情報セキュリティ白書

Information Security White Paper

2022

ゆらぐ常識、強まる脅威：想定外にたちむかえ

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2022」の刊行にあたって

2021 年も新型コロナウイルス変異株による感染拡大が継続しました。米欧では対策緩和の方針がとられましたが、ワクチン接種やそれに基づく移動許可等の可否について多くの議論を呼びました。日本は、厳しい規制の中で東京 2020 オリンピック・パラリンピック競技大会を無観客で開催、成功させましたが、その後も規制はゆるまず、テレワーク等の新しい業務形態が定着していきました。

この間、重要な組織やインフラを狙った攻撃も続きました。特に目立ったのがランサムウェア被害です。米国では 2021 年 5 月にエネルギー事業者が攻撃を受け、米国東部の石油供給が一時ストップしました。国内では 7 月に食品事業者がバックアップデータまで暗号化され、事業再開が遅れました。10 月には病院が攻撃を受けて診療に支障が出ました。2022 年 2 月には製造事業者が攻撃を受け、納入先の事業者の生産に影響が出ました。昨年の巻頭言で申し上げたとおり、こうした攻撃は巧妙化しており、システムの脆弱性やサプライチェーンを介して侵入し、情報を盗んで二重の脅迫を行う等、深刻な脅威となっています。一方脆弱性については、テレワークで活用が進んだ VPN 等の対策がまだ十分でなく、12 月には広範囲の Web システムに影響を及ぼす Log4j の脆弱性が報告されました。こうした懸念もあり、2022 年の 10 大脅威では修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）が初めてランクインしました。テレワークや DX 推進等によって生活や業務の各場面でデジタル化が進む中、安全で信頼できると思っていた機器やシステムに脆弱性が見つかり、ゼロデイ攻撃され、生活の一部が突然立ち行かなくなるかもしれない、そういう時代を私達は迎えつつあります。

更に 2021 年後半以降のウクライナ危機は、「まさかこのような事態が起こるとは」を私達に痛切に感じさせました。ロシアとウクライナの紛争は、情報セキュリティの視点からは、三つの点が特に注目されます。一つ目は、紛争が武力とサイバー空間上の攻防が組み合わされたハイブリッドな戦いであること。二つ目は、ネット等で配信される紛争関連情報が急増し、その信頼性の見極めが難しいこと。最後は、サイバー空間の攻防において、民間組織や個人が簡単に当事者になってしまうこと。私達は国家間の分断や物的な流通分断のリスクに加え、虚偽の情報に誘導される、サイバー攻撃の対象になる、等のリスクに直面することとなりました。

半年前まで想定できなかったこうした状況に私達はどう対応すればよいでしょうか。申し上げてきたことの繰り返しになりますが、リスク対応の基本が大切であると思います。情報セキュリティに関しては、機器やシステムの脆弱性をなくすこと、このサービスが止まったときにどうするか、の想像力を持つことは大変重要です。また虚偽の情報に惑わされないために、様々なソースの情報を参照し、視野を広く持つことも大切になるでしょう。本白書が、多くの方々に広く利用され、新しい生活や働き方のリスクに対する意識を高め、備えを実践するための一助となることを祈念します。

2022年7月

独立行政法人情報処理推進機構（IPA）

理事長　富田達夫

目次

コラム

情報セキュリティ白書

序章

2021年度の情報セキュリティの概況

2020年から世界中で流行した新型コロナウイルス感染症については、日本・米国・欧州ではワクチン接種が進み、感染者の増減はあるものの、経済活動は徐々に以前の状態に戻りつつある。国内では、感染拡大防止対策として実施されたテレワークやオンライン会議等が新しい働き方として定着しつつある。こうした業務の見直し、デジタル化は、組織におけるDX（デジタルトランスフォーメーション）の推進を後押しする形となっている。

2021年はランサムウェアの手口が巧妙化して被害が拡大し、サプライチェーンに関連したインシデントや脆弱性を狙った攻撃も引き続き発生した。警察庁によれば、2021年下期の被害報告件数は2020年下期の4倍となった。また、2021年7月の製粉会社、10月の病院の事案では、バックアップデータも暗号化されたために早期復旧が困難であった。データ保管方法の見直しや復旧計画の重要性が再確認された。

攻撃経路として、海外拠点、海外子会社、取引先が攻撃され、被害を受ける事案も多くみられた。2021年10月の医薬品メーカの情報漏えい事案は海外拠点が攻撃対象であった。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、部品供給先の自動車メーカの工場が1日停止した。サプライチェーン全体のセキュリティ強化が求められている。情報漏えい事案としては、マッチングアプリや大手製菓製造会社への不正アクセスにより合わせて300万件以上の大量の個人情報が流出した。

ソフトウェアの脆弱性を悪用した攻撃も継続して報告された。2021年に報告された脆弱性としては、VPN製品、Microsoft Exchange Serverの脆弱性、多くの製品やソフトウェアで使用されるJavaベースのロギングライブラリApache Log4jの脆弱性等、影響範囲が広く、攻撃により大きな被害が予想されるものが目立った。このほか、2021年初頭に欧州司法機関の一斉テイクダウンにより沈静化したウイルス「Emotet（エモテット）」の感染が再拡大し、2022年に入り注意喚起された。

セキュリティ政策面では、国内では2021年9月に「サイバーセキュリティ戦略」が閣議決定された。同戦略では「DX with Cybersecurity」として、デジタル社会の進展と併せてサイバーセキュリティ確保の取り組み推進が重要とされた。また同月にデジタル庁が発足、政府のIT基盤とセキュリティの整備を統括することとなった。サプライチェーンセキュリティについては、経済産業省がサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）等を継続的に推進した。

米国では、重要インフラやライフラインに関わる制御システムへの攻撃が相次ぎ、水道や浄水場等の制御システムへの攻撃、石油供給事業者へのランサムウェア攻撃が報告された。米国Biden政権は重要インフラのセキュリティ対策強化を打ち出し、これを受けた米国国立標準技術研究所（NIST）は、重要ソフトウェア調達におけるセキュリティガイドライン策定、消費者向けIoT製品のラベリング制度の検討等を実施した。NISTはまたサプライチェーンセキュリティに関する官民連携イニシアティブ（NIICS）の設置、サプライチェーンリスク管理の標準ガイド（NIST SP800-161）の改訂を進めた。今後の動向が注目される。

欧州では、欧州ネットワーク・情報セキュリティ機関（ENISA）が主導し、重要インフラに関するサイバーセキュリティ準拠法の改訂案（NIS2 Directive）審議、あるいは域内の製品・サービスのセキュリティを担保するサイバーセキュリティ認証スキーム（EUCC scheme V1.1.1）の構築等を中心としてセキュリティ政策を推進した。また欧州委員会は2021年4月、AI利用リスクへの対処に関する法案を公表した。同法は罰則を伴う初のAI利用規格として注目される。

このように、各国とも重要インフラやサプライチェーンへのセキュリティ対策強化を進めてきたが、2021年後半以降はウクライナ情勢が悪化、2022年2月のロシアのウクライナ侵攻により、世界は新たな緊張に直面している。この紛争は、武力とサイバー攻撃・防御あるいはサイバー空間での情報戦が組み合わさったハイブリッドな戦いが特徴であり、サイバー空間上では政府に加えて民間組織・個人が参画する、というまったく新たな状況が生まれている。政府の安全保障政策・サイバーセキュリティ政策は言うまでもなく、企業や個人がこのリスクへの対応、例えば、親ロシア系ハッカーの攻撃への備え、紛争に関連する情報の信頼度の見極め等をどうするべきか、が問われている。

2021 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
2021 年　4 月	● VPN 製品「Pulse Connect Secure」ゼロデイ攻撃発生（1.2.5） ● ファーストフードチェーン店でランサムウェア被害（1.2.8） ● マッチングアプリが不正アクセスを受け約 171 万件の個人情報流出（1.2.8、3.3.2）	■ 経済産業省「サイバーセキュリティ体制構築・人材確保の手引き」（第 1.1 版）改訂（2.1.2、2.3.1） ■ 欧州委員会「Artificial Intelligence Act」（AI 法）提出（3.4.2）
5 月	● 米石油供給事業者へのサイバー攻撃、身代金 500 万ドル相当を支払いか（3.4.1）	■ サプライチェーンセキュリティ強化を目指した米国大統領令 EO 14028 発表（3.4.1） ■ EU 域内のセキュリティ認証スキーム（EUCC scheme V1.1.1）公開（3.4.2）
6 月	● 無線通信機器メーカ、2017 年に不正アクセス確認から 3 年以上報告せず（1.2.8） ● 電子部品メーカの再委託先社員が取引先情報約 3 万件、従業員関連情報約 4 万件を不正持ち出し（1.2.8）	■ 総務省「スマートシティセキュリティガイドライン（第 2.0 版）」公開（2.1.3）
7 月	● 大手製粉会社がサイバー攻撃を受けシステム障害（1.2.2） ● IT 管理ツールをランサムウェア攻撃に悪用（1.1.1）	■ NISC「政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）」公開（2.1.1） ■ 総務省「ICT サイバーセキュリティ総合対策 2021」公開（2.1.3）
8 月	● ProxyShell の脆弱性を公表(1.2.5)	■ IPA「サイバーセキュリティ経営可視化ツール」公開（2.1.1） ■ NIST が「サプライチェーンセキュリティに関する官民を推進する国家イニシアティブ」を設置（3.4.1）
9 月		■ デジタル庁発足（2.1.1） ■ NISC「サイバーセキュリティ戦略」「サイバーセキュリティ 2021」決定（2.1.1）
10 月	● 徳島の町立病院でランサムウェアの被害発生（1.2.2） ● 医薬品メーカの国内外の拠点に不正アクセス（1.2.8）	■ NISC、第 14 回「日・ASEAN サイバーセキュリティ政策会議」開催（2.2.1） ■ Ransom Disclosure Act 米国議会に提出（3.4.1）
11 月	● 大手眼鏡販売チェーン持株会社で約 1 億円のビジネスメール詐欺被害（1.2.3） ● Emotet（エモテット）の攻撃活動再開（1.2.6）	■ NISC「クラウドを利用したシステム運用に関するガイダンス」公開（2.1.1、3.3.4） ■ CISA が既知の脆弱性悪用に関する重大リスクの削減に関する運用指令を公開（3.4.1）
12 月	● ロギングライブラリ Apache Log4j の任意のコード実行の脆弱性に関する注意喚起（1.1.1、1.3.2） ● スマホ決済のキャンペーン関係識別情報 13 万 3,484 件が GitHub 上で閲覧可能になっていたと発表（1.2.8）	■ 米 Biden 大統領が国防授権法に署名、アジア大平洋地域やウクライナ・NATO への関与を強化（3.4.1）
2022 年　1 月	● 決済サービス事業者不正アクセスによる情報漏えい公表（1.2.8）	
2 月	● ロシアがウクライナに侵攻（3.4.1） ● CISA、FBI がウクライナで使用された破壊的ウイルスに関し注意喚起（3.4.1）	■ NIST「ソフトウェアサプライチェーンセキュリティガイダンス」、NIST SP800-218 Ver.1.1 公開（3.4.1）
3 月	● 自動車部品会社がサイバー攻撃を受け、自動車メーカが国内工場停止（1.2.2） ● 大手製菓製造会社への不正アクセス（1.2.8） ● 複数の自治体で利用するクラウドが踏み台となり約 91 万件の迷惑メール発信（3.3.2）	■ CISA がウクライナ関連攻撃対策サイト「SHIELDS UP」を公開（3.4.1） ■ 総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」改訂版等公開（2.1.3）

※ 2021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。標的型攻撃、ランサムウェア被害、ビジネスメール詐欺、DDoS 攻撃、Web 改ざん、フィッシング等の攻撃や被害は通年で発生している。表中の数字は本白書中に掲載している項目番号である。特に注目されたもののみを挙げた。他のインシデントや手口と対策、及び政策・イベント等については本文を参照していただきたい。

第1章
情報セキュリティインシデント・脆弱性の現状と対策

2021年もテレワークやDX推進の取り組みが進む中、国内外でランサムウェアやサプライチェーン攻撃による大きな被害が続いた。Emotetの感染再拡大、影響と深刻度が大きいApache Log4jの脆弱性等も話題となった。

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 2021年度に観測されたインシデント状況

本節では2021年度に観測された世界と日本における情報セキュリティインシデントの発生状況について概説する。

1.1.1 世界における情報セキュリティインシデント状況

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。

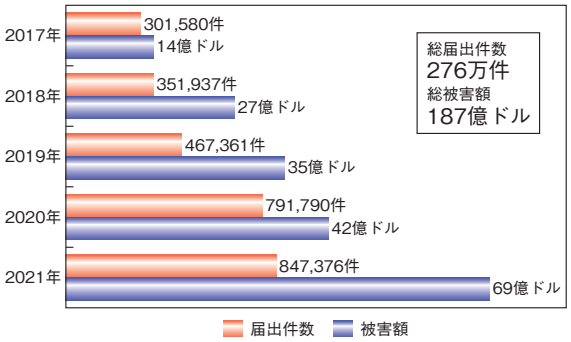
- 米国連邦捜査局（FBI：Federal Bureau of Investigation）：Internet Crime Report 2021※1
- Anti-Phishing Working Group, Inc（APWG）：Phishing Activity Trends Reports※2
- Verizon Communications Inc.（以下、Verizon社）：2022 Data Breach Investigations Report※3
- 日本アイ・ビー・エム株式会社（以下、IBM社）：IBM X-Force 脅威インテリジェンス・インデックス2022※4

(1) 広い範囲に影響を与えるサプライチェーンに対するインシデント

FBIによると、サイバー犯罪の件数と被害額は過去5年間増加を続け、2021の年間被害額は69億ドルとなった（図1-1-1）。

中でも、2021年は広範囲に影響を及ぼしたサプライチェーンに関わるインシデントが注目された。ここでは5件の事例を紹介する。

2021年5月、米Colonial Pipeline Companyがランサムウェアによるサイバー攻撃を受け、米国東海岸の燃料輸送が6日間にわたり停止し、多数のガソリンスタンドで売り切れや油価の高騰等、社会に大きな影響を与えた※5（「3.4.1 (1) (b) Colonial Pipeline事案とその対応」参照）。



■図1-1-1　サイバー犯罪の届出件数と被害額の推移
（出典）FBI「Internet Crime Report 2021」を基にIPAが編集

2021年の3月と8月に相次いで発見されたMicrosoft Exchange ServerのProxyLogon※6及びProxyShell※7の脆弱性においては、最も攻撃に晒されやすいインターネットに接続されたExchange Serverの総数が40万台以上にわたっていると報告された※8（「1.2.5 (2) Microsoft製品の脆弱性を対象とした攻撃」「3.4.1 (1) (a) Microsoft Exchange Server事案とその対応」参照）。

2021年12月には、Apache Log4jの任意のコードが実行される脆弱性（CVE-2021-44228）がアナウンスされた※9。Apache Log4jはApache Software Foundationが開発したオープンソースのJavaベースのロギングライブラリである。発見された脆弱性のCVSS（Common Vulnerability Scoring System）による深刻度は、最大値の10.0（レベルⅢ（危険））であった。影響を受ける最初のバージョンのリリースが2013年と古く、システムを開発する際に、開発者がこのモジュールを組み

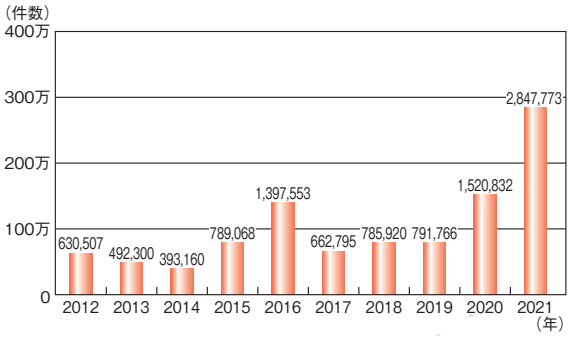
込むことが可能だったため、ソフトウェアの使用者が、Log4j が組み込まれていること自体を把握していなかったり、どのバージョンが組み込まれているかを把握することも困難だったりと、混乱が生じた（「3.1.2（1）（a）Log4Shell」参照）。

2020 年から続いた米 SolarWinds Worldwide, LLC. のネットワーク監視ソフト「Orion」の侵害による大規模な攻撃により、米政府機関を始め、同社顧客の 1 万 8,000 社が影響を受けた[※10]。このインシデントは、同社の正規アップデートファイルに悪意のあるウイルスが組み込まれた、サプライチェーン攻撃によるものであった（本インシデントに関係した米国の政策については「3.4.1 米国の政策」参照）。

2021 年 7 月には、米 Kaseya Limited の IT 管理ツール「VSA」がサイバー攻撃を受け、ランサムウェアを拡散する攻撃に悪用された。その結果、1,500 社近くの会社がランサムウェアによる攻撃を受けた可能性があると Kaseya Limited は発表している[※11]。

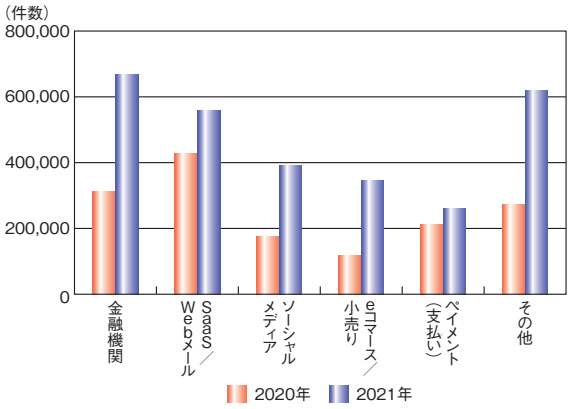
(2) フィッシングの傾向

APWG によると、2021 年の届け出されたフィッシングサイトの総数は約 284 万 8,000 件で、2020 年と比較して 87% 増と大幅に増加し、過去 10 年で最多となった（図 1-1-2）。



■図 1-1-2　世界における届け出されたフィッシングサイト件数
（出典）APWG「Phishing Activity Trends Reports」を基に IPA が作成

業種別のフィッシングサイト件数では、2021 年には、「金融機関」が 23.5%、「SaaS ／ Web メール」が 19.6%、「ソーシャルメディア」が 13.8% と続いている。2017 年から 2020 年までトップ 3 に入っていた「ペイメント（支払い）」は 9.2% と、全体に占める割合は減った。ただし、各業種別の件数を 2020 年と比較すると上記業種はいずれも増加しており、「ペイメント（支払い）」以上に件数が増加した業種が多かったに過ぎないことが分かる（図 1-1-3）。なお、フィッシングサイトの国内の傾向については「1.1.2 (3) フィッシングによる被害」を参照されたい。

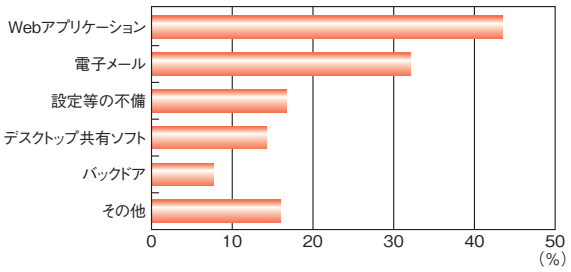


■図 1-1-3　業種別のフィッシングサイト件数（2020 年と 2021 年の比較）
（出典）APWG「Phishing Activity Trends Reports」を基に IPA が作成

(3) 情報漏えいインシデントの状況

Verizon 社によると、2021 年に同社が分析した 2 万 3,896 件のインシデントのうち、情報漏えい／侵害の件数は 5,212 件であり、2 万 9,207 件のインシデントのうち 5,258 件だった 2020 年[※12] に比べ、インシデント件数が 18.1% 減ったものの、情報漏えい／侵害の件数はほぼ横ばいだった。

情報漏えい／侵害の侵入手口では、「Web アプリケーション」の侵害が最も多く、「電子メール」「設定等の不備」「デスクトップ共有ソフト」と続いている（図 1-1-4）。



■図 1-1-4　情報漏えい／侵害の侵入手口（2021 年、n=3,279）
（出典）Verizon 社「2022 Data Breach Investigations Report」を基に IPA が編集

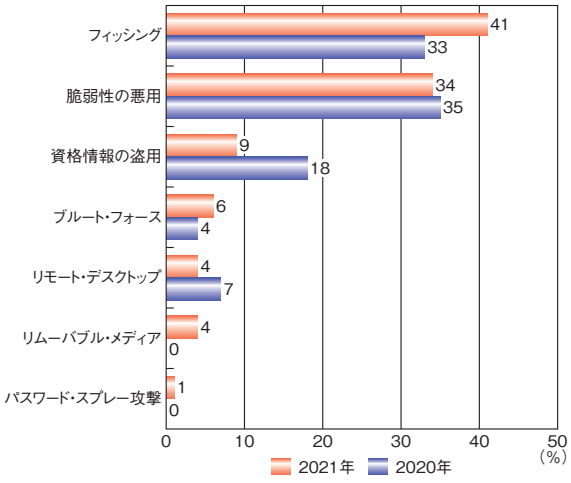
情報漏えい／侵害の 82% において、窃取された認証情報の利用、フィッシング、特権の誤用、ヒューマンエラー等、人的要因が関与していたという。

また、システムへの侵入インシデントの 62% がサプライチェーンを介して発生したという。

(4) 脆弱性とランサムウェアによる被害

IBM Security X-Force Incident response によって

観測された感染手口の内訳では、「フィッシング」と「脆弱性の悪用」が合わせて 75% と 2020 年に続いて多い。また、2021 年には、「リムーバブル・メディア」や「パスワード・スプレー攻撃※13」といった項目も新たに登場している（図 1-1-5）。



■図 1-1-5　上位の感染手口（2021 年と 2020 年の比較）
（出典）IBM 社「IBM X-Force 脅威インテリジェンス・インデックス 2022」を基に IPA が編集

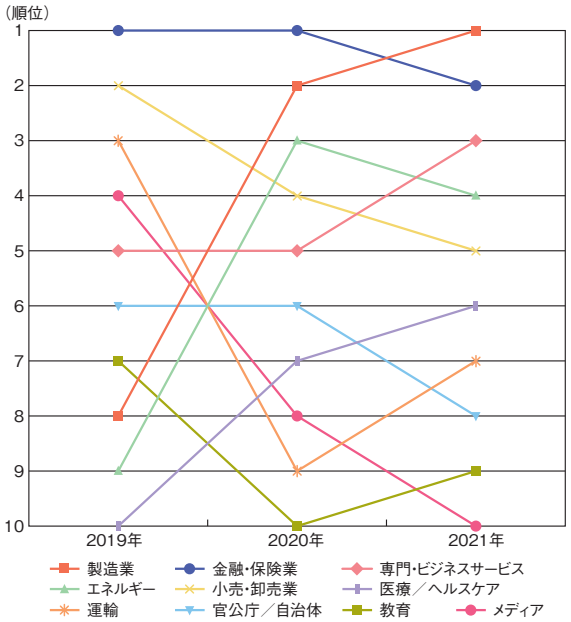
2021 年に頻繁に悪用された脆弱性の上位を表 1-1-1 に示す。2020 年には上位 10 件中 4 件※14 が 2 年以内に公表された脆弱性であったが、2021 年には上位 10 件中 8 件が 2 年以内に公表されたものとなった。

	CVE No.	内容
1	CVE-2021-34523	Microsoft Exchange server の ProxyLogon の脆弱性
2	CVE-2021-44228	Apache Log4j ライブラリの脆弱性
3	CVE-2021-26857	Microsoft Exchange Server におけるリモートでコードを実行される脆弱性
4	CVE-2020-1472	Netlogon の特権昇格の脆弱性
5	CVE-2021-27101	Accellion における SQL インジェクションの影響を受ける脆弱性
6	CVE-2020-7961	Liferay Porta におけるリモートでコードを実行される脆弱性
7	CVE-2020-15505	MobileIron におけるリモートでコードを実行される脆弱性
8	CVE-2018-20062	ThinkPHP におけるリモートでコードを実行される脆弱性
9	CVE-2021-35464	ForgeRock Access Management（OpenAM）におけるリモートでコードを実行される脆弱性
10	CVE-2019-19781	Citrix ADC および Citrix Gateway における任意のコードを実行される脆弱性

■表 1-1-1　2021 年に最も頻繁に悪用された上位の脆弱性
（出典）IBM 社「IBM X-Force 脅威インテリジェンス・インデックス 2022」を基に IPA が作成

この中でも Apache Log4j の脆弱性は 2021 年 12 月と比較的新しく報告されたものであるが、広く利用されているライブラリであるため、このように頻繁に悪用される結果になったと考えられる。

IBM 社によると 2021 年に攻撃の対象となった業種は、2020 年まで 1 位だった「金融・保険業」が 2 位となり、代わって「製造業」が初めて首位となった。また、2019 年の順位と比較すると「製造業」のほか、「エネルギー業」「医療／ヘルスケア」も順位が大きく上昇している（図 1-1-6）。

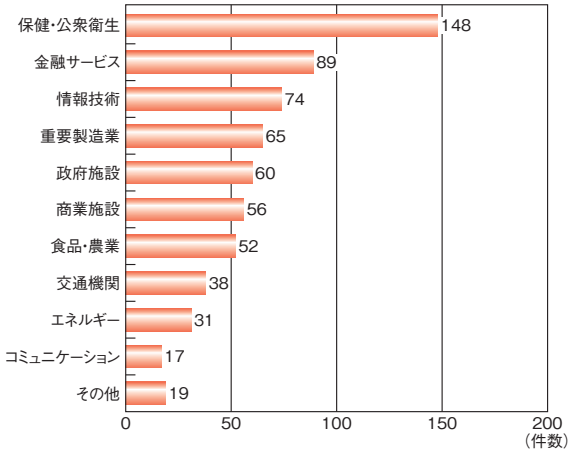


■図 1-1-6　最も頻繁に攻撃対象となった業界の順位（上位 10 業種）
（出典）IBM 社「IBM X-Force 脅威インテリジェンス・インデックス 2022」を基に IPA が作成

一方、FBI によると、ランサムウェア被害の届出件数と被害額は 2020 年には 2,474 件、29.1 万ドル※15 だったのに対し、2021 年には 3,729 件、49.2 万ドルと大幅に増加した。ランサムウェアの被害を受けた業界は、「保健・公衆衛生」が最も多く、「金融サービス」「情報技術」「重要製造業」が続いている（次ページ図 1-1-7）。

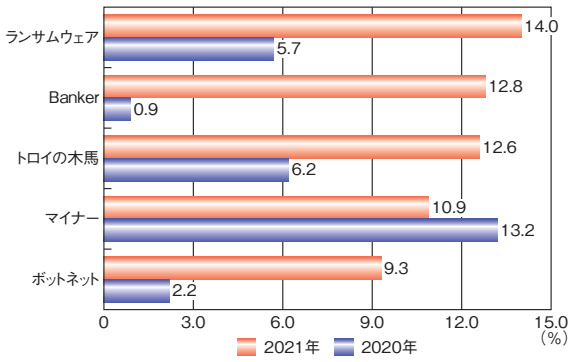
(5) Linux を狙うウイルス

Linux を狙うウイルスは年々増加しているが、IBM Security X-Force 脅威インテリジェンス・インデックスのパートナーである Intezer Labs の分析によると、ウイルス※14 のコードの多くが再利用されている場合は革新性は低く、独自のバリエーションが多い場合は革新性が高い、という方法論に基づく指標を用いて、固有のコードを持つ Linux 環境のウイルスの割合を調査した結果、2021 年は 2020 年よりはるかに固有のコードを持つウイル



■図 1-1-7　産業別ランサムウェア被害の届出件数
(出典)FBI「Internet Crime Report 2021」を基に IPA が編集

スの割合が高くなったと報告している（図 1-1-8）。更に、Linux のウイルスが増加している理由は、クラウドの利用増加に伴い、そこで運用される OS として Linux の比率が高いためと分析している。



■図 1-1-8　固有のコードを持つ Linux を狙うウイルス
（2021 年と 2020 年の比較）
(出典)IBM 社「IBM X-Force 脅威インテリジェンス・インデックス 2022」を基に IPA が編集

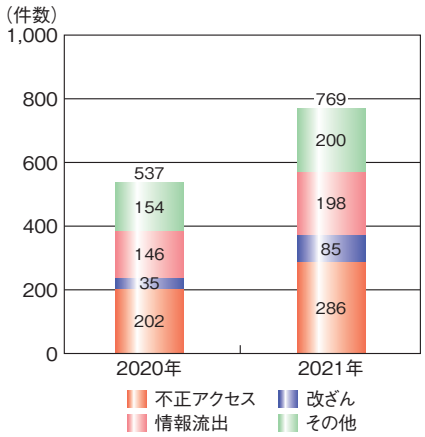
1.1.2 国内における情報セキュリティインシデント状況

国内における情報セキュリティのインシデント発生状況について、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※17
- 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）：インシデント報告対応レポート※18
- フィッシング対策協議会：月次報告書※19
- 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※20-1

(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 2021 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 769 件となり、2020 年の 537 件から 43.2% 増であった（図 1-1-9）。割合が最も多いのは「不正アクセス」で、37.2% であった。前年比では、「不正アクセス」が 141.6%、「改ざん」が 242.9%、「情報流出」が 135.6%、「その他」が 129.9% であった。



■図 1-1-9　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

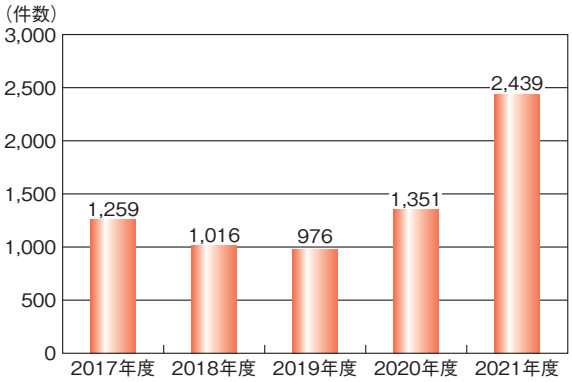
(2) Web サイト改ざんによる被害

2021 年 4 月 1 日から 2022 年 3 月 31 日までに JPCERT/CC へ報告された Web サイト改ざん件数は 2,439 件で前年比 180.5% と急増し、過去 5 年間では最多となった（図 1-1-10）。

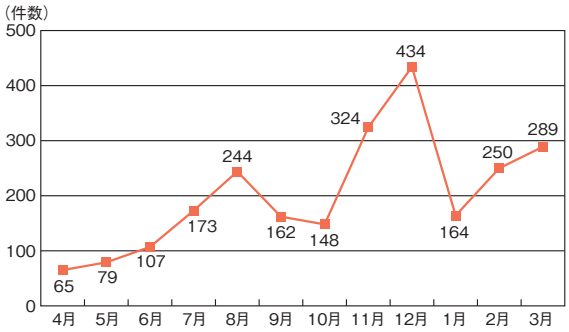
月別では 12 月が 434 件、四半期別では 2021 年 10 ～ 12 月が 906 件で最も多かった（次ページ図 1-1-11）。

(3) フィッシングによる被害

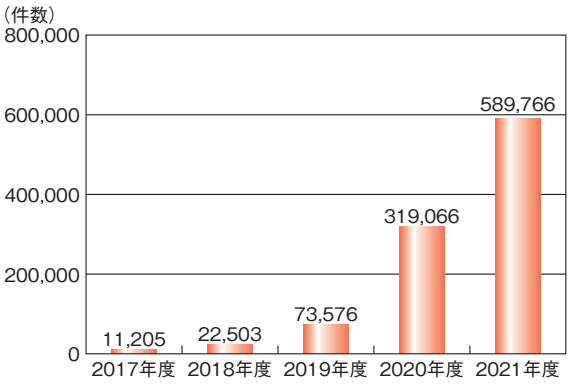
フィッシング対策協議会への 2021 年度の報告件数は



■図 1-1-10　Web サイト改ざん年度別件数推移（2017 ～ 2021 年度）
(出典)JPCERT/CC「インシデント報告対応レポート」（2017 年 4 月 1 日～ 2022 年 3 月 31 日）を基に IPA が作成



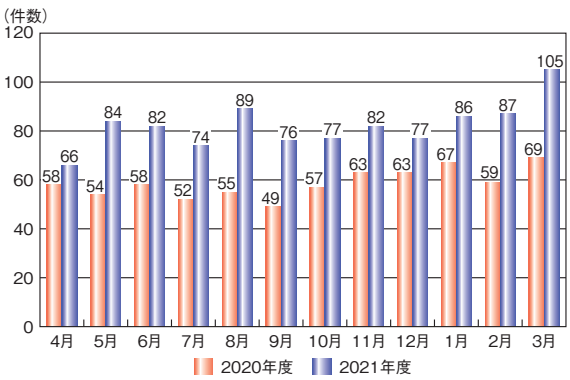
■図 1-1-11　Web サイト改ざん月別件数推移（2021 年度）
（出典）JPCERT/CC「インシデント報告対応レポート」（2021 年 4 月 1 日～ 2022 年 3 月 31 日）を基に IPA が作成



■図 1-1-12　年度別フィッシング報告件数（2017 ～ 2021 年度）
（出典）フィッシング対策協議会「月次報告書」（2017 年 4 月～ 2022 年 3 月）を基に IPA が作成

58 万 9,766 件で前年比 185% であった（図 1-1-12）。2020 年度の件数はその前の過去 3 年に比べて突出していたが、2021 年度は更にそれを上回り、2017 年度と比べると 52 倍以上に上る報告件数であった。この増加の内訳を悪用されたブランド数で見ると、2021 年度の各月ブランド数は 2020 年度の同月を 1.1 倍から 1.6 倍程度上回っていた（図 1-1-13）。

月によってブランドの変動はあるが、2020 年度は毎月上位四つのブランドで報告件数の約 9 割を占めていた[※20-2]。例えば「Amazon」「Apple」「LINE」「楽天」「三井住友カード」等である。しかし 2021 年度は悪用されるブランドが多岐にわたり、2020 年度のように特定のブランドが集中して悪用される傾向とは異なっている。



■図 1-1-13　悪用されたブランド数の比較（2020 年度、2021 年度）
（出典）フィッシング対策協議会「月次報告書」（2020 年 4 月～ 2022 年 3 月）を基に IPA が作成

