情報セキュリティ白書

Information Security White Paper

2021

進むデジタル、広がるリスク：守りの基本を見直そう

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

「情報セキュリティ白書2021」の刊行にあたって

2020 年度は、新型コロナウイルス感染症によるパンデミックに世界中が翻弄される年となりました。2020 年1月の中国を発端として、3月以降は世界各国で緊急事態宣言やロックダウンが実施され、サイバー空間では感染に関するデマや詐欺情報が氾濫し、インフォデミックと呼ばれる混乱状態が続きました。また感染対策として一斉に導入されたテレワークやオンライン会議に対するサイバー攻撃が急増し、IPA の「情報セキュリティ 10 大脅威 2021」では、「テレワーク等のニューノーマルな働き方を狙った攻撃」が組織編の第3位となりました。

この間、重要な組織やインフラを狙った攻撃も続きました。国内では、製造事業者、IT 事業者を狙ったサプライチェーン攻撃やランサムウェア攻撃が続き、情報流出や操業停止の被害を受けました。また米国では IT 事業者を経由した大規模サプライチェーン攻撃が、更に 2021 年5月にはエネルギー供給事業者に対するランサムウェア攻撃が発生しました。脆弱な組織からの侵入を狙ったサプライチェーン攻撃、また特定のターゲットからの高額な身代金を狙って手口が巧妙化したランサムウェア攻撃、これらが政府機関や企業にとって深刻な脅威であることが鮮明となりました。

日本政府を始め、各国政府はサイバーセキュリティ対策を引き続き強化し、IoT 機器の脆弱性対策、サプライチェーンにおけるリスクの可視化や情報共有、ガイドラインの整備、セキュリティ人材育成施策の整備等を進めてきましたが、まだまだ十分ではないことも鮮明となりました。

こうした中で、私達はパンデミック対策としての新しい生活・働き方（ニューノーマル）の定着、あるいは IT 活用による新しい価値創造を目指す DX の推進により、2年前に考えていたよりもはるかに速いテンポで生活や仕事のデジタル化を迫られています。日々の買い物ではスマートフォン決済が、仕事の打ち合わせや申請・承認手続きはオンラインが当たり前となり、ネット上での活動が記録・利活用されるようになる、といった変化がいつかは来るだろうがまだ先のこと、と思っていた私達は、否応なく巨大なデジタル空間に踏み出しつつあります。

セキュリティの視点からいえば、この変化は多くの不確定要因（リスク）を伴い、守れていると思っていたものが守れなくなる可能性があります。テレワークでは、情報システム部門がやっていた対策を自分自身でやる必要があるかもしれません。DX 推進では、デジタル化したデータの何を秘密とし、何を共有するかを決めるには試行錯誤が必要でしょう。デジタル化で広がるこうしたリスクを把握し、対処することは容易ではありませんが、まずは誰が責任を持ち、何を秘密として守るのかを見直し、共通認識とすることが大変重要ではないかと思います。そして、この見直しは今こそ必要であると思います。

本白書が、多くの方々に広く利用され、新しい生活や働き方のリスクに対する意識を高め、備えを実践するための一助となることを祈念します。

2021年7月

独立行政法人情報処理推進機構（IPA）

理事長　富田達夫

目次

コラム

2021

情報セキュリティ白書

序章

2020年度の情報セキュリティの概況

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

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

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

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

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

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

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

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

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

国内では、2020 年 6 月に「政府情報システムのためのセキュリティ評価制度（ISMAP）」が開始された。政府のクラウドサービス調達におけるセキュリティ水準の確保、クラウドサービスの円滑な導入に資することが期待される。また、11 月には中小企業を含むサプライチェーンのセキュリティ強化の枠組みとして、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）が設立された。サイバー攻撃の実態や取り組みに関する情報共有、中小企業に求められるセキュリティ水準検討等に関する業界横断的な活動が期待される。

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

2020 年度の情報セキュリティの概況

	主な情報セキュリティインシデント・事件	主な情報セキュリティ政策・イベント
2020 年　4 月	● テレワーク環境やオンライン会議サービスの脆弱性、及びビジネスメール詐欺について、国内外で注意喚起（1.2.3、1.3.1、2.2.2） ● イスラエル水道システムにサイバー攻撃（3.1.1）	■ 交通 ISAC が創設（3.1.4） ■ 米国でテレワークのセキュリティガイダンス、コロナ禍における重要インフラ基盤の運用と従業員の安全に関するガイダンスを公開（2.2.2）
5 月	● 情報通信事業者が海外拠点からの不正アクセスを公表（1.2.1） ● ノルウェーの投資ファンドが海外送金で 1,000 万ドルのビジネスメール詐欺被害（1.2.3）	■ 欧州で位置情報及び接触追跡ツールに関するガイドライン、研究目的の健康情報処理に関するガイドラインを公開（2.2.3） ■ 米国でサプライチェーンリスク管理指針を公開(2.2.2)
6 月	● 国内大手自動車メーカやアルゼンチン電力会社がランサムウェア攻撃被害を公表（3.1.1） ● Ripple20 のゼロデイ脆弱性を公表（1.2.5、3.1.2、3.2.2）	■「政府情報システムのためのセキュリティ評価制度（ISMAP）」運用開始（2.6.3）
7 月	● 情報通信事業者が BYOD 端末経由の不正アクセスを公表（1.2.1）	■「サイバーセキュリティ 2020」公開（2.1.1） ■「IoT・5G セキュリティ総合対策 2020」公開（2.1.3）
8 月	● IPA が新たなランサムウェア攻撃について注意喚起(1.2.2) ● 米国金融機関が海外送金 1,080 万ドルのビジネスメール詐欺被害(1.2.3)	■ IPA が「脆弱性対処に向けた製品開発者向けガイド」公開（3.2.4） ■ 米国 NIST が SP 800-207（ゼロトラストアーキテクチャ）公開（3.4.2）
9 月	● 携帯通信会社が提供するマネーサービスを介した銀行の預金の不正引き出しが発覚（1.1.2）	■ 経済産業省が「サイバーセキュリティ体制構築・人材確保の手引き第 1 版」公開（2.1.2、2.3.1）
10 月	● JPCERT/CC がランサム DDoS 攻撃の注意喚起（1.2.4）	■ 総務省が「スマートシティセキュリティガイドライン（第 1.0 版）」公開（2.1.3）
11 月	● ゲーム会社が「新たなランサムウェア攻撃」被害を公表（1.2.2） ● NISC が「新たなランサムウェア攻撃」について注意喚起（1.2.2）	■ サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）設立（2.1.2、2.4.2） ■「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」策定（2.1.2、3.1.4）
12 月	● NISC、JPCERT/CC が VPN 製品の脆弱性に対する注意喚起（1.2.5、1.3.1、3.1.2） ● 米国でネットワーク管理用プラットフォームのウイルス感染で大規模被害公表（3.1.1）	■「情報システム・モデル取引・契約書」第二版公開（2.1.2） ■ 米国 NIST が SP 800-53 Rev.5（組織のセキュリティ・プライバシー管理策）更新（3.4.2）
2021 年　1 月	● NISC がクラウドサービス製品の設定不備について注意喚起（1.2.8） ● Europol による Emotet テイクダウン（1.2.6）	■ 産業サイバーセキュリティ研究会 WG1 に宇宙産業 SWG を設置（2.1.2）
2 月	● 米国で浄水場への攻撃で薬品投入量を操作される被害（3.1.1）	■ 警察庁、総務省、ICT-ISAC、及び ISP 各社が連携して、Emotet 感染の恐れのある利用者に注意喚起を行う取り組みを開始（1.2.6）
3 月	● 海外航空会社の顧客管理システムが不正アクセスを受け、加盟していた日本の航空会社にも被害（1.2.8）	■ サイバーセキュリティに関する国連オープン・エンド作業部会最終会合開催（2.2.1）

※ 2020 年度の主な情報セキュリティインシデント・事件、及び主な情報セキュリティ政策・イベントを示している。標的型攻撃、ランサムウェア被害、ビジネスメール詐欺、DDoS 攻撃、Web 改ざん、フィッシング等の攻撃や被害は通年で発生している。表中の数字は本白書中に掲載している項番である。特に注目されたもののみを挙げた。他のインシデントや手口と対策、及び政策・イベント等については本文を参照していただきたい。

第1章
情報セキュリティインシデント・脆弱性の現状と対策

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

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

1.1 2020年度に観測されたインシデント状況

本節では2020年度に観測された世界と日本における情報セキュリティインシデントの発生状況について概説する。

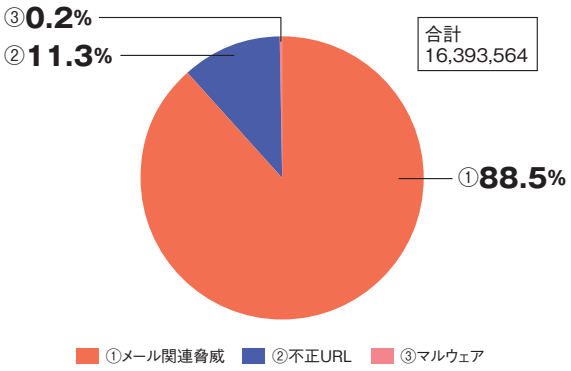
1.1.1 世界における情報セキュリティインシデント状況

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

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

(1) 新型コロナウイルス感染症に関連する脅威

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

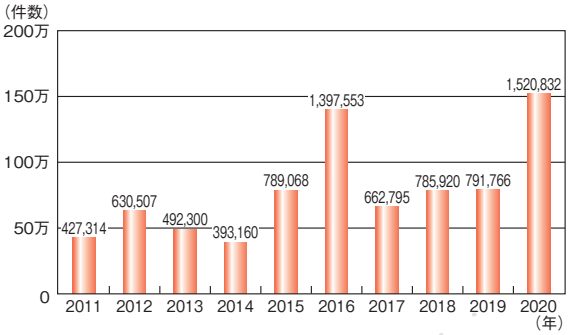


■図1-1-1　新型コロナウイルス関連脅威検出数のタイプ別割合（2020年）
（出典）トレンドマイクロ社「2020年年間セキュリティラウンドアップ」を基にIPAが編集※8

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

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

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



■図 1-1-2　世界における届け出されたフィッシングサイト件数（2011～2020年）
（出典）APWG「Phishing Activity Trends Reports」を基にIPAが作成

(2) フィッシングとビジネスメール詐欺の傾向

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

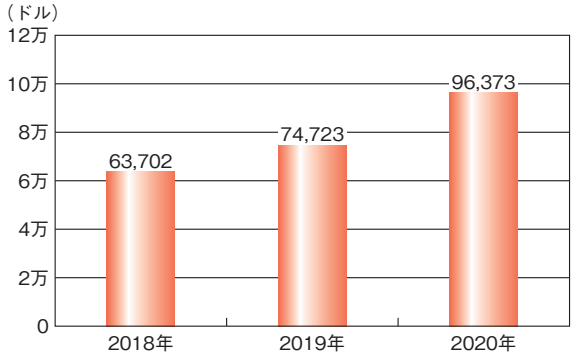
ターゲットとなる業種は、2020年の1年間では、「SaaS/Webmail」が28.1%、「金融機関」が20.5%、「ペイメント（支払い）」が14.0%と続いている。この3業種がターゲット業種の上位を占める傾向は2017年以降変わっていない。

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

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

(3) 情報漏えいインシデントの状況

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



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

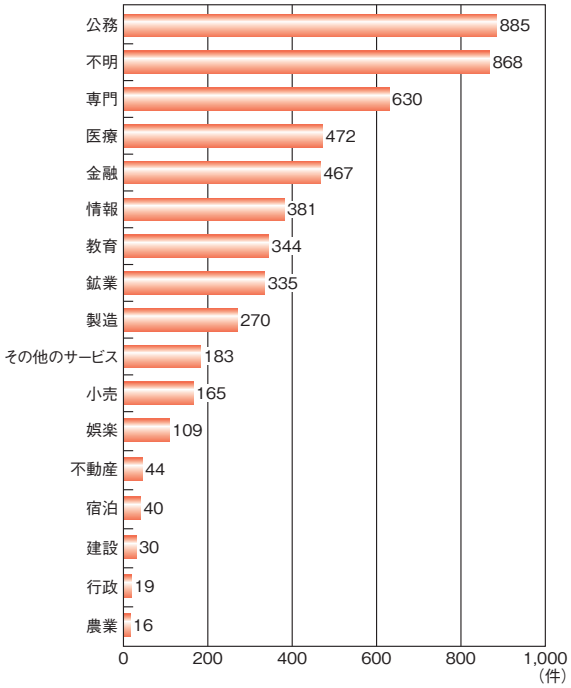
SolarWinds社）のネットワーク集中監視・管理用のソフトウェアプラットフォームOrionにおける事例を紹介する※10。SolarWinds社のOrionの正規のアップデートを通じてバックドアが組み込まれ、不正アクセスが行われた。攻撃の影響を受けたと見られる顧客数は約1万8,000に上った※11。米国の国土安全保障省（DHS：Department of Homeland Security）や国防総省（DoD：Department of Defense）等の政府機関やFireEye, Inc.※12のようなセキュリティベンダ等で様々な情報が窃取された（「2.2.2 (3) SolarWinds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

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

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

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

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

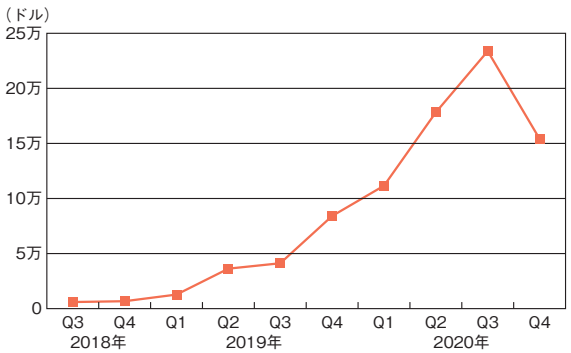


※「専門」とは、弁護士、会計士、アーキテクト、研究所、コンサルティング会社等を指す

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

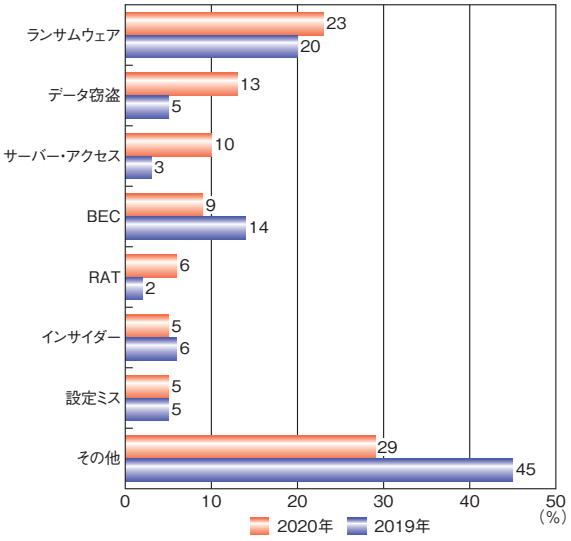
(4) ランサムウェアによる攻撃の傾向

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



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

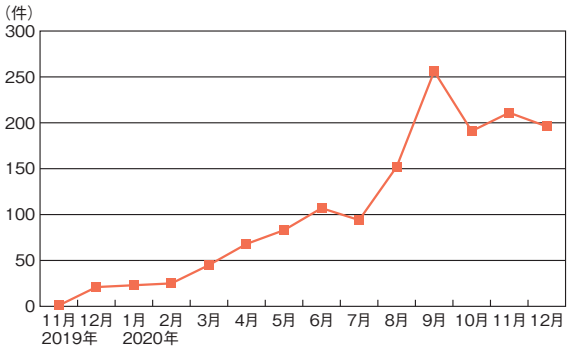
IBM 社によると、サイバーインシデントの主要な攻撃手法として 2020 年に最も多かったのは「ランサムウェア」の 23% で、続いて「データ窃盗」「サーバー・アクセス」となった（図 1-1-6）。



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

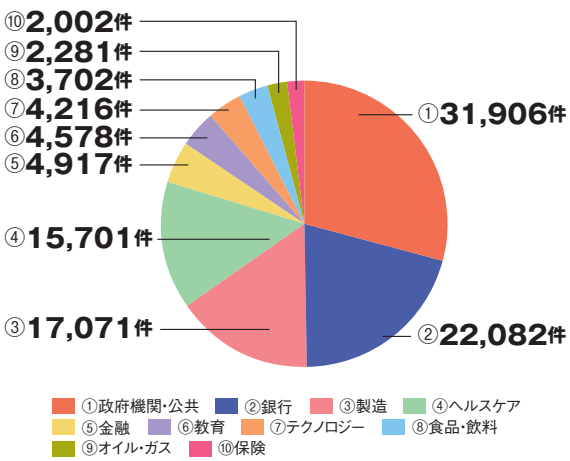
また、ランサムウェアによるサイバー攻撃のうち 59% が、ランサムウェアによるデータの暗号化に加えて、機密情報の窃取を行う「二重の脅迫」を用いた戦術であったとされる（「1.2.2 新たなランサムウェア攻撃」参照）。更に 2020 年に公表された情報漏えいのうち、ランサムウェア関連のデータ漏えいが 36% を占めていた。

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



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

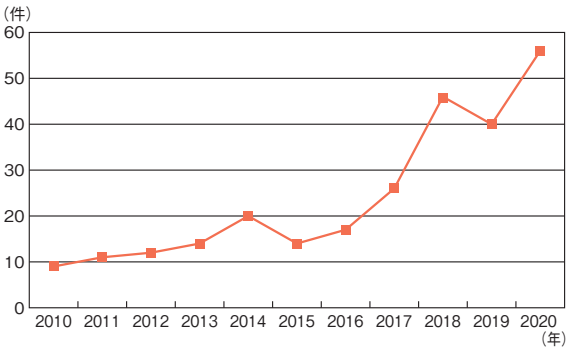
また、ランサムウェアが検出された件数が多かった上位 3 業種は「政府機関・公共」「銀行」「製造」だった（次ページ図 1-1-8）。



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

(5) ウイルスのマルチプラットフォーム化

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

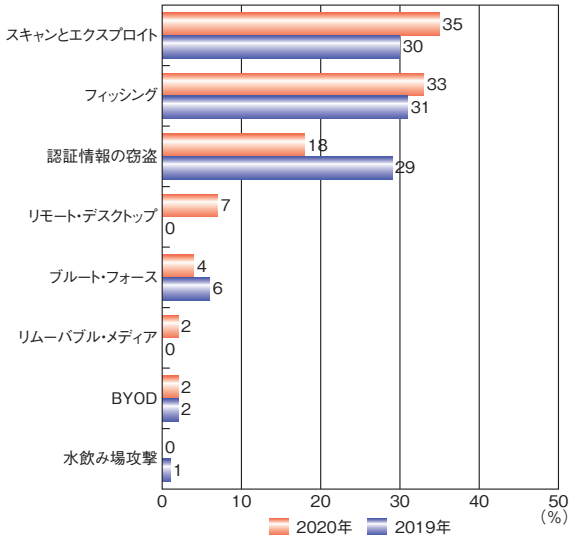


■図 1-1-9　新しく発見された Linux を狙ったウイルスのファミリー数の変化（2010 ～ 2020 年）
（出典）Intezer Labs「2020 Set a Record for New Linux malware families」を基に IPA が編集

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

(6) 脆弱性を突く攻撃の増加

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



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

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

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

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

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

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

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

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

1.1.2 国内における情報セキュリティインシデント状況

国内における情報セキュリティのインシデント発生状況について、主に以下の資料を参照して概説する。

- 三井物産セキュアディレクション株式会社（以下、MBSD 社）による集計情報※20
- トレンドマイクロ社：2020 年年間セキュリティラウンドアップ
- 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC：Japan Computer Emergency Response Team Coordination Center）：インシデント報告対応レポート※21
- フィッシング対策協議会：月次報告書※22

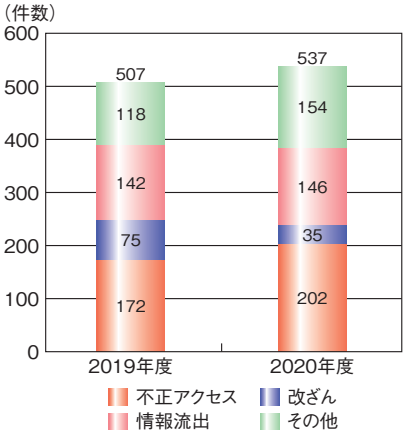
(1) 情報セキュリティインシデントの発生状況

MBSD 社によれば 2020 年の「情報セキュリティインシデントの種類別報道件数」は 537 件で、2019 年の 507 件から 5.9% 増であった（図 1-1-11）※23。割合が最も多いのは「不正アクセス」で、37.6% であった。前年比では、「不正アクセス」が 117.4%、「改ざん」が 46.7%、「情報流出」が 102.8%、「その他」が 130.5% であった。

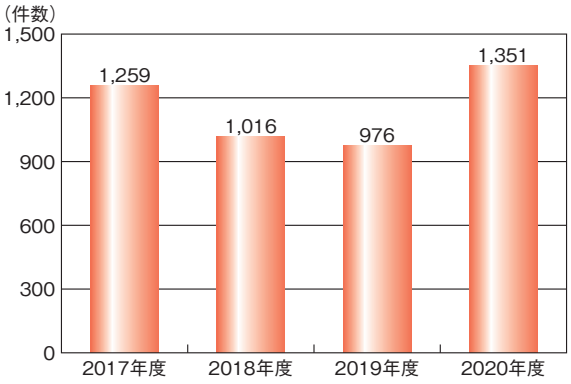
(2) Web サイト改ざんによる被害

2020 年 4 月 1 日から 2021 年 3 月 31 日までに JPCERT/CC へ報告された Web サイト改ざん件数は 1,351 件で前年比 138.4% であった（図 1-1-12）。

過去 4 年間では、2020 年度の報告件数が最も多い。

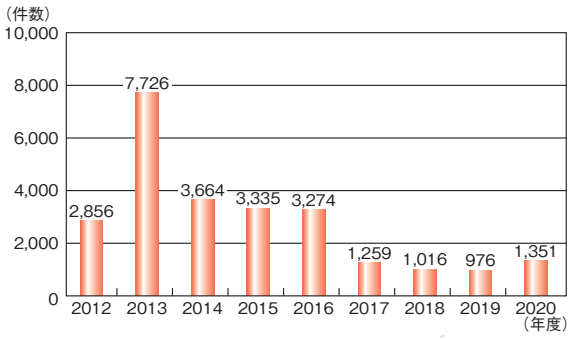


■図 1-1-11　情報セキュリティインシデントの種類別報道件数
（出典）MBSD 社の集計情報を基に IPA が作成



■図 1-1-12　Web サイト改ざん年度別件数推移（2017 ～ 2020 年度）
（出典）JPCERT/CC「インシデント報告対応レポート」（2017 年 4 月 1 日～ 2021 年 3 月 31 日）を基に IPA が作成

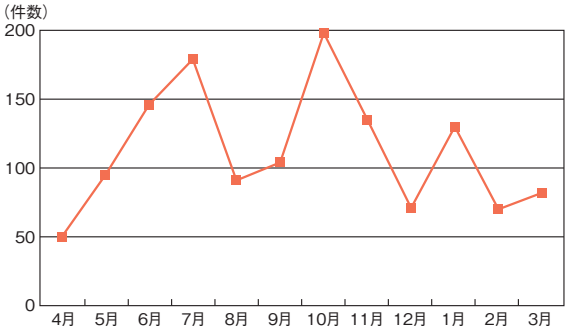
しかし更に遡れば、2014 年度から 2016 年度の 3 年間は 3,000 件を超える改ざんが報告されていた（図 1-1-13）。当時と比べて直近の 4 年間は 1,000 件前後で推移しており、小康を保っているといえる。



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

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

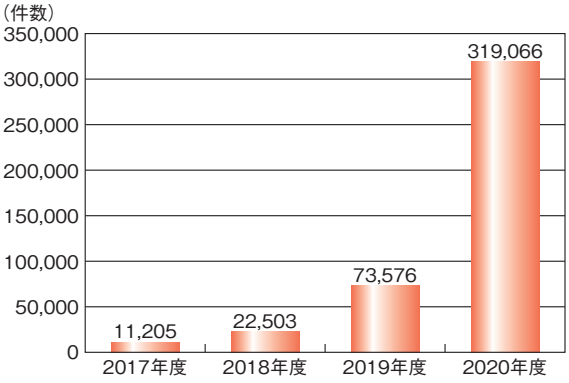
よれば当該四半期は、改ざんされたWebサイトから、特定ブランドを扱うEコマースサイトに誘導される事例が複数寄せられたという※24。そのほか、4～6月期にはWebサイトに不正に埋め込まれたコードによって「当選詐欺」のサイトに転送される事例が多く確認された。この当選詐欺ページでは個人情報の入力が求められることから、個人情報の収集が目的だと考察している※25。



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

(3) フィッシングによる被害

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

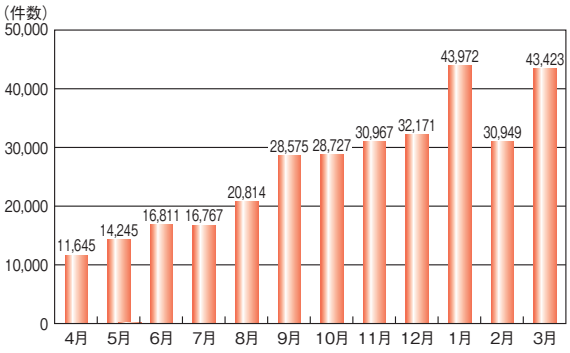


■図1-1-15　年度別フィッシング報告件数（2017～2020年度）
（出典）フィッシング対策協議会「月次報告書」（2017年4月～2021年3月）を基にIPAが作成

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

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

楽天も年度を通じ常に報告件数の上位4社に入って



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

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

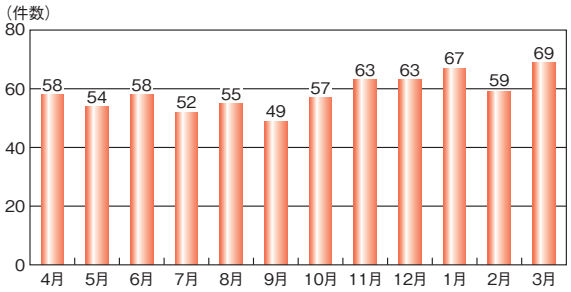
	4月	5月	6月	7月	8月	9月
1位	Amazon	Amazon	Amazon	Amazon	Amazon	Amazon
2位	Apple	Apple	Apple	Apple	LINE	楽天
3位	LINE	LINE	LINE	楽天	楽天	三井住友カード
4位	楽天	楽天	楽天	LINE	楽天カード	LINE
	10月	11月	12月	1月	2月	3月
1位	Amazon	Amazon	Amazon	Amazon	Amazon	Amazon
2位	三井住友カード	三井住友カード	三井住友カード	三井住友カード	三井住友カード	楽天
3位	楽天	楽天	楽天	楽天	楽天	MyJCB
4位	MyJCB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

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

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

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

フィッシングは従来のメールによるものだけでなく、SMS



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

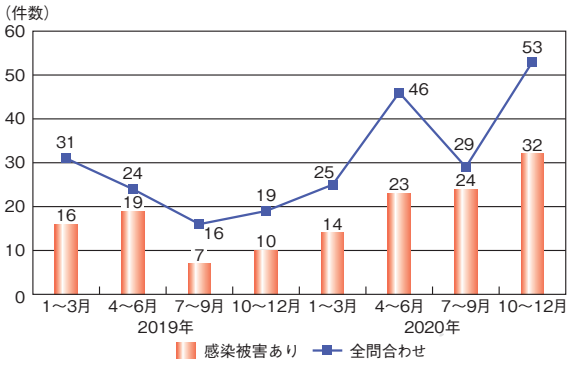
（Short Message Service）から誘導させるものがあり、メールに比べ本物と誤認したり、ついアクセスしてしまう傾向があるという。また、フィッシング以外にも年度を通じて、宅配業者の不在通知を装った SMS についての報告が多く受領されていた※29。IPA の安心相談窓口に寄せられる相談も前年を上回り、手口に変化が生じていることも確認している（「1.2.7（3）（a）宅配便の不在通知を装う SMS」参照）。

（4）注目された新たな脅威

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

（a）新たなランサムウェア

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



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

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

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

（b）VPN 製品の脆弱性

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

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

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

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

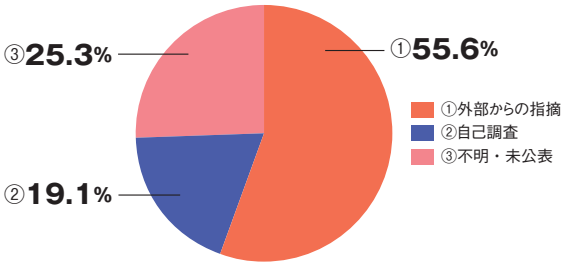
だけでなく、利用経験が浅く、不慣れなまま急速に利用が進み、脆弱性対策情報の収集やアップデートが疎かになった可能性をIPAでは指摘している（VPNの脆弱性については「1.3.1(3)テレワーク等で使われるソフトウェアの脆弱性について」参照。また攻撃については「1.2.5(1)VPN製品の脆弱性を対象とした攻撃」参照）。

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

(c)クラウドサービスからの情報漏えい

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

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

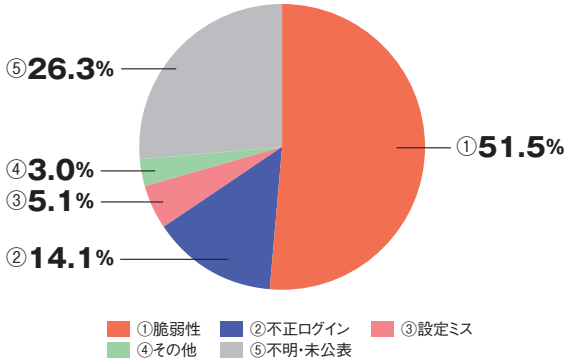


■図1-1-19　2020年に公表されたクラウドからの情報漏えい事例99件の発覚事由
（出典）トレンドマイクロ社「2020年年間セキュリティラウンドアップ」を基にIPAが編集

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

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

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



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

(d)「ドコモ口座」を利用した不正送金

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

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

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

COLUMN

AIとセキュリティ

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

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

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

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

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

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

1.2 情報セキュリティインシデント種類別の手口と対策

本節では、インシデントの種類別の発生状況と、具体的な事例について述べる。また、2020 年度に確認されたサイバー攻撃の手口を中心に解説する。

1.2.1 標的型攻撃

標的型攻撃とは、ある特定の企業・組織や業界等を狙って行われるサイバー攻撃の一種である。ウイルスメールやフィッシングメールを不特定多数の相手に無差別に送り付ける攻撃とは異なり、標的型攻撃は、特定の企業・組織や業界が持つ機密情報の窃取やシステム・設備の破壊・停止といった、明確な目的を持って行われる。また、標的型攻撃は長期間継続して行われることが多く、攻撃者が標的とする組織（以下、標的組織）の内部に数年間潜入して活動していたと考えられる事例も日本国内で確認されている※31。

IPA では、過去の事例等から、標的型攻撃の流れを五つの段階に分類している（図 1-2-1）。

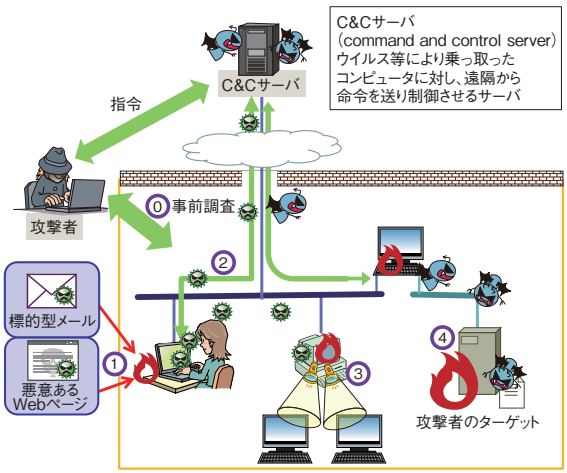
「事前調査段階」では、標的組織や業界の情報を収集する。公開されている情報を収集するだけでなく、標的組織と他の組織とのメールによるやり取りの盗聴等により必要な情報を収集することもある。

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

「初期潜入段階」で標的組織の内部に侵入した攻撃者は、「攻撃基盤構築段階」へと移り、標的組織内のパソコンを遠隔操作するため、遠隔操作ウイルス（RAT: Remote Access Trojan）に感染させることを試みる（バックドアの作成を試みる）。この際、遠隔操作を長期的かつ継続的に行うため、複数の RAT に感染させる場合もある。RAT への感染は、別のウイルスをダウンロードする機能を持つ「ダウンローダ」と呼ばれるウイルスを用いて行われることが多い。

次の「システム調査段階」では、「攻撃基盤構築段階」で感染させた RAT を使用して、組織内ネットワークの攻撃に必要なウイルスやツールを送り込む。これらのウイルスやツールを用いて、組織内ネットワークの調査、管理者権限の奪取、目的とする情報の探索等を行う。なお、「攻撃基盤構築段階」や「システム調査段階」で使われるツールには、感染したパソコン内で利用できる正規のツールや、広く公開されているオープンソースソフトウェアが悪用される場合もある。

「攻撃最終目的の遂行段階」では、攻撃者は、目的とする情報の窃取等を行う。海外の事例では、情報の窃取ではなく、工場や発電所といった生活インフラを支える施設の停止等を目的とした攻撃も確認されている※33。



⓪［事前調査段階］
ターゲットとなる組織を攻撃するための情報を収集する。

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

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

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

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

■図 1-2-1　標的型攻撃の流れ
（出典）IPA「標的型サイバー攻撃の脅威と対策※32」を基に編集

(1) 国内の標的型攻撃事例

ここでは、2020 年度に確認された、国内組織の海外

拠点を狙った標的型攻撃の事例を紹介する。

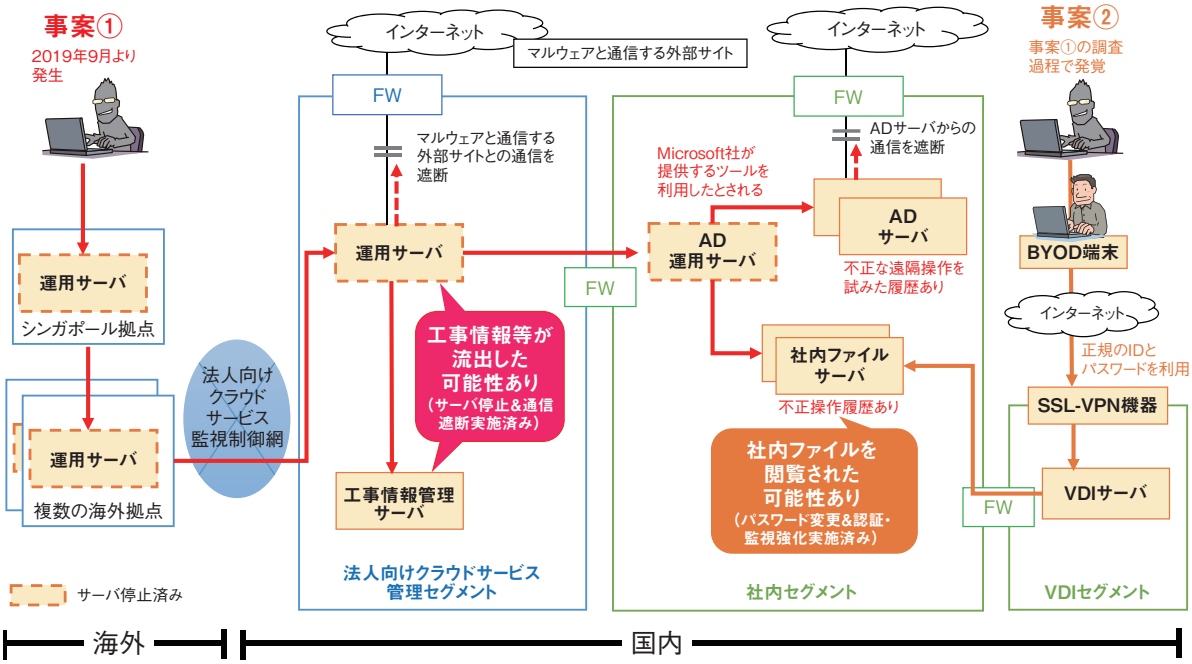
2020 年 5 月に、エヌ・ティ・ティ・コミュニケーションズ株式会社（以下、NTT コム社）の海外拠点への侵入を発端とした標的型攻撃の事案が、同社プレスリリースにて発表された※34。更に、7 月には第 2 報が報告された※35。

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

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

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

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



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

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

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

(2) 標的型攻撃の傾向

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

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

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

(3) 標的型攻撃の手口（初期侵入段階）

初期侵入段階における、代表的な標的型攻撃の手口を以下に示す。

なお記載する手口はこれまで確認されているものの一部であり、業務形態や IT 環境・セキュリティ対策の変化に合わせ、攻撃者もその手口を変化させていくことが容易に想像でき、新たな手口への注意も必要である。

(a) 標的型攻撃メール

標的型攻撃メールは、標的とする企業・組織・業界でよく用いられる言葉を使用し、メールの信憑性を高めることで、添付ファイルの実行または悪意のあるファイルのダウンロードを行わせるものである。

攻撃者はメールの信憑性を高めるため、標的とする企業に関係する組織や官公庁が公表している情報等から、その業界特有の用語や関係者の情報を「事前調査段階」で集め、それを件名、本文、署名等に利用するケースが過去に確認されている。2020 年には、「新型コロナウイルス」「日露や日韓の外交」「企業への履歴書や申し込み」等がメールの題材として悪用されていたことが確認されている※40。

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

(b) サプライチェーン・海外拠点等への攻撃

前述の国内組織の海外拠点を狙った事例のように、標的となる組織のネットワークやシステムを直接狙うのではなく、サプライチェーンにおける取引先企業や、海外拠点または海外の子会社を初期侵入のターゲットにした攻撃の手口が確認されている。

これは、海外拠点に対しては国内のセキュリティガバナンスが届きにくい傾向があり、特に小規模の組織や拠点ではセキュリティレベルが低くなる傾向が強いためである。攻撃者は事前調査段階で、標的組織のネットワークやサプライチェーン全体を見渡し、そのうちの脆弱な箇所を、侵入のための足掛かりとしている。

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

(c) VPN 製品や公開サーバ等の脆弱性を悪用した攻撃

国内のセキュリティベンダが観測した標的型攻撃では、攻撃者は標的組織への侵入経路として、SSL-VPN 製品の脆弱性を利用していたことが報告されている※41。

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

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

(d) SNS を悪用した攻撃

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

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

(4) 標的型攻撃の手口（攻撃基盤構築段階）

侵入後の攻撃基盤構築段階における手口の一部を、以下に示す。

(a) オープンソースソフトウェアや標準的なソフトウェア等を利用した攻撃

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

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

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

(b) 認証情報の取得

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

(c) AD サーバを標的とした攻撃

標的組織に侵入した攻撃者は、AD サーバを次のターゲットにする傾向がある。

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

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

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

なお AD サーバを攻撃目標とする事例は、標的型攻

撃だけではなく、ランサムウェア攻撃でも多く報告されている。

(5) 標的型攻撃への対策

標的型攻撃の傾向や手口に記載したとおり、攻撃者はあらゆる手段を利用し、計画的かつ巧妙に攻撃を遂行する。このため、ある対策を取れば完全に防御できるというものではなく、多層的防御が必要である。組織の規模や業種により取り得る対策は異なるが、情報資産を守る側としてはあらゆる可能性を考慮し、対策の検討と選別、実施が必要である。以下に、その一例を示す。

(a) 利用者の意識向上

利用者の意識向上を目的とした対策例を以下に示す。

- 不審メールに対する注意力の向上

  標的型攻撃では、標的とする企業・組織に関連する人物のメールアカウントを攻撃者が悪用してメールを送信するものや、組織や業界固有の用語等をメール本文中で用いて自然な文章を装ったもの等、受信者を騙すために巧妙な手口が使われることが多い。しかしながら、すべての標的型攻撃メールが見破れない程完成度の高いものではないことも事実としてある。

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

  不審メールにおいて注意すべき点の例を以下に示す。

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

- SNS を悪用した手口の周知

  攻撃者は SNS を悪用し、求人や共通の趣味等、個人への関心を装って対象者に近づき、信頼関係を構築する。そして、悪意のあるファイルを送り、それを開かせることで侵入経路を開拓する。

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

- マクロ機能の危険性の周知

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

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

- 標的型訓練メール等で実践的な訓練を実施

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

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

(b) 組織としての対応体制の強化

組織として攻撃に対応していくための体制の強化を図る対策例を以下に示す。

- CSIRT 設置と運用

  利用者が標的型攻撃メール等の不審なメールを受信した際に、連絡すべき窓口が組織内に周知されていることも対策の一つとして重要である。窓口が周知されていない場合、利用者がどこに連絡すればよいのか分からず、組織が攻撃を受けていることに気付くのが遅れてしまう可能性がある。また、組織外から連絡を受けて標的型攻撃の被害に気付くことも考えられる。そのため、外部からの連絡を受ける窓口を設けることも重要となる。

  このような、組織内部・外部における適切な連絡体制の整備やセキュリティインシデントが発生した際の調査・分析、セキュリティの教育・啓発活動の実施等を行う組織・体制のことを CSIRT（Computer Security Incident Response Team）と呼ぶ。セキュリティインシデントの未然防止、またはインシデント発生時の迅速な対応を行うために、CSIRT やそれに準ずる体制を組織内に設置することは有効な手段である。

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

- インシデント対応力の強化

  組織内に CSIRT 等の体制を整えるだけではなく、実際にセキュリティインシデントが発生した際、適切な対応ができるように対応能力を維持・向上させる取り組みが必要となる。

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

- 流行している攻撃の手口や対策の組織内共有

  今後も引き続き、標的型攻撃によるセキュリティインシデントが、その被害を受けた組織から公表され、また各報道機関やセキュリティベンダがその手口や対策を発表していくことが想定される。

  これらの情報を CSIRT 等が定期的に収集し、自組織において同様の脅威となり得るか確認し、必要であれば自組織の対策に組み込むことは重要である。具体的には、攻撃者の侵入手口が特定機器の脆弱性を突いたものであれば、自組織のシステムに該当する機器や脆弱性がないか確認し、修正プログラムが適用されていなければ適用する。標的型攻撃メールにより攻撃が行われたのであれば、社内の利用者にそのメールの特徴を周知することで、類似した攻撃メールによる被害が発生しないようにすることが望ましい。

- 海外拠点・サプライチェーンを意識したセキュリティの強化

  攻撃者グループはより侵入がしやすい海外拠点や海外子会社、取引先企業をターゲットにする傾向がある。このため、海外拠点・サプライチェーンを意識したセキュリティの強化が求められている。

  具体的には、海外拠点においても国内拠点と同様にセキュリティポリシーが策定・周知され、またセキュリティリスクの可視化と、改善や対策活動が行われることが望ましい。実施の際には、所在地の法制度や労働慣行の違い等も把握して、国内と同一の対策が取れない場合は代替策を考える必要がある。

  また、国内・海外を問わず取引先等においては、セキュリティの対策状況や連絡体制を事前に共有し、セキュリティインシデント発生時の連携を容易にすることで、サプライチェーンを狙った標的型攻撃にいち早く対処可能となる。

(c) システムによる対策

システムによる対策例を以下に示す。

- 不審メールを警告する仕組みの導入

  組織のメールシステムでメール受信時に、送信者（From）メールアドレスの偽装や、フリーメールアドレスの利用、悪用されやすい添付ファイルの拡張子やファイルタイプ、メール内の URL リンク先の情報等を検知し、必要に応じて利用者へ警告を行うことで、利用者に不審メールであると気付く機会を与えることが可能である。

  また添付ファイル付きメールの受信時やインターネット上のファイルダウンロード時には、ウイルス検査はもちろん、サンドボックス上で動的にファイル解析を行うことも有効である。

  加えてセキュリティインシデント発生に備え、不審メールを確保できる仕組みを導入することが望ましい。確保することで、不審メールの解析が可能となり、解析結果を組織全体で活用し対策を取ることができる。

- 適切な修正プログラムの適用
  標的型攻撃では、OS やアプリケーション、VPN 製品といった機器の脆弱性を悪用するケースも存在する。そのため、IT 資産管理システム等を活用し、組織内のすべてのサーバ・端末に適切に修正プログラムが適用できる仕組みを作ることが望ましい。
  特に今回手口として紹介したとおり、初期潜入段階ではインターネットに公開されたサーバや VPN 製品等のネットワーク製品の脆弱性を狙い、侵入後には AD サーバや情報の格納されたファイルサーバが攻撃の対象となる傾向があるので、それらについて抜かりなく対策していきたい。
- 通常業務で使わないファイルの実行・ソフトウェアの利用防止
  利用者が通常の業務で使わないであろうファイルや、ソフトウェアについては、あらかじめ、システムやポリシーで制御することが望ましい。具体的には、利用者の環境で実行可能なファイルの種類やソフトウェアを許可リスト化しておくことで、ウイルスへの感染を防止する。許可リストのみによる制限の実施が難しい場合は、利用者の環境で実行することが望ましくないファイルの種類やソフトウェアを特定し禁止リスト化する。
  例えば、悪用されることの多い PowerShell や JavaScript 等のスクリプトファイル（拡張子が .js や .ps1 等のファイル）のような、業務で使用しないであろうファイルの実行を禁止する。
- セキュリティ対策の再チェック
  2020 年は新型コロナウイルス感染拡大により、テレワークの新規開始や利用拡大等、働き方が大きく変化した年となった。このため一部の組織では、急遽、VPN 製品等のシステム導入や、システム構成または設定の変更を行った結果、適切なセキュリティ設計や設定が行われず、これが脆弱な箇所となるケースもあったと思われる。
  そのようにセキュリティ設定をあえて緩和したことを認識している場合には、改めてセキュリティ対策が現状のままでよいか再検討することが望ましい。
- ネットワーク構成の変化に合わせた対策
  働き方の多様化により、仕事場を従来の職場に限定せず、在宅でも可能にする勤務形態や、BYOD 端末の業務利用の広まりにより、これまでのような組織内ネットワークとインターネットの境界におけるセキュリティ対策だけでは、侵害を防ぐことが難しくなってきている。そのため、パソコンや携帯端末等の業務端末（エンドポイント）において不審な挙動を監視し、攻撃活動の抑え込みを行う EDR（Endpoint Detection and Response）製品の導入等を検討することも必要である。またクラウドの利用等によって、業務情報を自社システム外に保管するケースも増えてきており、データそのものへのセキュリティ対策（暗号化や DLP（Data Loss Prevention）等）を検討することも必要になるであろう。

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

1.2.2 新たなランサムウェア攻撃

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

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

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

開のための Web サイト（以下、リークサイト）にて公開される。

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

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

新たなランサムウェア攻撃では、IT システムを利用し、事業を行っている、あらゆる企業・組織が標的となり得る。2020 年 8 月に IPA[※51] が、また同年 11 月に内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）[※52] が注意喚起を行っており、非常に注意を要する状況にあるといえる。

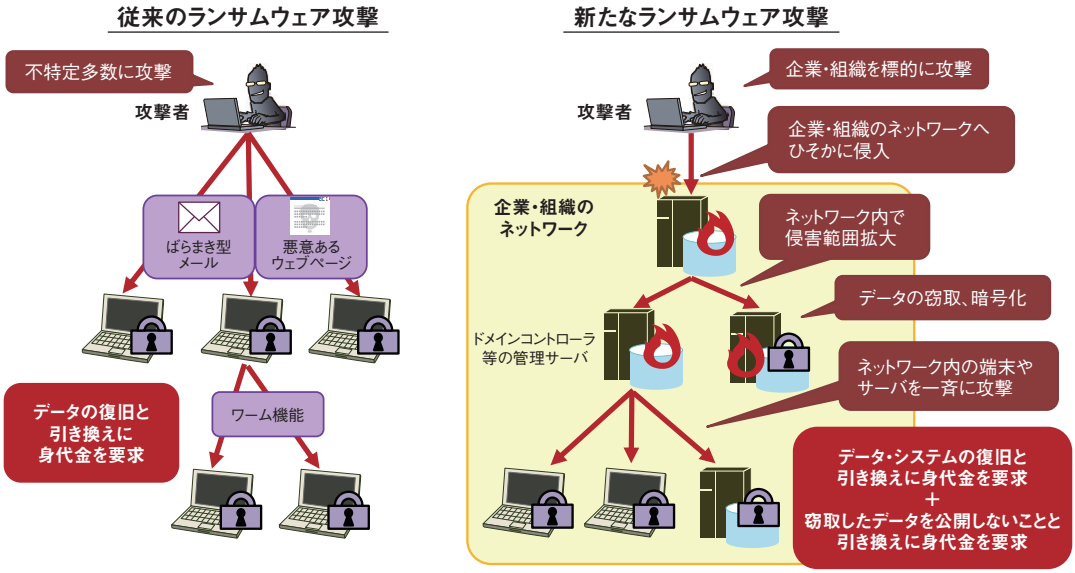
(1) 新たなランサムウェア攻撃の被害事例

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

(a) 国内のゲーム会社の被害事例

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

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



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

ること等を主張している。

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

(b) 国内の建設会社の被害事例

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

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

本事例は、数百台規模でデータの暗号化やセキュリティソフトのアンインストールが行われたことから、攻撃者が 1 台ずつ操作を行ったとは考えにくく、ドメインコントローラのような管理サーバ経由で、ランサムウェア感染やパソコンの不正操作が一斉になされたものと推測される。

(2) 新たなランサムウェア攻撃の傾向

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

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

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

(3) 攻撃手口

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

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

ここでは、各ステップで用いられると推測される攻撃手口について紹介する。

(a) ネットワークへの侵入

新たなランサムウェア攻撃は、攻撃者が企業・組織のネットワークへ侵入するところから始まる。ネットワークへの侵入手口として次のような手口が報告されている※63。

- リモートデスクトップサービスや VPN 製品を経由した侵入
  攻撃者は、企業・組織がインターネット上に公開しているリモートデスクトップサービスや VPN 製品を調査し、アクセス制御、認証に関する設定、パスワードの強度が不十分であれば、それを狙い、認証を突破し、侵入する。
- VPN 製品の脆弱性を悪用した侵入
  攻撃者は、企業・組織が使用している VPN 製品に残存する脆弱性を悪用して侵入する。例えば次のような脆弱性が悪用されたとの情報がある（VPN 製品の

脆弱性については「1.2.5 (1) VPN 製品の脆弱性を対象とした攻撃」参照)。
  - 認証情報を窃取することが可能な脆弱性（CVE-2018-13379、CVE-2019-11510 等）
  - 遠隔で任意のコードを実行することが可能な脆弱性（CVE-2019-1579、CVE-2019-19781 等）
- ウイルスメールによる侵入
  攻撃者は、企業・組織へ遠隔操作ウイルス等を添付したメールや、遠隔操作ウイルス等をダウンロードさせる URL リンクを記載したメールを送り付ける。受信者が不用意に添付ファイル等を開くことで、遠隔操作ウイルス等に感染させられ、パソコンが乗っ取られる。攻撃者は、そのパソコンを足掛かりとして組織内ネットワークへ侵入する。

(b) ネットワーク内の侵害範囲拡大

攻撃者は、企業・組織のネットワークへの侵入に成功した後、データの窃取やランサムウェアの感染範囲を拡げる目的で、ネットワーク内で侵害範囲拡大を行う。標的型攻撃同様、ネットワーク構成の把握や管理者権限の奪取を行い、これらの情報を基にして、機微情報等が保存されているパソコンやサーバ、ドメインコントローラ等の管理サーバ、そしてバックアップ用のサーバ等に侵入すると考えられる（ドメインコントローラの一種である Active Directory を標的とした攻撃については「1.2.1 (4) (c) AD サーバを標的とした攻撃」参照)。

(c) データ窃取

データの窃取は、攻撃者が二重の脅迫を狙っている場合に行われる。遠隔操作ウイルスを使用する等、攻撃者自身の操作によって、データの探索・収集、攻撃者のサーバやクラウドストレージへのアップロード等が行われるものと推測される。

(d) データの暗号化・システム停止

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

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

(e) 窃取したデータの公開

窃取したデータの公開は、攻撃者が二重の脅迫を狙っている場合に行われる。方法としては、リークサイトでの公開や、オークション形式での販売が挙げられる。攻撃者は窃取したデータをリークサイトで公開する際に、被害者への身代金支払いの圧力を高めるため、窃取したデータを一度にすべて公開するのではなく、一部だけ公開し、指定した期日までに身代金を支払わないと、徐々に公開するデータの範囲を広げるといった声明を出す場合がある。

(4) 新たなランサムウェア攻撃への対策

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

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

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

(a) 企業・組織のネットワークへの侵入対策

新たなランサムウェア攻撃は、攻撃者が企業・組織内のネットワークへ侵入することから始まる。そのため、次のような侵入対策を行うことが重要である。

- 攻撃対象領域(attack surface)の最小化
  攻撃対象領域とは、攻撃者が攻撃可能な範囲のことで、例えばインターネット上に公開されているサーバやネットワーク機器等を指す。インターネットからアクセス可能な、あるいは意図的に公開するサーバやネットワーク機器等を最小限にするとともに、アクセス可能なプロトコルやサービスも最小限にする。また、それらの機器が乗っ取られる可能性を考慮し、そこからアクセス可能な範囲を限定する。例えば、不用意にリモートデ

スクトップサービスをインターネット上に公開しない、業務に必要なサーバ等をインターネット上に公開する場合は、どの機器を公開しているか等の管理を行う、といった対策が挙げられる。

- アクセス制御と認証
  企業・組織外からアクセス可能な機器等を最小限にした上で、それらが攻撃者に不正に操作されないよう、適切なアクセス制御と認証を行う必要がある。例えば、運用上、機器へのアクセスが国内からのみであれば、海外の IP アドレスからのアクセスを遮断するといった対策が考えられる。また、多要素認証のような強固な認証方式を使用して、認証を突破しにくくすることや、アクセスや認証のログを取得、監視して、不審な行為や攻撃の検知を試みることも有効である。
- 脆弱性対策
  「1.2.2 (3) (a) ネットワークへの侵入」で紹介したとおり、攻撃者は脆弱性を悪用して、ネットワークへ侵入することがある。そのため、OS 及び利用ソフトウェア、ネットワーク機器のファームウェア等を常に最新の状態に保ち、脆弱性を悪用されないようにする。また、脆弱性が公開されてから、その脆弱性が悪用されるまでの期間が短くなっていることから、公開された脆弱性に迅速に対応できるよう体制や計画を整えておく。特にネットワーク機器の脆弱性への対応は、業務への影響が大きく、迅速な対応が困難な場合があるが、そのような脆弱性は攻撃者の狙い目となる可能性があり、注意が必要である。
- 拠点間ネットワークのセキュリティ強化
  新たなランサムウェア攻撃に限らず、自組織で複数の拠点をネットワークで接続している場合、例えば十分にセキュリティ対策ができていない防御の弱い海外拠点から侵入され、組織の中枢が侵害される場合がある。必要に応じ、拠点間のアクセス制御の強化も検討する。
- 攻撃メール対策
  新たなランサムウェア攻撃に限らず、攻撃メール対策も重要である。攻撃メール対策には、セキュリティ装置等を用いて不審なメールの検知・隔離を行うシステムによる対策や、従業員への社内教育、啓発、訓練による対策等がある（攻撃メール対策については「1.2.1 (5) 標的型攻撃への対策」参照）。

(b) ネットワーク内の侵害範囲拡大への対策

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

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

(c) データの暗号化やシステム停止への対策

データの暗号化やシステム停止への対策として、事業継続に重要なデータやシステムのバックアップを行う。ただし、新たなランサムウェア攻撃への対策として重要なことは、データの保護のみならず、「システムの再構築を含めた復旧計画」を事前に策定しておくことである。この攻撃では、企業・組織のパソコンやサーバ等が一斉に数千、数万台といった規模で暗号化され、バックアップしたデータまでもが暗号化される可能性がある。こうした状況に備え、業務継続やシステムの再構築に必要なリソース等を考慮した復旧計画を策定しておく。

(d) データの窃取とリークへの対策

データが窃取され、意図せず公開される脅威への対策として、IRM（Information Rights Management）[※65] 等の活用や、ネットワーク分離が挙げられる。IRM を活用し、データが窃取されても被害を限定的な範囲に留める。また、ネットワーク分離では、例えば、メールの送受信や Web 閲覧等で使用する一般的な業務用のネットワークと機密情報等を取り扱うネットワークを分離する。こうすることで、攻撃者に業務用のネットワークに侵入されたとしても、機密情報等を取り扱うネットワークには到達されないようにする。ただし、ネットワーク分離は運用コストや利便性に著しい影響があるため、重要性やリスクを踏まえて、実施を検討する必要がある。

(e) インシデント対応

被害を受けてしまった際のインシデント対応はケースバイケースとなるが、攻撃の手口が標的型攻撃と同様のため、対応も全体的に標的型攻撃と同様となる。インシデント対応の一般的な進め方について、JPCERT/CC が

マニュアル※66を公開しているため、参照いただきたい。

新たなランサムウェア攻撃のインシデント対応において、留意すべき点として、「ステークホルダーとのコミュニケーションができる体制作り」がある。新たなランサムウェア攻撃では、一般のインシデントと異なり、業務停止や顧客・取引先の情報漏えいが発生し、自組織内に閉じたインシデントで終わらない傾向がある。ステークホルダーとの適切な連絡・調整を含む、経営層を含めた体制作りが必要である。

1.2.3 ビジネスメール詐欺（BEC）

ビジネスメール詐欺（BEC：Business Email Compromise）は、巧妙な騙しの手口を駆使した偽のメールを企業・組織に送り付け、従業員を騙して送金取り引きに関わる資金を詐取する等の金銭被害をもたらすサイバー攻撃である。偽のメールを送るための前段階として、企業の従業員や取引先のメールアカウント情報を狙うため、フィッシング攻撃や情報を窃取するウイルスが使用されることもある※67。

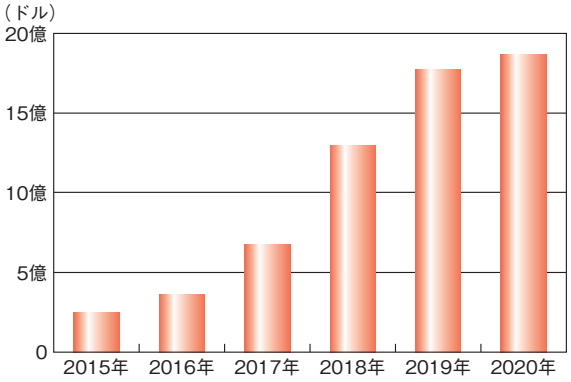
本項では、2020年度に公表されたビジネスメール詐欺の状況、事例を紹介し、その巧妙な手口と対策について解説する。

(1) ビジネスメール詐欺の被害状況

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

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

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



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

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

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

(2) 2020年度に報道された事例の概要

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

(3) IPAが情報提供を受けた事例の概要

IPAでは、実際に試みられたビジネスメール詐欺の事例を基に、2017年4月※90と2018年8月※91に続き、2020年4月に第三報※92として注意喚起を行った。また、サイバー情報共有イニシアティブ（J-CSIP※93：Initiative for Cyber Security Information Sharing Partnership

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

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

of Japan）の運用状況レポートで定期的に事例を公開している※94。

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

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

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

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

(4) IPA が情報提供を受けた事例

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

(a) 事例の概要

本事例は、2020 年 1 月、J-CSIP の参加組織（国内企業）の海外グループ企業（A 社：支払側）と、その海外取引先企業（B 社：請求側）との間で取引を行っている中、B 社の担当者になりすました攻撃者から、偽の口座への振り込みを要求するメールが送られたものである。

この手口は、IPA が 2017 年 4 月に公開した注意喚起※90 で紹介しているビジネスメール詐欺の五つのタイプのうち、「タイプ 1:取引先との請求書の偽装」に該当する。

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

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

- 請求書の修正を装い偽の口座を連絡する手口

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

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

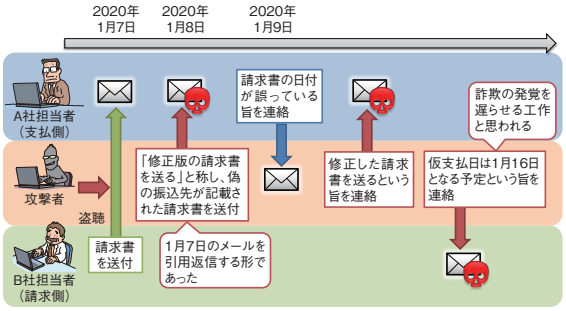
- 詐称用ドメインの取得と悪用

(b) 請求書の修正を装い偽の口座を連絡する手口

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

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

攻撃に関係したメールのやり取りの前半を図 1-2-5 に示す。



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

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

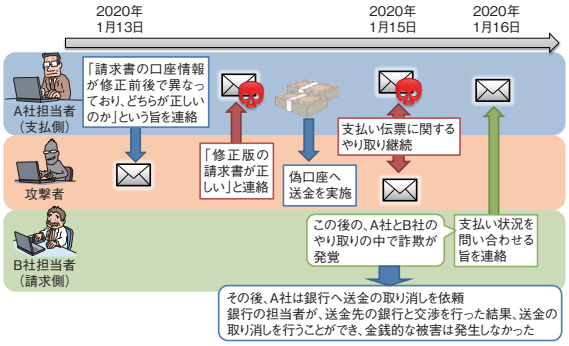
ビジネスメール詐欺では、本件のように、請求書等に記載された口座情報が、攻撃者によって改変されている手口が多く見られる。A 社担当者は、請求書の口座情報が異なっていることに気付いたタイミングで不審に思うことができた可能性はあるが、結果として偽のメールであると気付くことはできなかった。

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

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

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

攻撃に関係したメールのやり取りの後半を図 1-2-6 に示す。



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

(c) 詐称用ドメインの取得と悪用

攻撃者は A 社と B 社の正規のドメインに似通った「詐称用ドメイン」を新規に取得して、メールの送信に使用していた。詐称用ドメインは、図 1-2-7、図 1-2-8(次ページ)に示すように、正規のドメイン名を 1 文字変更したものであった。

(5) ビジネスメール詐欺の騙しの手口

ビジネスメール詐欺で用いられる騙しの手口は様々であるが、「情報セキュリティ白書 2020」の「1.2.2(5)ビジネスメール詐欺の騙しの手口」にて、実際に使われた具体

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

※実際に悪用されたものとは異なる。

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

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

※実際に悪用されたものとは異なる。

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

的な手口を紹介しているため、そちらを参照いただきたい。攻撃者は多様な手口を組み合わせて巧妙に攻撃を仕掛けてくる場合があり、注意が必要である。

(6) ビジネスメール詐欺への対策

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

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

(a) ビジネスメール詐欺の周知徹底と情報共有

ビジネスメール詐欺は、企業間のビジネス活動がメールに依存している点を悪用した巧妙な騙しの手口であり、その手口を知らなければ、被害を防止することは困難である。また、ビジネスメール詐欺におけるなりすましは外部企業との取り引きだけでなく、グループ会社同士の取り引きにおいても発生している。このため、海外関連企業を含む全グループ企業の全従業員に対して詐欺の手口について周知徹底し、ビジネスメール詐欺への意識を高めておくことが重要である。特に、最高財務責任者（CFO：Chief Financial Officer）や経理部門等金銭を取り扱う部門の担当者がビジネスメール詐欺の脅威についてよく理解し、送金前に攻撃に気付くことができれば、金銭的な被害を未然に防ぐ可能性が高まる。

メールに普段とは異なる言い回しや表現の誤りがあった、突然送信エラーメールを受信するようになった等、不審な兆候が見られた場合、CSIRT 等の社内の適切な部門に報告できる体制を整え、その情報を組織内外で共有することも重要である。ビジネスメール詐欺は、自組織だけではなく、取引先に被害が及ぶことがあり、取引先と情報を共有することにより、サプライチェーン全体でビジネスメール詐欺への耐性を高めることができる。自組織を詐称したビジネスメール詐欺を確認した場合や自組織が被害に巻き込まれた場合等に、取引先や、警察、金融機関へ報告し、同様な攻撃を受ける可能性のある企業一般に向けても注意喚起を行うといった体制を整えておくことで、更なる被害拡大を防ぐことが可能となる。

(b) 電子署名等によるなりすまし防止

ビジネスメール詐欺はメールのやり取りにおいて本物の担当者になりすますことで攻撃を成立させる。そのため、取引先と連携した対策として請求書等の重要情報をメールで送受信する際は電子署名を付ける等の手段で、なりすましを防止する対策も有効である[※101]。

(c) 送金処理のチェック体制強化

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

(d) 攻撃に使われるメールアドレスへの対策

ビジネスメール詐欺の攻撃者は、フリーメールを悪用する場合や、自組織のドメイン名に似せた詐称用のドメインを取得し、そのドメインのメールアドレスを用いて攻撃を行うことがある。フリーメールや自組織外のメールアドレスから着信したメールについて、件名や本文にその旨の警告を表示するメールシステムを採用すれば、従業員は、フリーメールや自組織と紛らわしいドメインからのメールを見分けやすくなる。なお、このようなメールシステムを利用していても、取引先の中小企業でフリーメールをビジネスに使っている場合や、攻撃者が取引先等のドメイン名に似せた詐称用のドメインを取得し、そのドメインのメールアドレスを用いる場合等、真正なメールと偽のメールの区別がつきにくい場合があるため、注意が必要である。また、メールを返信する際は、返信先のメールアドレスが

正しいかどうか、落ち着いて確認することが有効である。攻撃者が、送信元（From ヘッダ）を正しい送信者のメールアドレスに偽装し、返信先（Reply-To ヘッダ）を攻撃者のメールアドレスにする手口があるため、送信元（From ヘッダ）と返信先（Reply-To ヘッダ）が異なる際に警告を表示する機能があるメールシステムも有効である。

(e) フィッシング・ウイルス・不正アクセス対策

ビジネスメール詐欺では、攻撃者は攻撃に至る前に、何らかの方法でメールを盗み見ている場合がある。その方法として、フィッシング攻撃によるメールアカウントの詐取、ウイルス感染等によるメールの内容やメールアカウント情報の窃取、メールサーバへの不正アクセス等がある。そのため、基本的なフィッシング対策・ウイルス対策・不正アクセス対策が必要である。

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

また、攻撃者によってメールアカウントが乗っ取られ、利用者本人が行っていない転送設定やフォルダの振り分け設定がされている等、不正利用の兆候があった場合には、Microsoft 社等より該当アカウントへの対処方法が公開※103 されているため、そちらも参照いただきたい。

1.2.4 DDoS攻撃

DDoS（Distributed Denial of Service）攻撃とは、複数の送信元から同時に大量のパケットを送信することで、ネットワークやシステムリソースを消費させサービス遅延や停止を引き起こす攻撃である。結果として、正当なユーザによるサービスの利用が阻害される。

(1) DDoS 攻撃の動向

セキュリティベンダによれば、自社の DDoS 攻撃対策サービスで検知及びブロックした DDoS 攻撃数は 2020 年第 1 四半期から急増し、第 2 四半期には前年同期比で 3 倍にまで増加した。このような急激な増加は、新型コロナウイルスの世界的蔓延とロックダウン等の影響により、多くの日常的な活動がオンラインに移行したことで、潜在的な攻撃対象が増加したことが原因である可能性が高いという※104。

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

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

(a) リフレクション攻撃

リフレクション攻撃では、外部に公開されている UDP（User Datagram Protocol）※106 を用いて通信を行うサービス（以下、UDP サービス）を悪用した攻撃が多く観測されている※107。UDP サービスを悪用した攻撃では、UDP の以下の三つの特徴が悪用される。

①要求パケットの送信元 IP アドレスを確認しない。このため、送信元を偽装しやすい。
②要求パケットの長さよりも応答パケットの長さが大きくなる増幅効果（Amplification）がある。
③ UDP サービスを提供するサーバ（以下、UDP サーバ）へ行われたリクエストは、応答パケットとして、任意のホストへ反射（Reflection）される。

UDP サービスが DDoS 攻撃に悪用されると、①の特徴により攻撃元の特定が難しく、②③の特徴を悪用することで、送信するデータ量を数十倍から数百倍に増幅させた攻撃が可能となる。また、インターネット上からアクセス可能な UDP サーバへの通信そのものは正常であるため、攻撃が行われていることを把握し対応を行うには、後述の「1.2.4 (3) (b) 攻撃に加担しないための対策」が必要となる。

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

UDP サービスを悪用した攻撃は、新しい手法ではな

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

(b) DDoS攻撃の規模拡大の事例

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

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

(c) 仮想通貨を要求するDDoS攻撃の事例

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

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

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

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

(2) DDoS攻撃を行うボットネットの拡大

DDoS攻撃には、ボットネットと呼ばれる攻撃用ネットワークが使用される場合がある。ボットネットは、攻撃者が乗っ取った多数のコンピュータ、ネットワーク機器、IoT機器等と、それらに対して遠隔で指令を送信するためのC&Cサーバで構成されている。攻撃者がC&Cサーバを介して、ボットネットに攻撃指令を送信することで、ボットネットを構成する機器が一斉に攻撃を行う。ボットネットを構成する機器のほとんどは、サービスやソフトウェアの脆弱性を悪用されたりウイルスに感染させられたりした結果、制御を奪われた一般の機器である。

ボットネットは、より多くの機器を乗っ取るため、アップデートを繰り返すことで、最新の悪用手法等を取り入れ、様々なターゲットに対して攻撃を繰り返しながらボットネットを拡大させ、大規模なDDoS攻撃等を実行する。

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

このようなボットネットは、攻撃ツールとして、DDoS代行サービスを通じて有償で貸し出されることがある。拡大したボットネットがDDoS代行サービスに使用されることが、大規模なDDoS攻撃が発生しやすくなる要因となっている。

(3) DDoS攻撃への対策

DDoS攻撃への対策では、DDoS攻撃の被害に遭っ

た場合の対策に加えて、管理または所有するコンピュータ、ネットワーク機器、IoT 機器等が乗っ取られ、DDoS 攻撃に加担することを防ぐための対策も求められる。以下ではこれらの対策について解説する。

(a) DDoS 攻撃の被害に遭った場合の対策

DDoS 攻撃によって送られてくる通信データを遮断し、サービスを提供するサーバやネットワークのリソースを保護する対策が必要である。正常なアクセスと DDoS 攻撃によるアクセスを、どのように切り分けるかが対策のポイントとなる。以下に、具体的な対処方法を挙げる。

- アクセスログや通信ログ等を確認し、攻撃が特定の IP アドレスから行われていると判断できる場合は、当該 IP アドレスからのアクセスを遮断する。
- 国内からのアクセスを主に想定しているサイトでは、海外の IP アドレスからのアクセスを一時的に遮断することを検討する。
- 攻撃者が攻撃元の IP アドレスや攻撃方法を定期的に変更してくる場合があるため、継続して監視を行い、攻撃方法に合わせた対策を実施する。
- 組織内で対処しきれない程、大規模な攻撃や執拗な攻撃を受けている場合は、ISP 事業者との連携や警察等への通報を実施する。
- 攻撃の頻度や、攻撃対象サイトの重要性によっては、ISP 事業者が提供する DDoS 攻撃対策サービスやセキュリティベンダ等が提供する DDoS 攻撃対策製品の利用を検討する。

(b) 攻撃に加担しないための対策

自組織や個人で使用する機器が DDoS 攻撃に悪用されないように、セキュリティソフトを導入したり、適切な設定をしたりといった対策が必要である。また企業においては、自組織の機器を悪用された場合に、それを早期に検知できるように通信の監視を行うといった対策も推奨する。以下に、具体的な対処方法を挙げる。

- OS やファームウェアを最新の状態に保ち、ウイルス感染や脆弱性の悪用により制御を奪われることを防ぐ。
- パスワードが初期設定のままの機器が存在しないか確認し、存在した場合は適切なパスワードを設定する。
  パスワードが初期設定のままの機器は、攻撃者により容易に侵入され、制御を奪われてしまう可能性がある。
- 外部と接続されているネットワーク機器や IoT 機器をとおして組織内の他の機器に対して感染拡大を試みるウイルスも確認されているため、インターネットに直接つながっていない機器においても対策を行う。
- 組織内で稼働しているサービスを洗い出し、DDoS 攻撃に悪用される可能性があるサービスが適切に運用されていることを確認する。
  具体的には、これらのサービスが稼働するサーバに関して、OS を始め、各サービスが脆弱性を含むバージョンで稼働していないことや、DDoS 攻撃に悪用される設定になっていないことを確認する。
  また、それらのサービスを組織内のみで利用している場合でも、意図せずインターネット上に公開していないかを確認する。
- 組織内の機器の外向きの通信を監視し、異常な通信を確認した場合は、攻撃の踏み台となっている可能性がある。そういった機器は、ウイルス感染等が生じていないか調査し、対処を行う。自組織での対処が困難な場合は関係当局やセキュリティベンダ等への相談を検討する。

1.2.5 ソフトウェアの脆弱性を悪用した攻撃

2020 年度は、VPN 製品の脆弱性を狙った攻撃が多く報告された。また、多くの利用者がいる Windows や、多数の IoT 製品に影響があるとされる脆弱性も報告された。

本項では、これらの脆弱性を悪用した攻撃の状況と対策について解説する。

(1) VPN 製品の脆弱性を対象とした攻撃

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

2020 年度は、新型コロナウイルス感染拡大防止のためテレワークが強く推奨された影響から、VPN の利用に注目が集まった。その一方で、VPN 製品に脆弱性が相次いで発見され、脆弱性が解消されていない製品を狙った攻撃も多数報告された。

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

(a) 攻撃事例

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

(CVE-2018-13379※118)が発見された。

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

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

また、2019 年に Pulse Secure, LLC. は、同社の VPN 製品である Pulse Connect Secure に発見された複数の脆弱性を解消したバージョンのソフトウェア配布を開始した※120。解消された脆弱性のうち、悪用による被害が確認された CVE-2019-11510 及び CVE-2019-11539 の概要※121 は以下のとおりである。

- CVE-2019-11510 の脆弱性
  この脆弱性を悪用されると、認証されていない攻撃者により、細工した URI(Uniform Resource Identifier)と、パス・トラバーサルを狙った文字列を組み合わせたリクエストを送信され、当該製品上の任意のファイルにアクセスされる可能性がある。また、ユーザの認証情報を不正に取得され、正当なユーザになりすましてログインされる可能性がある。
- CVE-2019-11539 の脆弱性
  この脆弱性を悪用されると、当該製品において認証に成功した攻撃者により、Web GUI を介して、当該製品上で任意のコマンドが実行される可能性がある。

これらの VPN 製品は、脆弱性を解消したバージョンのソフトウェアプログラムが配布されたのは 2019 年だが、1 年が経過した 2020 年度においても、当該脆弱性を悪用した攻撃の被害が報告されている。

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

(b) 脆弱性を狙った攻撃への対策

脆弱性が発見されると攻撃者に狙われ、被害が発生してしまう可能性があるため、新たな脆弱性が公開された際は、迅速な対応が求められる。

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

対策の実施手順として、以下に示す内容をあらかじめ定めておくことを推奨する。

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

また、このような実施手順の準備に加え、侵害されている痕跡が存在するかの確認や攻撃を受けてしまった場合に実施する対応を定めておくことを推奨する。

(2) Microsoft 製品の脆弱性を対象とした攻撃

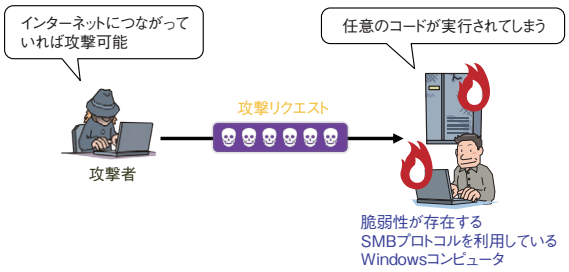
2020 年度も 2019 年度に引き続き、Microsoft 製品の脆弱性を狙った攻撃が多数報告されている。本項では、Microsoft SMB (Microsoft Server Message Block)の脆弱性を狙った事例を紹介する。

(a) 攻撃事例

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

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

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



■図 1-2-9　SMBGhost の脆弱性を悪用した攻撃イメージ

実行される可能性がある。

- SMBleed の脆弱性

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

(b) 脆弱性を狙った攻撃への対策

脆弱性を狙った攻撃による被害を防ぐため、修正プログラムが公開されたら、利用者は速やかにアップデートを実施することが求められる。また、事前に対策の実施手順を整えておくことを推奨する(「1.2.5 (1) (b) 脆弱性を狙った攻撃への対策」を参照)。

(3) IoT 製品を対象とした攻撃

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

(a) 多数の IoT 製品に影響する脆弱性

2020 年 6 月 16 日、イスラエルのサイバーセキュリティ企業である JSOF Ltd. より、「Ripple20」と呼ばれるゼロデイ※125 の脆弱性群に関する情報が公開された※126。

Ripple20 は、米国の Treck Inc. 製の組み込み機器用通信ソフトウェアに発見された 19 個の脆弱性の総称であり、これらの脆弱性が悪用された場合、攻撃者により、外部からネットワークに侵入され、ブロードキャストによって、ネットワーク内の脆弱性のあるすべての IoT 製品の乗っ取りや、情報窃取、製品の誤作動等の被害を一斉に引き起こされる可能性があるという。

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

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

(b) IoT 製品を対象とした攻撃への対策

前述の Ripple20 のような脆弱性の存在を踏まえて、IoT 製品を安全に保つためには、以下の対策が必要となる。

- 製品開発者が行うべき対策
  - IPA や JPCERT/CC 等の各組織が公開している IoT 製品の開発ガイドライン等を基に、企画・設計等を含めたすべての開発工程で実施すべきセキュリティ対策を明確にする (ガイドラインについては「3.2.4 (1) IoT 関連セキュリティガイド等の改訂・新規発行」参照)。
  - 製品で使用する部品の調達に関し、契約等において脆弱性対処の項目を含める。
  - 製品出荷後に修正プログラムによりアップデートが実施できるように製品に更新機能等を組み込む。
  - 製品に関する脆弱性が発見・報告された場合、速やかに修正プログラムを公開する。
  - 安全に運用するための注意点等の情報を製品利用者に提供する。
- 製品利用者が行うべき対策
  - 製品開発者が提供する安全に運用するための注意点やアップデート方法等の情報を確認した上で利用する。
  - 攻撃者に脆弱性を悪用されるリスクを低減するため、製品を利用するにあたって問題がなければ、インターネットから直接 IoT 製品にアクセスできないようにする。
  - 脆弱性情報を収集する。具体的には、IPA が公開している「JVN iPedia※127」や、IPA から送付されるセキュリティ対策情報のメールニュース、製品開発者の Web サイトで公開される情報等を定期的に確認する。
  - 製品開発者が修正プログラムを公開した場合、速やかに修正プログラムを適用する。

1.2.6 ばらまき型メールによる攻撃

特定の組織や個人ではなく、不特定多数の一般利用者を狙った、ウイルス感染を目的としたメールを本項では「ばらまき型メール」と呼ぶ。

2015 年 10 月ごろより、国内で日本語のばらまき型メールが多く観測されるようになった※128。ばらまき型メールには様々なバリエーションがあり、件名やメール本文が受信者とは関係のないメール、実在の組織をかたったメール、一見すると業務に関係のありそうな件名や本文のメール、「正規のメールへの返信」を装ったメール等が存在する。また、ばらまき型メールでウイルスに感染させる手口として、添付ファイルやメール本文中の URL を用いる手法が存在する。メールの添付ファイルには実行ファイルやマクロ付きの Word、Excel、PowerPoint ファイル、そしてこれらのファイルを圧縮した形式のファイル等が確認されている。

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

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

(1) ばらまき型メールによって感染するウイルス

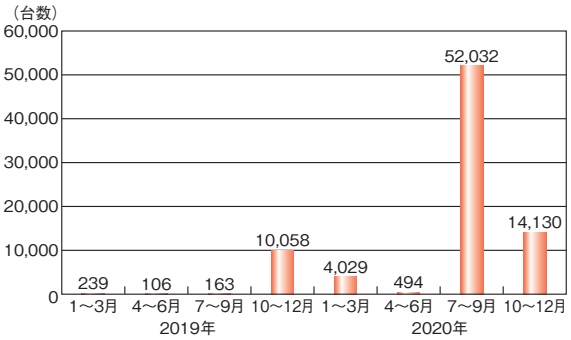
ばらまき型メールによって感染するウイルスは様々なものが存在し、個々のウイルスによって動作は異なる。2020 年度に観測された、ばらまき型メールによって感染するウイルスの一部について述べる。

(a) Emotet

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

Emotet は次の機能を持ち得るとされている※132。

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



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

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

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

(b) IcedID

IcedID は感染した端末のインターネットバンキングの

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

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

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

(c) Zloader

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

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

(d) 遠隔操作ウイルス（RAT）

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

(2) ばらまき型メールの偽装の手口

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

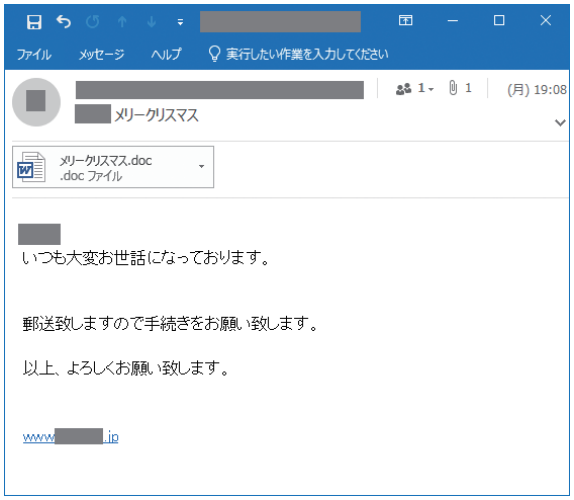
(a) 正規のメールへの返信、転送、及び再送を装う手口

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

このような手口のばらまき型メールは 2018 年 11 月から観測されている※142。Emotet のばらまき型メールでは、Emotet に感染した端末から窃取した情報を基に、Emotet に感染した端末で構成されるメール送信用のボットネットから、別の相手に対して正規のメールへの返信等を装うメールをばらまくことが確認されている※143。一方 IcedID のばらまき型メールでは、攻撃者がメールアカウントへ不正アクセスし、そのメールアカウントで受信していた正規のメールへの返信等を装ったり、既に窃取したメール情報を用いて正規のメールへの返信等を装うばらまき型メールを確認している。

(b) メール受信者の興味・関心を惹く題材を悪用する手口

2019 年 12 月には賞与を題材とした Emotet のばらまき型メールを、2020 年 1 月には新型コロナウイルスを題材とした Emotet のばらまき型メールを観測していた。その後、図 1-2-11 のように 2020 年 12 月にはクリスマスや賞与の支給を題材にした Emotet のばらまき型メールを観測した※130。また、2021 年 1 月には緊急事態宣言を題材にした Emotet のばらまき型メールを観測している。これらの手口から、攻撃者は日本国内のメール受信者の興味・関心を惹く題材を選んで継続的に攻撃を行って

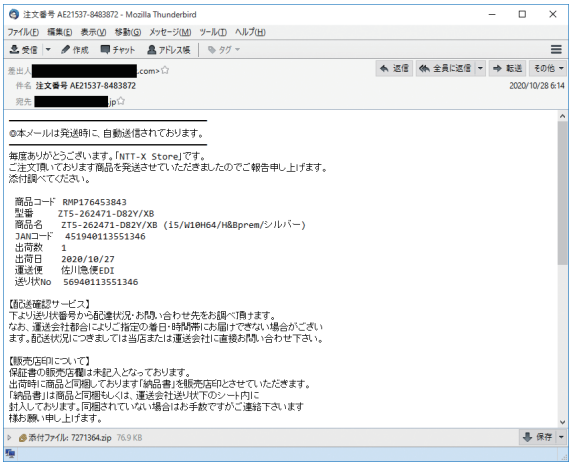


■図 1-2-11 「メリークリスマス」という Emotet のばらまき型メールの例（2020 年 12 月）
（出典）IPA「『Emotet』と呼ばれるウイルスへの感染を狙うメールについて※130」

いるといえる。

(c) 実在の組織をかたった手口

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



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

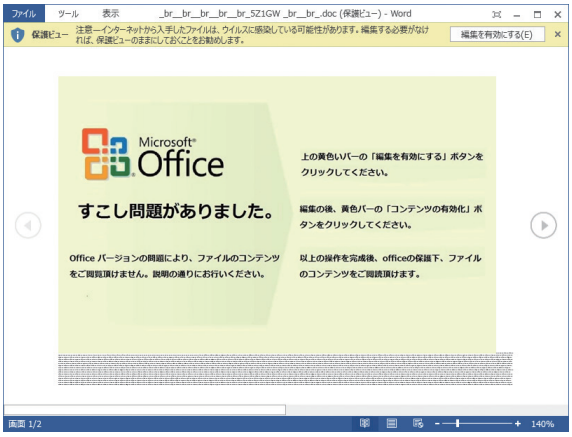
(3) ウイルスに感染させる手口

攻撃者がばらまき型メールを用いてウイルスに感染させる手口を解説する。

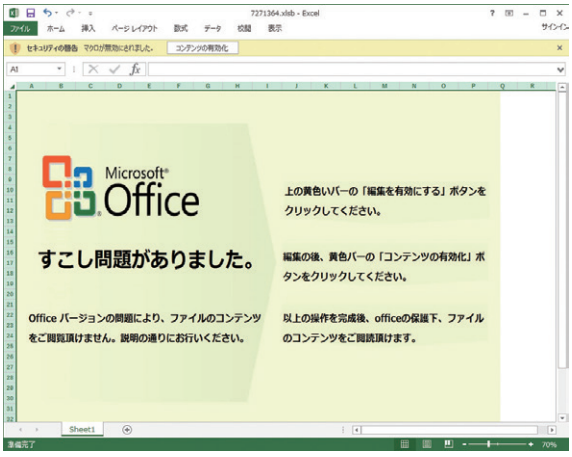
(a) マクロ付きの Office 文書ファイルを使用する手口

この手口では、マクロ付きの Word、Excel、PowerPoint ファイル内の悪意あるマクロが動作することでウイルスをダウンロードし感染させる。マクロ付き Word、Excel ファイルには、Microsoft や Office 等のロゴとともに、「文書ファイルを閲覧するには操作が必要である」という趣旨の記述と「Enable Editing」ボタンと「Enable Content」ボタンのクリックを促す指示が書かれているものがあることを確認している。2020 年 9 月まではこれらの記述は英語で書かれているもののみであったが、IPA では 2020 年 10 月に、図 1-2-13 や図 1-2-14 のように、日本語で指示が記載された Word ファイルや Excel ファイルを観測している。

マクロ付きの PowerPoint ファイルの場合、ファイルを



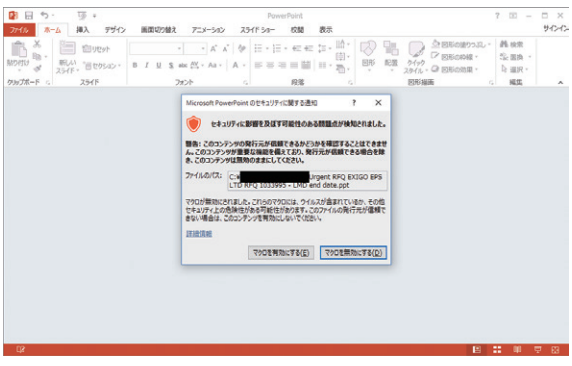
■図 1-2-13　日本語で記載されている Emotet への感染を狙う Word ファイルの例



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

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

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



■図 1-2-15　マクロ有効化を促す PowerPoint ファイルの例

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

(b) パスワード付きの ZIP ファイルを使用する手口

パスワード付きの ZIP ファイルがメールに添付され、そのパスワードがメール本文に記載されている Emotet のばらまき型メールと IcedID のばらまき型メールを確認している。ZIP ファイルを解凍すると、マクロ付きの Word ファイルが出力され、利用者がそのファイルを開いて「コンテンツの有効化」ボタンをクリックすることでウイルスに感染させられる。この手口自体は 2019 年 12 月に Ursnif のばらまき型メールで用いられていた。添付ファイルが暗号化されていることから、メール配送上でのセキュリティ製品や、セキュリティサービス、セキュリティソフトによる検知や検疫をすり抜け、受信者のもとに攻撃メールが届いてしまう確率が高い。また複数のばらまき型メールでこの手口が使われるようになっている。今後も攻撃者はこの手口を用いる可能性があるため、引き続き注意が必要である。

(c) メール本文中の URL リンクを使用する手口

この手口ではメール本文中に URL リンク先が記載され、URL リンクにアクセスすると悪意のあるマクロ付き Office 文書ファイル等をダウンロードさせ、前述の「(a) マクロ付きの Office 文書ファイルを使用する手口」を用いてウイルスに感染させる。URL リンク先は攻撃者が用意したサーバである場合や、Microsoft OneDrive、Google Drive 等のクラウドストレージの場合もある。この手口は新しいものではないが 2020 年度においても継続して用いられており、引き続き注意が必要である。

(4) ばらまき型メールへの対策

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

(a) 一般利用者における対策

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

- セキュリティソフトを導入する
  メール受信者がウイルスメールであると判断できずに添付ファイル等を開いてしまったとしても、セキュリティソフトが検知・検疫し、被害を免れる可能性がある。セキュリティソフトは導入するだけでなく、常に最新の状態に保つことも重要である。
- 不用意にメールや添付ファイル内の指示に従わない
  身に覚えのないメールの添付ファイルを開かないことや、本文中の URL リンクにアクセスしないことが重要である。また、受信したメールに疑問や不信感を抱いた場合は、送信元となっている企業や組織の公式サイトでばらまき型メールに関する注意喚起が公開されていないかを確認するほか、当該メールの送付有無を問い合わせる。受信メールの真偽が分からない段階では、メールへの返信、添付ファイルを開くこと、及び本文中に記載されている URL へのアクセスは避けるべきである。また、添付ファイルを開いたときに、警告ウィンドウが表示された場合、その警告の意味が分からないのであれば、操作を中断し、システム管理部門等へ報告を行う。
- OS やソフトウェアのバージョンを常に最新に保つ
  適宜、修正プログラムを適用し、既知の脆弱性を解消しておくことで、脆弱性を悪用した攻撃が成功する確率を下げる。
- Word、Excel、PowerPoint ファイルを開いたときにマクロを有効化しない
  正規のものであると確信の持てない Word、Excel、PowerPoint ファイルを何らかの方法で入手して開いたときに、マクロやセキュリティに関する警告が表示された場合は、不用意に「コンテンツの有効化」ボタンをクリックしないようにする。また、Word、Excel、PowerPoint の設定でマクロの自動実行を無効化する。業務等でマクロを使わないと分かっている場合にはマクロ機能自体を無効化する。

(b) 企業・組織における対策

企業・組織におけるばらまき型メールに対する対策は、「1.2.1 (5) 標的型攻撃への対策」で述べている内容と基本的には同じである。不審なメールを受信した際の報告窓口を設けることや、ウイルス感染を想定した利用者の訓練と教育を行うこと、システムでの対策として、不審なメールを解析するために確保できる仕組みの確立や適切な修正プログラムの適用、特定のファイル形式について実行許可・禁止の設定を行う、といった対策が重要である。

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

1.2.7 個人をターゲットにした騙しの手口

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

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

(1) 新たに出現したアプリやSNSへスパムを送り込む手口

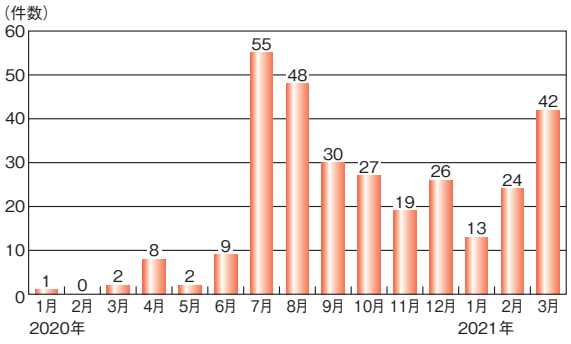
メールやWebだけでなく、アプリやSNSを悪用する新しい騙しの手口が登場した。

(a) iPhoneカレンダースパム

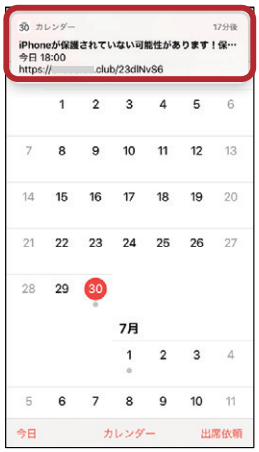
2020年1月から3月にかけて、「iPhoneのカレンダーから、ウイルス感染しているという通知が出る」「iPhoneのカレンダーに、身に覚えのないイベントが入っている」といったiPhoneのカレンダーアプリに関する相談が複数件寄せられたため、IPAは3月に「安心相談窓口だより」で注意喚起を実施した。しかし、この「iPhoneカレンダースパム」に関する相談が7月に急増した(図1-2-16)ことから、8月には注意喚起に新たに観測された手口の説明を追加し、10月には対処方法の更新を行った。また、2021年2月には、手口を検証する動画を追加した[※148]。

(ア) 手口

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



■図1-2-16 iPhoneカレンダースパムに関する月別相談件数推移



■図1-2-17 iPhone端末にカレンダーが通知された例

■図1-2-18 カレンダーに登録されたイベントとURLの例

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

①アカウント追加型:攻撃者の仕掛けたワナにはまる

②イベント・カレンダー共有型:攻撃者から一方的に送り付けられる

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

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

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

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

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

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

(イ) 対処

対処は、カレンダーがどのように入ったかによって異なる。

①アカウント追加型への対処

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

■図 1-2-21　カレンダーの削除方法（iOS 14 の場合）

②イベント・カレンダー共有型への対処

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

■図 1-2-22　カレンダーのスパム報告手順

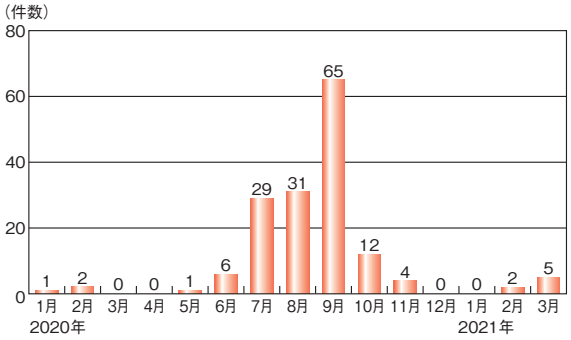
■図 1-2-23　共有カレンダーの削除手順

■図 1-2-24　共有イベントのスパム報告手順

「削除してスパムを報告」の操作を行う（図 1-2-24）。

(b) Facebook メッセンジャースパム

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



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

(ア) 手口

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

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

■図 1-2-26　動画を装ったスパムメッセージの例

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

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

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

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

なお、アプリのインストールへの誘導は、Facebook メッセンジャースパムの手口に限定されるものではなく、Web サイト閲覧中に「ウイルスに感染している」等の根拠のない警告画面を表示して騙す手口にも使われている（詳細は「1.2.7 (4) (b) アプリ誘導」参照）。

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

なお、Facebook の ID とパスワードを入力させる偽サ

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

イトに誘導されなかったという相談もあり、詳細については、不明な点がある。

(イ) 対処

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

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

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

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

(c) 公式アカウントを装った SNS の偽アカウント

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

(ア) 手口

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

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

(イ) 対処

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

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

(2) 世の中の関心に乗じるメールの手口

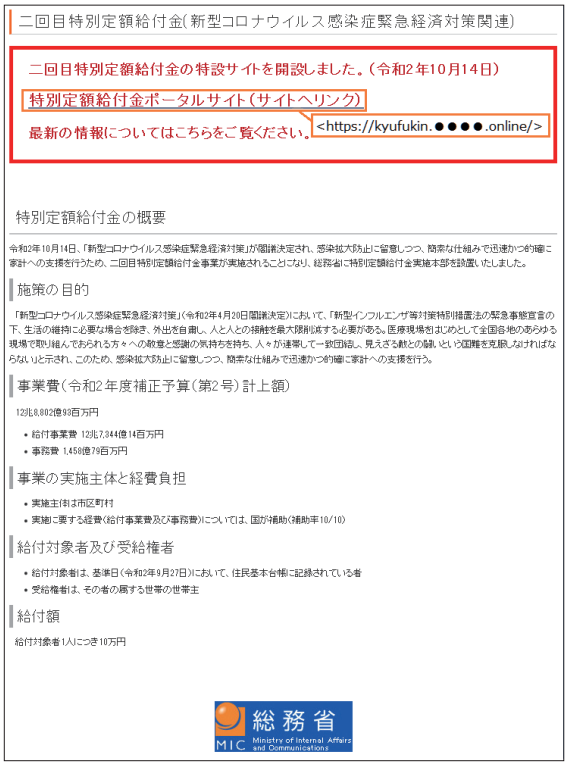
新型コロナウイルスの感染拡大に伴い、経済や社会に様々な影響が出ているが、新型コロナウイルスに関連した話題が、メールや SMS、偽サイトによるカード情報等の窃取へ誘導する騙しの手口に使われた。

(ア) 手口

2020 年度は「新型コロナウイルス感染症緊急経済対策」として家計支援のため、1 人あたり 10 万円が支給された「特別定額給付金」に関するものが多かった。特別定額給付金が 5 月より支給されたため、支給前の 4 月ごろから、特別定額給付金の手続きをかたるメールが送信されるようになった。10 月には、2 回目の特別定額給付金をかたったメールが送られたことが、フィッシング対策協議会から報告されている（次ページ図 1-2-29）。メール内のリンクをクリックすると、総務省の特別定額給付金のオンライン申請を装ったフィッシングサイトに誘導される。

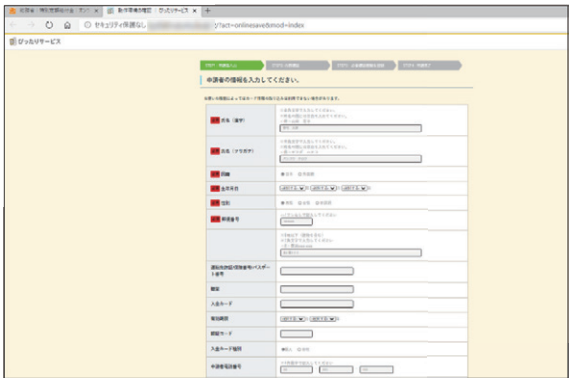
IPA では 10 月に特別定額給付金の偽サイト（次ページ図 1-2-30）を確認した。同サイトのオンライン申請という箇所をクリックすると、住所、氏名、カード情報等の個人情報を入力する画面に誘導される（次ページ図 1-2-31）。

また 2021 年 2 月以降、新型コロナウイルスのワクチン



■図 1-2-29　特別定額給付金の支給をかたるメール
(出典)フィッシング対策協議会「特別定額給付金に関する通知を装うフィッシング (2020/10/15)※154」

■図 1-2-30　特別定額給付金の偽サイト



■図 1-2-31　特別定額給付金の偽サイトの申請者情報入力画面

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

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

(イ)対処

総務省は、特別定額給付金について、政府からメール等で知らせることはないと説明している※156。また、新型コロナワクチン接種に関しては、「行政機関等をかたった " なりすまし " にご注意※157」という注意喚起が関係府省庁の連名で出され、電話・メールで個人情報を求めることはない、と説明している。

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

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

サイトについては、見た目だけでは本物のサイトか偽のサイトかは、判断できにくくなっているため、サイトのリンク以外の方法で運営者に確認するほか、フィッシング詐欺事例等がないかをインターネットで検索したりする等の対処を行う。

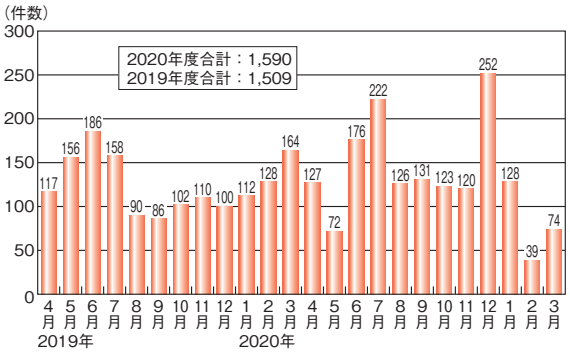
(3) 変化や拡大が続く SMS の手口

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

(a) 宅配便の不在通知を装う SMS

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

2020 年度、IPA の安心相談窓口には、前年度を上



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

回る 1,590 件の相談が寄せられた（図 1-2-32）。

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

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

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

(ア) 手口

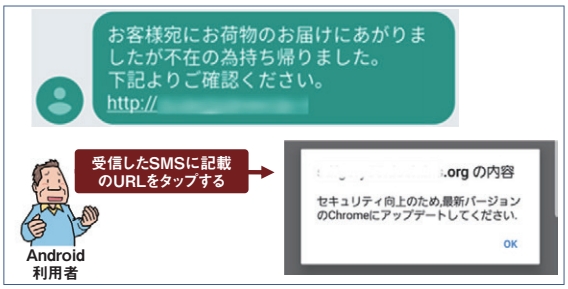
この手口は、「お客様宛にお荷物のお届けにあがりましたが不在の為持ち帰りました。」という宅配便の不在通知を装った SMS を送り付け、SMS 内のリンクから偽サイトへ誘導する。なお、リンクをタップした後の手口は変化を続けており、現時点（2021 年 3 月）の確認内容を説明する。

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

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

① Android の手口詳細

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



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

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

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

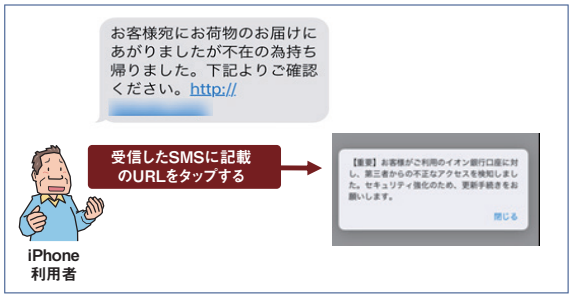
■図 1-2-34　不正なアプリのインストールに至る操作（Andoroid バージョン 10 の場合）

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

させるように誘導される。

② iPhone の手口詳細

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



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

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

（イ）被害

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

①Android における被害

Android における不正アプリの被害として、以下が確認されている。

- スマートフォンが攻撃の踏み台にされ、不特定多数の宛先（自身のアドレス帳にはない電話番号）へ、偽 SMS を勝手に送信される。
- スマートフォンから、アドレス帳の内容、SMS メッセージ等を窃取され、以下のように悪用される。
  - 携帯通信会社が提供するキャリア決済サービスにおいて、身に覚えのない請求が発生する。
  - フリーマーケットサービス、後払い決済サービス、その他のアカウントサービス等のアカウントを勝手に作成され、不正使用される。
- 不正なアプリをインストールした後、銀行を装った偽のセキュリティ警告のポップアップが表示され、タップするとフィッシングサイトに誘導される。

②iPhone における被害

iPhone におけるフィッシングの被害として、以下が確認されている。

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

（ウ）対処

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

（b）ネット通販会社を装う SMS

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

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

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

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

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

■図 1-2-38　Amazon を装う SMS の手口

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

(c) 金融機関を装う SMS

金融機関を装う手口は、メールによるものが多いが、2019 年 9 月に不正送金被害が急増し、メールの手口に加えて SMS が使用されるようになってきた。2020 年も引き続き金融機関を装う SMS が多数確認されている※163。一般財団法人日本サイバー犯罪対策センター（JC3：Japan Cybercrime Control Center）からの注意喚起も 2020 年 6 月と 8 月に更新されている※164。

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

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

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

(d) SMS の手口の変化、拡大への対策

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

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

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

通信会社や金融機関は、SMS を送信する場合の電話番号やアドレス、内容について公式サイトで説明を行っている。また、SMS での情報通知は行っていないとしている事業者も多い。公式サイト等の確かな情報源を使って確認していただきたい。特に SMS に記載されている URL には注意が必要である。また、送信元情報は偽装される場合もある。

相談の中では、荷物が到着する予定があったため、偽宅配事業者の SMS の URL をタップしてしまったという話が多く聞かれた。SMS を安全に利用するためには、受信しても、即座に反応せず、真偽の判断を行っていただきたい。

(4) 被害が続く Web ブラウザによる手口

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

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

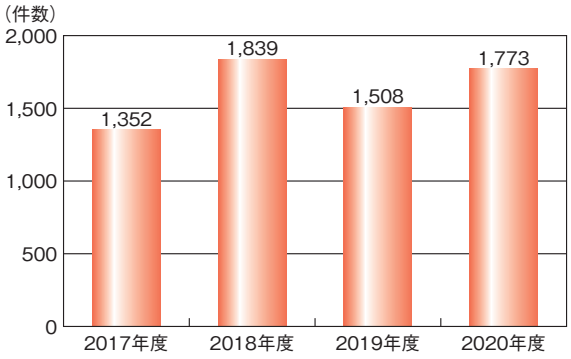
(a) 偽のセキュリティ警告

主にパソコンで Web サイト閲覧中に、突然警告音とともに、「ウイルスに感染している」等の警告画面が表示されたことをきっかけに、画面に表示された電話番号に電話をしてしまい、遠隔操作に誘導され被害に遭ってしまったという相談が 2020 年度も続いている。

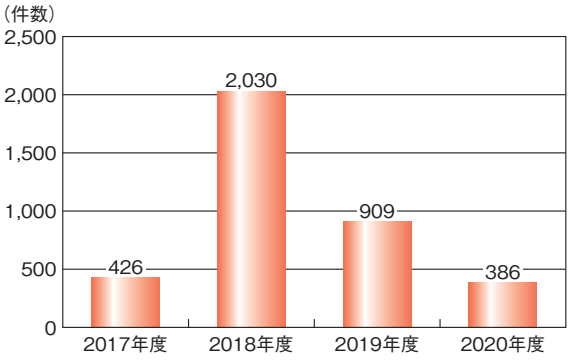
警告画面を出す手口に変化は少ないが、コンビニエンスストアで購入するプリペイドカードで支払わせる手口が増え、コンビニエンスストアの店員が説得して購入を思いとどまらせたというニュースが報道されるようになった。

2020 年度に IPA の安心相談窓口に寄せられた相談件数は、有償サポート契約に誘導される「偽警告」（別

名、サポート詐欺）が 1,773 件（図 1-2-39）、有償ソフトウェアの購入に誘導される「偽セキュリティソフト」が 386 件だった（図 1-2-40）。



■図 1-2-39　偽警告に関する年度別相談件数



■図 1-2-40　偽セキュリティソフトに関する年度別相談件数

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

（ア）手口

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

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

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

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

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

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

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

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

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

■図 1-2-41　遠隔操作に誘導する偽セキュリティ警告の手口

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

(イ)対処

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

パソコンの画面については、Web ブラウザを閉じるだけで問題はない。しかし、通常の操作で画面を閉じることができない場合もあるので、Windows であれば、タスクマネージャーから Web ブラウザを終了する、Mac であれば、「強制終了」ウィンドウから Web ブラウザを終了する、という方法で対処できる。また、どちらの OS の場合も、パソコンを再起動することでも対処できる。

パソコンに遠隔操作ソフトをインストールしてしまった場合は、アンインストールする。

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

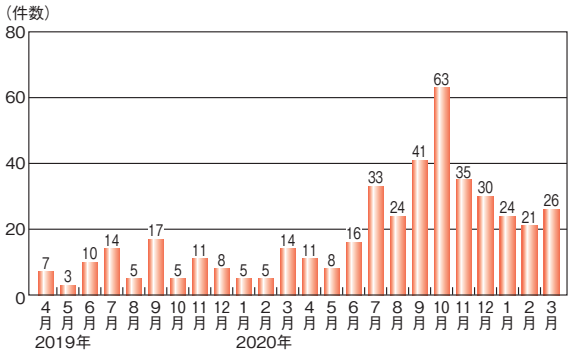
契約については、消費生活センター等※170 に相談し、クレジットカードで支払いを行った場合はクレジットカード会社にも連絡する必要がある。プリペイドカードで支払った場合は返金が困難な場合が多い。

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

(b)アプリ誘導

主にスマートフォンで、Web サイト閲覧中に「ウイルスに感染している」等の根拠のない警告画面を表示して騙す手口の相談が増えている。手口の変化は少なく、インターネット閲覧中に偽の警告から誘導される事例が多いが、「1.2.7 (1) 新たに出現したアプリや SNS へスパムを送り込む手口」で説明した iPhone カレンダースパムや Facebook メッセンジャースパムの手口で誘導される事例も増えている。

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



■図 1-2-42　アプリ誘導に関する相談件数

(ア)手口

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

■図 1-2-43　偽のセキュリティ警告から公式ストアのアプリへ誘導する流れの例(iPhone)

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

上記のケースでは、アプリインストール後の初回起動時に自動継続課金の確認メッセージが表示される（次ページ図 1-2-44）が、無料アプリだと誤解して承認してしまうと、無料期間は 3 日間から 1 週間程度であることが多く、無料試用期間の終了後に意図しない利用料金が発生することになる。

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

（イ）対処

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

アプリをインストールしてしまった場合は、不要であればアンインストールをする。アンインストールだけでは自動継続課金は解約されないので、自動継続課金の登録を取り消す必要がある。iPhone の場合はサブスクリプションの解約（図 1-2-45）、Android の場合は定期購入の解約も実施する。

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

（5）新たな騙しの手口への対策

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

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

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

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

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

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

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

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

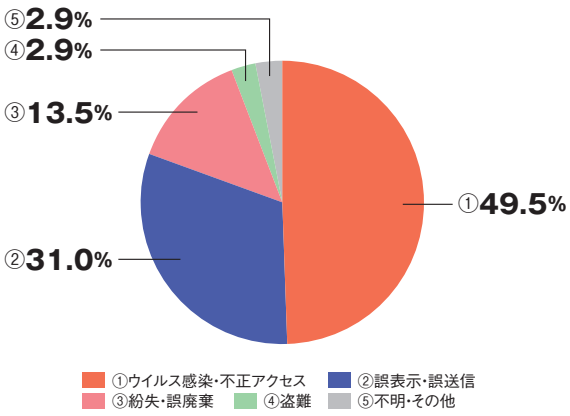
1.2.8　情報漏えいによる被害

2020 年度も、多数の情報漏えい被害が発生している。本項では、外部からの不正アクセス、操作ミス等の過失、内部者の故意による持ち出し、不適切な情報の取り扱い等を主な要因とする情報漏えい被害について述べる。

（1）2020 年の情報漏えいの概況

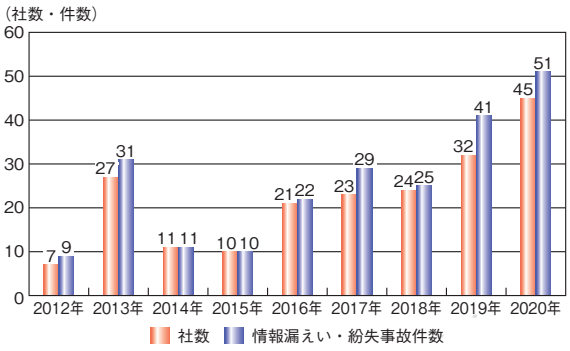
2021 年 1 月に株式会社東京商工リサーチ（以下、東京商工リサーチ社）が公開した「『上場企業の個人情報漏えい・紛失事故』調査（2020 年）[※173]」によると、2020 年に個人情報の漏えい・紛失事故を公表した上場企業は 88 社 103 件（2019 年は 66 社 86 件）、漏えいした個人情報は 2,515 万 47 人分（2019 年は 903 万 1,734 人分）に達した。東京商工リサーチ社が調査を開始した 2012 年以降で最多となった。

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



■図1-2-46 情報漏えい・紛失件数の原因別割合
(出典)東京商工リサーチ社「『上場企業の個人情報漏えい・紛失事故』調査(2020年)」を基にIPAが編集

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



■図1-2-47 ウイルス感染・不正アクセスによる事故の発生推移
(出典)東京商工リサーチ社「『上場企業の個人情報漏えい・紛失事故』調査(2020年)」を基にIPAが編集

(2)不正アクセスによる情報漏えい

不正アクセスの手口は年々巧妙化している。そしてシステムの脆弱性を利用したものや、対策が不十分な委託先、システム等、様々な原因から不正アクセスが発生している。

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

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

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

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

その他、外部からの不正アクセスによって情報漏えい

被害が発生した主な事例を表 1-2-3（次ページ）に示す。

(3) 過失やシステム不具合による情報漏えい・情報紛失

認定個人情報保護団体である一般財団法人日本情報経済社会推進協会（JIPDEC）が 2020 年 11 月に公表した「（2019 年度）『個人情報の取扱いにおける事故報告集計結果』[※191]」によると、事故の発生原因としては「誤送付」が 59.5% と最も多く、次いで「紛失」が 16.6% となっている（「その他漏えい」を除く）。事故原因として 2018 年度から 2019 年度にかけては誤廃棄が 24 件から 66 件と増加した。

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

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

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

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

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

(4) 内部不正による情報漏えい

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

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

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

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

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

(5) 不適切な情報の取り扱い

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

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

(6) 対策

情報漏えいの原因ごとに、被害を発生させないための対策を以下に示す。

(a) 不正アクセスへの対策

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

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

(b) 人為的な過失への対策

情報の取り扱いに人が介在する状況においては、過失による情報漏えい被害を完全に防ぐことは難しい。事故事例に基づく教育等で担当者の意識向上を図ることも有効であるが、それだけでなく、重要な情報の取り扱いルールを設け、その運用を徹底する、適宜見直す等で、過失の発生機会をできる限り削減していく体制づくりが望まれる。うっかりミスを減らすために、ダブルチェック等の対策が取られることも多いが、新型コロナウイルスの感染防止、あるいは省人化・自動化のため、1人で業務することも増えており、業務フローの見直しも含めたリスク低減策が必要である。

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

(c) 内部者の不正への対策

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

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

(d)不適切な取り扱いへの対策

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

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

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

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

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

COLUMN

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

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

表 情報セキュリティ 10 大脅威 2021「個人」・「組織」向け脅威の順位

「個人」向け脅威	順位	「組織」向け脅威
スマホ決済の不正利用	1	ランサムウェアによる被害
フィッシングによる個人情報等の詐取	2	標的型攻撃による機密情報の窃取
ネット上の誹謗・中傷・デマ	3	テレワーク等のニューノーマルな働き方を狙った攻撃
メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	4	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	5	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	6	内部不正による情報漏えい
インターネット上のサービスからの個人情報の窃取	7	予期せぬ IT 基盤の障害に伴う業務停止
偽警告によるインターネット詐欺	8	インターネット上のサービスへの不正ログイン
不正アプリによるスマートフォン利用者への被害	9	不注意による情報漏えい等の被害
インターネット上のサービスへの不正ログイン	10	脆弱性対策情報の公開に伴う悪用増加

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

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

「情報セキュリティ 10 大脅威 2021」解説書や、社内教育や研修に使える「情報セキュリティ 10 大脅威 2021」簡易説明資料／スライド形式、関連する IT 用語を解説した「知っておきたい用語や仕組み」は以下の URL からダウンロードできます。

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

1.3 情報システムの脆弱性の動向

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

1.3.1 JVN iPediaの登録情報から見る脆弱性の傾向

IPAは、脆弱性対策情報データベース「JVN iPedia※127」に、国内外のソフトウェア製品の脆弱性対策情報を収集し、蓄積している。このデータベースに登録されている脆弱性対策情報から、ソフトウェアに関する脆弱性の特徴を統計的に確認することができる。本項では、2020年12月までに登録されたJVN iPediaの脆弱性対策情報の傾向を分析する。

(1) JVN iPediaへの登録状況

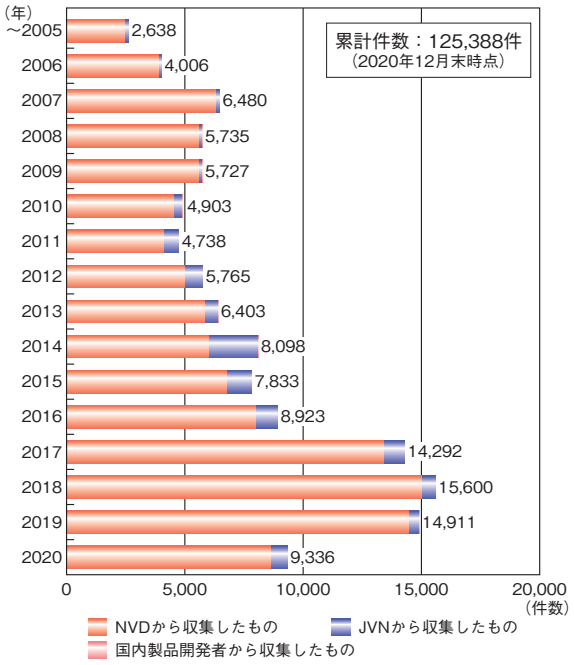
JVN iPediaは、国内外で利用されているソフトウェア製品の脆弱性対策情報を、以下の三つの公開情報から収集・蓄積しており、2007年4月25日から公開している。

- 脆弱性対策情報ポータルサイトJVN※204で公表された脆弱性対策情報
- 国内のソフトウェア開発者が公開した脆弱性対策情報
- 米国国立標準技術研究所（NIST：National Institute of Standards and Technology）の脆弱性データベース「NVD※205」で公開された脆弱性対策情報

(a) JVN iPediaの登録件数の推移

JVN iPediaに登録している情報を、製品ベンダやセキュリティ関連企業が脆弱性情報を公表した年別※206にまとめると、2011年を境にしてNVDから収集した脆弱性対策情報の登録件数がおおむね増加傾向となっている。なお、2020年の登録件数は12月末時点で9,336件であるが、脆弱性対策情報の公開からJVN iPediaへの登録までタイムラグがあるため、2020年の登録数も最終的には2019年と同程度になる見込みである（図1-3-1）。2017年以降、NVDに公開される脆弱性の件数が増加した理由としては、脆弱性を登録するための共通識別子であるCVE（Common Vulnerabilities and Exposures）※207の採番機関（CNA：CVE Numbering Authority）※208が増加したことが一因として挙げられる。The MITRE Corporation※209によると、2016年12月に47社※210だったCNAは、2020年12月には149社※211と約3倍になっている。この増加したCNAによって、多くの脆弱性にCVEが付与され、NVDに公開される脆弱性の件数増加につながった可能性がある。

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



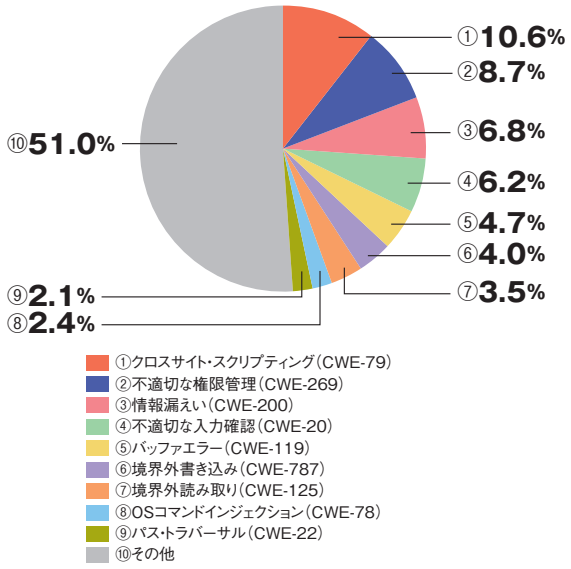
■図1-3-1 JVN iPedia登録状況（公表年別）
（出典）JVN iPediaの登録情報を基にIPAが作成

JVN iPediaは、発見された脆弱性の種類を識別するための共通脆弱性タイプ一覧CWE（Common Weakness Enumeration）※213を脆弱性対策情報に付与して登録を行っている。2020年に登録したCWEの割合は「クロスサイト・スクリプティング」が10.6%と最も高く、「不適切な権限管理」が8.7%、「情報漏えい」が6.8%、「不適切な入力確認」が6.2%と続いている（次ページ図1-3-2）。

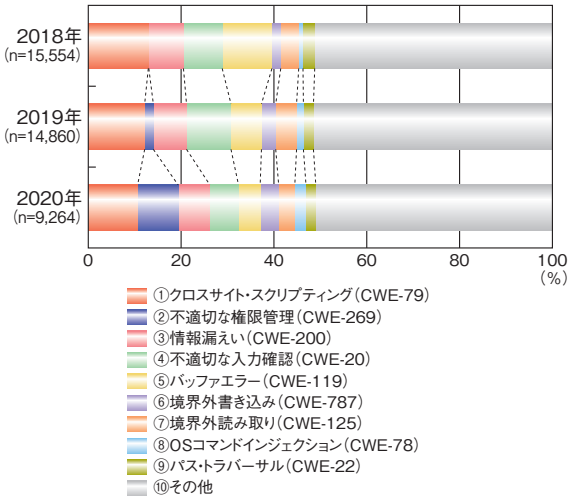
最も件数の多かった「クロスサイト・スクリプティング」に分類される脆弱性を悪用されると、偽のWebページが表示されたり、情報が漏えいしたりする恐れがある。

2018年以降のCWE別割合を年別に見ると、上位5

種では、「クロスサイト・スクリプティング」「情報漏えい」「バッファエラー」の割合は 2019 年以降減少傾向にあり、「不適切な入力確認」の割合も 2020 年に減少している。一方で、「不適切な権限管理」の割合のみ増加傾向である（図 1-3-3）。



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



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

(b) JVN iPedia の登録情報の深刻度

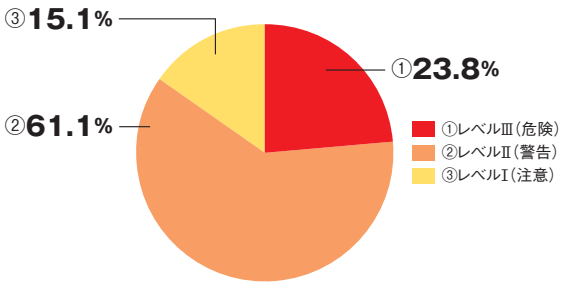
JVN iPedia は、オープンで汎用的な脆弱性評価手法である CVSS（Common Vulnerability Scoring System：共通脆弱性評価システム）※214 を用いて、脆弱性の深刻度を公開している。なお、JVN iPedia では CVSS v2 及び CVSS v3 の二つのバージョンの情報を公開しているが、本項では CVSS v2 を基に統計処理を行っている。

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

深刻度のレベルごとに想定される影響は以下である。

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

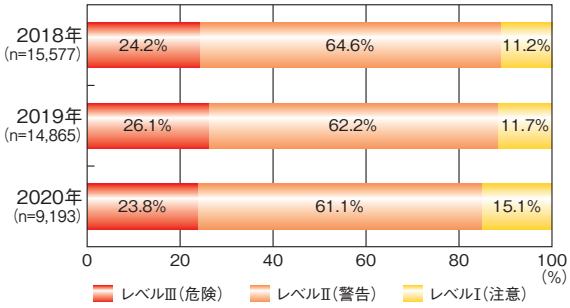
2020 年に登録された脆弱性対策情報を深刻度のレベルで分類すると、レベルⅢが 23.8%、レベルⅡが 61.1%、レベルⅠが 15.1% となっており、一部の情報漏えいやサービス停止につながるレベルⅡ以上の脆弱性が全体の 8 割以上を占めている（図 1-3-4）。



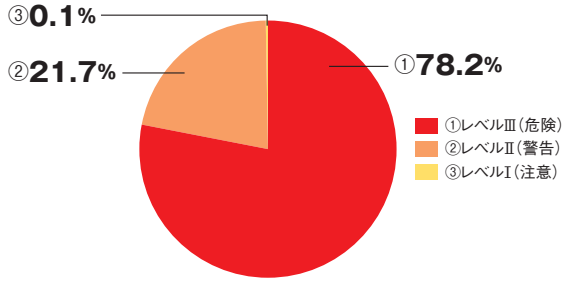
■図 1-3-4　JVN iPedia における脆弱性対策情報のレベル割合（2020 年、n=9,193）
（出典）JVN iPedia の登録情報を基に IPA が作成

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

製品開発者は、ソフトウェアの企画・設計・製造段階



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



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

からセキュアコーディング※215 を含めたセキュリティ対策を講じる等、脆弱性による被害を未然に防ぐための対応が必要となる。また、製品の利用者にも、日頃から新たに公開される脆弱性対策情報に注意を払い、脆弱性が公開された場合には製品を最新バージョンにアップデートする等の対応が求められる。

(2) Microsoft Server 製品の脆弱性について

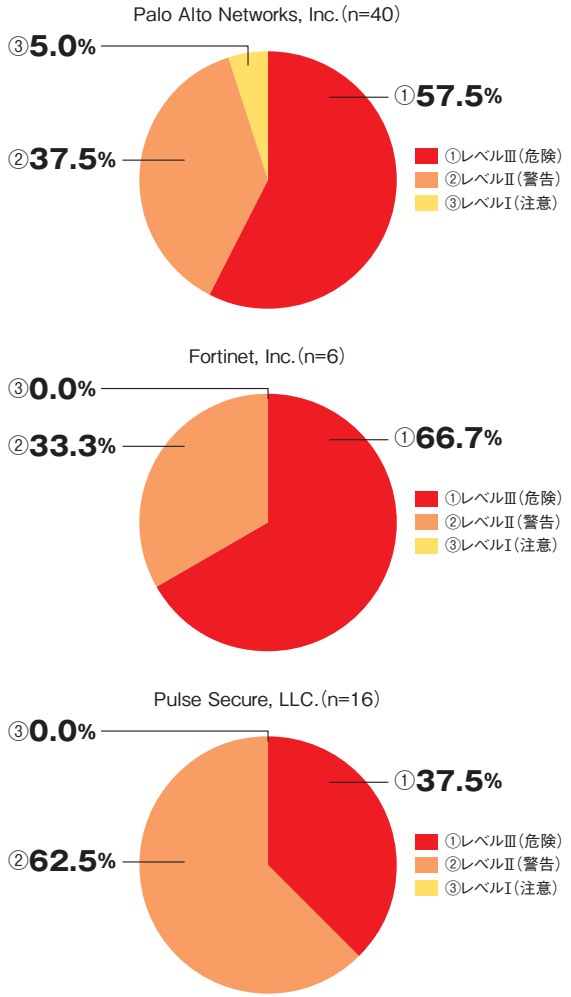
「Zerologon」と呼ばれる脆弱性（CVE-2020-1472）は、Windows Server 製品のドメインコントローラ機能で使われる Netlogon リモートプロトコル（MS-NRPC）に発見された特権昇格の脆弱性である。本脆弱性を悪用され、攻撃者にドメインの管理者権限を奪われてしまうと、組織の重要な機密情報が窃取されたり、ドメインに参加しているパソコンが攻撃者に乗っ取られたりする等の被害につながる恐れがある。本脆弱性は、2020 年 8 月に Microsoft 社から脆弱性対策情報※216 が提供された際、CVSS v3 基本値の深刻度が最も高い 10.0 と評価されており、そ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

