2021

情報セキュリティ白書

序章

2020年度の情報セキュリティの概況

2020 年は新型コロナウイルス感染症が世界中で流行し、経済活動や日々の暮らしに大きな影響を与えた。2020 年 1 月以降に各国で発出された緊急事態宣言により、多くの企業・組織が事業継続のためにネットワークを強化し、テレワークやオンライン会議により業務を実施した結果、このような環境の脆弱性を突く攻撃が国内外で発生した。

国内では、VPN 製品やオンライン会議サービスの脆弱性を狙った攻撃の増加に対し、各府省庁、JPCERT/CC、IPA 等から何度も注意喚起がなされた。しかし 7 月にはテレワークで使用した BYOD 端末からの不正アクセスが、11 月には自宅で利用した端末が SNS からウイルス感染し職場に持ち込んでしまう事故等が発生した。

一方で、新型コロナウイルスの感染原因や対策、ワクチンに関連した様々な偽情報（フェイクニュース）が溢れ、混乱に乗じた詐欺等により多くの被害も国内外で発生し、世界保健機関（WHO）を始めとする多くの組織が対策を呼びかけた。

2017 年に大きな被害をもたらしたランサムウェアはセキュリティ対策により減少していたが、2020 年は手口が巧妙になり、特定の企業・組織を標的に変え、更に「二重の脅迫」を行う新たな手口が観測された。11 月に公表されたゲーム会社の事例では、北米現地法人が攻撃を受け社内ネットワークに侵入され、1 万人以上の個人情報が流出し、米国と国内拠点の一部の機器のファイルが暗号化された。

このほか、海外拠点を介した攻撃では、2020 年 5 月に情報通信事業者の海外拠点から社内ネットワーク経由で不正アクセスが発生したと報告された。

クラウドサービスのサプライチェーンでも脅威が顕在化した。2021 年 1 月、内閣サイバーセキュリティセンター（NISC）は重要インフラ事業者等に向けて、特定のサービスを利用する際に、利用者の設定不備により外部から情報が参照される可能性について注意喚起を行った。セキュリティの責任分担について利用者の意識が低いままサービスが提供されるリスクが浮き彫りになった。

海外では、人々の生活に関わる水道システムや浄水場等の制御システムへの攻撃が報告された。また、Ripple20 という 19 種類のゼロデイ脆弱性が組み込み機器用通信ソフトウェアに発見された。当該ソフトウェアはルータ、プリンタ等で広く利用されており、数億個以上もの IoT 製品が影響を受ける可能性があると報告された。

また米国では、2020 年 12 月にネットワーク監視・管理用ソフトウェアプラットフォームの脆弱性を突き、連邦政府機関や大手企業等を一斉に狙った過去最大規模のサプライチェーン攻撃が発覚した。更に 2021 年 5 月には米国の燃料供給事業者がランサムウェア攻撃を受け、一時操業を停止した。こうした脅威に対して Biden 大統領は 2021 年 2 月、5 月にサプライチェーンセキュリティ強化を意図した大統領令を発表しており、今後の対応が注目される。

欧州では、新型コロナウイルス感染拡大対策において個人情報を保護するため、2020 年 5 月に位置情報及び接触追跡ツールに関するガイドライン、研究目的の健康情報処理に関するガイドラインを公開した。また欧州は、新型コロナウイルスや選挙に関する偽情報対策として、2020 年 12 月に欧州民主主義行動計画を発表し、SNS やネット上の政治広告等の監視強化を行うとした。

国内では、2020 年 6 月に「政府情報システムのためのセキュリティ評価制度（ISMAP）」が開始された。政府のクラウドサービス調達におけるセキュリティ水準の確保、クラウドサービスの円滑な導入に資することが期待される。また、11 月には中小企業を含むサプライチェーンのセキュリティ強化の枠組みとして、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）が設立された。サイバー攻撃の実態や取り組みに関する情報共有、中小企業に求められるセキュリティ水準検討等に関する業界横断的な活動が期待される。

新型コロナウイルス感染拡大防止のための緊急事態宣言、まん延防止等重点措置は 2021 年度も発出され、様々な制限の中、新しい働き方やルールが試行されている。このように、テレワークの導入や DX の推進等でデジタル化は急加速しつつあるが、セキュリティ対策が十分に検討されていない、あるいは、一時的に認めざるを得なかったセキュリティ対策の緩和や逸脱が放置されている可能性がある。リスクと対策の再確認、ルールの見直しが求められている。

2020 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
2020 年　4 月	● テレワーク環境やオンライン会議サービスの脆弱性、及びビジネスメール詐欺について、国内外で注意喚起（1.2.3、1.3.1、2.2.2） ● イスラエル水道システムにサイバー攻撃（3.1.1）	■ 交通 ISAC が創設（3.1.4） ■ 米国でテレワークのセキュリティガイダンス、コロナ禍における重要インフラ基盤の運用と従業員の安全に関するガイダンスを公開（2.2.2）
5 月	● 情報通信事業者が海外拠点からの不正アクセスを公表（1.2.1） ● ノルウェーの投資ファンドが海外送金で 1,000 万ドルのビジネスメール詐欺被害（1.2.3）	■ 欧州で位置情報及び接触追跡ツールに関するガイドライン、研究目的の健康情報処理に関するガイドラインを公開（2.2.3） ■ 米国でサプライチェーンリスク管理指針を公開(2.2.2)
6 月	● 国内大手自動車メーカやアルゼンチン電力会社がランサムウェア攻撃被害を公表（3.1.1） ● Ripple20 のゼロデイ脆弱性を公表（1.2.5、3.1.2、3.2.2）	■「政府情報システムのためのセキュリティ評価制度（ISMAP）」運用開始（2.6.3）
7 月	● 情報通信事業者が BYOD 端末経由の不正アクセスを公表（1.2.1）	■「サイバーセキュリティ 2020」公開（2.1.1） ■「IoT・5G セキュリティ総合対策 2020」公開（2.1.3）
8 月	● IPA が新たなランサムウェア攻撃について注意喚起(1.2.2) ● 米国金融機関が海外送金 1,080 万ドルのビジネスメール詐欺被害(1.2.3)	■ IPA が「脆弱性対処に向けた製品開発者向けガイド」公開（3.2.4） ■ 米国 NIST が SP 800-207（ゼロトラストアーキテクチャ）公開（3.4.2）
9 月	● 携帯通信会社が提供するマネーサービスを介した銀行の預金の不正引き出しが発覚（1.1.2）	■ 経済産業省が「サイバーセキュリティ体制構築・人材確保の手引き第 1 版」公開（2.1.2、2.3.1）
10 月	● JPCERT/CC がランサム DDoS 攻撃の注意喚起（1.2.4）	■ 総務省が「スマートシティセキュリティガイドライン（第 1.0 版）」公開（2.1.3）
11 月	● ゲーム会社が「新たなランサムウェア攻撃」被害を公表（1.2.2） ● NISC が「新たなランサムウェア攻撃」について注意喚起（1.2.2）	■ 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）設立（2.1.2、2.4.2） ■「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」策定（2.1.2、3.1.4）
12 月	● NISC、JPCERT/CC が VPN 製品の脆弱性に対する注意喚起（1.2.5、1.3.1、3.1.2） ● 米国でネットワーク管理用プラットフォームのウイルス感染で大規模被害公表（3.1.1）	■「情報システム・モデル取引・契約書」第二版公開（2.1.2） ■ 米国 NIST が SP 800-53 Rev.5（組織のセキュリティ・プライバシー管理策）更新（3.4.2）
2021 年　1 月	● NISC がクラウドサービス製品の設定不備について注意喚起（1.2.8） ● Europol による Emotet テイクダウン（1.2.6）	■ 産業サイバーセキュリティ研究会 WG1 に宇宙産業 SWG を設置（2.1.2）
2 月	● 米国で浄水場への攻撃で薬品投入量を操作される被害（3.1.1）	■ 警察庁、総務省、ICT-ISAC、及び ISP 各社が連携して、Emotet 感染の恐れのある利用者に注意喚起を行う取り組みを開始（1.2.6）
3 月	● 海外航空会社の顧客管理システムが不正アクセスを受け、加盟していた日本の航空会社にも被害（1.2.8）	■ サイバーセキュリティに関する国連オープン・エンド作業部会最終会合開催（2.2.1）

※ 2020 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番である。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

2020年は新型コロナウイルス感染症に関連した攻撃や、急速に普及したテレワークやオンライン会議環境の脆弱性を突く攻撃が世界的に問題となった。また、2017年に大きな被害をもたらしたランサムウェアが、企業・組織を標的に「二重の脅迫」を行う新たな攻撃となり観測された。

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

1.1 2020年度に観測されたインシデント状況

本節では2020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。

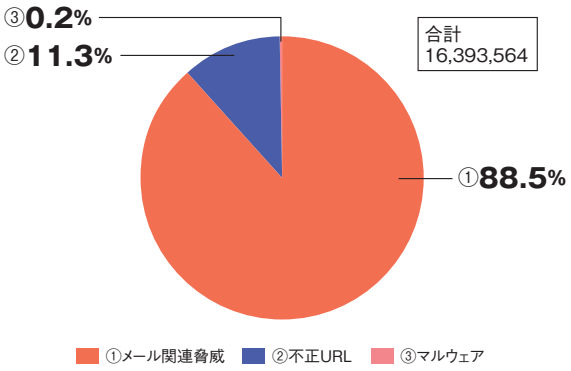
1.1.1 世界における情報セキュリティインシデント状況

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。

- トレンドマイクロ株式会社（以下、トレンドマイクロ社）：2020年年間セキュリティラウンドアップ※1
- 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2021※2
- Anti-Phishing Working Group, Inc.（以下、APWG）：Phishing Activity Trends Reports※3
- 米国連邦捜査局（FBI：Federal Bureau of Investigation）：Internet Crime Report 2020※4
- Verizon Communications Inc.（以下、Verizon社）：2021 Data Breach Investigations Report※5
- Coveware, Inc.：Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands※6
- Intezer Labs：2020 Set a Record for New Linux malware families※7

(1) 新型コロナウイルス感染症に関連する脅威

トレンドマイクロ社の調査によれば、2020年には、新型コロナウイルス感染症（以下、新型コロナウイルス）に関連して、「不正URL」「メール関連脅威」「マルウェア」合わせて1,600万件以上の脅威が検出された。そのうち90%近くがメール関連脅威であり、新しい情報提供に便乗するもの、給付金に関するもの、ワクチンに関するもの等、様々な情報を偽装した脅威が出現した（図1-1-1）（新型コロナウイルスを題材としたメールによる攻撃の手口については「1.2.1（3）（a）標的型攻撃メール」「1.2.3 ビジネスメール詐欺（BEC）」「1.2.6（2）（b）メール受信者の興味・関心を惹く題材を悪用する手口」「1.2.7（2）世の中の関心に乗じるメールの手口」参照）。

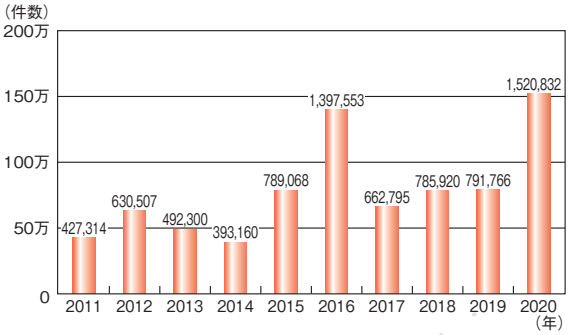


■図1-1-1　新型コロナウイルス関連脅威検出数のタイプ別割合（2020年）
（出典）トレンドマイクロ社「2020年年間セキュリティラウンドアップ」を基にIPAが編集※8

トレンドマイクロ社の調査によれば、新型コロナウイルスに便乗した手口による脅威の、脅威全体に対する割合は、新型コロナウイルスが猛威を振るった2020年上半期でも、表1-1-1（次ページ）のように1%未満に過ぎない。攻撃者は他の様々な手口を使って攻撃を行っているともいえる。

	脅威全般	新型コロナウイルス関連	割合
不正なサイトへのアクセス数の比較（2020年1～6月、全世界）	929,302,406	743,348	0.08%
フィッシングサイトへのアクセス数の比較（2020年1～6月、全世界）	102,312,289	80,586	0.08%
フィッシングサイトに誘導された利用者数の比較（2020年1～6月、全世界）	6,819,460	14,236	0.21%

■表 1-1-1　脅威の全体と新型コロナウイルスに便乗する脅威の比較（2020年上半期）
（出典）トレンドマイクロ社「2020年上半期セキュリティラウンドアップ※9」を基にIPAが作成



■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（2011～2020年）
（出典）APWG「Phishing Activity Trends Reports」を基にIPAが作成

(2) フィッシングとビジネスメール詐欺の傾向

APWGによると、2020年のフィッシングサイトの総数は約152万1,000件で、2019年と比較して92%増と大幅に増加し、過去10年で最多となった（図1-1-2）。

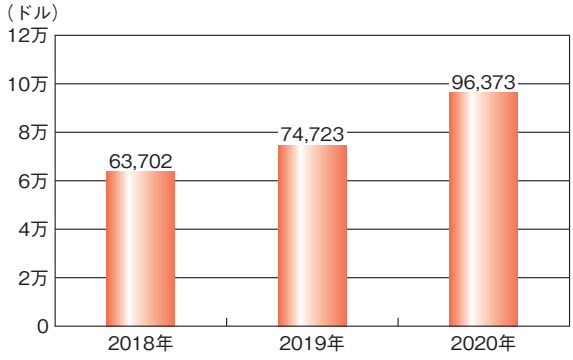
ターゲットとなる業種は、2020年の1年間では、「SaaS/Webmail」が28.1%、「金融機関」が20.5%、「ペイメント（支払い）」が14.0%と続いている。この3業種がターゲット業種の上位を占める傾向は2017年以降変わっていない。

ビジネスメール詐欺（BEC：Business Email Compromise）に関して、FBIの統計によると、2020年の米国国内の被害額は18億6,700万ドルとなっており、最も被害額の大きいサイバー犯罪と位置付けられている（「1.2.3 ビジネスメール詐欺（BEC）」参照）。

また、1件あたりの被害額も年々増加しており、2020年では約9万6,000ドルを超えた（図1-1-3）。

(3) 情報漏えいインシデントの状況

2020年に起きた大規模で深刻な情報漏えいインシデントとして、SolarWinds Worldwide, LLC.（以下、



■図 1-1-3　BECの1件あたりの損害額の推移（2018～2020年）
（出典）FBI「Internet Crime Report 2020」を基にIPAが作成

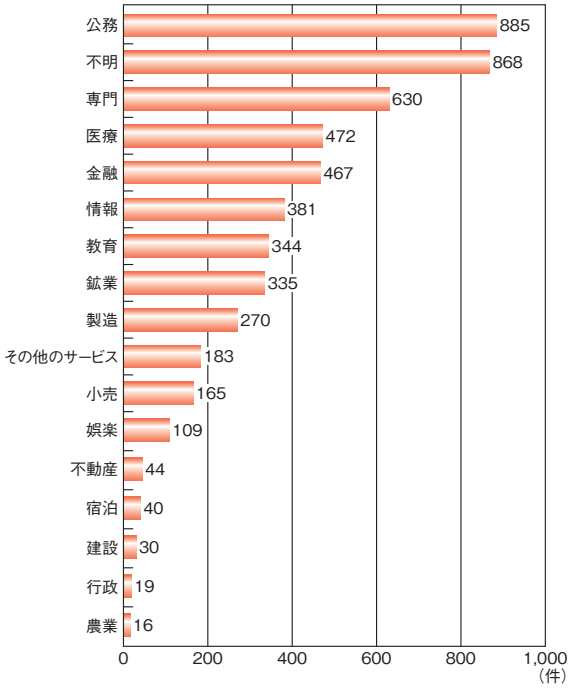
SolarWinds社）のネットワーク集中監視・管理用のソフトウェアプラットフォームOrionにおける事例を紹介する※10。SolarWinds社のOrionの正規のアップデートを通じてバックドアが組み込まれ、不正アクセスが行われた。攻撃の影響を受けたと見られる顧客数は約1万8,000に上った※11。米国の国土安全保障省（DHS：Department of Homeland Security）や国防総省（DoD：Department of Defense）等の政府機関やFireEye, Inc.※12のようなセキュリティベンダ等で様々な情報が窃取された（「2.2.2 (3) SolarWinds事案とその対応」「3.1.1 (4) ネットワーク管理用のソフトウェアの脆弱性に端を発する大規模な感染事例」参照）。

Verizon社によると、2020年に同社が分析した7万9,635件のインシデントのうち情報漏えい／侵害の件数は5,258件となり、15万7,525件のインシデントのうち3,950件だった2019年に比べて33.1%増加した。

最も発生件数の多い業種は「公務」の885件で、次いで「専門」が630件、「医療」が472件、「金融」が467件となっている（「不明」を除く）（次ページ図1-1-4）。

また、上記の情報漏えいの攻撃手法を分類した結果によると、2020年は2017年、2018年、2019年と1位が続いた「Webアプリケーション攻撃」が2位となり、代わって「ソーシャルエンジニアリング」が1位となった。更に3位は「システムへの侵入」、4位は「設定ミス」となった。

トレンドマイクロ社によると、2020年に検出されたウイルス※13の3位となっているEmotetは、主にメールに添付され、メールやパスワード等の情報を窃取し猛威を振るっていたが、2021年1月、Europol（欧州刑事警察機構）と欧米各国の共同作戦によるテイクダウンが行われ、運用メンバーの一部が逮捕されてEmotetをコントロールしていたC&Cサーバ※14が差し押さえられたことで、Emotetは無害化された※15（「1.2.6 ばらまき型メールによる攻撃」参照）。

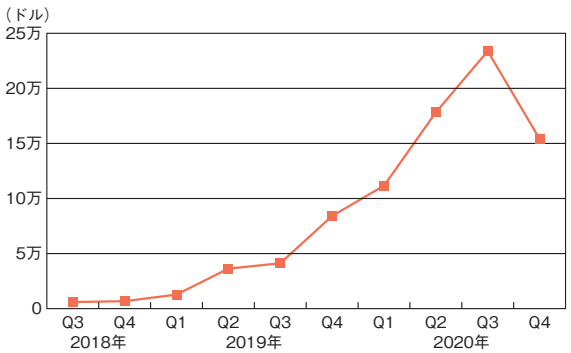


※「専門」とは、弁護士、会計士、アーキテクト、研究所、コンサルティング会社等を指す

■図 1-1-4　業種別の情報漏えいの件数（2020 年）
（出典）Verizon 社「2021 Data Breach Investigations Report」を基に IPA が作成

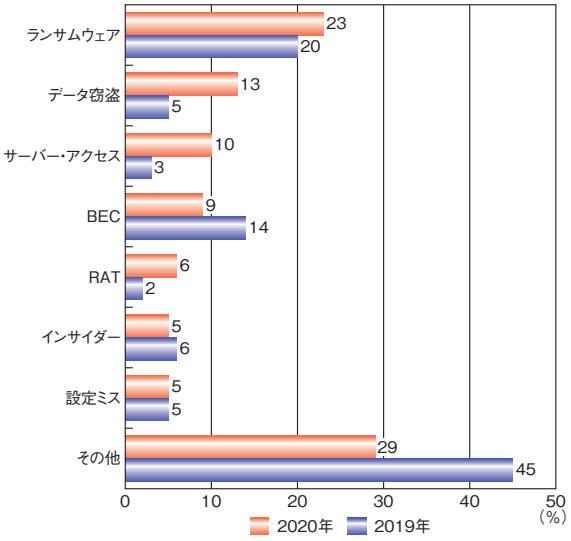
(4) ランサムウェアによる攻撃の傾向

Coveware, Inc. によると、ランサムウェアの暗号化解除のための平均支払額は年々上昇し、2020 年の四半期平均支払額は 16 万 9,446 ドルと、2019 年に比べ 288.7% 上昇した。四半期ごとの平均支払額を図 1-1-5 に示す。



■図 1-1-5　ランサムウェアによる四半期ごとの平均支払額
（2018 年第 3 四半期～ 2020 年第 4 四半期）
（出典）Coveware, Inc.「Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands」を基に IPA が編集

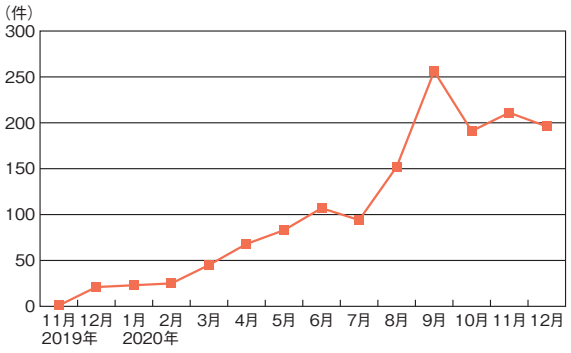
IBM 社によると、サイバーインシデントの主要な攻撃手法として 2020 年に最も多かったのは「ランサムウェア」の 23% で、続いて「データ窃盗」「サーバー・アクセス」となった（図 1-1-6）。



■図 1-1-6　主要な攻撃手法
（出典）IBM 社「IBM X-Force 脅威インテリジェンス・インデックス 2021」を基に IPA が編集

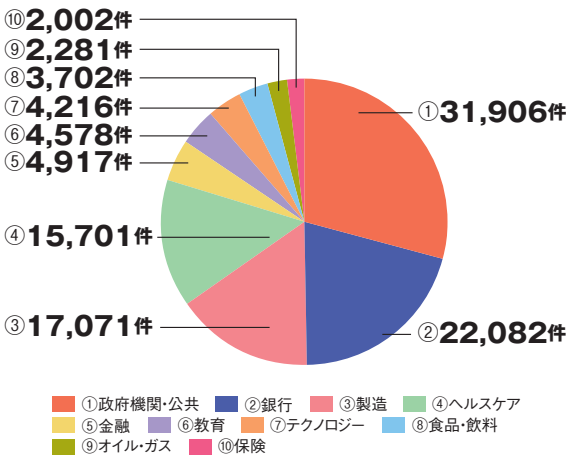
また、ランサムウェアによるサイバー攻撃のうち 59% が、ランサムウェアによるデータの暗号化に加えて、機密情報の窃取を行う「二重の脅迫」を用いた戦術であったとされる（「1.2.2 新たなランサムウェア攻撃」参照）。更に 2020 年に公表された情報漏えいのうち、ランサムウェア関連のデータ漏えいが 36% を占めていた。

トレンドマイクロ社の調査によれば、ランサムウェアの被害企業と窃取情報を掲載するための暴露サイト 22 種の月別の投稿件数は、図 1-1-7 のように急激に増加した。



■図 1-1-7　ランサムウェアの暴露サイト上で確認した投稿件数の推移
（2019 年 11 月～ 2020 年 12 月）
（出典）トレンドマイクロ社「2020 年年間セキュリティラウンドアップ」を基に IPA が編集

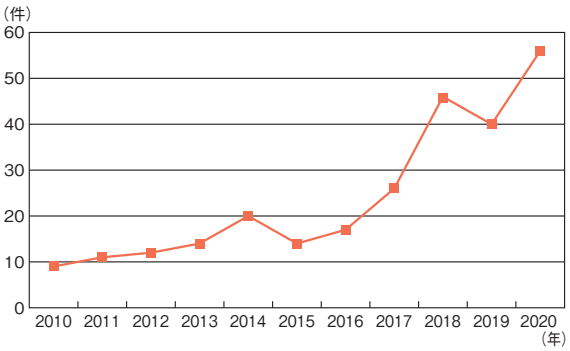
また、ランサムウェアが検出された件数が多かった上位 3 業種は「政府機関・公共」「銀行」「製造」だった（次ページ図 1-1-8）。



■図 1-1-8　業種別ランサムウェア検出台数トップ 10（2020 年）
（出典）トレンドマイクロ社「2020 年年間セキュリティラウンドアップ」を基に IPA が編集

(5) ウイルスのマルチプラットフォーム化

Intezer Labs の調査によると、Linux を狙ったウイルスが急増しており、2020 年には 56 件ものファミリーが観測された（図 1-1-9）。

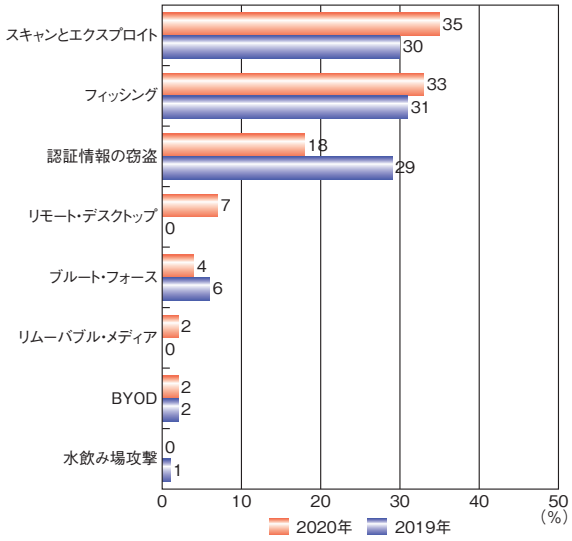


■図 1-1-9　新しく発見された Linux を狙ったウイルスのファミリー数の変化（2010 ～ 2020 年）
（出典）Intezer Labs「2020 Set a Record for New Linux malware families」を基に IPA が編集

IBM 社の調査によると、プログラミング言語の一つである Go で書かれたウイルスが 1 月から 6 月の間に 500% 増加したとしている。実際、Go は、ドイツの病院や日本の自動車メーカが被害に遭ったランサムウェア「SNAKE」（別名、EKANS）※16 の記述にも利用され、IoT の分野では Mirai のメイン（サーバ）側のプログラムの記述にも利用されている※17。Go は Windows のみでなく Linux や macOS 等のコンパイラがあり、一つのソースコードを作成することで、容易にマルチプラットフォーム化が実現できるため、ウイルスによる被害の拡大が懸念されている。

(6) 脆弱性を突く攻撃の増加

IBM 社によると、IBM Security X-Force Incident response によって観測された攻撃手口の内訳では、脆弱性の「スキャンとエクスプロイト」が最も多く、2019 年よりも増加している（図 1-1-10）。また、「リモート・デスクトップ」の増加は、テレワークに伴う自宅からのリモートアクセス、クラウドサービスやコラボレーションツールの利用拡大の影響があると考えられる。



■図 1-1-10　攻撃手口の内訳※18
（出典）IBM 社「IBM X-Force 脅威インテリジェンス・インデックス 2021」「IBM X-Force 脅威インテリジェンス・インデックス 2020※19」を基に IPA が編集

2020 年に頻繁に悪用された脆弱性の上位を表 1-1-2 に示す。2020 年に公表されたものよりも以前からある未修正の脆弱性を狙ったものが多い。

またテレワークが増加するとともに、外部の脅威から社内ネットワークを保護する目的で導入した VPN（Virtual Private Network）製品に存在する様々な脆弱性が攻

順位	CVE No.	内容
1	CVE-2019-19871	Citrix Application Delivery Controller
2	CVE-2018-20062	NoneCMS ThinkPHP のリモート・コード実行
3	CVE-2006-1547	Apache Software Foundation (SAF) Struts の ActionForm
4	CVE-2012-0391	Apache Struts の ExceptionDelegator コンポーネント
5	CVE-2014-6271	GNU Bash のコマンド・インジェクション

■表 1-1-2　2020 年に最も頻繁に悪用された上位五つの脆弱性
（出典）IBM 社「IBM X-Force 脅威インテリジェンス・インデックス 2021」を基に IPA が編集

撃者に悪用されている（「1.2.1 (3) (c) VPN 製品や公開サーバ等の脆弱性を悪用した攻撃」「1.2.2 (1) 新たなランサムウェア攻撃の被害事例」「1.2.5 (1) VPN 製品の脆弱性を対象とした攻撃」「1.3.1 (3) テレワーク等で使われるソフトウェアの脆弱性について」参照）。トレンドマイクロ社によると、2020 年には、主要な VPN 製品の脆弱性について表 1-1-3 に示す件数が検出されている。

CVE No.	内容	年間検出数
CVE-2019-11510	Pulse Secure VPN における複数の脆弱性	784,063
CVE-2018-13379	Fortinet FortiOS におけるパストラバーサルの脆弱性	413,641
CVE-2019-19781	Citrix Application Delivery Controller	21,652

■表 1-1-3　主要な VPN 製品の脆弱性の年間検出数
（出典）トレンドマイクロ社「2020 年年間セキュリティラウンドアップ」を基に IPA が作成

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※20
- トレンドマイクロ社：2020 年年間セキュリティラウンドアップ
- 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※21
- フィッシング対策協議会：月次報告書※22

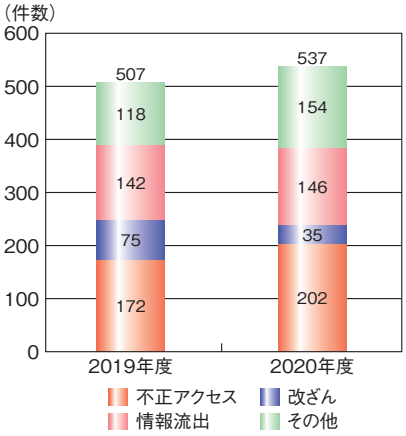
(1) 情報セキュリティインシデントの発生状況

MBSD 社によれば 2020 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 537 件で、2019 年の 507 件から 5.9% 増であった（図 1-1-11）※23。割合が最も多いのは「不正アクセス」で、37.6% であった。前年比では、「不正アクセス」が 117.4%、「改ざん」が 46.7%、「情報流出」が 102.8%、「その他」が 130.5% であった。

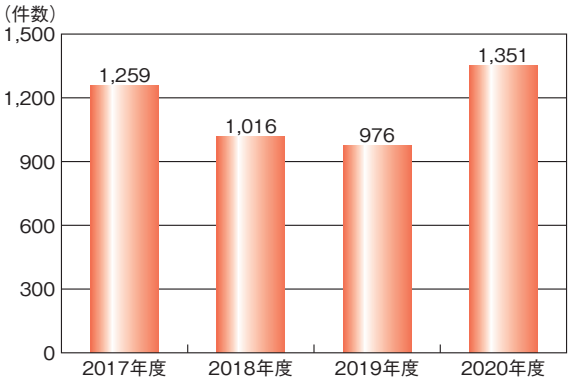
(2) Web サイト改ざんによる被害

2020 年 4 月 1 日から 2021 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 1,351 件で前年比 138.4% であった（図 1-1-12）。

過去 4 年間では、2020 年度の報告件数が最も多い。

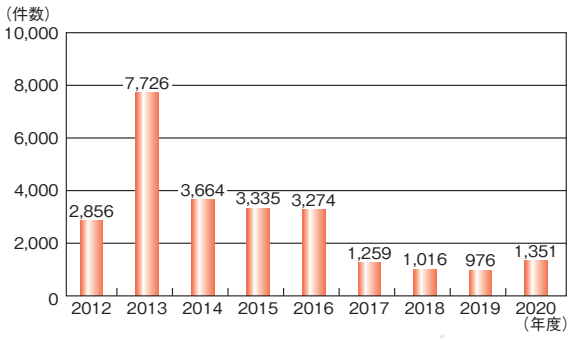


■図 1-1-11　情報セキュリティインシデントの種類別報道件数
（出典）MBSD 社の集計情報を基に IPA が作成



■図 1-1-12　Web サイト改ざん年度別件数推移（2017 ～ 2020 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～ 2021 年 3 月 31 日）を基に IPA が作成

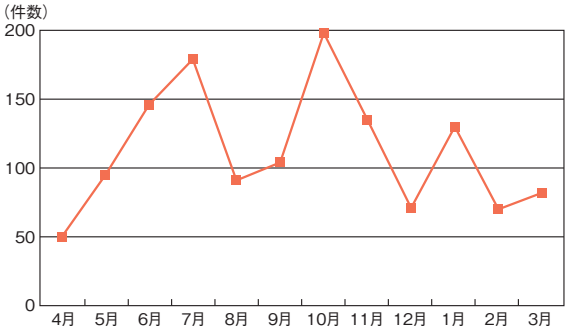
しかし更に遡れば、2014 年度から 2016 年度の 3 年間は 3,000 件を超える改ざんが報告されていた（図 1-1-13）。当時と比べて直近の 4 年間は 1,000 件前後で推移しており、小康を保っているといえる。



■図 1-1-13　Web サイト改ざん年度別件数推移（2012 ～ 2020 年度）
（出典）JPCERT/CC「インシデント報告対応レポート」（2012 年 4 月 1 日～ 2021 年 3 月 31 日）を基に IPA が作成

月別では 2020 年 10 月の 198 件、四半期別では 2020 年 10 ～ 12 月が 404 件で最も多かった（次ページ図 1-1-14）。JPCERT/CC の「インシデント報告対応レポート」に

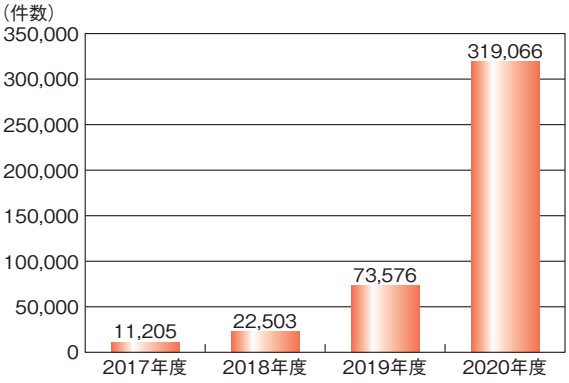
よれば当該四半期は、改ざんされたWebサイトから、特定ブランドを扱うEコマースサイトに誘導される事例が複数寄せられたという※24。そのほか、4～6月期にはWebサイトに不正に埋め込まれたコードによって「当選詐欺」のサイトに転送される事例が多く確認された。この当選詐欺ページでは個人情報の入力が求められることから、個人情報の収集が目的だと考察している※25。



■図1-1-14　Webサイト改ざん月別件数推移（2020年度）
（出典）JPCERT/CC「インシデント報告対応レポート」（2020年4月1日～2021年3月31日）を基にIPAが作成

(3) フィッシングによる被害

フィッシング対策協議会への2020年度の報告件数は前年の4.3倍にも上った。過去4年間を見ても突出した報告件数である（図1-1-15）。

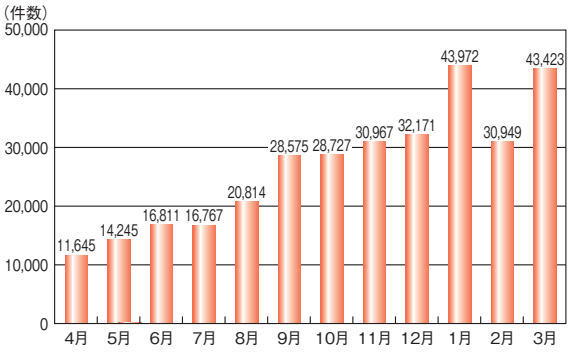


■図1-1-15　年度別フィッシング報告件数（2017～2020年度）
（出典）フィッシング対策協議会「月次報告書」（2017年4月～2021年3月）を基にIPAが作成

月別報告件数は8月に2万件を超過、11月には3万件を突破し、1月と3月には4万件を超す報告があった（図1-1-16）。

また、フィッシングに悪用されたブランドで年度を通じ、最も報告件数が多かったのがAmazonであった。全報告件数に占めるAmazonの割合が50%を超える月が8ヵ月もあった※26。

楽天も年度を通じ常に報告件数の上位4社に入って



■図1-1-16　月別フィッシング報告件数（2020年度）
（出典）フィッシング対策協議会「月次報告書」（2020年4月～2021年3月）を基にIPAが作成

いる。また、2020年度上半期にはApple、LINEの報告件数が上位に入っていたが、下半期にかけては三井住友カードが2位を占める月が多く、他の複数のクレジットカード銘柄が上位を占めていた（表1-1-4）。上位4社に関係する報告以外では、10月に総務省になりすまし、特別定額給付金に関する通知を装うフィッシングメールの送信が相次いだという※27。IPAでも同じ時期に、特別定額給付金の偽サイトを確認した（「1.2.7 (2) 世の中の関心に乗じるメールの手口」参照）。