表 1-1-2 は 2021 年度に悪用された各月の上位五つのブランドである。報告件数全体に占める割合は 2020 年度に比べ低下している。8 割を超過したのは 2021 年 4 月のみで、それ以降は 6 割から 7 割台半ばで推移し、2022 年 2 月、3 月には 6 割を切った。この傾向は上位の特定ブランド以外にも多くのブランドが悪用されたことが要因である。表 1-1-3（次ページ）は月間 1,000 件以上が報告されたブランドの数と全体に占める割合をまとめたものである。2020 年度の各月は上位 4 ブランドで約 9 割を占めていたが、2021 年 9 月以降は 10 以上のブランドで全体の約 8 割を占め、多種多様なブランドが悪用されていることがうかがえる。

警察庁によれば、フィッシングを主な手口とする「インターネットバンキングに係る不正送金」は、2019 年に被

	4 月	5 月	6 月	7 月	8 月	9 月
全件に占める割合	81.2%	76.6%	71.4%	67.8%	65.8%	64.0%
1 位	Amazon	Amazon	Amazon	Amazon	Amazon	Amazon
2 位	楽天	楽天	楽天	三井住友カード	三井住友カード	ETC 利用照会サービス
3 位	三菱 UFJ ニコス	三井住友カード	エムアイカード	楽天	エポスカード	イオンカード
4 位	三井住友カード	イオンカード	三井住友カード	イオンカード	イオンカード	三井住友カード
5 位	JCB	JCB	エポスカード	VISA	PayPay 銀行	コロナワクチンナビ
	10 月	11 月	12 月	1 月	2 月	3 月
全件に占める割合	66.6%	67.7%	74.0%	67.6%	56.6%	55.0%
1 位	Amazon	Amazon	Amazon	Amazon	Amazon	Amazon
2 位	メルカリ	メルカリ	メルカリ	メルカリ	メルカリ	メルカリ
3 位	三井住友カード	三井住友カード	三井住友カード	JCB	JCB	えきねっと
4 位	ETC 利用照会サービス	楽天	ETC 利用照会サービス	三井住友カード	—	—
5 位	楽天	ETC 利用照会サービス	JCB	—	—	—

■表 1-1-2　悪用された上位ブランド名と報告全件に占める割合
（出典）フィッシング対策協議会「月次報告書」（2021 年 4 月～ 2022 年 3 月）を基に IPA が作成

	9月	10月	11月	12月	1月	2月	3月
ブランド数	10	11	9	12	10	10	18
全件に占める割合	81.6%	83.2%	79.2%	88.4%	82.9%	74.2%	88.7%

■表 1-1-3　報告件数が月間 1,000 件を超過したブランド数と報告件数全体に占める割合
（出典）フィッシング対策協議会「月次報告書」（2021 年 9 月～ 2022 年 3 月）を基に IPA が作成

害額約 25 億 2,100 万円に達していたが、2021 年までに被害額は約 3 分の 1 に減少したという。一方、図 1-1-12（前ページ）のとおりフィッシングの報告件数は増加の一途をたどっている。

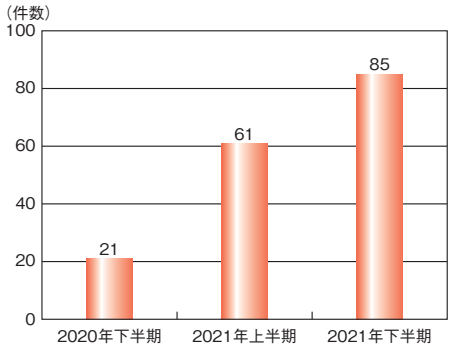
一般財団法人日本サイバー犯罪対策センター（JC3：Japan Cybercrime Control Center）によれば、2021 年は銀行を装ったフィッシングサイトの割合は少なく、ネット通販等の e コマース、通信事業者、クレジットカード会社等を装ったフィッシングサイトが多数を占めているという。「インターネットバンキングに係る不正送金」の被害額が減少している一方で、ネット通販等のクレジットカード情報を窃取するフィッシングサイトの割合が大きくなったことが、クレジットカード不正利用の被害額が増加している要因の一つと考えられるという。銀行等の金融機関から、クレジットカード情報や各種 EC サイトのアカウント情報へとフィッシングのターゲットが変化してきていることから、同センターは一層の警戒が必要あるという※20-3。

トレンドマイクロ株式会社（以下、トレンドマイクロ社）のレポートにおいても、誘導先となるフィッシングを含む詐欺サイトは、銀行等金融機関やクレジットカード関連のほか、モバイル決済、暗号資産取引所、生命保険、携帯通信会社、給付金・ワクチン等コロナ関連、水道等の公共料金支払い等、多岐に及ぶとしている。その要因として、これまでもサイバー犯罪における常套手段として用いられてきた詐欺手法が、コロナ禍における支払い・決済手段としてのインターネット需要の高まりにより、広く一般のインターネット利用者を狙う攻撃の中で拡大し、2021 年はその傾向が顕著化したとしている※20-4。

(4) 国内被害が拡大したランサムウェアについて

ランサムウェアについては、国内外で「二重恐喝」（窃取したデータを暗号化するだけでなく、金銭を支払わなければ、そのデータを公開すると二重に脅す手口。「二重の脅迫」とも呼ばれる）による被害の拡大や、産業制御システムに影響を及ぼすようなウイルスが引き続き確認されているほか、国内の医療機関等重要インフラ事業者が標的となり、市民生活にまで重大な影響を及ぼす事案も発生している。

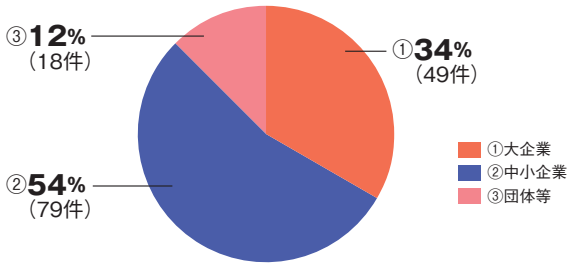
警察庁に報告された国内のランサムウェアによる被害の報告件数は、2020 年下半期 21 件から 2021 年上半期 61 件、同下半期 85 件と急激に増加した（図 1-1-14）。



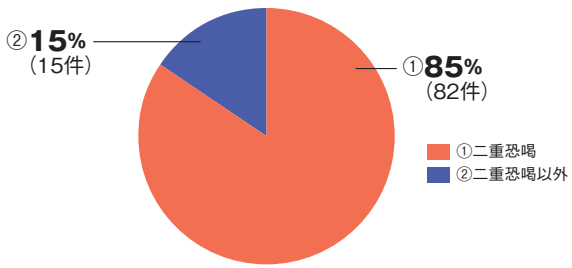
■図 1-1-14　企業・団体等におけるランサムウェア被害の報告件数の推移
（出典）警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

2021 年中にランサムウェア被害を警察に報告した企業に対し警察庁が行ったアンケート調査によると、企業・団体等の被害件数 146 件のうち、54% が「中小企業」であった（図 1-1-15）。また、金銭の要求が確認できたのはそのうち 97 件であり、「二重恐喝」による要求は 85% を占めたという（図 1-1-16）。

警察庁は被害のあった 146 件に対して、「復旧に要し



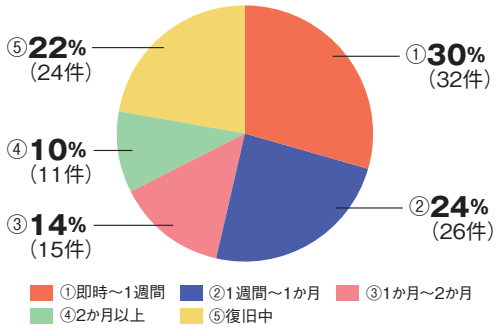
■図 1-1-15　被害企業・団体等の件数及び割合（n=146）
（出典）警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集



■図 1-1-16　被害の手口別件数及び割合（n=97）
（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」を基に IPA が編集

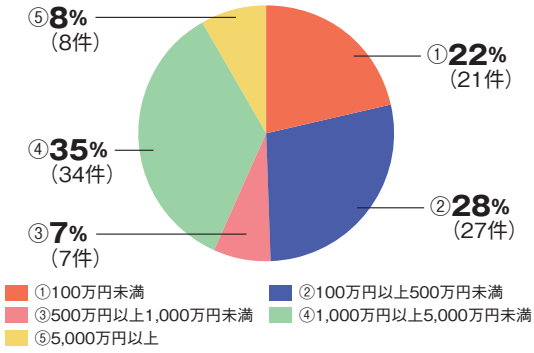
た期間」「調査・復旧費用の総額」「感染経路」についてアンケートを実施し、123 件の回答が得られた。

「復旧に 1 ケ月以上要した」のは、有効回答 108 件のうち 26 件、24% であった（図 1-1-17）。ランサムウェアの被害に遭うと、その後の事業継続に少なからず影響を及ぼすことが分かる。



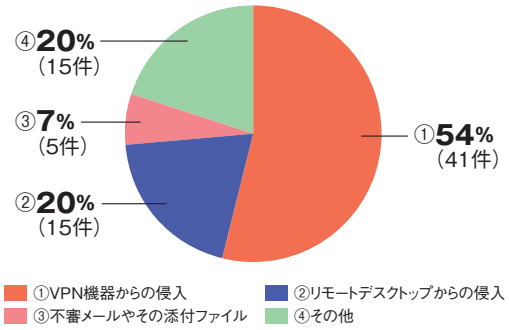
■図 1-1-17　復旧に要した期間（n=108）
（出典）警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

「調査・復旧費用の総額」で最多だったのは、有効回答 97 件のうち 34 件で 35% を占めた「1,000 万円以上～ 5,000 万円未満」であった（図 1-1-18）。被害に遭った企業・団体にとって、調査・復旧費用が重荷になっていると推察される。



■図 1-1-18　調査・復旧費用の総額（n=97）
（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」を基に IPA が編集

感染経路では、「VPN 機器からの侵入」が 54% と最も多く、「リモートデスクトップからの侵入」は 20% であった。一方で従来認識されていた「不審メールやその添付ファイル」を経由した侵入は 7% であり、テレワークの急速な拡大等に伴い生じた脆弱性を突いて攻撃している傾向が見受けられる（図 1-1-19）。



■図 1-1-19　感染経路（n=76）
（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」を基に IPA が編集

VPN やリモートデスクトップを感染経路としたランサムウェアは、新型コロナウイルス感染拡大で定着したリモートワークにより顕在化した脅威である。今後もリモートワークがゼロになることはなく、一般的なビジネス環境として活用が続くと考えられる。感染被害を引き起こさないためにも、企業・組織では脆弱性対策等の基本的対策のほか、万が一侵入された場合に備えた対策の充実が求められる（ランサムウェアの手口や対策については「1.2.2 ランサムウェア攻撃」参照）。

COLUMN

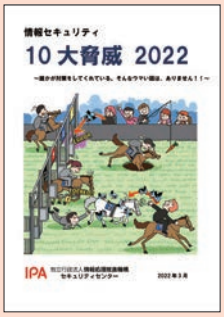
知ってる人は知っている、知らない人は多分ぜんぜん知らない 情報セキュリティの10大脅威

IPAが毎年、発表している情報セキュリティ10大脅威（表1）。2022年版では組織の7位に「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」が初ランクインしましたが、トップ10にランクインする顔ぶれは例年大きく変わることはありません。「毎年ほぼ同じ顔ぶれ」ということは残念ながら、これらの脅威はずっと、私たちの身近に存在し続けていると言えます。

表1 情報セキュリティ10大脅威 2022「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	標的型攻撃による機密情報の窃取
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	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	4	テレワーク等のニューノーマルな働き方を狙った攻撃
スマホ決済の不正利用	5	内部不正による情報漏えい
偽警告によるインターネット詐欺	6	脆弱性対策情報の公開に伴う悪用増加
不正アプリによるスマートフォン利用者への被害	7	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
インターネット上のサービスからの個人情報の窃取	8	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	9	予期せぬIT基盤の障害に伴う業務停止
インターネット上のサービスへの不正ログイン	10	不注意による情報漏えい等の被害

しかし、これらの脅威について一般のパソコン利用者の認知度を調査してみると、「ランサムウェア」が30.9%、「標的型攻撃」が26.8%、「ビジネスメール詐欺」が26.8%と決して高くはありません。最も認知度が高い脅威である「フィッシング」でも56.7%と、過半数を超えた程度です[i]。この認知度をどうとらえるかは人それぞれだと思いますが、職場やプライベートでインターネットの利用が不可避となる中、脅威を理解し、その対策を実践するのは、「ニューノーマルな生活の知恵」ではないでしょうか？　IPAは情報セキュリティの脅威とその対策が国民に広く浸透、理解されることを願っています。



「情報セキュリティ10大脅威 2022」解説書及び社内教育や研修に使える「情報セキュリティ10大脅威 2022」簡易説明資料（スライド形式）、関連するIT用語を解説した「知っておきたい用語や仕組み」は以下のURLからダウンロードできます。また、「情報セキュリティ10大脅威の活用法」も以下のURLで公開していますので併せてご活用ください。

https://www.ipa.go.jp/security/vuln/10threats2022.html

i　IPA：2021年度 情報セキュリティの倫理と脅威に対する意識調査－【脅威編】－
https://www.ipa.go.jp/security/economics/ishikichousa2021.html〔2022/5/23確認〕

1.2 情報セキュリティインシデント別の手口と対策

本節では、インシデント別の発生状況と、具体的な事例について述べる。また、2021 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 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。ウイルスメールやフィッシングメールを不特定多数の相手に無差別に送り付ける攻撃とは異なり、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、明確な目的を持って行われる。また、標的型攻撃は長期間継続して行われることが多く、攻撃者が標的とする組織（以下、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五つの段階に分類している（図 1-2-1）。

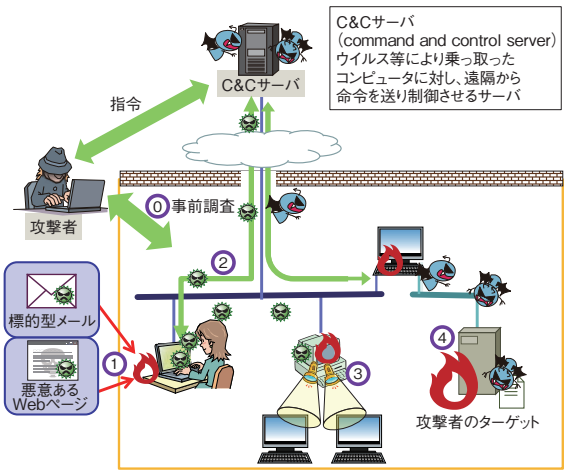
「事前調査段階」では、標的組織や業界の情報を収集する。公開されている情報を収集するだけでなく、標的組織と他の組織とのメールの盗聴等により必要な情報を収集することもある。

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、いわゆるサプライチェーン上のセキュリティの弱い部分を狙う手口に加え、VPN 製品や公開サーバ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。標的組織の人間に対し、ウイルスを仕込んだファイルが添付された、あるいは悪意のある URL リンクが記載された標的型攻撃メールを送り付ける手口も依然として確認されている。また、悪意のある Web サイトを閲覧しただけで、ウイルスに感染してしまうドライブ・バイ・ダウンロード攻撃が用いられることもある。

「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、標的組織内のパソコン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、遠隔操作を長期的かつ継続的に行うため、複数の RAT に感染させる場合もある。このとき、より隠密性の高いウイルス（ファイルレスマルウェア※22 等）を使うケースも確認されている。

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必要なウイルスやツールを送り込む。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、侵入したパソコン等に標準でインストールされてい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、国家間の政治的主張等を目的とした攻撃も確認されている※23。



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PC内でバックドアを作成し、外部のC&Cサーバと通信を行い、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 1-2-1　標的型攻撃の流れ
（出典）IPA「標的型サイバー攻撃の脅威と対策※21」を基に編集

(1) 国内の標的型攻撃事例

本項では、2021 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) ショートカットファイルを悪用した攻撃

JPCERT/CC のレポート※24 によると、2021 年 7 月から 9 月の間に、暗号資産交換業者を狙ったと考えられる

標的型攻撃の報告が寄せられたという。この攻撃は、標的組織に対し、ファイル共有を装ったメールが送られてくることから始まる。メールの本文中には URL リンクが記載され、URL リンクをクリックさせることで不正なショートカットファイルを格納した圧縮ファイルをダウンロードさせようとする。ショートカットファイルには、JavaScript ファイルをダウンロードして実行するコマンドが含まれており、最後には本命のウイルスに感染させられる。この攻撃手口は、2019 年 7 月に JPCERT/CC が公開した国内外の暗号資産に関連する組織を狙った攻撃キャンペーンと類似しているという※25。このキャンペーンでは、圧縮ファイルには、パスワードが設定された囮の文書とショートカットファイルが格納されている。ショートカットファイルには「パスワード.txt.lnk」のように二重拡張子で拡張子を偽装したファイル名が付けられており、囮の文書のパスワードを確認しようとショートカットファイルを開いてしまうと、攻撃が進行し、最終的には本命のウイルスに感染させられる※26。

手口が類似していることから、同じ攻撃者が継続して標的型攻撃を行っているものと思われる。

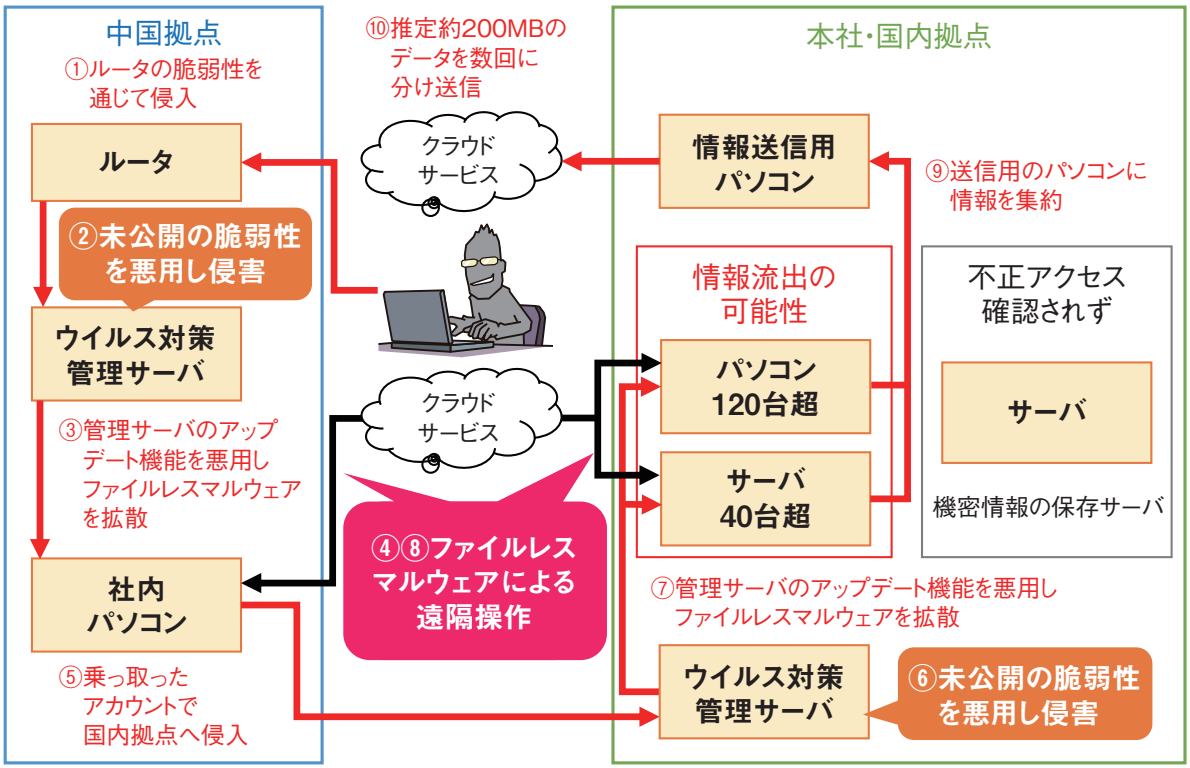
(b) 国内企業の海外拠点を狙った未公開の脆弱性を悪用した標的型攻撃

2019 年 6 月に三菱電機株式会社の国内拠点の端末のセキュリティソフトが不審な挙動を検知し、社内ネットワークが外部から不正アクセスを受けていたことが、同社プレスリリースにて 2020 年 1 月に公表された※27。2020 年 2 月に公表された第 3 報によると、中国にある海外拠点への侵入を発端とした標的型攻撃と考えているとのことであった※28。

2021 年 12 月、防衛省は、本件により流出した可能性のある防衛関連のデータファイル約 2 万件のうち、安全保障に影響を及ぼす恐れのあるデータファイルは 59 件であるとの調査結果を公表した※29。三菱電機株式会社も同時期に、第 4 報として本件により流出した可能性のある防衛関連の一部のデータの管理不備について、防衛省より注意・指導を受けたとの内容を公表した※30。

図 1-2-2 は、公表された資料を基に、システム構成の概略と攻撃経路を図示したものである。

本事例では、攻撃者は最初にルータの脆弱性を悪用し、中国拠点の社内ネットワークに侵入し、中国拠点のウイルス対策管理サーバ（以下、管理サーバ）へ未公開の脆弱性※32 を悪用した攻撃を行い、同サーバを侵害した。次に、管理サーバのパターンファイルアップデート機能を利用して拠点内の端末にファイルレスマルウェアを拡散した。感染した端末を大手クラウドサービス上に構築したサーバから遠隔操作し、中国拠点と同じ手口で日



■図 1-2-2　標的型攻撃の事例概要
（出典）三菱電機株式会社「不正アクセスによる個人情報と企業機密の流出可能性について（第 3 報）※28」及び piyolog「ログ消去もされていた三菱電機の不正アクセスについてまとめてみた※31」を基に IPA が編集

本国内の管理サーバを経由して国内の端末へ感染を拡大していった。

本事例では、セキュリティ対策が強固な日本国内のネットワークへ侵入するための足掛かりとして、中国拠点が狙われたものと思われる。攻撃者は中国拠点の管理サーバへの攻撃において、送信元アドレスを詐称し、特定を困難にしていたという。また、ファイルレスマルウェアの利用や不正通信先に大手クラウドサービスを利用するといった、ウイルス対策製品等で検知しづらい手法が用いられていた。更に、未公開の脆弱性を悪用するゼロデイ攻撃が行われていたため、侵入を完全に防ぐことは困難であったと言える。他のサイバー攻撃と同様に、侵入を前提とした多層的なセキュリティ対策を実施し、速やかに攻撃を発見し対応できる体制を整備しておくことが望ましい。

(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等が標的となった事例以降、継続的に発生している。

「1.2.1 (1) 国内の標的型攻撃事例」で紹介したように、海外関連組織を足掛かりとした攻撃も確認されており、海外を含む企業グループ全体でセキュリティ対策を講じていく必要がある。

初期潜入段階で用いられる手口としては、2020 年と同様に、標的型攻撃メールのみならず、テレワークの普及で利用が拡大した VPN 製品や外部からアクセス可能なサーバ等の脆弱性管理の不備を突く事例が報告されている。

一方、海外の事例では、重要インフラ組織や防衛・政府機関を標的とした攻撃が報告されている※33。今後日本の組織が攻撃されることも予想されるため、業種や規模にかかわらず、常に対策を講じておくことが重要である。

(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、代表的な標的型攻撃の手口を以下に示す。

なお、記載する手口はこれまでに確認されているものの一部であり、業務形態や IT 環境・セキュリティ対策の変化に応じて、攻撃者も手口を変化させていくことが予想されるため、新たな手口への注意も重要である。

(a) 標的型攻撃メール

標的型攻撃メールは、標的とする企業・組織・業界でよく用いられる言葉を使用し、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というソーシャルエンジニアリングの手口である。

攻撃者はメールの信憑性を高めるため、標的とする企業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するケースが過去に確認されている。

(b) サプライチェーン・海外拠点等への攻撃

「1.2.1 (1) (b) 国内企業の海外拠点を狙った未公開の脆弱性を悪用した標的型攻撃」や「情報セキュリティ白書 2021※34」の「1.2.1 (1) 国内の標的型攻撃事例」で紹介したように、標的となる組織のネットワークやシステムを直接狙うのではなく、取引先企業や海外拠点、または海外の子会社を初期潜入の標的にした攻撃の手口が確認されている。

これは、取引先企業が小規模の組織であるとセキュリティ対策が脆弱であったり、また海外拠点・組織に対しては国内のセキュリティガバナンスが効きにくかったりする傾向が強いためである。攻撃者は事前調査段階で、標的組織のネットワークやサプライチェーン全体を見渡し、そのうちの脆弱な箇所を侵入のための足掛かりとしている。

(c) VPN 製品や公開サーバ等の脆弱性を悪用した攻撃

米国政府機関によると、攻撃者は標的組織への侵入経路として、SSL-VPN 製品の脆弱性を利用している可能性があると報告されている※35。

また、Web サイトやユーザ向けシステム等、公開サーバの脆弱性を悪用した攻撃による被害も確認されている。特に近年、脆弱性情報が公開された後、その脆弱性を悪用した攻撃方法が作成されるまでの時間や、その攻撃方法が悪用されるまでの時間が短くなっている傾向がある※36。修正プログラムが作成される前に攻撃され、被害が発生してしまうこともある。

(4) 標的型攻撃の手口（攻撃基盤構築段階）

攻撃基盤構築段階における、最近確認している具体的な手口を紹介する。

(a) 感染の永続化

攻撃者は、標的組織内での活動を継続して行うため、

端末の起動時にRATが自動的に実行されるよう、レジストリの改変やタスクスケジューラの登録等を行う。このとき、ファイルレスマルウェアを用いることで、セキュリティソフト等による検知を避けようとする手口が確認されている※37。

(b) 組織内での侵害範囲拡大

前述の国内企業の海外拠点を狙った事例のように、セキュリティソフトのアップデート機能等、標的組織のシステムやアプリケーションソフトが持つファイルの共有・配布機能を悪用して組織内で侵害範囲を拡大する手口が確認されている。

(c) 感染端末と攻撃者のサーバとの通信

感染端末と攻撃者のサーバとの通信においては、通信先（攻撃者のサーバ）のIPアドレスやドメインを頻繁に変えるほか、前述の事例のように、大手クラウドサービスを通信先として悪用することで、正規の通信であるかのように見せかけ、セキュリティソフト等での検知を逃れようとする手口が確認されている。また、通信内容を暗号化したり、一見無害な画像データの中に命令を埋め込むステガノグラフィ技術を用いたりすることで、命令を隠ぺいする手口も確認されている※38。

(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、計画的かつ巧妙に攻撃を遂行する。このため、ある対策を取れば完全に防御できるということはなく、多層的防御が必要である。組織の規模や業種により取り得る対策は異なるが、情報資産を守るためには、あらゆる可能性を考慮し、対策の検討と選別、実施を行うことが重要である。以下に、その例を示す。

(a) 利用者の意識向上

利用者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

  標的型攻撃では、標的組織に関連する人物のメールアカウントを攻撃者が悪用してメールを送信するものや、組織や業界固有の用語等をメール本文中で用いて自然な文章を装ったもの等、受信者を騙すために巧妙な手口が使われることが多い。しかし、標的型攻撃メールがすべて精巧に作られているわけではない。そのため、組織としては、利用者へ不審メールに対する注意力向上に向けた教育や注意喚起を実施することが重要である。また、利用者が不審な点がないか注意し、不用意な添付ファイルの開封や、本文URLリンクのクリック、及びメールへの返信をしないことは、有効な対策である。添付ファイルを開いてしまい、不審と感じるメッセージやダイアログが表示された場合や、表示されたメッセージの意味が分からない場合はその指示に従わずに、企業のシステム管理部門へ連絡することが望ましい。

- SNSを悪用した手口の周知

  攻撃者はSNSを悪用し、求人や共通の趣味等、個人への関心を装って攻撃対象者に近づき、信頼関係を構築する。そして、悪意のあるファイルやURLリンクを送り、それを開かせることで初期潜入の経路を開拓することがある。

  個人の環境でSNS等の利用を制限することは難しいが、このようなケースがあることを周知し、利用者の警戒意識を高めることは有効である。また組織内の業務環境では、個人によるSNSの利用を制限することが望ましい。

- 標的型攻撃メール訓練等の実施

  擬似的な標的型攻撃メールを利用者に送信して、そのメールへの対応を行う訓練（標的型攻撃メール訓練）の実施も利用者の意識向上に有効である。訓練を通じて、不審メールを受信した場合に着目すべき箇所の再確認や、不審メールを受信した際、あるいは受信したメールの添付ファイルを開いてしまった（ウイルスに感染した）際に必要となる対処の再確認を行う。必要となる対処には、組織内の不審メール届出窓口への連絡も含まれる。不審メールを開封したことを責めず、利用者に報告してもらい、情報を共有することが重要である。また、利用者が不審メールを未読のまま削除するだけでは不十分であり、報告が必要であると理解してもらうことも重要である。

  このような訓練を定期的に行うことで、利用者の対応能力を維持・向上させる。また、具体的な攻撃手口を利用者に周知することも対応能力の向上に有効である。

(b) 組織としての対応体制の強化

組織として攻撃に対応していくための体制の強化を図る対策例を以下に示す。

- CSIRT設置と運用

  利用者が標的型攻撃メール等の不審なメールを受信した際に、連絡すべき窓口が組織内に周知されていることは重要である。また、組織外から連絡を受けて

標的型攻撃の被害に気付くことも考えられるため、外部からの連絡を受ける窓口を設けることも重要となる。このような、組織内部・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※39。

- インシデントの発生を想定した事前準備
  組織内にCSIRT等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（BCP：Business Continuity Plan）に情報セキュリティの観点を組み込み、運用しておくとよい。
  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て演習を行うことが望ましい。これは、組織全体の対応力・回復力（サイバーレジリエンス）の強靭化に有効である。
- 流行している攻撃の手口や対策の組織内共有
  今後も引き続き、標的型攻撃によるセキュリティインシデントが、被害を受けた組織から公表され、また各報道機関やセキュリティベンダがその手口や対策を発表していくことが想定される。
  これらの情報をCSIRT等が定期的に収集し、自組織において同様の脅威となり得るか確認し、必要であれば自組織の対策に組み込むことは重要である。具体的には、攻撃者の侵入手口が特定機器の脆弱性を突いたものであれば、自組織のシステムに該当する機器や脆弱性がないか確認し、修正プログラムが適用されていなければ適用する。標的型攻撃メールにより攻撃が行われたのであれば、社内にそのメールの特徴を周知することで、類似した攻撃メールによる被害が発生しないようにすることが望ましい。
- 海外拠点・サプライチェーンを意識したセキュリティ対策の強化
  前述のとおり、攻撃者はセキュリティ対策が脆弱な海外拠点や海外子会社、取引先企業を初期潜入の標的にする傾向がある。このため、海外拠点・サプライチェーンを意識したセキュリティ対策の強化が求められている。
  具体的には、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が策定・周知され、またセキュリティリスクの可視化と、改善や対策活動が行われることが望ましい。実施する際は、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。
  また、国内・海外を問わず取引先等とは、セキュリティ対策状況や連絡体制を共有し、セキュリティインシデント発生時の連携を容易にすることで、サプライチェーンを狙った標的型攻撃にいち早く対処可能となる。

（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リンク先の情報等を検知し、必要に応じて利用者に警告することで、利用者に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、ウイルス検査はもちろん、サンドボックス上で動的にファイル解析を行うことも有効である。なお、オンラインで提供されるサンドボックスを利用する際は、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。不審メールをいつでも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活用し対策を取ることができる。
- 適切な修正プログラムの適用
  システムの脆弱性を悪用する標的型攻撃に備え、IT資産管理システム等を活用し、組織内のすべてのサーバ・パソコン等に適切に修正プログラムが適用できる仕組みを作ることが望ましい。
  特に今回紹介した手口のように、初期潜入段階ではインターネットに公開されたサーバやVPN製品等の脆弱性が狙われる傾向がある。これらの製品は、システム環境によってはすぐに修正プログラムを適用できない場合もある。また、脆弱性情報が公開されたら速やかに対応することが望ましいが、その時点で修正プログラムが提供されていないこともある。その場合、ベン

ダから一時的な回避策が提示されていれば適用を検討する、提示されていなければ当該システムを一時的に停止する等の対応が有効である。修正プログラムを適用する場合、検証環境でテストし、問題がなければ本番環境に適用する等の対応が必要となることもあるため、適用するシステムを想定して、どのように対応していくか、事前に計画を立てておくことが望ましい。運用中のシステムの脆弱性対策を外部へ委託する場合、委託先と協議の上、事前に具体的な実施内容を取り決めておくことが重要である。

- 通常業務で使わないファイルの実行・ソフトウェアの利用防止
  利用者が通常の業務では使わないであろう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制御することが望ましい。具体的には、利用者の環境で実行可能なファイルの種類やソフトウェアを許可リスト化しておくことで、ウイルスへの感染を防止する。許可リストのみによる制限の実施が難しい場合は、利用者の環境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禁止リスト化する。
  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。
- セキュリティ対策の再チェック
  2021年度も新型コロナウイルスの流行は収束しておらず、テレワークを目的としたVPN製品等のシステムの導入や、システム構成または設定の変更等が継続して行われた。しかし、適切なセキュリティ設計や設定が行われていなかったり、セキュリティ設定をあえて緩和したりすることで、脆弱な箇所が発生するケースもあったと思われる。
  そのようなケースを認識している場合には、改めてセキュリティ対策が現状のままでよいか再検討することが望ましい。
- ネットワーク構成の変化に合わせた対策
  働き方の多様化により、仕事場を従来の職場に限定せず、在宅でも可能にする勤務形態や、BYOD（Bring Your Own Device）端末の業務利用の広まりにより、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業務端末（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（Endpoint Detection and Response）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マルウェア等の検知・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きており、データそのものへのセキュリティ対策（暗号化やDLP（Data Loss Prevention）等）を検討することも有効である。

