情報セキュリティ白書

Information Security White Paper

2020

変わる生活、変わらぬ脅威：自らリスクを考え新しい行動を

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2020」の刊行にあたって

2019 年度は国内・海外ともに、サイバーセキュリティや個人情報保護に向けた政策の着実な実践が続きました。国内では、東京 2020 オリンピック・パラリンピック競技大会に向けた重要インフラのセキュリティ体制の整備が継続されるとともに、脆弱な IoT 機器の対策、サプライチェーンのセキュリティ強化、政府のクラウド調達をセキュアにする政策の具体化等が進みました。

その一方で、システムの脆弱性を突くサイバー攻撃、人間を騙す詐欺的手法は巧妙化を続け、被害は後を絶ちませんでした。国内では、防衛関連企業への不正アクセスによる情報漏えい、個人を狙ったスマホ決済の不正利用、フィッシングによる金銭被害等が注目されました。クラウド利用においては、システム障害による企業・自治体のサービス停止事案が続きました。また、廃棄処分されるはずの自治体の HDD がサプライチェーンから不正に流出し、IPA が公開した「情報セキュリティ 10 大脅威 2020」では、「内部不正」が 2 位となりました。海外においては、米国で 1 億人以上の顧客情報がクラウドから漏えいする大規模事案がおこり、欧州では個人情報の不適切な管理が GDPR 違反であるとして、航空会社等に巨額の制裁金が課されました。

こうした中で、私達の生活は新型コロナウイルス感染症拡大の影響を大きく受けることとなりました。2020 年 1 ～ 3 月には、主に海外で新型コロナウイルス感染症対策をかたる詐欺メールや偽情報、医療機関を狙った攻撃等が急増し、米国国家安全保障省等による注意喚起が繰り返されました。更に 3 月以降、海外・国内ともテレワークの実施等、IT を活用した働き方が求められる状況となりました。

もちろんテレワークは以前から行われており、多くの組織では専用端末支給等の対策をとってきました。しかし今回、制度やシステムの準備が十分ではないが対応せざるを得ない、あるいは事業継続のためにセキュリティ対策は後回しにせざるを得ない、等の判断も組織によってはあったことでしょう。今後更に、サテライトオフィスでの業務や DX に向けたツール導入等の新しい働き方が求められるかもしれません。セキュリティの面から、私達は何をすればよいでしょうか。

「情報セキュリティ白書 2019」の巻頭では、「新しいサービスを利用するにあたり、リスクは何か、提供されるデータやシステムは信頼できるかを自分で考え、共有する」ことが大切であると申し上げました。この言葉をここでもう一度申し上げてもよいのではないか、と思います。新しいサービスの利用であれ、働き方であれ、リスクについて自ら考え、意見を共有することが対策の基本です。新しい生活や働き方を迫られるということは、逆に、リスクを見直し、新しい実践を始めるチャンスととらえても良いのではないでしょうか。

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。

2020年8月

独立行政法人情報処理推進機構（IPA）

理事長　富田達夫

目次

コラム

情報セキュリティ白書

序章

2019年度の情報セキュリティの概況

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

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

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

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

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

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

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

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

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

2019 年度の情報セキュリティの概況

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

※ 2019 年度の主な情報セキュリティインシデント・事件、及び主な情報セキュリティ政策・イベントを示している。標的型攻撃、ランサムウェア被害、DDoS 攻撃、Web 改ざん等の攻撃や被害は通年で発生している。表中の数字は本白書中に掲載している項目番号である。特に注目されたもののみを挙げた。他のインシデントや手口と対策、及び政策・イベント等については本文を参照していただきたい。

第1章
情報セキュリティインシデント・脆弱性の現状と対策

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

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

1.1 2019年度に観測されたインシデント状況

本節では、2019年度に観測された世界と日本における情報セキュリティインシデントの発生状況について概説する。

1.1.1 世界における情報セキュリティインシデント状況

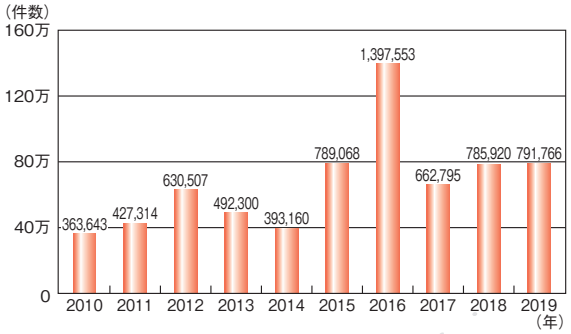
世界における情報セキュリティインシデントの発生状況について、公開されている以下の情報セキュリティ関連の報告書を参照し概説する。

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

(1) フィッシングとビジネスメール詐欺の傾向

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

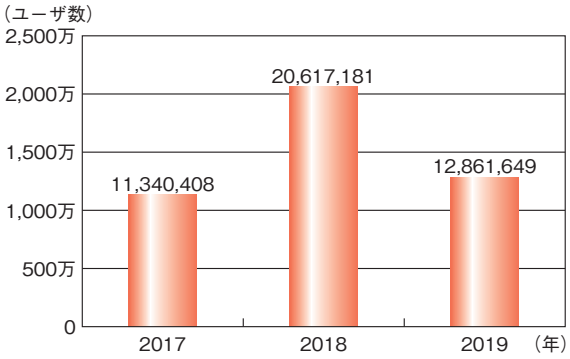
ターゲットとなる業種は、2019年1年間では「SaaS/Webmail」が33.9%、「ペイメント（支払い）」が22.4%、「金融機関」が18.2%と続いている。上位の順位は通年で変動していないが、2019年上期には合わせて6割を占めていた「SaaS/Webmail」「ペイメント（支払い）」をターゲットとしたフィッシングサイト数の割合は2019年下期には5割まで減少し、代わりに「金融機関」「eコマース」「ソーシャルメディア」をターゲットとしたフィッシングサイト数の割合が微増している。フィッシングの攻撃対象が少数の業種に集中しなくなっていることから、今後フィッシングの手口や、詐取した情報の悪用の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



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

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

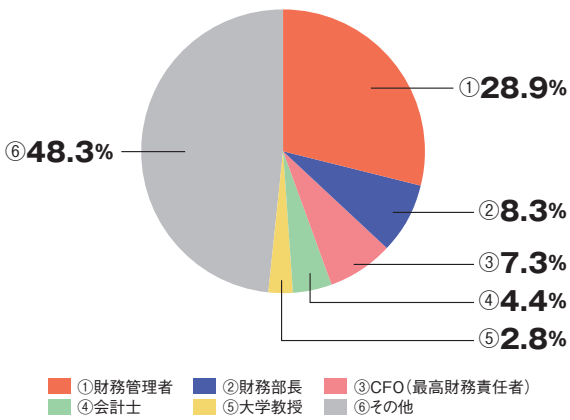
いた（フィッシングについては「1.2.6 個人をターゲットにした騙しの手口」参照）。



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

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

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



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

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

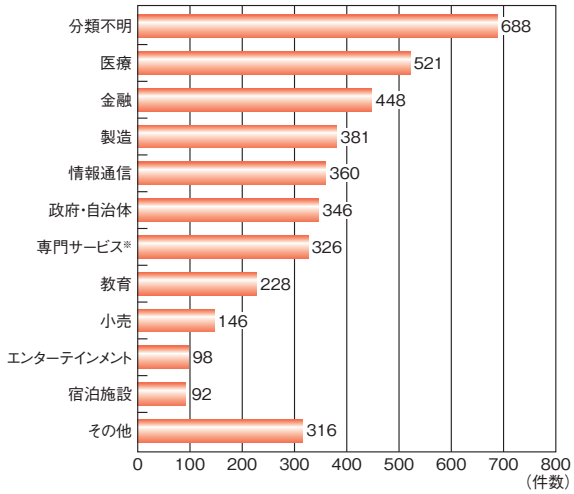
(2) 情報漏えいインシデントの状況

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

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

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

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



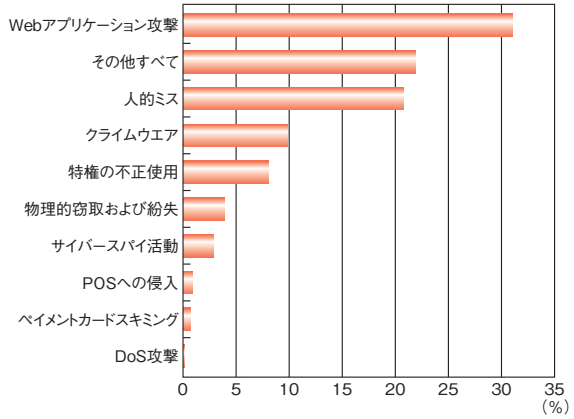
※専門サービスとは、弁護士、会計士、アーキテクト、研究所、コンサルティング会社等を指す

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

(「その他すべて」を除く)(図 1-1-5)。

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

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

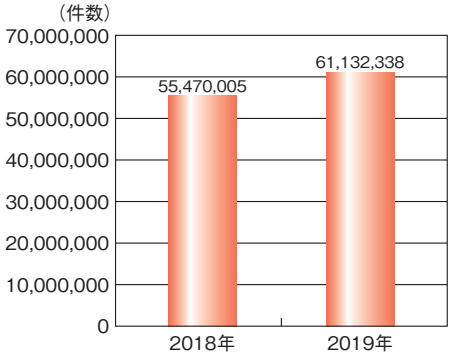


■図 1-1-5　情報漏えい事件の攻撃方法の分類
(出典)Verizon 社「2020 Data Breach Investigations Report」を基に IPA が編集

(3) ランサムウェアによる攻撃の傾向

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

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



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

(4) 攻撃手法の傾向と変化

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

この機器破壊型ウイルスの作成者は、脆弱性を放置

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

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

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

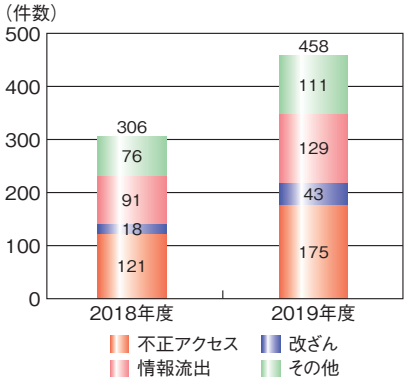
1.1.2 国内における情報セキュリティインシデント状況

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

- 三井物産セキュアディレクション株式会社（以下、MBSD 社）による集計情報[※20]
- トレンドマイクロ社：2019 年年間セキュリティラウンドアップ
- 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC：Japan Computer Emergency Response Team Coordination Center）：インシデント報告対応レポート[※21]
- フィッシング対策協議会：月次報告書[※22]

(1) 情報セキュリティインシデントの発生状況

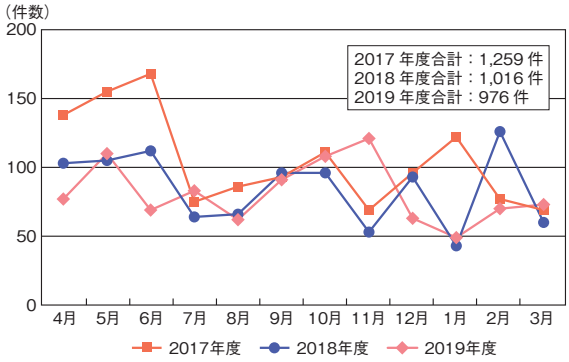
MBSD 社が集計した結果によると、2019 年度に報道された情報セキュリティインシデントの件数は 2018 年度の 306 件から 458 件に増加した（図 1-1-7）。インシデントの種類別に見ても、いずれも前年度比で 4 割以上増加した。2018 年度同様、最も件数が多いのは「不正アクセス」、最も件数が少ないのは「改ざん」だが、「改ざん」は前年度比で 2 倍以上に増加している。「不正アクセス」件数の増加は、IPA への届出件数の増加にも表れている（「付録」の「資料 B 2019 年のコンピュータ不正アクセス届出状況」参照）。報道数や届出件数が増加していることから、社会のインシデントへの意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



■図 1-1-7　情報セキュリティインシデントの種類別報道件数
（出典）MBSD 社の集計情報[※23] を基に IPA が作成

(2) Web サイト改ざんによる被害

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

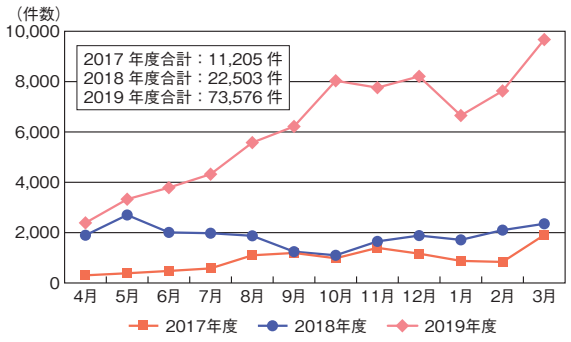


■図 1-1-8　Web サイト改ざん件数推移
（出典）JPCERT/CC「インシデント報告対応レポート」（2017 年 4 月 1 日～2020 年 3 月 31 日）を基に IPA が作成

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

(3) フィッシングによる被害

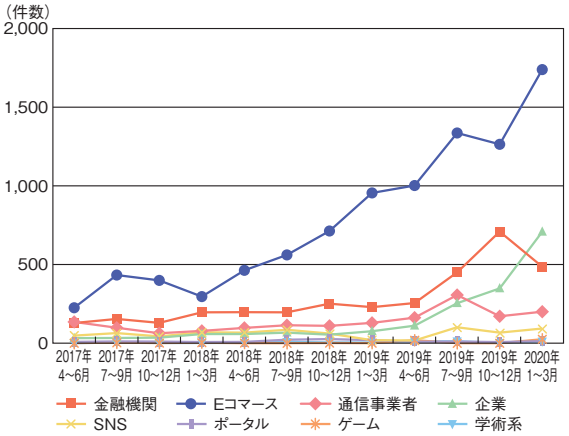
個人情報やクレジットカード番号、キャッシュレス決済等の各種サービスの認証情報等の詐取を目的としたフィッシングが継続している。ここ数年のフィッシング対策協議会への報告件数は、2017 年度が 1 万 1,205 件、2018 年度が 2 万 2,503 件と倍増し、2019 年度には前年度の 3 倍超の 7 万 3,576 件と急増している（図 1-1-9）。



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

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

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



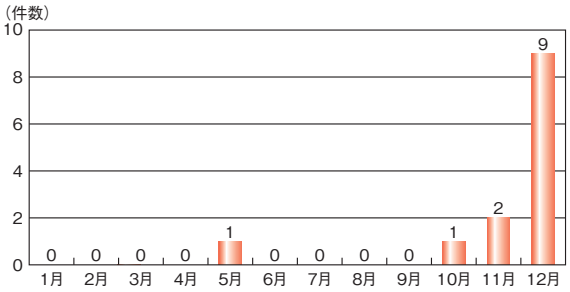
■図 1-1-10　フィッシングサイトのブランド別件数推移
（出典）JPCERT/CC「インシデント報告対応レポート」（2017 年 4 月 1 日～ 2020 年 3 月 31 日）を基に IPA が作成

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

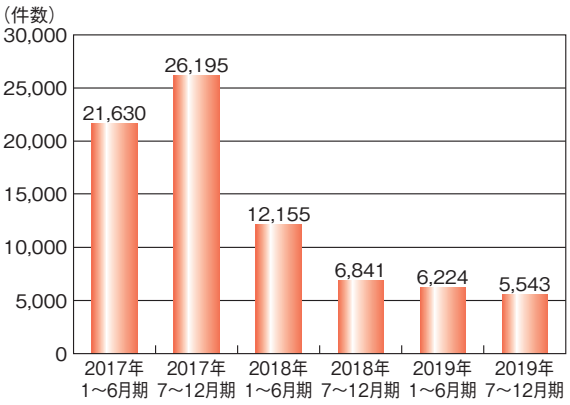
(4) 注目された新たな脅威

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

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

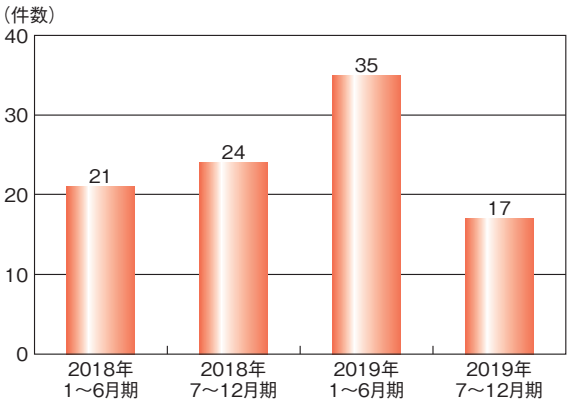


■図 1-1-11　2019 年公表の主な EMOTET 感染被害の件数推移
(出典)トレンドマイクロ社「2019 年年間セキュリティラウンドアップ」を基に IPA が編集



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

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



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

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

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

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

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

1.2 情報セキュリティインシデント別の手口と対策

本節では、インシデント別の発生状況と、具体的な事例について述べる。また、2019 年度に確認されたサイバー攻撃の手口を中心に解説する。

1.2.1 標的型攻撃

標的型攻撃とは、ある特定の組織・企業や業界等を狙って行われるサイバー攻撃の一種である。ウイルスメールやフィッシングメールを不特定多数の相手に無差別に送り付ける攻撃とは異なり、標的型攻撃は、特定の組織・企業や業界が持つ機密情報の窃取やシステム・設備の破壊・停止といった、明確な目的をもって行われる。また、標的型攻撃は長期間継続して行われることが多く、攻撃者が標的とする組織の内部に数年間潜入して活動していたと考えられる事例も日本国内で確認されている※35。

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

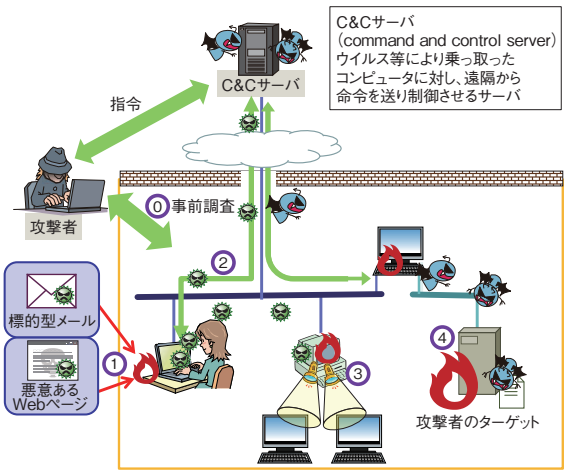
「事前調査段階」では、標的とする組織や業界の情報を収集する。公開されている情報を収集するだけでなく、標的とする組織と他の組織とのメールによるやり取りの盗聴等により必要な情報を収集することもある。

次の「初期潜入段階」では、「事前調査段階」で得られた情報を基に、標的とする組織の端末へのウイルス感染を試みる。多くの場合、標的とする組織の人間に対し、ウイルスを添付したメール（標的型攻撃メール）を送り付ける手法が用いられる。標的型攻撃メールでは、標的とする組織や業界に合わせてメール文面が作成されることが多い。また、ウイルスをパスワードが設定された圧縮ファイルに格納して添付することで、セキュリティソフトの検知を回避する工夫がなされることもある。

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

次の「システム調査段階」では、「攻撃基盤構築段階」で感染させた RAT を使用して、組織内ネットワークの攻撃に必要なウイルスやツールを送り込む。これらのウイルスやツールを用いて、組織内ネットワークの調査、管理者権限の奪取、目的とする情報の探索等を行う。

「攻撃最終目的の遂行段階」では、攻撃者は、目的とする情報の窃取等を行う。また、海外の事例では、情報の窃取ではなく、工場や発電所といった生活インフラを支える施設の停止等を目的とした攻撃も確認されている※37。



⓪［事前調査段階］
ターゲットとなる組織を攻撃するための情報を収集する。

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

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

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

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

■図 1-2-1　標的型攻撃の流れ
（出典）IPA「標的型サイバー攻撃の脅威と対策※36」を基に編集

(1) 国内の標的型攻撃事例

本項では、2019 年度に確認された 2 件の標的型攻撃の事例を紹介する。

(a) 国内組織の中国現地法人を狙った標的型攻撃

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

レポートによると、攻撃者はまず、日本国内の経済調

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

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

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

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

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

(b) 未公開の脆弱性を悪用した標的型攻撃

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

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

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

(2) 標的型攻撃の傾向

日本国内の組織を対象とした標的型攻撃は、2011 年に複数の重工業メーカ等が標的となった事例以降、継続的に発生している。2019 年においても、防衛関連企業 4 社から事例が公表されており※43、今後も日本の組織が標的とされる状況は続くと予想され、常に対策を講じておくことが重要である。また、「1.2.1 (1) 国内の標的型攻撃事例」で紹介したように、海外の関連組織を足掛かりとして国内組織に感染を広げていく手口が確認されており、組織ごとの対策だけではなく、海外を含む企業グループ全体でセキュリティ対策を講じていく必要がある。

(3) 標的型攻撃メールの手口

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

(a) メールにおける騙しの手口

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

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

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

(b) 添付ファイルの手口

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

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

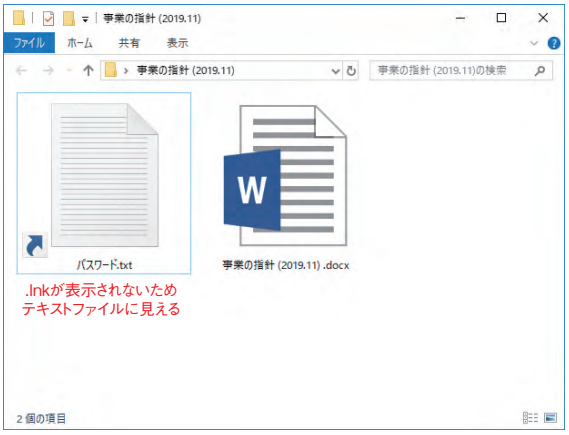


図 1-2-2　テキストファイルに見せかけるショートカットファイルの例

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

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

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

(4) 標的型攻撃への対策

標的型攻撃への対策を以下のように整理する。

(a) 利用者向けの対策

利用者向けの対策例を以下に示す。

- 不審メールに対する注意力の向上

  標的型攻撃では、標的とする企業・組織に関連する人物のメールアカウントを攻撃者が悪用してメールを送信するものや、組織や業界固有の用語等をメール本文中で用いて自然な文章を装ったもの等、受信者を騙すための巧妙な手口が使われていることが多い。一方で、送信元のメールアドレスに無料で取得できるフリーメールアドレスが使用されている等、不審な点に気付きやすいものも存在するため、利用者が不審な点がないか注意することは有効な対策の一つと言える。偽装の手口の一つとして、メールソフトが表示する送信者の名前を偽装しているメールも存在する。送信者の情報を確認する際は、表示されている送信者名ではなく、メールアドレスが正しいかどうかを確認する必要がある。身に覚えのないメールアドレスからのメールを受信した場合は、添付ファイルを開いたり、本文中のURLリンクにアクセスすることは控えるよう周知する。なお、メールの本文や署名欄に記載されている連絡先は攻撃者によって偽装されている可能性があるため、受信したメールが正規のものかどうかを確認する場合は、信頼できる公式の問い合わせ先を利用する。また、関係する組織・企業の Web サイトで「不審なメールの送信を確認している」といった注意喚起が掲載されていないか確認することも有効である。

- オンラインストレージサービスを悪用した手口の周知

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

- マクロ機能の危険性の周知

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

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

(b) 組織体制による対策

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

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

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

(c) ウイルス感染を想定した訓練と教育

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

例えば、利用者向けの取り組みでは、疑似的な標的型攻撃メールを利用者に送信して、そのメールへの対応を行う訓練（標的型攻撃メール訓練）がある。訓練を通じて、不審メールを受信した場合に着目すべき箇所の再確認や不審メールを受信した際、あるいは受信したメールの添付ファイルを開いてしまった（ウイルスに感染した）際に必要となる対処の再確認を行う。このような訓練を定期的に行うことで、利用者の対応能力を維持・向上させる。また、先に紹介したMicrosoft Officeの脆弱性の悪用等、具体的な攻撃手口を利用者に事前に周知することも対応能力の向上に有効である。

CSIRT向けの取り組みでは、他組織で発生したインシデントや自組織で起き得るインシデントを基にシナリオを作成し、インシデントが発生したことを想定して演習を行う[※47]。演習を通じて、CSIRTの対応能力の維持・向上や現在の対応体制の問題点の発見・改善を行い、実際のインシデントに備える。

(d) システムによる対策

システムによる対策例を以下に示す。

- 不審メールを確保できる仕組みの確立

  セキュリティ製品・サービスによっては、不審なメールを検知した際、メールの添付ファイルやメールそのものを削除・無害化・ブロックしてしまうものが存在する。このような場合、メールの送信元や添付されているウイルスの不正接続先といったセキュリティ対策に必要となる情報が失われてしまう可能性がある。不審なメールを検知した際は削除せず、システム管理者やCSIRTだけがアクセス可能な場所に隔離し、解析によって必要な情報が得られるように仕組みを確立することが有効である。
- 適切な修正プログラムの適用

  標的型攻撃では、OSやアプリケーションの脆弱性を悪用されるケースも存在する。脆弱性に対して適切な対応を行わずに放置した場合、その脆弱性を悪用され、攻撃者による侵入や攻撃を許してしまう危険性がある。

  そのため、IT資産管理システム等を活用し、組織内のすべてのサーバ・端末に適切に修正プログラムが適用できる仕組みを作ることが望ましい。

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

  あらかじめ、システムやポリシーで、利用者の環境で実行可能なファイルを制限（ホワイトリスト化）しておくことで、ウイルスへの感染を防止する。ホワイトリストによる制限の実施が難しい場合は、利用者の環境で実行することが望ましくないファイルの種類を制限（ブラックリスト化）する。

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

以上のように、利用者の不審メールに対する注意力の向上、インシデント発生時に適切に対応できる組織体制の構築、システムによる各種対策等、複数の観点を組み合わせ、多層的に対策を実施していくことが標的型攻撃への対策として重要である。

1.2.2 ビジネスメール詐欺（BEC）

ビジネスメール詐欺（BEC：Business Email Compromise）は、巧妙な騙しの手口を駆使した偽のメールを組織・企業に送り付け、従業員を騙して送金取り引きに関わる資金を詐取する等の金銭被害をもたらすサイバー攻撃である。偽のメールを送るための前段階として、企業の従業員や取引先のメールアカウント情報を狙うため、フィッシング攻撃や情報を窃取するウイルスが使用されることもある[※48]。

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

(1) ビジネスメール詐欺の被害状況

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

れた事例が報じられた※51。

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

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

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

(2) 2019 年度に報道された事例の概要

2019 年度に国内や海外で報道されたビジネスメール詐欺に関する事例について、概要を表 1-2-2（次ページ）に示す。多額の被害に遭った事例が多かったが、項番 8 のように保険で被害額を回復した事例もあった。

(3) IPA が情報提供を受けた事例の概要

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

(4) IPA が情報提供を受けた事例の中で特筆すべきもの

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

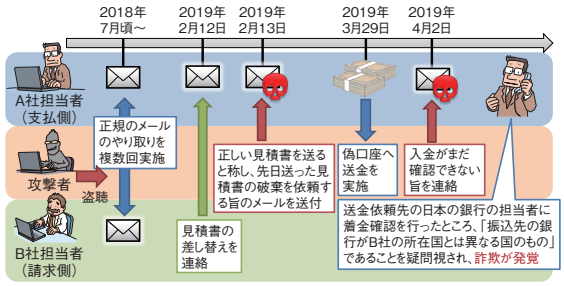
(a) 新規取引先の見積書の価格修正を装う攻撃

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

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

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

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



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

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

ていた。

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

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

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

■表1-2-2　2019年度に報道されたビジネスメール詐欺に関する事例の概要（報道または公表事例を基にIPAが作成）

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

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

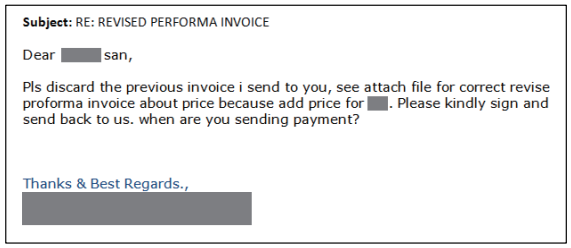
本事例は新規の取引先とのやり取りであり、過去の実績を基にした確認（これまで使っていた口座との比較等）ができず、送金前に経理部門による確認は行われていたものの、不審だとは気付けなかった。

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

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

(b) CEO を詐称する一連の攻撃

2019 年 10 月、J-CSIP の参加組織から、国内グルー



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

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

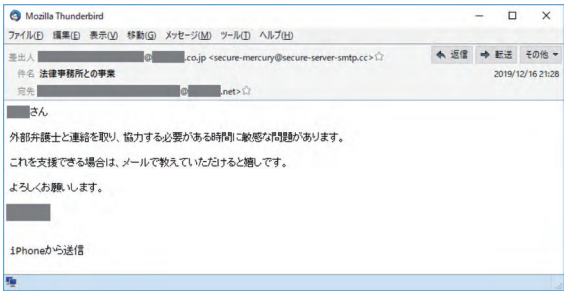
これらのメールには、メールの件名・本文や攻撃者のメールアドレス等に共通する特徴があり、同一の攻撃者による攻撃が、国内外の多数の組織へ行われたものと推測される。IPA ではこの一連の攻撃は、手口等からビジネスメール詐欺の一種であると考えている。

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

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

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

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



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

見えるメールであったとしても、侮るべきではない。

（5）ビジネスメール詐欺の騙しの手口

ビジネスメール詐欺で用いられる騙しの手口は様々であるが、ここでは J-CSIP の活動から得られた情報を基に、実際に使われた具体的な手口の一部を紹介する。攻撃者はここで紹介する手口を組み合わせて巧妙な攻撃を仕掛けてくる場合があり、注意が必要である。

（a）偽の口座へ振り込ませる手口

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

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

(b) メールの引用部分の改変の手口

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

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

(c) メールアドレスのなりすましの手口

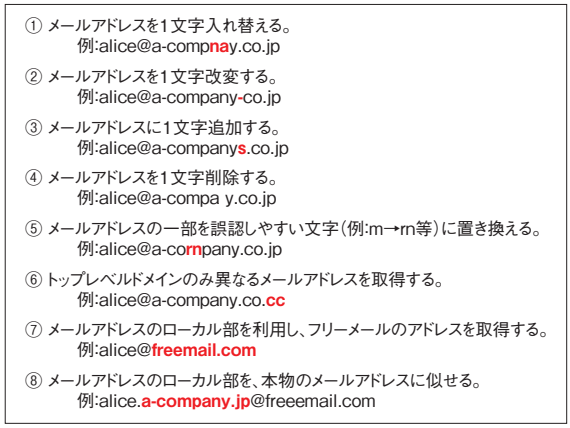
攻撃者が標的とした人物を騙すため、取引先等の本物のメールアドレスに似せた偽のメールアドレスを使い、なりすましを行う手口を確認している。

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

(d) 同報メールアドレスの改変の手口

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

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



■図 1-2-7　攻撃者によるメールアドレスのなりすましの例

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

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

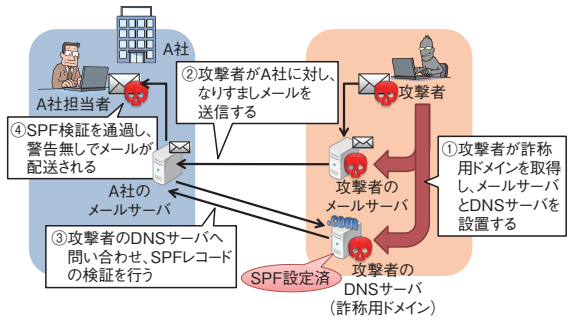
更に、別の例として A 社の関係者の同報メールアドレスは改変せずに B 社の関係者の同報メールアドレスのみを改変したケースも確認している。

(e) 詐称用ドメインの取得と悪用の手口

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

- SPF[※80]を悪用する手口

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



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

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

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

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

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

(f)送信元を偽装して攻撃者に返信させる手口

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

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

この手口を用いた例として、図1-2-10の例を確認している。

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

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

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

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

■図1-2-10　送信元を偽装して攻撃者に返信させる手口の例

(6)ビジネスメール詐欺への対策

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

(a)ビジネスメール詐欺の周知徹底と情報共有

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

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

(b)電子署名によるなりすまし防止

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

(c)送金処理のチェック体制強化

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

(d)類似ドメインへの対応

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

また、メールを返信する際は、返信先のメールアドレスが正しいアドレスであるか、落ち着いて確認することも有効である。

(e)フィッシング・ウイルス・不正アクセス対策

ビジネスメール詐欺では、攻撃者は攻撃に至る前に、フィッシング、メールの内容やメールアカウント情報を窃取するウイルスの感染等で情報を窃取し、メールサーバへの不正アクセス等の方法でメールを盗み見ている場合がある。そのため、基本的なフィッシング対策・ウイルス対策・不正アクセス対策が必要である。

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

また、メールアカウントが乗っ取られ、利用者本人が設定していない転送設定やフォルダの振り分け設定がされている等、不正利用の兆候がある場合の該当アカウントへの対処方法が Microsoft 社より公開[※82]されているため、そちらも参照していただきたい。

1.2.3 DDoS攻撃

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

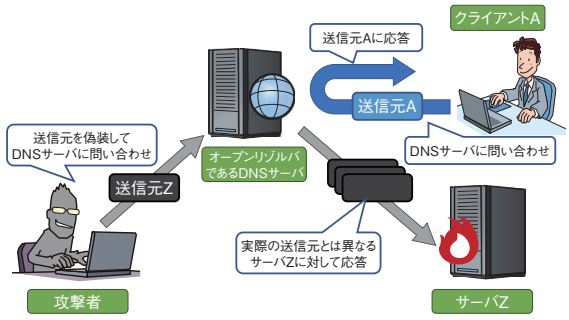
本項では、2019 年度に確認された DDoS 攻撃の事例とその対策を解説する。

(1)DDoS 攻撃の手口と事例

2019 年度における、DDoS 攻撃の主な手口と事例を紹介する。

(a) 通信プロトコルの挙動を悪用する事例

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



■図 1-2-11　リフレクター攻撃の例(DNS を悪用した場合)

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

(b) DDoS 攻撃を脅迫に用いる事例

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

一般的に、このような脅迫に応じることは推奨されない。脅迫に応じて仮想通貨を支払ったとしても、攻撃が行われない保証はなく、攻撃が成功して味を占めた攻撃者が同様の手口を繰り返したり、他の攻撃者が真似をしたりして被害が拡大する可能性もある。

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

(c) ラグビーワールドカップ期間中に確認された DDoS 攻撃

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

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

(2) DDoS 攻撃を行うボットネットの拡大

DDoS 攻撃には、「ボットネット」と呼ばれる攻撃用ネットワークが使用される場合がある。

ボットネットは、攻撃者が乗っ取った多数のコンピュータと、それらに対して遠隔で指令を送信するための C&C (Command and Control) サーバから形成されており、攻撃者が C&C サーバを介して、ボットネットに攻撃指令を送信することで、ボットネットを構成するコンピュータによって一斉に攻撃が行われる。

ボットネットを構成するコンピュータのほとんどは、サービスやソフトウェアの脆弱性を悪用されたり、ウイルスに感染させられたりした結果、制御を奪われた一般のコンピュータである。

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

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

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

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

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

(3) DDoS 攻撃への対策

DDoS 攻撃への対策では、DDoS 攻撃の被害に遭った場合の対策に加えて、管理または所有する端末が乗っ取られ、DDoS 攻撃に加担することを防ぐための対策も求められる。これらの対策について解説する。

(a) DDoS 攻撃の被害に遭った場合の対策

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

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

(b) 攻撃に加担しないための対策

自組織や個人で使用する端末、ネットワーク機器、IoT 製品が DDoS 攻撃に悪用されないように、ウイルス対策を導入する、適切な設定をする等の対策が必要である。また企業においては、自組織の端末を悪用された場合に、それを早期に検知できるように通信の監視を行うといった対策も推奨する。以下に、具体的な対処方法を挙げる。

- OS やファームウェアを最新の状態に保ち、ウイルス感染や脆弱性の悪用により制御を奪われることを防ぐ。
- パスワードが製品共通の初期設定のままの機器は、攻撃者により容易に侵入され、制御を奪われてしまう可能性がある。パスワードが製品共通の初期設定のままの機器が存在しないか確認し、存在した場合は適切なパスワードを設定する。
  パスワードが初期設定のまま外部と接続されているネットワーク機器や IoT 機器を狙って感染し、更に、その機器をとおして組織内の他の端末に対しても感染拡大を試みるウイルスも確認されているため、インターネットに直接つながっていない端末においても対策を行う。
- 組織内で稼働しているサービスを見直し、DDoS 攻撃に悪用され得るサービスが適切に運用されていることを確認する。
  具体的には、これらのサービスが稼働するサーバに関して、サーバの OS を始め、各サービスが脆弱性を含むバージョンで稼働していないことや、DDoS 攻撃に悪用され得る設定になっていないことを確認する。
  また、それらのサービスを組織内のみで利用している場合でも、意図せずインターネット上に公開していないかを確認する。
- 組織内の端末の外向けの通信を監視し、異常な通信を確認した場合は、組織内の端末が攻撃の踏み台となっている可能性がある。そのような端末に、ウイルス感染等が生じていないか調査を行う。自組織での

対処が困難な場合は警察やセキュリティベンダ等への相談を検討する。

1.2.4 ソフトウェアの脆弱性を悪用した攻撃

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

本項では、これらの脆弱性の状況と対策について解説する。

(1) Windows の脆弱性を対象とした攻撃

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

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

(a) BlueKeep の脆弱性を悪用した攻撃

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

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

(b) Windows の脆弱性を悪用した攻撃への対策

脆弱性をついた攻撃による被害を防ぐため、修正プログラムが公開されたら、利用者は速やかにアップデートを実施することが求められる。

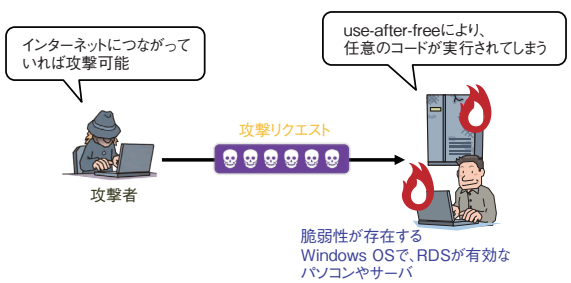
なお、2020 年 1 月 14 日には、Windows 7、Windows Server 2008 及び Windows Server 2008 R2 のサポートが終了している。一般にサポート終了後に発見された脆弱性については、修正プログラムが提供されなくなるため、サポートが終了した OS を使い続けると脆弱性を悪用した攻撃により、被害を受ける可能性が大きくなる。そのため、利用者は、ベンダのサポート情報を基に、計画的に最新の OS へ移行することが求められる。

(2) CMS の脆弱性を悪用した攻撃

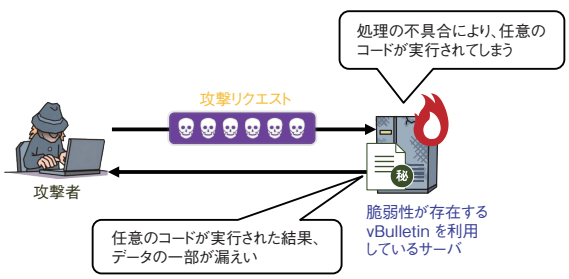
CMS は、Web サイトのコンテンツの作成・管理に使用されるソフトウェアの総称である。CMS には、「プラグイン」と呼ばれる拡張機能を導入することで、容易に機能を追加できるものもある。その手軽さから、CMS 本体だけでなく、プラグインも併せて広く利用されているため、プラグインに脆弱性が発見された場合も、攻撃者から狙われる。2019 年度も、CMS 本体やそのプラグインの脆弱性を悪用する攻撃が確認されている。

(a) CMS 本体の脆弱性を悪用した攻撃

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



■図 1-2-12　BlueKeep の脆弱性を悪用した攻撃イメージ



■図 1-2-13　vBulletin の脆弱性を悪用した攻撃イメージ

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

(b) CMSのプラグインの脆弱性を悪用した攻撃

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

(c) CMSの脆弱性を悪用した攻撃への対策

これらの事例のように、脆弱性が発見されると攻撃者にすぐに狙われ、被害が発生してしまうため、新たな脆弱性が公開された際は、迅速な対応が求められる。

このためには、事前の準備が重要である。自らが保有（利用）するシステムについて、構成管理を適切に行い、システムを構成するソフトウェア等の脆弱性に関する情報収集を日々行う必要がある。同時に、事前に対策の実施手順を整えておくことで、脆弱性の対応を遅延なく着実に実施できる。更に、公開しているWebサイトのステージング環境※98を事前に用意しておき、当該Webサイトへ対策を実施する前に、実施による不具合が発生しないか検証することが望ましい。

対策の実施手順として、以下に示す内容をあらかじめ定めておくことを推奨する。

- CMS本体やプラグイン、ミドルウェア等の脆弱性情報の収集方法
- 脆弱性が確認された場合の対応方法
- 緊急度や深刻度に応じた対応の優先度
- 他部署やベンダ等への連絡の要否基準

また、このような実施手順の準備に加え、攻撃を受けてしまった場合に実施する対応を定めておくことを推奨する。

(3) IoT機器を対象とした攻撃

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

(a) IoT機器の脆弱性を狙う新たなウイルス

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

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

(b) IoT機器を対象とした攻撃への対策

脆弱性が存在するIoT機器は、ウイルス感染によりボットとなり、攻撃に利用される可能性がある。IoTボットによる攻撃はDDoS攻撃だけでなく、情報窃取や機器破壊等、多様化している。それを踏まえて、IoT機器を安全に保つためには、以下の対策が必要となる。

- 製品開発者が行うべき対策
  - 各組織が公開しているIoT機器の開発ガイドライン等を基に、企画・設計工程等を含めた、すべての開発工程で実施すべきセキュリティ対策を明確にする（ガイドラインについては「3.2.3 (1) IoT関連セキュリティガイド等の改訂・新規発行」参照）。
  - 製品で使用する部品の調達に関し、契約等において脆弱性対処の項目を含める。
  - 製品に関する脆弱性が発見・報告された場合、速やかに修正プログラムを公開する。
  - 製品出荷後でも、修正プログラムによりアップデートが実施できるように製品に更新機能等を組み込む。
  - 安全に運用するための注意点等の情報を製品利用者に提供する。
- 製品利用者が行うべき対策
  - 製品開発者が提供する、安全に運用するための注意点や、アップデート方法等の情報を確認した上で使用する。
  - 脆弱性情報を収集する。具体的には、IPAが公

開している「JVN iPedia※100」や、IPA から送付されるセキュリティ対策情報のメールニュース、製品開発者の Web サイトで公開された情報がないか定期的に確認する。
- 製品開発者が修正プログラムを公開した場合、速やかに修正プログラムを適用する。
- 攻撃者に脆弱性を悪用されるリスクを低減するため、製品を利用するにあたって問題がなければ、インターネットから直接 IoT 機器にアクセスできないようにする。

1.2.5 ばらまき型メールによる攻撃

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

2015 年 10 月ごろより、国内で日本語のばらまき型メールが多く観測されるようになった※101。ばらまき型メールでウイルスに感染させる手口として、添付ファイルやメール本文中の URL による手法が存在する。メールの添付ファイルにはマクロ付きの Word ファイルや Excel ファイル、そして OLE 機能を悪用し、悪意のあるプログラムを埋め込んだ Word ファイル等が確認されている※102。また、ばらまき型メールの内容には、様々なバリエーションがあり、件名やメール本文が受信者と関係のないメールや、実在の組織をかたったメール、一見すると業務に関係ありそうな件名や本文のメール、過去の正規のやり取りがあったメールを引用し、「正規のメールへの返信」を装ったメール等が存在する。

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

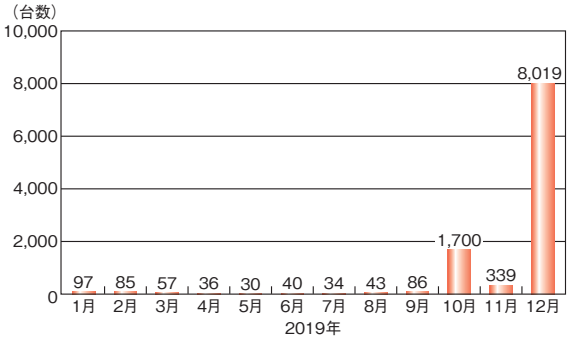
本項では、2019 年 9 月後半より日本国内に広くばらまかれた※29 Emotet のばらまき型メールを中心に、Ursnif 等別のウイルスへの感染を狙ったばらまき型メールも併せて解説する。

(1) Emotet のばらまき型メール

Emotet は感染した端末の情報窃取や他のウイルスへの感染のために使用されるウイルスである※103。Emotet の観測状況、Emotet のばらまき型メールの手口と対策等について述べる。

(a) 日本国内の観測状況

セキュリティベンダによると、Emotet は 2014 年ごろから存在が確認されているが、明確に日本を狙った攻撃は確認されていなかった※29。しかし、2019 年に入り、日本への Emotet のばらまき型メールによる攻撃が複数の国内組織・企業へ行われていることが確認された。一例として、2019 年 6 月に東京都の医療関連組織への Emotet の感染が公表された※104。そして、2019 年 9 月後半から Emotet のばらまき型メールによる攻撃が活発化し、2019 年 10 月の Emotet の検出台数は 9 月までと比較して急激に増加した。11 月は一時的に減少したとみられるが、12 月に再び急増した※105。図 1-2-14 に国内での Emotet の検出台数の推移を示す。



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

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

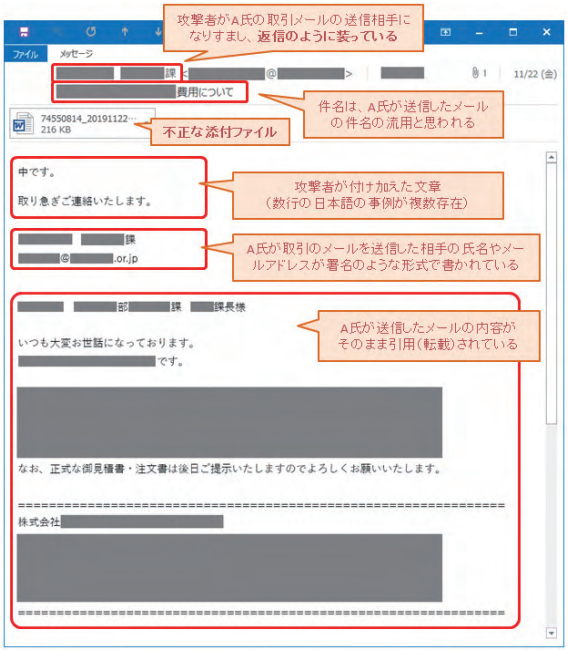
(b) Emotet のばらまき型メールの手口

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

- 本物のメールと信じ込ませる手口

  IPA では、Emotet のばらまき型メールにおいて、正規のメールへの返信を装うメールを観測している※34。このばらまき型メールでは、攻撃対象者が過去にメールのやり取りをしたことのある、実在する相手の氏名、メールアドレス、メールの内容等が流用され、その相手からの返信メールを装っている。

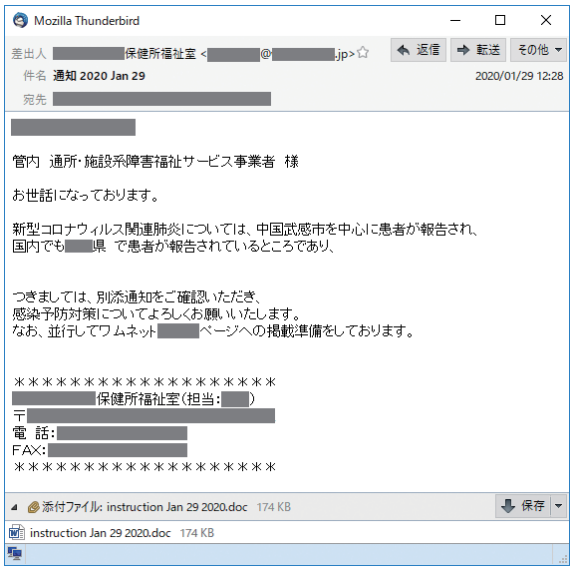
  正規のメールへの返信を装うメールの例を図 1-2-15 に示す。この例では、メールの受信者（A 氏）が以前、取引先へ送信したメールが丸ごと引用され、返信されてきたかのような内容となっている。また、件名や文面が受信者とまったく関係のない内容が記載されている事例や、引用部分の存在しない事例等も確認されている※34。正規のメールへの返信を装うばらまき型メールは 2018 年 11 月にも観測されており※107-2、この手口自体が新しいわけではない。しかし、Emotet の手口は、2018 年 11 月に観測された正規のメールへの返信を装うばらまき型メールとばらまき方が異なる。2018 年 11 月に観測された手口は攻撃者がメールアカウントへ不正アクセスし、そのメールアカウントで受信していたメールへ返信する形式であった。一方、Emotet の手口では感染端末から窃取した情報を基に、Emotet に感染した端末で構成されるメール送信用のボットネットから、別の相手に対して正規のメールへの返信を装うメールをばらまくことが確認されている※108。



■図 1-2-15　正規のメールへの返信を装う Emotet のばらまき型メールの例
（出典）IPA「『Emotet』と呼ばれるウイルスへの感染を狙うメールについて※34」

- メール受信者の興味・関心を惹く題材を悪用する手口

  IPA では、2020 年 1 月 29 日、正規のメールへの返信を装うメールとは異なる、新型コロナウイルスを題材とした Emotet のばらまき型メールを観測した※34。図 1-2-16 に新型コロナウイルスを題材とした Emotet のばらまき型メールの例を示す。



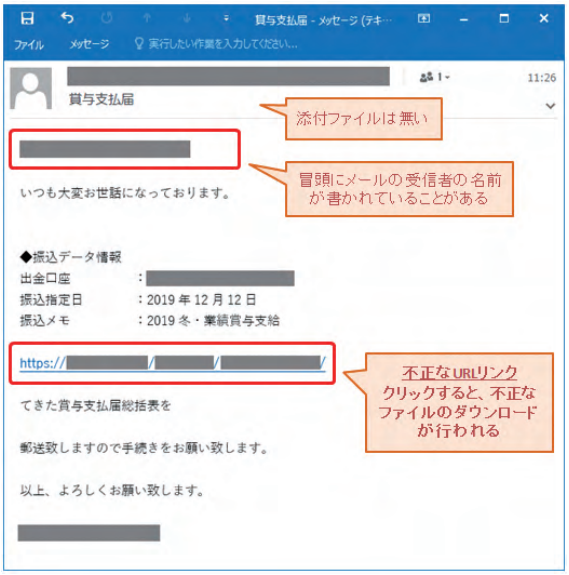
■図 1-2-16　新型コロナウイルスを題材とした Emotet のばらまき型メールの例
（出典）IPA「『Emotet』と呼ばれるウイルスへの感染を狙うメールについて」

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

これらの手口から、攻撃者は日本国内のメール受信者の興味・関心を惹く題材を選んで攻撃を行っていると推測され、執拗に日本国内を狙って攻撃していると言える。

- Emotet に感染させる手口

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



■図 1-2-17　不正な URL リンクを含む Emotet のばらまき型メールの例
（出典）IPA「『Emotet』と呼ばれるウイルスへの感染を狙うメールについて」

示す。

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

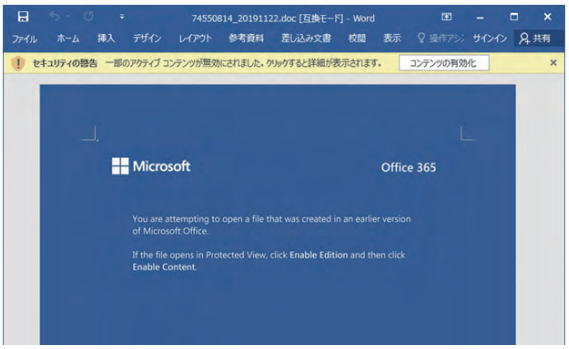
マクロ付き Word ファイルには、Microsoft や Office 等のロゴとともに、英語で「文書ファイルを閲覧するには操作が必要である」という趣旨の文と、次の二つのボタンのクリックを促す文が書かれている。

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

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

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

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



■図 1-2-18　マクロ付き Word ファイルを開いたときの画面の例
（出典）IPA「『Emotet』と呼ばれるウイルスへの感染を狙うメールについて」

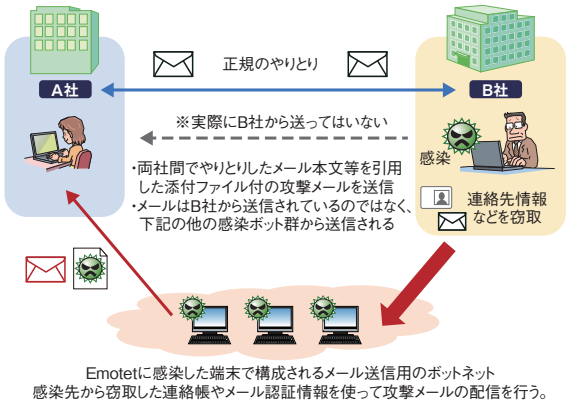
(c) Emotet の機能

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

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

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

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



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

呼ばれるランサムウェアに感染させる可能性がある※112。

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

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

(d) Emotet に感染しないための対策

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

(e) Emotet に感染した後の対応

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

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

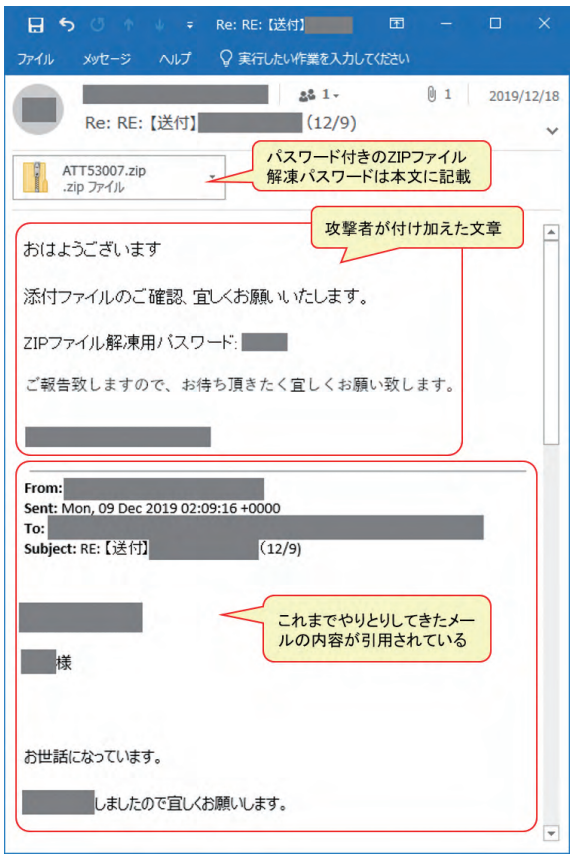
(2) Ursnif への感染を狙ったばらまき型メール

Ursnif は日本国内において、2016 年 3 月より観測されている、インターネットバンキングの情報を窃取し、不正送金を行うウイルスである※114。Ursnif には、DreamBot と呼ばれる亜種が存在し、2017 年 3 月と 12 月に一般財団法人日本サイバー犯罪対策センター（JC3：Japan Cybercrime Control Center）より、DreamBot に関する注意喚起情報が公開された※115。IPA は、2019 年 12 月にも Ursnif への感染を狙ったばらまき型メール（以下、Ursnif のばらまき型メール）を観測した※102。

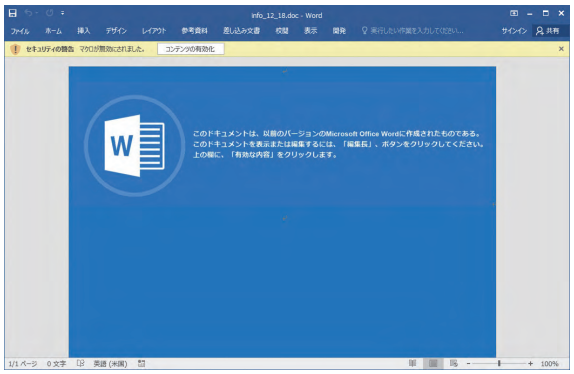
このばらまき型メールは、Emotet のばらまき型メールと同様、正規のメールへの返信を装うメールであった。メールにはパスワード付きの ZIP ファイルが添付されており、パスワードはメール本文に記載されていた。添付ファイルを解凍するとマクロ付き Word ファイルが出力され、利用者がそのファイルを開いて「コンテンツの有効化」ボタンをクリックすると Ursnif に感染させられる※77。Ursnif のばらまき型メールの例を図 1-2-20（次ページ）に、Ursnif のばらまき型メールの添付ファイル内にある Word ファイルの例を図 1-2-21（次ページ）に示す。

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

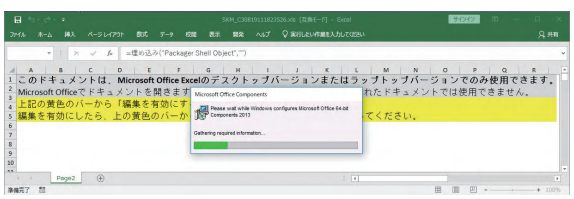
IPA は 2019 年 12 月に、Get2 Downloader と呼ばれるウイルスを使用し、別のウイルスへの感染を狙ったばらまき型メール（以下、Get2 Downloader のばらまき型メール）を観測した。Get2 Downloader のばらまき型メールにはマクロ付き Excel ファイルが添付されている。Excel ファイルのマクロを有効化すると Windows のプログレスバーのような画面が表示され（次ページ図 1-2-22）、何かのインストールを行っているように見える。しかし、実際は Get2 Downloader が Excel ファイルから端末へ設置、実行されており、更に別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



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



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



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

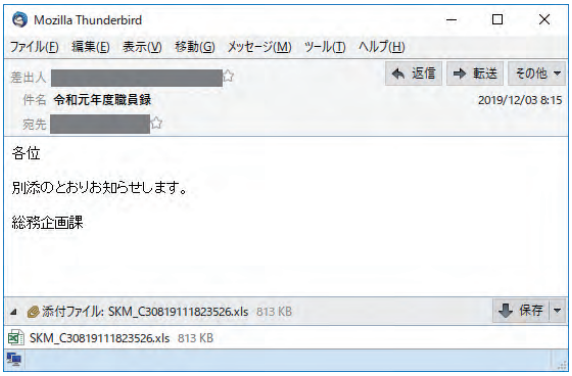
されておらず、日本で使用された Get2 Downloader のばらまき型メールから最終的に感染させられるウイルスの詳細は不明である。また、Get2 Downloader のばらまき型メールでは正規のメールへの返信を装う手口は見られず、メール本文がない、または数行程度の簡素な内容であった※102。図 1-2-23、図 1-2-24 に Get2 Downloader のばらまき型メールの例を示す。

(4) ばらまき型メールへの対策

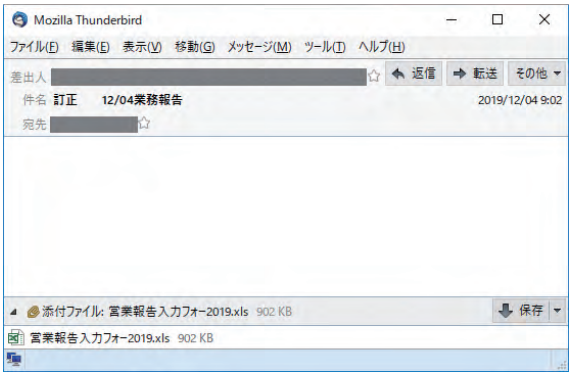
ばらまき型メールの攻撃者は、ウイルスに感染させる確率を上げるために様々な工夫を凝らしており、常に新たな手口で攻撃してくる可能性がある。セキュリティソフトの活用、スパムメール対策、メール受信者の自己防衛等の対策を実施し、多層的な防御を行うことが重要である。

(a) 一般利用者における対策

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



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



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

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

(b) 組織・企業における対策

組織・企業におけるばらまき型メールに対する対策は、「1.2.1 (4) 標的型攻撃への対策」で述べている内容と基本的には同じである。不審なメールを受信した際の報告窓口を設けることや、ウイルス感染を想定した利用者の訓練と教育を行うこと、システムでの対策として、不審なメールを確保できる仕組みの確立や適切な修正プログラムの適用、特定のファイル形式について実行許可・禁止の設定を行う、といった対策が重要である。

また、公開されているばらまき型メールに関する注意喚起情報を組織内で共有し、同様の攻撃による被害を受けないようにすることも重要である。

1.2.6 個人をターゲットにした騙しの手口

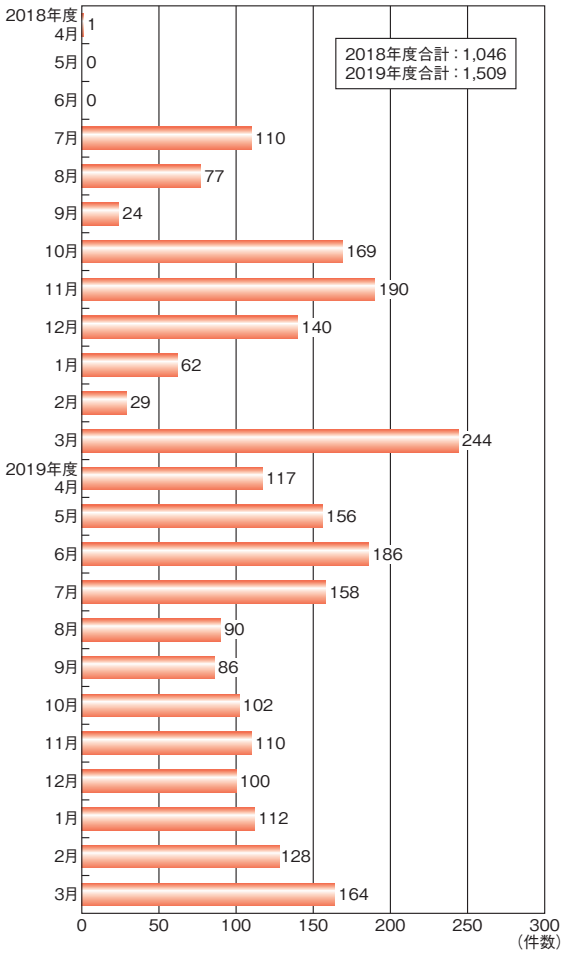
2019 年度は、個人を狙って騙そうとする手口による被害が目立った。本項では、騙しの手口を「遭遇するきっかけとなるサービス(SMS、メール、Web ブラウザ、アプリ)」別に、手口事例や対策を紹介する。また、最後に騙しの手口に共通の対策を解説する。

(1) SMS をきっかけとする手口

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

(a) 宅配便の不在通知を装う SMS

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



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

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

(ア)手口

この手口は、「お客様宛にお荷物のお届けにあがりましたが不在の為持ち帰りました。」という宅配便の不在通知を装った SMS を送り付け、SMS 内のリンクから、宅配便業者の正規サイトを模した偽サイトへ誘導する。

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

偽サイトでは、アクセスしたスマートフォンが、Android OS 端末(以下 Android)であるか、iPhone や iPad 等の iOS 端末(以下 iPhone)であるかによって、この後の手口が異なる。

Android の場合、偽サイトにアクセスすると、不正アプリの APK ファイル(Android アプリのパッケージファイル)が自動でダウンロードされる。偽サイトに記載の手順に従って不正アプリをインストールすると、被害につながる(図 1-2-26)。

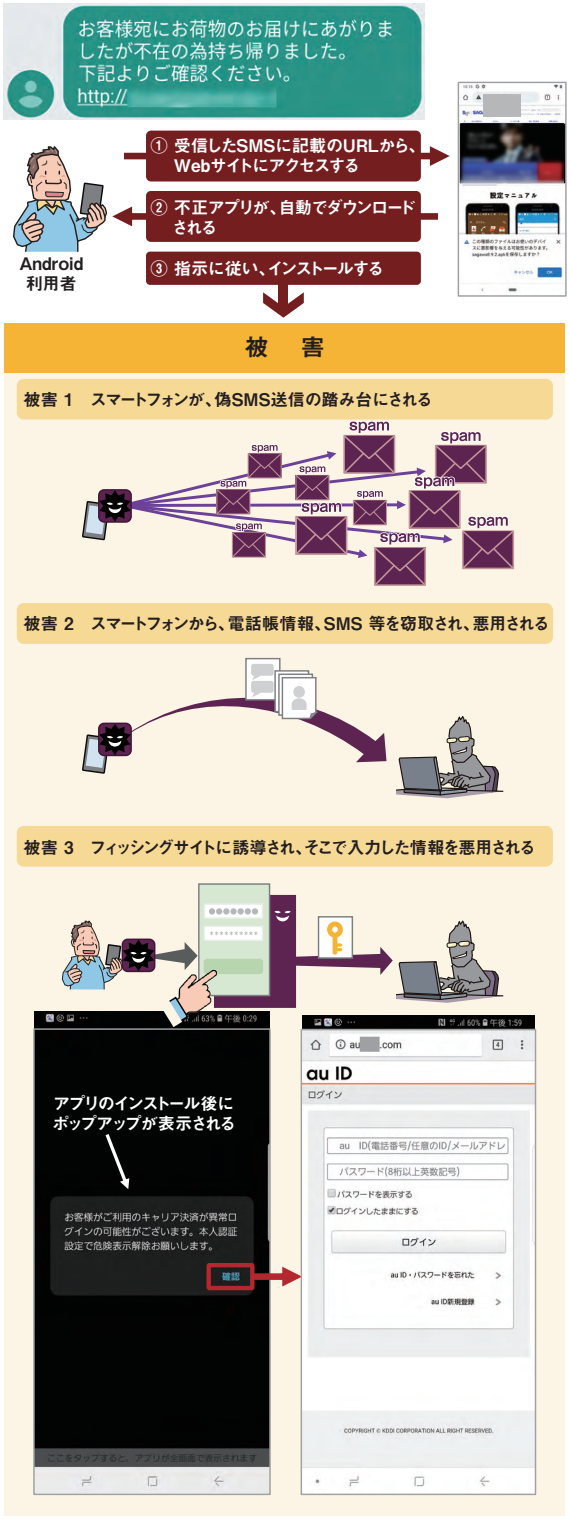
iPhone の場合、偽サイトにアクセスすると、フィッシングサイトが表示される。サイトの指示に従って「電話番号とキャリア決済の認証コード」や「Apple ID とパスワード」等、情報を入力すると、被害につながる。

Android における不正アプリの被害として、以下が確認されている。

①スマートフォンが攻撃の踏み台にされ、不特定多数の宛先(自身のアドレス帳にはない電話番号)へ、偽 SMS を勝手に送信される。

②スマートフォンから、アドレス帳の内容、SMS メッセージ等を窃取され悪用される。

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



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

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

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

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

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

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

iPhone におけるフィッシングの被害として、以下が確認されている。

①「電話番号と、キャリア決済の認証コード」を入力した場合、キャリア決済を不正使用される。

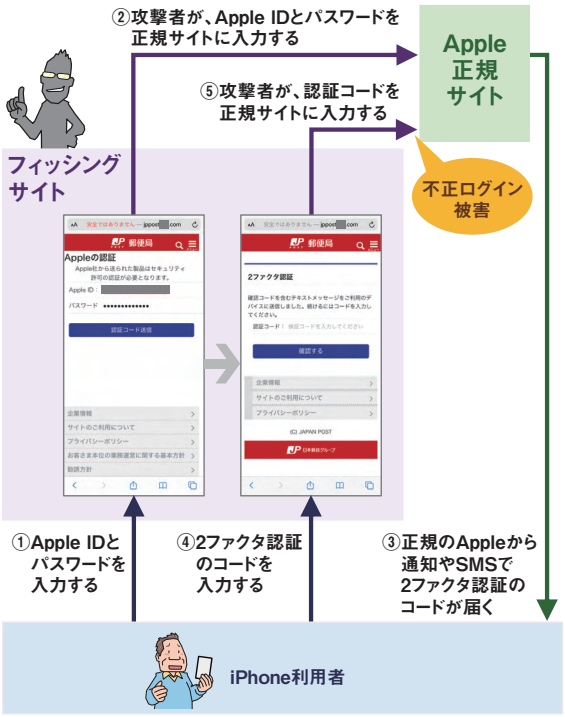
②「Apple ID とパスワード」を入力した場合、iCloud 等の Apple のサイトに不正ログインされる。

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

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

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

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



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

わかるように、内容が変化し続けている点に注意が必要である。

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

（イ）対処

Android で不正アプリをインストールした場合、以下の対処を推奨する。

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

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

③スマートフォンを初期化する。

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

⑤キャリア決済の不正使用がないか、携帯通信会社に確認する。

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

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

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

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

(b)送信元を偽装して携帯通信会社等を装うSMS

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

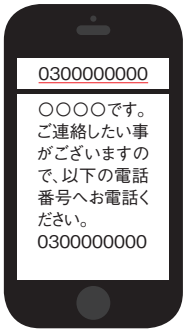
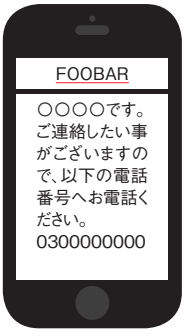
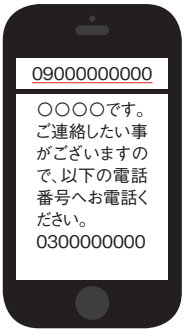
(ア)手口

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

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

(イ)対処

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

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

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

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

(c) 金融機関を装う SMS

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

金融機関を装う SMS の手口では、「セキュリティ強化のため利用を一時停止した」「口座が不正使用されている可能性がある」といった内容の偽の SMS を送り、対処が必要であるとして SMS 内のリンクからフィッシングサイトへ誘導する。

フィッシングサイトに表示される入力項目は、インターネットバンキングのアカウント情報(ログイン ID・パスワード)、銀行口座情報、電話番号等一様ではなく、各インターネットバンキングの認証システム仕様に合わせて情報を詐取していると考えられる。また、ワンタイムパスワード、乱数表等の多要素認証の情報も詐取する。これらを奪われることで多要素認証による本人確認も突破され、被害につながっている※127。

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

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

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

(d) SMS をきっかけとする手口に共通の対策

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

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

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

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

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

(2) メールをきっかけとする手口

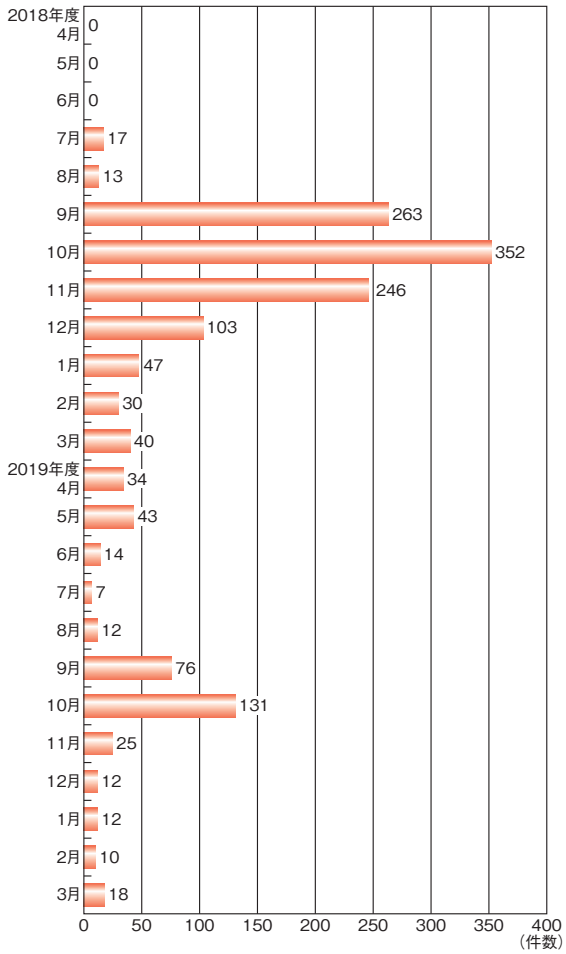
メールを用いる手口は、フィッシングメール、ばらまき型

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

(a)仮想通貨を要求する脅迫メール

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

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



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

(ア)手口

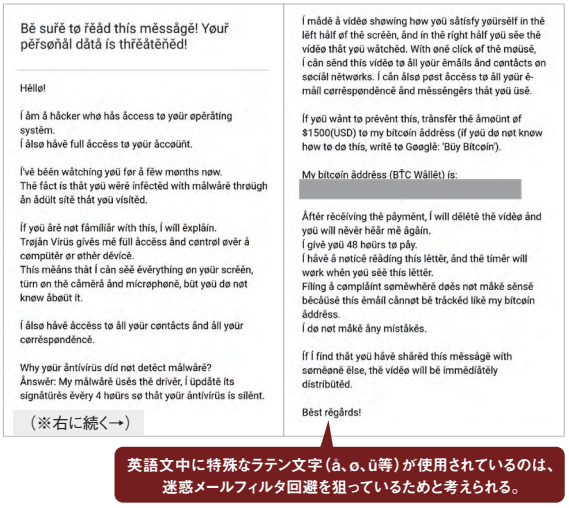
この手口のメールは、脅迫の内容や使用言語に多くのバリエーションがあるが、内容の要旨は当初から変わらない（図 1-2-30、図 1-2-31）。

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

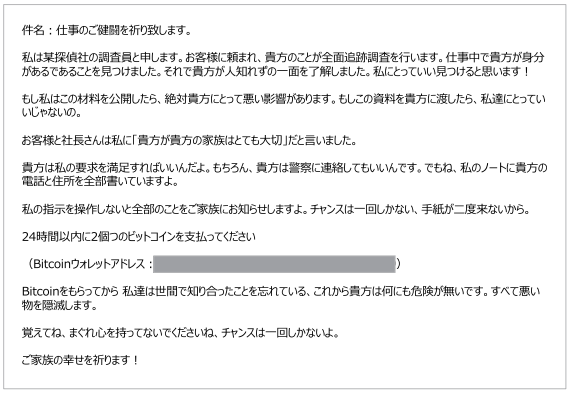
②盗んだ情報を連絡先等へばらまかれたくなければ、制限時間内に Bitcoin（ビットコイン）や Dash（ダッシュ）等の仮想通貨を送金するよう要求する。

③メールの送信元が、メール受信者自身のアドレスになっている場合がある。

④メールの件名や本文に、パスワードが一つ書かれている場合がある。



■図 1-2-30　仮想通貨を要求する英語の脅迫メールの例



■図 1-2-31　仮想通貨を要求する日本語の脅迫メールの例

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

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

(イ) 対処

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

(b) メールをきっかけとする手口に共通の対策

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

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

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

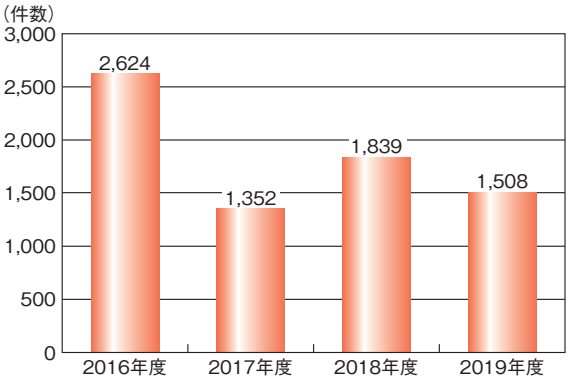
(3) Web ブラウザの表示をきっかけとする手口

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

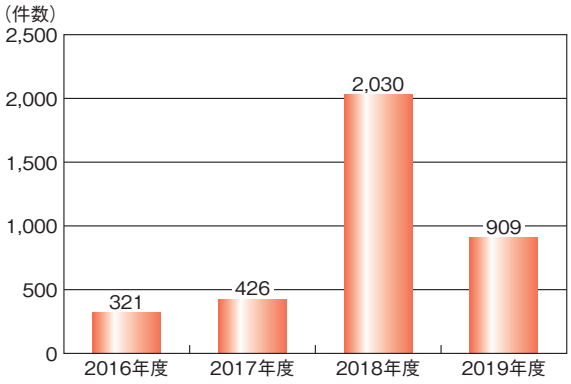
(a) 偽のセキュリティ警告

パソコンで Web サイト閲覧中に、突然「ウイルスに感染している」等の警告画面が表示されたことをきっかけに、有償のサポート契約やセキュリティソフト購入をしてしまう被害が、後を絶たない。

2019 年度に IPA の安心相談窓口に寄せられた相談件数は、有償サポート契約に誘導される「偽警告」(別名、サポート詐欺)が、1,508 件(図 1-2-32)、有償ソフトウェアの購入に誘導される「偽セキュリティソフト」が、909 件だった(図 1-2-33)。



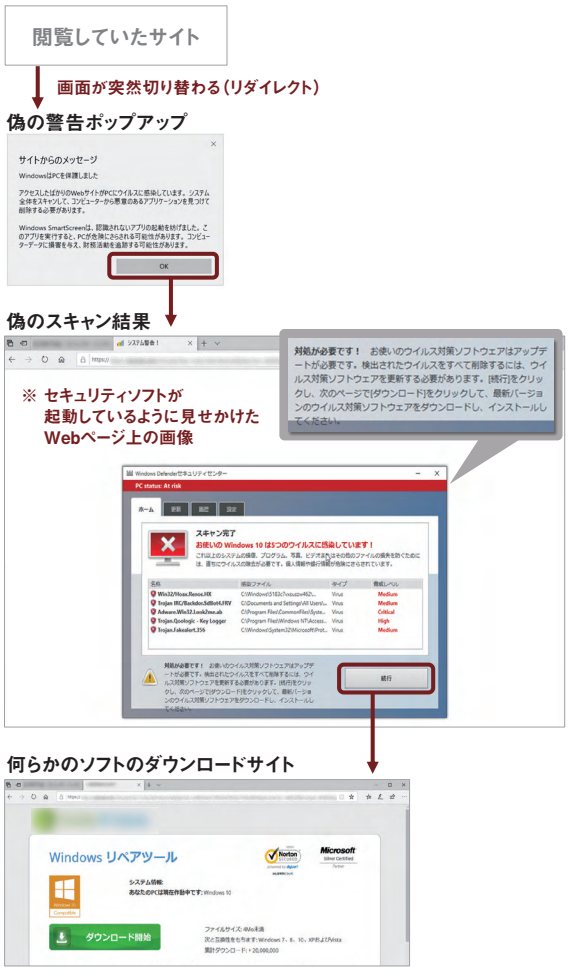
■図 1-2-32　偽警告に関する年度別相談件数



■図 1-2-33　偽セキュリティソフトに関する年度別相談件数

(ア) 手口

「偽警告」と「偽セキュリティソフト」の手口は、閲覧していたWebサイトから突然画面が切り替わり、偽のセキュリティ警告画面(図 1-2-34)が表示されることから始まる。警告画面は、「ウイルスに感染している」「システムが破



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

損する」等と、根拠のない内容で不安を煽る。

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

①警告画面に記載の電話番号に電話をかけると、オペレーターから至急パソコンの確認が必要であると説明される。

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

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

④支払いに応じると、オペレーターが遠隔操作で「パソコンの対処」と称する作業を行う。その作業の中で、セキュリティソフトであるとして詳細不明のソフトウェアをインストールされる場合もある。

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

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

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

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

(イ)対処

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

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

利用者自身やオペレーターが詳細不明のソフトウェアをインストールした場合は、より安全な対応として、当該ソフトをインストールする前の状態にシステムを戻すこと（Windows の「システムの復元」や、Mac の「Time Machine」で作成しておいたバックアップからの復元）や、パソコンの初期化をすることを推奨する。

契約については、消費生活センターに相談し、クレジットカードで支払いを行った場合はクレジットカード会社にも連絡していただきたい。

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

(b)アプリ誘導

Web サイト閲覧中に「ウイルスに感染している」等の根拠のない警告画面を表示して騙す手口は、パソコンだけでなく、スマートフォンでも存在する。

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

(ア)手口

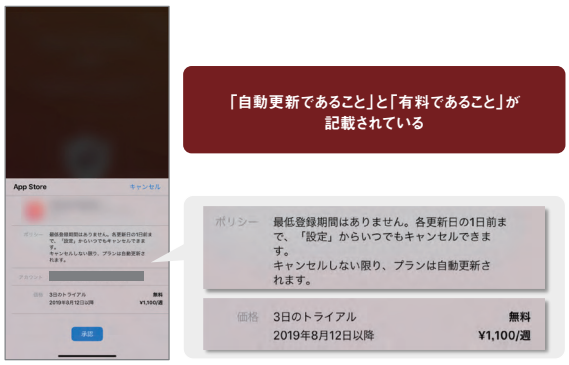
スマートフォンでの手口は、警告画面に表示された問題は「セキュリティアプリ」で解決できるとして、公式マーケット上のアプリに誘導するというものである（図 1-2-35）。

この手口の目的は不明だが、「利用者にアプリをインストールさせることによる報酬（PPI：Pay Per Install）」を得ようとするアフィリエイト（成果報酬型広告）ではないかと考えられる。なお、偽のセキュリティ警告の出力元（広告主）と誘導されるアプリの開発元との関係は判明していない。

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

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

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



■図 1-2-36　自動継続課金である旨の確認メッセージの例（iPhone）

（イ）対処

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

アプリをインストールしてしまった場合は、不要であればアンインストールをする。なお、アンインストールのみでは自動継続課金は解約にならない点に注意が必要である。自動継続課金に登録した場合は、iPhone の場合はサブスクリプションの解約、Android の場合は定期購入の解約も実施する。

（c）Web ブラウザの表示をきっかけとする手口に共通の対策

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

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

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

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

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

（4）アプリのインストールをきっかけとする手口

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

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

（a）公式マーケット上で配布された不正アプリ

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

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

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

度にわたり Google Play で公開されたとのことである。

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

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

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

(b) 公式マーケット以外で配布された不正アプリ

不正アプリは、公式マーケット以外の場所で配布されることが多い。

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

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

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

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

①正規の SNS アプリでビデオ通話をする

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

② App Store 以外からアプリを入手するよう誘導される

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

③ビデオ通話の動画を友人や知人にばらまくと脅され、金銭を要求される

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

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

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

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

(c) アプリのインストールをきっかけとする手口に共通の対策

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

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

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

(5) 騙しの手口に共通の対策

人間の心理を突いて騙す手口への対策は、以下のとおりである。

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

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

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

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

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

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

1.2.7 情報漏えいによる被害

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

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

(1) 外部からの攻撃による情報漏えい

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

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

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

性が判明した。

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

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

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

(2) 過失による情報漏えい

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

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

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

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

(3) 内部者の不正による情報漏えい

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

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

(4) 不適切な情報の取り扱いによる情報流出

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

(5) 対策

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

(a) 外部からの攻撃への対策

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

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

■表 1-2-5　外部からの攻撃による情報漏えいの主な事例（報道または公表事例を基に IPA が作成）

(b) 人為的な過失への対策

情報の取り扱いに人が介在する状況においては、過失による情報漏えい被害を完全に防ぐことは難しい。過去の事例に基づく教育等で担当者の意識向上を図ることも有効であるが、それだけでなく、重要な情報の取り扱いルールを設け、その運用を徹底する、適宜見直す

等で、過失の発生をできる限り抑止していく体制づくりが望まれる。

(c) 内部者の不正への対策

過失への対策と同様、内部不正による情報漏えい被害を完全に防ぐことは難しいが、情報を取り扱う者に対して正しい知識や規則を理解、遵守してもらう取り組みが不可欠である。その上で、監視カメラの設置や退職者のアカウント管理の徹底、通信や操作ログの監視及び保全、部署や役職に応じたアクセス権限の設定（最小権限化）等、不正を実行しにくい環境を整えることも望まれる。また、私用端末によるテレワークは情報の持ち出しなど、内部不正がおきやすい環境であるといえる。内部不正を起こさせないような注意喚起、あるいは私用端末では機微情報を扱わない、等のルール策定・周知も重要である。

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

(d) 不適切な情報の取り扱いへの対策

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

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

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

(6) 2019 年度に特徴的な情報保護対策

前述の対策以外に、2019 年度に動きがあった情報保護対策について述べる。

(a) クレジットカード情報の保護対策

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

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

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

(b) テレワークにおける対策

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

COLUMN

適切なインシデント対応に必要なのは、教育や規則だけじゃない

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

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

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

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

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

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

1.3 情報システムの脆弱性の動向

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

1.3.1 JVN iPediaの登録情報から見る脆弱性の傾向

IPA は、脆弱性対策情報データベース「JVN iPedia※100」に、国内外のソフトウェア製品の脆弱性対策情報を収集し、蓄積している。このデータベースに登録されている脆弱性対策情報から、ソフトウェアに関する脆弱性の特徴を統計的に確認することができる。本項では、2019 年 12 月までに登録された JVN iPedia の脆弱性対策情報の傾向を分析する。

