情報セキュリティ白書

序章

2019年度の情報セキュリティの概況

2019 年度に起きた情報セキュリティに関する主なインシデントや実施された政策・制度について概況を述べる。

2019 年度も、多数の情報流出事案が発生した。国外では、2019 年 7 月に米国の大手金融会社の 1 億人を超える顧客情報が、9 月にはエクアドルで国民ほぼ全員を含む 2,000 万人分の個人情報が流出した。国内でも、EC サイト等からクレジットカード情報や銀行口座情報等を含む個人情報が流出した。7 月に開始したスマホ決済サービスではアカウントが不正利用され、800 人を超える被害が発生し、9 月末にはサービス自体が廃止となった。また、2020 年 1 月には複数の防衛関連企業から不正アクセスによる情報流出が公表された。

金融機関をかたるフィッシングメールによるものとされる不正送金被害は 9 月から急増し、警察庁等が注意喚起を実施した。Emotet ウイルスの感染による情報窃取等を狙う攻撃が 2019 年 10 月から急増し、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）等が注意喚起を実施した。更に、企業や自治体のサービスに用いられるクラウドプラットフォームの障害による大規模なシステム停止が発生し、多くのビジネスや市民サービスに影響を与えた。

攻撃の基本的な手口については 2018 年度から目立った変化はなく、脆弱性の解消や適切なパスワード管理、不審なメールへの対処等、既知の対策で防げたはずの被害が多いが、対策が難しいゼロデイ攻撃による情報流出も見られた。また、内部不正や不適切なデータ管理ポリシーによる情報流出被害として、2019 年 12 月に情報機器リユース会社から廃棄予定の HDD が売却された事案、2019 年 8 月に就職情報サイト運営会社が「内定辞退率」等のデータを同意なく第三者に提供した事案等が発生した。

政策面については、2019 年度には日米欧で重要インフラやサプライチェーンのセキュリティ、個人情報保護に関する規則・情報共有等の運用が本格的に展開された。

日本国内では、基本政策である「サイバーセキュリティ戦略」に基づき、2019 年 5 月、内閣サイバーセキュリティセンター（NISC）から「サイバーセキュリティ 2019」が公開された。総務省の「NOTICE」プロジェクトでは、脆弱性の残る IoT 機器の利用者への注意喚起事業が開始された。経済産業省の「サイバーセキュリティお助け隊」プロジェクトでは、中小企業の努力だけでは実現が困難なセキュリティ対策支援が実施された。2020 年 3 月には「政府調達のためのセキュリティ評価制度（ISMAP）」のパブリックコメントが実施され、政府調達におけるクラウドセキュリティの確保が図られた。東京 2020 オリンピック・パラリンピック競技大会に向けては、重要インフラのリスク分析や情報共有、サイバー攻撃に備えた分野横断的演習、顔認証によるセキュリティチェックシステムの開発等が行われた。しかし、2020 年 2 月以降の新型コロナウイルス感染症の拡大により大会は 2021 年に延期となり、上記の施策は継続となった。

国外では、安全保障やサプライチェーンに関わるセキュリティの動向が注目された。まず米国は、サプライチェーンのセキュリティ政策として中国を想定した海外ベンダの排除姿勢を強めた。具体的には 2019 年 5 月、中国ベンダほか関連企業が輸出規制対象となり、8 月には中国ベンダ 5 社、及び 5 社と取引関係にある事業者の政府調達が禁止となった。サイバー防衛については、議会が 2020 年 3 月に敵対勢力への法執行や制裁等、サイバー攻撃以外の抑止的活動を強化することを求めた。

GDPR（一般データ保護規則）の本格運用が始まった欧州では、2019 年 7 月、航空会社、宿泊事業者に高額の制裁金が科せられた。中国との関係に関しては、EU は加盟国に 5G ネットワーク技術のセキュリティリスク評価を求め、リスクに応じた調達を行うことを許容したため、2019 年 12 月のドイツのモバイルネットワーク調達では、一部を中国ベンダと契約することが確定した。しかし、2020 年 1 月の新型コロナウイルス感染拡大以降、米国・欧州ともに中国の情報開示の仕方に、次いで香港に対する統治方針に不信感を抱き、サプライチェーンの中国への依存体質を大幅に見直すこととなった。更に、新型コロナウイルスに関する詐欺メール、偽情報が蔓延し、喫緊のセキュリティ課題となった。

当然ながら、日本はこうした米欧の動きに無関係ではいられない。サプライチェーンのセキュリティ、新型コロナウイルス関連のサイバー攻撃や偽情報、新しい働き方に対するセキュリティ等について、関係各国と連携して対処していく必要がある。

2019 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
2019 年　4 月		経済産業省、「サイバー・フィジカル・セキュリティ対策フレームワーク　Version1.0」を策定(2.1.1) NISC「小さな中小企業と NPO 向け情報セキュリティハンドブック」公開(2.4.2)
5 月	EC サイトのアカウント 46 万 1,000 件に不正アクセス(1.2.7) アンケートモニターサービスの登録アカウント 77 万 74 件に不正アクセス(1.2.7)	NISC「サイバーセキュリティ 2019」公開(2.1.1) 米国 で中国ベンダほか関連企業が輸出規制対象に(2.2.2)
6 月		G20 大阪サミット開催、信頼性のあるデータの自由な流通の概念を提唱(2.2.1) 経済産業省「サイバーセキュリティお助け隊」開始(2.4.2) 総務省・NICT「NOTICE」における注意喚起事業を開始(2.1.1、3.2.2)
7 月	米国の大手金融会社のクラウドから大量の個人情報漏えい(1.1.1、3.4.1) 福岡県警察、警視庁等、海賊版サイト運営者らを著作権法違反で検挙(2.1.4)	英国 ICO が航空会社及び宿泊事業者に GDPR 違反で巨額の制裁金(2.2.3)
8 月	スマホ決済サービスが不正アクセス被害を受けサービス廃止を発表(1.1.2) 就職情報サイト運営会社が「内定辞退率」データを販売(1.2.7) クラウドプラットフォームサービス大手が大規模障害で多数のサービスに影響(3.4.1)	米国で国防権限法 2019 が発効、中国の IT ベンダ・通信機器ベンダ 5 社の政府調達が禁止に(2.2.2) 東京 2020 組織委員会が AI を活用した顔認証技術導入を発表(3.3.3)
9 月	エクアドル国民約 2,000 万人分の個人情報流出(1.1.1) 大手新聞社米子会社、香港に 32 億円流出の詐欺被害(1.2.2)	経産省と IPA、インド太平洋地域向け日米サイバー演習を実施(2.1.1、2.2.1) ラグビーワールドカップ開催(1.2.3)
10 月	フィッシングの月間報告が 8,000 件を超え過去最多に(1.1.2、1.2.6)	EU 加盟国、5G セキュリティのリスク評価結果を報告(2.2.3) 重要インフラ専門調査会「『重要インフラの情報セキュリティ対策に係る第 4 次行動計画』に基づく情報共有の手引書(試行版)」策定(2.1.1)
11 月	JPCERT/CC、Emotet の感染に関する注意喚起(1.2.5)	NISC が東京 2020 オリンピック・パラリンピック競技大会を想定した「分野横断的演習」を実施(2.1.1)
12 月	情報機器リユース会社において廃棄予定 HDD の流出発覚(1.2.7) 自治体向けクラウドにおけるシステム障害でサービス停止等の影響(3.4.1) 日本への Emotet のばらまき型メールによる攻撃急増(1.2.5)	ドイツのモバイル通信ネットワーク構築で Huawei 社との契約が確定(2.2.3)
2020 年　1 月	国内防衛関連企業が不正アクセスによる情報流出を公表(1.2.1、1.2.7)	米国国防総省、サイバーセキュリティ成熟度モデル認証(CMMC)の初版を公開(2.2.2)
2 月	新型コロナウイルスに関連した内容の SMS からフィッシングサイトに誘導する手口発生(1.2.6)	英国、正式に EU を離脱、新しい自由貿易交渉開始(2.2.3)
3 月		個人情報保護法改正案閣議決定(1.2.7、2.7.4) 内閣府・経済産業省・総務省「政府調達のためのセキュリティ評価制度(ISMAP)」パブコメ開始(2.1.2、3.4.2) 米国国土安全保障省、新型コロナウイルス関連詐欺メール、詐欺サイトに注意喚起(2.2.2)

※ 2019 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、DDoS 攻撃、Web 改ざん等の攻撃や被害は通年で発生している。表中の数字は本白書中に掲載している項目番号である。特に注目されたもののみを挙げた。他のインシデントや手口と対策、及び政策・イベント等については本文を参照していただきたい。

第1章
情報セキュリティインシデント・脆弱性の現状と対策

2019年も引き続き脆弱性への攻撃や人を欺く巧妙な手口により、大量の情報漏えい、金銭被害等が発生している。従来の対策の継続に加えて、新しい技術・サービスに潜むリスクに注意し、組織を越えた情報共有や協力が求められている。

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 2019年度に観測されたインシデント状況

本節では、2019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

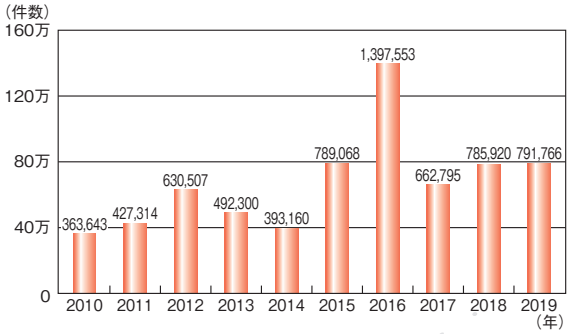
世界における情報セキュリティインシデントの発生状況について、公開されている以下の情報セキュリティ関連の報告書を参照し概説する。

- International Business Machines Corporation（以下、IBM社）：IBM X-Force 脅威インテリジェンス・インデックス 2020[※1]
- Verizon Communications Inc.（以下、Verizon社）：2020 Data Breach Investigations Report[※2]
- トレンドマイクロ株式会社（以下、トレンドマイクロ社）：2019年年間セキュリティラウンドアップ[※3]
- Anti-Phishing Working Group, Inc.（以下、APWG）：Phishing Activity Trends Report[※4]

(1) フィッシングとビジネスメール詐欺の傾向

APWGによると、2019年のフィッシングサイトの総数は約79万2,000件で、2018年と比較して0.7%の増加となり、依然高いレベルの脅威が継続している（図1-1-1）。なお、この件数はカスタマイズされたURL[※5]を含まないサイト固有のURLの件数である。実際のフィッシングメール内に書かれるURLのパターンは図1-1-1の件数よりも更に多くなる。中には巧妙なURLも多数あると考えられ、正しいWebサイトとの区別はますます難しくなると考えられる。

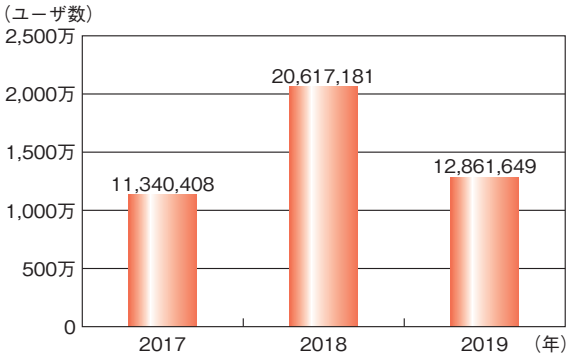
ターゲットとなる業種は、2019年1年間では「SaaS/Webmail」が33.9%、「ペイメント（支払い）」が22.4%、「金融機関」が18.2%と続いている。上位の順位は通年で変動していないが、2019年上期には合わせて6割を占めていた「SaaS/Webmail」「ペイメント（支払い）」をターゲットとしたフィッシングサイト数の割合は2019年下期には5割まで減少し、代わりに「金融機関」「eコマース」「ソーシャルメディア」をターゲットとしたフィッシングサイト数の割合が微増している。フィッシングの攻撃対象が少数の業種に集中しなくなっていることから、今後フィッシングの手口や、詐取した情報の悪用の方法が変化していく可能性に警戒が必要である。



■図1-1-1　世界における届け出されたフィッシングサイト件数
（出典）APWG「Phishing Activity Trends Report」（2010～2019年）を基にIPAが作成

一方、トレンドマイクロ社の調査によれば、実際にメール内のリンクをクリックしてフィッシングサイトに誘導されるところを未然にブロックされたユーザの数は、2019年は約1,286万2,000であり、2018年と比較して約4割減少し、2017年と比較して約13%増となった（図1-1-2）。誘導先のサイトをトレンドマイクロ社が分析した結果、URLにOffice 365やOutlookの文字列を含むフィッシングサイトの件数が2018年の約2倍の約13万2,000件となって

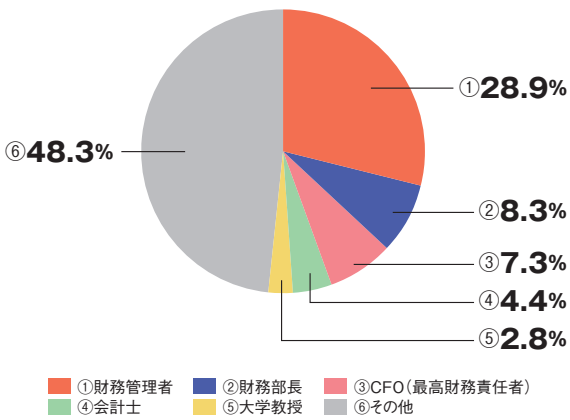
いた（フィッシングについては「1.2.6 個人をターゲットにした騙しの手口」参照）。



■図 1-1-2　フィッシング関連 URL へのアクセスがブロックされたユーザ数推移（全世界）
（出典）トレンドマイクロ社「2019 年年間セキュリティラウンドアップ」及び「2018 年年間セキュリティラウンドアップ※6」を基に IPA が編集

ビジネスメール詐欺（BEC：Business Email Compromise）に関して、米国連邦捜査局（FBI：Federal Bureau of Investigation）の統計※7によると、2019 年の米国国内の被害額は 17 億 7,654 万 9,688 米ドル（約 1,901 億円）となっており、最も被害金額の大きいサイバー犯罪と位置付けられている。

また、トレンドマイクロ社の調査によれば、ビジネスメール詐欺の関連メールは 2019 年も増え続け、前年比で約 5% 増の約 1 万 3,000 件となっており、2019 年にビジネスメールで最も多く詐称された役職はこれまでと同様に CEO（Chief Executive Officer：最高経営責任者）で全体の 41.1% であった。また、2019 年にビジネスメール詐欺で標的にされた職種には企業の財務部門の管理職や役員のほかに会計士や大学教授も含まれており、標的となる業界や職種の多様化が指摘されている（図 1-1-3）。攻撃者は事前調査にも力を入れており、前述の



■図 1-1-3　ビジネスメール詐欺の標的にされた職種の割合
（出典）トレンドマイクロ社「2019 年年間セキュリティラウンドアップ」を基に IPA が作成

Office 365 や Outlook の文字列を含むフィッシングサイトの一部も、企業で用いられている Microsoft アカウントを詐取しメールを盗み見る等、ビジネスメール詐欺への悪用を目的としているものと考えられる（ビジネスメール詐欺については「1.2.2 ビジネスメール詐欺（BEC）」参照）。

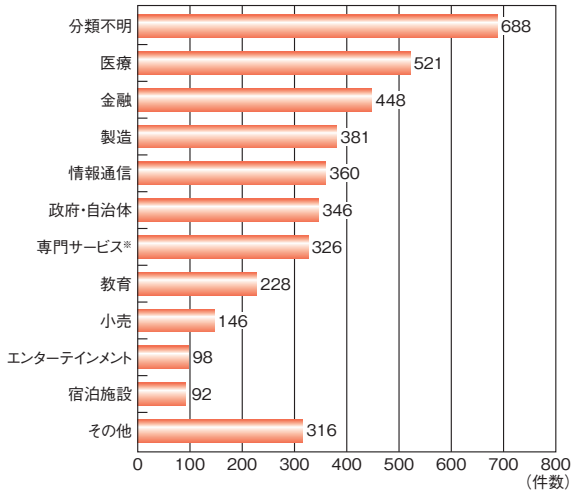
(2) 情報漏えいインシデントの状況

2019 年も多くの情報漏えいインシデントが発生した。ここでは、その規模や影響度の大きさから、2 件のインシデントについて紹介する。

- 2019 年 7 月 29 日、米金融大手 Capital One Financial Corporation は不正アクセスにより 1 億人を超える個人情報が流出したと発表した※8。流出したデータには、氏名、住所、郵便番号、電話番号、メールアドレス、生年月日、年収等が含まれており、約 114 万人分の社会保障番号、約 8 万件の銀行口座番号も含まれていた。攻撃者は WAF※9 の設定ミスを悪用して、SSRF 攻撃※10 によってデータを窃取したと見られている（インシデントの詳細は「3.4.1 (4) 設定ミスの悪用に起因するインシデント」参照）。
- 2019 年 9 月 16 日、エクアドル政府は国民ほぼ全員を含む約 2,000 万人分の個人情報が海外に流出したと発表した※11。流出したデータには、名前や個人識別番号、銀行口座残高が含まれていた。情報の流出元はエクアドルの民間企業が所有し、米国フロリダ州マイアミに設置されていたサーバで、セキュリティ保護が行われていなかったことが指摘されている。データが当該サーバに格納されていた詳しい経緯は不明であるが、エクアドルには個人情報保護法にあたる法律が存在しないことが背景にあるとの見方もある。

Verizon 社によると、2019 年に発生した情報漏えいインシデント 3,950 件の業種別件数について、最も発生件数が多い業種は「医療」で 521 件、次いで「金融」が 448 件、「製造」が 381 件、「情報通信」が 360 件となっている（「分類不明」を除く）（次ページ図 1-1-4）。

また、情報漏えいインシデントの攻撃方法の割合については、2019 年は 2018 年と同じく「Web アプリケーション攻撃」が全体の約 31% と最も多く、次いで「人的ミス」が約 21% と 2 位になっている。2018 年に 5 位（約 5%）だった「クライムウエア」は 2019 年には 3 位（約 10%）に上昇し、2018 年に 3 位（約 15%）だった「特権の不正使用」、4 位（約 13%）だった「サイバースパイ活動」は 2019 年にはそれぞれ 4 位（約 8%）、6 位（約 3%）に下降している



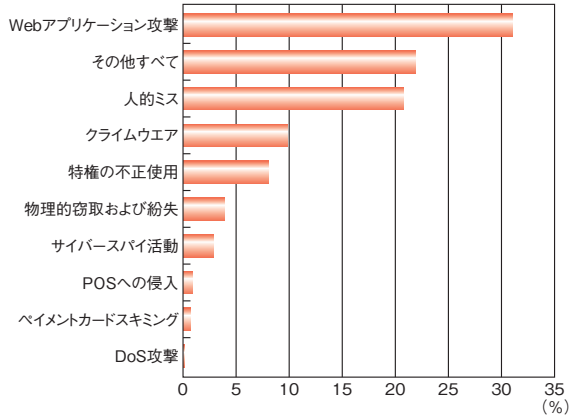
※専門サービスとは、弁護士、会計士、アーキテクト、研究所、コンサルティング会社等を指す

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

(「その他すべて」を除く)(図 1-1-5)。

IBM 社によると、2019 年の調査では 2018 年の漏えいレコード件数の 3 倍超にあたる 85 億件を超えるレコードが漏えいしたことが分かった。情報漏えいの原因としては、アクセス制御や保護が不十分、ネットワークエリアが意図せずインターネットに接続されている等の不適切なサーバ設定によるものが約 86% を占めているという。一方で 2019 年には、不適切なサーバ設定によるインシデントの件数自体は 2018 年より 14% 減少しており、インシデント 1 件あたりの漏えいレコードの数が著しく増えたと IBM 社は分析している。

今後、あらゆる業界でデータの保有量・共有量が増加していく中で、それらをどのように不正アクセスから保護し、活用していくのかが問われている（情報漏えいについては「1.2.7 情報漏えいによる被害」参照)。

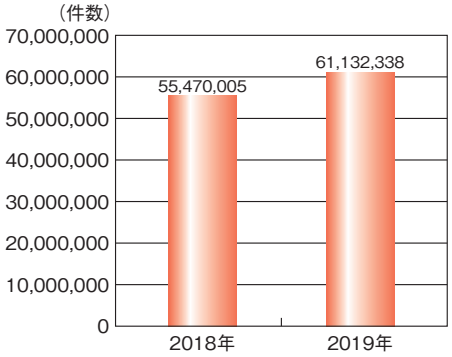


■図 1-1-5　情報漏えい事件の攻撃方法の分類
(出典)Verizon 社「2020 Data Breach Investigations Report」を基に IPA が編集

(3) ランサムウェアによる攻撃の傾向

トレンドマイクロ社によると、2019 年の世界のランサムウェア※12 検出数は約 6,113 万 2,000 件と 2018 年より約 10%増加した（図 1-1-6)。一方で、同年の日本のランサムウェア検出数は約 1 万 2,000 件と 2018 年より約 38% 減少しており、異なる傾向が見られる。世界で新たに確認されたランサムウェアファミリーの数は 2018 年の 222 から 2019 年の 95 と大幅に減少しており、ランサムウェアの攻撃者が標的を絞った上でそれに適した既存のランサムウェアファミリーを使用するようになっていると分析されている。

2019 年のランサムウェアの標的の中では、工場の制御システムを含むネットワーク※13、自治体の電話回線と金融システム※14 等、企業の収益や市民生活に影響が大きく高額の身代金の支払いが期待できそうなネットワークシステムが目立っていた。また、2020 年 6 月には日本企業でもランサムウェアにより工場の生産を停止する事態が発生している※15(「1.1.2(4)注目された新たな脅威」参照)。企業の本社・生産拠点間、地域等でネットワークを形成して稼働するシステムが増加する中、ランサムウェアの侵入と感染拡大には一層の警戒が必要である（制御システムを標的としたランサムウェアについては「3.1 制御システムの情報セキュリティ」参照)。



■図 1-1-6　世界におけるランサムウェアの攻撃総数
(出典)トレンドマイクロ社「2019 年年間セキュリティラウンドアップ」を基に IPA が作成

(4) 攻撃手法の傾向と変化

前項で述べたように、ランサムウェアによる攻撃で生活に必要なサービスが停止するリスクが高まっている。また、2019 年に IoT 機器を使用不能とする新たな機器破壊型ウイルス※16 が発見され、医療機器として使用されている IoT 機器が攻撃された場合、人命が脅かされるリスクが指摘されている※17。

この機器破壊型ウイルスの作成者は、脆弱性を放置

したままの機器をターゲットとする予定であることを公言している（機器破壊型ウイルスについては「3.2 IoT の情報セキュリティ」を参照）。また、IBM 社がウイルスメールを監視・分析した結果、既に修正プログラムが公開されている CVE-2017-0199[※18] と CVE-2017-11882[※19] の脆弱性を悪用するものが全体の 90% 近くを占めることが判明している。

脆弱性対策の状況を見ると、トレンドマイクロ社の調査では、2019 年 5 月に発表された脆弱性「BlueKeep」（CVE-2019-0708）については、世界規模での被害が指摘されたにもかかわらず修正プログラムが未適用のシステムが多く残っている等、脆弱性が放置されているケースが多かった（BlueKeep については「1.2.4 ソフトウェアの脆弱性を悪用した攻撃」を参照）。

感染すると重要なサービスの停止を招きかねないランサムウェアや、共通の脆弱性を持つ多くの IoT 機器に感染し、使用不能とするウイルス等の存在を考慮すると、今後、攻撃の入り口となる脆弱性やウイルスメールへの対策は、基本事項であるがより一層重要なものになっていくと考えられる。

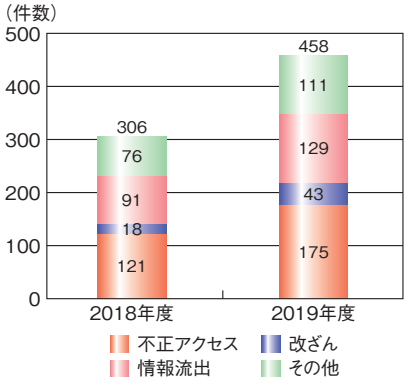
1.1.2 国内における情報セキュリティインシデント状況

国内における情報セキュリティインシデントの発生状況について、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：2019 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

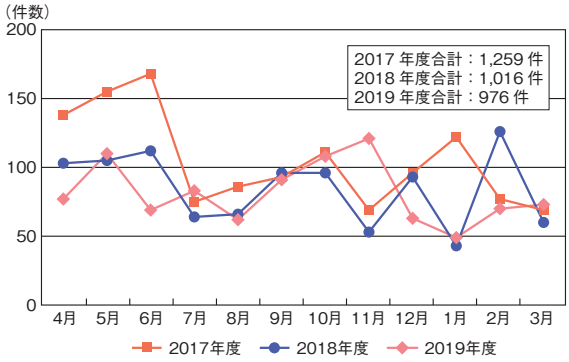
MBSD 社が集計した結果によると、2019 年度に報道された情報セキュリティインシデントの件数は 2018 年度の 306 件から 458 件に増加した（図 1-1-7）。インシデントの種類別に見ても、いずれも前年度比で 4 割以上増加した。2018 年度同様、最も件数が多いのは「不正アクセス」、最も件数が少ないのは「改ざん」だが、「改ざん」は前年度比で 2 倍以上に増加している。「不正アクセス」件数の増加は、IPA への届出件数の増加にも表れている（「付録」の「資料 B 2019 年のコンピュータ不正アクセス届出状況」参照）。報道数や届出件数が増加していることから、社会のインシデントへの意識や関心は高まっていると考えられる。



■図 1-1-7　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[※23] を基に IPA が作成

(2) Web サイト改ざんによる被害

2019 年度に JPCERT/CC へ報告された Web サイトの改ざん総件数は 976 件であった。ここ数年の傾向を見ると、2016 年度までは毎年 3,000 件を超えていたが、2017 年度は 1,259 件と大幅に減少し、2018 年度、2019 年度も減少傾向が続いている（図 1-1-8）。なお、前項の図 1-1-7 における「改ざん」の件数は増加しているが、この件数にはデータベースやプログラムの改ざん等 Web サイト閲覧者が確認できない改ざんも含まれているため、Web サイト閲覧者からの報告を集計した図 1-1-8 とは増減の傾向が異なるものと考えられる。

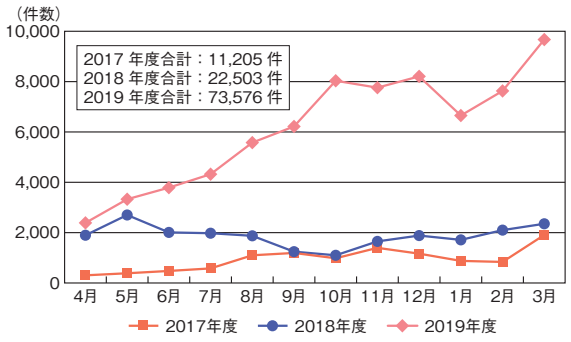


■図 1-1-8　Web サイト改ざん件数推移
（出典）JPCERT/CC「インシデント報告対応レポート」（2017 年 4 月 1 日～2020 年 3 月 31 日）を基に IPA が作成

JPCERT/CC は、Web サイト改ざんの傾向について、2018 年度に続き、不正に埋め込まれたスクリプトによって特定ブランドを扱う e コマースサイトやアダルトサイト等、閲覧者が意図しないサイトに転送させる事例を報告している。2019 年度に目立った手口として、WordPress や Magento といった広く利用されている CMS（Contents Management System）の脆弱性を悪用したものが確認されている（「1.2.4 (2) CMS の脆弱性を悪用した攻撃」参照）。Web サイト改ざんの目的はウイルスの配布、特定の Web サイトへの誘導、クレジットカード情報等の個人情報や他の攻撃の手掛かりになるシステム情報の窃取等、多岐にわたる。減少傾向にあるとはいえ今後も継続的な対策が必要である。

(3) フィッシングによる被害

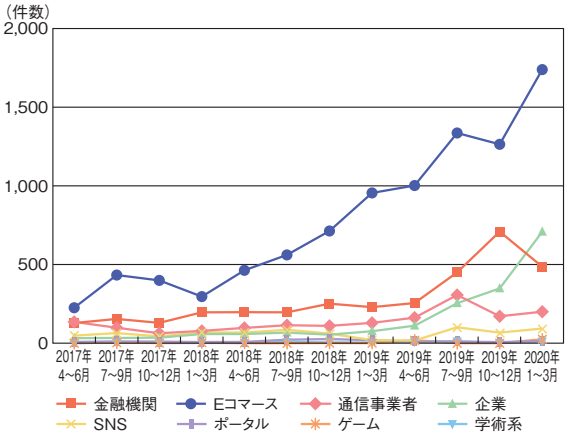
個人情報やクレジットカード番号、キャッシュレス決済等の各種サービスの認証情報等の詐取を目的としたフィッシングが継続している。ここ数年のフィッシング対策協議会への報告件数は、2017 年度が 1 万 1,205 件、2018 年度が 2 万 2,503 件と倍増し、2019 年度には前年度の 3 倍超の 7 万 3,576 件と急増している（図 1-1-9）。



■図 1-1-9　フィッシングの報告件数推移
（出典）フィッシング対策協議会「月次報告書」（2017 年 4 月～ 2020 年 3 月）を基に IPA が作成

JPCERT/CC で集計したフィッシングサイトの業界別件数の推移を見ると、2017 年度以降「E コマース」が最多で急増を続けており、2020 年 1 ～ 3 月期に過去最多の 1,739 件を記録した。「金融機関」は 2018 年から緩やかな増加傾向にあったが、2020 年 1 ～ 3 月期には急減し、2019 年に入ってから増加し始めた「企業」に追い抜かれた（図 1-1-10）。今後は企業の偽サイトにも注意が必要となる。

また、JPCERT/CC が収集したフィッシングサイトのプロトコルについて、2017 年から HTTPS を使用したサイトが増加し始め、2018 年には全体の 45%、また 2019 年には全体の 51% と半数以上のフィッシングサイトが HTTPS を使用していたことが報告された※24。メールに記載された URL が https で始まるものでも簡単に信用してはならないことを認識したい。



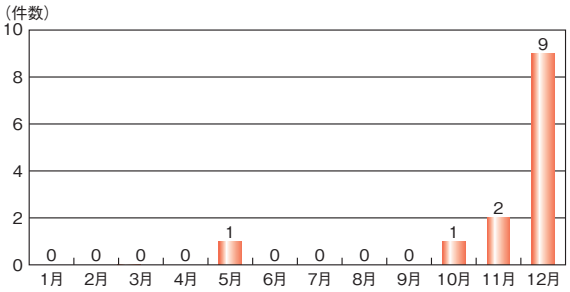
■図 1-1-10　フィッシングサイトのブランド別件数推移
（出典）JPCERT/CC「インシデント報告対応レポート」（2017 年 4 月 1 日～ 2020 年 3 月 31 日）を基に IPA が作成

2019 年 9 月から 11 月にかけて、フィッシングによるものと思われる不正送金被害が急増し、注意喚起が行われた※25。2019 年 12 月には同年 8 月の水準に戻った※26 ものの、被害急増の背景として多要素認証の突破や、不正アプリをインストールさせて被害を拡大させる手口等、フィッシングの巧妙化が指摘されており※27、また、フィッシングサイトを手軽に作成・運用するツールも出回っている※28 ため、引き続き警戒が必要である（フィッシングについては「1.2.6 個人をターゲットにした騙しの手口」参照）。

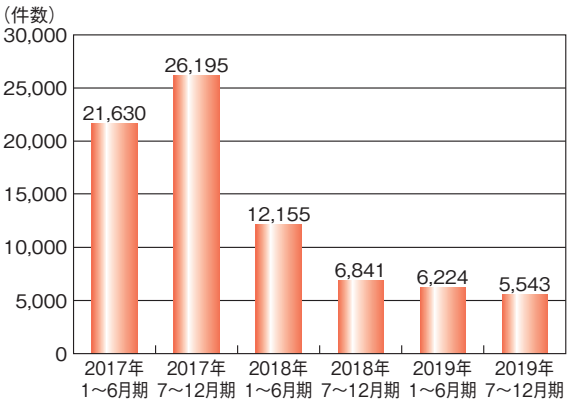
(4) 注目された新たな脅威

トレンドマイクロ社の調査によると、2019 年後半に「Emotet」と呼ばれるウイルスの検出数が急増し、2019 年第 1 ～第 3 四半期に毎期 300 件未満だった検出数は 2019 年第 4 四半期（10 ～ 12 月）に 1 万件を超えた。Emotet は 2019 年 2 月ごろから日本語のばらまき型メールで拡散されるようになり※29、日本の商習慣を利用する等、その後も手口が巧妙化してきた。2019 年 10 月からは、多数の法人組織で感染被害が公表され、被害件数が急増した（図 1-1-11）。2019 年の Emotet 感染による国内での被害は情報漏えいや感染端末から窃取した情報を元にしたなりすましメール送信が中心となっている（Emotet については「1.2.5 ばらまき型メールによる攻撃」参照）。