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

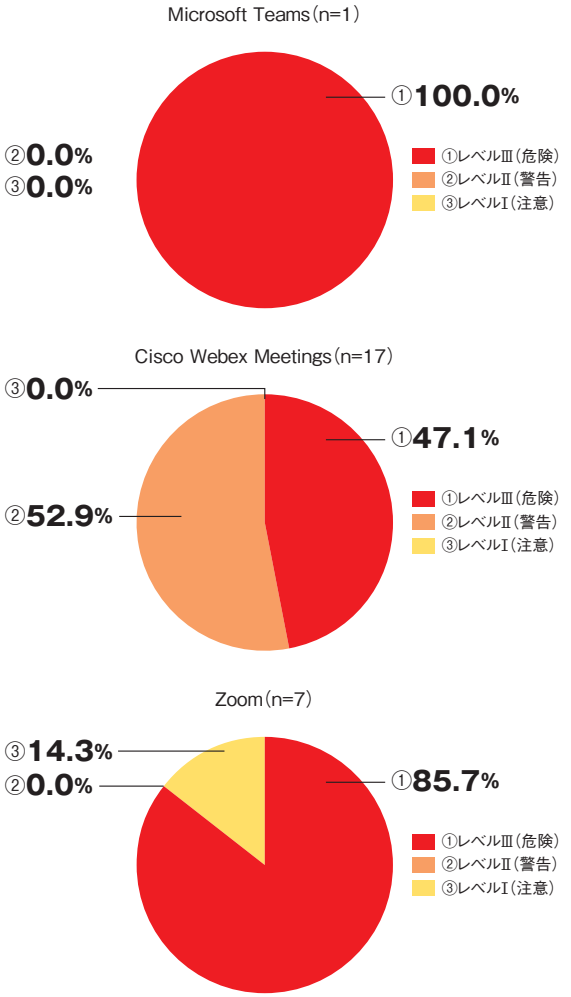
(3) テレワーク等で使われるソフトウェアの脆弱性について

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

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



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



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

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

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

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

(4) 今後の展望

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

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

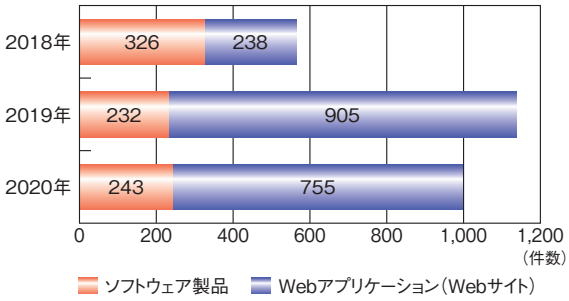
テレワークで使われるソフトウェアの脆弱性の中でも特に VPN 製品の脆弱性は、組織のネットワークの入り口に存在するため、それを悪用されることで組織内部に侵入される恐れがある。その後、ランサムウェア等のウイルスに感染させられた場合、組織は大きな二次被害を受けることになる。被害が脆弱性を有する VPN 製品単体にはとどまらないことを十分理解し、VPN 製品を利用する組織には適切な脆弱性の管理が求められる。なお、VPN 製品の脆弱性を突いた攻撃事例については「1.2.5 (1) VPN 製品の脆弱性を対象とした攻撃」を参照されたい。

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

1.3.2 早期警戒パートナーシップの届出状況から見る脆弱性の動向

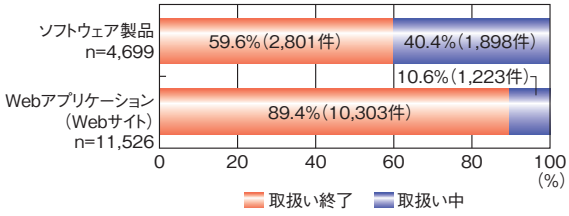
ソフトウェア製品や Web アプリケーション（Web サイト）の脆弱性を悪用した攻撃による情報漏えい、及び Web ページ改ざん等の被害は、2020 年も引き続き発生している。更に、修正プログラムが未適用で攻撃対象となる機器に関する情報が公開されるという事態も起こっている。例えば、脆弱性の影響を受ける VPN 製品のホスト情報が公開されたため、NISC や JPCERT/CC から注意喚起※222 がなされた。

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



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

パートナーシップ開始時点（2004 年 7 月 8 日）からの届出件数を累計すると、ソフトウェア製品は 4,699 件、Web サイトは 1 万 1,526 件となり、2020 年 12 月末時点までの合計が 1 万 6,225 件に上る。これらの届出のうち IPA での取り扱いが終了※224 した届出件数は、ソフトウェア製品 2,801 件（59.6%）、Web サイト 1 万 303 件（89.4%）という状況である（図 1-3-10）。



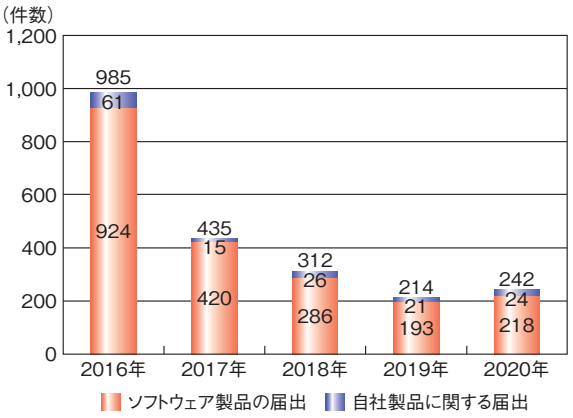
■図 1-3-10　脆弱性関連情報の種類別取扱終了状況
（2020 年末までの累計）
（出典）パートナーシップの届出状況を基に IPA が作成

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

(1) ソフトウェア製品の脆弱性

2020 年にパートナーシップで受け付けたソフトウェア製品の届出（不受理 1 件を除く）は、242 件であった。

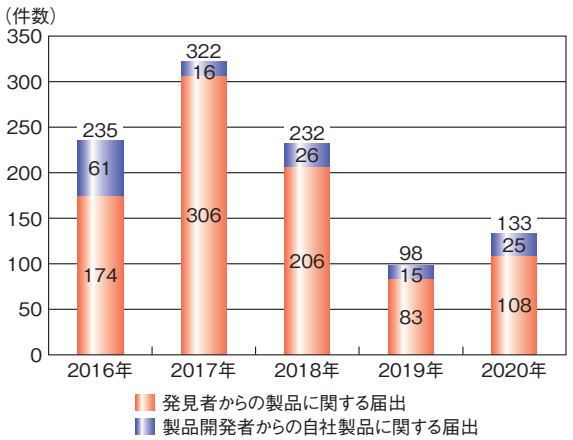
図 1-3-11（次ページ）は、2016 年から 2020 年までのソフトウェア製品の届出受付数（不受理を除く）を示している。2016 年からソフトウェア製品の届出は年々減少していたが、2020 年は 242 件となり、2019 年の 214 件を上回る件数となった。ソフトウェア製品の届出のうち、製品開発者からの自社製品に関する届出は、242 件中 24 件となり、2019 年の 21 件から増加した。



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

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

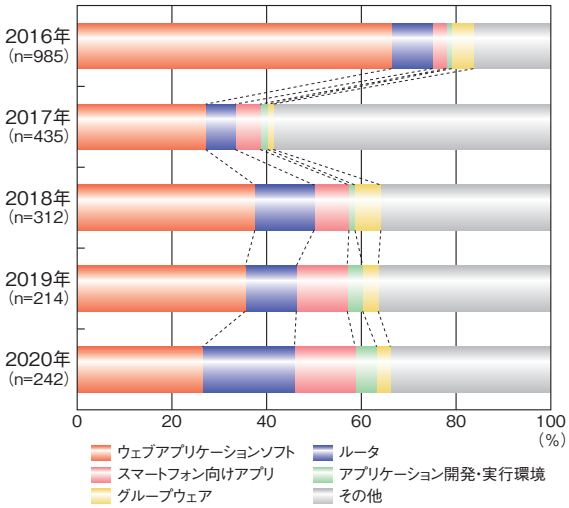
図 1-3-12 は、2016 年から 2020 年までの JVN 公表に至った届出数を示している。2017 年、2018 年、2019 年と年々 JVN 公表数は減少していたが、2020 年は一転して件数が増加した。自社製品に関する届出についても、2019 年の 15 件から増加し、2020 年は 25 件の公表となった。



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

(a) パートナーシップで取り扱ったソフトウェア製品の動向

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



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

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

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

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

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

利用者は、他のソフトウェア製品と同様にルータについても脆弱性が日々発見されていて、アップデートが必要となることを十分認識する必要がある。また、アップデートをするためには、JVN や製品開発者の Web サイト等を確認し、脆弱性対策情報やアップデート情報が新たに

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

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

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

(b) 公表判定委員会の判定による JVN 公表

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

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

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

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

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

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

製品の使用を停止することが求められる。

(c) 製品開発者による CNA への参加

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

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

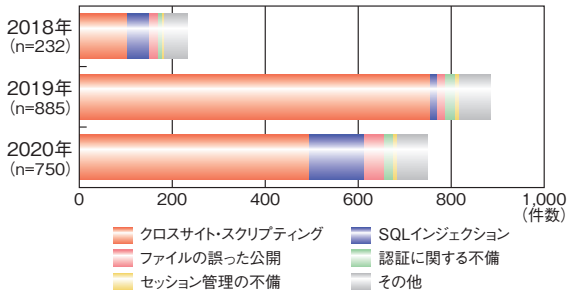
製品開発者が CNA として活動することで、自社の脆弱性情報の取り扱いレベルの向上やより効果的な流通が実現し、脆弱性悪用の被害が低減することが期待される。

(2) Web アプリケーション（Web サイト）の脆弱性

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

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

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



■図 1-3-14　脆弱性種類別の Web アプリケーションの届出受付数（2018 ～ 2020 年）
（出典）パートナーシップの届出状況を基に IPA が作成

SQL インジェクションは過去 10 年以上にわたり問題であり続け、IPA では 2008 年に「SQL インジェクション攻撃に関する注意喚起※229」、2017 年に「SQL インジェクションをはじめとしたウェブサイトの脆弱性の再点検と速やかな改修を※230」と題する注意喚起を行っているが 2020 年も解消されていない。

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

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

(a) SQL インジェクションの脆弱性

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

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

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

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

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

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

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

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

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

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

(c) Web サイト運営者に求められる対策

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

Web サイト運営者はまず、改めてそのような箇所に SQL インジェクションの脆弱性が存在していないか、IPA が公開している「ウェブ健康診断 仕様※231」等を参照の上、確認し、脆弱性が検出された場合は、詳細な診断を行うか、または改修を検討いただきたい。なお、Web サイト運営者が自組織だけで脆弱性の有無を確認できない場合は、セキュリティベンダに脆弱性診断を依頼する等の対応が考えられる。

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

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

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

COLUMN

「危険だから利用しない」ではなく「安全に利用するために」の対策を

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

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

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

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

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

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

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

認証を無効化されていた　https://xtech.nikkei.com/atcl/nxt/column/18/01157/081900017/〔2021/4/28 確認〕
※ 40 JPCERT/CC：マルウエア LODEINFO の進化　https://blogs.jpcert.or.jp/ja/2020/06/LODEINFO-2.html〔2021/4/28 確認〕
※ 41 株式会社ラック：【緊急レポート】Microsoft 社のデジタル署名ファイルを悪用する「SigLoader」による標的型攻撃を確認　https://www.lac.co.jp/lacwatch/report/20201201_002363.html〔2021/4/28 確認〕
※ 42 マクニカネットワークス株式会社、TeamT5, Inc.：標的型攻撃の実態と対策アプローチ 第 4 版　https://www.macnica.net/mpressioncss/feature_06.html〔2021/4/28 確認〕
※ 43 三菱重工業株式会社：当社グループ名古屋地区のネットワークに対する第三者からの不正アクセスに係る件　https://www.mhi.com/jp/notice/notice_200807.html〔2021/4/28 確認〕
※ 44 キヤノンマーケティングジャパン株式会社：航空宇宙・軍事企業を狙った標的型攻撃　https://eset-info.canon-its.jp/malware_info/trend/detail/200709.html〔2021/4/28 確認〕
※ 45 JPCERT/CC：JPCERT/CC インシデント報告対応レポート 2020 年 7 月 1 日～ 2020 年 9 月 30 日　https://www.jpcert.or.jp/pr/2020/IR_Report20201015.pdf〔2021/4/28 確認〕
※ 46 JPCERT/CC：Quasar Family による攻撃活動　https://blogs.jpcert.or.jp/ja/2020/12/quasar-family.html〔2021/4/28 確認〕
※ 47 JPCERT/CC：攻撃グループ Lazarus が侵入したネットワーク内で使用するツール　https://blogs.jpcert.or.jp/ja/2021/01/Lazarus_tools.html〔2021/4/28 確認〕
※ 48 https://www.jpcert.or.jp/research/AD.html〔2021/4/28 確認〕
※ 49 JPCERT/CC：Netlogon の特権の昇格の脆弱性（CVE-2020-1472）への早急な対応を　https://www.jpcert.or.jp/newsflash/2020091601.html〔2021/4/28 確認〕
※ 50 IPA：事業継続を脅かす新たなランサムウェア攻撃について　https://www.ipa.go.jp/files/000084974.pdf〔2021/5/13 確認〕
※ 51 IPA：【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について　https://www.ipa.go.jp/security/announce/2020-ransom.html〔2021/5/13 確認〕
※ 52 NISC：ランサムウエアによるサイバー攻撃について【注意喚起】　https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf〔2021/5/13 確認〕
※ 53 株式会社カプコン：不正アクセスによるシステム障害発生に関するお知らせ　https://www.capcom.co.jp/ir/news/html/201104.html〔2021/5/13 確認〕
※ 54 株式会社カプコン：不正アクセスによる情報流出に関するお知らせとお詫び　https://www.capcom.co.jp/ir/news/html/201116.html〔2021/5/13 確認〕
※ 55 株式会社カプコン：不正アクセスによる情報流出に関するお知らせとお詫び【第 3 報】　https://www.capcom.co.jp/ir/news/html/210112.html〔2021/5/13 確認〕
※ 56 株式会社カプコン：不正アクセスに関する調査結果のご報告【第 4 報】　https://www.capcom.co.jp/ir/news/html/210413.html〔2021/5/13 確認〕
※ 57 Bleeping Computer：Capcom hit by Ragnar Locker ransomware, 1TB allegedly stolen　https://www.bleepingcomputer.com/news/security/capcom-hit-by-ragnar-locker-ransomware-1tb-allegedly-stolen/〔2021/5/13 確認〕
※ 58 鉄建建設株式会社：サイバー攻撃による被害と復旧状況について　https://www.tekken.co.jp/topics/assets/20201009_topics.pdf〔2021/5/13 確認〕
※ 59 鉄建建設株式会社：サイバー攻撃による被害と復旧状況について（第三報）　https://www.tekken.co.jp/topics/assets/20201118_saibaosirase.pdf〔2021/5/13 確認〕
※ 60 株式会社 FFRI セキュリティ：標的型ランサムウェアの脅威　https://www.ffri.jp/blog/2020/06/2020-06-29-Targeted-ransomware-threat.htm〔2021/5/13 確認〕
※ 61 株式会社カスペルスキー：ランサムウェアを操る脅迫犯、盗んだデータを公開　https://blog.kaspersky.co.jp/ransomware-data-disclosure/26862/〔2021/5/13 確認〕
※ 62 マクニカネットワークス株式会社：ランサムウェア感染時の対応は本当に完璧ですか!?暴露型ランサムウェアの実態とその対応方法とは　https://www.macnica.net/sandj/ransomware.html/〔2021/5/13 確認〕
セキュアワークス株式会社：日本国内で増加する 標的型ランサムウェアインシデント　https://www.secureworks.jp/resources/at-targeted-ransomware-spreading-in-japan〔2021/5/13 確認〕
ZDNet：Ransomware gang publishes tens of GBs of internal data from LG and Xerox　https://www.zdnet.com/article/ransomware-gang-publishes-tens-of-gbs-of-internal-data-from-lg-and-xerox/〔2021/5/13 確認〕
パロアルトネットワークス株式会社：脅威に関する情報：Maze ランサムウェアのアクティビティ　https://unit42.paloaltonetworks.jp/threat-brief-maze-ransomware-activities/〔2021/5/13 確認〕
※ 63 三井物産セキュアディレクション株式会社：SNAKE（EKANS）ランサムウェアの内部構造を紐解く　https://www.mbsd.jp/blog/20200616.html〔2021/5/13 確認〕
IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2020 年 4 月～ 6 月]《付録》～ EKANS ランサムウェアの解析事例～　https://www.ipa.go.jp/files/000084401.pdf〔2021/5/13 確認〕
※ 64 JPCERT/CC：ランサムウエア対策特設サイト　https://www.jpcert.or.jp/magazine/security/nomore-ransom.html〔2021/5/13 確認〕
JPCERT/CC：高度サイバー攻撃（APT）への備えと対応ガイド～企業や組織に薦める一連のプロセスについて　https://www.jpcert.or.jp/research/apt-guide.html〔2021/5/13 確認〕
JPCERT/CC：高度サイバー攻撃への対処におけるログの活用と分析方法　https://www.jpcert.or.jp/research/apt-loganalysis.html〔2021/5/13 確認〕
IPA：ランサムウェア対策特設ページ　https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html〔2021/5/13 確認〕
IPA：『高度標的型攻撃』対策に向けたシステム設計ガイド　https://www.ipa.go.jp/security/vuln/newattack.html〔2021/5/13 確認〕
※ 65 IRM（Information Rights Management）：業務で使用する文書ファイル等を暗号化し、閲覧や編集等を制限する仕組み。
※ 66 JPCERT/CC：インシデントハンドリングマニュアル　https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf〔2021/5/13 確認〕
※ 67 トレンドマイクロ社：フィッシング攻撃に注意、「ビジネスメール詐欺」の攻撃手口を分析　https://blog.trendmicro.co.jp/archives/17003〔2021/4/28 確認〕
トレンドマイクロ社：経営幹部の Office 365 アカウントを狙う詐欺キャンペーン「Water Nue」　https://blog.trendmicro.co.jp/archives/26178〔2021/4/28 確認〕
パロアルトネットワークス株式会社：脅威攻撃グループ SilverTerrier による新型コロナウイルスをテーマにしたビジネスメール詐欺の手口　https://unit42.paloaltonetworks.jp/silverterrier-covid-19-themed-business-email-compromise/〔2021/4/28 確認〕
※ 68 被害金額については、2015 ～ 2020 年の年次報告書（IC3：Annual Reports　https://www.ic3.gov/Home/AnnualReports〔2021/4/28 確認〕）を参照した。
※ 69 FBI：FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic　https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic〔2021/4/28 確認〕
IC3：Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments　https://www.ic3.gov/Media/Y2020/PSA200401〔2021/4/28 確認〕
※ 70 Infosecurity Magazine：Australians Arrested Over $2.6m Email Scam　https://www.infosecurity-magazine.com/news/australians-arrested-over-26m/〔2021/4/28 確認〕
Mirage News：Five charged as part of ongoing investigations into $4.7 million business email compromise scam　https://www.miragenews.com/five-charged-as-part-of-ongoing-investigations-into-47-million-business-email-compromise-scam/〔2021/4/28 確認〕
U.S. Department of Justice：Nigerian National Brought to U.S. to Face Charges of Conspiring to Launder Hundreds of Millions of Dollars from Cybercrime Schemes　https://www.justice.gov/usao-cdca/pr/nigerian-national-brought-us-face-charges-conspiring-launder-hundreds-millions-dollars〔2021/4/28 確認〕
Liverpool City Champion Liverpool, NSW：Man arrested at Liverpool over alleged $6 million online scam　https://www.liverpoolchampion.com.au/story/6825426/man-arrested-at-liverpool-over-alleged-6-million-online-scam/〔2021/4/28 確認〕
U.S. Department of Justice：Rhode Island Man Pleads Guilty to Conspiracy to Launder Funds of Email Compromise Fraud Targeting Massachusetts Lawyer　https://www.justice.gov/usao-ma/pr/rhode-island-man-pleads-guilty-conspiracy-launder-funds-email-compromise-fraud-targeting〔2021/4/28 確認〕
U.S. Department of Justice：Three Chicago-Area Residents Charged With Conducting Online Romance Fraud and Other Schemes　https://www.justice.gov/usao-ndil/pr/three-chicago-area-residents-charged-conducting-online-romance-fraud-and-other-schemes〔2021/4/28 確認〕
Campbelltown-Macarthur Advertiser Campbelltown, NSW：

Glenfield man charged in relation to $4.7 million business email scam https://www.macarthuradvertiser.com.au/story/6929911/glenfield-man-charged-in-relation-to-47-million-business-email-scam/〔2021/4/28 確認〕
U.S. Department of Justice：Four Individuals Are Charged For Operating As 'Money Mules' In Separate Business Email Compromise Schemes https://www.justice.gov/usao-wdnc/pr/four-individuals-are-charged-operating-money-mules-separate-business-email-compromise〔2021/4/28 確認〕
U.S. Department of Justice：Six Defendants Arrested In Multiple States For Laundering Proceeds From Fraud Schemes Targeting Victims Across The United States Perpetrated By Ghana-Based Criminal Enterprise https://www.justice.gov/usao-sdny/pr/six-defendants-arrested-multiple-states-laundering-proceeds-fraud-schemes-targeting〔2021/4/28 確認〕
※ 71 産経新聞：犯罪収益引き出し疑い逮捕　島国バハマの法人被害か https://www.sankei.com/affairs/news/200716/afr2007160012-n1.html〔2021/4/28 確認〕
産経新聞：「ビジネスメール詐欺」被害総額2億円か　容疑の70代男ら逮捕 https://www.sankei.com/affairs/news/201013/afr2010130012-n1.html〔2021/4/28 確認〕
※ 72 INTERPOL：Three arrested as INTERPOL, Group-IB and the Nigeria Police Force disrupt prolific cybercrime group https://www.interpol.int/en/News-and-Events/News/2020/Three-arrested-as-INTERPOL-Group-IB-and-the-Nigeria-Police-Force-disrupt-prolific-cybercrime-group〔2021/4/28 確認〕
Group-IB：Operation Falcon Group-IB helps INTERPOL identify Nigerian BEC ring members https://www.group-ib.com/media/gib-interpol-bec/〔2021/4/28 確認〕
※ 73 Microsoft 社：Microsoft takes legal action against COVID-19-related cybercrime https://blogs.microsoft.com/on-the-issues/2020/07/07/digital-crimes-unit-covid-19-cybercrime/〔2021/4/28 確認〕
ZDNet：Microsoft seizes six domains used in COVID-19 phishing operations https://www.zdnet.com/article/microsoft-seizes-six-domains-used-in-covid-19-phishing-operations/〔2021/4/28 確認〕
ITmedia エンタープライズ：新型コロナウイルス便乗のビジネスメール詐欺、Microsoft がドメイン制圧 https://www.itmedia.co.jp/enterprise/articles/2007/09/news060.html〔2021/4/28 確認〕
※ 74 Proofpoint, Inc.：2020 'State of the Phish'：Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical〔2021/4/28 確認〕
ENISA：ENISA Threat Landscape 2020 – Phishing https://www.enisa.europa.eu/publications/phishing〔2021/4/28 確認〕
※ 75 トレンドマイクロ社：法人でのインシデント発生率は約 8 割、2021 年に向けて警戒すべき脅威とは https://blog.trendmicro.co.jp/archives/26357〔2021/4/28 確認〕
※ 76 一般社団法人日本損害保険協会:国内企業のサイバーリスク意識・対策実態調査 2020 https://www.sonpo.or.jp/cyber-hoken/data/2020-01/pdf/cyber_report2020.pdf〔2021/4/28 確認〕
※ 77 Check Point Software Technologies Ltd.：IR Case: The Florentine Banker Group https://research.checkpoint.com/2020/ir-case-the-florentine-banker-group/〔2021/4/28 確認〕
※ 78 Norfund：Norfund has been exposed to a serious case of fraud https://www.norfund.no/norfund-has-been-exposed-to-a-serious-case-of-fraud/〔2021/4/28 確認〕
Bleeping Computer：Scammers steal $10 million from Norway's state investment fund https://www.bleepingcomputer.com/news/security/scammers-steal-10-million-from-norways-state-investment-fund/〔2021/4/28 確認〕
バラクーダネットワークスジャパン株式会社：ほぼ完璧な BEC（ビジネスメール詐欺）によって 1000 万ドルの損害を受けたノルウェーの国有投資ファンド https://www.barracuda.co.jp/wonderfully-done-bec-scam-scores-10-million-from-a-norway-investment-fund/〔2021/4/28 確認〕
※ 79 徳島新聞：コロナ便乗メール詐欺　徳島県内初、県西企業 150 万円被害 https://www.topics.or.jp/articles/-/369213〔2021/4/28 確認〕
※ 80 独立行政法人石油天然ガス・金属鉱物資源機構：海外取引にかかる誤送金について http://www.jogmec.go.jp/news/release/news_01_000158.html〔2021/4/28 確認〕
※ 81 NZ Herald：Far North council scammed out of $100,000 after supplier's email hacked https://www.nzherald.co.nz/northern-advocate/news/far-north-council-scammed-out-of-100000-after-suppliers-email-hacked/7DZSNDDST3BNRLOVZZ6AJMLDWA/〔2021/4/28 確認〕
※ 82 BankInfoSecurity：BEC Scam Costs Trading Firm Virtu Financial $6.9 Million https://www.bankinfosecurity.com/bec-scam-costs-trading-firm-virtu-financial-69-million-a-14804〔2021/4/28 確認〕
※ 83 INTERPOL：Payments stopped, three arrested in medical supplies fraud case https://www.interpol.int/en/News-and-Events/News/2020/Payments-stopped-three-arrested-in-medical-supplies-fraud-case〔2021/4/28 確認〕
※ 84 AP NEWS：Wisconsin Republican Party says hackers stole $2.3 million https://apnews.com/article/wisconsin-republican-party-hackers-stole-641a8174e51077703888e2fa89070e12〔2021/4/28 確認〕
CNET Japan:トランプ氏の選挙資金、2 億円超がハッカーに盗まれる--ウィスコンシン州 https://japan.cnet.com/article/35161727/〔2021/4/28 確認〕
※ 85 The Star：Singapore sting international company in Hong Kong hit by US$6.6mil hacking scam https://www.thestar.com.my/tech/tech-news/2020/11/09/singapore-sting-international-company-in-hong-kong-hit-by-us66mil-hacking-scam〔2021/4/28 確認〕
South China Morning Post：Singapore sting: international company in Hong Kong hit by US$6.6 million hacking scam https://www.scmp.com/news/hong-kong/law-and-crime/article/3108831/singapore-sting-international-company-hong-kong-hit〔2021/4/28 確認〕
※ 86 日本経済新聞：JSP、虚偽の第三者指示で資金流出 最大 10 億円 https://www.nikkei.com/article/DGXMZO66375570Y0A111C2DTA000/〔2021/4/28 確認〕
株式会社 JSP：当社欧州グループ会社における資金流出事案に関する調査結果及び再発防止策の策定並びに役員報酬の一部自主返上に関するお知らせ https://www.co-jsp.co.jp/ir/upload_file/m000-/210430_europe.pdf〔2021/5/13 確認〕
※ 87 The Australian Financial Review：Fake Zoom invite cripples Aussie hedge fund with $8m hit https://www.afr.com/companies/financial-services/fake-zoom-invite-cripples-aussie-hedge-fund-with-8m-hit-20201122-p56f9c〔2021/4/28 確認〕
東洋経済オンライン：「なりすましメール」引っかかる人に共通する点 コロナ後を生き抜く https://toyokeizai.net/articles/-/397104?page=2〔2021/4/28 確認〕
※ 88 The Philadelphia Inquirer：Philly hunger relief group Philabundance lost nearly $1 million in cyberattack https://www.inquirer.com/business/philabundance-cybertheft-nearly-1-million-20201201.html〔2021/4/28 確認〕
※ 89 Business Insider：Thieves stole at least $2.7 million from political committees in 2020 cycle. Biden's campaign got hit, too. https://www.businessinsider.com/biden-campaign-money-stolen-pacs-political-committees-theft-embezzlement-2021-2〔2021/4/28 確認〕
The Hill：Federal political committees, campaigns lost $2.7M to theft, fraud in last cycle: report https://thehill.com/homenews/campaign/538448-federal-political-committees-campaigns-lost-27m-to-theft-fraud-in-last〔2021/4/28 確認〕
※ 90 IPA：【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口 https://www.ipa.go.jp/security/announce/20170403-bec.html〔2021/4/28 確認〕
※ 91 IPA：【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口（続報） https://www.ipa.go.jp/security/announce/201808-bec.html〔2021/4/28 確認〕
※ 92 IPA：【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口（第三報） https://www.ipa.go.jp/security/announce/2020-bec.html〔2021/4/28 確認〕
※ 93 J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan（サイバー情報共有イニシアティブ）の略称。IPA を情報ハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策につなげていく取り組み。
※ 94 IPA：サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））https://www.ipa.go.jp/security/J-CSIP/〔2021/4/28 確認〕
※ 95 IPA：情報セキュリティ白書 2020 https://www.ipa.go.jp/security/publications/hakusyo/2020.html〔2021/4/28 確認〕
※ 96 Agari, Inc.：Cosmic Lynx The Rise of Russian BEC https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-cosmic-lynx.pdf〔2021/4/28 確認〕
※ 97 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2020

年１月～３月］ https://www.ipa.go.jp/files/000081877.pdf〔2021/4/28 確認〕
※ 98 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2020年４月～６月］ https://www.ipa.go.jp/files/000084400.pdf〔2021/4/28 確認〕
※ 99 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2020年10月～12月］ https://www.ipa.go.jp/files/000088288.pdf〔2021/4/28 確認〕
※ 100 JPCERT/CC：ビジネスメール詐欺の実態調査報告書 https://www.jpcert.or.jp/research/BEC-survey.html〔2021/4/28 確認〕
マクニカネットワークス株式会社：ビジネスメール詐欺の実態と対策アプローチ 第1版 https://www.macnica.net/security/report_02.html/〔2021/4/28 確認〕
PwC：Business-Email-Compromise-Guide https://github.com/PwC-IR/Business-Email-Compromise-Guide/blob/main/PwC-Business_Email_Compromise-Guide.pdf〔2021/4/28 確認〕
※ 101 一般財団法人日本情報経済社会推進協会（JIPDEC）：なりすまし対策 ～電子証明書を使った本人確認と電子メールにおける送信元認証～ https://www.jipdec.or.jp/library/report/20201120_03.html〔2021/4/28 確認〕
一般財団法人日本情報経済社会推進協会（JIPDEC）：メールのなりすまし対策（S_MIMEとは） https://itc.jipdec.or.jp/jcan/smime-index.html〔2021/4/28 確認〕
迷惑メール対策委員会：電子メールのなりすまし対策 - 送信ドメイン認証でなりすましを防ぐ- https://www.dekyo.or.jp/soudan/data/anti_spam/auth_leaflet.pdf〔2021/4/28 確認〕
※ 102 IC3：Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud-Based Email Services, Costing US Businesses More Than $2 Billion https://www.ic3.gov/media/2020/200406.aspx〔2021/4/28 確認〕
※ 103 Microsoft 社：侵害された電子メール アカウントへの対応 https://docs.microsoft.com/ja-jp/microsoft-365/security/office-365-security/responding-to-a-compromised-email-account〔2021/4/28 確認〕
Microsoft 社：365 アカウントが Office されたかどうかを確認する方法 https://docs.microsoft.com/ja-jp/office365/troubleshoot/sign-in/determine-account-is-compromised〔2021/4/28 確認〕
TECH+：ビジネスメール詐欺に備えてメールの転送を見直そう https://news.mynavi.jp/itsearch/article/security/5349〔2021/4/28 確認〕
ファイア・アイ株式会社：Obscured by Clouds：Office 365 攻撃の洞察と Mandiant Managed Defense の調査方法 https://www.fireeye.com/blog/jp-threat-research/2020/07/insights-into-office-365-attacks-and-how-managed-defense-investigates.html〔2021/4/28 確認〕
※ 104 株式会社カスペルスキー：＜Kaspersky サイバー脅威調査：2020 年第２四半期の DDoS 攻撃＞新型コロナウイルスの流行下、DDoS 攻撃数は前年同期比の３倍に。人々の外出機会の減少が影響 https://www.kaspersky.co.jp/about/press-releases/2020_vir18092020〔2021/4/28 確認〕
Kaspersky Lab ZAO：DDoS attacks in Q1 2020 https://securelist.com/ddos-attacks-in-q1-2020/96837/〔2021/4/28 確認〕
Kaspersky Lab ZAO：DDoS attacks in Q2 2020 https://securelist.com/ddos-attacks-in-q2-2020/98077/〔2021/4/28 確認〕
※ 105 Kaspersky Lab ZAO：DDoS attacks in Q3 2020 https://securelist.com/ddos-attacks-in-q3-2020/99171/〔2021/4/28 確認〕
※ 106 UDP（User Datagram Protocol）：インターネットで標準的に使われているプロトコルの一種。接続のチェックが不要なコネクションレスなサービスに利用される。
※ 107 US-CERT：Alert (TA14-017A) UDP-Based Amplification Attacks https://us-cert.cisa.gov/ncas/alerts/TA14-017A〔2021/4/28 確認〕
※ 108 A10 ネットワークス株式会社：2020 年第２四半期の A10 DDoS 脅威インテリジェンスレポート：DDoS 攻撃が増大 https://www.a10networks.co.jp/news/blog/2020Q2Threatintelligencereport.html〔2021/4/28 確認〕
※ 109 A10 ネットワークス株式会社：日本はグローバルと比べ SSDP リフレクション攻撃に悪用されうる端末の割合が多い：最新の A10 国内脅威インテリジェンスレポート https://www.a10networks.co.jp/news/blog/Japanthreatreport1109.html〔2021/4/28 確認〕
※ 110 Amazon Web Services, Inc.：Threat Landscape Report – Q1 2020 https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf〔2021/4/28 確認〕
※ 111 アカマイ・テクノロジーズ合同会社：パケット／秒ベースで史上最大規模の DDOS 攻撃を AKAMAI が緩和 https://blogs.akamai.com/jp/2020/07/largest-ever-recorded-packet-per-secondbased-ddos-attack-mitigated-by-akamai.html〔2021/4/28 確認〕
※ 112 JPCERT/CC：DDoS 攻撃を示唆して仮想通貨による送金を要求する脅迫行為（DDoS 脅迫）について https://www.jpcert.or.jp/newsflash/2020090701.html〔2021/4/28 確認〕
※ 113 Bloomberg：ニュージーランド、危機管理計画を発動ー株式市場へのサイバー攻撃で https://www.bloomberg.co.jp/news/articles/2020-08-28/QFR9WPT0G1KZ〔2021/4/28 確認〕
※ 114 ZDNnet：DDoS extortionists target NZX, Moneygram, Braintree, and other financial services https://www.zdnet.com/article/ddos-extortionists-target-nzx-moneygram-braintree-and-other-financial-services/〔2021/4/28 確認〕
※ 115 Bitdefender：New dark_nexus IoT Botnet Puts Others to Shame https://labs.bitdefender.com/2020/04/new-dark_nexus-iot-botnet-puts-others-to-shame/〔2021/4/28 確認〕
※ 116 Mirai：IoT 機器に感染してボットネットを構成し、サイバー攻撃に悪用するウイルス。2016 年に史上最大規模の DDoS 攻撃を引き起こした。ソースコードが公開されていたため、様々な亜種が出現している。
※ 117 パス・トラバーサル：ファイルパス名の名前解決において特殊文字の処理に不備があり、本来アクセス権限のないディレクトリ等にアクセスできてしまう脆弱性。別名、ディレクトリ・トラバーサル。
※ 118 Fortinet, Inc.：FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests https://www.fortiguard.com/psirt/FG-IR-18-384〔2021/4/28 確認〕
※ 119 JPCERT/CC：Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について https://www.jpcert.or.jp/newsflash/2020112701.html〔2021/4/28 確認〕
※ 120 Pulse Secure, LLC.：SA44101 - 2019-04: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101〔2021/4/28 確認〕
※ 121 JPCERT/CC：Pulse Connect Secure の脆弱性を狙った攻撃事案 https://blogs.jpcert.or.jp/ja/2020/03/pulse-connect-secure.html〔2021/4/28 確認〕
※ 122 日経 XTECH：パッチ未適用のパルスセキュア社 VPN、日本企業 46 社の IP アドレスがさらされる https://xtech.nikkei.com/atcl/nxt/news/18/08605/〔2021/4/28 確認〕
※ 123 Microsoft 社：Windows SMBv3 クライアント / サーバーのリモートでコードが実行される脆弱性 https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2020-0796〔2021/4/28 確認〕
※ 124 Microsoft 社：Windows SMBv3 クライアント / サーバーの情報漏えいの脆弱性 https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2020-1206〔2021/4/28 確認〕
※ 125 ゼロデイ：脆弱性が発見・報告された日から、その脆弱性を解消するための手段が確立するまでの期間のこと。
※ 126 JSOF Ltd.：Ripple20 https://www.jsof-tech.com/disclosures/ripple20/〔2021/4/28 確認〕
※ 127 https://jvndb.jvn.jp/〔2021/4/28 確認〕
※ 128 IPA：【注意喚起】特定の組織からの注文連絡等を装ったばらまき型メールに注意 https://www.ipa.go.jp/security/topics/alert271009.html〔2021/4/28 確認〕
※ 129 キヤノンマーケティングジャパン株式会社：2019 年上半期マルウェアレポート https://eset-info.canon-its.jp/files/user/malware_info/images/ranking/pdf/MalwareReport_2019FirstHalf.pdf〔2021/4/28 確認〕
※ 130 IPA：「Emotet」と呼ばれるウイルスへの感染を狙うメールについて https://www.ipa.go.jp/security/announce/20191202.html〔2021/4/28 確認〕
※ 131 JPCERT/CC：マルウエア Emotet の感染に繋がるメールの配布活動の再開について（追加情報） https://www.jpcert.or.jp/newsflash/2020072001.html〔2021/4/28 確認〕
※ 132 キヤノンマーケティングジャパン株式会社：2019 年 10 月マルウェアレポート https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1910.html〔2021/4/28 確認〕
※ 133 トレンドマイクロ社：サイバー犯罪の根本解決：EUROPOL による EMOTET テイクダウン https://blog.trendmicro.co.jp/archives/27132〔2021/4/28 確認〕
※ 134 Europol：World's most dangerous malware EMOTET disrupted through global action https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action〔2021/4/28 確認〕
※ 135 Malwarebytes Inc.：Cleaning up after Emotet: the law enforcement file https://blog.malwarebytes.com/threat-analysis/2021/01/cleaning-up-after-emotet-the-law-enforcement-file/〔2021/4/28 確認〕

TECH+：Malwarebytes、マルウェア「Emotet」の削除を開始　https://news.mynavi.jp/article/20210428-1879994/〔2021/4/28 確認〕
※ 136 総務省：マルウェアに感染している機器の利用者に対する注意喚起の実施　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00095.html〔2021/4/28 確認〕
※ 137 Mal Eats：IcedID の感染につながる日本向けキャンペーンの分析　https://mal-eats.net/2020/11/12/analysis_of_the-_icedid_campaign_for_japan/〔2021/4/28 確認〕
※ 138 Juniper Networks, Inc.：COVID-19 and FMLA Campaigns used to install new IcedID banking malware　https://blogs.juniper.net/en-us/threat-research/covid-19-and-fmla-campaigns-used-to-install-new-icedid-banking-malware〔2021/4/28 確認〕
※ 139 ProofPoint, Inc.：ZLoader Loads Again: New ZLoader Variant Returns　https://www.proofpoint.com/us/blog/threat-insight/zloader-loads-again-new-zloader-variant-returns〔2021/4/28 確認〕
※ 140 株式会社ラック：分析レポート：Emotet の裏で動くバンキングマルウェア「Zloader」に注意　https://www.lac.co.jp/lacwatch/people/20201106_002321.html〔2021/4/28 確認〕
※ 141 Malwarebytes Inc.：The "Silent Night" Zloader/Zbot　https://resources.malwarebytes.com/files/2020/05/The-Silent-Night-Zloader-Zbot_Final.pdf〔2021/4/28 確認〕
※ 142 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2018年10月～12月］　https://www.ipa.go.jp/files/000071273.pdf〔2021/4/28 確認〕
※ 143 JPCERT/CC：マルウエア Emotet の感染活動について　https://www.jpcert.or.jp/newsflash/2019112701.html〔2021/4/28 確認〕
※ 144 トレンドマイクロ社：【注意喚起】トレンドマイクロのアンケートメールなどに偽装した偽メールに注意　https://www.is702.jp/news/3736/partner/12_t/〔2021/4/28 確認〕
※ 145 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2020年7月～9月］　https://www.ipa.go.jp/files/000086549.pdf〔2021/4/28 確認〕
※ 146 Lastline, Inc.：Evolution of Excel 4.0 Macro Weaponization　https://www.lastline.com/labsblog/evolution-of-excel-4-0-macro-weaponization/〔2021/4/28 確認〕
※ 147 サイバーリーズン・ジャパン株式会社：64 ビットの環境で Excel 4.0 のマクロを使用する攻撃　https://www.cybereason.co.jp/blog/cyberattack/3598/〔2021/4/28 確認〕
※ 148 IPA：安心相談窓口だより　iPhone に突然表示される不審なカレンダー通知に注意!　https://www.ipa.go.jp/security/anshin/mgdayori20200330.html〔2021/5/12 確認〕
※ 149 IPA：安心相談窓口だより　Facebook のメッセンジャーに届く動画に注意!　https://www.ipa.go.jp/security/anshin/mgdayori20200819.html〔2021/5/12 確認〕
※ 150 フィッシング対策協議会：2021/01 フィッシング報告状況　https://www.antiphishing.jp/report/monthly/202101.html〔2021/5/12 確認〕
※ 151 トレンドマイクロ社：【注意喚起】インスタグラムのなりすましアカウントに注意、不特定多数の法人アカウントで被害発生中　https://is702.jp/news/3801/〔2021/5/12 確認〕
※ 152 株式会社ユニクロ：ユニクロ公式インスタグラムを模倣した偽アカウントにご注意ください　https://faq.uniqlo.com/articles/FAQ/100006456〔2021/6/15 確認〕
※ 153 株式会社そごう・西武：【重要なお知らせ】弊社公式 SNS の「偽アカウント」にご注意ください　https://www.sogo-seibu.jp/ss/topics/page/instagram-info.html〔2021/6/15 確認〕
※ 154 https://www.antiphishing.jp/news/alert/kyufukin_20201015.html〔2021/5/12 確認〕
※ 155 独立行政法人国民生活センター：新型コロナウイルス感染症関連　http://www.kokusen.go.jp/soudan_now/data/coronavirus.html〔2021/5/12 確認〕
※ 156 総務省：特別定額給付金（新型コロナウイルス感染症緊急経済対策関連）　https://www.soumu.go.jp/menu_seisaku/gyoumukanri_sonota/covid-19/kyufukin.html〔2021/5/12 確認〕
※ 157 https://www.caa.go.jp/policies/policy/consumer_policy/assets/consumer_policy_cms102_210209_01.pdf〔2021/5/12 確認〕
※ 158 総務省:令和2年版 情報通信白書　第5章　第2節　ICT サービスの利用動向　https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/n5200000.pdf〔2021/5/12 確認〕
※ 159 IPA：安心相談窓口だより　宅配便業者をかたる偽ショートメッセージに引き続き注意!　https://www.ipa.go.jp/security/anshin/mgdayori20200220.html〔2021/5/12 確認〕
※ 160 独立行政法人国民生活センター:宅配便業者を装った「不在通知」の偽 SMS に注意しましょう― URL にはアクセスしない、ID・パスワードを入力しない！―　http://www.kokusen.go.jp/news/data/n-20201126_2.html〔2021/5/12 確認〕
※ 161 フィッシング対策協議会：Amazon をかたるフィッシング（2020/11/27）　https://www.antiphishing.jp/news/alert/amazon_20201127.html〔2021/5/12 確認〕
※ 162 楽天グループ株式会社：【ご注意ください】楽天市場を装った不審な SMS（商品発送通知を装った SMS）（2020 年 11 月 19 日更新）　https://ichiba.faq.rakuten.net/detail/000010078〔2021/5/12 確認〕
※ 163 読売新聞オンライン：ネット不正送金急増　4か月被害144件 過去の年間最多上回る　https://www.yomiuri.co.jp/local/aichi/news/20200522-OYTNT50103/〔2021/5/12 確認〕
※ 164 JC3：インターネットバンキングの不正送金の被害に注意　https://www.jc3.or.jp/topics/banking/phishing.html〔2021/5/12 確認〕
※ 165 フィッシング対策協議会：2020/12 フィッシング報告状況　https://www.antiphishing.jp/report/monthly/202012.html〔2021/5/12 確認〕
※ 166 沖縄タイムス：「異常ログインの可能性あり」銀行を装いショートメール　不正送金 1530 万円を確認　https://www.okinawatimes.co.jp/articles/gallery/676556?ph=1〔2021/5/12 確認〕
※ 167 IPA：安心相談窓口だより　遠隔操作を他人に安易に許可しないで!　https://www.ipa.go.jp/security/anshin/mgdayori20201125.html〔2021/5/12 確認〕
※ 168 消費者庁:「Microsoft」のロゴを用いて信用させ、パソコンのセキュリティ対策のサポート料などと称して多額の金銭を支払わせる事業者に関する注意喚起　https://www.caa.go.jp/notice/assets/consumer_policy_cms103_210219_1.pdf〔2021/5/12 確認〕
※ 169 Microsoft 社：テクニカル サポート詐欺から身を守る　https://support.microsoft.com/ja-jp/windows/ テクニカル - サポート詐欺から身を守る -2ebf91bd-f94c-2a8a-e541-f5c800d18435〔2021/5/12 確認〕
※ 170 独立行政法人国民生活センター：全国の消費生活センター等　http://www.kokusen.go.jp/map/〔2021/5/12 確認〕
※ 171 IPA：安心相談窓口だより　スマートフォンで偽のセキュリティ警告からアプリのインストールへ誘導する手口に注意　https://www.ipa.go.jp/security/anshin/mgdayori20190918.html〔2021/5/12 確認〕
※ 172 自動継続課金：ここでは「一定の利用期間ごとに定額を支払う料金方式、かつ、利用契約が自動更新される方式」を指す。なお、「一定の利用期間ごとに定額を支払う料金方式」は、Android では「定期購入」、iPhone では「サブスクリプション」と呼ばれる。
※ 173 https://www.tsr-net.co.jp/news/analysis/20210115_01.html〔2021/5/12 確認〕
※ 174 任天堂株式会社：「ニンテンドーネットワーク ID」に対する不正ログイン発生のご報告と「ニンテンドーアカウント」を安全にご利用いただくためのお願い　https://www.nintendo.co.jp/support/information/2020/0424.html〔2021/5/12 確認〕
ScanNetSecurity: 続報：ニンテンドーネットワーク ID 不正ログイン、新たに14万件判明（任天堂）　https://scan.netsecurity.ne.jp/article/2020/06/11/44194.html〔2021/5/12 確認〕
※ 175 NNID はニンテンドーのゲーム機でインターネットを利用するためのアカウントである。またニンテンドーアカウントはゲーム機以外のニンテンドーの機器を利用するためのアカウントである。
※ 176 株式会社カプコン：不正アクセスに関する調査結果のご報告【第4報】　https://www.capcom.co.jp/ir/news/html/210413.html〔2021/5/12 確認〕
Security NEXT：カプコンへの不正アクセス、侵入経路は予備に残した以前の VPN 機器　https://www.security-next.com/125237〔2021/5/12 確認〕
※ 177 Classi 株式会社：ご報告とご注意のお願い　https://corp.classi.jp/news/2154/〔2021/5/12 確認〕
※ 178 ナカバヤシ株式会社：弊社が運営する「フエルモール」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ【続報】https://www.nakabayashi.co.jp/news/2020/info/715〔2021/5/12 確認〕
※ 179 株式会社リジョブ：不正アクセスによる個人情報の流出について　https://rejob.co.jp/topics/2020041910295〔2021/5/12 確認〕
※ 180 株式会社キタムラ：「カメラのキタムラ ネットショップ」への"なりすまし"による不正アクセス発生について　https://www.kitamura.jp/topics/2020/20200615_01.html〔2021/5/12 確認〕
日本経済新聞：「カメラのキタムラ」個人情報 40 万件が閲覧された恐れ　https://www.nikkei.com/article/DGXMZO60440520X10C20A6000000/〔2021/5/12 確認〕
※ 181 株式会社キッチハイク：不正アクセスによる情報流出の可能性に関するお詫びとお知らせ（第四報・最終）　https://kitchhike.jp/newsblog/2020/7/24〔2021/5/12 確認〕
※ 182 QUOINE 株式会社：当社利用のドメイン登録サービスにおける不

正アクセスについて（最終報） https://blog.liquid.com/ja/20210120-important-notice-final〔2021/5/12 確認〕
※ 183 Peatix Inc.：弊社が運営する「Peatix(http://peatix.com/)」への不正アクセス事象に関する第三者調査機関による調査結果のご報告と今後の対応について https://announcement.peatix.com/20201216_ja.pdf〔2021/5/12 確認〕
※ 184 東建コーポレーション株式会社：不正アクセスによる個人情報流出について（第二報） https://www.token.co.jp/corp/information/about_unauthorized/〔2021/5/12 確認〕
※ 185 PayPay 株式会社：当社管理サーバーのアクセス履歴について - PayPay からのお知らせ https://paypay.ne.jp/notice/20201207/02/〔2021/5/12 確認〕
※ 186 株式会社駅レンタカーシステム：不正アクセスによるお客さまメールアドレス流出のお知らせとお詫びについて https://www.ekiren.co.jp/info/20201218_pressrelease.pdf〔2021/5/12 確認〕
※ 187 株式会社 TIMERS：不正アクセスによる情報流出に関するお詫びとお知らせ（第三報・最終） https://help.famm.us/hc/ja/articles/360054657071-%E4%B8%8D%E6%AD%A3%E3%82%A2%E3%82%AF%E3%82%BB%E3%82%B9%E3%81%AB%E3%82%88%E3%82%8B%E6%83%85%E5%A0%B1%E6%B5%81%E5%87%BA%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E3%81%8A%E8%A9%AB%E3%81%B3%E3%81%A8%E3%81%8A%E7%9F%A5%E3%82%89%E3%81%9B-%E7%AC%AC%E４%B８%８９%E５%A０%B１-%E６%９C%８０%E７%B５%８２-〔2021/5/12 確認〕
※ 188 株式会社マイナビ：「マイナビ転職」への不正ログイン発生に関するお詫びとお願い https://www.mynavi.jp/topics/post_29797.html〔2021/5/12 確認〕
※ 189 ANA：SITA 社システムへの不正アクセスによる ANA マイレージクラブ会員情報の漏洩について https://www.ana.co.jp/ja/jp/amc/news/info/2021/210306_memberinfo.html〔2021/5/12 確認〕
JAL：SITA 社セキュリティ事故による JAL マイレージバンク会員情報の漏洩について https://www.jal.co.jp/jp/ja/info/2021/other/210305/〔2021/5/12 確認〕
※ 190 株式会社アーバンリサーチ：アーバンリサーチ公式オンラインストアからの個人情報流出に関するお詫びとお願い https://www.urban-research.co.jp/news/company/2021/03/info210310/〔2021/5/12 確認〕
※ 191 https://privacymark.jp/system/reference/pdf/2019JikoHoukoku_201109.pdf〔2021/5/12 確認〕
※ 192 日本経済新聞：みずほ総研、顧客情報最大 250 万件紛失 https://www.nikkei.com/article/DGXMZO61780350R20C20A7EE9000/〔2021/5/12 確認〕
サイバーセキュリティ .com：250 万件の個人情報記録した媒体を誤廃棄 | みずほ総合研究所株式会社 https://cybersecurity-jp.com/news/37854〔2021/5/12 確認〕
※ 193 国土交通省神戸運輸監理部：行政文書の誤廃棄・紛失について https://wwwtb.mlit.go.jp/kobe/content/000161825.pdf〔2021/5/12 確認〕
※ 194 ヤフー株式会社：Yahoo! JAPAN ID の登録情報システム不具合に関するお詫びと不具合解消に関するお知らせ https://about.yahoo.co.jp/pr/release/2020/08/06b/〔2021/5/12 確認〕
※ 195 楽天株式会社：クラウド型営業管理システムへの社外の第三者によるアクセスについて https://corp.rakuten.co.jp/news/update/2020/1225_01.html〔2021/5/12 確認〕
※ 196 PayPay 株式会社：当社管理サーバーのアクセス履歴について - PayPay からのお知らせ https://paypay.ne.jp/notice/20201207/02/〔2021/5/12 確認〕
イオン株式会社：お問い合わせフォームへの社外の第三者によるアクセスについて https://www.aeon.info/wp-content/uploads/news/important/pdf/2021/01/210125R_1_1.pdf〔2021/5/14 確認〕
株式会社イオン銀行：「来店予約・オンライン相談サービス」システムへの第三者による不正アクセスについて https://www.aeonbank.co.jp/news/2021/0222_01.html〔2021/5/14 確認〕
独立行政法人国際観光振興機構：クラウド型情報管理システムへの第三者によるアクセスの可能性について https://www.jnto.go.jp/jpn/news/20210121.pdf〔2021/5/14 確認〕
※ 197 株式会社両備システムズ：クラウド型システムへの第三者からのアクセスについて（更新） https://www.ryobi.co.jp/news/notification20210212〔2021/5/14 確認〕
※ 198 セールスフォース社：【お知らせ】当社一部製品をご利用のお客様におけるゲストユーザに対する共有に関する設定について（セースルフォース・ドットコム） https://www.salesforce.com/jp/company/news-press/press-releases/2020/12/201225/〔2021/5/12 確認〕
セールスフォース社：ゲストユーザセキュリティポリシーのベストプラクティス https://help.salesforce.com/articleView?id=000355945&language=ja&mode=1&type=1〔2021/5/14 確認〕
セールスフォース社:コミュニティ、Salesforce サイト（旧 Force.com サイト）におけるゲストユーザの利用について https://help.salesforce.com/articleView?id=000356139&type=1&mode=1〔2021/5/14 確認〕
※ 199 NISC：Salesforce の製品の設定不備による意図しない情報が外部から参照される可能性について https://www.nisc.go.jp/active/infra/pdf/salesforce20210129.pdf〔2021/5/14 確認〕
※ 200 ソフトバンク株式会社：楽天モバイルへ転職した元社員の逮捕について https://www.softbank.jp/corp/news/press/sbkk/2021/20210112_01/〔2021/5/12 確認〕
※ 201 ソフトバンク株式会社：訪問販売代理店でのお客さま情報の不正取得について https://www.softbank.jp/corp/news/press/sbkk/2021/20210304_01/〔2021/5/12 確認〕
※ 202 ITmedia NEWS:NEC もソースコード流出を確認、GitHub で三井住友銀、NTT データに続き https://www.itmedia.co.jp/news/articles/2102/01/news118.html〔2021/5/12 確認〕
※ 203 LINE 株式会社：LINE における個人情報の取り扱いに関連する主な予定および取り組みについて https://linecorp.com/ja/pr/news/ja/2021/3680〔2021/5/12 確認〕
※ 204 JPCERT/CC、IPA：Japan Vulnerability Notes（JVN） https://jvn.jp/〔2021/4/28 確認〕
※ 205 NIST：National Vulnerability Database（NVD） https://nvd.nist.gov/〔2021/4/28 確認〕
※ 206 公表年は、ベンダがアドバイザリを公開した年、他組織やセキュリティポータルサイト等の登録／公開した年、発見者が一般向けに報告した年等、脆弱性対策情報が一般に公表された年を指す。なお、JVN iPedia で脆弱性対策情報を公開した年は「登録年」としている。
※ 207 IPA：共通脆弱性識別子 CVE 概説 https://www.ipa.go.jp/security/vuln/CVE.html〔2021/4/28 確認〕
※ 208 The MITRE Corporation：CVE Numbering Authorities https://cve.mitre.org/cve/cna.html〔2021/4/28 確認〕
※ 209 The MITRE Corporation：米国政府向けの技術支援や研究開発を行う非営利組織。80 を超える主要な脆弱性情報サイトと連携して、脆弱性情報の収集と、重複のない CVE の採番を行っている。
※ 210 The MITRE Corporation：CVE Adds 7 New CVE Numbering Authorities (CNAs) https://cve.mitre.org/news/archives/2016/news.html〔2021/4/28 確認〕
※ 211 The MITRE Corporation：Coalfire Labs Added as CVE Numbering Authority (CNA) https://cve.mitre.org/news/archives/2020/news.html〔2021/4/28 確認〕
※ 212 2014 年 9 月に「複数の Android アプリに SSL 証明書を適切に検証しない脆弱性」が公表されたことに伴い、1,200 件を超える Android アプリの脆弱性対策情報が JVN iPedia に登録された。
※ 213 IPA：共通脆弱性タイプ一覧 CWE 概説 https://www.ipa.go.jp/security/vuln/CWE.html〔2021/4/28 確認〕
※ 214 IPA：共通脆弱性評価システム CVSS 概説 https://www.ipa.go.jp/security/vuln/CVSS.html〔2021/4/28 確認〕
※ 215 JPCERT/CC：セキュアコーディング https://www.jpcert.or.jp/securecoding/〔2021/4/28 確認〕
※ 216 Microsoft 社：Netlogon の特権の昇格の脆弱性 https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2020-1472〔2021/4/28 確認〕
※ 217 Microsoft 社：Attacks exploiting Netlogon vulnerability (CVE-2020-1472) https://msrc-blog.microsoft.com/2020/10/29/attacks-exploiting-netlogon-vulnerability-cve-2020-1472/〔2021/4/28 確認〕
※ 218 NHK：リモート接続ねらうサイバー攻撃が急増 テレワーク増加で https://www3.nhk.or.jp/news/html/20201112/k10012708711000.html〔2021/4/28 確認〕
※ 219 JPCERT/CC：複数の SSL VPN 製品の脆弱性に関する注意喚起 https://www.jpcert.or.jp/at/2019/at190033.html〔2021/4/28 確認〕
JPCERT/CC：Palo Alto Networks 製品の脆弱性（CVE-2020-2021）について https://www.jpcert.or.jp/newsflash/2020063001.html〔2021/4/28 確認〕
JPCERT/CC：Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性（CVE-2018-13379）の影響を受けるホストに関する情報の公開について https://www.jpcert.or.jp/newsflash/2020112701.html〔2021/4/28 確認〕
JPCERT/CC：Pulse Connect Secure の脆弱性への対策や侵害有無などの確認を https://www.jpcert.or.jp/newsflash/2020041701.html〔2021/4/28 確認〕
※ 220 IPA：Zoom の脆弱性対策について https://www.ipa.go.jp/security/ciadr/vul/alert20200403.html〔2021/4/28 確認〕

※ 221 株式会社カスペルスキー：コロナ禍の1年：リモートデスクトッププロトコルへの攻撃が高い水準を維持　https://blog.kaspersky.co.jp/attacks-on-rdp-during-pandemic-year/30354/〔2021/4/28 確認〕
※ 222 NISC：Fortinet 製 VPN の脆弱性 (CVE-2018-13379) に関する重要インフラ事業者等についての注意喚起の発出について　https://www.nisc.go.jp/active/infra/pdf/fortinet20201203.pdf〔2021/4/28 確認〕
JPCERT/CC：Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について　https://www.jpcert.or.jp/newsflash/2020112701.html〔2021/4/28 確認〕
※ 223 IPA：脆弱性関連情報の届出受付　https://www.ipa.go.jp/security/vuln/report/index.html〔2021/4/28 確認〕
※ 224 ソフトウェア製品の取り扱い終了は、「不受理」「脆弱性でない」「脆弱性対策情報公表済み」「公表せずに製品開発者が利用者ごとに個別で対策を実施済み」のいずれかであることを指す。Web アプリケーションの取り扱い終了は、「不受理」「脆弱性でない」「連絡不可能」「修正完了」「IPA による注意喚起実施済み」のいずれかであることを指す。
※ 225 IPA：調整不能案件の公表判定業務における取扱いプロセス　https://www.ipa.go.jp/security/vuln/report/unreachable_process.html〔2021/4/28 確認〕
※ 226 LINE 株式会社：LINE が CVE Numbering Authority（CNA）の一員に　https://linecorp.com/ja/security/article/355〔2021/4/28 確認〕
※ 227 三菱電機株式会社：製品セキュリティーへの取組　https://www.mitsubishielectric.co.jp/psirt/〔2021/4/28 確認〕
※ 228 JPCERT/CC: CNA 活動レポート ～日本の 2 組織が新たに CNA に参加～　https://blogs.jpcert.or.jp/ja/2020/12/cna-2cna.html〔2021/4/28 確認〕
※ 229 IPA：SQL インジェクション攻撃に関する注意喚起　https://www.ipa.go.jp/security/vuln/documents/2008/200805_SQLinjection.html〔2021/4/28 確認〕
※ 230 IPA：【注意喚起】SQL インジェクションをはじめとしたウェブサイトの脆弱性の再点検と速やかな改修を　https://www.ipa.go.jp/security/announce/website_vuln.html〔2021/4/28 確認〕
※ 231 https://www.ipa.go.jp/files/000017319.pdf〔2021/4/28 確認〕
※ 232 https://www.ipa.go.jp/files/000017320.pdf〔2021/4/28 確認〕
※ 233 https://www.ipa.go.jp/files/000017316.pdf〔2021/4/28 確認〕

第2章
情報セキュリティを支える基盤の動向

2020 年度は、新型コロナウイルス感染症のパンデミックが国内外の政治・経済活動に大きな影響を及ぼした。人の移動が制限される中、フェイクニュースやフィッシングによる混乱、サプライチェーンを狙った攻撃が世界中で発生し、大きな被害が報告された。国内でも緊急事態宣言が発出され、テレワークやオンライン会議等の業務形態が急速に広まった。政府は新しい業務形態のセキュリティについて注意喚起を行うとともに、中小企業を含むサプライチェーンリスク対策、セキュリティ人材育成施策、他国と連携したセキュリティ対策の強化等を進めている。

本章では、情報セキュリティを支える基盤の動向として、国内外の主な政策、人材育成、国際標準化、各種認証、組織・個人における情報セキュリティの取り組みの実態等について解説する。

2.1 国内の情報セキュリティ政策の状況

本節では、政府が推進する情報セキュリティ対策の状況を述べる。

2.1.1 政府全体の政策動向

我が国のサイバーセキュリティに関わる政策や方針は、サイバーセキュリティ戦略本部で策定される。同戦略本部の事務局である内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）は、関連府省庁等と連携し、「サイバーセキュリティ戦略」「政府機関等の情報セキュリティ対策のための統一基準群※1」「重要インフラの情報セキュリティ対策に係る行動計画」等の策定、並びにサイバーセキュリティに関わる施策、国際連携、国民への普及啓発等を推進し、また行政機関等への監査や調査、助言等を実施している。

また、2021 年 9 月には行政におけるデジタル改革推進の司令塔となるデジタル庁の設置が予定されている。

本項では、2018 年 7 月に見直され、2021 年夏に再見直し案が閣議決定される予定の「サイバーセキュリティ戦略」と 2020 年度に実施された主な取り組みについて述べる。

(1) 次期「サイバーセキュリティ戦略」の検討

「サイバーセキュリティ戦略」とは、サイバーセキュリティ基本法に基づき策定された、我が国のサイバーセキュリティにおける基本的な立場等と策定後 3 年間の施策目標や実施方針を示した行動計画を指す。2015 年 9 月に初めて「サイバーセキュリティ戦略」が、2018 年 7 月にその後継となる「サイバーセキュリティ戦略」（以下、2018 年戦略）が閣議決定された。

2020 年度は 2018 年戦略の最終年度にあたる。このため、サイバーセキュリティ戦略本部では 2020 年 12 月より有識者会合を開始し、2021 年 2 月に「次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方※2」を公表し、同年 5 月に「次期サイバーセキュリティ戦略（骨子）※3」をまとめた。この骨子は、今後 3 年間における日本政府の目標や実施方針を示すものとなっており、現状認識、基本的な考え及び次期サイバーセキュリティ戦略の課題と方向性を示している。具体的には、経済社会の活力の向上及び持続的発展、国民が安全で安心して暮らせるデジタル社会、国際社会の平和・安定及び日本の安全保障への寄与等について記述している。

今後 IT 総合戦略本部及び国家保障会議からの意見聴取、パブリックコメントを実施し、閣議決定される予定である。

(2) 「サイバーセキュリティ 2020」の主な取り組み状況

「サイバーセキュリティ 2020※4」は、2018 年戦略の 2 年目にあたる 2019 年度の年次報告とそれを反映した 2020 年度の年次計画を統合したもので、府省庁はこれに基づき施策を実施してきた。2018 年戦略の最終年度にあたる 2020 年度は、主として 2019 年度までに実施さ

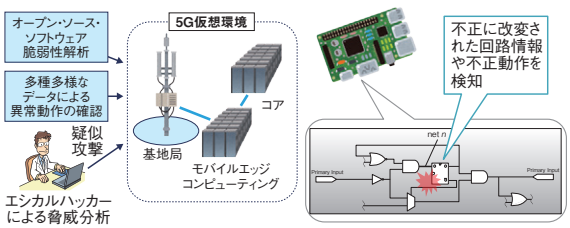
れた事業の継続や策定された指針・ガイドライン等の普及が計画された。以下、2018 年戦略の目的達成の施策として示されている四つの観点について、サイバーセキュリティ 2020 の計画に基づき実施された取り組みの中から注目すべきものを取り挙げる。

- 経済社会の活力の向上及び持続的発展

  内閣府は、戦略的イノベーション創造プログラム(SIP)第 2 期「IoT 社会に対応したサイバー・フィジカル・セキュリティ※5」により、様々な IoT 機器を守るため、中小企業を含むサプライチェーン全体を守ることに活用できる「サイバー・フィジカル・セキュリティ対策基盤」の研究開発を推進している。5 年間の研究期間の 3 年目にあたる 2020 年度には、中間報告として「SIP『IoT 社会に対応したサイバー・フィジカル・セキュリティ』ONLINE シンポジウム 2020※6」を開催した。

  経済産業省と IPA は、各社のサイバーセキュリティ経営実施状況の可視化のため、「サイバーセキュリティ経営ガイドライン実践のための可視化ツール」を開発している。2020 年 3 月にβ版が公開され、サイバーセキュリティ経営の定着度合い評価の試行が行われている(「2.4.1 (2) (a) 可視化ツールβ版の試用調査結果」参照)。また、先端技術を利活用したイノベーションを支えるため、知的財産の適切な管理の推進を目的とした「企業における営業秘密管理に関する実態調査 2020」を実施した(「2.8.1 営業秘密保護の動向」参照)。

  総務省は、2020 年 7 月に策定した「IoT・5G セキュリティ総合対策 2020」の一環として、5G ネットワークのセキュリティを担保できる仕組みの整備を進めている。まず、5G のネットワークやその構成要素及びサービスについて、ソフトウェア・ハードウェアの両面から技術的検証を行うとしている(図 2-1-1)。また、技術的検証における脆弱性調査、脅威分析の結果から「5G ネットワーク構築におけるセキュリティに関する対策等の留意点(令和 2 年度版)※7」を発行した(「IoT・5G セキュリティ総合対策 2020」のその他の取り組みについては「2.1.3 総務省の政策」を参照)。



■図 2-1-1　5G ネットワークのセキュリティ確保に向けた技術的検証のイメージ

(出典)総務省「令和 3 年度総務省サイバーセキュリティ関連予算概算要求について※8」を基に IPA が編集

- 国民が安全で安心して暮らせる社会の実現

  サイバーセキュリティ対策推進会議※9(CISO 等連絡会議)は、政府調達におけるサプライチェーン・リスク対策のため、2020 年 6 月、「委託先等で発生した政府機関の要保護情報に係るセキュリティインシデントの情報共有に関する申合せ※10」の新規合意と、「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ※11」の改正(独立行政法人及び基本法に定める指定法人を対象に追加)を実施した。総務省と経済産業省は 2020 年 6 月、官民双方が安心・安全にクラウドサービスを活用していくために、「政府情報システムのためのセキュリティ評価制度(Information system Security Management and Assessment Program:通称、ISMAP(イスマップ))」の運用を開始した。将来的に、制度の定着状況を見ながら独立行政法人や指定法人も対象としていき、重要インフラを始めとする民間企業に対しても周知を進めるとしている(制度の詳細は「2.6.3 政府情報システムのためのセキュリティ評価制度(ISMAP)」参照)。

- 国際社会の平和・安定及び我が国の安全保障への寄与

  外務省は 2020 年 5 月、国連安全保障理事会アリア・フォーミュラ会合に参加、新型コロナウイルス感染症(以下、新型コロナウイルス)に関連した医療セクターに対するサイバー攻撃への懸念を表明した※12。また、2021 年 3 月、国連オープン・エンド作業部会最終会合においてサイバー空間のルールについて報告書が採択され、外務省はこれに積極的に関与してきたとしている※13(「2.2.1 国際社会と連携した取り組み」参照)。

  内閣官房、総務省及び経済産業省は、2020 年 10 月の第 13 回「日・ASEAN サイバーセキュリティ政策会議」において、サイバーセキュリティ能力構築での連携・協力について協議した※14(「2.1.3 (1) (d) 研究開発や人材育成等の横断的施策」「2.2.1 (3) アジア太平洋地域のサイバー連携」参照)。

  NISC は、サイバーセキュリティ分野における我が国と欧米及び ASEAN 諸国との国際的な連携・取り組みを強化することを目的として、2018 年以降、年 1 回「国際サイバーセキュリティワークショップ・演習」を開催しており、2021 年は 2 月にオンラインで開催した。出席者は九つの国や地域のサイバーセキュリティ関係省庁のサイバー演習実務者と我が国の内閣官房・サイバーセキュリティ関係省庁、独立行政法人等から合計 20

名が参加した※15。

また、2021年2月、NISC及びタイ・電子取引開発機構（ETDA：Electronic Transactions Development Agency）が共催し、タイ現地企業向けにセキュリティアセスメントをテーマとして普及啓発セミナーをオンラインで開催し、日タイ両国の有識者6名が登壇、両国から240名が参加した※16。2021年3月も、一般社団法人情報サービス産業協会（JISA：Japan Information Technology Services Industry Association）及びインドネシア工業省他の共催により、インドネシア現地企業向けに同様のオンラインセミナーを開催し、日インドネシア両国の有識者7名が登壇し、両国から220名が参加した※17。

- 横断的政策

研究開発の推進としては、2020年7月、NISCの研究開発戦略専門調査会に研究・産学官連携戦略ワーキンググループを設置し、我が国のサイバーセキュリティ研究開発の国際競争力を躍進させるための産学官エコシステムの構築を中心ビジョンとして、課題を解決するための方策を議論、整理した。またこの結果をまとめ、2021年3月「サイバーセキュリティ研究・産学官連携戦略ワーキンググループ最終報告※18」を公表した。

経済産業省は、IPAの産業サイバーセキュリティセンターを通じて、戦略マネジメント層※19の育成を目的に2019年度に実施した「戦略マネジメント系セミナー」の「セキュリティ組織管理」コースを発展させ、オンラインで実施した（「2.3.2(2)(c)戦略マネジメント系セミナー」参照）。また、サイバーセキュリティ月間イベントとして2021年3月「戦略マネジメント層向けサイバーセキュリティセミナー サイバー攻撃の被害事例から学ぶ※20」を総務部門、経営企画部門、事業部門の部長や課長を対象に実施した。

IPA、一般社団法人サイバーリスク情報センター産業横断サイバーセキュリティ検討会（CRIC CSF）、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA：Japan Network Security Association）等の業界団体、企業と国立高等専門学校機構は、実務者層・技術者層の育成のための研修・講義を連携して実施している（「2.3.4（6）産学官で連携した国立高等専門学校での取り組み」参照）。

国立研究開発法人情報通信研究機構（NICT：National Institute of Information and Communications Technology）のナショナルサイバートレーニングセンターでは、2019年度に引き続き実践的サイバー防御演習「CYDER」※21を実施した。2020年度は、事前オンライン学習と集合演習で構成される演習を全国47都道府県において合計106回開催した。集合研修においては新型コロナウイルス感染拡大対策を徹底した上で実施された※22。CYDERの演習体験を通じて組織のインシデントハンドリングに対応できる人材の育成に貢献している。

(3) 重要インフラの情報セキュリティ対策強化

日本の重要インフラの防護に係る基本的な枠組みとして、サイバーセキュリティ戦略本部は2017年4月に「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※23」（以下、第4次行動計画）を決定した。続いて2018年7月に新たな重要インフラ分野として「空港」分野を追加、2020年1月に障害の報告に係る法令、ガイドライン等について、分野ごとに以下の改訂を行った※24。

- 鉄道分野は「鉄道分野における情報セキュリティ確保に係る安全ガイドライン」を追加
- ガス分野は「ガス事業法施行規則第112条」から「ガス関係報告規則第4条」へ変更
- 政府・行政サービス分野は「地方公共団体における情報セキュリティポリシーに関するガイドライン」を追加
- クレジット分野は「割賦販売法（後払分野）に基づく監督の基本方針」を追加

なお、第5次行動計画は2022年内に決定されるものと見られる※25。

以下、2020年度における主な活動について述べる。

(a) 重要インフラ専門調査会における取り組み

重要インフラ専門調査会※26では、2020年度は第4次行動計画に基づく関係府省庁取り組み状況及び第5次行動計画の検討に向けた情勢の共有が行われた。なお、施策・ガイドライン等の改訂や新規策定は実施されていない。

(b)「分野横断的演習」の実施

NISCは、重要インフラ事業者の事業継続計画や官民・分野横断的な情報共有体制に関する検証及び課題抽出を行うことにより、障害対応体制の強化を図ることを目的とした分野横断的演習を2020年12月に実施した※27。本演習は、2006年度から毎年実施してきたが、2020年度は新型コロナウイルス感染拡大対策のため、

集合会場を使用せず、自分の職場またはテレワーク環境から参加する方式とした。インシデント発生時の情報共有や復旧計画といった従来の確認事項に加え、テレワークのセキュリティリスクを勘案した対処体制の構築やインシデント対応が適切に行えるかどうかも確認した。重要インフラ14分野の事業者や所管府省庁、情報セキュリティ関係機関等から4,047名（465組織）が参加した。

また、同日、日本コンピュータセキュリティインシデント対応チーム協議会（日本シーサート協議会）は、NISCと連携して一般企業向けの分野横断的演習をオンラインで実施し、協議会の会員企業96社から488名が参加した※28。本演習は6回目の開催であり、オンラインでの実施は初の試みとなる。その他、2020年10月に実施された「金融業界横断的なサイバーセキュリティ演習※29（Delta Wall V）」等、各重要インフラ分野及び重要インフラ事業者内での演習が実施された。前述の「サイバーセキュリティ2020」計画には、このような業界団体等による演習の実施を促進し、インシデント対応人材の裾野を広げることも含まれている。

(4) デジタル庁の設置

2020年9月に就任した菅義偉首相は、就任時記者会見で、複数の府省庁に分かれている行政デジタル化の関連政策を取りまとめて推進するため、デジタル庁を新設することを明言した※30。同月、デジタル庁設置を主導するためにデジタル改革担当大臣の役職が設置され、平井卓也元情報通信技術（IT）政策担当大臣が就任した※31。

デジタル庁設置に先立ち、2020年10月から11月、デジタル・ガバメント閣僚会議※32のもとに設置したデジタル改革関連法案WGにおいて、高度情報通信ネットワーク社会形成基本法（IT基本法）の見直しに関する考え方が議論された。また、同WGのもとに設置された作業部会でデジタル庁の所管業務や各府省庁からの移管計画等の考え方が議論された。親会であるデジタル・ガバメント閣僚会議では2020年12月、これらの考え方を取りまとめて「デジタル社会の実現に向けた改革の基本方針※33」として公開した。サイバーセキュリティ戦略本部においては、2021年2月の会合で上記の「デジタル社会の実現に向けた改革の基本方針」のうち、サイバーセキュリティに関係する部分の抜粋が共有された。

2021年5月、「デジタル庁」新設を柱とするデジタル改革関連法案※34が成立し、デジタル庁が2021年9月1日に発足することとなった。内閣官房情報通信技術（IT）総合戦略室はデジタル庁のサイトを開設※35し、平井卓也デジタル改革担当大臣のメッセージやデジタル庁に関する法令等の情報発信を開始した。また、2021年5月よりコンテンツ配信サービス「note」を利用してデジタル庁創設に向けた情報配信を開始した※36。

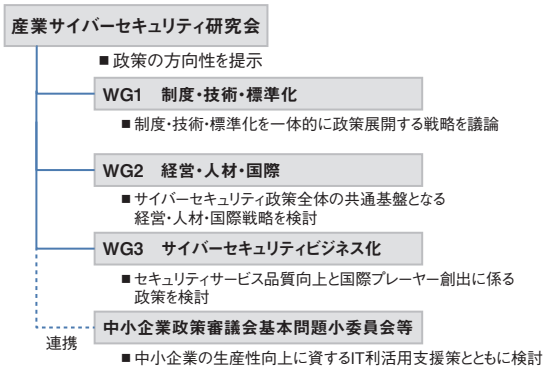
今後、デジタル庁設置に関しては、サイバーセキュリティ面での検証や議論も本格化するものと見られる。

2.1.2 経済産業省の政策

経済産業省は、サイバー空間、フィジカル空間を統合したサプライチェーン全体にわたるセキュリティ対策の実現に向け、制度、標準化、経営、人材、ビジネス等、様々な観点から施策を検討・実施している。

(1) 産業サイバーセキュリティ研究会

2017年12月、経済産業省は我が国の産業界が直面するサイバーセキュリティの課題を洗い出し、関連政策を推進するため、産業界を代表する経営者、インターネット関連の学識経験者等から構成される「産業サイバーセキュリティ研究会」を設置した※37。図2-1-2に同研究会の構成を示す。



■図2-1-2　産業サイバーセキュリティ研究会の構成
（出典）経済産業省「産業分野におけるサイバーセキュリティ政策※38」

同研究会では2020年4月に第4回会合を開催し、新型コロナウイルス関連詐欺、脆弱性、ランサムウェア等の直近の脅威への対策とデジタル化を進める中での対策を企業に呼びかけるため、「産業界へのメッセージ※39」を策定・公開した。また、2020年6月に第5回会合を開催し、「産業サイバーセキュリティ強化へ向けたアクションプラン※40」（2018年5月発表）における以下の四つのパッケージの進捗状況が共有され、今後の取り組み方針が合意された※41。

- サプライチェーンサイバーセキュリティ強化パッケージ

- サイバーセキュリティ経営強化パッケージ
- サイバーセキュリティ人材育成・活躍促進パッケージ
- セキュリティビジネスエコシステム創造パッケージ

以下では、本研究会で合意された取り組み方針に基づいた各 WG の 2020 年度の活動について述べる。

(a) WG1(制度・技術・標準化)

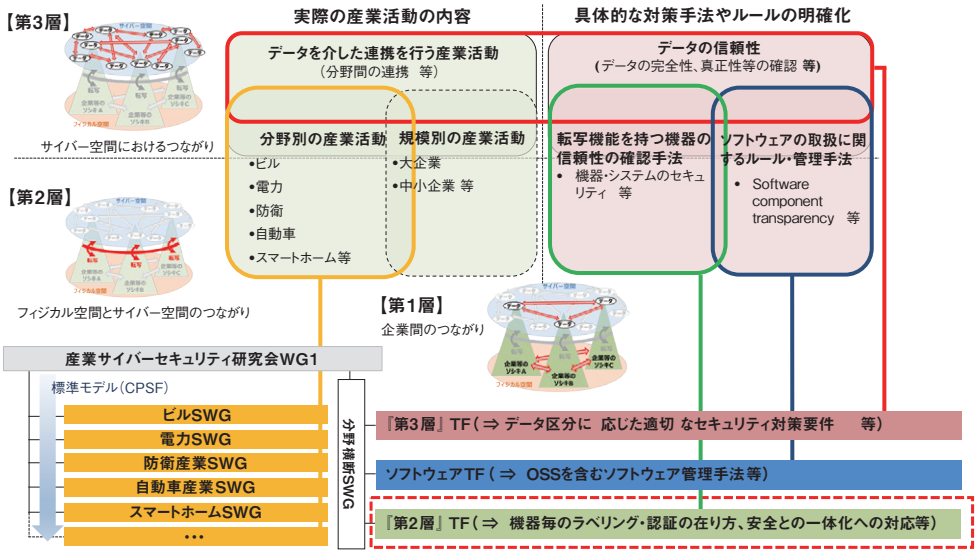
「サプライチェーンサイバーセキュリティ強化パッケージ」の活動を主に実施する WG1 では、産業サイバーセキュリティに関する制度・技術・標準化を一体として政策に展開する戦略を議論している。その前提として、サイバー空間とフィジカル空間の融合により、柔軟かつ動的なサプライチェーンが生まれるとし、これを価値創造過程(バリュークリエイションプロセス)と定義した。また、バリュークリエイションプロセス全体の業界横断的な標準モデルである「サイバー・フィジカル・セキュリティ対策フレームワーク※42 (The Cyber/Physical Security Framework) Version 1.0」(以下、CPSF)を 2019 年 4 月に策定した。

CPSF の具体化や実装、分野横断の共通課題を検討するため、WG1 には産業分野別サブワーキンググループ(SWG)と分野横断 SWG が設置されている。2020 年度の活動の主な成果について述べる。

産業分野別 SWG は、ビル、電力、防衛産業、自動車産業、スマートホーム、宇宙産業の六つの産業分野で活動している。ビル SWG は 2019 年 6 月に「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第 1 版※43」を公開した後、個別編(空調編)を作成中である。電力 SWG は 2021 年 2 月に「小売電気事業者のためのサイバーセキュリティ対策ガイドライン Ver1.0※44」を公開した。防衛産業 SWG は契約企業が保護すべき情報を取り扱う際に適用される「新情報セキュリティ基準(案)」を 2019 年 8 月に策定した。自動車産業 SWG は一般社団法人日本自動車工業会、一般社団法人日本自動車部品工業会と共同でセキュリティ対策項目、基準を策定し、2020 年上期に業界内各社でトライアルを行った結果を反映させ、同年 12 月に「自工会/部工会・サイバーセキュリティガイドライン 1.0 版※45」を公開した。スマートホーム SWG は、2021 年 4 月に「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン Ver1.0※46」を公開した。宇宙産業 SWG は、2021 年 1 月に新たに設置され、2021 年度中を目標に民間事業者向けの宇宙システムに関わるサイバーセキュリティ対策ガイドラインの開発を予定している。

分野横断 SWG は、2019 年度に引き続き CPSF の実装を促進するべく、第 2 層(フィジカル空間とサイバー空間のつながり)及び第 3 層(サイバー空間におけるつながり)に焦点を絞った層別タスクフォース(以下、TF)や、オープンソースソフトウェア(OSS:Open Source Software)等のソフトウェアの活用・脆弱性管理手法を検討するソフトウェア TF で議論を進めている(図 2-1-3)。

第 2 層 TF では、2020 年 11 月、「IoT セキュリティ・セーフティ・フレームワーク(IoT-SSF)」を策定し、公開



■図 2-1-3 タスクフォースの構成
(出典)経済産業省「『第 2 層:フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性※47」

した※48。本フレームワークはサイバー空間とフィジカル空間をつなぐ仕組みに起因する新たなリスクに着目し、リスク形態及びリスクに対応するセキュリティ・セーフティ対策の類型化の手法を提示している。IoT-SSF を活用することにより、フィジカル空間とサイバー空間をつなぐ機器やシステムに潜むリスクを踏まえて、機器やシステムのカテゴライズを行い、カテゴリごとのセキュリティ・セーフティ要求の観点を把握し、相互に比較することが可能となる。

第 3 層 TF では、データマネジメントを俯瞰するモデル及びデータの信頼性確保に求められる要件を検討している。2021 年 3 月の会合では「データの属性が場におけるイベントにより変化する過程を管理すること」をデータマネジメントの定義とし、「データが転々流通することにより、その属性を変えながら付加価値を生み出していく」社会に適合する形にモデルを策定することについて議論が行われた※49。

ソフトウェア TF では、OSS の管理手法に関するプラクティス集の策定及び国内でのSoftware Bill of Materials（SBOM）※50 の活用促進について検討している。2021 年 1 月の会合では、プラクティス集の作成計画と SBOM の活用促進に向けた実証事業の実施について議論が行われた※51。

なお、CPSF のモデルをサイバー・フィジカル・システム（CPS）をとらえるモデルの一つとして位置付け、日本案として国際標準化提案を行った。ISO/IEC JTC 1/SC 27 WG 4 で検討されている（「2.5.2 (4) WG 4（セキュリティコントロールとサービス）」参照）。

(b) WG2（経営・人材・国際）

「サイバーセキュリティ経営強化パッケージ」と「サイバーセキュリティ人材育成・活躍促進パッケージ」の活動を主に実践する WG2 では、サイバーセキュリティ対策における経営者の参画と人材育成、国際連携に関する政策を議論している。

経営に関しては、2017 年 11 月に公開した「サイバーセキュリティ経営ガイドライン Ver2.0※52」の普及・定着を図るため、IPA を通じて 2020 年 6 月に「サイバーセキュリティ経営ガイドライン Ver2.0 実践のためのプラクティス集 第 2 版」を公開した。また、2020 年 3 月にβ版が公開された「サイバーセキュリティ経営ガイドライン実践のための可視化ツール」についても、2021 年夏の Ver.1.0 リリースに向けて開発が進められている（「2.4.1 (2) セキュリティリスクマネジメント」参照）。

中小企業・地域に関しては、IPA を通じて、地域の事業者団体、セキュリティ企業、保険会社がチームを組み、中小企業向けのセキュリティ対策を支援する仕組みを構築することを目的とした「サイバーセキュリティお助け隊」の実証事業を 2019 年度に 8 地域で実施し、2020 年 6 月に報告書を公開した※53。2020 年度は、地域特性・産業特性等を考慮したマーケティング、機器・ソフトウェア・サービスの導入負荷低減、説明会等による普及啓発、支援のスリム化によるコスト低減等を目指し、13 地域と 2 産業分野においてインシデント対応支援を中心に実証事業を行い、2021 年 1 月に成果を報告した※54（「2.4.2 (2) (b) 中小企業向けサイバーセキュリティ対策支援体制構築事業」参照）。

IPA はこれらの実証事業の知見に基づき、中小企業向けのセキュリティサービスが満たすべき基準を整理し、2021 年 2 月「サイバーセキュリティお助け隊サービス基準（1.0 版）」「サイバーセキュリティお助け隊サービス審査登録機関基準（1.0 版）」を策定した。そして、サービス審査登録機関により、サービス基準を満たすことが確認されたサービスに対して「サイバーセキュリティお助け隊マーク」の使用権を付与する事業を開始した※55。

また経済産業省は 2020 年 6 月、「昨今の産業を巡るサイバーセキュリティに係る状況の認識と今後の取組の方向性について※56」の中で、サプライチェーン全体のセキュリティ確保に求められる取り組みの方向性を示し、官民協力のもと、サイバーセキュリティ対策の推進運動へつなげていくことを発表した。同報告書では、企業がリスクマネジメント強化のために取るべき三つのアクション「サプライチェーン共有主体間での高密度な情報共有」「機微技術情報の流出懸念時の経済産業省への報告」「適切な場合における（事案の）公表」が示された。2020 年 11 月、これらを基本行動指針として、大企業と中小企業がともにサイバーセキュリティ対策を推進する枠組み「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3：Supply Chain Cybersecurity Consortium）」が設立された（「2.4.2 (2) (a) サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）」参照）。SC3 には中小企業対策強化 WG が設置され、前出のサイバーセキュリティお助け隊の利用拡大等による中小企業の取り組み促進策について検討するとしている。

更に、地域の企業、行政機関、教育機関、関係団体等がセキュリティについて語り合い、「共助」の関係を築くコミュニティを形成するための「中小企業サイバーセキュリティ対策促進事業（地域 SECUNITY 形成促進事業）」を実施した（「2.4.2 (2) (d) 中小企業サイバーセ

キュリティ対策促進事業」を参照）。今後、SC3 等の枠組みも活用した、各地域におけるセキュリティ・コミュニティのプラクティスや課題の共有によるコミュニティ形成・活動強化の促進が検討される。

人材に関しては、独立行政法人国立高等専門学校機構、IPA、JPCERT コーディネーションセンター（JPCERT/CC：Japan Computer Emergency Response Team Coordination Center）及び業界団体と連携し、国立高等専門学校に対してセキュリティ人材育成のための、コンテンツ提供、講師派遣等の支援を行ってきた（「2.3.4 (6) 産学官で連携した国立高等専門学校での取り組み」参照）。今後、こうした連携を効果的かつ継続的なものとするために、多くの業界や地域の団体等が参加する SC3 の場を活用した取り組みの推進等が検討される。また、2020 年 9 月、先述の「サイバーセキュリティ経営ガイドライン Ver2.0」の付録文書として「サイバーセキュリティ体制構築・人材確保の手引き 第 1 版※57」を、2021 年 4 月には改定版として第 1.1 版※58 を公開した（「2.3.1 (3) (b)『サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版』の概要」参照）。

国際連携に関しては、IPA を通じて、2021 年 3 月に「インド太平洋地域向け日米産業制御システムサイバーセキュリティウィーク」を実施した（「2.3.2 (1) 中核人材育成プログラム」参照）。また、国際会議等で各国のステークホルダーと CPSF を軸とした議論を 2020 年 7 月～ 2021 年 1 月の間に合計 16 回行い、サイバー・フィジカル・セキュリティに関する共通認識を醸成した※59。

(c) WG3（サイバーセキュリティビジネス化）

「セキュリティビジネスエコシステム創造パッケージ」の活動を主に実践する WG3 では、セキュリティ製品・サービスの品質向上と国際プレイヤー創出に関わる政策として、サイバーセキュリティ製品の有効性を検証する検証基盤の整備を進めている。2020 年度は IPA を通じて、2019 年 9 月に設置した「サイバーセキュリティ検証基盤構築に向けた有識者会議」を非公開で 6 回開催し、検証基盤の構築・運用やスタートアップ等ベンダの市場参入支援の仕組みについて検討した※60。公募によって検証の対象とする 2 製品を選定し、検証を実施したほか、2020 年 4 月に公開した「試行導入・導入実績公表の手引き※61」について、ユーザ企業 2 社へのインタビュー調査等を基に改良を実施した※62。

経済産業省はまた、IoT 機器のセキュリティ検証サービスの高度化を目的に、2021 年 4 月「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き※63」を公開した。本手引きは、「機器のセキュリティ検証において検証サービス事業者が実施すべき事項」「より良い検証サービスを受けるために検証依頼者が実施すべき事項及び持つべき知識」「検証サービス事業者・検証依頼者間の適切なコミュニケーションのために二者間で共有すべき情報や留意すべき事項」を整理したものである。本手引きが検証サービス事業者及び依頼者に活用されることで、国内の検証サービスの水準向上や、適切な検証体制の構築が期待される。

更に IPA を通じて、2018 年 6 月から、サイバー・フィジカル・セキュリティに関する情報交流の場として「コラボレーション・プラットフォーム」を設置し、2020 年度も継続した※64。同プラットフォームは、毎回テーマを変えて資格を限定せずに参加を募り、講演や議論を通じてサイバーセキュリティ対策のニーズを明確化・具体化するとともに、シーズに関する情報提供・情報収集等を行うことで、政策等への意見反映や企業間のマッチングを図っている。2020 年度はオンライン形式で 4 回実施し、計約 450 人が参加した。

(2) その他の検討会等における活動

ここでは、主に AI・データ利活用及び DX（デジタルトランスフォーメーション）推進におけるセキュリティ及び情報システム・モデル取引・契約書の改定について述べる。

経済産業省は「AI 人材育成のための企業間データ提供促進検討会」を開催し、三者以上の間でデータの授受がある場合の AI 関連実務の課題について整理した「AI・データサイエンス人材育成に向けたデータ提供に関する実務ガイドブック※65」を策定した。また、IoT 推進コンソーシアムのデータ流通促進 WG において、「新たなデータ流通取引に関する検討事例集 第 1 分冊※66」を取りまとめ 2020 年 9 月に公開した。データには個人情報が含まれることが想定され、分野や取り扱うデータの特性に応じた安全・安心なデータ利活用方法を各所で検討している。

また DX 推進において、「Society5.0 時代におけるデジタル・ガバナンス検討会」は 2020 年 11 月、デジタル技術による社会変革を踏まえた経営ビジョンの策定・公表等の経営者に求められる対応を「デジタルガバナンス・コード※67」として取りまとめた。同時に「デジタルガバナンス・コード」に基づいた対応を実施した企業を審査・認定し、企業名をリスト化・公表する「DX 認定※68」制度の運用も開始した。本制度の認定基準の一つにサイバー

セキュリティ対策の推進があり、本項で述べた「サイバーセキュリティ経営ガイドライン」や「SECURITY ACTION制度」（「2.4.2（3）（c）SECURITY ACTION」参照）に基づいた対策を実施していることが要件となった。その他、IoT推進コンソーシアムのデータ流通促進WGのもとに設置された「企業のプライバシーガバナンスモデル検討会」は、2020年8月、「DX時代における企業のプライバシーガバナンスガイドブックver1.0※69」を策定した。

更に経済産業省はIPAを通じ、2020年12月22日、「情報システム・モデル取引・契約書」第二版を公開した※70。同モデル契約は、2020年4月に施行された改正民法に直接関係する論点を見直した「『情報システム・モデル取引・契約書』の民法改正を踏まえた見直し整理反映版」（2019年12月発行）に、民法改正に直接関わらない論点の見直しを加えたものである。このうちセキュリティについては、「ユーザとベンダとは、それぞれの立場に応じて必要な情報を示しつつ、リスクやコスト等について相互に協議することにより、システムに実装する『セキュリティ仕様』を決めることが必要である」との観点から見直された。また、ユーザとベンダのセキュリティリスク認識のすり合わせに資するセキュリティ仕様作成のための関連文書を同時に公開した※71。

（3）技術等情報管理認証制度の開始

2018年5月「産業競争力強化法等の一部を改正する法律」に基づき、同年9月から「技術等情報管理認証制度※72」を開始した。これは、企業の技術等の情報管理について、国が示す認証基準に適合していることを、事業所管大臣及び経済産業大臣が認定した認証機関から認証を受けられる制度である。認証機関に対する支援措置として、独立行政法人中小企業基盤整備機構やIPAからの情報提供支援があり、2021年3月現在6事業者が認定を受けている。認証を取得しようとする企業・団体に対しては、経済産業省が専門家を派遣して認証取得申請の支援を行う事業を行っており、2020年度は2020年10月～2021年3月の期間に実施した※73。

（4）情報セキュリティサービス審査登録制度

情報セキュリティサービスを安心して活用できる環境を醸成するべく、経済産業省は「情報セキュリティサービス基準」（以下、本サービス基準）及び「情報セキュリティサービスに関する審査登録機関基準」を策定し、2018年2月に公表した※74。本サービス基準は、情報セキュリティサービスについて一定の品質の維持・向上が図られているか否かを第三者が客観的に判断し、結果を公開することで、利用者が必要なセキュリティサービスを容易に選定できるようにする枠組みである。

IPAはこの枠組みに基づき、2018年7月から、審査登録機関※75による審査の結果、本サービス基準に適合すると認められ、当該機関の登録台帳に登録され、かつIPAに誓約書を提出した事業者の情報セキュリティサービスを「情報セキュリティサービス基準適合サービスリスト」（以下、本リスト）として公開している※76。また、2021年2月からは、本リスト利用者がサービスを選定する際の参考となるよう、サービスのホームページへのリンク、サービスの概要、主たる対象顧客の分野・業種、対象とする地域の情報を本リストに追加し、提供している。

本サービス基準では、情報セキュリティサービスを以下の四つに分類しており、これらのサービス登録数の合計は2021年4月に234件に達した。

- 情報セキュリティ監査サービス
- 脆弱性診断サービス
- デジタル・フォレンジックサービス
- セキュリティ監視・運用サービス

なお、本リストは、「政府機関等の対策基準策定のためのガイドライン※77」において、監査業務の外部委託先を選定する際に活用できるよう参照されている。また、本リストの「情報セキュリティ監査サービス」に掲載されているサービスを提供する監査機関であることは、「政府情報システムのためのセキュリティ評価制度（ISMAP）」において、評価を実施する監査機関の登録申請における要求事項の一つとなっている（「2.6.3 政府情報システムのためのセキュリティ評価制度（ISMAP）」参照）。

今後、本リストの活用が進むことで、情報セキュリティサービスの品質の維持・向上に加え、情報セキュリティサービス市場の活性化にもつながることが期待される。

（5）J-CSIP（サイバー情報共有イニシアティブ）

経済産業省の協力のもと、IPAでは2011年10月から、官民連携による標的型攻撃への対策を目的として、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）を運用している。

J-CSIPは、日本の基幹産業を担う企業を中心に、サイバー攻撃等に関する情報を相互に共有し、サイバー攻撃の防御とその被害の低減を目指している。2021年3月末日現在、IPAを情報の中継・集約点（情報ハブ）

として 15 の業界から 275 の企業や業界団体（以下、組織）が J-CSIP に参加している。

参加の形態としては、IPA と各組織との間で個別に NDA（Non-Disclosure Agreement：秘密保持契約）を締結して情報共有を行う業界単位のグループ（SIG※78）と、規約を基に業界の情報共有活動を支援するための枠組みである「情報連携体制」が存在する（図 2-1-4）。

また、J-CSIP は IPA を通じて、経済産業省やセプターカウンシルの C⁴TAP、JPCERT/CC 等とも連携している。

J-CSIP では、IPA と参加組織との間でサイバー攻撃に関する手口や被害の情報、標的型攻撃メール等に関する情報共有を行っている。なお、J-CSIP の中で共有される情報は、提供元が明らかにならないよう、情報提供者の固有の情報を除去するルールがある。

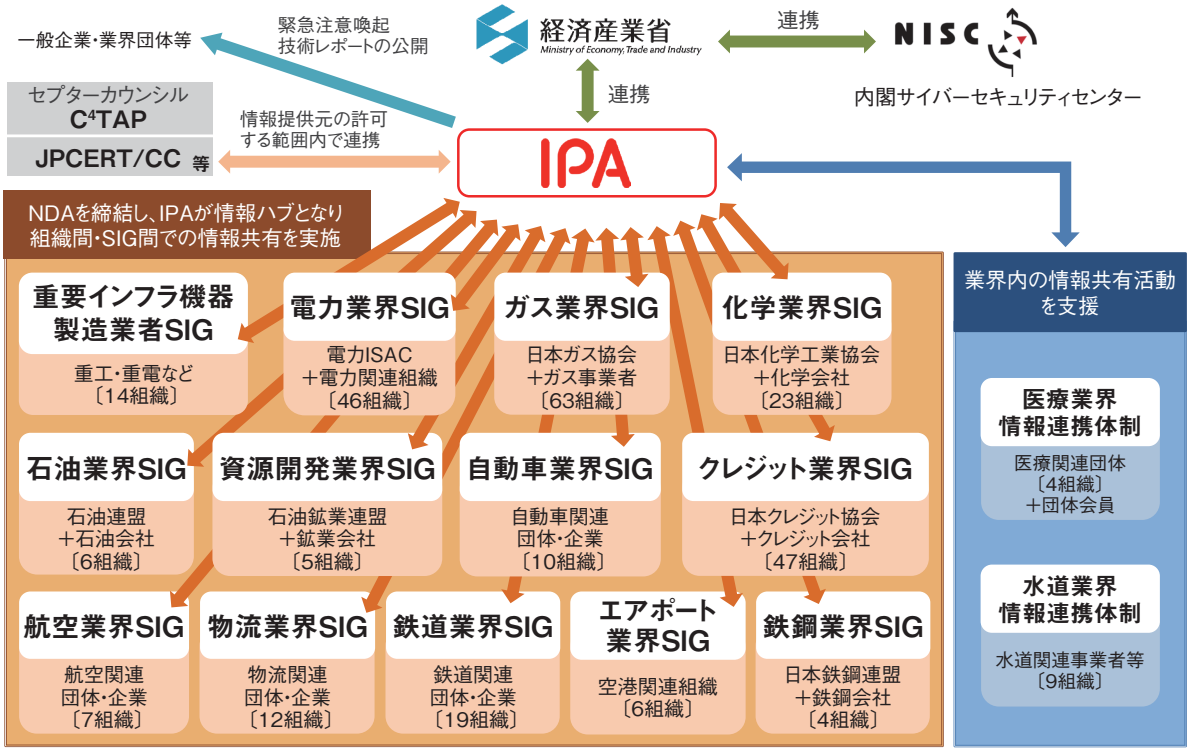
参加組織から提供された、不審なメール、ウイルス※80、攻撃の痕跡等の件数（情報提供件数）、提供を受けた情報のうち標的型攻撃メールと見なした件数（攻撃メール件数）、及びそれらを基に J-CSIP 内で情報共有を行った件数（情報共有件数）を表 2-1-1 に示す。年度により件数の増減はあるものの、継続して情報提供や共有が行われていることが分かる。

2020 年度の情報提供件数が大幅に増加しているが、これは「Emotet」と呼ばれるウイルスへの感染を狙うメールが一時的に大量にばらまかれ、その情報が提供されたことによる。具体的には、2020 年 7 月と 9 月、日本の利用者に対して Emotet のばらまき型メールが多数着信し、この時期だけで約 4,700 件の情報提供があった。

	2017 年度	2018 年度	2019 年度	2020 年度
参加組織からの情報提供件数	3,456 件	2,020 件	2,303 件	6,202 件
攻撃メール件数	274 件	213 件	401 件	125 件
情報共有件数	242 件	195 件	225 件	147 件

■表 2-1-1　J-CSIP の運用実績

J-CSIP では、無作為に送信されるような不審メールやウイルスメール（ばらまき型メール）については、一般的に脅威の度合いが低いと考えられることから、原則として情報の提供依頼や共有の対象とはしていない。しかし、Emotet については、無作為に近い攻撃でありながらも、窃取した正規メールの文面の流用、パスワード付き ZIP ファイルの悪用といった手口が駆使され、多数の企業・組織にとって深刻な脅威であると見なせる状況であった（「1.2.6 (1) (a) Emotet」参照）。このことから、特に攻撃手口等に大きな変化が確認できた際は、情報共有の対象とし、各組織による対応を促した※81。ばらまき型メールと見なせる攻撃であっても、かつて標的型攻撃で使わ



■図 2-1-4　J-CSIP の体制全体図
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2021 年 1 月～ 3 月］※79」

れていたような巧妙な手口が取り入れられている傾向があり、状況に応じ、今後とも情報共有を図っていく必要があると思われる。

ビジネスメール詐欺に関しては、2019 年度までと同様、多くの情報提供を受けた。実被害に至る前に偽のメールであることに気付けた事例もあれば、攻撃者の口座へ送金してしまった事例もあった。企業間の取り引きのメールに介入したり、CEO（Chief Executive Officer：最高経営責任者）になりすましたりする等、基本的な騙しの手口は変わらないが、細部においては、新型コロナウイルスの話題を持ち出すといった変化も見受けられた（「1.2.3 ビジネスメール詐欺（BEC）」参照）。これらの詳しい情報を J-CSIP 内で共有するとともに、情報提供元の許可が得られた範囲で、事例の一般公開も行っている※82。

このほか、最終的に諜報活動を目的とするような標的型攻撃であったのか不明であるが、新型コロナウイルスによる社会情勢悪化を題材とした不審メール、遠隔操作ウイルスへの感染を目的とする日本語の攻撃メール、Zoom ミーティングの招待メールを装うフィッシングメール、そして VPN 製品への攻撃試行といった情報提供があり、それぞれ共有を行った。

全体的には、2016 年度まで観測されてきた、諜報活動が目的と思われる、日本国内の特定の業界や組織に向けて多数のメールが送信されるような標的型攻撃は減少傾向にある。これは、攻撃者がより慎重に、目立たないように攻撃を行うようになったためであると考えられる。また、発端が標的型攻撃メールではなく、他の何らかの方法（VPN 製品への不正アクセス、経路不明等）で組織内ネットワークへ侵入されたという情報提供もあり、攻撃手口は多様化しているものと思われる。

情報共有活動は、攻撃の痕跡や手口の情報を基に、防御側で連携して対抗するための重要な施策の一つであり、IPA は引き続き J-CSIP の運用を継続していく。

(6) J-CRAT（サイバーレスキュー隊）

経済産業省の協力のもと、IPA は 2014 年 7 月に J-CRAT（Cyber Rescue and Advice Team against targeted attack of Japan：サイバーレスキュー隊）を発足させた。J-CRAT の目的を以下に示す。

- 攻撃に気付いた組織に対する被害拡大と再発の抑止・低減
- 標的型攻撃による諜報活動等の連鎖の遮断

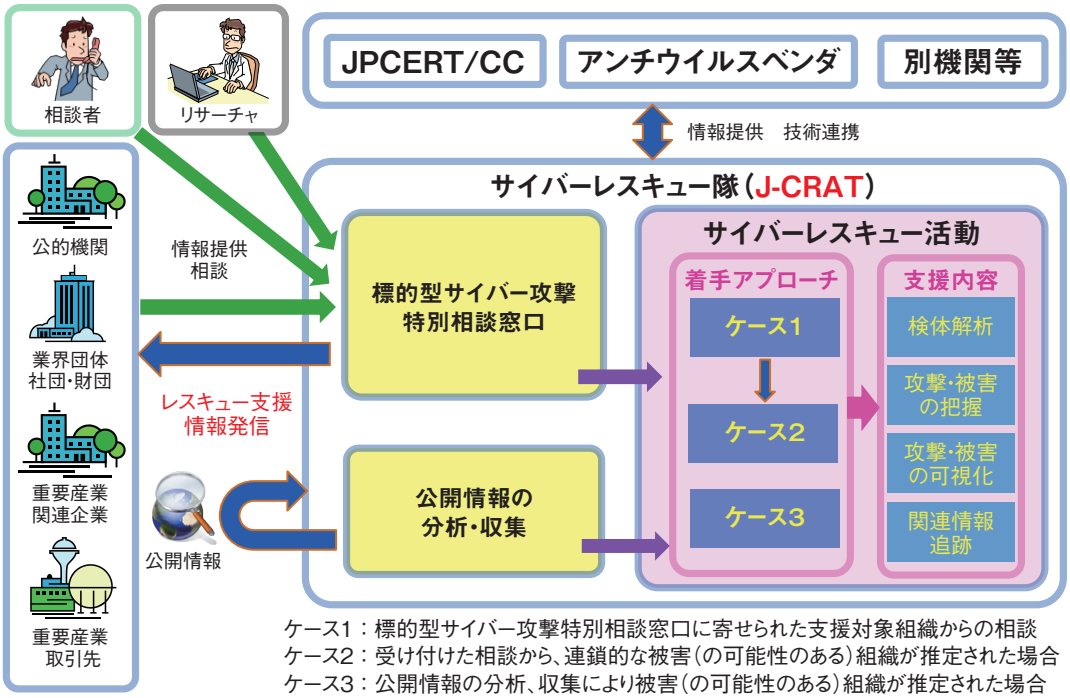
J-CRAT では、常時「標的型サイバー攻撃特別相談窓口」（以下、窓口）の運営と「公開情報の分析・収集」の二つの活動を実施している。

窓口では、主に公的機関等の組織から、標的型攻撃メールに関する情報提供や相談を受け付けている。「公開情報の分析・収集」では、日々公開されるインターネット上の情報等から、各種ウイルス情報等を収集している。これまでの活動実績から、地政学や国際政治、国際経済や科学技術等に関する動向との関連が明らかになったため、それらの情報収集を幅広く行っている。

標的型サイバー攻撃の被害に遭っている、または遭っている可能性が高い組織のうち、特に公的機関や業界団体、重要インフラ関連企業や取引先等サプライチェーンを構成する組織に対して、被害実態の確認と認知の支援、被害緩和の暫定対応における助言を「サイバーレスキュー活動」として実施している※83。また、窓口における対応の結果、必要があると判断した組織に対して、攻撃の期間・内容、感染範囲、想定被害等をヒアリングし、早急な対策着手が行えるよう、民間セキュリティ事業者への移行を前提とした助言を行っている（次ページ図 2-1-5）。

相談を受けた案件のうち、緊急を要する事案に対しては、「レスキュー支援」を行い、更に当該組織での対応が必要な場合は、隊員を派遣する「オンサイト支援」を行っている。それぞれの支援件数を表 2-1-2（次ページ）に示す。2020 年度の活動実績を 2019 年度と比較すると、「相談件数」は 3.6% 増加しており、内訳を見ると「レスキュー支援件数」が 26.6% 減少、「オンサイト支援件数」も 15.0% 減少している。

J-CRAT では、定期的に活動状況を公開するほか、情報収集活動や支援活動から得られた結果を技術レポートとして随時公開している。これらの取り組み等を通じ、被害組織におけるセキュリティインシデントに対する速やかな対応力向上や、平時における標的型攻撃への対策力向上に資する活動を行っている。また、活動を通じて組織のセキュリティ人材の育成、標的型サイバー攻撃の連鎖の解明、及び攻撃の連鎖を遮断することによる被害の低減を推進していく。



■図 2-1-5　J-CRAT の活動の全体像とスキーム
（出典）IPA「サイバーレスキュー隊 J-CRAT（ジェイ・クラート）※83」

	2017 年度	2018 年度	2019 年度	2020 年度
相談件数	412 件	413 件	392 件	406 件
レスキュー支援件数	144 件	127 件	139 件	102 件
オンサイト支援件数※	27 件	31 件	20 件	17 件

※一つの事案に対しての複数回のオンサイト対応を要した場合も、1 件として集計

■表 2-1-2　J-CRAT の活動実績

2.1.3 総務省の政策

総務省は、IoT 機器を踏み台としたサイバー攻撃等が深刻化している状況を踏まえ、サイバーセキュリティタスクフォース※84 が 2019 年 8 月に取りまとめた「IoT・5G セキュリティ総合対策※85」の改訂版として、2020 年 7 月に「IoT・5G セキュリティ総合対策 2020※86」（以下、総合対策 2020）を策定・公表した。総合対策 2020 には、新型コロナウイルス感染拡大に伴うテレワークの普及、及び本格的に稼働する 5G へのセキュリティ対策が盛り込まれた。

以下では、総合対策 2020 に示された総務省の主な取り組みの状況を述べる。また、テレワークにおけるセキュリティ確保のために実施している様々な取り組みについても述べる。

(1)「IoT・5G セキュリティ総合対策 2020」の概要

総合対策 2020 を基に、IoT・5G 時代においてセキュリティを確保するための政策課題と取り組み状況を述べる。

(a) クラウドのセキュリティ対策強化

新型コロナウイルス感染拡大防止のための緊急対策として、準備期間が十分とれずにテレワークを導入した企業等も多かったものと思われる。

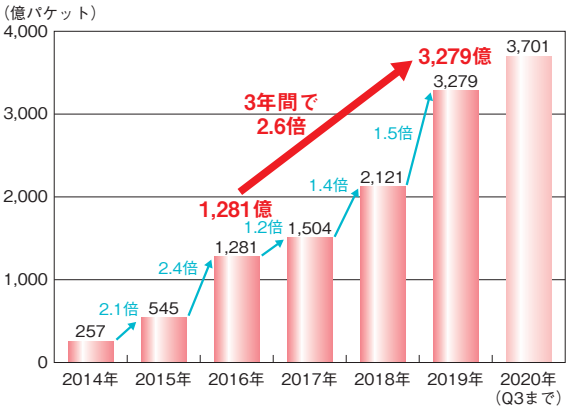
テレワーク中の情報共有や Web 会議システムの利用のため、クラウドサービスの利用も増加した※87。総合対策 2020 では、今後も組織における情報システムの構築や運用においてクラウドサービスの活用が進むことを指摘している。政府においても「政府情報システムにおけるクラウドサービスの利用に係る基本方針※88」を定め、情報システム調達に際しては、コスト削減や柔軟なリソースの増減等の観点から、クラウドサービスの利用を第一候補として検討を行う旨の方向性が示されている。

このような状況を踏まえ、現在、政府機関等の情報システムにおけるクラウドサービスの調達に関しては、「政府情報システムのためのセキュリティ評価制度（ISMAP）」の運用が開始されている※89（「2.6.3 政府情報システムのためのセキュリティ評価制度（ISMAP）」参

照）。クラウドサービスのセキュリティについては、既存の様々な認証・認定制度が存在しており、これらを利用者・調達者が積極的に参照していくことが期待されている。

(b) IoT のセキュリティ対策

NICT の観測によれば、IoT 機器を狙った攻撃は 2016 年の 1,281 億件から、3 年後の 2019 年には 3,279 億件と約 2.6 倍に増加している（図 2-1-6）。2020 年は第 3 四半期で、3,701 億件と 2019 年 1 年間の実績を既に上回っており、攻撃が更に増加していることがうかがえる。これまでの IoT のセキュリティ対策は IoT 機器の機能要件の設定や、パスワードの設定等に不備のある IoT 機器等の調査及び注意喚起の実施等、IoT 機器に対する対策が中心であった。しかし、総合対策 2020 によれば、対策をより実効的にするためには、サイバー攻撃が通過するネットワーク側で、より機動的な対処を行う環境整備が必要と考えられるという。



■図 2-1-6　IoT 機器を狙った攻撃の増加（NICTER により 1 年間に観測されたサイバー攻撃回数）
（出典）サイバーセキュリティタスクフォース事務局「サイバー攻撃の最近の動向について※90」を基に IPA が編集

2018 年 5 月に成立した「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」により一部改正された「電気通信事業法」に基づき、2019 年 2 月より総務省、NICT 及び電気通信事業者（ISP：Internet Services Provider）が連携し、IoT 機器へのアクセスによる、サイバー攻撃に悪用される恐れのある機器の調査及び当該機器の利用者への注意喚起を行う取り組み「NOTICE※91」が実施されており、2020 年は取り組みが更に強化されている（「3.2.4 (2) IoT 機器調査及び利用者への注意喚起の取り組みの強化」参照）※92。

また、2019 年 6 月より、ウイルスに感染している IoT 機器を NICT の「NICTER（Network Incident analysis Center for Tactical Emergency Response）」プロジェクトで得られた情報を基に特定し、ISP を通じて利用者へ注意喚起を行う取り組みも NOTICE とは別に実施されている。NICTER 観測レポート 2020※93 によると、NICTER プロジェクトの大規模サイバー攻撃観測網で 2020 年に観測されたサイバー攻撃関連通信は、2019 年と比べて約 1.5 倍と、2019 年と同様の増加傾向にあるという。

今後はこれらの注意喚起の取り組みを引き続き実施するとともに、取り組みに参加する ISP の拡大を図り、脆弱な状態にある IoT 機器を増やさないよう積極的に働きかけることが総合対策 2020 に盛り込まれている。なお、IoT のセキュリティ対策については「3.2.4 セキュリティ対策強化の取り組み」も参照されたい。

(c) 5G の本格開始に伴うセキュリティ対策の強化

5G の本格開始により、MEC※94 の活用に加え、ネットワーク機能の仮想化・ソフトウェア化等が一層進むことが想定されている。このため、総合対策 2020 では、サイバーセキュリティの観点からは、ソフトウェアを始めとするサプライチェーンリスクへの対応が不可欠であるとしている。また 5G のセキュリティの観点からは、ハードウェア・ソフトウェアの両面で脆弱性の検証手法等を確立することが必要であるとしている。

一方、5G の脆弱性の検証と合わせ、5G のネットワークを運用する事業者やベンダ、利用者等の間での脆弱性情報や脅威情報、更にこれらの対処に関する情報の共有が重視されている。2020 年 2 月、一般社団法人 ICT-ISAC で「5G セキュリティ推進グループ」が設立され※95、それらの民間の取り組みを踏まえつつ、引き続き、情報共有の促進が必要であるとしている。

具体的な施策として、5G の安全性・信頼性を確保しつつその適切な開発供給及び導入を促進することを目的に、全国 5G 及びローカル 5G※96 の導入事業者に対する税制優遇措置や導入事業者及び開発供給事業者に対する金融支援を盛り込んだ「特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律」が 2020 年 5 月に成立した※97。同法によれば、全国 5G では、携帯電話事業者に対して第 5 世代移動通信システム導入のための特定基地局の開設計画の認定において、サプライチェーンリスク対応を含む十分なサイバーセキュリティ対策を講ずることを条件としている。一方、ローカル 5G では、「ローカル 5G 導入に関するガイドライン※98」において、サプライチェーンリスク対応を含

む十分なサイバーセキュリティ対策を講じる旨を明記するとともに、それをローカル 5G の免許申請時の条件としている。

(d)研究開発や人材育成等の横断的施策

総合対策 2020 では、横断的施策として、研究開発の推進、人材育成の推進、国際連携の推進等が掲げられている。以下にそれぞれの概要を述べる。

- 研究開発の推進

  AI の進展や計算能力の向上等により攻撃手法・能力が巧妙化・大規模化する中、サイバーセキュリティに関する研究開発が重要な政策課題と位置付けられている。2020 年 12 月、NICT、学校法人慶應義塾(慶應大学)、株式会社三菱 UFJ フィナンシャル・グループ、株式会社みずほフィナンシャルグループは、超電導量子コンピュータ IBM Quantum を用いた離散対数問題の求解実験に成功した※99。これにより現在用いられている暗号技術の危殆化時期の見積り精度が向上し、暗号技術の安全性が高まる可能性があることが示唆されている。

- 人材育成オープンプラットフォームの構築

  NICT は、2021 年 2 月「サイバーセキュリティ統合知的・人材育成基盤 CYNEX(Cybersecurity Nexus:サイネックス)」構築の計画を明らかにした。NICT で実施してきた研究開発や人材育成の取り組みの知見を活用し、サイバーセキュリティ情報を国内で収集・分析・提供するとともに、社会全体でサイバーセキュリティ人材育成をするための共通基盤を構築し、産学官の結節点として開放することでサイバーセキュリティ対応能力の向上を図るとしている(図 2-1-7)。今後、人材育成オープンプラットフォームとして産学へ開放され、人材育成のコミュニティの形成やパイロットコンテンツ開発並びに利用が進むことが期待される。

- 地域のセキュリティ人材育成

  サイバーセキュリティ人材の育成は重要な政策課題となっているが、特に都市以外の地域において人材の確保が一層厳しい状況にある。そのため、地域においてセキュリティを地場産業化しようとしている民間企業等と総務省が連携し、地域における人材エコシステムを形成する取り組みが進められている。

- 国際連携の推進

  国境を越えて行われるサイバー攻撃についても、脅威情報等の国際的な共有により、早期の攻撃挙動等の把握が必要不可欠である。そのため、産業分野別の脅威情報等の共有・分析組織である ISAC(Information Sharing and Analysis Center)にお

■図 2-1-7　サイバーセキュリティ統合知的・人材育成基盤 CYNEX の構築
(出典)NICT「サイバーセキュリティ統合知的・人材育成基盤 CYNEX(サイネックス)の構築について※100」

いて、国際的なISAC間等の連携を引き続き促進していく必要がある。また、政府はサイバー空間における国際ルールをめぐる議論へも積極的に参加していく必要がある。

一方、政策面の国際連携としては、ASEANにおけるセキュリティ政策支援を協議する「日・ASEANサイバーセキュリティ政策会議」が2020年10月にオンラインで開催され、共同サイバー演習、共同意識啓発、能力構築及びインシデントの相互通知等の協力活動の確認・評価が行われた※101（「2.2.1（3）（a）日・ASEANサイバーセキュリティ政策会議」参照）。

(2) テレワークにおけるセキュリティ確保

テレワークはワークライフバランスの実現、人口減少時代における労働力人口の確保、地域の活性化等へも寄与する。総務省では、関係省庁と連携し、働き方改革実現の切り札として、テレワークの普及促進に資する様々な取り組みを進めてきた※102。更に2020年は新型コロナウイルス対策としてテレワークの積極的な活用を推し進めた※103。ここでは、総務省のテレワークにおけるセキュリティ確保の取り組みについて説明する。なお、テレワークのセキュリティの実態については「3.3 テレワークの情報セキュリティ」を参照されたい。

(a)「テレワークのセキュリティ あんしん無料相談窓口」の開設

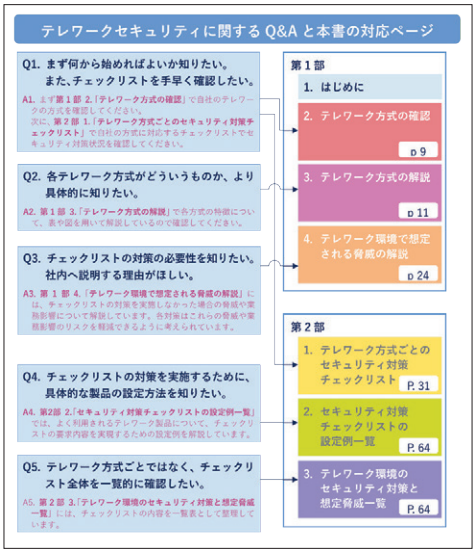
総務省はテレワーク導入の無料相談ができる「テレワークマネージャー派遣事業」（現、テレワークマネージャー相談事業）を2016年8月から実施してきた※104。2020年はテレワークの導入企業が増えたため、テレワークセキュリティについて相談対応体制を強化する目的で、同年7月に「テレワークのセキュリティ あんしん無料相談窓口」を開設した※105。セキュリティに関する不安、具体的なセキュリティ対策方法、ルール作りや自社の実施状況の適切性のコンサルティング等を、セキュリティの専門家がWebオンライン会議等でアドバイスする。

(b)「テレワークセキュリティガイドライン」の改訂

総務省は、企業等がテレワークを実施する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するため、2004年にセキュリティ対策についての考え方や対策例を示した「テレワークセキュリティガイドライン（初版）」を策定・公表した。2021年2月には、全面的な改訂となる第5版の案を公開した※106。本ガイドラインは、テレワークの活用が進む中、情報セキュリティ対策検討の参考となるよう策定されており、企業に所属しない個人事業主だけでなく、企業の経営者やシステム管理者向けに具体的な対策の考え方を紹介している。

(c)「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（初版）」の公表

総務省は2020年9月、セキュリティの専任担当がいないような中小企業等のシステム担当者を対象として、テレワークを実施する際に最低限のセキュリティを確実に確保するための手引き「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（初版）※107」を作成・公表した※108（図2-1-8）。今後は、より分かりやすい手引きの作成を行うとともに、設定解説資料※109等の対象製品を増やしていく予定としている。

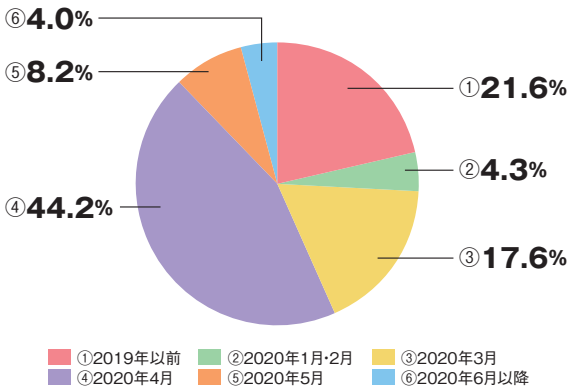


■図2-1-8　テレワークセキュリティに関するQ&Aと対応ページ
（出典）総務省「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（初版）」

(d)「テレワークセキュリティに係る実態調査」の実施

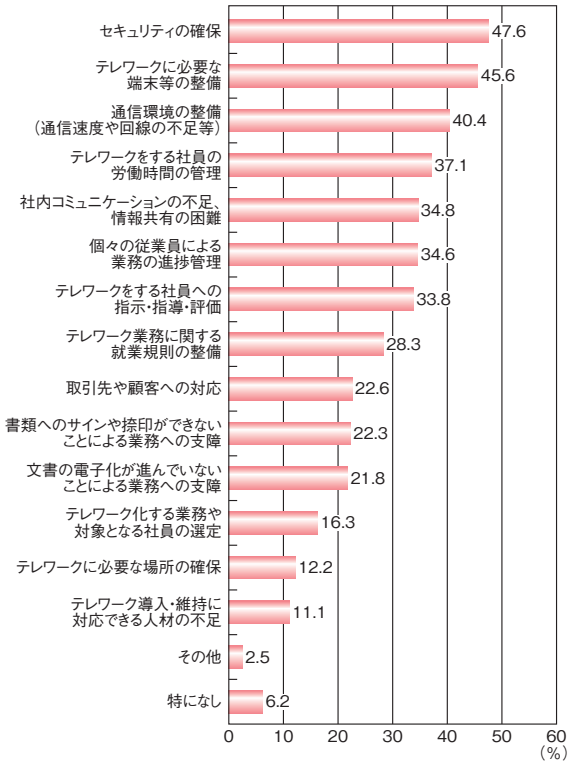
総務省は、2020年7～8月及び2020年12月～2021年1月の2度にわたり、テレワークを導入する企業等におけるセキュリティ対策状況の実態を把握するため「テレワークセキュリティに係る実態調査」を実施した（以下、それぞれを1次実態調査及び2次実態調査と呼ぶ）※110。1次実態調査の結果によると、テレワーク導入企業の過半が1回目の緊急事態宣言前後（2020年3～4月）に導入していることが分かった（次ページ図2-1-9）。また、テレワークを導入しない理由として、業務都合を除くとセキュリティに関する懸念がトップであった。総務省の「テレワークセキュリティガイドライン」について

は、認知度は 2 割弱にとどまった。対策状況については、情報セキュリティポリシーを策定している企業は約 3 分の 1 にとどまり、「セキュリティ対策ソフト」が常に最新になるように指示・設定している企業も 3 分の 2 にとどまった。



■図 2-1-9　テレワークの導入時期（n=1,569）
（出典）総務省「テレワークセキュリティに係る実態調査（1次実態調査）報告書[※111]」を基に IPA が編集

一方、2 次実態調査の結果によると、導入にあたっては、約半数近くの企業が「情報セキュリティの確保」が課題と感じているという調査結果（図 2-1-10）もあり、より一層のセキュリティ確保が必要となるとしている[※112]。



■図 2-1-10　テレワークの導入に当たり課題となった点（複数回答可、n=1,996）
（出典）総務省「テレワークセキュリティに係る実態調査（2次実態調査）報告書[※112]」を基に IPA が編集

(3) その他の取り組み

総務省のその他の取り組みについて述べる。

(a) 自治体情報セキュリティ対策

総務省は、2019 年 12 月より開催してきた「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会[※113]」で取りまとめた見直し内容を踏まえ、2020 年 12 月に「地方公共団体における情報セキュリティポリシーに関するガイドライン[※114]」及び「地方公共団体における情報セキュリティ監査に関するガイドライン[※115]」の改定を公表した。これらのガイドラインは、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考となるように、情報セキュリティポリシーの考え方や内容を解説している。具体的には、これまで「三層の対策」と呼ばれるマイナンバー利用事務系、LGWAN 接続系、インターネット接続系で分離構成した自治体強靭化モデルを見直し、効率性・利便性を向上させた新たな自治体情報セキュリティ対策等を盛り込んだ。新たな情報機器、サービス及び脅威等に対応した情報セキュリティ対策を追加しており、情報セキュリティポリシーの評価・見直しを行う際にも、本ガイドラインの活用が期待される。

(b) トラストサービス制度

Society 5.0 の実現に向けて、サイバー空間の自由で安心・安全なデータの流通を実現するためには、データの信頼性を確保する仕組みとして、トラストサービスが不可欠である。そのため、総務省が開催する「プラットフォームサービスに関する研究会」では、2019 年 1 月からトラストサービス[※116]に関する現状や課題について検討し、2020 年 2 月に最終報告を取りまとめた[※117]。報告書では、トラストサービスの制度的な枠組みの形成に向けた取り組みを一層加速する必要があるとしている。

また、総務省は 2020 年 4 月、「組織が発行するデータの信頼性を確保する制度に関する検討会[※118]」を発足し、トラストサービスの一つである組織が発行するデータの信頼性を確保する仕組み（通称、e シール）について、国際的な動向を踏まえつつ検討を実施している。

更に、総務省は 2020 年 3 月に、ある時刻にその電子データが存在していたことと、それ以降改ざんされていないことを証明するタイムスタンプ技術の認定制度の検討を開始した。検討では、従来の「タイムビジネス信頼・安心認定制度」における認定の対象や基準、期間及び認定にあたっての調査期間の要件、調査・監査の在り

方等の課題を踏まえ、国によるタイムスタンプ認定の方向性を取りまとめた。本制度は 2021 年 4 月に公布・施行されている※119。

(c) スマートシティのセキュリティ対策

総務省は 2020 年 10 月に、安心・安全なスマートシティの構築・運営に資するため、スマートシティのセキュリティの考え方やセキュリティ対策に関するガイドライン「スマートシティセキュリティガイドライン（第 1.0 版）※120」を発行した。本ガイドラインではスマートシティ特有の構造に関連して、特有のセキュリティ留意点を記載し、それぞれの留意点について起こり得る問題や対策の方向性を整理している。

(d) インターネット上の違法・有害情報への対応

総務省は、インターネット上の違法・有害情報に対して、情報による人権侵害等の被害の救済と表現の自由という重要な権利・利益のバランスに配慮しつつ、プロバイダの円滑な対応が促進されるような環境整備を行っている※121。2020 年度は、デマやフェイクニュースの実態を把握する目的で「新型コロナウイルス感染症に関する情報流通調査」「日本におけるフェイクニュースの実態等に関する調査研究」を実施し、結果を公表した※122（「2.7.2 With コロナにおける普及啓発活動」参照）。

また、「発信者情報開示の在り方に関する研究会」の最終結果を取りまとめ、インターネット上の誹謗中傷対策に乗り出した。更に、関係省庁や産学民のステークホルダーと連携して早急に対応していくべき取り組みについて具体化を図るため、2020 年 9 月「インターネット上の誹謗中傷への対応に関する政策パッケージ」を公開した※123（「2.7.1 (2) ネット上の誹謗中傷への対策」参照）。

2.1.4 警察によるサイバー犯罪対策

警察庁では、サイバーセキュリティ戦略※124 を踏まえ、2018 年 9 月、「サイバーセキュリティ重点施策」を改訂し※125、サイバー空間の脅威への対処に関する取り組みを推進している※126。