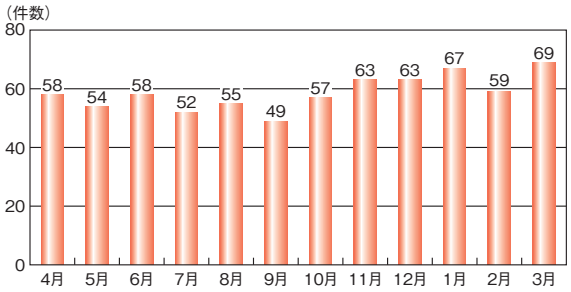
	4月	5月	6月	7月	8月	9月
1位	Amazon	Amazon	Amazon	Amazon	Amazon	Amazon
2位	Apple	Apple	Apple	Apple	LINE	楽天
3位	LINE	LINE	LINE	楽天	楽天	三井住友カード
4位	楽天	楽天	楽天	LINE	楽天カード	LINE
	10月	11月	12月	1月	2月	3月
1位	Amazon	Amazon	Amazon	Amazon	Amazon	Amazon
2位	三井住友カード	三井住友カード	三井住友カード	三井住友カード	三井住友カード	楽天
3位	楽天	楽天	楽天	楽天	楽天	MyJCB
4位	MyJCB	MyJCB	アプラス（新生銀行カード）	MyJCB	三菱UFJニコス	三井住友カード

■表1-1-4　フィッシングに悪用されたブランド月次トップ4（2020年度）
（出典）フィッシング対策協議会「月次報告書」（2020年4月～2021年3月）を基にIPAが作成

フィッシングに悪用されたブランドの月間件数は、年度を通じ50件から60件前後で推移している（次ページ図1-1-17）。

一方、表1-1-4にある悪用されたブランドの上位4位が報告件数全体の8割から9割を占めており、例えば、2020年8月は92.6%、9月は93.2%であった※28。

フィッシングは従来のメールによるものだけでなく、SMS



■図 1-1-17　フィッシングに悪用されたブランド件数（2020 年度）
（出典）フィッシング対策協議会「2021/03 フィッシング報告状況※29」を基に IPA が編集

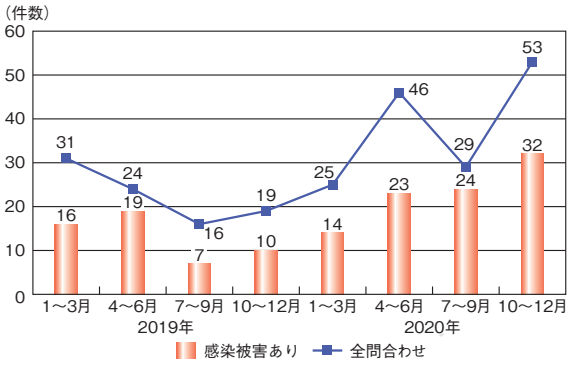
（Short Message Service）から誘導させるものがあり、メールに比べ本物と誤認したり、ついアクセスしてしまう傾向があるという。また、フィッシング以外にも年度を通じて、宅配業者の不在通知を装った SMS についての報告が多く受領されていた※29。IPA の安心相談窓口に寄せられる相談も前年を上回り、手口に変化が生じていることも確認している（「1.2.7（3）（a）宅配便の不在通知を装う SMS」参照）。

（4）注目された新たな脅威

2020 年度は世界中で新型コロナウイルスが蔓延し、生活環境が一変した。日本でもテレワークや業務・サービスのデジタル化が急速に進展し、新たなサイバー脅威となった。その一方で、既存の攻撃手法も巧妙化が続き、新たなサイバー脅威となった。

（a）新たなランサムウェア

トレンドマイクロ社の調査では、国内法人から報告されたランサムウェアの被害件数は 2019 年の 52 件から、2020 年には 93 件と前年比約 1.8 倍に増加した（図 1-1-18）。IPA が毎年発表する「情報セキュリティ 10 大脅威」



■図 1-1-18　国内法人からのランサムウェア関連の問い合わせ件数とそのうちの被害報告件数（2019 ～ 2020 年）
（出典）トレンドマイクロ社「2020 年年間セキュリティラウンドアップ」を基に IPA が編集

においても、2021 年版では組織のランキングで「ランサムウェアによる被害」が 1 位となった※30-1。2016 年版に初めてランキングされて以降、1 位になったのは初めてである※30-2。

同調査によれば 2020 年に国内で顕在化したのは「新たなランサムウェア攻撃」と呼ばれるもので、2019 年末に登場し、2020 年を通じて広がったという。新たな手口では、ランサムウェアに感染させ身代金を要求するだけでなく、ランサムウェアで暗号化する前に被害企業のデータを窃取しておき、支払わなければデータを暴露すると脅し、身代金の支払いを強要する（「1.2.2 新たなランサムウェア攻撃」参照）。被害に遭った株式会社カプコンの発表によれば※30-3、感染のきっかけは北米の現地法人が保有していた旧型 VPN 装置への不正侵入であったという。ウイルスメールを送り開封させることで、ネットワークに侵入するというこれまでの感染経路とも異なっている。新たなランサムウェアには、標的型攻撃と同様の多層的な対策が、従来の対策に加え必要である、と IPA も指摘している（「1.2.2（4）新たなランサムウェア攻撃への対策」参照）。

（b）VPN 製品の脆弱性

テレワーク普及に伴い、境界防御の限界が指摘されるようになった。テレワーク下では組織外からのアクセスが常態化するが、安全に接続するために VPN 製品の利用が広がった。トレンドマイクロ社によれば 2020 年を通じ、主要な VPN 製品（表 1-1-5）のうち Pulse Secure, LLC.、Fortinet, Inc.、Citrix Systems, Inc. の製品の四つの脆弱性を攻撃する通信を月平均 10 万件検出したという。

2020 年度に脆弱性対策情報データベース「JVN iPedia」に登録された VPN 製品の脆弱性対策情報の深刻度レベルでも、レベルⅡ（警告）以上が 9 割以上を占めていた。VPN 製品の脆弱性は深刻度の高さの問題

公表時期	社名	CVE	CVSS v3
2019 年 4 月	Pulse Secure	2019-11539	7.2（重要）
2019 年 4 月	Pulse Secure	2019-11510	8.8（重要）
2019 年 5 月	Fortinet	2018-13379	7.5（重要）
2019 年 7 月	Palo Alto Networks	2019-1579	8.1（重要）
2020 年 1 月	Citrix Systems	2019-19781	9.8（緊急）
2020 年 7 月	F5 Networks	2020-5902	9.8（緊急）

■表 1-1-5　主要 VPN 製品において公表された脆弱性のリスト
（出典）トレンドマイクロ社「2020 年年間セキュリティラウンドアップ」を基に IPA が編集

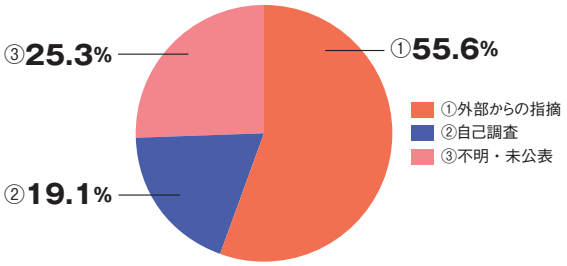
だけでなく、利用経験が浅く、不慣れなまま急速に利用が進み、脆弱性対策情報の収集やアップデートが疎かになった可能性をIPAでは指摘している（VPNの脆弱性については「1.3.1(3)テレワーク等で使われるソフトウェアの脆弱性について」参照。また攻撃については「1.2.5(1)VPN製品の脆弱性を対象とした攻撃」参照）。

なお、「情報セキュリティ10大脅威2021」では、VPNを狙った攻撃等が「テレワーク等のニューノーマルな働き方を狙った攻撃」として、初登場で3位となっている。

(c)クラウドサービスからの情報漏えい

クラウドサービスの利用は2019年までの過去5年で2割増加した※30-4。そして2020年に発生した新型コロナウイルスのパンデミックにより、企業のクラウド導入が数年加速されたという指摘もある※30-5。

トレンドマイクロ社によれば、2020年に公表された情報漏えい事例（Webやクラウドのシステムからの漏えい）は99件あり、約2,500万件の情報漏えいが公表された。漏えいが発覚した理由は55.6%が「外部からの指摘」であった（図1-1-19）。

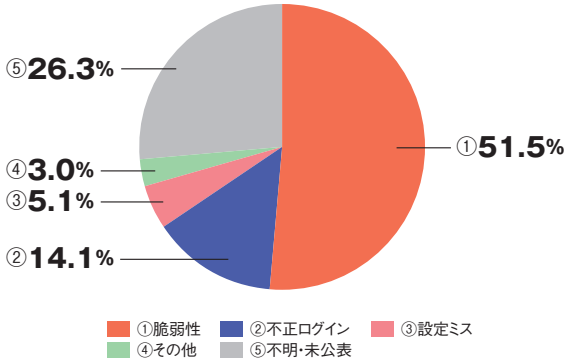


■図1-1-19　2020年に公表されたクラウドからの情報漏えい事例99件の発覚事由
（出典）トレンドマイクロ社「2020年年間セキュリティラウンドアップ」を基にIPAが編集

また、発生原因の51.5%が「脆弱性」を悪用した攻撃であった（図1-1-20）。「不明・未公表」を除くと、「不正ログイン」（14.1%）、「設定ミス」（5.1%）と続く。「設定ミス」の件数は少ないものの、漏えいした情報の件数では約2,156万件と全体の9割を占めた。

2021年にも38の自治体や国内企業の個人情報等が設定ミスにより外部から閲覧可能であったと報道され※30-6、設定ミスによる漏えいが相次いでいる（「1.2.8(3) 過失やシステム不具合による情報漏えい・情報紛失」参照）。

脆弱性も設定ミスも発生原因のほとんどがシステムの運用にあるため、対策次第では限りなくゼロに近づけることができる、とトレンドマイクロ社は指摘している。



■図1-1-20　2020年に公表されたクラウドからの情報漏えい事例99件における原因
（出典）トレンドマイクロ社「2020年年間セキュリティラウンドアップ」を基にIPAが編集

(d)「ドコモ口座」を利用した不正送金

2020年9月、株式会社NTTドコモが提供するマネーサービス「ドコモ口座」を介した銀行の預金の不正引き出しが発覚した。同社は2020年9月3日に銀行からの通報で事態を把握したという※30-7。9月9日には、17の地銀との「ドコモ口座」の連携を中断し※30-8、35行との新規登録を当面停止すると発表した※30-9。「ドコモ口座」はスマホ決済や送金が行えるサービスで、ドコモの通信回線利用者でなくても、「dアカウント」保有者であればメールアドレスだけで開設が可能であった。また本人認証は連携する銀行口座の登録をもって本人とみなしていたという※30-10。不正送金を引き起こした要因としては上記のような口座開設時の本人確認の甘さ、及び銀行口座連携時の本人認証の不備が指摘されている。各行の認証方式は一様ではなく※30-11、被害に遭った口座では多要素認証が採用されていなかったことが指摘されている。中でも株式会社ゆうちょ銀行は、他のサービスの連携においても多要素認証を導入しておらず、「ドコモ口座」以外でも被害を発生させていた※30-12。

株式会社NTTドコモは2021年1月29日に、停止していた銀行口座の新規登録及び銀行口座からのチャージを2月3日から順次再開すると発表した。サービス再開にあたっては、以下のような対策を実施するとしている※30-13。

- オンライン本人確認システム（eKYC）※30-14の導入
- dアカウントの連絡先携帯電話番号登録
- 専門スタッフによる24時間365日の監視

COLUMN

AIとセキュリティ

AIとセキュリティの関係は、① Attack using AI（AIを利用した攻撃）、② Attack by AI（AIによる攻撃）、③ Attack to AI（AIへの攻撃）、④ Measure using AI（AIを利用したセキュリティ対策）の観点に分けることができます[i]。

① Attack using AIは、人によって行われていた攻撃を、AIを用いて自動化するというものです。例えば、最近、ボットを利用して、コンサートなどのチケットの買い占めが試みられており、あるサイトではチケット購入のアクセスのうち9割超がボットでした[ii]。近い将来、AI機能付きのウイルスが誕生するだろうと言われており、大きな脅威をもたらすことが想定されます。

② Attack by AIは、AI自身による自律的な攻撃を指します。一部の識者にはAIが進化し、人間を超越するシンギュラリティが生じ、AIの攻撃により将来的に人間が絶滅させられるだろうという危惧があります。ただし、現状は「強いAI（汎用AI）」ではなく「弱いAI（専用AI）」の研究が中心であり、弱いAIが汎用的な能力を発揮し、高度なAIを自動的に作ることは困難という見方が多数を占めています[iii]。

③ Attack to AIには、訓練済みモデルの誤分類を誘発するノイズ付加攻撃があります。例えば、動物名を判定するシステムに対し、パンダの画像に微細なノイズを加えることにより、人間が見ればパンダですが、システムにテナガザルと誤判断させるような攻撃が知られています[iv]。また、機械学習に対して、偏った訓練データを意図的に与えること等により、不適切な判断をさせてしまう攻撃があります。例えば、米Microsoft社のチャットボット「Tay」は、クラウドソーシングを利用して学習させました。ところが悪意を持ったユーザたちが協力して差別的な意見を繰り返し入力したことで、Tayは差別発言を繰り返すようになってしまいました[v]。これらは、重要な課題であり、現在いろいろな研究が行われている分野です。

④ Measure using AIは、セキュリティ対策にAIを用いるアプローチです。論文やWeb上の製品紹介を調べたところ、「マルウェアの検出」「ログの監視･解析」「継続的な認証」「トラフィックの監視・解析」「セキュリティ診断」「スパムの検知」「情報流出」等にAIを使ったというセキュリティ対策ツールは各社から提供されており、そのメリットがWeb上で述べられています。このようにセキュリティ対策のために機械学習を中心とするAIが既に使われていますが、現状では実際のフィールドでどの程度有効であるのかは、多くの場合不明です。

i “A Study on Classification and Integration of Research on both AI and Security in the IoT Era,” Ryoichi Sasaki, Tomoko Kaneko, Nobukazu Yoshioka 11th International Conference on Information Science and Applications (ICISA2020), 2020
ii ITmedia NEWS：チケット購入のアクセス「9割がbot」にびっくり“知恵比べ”の舞台裏 https://www.itmedia.co.jp/news/articles/1809/05/news064.html〔2021/5/21確認〕
iii J. Searle, 1980, "Minds, Brains and Programs", The Behavioral and Brain Sciences, vol. 3. https://www.cambridge.org/core/journals/behavioral-and-brain-sciences/article/abs/minds-brains-and-programs/DC644B47A4299C637C89772FACC2706A〔2021/5/21確認〕
iv OpenAI：Attacking Machine Learning with Adversarial Examples https://openai.com/blog/adversarial-example-research/〔2021/5/21確認〕
v Microsoft社：Learning from Tay's introduction https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/〔2021/5/21確認〕

1.2 情報セキュリティインシデント種類別の手口と対策

本節では、インシデントの種類別の発生状況と、具体的な事例について述べる。また、2020 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）の内部に数年間潜入して活動していたと考えられる事例も日本国内で確認されている※31。

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）。

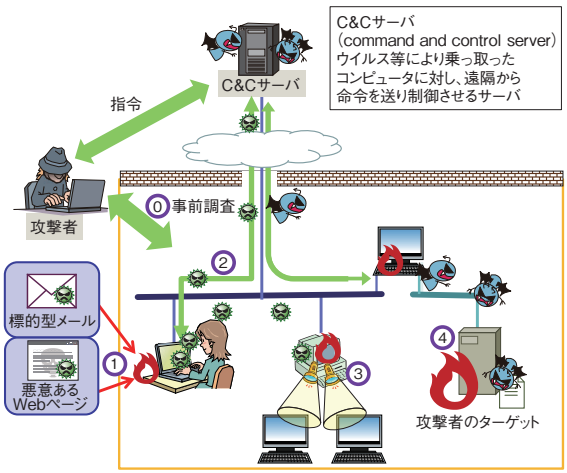
「事前調査段階」では、標的組織や業界の情報を収集する。公開されている情報を収集するだけでなく、標的組織と他の組織とのメールによるやり取りの盗聴等により必要な情報を収集することもある。

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。多くの場合、標的組織の人間に対し、ウイルスを仕込んだファイルを添付したメール（標的型攻撃メール）を送り付ける手口が用いられてきた。標的型攻撃メールでは、標的組織や業界に合わせてメール文面が作成されることが多い。また、ウイルスを仕込んだファイルをパスワードが設定された圧縮ファイルに格納して添付することで、セキュリティソフトの検知を回避する工夫がなされることもある。昨今の傾向としては、正規の SNS サービスやオンラインストレージサービスを悪用してウイルスに感染させる手口や、VPN 製品等の脆弱性を悪用した手口も確認されており、多様化、巧妙化している。

「初期潜入段階」で標的組織の内部に侵入した攻撃者は、「攻撃基盤構築段階」へと移り、標的組織内の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（バックドアの作成を試みる）。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。RAT への感染は、別のウイルスをダウンロードする機能を持つ「ダウンローダ」と呼ばれるウイルスを用いて行われることが多い。

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。なお、「攻撃基盤構築段階」や「システム調査段階」で使われるツールには、感染したパソコン内で利用できる正規のツールや、広く公開されているオープンソースソフトウェアが悪用される場合もある。

「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、工場や発電所といった生活インフラを支える施設の停止等を目的とした攻撃も確認されている※33。



⓪［事前調査段階］
ターゲットとなる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※32」を基に編集

(1) 国内の標的型攻撃事例

ここでは、2020 年度に確認された、国内組織の海外

拠点を狙った標的型攻撃の事例を紹介する。

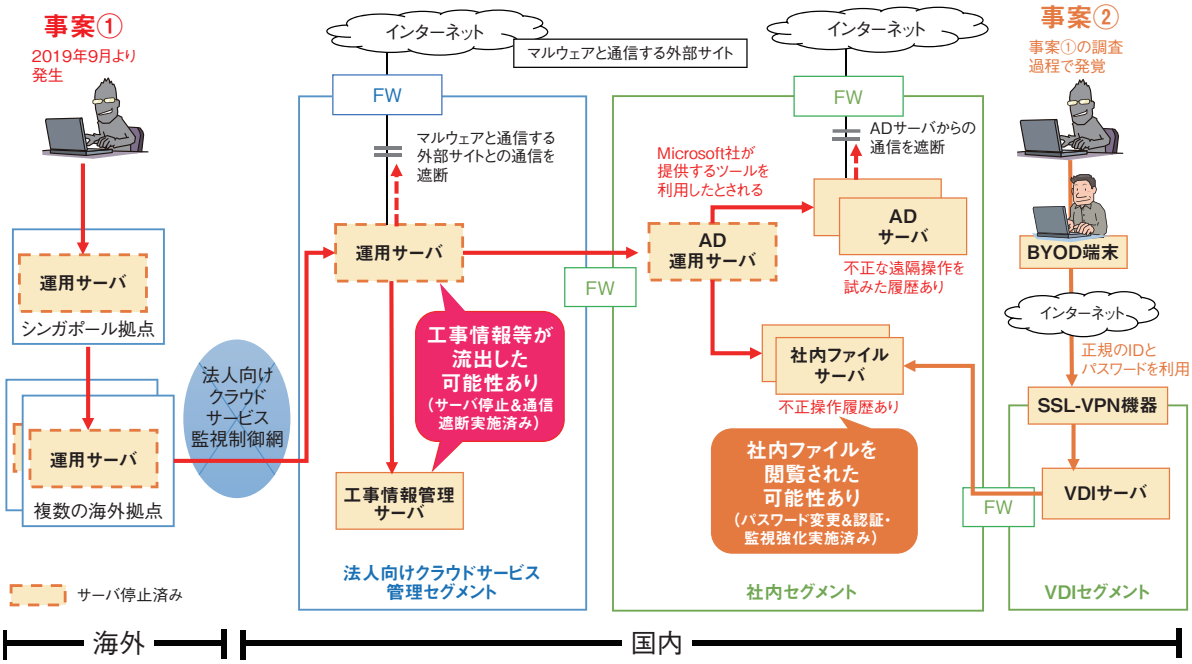
2020 年 5 月に、エヌ・ティ・ティ・コミュニケーションズ株式会社（以下、NTT コム社）の海外拠点への侵入を発端とした標的型攻撃の事案が、同社プレスリリースにて発表された※34。更に、7 月には第 2 報が報告された※35。

同社プレスリリースによれば、日本国内の同社社内セグメントにある AD（Active Directory）サーバに対して、不正な遠隔操作を試みたログによって、初めて異常が検知されたという。この事象を受け、同社は関連するシステムに対してフォレンジック調査を実施、調査結果を報告している。それによると、次に示す二つの事案が確認されたという。

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。

- 事案①：海外拠点を起点とする攻撃
  「初期潜入段階」として最初に侵害を受けたのは、シンガポール拠点の運用サーバであった。攻撃者グループはこの起点から複数の海外拠点のサーバを侵害、その後、監視制御網を経由して、同社が持つ国内の法人向けクラウドサービス※36 の管理セグメントに攻撃範囲を拡大していった。同セグメントで稼働していた運用サーバを侵害した後、同社社内の AD サーバにアクセス可能な社内セグメントの AD 運用サーバを侵害した。また、法人向けクラウドサービスの管理セグメントの運用サーバからは工事情報管理サーバにもアクセスが確認されており、業務情報の不正閲覧や漏えいの可能性があるとしている。更に社内セグメントの AD 運用サーバから、AD サーバと社内のファイルサーバにアクセスされたという。
  なお、AD サーバへのアクセスには、Microsoft 社が提供するツールが利用されていたという。また、法人向けクラウドサービスの管理セグメントの運用サーバ、社内セグメントの AD 運用サーバはともに、リプレースで廃棄された AD サーバ（初めに侵入を検知した AD サーバとは別）の管理アクセス用に用意されていたものであり、不正アクセス発生時点では使用されていなかったという※37。
- 事案②：BYOD※38 端末（VDI 接続）を起点とする攻撃
  事案①の調査のため、社内ファイルサーバをフォレンジック調査したところ、別の経路での侵害行為が確認された。これは社員が社外からのリモートアクセスに利用していた BYOD 端末からの不正アクセスであり、社内ファイルサーバ上のファイルが閲覧された可能性があるとしている。攻撃者は窃取された正当なアカウントとパスワードを用いていたため、閲覧された可能性のある情報の特定に時間を要したという。

結果として、事案①と事案②を合わせて約 900 社に関係する業務情報が流出した可能性があるとしている。



■図 1-2-2　標的型攻撃の事例概要
（出典）NTT コム社「当社への不正アクセスによる情報流出の可能性について（第 2 報）※35」を基に IPA が編集

また事案①と事案②について、直接的な結び付きは確認されていないが、同一攻撃者グループであるとすれば、攻撃者グループは複数の攻撃手法を用い、広範囲に攻撃を仕掛けたことになる。

本事例の特徴の一つは、廃棄予定であったサーバが攻撃者に利用されていた点である※37, 39。廃棄予定のシステムでは利用者がいないため、修正プログラムの適用といった運用が適切に行われず、セキュリティ監視や監査等も疎かになってしまいがちである。廃棄予定のシステムであっても、その廃棄が完了するまでは、適切なセキュリティ運用を維持すべきである。

(2) 標的型攻撃の傾向

日本国内の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。

2020 年の傾向としては、2019 年と同様に、海外の関連組織を足掛かりとした事例が複数報告されており、引き続き注意が必要である。また、これまで初期侵入段階では標的型攻撃メールが主な手口とされていたが、複数のセキュリティベンダによれば、VPN 製品の脆弱性を悪用しているケースや、悪意のあるファイルの受け渡し方法として SNS を介したもの等、複数の手口が報告されている。

加えて攻撃基盤構築段階においても、より検知されにくい方法を取る等、その手口は巧妙化している。

(3) 標的型攻撃の手口（初期侵入段階）

初期侵入段階における、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合わせ、攻撃者もその手口を変化させていくことが容易に想像でき、新たな手口への注意も必要である。

(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ものである。

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、署名等に利用するケースが過去に確認されている。2020 年には、「新型コロナウイルス」「日露や日韓の外交」「企業への履歴書や申し込み」等がメールの題材として悪用されていたことが確認されている※40。

標的型攻撃メールの添付ファイルの騙しの手口として、Word ファイルや Excel ファイルに悪意のあるマクロを忍ばせているケースや、PDF を装ったショートカットファイルを悪用するケースが確認されている。ショートカットファイルを悪用するケースでは、例えば悪意のあるファイルを Microsoft OneDrive 等のオンラインストレージに格納し、その URL リンクをメール本文や SNS 等のメッセージに張り付け、誘導する。また、添付ファイルに攻撃者が意図的にパスワードを付与するケースもあり、注意が必要である。パスワード付きファイルは、組織で実施しているセキュリティ対策の仕組みが十分に機能しない場合があり、攻撃者はセキュリティ対策を回避するために、悪用することがあり得る。

(b) サプライチェーン・海外拠点等への攻撃

前述の国内組織の海外拠点を狙った事例のように、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、サプライチェーンにおける取引先企業や、海外拠点または海外の子会社を初期侵入のターゲットにした攻撃の手口が確認されている。

これは、海外拠点に対しては国内のセキュリティガバナンスが届きにくい傾向があり、特に小規模の組織や拠点ではセキュリティレベルが低くな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。

取引先企業が狙われるケースでは、取引先企業の正規のメールアカウントが乗っ取られることもある。攻撃者はメールアカウントを乗っ取った後、実際にやり取りしているメールを取得・分析し、返信や再送という形で流用する。この場合、メール受信者が不審なメールであることを見抜ける可能性は大きく低下する。

(c) VPN 製品や公開サーバ等の脆弱性を悪用した攻撃

国内のセキュリティベンダが観測した標的型攻撃では、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たことが報告されている※41。

また別のセキュリティベンダのレポートでは、2020 年 1 月末から 2 月にかけて、「BlackTech」と呼ばれる攻撃者グループによる活動が報告された※42。BlackTech は、

当初台湾と台湾に関連した組織を標的としていたが、2017 年より日本も標的に加えている。この BlackTech が利用する攻撃ツールの一部には、Linux 版のウイルス（RAT）も確認されており、VPN 製品や公開サーバ等の脆弱性を悪用して侵入し、公開サーバにウイルスを設置する手法が取られている。

(d) SNS を悪用した攻撃

2020 年 8 月には三菱重工業株式会社が、社内ネットワークに対して第三者からの「不正アクセス」を受け、従業員の情報が流出したと発表した※43。このケースでは、同社グループ従業員が、在宅勤務時に社有のモバイルパソコンから外部ネットワーク上の SNS に直接アクセスし、SNS 上の第三者からウイルスを含んだファイルを受領、ウイルスに感染してしまった。その後、当該パソコンを社内ネットワークに接続したことで感染が拡大した。感染が拡大した一因として、感染したパソコン上のアカウントとパスワードを、社内ネットワーク上の一部サーバのローカル特権アカウントでも利用していたことが挙げられる。

また複数のセキュリティベンダから、ビジネス特化型 SNS である LinkedIn を悪用した攻撃手口が報告されている※44。攻撃者は標的組織に侵入するため、大手企業の人事担当を装って、標的組織の従業員に偽の求人情報を送信する。従業員が関心を示すと、更にウイルスを仕込んだ求人情報に関連するファイルを送り、実行させる。この攻撃については「Lazarus」と呼ばれる北朝鮮の攻撃者グループが関与しているとされている。なお、Lazarus の攻撃活動には日本の組織が標的となったものも確認されている。

(4) 標的型攻撃の手口（攻撃基盤構築段階）

侵入後の攻撃基盤構築段階における手口の一部を、以下に示す。

(a) オープンソースソフトウェアや標準的なソフトウェア等を利用した攻撃

JPCERT/CC のインシデント報告レポート※45 によると、2020 年 7 月から 9 月の期間に発生した Lazarus による攻撃では、侵入後の攻撃基盤構築段階で、GitHub 等で公開されているオープンソースのツールを悪用していることが報告されている。また、JPCERT/CC の公式ブログでは、多くの攻撃者グループに利用されているオープンソースの RAT である「Quasar 並びに Quasar から派生した QuasarFamily」の一部を紹介している※46。

このように攻撃者は、オープンソースのツールを駆使することで、既存のセキュリティソフト等のセキュリティシステムによる検知を回避し、かつ短期間での攻撃の成功を実現しようとしている。

また攻撃者は、侵入先で利用可能な標準的なソフトウェアやコマンドを利用して、ネットワーク内の攻撃基盤を広げる。このテクニックは、「環境寄生型」攻撃や「LOLBIN（Living Off the Land Binary）」を使用した攻撃と呼ばれている。JPCERT/CC の公式ブログでは、Lazarus が侵入したネットワーク内で使用する標準的なソフトウェアやコマンドを紹介している※47。

(b) 認証情報の取得

端末の侵害に成功した場合に、攻撃者はその端末内で使われている認証情報（ID・パスワード）の取得を試みる。その手法としては、「Mimikatz」というツールの悪用が有名である。Mimikatz は、古い Windows OS で使用されていたシングルサインオン機能の弱点を突いて、メモリ上からログイン情報を取得するツールであり、ペネトレーションテスト等でも利用されている。

(c) AD サーバを標的とした攻撃

標的組織に侵入した攻撃者は、AD サーバを次のターゲットにする傾向がある。

一般的に AD サーバはインターネットからアクセスできない内部ネットワーク上に構築されることから、セキュリティ上リスクが少ないサーバであると考えてしまう傾向が強い。更に、認証サーバの停止等が伴うメンテナンスは、影響が大きく、実施しづらい。このため、AD サーバの脆弱性への対応は疎かになりがちである。一方、攻撃者にとっては、仮に AD サーバを掌握できると、グループポリシーによるウイルスの配信が可能となる等、攻撃者が得るリターンが大きい。

標的型攻撃において AD サーバを狙う傾向は、以前からも確認されており、2017 年には、JPCERT/CC より「ログを活用した Active Directory に対する攻撃の検知と対策※48」というレポートも公開されている。

また 2020 年 8 月には、Windows が実装する Netlogon リモートプロトコルの脆弱性が報告され、早期のアップデートが推奨された※49。この脆弱性を突いた攻撃が成功すると、認証されていない第三者が AD のドメイン管理者のアクセス権を取得でき、ドメイン配下の機器が掌握される危険性があった。

なお AD サーバを攻撃目標とする事例は、標的型攻

撃だけではなく、ランサムウェア攻撃でも多く報告されている。

(5) 標的型攻撃への対策

標的型攻撃の傾向や手口に記載したとおり、攻撃者はあらゆる手段を利用し、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ものではなく、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、情報資産を守る側としてはあらゆる可能性を考慮し、対策の検討と選別、実施が必要である。以下に、その一例を示す。

(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、標的とする企業・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。しかしながら、すべての標的型攻撃メールが見破れない程完成度の高いものではないことも事実としてある。

  不審メールに対する注意力向上のため、組織としては利用者への教育や注意喚起を実施することが望ましい。また利用者自身も日頃から不審メールに対する意識を高め、不用意に開封や返信をしないことが求められる。

  不審メールにおいて注意すべき点の例を以下に示す。

  - 偽装の手口の一つとして、メールソフトが表示する送信者の名前を偽装しているメールも存在する。送信者の情報を確認する際は、表示されている送信者名ではなく、メールアドレスが正しいかどうかを確認する。また送信元のメールアドレスに無料で取得できるフリーメールアドレスが使用されていることも多く、不審メールかどうかの判断材料の一つになり得る。
  - これまでのやり取りでは想像できないような話題を持ちかけるメールや、添付ファイルやオンラインストレージサービス等の URL リンクを開くことを要求してくるメールに注意する。
  - メール本文中の署名欄に記載される連絡先は攻撃者によって偽装されている可能性があるため、受信したメールが正規のものかどうかを確認する場合は、信頼できる公式の問い合わせ先を利用する。
  - 関係する企業・組織の Web サイトで「不審なメールの送信を確認している」といった注意喚起が掲載されていないか確認することも有効である。

- 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を送り、それを開かせることで侵入経路を開拓する。

  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が有効である。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。

- マクロ機能の危険性の周知

  Microsoft Office のマクロ機能は便利な機能ではあるが、攻撃者が悪用すれば意図した処理が実行できる。マクロ機能はデフォルトでは無効となっており、ファイルを開いただけでは動作せず、手動で有効化する必要がある。しかし、マクロ機能は多くの組織で広く使用されており、危険性を知らずに有効化する利用者がいる可能性もある。

  マクロ機能の悪用は、標的型攻撃メールだけではなく、ばらまき型メールでも多く用いられるため、不用意に「コンテンツの有効化」(マクロの有効化)を行わないよう注意が必要である。マクロを有効化する場合は、受け取ったファイルが信頼できるものであるかを確認し、安全性を確保してから行うように周知する。

- 標的型訓練メール等で実践的な訓練を実施

  疑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。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、報告が必要であることを指導することが望ましい。

  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、先に紹介した Microsoft Office の脆弱性の悪用等、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も対策の一つとして重要である。窓口が周知されていない場合、利用者がどこに連絡すればよいのか分からず、組織が攻撃を受けていることに気付くのが遅れてしまう可能性がある。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。そのため、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・外部における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。

  また CSIRT は、組織内外から得られるセキュリティインシデントの関連情報を集約し、最高情報セキュリティ責任者（CISO：Chief Information Security Officer）や役員等と連携してセキュリティインシデントに対応することも重要である。

- インシデント対応力の強化

  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、適切な対応ができるように対応能力を維持・向上させる取り組みが必要となる。

  CSIRT 向けの取り組みでは、他組織で発生したインシデントや自組織で起こり得るインシデントを基にシナリオを作成し、インシデントが発生したことを想定して演習を行う。演習を通じて、CSIRT の対応能力の維持・向上や現在の対応や体制の問題点の発見・改善を行い、実際のインシデントに備える。

- 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、その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、社内の利用者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の強化

  攻撃者グループはより侵入がしやすい海外拠点や海外子会社、取引先企業をターゲットにする傾向がある。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。実施の際には、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においては、セキュリティの対策状況や連絡体制を事前に共有し、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へ警告を行うことで、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。

  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。確保することで、不審メール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
  標的型攻撃では、OS やアプリケーション、VPN 製品といった機器の脆弱性を悪用するケースも存在する。そのため、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・端末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。
  特に今回手口として紹介したとおり、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 製品等のネットワーク製品の脆弱性を狙い、侵入後には AD サーバや情報の格納されたファイルサーバが攻撃の対象となる傾向があるので、それらについて抜かりなく対策していきたい。
- 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 .js や .ps1 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。
- セキュリティ対策の再チェック
  2020 年は新型コロナウイルス感染拡大により、テレワークの新規開始や利用拡大等、働き方が大きく変化した年となった。このため一部の組織では、急遽、VPN 製品等のシステム導入や、システム構成または設定の変更を行った結果、適切なセキュリティ設計や設定が行われず、これが脆弱な箇所となるケースもあったと思われる。
  そのようにセキュリティ設定をあえて緩和したこと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 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）製品の導入等を検討することも必要である。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）を検討することも必要になるであろう。

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 新たな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。

従来のランサムウェア攻撃では、攻撃者は明確な標的を定めず、ウイルスを添付したメールのばらまき等によって、個人、企業・組織を問わず、ランサムウェアへの感染を試みていた。ところが近年、企業・組織を標的とした、次の二つの方法※50 を使用した新たな攻撃が観測されている。

- 人手によるランサムウェア攻撃（human-operated ransomware attacks）
  標的型攻撃と同様の手口で、攻撃者自身が様々な方法を駆使して、企業・組織のネットワークへ侵入し、侵害範囲を拡大して、企業・組織内のパソコンやサーバをランサムウェアに感染させる攻撃方法。
- 二重の脅迫（double extortion）
  ランサムウェアにより暗号化されたデータを復旧するための身代金の要求に加え、暗号化する前にデータを窃取しておき、支払わなければデータを公開する等と脅迫する攻撃方法。窃取されたデータは、攻撃者がインターネットやダークウェブ上に設置した、データ公