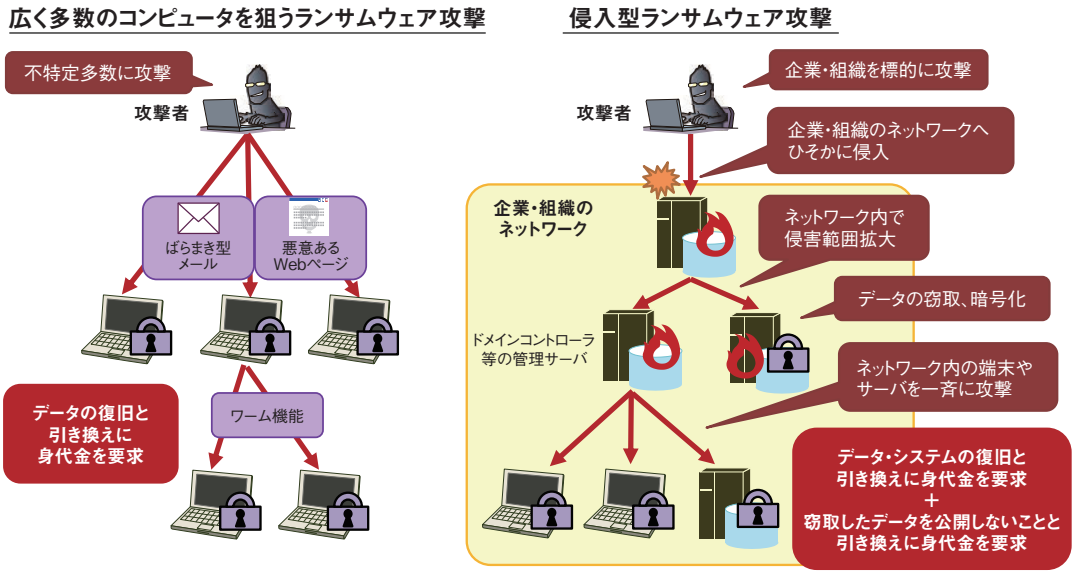
以上のように、利用者のセキュリティリテラシーの向上、インシデント発生時に適切に対応できる組織体制の構築、システムによる各種対策等、複数の観点を組み合わせ、多層的に対策を実施していくことが標的型攻撃への対策として重要である。

1.2.2 ランサムウェア攻撃

ランサムウェアとは「ransom」（身代金）と「software」（ソフトウェア）を組み合わせた造語で、パソコンやネットワーク接続された共有フォルダ等に保管されたファイルを暗号化することや、画面をロックすること等により、パソコンやファイルを使用不可にするウイルスの総称である。使用不可の状態から復旧することと引き換えに身代金を支払うように促すメッセージを表示することから、ランサムウェアと呼ばれている。本項では、ランサムウェアを使用したサイバー攻撃を「ランサムウェア攻撃」と呼ぶ。

ランサムウェア攻撃には、大きく分けて次の2種類がある（次ページ図1-2-3）。

- 広く多数のコンピュータを狙うランサムウェア攻撃
  ばらまき型メール、悪意のあるWebサイトからのダウンロード、脆弱性の悪用等で、広く不特定多数のコンピュータをランサムウェアに感染させようとする攻撃。2017年に多くの感染が確認された「WannaCry」と呼ばれるランサムウェアでは、感染拡大の方法として、脆弱性を悪用したワーム（自己複製）機能の手口が用いられた。
- 侵入型ランサムウェア攻撃
  攻撃者自身が様々な攻撃方法を駆使し、企業・組織のネットワークへひそかに侵入し、システムの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等、事業継続に関わるような被害を与える攻撃。組織の内部ネットワークへの侵入手口には標的型攻撃と同様の攻撃技術が使われる。海外では「human-operated ransomware attacks（人手によ



■図 1-2-3　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※40」を基に編集

るランサムウェア攻撃）」とも言われる。侵入型ランサムウェア攻撃では、データの復旧のために金銭を要求するだけでなく、データを窃取し、身代金を支払わない場合、データを公開するといった脅迫も行うことがある（「二重の脅迫」と呼ばれる）。

(1) ランサムウェア攻撃の傾向

従来の主流は「広く多数のコンピュータを狙うランサムウェア攻撃」であったが、2018※41 ～ 2019 年※42 ごろから「侵入型ランサムウェア攻撃」や「二重の脅迫」が観測され始めた。2020 年には、複数の日本企業・組織の被害が報道され、IPA※40 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）※43 が同攻撃の手口について注意喚起を行っている。

また、警察庁の公表した資料※44 によると、2020 年下期の企業・団体等におけるランサムウェア被害の報告件数が 21 件であったものが、2021 年上期は 61 件、2021 年下期は 85 件と急増した。2022 年 2 月にも、自動車部品会社である小島プレス工業株式会社がランサムウェア攻撃を受けたことにより、トヨタ自動車株式会社が国内全工場（14 工場 28 ライン）を 3 月 1 日に丸 1 日停止させるという被害が出ている※45。これらのことから、今後も日本の企業・組織が攻撃対象となる状況は続くと予想されるため、注意が必要である。

なお、ランサムウェア攻撃は 2015 年前後から高度に組織化・分業化※46 の動きも見られており、ランサムウェア（ウイルス）の開発、攻撃の実行、及び身代金の回収を別の攻撃者が分担して行う等のシステムが成立している。そのため、高度な技術を持たなくても、簡単に攻撃が行える状況となっており、多くの企業・組織が攻撃対象となり得る。

侵入の手口については、2021 年も継続して、VPN 製品※47 や Windows のリモートデスクトップサービス※48 の設定不備、あるいは脆弱性を悪用する手口が確認されている。従って、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、対策を講じる必要がある。

(2) ランサムウェア攻撃の被害事例

2021 年度に公表された事例から次の 2 件を紹介する。両事例ともにバックアップデータまで暗号化されて復旧が困難となり、被害が大きくなった。バックアップデータをオフラインで保存する等、暗号化されることのない状態でバックアップデータを管理することの重要性が示唆される。

(a) 国内病院の被害事例

2021 年 10 月 31 日、徳島県つるぎ町の町立半田病院は、ランサムウェアに感染した事実を公表した。報道※49 を基に被害状況や攻撃の手口を紹介する。

公表当日の 0 時半ごろ、同病院の電子カルテのデータが暗号化され、患者約 8 万 5,000 人分の記録が参照できなくなったほか、受付・診察・会計まで、すべての IT システムがダウンした。また、病院内のプリンタから大量に文章が印刷された。内容は「身代金を払わなければ、盗んだデータを公開する」といった旨の英語の脅迫

文であったという。

同病院では電子カルテのデータをバックアップサーバに保存していたが、バックアップサーバもランサムウェアにより暗号化されたため、システムの復旧が困難となった。同病院によると、バックアップサーバは災害時にメインサーバが壊れた場合の予備として用意していたもので、サイバー攻撃から守る仕組みにはなっていなかったという。

同病院は、電子カルテ復旧のため身代金の支払いも検討したが、身代金を支払ってもデータが復旧する保証がないこと等から、支払わないことを決め、約2億円をかけ新システムを構築することにした。しかしながら、窃取された可能性のある電子カルテ等の個人情報は、今後も流出のリスクが残存することとなった。

同病院では、少なくとも約4,000枚のカルテを手書きで作り直したが、過去の治療歴を正確に把握できなかったことや、新規患者や救急搬送の受け入れを停止せざるを得ない状況になったこと等、2022年1月4日の全面再開まで約2ヵ月間、病院の機能低下を強いられた。同病院は13の診療科を持ち、1日約300人が通院する県西部の主要な病院であったため、多くの通院者にも影響が生じた。

本事例は「Lockbit2.0」と呼ばれる攻撃者グループによるものと報じられている。システムログが攻撃者によって消去されていたため、攻撃者やウイルスの侵入経路は明らかになっていないが、同病院では脆弱性のあるVPN製品をテレワークで使用していたと報道されており、VPN製品を起点に不正アクセスされて「侵入型ランサムウェア攻撃」と「二重の脅迫」の被害に遭った可能性がある。

(b) 国内企業の被害事例

大手製粉会社である株式会社ニップンは、2021年7月9日に公表したシステム障害について、サイバー攻撃による被害であったことを2021年8月16日に公表した[※50]。それによると、2021年7月7日未明から同社グループの大部分のサーバ及び一部の端末に対し、同時多発的にデータが暗号化されるサイバー攻撃が発生したという。また、同社サーバへの不正アクセスにより、企業情報及び個人情報が一部流出した可能性があるとのことだ。同社では事業継続計画を策定していたが、災害時や単体のシステム障害を想定しており、本件のように同時多発的な攻撃を受けることは想定外だったとしている。

同社ではバックアップデータも暗号化されたため、サーバの早期復旧が難しく、通常は財務システムに自動入力される帳票を手作業で作成することになった。また、被害状況の調査、全面的なネットワーク環境の見直し、サーバの再構築等に時間を要することから、2021年度の第1四半期及び第2四半期の決算をそれぞれ延期せざるを得ない状況となった。

本事例は状況から「侵入型ランサムウェア攻撃」及び「二重の脅迫」、もしくはそれに類する攻撃を受けた可能性がある。また、同時多発的に全部または一部のデータを暗号化されたことから、攻撃者が1台ずつランサムウェアに感染させたとは考えにくい。ドメインコントローラのような管理サーバ経由でランサムウェア感染等が行われた可能性も考えられる。

(3) 侵入型ランサムウェア攻撃の手口

前述の被害事例からも分かるように、「侵入型ランサムウェア攻撃」は企業・組織にとって脅威である。ここではその手口について紹介する。

「侵入型ランサムウェア攻撃」は、次の(a)～(e)の五つのステップに分けられる。

(a) ネットワークへの侵入

「侵入型ランサムウェア攻撃」は、攻撃者が企業・組織のネットワークへ侵入するところから始まる。ネットワークへの侵入手口として次のようなものがある。

- ウイルスメールによる侵入
  攻撃者は、企業・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。受信者が不用意に添付ファイル等を開くことで、遠隔操作ウイルス等に感染させられ、パソコンが乗っ取られる。攻撃者は、そのパソコンを足掛かりとして組織内ネットワークへ侵入する。
- インターネットを経由した侵入
  攻撃者は、企業・組織がインターネット上に公開しているリモートデスクトップサービスやVPN製品を調査し、アクセス制御、認証に関する設定、パスワードの強度が不十分であれば、認証を突破して侵入する。
- 脆弱性を悪用した侵入
  攻撃者は、企業・組織が使用しているVPN製品等に残存する脆弱性を悪用して侵入する（「1.2.5 (1) VPN製品の脆弱性を対象とした攻撃」参照）。

(b) ネットワーク内の侵害範囲拡大

攻撃者は、企業・組織のネットワークへの侵入に成功した後、データの窃取やランサムウェアの感染範囲を広

げる目的で、ネットワーク内で侵害範囲拡大を行う。標的型攻撃同様、ネットワーク構成の把握や管理者権限の奪取を行い、これらの情報を基にして、機微情報等が保存されているパソコンやサーバ、ドメインコントローラ等の管理サーバ、バックアップ用のサーバ等に侵入すると考えられる。ドメインコントローラの一種である Active Directory サーバを掌握されると、グループポリシーによるウイルスの配信が可能となるため、組織内のパソコンやサーバのデータが一斉に暗号化される危険性がある。

(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。遠隔操作ウイルスを使用する等、攻撃者自身の操作によって、データの探索・収集、攻撃者のサーバやクラウドストレージへのアップロード等が行われる。

(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企業・組織のデータをランサムウェアで暗号化し、事業継続に関わる重要なシステムの停止を狙う。また、バックアップデータ等による業務復旧を妨害するため、「1.2.2 (2) ランサムウェア攻撃の被害事例」のように、ネットワーク経由で到達可能であれば、それらのデータも暗号化する可能性がある。

データを暗号化する際に OS の標準機能を使って暗号化する等、セキュリティ製品では検知されない機能を悪用した事例もある。例えば、Windows OS の標準機能である BitLocker を悪用してディスク全体を暗号化する事例が確認されている※51。

(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。公開方法としては、攻撃者がインターネットやダーク Web 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）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、被害者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。

身代金の交渉には電子メールのほかに、攻撃者が特定サイト内のチャットで個別にやり取りを要求する事例もある※52。

(4) 広く多数のコンピュータを狙うランサムウェア攻撃の手口

「広く多数のコンピュータを狙うランサムウェア攻撃」も依然として確認されており、感染させる手口は以下の (a) ～ (f) の六つが考えられる。なお、これらはランサムウェアに限らず、他のウイルスの感染経路となる可能性がある。

(a) ばらまき型メールによる感染

ばらまき型メールを介して、添付ファイルを開封させる方法や、メール本文の悪意のある URL リンクへ誘導し、「(b) Web サイトからの感染」の手口を使用する方法により、ランサムウェアに感染させる。

(b) Web サイトからの感染

悪意のある Web サイトからダウンロードしたファイルの実行によって感染させる。また、悪意のある Web サイトだけでなく、企業の正規の Web サイトが改ざんされて感染源となる場合もある。

(c) 脆弱性の悪用による感染

更新されていない端末等の OS の脆弱性を悪用し、リモートコードの実行や遠隔操作等で感染させる。また、悪意のある Web サイトにアクセスした際に、端末のソフトウェアの脆弱性を調査して攻撃する「エクスプロイトキット」というツールによって、ランサムウェアに感染させる※53。

(d) ワーム機能による感染

LAN に接続された端末にワーム（自己複製）機能を持つランサムウェアが感染すると、ワーム機能によりネットワークを介して他の端末にもランサムウェアを感染させる。

(e) 不正アプリによる感染

ゲームやセキュリティソフトを装った偽のアプリ（不正アプリ）のインストールによってランサムウェアに感染させる。パソコンだけでなく、スマートフォンやタブレットもランサムウェア感染のリスクがある。

(f) USB メモリ経由による感染

攻撃者が用意した USB メモリからランサムウェアに感染させる。例えば、攻撃者が差出人を偽装した郵送物に USB メモリが入っており、その USB メモリを接続した端末がランサムウェアに感染した事例がある※54。

(5) ランサムウェア攻撃への対策

ここではランサムウェア攻撃に対して、特に重要と考えられる対策について説明する。

(a) セキュリティソフトの導入

セキュリティソフトの導入は「侵入型ランサムウェア攻撃」及び「広く多数のコンピュータを狙うランサムウェア攻撃」双方で有効である。新しいウイルスを検知・駆除するために、セキュリティソフトは最新の状態に保つことも重要となる。ただし、「侵入型ランサムウェア攻撃」では、使用されるウイルスが標的の企業・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しにくい可能性もあるため、他の対策も併用することが望ましい。

(b) 攻撃メール対策

攻撃メール対策は、「侵入型ランサムウェア攻撃」及び「広く多数のコンピュータを狙うランサムウェア攻撃」双方で有効である。攻撃メール対策には、メールのフィルタ機能や、セキュリティ装置等を用いて不審なメールの検知・隔離を行うシステムによる対策や、従業員への教育、啓発、訓練による対策等がある。また、メール利用者一人ひとりが、「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が大切である。

(c) 不正アプリ対策

「広く多数のコンピュータを狙うランサムウェア攻撃」で使われる不正アプリは、主に非公式なアプリストアから配布される。改ざんされた Web サイト等では「ソフトウェアアップデート」や「システムエラー」の画面を表示して非公式のアプリストアへ誘導するため、これらの表示が出た場合は、ブラウザを閉じることで対処する。また、公式のアプリストアにも不正アプリが紛れ込んでいる場合があるため、注意が必要である。提供元が不明な信頼できないアプリのインストールをしないことが大切である。

(d) 脆弱性対策

脆弱性を悪用したウイルス感染やネットワークへの侵入を防ぐために、パソコンやサーバの OS 及び利用ソフトウェア、ネットワーク機器のファームウェア等を常に最新の状態に保つことは「侵入型ランサムウェア攻撃」及び「広く多数のコンピュータを狙うランサムウェア攻撃」双方で有効である。インターネットを経由して企業・組織内のネットワークに接続するための VPN 装置が攻撃者によく狙われるため、企業・組織では特に注意が必要である。また、脆弱性が公開されてから、その脆弱性が悪用されるまでの期間が短くなっていることから、公開された脆弱性に迅速に対応できるよう体制や計画を整えておくことが大切である。

(e) 企業・組織の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ことから始まる。そのため、次のような侵入対策を行うことが重要である。

- 攻撃対象領域の最小化
  インターネットからアクセス可能な、意図的に公開するサーバやネットワーク機器等を最小限にするとともに、アクセス可能なプロトコルやサービスも最小限にする。また、誤ってインターネットに公開している機器等がないか確認を行う。更に、それらの機器が乗っ取られる可能性を考慮し、そこからアクセス可能な範囲を限定する。例えば、不用意にリモートデスクトップサービスをインターネット上に公開しない、業務に必要なサーバ等をインターネット上に公開する場合は、どの機器を公開しているか等の管理を行う、といった対策が挙げられる。
- アクセス制御と認証
  企業・組織外からアクセス可能な機器等を最小限にした上で、それらが攻撃者に不正に操作されないよう、適切なアクセス制御と認証を行う必要がある。例えば、運用上、機器へのアクセスが国内からのみであれば、海外の IP アドレスからのアクセスを遮断するといった対策が考えられる。また、多要素認証のような強固な認証方式を使用して、認証を突破しにくくすることや、アクセスや認証のログを取得、監視して、不審な行為や攻撃の検知を試みることも有効である。
- 拠点間ネットワークのセキュリティ強化
  ランサムウェア攻撃に限らず、自組織で複数の拠点をネットワークで接続している場合、例えば十分にセキュリティ対策ができていない防御の弱い海外拠点から侵入され、組織の中枢が侵害される場合がある（「1.2.1 (1) (b) 国内企業の海外拠点を狙った未公開の脆弱性を悪用した標的型攻撃」参照）。必要に応じ、拠点間のアクセス制御の強化も検討する。

(f) ネットワーク内の侵害範囲拡大への対策

「侵入型ランサムウェア攻撃」を受けた場合、企業・

組織のネットワーク内における不審な活動を検知し、攻撃の早期発見と対応につなげる。統合ログ管理、内部ネットワーク監視、エンドポイント監視といった仕組み（製品等）を活用し、ネットワークのスキャン、通常発生しない不正な通信や認証の試行、無許可のユーザアカウント作成等の操作、無許可のプログラム設置・実行、イベントログの削除、シャドウコピーの削除等の攻撃者の活動を検知する。

被害者は、データの暗号化やシステム停止を受けて初めて、攻撃を受けていることを認識する場合があるが、データの暗号化等がされてからの対策・対応は困難であるため、より早期の検知を可能にすることが望ましい。

(g) バックアップからの復旧

「侵入型ランサムウェア攻撃」への対策として重要なことは、データの保護のみならず、「システムの再構築を含めた復旧計画」を事前に策定し、バックアップからの復旧を可能にしておくことである。「1.2.2 (2) ランサムウェア攻撃の被害事例」にもあるように、企業・組織のパソコンやサーバ等が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。こうした状況に備え、事業継続に重要なデータやシステムのバックアップデータをオフラインで管理するほか、必要に応じて業務継続やシステムの再構築に必要なリソース等を考慮した復旧計画を策定しておくことが大切である。

(h) 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）[※55] 等の活用や、ネットワーク分離が挙げられる。IRM を活用し、データが窃取されても被害を限定的な範囲に留める。また、ネットワーク分離では、例えば、メールの送受信や 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。こうすることで、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。ただし、ネットワーク分離は運用コストや利便性に著しい影響があるため、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必要がある。

(i) インシデント対応

ランサムウェア攻撃の被害を受けてしま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、「侵入型ランサムウェア攻撃」は、侵入の手口が標的型攻撃と同様のため、対応も全体的に標的型攻撃と同様となる（「1.2.1 (5) (b) 組織としての対応体制の強化」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[※56] を公開しているため、参照いただきたい。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[※57] についても公開しているため、こちらも参照いただきたい。

ランサムウェア攻撃のインシデント対応において、留意すべき点として、「ステークホルダーとのコミュニケーションができる体制作り」がある。ランサムウェア攻撃では、一般のインシデントと異なり、業務停止や顧客・取引先の情報漏えいが発生し、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。ステークホルダーとの適切で素早い連絡・調整を含む、経営層を含めた体制作りが必要である。

1.2.3 ビジネスメール詐欺（BEC）

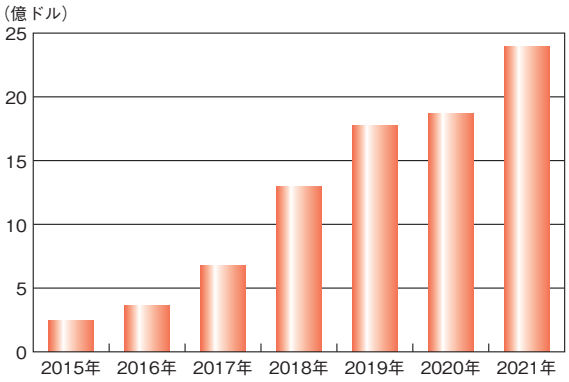
ビジネスメール詐欺（BEC：Business Email Compromise）は、巧妙な騙しの手口を駆使した偽のメールを企業・組織に送り付け、従業員を騙して送金取り引きに関わる資金を詐取する等の金銭被害をもたらすサイバー攻撃である。偽のメールを送るための前段階として、企業の従業員や取引先のメールアカウント情報を狙うため、フィッシング攻撃や情報を窃取するウイルスが使用されることもある。

本項では、2021 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

FBI のインターネット犯罪苦情センター（IC3：Internet Crime Complaint Center）が 2022 年 3 月に公開した年次報告書[※58] によると、2021 年度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 1.3 倍の約 23 億 9,600 万ドル（未遂を含む）となっている。また、2015 年から 2021 年までに発生した被害総額の推移をグラフで表すと、被害額が増加傾向にあることから、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 1-2-4）。

また、トレンドマイクロ社の報告によれば、同社のセキュリティ製品がビジネスメール詐欺と判定・検出したメール



■図 1-2-4　ビジネスメール詐欺の被害総額推移
（出典）IC3 年次報告書を基に IPA が作成

の件数が、2021 年の 1 月から 9 月にかけて徐々に増加しているという。特に 7 月から 9 月においては、検出数が約 5 万件と、新型コロナウイルス拡大前の 2019 年の同時期と比較して、約 3.5 倍になったとしている※59。また、国際的なフィッシング対策の非営利団体である APWG の報告によると、2021 年 5 月に、給与振込口座を変更させる手口が電信送金を利用する手口を上回り、増加したという※60。

一方で、世界の法執行機関等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表されている。2021 年の 6 月から 9 月までの 4 ヵ月間に行われた「HAECHI-II」と呼ばれる国際的な取り締まりでは、ビジネスメール詐欺等に関わっていた 1,003 人を逮捕し、金銭の詐取等に悪用されていた約 2,350 件の口座を凍結させ、約 2,700 万ドルの資金を押収することに成功したという※61。また、「情報セキュリティ白書 2021」の「1.2.3（1）ビジネスメール詐欺の被害状況」で紹介した、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等が行った共同調査による逮捕事例に関連し、2022 年 1 月、同じ犯罪組織のメンバーと見られる 11 人の容疑者が新たに逮捕された。逮捕された容疑者の一人は、自身のパソコン上に攻撃対象と思われる 80 万件以上のアカウント情報を所持していたという※62。そのほか、米国司法省（U.S. Department of Justice）の発表※63 によれば、ビジネスメール詐欺等を行い、少なくとも 100 人の被害者から 1,700 万ドル以上の金銭を詐取した 33 人の容疑者が逮捕されたほか、欧州においても、ビジネスメール詐欺等に関わっていたとされる 106 人の容疑者が逮捕されている※64。

（2）2021 年度に報道された事例の概要

2021 年度においても国内外で金銭被害に遭った事例が多数確認されている。国内で発生した事例としては、大手眼鏡販売チェーンの持株会社である株式会社ビジョナリーホールディングスの子会社の株式会社 VISIONIZE に対し、取引先関係者をかたった人物から仕入代金の送金を促すメールが送られ、当該子会社が約 1 億円を送金してしまったという※65。また、国内企業の海外子会社で発生した事例では、加賀電子株式会社の海外子会社が悪意の第三者による虚偽の送金指示に騙され、約 5 億円の資金を流出させてしまったという※66。海外で発生した事例では、韓国の航空関連企業である韓国航空宇宙産業に対し、取引先企業のメールアカウントを乗っ取った攻撃者が担当者になりすまして、口座を変更したという旨の偽メールを送ってきたという。当該企業の担当者は、そのメールを取引先企業からの正規のメールだと思い込み、約 16 億ウォンを送金してしまったという※67。

一方で、詐取された金銭を回収できた事例もあった。米国ミネソタ州レッドウッドフォール市で起きた事例では、同市が消防車の売買に関する担当者をかたった攻撃者とやり取りし、約 120 万ドルを送金してしまったが、調査の過程で資金が見つかったため、同市へと返還されることになったという※68。

（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 月に続き、2020 年 4 月に第三報として注意喚起を行った。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。

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 2021 年度に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 1 件（表 1-2-1 の項番 3）については、金銭的被害が確認されている。残り 8 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、IPA が 2021 年度に公開したビジネスメール詐欺事例の中から特筆すべき表 1-2-1（次ページ）の項番 3 と 8 について紹介する。

項番	事例概要	被害の有無	備考
1	2021 年 1 月、国内企業の取締役になりすました攻撃者から、海外グループ企業の担当者に対して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［2021 年 1 月～ 3 月］[※69]」に記載
2	2021 年 2 月、取引先ではない海外企業の担当者になりすました攻撃者から、国内企業の担当者に対し、偽の口座への支払いを要求するメールが送られた。	なし	同上
3	2021 年 4 月、国内企業の海外関連企業（請求側）と、海外取引先企業（支払側）との取り引きにおいて、請求側企業の担当者になりすました攻撃者から、偽の口座への振り込み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	「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2021 年 4 月～ 6 月］[※70]」に記載
4	2021 年 5 月、国内企業の役員になりすました攻撃者から、当該企業の複数の担当者に対して、同一内容の偽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	同上
5	2021 年 6 月、国内企業の役員になりすました攻撃者から、当該企業の複数の担当者に対して、英語と日本語で書かれた偽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	同上
6	2021 年 8 月、国内企業の海外関連企業の役員になりすました攻撃者から、当該企業の担当者に対して、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［2021 年 7 月～ 9 月］[※71]」に記載
7	2021 年 9 月、国内企業（支払側）と、海外取引先（請求側）との取り引きにおいて、請求側企業の担当者になりすました攻撃者から、偽の口座への振り込み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。	なし	「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2021 年 10 月～ 12 月］[※72]」に記載
8	2021 年 10 月、国内企業の代表取締役になりすました攻撃者から、当該企業の複数の役員に対して、約 2 時間の間に 17 通の偽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	同上
9	2021 年 10 月、国内企業の役員になりすました攻撃者から、当該企業の人事部門の担当者に対して、ビジネスメール詐欺が試みられた。	なし	同上

■表 1-2-1　IPA が情報提供を受け 2021 年度に公開したビジネスメール詐欺事例の概要

また、「情報セキュリティ白書 2020」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、注意喚起の第三報の「『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、多数の情報提供を受けたため、それぞれの概要を紹介する。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。

(a) 偽の口座への振り込みを要求する攻撃事例

本事例は、2021 年 4 月、J-CSIP の参加組織（国内企業）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）との間で取り引きを行っている中、A 社の担当者になりすました攻撃者から、偽の口座への振り込みを要求するメールが送られたものである。B 社の担当者が攻撃者の用意した偽の口座へと送金を行ってしまったため、金銭的な被害が発生した。

この手口は、IPA が 2017 年 4 月に公開した注意喚起[※73] で紹介しているビジネスメール詐欺の五つのタイプのうち、「タイプ 1:取引先との請求書の偽装」に該当する。

今回の事例では、やり取りされたメールはすべて英文であり、詐欺の過程において、次の手口が使われた。

- A 社と B 社のやり取りへ介入
- 正規のメールアドレスに似せた偽の詐称用ドメインの悪用
- メールの転送設定によるメールの盗聴

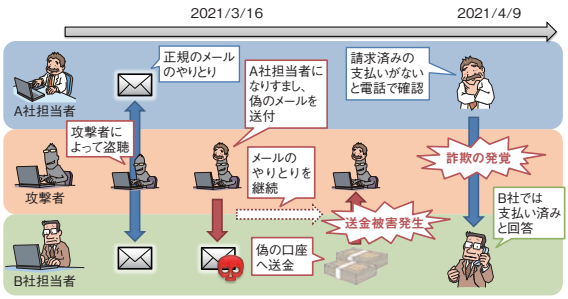
(ア) A 社と B 社のやり取りへ介入

A 社（海外関連企業）と、B 社（海外取引先）との間で、取り引きに係るビジネスメールをやり取りしている中、2021 年 3 月 16 日に攻撃者から B 社の担当者へ偽のメールが送られた。その後、B 社担当者と攻撃者間で複数回メールのやり取りを継続したと見られるが、詳細は情報提供外のため不明である。そのやり取りの中で、B 社担当者は攻撃者が用意した偽の口座へ支払いをしてしまったため、金銭的被害が発生した。

攻撃に関係したメールのやり取りを図 1-2-5（次ページ）に示す。

その後、2021 年 4 月 9 日に A 社から B 社へ、請求中の支払いがないため連絡をしたところ、B 社からは支払い済みであると回答を受けたことで事案が発覚した。B 社では偽の口座への振り込みの取り消し対応を行っており、当該口座は凍結されたとのことだが、送金した資金が回収できたかは不明である。

なお、本件で攻撃者が用意した偽の口座は、同時期



■図 1-2-5　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［2021年４月～６月］」

に本件とは別のビジネスメール詐欺と思われる詐欺行為でも悪用されていたことが判明している。攻撃者が、被害者を騙して振り込ませる口座を、複数の犯罪に使い回していることは推測されていたが、実際に複数の会社に対するビジネスメール詐欺が関係していたということが本事例をとおして確認された。

ビジネスメール詐欺にて確認した偽の口座情報を、銀行や警察等と連携することで、攻撃者の口座を凍結し、別の企業等に行われているビジネスメール詐欺の被害を未然に防げる可能性がある。攻撃者の口座が判明した際は、速やかに銀行や警察等へ連絡することを検討いただきたい。

（イ）正規のメールアドレスに似せた偽の詐称用ドメインの悪用

攻撃者からＢ社の担当者へ送られた偽メールでは、Ａ社の正規のドメインに似通った「詐称用ドメイン」がメールの送信に使用されていた。詐称用ドメインは、最初の攻撃メールが送られた当日（2021 年３月 16 日）に新規に取得され、図 1-2-6 に示すように、正規のドメイン名を１文字変更したものであった。

【本物のメールアドレス】alice @ abccompany-a . com
【偽物のメールアドレス】alice @ abcccompany-a . com
（「c」を一文字追加）

※実際に悪用されたものとは異なる。

■図 1-2-6　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［2021年４月～６月］」

（ウ）メールの転送設定によるメールの盗聴

攻撃者は何らかの方法でＢ社の Microsoft 365 のメールアカウントへ不正アクセスし、正規のＡ社の担当者から送られたメールを攻撃者の元へ転送するように設定していた。この設定を行うことで、攻撃者はＢ社が利用していたメールサービスに定期的にログインすることなく、Ａ社とＢ社のやり取りを盗み見ることが可能となっていたと見られる。

（b）経営者をかたる日本語の攻撃事例

本事例は、2021 年 10 月、J-CSIP の参加組織（国内企業）の複数の役員に対し、同社の代表取締役になりすました攻撃者から、約２時間の間に 17 通の偽のメールが送られたと情報提供があったものである。

攻撃者から送られた偽のメールは日本語であり、機密事項について助けが必要だという内容で、受信者に返信を依頼するものであった。メールの下部には実在する日本の弁護士事務所の弁護士から連絡があったように見せかける偽の内容が記載されていた。

本事例で、攻撃者から送られたメールを図 1-2-7 に示す。

■図 1-2-7　実在する代表取締役と弁護士を詐称する日本語のメール
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2021年 10 月～ 12 月］」

本メールの送信者のメールアドレスには、日本の金融庁のドメインに似た偽のメールアドレスも記載されており、この偽のメールアドレスへ返信されるように細工されていた。また、同報先（CC）には、弁護士のメールアドレスをかたった偽のメールアドレスが設定されており、あたかも

弁護士にも同報されているかのように見せかけていた。

このメールについては、IPA が 2018 年 8 月に公開した注意喚起の続報※74 のレポート事例 1 と同じ手口であり、継続して類似した攻撃が行われているものと推測される。

普段英語のメールでやり取りを行わないような企業や組織であっても、日本語で書かれた偽のメールが着信する可能性があるため、引き続き注意が必要である。

(c) CEO を詐称する一連の攻撃

2021 年においても、CEO（Chief Executive Officer）詐欺について継続して情報提供があった。更に IPA で J-CSIP 外の情報等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、これら二つの CEO 詐欺について説明する。

- 複数組織へ行われた CEO を詐称する一連の攻撃
- 「日本語化」された CEO 詐欺の攻撃

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、2021 年に 34 件の情報提供を受け、これまでに 207 件のメール検体を入手している。本攻撃は、2019 年 7 月以降継続して観測しており、国内外の複数の組織を対象として行われた痕跡を確認している。メールの件名や内容は時期ごとに変化が見られるが、メールのヘッダ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が公開しているレポートと同様の手口であることを確認している※75。

「日本語化」された CEO 詐欺の攻撃については、2021 年に 15 件の情報提供を受け、これまでに 68 件のメール検体を入手している。本攻撃は、2019 年 11 月以降継続して観測しており、国内外の複数の組織を対象として行われた痕跡を確認している。メールの件名や内容は一部に変化が見られるが、ほぼ同じ内容のメールであり、メールのヘッダ情報や、「SendGrid」や「SMTP2GO」というメールサービスを使用する場合がある等類似する点があり、一連の攻撃は同一の攻撃者によるものと推測している。

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を確認している。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。

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を使って被害者を騙そうとする等、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

ビジネスメール詐欺への対策を以下にまとめる。日頃からビジネスメール詐欺への意識を高め、組織内の送金チェック体制や監視体制、被害に遭ったときの迅速な対応体制を整えておくことが重要である。

また、JPCERT/CC や株式会社マクニカ、PwC の報告書等も、対策・対応について記載されており、そちらも活用いただきたい※76。

(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り引きだけでなく、グループ会社同士の取り引きにおいても発生している。このため、海外関連企業を含む全グループ企業の全従業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巻き込まれた場合は、取引先や、警察、金融機関へ報告し、同様の攻撃に対する注意喚起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)電子署名等によるなりすまし防止