本項では、2020 年度の警察におけるサイバーセキュリティ重点施策への取り組み状況及びサイバー犯罪の情勢等について、警察庁の「令和 2 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※127」等に基づいて述べる。

(1) 警察における主な取り組み

「サイバーセキュリティ重点施策」は、「サイバー空間の脅威への対応の強化」「警察における組織基盤の更なる強化」及び「国際連携及び産学官連携の推進」を主な柱としている。これらを踏まえ、2020 年度の警察におけるサイバー犯罪対策の主な取り組みについて述べる。

(a) サイバー空間の脅威への対応の強化

警察庁の「令和 2 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」によれば、2020 年は、テレワークの積極的な実施やキャッシュレス決済の普及等、サイバー空間が日常の活動と密接になりつつある中、手口が深刻化・巧妙化したサイバー攻撃やサイバー犯罪が国内外で多数発生し、サイバー空間における脅威は極めて深刻な情勢にあるという。

これに対し警察は、新型コロナウイルスワクチン開発に関連した製薬事業者等へのサイバー攻撃に関する注意喚起のほか、重要インフラ事業者等に対する Web 会議システムの脆弱性に関する注意喚起や、IT インフラ管理ソフトウェアの脆弱性に関する注意喚起等を実施した※128。

また、東京 2020 オリンピック・パラリンピック競技大会関連事業者等との間では、サイバー攻撃の発生を想定した共同対処訓練を実施（2020 年 7 月滋賀県警察※129、12 月富山・愛知県警察※130、2021 年 1 月青森県警察※131 等）し、対処能力の強化を図った。

また警察は、サイバー攻撃事案で使用された不正プログラムの解析等を通じて把握した国内 C&C（Command and Control）サーバの機能停止（テイクダウン）を、サーバを運営する事業者等に働きかけることによって促進している。警察が把握した C&C サーバの運営事業者に対し、不正な蔵置ファイルの削除を依頼する等により、C&C サーバの無害化措置が実施された結果、2020 年中に 89 台の機能が停止した。

その他、情報セキュリティに関する動画等※132 による情報発信、金融庁との連携によるスマートフォン決済サービスを利用した不正振替事犯の手口に関する注意喚起※133、金融機関等への本人確認徹底等の対策状況の確認や対策強化の働きかけ等を実施した。

関係事業者等との連携では、富山県警察は新型コロナウイルス感染症指定医療機関等との連携強化を実施した。また宮城県警察は、宮城県と協力して重要インフラ事業者、民間企業・団体、サイバー関連事業者、教育機関等合計 118 事業者からなるサイバーセキュリティ

協議会を発足させ、サイバーセキュリティに強い地域社会づくりを推進してきている※134。

(b) 警察における組織基盤の更なる強化

警察では、サイバー空間の脅威への対処に関する人材基盤を強化するため、サイバー犯罪・サイバー攻撃の捜査及び情報通信技術に関する知識等を有する人材の育成を推進している。2019年、警察庁において、サイバー犯罪等対処能力検定の初級に全警察官を合格させる等、警察全体で計画的な人材育成を推進するための「サイバー空間の脅威への対処に関する人材の育成計画」を策定、これを踏まえ、都道府県警察において実情に沿った育成計画の策定または見直しが指示された※135。

2020年度は、警察庁においても、サイバー犯罪・サイバー攻撃に対処する捜査員及び情報技術の解析に従事する職員の能力の更なる向上が図られた※136。

(c) 国際連携及び産学官連携の推進

国際連携については、情報技術解析（デジタルフォレンジック等）※137に関する専門的な国際会議における発表・議論、外国治安機関等との実務者会合を通じて、警察庁として技術情報の収集や各国の法執行機関等との連携の深化に努め、更なる対処能力の強化を図っている※138。

また警察での産学官連携の推進については、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）等と連携し、産学官の情報や知見をサイバー犯罪・サイバー攻撃の取り締り等に活用している。具体的には、総務省を装った偽の特別定額給付金の申請サイトへ誘導するメールに関する注意喚起※139、山形県警察によるサポート詐欺サイトでの被害発生を受けての注意喚起※140、愛知県警察、埼玉県警察によるネットショッピングに関する詐欺サイトの被害防止対策等の活動に取り組んでいる。

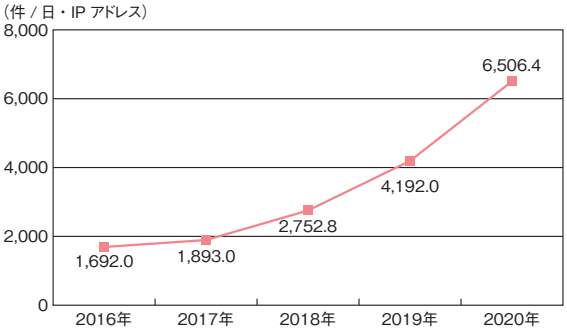
また警察庁のサイバーセキュリティ・情報化審議官主催の私的懇談会として、法務、技術、ITの各分野及びJC3等の官民有識者で構成されるサイバーセキュリティ政策会議が例年開催されている。2020年度の同会議では、警察が、政府全体の力を結集するための施策に安全・安心の観点から積極的・主体的に参画していく必要がある、との提言を含む報告書※141が取りまとめられ、2021年3月、警察庁より公開された。同報告書では「コロナ禍が顕在化させるサイバー空間の新たな脅威」「犯行手口等の悪質化と被害の深刻化」「国家の関与が疑われるサイバー攻撃被害の深刻化」といった生活様式の変化等によるサイバー空間の新たな脅威に対して、新たな基本理念としての「公共空間としての安全性確保」の実現が求められる、としている。

(2) 2020年のサイバー攻撃の情勢

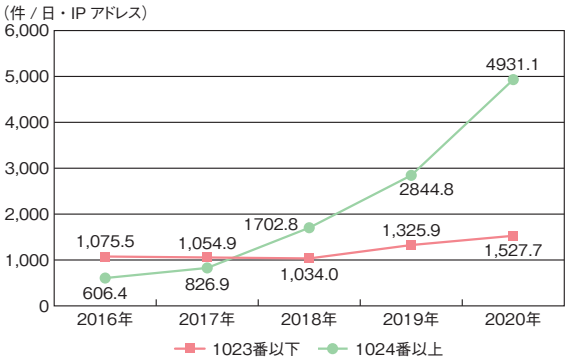
警察が把握する2020年のサイバー攻撃の情勢について述べる。

警察は先端技術を有する全国8,100の事業者等（2021年1月現在）との間で、情報窃取を企図したと見られるサイバー攻撃に関する情報共有の枠組みとして「サイバーインテリジェンス情報共有ネットワーク」を構築している。2020年中にサイバーインテリジェンス情報共有ネットワークを通じて把握した「標的型メール攻撃※142」の件数は4,119件であった。「標的型メール攻撃」のうち、同じ文面や不正プログラムが10ヵ所以上に送付される「ばらまき型」攻撃の割合が、全体の95%を占めていた。

また、警察庁では、インターネットとの接続点にセンサーを設置してリアルタイム検知ネットワークシステム※143を24時間体制で運用し、通常のインターネット利用では想定されない接続情報等を検知、集約・分析している。本システムが検知するアクセスの大半は、不特定多数のIPアドレスを対象とするサイバー攻撃やネットワークに接続された機器の脆弱性を探索するサイバー攻撃の準備行為と見られている。2020年に本システムで検知した不審なアクセス件数は、1日・1IPアドレスあたり6,506.4件と過去5年間で約4倍の増加となっている（図2-1-11）。検知したアクセスの宛先ポートも、主としてIoT機器が標準設定で使用するポート番号1024以上のポートへのアクセス件数が特に増加しており、普及するIoT機器の脆弱性の探索行為であると見られる（次ページ図2-1-12）。なお、脆弱なIoT機器の探索については「3.2.3



■図2-1-11　システムで検知したアクセス件数の推移
（出典）警察庁「令和2年におけるサイバー空間をめぐる脅威の情勢等について」を基にIPAが編集



■図 2-1-12　検知したアクセスの宛先ポートで比較した1日・1IPアドレス当たり件数の推移
(出典)警察庁「令和２年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

脆弱なIoT 機器とウイルス感染の実態」を参照されたい。

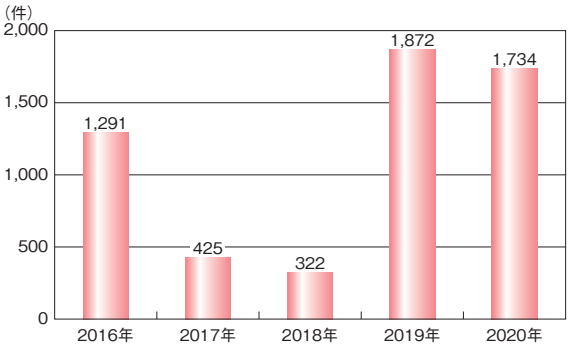
(3) 2020 年のサイバー犯罪の情勢等

警察が 2020 年に認知したサイバー犯罪の情勢等について述べる。

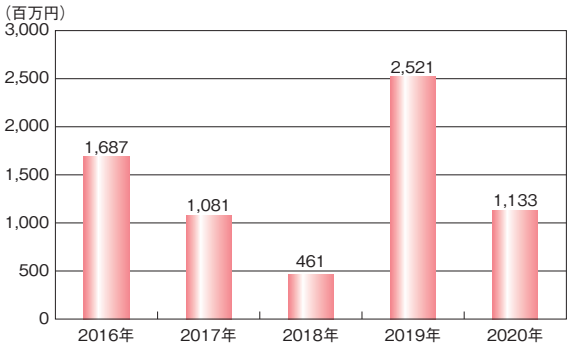
(a) サイバー犯罪の情勢

「インターネットバンキングに係る不正送金事犯」としては、SMS や電子メールを用いて金融機関、宅配事業者、通信販売事業者からの荷物の配達連絡を装ったフィッシングサイトへ誘導する手口が確認されているが、被害が急増した 2019 年と比べて、発生件数、被害額ともに減少した（図 2-1-13、図 2-1-14）。手口と対策の詳細については「1.2.7 個人をターゲットにした騙しの手口」を参照されたい。

2020 年は、社会情勢の変化や国民の不安感等に乗じて、新型コロナウイルスの感染状況やワクチン関連の情報をかたる不審メールや不審サイト、詐欺等の事案が増加した。新型コロナウイルスに関連するサイバー犯



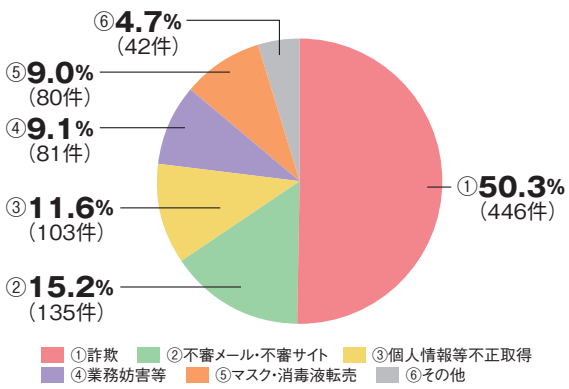
■図 2-1-13　インターネットバンキングに係る不正送金事犯の発生件数の推移
(出典)警察庁「令和２年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集



■図 2-1-14　インターネットバンキングに係る不正送金事犯の被害額の推移
(出典)警察庁「令和２年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

罪が疑われる事案として、都道府県警察から警察庁に報告された件数は 887 件であった（図 2-1-15）。

内訳としては、マスク不足に便乗した詐欺サイト等の「詐欺」が 446 件（50.3%）で半数を占める。次いで偽の給付金の申請サイト等の「不審メール・不審サイト」が 135 件（15.2%）、総務省を名乗り、「2 回目の特別定額給付金を支給する。」という内容のメールが届き、指定された URL にアクセスした結果、カード情報等を窃取された等の「個人情報等不正取得」が 103 件（11.6%）であった。



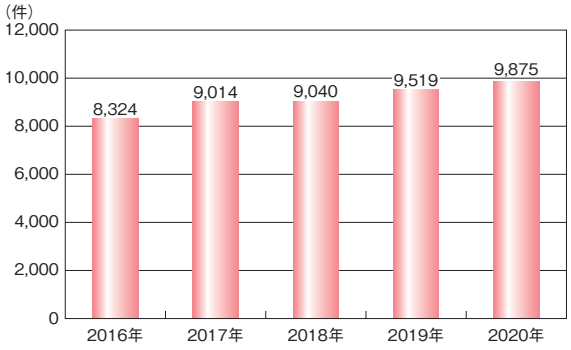
■図 2-1-15　新型コロナウイルスに関連するサイバー犯罪が疑われる事案の報告件数（n=887）
(出典)警察庁「令和２年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

(b) 検挙件数

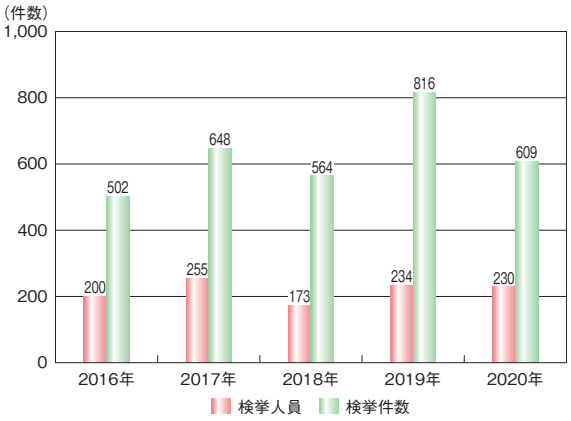
サイバー犯罪の検挙件数と主な事案事例について述べる。警察によれば、サイバー犯罪の検挙件数は増加傾向にあり、2020 年の検挙件数は 9,875 件と過去最多となった（次ページ図 2-1-16）。

その中で「不正アクセス禁止法違反」の検挙件数は 609 件と、前年の 816 件からは減少したものの（次ページ図 2-1-17）、「不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪」の検挙件数は前年

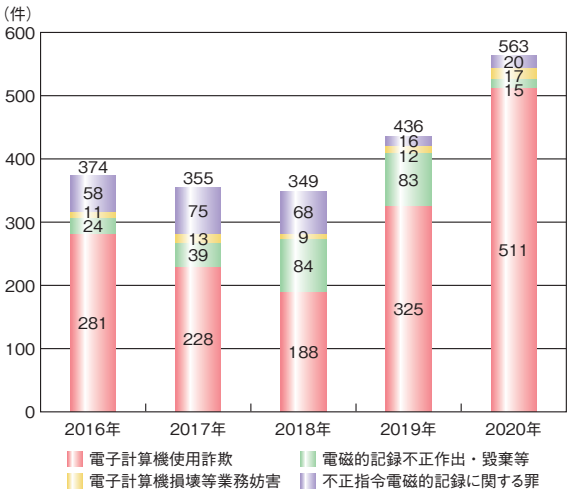
の 436 件を上回り、563 件と過去 5 年間で最多となった。そのうち「電子計算機使用詐欺」が 511 件と最も多く、全体の 90.8% を占めている（図 2-1-18）。



■図 2-1-16　サイバー犯罪の検挙件数の推移
（出典）警察庁「令和 2 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集



■図 2-1-17　不正アクセス禁止法違反の検挙件数の推移
（出典）警察庁「令和 2 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集



■図 2-1-18　コンピュータ・電磁的記録対象犯罪の検挙件数の推移
（出典）警察庁「令和 2 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

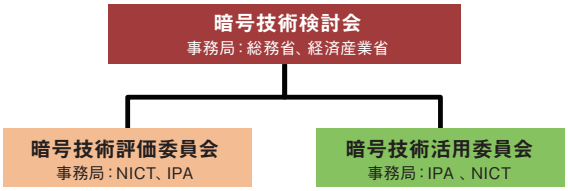
2.1.5 CRYPTRECの動向

電子政府の情報セキュリティを確保するため、総務省と経済産業省、NICT、及び IPA は安全性と実用性に優れた暗号技術を選び出すことを目的に、CRYPTREC（Cryptography Research and Evaluation Committees）を組織している。CRYPTREC では、電子政府システムでの利用を推奨する暗号アルゴリズム（CRYPTREC 暗号リスト※144）の安全性を評価、監視し、暗号技術の適切な実装法や運用法を調査、検討している。

(1) 2020 年度の体制

CRYPTREC は、総務省と経済産業省が運営し、政策的な判断を含む総合的な観点から電子政府の安全性及び信頼性を確保する活動を推進する「暗号技術検討会」、及び NICT と IPA が共同で運営し、主に技術的な評価を実施する委員会とで構成されている。

委員会には、暗号技術の安全性評価を中心とした技術課題を主に担当する「暗号技術評価委員会」と、セキュリティ対策の推進、暗号技術の利用促進に向けた環境整備を主に担当する「暗号技術活用委員会」が設置されている（図 2-1-19）。



■図 2-1-19　CRYPTREC の体制

暗号技術検討会と両委員会の主な役割は以下のとおりである。

- 暗号技術検討会

  CRYPTREC 活動計画の承認、委員会が作成する各種成果物の承認等、政策的な判断を含む総合的な観点から電子政府の安全性及び信頼性を確保する活動を推進する。量子コンピュータが実用化されても安全性が保てると期待される暗号「耐量子計算機暗号（PQC：Post-Quantum Cryptography）」を含む新たな暗号技術の動向等を踏まえ、次期 CRYPTREC 暗号リストに求められる要件や課題等を整理するため、傘下に「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」（以下、暗号の在り方 TF）が設置されている。

- 暗号技術評価委員会
  暗号技術に対する攻撃技術動向の調査や安全性評価等、暗号技術における技術的信頼に関する検討を担当する。傘下には、公開鍵暗号の中長期的な安全性の検証や新世代暗号に係る調査等を行う「暗号技術調査ワーキンググループ」が設置されている。
- 暗号技術活用委員会
  セキュリティ対策の推進、暗号技術の利用促進等に寄与する運用ガイドラインの整備を中心とした、暗号利用に関する課題の検討を担当する。

(2) 2020 年度の主な活動

2020 年度の暗号技術検討会及び各委員会の主な活動内容・成果について以下に述べる。

(a) 暗号技術検討会

2020 年度には、各委員会の 2019 年度活動報告、2020 年度活動計画、及び 2020 年度の活動報告の審議が行われ、承認された。

また、CRYPTREC 暗号リスト改定に向けた暗号の在り方 TF での検討内容が報告され※145、承認された。具体的には、検討継続課題となっていた CRYPTREC 暗号リストの取り扱いについて、以下のとおりの結論となった。

- CRYPTREC 暗号リストの構成は変更しない（「電子政府推奨暗号リスト」「推奨候補暗号リスト」「運用監視暗号リスト」の 3 リスト構成を維持する）。
- リスト間の移行ルールを整理し、特に「推奨候補暗号リスト」からの削除条件を明確化した。その条件とは、「安全性維持が困難（危殆化した）と判断した場合」と「CRYPTREC 暗号リスト（旧電子政府推奨暗号リストを含む）への掲載から 20 年を超えた後に実施する最初の利用実績調査までに、十分な利用実績を確認できなかった場合」であり、どちらかの条件に該当した場合に「推奨候補暗号リスト」から削除されることとなった。

(b) 暗号技術評価委員会

CRYPTREC 暗号リストに掲載されている暗号技術の安全性と実装性に関わる監視活動のほか、2020 年度の主な活動内容・成果は以下のとおりである。

- EdDSA の安全性評価
  TLS1.3 で採用され、次期米国政府標準デジタル署名方式（FIPS 186-5）でも追加予定となっている新しいデジタル署名 EdDSA※146 について、今後の利用拡大が見込まれることから、CRYPTREC 暗号リスト（推奨候補暗号リスト）への追加を視野に入れ、安全性評価を行った。その結果、EdDSA の曲線（Ed25519 と Ed448）及び方式の構成いずれについても安全性に問題は見つからなかったことから、引き続き、実装性能評価を行うこととなった。
- 暗号技術調査ワーキンググループの活動
  最近進展が著しい量子コンピュータによる暗号技術の安全性への懸念が提起されているため、2020 年度は、PQC を導入するための技術に関する動向、及び Shor の量子アルゴリズム※147 による現代暗号への脅威に関する調査を行った。本調査で注目すべきことは、「現状の量子コンピュータでは暗号で用いる程大きなパラメータの合成数を素因数分解することは困難であり、量子ビット数やゲート計算のエラー率等量子コンピュータの性能の大幅な向上がない限りは現代暗号の脅威にはならないと考えることができる」との見解をまとめたことである。また、主要な公開鍵暗号（RSA 暗号、楕円曲線暗号）の安全性の根拠となる「素因数分解問題」と「離散対数問題」の困難性に関して、CRYPTREC が公開している「予測図」の改訂も行った※146。

(c) 暗号技術活用委員会

2020 年度には、安全な暗号利用に関する運用ガイドラインを整備する観点から、「暗号鍵管理システム設計指針（基本編）※148」及び「TLS 暗号設定ガイドライン※149」を 2020 年 7 月に公開した。以下に概要を紹介する。

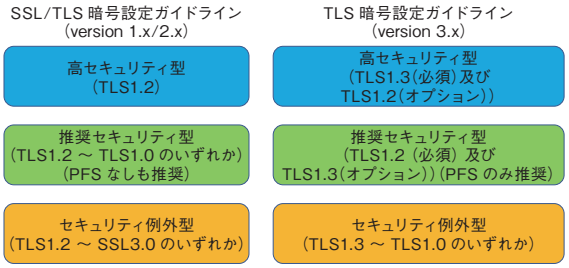
- 暗号鍵管理システム設計指針（基本編）
  本設計指針は、暗号鍵管理の必要性を認識するための「暗号鍵管理の在り方」についての解説部分と、鍵管理ガイドラインである NIST SP800-130 の解説書・利用手引書として活用できる「暗号鍵管理についての技術的内容」を取りまとめた部分とで構成される。具体的には、解説部分では暗号鍵管理の考え方や枠組み、暗号鍵管理において重要な「時間管理」の概念を説明している。
  また、技術的内容では、暗号鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき事項一覧（Framework Requirements）として NIST SP800-130 の内容を再整理して、暗号鍵管理システムのプロファイルや設計仕様書、運用マニュアル等の中で明示的に記載すべき要求事項を示している。
  ただし、本設計指針では具体的な特定のセキュリティ

機能の採用を義務付けていない。そのため、どのようにそれらの要求事項に対応するかは設計者や運用責任者に委ねられ、それらの対応方針をプロファイルや設計仕様書、運用マニュアル等に記載する必要がある。そこで、2021 年度以降、それらの作業を支援するためのプロファイル等の作成マニュアルを準備する計画である。まずは作成方法を整理する作業から始め、2022 年度に完成させる予定である。

- TLS 暗号設定ガイドライン

  本ガイドラインは、サーバの構築者･管理者向けにサーバでの適切な TLS 暗号設定方法を解説したもので、SSL/TLS 通信の規格化や技術環境の変化に対応するため、TLS1.3 の採用や SSL3.0 の禁止に伴って一段高い安全性を求める等、従来の暗号設定ガイドラインから全面的に内容を見直したものである（図 2-1-20）。2020 年 3 月時点における、TLS 通信で実現すべき安全性と、必要となる相互接続性とのバランスを考慮した三つの設定基準を提示している。また、これまでの必ず満たさなければならない「遵守項目」に加え、より良い安全性を実現するために満たすことが望ましい「推奨項目」を追加することで、より現実的かつ実効性･柔軟性が高い要求設定を可能にしている（表 2-1-3）。

また、今まで CRYPTREC 暗号リストに掲載されたアルゴリズムや鍵長の選定方法についてのガイダンスがなかったため、新たな取り組みとして、「鍵長設定要件（仮）」と「鍵長設定ガイダンス（仮）（一般用）」を作成することとし、作成方針を取りまとめた。これらのガイダンスは、2021 年度末に完成させる予定である。



■図 2-1-20　従来の暗号設定ガイドラインとの比較

要求設定	遵守項目	プロトコルバージョン	利用禁止プロトコルバージョンを利用不可にする設定
		サーバ証明書	利用する暗号アルゴリズムと鍵長の設定
			発行・更新時の鍵情報の生成方法の明確化
			警告表示の回避方法の明確化
		暗号スイート	利用禁止暗号アルゴリズムを利用不可にする設定
			公開鍵暗号の鍵長の設定
	推奨項目	プロトコルバージョン	利用プロトコルバージョンの優先順位付け
		暗号スイート	利用推奨暗号アルゴリズムのみでの設定
			推奨暗号スイートの優先順位付け

■表 2-1-3　要求設定における遵守項目と推奨項目

COLUMN

暗号の安全性を最終的に決めるものは？　ー各国の暗号政策調査からー

「暗号の安全性」といったとき、どんなことを思い浮かべますか？　この質問に対して、多くの場合は、「暗号アルゴリズムの安全性」を前提に話がされるのではないでしょうか。例えば、この暗号は安全である、今の公開鍵暗号は量子コンピュータで簡単に解読される、量子暗号は解読不可能な究極の暗号である、等々。

このこと自体は間違いではないのですが、注意する必要があるのは、システム全体から見れば、暗号アルゴリズムはあくまでも暗号処理を行うツールであって、「暗号システムの安全性」について何ら言及するものではない、ということです。もちろん、暗号アルゴリズム自体の安全性に問題があれば暗号システムの安全性にも直接的な悪影響を及ぼします。ところがその逆は成り立たず、暗号アルゴリズムが安全だからといって暗号システムが安全であるかどうかは分かりません。

では、暗号アルゴリズムの安全性以外に暗号システムの安全性に影響を与えるものにどんなものがあるでしょうか？　これには、暗号鍵の管理、ユーザに対する認証と権限管理、脆弱性がない製品の利用等といったものが考えられます。これら暗号システムの安全性に影響を与えるものの中には、相反する要求が出されることもあります。例えば、通信経路上を完全に暗号化する End-To-End 暗号化。確かに、ネットワークサービスの安全性確保や個人のプライバシー保護のことを考えれば End-To-End 暗号化は望ましい対策です。しかし一方で、内部不正による情報持出やサイバー攻撃による情報漏えい、ウイルスの流入等を管理部門がチェックできないということにつながることを考慮するなら End-To-End 暗号化はむしろ望ましくない対策であると言うこともできます。

つまり、暗号システムの安全性は、技術だけで決まるものではなく、暗号を使って何を達成したいのか、相反する要求をどのように調整するのかという「ポリシー」に大きく依存することになります。

実際、これが国家として（とりわけ、安全保障や重要インフラ保護、治安に関わるケース）の話となるとより鮮明に表れてきます。そのことを確かめるために、IPA では、米国、英国、フランス、ドイツ、エストニア、ロシア、中国、韓国、オーストラリア、EU の暗号に関わるセキュリティ政策に関する実施体制、法制度及び認証制度についての最新動向調査を実施してみました。

この調査で確認できたことは、これらの国々では国家における暗号に関わるセキュリティ政策に関する組織の指示・責任担当が一元化され、トップダウン型の強い権限が与えられていること、しかも近年その権限が強化されつつあることでした。例えば、中国では暗号法（2020年 1 月施行）を根拠法として、共産党中央委員会下に国家暗号管理局を設置しています。こうした、国家としての方針の徹底が図られているあたりは、暗号アルゴリズムと暗号システムの違いをよく理解していると感じられます。

なお、この調査報告書は以下の URL から入手できます。

https://www.ipa.go.jp/security/fy2021/reports/crypto_survey/index.html

2.2 国外の情報セキュリティ政策の状況

サイバー脅威・サイバー犯罪は国境を問わず、あらゆる国・地域の脆弱性を突き、ターゲットに攻撃を仕掛けてくる。また、IT 化した社会サービスやそれを支えるサプライチェーンは国境を越えてつながり合い、他国におけるサイバー脅威が自国に深刻な影響を与える可能性がある。更に近年、国家の支援を受けた攻撃者による他国へのサイバー脅威が現実になりつつある。こうした状況に国や地域が単独で対処することは難しく、国際連携が不可避である。本節では、国際連携に向けた状況理解のために、各国・各地域における情報セキュリティ政策について述べる。

2.2.1 国際社会と連携した取り組み

2019 年度に引き続き、日本政府は 2020 年度も米国、欧州、インド、ASEAN 諸国等とのサイバーセキュリティに関する連携協議や演習を実施した。それらの活動から主な取り組みを紹介する。2020 年度の全体的な傾向として、新型コロナウイルス感染拡大対策に関する国際連携が最重要課題となり、サイバーセキュリティに関する連携は現状維持とし、討議は縮小されたものが多い。

(1) 各国首脳・国際機関との連携

新型コロナウイルス感染は 2020 年 1 月以降世界的に広まり、中国、米国、欧州等各国で緊急事態が宣言された。これに伴い、2020 年 3 月 24 日、安倍晋三首相は東京 2020 オリンピック・パラリンピック競技大会の 1 年延期を Thomas Bach 国際オリンピック委員会（IOC：International Olympic Committee）会長と合意した、と発表した※150。この結果オリンピック大会は 2021 年 7 月 23 日開幕、パラリンピック大会は同年 8 月 24 日開幕と延期が決定した。

上記のように世界的な大規模イベント開催は延期等が相次ぎ、イベント対応のセキュリティ対策連携は継続の形になった。また各国首脳会談の多くもオンライン開催となり、政策課題については新型コロナウイルス対策が優先され、サイバーセキュリティに関する協議は安全保障等、限定的なものであった。

(a) G7 首脳会合・外相会合

G7 首脳は、新型コロナウイルス感染拡大への対処を協議すべく、2020 年 3 月 16 日、4 月 16 日にテレビ会議を行った。このうち 3 月 16 日の会議では、首脳声明として、新型コロナウイルス感染拡大対策の加速化、新型コロナウイルス流行の経済的影響への対応、経済成長を回復させることを表明した※151。また安倍首相は東京 2020 オリンピック・パラリンピック競技大会について、人類が新型コロナウイルスに打ち勝った証として完全な形で実施したいと述べ、各国の支持を得た。同会議に続き 3 月 25 日、G7 外相会合もオンラインで行われ、外務大臣間での連携が確認された。同会合では地域情勢も議論され、茂木敏充外務大臣は北朝鮮の弾道ミサイル発射実験等への抗議と各国の緊密な連携を呼びかけた※152。更に 4 月 16 日の G7 首脳テレビ会議では、各国の新型コロナウイルス感染拡大対策の取り組みが討議された。安倍首相は 4 月 7 日に発表した緊急事態宣言※153 と経済対策の紹介に加え、治療薬の開発、医療体制の脆弱な国の支援、情報の共有、世界の新型感染症予防体制の強化等を訴え、各国首脳の賛同を得た。

2020 年 8 月に予定されていた G7 米国サミットは、新型コロナウイルス感染拡大対応と米国大統領選挙によりいったん 11 月に延期されたが、開催が見送られた。G7 サミットでは例年、自由でオープンなサイバー空間の維持に関連する合意文書が出され、2019 年 8 月のフランス・ビアリッツサミットでは「開かれた自由で安全なデジタル化による変革のための戦略」が発表された※154 が、2020 年度はこの合意についても見送られた。

(b) 日米豪印外相会合

G7 の枠組みとは別に、2019 年以降、日米豪印（インド）4 ヵ国による協議が重ねられている。中国の東シナ海・南シナ海・インド洋への進出政策が各国共通の重要課題となっており、連携を強化する狙いがあると思われる。

2020 年 10 月 6 日、第 2 回日米豪印外相会合が東京で開催され、茂木外務大臣、Mike Pompeo 米国国務長官（Secretary of State of the United States）、Marise Payne オーストラリア連邦外務大臣（Minister for Foreign Affairs of the Commonwealth of Australia）、Subrahmanyam Jaishankar インド外務大臣（External Affairs Minister of India）が出席した※155。同会合でも新型コロナウイルス感染拡大対策での連携が確認されたほか、主要議題であるインド太平

洋地域の安全保障については、「自由で開かれたインド太平洋」ビジョンの重要性を再確認し、実現に向けた連携を広げること、特に「インド太平洋に関するASEANアウトルック※156」を通じてASEAN地域を支援すること、同ビジョン推進のために海洋安全保障、テロ対策、サイバーセキュリティ、人道・災害支援、人材教育等多方面で協力することで合意した。

更に2021年2月18日、米国Joe Biden大統領就任を受けた形で日米豪印外相電話会談が行われ、米国からはAntony Blinken国務長官が参加した※157。同会談では各国の実務レベルの協議・協力の進展を歓迎し、ASEAN、欧州との連携推進を確認したほか、茂木外務大臣からミャンマー情勢や中国海警法※158の成立に対する深刻な懸念が示され、力による現状変更の試みに対して強く反対することで合意した。

(c)国連によるサイバー脅威対策推進

国際連合(以下、国連)のサイバーセキュリティに関する国連オープン・エンド作業部会(OEWG:Open-ended Working Group)は、2018年12月の第73回国連総会決議(A/RES/73/27)に基づき、国際安全保障の文脈における情報、及び電気通信分野の発展に関して国連全加盟国が参加可能な議論の場として、2019年に設置された部会である※159。同年9月に第1回会合を開催して以来、サイバー空間における脅威認識、規範、国際法の適用、信頼醸成、能力構築等について検討が続けられ、日本もメンバーとして貢献してきた。2021年3月8～12日にOEWGの最終会合が開催され、検討成果の報告書が採択された※13。2021年の第75回国連総会に提出される見通しである。

同報告書はサイバー空間における脅威認識、責任ある国家の行動規範、サイバー空間で国際法がどのように適用されるか、信頼醸成、能力構築等について国連加盟国の共通認識を示し、サイバー空間の紛争防止・解決における国際法の適用を改めて確認したものである※160。承認されれば、サイバー空間上の紛争の抑止に一定の効力を持つことが期待される。

(2)2国間連携の取り組み

2019年度まで例年開催されてきた2国間のサイバー対話は、2020年4月以降、以下に示す日英サイバー対話以外ほとんど開催されていない(2021年4月現在)。以下ではスコープを広げ、日米安全保障協議委員会、日米首脳会談、日EU首脳テレビ会議についても紹介する。

(a)日英サイバー協議

2021年1月31日、東京において第5回日英サイバー協議が開催された※161。日本からは赤堀毅外務省総合外交政策局参事官兼サイバー政策担当大使を始めとする関係機関の代表者が、英国からはAlexander Evance外務省サイバー政策部長(Director Cyber, National Security Directorate, Foreign and Commonwealth Office)を始めとする関係機関の代表者が出席した。協議においては両国の最新のサイバーセキュリティ戦略と取り組みのほか、能力構築支援、国連を含む国際機関における双方向の連携等について意見を交換した。

(b)日米安全保障協議委員会

2021年3月16日、東京において日米安全保障協議委員会(日米「2+2」)が開催され、日本から茂木外務大臣と岸信夫防衛大臣、米国からAntony Blinken国務長官、Lloyd Austin国防長官(Secretary of Defense of the United States)が参加した※162。同委員会は、米国Biden政権との最初の閣僚級協議としてどのような合意になるかが注目された。

地域安全保障においては、2019年に懸念された北朝鮮の非核化に加え、中国の東シナ海・南シナ海への進出、海警法成立による中国国内法の外洋警備への適用、香港・新疆ウイグル自治区における人権問題等が深刻な懸念として共有され、日米豪印4ヵ国及びASEAN諸国との協力が再確認された。また防衛体制については、宇宙・サイバー領域における協力と情報保全の強化が強調された。

(c)日米首脳会談

日米「2+2」に引き続き、同年4月15～18日に菅義偉首相は米国を訪問、16日にワシントンDCにてJoe Biden大統領との日米首脳会談が行われた※163。同会談の共同声明「新たな時代における日米グローバル・パートナーシップ※164」においては、両国はパンデミックを終わらせ、「持続可能な、包摂的で、健康で、グリーンな世界経済の復興」を主導するために、デジタル経済の促進、気候変動に対応する脱炭素化、健康安全保障等において協力することが明記された。また、「自由で開かれたインド太平洋と包摂的な経済的繁栄の推進」のために両国の同盟を強化するとし、中国の「東シナ海における一方的な現状変更の試み」や「南シナ海における不

法な海洋権益に関する主張及び活動」に反対し、「台湾海峡の平和と安定」を重視することが明記された。

このように日米両国が共同声明で中国を非難することは異例であり、安全保障分野における中国との対立姿勢が鮮明となった。

(d)日 EU 首脳テレビ会議

2020 年 5 月 26 日、新型コロナウイルス感染拡大対策を主要議題として日 EU 首脳テレビ会議が開催された。日本からは安倍首相、EU からは Charles Michel 欧州理事会議長（President of the European Council）及び Ursula von der Leyen 欧州委員会委員長（President of the European Commission）が参加した※165。

同会議では、新型コロナウイルス感染終息後の経済復興について意見が交換され、高信頼通信インフラの整備拡充、強靭なサプライチェーンの構築、海外投資に対する安全保障上の観点からの適切な対応等、明らかに中国を意識した討議が行われた。また、新型コロナウイルス感染拡大の検証を公平で独立した形で行うこと、将来的な感染流行を防ぐために世界保健機関（WHO：World Health Organization）を含む国際機関の改革・効率化が重要であること等が確認された。

(3)アジア太平洋地域のサイバー連携

アジア太平洋地域における政府レベルの連携施策について述べる。CSIRT に関する連携施策については、「2.2.4 アジア太平洋地域での CSIRT の動向」を参照されたい。

(a)日・ASEAN サイバーセキュリティ政策会議

2020 年 10 月 20 日、第 13 回日・ASEAN サイバーセキュリティ政策会議（以下、政策会議）がオンラインで開催された※101。本会議は、サイバーセキュリティ分野における ASEAN 諸国との連携強化を目的として 2009 年より開催されている。

第 13 回政策会議は日本・カンボジアが議長国となり、日本から NISC、総務省、経済産業省の審議官、ASEAN 加盟国からサイバーセキュリティ・情報通信関係政府機関の局長・審議官等が参加した。同会議では、第 12 回政策会議で協力が合意された 9 項目（サイバー演習、重要インフラ保護、能力構築、インシデント相互通知、オンラインコミュニティ等）の活動状況を確認するとともに、今後の重点活動項目として、情報共有体制・インシデント対処体制の強化、能力構築・意識啓発分野の協力推進、産学官連携の事例共有等が議論され、活動の継続が確認された。

(b)ASEAN 地域フォーラム

ASEAN 地域フォーラム（ARF：ASEAN Regional Forum※166）は、ASEAN 地域の安全保障環境の向上を目的としたフォーラムで、日本政府は連携を継続している。サイバーセキュリティに関しては、シンガポール・マレーシアと共同で「サイバーセキュリティに関する会期間会合（ARF-ISM on ICTs Security）」を立ち上げ、2018 年 4 月より活動が始まっている。

2021 年 1 月 26 日、サイバーセキュリティに関する ARF 会期間会合のための第 6 回専門家会合※167 がオンラインで開催された。2020 年 1 月の第 5 回専門家会合と同様、日本・マレーシア・シンガポールが共同議長を務め、日本からは佐藤大輔外務省総合外交政策局経済安全保障政策室長が参加した。第 5 回に引き続き、国際的なサイバーセキュリティ環境や各国・地域の取り組み、今後取り組むべき信頼醸成措置について議論が行われた。また、サイバーセキュリティに関する国連政府専門家グループであるサイバー GGE（Group of Governmental Experts）※168 やオープン・エンド作業部会 OEWG（「2.2.1(1)(c)国連によるサイバー脅威対策推進」参照）等への参画を含め、世界的なサイバーセキュリティに関する議論に積極的に貢献することを確認した。

(c)インド太平洋地域に向けたサイバー演習

前出のように、インド太平洋地域のサイバーセキュリティ連携においてサイバー演習、能力構築は重要課題である。この状況のもとで 2021 年 3 月 8 ～ 12 日、経済産業省と IPA は米国政府と連携し、ASEAN を含むインド太平洋地域諸国を対象に、制御システムのサイバーセキュリティに関する演習をオンラインで実施した※169。また演習の一環としてポスト・コロナにおけるサイバーセキュリティに関する日米欧セミナーを開催した。本演習は制御システム等の重要インフラ防御に関するもので、ASEAN 及びインド太平洋地域から 40 名が参加した（演習内容は「2.3.2(1)中核人材育成プログラム」参照）。

(4)セキュリティ連携に関する国際会議

サイバーセキュリティの国際連携に関する主な会議として、2020 年度は、2019 年度に引き続き「サイバーセキュリティ国際シンポジウム」「サイバー・イニシアチブ東京」が開催された。

(a) 第 10 回サイバーセキュリティ国際シンポジウム

本シンポジウムは、サイバー脅威対応に向けた国際間の信頼構築を討議する場として、2016 年から日本で開催されている。2020 年は慶應義塾大学、同大学が主導する研究機関の国際連携組織 INCS-CoE（InterNational Cyber Security Center of Excellence）、米国 The MITRE Corporation[※170] の共催の形をとり、10 月 5 ～ 9 日にオンラインで開催された[※171]。また米国・英国・オーストラリア・イスラエル大使館及び駐日欧州連合代表部を始め、関係国の省庁が後援し、各国の有識者が参加した。会期中午後は国内向けの Japan Session、夜は Global Session という構成であった。

Global Session では、日本政府から河野太郎行政改革担当大臣が前防衛大臣の立場で講演し、基調パネルではパンデミック状況下のグローバルトラストをテーマとして、中満泉国際連合事務次長・軍縮担当上級代表（Under-Secretary-General and High Representative for Disarmament Affairs, United Nations）、Jeremy Jurgens 世界経済フォーラムマネージングディレクター・サイバーセキュリティセンター長（Managing Director & Head of the Centre for Cybersecurity, World Economic Forum）等が登壇、信頼構築について討議を行った。他の全体パネルでは、サイバーに関する規範、産学官のサイバー訓練、新型コロナウイルスの教訓、マルチステークホルダーによる国際トラスト等が議論された。産学官が連携した信頼構築に関する国際会議としてユニークなものと考えられる。

(b) サイバー・イニシアチブ東京 2020

世界各国の産学官のセキュリティ専門家を招いたサイバー・イシアチブ東京 2020 が、2020 年 11 月 24 ～ 25 日にオンラインで開催された[※172]。前出のサイバーセキュリティ国際シンポジウムと比較して、デジタルとリアルの融合に伴う脅威にフォーカスを当てた構成であった。

日本政府からは武田良太総務大臣、梶山弘志経済産業大臣、宇都隆史外務副大臣、岸信夫防衛大臣がそれぞれ講演したのを始め、関係省庁のセキュリティ関係者、国内・海外の民間有識者が参加し、ナショナルセキュリティ、ニューノーマルの安全保障、サプライチェーンリスク、医療セキュリティ、データ利活用等の多岐にわたる課題について議論が行われた。

2.2.2 米国の政策

2020 年度は米国にとり、新型コロナウイルスによるパンデミックへの対応、大統領選挙における世論の分断、Joe Biden 新大統領への政権移行、中国との継続的な関係悪化等が立て続けに起こる年となった。

米国のサイバーセキュリティ政策は、2019 年以降、サイバー空間の敵対的行動を監視し対抗する、という安全保障重視の姿勢を取り、サプライチェーンセキュリティの強化を進めている。しかし、SolarWinds Worldwide, LLC.（以下、SolarWinds 社）のネットワーク管理システムの脆弱性を突いたサプライチェーン攻撃、Colonial Pipeline Company（以下、Colonial 社）のパイプラインシステムを狙ったランサムウェア攻撃等が相次ぎ、米国政府・重要インフラへのサイバー脅威が深刻であることが改めて鮮明となった。

中国との関係においては、新型コロナウイルス対策における情報開示、海洋進出等の Trump 政権時からの課題に加え、香港・新疆ウイグル自治区における人権問題、台湾の主権帰属問題等から Biden 政権も中国に対して厳しい姿勢を取り、中国 IT 製品のサプライチェーンからの締め出し、及びグローバルサプライチェーンの再構築が継続される情勢である。

本項では、このような状況下で推進された米国政府のサイバーセキュリティ政策について述べる。

(1) 新型コロナウイルス対策とセキュリティリスク対応

新型コロナウイルスの蔓延と対策に関するセキュリティリスクの状況について述べる。

(a) 非常事態宣言

Donald Trump 大統領は 2020 年 3 月 13 日、新型コロナウイルス感染拡大について国家非常事態を宣言した[※173]。この宣言では、以下のような施策が盛り込まれた。

- 感染検査・治療対策に最大 500 億ドル（約 5 兆 4,000 億円）の連邦政府予算をあてる。
- 医療従事者に対する規制を緩和し、治療における最大限の柔軟性を与える。
- 病院に緊急対応計画の発動を要請する。
- PCR 検査を迅速に拡大する。
- 大学等が休校となった学生のローン返済を猶予する。

一方で、ニューヨーク州、カリフォルニア州等が独自

の緊急事態宣言を発動し、都市部のロックダウン等の厳しい措置をとったのとは対照的に、外出・旅行・マスク着用等に関する要請はなかった。

Biden 政権は 2021 年 2 月 24 日、パンデミックに対して引き続き警戒が必要であるとして、非常事態宣言の継続を宣言した※174。

(b) サプライチェーンリスクと中国との関係悪化

米中政府間では 2020 年 2 月初旬の中国滞在者の米国渡航制限以来、新型コロナウイルス感染原因の特定をめぐって相互に非難が続いた。Trump 大統領は同年 4 月、感染拡大防止でやるべきことをしていない、として中国を正面から批判※175、5 月には新型コロナウイルスが中国湖北省武漢にあるウイルス研究施設から流出したものか調査中であるとした※176。これらの発言はパンデミックと緊急事態宣言による経済停滞に苦しむ米国国民の支持を得て、2019 年秋の経済摩擦交渉で一時修復に向かった米中関係は急激に悪化した。一方、新型コロナウイルスの発生源とされ、また中国製造業の拠点でもある武漢市は 2020 年 1 月 23 日より 4 月 8 日まで完全にロックダウンされ※177、中国を起点とするグローバルサプライチェーンは甚大な影響を受けることとなった。

米国では既に、Huawei Technologies Co. Ltd. を始めとする中国 IT ベンダの製品が連邦政府システムや民間の重要インフラシステムにおいて調達されることが懸念され、サプライチェーンからの締め出し施策が実施されている（「情報セキュリティ白書 2020※178」の「2.2.2 米国の政策」参照）。加えて、パンデミックによりサプライチェーンリスクは更に深刻化し、これまで中国を起点としていたグローバルサプライチェーンの分散化・国内回帰の機運が米国・欧州・日本で高まりつつある。

Biden 大統領は選挙公約にサプライチェーンの米国回帰を掲げていたが、2021 年 2 月 24 日、サプライチェーン頑健化に関する大統領令に署名した※179。同大統領令では、頑健化の方針として安全、分散化、国産製品活用、冗長性、国内人材活用等が挙げられ、国家安全保障担当補佐官（APNSA：the Assistant to the President for National Security Affairs）、経済政策担当補佐官（APEP：the Assistant to the President for Economic Policy）が関係機関と協調してこれを実装するとし、施策として 100 日以内のサプライチェーンリスクレビュー、1 年以内の各政府機関のサプライチェーンアセスメント、及び過去 1 年にとられた対策の報告と提言を求めている。Biden 政権としては、パンデミック終息後の経済再建において環境問題・脱炭素を重視し、関連産業のサプライチェーン構築で脱中国を果たし、優位に立つ戦略があるものと思われる※180。

(c) CISA の新型コロナウイルス関連リスク対応

新型コロナウイルス関連のサイバーリスク対策は、国土安全保障省（DHS：Department of Homeland Security）配下でサイバーセキュリティと重要インフラセキュリティを統括する CISA（Cybersecurity and Infrastructure Security Agency）が中心となって推進している。2020 年 3 月 6 日、CISA はいち早く新型コロナウイルス関連詐欺メール・詐欺サイトに関する注意喚起を、また 3 月 18 日には重要インフラ保護、サプライチェーンの維持、リモート業務の保護、新型コロナウイルス関連詐欺対策を含むリスク管理ガイダンスを公開した※181。詐欺被害に関しては連邦捜査局（FBI：Federal Bureau of Investigation）も別途注意を呼びかけた※182。

また CISA は、英国国家サイバーセキュリティセンター（NCSC：National Cyber Security Centre）と共同で、新型コロナウイルスを話題とする標的型攻撃が急増する中、セキュリティ的に脆弱な環境でテレワークが行われている、として同年 4 月 8 日に注意喚起を行い※183、4 月 24 日にはテレワークのセキュリティガイダンスを公開した※184。また 4 月 17 日、コロナ禍における重要インフラ基盤の運用と従業員の安全に関するガイダンス（第 3 版）を公開した※185。更に 5 月 5 日、CISA と NCSC は新型コロナウイルス関連の医療研究機関・製薬企業の研究データや知的財産データが窃取される恐れがある、と警告した。続く 5 月 13 日における FBI と共同の注意喚起※186 では、「中国と関係するサイバーアクターが情報を狙っている」と初めて中国が名指しされた。

更に CISA は同年 8 月 12 日、中小企業庁（SBA：Small Business Administration）の新型コロナウイルス救済融資をかたるメールについて注意喚起を行った※187 が、この後、新型コロナウイルス関連の詐欺攻撃は一段落した模様で、2021 年 4 月時点まで CISA から注意喚起は行われていない。

(d) 新型コロナウイルスをめぐるインフォデミック

2020 年 1 月以降、米国国務省の官僚が「SNS 上で反米的な偽情報を拡散している」としてロシアを非難する※188 等、新型コロナウイルス感染拡大をめぐり、インターネット上で国家間の非難の応酬が続いた。

同年 3 月以降は感染源や対策、ワクチン等をめぐる

誤情報や偽情報（フェイクニュース）がネット上にあふれ、社会に悪影響を及ぼすインフォデミック（infodemic）の状況が各国で現出した。これに対しWHOは同年9月、国連や国際連合児童基金（UNICEF：United Nations International Children's Emergency Fund）等の国際機関と共同して、正確で信頼できる情報を提供し、誤情報・偽情報の拡散を防ぐ対策を講じることを加盟国に呼びかけた※189。

米国においては、CISAが詐欺攻撃への注意喚起のほか、誤情報・偽情報に対する注意喚起も行っている※190。CISAは注意喚起の中で、信頼できる情報源として米国疾病予防管理センター（CDC：Center for Disease Control and Prevention）、連邦緊急事態管理庁（FEMA：Federal Emergency Management Agency）のRumor controlサイト、WHOを挙げている。

一方、国防総省（DoD:Department of Defense）は、2020年4月の時点で中国、ロシアのコロナウイルスに関する情報発信が虚偽であり、特にロシアの情報（手洗いの効果はない）は対策を誤らせるとして非難していた※191。インフォデミックについても軍への波及の観点から警戒し、軍関係の情報で事実でないものを公開している※192。またコロナワクチン接種を控えさせかねない誤情報についてもこれを否定し※193、軍関係者に接種を促している。

民間組織もコロナ関連情報の監視を行っている。例えば情報監視サイトPOLYGRAPH.infoはSNS上で流通するコロナ情報のファクトチェックを行い、誤り（Misinformation）あるいはミスリーディングなもの（Disinformation）を根拠とともに公開している※194。言うまでもなく、こうした組織はパンデミック関連情報に限らず、政治・軍事・人権等様々なカテゴリのファクトチェックを行っている。

こうした努力にもかかわらず、インフォデミックの影響は米国では深刻と考えられる。2021年2月の民間調査によれば、民主党支持者の8割以上がパンデミックを深刻な脅威としたのに対し、共和党支持者で深刻な脅威とした人は半数に満たないことが確認された※195。このような分断状況が、事実を受け入れず偽の情報を流通させてしまう、場合によっては感染し死に至る、等の問題につながっている可能性がある。

(2) Trump政権下のセキュリティ施策

2021年1月までのTrump政権のもとで、各政府機関により推進されたセキュリティ施策について述べる。

(a) Trump政権の政策

2020年はTrump政権4年目であり、2018年9月に米国大統領として初めて発表したサイバーセキュリティ戦略を実装するべく、各政府機関が施策を推進してきた。この戦略は前述のように、国家安全保障の観点から敵対的勢力に対抗する施策・体制を盛り込んでいるが、同時に外交・経済制裁等を含め、同盟国・民間との連携を重視した協調的な姿勢も示してきた。

2018年9月にTrump大統領が公表した国家サイバーセキュリティ戦略を拡張する形で、同政権は2020年3月、セキュア5Gに関する国家戦略を発表した。CISAとNRMC（National Risk Management Center）はこれに基づき、2020年8月14日、セキュアで頑健な重要インフラのための5G戦略を発表した※196。大統領選挙前にセキュリティ関連戦略として具体化されたものは、これが最後となった。

一方で、サプライチェーンリスク対応には大統領任期満了までこだわり、2021年1月5日、Trump大統領はAnt Group Co., Ltd.の「Alipay（支付宝）」を含む八つの中国デジタル決済プラットフォームとの取り引きを禁止する大統領令に署名した※197。また1月20日、自身最後のサプライチェーンセキュリティ施策として、米国のIaaSプラットフォーム事業者に外国人利用者の記録を残すことを要請する大統領令に署名した※198。ただし、これらの施策の実施可否はBiden政権に委ねられた。

(b) DHSの施策

DHSでは、2018年11月にサイバーセキュリティと重要インフラセキュリティを統括する組織として改組されたCISAの活動が本格化している。活動のうち、新型コロナウイルス対策については既に記したが、このほかの重点項目として重要インフラセキュリティ、サプライチェーンセキュリティがある。このうち重要インフラセキュリティ、特に制御システムに対する脅威とその対策については「3.1 制御システムの情報セキュリティ」を参照されたい。

サプライチェーンセキュリティについては、2019年に設置したICT Supply Chain Risk Management（SCRM）Task Force（以下、Task Force）が中心となり、2020年2月に、IT製品・サービスの供給者視点でまとめたサプライチェーン脅威シナリオ第1版を、また2021年2月には脅威シナリオのインパクトと緩和策（mitigation）を分析した第2版を公開した※199。脅威シナリオは偽造、攻撃、内部不正、開発環境への攻撃、供給者の財務体質を含む包括的なもので、米国のサプライチェーンリ

スクのとらえ方がよく現れている。

これに続き2020年5月、Task Forceは企業のサプライチェーンリスク管理指針となるガイダンスとファクトシートを公開した※200。更に具体的なリスク管理ツールとして、米国標準技術研究所（NIST：National Institute of Standards and Technology）の規格群をベースとする製品・供給者・入札者に関する有資格リストの検討を進め、2021年4月に報告書を公開した※201。このリストがどの程度政治的な意味を持つかは未知数である。

一方でTask Forceは2020年11月、パンデミックで中国依存のリスクが顕在化したグローバルサプライチェーンの脆弱性、及びサプライチェーンを頑健化するための指針をまとめた※202。これには必ずしもITサプライチェーンにとどまらない課題と対応策が示されている。

(c) DoDのサプライチェーンセキュリティ施策

2020年1月31日、DoDは、新たなサイバーサプライチェーンセキュリティ規格として、サイバーセキュリティ成熟度モデル認証（CMMC：Cybersecurity Maturity Model Certification）の初版を公開した。また同年3月18日に改訂版Version1.02を公開した※203。「情報セキュリティ白書2020」の「2.2.2 米国の政策」で述べたとおり、調達者に対するセキュリティ規格NIST SP800-171の管理策徹底が厳しすぎる等で不評であったことから、5段階の成熟度モデル、5個のセキュリティマネジメントプロセス、171個のプラクティスで構成されるCMMCがより有効であるとして適用に踏み切ったものである。DoDは2020年3月に認証機関CMMC Accreditation Body（CMMC-AB）※204を設立、調達事業者認証に向けた準備を開始した。また、国防総省調達規則補足（DFARS: Defense Federal Acquisition Regulation Supplement）を改正し、2020年11月30日から2025年9月30日（会計年度終了）までのCMMCによる調達を暫定的に有効にする、とした※205。

このようにCMMCによる防衛調達制度が整備される一方で、認証のコスト、連邦政府とCMMC-ABとの責任分担等の問題が指摘され、2021年3月、DoDは制度の見直しにはいった※206。CMMCに限らず、高度なセキュリティ認証は高コストになりがちであるが、防衛サプライチェーンのセキュリティは米国の最重要課題ともいえる。DoDやBiden政権がどのような制度設計を行うか注目される。

(3) SolarWinds事案とその対応

2020年、連邦政府機関及びフォーチュン500に掲載される企業等を一斉に狙った過去最大規模のサプライチェーン攻撃が発覚した。同年12月13日、セキュリティベンダFireEye, Inc.は、ネットワーク管理ツールベンダSolarWinds社のネットワーク管理システムOrionへの大規模攻撃キャンペーン（UNC2452）を確認した、と発表した※207。これは、Orionのサードパーティサーバとのバックドアからトロイの木馬型プラグインを仕込み、Orionソフトウェアのアップデートにより管理対象機器にウイルスを感染させるというもので、2020年3月から始まったという。SolarWinds社は同13日にこの攻撃を認め、同社の顧客1万8,000社に影響した可能性がある、とした。CISAも同13日、連邦政府機関に対して緊急指令（Emergency Directive21-01）を発令し、サプライチェーン上で他者により利用・運用されている情報システムを保護し、脅威を緩和するための対策を求め※208、具体的な行動計画も明示した。

UNC2452の目標は情報窃取と考えられたが、調査の進展につれ、攻撃キャンペーンの広がりが深刻であることが明らかになった。FireEye, Inc.は、攻撃の水平展開の一環として、オンプレミスネットワークからOffice 365への不正アクセスが行われたとしている※209。少なくとも250の官民のネットワークが侵害され、これまで米国国家安全保障局（NSA：National Security Agency）が進めてきたインサイダー監視のための法規、DHSの防御施策、DoDのサイバーコマンド部隊が早期警戒のため海外ネットワークに設置した監視センサー等の対策がことごとく無効であったという※210。CISAは「連邦政府、州政府、自治体から重要インフラ企業のネットワークに至るまで影響は甚大である」とした※211。サイバーセキュリティやサプライチェーン関係各部門は、これまでの施策について大幅な見直しを迫られることになる。他の追跡調査については、「3.1.1(4)ネットワーク管理用のソフトウェアの脆弱性に端を発する大規模な感染事例」を参照されたい。

攻撃者については、米国大統領選挙に対するロシア政府の妨害工作が懸念されていた経緯から、ロシア情報機関とつながりのあるハッカー集団APT29による選挙妨害工作の一環である、と疑われた※212。2021年1月5日、FBI、CISA、国家情報長官室（ODNI：Office of the Director of National Intelligence）、NSAはサイバー統合調整グループUCG（Cyber Unified Coordination Group）を設置し、連邦政府ネットワーク

侵害等の重大事案に関する調査・脅威緩和を協力して行うこととした※213。この体制は言うまでもなくロシアへの対抗を意識したもので、関係4機関は翌6日、合同でSolarWinds社へのハッキングはロシアが主導した可能性が高い、と公式にロシアを非難した。これに先立ちTrump大統領は、選挙妨害は民主党の意を受けた中国による可能性もある、とSNSで発言したが、これは明確に否定された。

2021年4月15日、Biden大統領は調査結果を受け、ロシアに対する制裁措置に関する大統領令に署名した※214。同大統領令では、SolarWinds事案を含む米国に対する選挙妨害活動が、ロシア対外情報庁（SVR: Sluzhba vneshney razvedki Rossiyskoy Federatsii）によるものと断定、活動に協力したロシア企業6社を特定し、またロシア政府と米国金融機関の取り引きを一部停止するとした。当然ながらロシア政府はハッキングへの関与を否定し、制裁には報復措置を講ずるとしている※215。

(4) Microsoft Exchange事案とその対応

2021年3月2日、Microsoft Corporation（以下、Microsoft社）は、オンプレミス用メールサーバソフトウェアExchange Server 2010、2013、2016、2019の各バージョンに対する緊急セキュリティ更新プログラムをリリースした。対象となる脆弱性はExchangeサーバ上でリモートコード実行が可能になるもので、至急のパッチ適用と攻撃の調査が求められた※216。同社はまた、中国に支援された攻撃者グループHAFNIUMが高い確度でこの脆弱性を突いた限定的標的型攻撃を行っているとした※217。

セキュリティ専門家によれば、この攻撃は同年1月6日（一部Trump支持者の連邦議会占拠当日）に発見されていたが、Microsoft社の情報開示直後、パッチ未適用のExchangeサーバを持つ中小企業、自治体、学校等少なくとも3万の組織がHAFNIUMと目される中国ハッカー集団の攻撃を受け、メール通信の窃取が行われた可能性があるという※218。

これに対しCISAは3月3日に注意喚起を実施、政府機関に対しても緊急指令（Emergency Directive21-02）を発令してパッチ適用を指示した※219。Biden政権は15日に新たなUCGを招集、Microsoft社と連携して特に支援が必要な中小企業の対策・調査にあたるとともに、サイバー防御の一新のために民間との連携を強化するとした※220。民間との連携によるサイバー防御強化はTrump政権でも重点としていたが、これを踏襲した形である。

事案発覚後1ヵ月あまりで、この事案の深刻さが浮き彫りになってきた。中国のハッカーによるこれまでの不正な情報収集活動が今回の大規模な攻撃につながったといわれる※221。またMicrosoft社によれば、不正に収集されたメールアカウントの認証情報は特権昇格等の攻撃にこれからも悪用される恐れがあり、2021年4月時点においても被害の全貌が明らかになっていない可能性がある※222。同社は管理者権限の最小化等によって被害を低減するように呼びかけている。

本事案とSolarWinds事案との直接的な関係は見つかっていない。しかし、ネットワーク管理、メールサーバ等の基幹システムの脆弱性対策が機能せず、国家の支援による攻撃があれば甚大な被害となるという事態は米国を始め、欧州、日本等にも深刻な問題であり、Biden政権にとっても重要課題となると考えられる。

(5) Colonial Pipeline事案とその対応

SolarWinds、Microsoft Exchangeの各事案が収束しない2021年5月7日、石油パイプライン事業最大手のColonial社は、サイバー攻撃を受け、パイプラインの操業を停止したと発表し※223、翌8日にはネットワークへのランサムウェア攻撃を認めた。同社のパイプラインはテキサス州からニュージャージー州に及ぶ石油供給の45%を担う大動脈であり、米国東部の燃料不足が懸念される事態となった。連邦政府は直ちに対応し、10日、Biden大統領は「影響を緩和する措置をとり、攻撃を阻止し、攻撃者を訴追する」と言明し、FBIはRaaS（Ransomware as a Service）をビジネスとする東欧系ハッカー集団DarkSideによる攻撃であることを確認した※224。ロシアの関与の証拠はないとされたが、Biden大統領は「ロシアが一定の責任を負う」とコメントした。名指しされたDarkSideは、「攻撃の目的は金銭であり政治的混乱を起こす意図はない」とする声明を発表した※225。11日、FBIとCISAは更なるランサムウェア攻撃への対処について注意喚起を行った※226。

Colonial社は停止したパイプラインの再稼働を12日から始めるとし※227、フル稼働までに時間がかかるとしたが、燃料不足の懸念はひとまず沈静化した。一方、身代金については約75ビットコイン（500万ドル相当）の支払いがあったと報じられ※228、Colonial社のCEOも「早期復旧のために支払った」ことを認めた※229。

Biden政権は5月12日、サイバーセキュリティに関する大統領令※230を公表するところであったが、図らずも同時期に、重要インフラの防御が脆弱であり、被害の影

響が深刻であることが露呈してしまった。なお、大統領令については「2.2.2(7)Biden 政権の政策」で言及する。

(6) 大統領選挙とフェイクニュースの混乱

2020 年 11 月 3 日、第 59 回米国大統領選挙が実施され、共和党 Donald Trump 大統領、民主党 Joe Biden 候補が接戦を演じたが、鍵となるジョージア州、ペンシルベニア州等で優位に立った Biden 候補が 11 月 7 日に勝利を宣言した※231。選挙結果の確定は遅れ、11 月 23 日、Trump 大統領は政権移管手続きを認めた※232 ものの、慣例の敗北宣言をしなかった。同大統領は同年 9 月の時点で郵送による選挙に不正の危険があると SNS で発言、また開票中も「選挙は盗まれた」と不正を訴え、州政府に多くの訴訟を起こしたが、提出された証拠は薄弱であるとして却下された。連邦最高裁判所に提訴された 2 件についても 12 月 8 日、11 日に却下された※233。

こうした Trump 政権の「不正選挙」キャンペーンがフェイクニュースの氾濫、一部 Trump 支持者の過激な行動を誘発した。2021 年 1 月 6 日、連邦議会は Biden 候補の当選を承認する予定であったが、一部 Trump 支持者は力によりこれを防ぐとしてワシントン DC に集結した。Trump 大統領は彼らを扇動する発言を SNS で続け、更に 6 日午後、ホワイトハウス前で同様の演説を行った。これに乗じた支持者は警戒を破って連邦議会に侵入、占拠し、排除において死者 4 名が出る異常事態となった※234。翌 7 日、議会はあわただしく Biden 候補の当選を承認し、Pence 副大統領も Biden 候補の勝利を公式に認めた。また Trump 大統領は選挙の不正を主張し続けたものの「政権の秩序ある移行を行う」と SNS で表明した※235。1 月 20 日、Biden 次期大統領は大統領に就任したが、共和党員の支持はほとんどなく、分断状態となった米国の再統合という難しいかじ取りを迫られることとなった。

以上の経緯により、フェイクニュースの氾濫・誘導が世論を分断し、国家の安定を揺るがしかねないという深刻な課題が浮き彫りとなった。フェイクニュースのリスクはパンデミックで既に顕在化し、SNS ベンダは対策を強化していた。例えば Facebook, Inc.(以下、Facebook 社)は 2020 年 2 月、大統領選挙に向けたファクトチェック強化のため、Thomson Reuters Corp との提携を開始した※236。Twitter, Inc.(以下、Twitter 社)は、危害を加える、または誤解を招く可能性のあるツイートに対する警告ラベルの適用を強化した。2020 年 5 月 26 日、Trump 大統領のツイートに初めて警告し※237、同年 11 月 5 日の時点では、同大統領の「不正選挙」に関する 29 個のツイートのうち 11 個に警告したという※238。こうした警告とそれに伴う SNS サービスの利用制限は、一方で SNS ベンダの越権行為だと批判する声もあったが、フェイクニュースの混乱は加熱し、暴徒による議会占拠が起こってしまった。

ここに至り、Facebook 社は 1 月 6 日、Trump 大統領の Facebook アカウントを無期限に停止した。Twitter 社は同大統領のアカウントを凍結し、支持者応援演説の映像等を削除した上で凍結をいったん解除したが、同月 12 日、「さらなる暴力扇動のリスクを除く」として恒久的に Trump 大統領の Twitter 利用を禁止した※239。

上記 2 社はこれまで「表現の自由」を標榜し、政治家が SNS 上で行う発言には終始寛容であった。しかし 1 月以降、2 社は態度を 180 度転換し、Google LLC(傘下の Instagram 等へのアクセスを制限)とともに利用者に対する最も厳しい措置を取った。この結果、氾濫していたフェイクニュースが劇的に減少し、扇動による混乱が収まったことは事実である。

しかし一方で、この措置は「IT プラットフォーム事業者は個人の言論発表の機会に対して圧倒的な力を持ち得るが、その力の根拠は不明である」という新たな問題を提起し、様々な議論がおこった。例えば利用停止の直後、ドイツの Angela Merkel 首相は「言論の規制は法律に基づくべき」として、SNS ベンダの対応に疑問を呈した。「他に表現手段のない弱い立場の人が投稿を削除されることへの懸念」も表明された※240。特に EU 諸国は、米国の巨大プラットフォーム事業者による EU 域内の私権の制限に対する懸念が強いが、同じ問題は日本にも起こり得る。今後も注視すべき課題であるといえる※241。

なお大統領選挙に関して、AI 技術を悪用した Deep fake によりフェイク動画を作成し、選挙活動に干渉する攻撃が懸念されていたが、重大事案は報告されず、結果的には大きな問題とならなかった※242。

(7) Biden 政権の政策

Biden 政権は、SolarWinds、Microsoft Exchange、Colonial Pipeline の各事案のただ中で発足した。同政権はこれらの事案の収束とサイバーサプライチェーンリスク対応、基幹サービスのセキュリティ強化を中心として、セキュリティ政策を見直していくものと思われる。サプライチェーン再構築について、Biden 政権は「2.2.2. (1) (b)

サプライチェーンリスクと中国との関係悪化」で述べたとおり、2021年2月24日に大統領令を発表し、連邦政府機関と連携して100日以内に各機関のサプライチェーンリスクレビューを実施するとした。更に5月12日、Biden政権は前述のサイバーセキュリティに関する大統領令を発表した。主にサプライチェーンセキュリティ強化を意図したもので、以下の点が注目される。

- 官民の脅威情報共有の障壁除去
  政府システムにおける民間プラットフォーム・サービスの活用が拡大する中で、調達契約で記載するべきセキュリティリスク・対策等の要件とそれを表現する契約用語を明確にすることを求めている。ISACs、ISAOs（Information Sharing and Analysis Organizations）による現体制ではIT/OT事業者、クラウド事業者等が持つ脅威・インシデント情報を関係政府機関が共有できていないとの危機意識があると思われる。
- 連邦政府セキュリティの現代化（Modernization）
  政府システムのセキュリティ刷新はTrump政権からの継続事項となる。本大統領令では多要素認証を含むゼロトラストアーキテクチャの実装、政府共通のクラウドセキュリティ戦略等を新たに求め、政府調達クラウド認証制度FedRAMP（Federal Risk and Authorization Management Program）の現代化にも言及している。
- ソフトウェアサプライチェーンセキュリティの強化
  重要（Critical）なソフトウェアのセキュア開発・調達に関して、NISTを中心とした新たなガイドラインの1年以内の策定を求めている。検討項目にはコードチェック等の自動化、SBOM（Software Bill of Materials、ソフトウェア部品表）の採用等、懸案となってきたものも含まれる。ソフトウェア調達においてはこのガイドラインの遵守状況が審査されるため、どの程度厳しい内容になるか注目される。
  このほか、IoT機器のセキュリティに関する情報を利用者に提供する（Consumer labelling）パイロットプログラムの実施が求められている。

上記大統領令はサプライチェーンセキュリティに関しては包括的で歓迎の声もあるが、どこまで実装可能かは未知数である。また、Colonial Pipeline事案のような重要インフラの脆弱性対策等は含まれていない。Trump政権も発足当初にこのようなレビューと対策立案を実施したが、Biden政権は更に待ったなしの状況で、国家のサイバーセキュリティの火急の見直し・再構築が求められる。

人材面では、Trump政権末期には、不正選挙キャンペーンへの反発から、CISAのChris Krebs長官が更迭される等、セキュリティ人材が政府機関から流出していたが、2021年4月、Biden大統領はCISA新長官に元NSAのJen Easterly氏を、2021年の国防予算大綱である国防権限法（National Defense Authorization Act for Fiscal Year 2021）※243により新設された国家サイバー長官（National Cyber Director）に、同じく元NSAのJohn Chris Inglis氏を指名し、立て直しを図っている※244。

対外的には、Trump政権と同様に中国に対する厳しい姿勢をとりながら、SolarWinds事案で再燃したロシアへの対抗政策が求められる。中国、ロシアはともに米国にとってサイバーセキュリティ上の敵対勢力とみなされる国であるが、両国と同時に衝突することは得策ではなく、Biden政権がどのような交渉を行うか注目される。

2.2.3 欧州の政策

2020年2月1日、英国は正式にEUを離脱※245し、同年12月31日までを移行期間としてEU法制の適用を継続し、その間にEU・英国間の新しい自由貿易協定（FTA：Free Trade Agreement）等を締結することとなった。FTAをめぐる交渉は難航したが、時間切れ直前の12月24日、双方は合意に達した※246。合意文書「EU・英国の通商と協力に関する協定（TCA：EU-UK Trade and Cooperation Agreement）」※247は2021年1月1日に暫定的に発効し、英国は完全にEUから離脱した。同年4月27日、欧州議会（European Parliament）はTCA、及び付随する「EU・英国の情報セキュリティ協定（EU-UK Security of Information Agreement）」（以下、セキュリティ協定）を承認、翌28日に欧州理事会（European Council）がこれを批准し、合意は2021年5月1日から正式に有効となった※248。

一方で、2020年度は欧州各国も新型コロナウイルスによるパンデミック対応に追われ、セキュリティ面では米国同様にインフォデミックやサプライチェーンリスクへの対応が課題となった。以下では、英国を含むEU諸国のセキュリティ・データ保護に関する動向について述べる。

(1) EU・英国の交渉

2020年3月2日、ブリュッセルにてEUと英国の「将来関係交渉（EU-UK future partnership negotiations）」が開始され、11の分科会に分かれて討議（ラウンド）が

行われた※249。なお防衛に関しては、英国の意向で将来関係交渉には含めないこととなった。将来関係交渉の第2ラウンド～第4ラウンドは新型コロナウイルスの影響で主にビデオ会議の形式で行われた。交渉は当初予定の9月では決着せず、7回の延長交渉の末、「合意なき離脱」を避けるための最低限の合意に至った。主要な合意点は以下のようになる※250。

- EU・英国間で関税をゼロとするが、通関手続きは復活する。
- 鉄道・航空・海上輸送等は現状を維持する。
- 英国はEUの統一ルールや欧州司法裁判所の影響から外れ、金融等の規制・監督は独自に行う。
- 英国は公正な競争のためにEUルールを尊重する。
- 公正な競争がゆがめられた場合には必要な措置を取る。

以下では、争点となった課題・セキュリティ関連課題の合意内容について紹介する。

なお、以下の(a)(b)(c)は最後まで難航したが、形の上では英国が粘ってEUの統制をある程度弱めることに成功した点である。その一方、EU・英国間の貿易は煩雑・高コストとなり、英国からのEU単一市場へのアクセスは明らかにハードルが上がっている。

(a)漁業

漁業においては、英国が自国海域の漁獲枠を自国が決めるとしたのに対し、EUは保持している漁業権の維持を主張し、難航した。双方が歩み寄った結果、当面EU漁船の英国海域での操業は許可するが、今後5年間で現行のEUの漁獲割り当ての25%を英国に移行する、2026年6月以降、英国は自国海域でのEU漁船の操業を制限できるが、EU側も対抗策を実施できる等で合意した※251。

(b)公正な競争

公正な競争(Level playing field)とは、EU・英国間で企業の競争が同じ条件で行われることの保証である。EUは、域内企業に対する課税や環境対策・労働環境等の規制、及び補助金制度等について英国が独自に緩和し、域内企業が不利になることを警戒し、例えば英国政府が日産自動車株式会社に示したEU離脱後の保証が懸念材料となった※252。EUは同等の競争環境維持について英国に規則化を要求したが英国はこれを嫌い、交渉は難航した。

最終的には双方が歩み寄り、補助金制度は別々とする一方で双方の制度設計の原則を規定する、労働条件・環境対策の水準を低下させない互恵的約束を規定する、公平性の評価・修正の仕組みを作る等で合意した※253。

(c)ガバナンス

ガバナンスとは、EU・英国間のTCA違反等における紛争解決の統制のことである。EUは欧州司法裁判所による一律の統制を要求したと思われるが、英国はEUの法制度を適用されることに強く反発、国別に締結する経済連携協定（EPA：Economic Partnership Agreement)、FTA等により調停するべき、として難航した。最終的にはEUの法制適用は見送られ、双方がまず協議し、不調なら独立の仲裁パネルが調停を行うことで合意した。

(d)データの妥当性

データの妥当性(Data adequacy)は、EU・英国間の自由なデータ移転のための保護施策を保証することであり、特にGDPR(General Data Protection Regulation)に相当する英国の個人データ保護施策の認定（十分性の認定)が重要である。

英国は、GDPR施行に合わせて同規則遵守の体制を整えていたが、EU離脱前後の政治的混乱等から十分性認定の手続きが遅れ、2021年1月以降のEU・英国間のデータ移転に支障が出ることが危ぶまれていた。TCAではこれに対し、十分性認定が確定するまで最大6ヵ月間、欧州経済領域（EEA：European Economic Area。EUとノルウェー、リヒテンシュタイン、アイスランド等のEU非加盟国で構成）からの英国への個人データ移転を暫定的に認めることとした※254。続いて2021年2月19日、欧州委員会（European Commission）は英国の個人データ保護のレベルがEUの保護レベルと比較して妥当であるとの評価(Adequacy Decision)ドラフトを公表した※255。この評価は、欧州データ保護委員会（EDPB：European Data Protection Board）の助言のもとにEU加盟国、欧州委員会が承認する必要がある。4月16日、EDPBは同評価について、「評価を支持するが、今後の英国の動向を注視する」との意見を表明した※256。具体的な懸念として、移民の入国統制への意図しない個人データ利用、英国のデータ保護方針の変更、法執行機関からのアクセス等に言及している※257が、承認は問題なく行われると思われる。

(e) セキュリティ

EU は、国際犯罪や外交等における共通の安全上の脅威に関し、EU の機密情報を第三者と共有する場合は、個別事案に特化した情報セキュリティ合意（Security of Information Agreement）を求めている。しかし将来関係交渉においては、事案ごとの交渉が煩雑となり得ること等から、機密情報の格付け、保護、第三者開示、相互協力等に関して包括的な規定が作成された（前出のセキュリティ協定※258）。本セキュリティ協定の内容は非常に基本的なもので、TCA の改廃に連動する等、あくまで TCA に付随する扱いである。2020 年 12 月 24 日の最終討議で TCA とともに合意された。

一方、サイバーセキュリティは将来関係交渉の議題とならなかった。「情報セキュリティ白書 2020」の「2.2.3 欧州の政策」で述べたとおり、英国は EU の NIS 指令（Network and Information Security Directive）に対応する国内法も整備済みであり、EU 加盟国との連携も既存の枠組みでできていることから、従来どおりの連携が進むものと思われる。

(2) 新型コロナウイルスへの対応

欧州においても、2020 年 1 月以降、新型コロナウイルス感染が拡大し、各国は対策に追われた。

(a) 感染状況

欧州でのパンデミックはまず 2020 年 1 月末に中国からの渡航者が滞在したイタリア北部地域で発生、3 月 9 日にはイタリア全土にわたるロックダウンが開始された※259。フランスでも同年 2 月後半から感染者が急増し、同年 3 月 16 日、Emmanuel Macron 大統領は少なくとも 15 日間の全国的なロックダウンを要請した※260。

ドイツでも 1 月下旬の感染発覚以来感染者が急増し、3 月 13 日には各州の学校・幼稚園が閉鎖、16 日には国境管理の厳格化とともに各州におけるロックダウンの強化※261、17 日には EU 委員会提案に基づく EU 域内への 30 日間の入域制限が実施された。

英国政府は、2020 年 3 月初旬の時点では「科学に基づき、国民に免疫をつけさせることが有効」とし、ロックダウン等の強い施策を行わない方針であったが、医療専門家の批判を受けてこれを撤回、3 月 23 日に Boris Johnson 首相が「Stay at home」を要請した※262。

上記以外の欧州諸国も同様な対応を余儀なくされた。欧州各国は上記のパンデミック第 1 波の後、10 ～ 12 月の第 2 波、2021 年 3 ～ 4 月の第 3 波に襲われ、それぞれロックダウン等を迫られている。

なおこの間、英国では 2021 年 1 月からのワクチン接種が急速に進み、2021 年 4 月末時点で少なくとも 1 回接種した人は 3,436 万人を超えた。また 2021 年 1 月初旬に 6 万人超であった 1 日の感染者数が 4 月末時点で 2,300 人弱に減少している※263。

パンデミックの原因について、米国・欧州は 2020 年 1 月末時点から中国武漢市が起点であったとし、中国の情報開示の不十分さや自国のビジネスを優位にするかに見える対策支援の姿勢に不審感を抱いた。EU と中国は 2019 年までは 5G 関連の IT インフラ導入等で親密といえる関係にあったが、パンデミックによる中国への不信、グローバルサプライチェーンの中国依存体質の見直し、更には香港や新疆ウイグル自治区における人権問題により中国との関係は冷却し、英国と EU 諸国はこれを見直そうとしている。

(b) セキュリティ対策

パンデミックの影響で在宅勤務が増加し、詐欺情報やデマ情報が蔓延した状況は欧州も米国と同様である。欧州ネットワーク・情報セキュリティ機関（ENISA：The European Union Agency for Cybersecurity）は、各国のロックダウンが本格化した 2020 年 3 月 24 日、テレワークのセキュリティと新型コロナウイルス関連のフィッシングに注意喚起を※264、同月 31 日にはネットショッピングの急増に対し、フィッシングや決済の不正等に対する注意喚起を※265 行った。しかし 3 月以降、欧州のフィッシングメールによる攻撃件数は 1 ～ 2 月の 6 倍以上に急増し、5 月 6 日、再度注意喚起をせざるを得なくなった※266。ENISA はまた、4 月 24 日にオンライン会議ツール選択に関する注意喚起を行った※267。注意喚起では、欧州らしい特徴として、セキュリティに加え個人情報保護への配慮が注意点に含まれている。

(c) インフォデミック対策

フィッシングへの対処の一方、新型コロナウイルスの感染対策やワクチン接種、更には米国大統領選挙に関する虚偽情報・悪意の情報（フェイクニュース）による混乱・扇動（インフォデミック）に対し、欧州は厳しい態度をとり続けている。2020 年 12 月 3 日、欧州委員会はフェイクニュースによる政治活動過激化への対策として「欧州民主主義行動計画（European Democracy Action Plan）」（以下、行動計画）を発表した※268。行動計画は、「デジタル空間において、虚偽や悪意を排した事実に基づき、

自由でオープンな意見表明と討議を可能にし、欧州の民主主義を強化する」として、以下の3点について施策を講ずるとしている。
①自由で公正な選挙の推進
②メディアの自由と多元主義の強化
③虚偽・有害情報対策

①については、2016年、マイクロターゲティング技術を用いる選挙コンサルティング会社Cambridge Analytica Ltd.が英国の国民投票や米国大統領選挙に干渉したとされる事案や、英国のEU離脱国民投票をめぐる扇動、米国大統領選挙をめぐる扇動等の苦い経験から、政治広告への規制を行う、としている。

②については、加盟国においてジャーナリストの物理・サイバー両面の活動に対する外部の圧力が高まっているとし、ジャーナリスト（特に女性）の安全を確保し、メディアの多元性の強化を加盟国と推進する、としている。ここでいう外部の圧力・多元性の強化には、明言されないが、中国・ロシアの言論封殺や干渉に対する警戒があり、中国・ロシア資本によるメディアの所有や政治広告等に対する監視を強めるものと考えられる。

③については、欧州委員会が2019年に策定し、米国のプラットフォーム事業者が合意したSNS、ネット広告等における虚偽・有害情報に関する行動規範※269（Code of Practice on Disinformation、以下、行動規範）を強化するもので、欧州のデジタル市場戦略と重なる点で①②とは別の意味を持っている。行動計画では、現在義務化されていない行動規範を準規則化（co-regulatory framework）し、プラットフォーム事業者の監視を強める、としている。また行動規範の強化は、現在欧州委員会が策定中のデジタルプラットフォーム規制法「デジタルサービス法（Digital Services Act）」と整合させる、としている。同法法案は2020年12月15日、欧州議会に提出された※270。

「2.2.2 (6) 大統領選挙とフェイクニュースの混乱」で述べたように、2021年1月にTwitter社やFacebook社がTrump大統領（当時）のSNS利用を停止したことは、個人の言論を封じるような制裁を、法的権限を持たないプラットフォーム事業者が実施できるのかについて議論をまき起こした。これについて欧州は、消費者保護（域内市民保護）と競争確保の点から一貫してプラットフォーム事業者規制の立場をとっている。上記の行動計画やデジタルサービス法、及び並行して策定されているデジタル市場法（Digital Markets Act）※271により、欧州の描く公平・公正なデジタル市場の統制の形が見えてくると考えられる。

(3) GDPRの運用状況

GDPRの運用を行うEDPBや、各国のデータ保護委員会（DPA：Data Protection Authority）にとって、新型コロナウイルス感染対策は2020年度の重要課題となった。

(a) 新型コロナウイルス対応

新型コロナウイルス対応における個人データ管理についてEDPBは2020年3月16日に声明を発表し、企業・医療機関における同意なしの個人データ取得等の例外はGDPRが包括的に規定していること、位置情報は匿名化を基本とするが、例外処理が必要な場合は策定中のeプライバシー法（ePrivacy Directive）に準拠すべきこと、を明記した※272。EDPBは続けて5月9日、位置情報及び接触追跡ツールに関するガイドライン※273、研究目的の健康情報処理に関するガイドライン※274を公開した。その後欧州各国も、個人の行動や新型コロナウイルス感染の有無等のデータ管理に関するガイドラインを相次いで公開した。

2020年後半以降は、新型コロナウイルスに対するワクチン開発への期待から、移動制限・入国制限を緩和するための「ワクチン接種証明」が注目され、議論が継続している。海外渡航に必要なワクチン接種証明書の発行はWHOの管轄であるが、WHOは新型コロナウイルスに対するワクチン接種証明書には慎重であるといわれる※275。理由としては、疫学的エビデンスの不足、ワクチン供給に関する不公平、関係法制の不備、個人情報保護やデータ管理等の規格の共通化等の課題が挙げられている。

こうした懸念をよそに、欧州委員会はEU域内の自由で安全な移動を保証するワクチン接種証明書（Digital Green Certificate）の検討を進め、2021年3月17日、関連法案を発表した※276。同法案では、この証明がワクチン非接種者への差別要因とならないように、感染していないことの証明、感染から回復したことの証明を含める、記録する個人情報は最小限にする等としている。また接種証明は、EUが承認したワクチンが対象となるが、加盟国が独自にワクチンを追加してもよいとしている。

その一方、接種証明を政府がどのように使うのか、例えばある国のワクチンは承認しないとした場合（実質的なEU域内入国制限になる）の政治リスク、接種しない人

が差別される倫理面のリスク、ワクチンの効果に差があった場合の対応、証明書発行手続きにおけるプライバシー保護の合意等、様々な懸念が表明されている※277。

またイタリア政府は、国内の新型コロナウイルス感染の高リスク地域への移動を緩和するため、独自の「ワクチンパスポート」の導入法案を準備している※278。2021年5月4日、イタリアのDPAであるGaranteが同法案について、個人データ処理に伴う人権、プライバシー保護上の検討不備があるとして懸念を表明した※279。

こうした懸念に対し、欧州評議会(Council of Europe)は2021年4月14日、加盟国政府の接種証明導入における人権保護ガイダンスを公開した※280。

(b)GDPRの運用

GDPRの実際の運用は2018年5月の発効から2年半以上を経過し、厳格さを増している。2020年7月16日、欧州司法裁判所は、2016年以来米国とEUの間の包括的データ移転の枠組みであった「プライバシーシールド」が無効である、すなわち、米国に移転された個人データの保護はGDPRと同等のレベルにない、との判断を示した※281。これはFacebookからの個人情報流出に反発したEU域内利用者の訴訟に対する判決である。同判決ではGDPRの標準契約条項(SCC:Standard Contractual Clauses)による代替策は有効である、とされたものの煩雑となり、EU域内のデータを米国のAIで分析する等のサービスに影響が出ると思われる。

GDPR違反の摘発については、調査によれば2020年1月28日から2021年1月28日までの制裁金総額(1億5,850万ユーロ、約206億円)は、それ以前の20ヵ月の総額に比べ40%増加した。その一方、違反届け出件数等は国により開きがあり、パンデミックで経営が厳しくなったBritish Airways Plcの制裁金(2018年に1億8,300万ポンド、約245億円を課された)が2020年10月、2,000万ポンド(約27億円)に減額される※282等、画一的な運用はされていないという※283。このほか、2020年度に高額の制裁金が課された事例としては以下のものがある。

2020年7月13日、前出のGaranteは電話事業者Wind Tre S.p.A.に対し、ダイレクトマーケティングに関する利用者の同意のとり方についてGDPR違反があったとし、1,670万ユーロ(約21.7億円)の制裁金を課すと公表した※284。

同年10月2日、ハンブルク市のDPAであるThe Hamburg Commissioner for Data Protection and Freedom of Informationは、衣料小売企業H&M Hennes & Mauritz Online Shop A.B. & Co. KGに対し、従業員数百人の病歴等を含むプライベートな情報の登録を少なくとも2014年以来強制し、同社マネージャー50人がこの情報にアクセス、評価に利用していたとし、3,526万ユーロ(約45億8,300万円)の制裁金を課した※285。2019年にフランスのDPAであるCNIL(Commission nationalede l'informatique et des libertes)がGDPR発効直後、Google LLCに課した制裁金5,000万ユーロ(約65億円)に次ぐ高額となった※286。

更に10月30日、英国のDPAであるICO(Information Commissioner's Office)はMarriotto International Inc.(以下、Marriotto社)に対し、傘下のStarwood Hotels and Resorts Worldwide Inc.(以下、Starwood社)における延べ3億3,900万人に及ぶ顧客情報流出について、1,840万ポンド(約25億円)の制裁金を課した※287。本事案は英国のEU離脱前の2018年に発覚してGDPR違反の査察対象となり、ICOの調査の結果、Marriotto社が2015～2016年にStarwood社を買収した時点のセキュリティ体制整備に問題があったとしたが、Marriotto社による申し立てやパンデミックによる経営悪化の影響も加味して、当初9,920万ポンド(約135億円)とされた制裁金は減額された。この経緯は前述のBritish Airways Plcの事案でも同様である。

(4)新たなサイバーセキュリティ戦略

欧州委員会は2020年12月10日、「誰もが安全なデジタル生活を送る」ために、以下を柱とする「デジタル時代のサイバーセキュリティ戦略」を発表した※288。

- 基盤サービスとつながるモノのセキュリティ確保
- 主要なサイバー攻撃への対応能力強化
- 世界のパートナーとの連携

大方針としては従来の戦略と大きな差があるように感じられないが、基盤サービスとしての医療、エネルギー、交通等の重視、つながる機器を守るためのサプライチェーン重視、それに関わる海外パートナーとの連携、コロナ禍からのリカバリー施策としてのセキュリティ投資強化が主眼であると思われる※289。

更に欧州委員会は翌11日、欧州議会の承認を受け、上記戦略を推進する組織Cybersecurity Competence Center and Networkをブカレストに設置することを発表した※290。同組織はENISAとは別に、EUのデジタル投

資・研究投資ファンドである Digital Europe Programme、Horizon Europe を財源として中長期的なサイバーセキュリティ投資を行うとしている。同組織の提案は 2018 年時点で行われており[※291]、EU 域内産業のデジタル化・技術革新におけるサイバーセキュリティ重視の姿勢が感じられる。

(5) 重要インフラに関するセキュリティの状況

2016 年に発効し、ENISA が実践を統括する NIS 指令は、重要インフラセクターの共通なセキュリティ指針となっているが、以下では医療セクター・通信セクターに向けた ENISA の活動、及び関連する関係諸国の動向を紹介する。

(a) 医療セクターのセキュリティ

医療セクターのセキュリティ確保は 2020 年、大きな焦点となったが、ENISA は同年 2 月、医療機器・システム調達におけるセキュリティ確保のガイドラインを公開した[※292]。機器調達の計画・実施・運用におけるセキュリティについて、29 個のプラクティスが紹介されている。また 2021 年 1 月 18 日、医療クラウドのセキュリティに関する報告書が公開された[※293]。同報告書では、医療のクラウド化で対応すべき電子健康データ（EHR：Electronic Health Record）の収集と管理、遠隔治療、医療機器操作に対するセキュリティリスクアセスメント結果が示されている。

欧州における医療のデジタル化（eHealth）は、エストニアで先進サービスが試みられる一方、ドイツ・フランスでは EHR の扱いに慎重であり、対応は一様ではないが、コロナ禍や医療への AI 利用等により、今後デジタル化が加速する可能性がある[※294]。なお、ENISA は 2020 年 12 月 15 日、AI のセキュリティに関するエコシステムと脅威に関する報告書を公開した[※295]。機械学習を用いる AI の設計・開発・運用のライフサイクルに沿って、関係するエコシステム・サプライチェーンで生じ得る脅威の分析を行っている。

(b) 通信セクターのセキュリティ

2020 年 12 月 14 日、ENISA は 5G ネットワークに関する脅威分析の改訂を行った[※296]。公開された脆弱性情報等に基づき、2019 年 11 月発行のレポートを改訂したものである。続いて 2021 年 2 月 24 日、3GPP[※297] が規定した 5G のセキュリティ管理策に関する報告書を公開した[※298]。5G 機器ベンダ・サービス事業者（通信キャリア）・政府機関への規格実装のプラクティスを示し、5G 規格の複雑さへの対処に注意を促している。

「2.2.3 (2) (a) 感染状況」や「情報セキュリティ白書 2020」の「2.2.3 欧州の政策」で述べたとおり、2020 年、パンデミックに関する情報開示や人権侵害等の問題により欧州各国と中国との関係は冷却し、米国の制裁措置にならい、キャリア通信網からの中国ベンダ機器排除の動きが加速した。ただし、2021 年 4 月の時点では、各国の対応に濃淡が見える。

最も厳しい対応をしたのが英国である。英国政府は 2020 年 7 月 14 日、Huawei Technologies Co., Ltd.（以下、Huawei 社）、ZTE Corporation の 5G 機器の新規調達を同年 12 月末から禁じ、既存の中国製機器も 2027 年までに撤去することとした[※299]。更に政府は 11 月 24 日、通信事業者が調達する機器やベンダに対するセキュリティ要件を厳格化する法案（Telecommunication Security Bill）を議会に提出した[※300]。同法案では「ハイリスクベンダ」の排除、通信事業者のセキュリティ監査の強化、違反時のペナルティ等が明記されている。スウェーデン・フランスもこのような排除を前提とする対応を行っている。

一方ドイツは、どのベンダも 5G 機器調達から排除しないという方針を維持している。2020 年 12 月 16 日、ドイツ政府は、国内の IT セキュリティ基本法である「IT セキュリティ法 2.0」を閣議決定した[※301]。同法案には、重要インフラ事業者の調達における監督官庁の認可制度等、セキュリティ規制の強化が盛り込まれる一方、ハイリスクベンダの排除は含めず、調達可否は監督官庁の査閲に委ねられた。過去においてドイツの通信事業者が Huawei 社の機器を運用してきた経緯によると思われるが、排除を前提とする同盟国等とのデジタルプラットフォーム統合に関する軋轢、あるいは EU が希望する北大西洋条約機構（NATO：North Atlantic Treaty Organization）への米国のコミットメント強化に対する影響が懸念されている[※302]。

2.2.4 アジア太平洋地域でのCSIRTの動向

アジア太平洋地域の多くの国で、各国のインシデント対応連携の窓口となる National CSIRT が既に設立され運用されている。ここ数年は、サイバーセキュリティ戦略や新たな法律によって、National CSIRT 及び所管省庁の権限を強化したり、役割を明文化したりする動きが継続している。本項では、アジア太平洋地域におけ

るCSIRTの機能強化やインシデント対応の新たな取り組みに関する動き、CSIRT間の相互連携の実態について述べる。

(1) CSIRTの機能強化の動き

アジア太平洋地域における各国・地域のCSIRTの機能強化の動きについて述べる。

(a) オーストラリア

2020年8月6日、オーストラリアの内務省(Department of Home Affairs)から2020年版のサイバーセキュリティ戦略[※303]が発表された。これは2016年に発表された同戦略の更新版である。国民生活や企業活動のために安心安全に利用できるサイバー空間を創造するため、向こう10年間で16億7,000万豪ドル(約1,300億円余り)を計上することが盛り込まれている。National CSIRTの機能を担うACSC(Australian Cyber Security Centre)[※304]にも、そこから多くの予算が割り当てられ、機能が更に拡充される計画である。例えば、海外から同国を狙うサイバー犯罪の対策強化、重要インフラ事業者におけるセキュリティアセスメント及び対策の徹底、主に女性を対象としたサイバーセキュリティ教育やトレーニング機会の創設等にACSCが取り組むとされている。

(b) シンガポール

National CSIRTであるSingCERT[※305]を管轄するCSA(Cyber Security Agency:サイバーセキュリティ庁)[※306]は、2020年10月6日に「Singapore's Safer Cyberspace Masterplan 2020[※307]」を公開した。この文書には、「核となるデジタルインフラの保護」「サイバー空間での活動の安全性の確保」及び「サイバーセキュリティについて知識を持つ人たちの活躍」という三つの大目標と、それに付随する計11項目の取り組みが記載されている。例えば、「サイバー空間での活動の安全性の確保」の中では、AI(人工知能)を活用し、サイバー空間での不正な行為を迅速に検知し対応することが挙げられている。具体的には、AIを活用して情報を集約分析し、より重要度の高いインシデントをトリアージする機能を備えたサイバー・フュージョン・プラットフォームをCSAが創設する計画である。またIoTの分野では、グローバルな脅威動向や脆弱性の情報をモニタリングし攻撃の早期検知及び対応を行うために、CSAがIoTの脅威情報を関係組織と共有し分析するIoT脅威分析プラットフォームの運営が計画されている。関係組織と協同して分析することで、IoT機器に対する大規模な攻撃を事前に検知し、影響を把握することが可能になるという。それらに加えて、サイバー衛生[※308]に関するポータルサイトの作成、国内の中小企業に対するサイバーセキュリティ対策の支援、啓発活動の充実、5Gセキュリティの推進等にCSAが取り組むとされている。

(c) マレーシア

2020年10月、マレーシアのNACSA(National Cyber Security Agency:国家サイバーセキュリティ庁)[※309]は2020年から2024年にかけてのサイバーセキュリティ戦略[※310]を公開した。この戦略には、サイバーセキュリティに関する「ガバナンスとマネジメントの効率化」「法制度設計と施行の強化」「世界に通用するイノベーション、技術、研究、産業の促進」「能力開発、啓発、教育の促進」及び「国際連携」という五つの柱が掲げられている。「国際連携」の項では、国際連合やASEAN等の多国間のサイバーセキュリティに関する連携に積極的に参加し貢献を続けると明記している。この中には、National CSIRTの役割を担うCyberSecurity Malaysia[※311]が2020年現在議長を務めるAPCERTや、事務局を務めるOIC-CERT(Organisation of The Islamic Cooperation – Computer Emergency Response Teams)[※312]での活動も明記されており、今後もこれらのコミュニティにおける同組織のリーダーシップが期待される。

(d) 韓国

韓国のKrCERT/CC[※313]は、毎年国内のセキュリティ関連企業と協力し、今後猛威を振るう脅威を予測して「7大サイバー脅威」として公開している。2020年は、初めての試みとしてアジア太平洋地域のCSIRTに協力を募り、呼びかけに応じたAusCERT(オーストラリア)[※314]、CERT-In(インド)[※315]、Sri Lanka CERT|CC(スリランカ)[※316]と共同で、12月に「Cyber Threat Signal 2021[※317]」を公開した。この中で、AusCERTはEmotetを中心としたウイルスのばらまきキャンペーンを脅威の一つに挙げ、CERT-InはVPN機器等リモートワーク環境に対する攻撃が増える可能性を指摘している。またKrCERT/CCは企業から流出した情報のダークウェブ上での売買について、Sri Lanka CERT|CCは巧妙化するビジネスメール詐欺(BEC:Business Email Compromise)について警鐘を鳴らしている。

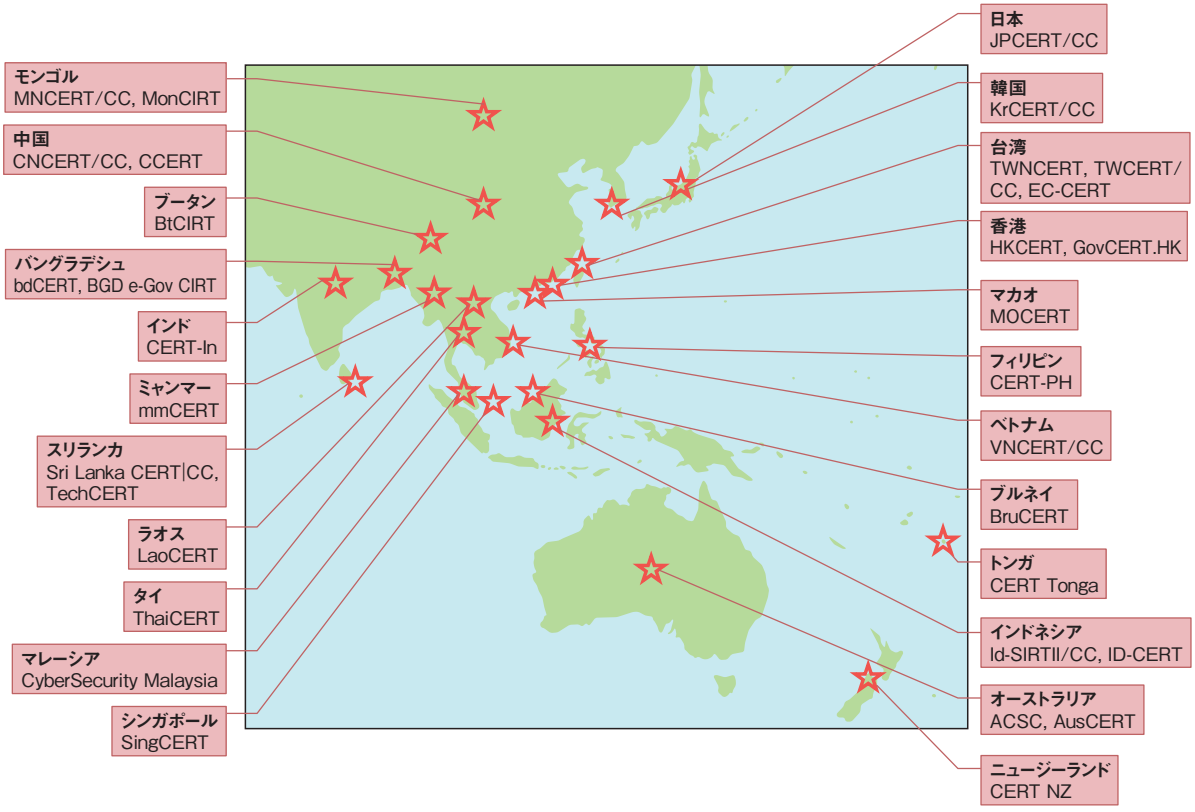
(2) アジア太平洋地域の CSIRT 間連携

アジア太平洋地域全体の CSIRT からなるコミュニティとして、APCERT（Asia Pacific Computer Emergency Response Team：アジア太平洋コンピュータ緊急対応チーム）[※318] があり、地域内で発生したインシデント対応における連携の円滑化や、サイバー脅威等に関する情報共有・技術交流の推進を目的に活動している。2003年の設立当初、参加メンバーは 12 の国・経済地域の 15 チームだったが、地域内で National CSIRT の立ち上げが進んだことや、CSIRT コミュニティへの参加を通じた情報共有等の重要性が高まったことから年々メンバーが増え、2020 年には南太平洋地域から初めてトンガの CERT Tonga [※319]、並びにフィリピンの CERT-PH [※320] 等が新たに加わった。2021 年 3 月末現在、23 の国･経済地域の 33 チームが、オペレーショナルメンバーとなっている（図 2-2-1）。

JPCERT/CC は、2003 年の APCERT 設立当初から事務局を務め、運営委員会の一員として組織運営を支えている。また、JPCERT/CC が主導するネットワーク定点観測共同プロジェクト「TSUBAME」に参加する APCERT メンバーも多く、APCERT 内にワーキンググループを設けて、センサーを用いたサイバー脅威動向の観測や情報共有を推進している。2021 年 3 月末現在、TSUBAME には APCERT メンバーを中心に 19 の国･経済地域から 24 チームが参加し、観測結果を共有している[※321]。

APCERT の主な活動は、年次サイバー演習の実施、年次報告書の発行及び年次会合の開催である。2020 年のサイバー演習は、「Banker Doubles Down on Miner（仮想通貨と金融機関）」をテーマに実施された[※322]。同演習には、APCERT のオペレーショナルメンバーのうち合計 19 の国・経済地域から 25 チームが参加した。年次報告書は、APCERT 全体の活動に加えて各チームの組織概要や、対応したインシデント統計等をまとめた文書で、Web サイトで公開されている[※323]。2020 年の年次会合は、新型コロナウイルス感染拡大の影響により、9 月に初めてオンラインで開催された。2019 年から議長を務めるマレーシアの CyberSecurity Malaysia が議長に、中国の CNCERT/CC [※324] が副議長にそれぞれ再選された。

このほか、APCERT では能力開発の取り組みとして、電話会議システムを利用してインシデント対応に関するノウハウを教えるオンライントレーニングを 2014 年以来継続している。新型コロナウイルス感染拡大が続き、対面で



■図 2-2-1　APCERT オペレーショナルメンバー（2021 年 3 月末現在）

のトレーニング開催が困難な中でも、こうしたオンラインで連携する取り組みを継続している。

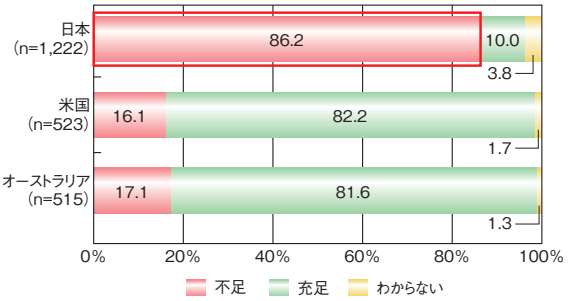
また、日本政府が出資してタイのバンコクに設立された AJCCBC（ASEAN Japan Cybersecurity Capacity Building Center：日 ASEAN サイバーセキュリティ能力構築センター）※325 は、2020 年 12 月に「Cyber SEA Game」と呼ばれる CTF イベントをオンラインで開催した※326。

その他のアジア太平洋地域のサイバーセキュリティ関連イベントの多くが、各国の National CSIRT が主催するカンファレンスを含め、2020 年はオンライン形式に移行して実施された。対面の会議や情報交換の機会が制限されている状況下でも、こうした場をとおして CSIRT 間の連携は継続して行われている。

2020 年中に JPCERT/CC に寄せられたインシデント報告件数は、特にフィッシングサイトに関するものを中心として、前年より高い水準で推移した。また、その内訳を見ると、インシデント拡大防止を目的とした調整のため、海外の CSIRT 等に通知を行ったケースも多かった※327。このようなインシデントへの対応を効果的に進めていくためには、諸外国や特に近隣地域の CSIRT と結束力を高めて連携していくことが必要であり、CSIRT コミュニティをとおした協力が更に推進されることが期待される。

2.3 情報セキュリティ人材の現状と育成

国内のサイバーセキュリティに関わる人材は質的にも量的にも不足しており、人材育成は各界が協力して解決すべき問題である。教育の充実、高度な人材の育成・確保、セキュリティ人材が将来にわたって活躍できる社会環境の整備等、様々な課題が挙げられている。本節では、セキュリティ人材の現状と、産学官における人材育成の取り組みについて述べる。



■図 2-3-1　セキュリティ対策に従事する人材の過不足感
(出典)NRI セキュアテクノロジーズ株式会社「NRI Secure Insight 2020※329」を基に IPA が編集

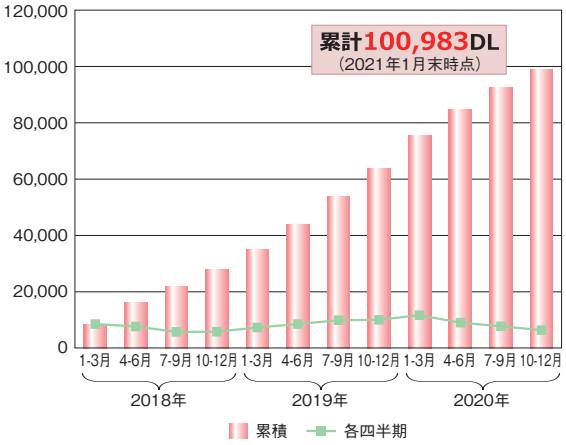
2.3.1 情報セキュリティ人材の状況

ここ数年来、政府や民間の組織において国内のセキュリティ人材育成のための活動が行われてきた。ユーザ企業、IT ベンダ・セキュリティベンダによりセキュリティ関連タスクの概念整理が行われ、ユーザ企業におけるセキュリティ体制については、経営層、戦略マネジメント層、実務者層・技術者層等に整理された。

2018 年度から、実際に人材育成を進める活動として、セキュリティ人材の役割定義に紐付くタスク・スキルの洗い出しを行うとともに、具体的に人材育成を行う試みの有効性に関する検討が行われてきている。

2020 年度においては、コロナ禍によるテレワークや DX の推進に拍車がかかる中、求められるセキュリティ人材の状況にも変化があり、ビジネスあるいは経営の観点でセキュリティ対策を理解し、実践する能力を持った人材への関心が高まりつつある。

このような背景を踏まえて、各所で計画・実施されている活動の概要を紹介する。



【参考】上場企業数　第一部　2,157社　第二部　488社　(日本取引所グループ公表 2019年12月17日時点)

■図 2-3-2　サイバーセキュリティ経営ガイドライン V2.0 のダウンロード数推移
(出典)経済産業省「事務局説明資料※331」(第 7 回 産業サイバーセキュリティ研究会 ワーキンググループ 2(経営・人材・国際) 資料 3)を基に IPA が編集

(1) セキュリティ人材不足に関する認識

米国 NIST の NICE(National Initiative for Cybersecurity Education)において発行されたニュースレターによると、セキュリティ関連職種の雇用需要は、2018 年から 2020 年にかけて、約 71 万 6,000 人から 92 万 3,000 人と、約 29% も増加しており、セキュリティ人材の供給は順調に成長しているにも関わらず、充足できていない雇用は 62% にまで達している状況である※328。日本はそのような状況にある米国と比較しても、セキュリティ人材の不足感が更に大きく、セキュリティ人材が不足している状況である(図 2-3-1)。

「サイバーセキュリティ経営ガイドライン」の普及(図 2-3-2)や、一般社団法人日本経済団体連合会(以下、経団連)の「経団連サイバーセキュリティ経営宣言※330」等により、サイバーセキュリティが経営課題であることが徐々に浸透していることから、様々な組織においてセキュリティ関連の役割を担う人材への需要は更に増えていると推定される。

NISC のまとめによれば、どのような種別の人材が不足しているかについて、2018 年では、1 位は「ログを監視・分析して、危険な兆候をいち早く察知できる」、2 位が「セキュリティ戦略・企画を策定する人」であったが、2019 年、2020 年は、1 位が「セキュリティ戦略・企画を策定する人」となっており、不足する人材の分野が、実務者層・技術者層から戦略・企画を担当する人材に変わってきている(次ページ表 2-3-1)。

	2018 年	2019 年	2020 年
1 位	ログを監視・分析して、危険な兆候をいち早く察知できる 57.0%	セキュリティ戦略・企画を策定する人 47.2%	セキュリティ戦略・企画を策定する人
2 位	セキュリティ戦略・企画を策定する 52.7%	セキュリティリスクを評価・監査する人 34.1%	セキュリティリスクを評価・監査する人
3 位	セキュリティインシデントへの対応・指揮ができる 44.1%	ログを監視・分析する人 34.1%	ログを監視・分析する人

セキュリティ対策にあたる実務者層・技術者層
戦略・企画を担当する人材
(データ出所)NRI セキュアテクノロジーズ㈱「企業における情報セキュリティ実態調査」より NISC 作成

■表 2-3-1　不足している人材の種別
(出典)NISC「人材の確保、育成、活躍促進に向けた今後の検討の方向性について(全体像)※332」を基に IPA が編集

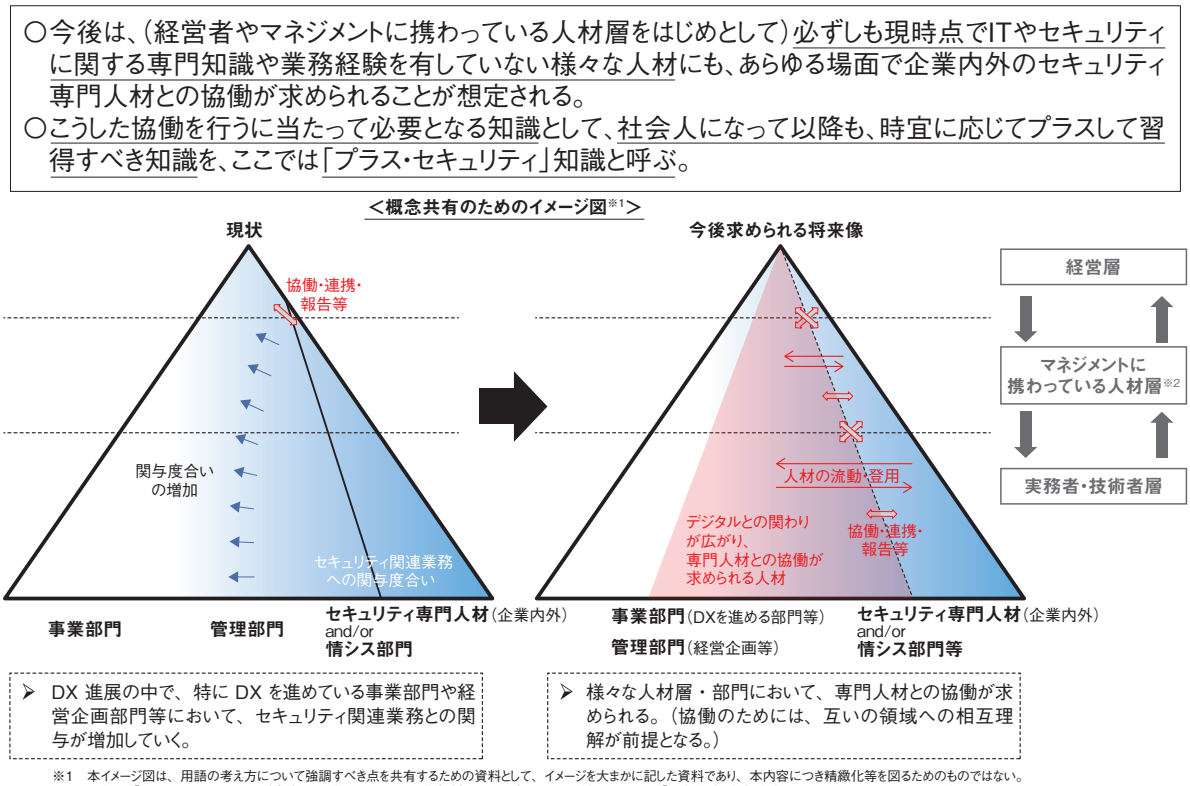
経済産業省の「デジタルトランスフォーメーションに向けた研究会」による「DX レポート※333」では、レポート中の「2025 年の崖」を克服する DX 実現シナリオにより変革された際の展望として、ユーザ企業とベンダ企業間の IT 人材分布は現在の 3:7 から、欧州並みの 5:5 になるとしている。

実際、株式会社デンソー※334、大和総研グループ※335、住友化学株式会社※336 等先進的なユーザ企業では、従来、情報システム部門を本社機構から切り離し情報子会社としていた体制を変更し、本社へ吸収・合併する事例が出始めている。

DX 推進とともに IT 人材の所属が変わり、IT ベンダ、情報子会社から、ユーザ企業へのシフトが起こりつつある。今後はユーザ企業も含め、セキュリティ人材の育成を考慮すべきである。

(2) NISC の取り組み

NISC では、2020 年 7 月に「普及啓発・人材育成専門調査会(第 13 回会合)」を開催し、DX 時代におけるサイバーセキュリティ人材の確保、育成、活躍の促進に係る政策課題について検討を始めた。DX の進展が予想される中、DX と同時にサイバーセキュリティ対策を組み込んでいくこと(DX with Cybersecurity)が求められているとしている。検討すべき三つの政策課題の一つとして、「DX に必要な『プラス・セキュリティ』知識を補充できる環境・人材育成の推進」を掲げており、2018 年の「サイバーセキュリティ戦略※337」で提言した戦略マネジメント層の確保・育成の一つのアプローチと考えられるとし



※1　本イメージ図は、用語の考え方について強調すべき点を共有するための資料として、イメージを大まかに記した資料であり、本内容につき精緻化等を図るためのものではない。
※2　現行の「サイバーセキュリティ戦略」(2018 年 7 月 27 日閣議決定)によれば、こうした人材層において、「経営戦略、事業戦略におけるサイバーセキュリティに係るリスクを認識し、経営層の方針を踏まえた対策を立案し、実務者・技術者を指導できる人材」が「戦略マネジメント層」と定義されている。

■図 2-3-3　「プラス・セキュリティ」知識の考え方
(出典)NISC「政策課題2 DX に必要な『プラス・セキュリティ』知識を補充できる環境・人材育成の推進※338」

ている。

NISC はまた、「プラス・セキュリティ」の考え方の概念的な表現として、セキュリティ専門人材と事業部門においてセキュリティ関連業務に関わるプラス・セキュリティの知識・役割を持つ人材の関係を示しており、相互に協働が必要であるとしている（前ページ図 2-3-3）。

NISC では、DX with cybersecurity を進めていく上で必要なプラス・セキュリティ知識を持った人材を育成するために必要な教育カリキュラムの検討を進めモデル化するとしている。また、企業において DX に対応した体制構築を行う際の参考となるように、ITSS+（セキュリティ領域）[※339] で定義されているセキュリティ関連タスクを担う分野において、どのようなプラス・セキュリティ知識が必要となり得るかを示している（図 2-3-4）。

これらの検討結果は、次期サイバーセキュリティ戦略に盛り込まれ、推進されるものと思われる。

(3) 経済産業省の取り組み

経済産業省のセキュリティ人材育成の取り組みについて述べる。

(a) 産業サイバーセキュリティ研究会 WG2（経営・人材・国際）

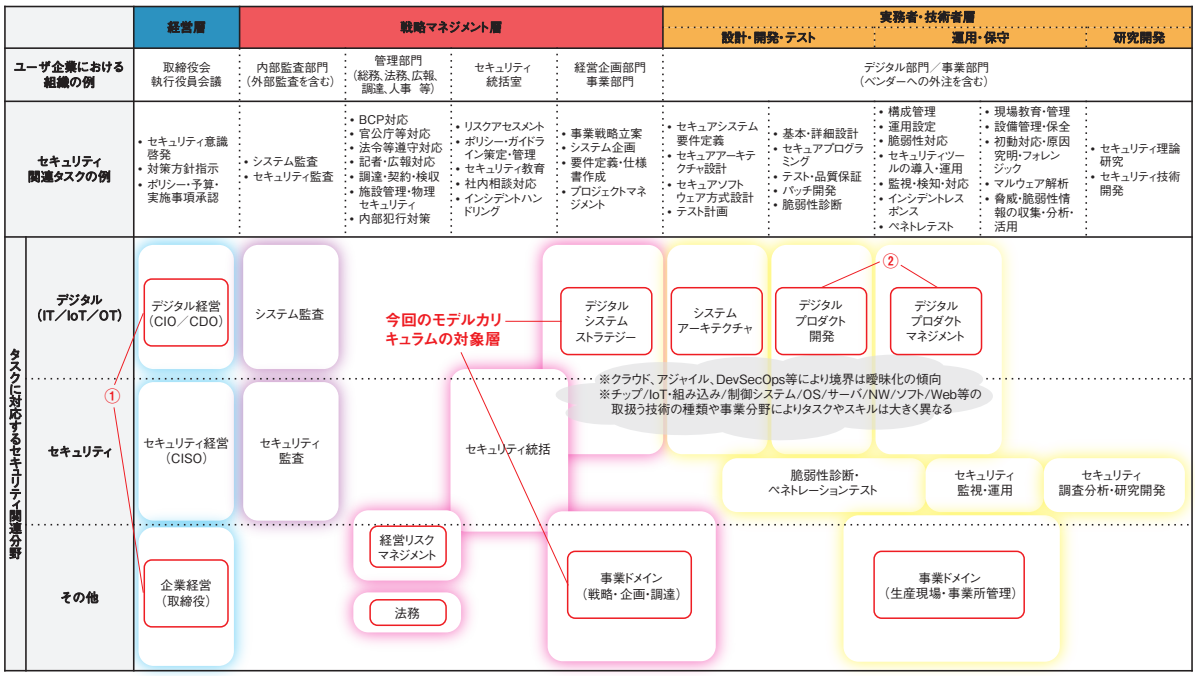
経済産業省では、産業サイバーセキュリティ研究会において、サイバー・フィジカル・セキュリティ対策フレームワークを軸として、各種取り組みを整理している（次ページ図 2-3-5）。

人材育成に関わる対策として、「サイバーセキュリティ経営ガイドライン」をより具体的に活用するための支援ツールの拡充並びに、産学官連携を推し進める取り組みが行われており、「サイバーセキュリティ人材育成・活躍促進パッケージ」として、以下の三つの施策が進められている。

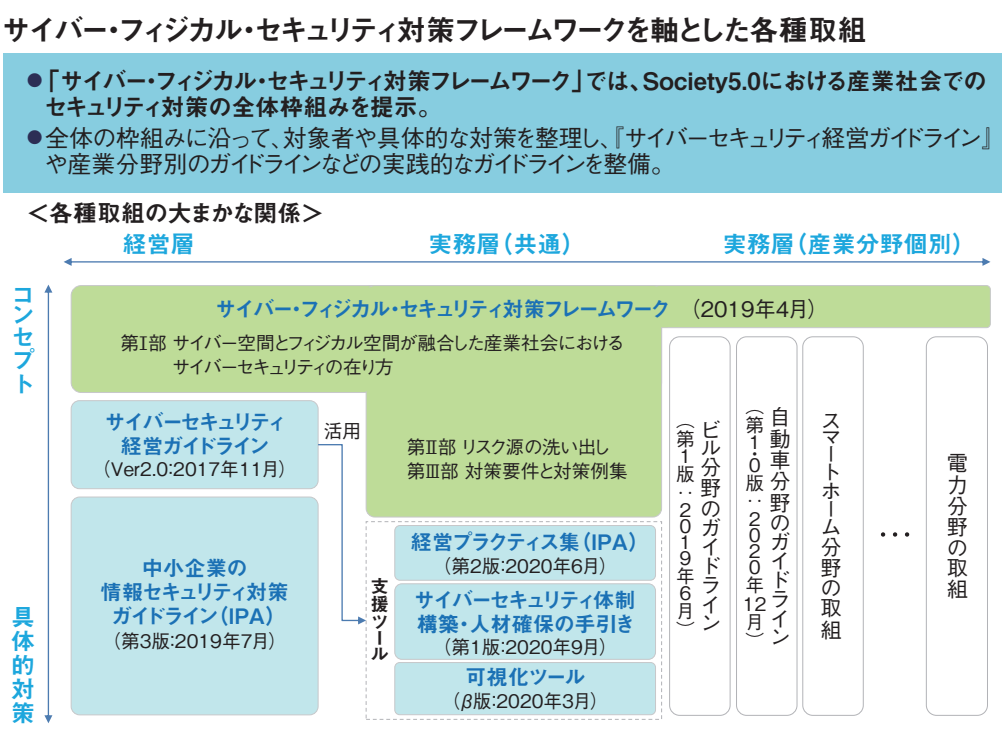
①「セキュリティ人材活躍モデル」の作成
②戦略マネジメント層の育成
③産学官の連携強化

「セキュリティ人材活躍モデル」の作成に関しては、経済産業省では、2018 年より関連有識者会合にて検討を重ね、2020 年 4 月以降は「セキュリティ経営・人材確保の在り方検討タスクフォース」において継続して検討が進められている。その成果として、2020 年 9 月「サイバーセキュリティ経営ガイドライン Ver2.0」の付録 F として「サイバーセキュリティ体制構築・人材確保の手引き 第 1 版」が、2021 年 4 月にはその改訂版として第 1.1 版が公開されている[※58]（「2.3.1 (3) (b)『サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版』の概要」参照）。

戦略マネジメント層の育成に関しては、2018 年より



■図 2-3-4　プラス・セキュリティ知識が必要となり得る分野
（出典）NISC「政策課題2 DX に必要な『プラス・セキュリティ』知識を補充できる環境・人材育成の推進」



■図 2-3-5 サイバー・フィジカル・セキュリティ対策フレームワークを軸とした各種取り組み
（出典）経済産業省「事務局説明資料」（第７回 産業サイバーセキュリティ研究会 ワーキンググループ２（経営・人材・国際）資料３）

IPA ICSCoEにおいて「戦略マネジメント系セミナー※340」を毎年開催している（「2.3.2 産業サイバーセキュリティセンター」参照）。また、東京工業大学 CUMOT において「サイバーセキュリティ経営戦略コース※341」が開講されている（「2.3.4 (5) サイバーセキュリティ経営戦略コース」参照）。更に、NISC では、情報セキュリティ大学院大学の協力により、「DX を推進する部門の責任者あるいは主要な役割を担う管理職」を対象層としてモデルカリキュラム開発を試行している。情報セキュリティ大学院大学では、開発カリキュラムをベースとし、DX 推進者を対象とした「DX with Cybersecurity 3日間教育コース※342」を実施した。2021 年度も同様に開催されるとともに、更にモデルカリキュラムをベースとして強化が進められる。

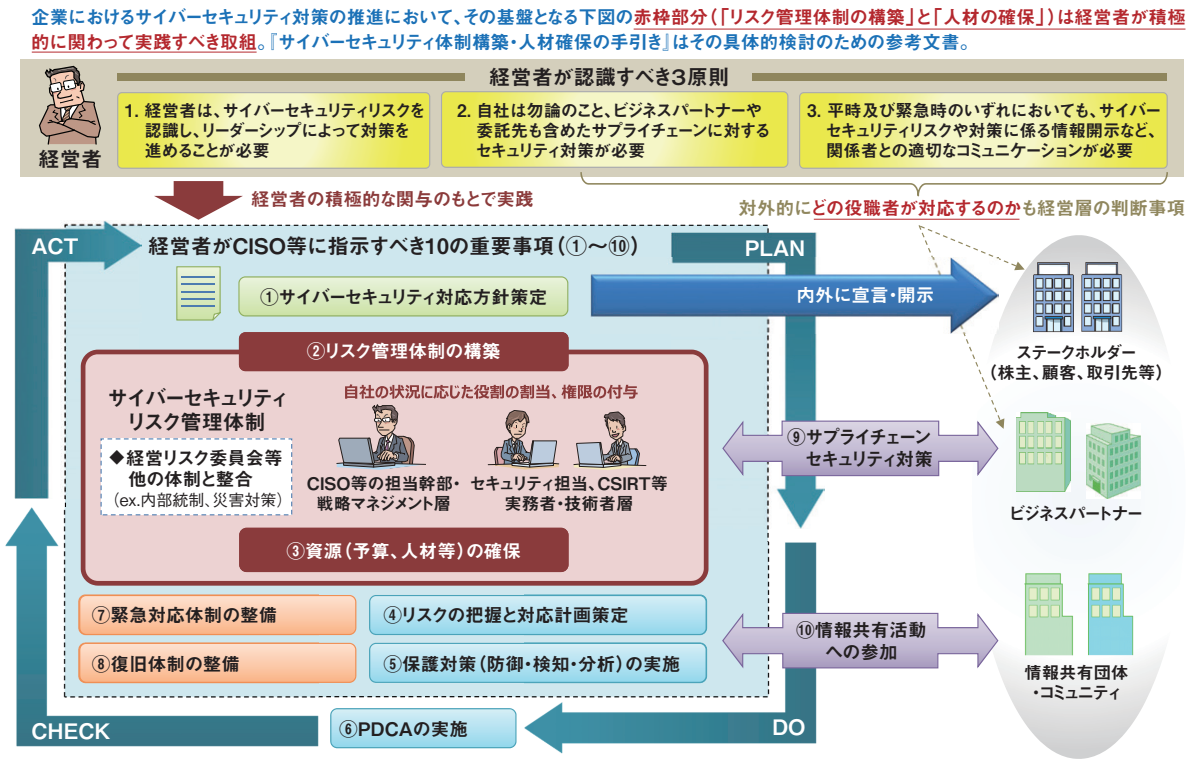
産学官の連携強化に関しては、経済産業省、IPA、JPCERT/CC 及び業界団体が国立高専機構と連携し、高専生の専攻（セキュリティ、IT、その他（機械、電気等））に応じた教育コンテンツの提供や講師の派遣等、産学官連携の具体化を進めている（「2.3.4 情報セキュリティ人材育成のための活動」参照）。また、地域におけるセキュリティ人材育成については、地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ活動（地域 SECUNITY）の中で、地域ごとに普及活動、人材育成を実施している（「2.4.2 中小企業に向けた情報セキュリティ支援策」参照）。

(b)「サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版」の概要

「サイバーセキュリティ経営ガイドライン」では、サイバーセキュリティについて経営者が認識すべき3原則を提示し、経営者が CISO 等に指示すべき重要 10 項目を説明している。その付属書である「サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版」（以下、手引き）では、重要 10 項目のうち、以下の二つの項目にフォーカスし、解説を行っている（次ページ図 2-3-6）。

