は、AI の安全で遵法的な利用に関する規則「Artificial Intelligence Act」（AI 法）を公表、2023 年 6 月には生成系 AI の利用や学習に関する規制を追加した修正案を採択した。米国は 2022 年 10 月、「AI 権利章典」を公開した。欧米それぞれで人権や安全に関する AI の不適切な利用への対処に進展が見られた。

2022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
2022年 4月	● CISA、ロシアのウクライナに対するサイバー攻撃情報開示（2.2.2）	● IPA、「組織における内部不正防止ガイドライン」第5版を公開（2.8.1） ● 警察庁にサイバー警察局、関東管区警察局にサイバー特別捜査隊を新設（2.1.5）
5月		● 「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律案」成立（2.1.1） ● 第28回日EU定期首脳協議開催、デジタルパートナーシップ合意（2.2.1）
6月	● 地方自治体の業務委託先が個人情報を保存したUSBメモリーを紛失（1.2.9） ● イタリアの地方行政機関がランサムウェア攻撃でサービス停止（3.1.1）	● G7エルマウサミット開催（2.2.1） ● 「デジタル社会の実現に向けた重点計画」が閣議決定（2.1.1） ● 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」公開（2.1.1）
7月	● ENISA、ランサムウェア脅威実態を報告（2.2.3）	
8月		● 総務省、「ICTサイバーセキュリティ総合対策2022」公開（2.1.4）
9月	● 親ロシア系攻撃集団、国内組織にDDoS攻撃（1.2.4） ● 家具製造小売業の持株会社が不正アクセスを受け、約13万2,000アカウント分の個人情報が流出（1.2.9）	● IPA、ビジネスメール詐欺の特設ページを開設（1.2.3） ● EU、デジタル製品の「サイバーレジリエンス法案」公開（2.2.3） ● ISMAP-LIU運用開始（2.7.3）
10月	● 大阪府の病院にランサムウェア攻撃、電子カルテシステムに障害が発生（1.2.1） ● 入力フォーム支援サービス事業者のサービスが不正アクセスを受け、入力情報が流出（1.2.9）	● 米国、「AI権利章典」公開（2.2.3）
11月	● IPA、学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について注意喚起（1.2.2） ● 厚生労働省、医療機関等のサイバーセキュリティ対策で注意喚起（2.1.1） ● オーストラリアの保険会社の個人情報970万人分が漏えい（1.1.1）	● 経済産業省、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」公開（2.1.3） ● EUの重要インフラの統一セキュリティ規格「NIS 2」が成立（2.2.3） ● EU、AI法修正案を公開（2.2.3）
12月	● フランスの病院がランサムウェア攻撃により患者を緊急移送（3.1.1）	● 安全保障関連3文書が閣議決定（2.1.1） ● 米国、国防授権法2023成立（2.2.2）
2023年 1月	● 保険会社の委託先に不正アクセス、顧客情報が流出（1.2.9） ● 米国ソーシャルテクノロジー企業にGDPR違反で3億9,000万ユーロの制裁金（2.2.3）	● 経済産業省、「クレジットカード決済システムのセキュリティ対策強化検討会 報告書」公開（2.1.3）
2月		● 日米豪印の4ヵ国（QUAD）で連携したサイバーセキュリティ月間実施（2.1.1）
3月	● IPA、Emotetの攻撃活動再開を観測（1.2.6）	● 経済産業省、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」公開（2.1.1、2.1.3） ● IPA、「サイバーセキュリティ経営ガイドライン」改訂（2.1.3） ● 米国、新サイバーセキュリティ戦略を公開（2.2.2）

※ 2022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。ランサムウェア攻撃、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されたい。

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

2022年度は、コロナ禍でのテレワークやDX推進の取り組みが定着しつつある中、サイバー攻撃は国内外ともに増加傾向が見られた。特に、国内では、ランサムウェア攻撃やサプライチェーンが狙われたインシデントが発生し、多数の被害が報告された。

本章では、国内外で発生した主なインシデントの概要と攻撃の手口や対策の状況、脆弱性の動向等について解説する。

1.1 2022年度に観測されたインシデント状況

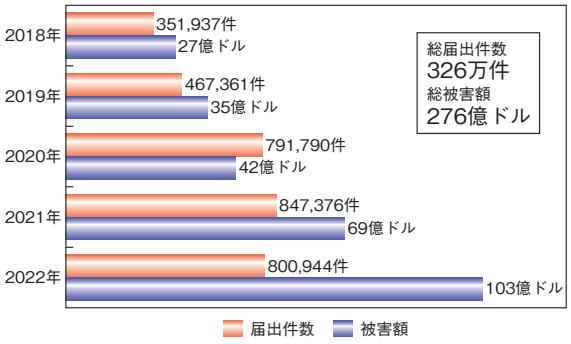
本節では2022年度に観測された世界と日本における情報セキュリティインシデントの発生状況について概説する。

1.1.1 世界における情報セキュリティインシデントの発生状況

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について、主に以下の情報セキュリティ関連の報告書を参照し概説する。

- 米国連邦捜査局（FBI：Federal Bureau of Investigation）：「Internet Crime Report 2022[※1]」
- Anti-Phishing Working Group, Inc.（以下、APWG）：「Phishing Activity Trends Reports[※2]」
- 日本アイ・ビー・エム株式会社（以下、IBM社）：「IBM X-Force 脅威インテリジェンス・インデックス 2023[※3]」
- Mandiant, Inc.（以下、Mandiant社）：「M-Trends 2023[※4]」

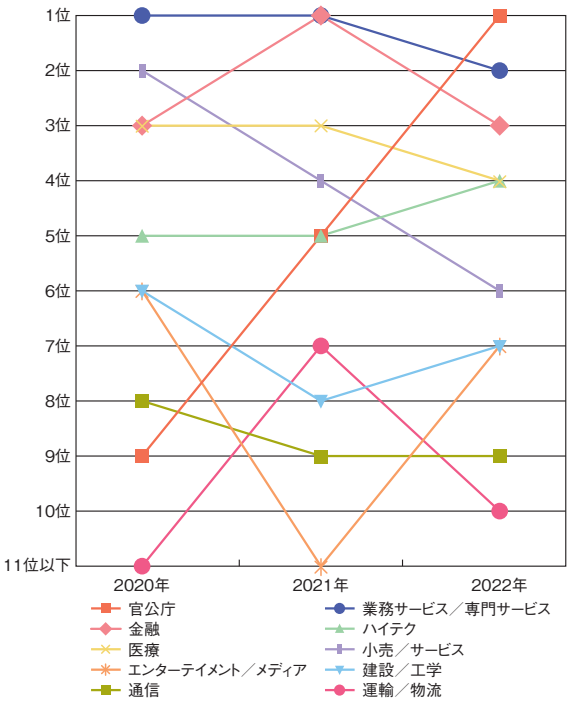
FBIによると、サイバー犯罪の件数と被害額は過去4年にわたり増加を続けてきた。2022年には件数は80万件と微減したが、被害額は大幅に増加し103億ドルとなった（図1-1-1）。



■図1-1-1　サイバー犯罪の届出件数と被害額の推移（2018～2022年）
（出典）FBI「Internet Crime Report 2022」を基にIPAが編集

（1）ウクライナ情勢によるセキュリティインシデントの急増

Mandiant社によると、全世界で標的とされている産業の各年の順位は、図1-1-2に示すように変化は大きくないが、「官公庁」は2022年には前年の5位から1位と急激に上昇している。これはMandiant社がウクライナに広範な支援を行った影響によるという。



■図1-1-2　全世界で標的とされている産業の順位（2020～2022年）
（出典）Mandiant社「M-Trends 2021[※5]」「M-Trends 2022[※6]」「M-Trends 2023」を基にIPAが編集

Microsoft Corporation（以下、Microsoft 社）の調査※7によると、2022 年 2 月 24 日のロシアによるウクライナ侵攻開始前である同年 1 月 13 日に、攻撃者が「WhisperGate」と呼ばれるワイパー型（データ破壊型）のウイルス※8をウクライナの政府機関や IT 部門へ拡散させた。同時にウクライナの政府サイトに対して同時多発的な改ざんが行われたとウクライナのセキュリティインシデント対応組織である CERT-UA（Computer Emergency Response Team of Ukraine）が発表した※9。更に 2 月 15 日には、ウクライナの軍や銀行等に DDoS 攻撃が行われた。侵攻開始前日の 2 月 23 日には、「HermeticWiper」と呼ばれるウイルスによる再度のワイパー攻撃と DDoS 攻撃が実施された。

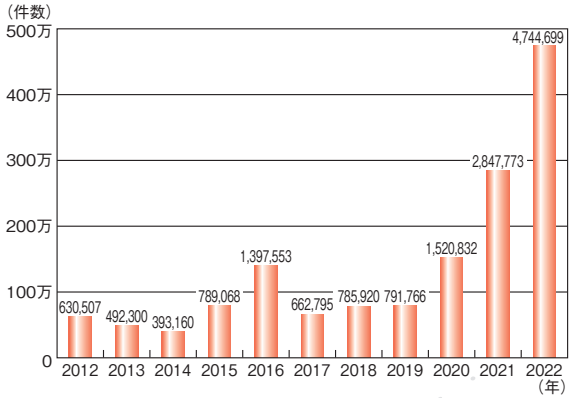
侵攻当日の 2 月 24 日には、攻撃者はヨーロッパに数万人の利用者がいる Viasat, Inc. のブロードバンド衛星インターネットサービスに対し、「AcidRain」の亜種と考えられるワイパー型ウイルスを使って、同社のシステムを破壊した。その影響はウクライナのみならず、ドイツのエネルギー企業やフランスのインターネットプロバイダー等、様々な分野に及び、2 週間以上の接続停止等が発生した（「3.1.1（1）ロシアのウクライナ侵攻に伴うサイバー攻撃」参照）。また、攻撃者はウクライナの首都キーウにある放送局へ「DesertBlade」と呼ばれるワイパー型ウイルスを送り込み、ミサイル攻撃とともに 3 月 1 日に情報発信を遮断した。

更に、NATO（North Atlantic Treaty Organization：北大西洋条約機構）加盟国であるモンテネグロの防衛省、財務省、内務省を含む政府機関に対し、2022 年 8 月 22 日、ロシアが支援していると見られる攻撃者がランサムウェアと DDoS 攻撃の両手法により攻撃を行い、電力、水道、輸送等、幅広い重要インフラにも影響を与えたという。

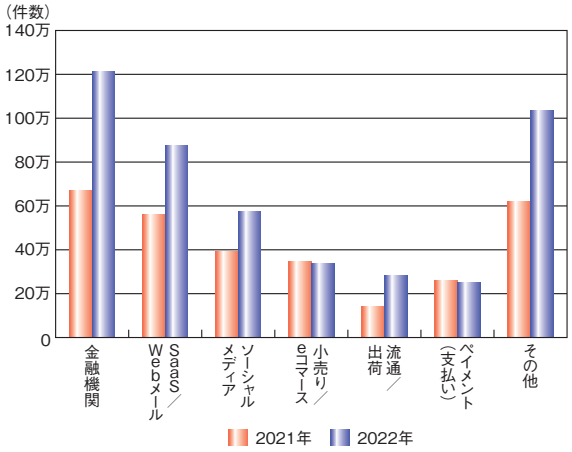
(2) フィッシングの傾向

APWG によると、2022 年に届け出されたフィッシングサイトの総数は約 474 万 5,000 件で、2021 年と比較して 66.6% 増と大幅に増加し、過去 11 年で最多となった（図 1-1-3）。

業界別のフィッシングサイト件数では、「金融機関」が最も多く、続いて「SaaS ／ Web メール」「ソーシャルメディア」と続き、その順位は 2021 年と変わっていない。一方「小売り／ e コマース」や「ペイメント（支払い）」では 2021 年よりも件数が減少しているが、「流通／出荷」で 102.7% 増という大幅な増加が認められた（図 1-1-4）。



■図 1-1-3　世界における届け出されたフィッシングサイト件数（2012 ～ 2022 年）
（出典）APWG「Phishing Activity Trends Reports」を基に IPA が作成



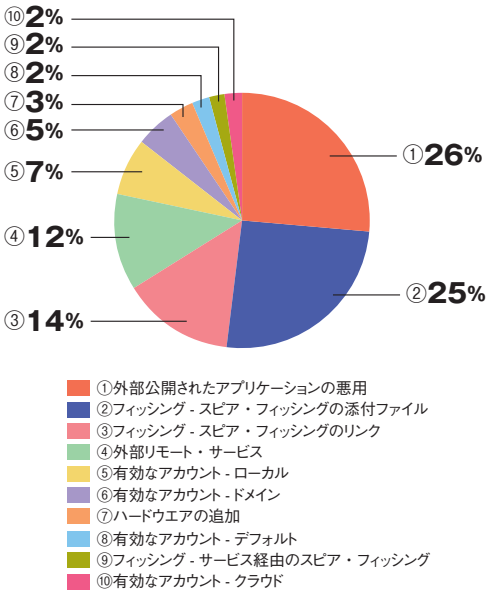
■図 1-1-4　業種別のフィッシングサイト件数（2021 年と 2022 年の比較）
（出典）APWG「Phishing Activity Trends Reports」を基に IPA が作成

(3) 侵入の手口とランサムウェア

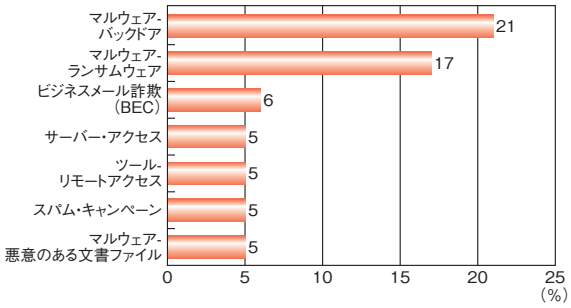
IBM 社によると、サイバー攻撃のきっかけとなる初期攻撃元を追跡した結果、「外部公開されたアプリケーションの悪用」が 26% と最も多く、次が「フィッシング - スピア・フィッシングの添付ファイル」によるものだった（次ページ図 1-1-5）。

また、攻撃者がターゲットのネットワークに対して行った具体的な行動を、目的実行方法として分類した結果によると、最も割合が多いのは「マルウェア - バックドア」で、次が「マルウェア - ランサムウェア」となっている（次ページ図 1-1-6）。

FBI の IC3（Internet Crime Complaint Center：インターネット犯罪苦情センター）に重要インフラ組織から届けられたランサムウェア攻撃の業界ごとの被害報告件数を図 1-1-7（次ページ）に示す。最も多かったのは「医療関連」で 210 件、続いて「重要分野製造業」の 157 件であった。中でも、「重要分野製造業」は 2021 年の 2.4 倍以上の件数となった。



■図 1-1-5　初期攻撃元区分の割合（2022 年）
（出典）IBM 社「X-Force 脅威インテリジェンス・インデックス 2023」を基に IPA が編集

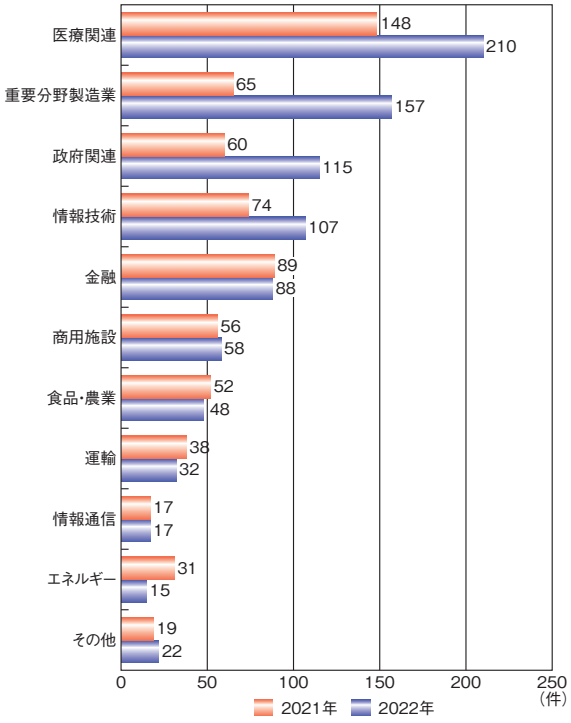


■図 1-1-6　目的実行方法の上位ランキング（2022 年）
（出典）IBM 社「X-Force 脅威インテリジェンス・インデックス 2023」

（4）情報漏えいインシデントの状況

2022 年も多くの情報漏えいインシデントが発生した。ここでは、頻繁に報じられた 3 件のインシデントについて紹介する。

- 2022 年 8 月、Twitter, Inc.（以下、Twitter 社。現、X Corp.）は、アカウントや名前等の公開情報と一部のメールアドレス等の個人情報が漏えいしたと公表した[※10-2]。これは 2021 年 12 月に Twitter の API の脆弱性を利用して窃取されたもので、その後 2023 年 1 月には 2 億人のアカウント情報が窃取されたと報じられた[※10-3]が、Twitter 社はこれを否定している[※10-4]。
- 2022 年 9 月、オーストラリアで第 2 位の規模の通信会社である SingTel Optus Pty Limited は、顧客の名前、生年月日、電話番号、電子メール、一部の顧客の住所、パスポートや運転免許証等の身分証明書番号が漏えいするインシデントが発生したと公表した[※10-5]。漏えいした 1,000 万件のアカウントのうち、



■図 1-1-7　攻撃対象となった業界ごとの被害報告件数（上位 10 業種、2021 年と 2022 年の比較）
（出典）FBI「Internet Crime Report 2021[※10-1]」「Internet Crime Report 2022」を基に IPA が編集

210 万件の身分証明書番号が公開されており、再発行が必要な可能性があるという[※10-6]。

- 2022 年 11 月、オーストラリア最大の健康保険会社である、Medibank Private Ltd. で 970 万人の名前、住所、メールアドレス等の個人情報が漏えいした[※10-7]。侵入者は身代金を要求したが、同社は支払わないと明言した。

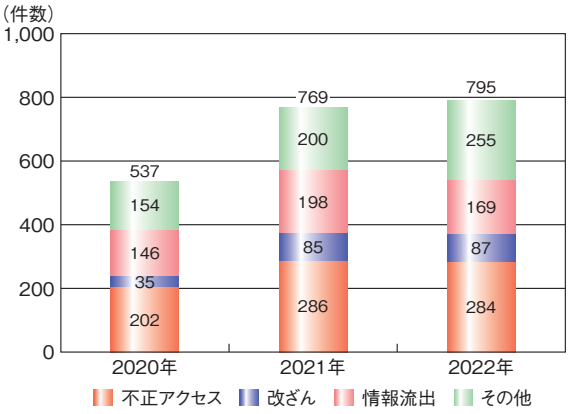
1.1.2 国内における情報セキュリティインシデントの発生状況

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。

- 三井物産セキュアディレクション株式会社（以下、MBSD 社）による集計情報[※10-8]
- 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 2023 年 1 月 1 日～2023 年 3 月 31 日[※10-9]」
- フィッシング対策協議会：「月次報告書[※10-10]」
- 警察庁：「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[※10-11]」「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[※10-12]」

(1) 情報セキュリティインシデントの発生状況

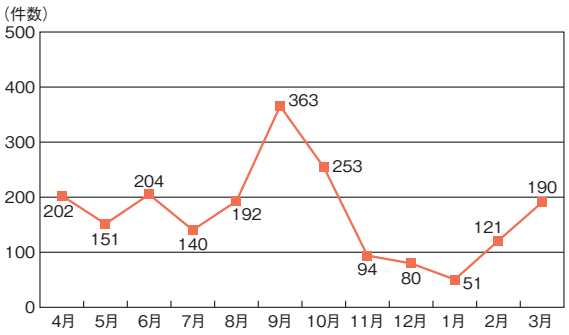
MBSD 社によれば、2022 年の情報セキュリティインシデントの種類別報道件数は全体で 795 件となり、2021 年に対し 3.4% 増であった。不正アクセス、改ざんがほぼ横ばいで、「情報流出」は前年比 14.6% 減、「その他」が 27.5% 増であった(図 1-1-8)。



■図 1-1-8 情報セキュリティインシデントの種類別報道件数
(出典)MBSD 社による集計情報を基に IPA が作成

(2) Web サイト改ざんによる被害

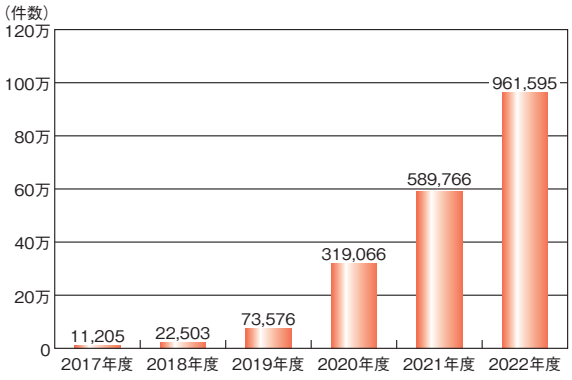
2022 年 4 月 1 日から 2023 年 3 月 31 日までに JPCERT/CC に報告された Web サイト改ざん件数は 2,041 件で、2021 年度(2,439 件)※10-13 の 83.7%であったが、2020 年度(1,351 件)※10-14 と比較すると 151% であった。月別では 9 月が 363 件と最も多かった(図 1-1-9)。



■図 1-1-9 2022 年度 Web サイト改ざん月別推移
(出典)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」を基に IPA が作成

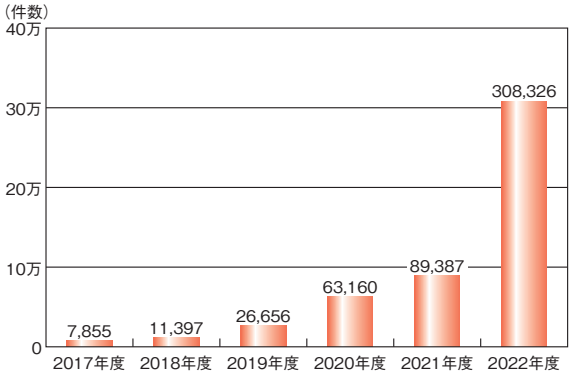
(3) フィッシングによる被害

フィッシング対策協議会への 2022 年度の報告件数は 96 万 1,595 件と前年度比 63% 増であり、2020 年度の約 3 倍、2019 年度の約 13 倍、2018 年度の約 43 倍、2017 年度の約 86 倍と、著しい増加を示している(図 1-1-10)。



■図 1-1-10 年度別フィッシング報告件数(2017 ～ 2022 年度)
(出典)フィッシング対策協議会「月次報告書」(2017 年 4 月～ 2023 年 3 月)を基に IPA が作成

図 1-1-11 にフィッシングサイトの URL 件数の年度別推移を示す。2022 年度は前年度比約 3.5 倍と顕著な増加が見られた。2022 年度の件数を 2017 年度と比較すると約 40 倍となっており、フィッシングを仕掛け、情報を詐取する手口が以前とは比較にならない程多くインターネット上に横行していることが分かる。



■図 1-1-11 フィッシングサイトの URL 件数の比較(2017～2022 年度)
(出典)フィッシング対策協議会「月次報告書」(2017 年 4 月～ 2023 年 3 月)を基に IPA が作成

また、警察庁によればフィッシング等に伴う不正送金被害の発生件数は 2021 年に前年までの 1,734 件から 584 件へ急減していたが、2022 年には再び反転し、1,136 件となったという(フィッシング被害については「2.1.5 (3)(a)サイバー犯罪の情勢」参照)。

フィッシング対策協議会のフィッシングの緊急情報の一覧※10-15 を見ると、2022 年度も金融機関やクレジットカード会社だけでなく多様なサービスが悪用されている。フィッシングにはスマートフォンの SMS (Short Message Service)からフィッシングサイトに誘導するスミッシングもあり、宅配便の不在通知、配達完了をかたり SMS から誘導する手口は、年度を通じて同協議会の月次報告書で

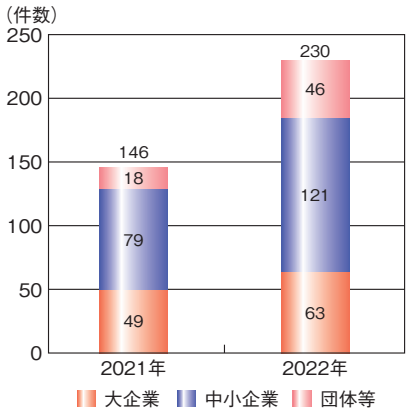
言及されていた。また、国税庁をかたり、個人情報やクレジットカード情報等の入力を促す手口について、同協議会が 2022 年 8 月から 2023 年 5 末までの間に 4 回にわたり注意喚起を実施している※10-16。IPA でも 2022 年 10 月 31 日に手口の解説とともに注意を呼び掛けた※10-17。

このほか、Google 翻訳の正規 URL からショッピングサイトやクレジットカード等のフィッシングサイトへ誘導する手口について、同協議会は 2022 年 8 月 9 日に緊急情報を発出している。この手口では URL フィルターで警告が出ないことがあるとされ※10-18、その後、2022 年 9 月、10 月の月次報告書においてフィッシングの報告が増加していることが指摘された。2023 年 1 月、2 月の月次報告書においても、この手口によるフィッシングが継続していると指摘されている※10-19。

フィッシングの増加により ID とパスワードを窃取され、スマートフォンアプリ等を介した金銭被害の急増が懸念される。フィッシングへの一層の注意が必要である。

(4) ランサムウェアによる被害

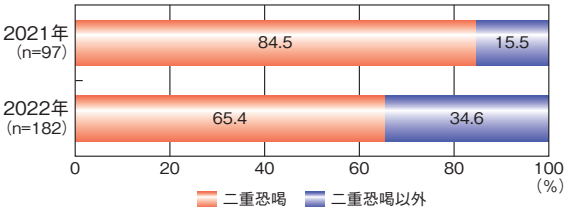
2022 年中に警察庁に報告された国内のランサムウェアによる被害は 230 件で、前年比 57.5% 増であった（図 1-1-12）。中小企業の被害件数が前年比 53.2% 増、団体等の被害件数が前年比 155.6% 増となっており、被害は企業、団体等の規模を問わず広範に及んでいることがうかがえる。



■図 1-1-12　国内のランサムウェアによる被害件数（2021 ～ 2022 年）
（出典）警察庁「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」「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」を基に IPA が作成

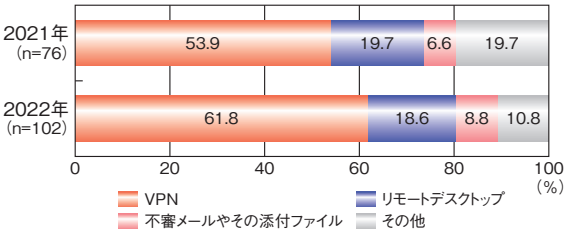
業種別で見ると、「製造業」が 32.6%（75 件）と最も多くを占め、次いで「サービス業」21.3%（49 件）、「医療、福祉」8.6%（20 件）と続く。それ以外は「卸売、小売業」「建設業」「情報通信業」がそれぞれ約 7%、「教育、学習支援業」が 6.1% と、業種を問わず被害が発生していることがうかがえる。

また手口を確認できたのは 230 件のうち 182 件であり、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 65.4%（119 件）を占めたという。「二重恐喝」の割合は 2021 年の 84.5%（82 件）より低いものの、件数は 119 件と前年比 45.1% 増となった（図 1-1-13）。



■図 1-1-13　手口別の報告件数割合（2021 ～ 2022 年）
（出典）警察庁「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」「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」を基に IPA が作成

感染経路としては、2021 年に引き続きインターネットに公開された VPN 機器等の脆弱性や強度の弱い認証情報等を悪用し、ランサムウェアに感染させる手口が多く見られたという。感染経路の有効回答を、2021 年（76 件）と 2022 年（102 件）で比較した結果を図 1-1-14 に示す。2021 年と同様に 2022 年も「VPN 機器からの侵入」の割合が最も高く、2021 年より約 8 ポイント増えている。

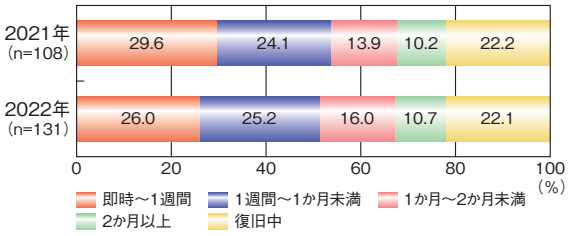


■図 1-1-14　ランサムウェアの感染経路（2021 ～ 2022 年）
（出典）警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」「令和 4 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

侵入経路とされる機器のセキュリティパッチの適用状況について、得られた 119 件の回答のうち、「最新のセキュリティパッチを適用済み」は 29.4%（35 件）、「未適用のセキュリティパッチがあった」は 54.6%（65 件）であった。またウイルス対策ソフトを導入していた被害企業・団体等 118 件のうち、ランサムウェアが検出できたのはわずか 7.6%（9 件）であった。

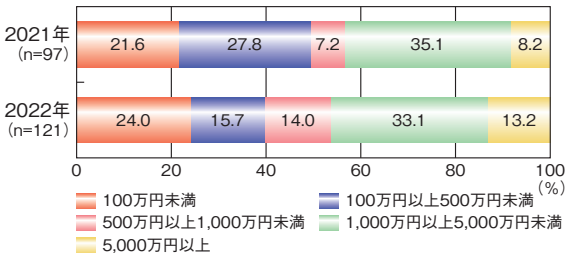
被害に遭った企業・団体等のうち有効回答が得られた 131 件について、復旧に要した期間を 2021 年の 108 件と比べてみると、「1 週間以内」の割合が約 4 ポイント減り、「1 週間～ 1 ヵ月未満」「1 ヵ月～ 2 ヵ月未満」がわ

ずかに増加している（図 1-1-15）。2022 年にランサムウェアに感染した企業・団体等のうち、復旧までに 1 週間以上かかった企業・団体等が 7 割以上あったことになる。



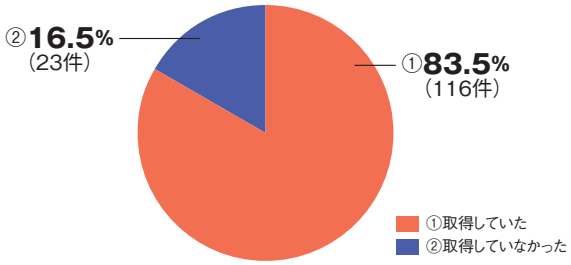
■図 1-1-15　復旧に要した期間（2021 ～ 2022 年）
（出典）警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」「令和 4 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

調査・復旧費用の総額について得られた有効回答を、2022 年（121 件）と 2021 年（97 件）で比較した結果を図 1-1-16 に示す。2021 年と同様に 2022 年も「1,000 万円以上 5,000 万円未満」の割合が最も高く、全体に占める割合に大きな変化はない。一方で「5,000 万円以上」が約 5 ポイント、「500 万円以上 1,000 万円未満」が約 7 ポイント、「100 万円未満」が約 2 ポイント増えている。逆に「100 万円以上 500 万円未満」は 12 ポイント減っている。

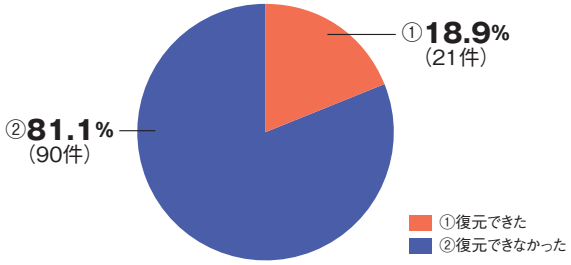


■図 1-1-16　調査・復旧費用の総額（2021 ～ 2022 年）
（出典）警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」「令和 4 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

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有効回答（139 件）の結果を図 1-1-17 に示す。取得していたバックアップから復元を試みた 111 件の復元結果を図 1-1-18 に示す。83.5% がバックアップを取得していた一方で、復元できたのは 18.9% に過ぎない。



■図 1-1-17　バックアップ取得の有無（2022 年、n=139）
（出典）警察庁「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」を基に IPA が編集



■図 1-1-18　バックアップからの復元結果（2022 年、n=111）
（出典）警察庁「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」を基に IPA が編集

2022 年中にランサムウェア被害を警察庁に報告した被害企業・団体等（有効回答数 140 件）のうち 12.9%（18 件）がすべての業務の停止に追い込まれており、ランサムウェア被害は事業継続を困難にし、サプライチェーンにも多大な影響を及ぼしかねない。感染被害を引き起こさないためにも、修正プログラムの適用等の基本的対策の実施はもとより、手口の理解、万が一侵入された場合に備えた対策の準備が必要である。これらについては「1.2.1 ランサムウェア攻撃」を参照されたい。

COLUMN

情報セキュリティ10大脅威 2023
～全部担当のせいとせず、組織的にセキュリティ対策の足固めを～

IPAが毎年発表している情報セキュリティ10大脅威。2023年版では「個人」向けと「組織」向けの脅威どちらも、昨年はランク外であった脅威が10位に入り、以下の表に示す順位になりました。これらは新しい脅威ではなく、いずれも2018年にはランクインしていました。このことから、ランク外になったとしても脅威がなくなったのではなく、その年は「他の脅威より目立たなかっただけ」と言えます。つまり、被害に遭うリスクは存在し続けており、対策が不十分であればリスクはより高まります。

情報セキュリティ10大脅威 2023「個人」・「組織」向け脅威の順位

「個人」向け脅威	順位	「組織」向け脅威
フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害
ネット上の誹謗・中傷・デマ	2	サプライチェーンの弱点を悪用した攻撃
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3	標的型攻撃による機密情報の窃取
クレジットカード情報の不正利用	4	内部不正による情報漏えい
スマホ決済の不正利用	5	テレワーク等のニューノーマルな働き方を狙った攻撃
不正アプリによるスマートフォン利用者への被害	6	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
偽警告によるインターネット詐欺	7	ビジネスメール詐欺による金銭被害
インターネット上のサービスからの個人情報の窃取	8	脆弱性対策情報の公開に伴う悪用増加
インターネット上のサービスへの不正ログイン	9	不注意による情報漏えい等の被害
ワンクリック請求等の不正請求による金銭被害	10	犯罪のビジネス化（アンダーグラウンドサービス）

また、脅威は単独ではなく複数が組み合わされる場合もあります。例えば「個人」向け脅威でランクインしている、「フィッシング」によって詐取された認証情報で「スマホ決済の不正利用」や「インターネット上のサービスへの不正ログイン」をされることがあります。また「組織」向け脅威でランクインしている、自組織の「サプライチェーン」に含まれる取引先等の関連組織が「ランサムウェア」の被害に遭い、最終的に自組織も被害を受けるような事例も発生しています。

組織においては特に、担当者や外注先任せとはせずに、役員等の組織上層部が中心となって対策を行うことが大切です。また、自組織に関係する他組織も含めた対策も必要になっています。関係する組織とともに自組織を取り巻く脅威にはどんなものがあるのか？　その対策は何をすればよいのか？　今一度、確認してみましょう。

前述した複数の脅威が組み合わされる状況から、「情報セキュリティ10大脅威 2023」では複数の脅威に有効な対策をまとめた「セキュリティ対策の基本と共通対策」を新しく公開しています。毎年公開している「解説書」と、社内教育や研修に使えるスライド形式の「簡易説明資料」等も以下のURLからダウンロードできます。併せてご活用ください。

https://www.ipa.go.jp/security/10threats/10threats2023.html

1.2 情報セキュリティインシデント、手口、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、2022 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り、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使用不能にするウイルスの総称である。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できるよう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、ばらまき型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。

また、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。

(1) ランサムウェア攻撃の傾向

ここ数年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) 被害件数と増加要因

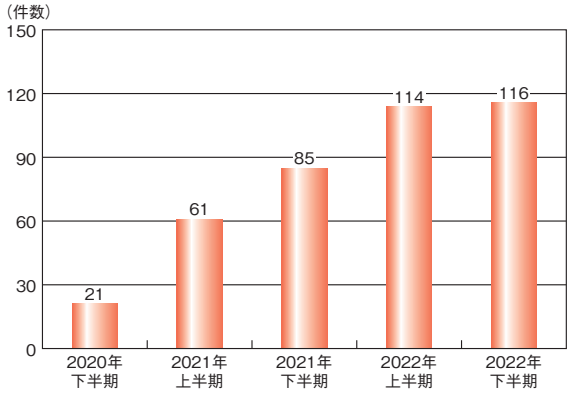
警察庁の調査結果※11 によると、企業・団体等におけるランサムウェア被害の報告件数が 2022 年上期は 114 件、下期は 116 件であり、2020 年下期から継続して増え続けている（図 1-2-1、その他の調査結果については「1.1.2(4) ランサムウェアによる被害」参照）。

ここ数年でランサムウェア被害が急増している要因として、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や、攻撃者の組織化・分業化が挙げられる。世界的に多くの被害が確認されている攻撃グループ LockBit、Conti、BlackCat 等は、より大きな報酬を得ながら効率的にランサムウェア攻撃を行うために、次のような分業体制（RaaS モデル）を敷いているという※12。

- オペレーター（RaaS 提供者）
  被害組織のデータを暗号化するためのランサムウェアを開発し、アフィリエイターへ提供する。オペレーターによっては、攻撃方法や被害組織との交渉方法等をマニュアル化し提供する組織もある。
- アクセスブローカー（IAB：Initial Access Broker）
  被害組織のネットワークへ侵入するために必要なアクセス情報を不正に入手し、アフィリエイターへ提供する。
- アフィリエイター
  提供されたアクセス情報とランサムウェアを用いて、被害組織に対しランサムウェア攻撃を実行する。

このような分業化によって、アフィリエイターはランサムウェア攻撃を構成する要素（ランサムウェアの開発、サーバー等の攻撃基盤の運用、脅迫や交渉等）すべてに関する技術・ノウハウを持たなくても、攻撃による報酬を得ることができるため、アフィリエイターの数が増加し、ランサムウェア攻撃の被害も増えたと考えられる。

また、働き方改革や新型コロナウイルスへの対応に伴う「テレワークの普及」も、ここ数年でランサムウェア被害



■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 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※11」を基に IPA が編集

が急増したもう一つの要因といえる。警察庁によれば、攻撃者による被害組織のネットワークへの侵入手口は2022年も継続して、テレワーク等に利用されるVPN製品やリモートデスクトップサービスの設定不備、脆弱性の悪用等が多く、全体の80％以上を占めていた※11。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。

(b) 被害を受けた企業・組織

セキュリティベンダーの調査によると、被害組織について、製造業や医療等の様々な業種や公共機関で被害が確認されている※13。また、警察庁によると、企業・組織の規模も大小を問わず広範に及んでおり、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が狙われ、サプライチェーン全体が影響を受ける被害や、国内企業の海外子会社が狙われるといった被害も確認されている※11。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) 身代金要求の手口

警察庁によると、身代金の支払いを促すための脅迫の手口において、二重の脅迫が行われた被害は、手口が確認できている182件のうち65%を占めていた※11。

更に、近年のランサムウェア攻撃においては、攻撃者は窃取したデータを暴露するといった「二重の脅迫」だけにとどまらず、被害組織へのDDoS攻撃（「三重の脅迫」とも呼ばれる）※14や、被害に遭った事実を被害組織の顧客や利害関係者に連絡する（「四重の脅迫」とも呼ばれる）といった脅迫手法※15も確認されているという。