ビジネスメール詐欺は、メールのやり取りにおいて本物の担当者になりすますことで攻撃を成立させる。そのため、取引先と連携した対策として、請求書等の重要情報をメールで送受信する際は電子署名を付ける等の手段で、なりすましを防止する対策が有効である。

(c)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（役員等権威ある立場からの通常の手順とは異なる支払い依頼や、企業間取り引き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。

(d)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、偽のメールだと気付かず返信してしまった場合でも、送信先や返信先に設定されているメールアドレスに注意していれば、攻撃と見抜ける可能性があ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、従業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）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）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）と返信先（Reply-Toヘッダ）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。

(e)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、メールサーバやメールアカウント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（旧称、G Suite）等のようなクラウド型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※77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、2021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によると、2021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540万回で、前年同期と比較して11%増加した※78。2020年以降、DDoS攻撃は急激に増加しているが、これは、新型コロナウイルスの世界的蔓延とロックダウン等の影響に

より、多くの日常的な活動がオンラインに移行したことで、潜在的な攻撃対象が増加したことが原因である可能性が高いとされる※79。

ここでは、2021 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、リクエストよりもレスポンス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アドレスに偽装したリクエストを大量に送信することで、増幅されたレスポンスが攻撃対象のアドレスに宛てて送信される。攻撃対象は、大量のデータを受信することになり、処理能力の限界を迎え、サービスのパフォーマンス低下や停止を起こす。このような DDoS 攻撃は「リフレクション攻撃」と呼ばれる。

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)※80を用いて通信を行うサービス (以下、UDP サービス) を悪用した攻撃が多く観測されている。UDP サービスを悪用した攻撃では、UDP の以下の三つの特徴が悪用される。

①要求パケットの送信元 IP アドレスを確認しない。このため、送信元を偽装しやすい。
②要求パケットの長さよりも応答パケットの長さが大きくなる増幅効果(Amplification)がある。
③ UDP サービスを提供するサーバ(以下、UDP サーバ)へ行われたリクエストは、応答パケットとして、送信元ホスト (攻撃においては送信元に偽装された攻撃対象のホスト)へ反射(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難しく、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、インターネット上からアクセス可能な UDP サーバへの通信そのものは正常であるため、攻撃が行われていることを把握し対応を行うには、後述の「1.2.4 (3) (b) 攻撃に加担しないための対策」が必要となる。

UDP サービスを悪用したリフレクション攻撃は、2021 年も定常的に確認されており、11 月には、Microsoft Azure のアジアユーザを対象とした、3.47Tbps(テラビット／秒)という過去最大規模の DDoS 攻撃が行われた※81。この事例では、大規模な DDoS 攻撃の兆候を検知した時点で、その攻撃に対する緩和策を既に Microsoft 社が構築・実施していたために被害は発生しなかったが、このようなリフレクション攻撃の頻度と規模は近年ますます増加している。

(b) オリンピック期間中に確認された DDoS 攻撃

CDN (Content Delivery Network)※82 事業者により、東京 2020 オリンピック・パラリンピック競技大会の競技開始後の日本国内への DDoS 攻撃の件数が、通常時の 10 倍以上に増加したとする調査データが公開された※83。

オリンピック・パラリンピックの開催中は、開催国へのサイバー攻撃が集中することがこれまでも観測されており、東京 2020 オリンピック・パラリンピック競技大会でも、攻撃が集中することが予測されていた。本大会では、組織委員会や関係機関が、開催前から攻撃への対策を強化すると宣言する等、事前に対策に乗り出していたこともあり、大会の開催期間中に運営に支障が出るような被害は生じなかった。

(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、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 サーバで構成されている。攻撃者が C&C サーバを介して、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が一斉に攻撃を行う。ボットネットを構成する機器のほとんど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させられたりした結果、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、アップデートを繰り返すことで、最新の悪用手法等を取り入れ、様々なターゲット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。

2021 年 6 月末ごろから、IoT 機器を悪用して DDoS 攻撃を仕掛ける「Mēris」と呼ばれるボットネットが新たに観測された※84。Mēris による攻撃トラフィックは、2016 年に猛威を振るった IoT マルウェアである Mirai※85 にて観測されたものの約 3 倍規模に相当し、Cloudflare, Inc. では 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※86。

このようなボットネットは、攻撃ツールとして、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、ISP 事業者が提供する DDoS 攻撃対策サービスやセキュリティベンダ等が提供する 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) 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といった対策が必要である。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といった対策も推奨する。以下に、具体的な対処方法を挙げる。

- 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等の機器や、自組織が外部で管理している 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、攻撃の踏み台となっ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

2021 年度は、2020 年度に引き続き 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、多数の IoT 製品に影響があるとされる脆弱性も報告された。

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。

2021 年度は、新型コロナウイルス感染拡大防止のため、2020 年度に引き続きテレワークが強く推奨された影響もあり、VPN 製品の脆弱性を悪用した攻撃数が依然として高い水準で推移した※87。また、VPN 製品の新

たな脆弱性が相次いで発見され、脆弱性が解消されていない製品を狙った攻撃も多数報告された。

(a) 攻撃事例

2021 年 2 月 に、SonicWall, Inc. 製 SonicWall SMA100 シリーズの SSL-VPN 機能に関して、SQL インジェクション※88 の脆弱性（CVE-2021-20016※89）が公表された。

この脆弱性は、SSL VPN ポータルに存在する。攻撃者は、細工したリクエストをポータルに送信することで、認証を必要とせずに SQL 文を実行し、認証やセッションに関連する情報にアクセスできる可能性があった。

2021 年 1 月 22 日、同社は当該脆弱性を悪用したと思われる標的型攻撃を観測し、1 月下旬より調査を進めていることを公表した。当該脆弱性が悪用された事例として、FiveHands ランサムウェアへの感染等がある※90。

また、2021 年 5 月に Pulse Secure, LLC. は、同社の VPN 製品である Pulse Connect Secure に発見された複数の脆弱性を解消する定例外の修正プログラムを公開した※91。解消された脆弱性のうち、CVE-2021-22893※92 については、悪用による被害が確認された。

この脆弱性を悪用されると、認証されていない攻撃者により、解放済みメモリ使用の脆弱性（Use After Free）を悪用され、当該製品上のライセンスサーバの Web サービスを経由して任意のコードを実行される可能性がある。また、認証を回避され、製品上に Web シェル※93 を設置されることで、システムが永続的に侵害される可能性がある。

これらの VPN 製品は、脆弱性を解消したバージョンのソフトウェアが配布されるまでに数週間から 1 ヵ月程の期間を要しており、脆弱性情報の公開後、当該脆弱性を悪用した攻撃の事例が報告されている。

これは、脆弱性情報の公開当初はソフトウェアの修正プログラムが公開されていなかったことに加え、修正プログラムを適用したとしても、適用前に脆弱性を悪用され、認証情報を不正に取得されていた場合、攻撃者が窃取した認証情報により不正アクセスできてしまうことが要因として挙げられる※94。

(b) 脆弱性を狙った攻撃への対策

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ため、新たな脆弱性が公開された際は、迅速な対応が求められる。

そのためには、事前の準備が重要である。自らが保有または利用するシステムについて、構成管理を適切に行い、システムを構成するソフトウェア等の脆弱性に関する情報収集を日々行う必要がある。また、事前に対策の実施手順を整えておき、脆弱性の対応を遅延なく着実に実施することが重要である。

対策の実施手順として、以下に示す内容をあらかじめ定めておくことを推奨する。

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

このような実施手順の準備に加え、侵害されている痕跡が存在するか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、近年の VPN 製品の需要の高まりから、古い製品を利用する必要に迫られることも考えられる。その際は、ベンダ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。

(2) Microsoft 製品の脆弱性を対象とした攻撃

2021 年度も 2020 年度に引き続き、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 Exchange Server の脆弱性を狙った事例を紹介する。

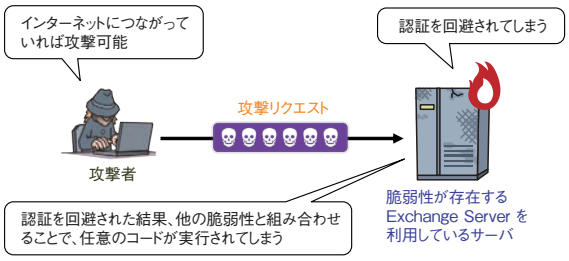
(a) 攻撃事例

Microsoft Exchange Server は、Microsoft 社が開発したメールサーバ及びグループウェアである。

ここでは、2021 年 3 月に公開された「ProxyLogon」と呼ばれる脆弱性（CVE-2021-26855※95 等）と、同年 8 月に公開された「ProxyShell」と呼ばれる脆弱性（CVE-2021-34473※96 等）を悪用した攻撃について解説する。

- ProxyLogon の脆弱性

  この脆弱性は、Exchange Server のプロキシアーキテクチャに認証の不備があることに起因する。攻撃者は、脆弱性が存在する Exchange Server を導入したサーバの 443 番ポートに対して細工したリクエストを送信する。脆弱性が存在すると、認証を回避して管理者になりすますことが可能となり、他の脆弱性と組み合わせることで、任意のコードが実行される（次ページ図 1-2-8）。
- ProxyShell の脆弱性



■図 1-2-8　ProxyLogon の脆弱性を悪用した攻撃イメージ

ProxyShell の脆弱性も、ProxyLogon の脆弱性と同様に、クライアントアクセスサービスに認証の不備があることに起因する。当該脆弱性により、攻撃者が標的となる Exchange Server に対し、細工したリクエストを送信することで、バックエンドサーバの任意の URL へアクセスできる。また、他の脆弱性と組み合わせることで、任意のファイルを上書きして Web シェルを設置すること等ができるとされている。

2021 年 1 月、ProxyLogon を悪用され、攻撃対象のサーバで認証を回避し、メール情報を窃取される事例が報告されている※97。

(b) 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、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。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) 脆弱性を狙った攻撃への対策」参照）。

(3) IoT 製品を対象とした攻撃

2021 年度も、多数の IoT 製品に影響を与える脆弱性が公開されている。本項では、「NAME:WRECK」と呼ばれる脆弱性を紹介する。

(a) 多数の IoT 製品に影響する脆弱性

2021 年 4 月 12 日、米国のサイバーセキュリティ企業である Forescout Technologies, Inc. 及びイスラエルのサイバーセキュリティ企業である JSOF Ltd. より、「NAME:WRECK」と呼ばれるゼロデイ※98 の脆弱性群に関する情報が公開された※99。NAME:WRECK は、TCP/IP スタック※100 に DNS プロトコルのメッセージ圧縮機能を持つ FreeBSD や Nucleus NET 等の IoT 機器向けの OS やソフトウェアライブラリに発見された 9 個の脆弱性の総称である。これらの脆弱性が悪用された場合、攻撃者により、IoT 製品を経由して外部からネットワークに侵入され、ブロードキャストによって、ネットワーク内の脆弱性がある機器の制御を奪取されたり、サービス妨害等を引き起こされたりする可能性があるという。

当該製品は、医療機器や制御システム等の組み込み機器で広く利用されていることから、少なくとも 1 億台の機器が影響を受ける可能性があるとされる※101。

今後も、NAME:WRECK の脆弱性が解消されていない IoT 製品を狙った攻撃が発生する可能性があり、対策が必要である。

(b) IoT 製品を対象とした攻撃への対策

前述の NAME:WRECK のような脆弱性の存在を踏まえて、IoT 製品を安全に保つためには、以下の対策が必要となる。

- 製品開発者が行うべき対策
  - IPA や JPCERT/CC 等の各組織が公開している IoT 製品の開発ガイドライン等を基に、企画・設計等を含めたすべての開発工程で実施すべきセキュリティ対策を明確にする（ガイドラインについては「3.2.4 (1) IoT 関連セキュリティガイド等の改訂・新規発行」参照）。
  - 製品で使用する部品の調達に関し、契約等において脆弱性対処の項目を含める。
  - 製品出荷後に修正プログラムによりアップデートが実施できるように製品に更新機能等を組み込む。
  - 製品に関する脆弱性が発見・報告された場合、速やかに修正プログラムを公開する。
  - 安全に運用するための注意点等の情報を製品利用者に提供する。
- 製品利用者が行うべき対策
  - 製品開発者が提供する安全に運用するための注意点やアップデート方法等の情報を確認した上で利用する。
  - 攻撃者に脆弱性を悪用されるリスクを低減するため、製品を利用するにあたって問題がなければ、インターネットから直接 IoT 製品にアクセスできないようにする。
  - 脆弱性情報を収集する。具体的には、IPA が公開している「JVN iPedia※102」や、IPA から送付されるセキュリティ対策情報のメールニュース、製品開発者の Web サイトで公開される情報等を定期的に確認する。
  - 製品開発者が修正プログラムを公開した場合、速やかに修正プログラムを適用する。

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※103。2021 年においても、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、添付ファイルやメール本文中の URL を用いる手法が存在する。メールの添付ファイルには実行ファイル、脆弱性を悪用する Office 文書ファイル、Office アプリケーションのアドインファイル等を確認している。また、マクロ付きの Office 文書ファイル、これらのファイルを圧縮した形式のファイルについても継続的に確認している。ばらまき型メー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ため注意が必要である。

IPA では、2019 年、2020 年に日本国内で多くの感染被害が発生した「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（以下、Emotet のばらまき型メール）を、2021 年 11 月に再度観測した。Emotet のばらまき型メールは、2021 年 1 月に欧州刑事警察機構（Europol）により Emotet の攻撃基盤（ウイルスをばらまいたり、感染したマシンを操作したりするための機器等）がテイクダウン（停止）された※104 ため、世界中で 2021 年 2 ～ 10 月の間、確認されていなかった。しかし、Emotet のばらまき型メールが再度観測されたことから、攻撃者はテイクダウンされた攻撃基盤とは別の攻撃基盤を用意し、Emotet のばらまき型メールを送信している可能性がある。国内では、2022 年 2 ～ 3 月にかけて、企業・組織における Emotet 感染が急増していると報告されている※105。このほか、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は、2021 年をとおして観測されている。

本項では、2021 年度に国内で観測された日本語のばらまき型メールによる攻撃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、及び再送を装う手口

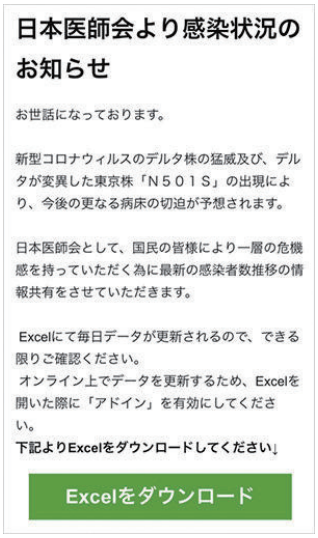
IPA では、正規のメールへの返信、転送、及び再送を装うばらまき型メール（以下、正規のメールへの返信等を装うメール）を観測している。このばらまき型メールでは、攻撃対象者が過去にメールのやり取りをしたことのある、実在する相手の氏名、メールアドレス、メールの内容等が流用され、その相手からの返信、転送、及び再送のメールを装っている。

この手口のばらまき型メールは 2018 年 11 月から観測されており※106、次の方法によってメールが送信される。

- ウイルスに感染した端末から窃取した情報を基に、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ばらまく方法※107。
- 攻撃者がメールアカウントへ不正アクセスし、そのメールアカウントで受信していた正規のメールへの返信等を装うメールをばらまく方法
- あらかじめ窃取したメール情報を用いて正規のメールへの返信等を装うメールをばらまく方法

(b) メール受信者の興味・関心を惹く題材を悪用する手口

IPA では、受信者の興味・関心を惹く題材をメールの件名・本文に記載するばらまき型メールを継続して観測している。2020 年 12 月にはクリスマスや賞与を題材と



■図 1-2-9　新型コロナウイルスを題材としたばらまき型メールの例
（出典）公益社団法人日本医師会「【注意喚起】日本医師会を騙る不審メールの流通について※108」

したばらまき型メールを、2021 年 1 月には緊急事態宣言を題材としたばらまき型メールを観測していた。その後、2021 年 7 ～ 10 月には請求書を題材としたばらまき型メールを、2021 年 9 月には図 1-2-9（前ページ）のように新型コロナウイルスを題材としたばらまき型メールを観測した。これらの手口から、攻撃者は日本国内のメール受信者の興味・関心を惹く題材を選んで継続的に攻撃を行っていると言える。

(c) 実在の組織をかたった手口

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 1-2-9（前ページ）や図 1-2-10 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を偽装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。

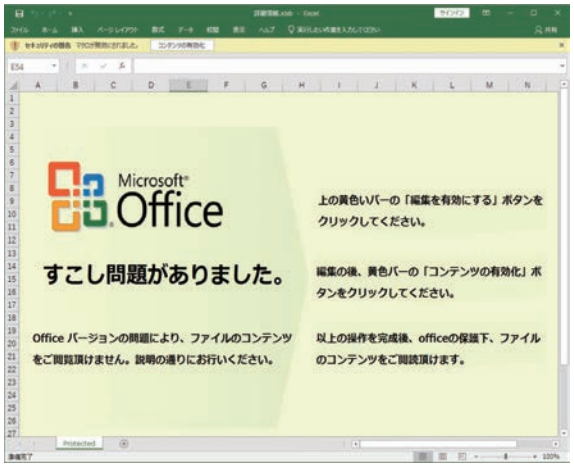
■図 1-2-10　実在する企業をかたるばらまき型メールの例

(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、マクロ付きの Word、Excel、PowerPoint といった Office 文書ファイル内の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。マクロ付き 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。2020 年 9 月まではこれらの記述は英語のみであったが、IPA では 2020 年 10 月以降、日本語で指示が記載された Word ファイルや Excel ファイルを確認している。2021 年 4 月にも図 1-2-11 に示すように、Excel ファイルを使用し、ウイルスに感染させようとするばらまき型メールを確認している※109。



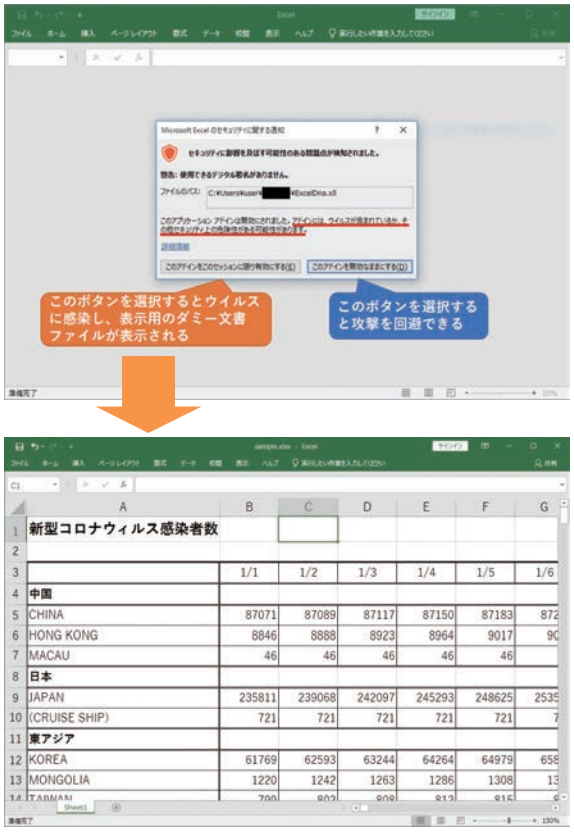
■図 1-2-11　日本語で記載されている Excel ファイルの例

(b) Excel アドインファイルを使用する手口

Excel アドイン（拡張子が .xll）のファイルを悪用する手口を確認している※110。この手口ではファイルを開くと、図 1-2-12（次ページ）のように、警告ウィンドウが表示される。警告ウィンドウで、利用者が「このアドインをこのセッションに限り有効にする」を選択すると、表示用のダミー文書ファイルが表示され、最終的にウイルスに感染する。

(c) 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 Word ファイルが出力され、利用者がそのファイルを開いて「コンテンツの有効化」ボタンをクリックすることでウイルスに感染する。添付ファイルが暗号化されていることから、メール配送中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、2021 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。



■図 1-2-12　Excel アドインのファイルを開いたときに表示される警告ウィンドウとダミー文書ファイルの例

(d) メール本文中の URL リンクを使用する手口

この手口ではメール本文中に URL リンクが記載されており、URL リンクをクリックしてアクセスすると、悪意のあるマクロ付き Office 文書ファイルや PDF 閲覧ソフトを装ったウイルスファイル等をダウンロードさせる Web サイトへ誘導される※111。Office 文書ファイルをダウンロードした場合、前述の「(a) マクロ付きの Office 文書ファイルを使用する手口」を用いてウイルスに感染させる。また、PDF 閲覧ソフトを装うウイルスファイルについては、脆弱性を悪用し更に別のウイルスに感染させることを確認している※112。URL リンク先は、攻撃者が用意したサーバである場合や、Microsoft OneDrive、Google Drive 等のクラウドストレージの場合もある。この手口は新しいものではないが 2021 年度も継続して使われており、引き続き注意が必要である。

(3) 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、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、添付ファイルを開くこと、及び本文中に記載されている 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へ報告・相談を行うことを推奨する。
- 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保護ビューの解除やマクロの有効化を行わない
  正規のものであると確信の持てない Word、Excel、PowerPoint 等のファイルを何らかの方法で入手して開いたときに、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 等の設定でマクロの自動実行を無効化する。業務等でマクロを使わないと分かっている場合にはマクロ機能自体を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、「1.2.1 (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。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いった組織的な取り組みのほか、システムの対策として、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。

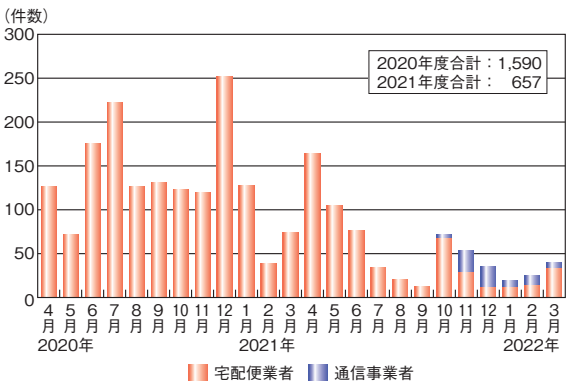
1.2.7 個人をターゲットにした騙しの手口

2021 年度は、手口の種類は増えてはいないが、手口の細かい部分で変化し続けているのが特徴と考えられる。

SMS（Short Message Service）の手口では、通信事業者をかたる SMS が出現した。一時期減少していた暗号資産を要求する脅迫メールの手口では、文面がより日本語らしくなったこともあり、本物と信じたという相談が増加している。Web からの騙しの手口では、2020 年度末から登場した Web ブラウザの通知機能を悪用する手口の相談が増加している。

(1) 変化が続く SMS の手口

2021 年度も、偽 SMS の手口に関する相談は継続して寄せられているが、従来の手口である宅配便業者をかたる SMS に加えて、通信事業者をかたった偽 SMS が登場した（図 1-2-13）。

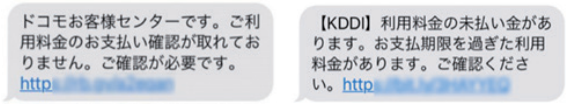


■図 1-2-13　偽 SMS に関する月別相談件数推移（2020～2021 年度）

これを受けて 2021 年 12 月、IPA では「安心相談窓口だより※113」に通信事業者をかたった手口の説明を追加し、注意喚起を行った。

(a) 通信事業者を装う SMS

2021 年 10 月ごろより、利用料金の支払いが確認できない等の偽の SMS 文面から URL をタップさせようとする手口の相談が多くなった。通信事業者は、当初、株式会社 NTT ドコモ（以下、NTT ドコモ）をかたっていたが、au（KDDI 株式会社）をかたるものも登場した（図 1-2-14）。



■図 1-2-14　通信事業者をかたる偽 SMS の例

(ア) 手口

この手口は、「利用料金に未払いがある」という通信事業者を装った SMS を送り付け、SMS 内のリンクから偽サイトへ誘導する。リンクをタップした後の手口は変化を続けている。以下は、2022 年 1 月時点の確認内容である。

偽サイトにアクセスしてしまうと、アクセスしたスマートフォンが Android OS 端末（以下、Android）であるか、iPhone や iPad 等の iOS 端末（以下、iPhone）であるかによって、この後遭遇する手口が異なる。

①Android を狙った手口の詳細

SMS の URL をタップすると、「システム警告」という画面が出て、「XXXセキュリティ」というアプリのバージョンアップを促されるが、これは不正なアプリをダウンロードさせようとしているものである（図 1-2-15）。

ダウンロードしただけでは被害にはつながらないが、

■図 1-2-15　KDDI セキュリティのアップデートをかたる例

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。

なお、偽のセキュリティアプリの名前は、かたる通信事業者に合わせ、au の場合は、「KDDI セキュリティ」、NTT ドコモの場合は、「NTT セキュリティ」となる。

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に誘導される場合がある（図 1-2-16）。

■図 1-2-16　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

削除される正規のセキュリティアプリは次の三つを確認している。

- あんしんセキュリティ（NTT ドコモ）
- 安心ネットセキュリティ（KDDI 株式会社）
- マカフィーモバイルセキュリティ（マカフィー株式会社）

②iPhone を狙った手口の詳細

iPhone を狙った手口は、以下の三つを確認している。

- 不正なアプリをインストールさせる手口

  SMS の URL のタップにより構成プロファイルをダウンロードさせ、偽のセキュリティアプリをインストールさせる（図 1-2-17）。

  構成プロファイルは主に通信事業者等が iPhone の設定を一括して行うために利用されるが、この手口では正規のアプリストアである Apple Store 以外から不正なアプリをインストールさせるためにダウンロードさせたものと考えられる。

- フィッシングサイトに誘導し、アカウント認証情報とクレジットカード情報を入力させる手口

  SMS の URL をタップすると、Apple Store アカウントに異常があったというポップアップメッセージが出て、メッセージをタップすると、Apple Inc. を装ったフィッシングサイトが表示される。

- フィッシングサイトに誘導し、アカウント情報とギフト券番号を入力させる手口

  au を装ったフィッシングサイトに誘導された場合は、au ID とパスワードを入力すると、未払い料金を請求する偽のメッセージと偽の請求額が表示される（図 1-2-18）。

■図 1-2-17　構成プロファイルをダウンロードさせ、不正なアプリをインストールさせる手口

（出典）一般財団法人日本サイバー犯罪対策センター「通信事業者を装ったフィッシング（不正アプリに注意）※114」を基に IPA が編集

■図 1-2-18　未払い料金を請求する偽のメッセージと偽の請求額が表示される画面

NTT ドコモを装ったフィッシングサイトに誘導された場合は、d アカウント ID とパスワードを入力すると、未払い料金を請求する偽のメッセージと偽の請求額が表示される。ログインページが出ず、偽の請求額が表示される場合もある。

（イ）被害

手口に遭遇した端末が、Android か iPhone であるかによって被害が異なる。

①Android における被害

Android における被害として、以下が確認されている。

- スマートフォンが攻撃の踏み台にされ、不特定多数の宛先（自身のアドレス帳にはない電話番号）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メッセージ等を窃取され、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。

② iPhoneにおける被害

iPhoneにおける被害として、以下が確認されている。

- 不正なアプリをインストールさせられた。

  不正なアプリを起動すると、ネットワーク暗証番号を入力させる画面が出て、入力した情報が詐取された。
- フィッシングサイトに誘導し、アカウント認証情報とクレジットカード情報を入力させられた。

  フィッシングサイトで情報を入力した場合は、その情報を不正使用される可能性がある。次のような相談が寄せられている。
  - Apple ID、パスワード、Apple ID確認コードを入力したところ、不正ログインされた。
  - 電話番号とキャリア決済サービスの認証コードを入力したところ、身に覚えのない請求が発生した。
  - 電話番号と認証コードを入力したところ、フリーマーケットサービス等にアカウントを勝手に作成された。
- フィッシングサイトに誘導し、アカウント情報とギフト券番号を入力させられた。

  「利用料金の未払い金があります。」という偽の画面から先へ進むと、ギフトカードで料金を支払うように誘導され、ギフトカードのシリアル番号を入力した場合は、購入したギフトカードの額面（金額）が相手に渡ってしまう（図1-2-19）。

■図1-2-19　ギフトカード番号の入力に誘導される画面

（ウ）対処

手口に遭遇した端末が、Androidか iPhoneであるかによって対処が異なる。

①Androidにおける対処

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2021」の「1.2.7（3）（a）（ウ）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。

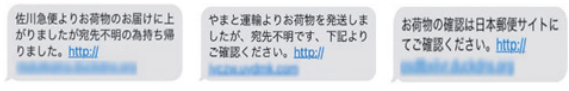
②iPhoneにおける対処

不正なアプリをインストールした場合の対処は、以下のとおりである。

- 不正なアプリのインストールによる、スマートフォン本体への影響範囲は不明なため、アンインストールだけではなく、スマートフォンの初期化を推奨する。
- 不正なアプリにネットワーク暗証番号を入力した場合は、ネットワーク暗証番号を変更する。
- 上記以外の対処は、「情報セキュリティ白書2021」の「1.2.7（3）（a）（ウ）対処」を参照いただきたい。

（b）宅配便業者を装うSMS

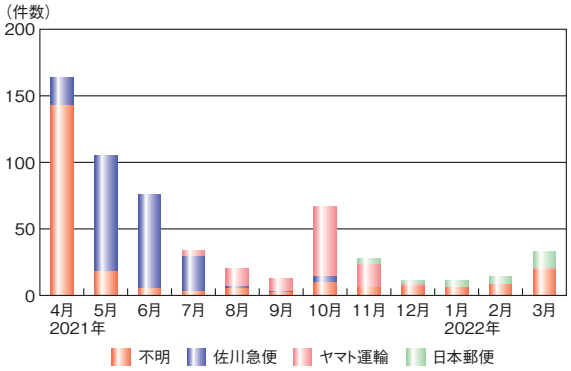
本件に関する相談は、2017年から確認されている。この手口は、当初佐川急便株式会社（以下、佐川急便）をかたるものであったが、2020年8月ごろからは、事業者名が記載されないものが登場し、2021年度は、かたる宅配便業者や不正なアプリの名前が変わる等、継続的に変化している（図1-2-20）。



■図1-2-20　宅配便業者をかたるSMSの例

2021年4月から佐川急便をかたるSMSによる相談が増加し、8月ごろからはヤマト運輸株式会社をかたるSMSの相談へ、更に11月からは日本郵便株式会社をかたるSMSの相談へと変化している。相談件数自体は減少傾向にある（次ページ図1-2-21）。

2021年5月初旬ごろから、再配達受付サイトを装っ



■図 1-2-21　宅配便業者をかたる SMS の件数推移（2021 年度）

た偽サイトに誘導し、運転免許証等の本人確認書類の写真を詐取する新たな手口に関する相談が増加した。IPA は「安心相談窓口だより※115」で、2021 年 6 月に注意喚起を行った。

以下では、この新たな手口について説明する。従来の Android 端末に不正なアプリをインストールさせる手口や、iPhone での偽のサイトに誘導する手口については、「情報セキュリティ白書 2021」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。

(ア) 手口

下記のような宅配便の不在通知を装った偽 SMS が送られてくる。偽 SMS に記載されている URL をタップすると、佐川急便を装った再配達受付の偽サイトに誘導される（図 1-2-22）。

■図 1-2-22　偽の不在通知 SMS から本人確認書類を詐取する手口

この手口は、従来の宅配便業者をかたる手口と異なり、Android も iPhone も同じ手口なのが特徴である。

偽サイトに記載されている指示に従い「電話番号」「本人確認書類（マイナンバーカード、運転免許証、パスポート）の写真」「メールアドレス」を入力すると、それらの情報が相手に伝わってしまうと考えられる。

(イ) 被害

入力した電話番号やメールアドレス宛に、不審な SMS や迷惑メールが届く可能性が考えられる。しかしながら、運転免許証、マイナンバーカード、パスポートの写真が悪意の第三者に渡った場合の被害については分かっていない。

(ウ) 対処

どのような対処が必要かについては、詐取された本人確認書類によって、以下の窓口等に相談することを検討いただきたい。

- 運転免許証の場合、住所地を管轄する警察署
- マイナンバーカード、パスポートの場合、交付元の各自治体

(c) SMS の手口の変化への対策

通信事業者は、SMS を送信する場合の電話番号やアドレス、内容について公式サイトで説明を行っている。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。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、送信元情報は偽装される場合もある。SMS を安全に利用するためには、受信しても即座に反応せず、真偽の判断を行っていただきたい。

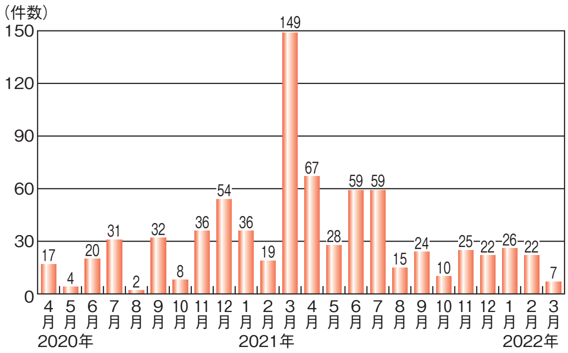
なお、2022 年 3 月から、各通信事業者が SMS を悪用したフィッシング詐欺への対策を開始した。NTT ドコモは、危険と判断したサイトの URL 等が含まれる SMS を自動で拒否する設定の自動適用を開始した※116。KDDI 株式会社は、迷惑メッセージブロック機能アプリの無償提供を開始し※117、ソフトバンク株式会社は迷惑 SMS 対策機能の提供を順次行っている※118。通信事業者が提供している機能を利用した対策を併せて行っていただきたい。

(2) 暗号資産を要求する脅迫メールの手口

この手口については 2018 年度より相談があり、2019

年度末以降は減少していたが、2020 年度末から 2021 年 7 月にかけて相談が増加した（図 1-2-23）。

従来は、外国語を日本語に直訳したような翻訳調の文面が多かったが、2020 年度末からは翻訳調ではなく顔文字を入れる等の日本語らしい文面のメールも登場したため、受信件数の増加に加えて、内容を信じて不安になり相談することが増えたと考えられる。



■図 1-2-23　暗号資産を要求する脅迫メールについての相談件数の推移（2020 ～ 2021 年度）

(a) 手口

脅迫メールの文面は変化を続けているが、盗んだ情報や盗撮したという動画を知人や動画サイトにばらまかれたくなければ、制限時間内に Bitcoin（ビットコイン）等の暗号資産を送金するよう要求する手口は変わっていない。