開のための Web サイト（以下、リークサイト）にて公開される。

攻撃者は、これらの攻撃方法を用いて、企業・組織が事業継続のために、金銭を支払わざるを得ない状況を作り上げ、より確実に、かつ高額な身代金を得ようとしている。

図 1-2-3 に従来のランサムウェア攻撃と、新たなランサムウェア攻撃の差異のイメージを示す。

新たなランサムウェア攻撃では、IT システムを利用し、事業を行っている、あらゆる企業・組織が標的となり得る。2020 年 8 月に IPA[※51] が、また同年 11 月に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）[※52] が注意喚起を行っており、非常に注意を要する状況にあるといえる。

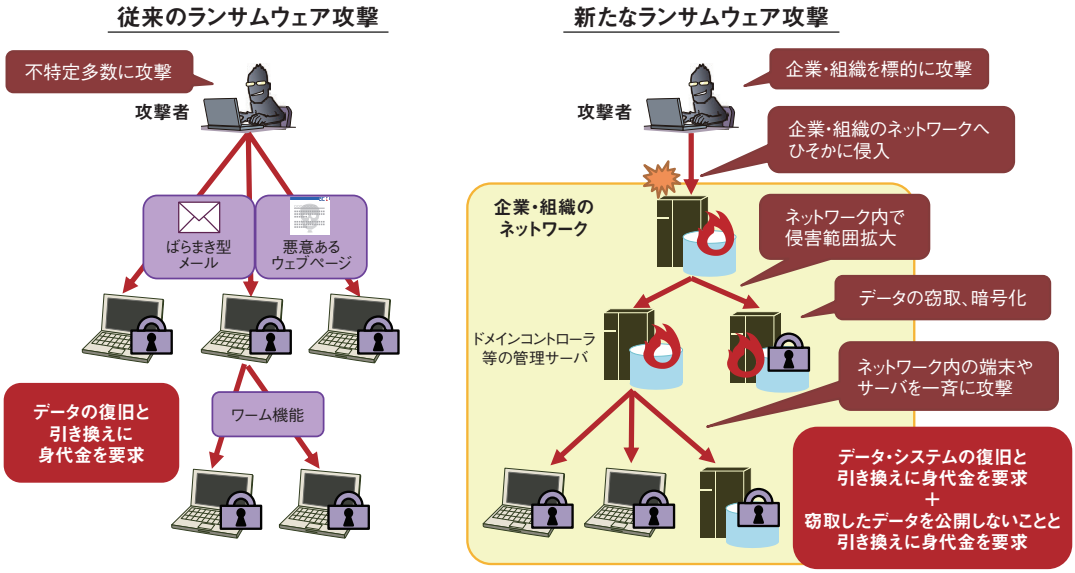
(1) 新たなランサムウェア攻撃の被害事例

2020 年度に公表された 2 件の新たなランサムウェア攻撃の被害事例を紹介する。

(a) 国内のゲーム会社の被害事例

2020 年 11 月 4 日、株式会社カプコンは、不正アクセスによるシステム障害について公表した[※53]。メールシステムやファイルサーバ等にアクセスしづらい障害が発生したとのことである。次いで、2020 年 11 月 16 日、不正アクセスによる情報流出についても公表した[※54]。11 月 16 日時点で、同社はこの攻撃により、元従業員の個人情報 5 件、現従業員の個人情報 4 件、計 9 件の個人情報が流出し、また顧客や取引先等の個人情報が最大で約 35 万件流出した可能性があるとした。そして、2021 年 1 月、更なる調査の結果、社員、退職者、取引先等、関係者合わせて 1 万 6,406 件の個人情報が流出したほか、約 5 万 8,000 人分の個人情報が流出した可能性があると公表した[※55]。

同社は、2021 年 4 月に被害原因や影響範囲等の調査結果について公表した[※56]。それによると、2020 年 10 月に同社の北米現地法人が保有していた予備の旧型 VPN 装置にサイバー攻撃を受け、社内ネットワークに侵入されたという。その後、当該旧型 VPN 装置を経由して米国及び国内拠点の一部の機器に対する乗っ取り行為が行われ、情報が窃取された。更に 2020 年 11 月に米国及び国内拠点の一部の機器がランサムウェアに感染させられ、各機器内のファイルが暗号化された。流出した個人情報について、2021 年 1 月時点では、累計 1 万 6,415 件としていたが、766 人減少し、1 万 5,649 件とのことである。また、同社は公表で、ランサムウェアに感染した機器上に攻撃者からの脅迫メッセージが残されており、攻撃者との交渉に向けたコンタクトを要求された事実を認めている。このときの脅迫メッセージには身代金額は記載されていなかったという。攻撃者と思われる者からの脅迫の詳細な内容について、同社は公表していないが、海外の報道で、脅迫文やリークサイトに関する情報が公開されている[※57]。攻撃者は、脅迫文で、同社のネットワークに侵入したことや、1T バイトものデータを窃取したこと、取引に応じない場合データを公開す



■図 1-2-3　従来の／新たなランサムウェア攻撃の差異
（出典）IPA「事業継続を脅かす新たなランサムウェア攻撃について[※50]」

ること等を主張している。

同社による公表や報道から、本事例は人手によるランサムウェア攻撃と二重の脅迫、すなわち新たなランサムウェア攻撃の被害に遭ったものと考えられる。

(b) 国内の建設会社の被害事例

2020 年 10 月、鉄建建設株式会社は、サイバー攻撃による被害について公表した※58。同社が保有するサーバ約 70 台のうち、約 95% が暗号化等の被害に遭ったとのことである。また、社員用パソコン約 3,000 台のうち、約 10% でセキュリティソフトがアンインストールされていたという。更には、専門会社の調査により、被害を受けたサーバのデータの一部が窃取され、リークサイトに公開されていることを確認したという。これらのことから、同社も新たなランサムウェア攻撃の被害に遭ったものと考えられる。

同社は 2020 年 11 月に、被害の原因や被害が拡大した理由についても公表した※59。それによると、同社の社員に届いたメールにウイルスが仕込まれたファイルが添付されており、社員がこれを開封し、ウイルスに感染したという。攻撃者は当該パソコンを含め合計 3 台のパソコンにリモートアクセスを行い、同社が保有する認証サーバへ到達し、管理者権限を奪った。そして、サーバのデータ暗号化、及び社員用パソコンのセキュリティソフトのアンインストールが実行され、被害が全社に拡大したとしている。

本事例は、数百台規模でデータの暗号化やセキュリティソフトのアンインストールが行われたことから、攻撃者が 1 台ずつ操作を行ったとは考えにくく、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やパソコンの不正操作が一斉になされたものと推測される。

(2) 新たなランサムウェア攻撃の傾向

新たなランサムウェア攻撃は、2018※60 ～ 2019 年※61 ごろから観測され始め、2020 年には、複数の日本企業の被害が報道された。今後も日本の企業・組織が標的とされる状況は続くと予想され、対策を講じておくことが重要である。

「1.2.2 (1) 新たなランサムウェア攻撃の被害事例」で紹介した事例やセキュリティベンダ等のレポート※62 から、企業・組織のネットワークへの侵入は、メールの添付ファイルを用いて組織内のパソコンを経由する手口だけでなく、VPN 製品やインターネット上に公開されている Windows のリモートデスクトップサービス（以下、リモートデスクトップサービス）に対して、設定不備や脆弱性を悪用して侵入する攻撃手口が確認されている。メールだけでなく、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。

また、新たなランサムウェア攻撃で使用されたとされる「SNAKE」（別名、EKANS）と呼ばれるランサムウェアは、観測時期によって挙動は異なるが、ある時期に観測された SNAKE は特定の企業のパソコンやサーバのみでデータの暗号化を行うようになっていた※63。具体的には、特定企業の内部ネットワークのみで有効なドメイン名の名前解決を行い、更に名前解決により得られる IP アドレスをチェックした上で、結果が期待どおりの場合のみ、データの暗号化を行っていた。このように、新たなランサムウェア攻撃では、今後も特定の企業への攻撃に特化したランサムウェアが使用される可能性がある。

(3) 攻撃手口

IPA では、公開されている事例等から、新たなランサムウェア攻撃の実行者（以下、攻撃者）の活動を次の五つのステップに分けている※50。

①ネットワークへの侵入
②ネットワーク内の侵害範囲拡大
③データの窃取
④データの暗号化・システム停止
⑤窃取したデータの公開

ここでは、各ステップで用いられると推測される攻撃手口について紹介する。

(a) ネットワークへの侵入

新たな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手口が報告されている※63。

- リモートデスクトップサービスや VPN 製品を経由した侵入
  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、それを狙い、認証を突破し、侵入する。
- VPN 製品の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 製品に残存する脆弱性を悪用して侵入する。例えば次のような脆弱性が悪用されたとの情報がある（VPN 製品の

脆弱性については「1.2.5 (1) VPN 製品の脆弱性を対象とした攻撃」参照)。
  - 認証情報を窃取することが可能な脆弱性（CVE-2018-13379、CVE-2019-11510 等）
  - 遠隔で任意のコードを実行することが可能な脆弱性（CVE-2019-1579、CVE-2019-19781 等）
- 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。

(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拡げる目的で、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、そして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 を標的とした攻撃については「1.2.1 (4) (c) AD サーバを標的とした攻撃」参照)。

(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ものと推測される。

(d) データの暗号化・システム停止

攻撃者は、最終的に、身代金要求の脅迫のため、ランサムウェアを使用して企業・組織のデータを暗号化する。暗号化は、システムだけでなく業務やサービスの停止にもつながる。場合によっては、当該企業・組織の事業継続に関わるデータやシステムが被害に遭う可能性があり、攻撃者も、それを狙っていると考えられる。バックアップデータ等による業務復旧を妨害するため、攻撃者は、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。

また、攻撃者はドメインコントローラに不正にアクセスし、ここからドメインに属するパソコンやサーバのデータを一斉に暗号化させることがある。

(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。方法としては、リークサイトでの公開や、オークション形式での販売が挙げられる。攻撃者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。

(4) 新たなランサムウェア攻撃への対策

新たなランサムウェア攻撃は、標的型攻撃と同様の手口で企業・組織のネットワークへ侵入し、侵害範囲を拡大し、サーバ等をランサムウェアに感染させたり、情報を窃取したりする。このため、従来のランサムウェア攻撃の対策に加え、標的型攻撃と同様の多層的な対策を行う必要がある(「1.2.1 (5) 標的型攻撃への対策」参照)。

新たなランサムウェア攻撃への対策については、IPA の注意喚起「事業継続を脅かす新たなランサムウェア攻撃について※50」を参照いただきたい。また、従来のランサムウェア攻撃への対策や標的型攻撃への対策は、JPCERT/CC や IPA が資料を公開※64しているのでそれらを参照いただきたい。

ここでは、新たなランサムウェア攻撃への対策として、特に重要と考えられる対策について説明する。

(a) 企業・組織のネットワークへの侵入対策

新たな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(attack surface)の最小化
  攻撃対象領域とは、攻撃者が攻撃可能な範囲のことで、例えばインターネット上に公開されているサーバやネットワーク機器等を指す。インターネットからアクセス可能な、あるいは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、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。
- 脆弱性対策
  「1.2.2 (3) (a) ネットワークへの侵入」で紹介したとおり、攻撃者は脆弱性を悪用して、ネットワークへ侵入することがある。そのため、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ち、脆弱性を悪用されないようにする。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。特にネットワーク機器の脆弱性への対応は、業務への影響が大きく、迅速な対応が困難な場合があるが、そのような脆弱性は攻撃者の狙い目となる可能性があり、注意が必要である。
- 拠点間ネットワークのセキュリティ強化
  新たな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。必要に応じ、拠点間のアクセス制御の強化も検討する。
- 攻撃メール対策
  新たなランサムウェア攻撃に限らず、攻撃メール対策も重要である。攻撃メール対策には、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、従業員への社内教育、啓発、訓練による対策等がある（攻撃メール対策については「1.2.1 (5) 標的型攻撃への対策」参照）。

(b) ネットワーク内の侵害範囲拡大への対策

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の被害を受けて初めて、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。

(c) データの暗号化やシステム停止への対策

データの暗号化やシステム停止への対策として、事業継続に重要なデータやシステムのバックアップを行う。ただし、新たな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」を事前に策定しておくことである。この攻撃では、企業・組織のパソコンやサーバ等が一斉に数千、数万台といった規模で暗号化され、バックアップしたデータまでもが暗号化される可能性がある。こうした状況に備え、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。

(d) データの窃取とリークへの対策

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）[※65] 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、重要性やリスクを踏まえて、実施を検討する必要がある。

(e) インシデント対応

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、攻撃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。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※66を公開しているため、参照いただきたい。

新たな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。新たな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な連絡・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※67。

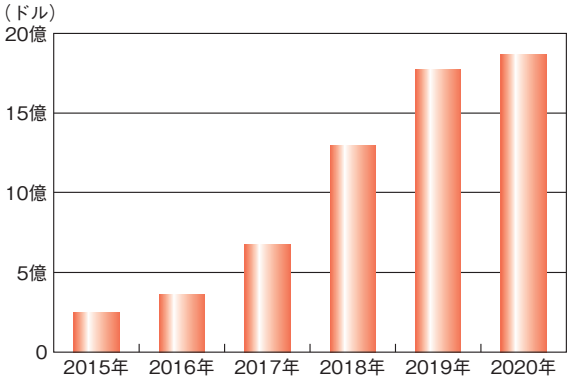
本項では、2020年度に公表されたビジネスメール詐欺の状況、事例を紹介し、その巧妙な手口と対策について解説する。

(1) ビジネスメール詐欺の被害状況

米国連邦捜査局（FBI：Federal Bureau of Investigation）のインターネット犯罪苦情センター（IC3：Internet Crime Complaint Center）の年次報告書※68によると、ビジネスメール詐欺の被害総額は年々増加し続けており、2015年約2億4,600万ドル、2016年約3億6,100万ドル、2017年約6億7,600万ドル、2018年約12億9,800万ドル、2019年約17億7,700万ドル、2020年は約18億6,700万ドルとなっている（図1-2-4）。

2020年4月には、新型コロナウイルスに関連したビジネスメール詐欺の増加を受け、FBIとIC3から注意喚起が行われた※69。

2020年度は世界の法執行機関等から逮捕・起訴事例も多数公表された※70。また、国内でも逮捕事例が公表された※71。ナイジェリアのラゴスで3人の容疑者が逮捕された事例では、INTERPOL（国際刑事警察機構）、セキュリティベンダであるGroup-IB、ナイジェリア警察の1年に及ぶ共同調査により、2017年以降、ウイルス配布、フィッシングキャンペーン、ビジネスメール詐欺を行ってきた犯罪組織が窃取したデータが特定された。このデータ



■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

は、日本を含む150ヵ国以上の政府及び民間企業約50万組織が侵害された結果、少なくとも約5万の組織から窃取されたものだという※72。他には、Microsoft社が司法当局の許可を得て、新型コロナウイルス感染対策に便乗した犯罪集団により世界62ヵ国で犯行に使われていたドメインを制圧したという※73。

米国のセキュリティベンダが2019年に実施した日本を含む7ヵ国を対象とした調査では、世界中の組織の86%がBEC攻撃に直面しているという※74。一方、セキュリティベンダによる国内法人組織を対象とした調査によると、2019年度に回答者の29.1%がビジネスメール詐欺のメールを受信していたという※75。更に、一般社団法人日本損害保険協会が2020年10月に実施した調査では、サイバー攻撃による被害を受けたことがある企業に対して、被害を受けた際の攻撃の種類を尋ねたところ、「不正送金を促すビジネスメール詐欺やフィッシングサイト」が24.4%であった※76。

(2) 2020年度に報道された事例の概要

2020年度に国内外で報道されたビジネスメール詐欺に関する事例について、その概要を表1-2-1（次ページ）に示す。多額の被害に遭った事例が多かったが、迅速な対応により全額回収できた事例もあった。特徴としては、新型コロナウイルスや米国の大統領選挙に関連する事例が見られた。

(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※90と2018年8月※91に続き、2020年4月に第三報※92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※93：Initiative for Cyber Security Information Sharing Partnership

項番	報道時期	概要	被害額
1	2020 年 4 月	英国とイスラエルに拠点を置く大規模な金融機関 3 社が、攻撃者に騙されて 110 万ポンド（約 1 億 6,500 万円）を送金した。57 万ポンド（約 8,600 万円）を回収したが、残りは回収できなかった。この一連の攻撃は「Florentine Banker」と呼ばれるグループの関与が示唆されている※77。	110 万ポンド（約 1 億 6,500 万円）※約 5 割回収
2	2020 年 5 月	カンボジアの小規模金融機関への送金において、送金権限のあるノルウェーの国有投資ファンド Norfund が、同ファンドの従業員をかたったメールにより、1,000 万ドル（約 10 億 6,000 万円）の被害を受けた。攻撃者は発覚を遅らせるため、パンデミックを取り巻く状況によって資金が遅延するという偽のメールをカンボジアの小規模金融機関に送信していた※78。	1,000 万ドル（約10億6,000万円）
3	2020 年 5 月	国内の機械部品製造会社に、ドイツの取引先を装った英文の偽メールが届き、商品代金 150 万円が詐取された。偽メールには「新型コロナウイルスの影響で銀行が機能していない」と書かれており、普段とは違う銀行口座に振り込むよう求めるものだった※79。	150 万円
4	2020 年 7 月	国内の独立行政法人である石油天然ガス・金属鉱物資源機構が、取引先（カナダの資源開発企業）をかたるなりすましメールによって、偽の請求書を受領し、当該請求書に記された指定口座へ誤送金した※80。	不明
5	2020 年 7 月	ニュージーランドの極北地区評議会は、取引先をかたった偽の銀行口座変更要求に従い、不正な銀行口座に 10 万 600.30 ニュージーランドドル（約 800 万円）を支払った。取引先による早期の通知と評議会職員による迅速な対応により、銀行は支払いを取り消すことができ、資金は全額回収された※81。	約 10 万ニュージーランドドル（約 800 万円）※全額回収
6	2020 年 8 月	米国の金融機関 VIRTU Financial Inc. の幹部のメールアカウントが不正アクセスされ、同社経理部門に偽メールが送付された。それを信じた従業員が、2 回にわたり中国の銀行に約 1,080 万ドル（約 11 億 4,500 万円）を送金した。そのうち 380 万ドル（約 4 億 300 万円）の送金は凍結できたが、残りは回収できなかった。同社は、損失を補償しないとする保険会社を訴え、裁判所は保険契約条項を基に、損失を補償すべきという同社の立場を支持した※82。	約 1,080 万ドル（約11億4,500万円）※ 4 割弱凍結
7	2020 年 9 月	イタリアの企業が人工呼吸器や新型コロナウイルス監視装置等の医療機器を中国企業から購入する中で、偽メールに騙され、3 回にわたり計 367 万ユーロ（約 4 億 7,700 万円）をインドネシアの口座に送金した。詐欺はすぐに発見され、各国当局は INTERPOL を介して迅速にコミュニケーションをとり、310 万ユーロ（約 4 億 300 万円）の不正な支払いを凍結し、国際犯罪シンジケートの 3 人のメンバーがインドネシアで逮捕された※83。	367 万ユーロ（約 4 億 7,700 万円）※約 8 割凍結
8	2020 年 10 月	米国大統領の選挙活動を行っていたウィスコンシン州の共和党が、偽の請求書に騙されて選挙資金 230 万ドル（約 2 億 4,400 万円）を失った※84。	230 万ドル（約 2 億 4,400 万円）
9	2020 年 11 月	香港の国際企業の財務責任者は、CFO になりすました攻撃者から 4 通の送金指示メールを受信し、騙されてシンガポールの口座に計 660 万ドル（約 7 億円）を送金した。その後、CFO がそのメールを送信していないことが分かり、詐欺であることが発覚した※85。	660 万ドル（約 7 億円）
10	2020 年 11 月	国内の化学企業である株式会社 JSP は、欧州のグループ会社で悪意の第三者による虚偽の指示に基づく資金流出が起きたと発表した。損失見込額は、2020 年 11 月時点で最大約 10 億円としている※86。	最大 10 億円
11	2020 年 11 月	オーストラリアのヘッジファンド共同創業者が、Zoom オンライン会議への偽招待メールの添付ファイルを開いてウイルスに感染させられ、メールシステムが乗っ取られた。その後、同社ファンド管理者に偽の請求書や承認メールが送られ、管理者は計 870 万豪ドル（約 7 億 4,000 万円）を偽口座に送金した。シンガポールに送られた 500 万豪ドル（約 4 億 2,500 万円）と、香港に送られた 250 万豪ドル（約 2 億 1,300 万円）は回収できたが、残りは回収できなかった。一連の事件を受け、同社の大口顧客が取り引きを中止したため、同社は倒産に追い込まれた※87。	870 万豪ドル（約 7 億 4,000 万円）※ 9 割弱回収
12	2020 年 12 月	米国フィラデルフィアのフードバンク Philabundance Community Kitchen が建設会社を装った偽メールに騙され、92 万 3,533 ドル（約 9,800 万円）の活動資金を失った※88。	92 万 3,533 ドル（約 9,800 万円）
13	2021 年 2 月	米国連邦政府に関する選挙候補者の支援委員会は、2020 年の選挙期間中に、全体で少なくとも 270 万ドル（約 2 億 8,600 万円）のビジネスメール詐欺による被害を受け、当時大統領候補だったバイデン氏の選挙運動でも 7 万 1,000 ドル（約 750 万円）の被害を受けた※89。	270 万ドル以上（約 2 億 8,600 万円以上）

■表 1-2-1　2020 年度に報道されたビジネスメール詐欺に関する事例の概要（報道または公表事例を基に IPA が作成）

of Japan）の運用状況レポートで定期的に事例を公開している※94。

「情報セキュリティ白書 2020※95」の「1.2.2(4)(b)CEO を詐称する一連の攻撃」で紹介した事例については、引き続き多数の情報提供があり、注意喚起の第三報にて「新型コロナウイルス感染症の話題を含めたメールによる攻撃」として紹介している。更に、J-CSIP の運用状況レポート※94 では「複数組織へ行われた CEO を詐称する一連の攻撃（続報）」として紹介している。なお、セキュリティベンダである Agari Data, Inc. が「Cosmic Lynx※96」

と呼ぶ犯罪グループによる攻撃と、この一連の攻撃は同じものと考えられる。また、注意喚起の第三報で「『日本語化』された CEO 詐称の攻撃」として紹介した事例についても、多数の情報提供があり、J-CSIP の運用状況レポートにて「『日本語化』された CEO 詐称の攻撃（続報）」として紹介している。詳細は、各レポートを参照いただきたい。

IPA が情報提供を受けたビジネスメール詐欺の事例のうち、J-CSIP の運用状況として 2020 年度に公開した事例の概要を表 1-2-2 に示す。なお、1 件（項番 2）で金銭的被害が確認されている。金銭的被害のなかった 8 件のうち 1 件（項番 1）は、送金した後に銀行と交渉し、送金の取り消しを行うことができたため、被害を免れている。残り 7 件は、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た。

偽のメールを受信した段階で気付くことも重要だが、送金してしまったとしても、詐欺に気付いた段階ですぐに銀行等に連絡することで、被害を免れる可能性が高まるため、迅速な対応が重要である。

(4) IPA が情報提供を受けた事例

ここでは、IPA が 2020 年度に公開したビジネスメール詐欺の事例の中で、表 1-2-2 の項番 1 について紹介する。

(a) 事例の概要

本事例は、2020 年 1 月、J-CSIP の参加組織（国内企業）の海外グループ企業（A 社：支払側）と、その海外取引先企業（B 社：請求側）との間で取引を行っている中、B 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。

この手口は、IPA が 2017 年 4 月に公開した注意喚起※90 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。

この事例では、偽の口座への送金にまで至ったものの、A 社の担当者が詐欺に気付き、銀行と交渉したところ、送金の取り消しを行うことができたため、金銭的な被害には至らなかった。

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、以下の手口が使われた。

- 請求書の修正を装い偽の口座を連絡する手口

項番	事例概要	被害の有無	備考
1	2020 年 1 月、国内企業の海外グループ企業（支払側）と、海外取引先企業（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が送られた。支払側企業の担当者が送金した後に詐欺に気付き、銀行と交渉したところ、送金の取り消しを行うことができた。	なし	「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2020 年 1 月～3 月］※97」に記載
2	2019 年 10 月、国内企業（支払側）と、海外グループ企業（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［2020 年 4 月～6 月］※98」に記載
3	2020 年 4 月、国内企業（支払側）と、海外取引先企業（請求側）との取り引きにおいて、攻撃者が請求側企業の担当者になりすますビジネスメール詐欺が試みられた。	なし	同上
4	2020 年 4 月、国内企業の CEO になりすました攻撃者により、海外グループ企業の CEO に対してビジネスメール詐欺が試みられた。	なし	同上
5	2020 年 5 月、国内企業の海外グループ企業（請求側）と、海外取引先企業（支払側）との取り引きにおいて、攻撃者が請求側企業の担当者になりすますビジネスメール詐欺が試みられた。	なし	同上
6	2020 年 10 月、国内企業の海外関連会社（支払側）に対して、海外の取引先企業（請求側）になりすました攻撃者により、偽のメールを送り付けるビジネスメール詐欺が試みられた。	なし	「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2020 年 10 月～12 月］※99」に記載
7	2020 年 11 月、国内企業の CEO になりすました攻撃者により、「年末が近づいており、債務者、未解決案件、担当者の詳細なリストがほしいので個人的に連絡を取りたい。」という英文の偽メールが同社従業員に送り付けられた。	なし	同上
8	2020 年 11 月、国内企業の海外関連会社（請求側）になりすました攻撃者により、海外の取引先企業（支払側）へ偽のメールを送り付けるビジネスメール詐欺が試みられた。	なし	同上
9	2020 年 11 月、国内企業の CEO になりすました攻撃者により、同社の社員に対してビジネスメール詐欺が試みられた。	なし	同上

■表 1-2-2　IPA が情報提供を受け 2020 年度に公開したビジネスメール詐欺事例の概要

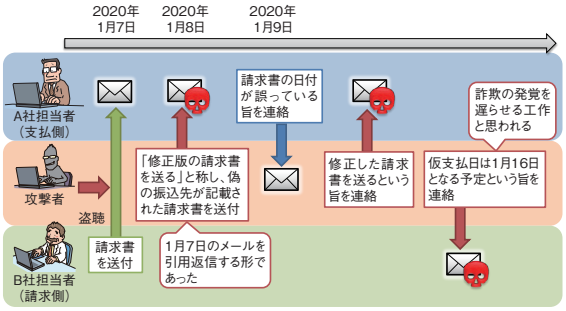
- 詐称用ドメインの取得と悪用

(b) 請求書の修正を装い偽の口座を連絡する手口

2020 年 1 月 7 日、B 社担当者から A 社担当者へ、正規の請求書がメールで送られた。その翌日(1 月 8 日)、B 社担当者になりすました攻撃者から、「修正版の請求書を送る」と称し偽の振込先口座が記載された請求書が A 社担当者へ送り付けられた。このときの攻撃者からのメールは、1 月 7 日に B 社担当者が送ったメールの内容を引用し、返信する形となっていた。攻撃者は、何らかの方法でメールのやり取りを盗み見ていたものと考えられる。

1 月 9 日に A 社担当者は、攻撃者から送られてきたメールを不審とは思わず偽の請求書の内容を確認したところ、偽の請求書の日付が誤っていたため、その旨を攻撃者へ返信した。すると、攻撃者から「入力ミスのため、修正した請求書を送る」という旨のメールが A 社担当者へ着信した。同じ日に、攻撃者は A 社担当者にもなりすまし、B 社の担当者宛に、「仮支払日は 1 月 16 日になる予定である」という旨のメールを送っている。攻撃者は、当面の間、B 社の担当者が A 社側へ連絡を取らないように誘導し、詐欺の発覚を遅らせようとしたものと考えられる。

攻撃に関係したメールのやり取りの前半を図 1-2-5 に示す。



■図 1-2-5　攻撃者とのやり取り(前半／2020 年 1 月 7 日～1 月 9 日まで)
(出典)IPA「サイバー情報共有イニシアティブ(J-CSIP) 運用状況[2020 年 1 月～3 月]」

1 月 13 日に A 社担当者から攻撃者へ、請求書の口座が修正前後で異なっていることを指摘する旨のメールを送ったところ、攻撃者から「修正版の請求書が正しい」という回答があった。その後、A 社担当者は、攻撃者の指定した偽の口座への送金を行った。

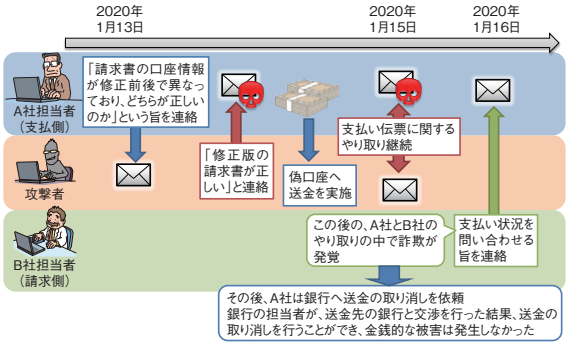
ビジネスメール詐欺では、本件のように、請求書等に記載された口座情報が、攻撃者によって改変されている手口が多く見られる。A 社担当者は、請求書の口座情報が異なっていることに気付いたタイミングで不審に思うことができた可能性はあるが、結果として偽のメールであると気付くことはできなかった。

1 月 15 日に攻撃者から A 社担当者へ、「支払伝票を送付してほしい」というメールが着信したため、複数回のやり取りの後、A 社担当者は攻撃者へ、支払伝票を送付した。

1 月 16 日に本物の B 社担当者から A 社の担当者へ、支払い状況を問い合わせるメールが着信した。本物の B 社からの連絡がこの日となったのは、攻撃者が送った「仮支払日は 1 月 16 日」という偽メールによる時間稼ぎが成功したためと見られる。支払い状況を確認するやり取りの中で、偽のメールが送られていることに気付き、送金先の口座が偽物であるということが発覚した。

その後、A 社は速やかに銀行へ送金の取り消し依頼を実施した。銀行の担当者が、送金先の銀行と交渉を行った結果、送金の取り消しを行うことができたため、金銭的な被害には至らなかった。

攻撃に関係したメールのやり取りの後半を図 1-2-6 に示す。



■図 1-2-6　攻撃者とのやり取り(後半／2020 年 1 月 13 日～16 日まで)
(出典)IPA「サイバー情報共有イニシアティブ(J-CSIP) 運用状況[2020 年 1 月～3 月]」

(c) 詐称用ドメインの取得と悪用

攻撃者は A 社と B 社の正規のドメインに似通った「詐称用ドメイン」を新規に取得して、メールの送信に使用していた。詐称用ドメインは、図 1-2-7、図 1-2-8(次ページ)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。

(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が、「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

【本物のメールアドレス】alice @ subdomain . a-company . com
【偽物のメールアドレス】alice @ subdomain - a-company . com
（「.」を「-」に1文字変更）

※実際に悪用されたものとは異なる。

■図 1-2-7　A 社の詐称用ドメインの例（B 社へ送られたメールで使われたドメインの例）

【本物のメールアドレス】alice @ b-company . com
【偽物のメールアドレス】alice @ b-compeny . com
（「a」を「e」に1文字変更）

※実際に悪用されたものとは異なる。

■図 1-2-8　B 社の詐称用ドメインの例（A 社へ送られたメールで使われたドメインの例）

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。攻撃者は多様な手口を組み合わせて巧妙に攻撃を仕掛けてくる場合があり、注意が必要である。

(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 やマクニカネットワークス株式会社、PwC の報告書等も、対策・対応について記載されているため、そちらも参照いただきたい[※100]。

(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。また、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）や経理部門等金銭を取り扱う部門の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。

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、取引先に被害が及ぶことがあり、取引先と情報を共有することにより、サプライチェーン全体でビジネスメール詐欺への耐性を高めることができる。自組織を詐称したビジネスメール詐欺を確認した場合や自組織が被害に巻き込まれた場合等に、取引先や、警察、金融機関へ報告し、同様な攻撃を受ける可能性のある企業一般に向けても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も有効である[※101]。

(c) 送金処理のチェック体制強化

ビジネスメール詐欺による被害防止のためには、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、企業との取り引きにおいて別の国の口座への突然の変更依頼、見積価格の修正、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ように、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の攻撃者は、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ことがある。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、従業員は、フリーメールや自組織と紛らわしいドメインか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、取引先の中小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、真正な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、メールを返信する際は、返信先のメールアドレスが

正しいかどうか、落ち着いて確認することが有効である。攻撃者が、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があるため、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も有効である。

(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では、攻撃者は攻撃に至る前に、何らかの方法でメール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・不正アクセス対策が必要である。

特に、Microsoft 365 や Google Workspace（旧称、G Suite）のようなクラウド型サービスを利用している場合は、多要素認証等の利用により、第三者による不正ログインを防ぐことが重要である※102。

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が公開※103 されているため、そちらも参照いただきたい。

1.2.4 DDoS攻撃

DDoS（Distributed Denial of Service）攻撃とは、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、ネットワークやシステムリソースを消費させサービス遅延や停止を引き起こす攻撃である。結果として、正当なユーザによるサービスの利用が阻害される。

(1) DDoS 攻撃の動向

セキュリティベンダによれば、自社の DDoS 攻撃対策サービスで検知及びブロックした DDoS 攻撃数は 2020 年第 1 四半期から急増し、第 2 四半期には前年同期比で 3 倍にまで増加した。このような急激な増加は、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いう※104。

2020 年第 3 四半期の攻撃数は、前年同期比では 1.5 倍であるものの直前の第 2 四半期と比較すると大幅な減少に転じた。これは、企業のテレワーク等のシステム環境が適切に整備されるようになったことと、仮想通貨（暗号資産）の高騰により、ボットネットが DDoS 攻撃ではなく仮想通貨のマイニングに振り分けられるようになったことが原因として考えられる※105。

攻撃対象としては引き続き、ISP（Internet Service Provider）事業者、Web サービス事業者を始め、企業、金融機関、教育機関、自治体等であり、それらの組織への大規模 DDoS 攻撃が観測されている。ここでは、2020 年度における、DDoS 攻撃の手口と主だった事例を紹介する。

(a) リフレクション攻撃

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）※106 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※107。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、任意のホストへ反射（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。

セキュリティベンダのレポート※108 によれば、2020 年第 2 四半期に DDoS 攻撃において利用されたプロトコルの 1 位が Portmap であり、SNMP（Simple Network Management Protocol）、SSDP（Simple Service Discovery Protocol）が続いた。これらはいずれも UDP を通信に用いるプロトコルである。また、DDoS 攻撃の半数以上が、これら複数の UDP サービスを悪用した攻撃を組み合わせたマルチベクトル型の攻撃であると見られている。

UDP サービスを悪用した攻撃は、新しい手法ではな

いが、テレワークやIoTの普及等により、ウイルスに感染した機器が増加したことに伴い、悪用されるUDPサービスの傾向に変化が見られる。セキュリティベンダの調査によると、他国と比較して、日本ではSSDPリフレクション攻撃に悪用され得る端末の割合が高いという※109。SSDPはネットワーク上の機器を自動的に発見し接続するUPnP（Universal Plug and Play）に用いられる、UDPサービスの一種である。

(b) DDoS攻撃の規模拡大の事例

Amazon Web Services, Inc.は、2020年2月に、CLDAP（Connection-less Lightweight Directory Access Protocol）リフレクション攻撃によると見られる、2.3Tbps（テラビット／秒）という過去最大規模のDDoS攻撃を観測した。この攻撃は、過去に自社で観測した最大のVolumetric攻撃（ネットワーク帯域を圧迫する攻撃）よりも、規模が約44%拡大した攻撃であった※110。

また、アカマイ・テクノロジーズ合同会社は、2020年6月21日に、自社プラットフォームにおける観測史上最大の8億900万パケット／秒を記録したDDoS攻撃を観測している※111。欧州の大手銀行を標的としたこの攻撃では、同社がこれまで観測した最大規模の2倍のパケット／秒が記録された。日本国内を含む広範囲にわたる攻撃元のIPアドレスは、初めて観測されたものが96.2%を占めており、新しいボットネットによる攻撃と考えられるという。