(2) ランサムウェア攻撃の被害事例

2022年度に公表または報道された国内における侵入型ランサムウェア攻撃の被害事例として、次の二つの事例を紹介する。両事例ともにサプライチェーンに存在する脆弱性が悪用されたことにより、サプライチェーン上の別の企業・組織に被害を及ぼした事例である。なお、紹介する二つの事例は、数多く確認されているランサムウェア攻撃による被害の一部である。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※16」の「2-2. 身代金を要求するサイバー攻撃の被害」を参照していただきたい。

(a) 自動車部品メーカーにおける被害事例

トヨタ自動車株式会社（以下、トヨタ自動車）は、取引先が侵入型ランサムウェア攻撃を受けたことから、国内全14工場28ラインの稼働を2022年3月1日に停止すると発表した※17。攻撃を受けたのは、トヨタ自動車の部品仕入先である小島プレス工業株式会社（以下、小島プレス工業）であり、小島プレス工業は同日、ウイルス感染被害によるシステム停止事案が発生したことを公表した※18。次いで、2022年3月31日、調査報告書にて被害の内容や原因等を公表した※19。

同調査報告書や報道によると、2022年2月26日、攻撃者によって、小島プレス工業の子会社が利用するリモート接続機器の脆弱性が悪用され、子会社の社内ネットワークに侵入された。更に、子会社のネットワークから小島プレス工業の社内ネットワークに侵入され、サーバーやパソコンに保管されていたデータが暗号化されたという※20。暗号化被害は、給与支払い等の総務部門のシステムや部品の生産に関わる受発注システムにまで及んでいたとされている※21。攻撃者によって身代金を要求する内容の脅迫文が残されていたが、要求には応じていないという※20。また、調査報告書の公表時点において、攻撃者により、外部へ情報が持ち出された痕跡は確認されていないとしている※19。なお、小島プレス工業のシステムの安全が確認されたため、トヨタ自動車は停止していた工場の稼働を翌3月2日から再開した。

本事例の攻撃者は「RobbinHood（ロビンフッド）」と呼ばれる攻撃グループとみられ、国内では過去に被害が確認されていないランサムウェアが使用されたと報じられている※22。トヨタ自動車は、攻撃に使用されたランサムウェアの詳細な挙動が不明であるため、入念に対応を検討する必要があると判断し、早期復旧を断念したとしている※21。

(b) 医療機関における被害事例

大阪市の地方独立行政法人大阪府立病院機構大阪急性期・総合医療センター（以下、同院）は、2022年10月31日、侵入型ランサムウェア攻撃と思われる攻撃により、電子カルテシステムに障害が発生したとことを公表した※23。その後、2023年3月28日、調査報告書にて被害の内容や原因等を公表した※24。

障害は、同院内のサーバーがランサムウェアに感染したことが原因であった。感染したサーバーには、「すべてのファイルを暗号化した。復号したければビットコインを支払え」という旨の英語の脅迫文が残されており、連絡

先のメールアドレスも記されていた。同院では、脅迫文に記載された連絡先への連絡は行わず、交渉に応じない方針とした※25。

残された脅迫文の情報から、攻撃に用いられたランサムウェアは、「Phobos（フォボス）」と呼ばれる攻撃グループが使用する「Elbie（エルビー）」である可能性が高いとしている※24。

同院は被害拡大防止措置として、電子カルテシステム及び関連するネットワークシステムを停止した。それに伴い、緊急以外の手術や外来診療等の通常診療を停止することとなった※26。システム障害後は電子カルテが使えないため、暫定的に紙カルテで対応を行った。電子カルテシステム以外にも、連携していた会計や薬の処方のためのシステムにも影響が及んだという※27。同院内でランサムウェア感染が確認されたサーバーは20台程度であった※24。

政府から派遣された専門チームの調査の結果、攻撃者は、同院が委託していた給食提供業者である社会医療法人生長会のシステムを経由して侵入した可能性が高いと見られている※28。攻撃者は、初めに給食提供事業者のデータセンターにあるVPN製品の脆弱性、または漏えいにより公開されていた認証情報を悪用し、外部から当該データセンターへ侵入したとされている※24。当該VPN製品は、リモートメンテナンス用に利用されており、被害発生当時、必要なソフトウェアの更新が行われていなかったという。

その後、攻撃者は、給食提供業者のサーバーから、同院内の栄養給食管理システムサーバーを侵害したのち、イントラネットに侵入したと見られている。同院では、給食をオーダーするため、同院のイントラネットと給食提供業者のデータセンターをVPNによる閉域網で接続していた※29。また、給食提供業者のサーバーから同院内の栄養給食管理システムサーバーに対して、リモートデスクトップによる接続が常時行われていた（図1-2-2）。

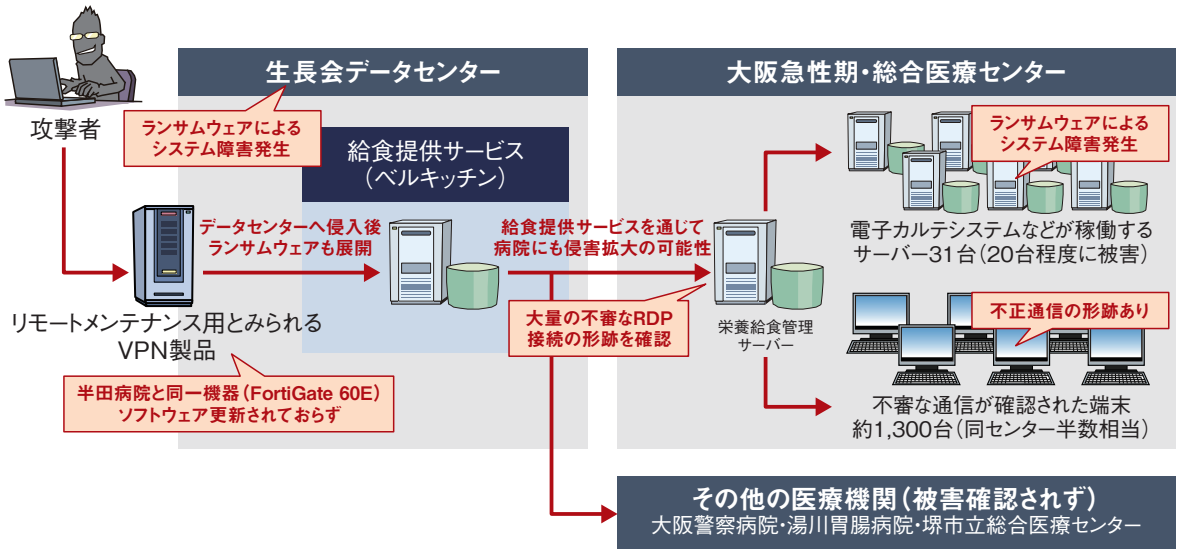
同院では、電子カルテのデータを、日次で差分バックアップ、週次でフルバックアップを取得していた。本事案ではバックアップサーバーも被害に遭ったが、遠隔地で磁気テープによるバックアップも取得しており、10月27日時点でのバックアップが無事だったという※29。同院は、このバックアップを元に段階的に復旧作業を進めた。完全復旧は2023年1月11日となり、攻撃を受けてから2ヵ月以上にわたり影響を受けることとなった。

(3) 侵入型ランサムウェア攻撃の手口

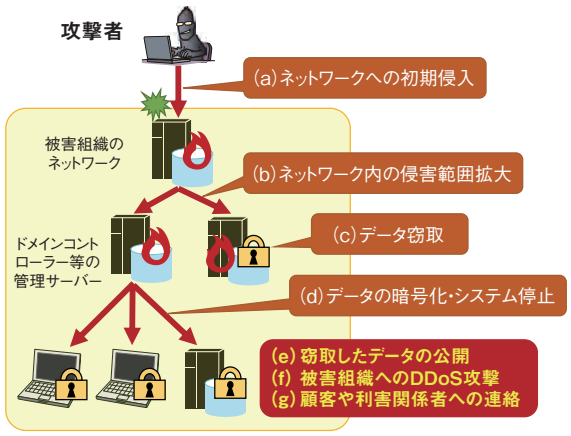
ここでは、侵入型ランサムウェア攻撃の手口について説明する。侵入型ランサムウェア攻撃は、次の(a)～(e)の五つのステップで行われる。加えて、近年確認されている手口として(f)と(g)の二つを説明する（次ページ図1-2-3）。

(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



■図1-2-2　大阪急性期・総合医療センターが受けたと見られる攻撃の流れ
（出典）piyolog「ランサムウエア起因による大阪急性期・総合医療センターのシステム障害についてまとめてみた※30」を基にIPAが編集



■図 1-2-3　侵入型ランサムウェア攻撃の手口のイメージ
（出典）IPA「【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について※31」を基に編集

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。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行う。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可能性がある※16。

(c)データ窃取

データの窃取は、攻撃者が「二重の脅迫」を狙っている場合に行われる。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・システム停止

攻撃者は、身代金を得るために被害組織のデータをランサムウェアによって暗号化し、事業継続に関わる重要なシステムの停止を狙う。バックアップデータによる復旧を妨害するため、バックアップデータも狙って暗号化する可能性がある。また、セキュリティ製品による検知を回避するために Windows OS の標準機能である BitLocker を悪用して暗号化を行う等、OS の正規の機能が悪用されることもある※16。

(e)窃取したデータの公開

窃取したデータの公開は、攻撃者が「二重の脅迫」を狙っている場合に行われる。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※32）での公開やオークション形式での販売が挙げられる。攻撃者は窃取したデータをリークサイトで公開する際に、被害組織への身代金支払いの圧力を高めるため、窃取したデータを一度にすべて公開するのではなく、一部だけ公開し、指定した期日までに身代金を支払わないと、徐々に公開するデータの範囲を広げるといった声明を出す場合がある。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。

(f)被害組織への DDoS 攻撃

被害組織への DDoS 攻撃は、攻撃者が「三重の脅迫」を狙っている場合に行われる。攻撃者は、被害組織に対して DDoS 攻撃を行い被害組織が提供するサービスを妨害することで、身代金の支払いに更なる圧力をかけるという※14。

(g)顧客や利害関係者への連絡

顧客や利害関係者への連絡は、攻撃者が「四重の脅迫」を狙っている場合に行われる。攻撃者は、被害組織がランサムウェア被害に遭ったことを被害組織の顧客や利害関係者へ連絡することで、身代金の支払いを促すという※15。

(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)バックアップの取得と復旧計画

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バックアップからの復旧計画を事前に策定する。特に、バックアップは取得するだけでなく、リ

ストアのテストを定期的に行う等をして、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。

また、侵入型ランサムウェア攻撃では、バックアップサーバーがオンライン上に存在する場合、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、事業継続に重要なデータやシステムのバックアップは複数取得し、そのうち最低一つは、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。オンライン環境にバックアップを保存する場合は、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。侵入型ランサムウェア攻撃を受けた場合でも、必ず復旧が可能なように複数のバックアップ方式を採用しておくことが重要である。

なお、バックアップからの復旧を事業継続計画（BCP：Business Continuity Plan）で策定している企業・組織でも、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ため、今一度、計画を見直していただきたい。例えば、「1.2.1(2)(b)医療機関における被害事例」では、災害時を想定してBCPを策定していたが、本事例のようなサイバー攻撃を受けることは想定しておらず、備えが不十分だったとしている※33。BCPの中で、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。

(b)ネットワークへの侵入対策

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。また、誤ってインターネット上に公開している機器等がないか確認することや、どの機器をどのような設定で公開しているか等の管理を行うといった対策も重要といえる。
- 脆弱性対策
  脆弱性を悪用した侵入や侵害範囲の拡大を防ぐために、VPN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、注意が必要である。また、脆弱性が公開されてから悪用されるまでの期間が短くなっていることから、公開された脆弱性対策情報に迅速に対応できるような体制や計画を整備しておくことも重要といえる。
- 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、推測されにくい強固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、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。

(c)侵害範囲拡大への対策

攻撃者によって、社内ネットワークへ侵入された場合を想定して、侵害範囲を最小限に抑えるために、次のような対策が重要である。なお、「(b) ネットワークへの侵入対策」と同様に、「脆弱性対策」「アクセス制御と認証の強化」を行うことも侵害範囲拡大の対策として有効である。

- 必要最小限の権限付与
  攻撃者によって、ネットワーク内のパソコンやサーバー等で利用しているアカウントが乗っ取られた場合、そのアカウントで行える操作権限が攻撃者によって悪用される可能性がある。そのため、攻撃者によってアカウ

ントが乗っ取られる可能性を考慮し、アカウントに付与する操作権限を必要最小限にすることが重要である。また、どのアカウントにどのような権限を付与しているのかを管理することや、権限昇格の脆弱性が悪用されないように脆弱性対策を実施することも重要である。

- パスワードの管理
  ネットワーク内の複数の機器において、一つのパスワードを使いまわしていた場合、攻撃者によって一つの機器の認証が突破されると、そのパスワードを使いまわしているすべての機器の認証も突破され、侵害範囲が拡大する可能性がある。このため、パスワードの使いまわしを行わないことが重要である。また、総当たり攻撃や辞書攻撃に対抗するため、パスワードポリシーを設定し、脆弱なパスワードを設定できないようにするといった対策も重要といえる。
- 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接続や他組織とのネットワーク接続において、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、ネットワーク経由で自拠点の中枢が侵害される可能性がある。そのため、各ネットワークの接続点では、アクセス制限や不正通信の監視等のセキュリティ強化を検討する必要がある。
- ドメインコントローラーのセキュリティ強化
  Active Directory 等により構成したドメインコントローラーは、ネットワーク内のユーザーやコンピューターを一元管理できるため、侵害範囲を拡大する目的で、攻撃者に狙われやすい傾向にある。攻撃者によって、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可能性があるため、脆弱性対策、強固なパスワードの使用、侵害検知装置の設置・強化等、侵害されないための対策を行うことが重要である。
- セキュリティソフトの導入
  侵入型ランサムウェア攻撃に伴うウイルスを検知・駆除するためにセキュリティソフトを導入することが重要である。なお、新しいウイルスを検知・駆除するためは、セキュリティソフトを最新の状態に保つ必要がある。ただし、侵入型ランサムウェア攻撃に使用されるウイルスは、標的とする組織向けにカスタマイズされている場合もあり、セキュリティソフトでは検知されない可能性もあるため、不審な動作や通信を監視するEDR（Endpoint Detection and Response）等の他の対策と併用することが望ましい。
- 正規プログラム・ツールの悪用への対策
  攻撃者によって、OS の正規プログラムやツール、本来は正当な目的で使用されるフリーソフト等が悪用された場合、セキュリティソフトによって検知することは困難である。そのため、業務上不要なツールの機能に制限を設けることや、使用許可のないフリーソフトをインストールできないようにすることが重要である。また、日頃からサイバー攻撃に関する脅威情報を収集し※34、攻撃者に悪用される可能性がある正規プログラムやツール※35を把握することは、利用制限を設ける際の判断材料にもなるため、可能であれば取り組んでいただきたい。

（d）データの窃取と公開への対策

侵入型ランサムウェア攻撃によりデータが窃取され、意図せず公開される脅威への対策として、IRM（Information Rights Management）※36を活用し、重要なデータが窃取されても被害を限定的な範囲に留めるといった対策が有効である。また、メール送受信やWeb 閲覧等で使用する一般的な業務用のネットワークと機密情報等を取り扱うネットワークを分離するといった対策も有効である。このような対策を行うことにより、攻撃者に業務用のネットワークに侵入されたとしても、機密情報等を取り扱うネットワークには到達されないようにすることができる。ただし、ネットワーク分離は運用コストの増加や利便性の低下等の影響があるため、機密情報等の重要性やリスクを踏まえて実施を検討することが望ましい。

（e）インシデント対応

侵入型ランサムウェア攻撃の被害に遭った際のインシデント対応はケースバイケースとなるが、標的型攻撃と同様の手口が使用されるため、対応も全体的には標的型攻撃と同様であるといえる（「1.2.2（5）標的型攻撃への対策」参照）。インシデント対応の一般的な進め方について、JPCERT/CC がマニュアル※37を公開しているため、参照していただきたい。また、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※38を公開しているため、こちらも参照していただきたい。なお、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。

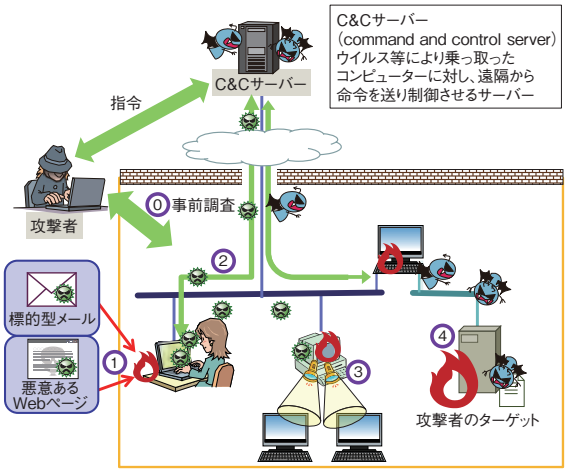
侵入型ランサムウェア攻撃によるインシデントは、業務

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、特定の企業・組織や業界が持つ機密情報の窃取やシステム・設備の破壊・停止といった、明確な目的をもって行われる。この目的を達成するため、標的とする企業・組織（以下、標的組織）向けに特別に改変・開発したウイルスを使うことがある※39。また、標的型攻撃は長期間継続して行われることが多く、標的組織の内部に長期間潜伏して活動するという特徴も持つ。

IPA では、過去の事例等から、標的型攻撃の流れを 5 段階に分類している（図 1-2-4）。



0 [事前調査段階]
標的組織を攻撃するための情報を収集する。

1 [初期潜入段階]
標的型攻撃メールや、Webサイト閲覧を通してウイルスに感染させる。

2 [攻撃基盤構築段階]
侵入したパソコン内でバックドアを作成し、外部のC&Cサーバーと通信を行い、新たなウイルスをダウンロードする。

3 [システム調査段階]
情報の存在箇所特定や情報の取得を行う。
攻撃者は取得情報を基に新たな攻撃を仕掛ける。

4 [攻撃最終目的の遂行段階]
攻撃専用のウイルスをダウンロードして、攻撃を遂行する。

■図 1-2-4 標的型攻撃の流れ
（出典）IPA「標的型攻撃／新しいタイプの攻撃の実態と対策※40」を基に編集

以下に、図 1-2-4 の標的型攻撃の流れについて概要を示す。なお、具体的な標的型攻撃のメカニズムについては IPA の「標的型攻撃／新しいタイプの攻撃の実態と対策」「標的型サイバー攻撃の事例分析と対策レポート※41」を参照いただきたい。

「事前調査段階」では、標的組織や業界の情報を収集する。公開されている情報を収集するだけでなく、標的組織と他の組織とのメールの盗聴等により必要な情報を収集することもある。

次の「初期潜入段階」では、「事前調査段階」で得られた情報を基に、標的組織の端末へのウイルス感染を試みる。海外拠点や取引先組織といった、サプライチェーン上のセキュリティの弱い組織を狙う手口に加え、VPN 製品や Web サーバー等のインターネットとの境界にある装置の脆弱性を悪用し、侵入する手口もある。標的組織の職員に対し、ウイルスを仕込んだファイルが添付された、あるいはウイルスをダウンロードする URL リンクが記載された標的型攻撃メールや SNS（Social Networking Service）によるメッセージを送り付ける手口も依然として確認されている。

「初期潜入段階」で標的組織の内部に侵入した攻撃者は、「攻撃基盤構築段階」へと移り、標的組織内の端末を遠隔操作するため、遠隔操作ウイルス（RAT：Remote Access Trojan）に感染させることを試みる。この際に、複数の RAT に感染させる場合がある。これは一つの RAT が発見され駆除や通信の遮断といった対応をされても、別の RAT での遠隔操作が継続可能なようにするためである。また、発見されないようにするため、より隠密性の高いウイルス（ファイルレスマルウェア※42 等）を使うケースも確認されている。攻撃者は遠隔操作が可能な状態を長期的に持続させるため、このような試みを複数行う。

次の「システム調査段階」では、「攻撃基盤構築段階」で感染させた RAT を使用して、組織内ネットワークの攻撃に使うウイルスやツールを送り込む。ツールは本来、攻撃以外の正規の目的を持つプログラムであるが、攻撃者にとっても有用なものは、悪用されてしまうケースがある。これらのウイルスやツールを用いて、組織内ネットワークの調査、管理者権限の奪取、目的とする情報の探索等を行う。このとき、侵入した端末等にインストールされている標準的なアプリケーションや業務でよく利用されるアプリケーションが悪用されることもある。

「攻撃最終目的の遂行段階」では、攻撃者は、目的とする情報の窃取等を行う。海外の事例では、情報の窃

取ではなく、国家間の事情を背景としたシステム破壊を目的とするインフラ攻撃等も確認されている※43。

(1) 国内の標的型攻撃事例

本項では、2022年度に確認された2件の標的型攻撃の事例を紹介する。

(a) メールのやり取りをする中で不正なファイルを実行させる攻撃

IPAのJ-CRAT（Cyber Rescue and Advice Team against targeted attack of Japan：サイバーレスキュー隊）は、国内の学術機関のエネルギー政策関係者等を標的とする攻撃（Op.EneLinkと呼称）を観測した※44。この攻撃は、標的組織に関係のある実在する組織や関係者を詐称した上で、イベント等の参加、取材、講演依頼等を持ち掛ける流暢かつ丁寧な日本語で書かれたメールから始まる。メールのやり取りの中でURLリンクを提示し、不正なファイルをダウンロード・実行させる。その後も日程調整等のやり取りを継続するが、新型コロナウイルス等を理由に依頼をキャンセルし、被害者に不信感を抱かせないように終了する。この攻撃で用いられるメールは、なりすます対象に似せたドメインを取得し、なりすます対象者を模したメールアドレスから送付されていることが確認されている。また、メールの宛先は組織のメールアドレスだけでなく、職員がプライベートで利用しているメールアドレスも対象となっていた。初期侵入の数日から十数日後には、ウイルスを用いて、端末内のドキュメントファイル等を窃取する動きが見られた。このウイルスは、オンラインストレージサービスの機能を悪用して、端末から窃取したファイルのアップロードと、攻撃者からの命令文を端末にダウンロードする動作を行うものであった。

この攻撃者グループによるものと考えられている一連の攻撃に関して、複数のセキュリティベンダーからも調査結果等が公開されている。NTTセキュリティホールディングス株式会社は、侵入テスト向けのオープンソースソフトウェア（OSS：Open Source Software）を悪用している可能性に言及している※45。株式会社マクニカは、Go言語で開発されたウイルスが使われていて解析が困難※46であったことを報告している※47。トレンドマイクロ株式会社（以下、トレンドマイクロ社）は、攻撃者を「Earth Yako」と呼び、短い期間内で新たなウイルスやその亜種を使用していること、攻撃の対象業種を頻繁に変更・拡大していることを指摘している※48-1。加えて、J-CRATでは、標的とする業種やプライベートで利用するメールアドレスを対象とした攻撃手法等、Op.EneLinkと共通点のある「LODEINFO」と呼ばれる諜報用ウイルスを用いた攻撃を観測している。トレンドマイクロ社も、同様の攻撃を観測しており、LODEINFOが断続的なバージョンアップ等、活発な標的型攻撃を行っているとしている※48-2。

このような攻撃について、警察庁と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）は、注意喚起を行っている※49。

(b) 境界装置の脆弱性を悪用した攻撃

2022年5月、ネットワーク境界に設置されるロードバランサー装置であるF5, Inc.社製のBIG-IPの脆弱性（CVE-2022-1388）が公表された※50。この脆弱性は、APIを使ってBIG-IPを管理するためのプログラムの一つであるiControlRESTコンポーネントにおいて、本来は必要な認証を回避して、リモートから任意のコードを実行できるというものであった。

同年5月ごろ、JPCERT/CCは、この脆弱性を悪用して、国内の組織への侵入を試みた事例を確認したという※51。本事例では、この脆弱性が悪用されてBIG-IP機器内部へ侵入され、BIG-IP内のデータが漏えいする被害が確認されている。本脆弱性を悪用する攻撃コードが設置されていた攻撃者のサーバーから、今回の攻撃コードとは別に、TSCookie、Bifrose等のウイルスが発見された。これらウイルスは、標的型攻撃グループ「BlackTech」が使用することで知られているため※52、本事例はBlackTechに関連のある活動と推測されている。J-CRATが収集した情報からは、攻撃に使用するためのインフラは活動が活発化する以前から段階的に整備・更新されていることや、当該脆弱性が公開されてからすぐに活動が活発化していることが見られたという。このことからJ-CRATでは、攻撃グループは常に攻撃準備を整えており、脆弱性情報に即応する体制を敷いていると推察している※44。

(2) 標的型攻撃の傾向

日本国内の企業・組織を対象とした標的型攻撃は、2011年に複数の重工業メーカー等が標的となった事例以降、継続的に発生している※41。

本項では、初期侵入と攻撃手法の傾向について述べる。まず、初期侵入では2022年度は2021年度と変わらず、標的型攻撃メールやSNSの悪用、ネットワーク境界装置からの侵入、サプライチェーン・海外拠点からの侵入が行われている。「1.2.2 (1) (a) メールのやり取りをする中で不正なファイルを実行させる攻撃」で紹介したよ

うに、組織で使うメールアドレスだけではなく、プライベートのメールアドレスにも標的型攻撃メールが届く事例が報告されている。組織が付与しているものと比較して防御が緩むと考えられるプライベートのメールアドレスやSNSアカウントを狙う攻撃は、近年の標的型攻撃の特徴である。

続いて攻撃手法の傾向としては、Go言語で開発されたウイルスの使用が挙げられる。過去にGo言語で開発されたウイルスを使った攻撃は確認されており、2022年度もGo言語で開発されたウイルスを使った標的型攻撃の事例が見られた※53。前項で述べたとおり、Go言語で開発されたウイルスの解析は難度が高い。このため、攻撃者からみれば、ウイルス解析に時間をかけさせ、標的組織側の対処を遅らせることが可能という利点があると考えられる。また、Go言語では、マルチプラットフォーム向けに開発可能であり、感染させる端末の対象を増やすことができる。このような特徴から今後もGo言語で開発されたウイルスを使用する攻撃が継続する可能性がある。

(3) 標的型攻撃の手口(初期潜入段階)

初期潜入段階における、標的型攻撃で用いられる代表的な手口を以下に示す。

(a) 標的型攻撃メール

攻撃者は、標的とする企業・組織・業界でよく用いられる用語を使用し、標的型攻撃メールの信憑性を高めることで、添付ファイルの実行または悪意のあるファイルのダウンロードを行わせるソーシャルエンジニアリングの手口を使う。標的型攻撃メールの信憑性を高めるため、攻撃者は標的組織に関係する組織や官公庁が公表している情報等から、その業界特有の用語や関係者の情報を「事前調査段階」で集め、それを件名、本文、署名、添付ファイル名や内容等に利用し、標的組織の職員が興味を持ち思わずクリックしたくなるメールを使うケースが確認されている。テーマを変えながら何度もメールを送り、粘り強く攻撃を継続していることもある※44。

(b) ネットワーク境界装置の脆弱性を悪用した攻撃

外部ネットワークとの境界に設置している装置を狙い、標的組織のネットワークへ侵入を試みる例が公表されている。具体的には、「1.2.2 (1) (b) 境界装置の脆弱性を悪用した攻撃」で紹介した攻撃や、SSL-VPN製品の脆弱性を悪用した攻撃※54等、ネットワーク境界装置を悪用して組織のネットワークへ侵入する手法が報告されている。

(c) SNSを悪用した攻撃

JPCERT/CCとNISCから、SNSを悪用した攻撃手法が報告されている※55。標的組織に侵入するため、攻撃者は標的組織と関わりのある他組織の職員のSNSのアカウントをあらかじめ乗っ取り、そのアカウントから、不正なファイルをSNSで送信しウイルスに感染させようとした事例や、標的組織の職員に対してSNSのチャットで接触を行い、複数回やり取りを行った後、最終的にウイルスが含まれる不正なファイルをSNSで送り付ける事例がある。このように攻撃者は、標的組織の職員へ、求人や共通の趣味等、個人への関心を装って接触を図り、信頼関係を構築し、不正なファイルを実行させるよう仕掛ける。

(d) サプライチェーン等への攻撃

NISCの事例集※56では、ITソリューション企業の国内グループ拠点のネットワーク・機微情報に不正アクセスされた事例が報告されている。セキュリティベンダーからは、子会社または関連会社の取引先を経由して標的組織へ攻撃を行っていた事例※57が報告されている。これらの事例のように、標的組織のネットワークやシステムを直接狙うのではなく、関連会社や子会社、取引先等、標的組織と関係を持つサプライチェーンを侵入の初期ターゲットとする攻撃の手口がある。これらの組織は、標的組織とシステム的なつながりや業務上の関係を持つ一方、標的組織と比較して、予算規模やセキュリティに対する意識に差があり、セキュリティ対策が不十分な場合がある。攻撃者は、このセキュリティレベルのギャップを狙うために、事前調査の段階で標的組織のサプライチェーン全体を見渡し、セキュリティ対策が脆弱な組織・拠点を侵入の初期ターゲットとしている。

(4) 標的型攻撃の手口(攻撃基盤構築段階)

初期潜入後、攻撃者が攻撃基盤を構築する段階における具体的な手口の例を紹介する。

(a) 感染の永続化

攻撃者は標的組織への初期潜入後、初期潜入した端末の制御を維持するためにウイルス感染の永続化を図る。端末の起動時にRAT等のウイルスが自動的に実行されるように、攻撃者は端末のレジストリの編集やタスクスケジューラーへの登録等を行う。

(b) 組織内での侵害範囲拡大

攻撃者は最初に感染した端末から別の端末や Active Directory サーバー、他のネットワーク等への侵害範囲拡大を行い、更に重要な情報の窃取を目指す。このため攻撃者自らがコントロール可能な端末上で様々なツールを使って認証情報窃取やネットワークスキャンを行い、端末が接続するネットワーク内にある別の端末の状況を調査し、それら端末への侵害を図り、侵害範囲を拡大する。

(c) 正規ツールや OSS の悪用

前述の「(a) 感染の永続化」や「(b) 組織内での侵害範囲拡大」の段階では、攻撃者が開発したウイルスが使われることに加えて、通常の業務で使用するソフトウェアや OS の標準機能として利用できるツール、システムの運用管理やシステムの脆弱性有無の調査等の正当な目的を持つツール(正規ツール)を悪用する例が報告されている※58。特にリモートアクセスツールやファイル転送ツール、クラウドストレージの同期ツール等のソフトウェアは、通常業務で利用されるため、業務での利用か攻撃者による悪用かの区別がつきにくく、セキュリティソフトでウイルスとして検知することが難しい。

セキュリティ技術者がシステムの脆弱性有無を調査するために使うツールや、システムの運用管理に使うツール等の正規ツールは OSS で提供されていることが多い。OSS は、誰でも容易に入手可能でありソースコードの変更も可能である。これら一部の OSS は、攻撃者に悪用されることがある。一方、セキュリティソフト等では、攻撃者の OSS 悪用を検知・防御するため、検知パターンに登録する等の対応を行っているものがある。このような防御策に対して攻撃者は、ソースコードを改造してセキュリティソフト等で検知されにくくした上で使用することがある。

(5) 標的型攻撃への対策

標的型攻撃の傾向や手口に記載したとおり、攻撃者は多種多様な手口で、用意周到に準備を行い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。変化した攻撃手法に対策が有効では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、あらゆる可能性の考慮に加え、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) 職員の意識向上

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、標的組織の職員の関心を引く題材を送る、標的組織の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。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、組織として職員に標的型攻撃を見抜くため教育や注意喚起、標的型攻撃メールを模した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
  攻撃者は、SNS で標的組織の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。このようなケースがあることや注意点を職員に周知し、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 設置と運用
  組織の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、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、攻撃者の侵入手口が特定機器の脆弱性を悪用したものであれば、自組織のシステムに該当する機器がないか確認し、該当するものがあれば速やかに脆弱性修正プログラムを適用する。標的型攻撃メールの情報が得られた場合は、社内にその特徴を周知し、メールのフィルタリング設定を行うことで、被害防止につなげることができる。もし、自組織が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（Indicator of Compromise：侵害指標）等の情報を積極的に共有してほしい。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※59。
- 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
  「1.2.2(3)(d)サプライチェーン等への攻撃」で述べたとおり、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※60」にも対策例が記載されているので、参考にしてほしい。
- 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、脆弱性修正プログラムの適用等の対応を漏れなく行える仕組みを作ることが望ましい。特に「1.2.2(1)(b)境界装置の脆弱性を悪用した攻撃」で紹介したように、ネットワーク境界装置は脆弱性が公表後すぐに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
  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、サンドボックスとよ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
  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、早期に検知するため、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※61。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。

1.2.3 ビジネスメール詐欺（BEC）

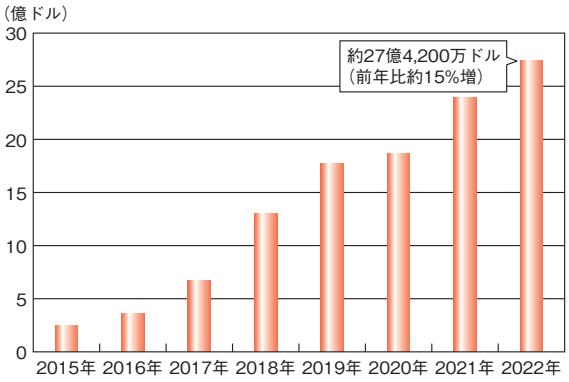
ビジネスメール詐欺（BEC：Business Email Compromise）は、巧妙な騙しの手口を駆使した偽のメールを企業・組織に送り付け、職員を騙して送金取引に関わる資金を詐取する等の金銭被害をもたらすサイバー攻撃である。偽のメールを送るための前段階として、企業の職員や取引先のメールアカウント情報を狙うため、フィッシング攻撃や情報を窃取するウイルスを使用することもある。

本項では、2022 年度に公表されたビジネスメール詐欺の状況、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

米国連邦捜査局（FBI：Federal Bureau of Investigation）のインターネット犯罪苦情センター（IC3：Internet Crime Complaint Center）が 2023 年 3 月に公開した年次報告書※62 によると、2022 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 15% 増の約 27 億 4,200 万ドルとなっている。また、IC3 が公開した 2015 年から 2022 年までの年次被害総額の推移をグラフで表すと、総額が継続して増加していることから、ビジネスメール詐欺の脅威がより深刻なものになっていることが分かる（次ページ図 1-2-5）。

その一方で、2022 年度は、前年度に引き続き世界の法執行機関がビジネスメール詐欺の容疑者を逮捕・起訴する事例も多数公開されている。2022 年 6 月から 11 月にかけて行われた「HAECHI-III」と呼ばれる国際的な取り締りでは、ビジネスメール詐欺ほかサイバー犯罪に関わっていた 975 人を逮捕し、悪用されていた約 2,800 件の銀行口座や暗号資産口座を凍結させ、1 億 3,000 万ドル相当の資産を押収したという※63。



■図 1-2-5　ビジネスメール詐欺の被害総額推移
(出典)IC3 年次報告書※62 を基に IPA が作成

また、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。「Operation Delilah」と呼ばれる国際的な取り組みでは、国際刑事警察機構（ICPO：International Criminal Police Organization、INTERPOL とも呼ばれる）やナイジェリア警察が、Group-IB、Palo Alto Networks, Inc.、トレンドマイクロ社の協力を得て、2015 年から活動している有名なビジネスメール詐欺の容疑者の逮捕に至った※64。「Operation Killer Bee」と呼ばれる取り組みでは、国際刑事警察機構、ナイジェリアの経済金融犯罪委員会、トレンドマイクロ社等の連携によって、日本を含む世界的な詐欺に関わっていた容疑者 3 名の逮捕に至った※65。

(2) 2022 年度に報道された事例の概要

2022 年度においても国内外で金銭被害に遭った事例が確認されている。国内企業に関連して発生した事例としては、コンサルティングサービスを展開するウィルソン・ラーニング ワールドワイド株式会社のグループ企業が、悪意ある第三者の虚偽のメールによる送金指示に騙され、約 550 万円の詐欺被害を受けたという※66。

国外で発生した事例では、米国の医療保障制度に関連する公的機関及び民間の健康保険企業に対し、病院のメールアドレスを偽装した攻撃者が、病院の担当者になりすまして送金先を偽の銀行口座に切り替えるよう指示し、合計 1,110 万ドル以上を騙し取ったという※67。

(3) IPA が情報提供を受けた事例の概要

IPA では、実際に試みられたビジネスメール詐欺の事例を基に、2017 年 4 月、2018 年 8 月、2020 年 4 月と三度にわたり注意喚起を行っており、2022 年 9 月からは Web サイト上で「ビジネスメール詐欺（BEC）対策特設ページ※68」（以下、特設ページ）と題して、事例や対策等を紹介している。また、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 が情報提供を受けたビジネスメール詐欺事例のうち、J-CSIP の運用状況レポートにて 2022 年度に公開した事例、及び手口等が特徴的であるとして特設ページの事例集にて初めて公開した事例の概要を表 1-2-1（次ページ）に示す。なお、このうちの 3 件（表 1-2-1 の項番 3、4、5）については、金銭的被害が確認されている。残り 4 件については、メールの受信者等が不審であることに気付いたため、被害を防ぐことができている。

(4) IPA が情報提供を受けた事例

ここでは、表 1-2-1（次ページ）の項番 2 について紹介する。なお、攻撃メールに見られる特徴等に関しては、表 1-2-1 の「備考」に記載した各レポートを参照いただきたい。

また、「情報セキュリティ白書 2020※76」の「1.2.2 (4) (b) CEO を詐称する一連の攻撃」で紹介した事例、及び、前述した 2020 年 4 月に IPA が行った注意喚起※77 の「『日本語化』された CEO 詐称の攻撃」で紹介した事例について、引き続き、多くの情報提供を受けたため、それぞれの概要を紹介する。

(a) 取引先担当者のメールアカウントを乗っ取って行われた攻撃事例

本事例は、2022 年 4 月、J-CSIP の参加組織の海外関連企業 A 社（請求側）と、その海外取引先企業 B 社（支払側）との間で取引を行っている中、A 社の担当者になりすました攻撃者から、偽の口座への振込を要求するメールが送られたものである。B 社の担当者はこのメールに返信してしまったが、その後に送られてきた攻撃者からの連絡内容を不審に思い関係者に通報を行ったため、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 1-2-6（次々ページ）に示す。