国内におけるランサムウェア感染を目的とした攻撃の検出数は 2017 年以降、減少傾向にある（図 1-1-12）。し

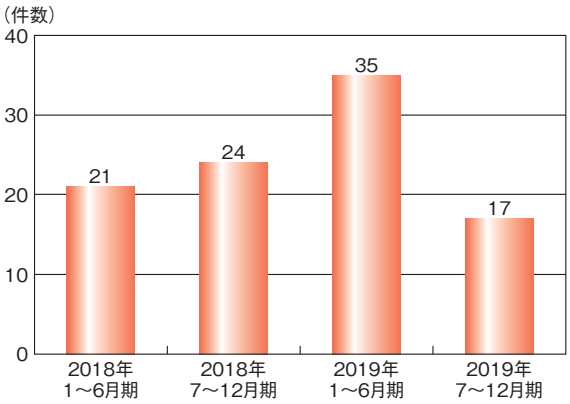


■図 1-1-11　2019 年公表の主な EMOTET 感染被害の件数推移
(出典)トレンドマイクロ社「2019 年年間セキュリティラウンドアップ」を基に IPA が編集



■図 1-1-12　国内におけるランサムウェアによる攻撃の検出数推移
(出典)トレンドマイクロ社「2019 年年間セキュリティラウンドアップ」を基に IPA が編集

かし、法人での被害報告は 2019 年上半期にピークとなった（図 1-1-13）。法人被害報告の増加の要因として、これまで標的型攻撃（「1.2.1 標的型攻撃」参照）で用いられてきたような事前調査を伴う計画的な手口が用いられるようになったことが指摘されている。2020 年 6 月に本田技研工業株式会社に対して行われたランサムウェア SNAKE（別名、EKANS）による攻撃では、目的のシステムにランサムウェアを感染させるためにネットワーク偵察



■図 1-1-13　国内法人のランサムウェア被害報告件数の推移
(出典)トレンドマイクロ社「2019 年年間セキュリティラウンドアップ」を基に IPA が作成

等の事前調査や感染経路の確保等が計画的に行われた可能性があるとされる※30。その他、標的型攻撃にも利用されている攻撃ツールやサーバ等の脆弱性を悪用してランサムウェアに感染させる手口、海外では前述の Emotet を利用してランサムウェアに感染させる手口が確認されている。

2013 年前後から表面化してきたパスワードリスト攻撃※31 は 2019 年度も継続しており、2019 年 7 月にはキャッシュレス決済サービス「7pay（セブンペイ）」（以下、7pay）における大規模な不正利用が発生した※32。7pay は 2019 年 7 月 1 日よりサービスを開始したが、翌日から身に覚えのない取り引きがあった旨の相談が寄せられ、株式会社セブン & アイ・ホールディングス及び株式会社セブン・ペイが外部の情報セキュリティ会社とともに調査した結果、第三者がパスワードリスト攻撃により不正ログインしていた可能性が高いことが明らかになった。被害に遭ったアカウントは同月末の時点で 808 人分、被害総額は 3,861 万 5,473 円と発表されており、同年 9 月 30 日には 7pay のサービス自体が廃止された。

被害が継続している背景には、様々な要因による ID とパスワードの漏えいと、それらの情報が蓄積されたリストの流通、そしてユーザのパスワードの使い回しがある。リストはダークウェブで販売される等、攻撃者の間で広く流通して悪用されるため、ユーザがパスワードを使い回している場合、ID とパスワードのみによる認証ではセキュリティの担保にならない。サービス提供者には複数の端末からのログインの制限や多要素認証等の追加のセキュリティ対策の実施が求められ、同時にユーザにも、複数のサービスにおいてパスワードの使い回しをしない、サービス側から提供される追加のセキュリティ機能を利用する、または追加のセキュリティ機能があるサービスを選ぶといった対策が求められる。

2020 年 1 月より、ウイルスやフィッシング、詐欺等の攻撃メールにおいて新型コロナウイルス感染症※33（以下、新型コロナウイルス）の流行に便乗した文面が確認されている※34。また、新型コロナウイルスの感染拡大を防ぐ目的で、テレワークや個人が所有する端末を業務で利用する BYOD（Bring Your Own Device）といった業務形態が急速に普及しており、使用するシステムや端末のセキュリティ対策強化の必要性が指摘されている（「1.3.1 (3)リモートデスクトップサービスに関連する脆弱性について」参照）。今後も新型コロナウイルスの流行や対策に伴う政策やサービスに便乗した新たな詐欺の手口や攻撃の出現が懸念され、引き続き警戒が必要である。

1.2 情報セキュリティインシデント別の手口と対策

本節では、インシデント別の発生状況と、具体的な事例について述べる。また、2019 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、ある特定の組織・企業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、特定の組織・企業や業界が持つ機密情報の窃取やシステム・設備の破壊・停止といった、明確な目的をもって行われる。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※35。

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）。

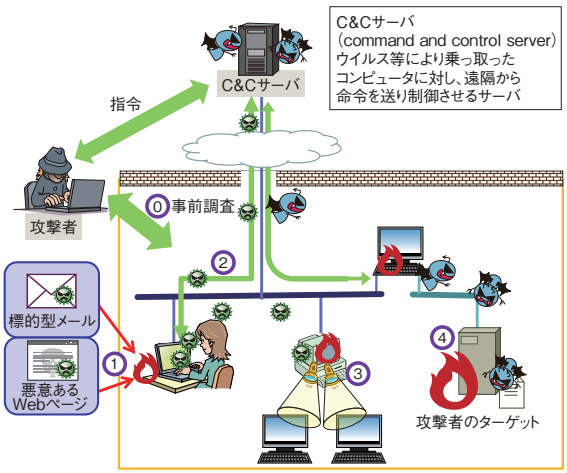
「事前調査段階」では、標的とする組織や業界の情報を収集する。公開されている情報を収集するだけでなく、標的とする組織と他の組織とのメールによるやり取りの盗聴等により必要な情報を収集することもある。

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、標的とする組織の端末へのウイルス感染を試みる。多くの場合、標的とする組織の人間に対し、ウイルスを添付したメール（標的型攻撃メール）を送り付ける手法が用いられる。標的型攻撃メールでは、標的とする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。

「初期潜入段階」で標的組織の内部に侵入した攻撃者は、「攻撃基盤構築段階」へと移り、標的組織内のパソコンを遠隔操作するため、遠隔操作ウイルス（RAT: Remote Access Trojan）に感染させることを試みる。この際、遠隔操作を長期的かつ継続的に行うため、複数の RAT に感染させる場合もある。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。

「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。また、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※37。



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※36」を基に編集

(1) 国内の標的型攻撃事例

本項では、2019 年度に確認された 2 件の標的型攻撃の事例を紹介する。

(a) 国内組織の中国現地法人を狙った標的型攻撃

2019 年初頭から、日本企業の中国子会社に対して、標的型攻撃が行われたというレポートがセキュリティベンダより公開されている※38。この攻撃は、防衛、化学、航空宇宙、衛星業界等の機密情報を取り扱う複数の組織に対して行われたとのことである。

レポートによると、攻撃者はまず、日本国内の経済調

査会社や PR 会社を攻撃し、電子メールのアカウント情報やダミー文書用のファイルの窃取等を行い、そのメールアカウントを送信元として、標的とする組織・企業へ標的型攻撃メールを送信していた。

送信された標的型攻撃メールは、日本語で書かれており、件名や添付ファイル名には、「昇給」や「求人」、中国の経済情勢に関連したものが使用される等、送信元とされたメールアカウントの組織の活動に沿ったものであった（表 1-2-1）。

添付ファイル名	日付
2018 年 12 月米中貿易摩擦調査 .pdf	2019/1/16
2019 {masked}CN Group Calendar - C.DOCX	2019/1/16
2018 年 12 月早会内容 .pdf	2019/2/17
2019 中国昇給率見通し各所発表 .pdf	2019/2/20
2019 中国商务环境调查报告 .pdf	2019/3/12
（詳細版）2019 年昇給率参考資料 .pdf	2019/3/22
{masked}- 中国経済週報（2019.3.21 ～ 3.29） .pdf	2019/4/1
新元号豆知識 - 元号 -{masked}20190408.pptx	2019/4/8
中国における日系企業の求人動向レポート 2019 年 3 月分 .pdf	2019/4/22
【顧客配布可】米中摩擦～新たな世界秩序と企業戦略～（日本語）.pdf	2019/5/22
20190523_{masked} 関連影響レポート _1900 時点 _{masked}.pdf	2019/5/31
{masked} 中国産業データ&リポート - 習主席 G20 欠席なら追加関税導入 -20190612.pdf	2019/6/15
2019{masked} 関連影響レポート _ 日系企業各社の対応 _{masked}.pdf	2019/6/26
20190625 米中貿易摩擦と金融・資本市場への影響（{masked}） .pdf	2019/7/5

■表 1-2-1　添付ファイルやダミー文書で使用されたファイル名
（出典）トレンドマイクロ社「Operation ENDTRADE: TICK's Multi-Stage Backdoors for Attacking Industries and Stealing Classified Data※39」を基に IPA が編集

本事例では、中国の子会社で感染したパソコンから、共有フォルダにウイルスを設置され、そのウイルスが日本の従業員によって実行された例も確認されているという。セキュリティ対策が強固な日本の組織・企業へ侵入するための足掛かりとして、中国の子会社が狙われたものと思われる。

(b) 未公開の脆弱性を悪用した標的型攻撃

2019 年 6 月、日本企業の国内研究所のサーバから不審なファイルが見つかり、社内ネットワークが外部から不正アクセスを受けていたことが発覚した※40。

報道によると、不正アクセスは日本企業の中国の子会社から始まり、子会社と日本国内の本社や拠点とを結ぶルータを経由して侵入されたという※41。その後、社内のパソコンに導入されていたセキュリティ製品の脆弱性を悪用されて管理サーバが乗っ取られ、管理サーバのパターンファイルアップデート機能により各パソコンにウイルスが配信されて感染が拡大した※42。攻撃者は機密情報を窃取するため、広い権限を持つ管理職層のパソコンを狙って不正アクセスを行っていた。情報は一つのパソコンに集められ、外部に送信されていたという。

この事例では、未公開の脆弱性を悪用するゼロデイ攻撃が行われている。脆弱性情報が公開されたときは、速やかに対応することが望ましいが、本事例のように脆弱性の公開前に攻撃が行われることもある。このような場合、ユーザ企業側で根本的な対策を行うことは困難だが、他のサイバー攻撃同様、多層的なセキュリティ対策を実施しておくことが被害の低減に有効である。

(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。2019 年においても、防衛関連企業 4 社から事例が公表されており※43、今後も日本の組織が標的とされる状況は続くと予想され、常に対策を講じておくことが重要である。また、「1.2.1 (1) 国内の標的型攻撃事例」で紹介したように、海外の関連組織を足掛かりとして国内組織に感染を広げていく手口が確認されており、組織ごとの対策だけではなく、海外を含む企業グループ全体でセキュリティ対策を講じていく必要がある。

(3) 標的型攻撃メールの手口

標的型攻撃メールは、標的とする組織や業界で用いられる文言を件名や本文に用いる等、非常に巧妙に本物のビジネスメールに偽装して送られてくる。そのため、標的型攻撃メールの開封を完全に防ぐことは難しい。しかし、標的型攻撃メールに関する教育・訓練により、攻撃手口を知っておくことで開封のリスクを低減できる。ここでは、標的型攻撃メールで用いられる手口についていくつか紹介する。

(a) メールにおける騙しの手口

攻撃者は、標的型攻撃メールが不審に思われないように、メールの件名や本文に、標的とする企業・組織・業界固有の単語や言い回しを使用することが多い。メー

ルの信憑性を高めるために、実在する関係者の名前が署名として記載されている場合もある。添付ファイルについても、本文や件名と関連するファイル名が付けられていることが多く、目視のみで不審であると見抜くことは困難である。

また、標的型攻撃メールは、送信元メールアドレスを偽装した、なりすましメールであることが多いが、「1.2.1(1)(a) 国内組織の中国現地法人を狙った標的型攻撃」で紹介したように、あらかじめ標的とする組織と関連のある組織のメールアカウントを窃取し、そのメールアカウントを悪用して標的型攻撃メールを送るといった手口も確認されている。このような場合、SPF（Sender Policy Framework）と呼ばれる、電子メールの送信元ドメインの詐称を検知する仕組みを回避して標的型攻撃メールが着信する可能性がある。

(b) 添付ファイルの手口

標的型攻撃メールの添付ファイルは、受信者に攻撃であることを気付かれないように、巧妙な細工が施されていることが多い。例えば、アイコンの偽装、RLO（Right-to-Left Override）等による拡張子の偽装、ショートカット（LNK）ファイルの悪用、Microsoft Office の脆弱性・マクロ機能・OLE（Object Linking and Embedding）[※44] オブジェクトの悪用等がある。ここでは、2019 年度に確認された手口について紹介する。

- ショートカットファイルを悪用する手口
  2018 年度には見られなかったが、2019 年度では再び Windows のショートカットファイル（拡張子が .lnk であるファイル）を悪用する手口が確認された[※45]。一般には、ショートカットファイルの危険性はあまり認識されていないが、スクリプトと呼ばれる命令を埋め込むことで、実行ファイルと同等の動作をさせることが可能である。また、ショートカットファイルの特徴として、拡張子を表示する設定をしていたとしても、拡張子が表示されないことがある（図 1-2-2）。なお、このような場合であっても、エクスプローラーの詳細表示や、ファイルのプロパティ情報から、ファイルの「種類」を確認することで、ショートカットファイルかどうかの判別は可能である。
- オンラインストレージサービスを悪用する手口
  標的型攻撃メールでは、メールにウイルスを添付して標的組織に送り付ける場合が多いが、正規のオンラインストレージサービスを悪用し、受信者にウイルスをダウンロードさせるという事例も確認されている。

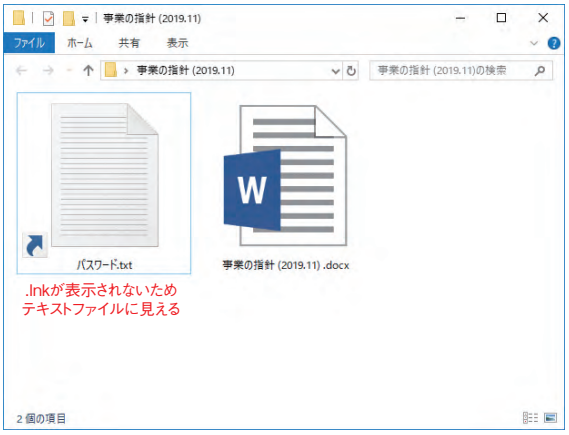


図 1-2-2　テキストファイルに見せかけるショートカットファイルの例

2019 年 4 月に国内で確認された標的型攻撃の事例では、標的型攻撃メールの本文中にオンラインストレージサービスの URL が記載されており、この URL には、ウイルスが格納された圧縮ファイルが配置されていた[※46]。正規のサービスを悪用しているため、受信者に気付かれる可能性が低いだけでなく、メールにウイルスを添付しないことにより、メールの配送経路上でのウイルスの検知を回避できる。オンラインストレージからのダウンロードを求めるメールには、十分な注意が必要である。

- Microsoft Office の脆弱性を悪用する手口
  標的型攻撃メールでは、Microsoft Office の脆弱性を悪用した Word 文書ファイルを添付する手口が多く見られる。2019 年度の標的型攻撃では、Microsoft Office の機能の一つである数式エディタの脆弱性を悪用し、ウイルスへの感染を試みる手口が確認された[※38]。
  この脆弱性が悪用された場合、受信者が添付ファイルを開いたり、Outlook やエクスプローラーのプレビュー機能で表示するだけでウイルスに感染させられてしまう可能性がある。
- Microsoft Office のマクロ機能を悪用する手口
  Microsoft Office には、VBA と呼ばれるプログラミング言語によって特定の処理を自動化するマクロ機能が存在する。この機能を悪用すると、不正なプログラムを文書ファイル内に仕込むことが可能である。不正なマクロが仕込まれた文書ファイルを開き、マクロを有効化すると、攻撃者が意図した処理が実行される。2019 年度に発生した標的型攻撃では、PowerShell を悪用した攻撃の足掛かりとして、標的型攻撃メールの添付ファイルでこの手口が使用された[※46]。マクロ機能

の悪用は、標的型攻撃に限らず、ウイルスに感染させるための手口として継続して使用されており、引き続き注意が必要である。

(4) 標的型攻撃への対策

標的型攻撃への対策を以下のように整理する。

(a) 利用者向けの対策

利用者向けの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、受信者を騙すための巧妙な手口が使われていることが多い。一方で、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等、不審な点に気付きやすいものも存在するため、利用者が不審な点がないか注意することは有効な対策の一つと言える。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必要がある。身に覚えのないメールアドレスからのメールを受信した場合は、添付ファイルを開いたり、本文中のURLリンクにアクセスすることは控えるよう周知する。なお、メールの本文や署名欄に記載されてい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。また、関係する組織・企業の 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。

- オンラインストレージサービスを悪用した手口の周知

  2018 年度に続き 2019 年度においても、メール本文中に記載された正規のオンラインストレージサービスの URL リンクから、ウイルスをダウンロードさせる攻撃が確認された。普段の業務でオンラインストレージサービスを利用している場合、このような手口が存在することを理解し、メール本文中に記載されたオンラインストレージサービスの URL リンクからファイルをダウンロードする際は、まず、メールが本物であるかどうかを確認するように周知する。

- 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、悪用すると攻撃者が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有効化するように周知する。

(b) 組織体制による対策

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標的型攻撃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である。

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。

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が重要である。

(c) ウイルス感染を想定した訓練と教育

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。

例えば、利用者向けの取り組みでは、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）がある。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。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事前に周知することも対応能力の向上に有効である。

CSIRT向けの取り組みでは、他組織で発生したインシデントや自組織で起き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[※47]。演習を通じて、CSIRTの対応能力の維持・向上や現在の対応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。

(d) 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。

- 不審メールを確保できる仕組みの確立

  セキュリティ製品・サービスによっては、不審なメールを検知した際、メールの添付ファイルやメールそのものを削除・無害化・ブロックしてしまうものが存在する。このような場合、メールの送信元や添付されているウイルスの不正接続先といったセキュリティ対策に必要となる情報が失われてしまう可能性がある。不審なメールを検知した際は削除せず、システム管理者やCSIRTだけがアクセス可能な場所に隔離し、解析によって必要な情報が得られるように仕組みを確立することが有効である。
- 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の脆弱性を悪用されるケースも存在する。脆弱性に対して適切な対応を行わずに放置した場合、その脆弱性を悪用され、攻撃者による侵入や攻撃を許してしまう危険性がある。

  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。

  運用上、サーバ・端末が停止できない場合や修正プログラムによりアプリケーションの動作に問題が発生する等の理由により、修正プログラムの適用が難しい場合は、脆弱性を悪用する攻撃を検知・遮断する仮想パッチによる脆弱性対策を検討するべきである。
- ファイルの実行防止

  あらかじめ、システムやポリシーで、利用者の環境で実行可能なファイルを制限（ホワイトリスト化）しておくことで、ウイルスへの感染を防止する。ホワイトリスト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を制限（ブラックリスト化）する。

  例えば、悪用されることの多いスクリプトファイル（拡張子が.jsや.ps1等であるファイル）のような、通常使用しないであろうファイルの実行を禁止することで、ウイルスへの感染を防止する。

以上のように、利用者の不審メールに対する注意力の向上、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 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組織・企業に送り付け、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[※48]。

本項では、2019年度に公開されたビジネスメール詐欺の状況、事例を紹介し、その巧妙な手口と対策について解説する。

(1) ビジネスメール詐欺の被害状況

FBIの統計[※49]によると、2019年7月までに、米国インターネット犯罪苦情センター（IC3：Internet Crime Complaint Center）を含む複数の組織に対して、全米50州と177ヵ国から報告されたビジネスメール詐欺の発生件数は16万件以上、被害総額は約262億米ドル（未遂を含む）に上っており、2018年5月に発表された前回統計値[※50]から件数及び被害総額ともに倍となっているという。全世界での発生件数の増加に伴い、法執行機関等も取り締まりを強化しており、世界10ヵ国でビジネスメール詐欺の容疑者が逮捕され、不正な送金が回収さ

れた事例が報じられた※51。

JPCERT/CC が 2019 年に実施した、国内企業 12 社を対象としたビジネスメール詐欺（未遂を含む）の調査結果では、被害の有無に関わらない不正な請求額の合計が約 24 億円であったという※52。また、国内企業に関連する被害額の大きな事例としては、2019 年 8 月に大手自動車部品メーカの欧州の子会社で外部者による虚偽の指示により約 40 億円の資金が流出した事例※53や、2019 年 9 月下旬に大手新聞社の米国の子会社で経営幹部を装った攻撃者による虚偽の指示に基づいて約 2,900 万ドル（約 32 億円）が流出した事例※54が挙げられる。

CEO や経営幹部になりすまし、緊急を装い最高財務責任者（CFO：Chief Financial Officer）や経理担当者等送金の権限を持つ従業員へ送金依頼メールを送り付けるタイプのビジネスメール詐欺は、「CEO 詐欺」とも呼ばれる。セキュリティベンダによると、この種の詐欺メールの数は 2018 年下半期（7 月～ 12 月）から 2019 年上半期（1 月～ 6 月）にかけて 52%増加しているという※55。

IPA でも、実際の組織・企業で試みられたビジネスメール詐欺の事例について、サイバー情報共有イニシアティブ（J-CSIP※56：Initiative for Cyber Security Information Sharing Partnership of Japan）の運用状況レポートで定期的に情報を公開している※57。

(2) 2019 年度に報道された事例の概要

2019 年度に国内や海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、概要を表 1-2-2（次ページ）に示す。多額の被害に遭った事例が多かったが、項番 8 のように保険で被害額を回復した事例もあった。

(3) IPA が情報提供を受けた事例の概要

ここでは、IPA が情報提供を受け、J-CSIP の運用状況として 2019 年度に公開したビジネスメール詐欺の事例の概要を表 1-2-3（次々ページ）に示す。なお、表 1-2-3 のうち 3 件（項番 1、2、7）で金銭的被害が確認されている。金銭的被害のなかった 12 件のうち 10 件は、メールの受信者または経理部門の担当者が不審であることに気付いたことにより、被害を防ぐことができた。残り 2 件は振り込みを行ってしまったものの、銀行が送金を停止したため、被害が防がれた。

(4) IPA が情報提供を受けた事例の中で特筆すべきもの

ここでは、IPA が 2019 年度に公開したビジネスメール詐欺の事例の中で特筆すべきものを 2 件紹介する。

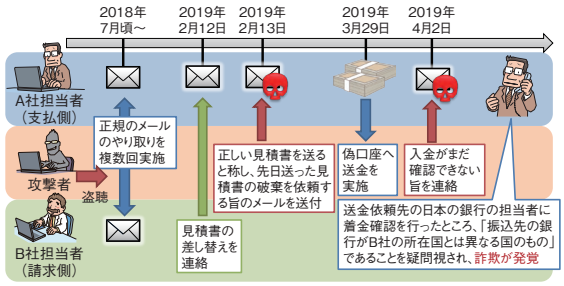
(a) 新規取引先の見積書の価格修正を装う攻撃

攻撃者が取引先とのやり取りに介入してくるタイプのビジネスメール詐欺では、振り込み先の口座の変更を要求する手口がこれまで多く発生していた。

しかしながら、2019 年 2 月、攻撃者が偽の口座を記載した見積書を「価格の修正」と称して送り付ける新たな手口について IPA に情報提供があった※78。

この事例は、国内関連企業（A 社：支払側）と、その「新規」海外取引先企業（B 社：請求側）との間で初めて行う請求と振り込みに関するやり取りを行っている中で、メールを盗聴していたと思われる攻撃者が B 社の担当者になりすまし、「新規に取り引きを開始する口座の情報を差し替える」手口で、見積価格の修正を装い偽の口座への振り込みを要求するメールを送り付けたものである。

攻撃者と A 社の担当者の具体的なやり取りは、図 1-2-3 のとおりである。この事例では、支払い側である A 社の担当者が攻撃者からの偽のメールであると気付かず、偽の口座へ振り込みを行ってしまったが、送金依頼先の日本の銀行担当者とのやり取りで不審な点に気付き、海外側の経由銀行へ連絡して送金を止めることができたため、金銭的な被害には至らなかった。



■図 1-2-3　攻撃者とのやり取り
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019 年 4 月～ 6 月］」

A 社と B 社のメールのやり取りを盗み見ていた攻撃者は、B 社から A 社に対して本物の見積書の差し替えを連絡するメールが送られた日（2019 年 2 月 12 日）の翌日、2 月 13 日に、「再度正しい見積書を送る」と称し、B 社から送られた本物の見積書を再度差し替える形で、偽の見積書を送り付けた。その際、偽の見積書に書かれていた支払先の銀行口座が、偽の口座情報に改変され

ていた。

この事例の特徴的な手口は、攻撃者は「口座の変更」とは伝えずに「見積書の価格の修正」と言い、実際には口座情報を改変していたという点である。更に、攻撃者は同時に「直前に送った見積書を破棄してください」とメールに記載しており、本物の見積書を破棄させることで、巧妙に偽の口座への送金を誘導している。実際にA社へ送られた偽のメールを図1-2-4(次々ページ)に示す。

このような手口によって担当者が騙された場合、経理部門等へは改変された後の偽の見積書しか渡されないという状況になりかねず、その場合、そもそも「口座に変更があった」という認識すらできないことになる。また、

項番	報道時期	概要	被害額
1	2019年4月	米国オハイオ州クリーブランドの教会は、大規模な修復工事の中で、配線工事の代金を請求する偽のメールに騙され、175万ドル（約1億9,300万円）の被害に遭った※58。	175万ドル（約1億9,300万円）
2	2019年5月	欧州でプレーしている南米サッカー選手の移籍において、移籍先クラブ（在フランス）が同選手の最初の所属クラブ（在アルゼンチン）に支払う129万9,377.48ユーロ（約1億5,600万円）のうち、51万9,750.99ユーロ（約6,200万円）が偽メールによって騙し取られた※59。	51万9,750.99ユーロ（約6,200万円）
3	2019年6月	東京都のプラスチック容器メーカは、2018年10月、台湾企業から生産設備を購入する取り引きに際し、偽メールの指示に従って香港の銀行の香港法人名義の偽口座に20万ドル（約2,200万円）を送金し、被害に遭った。2018年12月、送金先口座の名義を持つ香港法人を相手取り、返還を求める訴訟を香港の裁判所で起こした※60。	20万ドル（約2,200万円）
4	2019年6月	2019年2月ごろ、日本の電機メーカの米国子会社が韓国企業から機材を購入する取り引きで、偽メールの指示により、香港の口座に約40万ドル(約4,400万円)を送金した※60。	約40万ドル（約4,400万円）
5	2019年6月	米国の水力発電関連機関が2018年に2回、正当なベンダからのものであるように見える請求書の支払いにより、合計で217万ドル(約2億3,900万円)の被害に遭った※61。	217万ドル（約2億3,900万円）
6	2019年7月	米国ノースカロライナ州カバラス郡は、高校建設プロジェクトに関連し、2018年11月27日に開始された一連の偽メールにより、約250万ドル（約2億7,500万円）の被害に遭った。2019年2月に送金先の銀行が追跡可能な口座に残っていた約77万ドルを凍結して回収した。また郡が保険ブローカーと協力し保険代理店に請求し、2019年5月8日に7万5,000ドルの保険金を受け取った※62。	約250万ドル（約2億7,500万円）※一部回収
7	2019年8月	カナダのサスカチュワン州サスカトゥーンの自治体が、地元建設会社のCFOを装った偽メールにより、104万カナダドル（約8,600万円）を騙し取られた※63。	104万カナダドル（約8,600万円）
8	2019年8月	米国フロリダ州コリアー郡は、2018年末、工事請負業者に偽装された口座に18万4,000ドル（約2,000万円）を送金し被害に遭ったが、保険で回復した※64。	約18万4千ドル（約2,000万円）※保険で回復
9	2019年8月	英国のエネルギー企業のCEOが、ドイツの親会社のCEOになりすましたディープフェイク※65の音声で、ハンガリーのサプライヤーに22万ユーロ（約2,600万円）を至急送金するよう指示され、詐欺被害に遭った※66。	22万ユーロ（約2,600万円）
10	2019年9月	アイスランドの電力会社が、取引先への支払いに際し、約4億アイスランドクローナ（約3億4,800万円）相当の金額を攻撃者により詐取されたが、従業員が詐欺を発見し迅速に対応した。アイスランドと海外の警察当局が資金の回収に取り組んでおり、ほとんどの資金は回収される見込み※67。	約4億アイスランドクローナ（約3億4,800万円）※おおむね回収見込み
11	2019年10月	米国フロリダ州オカラ市は、空港ターミナルの建設会社従業員を装った偽メールに騙され、約75万ドル（約8,300万円）の被害に遭った。偽の口座には約11万ドル（約1,200万円）が残っていた※68。	約75万ドル（約8,300万円）※約11万ドル（約1,200万円）口座に残存
12	2019年11月	スイス企業のCEOが中米のベリーズの不動産を購入する過程で、売り主の弁護士をかたったメールで指示された偽口座に約100万ドル（約1億1,000万円）送金して被害に遭った※69。	約100万ドル（約1億1,000万円）
13	2019年11月	カナダのビールメーカは、2019年11月初旬、債権者の従業員になりすました偽の送金指示により、210万ドル（約2億3,100万円）を失った※70。	210万ドル（約2億3,100万円）
14	2019年12月	米国コロラド州エリー町の職員が、橋の建設工事の支払方法変更を要求する偽メールに騙され、約102万ドル（約1億1,200万円）を詐取された※71。	約102万ドル（約1億1,200万円）
15	2020年1月	米国テキサス州マナー市の独立学区は、取引先に偽装したメールにより、230万ドル（約2億5,300万円）を失った※72。	230万ドル（約2億5,300万円）
16	2020年1月	オランダの国立美術館が絵画の取り引きに関する交渉の中で、ロンドンのアートディーラーを装った偽メールに騙され、香港の口座に240万ポンド（約3億4,000万円）を支払い、被害に遭った※73。	240万ポンド（約3億4,000万円）

■表1-2-2　2019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）

項番	事例概要	被害の有無	備考
1	2018 年 10 月、国内企業（支払側）と、その海外取引先企業（請求側）で取り引きを行っている中で、攻撃者が請求側企業の担当者になりすまし、偽の振り込みを要求するメールが支払側企業に送られた。	あり	「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019 年 1 月～3 月］※74」に記載
2	2018 年 10 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、被害が生じた。	あり	「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019 年 4 月～6 月］※75」に記載
3	2019 年 2 月、国内企業の国内関連企業（支払側）と、新規の海外取引先企業（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 「1.2.2(4)(a) 新規取引先の見積書の価格修正を装う攻撃」参照
4	2019 年 3 月、国内企業の海外関連企業（請求側）と、海外取引先企業（支払側）との取り引きにおいて、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
5	2019 年 4 月、国内企業の海外関連会社において、同社の CEO になりすました攻撃者から、同社の財務部長へ国際送金をさせようとするビジネスメール詐欺が試みられた。	なし	同上
6	2019 年 1 月と 2019 年 7 月、国内企業の同一のメールアドレスに対し、当該企業と業務提携を結んでいる海外企業の担当者や CEO になりすます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［2019 年 7 月～9 月］※76」に記載
7	2019 年 6 月、国内企業の海外関係会社（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。	あり	同上
8	2019 年 7 月、国内企業において、当該企業の CEO になりすました攻撃者から、当該企業の複数の担当者へ、ビジネスメール詐欺の試みと思われるメールが送付された。	なし	同上
9	2019 年 7 月、国内企業（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
10	2019 年 7 月、国内企業（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
11	2019 年 8 月、国内企業（支払側）に対して、攻撃者が海外の取引先企業（請求側）になりすます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［2019 年 10 月～12 月］※77」に記載
12	2019 年 10 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
13	2019 年 8 月と 10 月、国内企業の別の国内グループ会社の経営層になりすました攻撃者から、それぞれの企業の海外関連企業の担当者に対しビジネスメール詐欺が試みられた。	なし	同上 「1.2.2（4）（b）CEO を詐称する一連の攻撃」参照
14	2019 年 11 月、国内企業の欧州子会社の担当者に対して、国内企業側の CEO になりすました攻撃者から、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
15	2019 年 11 月、国内企業の海外関連会社（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

■表 1-2-3　IPA が情報提供を受け 2019 年度に公開したビジネスメール詐欺事例の概要

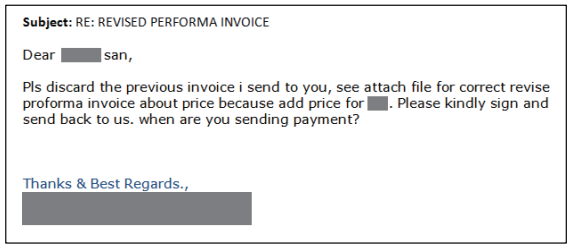
本事例は新規の取引先とのやり取りであり、過去の実績を基にした確認（これまで使っていた口座との比較等）ができず、送金前に経理部門による確認は行われていたものの、不審だとは気付けなかった。

IPA ではこれまで、ビジネスメール詐欺への対策として「急な振込先口座の変更等の対応を求められた場合には、事実関係を確認する」点に注意を促していた※79 が、本件のような手口では、この対策を取っていても急な振り込み先口座の変更であると認識することが難しい。

今後もこのような手口で偽の口座への振り込みを要求する攻撃が発生する可能性もあり、注意が必要である。

(b) CEO を詐称する一連の攻撃

2019 年 10 月、J-CSIP の参加組織から、国内グルー



■図 1-2-4　攻撃者からのメール
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019 年 4 月～ 6 月］」

プ会社の経営層を詐称したなりすましメールが送られたという情報提供があった。この情報を J-CSIP 内で共有したところ、複数の参加組織から類似した攻撃の情報提供があった。IPA では J-CSIP 外の情報等を含め、この攻撃について独自に調査を行ったところ、情報提供された件数と合わせて 62 件の類似する攻撃を確認した。