(1) JVN iPedia への登録状況

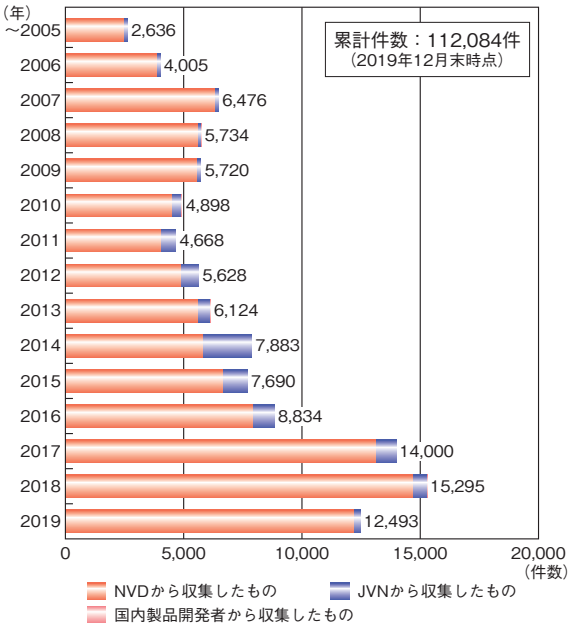
JVN iPedia は、国内外で利用されているソフトウェア製品の脆弱性対策情報を、以下の三つの公開情報から収集・蓄積しており、2007 年 4 月 25 日から公開している。

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

(a) JVN iPedia の登録件数の推移

JVN iPedia に登録している情報を、製品ベンダやセキュリティ関連企業が脆弱性情報を公表した年別※180にまとめると、2011 年を境にして NVD から収集した脆弱性対策情報の登録件数が増加傾向となっており、2017 年以降の JVN iPedia の登録件数は 1 万件を上回っている（図 1-3-1）。NVD に公開される脆弱性の件数が増加した理由としては、脆弱性を登録するための共通識別子である CVE（Common Vulnerabilities and Exposures）※181 の採番機関（CNA：CVE Numbering Authority）※182 が増加したことが一因として挙げられる。The MITRE Corporation※183 によると、2016 年 12 月に 47 社※184 だった CNA は、2019 年 12 月には 110 社※185 と約 2.3 倍になっている。この増加した CNA によって、多くの脆弱性に CVE が付与され、NVD に公開される脆弱性の件数増加につながった可能性がある。

一方、JVN から収集した脆弱性情報は、2014 年の 2,084 件を境に減少傾向となっており、2019 年は 318 件となっている。また、国内製品開発者から公表された脆弱性対策情報は、毎年数十件の登録となっており、2019 年は 16 件であった。

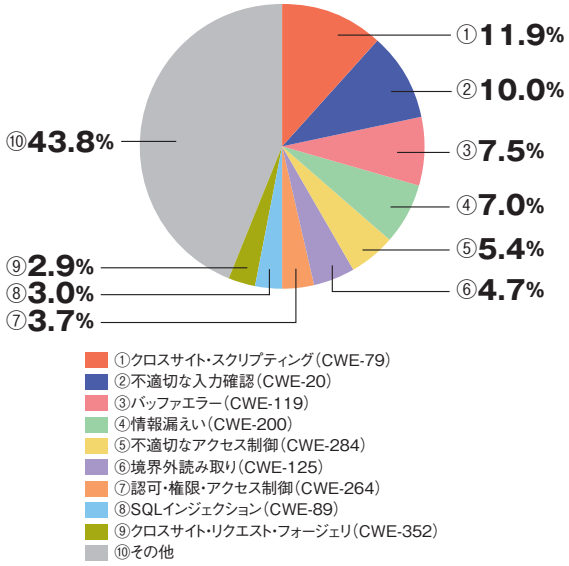


■図 1-3-1　JVN iPedia 登録状況（公表年別）
（出典）JVN iPedia の登録情報を基に IPA が作成

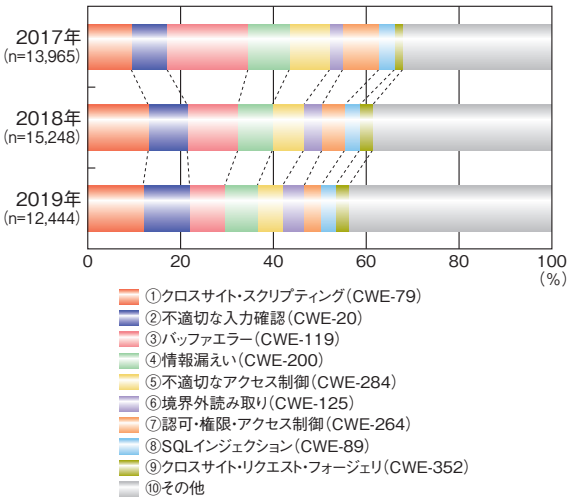
JVN iPedia は、発見された脆弱性の種類を識別するための共通脆弱性タイプ一覧 CWE（Common Weakness Enumeration）※186 を脆弱性対策情報に付与して登録を行っている。2019 年に登録した CWE の割合は「クロスサイト・スクリプティング」が 11.9%と最も高く、以下、「不適切な入力確認」が 10.0%、「バッファエラー」が 7.5%、「情報漏えい」が 7.0%と続いている（図 1-3-2）。

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

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



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



■図 1-3-3　JVN iPedia におけるソフトウェア製品の CWE 別割合（2017 ～ 2019 年）
（出典）JVN iPedia の登録情報を基に IPA が作成

(b) JVN iPedia の登録情報の深刻度

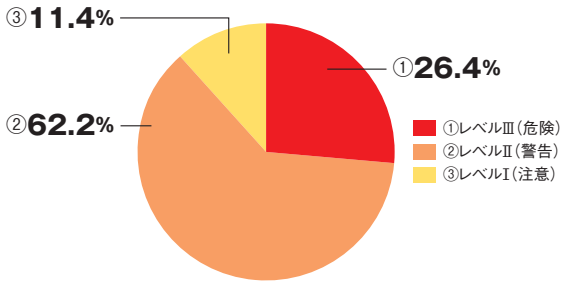
JVN iPedia は、オープンで汎用的な脆弱性評価手法である CVSS（Common Vulnerability Scoring System：共通脆弱性評価システム）※187 を用いて、脆弱性の深刻度を公開している。なお、JVN iPedia では CVSS v2 及び CVSS v3 の二つのバージョンの情報を公開しているが、本項では CVSS v2 を基に統計処理を行っている。

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

深刻度のレベルごとに想定される影響は以下である。

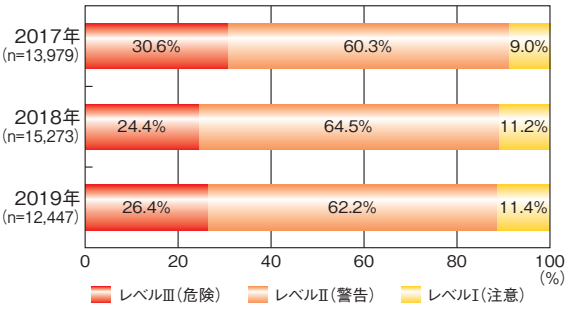
- 深刻度 レベルIII（危険）BM 7.0 ～ 10.0
  リモートからシステムを完全に制御されたり、大部分の情報が漏えいしたりする等の影響が想定される。
- 深刻度 レベルII（警告）BM 4.0 ～ 6.9
  一部の情報が漏えいしたり、サービス停止につながったりする等の影響が想定される。
- 深刻度 レベルI（注意）BM 0.0 ～ 3.9
  深刻度レベルII相当の影響があるが、攻撃するために複雑な条件を必要とする。

2019 年に登録された脆弱性対策情報を深刻度のレベルで分類すると、レベルIIIが 26.4%、レベルIIが 62.2%、レベルIが 11.4% となっており、一部の情報漏えいやサービス停止につながるレベルII以上の脆弱性が全体の約 9 割を占めている（図 1-3-4）。



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

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



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

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

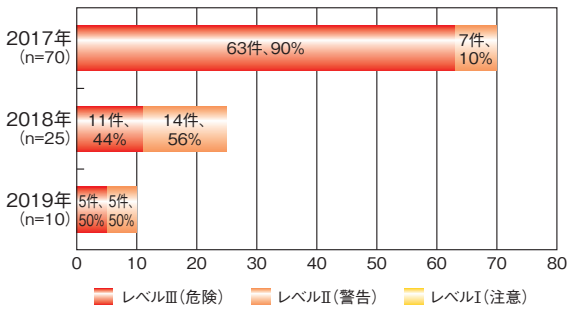
製品開発者は、ソフトウェアの企画・設計・製造段階からセキュアコーディング※188を含めたセキュリティ対策を講じる等、脆弱性による被害を未然に防ぐための対応が必要となる。また、製品の利用者にも、日頃から新たに公開される脆弱性対策情報に注意を払い、脆弱性が公開された場合には製品を最新バージョンにアップデートする等の対応が求められる。

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

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

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

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



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

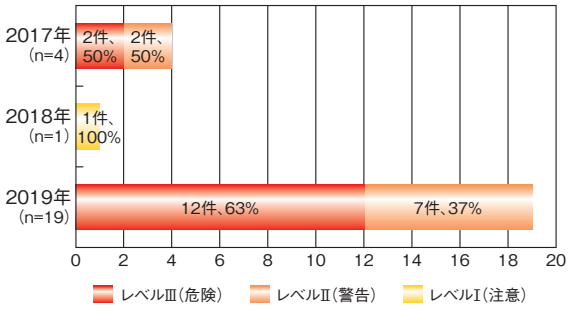
Adobe Flash Playerを利用するコンテンツを提供している組織においては、2020年末までにHTML5形式等の代替手段へ移行する必要がある。また、コンテンツの利用者に対して、移行方法等の周知を行う必要がある。コンテンツの利用者においては、Adobe Flash Playerのサポートが終了するまでは常に最新バージョンを使い、コンテンツの提供者から移行に関する情報が公開された場合は、早急にそれに従うことが望ましい。

(3) リモートデスクトップサービスに関連する脆弱性について

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

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

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



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

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

(4) 今後の展望

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

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

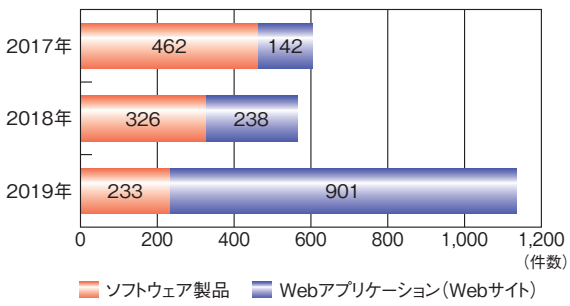
例えば、テレワークで BYOD を活用する場合は、外部から安全に社内にアクセスするための認証や VPN（Virtual Private Network）等の仕組みが必要であり、それに伴う新しい機器やシステムの導入及び管理が求められる。更に、これまで組織が従業員に貸与していた端末の管理に加え、従業員が所有している端末も安全なテレワークのために組織が定めたルールに基づく管理が必要となる。また、リモートデスクトップサービスを利用して社内に接続する場合は、「1.3.1 (3) リモートデスクトップサービスに関連する脆弱性について」で説明したように、利用端末の OS のバージョンを常に最新に保ち、脆弱性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

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

1.3.2 早期警戒パートナーシップの届出状況から見る脆弱性の動向

ソフトウェア製品や Web アプリケーションの脆弱性を悪用した攻撃による情報漏えい、及び Web ページ改ざん等の被害は、2019 年も引き続き発生している。例えば、脆弱性のある EC サイト構築パッケージを使って作られた Web サイトからクレジットカード番号等が窃取される被害が多く発生したことを受け、2019 年末に製品開発者に加え、経済産業省や IPA からも注意喚起※192 がなされた。

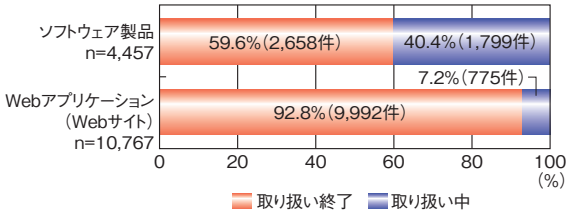
2019 年に「情報セキュリティ早期警戒パートナーシップ」（以下、パートナーシップ）に基づき IPA に届け出された脆弱性関連情報※193 の件数は、ソフトウェア製品が 233 件、Web サイトが 901 件、合計 1,134 件であった。2018 年の届出件数（564 件）と比較すると、約 2 倍に増加している。なお、それぞれの件数を 2018 年の届出件数（ソフトウェア製品：326 件、Web サイト：238 件）と比較すると、ソフトウェア製品に対する届出は約 29% 減少、Web サイトに対する届出は約 280% 増加した（図 1-3-8）。



■図 1-3-8　脆弱性関連情報の種類別届出状況（2017 ～ 2019 年）
（出典）パートナーシップの届出状況を基に IPA が作成

パートナーシップ開始時点（2004 年 7 月 8 日）からの届出件数を累計すると、ソフトウェア製品は 4,457 件、

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



■図 1-3-9　脆弱性関連情報の種類別取扱終了状況
（2019 年末までの累計）
（出典）パートナーシップの届出状況を基に IPA が作成

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

（1）ソフトウェア製品の脆弱性

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

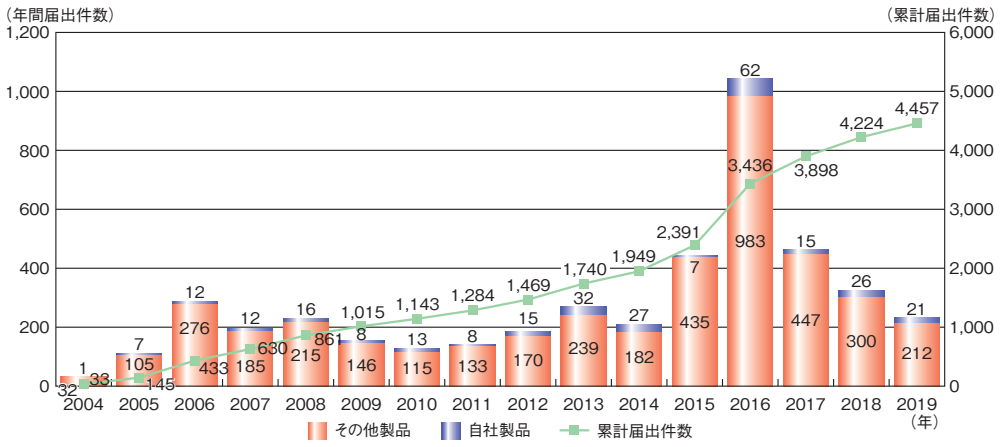
（a）パートナーシップの届出から見たソフトウェア製品の脆弱性

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

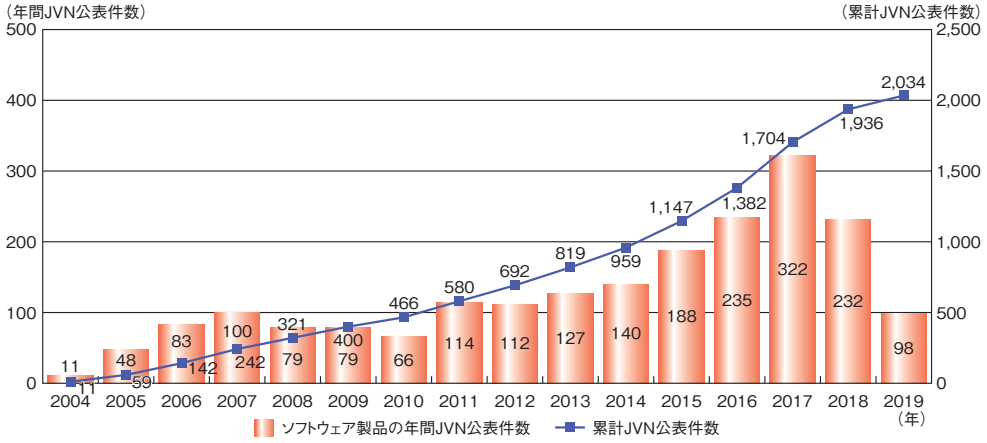
脆弱性をソフトウェア製品種類別（表 1-3-1）に見ると、届出件数の合計は 2018 年が 312 件、2019 年が 221 件と約 3 割減少している中、「スマートフォン向けアプリ」「システム管理ソフト」「アプリケーション開発・実行環境」は増加している。

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

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



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



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

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

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

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

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

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

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

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

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

(b)「重要なセキュリティ情報」から見たソフトウェア製品の脆弱性

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

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

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

(c) ソフトウェア製品における脆弱性対策の課題

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

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

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

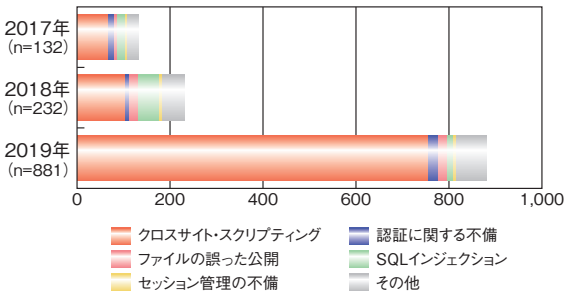
更に、一般の方が製品利用者である場合、利用しているソフトウェア製品を把握し、脆弱性情報を収集することは困難といえる。このため製品開発者は自動でアップデートできる機能の実装や、アップデートを促す警告を通知する機能を実装する等、製品利用者が受動的に対策をとれるように検討していただきたい。

(2) Web アプリケーション（Web サイト）の脆弱性

2019 年にパートナーシップで受け付けた Web アプリケーションの届出（不受理を除く）は、881 件であった。

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

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



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

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

(a) クロスサイト・スクリプティングの脆弱性

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

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

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

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

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

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

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

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

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

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

(c) Webサイト運営者に求められる対策

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

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

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

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

COLUMN

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

IPA では毎年、前年に発生したセキュリティ事故や攻撃の状況等から脅威を選出し、専門家等の投票により順位付けした「情報セキュリティ 10 大脅威」を発表しています。2020 年 1 月に公開した「情報セキュリティ 10 大脅威 2020」は、以下の表のとおりです。

表 情報セキュリティ 10 大脅威 2020「個人」・「組織」向け脅威の順位

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

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

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

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

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

※1　IBM 社：IBM X-Force 脅威インテリジェンス・インデックス　https://www.ibm.com/jp-ja/security/data-breach/threat-intelligence〔2020/6/30 確認〕
※2　Verizon 社：2020 Data Breach Investigations Report　https://enterprise.verizon.com/resources/reports/dbir/〔2020/6/30 確認〕
※3　トレンドマイクロ社：2019 年年間セキュリティラウンドアップ　https://resources.trendmicro.com/jp-docdownload-form-m197-web-2019-annualsecurityreport.html〔2020/6/30 確認〕
※4　APWG：PHISHING ACTIVITY TRENDS REPORTS　https://apwg.org/trendsreports/〔2020/6/30 確認〕
※5　URL を短縮する目的等で使用される、カスタマイズサービスのサイトを経由したリダイレクトによって元のサイトにアクセスする URL。
※6　トレンドマイクロ社：2018 年年間セキュリティラウンドアップ 騙しの手口の多様化と急増するメールの脅威　https://resources.trendmicro.com/jp-docdownload-form-m113-web-2018-annualsecurityreport.html〔2020/6/30 確認〕
※7　IC3：2019 Internet Crime Report　https://pdf.ic3.gov/2019_IC3Report.pdf〔2020/6/30 確認〕
※8　Piyolog：SSRF 攻撃による Capital One の個人情報流出についてまとめてみた　https://piyolog.hatenadiary.jp/entry/2019/08/06/062154〔2020/6/30 確認〕
ZDNet Japan：米金融大手 Capital One で 1 億人超の情報漏えい -- 容疑者は AWS 元従業員の可能性　https://japan.zdnet.com/article/35140621/〔2020/6/30 確認〕
※9　WAF（Web Application Firewall）：主に Web アプリケーションへの攻撃を防御するソフトウェアまたはハードウェア。
※10 SSRF（Server Side Request Forgery）攻撃：公開サーバ等の権限を悪用してイントラネット内のサーバに不正なコマンドを送る攻撃。
※11 日本経済新聞：全国民の個人情報が流出　エクアドルで 2000 万人分　https://www.nikkei.com/article/DGXMZO49918550Y9A910C1000000/〔2020/6/30 確認〕
WeLiveSecurity：Nearly all of Ecuador's citizens caught up in data leak　https://www.welivesecurity.com/2019/09/17/ecuador-citizens-data-leak/〔2020/6/30 確認〕
東洋経済オンライン：エクアドル、なぜほぼ全国民の情報漏れたのか　https://toyokeizai.net/articles/-/304865〔2020/6/30 確認〕
※12 ランサムウェア：パソコン及びネットワーク接続された共有フォルダ等に保管されたファイルを暗号化する、または画面ロック等によりパソコンを使用不可にするウイルスの総称。暗号化解除の条件と称して身代金の支払いを求める脅迫メッセージを表示するソフトウェアであることから「ransom」（身代金）と「software」（ソフトウェア）を組み合わせた造語で「ランサムウェア」と呼ばれている。
※13 Ars Technica：“Severe” ransomware attack cripples big aluminum producer　https://arstechnica.com/information-technology/2019/03/severe-ransomware-attack-cripples-big-aluminum-producer/〔2020/6/30 確認〕
※14 Trend Micro：California City Confirms Phone Line and Financial Data System Disruptions Caused by Ransomware　https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/california-city-confirms-phone-line-and-financial-data-system-disruptions-caused-by-ransomware
※15 ITmedia エンタープライズ：ホンダのシステム障害、原因は産業制御システムを狙うランサムウェア「Ekans」か　https://www.itmedia.co.jp/enterprise/articles/2006/11/news059.html〔2020/6/30 確認〕
※16 「マルウェア」等の用語を混在して使用すると、読者を混乱させる可能性があるため、本白書では特に断りのない限り、または文献引用上の正確性を期す必要のない限り、総称して「ウイルス」と表現する。
※17 DarkReading：Why Bricking Vulnerable IoT Devices Comes with Unintended Consequences　https://www.darkreading.com/iot/why-bricking-vulnerable-iot-devices-comes-with-unintended-consequences-/a/d-id/1336009〔2020/6/30 確認〕
※18 JVN iPedia：JVNDB-2017-002402 Microsoft OLE URL Moniker における遠隔の HTA データに対する不適切な処理　https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-002402.html〔2020/6/30 確認〕
※19 JVN iPedia：JVNDB-2017-009645 Microsoft Office 数式エディタにおけるスタックベースのバッファオーバーフローの脆弱性　https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-009645.html〔2020/6/30 確認〕
※20 当該集計情報は 2018 年度まで MBSD 社より「サイバーセキュリティ事件簿」という名称で公表されていたが、2019 年度からは MBSD 社の社内向け情報発信のために集計が継続されている。MBSD 社のご厚意により、ご提供いただいた集計情報を本白書では掲載している。
※21 https://www.jpcert.or.jp/ir/report.html〔2020/6/30 確認〕
※22 フィッシング対策協議会：月次報告書 一覧　https://www.antiphishing.jp/report/monthly/〔2020/6/30 確認〕
※23 2019 年度から「侵入感染」は「不正アクセス」、「改ざん・破壊」は「改ざん」、「情報流出・紛失」は「情報流出」、「妨害」は「その他」と事象分類の表記が変更された。
※24 JPCERT/CC：JPCERT/CC に報告されたフィッシングサイトの傾向 https://blogs.jpcert.or.jp/ja/2020/03/phishing2019.html〔2020/6/30 確認〕
※25 警察庁：フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（全銀協等と連携した注意喚起）https://www.npa.go.jp/cyber/policy/caution1910.html〔2020/6/30 確認〕
金融庁：インターネット・バンキングによる預金の不正送金事案が多発しています。　https://www.fsa.go.jp/ordinary/internet-bank_2.html〔2020/6/30 確認〕
全国銀行協会：フィッシング詐欺　https://www.zenginkyo.or.jp/hanzai/15300/〔2020/6/30 確認〕
JC3：インターネットバンキングの不正送金の被害に注意　https://www.jc3.or.jp/topics/banking/phishing.html〔2020/6/30 確認〕
フィッシング対策協議会：2019/11 フィッシング報告状況　https://www.antiphishing.jp/report/monthly/201911.html〔2020/6/30 確認〕
※26 警察庁：令和元年におけるサイバー空間をめぐる脅威の情勢等について　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R01_cyber_jousei.pdf〔2020/6/30 確認〕
※27 日経クロステック：サイバー攻撃を浴びる日本の銀行、2019 年 9 月に不正送金被害が急増した理由　https://xtech.nikkei.com/atcl/nxt/column/18/00001/03373/〔2020/6/30 確認〕
IPA：安心相談窓口だより　宅配便業者をかたる偽ショートメッセージに引き続き注意!　https://www.ipa.go.jp/security/anshin/mgdayori20200220.html〔2020/6/30 確認〕
※28 日経クロステック：ネットバンキングの不正送金被害が 11 月も過去最多を更新、警察庁が注意喚起　https://xtech.nikkei.com/atcl/nxt/news/18/06742/〔2020/6/30 確認〕
※29 トレンドマイクロ社：変化を続けるマルウェア「EMOTET」の被害が国内でも拡大　https://blog.trendmicro.co.jp/archives/22959〔2020/6/30 確認〕
※30 Yahoo ニュース：ホンダを狙ったサイバー攻撃。AD のドメインコントローラーの脆弱性が利用された可能性も。　https://news.yahoo.co.jp/byline/ohmototakashi/20200621-00184297/〔2020/6/30 確認〕
※31 ITmedia：相次ぐパスワードリスト攻撃に注意、パスワードの使い回しは厳禁　https://www.atmarkit.co.jp/ait/articles/1304/10/news092.html〔2020/6/30 確認〕
※32 株式会社セブン & アイ・ホールディングス：「7pay（セブンペイ）」サービス廃止のお知らせとこれまでの経緯、今後の対応に関する説明について　https://www.7andi.com/library/dbps_data/_template_/_res/news/2019/20190801_01.pdf〔2020/6/30 確認〕
※33 新型コロナウイルス感染症：2019 年 12 月に中華人民共和国にて新しく発生したとされるコロナウイルス。その後、新型コロナウイルス感染症は、世界保健機関（WHO：World Health Organization）により「COVID-19」と命名された。
※34 IPA：「Emotet」と呼ばれるウイルスへの感染を狙うメールについて　https://www.ipa.go.jp/security/announce/20191202.html〔2020/6/30 確認〕
※35 朝日新聞デジタル：経団連を標的、中国人ハッカー集団 ウイルスは 2 年潜伏　https://www.asahi.com/articles/ASM196VTPM19ULZU01B.html〔2020/6/10 確認〕
※36 https://www.ipa.go.jp/security/event/2013/isec-semi/documents/2013videosemi_targeted_cyber_attacks_v1.pdf〔2020/6/10 確認〕
※37 McAfee, LLC：Updated BlackEnergy Trojan Grows More Powerful　https://www.mcafee.com/blogs/other-blogs/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/〔2020/6/10 確認〕
※38 トレンドマイクロ社：サイバー攻撃集団「TICK」による「Operation ENDTRADE」　https://blog.trendmicro.co.jp/archives/23107〔2020/6/10 確認〕
※39 https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf〔2020/6/10 確認〕
※40 朝日新聞デジタル：【独自】三菱電機にサイバー攻撃　防衛などの情報流出か　https://www.asahi.com/articles/ASN1M6VDSN1MULFA009.html〔2020/6/10 確認〕
※41 朝日新聞デジタル：三菱電機へ高度なサイバー攻撃、中国政府の動きと呼応?　https://www.asahi.com/articles/ASN1X4JXHN1RULZU002.html〔2020/6/10 確認〕
※42 三菱電機株式会社：不正アクセスによる個人情報と企業機密の流

出の可能性について（第３報） https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf〔2020/6/10 確認〕
※ 43 三菱電機株式会社：不正アクセスによる個人情報と企業機密の流出の可能性について（第３報） https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf〔2020/6/10 確認〕
日本電気株式会社：当社の社内サーバへの不正アクセスについて https://jpn.nec.com/press/202001/20200131_01.html〔2020/6/10 確認〕
株式会社神戸製鋼所：当社ネットワークへの不正アクセスについて https://www.kobelco.co.jp/releases/files/20200206_1_01.pdf〔2020/6/10 確認〕
株式会社パスコ：社内ネットワーク端末に対する不正アクセスについて https://www.pasco.co.jp/press/2020/download/PPR20200206J.pdf〔2020/6/10 確認〕
※ 44 OLE：Windows 環境において、複数のソフトウェアが連携、データを共有するための技術。
※ 45 JPCERT/CC：マルウエアが含まれたショートカットファイルをダウンロードさせる攻撃 https://blogs.jpcert.or.jp/ja/2019/05/darkhotel_lnk.html〔2020/6/10 確認〕
JPCERT/CC：短縮 URL から VBScript をダウンロードさせるショートカットファイルを用いた攻撃 https://blogs.jpcert.or.jp/ja/2019/07/shorten_url_lnk.html〔2020/6/10 確認〕
※ 46 株式会社マクニカ：標的型攻撃の実態と対策アプローチ 第３版 日本を狙うサイバーエスピオナージの動向 2019 年度上期 https://www.macnica.net/mpressioncss/feature_04.html〔2020/6/10 確認〕
※ 47 日経ニューメディア：五輪開会式を想定して 70 社がサイバー演習、意外すぎる盲点に会場がざわつく https://tech.nikkeibp.co.jp/atcl/nxt/column/18/00001/03208/?ST=nnm〔2020/6/10 確認〕
※ 48 トレンドマイクロ社：フィッシング攻撃に注意、「ビジネスメール詐欺」の攻撃手口を分析 https://blog.trendmicro.co.jp/archives/17003〔2020/6/10 確認〕
※ 49 IC3：Business Email Compromise The $26 Billion Scam https://www.ic3.gov/media/2019/190910.aspx〔2020/6/10 確認〕
※ 50 IC3：Business E-mail Compromise The 12 Billion Dollar Scam https://www.ic3.gov/media/2018/180712.aspx〔2020/6/10 確認〕
※ 51 FBI：Worldwide Sweep Targets Business Email Compromise https://www.fbi.gov/news/stories/operation-rewired-bec-takedown-091019
※ 52 JPCERT/CC：ビジネスメール詐欺の実態調査報告書 https://www.jpcert.or.jp/research/20200325_BEC-survey.pdf〔2020/6/10 確認〕
※ 53 日本経済新聞：トヨタ紡織、欧州で最大 40 億円流出 業績修正を検討 https://www.nikkei.com/article/DGXMZO49508720W9A900C1CN8000/〔2020/6/10 確認〕
※ 54 日本経済新聞：日経米子会社、香港に 32 億円流出 詐欺被害か https://www.nikkei.com/article/DGXMZO51583520Q9A031C1SHA000/〔2020/7/27 確認〕
※ 55 トレンドマイクロ社：法人システムを狙う脅迫と盗用 2019 年上半期セキュリティラウンドアップ https://resources.trendmicro.com/jp-docdownload-form-m144-web-2019-1h-security-round-up.html〔2020/6/10 確認〕
※ 56 J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan（サイバー情報共有イニシアティブ）の略称。IPA を情報ハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策につなげていく取り組み。
※ 57 IPA：サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ） https://www.ipa.go.jp/security/J-CSIP/〔2020/6/10 確認〕
※ 58 Forbes JAPAN：「ビジネスメール詐欺」の被害額は年間 1.4 兆円、FBI が警告 https://forbesjapan.com/articles/detail/27057〔2020/6/10 確認〕
Bleeping Computer：$1.75 Million Stolen by Crooks in Church BEC Attack https://www.bleepingcomputer.com/news/security/175-million-stolen-by-crooks-in-church-bec-attack/〔2020/6/10 確認〕
cleveland.com：Email hackers steal $1.75 million from St. Ambrose Catholic Parish in Brunswick https://www.cleveland.com/crime/2019/04/email-hackers-steal-175-million-from-st-ambrose-catholic-parish-in-brunswick.html〔2020/6/10 確認〕
※ 59 株式会社カスペルスキー：だまされたサッカークラブ https://blog.kaspersky.co.jp/boca-juniors-case/23331/〔2020/6/10 確認〕
Infobae：Exclusivo: investigan el robo de 519.000 euros que el Paris Saint Germain le pagó a Boca por el pase de Paredes https://www.infobae.com/sociedad/policiales/2019/05/26/exclusivo-investigan-el-robo-de-519-000-euros-que-el-paris-saint-germain-le-pago-a-boca-por-el-pase-de-paredes/〔2020/6/10 確認〕
※ 60 日本経済新聞：ビジネスメール詐欺広がる 本物の書類でつい油断 https://www.nikkei.com/article/DGXMZO45609320T00C19A6000000/〔2020/6/10 確認〕
※ 61 St. Thomas Source：WAPA Missing $2.17 Million Was Stolen in Email Scam https://stthomassource.com/content/2019/06/11/wapa-missing-2-18-million-was-stolen-in-email-scam/〔2020/6/10 確認〕
※ 62 Bleeping Computer：North Carolina County Lost $1.7 Million in BEC Scam https://www.bleepingcomputer.com/news/security/north-carolina-county-lost-17-million-in-bec-scam/〔2020/6/10 確認〕
Cabarrus County：Cabarrus County Government targeted in social engineering scam https://cabarruscounty.us/news/cabarrus-county-government-targeted-in-social-engineering-scam/〔2020/6/10 確認〕
※ 63 650 CKOM：City of Saskatoon bilked out of more than $1 million https://www.ckom.com/2019/08/15/city-of-saskatoon-bilked-out-of-more-than-1-million-dollars/〔2020/6/10 確認〕
AFPBB News：カナダの自治体がフィッシング詐欺被害、8300 万円だまし取られる https://www.afpbb.com/articles/-/3240194〔2020/6/10 確認〕
※ 64 Naples Daily：Collier County scammed out of $184K in phishing scheme that investigators say originated abroad https://www.naplesnews.com/story/news/government/2019/08/19/collier-county-scammed-out-184-k-cyber-attack-phishing-scheme/2049019001/〔2020/6/10 確認〕
※ 65 ディープフェイク（deepfake）：AI（人工知能）技術の一つである「深層学習（deep learning）」と「偽物（fake）」を組み合わせた造語とされる。深層学習の技術を活用し、現実の映像や音声、画像の一部を加工して偽の情報を組み込み、あたかも本物のように見せかける。
※ 66 The Wall Street Journal：Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402〔2020/6/10 確認〕
ZDNet Japan：CEO になりすましたディープフェイクの音声で約 2600 万円の詐欺被害か https://japan.zdnet.com/article/35142255/〔2020/6/10 確認〕
※ 67 Iceland Review：Hackers Defraud Nearly Four Hundred Million From Power Company https://www.icelandreview.com/news/hackers-defraud-nearly-four-hundred-million-from-power-company/〔2020/6/10 確認〕
FRETTABLADID：Sviku út hundruð milljóna af HS Orku https://www.frettabladid.is/frettir/hundruum-milljona-stoli-af-hs-orku/
mbl.is：„Þetta er skipulögð og þróuð árás“ https://www.mbl.is/vidskipti/frettir/2019/09/09/thetta_er_skipulogd_og_throud_aras/〔2020/6/10 確認〕
※ 68 OCALA.com：Ocala police Scammers swiped nearly $750,000 from city https://www.ocala.com/news/20191028/ocala-police-scammers-swiped-nearly-750000-from-city
Bleeping Computer：BEC Fraudsters Divert $742,000 from Ocala City in Florida https://www.bleepingcomputer.com/news/security/bec-fraudsters-divert-742-000-from-ocala-city-in-florida/〔2020/6/10 確認〕
※ 69 Quartz：An extra letter “s” enabled a million-dollar real estate scam https://qz.com/1752282/how-compromised-emails-enable-cybercrime-and-real-estate-scams/〔2020/6/10 確認〕
※ 70 CTV News：Waterloo Brewing loses $2.1 million in wire transfer scam https://kitchener.ctvnews.ca/waterloo-brewing-loses-2-1-million-in-wire-transfer-scam-1.4695755〔2020/6/10 確認〕
※ 71 The Denver Post：Town of Erie scammed out of $1 million in Parkway Bridge project, town says https://www.denverpost.com/2019/12/30/erie-victim-financial-fraud-parkway-bridge/amp/〔2020/6/10 確認〕
CBS Denver：Erie Officials Release New Information In $1 Million Bridge Scam https://denver.cbslocal.com/2020/01/15/erie-bridge-scam-sema-construction/〔2020/6/10 確認〕
※ 72 トレンドマイクロ：米国の学校運営組織がビジネスメール詐欺により 230 万米ドルの被害 https://blog.trendmicro.co.jp/archives/23616〔2020/6/10 確認〕
KVUE-TV：Manor ISD loses $2.3M in phishing scam; police and FBI investigating https://www.kvue.com/article/news/education/schools/manor-isd-loses-millions-in-phishing-scam/269-296ff10a-c6d0-45e7-8b34-4fe0ed016715〔2020/6/10 確認〕

※ 73 Claims Journal：Fraudsters Posing as Art Dealer Got Gallery to Pay Millions https://www.claimsjournal.com/news/international/2020/01/30/295272.htm〔2020/6/10 確認〕
※ 74 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019年1月～3月］ https://www.ipa.go.jp/files/000073456.pdf〔2020/6/10 確認〕
※ 75 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019年4月～6月］ https://www.ipa.go.jp/files/000076713.pdf〔2020/6/10 確認〕
※ 76 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019年7月～9月］ https://www.ipa.go.jp/files/000078200.pdf〔2020/6/10 確認〕
※ 77 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019年10月～12月］ https://www.ipa.go.jp/files/000080133.pdf〔2020/6/10 確認〕
※ 78 IPA：プレス発表　本年確認されたビジネスメール詐欺の事例を解説、J-CSIP 運用状況レポートを公開 https://www.ipa.go.jp/about/press/20190726.html〔2020/6/10 確認〕
※ 79 IPA:【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口 https://www.ipa.go.jp/security/announce/20170403-bec.html〔2020/6/10 確認〕
※ 80 IPA：なりすましメール撲滅に向けたSPF（Sender Policy Framework）導入の手引き https://www.ipa.go.jp/security/topics/20120523_spf.html〔2020/6/10 確認〕
※ 81 一般財団法人インターネット協会：DKIM (Domainkeys Identified Mail) https://salt.iajapan.org/wpmu/anti_spam/admin/tech/explanation/dkim/〔2020/6/10 確認〕
※ 82 Microsoft 社：侵害された Office 365 電子メール アカウントへの対応 https://docs.microsoft.com/ja-jp/microsoft-365/security/office-365-security/responding-to-a-compromised-email-account〔2020/6/10 確認〕
※ 83 A10 ネットワークス株式会社：DDoS 攻撃者の武器 https://www.a10networks.co.jp/download/files/A10-EB-14115-JA2019Q2.pdf〔2020/6/10 確認〕
※ 84 wizSafe Security Signal 2019 年 1 月 観測レポート」～「wizSafe Security Signal 2019 年 12 月 観測レポート」を確認した。
株式会社インターネットイニシアティブ：観測レポートの記事一覧 https://wizsafe.iij.ad.jp/category/report/〔2020/6/10 確認〕
※ 85 Link11：Warning of Serious DDoS Blackmail Campaigns Attributed to Fancy Bear Group https://www.link11.com/en/blog/warning-of-serious-ddos-blackmail-campaigns-attributed-to-fancy-bear-group/〔2020/6/10 確認〕
※ 86 JPCERT/CC：DDoS 攻撃を示唆して、仮想通貨を要求する脅迫メールについて https://www.jpcert.or.jp/newsflash/2019103001.html〔2020/6/10 確認〕
※ 87 日本放送協会：ラグビーW杯組織委にサイバー攻撃 https://www.nhk.or.jp/politics/articles/lastweek/26369.html〔2020/6/10 確認〕
※ 88 Palo Alto Networks, Inc.：Muhstik Botnet Exploits the Latest WebLogicVulnerability for Cryptomining and DDoS Attacks https://unit42.paloaltonetworks.com/muhstik-botnet-exploits-the-latest-weblogic-vulnerability-for-cryptomining-and-ddos-attacks/〔2020/6/10 確認〕
※ 89 Palo Alto Networks, Inc.：Muhstik Botnet Attacks Tomato Routers to Harvest New IoT Devices https://unit42.paloaltonetworks.com/muhstik-botnet-attacks-tomato-routers-to-harvest-new-iot-devices/〔2020/6/10 確認〕
※ 90 株式会社インターネットイニシアティブ：Wikipedia, Twitch, Blizzard へ の DDoS 攻 撃 https://sect.iij.ad.jp/d/2019/09/175257.html〔2020/6/10 確認〕
※ 91 総務省：令和元年版情報通信白書 （2）IoT デバイスの急速な普及 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/html/nd112120.html〔2020/6/10 確認〕
※ 92 Microsoft 社：CVE-2019-0708 ¦ リモート デスクトップ サービスのリモートでコードが実行される脆弱性 https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2019-0708〔2020/6/10 確認〕
※ 93 Microsoft 社:CVE-2019-0708 のユーザー向けガイダンス ¦ リモート デスクトップ サービスのリモートでコードが実行される脆弱性：2019 年 5 月15日 https://support.microsoft.com/ja-jp/help/4500705/customer-guidance-for-cve-2019-0708〔2020/6/10 確認〕
※ 94 Microsoft 社：Microsoft works with researchers to detect and protect against new RDP exploits https://www.microsoft.com/security/blog/2019/11/07/the-new-cve-2019-0708-rdp-exploit-attacks-explained/〔2020/6/10 確認〕
※ 95 Comodo Security Solutions, Inc：Important Security Notice About Comodo Forums Accounts https://forums.comodo.com/general-announcements/important-security-notice-about-comodo-forums-accounts-t124921.0.html〔2020/6/10 確認〕
※ 96 株式会社ラック：【注意喚起】フォーラム構築ソフト「vBulletin」の深刻な脆弱性 (CVE-2019-16759) で攻撃通信の急増確認 https://www.lac.co.jp/lacwatch/alert/20190926_001937.html〔2020/6/10 確認〕
※ 97 WebARX：Critical Vulnerability In Ultimate Addons For Elementor & Ultimate Addons for Beaver Builder Plugins https://www.webarxsecurity.com/critical-vulnerability-in-ultimate-add-ons-elementor/〔2020/6/10 確認〕
※ 98 ステージング環境：運用（本番）環境と同等のシステム構成（ハードウェア、ソフトウェアとも）のテスト環境のこと。修正プログラム等の適用前に、適用による問題発生の有無を検証する環境。仮想化されたサーバ、ストレージ上に構築されることもある。
※ 99 トレンドマイクロ社：複数の脆弱性を利用してルータやデバイスを狙うボット型マルウェアの新亜種を確認 https://blog.trendmicro.co.jp/archives/22211〔2020/6/10 確認〕
※ 100 https://jvndb.jvn.jp/〔2020/6/10 確認〕
※ 101 IPA：【注意喚起】特定の組織からの注文連絡等を装ったばらまき型メールに注意 https://www.ipa.go.jp/security/topics/alert271009.html〔2020/6/10 確認〕
※ 102 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019年10月～12月］ https://www.ipa.go.jp/files/000080133.pdf〔2020/6/10 確認〕
IPA：OLE 機能を悪用した文書ファイルの手口に関する注意点 (第二版) https://www.ipa.go.jp/files/000080134.pdf〔2020/6/10 確認〕
※ 103 キヤノンマーケティングジャパン株式会社：MALWARE REPORT 2019 上 半 期 https://eset-info.canon-its.jp/files/user/malware_info/images/ranking/pdf/MalwareReport_2019FirstHalf.pdf〔2020/6/10 確認〕
※ 104 東京都：公益財団法人東京都保健医療公社が運用する端末等に対する不正アクセス被害の発生による、メールアドレス等の個人情報の流出と対応について（第二報） https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2019/06/07/06.html〔2020/6/10 確認〕
※ 105 トレンドマイクロ社：引き続き国内で拡大する「EMOTET」の脅威 https://blog.trendmicro.co.jp/archives/23648〔2020/6/10 確認〕
※ 106 JPCERT/CC：マルウエア Emotet の感染に関する注意喚起 https://www.jpcert.or.jp/at/2019/at190044.html〔2020/6/10 確認〕
※ 107-1 piyolog：国内で相次ぐ不審メールの注意喚起と返信型 Emotet についてまとめてみた https://piyolog.hatenadiary.jp/entry/2019/11/26/054443〔2020/6/10 確認〕
※ 107-2 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2018 年 10 月～ 12 月］ https://www.ipa.go.jp/files/000071273.pdf〔2020/6/10 確認〕
※ 108 JPCERT/CC：マルウエア Emotet の感染活動について https://www.jpcert.or.jp/newsflash/2019112701.html〔2020/6/10 確認〕
※ 109 ファイア・アイ株式会社：進化するマルウェア、EMOTET https://www.fireeye.jp/blog/jp-products-and-services/2019/12/evolving-malware-emotet.html〔2020/6/10 確認〕
※ 110 「編集を有効にする」ボタン：Microsoft Office の「保護ビュー」機能を有効にしている場合に、メールの添付ファイルやインターネット上のファイルを開くと表示されるボタン。
※ 111 キヤノンマーケティングジャパン株式会社：2019 年 10 月マルウェアレポート https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1910.html〔2020/6/10 確認〕
※ 112 サイバーリーズン・ジャパン株式会社:3 つの脅威:Emotet（エモテット）による TrickBot の展開と TrickBot によるデータの窃取および Ryuk の拡散 https://www.cybereason.co.jp/blog/cyberattack/3613/〔2020/6/10 確認〕
※ 113-1 ZDNet：Florida city fires IT employee after paying ransom demand last week https://www.zdnet.com/article/florida-city-fires-it-employee-after-paying-ransom-demand-last-week/〔2020/6/10 確認〕
※ 113-2 JPCERT/CC：マルウエア Emotet への対応 FAQ https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html〔2020/6/10 確認〕
※ 114 「情報セキュリティ白書 2018」の「1.3.4 ばらまき型メールによる攻撃」(p.34)を参照。
※ 115 JC3：インターネットバンキングマルウェア「DreamBot」による被害に注意 https://www.jc3.or.jp/topics/dreambot_cm.html〔2020/6/10 確認〕
JC3：インターネットバンキングの不正送金の被害に注意 https://www.jc3.or.jp/topics/dreambot.html〔2020/6/10 確認〕
※ 116 Proofpoint Inc.：Get2 ダウンローダーを使って新型の SDBbot リ

モートアクセス型トロイの木馬（RAT）を配信する TA505　https://www.proofpoint.com/jp/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader〔2020/6/10 確認〕
※ 117 JC3：運送系企業を装ったフィッシングの注意喚起　https://www.jc3.or.jp/topics/smsphishing.html〔2020/6/10 確認〕
JC3：不正アプリによる銀行を騙ったフィッシングサイトへの誘導　https://www.jc3.or.jp/topics/phishingsites.html〔2020/6/10 確認〕
※ 118 IPA：安心相談窓口だより　宅配便業者をかたる偽ショートメッセージに引き続き注意!　https://www.ipa.go.jp/security/anshin/mgdayori20200220.html〔2020/6/10 確認〕
※ 119 Gardia 株式会社：【お知らせ】運送会社や日本郵政を装った偽SMS（ショートメール）にご注意ください　https://gardia.jp/news/201909/sms/〔2020/6/10 確認〕
※ 120 朝日新聞：宅配業者装うSMSに注意　スマホ乗っ取られ詐欺に悪用　https://www.asahi.com/articles/ASM663JGXM66OIPE00G.html〔2020/6/10 確認〕
※ 121 JC3：新型コロナウイルスに乗じた犯罪　https://www.jc3.or.jp/topics/newmodel_coronavirus.html〔2020/6/10 確認〕
トレンドマイクロ株式会社：実例で見るネットの危険：「新型コロナウイルス」に便乗する攻撃メール　https://blog.trendmicro.co.jp/archives/23740〔2020/6/10 確認〕
※ 122 フィッシング対策協議会:ドコモをかたるフィッシング (2019/06/21)　https://www.antiphishing.jp/news/alert/docomo_20190621.html〔2020/6/10 確認〕
※ 123 独立行政法人国民生活センター：携帯電話会社をかたる偽 SMS にご注意!ーあなたのキャリア決済が狙われていますー　http://www.kokusen.go.jp/pdf/n-20190905_1.pdf〔2020/6/10 確認〕
JC3：通信事業者を騙るスミッシング詐欺の手法に係る注意喚起　https://www.jc3.or.jp/topics/smscert.html〔2020/6/10 確認〕
※ 124 フィッシング対策協議会：フィッシングレポート 2018　https://www.antiphishing.jp/report/pdf/phishing_report_2018.pdf〔2020/6/10 確認〕
フィッシング対策協議会：フィッシングレポート 2019　https://www.antiphishing.jp/report/pdf/phishing_report_2019.pdf〔2020/6/10 確認〕
※ 125 https://www.antiphishing.jp/report/pdf/phishing_report_2019.pdf〔2020/6/10 確認〕
※ 126 http://www.kokusen.go.jp/pdf/n-20190905_1.pdf〔2020/6/10 確認〕
※ 127 フィッシング対策協議会：月次報告書 2019/11 フィッシング報告状況　https://www.antiphishing.jp/report/monthly/201911.html〔2020/6/10 確認〕
※ 128 JC3：インターネットバンキングの不正送金の被害に注意　https://www.jc3.or.jp/topics/banking/phishing.html〔2020/6/10 確認〕
※ 129 フィッシング対策協議会：多くの金融機関をかたるフィッシング（2019/12/26）　https://www.antiphishing.jp/news/alert/phishbank_20191226.html〔2020/6/10 確認〕
※ 130 IPA：安心相談窓口だより　性的な映像をばらまくと恐喝し、仮想通貨で金銭を要求する迷惑メールに注意　https://www.ipa.go.jp/security/anshin/mgdayori20181010.html〔2020/6/10 確認〕
※ 131 セクストーション（性的脅迫）：スマートフォンの SNS アプリでのやり取り等で入手したプライベートな写真や動画をばらまくと脅して金銭を要求する脅迫。
※ 132 Microsoft 社：テクニカル サポート詐欺から身を守る　https://support.microsoft.com/ja-jp/help/4013405/windows-protect-from-tech-support-scams〔2020/6/10 確認〕
※ 133 IPA：安心相談窓口だより　スマートフォンで偽のセキュリティ警告からアプリのインストールへ誘導する手口に注意　https://www.ipa.go.jp/security/anshin/mgdayori20190918.html〔2020/6/10 確認〕
※ 134 自動継続課金：「一定の利用期間ごとに定額を支払う料金方式、且つ、利用契約が自動更新される」という意味で、当記事では用いている。なお、「一定の利用期間ごとに定額を支払う料金方式」は、Android では「定期購入」、iPhone では「サブスクリプション」と呼ばれる。
※ 135 McAfee, LLC：MoqHao Related Android Spyware Targeting Japan and Korea Found on Google Play　https://www.mcafee.com/blogs/other-blogs/mcafee-labs/moqhao-related-android-spyware-targeting-japan-and-korea-found-on-google-play/〔2020/6/10 確認〕
※ 136 ESET, spol. s r.o：Google Play にラジオアプリを偽装した新種のスパイウェアが侵入　https://www.eset.com/jp/blog/welivesecurity/first-spyware-android-ahmyth-google-play/〔2020/6/10 確認〕
※ 137 トレンドマイクロ株式会社：「App Store」と「Google Play」上で偽ギャンブルアプリが多数拡散　https://blog.trendmicro.co.jp/archives/22594〔2020/6/10 確認〕
※ 138 Google LLC：The App Defense Alliance: Bringing the security industry together to fight bad apps　https://security.googleblog.com/2019/11/the-app-defense-alliance-bringing.html〔2020/6/10 確認〕
※ 139 IPA：安心相談窓口だより　App Store 以外の配信アプリによるセクストーション被害を確認　https://www.ipa.go.jp/security/anshin/mgdayori20191224.html〔2020/6/10 確認〕
※ 140 Apple Inc.：Apple Developer Enterprise Program　https://developer.apple.com/jp/programs/enterprise/〔2020/6/10 確認〕
※ 141 東京 2020 オリンピック・パラリンピック競技大会のチケットの抽選結果を知らせるメールでも採用された。
公益財団法人東京オリンピック・パラリンピック競技大会組織委員会：観戦チケットに関する詐欺や模倣品の被害にご注意ください　https://tokyo2020.org/ja/news/notice-0006〔2020/6/10 確認〕
※ 142 https://www.tsr-net.co.jp/news/analysis/20200123_01.html〔2020/7/1 確認〕
※ 143 Security NEXT：登録者の個人情報 77 万件が流出 -「アンとケイト」　http://www.security-next.com/105209〔2020/7/1 確認〕
サイバーセキュリティ .com：不正アクセス被害の続報を発表、77 万件の顧客情報が流出｜アンとケイト　https://cybersecurity-jp.com/news/31442〔2020/7/1 確認〕
株式会社マーケティングアプリケーションズ：「アンとケイト」及び「ポケットアンとケイト」不正アクセスによるお客様情報流出に関するお詫びとご報告　https://www.ann-kate.jp/incident_reports/20190628/report3.html〔2020/7/1 確認〕
※ 144 Security NEXT：カードゲーム通販サイトで情報流出 - 旧サーバに不正アクセスか　http://www.security-next.com/112734〔2020/7/1 確認〕
サイバーセキュリティ .com：脆弱性悪用されサイト登録者情報 6 万 3 千件超流出か｜株式会社ホビーズファクトリー　https://cyberhoken-jp.com/news-235/〔2020/7/1 確認〕
株式会社ホビーズファクトリー：個人情報漏洩に関するお詫びとご報告　https://mtg.bigweb.co.jp/informations/press-release202002〔2020/7/1 確認〕
※ 145 Security NEXT：通販サイトに不正アクセス、個人情報流出の可能性 - 現代ギター社　http://www.security-next.com/111316〔2020/7/1 確認〕
サイバーセキュリティ .com：不正アクセスによりカード情報 133 件・顧客情報約2万件が流出か｜株式会社現代ギター社　https://cybersecurity-jp.com/news/34770〔2020/7/1 確認〕
株式会社現代ギター社：弊社が運営する「GG インターネットショップ」への不正アクセスによる個人情報流出に関するお詫びとお知らせ　https://info.gendaiguitar.com/owabi20200107.html〔2020/7/1 確認〕
※ 146 Security NEXT：「Emotet」に感染、メアド流出の可能性 - 関電グループ会社　http://www.security-next.com/112956〔2020/7/1 確認〕
ScanNetSecurity：Emotet 感染でメールアドレス約400件流出（関電アメニックス）　https://scan.netsecurity.ne.jp/article/2020/03/10/43798.html〔2020/7/1 確認〕
株式会社関電アメニックス：当社パソコンからの個人情報の流出の可能性について　https://www.k-amenix.co.jp/datas/news/pdf/020200306173217_JdXaU.pdf〔2020/7/1 確認〕
※ 147 朝日新聞デジタル：【独自】三菱電機にサイバー攻撃　防衛などの情報流出か　https://www.asahi.com/articles/ASN1M6VDSN1MULFA009.html〔2020/7/1 確認〕
朝日新聞デジタル：三菱電機へ高度なサイバー攻撃、中国政府の動きと呼応?　https://www.asahi.com/articles/ASN1X4JXHN1RULZU002.html〔2020/7/1 確認〕
三菱電機株式会社：不正アクセスによる個人情報と企業機密の流出の可能性について（第３報）　https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf〔2020/7/1 確認〕
ITmedia：三菱電機、約 8000 人の個人情報流出か　ウイルス対策システムにゼロデイ攻撃　https://www.itmedia.co.jp/news/articles/2001/21/news083.html〔2020/7/1 確認〕
※ 148 サイバーセキュリティ .com：不正アクセス被害で個人情報最大 3 万 1,231 件に流出の可能性｜エーデルワイン　https://cybersecurity-jp.com/news/31106〔2020/7/1 確認〕
株式会社エーデルワイン：弊社が運営する「エーデルワイン オンラインショップ」への不正アクセスによる個人情報流出に関するお詫びとお知らせ　https://edelwein.co.jp/1079〔2020/7/1 確認〕
※ 149 サイバーセキュリティ .com：ユニクロ・GU へ大規模なリスト型攻撃発生、顧客情報 46 万件超が流出か　https://cybersecurity-jp.com/news/31257〔2020/7/1 確認〕
株式会社ファーストリテイリング、株式会社ユニクロ、株式会社ジーユー:「リスト型アカウントハッキング（リスト型攻撃）」による弊社オンラインストアサイトへの不正ログインの発生とパスワード変更のお願いについて　https://

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

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

第2章
情報セキュリティを支える基盤の動向

2019 年度は、国内外で重要インフラやサプライチェーンのセキュリティ、個人情報保護に関する規則等の運用が本格的に展開された年であった。国内では、「サイバー・フィジカル・セキュリティ対策フレームワーク」の発行等、今後のセキュリティ対策に関わりが深いと思われる取り組みが行われた。またクラウドセキュリティ評価制度やサイバーセキュリティお助け隊等、政府や中小企業等の対策強化も進められた。国外では、米国の政府調達等における規制強化、欧州の GDPR 違反摘発の本格化と他国にも大きく影響を及ぼす政策が動き出した。

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。

本項では、2018 年 7 月に見直されたサイバーセキュリティ戦略と 2019 年度に実施された主な取り組みについて述べる。

(1)「サイバーセキュリティ戦略」の見直し

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（以下、2015 年戦略）が閣議決定され、2018 年 7 月に 2 回目となる新たな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（図 2-1-1）。

2015 年戦略の策定以降、サイバー空間とフィジカル（実）空間の統合化がより進んだことで、社会に豊かさがもたらされる可能性が高まる一方、サイバー攻撃によってフィジカル空間における多大な経済的・社会的損失のリスクが深刻化することが懸念されている。

そこで 2018 年戦略では、サイバーセキュリティ基本法の目的や、2015 年戦略の基本的な理念及び基本原則を堅持しつつ、経済社会が自律的・持続的に進化・発展していくために、以下の三つの観点から官民での取り組みを推進することが示されている。

- サービス提供者の任務保証

  任務保証とは、企業や政府機関を含むあらゆる組織において、自ら遂行すべき業務やサービスを「任務」ととらえ、これを着実に遂行するために必要な能力及び資産を確保することを指す。その際、責任を有する者（経営層や幹部）が主体となり、「任務」とする業務やサービスを選定し、安全かつ持続的な提供に関する責任を全うすることが重要である。
- リスクマネジメント

  各組織の「任務」の内容に応じて、リスクを特定・分析・評価し、リスクを許容し得る程度にまで低減する対応を指す。これは組織を指揮統制することで、組織の資源を適切に分配し、リスクに対応していく一連の活動全体を指す。

- 参加・連携・協働

  個人または組織が、サイバー空間の脅威から発生し得る被害やその拡大を防止するために平素から講じる基本的な取り組みを指す。セキュリティ脅威が日常化し、サイバー空間で活動する主体は個人・組織にかかわらず誰もが脅威に晒される可能性がある中、個々の努力による取り組みでは対応が困難であり、他者との協働が必要となる。個人や組織各々が常に情報共有を行い、連携・協働することを、サイバー空間における新たな公衆衛生活動ととらえる必要がある。

また、2018年戦略の目的達成の施策として、「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社会の実現」「国際社会の平和・安定及び我が国の安全保障への寄与」「横断的施策」の四つの観点が示されている。これらに関して2019年度に実行された施策について、次項で述べる。

(2)「サイバーセキュリティ2019」の主な取り組み状況

「サイバーセキュリティ2019[※2]」は、2018年戦略に基づく初めての年次報告とそれを反映した2019年度の年次計画を統合したもので、関連府省庁はこれに基づき施策を実施する。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2019で計画し実施された取り組みについて述べる。

- 経済社会の活力の向上及び持続的発展

  経済産業省は、第2期のCGS研究会[※3](コーポレート・ガバナンス・システム研究会)での議論を踏まえ、2019年6月に、グループ経営を行う上場企業を主な対象として、グループ全体の価値向上を図るためのガバナンスの在り方を示す「グループ・ガバナンス・システムに関する実務指針[※4]」を公開した(グループ・ガバナンス・システムに関する実務指針については、「2.1.2(1)(b)WG2(経営・人材・国際)」参照)。

  総務省は、サイバーセキュリティタスクフォース[※6]のもとに設置した情報開示分科会での検討を踏まえ、企

■図2-1-1 サイバーセキュリティ戦略の概要
(出典)NISC「サイバーセキュリティ戦略・サイバーセキュリティ2019の概要[※5]」

業がセキュリティ対策について積極的な情報開示を行い社会的な企業価値を向上させること等を目的とした「サイバーセキュリティ対策情報開示の手引き※7」を策定し、2019年6月に公開した（情報開示分科会での検討については「2.1.3（1）（d）民間企業等におけるセキュリティ対策の促進」参照）。

また経済産業省とIPAは、サイバーセキュリティの政策・課題に関する官民の情報共有や企業同士の連携を図るため、メンバーを限定しない情報交流の場「コラボレーション・プラットフォーム※8」を開催した（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」）。

サイバー空間とフィジカル空間を跨いだ新たな形のサプライチェーンのセキュリティに関しては、経済産業省が、全産業にほぼ共通して必要なセキュリティリスク管理の枠組みである「サイバー・フィジカル・セキュリティ対策フレームワークVersion 1.0※9」を2019年4月に策定した。また産業活動への本フレームワークの実装を促進するべく、三つのタスクフォースを設置し、議論を行った（本フレームワークについては「2.1.2（1）（a）WG1（制度・技術・標準化）」参照）。

- 国民が安全で安心して暮らせる社会の実現

  総務省と経済産業省は、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、信頼性確保の観点から同サービスの安全性評価について、2018年8月に「クラウドサービスの安全性評価に関する検討会」を立ち上げて検討を進めた。検討会での検討成果はパブリックコメントを経て、2020年1月に「クラウドサービスの安全評価に関する検討会 とりまとめ※10」として公開された（「2.1.2（2）政府情報システムのためのセキュリティ評価制度（ISMAP）」参照）。

  内閣官房は、2020年に開催が予定されていた東京2020オリンピック・パラリンピック競技大会に向けて、リスクマネジメントの促進と対処態勢の整備を実施した※11。まず、リスクマネジメントの促進については、同大会の開催・運営に影響を与え得る重要サービス事業者を選定してリスクアセスメントの実施を依頼し、その結果から経営資源、リスク源等の洗い出しの漏れの可能性についてフィードバックを行った。また、同大会会場で提供されるサービスの重要度に応じて事業者を選定し、サイバーセキュリティ対策の実施状況を検証する横断的リスク評価の第2回の取り組みを2019年2月から9月まで実施した。

  次に、対処態勢の整備については、2019年4月に構築した「サイバーセキュリティ対処調整センター※12」を大会までの大規模イベント（G20大阪サミット等関係閣僚会合、ラグビーワールドカップ等）において運用し、当該イベントに連絡要員を派遣するとともに、サイバーセキュリティ対処調整センターによる関係組織・機関への迅速な情報提供を実施した。

- 国際社会の平和・安定及び我が国の安全保障への寄与

  経済産業省及びIPAは、米国政府と連携し、インド太平洋地域※13から招聘した受講生と、IPA産業サイバーセキュリティセンターの中核人材育成プログラム※14の受講生を対象に、日米の専門家による制御システムのセキュリティに関する「インド太平洋地域向け日米サイバー演習※15」を実施した（同演習については「2.3.2 産業サイバーセキュリティセンター」参照）。また、関連府省庁は、ASEAN加盟国とサイバーセキュリティに関する協議を実施した（「2.2.1（5）ASEANとのサイバー連携」参照）。

- 横断的施策

  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※16の育成を目的に2018年度に実施した「戦略マネジメントセミナー」について、受講生のアンケート結果等からカリキュラムを見直し、「セキュリティ組織管理」コース及び「セキュリティ実務管理」コースの2コースを設置してトレーニングを実施した（「2.3.2（2）（d）戦略マネジメント系セミナー」参照）。

  総務省は、国立研究開発法人情報通信研究機構（NICT：National Institute of Information and Communications Technology）を通じて、サイバー攻撃に悪用される恐れのあるIoT機器を調査し、インターネットサービスプロバイダ（ISP：Internet Service Provider）を通じた利用者への注意喚起を行う取り組み「NOTICE※17」を2019年2月から実施している。2019年度は上記の取り組みに加えて、マルウェアに感染しているIoT機器をNICTの「NICTER※18」プロジェクトで得た情報を基に特定し、ISPから利用者へ注意喚起を行う取り組みを2019年6月から開始した（NOTICEについては「2.1.3 総務省の政策」「3.2.2（1）国内における実態」参照）。

（3）重要インフラの情報セキュリティ対策強化

我が国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※19」（以下、第 4 次行動計画）を決定した。続いて 2018 年 7 月、新たな重要インフラ分野として「空港」分野を追加する形で同計画を改定した※20。

また、各重要インフラ分野に共通して求められる情報セキュリティ対策の実施を訴求するため、2018 年 4 月に、サイバーセキュリティ戦略本部が「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）※21」を、重要インフラ専門調査会が「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第 1 版）※22」を発行した。以下、2019 年度における主な活動について述べる。

(a)「重要インフラの情報セキュリティに係る第 4 次行動計画」に基づく情報共有の手引書

重要インフラ専門調査会では、第 4 次行動計画に基づく情報共有体制の改善について審議を行い、第 4 次行動計画及び実施細目※23 の内容を取りまとめ、解説を加えた手引書を策定することとした。

同調査会はこれに基づき、2019 年 10 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』に基づく情報共有の手引書（試行版）※24」（以下、試行版）を策定した。2019 年 11 月に実施された後述の「分野横断的演習」において、同演習参加者（事業者）は試行版を参照し、情報連絡様式を実際に用いて情報連絡を実施した。事業者等から内容の修正を要するコメントはなかったため、同調査会は 2020 年 3 月を目途に正式版として制定するとしている。

(b)「分野横断的演習」の実施

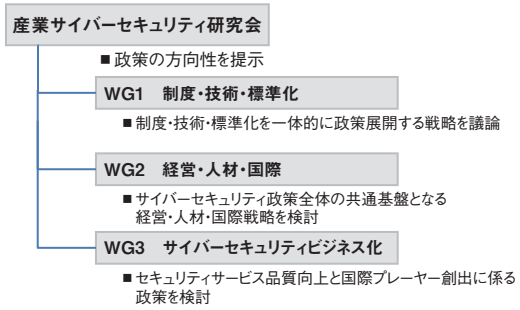
NISC は、重要インフラ事業者の事業継続計画や官民・分野横断的な情報共有体制に関する検証及び課題の抽出を行うことにより、障害対応体制の強化を図ることを目的とした分野横断的演習を 2019 年 11 月に実施した※25。重要インフラ 14 分野を対象に、重要インフラ事業者や所管省庁、情報セキュリティ関係機関等から、過去最大となる 4,967 名（717 組織）が参加した。同演習では東京 2020 オリンピック・パラリンピック競技大会開催期間中を想定した演習シナリオのもと、重要インフラ事業者等は事業継続計画等に基づいて、状況整理、所管省庁への情報連絡、対応方針検討、関係機関、他事業者等との情報共有等を実施した。

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※26。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※27」を基に IPA が編集

また、同研究会では 2018 年 5 月に発表した「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※28」を中心とした取り組みを更に加速して行くために、以下の三つの視点から重点施策を強化するとしている※29。

- 「グローバル」をリードする
- 「信頼の価値」を創出する
- 「中小企業・地域」まで展開する

各 WG の概要と活動状況は以下のとおりである。

(a) WG1（制度・技術・標準化）

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（The Cyber/

Physical Security Framework）Version 1.0」（以下、CPSF）を2019年4月に策定した※9。

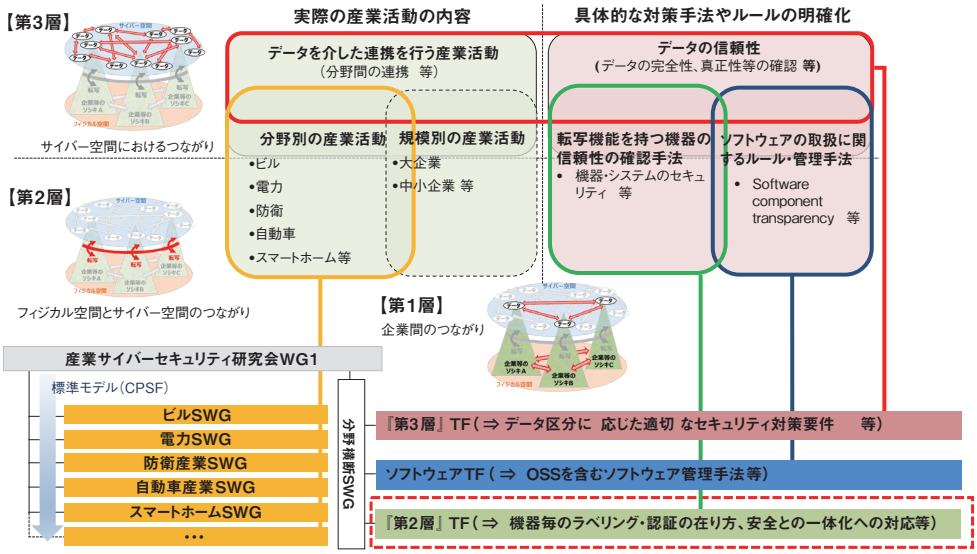
CPSFでは、産業社会を三つの層で整理した「3層構造モデル」ととらえることでセキュリティ確保のための信頼性の基点を明確化するとともに、バリュークリエイションプロセスに関与する、セキュリティ対策を講じる最小単位となる「六つの構成要素」を提示している。これらに基づいて、リスク源を洗い出し、その対策要件※30を特定できるとしている（リスクベースアプローチ）。

- 3層構造モデル
  第1層－企業間のつながり
  第2層－フィジカル空間とサイバー空間のつながり
  第3層－サイバー空間におけるつながり
- 六つの構成要素
  ソシキ:バリュークリエイションプロセスに参加する企業・団体・組織
  ヒト：ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人
  モノ:ハードウェア、ソフトウェア、及びそれらの部品（操作する機器を含む）
  データ:フィジカル空間にて収集された情報、及び共有・分析・シミュレーションを通じて加工された情報
  プロシージャ：定義された目的を達成するための一連の活動の手続き
  システム：目的を実現するためにモノで構成される仕組み・インフラ

3層構造モデルにおいて、第1層では企業ごとのマネジメントを中心にセキュリティ対策が実施される。一方第2層では、バリュークリエイションプロセスに直接関与する企業だけでなく、当該企業の転写※31機能を担うシステムの提供・運用を行う企業の協力が不可欠となる。また第3層では、データの流通に間接的に関与する企業も、セキュリティ確保のために一定の役割を果たすことが求められる。このように第2層、及び第3層では、マルチステークホルダによるセキュリティ対策への取り組みが重要となる。

WG1では2019年度、CPSFの実装を促進するべく、第2層及び第3層に焦点を絞り検討する各層別のタスクフォースや、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タスクフォースを設置し、議論を進めてきた（図2-1-3）。第2層タスクフォースでは、サイバー空間・フィジカル空間の転写機能を持つ機器等について、自己適合宣言・認証等の確認の在り方等を検討するとともに、産業保安・製品安全も考慮したセキュリティ対策の在り方について検討を進めている※32。第3層タスクフォースでは、データの信頼性確保のために、データの区分に応じた適切なセキュリティ対策要件及びデータの信頼性の確認手法について検討を進めている※33。ソフトウェアタスクフォースでは、ソフトウェア管理手法、脆弱性対応、OSSの利活用等について検討を進めている※34-1。

また、WG1ではCPSFを参考にしつつ、各産業分



■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※32」

野の特性に応じたセキュリティ対策の検討を進めるべく、五つの産業分野別サブワーキング（SWG）を設置している（図 2-1-3）。この中で、ビル SWG では、ビルシステムに関係する各種のサイバー攻撃のリスクと、それに対するサイバーセキュリティ対策を整理し、2019 年 6 月 17 日「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※34-2」を公表した。更に、自動車 SWG では自動車産業向けガイドラインを 2020 年 5 月 28 日に公表すべく準備を進めており、スマートホーム SWG でもガイドライン原案を作成し、公表に向けた準備を進めている。

（b）WG2（経営・人材・国際）

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、CGS 研究会（コーポレート・ガバナンス・システム研究会）（第 2 期）は 2019 年 6 月に、グループ経営を行う上場企業を主な対象として、グループ全体の価値向上を図るためのガバナンスの在り方を示す「グループ・ガバナンス・システムに関する実務指針※4」を公開した。本指針では、サイバーセキュリティを内部統制システム上の重要なリスク項目としてとらえ、親会社の取締役会レベルでグループ全体やサプライチェーンを考慮に入れたサイバーセキュリティ対策を行うことを検討すべきと明記されている。更に WG2 は、経営層に対して、自社のサイバーセキュリティ対策が「サイバーセキュリティ経営ガイドライン※35」に関してどの程度実践できているかを確認するための可視化ツールβ版を策定し、公開した※36（可視化ツールについては「2.4.1（2）（e）セキュリティ対策実践状況可視化ツール」参照）。

中小企業・地域への展開に関しては、IPA を通じて全国 8 地域において、地域の事業者団体、セキュリティ企業、保険会社がコンソーシアムを組み、中小企業向けのセキュリティ対策支援の仕組みの構築を目的とした「サイバーセキュリティお助け隊※37」の実証事業を実施した（サイバーセキュリティお助け隊については、「2.4.2（2）（a）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」参照）。

人材に関しては、WG2 は企業に求められるセキュリティ機能を遂行する人材の活用の進め方を「セキュリティ人材活用モデル」として整理したほか、ユーザ企業内のセキュリティ体制の整理等を実施した（「2.3.1（2）経済産業省の取り組み」参照）。関連して、戦略マネジメント層※38の育成に関する取り組みとして、IPA の産業サイバーセキュリティセンターで 2018 年度に開設した「戦略マネジメント系セミナー」を改変し、「セキュリティ組織管理」コース及び「セキュリティ実務管理」コースの 2 コースを開講して 2020 年 1 月に実施した（「2.3.2（2）（d）戦略マネジメント系セミナー」参照）。他にも、国立高等専門学校におけるセキュリティ教育が産業界の要請と整合していくために、独立行政法人国立高等専門学校機構と経済産業省、IPA 及び業界団体が連携し、高等専門学校生の専攻に応じた教育コンテンツの提供や講師の派遣等が推進された。

国際連携活動としては、IPA を通じて、2019 年 9 月 9～12 日に「インド太平洋地域向け日米サイバー演習※15」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と CPSF を軸とした議論を行い、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※39。

（c）WG3（サイバーセキュリティビジネス化）

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ー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による、国内セキュリティビジネスの競争力創出等の議論を行った※40。

検証基盤の整備については、IPA を通じて、「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※41」を 2019 年 9 月に設置し、本有識者会議の指導のもと、検証基盤の課題やあるべき姿を抽出することを目的に、セキュリティ製品を検証し、結果を公表する「試行検証」を実施した※42。

また WG3 は 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、2019 年度も継続した※8。ここでは参加資格を限定せず、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。2019 年度は 6 回実施し、計 567 人が参加した。

（2）政府情報システムのためのセキュリティ評価制度（ISMAP）

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※43」では、「クラウド・バイ・デフォルト原則」が掲げられた。一方で、クラウドサービスプロバイダに要求する統一的なセキュリティ要求基準は存在せず、各政府機関等が調達の際に、個別のプロバイダのセキュリティ対策を確認し調達を行っている。こうした現状を踏まえ、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※44」を発足させた。

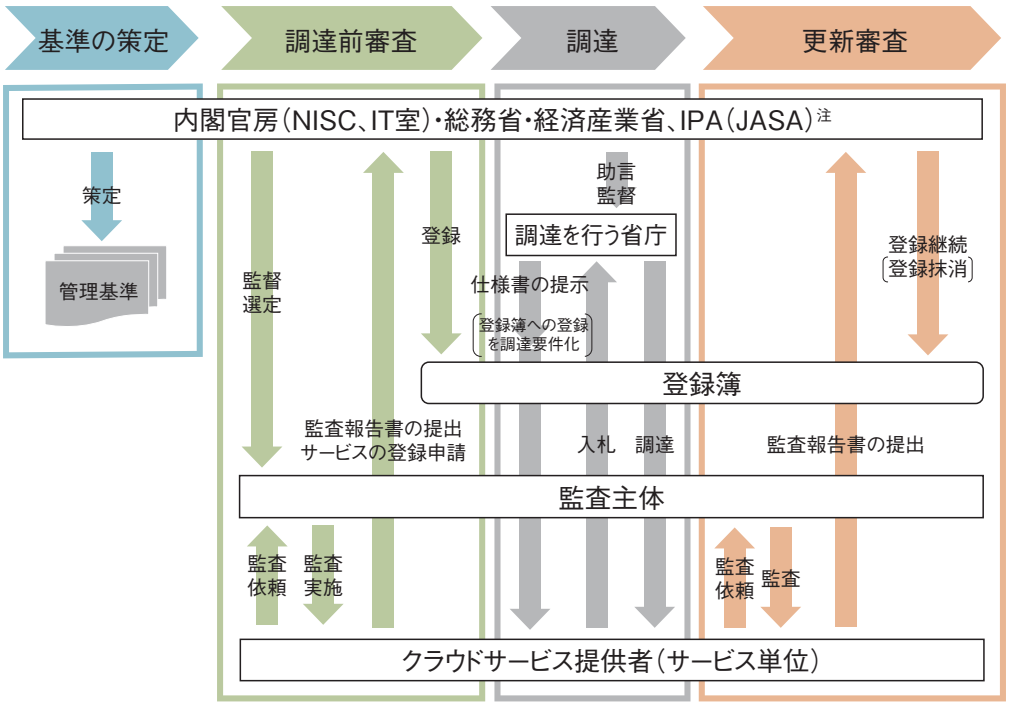
本検討会では、日本経済再生本部による「未来投資戦略2018※45」を踏まえ、クラウドサービスに関する既存のガイドラインや国内外の認証制度、監査制度等を整理するとともに、適切なセキュリティを満たすクラウドサービスを導入するために必要な評価方法等を検討し、2020年1月に「クラウドサービスの安全性評価に関する検討会とりまとめ※46」(以下、検討会取りまとめ)が公開された。また、同月のサイバーセキュリティ戦略本部会合において「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて※47」が決定された。

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・運用の基準を定めることとした。その上で、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を、本制度が公表するクラウドサービスリストに登録することとした。

また、本制度における監査を行うことができる監査機関は、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され、本制度が公表する監査機関リストに登録されるものとした。以上の制度のフローを図2-1-4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、所管政府機関に申請の上、登録簿にのせてもらう。省庁の調達者は登録簿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登録簿管理を行う。

従来、政府調達に当たっては、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、この確認負荷が省略できるとともに、本制度が要求する情報セキュリティ対策基準を満たすことが確認されたクラウドサービスを効率的に調達することができる。

2020年3月27日、経済産業省・内閣官房・総務省は上記の制度を「政府情報システムのためのセキュリティ評価制度(ISMAP:Information system Security Management and Assessment Program)」と称して各種基準(案)を公開、4月26日まで意見募集を実施した※49。



(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2-1-4　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※48」

ISMAPに関する規則、基準等は、以下のとおりである。

- ISMAP基本規程
- ISMAP運営規則
- ISMAPクラウドサービス登録規則
- ISMAP管理基準
- ISMAP監査機関登録規則
- 情報セキュリティ監査基準（既存文書）
- ISMAP情報セキュリティ監査ガイドライン
- ISMAP標準監査手続（別添非公開）

クラウドサービス事業者が遵守すべき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）※50」「NIST SP800-53 rev.4」を参照して作成されている。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）を参考としている。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）」を参考とし、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）を参考としている。

監査については、経済産業省がまとめた「情報セキュリティ監査基準（Ver1.0）※51」を監査基準とするとともに、ISMAPで定めた「ISMAP標準監査手続」（非公開）及び「ISMAP情報セキュリティ監査ガイドライン※52」に基づいて監査することとしている。

ISMAPの所管はNISC、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に置かれる。またISMAPの実施時期については、2019年12月の「デジタルガバメント実行計画※53」において、「2020年度（令和2年度）内に、全政府機関において（中略）利用の開始」が目標として掲げられていたが、2020年6月3日、ISMAPの運用開始が正式に発表され※54、運用実務はIPAが担当することとなった※55。

なお、ISMAPで公開される情報等については、重要産業分野等を始めとする民間においても参照することで、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、重要インフラにおけるクラウドサービスの利用について、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）※56」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。」と位置付けられている。

検討会取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、情報システム全体について、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。

(3) AI・データの利用に関する契約ガイドライン

契約におけるデータの利用権限を公平に取り決めるための考え方を示すため、経済産業省は、2017年5月に「データの利用権限に関する契約ガイドライン ver1.0※57」を公開した。一方で、IoTやAI技術の急速な進展に伴い、新たなデータの取り扱いや利活用の方法が現れてきている。そこで、データ契約の類型別整理やユースケースの充実等を図るとともに、新たにAIの開発・利用に関する契約実務等の考え方を追加した「AI・データの利用に関する契約ガイドライン※58」を2018年6月に策定した。

経済産業省は公開した本ガイドラインの内容を継続的に評価し、利便性を向上させるため2018年12月より「AI・データ契約ガイドライン検討会作業部会」を開催し、今後の課題や実務のニーズ等について検討を行った。検討においては、2018年の不正競法防止法改正※59（2019年7月施行）で盛り込まれた「限定提供データ」の不正取得等に関する民事措置や、2019年1月に公表された「限定提供データに関する指針※60」への対応が議論され、その成果として、本ガイドライン（データ編）をアップデートした「AI・データの利用に関する契約ガイドライン1.1版」を2019年12月に公開した※61。

(4) 産業競争力強化法等の一部改正

2018年5月、「産業競争力強化法等の一部を改正する法律」が成立し、同年7月に施行された※62。本法律には複数の法律における改正内容が含まれている。

セキュリティに関する事項として、産業競争力強化法の一部改正に基づき、同年9月から「技術等情報管理認証制度※63」が開始された。これは、企業の技術情

報等の管理について、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、2020年2月現在3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いる。更に、自社の情報管理状況を把握できる「セルフチェックシート」の一部（全事業者共通の必須事項のみ）を2019年12月に先行公開している。

(5) 情報セキュリティサービス基準適合サービス

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「セキュリティサービス認定検討会」を開催し、「情報セキュリティサービス基準」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※64。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※65による審査の結果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掲載した「情報セキュリティサービス基準適合サービスリスト」を公開している※66。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が2020年7月時点で192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は、「政府機関等の対策基準策定のためのガイドライン」から参照されている。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、前述の「ISMAP監査機関登録規則」において、監査機関登録の申請者への要求事項の一つとなっている。

今後、本サービスリストの活用が進むことで、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。

(6) 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。2020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262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※67）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2-1-5）。

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、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）等とも連携している。

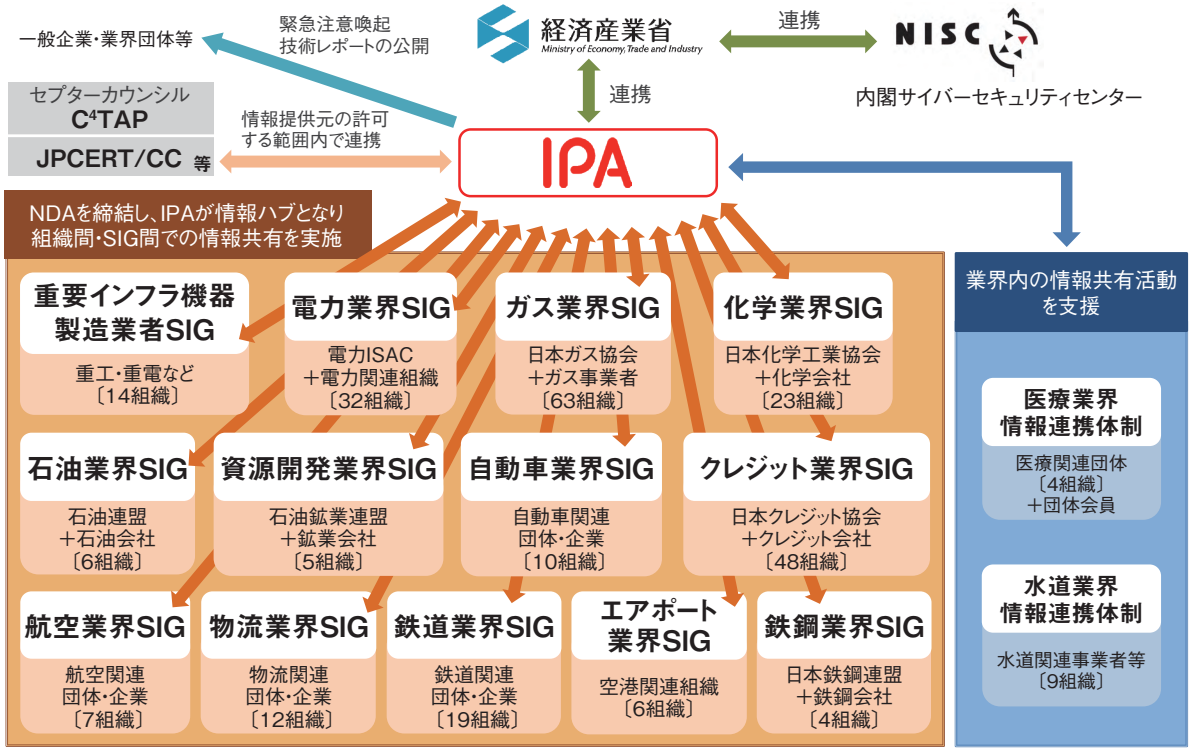
J-CSIPでは、IPAと参加組織との間でサイバー攻撃に関する手口や被害の情報、標的型攻撃メール等に関する情報共有を行っている。なお、J-CSIPの中で共有される情報は、提供元が明らかにならないよう、情報提供者の固有の情報を除去するルールがある。