この攻撃は、特設ページで紹介しているビジネスメール詐欺の二つのタイプのうち、「タイプ 1：取引先との請求書の偽装」に該当する※78。

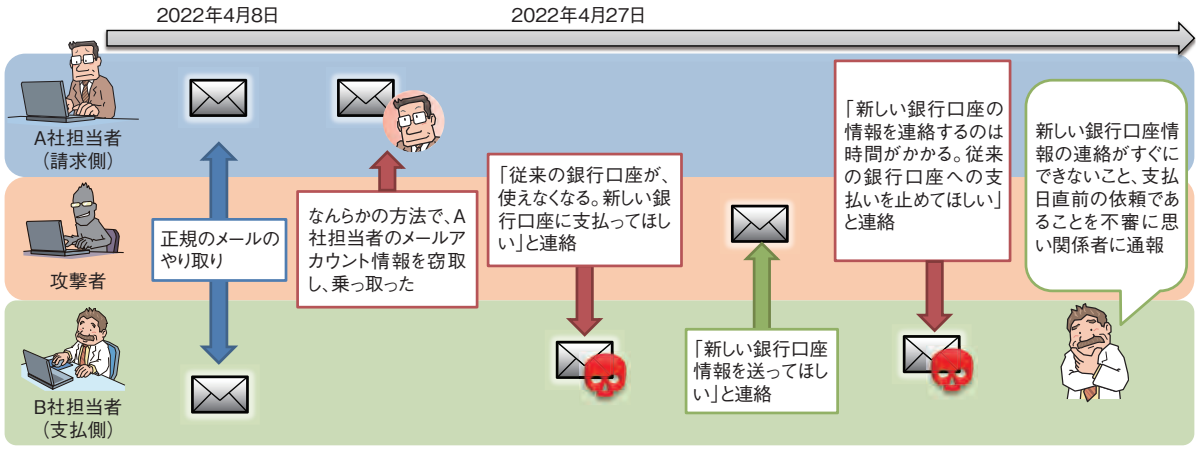
今回の事例では、A 社担当者のメールアカウントが攻撃者によって不正に乗っ取られて偽メールの送信が行われており、詐欺の過程において、次の手口が使われた。

項番	事例概要	被害の有無	備考
1	**攻撃者が実在する担当者を騙り、執拗に口座変更を依頼してきた事例** 2021 年 5 月、国内企業の米国グループ企業（請求側）の担当者になりすました攻撃者から、当該企業の取引先（支払側）に対し、偽の口座への振込を要求するメールを送り付けるビジネスメール詐欺が試みられた。支払側企業が請求側企業に問い合わせを行ったことで詐欺が発覚したため、支払側企業の担当者は攻撃者からのメールに反応はしなかったが、その後も攻撃者から複数回、偽の口座への振込を要求するメールが送られてきた。	なし	「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2022 年 1 月～ 3 月］[※69]」に記載
2	**攻撃者が担当者のメールアカウントを乗っ取って口座変更を依頼した事例** 2022 年 4 月、国内企業の海外関連企業（請求側）の担当者のメールアカウントを乗っ取った攻撃者から、当該企業の取引先（支払側）の担当者に対して、偽のメールを送り付けるビジネスメール詐欺が試みられた。	なし	「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2022 年 4 月～ 6 月］[※70]」に記載
3	**支払後、一部資金を取り戻すことに成功した事例** 2019 年 9 月、国内企業（支払側）と、海外取引先（請求側）との取引において、請求側企業の担当者になりすました攻撃者から、偽の口座への振込を要求するメールが送られ、支払側企業の担当者が送金した。 その後、送金された資金は攻撃者によって約半分が引き出されてしまったが、偽口座に残っていた資金については請求側企業や現地警察を交えた対応によって取り戻すことができた。	あり	特設ページの「ビジネスメール詐欺（BEC）の詳細事例 1[※71]」（2022 年 9 月 28 日公開）に記載
4	**攻撃者が証明書類を偽造して口座変更を依頼した事例** 2021 年 3 月、国内企業（支払側）と海外取引先（請求側）との取引において、請求側企業の担当者になりすました攻撃者から、銀行口座証明書類を偽造した上で、偽の口座への振込を要求するメールが送られ、支払側企業の担当者が送金した。	あり	特設ページの「ビジネスメール詐欺（BEC）の詳細事例 2[※72]」（2022 年 10 月 27 日公開）に記載
5	**攻撃者から毎月の支払方法を変えるよう依頼を受け、3 ヵ月にわたって偽の口座に送金した事例** 2021 年 2 月、国内組織の海外関連企業（支払側）と取引先（請求側）が、毎月、小切手で支払っている取引についてやり取りをしている中で、請求側企業の担当者になりすました攻撃者から、支払方法を変更して偽の口座へ振込を行うよう要求するメールが送られ、支払側企業の担当者が送金した。 その後、5 月に入って被害に気付くまでの期間、3 月、4 月にも続けて偽の口座に送金した。	あり	特設ページの「ビジネスメール詐欺（BEC）の詳細事例 3[※73]」（2022 年 11 月 29 日公開）に記載
6	**送金後すぐに詐欺である疑いを持って対処したことで、振込処理を停止させることができた事例** 2021 年 4 月、国内企業（請求側）と海外取引先（支払側）との取引において、請求側企業の担当者になりすました攻撃者から、偽の口座への振込を要求するメールが送られ、支払側企業の担当者が送金手続きを行った。 その直後に、支払側企業の担当者が攻撃者とのやり取りの内容に疑念を抱き、請求側企業に直接電話して事実確認を行い、本件が詐欺であることが発覚した。 すぐに請求側企業が送金先銀行に通報を行ったところ、振込が実施される前であったため送金が停止・返金され、金銭的な被害には至らなかった。	なし	特設ページの「ビジネスメール詐欺（BEC）の詳細事例 4[※74]」（2022 年 12 月 26 日公開）に記載
7	**攻撃者が支払側と請求側双方の担当者になりすましてビジネスメール詐欺を試みた事例** 2021 年 6 月、国内企業（支払側）と海外取引先（請求側）との取引において、攻撃者が支払側と請求側の双方の担当者になりすまして偽のメールを送り付けるビジネスメール詐欺が試みられた。 攻撃者は両者間のメールを盗み見た上で請求側企業の担当者になりすまし、支払側企業の担当者に偽の口座への振込を要求するメールを送った。不審に思った支払側企業の担当者が証明書類の提示を求めたところ、攻撃者は支払側企業の担当者になりすまして請求側企業の担当者から証明書類を騙し取り、支払側企業の担当者へ提示した。 最終的には、支払側企業の担当者が送信元メールアドレスについて請求側企業の担当者のものと異なっていることに気づき、請求側企業の担当者の正しいメールアドレスに連絡をとったことで詐欺であることが発覚し、金銭的な被害には至らなかった。	なし	特設ページの「ビジネスメール詐欺（BEC）の詳細事例 5[※75]」（2023 年 2 月 9 日公開）に記載

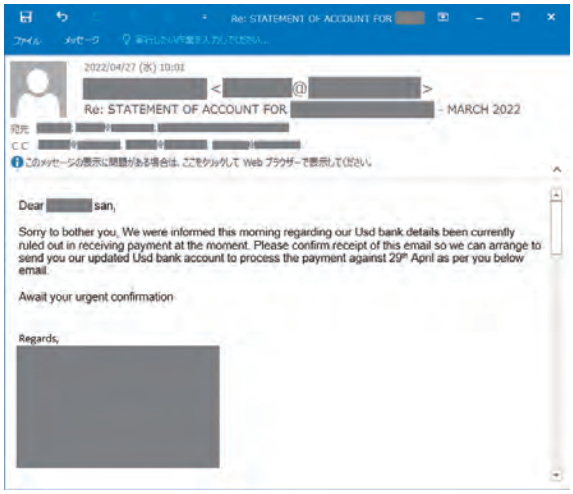
■表 1-2-1　IPA が情報提供を受け 2022 年度に公開したビジネスメール詐欺事例の概要

（ア）手口 1：正規のメールアカウントを使用し A 社と B 社のやり取りへ介入

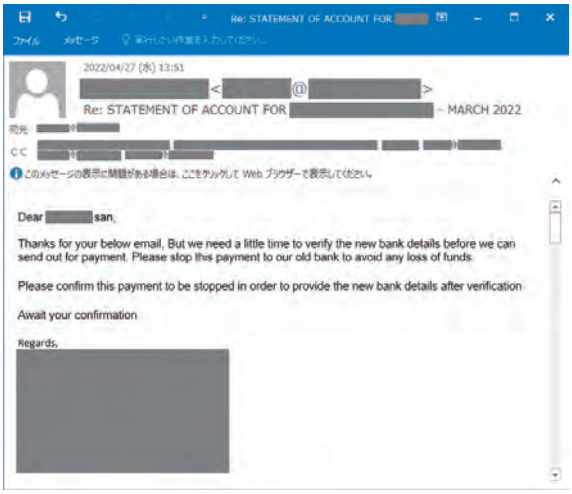
海外関連企業 A 社（請求側）と海外取引先 B 社（支払側）との間で、取引に関係したメールのやり取りをしている中で、2022 年 4 月 27 日、A 社担当者になりすました攻撃者から、現在の支払い口座が利用できなくなるという理由で、支払い先の銀行口座の変更を依頼する偽のメールが B 社担当者へ送られた。このとき、攻撃者から送られてきたメールは、何らかの方法で A 社の担当者のメールアカウントが乗っ取られて送付されたものであった。



■図 1-2-6　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［2022 年 4 月～ 6 月］」



■図 1-2-7　銀行口座の変更を依頼する偽のメール
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2022 年 4 月～ 6 月］」



■図 1-2-8　従来の口座への支払いを止めるよう依頼する偽のメール
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2022 年 4 月～ 6 月］」

攻撃者から送られた一通目のメールを図 1-2-7 に示す。

B 社担当者は、偽のメールであることに気づかず、新しい銀行口座の情報を送るように返信した。攻撃者は B 社担当者からのメールに対し、「新しい口座情報を連絡するには時間がかかるため、従来の口座への支払いを止めてほしい」という旨の内容を送信した。

攻撃者から送られた二通目のメールを図 1-2-8 に示す。

このメールを受け取った B 社担当者は、新しい銀行口座の情報がすぐに連絡されなかったことや支払日直前の急な銀行口座の変更であることを不審に思い、関係者へ通報したことで、偽のメールであることが発覚した。

（イ）手口 2：正規のメールアドレスに似せた偽のメールアドレスの使用

本事例で、攻撃者は A 社担当者のメールアカウントを不正に乗っ取ってメールを送信していたため、送信元（From）のメールアドレスは正規のものであった。しかし、同報先（CC）に指定されていた、A 社関係者のメールアドレスは、正規のメールアドレスに似せた偽のメールアドレスが使われていた。これは、A 社関係者にメールが届き、詐欺が発覚するのを避ける目的であったと考えられる。偽のメールアドレスのドメインは、攻撃メールが送られる前日（2022 年 4 月 26 日）に新規に取得され、図 1-2-9 に示すように、正規のドメイン名の「.」を「-」に変更、末尾に「.com」を追加したものであった。

【本物のメールアドレス】alice @ abc. ●●
【偽物のメールアドレス】alice @ abc- ●● . com
（「.」を「-」に変更、末尾に「.com」を追加）

※実際に悪用されたものとは異なる。

■図 1-2-9　A 社の詐称用ドメインの例（B 社へ送られた偽メールで使われたドメインの例）
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2022 年 4 月～ 6 月］」を基に作成

(b) CEO を詐称する一連の攻撃の事例

2022 年においても、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。

本項では、以下の二つの CEO 詐欺について説明する。

(ア) 複数組織へ行われた CEO を詐称する一連の攻撃

「複数組織へ行われた CEO を詐称する一連の攻撃」については、2022 年に 11 件、2021 年以前も含めると合計約 230 件のメール情報を入手している。本攻撃は、2019 年 7 月以降継続して観測されており、国内外の複数の組織を対象として行われた痕跡が確認されている。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。また、本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[※79]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、2022 年に 27 件、2021 年以前も含めると合計約 100 件のメール情報を入手している。本攻撃は、2019 年 11 月以降継続して観測されており、国内外の複数の組織を対象として行われた痕跡が確認されている。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」「Fastmail」「Mailgun」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される。

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の騙しの手口

ビジネスメール詐欺で用いられる騙しの手口は様々である。詳細は「情報セキュリティ白書 2020」の「1.2.2 (5) ビジネスメール詐欺の騙しの手口」にて、実際に使われた具体的な手口を紹介しているため、そちらを参照いただきたい。

また、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[※80]」の「3 ビジネスメール詐欺の代表的な手口の紹介」にも代表的な手口を掲載しているため、そちらも参照いただきたい。

なお、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、「新型コロナウイルスによる影響のため、通常の取引手続きではない方法で支払ってほしい」等と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。

(6) ビジネスメール詐欺への対策

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[※81]。

(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。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引だけでなく、グループ企業同士の取引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、突然送信エラーメールを受信するようになった等、不審な兆候が見られた場合、CSIRT 等の社内の適切な部門に報告できる体制を整え、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。もし、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は、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 への報告等を行うといった体制を整えておくことで、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 等の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、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、取引先の企業で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 ヘッダー）を正しい送信者のメールアドレスに偽装し、返信先（Reply-To ヘッダー）を攻撃者のメールアドレスにする手口もあり、送信元（From ヘッダー）と返信先（Reply-To ヘッダー）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 等のような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。

また、攻撃者によってメールアカウントが乗っ取られ、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、不正利用の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※82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、2022 年度に確認された DDoS 攻撃について事例と対策を解説する。

(1) DDoS 攻撃の動向

セキュリティベンダーによると、2022 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 602 万回で、前年同期比で 205% にまで増加した。近年、コロナ禍によるテレワークへの移行に伴い、DDoS 攻撃の急増が注目されており、2022 年度も引き続き VPN 製品やルーターを悪用したボットネットによる攻撃が増加傾向にある。

DDoS 攻撃の標的となった業界の割合を見ると、「ゲーム」が最多で全体の 40% を占め、続いて「IT 及び通信」（15%）、「動画配信サービス」（13%）、「クラウドサービス」（11%）の順で割合が多く、特にゲーム業界では、オンラインゲームに対する DDoS 攻撃を悪用した恐喝行為（DDoS Extortion）等が横行しているという※83。

また、2022 年 2 月にロシアがウクライナへ軍事侵攻を開始して以降、ウクライナ及び同国に対する支援を表明した国家への報復措置と見られる DDoS 攻撃が増加し

ている※84。

ここでは、2022年度における、DDoS攻撃に関する主だった事例を紹介する。

(a)リフレクション攻撃の事例

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ネットワーク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。攻撃対象はサイズの大きいパケットを大量に受信することになり、処理能力が限界に達することで、パフォーマンスの低下や動作の停止を引き起こす。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)※85を利用し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、多く観測されている※86。UDPサービスを対象とする攻撃では、UDPの以下の三つの特徴が悪用される。

①UDP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。

③UDP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。DDoS攻撃においては、送信元ホストとして偽装された攻撃対象のホストに対し、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、送信するデータ量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サーバーとの通信は正常であるため、攻撃の兆候を検出して対応を行うには、後述の「1.2.4(3)(b)DDoS攻撃に加担しないための対策」が必要となる。

2022年2月中旬には、PBX(Private Branch Exchange:構内電話交換機)とインターネット間のゲートウェイシステムの構築等に利用される、Mitel Networks Corp.製品(MiCollab及びMiVoice Business Express)の脆弱性(CVE-2022-26143※87)によって、インターネット上に意図せず公開された当該製品を悪用するDDoS攻撃が発生している。この事例では、5,300万pps(パケット/秒)という記録的な規模の攻撃であった点に加え、潜在的な増幅率が約43億倍であるという点が注目された※88。

UDPサービスを悪用したリフレクション攻撃では、2022年第4四半期において、Memcached(分散型メモリーキャッシュシステム)を悪用した攻撃が前四半期比1,338%増と最も高い増加率で観測され、次いでSNMP(Simple Network Management Protocol)を悪用した攻撃が前四半期比709%増で観測されたという※86。

リフレクション攻撃はその頻度や規模の拡大とともに、新たな手法やパケットの増幅率も年々増加しているため、今後も引き続き注意が必要である。

(b)ロシアのウクライナ侵攻時に国内で確認されたDDoS攻撃

2022年9月6日、親ロシア派を標榜するハクティビスト集団※89「Killnet」が日本の政府機関や民間企業に対するDDoS攻撃を示唆するコメントや動画をTelegram上に投稿した※90。

投稿があった後、ツールを使用したと推測されるDDoS攻撃が行われ、Killnetとの直接の関連性は不明であるものの※91、同時期に電子政府の総合窓口(e-Gov)や地方税ポータルシステム(eLTAX)等、国内の複数のサイトが一時的にアクセスできなくなる等の障害が発生した。一連の攻撃は、国連総会におけるロシアのウクライナ侵攻を非難する決議への日本の賛成や、北方領土の「ビザなし交流」に関する日ロ政府間協定をロシアが破棄したことに対し、日本政府が抗議の意を表明したこと等への反発が発端と考えられるという※92。

(2)DDoS攻撃を行うボットネットの拡大

DDoS攻撃には、ボットネットと呼ばれる攻撃用ネットワークが使用される場合がある。ボットネットは、攻撃者が乗っ取った多数のコンピューター、ネットワーク機器、IoT機器等と、それらに対して遠隔で指令を送信するためのC&C(Command and Control)サーバー※93で構成されている。攻撃者がC&Cサーバーを介して、ボットネットに攻撃指令を送信することで、ボットネットを構成する機器(ボット)が一斉に攻撃を行う。ボットの大半は組織や家庭で利用されているもので、サービスやソフト

ウェアの脆弱性を悪用されたり、ウイルスに感染した結果、制御を奪われた機器である。

攻撃者は、より多くの機器を乗っ取るため、最新の悪用手法等を取り入れてボットネットのアップデートを行い、様々な攻撃対象に対して攻撃を繰り返しながらボットネットを拡大させ、大規模なDDoS攻撃等を実行する。

2022年6月、クラウド上の仮想マシンやサーバーを悪用してDDoS攻撃を仕掛ける「Mantis」と呼ばれるボットネットが新たに観測された。Cloudflare,Inc.は、ボットネットとしては少数の5,000個のボットによる、2,600万rps（リクエスト／秒）という過去最大規模のDDoS攻撃を確認している。Mantisは、クラウド上の仮想マシンやサーバーでボットネットを構成することで、過去に猛威を振るったIoT機器を悪用するMirai※94やMēris※95とは比較にならない程、大きな攻撃能力を潜在的に保有すると見られている※96。

このようなボットネットは、ツールとして、DDoS代行サービスを通じて有償で貸し出されることがある。拡大したボットネットがDDoS代行サービスに使用され、攻撃者がそれを購入することで比較的手軽に悪用できることが、大規模なDDoS攻撃が発生しやすくなる要因となっている。

(3) DDoS攻撃への対策

DDoS攻撃への対策では、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攻撃に加担することを防ぐための対策も求められる。これらの対策について解説する。

(a) 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ため、継続して監視を行い、攻撃方法に合わせた対策を実施する。
- 攻撃の頻度や、攻撃対象サイト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。
- 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。

(b) 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を導入したり、適切な設定をしたりする対策が必要である。また企業においては、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。
- 組織内で稼働しているプリンター等の機器や、屋外に設置してリモートで管理しているWebカメラや気象センサー等の機器を洗い出し、DDoS攻撃に悪用される可能性があるサービスやソフトウェアが適切に運用されていることを確認する。具体的には、これらのサービスやソフトウェアが稼働する機器に関して、OSを始め、各サービス等が脆弱性を含むバージョンで稼働していないことや、DDoS攻撃に悪用される設定になっていないことを確認する。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。そういった機器は、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

2022 年度も、引き続き 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、影響範囲の広い開発フレームワーク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 2022 年度も続いた。2022 年 10 月に発生した大阪急性期・総合医療センターの事例では、給食提供業者の VPN 製品のソフトウェアのバージョンが古く、脆弱性が残存し、侵入経路となった可能性があることが報じられた※29（「1.2.1 (2) (b) 医療機関における被害事例」参照）。社会的に影響の大きいインシデントが依然として発生しており、警戒する必要がある。

(a) VPN 製品の脆弱性を狙った攻撃事例

Fortinet, Inc. は 2022 年 12 月 12 日に自社の FortiOS SSL-VPN に関して、ヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475※97）について公表し、脆弱性が解消されているバージョンへソフトウェアをアップデートすることを求めた。この脆弱性が悪用されると、認証されていない遠隔の攻撃者により、細工したリクエストを送信され、任意のコードやコマンドを実行される可能性がある。

同社がこの脆弱性を悪用して作成されたウイルスや攻撃を分析した結果、脆弱性を悪用するためには FortiOS と基盤となるシステムに関する深い知識が必要であることから、高度な技術を持つ攻撃者によって、政府または政府関係機関を標的とした攻撃活動が行われている可能性があるとしている※54。

また、2022 年 10 月 10 日、同社は、自社製 FortiOS、FortiProxy、FortiSwitchManager に関して、認証バイパスの脆弱性（CVE-2022-40684※98）についても公表し、脆弱性が解消されているバージョンへソフトウェアをアップデートすることを求めた。この脆弱性は、Web 管理インターフェースに存在する。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し、結果として攻撃者により任意の操作が行われる可能性がある。

同月 13 日、米国のセキュリティベンダーは、この脆弱性の攻撃コード（PoC※99）を公開した※100。同月 14 日、Fortinet, Inc. は脆弱性を悪用した攻撃を観測していると公表し、具体的な攻撃方法として、ターゲットとなるデバイスから設定ファイルを不正にダウンロードするほか、「fortigate-tech-support」と呼ばれる悪意ある管理者アカウントを追加する事例を報告した※101。

(b) VPN 製品の脆弱性を狙った攻撃への対策

近年のテレワークの普及等により VPN の必要性が高まっていることから、古い VPN 製品を利用せざるを得ない状況も考えられる。その際は、ベンダーから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することが望ましい。

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。脆弱性対応の実施手順の整備に加え、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。

なお、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、脆弱性の対応を遅滞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度
- 他部署やベンダー等への連絡の要否基準

(2) Microsoft 製品の脆弱性を対象とした攻撃

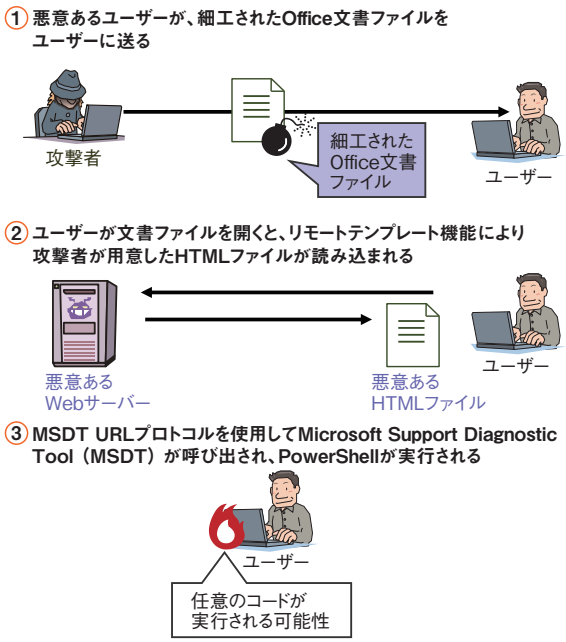
2022 年度も、Microsoft 製品の脆弱性を狙った攻撃が多数報告されている。本項では、Microsoft Support Diagnostic Tool（MSDT）の脆弱性を狙った事例を紹

介する。

(a) Microsoft 製品の脆弱性を狙った攻撃事例

MSDT は、Microsoft 社が開発し、Windows に標準搭載されているサポート診断ツールである。ここでは、2022 年 5 月に公表された「Follina」と呼ばれる脆弱性（CVE-2022-30190※102）を悪用した攻撃について解説する。

この攻撃では、Word 等の Office 文書ファイルにおけるリモートテンプレート機能の脆弱性が悪用されている。細工された文書ファイルを開くと、リモートテンプレート機能により攻撃者が用意した HTML ファイルが読み込まれ、MSDT URL プロトコルを使用して MSDT が呼び出されることで任意のコードが実行される（図 1-2-10）。マクロを使用していないことから、マクロが無効化されている場合でも攻撃が可能となる。



■図 1-2-10　Follina の脆弱性を悪用した攻撃イメージ

2022 年 4 月、この脆弱性を悪用した文書ファイルが VirusTotal 上にアップロードされていたことが確認されている※103。同年 6 月には、この脆弱性を悪用し、特定の政府関係機関を標的とした攻撃活動が展開されている可能性があることが報告された※104。

(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ら、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て、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) 開発フレームワークの脆弱性を悪用した攻撃

開発フレームワークに脆弱性が見つかった場合、作成されたアプリケーションにまで影響が及ぶ場合があり、影響範囲の調査や対策がより複雑になる可能性がある。ここでは、Spring Framework の脆弱性を悪用した攻撃について解説する。

(a) 開発フレームワークの脆弱性を狙った攻撃事例

Spring Framework は、Java 言語で開発を行う際に利用可能な開発フレームワークである。開発フレームワークは、アプリケーションを開発する場合に必要となる部品や、実装上のルール等を提供するもので、ソフトウェア開発における生産性や保守性の向上を目的としたものである。

VMware, Inc. は 2022 年 3 月 29 日、Spring Framework の Spring Cloud Function における任意のコードが実行される脆弱性（CVE-2022-22963※105）について公表した。この脆弱性は、Spring Cloud Function のルーティング機能を悪用したものである※106。細工したヘッダーを HTTP リクエストに追加することで、Spring Expression Language（SpEL※107）を介したコードの実行が可能となる。

また、同社は 2022 年 3 月 31 日、Spring Framework における任意のコードが実行される脆弱性（CVE-2022-22965※108）についても公表した。この脆弱性は 2021 年 12 月に報じられた Apache Log4j における「Log4Shell」と呼ばれる脆弱性（CVE-2021-44228※109）を想起させることから、「Spring4Shell」とも呼ばれている。この脆弱性は、データバインディングで使用されるクラス内において、特定のオブジェクトを安全に処理しないことに起因している※110。その結果、攻撃者により意図せずクラスローダーを呼び出され、システム内で任意の Java コードが実行される可能性がある。VMware, Inc. によれば、この脆弱性を悪用する攻撃を成功させるためには以下の複数の条件が必要であるとしている。

- JDK 9 以上を使用している。
- Apache Tomcat をサーブレットコンテナとして使用し

ている。

- WAR 形式でデプロイ※111 されている。
- プログラムが spring-webmvc あるいは spring-webflux に依存している。

本フレームワークで開発されたアプリケーションの構成によっては、認証されていない攻撃者によって遠隔から悪用される可能性がある※112。2022 年 4 月には、この脆弱性を悪用し、サーバーに暗号資産（仮想通貨）の採掘を行うコインマイナーを不正にインストールしようとする攻撃※113 や、Mirai を不正にインストールしようとする攻撃が観測された※114。

(b) 開発フレームワークの脆弱性を狙った攻撃への対策

このような攻撃による被害を防ぐため、利用する開発フレームワークは常に最新のバージョンにしておくことが望ましい。脆弱性によっては、アップデートによる対応が難しい場合でも脆弱性による影響を低減させる回避策が提示されている場合があり、必要に応じて対策を実施することが推奨される。開発フレームワークを直接使用していない場合でも、使用している製品内で開発フレームワークが使用されている場合は、脆弱性の影響を受ける可能性がある※115。どのようなフレームワーク、ライブラリ、コンポーネントを使用しているのか、平時からソフトウェア部品表（SBOM：Software Bill Of Materials）※116 等を活用し、利用しているソフトウェアを管理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）。

1.2.6 ばらまき型メールによる攻撃

特定の組織や個人ではなく、不特定多数の一般利用者を狙った、ウイルス感染を目的としたメールを本項では「ばらまき型メール」と呼ぶ。2015 年 10 月ごろより、国内で日本語のばらまき型メールによる攻撃が多く観測されるようになった※117。

2022 年度においても、件名やメール本文が受信者とは関係のないメール、実在の組織をかたったメール、一見すると業務に関係のありそうな件名や本文のメール、正規のメールへの返信を装ったメール等、様々なばらまき型メールを確認している。ばらまき型メールでウイルスに感染させる手口としては、添付ファイルを用いる手法を確認している。添付ファイルには、マクロ付きの Office 文書ファイルやショートカットファイル、これらのファイルを圧縮した ZIP 形式のファイル、OneNote 形式のファイルが使われることを確認している。添付ファイルによってウイルスに感染すると、感染した端末の情報窃取や遠隔操作、ランサムウェアへの感染等につながる場合もあるため※118、注意が必要である。

2019 ～ 2021 年に日本国内で多くの被害が発生した「Emotet」と呼ばれるウイルスへの感染を狙うばらまき型メールが、2022 年度も継続して IPA でも観測された。2022 年度に観測された時期は、2022 年 1 ～ 7 月中旬ごろ、11 月上旬ごろ、2023 年 3 月であり、再開と休止を繰り返していた。また、図 1-2-11（次ページ）に示すとおり、IPA の「情報セキュリティ安心相談窓口」でも、観測された時期に合わせて Emotet に関する相談件数が増減していた。

Emotet 以外のウイルスに感染させるばらまき型メールについても、2022 年度をとおして観測されている。本項では、主に 2022 年度に国内で観測された日本語のばらまき型メールで使用されたメール偽装の手口やウイルス感染の手口について解説する。

(1) 正規のメールと誤認させる手口

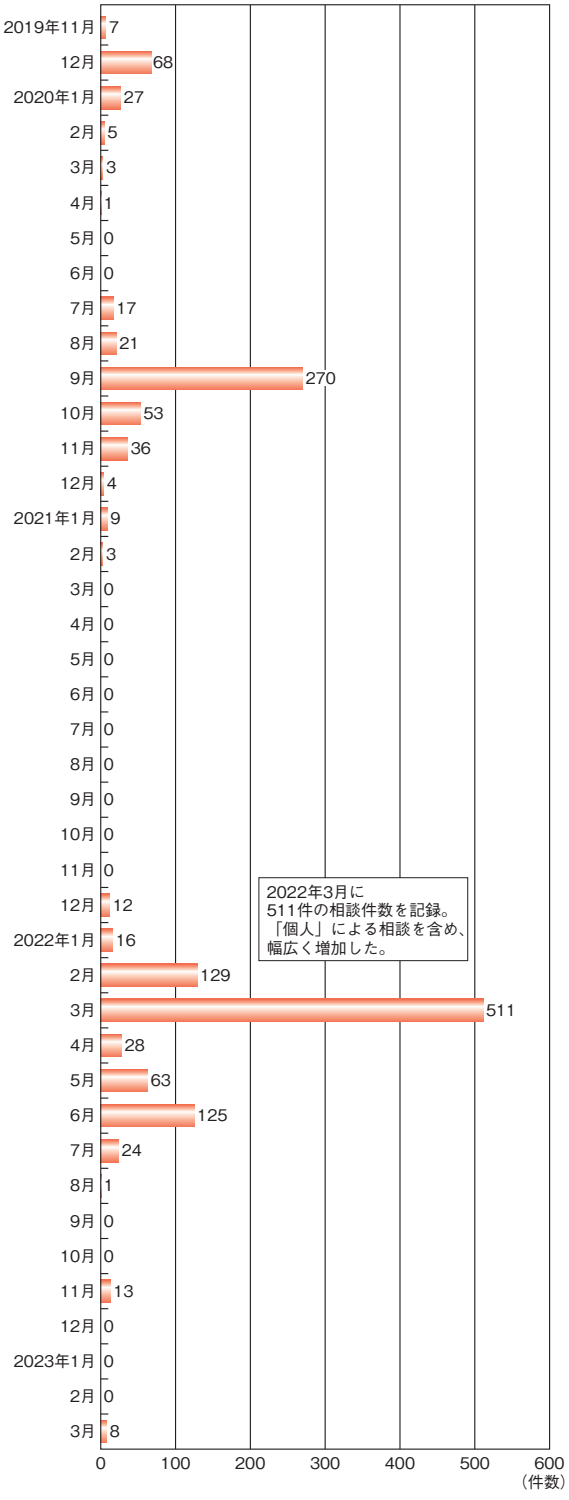
攻撃者が、ばらまき型メールの受信者に正規のメールと誤認識させるために使う手口について解説する。

(a) 正規のメールへの返信、転送を装う手口

IPA では、正規のメールへの返信、転送を装うばらまき型メール（以下、正規のメールへの返信等を装うメール）を観測している。このばらまき型メールでは、攻撃対象者が過去にメールのやり取りをしたことのある、実在する相手の氏名、メールアドレス、メールの内容等が流用され、その相手からの返信、転送のメールを装っている。

IPA では 2018 年 11 月からこのようなメールを観測しており※119、主に次の方法によってメールが送信されるという特徴が見られた。

- ウイルスに感染した端末から窃取したメールやアドレス帳に保存された情報を基に、メール送信用のボットネットから、別の相手に対して正規のメールへの返信等を装うメールを送信する方法※120
- ウイルスに感染した端末から窃取したメールアカウントの認証情報を悪用し、正規のメールアカウントから正規のメールへの返信等を装うメールを送信する方法※120

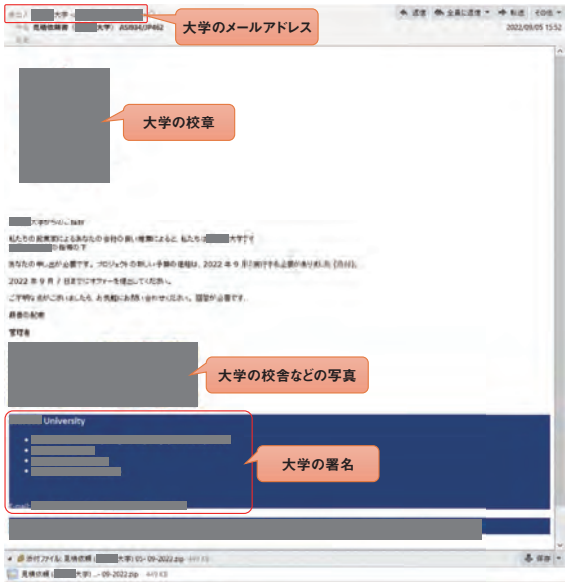


■図 1-2-11　Emotet に関する月別相談件数推移
（2019 年 11 月～2023 年 3 月）

(b) 実在の組織をかたる手口

実在する組織をかたるばらまき型メールも観測されている。

図 1-2-12 のように、実在する組織をかたり、あたかもその組織からの連絡であるかのように送信元や本文、署名を偽造したメールが送信される。この手口も継続して使われているため、引き続き注意が必要である。



■図 1-2-12　国内の大学をかたったばらまき型メール

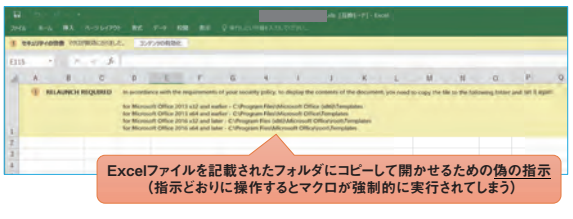
(2) ウイルスに感染させる手口

攻撃者がばらまき型メールを用いてウイルスに感染させる手口を解説する。

(a) マクロ付きの Office 文書ファイルを使用する手口

この手口では、Word、Excel、PowerPoint といった Office 文書ファイルに含まれている悪意あるマクロが動作することでウイルスに感染させる。攻撃に使用されたマクロ付きの Word、Excel ファイルには、Microsoft 社や Office 等のロゴとともに、「文書ファイルを閲覧するには操作が必要である」という趣旨の記述と「Enable Editing」（編集を有効にする）ボタンと「Enable Content」（コンテンツの有効化）ボタンのクリックを促す指示が書かれているものがあることを確認している。

2022 年 11 月には、図 1-2-13 に示すとおり、Excel ファイルを指定されたフォルダにコピーしてから開くように指示する新たな手口が確認された。ファイルのコピー先として指定されたフォルダは、Excel のデフォルト設定で信頼できる場所として設定されており、このフォルダ内に置かれ



■図 1-2-13　偽の指示が書かれている Excel ファイル

たマクロ付きの Office 文書ファイルは、開くとユーザーの確認なしにマクロが実行されてしまう※121。

(b) パスワード付きの ZIP ファイルを使用する手口

パスワード付きの ZIP ファイルが添付され、そのパスワードがメール本文に記載されているばらまき型メールを確認している。ZIP ファイルを解凍すると、マクロ付きの Office 文書ファイルやショートカットファイルが出力される。添付ファイルが暗号化されていることから、メールの配送経路上のセキュリティ製品や、セキュリティサービス、セキュリティソフトによる検知や検疫をすり抜け、受信者のもとに攻撃メールが届いてしまう確率が高い。この手口自体は 2019 年 12 月ごろから使われているが、2022 年度も継続的に使われており、引き続き注意が必要である。

(c) ショートカットファイルを使用する手口

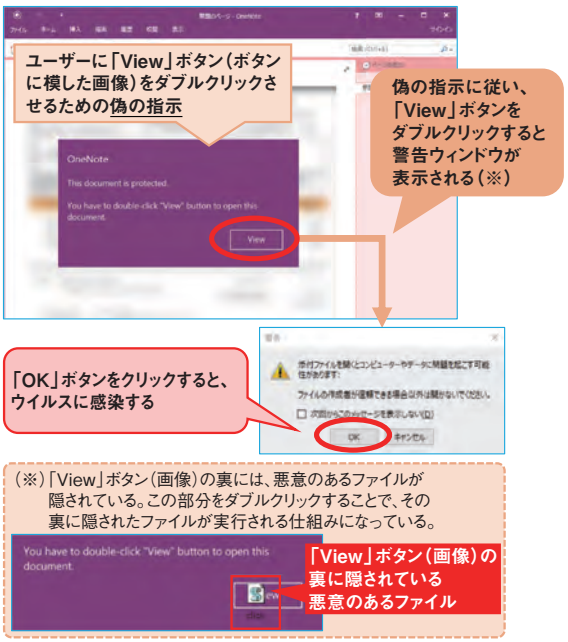
この手口では、メールに添付されたショートカットファイル、もしくは ZIP ファイルに含まれているショートカットファイルを開くと、ウイルスに感染する※122。ショートカットファイルには、特定の URL からウイルスをダウンロードし、感染させるスクリプトが記述されている。この手口はばらまき型メールに限らず、様々な攻撃で使われており、新しい手口ではないが、ショートカットファイルのアイコンが文書ファイルのように偽装されている場合があることや、Windows の標準設定では拡張子が表示されないといった特徴から、ファイル偽装に気づきにくい点に注意が必要である。

(d) ファイルサイズを意図的に大きくした Word ファイルを使用する手口

この手口では、1MB 未満の ZIP ファイルがメールに添付されて送付されてくるが、ZIP ファイルを展開すると 500MB を超える Word ファイルになる※123。Word ファイル自体は「(a) マクロ付きの Office 文書ファイルを使用する手口」と同じで悪意あるマクロが埋め込まれたものだが、ZIP ファイルを展開した後のファイルのサイズを大きくすることで、セキュリティソフト等の検知回避を企図していると考えられる※124。

(e) OneNote 形式のファイルを使用する手口

この手口では、悪意のあるスクリプトが埋め込まれた OneNote 形式のファイルが、メールに添付されて送られてくる。図 1-2-14 のように、ユーザーがファイルを開き、書かれている偽の指示に従って「View」ボタン（ボタンに模した画像）をダブルクリックすると、ファイルの開封を確認する警告ウィンドウが表示される。ここで「OK」ボタンをクリックすると、「View」ボタン（画像）の裏に隠されている悪意のあるスクリプトが実行され、ウイルスに感染する※125。



■図 1-2-14　OneNote 形式のファイルを開いてからウイルスに感染するまでの流れ

(3) Microsoft Office 文書ファイルのマクロデフォルト無効化を発端とした新たな手口

2022 年 2 月に Microsoft 社より、マクロを使用する攻撃に対処するため、インターネットからダウンロードした Office 文書ファイル内のマクロをデフォルトで無効化することが発表された※126。ばらまき型メールにおいても、この影響と考えられる攻撃手口の変化が観測されている。海外のセキュリティベンダーの観測によると、マクロを使用する攻撃が 2021 年 10 月から 2022 年 6 月の間に 66% 減少し、一方でマクロを使用しない手口（ISO、RAR 等のファイルや、ショートカットファイルを使用した攻撃）は 175%増加していたという※127。