②リスク管理体制の構築（以下、指示 2）
③資源（予算、人材等）の確保（以下、指示 3）

これは、サイバーセキュリティが経営課題であるという意識が浸透し、多くの企業が「サイバーセキュリティ経営ガイドライン」の実践に取り組む中で、管理体制の構築をどのように行えばよいか、また、資源人材の確保をどうすれば良いかが分からないという意見が多く寄せられたことによる。また、この二つの重要事項は、経営者の意思決定が求められる項目だからである。



■図 2-3-6 「サイバーセキュリティ体制構築・人材確保の手引き」のサイバーセキュリティ経営ガイドラインにおける位置付け
（出典）経済産業省・IPA「付録 F（概要版）サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版※343」

手引きにおける検討のポイントでは、指示 2 について、以下が挙げられている。

- 経営者のリーダーシップのもとでのセキュリティ機能と体制の検討
- セキュリティ統括機能の検討
- セキュリティ関連タスクを担う部門・関係会社の特定・責任明瞭化（ITSS+（セキュリティ領域）を参考にし、外部委託先の選定では情報セキュリティサービス基準適合サービスリスト等を活用）

指示 3 については、以下が挙げられている。

- 「セキュリティ人材」の確保（まずは、セキュリティ統括人材の確保を目指す。）
- 「プラス・セキュリティ」の取組推進
- 教育プログラム・試験・資格等の活用と人材育成計画の検討

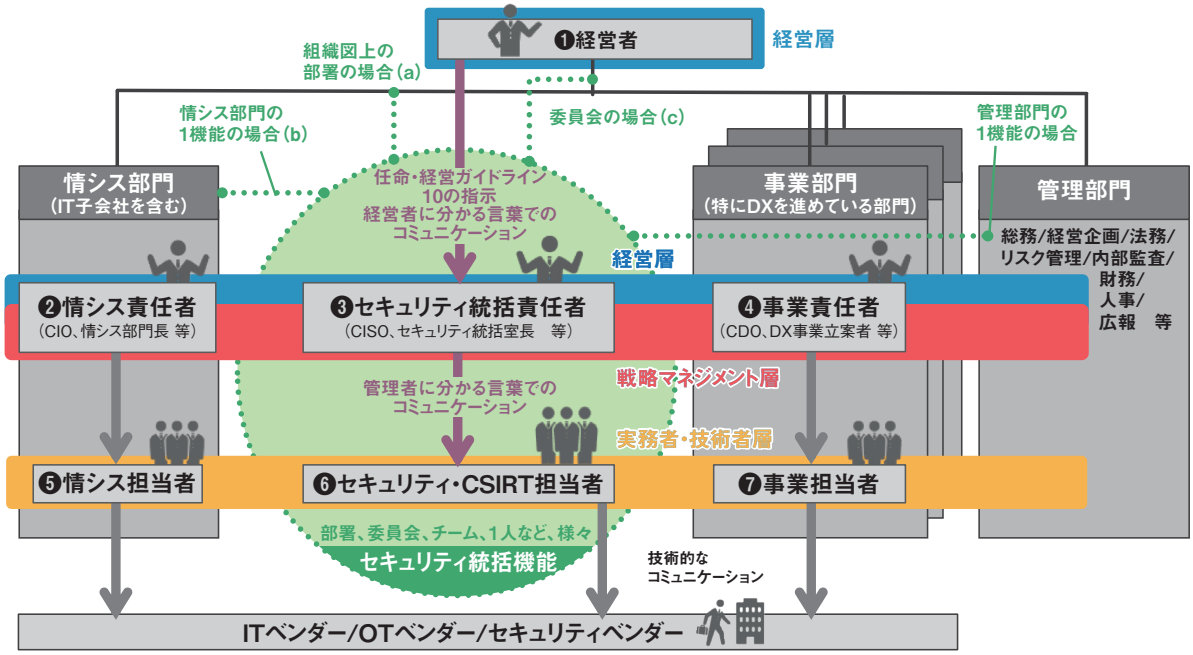
それらのポイントを理解し、利用する上で大事な概念として以下がある。

- セキュリティ統括機能
- ITSS+（セキュリティ領域）
- プラス・セキュリティ

セキュリティ統括機能は、セキュリティ対策及びインシデント対応において、CISO や経営層を補佐してセキュリティ対策を組織横断的に統括することにより、企業におけるリスクマネジメント活動の一部を担うとしている。2018 年ごろから「セキュリティ統括室」といった名称を明示した部署を設ける企業が出てきているが、手引きでは、セキュリティ統括は、「機能」であって「組織」として設置しなくてもよく、状況に応じて、組織に最適な形態を取るべきだとしている（次ページ図 2-3-7）。

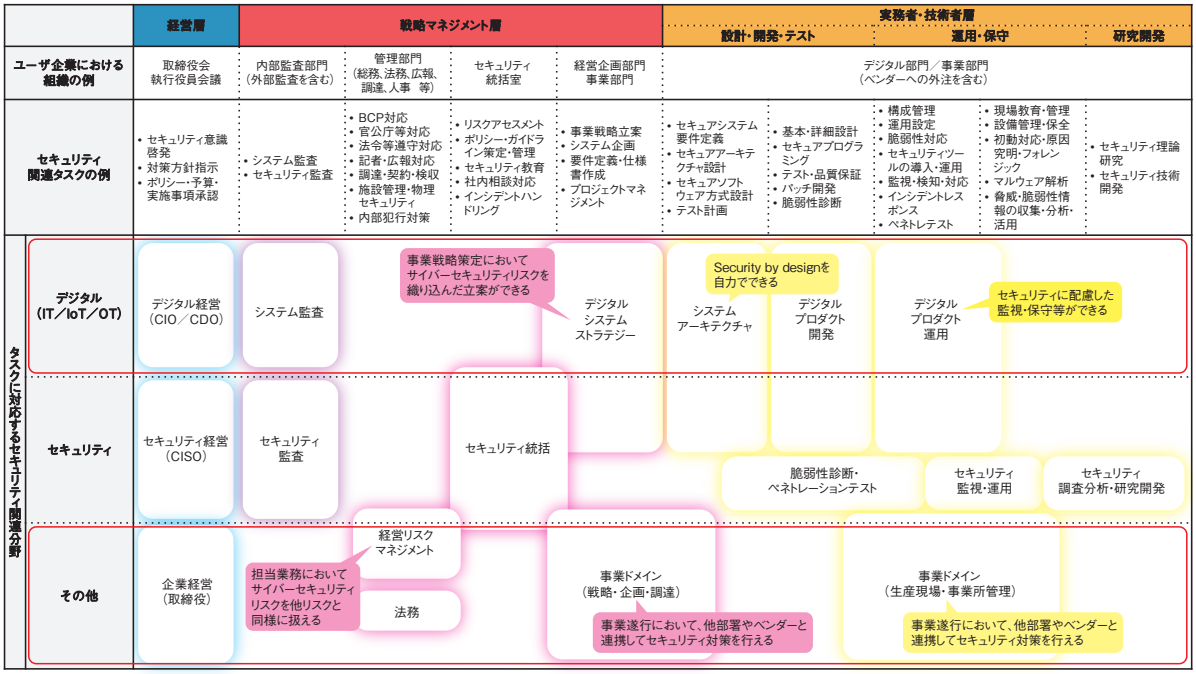
ITSS+（セキュリティ領域）は、企業のセキュリティ対策に必要となる関連業務を 17 分野に整理しており、それぞれの分野に求められるセキュリティ知識・スキルの概念をまとめることで、企業でセキュリティ体制を構築する際の業務役割を検討する際に利用できる。セキュリティの専門性の高い分野だけでなく、経営層や法務部門、事業ドメインまで、サイバーセキュリティ対策に関わる幅広い領域を網羅している（次ページ図 2-3-8）。

手引きでは、プラス・セキュリティを、「（セキュリティ対策を本務としていないが）自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態」と定義している。また、「プラス・セキュリティ」人材を業務担当者と別に確保する必要はなく、既存の



■図 2-3-7　セキュリティ統括機能のイメージ
(出典)経済産業省・IPA「付録 F(概要版)サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版」

ITSS+(セキュリティ領域)(赤枠が「プラス・セキュリティ」の分野)



■図 2-3-8　ITSS+(セキュリティ領域)
(出典)経済産業省・IPA「付録 F(概要版)サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版」

業務担当者がサイバーセキュリティの知識・スキルを習得し、実践することを通じて役割を担うとしている。また、プラス・セキュリティは、DX の取り組みの有無に関わりなく、IT を活用するすべての企業に必要であるとしている。

今回、手引きにおいて、指示 2 及び指示 3 の実践を担当する戦略マネジメント層が、セキュリティ統括人材とプラス・セキュリティ人材という二つの類型で整理された。この方針は、DX の活用・推進において必要なセキュリティを推進することを NISC で「DX with Cybersecurity」と呼称し、プラス・セキュリティ知識が必要としていることとも整合が取れている。

(4) NICE Framework の改訂

NIST のサイバーセキュリティ人材育成イニシアティブ NICE（National Initiative for Cybersecurity Education）では、米国のセキュリティ人材育成のため枠組として、Workforce Framework for Cybersecurity（以下、NICE Framework）を 2012 年から発行しており、第 3 版は 2017 年 8 月に NIST SP800-181[※344] として発行された。それが 2020 年 11 月に改訂され、最新版として NIST SP800-181 Revision 1[※345] が発行された（NIST の規格については「3.4 NIST のセキュリティ関連活動」参照）。

NICE Framework は、その時々の組織におけるサイバーセキュリティの要求や必要性に合う形で、サイバーセキュリティに関連する仕事や関わる人材の能力を記述する共通言語として機能することを目的としている。

日本の方向性との関連では、NICE Framework が目指している様々な関係者間での共通言語化は、日本において経済産業省や NISC が示している「役割定義の共通言語化等」と共通している[※346]。また、NICE Framework における「Cybersecurity Workforce」から「Learners」への変更は、日本において NISC 等が示しているプラス・セキュリティ、DX with Cybersecurity への取り組みとも同じ方向である。

(5) 総務省・NICT の取り組み

総務省の人材育成に関わる取り組みは、NICT を中心に行われており、ナショナルサイバートレーニングセンターで実施されている実践的サイバー防御演習「CYDER」、サイバーコロッセオや若手セキュリティ人材育成のための SecHack365 等の人材育成プログラムを展開している。

2021 年からは、「サイバーセキュリティ統合知的・人材育成基盤 CYNEX」構築を計画している（「2.1.3 総務省の政策」参照）。

(6) まとめ

DX の推進では、デジタル化を前提としたビジネスを考え実行する際にセキュリティを担う人が必要となってくる。

セキュリティ担当部門のみならず、事業部門にもセキュリティが分かり、必要なセキュリティ業務をこなすことが求められてきており、セキュリティに特化した能力だけではなく、デジタル化を前提とした事業を推進するために必要なセキュリティを確保できる能力が求められ、プラス・セキュリティ知識を持った人材育成が重要となっている。

一方で、組織全体での情報セキュリティ統制（ガバナンス）を考えて実行する機能・役割も必要である。自組織のビジネス・業務への深い知識と理解を持った上で、組織全体として統制の取れたセキュリティ対策を実施するセキュリティ統括の役割を担うセキュリティ専門人材が必要である。手引き書作成等の活動により、いままでの戦略マネジメント層は、DX with Cybersecurity を推進する人材像として以下のように整理された。

- セキュリティ統括：組織全体のセキュリティを統括的に担う人材
- プラス・セキュリティ：事業におけるセキュリティを担当する人材

今後、NISC、経済産業省、総務省等の官による施策は、2021 年に改定される次期「サイバーセキュリティ戦略」に盛り込まれ、計画、実施されていくものと思われる。それに加えて、SC3 等による民間での協調体制が徐々に構築され、相互に連携しながら、セキュリティ人材育成環境が整備されていくことが期待される。

2.3.2 産業サイバーセキュリティセンター

我が国の経済・社会を支える重要インフラ[※347] や産業基盤のサイバー攻撃に対する防御力を強化するため、IPA は 2017 年 4 月に産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）を発足させた。

ICSCoE は、重要インフラや産業基盤のサイバーセキュリティリスクに対応する人材・組織・システム・技術を生み出していくため、「人材育成事業」「制御システムの安全性・信頼性検証事業」「攻撃情報の調査・分析事業」の三つを事業の柱としている。本項では、「人材育成事業」について述べる。

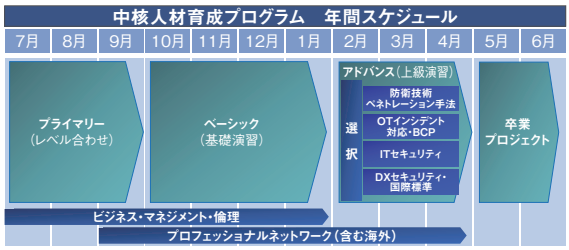
(1) 中核人材育成プログラム

ICSCoE は、2017 年 7 月、制御技術（OT：Operational Technology）と情報技術（IT）、マネジメント、ビジネス分野を総合的に学び、サイバーセキュリティ対策の中核となる人材を育成する「中核人材育成プログラム」を開始した。本プログラムでは、OT 及び IT 知識のレベル合わせからハイレベルな演習までを 1 年間のフルタイムで実施する。第 1 期は 76 名、第 2 期は 83 名、第 3 期は 69 名が参加し、2020 年 7 月に開講した第 4 期では、電力・鉄鋼・石油・化学・自動車・鉄道・放送・

通信・産業ベンダ等の幅広い業界から47名が参加した。

カリキュラムはOT分野の「防衛技術・ペネトレーション手法」（制御システム固有のセキュリティリスク、攻撃に対する防御技術の理解等）、「OTインシデント対応・BCP」（安全性と事業継続性を両立するOTインシデント対応、制御システムBCP対応の演習等）、IT分野の「ITセキュリティ」（制御システムセキュリティ実現のためのIT設計、ITインシデント対応、体制整備等）の3領域を基軸として、ビジネスマネジメントに関する実務家による講義や米国・欧州等の先進事例を学ぶ海外派遣演習等を含む構成となっている。

本プログラムは、過去の実施結果を踏まえて毎年カリキュラム及びスケジュールの改善を図っている。4年目となる2020年度は、「アドバンス（上級演習）」において選択可能な演習として、AI、IIoT（Industrial Internet of Things：産業分野向けIoT）、商用クラウド、DLT（Distributed Ledger Technology：分散台帳技術）のセキュリティ応用及びセキュリティ課題の講習等を実施する「DXセキュリティ・国際標準」を追加した（図2-3-9）。



■図2-3-9　第4期中核人材育成プログラムの年間スケジュール

2020年12月の海外派遣演習では、英国の政府機関・航空業界及び起業家の代表者によるサイバーセキュリティの取り組みや5Gのポリシーに関する講義をオンラインで実施した。2021年1月には、フランスのセキュリティ専門家による海運業界のサイバーセキュリティやデータ処理のセキュリティに関する講義をオンラインで実施した。

同年1月には、2017年5月に合意された「日イスラエル・イノベーション・パートナーシップ」等に基づき、イスラエルの重要インフラ企業やサイバーセキュリティ企業の担当者によるサイバーセキュリティ対策に関する講義をオンラインで実施した。

また同年3月には、米国政府・EUと連携した制御システムのサイバーセキュリティ対策に関するキャパシティビルディングプログラム「インド太平洋地域向け日米産業制御システムサイバーセキュリティウィーク※169」（「2.2.1（3）（c）インド太平洋地域に向けたサイバー演習」参照）を経済産業省と共催した。本演習には第4期の受講者及びインド太平洋地域から招聘した外国人受講者40名がオンラインで参加し、米国、EU及び日本の専門家によるエネルギー分野を含むサイバーセキュリティに関するワークショップ、リモートでのハンズオン演習等を実施した。

2018年7月、中核人材育成プログラムのOB会として、修了者コミュニティ「叶会※348」が発足し、2019年夏以降、本プログラムを通じて培った人脈の活用、知見やノウハウの共有を目指し、地域活動や技術をテーマにする複数の部会が設置された。また修了年次をまたがる縦のつながりの形成、最新情報及びノウハウ収集を目的とした叶会総会があり、2020年11月に第3回総会が開催された。叶会には第1期から第3期までの修了者に加え、2021年6月に修了した第4期生も参加しており、今後もコミュニティとしての規模を拡大しながら、お互いの顔が見える縦横の人的つながりを形成し、産業サイバーセキュリティに関する適時、適切な情報共有活動を継続することが期待される。

なお、同プログラムの修了者は、情報処理の促進に関する法律の規定に基づき、後述する情報処理安全確保支援士試験の全部免除を受けることができる※349。

（2）短期プログラム

ICSCoEでは、セキュリティに関連するスキルの習得機会が充分でない部門責任者や現場責任者、及びセキュリティ実務担当者に向けて、数日間で学ぶ短期演習形式の「製造・生産分野向けセキュリティ教育プログラム」「業界別サイバーレジリエンス強化演習」「戦略マネジメント系セミナー」及び「制御システム向けサイバーセキュリティ演習」を提供している。新型コロナウイルスへの対応の一環として、オンライン実施が可能なものはライブ配信または事前収録した動画のオンデマンド配信とした。

（a）製造・生産分野向けセキュリティ教育プログラム

「製造・生産分野向けセキュリティ教育プログラム※350」（旧称、製造・生産分野の管理監督者層向けプログラム）は、製造・生産のための制御系システムを日夜運用する管理監督者の方で、サイバー攻撃に対する防護力の強化に関心を持つ方を対象としたプログラムである。

2020年11～12月には「製造・生産現場のセキュリティに必要なIT・OT基礎コース」をオンライン（オンデマンド配信）と神戸での講習を組み合わせて実施した。本コースは製造・生産現場のセキュリティ対策に必要なIT・OTの基礎知識を理解すること、IT部門とOT部門が

連携してセキュリティを推進するための共通目線を獲得し相互理解を深めること等を目的としている。受講者からは、「理解度に応じて動画を繰り返し視聴できる点が良かった」「体系的に構成されており理解しやすかった」との反応があった。

また2021年1～2月には「製造・生産現場でのセキュリティ・インシデント対応実践方法コース」をオンライン（ライブ配信）で実施した。本コースは異常が発生した際、サイバー攻撃の可能性も考慮した初動対処を行い、障害の切り分けができること、社内外の関連組織と連携し、影響を最小化しながら、原因究明、事業継続等の対応ができること等を目的としている。受講者からは、「オンラインでもしっかり学べた」「座学で学んだ上で実践するスタイルが良かった」「サイバーセキュリティに精通していなくても理解できる内容であった」との反応があった。

(b) 業界別サイバーレジリエンス強化演習（CyberREX）

「業界別サイバーレジリエンス強化演習（CyberREX：Cyber Resilience Enhancement eXercise by industry）※351」は、電力、鉄道、ビル・物流、自動車（製造系）、ファクトリーオートメーション業界においてCISO（Chief Information Security Officer：最高情報セキュリティ責任者）に相当する役割を担う人材やIT部門、生産部門等の責任者・マネージャークラスの人材を対象としたプログラムである。

2020年11月に本演習をオンライン（ライブ配信）で実施した。本演習は、部署・部門のサイバーセキュリティに関する対応力・回復力を強化するため、業界の最新動向、業界別に考慮すべきセキュリティ要件、安全性要件を織り込んだ構成とし、仮想企業を想定したシナリオ形式による実践演習を中心に進められた。受講者に加え、サイバーセキュリティの専門家や監督省庁の関係者も参加した形式でのグループ演習を行った。受講者からは、「オンラインでの受講に問題なかった」「演習の内容が非常によく練られておりまるで訓練中かのような雰囲気で学べた」との反応があった。

(c) 戦略マネジメント系セミナー

「戦略マネジメント系セミナー※352」は、セキュリティ及びリスクマネジメントに係る方針や戦略を策定し、推進することを期待される管理職を対象としたプログラムである。

2021年2月に、本セミナーをオンライン（オンデマンド配信）で実施した。本セミナーでは、2019年度に実施した同セミナーの「セキュリティ組織管理」コースを発展させ、組織のセキュリティ体制を統括・推進するための考え方、セキュリティ対策の実践に向けたマネジメント手法等を習得することを目的とした。

具体的には、政府動向や先進事例の講演、セキュリティ対策のあるべき姿や対策推進時の悩み・解決策を有識者が議論するパネルディスカッション、現場でセキュリティ対策を実践するための体系的なノウハウの講演を動画で配信した。受講者からは、「オンデマンド配信は受講時間の自由度が高くなり良かった」「政府動向の要点をつかめる貴重な機会であった」「他社のセキュリティの取り組み状況や課題認識を知ることができて大変参考になった」との反応があった。

(d) 制御システム向けサイバーセキュリティ演習

「制御システム向けサイバーセキュリティ演習※353」は、制御システムのサイバーセキュリティを担当する、または今後担当予定の技術者を対象としたプログラムである。

2020年12月に東京で本演習を実施した。本演習は制御システムのサイバーセキュリティを理解するための導入的な位置付けであり、制御システムへの攻撃手法、及び制御システムのサイバーセキュリティ対策の基礎を、簡易模擬システムを用いた実機演習（ハンズオン演習）で体験し、制御システムのセキュリティについて実践的に理解することを目的としている。受講者からは、「非常に有益な研修であった」「これまで攻撃方法の実機演習の機会がなかったため今回深く学ぶことができた」との反応があった。

2.3.3 情報セキュリティ人材育成のための国家試験、国家資格制度

本項では、情報セキュリティ人材の育成や確保を目的とした国家試験や国家資格制度に関する動向を紹介する。

(1) 情報セキュリティマネジメント試験

企業・組織においては、組織が定めた情報セキュリティポリシーを部門内に周知して遵守を促し、部門の情報管理を実施する等、情報セキュリティ対策を推進する人材（情報セキュリティマネジメント人材）が必須である。こうした人材を育成するために、2016年度春期より「情報処理技術者試験」の新たな試験区分として「情報セキュリティマネジメント試験」が実施されている。2019年度までは、試験を年2回実施していたが、2020年度は、新型コロナウイルス感染拡大防止の観点から春期試験

(4 月)が中止となった。また、秋期試験(10 月)についても、新型コロナウイルスの影響により試験会場を十分に確保できないことから、試験の実施方式を、同一日に全国の試験会場で一斉実施する従来の紙試験から、複数日で実施する CBT（Computer Based Testing）方式※354 に移行した。CBT 方式への移行により、受験者は、自身で試験日、試験会場を選択することが可能となった。2020 年度は、CBT 方式による試験を 12 月 1 ～ 27 日の期間で実施し、応募者数 9,694 人、合格者数 6,071 人であった※355。2021 年度も CBT 方式での実施を継続する。

(2) 情報処理安全確保支援士制度

サイバー攻撃の増加・高度化に加え、社会的な IT 依存度の高まりから、企業・組織におけるサイバーセキュリティ対策の重要性が高まっている。それに伴い、企業・組織での安全なセキュリティ対策を高度なスキルを活かして推進できる人材が求められている。

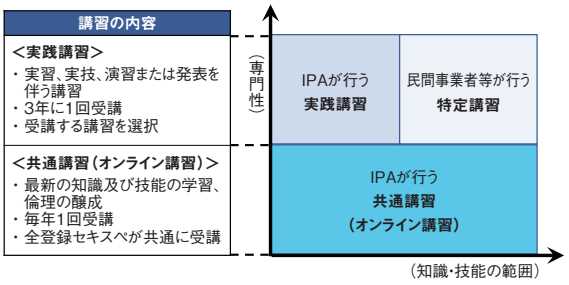
そこで、最新の知識・技能を備え、サイバーセキュリティ対策を推進する人材の育成と確保を目指し、2016 年 10 月、「情報処理の促進に関する法律」の改正法が施行され、新たな国家資格「情報処理安全確保支援士」制度が創設された。

情報処理安全確保支援士（以下、登録セキスペ）は、情報処理安全確保支援士試験合格者が登録簿に登録されることにより資格を取得する、サイバーセキュリティ分野初の国家資格である。試験は例年、年 2 回実施されているが、2020 年度は新型コロナウイルス感染拡大防止の観点から春期試験（4 月）が中止となり、実施された秋期試験（10 月）の応募者数は 1 万 6,597 人、合格者数は 2,253 人であった※356。

また、2020 年 5 月に「情報処理の促進に関する法律」が改正され、新たに更新制及び特定講習の制度が導入された。更新制とは登録から 3 年ごとに資格の更新を義務付けるものであり、サイバーセキュリティに関する最新の知識・技能の維持のみならず、欠格事由に該当していないか等、登録セキスペとしての資格を有しているかを改めて確認することで、情報処理安全確保支援士制度の信頼性向上を目的としている。2020 年 10 月 1 日に 5,865 人、2021 年 4 月 1 日に 1,847 人が登録セキスペ資格の更新を行った。2020 年度の新規登録者 1,111 人と合わせ、登録セキスペの登録人数は、2021 年 4 月 1 日時点で 2 万 178 人である※357。

登録セキスペには法定講習として、共通講習と実践講習の受講が義務付けられている。2021 年度から実践講習は、IPA が行う実践講習と民間事業者等が行う特定講習から選択できるようになった。特定講習は、一定の条件を満たした民間事業者等が実施する講習を経済産業大臣が法定講習として定める制度である※358。2021 年 3 月に 8 実施機関 23 講座が 2021 年度の特定講習として経済産業省より公開された※359。これにより、登録セキスペの多様なニーズに対応できるようになった。

登録セキスペに受講が義務付けられている法定講習の全体像を図 2-3-10 に示す※360。



■図 2-3-10　法定講習の全体像

IPA の行う実践講習は、グループディスカッションを中心とした内容で従来は集合形式で実施していたが、新型コロナウイルス感染拡大防止の観点から、2020 年 11 月からは Web 会議ツールを利用したリモート形式で実施しており、2021 年度も継続する。2020 年度には 1,243 名が受講し、集合形式と同等の満足度を実現している。受講者からは、「自分が普段携わっていないインシデント対応や CSIRT 構築・運用や経営目線等、様々な視点の考え方を学ぶことができた」「登録セキスペとしての倫理面での責任を改めて感じた」等の声が上がっている。また、「ディスカッションの内容をファイル共有ツールを介して即時にテキスト化でき、自分自身の考えが整理されるとともに他者の意見も理解しやすかった」「地域で集まるのではなく、全国の方と意見交換できるのはリモート講習ならではの貴重な場だと感じた」といったリモート形式ならではのメリットも挙がった※361。

2.3.4 情報セキュリティ人材育成のための活動

情報セキュリティに関する情報共有や情報セキュリティ人材育成の場として、様々なイベントが開催されている。また、複数の大学と産業界がネットワークを形成し、セキュリティ分野の人材を育成する事業が行われている。

(1) セキュリティ・キャンプ

「セキュリティ・キャンプ」は、若年層の情報セキュリティ意識の向上、並びに将来第一線で活躍できる高度な情報セキュリティ人材を発掘・育成する場として、一般社団法人セキュリティ・キャンプ協議会（以下、セキュリティ・キャンプ協議会）とIPAにより運営されている。

17回目となる2020年度の全国大会は、新型コロナウイルスの影響により2020年10月18日～12月6日にオンライン形式で開催され、選考を通過した85名が参加した※362。

また、過去のセキュリティ・キャンプ全国大会を修了、または同等以上のスキルを持つ25歳以下の学生を対象とした育成の場である「セキュリティ・ネクストキャンプ2020オンライン」も、全国大会と同期間に併催され、7名が参加した※363。

主に若年層を対象とした「セキュリティ・ミニキャンプ」については、新型コロナウイルスの影響により東京開催は中止となったが、北海道、青森、山梨、広島、福岡、沖縄は現地で開催され、大阪は3月にオンラインで開催された※364。

セキュリティ・キャンプ協議会が単独で主催するイベントである「Global Cybersecurity Camp」については、第3回が2021年1月16日～2月7日にオンライン開催された※365。このトレーニングキャンプは、「国籍・人種を越えた専門知識のあるグローバル人材の育成」「国境を越えた友情とゆるやかなコミュニティの形成」を目的として、セキュリティに興味を持つ、異なる国の若者がともに学び、友好を深める場を提供するものである。

セキュリティ・キャンプ協議会が実施するその他の活動として、2021年3月13日に「セキュリティ・キャンプフォーラム2021」がオンライン開催された。本フォーラムの目的は、セキュリティ・キャンプ修了生相互の年次を超えた交流と意見交換の場の提供、同修了生の認知度向上と現在の活動紹介による産業界での活躍支援のきっかけの提供、の2点である。当日は、セキュリティ・キャンプ修了生が情報セキュリティに関連する取り組みをテーマとしたプレゼンテーションを行った。また、優れた成果を上げた人や価値ある取り組みを表彰する「セキュリティ・キャンプアワード2021」の表彰を実施した。表彰後には、「セキュリティ・キャンプ交友会2021春オンライン版」が併せて開催された※4。

(2) enPiT

「enPiT（Education Network for Practical Information Technologies：成長分野を支える情報技術人材の育成拠点の形成）」は、情報技術を高度に活用して社会の具体的な課題を解決できる人材を育成するために、産学協働の教育ネットワークを形成し、PBL（Problem Based Learning：課題解決型学習）等の実践的な教育を推進・普及することを目的とした文部科学省の事業である。2012～2016年度までは大学院生を対象とした事業「第1期enPiT」が実施され、これを踏まえて2016年度から、学部生を対象とした「第2期enPiT」（以下、enPiT2）を実施している。enPiT2は、ビッグデータ・AI、セキュリティ、組み込みシステム、ビジネスシステムデザインの4分野を対象として教育プログラムを提供している。

このうちセキュリティ分野（enPiT-Security）では、2020年度は大学等31校、連携企業51社・団体が参加した（2021年3月現在）。東北大学を中核とした14の大学が連携して、高度化する情報セキュリティの脅威を理解し、リスクマネジメントに必要な知識、基本技術、実践力を備えた人材を育成する「Basic SecCapコース※366」を提供しており、210名が修了認定を取得した※367。

また、社会人を対象とした情報科学技術分野に関する体系的かつ高度で短期の実践教育プログラムとして「enPiT-Pro※368」がある。セキュリティ分野では、情報セキュリティ大学院大学、東北大学、大阪大学、和歌山大学、九州大学、長崎県立大学、慶應義塾大学の7大学が、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA：Japan Network Security Association）、一般社団法人サイバーリスク情報センター（CRIC）、及び地域の団体・官庁・企業（2021年2月時点で37社・団体）と連携し、多様な産業ニーズに即したプロ人材育成のための教育コース「enPiT-Pro Security※369」を展開している。

(3) SECCON 2020

SECCONは実践的情報セキュリティ人材の発掘・育成、技術の実践の場の提供を目的とする日本最大の情報セキュリティコンテストイベントである。

世界各国のセキュリティ専門家がCTF※370の技量を競うSECCON CTF 2020は、新型コロナウイルスの影響で例年の予選・決勝の形式をとらず、2020年10月10～11日にオンライン形式で開催された。世界88ヵ国から982チーム、1,862人の参加があった※371。

関連するイベントとして、新しいコンテストの企画案・

設計案をCFC（Call for Contest）として2020年10月に募集した（「Contest of Contest」）。またコンテストに関する講演・ワークショップのイベントとして、同年12月19日に「SECCON 2020電脳会議」を開催した。主催者、CTF参加者の講演等のほか、「Contest of Contest」の結果も発表された※372。

また、日本国内のCTF参加者を増やし、セキュリティ人材の底上げを図るためのワークショップ「SECCON Beginners※373」も開催した。まず2020年5月23～24日にはCTF初級者～中級者を対象とする「オンラインCTF」を開催し、1,070チームが参加した。10月17日には講演形式の「SECCON Beginners Live※374」を開催し、オンラインCTFの結果を解説した。

更に、情報セキュリティに興味がある女性を対象としたワークショップ「CTF for GIRLS※375」では、2020年9月18日にネットワーク、12月11日に暗号に関するオンラインワークショップを開催した。

JNSAは、このようにSECCONをとおして、専門家向けのCTFだけでなく、初級者・中級者を含めた様々なセグメントに対して実践的情報セキュリティ人材の発掘・育成の機会を提供している。

(4) 産学情報セキュリティ人材育成交流会

JNSAの産学情報セキュリティ人材育成交流会は、2012年2月に発足し、今後の情報セキュリティ業界を支える人材を育成するためのインターンシップの支援活動を実施している。将来情報セキュリティ業界で活躍したいと考える学生に対し、本交流会を介して、2020年度は6社の企業がインターンシップを実施した。CTF形式を取り入れたセキュリティ業務体験イベントや特別セミナーを開催した企業もあった※376。

(5) サイバーセキュリティ経営戦略コース

東京工業大学社会人アカデミーでは2021年2月18日、MOT（Management of Technology：技術経営）に関する社会人向けプログラムとして「キャリアアップMOT『サイバーセキュリティ経営戦略コース』」を開講した。本コースは新型コロナウイルス対策のため、オンライン講義形式となった※377。

本コースでは、サイバーセキュリティが企業・組織の経営に及ぼす影響を理解し、サイバーセキュリティ経営※378及びその戦略立案に求められる知識・能力を備え、企業・組織を先導する人材の育成を目指しており、多様な業界･業種から、経営者、マネージャー、若手等、多くの社会人が受講することを想定している。本コースは、週1回、産学官の実務経験豊富な有識者による関連技術・法制・世界情勢等の解説や、事例に基づく演習、討議等を含む全20回の講義で構成される。

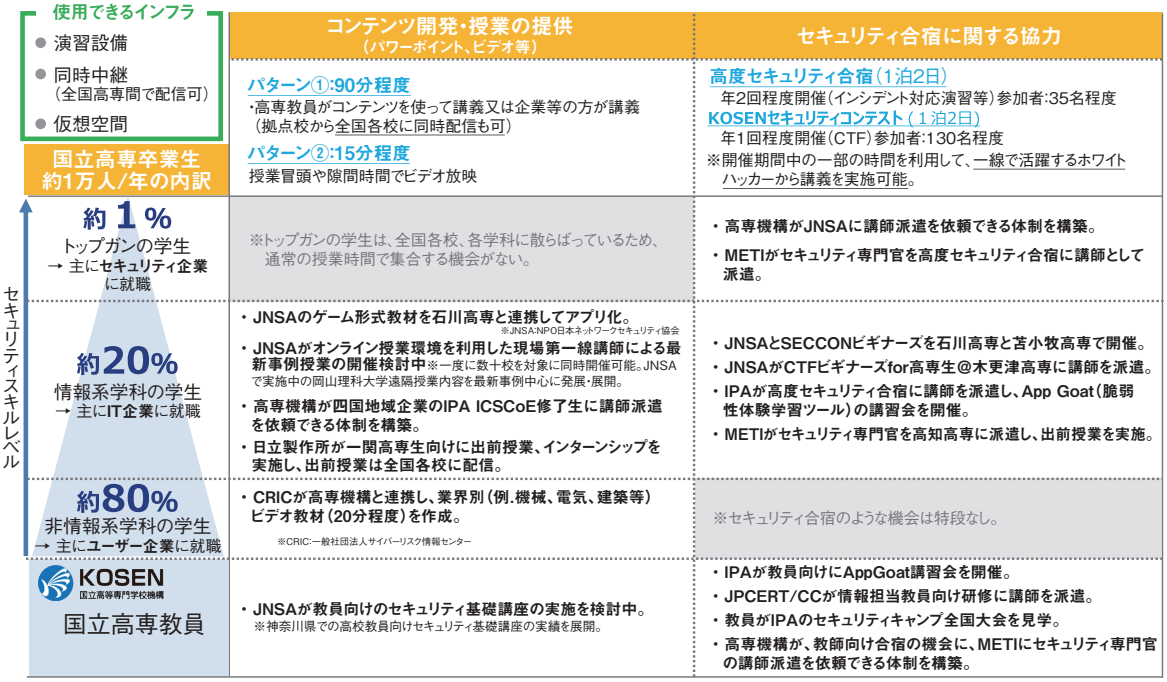
(6) 産学官で連携した国立高等専門学校での取り組み

国立高等専門学校（以下、高専）のセキュリティ教育において、産業界が求めるセキュリティ人材を育成・輩出する支援として、経済産業省、IPA、JPCERT/CC及びJNSA等の業界団体が、独立行政法人国立高等専門学校機構（以下、国立高専機構）と連携し、教育コンテンツの提供や講師の派遣等に取り組んでいる。

高専生の専攻（セキュリティ、IT、その他（機械、電気等））により、卒業後の就職先の業界に傾向があることに着目し、将来を見据えたセキュリティ人材育成を、2019年より産学官連携で行っている。約20%の人材（情報系の学生）への教育コンテンツ提供や講師派遣、80%の人材（非情報系学科の学生）に向けた一般社団法人サイバーリスク情報センター（CRIC）による業界別ビデオ教材の作成等を行っている。図2-3-11（次ページ）に具体的な取り組みを示す。

2020年は、JNSAによるオンライン授業環境を利用した最新事例授業や教員向けセキュリティ基礎講座等、これまでの実績をより広く展開する検討を行った。また、四国地域企業のIPA ICSCoE修了生を地域の高専に、経済産業省のセキュリティ専門官をセキュリティ合宿や教師向け合宿に講師派遣できる体制を構築した。

● METI、IPA、JPCERT及び業界団体が国立高専機構と連携し、高専生の専攻（セキュリティ、IT、その他（機械、電気等））に応じた教育コンテンツの提供や講師の派遣等、産学官連携の具体化を推進中。



■図 2-3-11　国立高専機構と産・官との連携促進・具体化
（出典）経済産業省「事務局説明資料」（第 7 回 産業サイバーセキュリティ研究会 ワーキンググループ 2（経営・人材・国際） 資料 3）を基に IPA が編集

2.4 組織・個人における情報セキュリティの取り組み

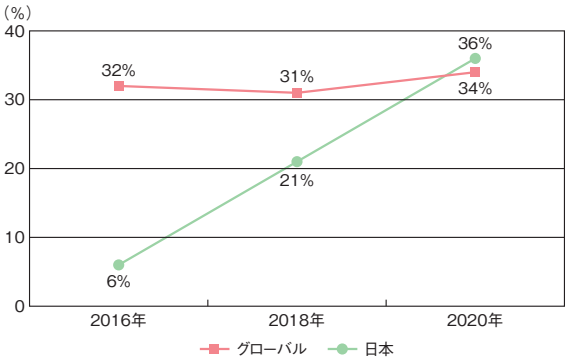
企業、教育機関、地方自治体、一般利用者の情報セキュリティの対策状況及び課題について、政府、IPA 等による取り組み及び公表されている資料等を基に述べる。

2.4.1 企業における対策状況

情報セキュリティに対する企業の対策状況、及びセキュリティマネジメントの取り組みについて述べる。

(1) 情報セキュリティに対する企業の対策状況

PwC が 2 年に 1 度実施している世界規模のアンケート調査※379 によると、日本の組織がサイバー攻撃の被害に遭った割合は上昇傾向にあり、2020 年には「グローバル」とほぼ同じ割合となっている（図 2-4-1）。この増加傾向は、「グローバル」の傾向とも異なって急激であり、これまで以上に国内企業・組織のセキュリティ対策が求められる。



■図 2-4-1「サイバー犯罪」の被害にあったと回答した組織の比率の推移
（出典）PwC Japan グループ「経済犯罪実態調査 2020 日本分析版※380」を基に IPA が編集

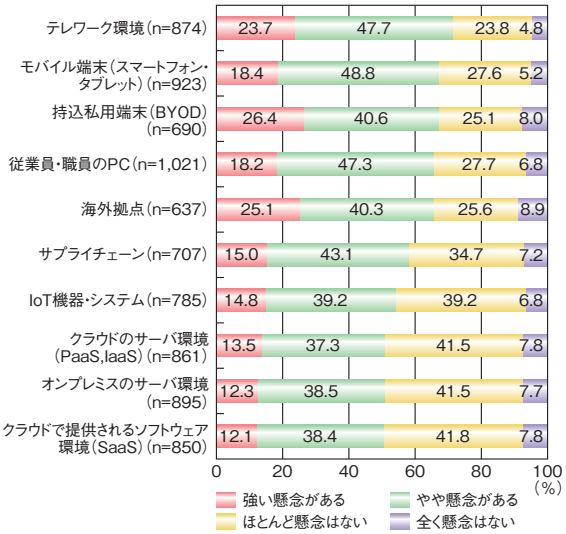
このような背景を踏まえ、企業のセキュリティ対策状況について、以下の資料を基に述べる。

- トレンドマイクロ株式会社（以下、トレンドマイクロ社）：2020 年度 法人組織のセキュリティ動向調査※381（民間企業 980 社及び官公庁自治体 106 団体を対象に調査。以下、トレンドマイクロ社調査）
- NRI セキュアテクノロジーズ株式会社（以下、NRI セキュア社）：NRI Secure Insight 2020※382（国内・海外企業 2,260 社を対象に調査。以下、NRI セキュア社調査）
- IPA：2020 年度サイバーセキュリティ経営ガイドライン実践のためのプラクティスの在り方に関する調査※383（国内企業 930 社を対象に調査。以下、プラクティス調査）

(a) セキュリティ対策の検討状況

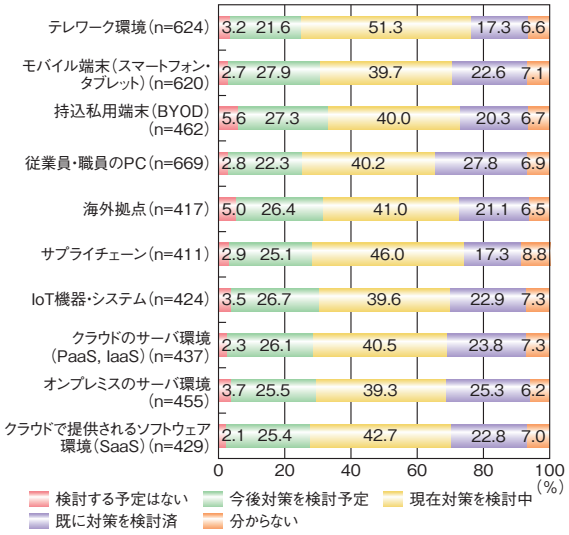
トレンドマイクロ社調査（図 2-4-2）によると、現在利用または今後利用予定がある IT 環境やシステムについて、「強い懸念がある」及び「やや懸念がある」を合わせた割合は、「テレワーク環境」（71.4%）が最も高く、「モバイル端末（スマートフォン・タブレット）」（67.2%）、「持込私用端末（BYOD）」（67.0%）、「従業員・職員の PC」（65.5%）と続く。テレワークの普及によって、これらの懸念が高まっている可能性がある。

また、「強い懸念がある」割合に着目すると、「持込私用端末（BYOD）」（26.4%）に次いで、「海外拠点」（25.1%）が高い。海外に拠点を持つ企業において、国内と比較して海外拠点のセキュリティ対策が課題になっている。

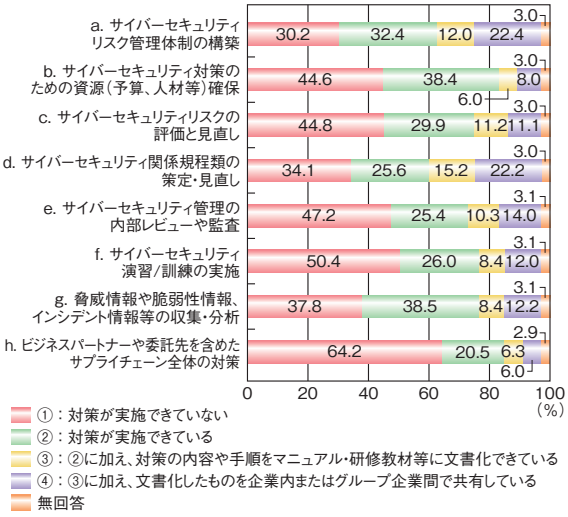


■図 2-4-2 IT 環境やシステムへの今後の懸念
（出典）トレンドマイクロ社「2020 年度 法人組織のセキュリティ動向調査」を基に IPA が編集

図 2-4-3（次ページ）に示すように、懸念がある IT 環境やシステム※384 に対する対策の検討状況について、「既に対策を検討済」の割合が最も低いのは「テレワーク環境」と「サプライチェーン」（ともに 17.3%）である。「テレワーク環境」及び「サプライチェーン」のセキュリティ対策を懸念している企業であっても、検討が不十分なまま導入・



■図 2-4-3　懸念がある IT 環境やシステムに対する対策の検討状況
（出典）トレンドマイクロ社「2020 年度 法人組織のセキュリティ動向調査」を基に IPA が編集



■図 2-4-4　サイバーセキュリティ対策の状況
（出典）IPA「2020 年度サイバーセキュリティ経営ガイドライン実践のためのプラクティスの在り方に関する調査」を基に作成

運用している状況がうかがえる（テレワークの脅威と対策については「3.3 テレワークの情報セキュリティ」参照）。

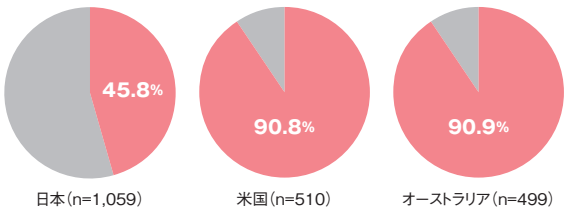
プラクティス調査（図 2-4-4）によると、個々のサイバーセキュリティ対策の実施状況に関して、対策が実施できている（②、③、④の合計）割合が高いのは、「a. サイバーセキュリティリスク管理体制の構築」（66.8%）、「d. サイバーセキュリティ関係規程類の策定・見直し」（63.0%）、及び「g. 脅威情報や脆弱性情報、インシデント情報等の収集・分析」（59.1%）である。このうち、文書化・共有化までできている（③と④の合計）割合が高いのは、「a. サイバーセキュリティリスク管理体制の構築」（34.4%）と「d. サイバーセキュリティ関係規程類の策定・見直し」（37.4%）である。

一方、対策が実施できていない（①）割合は、「h. ビジネスパートナーや委託先を含めたサプライチェーン全体の対策」（64.2%）が最も高く、「f. サイバーセキュリティ演習 / 訓練の実施」（50.4%）、「e. サイバーセキュリティ管理の内部レビューや監査」（47.2%）と続く。このうちサプライチェーン（h.）や演習／訓練（f.）は、サイバーセキュリティ対策を推進する部門以外を巻き込んだ活動であり、高コストやノウハウ・意識付けの不足等により実施が進んでいないことがうかがえる。これは、トレンドマイクロ社調査（前ページ図 2-4-2）において、サプライチェーンに関しては、そこで利用する IT 環境やシステムに対する懸念は比較的少ないことからも推察される。

体制の構築（a.）や規程類の策定・見直し（d.）では、文書化・共有化まではある程度実施できているものの、情報収集・分析（g.）に関しては、文書化・共有化まではできていない実態がうかがわれる。

(b) セキュリティ管理体制の構築状況

NRI セキュア社調査（図 2-4-5）によると、CISO を設置している企業の割合は、米国とオーストラリアが 90% 以上であるのに対し、日本は 45.8% にとどまっている。また、米国とオーストラリアに比べて、「経営層の兼務」の割合（75.2%）が高く、「社外有識者」の割合（1.8%）が低い。



CISOの属性とその割合

	経営層	非経営層	社外有識者
日本（n=1,059）	75.2%	23.0%	1.8%
米国（n=510）	49.8%	38.6%	11.6%
オーストラリア（n=499）	55.9%	33.6%	10.5%

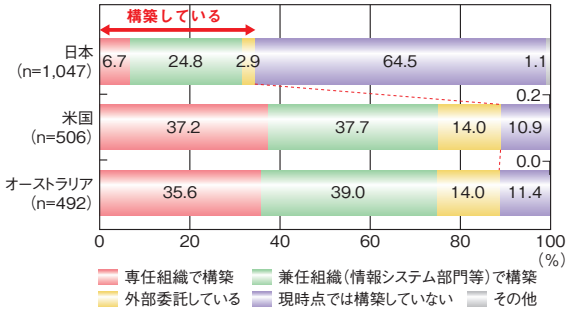
※わからないを除く

■図 2-4-5　CISO を設置している企業
（出典）NRI セキュア社「NRI Secure Insight 2020」を基に IPA が編集

図 2-4-6（次ページ）によると、CSIRT を構築している企業の割合は、米国とオーストラリアが約 90% であるのに対し、日本は 34.4% にとどまっている。また、CSIRT の構築形態では、米国とオーストラリアに比べて「専任組織で構築」の割合が 6.7%、「外部委託している」の割

合が 2.9% とともに低い。

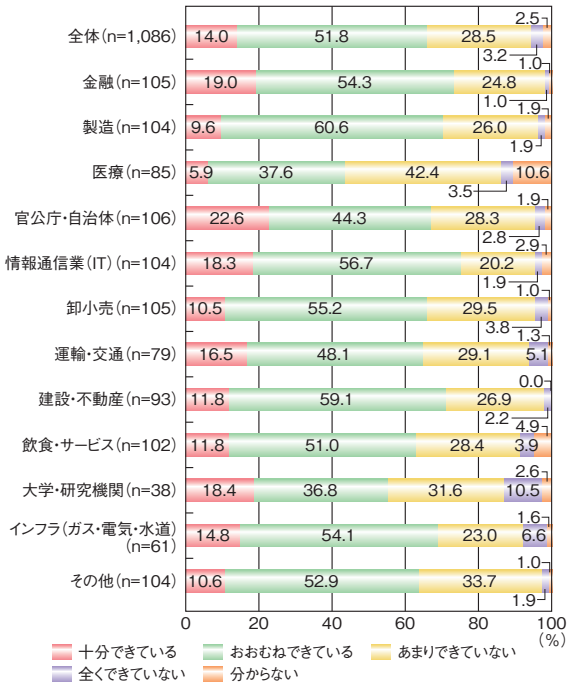
日本の企業では、CISO は経営者の兼務、また CSIRT は情報システム部門等の兼務が多く、専門家の不足、専門知識を持った外部人材の活用不足が推察される（セキュリティ人材に関する政府の施策については「2.3.1 情報セキュリティ人材の状況」参照）。



■図 2-4-6　CSIRT の構築状況
（出典）NRI セキュア社「NRI Secure Insight 2020」を基に IPA が編集

(c) セキュリティリスク管理の業種別実施状況

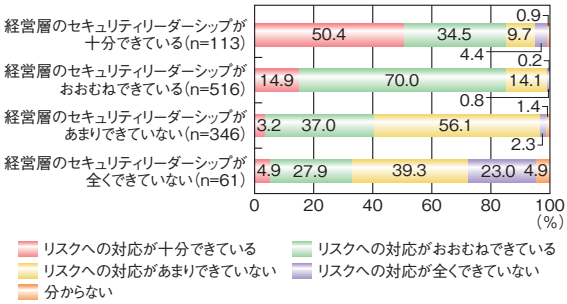
トレンドマイクロ社調査（図 2-4-7）によると、顕在化したリスクを適切に対処する事後のリスク対応の実施状況について、「十分できている」及び「おおむねできている」を合わせた割合は、全体で 65.8% となっており、業種別では「情報通信業（IT）」（75.0%）が最も高く、次いで「金融」（73.3%）が高い。一方、低かったのは、「医療」



■図 2-4-7　リスクへの対応の実施状況（業種別）
（出典）トレンドマイクロ社「2020 年度 法人組織のセキュリティ動向調査」を基に IPA が編集

（43.5%）、次いで「大学・研究機関」（55.2%）である。「医療」や「大学・研究機関」は、近年攻撃対象となることが増え、情報漏えい対策等の強化が望まれていながら、リスク対応が十分できていない業種であることがうかがわれる。

図 2-4-8 によると、「経営層のセキュリティリーダーシップ※385 が十分できている」企業は、「リスクへの対応が十分できている」の割合が 50.4% である。一方、「経営層のセキュリティリーダーシップが全くできていない」企業は、「リスクへの対応が十分できている」の割合はわずか 4.9% である。経営層のリーダーシップの重要性がうかがわれる。



■図 2-4-8　経営層のセキュリティリーダーシップとリスクへの対応の実施状況
（出典）トレンドマイクロ社「2020 年度 法人組織のセキュリティ動向調査」を基に IPA が編集

(d) まとめ

以上のように、国内企業が直面するセキュリティリスクとしては、テレワーク等の新しく常態化する IT 環境への対応、及びガバナンスが弱い海外拠点・業務委託先等のサプライチェーン対策等が懸念される。また対策実施面では、サプライチェーン対策や演習のコストとノウハウ・意識の不足、リスクに関する情報共有の不備、人材不足等による CISO/CSIRT 等の体制の不備等が懸念される状況である。

今後、企業の経営層は、これまで以上にリーダーシップを発揮し、業務アウトソース・人事を含む資源配分の最適化、新しい業務形態への対応、海外事業のガバナンス、サプライチェーンパートナーを含む情報共有等を推進することが求められる。

(2) セキュリティリスクマネジメント

国内の企業・組織は、前項「2.4.1 (1) 情報セキュリティに対する企業の対策状況」で述べたようなセキュリティリスクに直面している。組織のセキュリティリスクを把握・管理するリスクマネジメントは、企業にとって経営・事業

を守るための重要な課題の一つである。また前項で見たとおり、リスクマネジメントには経営層のリーダーシップが欠かせない。このため、経済産業省とIPAは、経営層のセキュリティリスクマネジメント向上のため、2017年に「サイバーセキュリティ経営ガイドライン Ver2.0[※386]」を発行した。また同ガイドラインの実践には対策状況の可視化や、参考となる実践事例（プラクティス）の提示が重要であると考え、それらに関する取り組みを行ってきた。

本項では、上記の活動を踏まえたセキュリティリスクマネジメントについて以下の資料を基に述べる。

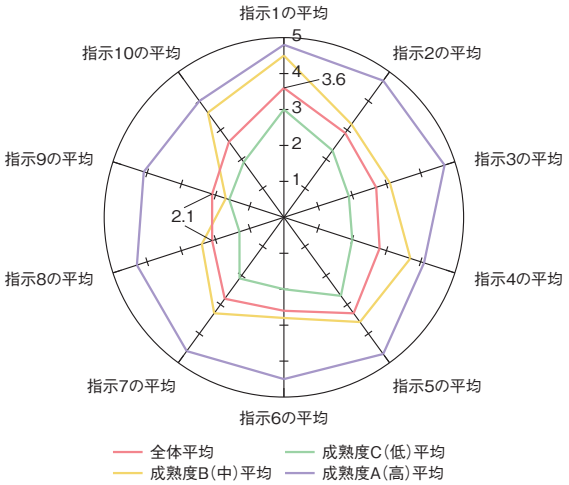
- 「可視化ツールβ版[※387]」の試用に関するJUAS（Japan Users Association of Information Systems：一般社団法人日本情報システム・ユーザー協会）調査（以下、可視化ツール調査、非公開）
- IPA：サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集 第2版[※388]（以下、プラクティス集）
- IPA：2020年度サイバーセキュリティ経営ガイドライン実践のためのプラクティスの在り方に関する調査（以下、プラクティス調査）

(a) 可視化ツールβ版の試用調査結果

本項の可視化ツールとは、サイバーセキュリティ経営ガイドラインにおいて経営層が指示すべき「重要10項目」に関する実施状況を、企業のCISO等がセルフチェックするツールであり、2020年3月にExcel形式によるβ版がリリースされた。またリリース直後、JUASがメンバー企業の協力を得て本ツールの試行を行った。

2020年9月に実施したJUASの可視化ツール調査では、可視化ツールβ版の試行を25社に対して行い、評価結果に基づいて企業を3グループに分け、グループごとの重要10項目の実施状況（以下、セキュリティ成熟度）の平均値を図示した（図2-4-9）。この図によれば、参加25社の全体平均（図2-4-9の赤線部）において、重要10項目の指示のうち、指示1（サイバーセキュリティリスクの認識、組織全体での対応方針の策定）へのセキュリティ成熟度が平均3.6ポイント（最高は5.0ポイント）で最も高い値となった。

一方、セキュリティ成熟度の全体平均において、指示8（インシデントによる被害に備えた復旧体制の整備）、指示9（ビジネスパートナーや委託先を含めたサプライチェーン全体の対策及び状況把握）のセキュリティ成熟度は、ともに2.1ポイントと低く、強化が必要であるとしている。

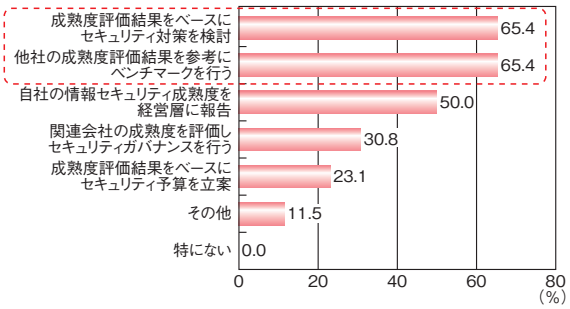


■図2-4-9　重要10項目の実施状況の平均値（n=25）
（出典）JUASの可視化ツール調査を基にIPAが編集

また、同調査において、可視化ツールβ版の利用場面について尋ねた結果、回答の65.4%がセキュリティ対策の検討やベンチマークの利用を想定していた（図2-4-10）。更に、経営層への報告の際のコミュニケーションツールとして可視化ツールを使いたい意図があると考えられる。

プラクティス調査において、セキュリティ対策実施状況の可視化は、対策検討・ベンチマークとしての利用が重要であること、そのためには現状の可視化結果と対策との紐付けが重要であること、が企業や有識者へのインタビューにより示唆された。

これらの結果から、可視化ツールβ版は、企業のセキュリティ成熟度を可視化してベンチマークを行い、具体的な対策を検討するために有効であると考えられる。このような可視化の手法を用いることでセキュリティリスクマネジメントの促進が期待される。



■図2-4-10　可視化ツールβ版の利用場面（n=26）
（出典）JUASの可視化ツール調査を基にIPAが編集

(b) プラクティス集への要望等に関する調査結果

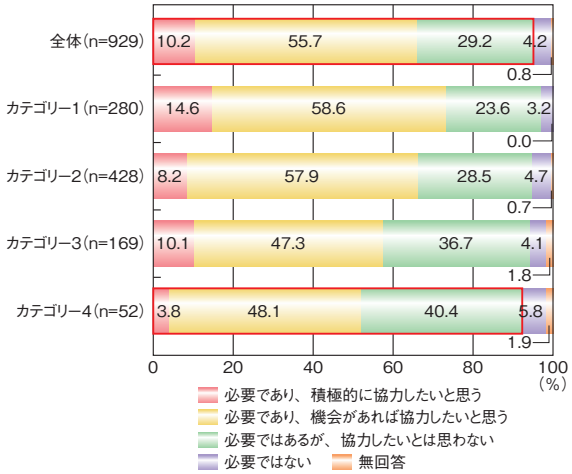
他社のセキュリティマネジメント実践事例を参考にして自社のセキュリティ課題を明らかにし、対策を行うことは

有効と考えられる。IPA は、これからサイバーセキュリティ対策に取り組む企業が重要 10 項目を実施するにあたっての考え方、ヒント、対策事例をまとめたプラクティス集を公開している。2020 年度は、プラクティス集の利用実態を把握し、その作成・共有のプロセスを含めたプラクティス集自体の在り方を検討することを目的に、企業の要望等の調査を実施した。本調査では、プラクティスに対するニーズが企業規模、IT 依存度により変化するとの仮説のもとに、それらに基づく企業の類型（以下、企業像）を定義し、企業像ごとのニーズを調査した。更にこの結果を基に、企業像をセキュリティ対策の成熟度に関して 3 グループに分類し、各グループのニーズを整理した。表 2-4-1 に各グループの特性と、ニーズから導いたセキュリティマネジメントの課題及び有効と思われるプラクティスを示す。

企業の特性	課題・有効なプラクティス
IT 依存度が低く、セキュリティのリソースが十分でない企業	自社の課題や取り組みが必要な領域・テーマが把握できていないため、サイバーセキュリティ体制構築の課題と実現のためのファーストステップを整理したプラクティスが有効。
IT 依存度が中程度以上で IT 化がある程度進んでいる企業	自社の課題や取り組みが必要な領域・テーマもある程度把握している。難度の高いサプライチェーン対策、インシデント対応力の強化や財務面のリスクヘッジ（サイバー保険）等のプラクティスが有効。
IT 依存度が高く、先進的な IT を導入している企業	自社の課題や取り組みが必要な領域・テーマを広く把握している。最新の技術・脅威に関する事例、解決策に関するプラクティスが有効。

■表 2-4-1　IT 依存度による企業分類と課題・対応策

IPA のプラクティス集利用者がコンスタントに増えている等、プラクティスの利用に対する期待はあると考えられる。一方で、プラクティスの収集や共有は一般には容易でない。そこで、プラクティス調査でプラクティスの効果的な収集や共有について尋ねたところ、プラクティスを共同で作成・共有する枠組みについて、「必要である※389-1」と回答した企業は、全体の 95.1% に上る（図 2-4-11）。この図において、カテゴリーとは前述の企業像を表し、カテゴリーの数値が小さい程、IT 依存度が高い（成熟度が高い）。最も IT 依存度の低いカテゴリー 4 の企業においても、作成・共有の枠組みが必要だとする回答は 90% を越えていることから、プラクティスに関する情報共有は、どのカテゴリーの企業にとっても重要と考えられる。



■図 2-4-11　プラクティスを共同で作成・共有する枠組みについて
（出典）IPA「2020 年度サイバーセキュリティガイドライン実践のためのプラクティスの在り方に関する調査」を基に編集

(c) セキュリティリスクマネジメントのフレームワーク

2021 年 2 月 18 日の経済産業省主催の第 7 回産業サイバーセキュリティ研究会 WG2 において、サイバーセキュリティ対策に関する取り組みのフレームワークが整理された。これによると、前掲のプラクティス集や可視化ツールはサイバーセキュリティ経営ガイドライン活用の支援ツールとして位置付けられる※389-2。今後は産業分野別等の実践的なガイドラインを整備するとしている。企業はこのフレームワークを活用してセキュリティリスクマネジメントの可視化・実践に取り組むことが期待される。

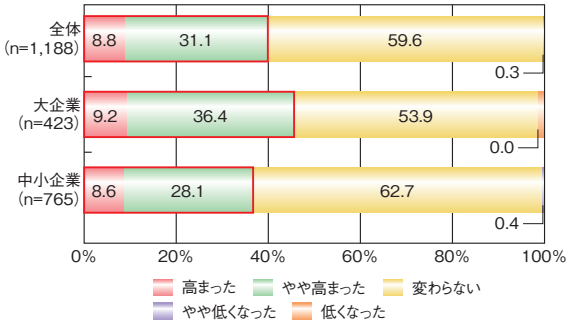
2.4.2 中小企業に向けた情報セキュリティ支援策

本項では、中小企業における情報セキュリティ、対策支援、及び普及啓発・対策ツールの現状について紹介する。

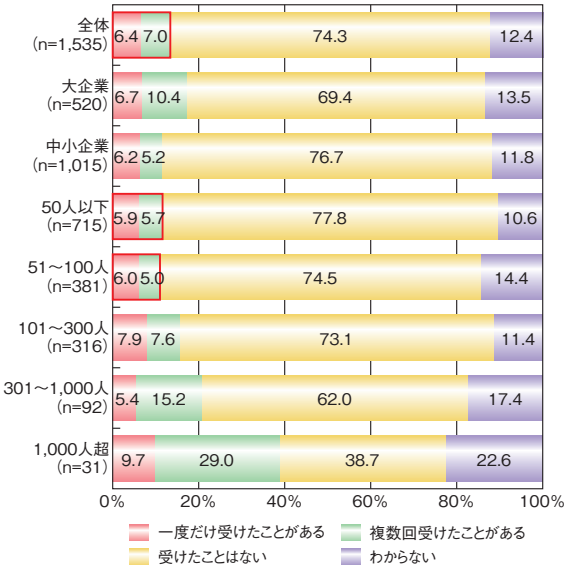
(1) 中小企業の情報セキュリティの現状

一般社団法人日本損害保険協会が 2020 年 12 月 9 日に発表した「国内企業のサイバーリスク意識・対策実態調査 2020 集計報告書※390」によると、新型コロナウイルスの感染拡大前と比べてサイバー攻撃を受ける可能性が「高まった」または「やや高まった」（次ページ図 2-4-12 の赤枠部分）と認識している企業の割合は 39.9% であった。企業規模別に見ると、大企業（45.6%）と比べて、中小企業では 36.7% と低くなっている。

サイバーリスク対策における課題については、「現在行っている対策が十分なのかわからない」と回答した割合が全体で 43.8% と最も高くなっている。「対策をする



■図 2-4-12　新型コロナウイルスの拡大以前と比べたサイバー攻撃を受ける可能性
(出典)一般社団法人日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020 集計報告書」を基に IPA が編集



■図 2-4-14　サイバー被害状況
(出典)一般社団法人日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020 集計報告書」を基に IPA が編集

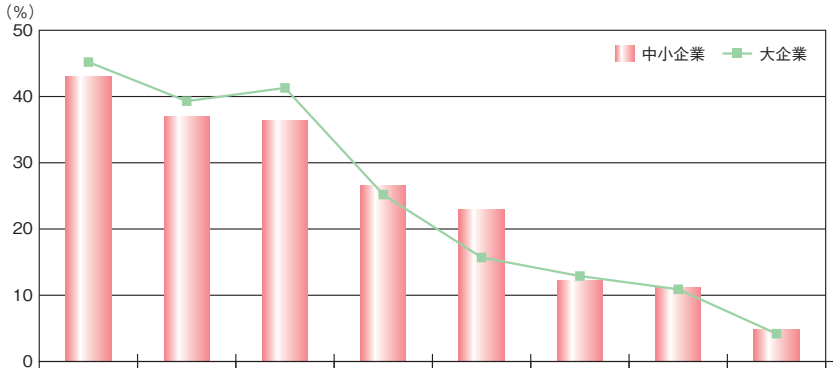
費用が足りない」と回答した企業の割合を企業規模別に見ると、大企業(15.7%)と比べて、中小企業では 23.0%と高くなっている(図 2-4-13)。

サイバー被害状況について、全体では 13.4% の企業がこれまでにサイバー被害を受けたことがあると回答しており、企業規模別に見ると、規模の小さい従業員 100 人以下の企業でも 1 割超がサイバー被害を経験している(図 2-4-14)。

また、サイバー被害を受けたことがある企業のうち、サイバー被害を受けた時期について、全体では 18.5%が「直近半年以内」と回答している。その割合を企業規模別に見ると、大企業 (16.9%) と比べて、中小企業では 19.8%と高くなっている(次ページ図 2-4-15)。

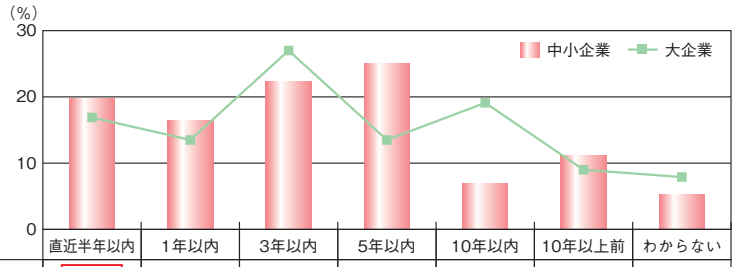
サイバー被害を受けた際の攻撃の種類としては、全体では「マルウェア」や「ランサムウェア」(いずれも31.7%)の割合が最も高く、「不正送金を促すビジネスメール詐欺やフィッシングサイト」(24.4%)、「標的型攻撃」(13.7%)と続いている。それらの割合を企業規模別に見ると、大企業と比べて、いずれも中小企業で割合が高くなっている(次ページ図 2-4-16)。

中小企業ではサイバーセキュリティ対策に十分な予算を割くことができていないため、サイバー攻撃を検知できていないという指摘がある。サイバーセキュリティ対策が強固とはいえない中小企業を標的としたサイバー攻撃やそれに起因する大企業等への被害が顕在化しているこ



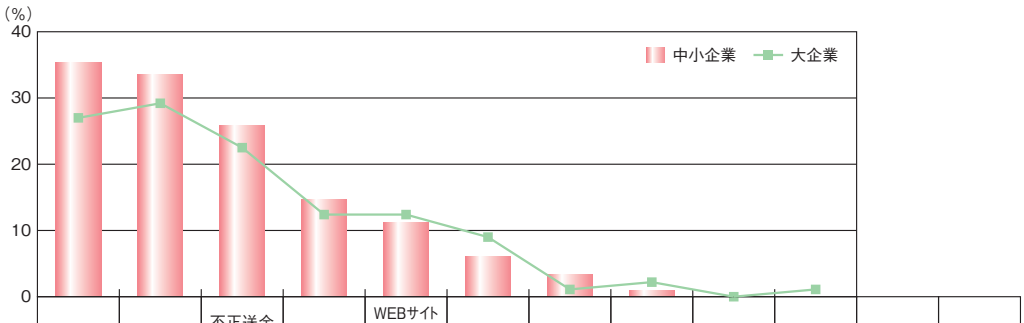
		現在行っている対策が十分なのか分からない	対策の効果測定が難しい	対策をする人手が足りない	社内や周囲に専門の人材がいない	対策をする費用が足りない	対策をする時間が足りない	特に課題はない	対策の必要性について社内の理解が得られず、十分な予算を獲得・確保できない	その他	わからない
全体(n=1,442)		43.8%	37.8%	38.1%	26.1%	20.5%	12.4%	11.1%	4.6%	0.6%	3.6%
企業規模別	大企業(n=496)	45.2%	39.3%	41.3%	25.2%	15.7%	12.9%	10.9%	4.2%	0.4%	4.6%
	中小企業(n=946)	43.0%	37.0%	36.4%	26.6%	23.0%	12.2%	11.2%	4.8%	0.6%	3.1%

■図 2-4-13　サイバーリスク対策における課題(複数回答)
(出典)一般社団法人日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020 集計報告書」を基に IPA が編集



		直近半年以内	1年以内	3年以内	5年以内	10年以内	10年以上前	わからない
全体(n=205)		18.5%	15.1%	24.4%	20.0%	12.2%	10.2%	6.3%
企業規模別	大企業(n=89)	16.9%	13.5%	27.0%	13.5%	19.1%	9.0%	7.9%
	中小企業(n=116)	19.8%	16.4%	22.4%	25.0%	6.9%	11.2%	5.2%

■図 2-4-15　サイバー被害を受けた時期(複数回答)
(出典)一般社団法人日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020 集計報告書」を基に IPA が編集



		マルウェア	ランサムウェア	不正送金を促すビジネスメール詐欺やフィッシングサイト	標的型攻撃	WEBサイトへの不正ログイン・情報窃取およびWEBサイトの改ざん	DDoS(サービス妨害)攻撃	制御システムに対する攻撃	PWリスト攻撃	IoTデバイスに対する攻撃	ゼロデイ攻撃	その他	わからない
全体(n=205)		31.7%	31.7%	24.4%	13.7%	11.7%	7.3%	2.4%	1.5%	0.0%	0.5%	4.9%	10.7%
企業規模別	大企業(n=89)	27.0%	29.2%	22.5%	12.4%	12.4%	9.0%	1.1%	2.2%	0.0%	1.1%	2.2%	14.6%
	中小企業(n=116)	35.3%	33.6%	25.9%	14.7%	11.2%	6.0%	3.4%	0.9%	0.0%	0.0%	6.9%	7.8%

■図 2-4-16　サイバー被害を受けた際の攻撃の種類(複数回答)
(出典)一般社団法人日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020 集計報告書」を基に IPA が編集

ともあり、中小企業を含むサプライチェーン全体でのセキュリティの確保が望まれている。

(2) 中小企業向け情報セキュリティ対策支援施策

政府が 2020 年度に新たに実施した中小企業向け情報セキュリティ対策支援施策を紹介する。

(a) サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)

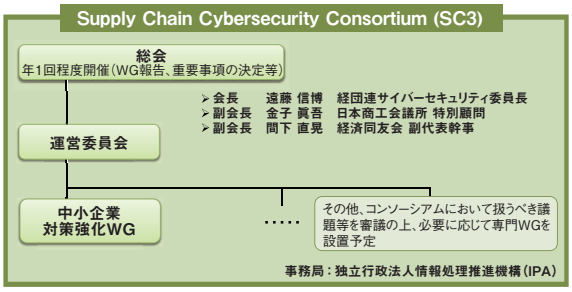
IPA による「情報セキュリティ 10 大脅威 2021[※391]」において、組織への脅威として第 4 位に「サプライチェーンの弱点を悪用した攻撃」が位置付けられているとおり、製造から販売までを含む一連の商流(サプライチェーン)において、セキュリティ対策が強固でない中小企業が攻撃の標的となることで、サプライチェーンに関わる組織が連鎖的に被害を受けるケースが懸念されている。

このような背景のもと、経済産業省は、2020 年 6 月、産業を巡るサイバーセキュリティの状況認識と、今後の取り組みの方向性を取りまとめた報告書[※56]を公表した。本報告書では、企業のリスクマネジメント強化のための基本行動指針として、以下の三つが提示された。

①共有:サプライチェーンを共有する企業間における高密度な情報共有
②報告:機微技術情報の流出懸念がある場合の報告
③公表:多数の関係者に影響する恐れがある場合の公表

そして 2020 年 11 月、この基本行動指針へのコミットメントとともに、産業界を挙げて中小企業を含むサプライチェーン全体のサイバーセキュリティ対策強化を目指す枠組みとして「サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3:Supply Chain Cybersecurity Consortium)[※392]」が設立された(次ページ図 2-4-17)。

SC3 中小企業対策強化 WG では、サイバー攻撃に



■図 2-4-17　SC3 の組織体制
(出典)IPA「サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)」

遭った際の事後支援を中心とした中小企業向けサイバーセキュリティ対策支援の仕組みである「サイバーセキュリティお助け隊サービス」の民間によるサービス展開に向けた検討が行われた(「2.4.2 (2) (b) 中小企業向けサイバーセキュリティ対策支援体制構築事業」参照)。

本検討に基づき、IPA は、2021 年 2 月に「サイバーセキュリティお助け隊サービス」の内容を明確化、同サービスとして充足すべき基準を「サイバーセキュリティお助け隊サービス基準 (1.0 版)※393」として策定・公表した。そして、同基準を充足するサービスのブランド化を通じて普及を図り、中小企業における無理のないサイバーセキュリティ対策の導入・運用について支援を進めることとした。

今後 SC3 では、サイバー攻撃の実態や官民における取り組み等についての情報共有、取引先企業が求める中小企業のセキュリティ水準についての検討等を予定しており、中小企業を含むサプライチェーン全体のサイバーセキュリティ対策について業界横断的な活動を展開していくことが期待される。

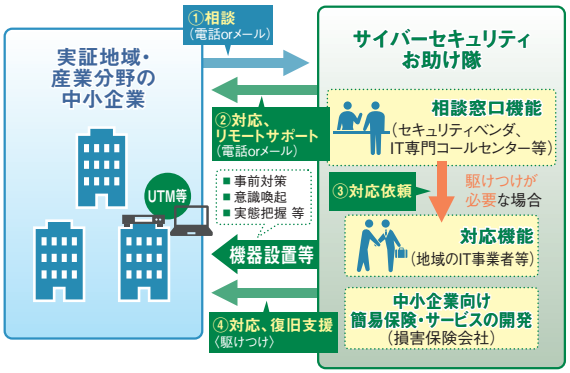
(b) 中小企業向けサイバーセキュリティ対策支援体制構築事業

経済産業省は 2020 年度、IPA を通じて「中小企業向けサイバーセキュリティ対策支援体制構築事業※54」(サイバーセキュリティお助け隊)を実施した(図 2-4-18)。本事業では、全国 24 道県 13 地域(①北海道、②宮城、山形、秋田、青森、③岩手、④岩手、宮城、福島、⑤千葉、埼玉、⑥千葉、⑦岐阜を中心とする中部エリア、⑧愛知、岐阜、三重、⑨滋賀、奈良、和歌山、⑩香川、⑪福岡、佐賀、長崎、熊本、大分、宮崎、⑫熊本、⑬沖縄)と 2 産業分野(⑭防衛・航空宇宙産業及び⑮自動車産業)の中小企業を対象として、サイバーインシデントが発生した際の事後対策支援を中心に実環境における実証を行い、合計 1,117 社の中小企業が参加した。

本実証においては、EDR (Endpoint Detection and Response) サービスにおける不正プログラム (ブラウザ・ハイジャッカー) の検知と駆除や、ウイルス感染の疑いのある通信の UTM (Unified Threat Management) による検知と駆除等の対応を行った。2020 年度は、新型コロナウイルスの影響もあり、リモートで管理可能な支援サービスの提供が多く行われ、インシデント発生に際してもおおむねリモートでの支援対応が実施された。また、UTM 機器等により、18 万件超の社内システムへの侵入等を試みる不審なアクセスが検知される等、2019 年度実証結果と同様に、業種や規模を問わず中小企業においても例外なくサイバー攻撃の危険に晒されていることが明らかとなった。本実証に参加した中小企業からは「サイバー攻撃が可視化され実際に攻撃を受けていることが認識できてよかった」「サイバーセキュリティ対策を実施していることは取引先に対する PR 材料にもなり、良いきっかけをもらえた」等の声が寄せられた。

このようなサイバー攻撃の危険があっても、人材・コスト面での制約もある中でセキュリティ対策に取り組むことができる中小企業は多くない。「サイバーセキュリティお助け隊サービス」の今後の民間でのサービス展開に際しては、個別の細やかなサポートと同時に、サービス内容のスリム化や導入・運用負荷を下げることが必要と考えられる。

2021 年度以降は、2 年間の実証事業で得られた知見、及び SC3 中小企業対策強化 WG の議論を踏まえた「サイバーセキュリティお助け隊サービス」のブランド化・普及により、中小企業において無理なくサイバーセキュリティ対策の導入・運用が可能となることが期待される。



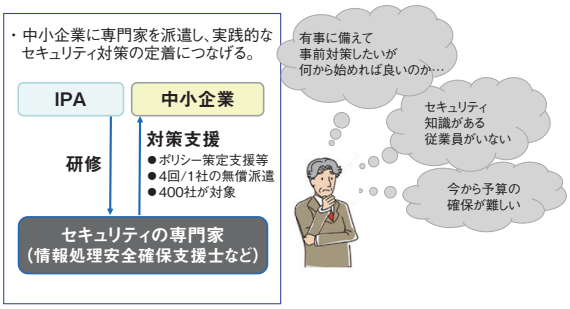
■図 2-4-18　サイバーセキュリティお助け隊の事業イメージ
(出典)IPA「サイバーセキュリティお助け隊(令和 2 年度中小企業向けサイバーセキュリティ対策支援体制構築事業)※54」を基に編集

(c) 中小企業の情報セキュリティマネジメント指導業務

経済産業省は 2020 年度、IPA を通じて、「中小企業の情報セキュリティマネジメント指導業務※394」を実施

した（図 2-4-19）。本事業では、全国の中小企業を対象として、情報処理安全確保支援士等の専門家が訪問し、セキュリティリスクの診断、情報セキュリティマネジメントに必要な基本方針・規程の策定支援等を実施した。

本事業には、全国の中小企業 395 社が参加した。このうち 97.6% の企業が成果を得られたと回答し、指導した専門家も 84.4% が指導先企業の経営層の意識が向上したと回答した。また、63.8% の企業が今後も専門家による指導・支援を希望すると回答した。本事業で作成し有効性が確認された指導要領等を、指導ツールとして専門家へ提供すること等が計画されており、今後の中小企業支援に活用されることが期待される。



■図 2-4-19　情報セキュリティマネジメント指導業務の事業イメージ
（出典）IPA「令和２年度中小企業の情報セキュリティマネジメント指導業務」を基に編集

(d) 中小企業サイバーセキュリティ対策促進事業

経済産業省は 2020 年度、「中小企業サイバーセキュリティ対策促進事業（地域 SECUNITY 形成促進事業）」を実施した。本事業では、地域の企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ（地域 SECUNITY）の形成、及びセキュリティ対策の実態把握のための調査やセミナー等を行った。将来的には、地域のニーズとシーズのマッチングによる課題解決・付加価値創出の場（コラボレーション・プラットフォーム）へと発展することを目指している（コラボレーション・プラットフォームについては「2.1.2 (1) (c) WG3（サイバーセキュリティビジネス化）」参照）。

また、2021 年 2 月 17 日、地域のセキュリティコミュニティの活動事例調査を踏まえ、「地域セキュリティコミュニティ【地域 SECUNITY】形成・運営のためのプラクティス集第 1 版[※395]」を公開した（図 2-4-20）。本資料では、コミュニティ形成の際に参考となる事例とポイント、地域のセキュリティコミュニティが主催するイベント等で活用できるセキュリティ講師派遣制度等の情報・問い合わせ先リストがまとめられている。

■図 2-4-20　地域セキュリティコミュニティ【地域 SECUNITY】形成・運営のためのプラクティス集のイメージ
（出典）経済産業省「地域セキュリティコミュニティ【地域 SECUNITY】形成・運営のためのプラクティス集」

(3) 普及啓発・対策ツール

中小企業に向けた情報セキュリティの普及啓発活動や対策ツールを紹介する。

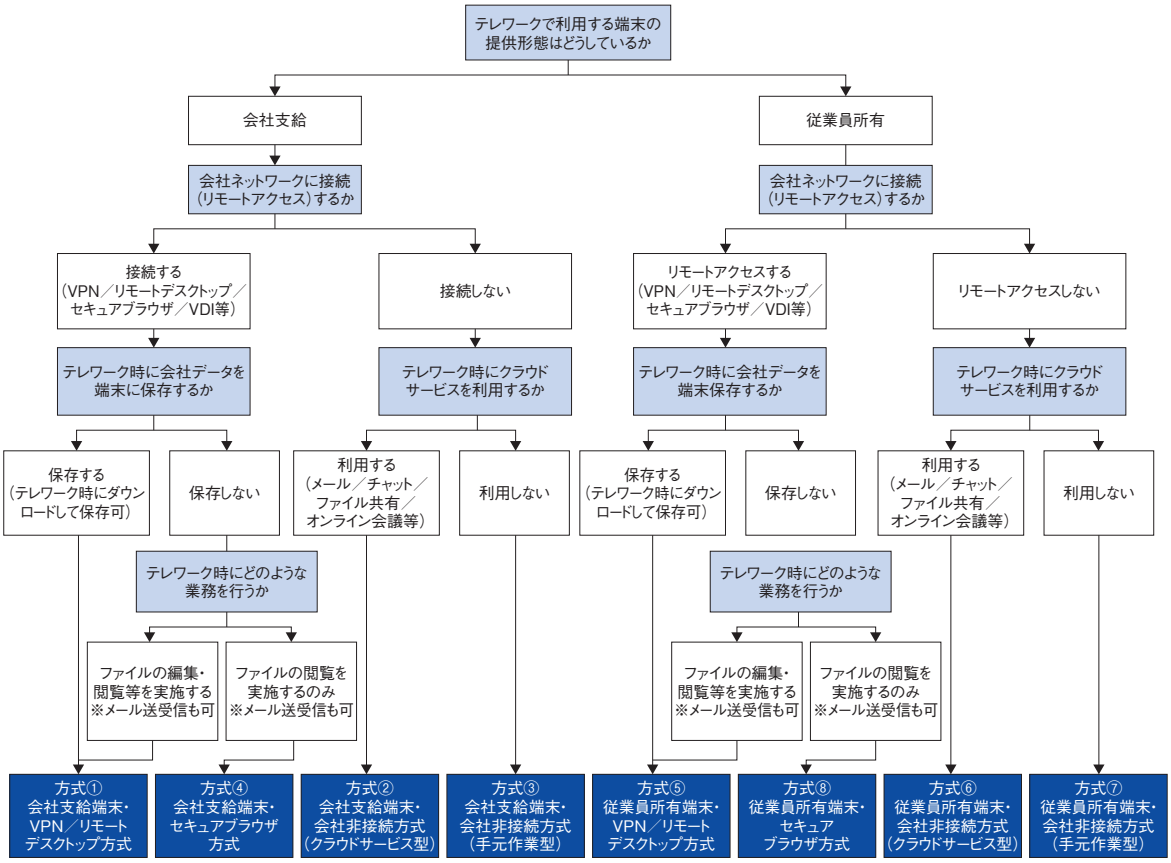
(a) 中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）

総務省は 2020 年 9 月 11 日、「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（初版）」を公表した。本手引きは、セキュリティの専任担当がいないような中小企業等におけるシステム管理担当者を対象として、テレワークを実施する際に最低限のセキュリティを確保するためのチェックリストを提供している。また、テレワークでよく利用されるオンライン会議ツール等の製品（Cisco Webex Meetings、Microsoft Teams、Zoom）の設定解説資料を同時公開している[※396]。

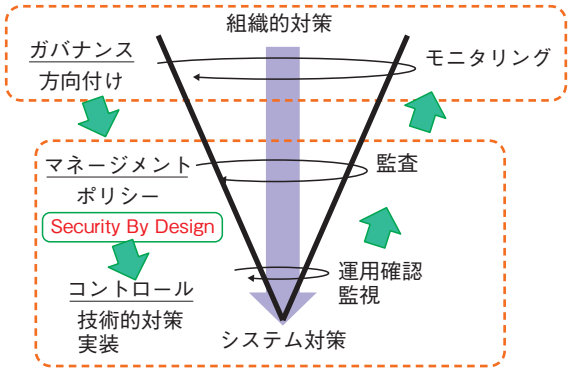
2021 年 5 月 31 日、「テレワークセキュリティガイドライン」の改定を受けて「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（第 2 版）[※397]」を公表した（次ページ図 2-4-21）。今後、設定解説資料への対象製品の追加が予定されている。

(b) 中小企業において目指す Security By Design

JNSA は 2020 年 11 月 5 日、「中小企業において目指す Security By Design[※398]」を公開した（次ページ図 2-4-22）。IT システムの開発・導入においては、機能要件の定義が主になり、セキュリティ機能は非機能要件として、重要視されず、後回しにされることが多々ある。しかし、一般に IT システムの開発・導入においては、後工程での修正程、コストが増加する傾向にあり、IT システム導入後、十分なセキュリティ対策を行うことは、



■図 2-4-21　テレワーク方式確認のフローチャート
(出典)総務省「中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)(第２版)」



■図 2-4-22　V 字モデルにおける「Security By Design」の位置付けのイメージ
(出典)JNSA「中小企業において目指す Security By Design」

困難となる。従って、IT システムの企画･設計段階から、セキュリティを考慮した設計(Security by Design)の導入が重要となる。本資料では、中小企業の情報システム部門が考えるべき IT システムの導入、運用、廃止までのライフサイクルを考慮した情報セキュリティのあるべき姿の検討結果をまとめている。

(c) SECURITY ACTION

IPA では、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度「SECURITY ACTION※399」を運営し、中小企業と関連の深い中小企業支援機関、士業団体、IT 関連団体と連携して SECURITY ACTION を通じた情報セキュリティの普及啓発を行っている(図 2-4-23)。

SECURITY ACTION に基づく自己宣言は、秋田県リモートワーク環境整備支援事業費補助金や堺市テレワーク導入支援補助金の申請要件になっていたほか、公的な補助金制度の申請要件としても活用されている。

2021 年 3 月末時点の宣言数は 14 万件(個人事業主を含む)を超えている。今後より多くの中小企業が SECURITY ACTION を宣言し、社内の意識付けや

■図 2-4-23　SECURITY ACTION のロゴマーク

社外への信頼性のアピール等に活用し、対策を推進することが望まれる。

2.4.3 教育機関・政府及び地方公共団体等法人における対策状況

教育機関・政府及び地方公共団体等法人における対策状況について、公表されている資料に基づいて述べる。

(1) 教育機関における個人情報紛失・漏えいの現状、文部科学省の対策、事故の事例

教育ネットワーク情報セキュリティ推進委員会（ISEN：Information Security for Education Network）は、毎年、学校等教育関連機関で発生した個人情報の紛失・漏えい事故について公開情報を調査し、公表している。2020年11月には、「令和元年度（2019年度）学校・教育機関における個人情報漏えい事故の発生状況 −調査報告書− 第2版※400」（以下、ISEN報告書）を公表した。本項では、ISEN報告書に基づいて、2019年4月1日～2020年3月31日の事故の傾向について述べる。次いで、政府が示している対策を紹介した後、事故事例について述べる。

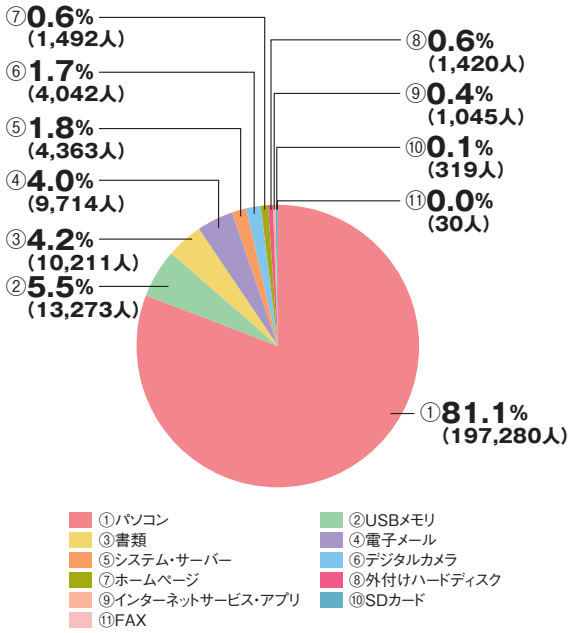
ISEN報告書によると、2019年度は226件の個人情報漏えい事故が発生し、合わせて23万2,857人分の個人情報が漏えいした。過去2年（2018年度5万7,629人、2017年度12万7,278人）に比べ急増しており、過去15年のうちで2番目に多い年度であった。

漏えいした個人情報の人数を経路・媒体ごとに比較すると、図2-4-24に示すように、2019年度は「パソコン」が全体の81.1%を占めており、2位の「USBメモリ」（5.5%）以下を大きく引き離している。

また事故の種類ごとの発生件数を調べると、「紛失・置き忘れ」「盗難」「誤廃棄」のように「意図せず失くす」事故が全体の約67%に上ることが分かる（図2-4-25）。

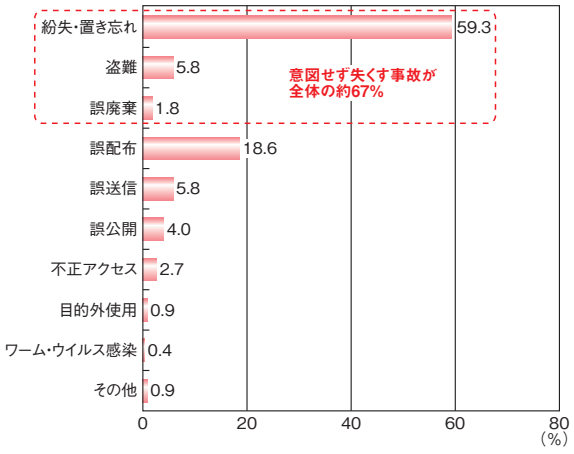
これらのことから、ノートパソコンやUSBメモリ等可搬性のある媒体を失くすことによる個人情報漏えいの対策に取り組むことで、大きな改善が見込めると推察される。

これらに有効な対策として、文部科学省の「教育情報セキュリティポリシーに関するガイドライン※401」では、ログインパスワード、起動時のBIOS・ハードディスク等のパスワード、多要素認証、セキュリティチップの暗号化機能、遠隔消去機能（リモートワイプ）等の利用を挙げている。また同ガイドラインでは、モバイル端末の持ち出しや外部での作業の実施は許可制とするのが適切であるとしており、情報セキュリティポリシーの例文に、端末や電子媒体の持ち出し・外部での作業の制限に関する事項を含めている。



※1件の事故で複数の経路・媒体から漏えいした場合は、それぞれの経路・媒体に含まれていた個人情報漏えい人数を合算

■図2-4-24 漏えい経路・媒体別個人情報漏えい人数
（出典）ISEN報告書を基にIPAが作成



■図2-4-25 漏えい事故種別発生割合
（出典）ISEN報告書を基にIPAが作成

次に、教育機関等における個人情報紛失の事故事例を取り上げる。2020年2月29日、金沢大学の教員が海外出張中にノートパソコンの盗難に遭い、教職員と学生の個人情報2万件以上を含むデータファイルを紛失した。これらの個人情報は、持ち出すにあたって保護管理者の許可を得ておらず、またパスワード設定等の対策も施されていなかった※402。2021年2月8日、東京藝術大学は、受験関係書類等個人情報115件が入った教員のノートパソコンが、学内の研究室から盗まれた

と発表した。これらの情報を格納したファイルには、パスワード設定が施されていなかった※403。2021年3月5日、立教大学は、91名分の一般選抜に関する個人情報が入ったUSBメモリを紛失したと発表した。USBメモリとファイルには、パスワードロック等の対策が施されていなかった※404。

このように、パソコンやUSB等個人情報を保存した媒体を意図せずに失くし、かつ有効な対策が施されていない事例が後を絶たない。前述のガイドライン等を参考に、対策の徹底が望まれる。

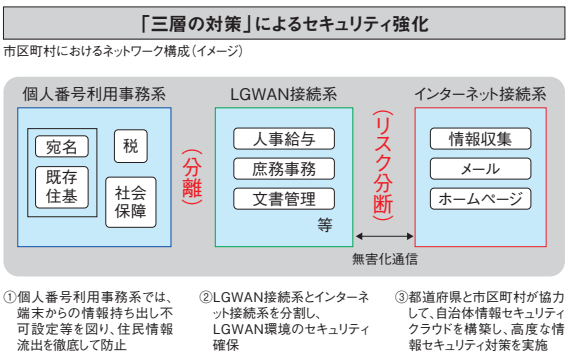
(2) 地方自治体等における対策状況

本項では、自治体等の情報セキュリティ対策とその課題、及び課題解決・改善のための対策見直しについて、総務省が2020年5月に公表した「自治体情報セキュリティ対策の見直しについて※405」(以下、「対策見直し」)に基づき、一部に他の公的機関や地方自治体から公表された資料を参照して述べる。

(a) 地方自治体等の従来対策

2015年5月、日本年金機構において、標的型攻撃による約125万件の個人情報流出が起きた。これを受け総務省は、同年12月に総務大臣通知「新たな自治体情報セキュリティ対策の抜本的強化について」を出し、自治体に「三層の対策」を講じるよう要請した。この対策は、自治体のネットワークを、住民情報等の特に機密性の高い情報を扱う「マイナンバー利用事務系」、職員に関する機微情報や非公開情報等の機密性の高い情報を扱う「LGWAN※406接続系」、インターネットメールや機密性の低い情報を扱う「インターネット接続系」の三つのセグメントに分離・分割するものである(図2-4-26)。

特に「マイナンバー利用事務系」(図2-4-26では「個人番号利用事務系」)をセグメントに分離することにより、



■図2-4-26 「三層の対策」によるセキュリティ強化
(出典)総務省「自治体情報セキュリティ対策の見直しのポイント※407」

住民情報の徹底した流出防止を図っている。この要請を受け、自治体は「三層の対策」への対応を2017年7月までに完了した。

更に、自治体では総務省の指導のもと、「自治体情報セキュリティクラウド」を構築した。それまで自治体ごとに行われていたインターネット接続と情報セキュリティ対策を、原則、都道府県単位に集約することで、セキュリティ対策の水準引き上げを図る施策である。

(b) 課題

前項で述べた対策の課題、発生したインシデントにより見えてきた課題について述べる。

- 従来対策の課題

  「対策見直し」によれば、これらの従来の対策により、インシデントやウイルスへの感染は、短期間で大幅に減少したという。その一方で、ネットワークを分離・分割したことでユーザビリティが下がり、自治体の事務効率に影響していると指摘された。具体的には、住民等によるオンラインの行政手続きデータをマイナンバー利用事務系に取り込んだり、メールの添付ファイルを取得したりすることが制限されているとの指摘である。加えて、働き方改革に伴うテレワーク実施やWeb会議、グループウェア等コミュニケーションツールの利用に制約がある等の課題も浮き彫りになった。

  また、自治体情報セキュリティクラウドについても、自治体へのアンケート調査の結果等から、個々のクラウドによって導入している機能や運営事業者のレベルに差異があることが判明した。また次に述べるインシデント等により、機器故障時や災害発生時の可用性等に課題があることが判明した。

- 重大インシデントにより判明した課題

  2019年12月、日本電子計算株式会社による自治体向けクラウドサービスに障害が発生、全国53団体の業務に影響し、自治体事務の一部には長期の支障が残った。直接の原因は、故障したストレージに依存しているシステムが利用できなくなったこと、データバックアップが不十分だったこと等であり、障害時の可用性の確保に課題があることが判明した。

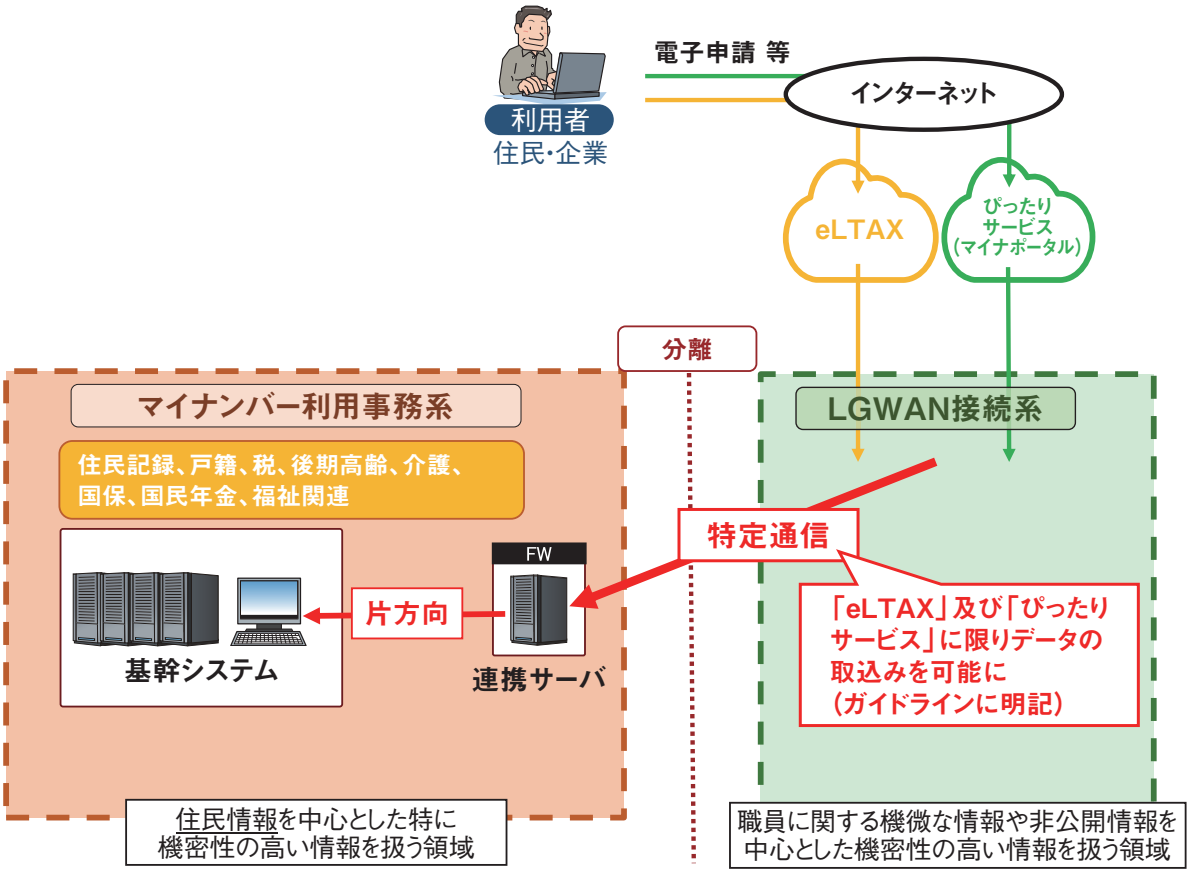
  また同月、神奈川県において、契約満了でリース事業者に返却され廃棄予定だったハードディスクが、不正に売却されたことによる情報流出のインシデントが発生し、対策の不備が判明した。当面の対応として、重要な情報を格納する記憶装置の廃棄にあたっては、物理的・磁気的に破壊すること、これらの処置

の完了まで自治体職員が立ち会うこと等の要請が行われた。

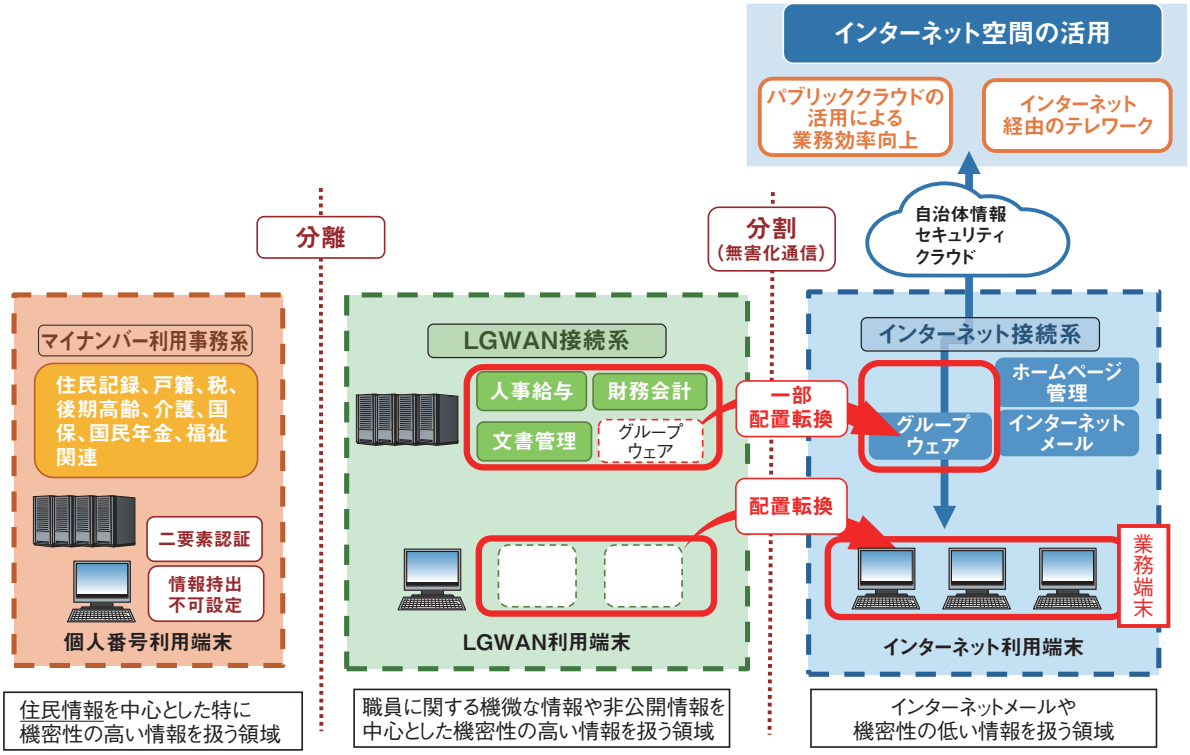
(c) 課題解決・改善のための対策見直し及び関連する動き

前述の課題を解決・改善する対策について、「対策見直し」に記載された主な事項とそれに関連した地方自治体・公的機関の動きについて述べる。

- 「三層の対策」におけるマイナンバー事務処理系の分離の見直し
  住民情報の流出防止徹底を重視し、マイナンバー事務処理系の他セグメントからの分離は、従来どおり維持した上で、住民等からのインターネット経由の申請データ等をこのセグメントに取り込めるように見直すとしている。具体的には、十分なセキュリティが確保されていることを国が確認した特定の通信(「eLTAX※408」と「ぴったりサービス※409」)を経由する場合に限って、データを取り込めるようにする(図 2-4-27)。
- 「三層の対策」における LGWAN 接続系とインターネット接続系の分割の見直し
  自治体内部の業務端末や、人事給与、財務会計等内部管理のシステムは、これまで LGWAN 接続系のセグメントに配置されていた。この一部については、業務効率改善を目的として、インターネット接続系に移動する新たなモデルが示された(次ページ図 2-4-28)。ただし、自治体がこのモデルを採用するには、セキュリティを維持するための条件を満たすことが求められる。具体的には情報資産単位でのアクセス制御、セキュリティ監視やセキュリティインシデントへの即応体制(CSIRT)の整備、職員のセキュリティリテラシーの向上等である。
- 自治体向けのテレワークの仕組みの検討
  本見直しまで、セキュリティ確保の観点からリモートアクセスの利用は限定的であったが、働き方改革等の動きを受け、テレワークの導入検討が検討会※410で行われた。まず、インターネットを介さずに LGWAN 接続系へリモートアクセスするための技術要件等が検討され、2020 年 1 月に中間報告が取りまとめられた。また、地方公共団体情報システム機構(J-LIS:Japan Agency for Local Authority Information Systems)は 2020 年 10 月、IPA と共同で、自治体職員が自宅から LGWAN 接続系のパソコンに接続する仕組み

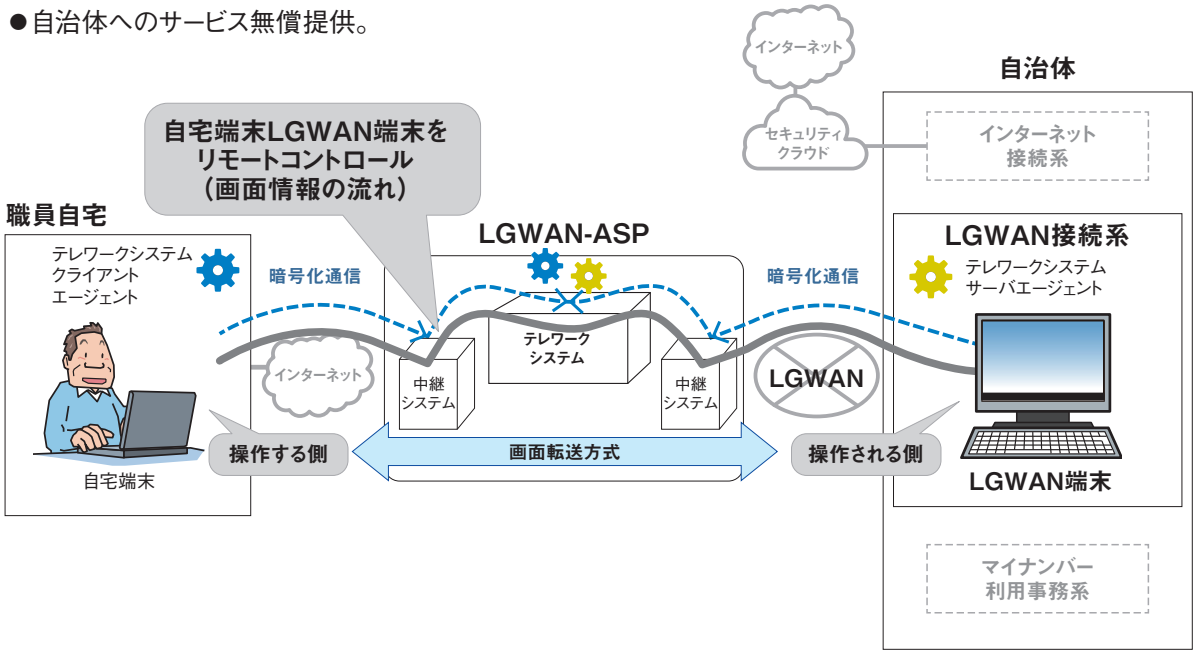


■図 2-4-27　マイナンバー利用事務系の分離に係る見直し
(出典)総務省「自治体情報セキュリティ対策の見直しのポイント」を基に IPA が編集



■図 2-4-28　LGWAN 接続系とインターネット接続系の分割の見直し
（出典）総務省「自治体情報セキュリティ対策の見直しのポイント」を基に IPA が編集

●職員宅から自治体LGWAN接続系へのテレワークを可能とするサービス提供。（リモートコントロール方式）
●LGWAN-ASPを介した職員自宅と自治体庁内の接続。
●自治体へのサービス無償提供。



■図 2-4-29　自治体テレワークシステム for LGWAN
（出典）J-LIS「緊急事態宣言（令和3年1月）の発出に伴う『自治体テレワークシステム for LGWAN』の一時提供について[※412]」を基に IPA が編集

「自治体テレワークシステム for LGWAN」（図 2-4-29）を提供し、テレワークの実証実験を行うとした[※411]。更に、新型インフルエンザ等対策特別措置法の規定に基づく緊急事態宣言の発出に伴い、自治体事務の業務継続の観点からテレワークの必要性が高まったことを受けて、2021 年 1 月、宣言の対象区域となった都道府県の自治体に対して、上記システムを一時的に提供することとなった[※412]。

- 自治体情報セキュリティクラウドの見直し

  自治体情報セキュリティクラウドは更新の時期が近づいており、前述の「対策見直し」は、サイバー攻撃の増加等の変化を踏まえた次期クラウドの在り方の検討が必要であるとしている。

  また現行の自治体情報セキュリティクラウドは、機能や運営事業者のレベルにばらつきが見られるが、次期クラウドではこうしたばらつきを抑え一定の水準を確保するため、総務省が標準的な要件を整備・提示することが望ましいとしている。2020年8月、総務省はこれを受けて、次期自治体情報セキュリティクラウドに係る標準要件※413を取りまとめ、公表した。

  また「対策見直し」は、新たなセキュリティ脅威に対抗するために、SOC※414の強化も必要であるとしている。加えて、災害発生時等に住民からのアクセスが輻輳した場合でも情報発信機能の可用性を維持するため、CDN※415が必要であるとしている。これらの要件は、前述の標準要件に盛り込まれた。

  こうした動きを背景に、各自治体では、それぞれが運営する自治体情報セキュリティクラウドの更新に向けて、具体的な取り組みが進められている。例えば、三重県では現行のセキュリティクラウドが2022年3月に保守期限を迎えることから、システム全体のクラウド化を前提としたシステム構築の検討を始める※416としており、茨城県でも同様の検討が始まっている※417。

- その他の対策見直し

  「対策見直し」では、自治体におけるクラウドサービスの選定にあたっては、クラウド上で運用するシステムごとに必要な可用性が提供されることを確認したり、SLA※418を含む契約を推進したりすることが必要としている。また、リース満了等による機器の廃棄に際しては、格納情報の機密性に応じた適切な廃棄の手法等を採用することも必要としている。

  総務省は、2020年12月に、本項で述べた検討内容を踏まえて「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改訂を行った（「2.1.3(3)(a)自治体情報セキュリティ対策」参照）。

2.4.4 一般利用者における対策状況

IPAが実施した「2020年度情報セキュリティに対する意識調査【倫理編】【脅威編】※419」の報告書の内容、及び追加分析の結果を基に、一般利用者におけるセキュリティ対策状況とその背景等を考察する。

2020年度調査では、対策の実施状況の設問において、パソコン利用者向けに20項目、スマートデバイス利用者向けに17項目の小問を設け調査した。図2-4-30（次ページ）と図2-4-33（次々ページ）は、それらの項目について、対策の実施率※420を高い順から並べたものである。なお、本項ではグラフの項目名を本文中で省略して記載する場合がある。

(1) パソコン利用者の対策状況

対策の実施率が高かった上位3位は、「怪しいと思ったウェブサイトに行き着いたら先に進まない、情報を入力しない」（76.9%）、「メールの添付や本文中のURLを不用意にクリックしない」（69.6%）、「ファイルのダウンロード時に安全性や信頼性を判断」（69.5%）であった。また上位8位までの実施率が50%を超えており、一般利用者において、基本的なセキュリティ対策がある程度定着していることがうかがえる（次ページ図2-4-30）。

下位3位は、「重要なファイルはパスワード付USBメモリでの持ち出し、パスワードをかけてメールを送信する」「無線LANルータの暗号化キーの変更」「HDDなど外部記憶装置全体の暗号化」であり、いずれも2割強の実施率であった。これら対策の実施率は例年最も低い傾向である。

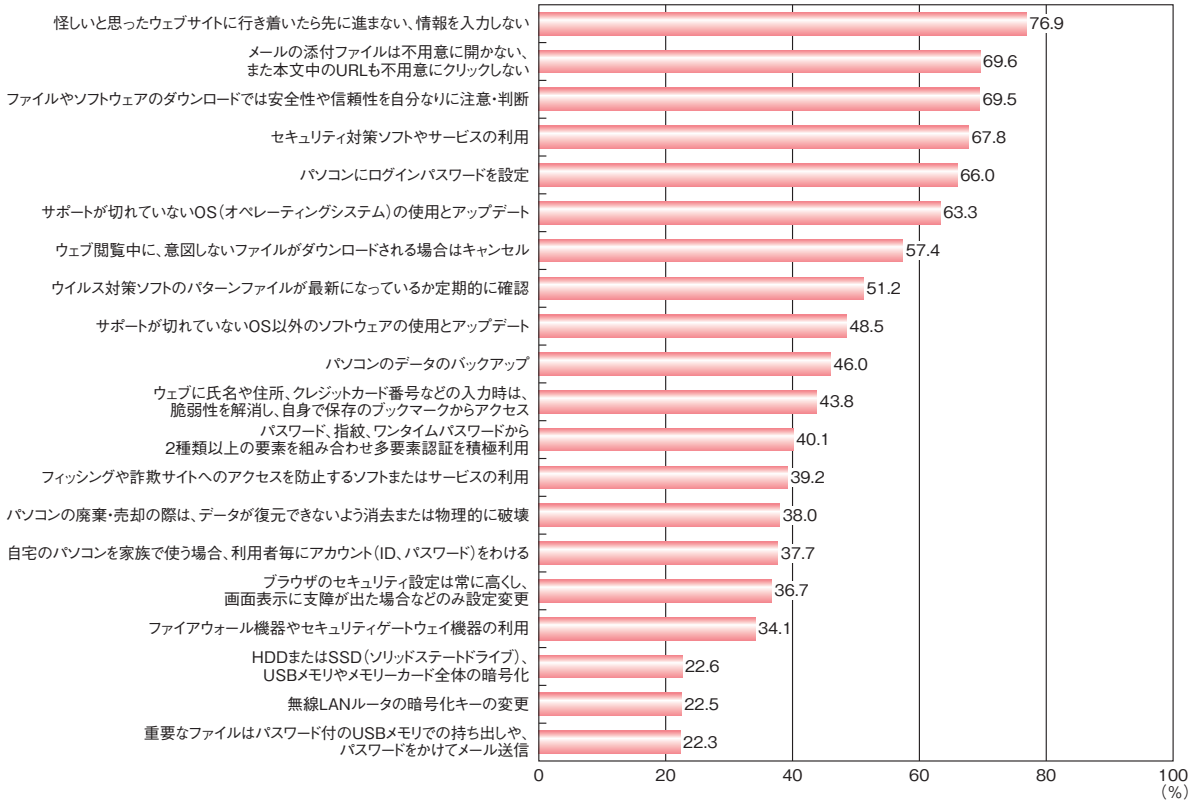
基本的なセキュリティ対策の一つとして挙げられる「サポートの切れていないOSの使用とアップデート」の実施率が全体では63.3%であったが、性別で実施率に差があり、男性が69.4%、女性が55.0%と約15%の開きがあった（次ページ図2-4-31）。

一方、男女で実施率がほぼ同程度となった対策は三つあった。それらは専用のソフトウェアや機器を使う必要がなく、自身の知識や注意等、意識次第で実施可能な対策で、「家族で自宅のパソコンを使う場合、利用者ごとにアカウントを分けている」「怪しいと思ったウェブサイトに行きついたら先に進まない、情報を入力しない」「パソコンにはログインパスワードを設定している」であった（次ページ図2-4-32）。

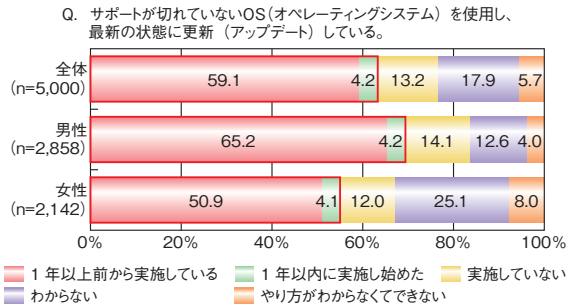
(2) スマートデバイス利用者の対策状況

2019年度以前の同調査では、スマートフォンやタブレットの利用を念頭に置いた対策の実施状況を調査していたが、本年はスマートスピーカーやネットワークカメラ等に対する対策の項目も新たに設けた。

対策の実施率が高かった上位3位は、「端末内のアプリのアップデート」（63.6%）、「公式サイト、マーケットか



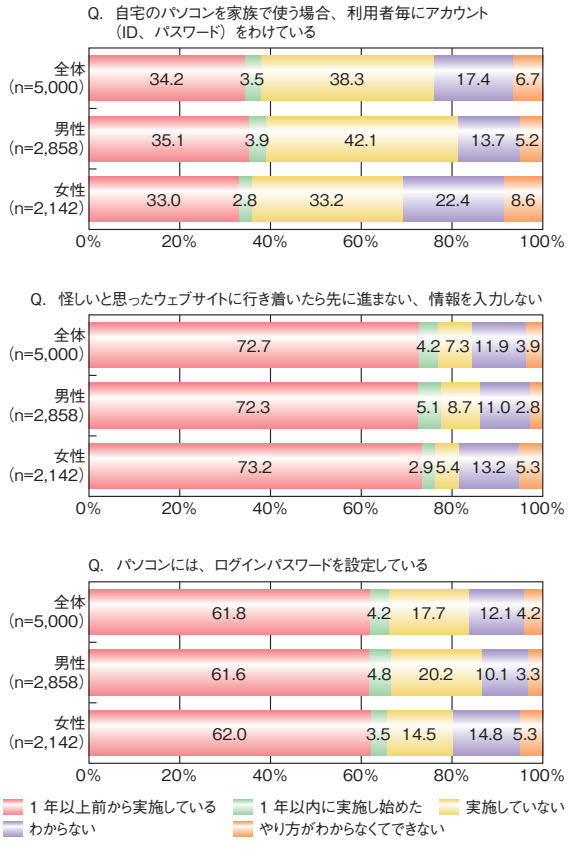
■図 2-4-30　パソコン利用者の対策実施状況



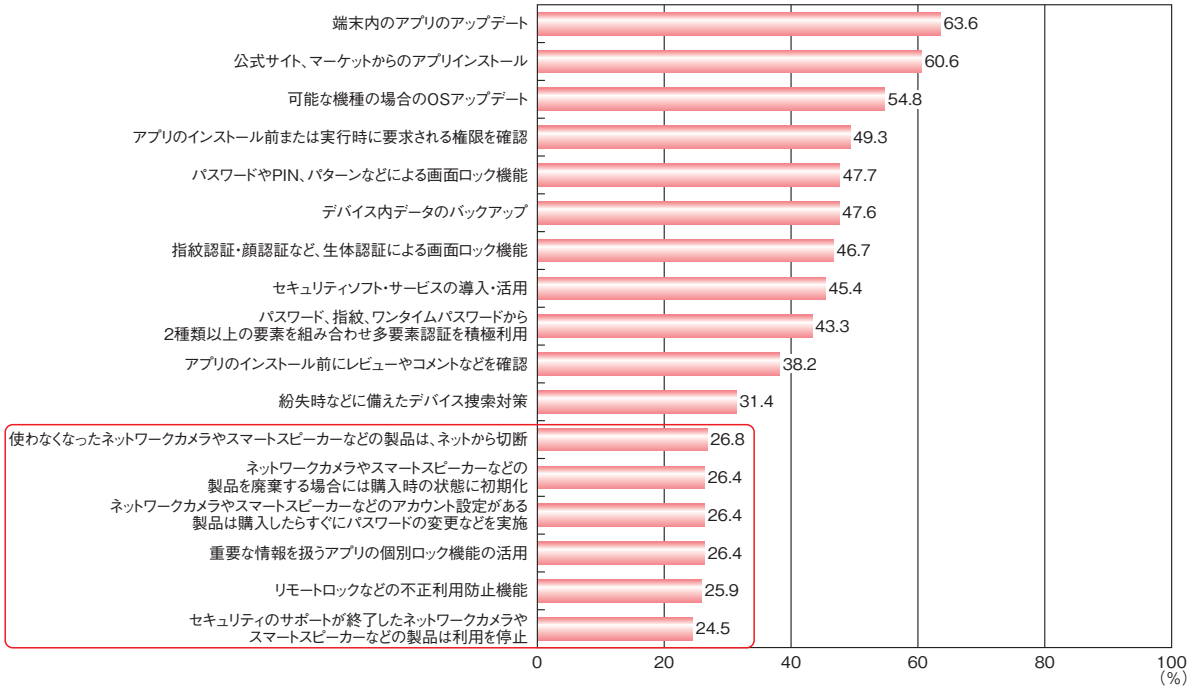
■図 2-4-31　パソコン利用者の OS アップデートに関する対策実施状況

らのアプリのインストール」（60.6%）、「OS のアップデート」（54.8%）であり、スマートフォンに求められる基本的な対策が並んだ（次ページ図 2-4-33）。反対に実施率が低かったのは、今回の調査で新たに設けた四つの項目と、スマートフォンのリモートロック設定及びアプリの個別ロック機能の活用に関する項目、の計六つ（次ページ図 2-4-33 の赤枠部分）で、いずれも 25% 前後の実施率であった。

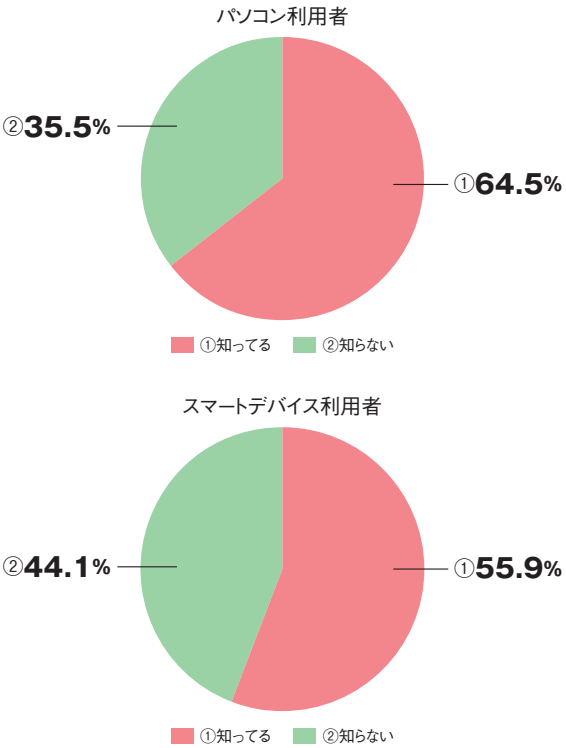
今回の調査結果から、IoT 機器のセキュリティ対策の実施状況はまだ途上で、対策の必要性及び方法について一層の普及啓発が必要と考えられる。



■図 2-4-32　パソコン利用者で男女の実施率が同程度の対策実施状況



■図 2-4-33　スマートデバイス利用者の対策実施状況



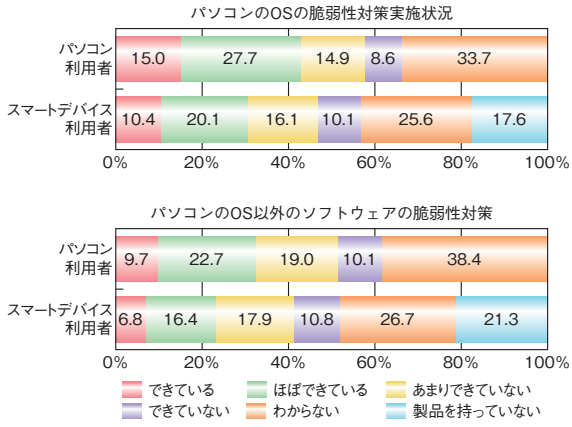
■図 2-4-34　パソコン利用者とスマートデバイス利用者の脆弱性対策に関する認識

(3) パソコン利用者とスマートデバイス利用者の比較

図 2-4-30（前ページ）と図 2-4-33 を比較すると、設問が一部異なるものの、全体的にスマートデバイス利用者の方が対策の実施率が低かった。

共通の設問としてセキュリティ対策の基本である脆弱性対策について尋ねており、その結果を紹介する。ソフトウェアに脆弱性対策が必要なことを「知っている」と回答した割合はスマートデバイス利用者の方が低いが、半数以上は対策が必要であることを認識していた（図 2-4-34）。

具体的なパソコン利用時の脆弱性対策の実施状況を尋ねた結果を図 2-4-35 に示す。スマートデバイス利用



■図 2-4-35　パソコン利用者とスマートデバイス利用者の脆弱性対策実施状況

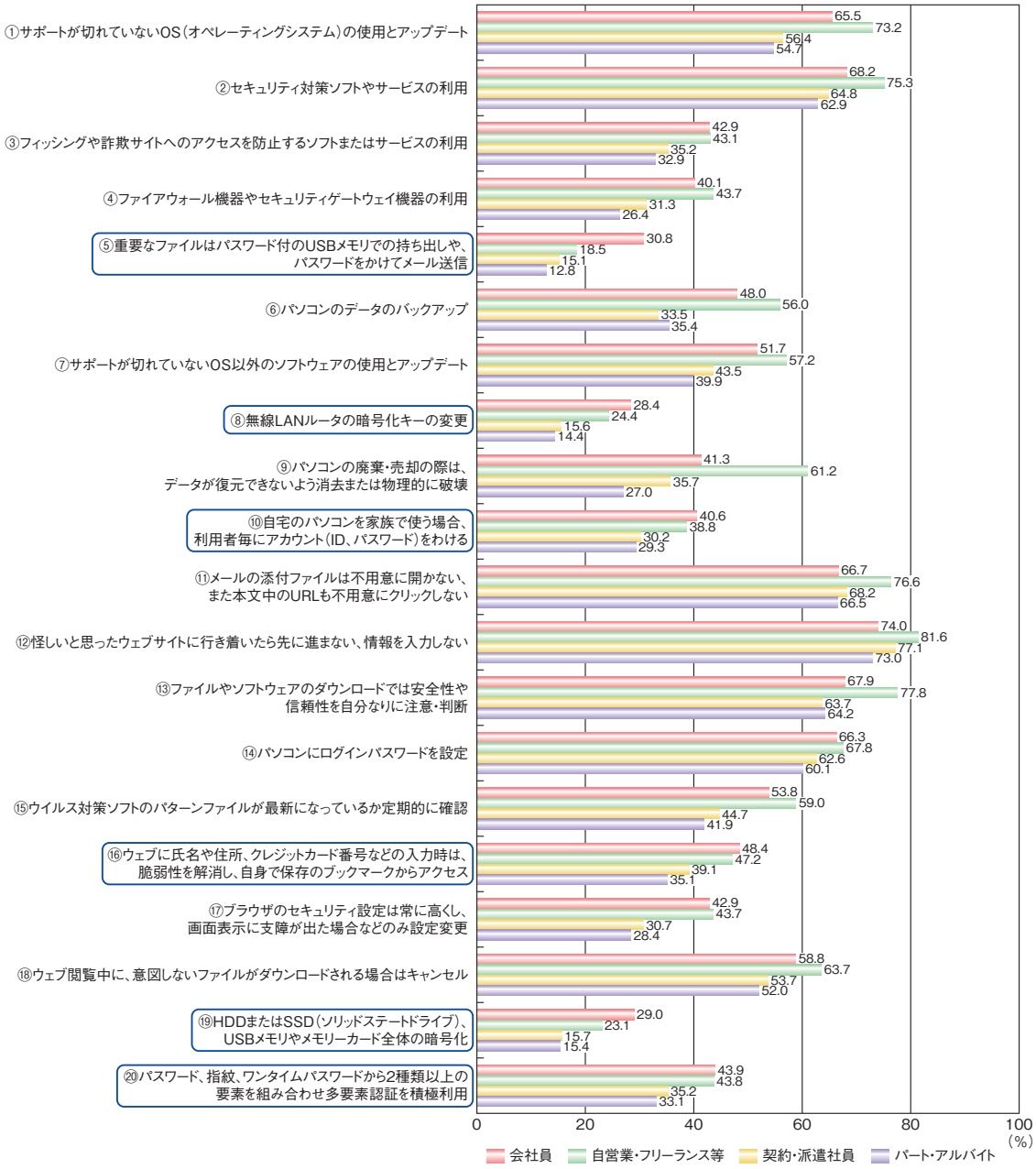
者の中には2割前後、パソコンを所有していないという回答が含まれるが、スマートデバイス利用者の「パソコンのOSの脆弱性対策」の実施率は30.5%、「パソコンのOS以外のソフトウェアの脆弱性対策」の実施率は23.2%であった。OSの場合、昨今は自動アップデートされることも多く、回答者の自覚と対策実施率が必ずしも同期しないと考えられる。しかし、あらゆる脅威への基本対策である脆弱性の解消は、その実施状況を利用者自身が自覚しておく必要がある。