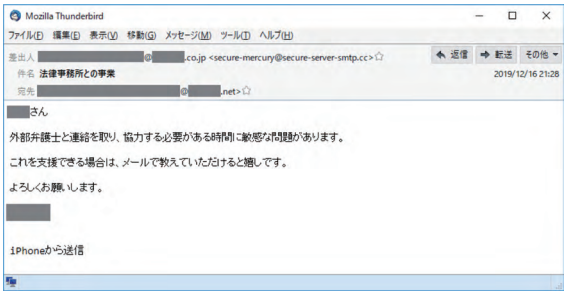
これらのメールには、メールの件名・本文や攻撃者のメールアドレス等に共通する特徴があり、同一の攻撃者による攻撃が、国内外の多数の組織へ行われたものと推測される。IPA ではこの一連の攻撃は、手口等からビジネスメール詐欺の一種であると考えている。

この一連の攻撃は、IPA で確認している限り 2019 年 7 月 23 日から 2020 年 1 月 16 日にかけて、国内外の組織に対して実在する CEO または弁護士を詐称するメールが多数の業種に対して送られたものと推測される。これらのメールの本文は 5 ～ 10 行程度の簡素なもので、具体的な用件は書かれていないが、「重要な用件がある」「計画について話がしたい」として、メールでの返信を求める内容である点が共通していた。件名や本文はほぼ英文であったが、日本語とスペイン語のメールも 1 件ずつ確認している。実際に送られた英語のメールを図 1-2-5 に、日本語のメールを図 1-2-6 に示す。

攻撃者が使用したメールアドレスは様々に異なるが、命名に規則性があり、差出人（From）や返信先（Reply-To）のメールアドレスに、「secure」という単語と、「mars」や「mercury」等天体（惑星・衛星等）に関する単語を組み合わせたものが使用されていた。今後も同様の手口での攻撃が継続する可能性があるため、日ごろからこのようなメールへの注意が必要である。

また、この一連の攻撃事例には受信者が攻撃者へ返信をしてしまっている例もあり、このような典型的な「CEO 詐称」のメールであっても、従業員が一定の確率で騙されてしまい、これを発端に、巧妙な詐欺が行われる可能性はあると考えられる。偽物だと見破ることが容易に

■図 1-2-5　実在する CEO を詐称するメール
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019 年 10 月～ 12 月］」



■図 1-2-6　実在する CEO を詐称するメール（日本語）
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019 年 10 月～ 12 月］」

見えるメールであったとしても、侮るべきではない。

（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、ここでは J-CSIP の活動から得られた情報を基に、実際に使われた具体的な手口の一部を紹介する。攻撃者はここで紹介する手口を組み合わせて巧妙な攻撃を仕掛けてくる場合があり、注意が必要である。

（a）偽の口座へ振り込ませる手口

攻撃者が用意した偽の口座へ振り込ませる手口として、次のようなものを確認している。これらは一例ではあるものの、このような内容のメールが取引先や経営層等から送られてきた場合、ビジネスメール詐欺を疑ってみる必要がある。

- 請求書に誤りがあったと連絡し、偽の口座が書かれた請求書を送付して支払いを要求する。
- 銀行口座が国の監査を受けているため振り込みができない、という理由を付けて偽の口座への支払いを要求する。
- 為替レートの問題があり、新たな口座を開設したと理由を付けて偽の口座への支払いを要求する。
- 経営者になりすまして「緊急かつ秘密の案件」や「ビットコインの購入が必要」と称して、送金を要求する。
- クレジットカードの支払いを受け付けられなくなったという理由を付けて偽の口座へ支払いを要求する。
- 見積書の価格に修正があったと連絡し、偽の口座が書かれた見積書を送付する。

(b) メールの引用部分の改変の手口

メールのやり取りの中で、攻撃者に都合が悪く矛盾のある点を隠蔽するために、引用部分の本文や From/To/Cc のメールアドレスの一部や署名部分の連絡先を削除または改変する手口を確認している。

このような手口で送られてきたメールを不審だと見破って調査を行う際にも、引用部分にあるメールのやり取りの経緯は信用するべきでない。どこから本物と偽物（攻撃者）が入れ替わったのかを特定するためには、過去の取引先とのメールを可能な限り回収し、調査する必要がある。

(c) メールアドレスのなりすましの手口

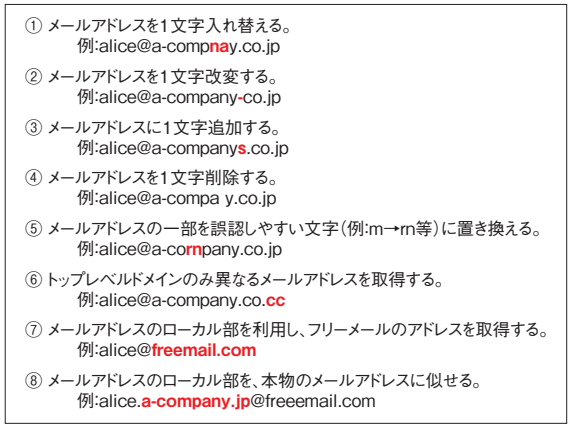
攻撃者が標的とした人物を騙すため、取引先等の本物のメールアドレスに似せた偽のメールアドレスを使い、なりすましを行う手口を確認している。

例えば、本物のメールアドレスが「alice@a-company.co.jp」である場合、攻撃者がなりすましに使う偽のメールアドレスの作り方には図 1-2-7 のような特徴がある。

(d) 同報メールアドレスの改変の手口

受信者に本物のメールであると錯覚させ、なりすましメールの発覚を遅らせるため、攻撃者がメールの Cc（同報先）に設定するメールアドレスを細工して、あたかも複数の担当者にも同報でメール送信がされているかのように見せる手口を確認している。

例えば、攻撃者が B 社の dave（請求担当者）になりすまし、A 社の alice（支払担当者）へ偽のメールを送る際に、A 社及び B 社の関係者として同報されているメールアドレスをすべて改変し、偽のメールが多数の取引関係者に対して同報されているように錯覚させる手口を図 1-2-8 に示す。



■図 1-2-7　攻撃者によるメールアドレスのなりすましの例

■図 1-2-8　同報メールアドレスの改変の手口
（出典）IPA「偽口座への送金を促す“ビジネスメール詐欺”の手口 ～ J-CSIP（サイバー情報共有イニシアティブ）から得られた手口の詳細とその対策 ～」

この手口で送られたメールは B 社の支払担当者（alice）にのみ届くため、正規のメールで同報されていた A 社及び B 社の関係者はなりすましメールが送信されていることに気付かない。

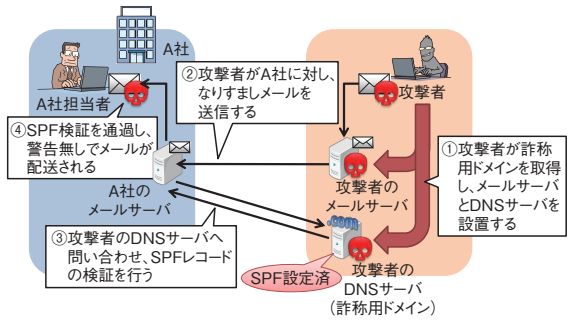
更に、別の例として A 社の関係者の同報メールアドレスは改変せずに B 社の関係者の同報メールアドレスのみを改変したケースも確認している。

(e) 詐称用ドメインの取得と悪用の手口

攻撃者がなりすましを行う企業のものとよく似た「詐称用ドメイン」を取得する手口を確認している。攻撃者はこの詐称用ドメインを利用してメールソフトの表示では正規のメールアドレスから送信されたように錯覚させる手口や、なりすましメールが正当なメールサーバから送信されたものであるかのように偽装し、送信ドメイン認証技術による警告対象となることを回避する手口を確認している。以下に送信ドメイン認証を回避する手口の例を記載する。

- SPF[※80]を悪用する手口

  攻撃者は、詐称用ドメインのDNS（Domain Name System）情報にSPFレコードを設定し、受信側のSPF検証を通過（Pass）させる。受信サーバ側は送信されたメールのドメイン名を基に、取得したDNSサーバのSPFレコードと送信元メールサーバのIPアドレスとの整合性が確認できれば送信ドメインを認証し、警告なしでメールを配信してしまう場合がある。攻撃者によって詐称用ドメインが取得され、DNSサーバに当該ドメインのSPFレコードが設定された場合に、なりすましメールが配送される流れを図1-2-9に示す。



■図1-2-9　SPFレコード設定済みの詐称用ドメインによるなりすましメールの配送

（出典）IPA「偽口座への送金を促す“ビジネスメール詐欺”の手口～J-CSIP（サイバー情報共有イニシアティブ）から得られた手口の詳細とその対策～」

- DKIM（Domain Keys Identified Mail）[※81]を悪用する手口

  攻撃者は、詐称用ドメインのDNS情報にDKIMレコードを設定し、なりすましメール送信の際に電子署名を付加することで、受信側のDKIM検証を通過（Pass）させる。DKIM検証の際、受信側で電子署名が照合できれば送信ドメインを認証し、警告なしでメールを配信してしまう場合がある。

送信ドメイン認証技術（SPFやDKIM）を悪用する手口では、攻撃者が詐称用ドメインを取得後、比較的短期間のうちにDNSやメールサーバの設定を実施し、なりすましメールを送信する傾向が見られた。不正な目的で自組織の類似ドメインが新たに取得されていないかを定期的にチェックしている企業があるが、そのような対策を回避しようとしているものと考えられる。あるいは、詐欺がうまく進みそうな場合に、状況に応じてドメインを適宜取得するという、柔軟かつ素早い行動を取っている事例もある。

(f)送信元を偽装して攻撃者に返信させる手口

攻撃者が送信元を偽装して攻撃者に返信させる手口を確認している。この手口では差出人（From）の表示名とメールアドレスを本物の表示名とメールアドレスに偽装し、返信先（Reply-To）メールアドレスを攻撃者のメールアドレスにするという手口と、差出人（From）の表示名のみを偽装し、差出人（From）のメールアドレスは攻撃者のメールアドレスを設定することで送信元を偽装している手口を確認している。

メールの仕組み上、差出人（Fromヘッダ）は、メールを送信する側が任意の内容に指定（偽装）できる。受信したメールをメールソフトによって表示した場合、差出人（From）の表示名には、このFromヘッダの内容が表示されるため、攻撃者がFromヘッダを偽装している場合、メールソフトで表示される差出人（From）の表示名からは、あたかも本物のメールアドレスから送信されたように見える。そのメールの返信先（Reply-Toヘッダ）に、攻撃者のメールアドレスが設定されていた場合、返信メールの作成画面ではReply-Toヘッダに設定されたメールアドレスが宛先となるため、この時点で偽装に気付かなければ、攻撃者とメールをやり取りしてしまうことになる。

この手口を用いた例として、図1-2-10の例を確認している。

①Fromヘッダに本物の担当者の情報を記載し、Reply-Toヘッダのメールアドレス部に攻撃者のメールアドレスを設定する手口
　From:本物の表示名<本物のメールアドレス>
　Reply-to:本物の表示名<**攻撃者のメールアドレス**>

②Fromヘッダに本物の担当者の名前を記載し、メールアドレス部に攻撃者のメールアドレスを設定する手口
　From:本物の表示名<**攻撃者のメールアドレス**>
　Reply-to:なし

③ FromヘッダまたはReply-Toヘッダに長い名前を記載して攻撃者のメールアドレスを確認しにくくする手口
　From:**長い表示名**<**攻撃者のメールアドレス**>

④ Fromヘッダにセミコロン（;）を用いて複数のメールアドレスを設定し、攻撃者のメールアドレスに返信させる手口
　From:本物の表示名<**偽のメールアドレス※**>;<**攻撃者のメールアドレス**>
　Reply-To:なし
　※「偽のメールアドレス」は送信エラーとなるメールアドレスを指す

■図1-2-10　送信元を偽装して攻撃者に返信させる手口の例

(6)ビジネスメール詐欺への対策

これまで説明してきたようにビジネスメール詐欺の手口は年々巧妙さが増している。このような攻撃の被害に遭わないための対策を以下にまとめる。これらの対策を通じて、ビジネスメール詐欺の手口を理解するとともに、不審なメールへの意識を高め、組織内の体制の強化や基本的なセキュリティ対策の実施等、複数の対策を組み合わせながら対策を行っていくこと（多層防御）が重要である。

(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、CFO 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、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、取引先全体や、警察、金融機関へ報告し、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、なりすましを検知する対策も有効である。

(c)送金処理のチェック体制強化

ビジネスメール詐欺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、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の通常と異なる対応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)類似ドメインへの対応

ビジネスメール詐欺の攻撃者は、自組織や取引先のドメイン名に似た詐称用のドメインを取得し、そのドメインを持つメールアドレスを用いて攻撃を行うことがある。自組織外のメールアドレスやフリーメールから着信したメールについて、件名や本文にその旨の注意喚起を表示するメールシステムを採用すれば、従業員は、紛らわしいドメインからのメールを見分けやすくなる。

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アドレスであるか、落ち着いて確認することも有効である。

(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、フィッシング、メールの内容やメールアカウント情報を窃取するウイルスの感染等で情報を窃取し、メールサーバへの不正アクセス等の方法でメールを盗み見ている場合がある。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、Office 365 や 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。

また、メールアカウントが乗っ取られ、利用者本人が設定し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る場合の該当アカウントへの対処方法が Microsoft 社より公開[※82]されているため、そちらも参照していただきたい。

1.2.3 DDoS攻撃

DDoS（Distributed Denial of Service）攻撃とは、Web サーバ等の攻撃対象に対して多数の端末からデータを送信することで、攻撃対象のリソースに負荷をかけ、サービス運用を妨害する攻撃を指す。

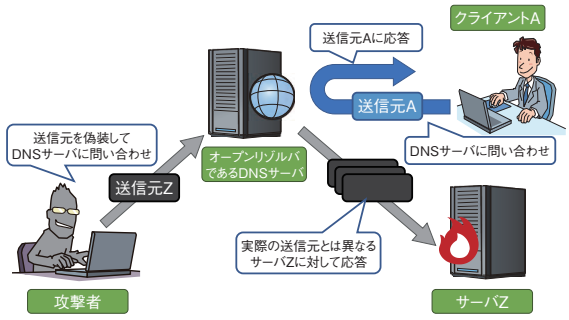
本項では、2019 年度に確認された DDoS 攻撃の事例とその対策を解説する。

(1)DDoS 攻撃の手口と事例

2019 年度における、DDoS 攻撃の主な手口と事例を紹介する。

(a) 通信プロトコルの挙動を悪用する事例

通信プロトコルの中には、リクエストよりもレスポンスのデータサイズが大きくなるものがある。攻撃者がそのような挙動を悪用し、送信元を攻撃対象のアドレスに偽装したリクエストを大量に送信することで、増幅されたレスポンスが攻撃対象のアドレスに宛てて送信される。攻撃対象は、大量のデータを受信することになり、処理能力の限界を迎え、サービスのパフォーマンスの低下や停止を起こす。このような DDoS 攻撃は「リフレクター攻撃」と呼ばれる(図 1-2-11)。



■図 1-2-11　リフレクター攻撃の例(DNS を悪用した場合)

リフレクター攻撃は 2019 年にも定常的に確認されている。A10 ネットワークス株式会社[※83]や、株式会社インターネットイニシアティブ[※84]が公開しているレポートによると、DNS (Domain Name System) や NTP (Network Time Protocol)、SSDP (Simple Service Discovery Protocol)、LDAP (Lightweight Directory Access Protocol)といった通信プロトコルが攻撃に使われており、数 Gbps ～数十 Gbps といった規模の攻撃トラフィックが毎月のように観測されている。

(b) DDoS 攻撃を脅迫に用いる事例

2019 年 10 月中旬以降、複数の組織を対象に、DDoS 攻撃をすると脅して仮想通貨を要求するメールが送付された事例をドイツのセキュリティベンダが確認した[※85]。また、JPCERT/CC によると、日本国内でも同様の脅迫メールを受信している組織が確認されており、注意喚起が呼びかけられた[※86]。

一般的に、このような脅迫に応じることは推奨されない。脅迫に応じて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、攻撃が成功して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たりして被害が拡大する可能性もある。

JPCERT/CC が公開した注意喚起においても、攻撃者の脅迫には応じず、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た。

(c) ラグビーワールドカップ期間中に確認された DDoS 攻撃

2019 年 9 月～11 月に開催されたラグビーワールドカップの期間中に、ラグビーワールドカップの組織委員会のシステムを狙った DDoS 攻撃やフィッシング攻撃が発生していたことが、大会期間後の 2019 年 11 月に報道された[※87]。

報道によると、DDoS 攻撃は大会期間中に、最低でも 12 回にわたって断続的に行われたが、一時的に回線を切断する等の対応を行った結果、大会の運営に支障が生じるような被害はなかったという。

(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と、それらに対して遠隔で指令を送信するための C&C (Command and Control) サーバから形成されており、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コンピュータによって一斉に攻撃が行われる。

ボットネットを構成するコンピュータのほとんどは、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コンピュータである。

ボットネットは、自身の機能をアップデートすることで、最新の悪用手法等を取り入れ、様々な対象への攻撃を繰り返すことで、その規模を拡大させている。

例えば、「Muhstik」と呼ばれるボットネットは、2018 年 3 月から確認されているが、最新の脆弱性の悪用手法等を取り入れて、その規模を拡大している。2019 年に確認された Muhstik の亜種では、Oracle Weblogic Server、WordPress、Drupal といった Web サイト構築に用いられるソフトウェアの脆弱性を悪用する手法を取り込んだもの[※88]や、ルータを攻撃対象にした手法を取り込んだものが確認された[※89]。Muhstik はこのように、様々な手法を追加してボットネットを拡大させ、DDoS 攻撃等に使用されている(「3.2.1 (1) (p) Muhstik の亜種」参照)。

また、別の事例としては 2019 年 9 月に、Wikipedia、Twitch、Blizzard の各サービスのサーバが「Moobot」と呼ばれるボットネットによる攻撃を受けた事例がある。こ

の Moobot は 2016 年に猛威を振るった IoT 機器を対象にしたウイルスである「Mirai」の亜種である。更にこのボットネットは、DDoS 攻撃代行サービスでも利用されていることが分かっており、何者かが DDoS 攻撃代行サービスを使用して攻撃を行った可能性が指摘されている※90。DDoS 攻撃代行サービスは、既存のボットネット等の DDoS 用の攻撃インフラを有償で提供して、誰でも簡単に DDoS 攻撃を行えるサービスである。拡大したボットネットがこのようなサービスに使用されることが、大規模な DDoS 攻撃が発生する要因となっている（「3.2.1 (1) (h) Moobot」参照）。

これらの事例から分かるように、攻撃者にとって IoT 機器は格好の標的となっている。総務省の「令和元年版情報通信白書※91」では、IoT 機器の数は急速に増加しており、2020 年には全世界で 400 億台近くの IoT 機器がインターネットに接続されると予測されている。しかしながら、性能やコスト面の制約から、十分なセキュリティ機能を備えていない IoT 機器が存在している状況である。そのような IoT 機器が、攻撃者に乗っ取られ、悪用されることで、DDoS 攻撃が今後更に大規模化することが懸念されている（IoT 機器の情報セキュリティについては「1.2.4 (3) IoT 機器を対象とした攻撃」「3.2 IoT の情報セキュリティ」参照）。

(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端末が乗っ取られ、DDoS 攻撃に加担することを防ぐための対策も求められる。これらの対策について解説する。

(a) DDoS 攻撃の被害に遭った場合の対策

DDoS 攻撃によって送られてくる通信データを遮断し、サービスを提供するサーバやネットワークのリソースを保護する対策が必要である。正常なアクセスと DDoS 攻撃によるアクセスを、どのようにして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（Internet Services Provider）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端末、ネットワーク機器、IoT 製品が DDoS 攻撃に悪用されないように、ウイルス対策を導入する、適切な設定をする等の対策が必要である。また企業においては、自組織の端末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。
- パスワードが製品共通の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。パスワードが製品共通の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外部と接続されているネットワーク機器や IoT 機器を狙って感染し、更に、その機器をとおして組織内の他の端末に対しても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端末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見直し、DDoS 攻撃に悪用され得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、サーバの 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 攻撃に悪用され得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。
- 組織内の端末の外向けの通信を監視し、異常な通信を確認した場合は、組織内の端末が攻撃の踏み台となっている可能性がある。そのような端末に、ウイルス感染等が生じていないか調査を行う。自組織での

対処が困難な場合は警察やセキュリティベンダ等への相談を検討する。

1.2.4 ソフトウェアの脆弱性を悪用した攻撃

2019 年度も、多くの利用者がいる Windows や、Web サイト構築に使用される CMS の脆弱性を狙った攻撃が多く報告された。また、IoT 機器の脆弱性を対象とした新たなウイルスが報告されている。

本項では、これらの脆弱性の状況と対策について解説する。

(1) Windows の脆弱性を対象とした攻撃

2019 年度も、2018 年度に引き続き、Windows の脆弱性を狙った攻撃が多く報告されている。

ここでは、2019 年 5 月に公開された「BlueKeep」と呼ばれる脆弱性 CVE-2019-0708[※92] について解説する。

(a) BlueKeep の脆弱性を悪用した攻撃

BlueKeep の脆弱性は、Windows 7 以前の OS に存在し、リモートデスクトップサービス（RDS：Remote Desktop Services）が接続要求を処理する際の不具合に起因している。攻撃者はリモートデスクトッププロトコル（RDP：Remote Desktop Protocol）を利用して、標的となるシステムの RDS に細工したリクエストを送信する。リクエストに対する妥当性の確認が不十分であるため、解放済みメモリ使用（use-after-free）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（図 1-2-12）。この脆弱性を悪用するウイルスが開発されると世界規模での被害が発生しかねないとして、既にサポートが終了している Windows XP 等の OS に対しても更新プログラムが提供された[※93]。

上記の Windows XP の更新プログラムとは別に、Microsoft 社は 5 月の定例更新において、BlueKeep に関する更新プログラムを提供しているが、11 月上旬には、インターネット上から BlueKeep を利用し、仮想通貨の発掘ツールを不正にインストールしようとする攻撃が観測されている[※94]。

(b) Windows の脆弱性を悪用した攻撃への対策

脆弱性をつい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。

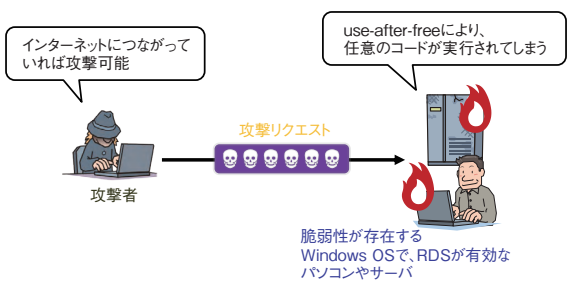
なお、2020 年 1 月 14 日には、Windows 7、Windows Server 2008 及び Windows Server 2008 R2 のサポートが終了している。一般にサポート終了後に発見された脆弱性については、修正プログラムが提供されなくなるため、サポートが終了した OS を使い続けると脆弱性を悪用した攻撃により、被害を受ける可能性が大きくなる。そのため、利用者は、ベンダのサポート情報を基に、計画的に最新の OS へ移行することが求められる。

(2) CMS の脆弱性を悪用した攻撃

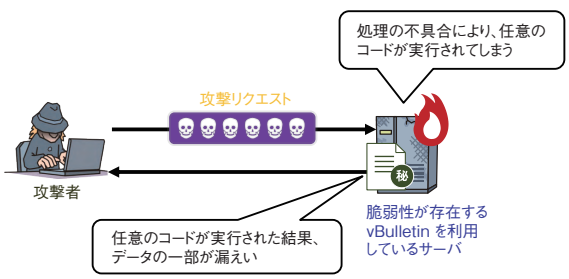
CMS は、Web サイトのコンテンツの作成・管理に使用されるソフトウェアの総称である。CMS には、「プラグイン」と呼ばれる拡張機能を導入することで、容易に機能を追加できるものもある。その手軽さから、CMS 本体だけでなく、プラグインも併せて広く利用されているため、プラグインに脆弱性が発見された場合も、攻撃者から狙われる。2019 年度も、CMS 本体やそのプラグインの脆弱性を悪用する攻撃が確認されている。

(a) CMS 本体の脆弱性を悪用した攻撃

CMS の一種である、フォーラムサイトを構築するソフトウェア「vBulletin」に、任意のコードを実行できる脆弱性が発見された。この脆弱性は、細工したリクエストを脆弱性が存在している vBulletin のサーバに対して送信するだけで、サーバ上で任意のコードが実行されるというものであり、これが悪用された結果、利用者の情報を窃取されるといった被害が発生している[※95]（図 1-2-13）。



■図 1-2-12　BlueKeep の脆弱性を悪用した攻撃イメージ



■図 1-2-13　vBulletin の脆弱性を悪用した攻撃イメージ

2019年9月24日にvBulletinの脆弱性が公表され、9月25日以降、この脆弱性を狙った攻撃通信が急増したことが報告されている※96。攻撃が急増した原因として、修正プログラムが提供されるより前に脆弱性が公表される、ゼロデイ脆弱性であったことと、悪用が容易であったことが挙げられる。

(b) CMSのプラグインの脆弱性を悪用した攻撃

2019年12月、WordPress向けプラグイン「Ultimate Addons for Elementor」と「Ultimate Addons for Beaver Builder」に認証を回避できる脆弱性が発見された。この脆弱性は、管理者のメールアドレスが分かれば、パスワードを必要とせずにWebサイトの管理アクセス権を取得可能、というものであった。これが悪用され、不正なプラグインのインストール等が行われたと報告されている※97。

(c) CMSの脆弱性を悪用した攻撃への対策

これらの事例のように、脆弱性が発見されると攻撃者にすぐに狙われ、被害が発生してしまうため、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。

このためには、事前の準備が重要である。自らが保有（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。同時に、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できる。更に、公開しているWebサイトのステージング環境※98を事前に用意しておき、当該Webサイトへ対策を実施する前に、実施による不具合が発生しないか検証することが望ましい。

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。

- CMS本体やプラグイン、ミドル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
- 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、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。

(3) IoT機器を対象とした攻撃

2019年度は、IoT機器の脆弱性を狙う新たなウイルスが多数報告されている。

(a) IoT機器の脆弱性を狙う新たなウイルス

トレンドマイクロ社によると、2019年7月22日～8月6日のわずかな期間に、IoT機器を対象とした攻撃を調査するために設置したハニーポットから、ルータ等を標的とする3種類のウイルス（「Neko」及びその亜種、「Mirai」の亜種である「Asher」、「Gafgyt」（別名、Bashlite、QBot等）の亜種である「Ayedz」）が確認されたという※99。これらのウイルスに感染したルータは、DDoS攻撃を実行するボットネットの一部として機能するという（各ウイルスの詳細については「3.2.1 (1) 機器乗っ取り型ウイルスの動向」参照）。

IoT機器を標的としたウイルスが増加する背景として、IoT機器の急速な普及が挙げられる。2020年には全世界で400億台近くのIoT機器がインターネットに接続されると予測されている※91。そのため、IoT機器を狙ったウイルスが今後も増加すると考えられる。

(b) IoT機器を対象とした攻撃への対策

脆弱性が存在するIoT機器は、ウイルス感染によりボットとなり、攻撃に利用される可能性がある。IoTボットによる攻撃はDDoS攻撃だけでなく、情報窃取や機器破壊等、多様化している。それを踏まえて、IoT機器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
  - 各組織が公開しているIoT機器の開発ガイドライン等を基に、企画・設計工程等を含めた、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「3.2.3 (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。
  - 製品出荷後でも、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。
  - 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使用する。
  - 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※100」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 サイトで公開された情報がないか定期的に確認する。
- 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。
- 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 機器にアクセスできないようにする。

1.2.5 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※101。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 による手法が存在する。メールの添付ファイルにはマクロ付きの Word ファイルや Excel ファイル、そして OLE 機能を悪用し、悪意のあるプログラムを埋め込んだ Word ファイル等が確認されている※102。また、ばらまき型メールの内容には、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関係のないメールや、実在の組織をかたったメール、一見すると業務に関係ありそうな件名や本文のメール、過去の正規のやり取りがあったメールを引用し、「正規のメールへの返信」を装ったメール等が存在する。

J-CSIP では、2019 年 10 ～ 12 月期に、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（ばらまき型メールの受信者）の端末へ送り込み、「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）を観測した。Emotet のばらまき型メールの件名・文面は、正規のメールへの返信を装ったものや、一見すると業務に関係ありそうなもの等が確認されている。Emotet のばらまき型メールとは別に、添付ファイルを介してマクロ付き Word ファイルを攻撃対象者の端末へ送り込むことで、「Ursnif」と呼ばれるウイルスへの感染を狙うばらまき型メールも同時期に確認されている。これには Emotet のばらまき型メールと同様、正規のメールへの返信を装う手口が使われていた。更に、Emotet や Ursnif への感染を狙った攻撃とは別のウイルスへの感染を狙った攻撃も観測された※77。

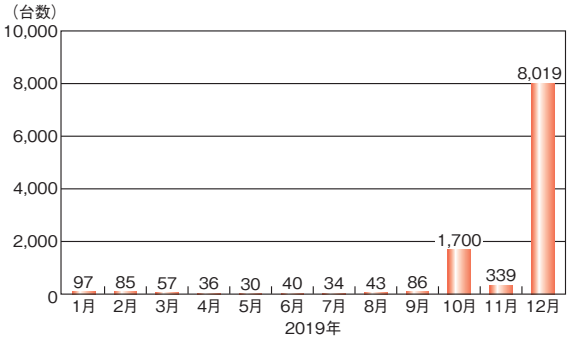
本項では、2019 年 9 月後半より日本国内に広くばらまかれた※29 Emotet のばらまき型メールを中心に、Ursnif 等別のウイルスへの感染を狙ったばらまき型メールも併せて解説する。

(1) Emotet のばらまき型メール

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※103。Emotet の観測状況、Emotet のばらまき型メールの手口と対策等について述べる。

(a) 日本国内の観測状況

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いるが、明確に日本を狙った攻撃は確認されていなかった※29。しかし、2019 年に入り、日本への Emotet のばらまき型メールによる攻撃が複数の国内組織・企業へ行われていることが確認された。一例として、2019 年 6 月に東京都の医療関連組織への Emotet の感染が公表された※104。そして、2019 年 9 月後半から Emotet のばらまき型メールによる攻撃が活発化し、2019 年 10 月の Emotet の検出台数は 9 月までと比較して急激に増加した。11 月は一時的に減少したとみられるが、12 月に再び急増した※105。図 1-2-14 に国内での Emotet の検出台数の推移を示す。



■図 1-2-14　国内での Emotet 検出台数推移（不正 Office 文書ファイル含む）
（出典）トレンドマイクロ社「引き続き国内で拡大する『EMOTET』の脅威※105」を基に IPA が編集

JPCERT/CC は、2019 年 10 月後半より、Emotet の感染に関する相談を多数受けているとして、2019 年 11 月 27 日、注意喚起情報を公開している※106。また、2019 年 10 月ごろより、Emotet に関連する、あるいは関連が推定される注意喚起や報道がなされている※107-1。

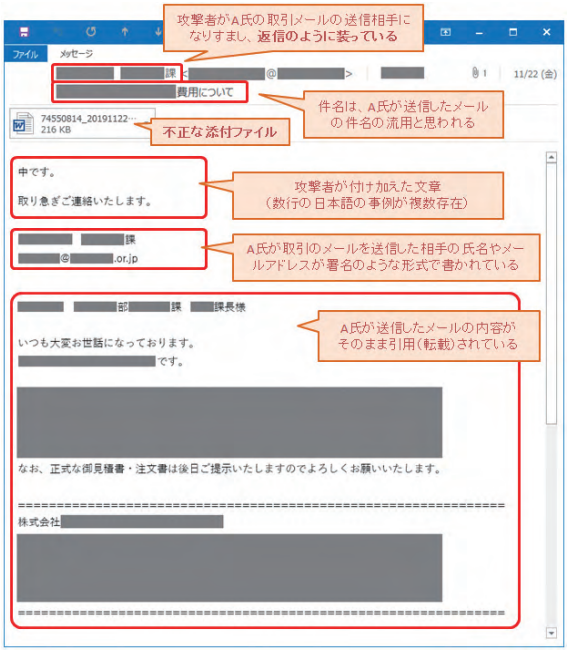
(b) Emotet のばらまき型メールの手口

攻撃者が Emotet のばらまき型メールを送信してからウイルスに感染させるまでの手口を解説する。

- 本物のメールと信じ込ませる手口

  IPA では、Emotet のばらまき型メールにおいて、正規のメールへの返信を装うメールを観測している※34。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メールを装っている。