参加組織からの情報提供件数、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。時期により件数の上下はあるものの、継続して情報提供や共有が行われていることが分かる。

2019年度は、2018年度までと同様、ビジネスメール

	2016年度	2017年度	2018年度	2019年度
参加組織からの情報提供件数	2,505件	3,456件	2,020件	2,303件
攻撃メール件数	177件	274件	213件	401件
情報共有件数	96件	242件	195件	225件

■表2-1-1　J-CSIPの運用実績



■図 2-1-5　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［2020 年 1 月～ 3 月］※68」

詐欺の事例に関する情報提供が多く寄せられた。偽のメールを駆使し、金銭の詐取を試みるという点は従来の事例と変わらないが、新たな騙しの手口が確認されている（「1.2.2 ビジネスメール詐欺（BEC）」参照）。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。

2019 年 8 月には、ある国内組織を詐称し、複数の別の国内組織に対して送信されたと思われる、Office 365 のアカウント情報を狙う日本語のフィッシングメールを確認した※69。Office 365 のアカウント情報が詐取され、不正アクセスされると、場合により企業秘密を含むメールやファイルが窃取される可能性がある。これらは攻撃者にとって魅力的な情報と考えられ、注意が必要である。

J-CSIP において、2017 年から「プラント関連事業者を狙う一連の攻撃」と呼んでいるウイルス※70 メールについて継続的に情報共有・分析を行ってきたところ、2019 年 11 月、IPA としては初めて、この攻撃者が日本語のウイルスメールを送信してきたことを確認した※71。この一連の攻撃は、プラント等の設備や部品のサプライヤに対し、実在しそうな開発プロジェクト名や事業者名を詐称し、プラントに使用する資機材の提案や見積もり等を依頼する内容の偽のメールを送り付け、添付ファイル（ウイルス）を開かせようとするものである。この偽メールでは、国内の実在する火力発電所に関するプロジェクトの提案依頼を装っていた。攻撃者の目的が、知財の窃取（産業スパイ）であるのか、あるいはビジネスメール詐欺のような詐欺行為の準備段階の情報窃取であるのかは不明であるが、引き続き注意が必要である。

2015 年 10 月ごろから国内で多く観測されるようになった「日本語のばらまき型メール」が 2019 年度も多く発生した。特に 2019 年 10 月以降、「Emotet」と呼ばれるウイルスに感染させることを目的とした日本語の攻撃メールが国内にばらまかれ、IPA への情報提供も増加した（「1.2.5（1）Emotet への感染を狙ったばらまき型メール」参照）。標的型攻撃とは異なり、広い範囲へ攻撃メールが着信することから、メールの配送経路やセキュリティソフトで検知・停止できる場合も多いと思われる。一方で、一部はそれらをすり抜けて、企業等の職員の手元まで着信しているという報告もある。日本は確実に攻撃の対象となっており、このような日本語のばらまき型メールは、2020 年以降も継続して発生すると思われる。

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、日本の組織を直接攻撃するのではなく、海外の拠点を先に攻撃するといった事例も公開されている※72（「1.2.1 (1) (a) 国内組織の中国現地法人を狙った標的型攻撃」参照）。攻撃手口が巧妙化している中、情報共有活動は、防御側における対抗策の一つであり、IPA は引き続き J-CSIP の運用を継続していく。

(7) 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

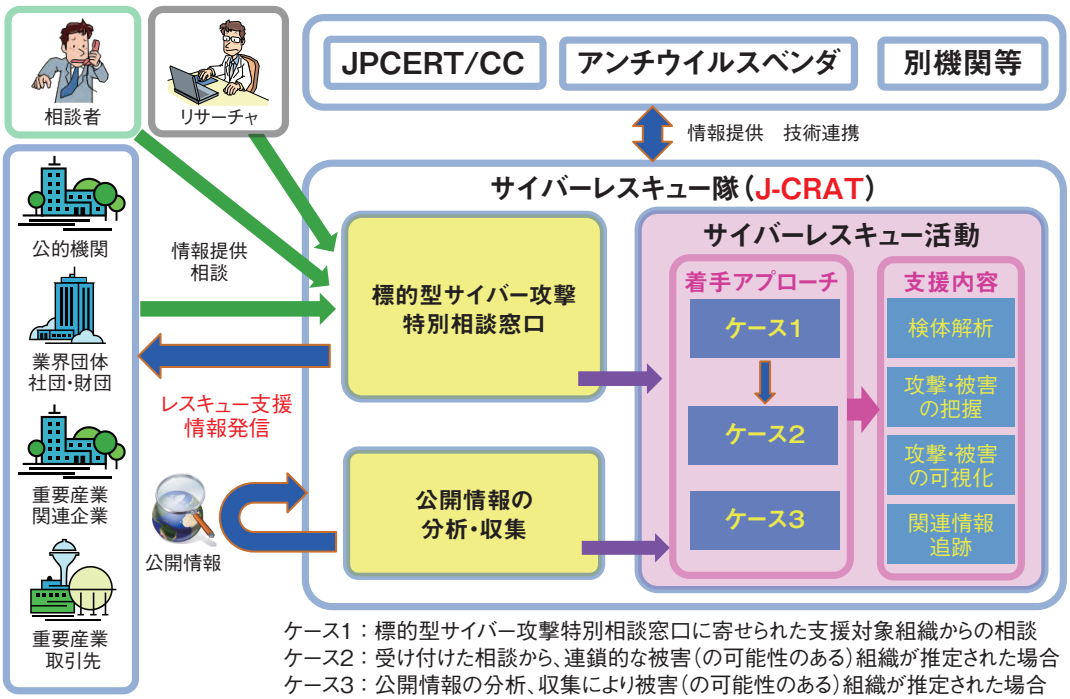
J-CRAT では、常時「標的型サイバー攻撃特別相談窓口」（以下、窓口）の運営と「公開情報の分析・収集」の二つの活動を実施している。

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※73。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（図 2-1-6）。

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 に示す。2019 年度の活動実績を 2018 年度と比較すると、「相談件数」は 5.1% 減少しており、内訳を見ると「レスキュー支援件数」が 9.4% 増加している一方、「オンサイト支援件数」は 35.5% 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



■図 2-1-6　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）※74」

	2016 年度	2017 年度	2018 年度	2019 年度
相談件数	519 件	412 件	413 件	392 件
レスキュー支援件数	123 件	144 件	127 件	139 件
オンサイト支援件数※	17 件	27 件	31 件	20 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

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。

2.1.3 総務省の政策

総務省は、IoT・AI 時代に対応したサイバーセキュリティ体制の早期確立を目指して 2017 年 1 月に「サイバーセキュリティタスクフォース」を発足させた※75。

サイバーセキュリティタスクフォースでは、IoT・5G の時代にふさわしいサイバーセキュリティ政策の在り方について検討し、2019 年 8 月に「IoT・5G セキュリティ総合対策※76」(以下、総合対策)を策定・公表した。

総合対策においては、その内容等について、「定期的に検証を行い、進捗状況を把握するとともに、本分野における技術革新や最新のサイバー攻撃の態様を踏まえ、必要に応じて随時見直しを行っていく」としており、総合対策の進捗状況と今後の取り組みの方向性を整理し、「IoT・5G セキュリティ総合対策プログレスレポート 2020」を公表している※77。

以下では本レポートに基づき、総務省の主な取り組みの状況を述べる。

(1)「IoT・5G セキュリティ総合対策」に基づく主な取り組み

総務省は、総合対策に基づき、脆弱性対策に関わる体制の整備、5G のセキュリティ対策、研究開発の推進、民間企業等におけるセキュリティ対策の推進、人材育成の強化等について取り組みを推進している。

(a) 脆弱性対策に関わる体制の整備に向けた主な取り組み

脆弱性のある機器を減らすための対策と端末設備の機能強化に向けた技術基準について述べる。

- 脆弱な IoT 機器の調査の実施

  IoT 機器に対するサイバー攻撃の脅威等に対応するため、2018 年 5 月、「国立研究開発法人情報通信研究機構法」及び「電気通信事業法」が改正された※78。同改正により、NICT の業務に、パスワード設定等に不備のある IoT 機器の調査等が追加された。

  これを受けて 2019 年 2 月 20 日、NICT は、パスワード設定等に不備のある IoT 機器を調査し、電気通信事業者を通じて利用者等へ注意喚起を行うプロジェクト「NOTICE※79」を開始した※80。また、2019 年 6 月からは、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、既にマルウェアに感染している IoT 機器の利用者に対し、ISP が注意喚起を行う取り組みを実施している※81。2020 年 3 月時点で、これらの注意喚起の取り組みに対して、50 社の ISP が参加しており、当該 ISP を利用している約 1.1 億 IP アドレスを対象に調査を実施している。このうち ID・パスワードが入力可能であったものが約 10 万件であり、更に、容易に推測可能な ID・パスワードによりログインでき、注意喚起の対象となったものは延べ 2,249 件であった（「3.2.2 (1) 国内における実態」参照）。

- IoT 機器のセキュリティ対策に関する技術基準の改正

  IoT 機器を含む端末設備のセキュリティ対策に関する技術基準の整備等を行うことを目的として、端末設備等規則が一部改正され、2020 年 4 月に施行された※82。この改正により、電気通信回線設備を介してインターネットに接続し、電気通信の送受信に関わる機能を操作することが可能な端末設備について、最低限のセキュリティ対策として、アクセス制御機能、初期設定のパスワードの変更を促す等の機能、ソフトウェアの更新機能またはこれらと同等以上の機能を具備することが技術基準（端末設備等規則）に追加された（「3.2.3 (2) IoT 機器に対する規制の強化」参照）。

(b) 5G のセキュリティ対策

2020 年度から第 5 世代移動通信システム（5G）の導入が本格化する。以下では、通信事業者が全国規模で展開するサービス（全国 5G）、自治体・企業等が地域において展開するサービス（ローカル 5G）のセキュリティ対策について述べる。

- 全国 5G のセキュリティ対策
  5G のサイバーセキュリティを確保するため、第 5 世代移動通信システムの導入のための特定基地局の開設に関する指針は、携帯電話事業者に対して、5G 導入に向けた特定基地局の開設計画の認定の際に、品質や普及等に関する条件並びにサプライチェーンリスク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付与した※83。
- ローカル 5G のセキュリティ対策
  ローカル 5G 導入に関するガイドラインにおいて、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、ローカル 5G の免許申請時の条件として付与した※84。
- 5G ネットワークの脆弱性対策
  総務省は 2019 年度から、5G 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実施している。ソフトウェアを中心としたネットワークの脆弱性については、5G の通信インフラとしての機能保証のため、オープンソースソフトウェア等の解析、多種多様なパターンのデータ入力による異常動作確認（ファジング）、エシカルハッカー※85 による脆弱性調査、脅威分析の実施を検討した。またハードウェアの脆弱性については 5G ネットワークを構成するハードウェア上に故意に組み込まれた不正なチップのリスクに対応するため、AI を活用し回路情報から不正に改変された回路を検知する技術や、電子機器外部で観測される情報から不正動作を検知する技術を開発した。2020 年度以降は検知技術の改良、改変や不正動作への対策の検証を行い、また、5G ネットワーク上での運用面の課題等について検討する予定である。

(c) 研究開発の推進の状況

「IoT・5G セキュリティ総合対策」に基づく研究開発の推進状況を述べる。

- 基礎的・基盤的な研究開発等の推進
  暗号技術分野については、NICT において、現在利用されている暗号技術及び今後の利用が想定される暗号技術の安全性評価、量子コンピュータ時代に向けた格子理論に基づく新たな公開鍵暗号の開発、プライバシーの保護に資する暗号化したままデータを解析する技術等の研究開発を行っており、2019 年度においては、多変数多項式暗号の安全性評価において世界記録を達成した※86。
- 広域ネットワークスキャンの軽量化への取り組み
  脆弱な IoT 機器のセキュリティ対策のために、効率的な広域的ネットワークスキャンを実現する必要がある。そのため、総務省は 2018 年度から、周波数有効利用のための IoT ワイヤレス効率広域ネットワークスキャン技術の研究開発に取り組んでいる。2019 年度は、通信量の抑制と精度の向上を実現する効率的な広域ネットワークスキャン技術を確立するため、周波数の利用状況の自動推定による広域ネットワークスキャン技術、広域ネットワークスキャンの無線通信量軽減技術に関する詳細な技術仕様の検討と性能評価を行った。また、研究成果の活用を目的として、IoT 機器の脆弱性調査を実施する NICT 等に対し、本研究で収集した広域スキャンデータや機器情報を提供した。
- AI を活用したサイバー攻撃の検知・解析技術の研究開発
  NICT では、高度化するサイバー攻撃に対応するため、機械学習を始めとする AI を活用したサイバーセキュリティの研究開発に取り組んでいる。2019 年度は、多種多様な観測手段から得られるサイバー攻撃情報に対し各種機械学習のエンジンを用いてウイルス挙動に関する多角的な特徴量を抽出する技術や、AI を用いた IoT を狙うウイルスの挙動検知技術の基本方式の設計を実施した※87。

(d) 民間企業等におけるセキュリティ対策の促進

民間企業等におけるセキュリティ対策を促進するための主な取り組みの進捗状況を述べる。

- サイバーセキュリティ対策に係る情報開示の促進
  複雑・巧妙化するサイバー攻撃に対する対策強化を進めるためには、企業が自社のセキュリティ対策情報を適切に開示し、様々なステークホルダから評価される仕組みの構築が求められる。
  そのため、2017 年 12 月、サイバーセキュリティタスクフォースのもとに「情報開示分科会」が設置され、民間企業のセキュリティ対策の情報開示に関する課題や普及の方策について検討が行われてきた。2018 年 6 月、その結果を取りまとめた「情報開示分科会報告書※88」が公表された。総務省では、この検討結果を踏まえ、民間企業のサイバーセキュリティ対策の自主的な情報開示を促進する観点から、2019 年 6 月「セキュリティ対策情報開示の手引き」の策定・公表した※7。
- 事業者間での情報共有を促進するための基盤の構築
  サイバー攻撃に迅速に対応して被害を最小化するた

めには、事業者間でサイバー攻撃に関する脅威情報を共有する仕組みを構築する必要がある。そのため、総務省では、一般社団法人 ICT-ISAC を中心に、脅威情報の収集・分析・配布を行う情報共有基盤を運用する実証事業を行い、2018 年 6 月に「脅威情報の情報共有基盤利用ガイドライン」を策定した※89。また総務省では、2019 年度から、IPA にて公表されている脆弱性情報を STIX 形式※90 にて情報共有基盤上で共有し、資産管理ツール上で紐づける実証実験を実施している。

(e) 人材育成の強化

巧妙化・複雑化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材を育成するため、NICT の「ナショナルサイバートレーニングセンター」を中心に人材育成に取り組んでいる。またサイバーセキュリティ人材が地域的に偏在しており、地方においては一層厳しい状況であることから「サイバーセキュリティタスクフォース・人材育成分科会」において課題と対応方策の検討を実施し、地域のセキュリティ人材育成に力を入れている。2019 年度の主な取り組みの進捗状況を述べる。

- 実践的サイバー防御演習の実施
  総務省は、セキュリティ人材育成のため、NICT を通じて、体験型の「実践的サイバー防衛演習『CYDER』(Cyber Defense Exercise with Recurrence)」を実施している。2019 年度の CYDER の実施に当たっては、未受講となる地方公共団体の参加を促す観点から、開催場所及び開催日程を含む開催方法の見直しを各地方の総合通信局等と連携して実施した。具体的には、開催場所については、従来、都道府県庁所在地を原則としていたが、これまでの参加実績を踏まえ変更や追加を実施した。また、開催日程については、同一地域での開催日を分散することにより、受講機会を拡大した。この結果、2017 年度及び 2018 年度に未受講であった地方公共団体 1,019 団体のうち 175 団体が新たに受講し、2019 年度までの未受講団体数は 844 団体となった。これにより、全地方公共団体(1,788 団体)の過半数が受講済となった※91。
- 東京 2020 オリンピック・パラリンピック競技大会に向けたサイバー演習の実施
  NICT では、東京 2020 オリンピック・パラリンピック競技大会の適切な運営に向け、大会組織委員会のセキュリティ関係者が、大会開催時を想定した模擬環境で、サイバー攻撃・防御双方の実践的な演習を行う「CYBER COLOSSEO」事業を実施している。2018 年からは、演習効果をより高めるために、実践的な演習だけでなく、大会のセキュリティ強化に必要な知識の習得を目的とした「コロッセオカレッジ」を新設した※92。2019 年度はコロッセオ演習として初級コース 4 回、中級コース 5 回及び準上級コース 6 回の計 15 回開催し、延べ 193 名が受講したほか、コロッセオカレッジを 59 回開催し、延べ 992 名が受講した。
- 若手セキュリティ人材の育成の促進
  25 歳以下の ICT 人材を対象にセキュリティイノベーターの育成に取り組む「SecHack365」を、2017 年度から、NICT のナショナルサイバートレーニングセンターを通じて実施している。2019 年度は更にコースを二つ追加して 5 コースとし、15 歳から 24 歳までの 45 名が修了した。
- 地域のセキュリティ人材育成
  2019 年度は、総務省において、「地域のセキュリティリーダーの育成」「地域でのセキュリティ人材のシェアリング」「地域における人材エコシステムの形成」について、それぞれ対象地域を特定した上でその有効性を確認するための実証的調査を実施した。今後も、地域で自立したサイバーセキュリティ人材の育成が行われる仕組みとなるよう実証的調査を継続するとともに、調査成果を調査対象地域以外でも活用できるよう横展開を進めていく、としている。

(2) 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) クラウドサービスのセキュリティ対策

政府の情報システムにおけるクラウドサービスの安全性評価については、2018 年 8 月より、総務省と経済産業省が事務局となって「クラウドサービスの安全性評価に関する検討会」を開催し、2020 年 1 月に検討結果の取りまとめを公表した。また同月、サイバーセキュリティ戦略本部において、政府情報システムにおけるクラウドサービスの安全性評価制度の基本的枠組みが本部決定された※47。これを受け、2020 年 5 月 25 日に本制度の最高意思決定機関として有識者と制度所管省庁(内閣官房・総務省・経済産業省)を構成員とした ISMAP 運営委員会を設置するとともに、同年 5 月 26 日に第 1 回 ISMAP 運営委員会を開催し、委員会において制度に関する各種規程等が決定され、ISMAP の運用を開始した(「2.1.2 (2) 政府情報システムのためのセキュリティ評

価制度（ISMAP）」参照）。

（b）「自治体情報セキュリティ対策の見直しについて」の公表

総務省は、2019 年 12 月より、「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」を開催し、2020 年 5 月「自治体情報セキュリティ対策の見直しについて」を公表した※93。これは自治体情報セキュリティ対策見直しに関わる具体的な施策を取りまとめたものであり、総務省に対して、次期自治体情報セキュリティクラウドの在り方についての自治体への助言や、「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※94」の改定等を提言している。

（c）トラストサービスの在り方の検討

データの改ざんや送信元のなりすましを防止し、データの信頼性を確保する仕組みであるトラストサービスは、Society5.0 時代において、社会全体のデジタル化に貢献するものである。「プラットフォームサービスに関する研究会※95」の傘下に 2019 年 1 月設置された「トラストサービス検討ワーキンググループ※96」においては、事業者やユーザ企業等からユースケース等のヒアリング等を行いつつ、トラストサービスの制度化の在り方に関する詳細な検討を行ってきた。

2020 年 2 月に同研究会の最終報告書が取りまとめられ、トラストサービスに関しては、本ワーキンググループの議論を基に、一定のサービス提供の実態または具体的なニーズの見込みがあるとされ、利用者がより安心して利用できる環境の構築に向けた課題が顕在化しているタイムスタンプ、e シール及びリモート署名について、今後の取り組みの方向性が示された※97。

2.1.4 警察によるサイバー犯罪対策

政府は、2018 年 7 月、サイバーセキュリティ基本法に基づきサイバーセキュリティ戦略を閣議決定した※98。警察庁においても、同戦略を踏まえ、2018 年 9 月、「サイバーセキュリティ戦略」「サイバーセキュリティ重点施策」を改定し、サイバー空間の脅威への対処に関する取り組みを一層推進することとした※99。

2019 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。この戦略を踏まえ、2019 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

警察は先端技術を有する全国約 8,100 の事業者等（2020 年 1 月現在）との間で、情報窃取を企図したとみられるサイバー攻撃に関する情報共有を行う枠組みとして「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。2019 年中の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攻撃の件数は 5,301 件であった※100。標的型攻撃のうち、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」攻撃が多発し、全体の 90% を占め、引き続き高い割合となった。

警察では、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の 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で促進している。警察が把握した C&C サーバを運営する事業者に対し、不正な蔵置ファイルの削除を依頼する等して C&C サーバの無害化措置が執られた結果、2019 年中に 16 台の機能停止が実施された。

2019 年 6 月の G20 大阪サミット 2019（金融・世界経済に関する首脳会合）、9 月～11 月のラグビーワールドカップ 2019 日本大会等に伴い、サイバー攻撃対策を実施したが、いずれも会合、試合等の進行に影響を与える被害の発生はなかった。しかし、2021 年に延期された東京 2020 オリンピック・パラリンピック競技大会においては、大会の妨害や情報窃取等を目的としたサイバー攻撃が発生することが懸念される。警察では本大会に向けて、既存の重要インフラ事業者に加え、大会組織委員会、競技場を始めとする大会関係施設等の大会関係事業者等と連携して、サイバー攻撃による被害の未然防止に努めている。2019 年は 1 月に都内重要インフラ事業者等とサイバー攻撃を想定したインシデント対応共同技術訓練、9 月に大会公式パートナー企業とサイバーインシデント対応演習、11 月に大会関係事業者等とサイバー攻撃を想定した共同対処訓練を実施した。

（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 4 月、警察におけるサイバーセキュリティ戦略の改定を踏まえ「サイバー空間の脅威への対処に係る人材育成方針」を改定し、サイバー空間の脅威に対する対処能力の強化を図ることとした。更に、警察全体で計画的な人材育成を推進するために 2011 年より行われている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、等を含む「サイバー空間の脅威への対処に関する人材の育成計画」を策定し、都道府県警察もこの計画や各都道府県警察の実情を踏まえた計画を策定または見直すことが指示された[※101]。

(c) 国際連携及び産学官連携の推進

警察は、一般社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・サイバー攻撃の取締り等に活用している。

インターネットバンキングの不正送金被害の急増を受けて、2019 年 10 月、JC3 と連携し、警察庁及び JC3 の Web サイトで注意喚起を実施した。また、全国銀行協会と手口や被害状況等に関する情報共有を行うとともに、12 月、同協会と連携し、それぞれの Web サイトにおいて、被害防止の注意喚起を実施した[※102]。

また、ショッピングサイト等を改ざんし、クレジットカード情報を窃取する手口が明らかになったことから、JC3 と連携し、サイトの運営者や利用者に対して、注意喚起を実施した[※103]。

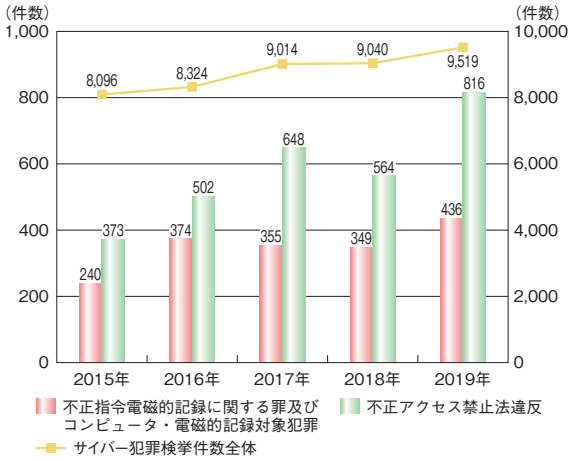
その他、2019 年 10 月フランスで開催された G7 ローマ／リヨングループに設置されたハイテク犯罪サブグループ会合、2019 年 11 月タイ・バンコクで開催された ASEAN + 3 国際犯罪閣僚会議及び日・ASEAN 国際犯罪閣僚会議等に警察庁から幹部・担当者が出席し、テロや国際犯罪への対策について各国代表と協議した[※104]（サイバーセキュリティに関する政府間連携については「2.2.1 国際社会と連携した取り組み」参照）。

(2) サイバー犯罪の検挙件数等

2019 年におけるサイバー犯罪の検挙件数、主な検挙事例について述べる。

(a) 2019 年のサイバー犯罪の情勢、検挙件数

警察によれば、サイバー犯罪の検挙件数は増加傾向

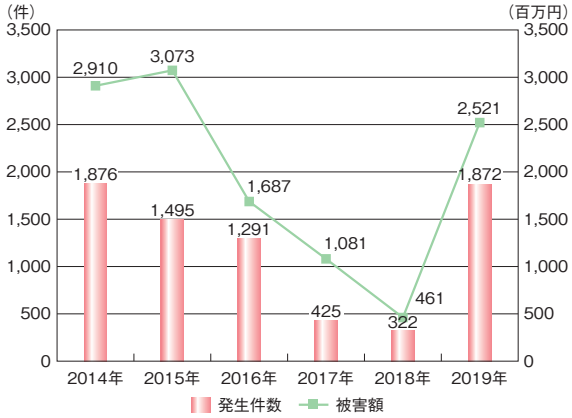


■図 2-1-7　サイバー犯罪検挙件数推移
（出典）警察庁「令和元年におけるサイバー空間をめぐる脅威の情勢等について[※100]」を基に IPA が作成

にあり、2019 年の検挙件数は 9,519 件と過去最多であった（図 2-1-7）。その中で「不正アクセス禁止法違反」の検挙件数は 816 件、「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 436 件であり、いずれも過去 5 年間では最多であった。

不正アクセス禁止法違反事案では、アクセス制御されているサーバに、ネットワークを通じて、他人の識別符号（ID・パスワード等）を入力して不正に利用する識別符号窃用型の犯罪の検挙が 785 件で全体の 96.2% を占めていた。

なお、2019 年におけるインターネットバンキングに関わる不正送金事案の発生件数は 1,872 件、被害額は約 25 億 2,100 万円であり、発生件数は過去最多であった 2014 年の 1,876 件に次ぐ件数であり、被害額も 2014 年の約 29 億にせまる勢いで大幅に増加した（図 2-1-8）。



■図 2-1-8　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と被害額の推移
（出典）警察庁「平成 30 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[※105]」「令和元年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

2019 年のインターネットバンキングに関わる被害は 9 月から急増しており、被害の多くは、SMS や電子メールを用いて、金融機関を装ったフィッシングサイトへ誘導する手口によるものと考えられる（金融機関を装う SMS の被害については「1.2.6(1)(c)金融機関を装う SMS」参照）。

その他、2019 年中のサイバー犯罪の発生状況で特徴的なものとしては、「コード決済」サービスに関するアカウントやクレジットカード情報を不正に利用されて、コンビニエンスストア等で商品を大量購入される事案や「Emotet」と呼ばれる不正プログラムに感染する事案が発生した（「1.1.2 (4) 注目された新たな脅威」「1.2.5 (1) Emotet のばらまき型メール」参照）。

(b) 主なサイバー犯罪の検挙事例

2019 年度における、サイバー犯罪の検挙事例から内部不正、コード決済の悪用、SNS がきっかけとなった不正利用、メディアで何度も取り上げられた著作権侵害の事例を紹介する。

- 2019 年 9 月、長崎県警察は、2017 年 1 月から 2019 年 2 月までの間、勤務先のサーバに対して、勤務先の職員の ID・パスワードを無断で使用して不正アクセスし、データを不正に入手した不正アクセス禁止法違反（不正アクセス行為）で同県職員の男性を検挙した※106。
- 2019 年 10 月、熊本県警察は、中国国籍の男性を、不正アクセス禁止法違反（不正アクセス行為）及び詐欺で検挙した。この男性は 2019 年 7 月、不正に取得した ID・パスワードを使用してコード決済システムに不正アクセスし、コンビニエンスストアにおいて、持っていたスマートフォンに表示した他人がユーザ登録した同システムのバーコード画面を提示し、電子タバコカートリッジを詐取した※107。
- 2019 年 10 月、鹿児島県警察は 2019 年 3 月から 4 月までの間、SNS で知り合った女性の携帯電話のキャリア決済に関する認証情報を、無断で自己のアカウントに関わる支払方法に設定し、デジタルコンテンツを購入した男性を私電磁的記録不正作出罪・同供用罪で検挙した※108。
- 福岡県警察、警視庁等は 2017 年 2 月から 2018 年 2 月までの間、設置場所不詳のサーバコンピュータに、著作物である漫画の画像データを記録保存し、インターネットを利用する不特定多数の者に自動的に公衆送信できる状態にして、海賊版サイトを運営し、著作権者等の著作権等を侵害したとして 2019 年 7 月から 10 月までの間、運営者らを著作権法違反で検挙した。また、同年 12 月、組織的犯罪処罰法違反（犯罪収益等の隠匿）で運営者を検挙した※109。

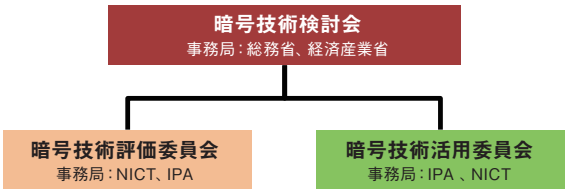
2.1.5 CRYPTRECの動向

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※110）の安全性を評価、監視し、暗号技術の適切な実装や運用法を調査、検討している。

(1) 2019 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 2-1-9）。



■図 2-1-9　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。2019 年度には、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）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）が設置された。

- 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。2018 年 5 月に一部改訂した「SSL/TLS 暗号設定ガイドライン」を大幅に見直すため、2019 年度には傘下に「TLS 暗号設定ガイドライン WG」が設置された。

(2) 2019 年度の主な活動

2019 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

2019 年度には、各委員会の 2019 年度活動計画、及び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、審議の結果、承認された。承認された内容は以下のとおりである。

- CRYPTREC 暗号リストの構成については引き続き検討する。
- 技術分類については現行のままとし、公募は実施しない。
- 耐量子計算機暗号、軽量暗号、及び高機能暗号については、次期 CRYPTREC 暗号リストには含めず、ガイドラインとして別途整備する。
- 推奨される暗号のパラメータについて、CRYPTREC 暗号リストから参照する形で別文書として整備する。

更に、XTS（Xor encrypt xor (XEX) Tweakable block cipher with ciphertext Stealing）モードを推奨候補暗号リストの「秘匿モード」に追加すること、EdDSA[※111-1]に関する安全性評価を進めること、及び運用監視暗号リストからの削除ルールを整備し、2021 年 3 月に RC4 を運用監視暗号リストから削除することを決定した。これにより 2021 年 4 月以降は、互換性維持の目的であっても RC4 の利用が認められなくなる。

(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、2019 年度の主な活動内容・成果は以下のとおりである。

- XTS モードの実装性評価
  ストレージデバイスのデータ暗号化に使用されている暗号利用モードである XTS モードについて、2018 年度の安全性評価に引き続き、実装性評価を実施し、CRYPTREC 暗号リスト（推奨候補暗号リスト）への追加に必要な条件を満たしているか検討を行った。その結果、XTS モードは、ストレージデバイスでの暗号化に限定して同リストへ掲載するのに十分な安全性及び実装性を有していると判断された。
- 暗号技術調査ワーキンググループの活動
  2018 年度の公開鍵暗号に引き続き、2019 年度には共通鍵暗号に関する耐量子計算機暗号の調査・検討を行った。具体的には、量子コンピュータが実用化されたと仮定したときの電子政府推奨暗号リストに掲載されている共通鍵暗号及び暗号利用モードに対する安全性評価を行い、2020 年 7 月に調査報告書が公開される見込みである。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」の改訂についての検討も行った。

(c) 暗号技術活用委員会

2019 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）」及び「TLS 暗号設定ガイドライン」の作成を行った。

- 暗号鍵管理システム設計指針（基本編）
  2018 年度から作成していた「暗号鍵管理システム設計指針（基本編）」のドラフト版を「CRYPTREC シンポジウム 2019」開催に合わせて公開し、パブリックコメントを実施した。その後も、あらゆる領域の暗号鍵管理システムに対し暗号鍵の管理を安全に行うための対応方針を決めるにあたって考慮すべき検討事項（Framework Requirements）を網羅的にカバーする指針として検討を行い、本ガイドラインは 2020 年 7 月に公開された[※111-2]。

- TLS 暗号設定ガイドライン
  2015 年に Ver1.0 及び Ver. 1.1、2018 年に Ver. 2.0 をリリースした「SSL/TLS 暗号設定ガイドライン」（以下、現行ガイドライン）は、累計で20万件以上ダウンロードされている等、TLS を利用する際の有用な運用ガイドラインとなっていると考えられる。
  しかし昨今、現行ガイドラインに記載されている内容に大きく影響する規格化が相次いで行われており、それに伴い SSL/TLS の利用環境も大きく変化している。そのため、位置付け及び想定読者に関しては現行ガイドラインを継承し従来の有用性を維持する一方、技術的には 2019 年度末時点での TLS の現状を踏まえて全面的に記載内容を改訂した。なお、今回の改訂で SSL 3.0 を全面的に禁止することになったため、ガイドラインの名称から「SSL」を削除し、「TLS 暗号設定ガイドライン」として 2020 年 7 月に公開した[※111-3]。

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、あらゆる国や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 化した社会基盤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

2018 年度に引き続き、日本政府は 2019 年度も米国、欧州、ASEAN 等の諸国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。

(1) G20 大阪サミット

2019 年 6 月 28 ～ 29 日、G20 大阪サミット 2019 が大阪市で開催された※112。日本が議長国となり、G20 メンバー国に加え、八つの招待国、九つの国際機関代表が参加する等、国内開催では最大の国際会議となった。同サミットの第 2 セッション「イノベーション」において、安倍晋三首相は経済・社会のデジタル化において、信頼性のある自由なデータ流通が不可欠であるとして、DFFT（Data Free Flow with Trust：信頼性のあるデータの自由な流通）の概念を提唱した。安倍首相は既に 2019 年 1 月 23 日の世界経済フォーラム年次総会（ダボス会議）※113において、DFFT の概念と世界貿易機関（WTO: World Trade Organization）加盟国による流通ルール作りを提案しており、G20 においては更に WTO による電子商取引ルール策定等を推進する「大阪トラック」を宣言し、具体的な検討が始まることとなった※114。

また、これに先立つ閣僚級会議として、6 月 8 ～ 9 日に G20 貿易・デジタル経済大臣会合がつくば市にて開催された※115。同会合においては DFFT に関する議論のほか、「人間中心」のデジタル化の方針として、自由・オープン及び安全なインターネットの推進、暴力・テロ目的のインターネット利用への対抗等、これまでの米欧日の基本方針を再確認した。更に同会議は「人間中心の人工知能（AI）」の概念を打ち出し、法の支配、プライバシーとデータの保護、倫理（差別の排除）、公平性、最終決定権を人間が持つ等の価値観やセキュリティの重要性を提唱した。この成果は付属書「G20 AI 原則」としてまとめられた※116。AI 事業者・技術者のコミュニティにおいても AI 利用の倫理・悪用防止・公平性等の議論が進んでおり、今後の国際連携の重要トピックになると考えられる（米国の AI 倫理政策に関しては「2.2.2 (5) DoD の政策」参照）。

(2) 日米のサイバー連携

2019 年 10 月 11 日、第 7 回日米サイバー対話が東京にて開催された※117。日本からは赤堀毅外務省総合外交政策局審議官兼サイバー政策担当大使を始め、国家安全保障局、NISC、内閣情報調査室、警察庁、総務省、経済産業省、防衛省等の関係者が参加した。米国からは Robert Strayer 国務省次官補代理（サイバー及び国際通信情報政策担当）（Deputy Assistant Secretary for Cyber and International Communications and Information Policy, Department of State）を始め、国家安全保障会議（NSC：National Security Council）、国土安全保障省（DHS：Department of Homeland Security）、商務省（Department of Commerce）、国防総省（DoD：Department of Defense）、連邦捜査局（FBI：Federal Bureau of Investigation）等の関係者が参加した。

討議では 2018 年の第 6 回日米サイバー対話のフォローアップを行い、重要インフラのセキュリティ、防衛面におけるサイバー連携や国際的なサイバーセキュリティ情報共有の強化に向け、協力することを確認した。また両国は、国際連合や ASEAN 地域フォーラム（後述）等の多国間会議におけるサイバー上の課題に関し共同歩調を取ることを再確認した。従来の両国の主張である「オープンで自由な情報流通・利用ができる安全なサイバー空間」を推進する、という立場を再確認したものである。

首脳レベルでは、2019 年 5 月 25 ～ 28 日、ドナルド・トランプ（Donald John Trump）大統領が日本を訪問し、5 月 27 日、安倍首相と会談を行った※118。主要議題は日米同盟の強化、北朝鮮・中国との外交方針のすり合わせ、同盟国・友好国のネットワーク構築、宇宙協力、経済協力等であった。このうちセキュリティ・安全保障に

関する話題としては、対北朝鮮外交姿勢の協調確認が最も大きいが、このほか「自由で開かれたインド太平洋」に向けた協調（インド・オーストラリアとの同盟強化、中国への牽制）、安全保障を含む宇宙協力の強化が挙げられる。

防衛面では2019年10月23日、日米サイバー防衛政策ワーキンググループ（CDPWG：Cyber Defense Policy Working Group）第7回会合が米国アーリントンにて開催された※119。日本側からは石川武防衛省国防政策局次長、米国からはB. Edwin Wilson国防次官補代理（Deputy Assistant Secretary of Defense）が参加し、2018年末に公表された米国国防計画の大綱等を踏まえ、情報共有、訓練及び人材育成の分野に関する連携について協議が行われた。一方、日米首脳会談で一部合意された宇宙、サイバー、電磁波等の「新しい領域」における協力も今後加速するものと思われる。

(3) EU諸国とのサイバー連携

2019年は、EU、フランス、英国とのサイバー協議が行われた。

(a) 日EUサイバー対話

2019年6月11日、第4回日EUサイバー対話がベルギー・ブリュッセルにて開催された※120。日本からは大鷹正人外務省総合外交政策局審議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、EUからはPawel Herczynski欧州対外活動庁共通安全保障・防衛政策（CSDP：Common Security and Defence Policy）危機管理総局長代行兼安全保障・防衛政策局長（Deputy Managing Director for CSDP and Crisis Response / Director for Security Policy and Defense, European External Action Service）を始めとする関係機関の代表者が出席した。協議においてはサイバーセキュリティに対する双方の戦略・政策と課題について広範な討議が行われ、2001年に採択されたサイバー犯罪におけるブダペスト条約※121を踏まえたサイバー犯罪対策の連携、サイバー空間における国際法や規範の遵守、不当な知的財産窃取への反対等が共同声明に盛り込まれた。

(b) フランスとのサイバー協議

2019年7月12日、第5回日仏サイバー協議がフランス・レンヌにて開催された※122。日本側共同議長は大鷹正人同審議官、フランス側共同議長はHenri Verdierフランス共和国欧州・外務省デジタル大使（Ambassador for Digital Affairs, Ministry of Europe and Foreign Affairs of the French Republic）が務め、両国の関係政府・産官学連携機関の代表者が出席した。

協議においては、両国の脅威認識とサイバーセキュリティ政策の進展の共有、2019年度G7議長国であるフランス、G20議長国である日本のデジタル分野における協働等について、G7、G20で発出・共有された「サイバー規範イニシアティブに関するディナール宣言※123」等の考え方を踏まえた討議が行われた。また両国は、オープンで自由かつ安全・公正なサイバー空間の維持に向けたコミットメントを再表明し、更に、東京2020オリンピック・パラリンピック競技大会、及び2024年パリ大会でのサイバーセキュリティ分野における協力を合意した。

(c) 英国とのサイバー協議

2020年1月31日、東京にて第5回日英サイバー協議が開催された※124。日本側共同議長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、英国側共同議長はDr. Alexander Evans外務省サイバー政策部長（Director Cyber, National Security Directorate, Foreign and Commonwealth Office）が務め、両国の関係機関の代表者が出席した。協議においては、双方のサイバーセキュリティ政策に関する最新情報共有のほか、能力構築への取り組み、国連を含む国際機関における双方向の連携等が議論された。

首脳レベルでは、2019年7月24日、ボリス・ジョンソン（Boris Johnson）新首相がEU離脱を掲げて就任したことを受け、2019年8月26日、安倍首相はG7参加で訪問中のフランスにてボリス・ジョンソン首相と首脳会談を行った※125。同会談では、英国のEU離脱後の新たな日英経済のパートナーシップを迅速に構築することで合意した。なお英国は2020年1月31日、正式にEUを離脱し、同年12月31日までの移行期間に入った※126（EU離脱後のEUとの交渉については「2.2.3 (1) 英国・EUの連携交渉に関する論点」参照）。

一方、安全保障面では、2017年12月以降中断している日英外務・防衛閣僚会合「2+2」の再開が議論されたが、2020年6月現在まだ開催には至っていない。

(4) ウクライナ・ロシアとのサイバー協議

2019年は、EU域外のロシア・ウクライナについて、政府レベルのサイバーセキュリティ協議が行われた。

(a) 日露サイバー協議

2019 年 11 月 20 日、第 3 回日露サイバー協議が 3 年ぶりに行われた※127。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、ロシアからは Andrey Krutskikh 情報セキュリティ国際協力担当露大統領特別代表・露外務省特任大使を始めとする関係機関の代表者が出席した。同協議ではサイバー空間の脅威の現状、政府の政策、多国間のセキュリティ連携や重要インフラ保護等について意見を交換した。サイバー空間におけるロシアとの政策連携は不確定部分が大きいが、今後重要になると考えられる。

(b) 日ウクライナサイバー協議

2020 年 1 月 23 日、第 2 回日ウクライナサイバー協議が 4 年ぶりに行われた※128。日本からは前出の赤堀毅外務省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、ウクライナからは Serhiy Demediuk 国家安全保障・国防会議副書記（Deputy Secretary of National Security and Defense Council of Ukraine）を始めとする関係機関の代表者が出席した。同協議では、サイバー分野における戦略や体制、情勢認識や具体的な取り組みについて双方の状況を説明し、意見を交換した。親 EU の現ウクライナ政府とも協議を行い、ロシアとバランスを取って連携を進めるものと思われる。

(5) ASEAN とのサイバー連携

ASEAN 地域における政府レベルの連携施策について紹介する。

(a) 日・ASEAN 情報セキュリティ政策会議

2019 年 10 月 29 ～ 30 日、タイ・バンコクにて第 12 回日･ASEAN 情報セキュリティ政策会議（以下、政策会議）が開催された※129。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 12 回政策会議は日本・タイが議長国となり、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。同協議では、第 11 回政策会議で合意された 8 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等）の活動状況を確認するとともに、今後の活動として情報共有体制、インシデント対処体制確立に向けた演習、重要インフラ保護に関するワークショップ実施の取り組み、能力構築・意識啓発に関する協力の推進等が議論され、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※130）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 ARF 会期間会合（ARF-ISM on ICTs Security）」（以下、会期間会合）を立ち上げ、2018 年 4 月より活動が始まっている。

2019 年には、1 月 29 日に会期間会合のための第 3 回専門家会合※131（以下、専門家会合）が、3 月 26 日に第 4 回専門家会合が開催され、サイバーセキュリティ環境に対する各国・地域の取り組みや今後構築すべき信頼醸成措置について議論が行われた。またこの成果を基に同年 3 月 28 ～ 29 日、シンガポールにて第 2 回会期間会合※132 が開催され、日本･マレーシア･シンガポールが共同議長を務めた。同会合では信頼醸成措置の具体化について合意するとともに、各国のサイバーセキュリティ政策に関して情報共有が行われた。

更に 2020 年 1 月 16 日、クアラルンプールにて第 5 回専門家会合※133 が開催され、第 4 回と同様日本･マレーシア・シンガポールが共同議長を務めた。引き続き、地域的･国際的なサイバーセキュリティ環境の見方や各国･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、2019 年に国連に設置されたサイバーセキュリティに関する政府専門家グループ※134 及びオープンエンド作業部会※135 における議論も含め、ARF の枠組みにおいても全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していくべきことを確認した。この成果は 2020 年開催予定の第 3 回会期間会合に提供される。

(c) ASEAN 諸国向けの演習・インドとの連携

2019 年 9 月 9 ～ 12 日、経済産業省と IPA は米国政府と連携し、ASEAN 加盟国を含むインド太平洋地域諸国を対象とする「インド太平洋地域向け日米サイバー演習」を東京にて実施した※15。同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政府関係者・重要インフラ事業者等 35 名が参加した（演習の内容は「2.3.2 (1) 中核人

材育成プログラム」参照）。

ここで、演習の対象地域が「インド太平洋」であることが注目される。中国のインド洋への進出を背景に、日米両国は ASEAN 諸国と歩調を合わせつつ、インドとの安全保障・セキュリティ分野での連携を進めている。インドとのサイバー協議は、2019 年 2 月の第 3 回日インドサイバー協議※136 以降、2020 年 6 月時点で第 4 回協議は開催されていないが、今後も連携が深まるものと思われる。

(6) 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、2019 年度は慶應義塾大学主催のサイバーセキュリティ国際シンポジウム等が開催された。

(a) 第 9 回サイバーセキュリティ国際シンポジウム

サイバー脅威に関する研究機関の国際連携組織 InterNational Cyber Security Center of Excellence（INCS-CoE）の活動の一環として開催されるシンポジウムで、2019 年は 12 月 11 ～ 12 日、慶應義塾大学にて開催された※137。米国・英国・オーストラリア・イスラエル等の大使館及び駐日欧州連合代表部を始め、関係国内省庁が後援している。同会議では、G20 大阪サミットで提唱された DFFT に関し、特に多国間連携によるトラストサービスに焦点を当て、後援組織の関係者及び有識者が一堂に介し講演・議論を行った。また IoT to 5G、経営、人材育成、サプライチェーンセキュリティ等の講演・討議も行われた。

(b) 情報セキュリティ国際シンポジウム

総務省と一般社団法人 ICT-ISAC は 2019 年 11 月 11 日、東京にてサイバーセキュリティ国際シンポジウムを開催した※138。同シンポジウムでは米国 DHS National Coordinating Center や Communication ISAC 等の代表者、及び米国 National Council of ISACs 議長等を迎え、日米の ISAC（Information Sharing and Analysis Center）におけるサイバーセキュリティ情報共有の在り方について議論が行われた。

(c) サイバー・イニシアチブ東京 2019

世界各国の民間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 2019 が、2019 年 12 月 12 ～ 13 日に開催された※139。日本からは高市早苗総務大臣、梶山弘志経済産業大臣、河野太郎防衛大臣、鈴木馨祐外務副大臣等が講演したのを始め、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て安全保障、大規模国際イベント・重要インフラの防衛、5G、AI 等のデジタル化革新技術の課題について議論を行った。

2.2.2 米国の政策

2018 年に引き続き、2019 年の米国のサイバーセキュリティ政策は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が鮮明であり、政府調達や重要インフラのサプライチェーンからの特定海外ベンダの排除が実施されつつある。この中で、安全保障・経済両面で対立する中国との交渉は波乱含みで、2020 年 2 月、いったん貿易摩擦交渉の歩みよりが見られたものの、3 月以降の新型コロナウイルス感染症（以下、新型コロナウイルス）の世界的蔓延（以下、パンデミック）で両国関係は急激に悪化し、先が見通せない状況である。本項では、このような状況下で策定された米国政府のサイバーセキュリティ戦略と政策について述べる。

(1) 米中貿易摩擦交渉の推移

2019 年上期に激化した米中貿易摩擦は、その後やや沈静化のきざしを見せ、2019 年 12 月 13 日、米中両政府は貿易協議の「第 1 段階」で正式合意したと発表した※140。この合意は農業、金融サービス、為替等、対立の小さい分野に限定されたものの、2019 年 9 月に実施するとした米国の制裁関税と中国の報復関税の発動を見送り、米国は発動済みの追加関税の一部を引き下げるとし、交渉の大きな転換点となった。米国大統領選を意識するトランプ政権と、景気失速を懸念する中国が妥協した形である。

2020 年 2 月 14 日に同合意は発効し、中国は米国への報復関税等の政策を相次いで解除した※141。米国も、新型コロナウイルス対策に配慮した形で中国からのマスク輸入（同年 2 月）、医療品輸入（同年 3 月）の関税を免除した※142。しかし、直後からのパンデミックによる世界経済の停滞等により、輸入目標の達成は難しくなり、更に後述する米中関係の悪化により、貿易摩擦交渉自体が頓挫してしまった。

(2) 新型コロナウイルス対策をめぐる米中関係悪化

2020 年 3 月以降の新型コロナウイルスの国内感染拡

大と景気後退は米国を大きく揺さぶっている。トランプ大統領は同年1月、中国発の新型コロナウイルスの蔓延について経済アドバイザー等から警告を受けていたが、当初はこれを無視したといわれる※143。世界保健機構（WHO：World Health Organization）のパンデミック宣言後、トランプ大統領は3月13日に国家非常事態を宣言※144、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とした。しかし、ニューヨーク州を筆頭に被害が激増、経済的な影響も甚大となり、初動対策の遅れに対する批判が相次いだ。

米中政府間では、2月初旬の中国滞在者の米国渡航制限以来、感染拡大の責任について非難の応酬が始まっていたが、トランプ大統領は4月に入り、WHOに対してパンデミックへの警告が不十分で、中国の影響を小さく見せていると批判、資金拠出の停止を発表した※145。同大統領は更に、中国がパンデミックについて「故意の責任があるなら報いを受けるべき」と中国を正面から批判※146、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※147。これらの発言は自身への批判をかわすためとも見られるが、中国への厳しい姿勢はパンデミックに苦しむ米国の世論となっており、欧州からも中国が情報を隠ぺいしたとの批判の声があがっている※148。米国政府は習近平主席への直接的な批判を避けてはいるものの、一時修復に向かった米中関係は急激に悪化している。

トランプ大統領は2020年5月5日、感染者や死者の増加につながるとしても、米国民は日常生活に戻り始めるべきだと述べ、経済活動再開への強い姿勢を示した※149。大統領選をにらみ、経済の立て直しが急務と考えていると思われる。更に米国経済の視点で見ると、今回のパンデミックで、重要な調達のサプライチェーンを海外（主として中国）に依存することのリスクが明らかになったといえる。トランプ政権は2018年から、政府調達サプライチェーンの脱中国化を宣言していたが、動機は主に安全保障面であった。2020年5月時点で、脱中国化は経済・安全保障両面での重要戦略となったと考えられる。

(3) 国防権限法

2019年の国防予算の大枠を決める「国防権限法2019※150（National Defense Authorization Act for Fiscal Year 2019）」は2019年8月13日から発効し、政府調達から中国のITベンダ・通信機器ベンダ5社※151の締め出しが実行されることとなった。上記5社の製品を利用する企業は今後政府調達に参入できないことになる。同法はまた、開発段階にある先端技術を輸出・投資の規制対象に含め、中国を念頭においた技術の海外流出への規制を大幅に強化した。

更に2019年12月20日、2020年度の国防予算を規定する「国防権限法2020」が成立した※152。同法の予算総額は2019年比約3%増の約7380億ドル（約80兆円）となり、軍備近代化、先端技術開発等に配分された。具体的には2019年に宣言された「宇宙軍」の創設費用が盛り込まれ、前述のIT・通信系中国企業5社の禁輸措置を容易に解除できなくするとともに、中国国営企業からの車両の調達等を新たに禁じた。

(4) 議会におけるサイバーセキュリティ戦略検討

国防権限法2019に基づき、超党派の上院議員によるCyberspace Solarium Commissionが設置され、「サイバー脅威からの国家重要インフラ保護」をテーマとして1年にわたり検討が行われ、2020年3月17日に報告書が公表された※153。同委員会はDwight Eisenhower大統領が冷戦時代の外交戦略を検討させたProject Solariumを範としている。同報告書では、「現在のサイバー空間には抑止（Deterrence）の概念がなく、米国政府は敵対的勢力が国家インフラに侵入できる事態に対し、必要なスピードと機敏さで行動できていない。多層的なサイバー抑止行動（Layered cyber deterrence）を実施すべきである」とし、六つの重要な柱に関して80項目に及ぶ勧告が示された※154。六つの柱とは以下である。

- 米国政府のサイバー空間に向けた組織構造改革
- 規範（国際標準）、非軍事的手段（法執行、条約、制裁他）による規制強化
- 国家レベルの頑健性（事業継続性）の推進
- サイバーエコシステムの再編（認証・保証、サプライチェーンのトラスト）
- 民間とのサイバーセキュリティ連携の運用
- （抑止に必要な）軍事機器を含む国家の力の蓄積と使用

勧告の中には、新たな議会の委員会により監督される「国家サイバー長官」の創設、サイバーオペレーションの訓練を受けた職員の増員、DHSや選挙支援委員会等の連邦機関が任務を遂行するための資金の増額等が含まれる。ここ数年、米国のセキュリティ戦略では「選挙に対する脅威」が重視されるが、本勧告にもそれが現れている。

米国政府は「マルチステークホルダによる自由で信頼できるサイバー空間」を最上の価値として、中国等による国家主権のサイバー空間への介入を批判し、攻撃力による抑止のような強権的施策は明言してこなかった。本勧告はその状況に不満を持つ議会が一石を投じたもので、今後の米国のサイバー空間のガバナンス方針に影響を与える可能性がある。

ただし、同報告書は「攻撃には攻撃で抑止」のような冷戦時代的な方針は表明していない。あくまで同盟する各国政府や民間組織との連携、法執行、外交等の手段により抑止を実現する、としていることに注意が必要である。

(5) DoD の政策

DoD は 2018 年に発表したサイバーセキュリティ戦略※155 の具体的な実装に着手し、サイバー軍の強化や DoD 自身の IT 基盤の頑健化・人材強化を進めている。

(a) 抑止的なサイバー軍の活動

サイバー軍の活動の全貌は未公開だが、前項で紹介した報告書の提言どおり抑止的であると予想される。例えば、上記サイバーセキュリティ戦略で明示される方針「Defend forward」が攻撃を意味するのではないかという懸念に対して、サイバー軍は米国外のサイバー空間でも活動するという意味で「forward」だが、あくまで防衛目的である、と説明されている※156。実際、サイバー軍の公式サイトでは、主としてウイルスの監視と対策に関する活動が紹介されている※157。

(b) 防衛調達における新しいフレームワークの採用

連邦政府の装備・システム調達におけるセキュリティ確保は DoD にとっても重要な課題である。2020 年 1 月 31 日、DoD は新しいサイバーセキュリティ成熟度モデル認証（CMMC：Cyber security Maturity Model Certification）の初版を公開した※158。CMMC は、サイバーセキュリティ対策実施の成熟度を基本から発展までの 5 段階に分けて評価、認証するフレームワークである。DoD は CMMC 取得を防衛関係調達契約のセキュリティ要件とし、防衛関連サプライチェーンのサイバーセキュリティ対策レベルを検証できるようにしたい、としている。

DoD は 2017 年の時点で、調達事業者に提供する「管理された非格付け情報（CUI：Controlled Unclassified Information）」の保護に関して、米国標準技術研究所（NIST：National Institute of Standards and Technology）の規格 SP800-171※159 の遵守を要請していた※160。CMMC の取得要請はこれに屋上屋を架すように見えるが、SP800-171 の遵守については調達事業者からかなりの負担である、と不満が出ていたといわれる。DoD はこうした不満に対し、リスクアセスメントで SP800-171 の中の必要な項目を選択して対応すればよいとしてきたが、今回、CUI の保護よりも包括的で、かつ 5 段階の成熟度モデルに基づく CMMC を採用し、防衛サプライチェーンのセキュリティ底上げに関して仕切り直しをしたと考えられる。SP800-171 は連邦政府の調達に関係する日本企業等にも影響を与えてきたが、CMMC にも注意が必要と思われる。

(c) 民間 IT 基盤の活用

連邦政府の IT 基盤の刷新、民間インフラの活用はセキュリティ戦略としても重要となっているが、DoD は 2019 年 10 月 25 日、クラウドコンピューティング基盤 JEDI（Joint Enterprise Defense Infrastructure）に関する発注契約を Microsoft Corporation（以下、Microsoft 社）が獲得した、と発表した※161。予算規模は 10 年間で総額 100 億ドル（約 1 兆 800 億円）といわれる。

この決定に対し、JEDI 受注の本命と見られていた Amazon.com, Inc. は、政治的介入があったとして連邦裁判所（U.S. Federal Court）に提訴、同裁判所はこれを認めて Microsoft 社の契約関連業務の一時差し止めを命じた※162。Amazon.com, Inc. は更に、トランプ大統領と Mark Esper 国防長官の証言を求めている。背景には、Amazon.com, Inc. の Jeff Bezos CEO とトランプ大統領の確執があるといわれる。JEDI は DoD の IT 基盤システムの革新を狙う重要プロジェクトだが、政治的な理由でつまずいた形である。

もう一点注目されるのは、IT の軍事利用についてグローバルベンダが一枚岩ではない点である。例えば Google LLC はドローン映像の AI による解析に関する DoD との契約について、従業員 4,000 人が抗議請願書に署名した事実を受け、これを更新しなかった。Microsoft 社においても Azure の軍事利用に反対する従業員は存在し、論争に発展する可能性をはらんでいる※163。

(d) AI 倫理原則の採用

Mark Esper 国防長官は 2020 年 2 月 24 日、DoD のアドバイザリーボード「Defense Innovation Board」が 2019 年 10 月に提出していた国防に関する AI 倫理原則の受け入れを発表した※164。同原則は以下のようなも

のである。

- Responsible：AI 機能の開発、展開、利用に責任を持ち、適切な判断を行う。
- Equitable：AI 機能の利用において偏見や意図しない展開が起こらないように熟慮する。
- Traceable：AI 機能に関する関係者の理解、開発、運用について、透明な方法で追跡可能とする。
- Reliable：明示的に正しく定義され、安全で安心できる検証可能な AI 機能の利用を行う。
- Governable：AI 機能が意図しない結果を生起させないように常に検知し管理する。

AI 技術者・研究者のコミュニティにおいては、AI を搭載した兵器やロボットが自律的に人間等を攻撃することへの倫理的懸念が表明されてきた。DoD も AI 専門家や政府・産業界と 15 ヵ月にわたり検討を進めてきたが、AI 導入の促進や技術革新のためにも倫理原則は重要と考え、受け入れに至ったと思われる。発表において DoD は、同倫理原則は、米国市民の自由と価値を守り、信頼できる AI 技術の革新を主導するトランプ政権の戦略（American AI Initiative※165）にそったものであるとしている。同盟各国にも倫理原則の受け入れを呼びかけるものと思われる。

(6) DHS 及び商務省の政策

2018 年 11 月、DHS は国家のサイバーセキュリティ、インフラストラクチャレジリエンス強化、緊急時コミュニケーション、重要インフラリスク管理の四つのミッションを統括する組織として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：Cyber Security and Infrastructure Security Agency）を設置した※166。CISA は 2019 年初頭より、官民連携による ICT Supply Chain Risk Management Task Force（以下、Task Force）の活動を統括する等、本格的な活動を開始している※167。

(a) サプライチェーンセキュリティ対策の推進

上記の Task Force では、通信業界、IT 業界、連邦政府の三セクターの代表 60 組織が参加し、情報共有、脅威の評価、調達参加資格、偽物調達防止政策の四つの WG に分かれ（2019 年 12 月に 1 個の WG を追加※168）、政府機関や産業界のサプライチェーンセキュリティの実態について検討が行われた。検討結果については、2019 年 9 月に中間報告が公表され、2020 年 5 月には企業のセキュリティ頑健性を高めるためのサプライチェーンリスク管理ガイダンスとファクトシートが発表された※169。ガイドラインとファクトシートはある意味基本的なものだが、NIST のサイバーセキュリティフレームワークのように産業界で実践されていくか、注目される。

CISA の活動とは別に、トランプ大統領は 2019 年 5 月、サプライチェーン情報通信技術のセキュリティに関する大統領令 13873 に署名した※170。商務省は同大統領令に基づき、2019 年 11 月 27 日から 2020 年 1 月 10 まで、サプライチェーンセキュリティリスク評価規則を公開、意見を募集した※171。同規則は、国家の安全に影響を及ぼす重要インフラやサービスのリスク評価手続きであり、「敵対的な海外勢力」との取り引きや特定条件の取り引きにケースバイケースで制限をかける等、中国製品を念頭においた調達規制が強く志向されている。しかし、民間から「ケースバイケース」の運用があいまいでビジネスに悪影響がある、等の懸念が示され※172、拙速の感は否めない。同規則の実施は、トランプ大統領が大統領選挙直前に中国との交渉条件とするのではないか、等の見方もされていたが、パンデミックの影響で不透明となっている。

一方 CISA は 2020 年 4 月、前述の Task Force と連携し、大統領令 13873 で指示された「最も重要な ICT 技術・サービス」の評価報告を公開した※173。同報告は 61 の重要な ICT 要素を抽出し、これを 5 個のロール（ローカルユーザアクセス、伝送、保存、処理、システム管理）と 11 個のサブロールに分類したもので、上記の商務省規則が適用される重要インフラ、サービスの特定に用いられると思われる。

(b) 敵対的勢力からのサイバー攻撃の監視

2020 年 1 月 6 日、CISA はイランによるサイバー攻撃への警戒を勧告した。同勧告では、直前におきた米軍のイラン軍 Qasem Soleimani 司令官殺害※174 に対する報復の可能性として、米国や関係国に対する「サイバー並びに軍事によるハイブリッド攻撃」への警戒が呼びかけられた※175。CISA による公式な勧告として初めてのものであったが、米国が敵対的とする勢力（イラン・北朝鮮・中国等）に関する注意喚起は 2020 年 5 月時点でこれのみであり、表面上は敵対的勢力のサイバー攻撃は沈静化しているように見える。

(c) 新型コロナウイルス対策としてのセキュリティ

2020 年 1 月以降は、新型コロナウイルス対策としてのサイバーセキュリティが世界的な関心事となっている。米

国ではCISAがいち早く新型コロナウイルス封じ込めと緩和のための情報共有を支援すると宣言し、同年3月6日に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[※176]を、また3月18日に重要インフラ保護、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[※177]。詐欺被害に関してはFBIも別途注意をよびかけた[※178]。

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日に注意喚起を行った[※179]。更に同年5月5日、CISAとNCSCは続報として、医療・ヘルスケア関連組織が攻撃対象になっており、特に製薬企業・医療研究機関に対し研究データや知的財産データの窃取を狙っている、と警告した[※180]。更にCISAは4月24日、遠隔会議システム等のテレワークのツールに対する攻撃が急増しているとして、テレワーキングのセキュリティに関するガイダンスを公開した[※181]。

これに加え、1月以降は新型コロナウイルス対策をめぐるデマや国家的な陰謀論が急浮上し、ネット上で批判の応酬が続いている。例えば米国国務省の官僚が「ロシアが数千に及ぶSNSアカウントで反米的な偽情報（新型コロナウイルスは米国の生物兵器である、等）を拡散している」としてロシアを非難する[※182]等、米国と敵対勢力との間で中傷が続き、SNS上では新型コロナウイルス関連の詐欺情報・偽情報が氾濫している状況にあるとみられる。

このように、新型コロナウイルス関連のサイバー攻撃・偽情報への対処は米国のパンデミック対策としても重要課題となっており、関係機関の対応が注目される。

2.2.3 欧州の政策

2020年2月1日、英国は正式にEUを離脱した[※183]。アイルランドと北アイルランドの国境問題等で懸念されていた合意なしの離脱はかろうじて避けられ、2020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、その間に英国・EU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。ただし、本当に厳しい交渉は移行期間が始まってからであり、難航するという見方もある[※184]。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) 英国・EUの連携交渉に関する論点

2020年3月2日、英国議会下院（the House of Commons）はEUと交渉すべき項目と論点を公開した[※185]。このうちセキュリティに関するものとしては、国内の法執行・国外の防衛、及びデータの妥当性（Data adequacy）があげられた。

(a) 国内の法執行

国内の法執行について、英国は欧州逮捕状（EAW：European Arrest Warrant）[※186]、犯罪情報・容疑者情報等のデータベースアクセス等、40以上のEU加盟国間の協調施策をいったん棄却し、関係を再構築する必要がある。これについて英国は、EU法制や欧州司法裁判所（CJEU：Court of Justice of the European Union）と国内法を切り離す「実用的な合意」を望んでおり、例えばEUのヨーロッパ人権条約（European Convention for Human Rights）[※187]が、刑事罰等に関する国内法に適用されうる現状を変えたい、としている。一方EUは、第三国に対し、法執行・司法については犯罪者情報の共有等で緊密に連携することを求めており、また第三国となる英国が他の第三国より多くの権限を持つようなことは避けたい、としているため、難しい交渉が予想される。

(b) 国外の防衛

国外の防衛について、EUはテロ対策、平和維持等の目的のため、共通防衛政策（Common Security and Defense Policy）を軍事・非軍事の両面で実践している[※188]。防衛に関してEUは立法権を持たず、必要に応じて加盟国の同意の基に組織が組まれるが、EU離脱後の英国のコミットメントが焦点となっている。英国政府は、防衛に関しては、既存の第三国との関係を超えた緊密な連携関係を維持する、ただしEUとの外交・防衛に関する制度的な連携は求めない、としている。EUも、英国の軍事面でのプレゼンスの大きさから緊密な連携を望んでいるが、同時に、第三国としての軍事情報へのアクセスには限界がある、あるいは外交と防衛は一つのパッケージとして合意する必要があるとし、必ずしも交渉は早期にまとまらない可能性がある。

(c) データの妥当性

データの妥当性とは、英国・EU間の自由なデータ移

転のためにデータ保護を保証することであり、特にEUから英国へのデータ移転において、GDPR（General Data Protection Regulation）に相当する英国の保護施策を取り決める必要がある（十分性の認定）。英国はGDPR遵守のために国内法の整備を完了しており、その点で問題は少ないと思われる。ただし、テロ対策を目的とする英国の調査権限法（Investigation Powers Act 2016）※189が電子メール監視等の点でGDPRにそぐわない、とする懸念がEU側に存在し、争点となりうる。

(d) サイバーセキュリティ

前述の英国議会下院の公開文書では、サイバーセキュリティに関する交渉への具体的な言及がなく、直近の課題とはみられていない。実際、英国はEU域内の重要インフラセキュリティ対策を規定するNIS指令（Network Information Security Directive）に準拠した国内法の整備を終えている※190。またNCSCのCiaran Martin CEOは2018年の時点で「英国・EUのサイバーセキュリティは2国間・多国間の連携」で担保されている、と述べている※191。その一方で、欧州委員会（EC：European Commission）のBrexit首席交渉官Michel Barnier氏は、英国とEUは特にサイバーセキュリティの新しい脅威に対して緊密に連携を取る必要がある、としている※192。もしEU離脱で課題があるとすれば、英国・EU間のセキュリティ人材の移動ではないか、とする意見もあるが、これに関しては2020年2月以降の新型コロナウイルス感染拡大で世界各国に影響が出ている可能性があり、推移を見守る必要がある。

(2) GDPR実施の状況

2018年5月のGDPR発効から1年以上を経過し、欧州ではGDPR違反の摘発が本格化している。

2019年7月8日、英国の個人データ保護監督機関（ICO：Information Commissioner's Office）は、British Airwaysに対し、2018年のサイバー攻撃により詐欺サイトが悪用され、顧客情報50万件が漏えいした事案について、セキュリティ対策に不備があったとして1億8,339万ポンド（約242億円）の制裁金を課すと発表した※193。更に翌7月9日、ICOはMarriott International, Inc.に対し、系列ホテルのグローバルな顧客情報約3億3,900万人分がシステムの脆弱性で4年以上暴露されていた事案につき、GDPRの注意義務違反があったとして9920万ポンド（約131億円）の制裁金を課した※194。

これらの制裁金はいずれもGDPRの上限には遠いが巨額であり、運用の「試用期間」を終えた監視機関は制裁の執行を躊躇しない、という事例となった※195。ただし、制裁対象の2社はともに不服を申し立て、2020年4月時点で最終決定には至っていない。

このほか、2019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。

2019年10月23日、オーストリアの個人データ保護監督機関Datenschutzbehördeは、国営郵便事業者Austrian Postに対し、「政治的な好み」を含む顧客データ220万件の第三者提供がGDPR違反にあたるとして、1,800万ユーロ（約22億円）の制裁金を課すと発表した※196。このデータは顧客の家庭の情報を含み、政党に選挙向けのマーケティング情報、あるいはデータそのものが渡りうるとして2019年当初から国内で批判が高まっていた。Austrian Postは提供したデータを削除すると釈明した※197。

2019年10月30日、ドイツの個人データ保護監督機関であるthe Berlin Commissioner for Data Protection and Freedom of Informationは、不動産事業者Deutsche Wohnen SEに対し、金融資産や給与を含むテナント情報が不必要な期間保存され、また、テナントに削除の機会が与えられなかった、等のアーカイブ管理がGDPR違反であるとして、1,450万ユーロ（約18億円）の制裁金を課すと発表した。同機関は、2017年の査察で既にアーカイブシステムの改修を勧告していたが、これが改められていなかったための制裁措置となった※198。

2020年1月15日、イタリアの個人データ保護機関Garanteは、通信事業者Telecom Italia（以下、TIM）に対し、マーケティング目的の不正なデータ処理がGDPR違反であるとして、2,780万ユーロ（約33億円）の制裁金を課すと発表した。Garanteは、2017年1月から2019年初頭までTIMに関連した迷惑な勧誘電話のクレームを数百件受理しており、中には、TIMが利用者に提供する懸賞が不公正だというクレームもあった。Garanteは制裁金に加え、TIMに対し、勧誘電話を拒否した利用者のデータをマーケティング目的に利用することを禁じる等、20余りの改善策を命じた※199。

(3) EUサイバーセキュリティ法の施行状況

2017年9月にECが提案したサイバーセキュリティ法案は、2018年12月10日に欧州議会（the European Parliament）、理事会（the Council）、ECの三者対話で合意された後、2019年3月12日、欧州議会におい

て正式に承認※200され、同年6月27日にEUサイバーセキュリティ法（EU Cybersecurity Act）※201として施行された※202。

同法により、欧州ネットワーク情報セキュリティ機関（ENISA：European Network and Information Security Agency）はEUサイバーセキュリティ庁（EU Agency for Cybersecurity）に格上げされ、時限的に存在する組織から恒久的機関となった。EUサイバーセキュリティ庁は、EU加盟国、関係機関及び関係団体間の、サイバーセキュリティにおける協力・調整に加え、EU cybersecurity certification framework（EUサイバーセキュリティ認証フレームワーク。以下、認証フレームワーク）を確立し、個々のカテゴリのICT製品、プロセス及びサービスに合わせた、EU内で統一された認証スキームが成立する環境の構築を目指している。この認証スキームにより取得された認証はEU全体で承認され、EU全体のセキュリティレベルを揃えることに寄与する。

(a) 認証フレームワークの構築状況

認証フレームワークについては、2018年2月13日※203、同3月1日※204、同11月20日※205、ブリュッセルにおいて、EUサイバーセキュリティ庁、EU加盟国の関係機関・事業者が集まり、スマートカード、自動車、医療、電力等の産業セグメントにおける認証スキームについて議論を行った。上記の産業セグメントでは、求められる認証スキームの特性がそれぞれ異なるため、各セグメントの知見を持つ開発・利用のエキスパートと、セキュリティ評価・認証の知見を持つエキスパートにより議論が続けられている。この活動は、EUサイバーセキュリティ法に定められたAd hoc WG※206（特定のセグメントにおける認証スキーム立上げを行う時限的なWG）で行われ、cPPP※207（Contractual public-private partnerships：契約に基づく官民連携組織）に基づきECSO※208（European Cyber Security Organization）がサポートしている。ECSOはメタスキームアプローチ※209と呼ばれる、既存の評価・認証結果を複合的に組み合わせる手法を提案している。

2019年11月18～19日にブリュッセルで開催されたカンファレンス（2019 International conference on the EU Cybersecurity Act※210）における、ECCG※211（European Cybersecurity Certification Group）立ち上げ主査の説明によれば、他のポリシーや特定分野のレギュレーションによって強制されない限り、EUサイバーセキュリティ認証の取得は事業者の自主的な判断によるという。一方、EUサイバーセキュリティ認証の認証スキームと重複する、メンバー各国の認証スキームは効力を停止する。

2019年11月の時点では、高い保証レベル（High）の認証スキームの最初の候補として、スマートカード等の欧州のコモンクライテリア（CC：Common Criteria）※212認証スキームが検討されている、とのことである。このほかに検討されている分野として、産業自動制御機器、クラウド認証、5G、IoTが言及されている。

認証フレームワークにおける保証レベルは、前述のHighに加え、Substantial、Basicの三段階があり、Basicレベルでは自己評価の選択肢も用意されている。急速な普及が見込まれているIoT機器については、ユースケースに応じてBasicからSubstantialの広い範囲の保証レベルが想定されている。

(b) プライベート認証に関する議論

前述のカンファレンスにおいては、GlobalPlatform※213、SESIP※214等のプライベート認証についても議論された。認証フレームワークにおいては、「適合規格が標準化機関によって精査・公開されること」及び「試験機関が公的な認定機関による認定を取得していること」が条件となるため、「プライベート認証は生き残れない。」という意見と、「最終的には市場が決めるので生き残る。」という意見の両論が出された。既に特定の産業分野に浸透しているプライベート認証については、今後も様々な議論やアライアンス形成の活動が行われるものと思われる。

(4) 5G導入に関するセキュリティ検討の状況

第5世代移動通信システム（5G）は、次世代の通信・インターネットの基盤インフラとして各国の安全保障・セキュリティにも密接に関わってくる。米国政府はこの観点から、2018年以降、5Gインフラの導入について中国系企業から調達をしないよう欧州に要請してきた。欧州委員会は2019年3月の勧告において、5Gのセキュリティリスク評価は各国が個別に行うこととし、リスクと対策を報告することを求めた※215。

これを受けたEU加盟国は、NIS指令第11条に基づくNIS Cooperation Group※216の活動として評価を実施、2019年10月9日に各国評価を調整した結果を報告した※217。同報告では5G特有の課題として、ソフトウェア依存性の増大による攻撃機会（バックドア等）、アーキテクチャの特性による特定機器・機能の影響の受けやすさ等をあげ、結果としてモバイルネットワーク事業

者・サプライヤへの依存がリスク要因であり、特にサプライヤに対する欧州以外の国からの影響の評価が重要である、とした。並行して EU サイバーセキュリティ庁は、2019 年 11 月、これを補完する形で 5G ネットワークの資産と脅威のマップを公開した※218。

NIS Cooperation Group は更に 2020 年 1 月、上記セキュリティリスクを緩和する共通の対策群（toolbox）とその適用に関するガイドラインを公開し、欧州委員会はこれを推奨（endorse）した※219。この対策群には、技術的な対策のほか、ネットワーク事業者に対するセキュリティ要件の強化、複数のサプライヤの使用、サプライヤのリスク評価、高リスクと見なされた事業者に対する適切な制限措置等が含まれている。

これらの対策は明らかに、中国系サプライヤ（特に Huawei Technologies Co., Ltd. 以下、Huawei 社）とそこから機器を調達するネットワーク事業者の監視強化を狙ったものだが、米国のように完全な調達排除はせず、リスクに見合った段階的導入を可能としている点が重要である。実際、大手ネットワーク事業者 Telefonica S.A. はドイツのモバイル通信ネットワーク運用を Deutsche Telekom AG から請け負っているが、2019 年 12 月 11 日、ドイツの 5G 機器導入に関して Huawei 社との契約を確定させた※220。また EU から離脱した英国政府も、2018 年当時から続く米国の説得に応じず、Huawei 機器の一部導入を公言しており※221、ガイドラインはこれらの動きを追認する形となっていた。

しかし 2020 年にはいり、新型コロナウイルス感染拡大とともに、欧州経済の中国依存政策は大きく見直されつつある。2020 年 1 月の時点で英国の Boris Johnson 首相は、Huawei 機器を導入する代わりに同社の英国内シェアを縮小させる提案に自信を見せていたが、議会の反発により同年 5 月 22 日、Huawei 社の役割を見直すと表明、導入政策は後退に追い込まれた※222。更に前述の Telefonica S.A. が 2020 年 6 月、ドイツの 5G コアネットワークを Huawei 社ではなくスウェーデンの Telefonaktiebolaget LM Ericsson に発注すると発表※223 する等、コアネットワークを欧州の事業者に乗り換える動きが顕著となっている。

この背景には、パンデミックに対する情報提供の遅れや、欧州に対して自国の貢献を大きく見せようとした中国の対応への不信感があるとみられ、EU 各国もサプライチェーンを中国に依存するリスクを真剣に考え出したと思われる。更に、2020 年 5 月 28 日、中国が香港の統制強化のために「国家安全法」の制定方針を採択した※224 ことが加わり、2020 年 1 月まで蜜月とみられていた欧州と中国の関係は大きく揺れ動いている。

2.2.4 アジア太平洋地域でのCSIRTの動向

アジア地域の多くの国では各国の窓口となる National CSIRT が既に設立され、運用が進んでいる。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。一方、南太平洋地域では National CSIRT がまだ存在しない国が多いが、新規設立に向けた動きが近年活発になっている。本項では、アジア太平洋地域における CSIRT の機能強化や新規設立に関する動きと、CSIRT 間の相互連携の実態について述べる。

(1) CSIRT の設立・機能強化の動き

各国・地域の CSIRT の設立、機能強化の動きについて述べる。

(a) 台湾

台湾では、最高行政機関である行政院内に設置された TWNCERT（Taiwan National Computer Emergency Response Team）※225 が中心となり、重要インフラセクターごとに設置された ISAC（Information Sharing and Analysis Center）から提供されるサイバー脅威情報を集約・分析する役割を担っている。

2019 年 1 月には、資通安全管理法（英語名：Cyber Security Management Act）※226 が施行された。同法は、政府機関及び特定の非政府組織が行うべきサイバーセキュリティ対策を明記している。特に政府機関に対しては、一定のサイバーセキュリティ対応能力基準を満たすこと、サイバーセキュリティ担当官を設置してサイバーセキュリティ管理計画を作成すること、定期的に監査を受けること等を義務付けている。また、政府機関がインシデントに関する情報を把握した場合は、所管省庁並びに行政院に報告することも義務付けた。これにより、政府機関がより統一的な基準のもとでサイバーセキュリティ対策を行うことや、TWNCERT が中心となり、より効率的なインシデント対応を行うことが期待されている。

(b) 韓国

韓国政府は、2019 年 4 月に同国初となるサイバーセキュリティ戦略※227 を発表した。この中では、今後国民

や企業及び政府が取り組むべき戦略目標として次の六つの項目を掲げている。
①国家の核となるインフラの安全性の向上
②サイバー攻撃への対応能力の強化
③政府が主体となっての信頼及び協力関係の構築
④サイバーセキュリティ産業が成長するための基盤の構築
⑤サイバーセキュリティ文化の醸成
⑥サイバーセキュリティにおける国際連携の主導

特に②の「サイバー攻撃への対応能力の強化」に関しては、国家安全を侵害するようなサイバー攻撃に能動的に対処することや、攻撃の原因を調査する能力を養成すること等を具体的な目標としている。また、サイバー攻撃や脅威に関する情報を関係組織間で共有・調査・対応する体制の強化、AIを用いたサイバー攻撃の検知、防御等も明記されており、National CSIRTであるKrCERT/CC※228もこうした役割の一端を担うものとみられる。

(c)ニュージーランド

ニュージーランドでは、2019年7月にサイバーセキュリティ戦略が4年ぶりに改訂された※229。2023年までに取り組む重要項目として、次の五つを提示している。
①市民がサイバーセキュリティに関して意識を高め、主体的に取り組むこと
②サイバーセキュリティのための質の高い労働力と強固なエコシステムを作ること
③国際社会において精力的に活動すること
④サイバー攻撃に対して堅固かつ機敏に反応すること
⑤サイバー犯罪への対応に積極的に取り組むこと

特に①の「市民がサイバーセキュリティに関して意識を高め、主体的に取り組むこと」を促すために、同国のNational CSIRTであるCERT NZ※230は、IT技術者向けの情報発信に加えて一般の企業や利用者向けの情報発信に努めている。例えばソフトウェアの脆弱性等の注意喚起情報については、IT技術者向けに技術的な説明を含む詳細な内容を記した文書※231を、一般の利用者向けには平易な言葉で簡素に記載した文書※232をそれぞれ公開している。インシデント報告は、Webサイト上で利用者が簡単な質問に選択式や穴埋めで答える仕組みとなっている。また一般利用者向けWebサイトでは、専門用語を避け、平易な言葉で説明している。このように、多様な層の国民を対象とした啓発の取り組みや、誰でも簡単にインシデントを報告して必要な支援を受けられる仕組みを引き続き提供していくとしている。

(d)南太平洋地域の国々

南太平洋地域では、National CSIRTが設立されていない国が依然として多いものの、National CSIRTの設立を促進・支援する活動が継続して行われている。例えば、APNIC（Asia Pacific Network Information Centre）※233は南太平洋地域への支援を続けており、2019年はナウルやバヌアツでワークショップを開催※234したほか、サモアではクック諸島、キリバス、ソロモン諸島等の近隣諸国も招いて、フォレンジックやネットワーク解析のトレーニングを実施した※235。このように、南太平洋地域ではサイバーセキュリティに関する関心が高まっており、向こう数年で新たなNational CSIRTが各地で誕生することが期待されている。

(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）※236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5月末現在22の国・経済地域の31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。2020年5月現在、TSUBAMEにはAPCERTメンバーを中心に18の国・経済地域から23チームが参加し、観測結果を共有している※237。

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。2019

■図 2-2-1　APCERT オペレーショナルメンバー（2020 年 5 月末現在）

年のサイバー演習は、「企業ネットワークからの情報漏えい」をテーマに実施された※238。同演習には、APCERT のオペレーショナルメンバーのうち合計 20 の国・経済地域から 26 チームが参加した。年次報告書は、APCERT 全体として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※239。

また、2019 年の年次会合は、シンガポールの SingCERT※240 がホストとなり、9 月にシンガポールで開催された※241。同会合では、APCERT の運営方針について議論されたほか、CSIRT 担当者やセキュリティ専門家らが最新のインシデント動向等について活発な意見を交わした。毎年半数が改選となる運営委員会の選挙では、今回新たにスリランカの Sri Lanka CERT|CC※242 が選出された。また、これまで 4 期にわたって議長を務めてきたオーストラリアの Australian Cyber Security Centre※243 が任期満了に伴い退任し、新たにマレーシアの CyberSecurity Malaysia※244 が議長に選出された。

このほか、APCERT では能力開発のための取り組みとして、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ほか、年次会合の場を利用して技術的なトレーニングのワークショップも開催されている。

一方、ASEAN においては、2019 年 10 月に行われた Singapore International Cyber Week においてシンガポール政府が ASEAN-Singapore Cybersecurity Centre of Excellence（ASCCE）を正式に立ち上げた、と発表した※245。このセンターは、ASEAN 地域の政策及び技術を担当する上級実務者向けのサイバーセキュリティに関するトレーニングを提供するほか、アジア地域の CSIRT 間の情報連携を促進させることを目的としている※246。サイバー演習環境用の施設を既に開設したほか、これとは別に 2020 年 4 月には多目的のトレーニングセンターが稼働する予定となっている。また、タイのバンコクには 2018 年に日本政府が出資して 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）※247 が設立され、本格的な運用が始まっている。このセンターは、ASEAN 地域の各国を対象に、実践的サイバー防御演習「CYDER」（Cyber Defense Exercise with Recurrence）や、デジタルフォレンジックのトレーニングを提供している※248。

また、南太平洋地域では、オーストラリア政府が主導する PaCSON（Pacific Cyber Security Operational Network：太平洋サイバーセキュリティオペレーションネットワーク）※249 が 2018 年から活動しており、年 1 回の会合を開催している。PaCSON は太平洋島嶼国の National CSIRT や政府のサイバーセキュリティ担当者

のサイバーセキュリティ能力の向上や、組織間の連携促進を目指している。

このように、アジア太平洋地域の各国がCSIRTの設立や役割強化に動くとともに、APCERTやASEAN等の国際的な団体もCSIRTの活動を後押しする取り組みを進めている。今後、主に南太平洋地域各国で新たなNational CSIRTが誕生することや、地域のCSIRT間の連携がより進むことで、アジア太平洋地域全体のサイバーセキュリティ能力の一層の強化・進展が期待されている。