回答者は今後もテレワークを奨励され、私物パソコン、あるいはスマートデバイスを業務に使用する等の可能性がある。テレワーク環境では職場の堅牢なセキュリティ対策は通用しないため、個人の意識と対策が一層問われることになる。なお、包括的なテレワークのセキュリティ対策については「3.3 テレワークの情報セキュリティ」を参照されたい。

(4) 回答者属性別の対策状況の特徴

パソコン利用者の調査結果に基づき、本白書では、情報システム・通信関係の業務に従事・関与しない利用者（会社員、自営業・フリーランス等、契約・派遣社員、パート・アルバイト）に対象を絞り、雇用形態別に回答者の対策状況のグラフを作成した（図2-4-36）。

自営業・フリーランス等と会社員[※421]を比較すると、



■図2-4-36　パソコン利用者の対策実施状況（雇用形態別）

自営業・フリーランス等の方が対策の実施状況が高い傾向にあった。例外は図中の六つの青枠で、これらの項目についてのみ会社員の対策実施率が高かった。

所属組織にもよるが、一般に会社員の方が、情報セキュリティに関する教育機会が多く、対策への認識、実施率は向上していると考えられる。しかし、情報セキュリティ教育が必ずしも提供されていない、自営業・フリーランス等の対策状況が高い結果となった。この理由について考察する。

項目別に見ると、まず「⑨パソコンの廃棄・売却時はデータが復元できないよう消去または物理的に破壊」では会社員よりも自営業・フリーランス等の実施率が約 20 ポイント高い。会社員が職場で使用するパソコンは通常、自身で廃棄処理を行う必要はほぼないと思われる。一方、自営業・フリーランス等は業務用パソコンの購入から廃棄までを自身で行うと考えられる。そのため、会社員が私物パソコンを所有していたとしても、廃棄における対策の必要性については、自営業・フリーランス等より認識が高くない可能性がある。

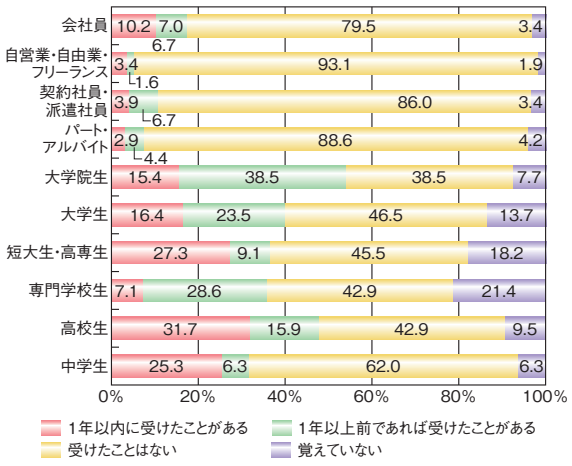
次に「⑪メールの添付ファイルや本文にある URL を不用意にクリックしない」「⑬ファイルなどのダウンロードでは安全性や信頼性を注意・判断する」では、自営業・フリーランス等が会社員より約 10 ポイント、対策実施率が高い結果であった。具体的な割合は⑪が 76.6%、⑬が 77.8% で、全体ではいずれも 69% 程度であるので、それと比較しても高い※422。自営業・フリーランス等は取引先とデータやファイルのやり取りをするために各種 Web サービスの利用頻度が高いと考えられる。そのため、セキュリティ対策への意識を高く持ち、対策を徹底していると考えられる。

続いて「⑤重要なファイルはパスワード付 USB で持ち出しや、メールはパスワードをかけて送信」について比較する。この項目では、自営業・フリーランス等の対策実施率が会社員に比べ 12.3 ポイント低い結果であった。加えて「⑲ HDD、USB メモリーカード全体の暗号化」の実施率も約 6 ポイント低い結果であった。

この 2 点について会社員の実施率が高いのは、勤務先のルールや対策の徹底が功を奏している可能性が考えられる。外部記憶媒体はデータの授受や持ち運びに便利なツールであるが、ひとたび紛失すれば、個人情報や営業秘密等の漏えいインシデントにつながり得る。そのため、多くの企業は情報持ち出し規則の周知やセキュリティ教育、暗号化機能が付いた媒体の利用等を徹底している。一方、自営業・フリーランス等は時にセキュリティ対策が十分といえない相手との仕事も避けられないと思われる。このような環境の違いが数値の差に表れていると考えられる。

一方で、契約・派遣社員の対策の実施率は、⑪、⑫を除きすべての項目で自営業・フリーランス等及び会社員と比較して低くなっている。例えば「⑩自宅のパソコンを家族で使う場合、利用者毎にアカウントをわける」については、契約・派遣社員及びパート・アルバイトの実施率は会社員及び自営業・フリーランス等と比べ 10 ポイント程度低い結果が見られた。

そこで、セキュリティに関する教育機会について尋ねた結果を見ると（図 2-4-37）、学生と社会人とで顕著な差が見られた。社会人の中で最も受講経験のある人の割合が高い会社員であっても、「過去に受講経験がある」とする回答は 17.2% と学生に比べ極めて低い。社会人には、雇用形態に合わせた多様な教育機会が提供されることが必要である。教育機関との連携や地域のコミュニティ等、職場以外でも学べる場を充実させていくことが望まれる。



■図 2-4-37　セキュリティ教育の受講経験

COLUMN

コロナ禍で「インターネット安全教室」はどのように変わったか

コロナ禍により人々の生活は様々な場面で大きな変化を求められることになりましたが、その一つに多くの組織で実施をしている「集合研修」が挙げられます。集合研修という知識や情報を共有する有効な手段がストップしたことは大きな痛手だったのではないでしょうか。

IPA でも集合研修形式で「インターネット安全教室」を全国各地で開催していました。インターネット安全教室は、家庭や学校等からインターネットにアクセスする一般利用者に向けた基本的な情報モラル・セキュリティの普及啓発の場、また、情報モラル・セキュリティ教育の指導者を育成する場となるものです。

2020 年度のインターネット安全教室では、集合研修形式に加えて、新型コロナウイルス感染症対策の一環として、初めてオンライン形式を導入しました。オンライン形式での開催は、依頼者の要望に合わせ、①講師及び参加者全員が Web 会議サービスを用いて開催するケース、②講師または参加者のどちらかがオンラインで接続し開催するケースの 2 種類の形式で行いました。

オンライン形式の導入により、交通アクセス等の事情で例年は受講がかなわなかった方も参加が可能になり、より広範囲での普及啓発が実現した一方で、課題や工夫を要する点も見えてきました。以下、開催にあたって必要となる対応や今後の課題についてご紹介します。併せて、IPA の「Web 会議サービスを利用する際のセキュリティ上の注意事項」（https://www.ipa.go.jp/security/announce/webmeeting.html）もご参照ください。

①事前準備について

インターネット安全教室では Web 会議サービスを利用する環境が整っていない参加者が多くいるため、タブレット端末、モバイル Wi-Fi ルータ、接続ケーブル等の機器の貸出しを行いました。また、オンライン講演の開催経験が浅い団体向けには事前に機器や Web 会議サービスの利用方法について、事務局からのレクチャーや入念な接続テストを行いました。オンライン形式では、開催者側はオフラインの場合と比較して、より入念な事前準備が必要であるといえます。

②講演中の対応について

インターネット安全教室では、参加者の反応を講演者が把握するため、ネット環境や個人情報の問題がなければ可能な限りビデオをオンにした状態で行いました。ビデオをオンにした状態で Web 会議を行う際は周囲の映り込みに注意を促すことが必要です。

チャット機能の使用やグループワーク等で参加者が発言する機会を用意すると、講演者側からの一方通行を防ぐことができます。また、オンラインでの講演に際して、意図しない第三者からのいたずらを防ぐため、参加者の制限を行う等の注意が必要です。

③講演後の対応について

講演後に行うアンケートの回収率は、集合形式の場合と比較して下がることが課題として挙げられます。オンライン形式では講演中の回収が難しく、現在は講演後、参加者にアンケートフォームにアクセスして回答していただく形をとる等、受講者側の手間を一つ増やす形を取っていますが、受講者の自発性に頼ることも限界があるため、改善の余地があるといえます。

2.5 国際標準化活動

国際標準とは、製品や技術を、国境を越えて利用するために制定される国際的な共通規格であり、国際規格とも呼ばれる。国際標準化は第4次産業革命時代の鍵を握る※423として、日本も積極的に活動に参画している。本節では、セキュリティ分野に関わる国際標準化活動の動向を紹介する。

2.5.1 様々な標準化団体の活動

日本の国際標準化活動への取り組みと、作成プロセスや作成組織の違いから見た標準の分類、及び情報セキュリティ分野の主な標準化団体の概要を示す。

(1) 日本の国際標準化活動への取り組み

企業が培ってきた技術や知的財産の秘匿化や、それらを知財として権利化する「クローズ戦略」に対して、標準化は「オープン戦略」に位置付けられている。クローズ戦略により企業のコア領域を守り、他社との差別化を図ることは重要であるが、その技術を利用する市場が広がらなければ、企業としては事業を拡大することが困難である。コア領域を守りつつ、市場を拡大する「オープン&クローズ戦略」が必要である。技術の発展、市場のグローバル化が進み、このオープン&クローズ戦略の考え方は企業にとどまらず、国の政策として位置付けられるようになった。知的財産戦略本部による「知的財産推進計画2020※424」では、デジタル技術を活用した社会的課題解決の取り組みを、複数の主体による協働・共創を通じて、持続可能なビジネスとして定着・拡大させていく上で、標準を戦略的に活用することも重要であるとしている。

2020年7月、国立研究開発法人産業技術総合研究所は「標準化推進センター」を設置した※425。政策的ニーズや産業界のニーズに基づく業界・領域横断的な分野の標準化を主導するとしている。また、標準化の専門人材として「標準化オフィサー」を新設し、標準化の専門知識と経験を活かして、ステークホルダー間の調整や標準の普及策検討等、標準化を一貫して推進するとしている。

(2) 標準の分類

国際標準には、公的な標準化団体により所定の手続きを経て行われる「デジュール標準(de jure standard)」、いくつかの団体(企業等)が協力して自主的に作成する「フォーラム標準(forum standard)※426」、公的な標準化団体を介さず、市場や業界において広く採用された結果として事実上標準化される「デファクト標準(de facto standard)」がある。

デジュール標準では、幅広くステークホルダーを集めて議論をとおして合意形成を行う。次項で紹介するISO、IEC、ITUが作成する国際規格やJIS等の国家規格が該当し、策定プロセスが規定されており、様々な規制等に用いられることも多い。合意形成のために複数の検討段階が設定されており、正式に発行するまでに時間がかかる(ISO/IECは約3年)。

フォーラム標準は業界団体等、共通の関心を持つ企業等が集まって議論し、業界ルール等限定的な範囲で合意される標準である。作成スピードは速く、業界の特性が反映されていることから該当する業界内では利用が促進されやすい。次項で紹介するIEEE、IETF、TCGが発行する標準が該当する。コンソーシアム標準と呼ばれることもある。業界のフォーラム標準が、その後、国際標準化団体に提案され、時間をかけてデジュール標準となる場合もある。

電気製品やIT製品等、開発サイクルの短い分野では、その時点の市場で一般的な規格としてデファクト標準が採用される傾向にある。例えばWindowsのようなOSやGoogleのような検索エンジン等、グローバルなIT企業の製品・サービスが事実上の国際標準となる傾向があり、合意形成プロセスは存在しない。

(3) 情報セキュリティ分野に関する標準化団体

情報セキュリティに関連するデジュール標準やフォーラム標準の策定を行っている主な国際標準化団体を以下に示す。

- ISO(International Organization for Standardization:国際標準化機構)/IEC(International Electrotechnical Commission:国際電気標準会議)JTC 1(Joint Technical Committee 1:第一合同技術委員会)※427:情報セキュリティを含む情報技術の国際規格を策定している。コンピュータや情報分野を扱う国際標準化団体としてISO、IECはそれぞれ独立に存在しているが、扱う領域の競合を避けるために双方が連携し、JTC 1が設立された。日本国内の標準化団体としては、日

本産業標準調査会（Japanese Industrial Standards Committee：JISC）がISO、IEC双方のメンバーであり、JTC 1でも活動している※428。

- ITU-T（International Telecommunication Union Telecommunication Standardization Sector：国際電気通信連合 電気通信標準化部門）：
  電気通信技術に関わる国際規格を策定している。情報セキュリティに関してはSG（Study Group）17が設置され※429、ISOや後述するIETFとともにネットワークやID管理等に関する標準化活動を行っている。策定した標準はITU勧告として定められる。

また、情報セキュリティ分野に関するフォーラム標準を策定する代表的な組織として、以下のようなものがある。

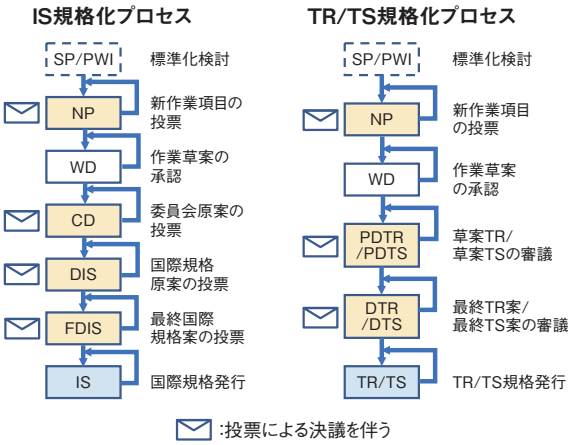
- IEEE（The Institute of Electrical and Electronics Engineers, Inc.）：
  電気工学・電子工学技術に関する国際学会である。標準化活動は内部組織であるIEEE-SA（Standards Association）が行っている。情報セキュリティについては、サイバーセキュリティ、ネットワークセキュリティ、IoTセキュリティ等の広範な領域で標準化を行っている。
- IETF（Internet Engineering Task Force）：
  インターネット技術の国際標準化を行う任意団体である。非常にオープンな組織であり、作業部会のメーリングリストに登録することで誰でも議論に参加することができる。情報セキュリティについては、インターネット上のセキュアなプロトコル、暗号、署名、認証、セキュリティ情報連携（セキュリティオートメーション）等の方式の標準化を行っている※430。標準化した技術文書はRFC（Request For Comments）として参照することができる。
- TCG（Trusted Computing Group）：
  信頼できるコンピューティング環境（組み込み機器、パソコン／サーバ、ネットワーク等）に関するセキュリティ技術の標準化を行う業界団体である。ハードウェア、ソフトウェア等のベンダやシステムインテグレータがメンバーとなり、中国、日本にregional forumがある※431。

2.5.2 情報セキュリティ、サイバーセキュリティ、プライバシー保護関係の規格の標準化（ISO/IEC JTC 1/SC 27）

ISO/IEC JTC 1/SC 27（以下、SC 27）は、ISO及びIECの合同専門委員会（ISO/IEC JTC 1）において、情報セキュリティに関する国際標準化を行う分科委員会（SC）である。SC 27は、テーマ別に以下の五つのWGで構成される。

WG 1：情報セキュリティマネジメントシステム
WG 2：暗号とセキュリティメカニズム
WG 3：セキュリティの評価・試験・仕様
WG 4：セキュリティコントロールとサービス
WG 5：アイデンティティ管理とプライバシー技術

ISO/IECにおける標準化作業は、策定する仕様の完成度によって図2-5-1のような状態があり、それぞれ各国の投票によって次の段階へ進む。なお、ISOにおいて、技術が未成熟である、またはガイダンス等の標準仕様ではないが重要であるとされたものは、技術報告書または技術仕様書として出版する。



■図2-5-1　ISO/IEC JTC 1/SC 27における文書のステータス
（出典）JISC「ISO規格の策定手順※432」を基にIPAが作成

図2-5-1の各文書のステータスと略号は以下のとおりである。なお本文中では、略号を使用する。

SP：研究期間（Study Period）
PWI：予備業務項目（Preliminary Work Item）
※SPとPWIのどちらを実施するかはWGによって異なる。
NP：新作業項目（New work item Proposal）
WD：作業原案（Working Draft）
CD：委員会原案（Committee Draft）
DIS：国際規格原案（Draft International Standard）
FDIS：最終国際規格案（Final Draft International Standard）
IS：国際規格（International Standard）
PDTR：予備技術報告原案（Preliminary Draft Technical Report）
PDTS：予備技術仕様書原案（Preliminary Draft Technical Specification）
DTR：技術報告書原案（Draft Technical Report）

DTS：技術仕様書原案（Draft Technical Specification）
TR：技術報告書（Technical Report）
TS：技術仕様書（Technical Specification）

以下に、各 WG の活動概要を述べる。

（1）WG 1（情報セキュリティマネジメントシステム）

WG 1 では、情報セキュリティマネジメントシステム（ISMS：Information Security Management System）に関する国際規格として、ISO/IEC 27001（ISMS 要求事項を示す規格）及び ISO/IEC 27002（情報セキュリティ管理策及び実施の手引きを示す規格）を中心に、ISO/IEC 27001 が示す ISMS 要求事項に関する手引きや指針を提供する規格、ISO/IEC 27001 及び ISO/IEC 27002 を土台とする分野別規格、及びその他トピックスに関する ISO/IEC 27000 ファミリー規格の国際標準化活動を実施している。

(a) ISO/IEC 27001 及び ISO/IEC 27002 の改訂に関する状況

2013 年の改訂から 5 年を経ている ISO/IEC 27002:2013 については、2018 年 3 月までの 1 年間の SP において、次期改訂の設計仕様（Design Specification）が決定され、改訂作業が開始された。2018 年 4 月に WD の初版を発行、エキスパートレベルでの審議を行い、2018 年 11 月には CD の初版を発行、国レベルでの審議にステージを移した。2021 年 4 月現在は、DIS 投票中の状況にある。管理策の全体構成も固まり、管理策の具体的な内容を決める最終段階となっている。2021 年 4 月の投票結果、及び 6 月に予定されている国際会合の結果によって FDIS 発行となるかが決定される。

ISO/IEC 27001:2013 については、2019 年に実施された、改訂の必要性を各国に問う定期レビューの結果、Confirm（改訂しない）という結論となり、改訂作業は開始されていない。これは、ISO/IEC 専門業務用指針、第 1 部において規定されたマネジメントシステム規格の共通フォーマットが改訂中である状況を考慮し、並行して ISO/IEC 27001 を改訂することは、改訂作業を複雑にすると考えての結論であった。しかし、2021 年 4 月現在、ISO/IEC 27002 の改訂が最終段階となったこと、また、管理策の構成等が現版から大きく変わることを受け、ISO/IEC 27001: 2013 の Annex A のみを改訂版 ISO/IEC 27002 と整合するように変更することを決定した。

(b) 分野別規格の国際標準化活動

分野別規格作成に関する要求事項を示す規格である ISO/IEC 27009 は 2016 年に発行された後、2017 年から早期改訂が行われ、2020 年 4 月に改訂版が発行された。2021 年 4 月現在は、ISO/IEC 27002 の改訂が最終段階になったことを受けて、それに伴う ISO/IEC 27009 の早期改訂についての検討を予定している。

分野別規格そのものについては、通信事業者のためのガイドライン規格 ISO/IEC 27011:2016、セクター間及び組織間コミュニケーションのためのガイドライン規格 ISO/IEC 27010:2015、クラウドサービスカスタマ及びプロバイダ向けのガイドライン規格 ISO/IEC 27017:2015 が発行済みである。これらは、いずれも ISO/IEC 27002 を拡張した分野別規格であるため、現在進行中の ISO/IEC 27002 の改訂が完了すれば、それに伴って改訂が行われる見込みである。実際、ISO/IEC 27011:2016 については、既に改訂を開始しており、WD を発行、エキスパートレベルの審議を行っている。

一方、ISO/IEC 27009 は、ISO/IEC 27001 を特定分野に適用した規格を作成する際の、規格の記述方法や様式等を定めた規格であり、ISO/IEC 27002 だけを対象に、特定分野に特化して修正することは適用範囲としていない。ISO/IEC 27009 に適合する規格としては、エネルギー分野に関する規格として ISO/IEC 27019:2017、プライバシー情報マネジメントに関する規格として ISO/IEC 27701:2019[※433] が発行済みである。なお、ISO/IEC 27701 については、これに基づく認証に対する市場ニーズが高いことから、ISO/IEC 27701 の認証機関に対する認定基準となる ISO/IEC TS 27006-2 を早期に策定するため、WG 1 と WG 5 の共同プロジェクトを開始、2020 年 2 月に発行に至った。また、ISO/IEC TS 27006-2 の発行に伴い、ISO/IEC 27001 の認証機関に対する認定基準 ISO/IEC 27006 についても、ISO/IEC 27006-1 への改番が必要となり、これに対応した改訂が予定されている。

(c) サイバーセキュリティ関連の国際標準化活動

サイバーセキュリティに関する規格化については、まず、サイバーセキュリティの既存のフレームワークと ISO 及び IEC 規格類との対応関係を示した技術報告書 ISO/IEC TR 27103 が 2018 年に発行された。次いで、サイバー保険に関する規格 ISO/IEC 27102 が 2019 年に発行された。サイバーセキュリティのフレームワーク構築に関する技術仕様書 ISO/IEC TS 27110 は 2021 年

2月に発行された。本規格は規格番号を27101として検討を進めてきたが、27110に変更しての発行となった。また、サイバーセキュリティの概念やコンセプトに関する技術仕様書ISO/IEC TS 27100についても2020年12月に発行された。

(d)その他のISO/IEC 27000ファミリー規格の国際標準化活動

ISO/IEC 27001:2013への本格的対応を積み残している情報セキュリティリスクマネジメントに関するガイドライン規格ISO/IEC 27005:2018については、2021年4月時点も改訂中でCDを審議中である。ISO/IEC 20000-1及びISO/IEC 27001の統合実践に関するガイドライン規格であるISO/IEC 27013:2015は、ISO/IEC 20000-1:2018の発行を受けて、2021年4月時点で改訂中であり、DIS投票を終え、結果に基づく国際会議の場での審議を予定している。情報セキュリティガバナンスの原則、及びプロセスの手引きを提供するISO/IEC 27014については、改訂を終えて2020年12月に発行された。

(2)WG 2(暗号とセキュリティメカニズム)

WG 2では、暗号プリミティブ(暗号アルゴリズム)や、デジタル署名技術、鍵共有のような汎用的かつ基本的な暗号プロトコル等の標準化を行っている。WG 2の国際主査、副主査ともに日本人が選出され、WG 2での活動をリードしている。2020年度は、新しい規格の発行はなかったが、既存規格10件の改訂版が発行された。このほかの主な活動内容について以下に示す。

(a)完全準同型暗号の規格化検討

完全準同型暗号は、暗号化したままで加算や乗算の両方が計算可能な公開鍵暗号である。完全準同型暗号を使用すれば、計算のためにデータの復号を行う必要がないため、守秘性の高いデータ処理を外部業者に委託する場合においても、負担をかけずにリスクを抑えることが可能となる。

2020年4月に米国より、この完全準同型暗号の規格化が提案され、議論を重ねた結果、2021年4月にISO/IEC 18033(暗号アルゴリズム)の第8部として規格化提案の投票にかけることが合意された(2021年6月現在投票中)。

(b)耐量子計算機暗号の文書を一般公開

耐量子計算機暗号[※434]の文書を2年程かけ作成してきたが、文書作成作業がいったん完了し、「ISO/IEC JTC 1/ SC 27/WG 2 Standing Document 8(SD8) Post-Quantum Cryptography[※435]」として2020年6月に一般公開された。

(3)WG 3(セキュリティの評価・試験・仕様)

WG 3は2020年4月、9月にZoomにて定期会合を開催した。なお、定期会合はサンクトペテルブルグ(ロシア)、ワルシャワ(ポーランド)での開催が予定されていたが、新型コロナウイルスのためキャンセルされ、オンライン開催となった。それらの会合の議論内容、特に新しい規格を開発するためにPWI[※436]でなされた議論に焦点を当てて以下に概説する。

(a)PWI“Evaluation criteria for connected vehicle information security based on ISO/IEC 15408”

自動車がネットワークにつながることで利便性が向上したと同時に、自動車に対するサイバー攻撃の脅威も高まっている。米国では、研究者がChryslerブランドの車両のエンジンを切る、ワイパーを動かす等のリモートハッキングを行って見せた[※437]。これに先立ち、事前通知を受けていたFCA US LLC(旧Chrysler Group LLC)は2015年7月にハッキング対象機種140万台のリコールを発表した[※438]。

そのような背景もあり、2020年6月にUNECE[※439]の自動車基準調和世界フォーラムWP.29にて自動車のサイバーセキュリティ基準が採択された。またISO/TC 22/SC 32/WG 11では、車載機器製造時に順守すべきサイバーセキュリティ要件やガイドラインを定めた「ISO/SAE 21434 Road vehicles — Cybersecurity engineering」の策定が進められている[※440]。しかしながら、自動車へのリモートハッキングの対象となっている車載エンターテインメントシステムや、エンジンやブレーキを制御する電子制御ユニット(ECU:Electronic Control Unit)に対し、具体的にどのような脆弱性分析や侵入テストを実施すべきかを定めた規格や指針は存在せず、WP.29のサイバーセキュリティ基準やISO/SAE 21434においてもその技術的詳細には一切触れられていない。

そのため、WG 3では2019年4月のテルアビブ会合から車載機器のセキュリティ評価基準に関する議論を行っていたが、2021年4月のZoom会議において、今までの議論結果をベースに新たな規格を開発するための新業務項目提案を行うことが合意された。なお、本PWIでは日本エキスパートがPWIのメンバーとして議論

に参加している。

(b) PWI “A general framework for runtime hardware security assessment”

半導体チップに集積されるトランジスターの数は、「ムーアの法則」に従い着実に増加し、最新のマイクロプロセッサーには、10 億個を軽く超える膨大な数のトランジスターが集積されている。また、その設計・製造には様々な企業が関わっており、ハードウェアトロイの脅威が高まっている。ハードウェアトロイとは、半導体チップに不正に仕込まれ、トリガーとなる事象（例えば、特定の入力等）が生じた場合に不正な活動を行う、悪意を持つ回路である。現在、マイクロプロセッサー等のハードウェアコンポーネントの稼働状況をモニタリングすることにより、ハードウェアの異常な振る舞いを検出する技術に関する研究が各国の研究者により進められている。

日本においても同様なテーマを題材にした総務省の「設計・製造におけるチップの脆弱性検知手法の研究開発」が立ち上がっており、そのプロジェクトメンバーも本 PWI の一員として議論に参加している。今後日本は、本プロジェクトの成果をベースに、ハードウェアトロイを検知するハードウェアモニタリング回路の評価手法に関し、その知見を本 PWI にインプットしていく予定である。

(c) PWI “Multi-party coordinated vulnerability disclosure and handling”

WG 3 では、IT 製品の脆弱性の開示・取り扱いに関する以下の二つの標準を既に出版している。

- ISO/IEC 29147：脆弱性情報の開示に向けて開発者に必要となるやり取り（外部からの脆弱性に関する情報の受領等）に関わる要件を規定
- ISO/IEC 30111：脆弱性取り扱いのプロセス（脆弱性の検証等）の要件を規定

しかしこれら二つの規格では、脆弱性を取り扱う関係者が多岐に渡るような場合に誰がどのような対応をすべきであるかに関する詳細な説明がされていない。例えば CPU に脆弱性が検出された場合、その脆弱性を修正するためには、CPU のみでなく CPU 上で稼働するファームウェア、オペレーティングシステムや各種ソフトウェアの更新が要求されるケースがある。また、複数の製品に共通して使用されているソフトウェアライブラリに脆弱性が発見されるといったケースも多々存在する。

本 PWI では、そのような多数の開発者が関わる脆弱性の取り扱いに際し、関係者間で協業、また時には分業しながら、脆弱性に関する情報を利用者に適切なタイミングで提供し、速やかに更新プログラムを開発し、利用者に更新プログラムを確実に提供するための指針を提供することを目指している。なお、本 PWI においても日本から脆弱性の取り扱いに関わるエキスパートが参加し、その知見を本活動に生かしている。

(d) 2020 年出版規格

2020 年には、日本のエキスパートがエディタとして多大な貢献をした以下の規格が出版された。なお、ISO/IEC 19989 に関しては、産業界にインパクトがある標準として、ISO よりプレスリリースが配信されている※441。

- ISO/IEC 19989-1 “Criteria and methodology for security evaluation of biometric systems – Part 1: Framework”
- ISO/IEC 19989-2 “Criteria and methodology for security evaluation of biometric systems – Part 2: Biometric recognition performance”
- ISO/IEC 19989-3 “Criteria and methodology for security evaluation of biometric systems – Part 3: Presentation attack detection”
- ISO/IEC 20897-1 “Physically unclonable functions – Part 1: Security requirements”

(4) WG 4（セキュリティコントロールとサービス）

WG 4 では、WG 1 が対象とする ISMS を実施・運用する際に必要となる具体的なセキュリティ対策、及びセキュリティサービスの標準化を行っている。以下に、WG 4 における 2020 年度の主な成果、活動を紹介する。

(a) IoT セキュリティ／プライバシーのための標準化活動

WG 4 では、IoT セキュリティ／プライバシーに関わる標準化として、以下の三つの活動を継続的に進めている。当初は、ばらばらの三つの規格としての位置付けだったが、2020 年に体系的な検討がなされ、Cybersecurity – IoT security and privacy と名付けられたプロジェクト群（ISO/IEC 27400 シリーズ）として規格番号の見直しを行い、規格間でも適切な参照を行うように修正された。

- ISO/IEC 27400（旧 27030）: Cybersecurity – IoT security and privacy – Guidelines
- ISO/IEC 27402: Cybersecurity – IoT security and privacy – Device baseline requirements
- ISO/IEC 27403（旧 24391）: Cybersecurity – IoT

security and privacy –Guidelines for IoT-domotics

（ア）ISO/IEC 27400: Cybersecurity – IoT security and privacy – Guidelines

日本は、IoT 関連の製品・システム開発の競争力を強化し、また IoT の国際的なセキュリティレベル向上に寄与するために、IoT 推進コンソーシアムが策定した「IoT セキュリティガイドライン※442」の国際標準化を提案した。具体的には、本ガイドラインに基づき、ISO/IEC 27400（IoT のセキュリティとプライバシー）、ISO/IEC 30147（IoT システム／サービスの信頼性のための方法論）の二つの規格案がそれぞれ SC 27/WG 4、及び SC 41/WG 3 で審議されている。以下に ISO/IEC 27400 の規格について概説する。

ISO/IEC 27400 の具体的内容にあたる第 5 章以降では、第 5 章で参照モデル、各利害関係者の役割、IoT ライフサイクルに触れ、第 6 章では IoT システムにおけるリスクマネジメントについて言及している。第 7 章では、セキュリティ対策及びプライバシー対策が、サービス開発者／サービスプロバイダ、ユーザのそれぞれの立場での対策内容、目的、導入ガイドといったガイドライン的な表現で記載されている。ここで、IoT 機器製造業者は IoT サービス開発者の中に含まれる。2020 年 9 月の SC 27/WG 4 オンライン会議（以下、2020 年 9 月オンライン会議）にて策定されたドキュメントの枠組みは以下のとおりである。

第 1 章～ 4 章：スコープ、文献、用語定義等
第 5 章：IoT 概念と参照モデル
　5.1 概要
　5.2 IoT システムの特徴
　5.3 IoT システムの利害関係者（利用者、サービス提供者、サービス開発者）
　5.4 IoT エコシステム
　5.5 IoT ライフサイクル
　5.6 ドメインに基づく参照モデル
第 6 章：IoT システムのリスクマネジメント
　6.1 導入
　6.2 リスク源（リスクソース）
　6.3 リスクシナリオと IoT システムのリスク
第 7 章：セキュリティ／プライバシーのための管理策
　7.1 セキュリティ管理策
　7.2 プライバシー管理策

2020 年 9 月オンライン会議において、ISO/IEC 27400 は CD3 となっており、次の段階では DIS への移行が想定できる完成度となっている。本規格に対するコメントは、日本、スイス、フランス、カナダ、ドイツ、インド、中国等の多くの機関から大量に提出されており、審議は継続的に極めて活発である。本規格は IoT セキュリティ及びプライバシーの規範となるガイドラインであるため、IoT 利害関係者における認証等への活用が期待されている。

（イ）ISO/IEC 27402: Cybersecurity – IoT security and privacy – Device baseline requirements

本規格は、米国が主導で進めており、IoT 機器が備えるべきセキュリティメカニズムのベースラインとなる要求条件の規定を目指している。ISO/IEC 27400 とは異なるスコープを掲げ、IoT 機器に特化した要件化を視野に入れ、NIST 及び ETSI（European Telecommunications Standards Institute：欧州電気通信標準化機構）の既存のガイドラインを下敷きに標準化を進めている。2020 年 4 月に WD1 が審議されたものの、NIST や ETSI の既存規格に基づいているため、一定の完成度と判断され、2020 年 9 月オンライン会議では、CD1 として進むことが決定された。通常の SC 27/WG 4 における規格策定の進め方としては考えられないスピードで規格策定が推進されている。2020 年 9 月オンライン会議にて策定されたドキュメントの枠組みは以下のとおりであり、IoT 機器製造者、及び IoT 機器のための要求事項がそれぞれ盛り込まれた。

第 1 章～ 4 章：スコープ、文献、用語定義、概要
第 5 章 要求事項
　5.1 IoT 機器製造者のための要求事項
　　5.1.1 リスクアセスメント
　　5.1.2 ユーザへのコミュニケーション
　　5.1.3 脆弱性の開示と処理プロセス
　5.2 IoT 機器のための要求事項
　　5.2.1 識別
　　5.2.2 構成
　　5.2.3 リセット
　　5.2.4 ユーザデータの削除
　　5.2.5 データの保護
　　5.2.6 インタフェースアクセス（Interface access）
　　5.2.7 ソフトウェアとファームウェアのアップデート
　　5.2.8 サイバーセキュリティイベント
　　5.2.9 安全な保存（Secure Storage）
　　5.2.10 データ検証

なお、インタフェースアクセスは、IoT デバイスにおいて、秘密鍵やパスワード等の重要なセキュリティパラメータを共有または再利用するためのインタフェースへのアクセスを許可された権限者に限定することに言及している。また、安全な保存は、ユーザにより IoT 機器で扱われる重要なデータの機器への保存に関するセキュリティ要求事項について述べている。

上記の要求事項に近い内容は、ハイレベルなセキュリティ対策として ISO/IEC 27400 においても触れられており、ISO/IEC 27400 と ISO/IEC 27402 は、ISO/IEC 27400 シリーズ規格として一貫性を確保する形で規格策定が進められている。

(ウ) ISO/IEC 27403: Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics

本規格は、2019 年 4 月テルアビブ会議において、中国から NP として提案され、同年 10 月のパリ会議では、NP の承認がなされ、2021 年 3 月までに WD4 に進んでいる状況にある。「IoT-Domotics」とは、娯楽、機器制御、監視等の用途として、居住環境で利用する IoT サービスをいう。本規格は、ISO/IEC 27400 との棲み分けが難しい部分が多いものの、IoT-Domotics の特性を抽出し、ISO/IEC 27400 とは異なる視点でセキュリティとプライバシーに関するガイドラインとして整理している。具体的には、IoT-Domotics のためのリスクアセスメントの実施を、①アプリケーション、②ネットワーク、③ハードウェアの三点から評価しており、それらの結果を受ける形で、IoT-Domotics を構成するサブシステムや IoT ゲートウェイのためのセキュリティ、及びプライバシーのガイドラインを整理する方向としている。

(b) ビッグデータセキュリティ／プライバシーのための標準化活動

ビッグデータとは、主にボリューム、多様性、速度、及び／または変動性の特性を有し、効率的な保管、操作、分析のためにスケーラブルなアーキテクチャを必要とする広範なデータセットのことを指す。ビッグデータを用いた分析により、より優れた意思決定や戦略的なビジネス行動につながる洞察等を導き出すことができるため、近年注目を浴びている。WG 4 では、ビッグデータのセキュリティ／プライバシーに関わる標準化として、以下の三つの活動を進めている。

- ISO/IEC 20547-4: Big data reference architecture – Part4: Security and privacy
- ISO/IEC 27045: Big data security and privacy – Processes
- ISO/IEC 27046: Big data security and privacy – Implementation guidelines

(ア) ISO/IEC 20547-4: Big data reference architecture – Part4: Security and privacy

ISO/IEC JTC 1/SC 42 で審議されている、ISO/IEC 20547（ビッグデータ参照体系）は四つのパートから成り立っている。そのうちパート 4 は、SC 42 の依頼により SC 27/WG 4 で審議されており、セキュリティ及びプライバシーに関わる参照体系を規定している。本規格は、2019 年パリ会議において DIS に進み、2020 年 4 月オンライン会議で FDIS に進むことが決定し、既に発行されている。

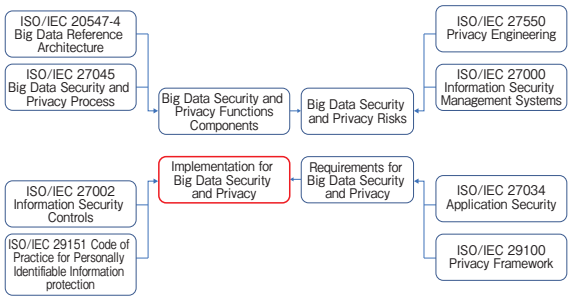
(イ) ISO/IEC 27045: Big data security and privacy – Processes

本規格は、組織のビッグデータのセキュリティとプライバシーを評価及び改善するためのプロセスの参照モデル、評価・成熟度モデルを規定する。プロセスには、プロセスパフォーマンスとプロセス機能の一連のインジケーターが含まれ、評価者が評価の良し悪しを決めるための客観的証拠の基礎として使用される。現在の規格内容は、ISO/IEC JTC 1/SC 7 で規格化されている ISO/IEC 33004、ISO/IEC 33002 等を参照する形で記載されており、2020 年度は数回のオンライン会議を開催して WD3 から WD6 まで規格の改善を進めた。WD6 においては、プロセスの参照モデルを策定し、組織としてのプロセス、マネジメントで必要となるプロセス、技術的なプロセスに分類し、整理を進めた。しかしながら、何度も大きな方針レベルの見直しをこれまで行っているため、規格として安定したものには未だ到達していない状況である。

(ウ) ISO/IEC 27046: Big data security and privacy – Implementation guidelines

本規格は、ビッグデータのセキュリティとプライバシーの主要な課題とリスクを分析し、ビッグデータのリソース、組織化、分散化、計算能力及び破壊等の視点から、ビッグデータのセキュリティとプライバシーの実装のためのガイドラインを記述することを狙っている。2020 年 9 月オンライン会議においては、WD3 への移行が決議され、本規格と他規格との関係については、図 2-5-2 （次ページ）

のように整理された。赤枠部分が本規格に対応する。なお、本図は、規格案（ISO/IEC 27046 WD3）の図 1 として利用されている。



■図 2-5-2　ビッグデータセキュリティ／プライバシーの関連規格間の関係性

(c) WG 4 に関連するその他の規格群

WG 4 では、上記の IoT 及びビッグデータ以外の課題についても、多数の重要な審議を進めている。以下にその審議課題項目、規格の番号、及び審議状況を示す。

- ビジネス継続のための ICT 準備技術（27031）：PWI、NWI の審議を経て、WD1 に進む
- インターネットセキュリティガイドライン（27032）：WD4 に進むことが決定
- ネットワークセキュリティ（27033-7）：ネットワーク仮想化セキュリティのガイドラインとして NP が成立し、WD1 に進む
- アプリケーションセキュリティ（27034）：パート 4 が FDIS に移行、他パートは規格化完了
- インシデントマネジメント（27035）：パート 3 が発行された
- サプライヤー関連セキュリティ（27036）：パート 1 から改版作業を開始
- デジタルエビデンスの識別、収集、確保、保全（27037）：改版作業なし
- リダクション（墨消し技術）（27038）：改版作業なし
- IDPS（侵入検知システム）（27039）：改版作業なし
- ストレージセキュリティ（27040）：大規模な改修を視野に入れ改版作業を開始、現在 WD1
- 仮想化サーバの設計／実装のためのセキュリティガイドライン（21878）：改版作業なし
- 産業用インターネット基盤のためのセキュリティ参照体系（24392）：WD5 に進む
- 仮想化された信頼のルートのためのセキュリティ要件（27070）：DIS に進む
- 公開鍵基盤における実践とポリシーの枠組み（27099）：CD3 に進む
- 機器とサービス間の信頼接続の構築のためのセキュリティ推奨（27071）：WD4 に進む
- 安全な配備、アップデート、及びアップグレード（4983）：NWI 審議を経て、WD1 に進む
- データの起源―参照モデル（データ追跡のため）（5158）：PWI として審議継続
- 情報セキュリティインシデント対応の調整（5189）：PWI として審議継続
- サイバーフィジカルシステムのためのセキュリティ参照体系：PWI として審議（日本提案）

(5) WG 5（アイデンティティ管理とプライバシー技術）

WG 5 では、アイデンティティ管理、プライバシー、バイオメトリクスの標準化を行っている。2020 年度の主な活動を紹介する。

(a) アイデンティティ管理

2013 年 4 月に発行されたユーザ認証についてのフレームワーク規格である ISO/IEC 29115（エンティティ認証保証フレームワーク）は、2020 年秋に改定プロジェクトがキャンセルとなり、複数要素認証等についての技術の状況や他の規格文書との整合性の観点から対象範囲を再検討している PWI 段階にある。

2015 年 6 月に発行された ISO/IEC 24760-2（アイデンティティ管理のフレームワーク パート 2：リファレンスアーキテクチャと要件）の定期見直しにおいては、確認（Confirmation）への投票が最も多く（9 ヵ国）、日本を含む 6 ヵ国が改訂または追補（Revision/Amend）に投票していたが、2020 年 4 月の WG 5 定期会合（オンライン会議）後、日本、フランス、ベルギー、ドイツ、米国、フィリピン、ルクセンブルク、カナダから構成されるアドホックグループが複数回にわたるオンライン会議を行った結果、コンテキストや機能面の改訂の必要性が認められた。現在、WD 段階にある。

2016 年 8 月に発行された ISO/IEC 24760-3（アイデンティティ管理のフレームワーク パート 3：実践）は改訂のための WD 段階にある。

(b) プライバシー

プライバシー対策に関わる ISO/IEC 27701: 2019 は、ISMS の要求事項を規定した ISO/IEC 27001 及び

ISMS を実施するためのプラクティスをまとめた ISO/IEC 27002 に、プライバシー対策に関する要求事項及びプラクティスを加えて拡張することにより、組織による PIMS（Privacy Information Management System：プライバシー情報マネジメントシステム）の構築を支援することを目的としている。2019 年 8 月に IS として発行され、日本語対訳書が 2020 年 3 月に出版された。

ISO/IEC 27701 は、PIMS を構築するためのものであるが、独立したマネジメントシステムではなく、ISMS によるマネジメントシステムの拡張として規定されている。このため ISO/IEC 27701 を基にして ISMS の審査及び認証を行う機関に対する要求事項が 2019 年 12 月に提案され、ISO/IEC 27006（Requirements for bodies providing audit and certification of information security management systems）の Part 2（Privacy information management systems） が TS として 2021 年 2 月に発行され、日本語対訳書が同年 3 月に出版された。

国内では、ISO/IEC 27701 を基にした ISMS 認定が 2020 年 12 月から開始されている。ISO/IEC 27006-2 については、更に内容を充実させるための IS 化の審議が継続されている。

日本提案の規格としては、経済産業省が 2014 年 10 月に公開した「消費者向けオンラインサービスにおける通知と同意・選択に関するガイドライン」に基づく国際規格である ISO/IEC 29184（オンラインにおけるプライバシーに関する通知と同意）が 2020 年 6 月に発行され、日本語対訳書が同年 11 月に出版されている。

また、同じく日本提案である ISO/IEC 27556（プライバシープリファレンスに基づいたユーザ主体の PII 処理）は、2019 年 5 月に新たな規格策定プロジェクトとして承認され、2021 年 4 月現在、CD 段階にある。

(c) バイオメトリクス

バイオメトリックデータの保護技術を扱う ISO/IEC 24745 は、2011 年に発行されたが、その後の新技術を反映するための改訂が進み、2021 年 4 月会合で FDIS 段階に進んだ。また、モバイル機器上でのバイオメトリクスを使った認証に対するセキュリティ要件を定めるプロジェクト ISO/IEC 27553 は、CD 段階にあったが、2021 年 4 月会合で適用範囲が問題となり、Part 1（Local modes）、Part 2（Remote modes）に分け、Part 1 は CD 段階の審議を継続、Part 2 は PWI から検討を開始することとなった。スマートフォンへのバイオメトリクスの適用が進みつつある中、ISO/IEC 27553 は関心を集めている。

COLUMN

2021年1月から「ISMS-PIMS認証」の審査始動!

2021年1月から、日本でもISO/IEC 27701:2019規格に基づいた「ISMS-PIMS（アイエスエムエスピムス）認証」の審査が開始しました。本認証では、PII（Personally Identifiable Information）の保護への対応が行えているかを確認する審査が行われます。PIIには、氏名等の「個人情報」だけでなく、免許証番号や住所、性別、年齢等と組み合わせることで「個人を特定できる情報」、例えば、位置情報、画像識別情報、遺伝子情報も含んでいます。個人情報保護法やGDPR等による規制はますます厳格になっており、企業・組織にとってPIIの適正な管理は重要課題です。

日本では、ISMS認証やプライバシーマークといった制度を活用している企業・組織がたくさんあります。ISMS-PIMS認証は、ISMS認証の基準となったISO/IEC 27001を拡張し、より具体的で実践的な個人情報やプライバシー保護のための情報マネジメントシステムであるISO/IEC 27701を基準としています。それ故、ISMS認証と親和性が高く、ISMS認証に付加する形でISMS-PIMS認証されます。プライバシーマークはJIS Q 15001に基づく国内制度ですが、ISMS-PIMS認証は国際標準を基にしているので、世界各国の個人情報、プライバシー保護の法律や規制との関係も整理しやすいです。ISO/IEC 27701の別添資料Annex DにはEU一般データ保護規則（GDPR）との対応表が提供されています。日本企業がGDPR等の海外の個人情報、プライバシー保護の法律や規制にも適合していく必要がでてきたことに応える認証制度として、ISMS-PIMS認証は注目され、大きな期待が寄せられています。

ISMS-PIMS認証の大きな特徴としては、「PII管理者」と「PII処理者」という2種類の振る舞いをする組織が定義しており、適用範囲がどちらに該当しているかで個別の要件が確認されることです。ISO/IEC 27701では、どんな情報をどんな目的、手段で収集・利用するのかを決めるPII管理者と実際のデータを保管・加工するPII処理者の各々が何に責任を持つのかが明確に規定されています。PII管理者とPII処理者は、同一組織内のこともあれば、委託元と委託先という関係のこともあります。パブリッククラウドを利用する場合も考慮されているので、PIIを扱う多くの組織でセキュリティ対策の検討に利用できます。

ISO/IEC 27701を委託先との個人情報に関する取り扱いの取り決め等で活用し、ISMS-PIMS認証を自社のセキュリティ対策強化・改善のきっかけにしてはいかがでしょうか。

2.6 安全な政府調達に向けて

IPA では情報セキュリティ対策の実現を目指し、国民に向けた情報提供や啓発活動、企業・組織に対するセキュリティ施策の促進とともに、政府機関や独立行政法人が安全に IT 製品やクラウドサービス等を調達するために活用できるいくつかの制度の運営を行っている。

本節では、政府機関等で使用される IT 製品のセキュリティ機能を評価する「IT セキュリティ評価及び認証制度」、及び政府機関等のシステムに組み込まれる暗号のアルゴリズムを確認する「暗号モジュール試験及び認証制度」の動向について報告する。また 2020 年度に開始した、政府が求めるセキュリティ要求を満たしているクラウドサービスを評価・登録する「政府情報システムのためのセキュリティ評価制度（ISMAP）」の概要を紹介する。

2.6.1 ITセキュリティ評価及び認証制度

サイバーセキュリティ戦略本部は、府省庁及び独立行政法人が遵守すべき情報セキュリティ対策を定めた「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）[※443]」（以下、政府統一基準）を発行した。この中では、国民の情報等を扱う公的なサービスを提供するシステムを構築する場合、そのシステムを構成する市販の IT 製品についてもセキュリティ要件を策定することを調達者に求めている。

IT 製品の調達において、セキュリティ要件を確認するための仕組みとして、セキュリティ評価の制度が先進国を中心に発展し、セキュリティ評価基準が国際規格として策定された。日本でも、このセキュリティ評価基準を用いて IT 製品を評価する「IT セキュリティ評価及び認証制度（JISEC：Japan Information Technology Security Evaluation and Certification Scheme）」を IPA が運営し、政府機関等の IT 製品調達に活用されている。

(1) 政府の IT 製品調達セキュリティ要件

政府統一基準では、調達及び運用において特にセキュリティ要件を策定すべき IT 製品分野として、経済産業省が発行している「IT 製品の調達におけるセキュリティ要件リスト[※444]」（以下、調達要件リスト）を参照している。調達要件リストには、利用者情報を扱うシステムの基盤となり、攻撃の対象となり得る以下の 11 の製品分野が指定されている。今後も対象製品分野は、拡大される予定である。

- デジタル複合機
- ファイアウォール
- 不正検知・防止システム
- サーバ OS
- データベース管理システム
- スマートカード
- 暗号化 USB メモリ
- ルータ／レイヤ 3 スイッチ
- ドライブ全体暗号化システム
- モバイル端末管理システム
- 仮想プライベートネットワークゲートウェイ

府省庁や独立行政法人の情報システムセキュリティ責任者は、これらの製品分野の IT 製品を調達する場合、想定されるセキュリティ上の脅威にそれらの製品が対抗できていることを確認することが義務付けられている。各組織が調達する IT 製品が、想定するセキュリティ要件を満たしていることを個別に確認する方法に加え、調達要件リストでは、国際標準に基づく第三者認証製品の活用も認めている。

JISEC は、IT 製品のセキュリティ評価の国際標準である ISO/IEC 15408 に基づく第三者認証制度を運営している。組織の調達責任者は、想定する脅威に対抗していることが評価され、JISEC で認証された IT 製品を購入することで、政府統一基準の要求を満たすことができる。

特に、システム構築とは独立して調達されることの多い「デジタル複合機」、国策としてセキュリティ対策が重要となる旅券やマイナンバー等の「スマートカード」の調達で JISEC の認証制度は活用されている。

(2) 認証制度の国際連携

JISEC でも採用しているセキュリティ評価基準である ISO/IEC 15408 は、欧米 6 ヵ国によるコモンクライテリア（共通基準）プロジェクトとして開発された。これらの国々では、同じセキュリティ評価基準であるコモンクライテリアを用いて、その国を代表する公的機関が運営する制度で評価された結果については相互に認め合うことで、調達国ごとに重複的な評価を行うコストを低減することを目的とした相互承認が締結された。この相互承認の

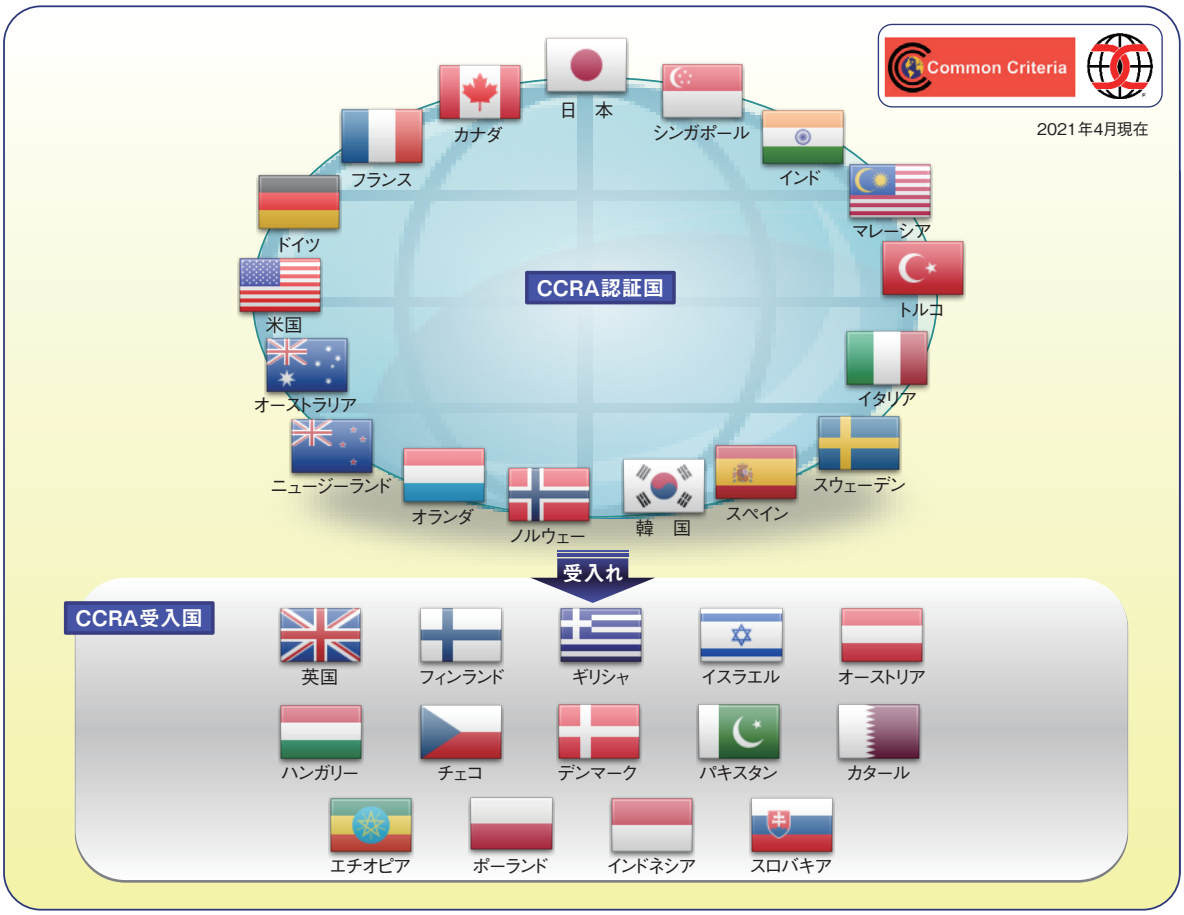
枠組みは、CCRA（Common Criteria Recognition Arrangement）と呼ばれ、その後多くの国が加盟し、JISEC を運営する日本も 2003 年に加盟している。これにより、日本のベンダは日本語の開発資料をそのまま利用し、JISEC で認証を取得した製品を CCRA 加盟国の政府調達の対象とすることができるようになった。

CCRA では、自国で認証制度を運営している「認証国」と、認証制度をまだ有しないが政府調達要件として認証結果を受け入れる「受入国」があり、近年は東ヨーロッパやアフリカの国が受入国として加盟している。2021 年 4 月現在、CCRA 加盟国は認証国 17 ヵ国、受入国 14 ヵ国の計 31 ヵ国に上る（図 2-6-1）。

(3) セキュリティ要件の共通化

コモンクライテリアでは、IT 製品が具備すべきセキュリティ要件を、規定された形式に従って記述する。例えば、アクセス制御機能においては、対象となるオブジェクトやサブジェクトのリスト、セキュリティ属性、それらを用いたアクセス方針をコモンクライテリアで規定された形式で記述する。これにより、調達者が必要としている IT 製品のセキュリティ要件仕様を、あいまいさを排除して製品開発者に伝えることを可能とする。このコモンクライテリア形式で表された調達要件仕様書を「プロテクションプロファイル」と呼び、CCRA 加盟国での IT 製品の政府調達に利用されている。加盟国の調達部門は、調達する IT 製品のセキュリティ要件をプロテクションプロファイルとして作成し、調達要件として公開している。これらのプロテクションプロファイルのうち汎用的なものは、CCRA のポータルサイト※445 にも掲載され、他の機関も同様の分野の製品を調達する際に用いることができる。日本においても、調達要件リストでは製品分野ごとにこれらのプロテクションプロファイルを指定している。また、独自の製品を調達する機関は、プロテクションプロファイルを自ら作成し※446、調達を実施している。

CCRA では、これまで調達者ごとに作成していたプロテクションプロファイルを、製品分野ごとに共通化する作業を行っている。同じ製品分野の IT 製品調達で、似たような調達仕様が調達者ごとに提示されることは、開発者にとっては負荷となる。そこで CCRA 加盟国の認証機関が中心となり、いくつかの製品分野で共通的に

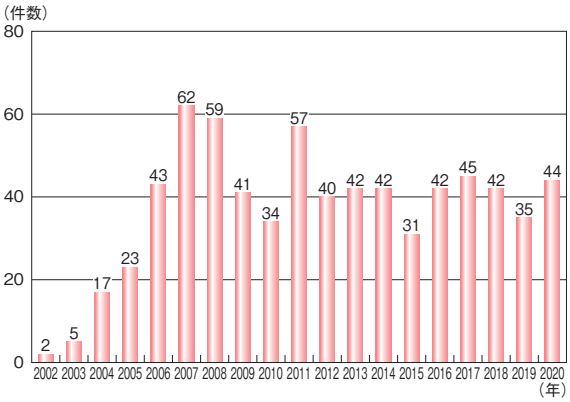


■図 2-6-1　CCRA 加盟国

用いるプロテクションプロファイルの策定を行っている。このプロテクションプロファイルは、cPP（collaborative Protection Profile）と呼ばれ、CCRA 加盟国は、該当する製品分野の調達には、このcPPを用いてセキュリティ要件を指定することとしている。既にファイアウォール、ディスク暗号ドライブ、ネットワークデバイスの製品分野について cPP が策定され、CCRA ポータルサイトで公開されている。現在も、バイオメトリクス認証やデータベースについて cPP の策定が進行中である。日本も、国内に多くの製品ベンダを有するデジタル複合機について、韓国の認証機関とともに発起人となり、各国のベンダや評価機関をメンバーとする技術コミュニティを発足し、2021 年内の公開を目指し cPP の策定を行っている。

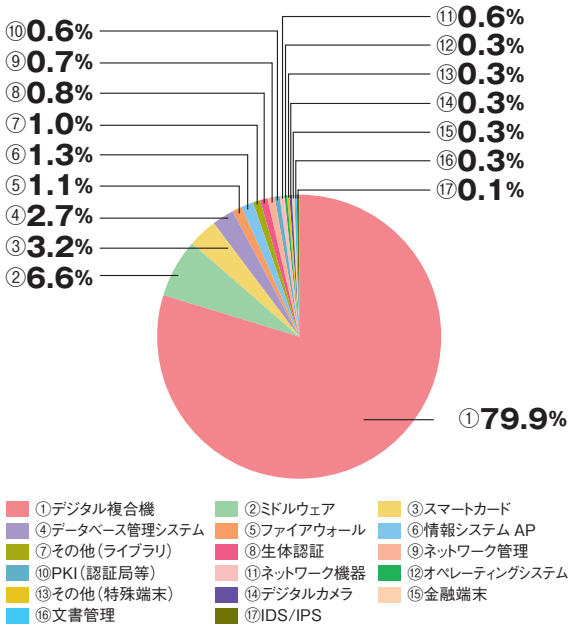
(4) 認証の状況

2020 年度までの JISEC における認証発行件数の推移を図 2-6-2 に示す。リーマンショックの影響による 2009 年の申請数の減少とそのリバウンド（2011 年度）以降、毎年 40 件前後の認証発行を行っている。



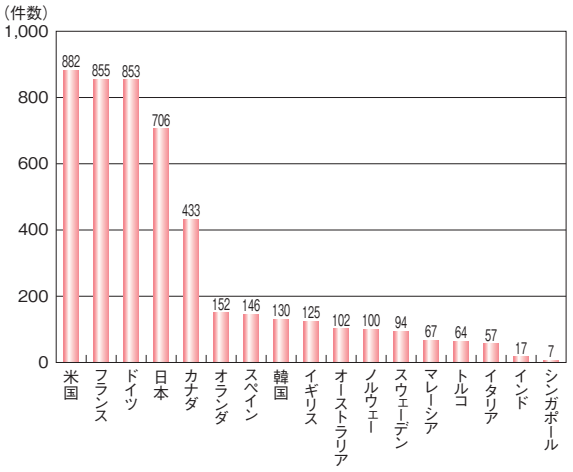
■図 2-6-2　JISEC の認証発行件数の推移

JISEC が認証発行した製品の分野の内訳を、図 2-6-3 に示す。認証製品分野としては、デジタル複合機が圧倒的に多い。これは前述のように、日本のベンダが国際的にもシェアを有し、CCRA 加盟国においても政府調達の対象となっているからである。また、その他の製品分野の認証が JISEC で少ないのは、セキュリティ製品全般において日本ベンダの国際的な競争力が弱く、デジタル複合機以外の認証申請取得がなされないこと、ファイアウォールやネットワーク管理製品のようにシステム構築の中で組み込まれてテストされ納入されることが多いため、製品単品での調達要件の対象とならないこと等が理由である。JISEC が毎年認証発行している 40 件前後は、ほとんどがデジタル複合機の新機種リリースによるものである。



■図 2-6-3　JISEC 認証発行の製品分野内訳

CCRA 加盟各国の認証機関が公開している認証発行件数の 2020 年度における累計を図 2-6-4 に示す。日本の認証発行件数は、米国、フランス、ドイツに次いで 4 番目に多い。これらの国は、政府調達に認証製品を活用しているのに加えて、国内に IT 製品の製造業者を多く持つ国々である。英国は、セキュリティ評価の歴史は長いにもかかわらず、国内の製造業者の減少により、2019 年に制度維持コストの削減を理由に認証国から受入国に移行している。韓国では、国際的に大きな市場を持つ製造業者が、製品仕向地によりモバイル製品は米国で、スマートカード関連製品はヨーロッパで認証を取得しているため、国内制度の認証発行件数は低い。



■図 2-6-4　CCRA 各国の認証件数

(5) 2020 年度のトピック

JISEC では IT 製品の認証実施のほか、国内やアジア地域における認証制度の活用や普及に向けた取り組みを行っている。

(a) IoT 製品分野セキュリティへの対応

政府統一基準では、調達要件リストとは別に、近年政府において活用されている IoT 製品についてもセキュリティ対策を求めている。更に 2020 年 4 月に施行された「電気通信事業法に基づく端末機器の基準認証」では、IoT 機器の技術基準にセキュリティ対策が追加された。このような背景を踏まえ JISEC では、IoT 製品分野に係る国内ベンダが多く存在することから、安全な政府調達の推進と国際的な市場競争力の確保を目的に、IoT 製品分野への認証制度活用に向けた取り組みを実施している。これまでにネットワークカメラシステム及び入退管理システムについて、調達者自身が調達時に必要なセキュリティ要件を確認できるようにチェックリストを公開している。2020 年度には、このうちネットワークカメラシステムのチェックリストの基本的なセキュリティ要件について、コモンクライテリアによる評価の検証を実施している。具体的には、脆弱性診断サービスを提供する民間機関 3 社により、市販のネットワークカメラシステム 3 製品を対象に、コモンクライテリアの評価手法に従った機能テスト及び脆弱性評定を実施した。この結果、短期間にいくつかの脆弱性が発見され、IoT 製品に対するコモンクライテリア適用の有効性が確認された。2021 年は IoT 機器の基本的セキュリティ要件についてプロテクションプロファイルを策定し、今後 IoT 製品分野の政府調達への活用を推進していく。

(b) ASEAN 諸国への協力

欧米諸国を中心として発足した CCRA にも、マレーシア、シンガポール、インドネシアのような東南アジアの国々が参加するようになった。JISEC は制度運営の経験を基に、セキュリティ評価制度の概要について、例年、独立行政法人国際協力機構（JICA：Japan International Cooperation Agency）が主催する ASEAN 各国の政府機関関係者に向けたセミナーを通じて情報共有を行ってきた。このセミナー参加国の一つであるベトナムから、コモンクライテリアを評価基準とするセキュリティ認証制度の確立に向けた検討のため、JICA を通じて協力依頼があった。JISEC では 2021 年 2 月及び 3 月に IT セキュリティ評価に関するオンラインセミナーを開催した。ベトナム政府の関係部門に対し、制度設立の経緯や現状及び CCRA 加盟に向けた手続きについて説明と質疑応答を行い、今後もベトナムのセキュリティ認証制度の設立と CCRA 加盟に向けた協力を継続的に行うことを約束した。

2.6.2 暗号モジュール試験及び認証制度

暗号モジュール試験及び認証制度（JCMVP：Japan Cryptographic Module Validation Program）とは、利用者が暗号モジュールの信頼性を客観的に把握できるように設けられた第三者適合性評価認証制度である。本制度に基づく認証を取得することにより、暗号アルゴリズムが適切に実装され、暗号鍵等の重要情報を適切に保護している暗号モジュールであることをアピールできる。本制度は、米国の NIST とカナダの CCCS（Canadian Centre for Cyber Security）により運営されている CMVP（Cryptographic Module Validation Program）と同等の制度であり、IPA が認証機関として運営している。本項では、JCMVP の最新動向、及び関連する CMVP の動向について述べる。

(1) 暗号モジュールのセキュリティ要求事項の新規格への移行及び CMVP の動向

JCMVP では、2018 年 6 月から、暗号モジュールが満たすべきセキュリティ要求事項（アクセス制御、物理的セキュリティ等）を定めた規格として、ISO/IEC 19790: 2012 を採用している※447。2020 年 10 月、JCMVP は ISO/IEC 19790: 2012 に基づいて、既存の承認された暗号モジュール試験機関 1 社の技能試験を実施した。

関連する CMVP の動向としては、FIPS 140-3（2019 年 9 月改訂）の暗号モジュールセキュリティ要件が ISO/IEC 19790 及び ISO/IEC 24759 の要件を参照するように変更された。これに伴い、FIPS 140-2 から FIPS 140-3 に移行するための計画※448 が公開され、2020 年 3 月に FIPS 140-3 の試験要件が SP 800-140x シリーズとして規定※449 された。その後の FIPS 140-3 への移行スケジュールは、以下のとおりである（⑤、⑥は予定）。

①2020 年 5 月 20 日：CMVP FIPS 140-2 Management Manual 改訂※450
②2020 年 7 月 1 日：Tester competency exam 改訂※451
③2020 年 9 月 21 日：FIPS 140-3 IG 公開※452、CMVP FIPS 140-3 Management Manual 改訂※453
④2020 年 9 月 22 日：FIPS 140-3 での申請受付開始

⑤2021 年 9 月 21 日：FIPS 140-2 新規申請停止
⑥2026 年 9 月 21 日：FIPS 140-2 認証は Historical List へ移動

JCMVP は、ISO/IEC 19790:2012 の採用にあたって得た知見を2019年12月にCMVPに対してフィードバックした。その概要及び FIPS 140-3 との差異について 2020 年 9 月 21 ～ 24 日に開催された暗号モジュールに関する国際会議 ICMC20※454 において報告した。

(2) 政府機関等における JCMVP・CMVP の活用

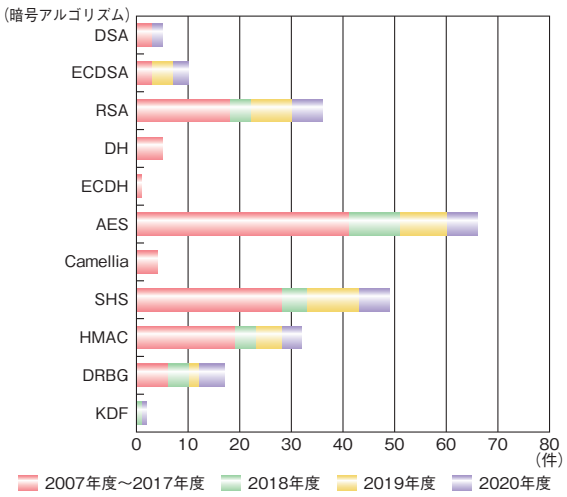
CMVP では、CMVP 認証を取得していない暗号モジュールについて、「認証されていない暗号は情報及びデータを保護しないとみなす。省庁が情報及びデータを暗号的に保護すべきであると指定した場合には、FIPS 140-2（2026 年 9 月 22 日まで）または FIPS 140-3（2020 年 9 月 22 日より）に準拠した保護が該当する。すなわち、暗号が必要であれば認証されたものでなければならず、認証が取り消されれば、その暗号モジュールを使用してはならない。※455」と規定している。

日本においては、各府省情報化統括責任者（CIO）連絡会議が決定し、2019 年 2 月に公開された「行政手続におけるオンラインによる本人確認の手法に関するガイドライン※456」において、JCMVP 認証されたハードウェアトークンに対して当人認証保証の最高レベル 3 を与えるとされた。

(3) IT セキュリティ評価及び認証制度（JISEC）との連携

IPA が運営する評価認証制度には、JISEC と JCMVP の二つがある。JISEC が 2016 年に発行、2020 年に改定したガイドライン※457 によって、JCMVP の活用方針が示されている（JISEC の活動については「2.6.1 IT セキュリティ評価及び認証制度」参照）。

2020 年度は、JISEC のもとで、この活用方針に関連する「Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015※458」に基づくデジタル複合機の認証が 28 件完了している※459。このプロテクションプロファイルでは、信頼できるツールを用いた暗号アルゴリズム実装のテストを求めている。このテストに、JCMVP の暗号アルゴリズム実装試験ツール（JCATT：Japan Cryptographic Algorithm implementation Testing Tool）が活用され、認証に貢献している。具体的には、図 2-6-5 に示すように、JCATT を使って確認された暗号アルゴリズム実装の実績が、2018 年度、2019 年度及び 2020 年度において堅調に増加している。また、2019 年度より楕円曲線暗号の一つである ECDSA（Elliptic Curve Digital Signature Algorithm）の実績が増えており、楕円曲線暗号のニーズが反映されていると考えられる。



■図 2-6-5　JCATT により確認された暗号アルゴリズム実装の実績
（出典）IPA の公開情報※460 を基に作成

(4) 承認されたセキュリティ機能等の見直し

2020 年度に JCMVP の下部組織である技術審議委員会において、暗号モジュールのセキュリティ要求事項に組み合わせることのできる暗号の一覧である「承認されたセキュリティ機能※461」の見直しに関して、以下の審議が実施された。

①RSA 1024 の署名検証の削除
②SHA-1 の署名検証の削除
③署名検証のパラメータ改正
④TLS version 1.0 及び 1.1 の鍵導出関数の削除
⑤TLS version 1.3 の鍵導出関数の NIST SP800-56C※462 への適合性

①②③は 2020 年 12 月施行の「電子署名及び認証業務に関する法律施行規則※463」の改正に対応したものである。同規則の改正内容は、署名検証においても、先行してセキュリティ上の条件（鍵長の制約や使用可能なハッシュ関数のアルゴリズム）が強化されていた署名生成と同じ条件に揃えるものであった。技術審議委員会では、同様の主旨の改正を「承認されたセキュリティ機能」に対して行うことの可否を審議した。その結果、「削除されるセキュリティ機能を実装した認証済みの製品の扱いや、

同セキュリティ機能を使い続けることが必須（例えば、長期署名の検証）の製品の認証について、認証機関として方針を定める」ことを条件として承認を得た。2021年5月現在、認証機関としての方針を策定中である。

④では、TLS（Transport Layer Security）version 1.0及び1.1の使用を非推奨とする国内外の動向や、実際のサポート状況を踏まえ、これらのTLSのバージョンで定められた鍵導出関数を「承認されたセキュリティ機能」から削除することについて審議し、技術審議委員会の承認を得た。

⑤では、TLSの新たなバージョンであるTLS version 1.3の鍵導出関数がNIST SP800-56Cに適合するかどうかを審議し、技術審議委員会は適合すると判断した。また同文書に適合する鍵導出関数は「承認されたセキュリティ機能」に含まれるため、新たにTLS version 1.3の鍵導出関数の実装試験仕様を整備していくことについて、技術審議委員会の承認を得た。

更に、2020年度から以下の事項について検討を進めることについても技術審議委員会の承認を得た。

- ECDSAの仕様変更への対応
- TLS version 1.3の鍵導出関数の実装試験仕様

前者は、「承認されたセキュリティ機能」におけるECDSAの仕様の参照先の一つであるANS X9.62-2005が2020年9月に廃止され、新たにANSI X9.142-2020がリリースされたことを受け、両規格の差分や既存の製品への影響を調査し、JCMVPとしての対応を検討するものである。後者は、TLS version 1.3の鍵導出関数の実装試験仕様を整備する方針を受け、対応する試験方法や内容を検討するものである。

(5) JCMVP規程類の改正

JCMVPの下部組織である運営審議委員会では、認証業務運営の方針に関する事項及びマネジメントシステムの維持に関する事項等の審議を行い、統括責任者に対する助言を行う役割を担っている。2020年度に運営審議委員会を開催し、JCMVP規程類の大規模な改正について審議を実施した。

今回の改正目的は、サプライチェーンリスクが重大なセキュリティ課題として認識されるようになってきている現状に鑑み、JCMVPの規程類では以下の事項についての取り扱い方法が明確化されていなかったため、規程として取り扱い方法を明確化することであった。

- サプライチェーンリスク等への対応方針
  - JCMVP認証制度の目的の明確化
  - 運営審議委員会の役割の追加
  - 暗号モジュール認証及び暗号アルゴリズム確認の申請の制限
  - 暗号モジュール認証及び暗号アルゴリズム確認の認証作業の中止、及び認証許諾拒否の新設
  - 日本または輸出貿易管理令別表第3の地域に本社を有しない企業等への暗号モジュール認証及び暗号アルゴリズム確認の譲渡に対する対策
- 認証済暗号モジュール及び確認済暗号アルゴリズムに対する認証効力の一時停止及び取り消しに関する条件
- 規程類が改正されたときの認証済及び認証中の暗号モジュール及び暗号アルゴリズムへの改正規程類の適用方針

改正の大きなポイントは、JCMVP認証制度の目的に「日本国内におけるセキュアな暗号モジュールの調達、購入及び利用に資する」と追加することで、サプライチェーンリスクへの対応を考慮し、必要に応じて適切な措置を講じることができることを明確にした点と、中立性・客観性の観点から、必要に応じて運営審議委員会から、申請の受付可否、認証の許諾、拒否または取り消し等に関する事項等の助言を得ることができることを明文化したことである。

なお、規程類の改正は2020年10月に行われ、同11月から適用開始となった※464。

2.6.3 政府情報システムのためのセキュリティ評価制度（ISMAP）

2020年6月3日、内閣官房、総務省、経済産業省は政府情報システムのためのセキュリティ評価制度（ISMAP）の開始をアナウンスした※465。本項では、ISMAPの概要について紹介する。

(1) ISMAPの概要

政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program:通称、ISMAP（イスマップ））は、政府が求めるセキュリティ要求を満たしているクラウドサービスをあらかじめ評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスの円滑な導入に資することを目的とした制度である。

従来、政府調達にあたっては、個々のクラウドサービスが実施していると表明する情報セキュリティ対策の実施状況を、調達者が直接確認することが必要であったが、本制度により、確認を省略でき負担を軽減できる。

(2) ISMAP 制定の経緯

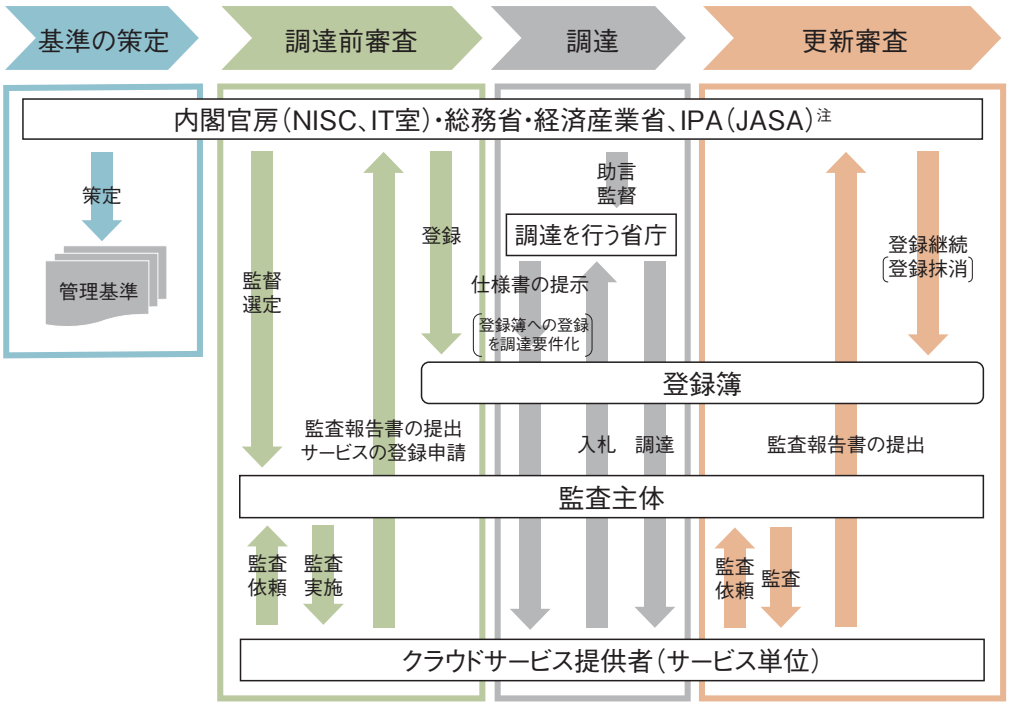
各府省情報化統括責任者（CIO）連絡会議において決定され、2018 年 6 月に公開された「政府情報システムにおけるクラウドサービスの利用に係る基本方針※466」（2021 年 3 月 30 日付けで ISMAP に関する記述が追記されている）では、「クラウド・バイ・デフォルト原則」が掲げられた。これを踏まえ、経済産業省と総務省は、2018 年 8 月から「クラウドサービスの安全性評価に関する検討会※467」を発足させ、適切なセキュリティ要件を満たすクラウドサービスを導入するために必要な評価方法等を検討し、2020 年 1 月に「クラウドサービスの安全性評価に関する検討会とりまとめ※468」が公開された。また、同月のサイバーセキュリティ戦略本部会合において「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて※469」が決定された。

また上記検討会において、2019 年 6 月から、政府情報システム調達に応募するクラウド事業者が遵守すべきセキュリティ管理基準（以下、ISMAP 管理基準）の検討が行われた。ISMAP 管理基準は、国際規格をベースに「政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版）」「NIST SP800-53 rev.4」を参照して作成された。国際規格としては、情報セキュリティに関しては JIS Q 27001（ISO/IEC 27001）、JIS Q 27002（ISO/IEC 27002）とクラウドサービスの情報セキュリティに関する JIS Q 27017（ISO/IEC 27017）が参考にされた。また、これらの国際規格に準拠して編成された「クラウド情報セキュリティ管理基準（平成 28 年度版）」が参考にされ、そこに含まれるガバナンス基準については JIS Q 27014（ISO/IEC 27014）が参考にされた。

(3) ISMAP の運用

本制度においては、まず、政府機関等が調達するクラウドサービスに対して要求するべき基本的な情報セキュリティ管理・運用の基準が後述する NISC 他の所管政府機関にて定められる。また、本制度で定められた情報セキュリティ監査の枠組みを活用した評価プロセスに基づき、上記の基準を満たすセキュリティ対策を実施していることが確認されたクラウドサービスが ISMAP クラウドサービスリスト（以下、サービスリスト）に登録される。政府機関がクラウドサービスを調達する場合、上記リストに登録されたサービスを選定候補とする。

また、本制度における監査を実施できる監査機関は、あらかじめ本制度で定める要求事項を満たすことが確認



（注）制度運用に係る実務及び評価に係る技術的な支援をIPAが行い、うち、監査機関の評価及び管理に関する業務についてJASAに再委託する。

■図 2-6-6　クラウドサービスの安全性評価の制度のフロー
（出典）内閣官房・総務省・経済産業省「政府情報システムのためのセキュリティ評価制度（ISMAP）について※470」

され、本制度が公表するISMAP監査機関リスト（以下、監査機関リスト）に登録される。

本制度のフローを図2-6-6（前ページ）に示す。図において、クラウドサービス提供者は監査機関リストに登録された機関による監査を受け、所管政府機関にサービス登録申請を行う。所管政府機関は審査を行い、承認されたサービスがサービスリスト（図では登録簿と表記）に掲載される。府省庁の調達者はサービスリストを使って調達先候補を選ぶ。所管政府機関は監査者認定と監査結果に基づくサービスリスト管理を行う。

（4）セキュアなクラウド利用に向けて

本制度は2020年6月、運用が開始された。

ISMAPの所管は2021年5月現在、NISC、内閣官房情報通信技術（IT）総合戦略室、総務省、経済産業省であり、最高意思決定機関としてISMAP運営委員会を設置し、事務局はNISCに置き、運用実務はIPAが担当している。

制度の概要、基準規程類、監査機関リスト、及びサービスリストは、ISMAPポータルサイト※471で公開されている。2021年4月時点で登録されている監査機関は4機関、また、クラウドサービスは10サービスである。

なお、IPAは総務省からの受託事業として、クラウドサービス事業者がサービスリストへの登録を行うにあたり、セキュリティ対策の進め方及び管理基準の理解の一助となることを目的として、管理基準マニュアルの検討を行っている。

また、ISMAPで公開される情報は、重要インフラ分野等を始めとする民間企業においても参照されることで、クラウドサービスの適切な活用の推進が期待される。これに関連して、2019年5月23日に改定されたNISCの「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）※472」においては、「事業環境の変化を捉え、インターネットを介したサービス（クラウドサービス等）を活用するなど新しい技術を利用する際には、国内外の法令や評価制度等の存在について留意する。」とされており、国内の評価制度としてはISMAPが該当すると考えられる。

「クラウドサービスの安全性評価に関する検討会とりまとめ」にも記載されたように、情報システムのセキュリティ確保の責任は、一義的に当該システムの調達者／利用者が負うものである。本制度に登録されたクラウドサービスを利用したとしても、それだけでは情報システム全体のセキュリティが十分に確保されることにはならない。情報システムの調達者／利用者は、利用するクラウドサービスについて適切な設定を行うことに加えて、情報システム全体のセキュリティリスクを分析し、適切な対策を行うことが求められる。

COLUMN

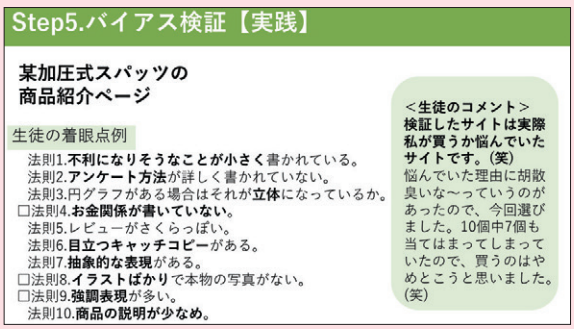
噂を信じてしまう法則って?
～日出学園中学・高等学校の取り組み～

インターネットの普及により、私達は知りたいと思った情報をすぐその場で調べることができるようになりました。しかし、その情報は、誰かが悪意を持って流した偽の噂(デマ)である危険性をはらみます。スマートフォンを通じて、SNS や Web サイトに触れる機会の多い中高生にとって、ネット上に溢れる情報に対し、高い情報モラルをもって接することは特に重要です。ここでは、第 16 回 IPA「ひろげよう情報モラル・セキュリティコンクール」2020 で文部科学大臣賞を受賞した、日出学園中学校・高等学校[i]の活動事例[ii]をご紹介します。

同校では、①「他人に相談せずに、自分だけで判断してしまうこと」、②「深く考えずに何となく行動してしまうこと」の二つを防ぐことを課題とした情報モラル教育に取り組みました。

まず、①を防ぐため、オンライン授業ツールの使い方や Web サイトの信頼性について、生徒同士で意見を交換することで、「対話的に」学び、他者に相談する意義を学びました。次に、②を防ぐため、普段何となく判断している基準を明文化することで、ネット上に溢れる情報を「深く」読み解くきっかけを作りました。噂を信じてしまう法則を身の回りの噂から考えてみたところ、生徒からは、「自分自身に関わること」「完全に否定できないこと」「具体的な人物や場所が出てくること」等が挙がりました。その後の実習では、これらの法則に基づいた「新しい噂」を作りました。また、隠れたバイアスを吟味する能力を養うべく、あえてバイアスを含んだ「怪しい広告」(図 1)を作成し、それを基に、広告を眺める際のチェックリスト(図 2)をまとめました。更にそのチェックリストを、実際の広告に照らし合わせ考察することで、日常においても都度触れる情報を「深く」考える習慣を身に付けています。

■図 1　生徒が制作した広告
(出典)日出学園中学校・高等学校より提供



■図 2　生徒による広告の検証例と感想
(出典)日出学園中学校・高等学校より提供

新型コロナウイルスの影響により、急速なオンライン化が進む中、情報モラル・セキュリティ教育の重要性はますます高まっています。本コンクールで受賞した学校の取り組みをぜひご覧いただき[ii]、今後の教育に活かしていただければ幸いです。学校関係者の皆様、ご家族に小・中・高校生がいらっしゃる皆様には、本コンクールへのご応募もお待ちしております。

i　https://high.hinode.ed.jp/〔2021/6/16 確認〕
ii　IPA：活動事例　https://www.ipa.go.jp/security/event/hyogo/2020/awd_katsudo.html〔2021/6/16 確認〕

2.7 情報セキュリティの普及啓発活動

2020 年は、これまで「当たり前」とされてきたことが新型コロナウイルスの感染拡大により、大きく覆された年となった。毎日の出勤はテレワークに切り替わり、対面での会議や授業はオンラインによる実施が推進された。

このように生活の中の IT 利用機会が大きく増え、それに伴うセキュリティ対策はこれまで以上に重要になっている。また情報セキュリティを含む IT 利用スキル（IT リテラシー）の向上も重要性を増している。

本節では、様々な組織・団体が各々の視点で実施した普及啓発活動について述べる。

2.7.1 恒常的な対策等に関する普及啓発活動

インターネットの利便性が広く知られる一方で、その危険性や利用上の注意に対する理解の深化は遅く、利用者への啓発が継続的に行われている。

(1) 多様なツールを活用した普及啓発活動

インターネットが生活の多くの場面で使用される中、未だインターネットを悪用した詐欺被害や SNS を介した未成年者誘拐、誹謗中傷等、事件や事故は後を絶たず、利用者の情報セキュリティ対策の実施状況も、情報セキュリティ意識の定着もまだ十分とはいえない。

ここでは、普段情報セキュリティを意識していない人でも意識を向けやすいよう工夫が施された資料やツールを紹介する。

NISC によるサイバーセキュリティ月間（2021 年 2 月 1 日～ 3 月 18 日）では、「ラブライブ!サンシャイン !!」とのタイアップによる短編アニメーションを公開した※ 473。「ラブライブ!」シリーズは、過去には紅白歌合戦に出場する等、若年層だけでなく広く国民の認知度を得ていることから、幅広い層への意識付けが期待された。

動画による啓発は、文字を読むよりも視聴者へのメッセージが伝わりやすく、興味を引きやすいため、他にも多数公開されている。山形県警察本部は、「『サポート詐欺』に騙されないで!※ 140」と題した 3 本の動画を公開した。これは、実際の偽の警告画面を基に、警察官が犯人とやり取りをした様子を記録したものである。文章だけでは伝わりにくい犯人の発語の特徴や画面の内容について理解することができる。埼玉県警察本部は、「ポッポくん、ポポ美ちゃんのサイバーセキュリティ教室」のシリーズとして「安全なパスワードの管理※ 474」や「システム・アプリのアップデート※ 475」の動画を公開し、手口や対策方法についてイラストを用いて解説している。

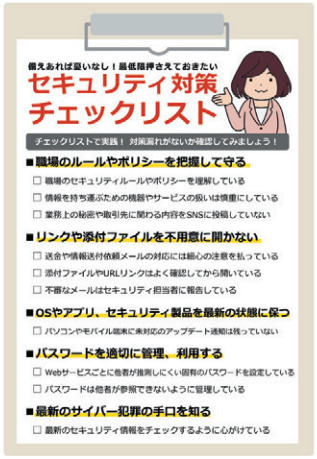
動画以外にも、様々なツールが公開された。警視庁は、サイバーセキュリティ学習用ボードゲームとして「サイバー迷宮脱出ゲーム」を公開した（図 2-7-1）。「オンラインゲームの課金」や「SNS への写真投稿」等、日常的に行っている行為が、どのような問題につながっていくのかをコマを進めることで学べるものとなっている。

■図 2-7-1　サイバー迷宮脱出ゲーム
（出典）警視庁「サイバーセキュリティ学習用ボードゲーム※ 476」

鳥取県警察本部は「インターネット安全利用啓発まんが※ 477」と題し、偽サイトや偽警告サイト・偽サポート請求、スマートフォンのセキュリティ対策等をテーマにした漫画を作成した。県民にとって読みやすい漫画というツールによって注意点が分かりやすく描かれている。

また、JNSA が「みんなの『サイバーセキュリティコミック』」プロジェクトを開始し、クラウドのセキュリティや情報漏えい対策等をテーマに、全 8 話の漫画による解説を公開した※ 478。

更に、社会人が身に付けるべき基本的な対策をまとめた「働く大人なら最低限知っておきたいネットセキュリティの基本 2021※ 479」がトレンドマイクロ株式会社から無償で提供されている（次ページ図 2-7-2）。新型コロナウイルスの影響で、新入社員等の集合研修が困難な中でも、Web サイトから資料をダウンロードし、各自で学習することができる。巻末には情報セキュリティ対策のチェックリストが掲載されており、これを活用した対策状況の確認が推奨される。



■図 2-7-2　セキュリティ対策チェックリスト
（出典）トレンドマイクロ株式会社「働く大人なら最低限知っておきたいネットセキュリティの基本 2021」

(2) ネット上の誹謗中傷への対策

2020 年 5 月、当時人気だったリアリティ番組の出演者の一人が自ら命を絶った。番組内での言動を端緒として中傷投稿が SNS 上にあふれ、それが一因となったと報道された※480。

このような状況のもと、総務省は 2020 年 8 月、「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（以下、プロバイダ責任制限法）の第 4 条第 1 項の発信者情報を定める省令に、発信者の電話番号を開示の対象として追加した※481。

誹謗中傷の投稿は匿名で行われることが多く、投稿の削除請求のためには、まず、投稿者を特定する必要がある※482。プロバイダ責任制限法では「情報の流通によって自己の権利を侵害された」場合、SNS 事業者等に投稿者の IP アドレスや投稿時間の開示を請求することができるとしている。次に、その情報を基に、プロバイダに対して氏名や住所の開示請求を行うことで、投稿者の特定ができる。しかし、SNS 事業者等が、IP アドレスを保存していないケースや、プロバイダが保有する接続記録が一定期間を経過すると消去されてしまうケース等、投稿者の特定に結びつかないことがあった。

今回の法改正により、投稿者の電話番号が開示されれば、電話会社に発信者の氏名や住所を照会することで投稿者の特定につながり、これが抑止効果となることが期待される。

2020 年 12 月、群馬県では全国に先駆けて「インターネット上の誹謗中傷等の被害者支援等に関する条例」を制定した。これは、誹謗中傷やプライバシー侵害により命に関わる事件が発生していることを背景に、県民が被害者にも加害者にもなることがないよう、正しくインターネットを活用する知識と能力を習得することを目的としたものである。本条例に関する知事のメッセージは YouTube で公開されている※483。

2020 年 4 月に ByteDance 株式会社、Facebook Japan 株式会社、LINE 株式会社、Twitter Japan 株式会社を中心とした SNS 事業者等によって設立された一般社団法人ソーシャルメディア利用環境整備機構は、SNS 等に起因する児童被害防止を強化し、ソーシャルメディアの健全な発展と、信頼される環境構築を目指すとしている（図 2-7-3）。同年 7 月には、法務省人権擁護局、総務省とともに「#NoHeartNoSNS※484」というスローガンを発表し、「誰かを傷つけてしまいそうなら」「あなたが傷ついたら」どうすればよいのか等について紹介する特設ページを公開した。特設ページでは、人権相談の窓口や、誹謗中傷等、ネット上で公開された情報を削除するにはどうすれば良いのか、相談員がアドバイスを行っていることも案内し、「あなたは一人ではありません。みんながあなたの力になります。」と締めくくっている。

■図 2-7-3　参加事業者が運営するサービス（2021 年 2 月現在）
（出典）一般社団法人ソーシャルメディア利用環境整備機構のホームページ※485 から抜粋

また、SNS 事業者等はルール改正等による課題の解決にも努めている。

Twitter Japan 株式会社は 2020 年 3 月、年齢、障がいや病気に基づいて人間性を否定する言葉を削除の対象に加えた※486。また、同年 8 月には投稿者が自分の投稿にリプライが可能なアカウントを選択できる機能※487を追加したこと等から、攻撃的なリプライの減少が期待されている。

TikTok 運営会社の日本法人である ByteDance 株式会社は、青少年を保護する対策の一環として 2021 年 1 月、16 歳未満の利用者については、初期設定を「非

公開」にした※488ほか、同年2月からは起動時に生年月日の入力を求める画面を表示し、利用者の年齢確認を開始している※489。

また、多くの投稿系サービスを提供するヤフー株式会社は、2020年6月「プラットフォームサービスの運営の在り方検討会」を設置し、AI等を利用した誹謗中傷等の投稿抑止と削減を進めるとともに、各サービスのポリシーや削除基準を明確化し、透明性の高いレポートを公表していくことを発表した※490。

まだまだ向上の余地はあるものの、公的機関、SNS事業者等は新たな誹謗中傷の被害者を出さないよう活動を行っている。一方、SNSの投稿者も自らの言動に責任を持ち、加害者とならないよう意識の変革が求められる。

2019年に行方不明になった小学生の母親に対し、「殺すぞ」等のメッセージをSNS上に投稿して脅迫した被告の初公判が2020年10月に開かれた。被告の男は、逮捕後に自分自身もインターネット上で誹謗中傷を受けており、初公判の場で「被害者の気持ちが身にしみて分かった」と謝罪を述べた※491。この言葉が一つの教訓となるのではないだろうか。

2.7.2 Withコロナにおける普及啓発活動

新型コロナウイルスの蔓延防止策の一つとして、一層利活用が進むインターネットを、安全に使用するための新たな取り組みについて考察する。

(1)テレワーク・オンライン授業

内閣府が発表した「新型コロナウイルス感染症の影響下における生活意識・行動の変化に関する調査※492」によると、国内のテレワーク実施率は2020年5月時点では全国平均で27.7%、同年12月には21.5%であった。テレワークは働き方改革の切り札の一つでもあることから、導入・実施の継続に対する期待が続いている。

2020年12月、厚生労働省はテレワークについて、実施の際の留意点や関連情報をまとめたリーフレット「テレワークを有効に活用しましょう※493」を公開した。テレワークを実施するまでの流れや労務管理はもちろん、情報セキュリティの必要性についても言及されており、テレワークの開始前に一読することが望まれる。また、総務省では、情報セキュリティの担当者が選任されていない中小企業においても、テレワークを実施する際に必要最低限の対策が行えるよう「テレワークセキュリティに関する手引き(チェックリスト)」を公開している※108。

IPAは、「不正アクセス防止対策に関する官民意見集約委員会(官民ボード)」の活動の一環として運営する情報セキュリティ・ポータルサイト「ここからセキュリティ!※494」上に、テレワークに関するセキュリティ情報を集約し公開した(図2-7-4)。このページでは、官民ボードメンバーが各々公開する情報の中から、テレワークを導入する際に参考となるガイドラインや、Web会議システムの利用時に必要な対策等30以上のコンテンツが紹介されている。

■図2-7-4　テレワークのセキュリティコンテンツ(一部)
(出典)IPA「ここからセキュリティ!」

2020年3月、政府の要請を受け、新型コロナウイルスの感染拡大防止策として多くの学校が休校となった。休校が長引くにつれて、オンライン授業の必要性が急浮上し、文部科学省は「新型コロナウイルスによる緊急事態宣言を受けた家庭での学習や校務継続のためのICTの積極的活用について※495」と題した事務連絡を各都道府県教育委員会に対して行った。この中で、家庭におけるICT機器利用の留意点として、情報セキュリティの確保の必要性が明記されている。また、付属のタブレット活用のルールのサンプルには、端末を使用する際に子ども達が注意すべき点が記載されており、安心・安全な利用のために必要な行動を学べる資料となっている。

更に、オンライン授業を早期に実現するため、2020年度第3次補正予算が成立しGIGAスクール構想が加速し始めた。GIGAスクール構想は、子ども達に1人1台の端末と通信ネットワークを提供し、個別最適化された学びを実現すること等を目的として2019年12月に文部科学省が打ち出した計画である※496。学校は計画を急ピッチで進めるだけではなく、2019年10月に文部科学省が改訂した「教育情報セキュリティポリシーに関するガイドライン※497」を実践することが不可欠である。

一部の学校では、インターネットを利用するために身に

付けるべき事項について、オンラインで学べるツールを開発し、臨時休業中も積極的な指導を行った。

立教新座中学校・高等学校では、インターネットを利用した授業は、「多くの情報から必要な情報を取捨選択する力の育成」「情報社会に積極的に参画する機会」であるととらえ、オンラインで視聴できる動画やオンライン確認テストを開発した（図 2-7-5）。

オンライン授業が推進される中、インターネットを利用する児童生徒が、インターネットを利用する前、または利用しながら情報モラルや情報セキュリティの知識を習得することは、今後一層重視されると予想される。

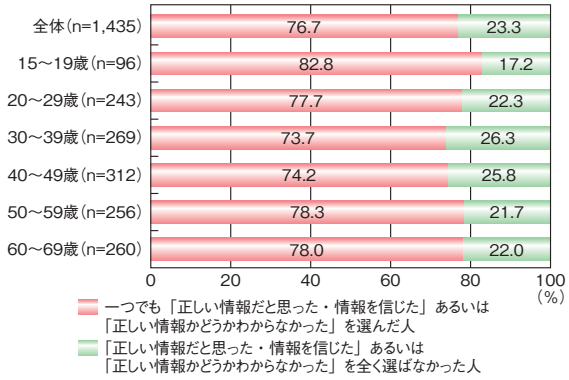
■図 2-7-5　オンライン教材（確認テスト）
（出典）立教新座中学校・高等学校提供

(2) フェイクニュースやデマへの対応

2020 年 4 月に出された緊急事態宣言下において、テレビのニュース番組では、スーパーマーケットのトイレットペーパー売り場に品物がなくなっている映像を繰り返し映し出した。「買いだめはしないでください」「紙はなくなっていません」というアナウンスよりも、映像のインパクトは大きかった。トイレットペーパーが品薄になるというデマは、SNS 上での発言が端緒ともいわれている※498。

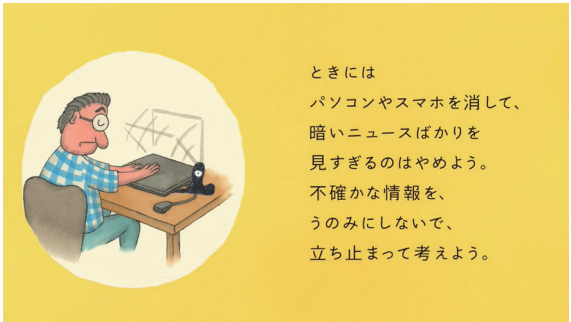
総務省が公表した「新型コロナウイルス感染症に関する情報流通調査※499」では、新型コロナウイルスに関するフェイクニュースやデマを見聞きした人は 72.0% に上った。そのうち、フェイクニュースやデマを「正しい情報だと思った・情報を信じた」あるいは「正しい情報かどうかわからなかった」人は 76.7% であった（図 2-7-6）。このうちの 35.5% は、その情報をほかの人と共有・拡散したと回答しており、少なくない人が偽の情報を広める側に回ってしまったことが分かる。

台湾においてもトイレットペーパーの在庫が切れるというデマがネット上で拡散されたが、お尻を振るマンガ絵の行政院長が「お尻はみんなひとつしかないよ」と語り、「マスクの原料は台湾産、ティッシュペーパーは南米産」と説明したポスターを投稿した。このユーモアのある投稿のおかげで正しい情報の方が、デマや誤情報よりも拡散されたため、台湾では事態の悪化が防げた※500。ユーモアのある投稿が拡散され、デマの力を弱めたと考えられており、学べることがありそうだ。



■図 2-7-6　新型コロナウイルスに関する間違った情報や誤解を招く情報への接触状況
（出典）総務省「新型コロナウイルス感染症に関する情報流通調査」を基に IPA が編集

人から人へと広がる玉石混交な情報に振り回され、新たな問題を引き起こしてしまうことがないよう、日本赤十字社が動画「ウイルスの次にやってくるもの※501」を公開している（図 2-7-7）。この中では、「誰にもまだわからないことは、誰にもまだわからないことでしかない。そのままを受け止めよう」と、情報を冷静に取り扱うことの重要性が訴えられている。



■図 2-7-7　心や社会を守る心構えを伝える動画コンテンツ
（出典）日本赤十字社「ウイルスの次にやってくるもの」

(3) コロナ差別への対応

新型コロナウイルスの患者や、医療従事者への偏見や差別が問題となっている。インターネット上で感染者やその家族を特定する動きや、感染者と思しき人に対する差別的な書き込みが行われ、ある被害者は「ウイルスより

恐ろしかった」としている※502。

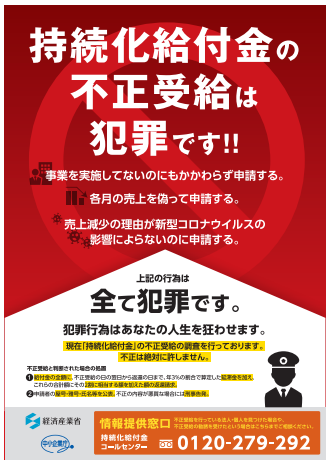
宮城県は、2020年12月、新型コロナウイルスの感染者やその関係者に対する誹謗中傷や偏見、差別の根絶を訴える決議案を可決した。これを受けて、行政、医療、学校等が連携し「ストップ!コロナ差別」の共同宣言が行われチラシが作成される等、啓発活動が行われた※503。

2021年2月、厚生労働省は新型コロナウイルスに関する偏見や差別を防止するための規定が設けられた「新型インフルエンザ等対策特別措置法等の一部を改正する法律」を公布した※504。この法律の改正により、感染者の個人名等を特定し、SNS等で公表・非難するような行為は許されない事例であることが示された。

(4) SNSによる悪質な勧誘への対応

特殊詐欺の「受け子」等に代表される「闇バイト」の勧誘は、SNSによって発信されるものが依然として少なくない。2020年は新型コロナウイルスの感染拡大防止のため、営業自粛等の影響を受ける事業者に対する支援策として持続化給付金が支給された。しかし、この制度を悪用した不正受給の勧誘が行われ、SNSもその手段の一つとなった。独立行政法人国民生活センターは「新型コロナウイルスに便乗した悪質商法にご注意!※505」と題した報道発表を行い、犯罪に加担しないよう注意を促した。また、経済産業省と中小企業庁は「犯罪行為はあなたの人生を狂わせます」と、犯罪抑止のメッセージを発信した(図2-7-8)。

また、犯罪被害につながるアルバイトにも注意が必要である。「荷物転送バイト」の勧誘は、新型コロナウイルスが蔓延する中、「自宅にいながら安全に稼ぐ方法」としてSNS上に広がっている。このアルバイトに登録する際には、写真付きの身分証明書等の個人情報の提示を求められ、この情報が携帯電話等の契約に悪用されている。知らぬ間に契約された登録者は、携帯電話の料金を請求されるほか、自分名義の携帯電話が特殊詐欺等に利用されてしまうことから、神奈川県と埼玉県は注意を呼びかけた※507。



■図2-7-8　持続化給付金の不正受給を抑止するためのチラシ
(出典)経済産業省・中小企業庁「持続化給付金の不正受給は犯罪です!!※506」

2.7.3 今後の課題

「2.7.2 Withコロナにおける普及啓発活動」に記したとおり、国内の多くの学校が新型コロナウイルスの感染予防対策による休校を余儀なくされた。教育委員会等から休校中に活用できる資料やツールが公開されている。

しかし、インターネットにアクセスする術を持たない子どもと、自由に通信機器を使用してインターネットにアクセスできる環境にある子どもとでは、その活用に大きな開きがあったことが推測される。また、保護者が傍らにいて、操作方法等について指導を受けた子どもとそうでない子どもとでは、インターネットの危険性を知る機会に差ができたことも推測される。

2021年2月、新型コロナウイルスのワクチン接種が開始され、日常を取り戻す兆しが見え始めた。ワクチン接種後の副反応が懸念される中、厚生労働省は接種を受けた後の健康状況についてSNSを利用した調査を行うこととした。また、同省は、新型コロナウイルスのワクチンに関する相談窓口等の情報や、新型コロナウイルスにより、家計に影響を受けたひとり親世帯に対する「ひとり親世帯臨時特別給付金」の受け取りの呼びかけ等、SNSを通じて様々な情報を発信している。

これらは、SNSで情報の収集や送信をしなければ、自分の行動や、更には生活にまで影響する重要な情報を得られない状況となりつつあることを示している。

インターネットのみならずSNSも生活の「インフラ」になったというのはたやすい。しかし、スマートフォンやタブレットを所有しない人や、新型コロナウイルスの影響で、ITサービスへの出費が困難になった人に、SNSを使った情報が届くのかどうか、課題は少なくない。

スマートフォン等のアプリケーションやサービスが多数提供されたことにより、メディアの種類は格段に増加しているといえる。様々な環境下にある人にどのようなメディアを使って平等に情報を伝えるのか、平等性が求められる学習や健康、生活等に関連する情報をすべての人に届ける手段について、情報発信者は十分に検討する必要があるだろう。

COLUMN

みんなバラバラにならないで!

こんにちは! ぼくは、IPA「ひろげよう情報モラル・セキュリティコンクール」応援隊長のまもるです。新型コロナウイルスの影響で、学校に行けなくなったり、家族がお家で仕事するようになったり、いろんなことが変わったね。頑張って変化に対応しながらも、みんなが元気でいてくれるといいな、と思っているよ!

さて、この新型コロナの発生によって、悲しい出来事がネットでもたくさん起きてしまいました。例えば、一生懸命患者さんを治療しているお医者さんや看護師さんに対して SNS で意地悪を言ったり、感染したお友達が通っている学校に「学校をなくしてしまえ」なんて悲しいメールを送ったり。コロナだけでもとても大変な状況なのに、どうしてこんなことになってしまうのかな。ぼくは、家族で話し合ったりネットで調べたりして、こう考えてみたよ。

世の中は「感染している人」と「感染していない人」だけがいると考えると、そこにはどうしても大きな溝ができてしまう。例えば「感染していない人」は感染したくないから「感染している人」とは距離を置きたくなる。もちろん、感染を拡大させないためには物理的な距離を置く必要はあるのだけれど、でも、心まで離れてしまう必要はないよね。

誰だって(もちろん、感染してしまった人だって!)コロナにかかりたくない。でも、目に見えないウイルスは、いつの間にか忍び寄って来て体を蝕む。それは、「感染した人」だって「感染していない人」だって気がつかないうちに起きていることなんだ。それに、自分は感染していないと思っている人も、本当は今「感染している」かもしれないし、「過去に感染していた」かもしれない。今感染していなくても、いつかかるかわからないから「感染していない人」は「まだ感染してない人」と言い換えることもできるよね。そう考えると「感染していない人」は、「感染している人」を攻撃できなくなるはずだよ!

東京都では「戦うべき本当の相手は人ではなくウイルスです[i]」というメッセージを出したよ。ほんとだね。誰だって新型コロナにかかりたくはないけれど、戦う相手が見えないから混乱して、本当に大切なことを見失ってしまっているのかもしれないね。

「コロナはとても嫌なウイルスで、この地球に来なければよかったのに」と思うけど、コロナはもう来てしまって、ぼくたちの健康を脅かしている。それにぼくたちを「感染している人」と「感染していない人」に分けて心の健康にまで影響してきているよ。心も体もコロナに負けちゃいけない。そして、ぼくたち自らが「分断」しちゃいけない。こんなときだからこそネットのコミュニケーションツールを良いほうに使おうよ。心を通わせたメッセージを発信しよう。みんなが、力を合わせられるように。

i 東京都:東京都総務局人権部 じんけんのとびら https://www.soumu.metro.tokyo.lg.jp/10jinken/〔2021/6/16 確認〕

2.8 その他の情報セキュリティ動向

営業秘密保護の動向、暗号技術の動向、及び情報セキュリティ市場の規模と成長の動向について述べる。

2.8.1 営業秘密保護の動向

企業の技術情報や顧客情報等、営業秘密の活用は企業の競争力の強化に重要な役割を果たす一方、ひとたび営業秘密が漏えいすると、事業に深刻な影響を及ぼすことから、その保護は喫緊の課題である。

営業秘密の保護については、業務のデジタル化を背景としたビッグデータの利活用や AI 等の解析技術の進展等を踏まえ、政府による環境整備が進められている。

法整備の面では、不正競争防止法※508 第五条の二（推定規定）の「技術上の秘密」として「情報の評価又は分析の方法」を対象とし、「技術上の秘密を使用したことが明らかな行為」として「情報の評価又は分析の方法を使用して評価し、又は分析する役務の提供」を対象とすること等を規定した不正競争防止法施行令が 2018 年 11 月に施行された※509。また、2019 年 7 月には「限定提供データ」の不正取得等を不正競争行為として追加した規定も施行された※510。

更に、クラウド等、情報の管理形態の多様化等を踏まえた営業秘密管理指針の改訂※511 も 2019 年 1 月に行われている。

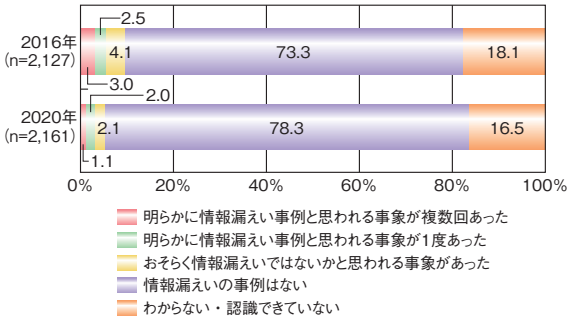
企業もこれらの動きに合わせ、営業秘密の保護に向けた情報セキュリティ対策等を強化していく必要がある。こうした状況を踏まえ、IPA は 2020 年度、「企業における営業秘密管理に関する実態調査 2020」を実施した※512。本調査では、2016 年に行った同一目的の調査※513（以下、前回調査）以降の情報漏えい発生状況、管理実態や対策の変化、法改正の影響等を企業アンケートやインタビューにより確認したほか、文献・裁判例の最新動向を調査した。その調査結果から、いくつかのポイントを紹介する。

(1) 営業秘密情報漏えいの実態

営業秘密情報の漏えいの実態としてインシデント発生状況とその原因について述べる。

(a) 情報漏えいインシデント発生状況

「明らかに情報漏えいと思われる事象が 1 回以上発生した」と回答した割合は 3.1% で、前回調査時の 5.5% より減少したが、この要因としては企業の対策が実際に進展した効果のほか、攻撃の巧妙化により事象そのものを認知しにくくなっている可能性等、複数の要因が作用しての結果と考えられる。また、「情報漏えいの事例はない」の割合が 78.3% で、前回の 73.3% から増加しており、情報漏えいの監視・検知は課題となっている（図 2-8-1）。



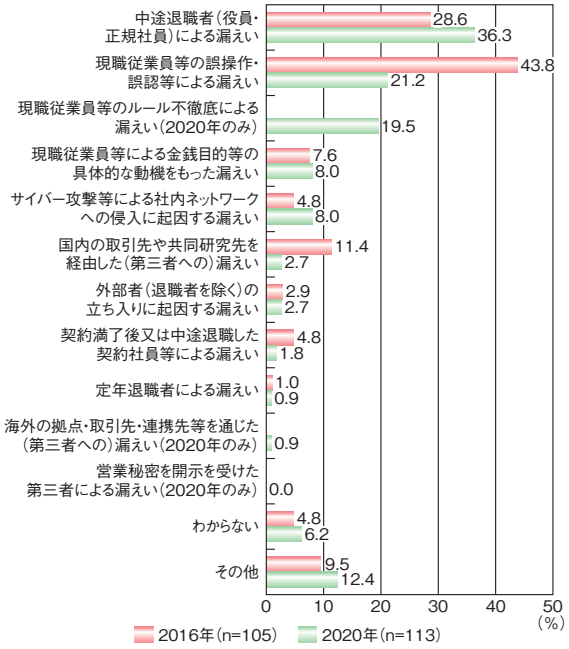
■図 2-8-1　営業秘密漏えいの発生状況（複数選択）
（出典）IPA「企業における営業秘密管理の実態調査 2020」を基に作成

(b) 秘密保持契約締結状況・情報漏えいの原因等

情報漏えいがあったと回答した企業の中で、役員を対象に秘密保持契約を締結している企業は前回調査の 36.3% から 44.6% へ増加した。また、従業員を対象に秘密保持契約を締結している企業も 46.1% から 56.6% へと増加した。ただし、秘密保持契約を締結していない企業のうち、「特に理由はない」と回答した比率が 37.4% とかなり高く、今後の改善の余地があることがうかがえる。

情報漏えいがあった場合の原因については、「誤操作、誤認等」が 21.2% と前回調査時と比べて約半減した一方、「中途退職者」が前回調査時より増加し、36.3% と項目の中で最多となった（次ページ図 2-8-2）。中途退職者による情報漏えいは技術的に防ぐことが難しく、状況の改善が容易ではないことがうかがえる。

情報漏えいが判明した場合に実施したアクションは、「行為者（と疑われる者）に対するヒアリング」や「ログ等の確認」の割合がそれぞれ 50.5%、43.2% と高かったものの、デジタルフォレンジック調査まで踏み込んで実施した比率は 10% に満たなかった。従業員 300 名以下の製造業では、「何をすべきかわからなかったので何もしなかった」割合が 17.2% と突出して高かった。



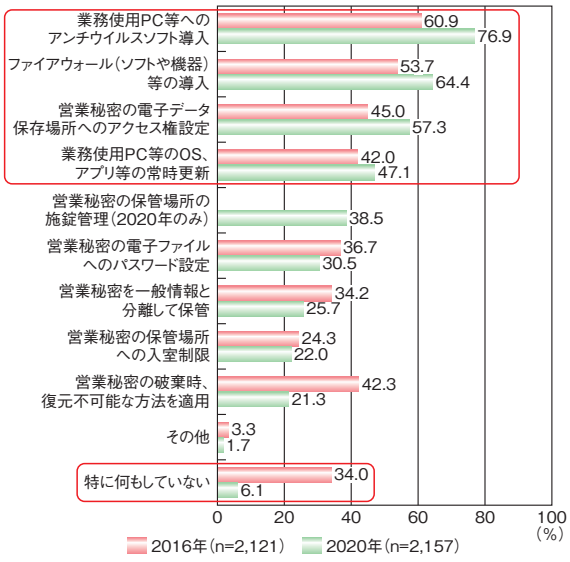
■図 2-8-2　営業秘密の漏えい原因
（出典）IPA「企業における営業秘密管理の実態調査 2020」を基に作成

(2) 漏えい対策・情報管理状況

営業秘密情報の漏えい対策や、情報管理状況のポイントについて述べる。

(a) 不正アクセスの防止対策状況

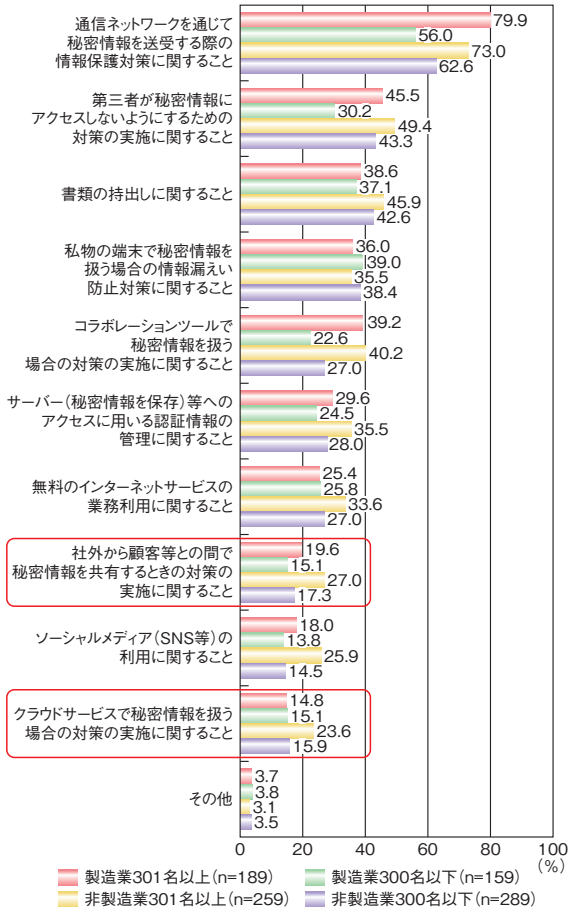
営業秘密情報への不正なアクセスの防止対策としては、「特に何もしていない」割合は 6.1% で、前回調査時の 34.0% と比較して大幅減となった。また、アンチウイルスソフト導入やファイアウォール等の導入、アクセス権の設定等、基礎的な対策の伸びが見られた（図 2-8-3）。



■図 2-8-3　営業秘密情報への不正なアクセスを防ぐための対策の実施状況
（出典）IPA「企業における営業秘密管理の実態調査 2020」を基に作成

(b) テレワーク（在宅勤務等）における管理規定の状況

テレワーク等に関して何らかの情報管理ルール等を整備している、と回答した企業に具体的な内容を尋ねた結果、「秘密情報を社外から取引先と共有する際のルール」や「クラウドサービスで扱う場合のルール」を取り決めている割合が低い（回答企業の各カテゴリーで 30% 未満）ことが分かった（図 2-8-4）。



■図 2-8-4　テレワークで営業秘密を扱う場合に規定したルール（企業規模・業種別）
（出典）IPA「企業における営業秘密管理の実態調査 2020」を基に作成

(3) 営業秘密管理の傾向と課題のまとめ

インタビューを含む調査結果を踏まえ、2020 年度調査による営業秘密保護状況の傾向と課題をまとめる。

- 情報漏えいインシデントの発生は減少したものの、攻撃側の手口の巧妙化等の複数の要因が作用し、減少したように見えている可能性もある。また、テレワーク・クラウド利用等の増加により、組織内に情報を保管して業務を行うよりも漏えい経路が増えていることに注意しなければならない。
- 企業の情報持ち出し規則の整備や普及啓発等により、従業員のミスによる漏えい割合は減少し、漏えい

原因の多くが中途退職者であった。この結果、内部不正による漏えいの割合は相対的に増加した。ますます進展すると想定される雇用の流動化に備え、中途退職者の不正防止対策を強化することが必要である。

- 漏えいが判明したときの対応として、ログの確認等は既に広く実施されているが、情報の廃棄状況の確認や漏えい時の証跡確保で重要となるデジタルフォレンジック調査等は、実施に困難が伴うこともあってまだ浸透していない。
- 基本的な対策として、従業員と秘密保持契約を締結する企業は増えた。不正アクセス防止についても、アクセス権設定等の基本的な対策を中心に進んだ。一方で、対策を従業員に周知していない企業が増加しており、心理的な抑止効果・啓発の観点からは周知が望まれる。
- テレワークの急速な普及により、これまで想定されていなかった環境下で営業秘密を扱う体制やルールの整備が求められており、特にテレワーク環境での他社との情報共有ルールやクラウドサービスでの秘密情報の扱い等について、体制やルールの整備を含む対策が求められている。

情報管理に従事する情報システムや知的財産管理の担当者は、これらの調査結果を自組織の状況と比較し、規程の整備や漏えい対策の強化等の活動の一助としていただきたい。

2.8.2 暗号技術の動向

本項では2020年度における、共通鍵暗号、公開鍵暗号、軽量暗号及び実装攻撃に関する研究及び標準化の動向についてそれぞれ解説する。

(1) 共通鍵暗号に関する研究動向

共通鍵暗号技術に対する攻撃としては、既存の暗号アルゴリズムへの攻撃について、攻撃に必要な計算量の削減等の進展があった。ここでは主な発表を紹介する。

差分攻撃[※514]の拡張であるBoomerang Attackの改良版が発表され[※515]、ラウンド数5のAES[※516]に適用した結果は計算量が$2^{16.5}$(すなわち、全鍵復元において9万回の暗号化と復号の操作しか要求しない)にまで改良した。AESに対する攻撃は2020年度も進展は見られたが、安全性マージンはまだあり、AESの安全性に直ちに影響を与えるものではない。

その他の暗号については、ARX(Addition, Rotation, and XOR)ベースの暗号に対する差分線形解析[※517]の改良が発表された[※518]。ストリーム暗号の一種であるChaCha[※519]がこのタイプに属する。ラウンド数6のChaChaでは時間計算量が$2^{77.4}$、データ計算量が2^{58}、ラウンド数7のChaChaでは時間計算量が$2^{230.86}$、データ計算量が$2^{48.83}$という結果になっており、これまでの記録を上回っているが、ChaCha20のラウンド数20にはまだ安全性マージンがあり、早急な対策が必要となるものではない。

(2) 公開鍵暗号に関する研究及び標準化の動向

公開鍵暗号に関しては、Crypto 2020においてフランス・リモージュ大学のFabrice Boudotらにより、795ビットの素因数分解(RSA-240)及び離散対数計算(DLP-240)に対する新記録が報告され[※520]、前者は約1,000コア年、後者は約3,200コア年の計算量であった。これまでの記録はいずれも768ビット(2009年のRSA-768と2016年の768ビット離散対数)であったが、例えば離散対数の関係探索においては前回時間よりも25%少ない時間で済む等、両計算においてかなりの高速化が実現された。また離散対数計算の素因数分解に対する計算量比率も約3倍と、これまで考えられていた程差があるわけではないことが判明した。更に、別の記録となるRSA-250に対する素因数分解の結果も報告され、本分野において多大な貢献があり、2020年に亡くなったPeter L. Montgomery氏に捧げられた。

NISTによる、量子コンピュータに耐性を持つ暗号「耐量子計算機暗号(PQC:Post-Quantum Cryptography)」の標準化は、2020年7月22日に候補を26件から15件に絞って第3ラウンドに入り、七つの最終候補(Finalist)及び八つの代替候補(Alternate)の評価が進められている。第3ラウンド候補数及び暗号名を表2-8-1(次ページ)に示す。2021年1月22日、PQC Forumメーリングリストにおいて、NISTは「最近の暗号解析が多変数署名Rainbow及びGeMSSに影響を与えたため、セキュリティ及びアプリケーションの観点から多様性欠如の懸念を持っている」旨のメールを投稿した。更にNISTは、第2ラウンド時のレポートから、SPHINCS+が第3ラウンドの終わりの時点で標準のアルゴリズムになる可能性について言及した部分、及び標準化プロセスにないスキームを採用する可能性について言及した部分を議論のスタートポイントとして提示し、意見を募った。今後の予断を許さない状況となり、第3回標

準化会議を2021年6月7～9日に開催する予定で論文募集が行われた（投稿締切り：4月23日、採録通知：5月7日）。

(3) 軽量暗号に関する標準化の動向

NISTのLightweight Cryptographyプロジェクトにおいて、軽量暗号の標準化が行われており、応募された57のアルゴリズムから32のアルゴリズムが残っていたが、2021年3月末にファイナリストとして、10のアルゴリズム（ASCON、Elephant、GIFT-COFB、Grain128-AEAD、ISAP、Photon-Beetle、Romulus、Sparkle、TinyJambu、Xoodyak）が選出された※522。

今後約1年かけて標準化するアルゴリズムが選出される予定である。

(4) 実装攻撃に関する研究動向

暗号実装に対する攻撃には、消費電力や処理時間等のサイドチャネル情報から暗号鍵等の秘密情報の復元を試みるサイドチャネル攻撃や、ICチップに一時的な誤動作を起こさせることによって暗号鍵等の秘密情報の暴露を試みる故障利用攻撃等が存在する。

具体的な暗号実装に対する攻撃として、ECDSA※523の実装に対するタイミング攻撃が発表された※524。この論文では、発表時において、数個のソフトウェア暗号ライブラリとハードウェア実装に対してこの攻撃が有効であることを示している。ECDSA署名の計算時に使用するnonce※525のビット長が、処理時間の差という形で漏えいする場合、数千個の署名生成の電力波形から秘密鍵が復元される可能性がある。この脆弱性に関するCVE※526も発行されている。この結果は、ECDSAを実装するにあたって、nonceの扱いに注意が必要であることを示している。別の種類の楕円曲線を使用する署名アルゴリズムであるEdDSAは、nonceの生成方法に違いがあることからこの攻撃に対しては耐性がある。

その他、具体的な実装に対する攻撃として、ECDSAとRSAの実装に対する、暗号演算に含まれるbinary GCDアルゴリズム※527のサイドチャネル攻撃に関する脆弱性の発表※528、楕円曲線演算における点の射影座標表現でのZ座標のリークを利用した攻撃の発表※529もあり、暗号演算の様々な箇所に対する実装攻撃が研究されている。

2.8.3 情報セキュリティ市場の動向

JNSAが発表した「2020年度 国内情報セキュリティ市場調査報告書※530」によると、2020年度の情報セキュリティ市場規模（ツールとサービスを合わせた数値）は、2019年度より3.5%の伸びとなる見込みである。

情報セキュリティのツールとサービスそれぞれの市場規模の推移を図2-8-5と図2-8-6（次ページ）に、調査市場区分を表2-8-2（次ページ）に示す。図中の2018年度、2019年度については売上高推定実績値で、2020年度については売上高推定見込値、2021年度については売上高予測値である。

情報セキュリティツールの市場規模全体では、2019年度に比べ2020年度は3.3%伸びている。ツールの区分別に見ても、「エンドポイント保護管理製品」の2019年度比9.5%増、「ネットワーク防御・検知／境界線防御製品」の2019年度比2.1%増等、すべての区分で増加傾向が続いている。

情報セキュリティサービスの市場規模全体では、2019年度に比べ2020年度は3.9%伸びている。サービスの区分別に見ても、「コンサルティング／診断サービス」の2019年度比3.7%増、「マネージド・運用サービス」の

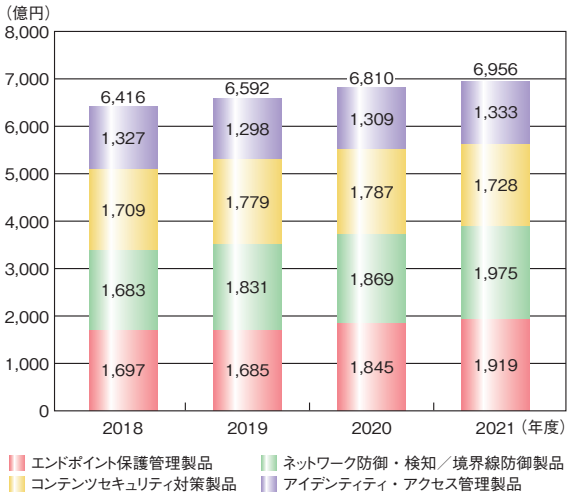
	電子署名		鍵カプセル化機構／暗号化		合計
	暗号名	候補数	暗号名	候補数	
格子ベース	Crystals-Dilithium (F), Falcon (F)	2	Crystals-Kyber (F), FrodoKEM (A), NTRU (F), NTRU Prime (A), Saber (F)	5	7
符号ベース	—	0	ClassicMcEliece (F), BIKE (A), HQC (A)	3	3
多変数	Rainbow (F), GeMSS (A)	2	—	0	2
ハッシュベース	SPHINCS+ (A), Picnic (A)	2	—	0	2
その他	—	0	SIKE (A)	1	1
合計	6 (F:3, A:3)		9 (F:4, A:5)		15

F：Finalist（最終候補）、A：Alternate（代替候補）

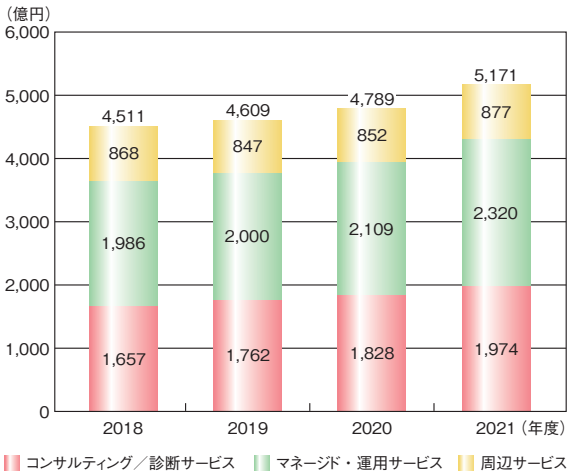
■表2-8-1 NIST PQCコンペティション応募暗号数及び暗号名（第3ラウンド）
（出典）Dustin Moody（NIST）「NIST PQC Standardization Update – Round 2 and Beyond※521」を基にIPAが編集