(c) 仮想通貨を要求するDDoS攻撃の事例

2020年8月以降、日本国内の金融、旅行、小売等の業者に対し、指定期間以内に仮想通貨を支払わなければ、DDoS攻撃を行う旨の脅迫状をメールで送り付ける身代金要求型のDDoS攻撃が観測されている。このような攻撃は、「ランサムDDoS攻撃」とも呼ばれる。脅迫状の送付が確認されたことを受け、2020年10月、JPCERT/CCから注意喚起※112が行われている。

関連する事例として、ニュージーランド証券取引所において、2020年8月25日から28日までの4日間に「ランサムDDoS攻撃」の影響で取引停止に追い込まれるインシデントが発生したと報じられている。ニュージーランド政府は国益・国際的な評価に脅威を及ぼすとして危機管理計画を発動し、対応に当たった※113。この身代金要求型の大規模なDDoS攻撃は、国外より複数回にわたって執拗に行われており、複数のUDPサービスを併用したマルチベクトル型の攻撃の手口が使われたと見られている※114。

攻撃者の要求に応じ仮想通貨を支払ったとしても、攻撃が行われない保証はなく、身代金を支払う企業や組織として特定されるばかりか、攻撃者に活動資金を提供することになる。味を占めた攻撃者が同様の手口を繰り返したり、他の攻撃者が真似をして攻撃が増加したりする可能性もあるため要求に応じてはならない。

JPCERT/CCが公開している注意喚起においても、攻撃者の要求には応じず、攻撃が行われる前提で、対応体制の確認や被害を緩和させる対策を行うことが呼びかけられている。

(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、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、制御を奪われた一般の機器である。

ボットネットは、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。

2020年4月には、IoT機器を悪用してDDoS攻撃を仕掛ける「Dark Nexus」と呼ばれるボットネットが新たに観測された※115。Dark Nexusは、資格情報の窃取や不正なソフトウェアのインストール等の特徴について、Mirai※116のボットネットと類似性があり、ルータ、ビデオレコーダ、サーマルカメラ等の複数の機器に対して、流失したユーザアカウント情報を悪用したパスワードリスト攻撃（Credential Stuffing攻撃）を仕掛け、ボットネットを形成する。

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コンピュータ、ネットワーク機器、IoT 機器等が乗っ取られ、DDoS 攻撃に加担することを防ぐための対策も求められる。以下では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。
- 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 事業者との連携や警察等への通報を実施する。
- 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。

(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。

- OS やファームウェアを最新の状態に保ち、ウイルス感染や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を設定する。
  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。
- 外部と接続され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つながっていない機器においても対策を行う。
- 組織内で稼働しているサービスを洗い出し、DDoS 攻撃に悪用される可能性があるサービスが適切に運用されていることを確認する。
  具体的には、これらのサービスが稼働するサーバに関して、OS を始め、各サービス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

2020 年度は、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 Windows 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。

2020 年度は、新型コロナウイルス感染拡大防止のためテレワークが強く推奨された影響から、VPN の利用に注目が集まった。その一方で、VPN 製品に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。

本項では、VPN 製品の脆弱性を悪用した攻撃事例とその脆弱性について紹介する。

(a) 攻撃事例

2019 年 5 月に、Fortinet, Inc. 製 FortiOS の SSL VPN 機能において、パス・トラバーサル※117 の脆弱性

(CVE-2018-13379※118)が発見された。

この脆弱性は、SSL VPN 機能の Web ポータルに存在する。攻撃者は、細工したリクエストを Web ポータルに送信することで、認証を必要とせずに、FortiOS システム上の任意のファイルにアクセスできる可能性があった。

2020 年 11 月 19 日以降、当該脆弱性を利用したと思われる攻撃により、VPN 製品のホストに関する情報が Web サイト等で公開された。公開された情報には、ホストの IP アドレスに加え、SSL VPN 接続を利用するユーザアカウント名や平文のパスワードが含まれていた※119。当該ホストへの攻撃が試みられた可能性がある。

また、2019 年に 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したバージョンのソフトウェア配布を開始した※120。解消された脆弱性のうち、悪用による被害が確認された CVE-2019-11510 及び CVE-2019-11539 の概要※121 は以下のとおりである。

- CVE-2019-11510 の脆弱性
  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、細工した URI(Uniform Resource Identifier)と、パス・トラバーサルを狙った文字列を組み合わせたリクエストを送信され、当該製品上の任意のファイルにアクセスされる可能性がある。また、ユーザの認証情報を不正に取得され、正当なユーザになりすましてログインされる可能性がある。
- CVE-2019-11539 の脆弱性
  この脆弱性を悪用されると、当該製品において認証に成功した攻撃者により、Web GUI を介して、当該製品上で任意のコマンドが実行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プログラムが配布されたのは 2019 年だが、1 年が経過した 2020 年度においても、当該脆弱性を悪用した攻撃の被害が報告されている。

これは、ソフトウェアのバージョンアップをまだ実施していない利用者が存在する※122 ことと、バージョンアップしたとしても、バージョンアップ以前に脆弱性を悪用され、認証情報を窃取されていた場合、攻撃者が盗んだ認証情報により不正アクセスできてしまうことが原因であるという。

(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くことで、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

また、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に実施する対応を定めておくことを推奨する。

(2) Microsoft 製品の脆弱性を対象とした攻撃

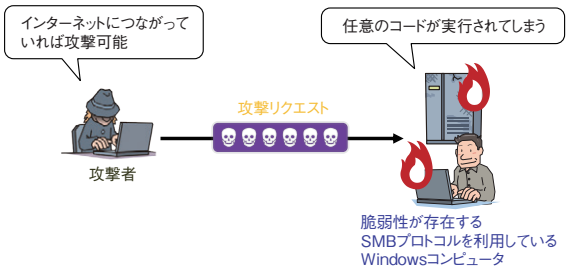
2020 年度も 2019 年度に引き続き、Microsoft 製品の脆弱性を狙った攻撃が多数報告されている。本項では、Microsoft SMB (Microsoft Server Message Block)の脆弱性を狙った事例を紹介する。

(a) 攻撃事例

Microsoft SMB とは、ファイル共有やプリンタ共有等に用いられる通信プロトコルの総称であり、Microsoft SMBv3(以下、SMBv3)はそのバージョン 3 である。

ここでは、2020 年 3 月に公開された「SMBGhost」と呼ばれる脆弱性 CVE-2020-0796※123 と、6 月に公開された「SMBleed」と呼ばれる脆弱性 CVE-2020-1206※124 を悪用した攻撃について解説する。

- SMBGhost の脆弱性
  この脆弱性は、SMBv3 プロトコル通信の処理中に、通信の圧縮データが適切に処理されないことに起因する。攻撃者は、Windows コンピュータの SMBv3 プロトコル通信を受け付ける 445 番ポートが開放されているかを確認し、標的となる SMB サーバに細工したリクエストを送信する。脆弱性が存在すると、リクエストのデータが圧縮される場合の処理が適切に行われないため、バッファオーバーフローが発生し、リクエストに含まれた任意のコードが実行される(次ページ図 1-2-9)。なお、この脆弱性を悪用されるのは SMB サーバだけでなく、SMB クライアントも、攻撃者が構成した悪意のある SMB サーバに接続する場合、任意のコードを



■図 1-2-9　SMBGhost の脆弱性を悪用した攻撃イメージ

実行される可能性がある。

- SMBleed の脆弱性
  SMBleed の脆弱性も、SMBGhost の脆弱性と同様に、通信の圧縮データが適切に処理されないことに起因する。当該脆弱性により、攻撃者が標的となる SMB サーバに対し、細工したリクエストを送信することで、そのサーバのカーネルメモリをリモートから読み取ることができるとされている。

(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」を参照)。

(3) IoT 製品を対象とした攻撃

2020 年度も IoT製品を狙った攻撃が多数報告されている。本項では、2020 年における IoT 製品の主だった脆弱性を紹介する。

(a) 多数の IoT 製品に影響する脆弱性

2020 年 6 月 16 日、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、「Ripple20」と呼ばれるゼロデイ※125 の脆弱性群に関する情報が公開された※126。

Ripple20 は、米国の Treck Inc. 製の組み込み機器用通信ソフトウェアに発見された 19 個の脆弱性の総称であり、これらの脆弱性が悪用された場合、攻撃者により、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のあるすべての IoT 製品の乗っ取りや、情報窃取、製品の誤作動等の被害を一斉に引き起こされる可能性があるという。

当該ソフトウェアは、組み込みシステムにおいて、TCP/IP プロトコルによるネットワーク接続機能を実装するためのライブラリであり、ルータやプリンタ等で広く利用されていることから、数億個以上もの IoT 製品が影響を受ける可能性があるという。

今後、Ripple20 の脆弱性を有したままの IoT 製品を狙ったウイルスが登場する可能性があり、対策が必要である (Ripple20 の詳細については「3.2.2 (1) Ripple20」参照)。

(b) IoT 製品を対象とした攻撃への対策

前述の Ripple20 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※127」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が多く観測されるようになった※128。ばらまき型メールには様々なバリエーションがあり、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」を装ったメール等が存在する。また、ばらまき型メールでウイルスに感染させる手口として、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やマクロ付きの Word、Excel、PowerPoint ファイル、そしてこれらのファイルを圧縮した形式のファイル等が確認されている。

IPA では、2019 年度に観測されていた、添付ファイルやメール本文中の URL を介して、マクロ付き Word ファイルを攻撃対象者（メール受信者）の端末に送り込み、「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 2020 年 7 月に再度観測した。また 2020 年 10 月には、Emotet のばらまき型メールと同様の手口で、マクロ付きの Office ファイルを攻撃対象者の端末へ送り込み、「Zloader」や「IcedID」と呼ばれるウイルスへの感染を狙うばらまき型メールを観測した。このほか、遠隔操作ウイルスへの感染を狙うばらまき型メールも継続的に観測された。

本項では 2020 年度に日本国内で観測されたばらまき型メールについて解説する。なお、ここで解説するばらまき型メールは日本語で書かれており、明確に日本国内を狙った攻撃活動だといえる。

(1) ばらまき型メールによって感染するウイルス

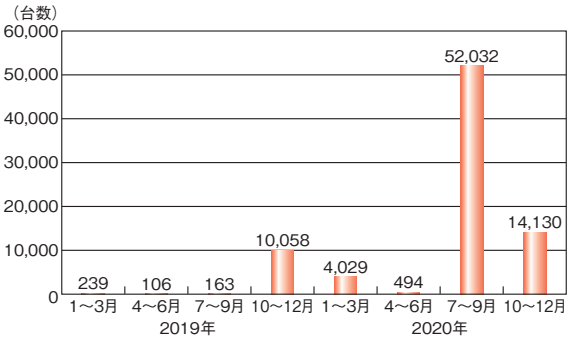
ばらまき型メールによって感染するウイルスは様々なものが存在し、個々のウイルスによって動作は異なる。2020 年度に観測された、ばらまき型メールによって感染するウイルスの一部について述べる。

(a) Emotet

Emotet は感染した端末の情報窃取や他のウイルスへの感染のために使用されるウイルスである。セキュリティベンダによると、Emotet は 2014 年ごろから存在が確認されており、もともとはインターネットバンキングの情報を窃取するウイルスとして、主に海外で確認されていた※129。2019 年末には、日本への Emotet のばらまき型メールによる攻撃が多数の国内組織、企業等を含むメール利用者へ行われるようになった。その後、一時的に活動を休止していたが、2020 年 7 月以降、数ヵ月にわたり国内への攻撃が激化し※130, 131、被害が多数発生した。図 1-2-10 に国内での Emotet の検出台数の推移を示す。

Emotet は次の機能を持ち得るとされている※132。

- ネットワークを経由した別の端末への感染
- メールアドレス情報の窃取
- Outlook のアドレス帳の窃取
- Outlook のメールデータの窃取
- Web ブラウザに保存されたアカウント資格情報の窃取
- Emotet のばらまき型メールの送信



■図 1-2-10　国内における Emotet 検出台数推移
（出典）トレンドマイクロ社「サイバー犯罪の根本解決：EUROPOL による EMOTET テイクダウン※133」を基に IPA が編集

なお、Emotet については 2021 年 1 月 27 日、Europol を中心とした複数国の法執行機関の連携により、その攻撃基盤の停止や一部犯人を逮捕したとの発表があった※134。1 月 27 日以降は攻撃基盤の停止により、ばらまき型メールの送信やウイルスのダウンロード等は確認されていない。更に、4 月 25 日には、法執行機関により、感染端末からの Emotet のアンインストールが行われた※135。ただし、Emotet がアンインストールされたとしても、Emotet は他のウイルスへ感染させる機能があるため、その機能によって感染した別のウイルスの除去が必要である。

日本においても総務省、警察庁、一般社団法人 ICT-ISAC、及び ISP 各社が連携して、国内の Emotet に感染しているパソコンの利用者に対して、2 月下旬から注意喚起を行うとの発表があった※136。

(b) IcedID

IcedID は感染した端末のインターネットバンキングの

情報窃取に使用されるウイルスである。2020 年 10 月と 11 月に IcedID への感染を狙ったばらまき型メール（以下、IcedID のばらまき型メール）が確認されている※137。IcedID は次の機能を持つとされている※138。

- インターネットバンキングの情報窃取
- ファイルのダウンロード及び実行
- メールソフトのアカウント情報窃取
- Web ブラウザに保存されたアカウント情報の窃取
- 感染した端末の情報の収集

また、IcedID のばらまき型メールの攻撃者は 2019 年に確認された Ursnif への感染を狙ったばらまき型メールの攻撃者と同一の可能性がある※137。

(c) Zloader

Zloader は前述の「(b) IcedID」と同様に、感染した端末のインターネットバンキングの情報窃取に使用されるウイルスである※139。これまで Zloader は Emotet の持つ別のウイルスに感染させる機能や Web ブラウザの脆弱性によって、感染することが確認されていた。しかし、2020 年 10 月に、Zloader へ直接感染させるばらまき型メールが確認された※140。Zloader は次の機能を持ち得るとされている※141。

- インターネットバンキングの情報窃取
- スクリーンショットの窃取
- Web ブラウザに保存された Cookie やパスワードの窃取
- Web ブラウザ上のキー入力の窃取

(d) 遠隔操作ウイルス（RAT）

感染した端末の遠隔操作を可能にするウイルスへの感染を狙うばらまき型メールを、IPA では 2020 年 10 ～ 12 月期に観測した※99。遠隔操作ウイルスに感染すると、感染した端末を足掛かりとして組織内ネットワークへ侵入され、被害が拡大する恐れがある。不特定多数にばらまかれるメールだとしても、標的型攻撃同様の深刻な被害を受ける可能性があるため注意が必要である。

(2) ばらまき型メールの偽装の手口

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。

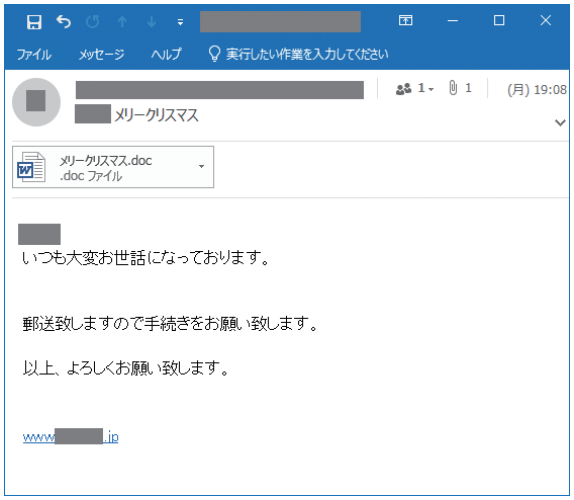
(a) 正規のメールへの返信、転送、及び再送を装う手口

IPA では、Emotet のばらまき型メールや IcedID のばらまき型メールにおいて、正規のメールへの返信、転送、及び再送を装うメール（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。

このような手口のばらまき型メールは 2018 年 11 月から観測されている※142。Emotet のばらまき型メールでは、Emotet に感染した端末から窃取した情報を基に、Emotet に感染した端末で構成される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ことが確認されている※143。一方 IcedID のばらまき型メールでは、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ったり、既に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ばらまき型メールを確認している。

(b) メール受信者の興味・関心を惹く題材を悪用する手口

2019 年 12 月には賞与を題材とした Emotet のばらまき型メールを、2020 年 1 月には新型コロナウイルスを題材とした Emotet のばらまき型メールを観測していた。その後、図 1-2-11 のように 2020 年 12 月にはクリスマスや賞与の支給を題材にした Emotet のばらまき型メールを観測した※130。また、2021 年 1 月には緊急事態宣言を題材にした Emotet のばらまき型メールを観測している。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

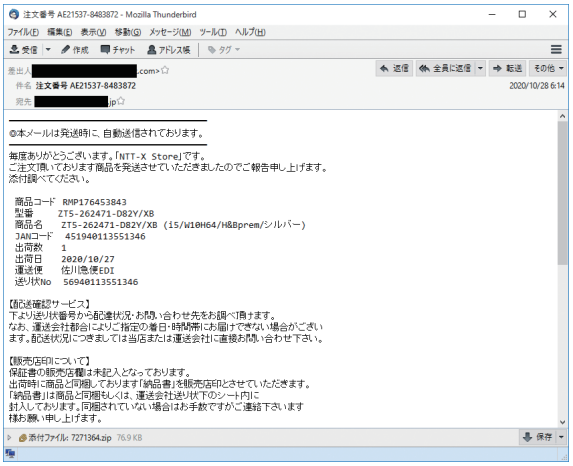


■図 1-2-11 「メリークリスマス」という Emotet のばらまき型メールの例（2020 年 12 月）
（出典）IPA「『Emotet』と呼ばれるウイルスへの感染を狙うメールについて※130」

いるといえる。

(c) 実在の組織をかたった手口

Emotet、Zloader、遠隔操作ウイルスへの感染を狙ったばらまき型メールにおいて、実在する組織をかたるメールを観測している※99, 144。この手口では、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本文を偽装したメールが送信される。図 1-2-12 のように一部のメールにおいては日本語に不自然な点が少ない。不自然さが少ないばらまき型メールは他にも観測されており、注意が必要である。



■図 1-2-12　日本語に不自然な点が少ない Zloader のばらまき型メールの例

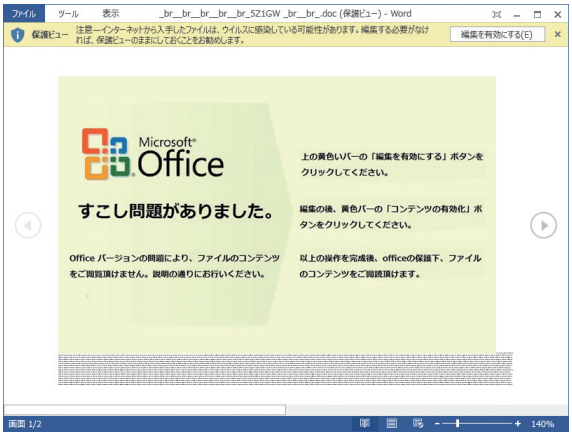
(3) ウイルスに感染させる手口

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。

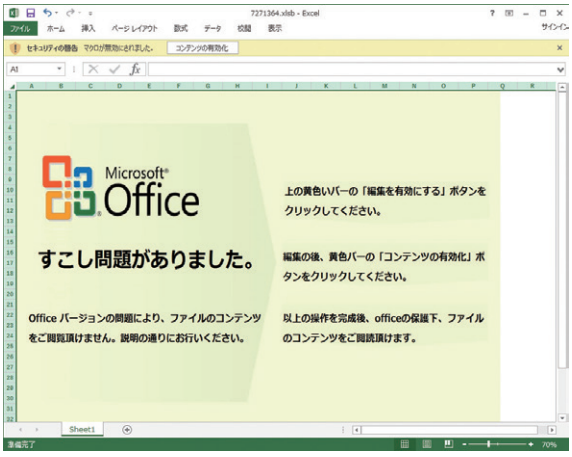
(a) マクロ付きの Office 文書ファイルを使用する手口

この手口では、マクロ付きの Word、Excel、PowerPoint 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をダウンロードし感染させる。マクロ付き Word、Excel ファイルには、Microsoft 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」ボタンと「Enable Content」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で書かれているもののみであったが、IPA では 2020 年 10 月に、図 1-2-13 や図 1-2-14 のように、日本語で指示が記載された Word ファイルや Excel ファイルを観測している。

マクロ付きの PowerPoint ファイルの場合、ファイルを



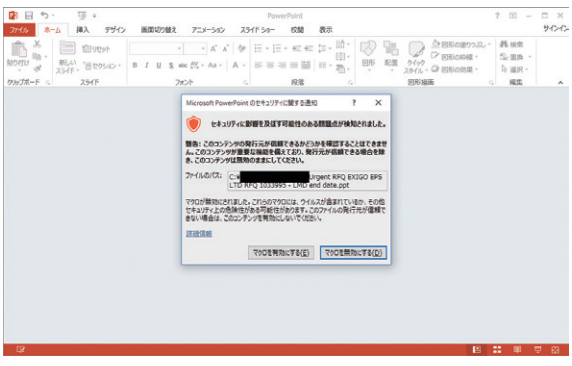
■図 1-2-13　日本語で記載されている Emotet への感染を狙う Word ファイルの例



■図 1-2-14　日本語で記載されている Zloader への感染を狙う Excel ファイルの例

開こうとすると、図 1-2-15 のように、マクロ有効化の許可を求めるポップアップが表示される。ここで許可すると、ウイルスがダウンロードされ、感染させられてしまう。

また、Excel ファイルについては、Excel 4.0 マクロを悪用し、ウイルスに感染させる手口も確認している※145。Excel 4.0 マクロは 1990 年代から存在している機能だが、2020 年に入り、多くの攻撃者がこの機能を悪用す



■図 1-2-15　マクロ有効化を促す PowerPoint ファイルの例

るようになったことが確認されている※146。Excel 4.0 マクロを悪用した手口は、セキュリティソフトによる検知が難しいと言われている※147。

(b) パスワード付きの ZIP ファイルを使用する手口

パスワード付きの ZIP ファイルがメールに添付され、そのパスワードがメール本文に記載されている Emotet のばらまき型メールと IcedID の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させられる。この手口自体は 2019 年 12 月に Ursnif のばらまき型メールで用いられていた。添付ファイルが暗号化されていることから、メール配送上で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。また複数のばらまき型メールでこの手口が使われるようになっている。今後も攻撃者はこの手口を用いる可能性があるため、引き続き注意が必要である。

(c) 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 リンク先が記載され、URL リンクにアクセスすると悪意のあるマクロ付き Office 文書ファイル等をダウンロードさせ、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。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 2020 年度においても継続して用いられており、引き続き注意が必要である。

(4) ばらまき型メールへの対策

ばらまき型メールの攻撃者は、ウイルスに感染させる確率を上げるために様々な工夫を凝らし、新たな手口を取り入れて攻撃をしている。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、メール受信者の自己防衛等の対策を実施し、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信感を抱いた場合は、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を行う。
- 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。
- Word、Excel、PowerPoint ファイルを開いたときにマクロを有効化しない
  正規のものであると確信の持てない Word、Excel、PowerPoint 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「コンテンツの有効化」ボタンをクリックしないようにする。また、Word、Excel、PowerPoint 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。

(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、ウイルス感染を想定した利用者の訓練と教育を行うこと、システムでの対策として、不審なメールを解析するために確保できる仕組みの確立や適切な修正プログラムの適用、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、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

2020年度は、従来のSMS(Short Message Service)やメール、Webからの騙しの手口での被害が継続していることに加え、アプリやSNSを悪用して不審サイトへ誘導する新たな手口が現れ、手口が多様化したことが大きな特徴と考えられる。また、新型コロナウイルス感染の不安に乗じた、偽メールや偽サイトの手口が現れた。

本項では、新たなスパムの手口、新型コロナウイルス感染に関する手口や、従来の手口の変化について事例を基に紹介し、それぞれの手口への対策を説明するとともに、最後に、新たに出現したアプリやSNSを悪用する手口への対策を説明する。

(1) 新たに出現したアプリやSNSへスパムを送り込む手口

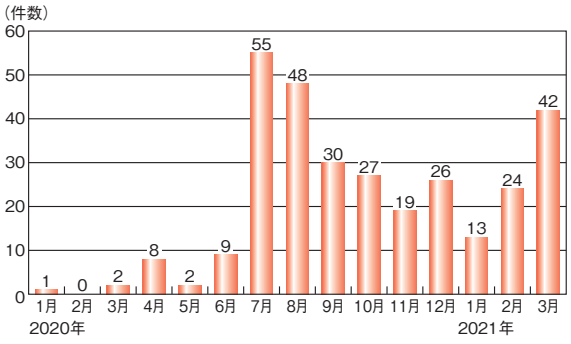
メールやWebだけでなく、アプリやSNSを悪用する新しい騙しの手口が登場した。

(a) iPhoneカレンダースパム

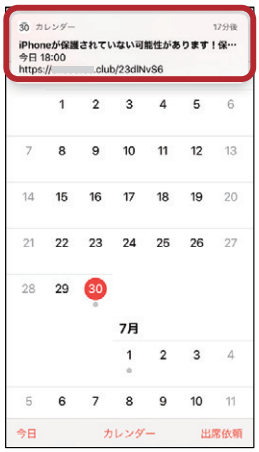
2020年1月から3月にかけて、「iPhoneのカレンダーから、ウイルス感染しているという通知が出る」「iPhoneのカレンダーに、身に覚えのないイベントが入っている」といったiPhoneのカレンダーアプリに関する相談が複数件寄せられたため、IPAは3月に「安心相談窓口だより」で注意喚起を実施した。しかし、この「iPhoneカレンダースパム」に関する相談が7月に急増した(図1-2-16)ことから、8月には注意喚起に新たに観測された手口の説明を追加し、10月には対処方法の更新を行った。また、2021年2月には、手口を検証する動画を追加した[※148]。

(ア) 手口

iPhoneに身に覚えのないカレンダーの通知が表示され(図1-2-17)、カレンダーに「iPhoneが保護されていない可能性があります!」「オンライン保護を確保します」等と記載されたイベントが登録される。イベントの詳細には、URLが記載されている(図1-2-18)。



■図1-2-16 iPhoneカレンダースパムに関する月別相談件数推移



■図1-2-17 iPhone端末にカレンダーが通知された例

■図1-2-18 カレンダーに登録されたイベントとURLの例

iPhoneのカレンダーに身に覚えのないイベントが入ってしまうパターンには、以下の二つがある。

①アカウント追加型:攻撃者の仕掛けたワナにはまる

②イベント・カレンダー共有型:攻撃者から一方的に送り付けられる

①のアカウント追加型では、Webサイト閲覧中に「カレンダーの照会を追加」や「このページを"カレンダー"で開きますか?」とポップアップが表示され、「OK」等をタップしてしまう(次ページ図1-2-19)ことで、自分のiPhone端末のカレンダーに外部のカレンダーが入り込む。アダルトコン

テンツのサイトから誘導されることが多いが、それ以外を扱うサイトから誘導されることもある。

■図 1-2-19　iPhone 端末のカレンダーに外部のカレンダーが入り込む例

②のイベント・カレンダー共有型では、カレンダーアプリの「共有機能」や「出席依頼機能」を悪用し、自分の Apple ID や、iCloud のメールアドレスを攻撃者のカレンダーアプリに共有先として設定されると、不審なイベントやカレンダーが自分の iPhone に登録される可能性がある（図 1-2-20）。

■図 1-2-20　不審なイベントやカレンダーが自分の iPhone に登録される例

①または②の方法で、自分の iPhone に外部のイベントやカレンダーが入ってしまった場合、イベント詳細に記載された URL をタップしてしまうと、不審なサイトに誘導される。誘導されたサイトでは、アプリのダウンロードページへ更に誘導されたり、入力した個人情報を詐取されたりする可能性がある。アプリをダウンロードしてインストールさせる手口については「1.2.7 (4) (b) アプリ誘導」で説明する。

(イ) 対処

対処は、カレンダーがどのように入ったかによって異なる。

①アカウント追加型への対処

アダルトサイト等の不審サイトに表示される画面を操作してしまうことで、自分の iPhone 端末のカレンダーに外部のカレンダーが入り込んでしまった場合は、「設定アプリ」から削除する。削除の方法は iOS のバージョンによって異なる。iOS 14 の場合の削除方法（2021 年 5 月 27 日 現在）を図 1-2-21 に示す。

■図 1-2-21　カレンダーの削除方法（iOS 14 の場合）

②イベント・カレンダー共有型への対処

- 身に覚えのない共有カレンダーの参加依頼がきた場合は、「削除してスパムを報告」の操作を行う（図 1-2-22）。
- 身に覚えのない共有カレンダーがある場合は、「カレンダーを削除」の操作を行う（図 1-2-23）。
- 身に覚えのないイベントの参加依頼がきた場合は、

■図 1-2-22　カレンダーのスパム報告手順

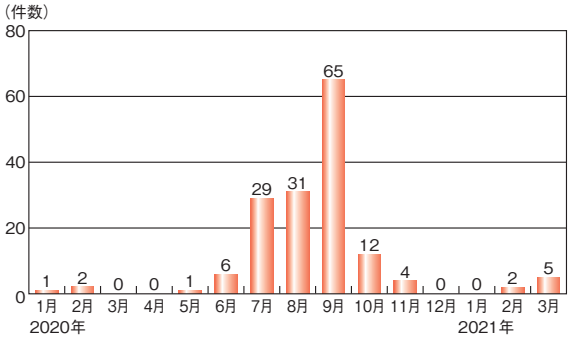
■図 1-2-23　共有カレンダーの削除手順

■図 1-2-24　共有イベントのスパム報告手順

「削除してスパムを報告」の操作を行う（図 1-2-24）。

(b) Facebook メッセンジャースパム

2020 年 1 月以降「Facebook のメッセンジャーで友達から動画が送られてきた」という相談が寄せられ、7 月には 29 件と急増（図 1-2-25）したことから、8 月に IPA は「安心相談窓口だより」で注意喚起した※149。



■図 1-2-25　Facebook メッセンジャースパムに関する月別相談件数推移

(ア) 手口

Facebook のメッセンジャーに、友達から「このビデオはいつでしたか?」等と書いてある動画を装ったメッセージが届く（図 1-2-26）。

これは単に URL が送られてきただけで、動画を再生しようとメッセージをタップしても再生されず、Facebook の ID とパスワードを入力させる偽サイトに誘導される（図 1-2-27）。

■図 1-2-26　動画を装ったスパムメッセージの例

偽サイトには「動画を見るには Facebook アカウント情報を確認する必要がある」というような内容が記載されている。偽サイトに自分の Facebook の ID とパスワードを入力すると、攻撃者にその情報が伝わり、Facebook へ不正ログインされる等の被害につながる。

Facebook へ不正ログインされると、Facebook アカウントに登録している友達に同じメッセージが送られ、被害が拡大していく。送信元が Facebook アカウントに登録している友達であったため、そのメッセージを信頼してタップしてしまったという相談者が多い。

■図 1-2-27　メッセージから誘導される「Facebook の偽サイト」画面の例

偽ページに Facebook の ID とパスワードを入力してログインボタンをタップすると、画面が切り替わり、更に不審なサイトに誘導される。「VPN アプリのインストール誘導」または「セキュリティ警告」のようなポップアップ画面や Web ページが表示され、アプリのダウンロードページへ誘導される（次ページ図 1-2-28）。

なお、アプリのインストールへの誘導は、Facebook メッセンジャースパムの手口に限定されるものではなく、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にも使われている（詳細は「1.2.7 (4) (b) アプリ誘導」参照）。

Facebook の偽サイトにログインした後の誘導先が、不審なアンケートサイトである場合もある。これも Facebook メッセンジャースパム固有の誘導先ということではなく、Web サイト閲覧中に偽サイトへ誘導する手口でも使用されているものである。

なお、Facebook の ID とパスワードを入力させる偽サ

■図 1-2-28　表示された「ポップアップ画面」と誘導された「VPN アプリ画面」

イトに誘導されなかったという相談もあり、詳細については、不明な点がある。

(イ) 対処

動画を装ったメッセージが送られてきた場合、不審なメッセージをタップしてはいけない。可能であれば、そのメッセージを送ってきた友達に、不審なメッセージが送られてきたことを伝える。

Facebook のアカウントとパスワードを入力してしまった場合は、Facebook アカウントのパスワードを変更する。また Facebook の二段階認証の設定を行う。

偽のセキュリティ警告等から誘導され、アプリをインストールしてしまった場合は、「1.2.7 (4) (b) アプリ誘導」で説明する対処を行う。

不審なアンケートサイト等でクレジットカード情報等を入力した場合は、速やかにクレジットカード会社に連絡し、対処について相談する。

(c) 公式アカウントを装った SNS の偽アカウント

2020 年 12 月から、SNS に関連した騙しの手口として、インスタグラムの公式アカウントを装った偽のアカウントによる手口の相談が寄せられるようになった。2021 年 1 月の月次報告書によると、フィッシング対策協議会でも、SNS の偽アカウントによる被害の報告を受けているという※150。

(ア) 手口

相談事例では、本物と同じ写真がインスタグラムの偽アカウントにあり、そこに記載されていた URL にアクセスしたところ、音楽サイトの契約画面に誘導された。別の事例では、偽アカウントを本物と間違えてメッセージを送ったところ、「当選したので Click」と返信がきてタップしたところ、画面が変わり、クレジットカード情報、Apple ID 等を入力してしまった。解約期間の表示があり、何らかのサービス契約をしてしまったと考えられる。

トレンドマイクロ社から 2021 年 1 月に同様な事例が報告され、注意喚起が行われている※151。法人の公式アカウントのなりすましも多く報告されており、なりすまされた法人から注意喚起が行われている※152、※153。

(イ) 対処

公式アカウントかどうかは、各 SNS サービスが認証することで付けられる認証マークを確認するか、公式サイトでアカウント名を確認する。なお、偽アカウントは、本物のアカウント名にピリオド「.」やアンダーバー「_」等が挿入されたものであることが多いため注意が必要である。

SNS のアカウントからメッセージが届いても、URL や表示をタップしない。クレジットカード情報等を入力して、サービス契約をしてしまった場合は、解約の手続きを行い、速やかにクレジットカード会社に連絡し、対処について相談する。

(2) 世の中の関心に乗じるメールの手口

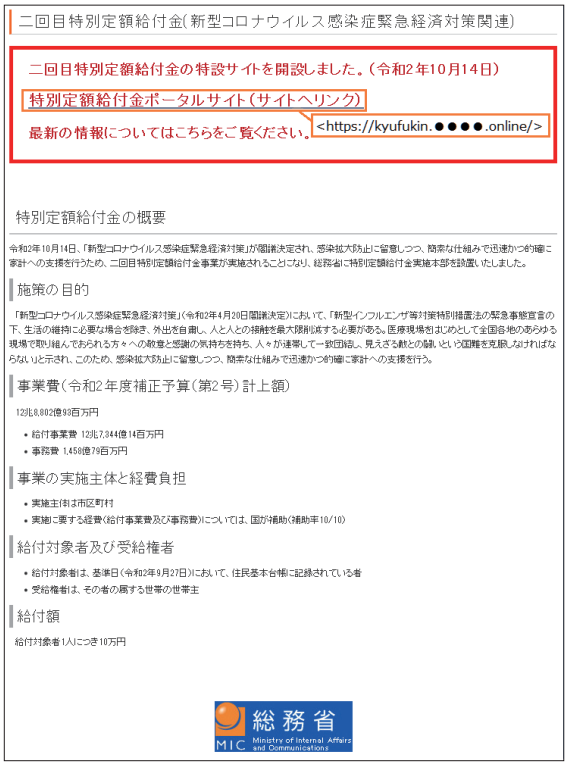
新型コロナウイルスの感染拡大に伴い、経済や社会に様々な影響が出ているが、新型コロナウイルスに関連した話題が、メールや SMS、偽サイトによるカード情報等の窃取へ誘導する騙しの手口に使われた。