今後、日本語のばらまき型メールでもマクロを使用しない手口が増える可能性もあるので注意が必要である。以下に代表的な手口を示す。

(a) ディスクイメージファイルを使用する手口

この手口では、悪意のあるファイルが格納されたディスクイメージファイル（ISO ファイル等）がメールに添付されて送られてくる。ディスクイメージファイルには非表示設定の

悪意のあるファイル（DLL ファイル等）と、それを読み込むためのコマンドが書かれたショートカットファイル等が格納されている。ユーザーがディスクイメージファイルをマウントし、ショートカットファイルを開くとウイルスに感染する。

Windows には、ディスクイメージファイル内のファイルに、Mark of the Web（MOTW）と呼ばれる、インターネット経由で入手したことを示す属性が伝達されない脆弱性（CVE-2022-41091）が存在していた※128。この手口では、その脆弱性を悪用し、MOTW を用いた Windows のセキュリティ機能を回避する目的があるとされている※129。MOTW が付与されたファイルを開くと、ユーザーに処理の続行等を確認するための警告メッセージが表示される。しかし、MOTW がないと、警告メッセージは表示されず、それが悪意のあるファイルだった場合、ウイルス感染にもつながるため、注意が必要である。

(b) HTML ファイルを使用する手口

この手口では、悪意のあるファイル（ZIP ファイル等）が埋め込まれた HTML ファイルがメールに添付されて送られてくる。ユーザーが HTML ファイルを開くと、埋め込まれている悪意のあるファイルがローカルに生成される。この手口は、HTML Smuggling と呼ばれており、インターネットやメールから受信するファイルの制限や検知の回避を目的に使用される※129。仮に ZIP ファイルが添付されたメールを配送されないように制限していても、ZIP ファイルが HTML ファイルに埋め込まれていれば制限を回避されてしまう可能性がある。セキュリティ対策を回避する手口として注意が必要である。

(4) ばらまき型メールへの対策

ばらまき型メールの攻撃者は、ウイルスに感染させる確率を上げるために様々な工夫を凝らし、新たな手口を取り入れて攻撃している。そのため利用者はセキュリティソフトの活用、スパムメール対策、メール受信者自身による防御等の対策を実施し、多層的な防御を行うことが重要である。

(a) 一般利用者における対策

次に示す対策は、ばらまき型メール以外の攻撃に対しても有効であり、徹底することを推奨する。

- セキュリティソフトを導入する
  メール受信者がウイルスメールであると判断できずに添付ファイル等を開いてしまったとしても、セキュリティソフトが検知・検疫し、被害を免れる可能性がある。セキュリティソフトは導入するだけでなく、常に最新の状態に保つことも重要である。
- 不用意にメールや添付ファイル内の指示に従わない
  身に覚えのないメールの添付ファイルを開かないことや、本文中の URL リンクにアクセスしないことが重要である。また、受信したメールに疑問や不審を抱いた場合は、送信元となっている企業や組織の公式サイトでばらまき型メールに関する注意喚起が公開されていないかを確認するほか、問い合わせ窓口から当該メールの送付有無を問い合わせる。受信メールの真偽が分からない段階では、メールへの返信、添付ファイルの開封、本文や添付ファイル中に書かれた指示に従った操作、URL へのアクセスは避けるべきである。また、添付ファイルを開いたときに、警告ウィンドウが表示された場合、その警告の意味が分からないのであれば、操作を中断し、システム管理部門等に報告・相談することを推奨する。また、個人であれば、信頼できる相手等に相談することを推奨する。
- OS やソフトウェアのバージョンを常に最新に保つ
  適宜、修正プログラムを適用し、既知の脆弱性を解消しておくことで、脆弱性を悪用した攻撃が成功する確率を下げることができる。
- Office 文書ファイルを開いたときに不用意に保護ビューの解除やマクロの有効化を行わない
  Office 文書ファイルを開いたとき、マクロやセキュリティに関する警告が表示された場合は、不用意に「編集を有効にする」ボタンや「コンテンツの有効化」ボタンをクリックしない。また、Word、Excel、PowerPoint 等の設定でマクロ機能が無効化されていない場合、業務等でマクロを使用しなければ無効化する、といった対策も有効である。

(b) 企業・組織における対策

企業・組織におけるばらまき型メールに対する対策は、「1.2.2 (5) 標的型攻撃への対策」で述べている内容と基本的には同じである。

加えて、組織的な対策として、不審なメールを受信した際の報告窓口を設けることや、利用者に対してウイルス感染を想定した訓練と教育を行うとよい。

システム的な対策では、不審なメールを解析する仕組みを確立する、適切な修正プログラムを適用する、特定のファイル形式について実行許可・禁止の設定を行う、使用しない特定のファイル形式のファイルが添付されたメールは受信を拒否する、使用しないクラウドサービスへ

のアクセスを禁止するといった対策が重要である。

また、公開されているばらまき型メールに関する注意喚起情報を組織内で共有し、同様の攻撃による被害を受けないようにすることも重要である。なお、企業や大学、個人等からも、ばらまき型メールに関する注意喚起が出されているため、これらの情報を収集し、活用することが望ましい。

1.2.7 個人を狙うSMS・SNS・メールを悪用した手口

フィッシングサイトへ誘導するメールの手口は、20年近く前から日本人を狙った日本語のものが出現している※130。当初は金融機関をかたるものが多かったが、フィッシング対策協議会の2022年12月の月次報告では、通販会社をかたるものが多くなっている※131。

サービスの利用停止や、料金の未払い等の文面から偽のサイトに誘導して、サービスのアカウント情報やクレジットカード情報を入力させる等を行う場合が多い。最近は、プリペイドカードの発行番号を入力させチャージ金額を不正使用するものも現れている。

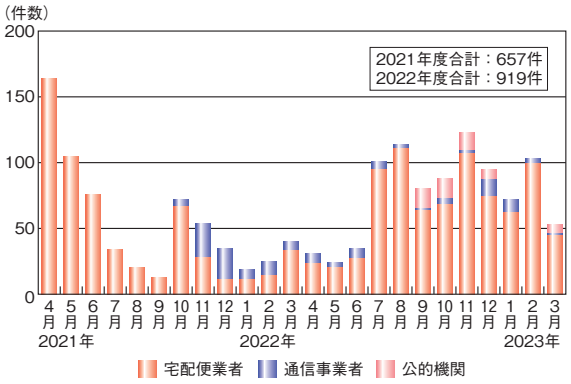
従来フィッシングサイトへの誘導は、主にメールで行われて来たが、SMSやSNSを悪用したものも増えてきている。個人がインターネットを利用する際の端末は、スマートフォンが6割を超え、SNSの個人利用率が8割近く※132になっていることも背景として考えられる。

2022年度にIPAの「情報セキュリティ安心相談窓口」に寄せられたSMSを悪用した手口の相談件数は、2021年度に比べ増加し、新たに国税庁等公的機関をかたるものが出現した。SNSでは「有名企業のXX周年記念で記念品が当たる」とかたり、友達とのリンク先の共有を受け取りの条件とするという、攻撃の拡散を意図した手口が出現した。

(1) SMSを悪用した手口

2022年も、偽の内容のSMS（以下、偽SMS）の手口に関する相談は継続して寄せられた。通信事業者をかたる偽SMSは減少する一方、宅配便業者をかたる偽SMSが増加し、新たに国税庁等公的機関をかたる偽SMSが出現した（図1-2-15）。

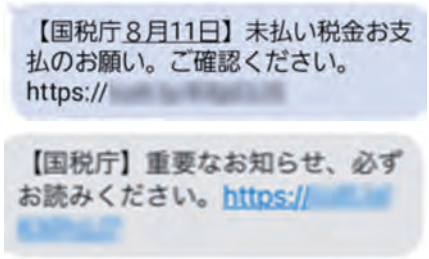
IPAは「安心相談窓口だより」に、新たに観測された手口の説明を追加し、2022年10月に注意喚起を行った※133。



■図1-2-15　偽SMSに関する月別相談件数推移（2021～2022年度）

(a) 国税庁を装う偽SMS

2022年8月ごろより、国税庁をかたる「未払いの税金がある」等の文面が記載された偽SMS（図1-2-16）から、URLをタップさせようとする手口の相談があり、同年9月ごろより増加した。相談件数は少ないが、公的機関をかたるものとして、警察庁をかたる偽SMSも出現した。



■図1-2-16　国税庁をかたる偽SMSの例

(ア) 手口

この手口では、「未払いの税金がある」「重要なお知らせ」という国税庁を装った偽SMSを送り付け、SMS内のリンクから偽サイトへ誘導する。iPhoneやiPad等のiOS端末（以下、iPhone）とAndroid端末（以下、Android）で共通して、偽SMSのURLをタップさせ、プリペイドカードの発行番号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。また、Androidにおいては、偽SMSのURLをタップさせ、不正なアプリをインストールさせる手口も確認されている。

①フィッシングサイトに誘導する手口

URLをタップさせ、国税庁になりすましたフィッシングサイトへ誘導し、メールアドレス、電話番号、氏名等の個人情報を入力させる（次ページ図1-2-17）。プリペイドカードの発行番号や額面を入力させ、更に券面の写真を撮影して送信させる手口も出現した。

②不正なアプリをインストールさせる手口

Androidにおいては SMSの URLをタップさせ、「シ

■図 1-2-17　フィッシングサイトに誘導する例（Android の画面）

ステム警告」という画面により「XXXセキュリティ」というアプリのインストールを促す場合がある（図 1-2-18）。これは不正なアプリのファイルをダウンロードさせようとするものである。

ファイルをダウンロードしただけでは被害にはつながらないが、ファイルをタップし、不正なアプリをインストールすると、被害につながる。

■図 1-2-18　セキュリティアプリのインストールに誘導する例

不正なアプリのインストールが終わった後、正規のセキュリティアプリの削除操作に誘導される場合がある（図 1-2-19）。

■図 1-2-19　セキュリティアプリ（あんしんセキュリティ）を削除させる例

（イ）被害

遭遇した手口によって、被害が異なる。

①フィッシングサイトに誘導する手口

被害として以下が確認されている。

- フィッシングサイトで入力したメールアドレス、電話番号、氏名等の個人情報が詐取された。
- プリペイドカードの発行番号や券面の写真を撮影して送信したため、プリペイドカードにチャージしていた金額が詐取された。

②不正なアプリをインストールさせる手口

被害として以下が確認されている。

- Android が攻撃の踏み台にされ、不特定多数の人へ、偽 SMS を勝手に送信された。
- スマートフォンから、アドレス帳の内容、SMS 等を窃取され、以下のように悪用された。
  - 通信事業者が提供するキャリア決済サービスにおいて、身に覚えのない請求が発生した。
  - フリーマーケットサービス、後払い決済サービス、その他のアカウントサービス等のアカウントを勝手に作成され、不正使用された。
- セキュリティアプリが削除され、セキュリティ対策が機能しなくなった。

（ウ）対処

遭遇した手口によって、対処が異なる。

①フィッシングサイトに誘導する手口への対処

- プリペイドカードの発行番号を入力した場合
  必要に応じてカードの発行元もしくは最寄りの消費生活センターに相談する※134。
- 個人情報を入力した場合
  更なる被害につながる不審なメールや SMS が届いたりする可能性がある。相手があたかも自身のことを知っているかのような文面を作成することも可能であるため、詐欺等の手口に十分注意する。

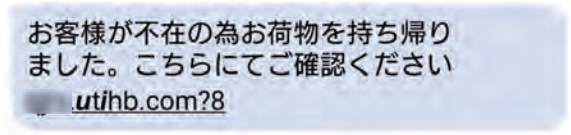
②不正なアプリをインストールさせる手口への対処

不正なアプリをインストールした場合の対処は、「情報セキュリティ白書 2020」の「1.2.6（1）（a）（イ）対処」を参照いただきたい。なお、正規のセキュリティアプリを削除してしまった場合は、セキュリティアプリの再インストールが必要である。また、セキュリティアプリの初期設定が必要な場合がある。

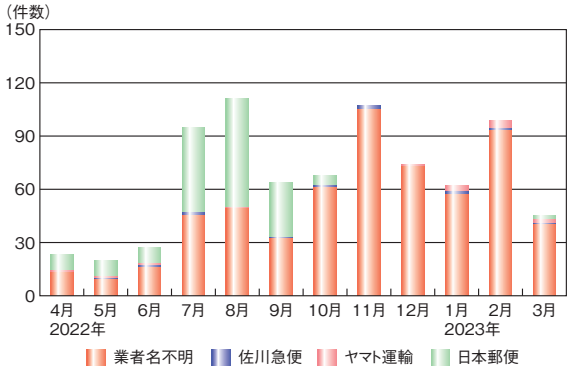
（b）宅配便業者を装う偽 SMS

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が、その後、業者名のない偽 SMS が出現した。2021 年 11 月ごろからは日本郵便株式会社をかたる偽 SMS が増加したが、2022 年 7 月からは、業者名のない偽 SMS（図 1-2-20）の相談が増加し、同年 11 月ごろからはほとんどの相談が、業者名のないものとなった（図 1-2-21）。



■図 1-2-20　宅配便業者をかたる偽 SMS の例



■図 1-2-21　宅配便業者をかたる SMS の月別相談件数推移（2022 年度）

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[※135]」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。

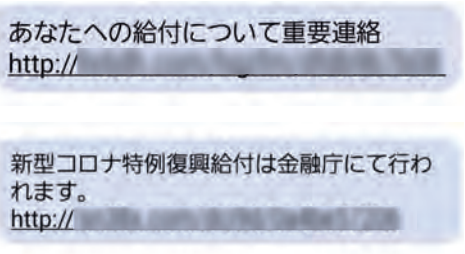
（c）世の中の関心に乗じる偽 SMS の手口

2022 年も、新型コロナウイルスの感染拡大が断続的に続き、経済や社会に様々な影響が生じた。それに乗じるものとして、2022 年 12 月ごろより、「新型コロナ特例復興給付金を受け取れる」という内容の偽 SMS を送信する手口が出現した。

（ア）手口

給付金が受け取れるかのような文面の偽 SMS（図 1-2-22）を送りつけ、URL をタップさせようとする。

URL をタップすると、Web メールのような画面が表示され、メッセージを確認するように促される。タップすると、至急連絡するように促され、入力して送信すると、メール BOX に新着があり、「受け取りの順番が自分で止まっている」と記載されたページが現れる（図 1-2-23）。給付金の受け取りのために振込手数料が必要で、Apple ギフトを購入して、番号と振込先をこのサイトの送信フォームで連絡するように書かれている。送信フォームで Apple ギフトの番号を送信すると、チャージしている金額が詐取される。



■図 1-2-22　新型コロナ特例復興給付金の給付をかたる SMS の例

■図 1-2-23　給付金の受け取りのため、Apple ギフトの番号を送信させるサイトの表示例

（イ）対処

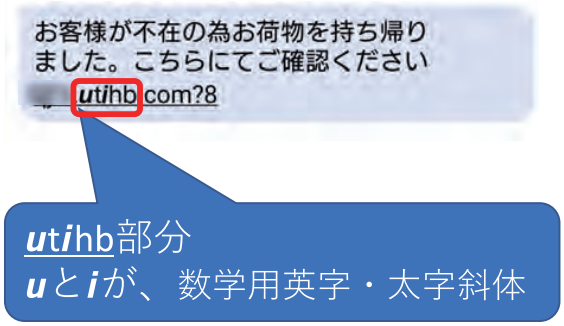
URL をタップして指示に従い、プリペイドカードの発行番号を入力した場合は、必要に応じてカードの発行元もしくは最寄りの消費生活センターに相談する[※136]。

（d）SMS を悪用した手口への対策

各通信事業者が SMS を悪用したフィッシングへの対策を開始している。株式会社 NTT ドコモは、2022 年 3 月から、危険と判断したサイトの URL 等が含まれる SMS を自動で拒否する設定の自動適用を開始した[※137]。ソフトバンク株式会社は 2022 年 6 月から「迷惑 SMS 対策」機能の提供を開始した[※138]。KDDI 株式会社は、2023 年 2 月に「迷惑 SMS ブロック」機能の提供を開始した[※139]。各社の提供する機能を利用して対策を行っていただきたい。

各社の機能の説明ページでも案内されているが、すべてのフィッシング SMS を拒否できるわけではない。URL の文字を通常の英字ではなく、数学用英字や、数学用英字・太字斜体を使う（次ページ図 1-2-24）等し

て、ブロックや拒否する対策の機能を回避していると考えられるものが現れている。



■図 1-2-24　URL の文字を変更している例

国税庁は、SMS による案内を送信していないと説明している※140。宅配便業者は、SMS で連絡することはないとサイトで案内している場合が多い。不審な SMS を受信した場合は、公式サイト等の確かな情報源を使って確認していただきたい。特に SMS に記載されている URL には注意が必要である。また、送信元情報の表示は偽装されている場合もある。

(2) SNS を悪用し偽サイトの URL の拡散を狙う手口

2022 年 12 月ごろより、LINE の友達から「企業のXX周年記念」をかたった偽の企業サイトの URL が送られてきた（図 1-2-25）という相談が寄せられるようになった。かたられている各社から注意喚起が行われている※141。

■図 1-2-25　LINEの友達から送られてくる偽の企業サイトのURLの例

(a) 手口

かたられる企業が異なっても手口は似通っている。現在確認されている手口を例に説明する。URL をタップすると、偽の企業サイトのアンケート回答画面が表示される。アンケートに 4 問答えると、記念品 5 万円が当たるチャンスの画面が表示されて、当たりの箱を選択させられる。2 回で当選する場合が多い（図 1-2-26）。

記念品を受け取るために、LINE のアプリでこのリンク先の URL を五つのグループまたは 20 人の友達と共有するように誘導する。「送信先を選択」と表示され、青いバーが 100%になるまで選択を促す（図 1-2-27）。

送信先を選択した友達に図 1-2-25 のようなリンク先の URL が送られるため、被害が拡大する可能性が高まる。なお、送信先を選択しなくても、「送信先を選択」の表示を繰り返すことで青いバーが最終的に 100%となるので、共有したかどうかを攻撃者は確認できていないものと思われる。

■図 1-2-26　偽の企業サイトで記念品が当選する例

■図 1-2-27　偽の記念品当選からリンク先情報を友達と共有させる例

青いバーが 100%になるまで情報共有先を選択して次に進むと、当初記念品は 5 万円の触れ込みだったが、アンケートで iPhone がプレゼントでもらえると、すり替わった表示になる。アンケートに答えていくと、先程と同様に、プレゼントが当たるチャンスの画面が出て、当たりの箱を選ぶ画面となる。2 回で当選する場合が多い。

この後、送料が 1 円かかるという名目で、名前やメールアドレス、電話番号を入力させ、クレジットカード情報を入力させる（次ページ図 1-2-28）。

(b) 被害

被害として以下が確認されている。

- フィッシングサイトで入力したメールアドレス、電話番号、氏名等の個人情報が詐取された。
- クレジットカード情報が詐取された。

■図 1-2-28　偽の iPhone 当選からクレジットカード情報の入力を促す例

(c) 対処

URL を友達に共有したかどうかや、入力してしまった内容によって、対処が異なる。

- 偽の企業サイトの URL を友達と共有した場合
  偽物のサイトであることを友達に連絡し、サイトにアクセスしないように注意喚起する。
- 個人情報を入力した場合
  更なる被害につながる不審なメールや SMS が届いたりする可能性がある。相手があたかも自身のことを知っているかのような文面を作成することも可能であるため、詐欺等の手口に十分注意する。
- クレジットカード情報を入力した場合
  カードの発行元もしくは最寄りの消費生活センターに相談する。

(3) メールによるフィッシングの手口

攻撃者はフィッシングサイトに誘導するため、QR コードを使うことでセキュリティ警告を出しにくくしたり、世の中の関心を利用した内容にメールを変えたりと、手口を進化させている。

(a) QR コードで偽サイトへ誘導する手口

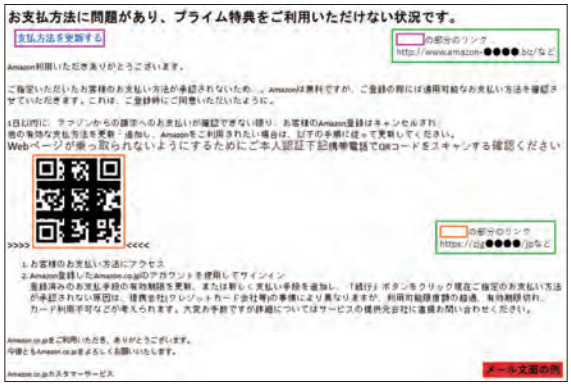
QR コードで支払いを行ったり、Web サイトを表示したりすることが一般的になってきたこともあり、騙しの手口にも QR コードを悪用したものが出現している。

(ア) 手口

フィッシングメールでは、ETC 関連サービスや、Amazon をかたるメールに、サイトへのアクセス先を QR コードで表示する手口が出現した（図 1-2-29）。不正な URL が平文でメールに表示されている場合は、メールサービスやメールソフト等で警告が表示される場合があるが、QR コードのみでは警告を表示できない場合があり、また、受信者は QR コードを見ただけでは、サイトの

■ETC 利用照会サービスをかたるフィッシングの例

■Amazon をかたるフィッシングの例



■図 1-2-29　QR コードが記載されたフィッシングメールの例
（出典）フィッシング対策協議会「ETC 利用照会サービスをかたるフィッシング（2022/11/15）※142」「Amazon をかたるフィッシング（2023/01/05）※143」

URL が分からないことを狙っているものと思われる。

(イ) 対処

入力してしまった内容によって、対処が異なる。

- 偽の ETC 関連サービスサイトでメールアドレスまたは携帯電話番号、パスワードを入力した場合
  メールアカウントや携帯電話番号でログインするサービスで使用しているパスワードを変更する。多要素認証のサービスが提供されていれば設定することを推奨する。
- 偽の Amazon サイトで ID やパスワードを入力した場合
  ログインパスワードを変更する。念のため「注文履歴」を確認して不正使用がないか、「アカウント設定」や「支払い&住所」が変更されていないか確認する。
- フィッシングサイトに入力したパスワードと同じものを他のサービスでも使用している場合
  アカウントに不正ログインされる恐れがあるため、そち

らのパスワードの変更も推奨する。

(b) 世の中の関心に乗じる手口

「1.2.7 (1) SMS を悪用した手口」で、給付金に関する偽 SMS の手口を説明したが、メールの手口では予防接種に関する「コロナワクチンナビ」をかたるものや、日本赤十字社の新型コロナウイルス感染症の活動報告をかたり寄付金を募るもの等が報告された※144。

「コロナワクチンナビ」をかたるものは、2021 年同様に引き続き報告されている※145。手口や対処については、「情報セキュリティ白書 2022※146」の「1.2.7 (3) 世の中の関心に乗じる手口」を参照いただきたい。

(4) SMS・SNS・メールを悪用した手口への対策

フィッシングの手口は、古くから悪用されているメール以外にも手段が増え、内容も変化し続けているが、基本の対策は変わらないと考えられる。

- 不審と感じたメールや SMS、SNS 情報の真偽は、公式サイト等の確かな情報源で確かめる。
- 判断に迷ったら、一度立ち止まり、身に覚えのない内容のメールや SMS の相手ではなく、信頼できる相手に相談する。友人からの SNS であっても、内容に URL が含まれる場合は、タップする前に友人に送信した意図を確かめる。

なお、SMS や SNS の騙しの手口では、不審なメッセージを受信した本人の被害だけでなく、他人や友達に被害の連鎖を拡げてしまいがちなことに注意が必要である。

1.2.8 個人を狙う様々な騙しと悪用の手口

本項では、「1.2.7 個人を狙う SMS・SNS・メールを悪用した手口」に続いて、個人を狙う騙しの手口として、Web ブラウザーを悪用した手口、遠隔操作アプリを悪用した副業詐欺及び偽 EC サイトについて説明し、その対策について述べる。

前者については、インターネット閲覧中に「パソコンがウイルスに感染した」等の偽のセキュリティ警告を突然表示させ、慌てた利用者に偽のサポートセンターに電話をかけさせた上で、サポート料金と称して高額な金銭を騙し取る手口の被害が拡大した。2022 年度は、IPA の「情報セキュリティ安心相談窓口」に寄せられた本手口の相談件数が、過去最高を記録した。後者については、買い物や働き方の変化を踏まえた手口の被害が増加した。消費生活センターによると、少しでもお得な買い物をしたいと思っている被害者を、格安商品を並べた EC サイトに誘い込む、偽 EC サイトの相談件数が約 2 倍に増加した※147。加えて、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副業詐欺の手口が出現した。

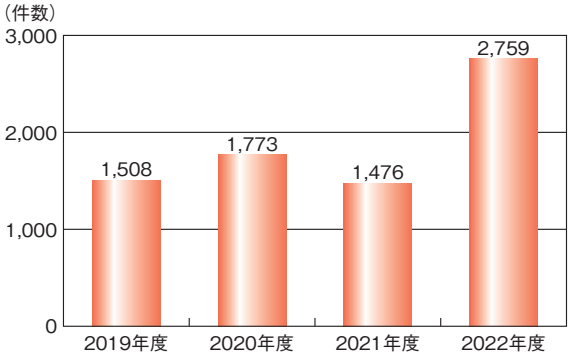
(1) 依然として続く Web ブラウザーを悪用した手口

パソコンでインターネットを閲覧中に突然別の警告画面に切り替わったり、スマートフォンに警告がポップアップ表示されたりする、「偽のセキュリティ警告」の手口に遭遇することがある。パソコンとスマートフォンで手口が異なるため、それぞれの詳細を以下に示す。

(a) 偽のセキュリティ警告 (パソコン)

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て、慌てた被害者に偽のサポート窓口に電話をかけさせる。その上で、サポート料金と称して高額の金銭を騙し取る※148。そのため、「サポート詐欺」とも呼ばれている。

手口に大きな変化はない一方で、2022 年度に IPA の「情報セキュリティ安心相談窓口」に寄せられた相談件数は 2,759 件となり、過去 4 年間で最高となった（図 1-2-30）。



■図 1-2-30 偽のセキュリティ警告 (パソコン) に関する相談件数の推移 (2019～2022 年度)

世界に目を向けると、FBI によれば、2022 年に「Call Center Fraud（コールセンター詐欺）」の一つである「Tech and Customer Support（技術・顧客サポート詐欺）」として申告を受けた件数が合計 3 万 2,538 件、被害総額が 8 億 655 万ドルに上ったという※149。また、セキュリティベンダーによると、2022 年第 3 四半期にこの攻撃を受けたユーザーの割合が最も高いのが日本で、

その後にドイツ、米国、カナダが続いている※150。

偽のセキュリティ警告は、Web 広告配信の仕組みを悪用して表示されている。例えば、訪問したサイトに偶然表示された罠の広告をクリックすると中間サイトに接続され、最終的に偽のセキュリティ警告を表示するサイトにリダイレクトされる事例を確認している。その際に、中間サイトで Web ブラウザーの言語設定等をチェックして、言語別の偽セキュリティ警告サイトにリダイレクトしていると考えられる。そのため、日本語表示に設定した端末からアクセスすると、図 1-2-31 のように日本語の偽のセキュリティ警告を表示するサイトにリダイレクトすると考えられる。この仕組みによって、複数の国々でこの手口による被害が発生している。

(ア)手口

具体的な手口について順を追って解説する。

①偽のセキュリティ警告で恐怖を煽る

主にパソコンで Web サイトを閲覧中に、ブラウザー画面に突然セキュリティ警告が表示される。画面を埋めつくすように次々と表示される警告の中には、「検出された脅威 : トロイの木馬スパイウェア」「パスワード、オンライン ID、財務情報、個人情報、画像、またはドキュメントを盗む可能性のある望ましくない可能性のあるアドウェアがこのデバイスで検出されました」等の警告文が書かれている(図1-2-31)。これらはすべて偽である。

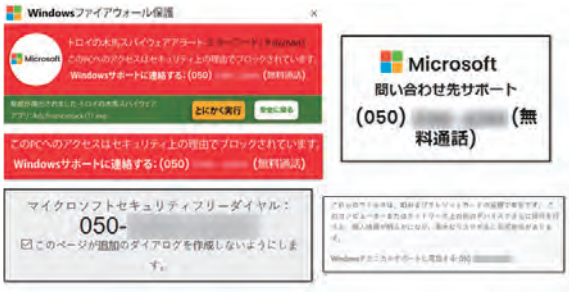
■図 1-2-31　次々と表示される警告画面の例

②巧妙な細工で焦らせる

偽のセキュリティ警告はブラウザーをフルスクリーンで表示して、ウィンドウの閉じるボタンを操作できないように細工している場合がある。加えてスピーカーからも、「IP アドレスが不正に使用された、再起動を行うとデータや個人情報の損失につながる、今すぐお電話ください」等のアナウンス音声が延々と流れ続ける場合がある。パソコンが正常に操作できないという焦りと、ウイルスに感染してしまったのではないかとう恐怖から、正常な判断力を奪おうとしていると考えられる。

③実在する企業の名前をかたり信用させる

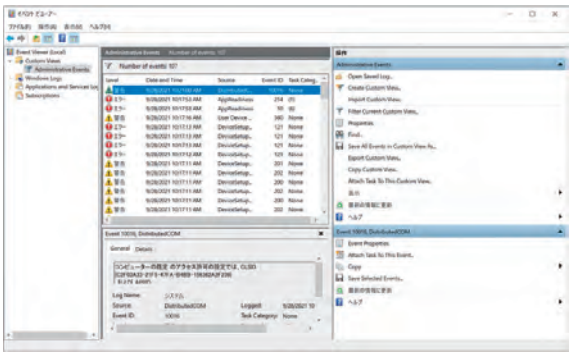
偽のセキュリティ警告画面には、Microsoft 社等の実在する企業のサポートセンターと称する電話番号が表示してあり、この番号に電話するように誘導する（図 1-2-32)。被害者を焦らせた上で、著名な企業名をかたることによって、「ここに電話すれば解決してもらえる」と思わせようとしていると考えられる。



■図 1-2-32　実在する企業名をかたる警告画面の例

④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、TeamViewer、UltraViewer 等の無償版を使用させる。遠隔操作ソフトウェアを使用して被害者のパソコンにリモート接続し、イベントビューアーで動作に支障がないエラー表示を見せる等して、パソコンがウイルス感染しているという虚偽の説明を行う(図 1-2-33)。



■図 1-2-33　動作に支障がないエラーをウイルスのせいであると虚偽説明する際のイベントビューアーの画面例

⑤電子マネー等を使った支払いを求める

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、クレジットカードではなく、「Google Play ギフトカード」等のプリペイドカードを悪用する。近くのコンビニに行って、こうしたプリペイドカードを買うように指示する。

そして、カード裏面の番号を電話で伝えさせる、もしくはパソコンに入力させて金銭を騙し取る。その際に、被害者が番号の 0（数字のゼロ）と O（アルファベットのオー）を間違って伝えたためカードが無効になった等と主張し、再度コンビニに行かせる場合もある。IPA では、このようにコンビニを何往復もさせられ、最終的に 100 万円を超える高額の金銭を騙し取られた被害の相談を受けている。

コンビニ各社が加盟する一般社団法人日本フランチャイズチェーン協会では、詐欺の被害に遭いやすい高齢者が電子マネーを購入する際に声掛けをする取り組みを行っている※151。この取り組みの結果、2021 年は、1 万 1,661 店舗で高額な電子マネーの購入を防止できたとしている※152。この数字には、偽のセキュリティ警告の手口による被害を防いだものが含まれると考えられ、こうした取り組みが更に広がることが望まれる。

(イ) 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問題はない。通常の操作で画面を閉じることができない場合、Windows であればタスクマネージャーから Web ブラウザーを終了する。

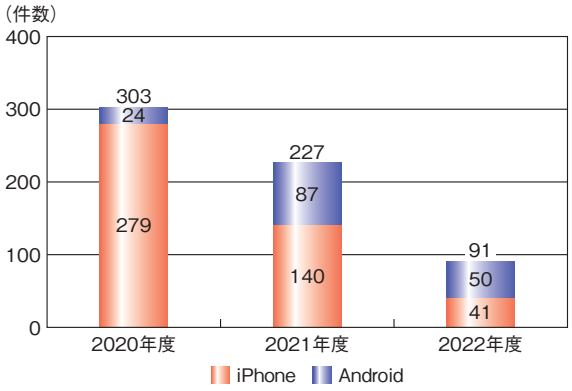
パソコンに遠隔操作ソフトウェアをインストールさせられた場合は、Windows の「システムの復元」機能を使用して、当該ソフトウェアをインストールする前の状態にシステムを戻すことを推奨する。遠隔操作の及ぼす影響について判断できないため、システムの復元ができない場合は、パソコンの初期化を推奨する。

(b) 偽のセキュリティ警告（スマートフォン）

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騙す手口の相談が継続して寄せられている（図 1-2-34）。

相談件数は減少しているものの、偽のセキュリティ警告から Android や iPhone 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※153 に誘導する相談が続いているため、IPA は「安心相談窓口だより」で、2022 年 10 月に注意喚起を行った※154。

手口の変化は少なく、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事例が多い。以下では、Android の場合の手口、対処を中心に説明する。



■図 1-2-34　偽のセキュリティ警告（スマートフォン）に関する相談件数の推移

(ア) 手口

この手口では、「スマホでウイルスが検出されました」「今すぐウイルスを除去」というように、偽のセキュリティ警告画面をポップアップ表示して公式ストア上のアプリを入手するよう誘導する（図 1-2-35）。

■図 1-2-35　偽のセキュリティ警告から公式ストアのアプリへ誘導する流れの例（Android の場合）

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誘導することであると考えられる。Android の場合、自動継続課金は、誘導されたアプリをインストールして起動した後、自動継続課金の登録画面で認証のために Google アカウントのパスワードを入力すると登録が完了する。利用開始当初は無料でも、最終的に意図しない料金が発生することになる。

誘導先のアプリは複数確認されている。何らかのセキュリティに関する機能を持つアプリであると説明されるものもあるが、スマートフォンの動作を改善させるという説明のクリーナーアプリや VPN のためのアプリのインストール等に誘導されることが多くなっている。

(イ)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、不要であればアンインストールをする。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、自動継続課金を登録した場合は取り消す必要がある。Android の場合は定期購入の解約、iPhone の場合はサブスクリプションの解約を実施する。

(c)Web ブラウザー通知機能の悪用

2020 年後半から、2021 年にかけて、パソコンやスマートフォンで、「『コンピュータが危険にさらされている』『携帯をクリーンアップしてください』等の警告が繰り返し表示された」という相談が急増した。

この表示は、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、不審なセキュリティソフトの購入や、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※155。「1.2.8(1)(a)偽のセキュリティ警告(パソコン)」で示した偽のセキュリティ警告と同様に、050 から始まる偽のサポートセンターの電話番号が表示される場合もある。

(ア)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何らか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

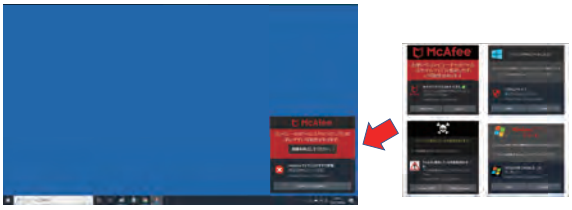
通知を受け取るためには、被害者が Web サイトからの通知を「許可」する必要がある。そのため、悪意のサイトを訪れた被害者を騙して通知を「許可」させようとする。

パソコンの場合は、Web ブラウザーに reCAPTCHAv2※156 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 1-2-36)。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。

②偽の通知が表示される

「許可」を押してしまうと、「パソコンがウイルス感染した」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 1-2-37)。スマートフォンの場合は、

■図 1-2-36　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)



■図 1-2-37　パソコンのデスクトップ右下に出現する通知表示事例

「スマートフォンをクリーンアップしてください」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。

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。

(イ)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 Web ブラウザー操作方法の詳細は、「安心相談窓口だより※155」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。

- 偽の通知に記載された番号に電話をしてしまった場合
  「1.2.8(1)(a)偽のセキュリティ警告(パソコン)」に記載した対処を行う。
- スマートフォンで不審アプリのインストールに誘導された場合
  「1.2.8(1)(b)偽のセキュリティ警告(スマートフォン)」に記載した対処を行う。

(2) 遠隔操作アプリを悪用した副業詐欺

多様な働き方を促進する社会の流れやテレワーク等による柔軟な働き方の普及に伴い、副業が注目を集めている。こうした中、国民生活センターや消費者庁から、高額な副業マニュアルの契約をさせられた被害に関する注意喚起が行われている※157。

中には、契約のために必要な資金を同時に複数の消費者金融から借り入れることを指示する悪質な例も現れている※158。こうした業者は、被害者のスマートフォンに遠隔操作アプリをインストールさせ、消費者金融に借り入れ申請等を行わせている。現時点では、遠隔操作アプリとして AnyDesk が悪用されていることを確認している。「情報セキュリティ安心相談窓口」でも、2022 年 5 月以降、金銭的な被害に至らなかった場合を含めて、遠隔操作アプリをインストールさせられたという相談を 27 件受けている。

以下では、遠隔操作アプリを悪用した副業詐欺の手口について説明する。

(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事業者の URL に誘導する。

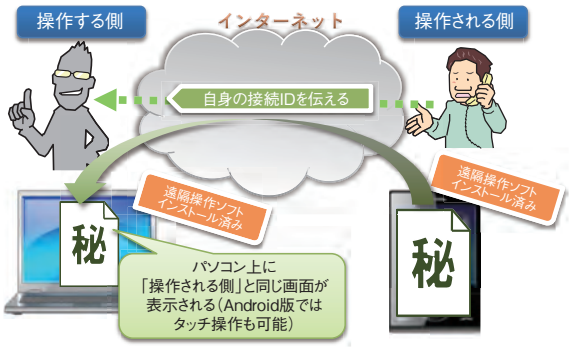
②高額なサポートプランに勧誘

副業紹介業者は、宣伝に興味を持った被害者を、業者の公式 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複数の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資金を持っていない場合、消費者金融業者から借り入れを行うように指示する。その際に、借り入れ金額が一つの消費者金融業者からの限度額を超える場合は、同時に複数の消費者金融業者から借り入れを行うように指示する。

副業紹介業者は、被害者に消費者金融からの借り入れを行わせる際に、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て、遠隔操作アプリの画面共有機能を使用して、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していると考えられる（図 1-2-38）。



■図 1-2-38　遠隔操作の概要

(b) 対処

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、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。その際は、端末内に残されたアクセス履歴等の証拠を保全するために、端末の電源をオフ状態にしておくことが望ましい。

(c) 対策

遠隔操作アプリの悪用に騙されないためには、遠隔操作のリスクについて知る必要がある。

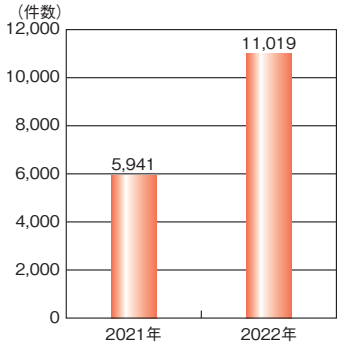
AnyDesk では、最初にアプリを起動した際に、遠隔操作を許可することによって「第三者があなたと同じ操作をできるようになる」ことを表示して、このリスクを「認識して承認」する画面が表示される。しかしながら、業者に操作をせかされてしまうと、被害者はこうしたリスクを認識できずに遠隔操作を許可している可能性がある。