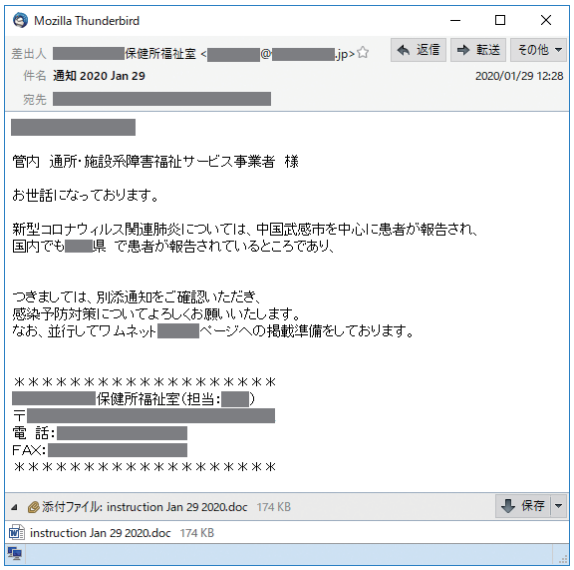
  正規のメールへの返信を装うメールの例を図 1-2-15 に示す。この例では、メールの受信者（A 氏）が以前、取引先へ送信したメールが丸ごと引用され、返信されてきたかのような内容となっている。また、件名や文面が受信者とまったく関係のない内容が記載されている事例や、引用部分の存在しない事例等も確認されている※34。正規のメールへの返信を装うばらまき型メールは 2018 年 11 月にも観測されており※107-2、この手口自体が新しいわけではない。しかし、Emotet の手口は、2018 年 11 月に観測された正規のメールへの返信を装うばらまき型メールとばらまき方が異なる。2018 年 11 月に観測された手口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メールへ返信する形式であった。一方、Emotet の手口では感染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を装うメールをばらまくことが確認されている※108。



■図 1-2-15　正規のメールへの返信を装う Emotet のばらまき型メールの例
（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※34」

- メール受信者の興味・関心を惹く題材を悪用する手口

  IPA では、2020 年 1 月 29 日、正規のメールへの返信を装うメールとは異なる、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た※34。図 1-2-16 に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の例を示す。



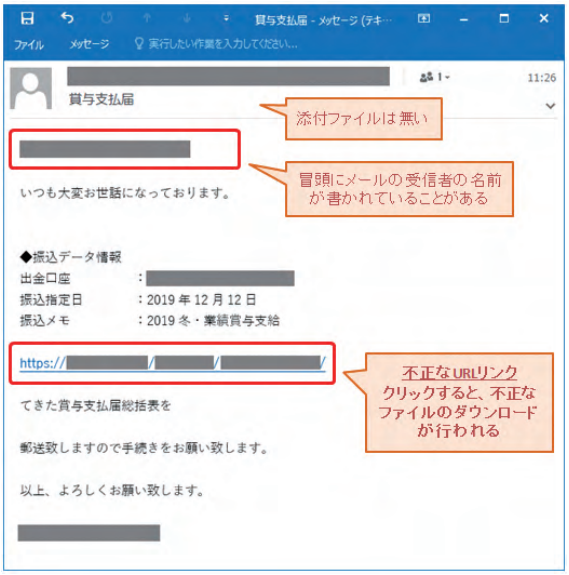
■図 1-2-16　新型コロナウイルスを題材とした Emotet のばらまき型メールの例
（出典）IPA「『Emotet』と呼ばれるウイルスへの感染を狙うメールについて」

また、2019 年 12 月には、賞与の支給を題材にした Emotet のばらまき型メールが観測された。メールの件名は「12 月賞与」や「賞与支払」等の賞与に関するもので複数のバリエーションが確認されている※105。

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攻撃を行っていると推測され、執拗に日本国内を狙って攻撃していると言える。

- Emotet に感染させる手口

  Emotet の感染を狙ったばらまき型メールでは、マクロ付き Word ファイルを添付する手口が多く観測されている※109。更に 2019 年 12 月 10 日ごろより、添付ファイルではなく、メール本文中に不正な URL リンクが記載され、URL リンクをクリックするとマクロ付き Word ファイルがダウンロードされる手口も観測されている※34。図 1-2-17（次ページ）にメール本文中に不正な URL リンクが記載された、Emotet のばらまき型メールの例を



■図 1-2-17　不正な URL リンクを含む Emotet のばらまき型メールの例
（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」

示す。

マクロ付き Word ファイルを攻撃対象者の端末へ送り込む手口は異なるが、添付ファイルによる手口でも、メール本文中に不正な URL リンクが記載される手口でも、当該 Word ファイル内の悪意のあるマクロが動作することで、外部 Web サイトに設置された Emotet をダウンロードし感染させる。

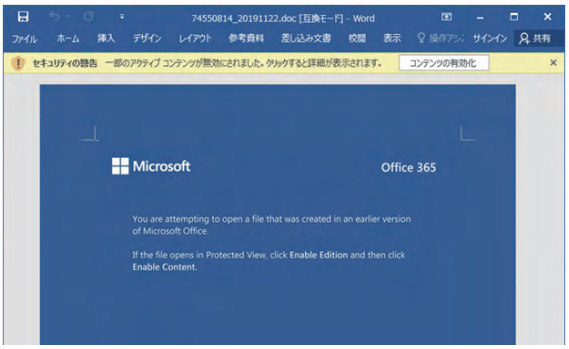
マクロ付き Word ファイルには、Microsoft や Office 等のロゴとともに、英語で「文書ファイルを閲覧するには操作が必要である」という趣旨の文と、次の二つのボタンのクリックを促す文が書かれている。

①「Enable Editing」（日本語版 Office では「編集を有効にする」）ボタン※ 110

②「Enable Content」（日本語版 Office では「コンテンツの有効化」）ボタン

①、②はいずれも Word ファイル上部の黄色いバーに表示される。①は添付ファイルを開いた状況により、表示されない場合があるが、表示される場合は①と②の両方を、①が表示されない場合は②をクリックすると、Word ファイル内の悪意のあるマクロが動作し、Emotet がダウンロードされ、感染させられる。

図 1-2-18 に Emotet のばらまき型メールで悪用されるマクロ付き Word ファイルの例を示す。図 1-2-18 の例以外にも複数のバリエーションが存在するが、①と②のボタンのクリックを促す文が書かれている点と、悪意のあるマクロが埋め込まれている点は共通している。



■図 1-2-18　マクロ付き Word ファイルを開いたときの画面の例
（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」

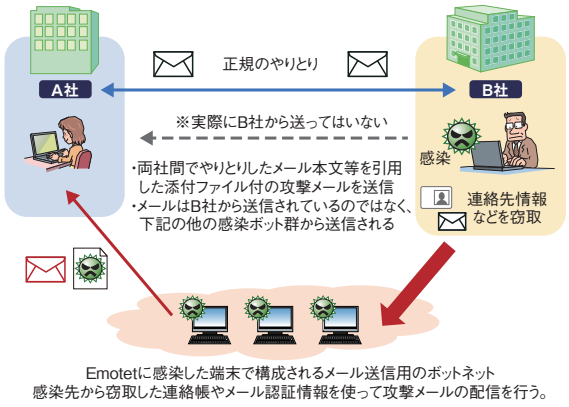
(c) Emotet の機能

Emotet は、もともとはインターネットバンキング等のサービスにおける認証情報を窃取することを目的としたウイルスとして利用されていたという※ 103。しかし、現在では Emotet は追加のモジュールをダウンロードすることで次の機能を持ち得るとされている※ 111。

①ネットワークを経由して別の端末へ感染拡大する機能
②メールアカウント情報の窃取機能
③Outlook のアドレス帳の窃取機能
④Outlook のメールデータの窃取機能
⑤Web ブラウザに保存されたアカウント資格情報の窃取機能
⑥Emotet のばらまき型メールの送信機能

2019 年後半に Emotet のばらまき型メールが大量にばらまかれた理由の一つとして、②、③、④、⑥の機能による感染拡大が考えられる。Emotet は②、③、④の機能によって感染者のメールに関する情報を窃取し、⑥の機能によって新たな攻撃対象者に対して、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 Emotet のばらまき型メールを送る。このようなサイクルを繰り返し、Emotet は感染の拡大を行っている※ 108。図 1-2-19 に Emotet の感染拡大のイメージを示す。

また、セキュリティベンダによると Emotet は別のウイルスをダウンロードする機能を有しており、「TrickBot」と呼ばれるウイルスをダウンロードすることがあるという。TrickBot はインターネットバンキングの情報窃取を目的としたウイルスとして知られているが、機密性の高い情報を窃取する機能や組織内のネットワークに感染を拡大する機能も有しており、組織内のネットワークに感染を拡大させ、サーバ等の情報を収集する。更に TrickBot は収集した情報を基に標的とする資産を定めて「Ryuk」と



■図 1-2-19　Emotet の感染拡大のイメージ
（出典）JPCERT/CC「マルウエア Emotet の感染活動について※108」を基に IPA が編集

呼ばれるランサムウェアに感染させる可能性がある※112。

海外の事例では、米国のフロリダ州レイクシティ市で Emotet により、同市のシステムに接続された端末に Ryuk がインストールされ、行政システムの全ファイルが暗号化されたというものがある※113-1。

このように Emotet に感染すると、その後、TrickBot、更には Ryuk に感染し、組織内のデータの窃取や暗号化等の被害が発生する可能性がある。Emotet への感染被害が Emotet の感染拡大につながってしまうことや、別のウイルスに感染し甚大な被害をもたらす可能性があることを十分認識し、感染被害に遭わないようにするべきである。

(d) Emotet に感染しないための対策

Emotet のばらまき型メールの攻撃者は、(b) で述べたようにマクロ付き Word ファイルの送り方を変える、時事を題材にしたメールをばらまく等、手口を変化させながら攻撃を行っている。今後も手口が変化する可能性があるため、JPCERT/CC※106 や IPA※34 が紹介している対策を検討するとともに、「1.2.5 (4) ばらまき型メールへの対策」に記載している一般的なウイルス対策と同様の多層的な防御を実施すること必要である。

(e) Emotet に感染した後の対応

JPCERT/CC は Emotet に感染した後の対応を紹介している※113-2。感染後の対応として、一般のウイルス感染と同様、感染端末のネットワークからの隔離や、組織内の全端末のセキュリティソフトによるフルスキャン等が挙げられている。また、Emotet がメール情報を窃取して新たなばらまき型メールを送るため、被害を受ける可能性のある関係者への注意喚起も挙げられている。

Emotet に感染しないための対策を徹底し、感染しないことが理想であるが、万が一感染してしまった場合に備え、組織として迅速に適切な対応を行える準備をしておくことも重要である。

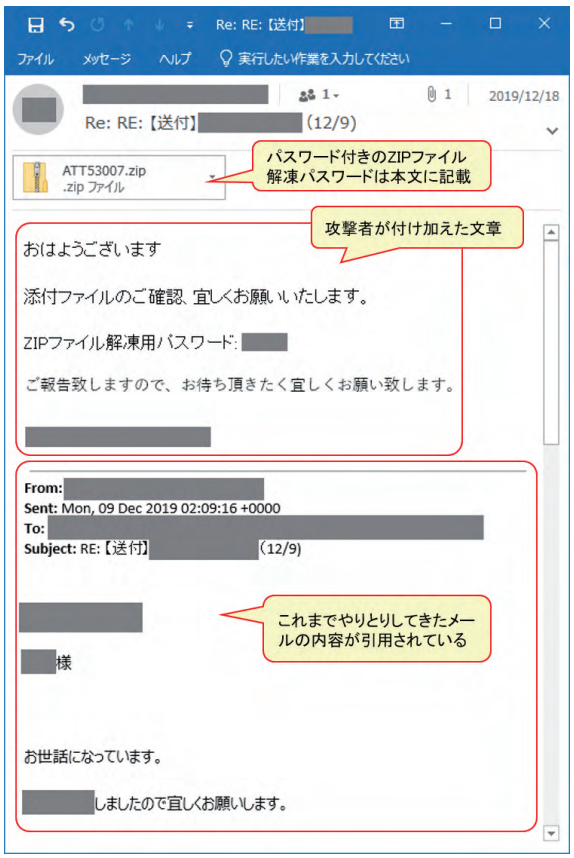
(2) Ursnif への感染を狙ったばらまき型メール

Ursnif は日本国内において、2016 年 3 月より観測されている、インターネットバンキングの情報を窃取し、不正送金を行うウイルスである※114。Ursnif には、DreamBot と呼ばれる亜種が存在し、2017 年 3 月と 12 月に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）より、DreamBot に関する注意喚起情報が公開された※115。IPA は、2019 年 12 月にも Ursnif への感染を狙ったばらまき型メール（以下、Ursnif のばらまき型メール）を観測した※102。

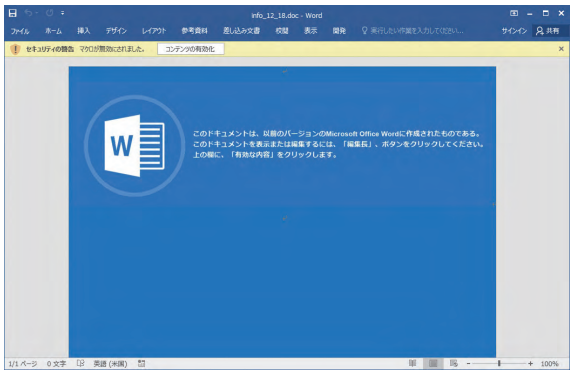
このばらまき型メールは、Emotet のばらまき型メールと同様、正規のメールへの返信を装うメールであった。メールにはパスワード付きの ZIP ファイルが添付されており、パスワードはメール本文に記載されていた。添付ファイルを解凍するとマクロ付き Word ファイルが出力され、利用者がそのファイルを開いて「コンテンツの有効化」ボタンをクリックすると Ursnif に感染させられる※77。Ursnif のばらまき型メールの例を図 1-2-20（次ページ）に、Ursnif のばらまき型メールの添付ファイル内にある Word ファイルの例を図 1-2-21（次ページ）に示す。

(3) Get2 Downloader と呼ばれるウイルスを使用し、別のウイルスへの感染を狙ったばらまき型メール

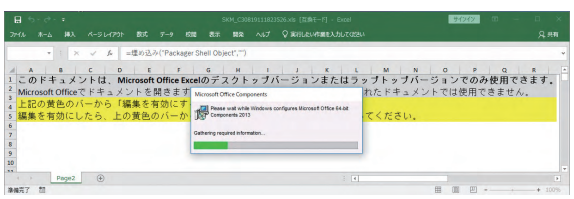
IPA は 2019 年 12 月に、Get2 Downloader と呼ばれるウイルスを使用し、別のウイルスへの感染を狙ったばらまき型メール（以下、Get2 Downloader のばらまき型メール）を観測した。Get2 Downloader のばらまき型メールにはマクロ付き Excel ファイルが添付されている。Excel ファイルのマクロを有効化すると Windows のプログレスバーのような画面が表示され（次ページ図 1-2-22）、何かのインストールを行っているように見える。しかし、実際は Get2 Downloader が Excel ファイルから端末へ設置、実行されており、更に別のウイルスがダウンロードされる。セキュリティベンダによると、海外の事例では、端末を遠隔操作する「FlawedGrace」「FlawedAmmyy」「SDBbot」と呼ばれる RAT が、Get2 Downloader が実行されることでダウンロードされたという※116。しかし、日本でこれらのウイルスがダウンロードされた事例は確認



■図 1-2-20　Ursnif への感染を狙うばらまき型メールの例
(出典)IPA「サイバー情報共有イニシアティブ(J-CSIP)運用状況[2019 年 10 月～ 12 月]※102」



■図 1-2-21　Ursnif への感染を狙うばらまき型メールの添付ファイル
(出典)IPA「サイバー情報共有イニシアティブ(J-CSIP)運用状況[2019 年 10 月～ 12 月]」



■図 1-2-22　Excel ファイルのマクロを有効にした際の画面
(出典)IPA「サイバー情報共有イニシアティブ(J-CSIP)運用状況[2019 年 10 月～ 12 月]」

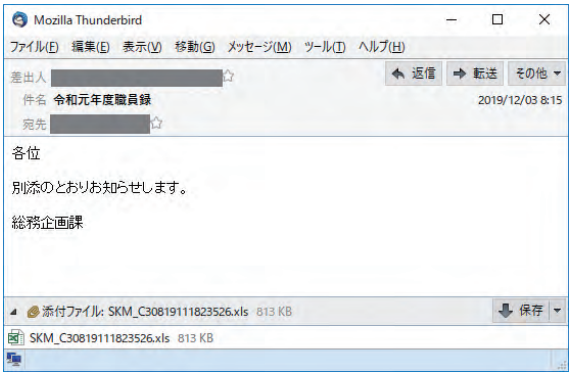
されておらず、日本で使用された Get2 Downloader のばらまき型メールから最終的に感染させられるウイルスの詳細は不明である。また、Get2 Downloader のばらまき型メールでは正規のメールへの返信を装う手口は見られず、メール本文がない、または数行程度の簡素な内容であった※102。図 1-2-23、図 1-2-24 に Get2 Downloader のばらまき型メールの例を示す。

(4) ばらまき型メールへの対策

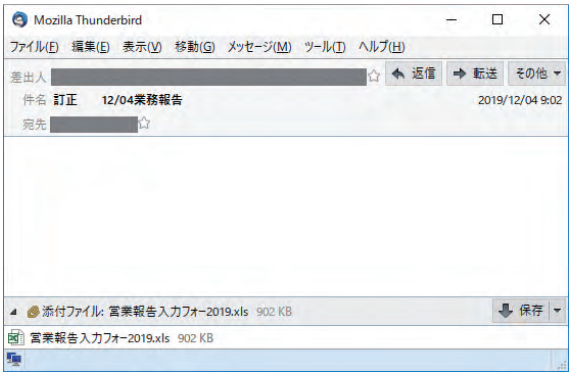
ばらまき型メールの攻撃者は、ウイルスに感染させる確率を上げるために様々な工夫を凝らしており、常に新たな手口で攻撃してくる可能性がある。セキュリティソフトの活用、スパムメール対策、メール受信者の自己防衛等の対策を実施し、多層的な防御を行うことが重要である。

(a) 一般利用者における対策

次に示す基本的な対策は、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。



■図 1-2-23　Get2 Downloader のばらまき型メールの例 1
(出典)IPA「サイバー情報共有イニシアティブ(J-CSIP)運用状況[2019 年 10 月～ 12 月]」



■図 1-2-24　Get2 Downloader のばらまき型メールの例 2
(出典)IPA「サイバー情報共有イニシアティブ(J-CSIP)運用状況[2019 年 10 月～ 12 月]」

- 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
  受信したメールに疑問や不審感を抱いた場合は、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の確認や、当該メールの送付有無を問い合わせてみる。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、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 ファイルや Excel 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を持てない Word や Excel 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 の設定でマクロの自動実行を無効化する。

(b) 組織・企業における対策

組織・企業におけるばらまき型メールに対する対策は、「1.2.1 (4) 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。

1.2.6 個人をターゲットにした騙しの手口

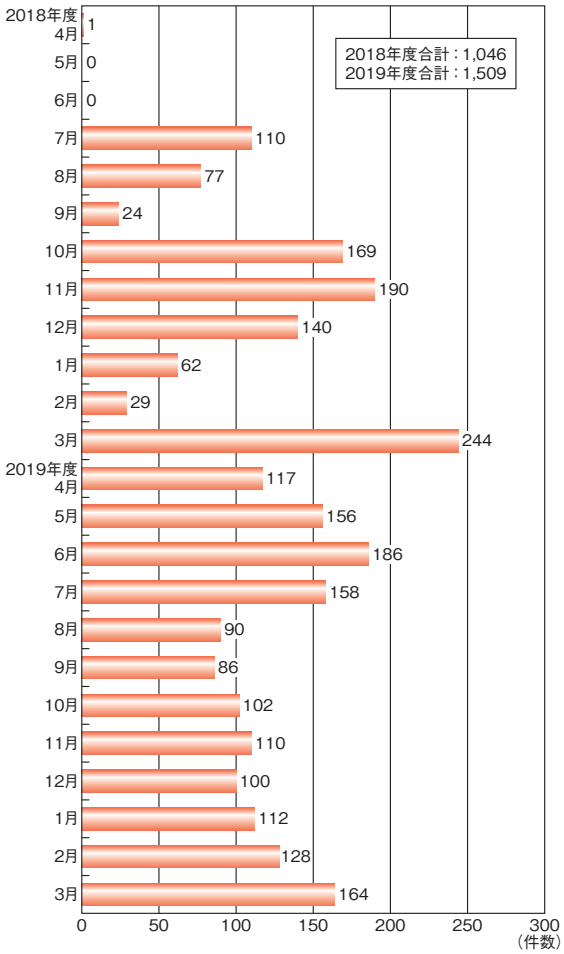
2019 年度は、個人を狙って騙そうとする手口による被害が目立った。本項では、騙しの手口を「遭遇するきっかけとなるサービス(SMS、メール、Web ブラウザ、アプリ)」別に、手口事例や対策を紹介する。また、最後に騙しの手口に共通の対策を解説する。

(1) SMS をきっかけとする手口

スマートフォンやタブレット端末 (以下スマートフォン) が普及し、企業からの認証コードや連絡事項の伝達手段として SMS (Short Message Service) の利用が拡大している中、それに乗じた騙しの手口が確認されている。

(a) 宅配便の不在通知を装う SMS

2019 年度も、宅配便の不在通知を装った偽の SMS を用いる手口で、被害が続いている。2019 年度、IPA の安心相談窓口には、昨年度を大きく上回る 1,509 件の相談が寄せられた(図 1-2-25)。



■図 1-2-25 宅配便の不在通知を装う SMS に関する月別相談件数推移(2018 ～ 2019 年度)

本件に関する相談は、2017 年度から確認されているが、その間、手口の詳細が変化し続けている。2019 年 5 月と 12 月、新たな手口が確認されたとして、JC3 が注意を呼びかけた※117。2020 年 2 月には、IPA が「安心相談窓口だより」で改めて注意喚起した※118。

(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、宅配便業者の正規サイトを模した偽サイトへ誘導する。

偽サイトは、当初は佐川急便株式会社を装うものであったが、その後、ヤマト運輸株式会社、日本郵便株式会社を装う事例も確認されている。

偽サイトでは、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、この後の手口が異なる。

Android の場合、偽サイトにアクセスすると、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。偽サイトに記載の手順に従って不正アプリをインストールすると、被害につながる(図 1-2-26)。

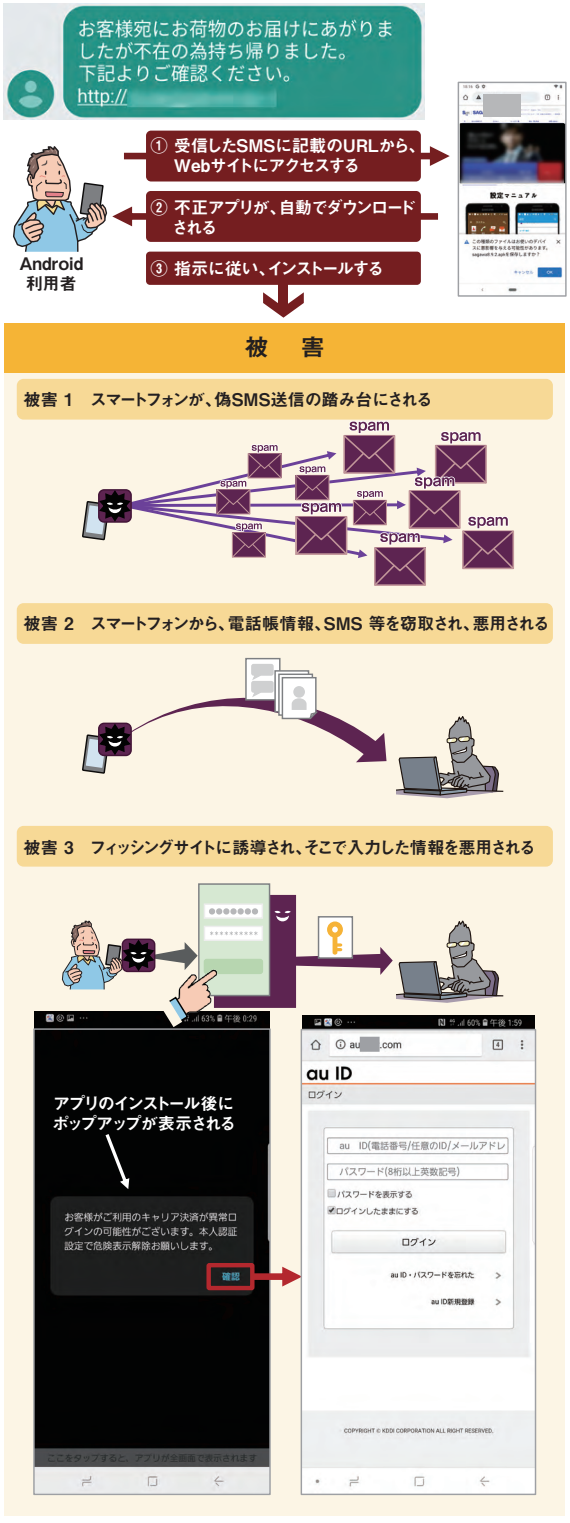
iPhone の場合、偽サイトにアクセスすると、フィッシングサイトが表示される。サイトの指示に従って「電話番号とキャリア決済の認証コード」や「Apple ID とパスワード」等、情報を入力すると、被害につながる。

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。

①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。

②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悪用される。

③銀行や携帯通信会社を装ったポップアップメッセージから、フィッシングサイトへ誘導される場合がある。



■図 1-2-26　宅配便の不在通知を装う SMS の手口と被害(Android の場合)

上記の Android の被害②については、以下のような相談事例が IPA に寄せられている。

- 携帯通信会社が提供するキャリア決済サービスにて、身に覚えのない請求が発生した。
- 自身が所有しているアカウントを不正使用された。
- フリーマーケットサービス、後払い決済サービス、その他のアカウントサービス等にアカウントを勝手に作成され、不正使用された。

このような被害は、電話番号と SMS に届く認証コードを窃取することにより、サービスの新規登録や利用時等の本人確認を突破されていることによるものと推測され

る。後払い決済サービスについては、Gardia 株式会社が、当該手口をきっかけとして、Visa 加盟店で利用できるプリペイドカードである「バンドルカード」の「ポチっとチャージ」という後払い決済方法が第三者に不正使用される事例が発生しているとして、注意喚起した※119。また、アカウントサービスについては、当該手口の被害者の電話番号で作成した PayPay のアカウントに、別途入手した他人のクレジットカード情報を登録して不正使用したという事例が報道された※120。

Android の被害③は、2019 年度に一時期確認された手口である。不正アプリをインストールすると、偽の警告メッセージが表示され、すぐに対処が必要であるとしてフィッシングサイトに誘導される。IPA での検証において、あらかじめ銀行アプリがインストールされていた場合は銀行を装うメッセージ、大手携帯通信会社の SIM カードを利用していた場合は携帯通信会社を装うメッセージが確認されたことから、スマートフォン内の状況に応じて警告内容と誘導先を変えているものと推測される。

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。

①「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。

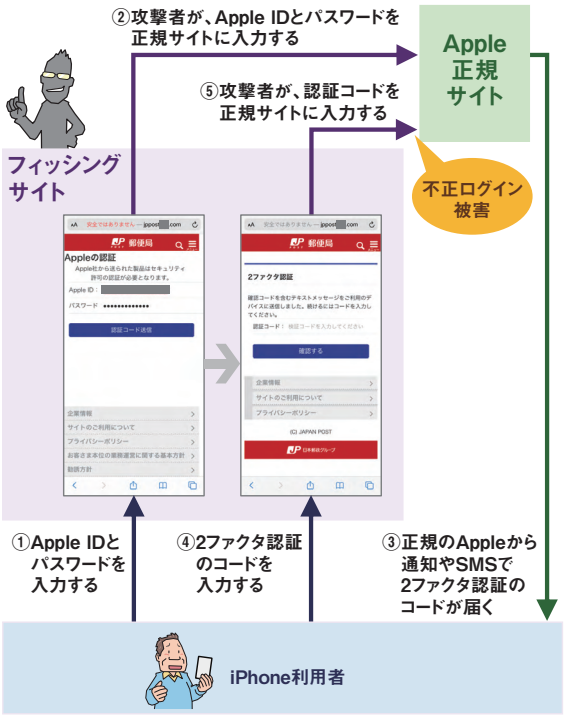
②「Apple ID とパスワード」を入力した場合、iCloud 等の Apple のサイトに不正ログインされる。

上記の iPhone の被害②については、「2 ファクタ認証」と呼ばれる Apple ID での多要素認証を設定している場合は、ID とパスワードのみでは不正ログインはされない。

しかし、2019 年度には、フィッシングサイトが 2 ファクタ認証の認証コードをも入力させるものに変化したため、2 ファクタ認証を設定している場合でも被害に遭うケースが出てきている（図 1-2-27）。

2 ファクタ認証の認証コードは、正規サイトに ID とパスワードを正しく入力すると発行される。そのため、攻撃者は、被害者がフィッシングサイトに ID とパスワードを入力したことを確認した後、すぐにその情報を使い正規サイトに入力して認証コードを発行させていると考えられる。ID とパスワードの詐取から認証コードの発行までが短時間で行われることから、攻撃者側の処理が自動化されている可能性も推測される。

この宅配便の不在通知を装う手口は、前述の Android の不正アプリに一時期フィッシングサイトへの誘導機能が追加されたことや、iPhone のフィッシングサイトが 2 ファクタ認証コードをも詐取する機能が追加されたこと等からも



■図 1-2-27　2 ファクタ認証コードを入力させるフィッシングサイトの手口の例（iPhone の場合）

わかるように、内容が変化し続けている点に注意が必要である。

2020 年 2 月には、この手口で用いられる Android の不正アプリから、偽の不在通知の SMS ではなく、新型コロナウイルスに関連した内容の SMS をばらまく事例が確認された※121。JC3 によれば、「新型コロナウイルスによる肺炎が広がっている問題で、マスクを無料送付確認をお願いします」（原文ママ）という文で、フィッシングサイトに誘導するものであったという。

（イ）対処

Android で不正アプリをインストールした場合、以下の対処を推奨する。

①スマートフォンを機内モード（Wi-Fi も OFF）にして、ネットワークから遮断する。

②設定画面のアプリケーション一覧から、不正アプリをアンインストールして、必要なデータをバックアップする。

③スマートフォンを初期化する。

④Google アカウント、及びスマートフォンで利用している SNS 等のサービスのアカウントのパスワードを変更する。

⑤キャリア決済の不正使用がないか、携帯通信会社に確認する。

⑥アプリのインストール以降、フリーマーケットサービス、後払い決済サービス、アカウントサービス等から、登

録や変更に関するメールやSMSが届いていた場合は、不正使用がないか等を当該サービス事業者に確認する。

iPhoneやAndroidで、フィッシングサイトに情報を入力してしまった場合は、入力した内容に応じて対処が必要となる。

- IDとパスワードを入力した場合は、パスワードを変更し、不正使用がないか等を確認する。
- 認証コードを入力した場合は、その認証コードの発行元のサービス事業者に相談する。
- キャリア決済等、決済サービスを不正使用された場合は、その決済の支払先（ショッピングサイト等）のサービス事業者にも相談する。

(b)送信元を偽装して携帯通信会社等を装うSMS

携帯通信会社や大手ショッピングサイト等を装うSMSによるフィッシングの手口において、送信元（Sender ID）を偽装して送信するケースが確認されている。2019年度、フィッシング対策協議会より事例が紹介された※122ほか、独立行政法人国民生活センターとJC3も注意喚起を行った※123。

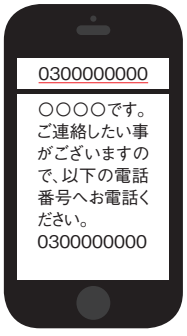
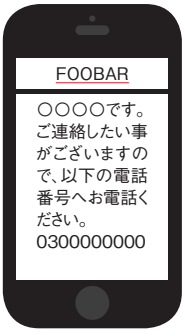
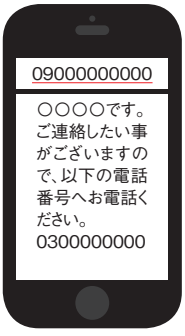
(ア)手口

SMS送信サービスのうち、国際網を経由するSMS配信では、発信者番号表示を任意のアルファベットにすることが、審査なしで可能である。これを悪用すると、実在する企業を装うことや、匿名にすることができる。このことは、フィッシング対策協議会より指摘されている※124（表1-2-4）。例えば、正規サービスが発信者番号表示にアルファベットを用いている場合、悪意ある第三者に同一文字列を使用されると、正規のSMSと偽のSMSがアプリ上の同一スレッドに表示されるため（図1-2-28）、真偽の判断が一層困難になると考えられる。

偽のSMS内のリンク先にアクセスしてしまうと、正規サイトを模したフィッシングサイトに誘導される。携帯通信会社を装う手口では、フィッシングサイトに、携帯通信会社のアカウントサービスのログインID・パスワード・暗証番号等を入力することで、キャリア決済を不正使用される被害が確認されている。

(イ)対処

フィッシングサイトでパスワードや認証コードを入力した場合は、すぐにパスワードを変更し、サービスの提供元に相談することを推奨する。

	国内直接接続のSMS配信	国際網を経由したSMS配信	携帯電話端末からのSMS配信
発信者番号表示	日本の電話番号 （例：03-0000-0000） 携帯キャリア毎の特別番号 （例：50000）	海外の電話番号 （例：+1 000-000-0000） アルファベット （例：FOOBAR）	携帯電話番号 （例：090-0000-0000）
発信者番号登録・変更	契約者が自由には登録・変更できず、事前申請が必要	契約者が任意のタイミングで自由に登録・変更することが可能	携帯キャリアからの払い出しのみ
利用審査の厳格性	現在、審査をしないまま偽名や匿名での申込者に提供している事業者が存在しない	審査がなく偽名や匿名での申込者へ提供する事業者が存在する	端末レンタルサービス等で十分な審査を実施しないまま提供する事業者が存在する
利用者の対策	発信者番号はWebサイト運営者が事前に告知している番号と異なるSMSを受信した場合、フィッシングの可能性を疑い慎重に行動する	Webサイト運営者を騙ったフィッシングの可能性を疑い、慎重に行動する	Webサイト運営者を騙ったフィッシングの可能性を疑い、慎重に行動する
発信者番号の表示イメージ			