COLUMN

5Gがもたらす恩恵とプライバシーリスク

移動体通信技術の発展は、これまで人々に多くの恩恵をもたらしてきました。1970年代後半に誕生した1Gが、音声をアナログの電波で通信する規格として自動車電話やショルダーフォン等に採用された後、移動体通信規格は約10年ごとに革新されてきました。2Gではデジタル方式により、音声通話だけでなくメールを始めとしたデータ通信サービスの利用が可能となり、3Gでは高速容量化により、画像や動画コンテンツが充実しました。更に、4Gでは動画配信サービスやモバイルゲームのような大容量コンテンツが充実し、そして2020年についに国内で5G(第5世代移動通信システム)の商用化が始まりました。

株式会社クロス・マーケティングの調査[i]によると、8割程度の人が5Gを「認知はしている」が、その多くは「名前だけ知っている」という状況で「内容まで知っている」人は2割にとどまっているようです。5Gの特徴としては、高速大容量・超低遅延・多数同時接続による通信が可能となることが挙げられます。これにより、あらゆるモノと人がつながるIoT時代のコミュニケーションが加速することが期待できます。例えば、スポーツイベントが開催されるスタジアムで、試合中の選手等をいろいろな角度から撮影し、その映像を同時に端末へ配信することで、利用者が複数の角度から映像を選んで楽しむAR(Augmented Reality:拡張現実)体験ができるようになります。また、医療現場では、医師が遠隔から高精細な映像を遅延なく利用して診察を行う遠隔診察や、医師が手術をしている際に手術映像を配信することで、最適な手術の進め方を遠隔からリアルタイムにサポートする遠隔手術支援等が可能になります。これにより、離島等に住む人が高度な医療サービスを享受することができるようになります。更に、大量に走行する車両に搭載されたセンサーからの膨大なデータを解析し、即座にフィードバックして交通流を制御する自動運転も5G技術の特徴を活かしたサービスとして期待されています。

このように人々の生活に大きなメリットをもたらす可能性のある5Gですが、一方でプライバシーのリスクがあることも忘れてはなりません。ARのようなサービスでは高画質・高精細なカメラ映像がリアルタイムに端末へ映し出され、遠隔診察では患者の診断情報が通信回線を通じてやり取りされることになります。そして、自動運転ではあらゆる場所で端末が自動認証あるいは常時認証され、車両の位置情報が収集されます。5G時代にはこれまで以上に端末から個人情報を収集するサービスが増えていきます。

5Gの時代では、個人のプライバシーを確保する上で、重要な個人情報を誰に対して提供し、どのような目的で使われるのか、一人ひとりが理解を深めて判断していかなければなりません。

i　株式会社クロス・マーケティング:5Gに関する調査　https://www.cross-m.co.jp/report/it/5g20200225/〔2020/7/8確認〕

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。

2.3.1 情報セキュリティ人材の状況

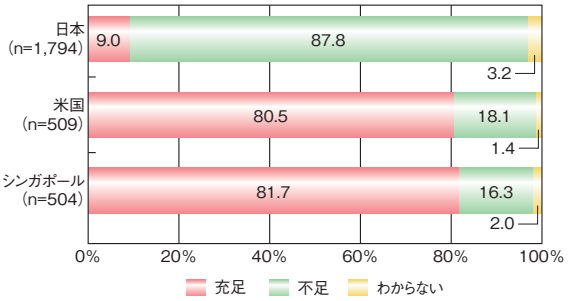
ここ数年来、政府や民間の組織等において国内のセキュリティ人材育成のための活動が行われてきた。経済産業省の 2016 年の調査で「2020 年に国内で 19 万人不足」という予想が発表され※250、その後、セキュリティ人材不足を解消するために、企業においてセキュリティに関わる役割定義や持つべきスキルに関する議論が行われた。また、ユーザ企業、IT ベンダ／セキュリティベンダでセキュリティ関連タスクの概念整理が行われ、ユーザ企業におけるセキュリティ体制については、経営層、戦略マネジメント層、実務者層・技術者層等に整理された。

2018 年度から政府や民間の組織等において、より実際的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、具体的な施策として人材育成を行う試みの有効性に関する検証が行われている。以下にセキュリティ人材に関する課題の現状と、各所で行われている活動の概要を紹介する。

(1) セキュリティ人材不足に関する認識

政府や民間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ているが、現時点でも企業におけるセキュリティ人材不足が解消されている状況にはない。NRI セキュアテクノロジーズ株式会社（以下、NRI セキュアテクノロジーズ社）の「NRI Secure Insight 2019※251」によれば、日本の企業の 9 割近くがセキュリティ対策に従事する人材が不足していると答えており、米国やシンガポールの不足感と比べて非常に高い比率を示している（図 2-3-1）。

8 割が「充足している」と回答している米国では、その理由として、「セキュリティ業務が標準化され、役割分担が明確」が 1 位に挙げられており、シンガポールでは「セキュリティ業務が自動化・省力化されている」が 1 位に挙げられている（表 2-3-1）。



■図 2-3-1　セキュリティ対策に従事する人材の充足状況
（出典）NRI セキュアテクノロジーズ社「NRI Secure Insight 2019」を基に IPA が編集

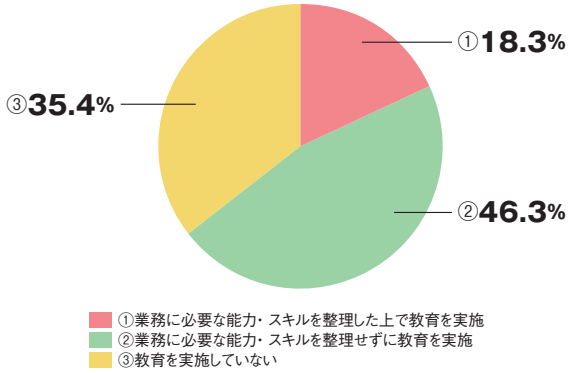
また、日本においては、6 割以上の企業がセキュリティ人材の育成を実施しているが、業務に必要な能力・スキルを整理した上でセキュリティ教育を実施しているのは全体の 2 割弱しかなく（次ページ図 2-3-2）、セキュリティ人材の育成・教育における課題として、適切なキャリアパスの不足を一番の課題として挙げている（次ページ図 2-3-3）。

日本の企業ではセキュリティ関連分野と、各分野の業務に関するタスク及びそれに紐づく能力・スキルが十分に整理されず、人材を効率的にセキュリティ業務に配置できていないことが人材充足感の低さにつながり、また、

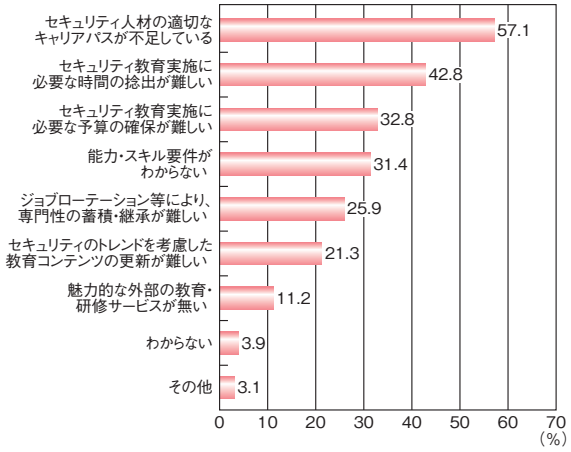
	日本 (n=161)	米国 (n=410)	シンガポール (n=412)
1 位	想定よりも有事対応が少ない	セキュリティ業務が標準化され、役割分担が明確	セキュリティ業務が自動化・省力化されている
2 位	セキュリティ業務の量が少ない	想定よりも有事対応が少ないため	想定よりも有事対応が少ない
3 位	セキュリティ業務が標準化され、役割分担が明確	経験豊富なメンバーで対応	セキュリティ業務が標準化され、役割分担が明確
4 位	経験豊富なメンバーで対応	セキュリティ業務が自動化・省力化されている	セキュリティ業務の量が少ない
5 位	セキュリティ業務を外部委託している	外部から経験豊富な人材を採用している	経験豊富なメンバーで対応

※その他の選択肢：社内・グループ内の異動で人員を補充／その他／わからない

■表 2-3-1　セキュリティ対策に従事する人材が充足していると考える理由
（出典）NRI セキュアテクノロジーズ社「NRI Secure Insight 2019」を基に IPA が編集



■図 2-3-2　セキュリティ人材育成の実施状況（日本、n=1,661）
（出典）NRI セキュアテクノロジーズ社「NRI Secure Insight 2019」を基に IPA が編集



■図 2-3-3　セキュリティ人材の育成・教育における課題（日本、n=1,794）
（出典）NRI セキュアテクノロジーズ社「NRI Secure Insight 2019」を基に IPA が編集

必要な能力・スキルがあいまいなまま人材を評価することでキャリアパス形成が難しい状況になっていると考えられる（セキュリティ関連分野については図 2-3-6 参照）。

(2) 経済産業省及び関連省庁等の取り組み

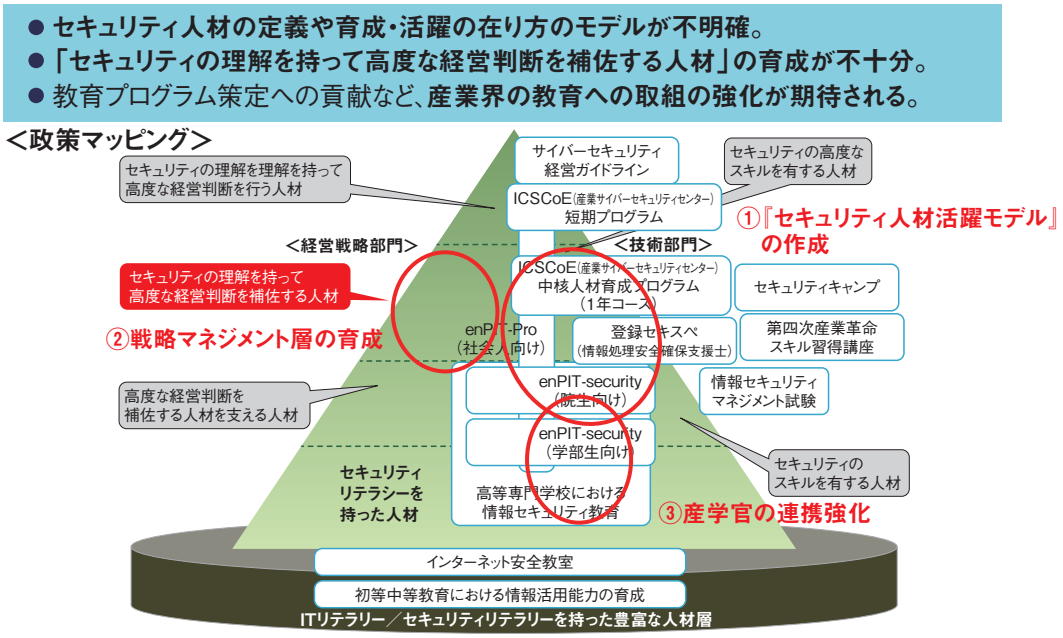
経済産業省は、産業サイバーセキュリティ研究会 WG2 においてサイバーセキュリティ人材育成・活躍促進パッケージとして、セキュリティ人材育成に関わる活動を検討している（図 2-3-4）。

本項では、この WG2 での検討内容を中心に、2019 年度の経済産業省及び関連省庁等のセキュリティ人材育成の取り組みについて述べる。

(a) セキュリティ人材活躍モデル

2019 年度は、日本の企業ではセキュリティ関連分野と各分野の業務に関するタスクが十分に整理されていないとの認識から、経済産業省では「セキュリティ人材活躍モデル」の構築を進めている（図 2-3-5）。

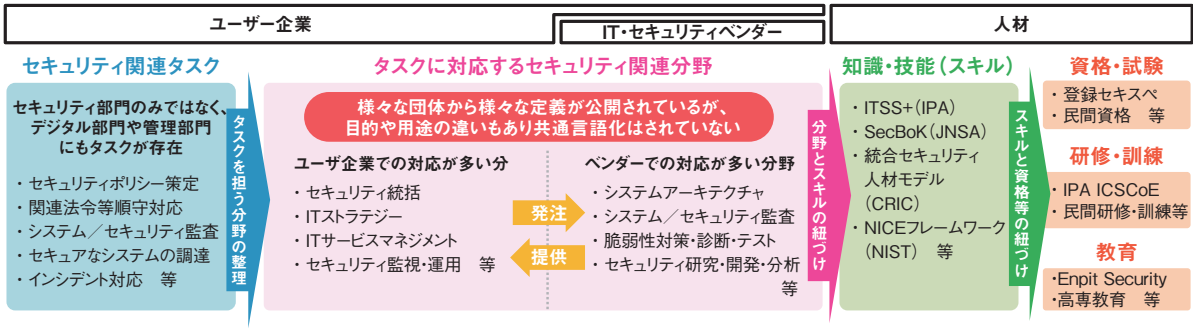
また、「セキュリティ人材活躍モデル」として企業におけるセキュリティ関連分野の概観についても検討している。図 2-3-6 に示すのは、2018 年度に行ったユーザ企業におけるセキュリティ体制・人材に関する概念整理を基に、人材を経営層、戦略マネジメント層、実務者・技術者層に分け、更に典型的な組織例とそれらに紐付けられるタスク例を挙げるとともに、ユーザ企業全体のセキュリティ関連分野を整理したものである（ただし、検討



■図 2-3-4　サイバーセキュリティ人材育成・活躍促進パッケージの全体像
（出典）経済産業省「事務局説明資料※39」（産業サイバーセキュリティ研究会 WG2（経営・人材・国際）第 5 回会合 資料 3）

セキュリティ人材の全体像の可視化や育成・活躍促進のためのモデルの構築

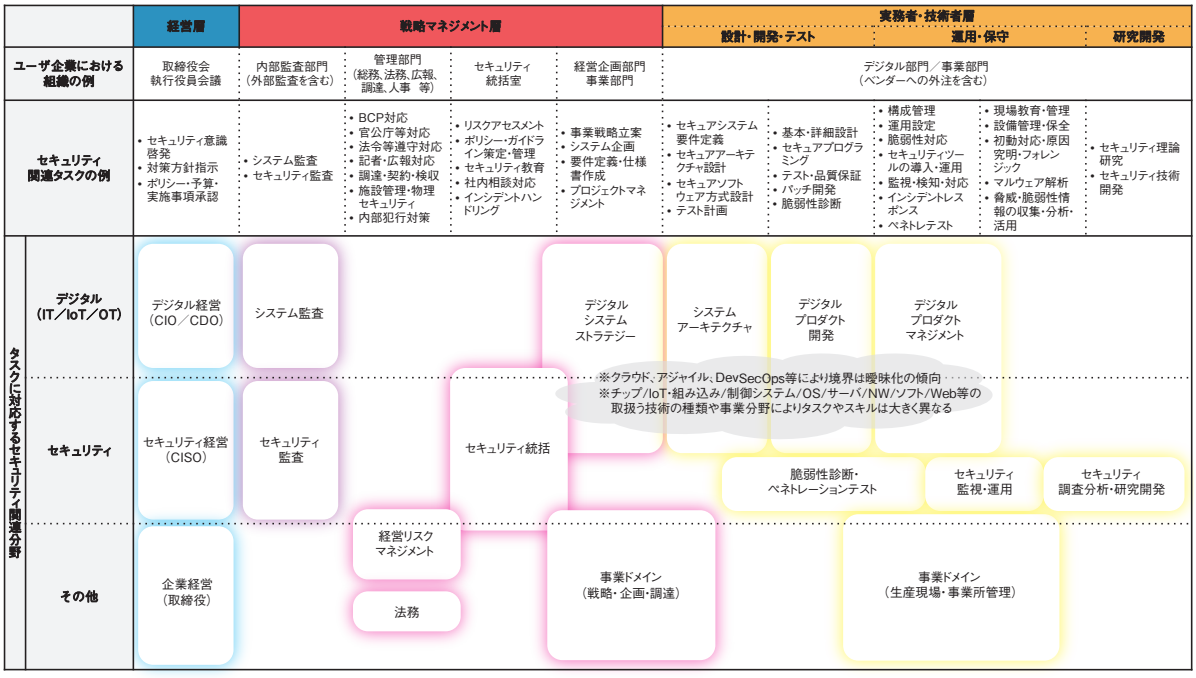
- ITSS+(セキュリティ領域)改定により、各分野に紐づくセキュリティ関連タスク等を整理中。
- その後、各分野に関するキャリアパス事例集や、ユーザ企業における体制・人材確保のプラクティス集等を開発。



■図 2-3-5　セキュリティ人材活躍モデルの構築
(出典)経済産業省「事務局説明資料」(産業サイバーセキュリティ研究会 WG2(経営・人材・国際)第 5 回会合 資料 3)

改訂中のITSS+(セキュリティ領域)におけるセキュリティ関連分野の概観(現状版)

- セキュリティ技術者のみではセキュリティは確保できない。IT/IoT/OT等のシステムの企画・設計・開発・運用・保守を行う人材や、管理部門等の人材にも、セキュリティ関連スキルは必須となってきている。
- こうした観点から、セキュリティ関連分野を以下の通り整理し、各分野に関連する主なタスク等を紐づけ中。



■図 2-3-6　セキュリティ関連分野の概観
(出典)経済産業省「事務局説明資料」(産業サイバーセキュリティ研究会 WG2(経営・人材・国際)第 5 回会合 資料 3)

途中であり、最終的なものではない)。

「セキュリティ人材活躍モデル」の特徴としては、セキュリティ技術者だけではセキュリティが確保できないという議論から、IT/IoT/OT 等のシステムの企画・設計・開発・運用・保守や、管理部門等企業全体をセキュリティ関連分野としてとらえていることが挙げられる。本モデルはそれらセキュリティ関連分野でどのような役割（人材）があるのかを示し、ITSS+[※252](セキュリティ領域)がそれらの役割（人材）の育成の指針となることを目指しており、それに併せて経済産業省では、キャリアパス事例集やユーザ企業の体制・人材確保のプラクティス集の検討を進めている。

(b) 人材育成プログラム

2018 年度から引き続いて、経済産業省及び関連省庁等において戦略マネジメント層の育成、産学官の連携強化の活動、及びリカレント教育におけるセキュリティ人材育成に関わる活動が行われている。

企業のセキュリティ体制において鍵となる戦略マネジメント層の育成については、2018 年に引き続き、IPA の産業サイバーセキュリティセンターが「戦略マネジメント系セミナー」を開催するとともに、東京工業大学の CUMOT（Career Up MOT）が「サイバーセキュリティ経営戦略コース」を開講し強化している（「2.3.2 (2) (d) 戦略マネジメント系セミナー」「2.3.4 (5) サイバーセキュリティ経営戦略コース」参照）。

産学官が協力してセキュリティ人材を育成する活動として、独立行政法人国立高等専門学校機構に対して、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人材育成検討会（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）といった業界団体や企業が 2018 年度に引き続き協力している。具体的には、キャリア教育、講師派遣や教材開発等の活動を行っており、例えば、CRIC CSF は高等専門学校に在籍する非情報系学科の学生に向けたキャリア教育として、ユーザ企業におけるセキュリティや IT の活用を知ってもらうためのビデオ教材の作成を、また、JNSA は情報系学科の学生に向けて、ゲーム形式の教材製作やセキュリティ関連イベント・講習への講師派遣を行っている。

リカレント教育においても、各省庁でセキュリティ人材育成に関する試みが行われている。経済産業省が 2018 年 4 月 20 日に発表した理工系人材需給状況に関する調査の取りまとめ※253 の「現在の業務で必要とする分野と大学で学んだ分野の比較」では学び直しのニーズが明確になっている。機械工学（設計、エンジン、材料、流体等）、ハード・ソフト（OS、アプリ）／プログラム系、通信／ネットワーク／セキュリティ系、データベース／検索系の各分野で、業務で必要だとする割合が、大学で学んだとする割合を大きく上回っており、企業のニーズが高いことが示されている。

また、5 年後に技術者が不足すると予想される分野としても通信／ネットワーク／セキュリティ系が挙げられており、今後は社会人の学び直しの場の充実が重要になってくると考えられる※254。

経済産業省では、IT・データを中心とした将来の成長が強く見込まれ、雇用創出に貢献する分野において、リカレント教育を推進する「第四次産業革命スキル修得講座認定制度」（通称、「Re スキル講座」）※255 を設けている。本制度は、社会人が高度な専門性を身に付けてキャリアアップを図ることを可能とする専門的・実践的な教育訓練講座を経済産業大臣が認定するものであり、現在、認定されている 109 講座のうち、17 講座がネットワーク、セキュリティ分野となっている※256。

また、厚生労働省では、委託事業「教育訓練プログラム開発事業※257」を行っており、その中でセキュリティ関連プログラムが開発されている。

(3) 一般社団法人日本経済団体連合会の取り組み

一般社団法人日本経済団体連合会（以下、経団連）では、2018 年 3 月に公表した「経団連サイバーセキュリティ経営宣言」を推進し、サイバーセキュリティ経営の一層の強化に向けた取り組みとして、2020 年 3 月 17 日に「経団連サイバーセキュリティ経営宣言に関する取組み※258」を提示している。その中で、サイバーセキュリティ人材の現状は、実態把握が十分でなく、組織内で担うべき業務や役割に応じて、スキルや経験を客観的に可視化することが必要であるとしている。

企業におけるサイバーセキュリティ人材が多様であり、前述のように、セキュリティ人材の役割定義に紐付くタスク・スキルを明確にすることが企業にとって課題であると認識されてきたことが背景にあり、経団連では更にそれを可視化することを求めている。「サイバーセキュリティ人材スキルの可視化」による効果として、以下の 3 点を挙げている。

①企業が組織の役割・業務を明確に整理でき、外部リソース及び社内人材の適切な配置が可能となる。
②サイバーセキュリティ人材のスキルが可視化され、目標とする将来像とのギャップが把握でき、キャリアパス設計が容易になる。
③仮に企業が自社のサイバーセキュリティの組織体制や人材構成について公表した場合、取引先や投資家が、人材の質（スキル）と量（人数）から当該企業のサイバーセキュリティ耐力を推量することができる。

また、人材スキル評価ツールとして、以下を参考としてあげ、様々な産業界の活動と連携して取り組んでいる。

- CRIC CSF：
  「人材定義リファレンス※259」

「OT セキュリティ人材スキル定義リファレンス※260」

- 情報セキュリティ教育事業者連絡会（ISEPA：Information Security Education Providers Association）：
  「セキュリティ業務を担う人材のスキル可視化ガイドライン（β版）※261」

(4) まとめ

セキュリティ人材育成は、単に不足しているという議論から始まった。その後、どのような人材が必要かという議論に進み、組織におけるセキュリティの役割の整理が行われた。

更にそれらの役割を機能させるために必要な考え方・体制はどういうものであるかの議論から、セキュリティ統括機能やユーザ企業と各種ベンダとの役割分担等、ユーザ企業でのセキュリティ関連組織の在り方の整理が行われてきた。

現時点では、組織のセキュリティに関連する役割や領域に紐付けられた知識・技能（スキル）の検討が行われている。それに併せて、資格・試験の改定、研修・訓練、教育等の様々な活動が進み始めている。

今後は、組織のセキュリティ人材育成・キャリアパス形成を、企業経営や組織運営のリスクマネジメントや内部統制の観点で包括的に検討することが重要である。

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※262 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。

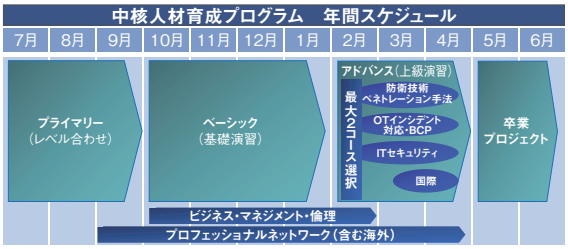
ICSCoE では、重要インフラや産業基盤のサイバーセキュリティリスクに対応する人材・組織・システム・技術を生み出していくため、「人材育成事業」「制御システムの安全性・信頼性検証事業」「攻撃情報の調査・分析事業」の三つを事業の柱としている。本項では、「人材育成事業」について述べる。

(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 名が参加し、2019 年 7 月に開講した第 3 期では、電力・自動車・鉄道・化学・放送・通信・産業ベンダ等の幅広い業界から 69 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。3 年目となる 2019 年度は、「アドバンス（上級演習）」において選択可能な演習を追加して複数コースを選択できるように見直しを実施した（図 2-3-7）。



■図 2-3-7　第 3 期中核人材育成プログラムの年間スケジュール

2019 年 9 月の海外派遣演習では、フランスにてセキュリティ専門家によるサイバーレジリエンスの強化を目的とした研究の講義を受講し、自動運転や鉄道制御の模擬システムを見学した。同年 12 月の海外派遣演習では、英国にて政府・自動車業界・海運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に関する講義を受講した。

また 2019 年 9 月には、米国政府と連携して制御システムのサイバーセキュリティ対策に関する「インド太平洋地域向け日米サイバー演習」を経済産業省と共催した※15。本演習には第 3 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 35 名が参加し、米国の有識者による講演に加え、各国での制御システムセキュリティに関する課題や対策を参加者間で共有するワークショップ

を実施し、国境を越えた積極的な意見交換がなされた（ASEAN・インドとのサイバー連携については「2.2.1 (5) (c) ASEAN 諸国向けの演習・インドとの連携」参照）。

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※263」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 2019 年 11 月には、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開催された。第 1 期及び第 2 期の修了者に加え、2020 年 6 月に修了した第 3 期生も叶会へ参加しており、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、中核人材育成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※264。

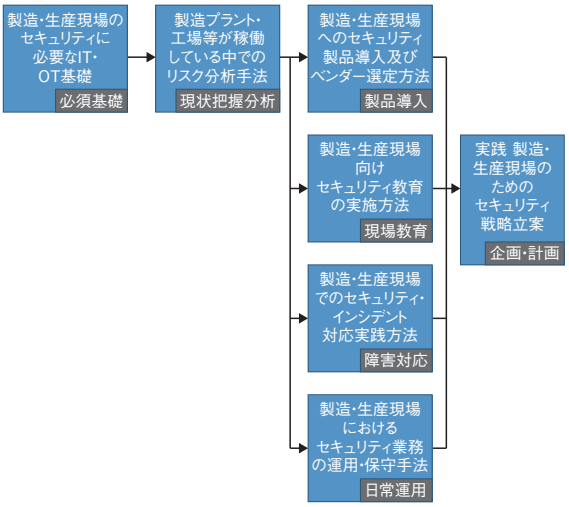
(2) 短期プログラム

ICSCoE では、セキュリティに関連するスキルの習得機会が十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・生産分野の管理監督者層向けプログラム」「サイバー危機対応机上演習（旧名称、国際トレーニング）」「業界別サイバーレジリエンス強化演習（旧名称、業界別トレーニング）」「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」を実施している。

(a) 製造・生産分野の管理監督者層向けプログラム

制御系システムの企画・導入・運用・保守を行う部署や、製造・生産に使用する設備を担う部署の管理監督者向けのトレーニングとして、「製造・生産分野の管理監督者層向けプログラム※265」を 2019 年度に新設した。

具体的には、ICSCoE が第 2 期中核人材育成プログラム受講者とともに、セキュリティ向上における組織の課題を調査・分析した結果に基づき、上記の部署、及び現場の QC（Quality Control：品質管理）、カイゼン、KY（Kiken Yochi：危険予知）活動に取り組む部署等の管理監督者の能力育成のため、7 種の研修コースを実施した（図 2-3-8）。



■図 2-3-8　製造・生産分野の管理監督者層向けコース体系図

本プログラムを通じて、製造・生産現場のセキュリティに必要な IT・OT の基礎知識からセキュリティ戦略立案まで、現場が主体的に取り組むためのマネジメントスキルを身に着けることが期待される。

(b) サイバー危機対応机上演習（CyberCREST）

2019 年 11 月及び 2020 年 2 月に「サイバー危機対応机上演習（CyberCREST：Cyber Crisis RESponse Table top exercise）※266」を実施した。本演習では、制御システムを有する企業・団体のサイバーセキュリティ対策の統括責任者を対象とし、米国サイバー軍の退役軍人や重要インフラ関連企業のサイバーセキュリティ対策責任者等が講師やファシリテーターとなり、講義や演習を行った。

演習においては、東京 2020 オリンピック・パラリンピック競技大会を想定したサイバー攻撃のシナリオを基に、受講者は CISO（Chief Information Security Officer）や広報担当、事業部門長等の役割に扮して経営判断まで含めたプロセスを疑似体験した。講師が扮するステークホルダとの対話を通じて実践的なインシデント対応のフレームワークを学習するとともに、参加企業に合わせたインシデント対応（IR：Incident Response）計画や机上演習（TTX：Table Top Exercise）シナリオの作成方法についても理解を深めた。

本演習を通じて、経営者の判断をサポートするためのリスク分析、迅速かつ適切な対策の提示、政府機関やマスメディアを含む様々なステークホルダとのコミュニケーション等、CISO 等がインシデント対応時に求められる役割について理解を深め、実践につなげることが期待さ

れる。

(c) 業界別サイバーレジリエンス強化演習（CyberREX）

2019 年 8 月及び 9 月に電力、鉄道、ビル、自動車（製造部門）、ファクトリーオートメーション業界において CISO 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て、「業界別サイバーレジリエンス強化演習（CyberREX：Cyber Resilience Enhancement eXercise by industry）※267」を実施した。

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。

(d) 戦略マネジメント系セミナー

2020 年 2 月に、セキュリティに関する方針・戦略・計画及び組織体制を策定する管理職向け、及びセキュリティ対策の実装・運用やセキュリティ体制の構築を担当する実務者向けの 2 コース構成で「戦略マネジメント系セミナー※268」を実施した。

NISC が提唱する「戦略マネジメント層」、及び経済産業省において示された「セキュリティ統括機能」の考えに基づき、サイバーセキュリティは経営課題であること、及び経営層を始めとする関係者が認知しておくべきセキュリティ機能の重要性を理解することを目指し、サイバーセキュリティ有識者の実務経験に基づく講演や、Society 5.0、DX 等の環境変化を踏まえた上で事業継続及び発展を実現するためのサイバーセキュリティ対策について講義を実施した。

(e) 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人材を対象とした実務者向けプログラムとして、「制御システム向けサイバーセキュリティ演習※269」を 2019 年度に新設し、東京、名古屋、大阪で開催した。

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の契機や手法、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実施した。

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。試験は年 2 回実施され、2019 年度の応募者数は 3 万 6,679 人であった※270。

同試験は、業種や組織を問わず、部門内で個人情報を取り扱う担当者や外部委託担当者、情報システム担当者等を主な対象者としている。2019 年度の受験者のうち 85.5%を社会人が占めている。更に業種別に見ると、IT 系企業が 52.6%、非 IT 系企業が 47.4%と、非 IT 系企業が半数近くを占めている。非 IT 系企業の業種も、製造業、サービス業等、幅広い業種の人が受験していることから、広く組織の情報セキュリティを推進する人材の強化に有効な試験と考えられていることがうかがえる※271。

(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は、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名称独占資格である。試験は年 2 回実

■図 2-3-9　登録セキスペのロゴマーク

施され、2019 年度の応募者数は 4 万 3,412 人であった。また、情報処理安全確保支援士の登録人数は、2020 年 4 月 1 日時点で 2 万 413 人となった※272。図 2-3-9 は、情報処理安全確保支援士の資格保有者（以下、登録セキスペ）、またはその所属企業・組織のみが使えるロゴマークである。

登録セキスペには法定講習の受講が義務付けられており、最新知識や実践的な能力の維持が求められる。法定講習は毎年 1 回のオンライン講習と 3 年に 1 回の実践講習からなり※273、受講者からは、「資料での学びに加え、経験者の意見を聞きながら、インシデント対応を体験できた」「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※274。

ユーザ企業においては、事業とのバランスを取りながら、セキュリティを担保する役割を登録セキスペに担わせることで、IT を活用した事業促進をセキュアに進めることができる。IT ベンダ企業においては、登録セキスペが在籍することで、提供する機能やサービスの信頼性向上、社会的評価・信頼の向上、入札要件の充足等によるビジネスチャンスの拡大等のメリットが期待できる。本制度を活用している企業・組織へのインタビューでは、「セキュリティを任せたいとお客様に考えていただくには、信頼が必須であり、情報処理安全確保支援士制度は信頼を頂く枠組みの 1 つとして活用している」「情報セキュリティにおける社員の共通言語や、共通の認識・理解・レベルを作るために、情報処理技術者試験・情報処理安全確保支援士制度を活用している」といった声が上がっている※275。

なお、2020 年 5 月に「情報処理の促進に関する法律」の改正法が施行され、次の 2 点が変更になった※276。

・更新制の導入
・義務講習の実施事業者の追加

「更新制の導入」により、更新手続きを通じて、登録セキスペの登録情報の変更や、欠格事由に該当していないことを確認することができ、本制度の信頼性が向上する。また、これまで義務講習の対象は IPA が実施するものに限られていたが、一定の条件を満たした民間事業者等が実施する講習も対象に追加されたことで、登録セキスペの多様なニーズに応じることができる。

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・キャンプ協議会と IPA が運営している。

2019 年 8 月 13 ～ 17 日に東京で 16 回目となる全国大会が開催され、76 名が参加した※277。また、主に若年層を対象としたセキュリティ・ミニキャンプも、セキュリティ人材育成に関心の高い地域（福岡／山形／山梨／愛知／北海道／広島／石川／沖縄／長崎）で開催された※278。更に、中学生を対象としたジュニアキャンプが高知で開催された※279。

その他、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に、更なる育成の場として、セキュリティ・ネクストキャンプが全国大会と同時に開催された※280。

一般社団法人セキュリティ・キャンプ協議会は、キャンプ修了生の情報セキュリティに関連する取り組みをテーマとしてプレゼンテーションを行う場を設け、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・キャンプアワードも例年開催している※281 が、2020 年 3 月に予定されていた最終選考及び表彰式は新型コロナウイルスの影響で延期となった※282。また、2019 年 1 月に始まった Global Cybersecurity Camp の第 2 回が 2020 年 2 月 10 日～ 14 日に千葉県で開催され、日本を含めて七つの国・経済地域から 29 名が参加した※283。

(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、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 2016 年度（同年度は準備期間の位置付け）から、学部生を対象とした事業「第 2 期 enPiT」（以下、enPiT2）を開始している。

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。セキュリティ分野では、2019 年度は大学等 41 校、連携企業等 43 社・団体が参加した。このうち、東北大学を中核とした 14 の大学が、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 コースを運営しており、323 名が修了認定を取得した※284。

上記以外では、社会人を対象に情報科学技術分野を中心と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 が 2017 年度に開始されている※285。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、enPiT-Pro Security※286 というプロ人材育成のための教育コースを幅広く展開している。

(3) SECCON 2019

JNSA は、日本における最大規模の CTF※287 大会である「SECCON 2019※288」を開催した。

2019 年 12 月 21 ～ 22 日の国際決勝大会では、64 ヵ国 799 チームの中からオンライン予選を勝ち抜いた 11 チームと、特別招待枠 3 チームの計 14 チーム（日本 4、韓国 2、中国 2、ロシア 1、ウクライナ 1、ポーランド 1、台湾 1、タイ 1、EAST ASIA チーム（東アジア連合チーム）1）が集まり、実力を競い合った。第 1 位（経済産業大臣賞）を獲得したのは日本チーム「NaruseJun」、第 2 位が韓国チーム「CodeRed」、第 3 位が中国チーム「Blue-Lotus」であった※289。

SECCON ではその他、CTF 未経験者でも参加可能な「SECCON Beginners※290」や、情報セキュリティに興味がある女性を対象とした「CTF for GIRLS※291」等のイベントを定期的に開催しており、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に取り組んでいる。

(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。2019 年度も昨年度に引き続き、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、インターンシップの受け入れを検討している企業との交流の場を提供する「産学情報セキュリティ人材育成交流会～これからの IT 人材のキャリアを考える－サイバーセキュリティの視点から－」を 2019 年 4 月 27 日に開催した。2019 年度は企業 17 社がインターンシップを実施した※292。

(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 2020 年 1 月、MOT（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※293。ここで育成を目指すのは、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であり、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、サイバーセキュリティ経営の経験を持つ産学官の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 14 回の講義で構成される。

2.4 組織・個人における情報セキュリティの取り組み

企業や政府、地方公共団体、教育機関、一般利用者の情報セキュリティの対策状況について、IPA による調査結果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

情報セキュリティへの企業等の対策状況、経営層の課題認識、CISO 等の役割やセキュリティリスクマネジメントへ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経営層・CISO 等の取り組み状況

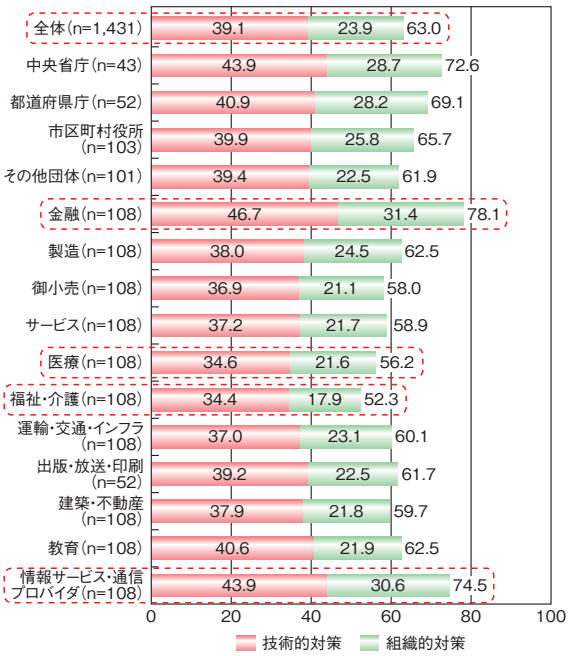
近年、企業経営においては、IT を活用した「攻めの経営」と情報資産やシステムを保護する「守りの経営」とを高いレベルで両立することが求められている。このためには、経営方針に基づき、セキュリティに関して企業内の調整や実務者層をリードする人材（CISO 等）、及び同方針に基づいた技術的・組織的なセキュリティ対策の実践が必要とされている。このような背景を踏まえ、企業の情報セキュリティ対策状況について、以下の資料を基に述べる。

- IPA：企業の CISO 等やセキュリティ対策推進に関する実態調査※294（国内の CISO 等を任命している企業 534 社を対象に調査。以下、IPA 実態調査）
- トレンドマイクロ株式会社（以下、トレンドマイクロ社）：法人組織におけるセキュリティ実態調査 2019 年版※295（国内企業 1,132 社及び官公庁自治体 299 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社：NRI Secure Insight 2019（国内・海外企業 2,807 社を対象に調査。以下、NRI セキュアテクノロジーズ社調査）

(a) 業界ごとのセキュリティ対策状況

トレンドマイクロ社調査（図 2-4-1）によると、調査対象全体のセキュリティ対策包括度スコア※296 は 63.0 点となっており、業種別で見ると、「金融」が 78.1 点でトップ、「情報サービス・通信プロバイダ」が 74.5 点で続く。金融情報を扱う金融業界では技術的対策・組織的対策の両軸で対策が進んでいることが分かる。また、「情報サービス・通信プロバイダ」においても様々な情報をオンラインで取り扱うことから、セキュリティ対策が進んでいることがうかがえる。

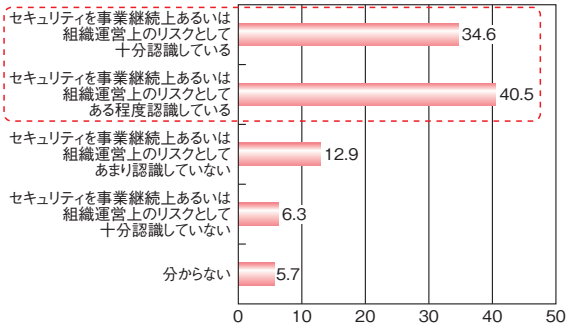
一方、スコアが最も低かったのは「福祉・介護」の 52.3 点で、「医療」が 56.2 点で続く。いずれも患者の医療情報や要介護者の機微情報等を取り扱っており、本来であれば高いセキュリティが求められる業種にもかかわらず、情報セキュリティの観点では他業種に遅れをとっている状況が浮き彫りとなっている。



■図 2-4-1　セキュリティ対策包括度スコア（業種別）
（出典）トレンドマイクロ社「法人組織におけるセキュリティ実態調査 2019 年版」を基に IPA が編集

(b) 経営層のセキュリティに対する意識

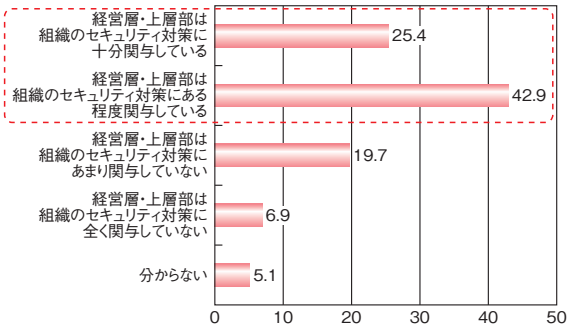
情報セキュリティに関する経営層・上層部のリスク認識について、トレンドマイクロ社調査（図 2-4-2）によると、



■図 2-4-2　情報セキュリティに関する経営層・上層部のリスク認識（n=1,431）
（出典）トレンドマイクロ社「法人組織におけるセキュリティ実態調査 2019 年版」を基に IPA が編集

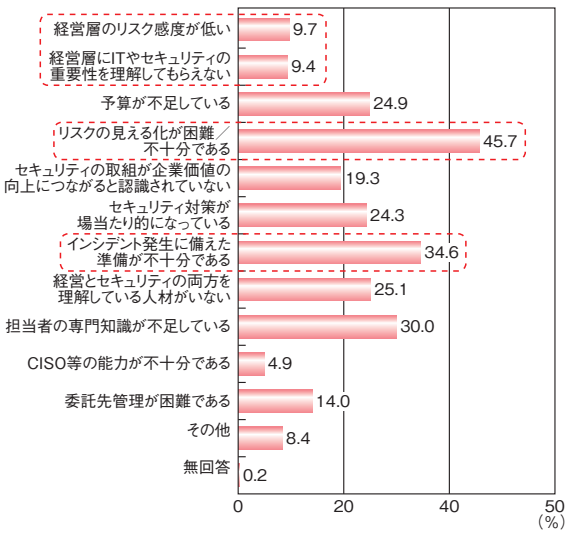
セキュリティを事業継続上あるいは組織運営上のリスクとして認識している経営者の割合は 75.1% と高い割合となり、昨年調査の 70.2% から 4.9 ポイント増加した。

また、図 2-4-3 に示すように、経営層・上層部のセキュリティ対策への関与について「十分関与している」「ある程度関与している」と答えた割合は合わせて 68.3% となっており、図 2-4-2 のリスク認識に比べてやや割合は低いものの、経営層の約 7 割がセキュリティに関与している状況がうかがえる。



■図 2-4-3　セキュリティ対策に関する経営層・上層部の関与度（n=1,431）
（出典）トレンドマイクロ社「法人組織におけるセキュリティ実態調査 2019 年版」を基に IPA が編集

企業の課題認識について、IPA 実態調査（図 2-4-4）によると、CISO 等を任命している企業では、「リスクの見える化が困難／不十分である」（45.7%）が最も多く、次いで「インシデント発生に備えた準備が不十分である」（34.6%）が多かった。これらの課題解決、対策強化の取り組み事例としては「2.4.1 (2) (a) スモールスタートでのリスク把握」「2.4.1 (2) (b) 業務に即したインシデント対応

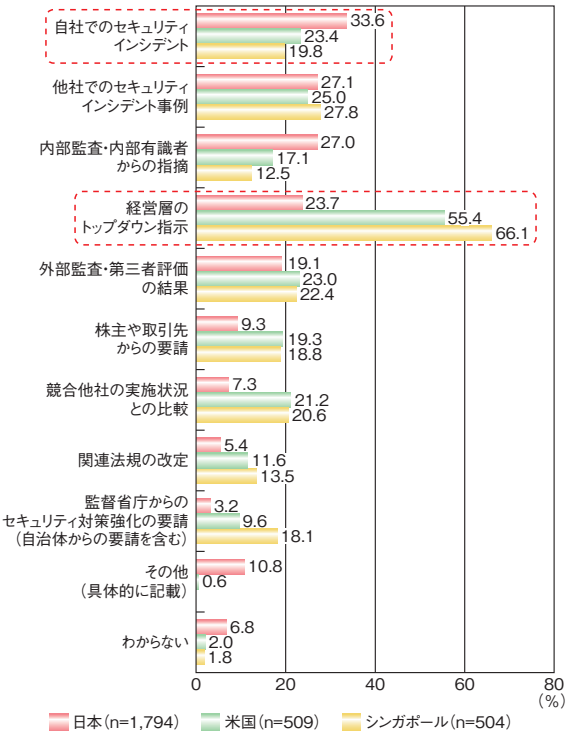


■図 2-4-4　サイバーセキュリティに関する企業の課題認識（n=534）
（出典）IPA「企業の CISO 等やセキュリティ対策推進に関する実態調査」を基に IPA が編集

演習や訓練」を参照いただきたい。

一方、「経営層のリスク感度が低い」や「経営層に IT やセキュリティの重要性を理解してもらえない」と回答した企業はそれぞれ約 10%にとどまり、当該企業の多くの経営層は、リスク把握やセキュリティの重要性を認知・理解していることがうかがえる結果であった。

過去 1 年間で実施したセキュリティ対策のきっかけや理由について、NRI 社が日本・米国・シンガポールにおいて同時期に実施した調査（図 2-4-5）によると、日本企業では「自社でのセキュリティインシデント（事件・事故）」（33.6%）がトップであったのに対して、米国とシンガポールの企業では「経営層のトップダウン指示」（米国企業 55.4%、シンガポール企業 66.1%）がトップであった。日本企業は、インシデントの発生をきっかけにセキュリティ対策を実施するという、後手に回った対応が多いとみられる。本調査では、デジタルトランスフォーメーション（通称、DX）やサイバーセキュリティ等、企業を取り巻く環境が目まぐるしく変化する中で、今後は、セキュリティ分野における経営のリーダーシップを向上させ、先を見据えた対策を打っていく必要があるとしている。

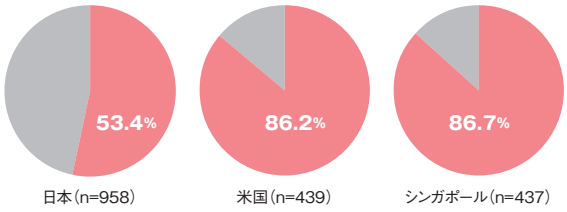


■図 2-4-5　過去 1 年間で実施したセキュリティ対策のきっかけ
（出典）NRI セキュアテクノロジーズ社「NRI セキュア、『企業における情報セキュリティ実態調査 2019』を実施～ DX の推進に向けて、セキュリティ対応の意識・行動改革が求められる日本企業～※297」を基に IPA が編集

(c) 企業のセキュリティ体制

企業におけるセキュリティ関連役職者の設置状況につ

いて、NRI セキュアテクノロジーズ社調査（図 2-4-6）によると、CISO を「設置している」と答えた企業が日本は 53.4% だったのに対して、米国は 86.2%、シンガポールは 86.7%であった。

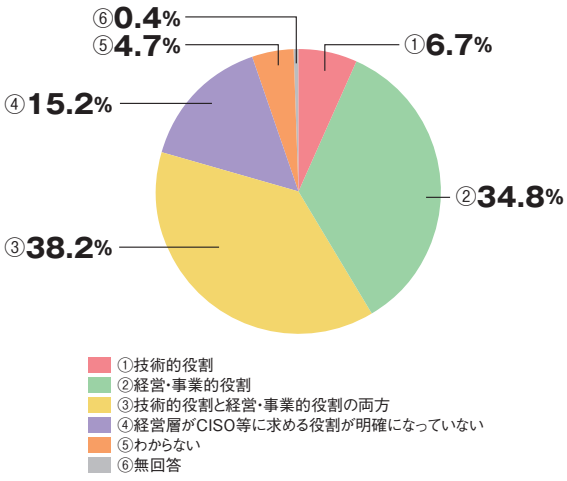


CISOの属性とその割合

	経営層	非経営層	社外有識者
日本（n=958）	70.3%	28.7%	1.0%
米国（n=439）	68.1%	26.2%	5.7%
シンガポール（n=437）	57.2%	34.1%	8.7%

■図 2-4-6　CISO を設置している企業
（出典）NRI セキュアテクノロジーズ社「NRI Secure Insight 2019」を基に IPA が編集

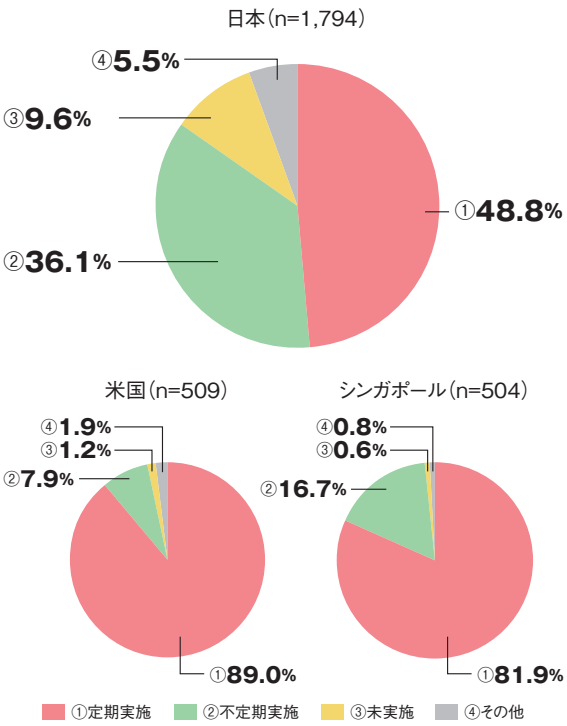
IPA では経営層が CISO 等に対して「経営・事業的役割」と「技術的役割」のどちらを求めているかを調査した（図 2-4-7）。その結果、「技術的役割」のみを求める割合は最も低く 6.7% であったのに対して、「経営・事業的役割」（34.8%）、「技術的役割と経営・事業的役割の両方」（38.2%）と「経営・事業的役割」を重視していることが分かった。日本企業において、CISO 等には技術的役割に加え、経営・事業的役割が求められていることがうかがえる。



■図 2-4-7　経営層が CISO 等に求める役割（n=534）
（出典）IPA「企業の CISO 等やセキュリティ対策推進に関する実態調査」を基に編集

(d) 企業のセキュリティ対策評価実施状況

NRI セキュアテクノロジーズ社調査（図 2-4-8）によると、セキュリティ対策評価（リスク評価）を定期的に実施する企業の割合は、米国が約 90%、シンガポールが約 80% である一方、日本は 50% に満たない結果となった。NRI セキュアテクノロジーズ社調査では、海外ではリスク評価を徹底し、評価結果に応じた合理的・効率的な対策を重視する考え方が根付いていると分析している。



■図 2-4-8　セキュリティ対策評価の実施状況
（出典）NRI セキュアテクノロジーズ社「NRI Secure Insight 2019」を基に IPA が編集

(e) まとめ

以上のように、国内企業における経営層のセキュリティリスク認識やセキュリティ対策への関与の度合いは高く、セキュリティに対する課題認識も持っているが、海外と比較すると経営層のセキュリティへの課題認識はあるものの、リスク評価等の具体的な取り組みに対応できていない状況である。

一方、企業のセキュリティ体制については、CISO 等に対してセキュリティ専門家としての技術的役割のみを期待する企業等は少なく、技術と経営・事業的な役割を合わせ持つことが期待されている。

今後は、企業の経営層はこれまで以上に CISO 等と連携してセキュリティリスクマネジメントを強化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

本項では、リスクマネジメントにおいて重要なリスクの把握、インシデント対応、情報共有、及びセキュリティ対策状況の可視化について述べる。リスクの把握、インシデント対応、及び情報共有については、IPA 実態調査、「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※298」(以下、IPA プラクティス集)、「IT システム・サービスの業務委託契約書見直しに関する調査※299」から、セキュリティ対策の取り組みについての調査結果を紹介する。また、対策状況の可視化については、「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※36」を紹介する。

(a) スモールスタートでのリスク把握

セキュリティへの経営者の取り組み姿勢は重要であり、自社のリスクを数値化しセキュリティの重要性の理解を深めていくことはセキュリティ対策強化に有効である※300。しかし、IPA 実態調査では、CISO 等がいる組織においてもセキュリティに関する事業リスク評価が未実施である割合は 53.4% であり、リスク評価の実施に何らかの難しさがあると推察される。IPA 実態調査で行った有識者ヒアリングでは、「初めから網羅性を目指さず、重要度の高い領域からスモールスタートで取り組みを始めることが肝要である」との知見が得られ、企業ヒアリングにおいても「リスクベースアプローチでリスクが高い領域から優先的に対策を実装する」等の取り組み事例が見られた。

リスクの把握のためには、守るべきシステムや情報資産を特定することが必要であるが、自社の IT システムについて網羅的な情報資産の洗い出しが困難な場合がある。こうした場合、スモールスタートの取り組みとして、リスクが高い攻撃手法とシステムの組み合わせを特定し、優先的に対策することが考えられる。IPA プラクティス集にまとめられた手順は以下のとおりである。

①重要度が高い情報資産に対して身近・手軽なツールを用いて、リスクアセスメントを実施する※301。
②同業他社等で発生したインシデントをリストアップし、自社の情報資産への被害発生可能性を特定※302 する。
③情報資産の重要度と攻撃手法の被害発生可能性からリスク値を算定し、リスク値の高い攻撃手法とシステムの組み合わせを決定する。

なお、①及び②の情報資産に対するリスク分析には、IPA の「中小企業の情報セキュリティ対策ガイドライン 第 3 版※302」及び付録 7「リスク分析シート※301」(図 2-4-9) も活用できる。

媒体・保存先	個人情報の種類			評価値			重要度	保存期限	登録日	現状から想定されるリスク（入力不要・自動表示）				
	個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性				脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性 ※「対策状況チェック」シートに入力すると表示		被害発生可能性	リスク値
事務所PC	有			2	0	0	2		2016/7/1	3 通常の状態で脅威が発生する（いつ発生してもおかしくない）	2 部分的に対策を実施している	2	可能性：中	4 リスク大
書類	有			2	2	2	2		2016/7/1	2 特定の状況で脅威が発生する（年に数回程度）	2 部分的に対策を実施している	1	可能性：低	2 リスク中
書類		有		2	2	1	2	5年	2016/7/1	2 特定の状況で脅威が発生する（年に数回程度）	1 部分的に対策を実施している	1	可能性：低	2 リスク中
事務所PC			有	2	2	1	2	7年	2016/7/1	3 通常の状態で脅威が発生する（いつ発生してもおかしくない）	2 部分的に対策を実施している	2	可能性：中	4 リスク大

■図 2-4-9　リスク分析シート
(出典) IPA「中小企業の情報セキュリティ対策ガイドライン 第 3 版」の付録7「リスク分析シート」

(b) 業務に即したインシデント対応演習や訓練

IPA 実態調査で行った有識者ヒアリングにおいて、PDCA サイクルの「Check」の取り組みの一つとして、業務に即したインシデント対応演習や訓練が考えられる、という意見が出された。演習シナリオは、必ずしも完成度が高いものである必要はなく、事業部門等関係者の意見を取り入れ、実際のヒヤリハット体験を生かす等により、参加者の関心を高めることができて効果的である。またインシデントについて顧客等、外部に説明するための材料を揃える、インシデント対応経験の豊富なベンダと連携する、等をシナリオに入れることも有効である。業務の実態に即したシナリオによる演習は、参加者の主体性を高め、当事者意識を醸成する効果が期待できる。

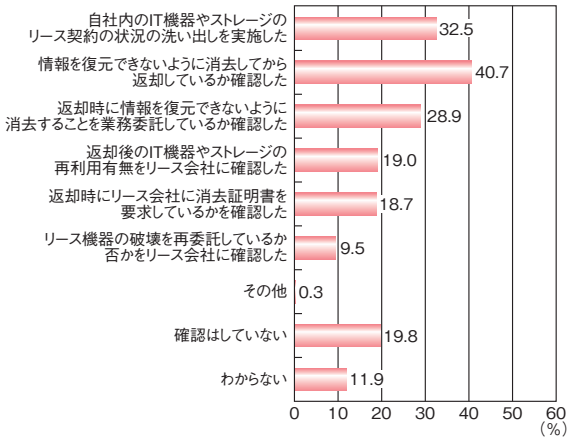
また、演習を通じて、インシデントが自社で生じた場合にどう対応するか考えることにより、「(システム停止等を) 判断する人がわからない」「連絡手段が定まっていない」等の課題点を明らかにしたり、演習で対応に手間取った部門には追加の教育を実施したりすることによって、組織としての対応力強化が期待できる。

(c) 情報の収集・共有活動

同業他社等で発生したサイバー攻撃の手口や利用された脆弱性等インシデントに関する情報を収集するためには、一方的な収集ではなく、コミュニティに参加して情報を共有しあうことも効果的である。IPA 実態調査で行った企業ヒアリングでは、外部のコミュニティ参加者と信頼関係を構築するためには、Give and Take の考え方が重要、という意見が出された。ただし、有益な情報を得るためには必ずしも高度な情報を提供する必要があるわけではない。情報提供は自分の課題を正直に話すという形でもよい。課題の共有でかえって信頼され、情報を得られることもある。それ以外にも、コミュニティ運営の支援やオフライン会議への参加等の貢献が考えられる。また、セキュリティベンダのユーザ会や、同業者以外のコミュニティでの情報共有も有用である。

(d) インシデント情報共有による改善活動

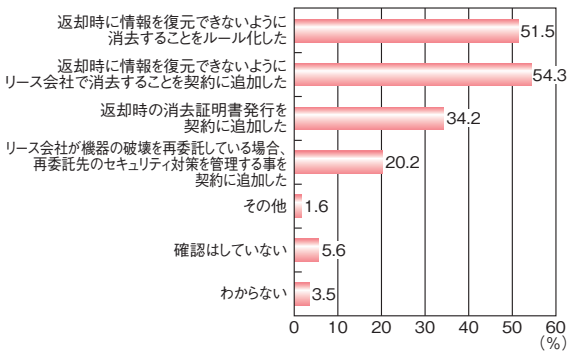
インシデント情報の共有により、セキュリティ対策の見直しを行うことも重要である。2019 年 12 月、リース契約満了により返却されたハードディスクの廃棄を再委託された会社の社員が窃盗・転売し、消去予定であった県の情報が漏えいするというインシデントが発生した※303（「1.2.7 (3) 内部者の不正による情報漏えい」参照）。多くの企業で IT 機器やストレージのリース契約が行われており、データ消去を委託する場合もあることから注目された。IPA による調査では、調査した企業の約 7 割で上記インシデントをきっかけに IT 機器やストレージに関するリース契約内容や情報の取り扱いについて何らかの確認作業が行われていた（図 2-4-10）。



■図 2-4-10　IT 機器やストレージに関するリース契約内容や情報の取り扱いの確認状況（n=911）
（出典）IPA「IT システム・サービスの業務委託契約書見直しに関する調査」を基に作成

更に、何らかの確認作業を行った企業のうち、半数以上がルール化や契約への追加等、管理を強化していた（図 2-4-11）。

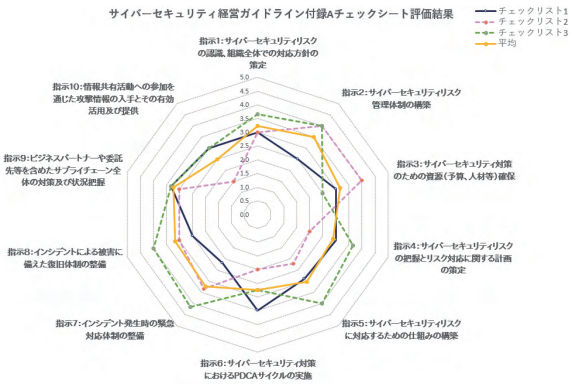
本インシデントはメディアで注目されたこともあり、調査した企業の約 7 割で見直しが実施されたが、メディアに大きく取り上げられないインシデントについても、自社に関係のあるインシデントが発生している場合は、セキュリティ対策の見直しを実施していくことが望ましい。



■図 2-4-11　IT 機器やストレージのリースの契約書の確認や見直し、情報の取り扱いの見直し状況（n=623）
（出典）IPA「IT システム・サービスの業務委託契約書見直しに関する調査」を基に作成

(e) セキュリティ対策実践状況の可視化

リスクマネジメントには、経営層と情報共有できるように状況を可視化することが重要である。経営層がリスクを評価し、最終的な判断ができることを目的とし、IPA と経済産業省は企業のセキュリティ対策実践状況を可視化するためのツールを作成した（図 2-4-12）。本ツールは「サイバーセキュリティ経営ガイドライン」を基にして構成され、経営層に向けたセキュリティマネジメント実施状況の可視化を志向している。企業によるセルフチェックを想定し、質問数は 50 問に満たない簡易な形式となっている。セルフチェックでは回答の信頼度に問題がある可能性があるが、役職・部門等の異なる複数人がチェックすることで精度を上げる、等の工夫も考えられる。回答の評価が実態に比べて高い、あるいは回答が一致しない等の項目はマネジメントに課題がある可能性があり、優先度を高めて調査・検討対象とする使い方も有効である。



■図 2-4-12　評価結果イメージ
（出典）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」

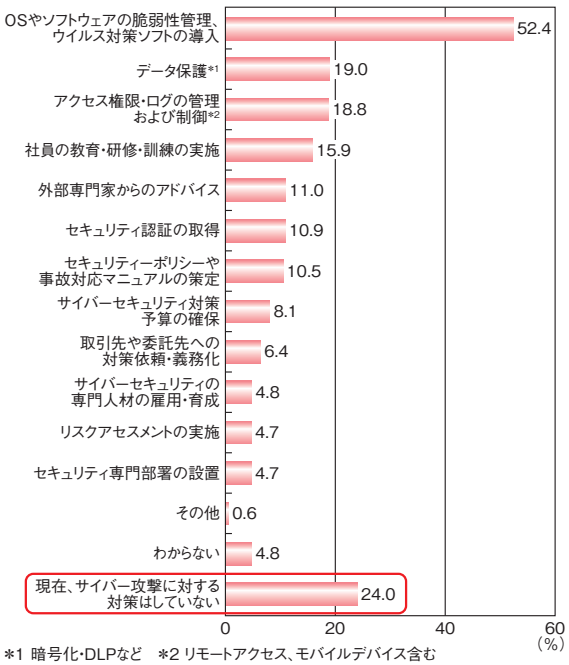
2.4.2 中小企業における情報セキュリティの取り組み

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 1 月 28 日に発表した「中小企業の経営者のサイバーリスク意識調査 2019※304」によると、サイバー攻撃への対策状況につ

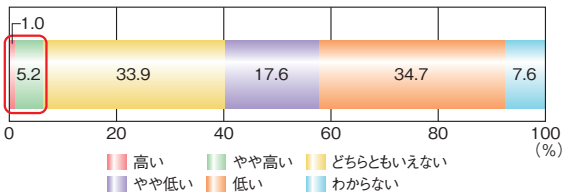
いて、中小企業の 4 社に 1 社は、今もなおサイバー攻撃への対策を実施していないと回答している（図 2-4-13）。



*1 暗号化・DLPなど　*2 リモートアクセス、モバイルデバイス含む

■図 2-4-13　サイバー攻撃への対策内容（n=825）
（出典）一般社団法人日本損害保険協会「中小企業の経営者のサイバーリスク意識調査 2019」を基に IPA が編集

サイバー攻撃の対象となる可能性については、自社がサイバー攻撃の対象となる可能性を認識している中小企業は 1 割未満であった（図 2-4-14）。

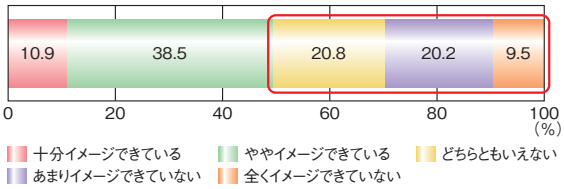


■図 2-4-14　サイバー攻撃の対象となる可能性（n=825）
（出典）一般社団法人日本損害保険協会「中小企業の経営者のサイバーリスク意識調査 2019」を基に IPA が編集

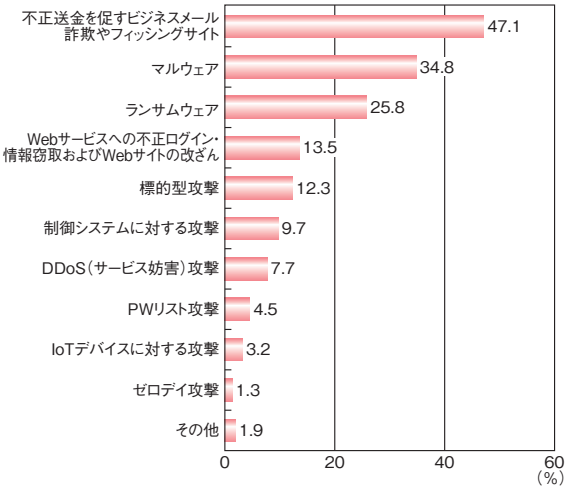
サイバー攻撃によって自社が被る被害については、中小企業の約半数が十分イメージできていないという結果であった（図 2-4-15）。

サイバー攻撃の被害経験については、825 社中 155 社が被害に遭っており、中小企業の約 2 割は何らかのサイバー攻撃の被害に遭っている。その被害内容を図 2-4-16 に示す。また、サイバー攻撃による被害総額は、図 2-4-17 に示すように、半数以上の企業で 50 万円を超えている。

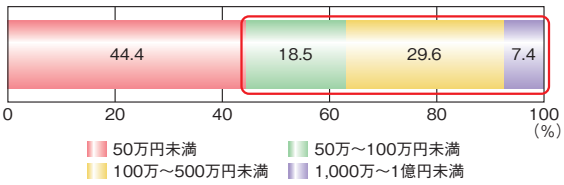
このような調査結果から、中小企業のサイバー攻撃対策は未対応の企業が四分の一である等、十分ではない。背景に、自社が攻撃対象になりうるという認識や攻撃被害のイメージの不足があると思われる。その一方で、サイバー攻撃の被害経験がある企業は少なくはなく、中小企業においても、経営課題の一つとして優先度を高め、サイバー攻撃対策を推進していくことが必要であると考えられる。



■図 2-4-15　サイバー攻撃の被害イメージ有無（n=825）
（出典）一般社団法人日本損害保険協会「中小企業の経営者のサイバーリスク意識調査 2019」を基に IPA が編集



■図 2-4-16　サイバー攻撃の被害内容（n=155）
（出典）一般社団法人日本損害保険協会「中小企業の経営者のサイバーリスク意識調査 2019」を基に IPA が編集



■図 2-4-17　サイバー攻撃による被害額（n=27）
（出典）一般社団法人日本損害保険協会「中小企業の経営者のサイバーリスク意識調査 2019」を基に IPA が編集

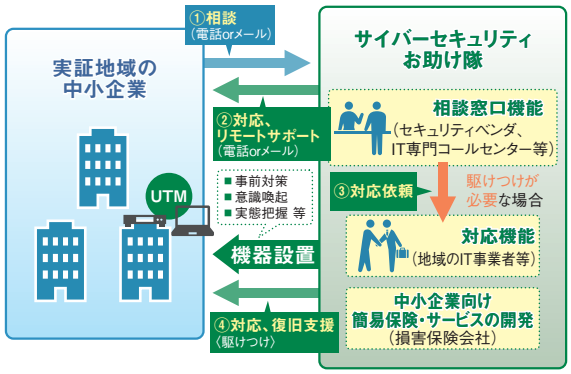
(2) 中小企業向け情報セキュリティ対策支援施策

政府が 2019 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) 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

経済産業省は2019年度、IPAを通じて、「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」（通称、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8地域の中小企業を対象として、サイバーセキュリティに関する悩みや、対策のニーズ、サイバー攻撃被害の実態等を把握するとともに、サイバーインシデントが発生した際の地域における支援体制の構築等に向けた実証を行った。

本事業には、19府県8地域（①岩手、宮城、福島、②新潟、③長野、群馬、栃木、茨城、埼玉、④神奈川、⑤石川、福井、富山、⑥愛知、⑦大阪、京都、兵庫、⑧広島、山口）の中小企業1,064社が参加した。このうち、727社にUTM（Unified Threat Management：統合脅威管理）等の機器を設置し、サイバー攻撃を観測した場合は地域のITベンダ等で構成されるサイバーセキュリティお助け隊が駆けつけ、対応、復旧支援等を行った。その結果、合計で128件のインシデントが発生しており、そのうち駆けつけ対応が18件発生している。本事業を通じて、中小企業においても業種や規模を問わず例外なくサイバー攻撃を受けているが、検知及び防御のための対策や社内体制の構築ができていない企業が多いことが明らかになった。本事業の報告書[※305]では、人的リソースの不足やコストに制約がある中小企業に、必要なセキュリティ対策を促すためには、「継続的な意識啓発」「導入・運用しやすい対策機器やサイバー保険の開発」「専門家の伴走型支援を含むワンパッケージ化」「コスト低廉化」が重要であり、これらを効果的に推進するため地域コミュニティとの連携促進やビジネス化に向けた情報共有の仕組みの構築が有効であるとまとめている。



■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「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）[※37]」を基に編集

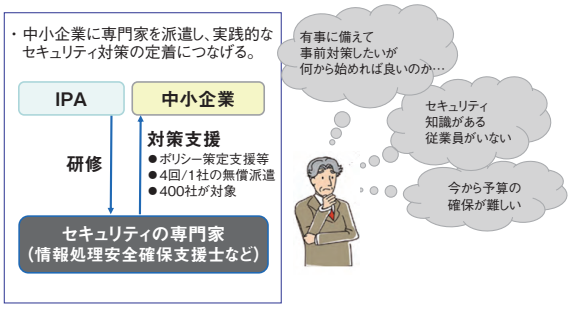
本事業において大阪府、京都府、兵庫県での実証を担当した大阪商工会議所は2020年4月、「サイバーセキュリティお助け隊」を中小企業向けサービス事業として、大阪府内を中心に京阪神でのサービス提供を開始した[※306]。今後、実証事業を踏まえた中小企業向けサービスの提供事業者の増加、提供地域の拡大が期待される。

(b) 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2019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」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、中小企業の現場に応じたリスクの洗い出しからマネジメントに必要なセキュリティ基本方針や関連規定の策定に向けて以下の指導を実施した。

- 1回目：情報セキュリティ診断等による潜在的リスクの洗い出し
- 2回目：診断結果に基づく重点領域の可視化、基本方針の策定、対策の決定
- 3回目：関連規定の策定に向けた検討
- 4回目：関連規定のレビューと専門家指導全体のまとめ

本事業には、全国の中小企業382社が参加した。その結果、96.4%の企業が成果を得られたと回答し、指導した専門家も92.0%が指導先企業のセキュリティレベルが上がったと回答した。また、今後実施すべきと考える取り組みについて、「体制整備・運用ルールの策定・継続的な改善」と回答した企業は79.9%であった。本事業を通じて、多くの企業がセキュリティレベルや継続的改善の意識の向上を果たした。



■図2-4-19　情報セキュリティマネジメント指導業務のイメージ
（出典）IPA「中小企業の情報セキュリティマネジメント指導業務[※307]」を基に編集

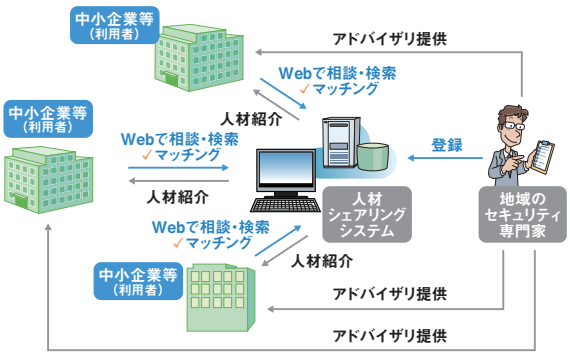
(c) 中小企業向けサイバーセキュリティ製品・サービスのプラットフォーム構築事業

経済産業省では 2019 年度、IPA を通じて、「中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築事業※308」を実施した。本事業は、中小企業でも扱いやすいセキュリティ製品・サービスを導入・運用することで得られる効果や費用、利用のし易さ、課題等を分かりやすく提示する枠組み（プラットフォーム）の実現可能性を調査するものである。具体的には、中小企業向けセキュリティ製品･サービスについて、「導入のし易さ」「運用のし易さ」「導入や運用に要する費用」「製品・サービスのセキュリティ性能」等の評価項目を仮設定した後、セキュリティ製品・サービスをユーザ企業に導入してもらい、ヒアリング調査にて評価項目の有効性を検証し、有識者委員会にて評価項目の設定を見直した。また、有識者委員会にて中小企業向けセキュリティ製品・サービスの情報提供プラットフォームのあるべき姿の検討等を行った。

本事業を通じて、情報提供プラットフォームのあるべき姿が明確となり、必要となる機能や運営方法の方向性が打ち出された。今後、本プラットフォームが構築されることで、中小企業におけるセキュリティ製品・サービスの選定が容易になり、導入や対策の実践が促進することが期待される。

(d) セキュリティ人材シェアリングモデル事業

総務省は2019年度、グローバルセキュリティエキスパート株式会社を通じて、「セキュリティ人材シェアリングモデル事業」を実施した（図 2-4-20）。本事業では、関西地域の中小企業 50 社を対象として、クラウド上の人材シェアリングシステム（人材登録やマッチング等を行う）を使用し、地域の中小企業が抱えるサイバーセキュリティの課題と、地域のサイバーセキュリティ専門家のセキュリティスキルをマッチングした。マッチングが成立した場合は、サイバーセキュリティ専門家が当該中小企業を訪問し、セキュリティに関する助言を行い、企業が抱えるサイバーセキュリティ上の課題解決を支援した。



■図 2-4-20　セキュリティ人材シェアリングモデル事業のイメージ
（出典）グローバルセキュリティエキスパート株式会社「セキュリティ人材シェアリングモデル事業※309」を基に IPA が編集

(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) 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」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※310。

SECURITY ACTION に基づく自己宣言は、一般社団法人クラウド活用・地域 ICT 投資促進協議会が実施する「全国中小企業クラウド実践大賞※311」の参加条件になるほか、公的な補助金制度の申請要件としても活用されている。

2020 年 3 月末時点の宣言数は 9 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。

(b) 小さな中小企業と NPO 向け情報セキュリティハンドブック

NISC は、2019 年 4 月に「小さな中小企業と NPO 向け情報セキュリティハンドブック※312」を公開した（次ページ図 2-4-21）。

本ハンドブックは、特に小規模事業者やセキュリティ担当者の設置が困難な中小企業及び NPO 等に向けて、サイバーセキュリティに関する脅威とその対策についてイラストを交えながら解説している。

本ハンドブックの著作権は NISC に留保されているが、自由な活用を目的に制作されており、企業内のサイバーセキュリティに関する社員研修等で利用したい場合は、印刷用の版下データや、イラスト単位で活用できるように画像データ等も提供されている。

■図 2-4-21　小さな中小企業と NPO 向け情報セキュリティハンドブック
(出典)NISC「小さな中小企業と NPO 向け情報セキュリティハンドブック」

(c) MY CISO ハンドブック・テンプレート

JNSA は、2019 年 9 月に「MY CISO ハンドブック・テンプレート」を公開した※313。

「MY CISO ハンドブック・テンプレート」は、2018 年 5 月に公開した「MY CISO ハンドブック」を中小企業向けに使いやすくしたものであり、中小企業の CISO やセキュリティ担当者が、セキュリティに関わる業務を執行し、経営陣と適切なコミュニケーションを進める上で明確にすべき項目と内容を例示している。例示されたものを自社に則した内容にカスタマイズし、独自の「MY CISO ハンドブック」を整備することで、日常的な業務の中にセキュリティ業務を組み込むことが期待できる。

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

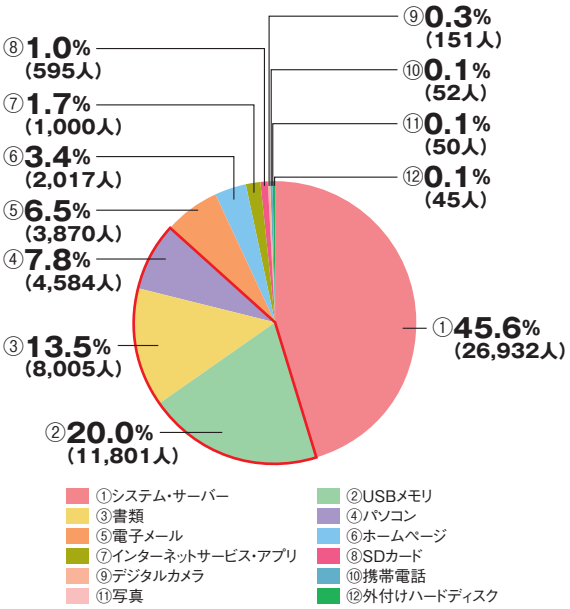
教育機関・政府及び地方公共団体等法人における対策状況について、公表されている資料に基づいて述べる。

(1) 教育機関における個人情報漏えいと政府による対策、インシデント事例

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）では、学校、公的教育機関、関連組織で発生した、児童・生徒・保護者等の個人情報を含む情報の紛失・漏えい事故について、公開情報を調査・集計した結果を「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－」（以下、ISEN 調査報告書）として毎年公表している。

ISEN 調査報告書※314 によると、2018 年度は 198 件の個人情報漏えい事故が発生しており、漏えいした件数は延べ 5 万 7,628 人分である。2017 年度の 187 件、2016 年度の 207 件と比べ※315、過去三年間の発生件数に大きな改善はない。

漏えいした個人情報の件数を経路・媒体ごとに比較すると、「システム・サーバー」が約半数の 45.6%（2 万 6,932 人）と最も多く、次いで「USB メモリ」が 20.0%（1 万 1,801 人）、「書類」が 13.5%（8,005 人）、「パソコン」が 7.8%（4,584 人）と続く。4 位までの経路・媒体を合計すると、漏えい件数の約 9 割を占める（図 2-4-22）。



■図 2-4-22　情報漏えいの経路・媒体別の事故発生比率※316
(出典)ISEN 調査報告書を基に IPA が作成

従って、これらの経路・媒体の利用に関する対策を徹底することによって、大幅な改善が見込める。なお、人数が 2 位～4 位の経路・媒体は、合計すると 41.3%（図 2-4-22 の赤枠部分）となり、1 位の「システム・サーバー」に匹敵する漏えい人数であるが、これらはいずれも、紛失したり置き忘れたりする人的ミスが漏えいの原因となる媒体であり、後述するように共通した対策が考えられる。

学校における個人情報漏えい事故に関する政府の取り組みとして、文部科学省は、学校を対象として「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）※317」を公表している。この中で、前述の「システム・サーバー」及び紛失・置き忘れの対象となる漏えい経路・媒体に関する対策等の考え方が示されている。

(a)「システム・サーバー」からの漏えいに対する施策

「システム・サーバー」については技術的な対策が主になるが、① Web 閲覧やメール等外部からアクセスが容易なシステムと、個人情報等機微な情報を扱う校務系システムとを論理的あるいは物理的に分離すること、②児童生徒による機微情報へのアクセスリスクを回避するために、校務系システムと学習系システムを分離すること、③学習系システムには機微な情報を保管しないことを原則とすること、等が対策として挙げられている。また、効率的にこうした対策を実現する上では、「システム・サーバー」の管理を学校現場等で行うのではなく、セキュリティ水準が第三者認証等によって確保されるクラウド事業者に任せる選択も効果的としている（クラウドについては「3.4 クラウドの情報セキュリティ」参照）。

(b) 人的ミスによる媒体からの漏えいに対する施策

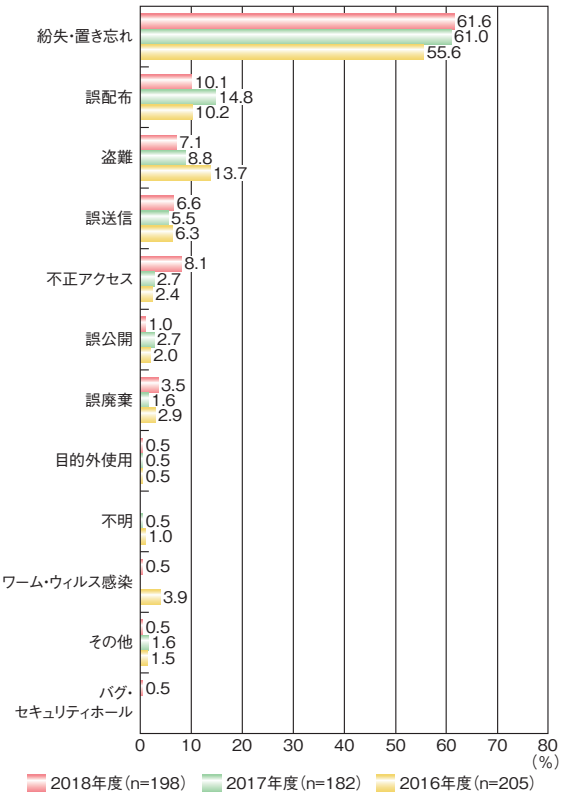
媒体の紛失・置き忘れの対策としては、管理されたUSB メモリやパソコン以外の使用を禁止し、適切なパスワード設定や個人情報等の暗号化を徹底すること等が挙げられている。ただし「書類」については、こうした技術的対策では保護が難しいため、人的・制度的なセキュリティ対策にも併せて取り組む必要がある。例えば、個人情報の外部持出しには教育情報セキュリティ管理者（ガイドラインでは、校長等を想定）の許可を得なければならないとする規則の制定・施行等である。

個人情報漏えい事故の原因別の統計を見ると、紛失・置き忘れは、発生件数の 61.6% を占めており、しかもこの状況が 2017 年度 61.0%、2016 年度 55.6% と過去 3 年間続いていることが分かる（図 2-4-23）。紛失・置き忘れによる情報漏えい事故の対策徹底は、依然として不十分であったことがうかがわれる。

紛失・置き忘れが原因とみられるインシデントの実例を以下に示す。

2019 年 8 月 30 日、富山大学で、学生 320 人の個人情報を格納した USB メモリの紛失が判明した。この大学では個人情報の持ち出しが原則禁止されており、持ち出しの場合は保護管理者の許可を得ることが定められていたが、この規則が守られていなかった上、USB メモリにはパスワード設定がされていなかった※318。

2019 年 9 月 12 日、静岡県立袋井商業高等学校で、生徒 64 人の個人情報を保存した教師の私物 USB メモリの紛失が判明した。校長の許可を得ずに USB メモリに個人情報を保存した上、パスワードを設定する等のセキュリティ対策もしていなかった。この高校では 4 月にも



■図 2-4-23　学校における個人情報漏えい事故
（出典）ISEN 調査報告書を基に IPA が作成

USB メモリの紛失が発生しているが、その際も、個人情報保護管理の徹底が不十分だったとみられる※319。

このように、前述の「教育情報セキュリティポリシーに関するガイドライン（令和元年 12 月版）」等において適切な技術的対策（パスワード等の適切な設定、機微な情報の暗号化等）や人的・制度的対策（個人情報持ち出しに確認・許可を必要とする規則の制定等）が示されていても、それが周知徹底されない、あるいは周知されても実践のスキルや時間的余裕がない状況が続いては、効果が発揮できない。上位の組織（地方自治体の教育委員会、私立の学校法人等）において標準的な施策を決め、対策予算やセキュリティ技術に詳しい人的リソースを用意し、実施状況の改善進捗を把握・管理する等、適切な支援が求められる。

(2) 地方公共団体における対策状況

総務省は、継続的に地方公共団体の情報セキュリティ対策の実施状況を調査している。ここでは総務省が公表している「地方自治情報管理概要～電子自治体の推進状況（令和元年度）～※320」に基づき、地方公共団体の情報セキュリティ対策の実施状況の変化について述べる。

表 2-4-1（次ページ）は、対策項目に関して、都道府

県及び市区町村の実施率をまとめたものである。2018年度と2019年度の実施率の差も併せて記載している。

2018年度に比べ2019年度は、多くの項目で実施率が向上した。特に市区町村では、10ポイント以上実施率が向上した項目が四つある。

基本的な個別対策（「情報セキュリティ責任者や管理者等の任命の有無」「情報資産の重要度に応じて保管やアクセス、持ち出しについて規定」「サーバ室等の入退室管理を行っている」等）は、都道府県・市区町村ともに高い実施率となっている。他方、調査・分析・計画等の項目（表中の（A）の項目）や監査・評価に関する項目（表中の（B）の項目）は、特に市区町村において、今後の改善が期待される。