第三者の言葉を鵜呑みにして遠隔操作アプリをスマートフォンにインストールしてしまうことは、見知らぬ訪問者を家に招き入れる行為と同じようなものであることを認識して、遠隔操作を他人に安易に許可しないことが重要である。

(3) 偽 EC サイト

ネットで検索して見つけた、格安商品を扱う EC サイトで購入した商品が届かない、もしくは偽物が届いたという被害が発生している。被害の原因は悪質な偽の EC サイトである。

国民生活センターによると、偽 EC サイトに関して消費生活センターに寄せられた 2022 年 4 ～ 12 月の相談件数は、2021 年同期間の約 2 倍に増加している（次ページ図 1-2-39）。



■図 1-2-39　偽 EC サイトに関する消費生活センターへの相談件数の推移（2022 年 4 ～ 12 月と、2021 年同期間の比較）
（出典）独立行政法人国民生活センター「その通販サイト本物ですか!?“偽サイト”に警戒を!!ー最近の“偽サイト”の見分け方を知って、危険を回避しましょう!ー[※147]」を基に IPA が編集

(a) 手口

以下の手口で被害者を偽 EC サイトに誘導する。

- 検索エンジンの検索結果を不正に操作
  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、偽 EC サイトは、Web 検索の機能を悪用して被害者を悪質なショッピングサイトに誘い込んでいる[※159]。具体的には、ほしい商品を探すために、商品名をキーワードにして Web 検索した際に、偽 EC サイトが検索結果の上位に表示されるように検索結果を不正に操作している。そのために、SEO ポイズニングと呼ばれる手法を用いている[※160]。
- 広告からの誘導
  検索結果の上部に表示される検索連動型広告や SNS の広告から偽 EC サイトに誘導する例も確認されている[※159]。

(b) 対処

「不審な EC サイトでショッピングを行ったが商品が届かない」「サイト運営者との連絡が取れなくなった」等、購入や支払いに関するトラブルが発生した際は、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。

配送のためにサイトに入力した住所・氏名・電話番号・メールアドレスが悪用される可能性も否定できないため、個人情報の悪用が懸念される際の対処は、フィッシングの被害に遭った場合と同様である。

- 名前や住所が記載された内容の、フィッシングメール、偽メール等の不審メールまたは SMS に注意する。
- 不審な郵便物や身に覚えがない代引きの荷物は受け取らない。
- それ以外の被害が発生した場合は、都度適切な窓口に相談する。

(c) 対策

偽 EC サイトには、以下に示す不自然な点、もしくは虚偽の記述が見受けられることが多い。

- 日本語の字体、文章表現がおかしい。
- 販売価格が大幅に割引されている。
- 事業者への連絡方法が、問い合わせフォームやフリーメールだけである。
- 事業者の住所の記載がない、記載されていても虚偽もしくは無関係な住所である、等

注文を行う前に、誘導された EC サイトにこうした点がないかを、今一度立ち止まって確認する必要がある。

(4) 騙しの手口に対する対策

「1.2.7 個人を狙う SMS・SNS・メールを悪用した手口」と本項に示した個人を狙う手口に共通する点は、様々な騙しのテクニックを使っていることである。こうした手口は、個人を狙う「サイバー攻撃」と言うよりは、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、騙されないようにすることである。

加えて、異常な動作と正常な動作を見分ける知識を持つことができると、より多くのシーンで騙しか否かを見抜くことができる。例えば、異常な動作である「突然表示されるけたたましいセキュリティ警告」は騙しであると知っているだけでなく、自らが使用している OS やセキュリティソフト等が正常に動作しているときにどのように警告を表示するかを知っていれば、偽のセキュリティ警告と同様の手口に騙される可能性を下げることができる。

このように、「普段と異なる状況等」に遭遇した場合は、これは正しいものなのかを今一度立ち止まって考え、少しでも不審に思った場合は、詳しい人や適切な窓口に相談することで被害に遭うリスクを減らすことができる。そのために米国の APWG（Anti-Phishing Working Group）と NCSA（National Cyber Security Alliance）が共同で提唱している「STOP. THINK. CONNECT.（立ち止まって理解する、何が起こるか考える、安心してインターネットを楽しむ）[※161]」を認識して実践していただきたい。

1.2.9 情報漏えいによる被害

2022 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) 2022 年の情報漏えい件数

2023 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の個人情報漏えい・紛失事故の調査結果※162-1 によると、2022 年に個人情報の漏えい・紛失事故を公表した上場企業は 150 社（2021 年は 120 社）、事故件数は 165 件※162-2（2021 年は 137 件）、漏えいした個人情報は 592 万 7,057 人分（2021 年は 574 万 9,773 人分）に達した。漏えい・紛失事故を公表した社数、事故件数はともに、東京商工リサーチ社が調査を開始した 2012 年以降の最多を 2 年連続で更新した。

(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。過去には金銭的被害も確認された事例があり、一層深刻な事態となっている。

(a) 不正アクセスによる情報流出事例

2022 年 9 月に公表された株式会社ニトリホールディングスの事例※163 では、同社アプリの会員情報の認証システムが不正アクセスを受け、約 13 万 2,000 アカウント分の個人情報が流出した。流出したと見られているのは、アプリや EC サイト等で会員登録をした利用者の氏名、住所、生年月日、クレジットカードの番号の一部等で、同社によれば別のサイトから漏れたパスワードと ID を用いる「リスト型攻撃」によって個人情報が漏えいした可能性があるという。

2022 年 10 月に公表された、入力フォーム支援サービスを提供する株式会社ショーケースの事例※164 では、同社が提供する「フォームアシスト」「サイト・パーソナライザ」「スマートフォン・コンバータ」において、第三者による不正アクセスでソースコードが書き換えられ、サービス利用企業の Web サイトで入力された情報が外部へ流出した可能性があると発表した。同社によれば、「フォームアシスト」のソースコードに不審な記述があるという指摘を利用企業から受けて調査したところ、システムの脆弱性を突いた第三者の不正アクセスによりソースコードが書き換えられ、一部利用企業の Web サイト等で入力された情報が外部へ流出した恐れがあるという。なお、情報漏えいの被害把握や原因究明を行うフォレンジック調査を実施したところ、情報が流出した可能性のある利用企業は限定的だったとしていたが、同社サービスを利用していた通販関連企業での被害が相次ぎ、株式会社ユーキャンは「生涯学習のユーキャン」サイトが第三者による不正アクセスを受け、顧客のクレジットカード情報 200 件が漏えいした恐れがあると発表した※165。また、株式会社エービーシー・マートはカード情報 2,298 件が漏えいした恐れがあると発表した※166。株式会社カクヤスはカード情報 8,094 件が漏えいしたことが確定したと発表した※167。いずれのケースも、カード情報入力画面で顧客が入力した、カード番号、有効期限、セキュリティコード等が漏えいしている。

2022 年 8 月に情報流出が公表された Twitter, Inc.（以下、Twitter 社）の事例※168 では、大量の Twitter アカウント情報を取得したと主張する投稿が、後述するとおり 3 回にわたってハッカーフォーラムに投稿されていたことを報道機関が複数回にわたって報じた。Twitter API には、第三者が他人のアカウント情報を取得できる脆弱性が 2021 年 6 月から 2022 年 1 月に修正されるまで存在していた。この脆弱性を使用して情報を取得したとして、2022 年 7 月に約 540 万件のアカウント情報を 3 万ドルで販売するという投稿がハッカーフォーラムに投稿された※169。また、2022 年 12 月には、約 4 億件を 20 万ドルで独占販売または 6 万ドルで複数販売するという投稿がされた※170。2023 年 1 月には、2 億件を超えるアカウント情報を公開したという投稿があったことが報道された※171。

(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 (5) 標的型攻撃への対策」を参照いただきたい。不正アクセスを認識した場合、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。情報流出の有無について調査でも判明しない場合は、不正アクセス対策を強化するとともに、定期的に流出した情報が悪用されていないかを確認することが必要である。

なお、2020 年 6 月に公布され、2022 年 4 月より全面施行された「個人情報の保護に関する法律等の一部を改正する法律」では、情報が漏えいした場合の個人情報保護委員会等への報告や本人への通知が、一定条件のもとで義務化された※172。個人情報については、必要以上に保有しないことも重要である。

(c) クラウドの設定不備による情報流出事例

2022 年 10 月に報道された株式会社 JTB の事例※173では、地域の観光資源を活用した看板商品を生み出す自治体や民間企業の取り組みを観光庁が補助する事業を受託した事務局で、最大 1 万 1,483 人分の個人情報等が流出した。事業に採択された約 700 事業者の情報をクラウドサービスで管理していたが、全事業者がアクセスできる状態に誤って設定していた。申請した事業者の担当者の名前や組織名、電話番号等が書かれた書類について、他の事業者もダウンロードできる状態になっており、個人情報が含まれていない書類の 3 回を含む計 18 回のダウンロードが確認され、同社が削除を依頼したという。

(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サーバー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。その他のクラウドの設定不備によるインシデントについては「3.3.2 クラウドサービスのインシデント事例」、対策については「3.3.3 (1) クラウドサービスのセキュリティの課題と対策」を参照いただきたい。

(e) 委託先のシステムが不正アクセスされたことによる漏えい事例

2023 年 1 月に公表されたアフラック生命保険株式会社とチューリッヒ保険株式会社の 2 社の事例※174では、2 社が委託していた米国の事業者が不正アクセスを受けてそれぞれ約 132 万人と約 75 万人の氏名（姓のみ）、年齢（生年月日）、性別等の顧客情報が海外サイトに掲載された。2 社とも外部委託先の事業者のサーバーが不正アクセスを受けた可能性があると説明している。また 2 社は同じ米国の事業者へ委託を行っていたことが報じられている※175。

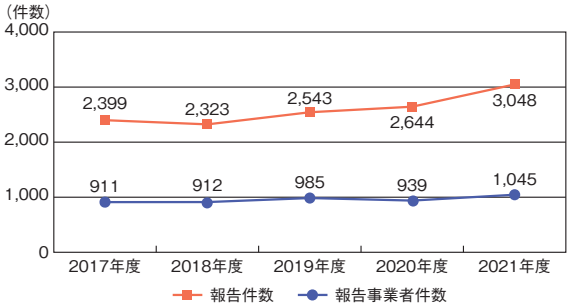
アフラック生命保険株式会社はダイレクトメールに記載された QR コードより視聴できる動画の配信業務を上記と同じ米国事業者に委託していた。

(f) 委託先のシステムへの不正アクセス対策・対処

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 2022 年 10 月 7 日に公表した「2021 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、2021 年度は 1,045 社のプライバシーマーク取得事業者から3,048 件の事故報告があった。2020 年度と比較すると、事故報告事業者数、事故報告件数ともに増加している（図 1-2-40）。2021 年度

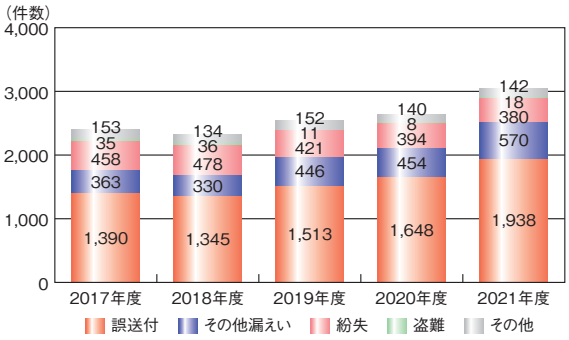


■図 1-2-40　事故報告の状況（2017～2021 年度）
（出典）JIPDEC「2021 年度『個人情報の取扱いにおける事故報告集計結果』」を基に IPA が編集

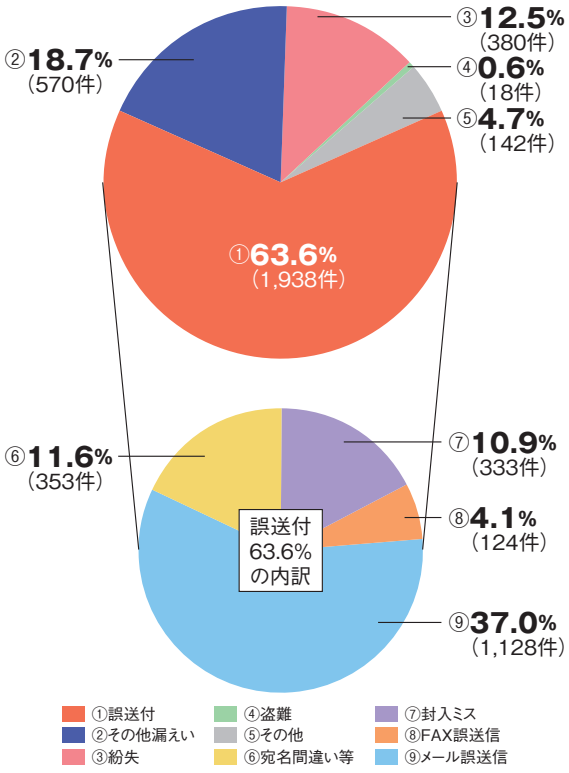
末時点のプライバシーマーク取得事業者数に占める事故報告事業者の割合は6.2%で、2020年度の5.6%から増加しているという。

事故原因は「誤送付」が最多の1,938件で63.6%を占め、「その他漏えい」が570件で18.7%、「紛失」が380件で12.5%と続いた(図1-2-41、図1-2-42)。「誤送付」の内訳は、「メール誤送信」が最多の1,128件で37.0%を占め、「宛名間違い等」が353件で11.6%、「封入ミス」が333件で10.9%と続いた。「メール誤送信」は2020年度の764件と比較し、約1.5倍に増加している。

「その他漏えい」(570件)の内訳は、「プログラム/システム設計・作業ミス(システムのバグを含む)」が最多の250件で43.9%を占め、「関係者事務処理・作業ミス等」が150件で26.3%、「不正アクセス・不正ログイン」が125件で21.9%、「口頭での漏えい」が38件で6.7%、「ウイルス感染」が7件で1.2%となり、約7割の漏えいが過失に起因するものであった。



■図1-2-41　原因別に見た事故報告件数の状況(2017～2021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』」を基にIPAが編集



■図1-2-42　「誤送付」の内訳(2021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』」を基にIPAが編集

(a)過失による情報漏えい事例

2022年6月23日に公表された尼崎市の事例※177では、業務委託先企業であるBIPROGY株式会社の関係会社社員が全市民46万人余りの個人情報を含むUSBメモリーを紛失した。紛失したUSBメモリーには同市全市民の住民基本台帳情報、住民税に係る税情報、非課税世帯等臨時特別給付金の対象世帯情報(2021年度分、2022年度分)、生活保護受給世帯口座情報、児童手当受給世帯口座情報等が含まれていた。

同社によると、関係会社社員が酒に酔って帰宅する途中に路上で寝てしまい、USBメモリーの入った鞄がなくなったことに気付いたことで表面化したという。6月24日に紛失した鞄ごとUSBメモリーが発見され、パスワードが変更された形跡はない、と同社は発表した※178。

同月28日、金子総務大臣は、地方自治体に対して情報セキュリティ対策を徹底するよう求める考えを示した※179。同年7月1日には、業務委託先企業が第三者委員会を※180、尼崎市が紛失事案調査委員会を設置したことを公表した※181。同年11月28日に、同調査委員会から本事案による市民の個人情報の漏えいは確認されなかったとの報告※182がなされた。

2022年6月に公表された杏林大学医学部付属病院の事例※183では、同院の医師が患者の個人情報入りUSBメモリーを紛失した。診療上のデータを院外に持ち出すのは禁止されていたが、データの判読に長時間を要することから、当該医師は院外にUSBメモリーを持ち出した。医師は帰宅後、患者27人の氏名やID番号、終夜睡眠ポリグラフ検査データ、睡眠時の状態を記録した動画が入ったUSBメモリーを紛失していることに気付いたという。紛失したUSBメモリーはパスワードロック等がされていなかったが、「この動画は赤外線を通して撮影しているため個人の特定は難しいと判断している」と説明した。また、終夜睡眠ポリグラフ検査データを診るには、市販されていない医療検査用の専門ソフトを必要とした。該当する患者には個別に文書で状況報告と謝罪をしたが、紛失11日後の時点でUSBメモリーは発見されていないという。

(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づくりが望まれる。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、新型コロナウイルス対策、あるいは省人化・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。

(4) 内部不正による情報漏えい

2022 年は大きく報道された内部不正の事例が目立つ年であった。営業秘密を不正に持ち出し、持ち出した先の会社で代表取締役社長になっていた人物が逮捕、起訴されるという、社会的にも反響の大きな事件に発展した。

(a) 内部不正による情報漏えい事例

2022 年 9 月に公表された、神戸の化学メーカーである株式会社 MORESCO における事例※184 では、元従業員が退職の際に、同社のダイカスト油剤等に関する営業秘密を不正に持ち出したことが、退職後の社内調査により判明した。同社は警察に相談し、捜査に全面的に協力していたが、2022 年 9 月に元従業員が不正競争防止法違反の容疑で兵庫県警に逮捕され公表に至った。

「かっぱ寿司」を運営するカッパ・クリエイト株式会社の事例※185 では、2022 年 9 月、カッパ・クリエイト株式会社元代表取締役社長が不正競争防止法違反罪で逮捕・起訴された。同時に法人としてのカッパ・クリエイト株式会社も同罪で起訴されている。不正に持ち出された競合他社「はま寿司」の営業秘密を、同社の業務で使用した等とされている。

どちらの事例も逮捕者が出ただけでなく、後者は上場企業の社長が逮捕されるという事態となった。

(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」第 5 版※186 を公開した。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（「2.8.1 内部不正防止対策の動向」参照）。

(5) 不適切な情報の取り扱い

紙媒体を含めた情報の不適切な管理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

2022 年 9 月に公表された株式会社イトーヨーカ堂の事例※187 では、自転車購入者 1,056 人分の氏名や住所、電話番号を記載した書類「自転車防犯登録カード」「自転車お客様カード申込書」を紛失した。

顧客からの要請で書類を確認したところ見当たらなかったことから紛失が判明した。情報の悪用は確認されておらず、同社が聞き取り調査をしたところ、2017 年に閉店した上大岡店で管理していた書類を横浜別所店に引き継いだ後、2019 年 10 月までに誤って廃棄した可能性が高いとの結論に至るにとどまった。

同社は紛失を謝罪した上で、「再度全従業員に指導を徹底し、再発防止に努めてまいります」とコメントを出している。

(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職員への教育等を継続して行う必要がある。

また「1.2.9 (5) (a) 不適切な情報の取り扱い事例」で見たとおり、紙媒体については、管理不備が見逃されやすいと考えられる。デジタル記録媒体か紙媒体かを問わず、管理の徹底が重要である。

COLUMN

便利な技術は悪用される

IT 技術やインターネット技術が進歩することにより、人々の生活は豊かで便利なものになっています。しかし、いつの時代でも、進歩によって生み出された便利な技術が本来の適切な使用方法とは異なった悪事に使用されてしまうという事態が度々発生しています。

IPA 情報セキュリティ安心相談窓口では、最近、ネット詐欺の手口において遠隔操作ソフト（アプリ）を悪用されたという相談が増加傾向にあります。

本来、遠隔操作ソフトは、インターネット経由で遠隔地にあるパソコンやスマートフォンを監視、操作する等の目的で利用されるものです。例えば、パソコンメーカーや通信事業者がパソコンやスマートフォンのユーザーサポートを行うために、遠隔操作ソフトを利用することがあります。パソコンやスマートフォンの操作に不慣れで、口で状況を説明するのが難しい人には大変便利な技術といえます。

しかし 2022 年 7 月以降、「副業サイトに登録をしたら電話が入り、高額なサポートプランの登録を勧められた。お金がないと言ったらスマートフォンの遠隔操作アプリをインストールするよう指示され、事業者にスマートフォンを遠隔操作され、複数の消費者金融から借り入れさせられてしまった。サポート内容が電話で聞いたものと違っており全く稼げなかった。」という相談が寄せられています[i]。

また、従来から相談の多い「サポート詐欺」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て、被害者に偽のサポート窓口に電話をかけさせ、その上で、遠隔操作ソフトを使い、偽のサポートサービスを提供し、高額の金銭を騙し取ろうとします[ii]。その金銭を支払わせるためにインターネットバンキングの画面を開かせ、振り込みによる支払いへと遠隔操作で誘導します。また、遠隔操作で振込み金額に勝手に末尾に「0」を加えて桁を増やしたという報道もありました[iii]。

第三者の言葉を鵜呑みにして自分のパソコンやスマートフォンの遠隔操作をさせることは、見知らぬ訪問者を家に招き入れる行為と同じようなものであることを認識して、遠隔操作を他人に安易に許可しないことが重要です[iv]。

せっかくの便利な技術が悪用されず、人々の生活に役立つ形で発展していくために、その技術を利用したソフトやサービスを提供する企業は悪用されにくい工夫をすること、必要に応じて業界は注意喚起や普及啓発等を行うことが望まれます。またそれを使用するユーザー側も、便利な技術には悪用されるリスクがあることを理解して、使用する際は慎重に使い始める等の心構えが必要です。

i　独立行政法人国民生活センター：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〔2023/6/13 確認〕
ii　IPA：安心相談窓口だより　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〔2023/5/15 確認〕
iii　朝日新聞デジタル：490 円→ 49 万円　勝手にゼロが増える振り込め詐欺、新手の手口か　https://www.asahi.com/articles/ASR356QFBR31PIHB00V.html〔2023/5/15 確認〕
iv　IPA：安心相談窓口だより　遠隔操作ソフト（アプリ）が悪用される手口に気をつけて!　https://www.ipa.go.jp/security/anshin/attention/2023/mgdayori20230411.html〔2023/5/15 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※188」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、ソフトウェアに関する脆弱性の特徴を統計的に確認することができる。本項では、2022 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。

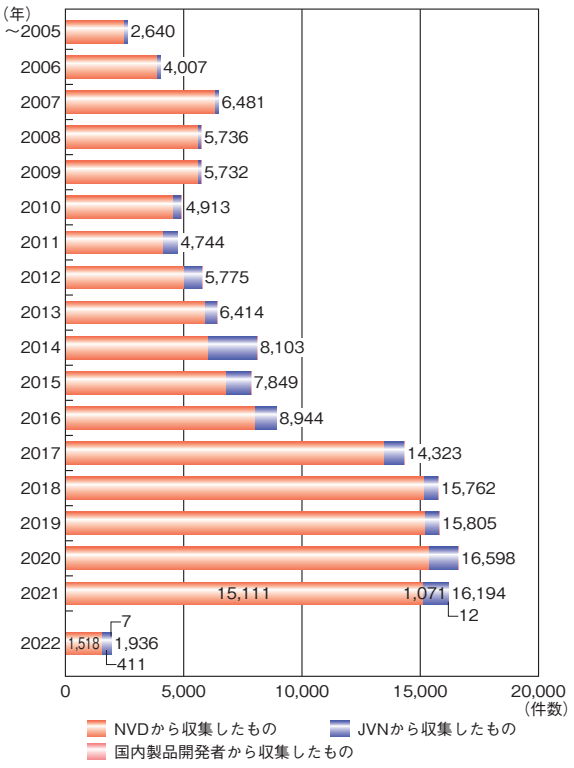
- 脆弱性対策情報ポータルサイト JVN※189 で公表した脆弱性対策情報
- 国内のソフトウェア開発者が公開した脆弱性対策情報
- 米国国立標準技術研究所（NIST：National Institute of Standards and Technology）の脆弱性データベース「NVD※190」で公開された脆弱性対策情報

(a) JVN iPedia の登録件数の推移

JVN iPedia に登録されている情報を、製品ベンダーや情報セキュリティ関連企業が脆弱性情報を公表した年別※191 にまとめると、2012 年以降は NVD から収集した脆弱性対策情報の登録件数がおおむね増加傾向となっており、2018 年以降は 1 万 5,000 件を超えている（図 1-3-1）。なお、2022 年の登録件数の合計は 12 月末時点で 1,936 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、2022 年の登録数も最終的には 2021 年と同程度になる見込みである。2017 年以降、NVD に公開される脆弱性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）※192 の採番機関（CNA：CVE Numbering Authority）※193 が増加したことが一因として挙げられる。The MITRE Corporation（以下、MITRE 社）※194 によると、2016 年 12 月に 47 組織※195 だった CNA は、2022 年 12 月には 263 組織※196 と約 5.6 倍となった。2022 年だけでも 54 組織※197 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情報のうち、JVN が 2022 年に公表したものは 411 件で、2021 年の 1,071 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 2021 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 件の登録があったが、2022 年は 7 件と減少した。なお、国内製品開発者から公表された脆弱性対策情報は通常、登録のタイムラグがないため、今後の大きな増加はない見込みである。

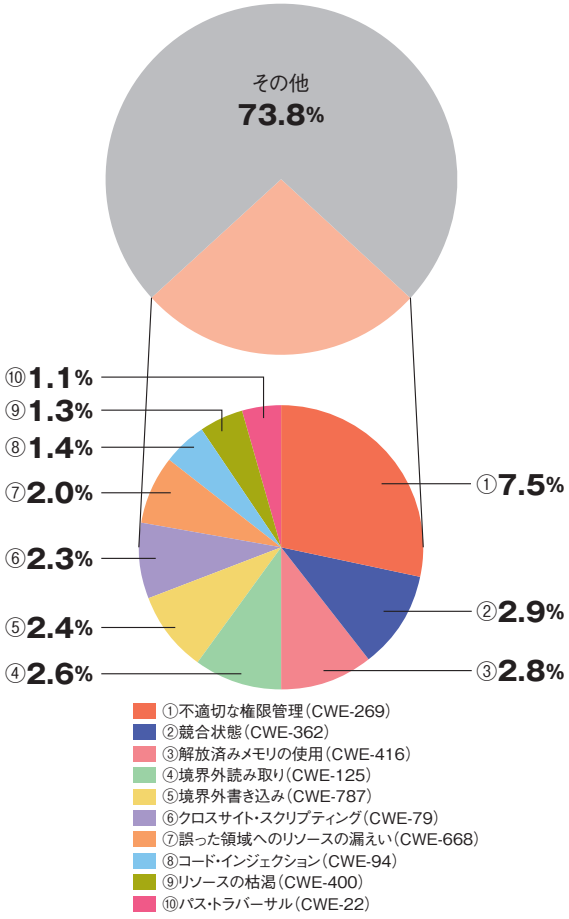
JVN iPedia は、発見された脆弱性の種類を識別するための共通脆弱性タイプ一覧 CWE（Common



■図 1-3-1　JVN iPedia における脆弱性対策情報の公表年別件数
（出典）JVN iPedia の登録情報を基に IPA が作成

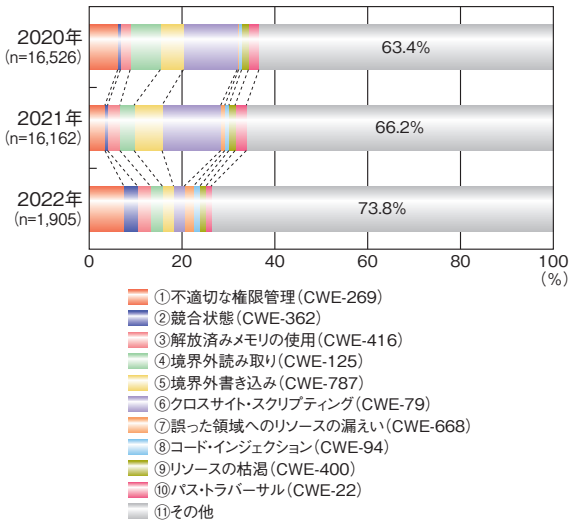
Weakness Enumeration)※198を脆弱性対策情報に付与して登録を行っている。2022年に登録したCWEの割合は上位10種が全体の26.2%を占めており、その内訳を見ると「不適切な権限管理」が7.5%と最も高く、「競合状態」が2.9%、「解放済みメモリの使用」が2.8%、「境界外読み取り」が2.6%と続いている(図1-3-2)。

最も件数の多かった「不適切な権限管理」に分類される脆弱性を悪用されると、管理者権限を取得され、システムを不正に操作される恐れがある。



■図1-3-2 JVN iPediaにおける脆弱性対策情報のCWE別割合(2022年、n=1,905)
(出典)JVN iPediaの登録情報を基にIPAが作成

2020年以降のCWE別割合を年別に見ると、今回1位、2位となった「不適切な権限管理」及び「競合状態」は増加傾向となった一方で、2020年、2021年において上位であった「クロスサイト・スクリプティング」及び「境界外書き込み」は大幅な減少傾向となっている(図1-3-3)。これは、近年NVDから公開される脆弱性対策情報が増加したことを受け、JVN iPediaがMicrosoft社製品やOracle社製品、Apache HTTP Server等広く使われ利用者への影響が大きい製品の脆弱性対策情報の登録を優先する運用としたことが影響していると考えられる。具体的には、優先的に登録した特定の製品の脆弱性対策情報の中で多く採番されたCWEが上位となり、2021年以前の登録の傾向と差異が出た可能性がある。また、11位以下をまとめた「その他」の割合を見ると2021年の66.2%から更に増加し2022年は73.8%となっている。この増加の一因として、JVN iPediaの情報の収集元であるNVDが近年CWEを細分化して採番する傾向にあることが挙げられる。これまで上位10種のCWEに分類されていた脆弱性の一部がそれ以外のより適切なCWEに分類されるようになり、上位10種以外の「その他」にあたるCWEの採番が増えたと考えられる。



■図1-3-3 JVN iPediaにおける脆弱性対策情報のCWE別割合(2020～2022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)※199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、本項と「1.3.1 (2) Internet Explorerのサポート終了について」ではCVSS v2を基に統計処理を行っている。

深刻度には、CVSS v2の基本評価基準(BM:Base Metrics)を基に評価した基本値によるレベルⅠ、レベルⅡ、レベルⅢの3段階があり、数値が大きい程深刻度が高い。

深刻度のレベルごとに想定される影響は以下である。

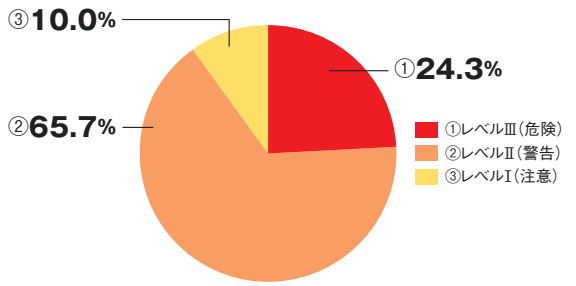
- 深刻度 レベルⅢ(危険):基本値 7.0～10.0

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。

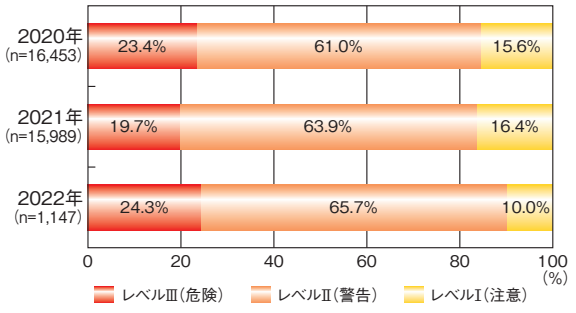
- 深刻度 レベルⅡ(警告):基本値 4.0 ～ 6.9
  一部の情報が漏えいしたり、サービス停止につながったりする等の影響が想定される。
- 深刻度 レベルI(注意):基本値 0.0 ～ 3.9
  深刻度レベルⅡ相当の影響があるが、攻撃するには複雑な条件を必要とする。

2022 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、「レベルⅢ(危険)」が 24.3%、「レベルⅡ(警告)」が 65.7%、「レベルI(注意)」が 10.0% となっており、一部の情報漏えいやサービス停止につながるレベルⅡ以上の脆弱性が全体の 9 割を占めている(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
(2022 年、n=1,147※200)
(出典)JVN iPedia の登録情報を基に IPA が作成

2020 年以降の深刻度のレベル別割合を年別に見ると、レベルⅡ以上の脆弱性の割合は 2020 年が 84.4%、2021 年が 83.6% と若干減少したが、2022 年は 90.0% と増加した。最も深刻度が高いレベルⅢに該当する脆弱性の割合に注目すると、2022 年は 24.3% と 2021 年の 19.7% から 4.6% 増加している(図 1-3-5)。これは、比較的レベルⅢに分類されることが多い「不適切な権限管理」の脆弱性の割合が増加したことや、全体の 73.8% を占める「その他」の脆弱性のうちレベルⅢに分類されるものの割合が増加したことが一因と考えられる。



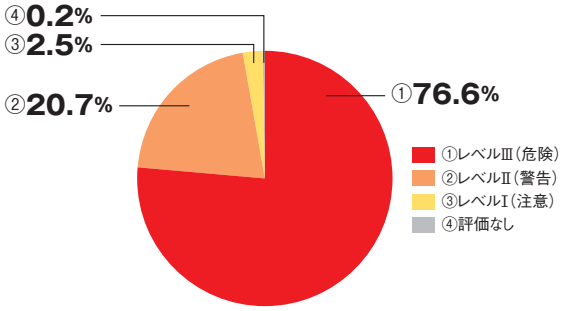
■図 1-3-5　JVN iPedia における脆弱性対策情報のレベル別割合
(2020 ～ 2022 年)
(出典)JVN iPedia の登録情報を基に IPA が作成

製品開発者は、ソフトウェアの企画・設計・製造段階からセキュアコーディング※201 を含めた情報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求められる。

(2) Internet Explorer のサポート終了について

2022 年 6 月 16 日(日本時間)に Microsoft 社より提供されていた Web ブラウザーである Internet Explorer のサポートが終了した※202。サポート終了後には Internet Explorer を利用しようとすると、Microsoft 社が提供する Microsoft Edge に切り替えるよう促す表示がされた。

JVN iPedia には Internet Explorer に関する脆弱性が 2022 年 12 月末時点で 2,045 件登録されている。全体の深刻度 (CVSS v2) の割合は最も高い「レベルⅢ(危険)」が 76.6%、次に高い「レベルⅡ (警告)」が 20.7%、「レベルI(注意)」が 2.5% であった(図 1-3-6)。



■図 1-3-6　2022 年までに JVN iPedia へ登録された Internet Explorer の脆弱性の深刻度別割合(CVSS v2、n=2,049)
(出典)JVN iPedia の登録情報を基に IPA が作成

注目すべき被害事例として、今回の Internet Explorer のサポート終了を契機に他の Web ブラウザーを利用していたにも関わらず、Internet Explorer をアンインストールしていなかったため、意図せず Internet Explorer に関連する、サポート終了後に発見された脆弱性が悪用される事例が発生している。2022 年 11 月に Microsoft 社が公表した Internet Explorer の JScript エンジン「jscript9.dll」におけるリモートコード実行の脆弱性「CVE-2022-41128」によるもので、このセキュリティ更新プログラムが公開される前の 10 月末時点で国家の関与が疑われる攻撃グループによって、ゼロデイ攻撃に悪用されていた※203。脆弱性を悪用する Word ファ

イルがオンライン上にアップロードされており、閲覧者がWordファイルを開いた後にマクロの実行許可を与えた場合、Internet Explorerを介してリモートでコードが実行される恐れがあった。なお、この脆弱性はMicrosoft社の11月のセキュリティ更新プログラムによりWindows OSを修正したことにより解消されている。

今回の被害事例のように、使用を止めてもアンインストールせず、そのまま機器に残しておくと、残存する脆弱性を悪用されてしまう場合がある。サポートが切れたソフトウェアはセキュリティ更新プログラムの配信が基本的に行われないため、アンインストール等の適切な対応が求められる。なお、今回の脆弱性CVE-2022-41128を受けてMicrosoft社からセキュリティ更新プログラムが公開されたが、これはあくまでも根本原因であったWindows OSの脆弱性に対するものであった。そのため、もし今回の根本原因がInternet Explorer側にあった場合はサポート終了しているためセキュリティ更新プログラムが公開されない可能性が高かったものと思われる。

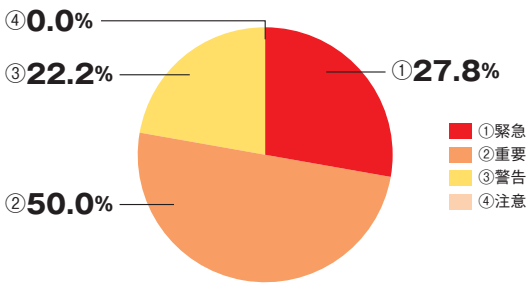
Internet Explorerのサポート終了に伴いMicrosoft社は、後継としてWindows 10から標準搭載されているMicrosoft EdgeにWebブラウザーを切り替えるようアナウンスしている。2029年までの期間限定ではあるものの、Internet Explorerと互換機能を持った「IEモード」が搭載されており、Internet Explorerでしか動作しないWebサイト等を閲覧している場合は、モードを切り替えて利用することもできる。そのため、必要に応じて「IEモード」を活用し、普段利用しているWebサイト等が正しく閲覧できることを検証の上、早期にMicrosoft Edgeへの移行を検討してほしい。更に、移行後はMicrosoft Edgeにおいても脆弱性が公開される可能性があるため、Microsoft社が公開するセキュリティ更新プログラムを定期的に適用することを推奨する。

(3) 標的型攻撃に悪用されたMicrosoft Exchange Serverの脆弱性について

2022年11月のMicrosoft社のセキュリティ更新プログラムの公開と同時に、標的型攻撃に悪用された脆弱性が公表された。今回悪用されたのはMicrosoft社が提供するメールシステムであるMicrosoft Exchange Serverの脆弱性CVE-2022-41040[※204]及びCVE-2022-41082[※205-1]であり、これら二つを組み合わせることで権限を不正に奪い、リモートから任意のコードを実行させることが可能であった。その攻撃手法は「ProxyNotShell」と呼ばれている。悪用されたCVE-2022-41040は権限管理に関する脆弱性で、CVE-2022-41082はリモートでコードが実行される脆弱性である。マイクロソフト社によれば、どちらもCVSS v3[※205-2]は8.8とされ、深刻度が2番目に高い「重要」(CVSS v3基本値7.0～8.9)となる脆弱性であった。

セキュリティ更新プログラムの公開後、ProxyNotShellを悪用した攻撃は減少に転じたが、2022年11月後半よりCVE-2022-41080[※206]及びCVE-2022-41082の二つを組み合わせて悪用する、ProxyNotShellの緩和策を回避する新たな攻撃が確認された。CVE-2022-41080はCVE-2022-41040に似た権限昇格の脆弱性である。今回の攻撃はExchange Serverに付随する「Outlook Web Access(OWA)」というシステムを介し、権限を不正に奪い、リモートでコードを実行するもので、この攻撃手法は、「OWASSRF」と呼ばれている[※207]。CVE-2022-41080はCVE-2022-41040及びCVE-2022-41082と同じく2022年11月のセキュリティ更新プログラムで修正された脆弱性であったが、攻撃者はアップデートを行っていないユーザーを標的として攻撃を仕掛けていた。

以下は2022年にJVN iPediaに登録されたExchange Serverに関する脆弱性の深刻度の割合である(図1-3-7)。



■図1-3-7　2022年にJVN iPediaへ登録されたExchange Serverの深刻度割合(CVSS v3、n=18)
(出典)JVN iPediaの登録情報を基にIPAが作成