■表1-2-4　SMSの配信経路ごとの特徴
（出典）フィッシング対策協議会「フィッシングレポート2019※125」を基にIPAが編集

■図 1-2-28 携帯通信会社からの正規の SMS が届くスレッドに偽の SMS が届いた場合のイメージ
(出典)独立行政法人国民生活センター「携帯電話会社をかたる偽 SMS にご注意!ーあなたのキャリア決済が狙われていますー※126」を基に IPA が編集

(c) 金融機関を装う SMS

2019 年 9 月に不正送金被害が急増し、10 月及び 11 月にも被害が多発した。金融機関を装うフィッシングのメールや SMS が多数確認されているとして、警察庁、金融庁、全国銀行協会、JC3、フィッシング対策協議会が注意喚起した(「1.1.2(3)フィッシングによる被害」参照)。

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、電話番号等一様ではなく、各インターネットバンキングの認証システム仕様に合わせて情報を詐取していると考えられる。また、ワンタイムパスワード、乱数表等の多要素認証の情報も詐取する。これらを奪われることで多要素認証による本人確認も突破され、被害につながっている※127。

フィッシングサイトの URL については、HTTPS や JP ドメイン名(日本を表す「.jp」で終わるドメイン名)が使用されているケースも確認されており、正規サイトであると誤認させやすくする狙いであると考えられる※128。

ターゲットとなった金融機関は、都市銀行のみならず、ゆうちょ銀行、信用金庫、地方銀行、ネット銀行等も確認された。

不正送金被害につながる SMS の手口は、金融機関を装うものだけでなく、携帯通信会社やショッピングサイト等を装う事例もある。例えば、携帯通信会社を装った内容の SMS から携帯通信会社の正規サイトを模したフィッシングサイトへ誘導し、当該サービスのアカウント情報を入力させた後、本人確認のためと称して金融機関のアカウント情報も求めてくるといったものである※129。

(d) SMS をきっかけとする手口に共通の対策

自身にとって身近な企業やサービスを装う手口では、不審に思うこと自体が難しい場合もあると考えられる。また、不審に思った場合でも、以下のような理由から、SMS や誘導先の Web サイトの真偽を判断することは容易ではない。

- SMS の送信元情報は偽装される場合があり、かつ、偽装されているかどうかは受信側では確認できない。
- SMS の文面が、自然な日本語で書かれていて違和感がない場合がある。
- 偽サイトの URL が正規サイトに似せて作られている場合がある。一方、正規サイトでは、ドメインを複数保有して使い分ける等により、正しい URL が覚えにくい場合がある。
- 誘導先の偽サイトが、正規サイトを基に作られることで、デザイン等から受ける印象が正規サイトと変わらない傾向にある。

安全のために日頃から、SMS 内のリンクは基本的に利用しないことを推奨する。よく利用する Web サイトは、正しいと確認できている URL をあらかじめ「お気に入り」(ブックマーク)に登録しておき、それを使用してアクセスすることが望ましい。もし SMS 内のリンクを使用する必要がある場合は、URL が正規のものであることを慎重に確認していただきたい。

SMS の真偽の判断に迷った場合は、確かな情報源を使って確認する。正規サイトでは、「SMS による不在通知は行っていない」「SMS から Web サイトに誘導することはない」等、注意喚起されていることが多い。

なお、真偽を確認しようとして、SMS へ返信することや電話すること、リンク先にアクセスすることは、被害につながる可能性があるため、行ってはならない。

(2) メールをきっかけとする手口

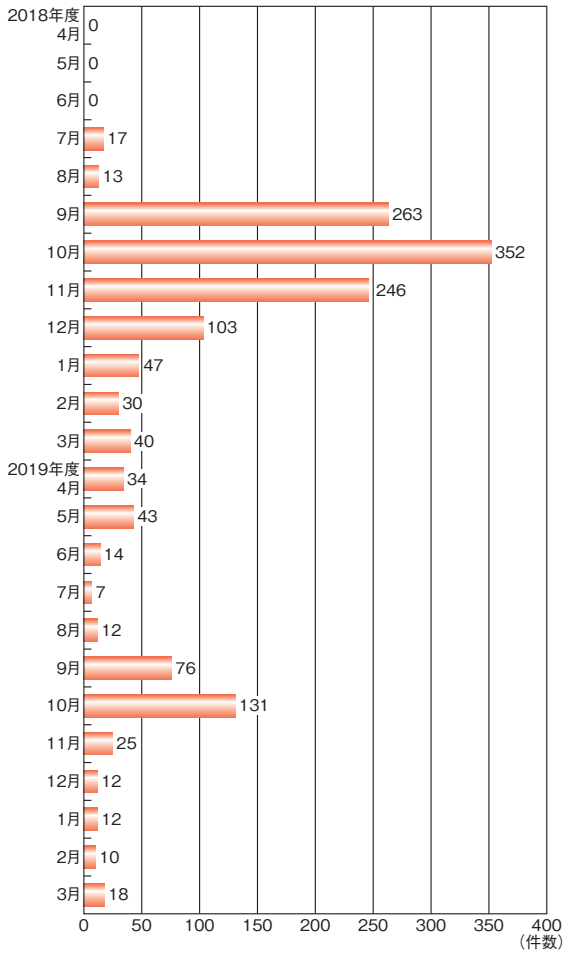
メールを用いる手口は、フィッシングメール、ばらまき型

メール、架空請求メール等様々存在するが、ここでは、人間の心理を突いた文章で騙す手口について紹介する。

(a)仮想通貨を要求する脅迫メール

2019 年度も、「あなたの性的な映像をばらまく」等と騙して、仮想通貨を要求する脅迫メールが多数出回った。

2019 年 10 月、IPA では、安心相談窓口への当該相談が増加したことを受けて（図 1-2-29）、改めて注意喚起を行った[※130]。



■図 1-2-29　仮想通貨を要求する脅迫メールに関する月別相談件数推移（2018 ～ 2019 年度）

(ア)手口

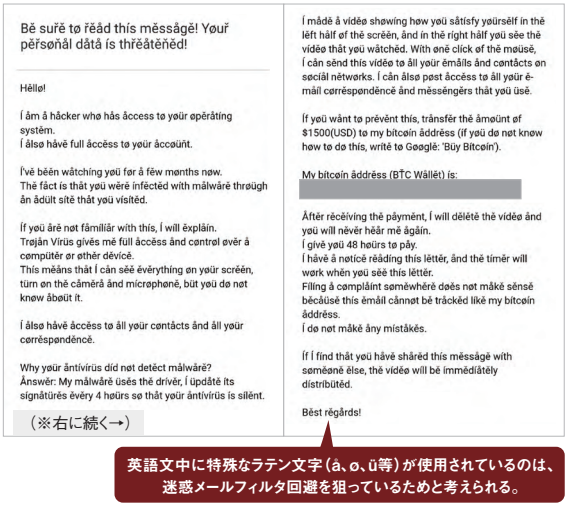
この手口のメールは、脅迫の内容や使用言語に多くのバリエーションがあるが、内容の要旨は当初から変わらない（図 1-2-30、図 1-2-31）。

①ハッカーや調査員等であると名乗り、他人に知られたくない情報（「アダルトサイトを閲覧している姿」「不正を行っている証拠」等）や、家族や友人の連絡先情報等を盗んだと騙す。

②盗んだ情報を連絡先等へばらまかれたくなければ、制限時間内に Bitcoin（ビットコイン）や Dash（ダッシュ）等の仮想通貨を送金するよう要求する。

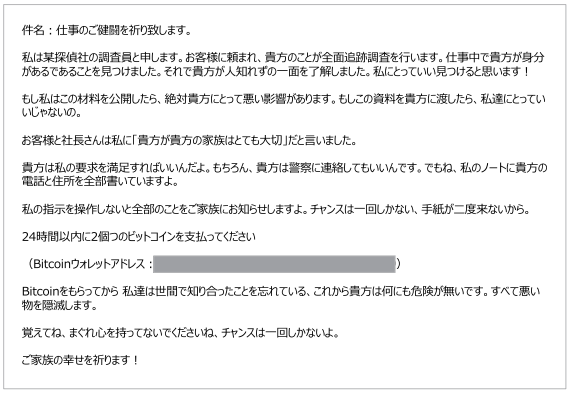
③メールの送信元が、メール受信者自身のアドレスになっている場合がある。

④メールの件名や本文に、パスワードが一つ書かれている場合がある。



英語文中に特殊なラテン文字（á、ø、ü等）が使用されているのは、迷惑メールフィルタ回避を狙っているためと考えられる。

■図 1-2-30　仮想通貨を要求する英語の脅迫メールの例


件名：仕事のご健闘を祈り致します。

私は某探偵社の調査員と申します。お客様に頼まれ、貴方のことが全面追跡調査を行います。仕事中で貴方が身分があるであることを見つけました。それで貴方が人知れずの一面を了解しました。私にとっていい見つけると思います！

もし私はこの材料を公開したら、絶対貴方にとって悪い影響があります。もしこの資料を貴方に渡したら、私達にとっていいじゃないの。

お客様と社長さんは私に「貴方が貴方の家族はとても大切」だと言いました。

貴方は私の要求を満足すればいいんだよ。もちろん、貴方は警察に連絡してもいいんです。でもね、私のノートに貴方の電話と住所を全部書いていますよ。

私の指示を操作しないと全部のことをご家族にお知らせしますよ。チャンスは一回しかない、手紙が二度来ないから。

24時間以内に2個つのビットコインを支払ってください

（Bitcoinウォレットアドレス：[redacted]）

Bitcoinをもらってから 私達は世間で知り合ったことを忘れている、これから貴方は何にも危険が無いです。すべて悪い物を隠滅します。

覚えてね、まぐれ心を持ってないでくださいね、チャンスは一回しかないよ。

ご家族の幸せを祈ります！

■図 1-2-31　仮想通貨を要求する日本語の脅迫メールの例

盗んだとする情報がメール内に記載・添付されていた事例や、支払いに応じなかったために情報がばらまかれた事例等は、確認されていない。このことから、「セクストーション（性的脅迫）[※131]」の手口を模して、根拠のない内容で脅迫していると推測される。

メールに書かれていたパスワードについては、IPA への相談事例では、受信者が設定したことのあるパスワードであった場合と心当たりがない場合があった。このことから、漏えいデータ等、何らかの方法でパスワードを入手しているケースもあると推測されるが、詳細は不明である。

(イ) 対処

当該メールが届いた場合は、メールを削除するだけで問題ない。現在使用しているパスワードが書かれていた場合は、すぐにパスワードを変更し、併せて、そのパスワードを使っていたサービスへの不正ログインがないか確認することを推奨する。

(b) メールをきっかけとする手口に共通の対策

見慣れないメールが届いた場合、まずは、真偽を確かめるようにしたい。本物であるという確証がない状況では、すぐに内容に反応しないことが重要である。

他者に相談しにくい心理に付け込む手口の不審メールを受け取った場合、孤立してしまい、冷静な判断が難しくなる場合も考えられる。身近な人への相談がためらわれる場合は、インターネット上に類似の手口に関する注意喚起がないか検索するという方法がある。

不審メールのフィルタリングサービスや、メールのチェック機能を持つセキュリティソフトを使用して、判断しやすくするのも一案である。

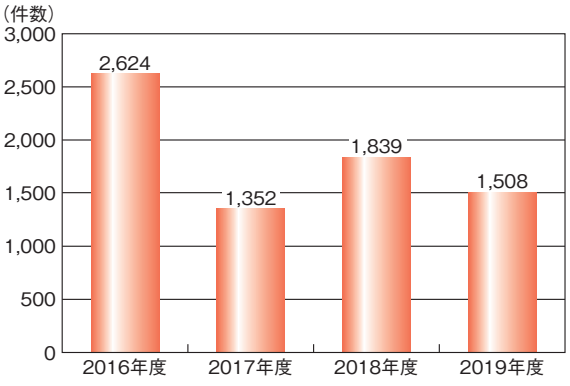
(3) Web ブラウザの表示をきっかけとする手口

パソコンやスマートフォンでインターネットを利用する際に、アクセスする Web サイトに注意していても、攻撃者の罠に遭遇することがある。

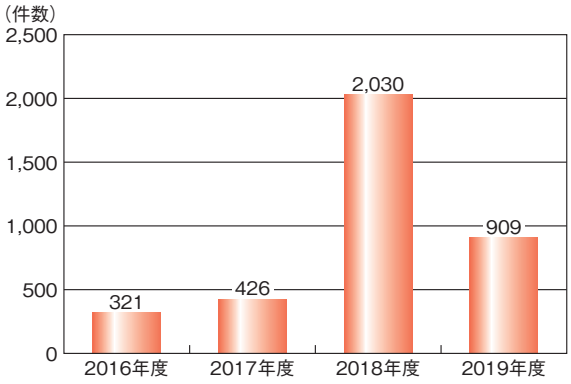
(a) 偽のセキュリティ警告

パソコンで Web サイト閲覧中に、突然「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、有償のサポート契約やセキュリティソフト購入をしてしまう被害が、後を絶たない。

2019 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、1,508 件(図 1-2-32)、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、909 件だった(図 1-2-33)。



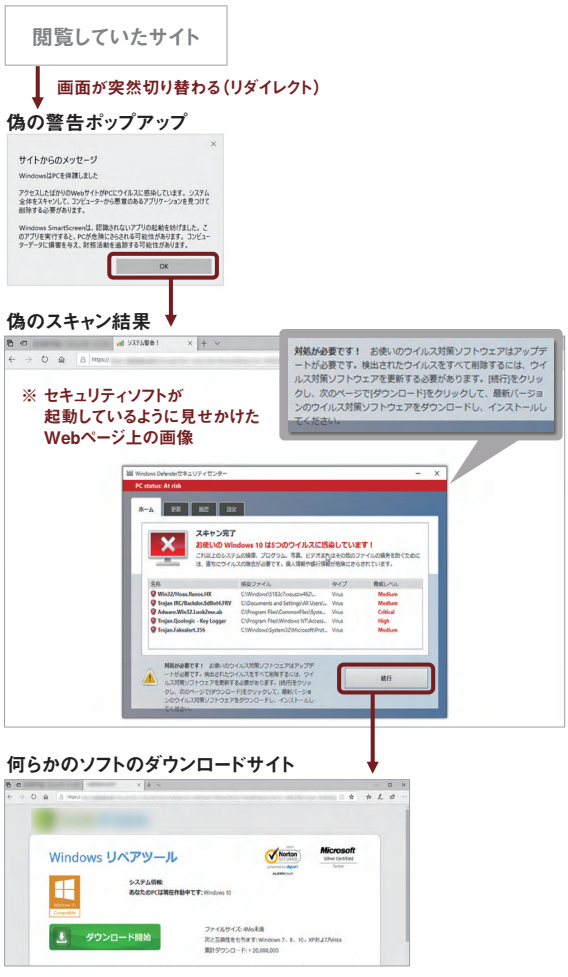
■図 1-2-32　偽警告に関する年度別相談件数



■図 1-2-33　偽セキュリティソフトに関する年度別相談件数

(ア) 手口

「偽警告」と「偽セキュリティソフト」の手口は、閲覧していたWebサイトから突然画面が切り替わり、偽のセキュリティ警告画面(図 1-2-34)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



■図 1-2-34　偽のセキュリティ警告画面の例(ソフトに誘導されるケース)

損する」等と、根拠のない内容で不安を煽る。

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警告画面に記載の電話番号に電話をかけると、オペレーターから至急パソコンの確認が必要であると説明される。

②オペレーターの指示に従い遠隔操作ソフトをインストールして接続を許可すると、遠隔操作でパソコン内の画面を示しながら危険な状況であると脅される。

③修復作業や今後の保守サポートの契約を持ちかけられ、クレジットカードやプリペイドカード等での支払いを求められる。

④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場合もある。

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

①警告画面に表示された問題を解決するためとして、「無料のセキュリティソフト」等と称するものをインストールするよう促される。

②ソフトウェアをインストールして実行すると、診断結果が表示され、対処には有償版が必要であるとして、購入画面へ誘導される。

近年は、「偽警告」と「偽セキュリティソフト」を組み合わせた手口も確認されている。例えば、有償ソフトウェアを購入させた上で、更にアクティベーション（ソフトウェアを使用可能にする操作）のために必要であるとして電話をかけさせ、サポート契約を迫る等がある。

(イ)対処

偽のセキュリティ警告が表示された場合は、Web ブラウザを閉じるだけで問題はない。もし、通常の操作で画面を閉じることができない場合は、Windows であれば、タスクマネージャーから Web ブラウザを終了する、Mac であれば、「強制終了」ウィンドウから Web ブラウザを終了するという方法がある。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。

利用者自身やオペレーターが詳細不明のソフトウェアをインストールした場合は、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（Windows の「システムの復元」や、Mac の「Time Machine」で作成しておいたバックアップからの復元）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していただきたい。

また、Microsoft 社では、当該手口に関する専用ページで手口や事例を紹介し、被害報告も受け付けている※132 ため、活用することも一案である。

(b)アプリ誘導

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は、パソコンだけでなく、スマートフォンでも存在する。

2019 年 9 月、IPA は、相談件数が前年度に比べて増加したことと、手口に変化が見られたことから、「安心相談窓口だより」で注意を呼びかけた※133。

(ア)手口

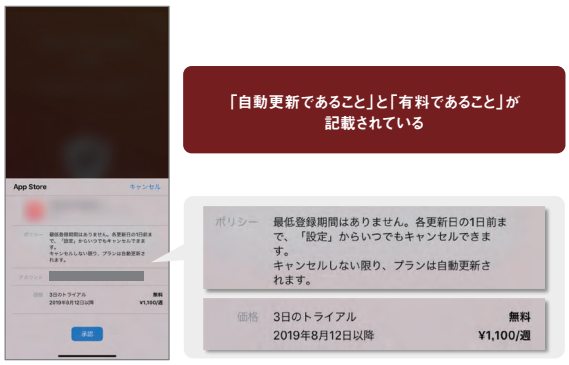
スマートフォンでの手口は、警告画面に表示された問題は「セキュリティアプリ」で解決できるとして、公式マーケット上のアプリに誘導するというものである（図 1-2-35）。

この手口の目的は不明だが、「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る。なお、偽のセキュリティ警告の出力元（広告主）と誘導されるアプリの開発元との関係は判明していない。

従来、この手口では、無料アプリに誘導されることが多かった。しかし、2019 年度に IPA へ寄せられた相談事例では、自動継続課金※134 の有料アプリに誘導さ

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

れるケースが増えている（図 1-2-36）。また、その利用料金は、週ごとに 1,000 円以上等、短い利用期間で高額な設定になっている例が多くみられた。アプリの初回起動時に表示される自動継続課金の確認メッセージに対し、無料アプリだと誤解して承認してしまうと、トライアル期間終了後に意図しない利用料金が発生することになる。



■図 1-2-36　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。なお、アンインストールのみでは自動継続課金は解約にならない点に注意が必要である。自動継続課金に登録した場合は、iPhone の場合はサブスクリプションの解約、Android の場合は定期購入の解約も実施する。

（c）Web ブラウザの表示をきっかけとする手口に共通の対策

パソコンやスマートフォンで偽のセキュリティ警告が表示される原因は、Web サイト内の広告枠に配信された不正プログラムを含む広告、あるいは Web サイトに故意または改ざんにより存在する不正プログラムが、偽の警告画面へリダイレクト（自動転送）していること等が考えられる。これは不審なサイトにアクセスしないことのみでは回避が困難であり、インターネットを利用していれば誰でも遭遇する可能性がある。

危険な状況であると思わせ、慌てるように仕向ける手口では、危機への対処をしようとして、目の前に示された情報をそのまま信じて行動してしまう場合も考えられる。

Web サイトの閲覧中に警告画面が表示された際には、Web ブラウザやセキュリティソフトによる本物の警告である可能性と、偽物である可能性の両方があることを想定した対応が必要である。特に、電話をかけることや、ソフトウェアやアプリの入手を促す場合は、偽物である可能性が高いため、警戒したい。

もし、警告画面の真偽の判断に迷った場合は、セキュリティソフトや、パソコン、スマートフォンのサポート窓口に相談する等、信頼できる情報源で確かめるようにしていただきたい。

日頃から、使用している Web ブラウザやセキュリティソフトによる正規の警告画面を把握する、セキュリティソフトのサポート窓口の連絡先を控える等の備えをしておくと、警告に遭遇した際の適切な対処につながると考えられる。

（4）アプリのインストールをきっかけとする手口

スマートフォンは、パソコンに比べて、第三者がアプリを勝手に入れ込むことが難しい。そのため、利用者を騙してインストールへ誘導する手段が用いられることが多くなる。

不正アプリは、審査をすり抜けて公式マーケットで配布される場合と、公式マーケット以外のサイトで配布される場合がある。

（a）公式マーケット上で配布された不正アプリ

2019 年度も、Android の公式マーケットである Google Play と、iPhone の公式マーケットである App Store で、不正アプリが確認された。

以下に、2019 年度に確認された、利用者を騙すタイプの不正アプリを紹介する。

- 正規セキュリティアプリを模した偽アプリ（Android）
  2019 年 8 月、日本と韓国の利用者を対象とした、セキュリティ関連のアプリを装ったスパイウェアを発見したと発表された※135。そのうち、日本を対象としたものは、日本のセキュリティアプリの偽物で、公式マーケットで 2 個確認された。アプリは、IMEI（International Mobile Equipment Identifier：国際移動体装置識別番号）や電話番号といった情報を収集し、SMS 等のメッセージの窃取をするものであったという。
- 正当な機能と不正機能を併せ持つアプリ（Android）
  同じく 2019 年 8 月、Radio Balouch という不正アプリを発見したと発表された※136。バローチスターンという地域の伝統音楽のストリーミングラジオアプリとして実際に機能するが、利用者の個人情報を盗めるようになっていたという。このアプリは、審査を通過して、2

度にわたり Google Play で公開されたとのことである。

- 正規アプリを装い、ギャンブル機能を隠し持つアプリ（Android、iPhone）

  2019 年 8 月、Google Play と App Store 上で、Google Play 及び App Store が定めるガイドラインを満たしていないギャンブル機能を隠し持つ偽アプリを数百件発見したと発表された[※137]。それらのアプリは、正規アプリの名前や機能を真似て様々なカテゴリで公開されていたという。

2019 年 11 月、Google LLC は、Google Play の安全性を確保するために、複数のセキュリティベンダと「App Defense Alliance」を結んだと発表した[※138]。こうした取り組みにより、今後、公式マーケットでの不正アプリ配布の減少が期待される。

(b) 公式マーケット以外で配布された不正アプリ

不正アプリは、公式マーケット以外の場所で配布されることが多い。

Android は、Google Play 以外の提供元からもアプリを入手できるため、これを悪用して不正アプリが配布される。「1.2.6 (1) (a) 宅配便の不在通知を装う SMS」の手口における不正アプリもこれに該当する。

iPhone は、基本的には App Store 以外からアプリを入手できないように制限されている。これに対し、「脱獄（Jailbreak）」と呼ばれる不正改造により制限を解除するよう誘導した上で不正アプリをインストールさせる手口がある。

2019 年 12 月、IPA は、安心相談窓口に寄せられたセクストーション（性的脅迫）に関する相談において、脱獄なしで iPhone に不正アプリをインストールさせる手口が確認されたことから、注意を呼びかけた[※139]。

IPA が確認した iPhone でのセクストーションの手口は、以下のような流れであった。

①正規の SNS アプリでビデオ通話をする

LINE で見知らぬ女性から突然コンタクトがある。親しくなった後、ビデオ通話等でお互いの性的な姿を見せ合うことをもちかけられる。

② App Store 以外からアプリを入手するよう誘導される

「LINE がつながりにくくなった」等の理由から他のアプリを紹介するとして、App Store 以外の Web サイトの URL を案内される。指示された Web サイトからアプリをインストールし、アクセス権限を許可する。

③ビデオ通話の動画を友人や知人にばらまくと脅され、金銭を要求される

LINE で見知らぬ男性から連絡があり、ビデオ通話の動画を録画していると伝えられる。iPhone の連絡先に登録している知人等にばらまかれたくなければ 20 万円を支払うよう要求される。また、情報を手にしている証拠として、録画された動画と連絡先のデータが送られてくる。

このセクストーションの手口で使用された不正アプリは、App Store で配信されているものではなかったが、脱獄せずにインストールが可能であった（図 1-2-37）。これは、企業や組織が独自に開発しその内部のみで利用するアプリを配信するための仕組みである「Apple Developer Enterprise Program[※140]」を悪用しているものと推察される。

この不正アプリをインストールし、連絡先データへのアクセス権限を与えることによって、情報が攻撃者に窃取されると考えられる。

■図 1-2-37　App Store 以外から不正アプリをインストールする流れ

(c) アプリのインストールをきっかけとする手口に共通の対策

アプリが様々な開発者から数多く提供され、利用者がアプリをインストールすることが日常的になっている状況に乗じて、攻撃者は不正アプリへ誘導しようとしてくる。そのため、不用意にアプリを入手していると、思わぬ被害につながる恐れがある。

不正アプリによる被害を回避するためには、iPhone、Android どちらの場合も、原則としてアプリは公式マーケットから入手し、アプリを選ぶ際は開発元の信頼性やアプリの機能、利用規約等を慎重に確認することが必要である。

Android については、アンチウイルス機能を持つセキュリティアプリがあるため、利用するのも一案である。

(5) 騙しの手口に共通の対策

人間の心理を突いて騙す手口への対策は、以下のとおりである。

①手口を知り、日頃の備えをする
②目にした情報の真偽は、確かな情報源で確かめる
③判断に迷ったら、信頼できる相手に相談する

「騙し」という、人間の脆弱性を標的とした攻撃は、被害を防ぐことが非常に難しい。そのため、被害に遭った場合の影響を小さくするための対策も行いたい。例として、以下のようなものがある。

- 多要素認証を利用することで、もしID・パスワードを伝えてしまった場合でも、不正ログインをされないようにする。
  ただし、多要素認証を利用していても、認証コードまで伝えてしまうと意味をなさない。騙しという手口に万能な対策ではないことには、注意したい。
- 利用しているサービスが備えているセキュリティ機能(ログインアラート等)を活用する。
- システムやデータの定期的なバックアップを実施することで、もしパソコンやスマートフォンの初期化が必要になった場合でも、復旧できるようにする。
- アカウントサービス等に紐づいている決済手段を把握し、不要であれば登録情報の削除や利用停止を行う。

上記の対策は、情報端末を所有する一人ひとりが行うことになる。しかし、情報セキュリティに対する意識や、知識を得る機会等には個人差がある。また、情報端末、特にスマートフォンは、利用者のすそ野が広く、例えば子どもや高齢者等のIT初心者がターゲットになる恐れもある。

個人を狙う手口という脅威に対しては、個人単位で対策するだけでなく、情報セキュリティの知識を持つ人々が中心となり、家族や友人、地域等のコミュニティで対策の輪を広げていくことも、必要と考えられる。

また、サービス提供者には、利用者が多様であることや攻撃傾向、人間心理等を踏まえた対応が望まれる。例として、アカウントサービスやショッピングサイト等で多要素認証が利用できるようにする、メール・SMS内にURLを記載しないことで偽メールの識別を容易にする※141、利用者が被害に遭ったときに相談できる窓口を設けて適切な対処方法を提供する等が挙げられる。

1.2.7 情報漏えいによる被害

2019年度も、多数の情報漏えい被害が発生している。本項では、外部からの攻撃、操作ミス等の過失、内部者の故意による不正、不適切な情報の取り扱いのいずれかを主な要因とする情報漏えい被害について述べる。

2020年1月に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※142」によると、2019年に個人情報の漏えい・紛失事故を公表した上場企業は66社86件、漏えいした個人情報は903万1,734人分に達した。なお、個人情報漏えいが発生した場合、現行法規においては、当局への通知は努力義務とされていたが、2020年6月に公布された「個人情報の保護に関する法律等の一部を改正する法律案」では、一定の条件を満たす場合については報告が義務化された(「2.7.4 (1) (c) 漏えい等報告の義務化(骨子II)」参照)。

(1) 外部からの攻撃による情報漏えい

株式会社マーケティングアプリケーションズの事例※143では、回答者へポイントを付与するアンケートモニターサービス「アンとケイト」への不正アクセスにより、メールアドレス、パスワード、生年月日、性別、電話番号、郵便番号、既婚状況、職業、業種、子どもの有無、世帯年収のほか、任意で回答した氏名、住所、金融機関の口座名義や番号、個人年収等を含む77万74件分の個人情報が流出した。

株式会社ホビーズファクトリーの事例※144では、2017年9月以前に同社が使用していたサーバへの不正なアクセスにより同社運営サイト「カードショップBIG-WEB」のユーザ登録情報6万3,587件が外部に流出していることが判明した。流出したのは2012年4月以前の登録情報で、ID、平文のパスワード、メールアドレスが含まれており、この情報を用いて不正にログインされた場合、氏名や送り先住所、電話番号等も取得された可能性がある。

株式会社現代ギター社の事例※145では、システムの脆弱性を突く不正アクセスにより、決済アプリケーションが改ざんされた状態となり、決済時に入力されたクレジットカードの名義や番号、有効期限、セキュリティコード等顧客133人分の個人情報が流出した恐れがある。更に、サーバ内にデータが残っていた1万9,328人分の氏名や住所、電話番号、性別、メールアドレス、暗号化されたログインパスワード等の個人情報が窃取された可能

性が判明した。

関西電力のグループ会社である株式会社関電アメニックスの事例※146では、従業員の端末がマルウェア「Emotet」に感染し、社外関係者のメールアドレス265件や社内関係者のメールアドレス183件、及びメール送信者の氏名が流出した可能性がある（Emotetについては「1.2.5(1)Emotetのばらまき型メール」参照）。

三菱電機株式会社の事例※147では、不正アクセスを受けて約200Mバイトに上る機密情報や個人情報を窃取され、外部に送信されていたことが判明した。原因は同社のマルウェア対策システムにおいて、修正プログラム公開前の脆弱性を突かれたとのことであった。監視や検知をすり抜ける高度な手法が用いられ、一部端末では送信されたファイルを特定するためのログが攻撃者によって消去されたことから調査に時間を要し検知から発表まで半年以上かかったとのことであった。

その他、外部からの攻撃によって情報漏えい被害が発生した主な事例を表1-2-5に示す。

(2) 過失による情報漏えい

認定個人情報保護団体である一般財団法人日本情報経済社会推進協会（JIPDEC）が2019年9月に公表した「（2018年度）『個人情報の取り扱いにおける事故報告集計結果』※166」によると、事故の発生原因としては「誤送付」が57.9%と最も多く、次いで「紛失」が20.6%となっている。

飲食店経営事業を行う株式会社ゼットンの事例※167では、店舗に予約した顧客の個人情報が保存された業務用ノートパソコン1台を、従業員が紛失した。このパソコンには予約時に告げられた氏名や企業名と電話番号が最大6万7,280件、うち最大1万475件にはメールアドレスが含まれていた。

茨城県稲敷市の事例※168では、タブレット端末型の水道管路台帳システムを紛失した。この端末には1万801件の加入者氏名と水道メーター器の設置場所、114件の電話番号が含まれていた。

横浜農業協同組合の事例※169では、顧客情報が記載された資料がインターネットを通じて外部に公開されていた。当該資料には、同組合へ貯金したことがあり、法人を含む顧客1万7,286人分の氏名や住所、電話番号、顧客番号、管理店舗名、取引開始日等が保存されており、特定の操作により閲覧することができた。同組合のWebサイトの更新作業中に操作を誤った可能性が高いという。

(3) 内部者の不正による情報漏えい

株式会社ブロードリンクの事例※170では、リース会社よりリース契約満了後に回収したハードディスクの破壊処分を受託していたにも関わらず、元従業員が破壊処分される予定のハードディスクを盗み出し、オークション等で売却していた。売却した機器は7,844台に及び、このうち3,904台についてはデータの記憶領域がある機器だった。オークションでのハードディスク購入者が、復元したデータの中に神奈川県の情報らしきデータを発見し、県に確認を依頼したことから発覚した。

NHKの事例※171では、受信料収納業務の委託先から受信契約者の個人情報が漏えいした。漏えいした情報には名古屋市と春日井市の受信契約者23人分の氏名や住所、電話番号、口座振替用の金融機関名等が含まれており、業務用携帯端末に表示される受信契約者情報を委託先社長が口頭で漏えいしたものであった。

(4) 不適切な情報の取り扱いによる情報流出

株式会社リクルートキャリアの事例※172では、「リクナビ」に登録された会員の個人データ9万5,590人のうち2万6,060人分が本人の同意なしに35社に提供されていた。対象となったのは同社が運営していた「リクナビDMPフォロー」という、就職情報サイトの閲覧履歴から、選考離脱や内定辞退の可能性をスコアリングし企業に提供するサービスだった。提供されたスコアを選考の合否判断の根拠には使用しないことを、サービス契約企業は約束していたとの事であったが、利用していた学生に大きな不安を引き起こした。