2.4.4 一般利用者における対策状況

IPAが実施した「2019年度情報セキュリティに対する意識調査[※322]」の結果を基に、一般利用者の情報セキュリティ対策の実施状況について述べる。

(1) パソコン利用者のセキュリティ対策実施状況

パソコン利用者のセキュリティ対策実施状況の調査結果によると、「Windows Updateなどによるセキュリティパッチの更新」をしている割合が50.8%（2018年度から4.9ポイント減）、「セキュリティソフト・サービスの導入・活用」をしている割合が55.1%（2018年度から5.8ポイント減）で、どちらも半数以上が実施しているが、2018年度よりも減少している（図2-4-24）。また、「不審な電子メー

対象項目		対策実施率	
		都道府県	市区町村
	情報セキュリティの責任者や管理者等の任命の有無	100.0% (0.0ポイント)	99.8% (+1.1ポイント)
(A)	緊急時対応計画を整備	100.0% (+2.1ポイント)	69.6% (+14.5ポイント)
	情報資産の重要度に応じて、保管やアクセス、持ち出しについて規定	100.0% (0.0ポイント)	92.9% (+4.6ポイント)
	情報資産について、機密性、完全性及び可用性により分類	74.5% (+4.3ポイント)	63.8% (+14.1ポイント)
(A)	主要な情報資産について調査及びリスク分析を行っている	74.5% (+6.4ポイント)	47.8% (+9.5ポイント)
	サーバ室等の入退室管理を行っている	100.0% (0.0ポイント)	99.3% (+0.2ポイント)
	サーバ等への停電や免振対策を実施している	100.0% (0.0ポイント)	97.4% (-1.2ポイント)
	重要情報を含む紙媒体を適切に管理している	100.0% (0.0ポイント)	98.6% (+1.2ポイント)
	CD-R、USBメモリ等によるデータの持ち出し、持ち込みを制限している	97.9% (0.0ポイント)	98.3% (+1.5ポイント)
	クラウドサービスやデータセンターを利用している	93.6% (0.0ポイント)	91.2% (+6.8ポイント)
	情報セキュリティ研修を職員に対して実施している	100.0% (0.0ポイント)	92.9% (+3.3ポイント)

対象項目		対策実施率	
		都道府県	市区町村
(B)	緊急時対応訓練を実施している	87.2% (+12.7ポイント)	33.0% (+6.8ポイント)
	重要なデータのバックアップを取得	100.0% (0.0ポイント)	99.9% (+0.2ポイント)
	機器や外部記録媒体を廃棄する際、重要なデータを抹消	100.0% (0.0ポイント)	99.3% (0.0ポイント)
	重要なデータへのアクセス制限（権限設定、認証）を実施	97.9% (−2.1ポイント)	99.7% (+0.7ポイント)
	許可されていないソフトウェアの導入を禁止	100.0% (0.0ポイント)	97.9% (+1.2ポイント)
	重要な情報システムのアクセスログを保存し、検査	100.0% (+2.1ポイント)	91.7% (0.0ポイント)
	重要なデータを暗号化し保存	87.2% (+6.3ポイント)	50.0% (+4.9ポイント)
	委託事業者に対し、情報漏えい防止策を契約等により義務付けている	100.0% (+2.1ポイント)	96.3% (+5.7ポイント)
	情報資産の調達の際、仕様書等に情報セキュリティポリシーに基づいた要件を記載している	97.9% (+6.4ポイント)	71.1% (+12.4ポイント)
(B)	情報システムの運用等の委託事業者に対する指導・監査を実施している	68.1% (+8.5ポイント)	49.5% (+9.9ポイント)
(B)	機密性、完全性及び可用性等についてサービス契約（SLA）に定め、委託事業者に対し定期的に報告することを定めている	59.6% (+8.5ポイント)	38.7% (+12.6ポイント)

（A）の項目は対策実施手順・ポリシーの策定や調査・分析・計画等の項目。（B）の項目は監査や評価に関する項目（本文参照）。各セルの1行目の値は2019年度の値。2行目の括弧付きの値は2018年度の値との差。

■表2-4-1　地方公共団体における主な情報セキュリティ対策状況（2019年度、47都道府県、1,741市区町村）
（出典）総務省「地方自治情報管理概要～電子自治体の推進状況（令和元年度）～」「地方自治情報管理概要～電子自治体の推進状況（平成30年度）～[※321]」を基にIPAが作成

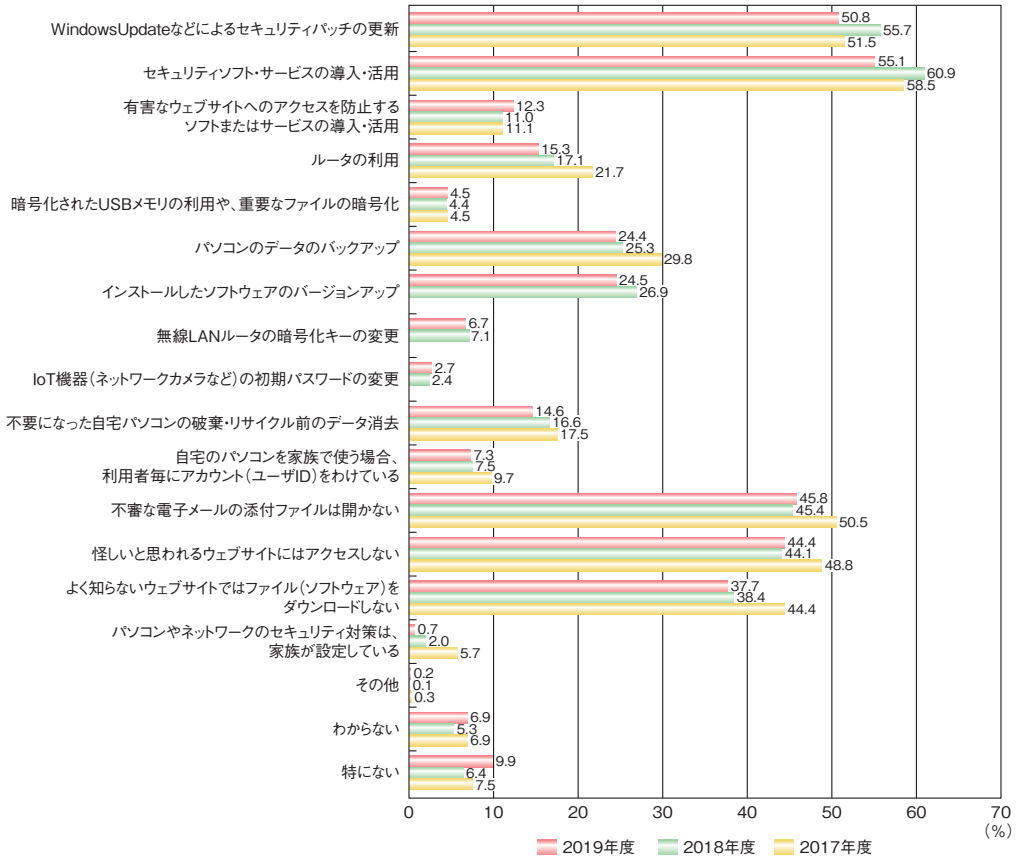
ルの添付ファイルは開かない」割合は 45.8%（2018 年度から 0.4 ポイント上昇）、「怪しいと思われるウェブサイトにはアクセスしない」割合は 44.4%（2018 年度から 0.3 ポイント上昇）である等、若干上昇している項目もあるものの、いずれも過半数には届かず伸び悩んでいる。

近年の OS（オペレーティングシステム）は利用者が意識しなくても初期設定でセキュリティパッチが自動更新されるものが増えており、Windows Defender ウイルス対策※323 のように、パソコンの購入時点でインストール済みのセキュリティソフトも存在する。そのため、本調査で各対策を「実施している」と回答しなかった利用者の中には、意識せずに対策を実施している人が含まれる可能性もある。しかし、利用しているパソコンで実施されている対策や設定を把握していないことは、偽警告や偽セキュリティソフト（「1.2.6 個人をターゲットにした騙しの手口」参照）等、別の被害につながる可能性がある。パソコンを購入した販売店にセキュリティソフトウェアについて相談する、あるいは OS 開発元のサイト※324 等を参考に設定を確認する、等の対応が望まれる。

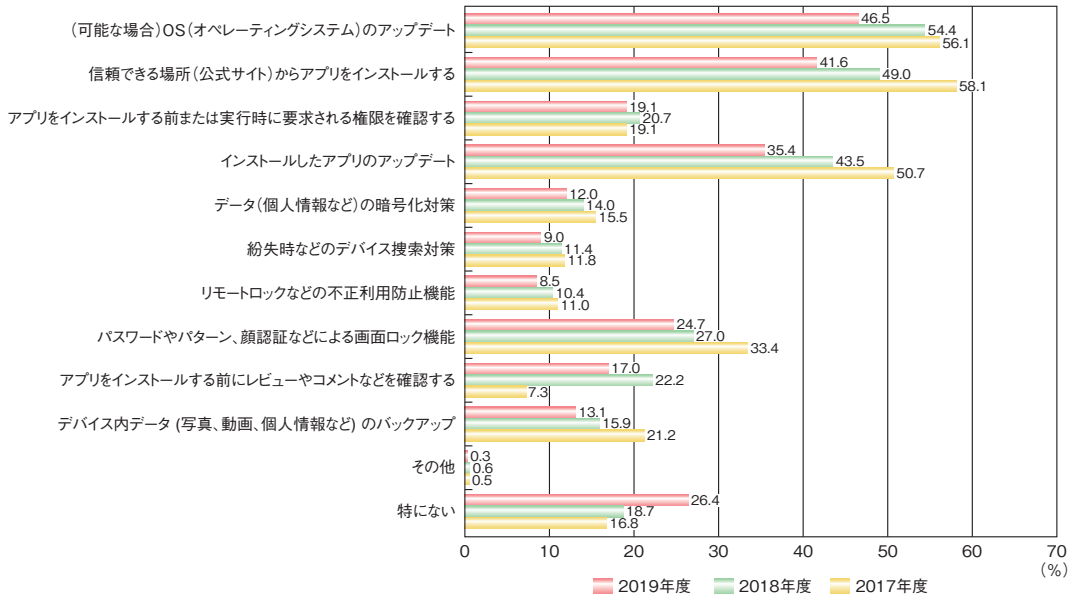
(2) スマートデバイス利用者のセキュリティ対策実施状況

スマートフォンやタブレット端末等のスマートデバイスのセキュリティ対策実施状況の調査結果によると、以前は半数が実施していた「（可能な場合）OS（オペレーティングシステム）のアップデート」（46.5%）、「信頼できる場所（公式サイト）からアプリをインストールする」（41.6%）、「インストールしたアプリのアップデート」（35.4%）の割合がいずれも 4 割前後まで低下している（次ページ図 2-4-25）。また、スマートデバイス紛失時の捜索や不正利用防止等、他の対策の実施割合も 2018 年度より低下している。

2019 年に急速に普及したスマートフォン決済サービス（スマホ決済）では、アカウント、あるいはアカウント情報の不正利用が大きな問題となっている。不正利用の原因としては、フィッシングや情報漏えいによって窃取された ID・パスワードを使った不正ログインの他に、決済アプリや決済のための情報が入ったスマホ自体を盗まれることや、アプリやサービスの脆弱性を悪用されること等が挙げられている※325-1。図 2-4-25（次ページ）の結果を見ると、スマホ決済を利用する人の多くがこのリスクに対処できていないことが懸念される。



■図 2-4-24　パソコン利用者のセキュリティ対策実施状況（n=5,000）
（出典）IPA「2019 年度情報セキュリティの脅威に対する意識調査※325-2」を基に作成



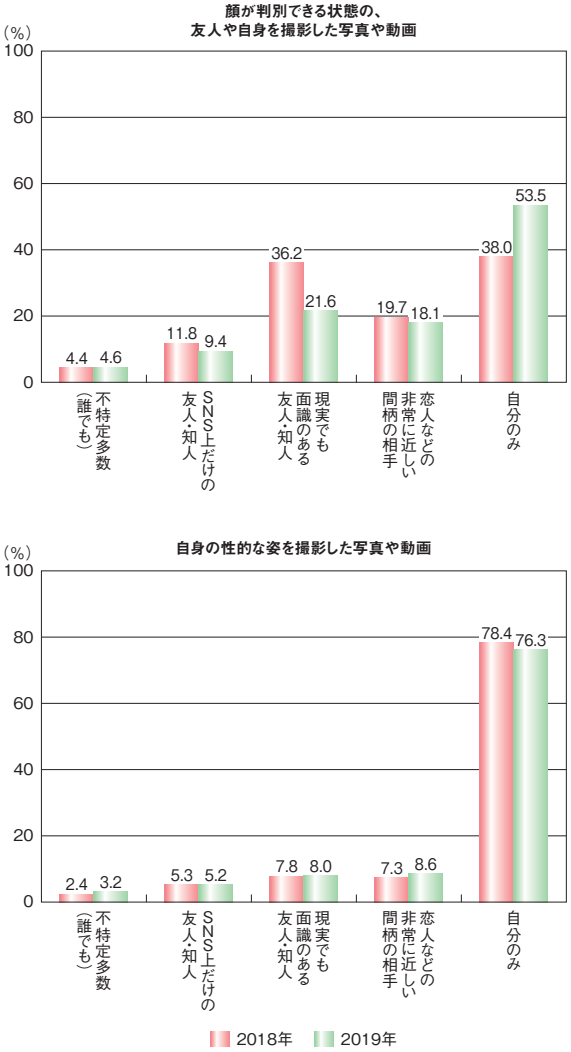
■図 2-4-25　スマートデバイス利用者のセキュリティ対策実施状況（n=5,000）
（出典）IPA「2019 年度情報セキュリティの脅威に対する意識調査」を基に作成

スマホ決済の不正利用による金銭被害を防ぐ意味でも、画面ロック機能を始めとする他者による不正操作の防止策を講じておくことや、スマホ決済アプリを公式マーケット等の信頼できるサイトからインストールし、通知があったら迅速にアップデートを実施することが推奨される。また、不正利用につながる個人情報を詐取されないよう、「1.2.6 個人をターゲットにした騙しの手口」を参考に対策を実施することも有効である。

(3) SNS 利用におけるリスクの認識状況

SNS の利用により、個人が簡単に情報を発信し、著名人や共通の興味・趣味を持つ人と立場を越えて交流することが可能となった。しかし同時に、コミュニケーション不備による炎上や情報の意図しない拡散、悪意の人物との接触のリスクも大きくなり、実際に犯罪被害が発生している（「1.2.6 個人をターゲットにした騙しの手口」「3.3 次代を担う青少年を取り巻くネット環境」参照）。犯罪に巻き込まれないためには、SNS 利用におけるリスクを認識し、慎重に行動することが重要である。

スマートデバイス利用者を対象とした SNS での写真・動画の共有相手に関する意識の調査結果（図2-4-26）によると、顔が判別できる状態の、友人や自身を撮影した写真や動画について、「恋人などの非常に近しい間柄の相手に共有してよい」と回答した割合は 18.1%、「現実でも面識のある友人・知人に共有してよい」と回答した割合は 21.6%、「SNS 上だけの友人・知人に共有してよい」と回答した割合は 9.4% であった。SNS 上に投



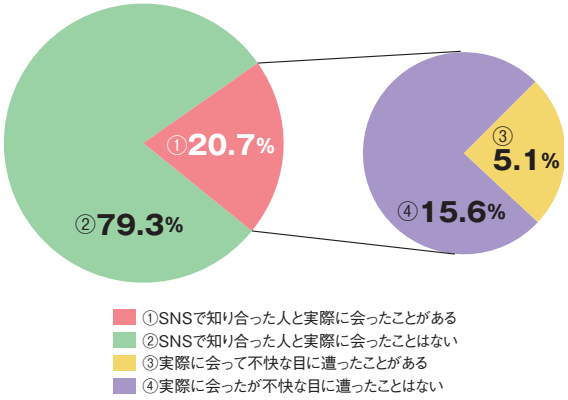
■図 2-4-26　SNSでの写真・動画の共有相手に関する意識（n=5,000）
（出典）IPA「2019 年度情報セキュリティの倫理に対する意識調査[※325-3]」を基に作成

稿した顔写真はストーカー行為等に悪用される可能性があるため、身元の分からない相手に送信するリスクはもとより、知人に送信する際にも、知人の端末から漏えいする、知人が勝手に公開する等のリスクがあることを認識しておきたい。

また、自身の性的な姿を撮影した写真や動画について、「恋人などの非常に近しい間柄の相手に共有してよい」と回答した割合は 8.6%、「現実でも面識のある友人・知人に共有してよい」と回答した割合は 8.0%、「SNS 上だけの友人・知人に共有してよい」と回答した割合は 5.2% であった。性的な映像はセクストーションやリベンジポルノといった犯罪に悪用されるリスクがあるため、SNS への投稿はもちろん、撮影することも控えるべきである。

更に、スマートデバイス利用者の中で、「SNS 上で交流がある人と実際に会ったことがある人」の割合は 20.7%、「実際に会って不快な目に遭ったことがある人」は 5.1% と、SNS 上で交流がある人と実際に会ったことのある人のうちおよそ 4 人に 1 人が実際に会った結果、不快な目に遭ったことがあると回答した（図 2-4-27）。SNS で知り合った人と実際に会ったことをきっかけとする意図しない特殊詐欺への加担や、誘拐等の被害が発生している昨今、SNS 上での交流の中で実際に会うという話題が出た際には、相手の目的、会う場所や時間等について慎重に判断すべきである。

以上のようなリスクを認識の上、SNS は慎重に利用することが望ましい。



■図 2-4-27　SNS 上で交流がある人と実際に会った経験（n=5,000）
（出典）IPA「2019 年度情報セキュリティの倫理に対する意識調査」を基に作成

COLUMN

サイバーの中心で、愛をさけぶ

皆さんは「セキュリティって何?」って考えたことがありますか? 堅苦しい定義で言えば、「機密性」「完全性」「可用性」を守ることになると思いますが、もう少し柔らかい言い方をすると、「私たちがインターネットやコンピュータ、スマートフォンを安心して使い続けられるように、大切な情報が流出したり、ウイルスなどに感染することから守ること」だと言えます。私たちの大切なものや大切な人の生活を、それらを脅かすもの者から守ること、これってまさに「愛」だと思いませんか? 突然何を言い出すのかと思われるかもしれませんが、私たちの生活にたくさんの「愛」が溢れているように、サイバーな世界にもたくさんの「愛」が必要で、それこそが「セキュリティ」なのです。

愛し愛されるためには努力が必要なように、セキュリティにも努力が必要です。愛を維持するために必要な努力の多くは、そのままセキュリティの維持にも必要なものです。

1. 愛(セキュリティ)とは、手間(時間)をかけること
   長いパスワードや、多要素認証など、ちょっと面倒だけどひと手間かけてください。
2. 愛(セキュリティ)とは、共有すること
   都合の悪い出来事(インシデント)こそ、隠さずに共有しましょう。組織内だけでなく、社会全体と共有することも大切です。
3. 愛(セキュリティ)とは、信頼すること
   サイバー空間では信頼できる相手(信頼点)の確保が重要です。信頼があるからこそ、確認(監査)ができるのです。
4. 愛(セキュリティ)とは、許すこと
   インシデントが発生した組織をあまり責めないでください。本当に悪いのは、悪意を持ってウイルスをばらまいたり、情報を流出させる人(集団)です。
5. 愛(セキュリティ)とは、忘れてはならない約束だということ
   職場で、家庭で、これだけは守ろうというルールを決めることが大切です。そして、それを忘れないように。
6. 愛(セキュリティ)とは、見返りを求めないこと
   セキュリティを強化したからといって直接的に利益が増えないばかりか、利用者に面倒がられるかもしれませんが、確かにそこに愛はあります!
7. 愛(セキュリティ)とは、楽しむこと
   人もいない、予算もつかない、平常時には褒められないなど、愚痴や文句のひとつも言いたくなるかもしれませんが、あなたはひとりではありません。一緒に楽しみましょう!

いかがですか? 「セキュリティ=愛」だということがおわかりいただけたのではないでしょうか。一緒にサイバーの世界を愛で満たしましょう!

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※326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

1995年にWTOにより、貿易の技術的障害に関する協定（WTO/TBT協定）が発効し、加盟国が製品や技術に適用する強制規格や適合性評価手続きの作成の際には、原則として国際規格（ISO/IEC等）を基礎とすることが義務付けられた※327。翌1996年、WTO政府調達協定が発効し、政府調達における技術仕様等には国際規格を基礎とすることが各国に義務付けられた。欧米各国は、国際競争力強化のために国際標準化活動を重要と考えて取り組んできたが、日本でも「知的財産推進計画2010※328」において国際標準化を知的財産政策の第1項に掲げ取り組んできた。

標準化は製品の仕様や性能等の実体物の形態や機能を対象として進展してきたが、徐々に対象が拡大し、サービスや社会システム・環境等の形のないものや仕組みを対象とするようになってきた。また、技術開発スピードの高まりや国際社会における新興国の存在感の高まり等により、標準化検討プロセスの加速や標準化活動を担う人材の育成が強く求められるようになった。このような環境変化に対応するため、日本における標準化活動の基盤となっている工業標準化法が2018年5月に改正され、2019年7月に施行された。これに伴い、「工業標準化法」は「産業標準化法」に、「日本工業規格（JIS: Japanese Industrial Standards）」は「日本産業規格（JIS）」に変わった。また、法目的に国際標準化の促進を追加するとともに、産業標準化及び国際標準化に関する国、国立研究開発法人・大学、事業者等の努力義務規定が設けられた※329。

(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制定される「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）※330」、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）※331：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、JTC1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※332。

- 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※333、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。

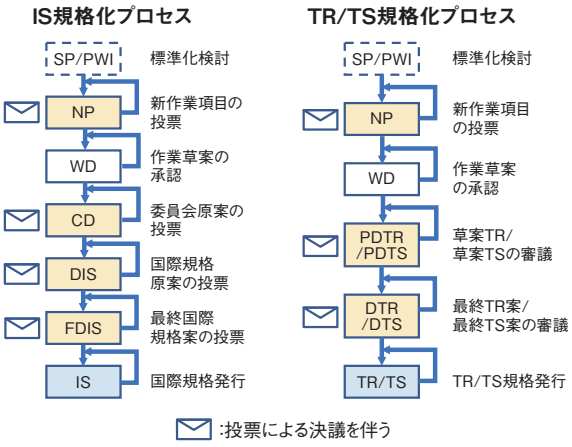
- IEEE（The Institute of Electrical and Electronics Engineers, Inc.）：
  電気工学・電子工学技術に関する国際学会である。標準化活動は内部組織であるIEEE-SA（Standards Association）が行っている。情報セキュリティについては、サイバーセキュリティ、ネットワークセキュリティ、IoTセキュリティ等の広範な領域で標準化を行っている。
- IETF（Internet Engineering Task Force）：
  インターネット技術の国際標準化を行う任意団体である。非常にオープンな組織であり、作業部会のメー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※334。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（埋め込み機器、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※335。

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※336-1」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）

2019年度は、4月にWG会議と総会がテルアビブ（イスラエル）、10月にWG会議がパリ及びサンドニ（フランス）で開催された（以下、テルアビブ会議、パリ会議）。

なお、SC27のタイトルについて、活動範囲が広がっていることから見直しがされ、総会において「Information security, cybersecurity and privacy protection」とすることが承認された※336-2。

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年を経た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ている。2018年4月及び10月、並びに2019年4月に、それぞれWDを発行し、エキスパートレベルでの審議を進めてきたが、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。2020年4月現在、管理策の全体構成については、大枠が固まり、今後は管理策の具体的な内容を決める段階となっている。

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の状況を考慮し、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る。ただし、今回の定期レビューの結論は改訂しないこととなったが、SC 27/WG 1では、共通フォーマット及びISO/IEC 27002の改訂がISO/IEC 27001に与える影響評価を継続して行っており、この評価結果によっては、次の定期レビューを待たずに、ISO/IEC 27001改訂を検討することも想定されている。

(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。

分野別規格そのものについては、ISO/IEC 27011:2016（通信事業者のためのガイドライン規格）、ISO/IEC 27010:2015（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 27017::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）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。

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だけの拡張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※337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WG 1とWG 5の共同プロジェクトを開始した（「2.5.2（5）（b）プライバシー」参照）。ISO/IEC 27002を拡張した分野別規格については、次期改訂において、ISO/IEC 27002の改訂への対応に加えて、ISO/IEC 27009への適合、すなわち、ISO/IEC 27001の要求事項の拡張についても検討される可能性がある。ISO/IEC 27011については、これら2点を主たる目的として、既に改訂が開始されている。

(c) サイバーセキュリティ関連の国際標準化活動

新たなトピックである、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 27101は、DTS審議中の状況にある。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規格についても検討が進められており、これはWD審議中の状況である。ただし、サイバーセキュリティに関する解釈は各国、各組織で多様化しているため、対象範囲の決定や用語定義等を行うことは難しく、規格化に向けた課題はまだ多い。

(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については、2020年4月時点でも改訂中でWDを検討中である。引用規格※338の改訂に伴う改訂も行われている。ISO/IEC 27007:2017は、ISO 19011にISMS固有のガイダンスを加えた規格であるが、ISO 19011:2018の発行に対応し、2020年に改訂版が発行された。ISO/IEC 27013:2015は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が、ISO/IEC 20000-1:2018の発行を受けて、2020年4月時点で改訂中である。

また、ISO/IEC 27009の発行、及びこれに適合した分野別規格の発行に伴い、分野別に拡張されたISMSを認証するニーズが生じてきている。ISO/IEC 27006は、ISMS認証を希望する組織の審査・認証を行う認証機関に対する要求事項を規定した規格であるが、分野別ISMS規格に対する認定のための要求事項について、ISO/IEC 27006に相当する規格の発行等の検討が開始されている。前述(b)のISO/IEC TS 27006-2の検討はこの取り組みの一つである。

(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。2019年度は、新しい規格3件(「暗号アルゴリズム　第6部:準同型暗号(ISO/IEC 18033-6)」「軽量暗号　第6部:メッセージ認証コード(MAC)(ISO/IEC 29192-6)」「軽量暗号　第7部:放送型認証プロトコル(ISO/IEC 29192-7)」)、及び既存規格3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) ブロック暗号Kuznyechikの標準化中止

「暗号アルゴリズム　第3部:ブロック暗号(ISO/IEC 18033-3)」へロシアからブロック暗号Kuznyechikの提案があり、追補として規格化作業が行われていた。一方、中国から同規格へブロック暗号SM4の提案があり、追補として規格化作業が並行して行われていた。両暗号がそれぞれ最終国際追補案(FDAM:Final Draft Amendment)へ到達したため、両暗号を盛り込んだ改訂版のFDISを準備していた。

しかし、2019年1月にフランスの研究者から、Kuznyechikに使用されているSボックス(入力・出力変換関数)は、設計者が主張するようなランダム性を持つようには生成されていないとの論文が発表された。このため、WG 2内でもKuznyechikの扱いが議論になった。解読はされていないので問題ないとのロシアの主張に対し、多くの国が安全性に疑義を持つことになったため標準化すべきではないとの意見が出された。

その後、ブロック暗号Kuznyechikの標準化中止(FDISのキャンセル)の提案が行われ、いくつかの投票を経て、最終的に標準化の中止が決まった。なお、中国のSM4には問題がないため、追補原案(DAM:Draft Amendment)から標準化作業を再開する。

(b) 安全なマルチパーティ計算の新規標準化

データを暗号化したままで処理することを可能にする秘密計算は、強固な情報漏えい対策技術として期待されている。秘密計算の中でもデータを複数のマシンに秘密分散したまま処理する技術がマルチパーティ計算である。

日本からマルチパーティ計算の標準化提案を行い、「安全なマルチパーティ計算　第1部:概要(ISO/IEC 4922-1)」「安全なマルチパーティ計算　第2部:秘密分散に基づく機構(ISO/IEC 4922-2)」の2部構成で標準化することが2020年4月に承認された。エディタは日本とオーストリアが務め、2023年の規格の発行を目指している。

(3) WG 3(セキュリティの評価・試験・仕様)

WG 3 は 2019 年 4 月にテルアビブ（イスラエル）、10 月にサンドニ（フランス）にて定期会議を開催した。2020 年 4 月にサンクトペテルブルグ(ロシア)で予定された会議は新型コロナウイルスのためキャンセルされ、Zoom 会議にてオンライン開催された。それらの会議の議論内容を以下に概説する。

(a) ISO/IEC 20897 の開発

ISO/IEC 20897（Security requirements, test and evaluation methods for physically unclonable functions for generating nonstored security parameters） で は、PUF（Physically Unclonable Function）と呼ばれる技術のセキュリティ要件、及びそのテスト手法に関する標準化が行われている。PUF は半導体チップ固有の物理特性から識別 ID や暗号鍵を生成し、IoT 機器等の認証やデータ秘匿等に用いる技術である。

本規格はパート 1、パート 2 に分かれており、パート 1 では PUF のセキュリティ要件(例えば、PUF から生成される識別 ID や暗号鍵は、予測不可能なランダムな値でなければならない等）を規定している。このパート 1 はテルアビブ会議にて DIS のための投票に進むことが合意され、その投票結果は Zoom 会議にて議論され、FDIS に進むことが合意された。パート 2 は、パート 1 のセキュリティ要件が正しく製品に実装されていることを検証するための手法を定めているが、その検証手法の大枠が定まったこともあり、サンドニ会議にて CD に進むことが合意され、Zoom 会議では更なる技術的な議論を行うため、CD2 に進むことが合意された。なお本標準化に関しては、昨年度より引き続き PUF の研究プロジェクト※339 の成果を反映すべく、日本の技術者が積極的に標準化に貢献している。

(b) ISO/IEC 23837 の開発

ISO/IEC 23837（Security requirements, test and evaluation methods for quantum key distribution）では、量子鍵配信(QKD：Quantum Key Distribution)のセキュリティ要件、及びそのテスト手法に関する標準化が行われている。QKD とは、暗号鍵を光子に乗せ伝送する技術であるが、この QKD による暗号鍵配送方式は、第三者による鍵の盗聴を確実に検知することが、量子力学の理論上保証されている。QKD を利用することにより、情報漏えいを完全に防げるとされる暗号技術、量子暗号通信が実現可能となる。

QKD では、光子の送受信は QKD 送信機及び受信機により行われるが、理論どおり鍵の盗聴を検知するためには、それら送受信機は所定のセキュリティ要件を満たす必要がある。例えば、送受信機には一般の IT 製品と同様に管理機能が存在するが、管理機能を悪用した攻撃が想定される。また、QKD 送受信機自体も、理論上セキュアであると保証された QKD プロトコルに従い光子を送受信しなければならない。本規格は、QKD 送受信機等が満たすべきセキュリティ要件及びその検証手法を定めることを目的にしており、テルアビブ会議にて規格開発が承認され、パリ会議、Zoom 会議にて WD1、WD2 に基づく議論が実施された。日本からも 2019 年に設立された一般社団法人量子 ICT フォーラム※340 のメンバーがこの WD1、WD2 に対し数多くのコメントを提出し、本規格開発に大きく貢献している。

(c) ISO/IEC 15408、ISO/IEC 18045 の改訂

ISO/IEC 15408（Evaluation Criteria for IT security）及び ISO/IEC 18045（Methodology for IT security evaluation）は WG 3 の主要規格の一つであり、IT 製品のセキュリティ機能を評価する手続きを定めた国際標準である。本規格をより柔軟に適用可能にするため、数々の新たな評価の枠組みが導入されたことを「情報セキュリティ白書 2019」にて概説※341 したが、CD の成熟度が高まったことからパリ会議にて DIS に進むことが合意され、早ければ 2020 年度中の出版が見込まれる状況にある。

(d) 研究期間による規格開発

2019 年、WG 3 においては、コネクテッドカーのセキュリティ評価やハードウェアトロイ等、計九つの SP を開始することが、中国、フランス、米国、英国等から提案され WG 3 総会で承認された。コネクテッドカーに関しては、現在 ISO/SAE 21434(Road vehicles — Cybersecurity engineering)を開発中の ISO/TC 22/SC 32/WG 11 議長等をパリ会議、Zoom 会議に招き、今後の規格開発の方向性を検討している。またハードウェアトロイに関しては、日本でも 2019 年度に研究プロジェクト※342 が立ち上がっており、そのプロジェクトメンバーも Zoom 会議に参加し、研究期間の副ラポータになることが承認された。

(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2019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進めている。

- ISO/IEC 27030: Cybersecurity – IoT security and privacy – Guideline
- ISO/IEC 24391: Security techniques – Guidelines for IoT-domotics security and privacy
- ISO/IEC 27402: Cybersecurity – IoT security and privacy – Device baseline requirements

(ア) ISO/IEC 27030: Cybersecurity – IoT security and privacy – Guideline

我が国は、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※343」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 27030（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 27030の規格について概説する。

ISO/IEC 27030の具体的内容に当たる第5章以降では、第5～6章で参照モデル、各ステークホルダーの役割、IoT ライフサイクルに触れ、IoT システムにおけるリスクについて言及する。第7章では、セキュリティ対策、及びプライバシー対策が、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表現で記載されている。

パリ会議において、ISO/IEC 27030は、CD1となり、規格案としての完成度が一定のレベルとなった。本規格に対するコメントは、日本、フランス、カナダ、ドイツ、米国、インド、中国等の多くの専門家から大量に提出されており、審議は極めて活発である。本規格はIoT セキュリティ及びプライバシーのための規範となるガイドラインであるため、IoT ステークホルダーにおける認証等への活用が期待されている。

(イ) ISO/IEC 24391: Security techniques – Guidelines for IoT-domotics security and privacy

本規格は、テルアビブ会議において、中国からNPとして提案され、パリ会議では、NPの承認がなされ、WD1が作成された。「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 27030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 27030と整合を取る形で規格化を進めるとしている。

(ウ) ISO/IEC 27402: Cybersecurity – IoT security and privacy – Device baseline requirements

本NPは、米国から強く提案されたもので、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件の規定を目指している。ISO/IEC 27030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することを想定している。NP案に添付されたベースライン的要件としては、以下が例示されている。

- Device Identification（機器の識別）
- Device Reset（機器のリセット）
- Configuration（構成）
- Data Protection/Security（データ保護とセキュリティ）
- Software and Firmware updates（ソフトウェア、ファームウェアのアップデート）
- Interface access（インタフェースアクセス）
- Telemetry（テレメトリ）
- Vulnerability Disclosure（脆弱性情報の開示）
- Secure Storage（セキュリティの確保されたストレージ）

上記の要件は、あるレベルでISO/IEC 27030においても記載されているため、今後の規格策定においては、ISO/IEC 27030との棲み分け、役割分担に注視する必要がある。

(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 – Guidelines for implementation

(ア) ISO/IEC 20547-4: Big data reference architecture – Part4: Security and privacy

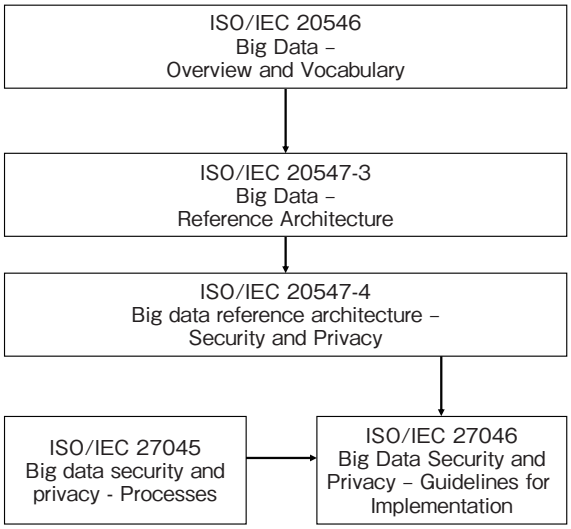
ISO/IEC JTC 1/SC 42 で審議されている、ISO/IEC 20547（ビッグデータ参照体系）は四つのパートから成り立っている。そのうちパート 4 は、SC 42 の依頼により SC 27/WG 4 で審議されており、セキュリティ及びプライバシーに関わる参照体系を規定している。本規格は、パリ会議において CD2 をベースにコメント審議を行った。日本は、品質や ISO/IEC 20547-3 との整合性の課題等の理由で DIS に進むことを反対し、米国、フランス、スウェーデン、スイスも同様に反対したものの、結果的には DIS に進むこととなった。

(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いる。パリ会議において、WD2 が審議され、次回の会議においては、WD3 に進めることとなった。

(ウ) ISO/IEC 27046: Big data security and privacy – Guidelines for implementation

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。パリ会議においては、前述の(ア)と(イ)の規格との差別化について審議され、図 2-5-2 のように整理された。



■図 2-5-2　ビッグデータセキュリティ／プライバシー関連規格間の関係性

本課題は、テルアビブ会議にて NP 提案がなされ、パリ会議ではその承認と WD1 に進むことの合意がなされた。

(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 から仕切り直し
- インターネットセキュリテイガイドライン（27032）：WD3 に進むことが決定
- ネットワークセキュリティ（27033）：改版作業なし
- アプリケーションセキュリティ（27034）：パート 4 が DIS 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 DIS に移行
- サプライヤー関連セキュリティ（27036）：全パートを視野に入れた改版作業の検討中
- 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）：大規模な改版を視野に入れ NP として仕切り直し

- 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):WD1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):CD1に進む
- 公開鍵基盤における実践とポリシーの枠組み(27099):CD1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):WD2に進む
- 安全な配備、アップデート、及びアップグレード(4983):NPの審議に進む
- データの起源―参照モデル（データ追跡のため):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:PWIとして審議継続
- セキュリティオペレーションセンター（SOC）のガイドライン:PWIとして審議継続

(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。2019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について、アイデンティティ管理全般についての規格であるISO/IEC 24760との整合性を確保したり、複数要素認証等の技術動向に合わせたりする改訂作業が進められている。

(b) プライバシー

プライバシー対策に関わる規格であるISO/IEC 27701:2019は、2019年8月にISとして発行された。本規格は、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追加することにより、プライバシー対策に関するマネジメントシステム構築を支援することを目的としている。本規格はこれまで、ISO/IEC 27552として規格策定作業が行われていたが、マネジメントシステム規格（MSS:Management System Standard）※344の番号付けルールに従い、IS発行時に番号がISO/IEC 27701と改められた。2019年12月には、本規格を基にして認証や審査を行う組織に対する要求事項を定める新たな規格提案があり、WG 1とWG 5合同のプロジェクトとして作業が開始された(「2.5.2(1)(b)分野別規格の国際標準化活動」参照)。

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が、2020年6月にISとして発行された。また、同じく日本提案である「ユーザのプライバシープリファレンスに基づくユーザ主導によるPII処理のためのフレームワーク」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た。2020年4月現在、CD投票に向けて規格案の内容を精査しているところである。

(c) バイオメトリクス

バイオメトリック認証をリモート環境でも使用可能にするためのデータ構造を定義するISO/IEC 24761:2019は、改訂が進められ、2019年10月にISとして発行された。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、CD段階にある。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、WD段階にある。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、このプロジェクトは関心を集めている。

2.5.3 信頼性の高いコンピューティング環境の実現に向けたセキュリティ標準(TCG)

TCG（Trusted Computing Group）※345は、高い信頼性を持つコンピューティング環境実現のため、多様な機器やネットワーク、あるいは異なるレベルに対応するセキュリティ技術に関して統一的な標準仕様を開発、策定、普及させることを目的とし、2003年に発足した国際的非営利団体（NPO:Non-Profit Organization）である。TCGは、2020年2月現在、世界各国77の企業、30以上の政府機関、業界団体、大学、専門家で構成されている。

日本からはIPA、NICTを始めとする多数の機関、企業、専門家が参加している。前身のTCPA(Trusted Computing Platform Alliance）発足が1999年であったことから、2019年に設立20周年を迎え、記念イベン

トの開催等のキャンペーンを行った。

セキュリティチップTrusted Platform Module（TPM）を信頼の基点（Root of Trust）とし、自己暗号化ドライブ、高信頼ネットワーク、高信頼なパソコン／スマートフォン／自動車／ IoT ／産業機器等を実現する多種の仕様策定、公開を進めている。

TPM は 2004 年に世界各社のパソコンに搭載が開始された。その仕様は 2009 年に ISO/IEC 11889：2009 として公開、更に 2015 年に改訂版 TPM2.0 仕様（TPM Library Specification）が ISO/IEC 11889：2015 として公開されている※346。

TCG 初となる地域支部は日本に 2008 年に設立された※347。この日本支部（JRF：Japan Regional Forum）では、国内に向けて、ストレージ、サーバ、ネットワーク等での TCG 標準仕様の普及を目指し、種々の活動を行っている。2019 年には勉強会やワークショップ※348 を開いており、その実績と経験を日本から世界へ発信している。

2020 年 2 月現在、20 あるワークグループが、2019 年 2 月から 2020 年 2 月の間に公開した活動※349 の中から、以下では三つのワークグループ、及び JRF のワークショップについて紹介する。

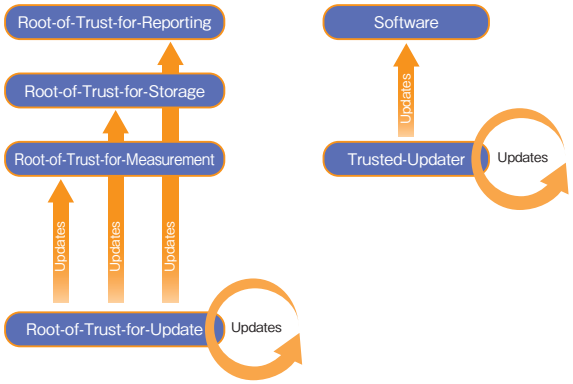
（1）組み込み機器ワークグループ（Embedded Systems WG）

パソコンへの実装から始まった TPM を、組み込み機器に幅広く展開する目的で活動している※350。

本 WG 配下の自動車サービスサブグループでは、TPM 仕様を自動車向けに最適化し、2015 年に初版公開、2018 年に Version 1.01 Revision 15 を改訂公開した※351。この版に合わせたセキュリティ要件（Protection Profile）に関しては、「Protection profile Automotive-Thin Specific TPM for TCG TPM 2.0 Automotive Thin Profile Family “2.0” Level 0」として 2019 年 2 月に確定版を公開した※352。自動車向けユースケースとしては、車載機器リモートメンテナンス、近年話題の自動運転用情報転送及びドライブレコーダ内データ保証等があり、これらについても検討を続けている。

同じく本 WG 配下の IoT サブグループでは、IoT 機器での TPM 活用による遠隔ソフト／ファームウェア更新のガイドラインとして「TCG Guidance for Secure Update of Software and Firmware on Embedded Systems※353」を 2020 年 2 月に公開した。本ガイドラインに記載されている「信頼されるプラットフォームに基づくアップデートの流れ」を図 2-5-3 に示す。作業の出発点として、TPM を主とする「Root-of-Trust-for-Update」を置き、そこでアップデート内容の信頼性を確認した後に順に上位層を動かしてアップデートを行う仕組みである（図 2-5-3 の左）。

また、IoT 機器の制約から簡略化した実装方式も用意されている。「Trusted-Updater」も、「Root-of-Trust-for-Update」と同様、作業の出発点として機能し、そこでアップデート内容の信頼性を確認した後に上位のソフトウェアのアップデートを行う仕組みである（図 2-5-3 の右）。



■図 2-5-3　信頼されるプラットフォームに基づくアップデートの流れ
（出典）TCG「TCG Guidance for Secure Update of Software and Firmware on Embedded Systems」を基に IPA が編集

（2）Device Identifier Composition Engine Architectures ワークグループ（DICE WG）

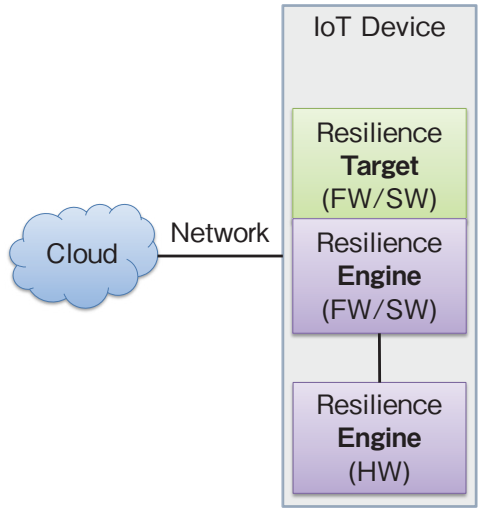
DICE WG は、前述の Embedded Systems WG から 2017 年に独立し、RIoT（Robust IoT）の Core 仕様上で動作するソフトウェア群の策定を目指している。特に TPM 利用システムだけでなく、TPM を使わないシステムでもデバイス ID を最小のシリコンリソースで実現できる新しい ID 管理アーキテクチャの開発を目指している。本 WG は 2020 年 1 月に「Symmetric Identity Based Device Attestation」を仕様として公開した※354。

（3）Cyber Resilient Technologies ワークグループ（CyRes WG）

2018 年 5 月に NIST が公開したファームウェアの攻撃耐性（レジリエンス）に関するセキュリティ規格である文書 SP800-193 を補完する（NIST の Requirement に対する実現可能な Solution を提供する）ことを目的の一つとして、2018 年 6 月に設立された WG である。NIST は TCG のリエゾンの一つであり、両者は密接に交流している。

2019 年 6 月の公開セミナーでは、本 WG の議長であ

る Microsoft 社のメンバーが「TCG Cyber Resilient Technologies - Trusted Computing Group」と題する講演を行った。この中で、本 WG と NIST SP800-193 の関係が説明された。図 2-5-4 は、その講演資料に記載されている「IoT を例とする遠隔からのリカバリーの流れ」である。この図で IoT Device の最下辺に位置する「Resilience Engine (HW)」は、図 2-5-3（前ページ）で説明した TPM を主とする「Root-of-Trust-for-Update」と同じ位置付けである。ここを信頼の基点として作業を進め、上位層を動かす仕掛けである。



■図 2-5-4　IoT を例とする遠隔からのリカバリーの流れ
（出典）TCG「TCG Cyber Resilient Technologies※355」を基に IPA が編集

(4) JRF の活動

JRF は 2008 年に発足して以来毎年イベントを開催している。2019 年 12 月には、FIDO Alliance※356-1、JPCERT/CC、IPA、NICT の協力／後援を受け、「IOT 時代に求められる Security by design のその先へ」をテーマに公開ワークショップを開催した。ワークショップでは、「TCG 最新動向の紹介」等の講演、パネルディスカッションのほか、多数のデモ展示が行われた※348。

COLUMN

セーフティ&セキュリティ

セーフティの英単語である Safety の意味は、安全、無事[i]等であり、セキュリティの英単語である Security の意味は、安全、安心、防衛[ii]等を意味します。どちらも「安全」の意味を持つので、違いがあまり分からないという方も多いかもしれません。

ISO や IEC 等の国際標準では、セーフティは、「許容不可能なリスクがないこと[iii]」、「許容できないリスクから免れている状態[iv]」、「安全（safety）とは，事故や損失がないことである。[v]」等と定義されます。一方、セキュリティとは、「攻撃により情報が漏えいする等の被害が起きないようシステムを守ること[vi]」等とされます。

また、両者の違いを「何を守るのか」という保護対象の観点で考えると、セーフティは人命、財産（家屋等）ですが、情報セキュリティでは情報の「機密性，完全性、可用性等[vii]」になります。そして「何から守るのか」という原因の観点で考えると、セーフティは偶発的なミス、故障等の確率的に発生する危険に対する安全を指すのに対し、セキュリティは、主に人為的に行われる脅威に対する安全を指します。つまり、原因に悪意があるかどうかが大きな違いになります。

モノづくりの国、日本において、自動車、家電、医療機器等の開発・生産とセーフティの関わりは深く、人の生命や健康に影響を及ぼすため、セーフティが重要視されてきたという長い歴史があります。セーフティは人のミス対応にはじまり、機械の故障対応、人と機械の協調対応へと対応の幅をひろげてきました。

一方、セキュリティはインターネットが一般に普及してきた 2000 年前後から注目され始め、インターネットを通じた攻撃の目的が、いたずらから金銭的利益へと変化するにつれて急速に重要分野となりました。サイバー犯罪のブラックマーケットは巨大化してきており、IoT をターゲットにした攻撃や AI を悪用した攻撃によって、更に社会に深刻な影響を与えることも想定されます。例えば、インターネットとつながる自動車や医療機器等も遠隔操作による攻撃を受け、人命を脅かすようなセキュリティの脅威に晒されることが分かり、各メーカも対応を進めています。

あらゆる機器・システムが複雑に影響を及ぼし合う AI と IoT の時代の到来に備えて、安全安心にシステムを利用できるように、セーフティ&セキュリティの実現が求められています。

i　株式会社研究社：新英和中辞典　https://ejje.weblio.jp/content/Safety〔2020/6/30 確認〕
ii　株式会社研究社：新英和中辞典　https://ejje.weblio.jp/content/security〔2020/6/30 確認〕
iii　ISO：ISO/IEC Guide 51:2014　https://www.iso.org/standard/53940.html〔2020/6/30 確認〕
iv　IEC：IEC 61508-4 Edition 2.0　https://www.iec.ch/functionalsafety/standards/page2.htm〔2020/6/30 確認〕
v　ナンシー・G・レブソン著、松原友夫監訳・訳、片平真史、吉岡律夫、西康晴、青木美津江訳：セーフウェア　安全・安心なシステムとソフトウェアを目指して、2009 年 10 月、p.175
vi　SQuBOK 策定部会編：ソフトウェア品質知識体系ガイド（第 2 版）－ SQuBOK Guide V2 －、2014 年 11 月、p.38
vii　ISO：ISO/IEC 27000:2018　https://www.iso.org/standard/73906.html〔2020/6/30 確認〕

2.6 安全な政府調達に向けて

IPA では、国民に向けた情報セキュリティに関する啓発活動のほか、政府機関や独立行政法人が安全に IT 製品等を調達するために活用できる制度の運営や利活用のための普及活動を行っている。

本節では、IT 製品のセキュリティ機能の適切性と妥当性を評価する「IT セキュリティ評価及び認証制度」の動向や安全な IT 調達に向けた新たな取り組み、及び暗号アルゴリズムの適切な実装を確認する「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。

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の発行した「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）」（以下、政府統一基準）では、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の基準を示しており、例えば公的なサービスにおいて国民の情報等を扱う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 製品の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。

このようなセキュリティ要件を確保する手段として、多くの国々では第三者が IT 製品の情報セキュリティを評価し、公的機関がその評価結果に基づき評価された IT 製品に認証を与える制度が用いられている。日本でも「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、政府機関等の調達に活用されている。

(1) 政府調達のセキュリティ要件

政府統一基準では、特にセキュリティ要件を策定すべき IT 製品として、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」（以下、要件リスト）を参照している。この要件リストには、情報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。

- デジタル複合機（MFP）
- ファイアウォール
- 不正検知システム／防止システム（IDS/IPS）
- OS（サーバ OS に限る）
- データベース管理システム（DBMS）
- 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（VPN）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。

要件リストには、これら対象製品において想定されるセキュリティ上の脅威が記載されている。例えば、ファイアウォールであれば、以下の脅威が想定されている。

- 管理機能等への不正アクセスによる不正な通信の発生
- ネットワーク処理の残存情報からの情報漏えい
- リモートで管理する場合の通信データの盗聴、改ざん
- 監査ログの改ざん・不正な削除

製品調達において、各組織の情報システムセキュリティ責任者は、これらの想定される脅威に対するセキュリティ要件を製品が満たしていることを、納品時に検査し確認することが求められる。

要件リストでは、セキュリティ要件の納品時検査の代替として、国際標準に基づく第三者認証製品の活用も認めている。日本における JISEC も、セキュリティ評価基準である ISO/IEC 15408 に基づく第三者認証の制度である。例えば、JISEC において先の四つの脅威に対抗できることが確認されたファイアウォール認証製品を購入することで、セキュリティ要件に関する納品時検査をしたものとみなされる。ただし、認証製品が想定していない個別のセキュリティ要件を調達に課した場合は、認証製品においても情報システムセキュリティ責任者は個別にその要件を確認しなければならない。

JISEC は、要件リストの中でも特に日本のベンダが世界的シェアを持つ製品分野である「デジタル複合機」、国策としてセキュリティが必要な旅券やマイナンバーカードといった「スマートカード」の調達に活用されている。

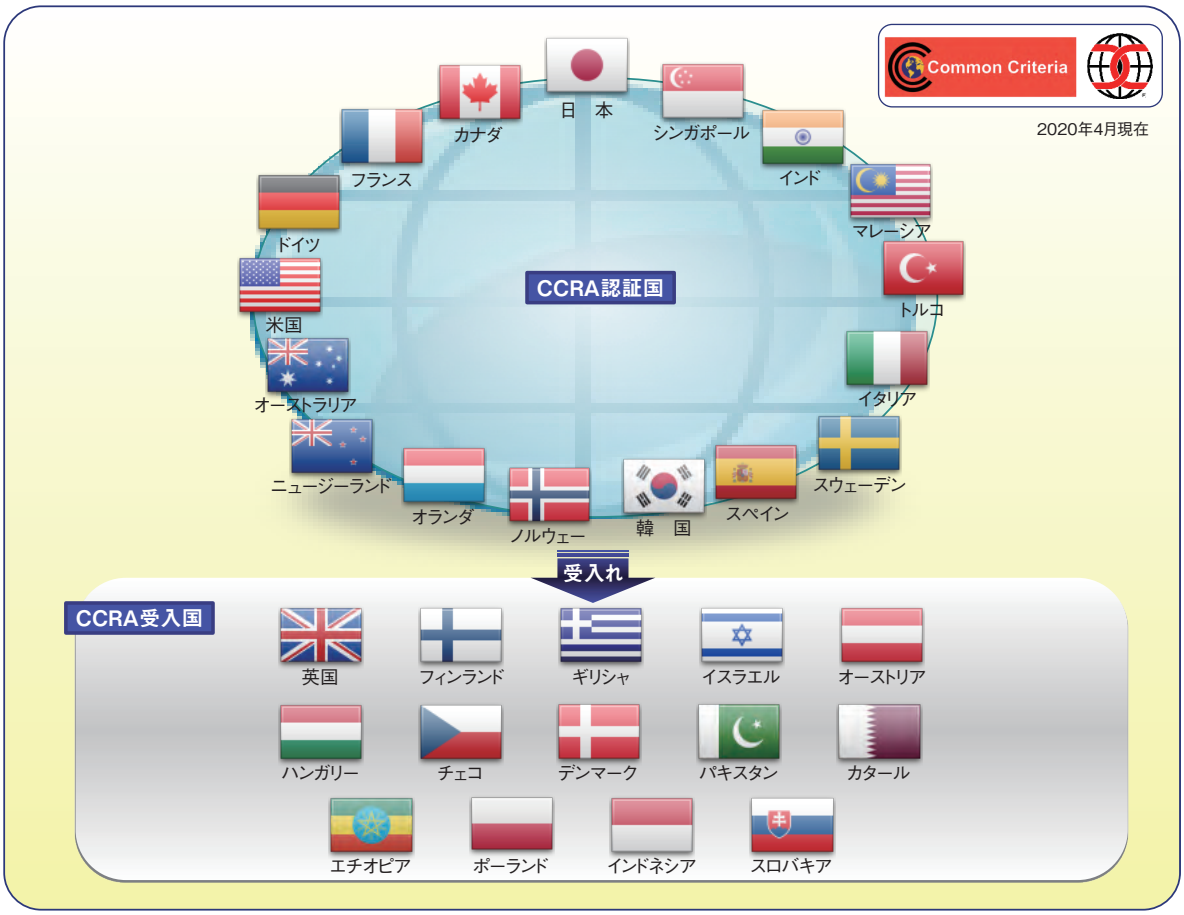
(2) 認証制度の国際連携

セキュリティ評価のための国際標準である 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。更に同じ評価基準であるコモンクライテリアにより評価された結果を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た。日本もコモンクライテリアに基づく認証制度であるJISECの運用を2001年に始め、2003年にCCRAへ加盟している。これにより、日本のベンダが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、近年は東南アジアや東ヨーロッパ諸国の受入国としての加盟が増加している。2019年9月にはスロバキアが受入国として加盟した。また、コモンクライテリアプロジェクトの初期メンバーである英国は、自国に認証を必要とする国際的な市場を持つセキュリティ製品ベンダがなく、2019年10月、制度維持のコスト削減を理由に認証国から受入国に移行した。2020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）。

CCRAでは、共通的なセキュリティ評価基準の策定や評価結果の相互承認に加えて、政府調達時の製品分野ごとの共通的なセキュリティ要件の策定も行っている。「2.6.1（1）政府調達のセキュリティ要件」で述べたように、各国政府はIT製品を調達する際に想定されるセキュリティ上の脅威に対抗できることを要件とし、その確認を行ってきた。この調達のためのセキュリティ要件をコモンクライテリアで規定された形式に従って記述したものを「プロテクションプロファイル」と呼び、各国の調達担当者は、IT製品の調達要件として多くのプロテクションプロファイルを策定し公開してきた。同一製品分野に対し国ごとに異なるプロテクションプロファイルへの適合を求めることによる製品ベンダの負荷を軽減するため、CCRAでは、製品分野ごとの共通のプロテクションプロファイルの策定を始めた。現在までに、ファイアウォール、ドライブ全暗号化、ネットワークデバイスについて共通プロテクションプ



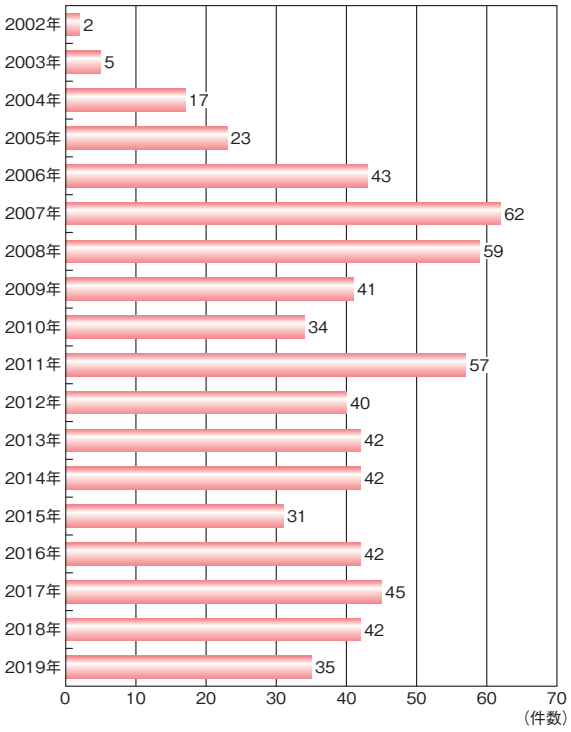
■図2-6-1　CCRA加盟国

ロファイルをCCRAのWebサイト※356-2で公開しており、要件リストにおいてもこれらの共通のプロテクションプロファイルに適合した製品を調達することで、確認すべき要件を満たすことが記載されている。

更に、日本が多くの製品ベンダを有するデジタル複合機についても、日本と韓国が発起人となり、関連するベンダや評価機関をメンバーとする技術コミュニティが発足し、共通のプロテクションプロファイルの策定を行っている。

(3) 認証の状況

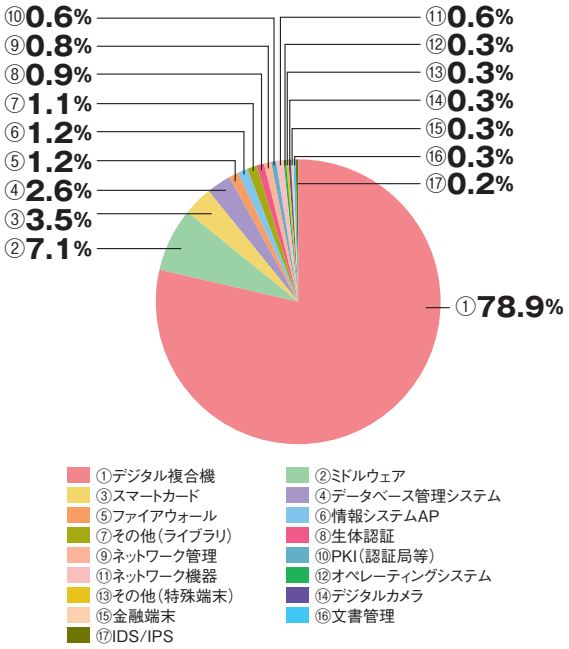
2019年度までのJISECでの認証発行件数の推移を図2-6-2に示す。制度設立当時は、製品のプロモーションを目的とし、政府調達に係ることのない多様な分野の製品の認証を発行していたが、2008年のリーマンショック以後は、申請される製品分野が政府調達の対象に絞られている。



■図2-6-2　JISECの認証発行件数の推移

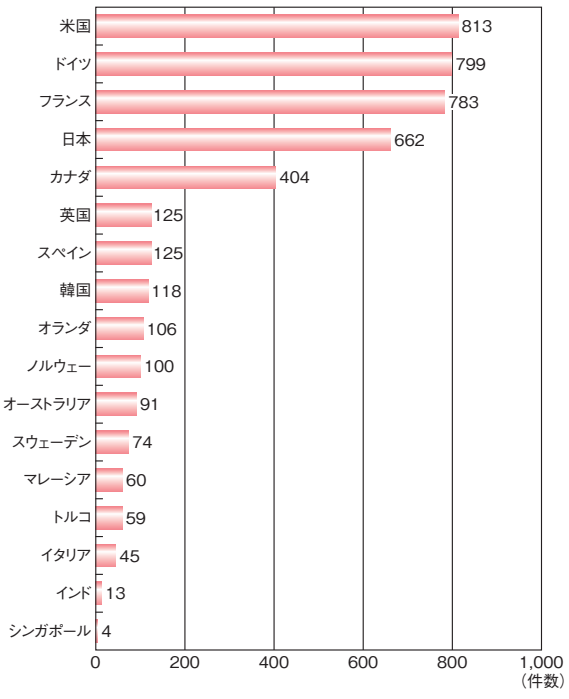
日本における認証発行製品分野の内訳は、図2-6-3に示すように圧倒的にデジタル複合機が多い。これは前述のように、多くの日本のベンダが国際的なシェアを有し、かつ政府調達の対象となる唯一のITセキュリティ製品だからである。デジタル複合機のような国際競争力を持つIT製品が新たに要件リストに追加されない限り、今後もこのような状況は続くと考えられる。

CCRA加盟各国が公開している認証製品の2019年



■図2-6-3　JISECの認証発行の製品分野内訳

度までの累計を図2-6-4に示す。日本は米国、ドイツ、フランスに次いで認証した製品が多い。米国とドイツは政府調達におけるプロテクションプロファイルの活用が活発であり、多くの情報サービス産業分野の製品が認証されている。一方で、フランスは認証製品の85%以上がスマートカード及び集積回路関連である。フランスでは1984年に設立された銀行カード協会が世界に先駆け銀



■図2-6-4　CCRA加盟国の認証数累計

行カードのスマートカード化を推進した結果、金融分野での利用を中心としたプロテクションプロファイルが策定され、高度な保証レベルの評価が数多く実施された。このような実績を背景に、日本のベンダを含め各国のスマートカード関連製品の評価がフランスで行われている。

(4) 2019 年度のトピック

まだ数は少ないが、日本の政府調達においても、調達部門が調達要件として自らプロテクションプロファイルを策定し、調達を実施している。要件リストに掲載されている JISEC で認証を取得したプロテクションプロファイルを表 2-6-1 に示す※357。

申請者	プロテクションプロファイルの名称	認証年月日
IPA	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015※358	2017 年 5 月 29 日
外務省領事局旅券課	旅券冊子用 IC のためのプロテクションプロファイル ― SAC 対応（BAC+PACE） 及び能動認証対応 ― 第 1.00 版※359	2016 年 3 月 22 日
外務省領事局旅券課	旅券冊子用 IC のためのプロテクションプロファイル ― SAC 対応（PACE） 及び能動認証対応 ― 第 1.00 版※360	2016 年 3 月 22 日
地方公共団体情報システム機構	個人番号カードプロテクションプロファイル 第 1.00 版※361	2014 年 5 月 15 日

■表 2-6-1　要件リストに掲載されている JISEC で認証を取得したプロテクションプロファイル

2019 年度には、外務省領事局旅券課が発行した「旅券冊子用 IC のためのプロテクションプロファイル SAC 対応（PACE）及び能動認証対応 - 第 1.00 版」並びに「旅券冊子用 IC のためのプロテクションプロファイル -SAC 対応（BAC+PACE）及び能動認証対応 - 第 1.00 版」にそれぞれ適合する 2 製品の旅券冊子用 IC が認証された※362。これらは、2015 年に国際民間航空機関（ICAO: International Civil Aviation Organization）が発行した、個人の生体情報を認証に利用した IC 旅券に関する規格「ICAO Doc 9309 Part 11」に対応したものである。これらの旅券冊子用 IC を搭載した IC シートが旅券冊子の製造を請け負う独立行政法人国立印刷局に約 92 万枚納入される予定である※363。

政府統一基準では、要件リストとは別に、近年政府においても活用される IoT 製品を含む情報システムについても、その調達や利用におけるセキュリティ対策を求めている。JISEC では、安全な政府調達を推進する立場から 2017 年度にネットワークカメラシステムのセキュリティ要件を調達者が自ら確認できるチェックリストを公開した※364。これに続き 2019 年度は、入退管理システムのチェックリストを策定し公開した※365。本チェックリストでは、入退管理システムの利用形態モデル（スタンドアローン、統合管理、クラウド）ごとに調達時に考慮すべき設定や運用、及びそれらを可能とするセキュリティ機能の要件を記載しており、調達者は本チェックリストを参照することにより、調達する入退管理システムの情報セキュリティ要件を確認できる。本チェックリストは、産業サイバーセキュリティ研究会が発行した「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※366」で参考文献として参照されている（産業サイバーセキュリティ研究会については「2.1.2（1）産業サイバーセキュリティ研究会」「3.1.4(1)日本政府の取り組み」参照）。

更に、JISEC では、2017 年度に作成したネットワークカメラシステムのチェックリストをセキュリティ要件とし、実際の製品に対するコモンクライテリアを用いた評価の実効性調査を 2019 年度に開始した※367。2020 年度は、この調査結果から、コモンクライテリアでの IoT 機器評価にかかる工数やコストと脆弱性評定効果とのバランスを調達者、ベンダ及び有識者で構成される委員会で検討し、プロテクションプロファイルを策定することで、IoT 製品分野での安全な政府調達を推進していく。

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。本制度は北米で運営されている CMVP（Cryptographic Module Validation Program）と同等の制度であり、国内では 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北米 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※368。これと並行して、JCMVP は、既存の承認された暗号モジュール試験機関について、ISO/IEC 19790：2012 に基づく暗号モジュール試験を実施する力量を有しているかを確認するための技能試験を実施し、1 社について力量を有していることを確認した※369。

関連する北米 CMVP の動向として、暗号モジュールのセキュリティ要求事項として NIST が策定中であった FIPS 140-3※370 が 2019 年 3 月 22 日に承認され、2019 年 5 月 1 日に米国連邦政府の官報に公示された※371。FIPS 140-3 は、その技術的内容について ISO/IEC 19790：2012 に準拠することを求めている。更に、FIPS 140-3 に適合するかどうか判断するにあたっての試験方法を定める NIST SP 800-140 シリーズのドラフトが 2019 年 10 月に公開され※372、2019 年 12 月までのパブリックコメントが実施された。

JCMVP は、このパブリックコメントを通じて、暗号モジュール認証を行う上での解釈の画一化等を目的として、ISO/IEC 19790:2012 を採用するにあたって得た知見のフィードバックを行った。NIST SP 800-140 シリーズの最終版は 2020 年 3 月に公開された※373。

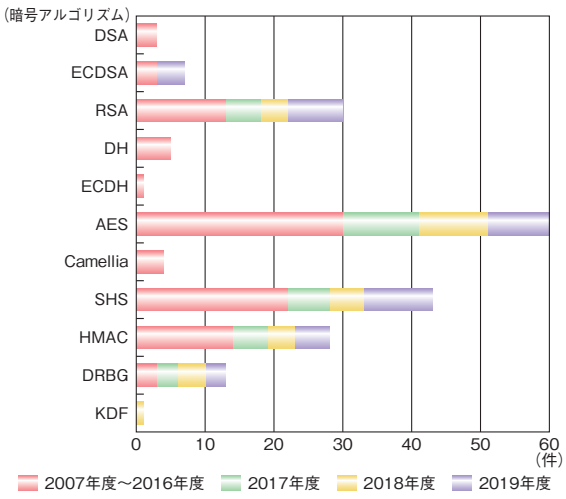
(2) 政府機関等における認証製品の活用

各府省情報化統括責任者（CIO）連絡会議が決定した「デジタル・ガバメント推進標準ガイドライン※374」に関連して、「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※375」が 2019 年 2 月に公開された。本ガイドラインでは、JCMVP によって耐タンパ※376 性※377 が確認されたハードウェアトークンは、当人認証保証レベルとして最高のレベル 3 に位置付けられている。

(3) IT セキュリティ評価及び認証制度との連携

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、2019 年に改定したガイドライン※378 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）。

2019 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※379」に基づくデジタル複合機の認証が 8 件完了している※380。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、2017 年度、2018 年度及び 2019 年度において堅調に増加している。また、2019 年度は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

(4) 承認されたセキュリティ機能の見直し

2019 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」の見直しに関して、以下の二点の審議が実施された。

- GCM-AES-XPN の追加
- 3-key Triple DES の削除

GCM-AES-XPN については 2019 年 7 月に承認されたセキュリティ機能に追加された。3-key Triple DES については、2019 年 12 月末を以て、承認されたセキュリティ機能から削除された※381。

また、2019 年度から次の事項について検討を進めている。

- RSA 1024 の署名検証機能の削除
- TLS version 1.0 及び 1.1 の鍵導出関数の削除
- TLS version 1.3 の鍵導出関数の追加

(a) RSA 1024 の署名検証機能の削除

公開鍵暗号方式の一つで、暗号アルゴリズムが RSA、鍵の長さを 1,024 ビットとしたものを RSA 1024 と呼んでいる。JCMVP では RSA 1024 の署名検証機能に限って承認されたセキュリティ機能に含めている。この RSA 1024 の政府機関等における使用の根拠となっている、「電子署名及び認証業務に関する法律施行規則」及び「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針」の見直しが進められている※382。これを受けて、RSA 1024 の署名検証機能についても、承認されたセキュリティ機能からの削除について、技術審議委員会配下の暗号アルゴリズム実装試験要件検討 WG において検討を行った。同 WG における検討の結果、削除時期は「電子署名法及び認証業務に関する法律施行規則」の改正の後とするという条件付きで、RSA 1024 の署名検証機能を削除する方針を技術審議委員会に答申することが決まった。なお、2020 年 3 月 30 日に「電子署名及び認証業務に関する法律施行規則」が改正されている※383。

(b) TLS version 1.0 及び 1.1 の鍵導出関数の削除

TLS（Transport Layer Security）version 1.0 及び 1.1 の使用を非推奨とするドラフトが IETF で検討されている※384。また、TLS のバージョン別のトラフィックに関するデータも公開されており※385、2020 年 2 月時点では TLS version 1.2 が主に使用されている。主要なブラウザにおいても、TLS version 1.0 及び 1.1 をサポートしない方向に舵を切る動きがある※386。これらに加え、米国※387、ドイツ※388、フランス※389 の動向を踏まえて、承認されたセキュリティ機能から TLS version 1.0 及び 1.1 の鍵導出関数を削除するスケジュールについて、暗号アルゴリズム実装試験要件検討 WG で検討を行った。同 WG において、CRYPTREC の動向を踏まえ、TLS version 1.0 及び 1.1 の鍵導出関数を削除する方針を技術審議委員会に答申することが決まった（2020 年 3 月末時点）。

(c) TLS version 1.3 の鍵導出関数の追加

前述の TLS version 1.0 及び 1.1 の鍵導出関数の削除の議論と並行して、承認されたセキュリティ機能に TLS version 1.3 の鍵導出関数を追加するための検討についても、暗号アルゴリズム実装試験要件検討 WG で開始した。TLS version 1.3 の鍵導出関数は、JCMVP の承認されたセキュリティ機能のうち、NIST SP 800-56C Rev.1※390 で規定された extraction-then-expansion 形式の鍵導出関数の expansion 部分に、NIST SP 800-108※391 で規定された Feedback Mode を用いた鍵導出関数を組み合わせた形を取っている。すなわち、TLS version 1.3 の鍵導出関数は、JCMVP の承認されたセキュリティ機能に含まれている鍵導出関数から構成されているとみなすことができるため、新たな安全性評価を行うことなく承認されたセキュリティ機能への追加を行うことが検討されている。この方向性は、同 WG において了承され、2020 年度から、TLS version 1.3 の鍵導出関数に対する試験仕様の検討を行うこととなった。

2.7 その他の情報セキュリティ動向

情報セキュリティ市場の規模と成長の動向、データ利活用の動向、及び暗号技術の動向、個人情報保護法の改訂について述べる。

2.7.1 情報セキュリティ市場の動向

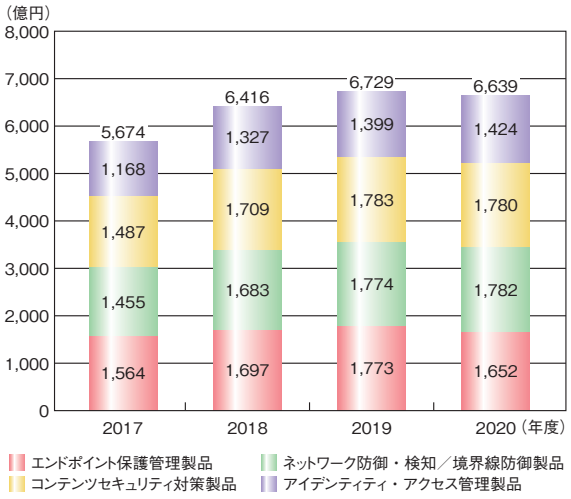
JNSA が発表した「2019 年度 国内情報セキュリティ市場調査報告書[※392]」によると、2019 年度の情報セキュリティ市場規模（ツールとサービスを合わせた数値）は、2018 年度より 5.0% の伸びとなる見込みである。

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 2-7-1 と図 2-7-2 に示す。図中の 2017 年度、2018 年度については推定実績値で、2019 年度については推定見込値、2020 年度については予測値である。

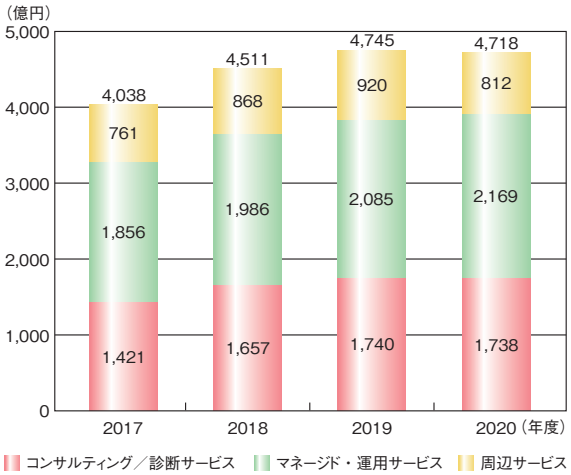
なお、JNSA では「2019 年度 国内情報セキュリティ市場調査報告書」から集計する際の市場区分を変更している[※393]（表 2-7-1、表 2-7-2）。

情報セキュリティツールの市場規模全体では、2018 年度から 2019 年度は 4.9% 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 2018 年度比 4.5% 増、「ネットワーク防御・検知／境界線防御製品」の 2018 年度比 5.4% 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、2018 年度から 2019 年度は 5.2% 伸びている。サービスの区分別に見ると、「コンサルティング／診断サービス」の 2018 年度比 5.0% 増、「マネージド・運用サービス」の 2018 年度比 5.0% 増を始め、すべての区分で増加傾向が続いている。



■図 2-7-1　国内情報セキュリティツール市場規模の推移
（出典）JNSA「2019 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 2-7-2　国内情報セキュリティサービス市場規模の推移
（出典）JNSA「2019 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

分類		説明
旧セキュリティツール	統合型アプライアンス	FW、IDS、ウイルス対策等複数機能を持ったアプライアンス
	ネットワーク脅威対策製品	FW、IDS ／ IPS、VPN、アプリケーションファイアウォール
	コンテンツセキュリティ対策製品	ウイルス対策、スパム対策、URL フィルタ、メールフィルタ、DLP 等
	アイデンティティ・アクセス管理製品	認証、ログオン管理・アクセス許可、PKI 製品
	システムセキュリティ管理製品	セキュリティ情報統合管理、ポリシー・アクティビティ管理ツール、脆弱性検査ツール　等
	暗号製品	暗号化製品、暗号モジュール
新セキュリティツール	エンドポイント保護管理製品	ウイルス対策製品、EDR 製品、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、物理セキュリティ
	コンテンツセキュリティ対策製品	情報漏えい対策 :DLP ／ DRM、暗号化製品、メール・セキュリティ対策、URL フィルタリング、脆弱性検査製品
	アイデンティティ・アクセス管理製品	個人認証用・生体認証デバイス及びその認証システム、アイデンティティ管理、ログオン管理／アクセス許可、PKI

■表 2-7-1　情報セキュリティツールの市場区分（新旧対照）
（出典）JNSA「2019 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

分類		説明
旧セキュリティサービス	情報セキュリティコンサルテーション	ポリシー構築、監査・診断等セキュリティ管理全般コンサルティング、規格認証取得支援サービス
	セキュアシステム構築サービス	IT セキュリティの設計、導入、製品選定支援　等
	セキュリティ運用・管理サービス	脆弱性検査、マネージドサービス（IT セキュリティの監視、運用支援）、プロフェッショナルサービス、電子認証サービス　等
	情報セキュリティ教育	教育実施、コンテンツ提供、教育 ASP、資格認定　等
	情報セキュリティ保険	情報セキュリティ及び IT セキュリティ保険
新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 2-7-2　情報セキュリティサービスの市場区分（新旧対照）
（出典）JNSA「2019 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

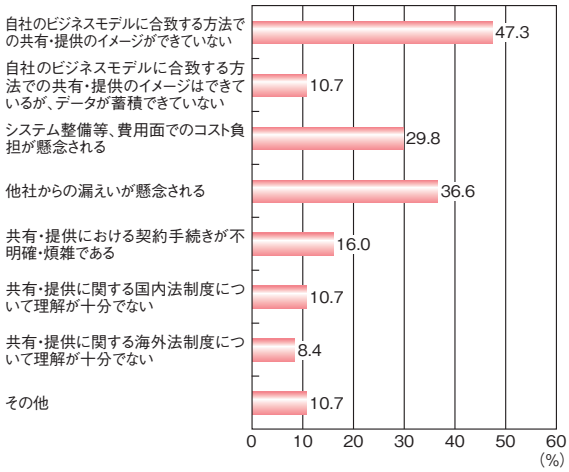
以上のように、情報セキュリティ市場の規模は 2019 年度まで拡大傾向が続いていたが、2020 年度以降については世界的な経済活動の縮小が予測されており※394、先行きが不透明である。

2.7.2 データ利活用の動向

近年、日本が目指す産業の在り方として、産業活動で生成されるデータを利活用することで技術革新や生産性向上等の新たな付加価値の創出や課題解決を目指す「Connected Industries」が提唱されている※395。データ利活用にあたり、AI、IoT 等の技術を背景とした DX を推し進め、新たな付加価値を創出することで競争力を高めていくことが各企業で重要なテーマとなっている。

データの利活用を自社内に限定せず、サプライチェーン上の関係会社や取引先企業にも展開すれば、既存製品・サービスの付加価値向上、新製品・サービスの開発、マーケティング戦略策定、不正防止等の様々な活用の可能性が広がる。ただし、自社の持つデータのみでは十分な活用ができない場合も多く、他社が保有しているデータも含めて効果的に活用していくことは、経営戦略・事業戦略上重要である。

一方で、データの提供を求められる側もデータを使用する側も、課題や懸念を抱える企業は少なくない。各企業は、データを活用したビジネス戦略を模索していることも多く、IPA が 2018 年度に実施した実態調査※396 では、「データ利活用による事業への効果が不透明」「他社からのデータ漏えいが懸念される」といった理由でデータの提供・共有が進んでいない企業が多く存在することが明らかとなった（図 2-7-3）。



■図 2-7-3　データを共有・提供しない理由（複数選択、n=131）
（出典）IPA「安全なデータ利活用に向けた準備状況及び課題認識に関する調査 調査実施報告書※397」を基に作成

こうした社会的状況を踏まえ、データ利活用の更なる推進に向けたビジネス、制度、セキュリティ等の施策を明らかにするため、IPA は、2019 年度に企業におけるデータ利活用・保護の戦略立案に関する調査を行った※398。本調査は、データ利活用に関する先進的な取り組みを行う企業及びデータ利活用に豊富な知見を持つ有識者 24 者に対するインタビュー調査が中心である。以下に、本調査で得られた、企業におけるデータ利活用のポイントを紹介する。

(1) データ利活用のポイント

調査の結果を、データ利活用を推進するために必要な四つの観点（「ビジネス開発」「データの共有における合意」「人材・組織」「リスクマネジメント」）に分類した。個々の観点からポイントを整理する。

(a) ビジネス開発

データを活用したビジネスモデルを構築し、事業の目標を設定する際、着目しておくべきポイントとして以下の 3 点が挙げられる。

- ビジネスの類型と価値創造の明確化

  データを活用して価値を創造するビジネスには、AI によるビッグデータ分析等の技術革新により新しいサービスを志向するものと、以前からあるデータを利用した

サービスの付加価値を向上させるものの二つの類型がある。企図するビジネスモデルの類型と、着地点となる価値創造が何か、をあらかじめ明確にしなければならない。

- 目的の具体化とデータの絞り込み
  必要となるデータはデータ利活用の目的に応じて決まるが、そのためには活用目的を具体化する必要がある。データ利活用の検討当初は何がどこまでできるかが不明瞭な場合もある。その際、小規模な PoC[※399] を繰り返しながら徐々に活用目的を明らかにし、必要となるデータを絞り込むことも重要である。
- データ利活用ビジネスに対する経営層の理解
  ビジネスモデルの構築段階から、PoC 等の試行による活用目的の明確化が必要となる等、既存の事業と異なる新たな取り組みとなることが多く、経営層の理解と判断が必要となる。

まずはこうしたデータ利活用ビジネスの特徴を理解し、適切なビジネス開発を行うことが、有効なデータ利活用の第一歩につながる。

(b) データの共有における合意

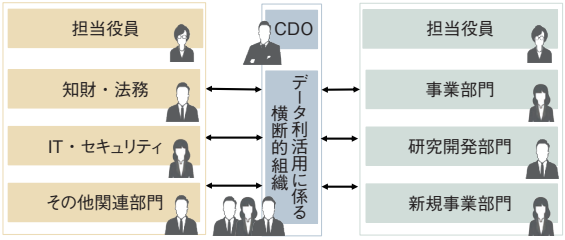
データを共有することで、自社のデータを自社のみで利用する場合と比べ、大きな価値が生まれる可能性が高まる一方で、情報漏えいリスク・法的リスク等のリスクも高まる。データ共有にあたり、こうしたリスクの把握と適切な管理が必要となる。共有するケースに応じて検討すべき事項を確認し、あらかじめ共有先と合意しておくことが重要である。

合意においては、リスクを過大にとらえて一律に広範な利用制限やアクセス制限を課すのではなく、共有相手の目的に応じて適切な利用範囲を設定し、合意することが、データ共有の効果を最大化するポイントである。試行用のデータを提供する場合は品質の保証をしないかわりに利用制限を緩和する、等の合意形成の工夫が一例である。

(c) 人材・組織

データ利活用の実務では、データに関する知識に加えて法的、経営的知見も用いて意思決定を行う必要がある。データ利活用ビジネスを行う組織には、そうした点も加味した組織のマネジメントが求められる。

- CDO 等の設置
  データ利活用に求められる知見を有し、データによるビジネス革新を推進する「データ人材」を最高データ責任者（CDO：Chief Data Officer）として設置する動きが進んでいる。CDO 等の設置により全社的なデータ利活用戦略に関する責任の所在を明確化し、経営層のコミットメントを強化することが求められる。
- 組織横断的な統括機能
  データの処理・管理・分析等のデータ利活用技術に精通したエンジニアを有する組織体制は必須である。一方、技術に限らない多様な機能（事業、IT セキュリティ、知財、法務等）との連携も求められることから、部門横断的にデータ利活用を統括する機能がポイントとなる。具体的には、機能別の組織に対して横串を通すような組織を設置することで、全社的な連携を図る等である（図 2-7-4）。



■図 2-7-4　データ利活用に係る横断的組織の機能例
（出典）IPA「企業におけるデータ利活用・保護の戦略立案のための手引書（案）の作成[※398]」を基に編集

なお、知財・法務部門は以前よりデータを企業が保有する情報資産として管理してきた部門であり、データの戦略的な保護・活用の観点から、更に横断的な機能を持たせることも一案である。

(d) リスクマネジメント

データ利活用のリスクに対する考え方として、全体最適の視点が大切である。洗い出したリスクをすべて回避するばかりでなく、適切にコントロールしてリスクを低減させること、及びデータ利活用を行わないことで逆に発生しうるビジネス上のリスク（事業機会の損失等）を考慮することが求められる。一般的にリスクはゼロにすることはできないため、最終的には意思決定権者による判断でリスク受容を行わなければならない。