盗んだとする情報がメールに記載・添付されていた事例や、支払いに応じなかったために情報がばらまかれた事例等は確認されていない。このことから、根拠のない内容で脅迫していると推測される。

①脅迫メールの文面の変化

過去から継続している脅迫メールの文面としては、ハッカーを名乗り、パソコンに「トロイの木馬ウイルスをインストールした」（図 1-2-24）、「ハッキング」した、という文面がある。

過去の文面と比較して、以下のような変化が観測された。

- ハッキングしたという内容は同様だが、スマートフォンを対象として、「あなたのモバイルストレージについてデータ侵害がありましたことをお知らせいたします。」という文面も登場した。
- パソコンやスマートフォンの中の情報から友人、知人に情報をばらまくというのが定番であったが、2021 年 12 月ごろから、盗撮した動画を動画サイトで公開するという脅迫の手口も登場した。

Re:悪いお知らせがあります。

数ヶ月前にあなたのデバイスにアクセスしました。
その後、あなたの活動を監視するようになりました。
私は、あなたがインターネットにアクセスするために使っているすべての機器のOSにトロイの木馬ウイルスをインストールしました。このソフトウェアは、あなたのデバイス上のすべてのコントローラにアクセスすることができます。
あなたの情報、データ、写真、閲覧履歴をすべて私のサーバーにアップロードしました。
あなたのすべてのデータ、メッセンジャー、ソーシャルネットワーク、メール、チャット履歴、連絡先にアクセスできます。
私のウイルスはシグネチャを更新し、ウイルス対策ソフトからは見えないようになっています。
あなたの情報を集めているうちに、あなたがアダルトサイトの大ファンで、中毒性のある動画を楽しみながら見ていることがわかりました。
あなたがオナニーをしてオーガズムに達するという、あなたの汚いシーンをなんとか録画しました。
少しでも疑問があれば、私が数回クリックするだけで、すべての動画が知り合いに表示されます。
また、あなたの通信簿や個人的な写真、すべての秘密のデータをインターネット上に掲載することもできます。
あなたの評判を永遠に台無しにしてしまうかもしれません。
あなたが好きなビデオの仕様を考えると（よくわかっていると思いますが）、それはあなたにとって本当の意味での災難となるでしょう。
このように解決しましょう。あなたが私に　109931　円
(JPY)（送金時の為替レートでビットコイン換算）を送金してくれれば、私はこの汚れをすぐに取り除きます。その後は、お互いのことを忘れてしまいます。
また、お客様のデバイスからすべてのマルウェアを無効にして削除することをお約束します。
私はいつも約束を守ります。
ここに私のビットコインウォレットがあります：　bc1qd0ggud54qfun6jkx0n38rfyfgvf9mzrtkpy8x3
このメールを開いた瞬間から3日間の猶予があります。
送金がない場合は、あなたのビデオと詳細情報がインターネット上に公開され、すべての人とあなたの愛する人が見ることができます。
あなたの評判を永遠に台無しにします。
私を探そうとしないでください。
警察やその他のセキュリティ機関に連絡しようとすると、あなたの詳細が公表されてしまいます。
私はあなたの秘密をたくさん知っています。 [redacted]
自分の評価を意識する。

■図 1-2-24　脅迫メールの例

②自然な日本語の文面

当初この手口はもっぱら英語の文面を用いていたが、その後機械翻訳されたと思われる日本語の文面が送られるようになり、2021 年度には自然な日本語の文面の脅迫メールが登場した。顔文字が入っているものもある（図 1-2-25）。元になる文面は英語と思われるが、翻訳ソフトの翻訳精度が上がってきたためではないかと考えられる。

Subject: アカウントからのお支払い。未払いがあります

こんにちは！
残念ながら凶報がございます。数ヶ月前、あなたがインターネット閲覧に利用しているデバイスへのアクセス権を取得しました。
さらに、あなたのインターネット活動の追跡も行いました。

下記は、それまでに至る経緯です。
以前、ハッカーから複数のメールアドレスへのアクセス権を購入しました（最近では、オンライン上で簡単に購入することが可能です）。
よって苦労することなく、あなたのメールアカウント（[redacted]）にログインしています。
あなたのデバイスにアクセスしてから１週間以内に、メールに利用されているデバイスのオペレーティングシステム全てにトロイの木馬ウイルスをインストールしました。実際、この操作はかなり単純です（なぜなら、あなたが受信メールをクリックしたからです）。スマートな物事は何でもかなり単純なのでしょう。(´▽`)

～～～～～～～　　以下　省略　～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～

■図 1-2-25　自然な日本語の脅迫メールの例

(b) 対処

当該メールが複数回届くため、パソコンやスマートフォンからの情報窃取が、事実ではないかと信じ始めて相談される場合や、メールソフトやメールサービスの「迷惑メールフォルダ」に振り分けられている脅迫メールを確認して心配になり相談されることが多くなった。メールが届いた場合は、メールを削除するだけで問題ない。

メールの送信元が、メール受信者自身のアドレスになっている場合があるが、送信元アドレスは技術的に詐称が可能であり、迷惑メールのフィルタリングを回避することや、あたかもメールアカウントをハッキングしたと信じさせることが目的と考えられる。また、現在使用しているパスワードが書かれていた場合は、すぐにパスワードを変更し、併

せて、そのパスワードを使っていたサービスへの不正ログインがないか確認することを推奨する。

(3) 世の中の関心に乗じる手口

2021 年度も、新型コロナウイルスの感染が続き、経済や社会に様々な影響が出ているが、関心の高かった予防接種に関する内容が、フィッシングメールの手口に使われた。

(a) 手口

2021 年 2 月より、新型コロナウイルスワクチンの先行接種が開始され※119、高齢者の接種に続いて、対象年齢が順次下げられていったが、予約が取りづらい状況にあった。これに乗じて、8 月ごろから、新型コロナワクチン接種に関するフィッシングが登場し、「大規模接種センターの予約サイト案内」をかたるフィッシングメールに関する相談があった。IPA でフィッシングサイトを確認したところ、各種個人情報、クレジットカード情報を詐取する画面に誘導されることが分かり（図 1-2-26）、注意喚起を行った※120。また、厚生労働省※121 や、国民生活センター※122 からも注意喚起が行われた。

■図 1-2-26　コロナワクチン接種の偽サイト

2020 年度は「新型コロナウイルス感染症緊急経済対策」として家計支援のため、1 人あたり 10 万円が支給された「特別定額給付金」に関するものが多かったが、2021 年度も、特別定額給付金に関する通知を装うフィッシングが、フィッシング対策協議会より報告されている（図 1-2-27）。

(b) 対処

新型コロナワクチン接種に関しては、「新型コロナウイルスを題材とした攻撃メールについて※119」という注意喚起が厚生労働省より出され、注意喚起が行われている。

■図 1-2-27　特別定額給付金の支給をかたるメール
（出典）フィッシング対策協議会「特別定額給付金に関する通知を装うフィッシング（2021/08/24）※123」を IPA にて編集

総務省は、特別定額給付金について、政府からメール等で知らせることはないと説明している※124。

今後も、新型コロナウイルスに関して、様々な手口が登場することが想定されるが、対処は他の不審メールやフィッシングメールへの対応と同様である。本物かどうか判断に迷った場合は、公式サイト等、確かな情報源を使って確認し、以下の対処を行う。

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

Web サイトについては、見た目だけでは本物のサイトか偽のサイトかは、判断できにくくなっているため、メールに記載された URL から Web サイトにアクセスする以外の方法で運営者に確認するほか、フィッシング詐欺事例等がないかをインターネットで検索する等の対処を行う。

(4) 悪質化する Web ブラウザによる手口

パソコンやスマートフォンでインターネット閲覧中に、突然別の Web サイトに遷移し、画面が切り替わったり、スマートフォンにポップアップが表示されたりすることで、「偽のセキュリティ警告」や「アプリ誘導」の手口に遭遇することがある。

2020 年度末から 2021 年度にかけては、Web ブラウザの通知機能を悪用した手口によって誘導される相談が多くなってきた。

(a) 偽のセキュリティ警告

主にパソコンで Web サイト閲覧中に、突然警告音とともに、「ウイルスに感染している」等の警告画面が表示されたことをきっかけに、画面に表示された電話番号に電話をしてしまい、遠隔操作に誘導され被害に遭ってしまったという相談が 2021 年度も続いている。IPA は 2021 年 11 月、「安心相談窓口だより※125」で改めて注意喚起を行った。

警告画面を出す手口に変化は少ないが、コンビニエンスストアでプリペイドカードを購入させ、その番号を伝えることによりサポート費用と称したお金を支払わせる手口の相談が多くなった。

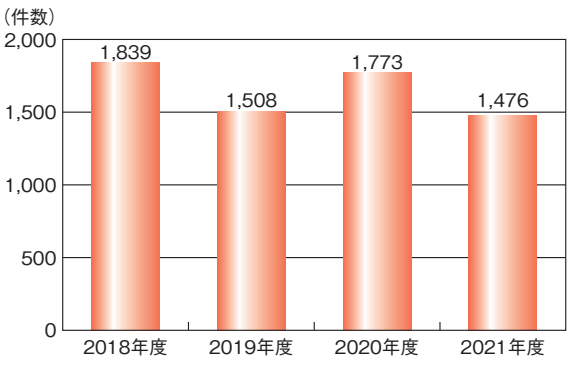
コンビニエンスストアのプリペイドカード売り場に注意喚起の表示がされるようになったが、被害が続いている。テレビやインターネットのニュース等でもこの手口が報道され、手口についての認識は広がっていると考えられるが、実際に遭遇すると、この手口に遭っていることに気が付かなかったという相談者も多い。

2022 年 1 月に、この手口で犯人が初めて逮捕されたとの報道があった。被害は 400 件以上でサポート費用と偽って銀行口座に振り込ませていたという※126。この報道の後も、相談件数は減らないため、この手口を用いる攻撃者は多く存在していると考えられる。

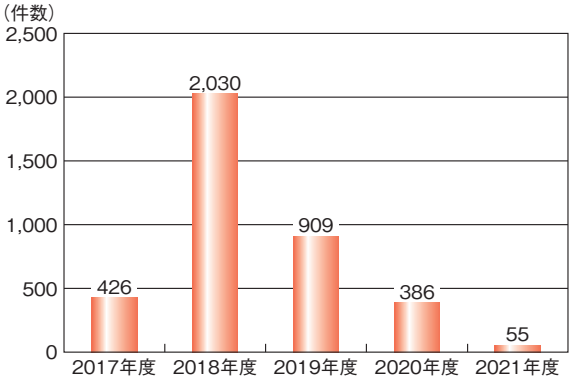
2021 年度に IPA の安心相談窓口に寄せられた相談件数は、有償サポート契約に誘導される「偽警告」(別名、サポート詐欺)が 1,476 件(図 1-2-28)、有償ソフトウェアの購入に誘導される「偽セキュリティソフト」が 55 件であった(図 1-2-29)。「偽セキュリティソフト」の購入に誘導する手口は減少している。

(ア) 手口

インターネット閲覧中の Web ブラウザ画面上に、本物に見せかけたセキュリティ警告を表示して、解決のため



■図 1-2-28　偽警告に関する年度別相談件数



■図 1-2-29　偽セキュリティソフトに関する年度別相談件数

に記載してある電話番号に電話をかけさせようとする。そのため、様々な誇大表現で危険性を訴えかけ、冷静な判断を妨げるよう仕組んでいると考えられる。

この手口は以下の①から④の流れとなる場合が多い。

①偽のセキュリティ警告画面が表示される

偽のセキュリティ警告画面の表示は以下のようになる場合が多い。

- 警告の画面が次々と重なって開く

  警告画面がいくつも重なって開き、しかも警告が全画面表示で固定されて「閉じるボタン」が隠されてしまい、画面を閉じることができない事例が多い(図 1-2-30)。

■図 1-2-30　警告画面が次々と全画面で開く画面の例

- 実在する企業やサービスのロゴ等が表示される

  Microsoft 社、マカフィー株式会社等の企業名やロゴ(次ページ図 1-2-31)、また Windows の標準機能からの警告を偽った表示が、繰り返し表示される。

- サポート窓口の電話番号が表示される

  問い合わせ先の電話番号が、繰り返し表示される。特に Microsoft 社のサポート窓口をかたる事例を多く確認している(次ページ図 1-2-32)。

②警告音やアナウンスが流れる

画面上の偽の警告表示に加えて、けたたましい警告

■図 1-2-31　実在する企業やサービスのロゴ等が表示された画面の例

■図 1-2-32　サポート窓口の電話番号が表示された画面の例

音や、テクニカルサポートを名乗る「ウイルス感染」等の警告アナウンスが大音量で延々と流れる。

③オペレーターが電話対応する

警告画面に記載されている電話番号に電話をかけると、オペレーターが状況を聞き、ウイルスに感染している等と言い、遠隔操作用ソフトウェアをダウンロードさせインストールをさせようとする。更に遠隔操作によって、パソコンに様々な画面を表示させ、危険性をあおり、有償サポート契約を勧める。

- 相手の反応を見ながら、「月契約」「年間契約」「永久契約」等の契約期間を説明し、期間に合わせて、数万～10万円程度の代金を提示することが多い。
- 入力フォームに住所・氏名等の個人情報の入力をさせることがある。
- デスクトップのアイコンを非表示にしたり、パソコン起動時に新たにパスワードの入力を必要にしたりする等、勝手にパソコンの設定を変更し、元に戻すために契約しろと要求する悪質な手口も確認している。

④サポート代金のプリペイドカードを繰り返し購入させる

2021年度は、購入したプリペイドカードのコードを伝えると「コードが間違っていてブロックされた」等と言い、繰り返しプリペイドカードを購入させ、複数回支払わせる例が増え、90万円を支払ったという相談事例もあった。

(イ)対処

パソコンの画面については、Webブラウザ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は、Windowsであれば、タスクマネージャーからWebブラウザを終了する、Macであれば、「強制終了」ウィンドウからWebブラウザを終了する、という方法で対処できる。また、どちらのOSの場合も、パソコンを再起動することでも対処できる。

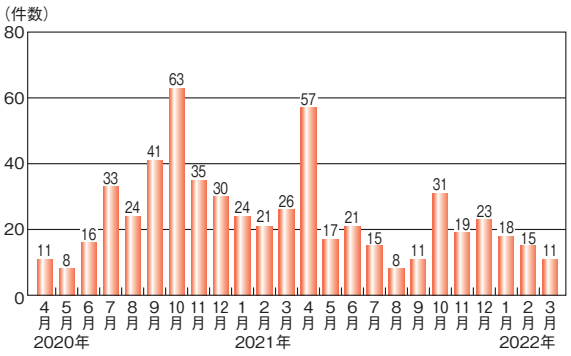
パソコンに遠隔操作用ソフトウェアをインストールしてしまった場合は、アンインストールする。

電話口のオペレーターに詳細不明のソフトウェアをインストールさせられた場合は、より安全な対応として、当該ソフトをインストールする前の状態にシステムを戻すことや、パソコンを初期化することを推奨する。

契約については、消費生活センター等※127に相談する。プリペイドカードでの支払いについては返金が困難な場合が多い。また、Microsoft社では、当該手口に関する専用ページ※128で手口や事例を紹介し、被害報告も受け付けているため、活用を検討いただきたい。

(b)アプリ誘導

主にスマートフォンで、Webサイト閲覧中に「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続いている(図1-2-33)。

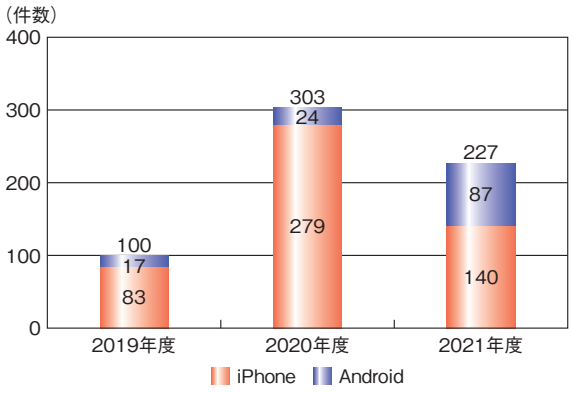


■図 1-2-33　アプリ誘導に関する相談件数(2020～2021年度)

手口の変化は少なく、インターネット閲覧中に偽の警告から誘導される事例が多い。

2020年度は、iPhoneカレンダースパムからこの手口に誘導されたため、iPhoneの相談が多かったが、2021年度は、Androidの相談が増えているのが特徴である(次ページ図1-2-34)。

以下では、Androidの場合の手口、対処を中心に説明する。



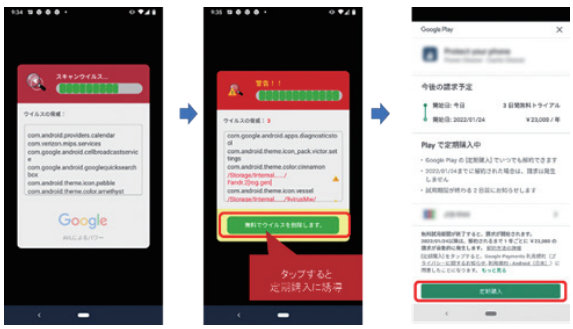
■図 1-2-34　アプリ誘導の端末別の年度別相談件数推移

(ア)手口

「あなたのスマホはウイルスに感染している可能性がある」「下のボタンをタップし無料で推奨セキュリティアプリをインストールして実行し、ウイルスを削除」というように、偽の警告画面を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手口である(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)

「サブスクリプション詐欺」を目的として、自動継続課金※129 に誘導することが目的と考えられ、アプリインストール後の初回起動時にウイルススキャンをしているかのような表示をしてウイルスを検出したと偽り、定期購入に誘導するものも登場した(図 1-2-36)。



■図 1-2-36　偽のウイルス検知画面から定期購入へ誘導する流れの例(Android の場合)

無料アプリだと誤解して承認してしまうと、無料期間は3日間から1週間程度であることが多く、無料試用期間の終了後に意図しない利用料金が発生することになる。

(イ)対処

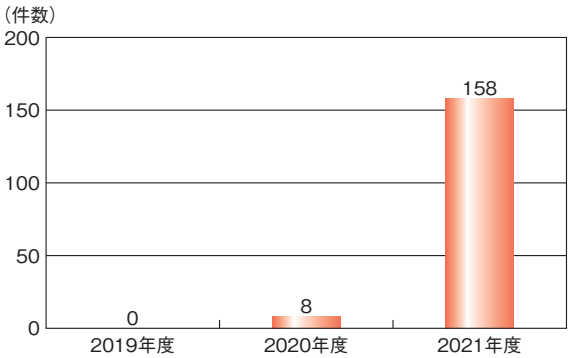
偽のセキュリティ警告が表示された場合は、Web ブラウザのタブを閉じる、または、Web ブラウザを終了し閲覧履歴を削除することで対処できる。

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、自動継続課金の登録を取り消す必要がある。Android の場合は定期購入の解約(図 1-2-37)、iPhone の場合はサブスクリプションの解約も実施する。

■図 1-2-37　定期購入の解約手順(Android 11 の場合)

(c)Web ブラウザの通知機能の悪用

2020 年度後半から、2021 年度にかけて、パソコンやスマートフォンで Web ブラウザを起動中に、「『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』 等のメッセージが繰り返し表示された」、またその表示画面から「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た」といった相談が急増した(図 1-2-38)。IPA は 2021 年 3 月、「安心相談窓口だより※130」で注意喚起を行った。



■図 1-2-38　Web ブラウザ通知機能の悪用の相談件数推移

(ア)手口

Web ブラウザの通知機能※131 を悪用し偽の通知を表示させ、不審サイトに誘導する手口である。以下の①から③の流れとなる場合が多い。

①サイト上で Web ブラウザの通知を許可するように誘導される

検索サイトで表示されたサイトにアクセスする等でサイトに訪れた人に Web ブラウザ通知の許可ボタンを表示し、アクセスした人に「許可」を押させようとする(図 1-2-39)。その際、reCAPTCHAv2 認証※132 を装った画面を表示して、「許可」ボタンを押させようと誘導する(図 1-2-40)。

■図 1-2-39 「許可」ボタンへの誘導事例(Android の場合)

■図 1-2-40 reCAPTCHAv2 認証を装った「許可」ボタンへの誘導事例(パソコンの場合)

② Web ブラウザ起動中に偽の通知が表示される

図 1-2-39 や、図 1-2-40 等の画面で「許可」を押してしまうと、当該不審サイトの通知許可が Web ブラウザに登録されてしまう。その後、Web ブラウザを起動中等に「パソコンがウイルス感染した」「スマートフォンをクリーンアップしてください」(図 1-2-41) 等の通知が表示

■図 1-2-41 スマートフォンに表示される通知表示事例(Android の場合)

■図 1-2-42 パソコンのデスクトップ右下に出現する通知表示事例

される。

パソコンではセキュリティベンダや、Windows のロゴを勝手に使用したと思われる通知がデスクトップの右下に表示される事例を確認している(図 1-2-42)。

これらの通知は根拠のない偽の内容であり、不安をあおって不審サイトに誘導する目的であると考えられる。

③通知表示をクリックすると不審なサイトに誘導される

通知表示をクリックすると、様々な不審サイトに誘導される。パソコンの場合、「偽のセキュリティ警告」が表示されるサイトや、「セキュリティソフト購入サイト」に誘導される。スマートフォンの場合、「不審アプリのインストール誘導サイト」が表示される事例を確認している。

(イ)対処

Web ブラウザ通知機能の悪用そのものへの対処、Web ブラウザ通知機能を悪用された結果起こった事象への対処、それぞれの対処方法について述べる。

① Web ブラウザの通知の削除方法

Web ブラウザ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 ブラウザ操作方法の詳細は、「安心相談窓口だより※128」や、パソコン・スマートフォンメーカのサポート情報、各 Web ブラウザのヘルプページを参照いただきたい。

②誘導された不審サイトで操作を行った場合

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。

- 偽のセキュリティ警告に誘導された場合
  「1.2.7(4)(a)偽のセキュリティ警告」に記載した対処を行う。
- セキュリティソフト購入サイトに誘導された場合
  マカフィー株式会社と思われるサイトに誘導された場合は、マカフィー株式会社の Web ページにある、「マカフィーを装う偽のポップアップ通知と問題の解消方法について※133」を参照して対処いただきたい。誤って製品等を購入した場合については、「一般的な FAQ※134」を参照いただきたい。
- 不審アプリのインストールサイトに誘導された場合
  「1.2.7(4)(b)アプリ誘導」に記載した対処を行う。

(5) 騙しの手口への対策

情報セキュリティへの意識の高まりを攻撃者に逆手にとられ、「ウイルス感染」や「トロイの木馬」「ハッキングした」等という文言を信じてしまい、被害に遭っていることが多いと考えられる。

日頃からしっかりとセキュリティ対策を行うことによって、不審な SMS やメール、端末への通知が来ても、いったん立ち止まり、対応を確認することができるので、過剰な心配をせず攻撃者に付け込まれないようにすることができると考える。

対策の例としては、以下のものがある。

- 使用している端末やアプリのアップデートを常日頃行う。
- サービスの利用にあたって、可能な場合は必ず多要素認証を設定する。
- 不審なメールや SMS、サイト等で目にした情報の真偽は、確かな情報源で確かめる。
- 判断に迷ったら、身に覚えのない内容のメールや画面に表示された電話番号の相手ではなく、信頼できる相手に相談する。

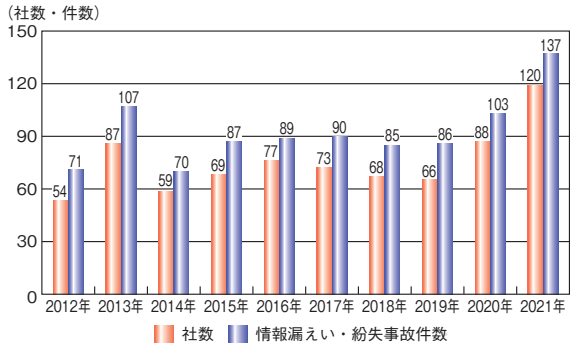
以上に加えて、日頃から最新情報を入手して手口を知ることが、騙しの手口への重要な対策となると考える。

1.2.8 情報漏えいによる被害

2021 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、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) 2021 年の情報漏えいの概況

2022 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※135 によると、2021 年に個人情報の漏えい・紛失事故を公表した上場企業は 120 社（2020 年※136 は 88 社）、事故件数は 137 件（2020 年は 103 件）、漏えいした個人情報は 574 万 9,773 人分（2020 年は 2,515 万 47 人分）に達した。漏えいした個人情報は大幅に減少しているが、公表した社数、事故件数ともに東京商工リサーチ社が調査を開始した 2012 年以降で最多となった（図 1-2-43）。



■図 1-2-43　漏えい・紛失事故の年次推移
（出典）東京商工リサーチ社「上場企業の個人情報漏えい・紛失事故は、調査開始以来最多の 137 件 574 万人分（2021 年）※135」を基に IPA が編集

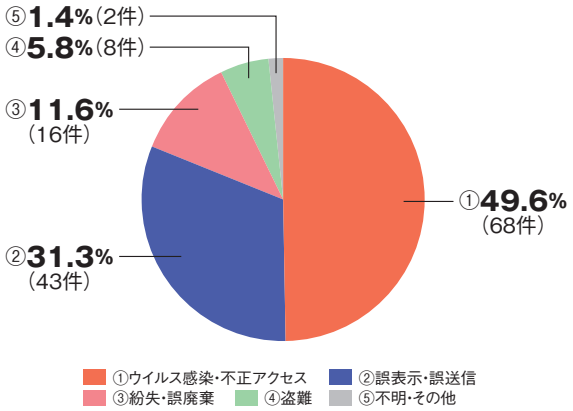
2021 年の情報漏えい・紛失事故 137 件のうち、原因として最も多かったのは「ウイルス感染・不正アクセス」の 68 件、構成比 49.6%（2020 年は 51 件、構成比 49.5%）、次いで「誤表示・誤送信」が 43 件、構成比 31.3%（2020 年は 32 件、構成比 31.0%）となっており、構成比の変化は小さいが、件数がともに 10 件以上増えており、過去最多となった要因になっている（次ページ図 1-2-44）。

(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利用したものや、対策が不十分な委託先、システム等、様々な原因から不正アクセスが発生している。

(a) 不正アクセスによる大量の情報流出事例

株式会社ネットマーケティングの事例※137 では、同社の運営する恋活・婚活マッチングアプリ「Omiai」から 171 万 1,756 件の年齢確認書類画像データが流出した。年齢確認書類画像データは法令で義務付けられた本人



■図 1-2-44　情報漏えい・紛失事故件数の原因別割合
(出典)東京商工リサーチ社「上場企業の個人情報漏えい・紛失事故は、調査開始以来最多の 137 件　574 万人分(2021 年)」を基に IPA が編集

確認に使用しており、運転免許証、健康保険証、パスポート、マイナンバーカード（表面）等が含まれていた。その他に登録されていた個人情報の流出は確認されていない(「3.3.2(2)不正アクセスに起因するインシデント」参照)。

森永製菓株式会社の事例※138-1では、同社運営のWeb サイト「森永ダイレクトストア」(旧「天使の健康」)の顧客 164 万 8,922 人分の個人情報(氏名や住所、連絡先等）が流出した可能性があると公表した。脆弱性が残存していたネットワーク機器への攻撃により侵入され、一部のデータは利用できない状態となった。

カジュアルウェア専門店株式会社ライトオンの事例では、公式オンラインショップに不正アクセスがあり、会員登録フォームより入力された個人情報（氏名や生年月日、性別、住所、電話番号、メールアドレス等）24 万 7,600 件が流出した※138-2。

臨床試験に関する業務を受託する株式会社リニカルの事例※139では、日本、台湾、欧州の同社拠点のサーバに対して不正アクセスがあり、犯行グループから窃取したとするデータに対して身代金を要求する脅迫メッセージがあった。日中韓台の採用応募者や株主情報等約 9 万 6,000 件、日欧中韓台の社員情報・人事情報約 12 万 5,000 件及び臨床試験関連文章や営業データ等が流出した可能性が判明した。

映像技術・マイクロ波・無線通信技術の専門メーカである株式会社ユピテルの事例※140では、同社は 52 万 8,563 件のデータ、会員情報 40 万 5,576 件が 2017 年 10 月に流出していたことを 2021 年 6 月に公表した。2017 年当時は不正アクセスを確認するも情報流出の痕跡は認められなかったため公表しなかったが、2021 年 5 月にサーバからハッキングした顧客情報を持っているとして、犯人と見られる人物から金銭を要求する脅迫メールが同社に届き、記載されたリンク先で上記情報を確認したという。

(b)不正アクセスによる情報流出への対策・対処

不正アクセスの事前対策については、「1.2.1 (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。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案」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(「2.8.1 個人情報保護法改正」参照)。

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。

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。前述の株式会社ネットマーケティングの事例では、会員情報の保管期間を一律で退会後 10 年間としていたが、被害後、年齢確認書類画像データは提出後 72 時間で自動削除、その他の個人データは退会後 90 日間と変更し、他の安全対策とともに運用を開始した。

(c)SQL インジェクション攻撃による情報流出事例

株式会社メタップスペイメントの事例※141では、決済情報等を格納した三つのデータベースに不正アクセスされ、そのうちの一つであるトークン方式クレジットカード決済情報データベースから最大 46 万 395 件のクレジットカード情報(カード番号、有効期限、セキュリティコード)が流出した可能性がある。本事例では SQL インジェクション攻撃と不正ファイル（バックドア）の設置が確認されている。同社の収納代行システムを利用する団体では、一部のカード決済機能の停止、チケット販売や新規入会停止等の影響が出た※142。

SQL インジェクション攻撃による情報の流出では、他に

も中学受験関連サービスを提供する株式会社日能研※143から最大28万106件、翻訳ソフトウェア事業等を展開するロゴヴィスタ株式会社※144から約12万8,000件、株式会社石橋楽器店※145から9万8,635件、自社ブランド製品の企画、開発を行うビーズ株式会社※146から2万3,435件のメールアドレスが、宅配クリーニングサービスのWebサイトを運営する株式会社ヨシハラシステムズ※147から5万8,813件のクレジットカード情報が流出した可能性があると公表されている。

(d) SQLインジェクション攻撃による情報流出への対策

SQLインジェクションは過去10年以上にわたり問題であり続けている。IPAでは2008年に「SQLインジェクション攻撃に関する注意喚起※148」、2017年に「SQLインジェクションをはじめとしたウェブサイトの脆弱性の再点検と速やかな改修を※149」と題する注意喚起を行っている。IPAが公開している「ウェブ健康診断仕様※150」「安全なウェブサイトの作り方※151」等を参照して、対策を検討いただきたい。

(e) ランサムウェア攻撃による情報流出事例

日本サブウェイ合同会社の事案※152では、ランサムウェア攻撃により、約30万件のサブクラブカード会員番号、約8万人分の顧客情報(誕生日、都道府県、職業等)、約1万人分の個人情報(名前、結婚歴、誕生日、性別、住所、職業、電話番号、職歴、メールアドレス、収入情報、銀行口座情報、自動車運転免許、国籍、クレジット歴、パスポート/ID、賞罰歴、ユーザネーム等)、64名の顧客情報(名前、年齢、電話番号)に不正アクセスされた恐れがあると公表している。

行政機関の公共事業を受託するランドブレイン株式会社の事例※153では、不正アクセスした攻撃者が、サーバ上の二つのファイルを開封した痕跡があり、データの暗号化、ファイルの作成が確認された。しかし、情報流出を示唆する明確な痕跡は確認されず、情報流出はないと判断したという。攻撃に用いられたランサムウェアは、「Crypt3r」「Ghost」「Phantom」「Vjiszy1lo」といった別名でも知られる「Cring」であることが判明した※154。

同じく公共事業を受託する株式会社オリエンタルコンサルタンツホールディングスの事例※155では、同社はグループ会社数社の複数のサーバがランサムウェア攻撃を受け、サーバ内の委託業務関連データの多くが暗号化され、外部流出した可能性があると公表した。流出の可能性のある情報には、千葉県、東京都、群馬県、滋賀県、埼玉県、岡山県等※156の建築関連の委託業務の図面や資料、関係者の個人情報等が含まれているが、どの情報が流出したかの特定には至っていない。同社は2021年9月期(2020年10月1日～2021年9月30日)の連結業績について、復旧に向けた関連費用として約7億5,000万円の特別損失を計上する見込みを発表した※157。

その他のランサムウェアの被害と対策については「1.2.2 ランサムウェア攻撃」を参照いただきたい。

(f) 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

富士通株式会社の事例※158では、同社はプロジェクト情報共有ツール「ProjectWEB」に不正アクセスがあり、保存していた情報の一部が不正に閲覧またはダウンロードされたと公表した。同社がプロジェクト運営に際し、委託元を含む関係者との情報共有にProjectWEBを利用しており、被害のあった顧客は行政機関(NISC、外務省、国土交通省、総務省等)や重要インフラ企業(成田国際空港株式会社等)等142に及んだ。閲覧またはダウンロードされた情報には、システムに関する情報(システムを構成する機器類の情報等)、プロジェクト関連資料(体制図、打合せメモ、作業項目一覧、進捗管理表、社内事務手続きの資料等)、顧客・関係者の個人情報(氏名・メールアドレス等)が含まれていたという。同社は、脆弱性を悪用した第三者がIDとパスワードを窃取し、外部から不正アクセスを行ったとしている。NISCは政府機関等、重要インフラ事業者等に向けて、同種ツールに対する不正アクセス対策の確認について注意喚起※159を行った。同社はProjectWEBの利用を停止し、その後の調査でProjectWEBに複数の脆弱性が存在していたこと、多要素認証を採用していなかったこと、不正アクセスを早期に検知する仕組みが十分でなかったこと等を認めた。

株式会社ジーアールの事例※160では、同社が運営する「オムニECシステム」に不正アクセスがあり、顧客情報やクレジットカード情報が流出した。クレジットカード会社から同システムを利用する流通大手企業に情報流出の懸念があると同社に連絡があり、発覚した。同システムは、小売店や製造販売会社のサービスのデジタル統合に利用されており、影響を受けた11社※161が被害を公表した。漏えいした情報は11社合わせて40万件以上に及ぶ。この事例の攻撃手法はクロスサイト・スクリプティングだったと報じられている。