2019 年度比 5.5% 増等、すべての区分で増加傾向が続いている。

以上のように、情報セキュリティ市場の規模は拡大傾向が続いている。2020 年度は新型コロナウイルスにより経済活動には大きな影響があったが、テレワークやオンライン会議等の普及や DX の推進、クラウドサービスの利用拡大に伴い、これらに対するサイバー攻撃へのセキュリティ対策等が促進されたと考えられる。2020 年度以降においても引き続き国内情報セキュリティ市場は堅調に推移することが予測される。



■図 2-8-5　国内情報セキュリティツール市場規模の推移
（出典）JNSA「2020 年度 国内情報セキュリティ市場調査報告書」を基に IPA が編集



■図 2-8-6　国内情報セキュリティサービス市場規模の推移
（出典）JNSA「2020 年度 国内情報セキュリティ市場調査報告書」を基に IPA が編集

大分類	中分類	小分類
情報セキュリティツール	エンドポイント保護管理製品	ウイルス対策、EDR、ポリシー管理・設定管理・動作監視制御製品
	ネットワーク防御・検知／境界線防御製品	FW、VPN 接続、IDS ／ IPS、WAF、UTM、セキュリティ情報管理システム、物理セキュリティシステム
	コンテンツセキュリティ対策製品	DLP（情報漏えい対策）、DRM、暗号化、メール・セキュリティ対策、URL フィルタリング、脆弱性検査
	アイデンティティ・アクセス管理製品	個人認証用デバイス及びその認証システム、個人認証用生体認証デバイス及びその認証システム、アイデンティティ（ID）管理、ログオン管理／アクセス許可、PKI システム及びそのコンポーネント
情報セキュリティサービス	コンサルティング／診断サービス	コンサルティング、監査・評価、診断、規格認証
	マネージド・運用サービス	SOC、インシデント対応・フォレンジック、インテリジェンス情報提供
	周辺サービス	電子証明書発行・PK 型認証、リテラシー教育、資格取得支援、保険

■表 2-8-2　情報セキュリティツール・サービスの調査市場区分
（出典）JNSA「2020 年度 国内情報セキュリティ市場調査報告書」を基に IPA が編集

※1　政府機関等の情報セキュリティ対策のための統一基準群：国の行政機関及び独立行政法人等の情報セキュリティ水準を向上させるための統一的な枠組みを指す。国の行政機関及び独立行政法人等の情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項を規定している。
NISC：「政府機関等の情報セキュリティ対策のための統一基準群（平成30年度版）」について　https://www.nisc.go.jp/active/general/kijun30.html〔2021/5/31 確認〕
※2　首相官邸：サイバーセキュリティ戦略本部について　https://www.kantei.go.jp/jp/tyoukanpress/202102/10_a.html〔2021/5/31 確認〕
NISC：次期サイバーセキュリティ戦略の検討について　https://www.nisc.go.jp/conference/cs/dai26/pdf/26shiryou01.pdf〔2021/5/31 確認〕
※3　NISC：次期サイバーセキュリティ戦略の骨子について　https://www.nisc.go.jp/conference/cs/dai28/pdf/28shiryou01.pdf〔2021/5/31 確認〕
※4　NISC：サイバーセキュリティ2020　https://www.nisc.go.jp/active/kihon/pdf/cs2020.pdf〔2021/5/31 確認〕
※5　NEDO：戦略的イノベーション創造プログラム（SIP）第2期／IoT社会に対応したサイバー・フィジカル・セキュリティ　https://www.nedo.go.jp/activities/ZZJP2_100123.html〔2021/5/31 確認〕
※6　NEDO：「SIP『IoT社会に対応したサイバー・フィジカル・セキュリティ』ONLINEシンポジウム2020」の開催　https://www.nedo.go.jp/events/IT_100060.html〔2021/5/31 確認〕
※7　https://www.soumu.go.jp/main_content/000750257.pdf〔2021/5/31 確認〕
※8　https://www.soumu.go.jp/main_content/000711459.pdf〔2021/5/31 確認〕
※9　NISC：サイバーセキュリティ対策推進会議（CISO等連絡会議）https://www.nisc.go.jp/conference/cs/taisaku/index.html〔2021/5/31 確認〕
※10 https://www.nisc.go.jp/active/general/pdf/itakusaki_moshiawase.pdf〔2021/5/31 確認〕
※11 https://www.nisc.go.jp/active/general/pdf/choutatsu_moshiawase_kaisei.pdf〔2021/5/31 確認〕
※12 外務省：国連安保理アリア・フォーミュラ会合（サイバー空間の安定化，紛争予防，能力構築）　https://www.mofa.go.jp/mofaj/fp/cp/page24_001098.html〔2021/5/31 確認〕
※13 外務省：サイバーセキュリティに関する国連オープン・エンド作業部会最終会合における報告書の採択　https://www.mofa.go.jp/mofaj/press/release/press3_000453.html〔2021/5/31 確認〕
※14 NISC：第13回　日・ASEANサイバーセキュリティ政策会議の結果　https://www.nisc.go.jp/press/pdf/aseanj_meeting20201106.pdf〔2021/5/31 確認〕
※15 NISC：国際サイバーセキュリティワークショップ・演習の開催　https://www.nisc.go.jp/active/kokusai/pdf/international_ws_ttx_20210305.pdf〔2021/5/31 確認〕
※16 NISC：サイバーセキュリティウェビナー「Control Cybersecurity Risk」の開催　https://www.nisc.go.jp/active/kokusai/pdf/seminar_thai_20210226.pdf〔2021/5/31 確認〕
※17 NISC：サイバーセキュリティウェビナー「Control Cybersecurity Risk」の開催（インドネシア）　https://www.nisc.go.jp/active/kokusai/pdf/seminar_indonesia_20210329.pdf〔2021/5/31 確認〕
※18 https://www.nisc.go.jp/conference/cs/kenkyu/wg/dai09/pdf/kenkyuwg-saishu.pdf〔2021/5/31 確認〕
※19 NISC：サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ 報告書 ～「戦略マネジメント層」の育成・定着に向けて～ https://www.nisc.go.jp/conference/cs/pdf/jinzai-sesaku2018set.pdf〔2021/5/31 確認〕
※20 https://www.nisc.go.jp/security-site/month/event/nisc-cs-seminar.html〔2021/5/31 確認〕
※21 https://cyder.nict.go.jp/index.html〔2021/5/31 確認〕
※22 NICT：2020年度 実践的サイバー防御演習「CYDER」の受講申込受付を開始　https://www.nict.go.jp/press/2020/07/01-3.html〔2021/5/31 確認〕
※23 NISC：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　https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf〔2021/5/31 確認〕
※24 NISC：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　https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r2.pdf〔2021/5/31 確認〕
※25 NISC：次期重要インフラ行動計画の検討について　https://www.nisc.go.jp/conference/cs/dai26/pdf/26shiryou06.pdf〔2021/5/31 確認〕
※26 NISC：重要インフラ専門調査会　https://www.nisc.go.jp/conference/cs/ciip/index.html〔2021/5/31 確認〕
※27 NISC：2020年度分野横断的演習について　https://www.nisc.go.jp/conference/cs/ciip/dai24/pdf/24shiryou04.pdf〔2021/5/31 確認〕
※28 日経クロステック：NCA初の「オンライン」サイバー攻撃演習、静寂の中で得た収穫と課題　https://xtech.nikkei.com/atcl/nxt/column/18/00001/04986/〔2021/5/31 確認〕
※29 金融庁：「金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅴ）」について　https://www.fsa.go.jp/news/r2/20201013.html〔2021/5/31 確認〕
※30 首相官邸：令和2年9月16日菅内閣総理大臣記者会見　https://www.kantei.go.jp/jp/99_suga/statement/2020/0916kaiken.html〔2021/5/31 確認〕
※31 日経クロステック：菅新政権の「デジタル庁」構想、焦点は人事権と内製化に　https://xtech.nikkei.com/atcl/nxt/column/18/01426/091700003/〔2021/5/31 確認〕
※32 首相官邸：デジタル・ガバメント閣僚会議　https://www.kantei.go.jp/jp/singi/it2/egov/〔2021/5/31 確認〕
※33 https://www.kantei.go.jp/jp/singi/it2/dgov/201225/siryou1.pdf〔2021/5/31 確認〕
※34 内閣官房：デジタル改革関連法案について　https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/dejigaba/dai14/siryou1.pdf〔2021/5/31 確認〕
※35 デジタル庁：https://www.digital.go.jp〔2021/5/31 確認〕
※36 デジタル庁：デジタル庁は「行政の透明化」を掲げ、noteでの発信を始めます。　https://note.digital.go.jp/n/n3690482b9676〔2021/5/31 確認〕
※37 経済産業省：産業サイバーセキュリティ研究会　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/〔2021/5/26 確認〕
※38 経済産業省：産業分野におけるサイバーセキュリティ政策　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/001_05_00.pdf〔2021/5/26 確認〕
※39 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20200417.pdf〔2021/5/26 確認〕
※40 経済産業省：産業サイバーセキュリティ強化へ向けたアクションプラン　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/002_03_00.pdf〔2021/5/26 確認〕
※41 経済産業省：第5回 産業サイバーセキュリティ研究会 事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/005_03_00.pdf〔2021/5/26 確認〕
※42 CPSFの詳細に関しては、「情報セキュリティ白書2020」の「2.1.2(1)(a)WG1（制度・技術・標準化）」(p.69)を参照。
※43 経済産業省：ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第1版　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/20190617_report.html〔2021/5/26 確認〕
※44 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/20210222_1.pdf〔2021/5/26 確認〕
※45 https://www.jama.or.jp/it/cyb_sec/download/cyb_sec_guideline_V01_00.pdf〔2021/5/26 確認〕
※46 https://www.meti.go.jp/press/2021/04/20210401005/20210401005-1.pdf〔2021/5/26 確認〕
※47 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/dainiso/pdf/004_03_00.pdf〔2021/5/26 確認〕
※48 経済産業省：IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）を策定しました　https://www.meti.go.jp/press/2020/11/20201105003/20201105003.html〔2021/5/26 確認〕
※49 経済産業省：『第3層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/daisanso/pdf/003_03_00.pdf〔2021/5/26 確認〕
※50 Software Bill of Material（SBOM）：ソフト部品構成表、ソフトウェア部品表等と呼ばれる、様々なソフトウェア部品の名称とそのライセンス等で構成される一覧表。米国商務省電気通信情報局（NTIA：National Telecommunications and Information Administration）が設立した「Software Component Transparency」において2018年から議論されている。
※51 経済産業省：サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/004_03_00.pdf〔2021/5/26 確認〕

※ 52 https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf〔2021/5/26 確認〕
※ 53 IPA：中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊）の報告書について https://www.ipa.go.jp/security/fy2019/reports/sme/otasuketai_houkoku.html〔2021/5/26 確認〕
※ 54 IPA：サイバーセキュリティお助け隊（令和２年度中小企業向けサイバーセキュリティ対策支援体制構築事業）https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index2020.html〔2021/5/26 確認〕
※ 55 IPA：サイバーセキュリティお助け隊サービス　https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html〔2021/5/26 確認〕
※ 56 経済産業省：昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性についての報告書を取りまとめました https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html〔2021/5/26 確認〕
※ 57 https://www.meti.go.jp/policy/netsecurity/downloadfiles/tebiki.pdf〔2021/5/26 確認〕
※ 58 経済産業省：「サイバーセキュリティ体制構築・人材確保の手引き」（第 1.1 版）を取りまとめました　https://www.meti.go.jp/press/2021/04/20210426002/20210426002.html〔2021/5/26 確認〕
※ 59 経済産業省：事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/006_03_00.pdf〔2021/5/26 確認〕
経済産業省：事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/007_03_00.pdf〔2021/5/26 確認〕
※ 60 経済産業省：事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/pdf/006_03_00.pdf〔2021/5/26 確認〕
※ 61 https://www.ipa.go.jp/files/000081564.pdf〔2021/5/26 確認〕
※ 62 IPA：2020 年度 セキュリティ製品の有効性検証の試行について　https://www.ipa.go.jp/security/economics/shikoukekka2021.html〔2021/5/26 確認〕
※ 63 経済産業省：機器のサイバーセキュリティ確保のためのセキュリティ検証の手引きを取りまとめました　https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html〔2021/5/26 確認〕
※ 64 IPA：コラボレーション・プラットフォームについて　https://www.ipa.go.jp/security/announce/collapla_index.html〔2021/5/26 確認〕
※ 65 https://www.meti.go.jp/press/2020/03/20210301004/20210301004-1.pdf〔2021/5/26 確認〕
※ 66 https://www.meti.go.jp/press/2020/09/20200930006/20200930006-2.pdf〔2021/5/26 確認〕
※ 67 https://www.meti.go.jp/shingikai/mono_info_service/dgs5/pdf/20201109_01.pdf〔2021/5/26 確認〕
※ 68 IPA：DX 認定制度　Web 申請受付開始のご案内　https://www.ipa.go.jp/ikc/info/dxcp.html〔2021/5/26 確認〕
※ 69 https://www.meti.go.jp/press/2020/08/20200828012/20200828012-1.pdf〔2021/5/26 確認〕
※ 70 IPA：「情報システム・モデル取引・契約書」第二版を公開 https://www.ipa.go.jp/ikc/reports/20201222.html〔2021/5/26 確認〕
※ 71 IPA：セキュリティ仕様策定プロセス　https://www.ipa.go.jp/files/000087454.docx〔2021/5/26 確認〕
IPA：情報システム開発契約のセキュリティ仕様作成のためのガイドライン ～ Windows Active Directory 編～　https://www.ipa.go.jp/files/000087453.docx〔2021/5/26 確認〕
※ 72 経済産業省：重要技術マネジメント　https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html〔2021/5/26 確認〕
※ 73 株式会社三菱総合研究所：「技術等情報管理認証制度に係る指導支援等の専門家派遣及び調査・広報事業」（経済産業省事業）において専門家の派遣を希望する事業者・団体の公募のご案内について https://www.mri.co.jp/news/public_offering/20201008.html〔2021/5/26 確認〕
※ 74 経済産業省：情報セキュリティサービス審査登録制度　https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html〔2021/5/20 確認〕
※ 75 審査登録機関：「情報セキュリティサービスに関する審査登録機関基準」に適合するとIPAが確認した機関。なお、申請事業者が「情報セキュリティサービス基準」に適合するか否かの審査・判定は、各審査登録機関がその責任において実施する。
※ 76 IPA：情報セキュリティサービス基準適合サービスリストの公開 https://www.ipa.go.jp/security/it-service/service_list.html〔2021/5/20 確認〕
※ 77 NISC：政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）　https://www.nisc.go.jp/active/general/pdf/guide30.pdf〔2021/5/20 確認〕
※ 78 SIG（Special Interest Group）：「特定の分野（各業界におけるサイバー攻撃に関する情報）について、情報を交換するグループ」という意味で、J-CSIP では各業界の参加組織の集合体を SIG と呼んでいる。
※ 79 https://www.ipa.go.jp/files/000090633.pdf〔2021/5/26 確認〕
※ 80 「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。
※ 81 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2020 年 7 月～ 9 月］　https://www.ipa.go.jp/files/000086549.pdf〔2021/5/26 確認〕
※ 82 IPA：サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））https://www.ipa.go.jp/security/J-CSIP/〔2021/5/26 確認〕
※事例については、上記 Web ページの「公開レポート」を参照。
※ 83 IPA：サイバーレスキュー隊 J-CRAT（ジェイ・クラート）　https://www.ipa.go.jp/security/J-CRAT/index.html〔2021/5/26 確認〕
IPA：J-CRAT ／標的型サイバー攻撃特別相談窓口　https://www.ipa.go.jp/security/tokubetsu/index.html〔2021/5/26 確認〕
※ 84 総務省：サイバーセキュリティタスクフォースの開催　https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000116.html〔2021/5/20 確認〕
※ 85 https://www.soumu.go.jp/main_content/000641510.pdf〔2021/5/20 確認〕
※ 86 https://www.soumu.go.jp/main_content/000698567.pdf〔2021/5/20 確認〕
※ 87 ITmedia NEWS：Microsoft のクラウドサービス、新型コロナ外出禁止地域での利用が 775％増　https://www.itmedia.co.jp/news/articles/2003/30/news075.html〔2021/5/20 確認〕
※ 88 https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf〔2021/5/20 確認〕
※ 89 総務省：「政府情報システムのためのセキュリティ評価制度（ISMAP）」の運用開始　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00071.html〔2021/5/20 確認〕
※ 90 https://www.soumu.go.jp/main_content/000722477.pdf〔2021/5/20 確認〕
※ 91 https://notice.go.jp/〔2021/5/20 確認〕
※ 92 総務省：サイバー攻撃に悪用されるおそれのある IoT 機器の調査（NOTICE）の取り組み強化　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00079.html〔2021/5/20 確認〕
※ 93 NICT：NICTER 観測レポート 2020 の公開　https://www.nict.go.jp/press/2021/02/16-1.html〔2021/5/20 確認〕
※ 94 MEC（Multi-access Edge Computing）：端末により近い場所にサーバを分散配置して処理するアーキテクチャ。
※ 95 一般社団法人 ICT-ISAC：5G セキュリティ推進グループの立ち上げについて　https://www.ict-isac.jp/news/news20200219.html〔2021/5/20 確認〕
※ 96 ローカル 5G：通信事業者ではない企業や自治体が、自らの建物内や敷地内でスポット的に柔軟に構築できる 5G システムのこと。
※ 97 参議院：議案情報　https://www.sangiin.go.jp/japanese/joho1/kousei/gian/201/meisai/m201080201022.htm〔2021/5/20 確認〕
※ 98 https://www.soumu.go.jp/main_content/000722596.pdf〔2021/5/20 確認〕
※ 99 NICT：量子コンピュータ実機を用いた離散対数問題の求解実験に成功　https://www.nict.go.jp/press/2020/12/09-1.html〔2021/5/20 確認〕
※ 100 https://www.soumu.go.jp/main_content/000733733.pdf〔2021/5/26 確認〕
※ 101 総務省：第 13 回 日・ASEAN サイバーセキュリティ政策会議の結果　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00083.html〔2021/5/20 確認〕
※ 102 総務省：テレワークの推進　https://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/index.htm〔2021/5/20 確認〕
※ 103 総務省：新型コロナウイルス感染症対策としてのテレワークの積極的な活用について　https://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/02ryutsu02_04000341.html〔2021/5/20 確認〕
※ 104 総務省：「テレワークマネージャー相談事業」について　https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000400.html〔2021/5/20 確認〕
※ 105 総務省：テレワークのセキュリティ安心無料相談窓口　https://www.soumu.go.jp/main_content/000697737.pdf〔2021/5/20 確認〕
※ 106 総務省：「テレワークセキュリティガイドライン（第 5 版）」（案）に対す

る意見募集 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00094.html〔2021/5/20 確認〕
※ 107 https://www.soumu.go.jp/main_content/000706649.pdf〔2021/5/20 確認〕
※ 108 総務省：テレワークセキュリティに関する手引き（チェックリスト）等の公表 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00080.html〔2021/5/20 確認〕
※ 109 設定解説資料は、手引き（チェックリスト）の内容を具体的な環境で実施する際の参考となるよう、テレワークで多く利用される製品を対象として補足的に作成している資料である。
※ 110 総務省：テレワークにおけるセキュリティ確保 https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/〔2021/5/20 確認〕
※ 111 https://www.soumu.go.jp/main_content/000711713.pdf〔2021/5/20 確認〕
※ 112 総務省：テレワークセキュリティに係る実態調査（2次実態調査）報告書 https://www.soumu.go.jp/main_content/000744643.pdf〔2021/5/20 確認〕
※ 113 総務省：「自治体情報セキュリティ対策の見直しについて」の公表 https://www.soumu.go.jp/menu_news/s-news/01gyosei07_02000098.html〔2021/5/20 確認〕
※ 114 https://www.soumu.go.jp/main_content/000727474.pdf〔2021/5/20 確認〕
※ 115 https://www.soumu.go.jp/main_content/000726080.pdf〔2021/5/20 確認〕
※ 116 トラストサービス：タイムスタンプ、eシール、リモート署名、eデリバリー、Webサイト認証等のサービスの総称で、日本が提唱する自由で信頼できるデータ流通（DFFT：Data Free Flow with Trust）の基盤である。トラストサービス検討WGにて各サービスの現状・課題・あるべき制度等の検討を行った。
※ 117 総務省：プラットフォームサービスに関する研究会における最終報告書（案）に対する意見募集の結果及び最終報告書の公表 https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000075.html〔2021/5/20 確認〕
※ 118 総務省：組織が発行するデータの信頼性を確保する制度に関する検討会 https://www.soumu.go.jp/main_sosiki/kenkyu/data_organization/index.html〔2021/5/20 確認〕
※ 119 総務省：タイムスタンプの国による認定制度 https://www.soumu.go.jp/main_content/000742673.pdf〔2021/5/20 確認〕
※ 120 https://www.soumu.go.jp/main_content/000710778.pdf〔2021/5/20 確認〕
※ 121 総務省：インターネット上の違法・有害情報に対する対応（プロバイダ責任制限法） https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/ihoyugai.html〔2021/5/26 確認〕
※ 122 総務省：インターネット上のフェイクニュースや偽情報への対策 https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/ihoyugai_05.html〔2021/5/26 確認〕
※ 123 総務省：インターネット上の誹謗中傷への対策 https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/hiboutyusyou.html〔2021/5/26 確認〕
※ 124 NISC：サイバーセキュリティ戦略 https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf〔2021/5/19 確認〕
※ 125 警察庁：サイバーセキュリティ重点施策の改定について（通達） https://www.npa.go.jp/cybersecurity/pdf/300906_juutensesaku.pdf〔2021/5/19 確認〕
※ 126 警察庁：サイバーセキュリティ戦略の改定について（依命通達） https://www.npa.go.jp/cybersecurity/pdf/300906_senryaku.pdf〔2021/5/19 確認〕
※ 127 警察庁：令和2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/R02_cyber_jousei.pdf〔2021/5/19 確認〕
※ 128 警察庁：治安の回顧と展望（令和2年版） https://www.npa.go.jp/bureau/security/publications/kaiko_to_tenbou/R2/kaitenR2.pdf〔2021/5/19 確認〕
※ 129 滋賀県警察：滋賀大学におけるサイバー攻撃共同対処訓練の実施 https://www.pref.shiga.lg.jp/police/seikatu/304024/terotaisaku/313411.html〔2021/5/19 確認〕
※ 130 日刊警察ニュース：富山県警察と愛知県警察でサイバー攻撃の共同対処訓練を実施 https://nikkankeisatsu.co.jp/news/201210-1.html〔2021/5/19 確認〕
※ 131 青森県警察：サイバーテロ対策担当者向け「共同対処訓練」 https://www.pi.jtua.or.jp/aomori/wp-content/uploads/sites/14/2020/12/8b34e36a9092699cbdaa4a4056090908.pdf〔2021/5/19 確認〕
※ 132 警察庁：情報セキュリティ対策ビデオ https://www.npa.go.jp/cyber/video/index.html〔2021/5/19 確認〕
※ 133 警察庁：スマートフォン決済サービスを利用した不正振替事犯に係る対策について https://www.npa.go.jp/cyber/policy/pdf/210318publicrelations.pdf〔2021/5/19 確認〕
※ 134 宮城県警察：宮城県サイバーセキュリティ協議会 https://www.police.pref.miyagi.jp/hp/cyber/kyougikai.html〔2021/5/19 確認〕
※ 135 警察庁：サイバー空間の脅威への対処に係る人材育成方針の改定について（通達） https://www.npa.go.jp/laws/notification/kanbou/kikaku/2019kikaku-h4.pdf〔2021/5/19 確認〕
※ 136 警察庁：令和2年度予算の概要 https://www.npa.go.jp/policies/budget/r2/r2tousyoyosan2.pdf〔2021/5/19 確認〕
※ 137 警察庁：電磁的記録の解析 https://www.npa.go.jp/joutuu/011.htm〔2021/5/19 確認〕
※ 138 警察庁：国際連携・協力 https://www.npa.go.jp/joutuu/013.htm〔2021/5/19 確認〕
※ 139 総務省・消費者庁・警察庁：給付金のサギ（詐欺）に注意!! https://www.npa.go.jp/bureau/soumu/corona/sagihigaibousi.pdf〔2021/5/19 確認〕
※ 140 山形県警察：山形県警察広報動画「サポート詐欺」にだまされないで!（その1）警告画面に表示された番号に電話をかけると https://www.youtube.com/watch?v=sWftPO_I3r8〔2021/5/19 確認〕
※ 141 サイバーセキュリティ政策会議：生活様式の変化等に伴うサイバー空間の新たな脅威に対処するための官民連携の更なる推進 https://www.npa.go.jp/cybersecurity/pdf/20210308_2.pdf〔2021/5/19 確認〕
※ 142 警察庁では、市販のウイルス対策ソフトでは検知できない不正プログラムを添付して、業務に関連した正当なものであるかのように装った電子メールを送信し、これを受信したコンピュータを不正プログラムに感染させる等して、情報の窃取を図るものを「標的型メール攻撃」として集計している。
※ 143 警察庁：サイバー攻撃に対する技術的対応 https://www.npa.go.jp/joutuu/012.htm〔2021/5/19 確認〕
※ 144 正式名称は「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」（https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r5.pdf〔2021/5/31 確認〕）。現在は、「電子政府推奨暗号リスト」「推奨候補暗号リスト」「運用監視暗号リスト」の三つのリストから構成される。
※ 145 CRYPTREC：2020年度 第2回 暗号技術検討会 資料3別添3 2020年度 暗号技術調査WG（暗号解析評価）活動報告 https://www.cryptrec.go.jp/report/cryptrec-mt-1021-2020.pdf〔2021/5/31 確認〕
※ 146 EdDSA（Edwards-curve Digital Signature Algorithm）：楕円曲線の一種であるエドワーズ曲線を用いたデジタル署名アルゴリズム。
※ 147 Shorの量子アルゴリズム：現代暗号の基盤である素因数分解や離散対数問題等を量子コンピュータによって効率的に解くアルゴリズム。
※ 148 IPA：暗号鍵管理ガイドライン https://www.ipa.go.jp/security/vuln/ckms.html〔2021/5/31 確認〕
※ 149 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〔2021/5/31 確認〕
※ 150 Kyodo：Tokyo Olympics postponed until 2021 due to coronavirus pandemic https://english.kyodonews.net/news/2020/03/529743138975-breaking-news-japan-pm-abe-plans-talks-with-ioc-chief-bach-over-phone-tues-source.html〔2021/5/12 確認〕
※ 151 外務省：G7首脳テレビ会議 https://www.mofa.go.jp/mofaj/ecm/ec/page6_000378.html〔2021/5/12 確認〕
※ 152 外務省：G7外相会合の実施 https://www.mofa.go.jp/mofaj/press/release/press4_008389.html〔2021/5/12 確認〕
※ 153 首相官邸：新型コロナウイルス感染症に関する安倍内閣総理大臣記者会見 https://www.kantei.go.jp/jp/98_abe/statement/2020/0407kaiken.html〔2021/5/12 確認〕
※ 154 外務省：Biarritz Strategy for an Open, Free and Secure Digital Transformation https://www.mofa.go.jp/mofaj/files/000512682.pdf〔2021/5/12 確認〕
※ 155 外務省：第2回日米豪印外相会合 https://www.mofa.go.jp/mofaj/press/release/press6_000682.html〔2021/5/12 確認〕
※ 156 外務省：第23回日・ASEAN首脳会議「インド太平洋に関するASEAN・アウトルック（AOIP）協力についての第23回日アセアン首脳会議共同首脳声明」の発出 https://www.mofa.go.jp/mofaj/a_o/rp/page3_002923.html〔2021/5/12 確認〕
※ 157 外務省：日米豪印外相電話会談 https://www.mofa.go.jp/mofaj/press/release/press3_000427.html〔2021/5/12 確認〕
※ 158 LAWFARE：China's New Coast Guard Law and Implications for Maritime Security in the East and South China Seas https://www.lawfareblog.com/

chinas-new-coast-guard-law-and-implications-maritime-security-east-and-south-china-seas〔2021/5/12 確認〕
※ 159 United Nations: Open-ended working group https://www.un.org/disarmament/open-ended-working-group/〔2021/5/12 確認〕
※ 160 United Nations：Open-ended working group on developments in the field of information and telecommunications in the context of international security Final Substantive Report https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf〔2021/5/12 確認〕
※ 161 外務省：第 5 回日英サイバー協議の開催 https://www.mofa.go.jp/mofaj/press/release/press4_008287.html〔2021/5/12 確認〕
※ 162 外務省：日米安全保障委員会 https://www.mofa.go.jp/mofaj/na/st/page1_000942.html〔2021/5/12 確認〕
※ 163 外務省：日米首脳会談 https://www.mofa.go.jp/mofaj/na/na1/us/page1_000951.html〔2021/5/13 確認〕
※ 164 https://www.mofa.go.jp/mofaj/files/100181507.pdf〔2021/5/13 確認〕
※ 165 外務省：日 EU 首脳テレビ会議の開催 https://www.mofa.go.jp/mofaj/erp/ep/page4_005157.html〔2021/5/12 確認〕
※ 166 https://aseanregionalforum.asean.org/〔2021/5/12 確認〕
※ 167 外務省：サイバーセキュリティに関する ARF 会期間会合のための第 6 回専門家会合の開催（結果） https://www.mofa.go.jp/mofaj/press/release/press3_000409.html〔2021/5/12 確認〕
※ 168 2018 年 12 月、第 73 回国連総会決議（A/RES/73/266）に基づき、国際安全保障の文脈におけるサイバー空間での責任ある国家の行動の進展に関して 25 ヵ国からの専門家（25 名）による専門的な議論の場として、国連のもとに立ち上がった会合。2019 年 12 月に第 1 回会合を開催し、全部で 4 回の本会合を経て 2021 年の国連総会において報告書を提出することとなっている。
※ 169 経済産業省：「インド太平洋地域向け日米産業制御システムサイバーセキュリティウィーク」を実施しました https://www.meti.go.jp/press/2020/03/20210315001/20210315001.html〔2021/5/12 確認〕
※ 170 The MITRE Corporation は 1958 年創立の非営利民間企業で、米国連邦政府機関の出資を受けた研究開発、及び成果の民間移転を推進している。 https://www.mitre.org/〔2021/5/12 確認〕
※ 171 慶應義塾大学：第 10 回サイバーセキュリティ国際シンポジウム https://symp.cysec-lab.keio.ac.jp/2020oct/program-j.html〔2021/5/12 確認〕
※ 172 日本経済新聞／株式会社日経 BP：サイバー・イニシアチブ東京 2020 https://project.nikkeibp.co.jp/event/2020z1124cit/〔2021/5/12 確認〕
※ 173 BBC：Trump declares national emergency over coronavirus https://www.bbc.com/news/world-us-canada-51882381〔2021/5/13 確認〕
※ 174 THE WHITE HOUSE：A Letter on the Continuation of the National Emergency Concerning the Coronavirus Disease 2019 (COVID-19) Pandemic https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/24/a-letter-on-the-continuation-of-the-national-emergency-concerning-the-coronavirus-disease-2019-covid-19-pandemic〔2021/5/13 確認〕
※ 175 AFP：トランプ氏が中国批判、故意ならパンデミックの「報いを受けるべき」 https://www.afpbb.com/articles/-/3279279〔2021/5/13 確認〕
※ 176 AFP：新型コロナ、武漢の研究所が発生源の可能性確信＝トランプ米大統領 https://jp.reuters.com/article/health-coronavirus-usa-idJPKBN22C3ZE〔2021/5/13 確認〕
※ 177 The New York Times：Wuhan, Center of Coronavirus Outbreak, Is Being Cut Off by Chinese Authorities https://www.nytimes.com/2020/01/22/world/asia/china-coronavirus-travel.html〔2021/5/13 確認〕
※ 178 IPA：情報セキュリティ白書 2020 https://www.ipa.go.jp/security/publications/hakusyo/2020.html〔2021/5/13 確認〕
※ 179 THE WHITE HOUSE：Executive Order on America's Supply Chains https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/〔2021/5/13 確認〕
※ 180 時事ドットコム：米、供給網で脱中国依存 日本など同盟国と連携 https://www.jiji.com/jc/article?k=2021022400885&g=int〔2021/5/13 確認〕
※ 181 CISA：CISA INSIGHTS Risk Management for Novel Coronavirus (COVID-19) https://www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf〔2021/5/13 確認〕
※ 182 FBI：Protect Your Wallet—and Your Health—from Pandemic Scammers https://www.fbi.gov/news/stories/protect-yourself-from-covid-19-scams-040620〔2021/5/13 確認〕
※ 183 CISA：Alert (AA20-099A) COVID-19 Exploited by Malicious Cyber Actors https://us-cert.cisa.gov/ncas/alerts/aa20-099a〔2021/5/13 確認〕
※ 184 CISA：Telework Guidance and Resources https://www.cisa.gov/telework〔2021/5/13 確認〕
※ 185 CISA：CISA RELEASES VERSION 3.0 OF GUIDANCE ON ESSENTIAL CRITICAL INFRASTRUCTURE WORKERS DURING COVID-19 https://www.cisa.gov/news/2020/04/17/cisa-releases-version-30-guidance-essential-critical-infrastructure-workers-during〔2021/5/13 確認〕
なお、同ガイダンスは同年 10 月に第 4 版が公開された。
※ 186 CISA&FBI：People's Republic of China (PRC) Targeting of COVID-19 Research Organizations https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf〔2021/5/13 確認〕
※ 187 CISA：Alert (AA20-225A) Malicious Cyber Actor Spoofing COVID-19 Loan Relief Webpage via Phishing Emails https://us-cert.cisa.gov/ncas/alerts/aa20-225a〔2021/5/13 確認〕
※ 188 BUSINESS INSIDER：US accuses Russia of spreading conspiracies about the Wuhan coronavirus, including that it's a CIA biological weapon https://www.businessinsider.com/us-officials-claim-russian-coronavirus-disinformation-campaign-2020-2?r=US&IR=T〔2021/5/13 確認〕
※ 189 WHO：Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation〔2021/5/13 確認〕
※ 190 CISA：COVID 19 DISINFORMATION TOOLKIT https://www.cisa.gov/publication/covid-19-disinformation-toolkit〔2021/5/13 確認〕
※ 191 Military.com：Russia and China Are Spreading Lies About Coronavirus, Pentagon Says https://www.military.com/daily-news/2020/04/10/russia-and-china-are-spreading-lies-about-coronavirus-pentagon-says.html〔2021/5/13 確認〕
※ 192 DoD：CORONAVIRUS:RUMOR CONTROL https://www.defense.gov/explore/spotlight/coronavirus/rumor-control/〔2021/5/13 確認〕
※ 193 Military.com：Navy Debunks Top 10 COVID-19 Vaccine Myths https://www.military.com/daily-news/2021/03/04/navy-debunks-top-10-covid-19-vaccine-myths.html〔2021/5/13 確認〕
※ 194 以下は 2021 年 4 月 2 日の事例である。
POLYGRAPH.info：Coronavirus: The Infodemic - April 2 https://www.polygraph.info/a/31183802.html〔2021/5/13 確認〕
※ 195 Pew Research Center：A Year of U.S. Public Opinion on the Coronavirus Pandemic https://www.pewresearch.org/2021/03/05/a-year-of-u-s-public-opinion-on-the-coronavirus-pandemic/〔2021/5/13 確認〕
※ 196 CISA：CISA RELEASES 5G STRATEGY FOR SECURE AND RESILIENT CRITICAL INFRASTRUCTURE https://www.cisa.gov/news/2020/08/24/cisa-releases-5g-strategy-secure-and-resilient-critical-infrastructure〔2021/5/13 確認〕
※ 197 Bloomberg：Trump Targets Ant's Alipay, WeChat Pay in Latest App Bans https://www.bloomberg.com/news/articles/2021-01-05/trump-order-would-ban-transactions-with-chinese-payment-apps〔2021/5/13 確認〕
※ 198 ZDNet：Trump decrees American cloud providers need to maintain records on foreign clients https://www.zdnet.com/article/trump-decrees-american-cloud-providers-need-to-maintain-records-on-foreign-clients/〔2021/5/13 確認〕
※ 199 CISA：ICT SCRM TASK FORCE: THREAT SCENARIOS REPORT https://www.cisa.gov/publication/ict-scrm-task-force-threat-scenarios-report〔2021/5/13 確認〕
※ 200 COVINGTON：CISA Information and Communications Technology Supply Chain Risk Management Task Force Releases New Guidance on Security Resiliency https://www.globalpolicywatch.com/2020/05/cisa-information-and-communications-technology-supply-chain-risk-management-task-force-releases-new-guidance-on-security-resiliency/〔2021/5/13 確認〕
※ 201 CISA：MITIGATING ICT SUPPLY CHAIN RISKS WITH QUALIFIED BIDDER AND MANUFACTURER LISTS https://

www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Qualified-Bidders-Lists_508.pdf〔2021/5/13 確認〕
※ 202 CISA：ICT SCRM TASK FORCE: LESSONS LEARNED DURING THE COVID-19 PANDEMIC REPORT https://www.cisa.gov/publication/ict-supply-chain-lessons-learned-covid-19〔2021/5/13 確認〕
※ 203 Office of the Under Secretary of Defense for Acquisition & Sustainment：CYBERESECURITY MATURITY MODDEL CERTIFICATION (CMMC) https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf〔2021/5/13 確認〕
※ 204 CMMC-AB：https://cmmcab.org/〔2021/5/13 確認〕
※ 205 OUSD A&S：Cybersecurity Maturity Model Certification Pilots for Fiscal Year 2021 https://www.acq.osd.mil/news/archive/2020/cybersecurity-maturity-model-certification-pilots-for-fiscal-year-2021.html〔2021/5/13 確認〕
※ 206 FEDSCOOP：CMMC is under an internal DOD review https://www.fedscoop.com/dod-cmmc-review-new-administration/〔2021/5/13 確認〕
※ 207 FireEye, Inc.：Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html〔2021/5/13 確認〕
※ 208 cyber.dhc.org：Emergency Directive 21-01 https://cyber.dhs.gov/ed/21-01/#supplemental-guidance-v3〔2021/5/13 確認〕
※ 209 FIREEYE：Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452 https://www.fireeye.com/blog/threat-research/2021/01/remediation-and-hardening-strategies-for-microsoft-365-to-defend-against-unc2452.html〔2021/5/13 確認〕
※ 210 The New York Times：As Understanding of Russian Hacking Grows, So Does Alarm https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html〔2021/5/13 確認〕
※ 211 arstechnica：SolarWinds hack that breached gov networks poses a “grave risk” to the nation https://arstechnica.com/information-technology/2020/12/feds-warn-that-solarwinds-hackers-likely-used-other-ways-to-breach-networks/〔2021/5/13 確認〕
※ 212 ITMediaビジネスオンライン：大手企業が次々と被害に ソーラーウィンズから連鎖した「サプライチェーン攻撃」の脅威 https://www.itmedia.co.jp/business/articles/2012/24/news031_3.html〔2021/5/13 確認〕
※ 213 CISA：JOINT STATEMENT BY THE FEDERAL BUREAU OF INVESTIGATION (FBI), THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), AND THE NATIONAL SECURITY AGENCY (NSA) https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure〔2021/5/13確認〕
※ 214 The White House：FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/〔2021/5/13 確認〕
※ 215 FCW：White House sanctions Russia over SolarWinds campaign, election interference https://fcw.com/articles/2021/04/15/katz-russia-cyber-sanctions.aspx〔2021/5/13 確認〕
※ 216 Microsoft Security Response Center：On-Premises Exchange Server Vulnerabilities Resource Center – updated March 25, 2021 https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/〔2021/5/13 確認〕
※ 217 Microsoft Security Response Center：HAFNIUM targeting Exchange Servers with 0-day exploits https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/〔2021/5/13 確認〕
※ 218 KrebsonSecurity：At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft’s Email Software https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/〔2021/5/13 確認〕
※ 219 CISA：CISA Issues Emergency Directive and Alert on Microsoft Exchange Vulnerabilities https://us-cert.cisa.gov/ncas/current-activity/2021/03/03/cisa-issues-emergency-directive-and-alert-microsoft-exchange〔2021/5/13 確認〕
※ 220 The White House：Statements by Press Secretary Jen Psaki & Deputy National Security Advisor for Cyber Anne Neuberger on Microsoft Exchange Vulnerabilities UCG https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/17/statements-by-press-secretary-jen-psaki-deputy-national-security-advisor-for-cyber-anne-neuberger-on-microsoft-exchange-vulnerabilities-ucg/〔2021/5/13 確認〕
※ 221 The Wall Street Journal：Suspected China Hack of Microsoft Shows Signs of Prior Reconnaissance https://www.wsj.com/articles/suspected-china-hack-of-microsoft-shows-signs-of-prior-reconnaissance-11617800400〔2021/5/13 確認〕
※ 222 ZDNet：Exchange Server attacks: Microsoft shares intelligence on post-compromise activities https://www.zdnet.com/article/exchange-server-attacks-microsoft-shares-intelligence-on-post-compromise-activities/〔2021/5/13 確認〕
※ 223 The New York Times：Cyberattack Forces a Shutdown of a Top U.S. Pipeline https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html〔2021/5/26 確認〕
※ 224 The New York Times：The F.B.I. confirms that DarkSide, a ransomware group, was behind the hack of a major U.S. pipeline. https://www.nytimes.com/2021/05/10/us/politics/dark-side-hack.html〔2021/5/26 確認〕
※ 225 WIRED：DarkSide Ransomware Hit Colonial Pipeline—and Created an Unholy Mess https://www.wired.com/story/darkside-ransomware-colonial-pipeline-response/〔2021/5/26 確認〕
※ 226 CISA：DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks https://us-cert.cisa.gov/ncas/alerts/aa21-131a〔2021/5/26 確認〕
※ 227 Forbes：Colonial Pipeline Restarts Operations As Biden Seeks To Protect Government From Cyber Attacks https://www.forbes.com/sites/edwardsegal/2021/05/12/colonial-pipeline-restarts-operations-as-biden-seeks-to-protect-government-from-cyber-attacks/?sh=17093d217814〔2021/5/26 確認〕
※ 228 The New York Times：Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html〔2021/5/26 確認〕
※ 229 The Wall Street Journal：Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636〔2021/5/26 確認〕
※ 230 The White House：Executive Order on Improving the Nation’s Cybersecurity https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/〔2021/5/26 確認〕
※ 231 The New York Times：Biden Wins Presidency, Ending Four Tumultuous Years Under Trump https://www.nytimes.com/2020/11/07/us/politics/biden-election.html〔2021/5/13 確認〕
※ 232 日本経済新聞：米、政権移行へ本格始動 トランプ氏が引き継ぎ容認 https://www.nikkei.com/article/DGXMZO66600380U0A121C2MM8000/〔2021/5/13 確認〕
※ 233 朝日新聞：トランプ氏側、最高裁で２度目の敗訴 大統領選不正訴訟 https://www.asahi.com/articles/ASNDD5HP6NDDUHBI00K.html〔2021/5/13 確認〕
最終的には 2021 年３月８日の連邦最高裁判決で Wisconsin 州の選挙に関する提訴が却下され、Trump 陣営の完全敗訴が確定した。
Reuters：U.S. Supreme Court dumps last of Trump's election appeals https://www.reuters.com/article/us-usa-court-election-idUSKBN2B01LE〔2021/5/13 確認〕
※ 234 The Washington Post：How one of America’s ugliest days unraveled inside and outside the Capitol https://www.washingtonpost.com/nation/interactive/2021/capitol-insurrection-visual-timeline/?utm_campaign=wp_graphics&utm_medium=social&utm_source=twitter〔2021/5/13 確認〕
※ 235 The New York Times：After Pro-Trump Mob Storms Capitol, Congress Confirms Biden’s Win https://www.nytimes.com/2021/01/06/us/politics/congress-gop-subvert-election.html〔2021/5/13 確認〕
※ 236 REUTERS：Reuters launches fact-checking initiative to identify misinformation, in partnership with Facebook https://www.reuters.com/article/rpb-fbfactchecking/reuters-launches-fact-checking-initiative-to-identify-misinformation-in-partnership-with-facebook-idUSKBN2061TG〔2021/5/13 確認〕
※ 237 REUTERS：Twitter fact-checks Trump tweet for the first

time https://www.reuters.com/article/us-twitter-trump-idUSKBN232389〔2021/5/13 確認〕
※ 238 The New York Times：Twitter Has Labeled 38% of Trump's Tweets Since Tuesday https://www.nytimes.com/2020/11/05/technology/donald-trump-twitter.html〔2021/5/13 確認〕
※ 239 The Washington Post: Twitter bans Trump's account, citing risk of further violence https://www.washingtonpost.com/technology/2021/01/08/twitter-trump-dorsey/〔2021/5/13 確認〕
※ 240 NHK：ツイッター アカウント永久停止の波紋 https://www.nhk.or.jp/ohayou/biz/20210128/index.html〔2021/5/13 確認〕
※ 241 Newsweek:Donald Trump's Twitter Ban Concerns World Leaders, Officials https://www.newsweek.com/donald-trump-twitter-ban-concerns-world-leaders-officials-1560771〔2021/5/13 確認〕
※ 242 WIRED：What happened to the deepfake threat to the US election? https://wired.me/business/what-happened-to-the-deepfake-threat-to-the-us-election/〔2021/5/13 確認〕
※ 243 GovTrack.us：S. 1790 (116th):National Defense Authorization Act for Fiscal Year 2020 https://www.govtrack.us/congress/bills/116/s1790〔2021/5/13 確認〕
※ 244 TechCrunch：Biden's cybersecurity dream team takes shape https://techcrunch.com/2021/04/12/bidens-cybersecurity-dream-team-takes-shape/〔2021/5/13 確認〕
※ 245 BBC：Brexit:UK leaves the European Union https://www.bbc.com/news/uk-politics-51333314〔2021/5/17 確認〕
※ 246 日本経済新聞：英国との FTA 暫定適用、EU 加盟国が承認 大使級会合 https://www.nikkei.com/article/DGXZQODB289LU0Y0A221C2000000/〔2021/5/17 確認〕
※ 247 The EU-UK Trade and Cooperation Agreement：TRADE AND COOPERATION AGREEMENT BETWEEN THE EUROPEAN UNION AND THE EUROPEAN ATOMIC ENERGY COMMUNITY, OF THE ONE PART, AND THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND, OF THE OTHER PART https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948119/EU-UK_Trade_and_Cooperation_Agreement_24.12.2020.pdf〔2021/5/17 確認〕
※ 248 POLITICO：European Parliament ratifies post-Brexit trade deal https://www.politico.eu/article/european-parliament-post-brexit-trade-deal-ratification/〔2021/5/17 確認〕
※ 249 European Council：EU-UK negotiations on the future relationship https://www.consilium.europa.eu/en/policies/eu-uk-negotiations-on-the-future-relationship/#:~:text=Negotiations%20on%20the%20future%20partnership,provisionally%20from%201%20January%202021.〔2021/5/17 確認〕
※ 250 日本経済新聞：英 EU、通商協定で合意 関税ゼロ維持へ https://www.nikkei.com/article/DGXZQOGM00090_09122020000000/〔2021/5/17 確認〕
※ 251 BBC：Brexit trade deal: What does it mean for fishing? https://www.bbc.com/news/46401558〔2021/5/17 確認〕
※ 252 Institute for Government：UK–EU future relationship: level playing field https://www.instituteforgovernment.org.uk/explainers/future-relationship-level-playing-field〔2021/5/17 確認〕
※ 253 JETRO：英国の EU 離脱後の通商・協力協定交渉の争点と進捗状況 https://www.jetro.go.jp/ext_images/world/europe/uk/referendum/brexit_outline_20210104.pdf〔2021/5/17 確認〕
※ 254 The Law Society：Personal data flows from the EU/EEA to the UK after Brexit https://www.lawsociety.org.uk/topics/brexit/eu-data-flows-after-brexit〔2021/5/17 確認〕
※ 255 European Commission：COMMISSION IMPLEMENTING DECISION of XXX pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom https://ec.europa.eu/info/sites/default/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_19_feb_2020.pdf〔2021/5/17 確認〕
※ 256 Data Protection Report：EDPB cautiously welcomes UK adequacy finding https://www.dataprotectionreport.com/2021/04/edpb-cautiously-welcomes-uk-adequacy-finding/〔2021/5/17 確認〕
※ 257 European Data Protection Board：EDPB Opinions on draft UK adequacy decisions https://edpb.europa.eu/news/news/2021/edpb-opinions-draft-uk-adequacy-decisions_en〔2021/5/17 確認〕
※ 258 European Commission：The EU-UK Security of Information Agreement https://ec.europa.eu/info/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement/eu-uk-security-information-agreement_en#:~:text=If%20a%20joint%20security%20threat,EU%20and%20a%20third%20country.〔2021/5/17 確認〕
※ 259 BBC：Coronavirus: Italy extends emergency measures nationwide https://www.bbc.com/news/world-europe-51810673〔2021/5/17 確認〕
※ 260 France24：Macron announces 15-day lockdown in French 'war' on coronavirus https://www.france24.com/en/20200316-live-france-s-macron-addresses-nation-amid-worsening-coronavirus-outbreak〔2021/5/17 確認〕
※ 261 France24：Germany closes public spaces, bans religious gatherings in virus clampdown https://www.france24.com/en/20200316-germany-closes-public-spaces-bans-religious-gatherings-in-virus-clampdown〔2021/5/17 確認〕
※ 262 The Guardian：UK coronavirus: Boris Johnson announces strict lockdown across country – as it happened https://www.theguardian.com/politics/live/2020/mar/23/uk-coronavirus-live-news-latest-boris-johnson-minister-condemns-people-ignoring-two-metre-distance-rule-in-parks-as-very-selfish〔2021/5/17 確認〕
※ 263 GOV.UK：Coronavirus（Covid-19）in the UK https://coronavirus.data.gov.uk/〔2021/5/17 確認〕
※ 264 ENISA：Tips for cybersecurity when working from home https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home〔2021/5/17 確認〕
※ 265 ENISA：Tips for cybersecurity when buying and selling online https://www.enisa.europa.eu/news/enisa-news/tips-for-cybersecurity-when-buying-and-selling-online〔2021/5/17 確認〕
※ 266 ENISA：Understanding and dealing with phishing during the COVID-19 pandemic https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic〔2021/5/17 確認〕
※ 267 ENISA：Tips for selecting and using online communication tools https://www.enisa.europa.eu/news/enisa-news/tips-for-selecting-and-using-online-communication-tools〔2021/5/17 確認〕
※ 268 European Commission：European Democracy Action Plan: making EU democracies stronger https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250〔2021/5/17 確認〕
※ 269 European Commission：Code of Practice on Disinformation https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation〔2021/5/17 確認〕
※ 270 European Commission：Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital〔2021/5/17 確認〕
※ 271 European Commission：The Digital Markets Act: ensuring fair and open digital markets https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en〔2021/5/17 確認〕
※ 272 European Data Protection Board：Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en〔2021/5/17 確認〕
※ 273 European Data Protection Board：Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf〔2021/5/17 確認〕
※ 274 European Data Protection Board：Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf〔2021/5/17 確認〕
※ 275 東洋経済：話題の「ワクチン接種証明書」とはいったい何か https://toyokeizai.net/articles/-/426924〔2021/5/17 確認〕
※ 276 European Commission：Coronavirus: Commission proposes a Digital Green Certificate https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1181〔2021/5/17 確認〕
※ 277 The Office of Privacy Commissioner：Covid-19 vaccine passports not immune to privacy concerns https://privacy.org.nz/blog/covid-19-vaccine-passports-not-immune-to-privacy-

concerns/〔2021/5/17 確認〕
※ 278 The Local：Italy to introduce new Covid 'pass' for travel in high-risk zones https://www.thelocal.it/20210420/covid-19-italy-to-introduce-new-vaccine-pass-for-travel-in-high-risk-zones/〔2021/5/17 確認〕
※ 279 European Data Protection Board：Italian DPA：Major Critical Issues for Vaccination Pass https://edpb.europa.eu/news/national-news/2021/italian-dpa-major-critical-issues-vaccination-pass_en〔2021/5/17 確認〕
※ 280 Council of Europe：Vaccine passports：Council of Europe issues guidance to governments to safeguard human rights https://www.coe.int/en/web/portal/-/vaccine-passports-council-of-europe-issues-guidance-to-governments-to-safeguard-human-rights〔2021/5/17 確認〕
※ 281 The New York Times：E.U. Court Strikes Down Trans-Atlantic Data Transfer Pact https://www.nytimes.com/2020/07/16/business/eu-data-transfer-pact-rejected.html〔2021/5/17 確認〕
※ 282 日本経済新聞：BA に GDPR 制裁金 27 億円　顧客情報流出、コロナで減 額 https://www.nikkei.com/article/DGXMZO065136230X11C20A0000000/〔2021/5/17 確認〕
ICO：ICO fines British Airways £20m for data breach affecting more than 400,000 customers https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/〔2021/5/17 確認〕
※ 283 DLA Piper：Privacy Matters DLA Piper's Global Privacy and Data Protection Resource https://blogs.dlapiper.com/privacymatters/dla-piper-gdpr-fines-and-data-breach-survey-january-2021/〔2021/5/17 確認〕
ZDNet：GDPR 制裁金、前年比で 39%増 -- さらに高額化する可能性も https://japan.zdnet.com/article/35165383/〔2021/5/17 確認〕
※ 284 GARANTE：Operatori telefonici: continua l' attività di controllo del Garante privacy, sanzione a Wind per 17 milioni di euro e a Iliad per 800 mila euro https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9435901#english〔2021/5/17 確認〕
DataGuidance：Italy: Garante fines Wind Tre €16.7M for unlawful direct marketing practices, highlights consent violations https://www.dataguidance.com/news/italy-garante-fines-wind-tre-%E2%82%AC167m-unlawful-direct-marketing-practices-highlights-consent〔2021/5/17 確認〕
※ 285 European Data Protection Board：Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en〔2021/5/17 確認〕
※ 286 TESSIAN：14 Biggest GDPR Fines of 2020 and 2021 (So Far) https://www.tessian.com/blog/biggest-gdpr-fines-2020/〔2021/5/17 確認〕
※ 287 ICO：ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/〔2021/5/17 確認〕
※ 288 European Commission：Shaping Europe's digital future https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade〔2021/5/17 確認〕
※ 289 European Commission：Shaping Europe's digital future https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies〔2021/5/17 確認〕
※ 290 European Commission：Commission welcomes political agreement on the Cybersecurity Competence Centre and Network https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2384〔2021/5/17 確認〕
※ 291 ENISA：ENISA welcomes the European Commission proposal to create a network of Cybersecurity Competence Centres https://www.enisa.europa.eu/news/enisa-news/enisa-welcomes-the-european-commission-proposal-to-create-a-network-of-cybersecurity-competence-centres〔2021/5/17 確認〕
※ 292 ENISA：Procurement Guidelines for Cybersecurity in Hospitals https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services〔2021/5/17 確認〕
※ 293 ENISA：Securing Cloud Services for Health https://www.enisa.europa.eu/news/enisa-news/securing-cloud-services-for-health〔2021/5/17 確認〕
※ 294 Health Advances, LLC：Reflections on Healthcare & Life Sciences Innovation https://healthadvancesblog.com/2020/03/24/e-health-in-france/〔2021/5/17 確認〕
※ 295 ENISA：Artificial Intelligence Cybersecurity Challenges https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges〔2021/5/17 確認〕
※ 296 ENISA：Updated ENISA 5G Threat Landscape Report to Enhance 5G Security https://www.enisa.europa.eu/news/enisa-news/updated-enisa-5g-threat-landscape-report-to-enhance-5g-security〔2021/5/17 確認〕
※ 297 https://www.3gpp.org/〔2021/5/17 確認〕
※ 298 ENISA：Cybersecurity for 5G: ENISA Releases Report on Security Controls in 3GPP https://www.enisa.europa.eu/news/enisa-news/cybersecurity-for-5g-enisa-releases-report-on-security-controls-in-3gpp〔2021/5/17 確認〕
※ 299 TechCrunch：UK U-turns on Huawei and 5G, giving operators until 2027 to rip out existing kit https://techcrunch.com/2020/07/14/uk-u-turns-on-huawei-and-5g-giving-operators-until-2027-to-rip-out-existing-kit/〔2021/5/17 確認〕
※ 300 GOV.UK：New telecoms security law to protect UK from cyber threats https://www.gov.uk/government/news/new-telecoms-security-law-to-protect-uk-from-cyber-threats〔2021/5/17 確認〕
※ 301 JETRO：IT セキュリティー法 2.0 を閣議決定、特定企業の排除は明示せず https://www.jetro.go.jp/biznews/2020/12/947abab1c5dedc9d.html〔2021/5/17 確認〕
※ 302 European Council on Foreign Relations：What Germany's new cyber security law means for Huawei, Europe, and NATO https://ecfr.eu/article/what-germanys-new-cyber-security-law-means-for-huawei-europe-and-nato/〔2021/5/17 確認〕
※ 303 Department of Home Affairs：Australia's Cyber Security Strategy 2020 https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy〔2021/5/19 確認〕
※ 304 https://www.cyber.gov.au/〔2021/5/19 確認〕
※ 305 https://www.csa.gov.sg/singcert〔2021/5/19 確認〕
※ 306 https://www.csa.gov.sg/〔2021/5/19 確認〕
※ 307 https://www.csa.gov.sg/news/publications/safer-cyberspace-masterplan〔2021/5/19 確認〕
※ 308 サイバー衛生：サイバー攻撃の原因となり得る問題を取り除くため、ソフトウェアや OS へのパッチ適用、ネットワーク設定の見直し、パスワード設定の強化等の予防的な対策を推進し、サイバー空間をセキュアに保つこと。
※ 309 https://www.nacsa.gov.my/〔2021/5/19 確認〕
※ 310 NACSA：Malaysia Cyber Security Strategy 2020-2024 https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf〔2021/5/19 確認〕
※ 311 https://www.cybersecurity.my/en/index.html〔2021/5/19 確認〕
※ 312 https://www.oic-cert.org/en/〔2021/5/19 確認〕
※ 313 https://www.boho.or.kr/krcert/intro.do〔2021/5/19 確認〕
※ 314 https://www.auscert.org.au/〔2021/5/19 確認〕
※ 315 https://www.cert-in.org.in/〔2021/5/19 確認〕
※ 316 https://www.cert.gov.lk/〔2021/5/19 確認〕
※ 317 KrCERT/CC：[INFORMATION] Cyber Threat Signal 2021 https://www.boho.or.kr/krcert/publicationView.do?bulletin_writing_sequence=35833〔2021/5/19 確認〕
※ 318 https://www.apcert.org/〔2021/5/19 確認〕
※ 319 https://www.cert.gov.to/〔2021/5/19 確認〕
※ 320 https://www.ncert.gov.ph/〔2021/5/19 確認〕
※ 321 APCERT：About TSUBAME Working Group https://www.apcert.org/about/structure/tsubame-wg/index.html〔2021/5/19 確認〕
※ 322 APCERT：APCERT CYBER DRILL 2020 "BANKER DOUBLES DOWN ON MINER" https://www.apcert.org/documents/pdf/APCERT_Drill2020_Press%20Release.pdf〔2021/5/19 確認〕
※ 323 APCERT：Documents https://www.apcert.org/documents/index.html〔2021/5/19 確認〕
※ 324 https://www.cert.org.cn/publish/english/index.html〔2021/5/19 確認〕
※ 325 https://ajccbc.org/index.html〔2021/5/19 確認〕
※ 326 AJCCBC：ASEAN-Japan Cybersecurity Capacity Building Centre https://www.facebook.com/permalink.php?story_fbid=209846830824990&id=107358564407151〔2021/5/19 確認〕
※ 327 JPCERT/CC：JPCERT/CC インシデント報告対応レポート

2020 年 7 月 1 日～ 2020 年 9 月 30 日　https://www.jpcert.or.jp/pr/2020/IR_Report20201015.pdf〔2021/5/19 確認〕
※ 328 NIST：NICE eNewsletter Winter 2020-21 Industry Spotlight　https://www.nist.gov/itl/applied-cybersecurity/nice/nice-enewsletter-winter-2020-21-industry-spotlight〔2021/5/11 確認〕
※ 329 https://www.nri-secure.co.jp/download/insight2020-report〔2021/5/11 確認〕
※ 330 経団連：経団連サイバーセキュリティ経営宣言　https://www.keidanren.or.jp/policy/2018/018.html〔2021/5/11 確認〕
※ 331 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/007_03_00.pdf〔2021/5/11 確認〕
※ 332 https://www.nisc.go.jp/conference/cs/jinzai/dai14/pdf/14shiryou02.pdf〔2021/5/11 確認〕
※ 333 経済産業省：DX レポート ～ IT システム「2025 年の崖」克服と DX の本格的な展開～　https://www.meti.go.jp/shingikai/mono_info_service/digital_transformation/20180907_report.html〔2021/5/11 確認〕
※ 334 株式会社デンソー：完全子会社 (株式会社デンソー IT ソリューションズ) との吸収合併 (簡易合併・略式合併) に関するお知らせ　https://www.denso.com/jp/ja/news/newsroom/2020/20200706-02/〔2021/5/11 確認〕
※ 335 株式会社大和証券グループ本社・株式会社大和総研ホールディングス・株式会社大和総研・株式会社大和総研ビジネス・イノベーション：株式会社大和総研ホールディングス、株式会社大和総研及び株式会社大和総研ビジネス・イノベーションの合併について　https://www.dir.co.jp/release/2020/2020122201.html〔2021/5/11 確認〕
※ 336 住友化学株式会社：完全子会社の吸収合併（簡易合併・略式合併）に関するお知らせ　https://www.sumitomo-chem.co.jp/news/files/docs/20210226_5.pdf〔2021/5/11 確認〕
※ 337 https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf
※ 338 https://www.nisc.go.jp/conference/cs/jinzai/dai14/pdf/14shiryou0105.pdf〔2021/5/11 確認〕
※ 339 IPA:ITSS+（プラス）・IT スキル標準（ITSS）・情報システムユーザースキル標準（UISS）関連情報　https://www.ipa.go.jp/jinzai/itss/itssplus.html
※ 340 https://www.ipa.go.jp/icscoe/program/middle/strategic_management/index.html〔2021/5/11 確認〕
※ 341 東京工業大学：サイバーセキュリティ経営戦略コース受講生募集のご案内　https://www.titech.ac.jp/company/news/pdf/info-26604.pdf〔2021/5/11 確認〕
※ 342 情報セキュリティ大学院大学：DX 推進者対象 DX with Cybersecurity 3 日間教育コース　https://www.iisec.ac.jp/event/pdf/20201118seminar_pamp.pdf〔2021/5/11 確認〕
※ 343 https://www.meti.go.jp/policy/netsecurity/downloadfiles/tebikigaiyou1.1.pdf〔2021/5/11 確認〕
※ 344 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf〔2021/5/11 確認〕
※ 345 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf〔2021/5/11 確認〕
※ 346 NISC：（事務局資料）政策議論のための補助フレームワーク　https://www.nisc.go.jp/conference/cs/jinzai/dai14/pdf/14sankou01.pdf〔2021/5/11 確認〕
※ 347 重要インフラ：他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもので、重要インフラ分野として指定する分野。具体的には、「情報通信」「金融」「航空」「空港」「鉄道」「電力」「ガス」「政府・行政サービス（地方公共団体を含む）」「医療」「水道」「物流」「化学」「クレジット」及び「石油」の 14 分野。
NISC：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　https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r2.pdf〔2021/05/19 確認〕
※ 348 IPA：中核人材育成プログラム修了者コミュニティ「叶会（かなえかい）」　https://www.ipa.go.jp/icscoe/program/core_human_resource/icscoe_alumni.html〔2021/05/19 確認〕
※ 349 IPA：情報処理安全確保支援士（登録セキスペ）になるには　https://www.ipa.go.jp/siensi/toberiss/index.html〔2021/05/19 確認〕
※ 350 IPA:管理監督者向けプログラム　製造・生産分野向けセキュリティ教育プログラム　https://www.ipa.go.jp/icscoe/program/middle/seizo-seisan/2020.html〔2021/05/19 確認〕
※ 351 IPA：責任者向けプログラム 業界別サイバーレジリエンス強化演習（CyberREX）　https://www.ipa.go.jp/icscoe/program/short/specific_industries/2020.html〔2021/05/19 確認〕
※ 352 IPA：戦略マネジメント系セミナー　https://www.ipa.go.jp/icscoe/program/middle/strategic_management/2020.html〔2021/05/19 確認〕
※ 353 IPA：実務者向けプログラム 制御システム向けサイバーセキュリティ演習　https://www.ipa.go.jp/icscoe/program/short/icssec/2020.html〔2021/05/19 確認〕
※ 354 CBT（Computer Based Testing）方式：試験会場に設置されたコンピュータを利用して実施する試験方式のこと。受験者はコンピュータに表示された試験問題に対して、マウスやキーボードを用いて解答する。
※ 355 IPA：情報処理技術者試験 情報処理安全確保支援士試験 統計資料 令和 2 年度試験全試験区分版　https://www.jitec.ipa.go.jp/1_07toukei/toukei_r02o.pdf〔2021/6/21 確認〕
※ 356 IPA：情報処理技術者試験 情報処理安全確保支援士試験 統計資料 令和 2 年度試験全試験区分版　https://www.jitec.ipa.go.jp/1_07toukei/toukei_r02o.pdf〔2021/6/21 確認〕
※ 357 IPA：国家資格「情報処理安全確保支援士」2021 年 4 月 1 日付登録者 804 名の内訳を公開しました　https://www.ipa.go.jp/siensi/data/20210401newriss.html〔2021/5/19 確認〕
※ 358 経済産業省：情報処理安全確保支援士特定講習　https://www.meti.go.jp/policy/it_policy/jinzai/tokutei.html〔2021/5/19 確認〕
※ 359 経済産業省：情報処理安全確保支援士特定講習一覧　https://www.meti.go.jp/press/2020/03/20210331004/20210331004-1.pdf〔2021/5/19 確認〕
※ 360 IPA：情報処理安全確保支援士（登録セキスペ）の受講する講習について　https://www.ipa.go.jp/siensi/lecture/index.html〔2021/5/19 確認〕
※ 361 IPA：国家資格「情報処理安全確保支援士」制度の仕組み　https://www.ipa.go.jp/files/000088283.pdf〔2021/5/19 確認〕
※ 362 IPA：セキュリティ・キャンプ全国大会 2020 オンライン　ホーム　https://www.ipa.go.jp/jinzai/camp/2020/zenkoku2020_index.html〔2021/5/19 確認〕
※ 363 IPA：セキュリティ・ネクストキャンプ 2020 オンライン　ホーム　https://www.ipa.go.jp/jinzai/camp/2020/next2020_index.html〔2021/5/19 確認〕
※ 364 IPA：セキュリティ・キャンプ　https://www.ipa.go.jp/jinzai/camp/index.html#section5〔2021/5/19 確認〕
※ 365 一般社団法人セキュリティ・キャンプ協議会事務局：セキュリティ・キャンプ　https://www.security-camp.or.jp/event/index.html〔2021/5/19 確認〕
※ 366 enPiT2：連携校によるネットワークで特徴ある講義・演習を相互に提供　https://www.seccap.jp/basic/seccap.html〔2021/5/19 確認〕
※ 367 大阪大学大学院情報科学研究科 enPiT 事務局：enPiT［文部科学省］成長分野を支える情報技術人材の育成拠点の形成 2020 年度 成果報告書　https://www.enpit.jp/files/enPiT_annualreport_uni_2020.pdf〔2021/5/19 確認〕
※ 368 https://enpit-pro.jp〔2021/5/19 確認〕
※ 369 https://www.seccap.pro/〔2021/5/19 確認〕
※ 370 CTF（Capture The Flag）：互いに相手陣地にある旗を奪い合う野外ゲームを情報セキュリティに適用したもので、例えば自分のホストを守りながら、相手チームのホストを攻撃する競技等がある。
※ 371 Security NEXT：SECCON 初のオンライン決勝、約 1000 チームが参戦 - 一時開催危ぶまれるも若手奮闘　https://www.security-next.com/120376〔2021/5/19 確認〕
※ 372 SECCON：SECCON 2020 電脳会議 2020.12.19(sat)　https://www.seccon.jp/2020/ep201219.html〔2021/5/19 確認〕
※ 373 SECCON：SECCON Beginners とは　https://www.seccon.jp/2020/beginners/about-seccon-beginners.html〔2021/5/19 確認〕
※ 374 SECCON：SECCON Beginners Live 開催のお知らせ　https://www.seccon.jp/2020/seccon_beginners/seccon_beginners_live.html〔2021/5/19 確認〕
※ 375 http://girls.seccon.jp/〔2021/5/19 確認〕
※ 376 JNSA：JNSA インターンシップ　https://www.jnsa.org/internship/index.html〔2021/5/19 確認〕
※ 377 東京工業大学：キャリアアップ MOT「2020 年度 サイバーセキュリティ経営戦略コース」受講生募集のご案内　https://www.titech.ac.jp/alumni/news/2020/048570.html〔2021/5/19 確認〕
※ 378 サイバーセキュリティ経営：経営戦略や事業リスク管理の一貫としてサイバーセキュリティリスク管理を実践すること。
※ 379 PwC Japan グループ：経済犯罪実態調査 2020 日本分析版　https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2020/assets/pdf/economic-crime-survey.pdf〔2021/5/26 確認〕
※ 380 https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2020/assets/pdf/economic-crime-survey.pdf〔2021/5/26 確認〕

※ 381 トレンドマイクロ社：法人組織のセキュリティ動向調査 2020 年版を発表 https://www.trendmicro.com/ja_jp/about/press-release/2020/pr-20201002-01.html〔2021/5/26 確認〕
※ 382 NRI セキュア社：NRI セキュア、「企業における情報セキュリティ実態調査 2020」を実施 https://www.nri.com/jp/news/newsrelease/lst/2020/cc/1215_1〔2021/5/26 確認〕
※ 383 IPA：「2020 年度サイバーセキュリティ経営ガイドライン実践のためのプラクティスの在り方に関する調査」報告書 https://www.ipa.go.jp/security/fy2020/reports/practice/index.html〔2021/5/26 確認〕
※ 384 「強い懸念がある」及び「やや懸念がある」を合わせた回答。
※ 385 情報セキュリティリスクの管理体制構築や情報セキュリティ対策の実装等を率先して指示することを指す。
※ 386 https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf〔2021/5/26 確認〕
※ 387 IPA：サイバーセキュリティ経営ガイドライン実践状況の可視化ツールβ版 https://www.ipa.go.jp/security/economics/checktool/index.html〔2021/5/26 確認〕
※ 388 https://www.ipa.go.jp/security/fy30/reports/ciso/index.html〔2021/5/26 確認〕
※ 389-1 「必要であり、積極的に協力したいと思う」「必要であり、機会があれば協力したいと思う」「必要ではあるが、協力したいとは思わない」の合計。
※ 389-2 経済産業省：事務局説明資料 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/007_03_00.pdf〔2021/6/25 確認〕
※ 390 https://www.sonpo.or.jp/cyber-hoken/data/2020-01/pdf/cyber_report2020.pdf〔2021/5/19 確認〕
※ 391 https://www.ipa.go.jp/files/000088835.pdf〔2021/5/19 確認〕
※ 392 https://www.ipa.go.jp/security/keihatsu/sme/sc3/〔2021/5/19 確認〕
※ 393 https://www.ipa.go.jp/files/000088836.pdf〔2021/5/19 確認〕
※ 394 IPA：令和 2 年度中小企業の情報セキュリティマネジメント指導業務 https://www.ipa.go.jp/security/keihatsu/sme/management/index.html〔2021/5/19 確認〕
※ 395 経済産業省：「地域セキュリティコミュニティ【地域 SECUNITY】形成・運営のためのプラクティス集」（第 1 版）を取りまとめました https://www.meti.go.jp/press/2020/02/20210217001/20210217001.html〔2021/5/19 確認〕
※ 396 経済産業省：テレワークにおけるセキュリティ確保 https://www.soumu.go.jp/main_sosiki/cybersecurity/telework〔2021/6/2 確認〕
※ 397 https://www.soumu.go.jp/main_content/000753141.pdf〔2021/6/2 確認〕
※ 398 https://www.jnsa.org/result/west/data/SecurityByDesign.pdf〔2021/5/19 確認〕
※ 399 https://www.ipa.go.jp/security/security-action/〔2021/5/19 確認〕
※ 400 https://school-security.jp/pdf/2019.pdf〔2021/5/25 確認〕
※ 401 文部科学省：教育情報セキュリティポリシーに関するガイドライン（令和元年 12 月版） https://www.mext.go.jp/content/20200219-mxt_jogai02-000003278_409.pdf〔2021/6/1 確認〕
※ 402 国立大学法人金沢大学：個人情報を保存したノートパソコンの窃盗による紛失について（事実報告とお詫び） https://www.kanazawa-u.ac.jp/news/83181〔2021/5/25 確認〕
※ 403 国立大学法人東京芸術大学：ノート PC 及び受験関係書類の盗難にかかる個人情報の紛失について https://www.geidai.ac.jp/news/2021021998422.html〔2021/5/25 確認〕
※ 404 学校法人立教大学：個人情報を含む USB メモリ紛失のお詫びとお知らせ https://www.rikkyo.ac.jp/news/2021/03/mknpps000001j46o.html〔2021/5/25 確認〕
※ 405 総務省：自治体情報セキュリティ対策の見直しについて https://www.soumu.go.jp/main_content/000688754.pdf〔2021/5/25 確認〕
※ 406 LGWAN（Local Government Wide Area Network）：総合行政ネットワークのこと。地方公共団体を相互に接続する行政専用のネットワークであり、地方公共団体相互間のコミュニケーションの円滑化、情報の共有による情報の高度利用を図るための基盤として整備され、全国の地方公共団体の組織内ネットワークを相互に接続している。
※ 407 https://www.soumu.go.jp/main_content/000688753.pdf〔2021/5/25 確認〕
※ 408 eLTAX:地方税ポータルシステムのこと。地方税における手続きを、インターネットを利用して行うためのシステムで、地方税共同機構が開発・運営。読み方は「エルタックス」。
※ 409 ぴったりサービス：地方公共団体が提供する行政サービスを、検索したりオンライン申請したりできるサービスの総称。内閣府番号制度担当室が運営。
※ 410 総務省：地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会 https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security/index.html〔2021/6/3 確認〕
※ 411 J-LIS：（全体運用の開始）「自治体テレワーク推進実証実験」について https://www.j-lis.go.jp/lgwan/news/lgwan-koubo_telework.html〔2021/5/25 確認〕
※ 412 J-LIS：緊急事態宣言（令和 3 年 1 月）の発出に伴う「自治体テレワークシステム for LGWAN」の一時提供について https://www.j-lis.go.jp/lgwan/news/lgwan-koubo_telework_1.html〔2021/5/25 確認〕
※ 413 総務省：次期自治体情報セキュリティクラウドの標準要件の決定について https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security/index_00001.html〔2021/5/25 確認〕
※ 414 SOC（Security Operation Center）：セキュリティ攻撃の検出・分析のため、システムやデバイス、ネットワーク等を監視するセキュリティ専門人材による組織。
※ 415 CDN（Content Delivery Network）：Web コンテンツを配信するために最適化されたネットワーク。オリジナルの Web コンテンツを格納するサーバである「オリジンサーバ」、代理で Web コンテンツを配信する「キャッシュサーバ」などから構成される。
※ 416 三重県：三重県自治体情報セキュリティクラウドの更改に関する情報提供依頼（RFI） https://www.pref.mie.lg.jp/IT/HP/m0009800059_00004.htm〔2021/5/25 確認〕
※ 417 茨城県：いばらき情報セキュリティクラウド導入にかかる情報提供依頼（RFI）の実施について https://www.pref.ibaraki.jp/kikaku/joho/denshi/20210308.html〔2021/5/25 確認〕
※ 418 SLA（Service Level Agreement）：サービス事業者と利用者の間で結ばれるサービスのレベル（定義、範囲、内容、達成目標等）に関する合意サービス水準、サービス品質保証のこと。
※ 419 IPA:「2020 年度情報セキュリティに対する意識調査【倫理編】【脅威編】」報告書 https://www.ipa.go.jp/security/economics/ishikichousa2020.html〔2021/6/4 確認〕
※ 420 選択肢「1 年以上前から実施している」「1 年以内に実施し始めた」の合計。
※ 421 IPA の「2020 年度情報セキュリティに対する意識調査【脅威編】」では、調査対象者のうち社会人を「情報システムおよび通信関係以外の業務」及び「情報システムおよび通信関係の業務」に分類し分析している。本白書用に実施した追加分析では前者の「情報システムおよび通信関係以外の業務」の従事者を対象とした。また、本調査では、情報システム・通信関係の業務に従事・関与しない対象者として「公務員」「教職員」の分類が存在する。しかし、サンプル数が少なく参考値扱いとなったため、追加分析の対象から除外した。
※ 422 IPA の「2020 年度 情報セキュリティに対する意識調査【脅威編】」の「職業軸 _ 脅威調査 PC」（https://www.ipa.go.jp/files/000088918.pdf〔2021/6/4 確認〕）では「電子メールにある添付ファイルは不用意に開かない、また本文中の URL も不用意にクリックしない」を「1 年以上前から実施している」「1 年以内に実施し始めた」の合計が 69.6%（p.81）、「ネットでファイルやソフトウェアをダウンロードする場合、安全性や信頼性を自分なりに注意・判断している」を「1 年前から実施している」「1 年以内に実施し始めた」割合が 69.5%（p.83）。
※ 423 経済産業省：知的財産と標準化によるビジネス戦略 https://www.jpo.go.jp/news/shinchaku/event/seminer/text/document/h30_jitsumusya_txt/34_pp.pdf〔2021/6/4 確認〕
※ 424 https://www.kantei.go.jp/jp/singi/titeki2/kettei/chizaikeikaku20200527.pdf〔2021/6/4 確認〕
※ 425 国立研究開発法人産業技術総合研究所：産業界の標準化活動をサポートする産総研標準化推進センターが始動 https://www.aist.go.jp/aist_j/news/pr20200701.html〔2021/6/4 確認〕
※ 426 フォーラム標準の定義については、「JIS Z 8002:2006」の「JA.1」の「100.5」を参照。
※ 427 ISO：ISO/IEC JTC 1 https://www.iso.org/committee/45020.html〔2021/6/4 確認〕
※ 428 日本産業標準調査会：JISC について https://www.jisc.go.jp/jisc/index.html〔2021/6/4 確認〕
※ 429 ITU：SG17: Security https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx〔2021/6/4 確認〕
※ 430 IETF：The IETF Security Area https://trac.ietf.org/trac/sec/wiki〔2021/6/4 確認〕
※ 431 TCG：Welcome to Trusted Computing Group https://trustedcomputinggroup.org/work-groups/regional-forums/japan〔2021/6/4 確認〕
※ 432 https://www.jisc.go.jp/international/iso-prcs.html〔2021/6/4 確認〕
※ 433 ISO/IEC 27701 は SC 27/WG 5 で検討、発行された規格である。
※ 434 耐量子計算機暗号：量子計算機が実用化されても安全性が保てると期待される暗号。

※ 435 ドイツ規格協会：Downloads　https://www.din.de/en/meta/jtc1sc27/downloads〔2021/6/4 確認〕
上記 Web ページの「SC27WG2 SD8 Post-Quantum Cryptography」をクリックすることでダウンロードできる。
※ 436 Preliminary Work Item（予備業務項目）：新しい標準を作成するための検討期間を指す。2020 年 9 月まで WG 3 内では研究期間（Study Period）と呼ばれていた。
※ 437 Black Hat：Remote Exploitation Of An Unaltered Passenger Vehicle　https://www.youtube.com/watch?reload=9&v=MAcHkASmXEc〔2021/5/19 確認〕
※ 438 日本経済新聞：クライスラー、ハッキング対策で 140 万台リコール　https://www.nikkei.com/article/DGXLASGM25H19_V20C15A7MM0000/〔2021/5/19 確認〕
※ 439 United Nations Economic Commission for Europe（国際連合欧州経済委員会）：国際連合の経済社会理事会の地域経済委員会の一つ。
※ 440 ISO：ISO/SAE FDIS 21434 Road vehicles — Cybersecurity engineering　https://www.iso.org/standard/70918.html〔2021/5/19 確認〕
※ 441 ISO：Biometric security　https://www.iso.org/contents/news/2021/01/Ref2613.html〔2021/5/19 確認〕
※ 442 IoT 推進コンソーシアム・総務省・経済産業省：IoT セキュリティガイドライン Ver1.0　https://www.soumu.go.jp/main_content/000428393.pdf〔2021/5/26 確認〕
※ 443 https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf〔2021/6/2 確認〕
※ 444 https://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf〔2021/6/2 確認〕
※ 445 https://www.commoncriteriaportal.org/〔2021/6/2 確認〕
※ 446 IPA：認証プロテクションプロファイルリスト　https://www.ipa.go.jp/security/jisec/certified_pps/pp_list.html〔2021/6/2 確認〕
※ 447 IPA：本制度に関連する ISO/IEC 規格　https://www.ipa.go.jp/security/jcmvp/topics.html〔2021/6/3 確認〕
※ 448 NIST：FIPS 140-3 Transition Effort　https://csrc.nist.gov/Projects/fips-140-3-transition-effort/fips-140-3-docs〔2021/6/3 確認〕
※ 449 NIST：Supporting Documents for FIPS 140-3 and the Cryptographic Module Validation Program (CMVP) Now Available: NIST Special Publication 800-140x Subseries　https://csrc.nist.gov/news/2020/nist-publishes-sp-800-140x-subseries-for-the-cmvp〔2021/6/3 確認〕
※ 450 NIST：FIPS 140-2 Cryptographic Module Validation Program Management Manual　https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Module-Validation-Program/documents/CMVPMM.pdf〔2021/6/3 確認〕
※ 451 NIST：FIPS 140-3 Transition Effort　https://csrc.nist.gov/projects/fips-140-3-transition-effort〔2021/6/3 確認〕
※ 452 NIST：FIPS 140-3 IG Announcements　https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements〔2021/6/3 確認〕
※ 453 NIST：FIPS 140-3 Management Manual　https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-140-3-management-manual〔2021/6/3 確認〕
※ 454 International Cryptographic Module Conference：https://icmconference.org/〔2021/6/3 確認〕
※ 455 NIST：Use of Unvalidated Cryptographic Modules by Federal Agencies and Departments　https://csrc.nist.gov/projects/cryptographic-module-validation-program〔2021/6/3 確認〕
※ 456 https://www.kantei.go.jp/jp/singi/it2/cio/kettei/20190225kettei1-1.pdf〔2021/6/3 確認〕
※ 457 IPA/JISEC：「ハードコピーデバイスのプロテクションプロファイル」適合の申請案件についてのガイドライン 第 1.8 版　https://www.ipa.go.jp/security/jisec/mfp/guidelineforHCD-PP_1.8.pdf〔2021/6/3 確認〕
※ 458 https://www.ipa.go.jp/security/jisec/certified_pps/c0553/c0553_pp.pdf〔2021/6/3 確認〕
※ 459 IPA/JISEC：認証製品リスト　https://www.ipa.go.jp/security/jisec/certified_products/cert_listv31.html〔2021/6/3 確認〕
※ 460 IPA：暗号アルゴリズム確認登録簿　https://www.ipa.go.jp/security/jcmvp/avallists.html〔2021/6/3 確認〕
※ 461 IPA/JCMVP：暗号モジュール試験及び認証制度（JCMVP）：承認されたセキュリティ機能　https://www.ipa.go.jp/security/jcmvp/algorithm.html〔2021/6/3 確認〕
※ 462 NIST：Recommendation for Key-Derivation Methods in Key-Establishment Schemes　https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr1.pdf〔2021/6/3 確認〕
※ 463 e-Gov 法令検索：電子署名及び認証業務に関する法律施行規則　https://elaws.e-gov.go.jp/document?lawid=413M60000418002〔2021/6/3 確認〕
※ 464 IPA：暗号モジュール試験及び認証制度（JCMVP）：規程集　https://www.ipa.go.jp/security/jcmvp/kitei.html〔2021/6/3 確認〕
※ 465 経済産業省：「政府情報システムのためのセキュリティ評価制度（ISMAP）」の運用を開始しました　https://www.meti.go.jp/press/2020/06/20200603001/20200603001.html〔2021/6/4 確認〕
※ 466 https://cio.go.jp/sites/default/files/uploads/documents/cloud_policy_20210330.pdf〔2021/6/4 確認〕
※ 467 経済産業省：クラウドサービスの安全性評価に関する検討会について　https://www.meti.go.jp/shingikai/mono_info_service/cloud_services/pdf/001_02_00.pdf〔2021/6/4 確認〕
※ 468 https://www.meti.go.jp/press/2019/01/20200130002/20200130002-1.pdf〔2021/6/4 確認〕
※ 469 https://www.nisc.go.jp/active/general/pdf/wakugumi2020.pdf〔2021/6/4 確認〕
※ 470 https://www.ismap.go.jp/sys_attachment.do?sys_id=c0b4525fdb53a4107766044cd3961942〔2021/6/4 確認〕
※ 471 https://www.ismap.go.jp〔2021/6/4 確認〕
※ 472 https://www.nisc.go.jp/active/infra/pdf/shishin5rev.pdf〔2021/6/4 確認〕
※ 473 NISC：『ラブライブ!サンシャイン !!』とのタイアップについて　https://www.nisc.go.jp/security-site/month/lovelive.html〔2021/5/19 確認〕
※ 474 https://www.youtube.com/watch?v=L7FQboNt9RI〔2021/5/19 確認〕
※ 475 https://www.youtube.com/watch?v=Cghzzqh33JA〔2021/5/19 確認〕
※ 476 https://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/csboardgame.html〔2021/5/19 確認〕
※ 477 https://www.itct-net.com/siryou#h.kaes1k95c2bs〔2021/5/19 確認〕
※ 478 JNSA：みんなの「サイバーセキュリティコミック」プロジェクト　https://www.jnsa.org/comic/〔2021/5/19 確認〕
※ 479 トレンドマイクロ株式会社：法人向けガイドブック「働く大人なら最低限知っておきたいネットセキュリティの基本」2021 年度版公開　https://www.is702.jp/news/3835/〔2021/5/19 確認〕
※ 480 NHK：木村花さんの死が問いかけるもの　https://www3.nhk.or.jp/news/html/20200604/k10012457591000.html〔2021/5/19 確認〕
※ 481 総務省：特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律第 4 条第 1 項の発信者情報を定める省令の一部を改正する省令の制定　https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000095.html〔2021/5/19 確認〕
※ 482 違法・有害情報相談センター：削除依頼の流れについて　https://ihaho.jp/guide/reqdelflow.html〔2021/5/19 確認〕
※ 483 https://www.pref.gunma.jp/07/cl01_00048.html〔2021/5/19 確認〕
※ 484 https://no-heart-no-sns.smaj.or.jp/〔2021/5/19 確認〕
※ 485 https://smaj.or.jp/〔2021/5/19 確認〕
※ 486 Twitter Japan 株式会社：https://twitter.com/twitterjp/status/1235685197959639042〔2021/5/19 確認〕
※ 487 Twitter Japan 株式会社：Twitter での会話について　https://help.twitter.com/ja/using-twitter/twitter-conversations#controls〔2021/5/19 確認〕
※ 488 ByteDance 株式会社：TikTok、青少年のオンライン上でのプライバシー保護に関する安全性を強化　https://newsroom.tiktok.com/ja-jp/strengthening-privacy-and-safety〔2021/5/19 確認〕
※ 489 ByteDance 株式会社：TikTok、青少年保護強化のために年齢認証システムを全ユーザー向けに変更　https://newsroom.tiktok.com/ja-jp/tiktok-changes-the-age-verification-system-to-be-applicable-for-all-users〔2021/5/19 確認〕
※ 490 ヤフー株式会社：ユーザーに安心してご利用いただくための自主ルール策定を目的とした「プラットフォームサービスの運営の在り方検討会」を開催　https://about.yahoo.co.jp/pr/release/2020/07/01a/〔2021/5/19 確認〕
※ 491 千葉日報：被告「被害者の気持ち分かった」　成田不明女児の母を脅迫　検察、懲役6月求刑　https://www.chibanippo.co.jp/news/national/731442〔2021/5/19 確認〕
※ 492 https://www5.cao.go.jp/keizai2/manzoku/pdf/result2_covid.pdf〔2021/5/19 確認〕
※ 493 https://www.mhlw.go.jp/content/000777425.pdf〔2021/5/19 確認〕
※ 494 https://www.ipa.go.jp/security/kokokara/〔2021/5/19 確認〕

※ 495 https://www.mext.go.jp/content/20200427-mxt_kouhou01-000004520_1.pdf〔2021/5/19 確認〕
※ 496 文部科学省：GIGA スクール構想について　https://www.mext.go.jp/a_menu/other/index_0001111.htm〔2021/5/19 確認〕
※ 497 文部科学省：「教育情報セキュリティポリシーに関するガイドライン」公表について　https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm〔2021/5/19 確認〕
※ 498 NHK：トイレットペーパー“品薄はデマ”も不安に歯止めかからず　https://www3.nhk.or.jp/news/html/20200302/k10012309761000.html〔2021/5/19 確認〕
※ 499 https://www.soumu.go.jp/main_content/000693280.pdf〔2021/5/19 確認〕
※ 500 ASCII.jp：オードリー・タン氏「台湾のデジタル社会イノベーションはどう実現したか」　https://ascii.jp/elem/000/004/033/4033626/2/〔2021/5/19 確認〕
※ 501 https://www.youtube.com/watch?v=rbNuikVDrN4〔2021/5/19 確認〕
※ 502 読売新聞オンライン：［STOP　ネット暴力］「うちの県にコロナ持ってきた」…「感染者狩り」横行、実名特定・中傷エスカレート　https://www.yomiuri.co.jp/national/20200804-OYT1T50069/〔2021/5/19 確認〕
※ 503 宮城県：「ストップ!コロナ差別」 啓発活動にご協力ください　https://www.pref.miyagi.jp/site/covid-19/corona-stopsenngenn.html〔2021/5/19 確認〕
※ 504 内閣官房：新型コロナウイルス感染症に関する偏見や差別を防止するための規定が設けられました!　https://corona.go.jp/emergency/pdf/henken_sabetu_20210212.pdf〔2021/5/19 確認〕
※ 505 http://www.kokusen.go.jp/pdf/n-20200710_1.pdf〔2021/5/19 確認〕
※ 506 https://www.meti.go.jp/covid-19/pdf/jizokuka-kyufukin_fusei.pdf〔2021/5/19 確認〕
※ 507 神奈川県：荷受代行や荷物転送のアルバイトにご注意!　https://www.pref.kanagawa.jp/docs/r7b/cnt/f370214/p1057013.html〔2021/5/19 確認〕
埼玉県：「荷受代行」「荷物転送」のアルバイトに気をつけて!　https://www.pref.saitama.lg.jp/b0304/soudanjirei/161125.html〔2021/5/19 確認〕
※ 508 経済産業省：不正競争防止法　https://www.meti.go.jp/policy/economy/chizai/chiteki/h30jyoubunn.pdf〔2021/5/19 確認〕
※ 509 経済産業省：「不正競争防止法第十八条第二項第三号の外国公務員等で政令で定める者を定める政令の一部を改正する政令」が閣議決定されました　https://www.meti.go.jp/press/2018/09/20180904001/20180904001.html〔2021/5/19 確認〕
※ 510 BUSINESS LAWYERS:第 1 回 2019 年 7 月施行、ビッグデータの保護に関する改正不正競争防止法の概要と保護の対象となるデータ　https://www.businesslawyers.jp/articles/583〔2021/5/19 確認〕
※ 511 経済産業省：営業秘密管理指針　https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf〔2021/5/19 確認〕
※ 512 IPA：「企業における営業秘密管理に関する実態調査 2020」報告書について　https://www.ipa.go.jp/security/fy2020/reports/ts_kanri/index.html〔2021/5/19 確認〕
※ 513 IPA：「企業における営業秘密管理に関する実態調査」報告書について　https://www.ipa.go.jp/security/fy28/reports/ts_kanri/index.html〔2021/5/19 確認〕
※ 514 差分攻撃：入力平文と出力暗号文の差分を用いる暗号攻撃手法。
※ 515 Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir：The Retracing Boomerang Attack　https://link.springer.com/chapter/10.1007%2F978-3-030-45721-1_11〔2021/5/19 確認〕
※ 516 AES（Advanced Encryption Standard）：米国で NIST により標準化された共通鍵暗号。
※ 517 差分線形解析：差分と線型近似とを組み合せた暗号攻撃手法。
※ 518 Christof Beierle, Gregor Leander, and Yosuke Todo：Improved Differential-Linear Attacks with Applications to ARX Ciphers　https://link.springer.com/chapter/10.1007/978-3-030-56877-1_12〔2021/5/19 確認〕
※ 519 ChaCha:Daniel J. Bernstein によって開発されたストリーム暗号。Chacha20 は ChaCha を基にした暗号であり、これとメッセージ認証子である Poly1305 とを組み合わせた ChaCha20-Poly1305 は、CRYPTREC の推奨候補暗号リストに入っている。
※ 520 Comparing the Difficulty of Factorization and Discrete Logarithm: A 240-Digit Experiment [Crypto2020] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann　https://link.springer.com/chapter/10.1007%2F978-3-030-56880-1_3〔2021/5/19 確認〕
※ 521 NIST：NIST PQC Standardization Update-Round 2 and Beyond　https://csrc.nist.gov/CSRC/media/Presentations/pqc-update-round-2-and-beyond/images-media/pqcrypto-sept2020-moody.pdf〔2021/5/19 確認〕
※ 522 NIST：Lightweight Cryptography Standardization: Finalists Announced　https://csrc.nist.gov/News/2021/lightweight-crypto-finalists-announced〔2021/5/19 確認〕
※ 523 ECDSA（Elliptic Curve Digital Signature Algorithm）：楕円曲線暗号を用いたデジタル署名アルゴリズム。
※ 524 Jan Jancar, Vladimir Sedlacek, Petr Svenda, and Marek Sys：Minerva: The curse of ECDSA nonces　https://tches.iacr.org/index.php/TCHES/article/view/8684〔2021/5/19 確認〕
※ 525 nonce：ある種の暗号演算において、1 度だけ使用される使い捨ての値。
※ 526 CVE（Common Vulnerabilities and Exposures）：個別製品中の脆弱性を対象として採番されている識別子。本件については実装ごとに CVE-2019-2894、CVE-2019-13627、CVE-2019-13628、CVE-2019-13629、CVE-2019-14318、CVE-2019-15819 が発行されている。
※ 527 binary GCD アルゴリズム：2 数の最大公約数を求めるアルゴリズムの一つ。ユークリッドの互除法と比較して、計算機に向くような単純な算術演算（シフト、比較、減算）のみを使用することで、高速に計算できるようにしている。
※ 528 Alejandro Cabrera Aldaya, and Billy Bob Brumley：When one vulnerable primitive turns viral: Novel single-trace attacks on ECDSA and RSA　https://tches.iacr.org/index.php/TCHES/article/view/8549〔2021/5/19 確認〕
※ 529 Alejandro Cabrera Aldaya, Cesar Pereida García and Billy Bob Brumley：From A to Z: Projective coordinates leakage in the wild　https://tches.iacr.org/index.php/TCHES/article/view/8596〔2021/5/19 確認〕
※ 530 https://www.jnsa.org/result/surv_mrk/2021/index.html〔2021/6/30 確認〕

第3章
個別テーマ

本章では個別テーマとして、制御システム、IoT、そして2020年に新型コロナウイルス感染症の影響により急速に普及したテレワークの情報セキュリティについて、報告されたインシデントや攻撃の実態、脆弱性や脅威の動向、国の施策や企業の対策の状況等を解説する。

また、企業・組織のサイバーセキュリティ対策の検討や、政府機関のセキュリティ規格の策定・改訂の際に参照されることが多くなった米国NISTのセキュリティに関する活動やSP 800シリーズ等の規格策定の動向等について紹介する。

3.1 制御システムの情報セキュリティ

制御システム（ICS：Industrial Control System）は、電力、ガス、水道、輸送・物流、製造ライン等、我々の生活を支える重要インフラサービス※1を提供するシステムである。従来、制御システムは独立したネットワーク、固有のプロトコル、事業者ごとに異なる仕様で構築・運用されることが多く、外部からサイバー攻撃を行うことは困難と考えられていた。しかし、近年ネットワーク化やオープン化（標準プロトコル・汎用製品の利用）が進んだこと、また、10～20年に及ぶライフサイクルの長さ故に、外部との接続やサイバー攻撃を想定していないシステムが今なお多数稼働していることから、制御システムに対するサイバー脅威が高まっている。実際に、サイバー攻撃による浄水施設における薬液注入量の改ざん、大規模停電等のインシデントも発生している。

本節では、制御システムのセキュリティの動向と主な取り組みについて述べる。

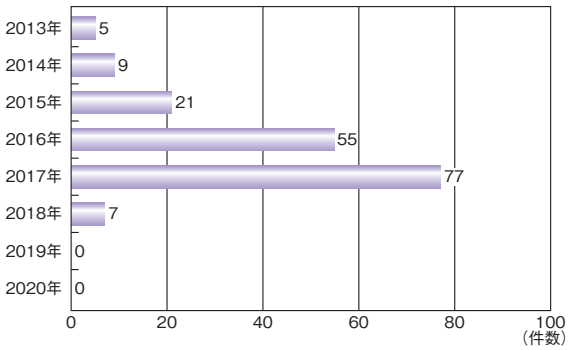
3.1.1 インシデントの発生状況と動向

国内においては、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）に2020年に報告された制御システムのインシデント件数は、2019年に引き続き0件であった（図3-1-1）。

しかし海外では、調査会社による制御システムユーザ等へのアンケート調査において、2019年同様、制御システムへの侵入や運用障害が発生したという回答が一定数以上あった。

例えば、製造事業者内のセキュリティ戦略、制御、運用に直接関与するサイバー及びITの専門家150名を対象とした調査結果では、調査対象者が所属する組織の53%が、過去12～24ヵ月の間に何らかのサイバー攻撃やその他のセキュリティインシデントに見舞われ、運用・制御技術（OT：Operational Technology）のインフラに影響があったと回答している※3。また、北米、欧州、アジアの重要インフラ組織の経営幹部400名以上を対象とした調査結果では、セキュリティ侵害があったという回答の85%のケースでOTネットワークまで侵入されており、そのうち36%がITシステムからの侵入であった※4。

2020年に公になったインシデントには、水道や電力等の重要インフラの制御システムを標的とした攻撃、ITシステムのウイルス※5感染による生産や重要サービスの停止、制御システムを標的としたランサムウェアによる攻撃、ネットワーク管理ソフトウェアの脆弱性に端を発する大規模な感染、USBメモリやパソコンを接続することによるウイルス感染の増加、という五つの特徴が見られた。



■図3-1-1　国内における制御システムのインシデント報告件数（2013～2020年）
（出典）JPCERT/CCのインシデント報告対応レポート※2を基にIPAが作成

(1) 水道や電力等の重要インフラの制御システムが標的となった事例

海外では、水道や電力等の重要インフラの制御システムが標的となったインシデントが報告された。

イスラエルの水道関連施設が、2020 年 4 月、6 月の 2 度攻撃された。4 月の攻撃は、廃水処理プラント、ポンプ場、下水処理場等 6 ヵ所の施設の SCADA（Supervisory Control And Data Acquisition：監視制御及びデータ収集）システムが標的となったが、イスラエル国家サイバー総局（INCD：Israel National Cyber Directorate）がリアルタイムで攻撃を検知し、阻止した[※6]。ある施設では、ポンプが連続運転状態となり、オペレータが自動運転モードを解除した[※7]。また、攻撃を阻止される前に攻撃者は浄水場の水の塩素レベルを変更しようとしたとの情報もあり、塩素または他の化学物質が誤った比率で水源に混入され、有害な状態のまま供給される恐れがあった[※8]。6 月の攻撃は、二つの農村地域の送水ポンプと農業用水ポンプが標的となったが、被害はなかった[※9]。

両方の攻撃はともに、イランによるものと考えられている。2020 年 5 月には、イラン最大の港であるシャヒード・ラジャーイー港の船舶、トラック、商品の流れを管理するコンピュータがサイバー攻撃を受けてシャットダウンする事態が発生した。これはイスラエルによる報復攻撃とされている[※10]。更に 12 月には、イランのハッキンググループが、イスラエルの再生水貯水池の監視制御システムの HMI（Human-Machine Interface）にアクセスするハッキング動画を公開した。ハッキングによる影響は明らかになっていないが、攻撃者は、貯水池の制御システムに簡単にアクセスし、水圧や温度等のシステム内の値を任意に変更することができた[※11、12]。これらの攻撃の応酬は、イスラエルとイランの国家間のサイバー戦争の様相を呈している。

2020 年 10 月 12 日、インドのムンバイで大規模停電が発生した。停電はムンバイ都市圏に影響を与え、交通管理システムや列車の運行に大きな混乱をもたらし、必要不可欠なサービスの復旧には 2 時間を要した。電力会社や送電会社のサーバへの複数の不審なログインが発見され、これらのサーバが操作されたことが、停電の引き金になったと考えられている。また、電力網の運用を監視、スケジューリングして配電する負荷分散センターの調査員がウイルスを発見したとも報じられている[※13]。

2021 年 2 月 5 日、米国フロリダ州ピネラス郡オールズマー市の浄水場がサイバー攻撃を受けた。攻撃者はリモートアクセスソフトウェアである TeamViewer を介して、SCADA システムにアクセスしたと考えられる。約 5 分間のアクセス中に、攻撃者は水酸化ナトリウムの投入設定値を約 100ppm から 1 万 1,100ppm に変更したが、監視していたオペレータが操作されていることに気付き、すぐに正常な値に戻した。水酸化ナトリウムは液体排水管クリーナーの主成分で、浄水場では水の酸性度をコントロールしたり、飲料水から金属を除去したりするために使用されている。浄水場のすべてのコンピュータの OS は、2020 年 1 月にサポートが終了した Windows 7 で、リモートアクセスに共有パスワードが使われていた[※14]。

(2) IT システムのウイルス感染によって生産や重要サービスが停止した事例

IT と OT の統合が進んでいることから、メールや Web サイト経由の IT システムのウイルス感染が制御システムまで拡大する例や、IT システムの感染から間接的に制御システムが影響を受け、生産ラインや重要サービスが停止する事例が増えている。

表 3-1-1（次ページ）に、2020 年に公にされた、IT システムのウイルス感染によって生産や重要サービスが停止したインシデント事例を示す。

「制御システムは IT システムの影響を受けない」という認識を見直し、攻撃や感染が IT から OT へ広がらないか等、IT、OT 個別の縦割りのリスク管理体制を越えた横断的なリスクの見直しが推奨される。

(3) 制御システムを標的としたランサムウェアによる攻撃事例

2019 年 12 月中旬、制御システムをも標的としたランサムウェア「SNAKE」（別名、EKANS）が新たに出現したが[※24]、ロシアのセキュリティベンダによると、2020 年には多くの企業が同ランサムウェアによる標的型攻撃を受けた[※25]。

2020 年 6 月、本田技研工業株式会社が SNAKE によるものと思われるサイバー攻撃を受けた。社内サーバが攻撃され、同社ネットワークを介してウイルスが拡散し、サーバ、メール、その他のシステムへのアクセスができなくなり、国内外の生産拠点の操業に影響が出た[※26]。

また、同日アルゼンチンの電力会社 Edesur SA（イタリアの多国籍エネルギー企業 Enel SPA の子会社）も、同様の攻撃を受けた。Enel SPA は、同年 10 月にもランサムウェア NetWalker による二度目の攻撃を受け、約 5T バイトのデータを攻撃者に窃取された[※27]。

SNAKE 等、一部のランサムウェアは、ファイルの暗号化といったランサムウェアの機能、データの削除といっ

事例名	発生国	発生年月（報道年月）	影響・被害	内容（原因等）
紡織機械製造企業の生産停止※15	ベルギー	2020年1月	紡織機械製造企業Picanolのベルギー、ルーマニア、中国の工場が約1週間生産停止した。ブリュッセル証券取引所の同社株式が、約3週間売買停止された。	ランサムウェアによる攻撃
天然ガス圧縮施設の停止※16	米国	2020年2月	天然ガス圧縮施設のITシステム及び制御システムがランサムウェアに感染し、2日間停止した。	不正なリンクを含むフィッシングメールによって、ITネットワークがウイルスに感染。制御システムを狙った攻撃ではなかったが、被害に遭った施設のITネットワークとOTネットワークの分離が不十分であったため、OTネットワークのWindowsベースの機器が感染
大手鉄鋼企業の生産停止※17	米国 カナダ	2020年3月	鉄鋼企業Evraz PLCの米国、カナダの複数の鉄鋼生産工場が稼働停止した。	ランサムウェアRyukによる攻撃を受け、ITシステムをシャットダウン
大手鉄鋼企業の製造システムの停止※18	オーストラリア	2020年5月	鉄鋼企業BlueScope Steel Limitedの全社の製造システムが停止した。手動操作に切り替えられた溶鉱炉も停止した。	従業員がメールの添付ファイルを開いたことでウイルスに感染
家電メーカの工場の稼働停止※19	ニュージーランド	2020年6月	家電メーカFisher & Paykel Appliances Holdings Limitedの製造及び流通に影響した。工場が稼働を停止した。	ランサムウェアNefilimによる攻撃。発覚後、すぐにITシステムをシャットダウン
半導体製造企業の生産停止※20	ドイツ	2020年7月	半導体製造企業X-FABの六つの製造拠点（ドイツ3拠点、米国、フランス、マレーシア）の生産が停止した。	ランサムウェアMazeによる攻撃
半導体製造企業の生産停止※21	イスラエル	2020年9月	半導体製造企業Tower Semiconductor Ltd.の一部の製造施設の操業が停止した。	ランサムウェアによる攻撃
大手鉄鋼企業の生産停止※22	カナダ	2020年10月	攻撃の範囲は限定的だったが、鉄鋼企業Stelco Holdings Inc.は予防措置として鉄鋼生産等、一部の業務を一時的に停止した。	ITシステムを標的としたランサムウェアによる攻撃
オフィス家具メーカの生産停止※23	米国	2020年10月	オフィス家具メーカSteelcase Inc.で攻撃の影響を受けたすべてのシステムと関連業務が約2週間、停止した。工場での製品の生産はすべて停止した。	ITシステムを標的としたランサムウェアRyukによる攻撃

■表3-1-1　2020年に公にされたITシステムのウイルス感染によって生産や重要サービスが停止したインシデント事例

た破壊型（ワイパー型）ウイルスの機能に加えて、特定の制御システムのプロセスを強制停止するように設計されている。従って、制御システムの所有者及び運用者は、こうした破壊型ウイルスの攻撃対象や感染する仕組みを理解した上で、防御策を講じることが強く推奨される（ランサムウェアの巧妙化については「1.2.2 新たなランサムウェア攻撃」参照）。

(4) ネットワーク管理用のソフトウェアの脆弱性に端を発する大規模な感染事例

2020年12月、ロシアが関連していると見られるハッキンググループが、米国のSolarWinds Worldwide, LLC.（以下、SolarWinds社）を攻撃し、同社のネットワーク集中監視・管理用のソフトウェアプラットフォームOrionの更新版に「Sunburst」（別名、Solorigate）と呼ばれるウイルスを混入させたことによって、世界中の多くの企業や政府機関のネットワークが感染したことが明らかとなった※28。その後の調査によると、最初の不正アクセスは2019年9月に発生し、Orionの10月の更新版で攻撃コードのテストが実施され、2020年2月からSunburstが仕込まれた更新版が展開されていた※29。そして5月から、「Teardrop」及び「Raindrop」と呼ばれるウイルス※30を使った本格的な攻撃が開始された。この間、SolarWinds社のOrionを使用していた政府機関や大手企業、セキュリティ企業は不正な挙動を検出することができなかったが※31、サイバーセキュリティ企業FireEye, Inc.が2020年12月に不正アクセスを受け、同社の多要素認証ソリューションに不正な端末登録が行われたという警告がきっかけで、この侵害が発覚した※32。

約1万8,000の同製品ユーザが、ウイルスが混入したバージョンをインストールしており、ロシアのセキュリティベンダの調査結果によると、20以上の産業部門の組織が攻撃を受けた可能性がある。その内訳は、製造業8、輸送及びロジスティクス6、ユーティリティ（電力・ガス・

水道等の公共サービス提供組織）4、建設 4、鉱業 3、エネルギー 2、で、地理的な分布は、北米からアジア太平洋まで、ほぼ全世界に及んでいた※33。米国国土安全保障省（DHS：Department of Homeland Security）のサイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA：Cybersecurity and Infrastructure Security Agency）の警告によると、米国の重要インフラ組織への侵害も確認されている※34。また、その後、同ソフトウェアのバグを悪用して、中国との関係が疑われるハッキンググループが、米国政府のコンピュータに侵入していたことも明らかになっている※35。

事業者は所有するソフトウェア及びハードウェア資産を常に正確に把握・管理し、所有資産の脆弱性に関する情報を収集して、新たな脅威に備える必要がある。

(5) USB メモリやパソコンを接続することによるウイルス感染の増加

業務用に持ち込んだ USB メモリやパソコンを接続することによるウイルス感染も、継続して発生している。Honeywell International, Inc. のレポート「Honeywell Industrial Cybersecurity USB Threat Report 2020※36」によると、同社が調査した全脅威のうち、制御システムに大きな混乱を引き起こす可能性のある、USB メモリを媒介とするウイルスの脅威は、2018 年の 26%から 59% へと 2 倍以上増加している。

制御システム運用者は、外部から持ち込む情報端末・機器や媒体の管理、及び接続前のウイルスチェックを今一度徹底させることが重要である。また、内部関係者の不正やヒューマンエラーによるリスクを軽減するために、セキュリティ教育や意識啓発等を通じて、従業員の情報リテラシーや情報モラルを向上させることも重要である。

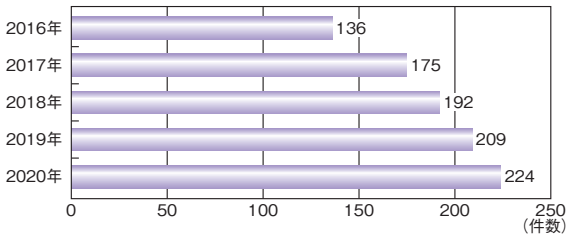
3.1.2 脆弱性及び脅威の動向

本項では、2020 年に見られた、制御システムの脆弱性及び脅威の動向について述べる。

(1) 脆弱性の動向

2020 年も、制御システムの脆弱性が多く公開された。制御システムの脆弱性情報を収集・公開している代表的な組織である米国 DHS の NCCIC（National Cybersecurity and Communications Integration Center）が、2020 年に公開したアドバイザリは 224 件であった。図 3-1-2 に示すように、増加傾向にある。

2020 年に NCCIC から公開された脆弱性で特に目立った傾向は、遠隔から攻撃可能な（Exploitable remotely）脆弱性が 174 件で、77.7%を占めた点である。IIoT（Industrial Internet of Things）機器の導入、クラウドとの接続、新型コロナウイルス感染症（以下、新型コロナウイルス）の感染拡大による遠隔アクセス等の利用拡大に伴い、これらの脆弱性によるリスクが高まっているため、インターネットに直接接続された機器を保護する等の脆弱性対策が重要である。



■図 3-1-2　NCCIC が公開した脆弱性アドバイザリの件数（2016 ～ 2020 年）
（出典）NCCIC の公開情報※37 を基に IPA が作成

非常に影響の大きい脆弱性も発見されている。イスラエルのセキュリティ企業 JSOF Ltd. が、多くの IoT 機器で利用されている米国 Treck, Inc. 製の TCP/IP ソフトウェアライブラリに、リモートでコードが実行可能な複数の脆弱性を発見した※38。「Ripple20」と名付けられたこれらの脆弱性が悪用されると、プリンタからデータが盗まれたり、輸液ポンプの動作が変更されたり、産業用制御機器が誤作動したりと、重要インフラを含む様々な業界で使用される数億個以上もの機器に影響を与える（Ripple20 の詳細については「3.2.2（1）Ripple20」参照）。

また、スペインの産業用サイバーセキュリティ企業 Titanium Industrial Security S.L. は、米 National Instruments Corporation の計測制御システム「CompactRIO」について、攻撃者が遠隔操作によって生産プロセスを混乱させることが可能な脆弱性（CVE-2020-25191※39）を発見した※40。同製品は、重機、製造業、輸送、発電、石油及びガス等の産業分野で使用されており、この脆弱性が悪用されると、生産プロセスが突然停止する可能性がある。米国の CISA は、この脆弱性についてのアドバイザリを発表した※41。

内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）は 2020 年 12 月 3 日、重要インフラ事業者に対し、米国 Fortinet, Inc. の製品の VPN 機能に存

在する脆弱性について、改めて注意を呼びかけた※42。Fortinet, Inc. 製の FortiOS の VPN 機能には、悪用されると、遠隔の第三者が当該製品から任意のファイルを読み込む可能性がある脆弱性（CVE-2018-13379※43）が存在していた。この脆弱性については 2019 年夏ごろより知られていたが、2020 年に入って、この脆弱性の影響を受ける機器や URL のリストがインターネットで公開され、悪用の危険度が増していた。NISC は、公開情報を基に情報収集・分析を行い、重要インフラ事業者等 218 社の VPN 装置、4,954 の IP アドレスが当該脆弱性の影響を受けることを確認し、所管省庁に対して注意喚起を行った（FortiOS の脆弱性を悪用した攻撃については「1.2.5(1)(a)攻撃事例」参照）。

脆弱性が公表された機器の所有者は、脆弱性の影響及び対応の可否を確認し、速やかに必要な対策を実施することが推奨される。

(2) 脅威の動向

2020 年の脅威の動向としては、「3.1.1 (3) 制御システムを標的としたランサムウェアによる攻撃事例」に示したようなランサムウェア攻撃の進化が挙げられる。

産業組織へのランサムウェア攻撃は、2018 年 1 月から 2020 年 10 月までの間に 6 倍に増加している※44。攻撃手法は、無差別にランサムウェアをばらまく攻撃から、特定の企業・組織を狙った「標的型」のランサムウェアへと劇的に進化した。更に、より確実に金銭的な利益を得るために、暗号化したデータの解読の脅迫に加え、標的企業から機密データを窃取し、それを公開すると脅迫して、身代金の支払いを強制する「二重の脅迫」（double extortion）が増えており、2020 年は、ランサムウェア Maze、RagnarLocker、Netwalker、Revil/Sodinokibi 等を使用する攻撃グループがこうした手法を使用していた※45（手口の詳細は「1.2.2 新たなランサムウェア攻撃」参照）。また、ランサムウェア Maze と Revil/Sodinokibi を使用する攻撃グループは、RaaS（Ransomware as a Service）モデルを使用しており、利益の一部を得る見返りにランサムウェアを複数の攻撃グループに提供していた。これによって、経験の浅い攻撃グループが、高度なツールを入手することができた※46。

「二重の脅迫」の事例としては、2020 年 3 月、米国の航空機メンテナンス専門企業 VT San Antonio Aerospace, Inc. が、ランサムウェア Maze を使った攻撃を受けた。攻撃者はサーバを暗号化する前に、1.5T バイト相当のファイルを窃取し、身代金を要求した。また、攻撃の証拠として財務スプレッドシート、サイバー保険契約等の 100 を超えるドキュメントを 4 月に公開した。攻撃者が公開したメモによると、まず侵害した管理者アカウントを使用して、同社のサーバにリモートデスクトップ接続し、次にデフォルトのドメイン管理者アカウントを侵害して、同社の二つのドメインにおいて、ドメインコントローラ、イントラネットサーバ、及びファイルサーバを攻撃した※47。

また、2020 年 5 月には、米国の半導体メーカ MaxLinear, Inc. が、ランサムウェア Maze による攻撃を受けた。同社コンピュータシステムの一部が暗号化され、1T バイト以上のデータが窃取された。その後同社が身代金を支払わなかったことから、攻撃者は 6 月 15 日に、窃取したデータのうち、10.3G バイトの会計・財務情報を公開した。同社が 6 月 16 日に米証券取引委員会に提出した文書によると、出荷、受注処理、及び生産には影響はなかった※48。

ランサムウェアへの対策として、基本的なウイルス対策、通信制御による対策、重要なデータのバックアップが適切に実施されているかの確認、等の感染や脅迫に備えたリスク管理対策を徹底することが推奨される（「1.2.2 (4) 新たなランサムウェア攻撃への対策」参照）。

3.1.3 海外の制御システムのセキュリティ強化の取り組み

本項では、海外における制御システムのセキュリティ強化に関する取り組みについて述べる。

(1) 米国政府の取り組み

米国 DHS の CISA は、2020 年 7 月、制御システムのサイバーセキュリティを強化するための新戦略「Securing Industrial Control Systems: A Unified Initiative※49」を発表した。この戦略の目的は、制御システムコミュニティである事業計画立案者、事業オーナー、オペレータ、ベンダ、インテグレータ、研究者等の、よりセキュアな制御システム運用につながる能力開発の支援であり、最終的には、CISA と制御システムコミュニティが、受動的な ICS セキュリティ対策から、より積極的な対策をとるようになることを目指している。

米国国立標準技術研究所（NIST：National Institute of Standards and Technology）は、製造業界向けのサイバーセキュリティフレームワーク「Cybersecurity Framework Version 1.1 Manufacturing Profile: NISTIR 8183 Revision 1※50」を 2020 年 10 月に公開した（「3.4.2 (4) フレームワーク」参照）。本文書は、製造

業の事業目標と業界のベストプラクティスに沿ってサイバーセキュリティリスクを軽減するためのロードマップとして使用できる。また、サイバーセキュリティ活動を管理し、製造システムに対するサイバーリスクを軽減するためのリスクベースのアプローチを提供している。

(2) 海事業界のセキュリティ

近年デジタル化が進んでいる海事業界でも、VSAT（Very Small Aperture Terminal）衛星通信技術の発達による船舶のインターネット常時接続の普及、船舶の運行データを陸上でモニタリングする等の船舶・陸上間のデータ共有の増加、船舶用機器のコンピュータ化や通信接続に伴い、船舶システムがウイルス感染や不正アクセスといったサイバー攻撃に晒されるリスクが高まっている。サイバーセキュリティ企業のレポートによると、海事業界の OT システムに対するサイバー攻撃は、過去 3 年間で 10 倍増加している※51。

2017 年 6 月の国際海事機関（IMO：International Maritime Organization）の第 98 回海上安全委員会において決議された「安全管理システムにおける海事サイバーリスクマネジメント（Res. MSC.428(98)）※52」では、2021 年 1 月以降、船舶のサイバーリスク対策は、船主・運航者の安全管理システム（SMS:Safety Management Systems）で対応することが強く推奨されている。

2020 年 12 月には、海運業界団体等から、海事サイバーセキュリティに関するガイドラインも公開された。これは、ボルチック国際海運協議会（BIMCO：Baltic and International Maritime Council）、国際海運会議所（ICS：International Chamber of Shipping）、国際乾貨物船主協会（INTERCARGO：International Association of Dry Cargo Shipowners）等の主要な海運業界団体が協力して策定した業界向けサイバーセキュリティガイドライン「The Guidelines on Cyber Security Onboard Ships」の第 4 版である※53。主な特徴として、サイバーリスク管理のベストプラクティスが更新され、リスクとリスク管理の概念が改善されている。

また同年 12 月に、欧州ネットワーク・情報セキュリティ機関（ENISA：EU Agency for Cybersecurity）が、DX（デジタルトランスフォーメーション）と規制強化の中で、欧州の港湾事業者のサイバーリスク管理を支援するためのサイバーセキュリティガイドライン「Guidelines - Cyber Risk Management for Port」を公開した※54。本ガイドラインは、2019 年のレポート「Port Cybersecurity※55」をベースに、欧州の海事部門が直面しているサイバーセキュリティの脅威とデジタル環境の変化に対応した実用的なプラクティスを提供している。

3.1.4 国内の制御システムのセキュリティ強化の取り組み

本項では、制御システムを含む、重要インフラサービスのセキュリティ強化に関する国内の主な取り組みの概要を紹介する。

(1) 日本政府の取り組み

包括的な重要インフラのセキュリティ政策については、「2.1.1 政府全体の政策動向」及び「2.1.2 経済産業省の政策」を参照されたい。ここでは特に、制御システムのセキュリティ強化に関連する取り組みについて触れる。

NISC が、2018 年度の我が国を取り巻くサイバーセキュリティの情勢、及び 2018 年 7 月に発表した「サイバーセキュリティ 2018」に掲げられた具体的な施策の実施状況等をまとめた「サイバーセキュリティ 2020※56」（2019 年度報告・2020 年度計画）を 2020 年 7 月に発表した。本報告の中から、代表的な取り組みを紹介する。

2020 年 4 月、国土交通省の支援のもと、交通機関へのサイバー攻撃に対抗するために、重要インフラ事業者等（航空、空港、鉄道、物流）が情報共有・分析及び対策を連携して行う組織として、一般社団法人交通 ISAC※57 が創設された。

経済産業省は、2020 年 11 月に、IoT や AI によって実現される「Society 5.0※58」及び「Connected Industries※59」における、フィジカル空間とサイバー空間のつながりの信頼性の確保の考え方を整理した「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」を策定した※60。IoT-SSF を活用することにより、フィジカル・サイバー間をつなぐ IoT 機器・システムに潜むリスクを踏まえて、機器・システムのカテゴライズを行い、カテゴリごとに求められるセキュリティ・セーフティ要求の観点を把握し、カテゴリ間で比較することが可能となる。

また、2021 年 2 月、経済産業省の「産業サイバーセキュリティ研究会 WG1」の電力 SWG は、小売電気事業者が各々の事業モデルに適したサイバーセキュリティ対策を実践していくための指針となる「小売電気事業者のためのサイバーセキュリティ対策ガイドライン Ver.1.0※61」を公開した。

(2) IPA の取り組み

2020 年、IPA では制御システムのセキュリティに関し

て、大きく二つの取り組みを行った。

(a) 制御システムのセキュリティリスクアセスメント普及活動

制御システムに対するセキュリティリスクアセスメントの普及を目的として、「制御システムのセキュリティリスク分析ガイド※62」(以下、リスク分析ガイド) を用いてリスク分析手法を解説するオンラインセミナーを 2020 年 9 月と 2020 年 12 月～ 2021 年 1 月の 2 回開催※63 した。同セミナーでは、約 350 社・団体からの受講者が、リスク分析ガイドを解説した合計約 3 時間の講義動画の視聴や、電子メールによる質疑応答を行った。また、過去数年間にわたって実施している重要インフラのリスク分析支援事業を、2020 年度は新電力分野及び物流分野に対して実施した。

また、「制御システム関連のサイバーインシデント事例シリーズ」を 2019 年 7 月以降、順次公開しており、2020 年は、事例 4 ～事例 7 を公開した※64 (表 3-1-2)。本シリーズでは、過去のインシデント事例の概要と攻撃の流れ (攻撃ツリー) を紹介しており、制御システム保有事業者は、リスク分析ガイドで提唱している「事業被害ベースのリスク分析※65」を実施する際に、事例に相当する攻撃ツリーの作成、セキュリティ対策の策定に活用することができる。

(b) 制御システムのサイバーセキュリティ人材の育成

2017 年 4 月に発足した産業サイバーセキュリティセンター (ICSCoE : Industrial Cyber Security Center of Excellence) では、模擬プラントを用いた演習や、攻撃防御の実践経験、最新のサイバー攻撃情報の調査・分析等を通じて、社会インフラ・産業基盤のサイバーセキュリティリスクに対応する人材の育成を支援している (「2.3.2 産業サイバーセキュリティセンター」参照)。2020 年は、リスク分析ガイドの演習付き講義 (3 日間) を、中核人材育成プログラム 4 期生に対して実施した。

No.	表題	内容	被害
1	2015 年ウクライナ大規模停電	制御端末の外部からの遠隔操作	大規模長時間停電
2	2016 年ウクライナマルウェアによる停電	マルウェアによる遮断器の操作	大規模停電
3	2017 年安全計装システムを標的とするマルウェア	安全計装機器への攻撃スクリプト送信	制御システムの停止
4	Stuxnet : 制御システムを標的とする初めてのマルウェア	USB メモリとゼロデイ脆弱性を利用した破壊工作	遠心分離機の破壊
5	2019 年ランサムウェアによる操業停止	情報系を中心としたシステム破壊	生産量の激減
6	2018 年 半導体製造企業のランサムウェアによる操業停止	ランサムウェアに感染した新規導入機器からの感染拡大と暗号化	製造システムの操業停止
7	2020 年 医療関連企業のランサムウェアによる業務停止	電子カルテサーバからのデータ窃取	業務停止と患者の個人情報の漏えい

■表 3-1-2 「制御システム関連のサイバーインシデント事例」シリーズ

COLUMN

自動車が守るべきセキュリティ基準

自動車は非常によくできた工業製品で、自動車に備わる機能そのものの問題で深刻な事故につながることは、滅多にないものです。これは自動車産業界挙げて技術の蓄積や安全基準遵守に取り組み、危険の芽をことごとく摘み取り、改善してきた賜物ですが、近年は潮目が変わってきました。「悪意のサイバー攻撃」により、自動車のセキュリティが脅かされ、自動車の機能そのものに悪影響を与えて安全が脅かされる事態が現実になってきたためです。

最近の自動車は、ソフトウェアで制御されている車載部品や通信経路が非常に多く、サイバー攻撃を受ける可能性が高まっています。外部と情報通信を行うコネクテッドカーや高度な自動運転を目指す流れともあいまって、自動車を制御する車載システムのセキュリティは、今どきの自動車のいわば「アキレス腱」になりました。こうした背景により、業界全体で自動車のセキュリティを確保するための検討を行う機運が高まり、この際、世界の英知を集め、国際的なセキュリティの標準や規格を定め、みんなでセキュリティをしっかりと確保していこう、という動きが盛んになっています。

主な動きの一つが、国連の欧州経済委員会（UNECE）のもとに組織された自動車基準調和世界フォーラム（WP29）の自動運転専門分科会（GRVA）の専門家会議による国際的なサイバーセキュリティ規則（UNR）の策定です。2020 年 6 月、WP29 により自動車へのサイバー攻撃対策を義務付ける指針が採択されました。我が国における自動車の開発や販売に際しても、今後、自動車メーカ・自動車部品メーカが遵守すべきサイバーセキュリティの法規の指針となるもので、これを遵守していかないと世界各地で車両の型式認定の相互承認がうまくいかず、自動車を販売することが難しくなりそうです。

動きをもう一つ挙げるなら、国際標準化機構（ISO）と自動車技術者協会（SAE）のジョイントビジネスによる自動車セキュリティの国際標準規格 ISO/SAE 21434 の策定でしょうか。こちらは、車載システムだけでなく、ネットワークでつながる外部のシステムまでも対象とした幅広いサイバーセキュリティ対策全般についての規格で、WP29 の規則でも具体的な実施要件としてこの規格を参照することになっています。この国際規格は、自動車製造時のセキュリティへの配慮だけでなく、サプライヤーを含めたサプライチェーン全体の組織としての認証や、車両のライフサイクル全般の活動にも言及し、ソフトウェアアップデート等、運用フェーズのシステムの脆弱性管理等についても対策が要求されています。

今後も、いろいろなアップデートが予想される自動車のセキュリティ基準の動向に注目しましょう。

3.2 IoTの情報セキュリティ

IoT（Internet of Things）技術の普及とともに、インターネット接続機能を有するコンピュータ以外の機器（IoT 機器）がサイバー攻撃の対象となり、10 年以上が経過した。新型コロナウイルス感染拡大に伴い、2020 年は新しい生活様式やテレワークを狙うサイバー攻撃が目立った反面、IoT のセキュリティ脅威に関する報道や情報公開は減少傾向にあった。しかしながら、IoT に対する脅威は継続的に存在しており、ゼロデイ脆弱性を感染手段に取り入れる等、攻撃手法の悪質化が進んでおり、脅威の深刻さを正しく理解して対策を推進する必要がある。

本節では、IoT に対する脅威の動向、IoT セキュリティのサプライチェーンリスク、脆弱な機器とウイルス感染の実態、セキュリティ対策強化の取り組みについて述べる。