2022年に登録されたExchange Serverの件数は18件であり、そのうち深刻度の最も高い「緊急」(CVSS v3基本値9.0～10.0)が27.8%、次に高い「重要」(CVSS v3基本値7.0～8.9)が50.0%となっており、脆弱性が確認された場合、早急に脆弱性の対応が必要な状況にあった。

今回解説したProxyNotShellの攻撃手法はゼロデイの脆弱性を悪用したもので、事前の対策は難しいものであった。しかし、対策情報の確認やセキュリティ更新プログラム公開後にアップデートを行うことでその後の被害を防ぐことができた。一方、OWASSRFは定期的なアッ

プデートを行っていれば防ぐことができるものであった。ゼロデイ攻撃の有無に関わらず被害に遭わないために、Microsoft 社等のベンダーからセキュリティ更新プログラムが公開されたら早急にアップデートすることを推奨する。なお、何らかの理由でアップデートが行えない場合は回避策や緩和策といった代替案を考慮したシステム運用規則を整備しておくことが重要である。

(4) 今後の展望

JVN iPedia へ登録された脆弱性対策情報の累計件数は、2022 年 12 月末時点で 15 万件を超えている。2018 年以降は毎年 1 万 5,000 件前後の脆弱性対策情報が登録されており、2023 年以降も同程度の件数が登録されていくものと考えられる。

2021 年から 2022 年にかけて、医療機関へのサイバー攻撃が複数確認された。例えば、2022 年 10 月、大阪市の病院にて電子カルテ等が暗号化によって閲覧できなくなるランサムウェア攻撃による被害が発生した※208。病院が契約する給食センターの VPN 製品の脆弱性が悪用され、病院とネットワークがつながっていたため、病院内のネットワークに悪意ある第三者が侵入した(「1.2.1(2)(b)医療機関における被害事例」参照)。

今回の被害が発生した背景・要因として、医療機関においては脆弱性への対応が難しいことが挙げられる。本事案で原因となった VPN 製品の脆弱性について、2022 年 1 月 31 日～ 2 月 28 日に実施された一般社団法人医療 ISAC のアンケート調査※209 によると、四病院団体協議会に加盟している調査対象の 1,144 病院のうち VPN 製品を利用しているのが 4 割、その中で 3 割程の病院が VPN 製品の脆弱性に未対応であると回答していた。また、2021 年 10 月に発生した徳島県つるぎ町立半田病院の事案に関して 2022 年 6 月に公表された調査報告書では、医療現場では利用しているシステムにおいてソフトウェアの予期せぬ不具合を避けようと OS 等のアップデートを行わず、脆弱性が残存すると考えられるアップデートされていない OS をそのまま使用していたことが指摘されている※210。

このような状況から、攻撃者にとって病院は攻撃が成功しやすい対象とみなされ、今後も医療機関を標的にするために関連する情報収集が行われる恐れがある。それとともに、セキュリティの研究者も医療関係機器やソフトウェアに対して調査・研究を行い、脆弱性が発見される可能性がある。その結果、それら脆弱性情報の公開が増え、2023 年以降 JVN iPedia にも多数登録されるのではないかと考える。

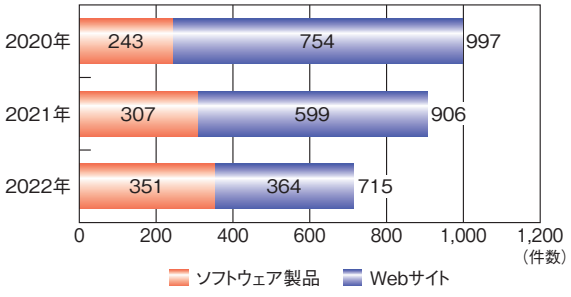
前述の医療機関だけでなく、それ以外の業種、分野においても、アップデートによるソフトウェアの不具合を懸念し、脆弱性に対して適切な対応が行われていないケースや、サポートが切れた古いソフトウェアを使い続けているケースがあると考える。自組織でも同様の被害が発生する恐れがあるということを認識し、情報収集の手段の一つとして JVN iPedia を活用いただきたい。

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、2022 年も引き続き発生している。

2022 年に脆弱性を悪用された被害事例として、Web サイトのシステムに脆弱性があり、その脆弱性が悪用された結果、クレジットカード情報が約 11 万件漏えいし、不正利用された可能性があるという発表がされた※212。このような情報漏えいを含め、脆弱性を悪用した攻撃による被害を抑制する仕組みとして、脆弱性に関する情報を発見者に届出してもらい、修正を促すため製品開発者や Web サイト運営者に連絡する情報セキュリティ早期警戒パートナーシップ制度がある。

「情報セキュリティ早期警戒パートナーシップ※213」(以下、パートナーシップ)は、IPA と JPCERT/CC が運営し、脆弱性関連情報の届出※214 を受け付けているが、2022 年に届出された件数は、ソフトウェア製品が 351 件、Web サイトが 364 件、合計 715 件であった(図 1-3-8)。

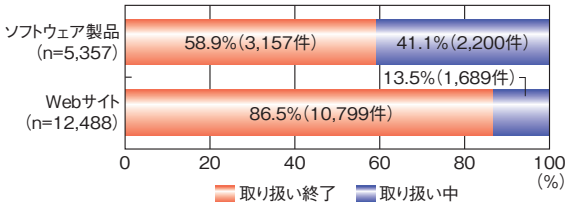


■図 1-3-8　脆弱性関連情報の種類別届出状況(2020 ～ 2022 年)
(出典)パートナーシップの届出状況を基に IPA が作成

2022 年のソフトウェア製品及び Web サイトの総届出件数(715 件)と、2021 年の件数(906 件)を比較すると、約 21% 減少している。なお、2022 年のソフトウェア製品と Web サイト個々の件数を 2021 年の件数と比較すると、ソフトウェア製品の届出は約 14% 増加、Web サイトの

届出は約 39% 減少した。

パートナーシップ開始時点（2004 年 7 月 8 日）から 2022 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 5,357 件、Web サイトは 1 万 2,488 件、合計は 1 万 7,845 件に上る。これらの届出のうち IPA での取り扱いが終了※215 した届出件数は、ソフトウェア製品 3,157 件（58.9%）、Web サイト 1 万 799 件（86.5%）である（図 1-3-9）。



■図 1-3-9　脆弱性関連情報の種類別取り扱い終了状況
（2022 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

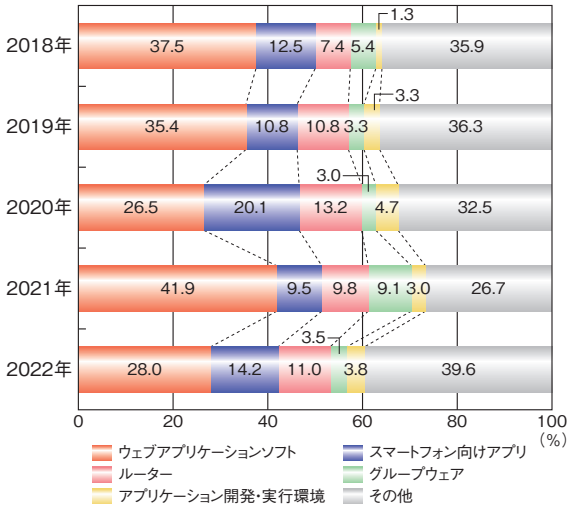
(1) ソフトウェア製品の脆弱性

2022 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) 2022 年のパートナーシップの届出受付動向

図 1-3-10 は、2018 年から 2022 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。届出受付数は、2019 年は前年より減少し 212 件だったが、2020 年から増加に転じ、2022 年は 346 件と過去 5 年間で一番多くなった。2022 年のソフトウェア製品の届出のうち、製品開発者による自社製品に関する届出は、346 件中 21 件であった。

図 1-3-11 は、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 年に割合が増加したものは「その他」を除くと「スマートフォン向けアプリ」「ルーター」「アプリケーション開発・実行環境」で、それぞれ前年の 9.5% から 14.2%、9.8% から 11.0%、3.0% から 3.8% に増加した。「ウェブアプリケーションソフト※216」「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。

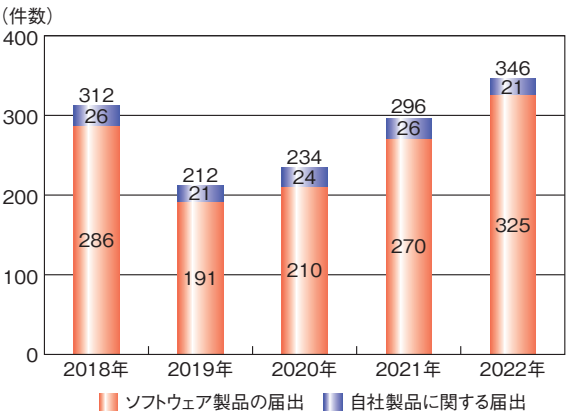


■図 1-3-11　製品種類別のソフトウェア製品の届出受付数の割合
（2018 ～ 2022 年）
（出典）パートナーシップの届出状況を基に IPA が作成

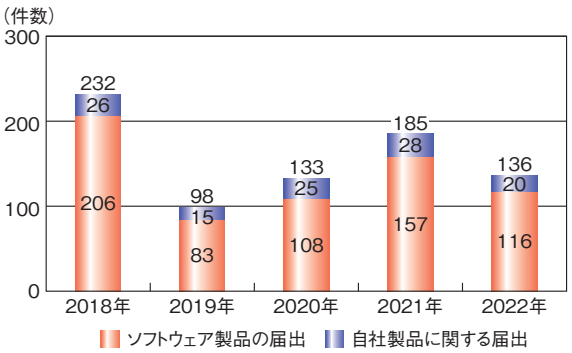
(b) 2022 年の JVN 公表の動向

パートナーシップに届出のあった脆弱性対策情報のうち 2022 年に JVN 公表に至った件数は、136 件であった。

図 1-3-12 は、届出のうち 2018 年から 2022 年までの 5 年間の JVN 公表数を示している。2018 年と比べて 2019 年では JVN 公表数は減少し、2020 年、2021 年と増加傾向にあったが、2022 年は再度減少し、2020 年と同程度の件数であった。また 2022 年に公表した自社製品に関する届出は 20 件であった。



■図 1-3-10　ソフトウェア製品の不受理を除いた届出受付数
（2018 ～ 2022 年）
（出典）パートナーシップの届出状況を基に IPA が作成



■図 1-3-12　届出されたソフトウェア製品のうち JVN 公表した件数
（2018 ～ 2022 年）
（出典）パートナーシップの届出状況を基に IPA が作成

JVN 公表の際に、製品利用者が脆弱性対策を実施する優先度を判断するのに重要な補足情報（当該脆弱性を使った攻撃が確認されている等）がある場合は、より迅速な脆弱性対策ができるよう、トップページの新着リスト及び脆弱性レポートの両方に「緊急」である旨を掲載している。2022 年に「緊急」とした JVN 公表は 3 件あった（表 1-3-1）。

項番	JVN 番号	件名	CVSSv3 基本値	攻撃の有無
1	JVN#74592196	bingo!CMS における認証回避の脆弱性	7.5	有
2	JVN#36454862	Trend Micro Apex One および Trend Micro Apex One SaaS における複数の脆弱性	8.2	有
3	JVN#96561229	FUJITSU Network IPCOM の運用管理インタフェースにおける複数の脆弱性	9.8	不明

■表 1-3-1　2022 年に「緊急」として JVN 公表した脆弱性対策情報（公表順）
（出典）JVN を基に IPA が作成

表 1-3-1 の中、最も影響が大きいものは JVN#96561229※217 であり、CVSS v3 基本値が 9.8 であった。これは、富士通株式会社の統合ネットワークアプライアンス FUJITSU Network IPCOM の運用管理インターフェースに、複数の脆弱性が存在しているもので、製品開発者が製品利用者へ広く周知するためにパートナーシップに届出し、JVN 公表に至った。複数の脆弱性とは、Web コンソールにおける OS コマンドインジェクション、及びコマンドラインインターフェースにおけるバッファーオーバーフローである。これらの脆弱性の想定される影響としては、遠隔の第三者によって、任意の OS コマンドを実行される、機微な情報を窃取または改ざんされる、サービス運用妨害（DoS：Denial of Service）攻撃を受ける等であった。

「緊急」として掲載されている脆弱性情報については、早急に自組織への影響を確認し、影響がある場合は対策を検討いただきたい。

(c) 製品開発者の CNA への参加

IPA とともにパートナーシップを運営している JPCERT/CC は、パートナーシップに届出された脆弱性を JVN 公表する際に、脆弱性の共通識別子である CVE※218 を採番している。この CVE を採番できる組織のことを、採番機関（CNA※219）という。CVE を運用している MITRE 社から認定を受けることで、CNA として CVE を採番できる。CNA の認定は、脆弱性の調整活動を行う中立的な組織だけでなく、製品開発者も受けることができる。

CNA として認定を受けるためには、脆弱性開示ポリシーを自組織サイトにおいて公表していること、セキュリティアドバイザリ掲載場所として URL 等が準備されていることといった一定の基準を満たす必要がある※220。

JPCERT/CC は、CNA の招致、トレーニング、管理等を実施する Root CNA（以下、Root）として 2018 年に MITRE 社から認定されており、その配下に複数の CNA が存在している。JPCERT/CC は、製品開発者が CNA として活動することを推奨※221 しており、2021 年までに 5 社が JPCERT/CC を Root とする CNA として登録されていたが、2022 年には新たに株式会社日立製作所とキヤノン株式会社の 2 社が CNA となり、Root の JPCERT/CC を含め 8 社となった。

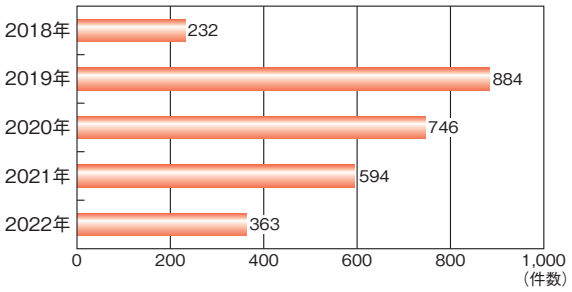
2023 年 3 月末現在、JPCERT/CC を Root としない 2 組織を含め、日本では 10 組織の CNA が活動しており、国別にみると、米国（149 組織）、中国（18 組織）、ドイツ（14 組織）に次いで 4 番目となっている※222。

製品開発者が CNA として活動することで、自社製品の脆弱性に対し、自ら CVE を採番でき、迅速な脆弱性対策の公表が可能になると考えられる。今後も CNA となる製品開発者が増えることが期待される。

(2) Web サイトの脆弱性

2022 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 1 件を除く）は、363 件であった。

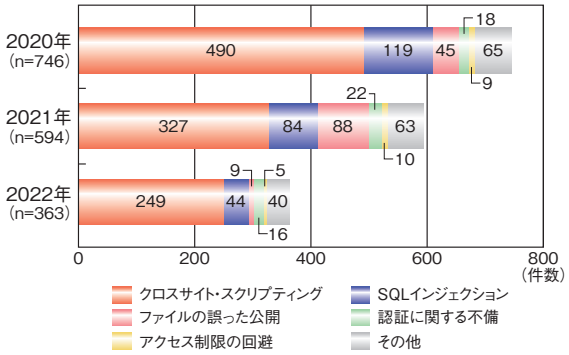
図 1-3-13 は、2018 年から 2022 年までの Web サイトの届出件数（不受理を除く）を示している。前年を大きく上回った 2019 年の届出件数をピークに、届出件数は減少傾向にある。



■図 1-3-13　Web サイトの不受理を除いた届出受付数（2018 ～ 2022 年）
（出典）パートナーシップの届出状況を基に IPA が作成

(a) パートナーシップから見る 2022 年の届出の傾向

図 1-3-14 は、2020 年から 2022 年までに受け付けた届出（不受理を除く）における脆弱性の種類別内訳を示している。2022 年も 2020 年、2021 年と同様に「クロスサイト・スクリプティング」と「SQL インジェクション」の届出件数が多い傾向にある。



■図 1-3-14　Web サイトの届出における脆弱性内訳（2020 ～ 2022 年）
（出典）パートナーシップの届出状況を基に IPA が作成

(b) Web サイト運営者による脆弱性対応期間の傾向

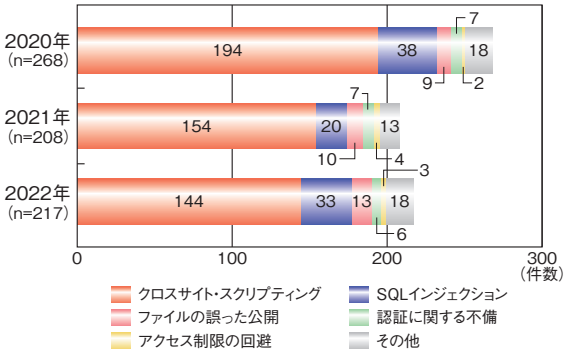
パートナーシップでは、届出された脆弱性情報を Web サイト運営者へ通知し、Web サイトの脆弱性対応が完了した際には、IPA に修正完了を報告するよう依頼している。

図 1-3-15 は、2020 年から 2022 年において、IPA にて修正が完了したと判断した届出について、脆弱性種別の内訳を示している。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。届出件数は、2021 年の 594 件から 2022 年の 363 件と大幅に減少している（図 1-3-14）一方で、修正完了件数は 2021 年と 2022 年ともに 200 件を超えている（図 1-3-15）。

パートナーシップのガイドライン※223 では、Web サイト運営者が IPA より脆弱性情報の通知を受け、修正完了報告を行うまでの期間の目処を 3 ヵ月以内と規定している。

脆弱性情報を Web サイト運営者へ通知し、修正完了と判断した日までの経過日数（以下、対応期間）について、修正が完了した件数が多い「クロスサイト・スクリプティング」の対応期間の割合を図 1-3-16 に示す。また、「SQL インジェクション」の対応期間の割合を図 1-3-17 に示す。

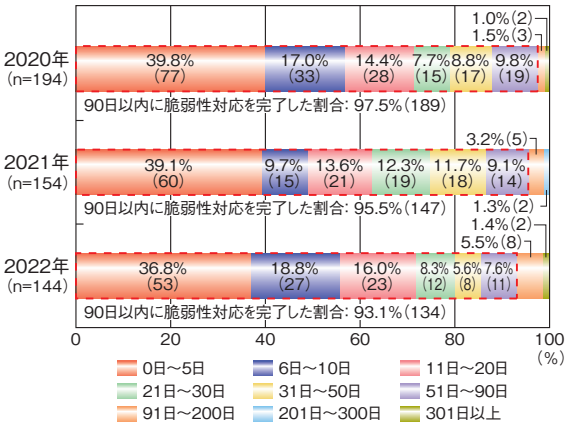
2022 年の「クロスサイト・スクリプティング」の対応期間は、修正完了件数（144 件）に対し、30 日以内に脆弱



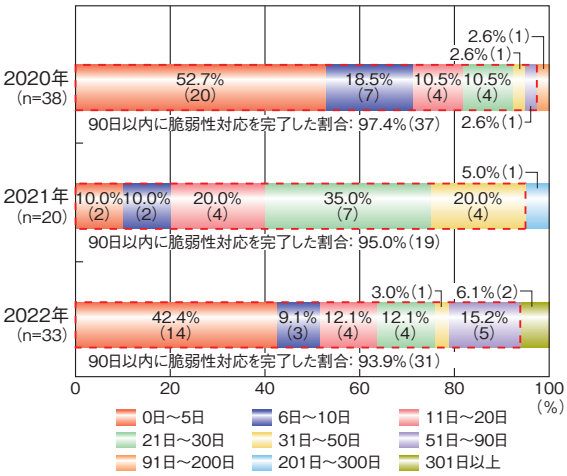
■図 1-3-15　修正完了と判断した件数（2020 ～ 2022 年）
（出典）パートナーシップの届出状況を基に IPA が作成

性対応を完了した割合は 79.9%（115 件）、90 日以内（図中の赤点線枠内）に脆弱性対応を完了した割合は 93.1%（134 件）であった（図 1-3-16）。

2022 年の「SQL インジェクション」の対応期間は、修正完了件数（33 件）に対し、30 日以内に完了した割合



■図 1-3-16　クロスサイト・スクリプティングにおける脆弱性対応期間の割合（2020 ～ 2022 年）
（出典）パートナーシップの届出状況を基に IPA が作成



■図 1-3-17　SQL インジェクションにおける脆弱性対応期間の割合（2020 ～ 2022 年）
（出典）パートナーシップの届出状況を基に IPA が作成

が 75.8%（25 件）、90 日以内に完了した割合が 93.9%（31 件）であった（前ページ図 1-3-17）。なお、2021 年の 0 日～ 5 日の対応期間の割合は、2020 年、2022 年と比べて大幅に低くなっている。これは新型コロナウイルスによる緊急事態宣言での勤務形態の変更や自宅療養者増加等を原因とした業務逼迫により、通常業務を優先し、脆弱性対応が後手に回った可能性が考えられる。ただし、2021 年の「SQL インジェクション」の修正完了件数は 20 件であり、2020 年の 38 件、2022 年の 33 件と比べ少なかったことから顕著な差異が発生した可能性もある。

「クロスサイト・スクリプティング」「SQL インジェクション」ともに 2020 年、2021 年、2022 年は、90 日以内に脆弱性対応を完了している割合が 90% を超えており、高い状態が継続している。

(c) Web サイト運営者に求められる対策

図 1-3-16（前ページ）、図 1-3-17（前ページ）のとおり、90 日以内に脆弱性対応を完了した割合が高く、Web サイト運営者が危機感を持ち迅速に対応したと推測される。一方で脆弱性の修正がされないまま対応が長期に渡っている組織もある。IPA が状況を確認したところ「来年のシステム改修時に対応する」との回答もあった。

Web サイトの脆弱性対応に当たっては、費用、体制、時間等のリソースが必要となる。Web サイトを新規に構築、更新する際には予算、スケジュール等をあらかじめ立てて対応できるが、脆弱性対応は、脆弱性の発見、インシデントの発生等により想定外のタイミングで必要となることが多い。

このため、脆弱性対応の必要性を理解し、あらかじめ脆弱性対応やインシデント対応時の方針を定めておくことが重要である。IPA では、「安全なウェブサイト運営にむけて※ 224」「ウェブサイト運営者のための脆弱性対応ガイド※ 225」「セキュリティ担当者のための脆弱性対応ガイド※ 226」等の資料を公表しているので、脆弱性対応の方針検討に活用いただきたい。

COLUMN

CODE BLUEが挑戦してきた、日本のサイバーセキュリティの多様性とエコシステム

サイバーセキュリティ国際会議 CODE BLUE　発起人　篠田 佳奈

2022 年で「CODE BLUE」の開催は 10 回目となり、世界トップクラスの、日本発のサイバーセキュリティ国際カンファレンスを作り上げていく中で、様々な多様性を含んだものに育っていきました。

まず、カンファレンスの審査に国際的な多様性を持たせることは、最初から意識していた点で、レビューボードは国内外の方々にお願いしました。日本の国境は海の上にありますから、会議名が表すとおり、「CODE（技術）」を使って「BLUE（海）」を超えること、すなわち、外から入れることにも、内から発信していくことにも、一貫して変わらず努力しています。言語のバリアフリー化ですべての内容を日本語と英語で提供し、海外の方にも分かるようにしてきました。英語を母国語としない講師が彼らの母国語で講演できるように通訳を用意するなど、国際ステージとして国内外の人に認められる舞台づくりを心がけてきました。講演内容もテクニカルのみならず、法律・政策、サイバー犯罪等を混ぜ、様々な分野の交流も試みてきました。専門化したイベントが増える中、「弁護士を混ぜるのは良いアイデアではないよ」と冷たい目で見る人もいましたが、多くの方から新しく学んだ喜びを伝えていただきました。

CBNOC（CODE BLUE Network Operation Center）というネットワークインフラ整備班を設けたのもその一つです。CBNOC は文字どおり CODE BLUE の通信インフラを担う役割ですが、裏の目的としてセキュリティ業界とネットワーク業界の間にある目に見えない溝を埋めてもらうことがあります。例えば、APNIC（Asia Pacific Network Information Centre）に参加した物理学専攻の女子学生が成人して CBNOC に来てくれたり、セキュリティに強い若者が CBNOC を縁としてネットワーク系企業に就職したり、今ではネットワーク系の集まりに参加すると「CBNOC でした!」と駆け寄ってくる若者が増えました。

若者を積極的に巻き込む施策として、25 歳以下の優秀な若者への講演枠「U25」や、優秀な発表者への研究奨励金の提供、学生スタッフの雇用があります。研究奨励金は、学校に目当てのコースがなくても自分で勉強ができる人等にも良いシステムではないかなと思います。

学生スタッフは、毎年定員の数倍もの応募がある人気のポストで、1 日働けば 1 日聴講できるシステムです。学生スタッフは自分達がこれから入る業界を知り、企業を知り、同年代の友を知り、時に講師やスタッフともつながります。最初は 1 名から始まった学生スタッフですが、最大で 60 名の時もありました。業界に入った学生スタッフが協賛企業の社員となって帰ってきたりすることも増えました。良いエコシステムとして育ってきていると思います。

こうして、ゆっくりとでも、CODE BLUE を介して、それまで交わりがなかった人達が交わり、影響を与え合うことで、必ず社会に良い価値を生んでくれることと信じています。

まだまだ挑戦したい試みはあります。これからもみなさんのご意見をうかがいながら、カラフルに CODE BLUE を成長させ、社会の役に立てていきたいと思います。

※ 1　https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf〔2023/5/11 確認〕
※ 2　https://apwg.org/trendsreports/〔2023/5/11 確認〕
※ 3　https://www.ibm.com/jp-ja/security/services/ibm-x-force-incident-response-and-intelligence〔2023/5/11 確認〕
※ 4　Mandiant 社：Get Your Copy of M-Trends 2023 Today https://www.mandiant.com/m-trends〔2023/5/11 確認〕
※ 5　https://mandiant.widen.net/s/rphjwkvzgp/rpt-mtrends-2021-3〔2023/7/3 確認〕
※ 6　https://mandiant.widen.net/s/bjhnhps2mt/m-trends-2022-report〔2023/7/3 確認〕
※ 7　Microsoft 社：An overview of Russia's cyberattack activity in Ukraine　https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd〔2023/5/19 確認〕
※ 8　「マルウェア」等の用語を混在して使用すると、読者を混乱させる可能性があるため、本白書では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、総称して「ウイルス」と表現する。
※ 9　CERT-UA：https://cert.gov.ua/article/18101〔2023/5/19 確認〕
上記の Web ページのタイトルはウクライナ語のため省略している。
※ 10-1 https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf〔2023/5/11 確認〕
※ 10-2 X Corp.：An incident impacting some accounts and private information on Twitter　https://privacy.twitter.com/en/blog/2022/an-issue-affecting-some-anonymous-accounts〔2023/5/11 確認〕
※ 10-3 REUTERS：Twitter hacked, 200 million user email addresses leaked, researcher says　https://www.reuters.com/technology/twitter-hacked-200-million-user-email-addresses-leaked-researcher-says-2023-01-05/〔2023/5/11 確認〕
※ 10-4 Bleeping Computer：Twitter claims leaked data of 200M users not stolen from its systems　https://www.bleepingcomputer.com/news/security/twitter-claims-leaked-data-of-200m-users-not-stolen-from-its-systems/〔2023/5/26 確認〕
BBC：Twitter says leaked emails not hacked from its systems　https://www.bbc.com/news/technology-64243369〔2023/5/26 確認〕
※ 10-5 Singtel Optus Pty Limited：Optus notifies customers of cyberattack compromising customer information　https://www.optus.com.au/about/media-centre/media-releases/2022/09/optus-notifies-customers-of-cyberattack〔2023/5/19 確認〕
※ 10-6 RREUTERS：Singtel assesses potential cost of Optus Australian data breach　https://www.reuters.com/technology/singtel-assesses-potential-cost-optus-australian-data-breach-2022-10-03/〔2023/5/19 確認〕
※ 10-7 REUTERS：Medibank says hacker accessed data of 9.7 million customers, refuses to pay ransom　https://www.reuters.com/business/healthcare-pharmaceuticals/medibank-says-hacker-accessed-data-97-mln-customers-refuses-pay-ransom-2022-11-06/〔2023/5/11 確認〕
※ 10-8 MBSD 社のご厚意により本白書向けに集計・提供頂いた情報を掲載している。
※ 10-9 https://www.jpcert.or.jp/pr/2023/IR_Report2022Q4.pdf〔2023/5/16 確認〕
※ 10-10 https://www.antiphishing.jp/report/monthly/〔2023/5/16 確認〕
※ 10-11 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf〔2023/5/16 確認〕
※ 10-12 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf〔2023/5/16 確認〕
※ 10-13 JPCERT/CC：JPCERT/CC インシデント報告対応レポート 2022 年 1 月 1 日 ～ 2022 年 3 月 31 日　https://www.jpcert.or.jp/pr/2022/IR_Report2021Q4.pdf〔2023/6/15 確認〕
※ 10-14 JPCERT/CC：JPCERT/CC インシデント報告対応レポート 2021 年 1 月 1 日 ～ 2021 年 3 月 31 日　https://www.jpcert.or.jp/pr/2021/IR_Report20210415.pdf〔2023/6/15 確認〕
※ 10-15 フィッシング対策協議会：緊急情報　https://www.antiphishing.jp/news/alert/〔2023/5/16 確認〕
※ 10-16 フィッシング対策協議会:国税庁をかたるフィッシング（2022/08/15）　https://www.antiphishing.jp/news/alert/nta_20220815.html〔2023/5/16 確認〕
フィッシング対策協議会：国税庁をかたるフィッシング（2022/08/23）　https://www.antiphishing.jp/news/alert/nta_20220823.html〔2023/5/16 確認〕
フィッシング対策協議会：国税庁をかたるフィッシング（2022/09/20）　https://www.antiphishing.jp/news/alert/nta_20220920.html〔2023/5/16 確認〕
フィッシング対策協議会：国税庁をかたるフィッシング（2023/05/15）　https://www.antiphishing.jp/news/alert/nta_20230515.html〔2023/5/30 確認〕
※ 10-17 安心相談窓口だより　国税庁をかたる偽ショートメッセージサービス（SMS）や偽メールに注意　https://www.ipa.go.jp/security/anshin/attention/2022/mgdayori20221031.html〔2023/5/16 確認〕
※ 10-18 フィッシング対策協議会：2022/09 フィッシング報告状況　https://www.antiphishing.jp/report/monthly/202209.html〔2023/5/16 確認〕
※ 10-19 フィッシング対策協議会：2022/09 フィッシング報告状況　https://www.antiphishing.jp/report/monthly/202209.html〔2023/5/16 確認〕
フィッシング対策協議会：2022/10 フィッシング報告状況　https://www.antiphishing.jp/report/monthly/202210.html〔2023/5/16 確認〕
フィッシング対策協議会：2023/01 フィッシング報告状況　https://www.antiphishing.jp/report/monthly/202301.html〔2023/5/16 確認〕
フィッシング対策協議会：2023/02 フィッシング報告状況　https://www.antiphishing.jp/report/monthly/202302.html〔2023/5/16 確認〕
※ 11　警察庁：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　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf〔2023/4/19 確認〕
※ 12　トレンドマイクロ社：2022 年脅威動向をふりかえる～広がり続けるアタックサーフェス、企業が取り組むべき最優先事項は何か～　https://www.trendmicro.com/ja_jp/jp-security/22/l/securitytrend-20221212-01.html〔2023/4/19 確認〕
ダイヤモンド・オンライン：ランサムウェア攻撃の被害が増加している背景は何か。デロイトが企業経営者に「攻撃者目線」での対策を主張している理由　https://diamond.jp/articles/-/312168〔2023/4/19 確認〕
サイバーリーズン合同会社：彼を知り己を知れば百戦殆からず ～ランサムウェアの歴史、組織、攻撃手法とその実態を徹底攻略～　https://www.cybereason.co.jp/blog/ransomware/9101/〔2023/4/19 確認〕
※ 13　トレンドマイクロ社：Smart Protection Network から見る世界と日本の最新サイバー脅威動向　https://www.trendmicro.com/ja_jp/jp-security/22/g/securitytrend-20220719-03.html〔2023/4/19 確認〕
※ 14　パロアルトネットワークス株式会社：LockBit 2.0: ランサムウェア・アズ・ア・サービス (RaaS) のオペレーションとその対策　https://unit42.paloaltonetworks.jp/lockbit-2-ransomware/〔2023/4/19 確認〕
※ 15　トレンドマイクロ社：「ランサムウェア攻撃 グローバル実態調査 2022 年版」を発表　https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220907-01.html〔2023/4/19 確認〕
※ 16　IPA：コンピュータウイルス・不正アクセスの届出事例［2022 年上半期（1 月～ 6 月）］　https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000100440.pdf〔2023/4/19 確認〕
IPA：コンピュータウイルス・不正アクセスの届出事例［2022 年下半期（7 月～ 12 月）］　https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000108764.pdf〔2023/4/19 確認〕
※ 17　NHK 政治マガジン：トヨタ国内全工場停止 サイバー攻撃の可能性　https://www.nhk.or.jp/politics/articles/lastweek/78407.html〔2023/5/11 確認〕
※ 18　小島プレス工業：ウィルス感染被害によるシステム停止事案発生のお知らせ　https://www.kojima-tns.co.jp/wp-content/uploads/2022/08/ ウィルス感染被害によるシステム停止事案発生のお知らせ-2.pdf〔2023/4/19 確認〕
※ 19　小島プレス工業：小島プレス工業株式会社 システム停止事案調査報告書（第 1 報）　https://www.kojima-tns.co.jp/wp-content/uploads/2022/03/20220331_システム障害調査報告書（第 1 報）.pdf〔2023/4/19 確認〕
※ 20　NHK NEWS WEB:小島プレス工業「子会社のリモート接続機器に“ぜい弱性”」　https://www3.nhk.or.jp/news/html/20220401/k10013563241000.html〔2023/2/10 確認〕
※ 21　読売新聞オンライン：トヨタ関連6万社のうち、1社のセキュリティー破られ…「賭けはできない」全工場停止　https://www.yomiuri.co.jp/national/20220614-OYT1T50054/〔2023/4/19 確認〕
※ 22　読売新聞オンライン：【独自】トヨタ工場の停止、ハッカー集団「ロビンフッド」関与…未確認ウイルスのため即復旧を断念　https://www.yomiuri.co.jp/national/20220613-OYT1T50213/〔2023/4/19 確認〕
※ 23　大阪急性期・総合医療センター：「電子カルテシステム」の障害発生について　https://www.gh.opho.jp/pdf/info20221031.pdf〔2023/4/19 確認〕
※ 24　大阪急性期・総合医療センター：情報セキュリティインシデント調査委員会報告書について https://www.gh.opho.jp/important/785.html〔2023/4/19 確認〕
※ 25　読売新聞オンライン:大阪の病院で電子カルテシステムに障害、「ラ