(g) 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割かれる。利用各社は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保管を委託する情報の種類、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 2021 年 10 月に公表した「（2020 年度）『個人情報の取扱いにおける事故報告集計結果』[※162]」によると、2020 年度は 939 のプライバシーマーク付与事業者から 2,644 件の事故報告があった。事故の発生原因としては「誤送付」が 62.3%（2019 年度は 59.5%）と最も多く、「紛失」が 14.9%（2019 年度は 16.6%）、「その他漏えい」が 17.2%（2019 年度は 17.5%）となっている。「誤送付」の中でも「メール誤送信」は過去 5 年間で最も多く、764 件に達している。これに対し、「宛名間違い」「封入ミス」「FAX 誤送信」等の紙媒体を伴う報告は減少しており、テレワークの導入等により、通信及び連絡手段が変化したことによるものと推測している。

(a) 過失による情報漏えい事例

日本年金機構の事例[※163]では、同機構は年金振込通知書の印刷誤りにより愛知県、三重県、和歌山県、奈良県、福岡県、山形県、富山県、静岡県、岐阜県の合わせて 97 万 5,065 件の受給者に、本人と別の受給者の情報が記載されたはがきを送付したと公表した。原因は、印刷業務を委託したサンメッセ株式会社での印刷工程の作業ミスであったが、その後の調査により、仕様書どおりの環境で作業せず同機構に虚偽の報告をしていた、出力設定に誤りがないことを確認する仕組みがなかった、仕様書に定められている宛名と記載情報の突合作業をしていなかった等、作業ミスの防止対策が実施されていなかったことが分かった[※164]。年金振込通知書の再作成・発送やお詫び状の送付等費用はサンメッセ株式会社が負担し、同社は 2022 年 3 月期第 2 四半期において 2 億 3,000 万円の特別損失を計上した[※165]。

LINE 株式会社の事例[※166-1]では、同社は LINE VOOM（旧タイムライン）において、システム移行時の設定ミスにより「友だち」の公開範囲の設定が適切に機能せず、利用者が非公開と設定した「友だち」が公開先リストに誤って含まれる不具合があったと公表した。この不具合により、約 111 万アカウント（国内約 84 万アカウント）において非公開投稿が誤って表示されたほか、非公開の「友だち」が「LINE 友だち」に追加されたアカウントは約 911 万アカウント（国内約 764 万アカウント）に上るという。

LINE Pay の事例[※166-2]では、LINE 株式会社がサービス利用ユーザのアカウント合計 13 万 3,484 件（うち国内ユーザは 5 万 1,543 件）のキャンペーン関係の識別情報（識別子・加盟店管理番号、キャンペーン情報）が GitHub 上で外部閲覧可能な状態にあったと公表した。同社の委託先であるグループ会社の従業員が、ポイント付与漏れの調査を行うプログラム及び対象となる決済に関する情報を無断で GitHub 上にアップロードしてしまい、閲覧できる状態であったという。部外者から GitHub の情報へのアクセスが 11 件あったことが確認され、流出対象となったユーザに通知を行った。

(b) 過失による情報漏えいへの対策

情報の取り扱いに人が介在する状況においては、過失による情報漏えい被害を完全に防ぐことは難しい。事故事例に基づく教育等で担当者の意識向上を図ることに加え、重要な情報の取り扱いルールを設け、運用を徹底する、適宜見直す等で、過失の発生機会をできる限り削減する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

IPA が実施した「企業における営業秘密管理に関する実態調査 2020[※167]」では、営業秘密の漏えい原因は「中途退職者」が 36.3% と最も多く、2016 年の調査から 7.7 ポイント上昇していた。同調査によれば、うっかりミス

は減少したが確信犯的な内部不正は増加しており、継続している傾向がうかがえる。

(a) 内部不正による情報漏えい事例

株式会社村田製作所の事例※168では、同社は委託先である日本アイ・ビー・エム株式会社の再委託先の中国法人 IBM Dalian Global Delivery Co., Ltd. の社員が同社の取引先情報 3 万 555 件、同社の従業員関連情報 4 万 1,905 件を含むプロジェクト管理データを許可なく業務用パソコンへダウンロードし、更にこれらのデータを中国国内クラウドストレージサービスの個人アカウントへアップロードしていたと公表した。再委託先の社内監視システムのセキュリティアラートにより検知された。

回転ずし大手「かっぱ寿司」を経営するカッパ・クリエイト株式会社の事例※169では、同社は代表取締役が競合する株式会社はま寿司（以下、はま寿司）の営業秘密を不正に取得したとして、不正競争防止法違反で警視庁から捜査され、はま寿司により告訴がなされたことを公表した。代表取締役は、同社の顧問となる以前は、はま寿司の親会社である株式会社ゼンショーホールディングスに勤めており、元同僚からはま寿司の日次売上データ等の送付を数回にわたって受けていた。

株式会社ハウスドゥ住宅販売の事例※170では、元従業員が 2021 年 1 月に同社を退職する際、所属部門に保管されていた顧客情報を持ち出した。同社は元従業員を不正競争防止法違反で刑事告訴し、愛知県警察による捜査で不正な持ち出しが判明した。

(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※171」第 5 版を公開した。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おり、参照いただきたい（「2.8.2 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

日本郵便株式会社の事例※172では、投資信託取り引き及び国債取り引きに関する「金融商品仲介補助簿」の社内紛失が全郵便局 1 万 9,816 局のうち 6,389 局（32.2%）で確認され、合わせて顧客約 7 万 2,000 人分と公表された。また「金融商品仲介補助簿」以外の書類を確認した結果、176 局で約 14 万 2,000 人分を紛失していた。「金融商品仲介補助簿」は法令上 7 年保存（社内規則上は 10 年保存）と定められていたが、大多数の郵便局において保存期間の認識相違や保存箱の入れ間違い等により、誤って廃棄してしまったという。

金沢信用金庫の事例※173では、同金庫は為替関係帳票、ATM ジャーナル、住宅ローン稟議書、伝票等の書類を保管していた文書箱合わせて 11 箱、延べ 55 万 1149 件の顧客情報の所在が不明であることを公表した。保存期限を経過した書類を廃棄（裁断）した際、誤ってこれらも廃棄（裁断）した可能性が高いと考えられている。

トヨタ自動車株式会社の事例※174では、同社が提供する顧客向け Web サイト認証サービス「TOYOTA/LEXUS の共通 ID」の ID 発行のため、本人の同意を得ずに顧客情報を登録していた。同社の販売店である福岡トヨペット株式会社において、同事象が発覚し、全国 257 社で同様の事例がないか調査した結果、27 社、5,797 人分の個人情報（名前、生年月日、性別、住所、電話番号、コネクテッドサービス契約車両の所有情報）が本人の同意を得ずに登録されていたという。このような個人情報の不適切な取り扱いの背景には、同社から販売店に同 ID の発行を推奨する活動を行っていたことがあるとされる。同様に、株式会社 SUBARU※175においても本人の同意を得ずに新規会員登録が行われていた。

新生銀行グループの事例※176では、株式会社新生銀行並びに新生フィナンシャル株式会社は複数の業務委託先に対して Web 解析や広告媒体事業に関するデータを提供する際、提供対象ではないデータが誤って含まれていたと公表した。同行において、Web 解析を目的に、業務委託先等のうち 1 社から還元を受けたデータを検証したところ、新生銀行グループの株式会社アプラスから提供したデータに、提供すべきでない ID・パスワードが含まれていたことから、同グループ内において類似の事象が発生していないか調査を実施した。その結果、七つの事案において延べ 8,875 件のデータが誤って業務委託先及び広告媒体会社 10 社に提供されていた。提供されたデータにはメールアドレス、住所、氏名、生年月日、会員番号、カード番号、カード暗証番号、金融機関と口座情報等が含まれていた。

株式会社新生銀行の別の事例※177では、同行は吸収分割契約によりマネックス証券株式会社へ承継する投資信託保護預かり口座の情報を提供する際、無関係の

口座情報 1,469 件を誤って提供したことを公表した。提供された情報には個人情報（マイナンバー、氏名、生年月日、口座番号）、法人情報（法人番号、法人名、口座番号）が含まれていた。

(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、社内ルールへの取り込みや周知徹底のために従業員への教育等を継続して行う必要がある。

COLUMN

子どもへの情報リテラシー教育のために

IPA では、情報セキュリティの基礎知識に加えて情報リテラシーの向上を目指し、「インターネット安全教室」という講義形式のセミナーを実施しています。対象は、「インターネットを利用するすべての方」で、子どもからシニア世代まで幅広く受講いただいています。受講された学校の先生から、「生徒の自宅での情報端末管理は各家庭に任せている」という声があり、家庭での情報リテラシー教育も重要なことを改めて認識しました。

インターネット利用開始時に誰に使い方を教えてもらったかを尋ねたところ、保護者と回答した割合が最も多かったという家庭教育の重要性を示す調査結果[i]があります。SNS をめぐるトラブルや情報流出等の事故を防ぐためには、判断能力が十分に備わっていない子どもに任せきりにせず、保護者との日頃のコミュニケーションを通じた学びが不可欠です。

子どもに情報端末を持たせるとき、保護者側が何らかのルールを設ける場合が多いものの、その内容は利用する時間・場所、利用料金や利用するサイトに関するものが多く[ii]、ID・パスワードの管理といったセキュリティ寄りの内容はやや不足しているように思われます。GIGA スクール構想で一人一台の情報端末が配布され、オンライン教育も当たり前のものとなった今、子どもにとって、インターネットを安全に利用するための情報セキュリティはより身近なものとなり、保護者自身も意識を高めていくことが重要です。

IPA では、Web サイト「#今こそ考えよう 情報モラル・セキュリティ[iii]」上で、対象者層ごとに適したコンテンツを紹介しています。更に、一般社団法人日本教育情報化振興会では、「ネット社会の歩き方[iv]」で、冊子・シミュレーション教材等を公開しています。ぜひ、これらの資料を活用しましょう。

一方、情報リテラシー啓発に携わる教育委員会の委員等からは、「保護者に啓発したいけれども、なかなかセミナーの場に参加していただけない」という声が聞かれました。今後、保護者層へ訴求していくためには、学校や公的機関による従来の情報提供の形に加えて、情報リテラシー分野をより敷居の低いのものとするため、TV アニメ化もされた漫画「はたらく細胞[v]」にみられるような、擬人化したキャラクターやストーリーをきっかけに、保護者・子どもが共に楽しみながら学べる新しいコンテンツ等も求められているのかもしれません。

i　総務省：2020 年度 青少年のインターネット・リテラシー指標等に係る調査結果　https://www.soumu.go.jp/main_content/000746185.pdf〔2022/5/23 確認〕
ii　内閣府：令和 2 年度 青少年のインターネット利用環境実態調査（PDF 版）　https://www8.cao.go.jp/youth/youth-harm/chousa/r02/net-jittai/pdf-index.html〔2022/5/23 確認〕
iii　https://www.ipa.go.jp/security/keihatsu/imakoso/〔2022/5/23 確認〕
iv　http://www2.japet.or.jp/net-walk/〔2022/5/23 確認〕
v　株式会社講談社：はたらく細胞　https://shonen-sirius.com/series/sirius/saibou/〔2022/5/23 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※102」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、2021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

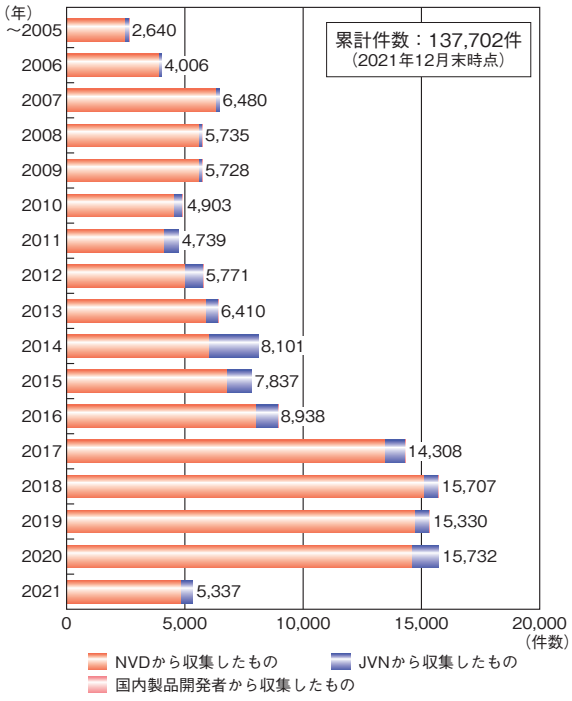
JVN iPediaは、国内外で利用されているソフトウェア製品の脆弱性対策情報を、以下の三つの公開情報から収集・蓄積しており、2007年4月25日から公開している。

- 脆弱性対策情報ポータルサイトJVN※178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※179」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に登録している情報を、製品ベンダやセキュリティ関連企業が脆弱性情報を公表した年別※180にまとめると、2011年を境にして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。なお、2021年の登録件数は12月末時点で5,337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、2021年の登録数も最終的には2020年と同程度になる見込みである（図1-3-1）。2017年以降、NVDに公開される脆弱性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脆弱性識別子CVE（Common Vulnerabilities and Exposures）※181の採番機関（CNA：CVE Numbering Authority）※182が増加したことが一因として挙げられる。The MITRE Corporation※183によると、2016年12月に47社※184だったCNAは、2021年12月には209社※185と約4.4倍となった。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は、2020年に公表されたものが1,120件で、2019年の594件から2倍近くになったが、2021年は再び減少し、半数以下の496件となった。また、国内製品開発者から公表された脆弱性対策情報は、毎年数十件の登録であり、2021年は12件であった。



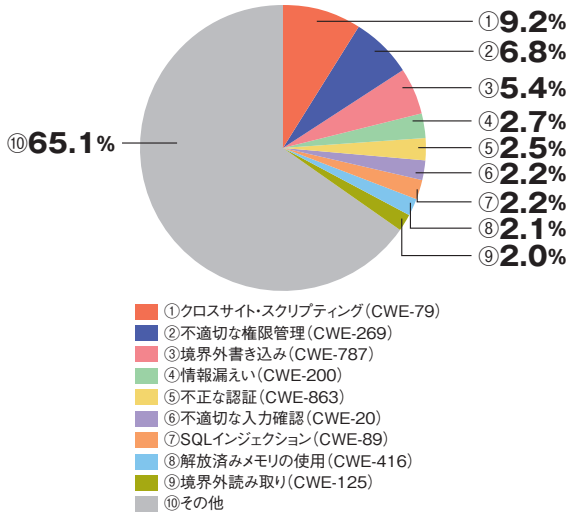
■図1-3-1 JVN iPedia登録状況（公表年別）
（出典）JVN iPediaの登録情報を基にIPAが作成

JVN iPediaは、発見された脆弱性の種類を識別するための共通脆弱性タイプ一覧（CWE：Common Weakness Enumeration）※186を脆弱性対策情報に付与して登録を行っている。2021年に登録したCWEの割合は「クロスサイト・スクリプティング」が9.2%と最も高く、「不適切な権限管理」が6.8%、「境界外書き込み」が5.4%、「情報漏えい」が2.7%と続いている（次ページ図1-3-2）。

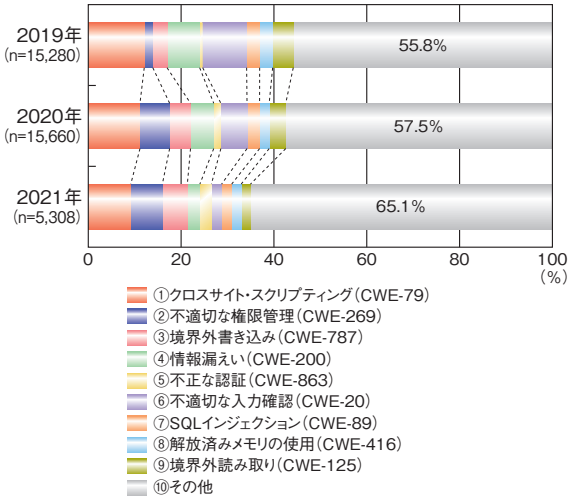
最も件数の多かった「クロスサイト・スクリプティング」に分類される脆弱性を悪用されると、偽のWebサイトへ

誘導され、情報が漏えいしたりする恐れがある。

2019 年以降の CWE 別割合を年別に見ると、上位 5 種では、「クロスサイト・スクリプティング」「情報漏えい」の割合が減少傾向にあり、「不適切な権限管理」「境界外書き込み」「不正な認証」の割合は増加傾向である（図 1-3-3）。一方で、上位 9 種と、10 位以下をまとめた「その他」の割合を見ると、上位 9 種については「不適切な入力確認」を始め、2020 年に比べて減少したものが多い。これに対して、「その他」の割合が 2021 年は 65.1%と 2020 年の 57.5%から増加している。この増加の一因としては、JVN iPedia の情報の収集元である NVD において、近年 CWE を細分化して採番する傾向があることが挙げられる。このため、これまで 9 種の CWE に分類されていた脆弱性の一部が「その他」に分類され、



■図 1-3-2　JVN iPedia における脆弱性対策情報の CWE 別割合（2021 年、n=5,308）
（出典）JVN iPedia の登録情報を基に IPA が作成



■図 1-3-3　JVN iPedia における脆弱性対策情報の CWE 別割合（2019 ～ 2021 年）
（出典）JVN iPedia の登録情報を基に IPA が作成

「その他」の採番が増えたと考えられる。

(b) JVN iPedia の登録情報の深刻度

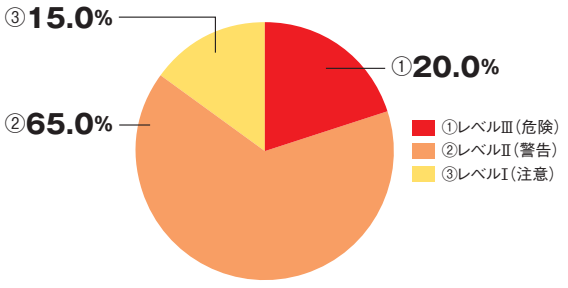
JVN iPedia は、オープンで汎用的な脆弱性評価手法である CVSS（Common Vulnerability Scoring System：共通脆弱性評価システム）[※187] を用いて、脆弱性の深刻度を公開している。なお、JVN iPedia では CVSS v2 及び CVSS v3 の二つのバージョンの情報を公開しているが、本項では CVSS v2 を基に統計処理を行っている。

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。

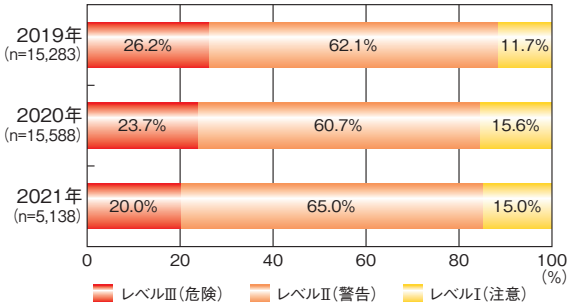
2021 年に登録された脆弱性対策情報を深刻度のレベル別で分類すると、レベルIIIが 20.0%、レベルIIが 65.0%、レベルIが 15.0%となっており、一部の情報漏えいやサービス停止につながるレベルII以上の脆弱性が全体の 8 割以上を占めている（図 1-3-4）。



■図 1-3-4　JVN iPedia における脆弱性対策情報のレベル別割合（2021 年、n=5,138）
（出典）JVN iPedia の登録情報を基に IPA が作成

2019 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 2019 年が 88.3%、2020 年が 84.4%と減少したが、2021 年は 85.0%とほぼ横ばいであった。更に 2021 年を 2020 年と比較すると、

最も深刻度が高いレベルⅢに該当する脆弱性の割合が3.7%減少し、レベルⅡの脆弱性の割合はその分増加している（図 1-3-5）。これは、比較的レベルⅡに分類されることが多い「不正な認証（CWE-863）」の脆弱性が増加したことや、全体の 65.1%を占める「その他」の脆弱性がレベルⅡに分類されることが多かっ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（2019 ～ 2021 年）
（出典）JVN iPedia の登録情報を基に IPA が作成

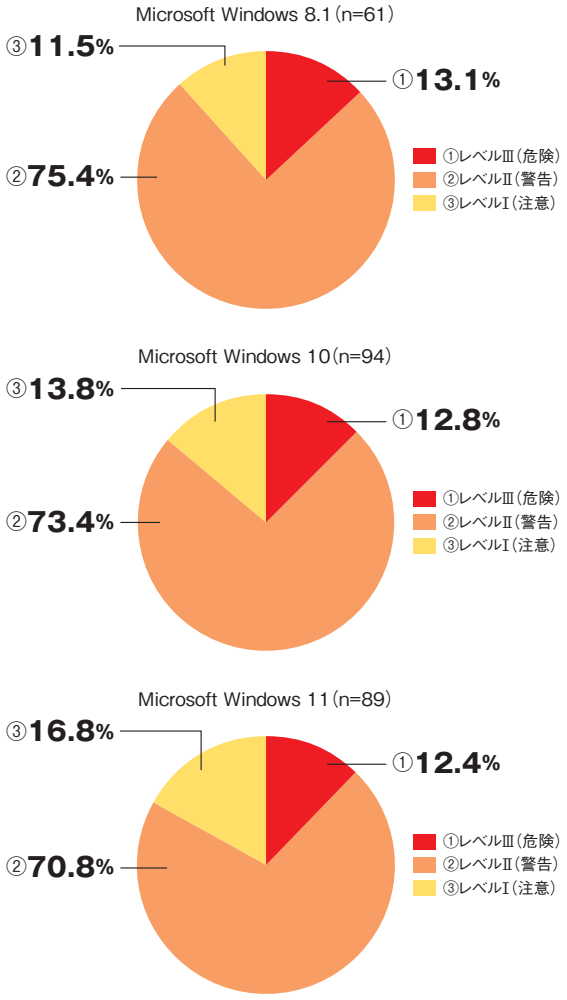
製品開発者は、ソフトウェアの企画・設計・製造段階からセキュアコーディング※188 を含めたセキュリティ対策を講じる等、脆弱性による被害を未然に防ぐための対応が必要となる。また、製品の利用者にも、日頃から新たに公開される脆弱性対策情報に注意を払い、脆弱性が公開された場合には製品を最新バージョンにアップデートする等の対応が求められる。

(2) Microsoft Windows 11 の脆弱性について

Microsoft 社より、Windows 11 が 2021 年 10 月 5 日（日本時間）にリリースされた。本製品は Windows 10 の後継バージョンとして注目を集め、無償でアップグレードできるため、徐々に利用者が増えている。同社は、Windows 11 は様々な新機能に加え、「何も信頼しない」を前提に対策を講じるゼロトラストの考え方を取り入れる等、セキュリティ面も強化したとしている※189。

その一方で、Windows 11 において既に多くの脆弱性が公開されている。リリースから 2021 年 12 月末までに、89 件の Windows 11 の脆弱性対策情報が JVN iPedia に登録された。その中には、深刻度の高い脆弱性も含まれている。図 1-3-6 は、2021 年第 4 四半期（10 月 1 日～ 12 月 31 日）に JVN iPedia へ登録された、現在 Microsoft 社でサポートされている Windows 8.1、Windows 10、Windows 11 の脆弱性対策情報の深刻度のレベル別割合である。

Windows 11 においては、脆弱性の深刻度が最も高



■図 1-3-6　JVN iPedia に登録された Microsoft Windows 製品の脆弱性対策情報の深刻度のレベル別割合（2021 年 10 ～ 12 月）
（出典）JVN iPedia の登録情報を基に IPA が作成

いレベルⅢが 12.4%、次に高いレベルⅡが 70.8%、レベルⅠが 16.8%である。レベルⅢ及びレベルⅡにあたる脆弱性が全体の 8 割以上を占めており、Windows 8.1、Windows 10 と比較して深刻度のレベル別割合に大きな差は見られなかった。このことから、2022 年以降も Windows 11 の脆弱性対策情報は、これまでの Windows OS と同様の傾向で公開されると見られる。

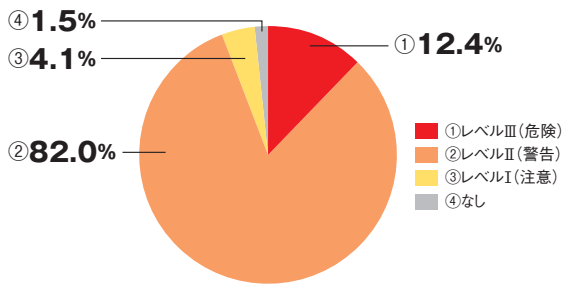
これらの脆弱性を解消し安全に Windows 11 を利用するためには、利用者は従来の Windows 製品と同様に Microsoft 社から公開される修正プログラムを速やかに適用することが推奨される。IPA においても、同社から月例の修正プログラムが公開された際、重要なセキュリティ情報として注意喚起情報を公開しており、特に脆弱性攻撃が確認されている場合は緊急対策情報として発信している。

(3) Apache HTTP Server の脆弱性について

2021 年 10 月に、Apache Software Foundation から Apache HTTP Server の脆弱性 CVE-2021-41773 の情報が公開され、IPA を始め複数の公的機関から脆弱性の悪用が確認されたとして注意喚起が発信された※190。本脆弱性はドキュメントルート外のファイルにアクセスされる恐れのあるパストラバーサルの脆弱性で、これを悪用されるとリモートから不正にファイルを操作される恐れがあった。脆弱性の深刻度を示す CVSS v2 基本値は 4.3※191 でレベルⅡにあたり、特別高い数値ではなかった。しかし、複数の実証コードが公開され、国内での攻撃が確認されたこともあり、脆弱性の影響を受けるバージョンを利用している組織は対策が求められた。

また、CVE-2021-41773 の修正版としてリリースされたバージョンの Apache HTTP Server にも、数日で別のパストラバーサルの脆弱性 CVE-2021-42013 が存在することが明らかになった。本脆弱性の CVSS v2 基本値は 7.5※192 で、レベルⅢに分類された。CVE-2021-41773 と同様に本脆弱性も実証コードの公開が確認され、また、CVE-2021-41773 の修正版のリリース直後に発見された脆弱性ということもあり、ネット記事等にも掲載され※193、広く注目された。

Apache HTTP Server は Apache Software Foundation がオープンソースソフトウェアとして提供している Web サーバ用のプログラムである。本製品の脆弱性対策情報は、JVN iPedia に 2021 年末までの累計で 194 件登録されている。図 1-3-7 はその深刻度別割合を示したものである。脆弱性の深刻度が最も高いレベルⅢが 12.4%、次に高いレベルⅡが 82.0%、レベルⅠが 4.1% となっており、脆弱性を悪用された場合の影響が大きい、レベルⅢ及びレベルⅡでほぼ占められている。



■図 1-3-7　JVN iPedia に登録された Apache HTTP Server の脆弱性対策情報のレベル別割合(2007 年 4 月～ 2021 年 12 月、n=194)
(出典)JVN iPedia の登録情報を基に IPA が作成

Apache HTTP Server のように広く利用されているソフトウェアは、脆弱性情報が公開されると攻撃者の注目も集まり、攻撃に悪用される恐れがある。利用者においては、継続的に脆弱性情報を収集し、修正プログラムが公開された場合は速やかに対応することが求められる。

(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、2021 年 12 月末時点で 13 万件を超えている。2017 年以降は毎年 1 万件前後の脆弱性対策情報が登録されており、2022 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 年は、2020 年に引き続き新型コロナウイルス感染への対応を迫られる年であった。対応の施策として、この間急速にテレワークの普及が進んだが、これに伴いテレワーク機器の脆弱性等を狙った攻撃も報告された※194。テレワーク対応のため急遽導入した機器については、業務の早期開始を重視した結果、脆弱性の管理がされていない等セキュリティに対して十分対応できないという課題が明らかになり、機器の運用管理の見直しが必要になった。

一方、2019 年の「情報処理の促進に関する法律の一部を改正する法律案」の閣議決定※195 等をきっかけに、DX (デジタルトランスフォーメーション) の考え方が注目されるようになり、組織においては業務の DX 化が求められるようになった。2022 年はテレワークに伴う業務のデジタル化が加速し、更に DX 導入が進展すると考えられる。これに伴い、AI (Artificial Intelligence：人工知能) や IoT 機器等を活用して DX 化を推進する様々な機器やソフトウェア、サービスが提供されると考えられる。このような DX 対応の機器やソフトウェアの導入にセキュリティ研究者や攻撃者が関心を持ち、新たな脆弱性を発見し、JVN iPedia 等の脆弱性対策情報データベースにおいて登録が増えることも予想される。

DX 化を推進する機器やソフトウェアの新たな脆弱性が発見されれば、それを狙った攻撃が増えると想定される。一方で、テレワーク対応機器の導入においては既知の脆弱性が放置され、被害が出た等の事例があり、DX 化を推進するための機器やソフトウェアの導入についても同様の問題が懸念される。これを防ぐために、導入した機器を構成するソフトウェア及びそのバージョンの把握、当該バージョンが影響を受ける脆弱性情報等の定期的な入手、アップデート対応等、基本的な脆弱性対策を適切に行っていくことを強く推奨する。その中の当該バージョンが影響を受ける脆弱性情報等の定期的な入手の一つの手段として、JVN iPedia をぜひ活用し

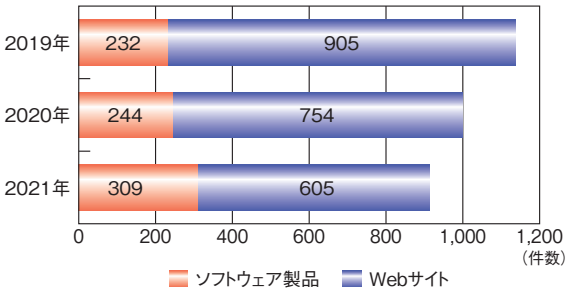
ていただきたい。

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）※196 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、2021 年も引き続き発生している。

社会的に大きな影響を与える恐れのある脆弱性については、開発者以外に関係機関から注意喚起等が出されることがある。例えば、2021 年 12 月には、多くの製品やソフトウェアで使用され、任意のコードが実行可能な Java ベースのロギングライブラリ Apache Log4j の脆弱性について、IPA 以外にも NISC 等複数機関から注意喚起※197 が出された。

「情報セキュリティ早期警戒パートナーシップ※198」（以下、パートナーシップ）では、脆弱性関連情報の届出※199 を受け付けているが、2021 年に届出された件数は、ソフトウェア製品が 309 件、Web サイトが 605 件、合計 914 件であった（図 1-3-8）。

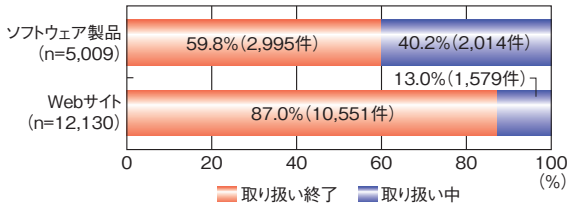


■図 1-3-8　脆弱性関連情報の種類別届出状況（2019 ～ 2021 年）
（出典）パートナーシップの届出状況を基に IPA が作成

2021 年のソフトウェア製品及び Web サイトの総届出件数（914 件）と、2020 年の件数（998 件）を比較すると、約 8% 減少している。なお、2021 年のソフトウェア製品と Web サイト個々の件数を 2020 年の件数と比較すると、ソフトウェア製品の届出は約 27% 増加、Web サイトの届出は約 20% 減少した。

パートナーシップ開始時点（2004 年 7 月 8 日）からの届出件数を累計すると、ソフトウェア製品は 5,009 件、Web サイトは 1 万 2,130 件となり、2021 年 12 月末時点での合計が 1 万 7,139 件に上る。これらの届出のうち IPA での取り扱いが終了※200 した届出件数は、ソフトウェア製品 2,995 件（59.8%）、Web サイト 1 万 551 件（87.0%）である（図 1-3-9）。

パートナーシップには、製品開発者と連絡が取れず進



■図 1-3-9　脆弱性関連情報の種類別取り扱い終了状況
（2021 年末までの累計）
（出典）パートナーシップの届出状況を基に IPA が作成

展が望めない届出（調整不能案件）を公表する手続きとして、公表判定委員会※201 がある。2021 年は、公表判定委員会の判定の結果、10 件の調整不能案件を JVN で公表した（「1.3.2 (1) (c) 公表判定委員会の判定による JVN 公表」参照）。

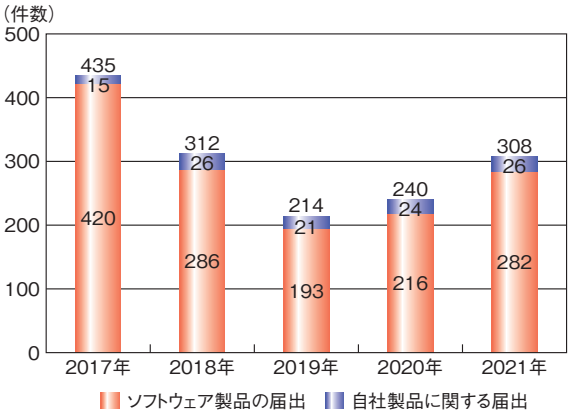
(1) ソフトウェア製品の脆弱性

2021 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) 2021 年のパートナーシップの届出受付動向

2021 年にパートナーシップで受け付けたソフトウェア製品の届出（不受理 1 件を除く）は、308 件であった。

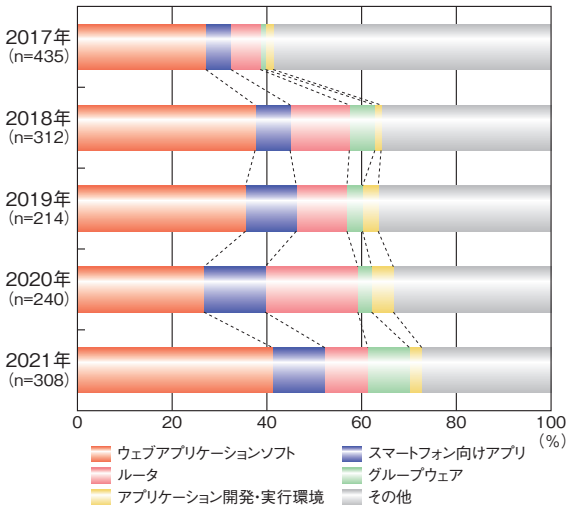
図 1-3-10 は、2017 年から 2021 年までのソフトウェア製品の届出受付数（不受理を除く）を示している。届出受付数は、2017 年の 435 件から 2019 年の 214 件まで減少したが、2020 年は 240 件、2021 年は 308 件と増えてきている。2021 年のソフトウェア製品の届出のうち、製品開発者による自社製品に関する届出は、308 件中 26 件であった。