(5) 対策

それぞれの原因について、情報漏えい被害を発生させないための対策を以下に示す。

(a) 外部からの攻撃への対策

外部からの不正アクセス被害は、個人情報等の秘密情報を管理しているシステムの脆弱性や、当該情報にアクセスできるアカウントの管理不備が原因であるケースが多い。そのため、システムに脆弱性が存在したままの状態での運用とならないよう、利用しているソフトウェアの適切なアップデート等を心がけたい。また、アカウントについては、適切なアクセス権の設定やパスワードの管理を実施することはもちろん、アカウント所有者がフィッシング等により情報を詐取されないように適宜注意を促すことも重要である。

情報公表日	法人・団体名	漏えい内容・詳細・二次被害（悪用）等
2019 年 4 月 23 日	株式会社エーデルワイン	運営するオンラインショップに不正アクセスが発生し、顧客の個人情報が最大 3 万 1,231 件流出した可能性。セキュリティコードも含む。不正アクセスの原因はシステム内の脆弱性と考えられる※148。
5 月 13 日	株式会社ファーストリテイリング	運営するアパレルブランド「ユニクロ」及び「ジーユー」の通販サイトに対しパスワードリスト（リスト型）攻撃が発生し、顧客情報 46 万 1,091 件が流出した可能性。情報の一部には、クレジットカード情報も含む※149。
5 月 29 日	株式会社ヤマダ電機	運営する「ヤマダウエブコム・ヤマダモール」で不正アクセスが発生。ペイメントアプリケーションを改ざんされ、期間中に登録された顧客情報最大 3 万 7,832 件が流出。情報にはクレジットカード情報も含まれ、不正利用の可能性も確認※150。
6 月 4 日	株式会社サンポークリエイト	運営する EC ショップ「アネモネ」に対し外部から不正プログラムが混入、顧客データベースの情報及びクレジットカード情報が流出した可能性。クレジットカード情報にはセキュリティコードも含む※151。
7 月 3 日	株式会社 DigiBook	運営する「みんなのデジブック広場」に対し、不正アクセスが発生。顧客のクレジットカード情報 1 万 5,370 件が流出した可能性。攻撃はシステムの脆弱性を悪用。流出した情報の一部は不正利用の可能性※152。
7 月 4 日	J. フロントリテイリング株式会社・（株式会社ディンプル）	人材派遣業を営む株式会社ディンプル（J. フロントリテイリング子会社）のホームページの不正アクセス被害。サーバに保存されていた登録者の個人情報約 12 万件に流出の可能性。データは暗号化されており、発表時点までに流出の証跡は確認されていない※153。
7 月 23 日	株式会社金剛堂	運営する「金剛堂オンラインストア」において、システムの脆弱性を悪用したフォームジャッキングが行われ、クレジットカード決済を行った顧客情報 3 万 830 件が流出※154。
8 月 5 日	株式会社おもちゃ箱	運営するオンラインショップ「omochabakoWEBSTORE」が不正アクセスを受け、クレジットカード情報 210 件に流出の証跡。また 4 万 233 件のカード情報も流出の可能性。不正アクセスの原因はシステムの脆弱性を利用した、第三者による決済アプリケーションの改ざん行為。攻撃者は約 1 ヵ月に渡り登録情報を盗み続けていた※155。
8 月 7 日	株式会社アルペン	運営する顧客管理システムにおいてパスワードリスト型攻撃による不正ログインが発生。被害件数は最大で 3 万 8,954 件。43 万 930 ポイントが不正に利用された可能性。同社は対象アカウントのログインパスワードをリセットし、ユーザに再設定を呼びかけ※156。
8 月 23 日	三井住友カード株式会社	会員向けスマートフォンアプリ「Vpass アプリ」においてパスワードリスト型攻撃が発生。顧客の ID 情報最大 1 万 6,756 件が不正侵入を受けた可能性。緊急対応として、不審な接続元を遮断するとともに、不正アクセスが確認された ID のパスワードを無効化※157。
9 月 4 日	株式会社みずほ銀行	サービス提供を行う「J-Coin Pay」の加盟店管理に関わるテスト用システムが不正アクセスを受け、加盟店の法人および窓口担当者の個人情報等が流出の可能性。J コインのユーザ情報等は含まれていない※158。
9 月 10 日	株式会社スープレックス	運営する「なんとかデータベース（ラーメンデータベース）」が不正アクセスを受け、会員情報 16 万 9,843 件のメールアドレス・ログインパスワードが流出した可能性。このうち 4 件のアカウントで流出の証跡を確認※159。
9 月 19 日	有限会社フィセル	運営する子供服通販サイト「10mois WEBSHOP」に不正アクセスが発生し、顧客の個人情報 10 万 8,131 件及びクレジットカード情報 1 万 1,913 件が流出の可能性。クレジットカード情報にはセキュリティコードも含む※160。
10 月 8 日	株式会社京都一の傳	運営するサイトに第三者が不正アクセスし、決済フォームを改ざん。セキュリティコードを含むクレジットカード情報 1 万 8,855 件、会員情報 7 万 2,738 件に流出の可能性※161。
10 月 15 日	株式会社 JIMOS	運営する「酒造 .com」「マキアレイベル」「Coyori」「代謝生活 CLUB」において、サイト内の脆弱性を悪用したサイバー攻撃が発生。セキュリティコードを含むクレジットカード情報 10 万 7,661 件が流出の可能性。一部情報は既に不正利用された可能性※162。
10 月 24 日	株式会社スタジオライン	運営する「MODERN BEAUTY TOKYO」に対し不正アクセスが発生し、顧客のクレジットカード情報 1 万 6,109 件が流出した可能性。流出情報にはセキュリティコードも含む※163。
12 月 5 日	象印マホービン株式会社	運営する「象印でショッピング」に対し不正アクセスが発生し、顧客情報最大 28 万 52 件が流出の可能性。不正アクセスの原因はサイト内の脆弱性と見られる。同社は 12 月 4 日以降、該当のショッピングサイトを公開停止。セキュリティ体制を整えてから再公開する見通し※164。
12 月 25 日	株式会社ビーグリー	運営する「ノベルバ」に対して不正アクセスが発生、登録者の個人情報 3 万 3,715 件が流出の可能性。また、報酬プログラムに登録していたユーザ 76 件については口座情報も流出した可能性※165。

■表 1-2-5　外部からの攻撃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）

(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。過去の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、過失の発生をできる限り抑止していく体制づくりが望まれる。

(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。その上で、監視カメラの設置や退職者のアカウント管理の徹底、通信や操作ログの監視及び保全、部署や役職に応じたアクセス権限の設定（最小権限化）等、不正を実行しにくい環境を整えることも望まれる。また、私用端末によるテレワークは情報の持ち出しなど、内部不正がおきやすい環境であるといえる。内部不正を起こさせないような注意喚起、あるいは私用端末では機微情報を扱わない、等のルール策定・周知も重要である。

IPA が公開している「組織における内部不正防止ガイドライン※173」や経済産業省が公開している「秘密情報の保護ハンドブック※174」等を参考に対策を検討する必要がある。

(d) 不適切な情報の取り扱いへの対策

個人情報を取り扱う事業者は個人情報保護法に基づき適切に情報の管理を行う義務がある。しかし、対策の不備やポリシー不徹底、誤認識等により、不適切な取り扱いをしていることがある。例えば、個人情報の第三者への提供については事前に本人の同意を取る必要がある。第三者に提供する個人情報に同意がとれていないデータが含まれていないか、あるいは同意が適切な形式で行われているか（提供の目的・範囲等が十分に説明されているか、同意を強制していないか等）に関して慎重な確認が必要である。

また第三者提供において、個人の特定ができないように匿名加工処理を施すことも考えられるが、提供先で保有する情報を組み合わせることにより個人が容易に識別できる場合、適切な加工とはならない。これについても慎重な確認が必要である。

なお、2020 年 6 月に公布された改正個人情報保護法では「仮名化情報」が導入された。詳細は「2.7.4 個人情報保護法の改訂」を参照されたい。

(6) 2019 年度に特徴的な情報保護対策

前述の対策以外に、2019 年度に動きがあった情報保護対策について述べる。

(a) クレジットカード情報の保護対策

表 1-2-5（前ページ）に示したように、クレジットカード情報の流出は、不正利用による二次被害の恐れもあり、クレジットカード情報に対しては厳格な管理が求められる。2018 年 6 月施行の改正割賦販売法により、クレジットカード情報保護対策については、加盟店におけるカード情報の「非保持化」またはカード情報を保持する事業者の PCI DSS 準拠が義務化された※175。また、クレジットカード情報偽造防止による不正対策としてクレジットカードの「100%IC 化」が推進され、一般社団法人日本クレジット協会に加盟するカード会社が発行するクレジットカードの IC 化の割合は 2019 年 12 月末の時点で 95.1%となった※176。

さらに、2020 年 6 月公布の改正割賦販売法では、新たに決済システムにおいて大量のクレジットカード番号等を取り扱う事業者（決済代行業者、QR コード決済事業者・EC モール事業者等）についても、クレジットカード番号等の適切管理を義務化することとなった※177。

クレジットカード決済を行う事業者は、同法に基づき、クレジットカード関連情報を適切に管理することが求められる。クレジットカード利用者も、自身の PC で当該情報を管理する際、セキュリティソフトウェアの導入等で端末をセキュアに保つことが重要である。

(b) テレワークにおける対策

2020 年 3 月以降、新型コロナウイルス感染対策としてテレワークが広く普及している。テレワークにおいて、リモート作業環境の整備不足等から私用端末を業務で利用することを迫られ、アクセス制御やウイルス対策等、セキュリティ面の配慮が必ずしも十分ではないケースがあると考えられる。こうした状況においては、テレワーク従事者はセキュリティソフトウェアの導入やセキュリティパッチの更新、さらには業務に関する情報の適切な管理を励行することが重要である。また、企業・組織は私用端末によるテレワークに関し、セキュリティ対策、情報管理のルールを至急策定し周知することが重要である。IPA では「テレワークを行う際のセキュリティ上の注意事項※178」を公表し対策の実施を呼びかけている。

COLUMN

適切なインシデント対応に必要なのは、教育や規則だけじゃない

現在では、セキュリティインシデントの発生に備えて規則を設けたり、所属員（会社であれば社員）に対して教育を実施したりしている組織がほとんどでしょう。しかし、所属員の心理面まで意識した対策、運用ができている組織となると、かなり少ないのではないでしょうか。

所属員が心理的な負荷から言動を控えてしまうような環境は、セキュリティインシデント対応にとっては好ましいものではありません。なぜなら、ミスを咎められるかもしれない、つまらない報告と非難されるかもしれないといった不安から、報告を上げない、すぐに報告しないということが起こり得るためです。その結果、インシデント対応の遅れを招き、組織内外で被害が拡大する恐れがあります。

例えば、ある企業において、社員が宣伝目的の単なるスパムメールであるのに逐一「不審メールを受信した」と報告していた場合、報告を処理する部門は面倒に感じるかもしれません。その場合、「それは不審メールではないので報告しなくて良い」と指摘するのではなく、まずは不審を抱いたメールを適切なルートで報告した行動が正しいことをしっかり伝える、といった対応が望まれます。その上で、報告対象とするメールの判断基準を設けて周知したり、スパムメールを受信しないようにフィルタ設定を追加したりといった対処をすることで、社員に報告する行為を萎縮させることもなく、企業全体として不審メールに対する強化が図れるでしょう。標的型攻撃訓練メールにおいても、添付ファイルを開いたり、URL をクリックしたりした社員がどれだけいたかという指標を用いることが一般的ですが、引っかかってしまった社員を咎めるのではなく、不審メールを受信した報告を上げた社員や引っかかったことを早急に報告した社員を褒めるような訓練とすることで、結果的に望ましい対応ができる社員が増えていくように思えます[i]。

昨今、「心理的安全性」という言葉を耳にする機会が増えた気がします。心理的安全性とはAmy C. Edmondson 氏が提唱した概念で「対人関係においてリスクのある行動をしてもこのチームでは安全であるという、チームメンバーによって共有された考え」と定義されています。米 Google LLC のリサーチ結果では、「無知、無能、ネガティブ、邪魔だと思われる可能性のある行動をしても、このチームなら大丈夫だ」と信じられるかどうかを意味するものとして、仕事におけるチームの効果性に影響を与える因子の中で、この心理的安全性が圧倒的に重要であるとされています[ii]。

セキュリティインシデントの発生に対する組織の備えとして、セキュリティ規則や運用の改定、所属員に対する教育実施といった施策だけでなく、失敗や些細な質問を不安や遠慮なく発言できる心理的安全性が担保された環境を整えていくことも必要と言えそうです。

i　IPA: 組織における標的型攻撃メール訓練は実施目的を明確に　https://www.ipa.go.jp/security/anshin/mgdayori20170731.html〔2020/7/17 確認〕
ii　Google LLC：「効果的なチームとは何か」を知る　https://rework.withgoogle.com/jp/guides/understanding-team-effectiveness/steps/identify-dynamics-of-effective-teams/〔2020/7/17 確認〕
Amy Edmondson：Psychological Safety and Learning Behavior in Work Teams　https://www.jstor.org/stable/2666999〔2020/7/17 確認〕

1.3 情報システムの脆弱性の動向

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

1.3.1 JVN iPediaの登録情報から見る脆弱性の傾向

IPA は、脆弱性対策情報データベース「JVN iPedia※100」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、2019 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

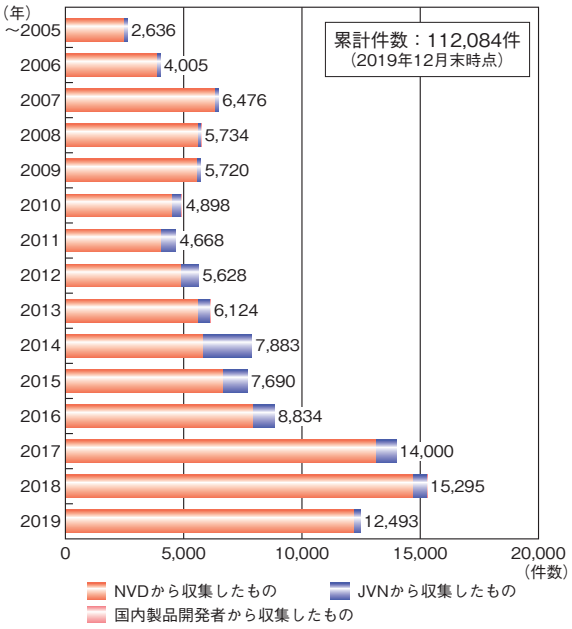
JVN iPedia は、国内外で利用されているソフトウェア製品の脆弱性対策情報を、以下の三つの公開情報から収集・蓄積しており、2007 年 4 月 25 日から公開している。

- 脆弱性対策情報ポータルサイト JVN で公表した脆弱性対策情報
- 国内のソフトウェア開発者が公開した脆弱性対策情報
- 米国国立標準技術研究所（NIST：National Institute of Standards and Technology）の脆弱性データベース「NVD※179」で公開された脆弱性対策情報

(a) JVN iPedia の登録件数の推移

JVN iPedia に登録している情報を、製品ベンダやセキュリティ関連企業が脆弱性情報を公表した年別※180にまとめると、2011 年を境にして NVD から収集した脆弱性対策情報の登録件数が増加傾向となっており、2017 年以降の JVN iPedia の登録件数は 1 万件を上回っている（図 1-3-1）。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）※181 の採番機関（CNA：CVE Numbering Authority）※182 が増加したことが一因として挙げられる。The MITRE Corporation※183 によると、2016 年 12 月に 47 社※184 だった CNA は、2019 年 12 月には 110 社※185 と約 2.3 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、2014 年の 2,084 件を境に減少傾向となっており、2019 年は 318 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、毎年数十件の登録となっており、2019 年は 16 件であった。

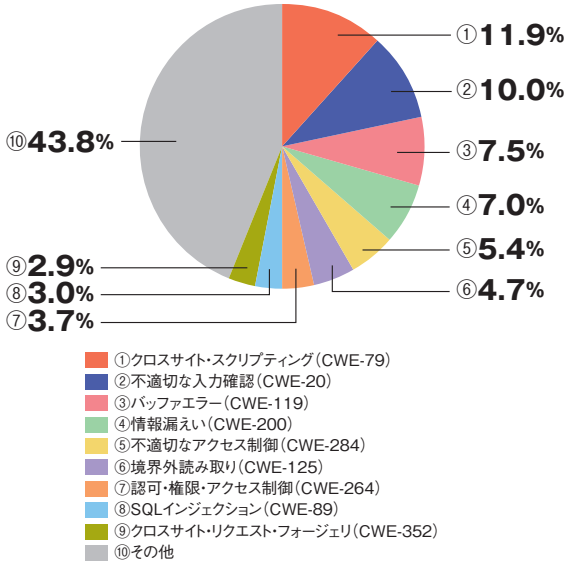


■図 1-3-1　JVN iPedia 登録状況（公表年別）
（出典）JVN iPedia の登録情報を基に IPA が作成

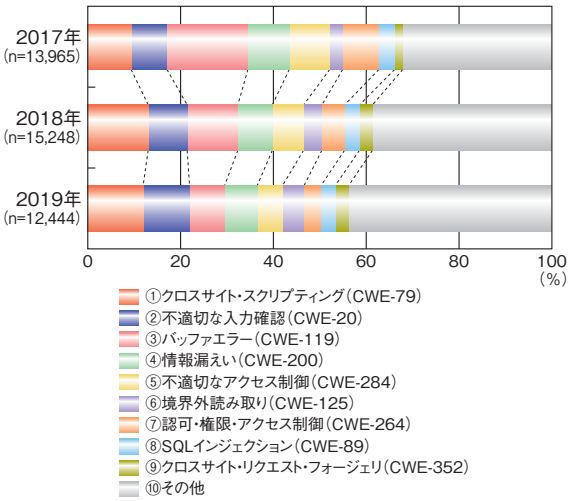
JVN iPedia は、発見された脆弱性の種類を識別するための共通脆弱性タイプ一覧 CWE（Common Weakness Enumeration）※186 を脆弱性対策情報に付与して登録を行っている。2019 年に登録した CWE の割合は「クロスサイト・スクリプティング」が 11.9%と最も高く、以下、「不適切な入力確認」が 10.0%、「バッファエラー」が 7.5%、「情報漏えい」が 7.0%と続いている（図 1-3-2）。

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

2017 年以降の CWE 別割合を年別に見ると、「バッファエラー」「情報漏えい」「不適切なアクセス制御」「認可・権限・アクセス制御」が 2017 年から減少し、それら以外は前年と同程度となっている（図 1-3-3）。



■図 1-3-2　JVN iPedia におけるソフトウェア製品の CWE 別割合（2019 年、n=12,444）
（出典）JVN iPedia の登録情報を基に IPA が作成



■図 1-3-3　JVN iPedia におけるソフトウェア製品の CWE 別割合（2017 ～ 2019 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

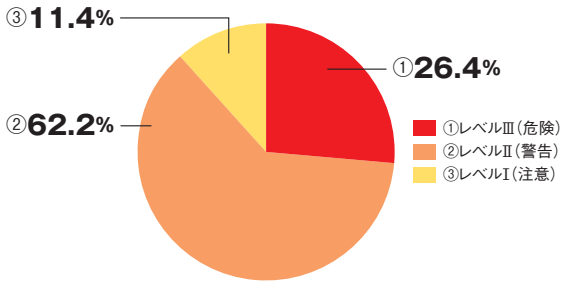
JVN iPedia は、オープンで汎用的な脆弱性評価手法である CVSS（Common Vulnerability Scoring System：共通脆弱性評価システム）※187 を用いて、脆弱性の深刻度を公開している。なお、JVN iPedia では CVSS v2 及び CVSS v3 の二つのバージョンの情報を公開しているが、本項では CVSS v2 を基に統計処理を行っている。

深刻度には、CVSS v2 の基本評価基準（BM：Base Metrics）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。

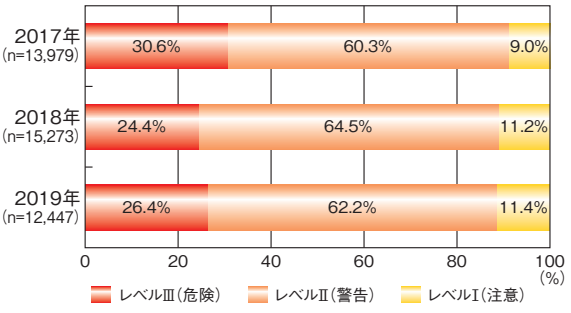
- 深刻度 レベルIII（危険）BM 7.0 ～ 10.0
  リモートからシステムを完全に制御されたり、大部分の情報が漏えいしたりする等の影響が想定される。
- 深刻度 レベルII（警告）BM 4.0 ～ 6.9
  一部の情報が漏えいしたり、サービス停止につながったりする等の影響が想定される。
- 深刻度 レベルI（注意）BM 0.0 ～ 3.9
  深刻度レベルII相当の影響があるが、攻撃するために複雑な条件を必要とする。

2019 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 26.4%、レベルIIが 62.2%、レベルIが 11.4% 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約 9 割を占めている（図 1-3-4）。



■図 1-3-4　JVN iPedia における脆弱性対策情報のレベル割合（2019 年、n=12,447）
（出典）JVN iPedia の登録情報を基に IPA が作成

2017 年以降の深刻度のレベル割合を年別に見ると、レベルII以上の脆弱性は 2017 年で 90.9%、2018 年で 88.9%、2019 年で 88.6%と 9 割前後で推移している。また、2018 年と 2019 年で比較すると、最も危険なレベルIIIに該当する脆弱性の割合は 2019 年で 2.0% 増加し、レベルIIに該当する脆弱性の割合は 2.3% 減少している（図 1-3-5）。これは、レベルIIとして評価されることが多い



■図 1-3-5　JVN iPedia における脆弱性対策情報のレベル割合（2017 ～ 2019 年）
（出典）JVN iPedia の登録情報を基に IPA が作成

「クロスサイト・スクリプティング」や「整数オーバーフローまたはラップアラウンド（CWE-190）」の脆弱性の割合が減少し、レベルⅢとして評価されることが多い「境界外書き込み（CWE-787）」の脆弱性の割合が増加したことが一因と考えられる。

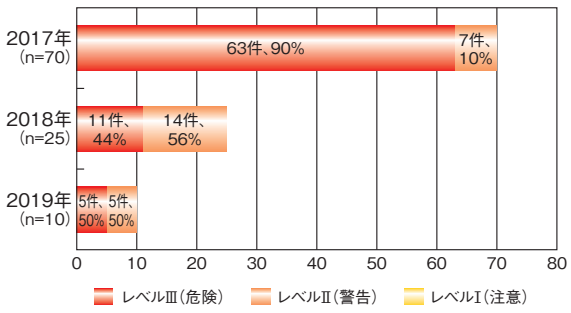
製品開発者は、ソフトウェアの企画・設計・製造段階からセキュアコーディング※188を含めたセキュリティ対策を講じる等、脆弱性による被害を未然に防ぐための対応が必要となる。また、製品の利用者にも、日頃から新たに公開される脆弱性対策情報に注意を払い、脆弱性が公開された場合には製品を最新バージョンにアップデートする等の対応が求められる。

(2) サポート終了が近づくAdobe Flash Playerの脆弱性について

Flash形式のコンテンツをブラウザ上で実行するためのプラグインであるAdobe Flash Playerの更新と配布を2020年末に停止し、同時にサポートを終了する、と開発元のAdobe Systems Inc.が告知している※189。

サポート終了後もAdobe Flash Playerを利用し続けた場合、新たな脆弱性が発見されても開発元から修正プログラムが提供されないため、脆弱性を悪用した攻撃により被害を受けるリスクが増大する。

図1-3-6は、2017年から2019年にかけてJVN iPediaに登録されたAdobe Flash Playerの脆弱性対策情報の深刻度別割合を示したものである。過去3年間に登録された脆弱性のすべてが、深刻度が最も高いレベルⅢ、または次に高いレベルⅡに分類されており、危険度が高い脆弱性が占めていることが分かる。登録件数を見ると、2017年に70件、2018年に25件、2019年に10件と減少傾向となっている。脆弱性の深刻度別割合の推移では、レベルⅢの割合が、2017年は90.0%、2018年は44.0%、2019年は50.0%となっており、2017年が突出し、2018年、2019年も半数近くを占めた。2020年も、件数は減少傾向が続く可能性があるものの深刻度が高い脆弱性情報が公開される恐れもあるため、適切な対策をとることが求められる。



■図1-3-6　JVN iPediaに登録されたAdobe Flash Playerの脆弱性対策情報のレベル別件数とレベル別割合(2017～2019年)
(出典)JVN iPediaの登録情報を基にIPAが作成

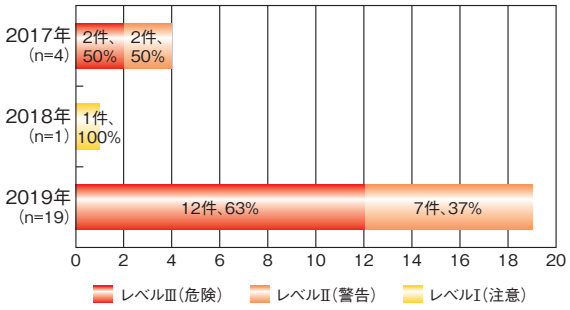
Adobe Flash Playerを利用するコンテンツを提供している組織においては、2020年末までにHTML5形式等の代替手段へ移行する必要がある。また、コンテンツの利用者に対して、移行方法等の周知を行う必要がある。コンテンツの利用者においては、Adobe Flash Playerのサポートが終了するまでは常に最新バージョンを使い、コンテンツの提供者から移行に関する情報が公開された場合は、早急にそれに従うことが望ましい。

(3) リモートデスクトップサービスに関連する脆弱性について

2019年5月、「BlueKeep」と呼ばれるWindowsのリモートデスクトップサービス（RDS：Remote Desktop Services）の脆弱性（CVE-2019-0708）がMicrosoft社より公開された※190。この脆弱性は、認証されていない遠隔の攻撃者が、標的となるシステム側の操作を介さずリモートデスクトッププロトコル（RDP：Remote Desktop Protocol）経由で攻撃可能という特性を持つ。そのため、2017年に猛威を振るった「Wanna Cryptor」（別名、WannaCry）のような、自己増殖機能を有しネットワーク上に感染を拡大するワーム型のウイルスに端末が感染する恐れがあるとされている。これを受けて、Microsoft社は注意喚起を行い、サポートが終了しているWindows XP及びWindows Server 2003のパッチを提供する等の異例の措置を講じた※191（手口については「1.2.4 (1)(a)BlueKeepの脆弱性を悪用した攻撃」参照）。

2019年は「BlueKeep」以外にも、リモートデスクトップサービスやその接続に使われるRDPに関連する脆弱性がMicrosoft社から多数公開されている。2017年から2019年にかけてJVN iPediaに登録されたMicrosoft社製品の当該脆弱性対策情報は、2017年が4件、2018年が1件であったのに対し、2019年は19件と急増している。また、2019年に登録されたこれらの脆弱性対策情報を深刻度別割合で見ると、全19件のうち12件が、深刻度が最も高いレベルⅢに分類されており、全体の63%を占めている。残りの7件も深刻度が次に高いレベルⅡとなり、レベルⅠは0件となった（図1-3-7）。

組織においては、業務でリモートデスクトップサービスを利用するケースが多々ある。また、リモートデスクトップサービスはWindowsで標準搭載される機能であるた



■図 1-3-7　JVN iPedia に登録されたリモートデスクトップサービス及び RDP に関連する Microsoft 製品の脆弱性対策情報のレベル別件数とレベル別割合（2017 ～ 2019 年）
（出典）JVN iPedia の登録情報を基に IPA が作成

め、端末を共同で利用している場合、意図せず有効になっていることがある。そのため、リモートデスクトップサービスが悪用され、リモートから攻撃されることにより大きな被害につながる恐れがあり、開発元から更新プログラムが公開された場合は早急な適用が必要である。

(4) 今後の展望

JVN iPediaへ登録された脆弱性対策情報の件数は、2019 年 5 月に 10 万件を突破し、2019 年 12 月末時点では 11 万 2,000 件を超え、今後も増加していくものと思われる。

また、昨今の働き方改革や新型コロナウイルス感染拡大への対応をきっかけに、テレワークや個人が所有する端末を業務で利用する BYOD といった新しい業務形態が注目を集めており、今後は利用が増えるものと思われる。これらの業務形態により、多様な働き方を可能としたり、新型コロナウイルス感染のリスクを低減するといったメリットがある一方で、業務環境が社外に広がり、また社内に接続する端末に個人が所有する端末が加わることから、これまでのセキュリティ対策に加えてそれらの環境に即したセキュリティ対策が求められる。

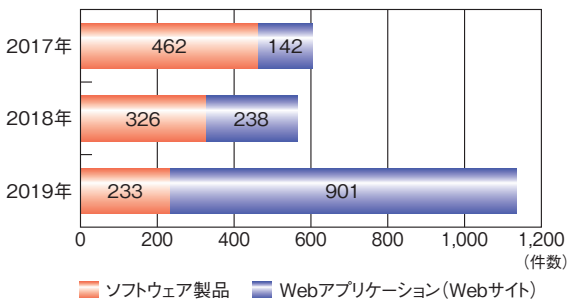
例えば、テレワークで BYOD を活用する場合は、外部から安全に社内にアクセスするための認証や VPN（Virtual Private Network）等の仕組みが必要であり、それに伴う新しい機器やシステムの導入及び管理が求められる。更に、これまで組織が従業員に貸与していた端末の管理に加え、従業員が所有している端末も安全なテレワークのために組織が定めたルールに基づく管理が必要となる。また、リモートデスクトップサービスを利用して社内に接続する場合は、「1.3.1 (3) リモートデスクトップサービスに関連する脆弱性について」で説明したように、利用端末の OS のバージョンを常に最新に保ち、脆弱性がない状態で利用するといった対応が求められる。また、業務以外で使っているプライベートなソフトウェアや家庭内のルータ等のネットワーク機器が攻撃に悪用される恐れもあるため、それらのセキュリティ対策も重要となる。

今後、このような業務形態が普及していく中で、組織においては従業員の業務環境を把握し、それぞれの環境に適した情報セキュリティ対策を推進していくことが求められる。また、プライベートなソフトウェアや家庭内の機器といった、組織による管理が難しい部分においては、テレワークを行う個人も JVN iPedia 等を活用して、利用している OS やソフトウェアに関する情報収集を行い、漏れなく脆弱性対策を実施していくことが望まれる。

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、2019 年も引き続き発生している。例えば、脆弱性のある EC サイト構築パッケージを使って作られた Web サイトからクレジットカード番号等が窃取される被害が多く発生したことを受け、2019 年末に製品開発者に加え、経済産業省や IPA からも注意喚起※192 がなされた。

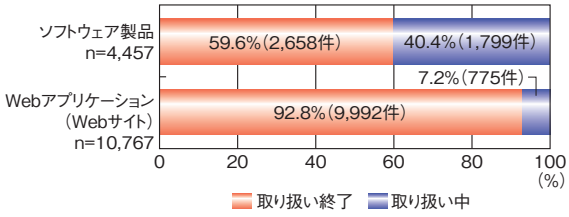
2019 年に「情報セキュリティ早期警戒パートナーシップ」（以下、パートナーシップ）に基づき IPA に届け出された脆弱性関連情報※193 の件数は、ソフトウェア製品が 233 件、Web サイトが 901 件、合計 1,134 件であった。2018 年の届出件数（564 件）と比較すると、約 2 倍に増加している。なお、それぞれの件数を 2018 年の届出件数（ソフトウェア製品：326 件、Web サイト：238 件）と比較すると、ソフトウェア製品に対する届出は約 29% 減少、Web サイトに対する届出は約 280% 増加した（図 1-3-8）。



■図 1-3-8　脆弱性関連情報の種類別届出状況（2017 ～ 2019 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 4,457 件、

Web サイトは 1 万 767 件となり、2019 年 12 月末時点までの合計が 1 万 5,224 件に上る。これらの届出のうち IPA での取り扱いが終了※194 した届出件数は、ソフトウェア製品 2,658 件（59.6%）、Web サイト 9,992 件（92.8%）という状況である（図 1-3-9）。



■図 1-3-9　脆弱性関連情報の種類別取扱終了状況
（2019 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

ソフトウェア製品については、取り扱いが終了していない届出が多いことから、パートナーシップでは、製品開発者と連絡が取れず進展が望めない届出を速やかに公表できるように手続きの簡略化等を検討した。併せて、「情報システム等の脆弱性情報の取扱いに関する研究会※195」においてソフトウェア製品に脆弱性を作り込まない観点から、製品開発者向けガイドの検討等の取り組みを行っている。

（1）ソフトウェア製品の脆弱性

2019 年のソフトウェア製品の脆弱性の状況を、パートナーシップへの届出件数、IPA が公表している「重要なセキュリティ情報※196」から解説する。

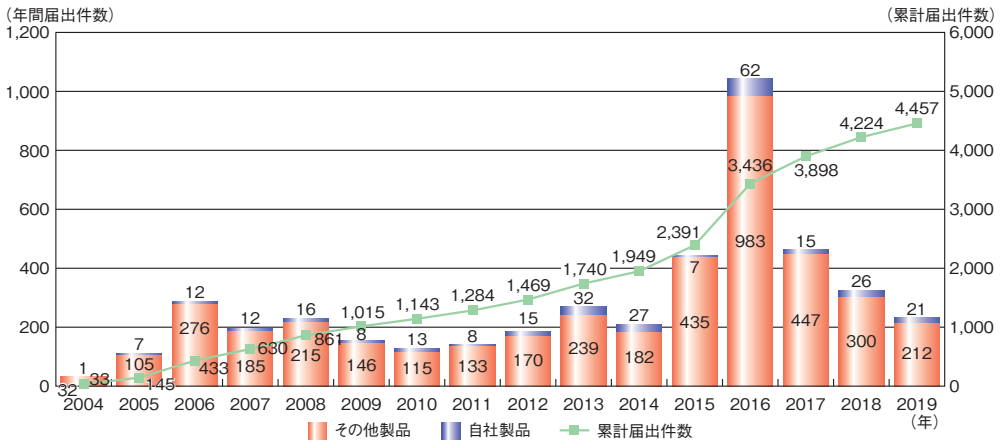
（a）パートナーシップの届出から見たソフトウェア製品の脆弱性

パートナーシップによると、2019 年のソフトウェア製品の届出件数は、製品開発者自らが利用者への周知のために自社製品の脆弱性の公表を目的とした届出が 21 件、一般の方からの届出が 212 件あり、合わせて 233 件（うち、不受理となった届出が 12 件）となった。またパートナーシップが開始された 2004 年 7 月から累計で 4,457 件となった（図 1-3-10）。このうち 2019 年に JVN で公表した脆弱性の届出件数は 98 件、累計 2,034 件となった（図 1-3-11）。