(2) データ利活用の課題

データ利活用を行うビジネスを展開していく上での課題について以下に整理する。

- データ利活用ビジネス開発に特有の課題
  － 試行的な PoC の課題

データ利活用ビジネスの開始段階においては、データの価値やビジネス上のリスクをあらかじめ測ることが困難であることから、試行的な PoC の実施が有益である。一方、PoC からサービス化への次の段階へ進むケースは必ずしも多くなく、一般に相当の試行錯誤が必要であること、共同開発契約等で定めるべき事項の把握が困難であること、PoC ごとに異なる個別対応による工数がかさむこと、等の課題が挙げられる。

- 組織的課題
  - データ利活用を推進する組織づくり

    部門横断的な統括組織を設置することの重要性は認識されても、機能ごとにそれぞれ高い専門性を求められるため、一度にすべての機能を備えて組織化することは困難である。
  - 中小・ベンチャー企業や大学等との連携

    中小・ベンチャー企業や大学等と共同開発等の形でビジネスモデルの検討を行う場合、連携を支援する IT 投資や知財、法務面での支援機能が充実していないケースが多い。そうした場合、これらの課題を解決しながらデータ利活用を推進することが困難である。
- データの価値・品質・リスクの測定
  - データの価値の測り方

    自社の複数の部門間、あるいは他社とのデータの共有にあたり、データの価値（対価）を測る共通指標が必ずしも確立されていない。これはビジネスモデル策定の障害となりうる。
  - データの品質の測り方

    データをビジネスに利用するには満足できる「データの品質」を規定しておくことが必要となるが、その定義がデータ利活用を行う当事者間で必ずしも定まっていない。データの品質に関する基準を明らかにするためには、当事者間で PoC 段階やサービスのリリース段階において都度契約で定める、あるいは事前調整により品質指標を策定する、等の複合的な施策が必要と想定される。
  - リスクの測り方

    データ利活用に伴うビジネス上のリスクを総合的に測ることが困難である。特に、データの不適切な使用や情報漏えい等に起因するレピュテーションリスクに関しては、予測することが極めて困難となる。これらを明確に把握できないことが、経営層がデータ利活用ビジネスにおけるリスクテイクを行えない要因の一つとなっている。

(3) データ利活用ビジネスと情報セキュリティの課題

データ利活用を行うビジネスに関するセキュリティ視点からの課題をまとめる。

前述のとおり、ビジネスモデルの開発が重要であり、ビジネスモデルを確立し、必要な精度で目的を実現するための試行が必須である。このとき、セキュリティやプライバシーに十分に配慮しながら、試行が容易に行えるような利用範囲・データ保護ルールを作ることが重要である。例えば、一部個人情報を含むデータによる試行においてはセキュリティ・プライバシー保護対策を厳しくルール化する一方、個人を特定できる情報を含まないテスト用データを別途作成して自由な流通や複製を許容し、より簡易に試行を行えるようにする、等の方策が考えられる。

同時に、データの漏えい、あるいは不正な転用によるビジネスリスク評価はセキュリティ観点からも大きな課題であり、漏えい防止・不正転用に関するルールの整備とともに、万一そのような事態が起きた場合のリスク評価や計測の手法が求められる。海外においては、データの価値・品質・リスクの測り方等に関し、定量的に分析する方法が報告されている※400 が、前述のレピュテーションリスクの評価・計測の検討は進んでおらず、対応は容易ではないと考えられる。一方で、インシデントに関するレピュテーションリスクは、情報開示を適切に行う、等のリスクマネジメント体制の整備により小さく抑えられる可能性がある。このように、データ利活用ビジネスの経営判断には、組織のリスクマネジメント体制を含めたリスク評価手法の充実が重要である。

2.7.3 暗号技術の動向

本項では 2019 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

共通鍵暗号に対する攻撃に関する研究として、2019 年度の大きなトピックは、「CRYPTREC 暗号リスト」の「運用監視暗号リスト」に掲載されているハッシュ関数 SHA-1 に対する攻撃が更に進展し、chosen-prefix collision attack と呼ばれる攻撃に成功したことを述べた論文※401 が Eurocrypt2019 で発表されたことである。本攻撃手

法は後述する collision attack より強力で、実環境における証明書やアプリケーション等の偽造につながり、ひいては TLS 等のインターネットプロトコルの安全性を揺るがす可能性がある。実際、過去にはハッシュ関数 MD5 に対する chosen-prefix collision attack が発表された翌年（2008 年）の年末に TLS で利用される中間 CA 証明書の偽造攻撃に成功したことが公表[※402]され、MD5 を使った証明書が一掃される契機ともなった。

(a) chosen-prefix collision attack とは

ハッシュ関数の攻撃には三つの段階がある。

第一段階は free-start collision attack と呼ばれるもので、本来は固定値である初期ベクトルの値を攻撃者が自由に設定した上で衝突するメッセージ組を見つける攻撃手法である。メッセージだけでなく、初期ベクトルも攻撃者が調整できるので衝突を見つけやすい。

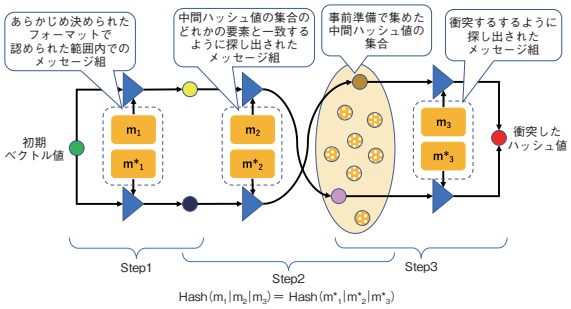
次の段階が collision attack と呼ばれるもので、メッセージだけを調整して衝突するメッセージ組を見つける攻撃手法である。一般に「ハッシュ関数の衝突」という場合はこの段階のことを言う。しかし、この攻撃手法では攻撃者がメッセージを制約なく調整できることが前提であるため、実環境の中では取りえない値のメッセージになる可能性もある。そういった場合には、アプリケーション側でのエラーチェック等で不正を検知できる可能性がある。

最後の段階が chosen-prefix collision attack である。これは、攻撃者が調整できるメッセージにある種の制約を加えた上で衝突するメッセージ組を見つける攻撃手法である。例えば、証明書の発行番号や発行者情報、有効期間等の部分はフォーマットがあらかじめ決まっていることから、そのフォーマットで認められる範囲内に収まるようにメッセージを調整した上で衝突するメッセージ組を見つける。こうすることによって、アプリケーション側でのエラーチェック等もすり抜けることが可能になる。

(b) 攻撃手法の概要

本攻撃手法は、MD5 や SHA-1、SHA-2 のような Merkle-Damgård 型のハッシュ関数を攻撃対象としている。攻撃は以下の事前準備と 3 ステップで行われる。Step1 から Step3 までで求めたメッセージ組（のブロック）を連結したものが衝突するメッセージ組となる（図 2-7-5）。

- ［事前準備］　Step3 で衝突するようなメッセージ組を作り出せる可能性が高い中間ハッシュ値の集合を集めておく。
- ［Step1］　あらかじめ決められたフォーマットで認められる範囲内に収まるような同じ長さのメッセージ組（のブロック）を作る。この部分が chosen-prefix に相当し、攻撃者にとっての制約条件となる。
- ［Step2］　Step1 で求めたメッセージ組に対して計算したハッシュ値それぞれを初期ベクトルとみなして、それぞれが事前準備で用意した集合中のどれかの要素と同じ中間ハッシュ値になるようなメッセージ組（のブロック）を探す。
- ［Step3］　Step2 で求めたメッセージ組に対して計算した中間ハッシュ値（事前準備で用意した集合のなかのある要素）から衝突するようなメッセージ組（のブロック）を探す。



■図 2-7-5　Eurocrypt2019 で発表された攻撃手法のイメージ

(c) 攻撃論文のインパクト

SHA-1 に対する chosen-prefix collision attack が可能であることが示されたものの、MD5 に対する場合と比較すると約 100 万～ 1 億倍以上の計算量が必要と見積もられている。このため、MD5 のときのような中間 CA 証明書の偽造攻撃が成功する、等の事態が直ちに発生する可能性は低いと考えられる。しかしながら、chosen-prefix collision attack が可能と示されたこと自体がハッシュ関数の安全性にとって従来とは違うステージに入ったことを意味しており、SHA-1 の寿命が尽きるところにまた一歩近づいたことになる。

(2) 公開鍵暗号に関する研究及び標準化の動向

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、2019 年 1 月 30 日に候補暗号を 64 件から 26 件に絞って第 2 ラウンドに入り、PQC を対象とする公開鍵暗号の研究はますます盛んになっている。直前に行われた暗号国際会議 CRYPTO と併催される形で、2019 年 8 月 24 ～ 26 日に米国カリフォルニア州サンタバーバラにて第 2 回 NIST PQC 標準化会議が開催された。同会議では各候補暗号の前回からの変更点の紹介、

及び安全性・処理性能・消費電力等、様々な観点からの評価結果が発表された。第1ラウンドから第2ラウンドへの応募暗号数の変化の内訳を表2-7-3に示す。

	署名	鍵確立／暗号化	合計
格子ベース	5→3	21→9	26→12
符号ベース	2→0	17→7	19→7
多変数	7→4	2→0	9→4
対称／ハッシュベース	3→2	0→0	3→2
その他	2→0	5→1	7→1
合計	19→9	45→17	64→26

■表2-7-3　NIST PQCコンペティション応募暗号数（第1ラウンド→第2ラウンド）
（出典）Dustin Moody（NIST）「The 2nd Round of the NIST PQC Standardization Process※403」を基にIPAが編集

会議冒頭にNISTのDustin Moody氏から開会挨拶があり、①候補暗号間の統合（マージ）はまだ許容されること、②第2ラウンドは12ヵ月～18ヵ月かかり、その後第3ラウンドに入ると予想していること、③ドラフト標準は2022年ごろを期待していること、④第2ラウンドは処理性能が大きな役割を果たすであろうこと等が述べられた。

今後は2020年7月ごろに候補を絞り込んだ後、第3ラウンドに入ることが予想される。2022～2024年ごろのドラフト標準作成やその後の標準化を通じて、2030年ごろを目指して移行を進めていく予定である。

(3) 軽量暗号に関する研究及び標準化の動向

NISTは、IoTやセンサーネットワーク、ヘルスケア等の制約のある環境で用いる暗号の標準化のため、2015年に「軽量暗号」のプロジェクトを開始した。候補暗号は公募され、2019年4月に応募された57件のうち56件を第1ラウンドの候補として発表、2019年8月に第2ラウンドとして更に32件に絞った※404。この32件中、日本人研究者が関与する候補暗号は11件である。

今後は、2020年9月ごろに第3ラウンドとして更に候補数を絞り、2021年に最終的に選抜したアルゴリズムを発表する予定である。

(4) 実装攻撃に関する研究の動向

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。

サイドチャネル攻撃に関しては、暗号のソフトウェア実装のキャッシュタイミングを利用したサイドチャネル攻撃（タイミング攻撃）に対して脆弱なソースコードを分析する手法を提案し、具体例としてOpenSSLに対する新たな脆弱性を指摘する論文が発表された※405。これはRSA鍵生成時に、キャッシュのヒット／ヒットミスの状況による実行時間の差を利用したサイドチャネル攻撃によって、生成された鍵が復元される可能性を示すものである。この脆弱性は、CVE-2018-0737として報告されている。

DSA（Digital Signature Algorithm）及びECDSAの署名生成処理において、剰余演算時の処理時間の差を利用したタイミング攻撃を提案する論文も発表された※406。その中でDSAやECDSAを実装している既存のオープンソースソフトウェアの約半数にこの脆弱性が存在していることも示された。この脆弱性が実際に悪用可能かどうかについては研究の進展を待つ必要があるが、暗号の実装にあたっては処理時間がパラメータによらず一定時間になることを、計算過程のあらゆる場面で注意深く確認してソースコードを記述する必要があるといえる。

故障利用攻撃に関しては、ICの側面からレーザ光を照射する攻撃に関する論文が発表された※407。レーザ攻撃は、ICの背面から照射する方法が最も効果的で多く使用されるが、最近のICのパッケージ技術ではICが3次元的に複雑な構造を持つことが多くなり、背面からの攻撃が困難であるケースが増えている。そのようなICに対しても、側面からのレーザ照射が効果的であることが示された。側面からの照射は、攻撃対象の回路への距離が背面からの照射に比較して遠いため、背面からの照射より効果は劣るが、現実的な脅威になり得る程の成功率が得られることが示されたことから、この攻撃の研究の進展に注意が必要と考えられる。

2.7.4 個人情報保護法の改正

2019年12月、個人情報保護委員会は、2020年の個人情報保護法の改正に向けて、「個人情報保護法いわゆる3年ごと見直し 制度改正大綱※408（以下、大綱）」を公表した。

大綱では、利用停止等の権利の拡充、開示のデジタル化推進、6ヵ月以内に消去するデータも保有個人データに包含すること、漏えい等報告の義務化、個人データの提供先基準の明確化等の新たな規定が盛り込まれているほか、ペナルティについては重科（重い罰則）の導入

を含め、必要に応じて見直すとしている。また、データ利活用を推進するために、「仮名化情報（仮称）」を導入するとしている。

(1) 大綱の概要

公表された大綱の骨子を表 2-7-4 に示す。

	合計
I. 個人データに関する個人の権利の在り方	利用の停止、消去、第三者提供の停止の請求に係る要件の緩和
	開示のデジタル化の推進
	開示等の対象となる保有個人データの範囲の拡大
	オプトアウト規制の強化
II. 事業者の守るべき責務の在り方	漏えい等報告及び本人通知の義務化
	適正な利用義務の明確化
III. 事業者における自主的な取組を促す仕組みの在り方	認定個人情報保護団体制度の多様化
	保有個人データに関する公表事項の充実
IV. データ利活用に関する施策の在り方	「仮名化情報」の創設
	提供先において個人データとなる場合の規律の明確化
	公益目的による個人情報の取扱いに係る例外規定の運用の明確化
	個人情報の保護と有用性に配慮した利活用相談の充実
V. ペナルティの在り方	法人処罰規定に係る重科の導入など
VI. 法の域外適用の在り方及び越境移転の在り方	域外適用の範囲の拡大
	外国にある第三者への個人データの提供制限の強化
VII. 官民を通じた個人情報の取扱い	行政機関、独立行政法人等に係る法制と民間部門に係る法制との一元化
	地方公共団体の個人情報保護制度

■表 2-7-4　大綱の改訂項目
（出典）個人情報保護委員会「個人情報保護法 いわゆる 3 年ごと見直し制度改正大綱（骨子）[※409]」を基に IPA が作成

以下では、特徴的な改訂項目について述べる。

(a) 開示のデジタル化推進（骨子 I）

自己データの開示について、電磁的形式による提供を求められるようになる。これにより業者をまたいだデータの移動、すなわちポータビリティが実現可能になるものと思われる。また、現行法では 6 ヵ月以内しか保有しない短期データは開示請求の対象外であるが、これも開示対象に含まれることとなる。

(b) オプトアウト規制の強化（骨子 I）

本人が積極的に反対しない限り個人情報の利用に同意したものとみなすオプトアウトへの規制が更に強化される。具体的には、オプトアウト規定に基づき本人同意なく第三者提供できる個人データの範囲がより限定されるほか、届出事項にも追加が行われる。一方で、現行の Web サービス等においてオプトアウトの手続きが必ずしも簡易でない、という課題は残っている。

(c) 漏えい等報告の義務化（骨子 II）

個人データ漏えいが発生した場合、現行法規において、当局への通知は努力義務とされているのが改められ、件数が多い場合や要配慮個人情報の漏えい等、一定の条件を満たす場合については報告が義務化される（罰則がある）。また報告先は、個人情報保護委員会または権限委任官庁に一本化される。一方で、報告時期の限定や個人への通知等については例外規定等を設けることで、事業者にも配慮している。

(d)「仮名化情報（仮称）」の創設（骨子 IV）

現行法では、個人情報を第三者に提供する際に「個人を特定できてはならない」という厳しい要件を付加し、この要件を満たすべく匿名加工処理を義務付けている。しかし同一事業者内での利用であれば、ここまで厳しい措置をしなくてもプライバシー等への影響は小さいと考えられる。仮名化情報はこれを考慮し、同一事業者内利用における利便性を高めるため、それ単体では個人は特定できないものの「他の情報と組み合わせれば個人が特定できる」ものについて、個人の開示等請求への対応義務を緩和し、様々な分析への活用を認めるものである。一方、仮名化情報は、匿名加工情報とは異なり、それ自体が個人情報であるため、第三者への提供にあたっては原則として本人同意が必要となる。仮名化情報の導入は、EU 等での仮名化情報の利用と整合をとることも目的と考えられる。

(e) 個人データの提供先基準の明確化（骨子 IV）

現行法制では、提供における個人情報の定義を「提供元で個人が特定されうる情報」としているため、提供した情報と提供先が保有する情報とを組み合わせて個人を特定してしまうことに対応できない。特に、提供先で他の情報と照合すれば個人と紐づけされることを認識しながら、クッキー（cookie）等の識別子を含んだ情報を提供する事業形態が問題となってきている。大綱では、提供

先が上記の手段で個人を特定できることが明らかな場合、個人を特定した利用はできないことが明確化される。ただし、「明らかな」をどのように定義するかは不透明であり、個々のケースで慎重な判断が必要と考えられる。

(f) 域外適用の範囲の拡大(骨子Ⅵ)

現行法では報告徴収や立ち入り検査等の強制力のある規定は外国の事業者に適用されず、事業者に違反行為があった場合の法執行が問題となっていた。これについては、外国にある事業者への矯正法執行を認めるべきか、外国の主権を尊重して法執行すべきでないか、意見が分かれていた。大綱では、法執行できる立場に立つことを明確にし、外国事業者も報告徴収や立ち入り検査の対象とする。ただし当該国の主権も尊重し、必要に応じてその国と執行について協力する、としている。

(2) 意見聴取と改正法案の提出

大綱について、2020 年 1 月 14 日まで意見募集が行われた。個人情報保護委員会は寄せられた意見を踏まえて「個人情報の保護に関する法律等の一部を改正する法律案」を策定、同法案は 2020 年 3 月 10 日に閣議決定され※410、第 201 回通常国会に提出された。

COLUMN

情報セキュリティ活動と法整備のジレンマ

仮想通貨のマイニングをする「Coinhive（コインハイブ）」を Web サイトに設置したことで、不正指令電磁的記録保管罪でサイト運営者が検挙された「Coinhive 事件」。2019 年 1 月から開かれた Coinhive 事件の裁判では、開廷前から傍聴希望者の列ができる等、世間の興味、関心の高さがうかがえました。約 1 年後となる 2020 年 2 月には、控訴審判決で 1 審の無罪判決が破棄され、逆転有罪となったことで再び注目を集めました[i]。

2017 年 10 月には、情報セキュリティ企業の社員が不正指令電磁的記録保管容疑で逮捕された事案（2018 年に地方検察庁によって不起訴が決定）[ii]、2019 年 3 月には、ポップアップが繰り返し表示されるサイトの URL を掲示板に書き込んだとして、不正指令電磁的記録供用未遂の疑いで摘発された「アラートループ事件[iii]」等がありました。

このような、近年の不正指令電磁的記録保管罪や不正指令電磁的記録供用罪での検挙に対して、情報セキュリティに関連する活動の萎縮を懸念する声が度々挙がっていました。実際、「アラートループ事件」の直後には、参加者が逮捕される可能性があるとして Web セキュリティの勉強会を自粛するといった萎縮の動きがありました[iv]。冒頭の Coinhive 事件でも、逆転有罪の判決を受け、弁護人は活動萎縮への懸念を強めているようです[v]。

情報セキュリティやソフトウェア開発の現場から懸念の声が挙がる要因として、新しい技術の進歩のスピードと、その技術を利用する際のルールを定める法整備を含めた世の中の動きに差があることが考えられます。

これまでの技術の進歩は、例えば、活版印刷や自動車等を見ても、世に初めて登場してから長い時間をかけ少しずつ進歩していったことで、紆余曲折がありながらも、世の中の動きもその変化に対応できていたものと思われます。しかし、インターネットやスマートフォン等は、その登場から進歩のスピードが著しく早く、結果的に変化に追いついていけるものと、いけないものとの二極化が発生する状況となっているようです。

急速な技術の進歩により、昨日はできなかったことが今日はできるといった便利な世の中が実現することは喜ばしいですが、それらは皆が安心・安全に利用できるという前提があってこそとなります。情報セキュリティやソフトウェア開発においても、その活動の安心・安全を担保できるよう、迅速な法整備やガイドライン等の整備が望まれます。

i　日経クロステック：Coinhive 設置で 1 審無罪の控訴審、東京高裁がサイト運営者に逆転有罪　https://xtech.nikkei.com/atcl/nxt/news/18/07046/?i_cid=nbpnxt_reco_atype〔2020/7/10 確認〕
ITmedia NEWS：「ウイルス罪」めぐる事件、セキュリティ事業者に余波　「活動の萎縮につながる」「指針が必要」　https://www.itmedia.co.jp/news/articles/1906/28/news088.html〔2020/7/10 確認〕
ii　株式会社ディアイティ：当社社員の不正指令電磁的記録（ウイルス）保管容疑で逮捕された件について　https://www.dit.co.jp/news/archive/2017/1101.html〔2020/3/16 確認〕
iii　ITmedia NEWS：「何回閉じても無駄ですよ〜」ブラクラ URL を掲示板に貼っただけで補導、「やり過ぎ」と物議　https://www.itmedia.co.jp/news/articles/1903/05/news080.html〔2020/7/10 確認〕
iv　ITmedia NEWS：セキュリティ勉強会休止、「攻撃コードの研究発表でも逮捕されかねない」と懸念　いたずら URL 事件受け　https://www.itmedia.co.jp/news/articles/1903/20/news079.html〔2020/7/10 確認〕
v　ITmedia NEWS：Coinhive 裁判、弁護側が IT 業界から意見書募集　Web 上の声をくみあげ、最高裁に提出　https://www.itmedia.co.jp/news/articles/2002/18/news108.html〔2020/7/10 確認〕

※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〔2020/6/30 確認〕
※2　NISC：サイバーセキュリティ2019　https://www.nisc.go.jp/active/kihon/pdf/cs2019.pdf〔2020/6/30 確認〕
※3　経済産業省：CGS（第2期）取りまとめ　https://www.meti.go.jp/shingikai/economy/cgs_kenkyukai/20190628_report.html〔2020/6/30 確認〕
※4　経済産業省：「グループ・ガバナンス・システムに関する実務指針」を策定しました　https://www.meti.go.jp/press/2019/06/20190628003/20190628003.html〔2020/6/30 確認〕
※5　NISC：サイバーセキュリティ戦略・サイバーセキュリティ2019の概要　https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-cs2019-gaiyou.pdf〔2020/6/30 確認〕
※6　サイバーセキュリティタスクフォース：総務省が2017年1月に設置した、IoT/AI時代を見据えたサイバーセキュリティに係る課題を整理するとともに、情報通信分野において講ずべき対策や既存の取り組みの改善等幅広い観点から検討を行い、必要な方策を推進することを目的とした組織。
※7　総務省：サイバーセキュリティ対策情報開示の手引き　https://www.soumu.go.jp/main_content/000630516.pdf〔2020/6/30 確認〕
※8　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〔2020/6/30 確認〕
※9　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〔2020/7/29 確認〕
※10　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　とりまとめ　https://www.meti.go.jp/shingikai/mono_info_service/cloud_services/pdf/20200130_report.pdf〔2020/6/30 確認〕
※11　NISC：2020年東京オリンピック・パラリンピック競技大会に向けての取組状況　https://www.nisc.go.jp/conference/cs/dai23/pdf/23shiryou06.pdf〔2020/6/30 確認〕
※12　NISC：サイバーセキュリティ対処調整センターについて　https://www.nisc.go.jp/conference/cs/ciip/dai18/pdf/18shiryou11.pdf〔2020/6/30 確認〕
東京都：東京2020大会の安全・安心の確保のための対処要領（第二版）　http://www.metro.tokyo.jp/tosei/hodohappyo/press/2019/04/16/documents/13_02.pdf〔2020/6/30 確認〕
※13　ASEAN加盟国（ブルネイ、カンボジア、インドネシア、ラオス、ミャンマー、フィリピン、シンガポール、タイ、ベトナム）、インド、バングラディッシュ、スリランカ、ニュージーランド、台湾。
※14　IPA：中核人材育成プログラム　https://www.ipa.go.jp/icscoe/program/core_human_resource/index.html〔2020/6/30 確認〕
※15　経済産業省：「インド太平洋地域向け日米サイバー演習」を実施しました　https://www.meti.go.jp/press/2019/09/20190912009/20190912009.html〔2020/6/30 確認〕
※16　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〔2020/6/30 確認〕
※17　総務省：IoT機器調査及び利用者への注意喚起の取組「NOTICE」の実施　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00011.html〔2020/6/30 確認〕
※18　NICT：NICTER観測レポート2019　https://www.nict.go.jp/cyber/report.html〔2020/6/30 確認〕
※19　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〔2020/6/30 確認〕
※20　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（改定）　https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r1.pdf〔2020/6/30 確認〕
※21　NISC：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）　https://www.nisc.go.jp/active/infra/pdf/shishin5.pdf〔2020/6/30 確認〕
※22　NISC：活動内容　https://www.nisc.go.jp/active/infra/shisaku1.html〔2020/6/30 確認〕
※23　政府内において第4次行動計画に基づく情報共有の実施に必要な事項を定めた「重要インフラ所管省庁との情報共有に関する実施細目」。
※24　https://www.nisc.go.jp/conference/cs/ciip/dai20/pdf/20shiryou07-2.pdf〔2020/6/30 確認〕
※25　NISC：重要インフラ専門調査会第21回会合（令和2年1月29日）　資料3　分野横断的演習（2019年度）の実施結果について　https://www.nisc.go.jp/conference/cs/ciip/dai21/pdf/21shiryou03.pdf〔2020/6/30 確認〕
※26　経済産業省：「産業サイバーセキュリティ研究会」を開催します　https://www.meti.go.jp/press/2017/12/20171226004/20171226004.html〔2020/6/30 確認〕
※27　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〔2020/6/30 確認〕
※28　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〔2020/6/30 確認〕
※29　経済産業省：産業サイバーセキュリティの加速化指針 ~ アクションプランの深化・拡大 ~　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/003_04_00.pdf〔2020/6/30 確認〕
※30　対策要件のカテゴリはNISTの「Cybersecurity Framework Version 1.1」に対応する形で整理している。
※31　転写：CPSFにおいては、温度や距離等の物理事象をデータに変換するといった、サイバー空間とフィジカル空間の境界において行われる情報の変換を意味する。
※32　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　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/dainiso/pdf/002_03_00.pdf〔2020/6/30 確認〕
※33　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/002_03_00.pdf〔2020/6/30 確認〕
※34-1　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/003_03_00.pdf〔2020/6/30 確認〕
※34-2　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/pdf/20190617_01.pdf〔2020/7/27 確認〕
※35　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〔2020/6/30 確認〕
※36　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〔2020/6/30 確認〕
※37　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）　https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html〔2020/6/30 確認〕
※38　「サイバーセキュリティ戦略」（https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf〔2020/6/30 確認〕）では、「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」と定義している。
※39　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/005_03_00.pdf〔2020/6/30 確認〕
※40　経済産業省：事務局説明資料（産業サイバーセキュリティ研究会WG3（サイバーセキュリティビジネス化）第3回）　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/pdf/003_03_00.pdf〔2020/6/30 確認〕
※41　IPA：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　https://www.ipa.go.jp/security/economics/kensyokiban2019.html〔2020/6/30 確認〕
※42　IPA：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/shikoukekka2019.html〔2020/6/30 確認〕
※43　https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf〔2020/6/30 確認〕
※44　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〔2020/6/30 確認〕
※45　https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2018_zentai.pdf〔2020/6/30 確認〕
※46　https://www.meti.go.jp/press/2019/01/20200130002/20200130002-1.pdf〔2020/6/30 確認〕
※47　サイバーセキュリティ戦略本部：「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」　https://www.nisc.go.jp/active/general/pdf/wakugumi2020.pdf〔2020/6/30 確認〕
※48　https://www.ipa.go.jp/files/000082669.pdf〔2020/6/30

確認〕
※ 49 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）における各種基準（案）の意見公募手続（パブリックコメント）を開始しました https://www.meti.go.jp/press/2019/03/20200327017/20200327017.html
※ 50 https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf〔2020/6/30 確認〕
※ 51 https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex04.pdf〔2020/6/30 確認〕
※ 52 https://www.ipa.go.jp/files/000082279.pdf〔2020/6/30 確認〕
※ 53 https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20191220/siryou.pdf〔2020/6/30 確認〕
※ 54 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
※ 55 IPA：政府情報システムのためのセキュリティ評価制度（ISMAP） https://www.ipa.go.jp/security/ismap/index.html〔2020/6/30 確認〕
※ 56 https://www.nisc.go.jp/active/infra/pdf/shishin5rev.pdf〔2020/6/30 確認〕
※ 57 経済産業省：データの利用権限に関する契約ガイドライン ver1.0 https://www.meti.go.jp/press/2017/05/20170530003/20170530003-1.pdf〔2020/6/30 確認〕
※ 58 経済産業省：「AI・データの利用に関する契約ガイドライン」を策定しました https://www.meti.go.jp/press/2018/06/20180615001/20180615001.html〔2020/6/30 確認〕
※ 59 経済産業省：「不正競争防止法等の一部を改正する法律案」が閣議決定されました https://www.meti.go.jp/press/2017/02/20180227001/20180227001.html〔2020/6/30 確認〕
※ 60 経済産業省：限定提供データに関する指針 https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31pd.pdf〔2020/6/30 確認〕
※ 61 経済産業省：「AI・データの利用に関する契約ガイドライン 1.1 版」を策定しました https://www.meti.go.jp/press/2019/12/20191209001/20191209001.html〔2020/6/30 確認〕
※ 62 衆議院：議案名「産業競争力強化法等の一部を改正する法律案」の審議経過情報 http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/keika/1DC7D8E.htm〔2020/6/30 確認〕
経済産業省：「産業競争力強化法」の一部改正が施行されました https://www.meti.go.jp/press/2018/07/20180709006/20180709006.html〔2020/6/30 確認〕
※ 63 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〔2020/6/30 確認〕
※ 64 経済産業省：情報セキュリティ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ました https://www.meti.go.jp/press/2017/02/20180228002/20180228002.html〔2020/6/30 確認〕
※ 65 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。
※ 66 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〔2020/6/30 確認〕
※ 67 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。
※ 68 https://www.ipa.go.jp/files/000081877.pdf〔2020/6/30 確認〕
※ 69 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019年 7 月～ 9 月］ https://www.ipa.go.jp/files/000078200.pdf〔2020/6/30 確認〕
※ 70 「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。
※ 71 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019年 10 月～ 12 月］ https://www.ipa.go.jp/files/000080133.pdf〔2020/6/30 確認〕
※ 72 トレンドマイクロ株式会社：サイバー攻撃集団「TICK」による「Operation ENDTRADE」 https://blog.trendmicro.co.jp/archives/23107〔2020/6/30 確認〕
※ 73 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〔2020/6/30 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〔2020/6/30 確認〕
※ 74 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〔2020/6/30 確認〕
※ 75 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〔2020/7/7 確認〕
※ 76 https://www.soumu.go.jp/main_content/000641510.pdf〔2020/7/7 確認〕
※ 77 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〔2020/7/7 確認〕
※ 78 総務省：新規制定・改正法令・告示 法律 https://www.soumu.go.jp/menu_hourei/s_houritsu.html〔2020/7/7 確認〕
上記 Web ページの「電気通信事業法及び国立開発研究法人情報通信研究機構法の一部を改正する法律（平成 30 年法律第 24 号）」を参照。
※ 79 https://notice.go.jp/〔2020/7/7 確認〕
※ 80 NISC：IoT機器調査及び利用者への注意喚起プロジェクト https://www.nisc.go.jp/conference/cs/dai21/pdf/21sankou.pdf〔2020/7/7 確認〕
Security NEXT：政府の脆弱 IoT 機器調査「NOTICE」、2 月 20 日から - イメージキャラクターにカンニング竹山さん http://www.security-next.com/102208〔2020/7/7 確認〕
※ 81 総務省・NICT・一般社団法人 ICT-ISAC：脆弱な IoT 機器及びマルウェアに感染している IoT 機器の利用者への注意喚起の実施状況 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00033.html〔2020/7/7 確認〕
※ 82 総務省：端末設備等規則等の一部改正について https://www.soumu.go.jp/main_content/000581187.pdf〔2020/7/7 確認〕
※ 83 総務省：第5世代移動通信システム（5G）の導入のための特定基地局の開設計画の認定（概要） https://www.soumu.go.jp/main_content/000613734.pdf〔2020/7/7 確認〕
※ 84 総務省：ローカル5G導入に関するガイドライン https://www.soumu.go.jp/main_content/000659870.pdf〔2020/7/7 確認〕
※ 85 高い倫理感、技術力を持ち合わせたハッカーをエシカルハッカーと呼ぶ。
※ 86 国立研究開発法人情報通信研究機構、公立大学法人首都大学東京：耐量子計算機暗号の安全性評価で世界記録を達成 https://www.nict.go.jp/press/2019/06/27-1.html〔2020/7/7 確認〕
※ 87 総務省：総務省におけるサイバーセキュリティ研究開発の取組み https://www.nisc.go.jp/conference/cs/kenkyu/dai10/pdf/10shiryou05.pdf〔2020/7/7 確認〕
※ 88 https://www.soumu.go.jp/main_content/000555901.pdf〔2020/7/7 確認〕
※ 89 総務省：サイバー攻撃の防御に向けた情報共有基盤に関する実証事業の成果の公表 https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000153.html〔2020/7/7 確認〕
※ 90 IPA：脅威情報構造化記述形式 STIX 概説 https://www.ipa.go.jp/security/vuln/STIX.html〔2020/7/7 確認〕
※ 91 NICT：実践的サイバー防御演習「CYDER」 https://cyder.nict.go.jp/〔2020/7/7 確認〕
※ 92 NICT：cyber colosseo https://colosseo.nict.go.jp/〔2020/7/7 確認〕
※ 93 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〔2020/7/7 確認〕
※ 94 https://www.soumu.go.jp/main_content/000575052.pdf〔2020/7/7 確認〕
※ 95 総務省：プラットフォームサービスに関する研究会の開催 https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000050.html〔2020/7/7 確認〕
※ 96 総務省：トラストサービス検討ワーキンググループ（第 1 回） https://www.soumu.go.jp/main_sosiki/kenkyu/platform_service/02cyber01_04000001_00016.html〔2020/7/7 確認〕
※ 97 総務省：プラットフォームサービスに関する研究会最終報告書 https://www.soumu.go.jp/main_content/000668595.pdf〔2020/7/7 確認〕
※ 98 NISC：サイバーセキュリティ戦略の変更について https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf〔2020/7/6 確認〕
※ 99 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〔2020/7/6 確認〕
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〔2020/7/6 確認〕
※ 100 警察庁：令和元年におけるサイバー空間をめぐる脅威の情勢等について https://www.npa.go.jp/publications/statistics/cybersecurity/data/R01_cyber_jousei.pdf〔2020/7/6 確認〕

※ 101 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〔2020/7/6 確認〕
※ 102 警察庁：フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（全銀協等と連携した注意喚起） http://www.npa.go.jp/cyber/policy/caution1910.html〔2020/7/6 確認〕
※ 103 JC3：クレジットカード情報窃取の手口に注意 https://www.jc3.or.jp/topics/credit_card.html〔2020/7/6 確認〕
※ 104 警察庁：令和元年の国際協力等の状況 https://www.npa.go.jp/about/overview/kokusai/kyouryoku/R01.pdf〔2020/7/6 確認〕
※ 105 https://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_cyber_jousei.pdf〔2020/7/6 確認〕
※ 106 サイバーセキュリティ.com：人事情報など167万件を不正閲覧、男性職員を停職及び降任処分｜長崎県 https://cybersecurity-jp.com/news/34706〔2020/7/6 確認〕
※ 107 産経新聞：7pay詐欺容疑で逮捕 熊本県警 https://www.sankei.com/region/news/191004/rgn1910040021-n1.html〔2020/7/6 確認〕
※ 108 産経新聞：ゲームアプリ不正使用の疑い https://www.sankei.com/region/news/191102/rgn1911020020-n1.html〔2020/7/6 確認〕
※ 109 日本経済新聞：元漫画村運営者「責任ある」、起訴内容認める 福岡 https://www.nikkei.com/article/DGXMZO53408570W9A211C1ACYZ00/〔2020/7/20 確認〕
※ 110 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-0001-2012r4.pdf〔2020/6/30 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。
※ 111-1 NIST:FIPS 186-5(Draft) Digital Signature Standard (DSS) https://csrc.nist.gov/publications/detail/fips/186/5/draft〔2020/6/30 確認〕
※ 111-2 IPA：暗号鍵管理ガイドライン https://www.ipa.go.jp/security/vuln/ckms.html〔2020/7/22 確認〕
※ 111-3 IPA:TLS 暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～ https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html〔2020/7/22 確認〕
※ 112 外務省：G20 大阪サミット https://www.mofa.go.jp/mofaj/gaiko/g20/osaka19/jp/〔2020/6/30 確認〕
※ 113 World Economic Forum 2019 https://www.weforum.org/events/world-economic-forum-annual-meeting-2019〔2020/6/30 確認〕
※ 114 外務省：大阪トラック https://www.mofa.go.jp/mofaj/ecm/it/page25_001989.html〔2020/6/30 確認〕
※ 115 外務省：河野外務大臣の G20 貿易・デジタル経済大臣会合（茨城県つくば市）への出席（結果） https://www.mofa.go.jp/mofaj/ecm/it/page4_005041.html〔2020/6/30 確認〕
※ 116 外務省：G20 AI 原則 https://www.mofa.go.jp/mofaj/gaiko/g20/osaka19/pdf/documents/jp/annex_08.pdf〔2020/6/30 確認〕
※ 117 U.S. Department of State：The Seventh U.S.-Japan Cyber Dialogue https://www.state.gov/the-seventh-u-s-japan-cyber-dialogue/〔2020/6/30 確認〕
※ 118 外務省：日米首脳会談 https://www.mofa.go.jp/mofaj/na/na1/us/page4_005001.html〔2020/6/30 確認〕
※ 119 防衛省：日米サイバー防衛政策ワーキンググループ（CDPWG）第7回会合について https://www.mod.go.jp/j/press/news/2019/10/25b.html〔2020/6/30 確認〕
※ 120 外務省：第4回日 EU サイバー対話 https://www.mofa.go.jp/mofaj/erp/ep/page23_003018.html〔2020/6/30 確認〕
※ 121 外務省：サイバー犯罪に関する条約（略称：サイバー犯罪条約） https://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html
※ 122 外務省：第5回日仏サイバー協議の開催 https://www.mofa.go.jp/mofaj/fp/cp/page22_003266.html〔2020/6/30 確認〕
※ 123 外務省：サイバー規範イニシアティブに関するディナール宣言 https://www.mofa.go.jp/mofaj/files/000466471.pdf〔2020/6/30 確認〕
※ 124 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〔2020/6/30 確認〕
※ 125 外務省：日英首脳会談 https://www.mofa.go.jp/mofaj/area/uk/page6_000372.html〔2020/6/30 確認〕
※ 126 BBC：What is the transition period? https://www.bbc.com/news/uk-politics-50838994〔2020/6/30 確認〕
※ 127 外務省：第3回日露サイバー協議の開催 https://www.mofa.go.jp/mofaj/press/release/press4_008022.html〔2020/6/30 確認〕
※ 128 外務省：第2回日ウクライナサイバー協議 https://www.mofa.go.jp/mofaj/erp/c_see/ua/page25_002085.html〔2020/6/30 確認〕
※ 129 総務省：第12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_00049.html〔2020/6/30 確認〕
※ 130 http://aseanregionalforum.asean.org/〔2020/6/30 確認〕
※ 131 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3回専門家会合の開催 https://www.mofa.go.jp/mofaj/press/release/press4_007030.html〔2020/6/30 確認〕
※ 132 外務省：サイバーセキュリティに関する第2回 ARF 会期間会合等の開催 https://www.mofa.go.jp/mofaj/press/release/press4_007262.html〔2020/6/30 確認〕
※ 133 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5回専門家会合の開催 https://www.mofa.go.jp/mofaj/press/release/press4_008249.html〔2020/6/30 確認〕
※ 134 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る会合。GGE は過去 5 会期にわたり実施されている。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。
※ 135 正式名称は「国際安全保障の文脈における情報及び電気通信分野での発展に関するオープン・エンド作業部会」。2018 年 12 月、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参加可能な議論の場として、2019 年より国連のもとに初めて立ち上がる会合。2019 年 9 月に第 1 回会合を開催し、全部で 3 回の本会合を経て 2020 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。
※ 136 外務省：第3回日・インドサイバー対話の開催 https://www.mofa.go.jp/mofaj/press/release/press1_000330.html〔2020/6/30 確認〕
「情報セキュリティ白書 2019」の「2.2.1（6）インドとのサイバー連携」（p.82）を参照。
※ 137 慶應義塾大学：第9回サイバーセキュリティ国際シンポジウム https://cysec-lab.keio.ac.jp/sympo1912/index-j.html〔2020/6/30 確認〕
※ 138 ICT ISAC Japan：サイバーセキュリティ国際シンポジウム https://www.ict-isac.jp/news/news20191008.html〔2020/6/30 確認〕
※ 139 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 2019 https://project.nikkeibp.co.jp/event/19z1212cit/〔2020/6/30 確認〕
※ 140 時事通信社：米中、貿易協議「第1段階」合意 追加関税の発動見送り―来月めど署名 https://www.jiji.com/jc/article?k=2019121400242&g=int〔2020/6/30 確認〕
※ 141 時事通信社：米中「第1段階」合意発効 初の関税下げ―摩擦緩和も火種残る https://www.jiji.com/jc/article?k=2020021400772&g=int〔2020/6/30 確認〕
※ 142 時事通信社：米政府、中国製マスクの制裁関税免除 新型コロナ配慮か https://www.jiji.com/jc/article?k=2020030700350&g=int〔2020/6/30 確認〕
※ 143 The Washington Post：Apparently, Trump ignored early coronavirus warnings. That has consequences https://www.washingtonpost.com/politics/2020/03/23/apparently-trump-ignored-early-coronavirus-warnings-that-has-consequences/〔2020/6/30 確認〕
※ 144 BBC：Trump declares national emergency over coronavirus https://www.bbc.com/news/world-us-canada-51882381〔2020/6/30 確認〕
※ 145 BBC：Coronavirus: US to halt funding to WHO, says Trump https://www.bbc.com/news/world-us-canada-52289056〔2020/6/30 確認〕
※ 146 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〔2020/6/30 確認〕
※ 147 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 https://jp.reuters.com/article/health-coronavirus-usa-idJPKBN22C3ZE〔2020/6/30 確認〕
※ 148 時事通信社：偽ニュース拡散、中国非難 警戒強めるEU―新型コロナ https://www.jiji.com/jc/article?k=2020061100867&g=int〔2020/6/30 確認〕
※ 149 Bloomberg：Trump Says U.S. Must Reopen Even If More Americans Get Sick, Die https://www.bloomberg.com/news/articles/2020-05-05/trump-says-u-s-must-reopen-even-if-more-americans-get-sick〔2020/6/30 確認〕
※ 150 CONGRESS.GOV：H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019 https://www.

congress.gov/bill/115th-congress/house-bill/5515/text〔2020/6/30 確認〕
※ 151 5 社とは、Huawei Technologies Co. Ltd.（ネットワーク機器）、ZTE Corporation（通信機器）、Hangzhou Hikvision Digital Technology Co., Ltd.（監視カメラ）、Dahua Technology Co. Ltd.（防犯カメラ）、Hytera Communications Co. Ltd.（無線機）。
※ 152 CONGRESS.GOV：H.R.2500 - National Defense Authorization Act for Fiscal Year 2020 https://www.congress.gov/bill/116th-congress/house-bill/2500〔2020/6/30 確認〕
※ 153 Cyberspace Solarium Commission：https://www.solarium.gov/home〔2020/6/30 確認〕
※ 154 BUSINESS INSIDER：A senate report says the US government's current plan to prepare for cyber doomsday isn't nearly strong enough https://www.businessinsider.com/senate-report-says-us-government-needs-stronger-cyber-doomsday-plan-2020-3〔2020/6/30 確認〕
※ 155 DoD：SUMMARY DEPARTMENT OF DEFENSE CYBER STRATEGY 2018 https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF〔2020/6/30 確認〕
※ 156 COUNCIL ON FOREIGN RELATIONS：U.S. Cyber Command's Malware Inoculation: Linking Offense and Defense in Cyberspace https://www.cfr.org/blog/us-cyber-commands-malware-inoculation-linking-offense-and-defense-cyberspace〔2020/6/30 確認〕
※ 157 U.S. Cyber Command：https://www.cybercom.mil/〔2020/6/30 確認〕
※ 158 DoD：DOD to Require Cybersecurity Certification in Some Contract Bids https://www.defense.gov/Explore/News/Article/Article/2071434/dod-to-require-cybersecurity-certification-in-some-contract-bids/〔2020/6/30 確認〕
※ 159 NIST：SP 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final〔2020/6/30 確認〕
※ 160 Defense Federal Acquisition Regulation Supplement：DFARS 252.204-7012 Defense Industrial Base Compliance Information https://www.acq.osd.mil/eie/Downloads/IE/DFARS%207012%20Information%20Paper.pdf〔2020/6/30 確認〕
※ 161 DoD：DOD Announces Enterprise General Purpose Cloud Contract Award https://www.defense.gov/Newsroom/Releases/Release/Article/1999651/dod-announces-enterprise-general-purpose-cloud-contract-award/〔2020/6/30 確認〕
※ 162 ZDNet：US Federal Court judge grants AWS request to temporarily block JEDI contract work https://www.zdnet.com/article/u-s-federal-court-judge-grants-aws-request-to-temporarily-block-jedi-contract-work/〔2020/6/30 確認〕
※ 163 WIRED：Microsoft Is the Surprise Winner of a $10B Pentagon Contract https://www.wired.com/story/microsoft-surprise-winner-dollar10b-pentagon-contract/〔2020/6/30 確認〕
※ 164 DoD：DOD Adopts Ethical Principles for Artificial Intelligence https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/source/GovDelivery/〔2020/6/30 確認〕
※ 165 The White House：Artificial Intelligence for the American People https://www.whitehouse.gov/ai/〔2020/6/30 確認〕
※ 166 DHS：CISA https://www.cisa.gov/〔2020/6/30 確認〕
※ 167 Task Forceについては「情報セキュリティ白書2019」の「2.2.2(2)(c)戦略の分析」(p.86)を参照。
※ 168 CISA：CISA'S ICT SUPPLY CHAIN RISK MANAGEMENT TASK FORCE APPROVES NEW WORKING GROUP FOR SECOND PHASE https://www.cisa.gov/news/2019/12/18/cisas-ict-supply-chain-risk-management-task-force-approves-new-working-group-second〔2020/6/30 確認〕
※ 169 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/〔2020/6/30 確認〕
※ 170 The White House：Executive Order on Securing the Information and Communications Technology and Services Supply Chain https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/〔2020/6/30 確認〕
※ 171 Federal Register：Securing the Information and Communications Technology and Services Supply Chain https://www.federalregister.gov/documents/2019/12/23/2019-27596/securing-the-information-and-communications-technology-and-services-supply-chain〔2020/6/30 確認〕
※ 172 Business Roundtable：Business Roundtable Comments to the Proposed Rule on Securing the Information and Communications Technology and Services Supply Chain https://www.businessroundtable.org/business-roundtable-comments-to-the-proposed-rule-on-securing-the-information-and-communications-technology-and-services-supply-chain〔2020/6/30 確認〕
※ 173 CISA：EXECUTIVE ORDER 13873 RESPONSE https://www.cisa.gov/sites/default/files/publications/eo-response-methodology-for-assessing-ict_v2_508.pdf〔2020/6/30 確認〕
※ 174 BBC：Qasem Soleimani: US kills top Iranian general in Baghdad air strike https://www.bbc.com/news/world-middle-east-50979463〔2020/6/30 確認〕
※ 175 CISA：CISA INSIGHTS Increased Geopolitical Tensions and Threats https://www.cisa.gov/sites/default/files/publications/CISA-Insights-Increased-Geopolitical-Tensions-and-Threats-S508C.pdf〔2020/6/30 確認〕
※ 176 CISA：Defending Against COVID-19 Cyber Scams https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams〔2020/6/30 確認〕
※ 177 CISA：CISA INSIGHTS Risk Management for Novel Coronavirus (COVID-19) https://www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf〔2020/6/30 確認〕
※ 178 FBI：Protect Your Wallet—and Your Health—from Pandemic Scammers https://www.fbi.gov/news/stories/protect-yourself-from-covid-19-scams-040620
※ 179 CISA：Alert (AA20-099A) https://www.us-cert.gov/ncas/alerts/aa20-099a〔2020/6/30 確認〕
※ 180 CISA：Alert (AA20-126A) https://www.us-cert.gov/ncas/alerts/AA20126A〔2020/6/30 確認〕
※ 181 CISA：Telework Guidance and Resources https://www.cisa.gov/telework〔2020/6/30 確認〕
※ 182 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〔2020/6/30 確認〕
※ 183 BBC：Brexit: UK leaves the European Union https://www.bbc.com/news/uk-politics-51333314〔2020/6/30 確認〕
※ 184 Bloomberg：U.K. and EU Draw Battle Lines as the Hard Part of Brexit Begins https://www.bloomberg.com/news/articles/2020-01-20/u-k-eu-draw-battle-lines-as-the-hard-part-of-brexit-begins〔2020/6/30 確認〕
※ 185 House of Commons Library：The UK-EU future relationship negotiations: process and issues https://commonslibrary.parliament.uk/research-briefings/cbp-8834/〔2020/6/30 確認〕
※ 186 欧州逮捕状（EAW）：EU 加盟国が、犯罪組織への参加、テロ行為、サイバー犯罪、殺人等の犯罪に加担したとして他の EU 加盟国が発行する逮捕状を自国で執行するシステム。
※ 187 European Court of Human Rights/Council of Europe:ヨーロッパにおける人権および基本的自由の保護のための条約 https://www.echr.coe.int/Documents/Convention_JPN.pdf〔2020/6/30 確認〕
※ 188 European Union External Action：The Common Security and Defence Policy (CSDP) https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/431/common-security-and-defence-policy-csdp_en〔2020/6/30 確認〕
※ 189 legislation.gov.uk：Investigatory Powers Act 2016 http://www.legislation.gov.uk/ukpga/2016/25/section/1/enacted〔2020/6/30 確認〕
※ 190 GOV.UK：The NIS Regulations 2018 https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018〔2020/6/30 確認〕
※ 191 Taylor & Francis Online: Brexit and Cyber Security https://www.tandfonline.com/doi/full/10.1080/03071847.2019.1643256〔2020/6/30 確認〕
※ 192 ZDNET：After Brexit, Europe wants cybersecurity pact with UK https://www.zdnet.com/article/after-brexit-europe-wants-cybersecurity-pact-with-uk/〔2020/6/30 確認〕
※ 193 ICO：Intention to fine British Airways £183.39m under GDPR for data breach https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-

british-airways/〔2020/6/30 確認〕
※ 194 ICO: Statement：Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach〔2020/6/30 確認〕
※ 195 DIGIDAY：250 億円!：GDPR 違反で、初の大型制裁金が科せられる https://digiday.jp/brands/2019-is-the-year-of-enforcement-gdpr-fines-have-begun/〔2020/6/30 確認〕
※ 196 European Data Protection Board：Administrative criminal proceedings of the Austrian data protection authority against Österreichische Post AG (Austrian Postal Service) https://edpb.europa.eu/news/national-news/2019/administrative-criminal-proceedings-austrian-data-protection-authority_en〔2020/6/30 確認〕
※ 197 LEXOLOGY：Austria：Data Protection Authority imposes EUR 18 million fine on Austrian Post https://www.lexology.com/library/detail.aspx?g=7865633f-6ad1-4919-911f-81c11ec65567〔2020/6/30 確認〕
※ 198 European Data Protection Board：Berlin Commissioner for Data Protection Imposes Fine on Real Estate Company https://edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_en〔2020/6/30 確認〕
※ 199 European Data Protection Board：MARKETING: THE ITALIAN SA FINES TIM EUR 27.8 MILLION https://edpb.europa.eu/news/national-news/2020/marketing-italian-sa-fines-tim-eur-278-million_en〔2020/6/30 確認〕
GARANTE：Provvedimento correttivo e sanzionatorio nei confronti di TIM S.p.A. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9256486〔2020/6/30 確認〕
※ 200 EC：The Cybersecurity Act strengthens Europe's cybersecurity https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity〔2020/6/30 確認〕
※ 201 EU：REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&qid=1579157494056&from=EN〔2020/6/30 確認〕
※ 202 Jones Day：INSIGHTS The EU Cybersecurity Act is Now Applicable https://www.jonesday.com/en/insights/2019/06/the-eu-cybersecurity-act-is-now-applicable〔2020/6/30 確認〕
※ 203 CEN-CENELEC Management Centre：Cybersecurity Act - Establishing the link between Srandardization and Certification https://www.cencenelec.eu/News/Events/Pages/EV-2018-001.aspx〔2020/6/30 確認〕
※ 204 EU サイバーセキュリティ庁：Conference: Towards the EU Cybersecurity Certification Framework https://www.enisa.europa.eu/events/towards_security_framework/towards_security_framework〔2020/6/30 確認〕
※ 205 EU サイバーセキュリティ庁：Conference: Towards the EU Cybersecurity Certification Framework https://www.enisa.europa.eu/events/towards_certification_framework/towards_security_framework〔2020/6/30 確認〕
※ 206 Ad hoc WG の設立は、EU サイバーセキュリティ法の Article 49 に規定されている。
※ 207 ECSO：About the cPPP https://ecs-org.eu/cppp〔2020/6/30 確認〕
※ 208 https://ecs-org.eu/〔2020/6/30 確認〕
※ 209 Dr. Martin Schaffer：European Cyber Security Certification: ECSO Meta-scheme Approach https://www.enisa.europa.eu/events/towards_security_framework/Presentation%20-%20Schaffer〔2020/6/30 確認〕
※ 210 https://eucyberact.org/〔2020/6/8 確認〕
※ 211 ECCG の設立は、EU サイバーセキュリティ法の Article 62 に規定されている。
※ 212 Common Criteria：https://www.commoncriteriaportal.org/〔2020/6/30 確認〕
SOG-IS（Senior Officials Group Information Systems Security）：https://www.sogis.eu/〔2020/7/22 確認〕
※ 213 GlobalPlatform：Security Certification https://globalplatform.org/certifications/security-certification/〔2020/6/30 確認〕
※ 214 TrustCB B.V.：IoT Evaluation and Certification https://www.trustcb.com/blog/iot-evaluation-and-certification/〔2020/6/30 確認〕
※ 215 European Commission:COMMISSION RECOMMENDATION (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0534&from=GA〔2020/6/30 確認〕
勧告の詳細については「情報セキュリティ 2019」の「2.2.3（4）(b) 5G ネットワークに関するリスクアセスメント指針」(p.89)を参照。
※ 216 European Commission：NIS Cooperation Group https://ec.europa.eu/digital-single-market/en/nis-cooperation-group〔2020/6/30 確認〕
※ 217 European Commission：Member States publish a report on EU coordinated risk assessment of 5G networks security https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049〔2020/6/30 確認〕
※ 218 EU サイバーセキュリティ庁：ENISA threat landscape for 5G networks https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks〔2020/6/30 確認〕
※ 219 European Commission：Secure 5G networks: Commission endorses EU toolbox and sets out next steps https://ec.europa.eu/commission/presscorner/detail/en/IP_20_123〔2020/6/30 確認〕
※ 220 The Japan Times：Huawei wins contract to develop German 5G network, subject to approval from Berlin https://www.japantimes.co.jp/news/2019/12/12/business/huawei-wins-contract-develop-german-5g-network-subject-berlins-nod/#.XtO-JTr7RPZ〔2020/6/30 確認〕
※ 221 独立行政法人日本貿易振興機構：英国政府、5G 通信網へのファーウェイの一部参入を容認 https://www.jetro.go.jp/biznews/2020/01/af47ec419f1668da.html〔2020/6/30 確認〕
※ 222 The Guardian：Boris Johnson forced to reduce Huawei's role in UK's 5G networks https://www.theguardian.com/technology/2020/may/22/boris-johnson-forced-to-reduce-huaweis-role-in-uks-5g-networks〔2020/6/30 確認〕
※ 223 South China Morning Post：Germany's Telefonica Deutschland picks Ericsson for 5G core network over Huawei https://www.scmp.com/tech/policy/article/3087184/germanys-telefonica-deutschland-picks-ericsson-5g-core-network-over〔2020/6/30 確認〕
※ 224 BBC：Hong Kong：US and allies defend 'bastion of freedom' https://www.bbc.com/news/world-asia-china-52837229〔2020/6/30 確認〕
※ 225 TWNCERT:https://www.twncert.org.tw/〔2020/6/30 確認〕
※ 226 全國法規資料庫：Cyber Security Management Act https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030297〔2020/6/30 確認〕
※ 227 National Security Office：National Cybersecurity Strategy https://www.krcert.or.kr/filedownload.do?attach_file_seq=2162&attach_file_id=EpF2162.pdf〔2020/6/30 確認〕
※ 228 KrCERT/CC：https://www.krcert.or.kr/krcert/intro.do〔2020/6/30 確認〕
※ 229 Department of the Prime Minister and Cabinet：New Zealand's Cyber Security Strategy 2019 https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2019〔2020/6/30 確認〕
※ 230 https://www.cert.govt.nz/〔2020/6/30 確認〕
※ 231 CERT NZ：Advisories https://www.cert.govt.nz/it-specialists/advisories/〔2020/6/30 確認〕
※ 232 CERT NZ：Alerts https://www.cert.govt.nz/individuals/alerts/〔2020/6/30 確認〕
※ 233 APNIC：https://www.apnic.net/〔2020/6/30 確認〕
※ 234 APNIC：Hands-on training seeks to secure Nauru' s future networks https://blog.apnic.net/2019/09/30/hands-on-training-seeks-to-secure-naurus-future-networks/〔2020/6/30 確認〕
APNIC：Register now for Information Security intermediate workshop in Vanuatu https://blog.apnic.net/2019/05/17/register-now-for-information-security-intermediate-workshop-in-vanuatu/〔2020/6/30 確認〕
※ 235 APNIC：Cybersecurity training series builds skills and regional cooperation https://blog.apnic.net/2019/06/13/cybersecurity-training-series-builds-skills-and-regional-cooperation/〔2020/6/30 確認〕
※ 236 APCERT：https://www.apcert.org/〔2020/6/30 確認〕
※ 237 APCERT：TSUBAME Working Group https://www.apcert.org/about/structure/tsubame-wg/index.html〔2020/6/30 確認〕
※ 238 APCERT：APCERT CYBER DRILL 2019“CATASTROPHIC SILENT DRAINING IN ENTERPRISE NETWORK” https://www.

apcert.org/documents/pdf/APCERT_Drill2019_Press%20Release.pdf〔2020/6/30 確認〕
※ 239 APCERT：Documents　https://www.apcert.org/documents/index.html〔2020/6/30 確認〕
※ 240 SingCERT：https://www.csa.gov.sg/singcert〔2020/6/30 確認〕
※ 241 SingCERT：APCERT Conference 2019　https://www.apcert2019.sg/〔2020/2/12 確認〕
※ 242 Sri Lanka CERT|CC：https://www.cert.gov.lk/〔2020/6/30 確認〕
※ 243 Australian Cyber Security Centre：https://www.cyber.gov.au/〔2020/6/30 確認〕
※ 244 CyberSecurity Malaysia：https://www.cybersecurity.my/en/index.html〔2020/6/30 確認〕
※ 245 Singapore Cyber Security Agency：Singapore International Cyber Week 2019 - Highlights and Testimonials https://www.csa.gov.sg/news/press-releases/sicw-2019---highlights-and-testimonials〔2020/6/30 確認〕
※ 246 The Straits Times：New Asean cyber-security centre launched to train response teams to combat online threats https://www.straitstimes.com/tech/new-asean-cyber-security-centre-launched-to-train-response-teams-to-combat-online-threats〔2020/6/30 確認〕
※ 247 総務省：日 ASEAN サイバーセキュリティ能力構築センターの設立　https://www.soumu.go.jp/menu_news/s-news/01tsushin09_02000074.html〔2020/6/30 確認〕
※ 248 OpenGov Asia：ETDA holds training to boost cybersecurity knowledge　https://www.opengovasia.com/etda-holds-training-to-boost-cybersecurity-knowledge/〔2020/6/30 確認〕
※ 249 Australian Cyber Security Centre: Strengthening cyber security across the Pacific　https://www.cyber.gov.au/news/pacific-islands〔2020/6/30 確認〕
※ 250 経済産業省：IT 人材の最新動向と将来推計に関する調査結果 ～ 報告書概要版 ～　https://warp.da.ndl.go.jp/info:ndljp/pid/10159415/www.meti.go.jp/press/2016/06/20160610002/20160610002-7.pdf〔2020/6/30 確認〕
※ 251 NRI セキュアテクノロジーズ社：NRI Secure Insight 2019 ～企業における情報セキュリティ実態調査～　https://www.secure-sketch.com/ebook-download/insight2019-report〔2020/6/30 確認〕
※ 252 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〔2020/6/30 確認〕
※ 253 経済産業省：理工系人材需給状況に関する調査結果概要 https://www.meti.go.jp/press/2018/04/20180420005/20180420005-1.pdf〔2020/6/30 確認〕
※ 254 経済産業省：理工系人材需給状況に関する調査結果を取りまとめました　https://www.meti.go.jp/press/2018/04/20180420005/20180420005.html〔2020/6/30 確認〕
※ 255 経済産業省：第四次産業革命スキル習得講座認定制度　https://www.meti.go.jp/policy/economy/jinzai/reskillprograms/index.html〔2020/6/30 確認〕
※ 256 経済産業省：第四次産業革命スキル習得講座 一覧　https://www.meti.go.jp/policy/economy/jinzai/reskillprograms/pdf/kouzaichiran.pdf〔2020/6/30 確認〕
※ 257 厚生労働省：教育訓練プログラムの開発　https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou_roudou/jinzaikaihatsu/program_development.html〔2020/6/30 確認〕
※ 258 https://www.keidanren.or.jp/policy/2020/025.html〔2020/6/30 確認〕
※ 259 https://cyber-risk.or.jp/cric-csf/jinzai_reference_2016.html〔2020/6/30 確認〕
※ 260 https://cyber-risk.or.jp/contents/CRICCSF_OT-Security_Skill-Reference_1.0_20190731.pdf〔2020/6/30 確認〕
※ 261 https://www.jnsa.org/isepa/images/outputs/JTAG_guideline-%CE%B2_190118.pdf〔2020/6/30 確認〕
※ 262 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。
NSC:「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（改定）」　https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r2.pdf〔2020/6/30 確認〕
※ 263 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〔2020/6/30 確認〕
※ 264 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#section1〔2020/6/30 確認〕
※ 265 IPA：製造・生産分野の管理監督者層向けプログラム　https://www.ipa.go.jp/icscoe/program/seizo-seisan/index.html〔2020/6/30 確認〕
※ 266 IPA：責任者向けプログラム サイバー危機対応机上演習（CyberCREST）　https://www.ipa.go.jp/icscoe/program/short/all_industries/2019.html
※ 267 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/2019.html〔2020/6/30 確認〕
※ 268 IPA：戦略マネジメント系セミナー　https://www.ipa.go.jp/icscoe/program/middle/strategic_management/2019.html〔2020/6/30 確認〕
※ 269 IPA：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/index.html〔2020/6/30 確認〕
※ 270 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 令和元年度秋期試験全試験区分版　https://www.jitec.ipa.go.jp/1_07toukei/toukei_r01a.pdf〔2020/6/30 確認〕
※ 271 IPA：プレス発表　平成 31 年度春期情報処理技術者試験（情報セキュリティマネジメント試験、基本情報技術者試験）の合格者を発表 https://www.ipa.go.jp/about/press/20190522.html〔2020/6/30 確認〕
IPA：令和元年度秋期情報処理技術者試験（情報セキュリティマネジメント試験、基本情報技術者試験）の合格者を発表　https://www.jitec.ipa.go.jp/1_00topic/topic_20191120.html〔2020/6/30 確認〕
※ 272 IPA：国家資格「情報処理安全確保支援士」2020 年 4 月 1 日付登録人数 1,096 人（総数 20,413 人）　https://www.ipa.go.jp/siensi/data/20200401newriss.html〔2020/6/30 確認〕
※ 273 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〔2020/6/30 確認〕
※ 274 IPA：セキュリティの実態を踏まえた登録セキスペへの期待と役割　https://www.ipa.go.jp/files/000079909.pdf〔2020/6/30 確認〕
※ 275 IPA：活用企業・組織のインタビュー　https://www.ipa.go.jp/siensi/data/interview.html〔2020/6/30 確認〕
IPA：情報処理安全確保支援士（登録セキスペ）制度のご紹介　https://www.ipa.go.jp/files/000063331.pdf〔2020/6/30 確認〕
※ 276 IPA：プレス発表　12 月 6 日公布の法律改正に伴う情報処理安全確保支援士制度の見直し　https://www.ipa.go.jp/about/press/20191212_3.html〔2020/6/30 確認〕
IPA：情報処理安全確保支援士（登録セキスペ）制度の見直しについて https://www.ipa.go.jp/siensi/kaisei.html〔2020/6/30 確認〕
※ 277 IPA：セキュリティ・キャンプ全国大会 2019　ホーム　https://www.ipa.go.jp/jinzai/camp/2019/zenkoku2019_index.html〔2020/6/30 確認〕
※ 278 一般社団法人セキュリティ・キャンプ協議会：地方大会　実施状況　https://www.security-camp.or.jp/minicamp/index.html〔2020/6/30 確認〕
※ 279 一般社団法人セキュリティ・キャンプ協議会：セキュリティ・ジュニアキャンプ in 高知 2019　https://www.security-camp.or.jp/minicamp/kochi2019.html〔2020/6/30 確認〕
※ 280 IPA：セキュリティ・ネクストキャンプ 2019　ホーム　https://www.ipa.go.jp/jinzai/camp/2019/next2019_index.html〔2020/6/30 確認〕
※ 281 一般社団法人セキュリティ・キャンプ協議会：セキュリティ・キャンプアワード 2020　https://www.security-camp.or.jp/event/award2020.html〔2020/6/30 確認〕
※ 282 IPA：「セキュリティ・キャンプフォーラム 2020」開催のご案内 https://www.ipa.go.jp/jinzai/camp/2019/forum2020.html〔2020/6/30 確認〕
一般社団法人セキュリティ・キャンプ協議会：セキュリティ・キャンプ交友会 2020 春　https://www.security-camp.or.jp/event/friend2020spr.html〔2020/6/30 確認〕
※ 283 一般社団法人セキュリティ・キャンプ協議会：GCC Tokyo - Global Cybersecurity Camp　https://www.security-camp.or.jp/event/gcc_tokyo.html〔2020/6/30 確認〕
ScanNetSecurity：サイバーセキュリティの新鋭集結、アジア各国の若者が互いの国を知る ～ GCC Tokyo 2020　https://scan.netsecurity.ne.jp/article/2020/03/24/43854.html〔2020/6/30 確認〕
※ 284 enPiT：2019 年度 成果報告　http://www.enpit.jp/files/enPiT_annualreport_uni_2019.pdf〔2020/6/30 確認〕
※ 285 文部科学省：平成 29 年度「成長分野を支える情報技術人材の育成拠点の形成（enPiT）」enPiT-Pro の選定状況について　http://

www.mext.go.jp/a_menu/koutou/kaikaku/enpit/1395904.htm〔2020/6/30 確認〕
※ 286 http://www.seccap.pro/〔2020/6/30 確認〕
※ 287 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。
※ 288 https://www.seccon.jp/2019/〔2020/6/30 確認〕
※ 289 NETIB-NEWS：CTF 国際大会第 1 位の栄冠を手にしたのは日本チーム! https://www.data-max.co.jp/article/34132/?rank〔2020/6/30 確認〕
※ 290 SECCON2019 運営事務局：SECCON Beginners とは https://www.seccon.jp/2019/beginners/about-seccon-beginners.html〔2020/6/30 確認〕
※ 291 SECCON2019 運営事務局：CTF for GIRLS とは https://www.seccon.jp/2019/girls/ctf-for-girls.html〔2020/6/30 確認〕
※ 292 JNSA：インターンシップ募集 https://www.jnsa.org/internship/2019/index.html〔2020/6/30 確認〕
※ 293 東京工業大学：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（2019 年度）」開講のお知らせ https://www.titech.ac.jp/company/news/2019/045588.html〔2020/6/30 確認〕
東京工業大学：カリキュラム概要 https://www.academy.titech.ac.jp/cumot/cy/schedule.html〔2020/6/30 確認〕
※ 294 IPA：企業の CISO 等やセキュリティ対策推進に関する実態調査 https://www.ipa.go.jp/security/fy2019/reports/2019DL_index.html〔2020/6/30 確認〕
※ 295 トレンドマイクロ社：法人組織におけるセキュリティ実態調査 2019 年版を発表 https://www.trendmicro.com/ja_jp/about/press-release/2019/pr-20191015-01.html〔2020/6/30 確認〕
※ 296 法人組織で講じられている対策の度合い、定期的な実施や見直しの徹底といった観点を基に、回答内容に応じてスコアリングすることでセキュリティ対策包括度を算出したもの。
※ 297 https://www.nri-secure.co.jp/news/2019/0718〔2020/6/30 確認〕
※ 298 https://www.ipa.go.jp/security/fy30/reports/ciso/index.html〔2020/6/30 確認〕
※ 299 IPA：「IT システム・サービスの業務委託契約書見直しに関する実態調査報告」について https://www.ipa.go.jp/security/fy2019/reports/scrm/index.html〔2020/6/30 確認〕
※ 300 一般社団法人日本サイバーセキュリティ・イノベーション委員会：サイバーセキュリティ情報公開のポイント～経営者の取組み姿勢が重要～ https://www.j-cic.com/pdf/report/Disclosure-Report.pdf〔2020/6/30 確認〕
※ 301 IPA：リスク分析シート https://www.ipa.go.jp/files/000055518.xlsx〔2020/6/30 確認〕
※ 302 IPA：中小企業の情報セキュリティ対策ガイドライン 第 3 版 https://www.ipa.go.jp/files/000055520.pdf〔2020/6/30 確認〕
※ 303 神奈川県：リース契約満了により返却したハードディスクの盗難及び再発防止策等について https://www.pref.kanagawa.jp/docs/fz7/cnt/p0273317.html〔2020/6/30 確認〕
※ 304 https://www.sonpo.or.jp/cyber-hoken/data/2019-01/pdf/cyber_report2019.pdf〔2020/6/30 確認〕
※ 305 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）- 成果報告書（全体版）- https://www.ipa.go.jp/files/000082722.pdf
※ 306 大阪商工会議所：サイバーセキュリティお助け隊の本格サービス化について https://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/200221cyber.pdf〔2020/6/30 確認〕
※ 307 https://www.ipa.go.jp/security/keihatsu/sme/management.html〔2020/6/30 確認〕
※ 308 IPA：「中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築に向けた実現可能性調査」報告書について https://www.ipa.go.jp/security/fy2019/reports/sme/smesecinfopf.html〔2020/6/30 確認〕
※ 309 https://www.gsx.co.jp/informationsecurity/mic_2019.html〔2020/6/30 確認〕
※ 310 IPA：SECURITY ACTION セキュリティ対策自己宣言 https://www.ipa.go.jp/security/security-action/index.html〔2020/6/30 確認〕
※ 311 https://www.cloudil.jp/contest〔2020/6/30 確認〕
※ 312 https://www.nisc.go.jp/security-site/files/blue_handbook-all.pdf〔2020/6/30 確認〕
※ 313 JNSA：MY CISO ハンドブック https://www.jnsa.org/result/2019/act_ciso/index.html〔2020/6/30 確認〕
※ 314 ISEN：平成 30 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 https://school-security.jp/pdf/2018.pdf〔2020/6/30 確認〕
ISEN：平成 29 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 https://school-security.jp/pdf/2017.pdf〔2020/6/30 確認〕
ISEN：平成 28 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 https://school-security.jp/pdf/2016.pdf〔2020/6/30 確認〕
※ 315 2017 年度と 2016 年度のセキュリティインシデント数は「平成 30 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－」に記載されているものである。図 2-4-23 は「平成 29 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－」及び「平成 28 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－」を基に作成しているため、本文のセキュリティインシデント数と図の標本数は異なった数になっている。
※ 316 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している。
※ 317 https://www.mext.go.jp/content/20200225-mxt_jogai02-100003157_001.pdf〔2020/6/30 確認〕
※ 318 富山大学：個人情報を含む USB メモリの紛失について https://www.u-toyama.ac.jp/news/2019/0830.html〔2020/6/30 確認〕
※ 319 ISEN: 県立高等学校、生徒 64 人の個人情報を保存した私物の USB メモリを紛失 https://school-security.jp/leak/2019/09/%e7%9c%8c%e7%ab%8b%e9%ab%98%e7%ad%89%e5%ad%a6%e6%a0%a1%e3%80%81%e7%94%9f%e5%be%9264%e4%ba%ba%e3%81%ae%e5%80%8b%e4%ba%ba%e6%83%85%e5%a0%b1%e3%82%92%e4%bf%9d%e5%ad%98%e3%81%97%e3%81%9f%e7%a7%81%e7%89%a9/〔2020/6/30 確認〕
静岡県：生徒の個人情報が保存されたUSBメモリーの紛失 http://www2.pref.shizuoka.jp/all/kisha19.nsf/c3db48f94231df2e4925714700049a4e/225635949fa6c55a49258472002e4f2c?OpenDocument〔2020/6/30 確認〕
※ 320 https://www.soumu.go.jp/main_content/000679388.pdf〔2020/6/30 確認〕
※ 321 https://www.soumu.go.jp/main_content/000610588.pdf〔2020/6/30 確認〕
※ 322 IPA：「2019 年度情報セキュリティに対する意識調査」報告書について https://www.ipa.go.jp/security/economics/ishikichousa2019.html〔2020/6/30 確認〕
※ 323 Microsoft 社：Windows セキュリティによる保護 https://support.microsoft.com/ja-jp/help/4013263/windows-10-stay-protected-with-windows-security〔2020/6/30 確認〕
※ 324 Microsoft 社：Windows Update の利用手順 – Windows 10 の場合 https://msrc-blog.microsoft.com/2018/10/18/wumusteps_win10/〔2020/6/30 確認〕
Apple Inc.：Mac の「セキュリティとプライバシー」の「一般」環境設定を変更する https://support.apple.com/ja-jp/guide/mac-help/mh11784/mac〔2020/6/30 確認〕
Apple Inc.：Mac の「ソフトウェア・アップデート」環境設定を変更する https://support.apple.com/ja-jp/guide/mac-help/mchla7037245/10.15/mac/10.15〔2020/6/30 確認〕
※ 325-1 トレンドマイクロ株式会社：スマホ決済を安全に利用するために確認したい 7 つのポイント https://www.is702.jp/special/3533/partner/200_k/〔2020/6/30 確認〕
※ 325-2 https://www.ipa.go.jp/files/000080784.pdf〔2020/6/30 確認〕
※ 325-3 https://www.ipa.go.jp/files/000080783.pdf〔2020/6/30 確認〕
※ 326 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〔2020/6/30 確認〕
※ 327 経済産業省：今後の基準認証の在り方ールール形成を通じたグローバル市場の獲得に向けてー答申 https://www.meti.go.jp/shingikai/sankoshin/sangyo_gijutsu/kijun_ninsho/pdf/20171011001_1.pdf〔2020/6/30 確認〕
※ 328 https://www.kantei.go.jp/jp/singi/titeki2/2010keikaku.pdf〔2020/6/30 確認〕
※ 329 経済産業省：JIS 法改正 https://www.meti.go.jp/policy/economy/hyojun-kijun/jisho/jis.html〔2020/6/30 確認〕
※ 330 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。
※ 331 ISO：ISO/IEC JTC 1 https://www.iso.org/committee/45020.html〔2020/6/30 確認〕
※ 332 日本工業標準調査会：JISC について http://www.jisc.go.jp/jisc/index.html〔2020/6/30 確認〕
※ 333 ITU：SG17: Security https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx〔2020/6/30 確認〕
※ 334 IETF：The IETF Security Area https://trac.ietf.org/trac/sec/wiki〔2020/6/30 確認〕

※ 335 TCG：Trusted Computing Group へようこそ https://trustedcomputinggroup.org/work-groups/regional-forums/japan〔2020/6/30 確認〕
※ 336-1 https://www.jisc.go.jp/international/iso-prcs.html〔2020/6/30 確認〕
※ 336-2 一般社団法人情報処理学会情報規格調査会：第 1 種専門委員会 https://www.itscj.ipsj.or.jp/hyojunka/h_sn_member/h_sn_katsudo/2019arfiles/SC27_2019R.pdf〔2020/6/30 確認〕
※ 337 ISO/IEC 27701 は SC 27/WG 5 で検討、発行された規格である。
※ 338 引用規格：ある規格から引用されることによって引用元の規格の一部を構成する規格。本項では ISO 19011、ISO 20000 が引用規格である。
※ 339 国立研究開発法人新エネルギー・産業技術総合開発機構による委託事業「高効率・高速処理を可能とする AI チップ・次世代コンピューティングの技術開発事業／高度な IoT 社会を実現する横断的技術開発／複製不可能デバイスを活用した IoT ハードウェアセキュリティ基盤の研究開発」を指す。
※ 340 https://qforum.org/〔2020/7/20 確認〕
産官学連携し、量子技術の標準化の支援等を目的に設立された一般社団法人。
※ 341 「情報セキュリティ白書 2019」の「2.5.2（3）（a）ISO/IEC 15408、ISO/IEC 18045 の改訂」(p.127)を参照。
※ 342 総務省が 2019 年度に実施した内閣府事業 PRISM（官民研究開発投資拡大プログラム）の対象研究開発課題「設計・製造におけるチップの脆弱性検知手法の研究開発」を指す。
※ 343 IoT 推進コンソーシアム：IoT セキュリティガイドライン Ver1.0 https://www.soumu.go.jp/main_content/000428393.pdf〔2020/6/30 確認〕
※ 344 JISC：マネジメントシステム規格とは https://www.jisc.go.jp/mss/〔2020/6/30 確認〕
※ 345 https://trustedcomputinggroup.org/〔2020/6/30 確認〕
※ 346 TCG：TPM 2.0 Library Specification https://trustedcomputinggroup.org/tpm-library-specification/〔2020/6/30 確認〕
※ 347 TCG：Trusted Computing Group へようこそ https://trustedcomputinggroup.org/work-groups/regional-forums/japan/〔2020/6/30 確認〕
※ 348 TCG：第 11 回 TCG 日本支部公開ワークショップ https://trustedcomputinggroup.org/work-groups/regional-forums/japan/jrfworkshop/〔2020/6/30 確認〕
※ 349 TCG：Resources Archive https://trustedcomputinggroup.org/resources/?〔2020/6/30 確認〕
※ 350 TCG：Embedded Systems https://trustedcomputinggroup.org/work-groups/embedded-systems/〔2020/6/30 確認〕
※ 351 TCG：TCG TPM 2.0 Automotive Thin Profile For TPM Family 2.0; Level 0 https://trustedcomputinggroup.org/resource/tcg-tpm-2-0-library-profile-for-automotive-thin/〔2020/6/30 確認〕
※ 352 TCG:Protection Profile Automotive-Thin Specific TPM for TCG TPM 2.0 Automotive Thin Profile Family “2.0” Level 0 https://trustedcomputinggroup.org/resource/protection-profile-automotive-thin-specific-tpm-for-tcg-tpm-2-0-automotive-thin-profile-family-2-0-level-0/〔2020/6/30 確認〕
※ 353 https://trustedcomputinggroup.org/resource/tcg-guidance-for-secure-update-of-software-and-firmware-on-embedded-systems/〔2020/6/30 確認〕
※ 354 TCG：Symmetric Identity Based Device Attestation https://trustedcomputinggroup.org/resource/symmetric-identity-based-device-attestation/〔2020/6/30 確認〕
※ 355 https://trustedcomputinggroup.org/wp-content/uploads/TCG-Cyber-Resilient-Technologies-%E2%80%93-Rob-Spiger-Microsoft.pdf〔2020/6/30 確認〕
※ 356-1 https://fidoalliance.org/〔2020/6/30 確認〕
※ 356-2 https://www.commoncriteriaportal.org/〔2020/7/20 確認〕
※ 357 JISEC：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〔2020/6/30 確認〕
※ 358 https://www.ipa.go.jp/security/jisec/certified_pps/c0553/c0553_it7627.html〔2020/6/30 確認〕
※ 359 https://www.ipa.go.jp/security/jisec/certified_pps/c0500/c0500_it5575.html〔2020/6/30 確認〕
※ 360 https://www.ipa.go.jp/security/jisec/certified_pps/c0499/c0499_it5574.html〔2020/6/30 確認〕
※ 361 https://www.ipa.go.jp/security/jisec/certified_pps/c0431/c0431_it4485.html〔2020/6/30 確認〕
※ 362 JISEC：ID&Trust IDentity-J with SAC (PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G v1.0.7052 https://www.ipa.go.jp/security/jisec/hardware/hw_certified_products/c0648/c0648_it8678.html〔2020/6/30 確認〕
JISEC：ID&Trust IDentity-J with SAC (BAC+PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G v1.0.7052 https://www.ipa.go.jp/security/jisec/hardware/hw_certified_products/c0649/c0649_it8679.html〔2020/6/30 確認〕
※ 363 独立行政法人国立印刷局の入札情報公開システム（https://www.npb.go.jp/ja/guide/finance/nyusatu/rakusatu.html〔2020/6/30 確認〕）で 2019 年度の「旅券用ICシート（SAC 対応）B」の入札・見積結果情報を確認した。
※ 364 JISEC：ネットワークカメラシステム チェックリスト https://www.ipa.go.jp/security/jisec/choutatsu/nwcs/index.html〔2020/6/30 確認〕
※ 365 JISEC：入退管理システムチェックリスト https://www.ipa.go.jp/security/jisec/choutatsu/ecs/index.html〔2020/6/30 確認〕
※ 366 https://www.meti.go.jp/press/2019/06/20190617005/20190617005_01.pdf〔2020/6/30 確認〕
※ 367 IPA：「特定用途機器 PP を用いた認証の実効性調査」に係る企画競争 https://www.ipa.go.jp/about/kobo/kobo20191211.html〔2020/6/30 確認〕
※ 368 IPA：本制度に関連する ISO/IEC 規格 https://www.ipa.go.jp/security/jcmvp/topics.html〔2020/6/30 確認〕
※ 369 NITE：ASNITE 0002 Testing 一般社団法人 IT セキュリティセンター 評価部の認定範囲 https://www.nite.go.jp/data/000000804.pdf〔2020/6/30 確認〕
※ 370 NIST：FIPS 140-3 Security Requirements for Cryptographic Modules https://csrc.nist.gov/publications/detail/fips/140/3/final〔2020/6/30 確認〕
※ 371 NIST：FIPS 140-3 Development https://csrc.nist.gov/projects/fips-140-3-development〔2020/6/30 確認〕
※ 372 NIST：SP 800-140(Draft) FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759 https://csrc.nist.gov/publications/detail/sp/800-140/archive/2019-10-09〔2020/6/30 確認〕
NIST：SP 800-140A(Draft) CMVP Documentation Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 https://csrc.nist.gov/publications/detail/sp/800-140a/archive/2019-10-09〔2020/6/30 確認〕
NIST：SP 800-140B(Draft) CMVP Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B https://csrc.nist.gov/publications/detail/sp/800-140b/archive/2019-10-09〔2020/6/30 確認〕
NIST：SP 800-140C(Draft) CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759 https://csrc.nist.gov/publications/detail/sp/800-140c/archive/2019-10-09〔2020/6/30 確認〕
NIST：SP 800-140D(Draft) CMVP Approved Sensitive Parameter Generation and Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759:2014(E) https://csrc.nist.gov/publications/detail/sp/800-140d/archive/2019-10-09〔2020/6/30 確認〕
NIST：SP 800-140E(Draft) CMVP Approved Authentication Mechanisms: CMVP Validation Authority Requirements for ISO/IEC 19790:2012 Annex E and ISO/IEC 24579:2017 https://csrc.nist.gov/publications/detail/sp/800-140e/archive/2019-10-09〔2020/6/30 確認〕
NIST：SP 800-140F(Draft) CMVP Approved Non-Invasive Attack Mitigation Test Metrics: CMVP Validation Authority Updates to ISO/IEC 24759:2014(E) https://csrc.nist.gov/publications/detail/sp/800-140f/archive/2019-10-09〔2020/6/30 確認〕
※ 373 NIST：SP 800-140 FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759 https://csrc.nist.gov/publications/detail/sp/800-140/final〔2020/6/30 確認〕
NIST：SP 800-140A CMVP Documentation Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 https://csrc.nist.gov/publications/detail/sp/800-140a/final〔2020/6/30 確認〕
NIST：SP 800-140B CMVP Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B https://csrc.nist.gov/publications/detail/sp/800-140b/final〔2020/6/30 確認〕
NIST：SP 800-140C CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759 https://csrc.nist.gov/publications/detail/sp/800-140c/final〔2020/6/30 確認〕
NIST：SP 800-140D CMVP Approved Sensitive Parameter Generation and Establishment Methods: CMVP Validation