(ア) 手口

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。特別定額給付金が 5 月より支給されたため、支給前の 4 月ごろから、特別定額給付金の手続きをかたるメールが送信されるようになった。10 月には、2 回目の特別定額給付金をかたったメールが送られたことが、フィッシング対策協議会から報告されている（次ページ図 1-2-29）。メール内のリンクをクリックすると、総務省の特別定額給付金のオンライン申請を装ったフィッシングサイトに誘導される。

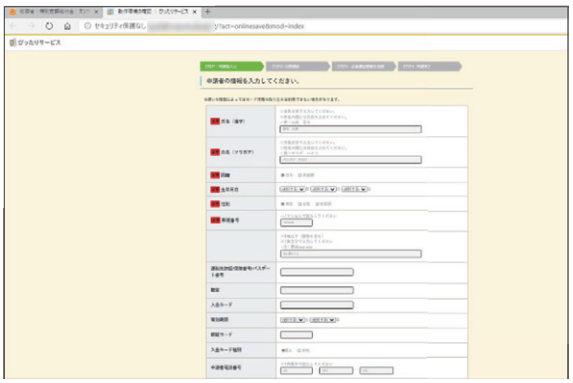
IPA では 10 月に特別定額給付金の偽サイト（次ページ図 1-2-30）を確認した。同サイトのオンライン申請という箇所をクリックすると、住所、氏名、カード情報等の個人情報を入力する画面に誘導される（次ページ図 1-2-31）。

また 2021 年 2 月以降、新型コロナウイルスのワクチン



■図 1-2-29　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 (2020/10/15)※154」

■図 1-2-30　特別定額給付金の偽サイト



■図 1-2-31　特別定額給付金の偽サイトの申請者情報入力画面

接種報道や政府による接種計画等が発表されたことから、ワクチン接種に関する不審なメールが確認されるようになった。

「新型コロナウイルス予防接種が優先的に打てる」といった内容で、URL も記載された SMS が届いたという内容の相談が、消費生活センター等に寄せられている※155。

(イ)対処

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※156。また、新型コロナワクチン接種に関しては、「行政機関等をかたった " なりすまし " にご注意※157」という注意喚起が関係府省庁の連名で出され、電話・メールで個人情報を求めることはない、と説明している。

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。

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、サイトのリンク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したりする等の対処を行う。

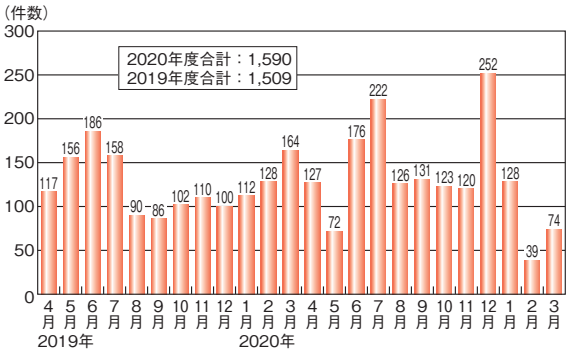
(3) 変化や拡大が続く SMS の手口

個人がインターネットを利用する際の端末は、スマートフォンが 6 割以上※158 となり、パソコンよりも多くなってきている。また、携帯電話の電話番号を宛先にしてメッセージをやり取りする SMS は、認証コード等の連絡手段に使われるため開封率が高いことから、フィッシングの手口が SMS を使ったものに拡大し、変化を続けている。

(a) 宅配便の不在通知を装う SMS

2020 年度も、宅配便の不在通知を装った SMS を用いる手口での被害が続いているが、その手口が一般に認知されつつあることから、手口の変化が見られる。

2020 年度、IPA の安心相談窓口には、前年度を上



■図 1-2-32　宅配便の不在通知を装うSMSに関する月別相談件数推移（2019 ～ 2020 年度）

回る 1,590 件の相談が寄せられた（図 1-2-32）。

本件に関する相談は、2017 年から確認されているが、手口が変化しながら被害が継続しているため、2020 年 6 月には、IPA が「安心相談窓口だより」で改めて注意喚起を行った※159。2020 年 11 月には、全国の消費生活センター等に相談が寄せられていると、国民生活センターから発表された※160。

2021 年 2 月初旬には、宅配便の不在通知を装う SMS に関する相談が一時的に収まった。しかし、春節（2 月 12 日）の連休後には、SMS のばらまきが復活した。この手口では攻撃の実施に人手が絡むプロセスがあると考えられ、春節の休暇の影響により、一時的に減少していたものと推測される。

ちなみに、2020 年の春節時（1 月 25 日）前後には、相談件数の減少は見られなかった。

(ア) 手口

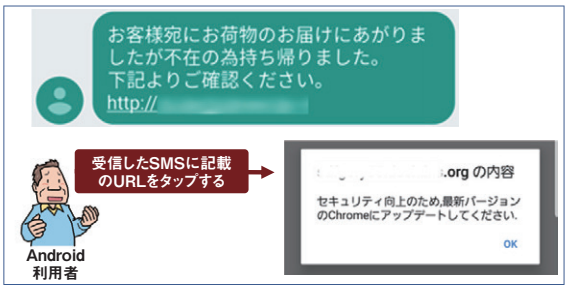
この手口は、「お客様宛にお荷物のお届けにあがりましたが不在の為持ち帰りました。」という宅配便の不在通知を装った SMS を送り付け、SMS 内のリンクから偽サイトへ誘導する。なお、リンクをタップした後の手口は変化を続けており、現時点（2021 年 3 月）の確認内容を説明する。

偽サイトは、2020 年 6 月ごろまでは、佐川急便株式会社、ヤマト運輸株式会社、日本郵便株式会社を装うものであったが、8 月ごろより、宅配便業者の偽サイトに誘導せず、ポップアップが表示される手口が大半となった。ポップアップを使わない手口では、ヤマト運輸株式会社、日本郵便株式会社を装うものになってきている。

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。

① Android の手口詳細

Android の場合、図 1-2-33 のように、ブラウザアプリである Chrome のアップデートをかたったポップアップメッセージが出るケースの相談が多くあった。



■図 1-2-33　Chrome のアップデートをかたるポップアップメッセージの例

「OK」をタップすると、不正アプリの APK ファイル（Android アプリのパッケージファイル）が自動でダウンロードされる。ダウンロードしただけでは被害にはつながらないが、ファイルをタップし、不正なアプリをインストールすると、被害につながる（図 1-2-34）。

不正なアプリをインストールしてしまうと、図 1-2-35 のようにChromeを装うか、AndroidのOSバージョンによっては、Google Play を装ってアプリ一覧に表示される。ヤマト運輸株式会社や、日本郵便株式会社を装った偽サイトでも、従来と同様に不正なアプリをダウンロード

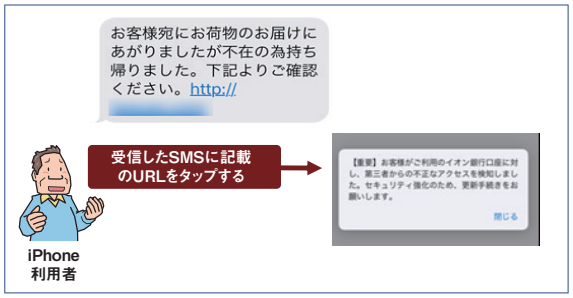
■図 1-2-34　不正なアプリのインストールに至る操作（Andoroid バージョン 10 の場合）

■図 1-2-35　アプリ一覧に表示された偽の Chrome と Google Play の不正アプリ（バージョンが Andoroid 10 の場合）

させるように誘導される。

② iPhone の手口詳細

iPhone の場合は、URL をタップすると、「銀行口座の不正アクセスがあった」というポップアップ表示から、銀行を装った偽サイトに誘導される相談が多くなった（図 1-2-36）。銀行は特定のものではなく、ジャパンネット銀行、au じぶん銀行等、バリエーションが増えている。また、Apple Inc. を装ったフィッシングサイトが表示される場合もある（図 1-2-37）。



■図 1-2-36　iPhone でのフィッシングサイトに誘導するポップアップメッセージの例

■図 1-2-37　Apple ID や銀行口座を入力させるフィッシングサイトの例

（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 における不正アプリの被害として、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 を勝手に送信される。
- 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る。
  - 携帯通信会社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する。
  - 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、不正使用される。
- 不正なアプリをインストールした後、銀行を装った偽のセキュリティ警告のポップアップが表示され、タップするとフィッシングサイトに誘導される。

②iPhone における被害

iPhone におけるフィッシングの被害として、以下が確認されている。

- 「Apple ID とパスワード」を入力した場合、iCloud 等の Apple のサイトに不正ログインされる。
- 偽の銀行のサイトで、口座番号、パスワード等を入力した場合、不正使用される。
- 「電話番号と、キャリア決済の認証コード」を入力した場合、キャリア決済を不正使用される。

（ウ）対処

誘導する手口は変化しているものの、URL をタップした後、不正アプリのインストールや、フィッシングサイトへ誘導するのは変わらない。対処については以前と同様であるため「情報セキュリティ白書 2020」の「1.2.6（1）（a）（イ）対処」「1.2.6（1）（b）（イ）対処」を参照いただきたい。

（b）ネット通販会社を装う SMS

ネット通販会社を装う手口は、メールによるものが多いが、2020 年からは、新たに SMS によるものが確認されるようになった。

Amazon を装う SMS の手口では、「お客様のアカウントは停止されました」「お客さま決済に異常ログインの可能性があります」といった内容の偽の SMS を送り、対処が必要であるとして SMS 内のリンクからフィッシングサイトへ誘導する（次ページ図 1-2-38）。

送信者が「Amazon」と表示された正規の SMS と同じスレッドに偽の SMS が表示されるケースが確認されている※150。

フィッシングサイトで入力を求められる項目は、当該サービスのアカウント情報（ログイン ID・パスワード）、氏名、住所等の個人情報、クレジットカード情報等がある※161。

楽天市場を装う手口では、「商品発送状況はこちらにてご確認ください」と SMS が送られ、偽サイトにアクセス

■図 1-2-38　Amazon を装う SMS の手口

すると、宅配業者を装った手口と同様に、Android の場合は不正アプリがダウンロードされ、iPhone の場合は au じぶん銀行を模したフィッシングサイトへ誘導される※162。

(c) 金融機関を装う SMS

金融機関を装う手口は、メールによるものが多いが、2019 年 9 月に不正送金被害が急増し、メールの手口に加えて SMS が使用されるようになってきた。2020 年も引き続き金融機関を装う SMS が多数確認されている※163。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）からの注意喚起も 2020 年 6 月と 8 月に更新されている※164。

フィッシング対策協議会の報告では、都市銀行のみならず、ゆうちょ銀行、ネット銀行のほか、2020 年度では特に信販会社や地方銀行をかたるケースが増えている※165。

地方銀行をかたった SMS では、高額の不正送金の事案も発生している※166。

金融機関を装う SMS の手口では、「セキュリティ強化のため利用を一時停止した」「口座が不正使用されている可能性がある」といった内容の偽の SMS を送り、対処が必要であるとして SMS 内のリンクからフィッシングサイトへ誘導する。フィッシングサイトに表示される入力項目は、インターネットバンキングのアカウント情報（ログイン ID・パスワード）、銀行口座情報、電話番号等、同一ではなく、各インターネットバンキングの認証システムに合わせて情報を詐取していると考えられる。

(d) SMS の手口の変化、拡大への対策

スマートフォンでのインターネット利用の拡大とともに、通信キャリア回線を使用したスマートフォンの利用を前提とした手軽な本人確認の手段として、SMS によるサービスの認証コードの送付や、通信会社や金融機関からの連絡等、様々なサービスでの SMS の利用が拡大している。

しかし、偽物ではないかという相談の中には、詳細に調べていくと正規の金融機関の SMS の場合もあり、本物かどうか紛らわしくなってきている。

今後も、SMS の文面を変え、かたる対象の事業者・組織の範囲を広げることで、手口の変化、拡大が続くものと考えられる。2020 年には、新型コロナウイルスに関する文面の手口も現れた。世の中の状況の変化に合わせた手口が出現することに注意したい。

通信会社や金融機関は、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。また、SMS での情報通知は行っていないとしている事業者も多い。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。

相談の中では、荷物が到着する予定があったため、偽宅配事業者の SMS の URL をタップしてしまったという話が多く聞かれた。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。

(4) 被害が続く 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。

Web ページの検索結果の一覧からクリックまたはタップした際にも同様な手口に遭遇することがある。

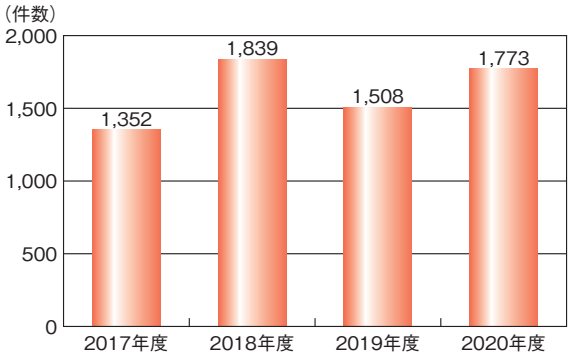
(a) 偽のセキュリティ警告

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 2020 年度も続いている。

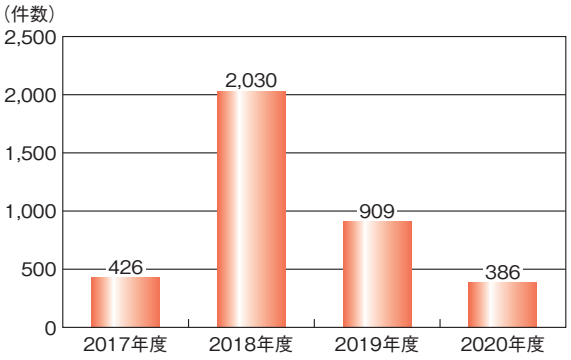
警告画面を出す手口に変化は少ないが、コンビニエンスストアで購入するプリペイドカードで支払わせる手口が増え、コンビニエンスストアの店員が説得して購入を思いとどまらせたというニュースが報道されるようになった。

2020 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 1,773 件（図 1-2-39）、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 386 件だった（図 1-2-40）。



■図 1-2-39　偽警告に関する年度別相談件数



■図 1-2-40　偽セキュリティソフトに関する年度別相談件数

この手口では、警告画面に記載された電話番号に電話をして遠隔操作されることがきっかけとなる。これについて、2020 年 11 月、IPA は「安心相談窓口だより」で改めて注意喚起を行った※167。また、2021 年 2 月に、「消費者の利益を不当に害するおそれがある行為（消費者を欺く行為）を確認した」として、消費者庁より消費者安全法に基づいて注意喚起が行われた※168。

（ア）手口

「偽警告」と「偽セキュリティソフト」の手口は、検索結果の一覧からリンクをクリックしたり、閲覧していた Web サイトから突然画面が切り替わる際に、偽のセキュリティ警告画面（図 1-2-41）が表示されることから始まる。

警告画面は、「ウイルスに感染している」「システムが破損する」等と、根拠のない内容で不安を煽る。パソコンで音を出せる状態にしている場合は、警告音や音声が連続して流れ、更に不安にさせられる。

偽のセキュリティ警告画面が表示された後、「偽警告」の手口では、以下のような流れとなる場合が多い。

①警告画面に記載されている電話番号に電話をかけると、オペレーターから状況を聞かれ、ウイルスに感染している等と言われ、遠隔操作に誘導される（図 1-2-41）。

②修復作業や今後の保守サポートの契約を持ちかけられ、プリペイドカード等での支払いを求められる。2020 年は、クレジットカードではなく、コンビニエンスストアでゲーム等の購入で使用するプリペイドカードでの支払いを要求される相談が増えている。

③支払いに応じると、オペレーターが遠隔操作で「パソコンの対処」と称する作業を行う。その作業の中で、セキュリティソフトであるとして詳細不明のソフトウェアをインストールされることもある。

④費用の支払いを断ると、パソコンにパスワードを設定されてログインできないようにされたり、パソコンのファイルを消されたりといった悪質な事例もある。

Microsoft 社をかたる手口が増えており、注意喚起が行われている※169。IPA に相談があった事例では、本当に Microsoft 社のオペレーターか確認しようとすると、遠隔操作で偽物の ID カードを画面に表示して見せる等、手口が巧妙になっている。

コンビニエンスストアでプリペイドカードを購入させる手口の認知が広がっているため、コンビニエンスストアの店

■図 1-2-41　遠隔操作に誘導する偽セキュリティ警告の手口

員に何に使うのか聞かれた際に怪しまれないための回答方法を説明されたり、遠隔操作されている画面にカードの番号を書き込み伝えると、「プリペイドカードの番号が間違っているのでプリペイドカードの会社が受け付けない。返金するので、新しいカードを購入して来てくれ。」と言って、何度もカードを購入させられ、結果的に高額な支払いをしてしまったといった相談が増えている。

(イ)対処

偽のセキュリティ警告が表示された場合は、落ち着くために、まずパソコンの音量を下げ、警告音や繰り返し流れるナレーションを止める。相談では、音やナレーションに驚いて相手に電話をしてしまった、という相談事例が多かった。

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。しかし、通常の操作で画面を閉じることができない場合もあるので、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ソフト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、パソコンの初期化をすることを推奨する。

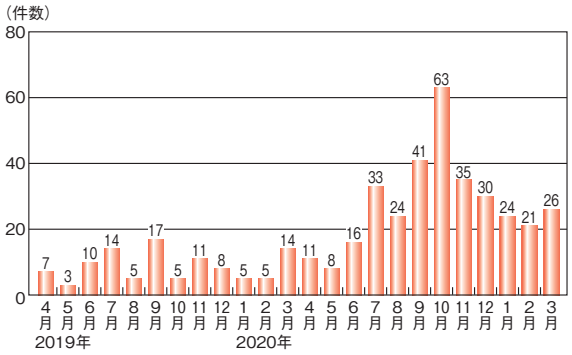
契約については、消費生活センター等※170 に相談し、クレジットカードで支払いを行った場合はクレジットカード会社にも連絡する必要がある。プリペイドカードで支払った場合は返金が困難な場合が多い。

また、Microsoft 社では、当該手口に関する専用ページ※169 で手口や事例を紹介し、被害報告も受け付けているため、活用も検討いただきたい。

(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増えている。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が、「1.2.7 (1) 新たに出現したアプリや SNS へスパムを送り込む手口」で説明した iPhone カレンダースパムや Facebook メッセンジャースパムの手口で誘導される事例も増えている。

2019 年 9 月、IPA は「安心相談窓口だより」で注意を呼びかけ※171、いったん相談件数は減少傾向にあったが、2020 年後半から増加している(図 1-2-42)。



■図 1-2-42　アプリ誘導に関する相談件数

(ア)手口

警告画面に表示された「ハッキングされている可能性があります」等の問題は、「推奨するセキュリティアプリケーションをインストールすると解決できる」とかたり、公式マーケット上のアプリを入手するよう誘導する手口である(図 1-2-43)。

■図 1-2-43　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(iPhone)

この手口の目的は不明だが、従来は「利用者にアプリをインストールさせることによる報酬（PPI：Pay Per Install）」を得ようとするアフィリエイト（成果報酬型広告）ではないかと考えられていた。しかし、2020 年に IPA へ寄せられた相談事例では、「サブスクリプション詐欺」を目的として、自動継続課金※172 の有料アプリに誘導されるケースが増えている。

上記のケースでは、アプリインストール後の初回起動時に自動継続課金の確認メッセージが表示される（次ページ図 1-2-44）が、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。

■図 1-2-44　自動継続課金である旨の確認メッセージの例（iPhone）

（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。iPhone の場合はサブスクリプションの解約（図 1-2-45）、Android の場合は定期購入の解約も実施する。

■図 1-2-45　サブスクリプションの解約手順（iOS14.4 の iPhone の場合）

（5）新たな騙しの手口への対策

2020 年度の相談件数全体では、依然としてメールや SMS、Web を悪用した手口の相談が多くを占めるが、「1.2.7（1）新たに出現したアプリや SNS へスパムを送り込む手口」で説明したように、アプリや SNS を悪用した手口が出現したことが特徴といえる。

今後増加すると考えられる、アプリや SNS を悪用した手口に対しては、以下の二つの対策が必要と考える。

一つ目は、アプリの機能を知ることである。アプリによっては、サービスを他の利用者に広げたり、利用頻度を高めるために、様々な外部連携機能を持つものがある。iPhone カレンダースパムの手口のように、メールサービスやクラウドサービスとの連携、新たなアカウント追加等、外部とつながりを持たせる機能が悪用されることがある。利用するアプリについては、どのような外部連携機能があるか確認し、不要な機能やアプリの権限を制限する等の対策を行う必要がある。また、自分が利用しているアプリを悪用する手口が広がっていないか、日頃から注意することも必要である。

二つ目は、つながる相手への信頼を利用した騙しの手口に注意することである。メールに代わって、SNS が連絡手段として定着しつつあるため、Facebook メッセンジャースパムのような手口で誰かが騙されると、連鎖して多くの知り合いや関係者が攻撃に巻き込まれることになる。不審な内容が届いた場合は、相手に確かめる等、騙された場合の影響を考えた慎重な対応が必要である。

また、次々と新たな SNS が登場してきていることからも、SNS のアカウントを本物のように見せかけて騙す手口は今後も続くものと考えられる。公式アカウントであることを示す認証マークを確認したり、アカウント名のわずかな違いにも注意することで、騙されることのないようにしたい。

なお、新たな騙しの手口が現れても、人間の心理の隙を突いて騙す手口への対策の基本は変わらず、以下の三つである。

- 手口を知り、日頃の備えをする。
- 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、信頼できる相手に相談する。

詳しくは、「情報セキュリティ白書 2020」の「1.2.6（5）騙しの手口に共通の対策」を参照いただきたい。

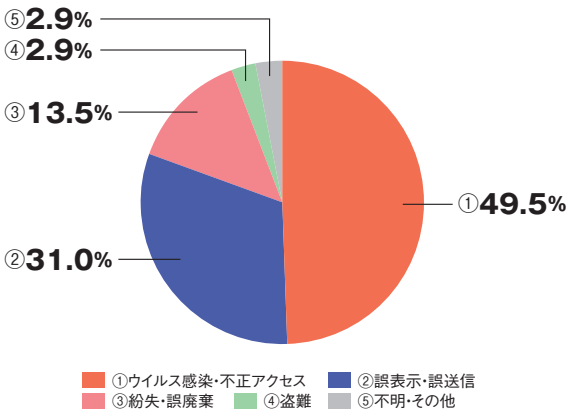
1.2.8　情報漏えいによる被害

2020 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）2020 年の情報漏えいの概況

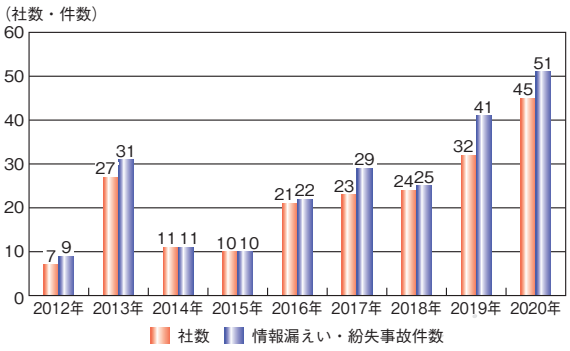
2021 年 1 月に株式会社東京商工リサーチ（以下、東京商工リサーチ社）が公開した「『上場企業の個人情報漏えい・紛失事故』調査（2020 年）[※173]」によると、2020 年に個人情報の漏えい・紛失事故を公表した上場企業は 88 社 103 件（2019 年は 66 社 86 件）、漏えいした個人情報は 2,515 万 47 人分（2019 年は 903 万 1,734 人分）に達した。東京商工リサーチ社が調査を開始した 2012 年以降で最多となった。

2020年の情報漏えい・紛失事故103件のうち、理由として最も多かったのは「ウイルス感染・不正アクセス」の51件(構成比49.5%)、次いで「誤表示・誤送信」が32件(同31.0%)となっている(図1-2-46)。



■図1-2-46 情報漏えい・紛失件数の原因別割合
(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』調査(2020年)」を基にIPAが編集

「ウイルス感染・不正アクセス」の事故は年々増加しており、東京商工リサーチ社の調査では、事故件数、社数ともに2年連続で最多を更新している(図1-2-47)。



■図1-2-47 ウイルス感染・不正アクセスによる事故の発生推移
(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』調査(2020年)」を基にIPAが編集

(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いる。そして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。

任天堂株式会社の事例※174では、何らかの方法により不正入手したログインIDとパスワード情報を用いて、「ニンテンドーネットワークID※175」(以下、NNID)になりすましログインが行われ、NNID経由で一部の「ニンテンドーアカウント」に不正ログインが行われたことを確認した。この不正アクセスにより、NNIDに登録されているニックネーム、生年月日、国/地域、メールアドレス、更にニンテンドーアカウントに登録されている氏名、生年月日、性別、国/地域、メールアドレス、約30万アカウント分の情報が第三者に閲覧された可能性がある。同社はNNIDを経由してニンテンドーアカウントにログインする機能を廃止し、不正ログインされた可能性のあるアカウントに対してパスワードリセットを行うとともに、利用者に対して、パスワードの使い回しを止め、二段階認証を設定するよう呼びかけた。

株式会社カプコンの事例※176では、1万5,649人の個人情報の流出が確認され、流出した可能性のある顧客・取引先等の個人情報は、最大約39万人分と公表した。この事例では新たなランサムウェア攻撃が行われていた。また、侵入経路としては、北米現地法人Capcom U.S.A., Inc.が保有していた予備の旧型VPN装置に対するサイバー攻撃で社内ネットワークへ不正侵入され、米国及び国内拠点の一部の機器が乗っ取られ、情報が窃取されるに至ったことが分かった(「1.2.2(1)(a)国内のゲーム会社の被害事例」参照)。

NTTコム社の事例では、2020年5月28日の第1報では、海外拠点(シンガポール)への攻撃及び侵入をきっかけとして日本のサーバに侵入され、621社の工事情報等が流出した可能性があると公表した※34。7月2日の第2報ではその後の調査により、更に83社の情報流出の可能性があること、及び調査の過程でリモートアクセスを利用したBYOD端末からの不正アクセスがあったことを公表した※35。BYOD端末からの不正アクセスでは、攻撃者により窃取された正当なアカウントとパスワードが利用されており、影響を受けた可能性のある顧客は188社と公表した(「1.2.1(1)国内の標的型攻撃事例」参照)。

三菱重工業株式会社の事例※43では、機微な情報や機密性の高い技術情報、取引先に係る重要な情報の流出はなかったが、従業員等の個人情報(氏名及びメールアドレス)のほか、サーバのログ、通信パケット、サーバ設定情報等のIT関連情報等の流出を確認した。この事例では、在宅勤務時に従業員が社内ネットワークを経由せずに社有パソコンを外部ネットワークへ接続、SNSを利用した際に、ウイルスを含んだファイルをパソコンにダウンロードしたことで感染し、出社の際、このパソコンを社内ネットワークに接続したため、ネットワークを通じ感染が拡大した(「1.2.1(3)(d)SNSを悪用した攻撃」参照)。

その他、外部からの不正アクセスによって情報漏えい

被害が発生した主な事例を表 1-2-3（次ページ）に示す。

(3) 過失やシステム不具合による情報漏えい・情報紛失

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 2020 年 11 月に公表した「（2019 年度）『個人情報の取扱いにおける事故報告集計結果』[※191]」によると、事故の発生原因としては「誤送付」が 59.5% と最も多く、次いで「紛失」が 16.6% となっている（「その他漏えい」を除く）。事故原因として 2018 年度から 2019 年度にかけては誤廃棄が 24 件から 66 件と増加した。

みずほ総合研究所株式会社（現、みずほリサーチ & テクノロジーズ株式会社。以下、みずほ総研）の事例[※192]では、顧客情報（66 万 9,000 件）のほか、みずほ総研が行ってきた講演やセミナーの参加者に関する情報（183 万 8,000 件）、重複を含めると最大で 250 万 7,000 件に上る情報を紛失したと公表した。保管していた記憶媒体の磁気テープを誤って廃棄した可能性が高く、現時点では第三者に情報が流出した疑いはないという。

国土交通省神戸運輸監理部の事例[※193]では、行政文書の一部を誤って廃棄していたことが分かった。自動車の検査・登録に関するもので保管期間満了前に廃棄した 242 万 2,653 件、内閣府の廃棄同意を得る前に廃棄した行政ファイル 371 万 733 件、そのほか公文書の内部管理に関するものが 270 件含まれていた。誤廃棄した文書は、委託業者により溶解処分されており、外部への流出の形跡はないという。

ヤフー株式会社の事例[※194]では、各種サービスで使用する Yahoo! JAPAN ID の登録情報システムに不具合が発生し、一部の利用者の ID 登録情報（氏名・住所・電話番号等）が、他の ID 登録情報（最大約 39 万 ID）に誤って反映されたことが判明したと発表した。これにより、一部の利用者の ID 登録情報が他の ID 保有者に閲覧される可能性、自分の ID 登録情報に他の利用者の ID 登録情報が誤って上書きされる可能性、誤って上書きされた情報を元に他の ID 保有者の注文した商品・サービスが ID を上書きされた利用者に届く可能性、逆に注文した商品やサービスが届かない可能性等が発生した。障害発生時間に ID 登録情報を編集した結果、他の ID 登録情報に誤って反映された可能性がある回数が最大 52 万 8,155 回、誤って上書きされた可能性のある ID が最大 38 万 7,460ID に及んだ。

楽天株式会社、楽天カード株式会社、楽天 Edy 株式会社の事例[※195]では、営業管理に用いていた社外のクラウドサービスの設定に不備があり、2016 年 1 月から 2020 年 11 月の期間、外部よりアクセスが可能となっていたことが、社外のセキュリティ専門家の指摘により判明した。社外の第三者からアクセスの可能性があった情報は、3 社合わせて最大 148 万 7,771 件であり、うち、アクセスが確認された件数は 614 件であった。

設定不備の対象となったのは株式会社セールスフォース・ドットコム（以下、セールスフォース社）のサービスだった。楽天が公表して以降、セールスフォース社のコミュニティ、Salesforce サイト（旧 Force.com サイト）、及び Site.com のサイト上に構築する公開サイト機能を利用する複数の企業（PayPay 株式会社、イオン株式会社、株式会社イオン銀行、独立行政法人国際観光振興機構等[※196]）が設定不備による情報流出を公表した。企業だけでなく、セールスフォース社の製品を利用して株式会社両備システムズが提供している自治体向けシステム（Web 住民けんしん予約、住民生活総合支援アプリ「i-Blend」、緊急通報システム「Net119」）にも設定不備があり、これらを導入している 71 団体のうち 13 団体で不正アクセスが確認された[※197]。問題になったのはセールスフォース社が提供している社外のユーザ（ゲストユーザ）にデータへのアクセスを許可する機能で、ゲストユーザへのアクセス権限をシステム管理者が設定する必要があったが、適切に設定されていなかったため、外部から第三者がアクセスしてしまった。セールスフォース社では、ゲストユーザのセキュリティ設定（アクセス制御の権限設定）の再確認について公開し[※198]、電話によるサポートも行っている。2021 年 1 月、NISC は、重要インフラ事業者等に向けてセールスフォース社の製品の設定不備による意図しない情報が外部から参照される可能性について注意喚起を行った[※199]。

(4) 内部不正による情報漏えい

ソフトバンク株式会社の事例[※200]では、元社員が秘密保持契約を締結していたにもかかわらず、退職申告から退職するまでの期間に、営業秘密に該当するネットワーク技術に関わる情報を不正に持ち出したとして、同社は警視庁へ被害を申告した。楽天モバイル株式会社に転職していた元社員は不正競争防止法違反の容疑で警視庁に逮捕された。

また、ソフトバンク株式会社が 3 月に公表した事例[※201]では、訪問販売やブース販売等の形で代理店業務を行っていた人物が、携帯電話の契約手続きをした顧客

情報公表日	法人・団体名	内　　容
2020 年 4 月 13 日	Classi 株式会社	株式会社ベネッセホールディングスとソフトバンク株式会社の合弁会社である Classi 株式会社が提供する、教育機関向けクラウドサービス「Classi」から最大 122 万件の情報が流出した可能性がある。流出した情報には、Classi を利用するための ID（約 122 万人分）、パスワードが暗号化された文字列（約 122 万人分）、任意記入の教員の公開用自己紹介文（2,031 件）が含まれる※177。
4 月 13 日	ナカバヤシ 株式会社	事務用品や文房具の通信販売サイト「フエルモール」が SQL インジェクション攻撃を受け、ペイメントアプリケーションが改ざんされ、クレジットカード情報を含む顧客情報が流出した可能性がある。流出したクレジットカード情報は 94 名分で、カード名義人名、クレジットカード番号、有効期限、セキュリティコードが含まれる。クレジットカード情報以外に 12 万件の顧客情報が流出した恐れがあり、流出した顧客情報には注文情報、購入者情報（氏名、住所、メールアドレス）、送付先情報（氏名、住所）が含まれる※178。
4 月 19 日	株式会社 リジョブ	過去に利用していたテストサーバから 2015 年 12 月 5 日以前に、求人サイト「リジョブ」に会員登録実績のあるユーザ、最大 20 万 6,991 件の情報が流出した可能性がある。流出した情報には、氏名、住所、生年月日、電話番号、メールアドレス、パスワード等が含まれる※179。
6 月 15 日	株式会社 キタムラ	電子商取引（EC）サイト「カメラのキタムラネットショップ」において、国外からの複数のなりすましによる不正アクセスで顧客情報約 40 万件が流出した可能性がある。流出した顧客情報には、氏名、フリガナ、郵便番号、住所、生年月日、電話番号、性別、メールアドレス、ニックネーム、利用店舗名最大 4 店、注文履歴・保有 T ポイント残高等が含まれる※180。
7 月 24 日	株式会社 キッチハイク	グルメアプリ「キッチハイク」のユーザ情報のバックアップデータを保存していた外部サーバから、最大 11 万 6,863 件のユーザ情報が流出した可能性がある。流出したユーザ情報には、氏名、電話番号、メールアドレス、ハッシュ化されたパスワード等が含まれる※181。
11 月 16 日	QUOINE 株式会社	ドメイン登録サービス「GoDaddy」内のアカウント・ドメイン登録情報が不正に変更され、不正アクセスにより顧客情報が 16 万 9,782 件流出した可能性がある。流出した顧客情報には、口座開設や取引開始の作業時に入力したメールアドレス、氏名、暗号化されたパスワード、API キー等が含まれる※182。
11 月 17 日	Peatix Japan	海外 IP アドレス経由でデータベースに不正アクセスされ、最大 677 万件の顧客情報が流出した可能性がある。流出した情報には、アカウント表示名、氏名、アカウント登録メールアドレス、言語設定、アカウント作成国、タイムゾーン、暗号化されたパスワードの 7 項目が含まれる。参加履歴や決済情報、アンケートデータの流出は確認されていない※183。
11 月 19 日	東建コーポレーション 株式会社	グループ会社のネットワークがサイバー攻撃を受け、グループサイト全般で不正アクセスにより 65 万 5,488 件の情報が流出した可能性がある。流出した情報には、2000 年 9 月から 2020 年 9 月までに対象となったグループ会社のサイトへの問い合わせ、ユーザ登録、各種キャンペーンに応募したユーザのメールアドレス、氏名、住所、電話番号、パスワード、性別、生年月日等が含まれる※184。
12 月 7 日	PayPay 株式会社	加盟店データベースの不備を狙った不正アクセスにより、加盟店等、約 260 万店舗の営業情報及び従業員やパートナー企業に関する情報が最大 2,007 万 6,016 件流出した可能性がある。ユーザ情報、クレジットカード情報は含まれていないが、加盟店の住所、連絡先、代表者氏名、生年月日、金融機関の口座情報等が含まれる※185。
12 月 11 日	株式会社駅レンタカーシステム	駅レンタカーの Web サイトがシステム設計段階に内在していた脆弱性が原因で不正アクセスを受け、顧客メールアドレス 25 万 3,979 件、及び同社と提携関係にあった営業所等のメールアドレスや電話番号が流出した可能性がある※186。
12 月 23 日	株式会社 TIMERS	スマートフォンアプリ「Famm（ファム）」のサーバから、最大 143 万件のユーザのテーブルが流出した可能性がある。テーブルには、ユーザのメールアドレス（最大 53 万 5,015 件）、暗号化されたパスワード（最大 53 万 5,015 件）、氏名（最大 24 万 3,617 件）、アカウント表示名（最大 18 万 5,073 件）、生年月日（最大 23 万 5,970 件）、ユーザが登録したユーザアイコン画像の URL（最大 10 万 2,763 件）等が含まれる※187。
2021 年 2 月 12 日	株式会社 マイナビ	総合転職情報サイト「マイナビ転職」を管理する Web サーバに対し、不正に取得されたと思われるパスワードを使ったなりすましによる不正アクセスがあったことを公表した。2000 年から公表までに「マイナビ転職」へ登録したユーザのうち、21 万 2,816 人分の Web 履歴書（退会者は除く）に不正アクセスされた可能性がある※188。
3 月 5 日	全日本空輸株式会社（ANA：All Nippon Airways） 日本航空株式会社（JAL：Japan Airlines）	航空会社向けにシステムを提供するスイスの国際航空情報推進機構（SITA：Société Internationale de Télécommunications Aéronautiques）が提供する航空会社向け顧客管理システム「SITA Passenger Service System（PSS）」が不正アクセスを受け、加盟各社で共有する顧客情報が流出した可能性がある。日本でも JAL と ANA で被害が発生した。流出したのは、サービス提供にあたり、アライアンスメンバー間で情報を共有するマイレージサービスにおいて上位ステータスにある顧客情報であり、アルファベット表記による氏名、会員番号、会員ステータスが含まれる。流出対象顧客数は ANA 約 100 万人、JAL91 万 9,685 人※189 であるという。
3 月 10 日	株式会社アーバンリサーチ	公式オンラインストアへの不正アクセスにより、UR CLUB 会員情報 31 万 7,326 人分 が流出した可能性がある。流出した会員情報には、住所、氏名、電話番号、メールアドレス、生年月日、性別、会員 ID、会員ステージ等が含まれる※190。