なお、本節中で記載されている脆弱性のうち、脆弱性データベースの登録 ID を記載しているものについては、表 3-2-1 に記載の各データベースで検索することによって、概要、詳細情報、関連情報へのリンク等を確認できる。

登録 ID の表記例	登録先データベース
CVE-20xx-xxxxx	NVD※66
JVNDB-20xx-xxxxxx	JVN iPedia※67
EDB-ID: xxxxx	Exploit Database※68

■表 3-2-1　脆弱性の登録 ID の表記例と登録先データベース

3.2.1 継続するIoTのセキュリティ脅威

「情報セキュリティ白書 2020」の本節では、IoT 機器に感染するウイルスを「機器乗っ取り型ウイルス」「機器保護型ウイルス」「機器破壊型ウイルス」の 3 種類に分類し、各分類のウイルスの状況を解説した。2020 年は、機器保護型ウイルスと機器破壊型ウイルスについて、目立った活動は見られなかった。一方、Mirai 及び Gafgyt に代表される機器乗っ取り型ウイルス※69 に関しては、新たな脆弱性の攻撃コード（PoC※70）を取り込み、様々な亜種・新種が発生している。

本項では、2020 年に発生した機器乗っ取り型ウイルスに関して、以下の報告について、時系列（一部例外を除き情報公開順）に沿って紹介する。

- IoT 機器に感染するウイルスや、ウイルスに感染した IoT 機器で構成されたボットネットの検知・検出
- 特定の IoT 機器の脆弱性を狙う攻撃活動・感染拡大活動の観測
- 上記サイバー攻撃に悪用可能な IoT 機器の脆弱性の発見

(1) TVT 社製 NVMS-9000 の脆弱性を狙う Mirai の亜種

2019 年 12 月 28 日から 2020 年 2 月 5 日にかけて、Mirai の亜種と考えられるウイルスによる TCP ポート番号 4567 へのアクセスの増加が観測された※71。アクセスの中には、Shenzhen TVT Digital Technology Co., Ltd.（深圳市同为数码科技股份有限公司。以下、TVT 社）製のデジタルビデオレコーダー（DVR：Digital Video Recorder）である NVMS-9000 及びその OEM 製品が有する脆弱性に対する攻撃コード※72 が含まれていた。攻撃コードに示す手順に従ってリモートから文字列を送信すると、ID とパスワードを含む設定ファイルを返す脆弱性が存在しており、認証情報を窃取しようと試みる攻撃であった。同機種には、リバースシェル※73 を用いてリモートコードを実行可能な脆弱性も存在しており、2019 年 10 月以降、この脆弱性の悪用を試みるアクセスが観測されていた※74。TVT 社は、2018 年 4 月にファームウェアの更新を呼びかけていた※75 が、適用せずにウイルス感染した機器が確認された。TVT 社製 DVR には 70 社以上の OEM 先が存在しており※76、世界中に感染対象機器が散在していると考えられる。

(2) PixelStor5000 の脆弱性を狙う Mirai の亜種「SORA」「UNSTABLE」

2020 年 2 月 5 日、Rasilient Systems Inc. 製の監視ビデオカメラ用ストレージシステム PixelStor5000 の非認証リモートコード実行の脆弱性（CVE-2020-6756（JVNDB-2020-001330））の悪用を試みる Mirai の亜種が発見され、「SORA」「UNSTABLE」と名付けられた※77。これらの新しい亜種は、従来の亜種と同様に、以下の脆弱性の悪用を試みる。

- CVE-2017-17215（JVNDB-2017-013014）：Huawei Technologies Co., Ltd 製ホームルータ HG532 の任意のコード実行の脆弱性
- CVE-2018-10561（JVNDB-2018-004885）：DASAN

Networks, Inc. 製 GPON ルータの認証回避の脆弱性

更に、「UNSTABLE」は、以下の脆弱性の悪用を試みるとともに、UPX 圧縮を用いて実行バイナリのサイズを縮小し、検出を回避することを試みていた。

- EDB-ID: 45978：Web アプリケーションフレームワーク「ThinkPHP 5.0.23/5.1.31」を用いた各機器の任意のコード実行の脆弱性

(3) Zyxel 社製 NAS の脆弱性を狙う Mirai の亜種「Mukashi」

2020 年 3 月 19 日、Zyxel Networks Corporation（合勤科技股份有限公司。以下、Zyxel 社）製 NAS（Network Attached Storage）のコマンドインジェクションの脆弱性（CVE-2020-9054（JVNDB-2020-001758））を狙う Mirai の亜種が発見され、「Mukashi」と名付けられた※78。悪用が極めて容易な脆弱性であり、同年 2 月 24 日から 3 月 11 日にかけて、Zyxel 社からアドバイザリが公開・更新されている※79。

(4) LILIN 社製 DVR のゼロデイ脆弱性を狙う攻撃

2020 年 3 月 20 日、Merit LILIN Ent. Co., Ltd.（利凌企業股份有限公司。以下、LILIN 社）製 DVR のゼロデイ脆弱性の悪用を試みるボットネットの情報が公開された※80。このゼロデイ脆弱性は、以下に示す 3 種類の脆弱性からなる。

- ハードコーディングされた認証情報（root/icatch99、report/8Jg0SE8K50）
- NTP 時刻同期コマンド NTPUpdate におけるコマンドインジェクションの脆弱性
- 設定ファイル中の FTP パラメータ及び NTP パラメータ改ざんによるコマンドインジェクションの脆弱性

2019 年 8 月 30 日、Mirai の亜種「Chalubo※81」による悪用で存在が認識されたこの脆弱性は、2020 年 1 月 11 日に Mirai の亜種「fbot※82」、同月 26 日に Mirai の亜種「Moobot※83」による悪用が確認され、LILIN 社に報告された。2020 年 2 月 13 日、LILIN 社は脆弱性を解消した更新ファームウェアを公開した※84。

(5) Xiongmai 社製 DVR/NVR のゼロデイ脆弱性を狙う攻撃

2020 年 2 月 11 日以降、Mirai の亜種と考えられるウイルスによる TCP ポート番号 9530 へのアクセスの増加が観測された※85。アクセスの中には、HiSilicon Technology Co., Ltd.（海思半导体有限公司）製 SOC チップセットと Hangzhou Xiongmai Technology Co., Ltd.（杭州雄迈信息技术有限公司。以下、Xiongmai 社）製ファームウェアを用いた DVR ／ネットワークビデオレコーダー（NVR：Network Video Recorder）及びその OEM 製品が有する脆弱性に対する攻撃が含まれていた。TCP ポート番号 9530 宛に「OpenTelnet:OpenOnce」という文字列を送信し、所定の応答を行うことで telnet を起動して外部からバックドアとして悪用可能となっており、2 月 4 日にゼロデイ脆弱性として公開されていた※86。2 月 20 日、Xiongmai 社は脆弱性情報を含むアドバイザリを公開した※87。インターネット接続機器検索サービス Shodan※88 を用いて当該機器を調査したところ、2020 年 3 月 23 日時点で全世界に約 26 万台が存在しており、うち約 1,900 台は日本国内であると報告されている※89。当該機器は、telnet を有効化した後、既知の認証情報の初期値（表 3-2-2）を用いたブルートフォース攻撃でログインし、外部から DVR/NVR に記録された映像データに不正アクセス可能となっていた。

ユーザ名	パスワード
root	xmhdipc
root	klv123
root	xc3511
root	123456
root	jvbzd
root	hi3518

■表 3-2-2　Xiongmai 社製 DVR/NVR の認証情報の初期値
（出典）Habr「Full disclosure: 0day vulnerability (backdoor) in firmware for Xiaongmai-based DVRs, NVRs and IP cameras※86」を基に IPA が編集

(6) DrayTek 社製ルータのゼロデイ脆弱性を狙う攻撃

2020 年 3 月 27 日、DrayTek Corporation（居易科技中国分公司。以下、DrayTek 社）製ブロードバンドルータの 2 種類のゼロデイ脆弱性の悪用を試みるボットネットの情報が公開された※90。これに先立ち、2019 年 12 月 4 日、DrayTek 社製 Vigor エンタープライズルータのコマンドインジェクションの脆弱性（認証処理において暗号化されたユーザ名とパスワードを復号する際のパラメータのフィルタリング漏れ）を狙う攻撃が検出され、同月 25 日、ゼロデイ脆弱性に対する攻撃として情報公開された。2020 年 1 月 28 日、同ルータのもう一つのコマンドインジェ

クションの脆弱性を狙う攻撃が検出された。2月1日、NVDにおいてCVE-2020-8515として脆弱性情報が公開された。2月6日、DrayTek社は脆弱性を解消した更新ファームウェアを、同月10日、本脆弱性に関するアドバイザリを公開した※91。

当該ルータには、その後も新たな脆弱性が発見されており、DrayTek社は4月8日、6月24日、2021年1月8日にアドバイザリを公開している※92。

(7) Gafgytの亜種「Hoaxcalls/XTC」

2020年4月3日、Gafgytの新たな亜種が発見され、C&Cサーバ※93との通信に用いるIRC※94チャネル名から「Hoaxcalls」と名付けられた※95。Hoaxcallsは、3月31日に攻撃コード※96が公開されたDrayTek社製ルータの脆弱性（CVE-2020-8515（JVNDB-2020-001735）、(6)参照）や、Grandstream Networks, Inc.製IP電話交換機Grandstream UCM6200のSQLインジェクションの脆弱性（CVE-2020-5722（JVNDB-2020-003190））を感染拡大に悪用する。

2020年4月20日、Hoaxcallsの亜種が発見された※97。この亜種は、3月9日に公開された※98、Zyxel社製Cloud CNM SecuManagerにおける非認証リモートコード実行の脆弱性（CVE-2020-15348（JVNDB-2020-007350）、CNVD-2020-16839※99）を攻撃対象に追加していることが判明した。Zyxel社は3月13日に本脆弱性を含む複数の脆弱性の存在を認めた※100が、日本国内においても4月12日以降、本脆弱性を狙ったTCPポート番号9673へのアクセスが観測されている※101。

2020年4月24日、Hoaxcallsの更なる亜種が発見された※102。3月26日に詳細が公開されたSymantec Corporation（現、Broadcom Ltd.）製Symantec Secure Web Gateway 5.0.2.8（ライフサイクル及びサポートの終了した旧製品）の認証後リモートコード実行の脆弱性※103を攻撃対象として追加するとともに、感染機器のリモートコントロール機能が強化されている。

なお、Hoaxcallsは、攻撃時のHTTP通信で用いるUser-Agentの値から「XTC」とも命名されており※104、5月以降も引き続き活発な活動が観測されている※105。

(8) Netlink社製GPONルータのゼロデイ脆弱性を狙う攻撃

2020年4月15日、Netlink ICT Pvt Ltd.（以下、Netlink社）製GPONルータのゼロデイ脆弱性の悪用を試みるMiraiの亜種Moobot及びGafgytの亜種によって構成されたボットネットの情報が公開された※106。これに先立ち、2020年2月28日、Moobotによる未知のエクスプロイトを用いた感染拡大の試みが検出され、3月17日、Netlink社製ルータのゼロデイ脆弱性を狙った攻撃であると認識された後、翌18日、Exploit Databaseにおいて、リモートコード実行の脆弱性（EDB-ID: 48225）として、攻撃コードとともに公開された。その後、3月19日には同攻撃コードのGafgytの亜種への取り込み、同月26日、Gafgytボットネットによるスキャン活動も検出されている。この時点において、Netlink社及び9社のOEM製品が感染対象となることが確認されている。

また、3月25日、公開後の同脆弱性を狙うMiraiの新たな亜種が発見され、亜種の命名に用いられるウイルスのファイル名には「rispek」の文字列が含まれていた※107。

(9) Moobotの亜種「LeetHozer」

2020年4月27日、Miraiの亜種Moobotを更に発展させたと考えられる新たなウイルス「LeetHozer」の情報が公開された※108。3月26日に発見されたLeetHozerは、Xiongmai社製ファームウェアを持つDVR/NVR等を攻撃対象としており、独自の暗号化方式や接続経路を匿名化するTor（The Onion Router）ネットワーク上のC&Cサーバとの通信機能を有する。

(10) D-Link社製ルータDIR-865Lの脆弱性

2020年2月28日、D-Link Corporation（友讯科技股份有限公司。以下、D-Link社）製ルータDIR-865Lの以下に示す6種類の脆弱性が発見されてD-Link社に報告された後、同年6月12日に情報が公開された※109。

- CVE-2020-13782（JVNDB-2020-006052）：コマンドインジェクションの脆弱性
- CVE-2020-13783（JVNDB-2020-006053）：情報漏えい（管理者パスワードの平文保存）の脆弱性
- CVE-2020-13784（JVNDB-2020-006054）：予測可能なseedを用いた疑似乱数生成の脆弱性
- CVE-2020-13785（JVNDB-2020-006038）：不十分な暗号強度（パスワードのブルートフォース攻撃に悪用可能な情報を平文のまま送信）の脆弱性
- CVE-2020-13786（JVNDB-2020-006039）：クロスサイトリクエストフォージェリの脆弱性
- CVE-2020-13787（JVNDB-2020-006040）：情報漏えい（パスワードを平文のまま送信するWEP（Wireless

Equivalent Privacy）を実装）の脆弱性

DIR-865L は 2016 年 1 月にライフサイクル及びサポート終了となっていたが、2020 年 5 月 26 日、D-Link 社は脆弱性を解消する更新ファームウェアを公開した※110。

（11）DrayTek 社製ルータを狙う新種「Bigviktor」

2020 年 6 月 17 日、DrayTek 社製 Vigor ルータの脆弱性（（6）参照）を狙う新たなウイルスが発見された※111。ファイル名に用いられた文字列「viktor」と検体中の特別な文字列「big boobs」から「Bigviktor」と名付けられた。Bigviktor は、ドメイン生成アルゴリズム（DGA：Domain Generation Algorithm）を用いて毎月 1,000 個の C&C サーバのドメイン名を生成してドメインを切り替え、C&C サーバの検出を困難とする。また、電子署名を付与したペイロードを JPEG 画像ファイルに偽装して、C&C サーバとの間で通信を行う。

（12）Comtrend 社製ルータ VR-3033 の脆弱性を狙う Mirai の亜種

2020 年 7 月 8 日、Comtrend Corporation（康全電訊股份有限公司。以下、Comtrend 社）製ルータ VR-3033 の OS コマンドインジェクションの脆弱性（CVE-2020-10173（JVNDB-2020-002596））の悪用を試みる Mirai の亜種が発見された※112。この脆弱性は、同年 2 月 27 日に脆弱性情報とともに攻撃コードが公開されていた（EDB-ID: 48142）が、今回初めて悪用が観測された。この亜種は、典型的な認証情報を用いた telnet と Secure Shell（SSH）に対するブルートフォース攻撃に加えて、以下の脆弱性の悪用も確認されている。

- EDB-ID: 48225（（8）参照）
- CVE-2018-17173（JVNDB-2018-010306）：LG SuperSign CMS のリモートコード実行の脆弱性
- EDB-ID: 31683：Linksys E-Series ルータのリモートコード実行の脆弱性
- EDB-ID: 40500：AVTECH Corporation（以下、AVTECH 社）製ネットワークカメラ／ NVR ／ DVR の複数の脆弱性
- EDB-ID: 27044：D-Link デバイスの UPnP SOAP コマンド実行の脆弱性
- EDB-ID: 41471：MVPower DVR のシェルコマンド実行の脆弱性
- CVE-2020-15348（（7）参照）
- EDB-ID: 45978：ThinkPHP 5.0.23/5.1.31 のリモートコード実行の脆弱性

（13）Tenda 社製 AC1900 ルータ AC15 の脆弱性

2020 年 7 月 11 日、Shenzhen Tenda Technology Co.,Ltd.（深圳市吉祥腾达科技有限公司。以下、Tenda 社）製 AC1900 ワイヤレスルータ AC15 の脆弱性についての情報が公開された※113。これに先立ち、同年 1 月 2 日、発見者は Tenda 社に連絡した後、同月 17 日、以下に示す 5 種類の脆弱性の詳細を報告した。

- CVE-2020-10986（JVNDB-2020-007725）：クロスサイトリクエストフォージェリの脆弱性
- CVE-2020-10987（JVNDB-2020-007726）：インジェクションの脆弱性
- CVE-2020-10988（JVNDB-2020-007727）：ハードコーディングされた認証情報の脆弱性
- CVE-2020-10989（JVNDB-2020-007728）：クロスサイトスクリプティングの脆弱性
- CVE-2020-15916（JVNDB-2020-008663）：OS コマンドインジェクションの脆弱性

Tenda 社が報告を無視したため、発見者は半年後に脆弱性の詳細を公開した。

（14）F5 社製ロードバランサ BIG-IP の脆弱性を狙う「SORA」の亜種

2020 年 7 月 11 日、F5, Inc.（以下、F5 社）製ロードバランサ BIG-IP の脆弱性（CVE-2020-5902（JVNDB-2020-007318））を悪用して感染を試みるウイルスが発見された※114。ウイルスのファイル名から「SORA」（（2）参照）の亜種と考えられる。7 月 1 日に BIG-IP の管理インタフェース TMUI（Traffic Management User Interface）に存在するリモートコード実行の脆弱性が公開されており、F5 社はソフトウェア更新の呼びかけを含むアドバイザリを公開していた※115。この亜種では、以下の脆弱性の悪用も確認されている。

- CVE-2020-1956（JVNDB-2020-008140）：Apache Kylin の OS コマンドインジェクションの脆弱性
- CVE-2020-7115（JVNDB-2020-006059）：Aruba ClearPass Policy Manager の非認証リモートコード実行の脆弱性
- CVE-2020-10173（（12）参照）
- CVE-2020-7209（JVNDB-2020-002007）：HP LinuxKI

のリモートコマンドインジェクションの脆弱性

- CVE-2020-10987（（13）参照）
- CVE-2020-10204（JVNDB-2020-003570）：Sonatype Nexus Repository Manager のリモートコード実行の脆弱性
- EDB-ID: 48225（（8）参照）
- Netgear R7000 ルータのリモートコード実行の脆弱性※116
- EDB-ID: 48646：Sickbeard のリモートコマンドインジェクションの脆弱性

（15）ZeroShell の脆弱性を狙う攻撃

2020 年 7 月 16 日以降、Linux ディストリビューションの一つであり、サーバや組み込み機器用ネットワークサービスとしてルータやファイアウォール機能を提供する ZeroShell の脆弱性を狙う攻撃が観測された※117。以下に示す脆弱性を攻撃対象としており、Mirai の亜種による感染活動と考えられる。

- CVE-2019-12725（JVNDB-2019-006591）：ZeroShell 3.9.0 の OS コマンドインジェクションの脆弱性
- CVE-2009-0545（JVNDB-2009-005813）：ZeroShell 1.0beta11 及びそれ以前の任意のコマンド実行の脆弱性

（16）ADB ポートを狙う Mirai の亜種

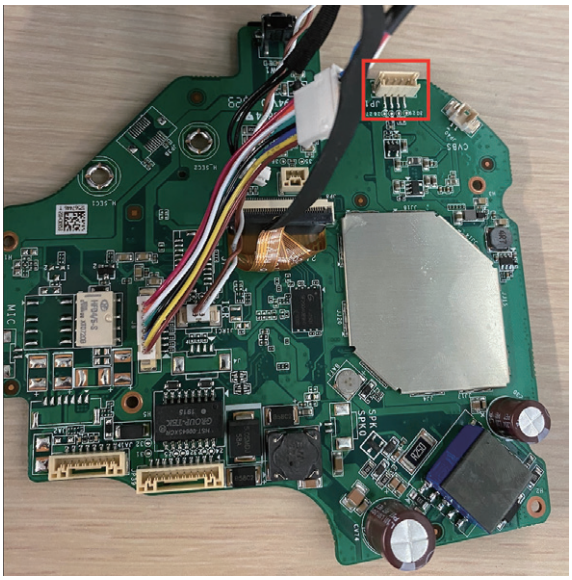
2020 年 7 月 16 日以降、TCP ポート番号 5555 を用いて Android 端末上のコマンド操作を行う ADB（Android Debug Bridge）に対して、特定のコマンドにより外部サーバからシェルスクリプトをダウンロードして実行を試みるアクセスの増加が観測された※118。Mirai またはその亜種と考えられる。ADB ポートを狙った攻撃は 2018 年 2 月 3 日以降観測されるようになった※119 が、再び攻撃が活性化している。

（17）AvertX 社製ネットワークカメラの脆弱性

2020 年 7 月 17 日、AvertX Systems（以下、AvertX 社）製ネットワークカメラ HD838 及び 438IR の脆弱性についての情報が公開された※120。これに先立ち、同年 2 月 24 日、以下に示す 3 種類の脆弱性が発見され、AvertX 社に報告されていた。

- CVE-2020-11623（JVNDB-2020-008740）：公開された危険な機能（UART インタフェースのコネクタが基板上に存在）の脆弱性
- CVE-2020-11624（JVNDB-2020-008828）：脆弱なパスワード要件（管理者アカウントのデフォルトパスワードからの変更が不要）の脆弱性
- CVE-2020-11625（JVNDB-2020-008827）：アカウントの有無によりログイン失敗時の応答が変化し、ユーザアカウントの存在が漏えいする（ユーザ列挙）脆弱性

HD838 及び 438IR は、Hangzhou Hikvision Digital Technology Co., Ltd.（杭州海康威视数字技术股份有限公司）製カメラに変更を加えてブランド名を付け替えた製品であり、AvertX 社は更新ファームウェアを公開した。また、最新製造ロットでは、悪用防止のため基板上から UART コネクタ（図 3-2-1 の赤枠部分）を削除した。



■図 3-2-1　ネットワークカメラの基盤上に設置された UART インタフェースのコネクタ（赤枠部分）
（出典）Palo Alto Networks, Inc.「3 Vulnerabilities Found on AvertX IP Cameras※120」

（18）IoT を狙い始めた「Ngioweb」の亜種

2020 年 8 月 4 日、Ngioweb の亜種が発見された。同月 16 日、x 86（32 ビット／ 64 ビット）、ARM（32 ビット／ 64 ビット）、MIPS（MIPS32 ／ MIPS- Ⅲ）、PPC 等の様々な CPU アーキテクチャ対応に拡張され、IoT 機器も攻撃対象となっていることが確認された※121。Ngioweb は 2019 年 5 月 27 日に初めて発見されたウイルスで、当時は Linux 上で動作する Web サーバを感染対象としていた※122。バージョン V2 と見なされる亜種は、従来のウイルスと比較して、①設定情報の AES 暗号化、② DGA を用いた C&C サーバのドメイン名生成、③ C&C サーバと接続するためのボットネットの入口名を設定ファイル中の記述から選択する、等の特徴を有する。

(19) AVTECH 社製 IP カメラ／ NVR ／ DVR を狙う「Specter」

2020 年 8 月 20 日、AVTECH 社製の IP カメラ／ NVR ／ DVR の複数の脆弱性（EDB-ID: 40500）の悪用を試みる新しいボットネットが発見され、ファイル名に含まれる文字列から「Specter」と命名された※123。Linux 上で動作する IoT 機器を狙ったこのウイルスは、C&C サーバとの通信に TLS 1.2（暗号化アルゴリズム ChaCha20、ハッシュアルゴリズム lz4）を用いて、認証及び暗号化を行う。攻撃手法として高度とは思えない側面（ランタイムライブラリとの動的リンク、メモリへの直接ロード、2016 年 10 月に公開された古い脆弱性の悪用）と、高度な側面（レイヤ設計、複雑なネットワーク通信等）を併せ持っており、開発途中の試験運用ではないかと考えられている。

(20) QNAP 社製 NAS の非公開の脆弱性を狙う攻撃

2020 年 8 月 31 日、QNAP Systems, Inc.（威聯通科技股份有限公司。以下、QNAP 社）製 NAS の非公開の脆弱性の悪用を試みるウイルスの情報が公開された※124。これに先立ち、同年 4 月 21 日以降、非公開の脆弱性（非認証のリモートコマンド実行）を狙う攻撃が観測された後、5 月 13 日に QNAP 社に攻撃コードが報告された。8 月 12 日、QNAP PSIRT（Product Security Incident Response Team）からは「最新版のアップデートで脆弱性は解決済みであるが、未適用機器のインターネット上の存在を確認」との回答が得られた。2017 年 7 月 21 日に脆弱性を解消したファームウェア QTS 4.3.3 が公開されているが、未適用の機器が世界中に散在していると考えられる。

(21) Tenda 社製ルータのゼロデイ脆弱性を狙う「Ttint」

2020 年 10 月 1 日、Tenda 社製ルータのゼロデイ脆弱性の悪用を試みる Mirai の亜種の情報が公開された※125。

これに先立ち、2019 年 11 月 9 日、Tenda 社製ルータのゼロデイ脆弱性を攻撃するウイルスが発見された。感染した IoT 機器を DDoS 攻撃の踏み台に悪用する機能に加えて、ルータの Socket5 プロキシ化、DNS 改ざん、iptables 設定、カスタムシステムコマンド実行等、12 種類の RAT（Remote Access Trojan）機能を実装していた。発見者はこのウイルスによるボットネットを「Ttint」と名付けた。当該のゼロデイ脆弱性は、2020 年 7 月に CVE-2020-10987 として公開された（(13) 参照）。

2020 年 8 月 21 日、Tenda 社製ルータの別のゼロデイ脆弱性（詳細非公開）を攻撃する Ttint の新しい版（v2）が発見された。C&C サーバとの通信に WSS（WebSocket over TLS）プロトコルを用いて、Mirai 型のトラフィック検知を回避しつつ、通信内容を暗号化する機能が拡張されていた。影響を受ける機種は、Tenda 社製ルータ AC9、AC10U、AC15、AC18 等である。脆弱性を有したままインターネットに接続された当該ルータの国別分布を、表 3-2-3 に示す。発見者は 8 月 28 日に脆弱性を攻撃コードとともに報告したが、Tenda 社からは回答は得られていない。

国名	台数
ブラジル	37,967
米国	9,271
南アフリカ	8,847
インド	8,195
ロシア	3,462
中国	3,265
イタリア	2,942

■表 3-2-3　Tenda 社製ルータのゼロデイ脆弱性を有する国別分布
（出典）Qihoo 360 Technology Co., Ltd.「Ttint: An IoT Remote Access Trojan spread through 2 0-day vulnerabilities※125」を基に IPA が作成

(22) P2P プロトコルを用いる自爆機能付き「HEH」

2020 年 10 月 6 日、最近発見された、IoT 機器を狙う未知のウイルスに関する情報が公開された※126。x86（32 ビット／ 64 ビット）、ARM（32 ビット／ 64 ビット）、MIPS（MIPS32 ／ MIPS- Ⅲ）といった様々な CPU アーキテクチャに対応し、ポート番号 23 または 2323 の telnet に対するブルートフォース攻撃を用いて感染拡大を図る。Go 言語で記述されており、独自仕様の P2P プロトコルを用いる。ソースファイルのパス名（プロジェクト名）に「heh」の文字列が用いられていることから、「HEH」と名付けられた。自爆コマンド（コード番号 8）を受信すると、すべてのディスク上の全データを消去する機能が実装されており、証拠隠滅を目的としていると考えられる。

(23) 新しい脆弱性を狙う Mirai の亜種

2020 年 10 月 14 日、IoT 機器の新しい 2 種類の脆弱性と、各々の脆弱性を攻撃する 2 種類ずつ（合計 4 種類）の Mirai の亜種の情報が公開された※127。第一

の脆弱性は、NTP サーバ設定機能を有する Web サービスにおけるコマンドインジェクションの脆弱性（HTTP リクエストのパラメータ NTP_SERVER の値における不十分なサニタイズ※128 処理）で、同年 7 月 23 日から 9 月 23 日にかけて攻撃が観測されていた。

第二の脆弱性は、ある種のリモート管理ツールにおけるコマンドインジェクションの脆弱性（HTTPリクエストのパラメータ pid における不十分なサニタイズ処理）で、8 月 16 日のみ攻撃が観測されていた。

(24) TCP ポート 5501 を狙う Mirai の亜種

2020 年 10 月 20 日以降、TCP ポート番号 5501 への攻撃を試みる Mirai の亜種の活動が観測された※129。海外製 DVR 等への感染を試みる Mirai の亜種と考えられる。

(25) UNIX CCTV 社製 DVR/NVR の脆弱性を狙う「Moobot」の亜種

2020 年 11 月 20 日、UNIX CCTV Corp.（以下、UNIX CCTV 社）製 DVR/NVR のゼロデイ脆弱性（リモートコマンドインジェクション）の悪用を試みる Moobot の亜種に関する情報が公開された※130。これに先立ち、同年 6 月 9 日、ゼロデイ脆弱性を狙うスキャン活動が初めて発見され、同月 24 日、この脆弱性を感染拡大に悪用する Moobot の検体が採取された。感染対象となる DVR/NVR では、ポート番号 8000 でリモート管理機能が有効となっており、システム時間を遠隔更新する際に NTP サーバ名を指定するパラメータのチェック漏れにより、不正なコマンドが実行可能となっていた。インターネット上に約 8,000 台の接続が発見されており、その大半は米国であった。国別分布を表 3-2-4 に示す。8 月 24 日、UNIX CCTV 社は、脆弱性を解消した更新ファームウェアを公開した。

(26) 既知の脆弱性を狙う攻撃の再活性化

2020 年の終わりには、以下のように既知の IoT 機器の脆弱性を狙う攻撃が再活性化した※131。

- 11 月 21 日以降、Huawei Technologies Co., Ltd. 製ルータ HG532 における任意のコード実行の脆弱性（CVE-2017-17215（JVNDB-2017-013014））を狙う Mirai の亜種のアクセスの増加が観測された。
- 12 月 20 日以降、Realtek SDK を用いた IoT 機器における UPnP miniigd SOAP サービスの任意のコード実行の脆弱性（CVE-2014-8361（JVNDB-2014-008039））を狙う Mirai の亜種のアクセスの増加が観測された。
- 12 月 15 日以降、SIA Mikrotīkls 製ルータにおける MikroTik RouterOS の認証に関する脆弱性（CVE-2018-14847（JVNDB-2018-008866））を狙うウイルス Glupteba※132 のアクセス増加が観測された。

国名	台数
米国	4,529
韓国	789
カナダ	84
日本	73
オランダ	66
オーストラリア	56
ドイツ	55
英国	31
ベトナム	23
マレーシア	19
サウジアラビア	15
チェコ	15
スイス	14
中国	11

■表 3-2-4　UNIX CCTV 社製 DVR/NVR のゼロデイ脆弱性を有する国別分布
（出典）Qihoo 360 Technology Co., Ltd.「MooBot on the run using another 0 day targeting UNIX CCTV DVR※130」を基に IPA が作成

3.2.2 IoTセキュリティのサプライチェーンリスク

IoT のセキュリティ対策、特に脆弱性対策を困難としている理由の一つに、IoT 機器のサプライチェーンリスクがある。本項では、2020 年に発生したサプライチェーンに起因する脆弱な IoT 機器の流通事例を紹介する。

(1) Ripple20

2020 年 6 月 16 日、多くの IoT 機器において組み込みソフトウェアとして採用されている Treck, Inc.（以下、Treck 社）製ライブラリの TCP/IP スタックにおいて発見された 19 種類のゼロデイ脆弱性（次ページ表 3-2-5）が報告されるとともに、「Ripple20」と名付けられた※38。脆弱性を有する Treck 社のライブラリは、過去 20 年以上の間、直接的あるいは間接的に世界中で広く利用されており、複数のリモートコード実行の脆弱性を有する IoT 機器が数億台以上存在すると考えられる。脆弱性を発見した JSOF Ltd. は、Treck 社のライブラリを用いた UPS（無停電電源装置）を乗っ取り、UPS に接続され

た輸液ポンプ、プリンタ、照明器具等を誤動作させるデモ動画を公開し、潜在的なリスクの一例を示した※133。

JSOF Ltd. の報告と同日の16日に、DHS傘下のICS-CERTはアドバイザリを公開し、その後も随時情報を更新している※134。

Treck社は、アドバイザリを公開し、最新版への更新を推奨した※135。

1990年代にTreck社と提携していたエルミックシステム株式会社（現、図研エルミック株式会社）製TCP/IPライブラリ「KASAGO」においても、同等の脆弱性が分岐する形で存在しており、6月17日、図研エルミック株式会社は回避策の適用及び修正プログラムの適用を呼びかけた※136。

6月24日、NISCは、ネットワーク製品に組み込まれているライブラリに深刻な脆弱性が発見され、影響範囲が広い反面、特定・対応が容易でないことから、重要インフラ事業者等に向けて、対象製品と対応を含む参考情報を公開した※137。

2020年10月25日の時点で以下の31社の製品に影響が及ぶことが確認されている※38。

- ABB Ltd.
- Aruba Networks（Hewlett Packard Enterprise Co. の一部門）
- AudioCodes Limited
- B. Braun Medical Inc.
- Baxter International Inc.
- Becton, Dickinson and Company（BD）
- ブラザー工業株式会社※138
- Carestream Health, Inc.
- Caterpillar Inc.
- Cisco Systems Inc.
- Dell Inc.※139
- Digi International Inc.
- Eaton Corporation
- Green Hills Software, Inc.
- HCL Technologies Limited
- HP Inc.
- Hewlett Packard Enterprise Co.
- Intel Corporation
- Johnson Controls, Inc.
- MaxLinear, Inc.
- Miele & Cie. KG
- 三菱電機株式会社※140
- Opto 22
- 株式会社リコー※141
- Rockwell Automation, Inc.
- Schneider Electric SE
- Smiths Medical（Smiths Group plc の一部門）
- Telit
- Teradici Corporation
- Xerox Corporation
- 図研エルミック株式会社※136

更に、当該各社の製品をOEM販売している会社や

脆弱性ID	概要
CVE-2020-11896※142 （JVNDB-2020-006776）	リモートコード実行の脆弱性 （CVSS v3 基本値：10）
CVE-2020-11897 （JVNDB-2020-006777）	境界外書き込みの脆弱性 （CVSS v3 基本値：10）
CVE-2020-11898※142 （JVNDB-2020-006778）	情報漏えいの脆弱性 （CVSS v3 基本値：9.1）
CVE-2020-11899 （JVNDB-2020-006779）	境界外読み取りの脆弱性 （CVSS v3 基本値：5.4）
CVE-2020-11900 （JVNDB-2020-006766）	二重解放の脆弱性 （CVSS v3 基本値：8.2）
CVE-2020-11901※143 （JVNDB-2020-006767）	リモートコード実行の脆弱性 （CVSS v3 基本値：9.0）
CVE-2020-11902 （JVNDB-2020-006768）	境界外読み取りの脆弱性 （CVSS v3 基本値：7.3）
CVE-2020-11903 （JVNDB-2020-006763）	境界外読み取りの脆弱性 （CVSS v3 基本値：6.5）
CVE-2020-11904 （JVNDB-2020-006764）	境界外書き込みの脆弱性 （CVSS v3 基本値：7.3）
CVE-2020-11905 （JVNDB-2020-006765）	境界外読み取りの脆弱性 （CVSS v3 基本値：6.5）
CVE-2020-11906 （JVNDB-2020-006758）	整数アンダーフローの脆弱性 （CVSS v3 基本値：6.3）
CVE-2020-11907 （JVNDB-2020-006759）	不特定の脆弱性 （CVSS v3 基本値：6.3）
CVE-2020-11908 （JVNDB-2020-006760）	不特定の脆弱性 （CVSS v3 基本値：4.3）
CVE-2020-11909 （JVNDB-2020-006761）	整数アンダーフローの脆弱性 （CVSS v3 基本値：5.3）
CVE-2020-11910 （JVNDB-2020-006755）	境界外読み取りの脆弱性 （CVSS v3 基本値：5.3）
CVE-2020-11911 （JVNDB-2020-006756）	認証の欠如に関する脆弱性 （CVSS v3 基本値：5.3）
CVE-2020-11912 （JVNDB-2020-006757）	境界外読み取りの脆弱性 （CVSS v3 基本値：5.3）
CVE-2020-11913 （JVNDB-2020-006753）	境界外読み取りの脆弱性 （CVSS v3 基本値：5.3）
CVE-2020-11914 （JVNDB-2020-006754）	境界外読み取りの脆弱性 （CVSS v3 基本値：4.3）

■表3-2-5　Treck社製TCP/IP Stackのゼロデイ脆弱性
（出典）JSOF Ltd.「Ripple20※38」、NVD※66、JVN iPedia※67を基にIPAが作成

自社製品の一部に組み込んでいる会社も含めて、世界中で多くの企業が対応策等の情報公開に追われた。

2020年12月18日、Treck社のTCP/IPスタックにおける4種類の新たな脆弱性が公表された※135。同日、ICS-CERTからアドバイザリが公開されている※145。国内で販売される家電製品等が影響を受け、回避策が公開されている※146。

(2) AMNESIA:33

2020年12月8日、オープンソースとして公開されている4種類のTCP/IPスタック(uIP、FNET、picoTCP、Nut/Net)において発見された33種類の脆弱性が報告されるとともに、「AMNESIA:33」と名付けられた※147。4種類の深刻な脆弱性を含み、150社以上のベンダ、100万台以上のIoT機器に影響を与えるとされている。同日、ICS-CERTはアドバイザリを公開している※148。

(3) サプライチェーンによる影響範囲の拡大

「3.2.1 継続するIoTのセキュリティ脅威」にて紹介した、2020年に発生したIoTのセキュリティ脅威においても、サプライチェーンにより影響範囲が拡大した事例が多く含まれている。

- 複数の会社経由でOEM製品として販売されているIoT機器に脆弱性が発見された例
  該当製品が世界中に拡散している上、エンドユーザは自分が使用している機器がOEM製品であるか否か気付くことが困難である(「3.2.1 (1) TVT社製NVMS-9000の脆弱性を狙うMiraiの亜種」「3.2.1(8) Netlink社製GPONルータのゼロデイ脆弱性を狙う攻撃」「3.2.1 (17) AvertX社製ネットワークカメラの脆弱性」参照)。
- 複数のIoT機器の開発に利用されているハードウェア部品やソフトウェア部品に脆弱性が発見された例
  当該部品を用いた機器が世界中に拡散している上、エンドユーザは自分が使用している機器が該当するか否か気付くことが極めて困難である(「3.2.1 (5) Xiongmai社製DVR/NVRのゼロデイ脆弱性を狙う攻撃」「3.2.1(9)Moobotの亜種『LeetHozer』」「3.2.1(15)ZeroShellの脆弱性を狙う攻撃」参照)。

世界中に同一機種や同等機種が多数散在するIoT機器をウイルス感染対象とすることは、サイバー攻撃者にとっては、容易に多数の機器を侵害することを可能にする。2020年には、このような条件を満たす機器のゼロデイを含む脆弱性を攻撃する傾向が目立った。

サプライチェーンに関わるIoTの脅威として、以下に示す事例も報告されている※149。

- 2020年7月15日、IT企業で発見されたCisco Systems Inc.製ネットワークスイッチCatalyst 2960-Xシリーズの偽物に関する情報が公開された※150。ソフトウェアのアップグレード後に障害が発生したことから、偽造品であることが判明した。明確なバックドア機能は発見されなかったが、偽造品の動作を排除するための検証プロセスを回避するためのアドオン回路が組み込まれていた。
- 2020年3月26日、ファームウェア更新機能を容易に提供可能なため、ネットワーク機器の開発に使用されている組み込み用Linuxディストリビューションのオープンソース OpenWrtに、リモートコード実行の脆弱性(CVE-2020-7982 (JVNDB-2020-003125))が発見された※151。悪用されると不正なファームウェアへの更新に誘導される恐れがあった。

3.2.3 脆弱なIoT機器とウイルス感染の実態

IoT機器を狙うサイバー攻撃が継続する中、ウイルス感染の恐れがある脆弱なIoT機器や実際にウイルス感染したIoT機器は、国内外にどれだけ存在しているのか。本項では、セキュリティ対策強化の取り組みの公開情報等から、脆弱なまま運用されているIoT機器とウイルス感染の実態を考察する。

(1) 国内における実態

総務省及びNICTは、2019年2月以降、インターネット接続事業者と連携し、サイバー攻撃に悪用される恐れのあるIoT機器の調査及び当該機器の利用者への注意喚起を行う取り組み「NOTICE (National Operation Towards IoT Clean Environment)※152」を継続してきた。

2020年6月17日、実施状況の定期的な公表が開始された※153。2020年5月以降の取り組み結果を、表3-2-6(次ページ)に示す(同年4月の調査は新型コロナウイルス拡大防止のため未実施)。

- 「NOTICE注意喚起」(ログイン可能機器利用者への注意喚起)は、2020年10月以降大幅に増加しているが、調査強化(「3.2.4(2)IoT機器調査及び利用者への注意喚起の取り組みの強化」参照)の成果であり、実態としては大きな変化はないと考えられる。

- 「NICTER 注意喚起」（ウイルス感染機器利用者への注意喚起）は、2020 年 8 月のみ大幅に急増しているが、同一機器の IP アドレスが頻繁に切り替わったことによる多重計上の影響であり、実態としては大きな変化はないと考えられる。

	NOTICE 注意喚起（ログイン可能機器）	NICTER 注意喚起（ウイルス感染機器）
2020 年 5 月	287 件	平均 154 件／日
2020 年 6 月	293 件	平均 167 件／日
2020 年 7 月	338 件	平均 209 件／日
2020 年 8 月	309 件	平均 700 件／日
2020 年 9 月	319 件	平均 186 件／日
2020 年 10 月	1,852 件	平均 138 件／日
2020 年 11 月	1,992 件	平均 114 件／日
2020 年 12 月	2,002 件	平均 113 件／日
2021 年 1 月	1,581 件	平均 79 件／日
2021 年 2 月	1,948 件	平均 94 件／日
2021 年 3 月	1,883 件	平均 469 件／日

■表 3-2-6　国内における注意喚起の取り組みの実施結果
（出典）NOTICE サポートセンター「実施状況[※153]」を基に IPA が作成

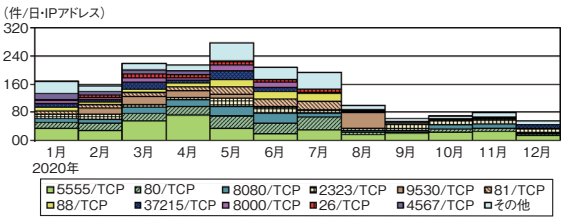
(2) 国内の IoT 機器を狙ったアクセスの観測

警察庁が国内の IoT 機器を狙ったアクセスについて、2020 年 1 ～ 12 月の通年観測状況を公開した[※154]。

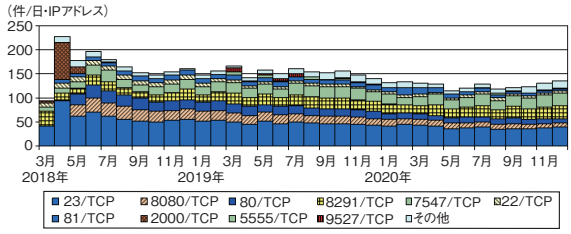
- 機器乗っ取り型ウイルス「Mirai」及びその亜種に感染した IoT 機器で構成されるボットネットによると思われるアクセスは、通年で継続的に観測された（図 3-2-2）。「Mirai」及びその亜種は、特定の IoT 機器の脆弱性を感染拡大手段として随時取り込んでおり、宛先ポートを攻撃の流行に応じて変化させながら、活動を継続していることが分かる。
- 機器保護型ウイルス「Hajime[※155]」に感染した IoT 機器で構成されるボットネットによると思われるアクセスは、通年で継続的に観測された（図 3-2-3）。

(3) DDoS 攻撃の対象国分布

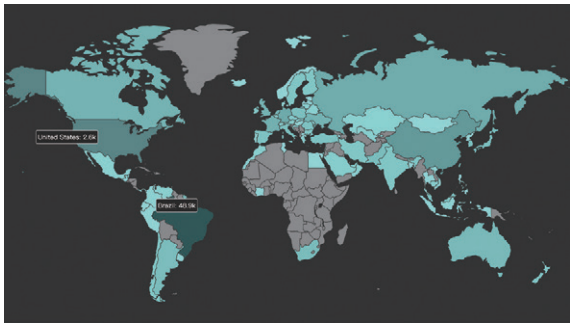
Mirai の亜種 Moobot の活動を観察しているセキュリティベンダが 2020 年 3 月末から 5 月初旬にかけて、数百から 2 万へ急増した DDoS 攻撃について報告している[※156]。図 3-2-4 は攻撃対象の国別分布であり、地図上の濃淡は攻撃数の大小を示す。それによると、攻撃対象国は世界中に分布しているが、ブラジル（約 4 万 8,900）と米国（約 2,600）に集中しており、中国とロシアがそれに続いていることが分かる。



■図 3-2-2　Mirai 及びその亜種と思われるアクセス件数の推移
（出典）警察庁「インターネット観測結果等（令和2年）[※154]」を基に IPA が編集



■図 3-2-3　Hajime と思われるアクセス件数の推移
（出典）警察庁「インターネット観測結果等（令和2年）」を基に IPA が編集



■図 3-2-4　DDoS 攻撃の対象国分布例
（出典）Qihoo 360 Technology Co. Ltd.「An Update for a Very Active DDos Botnet: Moobot[※156]」

3.2.4 セキュリティ対策強化の取り組み

これまで述べたように、IoT に対する脅威は継続しており、世界中に存在する IoT 機器に対して、ゼロデイ対策を含む脆弱性対応やセキュリティ対策を継続的に実施していくことが急務となっている。本項では、対策を検討・推進する上で参考となるセキュリティガイド等の発行状況や、政府の取り組みとしての法規制の強化、民間の取り組みについて紹介する。

(1) IoT 関連セキュリティガイド等の改訂・新規発行

これまでに公開された IoT のセキュリティに関するガイドラインや手引き等の改訂版、新たに発行されたガイドライン等が引き続き公開されている。2020 年以降に国内及び海外で公開された資料を、表 3-2-7（次ページ）と表

3-2-8（次ページ）に示す。

(2) IoT 機器調査及び利用者への注意喚起の取り組みの強化

NOTICE（「3.2.3 (1) 国内における実態」参照）では、IoT 機器を狙う新たなウイルスが継続的に出現し、感染時に悪用される認証情報が増加していることから、2020 年 10 月以降、調査に用いる ID とパスワードの組み合わせを大幅に追加した。また、調査に必要となる通信量が増加することから、調査のための特定アクセス行為の送信元として使用する IP アドレスを増強した（次ページ表 3-2-9）[※157]。

また、国内の重要施設に設置されている IoT 機器において、利用事業者名や用途がインターネット上から容易に判別可能である等、サイバー攻撃を受けやすい状態にある機器が一定数存在することが確認されたため、2020 年 7 月 28 日、一般社団法人 ICT-ISAC は、実態調査、及び該当機器を使用している法人の所有者・運用者等への注意喚起や対策実施の促進を開始した[※158]。

(3) 米国内で拡がる規制の強化

2020 年 1 月 1 日以降、米国カリフォルニア州において IoT 機器の製造業者にセキュリティ対策強化を義務付ける「IoT セキュリティ法[※159]」の施行が開始されたが、米国内の他の州においても規制が強化されている[※160]。

カリフォルニア州に続いて可決されたオレゴン州の IoT

公開機関・団体	公開資料名	対象読者	主な内容	公開年月
経済産業省	IoT セキュリティ・セーフティ・フレームワーク[※60]	設計者、開発者、運用者、利用者	IoT 機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有するための基本的共通基盤（「2.1.2（1）(a) WG1（制度・技術・標準化）」参照）	2020 年 11 月
	機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き[※168]	IoT 機器のセキュリティ検証サービス事業者、検証依頼者（機器製造者）	検証サービス事業者の実施事項、検証依頼者の準備情報、二者間コミュニケーションにおける留意事項、信頼できる事業者の判断基準	2021 年 4 月
総務省	IoT・5G セキュリティ総合対策 プログレスレポート 2020[※169]	IoT セキュリティ関係者	「IoT・5G セキュリティ総合対策」の進捗状況及び今後の取り組み	2020 年 5 月
	IoT・5G セキュリティ総合対策 2020[※170]	IoT セキュリティ関係者	IoT・5G に関するセキュリティ対策の総合的な推進に向けて取り組むべき課題（「2.1.3 (1)『IoT・5G セキュリティ総合対策 2020』の概要」参照）	2020 年 7 月
	電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第 2 版）[※171]	IoT 機器の製造者	インターネットに直接接続する機能を有する IoT 機器に対する規制の強化点	2020 年 9 月
IPA	脆弱性対処に向けた製品開発者向けガイド[※172]	一般消費者が利用するネットワーク接続機器の開発事業者	実施すべき脆弱性対処とその開示方法	2020 年 8 月
一般社団法人 重要生活機器連携セキュリティ協議会（CCDS：Connected Consumer Device Security Council）	IoT 分野共通セキュリティ要件ガイドライン 2021 年版 Ver.1.0[※173]	IoT 機器のサーティフィケーションプログラム（「3.2.4（4）民間における取り組み」参照）申請者	IoT 機器の最低限のセキュリティ要件	2020 年 11 月
	IoT 機器セキュリティ実装ガイドライン ソフトウェア更新機能[※174]	IoT 機器の製造者	ソフトウェア更新機能の実装に関する具体的なセキュリティ要件	2020 年 12 月
一般社団法人日本スマートフォンセキュリティ協会（JSSEC：Japan Smartphone Security Association）	IoT セキュリティチェックシート 第 2.1 版[※175]	IoT を利用・導入する一般企業	IoT 利用・導入時に検討・考慮すべき項目	2020 年 2 月

■表 3-2-7　2020 年以降に国内で新規公開・改訂された IoT 関連のガイドライン等
（出典）各団体の公開情報を基に IPA が作成

公開機関・団体	公開資料名	対象読者	主な内容	公開年月
NIST（National Institute of Standards and Technology：米国国立標準技術研究所）（NISTの成果公開については「3.4.2 成果紹介」参照）	NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers※176	IoT機器の製造者	販売前に（主に設計工程で）考慮すべき推奨事項	2020年5月
	NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline※177	IoT機器の製造者	IoT機器のセキュリティ機能のコアとなるベースライン	2020年5月
	Draft NIST Special Publication 800-213: IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements※178	米国政府機関職員	IoT機器の視点からシステムセキュリティを検討するためのガイダンス	2020年12月
	Draft NISTIR 8259B: IoT Non-Technical Supporting Capability Core Baseline※179	IoT機器の製造者	製造者が導入を検討すべき四つの非技術的サポート機能	2020年12月
	Draft NISTIR 8259C: Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline※180	IoT機器の製造者	特定の顧客またはアプリケーション向けにカスタマイズしたプロファイルの作成方法	2020年12月
	Draft NISTIR 8259D: Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government※181	IoT機器の製造者	8259C記載の方法を用いて作成した米国政府向けプロファイル	2020年12月
ENISA（European Union Agency for Cybersecurity/ European Network and Information Security Agency：欧州ネットワーク・情報セキュリティ機関）	Guidelines for Securing the Internet of Things - Secure Supply Chain for IoT※182	IoTソフトウェアの開発者・製造者、プロジェクトマネージャ、調達チーム	IoTサプライチェーンのセキュリティ脅威、考慮事項、グッドプラクティス	2020年11月
	Cybersecurity Stocktaking in the CAM - Stakeholder mapping and stocktaking of connected and automated mobility (CAM) cyber-security※183	コネクテッドカー／自動運転車のすべての関係者	コネクテッドカー／自動運転車のセキュリティ	2020年11月
ETSI（European Telecommunications Standards Institute：欧州電気通信標準化機構）	ETSI TS 303 645 v2.1.1 (2020-06): CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements※184	コンシューマ向けIoT製品の開発者・製造者	すべてのコンシューマ向けIoT製品に適用可能なベースライン規定	2020年6月

■表 3-2-8　2020年以降に海外で新規公開・改訂されたIoT関連のガイドライン等
（出典）各団体の公開情報を基にIPAが作成

調査時期	ID・パスワード	IPアドレス
～2020年9月	約100通り	41個
2020年10月～	約600通り	54個

■表 3-2-9　NOTICEの取り組み強化
（出典）総務省「サイバー攻撃に悪用されるおそれのあるIoT機器の調査（NOTICE）の取組強化※157」を基にIPAが作成

法（House Bill 2395）も2020年1月1日に施行されており、主に個人・家族・家庭で使用するIoT機器の製造者や販売者に対して、合理的なセキュリティ機能の装備を義務付けている※161。

また、イリノイ州※162、メリーランド州※163、バーモント州、マサチューセッツ州※164、ワシントン州※165においてもIoT法案が提出されている。

(4) 民間における取り組み

民間団体及び民間企業においても、IoTセキュリティ向上のための取り組みが行われている。

- 2020年9月1日、一般社団法人日本スマートフォンセキュリティ協会（JSSEC：Japan Smartphone Security Association）は、「IoTセキュリティチェックシート」（前ページ表3-2-7）をオンラインで解説するセミナー動画「IoTセキュリティチェックシート入門」を公開した※166。
- 2020年11月24日、一般社団法人重要生活機器連携セキュリティ協議会（CCDS：Connected Consumer Device Security Council）は、2019年11月から実施している「IoT機器向けサーティフィケーションプログラム」を拡張し、スマートホーム分野サービス向けプログラムを実施すると発表した※167。

COLUMN

リモート監査が主流となる時代の幕開け!!

リモート監査は、オンサイト監査と同じ、ドキュメント及び記録のレビュー、監査対象の施設の見学、担当者へのインタビュー、監査結果のプレゼンテーション等を、ICT ツールを介して行います。ICT ツールを用いて遠隔から監査を実施する手法は、既に 2008 年に IAF（国際認定フォーラム）の基準文書 MD 4 で公開されていましたが、日本ではそれほど実施されているという印象はありませんでした。しかし、新型コロナウイルスの感染拡大に伴って、日本では多くの監査法人や認証機関、企業で監査／審査が延期されるという事態が発生し、急に利用が拡大していきました。

海外諸国では離れた拠点でリモート監査を実施することに慣れていましたが、日本では対面で話を伺う、直接ドキュメントを確認することが一般的な監査の進め方だったので、リモート監査を実施するための環境を構築することから始めなければなりませんでした。

第一段階として、自宅でテレワークを行うためのインフラ環境として普及した Web 会議サービスを利用した監査の検討が進みました。そして、証跡として文書確認は事前にできるものの現場観察が不足していたことから、デバイス（スマートフォン、タブレット PC）、書画カメラ等を用いて現場確認を行うことで証跡を補うことができるようになりました。第二段階でビデオ機能を搭載したスマートフォンやタブレット等のモバイルテクノロジーと組み合わせたライブストリーミング、更に第三段階でスマートグラス技術とビデオヘッドセットを組み合わせたライブストリーミング等の利用が検討されています。

このように、観る、聴く、伺うといったことはリモート監査でもできるようになりつつありますが、監査員が現場で直接感じ、経験として蓄積してきたノウハウ、例えばインタビュー相手の態度（表情以外）や職場の雰囲気、日常的に使用されている文書かを知る紙質、古さ加減、データセンター、サーバルーム、情報機器等の異常（温度、異音、異臭等）等からリスクを認識することは困難です。

リモート監査をより効果的なものとしていくためには、データに注目した確認が重要です。どのようなデータがどこ（クラウド、業務システム、部門サーバ等）にあるのか、そのデータ項目の存在意義は何か等を把握し、更には、ワークフローや業務システムではどのようなログが取得され、どの程度の期間保存されているのかを把握する必要もあります。そして、これらのデータを活用している AI、ビッグデータ、IoT、RPA 等、様々な ICT にどのようなリスクがあるのかを認識し、その大きさを評価するような監査が求められています。

このようにリモート監査では、過去のみが監査の対象ではなく、未来を見て組織の予測を行い、改善提案を行うことが重要となります。これからの組織はリスクに対する想像力を高めるようなリモート監査を要件として取り組むことが重要ではないでしょうか。

3.3 テレワークの情報セキュリティ

2020 年 4 月 7 日、新型コロナウイルス拡大防止のために緊急事態宣言が発出され、外出自粛が求められたことにより、多くの企業・組織で、オフィス以外の場所から勤務を行う形態での業務（以下、テレワーク）が実施されるようになった。

テレワークを行うために必要な IT 製品・サービスの利用拡大に伴い、脆弱性の発見や、テレワーク端末が原因となったウイルス感染や情報漏えい等の被害の発生が確認されている。

本節ではテレワーク普及の経緯やテレワークのセキュリティ脅威と対策について、IPA が実施した調査結果を踏まえて述べる。

3.3.1 テレワークの広がりと推進活動

テレワークの利用状況の変化と利用拡大、セキュリティ対策の強化のための推進活動について述べる。

(1) テレワーク利用状況の変化

テレワークとは、情報通信技術（ICT：Information and Communication Technology）を活用した、場所や時間にとらわれない柔軟な働き方のことである。テレワークの形態には、表 3-3-1 に示すように、在宅勤務、モバイルワーク、サテライト／コワーキング、ワーケーションがある。

在宅勤務	自宅を就業場所とする働き方。通勤時間の削減、移動による身体的負担の軽減が図れ、時間の有効活用ができる。
モバイルワーク	電車や新幹線、飛行機の中等で行うもの、移動の合間に喫茶店などで行うものも含み、業務の効率化に繋がる。
サテライト／コワーキング	企業のサテライトオフィスや一般的なコワーキングスペースで行うもの。企業が就業場所を規定する場合も、個人で選択する場合も含む。
ワーケーション	リゾートなどバケーションも楽しめる地域でテレワークを行うもの。ビジネスの前後に出張先などで休暇を楽しむブレジャーも含む。

■表 3-3-1　テレワークとは
（出典）一般社団法人日本テレワーク協会「テレワークとは※185」を基に IPA が編集

(a) 2019 年までの経緯

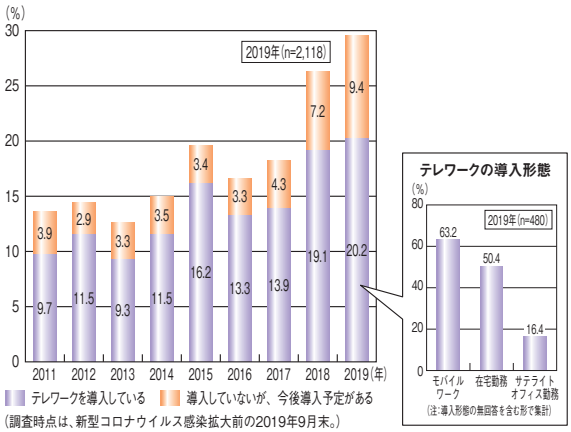
「テレワーク」が生まれたのは、1970 年代の米国である※186。当時の米国では、大気汚染やオイルショック等への危機感から、一部の企業を中心に自宅で仕事をするスタイルが導入された。2001 年 9 月 11 日の米国同時多発テロ事件をきっかけに危機管理の方策としてテレワークが認識され、2010 年にはテレワーク強化法が施行された。この法律は連邦政府職員がテレワークを推進するための様々な義務を定めている。

日本では、1984 年に日本電気株式会社によりサテライトオフィスが作られ、これが日本で初めて「テレワーク」が導入された事例とされている※187。

その後、テレワークは、育児・介護、障がい等により、恒常的または一時的に通勤が困難な人でも在宅で勤務することにより、雇用を継続するために有効であるとして導入の検討が進められた。また、モバイルワークは、営業や SE 等接客機会の多い人が、外出先や移動中でも社内システムへのアクセスや、書類の作成を可能にすることで業務効率化が図れるとして注目された。更に 2011 年 3 月 11 日の東日本大震災以降、自然災害等により通勤が困難になる事態においても事業継続の手段としてテレワークが効果的であると考えられるようになった。他にも図 3-3-1 に示すように社会的な効果が期待されている。

■図 3-3-1　テレワークの効果
（出典）一般社団法人日本テレワーク協会「テレワークを導入する効果※188」を基に IPA が編集

更に、安価で安定した通信インフラの普及と働き方改革への関心の高まりや、東京 2020 オリンピック・パラリンピック競技大会期間中の交通渋滞緩和策として、政府がテレワークによる外出者の削減を奨励したこともあり、テレワークを導入する企業・組織は増加した。図 3-3-2（次ページ）にテレワーク導入状況の推移を示す。



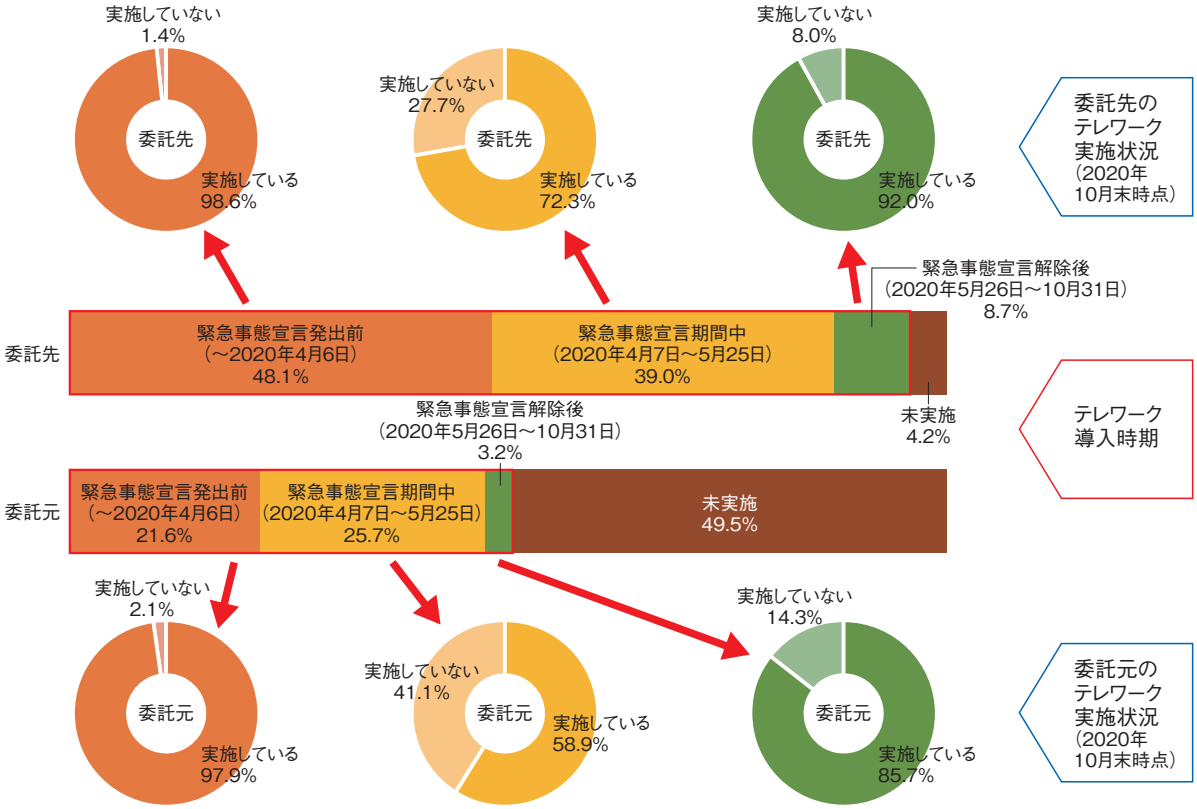
■図 3-3-2　テレワークの導入状況
(出典)総務省「令和元年通信利用動向調査※189」を基に IPA が編集

(b) 2020 年以降の経緯

2019 年 12 月に中国武漢市から広まったとされる新型コロナウイルスの感染拡大が深刻化し、2020 年 4 月 7 日、日本政府は 1 回目の「新型コロナウイルス感染症緊急事態宣言※190」(以下、緊急事態宣言)を発出し、不要不急の外出を控えることを強く求めた。このため多くの企業・組織は、テレワークを導入し、在宅勤務により、出社しなければならない人を最小限にした。以前よりテレワークを推進していた一部の企業では、在宅勤務の期間や回数が増える程度のことで済んだが、それ以外の企業・組織は可用性確保のためネットワークや端末の増強に追われた。

5 月 25 日に「新型コロナウイルス感染症緊急事態解除宣言※191」(以下、緊急事態宣言解除)が発出されたが、職場への出勤等については慎重な意見が多く、政府もテレワーク、時差出勤、自転車通勤等、人との接触を低減する取り組みを呼びかけた※192。その後も 2021 年 1 月 7 日に 2 回目の緊急事態宣言が発出される等、感染者の増減が繰り返され、多くの企業・組織が 1 年以上にわたり、テレワークを継続している。このような、オフィス以外の場所で業務を行う働き方は不可逆的な変化として定着しつつあり、「新常態(ニューノーマル)」と呼ばれている。

IPA は 2021 年 4 月、「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査※193」の結果を公開した(図 3-3-3)。ユーザ企業から業務委託を受ける IT 企業やベンダ(以下、委託先)と業務委託するユーザ企業(以下、委託元)を対象に、テレワークの導入時期と継続状況を 2020 年 11 月に調査したものである。この調査では、10 月 31 日時点で委託先の 95.8%、委託元の 50.5% の組織がテレワークを実施した



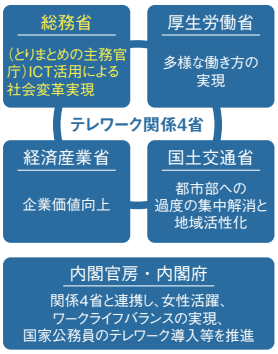
■図 3-3-3　テレワーク導入時期と継続状況(n=505)
(出典)IPA「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」を基に編集

ことがあると回答した。1回目の緊急事態宣言発出前からテレワークを実施していた委託先は48.1%、委託元は21.6%となっており、IT企業の多い委託先では、テレワークの導入が進んでいた。一方、1回目の緊急事態宣言期間中にテレワークを導入した委託先は39.0%、委託元は25.7%となっており、短期間に多くの企業・組織で導入されたことが分かる。一時はパソコン、ネットワークのリソース不足※194等が発生し、企業・組織は応答遅延等、厳しい環境での業務を迫られた。

更に、前述の緊急事態宣言期間中にテレワークを導入したと回答した組織のうち、委託先の27.7%、委託元の41.1%が、2020年10月31日時点でテレワークを実施していないと回答しており、テレワークが一時的な対応にとどまっていたことがうかがえる。しかし、緊急事態宣言発出前、あるいは緊急事態宣言解除後から実施・導入していた組織の9割はテレワークを継続しており、今後も組織の勤務形態としてテレワークが定着することが予想される（そのほかの調査結果については「3.3.3 テレワークのセキュリティ実態調査」参照）。

(2) テレワークとセキュリティ対策の推進

テレワークは、ワークライフバランスの実現、人口減少時代における労働力の確保、地域の活性化、非常時における業務継続等に有効と考えられ、関係府省が連携して普及・推進を図ってきた。2016年7月からは内閣官房長官指示により関係府省連絡会議が開催され、テレワーク推進に向けた取り組みの共有や連携施策の検討・推進がなされている（図3-3-4）。



構成員（政務）	
総務省	総務副大臣（議長）
厚生労働省	厚生労働副大臣
経済産業省	経済産業副大臣
国土交通省	国土交通副大臣

構成員（事務）	
内閣官房	内閣審議官（IT総合戦略室 室長代理）
内閣府	官房審議官（男女共同参画局担当）
総務省	官房総括審議官（情報通信担当）
厚生労働省	雇用環境・均等局長
経済産業省	官房審議官（商務情報政策局担当）
国土交通省	官房審議官（都市担当）

■図3-3-4　テレワーク関係府省連絡会議
（出典）厚生労働省「テレワーク総合ポータルサイト　政府のテレワークへの取り組み※195」

この中で、テレワークの導入支援を目的とした情報提供手段として、総務省が「テレワーク総合情報サイト※196」を、厚生労働省が「テレワーク総合ポータルサイト※197」を開設し、テレワークの導入事例や導入にあたって活用可能な支援策等が示された。また、総務省は2018年

テレワーク関連ガイドライン・情報サイト名	発行元・運用者	概要
みんなでしっかりサイバーセキュリティ※201	NISC	テレワーク実施者を対象とし、情報セキュリティを確保するための対策や注意点を簡易に説明している。
テレワークセキュリティガイドライン第5版※202	総務省	テレワークにおける情報セキュリティ対策の考え方、ポイント、テレワークトラブル事例と対策一覧等をまとめている。2021年5月に全面的に改定された。
中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）※202	総務省	テレワークセキュリティガイドラインを補完する。セキュリティの専任担当がいない中小企業等がテレワークを実施する際に最低限のセキュリティを確保するためのチェックリスト。
テレワーク時における秘密情報管理のポイント（Q&A解説）※203	経済産業省	テレワークに対応した規程の整備等について、Q&A形式でまとめている。
テレワークモデル就業規則～作成の手引き～※204	厚生労働省	テレワーク導入の際に検討が必要な就業規則についての考え方や、参考とすべき規定例、組織におけるセキュリティガイドライン策定の必要性等をまとめている。
テレワークの適切な導入及び実施の推進のためのガイドライン※205	厚生労働省	テレワークの導入・実施にあたり、労務管理を中心に、労使双方の留意点、望ましい取り組み等を明らかにしている。
テレワークを行う際のセキュリティ上の注意事項※206	IPA	テレワーク環境提供の有無、使用場所の違い、テレワーク環境から職場に戻る際の注意点等、テレワーク実施時のセキュリティ上の注意を促している。
Web会議サービスを使用する際のセキュリティ上の注意事項※207	IPA	組織のWeb会議主催者、情報システム部門を対象に、Web会議サービス選定時に考慮すべきセキュリティ上のポイントを挙げている。
テレワークのガイド・事例等※208	一般社団法人日本テレワーク協会	テレワーク導入の際に参考となる各種ガイドラインや事例集等を掲載している。

■表3-3-2　テレワーク関連ガイドライン・情報サイト概要
（出典）各組織の公開情報を基にIPAが作成

4月に、企業等が情報セキュリティ上の不安を払拭してテレワークを導入・活用するための指針「テレワークセキュリティガイドライン 第4版[※198]」を、厚生労働省は2018年2月に、テレワークにおける労務管理の留意点を記載した「情報通信技術を利用した事業場外勤務の適切な導入及び実施のためのガイドライン[※199]」や、自営型テレワークの実施に向けた「自営型テレワークの適切な実施のためのガイドライン[※200]」を公表した。2020年には情報サイトが更に増え、テレワークセキュリティガイドライン等既存のガイドラインも改版・拡充された。表3-3-2（前ページ）に主なガイドライン、情報サイトとその概要を示す。

2020年は更に、「新型コロナウイルス感染症緊急経済対策」（2020年4月7日閣議決定）や2020年度第一次・二次補正予算において、税制措置としてテレワーク等のための設備投資が中小企業経営強化税制の対象とされたほか、経済産業省、総務省、厚生労働省からテレワーク促進のため助成金等、各種予算措置が取られることとなり、テレワーク導入企業の裾野を広げる機運が高まっている。

3.3.2 テレワークに関連した問題

2020年に報告された脅威や実際に発生した被害の中には、テレワーク環境に関わる脆弱性や攻撃が存在した。以下はその解説である。

(1) 2020年に発生したインシデント事例

2020年に報告されたテレワーク環境に起因するインシデント事例を紹介する。

(a) Web会議サービス利用時の問題

テレワークの普及に伴い、Web会議サービスを利用する組織が増加した。しかし、これらのサービスのクライアントアプリケーション（以下、アプリ）に脆弱性が発見されたり、利用者の不注意により被害が生じたりしている。

2020年3月、Web会議サービス「Zoom」のWindows向けアプリに脆弱性が発見された。この脆弱性を悪用された場合、認証情報を窃取されたり任意の実行可能ファイルを起動されたりする可能性があった。この脆弱性は製品開発者により速やかに修正され、発見の翌日に修正バージョンが公表された[※209]。Zoomに関してはその後、セキュリティについて大幅な修正が行われ、通信内容のエンドツーエンドでの暗号化機能等が実装された。

上記のようなWeb会議サービスの脆弱性は、Zoomのみではなく、TeamsやWebex等のアプリにおいても報告されており、随時修正が行われている。

また、Zoomについては Zoom 爆弾という荒らし行為による被害が確認されている。Zoomでは会議を設定すると会議参加用のURLが発行される。このURLには会議のIDが含まれており、攻撃者が総当たり攻撃を行うことでIDが推測される。このとき、会議への参加にパスワードが設定されていないと、意図しない参加者が会議に参加できてしまう。実際に攻撃者によって、IDを推測され、会議に侵入された際に不適切な画像を画面共有される等の被害が発生した。Zoom爆弾の被害が報告された後、会議にパスワードを設定する等の対策が呼びかけられている[※210]。

これまでに紹介した被害の発生に伴い、IPAではWeb会議サービスを安全に利用するための注意事項として、「Web会議サービスを使用する際のセキュリティ上の注意事項[※207]」を公開し、Web会議サービス選定時に考慮すべきポイントや会議準備、会議実施のタイミングでの注意すべきポイントについて、解説を行っている。

(b) VPN製品の脆弱性

2020年には、Fortinet, Inc.製FortiOSのSSL VPN機能の脆弱性「CVE-2018-13379」について、修正バージョンへのアップデートが未実施である機器のIPアドレス情報が、インターネット上で公開された。この脆弱性は2019年に公表され、同年11月に修正バージョンのファームウェアが公表されていた。しかし、何らかの理由により、アップデートが行われなかった機器のIPアドレス情報が2020年になって公開されたものである。この中には日本企業や警視庁、大学等のホストも存在したとの報道もあり、脆弱性を悪用されたことによる被害が国内でも報告されている[※211]（FortiOSの脆弱性を悪用した攻撃については「1.2.5(1)(a)攻撃事例」参照）。

Fortinet, Inc.の製品に加え、2019年にはPalo Alto Networks, Inc.やPulse Secure, LLC.のSSL VPN製品でも脆弱性が公表され、JPCERT/CCから注意喚起が行われている[※212]。また、2021年4月にもPulse Secure, LLC.のSSL VPN製品について、任意のコマンド実行につながる脆弱性「CVE-2021-22893[※213]」が発表されている。このようにVPN製品等のテレワークで用いる通信機器にも脆弱性が発見・報告されており、各組織のネットワーク管理者は常に情報を収集することが求められている。

(c) テレワーク端末や個人を標的とした攻撃

2020 年 8 月、三菱重工グループにおいて、不正アクセスがあったことが報告された。この事案では、グループ内のネットワークにおいてウイルス感染が発生し、ウイルスに感染した端末が悪用されて不正アクセスが生じたとされている。三菱重工グループの報告によれば、テレワーク中の従業員が自宅に持ち帰っていた社用パソコンを使用し SNS を参照した際、ウイルスをダウンロードしてしまい感染、その後オフィスに出社した際にウイルスに感染したパソコンをグループ内のネットワークに接続したことで、ウイルスが持ち込まれたとしている※214(「1.2.1 (3) (d) SNS を悪用した攻撃」参照)。

オフィス等組織内で業務を行う形態では、組織が管理するファイアウォールやセキュリティ製品により各従業員が利用する端末やネットワークは保護されている。しかし、テレワーク環境では、各従業員の端末は、自宅のルータや各端末に導入したセキュリティソフトによる対策で守る必要があり、組織内と同様のセキュリティ強度を維持することが困難となっている。また、業務端末の管理が各従業員に一任される状態となっており、OS やソフトウェア製品のアップデートが実施されているのかを管理することが、オフィス勤務よりも難しくなっている。

加えて、自然災害が発生したとき等と同様に、新型コロナウイルスへの不安に便乗したフィッシング等も発生している※215(個人を対象とした同様なフィッシングについては「1.2.7 個人をターゲットにした騙しの手口」参照)。これについても、オフィス勤務であれば気が付いた従業員が周囲に簡単に注意喚起を行うことができたが、テレワーク環境では注意喚起が容易ではなくなっており、フィッシング等の被害が発生する危険性が高まっていると考えられる。

(2) テレワーク環境を取り巻く脅威

オフィスでは物理的な隔離等の対策が組織で可能であったが、テレワーク環境では個人でパソコンの管理やソフトウェアの更新、ネットワークの安全性等に責任を持たなければならず、オフィス程堅牢な対策はとれないため、攻撃者に狙われる可能性は高い。テレワーク環境を取り巻く脅威を、テレワーク環境で働く従業員（個人）を狙ったものと、テレワークを実施する組織を狙ったものに大別して解説する（対策については「3.3.4 テレワークのセキュリティ対策」参照)。

(a) 個人が注意すべき脅威

テレワークの実施に際し、個人を標的として予想される脅威の代表例を以下に示す。

① 不正アクセス
② ウイルス感染
③ フリー Wi-Fi からの盗聴
④ ソーシャルハッキング
⑤ 端末や業務資料の紛失

不正アクセスやウイルス感染が発生する原因としては、業務用パソコンで使用しているソフトウェアや自宅のルータのファームウェア、セキュリティソフト等の更新が行われず、脆弱性を狙った攻撃や最新のウイルスへの対応が行われないことが想定される。

また、自宅やオフィス以外で仕事をする際、Wi-Fi のフリースポットを使用して通信内容を盗聴される被害や、社外秘の資料を開いた画面を覗かれ、情報が盗まれるソーシャルハッキングによる被害の発生が予想される。特に、ソーシャルハッキングについては自宅においても、家族が社外秘の資料を見て、悪意を持たず第三者に話してしまうといった事態も想定される。

組織がテレワークを主とした業務形態に移行しても、必要に応じて出勤する場合や、オフィスから業務用パソコンや業務上必要な書類を自宅へ持ち帰る場合等が考えられる。このような場合、通勤経路や自宅で端末や業務資料の紛失が生じる可能性がある。公共交通機関におけるカバン等の置き引きや置き忘れは、以前から注意喚起されており、従業員も警戒していると考えられる。しかし自宅内において、重要書類を誤って廃棄し、廃棄した書類が第三者に拾われる、あるいは空き巣被害によって重要書類や業務用パソコンが盗まれるといった被害も想定される。

(b) 組織が注意すべき脅威

組織が直面する脅威として、以下が予想される。

① 規則違反
② ソフトウェア等の資産管理不備
③ サーバ等の ID 漏えいによる不正アクセス
④ 問い合わせ・報告先の不備

まず、テレワークを実施するに際し、組織が定めたテレワーク規則について従業員が重要性を理解していないため、規則に違反してしまいウイルス感染や盗聴、端末の紛失といった被害が発生することが想定される。

また、各従業員が使用する業務端末や端末上のソフトウェアがオフィス外にあるため資産管理ができず、アップデート状況やライセンスの継続状況が把握できなくなることが想定される。

加えて従業員が各自宅等から、組織のサーバ等の資産にアクセスするため、ID やパスワードのメモを持ち帰った後に紛失したり、フィッシング等により窃取されたりすることで、ID やパスワードの漏えい被害の発生が想定される。

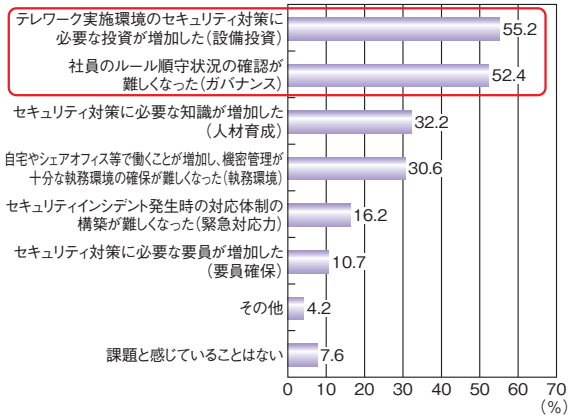
上記のような被害やトラブルが発生した際に、組織内の連絡先となる窓口が整備されていなかったり、従業員に展開されていなかったりする場合、対応の遅れが生じ被害の拡大につながると想定される。

3.3.3 テレワークのセキュリティ実態調査

コロナ禍での事業継続のため利用が拡大したテレワークやオンラインによるコミュニケーションといった変化に対して、組織のセキュリティ対策は十分なのか、リスクは顕在化していないのか、等の実態を把握するため IPA では 2020 年度に「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」を実施した。以降にその結果を述べる。なお、調査時期は、2020 年 11 月、調査対象は企業データベース等から抽出した企業・組織の情報システム・IT 企画関連業務の担当者である。

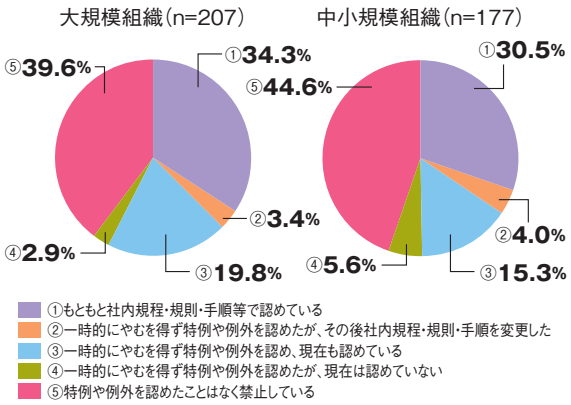
(1) テレワーク実施時のセキュリティ上の課題

テレワークを実施する上でのセキュリティ上の課題について調査した結果を図 3-3-5 に示す。「テレワーク実施環境のセキュリティ対策に必要な投資が増加した」という回答が最も多く（55.2%）、「社員のルール順守状況の確認が難しくなった（ガバナンス）」が 52.4% で続いた。



■図 3-3-5　テレワーク実施時のセキュリティ上の課題（複数回答）
（出典）IPA「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」を基に編集

緊急事態宣言中またはコロナ禍の影響により、例外として個人が所有する端末（パソコン・スマートフォン等）の業務利用を認めたかを調査した結果を図 3-3-6 に示す。「一時的にやむを得ず特例や例外を認め、現在も認めている」という回答が大規模組織で 19.8%、中小規模組織で 15.3% であった。



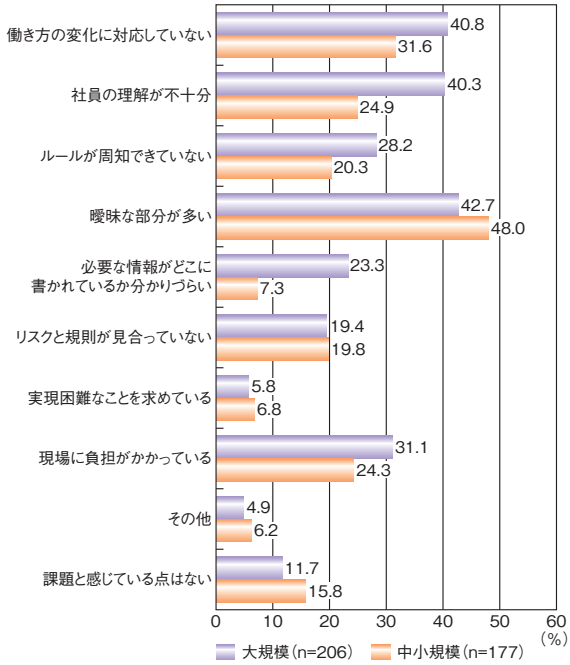
■図 3-3-6　緊急事態宣言中またはコロナ禍の影響により特例や例外を認めたセキュリティ対策の社内規定・規則（個人が所有する端末（パソコン・スマートフォン等）の業務利用）
（出典）IPA「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」を基に編集

緊急事態により一時的に例外や特例を認めることは、業務継続を優先するという観点からやむを得ないと判断されたと思われる。しかし、例外や特例で規則が緩和されることにより脆弱性が増し、セキュリティリスクは大きくなる。緩和された状態が常態化することによって、セキュリティインシデントの発生が懸念される。組織は、緩和によるリスクと事業継続の状況等を総合的に判断し、リスク低減のための対策（規定・規則の見直し、対象範囲の縮小、ツールの導入等）の検討、あるいは、例外や特例の撤廃により、リスクを受容可能なレベルまで小さくすることが望ましい。なお、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を公開している※206。テレワークを行う際の規定の見直しと制定の参考としていただきたい。

(2) 社内規定・規則・手順の課題

テレワークに関する社内規定・規則・手順についての課題について調査した結果を図 3-3-7（次ページ）に示す。企業規模に関わらず「曖昧な部分が多い」という回答が最も多く、「働き方の変化に対応していない」「社員の理解が不十分」が続いた。

「働き方の変化に対応していない」という課題は新型コ



■図 3-3-7　社内規定・規則・手順の課題
(出典)IPA「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」を基に編集

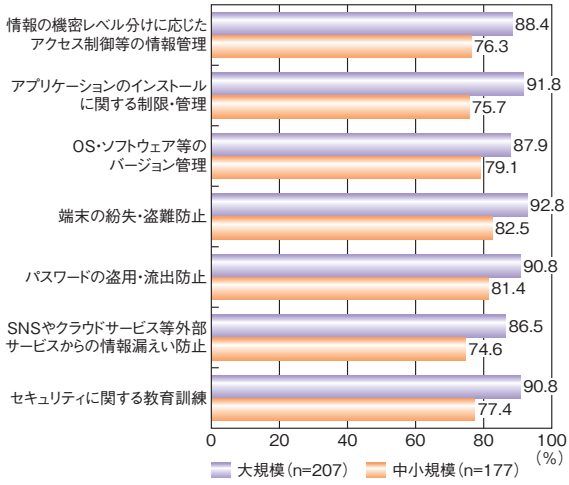
ロナウイルス対策としてテレワークの導入や利用が急増したことに対して、社内規定・規則・手順の作成や見直しが追い付いていないことが理由であると考えられる。

中小規模企業と大規模企業の違いとして、「社員の理解が不十分」という回答において中小規模企業では 24.9%、大企業では 40.3% と 15.4 ポイントの差が見られ、「必要な情報がどこに書かれているのかわかりにくい」という回答において中小規模企業では 7.3%、大規模企業では 23.3% と 16 ポイントの差が見られた。この結果から、大規模企業の場合、多くの規定・規則・手順が定められてはいるが管理・周知や理解が十分できていないことが推測できる。どのような場合にどの規定に従えばよいのか、またその規定はどこに記載されているのかを従業員が理解していないことがインシデントの発生等につながる恐れがある。

(3) テレワーク実施に関するセキュリティ対策規則の制定状況

テレワークに関するセキュリティ対策規定の制定状況について調査した結果を図 3-3-8 に示す。中小規模企業の 75% 以上、大規模企業の 85% 以上がテレワークに関するセキュリティ対策規則を制定しているという結果となった。

企業規模による規定制定状況のばらつきは見られず、全体的に高い割合で制定されていることがうかがえる

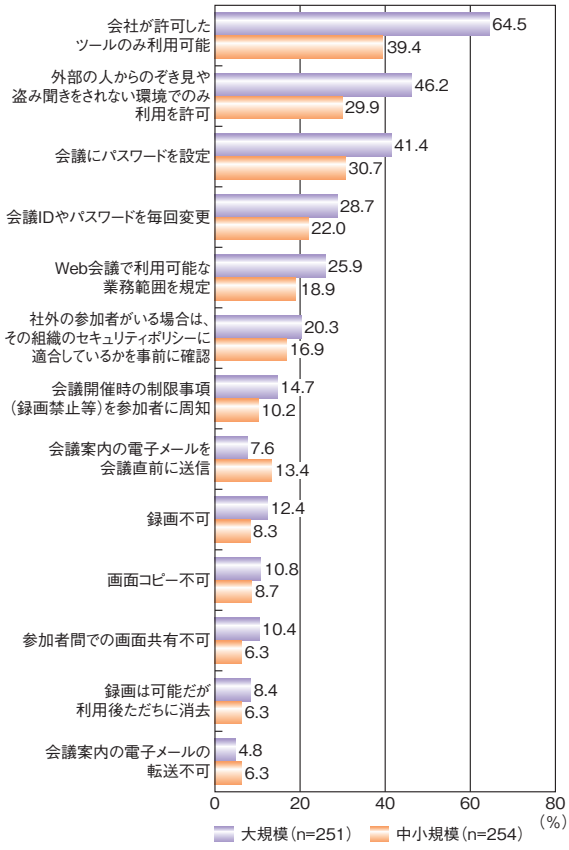


■図 3-3-8　テレワーク実施に関するセキュリティ対策規則の制定状況
(出典)IPA「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」を基に編集

が、規定がない状況でテレワークを実施している企業も一定数存在することが確認された。

(4) Web 会議サービス利用時の規則制定状況

Web 会議サービス利用時の規則制定状況について調査した結果を図 3-3-9 に示す。企業規模に関わらず、「会社が許可したツールのみ利用可能」という回答が最も

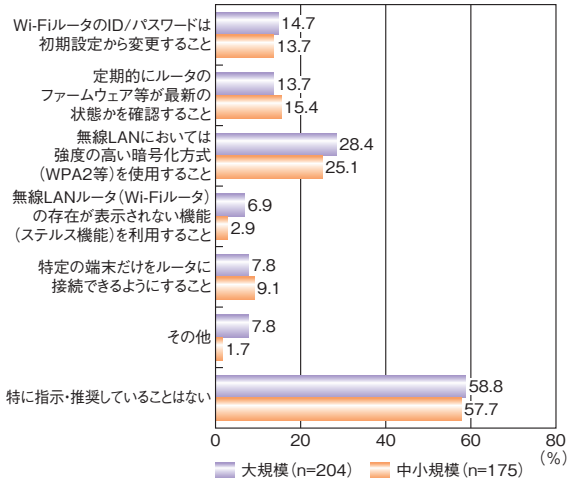


■図 3-3-9　Web 会議サービス利用時の規則制定状況
(出典)IPA「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」を基に編集

多く、「外部の人からのぞき見や盗み聞きをされない環境でのみ利用を許可」「会議にパスワードを設定」が続いた。

規則を制定している割合について企業規模による偏りは見られないが、最も回答が多かった「会社が許可したツールのみ利用可能」では、大規模企業の 64.5% に対し、中小規模企業は 39.4% であり、25.1 ポイントの差が見られた。大規模企業では離れた拠点間の会議等でコロナ禍以前から Web 会議サービスを利用していた企業が多く、規則が決まっていたのに対して、中小規模企業ではコロナ禍以降に Web 会議サービスを導入したため、規則が間に合っていない企業が多かったことが影響していると考えられる。また、「会社が許可したツールのみ利用可能」以外の規則の制定状況はいずれも 50% 以下であり、図 3-3-8（前ページ）のテレワーク実施に関する規則と比較すると、「Web 会議サービス利用時の規則」はテレワークの規則に比べ制定の割合が低いことが分かった。

規則がない状態で Web 会議サービスを利用すると、使い方を誤り、気付かないうちに情報を漏えいさせてしまう恐れがある。また、規定を決めても Web 会議の相手に同様の規定がなければ Web 会議サービスの設定や情報の取り扱いが異なることによって、セキュリティリスクが高まる恐れがあるため、Web 会議で機密情報を扱う場合は、情報の管理方法や参加者の限定・表記等のルール等を双方で確認することが重要である。IPA では Web 会議サービスを利用する際のセキュリティ上の注意事項を公開している※207。Web 会議サービスの規定の見直しと制定の参考としていただきたい。



■図 3-3-10　テレワークで自宅のホームネットワークを利用する際の指示、推奨事項（複数回答）
（出典）IPA「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」を基に編集

(5) テレワークで自宅のホームネットワークを利用する際の指示、推奨事項

テレワークで自宅のホームネットワークを利用する際の指示、推奨事項について調査した結果を図 3-3-10 に示す。約 6 割が「特に指示・推奨していることはない」と回答しているが、残りの企業・組織では何らかの指示・推奨をしていると回答した。

テレワークにおいて自宅のホームネットワークを利用するケースも増加していることが考えられるが、ホームネットワークに関する指示や推奨事項を決めている企業は少ないことが分かった。ホームネットワークは新たなリスクになることが想定されるため、安全な使い方の指示や推奨事項についての検討が急務である。

3.3.4 テレワークのセキュリティ対策

テレワーク実施時のインシデントの被害やトラブルの発生原因が個人と組織で異なるため、対策についてもそれぞれの立場で検討する必要がある。

(1) 個人が実施すべき対策

テレワークの実施に際し、個人を標的とする脅威の代表例を再掲し、それぞれについて実施すべき対策を述べる。

① 不正アクセス
② ウイルス感染
③ フリー Wi-Fi からの盗聴
④ ソーシャルハッキング
⑤ 端末や業務資料の紛失

①と②に対しては、脆弱性対策、ウイルス対策が必要である。使用するパソコンの OS やソフトウェア、自宅のルータのファームウェア、セキュリティソフトのパターンファイルを最新の状態に保つことが第一の対策となる。また、脆弱性を悪用した不正アクセスやウイルス感染等の早期検知の方法として、近年はホームルータにも UTM や類似の機能が組み込まれているものがあるため、必要に応じてセキュリティ設定を有効にすることも検討すべきである。

③と④に対しては、各組織のテレワークに関するルールを順守しつつ、業務を実施する環境を見直す必要がある。

例えば、自宅以外の場所で業務を行う際にインターネットを利用する場合は、フリー Wi-Fi を利用せず、会社貸与のモバイルルータを利用することや、フリー Wi-Fi を利

用する場合は、各組織のネットワークに VPN 接続して組織のファイアウォールを経由して通信する、等の対策を検討すべきである。

また、ソーシャルハッキングへの対策としては、第三者の出入りが多いカフェやレストラン等での業務を避けるほか、自宅内においても個室で業務を行い、席を離れる際はパソコンを必ずロックし、業務書類や手帳等も引き出し等にしまい、放置しないといった対策を徹底することが重要である。

⑤に対しては、ワイヤーロック等の盗難対策や片付けの徹底が第一の対策となる。特に第三者が出入りするカフェやホテル等では、パソコンや資料から目を離さないようにし、もし目の届かない状態になる場合は、鍵付きのカバン等に確実に収納し、ワイヤーロック等を使い盗難を防止する等の対策が必要である。

また、自宅においても書類がチラシ等に紛れてしまい、誤って廃棄される等の事態を防ぐために、専用のファイルに収納する等の対策を検討すべきである。その他、空き巣等による業務用パソコンの盗難を防止するため、自宅内でもワイヤーロックを使用し、パソコンを使用しない場合は鍵のかかる引き出し等に保管するといった対策が必要である。

(2) 組織が実施すべき対策

組織が直面すると予想される脅威を再掲し、それぞれについて実施すべき対策を述べる。

① 規則違反
② ソフトウェア等の資産管理不備
③ サーバ等の ID 漏えいによる不正アクセス
④ 問い合わせ・報告先の不備

①に対しては、各組織において、業務内容に応じた規則を設定、あるいは見直しを行い、従業員に徹底する必要がある。規則の徹底においては、業務内容から想定される被害の大きさを認識させ、被害防止のために実施すべきことを従業員に理解してもらう必要がある。

②に対しては、各従業員の作業端末や組織のサーバ等で使用するソフトウェアが常に最新の状態に保たれるようにテレワーク環境でどのようにメンテナンスを行うか、作業手順を整備する必要がある。必要に応じて、資産管理ソフトウェア等を新規に導入する等、管理体制の見直しが必要である。

③に対しては、サーバ等へのログイン情報の管理を行う。各従業員が自宅等から日常的に組織のサーバを利用するため、不正アクセスには特に注意が必要となる。ワンタイムパスワードを使用した認証や、多要素認証等を用いて ID やパスワードが漏えいした際への対策を進めることを検討すべきである。

また、各従業員の通信内容の盗聴を避けるため、組織のネットワークと VPN による接続を行うことも検討すべきである。

④に対しては、情報提供窓口やインシデント発生時の通報窓口の再確認、整備が必要である。一般向けの窓口は、通常の問い合わせとインシデント報告先の窓口が識別しやすい名称でないと、適切な窓口に連絡されず、スムーズな対応ができないことが想定される。

テレワーク業務では、オフィス等に従業員が集まっていないため、インシデント発生時の連絡先が通常と異なる。インシデント発生時の連絡先や対応担当者が適切に整備されず、通報者が連絡先を確認できない場合、報告・初動対応が遅れてしまい、被害の拡大につながるリスクがある。

従業員が適切な連絡先をスムーズに確認できない場合、業務を優先してしまうことで、重大事象の通報を後回しにしたり、通報自体を放棄したり、失念したりすることで被害の発生を見過ごす事態も想定される。

特にテレワーク業務では、インシデントや不審な事象の発生時に各従業員が発生事象について周囲に相談や報告を行うことが難しいため、誤って報告すべき事象を過小評価し、報告しないことも想定される。結果として、組織内のインシデントの発生が見過ごされてしまう危険がある。

また、テレワーク環境ではトラブルが発生した場合の連絡手段が限られ、担当部署の従業員が直接端末等を確認することもできないため、事象の調査にはオフィス勤務の場合以上に時間を要すると考えられる。このため、問い合わせ・報告先とともに、事象発生時にどのような情報を取得し、どのような形式で担当部署へ展開すべきかを整備しておくことも、迅速な対応のために重要である。

3.3.5 今後のテレワークのセキュリティ

勤務場所の多様化、業務のデジタル化・オンライン化といった働き方の変化は、試行錯誤が続きつつもニューノーマルとして定着すると想定される。2020 年は業務継続のため、十分な準備ができないままテレワークや Web 会議を導入した企業・組織が多く、サービスの利用や、情報の取り扱いに関するルールの緩和等で急場しのぎせ

ざるを得なかった。しかし、このようなセキュリティ対策の特例や例外を認め、リスクの低減策が検討されない状態が常態化することによって、インシデントの発生、被害の拡大を招くことが懸念される。具体的には、組織が管理できない機器の増加、新サービスの脆弱性、自宅で利用する機器のメンテナンス不備等により、従来の組織統制のもとでの働き方に比べ、攻撃のリスクが増えている。またテレワークという新しい環境に便乗したフィッシング、ウイルス感染や自宅での管理不備による情報流出等、人的要因による被害リスクも増えている。

テレワークでは固定的なセキュリティ境界はなくなり、自宅やクラウドといった、組織のガバナンスでは統制しにくい状況でセキュリティのレベルを保つことが求められる。テレワークで利用する端末・ネットワーク・サービスの特定とそれに基づくリスクアセスメント、可用性重視で暫定的に作成したルールの再整備と周知徹底、インシデント対応の見直し、機器や人の認証の強化を含むゼロトラストの考え方の導入、最新の攻撃やフィッシング等の脅威に関する情報の共有等について、できることから検討していただきたい。

COLUMN

情報セキュリティをテレワークができない理由にしないで

新型コロナウイルス対応で、民間企業だけでなく多くの組織でこれまでの働き方を変える必要に迫られました。そんな中で自宅等オフィス以外の場所で働くいわゆるテレワークやリモートワークが急速に広まりました。しかし新型コロナウイルス禍前までは、正直言ってテレワークの普及は遅々として進まなかったというのが実情でした。

なぜテレワークが普及しないのかという理由について、各種調査や専門家による分析が行われましたが、労務管理や業績評価の難しさ、社内ルールや IT インフラの未整備、上司と部下・社員同士のコミュニケーションの難しさと並んで必ず上位に挙げられるのが情報セキュリティの問題です。もちろん、テレワークの実施にあたっては、オフィス外で機密性の高い情報を扱うことになるケースもあるわけですから、情報セキュリティ対策に十分配慮することが求められるのは確かです。しかし、情報セキュリティが心配だからテレワークを導入できないというのは単なる言いわけだと思われても仕方ありません。

新型コロナウイルス禍という困難な状況において求められているのは働き方の「変革」です。従来の働き方や情報の取り扱い方法を改善して業務を改革していくというだけではこの状況を変えることは難しいのではないでしょうか。いったん、「いままではこうだった」という考え方を置いて、業務のやり方、IT インフラの在り方、情報の取り扱い方法等、まずは大胆な発想で働き方を変えていくということが大切ではないでしょうか。想像してください。人口の減少や高齢化による労働人口の減少、今後予想されている大規模災害、新たなウイルスの出現等、今ここで変わっておかないと、後々大変なことになるかもしれません。

もちろん、詳細を検討していくと、経営者や中間管理職の皆さんにとっては、「そうは言っても」とか「現実的には」と言いたくなる場面があるかもしれません。そこを社員の皆さんの変わろうとする勇気と知恵で、一つでも二つでも乗り越えていこうというパワーこそが変革につながっていくのではないでしょうか。そして経営者や中間管理職の皆さんは、そういう社員の変革への意欲・提案を受け止めていただき、テレワークができない理由を考えるのではなく、どうしたらできるのかについて、公表されている他社事例や専門家のアドバイス等を参考にして、組織一丸となって検討をしていただきたいと思います。

特にテレワークにおける情報セキュリティは、業務に携わる人達の責任と自覚、そして技術によって、十分に解決可能な問題だと考えます。比較的安価なクラウドサービス、Web 会議システムやシンクライアントシステム等の提供がテレワークの推進を後押ししてくれるでしょう。こういった技術を安全に利用するための情報を IPA は提供していきます。情報セキュリティをテレワークができない理由にしないで、この困難な状況を乗り越えるべく、働き方の「変革」を実現しましょう。

3.4 NISTのセキュリティ関連活動

組織のサイバーセキュリティ対策を検討する場合、自らの対策がグローバルなセキュリティ基準と整合しているか、グローバルな基準のどのレベルに相当するか、等を考える際によく参照される規格として、国際標準化機構（ISO:International Organization for Standardization）のSC 27専門委員会※216が策定するISO/IEC 27000シリーズ、及び米国国立標準技術研究所（NIST：National Institute of Standards and Technology）※217の策定するNIST SP 800シリーズがある。

ISO/IEC 27000シリーズは、国内では日本産業規格（JIS：Japanese Industrial Standards）として日本語化され、活用されている。また本白書では、SC 27専門委員会等の最新標準化動向を紹介している（「2.5.2 情報セキュリティ、サイバーセキュリティ、プライバシー保護関係の規格の標準化（ISO/IEC JTC 1/SC 27）」参照）。これに対し、NISTの活動は国内で十分に紹介され、理解されているとはいえないが、その規格やガイドラインへの注目度は高い。

例えば、国内政府機関のセキュリティ規格の策定・改訂において、米国連邦政府機関が採用すべき管理策を定めたNIST SP 800-53やNIST SP 800-171は頻繁に参照される。またNISTが策定したCybersecurity Framework※218は、経営層とセキュリティ担当部門がコミュニケーションをとるための共通言語として、連邦政府機関・民間企業のみならず各国から注目されている。経済産業省とIPAも、国内施策であるサイバーセキュリティ経営ガイドライン※219やサイバー・フィジカル・セキュリティ対策フレームワーク※220の活動をNISTのCybersecurity Framework、あるいはSP 800-160※221等の関連規格に整合させ、国内の施策が容易にグローバル展開できるように努めている。

本項では、NISTのセキュリティに関する活動の概要と規格策定の最新動向について紹介する。

3.4.1 NISTの活動概要

NISTは米国の産業競争力に関わるあらゆる標準規格・ガイドライン策定、計測技術の開発を担っている組織であり、活動も多様な形態をとっている。

(1) 組織の沿革と体制

NISTの沿革と組織体制について述べる。

(a) 沿革とミッション

NISTは、産業競争力のベースとなる計測技術基盤を強化するために、議会が1901年に設立した国立規格基準局（NBS：National Bureau of Standards）を前身とし、現在は米国商務省（DoC：Department of Commerce）の傘下で「経済的安全保障を高め、生活を向上させるように科学的測定手法、標準、技術を進歩させ、米国の技術革新、及び産業競争力を促進すること」をミッションに掲げている。計測や標準化の対象はナノスケールの材料やコンピュータチップ、サイバー空間から巨大建造物・ネットワークまで多岐にわたり、「重要な測定ソリューション、公平な基準の作成・推進により世界をリードし、イノベーションを刺激し、産業競争力を促進し、生活の質を改善すること」をビジョンとしている。

(b) 組織

組織は以下の五つの研究所と二つのユーザ用施設で構成される。

- 通信技術研究所（CTL：Communications Technology Laboratory）
- エンジニアリング研究所（EL：Engineering Laboratory）
- 情報技術研究所（ITL：Information Technology Laboratory）
- 材料計測研究所（MML：Material Measurement Laboratory）
- 物理計測研究所（PML：Physical Measurement Laboratory）
- NISTニューロン研究センター（NCNR：NIST Center for Neutron Research）
- ナノスケール科学技術センター（Center for Nanoscale Science & Technology）

このうち情報技術研究所は、情報システム技術に関する標準、測定、相互運用性のテスト、セキュリティ、有用性、及び情報システムの信頼性に関する技術を開発し、普及させるミッションを持ち、下記の6部門で構成される。このうちセキュリティに関する活動を担当するのは、高度ネットワーク技術部（ルーティング等のネットワーク

セキュリティ）、応用サイバーセキュリティ部、コンピュータセキュリティ部、情報アクセス部の 4 部門である。

- 高度ネットワーク技術部（Advanced Network Technologies Division）
- 応用計算数学部（Applied and Computational Mathematics Division）
- 応用サイバーセキュリティ部（Applied Cybersecurity Division）
- コンピュータセキュリティ部（Computer Security Division）
- 情報アクセス部（Information Access Division）
- ソフトウェア・システム部（Software and Systems Division）

(2) 活動と成果公開

NIST の活動の特徴、及び成果公開の形式について述べる。

(a) 活動

NIST の活動の中心は、産業競争力強化の基盤となる度量衡の計測技術開発とその規格化であり、高度な計測サービス等により、民間における技術の発展を支援している※222。一方で情報技術研究所はこうした規格に基づき、連邦政府が遵守すべき調達規格やガイドラインを策定しているが、この規格には IT システムの運用が含まれ、結果として連邦政府機関のセキュリティ対策を主導している。規格策定における NIST の活動の特徴は、産学の専門家と連携する、あるいはドラフト段階から内容を公開したりワークショップを開催したりして積極的に外部のフィードバックを求める、等のオープン性にあると考えられる。

更に NIST は、策定した規格の機器・ツール等への実装を産学官連携の枠組みで支援し、成果の民間移管を促している。セキュリティ分野では情報技術研究所内の NCCoE（National Cybersecurity Center of Excellence）がこれを担当する※223。NCCoE では例えば、サプライチェーンリスク管理プラクティス SP 1800-34 ドラフト版に基づく「調達コンピュータ機器の検証」の方式実装に向けたプロジェクトを実施中である（2021 年 4 月現在）※224。SP 1800-34 がまだドラフト段階でありながら実装プロジェクトを立ち上げ、パブリックコメント募集もその中で実施する点は非常に機動的であると感じられる。

NIST はまた、連邦資金研究開発センター（FFRDCs: Federally Funded Research and Development Centers）の一つである非営利組織 MITRE Corporation※225（以下、MITRE 社）のスポンサーとなっている。サイバーセキュリティ分野では、MITRE 社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）、サイバー攻撃のライフサイクルに基づく攻撃手法・対策知識ベース MITRE ATT&CK※226 等の活動で近年注目されているが、NIST はこのような民間で利用されるツールの実装を視野に入れつつ、規格を策定することが可能である。

NIST の活動のもう一方の特徴として、将来を見据えた研究と評価がある。NIST には個々の技術分野の専門家が集まっており、将来的な技術の方向性を明らかにする研究や技術評価が行われる。セキュリティ分野においては例えば、耐量子暗号アルゴリズムの提案評価プロジェクト（PQC：Post-Quantum Cryptography）を主導している※227。技術革新と将来的な規格化を視野に入れたものと考えられる。なお、PQC の最新動向は「2.8.2 (2) 公開鍵暗号に関する研究及び標準化の動向」を参照されたい。

以上のように NIST の活動は、企業の産業競争力強化と連邦政府機関の技術導入の双方を支援する、機器や部品の計測から IT システムの運用まで、及び研究開発から産学官連携による成果移管までを行う等、非常に多面的、重層的である。計測等の基盤技術を把握し、産学と連携した実装までをスコープとしていることが、NIST の規格・ガイドラインへの信頼を生み出しているものと考えられる。

(b) 成果公開

NIST の活動成果は主に出版物として公開される。ドラフト段階にある文書も公開され、自由に意見を提出できる。前述のミッションに基づき、NIST は産業競争力強化のための測定技術研究、及び技術規格の標準・ガイドライン策定の二つの活動を行うが、公開文書はそれに従い、以下のような分類となっている。

- 連邦情報処理標準（FIPS：Federal Information Processing Standards）
  連邦政府機関が利用する情報通信機器に法令で求められるセキュリティ技術標準。
- SP（Special Publication）
  FIPS の実践に役立つ勧告やベストプラクティスを記載した文書。このうち SP 800 シリーズは具体的なセキュリティ要件、管理策、ガイドライン等がまとめられている。

- NISTIR（NIST Interagency/Internal Report）
  FIPS や SP 策定に関する技術研究や仕様検討等の報告。中間成果も公開される。

各シリーズは別々に策定されるが、特定トピックの要件・管理策・プラクティス・技術報告のように、相互に関連し合う文書群として利用されることもある。

3.4.2 成果紹介

以下では、2020 年度に公開された成果を中心に、文書シリーズごとに紹介する。

(1) FIPS

NIST は、連邦情報セキュリティマネジメント法（FISMA：Federal Information Security Management Act of 2002）に基づき、連邦政府に求められるセキュリティ要件を策定する責務を負う。この要件に関する規格文書が連邦情報処理標準（FIPS：Federal Information Processing Standards）である。代表的な規格として、連邦政府が扱う情報や情報システムのセキュリティレベル、及びセキュリティ脅威の影響度に関する分類規格 FIPS 199、連邦政府の情報や情報システムに対する最低限のセキュリティ要件を定めた規格 FIPS 200 がある[※228]。2020 年 11 月には、連邦政府職員・契約事業者のアイデンティティ情報の検証に関する FIPS 201-3ドラフト版が公開され、2021 年 2 月 11 日まで意見募集が行われた[※229]。2020 年度に発行された FIPS の出版物は表 3-4-1 のとおりである。

(2) SP 800 シリーズ

SP 800 シリーズは情報セキュリティ全般にわたるガイド、推奨、技術仕様、NIST 活動報告に関する文書[※230]である。2020 年度に発行された主な SP 800 シリーズの出版物は表 3-4-1 のとおりである。

(3) SP 1800 シリーズ

実用的で使用可能なサイバーセキュリティソリューションに関する文書である。ベストプラクティスが記載される等、実践的であり、SP 800-53 や Cybersecurity Framework 等との対応も記載される。コンプライアンス対応状況も把握しやすい。2020 年度に発行された SP 1800 シリーズの出版物は表 3-4-1 のとおりである。

識別子	タイトル	ステータス	公開日	概要	関連規格・IR
連邦情報処理標準（FIPS）					
FIPS 201-3 (Draft)	Personal Identity Verification (PIV) of Federal Employees and Contractors	Draft	2020 年 11 月 2 日	連邦職員・契約者の身分証明	—
ガイド・管理策（SP 800 シリーズ）					
SP 800-213	IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements	Draft	2020 年 12 月 15 日	IoT 機器のセキュリティガイド	NISTIR 8259B NISTIR 8259C NISTIR 8259D
SP 800-210	General Access Control Guidance for Cloud Systems	Final	2020 年 7 月 31 日	クラウドのアクセス制御ガイド	—
SP 800-209	Security Guidelines for Storage Infrastructure	Final	2020 年 10 月 26 日	ストレージ基盤アーキテクチャのセキュリティガイド	—
SP 800-208	Recommendation for Stateful Hash-Based Signature Schemes	Final	2020 年 10 月 29 日	ハッシュベース署名スキームの推奨アルゴリズム	—
SP 800-207	Zero Trust Architecture	Final	2020 年 8 月 11 日	ゼロトラストアーキテクチャ（日本語版発行）	—
SP 800-181 Rev. 1	Workforce Framework for Cybersecurity (NICE Framework)	Final	2020 年 11 月 16 日	セキュリティ人材育成フレームワーク	NISTIR 8355

■表 3-4-1　2020 年に発行された出版物（FIPS、SP 800 シリーズ、SP 1800 シリーズ）(1/3)

識別子	タイトル	ステータス	公開日	概要	関連規格・IR
SP 800-172	Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171	Final	2021 年 2 月 2 日	SP 800-171 Rev. 2 の追補	SP 800-171 Rev. 2
SP 800-171 Rev. 2	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	Final	2021 年 1 月 28 日	政府調達事業者の CUI 保護規定（日本語版発行）	SP 800-172 SP 800-161 Rev. 1
SP 800-161 Rev. 1	Cyber Supply Chain Risk Management Practices for Systems and Organizations	Draft	2021 年 4 月 29 日	サイバーサプライチェーンリスク管理プラクティス	SP 800-171 Rev. 2 NISTIR 8276
SP 800-140	FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759	Final	2020 年 3 月 20 日	暗号モジュール検証プログラム（CMVP）の FIPS 140-3 発行に伴う改訂（「2.6.2 暗号モジュール試験及び認証制度」参照）	SP 800-140A SP 800-140B SP 800-140C SP 800-140D SP 800-140E SP 800-140F
SP 800-137A	Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment	Final	2020 年 5 月 21 日	情報セキュリティ継続モニタリング（ISCM）のアセスメント	SP 800-137 NISTIR 8212
SP 800-124 Rev. 2	Guidelines for Managing the Security of Mobile Devices in the Enterprise	Draft	2020 年 3 月 24 日	企業のモバイルセキュリティガイドライン	—
SP 800-77 Rev. 1	Guide to IPsec VPNs	Final	2020 年 6 月 30 日	IPsec 利用ガイド	—
SP 800-57 Part1 Rev. 5	Recommendation for Key Management: Part 1 – General	Final	2020 年 5 月 4 日	鍵管理ガイドの改訂	SP 800-57 Part2 Rev. 1 SP 800-57 Part3 Rev. 1
SP 800-56C Rev. 2	Recommendation for Key-Derivation Methods in Key-Establishment Schemes	Final	2020 年 8 月 18 日	秘密分散の鍵生成に関する推奨	SP 800-56A Rev. 3 SP 800-56B Rev. 2
SP 800-53 Rev. 5	Security and Privacy Controls for Information Systems and Organizations	Final	2020 年 9 月 23 日（2020 年 12 月 10 日更新）	組織のセキュリティ・プライバシー管理策（民間組織を含む）	SP 800-53A Rev. 4（Rev. 4 は日本語版発行） SP 800-53B
SP 800-53B	Control Baselines for Information Systems and Organizations	Final	2020 年 12 月 10 日	政府システムのベースライン管理策	SP 800-53 Rev. 5
プラクティス（SP 1800 シリーズ）					
SP 1800-34	Validating the Integrity of Computing Devices (Preliminary Draft)	Draft	2021 年 3 月 17 日	コンピュータデバイスの検証（サプライチェーンリスク管理）	—
SP 1800-33	5G Cybersecurity (Preliminary Draft)	Draft	2021 年 2 月 1 日	5G セキュリティ	—
SP 1800-31	Improving Enterprise Patching for General IT Systems: Utilizing Existing Tools and Performing Processes in Better Ways (Preliminary Draft)	Draft	2020 年 9 月 10 日	企業システムパッチ強化：ツール利用・プロセスの改善	—
SP 1800-30	Securing Telehealth Remote Patient Monitoring Ecosystem (2nd Draft)	Draft	2021 年 5 月 6 日	遠隔医療モニタリング	—

■表 3-4-1　2020 年に発行された出版物（FIPS、SP 800 シリーズ、SP 1800 シリーズ）(2/3)

識別子	タイトル	ステータス	公開日	概要	関連規格・IR
SP 1800-27	Securing Property Management Systems	Final	2021 年 3 月 30 日	資産管理	—
SP 1800-26	Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events	Final	2020 年 12 月 8 日	データ保護：ランサムウェア検知・対応	SP 1800-11 SP 1800-25
SP 1800-25	Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events	Final	2020 年 12 月 8 日	データ保護：ランサムウェアからの資産保護	SP 1800-11 SP 800-26
SP 1800-24	Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector	Final	2020 年 12 月 21 日	医療画像保護	—
SP 1800-23	Energy Sector Asset Management: For Electric Utilities, Oil & Gas Industry	Final	2020 年 5 月 20 日	エネルギー産業の資産保護	—
SP 1800-21	Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)	Final	2020 年 9 月 15 日	業務用モバイル機器のセキュリティ	—
SP 1800-19	Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments	Draft	2020 年 4 月 13 日	トラステッドクラウド	
SP 1800-16	Securing Web Transactions: TLS Server Certificate Management	Final	2020 年 6 月 16 日	TLS サーバ証明書管理	—
SP 1800-15	Securing Small Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)	Final	2021 年 5 月 26 日	中小企業・ホーム IoT 機器の保護	—
SP 1800-11	Data Integrity: Recovering from Ransomware and Other Destructive Events	Final	2020 年 9 月 22 日	データ保護：ランサムウェア事故復旧	SP 1800-25 SP 1800-26

※年次報告、ドラフト未公開のものは記載していない。

■表 3-4-1　2020 年に発行された出版物（FIPS、SP 800 シリーズ、SP 1800 シリーズ）(3/3)

(4) フレームワーク

「3.4.1 (2)(b) 成果公開」で記載したシリーズ以外の文書で重要なものに Cybersecurity Framework、Privacy Framework がある。このほか、包括的なリスクマネジメントの枠組みとして Risk Management Framework（RMF）がある。SP シリーズ（SP 800-37 Rev.2）として文書化され、Rev.1 は日本語化されている（p.231 表 3-4-3）。これらは連邦政府機関だけでなく、重要インフラ企業を含む民間企業のセキュリティマネジメント、プライバシーマネジメントに関して、経営層とセキュリティ部門のコミュニケーションツールとして策定されている。

2020 年に公開された NISTIR 文書、フレームワークは表 3-4-2（次ページ）のとおりである。

(5) 注目される規格・プロジェクト

2020 年度で注目された規格・プロジェクトについて紹介する。

(a) SP 800-53 Rev. 5 の発行

SP 800-53 は連邦政府機関のセキュリティ管理策標準であるが、近年は ISO/IEC 27001、27002 と並び各国のセキュリティ規格策定において参照され、影響を与え続けている。第 5 版は、2014 年 1 月の第 4 版更新以来 7 年ぶりの改訂となり、クラウド・モバイル・IoT 等の管理対象範囲の拡大、プライバシー保護等への要請を踏まえ、2020 年 9 月 23 日に公開、同年 12 月 10 日に更新された。管理対象を政府組織から民間組織に拡張し、20 のカテゴリーにおいて 1,000 を越える多様な管理

識別子	タイトル	ステータス	公開日	概要	関連規格・IR、法令
組織横断・内部報告（NISTIR シリーズ）					
NISTIR 8323	Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services	Final	2021 年 2 月 11 日	測位サービスのセキュリティプロファイル	大統領令 13905（2020 年 2 月 12 日）
NISTIR 8320A	Hardware-Enabled Security: Container Platform Security Prototype	Draft	2020 年 12 月 7 日	ハードウェアセキュリティ：コンテナ基盤セキュリティ	NISTIR 8320
NISTIR 8312	Four Principles of Explainable Artificial Intelligence (Draft)	Draft	2020 年 8 月 18 日	説明可能な AI に関する 4 原則	—
NISTIR 8309	Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process	Final	2020 年 7 月 22 日	NIST の耐量子暗号標準化状況報告	NISTIR 8240
NISTIR 8301	Blockchain Networks: Token Design and Management Overview	Final	2021 年 2 月 9 日	ブロックチェーンネットワーク：トークン設計と管理	NISTIR 8202
NISTIR 8294	Symposium on Federally Funded Research on Cybersecurity of Electric Vehicle Supply Equipment (EVSE)	Final	2020 年 4 月 29 日	電気自動車充電装置（EVSE）のセキュリティシンポジウム	—
NISTIR 8287	A Roadmap for Successful Regional Alliances and Multistakeholder Partnerships to Build the Cybersecurity Workforce	Final	2020 年 2 月 20 日	セキュリティ人材育成の地域連携プログラム	—
NISTIR 8286A	Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)	Draft	2020 年 12 月 14 日	企業リスク管理におけるセキュリティリスク評価	NISTIR 8286
NISTIR 8286	Integrating Cybersecurity and Enterprise Risk Management (ERM)	Final	2020 年 10 月 13 日	企業リスク管理へのサイバーセキュリティの統合	NISTIR 8286A NISTIR 8170
NISTIR 8278A	National Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers	Final	2020 年 11 月 20 日	OLIR（NIST 規格と他規格のリファレンス）：標準リファレンス作成ガイド	NISTIR 8278
NISTIR 8278	National Online Informative References (OLIR) Program: Program Overview and OLIR Uses	Final	2020 年 11 月 20 日	OLIR：プログラム概要と利用	大統領令 13636
NISTIR 8276	Key Practices in Cyber Supply Chain Risk Management: Observations from Industry	Final	2021 年 2 月 11 日	産業界のサプライチェーンリスク管理プラクティス	SP 800-161 Rev. 1
NISTIR 8259D	Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government	Draft	2020 年 12 月 15 日	IoT コアベースライン、非技術ベースラインの連邦政府機関プロファイル	SP 800-213 NISTIR 8259 NISTIR 8259A NISTIR 8259B NISTIR 8259C
NISTIR 8259C	Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline	Draft	2020 年 12 月 15 日	IoT コアベースライン、非技術ベースラインの作成	SP 800-213 NISTIR 8259 NISTIR 8259A NISTIR 8259B NISTIR 8259D

■表 3-4-2　2020 年に発行された出版物（NISTIR シリーズ、フレームワーク）（1/2）

識別子	タイトル	ステータス	公開日	概要	関連規格・IR、法令
NISTIR 8259B	IoT Non-Technical Supporting Capability Core Baseline	Draft	2020 年 12 月 15 日	IoT 機器製造者の非技術（共通）セキュリティ実践能力	SP 800-213 NISTIR 8259 NISTIR 8259A NISTIR 8259C NISTIR 8259D
NISTIR 8259	Foundational Cybersecurity Activities for IoT Device Manufacturers	Final	2020 年 5 月 29 日	IoT 機器製造者の基本的セキュリティ対策	SP 800-213 NISTIR 8228
NISTIR 8246	Collaborative Vulnerability Metadata Acceptance Process (CVMAP) for CVE Numbering Authorities (CNAs) and Authorized Data Publishers	Final	2020 年 12 月 15 日	CVMAP（脆弱性メタデータ共同受容プロセス）	—
NISTIR 8235	Security Guidance for First Responder Mobile and Wearable Devices	Draft	2020 年 9 月 28 日	救急モバイル・ウェアラブル機器のセキュリティガイド	—
NISTIR 8219	Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection	Final	2020 年 7 月 16 日	製造制御システムの保護：動作異常検知	—
NISTIR 8214A	NIST Roadmap Toward Criteria for Threshold Schemes for Cryptographic Primitives	Final	2020 年 7 月 7 日	秘密分散のしきい値法に関する基準策定ロードマップ	NISTIR 8214
NISTIR 8212	ISCMA: An Information Security Continuous Monitoring Program Assessment	Final	2021 年 3 月 31 日	ISCMA（セキュリティ継続モニタリングプログラム）の評価	SP 800-137 SP 800-137A
NISTIR 8183 Rev. 1	Cybersecurity Framework Version 1.1 Manufacturing Profile	Final	2020 年 10 月 7 日	製造業向けサイバーセキュリティフレームワーク V1.1 プロファイル	NISTIR 8183
NISTIR 8170	Approaches for Federal Agencies to Use the Cybersecurity Framework	Final	2020 年 3 月 19 日	連邦政府機関のサイバーセキュリティフレームワーク実践事例	NISTIR 8286 SP 800-53 Rev. 5
NISTIR 8006	NIST Cloud Computing Forensic Science Challenges	Final	2020 年 8 月 25 日	クラウドフォレンジックの課題	—
フレームワーク					
Privacy Framework Version 1.0	The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0	Final	2020 年 1 月 16 日	プライバシーフレームワーク	Cybersecurity Framework Version 1.1

■表 3-4-2　2020 年に発行された出版物（NISTIR シリーズ、フレームワーク）（2/2）

策が記載されている。主な改訂のポイントは以下のとおりである。

- 情報セキュリティ管理策とプライバシー管理策の統合
- サプライチェーンリスク管理の統合
- 最新の脅威インテリジェンスとサイバー攻撃データに基づく管理策の追加
- 管理策を成果ベースで構成
- コンテンツ関係の記述改善
- 管理策の選択プロセスの管理策からの分離
- 情報システム・組織の管理策ベースラインの SP 800-53B への移行

なお、同時に公開された SP 800-53B は連邦政府のベースラインとなる管理策をまとめている。

(b) サプライチェーンセキュリティ関連規格・プラクティス

2020 年 2 月 21 日、政府調達事業者に連邦政府機関が提供する情報（CUI：Controlled and Unclassified

Information）の保護規定の改訂第2版SP 800-171 Rev. 2が公開され、2021年1月28日に更新された。続いて2021年2月11日、サイバーサプライチェーンリスク管理について、4年にわたり産業界のキープラクティスを収集してきた結果をまとめたNISTIR 8276確定版が公開された。更に同年4月29日、サイバーサプライチェーンリスク管理プラクティスの改訂版SP 800-161 Rev. 1ドラフト版が公開され、コメントが募集された。

こうした規格群が整備される一方で、2020年12月のSolarWinds事案は米国政府・企業のサプライチェーンセキュリティに深刻な課題があることを示し、2021年5月12日、Biden政権はサプライチェーンセキュリティ対策強化を主眼とする大統領令（以下、大統領令）を発表した（「2.2.2（3）SolarWinds事案とその対応」「2.2.2（7）Biden政権の政策」参照）。この中で、NISTには関係部門と協力し、ソフトウェア開発委託に関するガイドラインの暫定版を180日以内に、完全版を360日以内に発行することが求められた。これまでのNISTによるリスクマネジメントやデータ保護の規格化だけではサプライチェーンセキュリティ対策は不十分とされたと考えられる。ソフトウェア調達分野でNISTがどのようなガイドラインを提示するか、注目される。

（c）IoTセキュリティ関連の規格・ガイダンス

2020年12月15日、NISTは連邦政府機関向けのIoT機器調達におけるデバイスセキュリティガイダンスSP 800-213ドラフト版、及びIoTセキュリティに関する非技術支援機能のベースライン、応用別プロファイル作成、実践事例に関する3件のNISTIR（NISTIR 8259B、8259C、8259D）のドラフト版を公開した。同年12月4日に成立したIoT Cybersecurity Improvement Act of 2020[※231]に呼応したものである。NISTはまた、上記ドラフト版と関連文書群の関連をブログで公開した[※232]。このブログではSP 800-213で定めるセキュリティ要件に対して、NISTIR 8259シリーズで提供されるツールを用いて、SP 800-53等の管理策のカタログから具体的なプラクティスを作ってもらう、という構想が説明されている。

（d）ゼロトラストアーキテクチャ関連ガイド

ゼロトラストアーキテクチャへの関心が高まる中、NISTは2020年8月11日、ゼロトラストアーキテクチャのガイドラインSP 800-207を公開した。ゼロトラストの定義や七つの理念、論理アーキテクチャを記載している。また、リソースの認証・認可・アクセス制御が動的なポリシーによって実施されること等を記載している。

更に2021年5月12日、前述の大統領令において、連邦政府システムのサイバーセキュリティ現代化（Modernization）が重要課題とされ、その施策の筆頭にゼロトラストアーキテクチャが明記された。具体的には、各省庁は既存のNISTの規格・ガイダンスに合わせ、ゼロトラストアーキテクチャを段階的に埋め込む（Migration）計画を60日以内に策定することが求められ、連邦政府において同アーキテクチャの実装が火急の課題となった。

（e）人材育成フレームワーク

2020年11月16日、NISTはサイバーセキュリティ教育・人材育成の国家イニシアティブ（NICE：National Initiative for Cybersecurity Education）に基づく枠組みNICE Frameworkを改訂、SP 800-181 Rev. 1として公開した（「2.3.1（4）NICE Frameworkの改訂」参照）。NICE Frameworkは、各職務で行うセキュリティに関するタスクとそれに必要な知識・スキルを示したリファレンスである。

今回の改訂では、煩雑となっていた用語とその関係が簡易化され、Work Role、Tasks、及びKnowledge、Skillsの各用語が残された。また、セキュリティ人材の呼称をより包括なLearnersとする一方、Learnersの評価の記述を示す用語としてCompetenciesが再導入された。NISTは、Cybersecurity Frameworkの成功にならい、NICE Frameworkもサイバーセキュリティ業務・能力記述の共通言語とし、セキュリティ教育・人材育成のエコシステムを構築したいとしている[※233]。

（f）ランサムウェア対策関連プラクティス

世界的に被害が拡大しているランサムウェア対策について、NISTは前掲のNCCoEにおいて、企業のセキュリティ専門家と対策事例（プラクティス）集の策定を進めてきたが、2020年9月22日にランサムウェア事故からの復旧のプラクティス集SP 1800-11を、12月8日に資産管理・防御のプラクティス集SP 1800-25、及び攻撃検知・対処のプラクティス集SP 1800-26を公開した。これらに記載されたプラクティスは「破壊的イベント」におけるデータ一貫性の維持と事業継続に主眼が置かれ、身代金支払い等の経営判断には言及していない。