Authority Updates to ISO/IEC 24759 https://csrc.nist.gov/publications/detail/sp/800-140d/final〔2020/6/30 確認〕
NIST：CMVP Approved Authentication Mechanisms: CMVP Validation Authority Requirements for ISO/IEC 19790 Annex E and ISO/IEC 24579 Section 6.17 https://csrc.nist.gov/publications/detail/sp/800-140e/final〔2020/6/30 確認〕
NIST：SP 800-140F CMVP Approved Non-Invasive Attack Mitigation Test Metrics: CMVP Validation Authority Updates to ISO/IEC 24759 https://csrc.nist.gov/publications/detail/sp/800-140f/final〔2020/6/30 確認〕
※ 374 https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline_20190225.pdf〔2020/6/30 確認〕
※ 375 https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline_honninkakunin_20190225.pdf〔2020/6/30 確認〕
※ 376 日本産業規格 JIS X 19790「セキュリティ要求事項―暗号モジュールのセキュリティ要求事項」においては、用語として「タンパー」を用いている。
※ 377 耐タンパ性：モジュールがあらかじめ準備したインタフェース以外のアクセス手段を用いて、許可なくモジュールの内部情報を読み取ろうとする攻撃に対する耐性。
※ 378 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 1.6 版 https://www.ipa.go.jp/security/jisec/application/documents/guidelineforHCD-PP_1.6.pdf〔2020/6/30 確認〕
※ 379 https://www.ipa.go.jp/security/jisec/certified_pps/c0553/c0553_pp.pdf〔2020/6/30 確認〕
※ 380 IPA/JISEC：認証製品リスト https://www.ipa.go.jp/security/jisec/certified_products/cert_listv31.html〔2020/6/30 確認〕
※ 381 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〔2020/6/30 確認〕
※ 382 e-Gov：電子政府の総合窓口 電子署名及び認証業務に関する法律施行規則の改正案等に対する意見募集 https://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=145209452&Mode=0〔2020/6/30 確認〕
e-Gov：電子署名及び認証業務に関する法律施行規則の一部を改正する省令 https://search.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000197437〔2020/6/30 確認〕
e-Gov：電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針 https://search.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000197438〔2020/6/30 確認〕
※ 383 e-Gov：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/search/elawsSearch/elaws_search/lsg0500/detail?lawId=413M60000418002〔2020/6/30 確認〕
※ 384 IETF：Deprecating TLSv1.0 and TLSv1.1 draft-ietf-tls-oldversions-deprecate-06 https://tools.ietf.org/id/draft-ietf-tls-oldversions-deprecate-06.html〔2020/6/30 確認〕
※ 385 Qualys SSL Labs：SSL Pulse https://www.ssllabs.com/ssl-pulse/〔2020/6/30 確認〕
※ 386 Microsoft Security Response Center https://msrc-blog.microsoft.com/2018/10/16/tlsdeprecation/〔2020/6/30 確認〕
※ 387 NIST：NIST Special Publication 800-52 Revision 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf〔2020/6/30 確認〕
※ 388 Federal Office for Information Security：BSI TR-02102-2：“Technical Guideline TR-02102-2Cryptographic Mechanisms: Recommendations and Key Lengths, Part 2 – Use of Transport Layer Security (TLS)” https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-2.pdf〔2020/6/30 確認〕
※ 389 Agence nationale de la sécurité des systèmes d’information：Security Recommendations for TLS https://www.ssi.gouv.fr/uploads/2017/02/security-recommendations-for-tls_v1.1.pdf〔2020/6/30 確認〕
※ 390 NIST：NIST Special Publication 800-56C Revision 1 Recommendation for Key-Derivation Methods in Key-Establishment Schemes https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr1.pdf〔2020/6/30 確認〕
Draft NIST Special Publication SP 800-56C Revision 2 Recommendation for Key-Derivation Methods in Key-Establishment Schemes https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2-draft.pdf〔2020/6/30 確認〕
※ 391 NIST：NIST Special Publication 800-108 Recommendation for Key Derivation Using Pseudorandom Functions https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf〔2020/6/30 確認〕
※ 392 https://www.jnsa.org/result/surv_mrk/2020/〔2020/6/30 確認〕
※ 393 「2019 年度 国内情報セキュリティ市場調査報告書」では、変更後の市場区分定義に沿って 2017 ～ 2020 年度の市場規模を新たに集計している。また、JNSA の「2019 年度 国内情報セキュリティ市場調査報告書」の Web ページ（https://www.jnsa.org/result/surv_mrk/2020/〔2020/6/30 確認〕）では、従来の市場区分の集計結果も公表している。
※ 394 公益社団法人日本経済研究センター：短期経済予測（第 181 回再改訂 /2020 年 1-3 月期～ 2022 年 1-3 月期）年内に自粛解除でも、20 年度マイナス 8%成長―新興国の感染拡大に懸念― https://www.jcer.or.jp/economic-forecast/20200424.html〔2020/7/10 確認〕
※ 395 経済産業省：Connected Industries https://www.meti.go.jp/policy/mono_info_service/connected_industries/index.html〔2020/7/1 確認〕
※ 396 IPA：「安全なデータ利活用に向けた準備状況及び課題認識に関する調査」報告書について https://www.ipa.go.jp/security/fy30/reports/ts_research/index.html〔2020/7/1 確認〕
※ 397 https://www.ipa.go.jp/files/000072809.pdf〔2020/7/1 確認〕
※ 398 IPA：「企業におけるデータ利活用・保護の戦略立案のための手引書（案）の作成」調査報告書 https://www.ipa.go.jp/security/fy2019/reports/ts_research/20200327.html〔2020/7/1 確認〕
※ 399 PoC（Proof of Concept：概念実証）：新しい概念や理論、原理、アイディアの実証を目的とした検証やデモンストレーション。
※ 400 研究の例としては、以下がある。
Batini, Carlo, and Monica Scannapieco. “Data Quality: Concepts, Methodologies and Techniques” Springer (2006)
Rajesh Jugulum, “Competing with High Quality Data: Concepts, Tools, and Techniques for Building a Successful Approach to Data Quality” Wiley (2014)
Aiken, Peter and Billings, “Monetizing Data Management” Technics Publishing, LLC (2014)
Aiken, Peter and Harbour, “Data Strategy and the Enterprise Data Executive” Technics Publishing, LLC (2017)
※ 401 G. Leurent, T. Peyrin, From Collision to Chosen-Prefix Collisions Application to Full SHA-1, EUROCRYPT 2019, LNCS 11478, pp. 527-555
※ 402 Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger：MD5 considered harmful today https://www.win.tue.nl/hashclash/rogue-ca/〔2020/6/30 確認〕
※ 403 NIST：The 2nd Round of the NIST PQC Standardization Process-Opening Remarks at PQC 2019: https://csrc.nist.gov/CSRC/media/Presentations/the-2nd-round-of-the-nist-pqc-standardization-proc/images-media/moody-opening-remarks.pdf〔2020/6/30 確認〕
※ 404 NIST：Lightweight Cryptography https://csrc.nist.gov/projects/lightweight-cryptography〔2020/6/30 確認〕
※ 405 A. C. Aldaya, C. P. García, L. M. A. Tapia, B. B. Brumley：Cache-Timing Attacks on RSA Key Generation https://tches.iacr.org/index.php/TCHES/article/view/8350〔2020/6/30 確認〕
※ 406 K. Ryan：Return of the Hidden Number Problem https://tches.iacr.org/index.php/TCHES/article/view/7337〔2020/6/30 確認〕
※ 407 J. Rodriguez, A. Baldomero, V. Montilla, J. Mujal：LLFI: Lateral Laser Fault Injection Attack https://fdtc.deib.polimi.it/FDTC19/shared/FDTC%202019%20-%20session%203.1.pdf〔2020/6/30 確認〕
※ 408 個人情報保護委員会：個人情報保護法 いわゆる3年ごと見直し制度改正大綱 https://www.ppc.go.jp/files/pdf/200110_seidokaiseitaiko.pdf〔2020/6/30 確認〕
※ 409 個人情報保護委員会：個人情報保護法 いわゆる3年ごと見直し制度改正大綱（骨子） https://www.ppc.go.jp/files/pdf/191129_houdou_koshi.pdf〔2020/6/30 確認〕
※ 410 個人情報保護委員会：「個人情報の保護に関する法律等の一部を改正する法律案」の閣議決定について https://www.ppc.go.jp/news/press/2019/20200310/〔2020/6/30 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 のセキュリティ、次代を担う青少年を取り巻くネット環境、クラウドのセキュリティについて取り上げた。また、セキュリティマネジメントの日米企業比較に関する特別寄稿を掲載した。

制御システム、IoT については、国内外で報告されているインシデントや攻撃の実態、脆弱性や脅威の動向、そして国の施策や企業の対策の状況を解説する。

また、近年の新たな課題となっている青少年のネット利用、企業・組織のクラウド利用におけるセキュリティについて取り上げた。

3.1 制御システムの情報セキュリティ

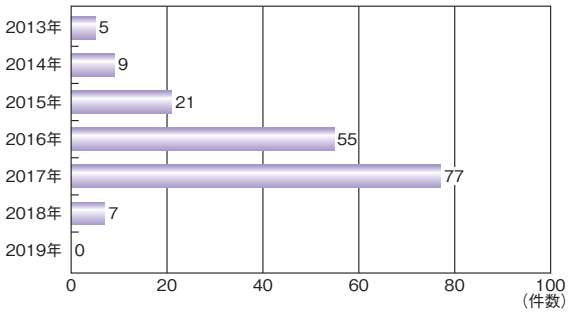
制御システム（ICS：Industrial Control System）は、電力、ガス、水道、輸送・物流、製造ライン等、我々の生活を支える重要インフラサービス※1 を動かしているシステムである。従来、制御システムは独立したネットワーク、固有のプロトコル、事業者ごとに異なる仕様で構築・運用されることが多く、外部からサイバー攻撃を行うことは困難と考えられていた。しかし、近年ネットワーク化やオープン化（標準プロトコル・汎用製品の利用）が進んだこと、また、10 ～ 20 年に及ぶライフサイクルの長さ故に、外部との接続やサイバー攻撃を想定していないシステムが今なお多数稼働していることから、制御システムに対するサイバー脅威が高まっている。世界的に有名なハッキングコンテスト※2 でも制御システムを攻撃対象としたものが多く開催されている。

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

2019 年も制御システムそのものを標的としたサイバー攻撃による重大インシデントはなかったが、米国エネルギー省（DOE：Department of Energy）のレポートによると、2019 年 3 月 5 日、米国の Sustainable Power Group, LLC で、ファイアウォールの既知の脆弱性を悪用する DoS 攻撃によって、太陽光及び風力発電施設との通信が一時的に中断した※3。このインシデントは、米国電力システムへの公になった初のサイバー攻撃として話題となった※4。

国内においては、JPCERT コーディネーションセンター（JPCERT/CC：Japan Computer Emergency Response Team Coordination Center）に 2019 年に報告された制御システムのインシデント件数は 0 件であった。2017 年の 77 件、2018 年の 7 件から減少しており、「制御システム」のカテゴリが追加された 2013 年以降初の 0 件となった（図 3-1-1）。



■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 ～ 2019 年）
（出典）JPCERT/CC のインシデント報告対応レポート※5 を基に IPA が作成

一方、調査会社による海外における制御システムユーザ等へのアンケート調査では、前年同様、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は一定数以上あった。

例えば、制御システム／運用・制御技術（OT：Operational Technology）を利用する重要インフラ事業者 701 社を対象とした調査では、約 62% が過去 2 年間に 2 回以上サイバー攻撃による情報漏えい、障害、ダウンタイムが発生したと回答している※6。また、電力・ガス・水道等の公共サービス提供会社の OT サイバーリスク対応担当者 1,726 名を対象とした調査では、56%

が少なくとも1年に1回システム停止または運用データの損失を経験したと回答している※7。

従って、公にはなっていないが、制御システムの運用や機器に実害をもたらしたインシデントは、2019年も一定程度発生したと推察される。一方で、公になったインシデントには、持ち込み機器・媒体によるウイルス※8感染、ITシステムのウイルス感染による生産や重要サービスの停止、という二つの特徴が見られた。

(1)引き続き多い、持ち込み機器・媒体によるウイルス感染

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感染は2019年も継続して発生している。

2019年9月、インドのクダンクラム原子力発電所で、内部関係者がウイルス「Dtrack」に感染したパソコンを発電所の管理ネットワークに接続した※9。インド原子力発電公社によると、この管理ネットワークは制御ネットワークと分離されているため、原子炉の制御に影響はなかったとしているが、制御システムに影響があれば大事故となっていた可能性もある。

SANS Instituteの調査「SANS 2019 State of OT/ICS Cybersecurity Survey」によると、制御システム／OTのセキュリティインシデントにおける侵入口のトップは「物理アクセス」（USBメモリや機器への物理アクセス）で56.3%だった※10。また、金融、ヘルスケア、製造、電力等の業界の従業員約300人を対象に行った調査では、従業員はUSBメモリの使用に関するセキュリティリスクを認識しているものの、ルールに従わずに使用しているケースも多いことが判明した。具体的には、64%がUSBの使用ポリシーが規定されていると回答しているが、同じく64%が必要な許可を事前に得ることなくUSBを使用していると回答している※11。

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、内部関係者の不正による脅威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。

(2)ITシステムのウイルス感染により生産や重要サービスが停止する事例の増加

IT/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きている。

例えば2019年3月、ノルウェーのアルミ生産大手Norsk Hydro ASAの米国内事業所でランサムウェアの感染が発生した。攻撃者は、数ヵ月前にフィッシングメールによってITシステムの業務端末にバックドアを生成し、その後、ランサムウェア「LockerGoga」を配布した。同社は40ヵ国の事業所に次々と感染が拡大したため、社内ネットワークを遮断し、全コンピュータを停止した※12。その結果、工場間のネットワークも遮断されたため、手動操業できない一部の工場で生産が停止した。金銭的損失は通年で約77億～89億円（約6億5千万～7億5千万ノルウェークローネ）と推定されている※13。

同年2月には、光学機器・ガラスメーカであるHOYA株式会社のタイ工場で、約100台のコンピュータがウイルスに感染し、一部の生産ラインが3日間停止した※14。工場の生産性が約60%落ちたほか、日本の本社でも請求書が発行できない等の影響が出た。

同年7月には、南アフリカのヨハネスブルグ市で、配電公社City Powerのコンピュータシステムがランサムウェア「GandCrab」に感染した※15。その結果、プリペイド式電力供給契約の顧客で、チャージ額を使い果たした顧客がチャージできず、寒波に見舞われている冬の最中に電気が止められてしまう事態が発生した。

ロシアのセキュリティベンダのレポートによると、攻撃者が企業のITインフラの脆弱性を利用して侵入した事例の82%において、制御システムまで到達できた可能性があると指摘している※16。従って、制御システムはITシステムの影響は受けない、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の縦割りの管理体制を超えた横断的なリスクの見直しが推奨される。

3.1.2 脆弱性／脅威の動向

本項では、2019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。

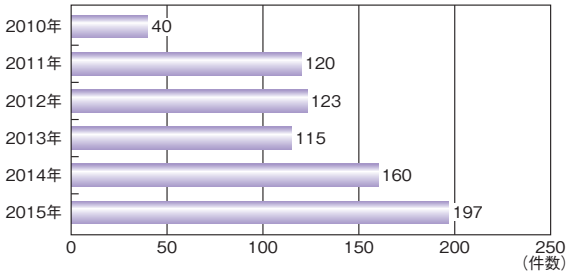
(1)脆弱性の動向

2019年も、制御システムの脆弱性が多く公開された。

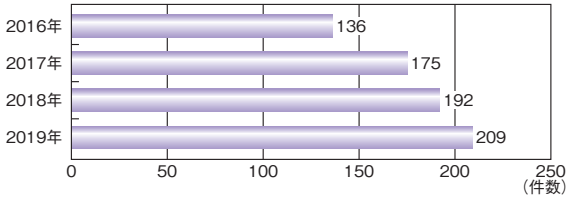
制御システムの脆弱性情報を収集・公開している代表的な組織である米国国土安全保障省（DHS：Department of Homeland Security）のNCCIC

（National Cybersecurity and Communications Integration Center）が 2019 年に公開したアドバイザリは 209 件で※17、図 3-1-2 及び図 3-1-3 に示す公開件数から分かるように、増加傾向にある（2016 年から NCCIC における脆弱性情報の公開件数のカウント方法が見直されたため、同じカウント方法で比較できるように図を分けている）。2019 年に公開された脆弱性で特に目立った傾向は、脆弱性確認ツールで検出可能なものや、設計時からセキュリティを確保するセキュリティ・バイ・デザインによって回避できるものが多く見られたことである。制御システムベンダには、脆弱性を作り込まないセキュリティ・バイ・デザインの徹底が求められる。

また、非常に影響の大きい脆弱性も発見された。米国の IoT セキュリティベンダである Armis Inc. の研究者らが、Wind River Systems, Inc. のリアルタイム OS「VxWorks」の TCP/IP スタック「IPnet」に 11 個の脆弱性を発見した※18。VxWorks は、SCADA（Supervisory Control And Data Acquisition）システム、エレベーター、産業用制御装置、患者モニタや MRI 機器、更にファイアウォール、ルータ、衛星モデム等、20 億以上もの機器に実装されている。「Urgent11」と総称されるこれらの脆弱性には、リモートコード実行を可能にする脆弱性六つと、DoS、情報漏えいまたはエラーを引き起こす可能性がある脆弱性五つが含まれていた※19。Armis Inc. は 2019 年 6 月にパッチを作成して影響を受ける機器の製造元に提供し、Wind River Systems, Inc. は同年 7 月にパッチ及び脆弱性の修正を含めた新バージョンをリリースした。



■図 3-1-2　NCCIC が公開した脆弱性アドバイザリの件数（2010 ～ 2015 年）
（出典）NCCIC の公開情報※21 を基に IPA が作成



■図 3-1-3　NCCIC が公開した脆弱性アドバイザリの件数（2016 ～ 2019 年）
（出典）NCCIC の公開情報※22 を基に IPA が作成

2020 年 1 月に米国マイアミで開催されたハッキングコンテスト「Pwn2Own」では、制御システムの脆弱性を使用したリモートコード実行（RCE：Remote Code Execution）が成功したという※20。制御システムの運用者はこのような脆弱性に関する情報を収集し、新たな脅威に備える必要がある。修正プログラムの適用が難しい場合には、脆弱性の緩和策を実施する等の脆弱性対策が重要である。

(2) 脅威の動向

2019 年の脅威の動向としては、主に以下の三つが挙げられる。

(a) 一般的な脅威の動向

ドイツ連邦政府の情報セキュリティ庁（BSI：Bundesamt für Sicherheit in der Informationstechnik）が「Industrial Control System Security - Top 10 Threats and Countermeasures 2019※23」（「産業用制御システム（ICS）のセキュリティ -10 大脅威と対策 2019-※24」）を公開した。本報告によると、前回の 2016 年版に比べて、制御システムにおけるアウトソーシングやクラウドの利用増加に伴い、クラウドコンポーネントや外部ネットワークへの攻撃の脅威が高まっている。一方、ソーシャルエンジニアリングやフィッシングの脅威は、相対的に低下している。最も多かった脅威は、リムーバブルメディアや外部機器経由のウイルス感染で、次いでインターネットやイントラネット経由のウイルス感染、ヒューマンエラーと妨害行為、となっている。

(b) ランサムウェアの標的型化

従来のランサムウェア攻撃では、攻撃者は無差別にランサムウェアをばらまき、感染してデータを暗号化された被害者に「復号のため」と称して身代金を要求していた。しかし、これは攻撃者にとって効率が悪いため、特定の企業・組織を狙って、できるだけ多くのコンピュータに感染させて身代金を要求する「標的型」のランサムウェア攻撃が海外で増えている。

Europol（欧州刑事警察機構）が公表した、サイバー犯罪の脅威の状況に関する年次報告書「INTERNET ORGANISED CRIME THREAT ASSESSMENT（IOCTA）2019※25」によると、ランサムウェア攻撃の数

は減少しているものの、企業を標的とした攻撃キャンペーンへシフトしており、本報告書でトップの脅威となっている※26。

例えば2019年3月、米国の大手飲料水メーカArizona Beveragesが大規模なランサムウェア感染被害に遭い、外部のインシデント対応サービスに対応を依頼するまでの数日間、販売活動が停止した。使われたランサムウェアは「iEncrypt」で、身代金要求メッセージの中で同社を名指ししており、ばらまき型ではなく同社を標的とした攻撃と見られる。200台以上のサーバやコンピュータが感染し、多くはサポートが終了したWindows OS機器であった。また、バックアップも設定不備のため使用できない状態だったとされる※27。

また、米国の製造会社を狙った標的型と見られるランサムウェア攻撃も確認されている。セキュリティベンダの調査によると、前述の飲料水メーカ同様、身代金要求のメッセージで攻撃された企業が名指ししてあった。被害自体は、振る舞い検知を始めとするウイルス対策ソリューションにより最小限に抑えられたという※28。

更にここ最近、攻撃者は、より確実に金銭的な利益を得るために、ランサムウェアで標的となった企業のデータを暗号化するだけでなく、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という戦術をとっている。

例えば2019年12月、米国の大手電線・ケーブル製造メーカSouthwire Company, LLCの878台の機器がランサムウェア「Maze」に感染し、全社のネットワークが停止した※29。その結果、製造及び出荷に影響が発生した。攻撃者は同社のファイル120GBを窃取し、身代金としてビットコイン850BTC（約6億6千万円）を要求した。また、身代金が支払われるまで、このファイルを毎週少しずつWeb上で公開すると脅迫し、実際に公開を始めた。同社は身代金を支払わないという決断の後、ジョージア州の裁判所に、ネットワークへの不正アクセス、データ窃取、コンピュータの暗号化及び窃取データの公開について、身元不明の攻撃者に対する訴訟を起こした。また、窃取データが投稿されたサイトをホストしている企業に対する差し止め命令も求めている※30。

また、2020年1月には、ドイツの自動車部品製造メーカGedia Automotive Groupがランサムウェア「Sodinokibi」によるサイバー攻撃を受けてITシステムを停止し、本社の300名以上の従業員が自宅待機となった※31。攻撃の影響は広範囲に及び、スペイン、ポーランド、ハンガリー及び米国工場の操業にも影響を及ぼした。攻撃者グループは、設計図や従業員・顧客情報を含む50GBの機密情報を窃取し、身代金を支払わないとこれらの情報を公開する、と脅していた。

ランサムウェア対策として、基本的なウイルス対策と、通信制御による対策、及び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。

(c) 破壊型攻撃の増加

International Business Machines Corporation（以下、IBM社）のX-Force Incident Response and Intelligence Services（IRIS）の報告書※32によると、2019年前半は破壊型ウイルス（攻撃対象システムの全体あるいは一部（データ等）の破壊を目的としたサイバー攻撃において用いられるウイルス）の使用が2018年後半に比べて2倍になり、影響を受けた組織の50%が製造業であった。過去においては、破壊型ウイルスは主に国家が使用してきたが、特に2018年後半以降、サイバー犯罪者が「LockerGoga」や「MegaCortex」といった新しい種類のランサムウェアを使用する等、データを消去・破壊する機能を持ったワイパー型のウイルスを攻撃に取り入れている。同社がインシデント対応した破壊的なサイバー攻撃に遭った企業は、平均して12,000台を超えるコンピュータが何らかの形で損傷し、事態の収拾には512時間以上かかった※33。

また、制御システムに特化したセキュリティベンダのレポートによると、2016年12月に発生したウクライナの送電網へのウイルス「Industroyer」（「Crash Override」とも呼ばれる）を使用したサイバー攻撃では、ウイルスが停電を起こしたのは罠であり、復電の際に、機器損壊や感電等の生命に関わる可能性のある物理的被害、及び大規模停電を引き起こすことがハッカーの本来の目的であったことが分かった※34。同社が電力会社のネットワークログを政府機関から入手し、攻撃のタイムラインを再構築したところ、攻撃者は、まずサーキットブレーカーを開いて停電を引き起こし、1時間後に監視システムを無効化した。その後、保護リレーをハッキングして機器のフェールセーフ機能を無効化するはずだったが、攻撃者側の何らかのミスにより失敗していた。成功していれば、手動による機器の再起動時に変圧器または電力線の電流の過負荷が発生し、長期間の停電が起きていた。

金銭目的のサイバー犯罪者が、脅迫の手段として「情報曝露」から「破壊」へと方針を転換する可能性や、国家のサイバー組織が有事の優位性確保のために、破壊を含めた制御システムの乗っ取りを狙う可能性もあり、今

後、破壊型攻撃は更に増加することが推測され、警戒が必要である。

ランサムウェアや破壊型ウイルス対策として、基本的なウイルス対策、脆弱性への至急の対策が難しい場合の通信制御による対策、及び感染に備えた対策を徹底し、感染後にシステムが運用できない事態に備えて定期的にオフラインを含むバックアップを行うことが推奨される。また、手動オペレーションを含めた代替案や復旧訓練の実施も検討する価値がある。

2019 年 12 月中旬には、制御システムを標的とした新たなランサムウェア SNAKE（別名、EKANS）の出現も確認されている※35。破壊型を含むランサムウェアの脅威はますます増大すると思われ、セキュリティ対策の改善・強化やインシデント対応への備えが重要である。

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

米国では、地政学的緊張が高まる中、敵対する勢力から最も攻撃の対象となり得る重要インフラのセキュリティ強化に関する取り組みが目立った。

2019 年 4 月、DHS の Cybersecurity and Infrastructure Security Agency（CISA）が、国家の安全保障、経済、公衆衛生・安全の確保に必要不可欠な 55 の機能（function）の一覧「National Critical Functions」を発表し※36、重要インフラを従来の「業界」でなく、果たす役割である「機能」で特定する方向にシフトしている。これは、業界内及び業界間で影響を与える可能性のあるリスクと依存関係をより包括的に把握し、重要インフラのエコシステム全体を、より戦略的な方法で強化することを目的としている。55 の機能は「Connect」「Distribute」「Manage」「Supply」の四つの区分に分類され、例えば「無線ネットワークサービスの提供」等の機能は Connect、「配電」「送電」や「船舶による輸送」等は Distribute、「下水の管理」「医療の提供」等は Manage、「水道水の提供」「発電」等は Supply と区分している。

5 月には、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）が、米国電力業界でも急速に普及が進んでいる IIoT（Industrial Internet of Things）のサイバーセキュリティ対策を促進するべく、National Cybersecurity Center of Excellence（NCCoE）を通じて電力業界向けの IIoT セキュリティガイドの策定に取り組んでいることを明らかにした※37。同ガイドは五つの分野（「配電設備と分散型エネルギー資源（DER）システム間のデータ交換」「信頼できる機器の識別、機器間の通信プロセス及びセキュリティ技術」「マルウェアの検知・防止」「データの完全性の担保」「データに基づくセキュリティ分析」）にフォーカスする予定である。NIST はまた、2017 年 9 月に公開した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 Manufacturing Profile（NIST IR 8183）」を 2019 年 5 月に更新し、汎用の実装ガイド（Vol.1）、プロセス製造業向け実装ガイド（Vol.2）、組立製造業向け実装ガイド（Vol.3）のドラフト版と併せて公開した※38。

2019 年 12 月に米国で成立した国防権限法「National Defense Authorization Act（NDAA）」には、サイバー攻撃から電力網を保護する法律「Securing Energy Infrastructure Act」が組み込まれた。組み込まれた法律は、DOE の国立研究所で電力網の脆弱性を排除するためのパイロットプログラムを立ち上げ 2 年間実施する、というもので、このプログラムの結果を基にした勧告によって、連邦政府機関とエネルギー産業によって作成された電力網をサイバー攻撃から保護するための国家戦略が策定される※39。

(2) 民間の取り組み

民間では、制御システムのセキュリティ強化や情報共有に関する、グローバルアライアンスやサポート組織の設立が相次ぎ、また、制御システムを狙う攻撃の戦略や手法の理解に役立つナレッジベース／フレームワークの制御システム版が公開された。

2019 年 7 月、International Society of Automation（ISA）が、Global Cybersecurity Alliance（GCA）を設立した※40。GCA は、FA（Factory Automation）や PA（Process Automation）関連企業におけるサイバーセキュリティ意識とサイバー攻撃への備えを向上させるため、ISO/IEC62443 の活用・準拠の促進や、情報・知識の共有、ベストプラクティスツールの開発等を行っていく。2020 年 1 月現在、23 の企業・組織がメンバーとなっている※41。

同年 10 月には、OT のセキュリティ課題に対処する企業を支援するために、電力・ガス・水道等の公共サービス業及び石油・ガス業界のリーダーによるアライアンス Operational Technology Cyber Security Alliance

(OTCSA)が設立された※42。

また11月には、米国の13の地域電力会社を傘下に持つ持株会社 American Electric Power, Inc.(AEP)と情報セキュリティ会社Fortress Information Securityが、サイバーセキュリティ規制遵守にかかるコスト削減のために、電力会社間のコラボレーションを促進する合弁事業 Asset to Vendor Network for Power Utilities(A2V)を開始した※43。連邦エネルギー規制委員会(FERC:Federal Energy Regulatory Commission)が発行した新しい規則では、電力会社はサプライチェーンに関連するサイバーリスクの管理計画を作成し、2020年6月までにFERCに提出することを要求される。そのためには、リスク評価の要件に基づいてサプライチェーンベンダに優先順位を付け、また、ソフトウェアメーカの信頼性とソフトウェアアップデートの完全性を検証する必要がある。A2Vは、この規制遵守要件を満たすよう努力するベンダをサポートするための技術及び情報共有のプラットフォームとして設立された。

2020年1月、米国の非営利団体The MITRE Corporationは、攻撃者が使用する様々な攻撃タイプの戦術、手法、手順を体系化したナレッジベース及びフレームワーク「ATT&CK」(Adversarial Tactics, Techniques, and Common Knowledge)の産業用制御システム版「ATT & CK for ICS」を公開した※44。これにより、発電及び配電施設、石油精製所、下水道処理施設、交通機関等を含む重要インフラの制御システムで使用される特殊なアプリケーションやプロトコルのどれが攻撃者に悪用されるのかについて情報を提供している。

(3)航空宇宙分野における衛星通信のセキュリティ

民間企業による衛星の打ち上げが相次ぎ、日常生活の多くの側面において、衛星の活用による利便性の向上が進んでいる。それに伴い、衛星通信のセキュリティの重要度が増している。衛星通信の脆弱性については、数年前からセキュリティ研究者によって指摘されてきたが、宇宙機器のサイバーセキュリティに関するレポートが公開されたことによって、取り組みが活性化した。

2019年7月、英国王立国際問題研究所(通称、チャタムハウス)が、レポート「Cybersecurity of NATO's Space-based Strategic Assets」を公開した※45。現代の軍事活動のほぼすべてが衛星を利用する中、ハードウェア・ソフトウェア・デジタル技術に依存する宇宙機器に対するサイバー脅威が、国家の活動を阻害するリスクがあるとして、本レポートでは宇宙機器に対する脅威、脆弱性、発生しうる事態を評価している。

米国では、政府や軍で衛星通信のセキュリティに関する取り組みが立て続けに発表された。

国防総省(DoD:Department of Defense)の商業衛星通信サービスの調達を担当している米国空軍の宇宙軍団(AFSPC:Air Force Space Command)は、軍事ネットワークの保護を強化するために、商業衛星通信プロバイダのサイバーセキュリティを監査するプログラム「Infrastructure Asset Pre-Assessment(IA-Pre)」を2020年に開始する※46。商業衛星通信プロバイダは、NIST SP800-53(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)のサイバーセキュリティ基準を満たしているかどうか、サードパーティの監査を受ける必要がある。

また、米国空軍は2020年8月にラスベガスで開催される情報セキュリティに関する世界最大級の国際会議「DEF CON」のハッキングコンテストで、ハッカーに軌道衛星をハッキングさせることを発表した※47。これは、航空宇宙関連の企業にサイバーセキュリティの重要性を周知し、また、サイバーセキュリティのアプローチ方法に欠陥があるかどうかを確認することが狙いである。

DHSは、PNT(Positioning(測位)、Navigation(ナビゲーション)、Timing(タイミング))情報を提供するシステムのレジリエンス能力を高めるためのフレームワーク「Resilient PNT Conformance Framework」を策定する予定である※48。電力網、通信網、金融機関等の国の重要インフラが正常に機能するためには、GPS衛星から受信するPNT情報は必須だが、GPS信号は低出力で暗号化されておらず、意図的な、または意図しない妨害を受けやすい。このフレームワークは、企業がよりレジリエンス能力のあるPNTシステムを構築するのに役立つと期待されており、また、このようなシステムのユーザが戦術、技術、手順を開発し、ベストプラクティスを採用するのにも役立つ。

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

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」で取り上げているので、そちらを参照されたい。ここでは特に、制御システムのセキュリティ強化に関する取り組みについて触れる。

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）が、2018 年度における我が国を取り巻くサイバーセキュリティに関する情勢、及び 2018 年 7 月に発表された「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 2019※49」（2018 年度報告・2019 年度計画）を 2019 年 5 月に発表した。本報告書の中から、代表的な取り組みを紹介する。

2019 年の主な成果として、経済産業省の「産業サイバーセキュリティ研究会 WG1」で、様々なつながりによって新たな付加価値を創出する「Connected Industries」におけるサプライチェーンのサイバーセキュリティ対策指針として「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」が 4 月に策定された※50（CPSF については「2.1.2（1）（a）WG 1（制度・技術・標準化）」参照）。

6 月には、同 WG のビルサブワーキンググループによる「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」が公開された※51。同ガイドラインは、建物の空調、エレベーター、防災設備等を監視・制御するビルディング・オートメーション・システムにおいて考慮すべきセキュリティリスク及び対策をまとめている。

また、経済産業省は、ガス事業法第 97 条によってガス事業者に策定と遵守が義務付けられている保安規定に、「製造・供給に係る制御システムのサイバーセキュリティ対策」に関する規定を盛り込んだガス事業法施行規則の改正を 2019 年 1 月 30 日付けで行い、4 月 1 日に施行した※52。

同年 12 月、経済産業省は「ERAB に関するサイバーセキュリティガイドライン Ver.2.0」を公開した※53。本ガイドラインは、需要家側のエネルギーリソース（小規模電源・蓄電システム・ディマンドリスポンス等）を活用したエネルギー・リソース・アグリゲーション・ビジネス（ERAB：Energy Resource Aggregation Businesses）に参画する事業者が取り組むべきサイバーセキュリティ対策の指針を示している。

（2）IPA の取り組み

2019 年、IPA では制御システムのセキュリティに関して、大きく三つの取り組みを行った。

（a）産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）

2017 年 4 月に発足した ICSCoE 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）。

（b）制御システムのセキュリティリスクアセスメント

IPA では、制御システムに対するリスクアセスメント実施支援活動の経験を踏まえて作成・公開した「制御システムのセキュリティリスク分析ガイド※54」（以下、リスク分析ガイド）に関して、2019 年に制御システム保有事業者及びインテグレータ／ベンダ／メーカを対象としたセミナーを 2 回開催※55 するとともに、リスク分析ガイドを 2020 年 3 月に改訂した。

また、2019 年 7 月及び 2020 年 3 月に「制御システム関連のサイバーインシデント事例」シリーズを公開した※56（表 3-1-1）。制御システム保有事業者にとって、国内外で発生したインシデント事例の情報を基に、自社の制御システムに対して同様の脅威が発生した場合のリスクアセスメントを実施することは、セキュリティ管理の強化につながる。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、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※57」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。

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 メモリとゼロディ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

■表 3-1-1　「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

(c) ES-C2M2 解説資料の公開

「ES-C2M2」とは、DoE が、米国内の電力会社がセキュリティマネジメントを自己評価するために発行したもので、サイバーセキュリティ成熟度モデル（C2M2：Cybersecurity Capability Maturity Model）の一つである。IPA は、国内の重要インフラ業界のセキュリティ対策の支援を目的に、「ES-C2M2」の解説書及びチェックシートを 2019 年 10 月に公開した※58。本モデルを活用することで、企業が現在取り組んでいるセキュリティ対策や手法等の能力レベルの評価と、それによる対策の目標や改善項目の優先順位の設定が可能となる。

COLUMN

インシデント公表後に株価が上昇した企業

2019 年 3 月 19 日、ノルウェーのアルミ生産大手 Norsk Hydro ASA の米国内事業所でランサムウェアの感染が発生し、一部の工場で生産が停止、多大な金銭的損失が発生することになりました[i]。インシデント発生直後、同社の経営陣は緊急会議を開き、身代金を支払わない、インシデント情報を完全にオープンにする、Microsoft Corporation のサイバーセキュリティチームに業務復旧の支援を要請する、という三つの事項を迅速に決定しました。復旧の過程において、Facebook に最新情報を投稿し、連日経営者のコメントを含むプレスリリースで状況を詳細に公開しました。また、本社で記者会見し、報道関係者を運用管理室にも入れました。約 2 週間後の 4 月 2 日には、インシデントについてまとめた動画を YouTube で公開しています[ii]。インシデント発生後に、同社が Transparency（透明性）と Openness（率直さ）をポリシーとし、今後の被害防止の参考とするため情報公開の姿勢を貫いたことは高く評価されました[iii]。

セキュリティインシデントが公表されると、企業の株価は下落することが多いのですが、同社株価は、インシデント公表後に上昇しました[iv]。また、同社はこの一連の対応によって、European Excellence Awards 2019 の「Crisis Communications」部門で最優秀賞を受賞しました[v]。

この事例は、インシデント発生時の積極的な情報開示が、企業の社会的評価に大きく影響することを示しています。インシデント発生時のリスクコミュニケーションをどのように行うか、企業として常に議論し、計画しておくことが重要です。

i InsuranceBUSINESS AMERICA：Norsk Hydro gets more cyber insurance compensation https://www.insurancebusinessmag.com/us/news/cyber/norsk-hydro-gets-more-cyber-insurance-compensation-213096.aspx〔2020/6/25 確認〕
ii Norsk Hydro ASA：Cyber attack on Hydro Magnor https://www.youtube.com/watch?v=S-ZIVuM0we0〔2020/6/25 確認〕
iii Norsk Hydro ASA：Hydro awarded for cyber-attack transparency https://www.hydro.com/en-NO/media/news/2019/hydro-awarded-for-cyber-attack-transparency/〔2020/6/25 確認〕
Microsoft Corporation：Hackers hit Norsk Hydro with ransomware. The company responded with transparency https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/〔2020/6/25 確認〕
iv Bloomberg：NHY:NO Norsk Hydro ASA https://www.bloomberg.com/quote/NHY:NO（2019/3/20-2019/4/23）〔2020/6/25 確認〕
v EUROPEAN EXCELLENCE WARDS：Winnerlist 2019 https://eu-pr.excellence-awards.com/best-of-2019〔2020/6/25 確認〕

3.2 IoTの情報セキュリティ

IoT（Internet of Things）技術の組織における活用や個人における利用が増大し、インターネットにつながる機器（IoT 機器）の台数は、年々増加している。高い処理能力を有する多くの IoT 機器が世界中でインターネットに接続されている現状は、サイバー攻撃者にとって、悪用可能な攻撃対象が豊富に存在することを意味する。脆弱性が発見された IoT 機器は、対策を怠ると早々にウイルスに感染し、サイバー攻撃者に乗っ取られることとなる。

安心安全な IoT 社会を実現するためには、IoT 技術の恩恵を受けるすべての組織・個人が一丸となって対策に取り組み、脆弱性を解消していく必要がある。

本節では、IoT に対する脅威の動向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、本節中に番号（「CVE-2018-17173（JVNDB-2018-010306）」等）で記載している脆弱性については、「JVNDB-」で始まる番号を JVN iPedia※59 で検索することによって、日本語で概要及び関連情報へのリンクを確認できる。

3.2.1 常態化したIoTのセキュリティ脅威

IoT 機器を感染対象とするウイルスでは、感染手段として、「root」「password」「123456」といった初期値としてよく使われる文字列を含む ID、パスワードの組み合わせ等の典型的な認証情報※60 を用いた辞書攻撃に加えて、特定の IoT 機器が持つ脆弱性を狙い感染を試みる攻撃を併用することが定着してきた。脆弱な状態を放置したまま IoT 機器の運用を続けると、ウイルス感染が避けられない状況にあり、IoT 機器にはパソコンやサーバと同様の脆弱性対策が求められている。IoT 機器に感染するウイルスは、その特徴から「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」に分類することができる（表 3-2-1）。本項では、それぞれの分類ごとのウイルスの状況について解説する。

(1) 機器乗っ取り型ウイルスの動向

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の典型例である Mirai 及び Gafgyt（別名、Bashlite、QBot 等）は、それぞれソースコードが公開されていることもあり、様々な亜種が出現している。古くから存在する脆弱性や新たに発見された脆弱性を取り込み、感染対象とする IoT 機器を拡大するとともに、主な悪用目的である DDoS 攻撃能力の強化や、セキュリティ対策を回避するための隠密性の強化等、進化が続いている。また、Mirai や Gafgyt とは異なる機器乗っ取り型ウイルスも出現している。

(a) ファイル名が「clean」である Mirai の亜種

2019 年 1 月、新たに複数の IoT 機器の脆弱性への攻撃方法が追加された Mirai の新しい亜種が発見された※66。Barco, Inc. 社製ワイヤレスプレゼンテーションシステムや LG Electronics Incorporated 社製デジタルサイネージシステムといった企業向け製品を攻撃対象として追加しており、標的となる IoT 機器が企業所有の IoT 機器に移行していく可能性が示唆された。

IPA による分類	特徴	代表的なウイルスの例
機器乗っ取り型ウイルス	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、サイバー攻撃への悪用を試みる。 主な悪用方法は、DDoS 攻撃の踏み台としての利用であるが、このほかに不特定多数を対象とした不正なアプリケーション（ウイルス）感染、プロキシサーバとしての悪用、暗号通貨（暗号資産）のマイニングへの悪用等と、方法が多様化しており、IoT 機器の利用者自身に被害が及ぶ恐れもある※61。 また、同じウイルスに感染可能な IoT 機器を探索し、ボットネットの拡大を図る。	・Mirai※62 とその亜種 ・Gafgyt とその亜種 ・VPNFilter※63
機器保護型ウイルス	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行して、結果的に機器を他のウイルス感染から防御する。サイバー攻撃への悪用は行わない。 また、同じウイルスに感染可能な IoT 機器を探索し、ボットネットの拡大を図る。	・Hajime※64
機器破壊型ウイルス	感染した IoT 機器上で不正なプログラムを実行し、機器の機能を破壊することで使用不能とする。	・BrickerBot※65

■表 3-2-1　IoT 機器に感染するウイルスの分類

この亜種は、以下に示す特徴を有する。

- 初めて観測されたエクスプロイト※67（表 3-2-2）を含む、27 件のエクスプロイトを含む。
- 感染機器にダウンロードされるウイルスのファイル名（亜種の命名として採用される場合がある）に「clean」という文字列が用いられている。
- Mirai と同じ暗号化方式を採用している。
- 辞書攻撃に用いる認証情報の既定値として、これまで確認されたことのない組み合わせ（表 3-2-3）を有する。
- 他の脆弱な IoT 機器を探索する機能に加えて、HTTP フラッド攻撃（DDoS 攻撃の一手法）を実行する機能を有する。
- 脆弱性を悪用して機器にウイルスをダウンロードさせるシェルスクリプトの配布に、コロンビアにあるセキュリティ会社の侵害済み Web サイトを悪用する。

(b) fbot

2019 年 2 月、Mirai の亜種の一つである「fbot」が進化し、HiSilicon Technology Co., Ltd. 製の DVR（デジタルビデオレコーダー）／ NVR（ネットワークビデオレコーダー）用 SOC チップセットを用いた IoT 機器に感染が拡大し、ボットネットを構成していることが報告された※76。fbot は、2018 年 9 月に初めて報告されたウイルスで、2017 年 11 月に日本国内で感染が急増した Mirai の亜種「Satori※77」との強い関連が指摘されていた※78。その後、同社のチップセットを用いて開発された特定ベンダの製品において、TCP の 34567 番ポートで動作する DVRIP プロトコルの実装に脆弱性が存在し、以下に示す手順で感染可能となっていた。

①fbot に感染した機器は、TCP の 80、81、88、8000、8080 番ポートをとおして HTTP リクエストを送信して、

No.	ベンダ名	機器名	脆弱性
1	LG Electronics Incorporated	デジタルサイネージシステム SuperSign TVs	CVE-2018-17173（JVNDB-2018-010306）（LG SuperSign CMS リモートコード実行の脆弱性）
2	Barco, Inc.	ワイヤレスプレゼンテーションシステム wePresent WiPG-1000	wePresent WiPG-1000 コマンドインジェクションの脆弱性※68
3	D-Link Systems, Inc.	ネットワークビデオカメラ DCS-930L	D-Link DCS-930L リモートコマンド実行の脆弱性※69
4	D-Link Systems, Inc.	ルータ DIR-645、DIR-815	D-Link DIR-645/DIR-815 diagnostic.php コマンド実行の脆弱性※70
5	ZyXEL Technologies Co., Ltd.	ルータ P-660HN-T v1、P-660HN-T v2（TrueOnline※71 向け製品）	ZyXEL/Billion/TrueOnline リモートコマンド実行の複数の脆弱性※72（CVE-2017-18368（JVNDB-2017-014439）、CVE-2017-18370（JVNDB-2017-014437）、CVE-2017-18371（JVNDB-2017-014436）、CVE-2017-18374（JVNDB-2017-014433））
6	NETGEAR, Inc.	ワイヤレスアクセスポイント WG102、WG103、WN604、WNDAP350、WNDAP360、WNAP320、WNAP210、WNDAP660、WNDAP620	CVE-2016-1555（JVNDB-2016-008523）（非認証のリモートコマンド実行の脆弱性）
7	NETGEAR, Inc.	N300 ワイヤレス ADSL2+ モデムルータ DGN2200	CVE-2017-6077（JVNDB-2017-001693）（ping.cgi リモートコマンド実行の脆弱性）、CVE-2017-6334（JVNDB-2017-002116）（dnslookup.cgi リモートコマンド実行の脆弱性）
8	NETGEAR, Inc.	ワイヤレスコントローラ WC9500、WC7600、WC7520	Netgear Prosafe リモートコマンド実行の脆弱性※73

■表 3-2-2　ファイル名が「clean」である Mirai の亜種が感染に悪用する新たな脆弱性
（出典）Palo Alto Networks, Inc.「New Mirai Variant Targets Enterprise Wireless Presentation & Display Systems※8」を基に IPA が作成

ユーザ名	パスワード	該当する IoT 機器の例
admin	huigu309	メキシコの ISP、Axtel S.A.B. de C.V. が顧客に配布した以下のルータ※74 ・Dasan Zhone Solutions, Inc. 製 GPON ルータ ZNID-GPON-2520 ・Alcatel-Lucent S.A.（現 Nokia Corporation, Nokia Networks division）ルータ I-240W-Q
root	huigu309	
CRAFTSPERSON	ALC#FGU	
root	videoflow	VideoFlow Ltd. 製 Digital Video Protection DVP 10 version 2.10※75

■表 3-2-3　ファイル名が「clean」である Mirai の亜種に組み込まれた不正ログイン用認証情報の例
（出典）Palo Alto Networks, Inc.「New Mirai Variant Targets Enterprise Wireless Presentation & Display Systems」を基に IPA が作成

その戻り値から、同様に感染可能な機器を探索する。

②fbot に感染した機器は、発見した機器の IP アドレスとポート番号を Reporter（攻撃者のサーバ）に報告する。

③Reporter と Fbot Loader（攻撃者の別のサーバ）は、新たな感染対象機器の IP アドレスとポート番号を共有する。

④Fbot Loader は、新たな感染対象機器上で動作している Web サーバに認証情報の初期値「admin/ 空パスワード」でログインする。

⑤ログインに成功した場合、Fbot Loader は、DVRIP プロトコルのポート（TCP の 34567 番ポート）に認証情報の初期値「admin/tlJwpbo6」でログインする。

⑥Fbot Loader は、感染対象機器の TCP の 9000 番ポートで telnet バックドアを構築する。

⑦Fbot Loader は、感染対象機器の telnet バックドアを介して fbot ウイルスのダウンローダーをダウンロードさせる。

2019 年 2 月の時点では、2 万 4,528 台の感染が観測されている。国・地域別の感染機器台数の分布を表 3-2-4 に示す。

2019 年 9 月、「Nexus-Zeta」を名乗る 21 歳の青年は、fbot を含む Mirai の亜種 Satori、Okiru、Masuta、Tsunami を作成・運用した罪状を、アラスカ州の米国地方裁判所に対して認めた[※79]。

順位	国・地域名	機器台数	順位	国・地域名	機器台数
1	ベトナム	6,760	19	フランス	255
2	台湾	2,110	20	パキスタン	237
3	タイ	1,459	21	ウルグアイ	185
4	ブラジル	1,276	22	ポーランド	184
5	トルコ	1,137		英国	
6	インド	942	24	ベネズエラ	183
7	イラン	892	25	チリ	177
8	ロシア	862	26	モロッコ	176
9	インドネシア	609	27	ウクライナ	166
10	ルーマニア	579	28	ブルガリア	147
11	マレーシア	553	29	ギリシャ	142
12	イタリア	489	30	ハンガリー	141
13	コロンビア	363	31	シンガポール	130
14	エジプト	362	32	イスラエル	123
15	スリランカ	360	33	ドイツ	109
16	米国	328	34	バングラデシュ	106
17	アルゼンチン	310	35	スペイン	103
18	メキシコ	293			

■表 3-2-4　ウイルス fbot 感染機器の国・地域別分布
（出典）Qihoo 360 Technology Co. Ltd.「The new developments Of the Fbot[※76]」を基に IPA が作成

No.	ベンダ名	機器名	脆弱性
1	D-Link Systems, Inc.	Realtek SDK を用いたルータ該当製品	UPnP SOAP TelnetD コマンド実行の脆弱性（CVE-2014-8361（JVNDB-2014-008039））
2	Vera Control Ltd.	スマートホームコントローラ Mi Casa Verde VeraLite	リモートコード実行の脆弱性[※84]（CVE-2013-4863（JVNDB-2013-007151）、CVE-2016-6255（JVNDB-2016-007882））
3	各社	Realtek SDK を用いた各機器	Miniigd UPnP SOAP 任意のコード実行の脆弱性（CVE-2014-8361（JVNDB-2014-008039））
4	ZyXEL Technologies Co., Ltd.	ルータ ZyXEL P-660HN-T v1	ViewLog.asp remote host を介した権限昇格の脆弱性[※85]
5	DASAN Networks, Inc.	GPON ルータ	CVE-2018-10561（JVNDB-2018-004885）（認証回避の脆弱性） CVE-2018-10562（JVNDB-2018-004886）（コマンドインジェクションの脆弱性）
6	Huawei Technologies Co., Ltd.	ホームルータ HG532	CVE-2017-17215（JVNDB-2017-013014）（任意のコード実行の脆弱性）
7	Belkin International, Inc.	Linksys E-Series ルータ	リモートコード実行の脆弱性[※86]
8	各社	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	リモートコード実行の脆弱性[※87]

■表 3-2-5　Mirai の亜種「ECHOBOT」が感染に悪用する脆弱性
（出典）Trend Micro Incorporated「Mirai Variant Spotted Using Multiple Exploits, Targets Various Routers[※80]」を基に IPA が作成

(c) ECHOBOT

2019 年 4 月、表 3-2-5 に示す複数の脆弱性を悪用して感染を試みる、Mirai の新たな亜種「ECHOBOT」が発見された※80。辞書攻撃に用いる認証情報の既定値として、新たに追加された組み合わせ（表 3-2-6 の「admin/wbox123」）も観測された。

2019 年 6 月、同年 5 月下旬に更新されたと考えられる「ECHOBOT」が発見され、感染時に悪用する脆弱性や辞書攻撃用の認証情報が更に追加されていた※81。初めて実際に悪用が確認された脆弱性を表 3-2-7 に、過去に Mirai の他の亜種等で悪用が確認されていた脆弱性を表 3-2-8（次ページ）に示す。また、これまで確認されていなかった認証情報の既定値を表 3-2-9（次ページ）に示す。

2019 年 8 月、感染時に悪用する脆弱性や辞書攻撃用の認証情報が更に追加された「ECHOBOT」が発見された※82。新たに確認された脆弱性を表 3-2-10（次々ページ）に示す。

2019 年 12 月、感染時に悪用する脆弱性や辞書攻撃用の認証情報が更に追加された「ECHOBOT」が発見された※83。過去に Mirai の様々な亜種で悪用された脆弱性も組み込まれており、その総数は 70 を超えていた。新たに確認された脆弱性を表 3-2-11（172 ページ）に示す。

Mirai の亜種の多くは、大量に流通している特定の IoT 機器を感染対象として狙いを定め、その機器の脆弱性に絞り込んだ感染手段を用いる傾向がある。これに対して、「ECHOBOT」にはそれとは異なる傾向が見られ、2003 年に発見された非常に古い脆弱性から直近の 2019 年 12 月上旬に公開された脆弱性まで、新旧様々

ユーザ名	パスワード	該当する IoT 機器の例
admin	huigu309	表 3-2-3 参照
root	huigu309	
CRAFTSPERSON	ALC#FGU	
root	videoflow	
admin	wbox123	ADI Global Distribution（ADI-Gardiner Limited）製 W Box Technologies※88 ネットワークカメラ、NVR、DVR

■表 3-2-6　Mirai の亜種「ECHOBOT」に組み込まれた不正ログイン用認証情報の例
（出典）Trend Micro Incorporated「Mirai Variant Spotted Using Multiple Exploits, Targets Various Routers」を基に IPA が作成

No.	ベンダ名	機器名	脆弱性
9	Barco, Inc.（旧 Awind Inc.） 及び OEM 各社	ワイヤレスプレゼンテーションシステム wePresent WiPG-1000P、WiPG-1600W 他	CVE-2019-3929（JVNDB-2019-004073） （コマンドインジェクションの脆弱性）
10	各社	OpenDreamBox 2.0.0 を実行するデバイス セットボックス用の組み込み Linux ディストリビューションを用いた各機器	OpenDreamBox のリモートコード実行の脆弱性※89
11	各社	VMware NSX SD-WAN Edge 3.1.1 及びそれ以前のバージョン※90 を用いた各機器	CVE-2018-6961（JVNDB-2018-006479） （コマンドインジェクションの脆弱性）
12	各社	Schneider Electric 製 LifeSpace Management System U.motion Builder Software を用いた各機器	CVE-2018-7841（JVNDB-2018-015483） （SQL インジェクションの脆弱性）
13	Dell Inc.	Dell KACE Systems Management Appliance	Dell KACE のリモートコード実行の脆弱性※91
14	Geutebrück GmbH	ネットワークカメラ G-Cam/EFD-2250	CVE-2017-5174（JVNDB-2017-004264） （認証回避の脆弱性） CVE-2017-5173（JVNDB-2017-004263） （リモートコード実行の脆弱性）
15	Shenzhen Sunvalley Innovation Company Limited	モバイルルータ HooToo HT-TM05 TripMate	HooToo TripMate のリモートコード実行の脆弱性※92
16	各社	Asustor Inc. 製 NAS 用アプリケーション ADM 3.1.2.RHG1 及びそれ以前のバージョンをインストールした各機器	CVE-2018-11510（JVNDB-2018-007044） （非認証のリモートコード実行の脆弱性）

■表 3-2-7　Mirai の亜種「ECHOBOT」（2019 年 5 月下旬版）に追加された新しい脆弱性
（出典）Palo Alto Networks, Inc.「New Mirai Variant Adds 8 New Exploits, Targets Additional IoT Devices※81」を基に IPA が作成

な脆弱性を取り込んでいる。

(d)「Shiina」を含む URL からダウンロードされる Mirai の亜種

2019 年 5 月、Mirai の新たな亜種が発見された※114。過去に Mirai の亜種が感染手段として悪用した脆弱性のうち、13 種類(173 ページ表 3-2-12)を選択して採用しており、ウイルスをダウンロードする URL 中に「Shiina」という文字列が含まれていた。前述の「ECHOBOT」は新旧様々な脆弱性の悪用を試みるが、この亜種は、悪用実績が豊富で感染効果が見込める脆弱性を選択採用しており、Mirai の亜種の典型的な特徴を有する。

(e) Miori の亜種

2019 年 7 月、Mirai の亜種「Miori」の新たな亜種が発見された※128。この亜種は、以下に示す特徴を有しており、感染活動の発覚を妨害しつつ、発覚後の解析を困難とする狙いがあると考えられる。

- Miori は C&C サーバ※129 と通信する際、最初にポート番号 10019 に接続し、特定の文字列を送信してアクセスの許可を得る。この手順を踏まずに C&C サーバに telnet で接続を試みると、ログインプロンプトを表示する代わりに、セキュリティ研究者を侮辱するメッセージを表示して、接続を拒否する。セキュリティ研究者による C&C サーバの挙動解析を妨害する目的と考え

No.	ベンダ名	機器名	脆弱性
17	各社	Oracle WebLogic Server を用いた各機器	CVE-2019-2725（JVNDB-2019-002989）（Oracle WebLogic Server における Web Services に関する脆弱性）
18	LG Electronics Incorporated	デジタルサイネージシステム SuperSign TVs	CVE-2018-17173（JVNDB-2018-010306）（LG SuperSign CMS リモートコード実行の脆弱性）
19	Barco, Inc.（旧 Awind Inc.）	ワイヤレスプレゼンテーションシステム wePresent WiPG-1000	wePresent WiPG-1000 コマンドインジェクションの脆弱性※68
20	ASUSTeK Computer Inc.	ワイヤレス ADSL モデムルータ DSL-N12E_C1	ASUS DSL モデムのリモートコード実行の脆弱性※93
21	Belkin International, Inc.	スマートホーム機器 WeMo 各機器	Belkin WeMo UPnP リモートコード実行の脆弱性※94
22	NETGEAR, Inc.	ネットワークストレージ ReadyNAS	NETGEAR ReadyNAS のリモートコマンド実行の脆弱性※95
23	NUUO Inc.	NAS 機能付きネットワークビデオレコーダー NUUO NVRmini	NUUO NVRmini のリモートコマンド実行の脆弱性※96
24	各社	GoAhead Software Inc.（現 Oracle Corporation）製組み込み Web サーバ GoAhead を用いたネットワークカメラ	Wireless IP Camera (P2P) WIFICAM における複数の脆弱性※97

■表 3-2-8　Mirai の亜種「ECHOBOT」(2019 年 5 月下旬版)に追加された既存の脆弱性
(出典)Palo Alto Networks, Inc.「New Mirai Variant Adds 8 New Exploits, Targets Additional IoT Devices」を基に IPA が作成

ユーザ名	パスワード	該当する IoT 機器の例
blueangel	blueangel	5VTechnologies 製の組み込み機器 VoIP/SIP サービス用アプリケーション Blue Angel Software Suite※98
root	abnareum10	
root	Admin@tbroad	
root	superuser	
admin	pfsense	ファイアウォール／ルータ用オープンソースソフトウェア pfSense、pfSense を用いた Rubicon Communications, LLC 製 Netgate ブランドの各製品※99
admin	aerohive	Aerohive Networks, Inc.（現 Extreme Networks, Inc.）製 Wi-Fi アクセスポイント※100
root	awind5885	Crestron Electronics, Inc. 製 AirMedia Presentation Gateway AM-100※101
hadoop	123456	オープンソース Apache Hadoop を用いた各機器
hadoop	hadoop@123	
hadoop	hadoopuser	
root	ikwd	東芝製ネットワークカメラ

■表 3-2-9　Mirai の亜種「ECHOBOT」(2019 年 5 月下旬版)に追加された不正ログイン用認証情報の例
(出典)Palo Alto Networks, Inc.「New Mirai Variant Adds 8 New Exploits, Targets Additional IoT Devices」を基に IPA が作成

られる。
- 感染成功の判定に用いる、設定情報中の文字列に、亜種固有の文字列を含まない。セキュリティ研究者による亜種分類を妨害する目的と考えられる。
- ウイルス検体内部に、ソースコードを110ドルで販売するサイトのURLの文字列を含む。

(f) 文字列「LONGNOSE」を含みTorを利用するMiraiの亜種

2019年7月、Miraiの新たな亜種が発見されて、接続経路を匿名化するTor(The Onion Router)ネットワーク上にC&Cサーバを設置していることが判明した※130。この亜種は、以下に示す特徴を有する。
- ウイルス内部にsocks5プロキシサーバのリストを初期接続先アドレスとして保持し、Torネットワークを経由してC&Cサーバと通信を行う。
- 従来のMiraiの亜種が亜種固有の文字列を保持していた設定情報中の該当箇所に、「LONGNOSE」の文字列がある。
- 以下に示す脆弱性を悪用して感染拡大を試みる。
  - CVE-2017-11633(JVNDB-2017-012792)(Wireless IP Camera 360デバイスの脆弱性、TCPの9527番ポート経由のアクセスでRTSP(Real Time Streaming Protocol)認証情報の窃取可能)
  - DVRの34567番ポートに送信する遠隔管理用の認証情報の既定値(m3FSAeG3:admin)

Torを利用するのは、C&Cサーバの IPアドレスが発覚し、ホスティングサーバの停止やインターネットサービスプロバイダ(ISP:Internet Service Provider)による通信遮断等のセキュリティ対策が実施されることを回避するためであると考えられる。

No.	ベンダ名	機器名	脆弱性
25	Citrix Systems, Inc.	Citrix SD-WAN アプライアンス (旧 NetScaler SD-WAN アプライアンス)	CVE-2019-12991 (JVNDB-2019-006394) (コマンドインジェクションの脆弱性) CVE-2019-12989 (JVNDB-2019-006400) (SQL インジェクションの脆弱性)
26	EyeLock LLC	バイオメトリクス虹彩リーダー nano NXT	EyeLock nano NXT のリモートコード実行の脆弱性※102
27	Iris ID, Inc.	ICU7000-2	Iris ID IrisAccess ICU のクロスサイトスクリプティングの脆弱性※103
28	Beckhoff Automation GmbH	プログラマブルロジックコントローラ(PLC) CX9020 Basic CPU Module	CVE-2015-4051 (JVNDB-2015-002962) (DoS の脆弱性)
29	Comcast Corporation	Xfinity Gateway	Xfinity Gateway のリモートコード実行の脆弱性※104
30	Beward R&D Co., Ltd.	ネットワークカメラ Beward N100	Beward N100 のリモートコード実行の脆弱※105
31	AVM Computersysteme Vertriebs GmbH	ブロードバンドルータ Fritz!Box シリーズ	Fritz!Box Webcm のコマンドインジェクションの脆弱性※106
32	FLIR Systems, Inc.	サーマルネットワークカメラ ELARA FC-Series S、サポートセンサー Triton PT-Series	FLIR Thermal Camera のコマンドインジェクションの脆弱性※107
33	Sapido Technology Inc.	ルータ RB-1732	Sapido RB-1732 のリモートコマンド実行の脆弱性※108
34	各社	オープンソースの Web アプリケーションフレームワーク Ruby on Rails を用いた機器	CVE-2016-0752 (JVNDB-2016-001581) (ディレクトリトラバーサルとリモートコード実行の脆弱性)
35	各社	Rocket Software, Inc. 製バックアップ&データ保護用ソフトウェア Rocket Servergraph を使用するサーバ	CVE-2014-3914 (JVNDB-2014-003690) (ディレクトリトラバーサルの脆弱性)
36	各社	PHP で記述されたデータベース MongoDB 管理ツール PHPMoAdmin をインストールした機器	CVE-2015-2208 (JVNDB-2015-001796) (リモートコード実行の脆弱性)

■表 3-2-10　Mirai の亜種「ECHOBOT」(2019 年 8 月上旬版)に追加された新しい脆弱性
(出典)Palo Alto Networks, Inc.「iocs / mirai / ECHOBOT_6thAug2019.md※82」を基に IPA が作成

(g) Asher

2019 年 7 月、Mirai の新たな亜種「Asher」が発見された※131。ウイルス内部に埋め込まれた認証情報を用いた辞書攻撃に加えて、以下に示す脆弱性を悪用した感染を試みる。

- CVE-2018-10561（JVNDB-2018-004885）、CVE-2018-10562（JVNDB-2018-004886）
- MVPower DVR におけるシェルコマンド実行の脆弱性※125
- CVE-2014-8361（JVNDB-2014-008039）

(h) Moobot

2019 年 9 月、Wikimedia Foundation, Inc. が運営する Wikipedia、Amazon.com, Inc. が運営するライブストリーミングサービス Twitch、Blizzard Entertainment, Inc. が運営するオンラインゲーム World of Warcraft Classic のサーバに対して、UkDrillas と名乗る攻撃者による DDoS 攻撃が発生した※132。同年 8 月末から DVR を対象として感染を拡大していた Mirai の亜種「Moobot※133」による攻撃であると指摘されている※134。感染拡大のためにスキャンするポートや悪用する脆弱性の違いから、Moobot によって構築されたボットネットは以下の 3 種類に分類されている。

①TCP の 34567 番ポート（DVRIP プロトコル）をスキャンするタイプ
既定の認証情報でログインし、コマンドを実行することで特定のポートにバックドアを開け、そこからサーバに接続してウイルスのダウンロード、感染を行う。fbot（「3.2.1 (1) (b) fbot」参照）と類似の攻撃方法である。

②TCP の 80、81、82、83、85、88、8000、8080、8081、9090 番ポート（HTTP プロトコル）をスキャンするタイプ

No.	ベンダ名	機器名	脆弱性
37	YachtControl bv.	ヨットの制御用 Web サービスアプリケーション Yachtcontrol Webapplication 1.0	CVE-2019-17270（JVNDB-2019-013319）（リモートコード実行の脆弱性）
38	Technicolor SA	ルータ TD5130v2、TD5336	CVE-2019-18396（JVNDB-2019-011532）（SQL インジェクションの脆弱性） CVE-2017-14127（JVNDB-2017-007686）（コマンドインジェクションの脆弱性）
39	Epross Technology Co., Ltd.	ビデオカンファレンスシステム AVCON6	AVCON6 のリモートコード実行の脆弱性※109
40	各社	NETSAS Pty Ltd. 製ネットワーク管理ツール Enigma NMS をインストールした機器	CVE-2019-16072（JVNDB-2019-015139）（コマンドインジェクションの脆弱性）
41	三菱電機株式会社 INEA d.o.o.	プログラマブルロジックコントローラ（PLC） リモートターミナルユニット Mitsubishi Electric smartRTU INEA ME-RTU	CVE-2019-14931（JVNDB-2019-011332）（コマンドインジェクションの脆弱性）
42	各社	Sar データ（Linux システム統計情報）のグラフィカル変換ツール sar2HTML をインストールした機器	sar2HTML のリモートコード実行の脆弱性※110
43	NetGain Systems	IT 監視アプライアンス NetGain Enterprise Manager	CVE-2017-16602（JVNDB-2017-012144）（任意のコード実行の脆弱性）
44	Citrix Systems, Inc.	Citrix SD-WAN アプライアンス （旧 NetScaler SD-WAN アプライアンス）	CVE-2017-6316（JVNDB-2017-005962）（非認証のリモートコード実行の脆弱性）
45	Thomson Reuters Corporation	Velocity Analytics Vhayu Analytic Server	CVE-2013-5912（JVNDB-2013-005263）（コードインジェクションの脆弱性）
46	ACTi Corporation	ACTi ASOC 2200 Web Configurator	ACTi ASOC2200 のリモートコード実行の脆弱性※111
47	3Com Corporation（現 Hewlett Packard Enterprise Co.）	ルータ 3Com OfficeConnect	3Com Office Connect のリモートコード実行の脆弱性※112
48	Barracuda Networks, Inc.	スパムメール対策アプライアンス Barracuda Spam Firewall （現 Barracuda Email Security Gateway）	CVE-2006-4000（JVNDB-2006-001041）（ディレクトリトラバーサルの脆弱性）
49	CCBill LLC.	オンライン支払システム CCBill Online Payment Services	CCBill のリモートコード実行の脆弱性※113

■表 3-2-11　Mirai の亜種「ECHOBOT」（2019 年 12 月上旬版）に追加された新しい脆弱性
（出典）Palo Alto Networks, Inc.「Mirai Variant ECHOBOT Resurfaces with 13 Previously Unexploited Vulnerabilities※83」を基に IPA が作成

HiSilicon Technology Co., Ltd. 製の SOC チップセットを用いた DVR の RCE 脆弱性※135 を悪用して機種を特定し、機種固有の脆弱性を狙って感染拡大を図る。

③TCP の 60001 番ポート（HTTP プロトコル）をスキャンするタイプ

JAWS Web Server の RCE 脆弱性※125 を悪用してコマンドを実行することで、シェルスクリプトをダウンロードし、スクリプトがウイルスのダウンロード、感染を行う。

同年 9 月末には、更に多くの Moobot の亜種が発見されており、下記に示すポートのスキャン活動が報告されている※136。

No.	脆弱性	悪用実績
1	Vacron NVR における RCE※115 脆弱性※116	Omni※117
2	CVE-2018-10561（JVNDB-2018-004885）、CVE-2018-10562（JVNDB-2018-004886）	Omni
3	CVE-2015-2051（JVNDB-2015-001591）	Omni、Hakai※118
4	複数ベンダの CCTV/DVR における RCE 脆弱性※119	Omni、Yowai※120
5	CVE-2014-8361（JVNDB-2014-008039）（Miniigd UPnP SOAP 任意のコード実行の脆弱性）	Omni
6	D-Link 製品における UPnP SOAP TelnetD コマンド実行の脆弱性※121	Omni
7	eir D1000 における WAN 側からのリモートコードインジェクションの脆弱性※122（CVE-2016-10372（JVNDB-2016-008586））	Omni
8	Netgear 製ルータの setup.cgi における RCE 脆弱性※123	Omni
9	CVE-2016-6277（JVNDB-2016-006166）（Netgear 製の複数のルータ（R7000、R6400 等）における cgi-bin コマンドインジェクションの脆弱性※124）	Omni、VPNFilter
10	MVPower DVR におけるシェルコマンド実行の脆弱性※125	Omni
11	CVE-2017-17215（JVNDB-2017-013014）	Omni、Satori、Miori※126
12	LinkSys E-Series ルータにおける RCE 脆弱性※86	TheMoon※127
13	ThinkPHP 5.0.23/5.1.31 における RCE 脆弱性※87	Hakai、Yowai

■表 3-2-12 「Shiina」を含む URL からダウンロードされる Mirai の亜種が感染に悪用する脆弱性
（出典）Trend Micro Incorporated「New Mirai Variant Uses Multiple Exploits to Target Routers and Other Devices※114」を基に IPA が作成

- TCP の 84、1588、5984、8181、8888、9200 番ポート（HTTP プロトコル、前述の②③に示したポート番号に加えてスキャンする）
- TCP の 5555 番ポート（ADB）
- TCP の 23 番ポート（TELNET）

報告当時、一週間で約 6 万 6,000 台の感染が観測されており、感染機器は世界中に散在していることが確認されている。国・地域別の感染機器台数の分布を、表 3-2-13 に示す。

順位	国・地域名	機器台数	順位	国・地域名	機器台数
1	ブラジル	7,913	26	チリ	577
2	中国	5,749	27	ポーランド	497
3	ベトナム	5,305	28	カタール	477
4	タイ	4,514	29	南アフリカ	472
5	ウルグアイ	4,510	30	イスラエル	456
6	イタリア	3,685	31	ドミニカ	455
7	ロシア	3,070	32	ウクライナ	417
8	アルゼンチン	2,440	33	コロンビア	415
9	トルコ	2,410	34	エジプト	407
10	マレーシア	2,073	35	ハンガリー	376
11	韓国	2,068	36	チュニジア	370
12	インド	1,783	37	フランス	322
13	ドイツ	1,594	38	カザフスタン	295
14	米国	1,554	39	サウジアラビア	279
15	イラン	1,433	40	オーストラリア	273
16	メキシコ	1,132	41	シンガポール	271
17	スペイン	1,062	42	ブルガリア	244
18	英国	967	43	UAE	232
19	モロッコ	946	44	カナダ	185
20	ギリシャ	937	45	ヨルダン	136
21	インドネシア	798	46	オマーン	120
22	ベネズエラ	782	47	セルビア	114
23	パキスタン	774	48	ポルトガル	112
24	ルーマニア	758	49	プエルトリコ	101
25	日本	632			

■表 3-2-13 ウイルス Moobot 感染機器の国・地域別分布
（出典）Qihoo 360 Technology Co. Ltd.「The Botnet Cluster on the 185.244.25.0/24※136」を基に IPA が作成

(i) Momentum

2019 年 12 月、Mirai の新しい亜種「Momentum」が発見された※137。Momentum が感染に悪用する脆弱性を、以下に示す。

- 複数ベンダの CCTV/DVR における RCE 脆弱性※119
- ZyXEL ルータの脆弱性

（CVE-2017-18368（JVNDB-2017-014439）に類似）
- CVE-2017-17215（JVNDB-2017-013014）
- 複数ベンダのワイヤレスプレゼンテーションシステムにおけるコマンドインジェクションの脆弱性
（CVE-2019-3929（JVNDB-2019-004073）に類似）
- D-Link ルータの HNAP 実装の脆弱性※138
- Realtek SDK における UPnP SOAP コマンド実行の脆弱性
（CVE-2014-8361（JVNDB-2014-008039））
- CVE-2018-10562（JVNDB-2018-004886）
- JAWS Web Server における RCE 脆弱性※125
- Vacron NVR における RCE 脆弱性※116
- UPnP SOAP Command Execution の脆弱性
（CVE-2016-10372（JVNDB-2016-008586）に類似）
- ThinkPHP における RCE 脆弱性※139
- HooToo TripMate における RCE 脆弱性※92

(j) その他の Mirai の亜種

2020 年に入ってからも Mirai の様々な亜種が発見されている。

- 2020 年 2 月、Rasilient Systems, Inc. 製の監視カメラ用ストレージシステムの脆弱性（CVE-2020-6756（JVNDB-2020-001330））の悪用を試みる Mirai の亜種「SORA」「UNSTABLE」が発見された※140。
- 2020 年 3 月、ZyXEL Technologies Co., Ltd. 製の NAS のコマンドインジェクションの脆弱性（CVE-2020-9054（JVNDB-2020-001758））の悪用を試みる Mirai の亜種「Mukashi」が発見された※141。
- 2020 年 3 月、Netlink ICT Pvt Ltd. 製 GPON ルータの脆弱性※142 を狙う Mirai の亜種が発見された※143。ウイルスのファイル名に「rispek」という文字列が用いられている。

(k) Gafgyt の様々な亜種

Gafgyt は、2015 年初めにソースコードが公開されて以来、様々な亜種が発生しており、近年では Mirai と同様に特定の IoT 機器の脆弱性を狙った感染手段の拡張が行われている。

2019 年 1 月、Mirai の亜種が発見されたホストにおいて、ファイル名に「eeppinen」という文字列が用いられた Gafgyt の亜種が発見された※66。

2019 年 4 月、Belkin International, Inc. のスマートホーム機器 WeMo を狙う Gafgyt の亜種が発見された※144。この亜種は、2018 年 5 月に発見された Gafgyt の亜種「Hakai※118」が進化したものと考えられ、Universal Plug and Play（UPnP）API を有効化した WeMo のリモートコード実行の脆弱性※94 を悪用して感染を拡大する。

2019 年 8 月、Gafgyt の新たな亜種「Ayedz」が発見された※131。感染後、攻撃者に送信する機器の情報（動作しているプロセス、保有する実行モジュール、Linux のディストリビューションの種類等）や攻撃者から DDoS 攻撃を指示するコマンド群等の解析結果が報告されている。

2019 年 9 月、小規模オフィス／家庭向けルータに感染しようとする Gafgyt の亜種が発見された※145。この亜種は、JenX ／ Jennifer※146 に由来するものと考えられる。感染対象機器と感染に悪用する脆弱性を、以下に示す。

- ZyXEL P660HN-T1A
（CVE-2017-18368（JVNDB-2017-014439））
- Huawei HG532
（CVE-2017-17215（JVNDB-2017-013014））
- Realtek RTL81XX チップセットを用いた各機器
（CVE-2014-8361（JVNDB-2014-008039））

この亜種は、Valve Corporation によって開発された Source Engine を採用したゲームサーバに対して DoS 攻撃を実行する専用のコマンドを有すること、感染機器上で動作している他のウイルスのプロセスを終了させること、を特徴とする。また、JenX ／ Jennifer と同様に、DDoS 攻撃をレンタル提供するサービスに悪用されている。

(l) Hide 'N Seek

Hide 'N Seek（別名、HNS）は、2018 年 1 月に発見された IoT ボットネットで、ウイルスに感染した IoT 機器の通信に P2P（Peer-to-Peer）を用いることを特徴とする※147。2019 年 2 月、以下に示す脆弱性を感染手段として追加された亜種が発見された※148。

- CVE-2019-7238（JVNDB-2019-002836）
（Sonatype Nexus Repository Manager のインストールにおける RCE 脆弱性）
- CVE-2018-20062（JVNDB-2018-012013）
（Web アプリケーションフレームワーク ThinkPHP における RCE 脆弱性）
- CVE-2018-7297（JVNDB-2018-002349）
（HomeMatic Zentrale CCU2 における RCE 脆弱性）
- Apache CouchDB における RCE 脆弱性※149
- OrientDB における RCE 脆弱性※150

- Netgear 製ルータ DGN1000 の setup.cgi における RCE 脆弱性※123
- AVTECH 製ネットワークカメラ／ DVR ／ NVR における RCE 脆弱性※151
- TP-Link 製ルータ TL-WDR4300 におけるバックドア※152

(m) Neko

2019 年 7 月、IoT 機器に感染してボットネットを構築する新たなウイルス「Neko」が発見された※131。「Neko」は複数のアーキテクチャに対応しており、感染機器内に存在する他のウイルスのプロセスを終了する機能や、UDP フラッド攻撃等を用いて DDoS 攻撃を仕掛ける機能を有する。以下に示す脆弱性を悪用して感染を試みる。

- ルータ eir D1000 における WAN 側の RCE 脆弱性※122
- CVE-2015-2051（JVNDB-2015-001591）
- CVE-2017-17215（JVNDB-2017-013014）
- CVE-2018-10561（JVNDB-2018-004885）、CVE-2018-10562（JVNDB-2018-004886）
- LinkSys E-Series ルータにおける RCE 脆弱性※86
- MVPower DVR におけるシェルコマンド実行の脆弱性※125
- ThinkPHP 5.0.23/5.1.31 における RCE 脆弱性※87
- Realtek SDK における Miniigd UPnP SOAP コマンド実行の脆弱性
（CVE-2014-8361（JVNDB-2014-008039））

同月末、感染拡大の悪用手段として、下記に示す脆弱性が追加された亜種が発見された。

- Netgear 製のルータ DGN1000/DGN2200 における複数の脆弱性※153
- 複数ベンダの CCTV/DVR における RCE 脆弱性※119
- Netgear 製の複数のルータ（R7000、R6400 等）における cgi-bin コマンドインジェクションの脆弱性
（CVE-2016-6277（JVNDB-2016-006166））
- Vacron NVR における RCE 脆弱性※116
- CVE-2018-15379（JVNDB-2018-013332）
- Linksys ルータ WAP54Gv3 におけるリモートデバッグルートシェルの脆弱性※154

(n) Mozi

2019 年 9 月、Gafgyt のソースコードを流用し、ウイルスに感染した IoT 機器間の通信に DHT プロトコルをベースとした P2P 通信を用いるように拡張された「Mozi」が発見された※155。Mozi は、認証情報の既定値または以下に示す脆弱性を悪用して感染を拡大する。

- ルータ eir D1000 における WAN 側の RCE 脆弱性※122
- Vacron NVR における RCE 脆弱性※116
- CVE-2014-8361（JVNDB-2014-008039）
- Netgear 製の複数のルータ（R7000、R6400 等）における cgi-bin コマンドインジェクションの脆弱性
（CVE-2016-6277（JVNDB-2016-006166））
- Netgear 製ルータ DGN1000 の setup.cgi における RCE 脆弱性※123
- MVPower DVR に搭載された JAWS Web Server における RCE 脆弱性※125
- CVE-2017-17215（JVNDB-2017-013014）
- D-Link 製品における HNAP SOAPAction-Header コマンド実行の脆弱性
（CVE-2015-2051（JVNDB-2015-001591））
- CVE-2018-10561（JVNDB-2018-004885）、CVE-2018-10562（JVNDB-2018-004886）
- D-Link 製品における UPnP SOAP TelnetD コマンド実行の脆弱性
（CVE-2014-8361（JVNDB-2014-008039））
- 複数ベンダの CCTV/DVR における RCE 脆弱性※119

2019 年 11 月から 2020 年 1 月にかけて、日本国内においても Mozi の感染拡大を図るアクセスの増加が観測されている※156。

(o) LiquorBot

2020 年 1 月、暗号通貨 Monero のマイニング機能を有するウイルス「LiquorBot」の活動の観測結果が公開された※157。LiquorBot は、2019 年 5 月に初めて検出されたウイルスで、プログラミング言語 Go（golang）で記述されている。2019 年 7 月に検出された検体は、82 種類の既定の認証情報を用いた辞書攻撃に加えて、以下に示す様々な IoT 機器の脆弱性を悪用して感染する。

- CVE-2015-2051（JVNDB-2015-001591）
- CVE-2016-1555（JVNDB-2016-008523）
- CVE-2016-6277（JVNDB-2016-006166）
- CVE-2018-17173（JVNDB-2018-010306）
- CVE-2017-6884（JVNDB-2017-002996）
- CVE-2018-10562（JVNDB-2018-004886）
- CVE-2017-6077（JVNDB-2017-001693）

- CVE-2017-6334（JVNDB-2017-002116）
- CVE-2016-5679（JVNDB-2016-004493）
- CVE-2018-9285（JVNDB-2018-004344）
- CVE-2013-3568（JVNDB-2013-007218）
- CVE-2019-12780（JVNDB-2019-005521）

(p) Muhstik の亜種

2019 年 12 月、Muhstik の新しい亜種が発見された※158。Muhstik は 2018 年 3 月から稼働しているボットネットで、この亜種はオープンソースのファームウェア Tomato を用いたルータを攻撃する機能が追加されており、既定の認証情報である admin:admin、root:admin を用いて侵入を試みる。インターネット接続機器検索サービス Shodan※159 を用いた調査によると、この時点でインターネット上に約 4,600 台の潜在的被害端末が存在することが報告されている。

(2) 機器保護型ウイルスの動向

感染した IoT 機器の特定のポートへの通信を遮断して、結果的に感染機器を他のウイルス（Mirai やその亜種等）による感染から防御する Hajime は、2016 年 10 月に初めて発見された※64。当初は、各機器の既定の認証情報※160 を用いたログインを感染手段としていたが、Mirai の亜種が特定機器の脆弱性を感染手段として悪用を開始すると、同様の感染手段を取り込み、Mirai の亜種と感染について競合する形となっている。

2018 年 5 月に発見された検体を最後に、更新された Hajime は検出されておらず※161、以降は同じ感染手段での活動を継続しているとみられる。これまで Hajime が用いたことが確認された感染手段を、表 3-2-14 に示す。

(3) 機器破壊型ウイルスの動向

感染した IoT 機器を使用不能とし、他のウイルス感染を防止しようとする機器破壊型ウイルスとしては、2016 年 11 月から活動を開始した BrickerBot が存在したが、2017 年 12 月に作者が「1,000 万台以上の IoT 機器を使用不能にしたインターネット化学療法を終了する」と宣言し、活動を終了した。

2019 年、IoT 機器を使用不能とする新たな機器破壊型ウイルスが出現した。機器の種別を特定せずに無差別に攻撃を仕掛けるため、産業ネットワークやヘルスケアで用いられている IoT 機器が攻撃された場合、生命が脅かされるリスクが指摘されている※166。

(a) Silex

2019 年 6 月、IoT 機器のファームウェアを消去して使用不能とする新たなウイルス「Silex」の活動が発見された※167。発見当初、約 350 台の機器を破壊していた Silex は、1 時間後には 2,000 台の機器を使用不能とした。Silex は、以下に示す手順で IoT 機器を破壊する。

①機器のストレージの破壊
（パーティションへのランダムデータの書き込み）
②ルーティングテーブルの削除
③ネットワーク構成の削除
④機器の停止
（起動不能状態にした上での再起動）

検出された機器破壊用コマンド群を、図 3-2-1 に示す。回復にはファームウェアの再インストールが必要であり、エンドユーザが実施することは困難である。ウイルス感染に気付かないユーザは、ハードウェア障害が発生したと思い込み、機器を捨ててしまう可能性が高い、と指摘