■図 1-3-10　ソフトウェア製品の届出受付数（2017 ～ 2021 年）
（出典）パートナーシップの届出状況を基に IPA が作成

図 1-3-11（次ページ）は、同期間の製品の種類別の届出受付数の割合を示している。2021 年に割合が大き

く増加したものは「ウェブアプリケーションソフト※202」と「グループウェア」であった。「ウェブアプリケーションソフト」は41.2%と直近5年で最も大きな割合となっている。また、「グループウェア」は前年の2.9%から約3倍の8.8%になった。

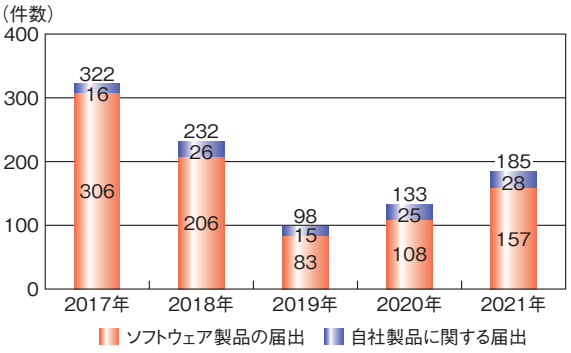


■図1-3-11　製品種類別のソフトウェア製品の届出受付数の割合（2017～2021年）
（出典）パートナーシップの届出状況を基にIPAが作成

(b) 2021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の対策情報のうち2021年にJVN公表に至った件数は、185件であった。

図1-3-12は、届出のうち2017年から2021年までのJVN公表数を示している。2017年から2019年までJVN公表数は減少していたが、2020年からは一転して増加している。また2021年に公表した自社製品に関する届出は28件であった。



■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（2017～2021年）
（出典）パートナーシップの届出状況を基にIPAが作成

2021年は、Webサイト構築に使用されるCMS（Content Management System）の脆弱性に関するJVN公表が31件あった。

CMSは、Webサイトのコンテンツの作成・管理に使用されるソフトウェア製品である。CMSの特徴として、「プラグイン」と呼ばれる拡張ソフトウェア製品を導入することで、機能の拡張が容易であることが挙げられる。CMSとプラグインを利用することで、Webサイトの運営者に専門知識がなくても、自組織のニーズに合わせたWebサイトの作成・管理が可能となる。代表的なCMSとしてはWordPressやMovable Type、EC-CUBE等が挙げられる。

2021年にJVNに公表したEC-CUBEに関連した対策情報を見ると、EC-CUBE本体だけでなく、プラグインも含めて脆弱性が発見されており（表1-3-1）、8件中6件がクロスサイト・スクリプティングの脆弱性であった。

項番	JVN番号	件名
1	JVN#97554111	EC-CUBEにおけるクロスサイトスクリプティングの脆弱性
2	JVN#79254445	複数のETUNA製 EC-CUBE用プラグインにおけるクロスサイトスクリプティングの脆弱性
3	JVN#57524494	複数のイーシーキューブ製EC-CUBE用プラグインにおける複数のクロスサイトスクリプティングの脆弱性
4	JVN#95292458	EC-CUBEにおける複数のクロスサイトスクリプティングの脆弱性
5	JVN#57942445	EC-CUBEにおけるアクセス制限不備の脆弱性
6	JVN#46313661	EC-CUBE用プラグイン「一覧画面（受注管理）項目変更プラグイン」におけるクロスサイトスクリプティングの脆弱性
7	JVN#23406150	EC-CUBE用プラグイン「注文ステータス一括変更プラグイン」におけるクロスサイトスクリプティングの脆弱性
8	JVN#75444925	EC-CUBE 2系における複数の脆弱性

■表1-3-1　2021年にJVN公表した「EC-CUBE」に関連した脆弱性対策情報
（出典）JVNを基にIPAが作成

公表した脆弱性の中でも、影響が大きいものとしてJVN#97554111※203がある。これは、EC-CUBE本体にクロスサイト・スクリプティングの脆弱性が存在したため、EC-CUBEを用いて作成したECサイトにおいて、攻撃者が特定の入力欄にスクリプトを入力することにより、ECサイト管理者のWebブラウザ上で任意のスクリプトが実行される可能性がある、というものであった。また、この脆弱性を悪用した攻撃が確認されており、実際にクレジットカード情報が流出したため注意喚起が出された※204。

CMSの脆弱性対策としては、CMS本体やそのプラ

グインを、常に最新の状態に維持（アップデート）することが重要である。アップデートをするためには、JVN や製品開発者の Web サイト等を確認し、脆弱性対策情報やアップデート情報が新たに公表されていないか定期的に確認しなければならない。また、開発・サポートが終了したプラグインについては、使用をやめる必要がある。

このようなアップデート情報の確認やアップデートの適用作業等が負担となる場合には、Web サイトの運用・保守作業を委託することや、CMS 本体を、自動アップデート機能を持つクラウド版に置き換えることも一つの方策となる。

(c) 公表判定委員会の判定による JVN 公表

パートナーシップでは、原則として、製品開発者の合意のもとで、脆弱性対策情報を JVN で公表しているが、届出の中には、製品開発者との連絡が取れない等の様々な理由により、公表に向けての調整が難航してしまう調整不能案件が存在する。

製品利用者が被害を受ける可能性を低減するため、IPA では、調整不能案件の脆弱性情報について、公表が適当か否かを判定する第三者委員会である「公表判定委員会」を組織している。

2021 年には、同委員会での判定に基づき、10 件の脆弱性情報を JVN に公表した（表 1-3-2）。JVN での調整不能案件の公表は 2020 年の 9 件に続き、2 年連続となった。また、公表した 10 件のうち 9 件は、深刻度の 3 段階レベルのうちレベルⅡの「警告」と判断され、残りの 1 件はレベルⅠの「注意」と判断された。

公表した脆弱性は、いずれも製品開発者と連絡が取れないことを理由に調整不能となったもので、アップデート等の対策は提供されていない。また、IPA において届出情報を基に製品を検証しており、脆弱性が存在することが確認されている。利用者には脆弱性を回避する対策として、製品の使用をやめることが求められる。

項番	JVN 番号	深刻度	件名
1	JVN#97370614	警告	マガジンガーZにおけるクロスサイトスクリプティングの脆弱性
2	JVN#12559271	警告	影舞におけるクロスサイトスクリプティングの脆弱性
3	JVN#42220311	警告	影舞におけるクロスサイトスクリプティングの脆弱性
4	JVN#11438679	注意	影舞におけるクロスサイトリクエストフォージェリの脆弱性
5	JVN#93207949	警告	Click Ranker におけるクロスサイトスクリプティングの脆弱性
6	JVN#37179202	警告	Yomi-Search におけるクロスサイトスクリプティングの脆弱性
7	JVN#83042295	警告	Yomi-Search におけるクロスサイトスクリプティングの脆弱性
8	JVN#94705238	警告	Yomi-Search におけるクロスサイトスクリプティングの脆弱性
9	JVN#68244135	警告	rNote におけるクロスサイトスクリプティングの脆弱性
10	JVN#55833077	警告	yappa-ng におけるクロスサイトスクリプティングの脆弱性

■表 1-3-2　2021 年に JVN 公表した調整不能案件
（出典）JVN を基に IPA が作成

(d) 製品開発者の脆弱性対策に関する取り組み

IPA とともにパートナーシップを運営している JPCERT/CC は、インシデント報告や脆弱性報告で顕著な貢献をした報告者を顕彰するための「ベストレポーター賞※205」を 2021 年に制定し、同年に初の贈呈を実施した。

同賞の脆弱性報告部門では、トレンドマイクロ社が製品開発者の脆弱性対応の取り組みとして、社内外で発見された自社製品の脆弱性について、その悪用の有無を含め多数報告し、脆弱性情報流通に対して前向きに対処、協力している姿勢が評価され受賞した。

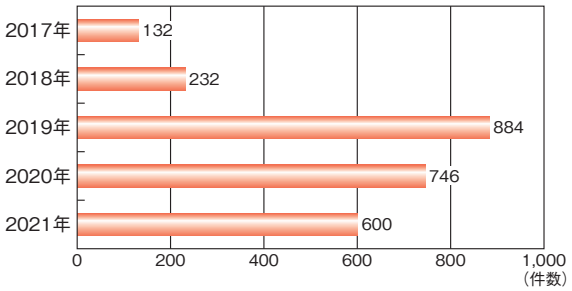
パートナーシップでは、製品開発者からの自社製品の脆弱性の届出も受け付けているが、2021 年の自社製品の届出は 26 件と多くない。

製品開発者から自社製品の脆弱性について報告が増えることで、製品開発者側での公表や JVN での公表も増え、より多くの利用者に対策情報が認識されるようになり、脆弱性悪用の被害が低減することが今後期待される。

(2) Web サイト※196 の脆弱性

2021 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 5 件を除く）は、600 件であった。

図 1-3-13 は、2017 年から 2021 年までの Web サイトの届出受付数（不受理を除く）を示している。前年を大きく上回る 2019 年の 884 件をピークに、2020 年より届出

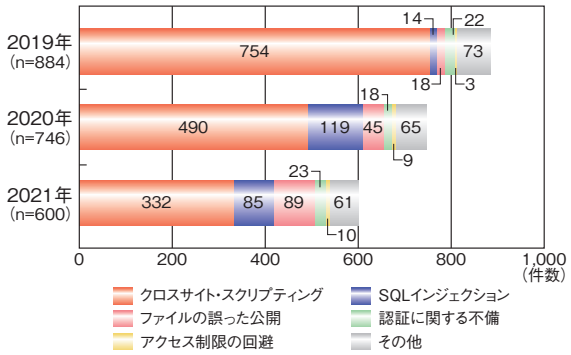


■図 1-3-13　Web アプリケーションの不受理を除いた届出件数（2017 ～ 2021 年）
（出典）パートナーシップの届出状況を基に IPA が作成

は減少してきている。

(a) パートナーシップから見る 2021 年の届出の傾向

図 1-3-14 は、2019 年から 2021 年までの脆弱性の種類別の届出受付数（不受理を除く）を示している。2020 年では届出全体に対する割合が多かった「クロスサイト・スクリプティング」と「SQL インジェクション」は、2021 年では減少した。他方、2021 年に増加したものに、「ファイルの誤った公開」がある。この脆弱性の 2021 年届出数は 89 件であり、2020 年の 45 件と比較すると 2 倍に増加した。これは、2004 年の制度開始から 2021 年までの間で当該脆弱性に関して最も多い件数である。



■図 1-3-14　脆弱性種類別の Web アプリケーションの届出受付数（2019 ～ 2021 年）
（出典）パートナーシップの届出状況を基に IPA が作成

「ファイルの誤った公開」は 2018 年当時からあり、決して少なくない。そのため同年の第 4 四半期の「ソフトウェア等の脆弱性関連情報に関する届出状況[※206]」では「機密情報の意図しない公開に注意」と題して、Web サイト運営者に注意を促していた。

しかしながら、その後も数の増減はあるもののパートナーシップには毎年一定数届出されている。前述のとおり、2021 年はこれまでで最多であり、依然としてこの脆弱性が残存する Web サイトが多数あると考えられる。

(b)「ファイルの誤った公開」の脆弱性の現状

「ファイルの誤った公開」とは、Web サイトの管理・運用においてアクセス制限等の設定不備により、意図せずファイルにアクセスされてしまう問題であり、このファイルに保存されている管理者権限のアカウントやパスワードが外部に流出すると、第三者に悪用され被害が深刻化する等の脅威が発生する。ディレクトリ・トラバーサルのようなソフトウェアの設計に起因する問題とは異なり、基本的には Web サイト運営者による不適切な運用の問題に起因する。

パートナーシップでは、このような問題についても、脆弱性の一種と定義し取り扱っている。

2021 年のパートナーシップに届出があった「ファイルの誤った公開」の主な要因は、CMS のような「ウェブアプリケーションソフト」を初期設定のまま使用し構築した問題であった。それにより Web サイトでは、公開領域に機密情報が含まれるファイルが生成、配置される作りとなっていた。

上記は「ウェブアプリケーションソフト」の仕様であり、この仕様に気が付かずそのまま運用していたため、意図せず機密情報が含まれるファイルが誰でもアクセスできるようになっており、その多くは検索エンジンから特定のキーワードで検索することにより、アカウント情報を含む機密情報が公開状態にあることを容易に知ることができたというものであった。

(c) Web サイト運営者に求められる対策

前述のとおり、「ファイルの誤った公開」の届出では、「ウェブアプリケーションソフト」の仕様を確認しないまま利用していたため、非公開にすべきファイルが公開されているという届出が多数を占めていた。

まず、Web サイト運営者は「ウェブアプリケーションソフト」の現状の設定を確認していただきたい。併せて、IPA が公開している「安全なウェブサイトの運用管理に向けての 20 ヶ条[※207]」や「Web サーバからのファイル流出対策[※208]」等を参考にして、非公開にすべきファイルが公開されていないか、設定やファイルの配置場所等を見直すことも必要である。

なお、Web サイト運営者が自組織で確認できない場合は、セキュリティベンダに脆弱性診断を依頼する等の対応が考えられる。

問題を確認した場合は、公開しているファイルを速やかに非公開設定にする。加えて、漏えいが疑われる情報は、検索エンジンでキャッシュされている場合があるため、各検索エンジンを運営する事業者へ問題となったページやファイルのキャッシュ情報の削除を依頼する等の対応を検討いただきたい。

また、クロスサイト・スクリプティングや SQL インジェクション等の脆弱性についても、未だに多くの届出がある。Web サイト運営者は、ページの新規追加や変更を行う際に、IPA が公開している「ウェブ健康診断仕様[※150]」「安全なウェブサイトの作り方[※151]」等を参照して、運営する Web サイトの現状を確認し、対策や見直しを検討いただきたい。

COLUMN

多様化する「だまし」の手口に対抗するには

IPAの「情報セキュリティ安心相談窓口」には日々様々な相談が寄せられています。中でも、「偽サイトや不審サイトにアクセスして、大事な情報をサイトに入力した」「不審なアプリをサイトからインストールした」という相談が多く寄せられています。

そのような偽サイトや不審サイトへの誘導方法としては、メールやSMSを不特定多数にばらまく手法が従来の代表的な手口です。しかし、最近では、それ以外の方法により偽サイトや不審サイトへ誘導する手口の相談も増えており、「だまし」の手口が多様化しているといえる状況です。例えば、「スマートフォンのカレンダー機能」「SNSのメッセージ機能」「ブラウザの通知機能」等を悪用して、ユーザが利用する端末に不審なURLを送り付ける手口も確認しています。これらのどの手口においても、基本的にはURLリンクをタップ／クリックすることで被害につながります。URLをタップ／クリックさえしなければ被害につながることはありません（図1）。

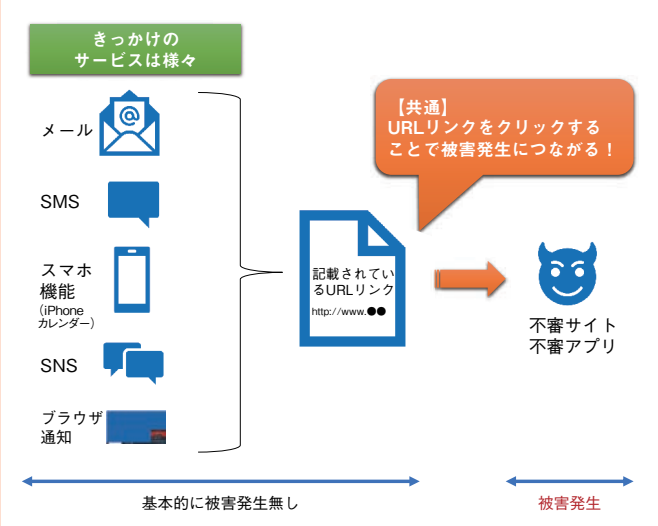


図1　URLリンクからの被害発生のイメージ

これらの手口があることを知っていれば、実際にそのような場面に遭遇しても、怪しいことに気が付き、被害の発生を防げる可能性が高まります。そのため情報セキュリティ安心相談窓口では、以下の情報発信を行っています。

- 「Twitter安心相談窓口公式アカウント」（https://twitter.com/IPA_anshin）では新たな手口が確認された場合に速やかに情報を提供しています。
- 「安心相談窓口だより」（https://www.ipa.go.jp/security/anshin/mgdayoriindex.html）では確認された手口と対処、被害に遭わないための対策等を分かりやすく詳細に説明しています。

「だまし」の手口に引っかからないように、「Twitter公式アカウント」をフォローして、「安心相談窓口だより」を定期的にチェックしてください。

※ 1　https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf〔2022/5/17 確認〕
※ 2　https://apwg.org/trendsreports/〔2022/5/17 確認〕
※ 3　https://www.verizon.com/business/resources/reports/dbir/〔2022/5/27 確認〕
※ 4　https://www.ibm.com/security/jp-ja/data-breach/threat-intelligence/〔2022/5/17 確認〕
※ 5　CNN.co.jp：米首都のガソリンスタンド、8割が売り切れ　パイプライン停止の影響続く　https://www.cnn.co.jp/business/35170841.html〔2022/5/17 確認〕
※ 6　Microsoft 社：Microsoft Exchange Server のリモートでコードが実行される脆弱性 CVE-2021-26855　https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855〔2022/5/17 確認〕
※ 7　Microsoft 社：Microsoft Exchange Server のリモートでコードが実行される脆弱性 CVE-2021-34473　https://msrc.microsoft.com/update-guide/ja-jp/vulnerability/CVE-2021-34473〔2022/5/17 確認〕
NIST：CVE-2021-34523 Detail　https://nvd.nist.gov/vuln/detail/CVE-2021-34523〔2022/5/17 確認〕
NIST：CVE-2021-31207 Detail　https://nvd.nist.gov/vuln/detail/CVE-2021-31207〔2022/5/17 確認〕
※ 8　Orange Tsai：ProxyLogon is Just the Tip of the Iceberg, A New Attack Surface on Microsoft Exchange Server!　https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-ProxyLogon-Is-Just-The-Tip-Of-The-Iceberg-A-New-Attack-Surface-On-Microsoft-Exchange-Server.pdf〔2022/5/17 確認〕
※ 9　JVN iPedia：JVNDB-2021-005429 Apache Log4j における任意のコードが実行可能な脆弱性　https://jvndb.jvn.jp/ja/contents/2021/JVNDB-2021-005429.html〔2022/5/17 確認〕
※ 10　Solar Winds Worldwide, LLC.：SolarWinds Security Advisory　https://www.solarwinds.com/ja/sa-overview/securityadvisory〔2022/5/17 確認〕
※ 11　Reuters：Kaseya ransomware attack sets off race to hack service providers -researchers　https://www.reuters.com/technology/kaseya-ransomware-attack-sets-off-race-hack-service-providers-researchers-2021-08-03/〔2022/5/17 確認〕
Kaseya Limited：Incident Overview & Technical Details　https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961-Incident-Overview-Technical-Details〔2022/5/17 確認〕
※ 12　Verizon 社：2021 Data Breach Investigations Report　https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf〔2022/5/27 確認〕
なお、本文に記載した 2020 年のインシデント件数である 2 万 9,207 件は、7 万 9,635 件のうちの適格性の基準を満たした件数である。
※ 13　パスワード・スプレー攻撃：同じパスワードを使って複数のアカウントへのログインを試みる攻撃手法。ログイン制御が施されているシステムに対して、同じアカウントへの複数回のログイン試行を回避できる。
※ 14　IBM 社：X-Force 脅威インテリジェンス・インデックス 2021 エグゼクティブ・サマリー　https://www.ibm.com/downloads/cas/98Z6YYG6〔2022/5/17 確認〕
※ 15　FBI：Internet Crime Report 2020　https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf〔2022/5/17 確認〕
※ 16　「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。
※ 17　MBSD 社のご厚意により、ご提供いただいた集計情報を本白書では掲載している。
※ 18　https://www.jpcert.or.jp/ir/report.html〔2022/5/16 確認〕
※ 19　フィッシング対策協議会：月次報告書 一覧　https://www.antiphishing.jp/report/monthly/〔2022/5/16 確認〕
※ 20-1　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf〔2022/5/16 確認〕
※ 20-2「情報セキュリティ白書 2021」（https://www.ipa.go.jp/security/publications/hakusyo/2021.html〔2022/5/16 確認〕）の「1.1.2 (3) フィッシングによる被害」(p.13) 参照。
※ 20-3　JC3：フィッシングターゲットの変遷　https://www.jc3.or.jp/threats/topics/article-430.html〔2022/5/16 確認〕
※ 20-4　トレンドマイクロ社：2021 年年間セキュリティラウンドアップ　https://resources.trendmicro.com/jp-docdownload-form-m449-web-2021-annualsecurityreport.html〔2022/5/16 確認〕
※ 21　https://www.ipa.go.jp/security/event/2013/isec-semi/documents/2013videosemi_targeted_cyber_attacks_v1.pdf〔2022/4/18 確認〕
※ 22　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。
※ 23　ITmedia NEWS：ベラルーシのハクティビスト、ロシア軍阻止目的で国鉄にランサムウェア攻撃と声明　https://www.itmedia.co.jp/news/articles/2201/25/news080.html〔2022/4/18 確認〕
※ 24　JPCERT/CC：JPCERT/CC インシデント報告対応レポート〔2021 年 7 月 1 日～ 2021 年 9 月 30 日〕　https://www.jpcert.or.jp/pr/2021/IR_Report20211014.pdf〔2022/4/18 確認〕
※ 25　JPCERT/CC：短縮 URL から VBScript をダウンロードさせるショートカットファイルを用いた攻撃　https://blogs.jpcert.or.jp/ja/2019/07/shorten_url_lnk.html〔2022/4/18 確認〕
※ 26　NTT セキュリティ株式会社：標的型攻撃グループ CryptoMimic の攻撃手法の変化について　https://insight-jp.nttsecurity.com/post/102gpur/cryptomimic〔2022/4/18 確認〕
※ 27　三菱電機株式会社：不正アクセスによる個人情報と企業機密の流出可能性について　https://www.mitsubishielectric.co.jp/news/2020/0120-b.pdf〔2022/4/18 確認〕
※ 28　三菱電機株式会社：不正アクセスによる個人情報と企業機密の流出可能性について（第 3 報）　http://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf〔2022/4/18 確認〕
※ 29　防衛省：三菱電機株式会社に対する不正アクセスによる安全保障上の影響に関する調査結果について　https://www.mod.go.jp/j/press/news/2021/12/24c.pdf〔2022/4/18 確認〕
※ 30　三菱電機株式会社：不正アクセスによる個人情報と企業機密の流出可能性について（第 4 報）　http://www.mitsubishielectric.co.jp/news/2021/1224.pdf〔2022/4/18 確認〕
※ 31　https://piyolog.hatenadiary.jp/entry/2020/01/20/172436〔2022/4/18 確認〕
※ 32　報道によると Trend Micro ウイルスバスター法人向け製品の脆弱性を悪用されたとのこと。当時は未公開であったが、2022 年時点では修正パッチが提供されている。
ZDNet：Two Trend Micro zero-days exploited in the wild by hackers　https://www.zdnet.com/article/two-trend-micro-zero-days-exploited-in-the-wild-by-hackers/〔2022/4/18 確認〕
※ 33　TechCrunch：US says Iran-backed hackers are now targeting organizations with ransomware　https://techcrunch.com/2021/11/17/cisa-iran-hackers-ransomware/〔2022/4/18 確認〕
Security Affairs：China-linked APT used Pulse Secure VPN zero-day to hack US defense contractors　https://securityaffairs.co/wordpress/117060/apt/pulse-secure-vpn-zeroday-attacks.html〔2022/4/18 確認〕
※ 34　IPA：情報セキュリティ白書 2021　https://www.ipa.go.jp/security/publications/hakusyo/2021.html〔2022/4/18 確認〕
※ 35　Cybersecurity and Infrastructure Security Agency（CISA）：FBI-CISA Joint Advisory on Exploitation of Fortinet FortiOS Vulnerabilities　https://www.cisa.gov/uscert/ncas/current-activity/2021/04/02/fbi-cisa-joint-advisory-exploitation-fortinet-fortios〔2022/4/18 確認〕
※ 36　IPA：IPA 脆弱性対策コンテンツリファレンス　https://www.ipa.go.jp/files/000051352.pdf〔2022/4/18 確認〕
※ 37　INTERNET Watch：カスペルスキー、マルウェア「LODEINFO」の亜種が観測されたと発表　https://internet.watch.impress.co.jp/docs/news/1374019.html〔2022/4/18 確認〕
※ 38　シスコシステムズ合同会社：侵害された Web サイトを使用した新しいキャンペーンで ObliqueRAT が復活　https://gblogs.cisco.com/jp/2021/03/talos-obliquerat-new-campaign/〔2022/4/18 確認〕
※ 39　一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会：What's CSIRT？　https://www.nca.gr.jp/imgs/CSIRT.pdf〔2022/4/18 確認〕
※ 40　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/security/announce/2020-ransom.html〔2022/4/18 確認〕
※ 41　株式会社 FFRI セキュリティ：標的型ランサムウェアの脅威　https://www.ffri.jp/blog/2020/06/2020-06-29-Targeted-ransomware-threat.htm〔2022/4/18 確認〕
※ 42　株式会社カスペルスキー：ランサムウェアを操る脅迫犯、盗んだデータを公開　https://blog.kaspersky.co.jp/ransomware-data-disclosure/26862/〔2022/4/18 確認〕
※ 43　NISC：ランサムウエアによるサイバー攻撃について【注意喚起】　https://www.nisc.go.jp/pdf/policy/infra/ransomware20201126.pdf〔2022/4/18 確認〕
※ 44　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　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf〔2022/4/18 確認〕
※ 45　日本経済新聞：ハッカーに狙われたトヨタの部品　小島プレスがなぜ　https://www.nikkei.com/article/DGXZQOUC0319Y0T00C22

A3000000/〔2022/4/18 確認〕
※ 46 トレンドマイクロ社：闇市場とサイバー犯罪：「RaaS」ランサムウェアのサービス化 https://blog.trendmicro.co.jp/archives/17416〔2022/4/18 確認〕
※ 47 トレンドマイクロ社：ランサムウェア「Cring」の被害が国内で拡大、VPN 脆弱性を狙い侵入 https://blog.trendmicro.co.jp/archives/27830〔2022/4/18 確認〕
※ 48 ESET：ESET サイバーセキュリティ脅威レポート 2021 年第 2 三半期版を公開 ～侵入口として悪用される RDP/ オリンピック期間中の動向も～ https://www.eset.com/jp/blog/threat-report/2021-t2/〔2022/4/18 確認〕
※ 49 NHK：病院がサイバー攻撃を受けたとき 消えた電子カルテの衝撃 https://www3.nhk.or.jp/news/special/sci_cul/2021/11/special/story_20211119〔2022/4/18 確認〕
MBS：サイバー攻撃と戦った公立病院の 2 か月間『電子カルテが暗号化』過去の検査結果も病歴もわからず ... 手書き対応にも苦労 https://www.mbs.jp/4chantv/news/kodawari/article/2022/01/087200.shtml〔2022/4/18 確認〕
MBS：【特集】サイバー攻撃と戦った公立病院の2か月間『電子カルテが暗号化』過去の検査結果も病歴もわからず ... 手書き対応にも苦労（2021 年 1 月 6 日） https://www.youtube.com/watch?v=eb8RLIlaBn4〔2022/4/18 確認〕
MBSD：ランサムウェア「LockBit2.0」の内部構造を紐解く https://www.mbsd.jp/research/20211019/blog/〔2022/4/18 確認〕
日本経済新聞：身代金払わず 2 億円で新システム 徳島サイバー被害病院 https://www.nikkei.com/article/DGXZQOUE25C3L0V21C21A1000000/〔2022/4/18 確認〕
※ 50 株式会社ニップン：ウィルス攻撃感染被害によるシステム障害発生のお知らせ https://www.nippn.co.jp/topics/detail/__icsFiles/afieldfile/2021/07/09/20210709system.pdf〔2022/4/18 確認〕
株式会社ニップン：システム障害発生のお知らせ（続報） https://www.nippn.co.jp/topics/detail/__icsFiles/afieldfile/2021/08/16/20210816.pdf〔2022/4/18 確認〕
株式会社ニップン：2022 年 3 月期第 1 四半期報告書の提出期限延長に関する承認申請書提出のお知らせ https://www.nikkei.com/nkd/disclosure/tdnr/d2a0bf/〔2022/4/18 確認〕
ITmedia NEWS：ニップン、前例ないサイバー攻撃で延期した 1Q 決算は増収増益に 影響は「引き続き調査中」 https://www.itmedia.co.jp/news/articles/2110/29/news202.html〔2022/4/18 確認〕
ITmedia NEWS：日本の製粉大手に「前例ない」大規模攻撃 大量データ暗号化 起動不能、バックアップもダメで「復旧困難」 https://www.itmedia.co.jp/news/articles/2108/17/news121.html〔2022/4/18 確認〕
※ 51 NTT Com DD 株式会社：予測不能に進化し続けるネットワークの脅威 – 最近のランサムウェアとマルウェアはどんなもの? https://nttcdd.jp/blog/2107/〔2022/4/18 確認〕
※ 52 トレンドマイクロ社：ランサムウェア攻撃後に予期される身代金交渉の実状を解説 https://blog.trendmicro.co.jp/archives/30035〔2022/4/18 確認〕
※ 53 Avast Software s.r.o.：Magnitude Exploit Kit: Still Alive and Kicking https://decoded.avast.io/janvojtesek/magnitude-exploit-kit-still-alive-and-kicking/〔2022/4/18 確認〕
※ 54 Gigazine：ランサムウェア入り USB メモリを送りつける詐欺が増加中、データを暗号化して使用不能にし元に戻すための身代金を要求する手口 https://gigazine.net/news/20220111-cyber-criminals-mailing-usb-drives-ransomware/〔2022/4/18 確認〕
※ 55 IRM：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。
※ 56 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〔2022/4/18 確認〕
※ 57 JPCERT/CC：CSIRT：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〔2022/4/18 確認〕
※ 58 被害金額については、2015 ～ 2021 年の年次報告書（IC3：Annual Reports https://www.ic3.gov/Home/AnnualReports〔2022/4/18 確認〕）を参照した。
※ 59 トレンドマイクロ社：電子メールサービスの特性を悪用する様々なビジネスメール詐欺の手口を解説 https://blog.trendmicro.co.jp/archives/29272〔2022/4/18 確認〕
日本経済新聞：ビジネスメール詐欺が急増、トレンドマイクロ調べ https://www.nikkei.com/article/DGXZQOUC09CGM0Z01C21A2000000/〔2022/4/18 確認〕
※ 60 APWG：Phishing Activity Trends Reports 2nd Quarter 2021 https://docs.apwg.org/reports/apwg_trends_report_q2_2021.pdf〔2022/4/18 確認〕
※ 61 INTERPOL：More than 1,000 arrests and USD 27 million intercepted in massive financial crime crackdown https://www.interpol.int/News-and-Events/News/2021/More-than-1-000-arrests-and-USD-27-million-intercepted-in-massive-financial-crime-crackdown〔2022/4/18 確認〕
※ 62 INTERPOL：Nigerian cybercrime fraud: 11 suspects arrested, syndicate busted https://www.interpol.int/News-and-Events/News/2022/Nigerian-cybercrime-fraud-11-suspects-arrested-syndicate-busted〔2022/4/18 確認〕
※ 63 The Record：US arrests 33 BEC scammers linked to Nigerian crime syndicate https://therecord.media/us-arrests-33-bec-scammers-linked-to-nigerian-crime-syndicate/〔2022/4/18 確認〕
※ 64 Europol：106 arrested in a sting against online fraudsters https://www.europol.europa.eu/newsroom/news/106-arrested-in-sting-against-online-fraudsters〔2022/4/18 確認〕
※ 65 株式会社ビジョナリーホールディングス：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/9263/tdnet/2092784/00.pdf〔2022/5/19 確認〕
※ 66 加賀電子株式会社：当社米国子会社における資金流出事案について https://www.taxan.co.jp/jp/ir/upload_file/tdnrelease/8154_20210319481006_P01_.pdf〔2022/4/18 確認〕
※ 67 dongA.com：KAI, 해커 일당에 16 억원 '피싱사기' 당해… "후속 조치 협조" https://www.donga.com/news/Society/article/all/20210618/107504131/1/〔2022/4/18 確認〕
※ 68 KNUJ Radio：City of Redwood Falls victim of bank wire scam over fire truck; funds recovered https://knuj.net/2021/06/19/city-of-redwood-falls-victim-of-bank-wire-scam-over-fire-truck-funds-recovered/〔2022/4/18 確認〕
※ 69 https://www.ipa.go.jp/files/000090633.pdf〔2022/4/18 確認〕
※ 70 https://www.ipa.go.jp/files/000092808.pdf〔2022/4/18 確認〕
※ 71 https://www.ipa.go.jp/files/000094117.pdf〔2022/4/18 確認〕
※ 72 https://www.ipa.go.jp/files/000095766.pdf〔2022/4/18 確認〕
※ 73 IPA：ビジネスメール詐欺「BEC」に関する事例と注意喚起 https://www.ipa.go.jp/files/000058478.pdf〔2022/4/18 確認〕
※ 74 IPA：【注意喚起】偽口座への送金を促す"ビジネスメール詐欺"の手口（続報） https://www.ipa.go.jp/security/announce/201808-bec.html〔2022/4/18 確認〕
※ 75 Agari：Cosmic Lynx: A Russian Threat Hits the BEC Scene https://www.agari.com/email-security-blog/cosmic-lynx-russian-bec/〔2022/4/18 確認〕
※ 76 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〔2022/4/18 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〔2022/4/18 確認〕
PwC：Business-Email-Compromise-Guide https://github.com/PwC-IR/Business-Email-Compromise-Guide/blob/main/PwC-Business_Email_Compromise-Guide.pdf〔2022/4/18 確認〕
※ 77 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〔2022/4/18 確認〕
Microsoft 社：アカウントが侵害されたかどうかを Office 365 する方法 https://docs.microsoft.com/ja-jp/office365/troubleshoot/sign-in/determine-account-is-compromised〔2022/4/18 確認〕
FireEye：Obscured by Clouds：Office 365 攻撃の洞察と Mandiant Managed Defense の調査方法 https://www.fireeye.com/blog/jp-threat-research/2020/07/insights-into-office-365-attacks-and-how-managed-defense-investigates.html〔2022/4/18 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〔2022/4/18 確認〕
※ 78 NetScout Systems, Inc.：ISSUE 7: FINDINGS FROM 1H 2021 NETSCOUT THREAT INTELLIGENCE REPORT https://www.netscout.com/sites/default/files/2021-10/SECIG_015_EN-2101-Threat_Report_SP_Infographic.pdf〔2022/4/18 確認〕
※ 79 株式会社カスペルスキー：＜Kaspersky サイバー脅威調査：2020 年第 2 四半期の DDoS 攻撃＞新型コロナウイルスの流行下、DDoS 攻撃数は前年同期比の 3 倍に。人々の外出機会の減少が影響 https://www.kaspersky.co.jp/about/press-releases/2020_vir18092020〔2022/4/18 確認〕
※ 80 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。