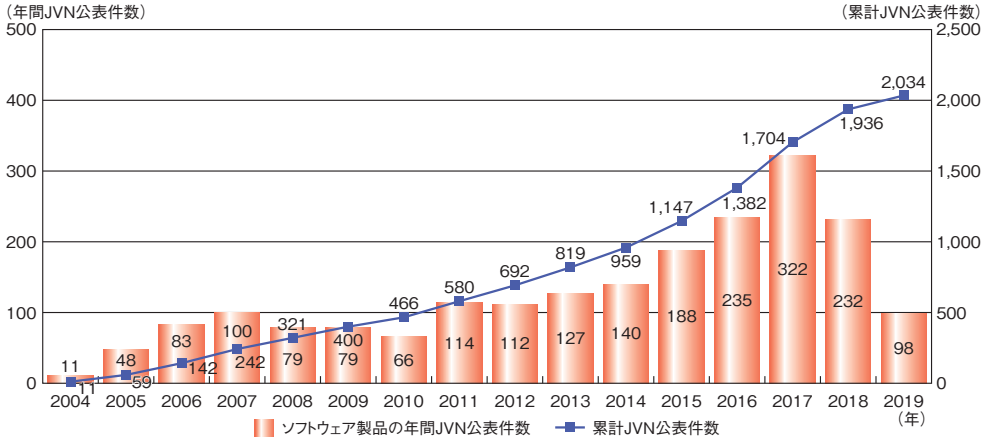
脆弱性をソフトウェア製品種類別（表 1-3-1）に見ると、届出件数の合計は 2018 年が 312 件、2019 年が 221 件と約 3 割減少している中、「スマートフォン向けアプリ」「システム管理ソフト」「アプリケーション開発・実行環境」は増加している。

また脆弱性を原因別（表 1-3-2）に見ると、「アクセス制御の不備」「証明書の検証に関する不備」「バッファのチェックの不備」が増加している。中でも「証明書の検証に関する不備」に関しては、2018 年が 11 件、2019 年が 18 件と約 1.6 倍に増加した。これはソフトウェア製品種類別（表 1-3-1）で示した「スマートフォン向けアプリ」等が「盗聴」「なりすまし」「改ざん」の被害を防ぐことを目的にサーバ証明書を導入しているにも関わらず、サーバ証明書の正当性を検証していないため、「盗聴」「なりすまし」「改ざん」の被害に遭う可能性がある、という届出である。

また、「証明書の検証に関する不備」に関する JVN 公表が 2019 年度は 5 件であったが、そのうちの 3 件は 1 月下旬に集中していた（表 1-3-3）。中でも 2020 年 1 月



■図 1-3-10　ソフトウェア製品の脆弱性の年別届出件数の推移（2004 ～ 2019 年）
（出典）パートナーシップの届出状況を基に IPA が作成



■図 1-3-11　JVN で公表したソフトウェア製品の脆弱性の年別公表件数の推移（2004 ～ 2019 年）
（出典）パートナーシップの届出状況を基に IPA が作成

ソフトウェア製品種類別	届出件数	
	2018 年	2019 年
Web アプリケーションソフト	117	78
スマートフォン向けアプリ	23	25
ルータ	39	23
情報家電	27	19
システム管理ソフト	6	8
アプリケーション開発・実行環境	4	7
グループウェア	17	7
その他	79	54
計	312	221

■表 1-3-1　2019 年のソフトウェア製品種類別届出件数（不受理を除く）
（出典）パートナーシップの届出状況を基に IPA が作成

脆弱性の原因別	届出件数	
	2018 年	2019 年
Web アプリケーションの脆弱性	165	99
その他実装上の不備	102	71
アクセス制御の不備	18	21
証明書の検証に関する不備	11	18
バッファのチェックの不備	4	6
ファイルのパス名、内容のチェックの不備	12	5
その他	0	1
計	312	221

■表 1-3-2　2019 年の脆弱性の原因別届出件数（不受理を除く）
（出典）パートナーシップの届出状況を基に IPA が作成

28 日に公表された Android アプリ「MyPallete」の脆弱性は、同製品を使用している複数の銀行のバンキングアプリ※197 に影響がある。アプリをアップデートすることで脆弱性を解消できるため、MyPallete を利用しているバンキングアプリ等は速やかに対応していただきたい。

公表日	タイトル
2019 年 5 月 24 日	Android アプリ「Tootdon for マストドン（Mastodon）」（JVN#57806517）
12 月 19 日	Android アプリ「日テレニュース 24」（JVN#01236065）
2020 年 1 月 21 日	富士ゼロックス製の複数のスマートフォンアプリ（JVN#66435380）
1 月 28 日	Android アプリ「MyPallete」（JVN#28845872）
1 月 31 日	スマートフォンアプリ「AWMS Mobile」（JVN#00014057）

■表 1-3-3　「証明書の検証に関する不備」に関する JVN 公表※198
（2020 年 2 月 5 日時点）
（出典）JVN を基に IPA が作成

証明書の検証に関する不備の原因は、開発環境の制約等からサーバ証明書の正当性の検証を行わないまま開発を進め、そのまま本稼働してしまうこと等が考えられる。サーバ証明書を導入している、または導入を検討している製品を提供する製品開発者は、リリース時のチェック項目に加える等、忘れずに対応していただきたい。なお、IPA では「TLS 暗号設定ガイドライン※199」を公表している。サーバ証明書の導入、運用時の参考にしていただきたい。

(b)「重要なセキュリティ情報」から見たソフトウェア製品の脆弱性

IPA ではソフトウェア製品における「重要なセキュリティ情報」を公表しており、2019 年に公表した情報は 39 件であった。このうち、脆弱性を悪用した攻撃が確認されていること等を理由として緊急に公表したものは 10 件であった（次ページ表 1-3-4）。

公表日（2019 年）	タイトル
2 月 13 日	Microsoft 製品の脆弱性対策について
3 月 13 日	Microsoft 製品の脆弱性対策について
4 月 10 日	Microsoft 製品の脆弱性対策について
5 月 15 日	Microsoft 製品の脆弱性対策について
7 月 10 日	Microsoft 製品の脆弱性対策について
9 月 10 日	ウイルスバスターコーポレートエディションの脆弱性（CVE-2019-9489）について
9 月 12 日	Microsoft 製品の脆弱性対策について
9 月 24 日	Microsoft Internet Explorer の脆弱性対策について（CVE-2019-1367）
11 月 13 日	Microsoft 製品の脆弱性対策について
12 月 11 日	Microsoft 製品の脆弱性対策について

■表 1-3-4　2019 年に公表したソフトウェア製品における重要なセキュリティ情報（緊急）
（出典）IPA による重要なセキュリティ情報の公表データを基に IPA が作成

(c) ソフトウェア製品における脆弱性対策の課題

2019 年も前述のとおり、ソフトウェア製品の脆弱性を悪用した攻撃が確認されていること等を理由として緊急対策情報を公表している。製品利用者のみならず、当該製品を利用して製品を開発している製品開発者においても、既知の脆弱性に対する基本的な対策である最新バージョンへのアップデートを迅速に行うことを、製品を利用する上での責務として対応していただきたい。

企業や組織で製品を利用する場合、迅速なアップデートを実現するためには、様々な課題が存在している。例えば、あるソフトウェア製品がミドルウェア等に限らず、複数の他の製品に密接に影響している場合がある。当該製品を最新バージョンにアップデートすることで、関係するほかの製品本来の機能に影響をきたす可能性があるため、検証が必要になる。更に、いったん開発が完了した後は開発チームが解散する等により、仕様を理解する担当者が不在になることもあり得る。こういった様々な要因で迅速に対応することが困難になることがある。

このため、事前に検証項目や検証手順を用意する、製品の仕様を熟知した担当者を必要に応じてアサインできる体制にしておく等、自組織の環境に照らし合わせて具体的かつ現実的に実行可能な手段を検討しておくことが重要である。

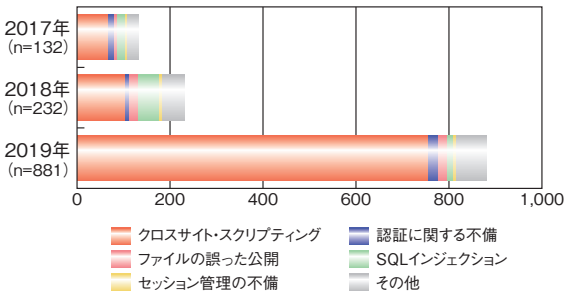
更に、一般の方が製品利用者である場合、利用しているソフトウェア製品を把握し、脆弱性情報を収集することは困難といえる。このため製品開発者は自動でアップデートできる機能の実装や、アップデートを促す警告を通知する機能を実装する等、製品利用者が受動的に対策をとれるように検討していただきたい。

(2) Web アプリケーション（Web サイト）の脆弱性

2019 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（不受理を除く）は、881 件であった。

図 1-3-12 は、2017 年から 2019 年までの脆弱性の種別ごとの届出受付数（不受理を除く）を示している。「SQL インジェクション」や「ファイルの誤った公開」等、2017 年から 2018 年では増加傾向にあったものの 2019 年では届出数が減少したものもある。他方、前年から引き続き増加したものとしては、「クロスサイト・スクリプティング」がある。2019 年も 754 件と最も多く届出されており、全体の 86%を占めている。2018 年の「クロスサイト・スクリプティング」の届出は 102 件であり、2019 年は約 7.4 倍に増加した。

「クロスサイト・スクリプティング」は、例年最も多く届出がなされている脆弱性であるが、754 件という届出数は、2004 年の制度開始からしても、2008 年の 1,039 件に次いで過去 2 番目に多い。



■図 1-3-12　脆弱性種類別の Web アプリケーションの届出受付数（2017 ～ 2019 年）
（出典）パートナーシップの届出状況を基に IPA が作成

2000 年に米国の CERT/CC（CERT Coordination Center）と Microsoft 社からアドバイザリが公表されたことで、クロスサイト・スクリプティングは広く知られるようになったが、2019 年においても、未だ多くの Web サイトに存在していることがうかがえる。

(a) クロスサイト・スクリプティングの脆弱性

クロスサイト・スクリプティングとは、リクエスト等に含まれる情報を Web ページへ出力する処理が悪用されることにより、被害者の Web ブラウザ上で不正なスクリプトが実行されてしまう脆弱性である。

セッション ID 等 Cookie に格納されている情報が漏えいしたり、Web サイトが改ざんされフィッシング詐欺に悪用されたりすることが、脅威として挙げられる。

対策としては、HTMLにおいて特殊な意味を持つ記号や文字を安全なものに置き換える（エスケープ処理）等、ユーザからの入力に含まれる不正なスクリプトを何らかの方法でスクリプトとしてブラウザが解釈しないように対処することが有効である。

(b) パートナーシップから見る2019年のクロスサイト・スクリプティングの現状

2019年のクロスサイト・スクリプティングの届出の半数以上は、検索フォームやお問い合わせフォームの氏名欄等、利用者がブラウザから直接任意の文字を入力するテキスト欄において不正な入力が可能であることを指摘するものであった。

これらの箇所に、クロスサイト・スクリプティングが作り込まれやすいことは、以前から知られており、特に新しいものではない。IPAが発行する「安全なウェブサイトの作り方※200」でも、クロスサイト・スクリプティングが生じやすい機能の例として、以下のような入力結果の確認画面や検索結果表示画面を挙げ、注意を促している。

- 入力内容を確認させる表示画面（会員登録、アンケート等）
- 誤入力時の再入力を要求する画面で、前の入力内容を表示するとき
- 検索結果の表示
- エラー表示
- コメントの反映（ブログ、掲示板等）等

2019年にこれらの機能に対する多くの届出があったことは、多くのWebサイトにおいて、未だに注意が必要である箇所にさえ対策がなされていないことを示唆している。

また、クロスサイト・スクリプティングは、利用者がブラウザから直接任意の文字を入力できないセレクトボックスやラジオボタン等で選択する箇所や、Hidden属性のパラメータにも存在し得る。直接入力ができない箇所は、任意の文字列が挿入可能であることをWebサイト運営者が認識しづらく、対策の見落としが生じてしまうことがある。他方、発見の容易さから見ても、直接入力できる箇所では特殊記号の誤入力による挙動等から偶然発見することはあっても、直接入力できない箇所では文字列を入力しないため発見の機会も多くはない。

そのため、対策がされず、発見もなされていないクロスサイト・スクリプティングが相当数存在すると推測される。パートナーシップの届出状況が示す以上に、2019年のWebサイトの脆弱性の現状は思わしくないといえよう。

(c) Webサイト運営者に求められる対策

前述のとおり、2019年のクロスサイト・スクリプティングの届出では、文字列を入力するフォームに問題があることを指摘するものが多数を占めている。

Webサイト運営者はまず、改めてそのような箇所にクロスサイト・スクリプティングが存在しないか確認していただきたい。

また、すべてに予防的な対策がとれない場合を想定して、攻撃による影響を軽減する対策をとることも重要である。そのような対策としては、Webアプリケーションファイアウォール（WAF）の導入が挙げられる。IPAが2019年に公開した資料「Web Application Firewallの導入に向けた検討項目※201」を、WAFの新規導入や運用見直しの際の検討の補助資料として参照していただきたい。

2019年10月には、主要なブラウザであるGoogle Chromeに搭載されていたクロスサイト・スクリプティング攻撃のブロックを試みる機能である「XSS Auditor」が削除された※202。このことからも、Webサイトを閲覧する利用者の側での対策に頼ることのない、Webサイト運営者によるWebサイト側の対策が求められる状況となっている。パートナーシップにおいて多数の届出があったことを対岸の火事と思うことなく、自らが運営するWebサイトのセキュリティ対策を振り返る契機としていただきたい。

COLUMN

情報セキュリティ10大脅威 2020
～セキュリティ対策は一丸となって、Let's Try!!～

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。2020 年 1 月に公開した「情報セキュリティ 10 大脅威 2020」は、以下の表のとおりです。

表 情報セキュリティ 10 大脅威 2020「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	標的型攻撃による機密情報の窃取
フィッシングによる個人情報等の詐取	2	内部不正による情報漏えい
クレジットカード情報の不正利用	3	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	4	サプライチェーンの弱点を悪用した攻撃
メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	5	ランサムウェアによる被害
不正アプリによるスマートフォン利用者への被害	6	予期せぬ IT 基盤の障害に伴う業務停止
ネット上の誹謗・中傷・デマ	7	不注意による情報漏えい
インターネット上のサービスへの不正ログイン	8	インターネット上のサービスからの個人情報の窃取
偽警告によるインターネット詐欺	9	IoT 機器の不正利用
インターネット上のサービスからの個人情報の窃取	10	サービス妨害攻撃によるサービスの停止

「個人」向け脅威では「スマホ決済の不正利用」が初登場で 1 位となりました。スマホ決済は、昨年 10 月 1 日の消費増税に併せた消費者還元事業（ポイント還元事業）により、普及が進みました。しかし、一部のスマホ決済では、決済方法の不備により、利用者が金銭被害に遭う事案が発生しました。スマホ決済を利用する際には、提供されているセキュリティ機能の利用とともに、不正利用されていないか決済情報や利用明細を確認することが求められます。

「組織」向け脅威では「内部不正による情報漏えい」が昨年の 5 位から 2 位に上昇しました。情報機器リユース業者において、廃棄予定のハードディスクドライブが社員により不正に持ち出し及び転売され、その中に個人情報等が残っていたことが発覚して大きな問題となりました。今回の持ち出しのような内部不正を防止するためには、被害の予防策の検討、従事者のモラルの向上、被害の早期検知、そして被害を検知した場合への備えが大切です。

10 大脅威のほか、「知っておきたい用語や仕組み」や、「情報セキュリティ 10 大脅威の活用法」についても解説している「『情報セキュリティ 10 大脅威 2020』解説書」は、以下の URL からダウンロードできます。

https://www.ipa.go.jp/security/vuln/10threats2020.html

※1　IBM 社：IBM X-Force 脅威インテリジェンス・インデックス　https://www.ibm.com/jp-ja/security/data-breach/threat-intelligence〔2020/6/30 確認〕
※2　Verizon 社：2020 Data Breach Investigations Report　https://enterprise.verizon.com/resources/reports/dbir/〔2020/6/30 確認〕
※3　トレンドマイクロ社：2019 年年間セキュリティラウンドアップ　https://resources.trendmicro.com/jp-docdownload-form-m197-web-2019-annualsecurityreport.html〔2020/6/30 確認〕
※4　APWG：PHISHING ACTIVITY TRENDS REPORTS　https://apwg.org/trendsreports/〔2020/6/30 確認〕
※5　URL を短縮する目的等で使用される、カスタマイズサービスのサイトを経由したリダイレクトによって元のサイトにアクセスする URL。
※6　トレンドマイクロ社：2018 年年間セキュリティラウンドアップ 騙しの手口の多様化と急増するメールの脅威　https://resources.trendmicro.com/jp-docdownload-form-m113-web-2018-annualsecurityreport.html〔2020/6/30 確認〕
※7　IC3：2019 Internet Crime Report　https://pdf.ic3.gov/2019_IC3Report.pdf〔2020/6/30 確認〕
※8　Piyolog：SSRF 攻撃による Capital One の個人情報流出についてまとめてみた　https://piyolog.hatenadiary.jp/entry/2019/08/06/062154〔2020/6/30 確認〕
ZDNet Japan：米金融大手 Capital One で 1 億人超の情報漏えい -- 容疑者は AWS 元従業員の可能性　https://japan.zdnet.com/article/35140621/〔2020/6/30 確認〕
※9　WAF（Web Application Firewall）：主に Web アプリケーションへの攻撃を防御するソフトウェアまたはハードウェア。
※10 SSRF（Server Side Request Forgery）攻撃：公開サーバ等の権限を悪用してイントラネット内のサーバに不正なコマンドを送る攻撃。
※11 日本経済新聞：全国民の個人情報が流出　エクアドルで 2000 万人分　https://www.nikkei.com/article/DGXMZO49918550Y9A910C1000000/〔2020/6/30 確認〕
WeLiveSecurity：Nearly all of Ecuador's citizens caught up in data leak　https://www.welivesecurity.com/2019/09/17/ecuador-citizens-data-leak/〔2020/6/30 確認〕
東洋経済オンライン：エクアドル、なぜほぼ全国民の情報漏れたのか　https://toyokeizai.net/articles/-/304865〔2020/6/30 確認〕
※12 ランサムウェア：パソコン及び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、または画面ロック等によりパソコンを使用不可にするウイルスの総称。暗号化解除の条件と称して身代金の支払いを求める脅迫メッセージを表示するソフトウェアであることから「ransom」（身代金）と「software」（ソフトウェア）を組み合わせた造語で「ランサムウェア」と呼ばれている。
※13 Ars Technica：“Severe” ransomware attack cripples big aluminum producer　https://arstechnica.com/information-technology/2019/03/severe-ransomware-attack-cripples-big-aluminum-producer/〔2020/6/30 確認〕
※14 Trend Micro：California City Confirms Phone Line and Financial Data System Disruptions Caused by Ransomware　https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/california-city-confirms-phone-line-and-financial-data-system-disruptions-caused-by-ransomware
※15 ITmedia エンタープライズ：ホンダのシステム障害、原因は産業制御システムを狙うランサムウェア「Ekans」か　https://www.itmedia.co.jp/enterprise/articles/2006/11/news059.html〔2020/6/30 確認〕
※16 「マルウェア」等の用語を混在して使用すると、読者を混乱させる可能性があるため、本白書では特に断りのない限り、または文献引用上の正確性を期す必要のない限り、総称して「ウイルス」と表現する。
※17 DarkReading：Why Bricking Vulnerable IoT Devices Comes with Unintended Consequences　https://www.darkreading.com/iot/why-bricking-vulnerable-iot-devices-comes-with-unintended-consequences-/a/d-id/1336009〔2020/6/30 確認〕
※18 JVN iPedia：JVNDB-2017-002402 Microsoft OLE URL Moniker における遠隔の HTA データに対する不適切な処理　https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-002402.html〔2020/6/30 確認〕
※19 JVN iPedia：JVNDB-2017-009645 Microsoft Office 数式エディタにおけるスタックベースのバッファオーバーフローの脆弱性　https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-009645.html〔2020/6/30 確認〕
※20 当該集計情報は 2018 年度まで MBSD 社より「サイバーセキュリティ事件簿」という名称で公表されていたが、2019 年度からは MBSD 社の社内向け情報発信のために集計が継続されている。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〔2020/6/30 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/〔2020/6/30 確認〕
※23 2019 年度から「侵入感染」は「不正アクセス」、「改ざん・破壊」は「改ざん」、「情報流出・紛失」は「情報流出」、「妨害」は「その他」と事象分類の表記が変更された。
※24 JPCERT/CC：JPCERT/CC に報告されたフィッシングサイトの傾向 https://blogs.jpcert.or.jp/ja/2020/03/phishing2019.html〔2020/6/30 確認〕
※25 警察庁：フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（全銀協等と連携した注意喚起）https://www.npa.go.jp/cyber/policy/caution1910.html〔2020/6/30 確認〕
金融庁：インターネット・バンキングによる預金の不正送金事案が多発しています。　https://www.fsa.go.jp/ordinary/internet-bank_2.html〔2020/6/30 確認〕
全国銀行協会：フィッシング詐欺　https://www.zenginkyo.or.jp/hanzai/15300/〔2020/6/30 確認〕
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〔2020/6/30 確認〕
フィッシング対策協議会：2019/11 フィッシング報告状況　https://www.antiphishing.jp/report/monthly/201911.html〔2020/6/30 確認〕
※26 警察庁：令和元年におけるサイバー空間をめぐる脅威の情勢等について　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R01_cyber_jousei.pdf〔2020/6/30 確認〕
※27 日経クロステック：サイバー攻撃を浴びる日本の銀行、2019 年 9 月に不正送金被害が急増した理由　https://xtech.nikkei.com/atcl/nxt/column/18/00001/03373/〔2020/6/30 確認〕
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〔2020/6/30 確認〕
※28 日経クロステック：ネットバンキングの不正送金被害が 11 月も過去最多を更新、警察庁が注意喚起　https://xtech.nikkei.com/atcl/nxt/news/18/06742/〔2020/6/30 確認〕
※29 トレンドマイクロ社：変化を続けるマルウェア「EMOTET」の被害が国内でも拡大　https://blog.trendmicro.co.jp/archives/22959〔2020/6/30 確認〕
※30 Yahoo ニュース：ホンダを狙ったサイバー攻撃。AD のドメインコントローラーの脆弱性が利用された可能性も。　https://news.yahoo.co.jp/byline/ohmototakashi/20200621-00184297/〔2020/6/30 確認〕
※31 ITmedia：相次ぐパスワードリスト攻撃に注意、パスワードの使い回しは厳禁　https://www.atmarkit.co.jp/ait/articles/1304/10/news092.html〔2020/6/30 確認〕
※32 株式会社セブン & アイ・ホールディングス：「7pay（セブンペイ）」サービス廃止のお知らせとこれまでの経緯、今後の対応に関する説明について　https://www.7andi.com/library/dbps_data/_template_/_res/news/2019/20190801_01.pdf〔2020/6/30 確認〕
※33 新型コロナウイルス感染症：2019 年 12 月に中華人民共和国にて新しく発生したとされるコロナウイルス。その後、新型コロナウイルス感染症は、世界保健機関（WHO：World Health Organization）により「COVID-19」と命名された。
※34 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〔2020/6/30 確認〕
※35 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〔2020/6/10 確認〕
※36 https://www.ipa.go.jp/security/event/2013/isec-semi/documents/2013videosemi_targeted_cyber_attacks_v1.pdf〔2020/6/10 確認〕
※37 McAfee, LLC：Updated BlackEnergy Trojan Grows More Powerful　https://www.mcafee.com/blogs/other-blogs/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/〔2020/6/10 確認〕
※38 トレンドマイクロ社：サイバー攻撃集団「TICK」による「Operation ENDTRADE」　https://blog.trendmicro.co.jp/archives/23107〔2020/6/10 確認〕
※39 https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf〔2020/6/10 確認〕
※40 朝日新聞デジタル：【独自】三菱電機にサイバー攻撃　防衛などの情報流出か　https://www.asahi.com/articles/ASN1M6VDSN1MULFA009.html〔2020/6/10 確認〕
※41 朝日新聞デジタル：三菱電機へ高度なサイバー攻撃、中国政府の動きと呼応?　https://www.asahi.com/articles/ASN1X4JXHN1RULZU002.html〔2020/6/10 確認〕
※42 三菱電機株式会社：不正アクセスによる個人情報と企業機密の流

出の可能性について（第３報） https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf〔2020/6/10 確認〕
※ 43 三菱電機株式会社：不正アクセスによる個人情報と企業機密の流出の可能性について（第３報） https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf〔2020/6/10 確認〕
日本電気株式会社：当社の社内サーバへの不正アクセスについて https://jpn.nec.com/press/202001/20200131_01.html〔2020/6/10 確認〕
株式会社神戸製鋼所：当社ネットワークへの不正アクセスについて https://www.kobelco.co.jp/releases/files/20200206_1_01.pdf〔2020/6/10 確認〕
株式会社パスコ：社内ネットワーク端末に対する不正アクセスについて https://www.pasco.co.jp/press/2020/download/PPR20200206J.pdf〔2020/6/10 確認〕
※ 44 OLE：Windows 環境において、複数のソフトウェアが連携、データを共有するための技術。
※ 45 JPCERT/CC：マルウエアが含まれたショートカットファイルをダウンロードさせる攻撃 https://blogs.jpcert.or.jp/ja/2019/05/darkhotel_lnk.html〔2020/6/10 確認〕
JPCERT/CC：短縮 URL から VBScript をダウンロードさせるショートカットファイルを用いた攻撃 https://blogs.jpcert.or.jp/ja/2019/07/shorten_url_lnk.html〔2020/6/10 確認〕
※ 46 株式会社マクニカ：標的型攻撃の実態と対策アプローチ 第３版 日本を狙うサイバーエスピオナージの動向 2019 年度上期 https://www.macnica.net/mpressioncss/feature_04.html〔2020/6/10 確認〕
※ 47 日経ニューメディア：五輪開会式を想定して 70 社がサイバー演習、意外すぎる盲点に会場がざわつく https://tech.nikkeibp.co.jp/atcl/nxt/column/18/00001/03208/?ST=nnm〔2020/6/10 確認〕
※ 48 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〔2020/6/10 確認〕
※ 49 IC3：Business Email Compromise The $26 Billion Scam https://www.ic3.gov/media/2019/190910.aspx〔2020/6/10 確認〕
※ 50 IC3：Business E-mail Compromise The 12 Billion Dollar Scam https://www.ic3.gov/media/2018/180712.aspx〔2020/6/10 確認〕
※ 51 FBI：Worldwide Sweep Targets Business Email Compromise https://www.fbi.gov/news/stories/operation-rewired-bec-takedown-091019
※ 52 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/20200325_BEC-survey.pdf〔2020/6/10 確認〕
※ 53 日本経済新聞：トヨタ紡織、欧州で最大 40 億円流出 業績修正を検討 https://www.nikkei.com/article/DGXMZO49508720W9A900C1CN8000/〔2020/6/10 確認〕
※ 54 日本経済新聞：日経米子会社、香港に 32 億円流出 詐欺被害か https://www.nikkei.com/article/DGXMZO51583520Q9A031C1SHA000/〔2020/7/27 確認〕
※ 55 トレンドマイクロ社：法人システムを狙う脅迫と盗用 2019 年上半期セキュリティラウンドアップ https://resources.trendmicro.com/jp-docdownload-form-m144-web-2019-1h-security-round-up.html〔2020/6/10 確認〕
※ 56 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。
※ 57 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/〔2020/6/10 確認〕
※ 58 Forbes JAPAN：「ビジネスメール詐欺」の被害額は年間 1.4 兆円、FBI が警告 https://forbesjapan.com/articles/detail/27057〔2020/6/10 確認〕
Bleeping Computer：$1.75 Million Stolen by Crooks in Church BEC Attack https://www.bleepingcomputer.com/news/security/175-million-stolen-by-crooks-in-church-bec-attack/〔2020/6/10 確認〕
cleveland.com：Email hackers steal $1.75 million from St. Ambrose Catholic Parish in Brunswick https://www.cleveland.com/crime/2019/04/email-hackers-steal-175-million-from-st-ambrose-catholic-parish-in-brunswick.html〔2020/6/10 確認〕
※ 59 株式会社カスペルスキー：だまされたサッカークラブ https://blog.kaspersky.co.jp/boca-juniors-case/23331/〔2020/6/10 確認〕
Infobae：Exclusivo: investigan el robo de 519.000 euros que el Paris Saint Germain le pagó a Boca por el pase de Paredes https://www.infobae.com/sociedad/policiales/2019/05/26/exclusivo-investigan-el-robo-de-519-000-euros-que-el-paris-saint-germain-le-pago-a-boca-por-el-pase-de-paredes/〔2020/6/10 確認〕
※ 60 日本経済新聞：ビジネスメール詐欺広がる 本物の書類でつい油断 https://www.nikkei.com/article/DGXMZO45609320T00C19A6000000/〔2020/6/10 確認〕
※ 61 St. Thomas Source：WAPA Missing $2.17 Million Was Stolen in Email Scam https://stthomassource.com/content/2019/06/11/wapa-missing-2-18-million-was-stolen-in-email-scam/〔2020/6/10 確認〕
※ 62 Bleeping Computer：North Carolina County Lost $1.7 Million in BEC Scam https://www.bleepingcomputer.com/news/security/north-carolina-county-lost-17-million-in-bec-scam/〔2020/6/10 確認〕
Cabarrus County：Cabarrus County Government targeted in social engineering scam https://cabarruscounty.us/news/cabarrus-county-government-targeted-in-social-engineering-scam/〔2020/6/10 確認〕
※ 63 650 CKOM：City of Saskatoon bilked out of more than $1 million https://www.ckom.com/2019/08/15/city-of-saskatoon-bilked-out-of-more-than-1-million-dollars/〔2020/6/10 確認〕
AFPBB News：カナダの自治体がフィッシング詐欺被害、8300 万円だまし取られる https://www.afpbb.com/articles/-/3240194〔2020/6/10 確認〕
※ 64 Naples Daily：Collier County scammed out of $184K in phishing scheme that investigators say originated abroad https://www.naplesnews.com/story/news/government/2019/08/19/collier-county-scammed-out-184-k-cyber-attack-phishing-scheme/2049019001/〔2020/6/10 確認〕
※ 65 ディープフェイク（deepfake）：AI（人工知能）技術の一つである「深層学習（deep learning）」と「偽物（fake）」を組み合わせた造語とされる。深層学習の技術を活用し、現実の映像や音声、画像の一部を加工して偽の情報を組み込み、あたかも本物のように見せかける。
※ 66 The Wall Street Journal：Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402〔2020/6/10 確認〕
ZDNet Japan：CEO になりすましたディープフェイクの音声で約 2600 万円の詐欺被害か https://japan.zdnet.com/article/35142255/〔2020/6/10 確認〕
※ 67 Iceland Review：Hackers Defraud Nearly Four Hundred Million From Power Company https://www.icelandreview.com/news/hackers-defraud-nearly-four-hundred-million-from-power-company/〔2020/6/10 確認〕
FRETTABLADID：Sviku út hundruð milljóna af HS Orku https://www.frettabladid.is/frettir/hundruum-milljona-stoli-af-hs-orku/
mbl.is：„Þetta er skipulögð og þróuð árás“ https://www.mbl.is/vidskipti/frettir/2019/09/09/thetta_er_skipulogd_og_throud_aras/〔2020/6/10 確認〕
※ 68 OCALA.com：Ocala police Scammers swiped nearly $750,000 from city https://www.ocala.com/news/20191028/ocala-police-scammers-swiped-nearly-750000-from-city
Bleeping Computer：BEC Fraudsters Divert $742,000 from Ocala City in Florida https://www.bleepingcomputer.com/news/security/bec-fraudsters-divert-742-000-from-ocala-city-in-florida/〔2020/6/10 確認〕
※ 69 Quartz：An extra letter “s” enabled a million-dollar real estate scam https://qz.com/1752282/how-compromised-emails-enable-cybercrime-and-real-estate-scams/〔2020/6/10 確認〕
※ 70 CTV News：Waterloo Brewing loses $2.1 million in wire transfer scam https://kitchener.ctvnews.ca/waterloo-brewing-loses-2-1-million-in-wire-transfer-scam-1.4695755〔2020/6/10 確認〕
※ 71 The Denver Post：Town of Erie scammed out of $1 million in Parkway Bridge project, town says https://www.denverpost.com/2019/12/30/erie-victim-financial-fraud-parkway-bridge/amp/〔2020/6/10 確認〕
CBS Denver：Erie Officials Release New Information In $1 Million Bridge Scam https://denver.cbslocal.com/2020/01/15/erie-bridge-scam-sema-construction/〔2020/6/10 確認〕
※ 72 トレンドマイクロ：米国の学校運営組織がビジネスメール詐欺により 230 万米ドルの被害 https://blog.trendmicro.co.jp/archives/23616〔2020/6/10 確認〕
KVUE-TV：Manor ISD loses $2.3M in phishing scam; police and FBI investigating https://www.kvue.com/article/news/education/schools/manor-isd-loses-millions-in-phishing-scam/269-296ff10a-c6d0-45e7-8b34-4fe0ed016715〔2020/6/10 確認〕