ンサムウェア」によるサイバー攻撃か　https://www.yomiuri.co.jp/national/20221031-OYT1T50162/〔2023/4/19 確認〕
※ 26 朝日新聞デジタル：大阪の医療センターにサイバー攻撃　手術延期、外来診療できない状態　https://www.asahi.com/articles/ASQB075DWQB0OXIE022.html〔2023/4/19 確認〕
※ 27 NHK NEWS WEB：大阪急性期・総合医療センター サイバー攻撃で診療影響続く　https://www3.nhk.or.jp/kansai-news/20221101/2000067859.html〔2023/2/10 確認〕
※ 28 NHK NEWS WEB：サイバー攻撃受けた病院 給食業者経由でウイルス侵入か 大阪　https://www3.nhk.or.jp/kansai-news/20221107/2000068042.html〔2023/2/10 確認〕
朝日新聞デジタル：病院へのサイバー攻撃、リモート操作許し被害拡大か　3病院にも影響　https://www.asahi.com/articles/ASQDR67BWQDQULZU00J.html〔2023/4/19 確認〕
※ 29 Security NEXT：給食委託先経由で侵入された可能性 - 大阪急性期・総合医療センター　https://www.security-next.com/141214/2〔2023/4/19 確認〕
※ 30 https://piyolog.hatenadiary.jp/entry/2022/11/01/013707〔2023/4/19 確認〕
※ 31 IPA：【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について　https://www.ipa.go.jp/archive/security/security-alert/2020/ransom.html〔2023/4/19 確認〕
※ 32 Zscaler, Inc.：2022 年版 ThreatLabz ランサムウェアレポート　https://www.zscaler.jp/resources/industry-reports/2022-threatlabz-ransomware-report.pdf〔2023/4/19 確認〕
※ 33 読売新聞オンライン：サイバー攻撃受けた大阪の病院、災害用BCPは作成していたが…「訓練とは全く違った」　https://www.yomiuri.co.jp/national/20221211-OYT1T50104/〔2023/4/19 確認〕
※ 34 サイバーリーズン合同会社：脅威ハンティング：LOLBin から企業の最重要資産まで　https://www.cybereason.co.jp/blog/cyberattack/7964/〔2023/4/19 確認〕
※ 35 日経クロステック：検知困難な「LOL 攻撃」の実態　https://xtech.nikkei.com/atcl/nxt/mag/nnw/18/111900071/051800031/〔2023/4/19 確認〕
トレンドマイクロ社：ランサムウェア攻撃で悪用された正規ツールを解説　https://www.trendmicro.com/ja_jp/research/21/i/describing-legitimate-tools-exploited-for-ransomware-attacks.html〔2023/4/19 確認〕
※ 36 IRM（Information Rights Management）：業務で使用する文書ファイル等を暗号化し、閲覧や編集等を制限する仕組み。
※ 37 JPCERT/CC：インシデントハンドリングマニュアル　https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20211130.pdf〔2023/4/19 確認〕
※ 38 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〔2023/4/19 確認〕
※ 39 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〔2023/4/19 確認〕
※ 40 https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000024542.pdf〔2023/4/19 確認〕
※ 41 IPA：標的型サイバー攻撃の事例分析と対策レポート　https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000024536.pdf〔2023/4/19 確認〕
※ 42 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、メモリ上で実行・動作するタイプのウイルスのこと。
※ 43 Cybersecurity and Infrastructure Security Agency（CISA）：CISA, FBI, NSA, and International Partners Issue Advisory on Demonstrated Threats and Capabilities of Russian State-Sponsored and Cyber Criminal Actors　https://www.cisa.gov/news/2022/04/20/cisa-fbi-nsa-and-international-partners-issue-advisory-demonstrated-threats-and〔2023/4/19 確認〕
トレンドマイクロ社：ウクライナ侵攻とサイバー攻撃 ～日本企業が行うべき対策～　https://www.trendmicro.com/ja_jp/jp-security/22/e/securitytrend-20220516-01.html〔2023/4/19 確認〕
※ 44 IPA：サイバーレスキュー隊（J-CRAT）活動状況［2022 年度上半期］　https://www.ipa.go.jp/security/j-crat/ug65p9000000nks8-att/000106897.pdf〔2023/4/19 確認〕
※ 45 NTT セキュリティホールディングス株式会社：Operation RestyLink: 日本企業を狙った標的型攻撃キャンペーン　https://insight-jp.nttsecurity.com/post/102ho8o/operation-restylink〔2023/4/19 確認〕
※ 46 Go 言語製のウイルスは、C/C++ 言語製のウイルスと比べてまだ一般的ではない。Go 言語では、関数量が膨大であるという特徴を持つため解析に時間がかかるとされる。
株式会社 FFRI セキュリティ：進化する Go 言語製マルウェアとどう戦うか？：解析能力向上に向けての実践的テクニック　https://jsac.jpcert.or.jp/archive/2023/pdf/JSAC2023_2_1_kuwabara_jp.pdf〔2023/4/19 確認〕
※ 47 株式会社マクニカ：ショートカットと ISO ファイルを悪用する攻撃キャンペーン　https://security.macnica.co.jp/blog/2022/05/iso.html〔2023/4/19 確認〕
※ 48-1 トレンドマイクロ社：日本を含む東アジアを狙った「Earth Yako」による標的型攻撃キャンペーンの詳解　https://www.trendmicro.com/ja_jp/research/23/a/targeted-attack-campaign-earth-yako.html〔2023/4/19 確認〕
※ 48-2 トレンドマイクロ社：標的型攻撃のターゲットは組織内から組織外の個人へ～サプライチェーンを形成する標的型攻撃～　https://www.trendmicro.com/ja_jp/jp-security/23/f/expertview-20230626-03.html〔2023/7/3 確認〕
※ 49 警察庁、NISC：学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について（注意喚起）　https://www.nisc.go.jp/pdf/press/20221130NISC_press.pdf〔2023/4/19 確認〕
NISC：標的型サイバー攻撃、不審メールにご注意ください!　https://www.nisc.go.jp/pdf/press/20221130NISC_gaiyou.pdf〔2023/4/19 確認〕
※ 50 NIST：CVE-2022-1388 Detail　https://nvd.nist.gov/vuln/detail/CVE-2022-1388〔2023/4/19 確認〕
F5, Inc.：Final - K23605346: BIG-IP iControl REST vulnerability CVE-2022-1388　https://support.f5.com/csp/article/K23605346〔2023/4/19 確認〕
※ 51 JPCERT/CC：攻撃グループ BlackTech による F5 BIG-IP の脆弱性（CVE-2022-1388）を悪用した攻撃　https://blogs.jpcert.or.jp/ja/2022/09/bigip-exploit.html〔2023/4/19 確認〕
※ 52 NTT セキュリティ・ジャパン株式会社：BlackTech 標的型攻撃解析レポート　https://jp.security.ntt/resources/BlackTech_2021.pdf〔2023/4/19 確認〕
※ 53 JPCERT/CC：攻撃グループ Lazarus が使用するマルウェア YamaBot　https://blogs.jpcert.or.jp/ja/2022/06/yamabot.html〔2023/4/19 確認〕
株式会社マクニカ：ショートカットと ISO ファイルを悪用する攻撃キャンペーン　https://security.macnica.co.jp/blog/2022/05/iso.html〔2023/4/19 確認〕
※ 54 Fortinet, Inc.：Analysis of FG-IR-22-398 – FortiOS - heap-based buffer overflow in SSLVPNd　https://www.fortinet.com/blog/psirt-blogs/analysis-of-fg-ir-22-398-fortios-heap-based-buffer-overflow-in-sslvpnd〔2023/4/19 確認〕
※ 55 JPCERT/CC：JPCERT/CC 活動四半期レポート 2022 年 1 月 1 日 ～ 2022 年 3 月 31 日　https://www.jpcert.or.jp/pr/2022/PR_Report2021Q4.pdf〔2023/4/19 確認〕
JPCERT/CC：JPCERT/CC インシデント報告対応レポート 2022 年 10 月 1 日 ～ 2022 年 12 月 31 日　https://www.jpcert.or.jp/pr/2023/IR_Report2022Q3.pdf〔2023/4/19 確認〕
NISC：北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について（注意喚起）　https://www.nisc.go.jp/pdf/press/20221014NISC_press.pdf〔2023/4/19 確認〕
※ 56 NISC：サイバー攻撃を受けた組織における対応事例集（実事例における学びと気づきに関する調査研究）　https://www.nisc.go.jp/pdf/policy/inquiry/kokai_jireishu.pdf〔2023/4/19 確認〕
※ 57 株式会社ラック：日本組織を狙った新たな標的型攻撃（Operation MINAZUKI）https://www.lac.co.jp/lacwatch/report/20220630_003037.html〔2023/4/19 確認〕
※ 58 JPCERT/CC：攻撃グループ Lazarus が侵入したネットワーク内で使用するツール　https://blogs.jpcert.or.jp/ja/2021/01/Lazarus_tools.html〔2023/4/19 確認〕
トレンドマイクロ社：Python 製ペネトレーションテストツール「Impacket」、「Responder」の悪用手口を分析　https://www.trendmicro.com/ja_jp/research/22/i/analyzing-penetration-testing-tools-that-threat-actors-use-to-br.html〔2023/4/19 確認〕
Palo Alto Networks, Inc.：ペンテストツール Brute Ratel C4: 脅威アクターによるレッドチームツール悪用　https://unit42.paloaltonetworks.jp/brute-ratel-c4-tool/〔2023/4/19 確認〕
※ 59 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〔2023/4/19 確認〕
※ 60 経済産業省・独立行政法人情報処理推進機構：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〔2023/4/19 確認〕

※ 61 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〔2023/4/19 確認〕
JPCERT/CC：ログを活用した高度サイバー攻撃の早期発見と分析（プレゼンテーション資料） https://www.jpcert.or.jp/research/APT-loganalysis_Presen_20151117.pdf〔2023/4/19 確認〕
※ 62 被害金額については、2015 ～ 2022 年の年次報告書（IC3：Annual Reports https://www.ic3.gov/Home/AnnualReports〔2023/4/19 確認〕）を参照した。
※ 63 INTERPOL：Cyber-enabled financial crime: USD 130 million intercepted in global INTERPOL police operation https://www.interpol.int/en/News-and-Events/News/2022/Cyber-enabled-financial-crime-USD-130-million-intercepted-in-global-INTERPOL-police-operation〔2023/4/19 確認〕
※ 64 INTERPOL：Suspected head of cybercrime gang arrested in Nigeria https://www.interpol.int/News-and-Events/News/2022/Suspected-head-of-cybercrime-gang-arrested-in-Nigeria〔2023/4/19 確認〕
Group-IB：Operation Delilah: Group-IB helps INTERPOL nab suspected leader of transnational phishing ring https://www.group-ib.com/media-center/press-releases/interpol-gib-delilah/〔2023/4/19 確認〕
Palo Alto Networks, Inc.：オペレーションデリラ：Unit 42、国際刑事警察機構（INTERPOL）に協力しナイジェリア系ビジネスメール詐欺アクターを特定 https://unit42.paloaltonetworks.jp/operation-delilah-business-email-compromise-actor/〔2023/4/19 確認〕
※ 65 トレンドマイクロ社:ナイジェリアの BEC グループ逮捕でインターポール、ナイジェリア EFCC、トレンドマイクロが連携〔2023/4/19 確認〕 https://www.trendmicro.com/ja_jp/research/22/f/trend-micro-partners-with-interpol-and-nigeria-efcc-for-operation.html〔2023/4/19 確認〕
※ 66 ウィルソン・ラーニング ワールドワイド株式会社：当社子会社における資金流出事案の発生並びに特別損失の計上に関するお知らせ https://ssl4.eir-parts.net/doc/9610/tdnet/2203725/00.pdf〔2023/4/19 確認〕
※ 67 Bleeping Computer：US charges BEC suspects with targeting federal health care programs https://www.bleepingcomputer.com/news/security/us-charges-bec-suspects-with-targeting-federal-health-care-programs/〔2023/4/19 確認〕
※ 68 https://www.ipa.go.jp/security/bec/about.html〔2023/4/19 確認〕
※ 69 https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000098129.pdf〔2023/4/19 確認〕
※ 70 https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000100056.pdf〔2023/4/19 確認〕
※ 71 https://www.ipa.go.jp/security/bec/hjuojm0000003c8r-att/000102394.pdf〔2023/4/19 確認〕
※ 72 https://www.ipa.go.jp/security/bec/hjuojm0000003c8r-att/000103087.pdf〔2023/4/19 確認〕
※ 73 https://www.ipa.go.jp/security/bec/hjuojm0000003c8r-att/000104237.pdf〔2023/4/19 確認〕
※ 74 https://www.ipa.go.jp/security/bec/hjuojm0000003c8r-att/000106449.pdf〔2023/4/19 確認〕
※ 75 https://www.ipa.go.jp/security/bec/hjuojm0000003c8r-att/000107272.pdf〔2023/4/19 確認〕
※ 76 https://www.ipa.go.jp/publish/wp-security/sec-2020.html〔2023/4/19 確認〕
※ 77 IPA：ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報） https://www.ipa.go.jp/archive/files/000081866.pdf〔2023/4/19 確認〕
※ 78 IPA：ビジネスメール詐欺（BEC）対策特設ページ 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〔2023/4/19 確認〕
※ 79 Agari：Cosmic Lynx: A Russian Threat Hits the BEC Scene https://www.agari.com/email-security-blog/cosmic-lynx-russian-bec/〔2023/4/19 確認〕
※ 80 https://www.ipa.go.jp/security/bec/hjuojm00000037nn-att/000102392.pdf〔2023/4/19 確認〕
※ 81 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〔2023/4/19 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.net/security/report_02.html〔2023/4/19 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〔2023/4/19 確認〕
※ 82 Microsoft 社：侵害された電子メールアカウントへの対応 https://docs.microsoft.com/ja-jp/microsoft-365/security/office-365-security/responding-to-a-compromised-email-account?view=o365-worldwide〔2023/4/19 確認〕
Microsoft 社：Microsoft 365 アカウントが侵害されているかどうかを確認する方法 https://docs.microsoft.com/ja-jp/office365/troubleshoot/sign-in/determine-account-is-compromised〔2023/4/19 確認〕
Mandiant：Obscured by Clouds: Insights into Office 365 Attacks and How Mandiant Managed Defense Investigates https://www.mandiant.com/resources/blog/insights-into-office-365-attacks-and-how-managed-defense-investigates〔2023/4/19 確認〕
Google LLC：ハッキングまたは不正使用された Google アカウントを保護する https://support.google.com/accounts/answer/6294825?hl=ja〔2023/4/19 確認〕
※ 83 NSFOCUS：H1 2022 Global DDoS Attack Landscape Report https://nsfocusglobal.com/company-overview/resources/h1-2022-global-ddos-attack-landscape/〔2023/4/19 確認〕
※ 84 piyolog：2022 年 2 月に発生したウクライナへの DDoS 攻撃についてまとめてみた https://piyolog.hatenadiary.jp/entry/2022/02/16/233637〔2023/4/19 確認〕
Security NEXT：対ウクライナ DDoS 攻撃の余波を観測 - JPCERT/CC https://www.security-next.com/136085〔2023/4/19 確認〕
※ 85 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。
※ 86 Cloudflare, Inc.：2022 年第 4 四半期の Cloudflare DDoS 脅威レポート https://blog.cloudflare.com/ja-jp/ddos-threat-report-2022-q4-ja-jp/〔2023/4/19 確認〕
※ 87 Mitel Networks Corp.：Mitel Product Security Advisory 22-0001 MiCollab, MiVoice Business Express Access Control Vulnerability https://www.mitel.com/en-ca/support/security-advisories/mitel-product-security-advisory-22-0001〔2023/4/19 確認〕
※ 88 Akamai Technologies：Akamai Blog ¦ CVE-2022-26143: TP240PhoneHome Reflection/Amplification DDoS Attack Vector https://www.akamai.com/blog/security/phone-home-ddos-attack-vector〔2023/4/19 確認〕
TECH+：43 億倍という記録的な潜在増幅率持つ新しい DDoS ベクトルの悪用確認 https://news.mynavi.jp/techplus/article/20220311-2289948/〔2023/4/19 確認〕
※ 89 ハクティビスト集団：社会的・政治的な主張を目的としたハッキング活動を行う集団。
※ 90 piyolog：Killnet による国内サイトへの攻撃示唆についてまとめてみた https://piyolog.hatenadiary.jp/entry/2022/09/07/025039〔2023/4/19 確認〕
※ 91 Security NEXT：「e-Gov」の障害原因が明らかに - 攻撃元など非公表 https://www.security-next.com/139731〔2023/4/19 確認〕
※ 92 TechTarget ジャパン：親ロシア派ハッカー集団「Killnet」が派手に攻撃するのは“あれ”狙い? https://techtarget.itmedia.co.jp/tt/news/2210/21/news02.html〔2023/4/19 確認〕
SOMPO リスクマネジメント株式会社：ロシアよりのハッカー集団「Killnet（キルネット）」が日本のウェブサイトを攻撃 https://www.sompocybersecurity.com/column/column/a300〔2023/4/19 確認〕
サイカルジャーナル：「キルネット」とは何者か? https://www3.nhk.or.jp/news/special/sci_cul/2022/09/special/2022-09-cyber/〔2023/4/19 確認〕
※ 93 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。
※ 94 Mirai：IoT 機器に感染してボットネットを構成し、サイバー攻撃に悪用するウイルス。2016 年に史上最大規模の DDoS 攻撃を引き起こした。ソースコードが公開されていたため、様々な亜種が出現している。
※ 95 Mēris：IoT 機器に感染してボットネットを構成し、サイバー攻撃に悪用するウイルス。2021 年に Mirai の攻撃トラフィックの約 3 倍に相当する 1,720 万 rps（リクエスト／秒）という大規模な DDoS 攻撃が確認されている。
※ 96 Cloudflare, Inc.：Cloudflare が 1 秒あたり 2600 万件のリクエストを送信する DDoS 攻撃を軽減 https://blog.cloudflare.com/ja-jp/26m-rps-ddos-ja-jp/〔2023/4/19 確認〕
Cloudflare, Inc.：DNS および DDoS の脅威 https://www.cloudflare.com/static/a67661e4cd7bc35cf54bb1827e4630a6/Whitepaper_DNS-and-the-Threat-of-DDoS_Japanese_20230103.pdf〔2023/4/19 確認〕
Cloudflare, Inc.：Mantis - the most powerful botnet to date

https://blog.cloudflare.com/mantis-botnet/〔2023/4/19 確認〕
※ 97 Fortinet, Inc.：FortiOS - heap-based buffer overflow in sslvpnd https://www.fortiguard.com/psirt/FG-IR-22-398〔2023/4/19 確認〕
※ 98 Fortinet, Inc.：FortiOS / FortiProxy / FortiSwitchManager - Authentication bypass on administrative interface https://www.fortiguard.com/psirt/FG-IR-22-377〔2023/4/19 確認〕
※ 99 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。IoT 機器を狙うサイバー攻撃において、不正侵入やウイルス感染を試みる悪意のプログラムの一部として悪用されることがある。
※ 100 Horizon3 AI, Inc.:FortiOS, FortiProxy, and FortiSwitchManager Authentication Bypass Technical Deep Dive (CVE-2022-40684) https://www.horizon3.ai/fortios-fortiproxy-and-fortiswitchmanager-authentication-bypass-technical-deep-dive-cve-2022-40684/〔2023/4/19 確認〕
※ 101 Fortinet, Inc.：CVE-2022-40684 に関するアップデート https://www.fortinet.com/jp/blog/psirt-blogs/update-regarding-cve-2022-40684〔2023/4/19 確認〕
※ 102 Microsoft 社：Microsoft Windows Support Diagnostic Tool（MSDT）のリモートでコードが実行される脆弱性 https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2022-30190〔2023/4/19 確認〕
※ 103 piyolog：Microsoft サポート診断ツールの脆弱性（CVE-2022-30190）についてまとめてみた https://piyolog.hatenadiary.jp/entry/2022/06/02/010119〔2023/4/19 確認〕
※ 104 Threatpost：Microsoft Releases Workaround for 'One-Click' 0Day Under Active Attack https://threatpost.com/microsoft-workaround-0day-attack/179776/〔2023/4/19 確認〕
Proofpoint, Inc.：https://twitter.com/threatinsight/status/1531688214993555457〔2023/4/19 確認〕
※ 105 VMware, Inc.：CVE-2022-22963: Remote code execution in Spring Cloud Function by malicious Spring Expression https://tanzu.vmware.com/security/cve-2022-22963〔2023/4/19 確認〕
※ 106 VMware, Inc.：Impact of Spring4Shell CVE-2022-22965 and CVE-2022-22963 on VMware Blockchain (88203) https://kb.vmware.com/s/article/88203〔2023/4/19 確認〕
※ 107 VMware, Inc.：6. Spring Expression Language (SpEL) https://docs.spring.io/spring-framework/docs/3.0.x/reference/expressions.html〔2023/4/19 確認〕
※ 108 VMware, Inc.：CVE-2022-22965: Spring Framework RCE via Data Binding on JDK 9+ https://spring.io/security/cve-2022-22965〔2023/4/19 確認〕
※ 109 The Apache Software Foundation：Apache Log4j Security Vulnerabilities https://logging.apache.org/log4j/2.x/security.html〔2023/4/19 確認〕
※ 110 JVN：JVNVU#94675398 Spring Framework における不適切なデータバインディング処理による任意コード実行の脆弱性 https://jvn.jp/vu/JVNVU94675398/〔2023/4/19 確認〕
※ 111 デプロイ：配置する、展開するといった意味の英単語であり、ここではアプリケーション等を実行可能な状態にすることを指す。
※ 112 VMware, Inc.：How to hunt for Spring4Shell and Java Spring Vulnerabilities https://blogs.vmware.com/security/2022/04/how-to-hunt-for-spring4shell-and-java-spring-vulnerabilities.html〔2023/4/19 確認〕
※ 113 トレンドマイクロ社：Spring4Shell（CVE-2022-22965）を悪用したコインマイナーの攻撃を観測 https://www.trendmicro.com/ja_jp/research/22/e/spring4shell-exploited-to-deploy-cryptocurrency-miners0.html〔2023/4/19 確認〕
※ 114 トレンドマイクロ社：Spring4Shell（CVE-2022-22965）を悪用したボットネット「Mirai」の攻撃を観測 https://www.trendmicro.com/ja_jp/research/22/d/Mirai-exploits-Spring4Shell.html〔2023/4/19 確認〕
※ 115 株式会社東陽テクニカ：【重要】Spring Framework 脆弱性（CVE-2022-22965）の影響について https://www.toyo.co.jp/onetech_blog/articles/detail/id=36106〔2023/4/19 確認〕
※ 116 ソフトウェア部品表（SBOM：Software Bill Of Materials）：ソフトウェアに含まれるコンポーネントをデータベース化し、一覧で管理する手法の一つ。
PwC：SBOM 普及の本格化～ソフトウェアサプライチェーンの構造的な課題と解決策～ https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/vulnerability-management-sbom1.html〔2023/4/19 確認〕
※ 117 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2015 年 10 月～ 12 月］ https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000050428.pdf〔2023/4/19 確認〕
※ 118 Cynet：Orion Threat Alert:Qakbot TTPs Arsenal and the Black Basta Ransomware https://www.cynet.com/blog/orion-threat-alert-qakbot-ttps-arsenal-and-the-black-basta-ransomware/〔2023/4/19 確認〕
※ 119 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2018 年 10 月 ～ 12 月 ］ https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000071273.pdf〔2023/4/19 確認〕
※ 120 JPCERT/CC：マルウェア Emotet の感染再拡大に関する注意喚起 https://www.jpcert.or.jp/at/2022/at220006.html〔2023/4/19 確認〕
※ 121 IPA：Excel ファイル内に書かれている偽の指示の変更について（2022 年 11 月 4 日） https://www.ipa.go.jp/security/emotet/situation/emotet-situation-13.html〔2023/6/30 確認〕
※ 122 ショートカットファイルを悪用した攻撃（2022 年 4 月 26 日） https://www.ipa.go.jp/security/emotet/situation/emotet-situation-11.html〔2023/6/30 確認〕
※ 123 株式会社マクニカ：2023 年 3 月に活動を再開した「Emotet」マルウェアの検知について https://www.macnica.co.jp/public-relations/news/2023/143204/〔2023/4/19 確認〕
※ 124 IPA：Emotet の攻撃活動再開について（2023 年 3 月 9 日） https://www.ipa.go.jp/security/emotet/situation/emotet-situation-14.html〔2023/6/30 確認〕
※ 125 IPA：Microsoft OneNote 形式のファイルを悪用した攻撃（2023 年 3 月 17 日） https://www.ipa.go.jp/security/emotet/situation/emotet-situation-15.html〔2023/6/30 確認〕
※ 126 Microsoft 社：Helping users stay safe: Blocking internet macros by default in Office https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805〔2023/4/19 確認〕
※ 127 日本プルーフポイント株式会社：攻撃者はマクロ無効化にどう適用するのか? https://www.proofpoint.com/jp/blog/threat-insight/how-threat-actors-are-adapting-post-macro-world〔2023/4/19 確認〕
※ 128 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/ja-JP/vulnerability/CVE-2022-41091〔2023/4/19 確認〕
※ 129 Fortinet, Inc.：Delivery of Malware: A Look at Phishing Campaigns in Q3 2022 https://www.fortinet.com/blog/threat-research/delivery-of-malware-phishing-campaigns-in-q3-2022〔2023/4/19 確認〕
※ 130 JPCERT/CC：インターネットセキュリティの歴史 第 25 回「VISA やイーバンク銀行を騙る日本語フィッシングメール」 https://www.jpcert.or.jp/tips/2009/wr090301.html〔2023/4/19 確認〕
※ 131 フィッシング対策協議会：2022/12 フィッシング報告状況 https://www.antiphishing.jp/report/monthly/202212.html〔2023/4/19 確認〕
※ 132 総務省：令和3年通信利用動向調査の結果 https://www.soumu.go.jp/johotsusintokei/statistics/data/220527_1.pdf〔2023/4/19 確認〕
※ 133 IPA：国税庁をかたる偽ショートメッセージサービス（SMS）や偽メールに注意 https://www.ipa.go.jp/security/anshin/attention/2022/mgdayori20221031.html 〔2023/4/19 確認〕
※ 134 ライフカード株式会社：【お客様への注意喚起】国税庁を騙る未払い請求の案内について https://vpc.lifecard.co.jp/news/20220816.html〔2023/4/19 確認〕
※ 135 https://www.ipa.go.jp/publish/wp-security/sec-2021.html〔2023/4/19 確認〕
※ 136 Apple Inc.：ギフトカード詐欺について https://support.apple.com/ja-jp/gift-card-scams〔2023/4/19 確認〕
※ 137 株式会社 NTT ドコモ：SMS 拒否設定 https://www.docomo.ne.jp/info/spam_mail/sms/〔2023/4/19 確認〕
※ 138 ソフトバンク株式会社：迷惑 SMS 対策機能（無料）を提供開始 https://www.softbank.jp/mobile/info/personal/news/service/20220602a/〔2023/4/19 確認〕
※ 139 KDDI 株式会社：迷惑 SMS ブロック https://www.au.com/mobile/service/sms/filter/〔2023/4/19 確認〕
※ 140 国税庁：不審なショートメッセージやメールにご注意ください https://www.nta.go.jp/data/040721_03jouhou.pdf〔2023/4/19 確認〕
※ 141 株式会社ローソン：「ローソン 83 周年記念ギフト」となりすました偽装 LINE にご注意ください https://www.lawson.co.jp/info/20221206_snsinfo.html〔2023/4/19 確認〕
株式会社ユニクロ：「ユニクロ 38 周年記念買物手当」とユニクロになりすました偽 LINE メッセージにご注意ください https://faq.uniqlo.com/articles/FAQ/100008430/〔2023/4/19 確認〕
※ 142 https://www.antiphishing.jp/news/alert/etcQR_20221115.html〔2023/4/19 確認〕

※ 143 https://www.antiphishing.jp/news/alert/amazonQR_20230105.html〔2023/4/19 確認〕
※ 144 フィッシング対策協議会：日本赤十字社をかたるフィッシング（2022/09/20） https://www.antiphishing.jp/news/alert/jrc_20220920.html〔2023/4/19 確認〕
※ 145 フィッシング対策協議会：厚生労働省（コロナワクチンナビ）をかたるフィッシング（2022/04/13） https://www.antiphishing.jp/news/alert/mhlw_20220413.html〔2023/4/19 確認〕
※ 146 https://www.ipa.go.jp/publish/wp-security/sec-2022.html〔2023/4/19 確認〕
※ 147 独立行政法人国民生活センター：その通販サイト本物ですか!? “偽サイト”に警戒を!!ー最近の“偽サイト”の見分け方を知って、危険を回避しましょう!ー https://www.kokusen.go.jp/news/data/n-20230130_1.html〔2023/4/19 確認〕
※ 148 IPA：安心相談窓口だより 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〔2023/4/19 確認〕
※ 149 FBI：Internet Crime Report 2022 https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf〔2023/4/19 確認〕
※ 150 Avast：Avast Q3/2022 Threat Report - Technical support scams https://decoded.avast.io/threatresearch/avast-q3-2022-threat-report/〔2023/4/19 確認〕
※ 151 一般社団法人日本フランチャイズチェーン協会：SS 広場 https://ss.jfa-fc.or.jp/〔2023/4/19 確認〕
※ 152 一般社団法人日本フランチャイズチェーン協会：コンビニエンスストアセーフティステーション活動アンケートリポート 2021 年度版 https://ss.jfa-fc.or.jp/folder/top/img/n_20220517112157yb2tsksvrmwk35gq.pdf〔2023/4/19 確認〕
※ 153 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。
※ 154 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〔2023/4/19 確認〕
※ 155 IPA：安心相談窓口だより ブラウザの通知機能から不審サイトに誘導する手口に注意 https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210309.html〔2023/4/19 確認〕
※ 156 reCAPTCHAv2：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。
※ 157 独立行政法人国民生活センター：簡単に高額収入を得られるという副業や投資の儲け話に注意!ーインターネット等で取引される情報商材のトラブルが急増ー https://www.kokusen.go.jp/news/data/n-20180802_1.html〔2023/4/19 確認〕
消費者庁：「スマホで簡単 月収 100 万円」、「定型文を送信した分だけ報酬発生」などとうたう副業のマニュアルを購入させ、ライブ配信希望者のエージェントになるためとして高額なサポートプランを契約させる事業者に関する注意喚起 https://www.caa.go.jp/notice/assets/consumer_policy_cms103_221117_0001.pdf〔2023/4/19 確認〕
※ 158 東京都消費生活総合センター -『遠隔操作アプリ』を悪用して借金をさせる手口が増えています！ https://www.shouhiseikatu.metro.tokyo.lg.jp/sodan/kinkyu/20230303.html〔2023/4/19 確認〕
※ 159 JC3：偽ショッピングサイトに注意 https://www.jc3.or.jp/threats/topics/article-462.html〔2023/4/19 確認〕
※ 160 トレンドマイクロ社：SEO ポイズニングによる偽ショッピングサイトへの誘導を行う PHP マルウェアの解析 https://www.trendmicro.com/ja_jp/research/22/j/seo-poisoning.html〔2023/4/19 確認〕
※ 161 STOP. THINK. CONNECT.：米国 APWG と NCSA が共同で開始したインターネットを安全に使うための消費者向けセキュリティ普及啓発キャンペーン。日本では、安全なインターネット社会に貢献したいメンバーが業界を問わず広く参画して活動が行われている。
STOP. THINK. CONNECT.：https://stopthinkconnect.jp/〔2023/4/19 確認〕
※ 162-1 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 ～ http://www.tsr-net.co.jp/data/detail/1197322_1527.html〔2023/4/25 確認〕
※ 162-2 事故件数は「事故を公表した企業による発表件数」を集計したもので、「1.2.9（3）過失による情報漏えい」に掲載した JIPDEC が集計した届け出義務を負うプライバシーマーク取得企業の事故報告件数とは、集計方法が異なる。
※ 163 日本経済新聞：ニトリ、13 万件の個人情報流出か 不正アクセス被害で https://www.nikkei.com/article/DGXZQOUC2175K0R20C22A9000000/〔2023/4/19 確認〕
※ 164 株式会社ショーケース：不正アクセスに関するお知らせとお詫び https://www.showcase-tv.com/pressrelease/202210-fa-info/〔2023/4/19 確認〕
通販新聞社：ショーケース 入力支援サービスに不具合、カード情報流出、ユーキャンなど被害 https://www.tsuhanshimbun.com/products/article_detail.php?product_id=6502〔2023/4/19 確認〕
※ 165 株式会社ユーキャン：弊社が運営する「生涯学習のユーキャン」サイトにおける個人情報漏洩に関するお詫びとお知らせ https://www.u-can.co.jp/info/release.html〔2023/4/19 確認〕
※ 166 株式会社エービーシーマート：弊社が運営する「ABC-MART 公式オンラインストア」における個人情報漏えいの可能性に関するお詫びとお知らせ https://www.abc-mart.net/shop/pages/info-2022.aspx〔2023/4/19 確認〕
※ 167 株式会社カクヤス：【重要】クレジットカード情報漏洩に関するお詫びとお知らせについて https://www.kakuyasu.co.jp/corporate/topics/20221101.pdf〔2023/4/19 確認〕
※ 168 NHK NEWS WEB：ツイッター 利用者約 2 億 3000 万人分の個人情報 流出か https://www3.nhk.or.jp/news/html/20230106/k10013943361000.html〔2023/1/24 確認〕
※ 169 Bleeping Computer：Twitter confirms zero-day used to expose data of 5.4 million accounts https://www.bleepingcomputer.com/news/security/twitter-confirms-zero-day-used-to-expose-data-of-54-million-accounts/〔2023/4/19 確認〕
※ 170 Bleeping Computer：Hacker claims to be selling Twitter data of 400 million users https://www.bleepingcomputer.com/news/security/hacker-claims-to-be-selling-twitter-data-of-400-million-users/〔2023/4/19 確認〕
※ 171 Bleeping Computer：200 million Twitter users' email addresses allegedly leaked online https://www.bleepingcomputer.com/news/security/200-million-twitter-users-email-addresses-allegedly-leaked-online/〔2023/4/19 確認〕
※ 172 「情報セキュリティ白書 2022」（https://www.ipa.go.jp/publish/wp-security/sec-2022.html〔2023/4/19 確認〕）の「2.8.1 個人情報保護法改正」（p.150）を参照。
※ 173 朝日新聞デジタル：JTB、事業者の 1 万人超の個人情報を流出 観光庁の事業で https://www.asahi.com/articles/ASQBT6DG8QBTULFA01C.html〔2023/4/19 確認〕
※ 174 毎日新聞：アフラック生命とチューリッヒ保険で情報漏えい 同じ米企業に委託 https://mainichi.jp/articles/20230110/k00/00m/040/240000c〔2023/4/19 確認〕
※ 175 朝日新聞デジタル：200 万人以上の個人情報が流出 アフラック生命とチューリッヒ保険 https://www.asahi.com/articles/ASR1B6V3KR1BULFA01Q.html〔2023/4/19 確認〕
※ 176 https://privacymark.jp/news/other/2022/1007.html〔2023/4/19 確認〕
※ 177 NHK NEWS WEB：尼崎市 紛失の USB メモリー見つかる 全市民 46 万人余の個人情報 https://www3.nhk.or.jp/news/html/20220624/k10013686601000.html〔2023/4/19 確認〕
※ 178 朝日新聞デジタル：尼崎の紛失 USB、スマホ位置情報で発見 パスワード変更の形跡なし https://www.asahi.com/articles/ASQ6S6JJBQ6SPTIL03F.html〔2023/4/19 確認〕
※ 179 NHK NEWS WEB：USB メモリー紛失受け“情報セキュリティー対策徹底を”総務相 https://www3.nhk.or.jp/news/html/20220628/k10013692041000.html〔2023/4/19 確認〕
※ 180 BIPROGY 株式会社：USB メモリー紛失事案に関する第三者委員会の設置について https://www.biprogy.com/pdf/news/nr_220701.pdf〔2023/4/19 確認〕
※ 181 尼崎市：個人情報を含む USB メモリーの紛失事案について https://www.city.amagasaki.hyogo.jp/kurashi/seikatusien/1027475/1030947.html〔2023/4/19 確認〕
※ 182 尼崎市 USB メモリー紛失事案調査委員会：尼崎市 USB メモリー紛失事案に関する調査報告書 https://www.city.amagasaki.hyogo.jp/_res/projects/default_project/_page_/001/030/947/houkokusyo.pdf〔2023/4/19 確認〕
※ 183 杏林大学医学部付属病院：個人情報を含む USB メモリーの紛失について https://www.kyorin-u.ac.jp/hospital/introduction/info/news_detail/5999/〔2023/4/19 確認〕
ITmedia NEWS：また USB 紛失 患者の個人情報入り、杏林大病院 院外持ち出し禁止のはずが https://www.itmedia.co.jp/news/articles/2207/01/news116.html〔2023/4/19 確認〕
※ 184 株式会社 MORESCO：元従業員の逮捕について https://www.moresco.co.jp/news/20220915_3368.php〔2023/1/23 確認〕
※ 185 日本経済新聞：狙われる「営業秘密」「かっぱ寿司」起訴 https://www.nikkei.com/article/DGKKZO65364290R21C22A0

CM0000/〔2023/4/19 確認〕
※ 186 https://www.ipa.go.jp/security/guide/insider.html〔2023/4/19 確認〕
※ 187 日本経済新聞：イトーヨーカ堂、個人情報 1056 人分紛失　氏名や電話番号　https://www.nikkei.com/article/DGXZQOUC214840R20C22A9000000/〔2023/4/19 確認〕
※ 188 IPA：JVN iPedia 脆弱性対策情報データベース　https://jvndb.jvn.jp/〔2023/4/19 確認〕
※ 189 JPCERT/CC、IPA：Japan Vulnerability Notes（JVN）　https://jvn.jp/〔2023/4/19 確認〕
※ 190 NIST：National Vulnerability Database（NVD）　https://nvd.nist.gov/〔2023/4/19 確認〕
※ 191 公表年は、ベンダーがアドバイザリを公開した年、他組織や情報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。
※ 192 IPA：共通脆弱性識別子 CVE 概説　https://www.ipa.go.jp/security/vuln/scap/cve.html〔2023/4/19 確認〕
※ 193 MITRE 社：CVE Numbering Authorities（CNA）　https://www.cve.org/ProgramOrganization/CNAs〔2023/4/25 確認〕
※ 194 MITRE 社：正式名称は 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。
※ 195 MITRE 社：CVE Adds 7 New CVE Numbering Authorities (CNAs)　https://cve.mitre.org/news/archives/2016/news.html〔2023/4/19 確認〕
※ 196 MITRE 社：Tribe29 Added as CVE Numbering Authority (CNA)　https://www.cve.org/Media/News/item/news/2022/12/28/Tribe29-Added-as-CVE-Numbering〔2023/4/19 確認〕
※ 197 2021 年 12 月 21 日時点の CAN の数は 209 組織であった。
MITRE 社：VulDB Added as CVE Numbering Authority (CNA)
https://www.cve.org/Media/News/Item/news/2021/12/21/VulDB-Added-as-CVE-Numbering〔2023/4/19 確認〕
※ 198 IPA：共通脆弱性タイプ一覧 CWE 概説　https://www.ipa.go.jp/security/vuln/scap/cwe.html〔2023/4/19 確認〕
※ 199 IPA：共通脆弱性評価システム CVSS 概説　https://www.ipa.go.jp/security/vuln/scap/cvss.html〔2023/4/19 確認〕
※ 200 図 1-3-4 の数値が図 1-3-1 や図 1-3-3 と異なっているのは、CWE や CVSS v2 の登録がない脆弱性もあるためである。
※ 201 JPCERT/CC：セキュアコーディング　https://www.jpcert.or.jp/securecoding/〔2023/4/19 確認〕
※ 202 Microsoft 社 :Internet Explorer は Microsoft Edge へ - Windows 10 の Internet Explorer 11 デスクトップアプリは 2022 年 6 月 15 日にサポート終了　https://blogs.windows.com/japan/2021/05/19/the-future-of-internet-explorer-on-windows-10-is-in-microsoft-edge/〔2023/4/19 確認〕
※ 203 窓の杜：Google が IE のゼロデイ脆弱性を突いて韓国のユーザーを狙った北朝鮮発の攻撃を解説　https://forest.watch.impress.co.jp/docs/news/1462309.html〔2023/4/19 確認〕
※ 204 IPA：Microsoft Exchange Server における権限管理に関する脆弱性　https://jvndb.jvn.jp/ja/contents/2022/JVNDB-2022-002439.html〔2023/4/19 確認〕
※ 205-1 IPA：Microsoft Exchange Server における脆弱性　https://jvndb.jvn.jp/ja/contents/2022/JVNDB-2022-002438.html〔2023/4/19 確認〕
※ 205-2 マイクロソフト社が CVSSv3 の評価のみを公開しているため、CVSSv3 で記述している。なお、CVSSv3 の深刻度は、「緊急」（基本値 9.0 ～ 10.0）、「重要」（基本値 7.0 ～ 8.9）、「警告」（基本値 4.0 ～ 6.9）、「注意」（基本値 0.1 ～ 3.9）、「なし」（基本値 0）である。
※ 206 IPA：Microsoft Exchange Server における権限を昇格される脆弱性　https://jvndb.jvn.jp/ja/contents/2022/JVNDB-2022-002733.html〔2023/4/19 確認〕
※ 207 Security NEXT：新手の攻撃手法「OWASSRF」-「ProxyNotShell」軽減策をバイパス　https://www.security-next.com/142582〔2023/4/19 確認〕
※ 208 Security NEXT：給食委託先経由で侵入された可能性 - 大阪急性期・総合医療センター　https://www.security-next.com/141214〔2023/4/19 確認〕
※ 209 一般社団法人医療 ISAC：四病院団体協議会の加盟病院を対象としたセキュリティアンケートの調査結果を公開　https://m-isac.jp/2022/04/02/report01-3/〔2023/4/19 確認〕
※ 210 つるぎ町立半田病院コンピュータウイルス感染事案有識者会議：徳島県つるぎ町立半田病院 コンピュータウイルス感染事案 有識者会議調査報告書　https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf〔2023/4/19 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 ソースネクスト株式会社：当サイトへの不正アクセスによる個人情報漏えいに関するお詫びとお知らせ　https://www.sourcenext.com/support/i/2023/0214_info/?i=gtnews〔2023/4/19 確認〕
※ 213 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〔2023/4/19 確認〕
※ 214 IPA：脆弱性関連情報の届出受付　https://www.ipa.go.jp/security/todokede/vuln/uketsuke.html〔2023/4/19 確認〕
※ 215 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。
※ 216 「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 サイト構築関連のソフトウェアを指す。これは、IPA の「四半期ごとの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〔2023/4/19 確認〕）で使用している「ソフトウェア製品の製品種類」の一つである。
※ 217 JVN：JVN#96561229 FUJITSU Network IPCOM の運用管理インタフェースにおける複数の脆弱性　https://jvn.jp/jp/JVN96561229/index.html〔2023/4/19 確認〕
※ 218 MITRE 社:Overview　https://www.cve.org/About/Overview〔2023/4/19 確認〕
※ 219 JPCERT/CC：CNA (CVE Numbering Authority)　https://www.jpcert.or.jp/vh/cna.html〔2023/4/19 確認〕
MITRE 社:Partner　https://www.cve.org/PartnerInformation/Partner〔2023/4/19 確認〕
※ 220 MITRE 社：Becoming a CVE Numbering Authority (CNA)
https://cve.mitre.org/cve/cna/Becoming_a_CNA_ja.pptx〔2023/4/19 確認〕
※ 221 JPCERT/CC：JPCERT/CC 活動四半期レポート 2022 年 10 月 1 日 ～ 2022 年 12 月 31 日　https://www.jpcert.or.jp/pr/2023/PR_Report2022Q3.pdf〔2023/4/19 確認〕
※ 222 MITRE 社：CVE Numbering Authorities (CNAs)　https://www.cve.org/ProgramOrganization/CNAs〔2023/3/31 確認〕
※ 223 IPA：情報セキュリティ早期警戒パートナーシップガイドライン
https://www.ipa.go.jp/security/todokede/vuln/ug65p90000019gda-att/000098799.pdf〔2023/4/19 確認〕
※ 224 https://www.ipa.go.jp/security/todokede/vuln/ug65p90000019gda-att/000089537.pdf〔2023/4/19 確認〕
※ 225 https://www.ipa.go.jp/security/todokede/vuln/ug65p90000019gda-att/000058492.pdf〔2023/4/19 確認〕
※ 226 https://www.ipa.go.jp/security/todokede/vuln/ug65p90000019gda-att/000058493.pdf〔2023/4/19 確認〕