2021年5月のColonial Pipeline Companyの石油パイプライン停止により、米国重要インフラ企業のランサムウェア対策は喫緊の課題となった（「2.2.2（5）Colonial Pipeline事案とその対応」参照）。上記プラクティス集の

普及に加え、NISTには更なる事例やガイドラインの策定が求められる可能性がある。

(g)その他の規格

NISTは、2008年に発行した情報セキュリティの性能指標ガイドの改訂版発行(SP 800-55 Rev. 2)を計画し、2020年9月から12月10日まで事前意見募集(Pre-draft Call for Comments)を行った※234。2021年5月時点でRev. 2のドラフト版は発行されていない(表3-4-1には未記載)。今後どのような性能指標ガイドが提示されるか、注目される。

Trump政権は2019年2月、頑健で信頼できるAI利用システム開発の技術標準とツールに関する計画の策定をNISTに命じた※235。NISTはこれを受けて計画を発表、意見募集とワークショップを重ねてきたが、2020年8月18日、説明可能なAI(Explainable AI)の4原則をNISTIR 8312としてドラフト版を公開した。AIの判断結果に関する説明性の担保は、特に統計的機械学習技術の信頼性の課題として広く議論されているが、上記NISTIRはNISTの最初の検討成果として注目された。今後も継続的な成果の公開が期待される。

(6)日本のセキュリティ規格・対策との関係

NISTの規格・活動が日本に与える影響について述べる。

(a)NISTシリーズのインパクト

NISTの策定する要件・管理策は国内政府機関のセキュリティ仕様策定において、ISO/IEC 27000シリーズと並び、参照されることが多くなっている。例えば2020年に運用を開始した「政府情報システムのためのセキュリティ評価制度(ISMAP)※236」の管理基準策定においては、グローバル規格としてISO/IEC 27001、27002とともにSP 800-53 Rev. 4がレビューされた(ISMAPの運用については「2.6.3 政府情報システムのためのセキュリティ評価制度(ISMAP)」参照)。また、政府調達事業者が遵守すべきセキュリティ要件については、SP 800-171が注目され、国内政府機関、国内の調達事業者にレビューされてきた※237。サイバーセキュリティ規格が国内に限定されることは効果的でなく、海外規格との整合・海外との連携が必須であるとの認識が政府にも強まっている。

企業においても、米国政府調達に関わる場合はもちろん、グローバルに事業を展開するためには海外規格への対応は必須である。実効的に米国のセキュリティ規格を牽引するNISTの文書を参照する企業が増えている。

(b)規格の日本語化

NIST出版物の分析、国内への展開は主にIPAがその任を担っている。IPAはNIST出版物の概要を紹介するとともに、重要な規格等について日本語版を公開している※238。主として2011年以降に日本語化されたNIST出版物のうち、IPAのWebサイトで掲載しているものを表3-4-3(次ページ)に示す。なお、日本語化はタイムラグが発生する作業であるため、公開版は必ずしも最新バージョンではない(公開後改訂されたものは表中に明記している)。また、仕様の正しい意味を確認する際には原文を参照していただきたい。

(c)NIST事業との連携

IPAは前述したNIST出版物の展開のほか、政府調達暗号(CRYPTREC)に関する技術討議、脆弱性データベースNVD(National Vulnerability Database)※239、NIST Cybersecurity Frameworkと経済産業省のサイバーセキュリティ経営ガイドラインとの整合等で情報共有・連携を行っている。IPAはまた脆弱性管理について、MITRE社の採番するCVEを活用している。IPA以外では、例えば一般社団法人サイバーリスク情報センター産業横断サイバーセキュリティ検討会(CRIC CSF)※240は、Cybersecurity Frameworkの活用を含むサイバーセキュリティマネジメント強化に取り組み、2018年9月にNISTのワークショップで事例を報告している※241。更に、前掲のPQC等の暗号化アルゴリズムプロジェクトでは、日本の研究者も参画、貢献している。

(7)まとめ

NISTは本来米国企業の産業競争力を強化するための連邦政府機関であり、規格や標準化も米国企業、あるいは連邦政府のために策定される。しかし、これまで見たようにその影響力は大きく、策定される標準やガイドライン・フレームワークは世界から参照されるに足る品質と水準を持っている。日本国内のセキュリティ規格、ガイドライン、対策もNISTの活動と整合を保ち、ときにはNISTと協力して推進していくことが望まれる。

識別子	発行日	タイトル	IPA 掲載日	補足
FIPS				
FIPS 199	2004 年 2 月	連邦政府の情報および情報システムに対するセキュリティ分類規格 Standards for Security Categorization of Federal Information and Information Systems	2006 年 8 月	セキュリティ目的と潜在的影響レベルの定義、セキュリティ分類
FIPS 200	2006 年 2 月	連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項 Minimum Security Requirements for Federal Information and Information Systems	2006 年 9 月	最低限のセキュリティ要求事項と影響レベルに合わせた管理策の選択
FIPS 201-1	2006 年 3 月	連邦職員および委託業者のアイデンティティの検証 Personal Identity Verification (PIV) of Federal Employees and Contractors	2011 年 3 月	―
SP 800 シリーズ				
SP 800-30 Rev. 1	2012 年 9 月	リスクアセスメントの実施の手引き Guide for Conducting Risk Assessments	2013 年 2 月	リスクアセスメントの基礎
SP 800-37 Rev. 1	2010 年 2 月	連邦政府情報システムに対するリスクマネジメントフレームワーク適用ガイド：セキュリティライフサイクルによるアプローチ Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach	2011 年 3 月	2018 年 12 月 20 日 Rev. 2 発行（未訳）
SP 800-40 Rev. 2	2005 年 11 月	パッチおよび脆弱性管理プログラムの策定 Creating a Patch and Vulnerability Management Program	2007 年 12 月	2013 年 7 月 22 日 Rev. 3 発行（未訳）
SP 800-52 Rev. 1	2014 年 4 月	トランスポート層セキュリティ(TLS)実装の選択、設定、および使用のためのガイドライン Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations	2017 年 1 月	2019 年 8 月 29 日 Rev. 2 発行（未訳）
SP 800-53 Rev. 4	2013 年 4 月	連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策 Recommended Security Controls for Federal Information Systems	2017 年 1 月	2020 年 12 月 10 日 Rev. 5 更新（未訳）
SP 800-57 Part 1 Rev. 5	2020 年 5 月	鍵管理における推奨事項　第一部：一般事項 Recommendation for Key Management Part 1: General	2021 年 5 月	―
SP 800-57 Part 3 Rev. 1	2015 年 1 月	鍵管理における推奨事項　第三部：アプリケーション特有の鍵管理ガイダンス Recommendation for Key Management Part 3: Application-Specific Key Management Guidance	2016 年 11 月	―
SP 800-61 Rev. 1	2008 年 3 月	コンピュータインシデント対応ガイド Computer Security Incident Handling Guide	2009 年 1 月	2012 年 8 月 6 日 Rev. 2 発行（未訳）
SP 800-63	2006 年 4 月	電子的認証に関するガイドライン Electronic Authentication Guideline	2007 年 8 月	2017 年 12 月 1 日 63-3 発行（未訳） 2020 年 6 月 8 日 63-4 ドラフト版発行（未訳）
SP 800-70	2005 年 5 月	IT 製品のためのセキュリティ設定チェックリストプログラム - チェックリスト利用者と開発者のための手引き Security Configuration Checklists Program for IT Products - Guidance for Checklists Users and Developers	2007 年 3 月	2018 年 2 月 15 日 Rev. 4 発行（未訳）
SP 800-73 Rev. 1	2005 年 4 月	個人識別情報の検証インタフェース Interfaces for Personal Identity Verification	2006 年 10 月	2016 年 2 月 12 日 73-4 発行（未訳）

■表 3-4-3　日本語化された主な NIST 出版物（FIPS、SP 800 シリーズ、フレームワーク）（2021 年 5 月時点）（1/2）

識別子	発行日	タイトル	IPA 掲載日	補足
SP 800-76-1	2007 年 1 月	個人識別情報の検証における生体認証データ仕様（改訂版） Biometric Data Specification for Personal Identity Verification (Rev. 1)	2009 年 10 月	2013 年 7 月 11 日 76-2 発行（未訳）
SP 800-81	2006 年 5 月	セキュアなドメインネームシステム（DNS）の配備ガイド Secure Domain Name System (DNS) Deployment Guide	2009 年 9 月	2013 年 9 月 18 日 81-2 発行（未訳）
SP 800-82 Rev. 2	2015 年 5 月	産業制御システム (ICS) セキュリティ Guide to Industrial Control Systems (ICS) Security	2016 年 3 月	―
SP 800-83	2005 年 11 月	マルウェアによるインシデントの防止と対応のためのガイド Guide to Malware Incident Prevention and Handling	2008 年 9 月	2013 年 7 月 22 日 Rev. 1 発行（未訳）
SP 800-88	2006 年 9 月	媒体のサニタイズに関するガイドライン Guidelines for Media Sanitization	2009 年 9 月	2014 年 12 月 17 日 Rev. 1 発行（未訳）
SP 800-94	2007 年 2 月	侵入検知および侵入防止システム（IDPS）に関するガイド Guide to Intrusion Detection and Prevention Systems (IDPS)	2011 年 3 月	―
SP 800-130	2013 年 8 月	暗号鍵管理システム設計のフレームワーク A Framework for Designing Cryptographic Key Management Systems	2020 年 7 月	―
SP 800-144	2011 年 12 月	パブリッククラウドコンピューティングのセキュリティとプライバシーに関するガイドライン Guidelines on Security and Privacy in Public Cloud Computing	2014 年 3 月	―
SP 800-145	2011 年 9 月	NIST によるクラウドコンピューティングの定義 The NIST Definition of Cloud Computing	2011 年 12 月	NIST によるクラウド定義
SP 800-146	2012 年 5 月	クラウドコンピューティングの概要と推奨事項 Cloud Computing Synopsis and Recommendations	2012 年 8 月	―
SP 800-171 Rev. 2	2020 年 2 月	非連邦政府組織およびシステムにおける管理対象非機密情報 CUI の保護 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	2021 年 2 月	―
SP 800-175A	2016 年 8 月	米国連邦政府での暗号標準利用のためのガイドライン：指令、命令、及び方針 Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies	2021 年 5 月	―
SP 800-175B Rev. 1	2020 年 3 月	米国連邦政府での暗号標準利用のためのガイドライン：暗号メカニズム Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	2021 年 5 月	―
SP 800-190 Rev. 1	2017 年 9 月	アプリケーションコンテナセキュリティガイド Application Container Security Guide	2020 年 9 月	―
SP 800-207	2020 年 8 月	ゼロトラスト・アーキテクチャ Zero Trust Architecture	2020 年 12 月	アーキテクチャ解説
フレームワーク				
Cybersecurity Framework Version 1.1	2018 年 4 月	重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1 版 Framework for Improving Critical Infrastructure Cybersecurity Version 1.1	2019 年 1 月	―

■表 3-4-3　日本語化された主な NIST 出版物（FIPS、SP 800 シリーズ、フレームワーク）（2021 年 5 月時点）（2/2）

※1　NISC が重要インフラの運営を担う事業者と、そこで行われるセキュリティ対策を支援する所管省庁が参照すべき指針として公表している「重要インフラの情報セキュリティ対策に係る行動計画」では、「重要インフラ」として 14 分野が定義されている。
NISC：活動内容　https://www.nisc.go.jp/active/infra/outline.html〔2021/4/27 確認〕
※2　インシデント件数については「JPCERT/CC インシデント報告対応レポート［2013 年 1 月 1 日～ 2013 年 3 月 31 日］」～「JPCERT/CC インシデント報告対応レポート［2020 年 10 月 1 日～ 2020 年 12 月 31 日］」（JPCERT/CC：インシデント報告対応レポート　https://www.jpcert.or.jp/ir/report.html〔2021/4/27 確認〕）を参照した。
※3　TrapX Security Inc.：53% of Manufacturing Organizations Say Operational Technology is Vulnerable to Cyber Attacks　https://trapx.com/53-of-manufacturing-organizations-say-operational-technology-is-vulnerable-to-cyber-attacks/〔2021/4/27 確認〕
※4　Scoop News：Survey Shows Staff Bigger Threat To Cyber And Physical Security Than Cyber Criminals　https://www.scoop.co.nz/stories/BU2003/S00430/survey-shows-staff-bigger-threat-to-cyber-and-physical-security-than-cyber-criminals.htm〔2021/4/27 確認〕
※5　「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。
※6　American Military University Edge：Israeli cyber chief: Major attack on water systems thwarted　https://amuedge.com/israeli-cyber-chief-major-attack-on-water-systems-thwarted/〔2021/4/27 確認〕
※7　The Times of Israel：6 facilities said hit in Iran's cyberattack on Israel's water system in April　https://www.timesofisrael.com/6-facilities-said-hit-in-irans-cyberattack-on-israels-water-system-in-april/〔2021/4/27 確認〕
SecurityWeek：Israel Says Hackers Targeted SCADA Systems at Water Facilities　https://www.securityweek.com/israel-says-hackers-targeted-scada-systems-water-facilities〔2021/4/27 確認〕
※8　ZDNet：Two more cyber-attacks hit Israel's water system　https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/〔2021/4/27 確認〕
※9　The Times of Israel：Cyber attacks again hit Israel's water system, shutting agricultural pumps　https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/〔2021/4/27 確認〕
※10　The Washington Post：Officials: Israel linked to a disruptive cyberattack on Iranian port facility　https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html〔2021/4/27 確認〕
※11　Industrial Cyber：OTORIO confirms Iranian hackers gained access to ICS at an Israeli water reservoir　https://industrialcyber.co/threats-attacks/industrial-cyber-attacks/otorio-confirms-iranian-hackers-gained-access-to-ics-at-an-israeli-water-reservoir/〔2021/4/27 確認〕
※12　OTORIO Ltd.：What We've Learned from the December 1st Attack on an Israeli Water Reservoir?　https://www.otorio.com/blog/what-we-ve-learned-from-the-december-1st-attack-on-an-israeli-water-reservoir/〔2021/4/27 確認〕
※13　SecurityWeek：Major Power Outage in India Possibly Caused by Hackers: Reports　https://www.securityweek.com/major-power-outage-india-possibly-caused-hackers-reports〔2021/4/27 確認〕
※14　ZDNet：Hacker modified drinking water chemical levels in a US city　https://www.zdnet.com/article/hacker-modified-drinking-water-chemical-levels-in-a-us-city/〔2021/4/27 確認〕
ZDNet：Following Oldsmar attack, FBI warns about using TeamViewer and Windows 7
https://www.zdnet.com/article/following-oldsmar-attack-fbi-warns-about-using-teamviewer-and-windows-7/〔2021/4/27 確認〕
CyberScoop：Investigators suggest hackers exploited weak password security to breach Florida water facility　https://www.cyberscoop.com/florida-water-facility-hack-password/〔2021/4/27 確認〕
※15　The Brussels Times：Cyber attack sees Picanol shares suspended　https://www.brusselstimes.com/news-contents/economic/89253/cyber-attack-sees-picanol-shares-suspended/〔2021/4/27 確認〕
Picanol：Press release: cyber attack - update January 31, 2020
https://www.picanol.be/news/press-release-cyber-attack-update-january-31-2020〔2021/4/27 確認〕
※16　Dragos, Inc.：Assessment of Ransomware Event at U.S. Pipeline Operator　https://www.dragos.com/blog/industry-news/assessment-of-ransomware-event-at-u-s-pipeline-operator/〔2021/4/27 確認〕
CISA：Alert (AA20-049A)Ransomware Impacting Pipeline Operations　https://us-cert.cisa.gov/ncas/alerts/aa20-049a〔2021/4/27 確認〕
※17　ZDNet：One of Roman Abramovich's companies got hit by ransomware　https://www.zdnet.com/article/one-of-roman-abramovichs-companies-got-hit-by-ransomware/〔2021/4/27 確認〕
※18　iTnews：BlueScope IT 'disruption' feared to be ransomware attack　https://www.itnews.com.au/news/bluescope-it-disruption-feared-to-be-ransomware-attack-548127〔2021/4/27 確認〕
BlueScope Steel Limited：BLUESCOPE RESPONSE TO CYBER INCIDENT　https://secure.weblink.com.au/clients/WebChartClient/clients/BlueScopeSteel2/article.asp?view=3541284〔2021/4/27 確認〕
※19　iTnews：Fisher & Paykel Appliances struck by Nefilim ransomware　https://www.itnews.com.au/news/fisher-paykel-appliances-struck-by-nefilim-ransomware-549102〔2021/4/27 確認〕
※20　Business Wire：X-FAB Affected by Cyber Attack　https://www.businesswire.com/news/home/20200705005045/en/X-FAB-Affected-Cyber-Attack〔2021/4/27 確認〕
Business Wire：X-FAB on Track to Resume Production After Cyber Attack　https://www.businesswire.com/news/home/20200712005045/en/X-FAB-Track-Resume-Production-Cyber-Attack〔2021/4/27 確認〕
※21　The Times of Israel：Israeli chip manufacturer Tower says it was targeted in cyberattack　https://www.timesofisrael.com/israeli-chip-manufacturer-tower-says-it-was-targeted-in-cyberattack/〔2021/4/27 確認〕
eeNews Europe：Cyberattack is resolved but will hit Tower's results　https://www.eenewseurope.com/news/cyberattack-resolved-will-hit-towers-results〔2021/4/27 確認〕
※22　NorfolkToday.ca：A Ransomware Attack Temporarily Shut Down Steel Production At Stelco　https://www.norfolktoday.ca/2020/10/28/a-ransomware-attack-temporarily-shut-down-steel-production-at-stelco/〔2021/4/27 確認〕
※23　BleepingComputer：Steelcase furniture giant down for 2 weeks after ransomware attack　https://www.bleepingcomputer.com/news/security/steelcase-furniture-giant-down-for-2-weeks-after-ransomware-attack/〔2021/4/27 確認〕
※24　Dragos, Inc.：EKANS Ransomware and ICS Operations　https://dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/〔2021/4/27 確認〕
※25　AO Kaspersky Lab：Targeted attacks on industrial companies using Snake ransomware　https://ics-cert.kaspersky.com/alerts/2020/06/17/targeted-attacks-on-industrial-companies-using-snake-ransomware/〔2021/4/27 確認〕
※26　BANK INFO SECURITY：Honda Confirms Hack Attack Disrupted Global Production　https://www.bankinfosecurity.com/honda-confirms-cyberattack-affecting-global-production-a-14410〔2021/4/27 確認〕
※27　BleepingComputer：Enel Group hit by ransomware again, Netwalker demands $14 million　https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million/〔2021/4/27 確認〕
※28　ZDNet：Microsoft, FireEye confirm SolarWinds supply chain attack　https://www.zdnet.com/article/microsoft-fireeye-confirm-solarwinds-supply-chain-attack/〔2021/4/27 確認〕
※29　ChannelE2E：SolarWinds Orion Security Breach: Cyberattack Timeline and Hacking Incident Details　https://www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details/〔2021/4/27 確認〕
※30　ITmedia エンタープライズ：第 4 のマルウェア「Raindrop」発見 続く SolarWinds サイバー攻撃の解析　https://www.itmedia.co.jp/enterprise/articles/2101/20/news118.html〔2021/4/27 確認〕
※31　ITmedia NEWS：1 年以上も検出できなかった「史上最大級の高度な攻撃」、同じ弱点は世界中に　https://www.itmedia.co.jp/news/articles/2101/25/news064.html〔2021/4/27 確認〕
※32　POLITICO：How suspected Russian hackers outed their massive cyberattack　https://www.politico.com/news/2020/12/

16/russian-hackers-fireeye-cyberattack-447226〔2021/4/27 確認〕
FireEye, Inc.：Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html〔2021/4/27 確認〕
※ 33 AO Kaspersky Lab：SunBurst industrial victims https://ics-cert.kaspersky.com/reports/2021/01/26/sunburst-industrial-victims/〔2021/4/27 確認〕
※ 34 CISA：Alert (AA20-352A)：Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations https://us-cert.cisa.gov/ncas/alerts/aa20-352a〔2021/4/27 確認〕
※ 35 Reuters：Exclusive: Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency – sources https://www.reuters.com/article/us-cyber-solarwinds-china/exclusive-suspected-chinese-hackers-used-solarwinds-bug-to-spy-on-u-s-payroll-agency-sources-idUSKBN2A22K8〔2021/4/27 確認〕
※ 36 https://discover.honeywell.com/USBThreatReport-8156-Registrationpage.html〔2021/4/27 確認〕
※ 37 ICS-CERT の Web サイトで暦年（1/1 ～ 12/31）ごとに公開された ICSA Advisories の件数をカウントした。ただし、ICSMA（医療機器の脆弱性）は除く。カウントは公表日ベースとした（公表日が 2020 年なら、採番年度が 2019（ICSA-2019-xxx-x）でも 2020 年でカウント）。
NCCIC：ICS-CERT Advisories https://ics-cert.us-cert.gov/advisories〔2021/4/27 確認〕
※ 38 JSOF Ltd.：Ripple20 https://www.jsof-tech.com/disclosures/ripple20/〔2021/4/27 確認〕
※ 39 https://nvd.nist.gov/vuln/detail/CVE-2020-25191〔2021/4/27 確認〕
※ 40 SecurityWeek：Vulnerability in NI Controller Can Allow Hackers to Remotely Disrupt Production https://www.securityweek.com/vulnerability-ni-controller-can-allow-hackers-remotely-disrupt-production〔2021/5/27 確認〕
※ 41 CISA：ICS Advisory (ICSA-20-338-01) National Instruments CompactRIO https://us-cert.cisa.gov/ics/advisories/icsa-20-338-01〔2021/4/27 確認〕
※ 42 NISC：Fortinet 製 VPN の脆弱性 (CVE-2018-13379) に関する重要インフラ事業者等についての注意喚起の発出について https://www.nisc.go.jp/active/infra/pdf/fortinet20201203.pdf〔2021/4/27 確認〕
※ 43 NIST：CVE-2018-13379 Detail https://nvd.nist.gov/vuln/detail/CVE-2018-13379〔2021/4/27 確認〕
※ 44 Dragos, Inc.：Ransomware in ICS Environments https://www.dragos.com/resource/ransomware-in-ics-environments/〔2021/4/27 確認〕
※ 45 Back End News：Sophos releases cyber attack trends to shape IT security in 2020 https://backendnews.net/sophos-releases-cyber-attack-trends-to-shape-it-security-in-2020/〔2021/4/27 確認〕
※ 46 PhishLabs：Year In Review: Ransomware https://info.phishlabs.com/blog/year-in-review-ransomware〔2021/4/27 確認〕
※ 47 BleepingComputer：US aerospace services provider breached by Maze Ransomware https://www.bleepingcomputer.com/news/security/us-aerospace-services-provider-breached-by-maze-ransomware/〔2021/4/27 確認〕
※ 48 BleepingComputer：Chipmaker MaxLinear reports data breach after Maze Ransomware attack https://www.bleepingcomputer.com/news/security/chipmaker-maxlinear-reports-data-breach-after-maze-ransomware-attack/〔2021/4/27 確認〕
※ 49 https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_Control_Systems_S508C.pdf〔2021/4/27 確認〕
※ 50 NIST：NISTIR 8183 Rev. 1 https://csrc.nist.gov/publications/detail/nistir/8183/rev-1/final〔2021/4/27 確認〕
※ 51 Marine Log：Cybersecurity: Attacks on OT systems are on the increase https://www.marinelog.com/news/cybersecurity-attacks-on-ot-systems-are-on-the-increase/〔2021/4/27 確認〕
※ 52 IMO：RESOLUTION MSC.428(98) https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428(98).pdf〔2021/4/27 確認〕
※ 53 https://www.intercargo.org/wp-content/uploads/2020/05/2021-12-23-Guidelines-on-Cyber-Security-Onboard-Ships-v.4.pdf〔2021/4/27 確認〕
※ 54 ENISA：Cybersecurity in the Maritime Sector: ENISA Releases New Guidelines for Navigating Cyber Risk https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-maritime-sector-enisa-releases-new-guidelines-for-navigating-cyber-risk〔2021/4/27 確認〕
※ 55 ENISA：Port Cybersecurity - Good practices for cybersecurity in the maritime sector https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector〔2021/4/27 確認〕
※ 56 サイバーセキュリティ戦略本部：サイバーセキュリティ 2020（2019 年度年次報告・2020 年度年次計画） https://www.nisc.go.jp/active/kihon/pdf/cs2020.pdf〔2021/4/27 確認〕
※ 57 https://t-isac.or.jp/〔2021/4/27 確認〕
※ 58 内閣府：Society 5.0 https://www8.cao.go.jp/cstp/society5_0/〔2021/4/27 確認〕
※ 59 経済産業省：Connected Industries https://www.meti.go.jp/policy/mono_info_service/connected_industries/index.html〔2021/4/27 確認〕
※ 60 経済産業省：IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）を策定しました https://www.meti.go.jp/press/2020/11/20201105003/20201105003.html〔2021/4/27 確認〕
※ 61 https://www.meti.go.jp/press/2020/02/20210222004/20210222004-1.pdf〔2021/6/10 確認〕
※ 62 IPA：「制御システムのセキュリティリスク分析ガイド 第 2 版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～」を公開 https://www.ipa.go.jp/security/controlsystem/riskanalysis.html〔2021/4/27 確認〕
※ 63 IPA：制御システムのセキュリティリスク分析ガイド：セミナー https://www.ipa.go.jp/security/controlsystem/seminar.html〔2021/4/27 確認〕
※ 64 IPA：制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ https://www.ipa.go.jp/security/controlsystem/incident.html〔2021/4/27 確認〕
※ 65 詳細リスク分析手法の一つで、サイバー攻撃で想定される事業被害に基づいてリスク分析を行う。
※ 66 NIST：National Vulnerability Database（NVD） https://nvd.nist.gov/〔2021/4/28 確認〕
※ 67 IPA：JVN iPedia 脆弱性対策情報データベース https://jvndb.jvn.jp/〔2021/4/28 確認〕
※ 68 OffSec Services Limited：Exploit Database https://www.exploit-db.com/〔2021/4/28 確認〕
※ 69 感染した IoT 機器上で不正なプログラムを実行し、ボットネットを構成するとともに、DDoS 攻撃の踏み台等のサイバー攻撃への悪用を試みるウイルス。典型例である「Mirai」や「Gafgyt（別名、Bashlite、QBot 等）」は、それぞれソースコードが公開されており、様々な亜種が出現している。Mirai の詳細に関しては、「情報セキュリティ白書 2017」の「3.2.1（1）Mirai による DDoS 攻撃の脅威」（p.174）を参照。
※ 70 PoC（Proof of Concept）：発見された脆弱性を実証するために公開されたプログラムコード。IoT 機器を狙うサイバー攻撃において、不正侵入やウイルス感染を試みる悪意のプログラムの一部として悪用されることがある。
※ 71 警察庁：宛先ポート 4567/TCP に対する Mirai ボットの特徴を有するアクセスの増加等について https://www.npa.go.jp/cyberpolice/detect/pdf/20200226.pdf〔2021/4/28 確認〕
※ 72 mcw0：PoC / TVT_and_OEM_IPC_NVR_DVR_RCE_Backdoor_and_Information_Disclosure.txt https://github.com/mcw0/PoC/blob/master/TVT_and_OEM_IPC_NVR_DVR_RCE_Backdoor_and_Information_Disclosure.txt〔2021/4/28 確認〕
※ 73 リバースシェル：ウイルス感染させた IoT 機器から攻撃者がインターネット上に用意したサーバにアクセスさせることによって、感染 IoT 機器の遠隔操作を試みる攻撃手法。
※ 74 警察庁：複数の IoT 機器等の脆弱性を標的としたアクセスの増加等について https://www.npa.go.jp/cyberpolice/detect/pdf/20200130.pdf〔2021/4/28 確認〕
※ 75 TVT 社：Notification of Critical Vulnerabilities http://en.tvt.net.cn/news/227.html〔2021/4/28 確認〕
※ 76 IPVM：A List Of TVT's 79 DVR OEMs https://ipvm.com/forums/video-surveillance/topics/a-list-of-tvt-s-79-dvr-oems〔2021/4/28 確認〕
※ 77 Trend Micro Incorporated：SORA and UNSTABLE: 2 Mirai Variants Target Video Surveillance Storage Systems https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/sora-and-unstable-2-mirai-variants-target-video-surveillance-storage-systems/〔2021/4/28 確認〕
※ 78 Palo Alto Networks, Inc.：New Mirai Variant Targets Zyxel Network-Attached Storage Devices https://unit42.paloaltonetworks.

com/new-mirai-variant-mukashi/〔2021/4/28 確認〕
パロアルトネットワークス株式会社：Zyxel の NAS の脆弱性（CVE-2020-9054）を標的にした新しい Mirai 亜種、Mukashi が発見される https://unit42.paloaltonetworks.jp/new-mirai-variant-mukashi/〔2021/4/28 確認〕
※ 79 Zyxel 社：Zyxel security advisory for the remote code execution vulnerability of NAS and firewall products https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml〔2021/4/28 確認〕
※ 80 Qihoo 360 Technology Co., Ltd.：Multiple botnets are spreading using LILIN DVR 0-day https://blog.netlab.360.com/multiple-botnets-are-spreading-using-lilin-dvr-0-day-en/〔2021/4/28 確認〕
※ 81 Sophos Ltd.：Chalubo botnet wants to DDoS from your server or IoT device https://news.sophos.com/en-us/2018/10/22/chalubo-botnet-wants-to-ddos-from-your-server-or-iot-device/〔2021/4/28 確認〕
※ 82 fbotの詳細に関しては、「情報セキュリティ白書2020」の「3.2.1（1）（b）fbot」（p.167）を参照。
※ 83 Moobotの詳細に関しては、「情報セキュリティ白書2020」の「3.2.1（1）（h）Moobot」（p.172）を参照。
※ 84 LILIN 社：利凌企業股份有限公司網路商品資安漏洞修正通知／Merit LILIN Network Product Vulnerability Notification https://www.meritlilin.com/assets/uploads/support/file/M00158-TW.pdf〔2021/4/28 確認〕
※ 85 警察庁：Apache Tomcat の脆弱性 (CVE-2020-1938) を標的としたアクセスの観測等について https://www.npa.go.jp/cyberpolice/detect/pdf/20200325.pdf〔2021/4/28 確認〕
※ 86 Habr：Full disclosure: 0day vulnerability (backdoor) in firmware for Xiaongmai-based DVRs, NVRs and IP cameras https://habr.com/en/post/486856/〔2021/4/28 確認〕
※ 87 Xiongmai 社：Security Advisory – Vulnerability of some XM product before year 2017 https://www.xiongmaitech.com/en/index.php/news/info/12/68〔2021/4/28 確認〕
※ 88 https://www.shodan.io/〔2021/4/28 確認〕
※ 89 国立研究開発法人情報通信研究機構 NICTER Blog:ビデオレコーダを狙った 9530/tcp 宛通信の増加について https://blog.nicter.jp/2020/04/nvr-9530/〔2021/4/28 確認〕
※ 90 Qihoo 360 Technology Co., Ltd.：Two zero days are Targeting DrayTek Broadband CPE Devices https://blog.netlab.360.com/two-zero-days-are-targeting-draytek-broadband-cpe-devices-en/〔2021/4/28 確認〕
※ 91 DrayTek 社：Vigor3900 / Vigor2960 / Vigor300B Router Web Management Page Vulnerability (CVE-2020-8515) https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-router-web-management-page-vulnerability-(cve-2020-8515)/〔2021/4/28 確認〕
※ 92 DrayTek 社：DrayTek Security Advisory https://www.draytek.com/about/security-advisory〔2021/4/28 確認〕
※ 93 C&C サーバ：Command and Control サーバの略。ウイルス等により乗っ取ったコンピュータ等（ここでは IoT 機器）に対し、遠隔から命令を送り制御するサーバ。
※ 94 IRC（Internet Relay Chat）：サーバを介してクライアント同士がテキストベースの通信を行うプロトコル。サイバー攻撃において、C&C サーバと乗っ取った IoT 機器との間の通信に悪用される。
※ 95 Palo Alto Networks, Inc.：Grandstream and DrayTek Devices Exploited to Power New Hoaxcalls DDoS Botnet https://unit42.paloaltonetworks.com/new-hoaxcalls-ddos-botnet/〔2021/4/28 確認〕
パロアルトネットワークス株式会社：Grandstream および DrayTek デバイスのエクスプロイトで拡大する新たな Hoaxcalls DDoS ボットネット https://unit42.paloaltonetworks.jp/new-hoaxcalls-ddos-botnet/〔2021/4/28 確認〕
※ 96 Packet Strom：DrayTek Vigor2960 / Vigor3900 / Vigor300B Remote Command Execution https://packetstormsecurity.com/files/156979/DrayTek-Vigor2960-Vigor3900-Vigor300B-Remote-Command-Execution.html〔2021/4/28 確認〕
※ 97 Radware Ltd.：Evolution of Hoaxcalls https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/hoaxcalls-evolution/〔2021/4/28 確認〕
※ 98 IT Security Research by Pierre：Multiple vulnerabilities found in Zyxel CNM SecuManager https://pierrekim.github.io/blog/2020-03-09-zyxel-secumanager-0day-vulnerabilities.html〔2021/4/28 確認〕
※ 99 国家信息安全漏洞共享平台（CNVD：China National Vulnerability Database）：ZyXEL Cloud CNM SecuManager 未授权远程代码执行漏洞 https://www.cnvd.org.cn/flaw/show/CNVD-2020-16839〔2021/4/28 確認〕
※ 100 Zyxel 社：Zyxel security advisory for vulnerabilities of CloudCNM SecuManager https://www.zyxel.com/support/vulnerabilities-of-CloudCNM-SecuManager.shtml〔2021/4/28 確認〕
※ 101 警察庁：Zyxel CNM SecuManager の脆弱性を標的としたアクセスの観測等について https://www.npa.go.jp/cyberpolice/detect/pdf/20200605.pdf〔2021/4/28 確認〕
※ 102 Palo Alto Networks, Inc.：Mirai and Hoaxcalls Botnets Target Legacy Symantec Web Gateways https://unit42.paloaltonetworks.com/hoaxcalls-mirai-target-legacy-symantec-web-gateways/〔2021/4/28 確認〕
パロアルトネットワークス株式会社:Mirai、Hoaxcalls が標的を拡大 サポート終了バージョンの Symantec Web Gateway を狙う https://unit42.paloaltonetworks.jp/hoaxcalls-mirai-target-legacy-symantec-web-gateways/〔2021/4/28 確認〕
※ 103 code16（cody sixteen）：HUNTING 0DAYS with Symantec Web Gateway 5.0.2.8 https://dl.packetstormsecurity.net/2004-exploits/symantecwg5028-exec.pdf〔2021/4/28 確認〕
※ 104 Internet Initiative Japan Inc.：Mirai 亜種（XTC）による感染活動の観測 https://wizsafe.iij.ad.jp/2020/05/967/〔2021/4/28 確認〕
※ 105 Internet Initiative Japan Inc.：wizSafe Security Signal 2020 年 5 月 観測レポート https://wizsafe.iij.ad.jp/2020/06/1004/〔2021/4/28 確認〕
※ 106 Qihoo 360 Technology Co., Ltd.：Multiple fiber routers are being compromised by botnets using 0-day https://blog.netlab.360.com/multiple-fiber-routers-are-being-compromised-by-botnets-using-0-day-en/〔2021/4/28 確認〕
※ 107 Trend Micro Incorporated：Mirai Updates: New Variant Mukashi Targets NAS Devices, New Vulnerability Exploited in GPON Routers, UPX-Packed FBot https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mirai-updates-new-variant-mukashi-targets-nas-devices-new-vulnerability-exploited-in-gpon-routers-upx-packed-fbot〔2021/4/28 確認〕
※ 108 Qihoo 360 Technology Co., Ltd.：The LeetHozer botnet https://blog.netlab.360.com/the-leethozer-botnet-en/〔2021/4/28 確認〕
※ 109 Palo Alto Networks, Inc.：6 New Vulnerabilities Found on D-Link Home Routers https://unit42.paloaltonetworks.com/6-new-d-link-vulnerabilities-found-on-home-routers/〔2021/4/28 確認〕
パロアルトネットワークス株式会社：D-Link ホームルーターで発見された 6 つの新たな脆弱性 https://unit42.paloaltonetworks.jp/6-new-d-link-vulnerabilities-found-on-home-routers/〔2021/4/28 確認〕
※ 110 D-Link 社：DIR-865L :: Rev. Ax :: End of Support / End of Life Product :: Reporting Multiple Vulnerabilities https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10174〔2021/4/28 確認〕
※ 111 Qihoo 360 Technology Co., Ltd.：The new Bigviktor Botnet is Targeting DrayTek Vigor Router https://blog.netlab.360.com/bigviktor-dga-botnet/〔2021/4/28 確認〕
※ 112 Trend Micro Incorporated：New Mirai Variant Expands, Exploits CVE-2020-10173 https://www.trendmicro.com/en_us/research/20/g/new-mirai-variant-expands-arsenal-exploits-cve-2020-10173.html〔2021/4/28 確認〕
トレンドマイクロ株式会社：ルータの脆弱性「CVE-2020-10173」を利用する IoT マルウェア https://blog.trendmicro.co.jp/archives/25896〔2021/4/28 確認〕
※ 113 Medium：Tenda AC15 AC1900 Vulnerabilities Discovered and Exploited https://blog.securityevaluators.com/tenda-ac1900-vulnerabilities-discovered-and-exploited-e8e26aa0bc68〔2021/4/28 確認〕
※ 114 Trend Micro Incorporated：Mirai Botnet Attack IoT Devices via CVE-2020-5902 https://www.trendmicro.com/en_us/research/20/g/mirai-botnet-attack-iot-devices-via-cve-2020-5902.html〔2021/4/28 確認〕
トレンドマイクロ株式会社：「BIG-IP」の脆弱性「CVE-2020-5902」を利用する IoT マルウェアを確認 https://blog.trendmicro.co.jp/archives/26197〔2021/4/28 確認〕
※ 115 F5 社：K52145254: TMUI RCE vulnerability CVE-2020-5902 https://support.f5.com/csp/article/K52145254〔2021/4/28 確認〕
※ 116 GRIMM Blog（SMFS, Inc.）：SOHO Device Exploitation https://blog.grimm-co.com/2020/06/soho-device-exploitation.html〔2021/4/28 確認〕

※ 117 警察庁：ZeroShell の脆弱性を標的としたアクセスの観測について https://www.npa.go.jp/cyberpolice/detect/pdf/20200811.pdf〔2021/4/28 確認〕
※ 118 警察庁：vBulletin の脆弱性（CVE-2020-17496）を標的としたアクセスの観測等について https://www.npa.go.jp/cyberpolice/detect/pdf/20201016.pdf〔2021/4/28 確認〕
※ 119 「情報セキュリティ白書 2019」の「3.2.1 (2) (c) 仮想通貨マイニングへの悪用（ADB.Miner）」（p.167）を参照。
※ 120 Palo Alto Networks, Inc.：3 Vulnerabilities Found on AvertX IP Cameras https://unit42.paloaltonetworks.com/avertx-ip-cameras-vulnerabilities/〔2021/4/28 確認〕
パロアルトネットワークス株式会社：AvertX 製 IP カメラで 3 つの脆弱性が見つかる https://unit42.paloaltonetworks.jp/avertx-ip-cameras-vulnerabilities/〔2021/4/28 確認〕
※ 121 Qihoo 360 Technology Co., Ltd.：Quick update on the Linux.Ngioweb botnet, now it is going after IoT devices https://blog.netlab.360.com/linux-ngioweb-v2-going-after-iot-devices-en/〔2021/4/28 確認〕
※ 122 Qihoo 360 Technology Co., Ltd.：An Analysis of Linux.Ngioweb Botnet https://blog.netlab.360.com/an-analysis-of-linux-ngioweb-botnet-en/〔2021/4/28 確認〕
※ 123 Qihoo 360 Technology Co., Ltd.：Ghost in action: the Specter botnet https://blog.netlab.360.com/ghost-in-action-the-specter-botnet/〔2021/4/28 確認〕
※ 124 Qihoo 360 Technology Co., Ltd.：In the wild QNAP NAS attacks https://blog.netlab.360.com/in-the-wild-qnap-nas-attacks-en/〔2021/4/28 確認〕
※ 125 Qihoo 360 Technology Co., Ltd.：Ttint: An IoT Remote Access Trojan spread through 2 0-day vulnerabilities https://blog.netlab.360.com/ttint-an-iot-remote-control-trojan-spread-through-2-0-day-vulnerabilities/〔2021/4/28 確認〕
※ 126 Qihoo 360 Technology Co., Ltd.：HEH, a new IoT P2P Botnet going after weak telnet services https://blog.netlab.360.com/heh-a-new-iot-p2p-botnet-going-after-weak-telnet-services/〔2021/5/27 確認〕
※ 127 Palo Alto Networks, Inc.：Two New IoT Vulnerabilities Identified with Mirai Payloads https://unit42.paloaltonetworks.com/iot-vulnerabilities-mirai-payloads/〔2021/4/28 確認〕
パロアルトネットワークス株式会社：Mirai 亜種のペイロードに 2 つの新しい IoT 脆弱性を特定 https://unit42.paloaltonetworks.jp/iot-vulnerabilities-mirai-payloads/〔2021/4/28 確認〕
※ 128 サニタイズ（無害化）：値をチェックして攻撃に使用されるコードが含まれていた場合は除去（無効化）すること。
※ 129 警察庁：Oracle WebLogic Server の脆弱性（CVE-2020-14882）を標的としたアクセスの観測等について https://www.npa.go.jp/cyberpolice/detect/pdf/20201224.pdf〔2021/4/28 確認〕
※ 130 Qihoo 360 Technology Co., Ltd.：MooBot on the run using another 0 day targeting UNIX CCTV DVR https://blog.netlab.360.com/moobot-0day-unixcctv-dvr-en/〔2021/4/28 確認〕
※ 131 警察庁：脆弱性が存在する複数の IoT 機器を標的としたアクセスの増加等について https://www.npa.go.jp/cyberpolice/detect/pdf/20210305.pdf〔2021/4/28 確認〕
※ 132 Sophos Ltd.：Glupteba: Hidden Malware Delivery in Plain Sight https://news.sophos.com/wp-content/uploads/2020/06/glupteba_final.pdf〔2021/4/28 確認〕
※ 133 YouTube JSOF Channel：JSOF Ripple20 Exploit UPS https://www.youtube.com/watch?v=jkfNE_Twa1s〔2021/4/28 確認〕
※ 134 ICS-CERT：ICS Advisory (ICSA-20-168-01) Treck TCP/IP Stack (Update G) https://us-cert.cisa.gov/ics/advisories/icsa-20-168-01〔2021/4/28 確認〕
※ 135 Treck 社：Vulnerability Response Information https://treck.com/vulnerability-response-information/〔2021/4/28 確認〕
※ 136 図研エルミック株式会社：KASAGO 製品における脆弱性に関するお知らせ https://www.elwsc.co.jp/wp-content/uploads/2020/06/KASAGO202006-1.pdf〔2021/4/28 確認〕
※ 137 NISC：多くのデバイスが影響を受ける複数の脆弱性「Ripple20」に関する参考情報 https://www.nisc.go.jp/active/infra/pdf/Ripple2020200624.pdf〔2021/4/28 確認〕
※ 138 ブラザー工業株式会社：セキュリティーデータベース脆弱性識別番号 CVE-2020-11896 等、複数の脆弱性の対応について https://support.brother.co.jp/j/b/faqend.aspx?c=jp&lang=ja&prod=group2&faqid=faq00100718_002〔2021/4/28 確認〕
※ 139 デル・テクノロジーズ株式会社：Ripple20 の脆弱性に対するデルの対応 https://www.dell.com/support/kbdoc/ja-jp/000126658〔2021/4/28 確認〕
※ 140 三菱電機株式会社：TCP/IP スタックにおける複数の脆弱性（Ripple20）の影響について https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2020-010.pdf〔2021/4/28 確認〕
※ 141 株式会社リコー：「Ripple20」によるリコー製品への影響について https://jp.ricoh.com/info/notice/2020/0731_1〔2021/4/28 確認〕
※ 142 JSOF Ltd.：CVE-2020-11896 RCE CVE-2020-11898 Info Leak https://www.jsof-tech.com/jsof_ripple20_technical_whitepaper_june20/〔2021/4/28 確認〕
※ 143 JSOF Ltd.：CVE-2020-11901 https://www.jsof-tech.com/ripple20_cve-2020-11901-august20/〔2021/4/28 確認〕
※ 144 JVN：JVNVU#94829658 Treck 社製 TCP/IP スタックに複数の脆弱性 https://jvn.jp/vu/JVNVU94829658/index.html〔2021/4/28 確認〕
※ 145 ICS-CERT：ICS Advisory (ICSA-20-353-01) Treck TCP/IP Stack (Update A) https://us-cert.cisa.gov/ics/advisories/icsa-20-353-01〔2021/4/28 確認〕
※ 146 三菱電機株式会社：当社製品の TCP プロトコルスタックにおける悪意のあるプログラムが実行される脆弱性 https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2020-022.pdf〔2021/4/28 確認〕
※ 147 Forescout Technologies Inc.：AMNESIA:33 https://www.forescout.com/research-labs/amnesia33/〔2021/4/28 確認〕
※ 148 ICS-CERT：ICS Advisory (ICSA-20-343-01) Multiple Embedded TCP/IP Stacks https://us-cert.cisa.gov/ics/advisories/icsa-20-343-01〔2021/4/28 確認〕
※ 149 Palo Alto Networks, Inc.：Risks in IoT Supply Chain https://unit42.paloaltonetworks.com/iot-supply-chain/〔2021/4/28 確認〕
パロアルトネットワークス株式会社：IoT サプライチェーンのリスク https://unit42.paloaltonetworks.jp/iot-supply-chain/〔2021/4/28 確認〕
※ 150 F-Secure Corporation：THE FAKE CISCO - Hunting for backdoors in Counterfeit Cisco devices https://labs.f-secure.com/assets/BlogFiles/2020-07-the-fake-cisco.pdf〔2021/4/28 確認〕
※ 151 ForAllSecure, Inc.：Uncovering OpenWRT Remote Code Execution (CVE-2020-7982) https://forallsecure.com/blog/uncovering-openwrt-remote-code-execution-cve-2020-7982〔2021/4/28 確認〕
※ 152 https://notice.go.jp/〔2021/4/28 確認〕
※ 153 NOTICE サポートセンター：実施状況 https://notice.go.jp/status〔2021/4/28 確認〕
※ 154 警察庁：インターネット観測結果等（令和2年） https://www.npa.go.jp/cyberpolice/detect/pdf/20210316.pdf〔2021/4/28 確認〕
※ 155 感染した IoT 機器上で不正なプログラムを実行し、ボットネットを構成するとともに、IoT 機器を狙った他のウイルスが感染に悪用する通信ポートの遮断等を実施して、結果的に機器を他のウイルス感染から防御するウイルス。Hajime の詳細に関しては、「情報セキュリティ白書 2018」の「3.1.1 (1) IoT 機器の Mirai 等の感染に対抗する『Hajime』」（p.162）を参照。
※ 156 Qihoo 360 Technology Co., Ltd.：An Update for a Very Active DDos Botnet: Moobot https://blog.netlab.360.com/ddos-botnet-moobot-en/〔2021/4/28 確認〕
※ 157 総務省：サイバー攻撃に悪用されるおそれのある IoT 機器の調査（NOTICE）の取組強化 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00079.html〔2021/4/28 確認〕
※ 158 一般社団法人 ICT-ISAC：脆弱な状態にある重要 IoT 機器の調査及び注意喚起について https://www.ict-isac.jp/news/news20200728.html〔2021/4/28 確認〕
※ 159 「IoT セキュリティ法」の詳細に関しては、「情報セキュリティ白書 2020」の「3.2.3 (2) (b) カリフォルニア州における法規制の施行開始」（p.180）を参照。
※ 160 Fox Rothschild LLP：The Internet of (Secure) Things: California Now Regulates Security of IoT Devices https://www.foxrothschild.com/publications/the-internet-of-secure-things-california-now-regulates-security-of-iot-devices/〔2021/4/28 確認〕
※ 161 Oregon State Legislature：Enrolled House Bill 2395 https://olis.leg.state.or.us/liz/2019R1/Downloads/MeasureDocument/HB2395/Enrolled〔2021/4/28 確認〕
※ 162 Illinois General Assembly：Bill Status of HB3391 101st General Assembly https://www.ilga.gov/legislation/BillStatus.asp?DocNum=3391&GAID=15&DocTypeID=HB&LegId=119982&SessionID=108&GA=101〔2021/4/28 確認〕
※ 163 Maryland General Assembly：Legislation - HB1276 https://mgaleg.maryland.gov/mgawebsite/legislation/details/hb1276?ys=2019rs〔2021/4/28 確認〕
※ 164 General Court of the Commonwealth of Massachusetts：Bill S.2056 191st(2019-2020) https://malegislature.gov/Bills/

191/S2056〔2021/4/28 確認〕
※ 165 Washington State Legislature：HOUSE BILL 2365 https://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/House%20Bills/2365.pdf〔2021/4/28 確認〕
※ 166 JSSEC：『IoT セキュリティチェックシート入門』を公開しました。https://www.jssec.org/report/20200901.html〔2021/4/28 確認〕
※ 167 CCDS：CCDS スマートホーム分野サービス向けサーティフィケーションプログラム実施に向けて https://www.ccds.or.jp/public/document/other/[CCDS]PressRelease_ スマートホーム分野サービス向けサーティフィケーションプログラム実施 .pdf〔2021/4/28 確認〕
※ 168 経済産業省：機器のサイバーセキュリティ確保のためのセキュリティ検証の手引きを取りまとめました https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html〔2021/4/28 確認〕
※ 169 総務省：「IoT・5G セキュリティ総合対策 プログレスレポート 2020」の公表 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00068.html〔2021/4/28 確認〕
※ 170 総務省：「IoT・5G セキュリティ総合対策 2020（案）」に対する意見募集の結果及び「IoT・5G セキュリティ総合対策 2020」の公表 https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00126.html〔2021/4/28 確認〕
※ 171 総務省：「電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第２版）」（案）についての意見募集の結果及びガイドラインの公表 https://www.soumu.go.jp/menu_news/s-news/01kiban05_02000209.html〔2021/4/28 確認〕
※ 172 IPA：脆弱性対処に向けた製品開発者向けガイド https://www.ipa.go.jp/security/vuln/report/notice/guideforvendor.html〔2021/4/28 確認〕
※ 173 https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTCommonReq_2021_v1.0_jpn.pdf〔2021/4/28 確認〕
※ 174 https://www.ccds.or.jp/public/document/other/CCDS_IoT 機器セキュリティ実装ガイドライン（ソフトウェア更新機能）_v1.0.pdf〔2021/4/28 確認〕
※ 175 JSSEC:『IoT セキュリティチェックシート』および、『IoT 利用アンケート』 https://www.jssec.org/iot〔2021/4/28 確認〕
※ 176 NIST：NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers https://csrc.nist.gov/publications/detail/nistir/8259/final〔2021/4/28 確認〕
※ 177 NIST：NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline https://csrc.nist.gov/publications/detail/nistir/8259a/final〔2021/4/28 確認〕
※ 178 NIST：Draft NIST Special Publication 800-213: IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements https://csrc.nist.gov/publications/detail/sp/800-213/draft〔2021/4/28 確認〕
※ 179 NIST：Draft NISTIR 8259B: IoT Non-Technical Supporting Capability Core Baseline https://csrc.nist.gov/publications/detail/nistir/8259b/draft〔2021/4/28 確認〕
※ 180 NIST：Draft NISTIR 8259C: Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline https://csrc.nist.gov/publications/detail/nistir/8259c/draft〔2021/4/28 確認〕
※ 181 NIST：Draft NISTIR 8259D: Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government https://csrc.nist.gov/publications/detail/nistir/8259d/draft〔2021/4/28 確認〕
※ 182 ENISA：Guidelines for Securing the Internet of Things https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things〔2021/4/28 確認〕
※ 183 ENISA：Cybersecurity Stocktaking in the CAM https://www.enisa.europa.eu/publications/cybersecurity-stocktaking-in-the-cam〔2021/4/28 確認〕
※ 184 ETSI：ETSI TS 303 645 v2.1.1 (2020-06): CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf〔2021/4/28 確認〕
※ 185 https://japan-telework.or.jp/tw_about/〔2021/6/8 確認〕
※ 186 従来は「テレコミューティング（telecommuting）」（遠隔通勤）という用語が用いられた。1973 年、米物理学者で当時、米航空宇宙局（NASA）の複雑な通信システム作業を自宅から行っていた Jack Nilles 氏が自身の勤務体制を「テレコミューティング（telecommuting）」と表現したのが始まりである。
※ 187 日本テレワーク学会：NECにおけるテレコミューティングへの取り組み http://www.telework-gakkai.jp/archive/IFF/newsletter-j/V3N10/nec.html〔2021/5/25 確認〕
※ 188 https://japan-telework.or.jp/tw_about/tw_effect/〔2021/6/8 確認〕
※ 189 総務省：令和元年通信利用動向調査の結果（概要） https://www.soumu.go.jp/main_content/000689455.pdf〔2021/5/25 確認〕
※ 190 https://corona.go.jp/news/pdf/kinkyujitai_sengen_0407.pdf〔2021/5/25 確認〕
※ 191 https://corona.go.jp/news/pdf/kinkyujitaisengen_gaiyou0525.pdf〔2021/5/25 確認〕
※ 192 内閣官房：新型コロナウイルス感染症緊急事態宣言・まん延防止等重点措置 https://corona.go.jp/emergency/〔2021/5/25 確認〕
※ 193 https://www.ipa.go.jp/security/fy2020/reports/scrm/index-final.html〔2021/5/25 確認〕
※ 194 日本経済新聞：パソコン供給追いつかず 在宅勤務で需要増 中国に生産偏り、部品調達遅れ https://www.nikkei.com/article/DGKKZO57950540Q0A410C2TJC000/〔2021/5/25 確認〕
日経クロステック：5700 人テレワークで VPN のリソース不足に直面、東京ガスの講じた混雑解消策 https://xtech.nikkei.com/atcl/nxt/column/18/01298/060200008/〔2021/5/25 確認〕
ITmedia NEWS：社内システム使えず「テレワークできない」→ 4000 人が VPN 同時接続 シオノギ製薬グループの“激動の５日間” https://www.itmedia.co.jp/news/articles/2009/23/news043.html〔2021/5/25 確認〕
株式会社アシスト：情報システム担当者の奮闘記～新型コロナで全社員がテレワークへ移行。緊急対応で学んだ危機管理～ https://www.ashisuto.co.jp/pr_blog/article/1211682_5736.html〔2021/5/25 確認〕
※ 195 厚生労働省：政府のテレワークへの取り組み https://telework.mhlw.go.jp/telework/gvm/〔2021/5/25 確認〕
※ 196 https://telework.soumu.go.jp/〔2021/5/25 確認〕
※ 197 https://telework.mhlw.go.jp/〔2021/5/25 確認〕
※ 198 https://www.soumu.go.jp/main_content/000545372.pdf〔2021/5/25 確認〕
※ 199 https://www.mhlw.go.jp/content/11911500/000690830.pdf〔2021/6/8 確認〕
※ 200 https://www.mhlw.go.jp/file/06-Seisakujouhou-11900000-Koyoukintoujidoukateikyoku/0000198641_1.pdf〔2021/5/25 確認〕
※ 201 https://www.nisc.go.jp/security-site/telework/index.html〔2021/5/25 確認〕
※ 202 総務省：テレワークにおけるセキュリティ確保 https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/〔2021/6/8 確認〕
※ 203 https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/teleworkqa_20200507.pdf〔2021/5/25 確認〕
※ 204 https://www.tw-sodan.jp/dl_pdf/16.pdf〔2021/5/25 確認〕
※ 205 https://www.mhlw.go.jp/content/000759469.pdf〔2021/6/8 確認〕
※ 206 IPA：テレワークを行う際のセキュリティ上の注意事項 https://www.ipa.go.jp/security/announce/telework.html〔2021/5/25 確認〕
※ 207 IPA：Web 会議サービスを使用する際のセキュリティ上の注意事項 https://www.ipa.go.jp/security/announce/webmeeting.html〔2021/5/25 確認〕
※ 208 https://japan-telework.or.jp/suguwakaru/guide/〔2021/5/25 確認〕
※ 209 IPA：Zoom の脆弱性対策について https://www.ipa.go.jp/security/ciadr/vul/alert20200403.html〔2021/5/25 確認〕
※ 210 NEC ネッツエスアイ株式会社：「Zoom-Bombing」と呼ばれる事象への対処方法について https://symphonict.nesic.co.jp/zoom/update-all/notification-002/〔2021/5/25 確認〕
※ 211 piyolog：警察庁内端末不正アクセスと５万件の脆弱な VPN ホストの公開についてまとめてみた https://piyolog.hatenadiary.jp/entry/2020/11/30/063636〔2021/5/25 確認〕
※ 212 JPCERT/CC：複数の SSL VPN 製品の脆弱性に関する注意喚起 https://www.jpcert.or.jp/at/2019/at190033.html〔2021/5/25 確認〕
※ 213 Pulse Security, LLC.：SA44784 - 2021-04: Out-of-Cycle Advisory: Multiple Vulnerabilities Resolved in Pulse Connect Secure 9.1R11.4 https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784〔2021/5/25 確認〕
※ 214 三菱重工業株式会社：当社グループ名古屋地区のネットワークに対する第三者からの不正アクセスに係る件 https://www.mhi.com/jp/notice/notice_200807.html〔2021/5/25 確認〕
※ 215 サービス & セキュリティ株式会社：新型コロナウイルスに便乗したフィッシング https://www.ssk-kan.co.jp/topics/?p=10717〔2021/5/25 確認〕
※ 216 ISO：ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection https://www.iso.org/committee/45306.html〔2021/6/7 確認〕
※ 217 https://www.nist.gov/〔2021/6/7 確認〕

※ 218 NIST：CYBERSECURITY FRAMEWORK　https://www.nist.gov/cyberframework〔2021/6/7 確認〕
※ 219 経済産業省：サイバーセキュリティ経営ガイドライン　https://www.meti.go.jp/policy/netsecurity/mng_guide.html〔2021/6/7 確認〕
※ 220 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（CPSF）を策定しました　https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html〔2021/6/7 確認〕
※ 221 NIST：SP 800-160 Vol. 1 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems　https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final〔2021/6/7 確認〕
※ 222 NIST：Work with NIST　https://www.nist.gov/about-nist/work-nist〔2021/6/7 確認〕
※ 223 NIST：National Cybersecurity Center of Excellence　https://www.nccoe.nist.gov〔2021/6/7 確認〕
※ 224 NIST：Validating the Integrity of Computing Devices　https://www.nccoe.nist.gov/sites/default/files/library/sp1800/nist-sp1800-34a-tpm-sca-preliminary-draft.pdf〔2021/6/7 確認〕
※ 225 MITRE 社：We operate FFRDCs　https://www.mitre.org/centers/we-operate-ffrdcs〔2021/6/7 確認〕
※ 226 MITRE 社：MITRE ATT&CK　https://attack.mitre.org/〔2021/6/7 確認〕
※ 227 NIST：Post-Quantum Cryptography　https://csrc.nist.gov/projects/post-quantum-cryptography〔2021/6/7 確認〕
※ 228 NIST：FIPS 199 Standards for Security Categorization of Federal Information and Information Systems　https://csrc.nist.gov/publications/detail/fips/199/final〔2021/6/7 確認〕
NIST：FIPS 200 Minimum Security Requirements for Federal Information and Information Systems　https://csrc.nist.gov/publications/detail/fips/200/final〔2021/6/7 確認〕
※ 229 NIST:FIPS 201-3 (Draft) Personal Identity Verification (PIV) of Federal Employees and Contractors　https://csrc.nist.gov/publications/detail/fips/201/3/draft〔2021/6/7 確認〕
※ 230 NIST CSRC:Publications　https://csrc.nist.gov/publications〔2021/6/7 確認〕
※ 231 CONGRESS.GOV：H.R.1668 - IoT Cybersecurity Improvement Act of 2020　https://www.congress.gov/bill/116th-congress/house-bill/1668〔2021/6/7 確認〕
※ 232 NIST：Rounding Up Your IoT Security Requirements：Draft NIST Guidance for Federal Agencies　https://www.nist.gov/blogs/cybersecurity-insights/rounding-your-iot-security-requirements-draft-nist-guidance-federal〔2021/6/7 確認〕
※ 233 NIST：NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)　https://www.nist.gov/itl/applied-cybersecurity/nice〔2021/6/7 確認〕
※ 234 NIST：SP 800-55 Rev. 2 (Draft) PRE-DRAFT Call for Comments: Performance Measurement Guide for Information Security　https://csrc.nist.gov/publications/detail/sp/800-55/rev-2/draft〔2021/6/7 確認〕
※ 235 Federal Register：Maintaining American Leadership in Artificial Intelligence　https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence〔2021/6/7 確認〕
※ 236 https://www.ismap.go.jp/〔2021/6/7 確認〕
※ 237 2020 年に入り、DoD は調達事業者に対して、サイバーセキュリティ成熟度モデル認証（CMMC：Cyber security Maturity Model Certificate）への対応を義務化することを検討している。これによって SP 800-171 への対応が無用になることはないが、国内の防衛産業は CMMC にも注意が必要となる。CMMC 運用の動向については「2.2.2 米国の政策」を参照されたい。
※ 238 IPA：セキュリティ関連 NIST 文書　https://www.ipa.go.jp/security/publications/nist/〔2021/6/7 確認〕
※ 239 NIST：NATIONAL VULNERABILITY DATABASE　https://nvd.nist.gov/vuln〔2021/6/7 確認〕
※ 240 https://cyber-risk.or.jp/〔2021/6/7 確認〕
発表当時の団体名は「産業横断サイバーセキュリティ人材育成検討会」である。
※ 241 NIST：Success Story: Japanese Cross-Sector Forum　https://www.nist.gov/cyberframework/success-stories/japanese-cross-sector-forum〔2021/6/7 確認〕

付録

資料･ツール

資料A　2020年のコンピュータウイルス届出状況

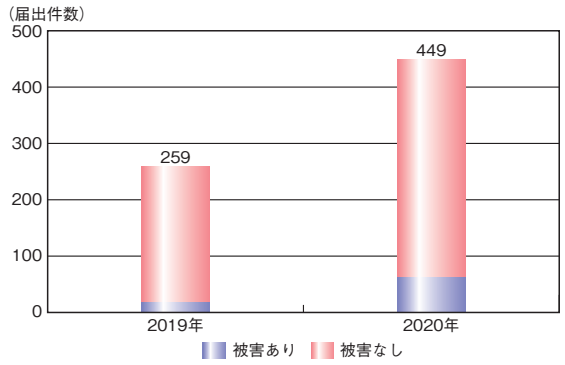
IPA が 2020 年 1 月から 12 月の期間に受け付けたコンピュータウイルス（以下、ウイルス）届出の集計結果について述べる。

なお、届出の集計方法は 2019 年から一部変更している（「A.4 集計方法の変更」参照）。

A.1　届出件数

2020 年の年間届出件数は、前年の 259 件より 190 件（73.4%）多い 449 件であった（図 A-1）。そのうち、ウイルス感染被害があった届出は 62 件であり、387 件はウイルス検知のみの届出であった。ウイルス感染被害の主なものは Emotet 感染被害 39 件、ランサムウェア感染被害 11 件であった。ばらまき型メールの攻撃によりウイルスに感染したと思われる届出も多かったため、本白書の「1.2.6 ばらまき型メールによる攻撃」等を参考に対策を行うことが望ましい。

なお、2018 年以前の届出件数については集計方法が異なるため掲載していない。2018 年以前の届出件数については、「コンピュータウイルス・不正アクセスの届出状況［2019 年（1 月～ 12 月）］」または「情報セキュリティ白書 2019」の「資料 A」を参照されたい。



■図 A-1　ウイルス届出件数推移（2019～2020 年）

A.2　届出のあったウイルス等検出数

2020 年に寄せられたウイルス等の検出数は、前年の 74 万 6,206 個より 23 万 3,233 個（31.3%）多い 97 万 9,439 個であった（図 A-2）。

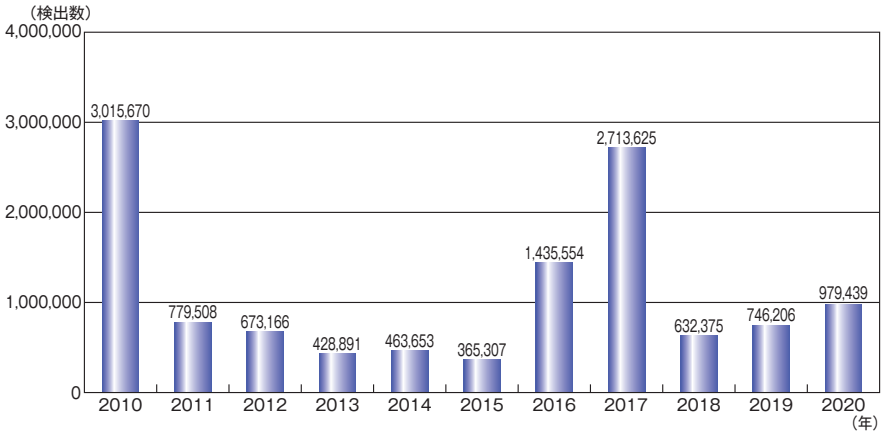
A.3　届出者の主体別届出件数

2020 年より、ウイルス届出者の主体別届出件数を「コンピュータウイルス・不正アクセスの届出状況［2020 年（1 月～ 12 月）］」と同様に掲載する。

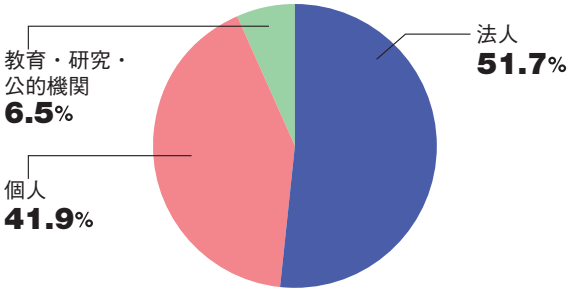
2020 年は前年と比較すると、全体の届出件数は増加した一方で、「教育・研究・行政機関」からの届出は減少した。届出者の主体別の比率では、「法人」からの届出が 232 件（51.7%）と最も多かった（表 A-1、図 A-3）。

届出者の主体	2019 年	2020 年
法人	195	232
個人	28	188
教育・研究・行政機関	36	29
合計（件）	259	449

■表 A-1　ウイルス届出者の主体別届出件数（2019～2020 年）



■図 A-2　ウイルス等検出数推移（2010～2020 年）



■図 A-3　ウイルス届出者の主体別届出件数の比率（2020 年）

A.4 集計方法の変更

近年、ウイルス（本資料では、マルウェア／不正プログラムと呼ばれる、利用者にとって期待しない動作をする、より広い意味での不正なソフトウェア全般を含む）が多様化するとともに、無数の亜種が存在することにより、発見された個々のウイルスを分類し、それを数えるといった方法での分析が不確実なものとなった。また、例えば、届出で報告される、セキュリティソフトでウイルスを検知した際に表示される名称（検知名）からは、それが何らかの不正なソフトウェアであることまでは分かるが、ウイルスの種類を判別するには不十分であることが多い。

これらの状況から、IPA では 2019 年より、ウイルスの検知名を基にした分類を取りやめる等、集計方法を表 A-2 のとおり変更した。ただし、公的機関やセキュリティベンダが注意喚起したウイルスについては、感染状況の把握や注意喚起のための情報として、個別に集計することがある。

集計内容	2018 年まで	2019 年以降
ウイルス届出件数	1 回の届出において、複数のウイルス（の検知名）が届出様式に記入されている場合、別々の届出（ウイルス種別ごとに 1 件）として集計。	複数のウイルス（の検知名）が届出様式に含まれる場合でも、届出 1 回につき 1 件として集計。
ウイルス等検出件数、及び検出ウイルスの種類	特性により「ウイルス」と「不正プログラム」を別々に集計。また、各ベンダが命名した一般的な検知名を「ウイルスの種類」とし、一部個別に集計。	ウイルス／不正プログラム等は区別せず集計。ウイルスの種類（検知名）による集計は行わない。

■表 A-2　ウイルス届出の集計方法の変更点

参照

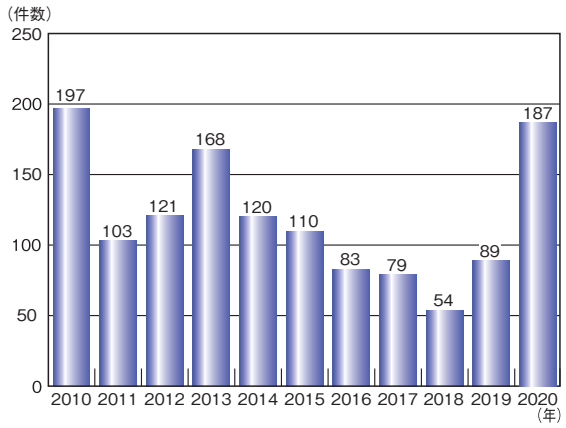
■コンピュータウイルス・不正アクセスの届出状況［2020年（1月～12月）］
https://www.ipa.go.jp/security/outline/todokede-j.html

資料B　2020年のコンピュータ不正アクセス届出状況

IPA が 2020 年 1 月から 12 月の期間に受け付けたコンピュータ不正アクセス（以下、不正アクセス）届出の集計結果について述べる。

B.1　届出件数

2020 年の年間届出件数は 187 件となり、2019 年の届出件数 89 件から 98 件（110.1%）の大きな増加となった（図 B-1）。



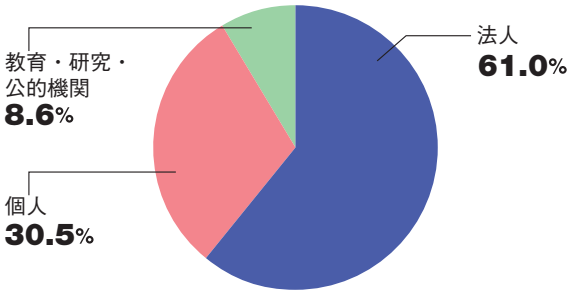
■図 B-1　不正アクセス届出件数推移（2010 年～2020 年）

B.2　届出者の主体別届出件数

2020 年は前年と比較すると、届出者別に見ても「法人」「個人」「教育・研究・公的機関」のすべてにおいて届出件数が増加した。届出者の主体別の比率では「法人」からの届出が 114 件（61.0%）と最も多く、2019 年の 49 件から 65 件（132.7%）増加した（表 B-1、図 B-2）。

届出者の主体	2018 年	2019 年	2020 年
法人	35	49	114
個人	14	30	57
教育・研究・行政機関	5	10	16
合計（件）	54	89	187

■表 B-1　不正アクセス届出者の主体別届出件数（2018～2020 年）

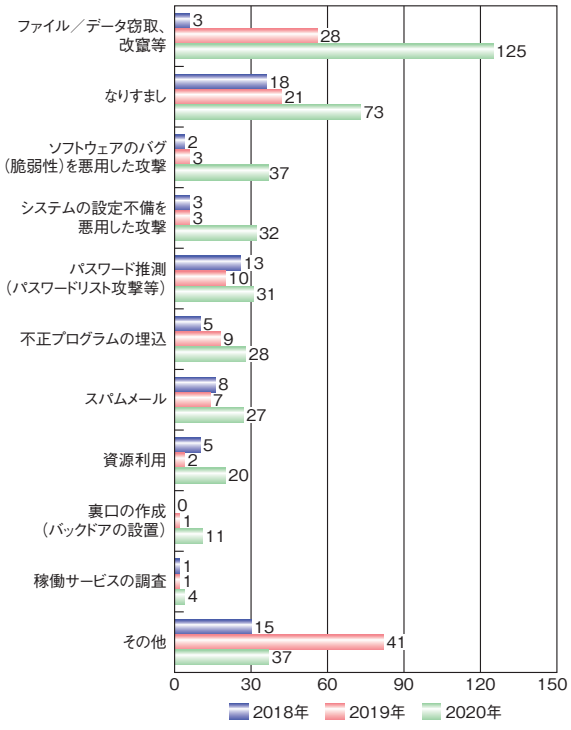


■図 B-2　不正アクセス届出者の主体別届出件数の比率（2020 年）

B.3　手口別件数

届出を攻撃行為（手口）により分類した件数を図 B-3 に示す。なお、以降の分類も含め、届出 1 件につき、複数の分類項目が該当する場合がある。その場合は該当する項目のそれぞれにカウントした。また、本分類の項目は「コンピュータウイルス・不正アクセスの届出状況［2020 年（1 月～ 12 月）］」の手口別件数の項目を細分化したものである。

2020 年の届出において最も多く見られた手口は、前年と同様に「ファイル／データ窃取、改竄等」の 125 件であり、2019 年の 28 件から 97 件（346.4%）増加した。次



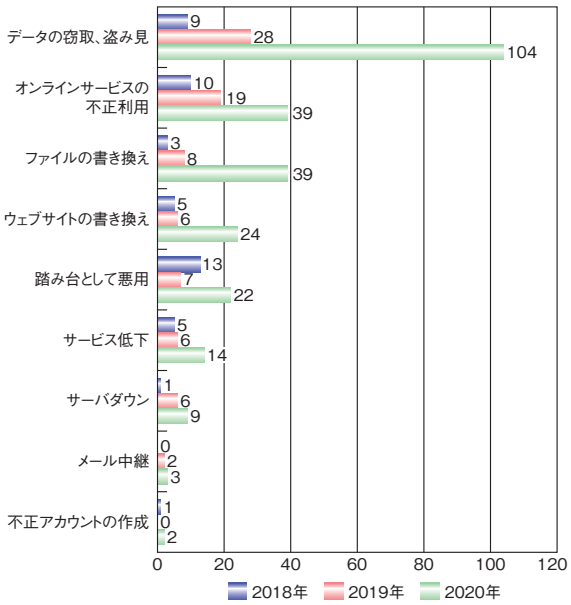
■図 B-3　不正アクセス手口別件数の推移（2018～2020 年）

いで「なりすまし」が 73 件、「ソフトウェアのバグを悪用した攻撃」が 37 件といずれも 2019 年から大幅に増加した。

B.4 被害内容別件数

届出のうち被害未遂のものを除いた、実際に被害に遭った届出について、被害内容で分類した件数を図 B-4 に示す。2020 年の届出において最も多く見られた被害は、2019 年と同様に「データの窃取、盗み見」(104 件)であり、2019 年の 28 件から 76 件(271.4%)増加した。次いで「オンラインサービスの不正利用」と「ファイルの書き換え」がそれぞれ 39 件であり、いずれも 2019 年から大幅に増加した。

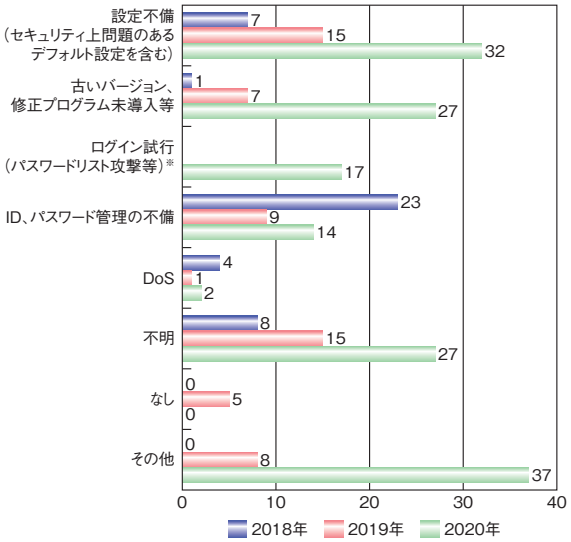
なお、具体的な被害事例については、「コンピュータウイルス・不正アクセスの届出事例[2020 年上半期(1 月～ 6 月)]」及び「コンピュータウイルス・不正アクセスの届出事例 [2020 年下半期 (7 月～ 12 月)]」(https://www.ipa.go.jp/security/outline/todokede-j.html) において紹介している。そちらも、ぜひ参考にしていただきたい。



■図 B-4　不正アクセス被害内容別件数の推移（2018～2020 年）

B.5 原因別件数

届出のうち実際に被害に遭った届出について、不正アクセスの原因となった問題点／弱点で分類した件数を図 B-5 に示す。2020 年の届出において最も多く見られた原因は、前年と同様に「設定不備(セキュリティ上問題のあるデフォルト設定を含む)」であり 32 件であった。次いで「古いバージョン、修正プログラム未導入等」が 27 件であった。また、パスワードリスト攻撃等による、会員制サイト等への不正なログインを大量に試行する攻撃被害の増加傾向が見られた。このため、2020 年より原因別の分類項目に「ログイン試行(パスワードリスト攻撃等)」を追加した。その結果、17 件が分類された。



※原因として増加の兆しが見えたため、項目を新設した。

■図 B-5　不正アクセス原因別件数の推移（2018～2020 年）

B.6 対策情報

2020 年は、会員制サイトへのパスワードリスト攻撃等のログイン試行による不正ログインが原因の会員情報窃取や不正なポイント交換の被害が多く見られた。一方で、EC サイトの改ざん等によるクレジットカード情報の窃取や、システムのデータベース等を消去または暗号化され、データの復旧のために身代金を要求されるといった被害も依然として多く見られた。

対策として、会員制サイト等への不正ログインに対しては、まず、利用者側で「他者に推測されにくい複雑なパスワードを設定する」「パスワードの使いまわしをしない」といった基本的な対策を徹底することに加えて、「二要素認証等のセキュリティ機能を積極的に活用する」等で適切なアカウント管理とリスクへの対策を実施することが推奨される。

また、EC サイト等、サーバへの不正アクセスに対しては、システム管理者側で「サーバのアクセス権の適切な設定」「ウェブアプリケーションの定期的な脆弱性対策の実施」「サーバ上の不要なサービスの停止」等により、サーバのセキュリティホールをなくしていくことや、「大量ログイン試行発生の監視・遮断機能の導入」等、不正アクセスを早急に検知し、被害を最小にするような仕組みを追加することも望ましい。

参照

■コンピュータウイルス・不正アクセスの届出状況［2020年（1月～12月）］
https://www.ipa.go.jp/security/outline/todokede-j.html

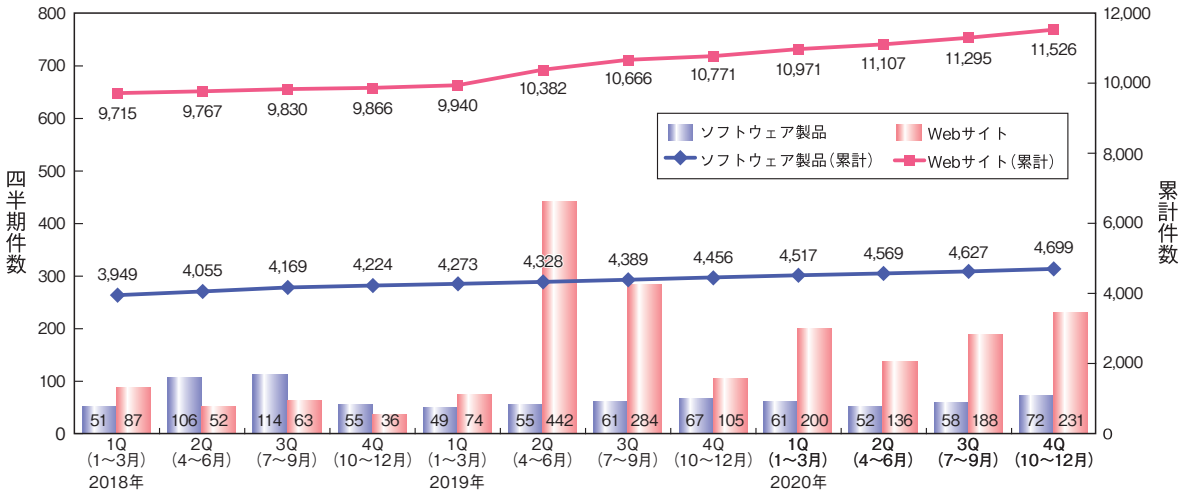
資料C　ソフトウェア等の脆弱性関連情報に関する届出状況

IPA が受け付けた脆弱性関連情報に関する届け出は、2020 年末までに 1 万 6,225 件に達した。

C.1　脆弱性の届出概況

2020 年末時点で、届出受付開始（2004 年 7 月 8 日）からの累計は、ソフトウェア製品に関するもの 4,699 件、Web サイトに関するもの 1 万 1,526 件、合計 1 万 6,225 件で、Web サイトに関する届出が全体の 71.0% を占めている（図 C-1）。

表 C-1 に示すように、届出受付開始から各四半期末時点までの就業日 1 日あたりの届出件数は、2020 年第 4 四半期末時点で 4.04 件となっている。届けられた脆弱性の種類はソフトウェア製品、Web サイトともにクロスサイト・スクリプティングの脆弱性が一番多くなっている。



■図 C-1　脆弱性関連情報の届出件数の四半期別推移

2019年1Q（1～3月）	2019年2Q（4～6月）	2019年3Q（7～9月）	2019年4Q（10～12月）	2020年1Q（1～3月）	2020年2Q（4～6月）	2020年3Q（7～9月）	2020年4Q（10～12月）
3.96	4.03	4.06	4.04	4.04	4.03	4.03	4.04

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

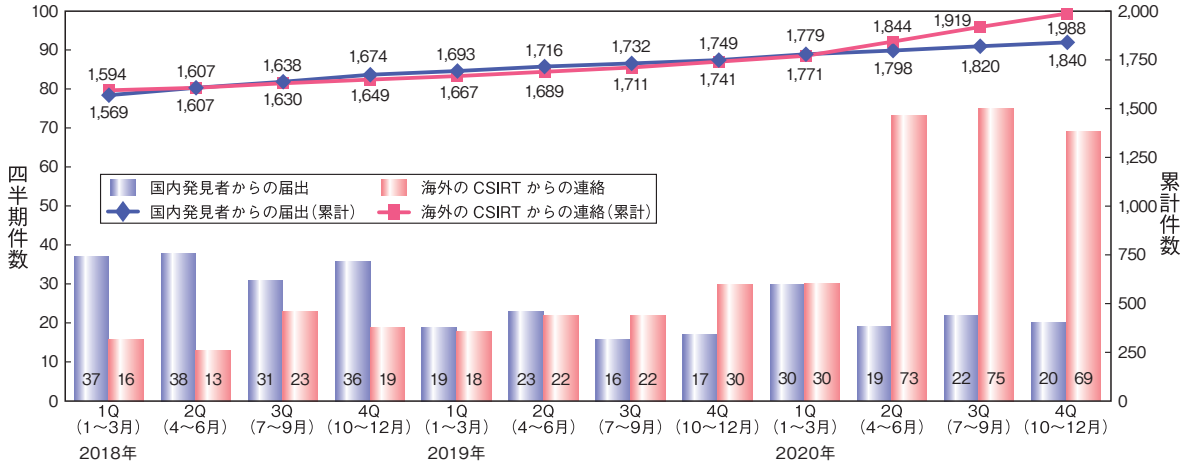
C.2　ソフトウェア製品の脆弱性の処理状況届出種別

2020 年末時点のソフトウェア製品に関する脆弱性の処理状況は、JPCERT/CC が調整を行い、製品開発者が脆弱性の修正を完了し、JVN で対策情報を公表したものは 2,167 件、製品開発者からの届出のうち JVN で公表せず製品開発者が個別対応を行ったものは 40 件、製品開発者が脆弱性ではないと判断したものは 99 件、告示で定める届出の対象に該当せず不受理としたものは 495 件で、これらの取り扱いを終了したものの合計は 2,801 件に達した（表 C-2）。

このほか、海外の CSIRT から JPCERT/CC が連絡を受けた 1,988 件を JVN で公表した。これらの公表済み件数の期別推移を（図 C-2）に示す。

分類		累計件数
修正完了	公表済み	2,167件
	個別対応	40件
脆弱性ではない		99件
不受理		495件
合計		2,801件

■表 C-2　ソフトウェア製品の脆弱性の終了件数



■図 C-2　ソフトウェア製品の脆弱性対策情報の公表件数

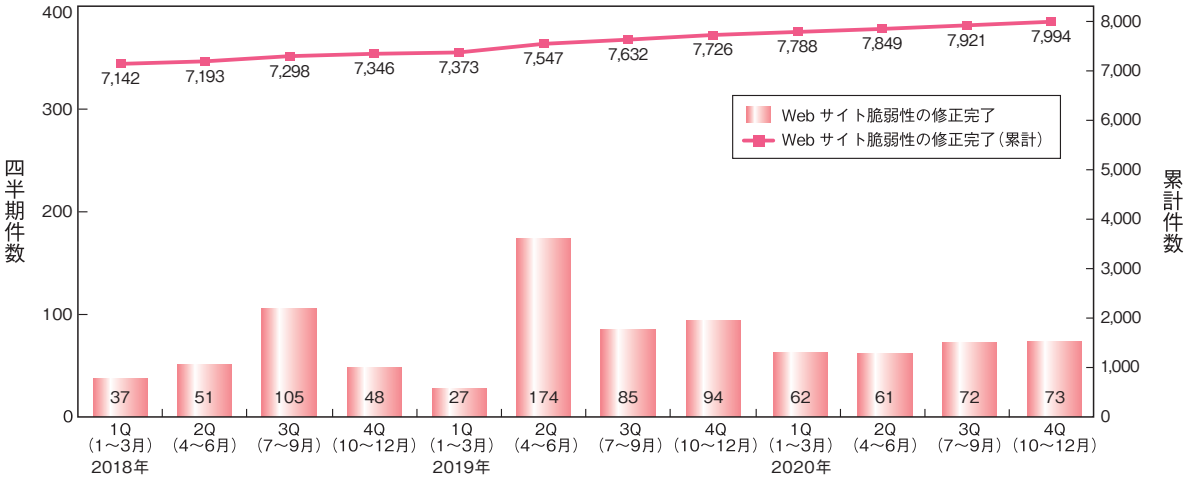
C.3 Webサイトの脆弱性の処理状況

2020 年末時点の Web サイトに関する脆弱性の処理状況は、IPA が通知を行い Web サイト運営者が修正を完了したものは 7,994 件、IPA が注意喚起等を行った後に処理を終了させたものは 1,130 件、IPA 及び Web サイト運営者が脆弱性ではないと判断したものは 687 件、Web サイト運営者と連絡が不可能なもの、または Web サイト運営者の対応により取り扱いが不能なものが 216 件、告示で定める届出の対象に該当せず不受理としたものは 276 件で、これらの取り扱いを終了したものの合計は 1 万 303 件に達した（表 C-3）。

これらのうち、修正完了件数の期別推移を（図 C-3）に示す。

分類	累計件数
修正完了	7,994件
注意喚起	1,130件
脆弱性ではない	687件
取扱不能	216件
不受理	276件
合計	10,303件

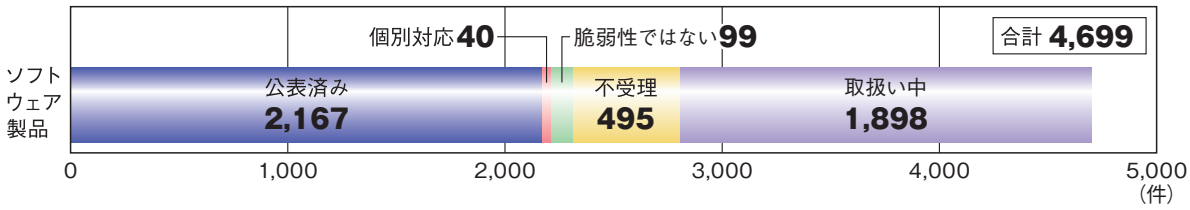
■表 C-3　Web サイトの脆弱性の終了件数



■図 C-3　Web サイトの脆弱性の修正完了件数

C.4 ソフトウェア製品の脆弱性の届出の処理状況

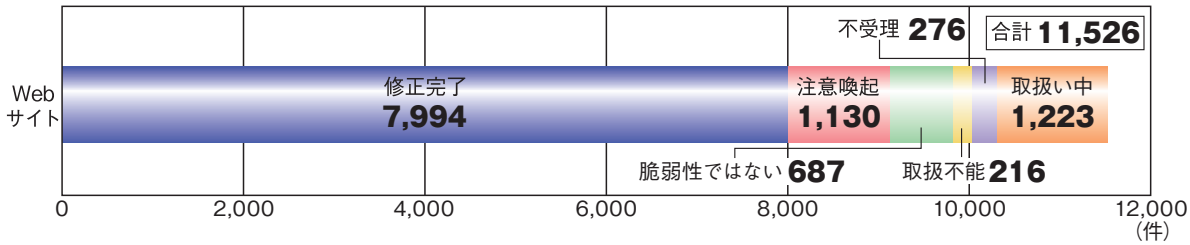
ソフトウェア製品の脆弱性関連情報の届出について処理状況を(図 C-4)に示す。



■図 C-4　ソフトウェア製品の脆弱性関連情報届出の処理状況

C.5 Webサイトの脆弱性の届出の処理状況

Web サイトの脆弱性関連情報の届出について処理状況を(図 C-5)に示す。



■図 C-5　Web サイトの脆弱性関連情報届出の処理状況

参照

■ソフトウェア等の脆弱性関連情報に関する届出状況[2020年第4四半期(10月～12月)]
https://www.ipa.go.jp/security/vuln/report/vuln2020q4.html

IPAの便利なセキュリティツール

情報セキュリティ対策ベンチマーク
https://security-shien.ipa.go.jp/diagnosis/

診断

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

概要

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

■提供される診断結果
- セキュリティレベルを示したスコア(最高点 135 点、最低点 27 点)と度数分布状況と偏差値
- 情報セキュリティリスクの指標の分布と企業規模、業種、情報資産数等が自組織と近い他組織と比較し、自組織の位置が示された散布図
- 自組織の過去診断結果との比較や従業員数別での比較を含む 4 種類のレーダーチャート
- 結果に応じた推奨される取り組み

○ベンチマークに使用する診断データは 2020 年 6 月に Ver.5.0 にアップデート

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

学習

用途・目的	脆弱性の基礎的な知識の学習
利用対象者	• アプリケーション開発者 • Web サイト管理者
特 長	脆弱性の概要や対策方法等、脆弱性に関する基礎的な知識を実習形式で体系的に学べる 3 種のツール

概要

■ AppGoat の種類
- Web アプリケーション用学習ツール(個人学習モード)、(集合学習モード)
  SQL インジェクション、クロスサイト・スクリプティング等 12 種の脆弱性を学習
- サーバ・デスクトップアプリケーション用学習ツール
  バッファオーバーフロー、ディレクトリ・トラバーサル等 7 種の脆弱性を学習

■活用方法例

○Web アプリケーション用学習ツール(個人学習モード)やサーバ・デスクトップアプリケーション用学習ツールを利用した、自宅等での個人学習

○Web アプリケーション用学習ツール(集合学習モード)を利用した、学校の講義や組織内のセミナー等における複数人での学習

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

対策

用途・目的	自組織で使用しているソフトウェア製品の脆弱性の確認と対策
利用対象者	• システム管理者 • 製品・サービスの保守を担う担当者
特 長	10 万件超の国内外のソフトウェア製品の公開された脆弱性の対策情報が掲載されたキーワードで検索が可能なデータベース

概要

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

■活用方法例

○ネット記事等に記載された CVE 番号を JVN iPedia で検索し、脆弱性の詳細を確認

○自組織で使用している製品名で検索し、脆弱性の詳細を確認

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

対策

用途・目的	PC にインストールされたソフトウェア製品が最新バージョンかどうかを確認
利用対象者	PC 利用者全般
特 長	対象製品を使用している場合、最新バージョンかを一括確認でき、判定結果とインストールされているソフトウェアのバージョン等を表示

概要

■判定対象ソフトウェア製品

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

■活用方法例

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

■動作環境・必須ソフトウェア

- Windows 8、10
- .NET Framework

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

対策

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

概要

■「重要なセキュリティ情報」発信例

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

■活用方法例

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

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

対策

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

概要

■掲載情報例

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

■活用方法例

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

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

診断

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

概要

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

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

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

知っていますか？脆弱性
https://www.ipa.go.jp/security/vuln/vuln_contents/

学習

用途・目的	Web サイトの脆弱性の理解
利用対象者	• Web サイト制作者・運営者 • 一般利用者
特 長	Web サイトにおける、よくありがちな運営上の不備と脆弱性の特徴、攻撃例、及び対策を説明

概要

ありがちなシチュエーションで発生した問題を「博士」役が対話形式で、分かりやすく解説します。

■対象の脆弱性
- SQL インジェクション
- クロスサイト・スクリプティング
- クロスサイト・リクエスト・フォージェリ
- パス名パラメータの未チェック／ディレクトリ・トラバーサル
- OS コマンド・インジェクション
- セッション管理の不備
- HTTP ヘッダ・インジェクション
- HTTPS の不適切な利用
- サービス運用妨害（DoS）
- メール不正中継

情報セキュリティ対策支援サイト
https://security-shien.ipa.go.jp/

対策

用途・目的	立場、役割に応じた情報セキュリティ対策に関する情報の収集
利用対象者	経営者、対策実践者、従業員、啓発者、教職員、学生等
特 長	情報セキュリティ対策について「知りたい」「学びたい」「続けたい」当事者に対して、IPA が提供するサービスを一元的にまとめたポータルサイト

概要

「経営者」「対策実践者」「啓発者／教職員」「一般／学生」といった立場、役割別に、情報セキュリティ対策に必要な情報（実践すべきこと、資料、ツール、動画等）を分類し、一元化しています。
特に経営者に対しては情報セキュリティ対策の重要性を理解できるよう「対策を怠ることで組織が被る不利益」「経営者が追う法的・社会的責任」といった問題を具体的に提示し、対策の実践に必要な材料を提供しています。
また、セキュリティ対策を普及啓発するセキュリティプレゼンターの登録、利用方法についても紹介しています。

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

学習 診断 対策

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

概要

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

サイバーセキュリティ経営ガイドライン実施状況の可視化ツールβ版
https://www.ipa.go.jp/security/economics/checktool/index.html

診断

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

概要

チェック項目は、サイバーセキュリティ経営ガイドラインに記載されている「経営者が情報セキュリティ対策を実施する上で責任者となる担当幹部（CISO 等）に指示すべき“重要 10 項目”」に沿って構成されており、全部で 39 項目あります。
回答方式は 5 段階の成熟度モデルで、すべての質問にセルフチェックで回答すると、“重要 10 項目”のスコアが自動生成され、レーダーチャートでも表示されます。
本ツールは「使い方ガイド」「チェックリスト」「結果」というワークシートで構成されおり、三つあるチェックリストを活用することで、グループ企業等 3 社の診断結果がレーダーチャート上にオーバーレイ表示され、視覚的な比較が容易です。
この診断結果は、経営者への自社のセキュリティ対策の実施状況の説明資料として利用でき、経営者が対策状況を定量的に把握することで、サイバーセキュリティに関する方針の策定や適切なセキュリティ投資の検討、投資家等ステークホルダとのコミュニケーション等に役立てることができます。

IPAコンクール応援隊長「まもるくん」

第16回 IPA

「ひろげよう情報モラル・セキュリティコンクール」2020 受賞作品

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

ここでは、全59,881点の応募作品の中から、受賞した作品の一部をご紹介いたします。なお、すべての受賞作品は下記のWebサイトで公開しています。

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

最優秀賞

〈標語部門〉

いいねより
いいよねと話せる
友がいい

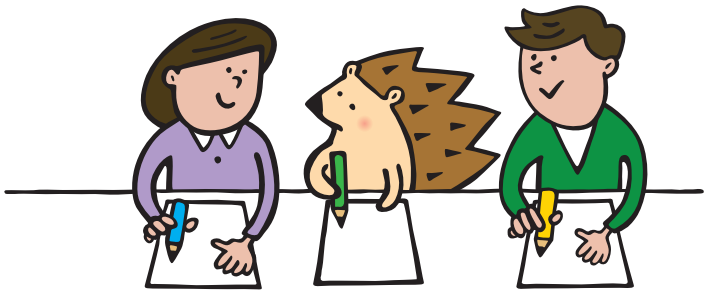
長崎県 諫早市立西諫早中学校 1年
石橋 蘭さん

〈ポスター部門〉

茨城県 茨城町立長岡小学校 2年
道川 結斗さん

〈4コマ漫画部門〉

山口県 山口県立防府商工高等学校 1年
國澤 彩葉さん



優秀賞

〈独立行政法人情報処理推進機構〉

〈標語部門〉

つながった　知らない人だ　そうだんだ

大阪府　大阪信愛学院小学校　5年
林 真央さん

その写真　盛れているけど　漏れている

沖縄県　昭和薬科大学附属中学校　2年
佐次田 ひろ志さん

基本嘘　限定･特別　あなただけ

大阪府　桃山学院高等学校　2年
茂上 晴香さん

〈ポスター部門〉

埼玉県 さとえ学園小学校 4年
竹井 優さん

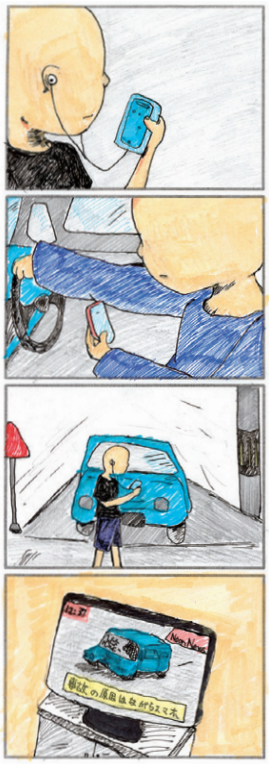
長崎県 諫早市立西諫早中学校 3年
大町 咲帆さん

鳥取県 鳥取県立鳥取湖陵高等学校 3年
岡垣 成美さん

〈4コマ漫画部門〉

山梨県 山梨学院小学校 6年
古屋 麻奈実さん

兵庫県 西宮市立鳴尾中学校 3年
濱岡 彩乃さん



島根県 島根県立大田高等学校 1年
大國 華奈さん

標語部門　優秀賞

〈警察庁〉
あぶないよ　あたしもとける　パスワード
埼玉県　さとえ学園小学校　1年
阿部 寧々さん

〈一般社団法人コンピュータソフトウェア著作権協会〉
利用する　画像の権利は　誰のもの
岐阜県　岐阜県立岐南工業高等学校　2年
奥田 琉太郎さん

〈公益社団法人著作権情報センター〉
無料だが　裏にはいるかも　犯罪者
兵庫県　雲雀丘学園小学校　6年
西井 優さん

〈特定非営利活動法人ITコーディネータ協会〉
セキュリティ　自分の意識も　更新を
福岡県　福岡市立那珂中学校　1年
山﨑 紗衣さん

〈一般社団法人情報サービス産業協会〉
指だけで　相手を守る　傷つける
東京都　お茶の水女子大学附属中学校　1年
金沢 柚奈さん

〈一般社団法人組込みシステム技術協会〉
その指止まれ　世界中に　広がる前に
鹿児島県　鹿児島市立名山小学校　4年
田中 梨央那さん

〈特定非営利活動法人日本ネットワークセキュリティ協会〉
セキュリティ　自分とスマホの　おまもりに
宮城県　大崎市立古川中学校　2年
門田 環菜さん

〈一般社団法人日本情報システム・ユーザー協会〉
その写真　一生ネットの　フリー素材
愛知県　愛知県立知立高等学校　3年
遠山 翼さん

〈一般社団法人全国地域情報産業団体連合会〉
気をつけよう　機械も体も　ウイルスに
高知県　南国市立久礼田小学校　6年
松村 朋実さん

〈一般社団法人日本教育情報化振興会〉
その言葉　表情なしで　伝わった?
大阪府　泉佐野市立日根野中学校　1年
中尾 和奏さん

〈フィッシング対策協議会　「STOP.　THINK.　CONNECT.」〉
「よし、やめよう」　自分でとめる　心のブレーキ
鹿児島県　鹿児島市立星峯中学校　3年
下之園 直輝さん

〈マカフィー株式会社〉
ネットいじめ　いつか自分に　ブーメラン
東京都　江戸川区立松江第二中学校　1年
吉井 淳平さん

〈株式会社ディー・エヌ・エー〉
いいねより　自分の「いいな」を　大切に
北海道　北海道帯広柏葉高等学校　2年
福井 桃可さん

〈株式会社ネットワールド〉
ぼくをみて　スマホよりも　だいじでしょ
鹿児島県　鹿児島市立玉江小学校　1年
池内 颯星さん

〈株式会社ラック〉
さくじょボタンじゃ　消えないよ　心の中についたきず
埼玉県　さとえ学園小学校　3年
宮本 いおりさん

〈一般社団法人北海道情報システム産業協会〉
スマホから　離れてみると　新世界
北海道　北海道帯広柏葉高等学校　2年
平山 愛梨さん

〈一般社団法人宮城県情報サービス産業協会〉
SNS　その書き込みで　SOS
宮城県　宮城県涌谷高等学校　1年
髙橋 修兵さん

〈秋田県警察本部〉
載せてから　友達からの　冷たい目
秋田県　秋田市立御所野学院中学校　1年
山中 陶子さん

〈茨城県〉
その言葉で　消える笑顔と　消えない後悔
茨城県　北茨城市立中郷中学校　3年
直井 夕芽さん

〈茨城県警察本部〉
ハイチーズ　瞳の奥で　自己紹介
茨城県　茨城県立下妻第二高等学校　2年
岡野 亜耶さん

〈茨城県情報通信ネットワークセキュリティ協議会〉
フリーWi-Fi　便利と危険が　隣り合う
茨城県　茨城県立下妻第二高等学校　2年
霜村 泰斗さん

〈公益社団法人埼玉県情報サービス産業協会〉
ウイルスは　ネット社会でも　流行ってる
埼玉県　立教新座高等学校　2年
吉見 響さん

〈東京情報大学〉
映えよりも　熱々食べよう　おいしいご飯
千葉県　白井市立七次台小学校　3年
涌井 千勢さん

〈富山県警察本部〉
これほんと?　止まって疑う　目が大事
富山県　富山県立砺波高等学校　2年
山田 潤苗さん

〈福井県警察本部〉
ネットの情報　広がる速さは　コロナ以上
福井県　北陸高等学校　3年
田野辺 優さん

〈山梨県警察本部〉
その油断　自分の未来を　傷つける
山梨県　山梨県立白根高等学校　1年
村松 結希菜さん

〈一般社団法人長野県情報サービス振興協会〉
誰かをね　クリック1つで　傷つける
長野県　南木曽町立南木曽中学校　1年
場作 快生さん

〈長野県青少年インターネット適正利用推進協議会〉
簡単に　悪口書くな　インターネット
長野県　南木曽町立南木曽中学校　1年
楯 樹希さん

〈長野県インターネットプロバイダ防犯連絡協議会〉
インターネットは　いじめの道具じゃ　ないんだよ
長野県　南木曽町立南木曽中学校　1年
橋場 好生さん

〈岐阜県警察本部〉
悪気ない　一つの投稿　大炎上
岐阜県　富田高等学校　3年
川瀬 碧未さん

〈静岡県警察本部〉
「今のなし」　通用しない　その投稿
静岡県　静岡県立浜松南高等学校　1年
加藤 風花さん

〈京都府教育委員会〉
その言葉　自分宛だと　どう思う?
京都府　舞鶴市立城北中学校　2年
岩間 千和さん

〈京都市教育委員会〉
その発言　言葉をナイフに　させるかも
京都府　京都市立東山総合支援学校高等部　3年
市川 紗千さん

〈京都府私立中学高等学校情報科研究会〉
いいね! では　評価されない　現実社会
京都府　京都産業大学附属高等学校　1年
下門 天駿さん

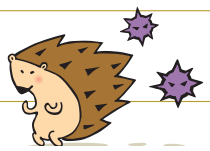
〈京都コンピュータ学院〉
SNS　怪しい人との　ディスタンス
京都府　舞鶴市立青葉中学校　3年
大田 恭平さん

〈京都情報大学院大学〉
スマホはね　使い方も　スマートに
京都府　京都府立洛西高等学校　3年
門野 泰成さん

〈大阪府警察本部〉
人の価値　フォロワーではね　決まらない
大阪府　桃山学院中学校　3年
福地 祐治さん

〈奈良県警察本部〉
一般人　炎上したら　有名人
奈良県　奈良文化高等学校　1年
中川 歩さん

〈鳥取県警察本部〉
軽い指　その判断が　重い罪
鳥取県　鳥取県立鳥取西高等学校　1年
青木 莉恋さん



〈島根県警察本部〉
考えよう　それってほんとに　書いていい?
島根県　島根県立松江商業高等学校　1年
奥原 彩恵さん

〈島根県教育委員会〉
変えてみよう　スマホの時間を　会話にね
島根県　島根県立松江商業高等学校　1年
西山 睦生さん

〈岡山県警察本部〉
「いいね」より　大切にしよう　個人情報
岡山県　岡山大学教育学部附属中学校　2年
木元 聡悟さん

〈一般社団法人システムエンジニアリング岡山〉
悪口は　心とネットに　残るもの
岡山県　金光学園高等学校　1年
安達 唯月さん

〈一般社団法人広島県情報産業協会〉
そのDM　ホントに返して　大丈夫?
広島県　熊野町立熊野東中学校　3年
中原 千裕さん

〈広島県インターネット・セキュリティ対策推進協議会〉
大丈夫?　送信先は　全世界
広島県　広島県立大門高等学校　1年
梅本 陽菜さん

〈徳島県教育委員会〉
インターネット　便利の裏には　危険がいっぱい
徳島県　阿南市立伊島小学校　6年
川西 菜々子さん

〈一般社団法人徳島県情報産業協会〉
かきません　人がいやがる　その言葉
徳島県　阿南市立羽ノ浦中学校　1年
松島 心優さん

〈公益財団法人e-とくしま推進財団〉
ネットでもリアルでも　言葉の重みは　みな同じ
徳島県　美馬市立脇町中学校　1年
森藤 優太さん

〈香川県プロバイダ等防犯連絡協議会〉
ワンタッチ　それで情報　こわれてきえる
香川県　高松市立香東中学校　2年
二川 柾也さん

〈情報通信交流館(e-とぴあ・かがわ)〉
その一言　相手にとっては　心のナイフ
香川県　高松市立香東中学校　1年
和田 響太さん

〈愛媛県情報サービス産業協議会〉
スマホなの?　あなたにとっての　友達は
愛媛県　愛媛県立松山西中等教育学校　4年
石田 紗月さん

〈高知県教育委員会〉
今もある　消したはずの　あの言葉
高知県　明徳義塾高等学校　1年
竹内 晴紀さん

〈一般社団法人高知県情報産業協会〉
その一言が　見えない社会の　落とし穴
高知県　高知県立高知南中学校　3年
田村 夏凛さん

〈福岡県教育委員会〉
消しゴムじゃ　ネットの世界は　消せないよ
福岡県　福岡市立那珂中学校　3年
梅津 凜央さん

〈長崎県警察本部〉
マスク(パスワード)して　自分の情報　感染予防
長崎県　諫早市立諫早中学校　3年
松田 朋幸さん

〈大分県情報サービス産業協会〉
SNS　気づけば僕は　フリー素材
大分県　大分県立大分上野丘高等学校　1年
佐藤 稜真さん

〈一般社団法人宮崎県情報産業協会〉
なりすまし　文字の奥には　別の顔
宮崎県　宮崎県立宮崎南高等学校　1年
田村 恵理さん

〈鹿児島県警察本部〉
クリック一つの　言葉の刃
鹿児島県　鹿児島市立天保山中学校　3年
松元 哉連さん

〈鹿児島県教育委員会〉
スマホにね　自分の人生　かけちゃダメ
鹿児島県　薩摩川内市立入来中学校　3年
花崎 智亮さん

〈鹿児島市教育委員会〉
ネットでも　傷つく言葉に　ディスタンス
鹿児島県　鹿児島市立緑丘中学校　1年
山中 知里さん

〈一般社団法人鹿児島県情報サービス産業協会〉
スマホきけん?　何がきけんか　しらないきけん
鹿児島県　鹿児島市立広木小学校　2年
竹之内 俐勇さん

〈特定非営利活動法人鹿児島インファーメーション〉
知らぬ間に　体をむしばむ　ネット依存
鹿児島県　南さつま市立田布施小学校　5年
黒瀬 光さん

ポスター部門 優秀賞

〈一般社団法人コンピュータソフトウェア協会〉

愛知県 名古屋市立工芸高等学校 3年

志賀 葵さん

〈一般社団法人 JPCERT コーディネーションセンター〉

埼玉県 埼玉県立滑川総合高等学校 3年

岸波 春樹さん

〈実教出版株式会社〉

大阪府 大阪府立三国丘高等学校 2年

寺田 佑香さん

〈株式会社カスペルスキー〉

青森県 弘前大学教育学部附属中学校 1年

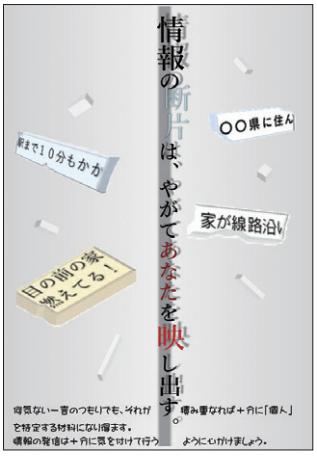
川口 真緒さん

〈株式会社ノートンライフロック〉

佐賀県 鹿島市立東部中学校 1年

中村 瞬さん

〈北海道警察〉



北海道 苫小牧市立光洋中学校 3年

飯田 明洋さん

〈岩手県警察本部〉

岩手県 盛岡市立厨川中学校 2年

種綿 一愛さん

〈茨城県メディア教育指導員連絡会〉

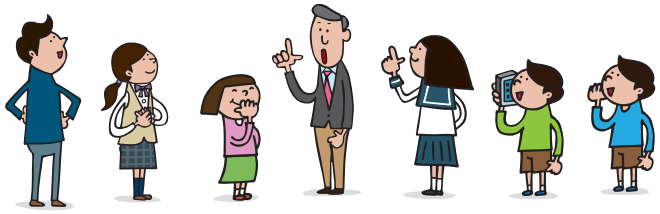
茨城県 神栖市立神栖第三中学校 2年

吉川 美桜さん

〈栃木県警察本部〉

栃木県 那須塩原市立三島中学校 3年

菊池 梨々香さん



〈群馬県警察本部〉

群馬県 群馬県立高崎女子高等学校 1年

町田 真彩さん

〈埼玉県警察本部〉

埼玉県 埼玉県立新座総合技術高等学校 2年

増川 晴菜さん

〈千葉県警察本部〉

千葉県 千葉明徳高等学校 1年

横井 琴子さん

〈警視庁生活安全部サイバー犯罪対策課〉

東京都 東京都立両国高等学校 2年

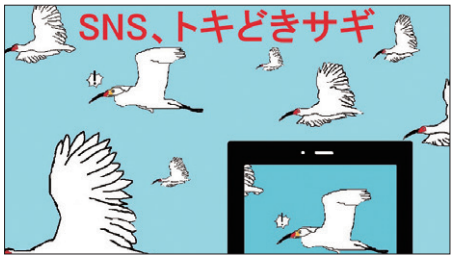
秋山 鼓太郎さん

〈神奈川県警察本部〉

神奈川県 神奈川県立金井高等学校 1年

八木 遥奈さん

〈新潟県警察本部〉



新潟県 新潟県立新潟向陽高等学校 3年

白井 優那さん

〈長野県警察本部〉

長野県 南箕輪村立南箕輪中学校 1年

堀 颯月さん

〈ネット安全・安心ぎふコンソーシアム〉

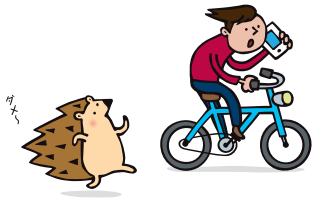
岐阜県 岐阜県立大垣養老高等学校 3年

三輪 成美さん

〈愛知県警察本部〉

愛知県 刈谷市立依佐美中学校 2年

加藤 遥さん



〈三重県警察本部〉

三重県 三重県立名張高等学校 3年

釘田 慈さん

〈滋賀県警察本部〉

滋賀県 滋賀県立河瀬高等学校 2年

山邊 ひよりさん

〈京都府警察本部〉

京都府 京都府立京都すばる高等学校 3年

宮村 愛果さん

〈公益社団法人京都府防犯協会連合会〉

京都府 京都府立大江高等学校 2年

衣川 翼さん

〈兵庫県警察本部〉

兵庫県 兵庫県立姫路工業高等学校 2年

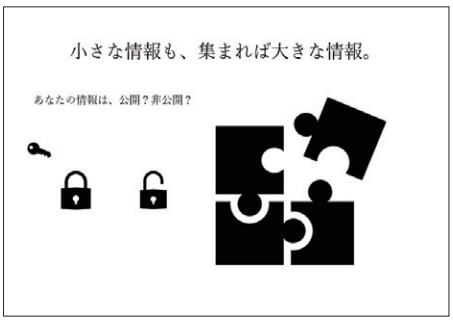
神田 希海さん

〈和歌山県警察本部〉

和歌山県 有田川町立吉備中学校 3年

小島 佑斗さん

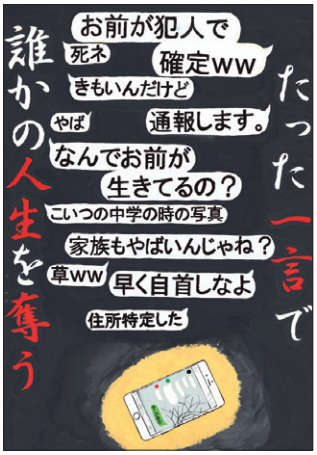
〈広島県警察本部〉



広島県 安田女子高等学校 1年

高野 優希さん

〈山口県警察本部〉



山口県 宇部フロンティア大学付属香川高等学校 3年

竹内 妃芙未さん

〈香川県教育委員会〉

香川県 香川県立高松工芸高等学校 3年

竹内 夏子さん

〈愛媛県警察本部〉

愛媛県 愛光高等学校 1年

米田 陽さん

〈高知県警察本部〉

高知県 高知市立高知商業高等学校 2年

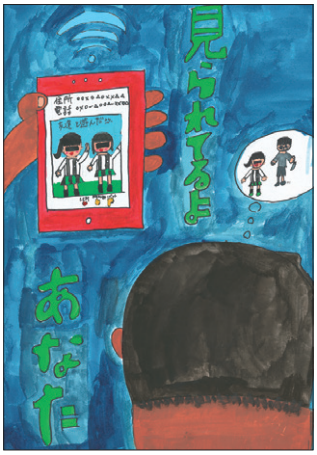
岡林 桃香さん

〈福岡県警察本部〉

福岡県 大牟田高等学校 3年

平原 秀人さん

〈佐賀県警察本部〉



佐賀県 小城市立三日月小学校 5年

松田 梨鈴さん

〈長崎県ネットワーク・セキュリティ連絡協議会〉

長崎県 諫早市立西諫早中学校 3年

馬場 優亜さん

〈熊本県警察本部〉

熊本県 宇城市立松橋中学校 2年

藤本 愛歌さん

〈宮崎県警察本部〉

宮崎県 宮崎市立佐土原中学校 1年

濵田 由菜さん

〈沖縄県〉

沖縄県 沖縄県立首里高等学校 2年

奥間 琉乃さん

〈沖縄県警察本部〉

沖縄県 沖縄県立那覇商業高等学校 3年

伊佐 かおりさん

4コマ漫画部門 優秀賞

〈ソースネクスト株式会社〉

パスワード設定はしんちょうに

千葉県 千葉県立松戸馬橋高等学校 2年

沖田 音葉さん

〈青森県警察本部〉

情報にロックを！

青森県 三沢市立第一中学校 2年

砂倉 彩花さん

〈宮城県警察本部〉

こんなはずじゃなかった

宮城県 聖和学園高等学校 3年

桑野 真緒さん

〈山形県警察本部〉

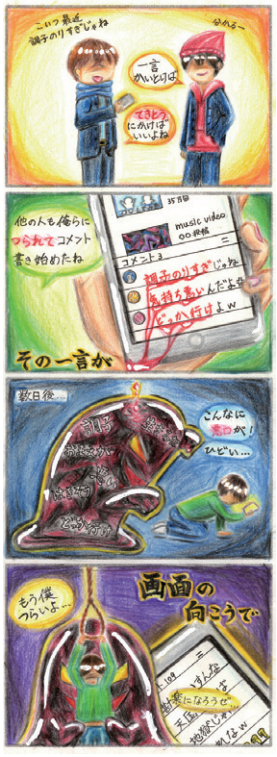
特定

山形県 山形県立酒田光陵高等学校 2年

小林 紘也さん

〈福島県警察本部〉

その一言が画面の向こうで

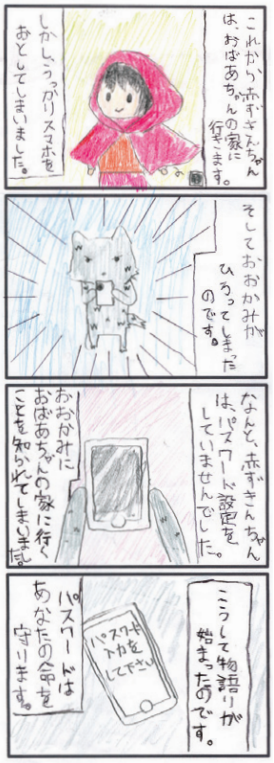


福島県 いわき市立平第一中学校 3年

吉野 遥南さん

〈茨城県教育庁学校教育部義務教育課〉

赤ずきんちゃん物語り



茨城県 青葉台中等学部 2年

小澤 稟香さん

〈茨城県教育庁学校教育部高校教育課〉

歩きスマホ

茨城県 水戸女子高等学校 1年

牛木 あかねさん

〈一般社団法人東京都情報産業協会〉

知らない間に…？

東京都 東京都立葛飾総合高等学校 3年

小泉 璃子さん

〈石川県警察本部〉

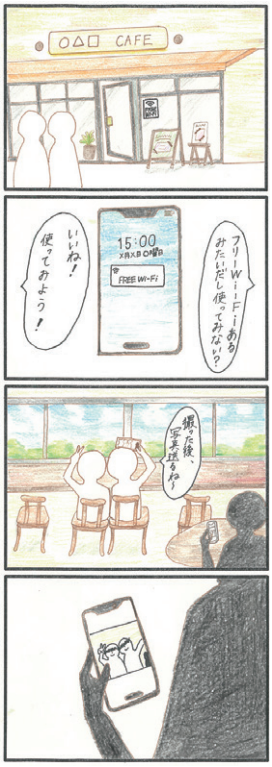
SNS 上で知り合った人には気をつけよう！

石川県 石川県立小松明峰高等学校 1年

出村 莉音さん

〈一般社団法人石川県情報システム工業会〉

フリー Wi-Fi の危険性



石川県 石川県立小松明峰高等学校 1年

宮﨑 愛巳さん

〈一般社団法人山梨県情報通信業協会〉

べから ZOO

山梨県 山梨英和高等学校 3年

松﨑 結衣さん

〈特定非営利活動法人ふじのくに情報ネットワーク機構〉

あなたは大丈夫？

静岡県 静岡県立三島南高等学校 1年

岩田 琴音さん

〈一般社団法人京都府情報産業協会〉

時間は戻らない

京都府 ノートルダム女学院高等学校 1年

木下 瑠菜さん

〈大阪私学教育情報化研究会〉

悪質なデマに気を付けよう‼

大阪府 大阪府立三島高等学校 2年

向田 真人さん

〈特定非営利活動法人奈良地域の学び推進機構〉

「あなたにはわかりますか？」

奈良県 奈良県立香芝高等学校 1年

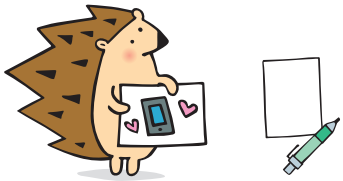
山下 愛菜さん

〈鳥取県サイバーセキュリティ対策ネットワーク〉

SNS の闇

鳥取県 倉吉市立鴨川中学校 2年

山田 麻琴さん



〈一般社団法人島根県情報産業協会〉

無断転載

島根県 島根県立大田高等学校 1年

永田 絢弓さん

〈岡山県情報セキュリティ協議会〉

パスワード

岡山県 岡山市立石井中学校 3年

藤原 柚香さん

〈徳島県警察本部〉

自分の情報が自分を傷つける

徳島県 吉野川市立鴨島第一中学校 1年

安岡 優菜さん

〈かがわ情報化推進協議会〉

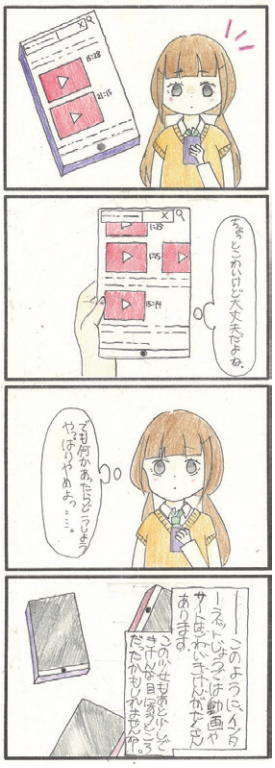
甘い誘惑にだまされないで

香川県 東かがわ市立白鳥中学校 1年

岡田 愛祝さん

〈特定非営利活動法人ＩＴサポートさが〉

インターネットのきけん



佐賀県 唐津市立西唐津小学校 6年

佐伯 心花さん

〈一般社団法人長崎県情報産業協会〉

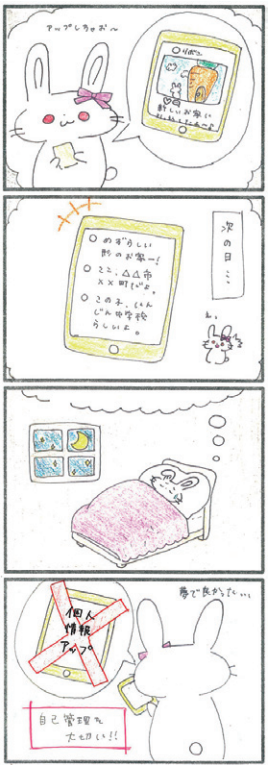
危ない！

長崎県 諫早市立西諫早中学校 1年

赤石 心奈さん

〈大分県警察本部〉

自己管理

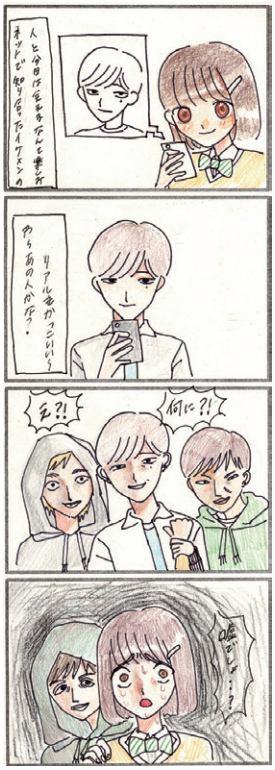


大分県 臼杵市立北中学校 2年

重野 凛さん

〈沖縄県情報通信関連産業団体連合会〉

ネットで出会う



沖縄県 沖縄県立浦添工業高等学校 1年

西村 優羽香さん

索引

J

L

M

N

P

R

S

T

U

さ

た

な

は

ま

ら

おわりに

本年の白書制作着手時に念頭にあったのは、発刊時期を昨年のように遅らせない、ということでした。昨年は4月に緊急事態宣言が発令され、ニューノーマルに適応しながら手探りでの制作となりました。

2021年版のトピックでは当然のことながらニューノーマル、 テレワークといったキーワードが多く出現し、3章で「3.3テレワークの情報セキュリティ」 として取り上げました。 海外では、セキュリティの最先進国であるはずの米国で大規模インシデントが続けて発生。 対策は未だ道半ばであることを思い知らされました。 インシデントの経緯や米国政府の対応については「2.2.2 米国の政策」や「3.4 NISTのセキュリティ関連活動」をご覧ください。

一方で、私達の生活はニューノーマルへの適応に加え、DX推進により急速にデジタル化への取り組みが求められています。 こうした大きな変化、うねりの中でどのようにセキュリティを守っていくのか、基本に立ち返り考えようという思いを込め、「進むデジタル、広がるリスク:守りの基本を見直そう」というサブタイトルとしました。

本白書は多岐にわたるサイバーセキュリティに関する国内外の事象や動向を調査・分析し、分かりやすい解説を心掛け、IPA職員だけでなく外部有識者の協力を得て作成しています。

また、白書のPDF版をIPAのWebサイトから無料でダウンロードできます。 冊子、PDF版を用途にあわせて使い分け、皆さまの対策の検討・実践の一助としていただければ幸いです。

編集子

著作・製作　独立行政法人情報処理推進機構（IPA）

編集責任　瓜生 和久　小川 隆一　山田 彩歌　白石 歩　小山 明美
佐川 陽一　石田 茂

執筆者　IPA
小川 隆一　西尾 秀一　山里 拓己　小山明美　佐藤 眞司
白石 歩　武智 洋　神田 雅透　島田 毅　松坂 志
赤木 伸悟　板垣 寛二　伊藤 彰朗　伊藤 吉史　薄羽 利光
江島将和　大島 尚　奥田 美幸　大友 更紗　甲斐 成樹
亀山 友彦　唐亀 侑久　木村 泰介　熊谷 悠平　栗原 史泰
黒岩 俊二　黒谷 欣史　小暮 淳　小幡 宗宏　佐伯 稔
酒井 亜里沙　佐川 陽一　佐藤 輝夫　柴田 直　白鳥 悦正
竹内 俊輝　竹内 智子　田村 百合子　近澤 武　辻 宏郷
土屋 昭治　土屋 正　中田 量子　橋本 徹　畑野 元
半貫 貴久　福原 聡　松島 伸彰　森 淳子　安田 進
山田 彩歌　渡邉 祥樹
株式会社日立製作所　相羽 律子
一般社団法人 JPCERT コーディネーションセンター　内田 有香子
国立情報学研究所　金子 朋子
国立研究開発法人情報通信研究機構　中尾 康二
株式会社日立システムズ　野澤 裕一
情報規格調査会 JTC 1 ／ SC 27 ／ WG 5 小委員会

協力者　IPA
桑名 利幸　松井 洋二　本多　康弘　加賀谷 伸一郎　石田 茂
前田 祐子　横山 尚人　渡辺 貴仁　日向 英俊　田口 聡
伊藤 博康　石田 淳一　板橋 博之　川﨑 宏　宮本 一弘
今村 新　西原 栄太郎
一般社団法人 JPCERT コーディネーションセンター　江田 佳領子
日本電信電話株式会社　畑田 充弘
三井物産セキュアディレクション株式会社　増田 聖一
一般社団法人日本情報システム・ユーザー協会
特定非営利活動法人日本ネットワークセキュリティ協会
経済産業省商務情報政策局サイバーセキュリティ課

・本白書は著作権法上の保護を受けています。
・本白書よりの引用、転載については、IPA Web サイトの「よくある質問と回答」（https://www.ipa.go.jp/sec/qa/index.html）に掲載されている「著作権および出版権等について」をご参照ください。なお、出典元が IPA 以外の場合、当該出典元の許諾が必要となる場合があります。
・本白書は 2020 年度の出来事を主な対象とし、執筆時点の情報に基づいて記載しています。
・電話によるご質問、及び本白書に記載されている内容以外のご質問には一切お答えできません。
あらかじめご了承ください。
・本白書に記載されている会社名、製品名、及びサービス名は、それぞれ各社の商標または登録商標です。
本文中では、™ または ® マークは明記しておりません。
・本白書に掲載しているグラフ内の数値の合計は、小数点以下の端数処理により、100% にならない場合があります。

情報セキュリティ白書 2021

進むデジタル、広がるリスク：守りの基本を見直そう

2021 年 7 月 30 日　第 1 版発行

企画・著作・制作・発行　**独立行政法人情報処理推進機構（IPA）**
〒 113-6591
東京都文京区本駒込2丁目 28 番8号
文京グリーンコートセンターオフィス 16 階
URL　https://www.ipa.go.jp/
電話　03-5978-7503
E-Mail spd-book@ipa.go.jp

表紙デザイン／本文 DTP・編集　**伊藤 千絵、久磨 公治、涌田 明夫、北林 俊平**

Copyright © 2021 Information-technology Promotion Agency, Japan.