※ 73 Claims Journal：Fraudsters Posing as Art Dealer Got Gallery to Pay Millions https://www.claimsjournal.com/news/international/2020/01/30/295272.htm〔2020/6/10 確認〕
※ 74 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019年1月～3月］ https://www.ipa.go.jp/files/000073456.pdf〔2020/6/10 確認〕
※ 75 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019年4月～6月］ https://www.ipa.go.jp/files/000076713.pdf〔2020/6/10 確認〕
※ 76 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019年7月～9月］ https://www.ipa.go.jp/files/000078200.pdf〔2020/6/10 確認〕
※ 77 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019年10月～12月］ https://www.ipa.go.jp/files/000080133.pdf〔2020/6/10 確認〕
※ 78 IPA：プレス発表　本年確認されたビジネスメール詐欺の事例を解説、J-CSIP 運用状況レポートを公開 https://www.ipa.go.jp/about/press/20190726.html〔2020/6/10 確認〕
※ 79 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〔2020/6/10 確認〕
※ 80 IPA：なりすましメール撲滅に向けたSPF（Sender Policy Framework）導入の手引き https://www.ipa.go.jp/security/topics/20120523_spf.html〔2020/6/10 確認〕
※ 81 一般財団法人インターネット協会：DKIM (Domainkeys Identified Mail) https://salt.iajapan.org/wpmu/anti_spam/admin/tech/explanation/dkim/〔2020/6/10 確認〕
※ 82 Microsoft 社：侵害された Office 365 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〔2020/6/10 確認〕
※ 83 A10 ネットワークス株式会社：DDoS 攻撃者の武器 https://www.a10networks.co.jp/download/files/A10-EB-14115-JA2019Q2.pdf〔2020/6/10 確認〕
※ 84 wizSafe Security Signal 2019 年 1 月 観測レポート」～「wizSafe Security Signal 2019 年 12 月 観測レポート」を確認した。
株式会社インターネットイニシアティブ：観測レポートの記事一覧 https://wizsafe.iij.ad.jp/category/report/〔2020/6/10 確認〕
※ 85 Link11：Warning of Serious DDoS Blackmail Campaigns Attributed to Fancy Bear Group https://www.link11.com/en/blog/warning-of-serious-ddos-blackmail-campaigns-attributed-to-fancy-bear-group/〔2020/6/10 確認〕
※ 86 JPCERT/CC：DDoS 攻撃を示唆して、仮想通貨を要求する脅迫メールについて https://www.jpcert.or.jp/newsflash/2019103001.html〔2020/6/10 確認〕
※ 87 日本放送協会：ラグビーW杯組織委にサイバー攻撃 https://www.nhk.or.jp/politics/articles/lastweek/26369.html〔2020/6/10 確認〕
※ 88 Palo Alto Networks, Inc.：Muhstik Botnet Exploits the Latest WebLogicVulnerability for Cryptomining and DDoS Attacks https://unit42.paloaltonetworks.com/muhstik-botnet-exploits-the-latest-weblogic-vulnerability-for-cryptomining-and-ddos-attacks/〔2020/6/10 確認〕
※ 89 Palo Alto Networks, Inc.：Muhstik Botnet Attacks Tomato Routers to Harvest New IoT Devices https://unit42.paloaltonetworks.com/muhstik-botnet-attacks-tomato-routers-to-harvest-new-iot-devices/〔2020/6/10 確認〕
※ 90 株式会社インターネットイニシアティブ：Wikipedia, Twitch, Blizzard へ の DDoS 攻 撃 https://sect.iij.ad.jp/d/2019/09/175257.html〔2020/6/10 確認〕
※ 91 総務省：令和元年版情報通信白書 （2）IoT デバイスの急速な普及 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/html/nd112120.html〔2020/6/10 確認〕
※ 92 Microsoft 社：CVE-2019-0708 ¦ リモート デスクトップ サービスのリモートでコードが実行される脆弱性 https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2019-0708〔2020/6/10 確認〕
※ 93 Microsoft 社:CVE-2019-0708 のユーザー向けガイダンス ¦ リモート デスクトップ サービスのリモートでコードが実行される脆弱性：2019 年 5 月15日 https://support.microsoft.com/ja-jp/help/4500705/customer-guidance-for-cve-2019-0708〔2020/6/10 確認〕
※ 94 Microsoft 社：Microsoft works with researchers to detect and protect against new RDP exploits https://www.microsoft.com/security/blog/2019/11/07/the-new-cve-2019-0708-rdp-exploit-attacks-explained/〔2020/6/10 確認〕
※ 95 Comodo Security Solutions, Inc：Important Security Notice About Comodo Forums Accounts https://forums.comodo.com/general-announcements/important-security-notice-about-comodo-forums-accounts-t124921.0.html〔2020/6/10 確認〕
※ 96 株式会社ラック：【注意喚起】フォーラム構築ソフト「vBulletin」の深刻な脆弱性 (CVE-2019-16759) で攻撃通信の急増確認 https://www.lac.co.jp/lacwatch/alert/20190926_001937.html〔2020/6/10 確認〕
※ 97 WebARX：Critical Vulnerability In Ultimate Addons For Elementor & Ultimate Addons for Beaver Builder Plugins https://www.webarxsecurity.com/critical-vulnerability-in-ultimate-add-ons-elementor/〔2020/6/10 確認〕
※ 98 ステージング環境：運用（本番）環境と同等のシステム構成（ハードウェア、ソフトウェアとも）のテスト環境のこと。修正プログラム等の適用前に、適用による問題発生の有無を検証する環境。仮想化されたサーバ、ストレージ上に構築されることもある。
※ 99 トレンドマイクロ社：複数の脆弱性を利用してルータやデバイスを狙うボット型マルウェアの新亜種を確認 https://blog.trendmicro.co.jp/archives/22211〔2020/6/10 確認〕
※ 100 https://jvndb.jvn.jp/〔2020/6/10 確認〕
※ 101 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〔2020/6/10 確認〕
※ 102 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019年10月～12月］ https://www.ipa.go.jp/files/000080133.pdf〔2020/6/10 確認〕
IPA：OLE 機能を悪用した文書ファイルの手口に関する注意点 (第二版) https://www.ipa.go.jp/files/000080134.pdf〔2020/6/10 確認〕
※ 103 キヤノンマーケティングジャパン株式会社：MALWARE REPORT 2019 上 半 期 https://eset-info.canon-its.jp/files/user/malware_info/images/ranking/pdf/MalwareReport_2019FirstHalf.pdf〔2020/6/10 確認〕
※ 104 東京都：公益財団法人東京都保健医療公社が運用する端末等に対する不正アクセス被害の発生による、メールアドレス等の個人情報の流出と対応について（第二報） https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2019/06/07/06.html〔2020/6/10 確認〕
※ 105 トレンドマイクロ社：引き続き国内で拡大する「EMOTET」の脅威 https://blog.trendmicro.co.jp/archives/23648〔2020/6/10 確認〕
※ 106 JPCERT/CC：マルウエア Emotet の感染に関する注意喚起 https://www.jpcert.or.jp/at/2019/at190044.html〔2020/6/10 確認〕
※ 107-1 piyolog：国内で相次ぐ不審メールの注意喚起と返信型 Emotet についてまとめてみた https://piyolog.hatenadiary.jp/entry/2019/11/26/054443〔2020/6/10 確認〕
※ 107-2 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〔2020/6/10 確認〕
※ 108 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〔2020/6/10 確認〕
※ 109 ファイア・アイ株式会社：進化するマルウェア、EMOTET https://www.fireeye.jp/blog/jp-products-and-services/2019/12/evolving-malware-emotet.html〔2020/6/10 確認〕
※ 110 「編集を有効にする」ボタン：Microsoft Office の「保護ビュー」機能を有効にしている場合に、メールの添付ファイルやインターネット上のファイルを開くと表示されるボタン。
※ 111 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〔2020/6/10 確認〕
※ 112 サイバーリーズン・ジャパン株式会社:3 つの脅威:Emotet（エモテット）による TrickBot の展開と TrickBot によるデータの窃取および Ryuk の拡散 https://www.cybereason.co.jp/blog/cyberattack/3613/〔2020/6/10 確認〕
※ 113-1 ZDNet：Florida city fires IT employee after paying ransom demand last week https://www.zdnet.com/article/florida-city-fires-it-employee-after-paying-ransom-demand-last-week/〔2020/6/10 確認〕
※ 113-2 JPCERT/CC：マルウエア Emotet への対応 FAQ https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html〔2020/6/10 確認〕
※ 114 「情報セキュリティ白書 2018」の「1.3.4 ばらまき型メールによる攻撃」(p.34)を参照。
※ 115 JC3：インターネットバンキングマルウェア「DreamBot」による被害に注意 https://www.jc3.or.jp/topics/dreambot_cm.html〔2020/6/10 確認〕
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/dreambot.html〔2020/6/10 確認〕
※ 116 Proofpoint Inc.：Get2 ダウンローダーを使って新型の SDBbot リ

モートアクセス型トロイの木馬（RAT）を配信する TA505　https://www.proofpoint.com/jp/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader〔2020/6/10 確認〕
※ 117 JC3：運送系企業を装ったフィッシングの注意喚起　https://www.jc3.or.jp/topics/smsphishing.html〔2020/6/10 確認〕
JC3：不正アプリによる銀行を騙ったフィッシングサイトへの誘導　https://www.jc3.or.jp/topics/phishingsites.html〔2020/6/10 確認〕
※ 118 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〔2020/6/10 確認〕
※ 119 Gardia 株式会社：【お知らせ】運送会社や日本郵政を装った偽SMS（ショートメール）にご注意ください　https://gardia.jp/news/201909/sms/〔2020/6/10 確認〕
※ 120 朝日新聞：宅配業者装うSMSに注意　スマホ乗っ取られ詐欺に悪用　https://www.asahi.com/articles/ASM663JGXM66OIPE00G.html〔2020/6/10 確認〕
※ 121 JC3：新型コロナウイルスに乗じた犯罪　https://www.jc3.or.jp/topics/newmodel_coronavirus.html〔2020/6/10 確認〕
トレンドマイクロ株式会社：実例で見るネットの危険：「新型コロナウイルス」に便乗する攻撃メール　https://blog.trendmicro.co.jp/archives/23740〔2020/6/10 確認〕
※ 122 フィッシング対策協議会:ドコモをかたるフィッシング (2019/06/21)　https://www.antiphishing.jp/news/alert/docomo_20190621.html〔2020/6/10 確認〕
※ 123 独立行政法人国民生活センター：携帯電話会社をかたる偽 SMS にご注意!ーあなたのキャリア決済が狙われていますー　http://www.kokusen.go.jp/pdf/n-20190905_1.pdf〔2020/6/10 確認〕
JC3：通信事業者を騙るスミッシング詐欺の手法に係る注意喚起　https://www.jc3.or.jp/topics/smscert.html〔2020/6/10 確認〕
※ 124 フィッシング対策協議会：フィッシングレポート 2018　https://www.antiphishing.jp/report/pdf/phishing_report_2018.pdf〔2020/6/10 確認〕
フィッシング対策協議会：フィッシングレポート 2019　https://www.antiphishing.jp/report/pdf/phishing_report_2019.pdf〔2020/6/10 確認〕
※ 125 https://www.antiphishing.jp/report/pdf/phishing_report_2019.pdf〔2020/6/10 確認〕
※ 126 http://www.kokusen.go.jp/pdf/n-20190905_1.pdf〔2020/6/10 確認〕
※ 127 フィッシング対策協議会：月次報告書 2019/11 フィッシング報告状況　https://www.antiphishing.jp/report/monthly/201911.html〔2020/6/10 確認〕
※ 128 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〔2020/6/10 確認〕
※ 129 フィッシング対策協議会：多くの金融機関をかたるフィッシング（2019/12/26）　https://www.antiphishing.jp/news/alert/phishbank_20191226.html〔2020/6/10 確認〕
※ 130 IPA：安心相談窓口だより　性的な映像をばらまくと恐喝し、仮想通貨で金銭を要求する迷惑メールに注意　https://www.ipa.go.jp/security/anshin/mgdayori20181010.html〔2020/6/10 確認〕
※ 131 セクストーション（性的脅迫）：スマートフォンの SNS アプリでのやり取り等で入手したプライベートな写真や動画をばらまくと脅して金銭を要求する脅迫。
※ 132 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/help/4013405/windows-protect-from-tech-support-scams〔2020/6/10 確認〕
※ 133 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〔2020/6/10 確認〕
※ 134 自動継続課金：「一定の利用期間ごとに定額を支払う料金方式、且つ、利用契約が自動更新される」という意味で、当記事では用いている。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。
※ 135 McAfee, LLC：MoqHao Related Android Spyware Targeting Japan and Korea Found on Google Play　https://www.mcafee.com/blogs/other-blogs/mcafee-labs/moqhao-related-android-spyware-targeting-japan-and-korea-found-on-google-play/〔2020/6/10 確認〕
※ 136 ESET, spol. s r.o：Google Play にラジオアプリを偽装した新種のスパイウェアが侵入　https://www.eset.com/jp/blog/welivesecurity/first-spyware-android-ahmyth-google-play/〔2020/6/10 確認〕
※ 137 トレンドマイクロ株式会社：「App Store」と「Google Play」上で偽ギャンブルアプリが多数拡散　https://blog.trendmicro.co.jp/archives/22594〔2020/6/10 確認〕
※ 138 Google LLC：The App Defense Alliance: Bringing the security industry together to fight bad apps　https://security.googleblog.com/2019/11/the-app-defense-alliance-bringing.html〔2020/6/10 確認〕
※ 139 IPA：安心相談窓口だより　App Store 以外の配信アプリによるセクストーション被害を確認　https://www.ipa.go.jp/security/anshin/mgdayori20191224.html〔2020/6/10 確認〕
※ 140 Apple Inc.：Apple Developer Enterprise Program　https://developer.apple.com/jp/programs/enterprise/〔2020/6/10 確認〕
※ 141 東京 2020 オリンピック・パラリンピック競技大会のチケットの抽選結果を知らせるメールでも採用された。
公益財団法人東京オリンピック・パラリンピック競技大会組織委員会：観戦チケットに関する詐欺や模倣品の被害にご注意ください　https://tokyo2020.org/ja/news/notice-0006〔2020/6/10 確認〕
※ 142 https://www.tsr-net.co.jp/news/analysis/20200123_01.html〔2020/7/1 確認〕
※ 143 Security NEXT：登録者の個人情報 77 万件が流出 -「アンとケイト」　http://www.security-next.com/105209〔2020/7/1 確認〕
サイバーセキュリティ .com：不正アクセス被害の続報を発表、77 万件の顧客情報が流出｜アンとケイト　https://cybersecurity-jp.com/news/31442〔2020/7/1 確認〕
株式会社マーケティングアプリケーションズ：「アンとケイト」及び「ポケットアンとケイト」不正アクセスによるお客様情報流出に関するお詫びとご報告　https://www.ann-kate.jp/incident_reports/20190628/report3.html〔2020/7/1 確認〕
※ 144 Security NEXT：カードゲーム通販サイトで情報流出 - 旧サーバに不正アクセスか　http://www.security-next.com/112734〔2020/7/1 確認〕
サイバーセキュリティ .com：脆弱性悪用されサイト登録者情報 6 万 3 千件超流出か｜株式会社ホビーズファクトリー　https://cyberhoken-jp.com/news-235/〔2020/7/1 確認〕
株式会社ホビーズファクトリー：個人情報漏洩に関するお詫びとご報告　https://mtg.bigweb.co.jp/informations/press-release202002〔2020/7/1 確認〕
※ 145 Security NEXT：通販サイトに不正アクセス、個人情報流出の可能性 - 現代ギター社　http://www.security-next.com/111316〔2020/7/1 確認〕
サイバーセキュリティ .com：不正アクセスによりカード情報 133 件・顧客情報約2万件が流出か｜株式会社現代ギター社　https://cybersecurity-jp.com/news/34770〔2020/7/1 確認〕
株式会社現代ギター社：弊社が運営する「GG インターネットショップ」への不正アクセスによる個人情報流出に関するお詫びとお知らせ　https://info.gendaiguitar.com/owabi20200107.html〔2020/7/1 確認〕
※ 146 Security NEXT：「Emotet」に感染、メアド流出の可能性 - 関電グループ会社　http://www.security-next.com/112956〔2020/7/1 確認〕
ScanNetSecurity：Emotet 感染でメールアドレス約400件流出（関電アメニックス）　https://scan.netsecurity.ne.jp/article/2020/03/10/43798.html〔2020/7/1 確認〕
株式会社関電アメニックス：当社パソコンからの個人情報の流出の可能性について　https://www.k-amenix.co.jp/datas/news/pdf/020200306173217_JdXaU.pdf〔2020/7/1 確認〕
※ 147 朝日新聞デジタル：【独自】三菱電機にサイバー攻撃　防衛などの情報流出か　https://www.asahi.com/articles/ASN1M6VDSN1MULFA009.html〔2020/7/1 確認〕
朝日新聞デジタル：三菱電機へ高度なサイバー攻撃、中国政府の動きと呼応?　https://www.asahi.com/articles/ASN1X4JXHN1RULZU002.html〔2020/7/1 確認〕
三菱電機株式会社：不正アクセスによる個人情報と企業機密の流出の可能性について（第３報）　https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf〔2020/7/1 確認〕
ITmedia：三菱電機、約 8000 人の個人情報流出か　ウイルス対策システムにゼロデイ攻撃　https://www.itmedia.co.jp/news/articles/2001/21/news083.html〔2020/7/1 確認〕
※ 148 サイバーセキュリティ .com：不正アクセス被害で個人情報最大 3 万 1,231 件に流出の可能性｜エーデルワイン　https://cybersecurity-jp.com/news/31106〔2020/7/1 確認〕
株式会社エーデルワイン：弊社が運営する「エーデルワイン オンラインショップ」への不正アクセスによる個人情報流出に関するお詫びとお知らせ　https://edelwein.co.jp/1079〔2020/7/1 確認〕
※ 149 サイバーセキュリティ .com：ユニクロ・GU へ大規模なリスト型攻撃発生、顧客情報 46 万件超が流出か　https://cybersecurity-jp.com/news/31257〔2020/7/1 確認〕
株式会社ファーストリテイリング、株式会社ユニクロ、株式会社ジーユー:「リスト型アカウントハッキング（リスト型攻撃）」による弊社オンラインストアサイトへの不正ログインの発生とパスワード変更のお願いについて　https://

www.uniqlo.com/jp/corp/pressrelease/2019/05/19051409_uniqlo.html〔2020/7/1 確認〕
※ 150 サイバーセキュリティ .com：不正アクセスでカード情報 3 万 7 千件超が流出、不正利用の可能性も｜ヤマダ電機　https://cybersecurity-jp.com/news/31526〔2020/7/1 確認〕
株式会社ヤマダ電機：弊社が運営する「ヤマダウエブコム・ヤマダモール」への不正アクセスによる個人情報流出に関するお詫びとお知らせ　https://www.yamada-denki.jp/information/190529/〔2020/7/1 確認〕
※ 151 サイバーセキュリティ .com：不正プログラム混入で個人情報 4 万件超、クレカ情報 2,600 件に流出か｜株式会社サンポークリエイト　https://cybersecurity-jp.com/news/31610〔2020/7/1 確認〕
株式会社サンポークリエイト：不正プログラム混入による個人情報流出に関するお詫びとご報告　https://www.sanpogroup.jp/news/info/〔2020/7/1 確認〕
※ 152 サイバーセキュリティ .com：脆弱性悪用でクレカ情報 1 万 5 千件超流出、一部不正利用も｜株式会社 DigiBook　https://cybersecurity-jp.com/news/32091〔2020/7/1 確認〕
※ 153 サイバーセキュリティ .com：人材派遣会社ウェブサイトが不正アクセス被害、個人情報約 12 万件流出の可能性　https://cybersecurity-jp.com/news/32179〔2020/7/1 確認〕
株式会社ディンプル：弊社ホームページへの不正アクセスに関する調査報告について　https://www.dimples.co.jp/staff/page/info/334.html〔2020/7/1 確認〕
※ 154 サイバーセキュリティ .com：フォームジャッキングでクレカ情報 3 万件超流出の可能性｜株式会社金剛堂　https://cybersecurity-jp.com/news/32577〔2020/7/1 確認〕
株式会社金剛堂：弊社が運営する「金剛堂オンラインストア」への不正アクセスによるクレジットカード情報流出に関するお詫びとご報告　https://kongodo.co.jp/creditcard_info.php〔2020/7/1 確認〕
※ 155 サイバーセキュリティ .com：クレカ情報 210 件の流出を確認、さらに 4 万件超流出の可能性も｜株式会社おもちゃ箱　https://cybersecurity-jp.com/news/32854〔2020/7/1 確認〕
※ 156 サイバーセキュリティ .com：パスワードーリスト型攻撃で最大 3 万 8 千件超の個人情報流出か、43 万ポイント不正利用も｜株式会社アルペン　https://cybersecurity-jp.com/news/32955〔2020/7/1 確認〕
株式会社アルペン：「リスト型アカウントハッキング（リスト型攻撃）」による弊社会員管理システムへの不正ログインの発生とパスワード変更のお願いについて　https://store.alpen-group.jp/corporate/news/docs/20190807s02.pdf〔2020/7/1 確認〕
※ 157 サイバーセキュリティ .com：三井住友カード「Vpass アプリ」が不正アクセス被害、1 万 6,756 件の情報閲覧か　https://cybersecurity-jp.com/news/33067〔2020/7/1 確認〕
三井住友カード株式会社：弊社会員向けスマートフォンアプリでの不正ログインについて　https://www.smbc-card.com/company/news/news0001468.pdf〔2020/7/1 確認〕
※ 158 サイバーセキュリティ .com：みずほ「J コイン」のテスト用システムが不正アクセス被害、データ約 1 万 8 千件に流出の可能性　https://cybersecurity-jp.com/news/33234〔2020/7/1 確認〕
株式会社みずほフィナンシャルグループ 株式会社みずほ銀行：J-Coin Pay 加盟店管理に関わるテスト用システムへの 不正アクセスについて　https://www.mizuhobank.co.jp/release/pdf/20190904release_jp.pdf〔2020/7/1 確認〕
※ 159 サイバーセキュリティ .com：ラーメンデータベースが不正アクセス被害、利用会員 16 万 9,843 件のパスワード等流出か　https://cybersecurity-jp.com/news/33363〔2020/7/1 確認〕
株式会社スープレックス：不正アクセスによる会員様情報流出に関するお知らせとお詫び　https://ramendb.supleks.jp/information#99
※ 160 サイバーセキュリティ .com：子供服通販ショップが不正アクセス被害、カード情報 1 万 1 千件や登録個人情報 10 万件に流出の可能性　https://cybersecurity-jp.com/news/33533〔2020/7/1 確認〕
有限会社フィセル：個人情報流出に関するお詫びとお知らせ　https://www.ficelle.co.jp/?p=2490〔2020/7/1 確認〕
※ 161 サイバーセキュリティ .com：決済システム改ざん、カード情報含む 9 万件超の個人情報流出か｜京都一の傳　https://cybersecurity-jp.com/news/33758〔2020/7/1 確認〕
株式会社京都一の傳：弊社が運営する「京都一の傳　お取り寄せページ」への不正アクセスによる個人情報流出に関するお詫びとご報告　https://www.ichinoden.jp/topic/info01/〔2020/7/1 確認〕
※ 162 サイバーセキュリティ .com：セキュリティコード含む 10 万件超のクレカ情報流出、株式会社 JIMOS 運営サイトへサイバー攻撃　https://cybersecurity-jp.com/news/33825〔2020/7/1 確認〕
株式会社 JIMOS：不正アクセスによるお客様情報流出に関するお詫びとご報告 https://www.jimos.co.jp/release/detail.php?type=3&pk=122〔2020/7/1 確認〕
※ 163 サイバーセキュリティ .com：不正アクセス受けカード情報 1 万 6,109 件が流出か｜株式会社スタジオライン　https://cyberhoken-jp.com/news-200/〔2020/7/1 確認〕
株式会社スタジオライン：「MODERN BEAUTY TOKYO」への不正アクセス発生についてのご報告とお詫び　https://www.modernbeauty.jp/info/2019/〔2020/7/1 確認〕
※ 164 サイバーセキュリティ .com：不正アクセスで顧客情報約 28 万件流出の可能性｜象印マホービン株式会社　https://cybersecurity-jp.com/news/34443〔2020/7/1 確認〕
象印マホービン株式会社：【重要】個人情報流出についてのお知らせ（象印でショッピング）　https://www.zojirushi.co.jp/important_info.pdf〔2020/7/1 確認〕
※ 165 サイバーセキュリティ .com：電子小説サービスが不正アクセス被害、メールアドレスなど最大 3 万 3 千件超流出の可能性　https://cybersecurity-jp.com/news/34703〔2020/7/1 確認〕
株式会社ビーグリー：個人情報の流出に関するお詫びとお知らせ　https://www.beaglee.com/news/info/2019/12/5767/〔2020/7/1 確認〕
※ 166 https://privacymark.jp/system/reference/pdf/2018JikoHoukoku_190918.pdf〔2020/7/1 確認〕
※ 167 Security NEXT：顧客情報最大 6.7 万件が保存された PC を紛失 - ゼットン　http://www.security-next.com/107991〔2020/7/1 確認〕
株式会社ゼットン：ノートパソコン遺失による個人情報漏洩の可能性に関するお詫びとお知らせ　http://www.zetton.co.jp/company/IR/docs/ir_20190906.pdf〔2020/7/1 確認〕
※ 168 Security NEXT：水道利用者の個人情報 1.1 万件含む端末紛失 - 稲敷市　http://www.security-next.com/107687〔2020/7/1 確認〕
稲敷市：水道情報を記録した携帯型タブレット端末の紛失について　https://www.city.inashiki.lg.jp/page/page006138.html〔2020/7/1 確認〕
※ 169 Security NEXT：貯金者情報 1.7 万件含む資料をネット上に誤公開 - JA 横浜　http://www.security-next.com/110769〔2020/7/1 確認〕
JA 横浜：顧客情報流出に関するお詫びとお知らせ　https://ja-yokohama.or.jp/oshirase/20200221_01〔2020/7/1 確認〕
※ 170 株式会社ブロードリンク：盗難事件の経緯と再発防止について　https://www.broadlink.co.jp/safety/incident/overview/〔2020/7/1 確認〕
ITmedia：HDD など転売「7844 個」――行政文書流出、ブロードリンクが謝罪　ずさんな管理体制明らかに　https://www.itmedia.co.jp/news/articles/1912/09/news129.html〔2020/7/1 確認〕
※ 171 NHK 名古屋拠点放送局：個人情報の漏えいについてのお詫びとお知らせ　https://www.nhk.or.jp/privacy/oshirase/20191112.pdf〔2020/7/1 確認〕
※ 172 株式会社リクルートキャリア：『リクナビ DMP フォロー』の法的な不備とその影響範囲　https://www.recruitcareer.co.jp/r-dmpf/05/〔2020/7/1 確認〕
※ 173 https://www.ipa.go.jp/files/000057060.pdf〔2020/7/1 確認〕
※ 174 https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf〔2020/7/1 確認〕
※ 175 日本クレジットカード協会：クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画について　http://www.jcca-office.gr.jp/dealer/plan.html〔2020/7/1 確認〕
※ 176 一般社団法人日本クレジット協会：クレジットカードの不正利用防止対策と IC 化の取組み状況について　https://www.j-credit.or.jp/download/news20200228a1_2.pdf〔2020/7/1 確認〕
※ 177 経済産業省：「割賦販売法の一部を改正する法律案」が閣議決定されました　https://www.meti.go.jp/press/2019/03/20200303001/20200303001.html〔2020/7/1 確認〕
経済産業省：時代の要請を受けた消費者保護～ QR コード決済事業者等のセキュリティ対策～　https://www.meti.go.jp/shingikai/sankoshin/shomu_ryutsu/kappu_hambai/pdf/025_04_00.pdf〔2020/7/1 確認〕
※ 178 https://www.ipa.go.jp/security/announce/telework.html〔2020/7/1 確認〕
※ 179 NIST：National Vulnerability Database（NVD）　https://nvd.nist.gov/〔2020/6/10 確認〕
※ 180 公表年は、ベンダがアドバイザリを公開した年、他組織やセキュリティポータルサイト等の登録／公開した年、発見者が一般向けに報告した年等、脆弱性対策情報が一般に公表された年を指す。なお、JVN iPedia で脆弱性対策情報を公開した年は「登録年」としている。
※ 181 IPA：共通脆弱性識別子 CVE 概説　https://www.ipa.go.jp/security/vuln/CVE.html〔2020/6/10 確認〕
※ 182 The MITRE Corporation：CVE Numbering Authorities　https://cve.mitre.org/cve/cna.html〔2020/6/10 確認〕
※ 183 The MITRE Corporation：米国政府向けの技術支援や研究開発を行う非営利組織。80 を超える主要な脆弱性情報サイトと連携して、

脆弱性情報の収集と、重複のない CVE の採番を行っている。
※ 184 The MITRE Corporation：CVE Adds 7 New CVE Numbering Authorities (CNAs)　https://cve.mitre.org/news/archives/2016/news.html〔2020/6/10 確認〕
※ 185 The MITRE Corporation：Opera Added as CVE Numbering Authority (CNA)　https://cve.mitre.org/news/archives/2019/news.html〔2020/6/10 確認〕
※ 186 IPA：共通脆弱性タイプ一覧 CWE 概説　https://www.ipa.go.jp/security/vuln/CWE.html〔2020/6/10 確認〕
※ 187 IPA：共通脆弱性評価システム CVSS 概説　https://www.ipa.go.jp/security/vuln/CVSS.html〔2020/6/10 確認〕
※ 188 JPCERT/CC：セキュアコーディング　https://www.jpcert.or.jp/securecoding/〔2020/6/10 確認〕
※ 189 Adobe Systems Inc.：Flash & The Future of Interactive Content – Adobe　https://theblog.adobe.com/adobe-flash-update/〔2020/6/10 確認〕
※ 190 Microsoft 社：CVE-2019-0708 ¦ リモート デスクトップ サービスのリモートでコードが実行される脆弱性　https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/CVE-2019-0708〔2020/6/10 確認〕
※ 191 ASCII.jp：新たな「WannaCryptor」になるかもしれない脆弱性「BlueKeep」とは?　https://ascii.jp/elem/000/001/890/1890827/〔2020/6/10 確認〕
※ 192 株式会社イーシーキューブ：【重要】クレジットカード流出被害が増加しています。EC-CUBE ご利用店舗のセキュリティチェックをお願いいたします。（2019/12/23）　https://www.ec-cube.net/news/detail.php?news_id=348〔2020/6/10 確認〕
経済産業省：株式会社イーシーキューブが提供するサイト構築パッケージ「EC-CUBE」の脆弱性等について（注意喚起）　https://www.meti.go.jp/press/2019/12/20191220013/20191220013.html〔2020/6/10 確認〕
IPA：EC サイト構築で多く利用されている「EC-CUBE」を用いたウェブサイトでの情報漏えい被害の増加について　https://www.ipa.go.jp/security/announce/alert20191225.html〔2020/6/10 確認〕
※ 193 IPA：脆弱性関連情報の届出受付　https://www.ipa.go.jp/security/vuln/report/index.html〔2020/6/10 確認〕
※ 194 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」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」であることを指す。
※ 195 IPA：情報システム等の脆弱性情報の取扱いにおける報告書を公開　https://www.ipa.go.jp/security/fy2019/reports/vuln_handling/index.html〔2020/6/10 確認〕
※ 196 IPA：重要なセキュリティ情報一覧　https://www.ipa.go.jp/security/announce/alert.html〔2020/6/10 確認〕
※ 197 該当するバンキングアプリは、以下の Web ページに掲載されている。
株式会社エヌ・ティ・ティ・データ：Android アプリ「My Pallete」における SSL 通信時の脆弱性に関するお知らせ　http://www.dokodemobank.ne.jp/info_20200128_bankingapp.html〔2020/6/10 確認〕
※ 198 JVN:新着リスト　https://jvn.jp/index.html〔2020/6/10 確認〕
※ 199 IPA：TLS 暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）　https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html〔2020/7/7 確認〕
※ 200 IPA：安全なウェブサイトの作り方　https://www.ipa.go.jp/security/vuln/websecurity.html〔2020/6/10 確認〕
※ 201 IPA：Web Application Firewall(WAF) の導入に向けた検討項目～ WAF の製品・サービスの種類と選択基準について～　https://www.ipa.go.jp/files/000072484.pdf〔2020/6/10 確認〕
※ 202 The Chromium Projects：XSS Auditor　https://www.chromium.org/developers/design-documents/xss-auditor〔2020/6/10 確認〕