■表 1-2-3　外部からの不正アクセスによる情報漏えいの主な事例（報道または公表事例を基に IPA が作成）

情報を不正に取得し、その情報を悪用して金融口座から不正引き出しを行っていた。不正取得した個人情報は、氏名、住所、生年月日、連絡先電話番号、携帯電話番号、携帯電話機の製造番号（IMEI）、交換機暗証番号、料金支払い用の金融機関名及び口座番号を含む6,347件であり、不正引き出し被害は62件に及んだ。

(5) 不適切な情報の取り扱い

ソースコード共有サービス「GitHub」に、複数の企業のシステムに関するソースコードが無断公開されていた※202。各社の委託先に所属していたSEと見られる人物が、自分が書いたソースコードから年収を診断できるWebサービスを利用するためにGitHubに公開したものであった。各社ともソースコードは公開されたが、顧客情報の流出やこのソースコードを含むシステムのセキュリティに影響はないことを確認している。

LINE株式会社の事例※203では、ユーザの個人情報が業務委託先である中国の関連企業からアクセスできる状態になっていた。中国の拠点では、タイムライン、オープンチャット、ユーザから「通報」されたメッセージ等について、スパム行為やフィッシング等の迷惑行為がないか、未成年との不適切な出会いに関するメッセージがやり取りされていないか等のモニタリング業務を現地企業に委託していた。また、同社決済サービスのLINE Payについては、取引情報、利用者情報を韓国の同社データセンターで保管していた。LINEのプライバシーポリシーでは「パーソナルデータを第三国に移転することがある」と明記していたが、具体的な国名は明記していなかった。「中華人民共和国国家情報法」では、「いかなる組織も公民も、国の情報活動に協力しなければならない」と定めており、業務委託であろうと、中国政府が要請すれば、情報を提供しなければならない。LINE株式会社では、「中国からの完全アクセス遮断、中国での業務終了」「トークデータの完全国内移転」を発表し、中国からのアクセスは2021年3月23日に遮断された。

(6) 対策

情報漏えいの原因ごとに、被害を発生させないための対策を以下に示す。

(a) 不正アクセスへの対策

外部からの攻撃は巧妙化、高度化しているが、堅牢なセキュリティ対策を施されているシステムや業務は攻撃者にとっても手が出しにくい。そこで、直接攻撃するのではなく、周辺の脆弱な環境を見つけ出し、そこを経由して侵入する手口が増えてきている。2020年度も海外拠点を経由したり、対策があまり施されていないシステムの脆弱性が狙われたりした。例えば2020年度はセキュリティ対策が十分でないテレワークやオンライン会議が増えたと思われ、今まで以上に攻撃の対象が増えている。境界防御だけでなく端末、利用者の認証等を強化するゼロトラストの考え方を取り入れ、多要素認証、多段階認証等を導入したり、端末や機器のセキュリティ設定やパッチ更新を正しく行う等、リスクに応じた対策が必要である。

また、実際に不正アクセスの被害を受けた場合は、原因分析に専門的な知識が必要なことも多く、セキュリティ担当者のスキルや、いざというときに頼れるセキュリティベンダ等のパートナーの支援が重要である。

(b) 人為的な過失への対策

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も有効であるが、それだけでなく、重要な情報の取り扱いルールを設け、その運用を徹底する、適宜見直す等で、過失の発生機会をできる限り削減していく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の感染防止、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。

上記の見直しにおいて、様々なクラウドサービスの利用が拡大しているが、クラウドサービスのセキュリティはサービス事業者とサービス利用者がそれぞれの役割・責任を分担し、対策を実施することが求められる。例えばIaaS（Infrastructure as a Service）利用において、ユーザデータの管理・廃棄は利用者の責任であり、SaaS（Software as a Service）利用においても端末におけるアカウント情報の保護はサービス利用者の責任となる等、求められる役割を正しく認識する必要がある。

(c) 内部者の不正への対策

過失への対策と同様、内部不正による情報漏えい被害を完全に防ぐことは難しいが、情報を取り扱う者に対して正しい知識や規則を理解、遵守してもらう取り組みが不可欠である。在宅勤務や客先での作業等の、孤立した環境は、同僚や上司の目が気にならないため、コ

ンプライアンス意識を維持しにくい。また、仕事のためだと都合の良い解釈をして情報を持ち出すことを正当化しやすくしてしまう。今一度、職場での定期的な情報の取り扱いルールの確認、遵守できていることの点検をする必要がある。

(d)不適切な取り扱いへの対策

個人情報や営業秘密の取り扱いについては、法律やガイドライン等により、基本的な考え方や取り扱い方法について規定されている。それらの規定は情報を守るだけでなく、適切に利用するためのものでもある。しかし、実際に情報を取り扱う場面では、様々な状況があるため、規定どおりであるかということだけでなく、想定されるリスクも含めて検討する必要がある。「1.2.8 (5) 不適切な情報の取り扱い」で取り上げた2020年の事例では、具体的な被害は出ていない。しかし、これは現時点では被害がなかったというだけである。

業務委託等で作成したソースコードは、契約等により権利の帰属が定められており、通常は個人ではなく所属する組織、あるいは委託元の組織のものである。また、ソースコードには、機密性の高い情報が含まれることもある。組織は、開発(コーディング)から運用・廃棄までの情報管理についてリスクを把握し、従業員に取り扱い方法を周知し、遵守されていることを確認しなければならない。

また業務やIT環境のクラウド化・グローバル化により、情報の管理を組織の外部、場合によっては海外で行うことが増えている。自組織の統制が及ばないところに重要な情報を置くことのリスクについて、十分な検討が必要である。クラウドのセキュリティについては前述のようにクラウドサービス事業者との責任分担を正しく認識し、実践すること、また委託するクラウドサービス事業者の対策が妥当であることを確認することが重要である(対策の詳細については「情報セキュリティ白書2020」の「3.4 クラウドの情報セキュリティ」参照)。

更に、海外にデータを置く場合は、そこで適用される法制に関するリスクがある。これは、2020年のLINE株式会社の事例で、収集した個人データの中国移転について、現地法制による意図しないアクセスがあり得る、というリスクとして顕在化した。これについては、個人データ収集時点での利用者へのリスクの説明が十分でなかったとされている。今後は、海外のどこにデータを置くとどのようなリスクがあるか、法制面も含めてクラウドサービス事業者・利用者ともに十分検討する必要がある。

また、欧州で個人データを収集してサービスを行う場合はGDPR(General Data Protection Regulation:一般データ保護規則)への準拠が必要である。GDPRに関するリスクについては2018年の施行以来ある程度周知され、国内企業の対応も進んでいると考えられるが、GDPRの運用にもまだ幅があり、注視する必要がある(GDPRの運用については「2.2.3 (3) GDPRの運用状況」参照)。

COLUMN

情報セキュリティ10大脅威 2021
～よもや自組織が被害に!呼吸を合わせて全力防御!～

IPA では毎年、前年に発生したセキュリティ事故や攻撃の状況等から脅威を選出し、専門家等の投票により順位付けした「情報セキュリティ 10 大脅威」を発表しています。2021 年 1 月に公開した「情報セキュリティ 10 大脅威 2021」は、下表のとおりです。

表 情報セキュリティ 10 大脅威 2021「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
スマホ決済の不正利用	1	ランサムウェアによる被害
フィッシングによる個人情報等の詐取	2	標的型攻撃による機密情報の窃取
ネット上の誹謗・中傷・デマ	3	テレワーク等のニューノーマルな働き方を狙った攻撃
メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	4	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	5	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	6	内部不正による情報漏えい
インターネット上のサービスからの個人情報の窃取	7	予期せぬ IT 基盤の障害に伴う業務停止
偽警告によるインターネット詐欺	8	インターネット上のサービスへの不正ログイン
不正アプリによるスマートフォン利用者への被害	9	不注意による情報漏えい等の被害
インターネット上のサービスへの不正ログイン	10	脆弱性対策情報の公開に伴う悪用増加

「個人」向け脅威では「スマホ決済の不正利用」が 2 年連続で 1 位となりました。スマホ決済サービスを悪用して他人の銀行口座から残高をチャージ（他人の口座からの金銭窃取）する事案等が引き続き発生しています。また、「ネット上の誹謗・中傷・デマ」が昨年の 7 位から 3 位に上昇しました。

「組織」向け脅威では「ランサムウェアによる被害」が昨年の 5 位から 1 位に上昇しました。また、「テレワーク等のニューノーマルな働き方を狙った攻撃」が初登場で 3 位になりました。被害例や対策については、本白書の 1 章、3 章でも紹介しています。

「情報セキュリティ 10 大脅威 2021」解説書や、社内教育や研修に使える「情報セキュリティ 10 大脅威 2021」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。

https://www.ipa.go.jp/security/vuln/10threats2021.html

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※127」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、2020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

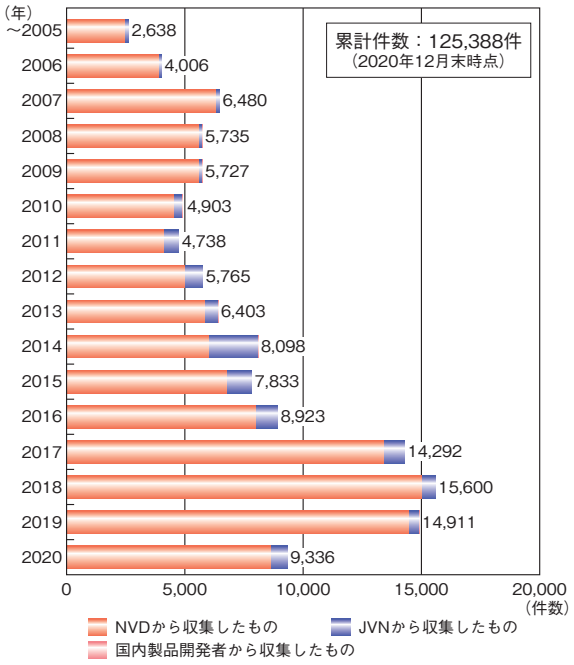
JVN iPediaは、国内外で利用されているソフトウェア製品の脆弱性対策情報を、以下の三つの公開情報から収集・蓄積しており、2007年4月25日から公開している。

- 脆弱性対策情報ポータルサイトJVN※204で公表された脆弱性対策情報
- 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※205」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※206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いる。なお、2020年の登録件数は12月末時点で9,336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、2020年の登録数も最終的には2019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増加した理由としては、脆弱性を登録するための共通識別子であるCVE（Common Vulnerabilities and Exposures）※207の採番機関（CNA：CVE Numbering Authority）※208が増加したことが一因として挙げられる。The MITRE Corporation※209によると、2016年12月に47社※210だったCNAは、2020年12月には149社※211と約3倍になっている。この増加したCNAによって、多くの脆弱性にCVEが付与され、NVDに公開される脆弱性の件数増加につながった可能性がある。

一方、JVNから収集した脆弱性情報は、極端に登録数の多かった2014年の2,085件※212を境に年々減少していたが、2020年は前年の453件より200件以上増加し、689件となっている。また、国内製品開発者から公表された脆弱性対策情報は、毎年数十件の登録であるが、2020年は19件であった。



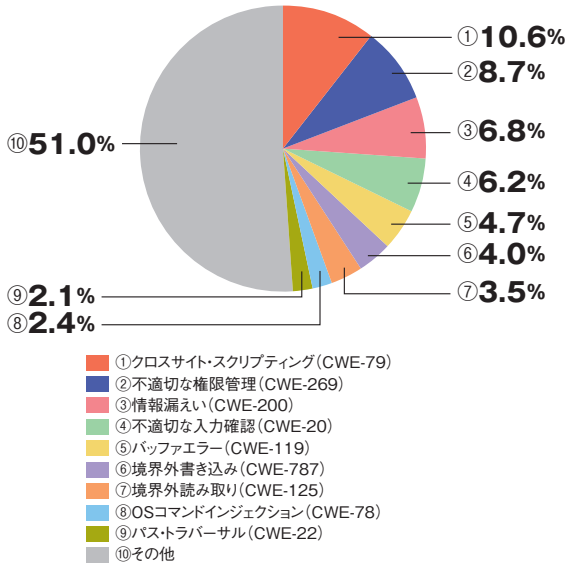
■図1-3-1 JVN iPedia登録状況（公表年別）
（出典）JVN iPediaの登録情報を基にIPAが作成

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）※213を脆弱性対策情報に付与して登録を行っている。2020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10.6%と最も高く、「不適切な権限管理」が8.7%、「情報漏えい」が6.8%、「不適切な入力確認」が6.2%と続いている（次ページ図1-3-2）。

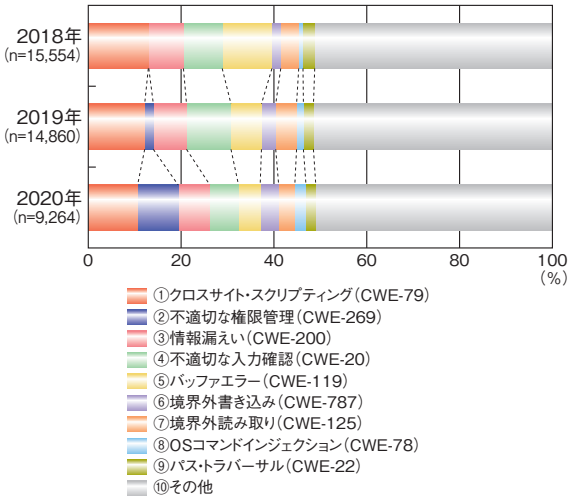
最も件数の多かった「クロスサイト・スクリプティング」に分類される脆弱性を悪用されると、偽のWebページが表示されたり、情報が漏えいしたりする恐れがある。

2018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」「バッファエラー」の割合は 2019 年以降減少傾向にあり、「不適切な入力確認」の割合も 2020 年に減少している。一方で、「不適切な権限管理」の割合のみ増加傾向である（図 1-3-3）。



■図 1-3-2　JVN iPedia における脆弱性対策情報の CWE 別割合（2020 年、n=9,264）
（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（2018 ～ 2020 年）
（出典）JVN iPedia の登録情報を基に IPA が作成

(b) JVN iPedia の登録情報の深刻度

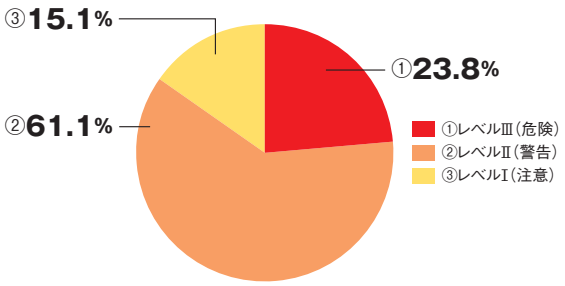
JVN iPedia は、オープンで汎用的な脆弱性評価手法である CVSS（Common Vulnerability Scoring System：共通脆弱性評価システム）※214 を用いて、脆弱性の深刻度を公開している。なお、JVN iPedia では CVSS v2 及び CVSS v3 の二つのバージョンの情報を公開しているが、本項では CVSS v2 を基に統計処理を行っている。

深刻度には、CVSS v2 の基本評価基準（BM：Base Metrics）の数値を基に評価したレベル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）BM 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）BM 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）BM 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。

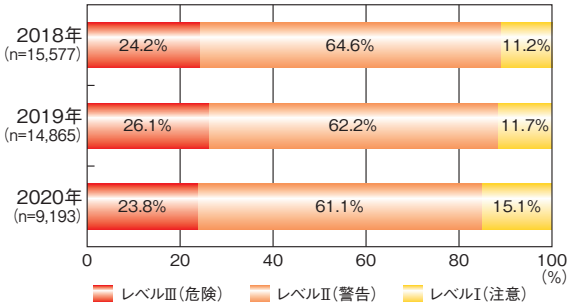
2020 年に登録された脆弱性対策情報を深刻度のレベルで分類すると、レベルⅢが 23.8%、レベルⅡが 61.1%、レベルⅠが 15.1% となっており、一部の情報漏えいやサービス停止につながるレベルⅡ以上の脆弱性が全体の 8 割以上を占めている（図 1-3-4）。



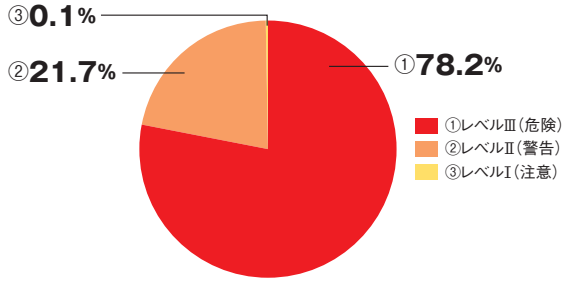
■図 1-3-4　JVN iPedia における脆弱性対策情報のレベル割合（2020 年、n=9,193）
（出典）JVN iPedia の登録情報を基に IPA が作成

2018 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 2018 年が 88.8%、2019 年が 88.3% であったが、2020 年は 84.9% と若干減少した。2020 年を 2019 年と比較すると、最もレベルが低いレベルⅠに該当する脆弱性の割合が 3.4% 増加し、レベルⅡ以上の脆弱性の割合はその分減少している（次ページ図 1-3-5）。これは、レベルⅠとして評価される脆弱性の登録件数が前年と同程度だったのに対し、レベルⅡやレベルⅢに評価される「クロスサイト・スクリプティング」や「バッファエラー」等の登録件数が 2020 年に減少したことが一因と考えられる。

製品開発者は、ソフトウェアの企画・設計・製造段階



■図 1-3-5　JVN iPedia における脆弱性対策情報のレベル割合（2018 ～ 2020 年）
（出典）JVN iPedia の登録情報を基に IPA が作成



■図 1-3-6　JVN iPedia に登録された Microsoft Server の脆弱性対策情報のレベル割合（2020 年、n=747）
（出典）JVN iPedia の登録情報を基に IPA が作成

からセキュアコーディング※215 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 Server 製品の脆弱性について

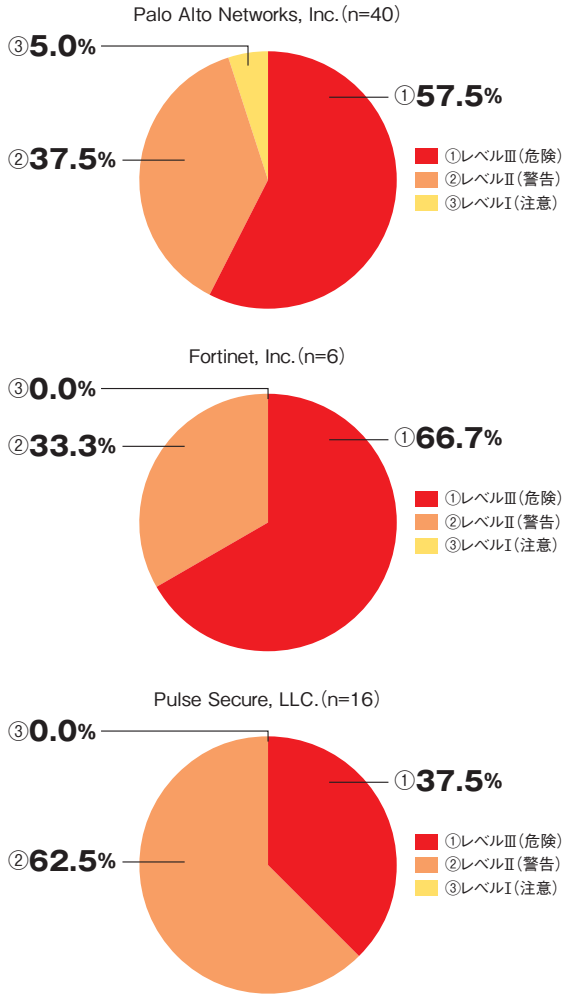
「Zerologon」と呼ばれる脆弱性（CVE-2020-1472）は、Windows Server 製品のドメインコントローラ機能で使われる Netlogon リモートプロトコル（MS-NRPC）に発見された特権昇格の脆弱性である。本脆弱性を悪用され、攻撃者にドメインの管理者権限を奪われてしまうと、組織の重要な機密情報が窃取されたり、ドメインに参加しているパソコンが攻撃者に乗っ取られたりする等の被害につながる恐れがある。本脆弱性は、2020 年 8 月に Microsoft 社から脆弱性対策情報※216 が提供された際、CVSS v3 基本値の深刻度が最も高い 10.0 と評価されており、その後、Microsoft 社から本脆弱性を悪用する攻撃を確認したとの情報も公開※217 されたため、利用者は早急に対応を行う必要があった。

また、2020 年は Zerologon 以外にも Microsoft Server 製品の脆弱性が多数公開された。図 1-3-6 は、2020 年の 1 年間に JVN iPedia へ登録された Microsoft Server 製品に関する脆弱性対策情報の深刻度のレベル別割合である。登録された脆弱性のうち、深刻度が最も高いレベルⅢに分類された脆弱性が 78.2%、その次に高いレベルⅡが 21.7% となっており、ほぼすべての脆弱性がレベルⅡ以上の深刻度に分類されている。2021 年以降も同様の傾向で脆弱性が公開される可能性がある。製品利用者は最新の修正プログラムが Microsoft 社から公開されているか日頃から確認し、脆弱性対策情報が公開された場合には、速やかに対策を実施することが求められる。なお、Microsoft 製品を狙った攻撃事例については「1.2.5 (2) Microsoft 製品の脆弱性を対象とした攻撃」を参照されたい。

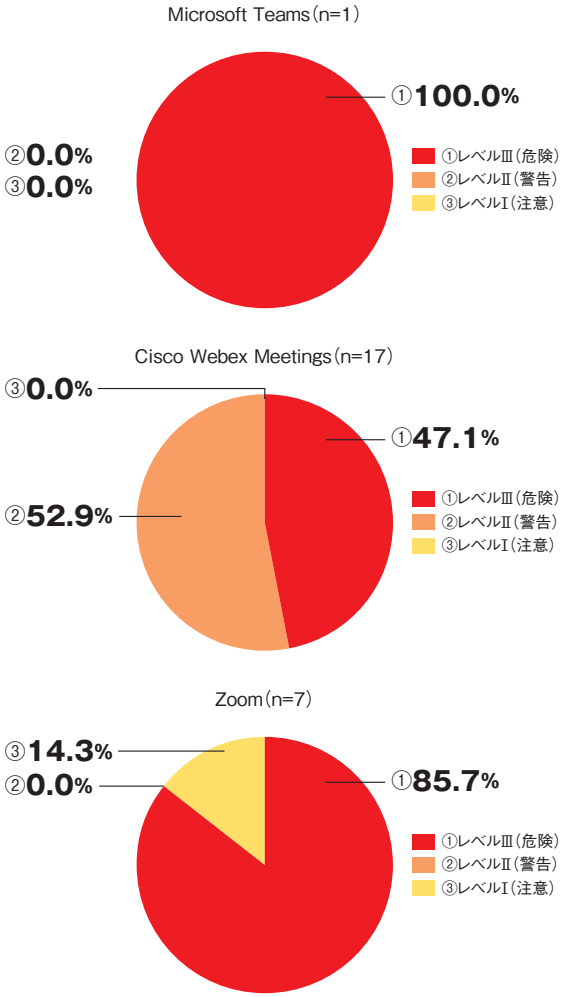
(3) テレワーク等で使われるソフトウェアの脆弱性について

2020 年は新型コロナウイルスの影響により、組織においてテレワークの普及が急速に進んだ。テレワークで利用するようになった VPN 製品や Web 会議サービスは、利用者が初めて使うものや、緊急時用に導入していたが日々の業務では使っていなかったものである等の理由により、利用経験が浅く、情報の収集先やアップデートの適用方法を知らないまま利用を続けているケースが少なからずあると考えられる。しかし、脆弱性対策が不十分なまま利用を続けると、攻撃者に脆弱性を悪用され、ソフトウェアの認証情報や組織の機密情報が窃取されたり、Web 会議をのぞき見されたりする等の被害に遭う恐れがある。実際に攻撃者が重要な情報を窃取するため、テレワーク環境を標的とした攻撃を行っているとの情報も公開※218 されており、VPN 製品や Web 会議サービス等のテレワーク環境で使われるソフトウェアを利用する際は十分注意する必要がある（「3.3.2 テレワークに関連した問題」参照）。

2019 年及び 2020 年に JPCERT/CC より、悪用の可能性がある複数の VPN 製品について注意喚起等※219 が公開されている。図 1-3-7（次ページ）は、当該注意喚起等に記載されている Palo Alto Networks, Inc. の VPN 製品（PAN-OS）、Fortinet, Inc. の VPN 製品（FortiOS）、Pulse Secure, LLC. の VPN 製品（Pulse Policy Secure 及び Pulse Connect Secure）に関して、2020 年に JVN iPedia に登録された脆弱性対策情報の深刻度のレベル別割合である。いずれもレベルⅡ以上に分類される脆弱性が 9 割以上を占めていた。ベンダから修正プログラムがリリースされた際には早急に対応を行



■図 1-3-7　JVN iPedia に登録された VPN 製品の脆弱性対策情報のレベル割合
(出典)JVN iPedia の登録情報を基に IPA が作成



■図 1-3-8　JVN iPedia に登録された Web 会議サービスの脆弱性対策情報のレベル割合
(出典)JVN iPedia の登録情報を基に IPA が作成

うことが求められる。特に注意喚起等が行われている脆弱性については、悪用される可能性が高いため、アップデートの見落としがないか十分に確認する必要がある(当該脆弱性を悪用した攻撃については「1.2.5(1)(a)攻撃事例」参照)。

図 1-3-8 は、Web 会議サービスである Microsoft 社の Microsoft Teams、Cisco Systems, Inc. の Cisco Webex Meetings(Desktop と Online を含む)、Zoom Video Communications, Inc. の Zoom(Client と Meetings を含む)のそれぞれについて、2020 年に JVN iPedia へ登録された脆弱性対策情報の深刻度のレベル別割合である。件数としては少ないが、図 1-3-7 と同様に、レベルⅡ以上に分類される脆弱性の割合が大きく注意が必要である。このうち、Zoom の脆弱性に関しては、2020 年 4 月 3 日に IPA より注意喚起[※220]を実施している。

VPN 製品や Web 会議サービス等の脆弱性を悪用する攻撃の被害を防ぐためには、利用しているソフトウェアの脆弱性対策情報やそのアップデートがどこで公開されているかを調べた上で、日頃から情報収集を行い、ベンダから修正プログラムが提供された際には速やかに適用する等の対策を実施することが求められる。また、クライアント側のソフトウェアだけでなく、自組織でサーバを構築している場合は、サーバ側のソフトウェアについても同様の対応が必要となる。更に、システム管理者は外部からサイバー攻撃を受けた形跡がないか等の確認を行い、適宜、組織の規定や対策の見直しを行うことも重要である。

(4) 今後の展望

JVN iPedia へ登録された脆弱性対策情報の累計件数は、2020 年 12 月末時点で 12 万 5,000 件を超えている。2017 年以降は毎年 1 万 5,000 件前後の脆弱性対策情報が登録されており、2021 年以降も同様の傾向で登録されていくものと考えられる。

2020 年は新型コロナウイルスの影響により、組織はテレワークへの移行等、働き方の大きな転換が必要となった。その一方、テレワークで使われるソフトウェア等を狙った攻撃が増加した※221。今後の新型コロナウイルスの感染状況にもよるが、2021 年以降も継続してテレワークは行われていくと考えられる。それを想定した場合、開発者やセキュリティ技術者だけでなく、脆弱性を悪用する攻撃者にとっても、テレワークで使われるソフトウェアの脆弱性は注目の対象となり、2021 年には 2020 年以上に脆弱性が多く発見され、JVN iPedia で公開される可能性がある。

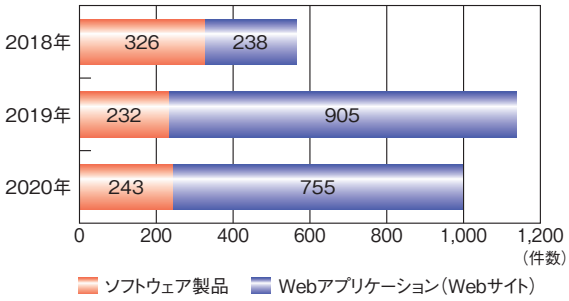
テレワークで使われるソフトウェアの脆弱性の中でも特に VPN 製品の脆弱性は、組織のネットワークの入り口に存在するため、それを悪用されることで組織内部に侵入される恐れがある。その後、ランサムウェア等のウイルスに感染させられた場合、組織は大きな二次被害を受けることになる。被害が脆弱性を有する VPN 製品単体にはとどまらないことを十分理解し、VPN 製品を利用する組織には適切な脆弱性の管理が求められる。なお、VPN 製品の脆弱性を突いた攻撃事例については「1.2.5 (1) VPN 製品の脆弱性を対象とした攻撃」を参照されたい。

テレワーク等の新たな働き方を支えるシステム管理者やセキュリティの担当者が JVN iPedia に掲載される脆弱性対策情報を活用し、組織のセキュリティ対策に役立てることが期待される。

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

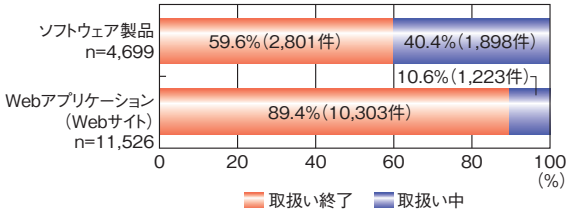
ソフトウェア製品や Web アプリケーション（Web サイト）の脆弱性を悪用した攻撃による情報漏えい、及び Web ページ改ざん等の被害は、2020 年も引き続き発生している。更に、修正プログラムが未適用で攻撃対象となる機器に関する情報が公開されるという事態も起こっている。例えば、脆弱性の影響を受ける VPN 製品のホスト情報が公開されたため、NISC や JPCERT/CC から注意喚起※222 がなされた。

「情報セキュリティ早期警戒パートナーシップ」（以下、パートナーシップ）では、脆弱性関連情報の届出※223 を受け付けているが、2020 年に届出された件数は、ソフトウェア製品が 243 件、Web サイトが 755 件、合計 998 件であった。2019 年のソフトウェア製品と Web サイトの総届出件数（1,137 件）と比較すると、約 12% 減少している。なお、それぞれの件数を 2019 年の届出件数（ソフトウェア製品：232 件、Web サイト：905 件）と比較すると、ソフトウェア製品に対する届出は約 5% 増加、Web サイトに対する届出は約 17% 減少した（図 1-3-9）。



■図 1-3-9　脆弱性関連情報の種類別届出状況（2018 ～ 2020 年）
（出典）パートナーシップの届出状況を基に IPA が作成

パートナーシップ開始時点（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 4,699 件、Web サイトは 1 万 1,526 件となり、2020 年 12 月末時点までの合計が 1 万 6,225 件に上る。これらの届出のうち IPA での取り扱いが終了※224 した届出件数は、ソフトウェア製品 2,801 件（59.6%）、Web サイト 1 万 303 件（89.4%）という状況である（図 1-3-10）。



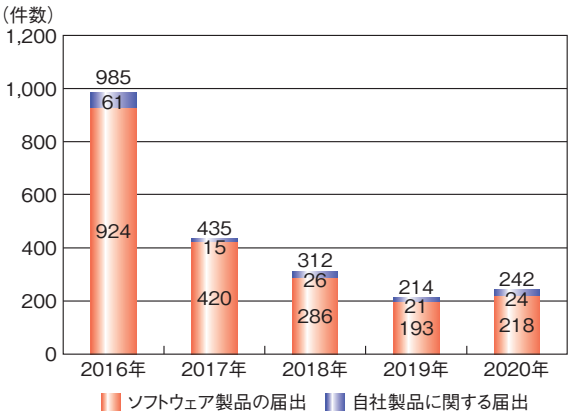
■図 1-3-10　脆弱性関連情報の種類別取扱終了状況
（2020 年末までの累計）
（出典）パートナーシップの届出状況を基に IPA が作成

パートナーシップには、製品開発者と連絡が取れず進展が望めない届出を公表する手続きとして、公表判定委員会※225 がある。2020 年は、公表判定委員会の判定の結果、9 件の調整不能案件を JVN で公表した（「1.3.2 (1) (b) 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

2020 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、242 件であった。

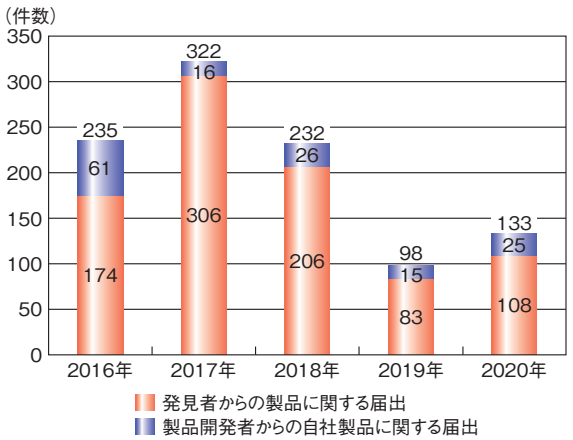
図 1-3-11（次ページ）は、2016 年から 2020 年までのソフトウェア製品の届出受付数（不受理を除く）を示している。2016 年からソフトウェア製品の届出は年々減少していたが、2020 年は 242 件となり、2019 年の 214 件を上回る件数となった。ソフトウェア製品の届出のうち、製品開発者からの自社製品に関する届出は、242 件中 24 件となり、2019 年の 21 件から増加した。