付録

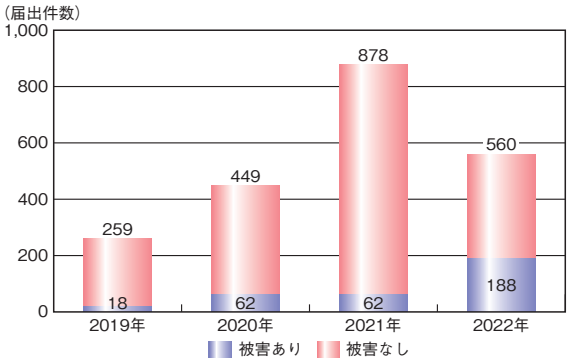
資料

資料A　2022年のコンピュータウイルス届出状況

IPA が 2022 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

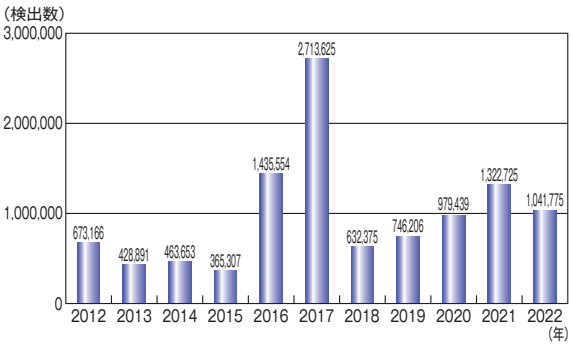
2022 年の年間届出件数は、前年の 878 件より 318 件（36.2%）少ない 560 件であった（図 A-1）。そのうち、ウイルス感染の実被害があった届出は 188 件であった。



■図 A-1　ウイルス届出件数推移（2019～2022 年）

A.2　届出のあったウイルス等検出数

2022 年に寄せられたウイルス等の検出数は、前年の 132 万 2,725 個より 28 万 950 個（21.2%）少ない 104 万 1,775 個であった（図 A-2）。



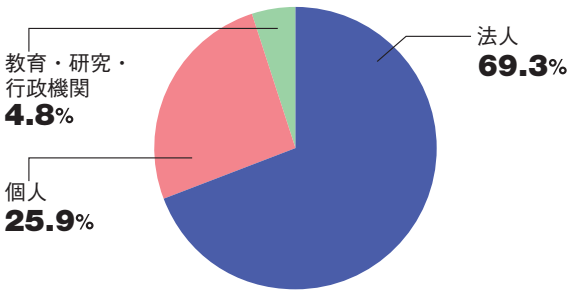
■図 A-2　ウイルス等検出数推移（2012～2022 年）

A.3　届出者の主体別届出件数

2022 年は前年と比較すると、全体の届出件数は減少した一方で、「法人」からの届出は増加した。届出者の主体別の比率では「法人」からの届出が 69.3%（388 件）と最も多かった（表 A-1、図 A-3）。

届出者の主体	2020 年	2021 年	2022 年
法人	232	284	388
個人	188	578	145
教育・研究・行政機関	29	16	27
合計（件）	449	878	560

■表 A-1　ウイルス届出者の主体別届出件数（2020～2022 年）



■図 A-3　ウイルス届出者の主体別届出件数の比率（2022 年）

A.4　傾向

2022 年でウイルス感染の実被害に遭った届出 188 件のうち、145 件が Emotet に感染した被害であり、半数以上を占めた。特に 3 月においては 42 件の被害の届出があり、これは IPA が 2 月に「Emotet の攻撃活動の急増」として、注意喚起を行った時期と一致する。これらの届出件数の詳細は、下記の資料を参照いただきたい。また、本白書では「1.2.6 ばらまき型メールによる攻撃」にて、メールを介してウイルスを感染させる攻撃手口や対策について詳しく述べているので、ぜひこちらも一読いただきたい。

参照

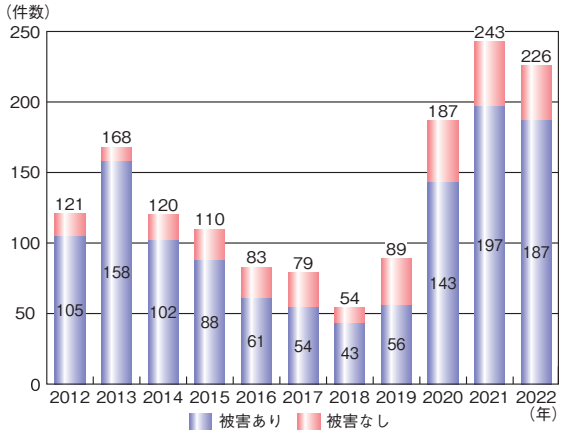
■コンピュータウイルス・不正アクセスの届出状況［2022年（1月～12月）］
https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000108005.pdf

資料B　2022年のコンピュータ不正アクセス届出状況

IPA が 2022 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

2022 年の年間届出件数は、前年の 243 件より 17 件（7.0%）少ない 226 件であった（図 B-1）。そのうち、実被害があった届出は 187 件であった。



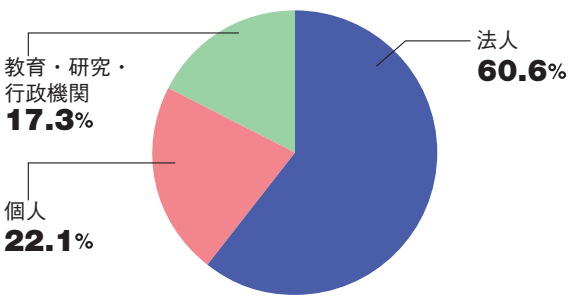
■図 B-1　不正アクセス届出件数推移（2012 年～2022 年）

B.2　届出者の主体別届出件数

2022 年は前年と比較すると、「法人」からの届出件数が減少しているが、届出者の主体別の比率では「法人」からの届出が 60.6%（137 件）と最も多かった（表 B-1、図 B-2）。

届出者の主体	2020 年	2021 年	2022 年
法人	114	156	137
個人	57	46	50
教育・研究・行政機関	16	41	39
合計（件）	187	243	226

■表 B-1　不正アクセス届出者の主体別届出件数（2020～2022 年）

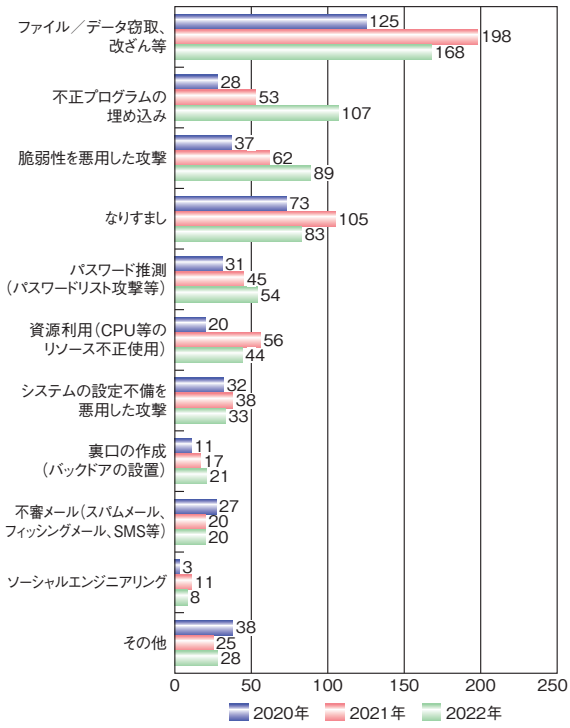


■図 B-2　不正アクセス届出者の主体別届出件数の比率（2022 年）

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。

2022 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「不正プログラムの埋め込み」が 107 件、「脆弱性を悪用した攻撃」が 89 件であった。



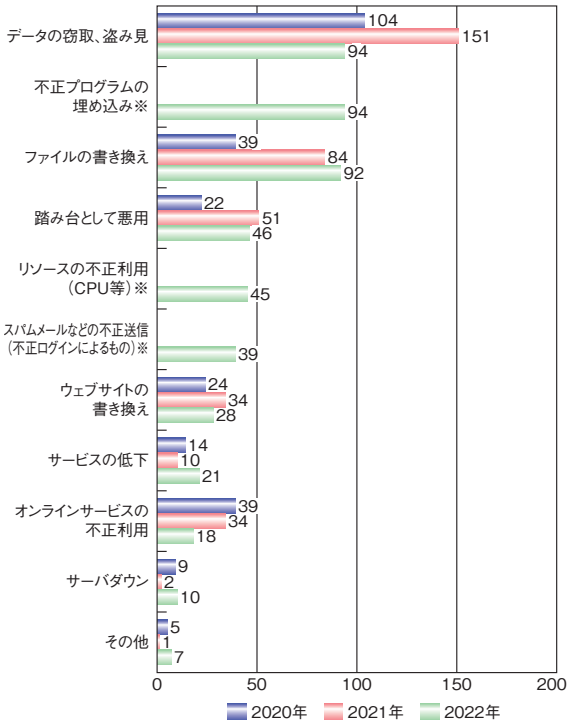
■図 B-3　不正アクセス手口別件数の推移（2020～2022 年）

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。2022 年の届出において最も多く見られた被害は、「データの窃取、盗み見」と「不正プログラムの埋め込み」の 94 件であった。次いで「ファイルの書き換え」が 92 件、「踏み台として悪用」が 46 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.

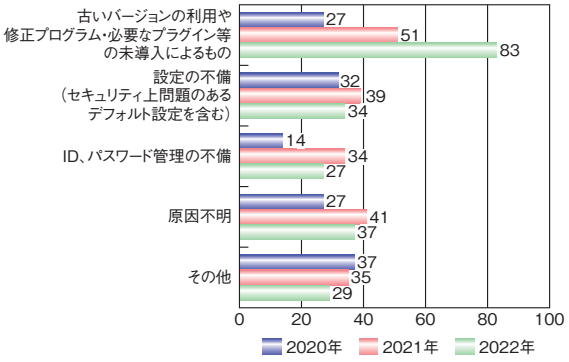
html）において「コンピュータウイルス・不正アクセスの届出事例［2022 年上半期（1 月～ 6 月）］」及び「コンピュータウイルス・不正アクセスの届出事例［2022 年下半期（7 月～ 12 月）］」を紹介している。そちらも、ぜひ参考にしていただきたい。



■図 B-4　不正アクセス被害内容別件数の推移（2020～2022 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。2022 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 83 件であった。次いで「設定不備（セキュリティ上問題のあるデフォルト設定を含む）」が 34 件、「ID、パスワード管理の不備」が 27 件であった。



■図 B-5　不正アクセス原因別件数の推移（2020～2022 年）

B.6 傾向と対策

不正アクセス被害の傾向と対策について述べる。

(1) 企業・組織の被害の傾向と対策

2022 年は Web サイト（EC サイトを含む）の脆弱性や設定不備を悪用した不正アクセスに関する被害が多く見られた。また、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不正侵入に関する被害も依然として多く確認されている（「1.2.5 (1) VPN 製品の脆弱性を対象とした攻撃」「1.2.1 ランサムウェア攻撃」参照）。

対策としては、Web サイトや VPN 装置等に限らず、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と修正プログラムの適用、設定の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。更に、Web アプリケーションの脆弱性診断の実施等も含めて、着実に脆弱性や設定不備を解消していく必要がある。

(2) システム利用者の被害の傾向と対策

2022 年も引き続き、パスワードリスト攻撃や総当たり攻撃により、認証が突破されたことで、メールアカウント等が不正利用されたとする被害が依然として見られた。

システム利用者においては、他者に推測されにくい複雑なパスワードを設定する、パスワードの使いまわしをしないといった基本的な対策を実施することに加えて、多要素認証等のセキュリティオプションを積極的に採用する等、自身が所有するアカウントが適切に管理できているか今一度見直していただきたい。

参照

■コンピュータウイルス・不正アクセスの届出状況［2022年（1月～12月）］
https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000108005.pdf

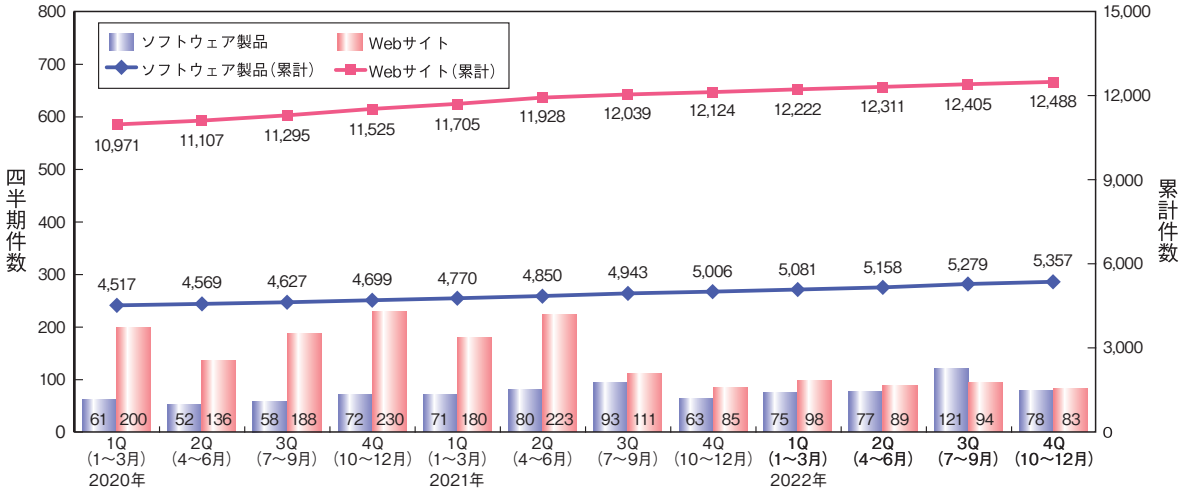
資料C　ソフトウェア等の脆弱性関連情報に関する届出状況

IPA が受け付けた脆弱性関連情報に関する届出は、2022 年末までに 1 万 7,845 件に達した。

C.1　脆弱性の届出概況

2022 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 5,357 件、Web サイトに関するもの 1 万 2,488 件、合計 1 万 7,845 件で、Web サイトに関する届出が全体の 70.0% 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、2022 年第 4 四半期末時点で 3.97 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

2020年1Q（1~3月）	2020年2Q（4~6月）	2020年3Q（7~9月）	2020年4Q（10~12月）	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）
4.04	4.03	4.03	4.04	4.04	4.06	4.05	4.02	4.01	3.99	3.98	3.97

■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）

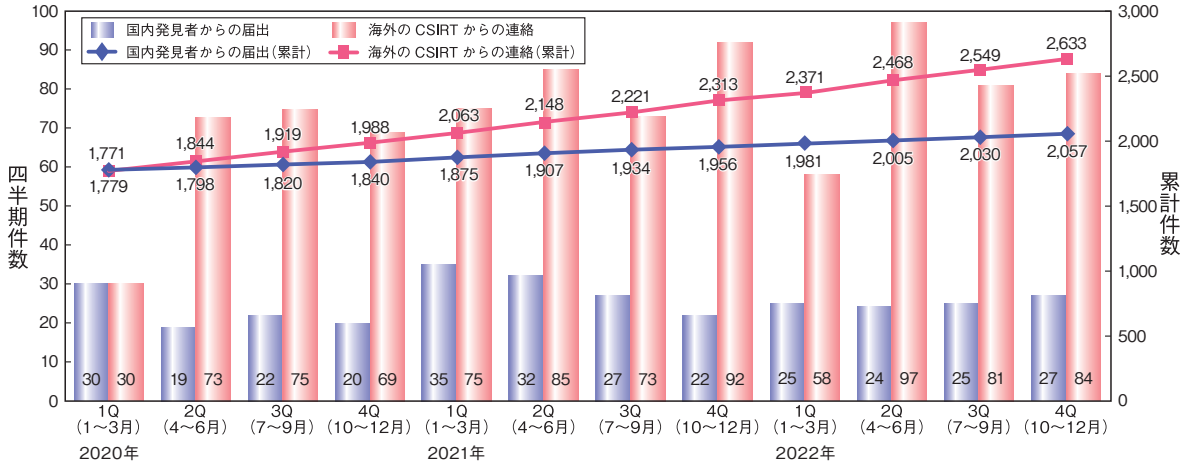
C.2　ソフトウェア製品の脆弱性の処理の終了状況

2022 年末時点のソフトウェア製品に関する脆弱性の処理状況は、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ものは 2,488 件、JVN で公表せず製品開発者が個別対応を行ったものは 40 件、製品開発者が脆弱性ではないと判断したものは 108 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 521 件で、処理の終了件数の合計は 3,157 件に達した（表 C-2）。

このほか、海外の CSIRT から JPCERT/CC が連絡を受けた 2,633 件を JVN で公表した。これらの脆弱性対策情報の公表件数の期別推移を図 C-2 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、表 C-2 の「公表済み」の件数と図 C-2 の公表件数は異なっている。

分類		累計件数
修正完了	公表済み	2,488件
	個別対応	40件
脆弱性ではない		108件
不受理		521件
合計		3,157件

■表 C-2　ソフトウェア製品の脆弱性の処理終了件数



■図 C-2　ソフトウェア製品の脆弱性対策情報の公表件数

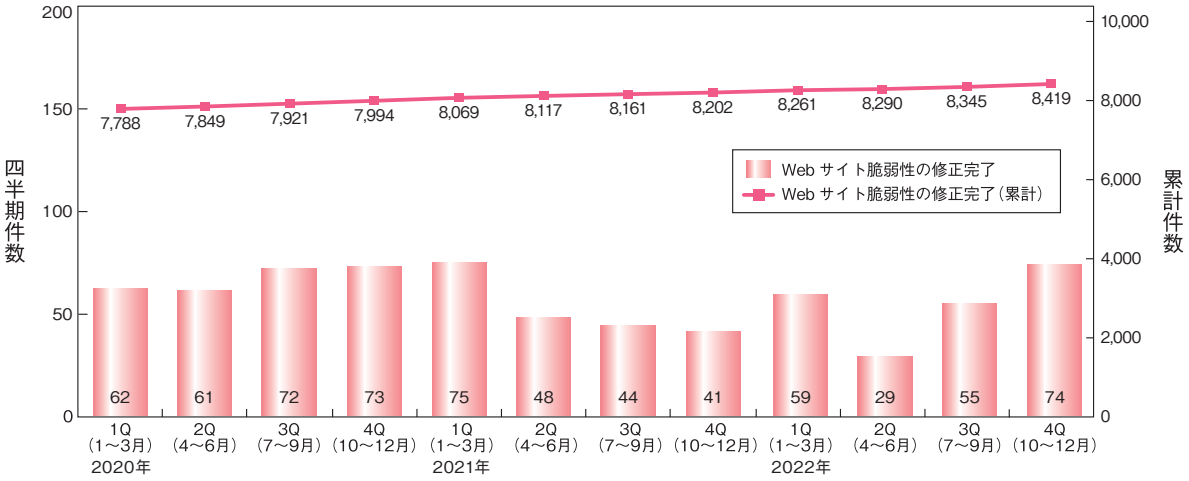
C.3 Webサイトの脆弱性の処理の終了状況

2022 年末時点の Web サイトに関する脆弱性の処理状況は、IPA が通知を行い Web サイト運営者が修正を完了したものは 8,419 件、IPA が注意喚起等を行った後に処理を終了したものは 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 732 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り扱いが不能なものが 232 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 286 件で、処理の終了件数の合計は 1 万 799 件に達した（表 C-3）。

これらのうち、修正完了件数の期別推移を図 C-3 に示す。

分類	累計件数
修正完了	8,419件
注意喚起	1,130件
脆弱性ではない	732件
取扱不能	232件
不受理	286件
合計	10,799件

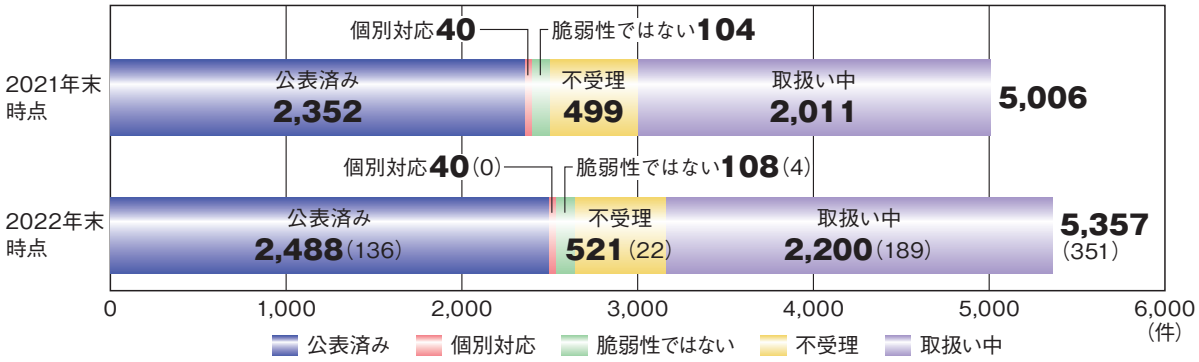
■表 C-3　Web サイトの脆弱性の終了件数



■図 C-3　Web サイトの脆弱性の修正完了件数

C.4 ソフトウェア製品の脆弱性の届出の処理状況

ソフトウェア製品の脆弱性関連情報の届出について処理状況を図 C-4 に示す。2022 年に JVN で「公表済み」となったソフトウェア製品の件数は 136 件で累計 2,488 件となった。また、「取扱い中」の届出は 189 件増加し、2,200 件となった。「処理終了」した届出は、162 件増加し、累計 3,157 件となった。

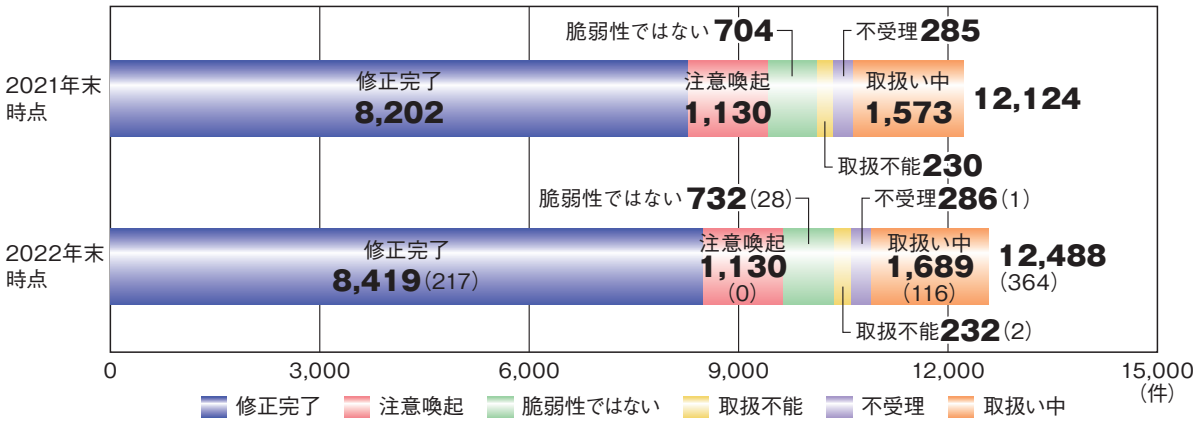


※( )内の数値は 2021 年末時点と 2022 年末時点の差分

■図 C-4　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

C.5 Webサイトの脆弱性の届出の処理状況

Web サイトの脆弱性関連情報の届出について処理状況を図 C-5 に示す。2022 年に「修正完了」した Web サイトの件数は 217 件で累計 8,419 件となった。また、「取扱い中」の届出は 116 件増加し、1,689 件となった。「処理終了」した届出は、248 件増加し、累計 10,779 件となった。



※( )内の数値は 2021 年末時点と 2022 年末時点の差分

■図 C-5　Web サイトの脆弱性関連情報の届出の処理状況の推移

参照

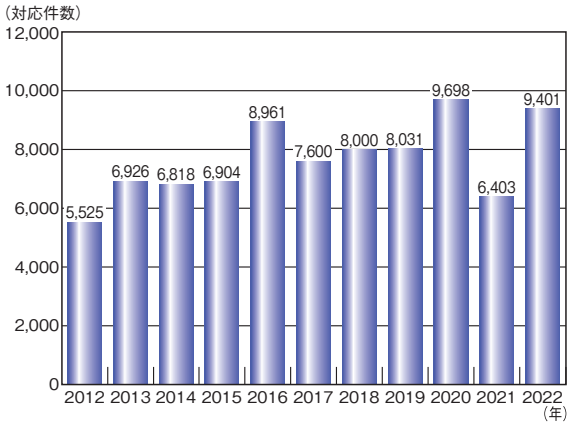
■ソフトウェア等の脆弱性関連情報に関する届出状況［2022年第4四半期（10月～12月）］
https://www.ipa.go.jp/security/reports/vuln/software/2022q4.html

資料D　2022年の情報セキュリティ安心相談窓口の相談状況

IPA が 2022 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

2022 年の年間相談対応件数は 9,401 件となり、2021 年の相談対応件数 6,403 件より 2,998 件（46.8%）の増加となった（図 D-1）。



■図 D-1　相談対応件数推移（2012～2022 年）

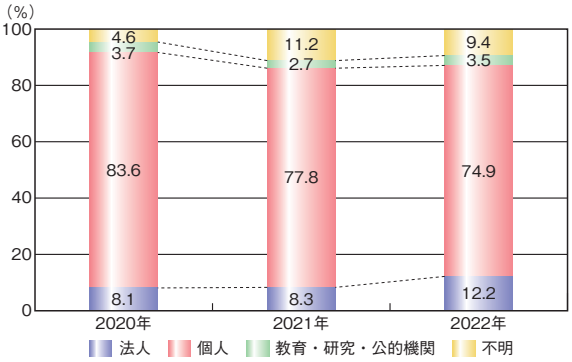
D.2　相談者の主体別相談件数

2022 年は個人からの相談が 7,043 件（74.9%）と最も多かった。

相談者の主体別相談比率の推移では、法人からの相談比率が 2 年連続で前年を上回り、2022 年は 1,145 件（12.2%）に達した（表 D-1、図 D-2）。

相談者の主体	2020 年	2021 年	2022 年
法人	782	530	1,145
個人	8,110	4,984	7,043
教育・研究・公的機関	359	170	330
不明	447	719	883
合計（件）	9,698	6,403	9,401

■表 D-1　情報セキュリティ安心相談窓口の主体別相談対応件数（2020～2022 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（2020～2022 年）

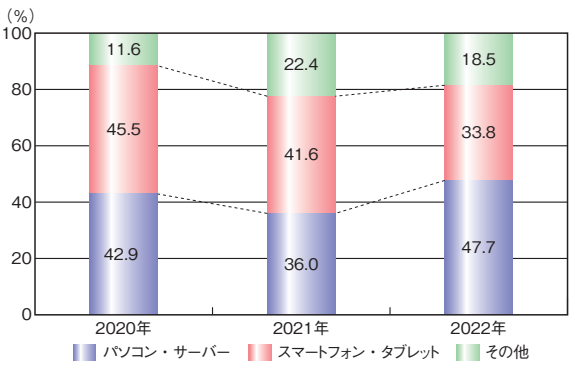
D.3　相談者の機器種別相談件数

2022 年は「パソコン・サーバー」に関する相談が 4,487 件（47.7%）と最も多かった。

相談者の機器種別相談比率の推移では、「スマートフォン・タブレット」に関する相談が減少する一方で、「パソコン・サーバー」に関する相談は大幅に増加した（表 D-2、図 D-3）。「Emotet 関連」についての相談増加が、要因の一つと考えられる。

機器種別の主体	2020 年	2021 年	2022 年
パソコン・サーバー	4,163	2,304	4,487
スマートフォン・タブレット	4,411	2,666	3,173
その他	1,124	1,433	1,741
合計（件）	9,698	6,403	9,401

■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（2020～2022 年）

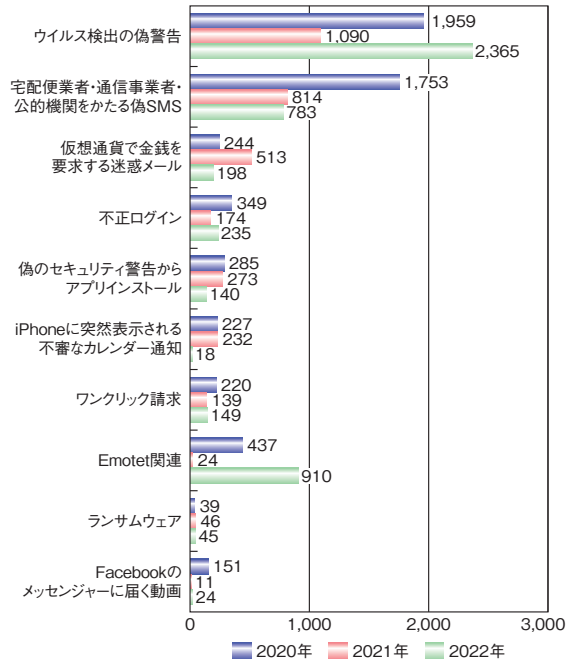


■図 D-3　情報セキュリティ安心相談窓口の機器種別相談件数の比率推移（2020～2022 年）

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。2022 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2,365 件（25.2%）であった。次いで、「Emotet 関連」についての相談が 910 件（9.7%）、「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 783 件（8.3%）であった。上位三つの手口による相談件数の合計は 4,058 件で、全相談件数（9,401 件）の 43.2% 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（2020～2022 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

IPAコンクール応援隊長「まもるくん」

第18回 IPA「ひろげよう情報モラル・セキュリティコンクール」2022 受賞作品

IPAは、子どもたちがインターネットにまつわる課題に自ら向き合い、解決策を見出すきっかけとして、全国の小学生・中学生・高校生・高専生を対象とするコンクールを開催しています。

ここでは、全61,962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。なお、すべての受賞作品は下記のWebサイトで公開しています。

[https://www.ipa.go.jp/security/hyogo/]

最優秀賞

〈独立行政法人情報処理推進機構〉

〈標語部門〉

話すのは
ネット上でも
人と人

北海道 北海道帯広柏葉高等学校 2年 **小沼 裕詞郎**さん

〈ポスター部門〉

青森県 弘前大学教育学部附属中学校 2年 **橋本 和香**さん

〈4コマ漫画部門〉

沖縄県 沖縄市立沖縄東中学校 2年
安慶田 ひよりさん

優秀賞

〈独立行政法人情報処理推進機構〉

〈標語部門〉

だいじだよ　ぼくのぶんしん　パスワード

東京都　世田谷区立東玉川小学校　1年
加藤 佑悟さん

ネットだと　ついつい緩む　心の扉

福岡県　福岡市立那珂中学校　3年
柳瀬 優月さん

鍵はした?　家もスマホも　一緒だよ

兵庫県　神戸学院大学附属高等学校　3年
森岡 泰椛さん

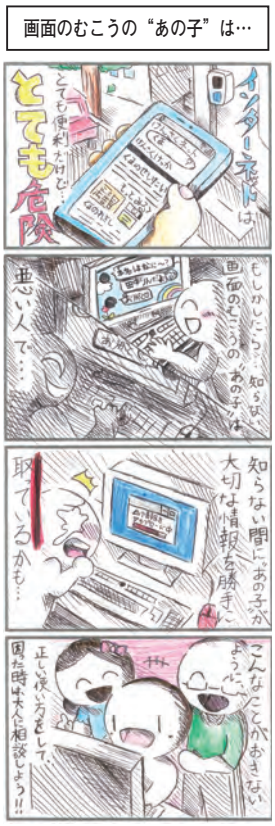
〈ポスター部門〉

愛知県 知立市立知立小学校 5年
石川 花凛さん

埼玉県 越谷市立千間台中学校 2年
北村 汐月さん

長崎県 長崎県立長崎工業高等学校 2年
藤本 佳穂さん

〈4コマ漫画部門〉



山梨県 山梨学院小学校 6年
大代 花凛さん

奈良県 香芝市立香芝北中学校 3年
内海 花菜さん

佐賀県 佐賀県立白石高等学校 1年
髙岸 孝仁さん

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://security-shien.ipa.go.jp/diagnosis/benchmark/index.html?bm_id=1

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)と度数分布状況と偏差値
- 情報セキュリティリスクの指標の分布と企業規模、業種、情報資産数等が自組織と近い他組織と比較し、自組織の位置が示された散布図
- 自組織の過去診断結果との比較や従業員数別での比較を含む 4 種類のレーダーチャート
- 結果に応じた推奨される取り組み

※ベンチマークに使用する診断データは 2022 年 3 月に Ver.5.1 にアップデート

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	脆弱性の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 12 種の 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

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	国内外のソフトウェア製品の公開された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が最新バージョンかどうかを確認
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とインストールされているバージョン等を一括確認できる

概要

■判定対象ソフトウェア製品

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

■動作環境・必須ソフトウェア

- Windows 10、11
- .NET Framework

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	日本で広く利用され、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
- BIND
- WordPress
- Apache Struts
- Joomla!
- 重要なセキュリティ情報
- Apache Tomcat
- OpenSSL

■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、IPA が発信する「重要なセキュリティ情報」とリアルタイムに同期した情報を表示させる

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
- サイバー攻撃への注意喚起
- 広く使われる製品のサポート終了情報

■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サーバー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

5 分でできる！情報セキュリティ自社診断
https://security-shien.ipa.go.jp/diagnosis/selfcheck/

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、診断結果に即した推奨資料やツールが確認できる

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。
オンライン版では、25 の質問に答えるだけで診断することができ、過去の診断結果や同業他社との比較もできます。また、診断結果に合わせてお薦めする資料、ツールが紹介されるため、今後どのような対策に取り組むべきかを把握することができます。

情報セキュリティ・ポータルサイト「ここからセキュリティ！」

学習 診断 対策

https://www.ipa.go.jp/security/kokokara/

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

概要

• セキュリティベンダー、公的機関、政府等から発信される注意喚起や、資料・動画・ツール等のコンテンツを網羅的に掲載したポータルサイト
• コンテンツを「被害に遭ったら」「対策する」「教育・学習」「セキュリティチェック」「データ＆レポート」に分類。必要な情報が見つけやすい
• セキュリティレベルを診断するクイズを「小学生」「中高生・ホームユーザ」「社会人」というカテゴリー別に紹介。楽しみながら学べる

サイバーセキュリティ経営ガイドライン実施状況の可視化ツール

診断

https://www.ipa.go.jp/security/economics/checktool.html

用途・目的	セキュリティ対策の実施状況のセルフチェック
利用対象者	主に従業員 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に準拠したセキュリティ対策の実施状況を成熟度モデルで自己診断し、レーダーチャートで可視化

概要

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

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

5 分でできる！情報セキュリティポイント学習

学習

https://security-shien.ipa.go.jp/learning/

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 e-Learning 形式で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。
また、利用者登録をしていただくと、学習の中断・再開ができ、これまでの学習進捗状況を表形式で確認することができます。

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

「標的型サイバー攻撃」「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」「スマートフォンのセキュリティ」「新入社員向け」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
- What' s BEC ？～ビジネスメール詐欺 手口と対策～
- 妻からのメッセージ ～テレワークのセキュリティ～
- 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

さ

た

な

は

ま

ら

わ

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　小川 隆一

執筆者

IPA

和泉 隆平	板垣 寛二	伊藤 彰朗	伊藤 吉史	内海 百葉
大島 尚	大友 更紗	小川 隆一	奥田 美幸	小幡 宗宏
甲斐 成樹	金子 成徳	神谷 健司	亀田 恭史	唐亀 侑久
河合 真吾	神田 雅透	木下 弦	小山 明美	佐川 陽一
佐藤 栄城	柴本 憲一	清水 碩人	白石 歩	菅 大豪
竹内 智子	武智 洋	田島 威史	丹野 菜美	近澤 武
辻 宏郷	中島 健児	中島 尚樹	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	古居 敬大	松島 伸彰
松田 琳花	宮本 冬美	森 淳子	安田 進	湯澤 凱貴
横山 美晴	吉野 和博	吉本 賢樹	與那嶺 崇	渡邉 祥樹
藁科 綾子				

株式会社日立製作所　相羽 律子
サイバーセキュリティ国際会議 CODE BLUE　発起人　篠田 佳奈
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
国立研究開発法人情報通信研究機構　横山 輝明
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

板橋 博之	伊藤 真一	井上 佳春	江島 将和	小沢 理康
加賀谷 伸一郎	亀山 友彦	菅野 和弥	栗原 史泰	桑名 利幸
小杉 聡志	塩田 英二	柴田 直	白鳥 悦正	高見 穣
高柳 大輔	田口 聡	土屋 正	遠山 真	西原 栄太郎
日向 英俊	前島 肇	前田 祐子	松田 修平	宮崎 卓行
渡辺 貴仁				

国立研究開発法人情報通信研究機構　井上 大介
一般社団法人 JPCERT コーディネーションセンター　江田 佳領子
長崎県立大学　島 成佳
三井物産セキュアディレクション株式会社　増田 聖一
明治大学　湯淺 墾道
経済産業省商務情報政策局サイバーセキュリティ課
経済産業省貿易経済協力局安全保障貿易管理課

おわりに

新型コロナウイルス感染症の拡大防止対策は結果としてテレワークやDXの推進を加速させ、ニューノーマルと呼ばれる大きな変化をもたらしました。そして、2022年2月に勃発したロシアによるウクライナ侵攻では、国同士の武力による衝突に、 サイバー攻撃や情報戦という新しい戦いが重大な要素として含まれるようになりました。2022年後半は生成系AIが話題となり身近なツールとして誰もがAIを利用できるようになりました。こんなに急激で大きな技術、環境の変化は経験したことがありません。本白書のサブタイトルの「進む技術と未知の世界 新時代の脅威に備えよ」には、このような大きな変化に潜む脅威に対しても基本を見失わず、連携して対処しなければならないという思いを込めています。

本白書は多岐にわたるサイバーセキュリティに関する国内外の事象や動向を調査・分析し、分かりやすい解説を心掛け、IPA職員だけでなく外部有識者の協力を得て作成しています。なお、IPAのWebサイトから本白書のPDF版が無料でダウンロードいただけます。 冊子、PDF版ともに、皆さまのサイバーセキュリティ対策の検討・実践の一助となれば幸いです。

編集子

情報セキュリティ白書 2023

進む技術と未知の世界：新時代の脅威に備えよ

2023 年 7 月 25 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**