※ 81 Microsoft 社：Azure DDoS Protection—2021 Q3 and Q4 DDoS attack trends https://azure.microsoft.com/en-us/blog/azure-ddos-protection-2021-q3-and-q4-ddos-attack-trends/〔2022/4/18 確認〕
※ 82 CDN（Content Delivery Network）：Web コンテンツを配信するために最適化されたネットワーク。オリジナルの Web コンテンツを格納するサーバである「オリジンサーバ」、代理で Web コンテンツを配信する「キャッシュサーバ」などから構成される。
※ 83 INTERNET Watch：オリンピック開始後、DDoS 攻撃が 10 倍超に増加。Cloudflare がトラフィック動向を発表 https://internet.watch.impress.co.jp/docs/news/1341736.html〔2022/4/18 確認〕
※ 84 GIGAZINE:史上最大規模の DDoS 攻撃を行う「Mēris ボットネット」が出現 https://gigazine.net/news/20210910-meris-botnet/〔2022/4/18 確認〕
※ 85 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。
※ 86 Cloudflare, Inc.：Cloudflare が 1720 万 RPS（記録上最大規模）の DDoS 攻撃を防御 https://blog.cloudflare.com/ja-jp/cloudflare-thwarts-17-2m-rps-ddos-attack-the-largest-ever-reported-ja-jp/〔2022/4/18 確認〕
※ 87 トレンドマイクロ社：2021 年年間セキュリティラウンドアップ https://resources.trendmicro.com/jp-docdownload-form-m449-web-2021-annualsecurityreport.html〔2022/4/19 確認〕
※ 88 SQL インジェクション：SQL 文の組み立てにおいて、利用者からの入力情報を基に細工された SQL 文を埋め込まれると、データベースを不正に操作されてしまう脆弱性。
※ 89 SonicWall, Inc.：CONFIRMED ZERO-DAY VULNERABILITY IN THE SONICWALL SMA100 BUILD VERSION 10.X https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001〔2022/4/19 確認〕
※ 90 FBI：CU-000154-MW: Fivehands-HelloKitty FLASH Cord Final (002) https://www.ic3.gov/Media/News/2021/211029.pdf〔2022/4/19 確認〕
※ 91 Pulse Secure, LLC.：SA44784 - 2021-04: Out-of-Cycle Advisory: Multiple Vulnerabilities Resolved in Pulse Connect Secure 9.1R11.4 https://kb.pulsesecure.net/articles/Pulse_Secure_Article/SA44784/〔2022/4/19 確認〕
※ 92 JPCERT/CC：Pulse Connect Secure の脆弱性（CVE-2021-22893）に関する注意喚起 https://www.jpcert.or.jp/at/2021/at210019.html〔2022/4/19 確認〕
※ 93 Web シェル：Web サーバに不正にアップロードされるバックドアプログラム。
※ 94 Palo Alto Networks, Inc.：ランサムウェアギャング REvil：Kaseya VSA 攻撃の背後にいる攻撃グループを理解する https://unit42.paloaltonetworks.jp/revil-threat-actors/〔2022/4/19 確認〕
※ 95 Microsoft 社：Microsoft Exchange Server Vulnerabilities Mitigations – updated March 15, 2021 https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/〔2022/4/19 確認〕
※ 96 Microsoft 社：April 2021 Update Tuesday packages now available https://msrc-blog.microsoft.com/2021/04/13/april-2021-update-tuesday-packages-now-available/〔2022/4/19 確認〕
※ 97 Volexity：Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/〔2022/4/19 確認〕
※ 98 ゼロデイ：脆弱性が発見・報告された日から、その脆弱性を解消するための手段が確立するまでの期間のこと。
※ 99 Forescout Technologies, Inc.：NAME:WRECK https://www.forescout.com/research-labs/namewreck/〔2022/4/19 確認〕
※ 100 TCP/IP スタック：IoT 機器のファームウェア等に追加されるネットワーク機能を提供するためのライブラリ。
※ 101 Forescout Technologies, Inc.：NAME:WRECK: Breaking and fixing DNS implementations https://www.forescout.com/resources/namewreck-breaking-and-fixing-dns-implementations/〔2022/4/19 確認〕
※ 102 https://jvndb.jvn.jp/〔2022/4/19 確認〕
※ 103 IPA：【注意喚起】特定の組織からの注文連絡等を装ったばらまき型メールに注意 https://www.ipa.go.jp/security/topics/alert271009.html〔2022/4/18 確認〕
※ 104 Europol：World's most dangerous malware EMOTET disrupted through global action https://www.europol.europa.eu/media-press/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action〔2022/4/18 確認〕
※ 105 IPA：「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて https://www.ipa.go.jp/security/announce/20191202.html〔2022/4/18 確認〕
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〔2022/4/18 確認〕
※ 106 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/files/000071273.pdf〔2022/4/18 確認〕
※ 107 JPCERT/CC：マルウエア Emotet の感染活動について https://www.jpcert.or.jp/newsflash/2019112701.html〔2022/4/18 確認〕
※ 108 https://www.med.or.jp/nichiionline/article/010228.html〔2022/4/18 確認〕
※ 109 Mal-Eats：日本を狙う新たな攻撃キャンペーン Campo の全体像 https://mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/〔2022/4/18 確認〕
※ 110 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2021 年 7 月～ 9 月］ https://www.ipa.go.jp/files/000094117.pdf〔2022/4/18 確認〕
デジタルアーツ株式会社：見慣れない XLL ファイル（Excel アドイン）を使う攻撃に要注意! https://www.daj.jp/webtopics/102/〔2022/4/18 確認〕
※ 111 IPA:「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて https://www.ipa.go.jp/security/announce/20191202.html〔2022/4/18 確認〕
※ 112 BleepingComputer：Microsoft fixes Windows AppX Installer zero-day used by Emotet https://www.bleepingcomputer.com/news/Microsoft/Microsoft-fixes-windows-appx-installer-zero-day-used-by-emotet/〔2022/4/18 確認〕
※ 113 IPA：安心相談窓口だより 宅配便業者に加えて通信事業者をかたる偽ショートメッセージサービス（SMS）が増加中 https://www.ipa.go.jp/security/anshin/mgdayori20211222.html〔2022/4/18 確認〕
※ 114 https://www.jc3.or.jp/threats/examples/article-409.html〔2022/4/18 確認〕
※ 115 IPA：安心相談窓口だより 安易に運転免許証など本人確認書類の写真を送信しないで! https://www.ipa.go.jp/security/anshin/mgdayori20210623.html〔2022/4/18 確認〕
※ 116 NTT ドコモ：フィッシング詐欺を未然に防ぐ「危険 SMS 拒否設定」の提供を開始＜2022 年 1 月 13 日＞ https://www.nttdocomo.co.jp/info/news_release/2022/01/13_00.html〔2022/4/18 確認〕
NTT ドコモ：SMS 拒否設定 https://www.docomo.ne.jp/info/spam_mail/sms/〔2022/4/18 確認〕
※ 117 KDDI 株式会社：迷惑メッセージブロック機能を au・UQ mobile・povo 向けに提供 https://news.kddi.com/kddi/corporate/newsrelease/2022/03/16/5928.html〔2022/4/18 確認〕
※ 118 ソフトバンク株式会社：迷惑 SMS 対策機能を提供開始 https://www.softbank.jp/corp/news/press/sbkk/2022/20220113_02/〔2022/4/18 確認〕
※ 119 厚生労働省：新型コロナウイルスワクチンの接種の実施について https://www.mhlw.go.jp/stf/newpage_16799.html〔2022/4/18 確認〕
※ 120 IPA（情報セキュリティ安心相談窓口 Twitter アカウント）：https://twitter.com/IPA_anshin/status/1432190641866358784〔2022/4/18 確認〕
※ 121 厚生労働省：新型コロナウイルスを題材とした攻撃メールについて https://www.mhlw.go.jp/stf/newpage_09393.html〔2022/4/18 確認〕
※ 122 厚生労働省：新型コロナワクチン接種の予約を案内する怪しいメールに注意!ー国がコロナワクチン接種に関連して金銭やクレジットカード番号を求めることはありませんー https://www.kokusen.go.jp/news/data/n-20210902_7.html〔2022/4/18 確認〕
※ 123 https://www.antiphishing.jp/news/alert/kyufukin_20210824.html〔2022/4/18 確認〕
※ 124 総務省：特別定額給付金の給付を騙ったメールに対する注意喚起 https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000438.html〔2022/4/18 確認〕
※ 125 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/mgdayori20211116.html〔2022/4/18 確認〕
※ 126 朝日新聞：PC 画面に「ウイルス感染」偽の警告…「サポート詐欺」容疑で初逮捕 https://www.asahi.com/articles/ASQ1L3G76Q1LUTIL001.html〔2022/4/18 確認〕
※ 127 独立行政法人国民生活センター：全国の消費生活センター等 http://www.kokusen.go.jp/map/〔2022/4/18 確認〕
※ 128 Microsoft 社：テクニカル サポート詐欺から身を守る https://support.microsoft.com/ja-jp/windows/ テクニカル - サポート詐欺から身

を守る -2ebf91bd-f94c-2a8a-e541-f5c800d18435〔2022/4/18 確認〕
※ 129 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。
※ 130 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/mgdayori20210309.html〔2022/4/18 確認〕
※ 131 ブラウザの通知機能：ウェブサイトからブラウザを通じて画面上に配信されるプッシュ型の通知サービス。2021 年 3 月 9 日現在、iOS 端末（iPhone、iPad 等）にはブラウザ通知機能は搭載されていない。
※ 132 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。
※ 133 https://www.mcafee.com/ja-jp/consumer-support/help/support/block-fake-alert.html〔2022/4/18 確認〕
※ 134 https://www.mcafee.com/ja-jp/consumer-support/help/common-faq.html?culture=ja-jp&id=commonFAQ〔2022/4/18 確認〕「間違って購入してしまいました。払い戻しの方法を教えてください。」を参照。
※ 135 東京商工リサーチ社：上場企業の個人情報漏えい・紛失事故は、調査開始以来最多の 137 件 574 万人分（2021 年）　https://www.tsr-net.co.jp/news/analysis/20210117_01.html〔2022/4/20 確認〕
※ 136 東京商工リサーチ社：「上場企業の個人情報漏えい・紛失事故」調査（2020 年）　https://www.tsr-net.co.jp/news/analysis/20210115_01.html〔2022/4/20 確認〕
※ 137 株式会社ネットマーケティング：不正アクセスによる会員様情報流出の調査結果と今後の対応について　https://www.net-marketing.co.jp/news/6001/〔2022/4/20 確認〕
※ 138-1 森永製菓株式会社：不正アクセス発生による個人情報流出の可能性のお知らせとお詫び　https://www.morinaga.co.jp/company/newsrelease/detail.php?no=2178〔2022/4/20 確認〕
※ 138-2 弊社公式オンラインショップへの不正アクセスによる個人情報流出に関するお詫びとご報告　https://biz.right-on.co.jp/news/topics/1104-2.php〔2022/5/19 確認〕
※ 139 株式会社リニカル：不正アクセスに伴う原因究明のためのサーバーの一時停止措置に関するお詫びとご報告　https://www.linical.co.jp/news/7ca5d9e93f2674a92830d2dec379d16d1d67f170.pdf〔2022/4/20 確認〕
株式会社リニカル：不正アクセスによる個人情報等流出の可能性に関するお知らせとお詫び　https://www.linical.co.jp/news/17705e29046d75409e91d377bb1410558f8e6e21.pdf〔2022/4/20 確認〕
※ 140 株式会社ユピテル：My Yupiteru 会員様情報の一部流出のお詫びとお知らせ　https://www.yupiteru.co.jp/corp/important/210607.html〔2022/4/20 確認〕
※ 141 株式会社メタップスペイメント：不正アクセスによる情報流出に関するご報告とお詫び　https://www.metaps-payment.com/company/20220228.html〔2022/4/20 確認〕
※ 142 コンディショニングジム GOING：【重要】会費ペイによるクレジット決済停止のお知らせ　https://www.facebook.com/cggoing/posts/3237118433079143〔2022/5/19 確認〕
子どもの発達支援を考える ST の会：「会費徴収システムの情報漏洩に関するご報告」　https://www.kodomost.jp/announce/kaihipay.pdf〔2022/4/20 確認〕
一般社団法人日本機械学会：イベントペイ　クレジットカード不正利用疑いと決済機能の一時停止について　https://www.jsme.or.jp/20211227-2/〔2022/4/20 確認〕
NSフィットネス：【お詫び】WEB 入会時にクレジットカード決済が出来ない件について　https://ns-fit-fukusaki.com/news/【お詫び】WEB 入会時にクレジットカード決済が出 /〔2022/4/20 確認〕
一般社団法人日本集中治療医学会：イベントペイ　クレジットカード不正利用疑いと決済機能の一時停止について　https://www.jsicm.org/news/news211228.html〔2022/4/20 確認〕
有限会社アップリンク：【重要なお知らせ】オンラインチケット一部販売再開のお知らせ　https://joji.uplink.co.jp/news/2022/13116〔2022/4/20 確認〕
※ 143 株式会社日能研：不正アクセスによるメールアドレス流出の可能性に関するお詫びとお知らせ　https://www.nichinoken.co.jp/info/owabi/220129.html〔2022/4/20 確認〕
※ 144 ロゴヴィスタ株式会社：弊社ホームページへの不正アクセスによる被害発生のお詫びとお知らせ　https://www.logovista.co.jp/Iverp/information/information/emergency.html〔2022/4/20 確認〕
※ 145 株式会社石橋楽器店：株式会社石橋楽器店への不正アクセスによる情報流出の可能性に関するお詫びとお知らせ　https://www.ishibashi.co.jp/company/20220111.html〔2022/4/20 確認〕
※ 146 ビーズ株式会社：不正アクセスによるメールアドレス流出の可能性に関するお詫びとお知らせ　https://www.be-s.co.jp/notice/4168〔2022/4/20 確認〕
※ 147 株式会社ヨシハラシステムズ：弊社が運営する「せんたく便」への不正アクセスによる個人情報流出に関するお詫びとお知らせ　https://www.sentakubin.co.jp/news/20210405.html〔2022/4/20 確認〕
※ 148 https://www.ipa.go.jp/security/vuln/documents/2008/200805_SQLinjection.html〔2022/4/20 確認〕
※ 149 IPA：【注意喚起】SQL インジェクションをはじめとしたウェブサイトの脆弱性の再点検と速やかな改修を　https://www.ipa.go.jp/security/announce/website_vuln.html〔2022/4/20 確認〕
※ 150 https://www.ipa.go.jp/files/000017319.pdf〔2022/4/20 確認〕
※ 151 https://www.ipa.go.jp/security/vuln/websecurity.html〔2022/4/20 確認〕
※ 152 日本サブウェイ合同会社：サーバー不正アクセスのご報告（2）https://origin.subway.co.jp/upload/press/f28005a86357b259abfe324a355631e7f8f8f1a2.pdf〔2022/4/20 確認〕
日本サブウェイ合同会社：サーバー不正アクセスのご報告（3）　https://www.subway.co.jp/press/year2021/news2582/〔2022/4/20 確認〕
※ 153 ランドブレイン株式会社：弊社サーバーのウイルス感染及び情報流出に関する調査結果のご報告　https://www.landbrains.co.jp/hp/doc/210519.pdf〔2022/4/20 確認〕
※ 154 Security NEXT：不正アクセス被害のランドブレイン、調査結果を公表 - ランサムウェアは「Cring」　https://www.security-next.com/126310〔2022/4/20 確認〕
※ 155 株式会社オリエンタルコンサルタンツホールディングス：ランサムウェア攻撃に関するご報告　https://www.oriconhd.jp/files/information/news20211008_01.pdf〔2022/4/20 確認〕
※ 156 市原市：委託事業者のサーバーへの不正アクセスについて（調査結果のお知らせ）　https://www.city.ichihara.chiba.jp/article?articleId=6170b83e910de2089661fe84〔2022/4/20 確認〕
市川市：本市の業務委託先の業者のサーバーがサイバー攻撃を受けた件について　https://www.city.ichikawa.lg.jp/sys07/0000373622.html〔2022/4/20 確認〕
東京都総務局：委託業務受託者のサーバーに対するサイバー攻撃について　https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/09/01/01.html〔2022/4/20 確認〕
東京都港湾局：委託業務受託者へのサイバー攻撃について　https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/09/01/14.html〔2022/4/20 確認〕
東京都建設局：委託業務受託者へのサーバー攻撃について　https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/09/01/13.html〔2022/4/20 確認〕
東京都都市整備局：委託業務受託者へのサイバー攻撃について　https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/09/01/15.html〔2022/4/20 確認〕
東京都下水道局：委託業務受託者へのサイバー攻撃について　https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/09/03/04.html〔2022/4/20 確認〕
東京都水道局：業務受託者へのサイバー攻撃について　https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/09/03/01.html〔2022/4/20 確認〕
葛飾区：令和 3 年 8 月に発生した本区業務委託事業者へのサイバー攻撃について（令和 4 年 3 月更新）　https://www.city.katsushika.lg.jp/information/kouho/1005542/1026867.html〔2022/4/20 確認〕
埼玉県：本県業務委託事業者へのサイバー攻撃について　https://www.pref.saitama.lg.jp/a1002/news/page/news20210826.html〔2022/4/20 確認〕
群馬県：【9 月 3 日】本県業務委託事業者へのサイバー攻撃について（建設企画課）　https://www.pref.gunma.jp/houdou/h81g_00043.html〔2022/4/20 確認〕
滋賀県：本県業務委託事業者へのサイバー攻撃について　https://www.pref.shiga.lg.jp/kensei/koho/e-shinbun/oshirase/320910.html〔2022/4/20 確認〕
倉敷市：本市の業務委託（依頼）業者が受けたサイバー攻撃に関する調査状況について　https://www.city.kurashiki.okayama.jp/item/142781.htm#itemid142781〔2022/4/20 確認〕
※ 157 株式会社オリエンタルコンサルタンツホールディングス：特別損失の計上及び業績予想の修正に関するお知らせ　https://www.oriconhd.jp/files/information/news20210917_01.pdf〔2022/4/20 確認〕
※ 158 富士通株式会社：プロジェクト情報共有ツールへの不正アクセスについて（第五報）　https://pr.fujitsu.com/jp/news/2022/03/7-1.html〔2022/4/20 確認〕
富士通株式会社：プロジェクト情報共有ツールへの不正アクセスについて（第四報）　https://pr.fujitsu.com/jp/news/2021/12/9-1.html〔2022/

4/20 確認〕
総務省：富士通株式会社が管理・運営するプロジェクト情報共有ツールへの不正アクセスによる情報の流出　https://www.soumu.go.jp/menu_news/s-news/01kanbo05_02000152.html〔2022/4/20 確認〕
国土交通省：富士通株式会社が管理・運営するプロジェクト情報共有ツールへの不正アクセスによる国土交通省関係情報の流出について　https://www.mlit.go.jp/report/press/joho02_hh_000004.html〔2022/4/20 確認〕
外務省：富士通株式会社が管理・運営するプロジェクト情報共有ツールへの不正アクセスによる情報の流出について　https://www.mofa.go.jp/mofaj/press/release/press4_009061.html〔2022/4/20 確認〕
内閣官房内閣サイバーセキュリティセンター：富士通株式会社が管理・運営するプロジェクト情報共有ツールへの不正アクセスによる情報の流出について　https://www.nisc.go.jp/pdf/press/20210602NISC_press.pdf〔2022/4/20 確認〕
NHK：成田空港 運航管理情報システムへの不正アクセス受け注意喚起　https://www3.nhk.or.jp/news/html/20210526/k10013051551000.html〔2022/4/20 確認〕
※ 159 内閣官房内閣サイバーセキュリティセンター：プロジェクト情報共有ツールに対する不正アクセス対策の確認 に関する政府機関等及び重要インフラ事業者等への注意喚起の発出について　https://www.nisc.go.jp/pdf/press/projectist20210525.pdf〔2022/4/20 確認〕
※ 160 株式会社ジーアール：「オムニECシステム」一部サーバーへの不正アクセスについて　https://www.grinc.co.jp/information202109.pdf〔2022/4/20 確認〕
※ 161 株式会社ベイジア：弊社「ベイシアネットショッピング」委託先への不正アクセスによるお客様情報流出に関するお詫びとお知らせ　https://www.beisia.co.jp/wp-content/uploads/2021/10/c9f3e8b196c27d7f25d6e823c664f247.pdf〔2022/4/20 確認〕
サミット株式会社：弊社「サミット予約ネット」委託先への不正アクセスによるお客様情報流出に関するお詫びとお知らせ　https://www.summitstore.co.jp/20210916net.pdf〔2022/4/20 確認〕
株式会社リウボウストア：オンラインショップへの不正アクセスによる個人情報漏えいについて　https://ryubostore.jp/news_detail.html?code=65〔2022/4/20 確認〕
株式会社天満屋ストア：お客様情報の流出の可能性に関するお知らせとお詫び　http://www.tenmaya-store.co.jp/assets/images/sys/2021/09/20210916_2.pdf〔2022/4/20 確認〕
株式会社丸久：お客様情報の流出の可能性に関するお知らせとお詫び　http://www.mrk09.co.jp/ 重要なお知らせ /〔2022/4/20 確認〕
株式会社マルヨシセンター：弊社が使用する「オンライン予約販売システム」への不正アクセスによるお客様情報の流出に関するお詫びとお知らせ　https://ww2.maruyoshi-center.co.jp/upload/news/202109/ 2021年9月16日発信文書② .pdf〔2022/4/20 確認〕
グラントマト株式会社：不正アクセスによる個人情報流出の可能性に関する調査結果のご報告　https://www.grantomato.jp/topics/topics.php?id=687〔2022/4/20 確認〕
株式会社杏林堂薬局：「杏林堂（公式）オンラインショップおよび「店頭予約者情報」への不正アクセスによる お客様情報漏えいに関するお詫びとお知らせ　https://www.kyorindo.co.jp/news/pdf/kyorindo_online_news.pdf〔2022/4/20 確認〕
株式会社芝寿し：弊社「芝寿しオンラインショップ」委託先への不正アクセスによるお客様情報流出に関するお詫びとお知らせ　https://www.online-shibazushi.com/user_data/20211130_oshirase.pdf〔2022/4/20 確認〕
株式会社アヤハディオ：弊社が運営する「アヤハディオネットショッピング」への不正アクセスによるお客様情報漏洩に関するお詫びとお知らせ　https://www.ayahadio.jp/user_data/20211201.pdf〔2022/4/20 確認〕
沓間水産株式会社：弊社が運営する「魚がし鮨お持ち帰り予約サイト」への不正アクセスによるお客様情報流出に関するお詫びとお知らせ　https://www.uogashizushi.co.jp/wp-content/uploads/2021/12/sps03.pdf〔2022/4/20 確認〕
※ 162 https://privacymark.jp/system/reference/pdf/2020JikoHoukoku_211005.pdf〔2022/4/20 確認〕
※ 163 日本年金機構：年金振込通知書の印刷誤りについて　https://www.nenkin.go.jp/oshirase/taisetu/2021/202110/100602.html〔2022/4/20 確認〕
日本年金機構：年金振込通知書（令和３年 10 月定期支払）の再送付について　https://www.nenkin.go.jp/oshirase/taisetu/2021/202110/1013.html〔2022/4/20 確認〕
※ 164 日本年金機構：「年金振込通知書」（令和3年10月定期支払）の印刷誤り事案に係る検証状況報告について　https://www.nenkin.go.jp/oshirase/taisetu/2021/202112/1203.files/1203.pdf〔2022/4/20 確認〕
※ 165 サンメッセ株式会社：特別損失（製品保証引当金繰入額）の計上及び 2022 年3月期第2四半期連結累計期間の業績予想値と実績値との差異に関するお知らせ　https://www.sunmesse.co.jp/ir/news/file/20211104155237.pdf〔2022/4/20 確認〕
※ 166-1 LINE 株式会社：LINE VOOM の公開範囲の設定における不具合のお知らせとお詫び　https://linecorp.com/ja/security/article/400〔2022/4/20 確認〕
※ 166-2 LINE 株式会社：【LINE Pay】一部ユーザーのキャンペーン参加に関わる情報が閲覧できる状態になっていた件のお知らせとお詫び　https://linecorp.com/ja/pr/news/ja/2021/4032〔2022/4/20 確認〕
※ 167 IPA：「企業における営業秘密管理に関する実態調査 2020」報告書について　https://www.ipa.go.jp/security/fy2020/reports/ts_kanri/index.html〔2022/4/20 確認〕
※ 168 株式会社村田製作所：再委託先社員による不適切なデータの取り扱いについてのお知らせとお詫び　https://corporate.murata.com/ja-jp/newsroom/news/company/general/2021/0805〔2022/4/20 確認〕
※ 169 カッパ・クリエイト株式会社：当社役員に対する競合会社からの告訴について　https://www.kappa-create.co.jp/blog/wp-content/uploads/2021/07/ 当社役員に対する競合会社からの告訴について_20210705.pdf〔2022/4/20 確認〕
※ 170 株式会社 And Do ホールディングス：当社子会社の元従業員の不正行為について　https://www.housedo.co.jp/and-do/news/2022/20220118.html〔2022/4/20 確認〕
※ 171 https://www.ipa.go.jp/security/fy24/reports/insider/〔2022/4/20 確認〕
※ 172 日本郵便株式会社、株式会社ゆうちょ銀行：郵便局におけるお客さま情報の紛失（調査結果）　https://www.post.japanpost.jp/notification/pressrelease/2021/00_honsha/1215_02_01.pdf〔2022/4/20 確認〕
※ 173 金沢信用金庫：お客さま情報の紛失について　http://www.shinkin.co.jp/kanazawa/material/top_news/2022.1.28.pdf〔2022/4/20 確認〕
※ 174 トヨタ自動車株式会社：トヨタ販売店におけるお客様の個人情報の不適切な取扱いについて　https://global.toyota/jp/newsroom/corporate/35909023.html〔2022/4/20 確認〕
トヨタ自動車株式会社：トヨタ販売店におけるお客様の個人情報の不適切な取扱いについて　https://global.toyota/jp/newsroom/corporate/36003832.html〔2022/4/20 確認〕
※ 175 株式会社 SUBARU：SUBARU 販売特約店における、お客様情報の不適切な取り扱いについて　https://www.subaru.co.jp/news/2021_10_27_162724/〔2022/4/20 確認〕
※ 176 株式会社新生銀行、新生フィナンシャル株式会社：業務委託先等への提供データに一部のお客さま情報が含まれていたことに関するお詫び　https://www.shinseibank.com/corporate/news/pdf/pdf2021/210927_personal_info_j.pdf〔2022/4/20 確認〕
株式会社新生銀行、新生フィナンシャル株式会社：業務委託先等への提供データに一部のお客さま情報が含まれていたことに関するお詫び(2)　https://www.shinseibank.com/corporate/news/pdf/pdf2021/220127_personal_info_j.pdf〔2022/4/20 確認〕
※ 177 株式会社新生銀行：お客さま情報を誤って提供したことについてのお詫びとご説明　https://www.shinseibank.com/corporate/news/pdf/pdf2021/220127_personal_info_j.pdf〔2022/4/20 確認〕
※ 178 JPCERT/CC、IPA：Japan Vulnerability Notes　https://jvn.jp/〔2022/4/19 確認〕
※ 179 NIST：National Vulnerability Database　https://nvd.nist.gov/〔2022/4/19 確認〕
※ 180 公表年は、ベンダがアドバイザリを公開した年、他組織やセキュリティポータルサイト等の登録／公開した年、発見者が一般向けに報告した年等、脆弱性対策情報が一般に公表された年を指す。なお、JVN iPedia で脆弱性対策情報を公開した年は「登録年」としている。
※ 181 IPA：共通脆弱性識別子 CVE 概説　https://www.ipa.go.jp/security/vuln/CVE.html〔2022/4/19 確認〕
※ 182 The MITRE Corporation:CVE Numbering Authorities（CNA）　https://www.cve.org/ProgramOrganization/CNAs〔2022/4/19 確認〕
※ 183 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。
※ 184 The MITRE Corporation：CVE Adds 7 New CVE Numbering Authorities (CNAs)　https://cve.mitre.org/news/archives/2016/news.html〔2022/4/19 確認〕
※ 185 The MITRE Corporation：VulDB Added as CVE Numbering Authority (CNA)　https://www.cve.org/Media/News/item/news/2021/12/21/VulDB-Added-as-CVE-Numbering〔2022/4/19 確認〕

※ 186 IPA：共通脆弱性タイプ一覧 CWE 概説　https://www.ipa.go.jp/security/vuln/CWE.html〔2022/4/19 確認〕
※ 187 IPA：共通脆弱性評価システム CVSS 概説　https://www.ipa.go.jp/security/vuln/CVSS.html〔2022/4/19 確認〕
※ 188 JPCERT/CC：セキュアコーディング　https://www.jpcert.or.jp/securecoding/〔2022/4/19 確認〕
※ 189 Microsoft 社：Windows 11: ハイブリッド ワークと学習のためのオペレーティング システム　https://blogs.windows.com/japan/2021/06/25/windows-11-the-operating-system-for-hybrid-work-and-learning/〔2022/4/19 確認〕
※ 190 IPA：更新：Apache HTTP Server の脆弱性対策について (CVE-2021-41773, CVE-2021-42013)　https://www.ipa.go.jp/security/ciadr/vul/alert20211006.html〔2022/4/19 確認〕
JPCERT/CC：Apache HTTP Server のパストラバーサルの脆弱性（CVE-2021-41773）に関する注意喚起　https://www.jpcert.or.jp/at/2021/at210043.html〔2022/4/19 確認〕
※ 191 NVD：CVE-2021-41773 Detail　https://nvd.nist.gov/vuln/detail/CVE-2021-41773〔2022/4/19 確認〕
※ 192 NVD：CVE-2021-42013 Detail　https://nvd.nist.gov/vuln/detail/CVE-2021-42013〔2022/4/19 確認〕
※ 193 Security NEXT：わずか 3 日、「Apache HTTPD」が再修正 - 前回修正は不十分、RCE のおそれも　https://www.security-next.com/130520〔2022/4/19 確認〕
※ 194 日本経済新聞：VPN 認証情報また流出　日本は 1000 社、中小企業中心　https://www.nikkei.com/article/DGXZQOUE110A80R10C21A9000000/〔2022/4/19 確認〕
※ 195 経済産業省：「情報処理の促進に関する法律の一部を改正する法律案」が閣議決定されました　https://www.meti.go.jp/press/2019/10/20191015002/20191015002.html〔2022/4/19 確認〕
※ 196 「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。
※ 197 NISC：ApacheLog4j の脆弱性 (CVE-2021-44228) に関する注意喚起　https://www.nisc.go.jp/pdf/press/20211213NISC_press.pdf〔2022/4/18 確認〕
JPCERT/CC：Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起　https://www.jpcert.or.jp/at/2021/at210050.html〔2022/4/18 確認〕
IPA：更新：Apache Log4j の脆弱性対策について (CVE-2021-44228)　https://www.ipa.go.jp/security/ciadr/vul/alert20211213.html〔2022/4/18 確認〕
※ 198 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/files/000044731.pdf〔2022/4/18 確認〕
※ 199 IPA：脆弱性関連情報の届出受付　https://www.ipa.go.jp/security/vuln/report/index.html〔2022/4/18 確認〕
※ 200 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。
※ 201 IPA：調整不能案件の公表判定業務における取扱いプロセス　https://www.ipa.go.jp/security/vuln/report/unreachable_process.html〔2022/4/18 確認〕
※ 202 「1.3.2 早期警戒パートナーシップの届出状況から見る脆弱性の動向」では、「ウェブアプリケーションソフト」は、Web サイト構築関係のソフトウェアを指す。これは、四半期ごとの脆弱性関連情報の届出状況のレポート（IPA：脆弱性関連情報の届出状況　https://www.ipa.go.jp/security/vuln/report/press.html〔2022/4/18 確認〕）で使用している「製品情報種類」の分野種別と同じである。
※ 203 JVN：JVN#97554111 EC-CUBE におけるクロスサイトスクリプティングの脆弱性　https://jvn.jp/jp/JVN97554111/index.html〔2022/4/18 確認〕
※ 204 株式会社イーシーキューブ：【重要】EC-CUBE 4.0 系における緊急度「高」の脆弱性（JVN#97554111）発覚と対応のお願い（2021/5/24 17:00　更新）（2021/05/24）　https://www.ec-cube.net/news/detail.php?news_id=383〔2022/4/18 確認〕
※ 205 JPCERT/CC：JPCERT/CC　ベストレポーター賞 2021　https://www.jpcert.or.jp/award/best-reporter-award/2021.html〔2022/4/18 確認〕
※ 206 IPA：ソフトウェア等の脆弱性関連情報に関する届出状況［2018 年第 4 四半期（10 月～ 12 月）］　https://www.ipa.go.jp/security/vuln/report/vuln2018q4.html〔2022/4/18 確認〕
※ 207 https://www.ipa.go.jp/security/vuln/websitecheck.html〔2022/4/18 確認〕
※ 208 IPA：セキュアプログラミング講座 Web アプリケーション編 第 5 章 暴露対策 Web サーバからのファイル流出対策　https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/401.html〔2022/4/18 確認〕