■図 1-3-11　ソフトウェア製品の届出受付数（2016 ～ 2020 年）
（出典）パートナーシップの届出状況を基に IPA が作成

また、パートナーシップに届出のあった脆弱性の対策情報が JVN 公表に至った件数は、133 件であった。

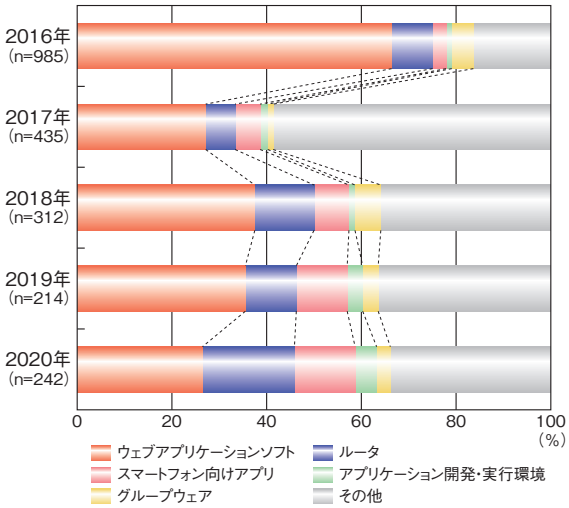
図 1-3-12 は、2016 年から 2020 年までの JVN 公表に至った届出数を示している。2017 年、2018 年、2019 年と年々 JVN 公表数は減少していたが、2020 年は一転して件数が増加した。自社製品に関する届出についても、2019 年の 15 件から増加し、2020 年は 25 件の公表となった。



■図 1-3-12　ソフトウェア製品の JVN 公表した届出数（2016 ～ 2020 年）
（出典）パートナーシップの届出状況を基に IPA が作成

(a) パートナーシップで取り扱ったソフトウェア製品の動向

図 1-3-13 は、製品の種類別の届出受付数の割合を示している。2020 年も、例年と同様、「ウェブアプリケーションソフト」の割合が最も大きく 26.4% を占めたが、直近 5 年においては、最も小さい割合となっている。対して、割合が大きく増加したものとしては「ルータ」と「スマートフォン向けアプリ」がある。「スマートフォン向けアプリ」は年々増加する傾向にあり、2020 年も 2019 年の 10.7% から増加し、12.8% となった。他方、「ルータ」は 2019



■図 1-3-13　製品種類別のソフトウェア製品の届出受付数の割合（2016 ～ 2020 年）
（出典）パートナーシップの届出状況を基に IPA が作成

年には前年から割合が減少し 10.7% となっていたが、2020 年は 19.4% と約 2 倍となり、2004 年の制度開始以来で最大となった。

「ウェブアプリケーションソフト」や「スマートフォン向けアプリ」等は、インターネット等からダウンロードすることで入手可能であり、また、無償であるものも多い。一方で「ルータ」は一般的には物理的なハードウェアであり、かつ有償の製品である。そのため、脆弱性の発見者にとって脆弱性の調査には一定のハードルがあるといえる。2020 年に届出が増加したのは、テレワークの普及拡大等により、インターネット環境の基盤となるネットワーク機器として、ルータの社会的重要性が高まったことが遠因となり、発見者からも調査対象として着目された可能性が考えられる。

ルータの脆弱性には、パケット処理に起因するもの等、ネットワーク機器に特有のものもあるが、Web ブラウザからアクセスできる管理コンソールを備えているルータには、クロスサイト・スクリプティングやクロスサイト・リクエスト・フォージェリといった、一般的な Web アプリケーションソフトに発見される脆弱性が存在する可能性がある。

JVN において 2020 年に公表した脆弱性対策情報をみても、ルータには、上述したクロスサイト・スクリプティングを含め様々な種別の脆弱性が発見されていることが分かる（次ページ表 1-3-1）。

利用者は、他のソフトウェア製品と同様にルータについても脆弱性が日々発見されていて、アップデートが必要となることを十分認識する必要がある。また、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

JVN 番号	件名
JVN#21753370	Junos OS におけるクロスサイトスクリプティングの脆弱性
JVN#07375820	Junos OS におけるディレクトリトラバーサルの脆弱性
JVN#25766797	Aterm WF1200CR、WG1200CR および WG2600HS における複数の OS コマンドインジェクションの脆弱性
JVN#38732359	ヤマハ製の複数のネットワーク機器におけるサービス運用妨害（DoS）の脆弱性
JVN#09166495	AirStation WHR-G54S における複数の脆弱性
JVN#82892096	複数のエレコム製 LAN ルーターにおける OS コマンドインジェクションの脆弱性
JVN#55917325	NEC Aterm SA3500G における複数の脆弱性

■表 1-3-1　2020 年に JVN 公表した「ルータ」の脆弱性対策情報
（出典）JVN を基に IPA が作成

公表されていないか定期的に確認しなければならない。そ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が負担となる場合には、自動アップデート機能があるルータに置き換えることも一つの方策となる。新たにルータを購入する際には、アップデート対応は誰が実施するのか、という視点をもって製品情報を事前に調べておくことが、セキュリティを確保する上で重要となる。

(b) 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 で公開しているが、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、公開に向けての調整が難航してしまうものが存在する。

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。

2020 年には、公表判定委員会での判定を経て、9 件の脆弱性情報が JVN に公表された（表 1-3-2）。JVN での調整不能案件の公表は 2018 年以来 2 年ぶりとなった。また、公表されたもののうち 4 件は、深刻度の 3 段階レベルのうち最上位の「危険」と判断される影響の大きい脆弱性であった。

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、

JVN 番号	深刻度	件名
JVN#85942151	警告	メールフォームにおけるクロスサイトスクリプティングの脆弱性
JVN#77634892	危険	メールフォームにおいて任意の PHP コードが実行可能な脆弱性
JVN#32415420	危険	私本管理 Plus GOOUT における複数の脆弱性
JVN#63834780	危険	私本管理 Plus GOOUT における OS コマンドインジェクションの脆弱性
JVN#29095127	警告	Cute News におけるクロスサイトスクリプティングの脆弱性
JVN#58176087	警告	Cute News において任意の PHP コードが実行可能な脆弱性
JVN#88033799	警告	WL-Enq（WEB アンケート）におけるクロスサイトスクリプティングの脆弱性
JVN#27951364	警告	WL-Enq（WEB アンケート）における OS コマンドインジェクションの脆弱性
JVN#88277644	危険	掲示板 積木における OS コマンドインジェクションの脆弱性

■表 1-3-2　2020 年に JVN 公表した調整不能案件
（出典）JVN を基に IPA が作成

製品の使用を停止することが求められる。

(c) 製品開発者による CNA への参加

IPA とともにパートナーシップを運営している JPCERT/CC は、パートナーシップに届出がなされた脆弱性を JVN 公表する際に、脆弱性の共通識別子である CVE を採番している。

組織がこの CVE の採番を実施するためには、採番機関である CNA として承認される必要があるが、2020 年には、日本国内組織として LINE 株式会社[※226]と三菱電機株式会社[※227]の 2 社が新たに CNA として承認された[※228]。CNA として承認されることで自社製品の脆弱性について、自社の判断において CVE を採番することが可能となり、それによって脆弱性情報の識別・管理がより迅速に、容易に実施できるようになる。

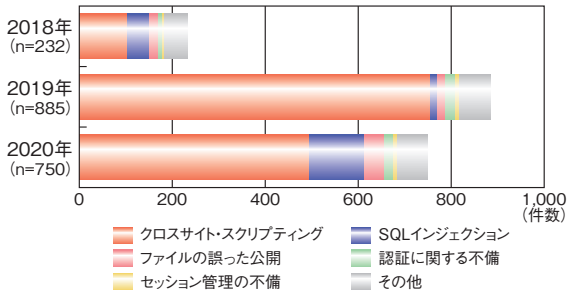
製品開発者が CNA として活動することで、自社の脆弱性情報の取り扱いレベルの向上やより効果的な流通が実現し、脆弱性悪用の被害が低減することが期待される。

(2) Web アプリケーション（Web サイト）の脆弱性

2020 年にパートナーシップで受け付けた Web アプリケーションの届出（不受理 5 件を除く）は、750 件であった。

図 1-3-14（次ページ）は、2018 年から 2020 年までの脆弱性の種別の届出受付数（不受理を除く）を示してい

る。「クロスサイト・スクリプティング」は、2018 年から 2019 年では届出全体に対する割合が増加傾向にあったものの 2020 年では減少した。他方、2019 年から増加したものとしては、「SQL インジェクション」と「ファイルの誤った公開」がある。「SQL インジェクション」の届出は、2020 年は 119 件であり、全体の 15.9% を占めている。2019 年の「SQL インジェクション」の届出は 14 件であり、全体の 1.6% にとどまっていた。2019 年と 2020 年の「SQL インジェクション」の届出を比較すると件数は 8.5 倍に増加した。



■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（2018 ～ 2020 年）
（出典）パートナーシップの届出状況を基に IPA が作成

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、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※229」、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※230」と題する注意喚起を行っているが 2020 年も解消されていない。

届出の状況からしても、SQL インジェクションの脆弱性は修正にかかる時間が長期化する傾向がある。例えば、クロスサイト・スクリプティングの脆弱性では修正までに 90 日以上を要した届出の割合は 30.3% であるが、SQL インジェクションの脆弱性は 47.2% を占めており、速やかな対策が難しいことがうかがえる。

SQL インジェクションの脆弱性は、情報漏えい等により事業継続の面で大きな影響を受ける恐れがあるため、早期に対策することが望まれる。

(a) SQL インジェクションの脆弱性

SQL インジェクションとは、データベースへの命令文である SQL 文の組み立て方法に問題があり、悪意あるリクエストによって、不正な SQL 文が生成・実行され、データベースを不正利用されてしまうという攻撃である。インジェクション（injection）は「注入」という意味である。

SQL インジェクションの脆弱性により、データベースを直接操作され、データベース内に格納された営業秘密等の機密情報や個人情報が窃取されたり、情報が消去・改ざんされる等の脅威が発生する。

個人情報等の重要な情報をデータベースに格納している Web サイトは、特に注意が必要である。

対策としては、プレースホルダという変数を使って構成した SQL 文の雛形を事前に作成し、その変数に外部から渡される値を機械的な処理で割り当てるバインドを利用する方法がある。その中でも、バインドの処理をデータベースエンジン側で行う静的プレースホルダを利用することが、セキュリティの観点から安全であることが知られている。ただし、データベースエンジンによってはサポートしていない場合もある。

別の対策としては、SQL 文にとって特殊な意味を持つ記号・文字をエスケープ処理する方法も有効である。しかし、データベースエンジンの種類や設定ごとにエスケープすべき対象が異なる点に注意する必要がある。

また、Web サイトのアプリケーションだけでなく、Web サイトの構築に利用している CMS（Contents Management System）や、CMS のプラグインに SQL インジェクションの脆弱性が存在する場合もあるため、CMS やプラグインを最新バージョンにアップデートして利用する必要がある。

(b) パートナーシップから見る 2020 年の SQL インジェクション届出の現状

2020 年の SQL インジェクションの届出の半数以上は、URL パラメータへの特殊文字の入力や、文字列を入力するフォームへの特殊文字の入力により、想定されないリクエストが Web アプリケーションに送信され、Web サイトにおける通常の挙動とは異なるエラーメッセージが表示され発見に至ったというものであった。

そこで表示されるエラーメッセージには、実行エラーとなった SQL 文の情報が含まれていることがあり、その情報を基に SQL インジェクションの脆弱性が存在していることが推測できる。

また、同一の Web サイトに SQL インジェクションとクロスサイト・スクリプティングの二つの脆弱性があると届出されたものもあった。

(c) Web サイト運営者に求められる対策

前述のとおり、2020 年の SQL インジェクションの届出では、URL パラメータや文字列を入力するフォームへの特殊文字の入力によって問題があることを指摘するものが多数を占めていた。

Web サイト運営者はまず、改めてそのような箇所に SQL インジェクションの脆弱性が存在していないか、IPA が公開している「ウェブ健康診断 仕様※231」等を参照の上、確認し、脆弱性が検出された場合は、詳細な診断を行うか、または改修を検討いただきたい。なお、Web サイト運営者が自組織だけで脆弱性の有無を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。

対策を行う際には、IPA が公開している「安全な SQL の呼び出し方※232」等を参照し、根本的な対策を実施していただきたい。また、エラーメッセージの情報が SQL インジェクションの発見とその悪用を容易にしてしまう可能性があるため、根本的な対策と併せてエラーメッセージの表示を抑制する対策も必要である。

また、クロスサイト・スクリプティングの脆弱性も同一の Web サイトに見つかった事例があり、クロスサイト・スクリプティングも依然として大きな脅威である。SQL インジェクション以外の脆弱性が Web サイトに存在する可能性もあるため、IPA が公開している「安全なウェブサイトの作り方※233」を参照し見直しをしていただきたい。

なお、Web サイトにページの新規追加や変更を行って、Web サイトを一般へ公開する際にも脆弱性が存在しないか都度確認をすることが必要である。

COLUMN

「危険だから利用しない」ではなく「安全に利用するために」の対策を

2021 年 1 月 28 日、GitHub 上に公開されているソースコードが企業のシステムのものではないかと、機密情報の流出疑惑が SNS で話題となりました。翌日には、公開されていた情報が自社の業務システムのソースコードの一部であることを三井住友銀行が確認したと報じられ、以降も複数の企業で実際に情報が流出していたことが明らかになりました[i]。ただし、いずれもセキュリティに影響を与えるような情報ではなかったことは不幸中の幸いといえます。

この流出事例は、当該システムの開発に関わった人物における、GitHub というサービスについての理解や情報の取り扱いに対する意識の不十分さから、意図せず公開してしまったことで発生したと見られています[ii]。当然、GitHub を利用すること自体が危険というわけではありませんが、このような事例が発生すると、組織によってはサービスの利用禁止を検討することもあるでしょう。そのような動きを案じてか、一般社団法人コンピュータソフトウェア協会（CSAJ）では、同年 2 月 2 日に GitHub についての正しい理解と対応に向けた文書を発表しています[iii]。

今回の事例は、現在のソフトウェア開発におけるセキュリティ確保の難しさについて多くのことを示唆しています。そもそもアップロードした人物の手元にソースコードが存在していたことが問題であって、要因としてもサプライチェーンリスクを考慮した契約が十分であったか、業務に関する情報を容易に持ち出せない開発環境であったか、開発担当者の情報資産に対する意識向上を図る教育は十分に実施されていたか等が考えられます。それゆえ、情報流出のリスク低減のために、単にサービスの利用を禁止するのは賢明とは言えません。

例えば、エレベータで事故が起きたという報道があった場合、会社やマンション等で危険だからとエレベータを利用禁止とするのではなく、安全に利用するためのルールを決めて周知したり、点検する項目や回数を増やす等、事故を起こさないような対策を検討することが多いのではないでしょうか。

あるサービスの利用が原因で発生した被害を自組織でも起こさないようにと、そのサービスを利用しないことを対策とするのは簡単です。しかし、リスクだけでなく、サービスの利用により生じるメリット、またサービスを利用しないことのデメリットにも注目し、更に自組織の運用実態をも加味した上で十分に検討を重ねて結論を出すことが望まれます。利便性とセキュリティは背反する関係性であるため、安全に利用できるバランスを見極めることは容易ではありませんが、今一度セキュリティ対策を見直すとともに、情報資産の取り扱いに対する意識向上の必要性についても振り返ってほしいものです。

i　日経クロステック：GitHub 上に三井住友銀の一部コードが流出、「事実だがセキュリティーに影響せず」 https://xtech.nikkei.com/atcl/nxt/news/18/09551/〔2021/6/2 確認〕
日経クロステック：GitHub 上のソースコード流出問題の被害は 5 社に、NEC とコアも確認 https://xtech.nikkei.com/atcl/nxt/news/18/09574/〔2021/6/2 確認〕
ii　ITmedia NEWS：三井住友銀行などのソースコードが流出 “年収診断”したさに GitHub に公開か【追記あり】 https://www.itmedia.co.jp/news/articles/2101/29/news107.html〔2021/6/2 確認〕
iii　CSAJ：GitHub に関する対応とお願い https://www.csaj.jp/NEWS/pr/210202_github.html〔2021/6/2 確認〕

※1 https://resources.trendmicro.com/jp-docdownload-form-m308-web-2020-annualsecurityreport.html〔2021/6/1 確認〕
※2 IBM 社：IBM X-Force 脅威インテリジェンス・インデックス・レポート https://www.ibm.com/jp-ja/security/data-breach/threat-intelligence〔2021/6/1 確認〕
※3 https://apwg.org/trendsreports/〔2021/6/1 確認〕
※4 https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf〔2021/6/1 確認〕
※5 https://www.verizon.com/business/resources/reports/dbir/〔2021/6/1 確認〕
※6 https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020〔2021/6/1 確認〕
※7 https://www.intezer.com/blog/cloud-security/2020-set-record-for-new-linux-malware-families/〔2021/6/1 確認〕
※8 「2020 年年間セキュリティラウンドアップ」に掲載されているグラフでは「URL」と記載されているが、「2020 年年間セキュリティラウンドアップ」本文の記載にあわせて「不正 URL」とした。
※9 https://www.trendmicro.com/content/dam/trendmicro/global/ja/security-intelligence/security-report/2020h1/2020-h1-security-roundup.pdf〔2021/6/1 確認〕
※10 SolarWinds 社：SolarWinds Security Advisory https://www.solarwinds.com/ja/sa-overview/securityadvisory〔2021/6/1 確認〕
※11 REUTERS：U.S. Homeland Security, thousands of businesses scramble after suspected Russian hack https://www.reuters.com/article/global-cyber-idUSKBN28026X〔2021/6/1 確認〕
※12 FireEye, Inc.：Global Intrusion Campaign Leverages Software Supply Chain Compromise https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html〔2021/6/1 確認〕
※13 「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。
※14 C&C サーバ：Command and Control サーバの略。ウイルス等により乗っ取ったコンピュータ等に対し、遠隔から命令を送り制御するサーバ。
※15 JPCERT/CC：マルウェア Emotet のテイクダウンと感染端末に対する通知 https://blogs.jpcert.or.jp/ja/2021/02/emotet-notice.html〔2021/6/1 確認〕
※16 MBSD 社：SNAKE(EKANS) ランサムウェアの内部構造を紐解く https://www.mbsd.jp/blog/20200616.html〔2021/6/1 確認〕
※17 @IT：「Mirai」ソースコード徹底解剖ーその仕組みと対策を探る https://www.atmarkit.co.jp/ait/articles/1611/08/news028.html〔2021/6/1 確認〕
※18 「IBM X-Force 脅威インテリジェンス・インデックス 2021」のグラフでは「水飲み場攻撃」は項目として存在しない。IBM X-Force 脅威インテリジェンス・インデックス 2020」のグラフでは「リモート・デスクトップ」「リムーバブル・メディア」は項目として存在しない。
※19 IBM 社：X-Force 脅威インテリジェンス・インデックス 2020 公開 https://www.ibm.com/blogs/security/jp-ja/x-force-threat-intelligence-index-reveals-top-cybersecurity-risks-of-2020/〔2021/6/1 確認〕
※20 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。
※21 https://www.jpcert.or.jp/ir/report.html〔2021/6/1 確認〕
※22 フィッシング対策協議会：月次報告書 一覧 https://www.antiphishing.jp/report/monthly/〔2021/6/1 確認〕
※23 MBSD 社において集計方法および対象期間が 2020 年より変更された。2019 年までの年度（4 月～翌年 3 月）集計から、1 月から 12 月末となった。そのため、「情報セキュリティ白書 2020」の図 1-1-7（p.11）の 2019 年度件数（458 件）と整合しない。
※24 JPCERT/CC：インシデント報告対応レポート 2020 年 10 月 1 日～ 2020 年 12 月 31 日 https://www.jpcert.or.jp/pr/2021/IR_Report20210121.pdf〔2021/6/1 確認〕
※25 JPCERT/CC：インシデント報告対応レポート 2020 年 4 月 1 日～ 2020 年 6 月 30 日 https://www.jpcert.or.jp/pr/2020/IR_Report20200714.pdf〔2021/6/1 確認〕
※26 フィッシング対策協議会の 2020 年 4 月～ 2021 年 3 月の「フィッシング報告状況」の「総評」によれば、報告件数に占める Amazon のフィッシングメールの占める割合は、6 月 56%、7 月 62%、8 月 67.3%、11 月 62.3%、12 月 50%、1 月 61.4%、2 月 60.4%、3 月 51.9%。
フィッシング対策協議会：月次報告書 一覧 https://www.antiphishing.jp/report/monthly/〔2021/6/1 確認〕
※27 フィッシング対策協議会：2020/10 フィッシング報告状況 https://www.antiphishing.jp/report/monthly/202010.html〔2021/6/1 確認〕
※28 フィッシング対策協議会の 2020 年 4 月～ 2021 年 3 月の「フィッシング報告状況」の「総評」によれば、4 ブランドの占める割合は、6 月 88%、7 月 90%、8 月 92.6%、9 月 93.2%、10 月 90.9%、11 月 90.1%、12 月 86%、1 月 88.6%、2 月 90.8%、3 月 81.7%。
フィッシング対策協議会：月次報告書 一覧 https://www.antiphishing.jp/report/monthly/〔2021/6/1 確認〕
※29 https://www.antiphishing.jp/report/monthly/202103.html〔2021/6/1 確認〕
※30-1 IPA：情報セキュリティ 10 大脅威 2021 https://www.ipa.go.jp/security/vuln/10threats2021.html〔2021/6/1 確認〕
※30-2 「情報セキュリティ 10 大脅威」の「組織におけるランキング」において、ランサムウェアは 2016 年 7 位、2017 年 2 位、2018 年 2 位、2019 年 3 位、2020 年 5 位。
※30-3 株式会社カプコン：不正アクセスに関する調査結果のご報告【第 4 報 】 https://www.capcom.co.jp/ir/news/html/210413.html〔2021/6/1 確認〕
※30-4 総務省：第 2 節 ICT サービスの利用動向 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/n5200000.pdf〔2021/6/1 確認〕
※30-5 ロイター：企業のクラウド導入加速、コロナ流行で＝アマゾン AWS トップ https://jp.reuters.com/article/amazoncom-aws-idJPL4N2IH3WO〔2021/6/1 確認〕
※30-6 読売新聞オンライン：【独自】米企業クラウド「難解で手に負えず」、ペイペイも楽天も神戸市も・・・設定ミスで情報流出か https://www.yomiuri.co.jp/national/20210502-OYT1T50200/〔2021/6/1 確認〕
※30-7 ITmedia NEWS：「ドコモ口座」不正預金引き出し、記者会見の一問一答まとめ https://www.itmedia.co.jp/news/articles/2009/10/news154_2.html〔2021/6/1 確認〕
※30-8 朝日新聞デジタル：ドコモ口座、17 行と連携中断 被害さらに広がるおそれ https://digital.asahi.com/articles/ASN986X6LN98ULFA00L.html?iref=pc_ss_date_article〔2021/6/1 確認〕
※30-9 株式会社 NTT ドコモ：ドコモ口座への銀行口座の新規登録における対策強化について https://www.nttdocomo.co.jp/info/news_release/detail/20200909_00_m.html〔2021/6/1 確認〕
※30-10 日経クロステック：厄介な「ドコモ口座」不正引き出し問題、解決に求められるのは https://xtech.nikkei.com/atcl/nxt/column/18/00086/00137/〔2021/6/1 確認〕
※30-11 NHK：注目ニュースのポイントを Q&A で解説 サクサク経済 Q&A ドコモ口座で何が起きたのか？ https://www3.nhk.or.jp/news/special/sakusakukeizai/articles/20200911.html〔2021/6/1 確認〕
※30-12 朝日新聞デジタル：ドコモ口座被害、6 割がゆうちょ メルペイルートも判明 https://digital.asahi.com/articles/ASN9J72NVN9JULFA017.html?iref=pc_rellink_02〔2021/6/1 確認〕
株式会社ゆうちょ銀行：即時振替サービスの再開について（2 月 19 日更新） https://www.jp-bank.japanpost.jp/news/2020/news_id001629.html〔2021/6/1 確認〕
※30-13 株式会社 NTT ドコモ：（お知らせ）「ドコモ口座」における銀行口座の新規登録および銀行口座からのチャージ再開について https://www.nttdocomo.co.jp/info/news_release/2021/01/29_00.html〔2021/6/1 確認〕
※30-14 eKYC（electronic Know Your Customer）：オンラインで本人の確認を行う仕組み。
※31 朝日新聞デジタル：経団連を標的、中国人ハッカー集団 ウイルスは 2 年潜伏 https://www.asahi.com/articles/ASM196VTPM19ULZU01B.html〔2021/4/28 確認〕
※32 https://www.ipa.go.jp/security/event/2013/isec-semi/documents/2013videosemi_targeted_cyber_attacks_v1.pdf〔2021/4/28 確認〕
※33 McAfee, LLC：Updated BlackEnergy Trojan Grows More Powerful https://www.mcafee.com/blogs/other-blogs/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/〔2021/4/28 確認〕
※34 NTT コム社：当社への不正アクセスによる情報流出の可能性について https://www.ntt.com/about-us/press-releases/news/article/2020/0528.html〔2021/4/28 確認〕
※35 NTT コム社：当社への不正アクセスによる情報流出の可能性について（第 2 報） https://www.ntt.com/about-us/press-releases/news/article/2020/0702.html〔2021/4/28 確認〕
※36 NTT コム社のクラウドサービスである「Biz ホスティング エンタープライズ」「ECL オプションサービス」。
※37 2020 年 10 月 14 ～ 16 日に開催されたオンラインイベント「NTT Communications Digital Forum 2020」の特別講演「【実録】サイバー攻撃が残した教訓～アフター APT のセキュリティ対策とは～」の講演内容に基づいて記載。
※38 BYOD（Bring your own device）：従業員が個人保有している PC や携帯機器を、職場や自宅などから業務利用すること。
※39 日経クロステック：NTT コム・サイバー攻撃事件の深層、多要素

認証を無効化されていた　https://xtech.nikkei.com/atcl/nxt/column/18/01157/081900017/〔2021/4/28 確認〕
※ 40 JPCERT/CC：マルウエア LODEINFO の進化　https://blogs.jpcert.or.jp/ja/2020/06/LODEINFO-2.html〔2021/4/28 確認〕
※ 41 株式会社ラック：【緊急レポート】Microsoft 社のデジタル署名ファイルを悪用する「SigLoader」による標的型攻撃を確認　https://www.lac.co.jp/lacwatch/report/20201201_002363.html〔2021/4/28 確認〕
※ 42 マクニカネットワークス株式会社、TeamT5, Inc.：標的型攻撃の実態と対策アプローチ 第 4 版　https://www.macnica.net/mpressioncss/feature_06.html〔2021/4/28 確認〕
※ 43 三菱重工業株式会社：当社グループ名古屋地区のネットワークに対する第三者からの不正アクセスに係る件　https://www.mhi.com/jp/notice/notice_200807.html〔2021/4/28 確認〕
※ 44 キヤノンマーケティングジャパン株式会社：航空宇宙・軍事企業を狙った標的型攻撃　https://eset-info.canon-its.jp/malware_info/trend/detail/200709.html〔2021/4/28 確認〕
※ 45 JPCERT/CC：JPCERT/CC インシデント報告対応レポート 2020 年 7 月 1 日～ 2020 年 9 月 30 日　https://www.jpcert.or.jp/pr/2020/IR_Report20201015.pdf〔2021/4/28 確認〕
※ 46 JPCERT/CC：Quasar Family による攻撃活動　https://blogs.jpcert.or.jp/ja/2020/12/quasar-family.html〔2021/4/28 確認〕
※ 47 JPCERT/CC：攻撃グループ Lazarus が侵入したネットワーク内で使用するツール　https://blogs.jpcert.or.jp/ja/2021/01/Lazarus_tools.html〔2021/4/28 確認〕
※ 48 https://www.jpcert.or.jp/research/AD.html〔2021/4/28 確認〕
※ 49 JPCERT/CC：Netlogon の特権の昇格の脆弱性（CVE-2020-1472）への早急な対応を　https://www.jpcert.or.jp/newsflash/2020091601.html〔2021/4/28 確認〕
※ 50 IPA：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/files/000084974.pdf〔2021/5/13 確認〕
※ 51 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〔2021/5/13 確認〕
※ 52 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/active/infra/pdf/ransomware20201126.pdf〔2021/5/13 確認〕
※ 53 株式会社カプコン：不正アクセスによるシステム障害発生に関するお知らせ　https://www.capcom.co.jp/ir/news/html/201104.html〔2021/5/13 確認〕
※ 54 株式会社カプコン：不正アクセスによる情報流出に関するお知らせとお詫び　https://www.capcom.co.jp/ir/news/html/201116.html〔2021/5/13 確認〕
※ 55 株式会社カプコン：不正アクセスによる情報流出に関するお知らせとお詫び【第 3 報】　https://www.capcom.co.jp/ir/news/html/210112.html〔2021/5/13 確認〕
※ 56 株式会社カプコン：不正アクセスに関する調査結果のご報告【第 4 報】　https://www.capcom.co.jp/ir/news/html/210413.html〔2021/5/13 確認〕
※ 57 Bleeping Computer：Capcom hit by Ragnar Locker ransomware, 1TB allegedly stolen　https://www.bleepingcomputer.com/news/security/capcom-hit-by-ragnar-locker-ransomware-1tb-allegedly-stolen/〔2021/5/13 確認〕
※ 58 鉄建建設株式会社：サイバー攻撃による被害と復旧状況について　https://www.tekken.co.jp/topics/assets/20201009_topics.pdf〔2021/5/13 確認〕
※ 59 鉄建建設株式会社：サイバー攻撃による被害と復旧状況について（第三報）　https://www.tekken.co.jp/topics/assets/20201118_saibaosirase.pdf〔2021/5/13 確認〕
※ 60 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〔2021/5/13 確認〕
※ 61 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/〔2021/5/13 確認〕
※ 62 マクニカネットワークス株式会社：ランサムウェア感染時の対応は本当に完璧ですか!?暴露型ランサムウェアの実態とその対応方法とは　https://www.macnica.net/sandj/ransomware.html/〔2021/5/13 確認〕
セキュアワークス株式会社：日本国内で増加する 標的型ランサムウェアインシデント　https://www.secureworks.jp/resources/at-targeted-ransomware-spreading-in-japan〔2021/5/13 確認〕
ZDNet：Ransomware gang publishes tens of GBs of internal data from LG and Xerox　https://www.zdnet.com/article/ransomware-gang-publishes-tens-of-gbs-of-internal-data-from-lg-and-xerox/〔2021/5/13 確認〕
パロアルトネットワークス株式会社：脅威に関する情報：Maze ランサムウェアのアクティビティ　https://unit42.paloaltonetworks.jp/threat-brief-maze-ransomware-activities/〔2021/5/13 確認〕
※ 63 三井物産セキュアディレクション株式会社：SNAKE（EKANS）ランサムウェアの内部構造を紐解く　https://www.mbsd.jp/blog/20200616.html〔2021/5/13 確認〕
IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2020 年 4 月～ 6 月]《付録》～ EKANS ランサムウェアの解析事例～　https://www.ipa.go.jp/files/000084401.pdf〔2021/5/13 確認〕
※ 64 JPCERT/CC：ランサムウエア対策特設サイト　https://www.jpcert.or.jp/magazine/security/nomore-ransom.html〔2021/5/13 確認〕
JPCERT/CC：高度サイバー攻撃（APT）への備えと対応ガイド～企業や組織に薦める一連のプロセスについて　https://www.jpcert.or.jp/research/apt-guide.html〔2021/5/13 確認〕
JPCERT/CC：高度サイバー攻撃への対処におけるログの活用と分析方法　https://www.jpcert.or.jp/research/apt-loganalysis.html〔2021/5/13 確認〕
IPA：ランサムウェア対策特設ページ　https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html〔2021/5/13 確認〕
IPA：『高度標的型攻撃』対策に向けたシステム設計ガイド　https://www.ipa.go.jp/security/vuln/newattack.html〔2021/5/13 確認〕
※ 65 IRM（Information Rights Management）：業務で使用する文書ファイル等を暗号化し、閲覧や編集等を制限する仕組み。
※ 66 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_20151126.pdf〔2021/5/13 確認〕
※ 67 トレンドマイクロ社：フィッシング攻撃に注意、「ビジネスメール詐欺」の攻撃手口を分析　https://blog.trendmicro.co.jp/archives/17003〔2021/4/28 確認〕
トレンドマイクロ社：経営幹部の Office 365 アカウントを狙う詐欺キャンペーン「Water Nue」　https://blog.trendmicro.co.jp/archives/26178〔2021/4/28 確認〕
パロアルトネットワークス株式会社：脅威攻撃グループ SilverTerrier による新型コロナウイルスをテーマにしたビジネスメール詐欺の手口　https://unit42.paloaltonetworks.jp/silverterrier-covid-19-themed-business-email-compromise/〔2021/4/28 確認〕
※ 68 被害金額については、2015 ～ 2020 年の年次報告書（IC3：Annual Reports　https://www.ic3.gov/Home/AnnualReports〔2021/4/28 確認〕）を参照した。
※ 69 FBI：FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic　https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic〔2021/4/28 確認〕
IC3：Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments　https://www.ic3.gov/Media/Y2020/PSA200401〔2021/4/28 確認〕
※ 70 Infosecurity Magazine：Australians Arrested Over $2.6m Email Scam　https://www.infosecurity-magazine.com/news/australians-arrested-over-26m/〔2021/4/28 確認〕
Mirage News：Five charged as part of ongoing investigations into $4.7 million business email compromise scam　https://www.miragenews.com/five-charged-as-part-of-ongoing-investigations-into-47-million-business-email-compromise-scam/〔2021/4/28 確認〕
U.S. Department of Justice：Nigerian National Brought to U.S. to Face Charges of Conspiring to Launder Hundreds of Millions of Dollars from Cybercrime Schemes　https://www.justice.gov/usao-cdca/pr/nigerian-national-brought-us-face-charges-conspiring-launder-hundreds-millions-dollars〔2021/4/28 確認〕
Liverpool City Champion Liverpool, NSW：Man arrested at Liverpool over alleged $6 million online scam　https://www.liverpoolchampion.com.au/story/6825426/man-arrested-at-liverpool-over-alleged-6-million-online-scam/〔2021/4/28 確認〕
U.S. Department of Justice：Rhode Island Man Pleads Guilty to Conspiracy to Launder Funds of Email Compromise Fraud Targeting Massachusetts Lawyer　https://www.justice.gov/usao-ma/pr/rhode-island-man-pleads-guilty-conspiracy-launder-funds-email-compromise-fraud-targeting〔2021/4/28 確認〕
U.S. Department of Justice：Three Chicago-Area Residents Charged With Conducting Online Romance Fraud and Other Schemes　https://www.justice.gov/usao-ndil/pr/three-chicago-area-residents-charged-conducting-online-romance-fraud-and-other-schemes〔2021/4/28 確認〕
Campbelltown-Macarthur Advertiser Campbelltown, NSW：

Glenfield man charged in relation to $4.7 million business email scam https://www.macarthuradvertiser.com.au/story/6929911/glenfield-man-charged-in-relation-to-47-million-business-email-scam/〔2021/4/28 確認〕
U.S. Department of Justice：Four Individuals Are Charged For Operating As 'Money Mules' In Separate Business Email Compromise Schemes https://www.justice.gov/usao-wdnc/pr/four-individuals-are-charged-operating-money-mules-separate-business-email-compromise〔2021/4/28 確認〕
U.S. Department of Justice：Six Defendants Arrested In Multiple States For Laundering Proceeds From Fraud Schemes Targeting Victims Across The United States Perpetrated By Ghana-Based Criminal Enterprise https://www.justice.gov/usao-sdny/pr/six-defendants-arrested-multiple-states-laundering-proceeds-fraud-schemes-targeting〔2021/4/28 確認〕
※ 71 産経新聞：犯罪収益引き出し疑い逮捕　島国バハマの法人被害か https://www.sankei.com/affairs/news/200716/afr2007160012-n1.html〔2021/4/28 確認〕
産経新聞：「ビジネスメール詐欺」被害総額2億円か　容疑の70代男ら逮捕 https://www.sankei.com/affairs/news/201013/afr2010130012-n1.html〔2021/4/28 確認〕
※ 72 INTERPOL：Three arrested as INTERPOL, Group-IB and the Nigeria Police Force disrupt prolific cybercrime group https://www.interpol.int/en/News-and-Events/News/2020/Three-arrested-as-INTERPOL-Group-IB-and-the-Nigeria-Police-Force-disrupt-prolific-cybercrime-group〔2021/4/28 確認〕
Group-IB：Operation Falcon Group-IB helps INTERPOL identify Nigerian BEC ring members https://www.group-ib.com/media/gib-interpol-bec/〔2021/4/28 確認〕
※ 73 Microsoft 社：Microsoft takes legal action against COVID-19-related cybercrime https://blogs.microsoft.com/on-the-issues/2020/07/07/digital-crimes-unit-covid-19-cybercrime/〔2021/4/28 確認〕
ZDNet：Microsoft seizes six domains used in COVID-19 phishing operations https://www.zdnet.com/article/microsoft-seizes-six-domains-used-in-covid-19-phishing-operations/〔2021/4/28 確認〕
ITmedia エンタープライズ：新型コロナウイルス便乗のビジネスメール詐欺、Microsoft がドメイン制圧 https://www.itmedia.co.jp/enterprise/articles/2007/09/news060.html〔2021/4/28 確認〕
※ 74 Proofpoint, Inc.：2020 'State of the Phish'：Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical〔2021/4/28 確認〕
ENISA：ENISA Threat Landscape 2020 – Phishing https://www.enisa.europa.eu/publications/phishing〔2021/4/28 確認〕
※ 75 トレンドマイクロ社：法人でのインシデント発生率は約 8 割、2021 年に向けて警戒すべき脅威とは https://blog.trendmicro.co.jp/archives/26357〔2021/4/28 確認〕
※ 76 一般社団法人日本損害保険協会:国内企業のサイバーリスク意識・対策実態調査 2020 https://www.sonpo.or.jp/cyber-hoken/data/2020-01/pdf/cyber_report2020.pdf〔2021/4/28 確認〕
※ 77 Check Point Software Technologies Ltd.：IR Case: The Florentine Banker Group https://research.checkpoint.com/2020/ir-case-the-florentine-banker-group/〔2021/4/28 確認〕
※ 78 Norfund：Norfund has been exposed to a serious case of fraud https://www.norfund.no/norfund-has-been-exposed-to-a-serious-case-of-fraud/〔2021/4/28 確認〕
Bleeping Computer：Scammers steal $10 million from Norway's state investment fund https://www.bleepingcomputer.com/news/security/scammers-steal-10-million-from-norways-state-investment-fund/〔2021/4/28 確認〕
バラクーダネットワークスジャパン株式会社：ほぼ完璧な BEC（ビジネスメール詐欺）によって 1000 万ドルの損害を受けたノルウェーの国有投資ファンド https://www.barracuda.co.jp/wonderfully-done-bec-scam-scores-10-million-from-a-norway-investment-fund/〔2021/4/28 確認〕
※ 79 徳島新聞：コロナ便乗メール詐欺　徳島県内初、県西企業 150 万円被害 https://www.topics.or.jp/articles/-/369213〔2021/4/28 確認〕
※ 80 独立行政法人石油天然ガス・金属鉱物資源機構：海外取引にかかる誤送金について http://www.jogmec.go.jp/news/release/news_01_000158.html〔2021/4/28 確認〕
※ 81 NZ Herald：Far North council scammed out of $100,000 after supplier's email hacked https://www.nzherald.co.nz/northern-advocate/news/far-north-council-scammed-out-of-100000-after-suppliers-email-hacked/7DZSNDDST3BNRLOVZZ6AJMLDWA/〔2021/4/28 確認〕
※ 82 BankInfoSecurity：BEC Scam Costs Trading Firm Virtu Financial $6.9 Million https://www.bankinfosecurity.com/bec-scam-costs-trading-firm-virtu-financial-69-million-a-14804〔2021/4/28 確認〕
※ 83 INTERPOL：Payments stopped, three arrested in medical supplies fraud case https://www.interpol.int/en/News-and-Events/News/2020/Payments-stopped-three-arrested-in-medical-supplies-fraud-case〔2021/4/28 確認〕
※ 84 AP NEWS：Wisconsin Republican Party says hackers stole $2.3 million https://apnews.com/article/wisconsin-republican-party-hackers-stole-641a8174e51077703888e2fa89070e12〔2021/4/28 確認〕
CNET Japan:トランプ氏の選挙資金、2億円超がハッカーに盗まれる--ウィスコンシン州 https://japan.cnet.com/article/35161727/〔2021/4/28 確認〕
※ 85 The Star：Singapore sting international company in Hong Kong hit by US$6.6mil hacking scam https://www.thestar.com.my/tech/tech-news/2020/11/09/singapore-sting-international-company-in-hong-kong-hit-by-us66mil-hacking-scam〔2021/4/28 確認〕
South China Morning Post：Singapore sting: international company in Hong Kong hit by US$6.6 million hacking scam https://www.scmp.com/news/hong-kong/law-and-crime/article/3108831/singapore-sting-international-company-hong-kong-hit〔2021/4/28 確認〕
※ 86 日本経済新聞：JSP、虚偽の第三者指示で資金流出 最大 10 億円 https://www.nikkei.com/article/DGXMZO66375570Y0A111C2DTA000/〔2021/4/28 確認〕
株式会社 JSP：当社欧州グループ会社における資金流出事案に関する調査結果及び再発防止策の策定並びに役員報酬の一部自主返上に関するお知らせ https://www.co-jsp.co.jp/ir/upload_file/m000-/210430_europe.pdf〔2021/5/13 確認〕
※ 87 The Australian Financial Review：Fake Zoom invite cripples Aussie hedge fund with $8m hit https://www.afr.com/companies/financial-services/fake-zoom-invite-cripples-aussie-hedge-fund-with-8m-hit-20201122-p56f9c〔2021/4/28 確認〕
東洋経済オンライン：「なりすましメール」引っかかる人に共通する点 コロナ後を生き抜く https://toyokeizai.net/articles/-/397104?page=2〔2021/4/28 確認〕
※ 88 The Philadelphia Inquirer：Philly hunger relief group Philabundance lost nearly $1 million in cyberattack https://www.inquirer.com/business/philabundance-cybertheft-nearly-1-million-20201201.html〔2021/4/28 確認〕
※ 89 Business Insider：Thieves stole at least $2.7 million from political committees in 2020 cycle. Biden's campaign got hit, too. https://www.businessinsider.com/biden-campaign-money-stolen-pacs-political-committees-theft-embezzlement-2021-2〔2021/4/28 確認〕
The Hill：Federal political committees, campaigns lost $2.7M to theft, fraud in last cycle: report https://thehill.com/homenews/campaign/538448-federal-political-committees-campaigns-lost-27m-to-theft-fraud-in-last〔2021/4/28 確認〕
※ 90 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 https://www.ipa.go.jp/security/announce/20170403-bec.html〔2021/4/28 確認〕
※ 91 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〔2021/4/28 確認〕
※ 92 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（第三報） https://www.ipa.go.jp/security/announce/2020-bec.html〔2021/4/28 確認〕
※ 93 J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan（サイバー情報共有イニシアティブ）の略称。IPA を情報ハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策につなげていく取り組み。
※ 94 IPA：サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））https://www.ipa.go.jp/security/J-CSIP/〔2021/4/28 確認〕
※ 95 IPA：情報セキュリティ白書 2020 https://www.ipa.go.jp/security/publications/hakusyo/2020.html〔2021/4/28 確認〕
※ 96 Agari, Inc.：Cosmic Lynx The Rise of Russian BEC https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-cosmic-lynx.pdf〔2021/4/28 確認〕
※ 97 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2020

年１月～３月］ https://www.ipa.go.jp/files/000081877.pdf〔2021/4/28 確認〕
※ 98 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2020年４月～６月］ https://www.ipa.go.jp/files/000084400.pdf〔2021/4/28 確認〕
※ 99 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2020年10月～12月］ https://www.ipa.go.jp/files/000088288.pdf〔2021/4/28 確認〕
※ 100 JPCERT/CC：ビジネスメール詐欺の実態調査報告書 https://www.jpcert.or.jp/research/BEC-survey.html〔2021/4/28 確認〕
マクニカネットワークス株式会社：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/〔2021/4/28 確認〕
PwC：Business-Email-Compromise-Guide https://github.com/PwC-IR/Business-Email-Compromise-Guide/blob/main/PwC-Business_Email_Compromise-Guide.pdf〔2021/4/28 確認〕
※ 101 一般財団法人日本情報経済社会推進協会（JIPDEC）：なりすまし対策 ～電子証明書を使った本人確認と電子メールにおける送信元認証～ https://www.jipdec.or.jp/library/report/20201120_03.html〔2021/4/28 確認〕
一般財団法人日本情報経済社会推進協会（JIPDEC）：メールのなりすまし対策（S_MIMEとは） https://itc.jipdec.or.jp/jcan/smime-index.html〔2021/4/28 確認〕
迷惑メール対策委員会：電子メールのなりすまし対策 - 送信ドメイン認証でなりすましを防ぐ- https://www.dekyo.or.jp/soudan/data/anti_spam/auth_leaflet.pdf〔2021/4/28 確認〕
※ 102 IC3：Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud-Based Email Services, Costing US Businesses More Than $2 Billion https://www.ic3.gov/media/2020/200406.aspx〔2021/4/28 確認〕
※ 103 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〔2021/4/28 確認〕
Microsoft 社：365 アカウントが Office されたかどうかを確認する方法 https://docs.microsoft.com/ja-jp/office365/troubleshoot/sign-in/determine-account-is-compromised〔2021/4/28 確認〕
TECH+：ビジネスメール詐欺に備えてメールの転送を見直そう https://news.mynavi.jp/itsearch/article/security/5349〔2021/4/28 確認〕
ファイア・アイ株式会社：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〔2021/4/28 確認〕
※ 104 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〔2021/4/28 確認〕
Kaspersky Lab ZAO：DDoS attacks in Q1 2020 https://securelist.com/ddos-attacks-in-q1-2020/96837/〔2021/4/28 確認〕
Kaspersky Lab ZAO：DDoS attacks in Q2 2020 https://securelist.com/ddos-attacks-in-q2-2020/98077/〔2021/4/28 確認〕
※ 105 Kaspersky Lab ZAO：DDoS attacks in Q3 2020 https://securelist.com/ddos-attacks-in-q3-2020/99171/〔2021/4/28 確認〕
※ 106 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。
※ 107 US-CERT：Alert (TA14-017A) UDP-Based Amplification Attacks https://us-cert.cisa.gov/ncas/alerts/TA14-017A〔2021/4/28 確認〕
※ 108 A10 ネットワークス株式会社：2020 年第２四半期の A10 DDoS 脅威インテリジェンスレポート：DDoS 攻撃が増大 https://www.a10networks.co.jp/news/blog/2020Q2Threatintelligencereport.html〔2021/4/28 確認〕
※ 109 A10 ネットワークス株式会社：日本はグローバルと比べ SSDP リフレクション攻撃に悪用されうる端末の割合が多い：最新の A10 国内脅威インテリジェンスレポート https://www.a10networks.co.jp/news/blog/Japanthreatreport1109.html〔2021/4/28 確認〕
※ 110 Amazon Web Services, Inc.：Threat Landscape Report – Q1 2020 https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf〔2021/4/28 確認〕
※ 111 アカマイ・テクノロジーズ合同会社：パケット／秒ベースで史上最大規模の DDOS 攻撃を AKAMAI が緩和 https://blogs.akamai.com/jp/2020/07/largest-ever-recorded-packet-per-secondbased-ddos-attack-mitigated-by-akamai.html〔2021/4/28 確認〕
※ 112 JPCERT/CC：DDoS 攻撃を示唆して仮想通貨による送金を要求する脅迫行為（DDoS 脅迫）について https://www.jpcert.or.jp/newsflash/2020090701.html〔2021/4/28 確認〕
※ 113 Bloomberg：ニュージーランド、危機管理計画を発動ー株式市場へのサイバー攻撃で https://www.bloomberg.co.jp/news/articles/2020-08-28/QFR9WPT0G1KZ〔2021/4/28 確認〕
※ 114 ZDNnet：DDoS extortionists target NZX, Moneygram, Braintree, and other financial services https://www.zdnet.com/article/ddos-extortionists-target-nzx-moneygram-braintree-and-other-financial-services/〔2021/4/28 確認〕
※ 115 Bitdefender：New dark_nexus IoT Botnet Puts Others to Shame https://labs.bitdefender.com/2020/04/new-dark_nexus-iot-botnet-puts-others-to-shame/〔2021/4/28 確認〕
※ 116 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。
※ 117 パス・トラバーサル：ファイルパス名の名前解決において特殊文字の処理に不備があり、本来アクセス権限のないディレクトリ等にアクセスできてしまう脆弱性。別名、ディレクトリ・トラバーサル。
※ 118 Fortinet, Inc.：FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests https://www.fortiguard.com/psirt/FG-IR-18-384〔2021/4/28 確認〕
※ 119 JPCERT/CC：Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について https://www.jpcert.or.jp/newsflash/2020112701.html〔2021/4/28 確認〕
※ 120 Pulse Secure, LLC.：SA44101 - 2019-04: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101〔2021/4/28 確認〕
※ 121 JPCERT/CC：Pulse Connect Secure の脆弱性を狙った攻撃事案 https://blogs.jpcert.or.jp/ja/2020/03/pulse-connect-secure.html〔2021/4/28 確認〕
※ 122 日経 XTECH：パッチ未適用のパルスセキュア社 VPN、日本企業 46 社の IP アドレスがさらされる https://xtech.nikkei.com/atcl/nxt/news/18/08605/〔2021/4/28 確認〕
※ 123 Microsoft 社：Windows SMBv3 クライアント / サーバーのリモートでコードが実行される脆弱性 https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2020-0796〔2021/4/28 確認〕
※ 124 Microsoft 社：Windows SMBv3 クライアント / サーバーの情報漏えいの脆弱性 https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2020-1206〔2021/4/28 確認〕
※ 125 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。
※ 126 JSOF Ltd.：Ripple20 https://www.jsof-tech.com/disclosures/ripple20/〔2021/4/28 確認〕
※ 127 https://jvndb.jvn.jp/〔2021/4/28 確認〕
※ 128 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〔2021/4/28 確認〕
※ 129 キヤノンマーケティングジャパン株式会社：2019 年上半期マルウェアレポート https://eset-info.canon-its.jp/files/user/malware_info/images/ranking/pdf/MalwareReport_2019FirstHalf.pdf〔2021/4/28 確認〕
※ 130 IPA：「Emotet」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〔2021/4/28 確認〕
※ 131 JPCERT/CC：マルウエア Emotet の感染に繋がるメールの配布活動の再開について（追加情報） https://www.jpcert.or.jp/newsflash/2020072001.html〔2021/4/28 確認〕
※ 132 キヤノンマーケティングジャパン株式会社：2019 年 10 月マルウェアレポート https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1910.html〔2021/4/28 確認〕
※ 133 トレンドマイクロ社：サイバー犯罪の根本解決：EUROPOL による EMOTET テイクダウン https://blog.trendmicro.co.jp/archives/27132〔2021/4/28 確認〕
※ 134 Europol：World's most dangerous malware EMOTET disrupted through global action https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action〔2021/4/28 確認〕
※ 135 Malwarebytes Inc.：Cleaning up after Emotet: the law enforcement file https://blog.malwarebytes.com/threat-analysis/2021/01/cleaning-up-after-emotet-the-law-enforcement-file/〔2021/4/28 確認〕

TECH+：Malwarebytes、マルウェア「Emotet」の削除を開始　https://news.mynavi.jp/article/20210428-1879994/〔2021/4/28 確認〕
※ 136 総務省：マルウェアに感染している機器の利用者に対する注意喚起の実施　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00095.html〔2021/4/28 確認〕
※ 137 Mal Eats：IcedID の感染につながる日本向けキャンペーンの分析　https://mal-eats.net/2020/11/12/analysis_of_the-_icedid_campaign_for_japan/〔2021/4/28 確認〕
※ 138 Juniper Networks, Inc.：COVID-19 and FMLA Campaigns used to install new IcedID banking malware　https://blogs.juniper.net/en-us/threat-research/covid-19-and-fmla-campaigns-used-to-install-new-icedid-banking-malware〔2021/4/28 確認〕
※ 139 ProofPoint, Inc.：ZLoader Loads Again: New ZLoader Variant Returns　https://www.proofpoint.com/us/blog/threat-insight/zloader-loads-again-new-zloader-variant-returns〔2021/4/28 確認〕
※ 140 株式会社ラック：分析レポート：Emotet の裏で動くバンキングマルウェア「Zloader」に注意　https://www.lac.co.jp/lacwatch/people/20201106_002321.html〔2021/4/28 確認〕
※ 141 Malwarebytes Inc.：The "Silent Night" Zloader/Zbot　https://resources.malwarebytes.com/files/2020/05/The-Silent-Night-Zloader-Zbot_Final.pdf〔2021/4/28 確認〕
※ 142 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〔2021/4/28 確認〕
※ 143 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〔2021/4/28 確認〕
※ 144 トレンドマイクロ社：【注意喚起】トレンドマイクロのアンケートメールなどに偽装した偽メールに注意　https://www.is702.jp/news/3736/partner/12_t/〔2021/4/28 確認〕
※ 145 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2020年7月～9月］　https://www.ipa.go.jp/files/000086549.pdf〔2021/4/28 確認〕
※ 146 Lastline, Inc.：Evolution of Excel 4.0 Macro Weaponization　https://www.lastline.com/labsblog/evolution-of-excel-4-0-macro-weaponization/〔2021/4/28 確認〕
※ 147 サイバーリーズン・ジャパン株式会社：64 ビットの環境で Excel 4.0 のマクロを使用する攻撃　https://www.cybereason.co.jp/blog/cyberattack/3598/〔2021/4/28 確認〕
※ 148 IPA：安心相談窓口だより　iPhone に突然表示される不審なカレンダー通知に注意!　https://www.ipa.go.jp/security/anshin/mgdayori20200330.html〔2021/5/12 確認〕
※ 149 IPA：安心相談窓口だより　Facebook のメッセンジャーに届く動画に注意!　https://www.ipa.go.jp/security/anshin/mgdayori20200819.html〔2021/5/12 確認〕
※ 150 フィッシング対策協議会：2021/01 フィッシング報告状況　https://www.antiphishing.jp/report/monthly/202101.html〔2021/5/12 確認〕
※ 151 トレンドマイクロ社：【注意喚起】インスタグラムのなりすましアカウントに注意、不特定多数の法人アカウントで被害発生中　https://is702.jp/news/3801/〔2021/5/12 確認〕
※ 152 株式会社ユニクロ：ユニクロ公式インスタグラムを模倣した偽アカウントにご注意ください　https://faq.uniqlo.com/articles/FAQ/100006456〔2021/6/15 確認〕
※ 153 株式会社そごう・西武：【重要なお知らせ】弊社公式 SNS の「偽アカウント」にご注意ください　https://www.sogo-seibu.jp/ss/topics/page/instagram-info.html〔2021/6/15 確認〕
※ 154 https://www.antiphishing.jp/news/alert/kyufukin_20201015.html〔2021/5/12 確認〕
※ 155 独立行政法人国民生活センター：新型コロナウイルス感染症関連　http://www.kokusen.go.jp/soudan_now/data/coronavirus.html〔2021/5/12 確認〕
※ 156 総務省：特別定額給付金（新型コロナウイルス感染症緊急経済対策関連）　https://www.soumu.go.jp/menu_seisaku/gyoumukanri_sonota/covid-19/kyufukin.html〔2021/5/12 確認〕
※ 157 https://www.caa.go.jp/policies/policy/consumer_policy/assets/consumer_policy_cms102_210209_01.pdf〔2021/5/12 確認〕
※ 158 総務省:令和2年版 情報通信白書　第5章　第2節　ICT サービスの利用動向　https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/n5200000.pdf〔2021/5/12 確認〕
※ 159 IPA：安心相談窓口だより　宅配便業者をかたる偽ショートメッセージに引き続き注意!　https://www.ipa.go.jp/security/anshin/mgdayori20200220.html〔2021/5/12 確認〕
※ 160 独立行政法人国民生活センター:宅配便業者を装った「不在通知」の偽 SMS に注意しましょう― URL にはアクセスしない、ID・パスワードを入力しない！―　http://www.kokusen.go.jp/news/data/n-20201126_2.html〔2021/5/12 確認〕
※ 161 フィッシング対策協議会：Amazon をかたるフィッシング（2020/11/27）　https://www.antiphishing.jp/news/alert/amazon_20201127.html〔2021/5/12 確認〕
※ 162 楽天グループ株式会社：【ご注意ください】楽天市場を装った不審な SMS（商品発送通知を装った SMS）（2020 年 11 月 19 日更新）　https://ichiba.faq.rakuten.net/detail/000010078〔2021/5/12 確認〕
※ 163 読売新聞オンライン：ネット不正送金急増　4か月被害144件 過去の年間最多上回る　https://www.yomiuri.co.jp/local/aichi/news/20200522-OYTNT50103/〔2021/5/12 確認〕
※ 164 JC3：インターネットバンキングの不正送金の被害に注意　https://www.jc3.or.jp/topics/banking/phishing.html〔2021/5/12 確認〕
※ 165 フィッシング対策協議会：2020/12 フィッシング報告状況　https://www.antiphishing.jp/report/monthly/202012.html〔2021/5/12 確認〕
※ 166 沖縄タイムス：「異常ログインの可能性あり」銀行を装いショートメール　不正送金 1530 万円を確認　https://www.okinawatimes.co.jp/articles/gallery/676556?ph=1〔2021/5/12 確認〕
※ 167 IPA：安心相談窓口だより　遠隔操作を他人に安易に許可しないで!　https://www.ipa.go.jp/security/anshin/mgdayori20201125.html〔2021/5/12 確認〕
※ 168 消費者庁:「Microsoft」のロゴを用いて信用させ、パソコンのセキュリティ対策のサポート料などと称して多額の金銭を支払わせる事業者に関する注意喚起　https://www.caa.go.jp/notice/assets/consumer_policy_cms103_210219_1.pdf〔2021/5/12 確認〕
※ 169 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〔2021/5/12 確認〕
※ 170 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/〔2021/5/12 確認〕
※ 171 IPA：安心相談窓口だより　スマートフォンで偽のセキュリティ警告からアプリのインストールへ誘導する手口に注意　https://www.ipa.go.jp/security/anshin/mgdayori20190918.html〔2021/5/12 確認〕
※ 172 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。
※ 173 https://www.tsr-net.co.jp/news/analysis/20210115_01.html〔2021/5/12 確認〕
※ 174 任天堂株式会社：「ニンテンドーネットワーク ID」に対する不正ログイン発生のご報告と「ニンテンドーアカウント」を安全にご利用いただくためのお願い　https://www.nintendo.co.jp/support/information/2020/0424.html〔2021/5/12 確認〕
ScanNetSecurity: 続報：ニンテンドーネットワーク ID 不正ログイン、新たに14万件判明（任天堂）　https://scan.netsecurity.ne.jp/article/2020/06/11/44194.html〔2021/5/12 確認〕
※ 175 NNID はニンテンドーのゲーム機でインターネットを利用するためのアカウントである。またニンテンドーアカウントはゲーム機以外のニンテンドーの機器を利用するためのアカウントである。
※ 176 株式会社カプコン：不正アクセスに関する調査結果のご報告【第4報】　https://www.capcom.co.jp/ir/news/html/210413.html〔2021/5/12 確認〕
Security NEXT：カプコンへの不正アクセス、侵入経路は予備に残した以前の VPN 機器　https://www.security-next.com/125237〔2021/5/12 確認〕
※ 177 Classi 株式会社：ご報告とご注意のお願い　https://corp.classi.jp/news/2154/〔2021/5/12 確認〕
※ 178 ナカバヤシ株式会社：弊社が運営する「フエルモール」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ【続報】https://www.nakabayashi.co.jp/news/2020/info/715〔2021/5/12 確認〕
※ 179 株式会社リジョブ：不正アクセスによる個人情報の流出について　https://rejob.co.jp/topics/2020041910295〔2021/5/12 確認〕
※ 180 株式会社キタムラ：「カメラのキタムラ ネットショップ」への"なりすまし"による不正アクセス発生について　https://www.kitamura.jp/topics/2020/20200615_01.html〔2021/5/12 確認〕
日本経済新聞：「カメラのキタムラ」個人情報 40 万件が閲覧された恐れ　https://www.nikkei.com/article/DGXMZO60440520X10C20A6000000/〔2021/5/12 確認〕
※ 181 株式会社キッチハイク：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（第四報・最終）　https://kitchhike.jp/newsblog/2020/7/24〔2021/5/12 確認〕
※ 182 QUOINE 株式会社：当社利用のドメイン登録サービスにおける不

正アクセスについて（最終報） https://blog.liquid.com/ja/20210120-important-notice-final〔2021/5/12 確認〕
※ 183 Peatix Inc.：弊社が運営する「Peatix(http://peatix.com/)」への不正アクセス事象に関する第三者調査機関による調査結果のご報告と今後の対応について https://announcement.peatix.com/20201216_ja.pdf〔2021/5/12 確認〕
※ 184 東建コーポレーション株式会社：不正アクセスによる個人情報流出について（第二報） https://www.token.co.jp/corp/information/about_unauthorized/〔2021/5/12 確認〕
※ 185 PayPay 株式会社：当社管理サーバーのアクセス履歴について - PayPay からのお知らせ https://paypay.ne.jp/notice/20201207/02/〔2021/5/12 確認〕
※ 186 株式会社駅レンタカーシステム：不正アクセスによるお客さまメールアドレス流出のお知らせとお詫びについて https://www.ekiren.co.jp/info/20201218_pressrelease.pdf〔2021/5/12 確認〕
※ 187 株式会社 TIMERS：不正アクセスによる情報流出に関するお詫びとお知らせ（第三報・最終） https://help.famm.us/hc/ja/articles/360054657071-%E4%B8%8D%E6%AD%A3%E3%82%A2%E3%82%AF%E3%82%BB%E3%82%B9%E3%81%AB%E3%82%88%E3%82%8B%E6%83%85%E5%A0%B1%E6%B5%81%E5%87%BA%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E3%81%8A%E8%A9%AB%E3%81%B3%E3%81%A8%E3%81%8A%E7%9F%A5%E3%82%89%E3%81%9B-%E7%AC%AC%E４%B８%８９%E５%A０%B１-%E６%９C%８０%E７%B５%８２-〔2021/5/12 確認〕
※ 188 株式会社マイナビ：「マイナビ転職」への不正ログイン発生に関するお詫びとお願い https://www.mynavi.jp/topics/post_29797.html〔2021/5/12 確認〕
※ 189 ANA：SITA 社システムへの不正アクセスによる ANA マイレージクラブ会員情報の漏洩について https://www.ana.co.jp/ja/jp/amc/news/info/2021/210306_memberinfo.html〔2021/5/12 確認〕
JAL：SITA 社セキュリティ事故による JAL マイレージバンク会員情報の漏洩について https://www.jal.co.jp/jp/ja/info/2021/other/210305/〔2021/5/12 確認〕
※ 190 株式会社アーバンリサーチ：アーバンリサーチ公式オンラインストアからの個人情報流出に関するお詫びとお願い https://www.urban-research.co.jp/news/company/2021/03/info210310/〔2021/5/12 確認〕
※ 191 https://privacymark.jp/system/reference/pdf/2019JikoHoukoku_201109.pdf〔2021/5/12 確認〕
※ 192 日本経済新聞：みずほ総研、顧客情報最大 250 万件紛失 https://www.nikkei.com/article/DGXMZO61780350R20C20A7EE9000/〔2021/5/12 確認〕
サイバーセキュリティ .com：250 万件の個人情報記録した媒体を誤廃棄 | みずほ総合研究所株式会社 https://cybersecurity-jp.com/news/37854〔2021/5/12 確認〕
※ 193 国土交通省神戸運輸監理部：行政文書の誤廃棄・紛失について https://wwwtb.mlit.go.jp/kobe/content/000161825.pdf〔2021/5/12 確認〕
※ 194 ヤフー株式会社：Yahoo! JAPAN ID の登録情報システム不具合に関するお詫びと不具合解消に関するお知らせ https://about.yahoo.co.jp/pr/release/2020/08/06b/〔2021/5/12 確認〕
※ 195 楽天株式会社：クラウド型営業管理システムへの社外の第三者によるアクセスについて https://corp.rakuten.co.jp/news/update/2020/1225_01.html〔2021/5/12 確認〕
※ 196 PayPay 株式会社：当社管理サーバーのアクセス履歴について - PayPay からのお知らせ https://paypay.ne.jp/notice/20201207/02/〔2021/5/12 確認〕
イオン株式会社：お問い合わせフォームへの社外の第三者によるアクセスについて https://www.aeon.info/wp-content/uploads/news/important/pdf/2021/01/210125R_1_1.pdf〔2021/5/14 確認〕
株式会社イオン銀行：「来店予約・オンライン相談サービス」システムへの第三者による不正アクセスについて https://www.aeonbank.co.jp/news/2021/0222_01.html〔2021/5/14 確認〕
独立行政法人国際観光振興機構：クラウド型情報管理システムへの第三者によるアクセスの可能性について https://www.jnto.go.jp/jpn/news/20210121.pdf〔2021/5/14 確認〕
※ 197 株式会社両備システムズ：クラウド型システムへの第三者からのアクセスについて（更新） https://www.ryobi.co.jp/news/notification20210212〔2021/5/14 確認〕
※ 198 セールスフォース社：【お知らせ】当社一部製品をご利用のお客様におけるゲストユーザに対する共有に関する設定について（セースルフォース・ドットコム） https://www.salesforce.com/jp/company/news-press/press-releases/2020/12/201225/〔2021/5/12 確認〕
セールスフォース社：ゲストユーザセキュリティポリシーのベストプラクティス https://help.salesforce.com/articleView?id=000355945&language=ja&mode=1&type=1〔2021/5/14 確認〕
セールスフォース社:コミュニティ、Salesforce サイト（旧 Force.com サイト）におけるゲストユーザの利用について https://help.salesforce.com/articleView?id=000356139&type=1&mode=1〔2021/5/14 確認〕
※ 199 NISC：Salesforce の製品の設定不備による意図しない情報が外部から参照される可能性について https://www.nisc.go.jp/active/infra/pdf/salesforce20210129.pdf〔2021/5/14 確認〕
※ 200 ソフトバンク株式会社：楽天モバイルへ転職した元社員の逮捕について https://www.softbank.jp/corp/news/press/sbkk/2021/20210112_01/〔2021/5/12 確認〕
※ 201 ソフトバンク株式会社：訪問販売代理店でのお客さま情報の不正取得について https://www.softbank.jp/corp/news/press/sbkk/2021/20210304_01/〔2021/5/12 確認〕
※ 202 ITmedia NEWS:NEC もソースコード流出を確認、GitHub で三井住友銀、NTT データに続き https://www.itmedia.co.jp/news/articles/2102/01/news118.html〔2021/5/12 確認〕
※ 203 LINE 株式会社：LINE における個人情報の取り扱いに関連する主な予定および取り組みについて https://linecorp.com/ja/pr/news/ja/2021/3680〔2021/5/12 確認〕
※ 204 JPCERT/CC、IPA：Japan Vulnerability Notes（JVN） https://jvn.jp/〔2021/4/28 確認〕
※ 205 NIST：National Vulnerability Database（NVD） https://nvd.nist.gov/〔2021/4/28 確認〕
※ 206 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。
※ 207 IPA：共通脆弱性識別子 CVE 概説 https://www.ipa.go.jp/security/vuln/CVE.html〔2021/4/28 確認〕
※ 208 The MITRE Corporation：CVE Numbering Authorities https://cve.mitre.org/cve/cna.html〔2021/4/28 確認〕
※ 209 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。
※ 210 The MITRE Corporation：CVE Adds 7 New CVE Numbering Authorities (CNAs) https://cve.mitre.org/news/archives/2016/news.html〔2021/4/28 確認〕
※ 211 The MITRE Corporation：Coalfire Labs Added as CVE Numbering Authority (CNA) https://cve.mitre.org/news/archives/2020/news.html〔2021/4/28 確認〕
※ 212 2014 年 9 月に「複数の Android アプリに SSL 証明書を適切に検証しない脆弱性」が公表されたことに伴い、1,200 件を超える Android アプリの脆弱性対策情報が JVN iPedia に登録された。
※ 213 IPA：共通脆弱性タイプ一覧 CWE 概説 https://www.ipa.go.jp/security/vuln/CWE.html〔2021/4/28 確認〕
※ 214 IPA：共通脆弱性評価システム CVSS 概説 https://www.ipa.go.jp/security/vuln/CVSS.html〔2021/4/28 確認〕
※ 215 JPCERT/CC：セキュアコーディング https://www.jpcert.or.jp/securecoding/〔2021/4/28 確認〕
※ 216 Microsoft 社：Netlogon の特権の昇格の脆弱性 https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2020-1472〔2021/4/28 確認〕
※ 217 Microsoft 社：Attacks exploiting Netlogon vulnerability (CVE-2020-1472) https://msrc-blog.microsoft.com/2020/10/29/attacks-exploiting-netlogon-vulnerability-cve-2020-1472/〔2021/4/28 確認〕
※ 218 NHK：リモート接続ねらうサイバー攻撃が急増 テレワーク増加で https://www3.nhk.or.jp/news/html/20201112/k10012708711000.html〔2021/4/28 確認〕
※ 219 JPCERT/CC：複数の SSL VPN 製品の脆弱性に関する注意喚起 https://www.jpcert.or.jp/at/2019/at190033.html〔2021/4/28 確認〕
JPCERT/CC：Palo Alto Networks 製品の脆弱性（CVE-2020-2021）について https://www.jpcert.or.jp/newsflash/2020063001.html〔2021/4/28 確認〕
JPCERT/CC：Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性（CVE-2018-13379）の影響を受けるホストに関する情報の公開について https://www.jpcert.or.jp/newsflash/2020112701.html〔2021/4/28 確認〕
JPCERT/CC：Pulse Connect Secure の脆弱性への対策や侵害有無などの確認を https://www.jpcert.or.jp/newsflash/2020041701.html〔2021/4/28 確認〕
※ 220 IPA：Zoom の脆弱性対策について https://www.ipa.go.jp/security/ciadr/vul/alert20200403.html〔2021/4/28 確認〕

※ 221 株式会社カスペルスキー：コロナ禍の1年：リモートデスクトッププロトコルへの攻撃が高い水準を維持　https://blog.kaspersky.co.jp/attacks-on-rdp-during-pandemic-year/30354/〔2021/4/28 確認〕
※ 222 NISC：Fortinet 製 VPN の脆弱性 (CVE-2018-13379) に関する重要インフラ事業者等についての注意喚起の発出について　https://www.nisc.go.jp/active/infra/pdf/fortinet20201203.pdf〔2021/4/28 確認〕
JPCERT/CC：Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について　https://www.jpcert.or.jp/newsflash/2020112701.html〔2021/4/28 確認〕
※ 223 IPA：脆弱性関連情報の届出受付　https://www.ipa.go.jp/security/vuln/report/index.html〔2021/4/28 確認〕
※ 224 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。
※ 225 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〔2021/4/28 確認〕
※ 226 LINE 株式会社：LINE が CVE Numbering Authority（CNA）の一員に　https://linecorp.com/ja/security/article/355〔2021/4/28 確認〕
※ 227 三菱電機株式会社：製品セキュリティーへの取組　https://www.mitsubishielectric.co.jp/psirt/〔2021/4/28 確認〕
※ 228 JPCERT/CC: CNA 活動レポート ～日本の 2 組織が新たに CNA に参加～　https://blogs.jpcert.or.jp/ja/2020/12/cna-2cna.html〔2021/4/28 確認〕
※ 229 IPA：SQL インジェクション攻撃に関する注意喚起　https://www.ipa.go.jp/security/vuln/documents/2008/200805_SQLinjection.html〔2021/4/28 確認〕
※ 230 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〔2021/4/28 確認〕
※ 231 https://www.ipa.go.jp/files/000017319.pdf〔2021/4/28 確認〕
※ 232 https://www.ipa.go.jp/files/000017320.pdf〔2021/4/28 確認〕
※ 233 https://www.ipa.go.jp/files/000017316.pdf〔2021/4/28 確認〕