No.	ポート	プロトコル	感染手段
1	TCP:23	TELNET	既定の認証情報を用いた辞書攻撃による不正ログイン
2	TCP:5358		
3	TCP:7547	HTTP	ホームルータ管理プロトコル TR-069 の実装上の脆弱性※162
4	TCP:81	HTTP	GoAhead Web Server を搭載したネットワークカメラにおける複数の脆弱性※97
5	TCP:9000	MCTP	KGurad Security 製 DVR における脆弱性（CVE-2015-4464（JVNDB-2015-007803））
6	TCP:8291	Winbox 独自	SIA Mikrotīkls 製 MikroTik RouterOS の管理アプリケーション Winbox の RCE 脆弱性※163
7	TCP:2000		
8	TCP:80	HTTP	DASAN Networks, Inc. 製 GPON ルータにおける脆弱性（CVE-2018-10561（JVNDB-2018-004885）、CVE-2018-10562（JVNDB-2018-004886））
9	TCP:8080		

■表 3-2-14　Hajime が用いたことが確認された感染手段
（出典）株式会社インターネットイニシアティブ「Hajime ボットの観測状況※164」「Hajime ボットによる 8291/tcp へのスキャン活動※165」「2018 年の IoT ボット観測状況と最近の動向※161」等を基に IPA が作成

されている。

14 歳であると主張し「Light Leafon」と名乗る Silex の作者は、現時点では認証情報が初期設定値のままの IoT 機器を感染対象としているが、今後は Mirai や Gafgyt の亜種と同様に、脆弱性を放置した特定の機器を攻撃対象と追加していく計画である、と表明した。

```
fdisk -l
busybox cat /dev/urandom >/dev/mtdblock0
busybox cat /dev/urandom >/dev/sda
busybox cat /dev/urandom >/dev/ram0
busybox cat /dev/urandom >/dev/mmc0
busybox cat /dev/urandom >/dev/mtdblock10
fdisk -C 1 -H 1 -S 1 /dev/mtd0
fdisk -C 1 -H 1 -S 1 /dev/mtd1
fdisk -C 1 -H 1 -S 1 /dev/sda
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
illed bot process
route del default
iproute del default
ip route del default
rm -rf /* 2</dev/null
sysctl -w net.ipv4.tcp_timestamps=0
sysctl -w kernel-threads-max=1
iptables -F;iptables -t nat -F;iptables -A INPUT -j DROP;iptables -A FORWARD -j DROP
halt -n -f
reboot
```

■図 3-2-1　Silex の機器破壊コマンド群
（出典）Larry W. Cashdollar r00t folding team #258829 のツイート※168

(b) handymanny

2019 年 9 月、感染した IoT 機器を破壊する新たなウイルス「handymanny」が発見された※136。Silex と同様の手順で、機器を使用不能とするコマンド群を内部に保持することが確認されている。

3.2.2 脆弱な IoT 機器とウイルス感染の実態

脆弱な状態にある IoT 機器を狙うサイバー攻撃が常態化する中、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だろうか。本項では、IoT 機器のセキュリティ対策強化の取り組みとして公開されている情報から、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

2019 年 2 月、総務省及び国立研究開発法人情報通信研究機構（NICT：National Institute of Information and Communication Technology）は、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）※169」を開始した※170。

また、2019 年 6 月、総務省、NICT、一般社団法人 ICT-ISAC 及びインターネット接続事業者が連携して、NICT の NICTER プロジェクト※171 によりウイルス感染を原因とする通信を行っていることが検知された IoT 機器について、インターネット接続事業者が当該機器の利用者を特定の上、利用者に注意喚起を実施する取り組みを開始した※172。

総務省、NICT、ICT-ISAC は、2019 年度四半期ごと（2019 年 4 ～ 6 月、7 ～ 9 月、10 ～ 12 月、2020 年 1 ～ 3 月）の取り組み実施結果を集計し、2019 年 6 月、同年 10 月、2020 年 1 月、同年 5 月に公開（表 3-2-15）しており、国内における脆弱な IoT 機器とウイルス感染の実態を以下のように考察している。

- 第 1 四半期では、脆弱な IoT 機器（容易に推測される ID・パスワードを設定している IoT 機器）の検出件数、ウイルス感染した IoT 機器の利用者への注意喚起の件数は少ない状況にある。

調査内容と取り組み		調査期間			
		2019 年度 第 1 四半期（2019 年 4～6 月）	2019 年度 第 2 四半期（2019 年 7～9 月）	2019 年度 第 3 四半期（2019 年 10～12 月）	2019 年度 第 4 四半期（2020 年 1～3 月）
参加 ISP 社数		33 社	34 社	41 社	50 社
調査対象	調査対象 IP アドレス	約 0.9 億アドレス	約 1.0 億アドレス	約 1.1 億アドレス	約 1.1 億アドレス
	調査対象ポート	非公開	非公開（ただし、第 1 四半期より増加）		
NOTICE の取り組み結果	ID・パスワードが入力可能であった IoT 機器	約 4 万 2,000 件	約 9 万 8,000 件	約 11 万 1,000 件	約 10 万件
	内、ログイン可能であった注意喚起の対象 IoT 機器	147 件	358 件	823 件	921 件
感染機器の利用者への注意喚起	ISP に対する通知の対象（1 日当たり）	112 ～ 155 件	80 ～ 559 件（第 2 四半期までの累計平均 197 件）	60 ～ 598 件（第 3 四半期までの累計平均 176 件）	46 ～ 524 件（第 4 四半期までの累計平均 162 件）

■表 3-2-15　国内における注意喚起の取り組みの実施結果
（出典）総務省、NICT、ICT-ISAC の公開情報※173 を基に IPA が作成

- 第 2 四半期では、第 1 四半期までと比較して脆弱な IoT 機器の検出件数が増加しているが、調査対象 IP アドレス及び調査対象ポートの拡大、並びに調査プログラムの改良によるものと考えられ、脆弱な IoT 機器の割合については大きな変化はない。また、ウイルス感染した IoT 機器の利用者への注意喚起の件数も 2019 年 8 月末から増加しているが、長期的な観測傾向から見ると大きな変化はない。
- 第 3 四半期では、第 2 四半期までと比較して脆弱な IoT 機器の検出件数が増加しているが、調査対象 IP アドレスの拡大及び調査プログラムの改良によるものと考えられ、脆弱な IoT 機器の割合については大きな変化はない。また、ウイルス感染した IoT 機器の利用者への注意喚起の件数も、長期的な観測傾向から見ると大きな変化はない。
- 第 4 四半期では、脆弱な IoT 機器の検出件数及び割合については大きな変化はない。また、ウイルス感染した IoT 機器の利用者への注意喚起の件数は、2020 年 2 月下旬から 3 月上旬にかけて一時的に増加しているが、Mirai の亜種の活動が一時的に活発化した影響と考えられ、長期的な観測傾向から見ると大きな変化はない。

以上のことから、国内において容易に推測される ID・パスワードを設定している IoT 機器、既にウイルス感染していると判明した IoT 機器の数は、2019 年度の一年間をとおして少ない状況にある、と報告している。

(2) ハニーポットにおける IoT ボットネットの観測

株式会社インターネットイニシアティブが実施しているマルウェア活動観測プロジェクトで設置したハニーポットにおける観測結果として、ウイルスに感染した IoT 機器によるボットネットの活動状況が報告されている※174。

IoT 機器に感染したウイルスの大半は、同様に感染可能な脆弱な IoT 機器をスキャンするためのパケットを送信する機能を有するため、ハニーポットに対してパケットを送信してきたユニークな送信元アドレスの数は、ウイルスに感染した IoT 機器の台数を反映した値であると考えられる。これらの観測結果（アドレス数の推移、アドレス数の国別推移）から、世界中の IoT 機器のウイルス感染状況や国別分布を考察することが可能となる。

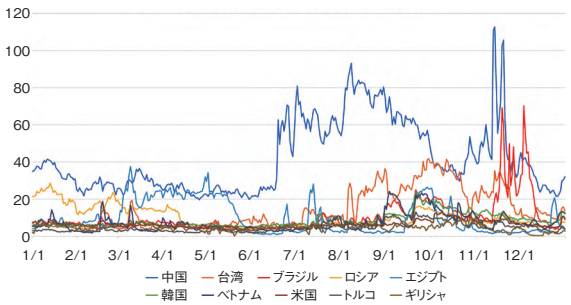
(a) Mirai の亜種の観測結果

ハニーポットにおいて検出された Mirai の亜種によるスキャン通信（Mirai の特徴に合致するパケット）について、ユニークな送信元アドレス数の 1 年間の推移を図 3-2-2 に、上位 10 位までの国・地域（中国、台湾、ブラジル、ロシア、エジプト、韓国、ベトナム、米国、トルコ、ギリシャ）の個別の推移を図 3-2-3 に示す。

2019 年前半、感染は減少傾向が見られたものの、7 月以降増加に転じ、11 月ごろのピークを迎えて再び減少傾向となり、最終的に年初とほぼ同じアドレス数に帰着している。7 月後半～ 9 月の増加は、Huawei Technologies Co., Ltd. 製ルータ HG532 の脆弱性（CVE-2017-17215（JVNDB-2017-013014））を悪用した感染が拡大したことによる増加と言われている。また、9 月～ 11 月の増加は、特定の IoT 機器固有の脆弱性を狙った fbot（「3.2.1 (1) (b) fbot」参照）や Moobot（「3.2.1 (1) (h) Moobot」参照）の活動が活発になった影響による増加と言われている。

国・地域別では、年間を通じて中国の感染台数が最も多い。また、脆弱性を狙う特定の亜種による活動の活発化に伴い、対応する国・地域（台湾、ブラジル、エジプト等）の感染台数が一時的に増加する傾向が見られる。これは、脆弱性を狙われる IoT 機器の一部は、インターネット接続事業者により顧客に配布されるルータやモデムのように、特定の国・地域において一定の台数が配布・流通されていることがあるためと考えられる。

■図 3-2-2　Mirai 亜種ユニーク送信元アドレス数の推移
（出典）株式会社インターネットイニシアティブ「2019 年の IoT ボット観測状況※174」を基に IPA が編集



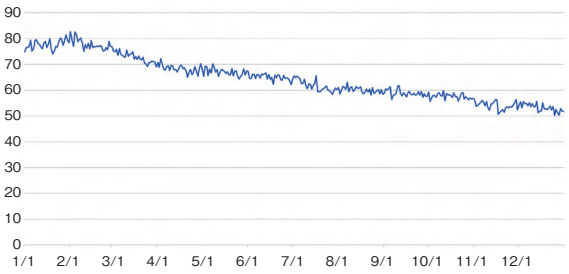
■図 3-2-3　Mirai 亜種ユニーク送信元アドレス数の国・地域別推移
（出典）株式会社インターネットイニシアティブ「2019 年の IoT ボット観測状況※174」を基に IPA が編集

(b) Hajime の観測結果

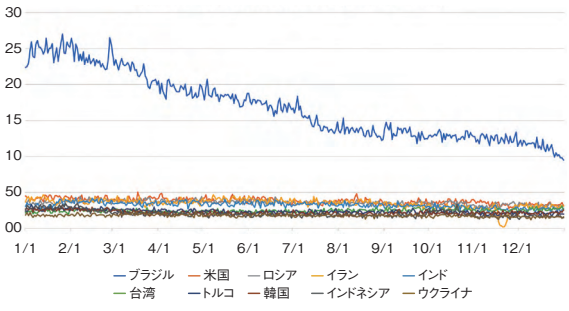
ハニーポットにおいて検出された Hajime によるスキャン通信（Hajime の特徴に合致するパケット）について、ユニークな送信元アドレス数の 1 年間の推移を図 3-2-4 に、上位 10 位までの国・地域（ブラジル、米国、ロシア、イラン、インド、台湾、トルコ、韓国、インドネシア、ウクライナ）の個別の推移を図 3-2-5 に示す。

2019 年冒頭、Mirai の亜種の約半分のアドレス数を示していた Hajime は、緩やかな減少傾向を続けて、年末までに約 20% ～ 25% 感染が減少している。

国・地域別では、ブラジル一国に集中しており、感染台数の約 4 分の 1 を占める。Hajime は 2018 年 5 月以降更新を停止しており（「3.2.1 (2) 機器保護型ウイルスの動向」参照）、感染に悪用する脆弱性が追加されていないため、ブラジル以外に設置された新しい IoT 機器への感染が非常に少ないと考えられる。また、ブラジルの感染台数も 1 年間で半数以下に減少しており、全体の感染台数減少につながっている。



■図 3-2-4　Hajime ユニーク送信元アドレス数の推移
（出典）株式会社インターネットイニシアティブ「2019 年の IoT ボット観測状況※117」を基に IPA が編集



■図 3-2-5　Hajime ユニーク送信元アドレス数の国・地域別推移
（出典）株式会社インターネットイニシアティブ「2019 年の IoT ボット観測状況※117」を基に IPA が編集

Mirai の亜種は、様々な脆弱性を感染拡大手段として取り込みつつ、多様な亜種が発生し、世界中の IoT 機器を攻撃対象とした活動を継続している。Mirai と並び IoT 機器を感染対象とする Gafgyt は、通信に特徴が見られず、またスキャン活動を行わない検体も多いことから、全体の感染規模は不明であるが、様々な亜種が派生していることは確認されている。結果的に Mirai や Gafgyt の亜種の感染から IoT 機器を防御している Hajime は、更新が停止されていることから、その活動は縮小傾向にある。今後も、Mirai 及び Gafgyt の亜種による IoT に対する脅威が継続することが考えられる。

3.2.3 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 に対する脅威は常態化しており、世界中に存在する IoT 機器に対する脆弱性対応を含むセキュリティ対策が必須となっている。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、新たに発行されたセキュリティガイド等が引き続き公開されている。2019 年以降に国内及び海外で公開された資料を、表 3-2-16（次ページ）と表 3-2-17（次々ページ）に示す。

(2) IoT 機器に対する規制の強化

初期状態で脆弱な IoT 機器が市場に流通することを防止するために、各国において IoT 機器の製造者や販売者に対する法規制の制定・施行が始まっている。ここでは、主なものを紹介する。

(a) 電気通信事業法における端末設備等規則

総務省は、IoT 機器を含む端末設備の技術基準にセキュリティ対策を追加するための改正省令「端末設備等規則及び電気通信主任技術者規則の一部を改正する省令（平成 31 年総務省令第 12 号）」を 2019 年 3 月 1 日に公布した※193。その後、「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 1 版）」を策定し、2019 年 4 月 22 日に公開した※194。これにより、IoT 機器を含む端末設備の技術基準にセキュリティ対策を追加するための「端末設備等規則（昭和 60 年郵政省令第 31 号）」の一部改正を 2020 年 4 月 1 日に施行し、パソコンやスマートフォン等を除く、インターネットに直接接続する機能を有する IoT 機器に対する規制を強化して、以下の各機能の実装を必須とした。

①電気通信機能の設定変更に対するアクセス制御機能（ID・パスワードを用いた利用者認証等）を有すること。
②アクセス制御のための認証情報の初期設定値からの変更を促す機能若しくはそれに準ずるものを有すること。あるいは、あらかじめ機器ごとに異なる初期設定値が付されていること若しくはこれに準ずる措置が講じられていること。なお、取扱説明書等に初期設定値の変更を促す記載をするだけでは不可。
③ファームウェアの更新機能を有すること。
④端末への電源供給が停止した場合でも、機能①及び機能③と当該機能により設定された機器の状態を維持すること。

（b）カリフォルニア州における法規制の施行開始

米国カリフォルニア州では、2018 年 9 月 28 日に 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法案 SB-327（Senate Bill No.327）※195、通称「IoT セキュリティ法」が成立しており、2020 年 1 月 1 日に施行が開始された。インターネットに直接的または間接的に接続する機器には、不正アクセス、破壊、不正利用、改ざん、情報漏えいから保護するための「合理的な」セキュリティ機能の実装が必須となった。IoT 機器が外部ネットワークからの認証機能を備えている場合、以下のいずれかを満たしていれば、合理的なセキュリティ機能と見なすとしている。
①事前にプログラムされたパスワードは、製造する機器ごとに異なること。
②機器への初めてのアクセスを許可する前に、利用者に新しい認証情報の生成を強制するセキュリティ機能を有すること。

公開機関・団体	公開資料名	対象読者と主な内容	公開年月
IPA	入退管理システムにおける情報セキュリティ対策要件チェックリスト※175	・調達者、運用者 ・対策要件、対策方法	2019 年 5 月
	脆弱性対処に向けた製品開発者向けガイド※176	・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 7 月
JPCERT/CC	IoT セキュリティチェックリスト※177	・IoT システム・機器の開発者、利用者 ・開発時の確認項目、利用時の確認項目	2019 年 6 月
	IoT セキュリティチェックリスト利用説明書※177	・IoT システム・機器の開発者、利用者 ・チェックリストの利用方法	
	IoT セキュリティチェックリスト解説図※177	・IoT システム・機器の開発者、利用者 ・セキュリティ機能の目的・説明	
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）	製品分野別セキュリティガイドライン スマートホーム編 1.0 版※178	・住設機器の設計者、開発者、生産者、提供者、運用保守担当者、スマートホームの設計者、生産・施工者、管理者、現場監督者、運用保守担当者 ・各ライフサイクルにおいて考慮すべきセキュリティ対策の方針	2019 年 10 月
	IoT 分野共通セキュリティ要件ガイドライン 2019 年版 Ver.2.0※179	・IoT 機器のサーティフィケーションプログラム（「3.2.3（3）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 2 月
一般社団法人日本クラウドセキュリティアライアンス（CSA-JC：Cloud Security Alliance Japan Chapter）	CSA IoT セキュリティコントロールフレームワーク 利用ガイド※180（2019 年 3 月公開英語版の翻訳）	・IoT システムの設計者、開発者、評価者 ・フレームワークスプレッドシートを用いた IoT システムの評価・実装方法	2019 年 11 月
	CSA IoT セキュリティコントロールフレームワークスプレッドシート※181（2019 年 3 月公開英語版の翻訳）	・IoT システムの設計者、開発者、評価者 ・IoT システムの評価・実装に利用可能なセキュリティコントロール	
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※182	・IoT を利用・導入する一般企業 ・各段階において検討・考慮すべき項目	2020 年 2 月
一般社団法人デジタルライフ推進協会（DLPA：Digital Life Promotion Association）	ご家庭で Wi-Fi ルーターをより安全にお使い頂くために※183	・Wi-Fi ルータの利用者 ・推奨利用方法	2019 年 12 月

■表 3-2-16　2019 年以降に国内で新規公開・改訂された IoT 関連のセキュリティガイド等
（出典）各団体の公開情報を基に IPA が作成

(c) 英国政府による法規制の公表

2020 年 1 月 27 日、英国政府は、デジタル・文化・メディア・スポーツ省（Department for Digital, Culture, Media & Sport）が作成した計画に従って、英国内で販売されるすべての消費者向けスマートデバイスに以下の三つの厳しい IoT セキュリティ要件を満たさなければならない、と発表した※196。

①インターネットに接続するすべての消費者向け IoT 機器のパスワードは一意であり、共通の工場出荷値にリセットできないようにすること。

②消費者向け IoT 機器の製造者は、誰もが脆弱性を報告できるように窓口を提供し、迅速に対応すること。

③消費者向け IoT 機器の製造者は、店頭またはオンラインのいずれかにおいて、販売時点での機器向けセキュリティ更新の最低限の提供時間を明示しなければならない。

(3) 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。

- 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、すべての IoT 機器が最低限守るべき 11 項目のセキュリティ要件※179 を定めて、2019 年 10 月から会員企業を対象としたサーティフィケーションプログラムを開始した※197。CCDS がマークを付与した製品には、保険会社による IoT サイバー保険が自動付帯される。
- 2020 年 3 月、セキュリティベンダから、家庭内ネットワークにつながるスマート家電の安全性を診断する無償のスマートフォン用アプリケーションの配布が開始された※198。

公開機関・団体	公開資料名	対象読者と主な内容	公開年月
NIST（National Institute of Standards and Technology：米国国立標準技術研究所）	DRAFT Considerations for a Core IoT Cybersecurity Capabilities Baseline※184	・IoT 機器の製造者、ベースラインを開発するコミュニティ ・IoT 機器のセキュリティ機能のコアとなるベースライン候補	2019 年 2 月
	NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks※185	・IoT 機器の導入に伴い生じるサイバーセキュリティとプライバシーのリスク管理担当者 ・リスクを軽減するための対策例	2019 年 6 月
	DRAFT NISTIR 8267: Security Review of Consumer Home Internet of Things (IoT) Products※186	・家庭用 IoT 機器の製造者 ・開発時に考慮すべき事項	2019 年 10 月
	NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers※187-1	・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※187-2	・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
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）	IoT Security Standards Gap Analysis※188 IoT のセキュリティ標準のギャップ分析※189（IPA による日本語訳）	・IoT セキュリティ標準の開発者 ・IoT におけるセキュリティ・プライバシーの要件と既存の標準との対応	2019 年 1 月
	Good Practices for Security of IoT - Secure Software Development Lifecycle※190	・IoT ソフトウェア開発者、インテグレータ、プラットフォーム・システムエンジニア ・IoT ソフトウェア開発のすべてのフェーズにおけるセキュリティ上の懸念や考慮すべき重要なポイント	2019 年 11 月
	ENISA good practices for security of Smart Cars※191	・自動車製造業者、自動車部品提供者、アフターマーケット提供者 ・グッドプラクティスとセキュリティ対策	2019 年 11 月
ETSI（European Telecommunications Standards Institute：欧州電気通信標準化機構）	ETSI EN 303 645 v2.1.1 (2020-06): CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements※192	・コンシューマ向け IoT 製品の開発者・製造者 ・セキュリティの基礎	2019 年 2 月（v1.1.1） 2020 年 6 月（v2.1.1）

■表 3-2-17　2019 年以降に海外で新規公開・改訂された IoT 関連のセキュリティガイド等
（出典）各団体の公開情報を基に IPA が作成

3.3 次代を担う青少年を取り巻くネット環境

現代の青少年は、インターネットを介した様々なサービスを活用するデジタルネイティブ世代である。インターネットの利便性を享受する一方で、インターネットを介して犯罪に関わってしまうケースも少なくない。

本節では、インターネット環境の最新動向とそこに潜む脅威について述べ、特に犯罪への関与をどう防ぐべきかを考察する。また、青少年自身だけでなく、見守る側の留意点についても目を向ける。

3.3.1 18歳成年

2022年4月1日から成年年齢が18歳に引き下げられる。これによって、18歳になれば親の同意を得ずに携帯電話を契約したり、クレジットカード作成の申請をしたりと、様々な契約行為が可能となり、責任能力を有する者と判断されることになる。

現在、未成年者でもプリペイドカードを利用したチャージ等により、スマートフォンでの支払いができる。今後、クレジットカードを所有すれば支払い可能な額が増え、電子決済アプリと連動させることによって、利用の幅が一層広がる。

しかし、その一方で、自らの就労によって報酬を得る経験が十分ではなく、普段はお金の価値を考えることが少なかった青少年が、身近なスマートフォンを介したクレジットサービスを利用することで、トラブルに巻き込まれる危険もある。成人としての責任が伴うことを念頭に置いた慎重な利用が望まれる。主な注意点として、以下が挙げられる。

- スマートフォンやアプリのセキュリティ対策
- インターネットショッピング等のトラブル対策
- 使い過ぎの防止　等

(1) スマートフォンやアプリのセキュリティ対策

まず、セキュリティ対策では、パスワードの設定と管理が重要となる。スマートフォンは持ち歩いて、外出先で使用する機会が多い。その際に気を付けたいのが、盗難、置忘れである。

警視庁によると、2019年中の遺失届のうち携帯電話類は24万7,771件[※199]に上っており、外出先でスマートフォンを紛失するケースは少なくない。パスワードを設定していない場合は、拾った人間にスマートフォンで決済されてしまい、金銭的被害が発生する危険がある。パスワード設定等の対策を怠らないように心がけたい。

また、他人が勝手に使用しないように、アプリ自体にロックをかけられる決済サービスもある。指紋認証等の生態認証やパスワードの設定で不正利用を回避できるため、積極的な利用が望まれる。ただし、スマートフォン自体と決済アプリのパスワードが同じでは、ロックが一つであるのと変わらない。決済アプリのみならず、利用している様々なサービスも含め、パスワードの使い回しを避けることは対策の基本である。IPAが公開するパスワードに関する情報[※200]等を参考に、設定を今一度見直していただきたい。

QRコードを読み取ることで手軽に支払いできるQRコード決済サービスを悪用した「偽装QRコード」による詐欺や、「7pay（セブンペイ）」の不正利用事案、Paidyを使った詐欺等も発生しており、便利さの裏側には危険が潜んでいることを、改めて認識する必要がある。

マカフィー株式会社は、スマートフォンを利用して決済する際の注意点をまとめており（図3-3-1）、また、トレンドマイクロ株式会社も「スマホ決済を安全に利用するために確認したい7つのポイント[※201]」を公開した。このような資料を参考にし、被害に遭う前に、スマートフォン決済のリスクについて家族で話し合うことが望まれる。また、オートチャージ機能を使わず、残高が減った都度、現金でチャージする等のルールを決めることで、お金を支払っているという意識付けができる。詐欺の手口の情報にアンテナを張り、他人事ではなく、自分にも降りかかる問題として意識を向けることが重要である。

■図3-3-1　増える「Pay」――スマホ決済の注意点
（出典）マカフィー株式会社「増える「Pay」――スマホ決済の注意点[※202]」

(2) インターネットショッピング等のトラブル対策

PIO-NET（全国消費生活情報ネットワークシステム）[※203]の情報を基にしたレポートによると、青少年（小

学生・中学生・高校生）のインターネットショッピング等のトラブルとして最も多かったのは、オンラインゲームに関するものである（表 3-3-1）。「保護者に内緒で課金をしていた」等がその代表例である。中高生の相談では、健康食品や化粧品等の相談が上位を占め、商品が届かなかったり、偽物が届いたりというトラブルが発生している。

インターネット上では、通常の買い物とは比べ物にならない程、多数の商品が視界に入ってくること、また、直接現金による支払いが生じないことから、必要以上に購入してしまうことがある。クレジットカードや電子決済でも、最終的にはお金を支払っている、という仕組みを、周囲の大人が指導しなければならない。また、現物がなくても、商品の画像と文字情報を表示すれば、売買ができるように見せかけることができるため、インターネット上には、悪意を持った業者も存在している。購入の際には、本当に実在する会社なのか、所在地や電話番号等の連絡先や、代表者名が記載されているかどうかを確認することは、最低限の対策と言える。

全体		6,654
1	オンラインゲーム	1,713
2	アダルト情報サイト	1,068
3	健康食品	881
4	デジタルコンテンツその他	800
5	化粧品	657
6	紳士・婦人洋服	187
7	商品一般	146
8	靴・運動靴	145
9	コンサート	128
10	出会い系サイト	102

■表 3-3-1　契約当事者が小学生・中学生・高校生の電子商取引に関する相談における上位商品・役務等（2018 年度、単位:件）
（出典）独立行政法人国民生活センター「オンラインゲーム、アダルトサイト、健康食品・化粧品の定期購入、SNS きっかけも 家族で防ごう!子どものネットトラブル※204」

(3) 使い過ぎの防止

ゲーム課金の例にあるように、現金がなくても簡単に支払いができることによる使い過ぎの恐れは、大人にも子どもにもある。

一般社団法人日本クレジット協会の Web ページ※205では、クレジットの仕組みや支払計画を立てることの必要性や、インターネットで利用する際の注意点等を学ぶことができる資料を公開している。日頃からこのような資料を使って、保護者を中心とした周囲の大人達もともに学んだり、お金にまつわる経験を話したりして、子ども達の自己管理意識を育てることも必要になっている。また、毎月の利用明細を基に、各支払い項目の有用性を評価することで、無駄遣いの可視化と防止が期待できる。

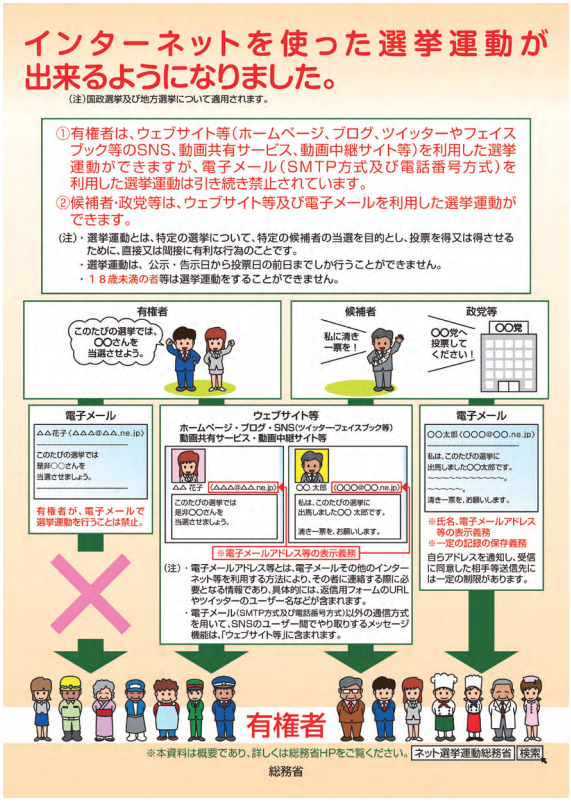
現時点では、クレジットカード会社の規約により高校生がクレジットカードを所有することはないものの、18 歳成人に向けて、商品や出店企業等の情報の見極めや、支払いの慎重さを意識する機会を青少年が得られるよう、周囲の大人の働きかけが求められる。

3.3.2 インターネットと選挙

成年年齢引き下げに先駆けて、改正公職選挙法が 2016 年 6 月に施行され、選挙権年齢が満 18 歳以上に引き下げられた。これにより、18 歳になれば、高校生も投票及び選挙運動が可能となった。

また、インターネットの普及を背景に、Web サイト、SNS、インターネット動画共有サービス等を用いた選挙運動が解禁されている（図 3-3-2）。しかし、18 歳がインターネット上で選挙運動を行う際には注意が必要である。

例えば、高校 3 年生は、18 歳と 17 歳が大多数を占める。18 歳以上であれば、SNS を使って候補者を支援するメッセージを発信できるが、その SNS でつながる同じクラスの 18 歳未満が同様の発信を行うと、公職選挙



■図 3-3-2　インターネットを使った選挙運動
（出典）総務省「インターネットを使った選挙運動が出来るようになりました。※206」

法違反となってしまう。

18 歳未満は一切の選挙運動が禁止されており、SNS の拡散機能（リツイートやシェア等）によって、情報を広めることも禁止行為とされている。18 歳の有権者が SNS で発信したメッセージを同じクラスの 17 歳が拡散する可能性も考えられ、情報の発信源でなくとも法を犯す危険がある。

更に、公職選挙法第 235 条第 2 項では、候補者に関する虚偽の情報をインターネット等で発信することは「虚偽事項公表罪」として処罰の対象になることが定められている。また、インターネット上であっても名誉毀損罪や侮辱罪、脅迫罪は適用される。

インターネット選挙運動の解禁は、2013 年と比較的新しい。選挙運動用の挨拶状やポスターのデータ等を電子メールで送信できるのは、候補者や政党等に限定されており、それ以外の人は、例えメールの転送であっても禁止されている。このように、インターネット選挙運動については、大人でも認識しなければならない内容もあり、高校生への教育支援はもちろん、大人もともに学ぶ環境が必要とされている。

3.3.3 SNSを介した犯罪

SNS に投稿されている情報は、決して楽しいものだけではなく、犯罪への入り口が潜んでいることがある。

警察庁の発表によると、2019 年の特殊詐欺に関係する検挙人員は 2,861 人、このうち少年の検挙人員は 619 人となり、特殊詐欺全体の検挙人員の 21.6%を占めた※207。

このような状況下において、2019 年 8 月、愛知県警察※208 は SNS 上に投稿されている特殊詐欺の実行犯役募集に対し、全国初となる取り組みを実施した。これは、ツイッター上の実行犯役募集に関連すると思しき投稿に「あなたの人生を台無しにします‼」等の警告を返信するものである。1 日約 1,000 件を数えるこうした特殊詐欺の実行犯役募集の投稿に、青少年は「小遣い稼ぎのアルバイト」という感覚で応募してしまうようだが、詐欺罪に問われれば 10 年以下の懲役刑が科せられる、ということを認識する必要がある。

大阪府では、ツイッター等の SNS を通じた募集によって、軽い気持ちで犯罪に加担している青少年が増えているとして、特殊詐欺被害防止啓発漫画を作成し公開した（図 3-3-3）。これは、大阪アニメーションスクール専門学校の協力によって作成されたもので、主人公が、SNS 上で高収入をうたったアルバイト募集の情報を見つける様子や、一度特殊詐欺に手を染めると抜けられなくなる手口が具体的に示されている。こうした啓発漫画の利活用による犯罪抑止が期待される。

■図 3-3-3　闇バイト（受け子）
（出典）大阪府「特殊詐欺被害防止啓発漫画を作成しました※209」

2021 年に延期が決定※210 した東京 2020 オリンピック・パラリンピック競技大会では、選手を始め、ボランティアを含む大会関係者が会場に入場するための本人確認として、顔認証システムが導入される。これによって不正な入場を防止するとともに、確認の自動化による混雑の緩和が期待されている。「顔」のデータがセキュリティと利便性向上に活用される例である。

一方で、SNS に投稿された写真を悪用した以下のストーカー事案が発生し、男が逮捕されている。

アイドル活動をしている女性が自宅近くの駅で自撮り画像を撮影し、それを SNS 上で公開した。この画像にはその駅がどこであるのかを判別する情報は映っていなかったとされている。しかし、その女性の「瞳」には、駅の景色が映っており、男は、その画像を基に駅を特定して待ち伏せする等のストーカー行為をはたらいた。このよ

うに、「顔」の画像は重要な個人情報であり、SNS 等に安易に公開することで、思わぬ事件を引き起こしてしまう危険がある。

13 歳から 19 歳の青少年のスマートフォン個人保有率は 79.5%※211 となり、多くの子ども達が自分のスマートフォンを自由に使える環境となっている。そのスマートフォンで撮影された顔写真がインターネット上に公開されることも少なくない（一般利用者の顔写真公開に対する意識については「2.4.4(3)SNS 利用におけるリスクの認識状況」参照）。

子ども達には、簡単に画像を共有できる SNS は便利で楽しいツールであるが、共有する内容に個人情報が含まれている場合には、大きなリスクが伴うことを意識付けたい。また、子どもの個人情報は、保護者であっても安易に公開して良い、というものではないことを認識する必要がある。

3.3.4 不確かな情報

2019 年 8 月、高速道路で悪質なあおり運転を行った上、あおった相手の男性を殴るという事件が発生した。この事件では、あおり運転をしていた自動車の同乗者に似ているとして、まったく関係のない女性が SNS 上で犯人扱いを受け、名誉を傷つけられる事案が起きた。「自首して」等の書き込みに加え、名前や写真までも公開される事態に発展している※212。

このように、思い込みによって真偽の不明な情報を拡散させ、新たな被害者を生み出してしまうことがある。また、拡散することが被害の拡大を助長し、結果的に加害者に加担してしまうようなケースも考えられる。

警視庁は「不確かな情報に惑わされないために」と題した Web ページを公開し、情報の真偽を判断するためのヒントを公開している（図 3-3-4）。ぜひ活用していただきたい。

特定非営利活動法人 IT サポートさがが制作した情報モラル啓発動画「正義感で大誤爆　－ SNS 投稿トラブル編－※214」では、災害発生に便乗して、SNS 上に虚偽の情報を投稿した高校生を、懲らしめようとする女子高校生が描かれている。虚偽情報の発信者だと信じて女子高校生が取った行動によって、新たな被害者が生まれることを予感させる展開となっている。

このような不確かな情報が作り出されたり、拡散されたりと増加する中、情報の検証を行い、誤情報の拡散を防ぐ仕組みの構築を目指す組織として、特定非営利活動法人ファクトチェック・イニシアティブ（FIJ：FactCheck Initiative Japan）が発足した。FIJ は世の中に出回る情報についての真偽を検証し、正確な情報を広く共有する活動を行っている(図 3-3-5)。

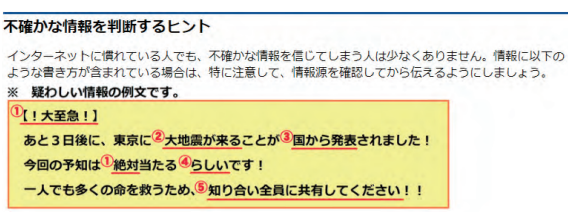
このように検証された情報を活用すれば、誤った情報に振り回されず、また、自分自身が拡散する側になることを防ぐことが期待できる。子ども達だけではなく、インターネットを利用するすべての国民による活用が望まれる。

■図 3-3-5　新型コロナウイルス特設サイト
(出典)FIJ「新型コロナウイルス特設サイト※215」

前述の高速道路あおり運転の事件では、弁護士が「虚偽の情報を広める者には法的措置を検討する」とデマ情報を流された女性が経営する会社のホームページ上に声明文を出し、その後、民事訴訟を提起している。

SNS は、誰もが気軽に投稿できる便利なツールである。しかし、投稿前に内容の虚実をチェックする機能はない。これは、インターネット上の情報の真偽は誰も保証していない、ということを意味する。不確かな情報の発信・拡散は、自らの立場を危うくすることがある。また、新型コロナウイルス感染症（以下、新型コロナウイルス）にまつわるデマのように、誤った予防策※216 を広めることで、必要な対策が疎かになり、多くの人の命に関わることも考えられる。

情報が拡散することの影響力を念頭に置き、また、FIJ による情報を参考にする等、ネットの情報に振り回されず、冷静に判断する、という意識が重要である。


不確かな情報を判断するヒント

インターネットに慣れている人でも、不確かな情報を信じてしまう人は少なくありません。情報に以下のような書き方が含まれている場合は、特に注意して、情報源を確認してから伝えるようにしましょう。

※　疑わしい情報の例文です。

①【！大至急！】
あと３日後に、東京に②大地震が来ることが③国から発表されました！
今回の予知は①絶対当たる④らしいです！
一人でも多くの命を救うため、⑤知り合い全員に共有してください！！

■図 3-3-4　不確かな情報を判断するヒント(一部)
(出典)警視庁サイバー犯罪対策課「不確かな情報に惑わされないために※213」

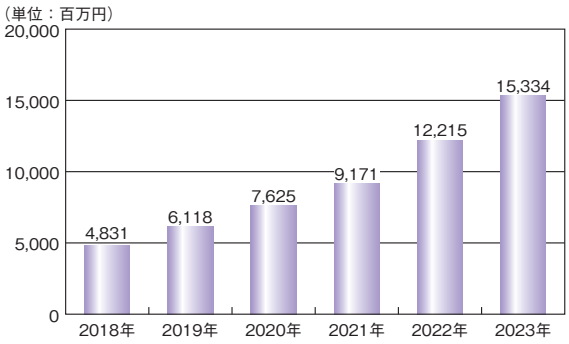
3.3.5 eスポーツとオンラインゲーム

eスポーツは、インターネットを介して世界中のプレイヤーがコンピュータゲームで対戦する競技である。世界大会も開催され、最も大きな大会の一つであるIEM Katowice 2019の3Dアクションゲーム「カウンターストライク：グローバルオフェンシブ」を用いた試合では、全世界の約1億9,500万人がオンラインで観戦し、また、ポーランドの会場には、17万人を超える観戦者が訪れた[※217]。

日本では、2018年に一般社団法人日本eスポーツ連合が設立され、また、プロリーグが発足した。株式会社KADOKAWA Game Linkageの発表によると、2019年にeスポーツを観戦したり、動画を視聴したりした人は約483万人であり、2023年には約1,215万人に増加すると予測されている[※218]。

2019年には、「いきいき茨城ゆめ国体」の文化プログラムの一環として「全国都道府県対抗eスポーツ選手権2019IBARAKI[※219]」が開催された。小学生の部、一般の部（12歳以上）の2部門があり、8歳の小学生も参加した。eスポーツは、今後の成長分野の一つとして期待されており、2023年には約150億円規模に成長すると見込まれている（図3-3-6）。

このような状況を背景に、経済産業省は2019年9月より、一般社団法人日本eスポーツ連合とともに「eスポーツを活性化させるための方策に関する検討会」を開催した[※220]。



■図3-3-6　日本eスポーツ市場規模推移
（出典）株式会社KADOKAWA Game Linkage「2019年 日本eスポーツ市場規模は60億円を突破。[※218]」を基にIPAが編集

eスポーツ市場が成長する一方で、サイバー犯罪者による攻撃も確認されている。

2019年、全世界のプレイヤー人口が約2億5,000万人[※221]と推計されるオンライン対戦ゲーム「フォートナイト（Fortnite）」のユーザが、「Syrk」と呼ばれるランサムウェアの標的となった。ユーザは、ゲームを有利に進めるために不正等を行うチートツールを装うSyrkによって、コンピュータに保存されているデータファイルを暗号化され、身代金を要求される。

また、NEXON Co.Ltd等のゲーム事業者を装って「アカウントに重大な問題が起きたため、パスワードの変更が必要」等のメッセージとともに偽サイトへ誘導するURLを送信するフィッシングの手口もあり、ID・パスワードやクレジットカード情報等を窃取される危険も出てきた。

こうした脅威に対処するための例として、トレンドマイクロ株式会社が公開した「オンラインゲームを安全に楽しむための10のポイント」がある（図3-3-7）。これらのポイントは「チャット内のURLリンクを不用意に開かない」「アカウントを厳重に管理する」等、オンラインゲームに限らない項目であり、インターネット使用時の一般的な注意点と共通している。

■図3-3-7　オンラインゲームのアイテムを盗まれる!?
（出典）トレンドマイクロ株式会社「オンラインゲームのアイテムを盗まれる!?[※222]」

また、青少年がオンラインゲームに費やす時間等をコントロールできなくなるゲーム障害も懸念されている。

WHO（World Health Organization：世界保健機関）は、2019年、ゲーム障害を国際疾病として認定した。時間等の制御ができず、ゲームを最優先することによって、日常生活に問題が起きているのに改善することができない、等の状態が12ヵ月以上続く場合、ゲーム障害と診断される可能性がある[※223]。

依存治療研究部門を設ける独立行政法人国立病院機構久里浜医療センターのゲーム障害患者は、約70%が未成年者だという。保護者等、周囲の人が、時間管理や生活向上のために必要なことについて、話し合いを持つことが重要だとしている[※224]。

3.3.6 生徒・大学生による啓発活動

青少年による、安全なインターネット利用のための普及啓発活動が行われている。IPA の「ひろげよう情報モラル・セキュリティコンクール」において文部科学大臣賞を受賞した南阿蘇村立南阿蘇中学校では、生徒会執行部が中心となり、情報通信機器の利用に関するルール作りを行った※225。「生活面」「モラル面」「学習面」等の項目について、通信機器の利用時間や個人情報の取り扱いに注意すること等を定めている。

九州の大学を中心とした学生ボランティアによって構成される福岡県警察サイバーパトロールモニタは、インターネット上をパトロールし、違法情報等の発見に努めている。また、SNS を活用した広報啓発を行う等、安全なサイバー空間の実現に向けた活動を行っている※226。

明治大学では、「明大 SNS スタイル」と題した漫画をホームページに掲載した。就職活動中に SNS 上に書き込んだ面接官の批判内容が、どのような影響をもたらすのかや、友達の写真を安易に公開することのリスクを分かりやすく説明し、学生に SNS 利用時の注意として呼び掛けている（図 3-3-8）。

■図 3-3-8 明大 SNS スタイル 学生生活編
（出典）明治大学「明大スタイル（SNS 利用時の注意）※227」

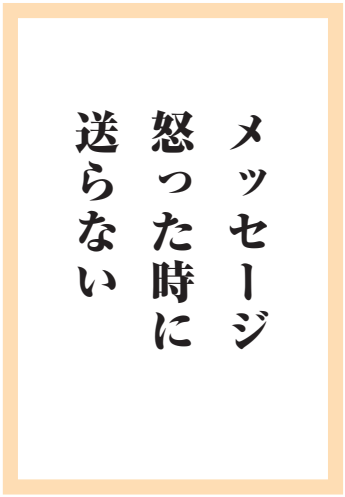
3.3.7 青少年の育成と共生に向けて

一般社団法人セキュリティ・キャンプ協議会事務局は、セキュリティ・ミニキャンプと称して、全国各地において情報セキュリティ人材の育成等を目的とした講座を開催している。25 歳以下の生徒・学生が参加でき、青少年にとって、遠方に行かずとも専門的な講義を受けるチャンスとなっている。また、セキュリティ・キャンプ全国大会では、倫理やモラル意識を重視し、生活を豊かにするために技術を活かす意識の醸成を目的とした講演や、コミュニケーション力の向上を目指したグループワークも実施する。技術や知識に限定せず、将来、社会で活躍できる青少年を育てる活動が行われている。

2019 年における日本の 15 歳未満の人口比率は 12.1%※228 と過去最低となった。65 歳以上の人口比率が 28.4% であることと比較しても、14 歳までの子どもは「少数派」であることが分かる。はたして、「多数派」である大人は、「少数派」の子ども達を理解できているだろうか。

前述の「ひろげよう情報モラル・セキュリティコンクール」において優秀賞（図 3-3-9）を受賞した小学生が、作品に込めた思いとして次のように述べている。

「SNS で送ったメッセージは、相手にいつまでも残ります。自分がイライラしている時や相手に怒っている時に送信すると、怒った時の自分が保存されてしまいます。すぐに伝えられる方法だからこそ、間をおいて考える時間をもつことが大事なことだと思います。」



■図 3-3-9 第 14 回「ひろげよう情報モラル・セキュリティコンクール」受賞作品
（出典）IPA「標語部門※229」

「怒った時の自分が保存されてしまう」と表現する感性を持ち合わせる大人は多くはないだろう。子どもは子どもなりに、自分の感情や周囲の状況を把握しており、インターネットを利用する際に配慮すべき点に気づいているだろうことが作品からも読み取れる。

デジタルネイティブな子ども達にとって、スマートフォンや SNS が果たす役割の重みは、大人とは異なっているように見える。子ども達と同じようにインターネットを利用する大人は、子ども達の手本となっているのか、今一度振り返り、襟を正したい。

SNS を活用して「少数派」とみられていた人々が声を上げ、状況を改善する行動も可能となっている。

日本航空株式会社は、女性客室乗務員が着用する靴のルール「3 ～ 4cm のヒールがあるパンプス」を撤廃した※230。これは、SNS のハッシュタグ「#KuToo」による発言も後押ししたと見られており、「少数派」も SNS で声を集約することで、大きなムーブメントを起こせることが分かる。これは、大人が示した SNS 利用の好例と言えよう。

しかし、他方では大人達が、SNS 上に特定の人物の存在そのものを否定するような誹謗中傷を書き込み、死に追いやるという悪用も発覚している※231。青少年による「ネットいじめ」の問題を議論してきた大人達だが、はたして、子ども達の悪い手本とならないような行動をとってきただろうか、と猛省し、これを教訓とする機会としたい。私達は、通信技術の発達と浸透によって、とてつもなく多くの情報に触れることができるようになった。これは、多様な意見、立場、環境があることを知る機会が増えたことでもある。

大人は、自分達がこれまで経験してきたものの見方や行動を見直し、若者や「少数派」との違いを受け入れて共生することによって、より一層豊かな社会を子ども達とともに目指す必要があるのではないだろうか。

COLUMN

見せかけと見映えと本当に大切なこと

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。「まもりの国」に住んでいます。今回は、「見せかけ」と「見栄え」と「本当に大切なこと」について、ぼくが感じたことをお話しします。

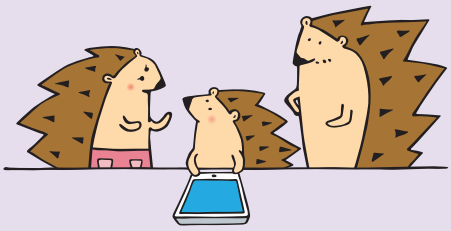
ぼくは、インターネットのゲームが大好きです。会ったことがない人と仲間になって一緒に戦ったり、購入したアイテムで敵を倒したりして、レベルもどんどんアップする。だから止められない！　この前は、お父さんに注意されたんだけど、みんなで戦っていたときだったから、ぼくだけ勝手に抜け出せなくて、ついつい遅い時間になっちゃった。こんなぼくは、近頃あまり予習復習をしなくなっていて、先週のテストではなんと 47 点しか取れなかったの。そうしたら弱い自分がでてきて、悪いことを考えてしまいました。「あーあ。叱られちゃうといやだな。テストの点数をこっそり変えられないかな」と。

そんなとき、隣の国で「学校の先生用のサーバに生徒がこっそり入り込んで、自分の成績を変更した」という事件が起きました。このニュースを見て、お父さんがぼくにこう言ったんだ。「悪いことをして成績がいいように見せかけても、事実は変わらない。そんなことをするより、成績が悪かった自分をちゃんと認めて、次にどうするかを考えたほうがいい。それに、素直に悪い成績を見せてくれたら、家族も一緒に対策を考えて応援することができるよね」

これを聞いてぼくは、はっとしたよ。テストの点数が悪かったのはぼくが授業の内容を覚えていなかったから。テストの点数を書き換えたって、ぼくの知識が増えるわけじゃない。「それに、ゲームでは地位や強さをお金で買えるかもしれないけど、現実はそうはいかない。いくらお金を払っても事実より高い評価は買えないんだ。本当の自分がどんな人間なのか、自分をごまかさず真実を見なければいけないね」　そうか、どんどん課金して、強力な武器や便利なアイテムを購入したら、敵を打ち負かすことができる。でも、それは、ぼく自身が強くなったんじゃなくて、ゲームのキャラクターが強くなっただけなんだね。

それから、「映え」を狙って写真を撮るだけのために、食べきれないメガ盛りや嫌いなものが入っていても見映えの良い料理を注文する人がいる、っていう話も学校で聞きました。見せかけの楽しさや美しさばかりを追求して、本来の「食べ物を食べる」ということをしない人がいることで、せっかくの料理を捨ててしまうことがあるみたい。心を込めて作った料理を残してしまう人は来ないでね、って SNS に投稿したお店も出てきているんだって。食べ物をいただくってことは、その食材の命をいただくっていうこと。写真を撮るだけでその命を捨ててしまうことは、やっぱりしてはいけないことだよね。

物事には「本質」というものがあって、それを見誤ってはいけないって、お父さんが教えてくれました。「何のために勉強するのか、食事をする意味は何なのか。ネットで見栄を張ったり情報をごまかしたりするのは『本質』を忘れた行為だ」って。ぼくは「本質」を見失わずに生きていきたいと思いました。



IPA コンクール応援隊長「まもるくん」

3.4 クラウドの情報セキュリティ

近年、企業・組織において、オンプレミスシステムからIaaS（Infrastructure as a Service）への移行に加え、PaaS（Platform as a Service）/SaaS（Software as a Service）の業務利用が急速に進んでいる。一般社団法人日本情報システム・ユーザー協会（JUAS：Japan Users Association of Information Systems）の「企業IT動向調査報告書2020[※232]」によれば、967社を対象とする調査において、パブリック・クラウド（SaaS）を「導入済み」と回答した企業が60.4%、パブリック・クラウド（IaaS・PaaS）を導入済みと回答した企業が49.2%となり、クラウドの導入が進みつつある傾向がみられるという。また総務省の「令和元年通信利用動向調査[※233]」によれば、従業員100人以上の企業2,122社について、クラウドサービスを導入していると回答した割合は64.7%で、同調査で初めて6割を超えた（平成30年度調査では58.7%）。

政府のクラウド利用については、2018年6月7日、「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」が公開され、クラウド・バイ・デフォルト原則が明示された[※234]。また2020年6月11日、政府調達に参画するクラウド事業者のセキュリティを担保するため、「政府情報システムのためのセキュリティ評価制度（ISMAP：Information system Security Management and Assessment Program）[※235]」が開始された（「2.1.2（2）政府情報システムのためのセキュリティ評価制度（ISMAP）」参照）。

一方、個人についても、SNS、コンテンツ視聴、パソコンやスマートフォンにおけるデータの保管、オンラインショッピング等、多くのサービスにおいて、それとは意識せずにクラウドを利用している。更に2020年3月以降、新型コロナウイルス対策でテレワーク等の新しい働き方が求められる中、クラウドの情報セキュリティは国民全体のIT利用の可否を左右する重要課題となっている。

本節ではクラウドのセキュリティについて、脅威の実態、クラウドセキュリティの技術面・マネジメント面の課題、とるべき対策の各観点から整理を行う。

3.4.1 クラウドサービスのインシデント、被害の実態

表3-4-1に2019年度に発生したクラウドサービスに関するインシデントの起因別の分類を示す。障害の発生に伴い、サービスの継続に不具合が生じたものと、サービスからの情報漏えいが生じたものに大別している。2019年は、大手クラウドベンダの大規模な障害や、復旧までに時間を要する障害の発生が目立った。起因としてはシステムの変更に関する設定ミス等が多くみられた。主なインシデントについて以下に述べる。

サービス障害	(1)システムバグ	制御システムのバグによるサーバのオーバーヒート
	(2)システム設定更新・機能更新不備	(a) 設定更新不備
		(b) 機能更新不備
	(3)システム故障	ストレージの故障
情報漏えい	(4)設定ミスの悪用	WAFの設定ミスに付けこまれた不正アクセス
	(5)情報提供先での管理不備	情報提供先での情報管理ミス
	(6)不正アクセスとデータ保護の不備	クラウドサーバへの不正アクセスとデータ暗号化の不備

■表3-4-1　2019年に発生したクラウドサービスに関係するインシデントの起因別分類

(1)システムバグに起因するインシデント

2019年8月、Amazon Web Services（AWS）の東京リージョンにおいて、オーバーヒートによりサーバが停止した。復旧までに約10時間を要し、決済系（PayPay等）、SNS（mixi、ピグパーティ等）、サービス（楽天株式会社のラクマ、スターバックスコーヒージャパン株式会社等）、ECサイト（株式会社ユニクロ、株式会社東急ハンズ等）等のテナントサービスで接続不可、ログイン障害、サービスが利用できない等の障害が発生した[※236]。データセンターの冷却システムの制御と最適化に使用される制御システムがバグで応答しなくなり、一部の冷却システムが停止し、オペレータが手動で操作をしたが、空調ユニットを制御するPLC（Programmable Logic Controller）が一部応答せず、オーバーヒートが発生してサーバの停止に至ったとされた。

アマゾンジャパン合同会社は、この制御システムのバグについてシステム供給事業者と協力して調査するとともに、今回のような不具合が再び発生した場合に速やかに対応できるようにオペレータをトレーニングした、としている[※237]。

(2) システムの設定・更新不備に起因するインシデント

システムの設定不備、機能更新不備に起因するインシデント事例を紹介する。

(a) 設定更新不備

2019 年 5 月、Microsoft Azure、Office 365/Microsoft 365 や Microsoft Dynamics 等、Microsoft Corporation（以下、Microsoft 社）のクラウドサービスに対して、ほぼ世界的に約 3 時間にわたり接続できなくなる障害が発生した。データセンターのメンテナンス作業において、Azure Storage や Azure SQL Database 等を含む複数のサービスへのアクセスに使用される DNS ゾーンのネームサーバの設定変更を誤ったことが原因とされた。Microsoft 社は、同様な障害を防ぐための施策として、メンテナンス作業におけるチェック体制の追加、実行前モデリングによる設定変更後の結果予測、問題を迅速に検出するためのモニタリングの追加、変更の影響を更に小さくするための設計改善等を行うとした。なお、日本では連休中の早朝だったこともあり、影響は大きなものではなかった[※238]。

2019 年 6 月、米国で約 4 時間にわたり、Google Cloud の Compute Engine や Cloud Storage、更にその影響を受けた YouTube や G Suite 等のサービスの応答が遅い、利用できない等の障害が発生した。Google Cloud のオペレータがサーバの設定変更を誤り、単一リージョン内の数台のサーバに対する設定変更のつもりが、隣接する複数のリージョンの多数のサーバに対しても設定変更が適用され、ネットワークで輻輳が発生したことが原因とされた。

Google LLC（以下、Google 社）は発生した輻輳の要因と復旧に時間がかかった要因等を改めて分析し、今後の対応に活かすとしている[※239]。なお本障害は発生した時間帯の関係で、日本への影響は大きなものではなかった[※240]。

(b) 機能更新不備

2019 年 11 月、オーストラリア、日本、インドにおいて約 10 時間にわたり Microsoft Office 365 で提供される Exchange Online でメールが届かない、届くまで時間がかかる、等の障害が発生した。Microsoft 社の調査によると、スパム対策機能の更新が行われた際にメールフローに予想外の影響が発生した可能性があるとして、スパム対策機能更新のロールバックを行うことでサービスを復旧した。

Microsoft 社は影響を受けたシステムのパフォーマンスを分析し、再発を防止するとしている[※241]。

(3) システム故障に起因するインシデント

2019 年 12 月、日本電子計算株式会社が提供する自治体向け IaaS サービス「Jip-Base」でシステム障害が発生した。Jip-Base 上では 70 の団体の業務サービスが稼働しており、サービスを利用する複数の自治体で Web サイトが閲覧できなくなる等の障害が発生した。これらの障害は外部からの攻撃によるものではなく、情報漏えい等の被害はなかったが、二つの不具合が複合的に発生したことで復旧に時間を要した。具体的には、Jip-Base のストレージのファームウェアの不具合に起因したハードウェア故障、及びストレージの復旧後、データへのアクセス処理が正しく動作しないという不具合であった。2020 年 1 月、本障害で影響を受けた 1,318 の仮想 OS のうち 98.1% が復旧したが、復旧できないものに関しては新たな利用環境の構築等を行う等の対応をすることとなった[※242]。

(4) 設定ミスの悪用に起因するインシデント

2019 年 7 月、米国金融機関大手 Capital One Financial Corporation（以下、Capital One 社）への不正アクセスにより、米国で約 1 億人、カナダで約 600 万人を超える社会保険番号や銀行口座番号、カードの支払い履歴等の個人情報が流出した。容疑者はすぐに逮捕され、2015 年 5 月～ 2016 年 9 月の間、Amazon.com, Inc.（以下、Amazon 社）のクラウド部門の従業員であったことが分かった。逮捕者は Capital One 社から窃取した情報を外部と共有するため、自分の Slack チャンネルに窃取した情報のリストを投稿したと主張した。本インシデントの手口は、WAF（Web Application Firewall）の設定ミスを悪用した Server Side Request Forgery（SSRF）攻撃[※243]であった。攻撃を受けた WAF は、Apache HTTP Server で動作するオープンソースの WAF「Mod Security」を採用して、Capital One 社が独自に構築したものであった[※244]。

株式会社ラックの「サイバー救急センターレポート第 8 号[※245]」によれば、国内においても IaaS 利用者の設定不備を突いた攻撃が増加し、注意が必要であるとしている。具体的には、オンプレミスから IaaS へのシステム移行時に利用した検証環境のセキュリティグループ設定等を脆弱なまま放置し、本番環境に移行して不正アクセ

スを許した例が示された。同報告はまた、単純なパスワードを設定する等、認証パスワードの不適切な設定を突いて攻撃される例が多くあるとし、利用者に設定を適切に行うよう呼びかけている。

(5) 情報提供先での管理不備に起因するインシデント

2019 年 4 月、米国の Facebook, Inc.（以下、Facebook 社）のユーザのデータ約 5 億 4,000 万件が、AWS のクラウド上に放置され、ユーザ ID やコメント、「いいね!」をしたか等の情報が外部からアクセス可能となっていたことが分かった。当該データは、メキシコのデジタルメディア企業 Cultura Colectiva が取得したもので、Facebook 社は、Cultura Colectiva のプラットフォーム上で動くアプリケーションの開発会社とのユーザ情報共有を認めていたが、Cultura Colectiva のミスによって、同データが放置されたとみられる。Facebook 社は Amazon 社と連携してデータを削除したとしているが、データがどれだけの期間、外部からアクセス可能になっていたか、第三者による悪用があったか等については明らかになっていない。

Facebook 社は 2018 年 3 月、ケンブリッジ大学の研究用途に提供した API（Application Programming Interface）を介して英国コンサルティング会社に約 8,700 万人の個人情報が流出していたことが発覚、Mark Zuckerberg 最高経営責任者（CEO）は米国下院公聴会において情報管理の徹底を約束した[※246]。このときは顧客情報に関するプライバシー保護の弱さ、データ提供におけるユーザとの合意の妥当性等が問題となったが、後者に関連した情報流出事故がその後も続いている。

(6) 不正アクセスとデータ保護の不備に起因するインシデント

大容量ファイル転送サービス「宅ふぁいる便」のサーバが不正アクセスを受け、運営会社である株式会社オージス総研は 2019 年 1 月 23 日にサービスを停止、翌 24 日に顧客情報が流出したと公表した。同年 3 月 14 日付の同社発表によれば、宅ふぁいる便に用いられる一部サーバの脆弱性を攻撃され、氏名・メールアドレス・パスワード・居住地・生年月日等を含む顧客情報 481 万 5,399 件が流出したという[※247]。事故直後のインシデント公表が迅速であった点は評価されたが、ID・パスワード等を暗号化せずに保存していた点は問題視された[※248]。同社は当初、サービスの再構築を目指し、ユーザサポートも継続してきたが、高コストであるとして同サービスの再開を断念、2020 年 3 月 31 日で終了すると発表した（ただしビジネス向けは継続）[※249]。

(7) インシデント・被害状況の整理

以上のように、近年のクラウドに関係するインシデントは、セキュリティ以外の要因によるサービス遅延・停止と、運用ミスやサイバー攻撃による情報漏えい（運用ミスとサイバー攻撃の複合形態による情報漏えいも含む）の二つに大別される。海外では大規模な情報流出事故が継続しているのに対し、国内ではサービス遅延・停止、漏えいのいずれについても被害は比較的小さく推移している。

サービス遅延や停止については、クラウド基盤システムの可用性の維持についてクラウド事業者が引き続き対策を強化する必要がある。一方で、利用者側も、例えば重要な業務を IaaS/PaaS で構築する場合等の冗長化やバックアップ等、インシデントを想定した対応を検討することも必要と考えられる。

情報漏えいについて見ると、クラウドの設定不備、脆弱性を突いたサイバー攻撃、あるいはその複合形態が原因となっている。クラウドサービス事業者とクラウド利用者がそれぞれの責任分担に基づき、両者が対策を補完的に行うことが必要である。例えば IaaS/PaaS の場合、アプリケーションデータの更新・削除や暗号化、不正アクセス監視等は利用者が実施すべきもので、事業者はそのためのセキュリティ機能を提供することが責任範囲となる。また SaaS の場合、事業者は強い認証機能を提供し、利用者はエンドポイントで ID・パスワードを保護する必要がある。前掲の「サイバー救急センターレポート第 8 号」では、クラウドのアカウント情報の窃取・悪用が増加した、としており、強いパスワードの設定、あるいは多要素認証等の備えが求められる。

更に 2020 年 1 月以降、新型コロナウイルス感染対策としてのテレワーク実施の切迫した要請により、リモート会議システムのセキュリティや情報管理のリスクポイント等を整理できないまま、在宅でクラウドを利用する個人が増えているのではないか、という懸念がある。次項では、この懸念を含めたクラウドのセキュリティ課題について紹介する。

3.4.2 クラウドのセキュリティ課題と対応

企業がクラウドを利用する上で、セキュリティ上の課題として近年注目、検討されている事項を技術面、マネジ

メント面に分けて概観する。

(1)技術面の課題

クラウドの技術面の課題は主としてクラウド事業者、またはクラウドシステム・サービスの構築事業者が対応すべき事項だが、エンドポイントのセキュリティについては利用者の対策も重要となる。

(a)ゼロトラストモデルへの対応

ネットワーク境界の内側（イントラネット）は定常的にセキュアである、という従来の境界防御モデルはもはや通用せず、「すべての端末やトラフィックを疑う必要がある」とするゼロトラストの考え方は2010年に提唱されたが、近年急速に普及しつつある。ゼロトラストモデルではネットワークセグメント単位ではなく、個々のリソース単位に不正アクセスや攻撃を防ぐことが求められ、個人や接続機器の認証の重要性が増すこととなる。2020年2月にはNISTがゼロトラストアーキテクチャに関する規格SP800-207の2nd draftを公開している※250。

クラウドにおいても、SaaSサービスの急増、モバイル・IoT機器等のデバイスの急増に伴い、インバウンド・アウトバウンドのネットワーク監視はもとより、クラウド利用者やデバイスの認証強化、エンドポイントのセキュリティ強化が重要となっている。クラウド事業者はこれに対応して、アイデンティティ管理・認証、デバイス（エンドポイント）の可視化、最小権限ポリシーに基づく特権管理等の機能強化を進め、利用者に推奨している。ID統合により、クラウド、エンドポイント、オンプレミス等のセキュリティを一括管理する提案もある※251。

ゼロトラスト対応のネットワークセキュリティモデルとして、Software Defined Perimeter（SDP）がある※252。SDPは、クライアント認証をベースとして、データセンターを横断する仮想クラウドネットワークを構築するパラダイムであり、クラウドセキュリティのベストプラクティスを策定する非営利団体Cloud Security Alliance※253が2013年に提唱、推進している。SDPでは、クラウドにアクセスするすべての利用者・デバイスの認証・認可をクラウドとは別のSDPコントローラで行い、認証・認可が成功するまでクラウドへの接続を許可しない構成をとる※254。クラウドベンダ等の協力により実施したハッカソンでは一度も攻撃が成功しなかったとしている。SDPは特に、複数のクラウドを横断的に利用する企業が共通の方式でゼロトラストセキュリティを確保するのに適している。その場合は、クラウド事業者とは独立したSDPコントローラを運用するネットワーク事業者への信頼が前提となる。

(b)コンテナ技術

コンテナ技術とは、ホストOSの上でアプリケーション、ミドルウェア、設定ファイル等をパッケージ化し、他のプロセスから隔離して実行させる技術である。ハイパーバイザーでハードウェアを仮想化する仮想マシン技術と比較して、動作が軽量で可搬性が高く、同一のコンテナ（実行環境）で検証と実運用を行えることから、アジャイル型開発（DevOps）とも親和性がよい。例えばGoogle社では、提供サービスのコンテナ化を実現しており、同社が開発したオープンソースのコンテナオーケストレーションプラットフォーム「Kubernetes」は、クラウドネイティブソフトウェア※255のメンテナンスに関する非営利団体Cloud Native Computing Foundation（CNCF）※256によって管理されている（2020年4月の時点で会員数560）。今後はCNCFのようなクラウドネイティブソフトウェア開発のエコシステムが核となり、IaaS/PaaSの利用者システムも、コンテナによる開発が主流になる可能性がある。

IDC Japan株式会社は2020年5月12日、日本国内におけるコンテナ技術「Docker」とKubernetesの導入に関する調査結果を発表した※257。発表によれば、コンテナを本番環境で使用している企業は、2019年の調査から5.0ポイント増加の14.2%、導入構築／テスト／検証段階の企業が18.6%、導入計画／検討段階の企業が19.0%で、その総計が50%を越えたという。

一方で、コンテナ導入における課題も多い。アプリケーションのコンテナ化のための技術課題に加え、日本国内ではアジャイル型開発が未だに定着しているとはいえない。またグローバルに見ても、コンテナ化におけるセキュリティ対策は十分できているとは言えない。NISTは2017年の時点でコンテナ化に関するセキュリティ指針NIST SP800-190※258を公開し、検討を促してきたが、2019年のPalo Alto Networks, Inc.のUnit42の調査によれば、40,000以上のコンテナシステムが、脆弱な初期設定・プロトコルを利用して動作していたという※259。特にウイルスや脆弱性の作り込み・混入をコンテナから排除することは非常に重要であり、セキュアなコンテナ開発の方式を早期に具体化することが求められる。

(c)データのライフサイクル管理

クラウドサービスで蓄積したユーザデータのライフサイクル管理は、運用事業者等にこれを委託する場合も、第一義的にはクラウド利用者の責任とされる。しかし、サー

ビスの利用終了後、データが記録媒体から消去されたことを利用者はどう確認したらよいか、という課題がある。これは、例えば大量の個人情報をクラウドで管理する場合に懸案となる事項である。2019 年 12 月、リース契約満了に伴う廃棄予定 HDD の盗難・売却事案[※260] が公表され、個人情報の流出案件であったため、改めて議論となった（同事案の内容と対策については「1.2.7 情報漏えいによる被害」参照）。

これに関して、前述の ISMAP の管理基準は、消去の定義について「論理的消去」、すなわち暗号化したデータの鍵を廃棄して復号できなくすることも「消去」に含めた点が注目される（「ISMAP 管理基準[※261]」の第 1 章に記載）。データの消去を物理的・電磁的な手段に限定した場合、その確認作業が高負荷になり得ることを考慮し、上記の定義が追加されたと考えられる。

(d)リモート会議システムの脆弱性と対応

2020 年 1 月以降、セキュリティ対策の重要性が増しているクラウド利用アプリケーションとして、リモート会議システムがある。新型コロナウイルス対策による急激な普及以降、リモート会議システムの脆弱性や攻撃に関する報告が相次いでいる。

2020 年 4 月 3 日、IPA はリモート会議アプリケーション「Zoom」の脆弱性について、Windows クライアントのチャット機能における UNC（Universal Naming Convention）パスの処理に関する脆弱性により、認証情報の窃盗や任意のファイルを起動される可能性がある、とする注意喚起を行った[※262]。また Zoom での会議において、会議 URL を入手した第三者が勝手に参加し、不適切なコンテンツ表示等で会議を妨害する攻撃「ズーム爆弾（Zoom Bombing）」が問題となった[※263] 他、エンドツーエンド暗号化方式の不備等複数の脆弱性が指摘された。対応が注目された Zoom Video Communications, Inc.（以下、Zoom 社）は、4 ～ 6 月の 90 日間はセキュリティ対策の強化のみに注力するとし、4 月 8 日には会議の隔離・参加者の管理・会議 ID 秘匿等の機能追加を公表した[※264]。また 4 月 27 日にリリースしたクライアントソフトウェア Zoom 5.0 ではセキュリティ強化のため認証付き暗号（AES256 ビット GCM）をサポートし、5 月 30 日にシステムでの運用が可能となった。他にも「ユーザへの報告」機能の提供、デフォルトセキュリティ設定の更新等が実施された[※265]。

一方、同年 6 月 11 日、天安門事件に関する Zoom 会議の開催が中止され、また会議を主催した中国の活動家のアカウントが停止された。Zoom 社はこれが中国政府の要求であったことを認め、会議を主催した場所は米国だが、中国本土の参加者が多かったための措置であるとしたが、自社の利用ポリシーに不備があるとし、改善を約束した[※266]。

他のリモート会議システムに関する脆弱性の報告も相次いだ。2020 年 1 ～ 6 月の間、Cisco Webex に関する脆弱性が以下のように報告された。

- CVE-2020-3142（1 月 29 日）：Cisco Webex Meetings Suite と Cisco Webex Meetings Online における未認証会議参加の脆弱性[※267]。
- CVE-2020-3194（5 月 4 日）：Cisco Webex ネットワーク録画プレーヤーおよび Cisco Webex プレーヤーの任意のコード実行に関する脆弱性[※268]。
- CVE-2020-3263（6 月 17 日）：Cisco Webex Meetings デスクトップアプリの URL フィルタリングの任意プログラム実行に対する脆弱性[※269]。

Cisco Systems, Inc. は、以上の脆弱性については対策済みであり、それぞれのアプリケーションを最新版に更新することで対応できるとしている。

また同年 4 月 27 日、CyberArk Software, Inc. は Microsoft Teams について、アカウントの乗っ取りとデータ窃取が可能な脆弱性が存在すると報告した[※270]。この脆弱性の情報は Microsoft 社に提供され、既に対策がとられたという。

以上のように、リモート会議システムの脆弱性の発見と対策は矢継ぎ早に進んでおり、利用者は最新の情報を収集し、最新のバージョンを利用する等の対応が求められる。

(2)マネジメント面の課題

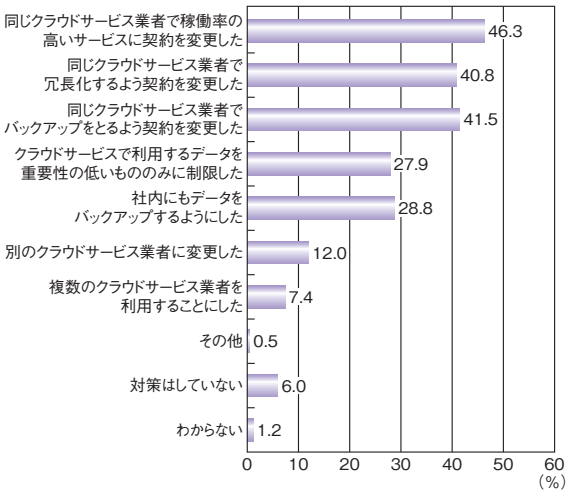
クラウドのマネジメント面の課題はクラウド事業者、クラウド利用者どちらにもあると考えられるが、以下では利用者の課題に注目する。

(a)リスク評価と対策の見直し

クラウド利用を検討するにあたり、クラウド上で行う業務の目的や処理する情報の重要度に合わせてリスクを評価し、サービスを選定することが重要である。「3.4.1 クラウドサービスのインシデント、被害の実態」で見たように、高可用性や高度なセキュリティ対策を具備しているクラウドサービスでもインシデントは起こり、クラウド事業者の対策は継続的に強化されている。実際の事例を基に、

インシデント防止やインシデント対応のために何をするべきか、対策や運用を常に見直すことが求められる。

IPA では 2019 年度、「IT システム・サービスの業務委託契約書見直しに関する実態調査[※271]」を実施した。クラウドサービスのインシデント発生をきっかけに見直した契約内容について調査した結果を図 3-4-1 に示す。稼働率の高いサービスへ変更する、冗長化するように変更する、バックアップを取得するように変更する、といった契約内容の見直しが多いことが分かった。



■図 3-4-1　クラウドサービス障害事故をきっかけとして契約を見直した内容（複数回答可、n=434）

新たにクラウドを利用する場合だけでなく、運用中のクラウドの契約の見直しも含め、サービス停止、データ消失、情報漏えい等が発生した場合に事業にどのような影響があるかを検討し、契約内容やデータバックアップ等の対策を見直していくことが重要である。

(b) クラウド利用のガバナンス

キヤノンマーケティングジャパン株式会社が 2020 年 3 月に公表したシャドー IT に関する実態調査報告[※272]（企業従業員 700 人対象）によると、個人的に登録・契約し、業務で使用しているクラウドサービス・アプリがある、と回答した従業員は 25.3%で、利用サービスは Web メール、ストレージ、コラボレーションサービス／リモート会議、ファイル転送が主なものだったという。また同調査によれば、個人の端末を業務に利用すると回答した従業員が 40.7%、そのうち 43.1%が勤務先の許可を得ていない、あるいは許可は不要と回答していた。

本調査は 2019 年に実施されたものだが、企業が把握できないクラウドサービス利用を従業員の 20%程度が行っており、その何割かは私用パソコン等を業務に利用していることが想定され、組織のガバナンスがほぼ効かない状態でメール・ファイル共有・コラボレーションサービス等の利用を行っているリスクがあることが示された。更に 2020 年以降、新型コロナウイルス対策でテレワークが急激に推進された結果、私用端末の利用や私的なクラウド利用（特にリモート会議）が拡大した可能性がある。クラウドを含むシャドー IT のガバナンスは喫緊の課題になったと考えられる。

企業の IT 部門が把握できていないクラウド利用（いわゆる「野良クラウド」）の把握・統制は近年ガバナンスの課題とされ、解決策として Cloud Access Security Broker（CASB）の導入が提唱されてきた。CASB はクラウドと企業従業員が利用する端末との間でアクセストラフィックを可視化し、不要なアクセスを遮断し、必要なアクセスについてはセキュリティ設定等を行う等、統合的な対策が可能となる。ただし、CASB の導入には、クラウド利用に関する企業のルール（許容する利用の範囲、申請・セキュリティ審査の方法等の規定）がまず必要となるという点が重要である。

更に、企業が関知しない私用端末で自宅からクラウドを利用するような業務が許容された場合、CASB の可視化対象にはならない点に注意が必要である。クラウド利用に使われるべき端末を把握し、CASB でチェックできるか確認することもクラウドのガバナンスにとって重要である。

(c) クラウドセキュリティ実施状況の評価

クラウド利用のガバナンスのもう一つの課題として、クラウド事業者のセキュリティ対策実施状況のチェックがある。これまでに、経済産業省、総務省等がクラウドセキュリティガイドラインを公開し、また国際標準として ISO/IEC 27017 が策定されている。クラウド事業者は、これらに対する対応状況を自己宣言するか、あるいは JASA - クラウドセキュリティ推進協議会（JCISPA：JASA - Cloud Information Security Promotion Alliance）が認証する CS マーク[※273]、または ISO/IEC 27017 のクラウドセキュリティ認証[※274]を取得することで、セキュリティへの取り組みを保証している。クラウド利用者がクラウド事業者のチェックを行うことは容易ではないため、事業者の自己宣言や認証の取得状況等は、利用者にとっては重要な情報である。今後はこれに事業者の ISMAP への登録（登録により「ISMAP 管理基準」を遵守している事業者と認められる）が加わる可能性がある。

利用者によるクラウド事業者の対策実施状況のチェッ

クについて、特にパブリッククラウドの場合は難しいと考えられる。現在一般に行われているのは、クラウドで行う業務のリスク分析やクラウド事業者のセキュリティ対策の妥当性を検討したか、等の利用者側のマネジメントを含めたチェックシートを作成し、これに基づき運用状況を確認する、また高いセキュリティレベルが求められるクラウド利用については、クラウド事業者との合意の基に脆弱性診断テストを実施して対策を確認する、等である。チェックシートやテストの手法については、利用者が共通に使える形式は確立されておらず、各企業が構築事業者等の支援を受けながら、クラウド業務のリスク分析に基づき、個々に対応している状況であると思われる。

一方で、前述の「令和元年度通信利用動向調査」では、企業のクラウドサービス利用形態について、ファイル保管・データ共有が 56.0%、電子メールが 48.0%、社内情報共有・ポータルが 43.0%であり、営業支援や生産管理等の高度な利用は低水準にとどまっているという。現行のクラウドの主たる利用形態はデータ共有・メール等の基本サービスであるが、これらについて利用者によるセキュリティチェックは十分されていない、という可能性が考えられる。また、セキュリティへの投資が難しい中小企業の SaaS 利用において、認証情報やエンドポイントを含めたセキュリティのチェックが十分されていない可能性も考えられる。今後こうした基本サービスや SaaS の利用におけるセキュリティチェックが重要になると考えられる。

3.4.3 まとめ

クラウドサービスの情報セキュリティは事業者と利用者が責任を分担して実現すべきであり、利用者は利用するクラウドについて何をすべきかを理解し、その範囲において責任を持った対応が求められる。以下ではクラウド利用者の責任分担について、IaaS/PaaS、SaaS の二つの観点からまとめる。

(1) IaaS/PaaS 利用において

クラウド上で行う業務のリスク分析とセキュリティレベルの決定については、システム構築事業者の支援を得ることが多いと思われるが、とるべきセキュリティ対策の決定は利用者の責任において行いたい。オンプレミス環境からの移行を行う場合、検証環境、検証環境から本番環境への移行において、システムのセキュリティ設定・認証情報の設定、またデータ移行における情報漏えい対策、アプリケーションへの不正アクセス監視やデータ保護施策等は利用者の責任となる。実施すべき事項としては、例えば以下がある。

- 認証情報には強いものを設定し、アクセス権付与は必要最小限とする。
- アプリケーション構築においては、脆弱性を作り込まない対策を構築事業者と協議し、実施する。
- アプリケーションに関連する脆弱性情報に常に注意を払い、脆弱性が発見された場合は修正プログラムの適用等、必要な対応をとる。
- 検証環境で一時的にインターネットからのアクセスを認める、等の設定をした場合には設定を必ず元に戻す。
- 運用期間中、関連するインシデント等が発生した場合は都度運用や契約内容を見直し、適宜必要な対策をとる。

クラウド利用終了時の利用者データ削除については、一義的には利用者が責任を負うことになる。クラウド上で管理していた個人情報等が確実に削除されたことを確認したい等のケースについては、「ISMAP 管理基準」が参考になると考えられる。

(2) SaaS 利用において

SaaS においてはシステム構築・移行等におけるセキュリティ対策の負荷は生じないが、様々な SaaS サービスのアカウント情報の管理が重要な課題となる。強いパスワードが推奨されるが、パスワードの管理負荷が大きくなると使い回しのリスクが発生し、注意する必要がある。高負荷にならないよう、適切な運用ルールを策定したい。高いレベルのセキュリティを求められるサービスでは、多要素認証等の強い認証方式を採用したい。また「3.4.1 (7) インシデント・被害状況の整理」で見たように、アカウント情報の窃取ではフィッシング等、利用者（エンドポイント）への攻撃も想定される。エンドポイントのセキュリティ対策について、利用者は責任を持って対策する必要がある。

SaaS サービスのデータ管理は、一義的にはクラウド事業者側の責任となるが、コラボレーションサービスやストレージサービスにおいては、利用者の不適切な運用で漏えいに至るリスクがある。情報共有ルールの策定と適切なアクセス権設定を行いたい。

また「3.4.2 (2) (b) クラウド利用のガバナンス」で見たように、SaaS のような少額で利用できるクラウドサービスは、個々の事業部門がセキュリティリスク等について独自に判断し独自に調達する、あるいはテレワークの要請により、未登録の私用端末を業務に用いてクラウドを利用する、

等のガバナンスの問題が生じ得る。IT セキュリティ部門が把握していないツール・端末で不適切な情報共有が行われないよう、クラウド調達に関するルール化、利用状況の可視化が求められる。

更に「3.4.2 (1) (d) リモート会議システムの脆弱性と対応」で見たように、SaaS サービスの利用にあたっては、アプリケーションの脆弱性・脅威に関して最新の情報を収集し、利用形態やセキュリティについて慎重な判断が求められる。このうち、リモート会議システムの利用について、利用者が事前に検討すべき事項としては、例えば以下がある。

- リモート会議に要求されるセキュリティレベルを明らかにする。
- リモート会議システムが提供するセキュリティ機能、例えば通信データの暗号化方式、暗号鍵の管理方式(リモート会議サービスベンダが鍵を保有するか、等)、共有されるデータの管理方式(データはどこで保有され、どのように削除されるか、等)について確認する。
- 脆弱性に関する情報をチェックし、対策済みの最新のバージョンを利用する。

リモート会議システムを使用する際に注意すべきポイントについては、2020 年 7 月に IPA が公開した「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[※275]」を参照されたい。

COLUMN

コネクテッドカーのセキュリティって?

世は押しなべて「情報やデータの集積と活用」がキーワードですが、自動車の世界も例外ではないようです。最近の自動車では、合計すると軽く 3 桁を越える数の制御用コンピュータ(ECU : Electronic Control Unit)が、様々な部分に搭載されています。それらが車載ネットワークで相互に接続され、制御用のソフトウェアが動作しており、もはや自動車は「ソフトウェアのかたまり」が道を走っているとも言えます。また、自動車の運転支援または自動運転を実現するため、外部の交通情報や、自動車に搭載されたカメラ等の各種センサーから安全な走行に必要な車両周辺情報を取り込むといった、大きなシステムに接続されて走行するという観点からも「コネクテッドカー」とうたわれるようです。

一方、今やパソコンやサーバのみならず、制御システムや重要インフラに対するサイバー攻撃は猛威を振るっており、その手口の多様化・巧妙化はとどまるところを知りません。自動車に対しても、多くは研究者による実験レベルのものではありますが、様々な攻撃が日々試されており、攻撃成功の報告が後を絶たない状況です。攻撃手法は自動車への通信を用いたリモートからの攻撃を始め、車載ネットワークや ECU へのウイルス感染による攻撃等、多種多様です。多くの ECU と情報が相互に連携して動作するコネクテッドカーの安全を担保するためには、考えなければならないセキュリティ対策は多岐にわたります。そして、コネクテッドカーのセキュリティを守るときには、「自動車と乗員と周囲の人の安全」が最重要となります。

車載コンピュータのリソースはパソコンと異なり潤沢とはいえないので、限られたリソースをうまく活用する設計・開発・運用が必要です。設計段階では、後の工程での手戻りを防ぐためにも、遵守すべきセキュリティ標準に配慮して開発することが重要ですし、安全確保のため要所要所で軽量暗号、認証、ファイアウォール等の対策が必要です。攻撃を受けたときは、それぞれの自動車で対処しなければならないのはもちろんですが、攻撃の手口をクラウド上で共有し、他の自動車に一斉に通知して同様の攻撃を未然に防御する、といった試みもあります。車載ネットワークでは、「ふるまい検知」等の技術を活用した攻撃監視を、少ないリソースでいかに強化していくかが、攻撃に適切に対応するためのキーテクノロジーになっていくでしょう。

特別寄稿

セキュリティマネジメントの日米企業比較
～組織論の観点から～

Comparison of Information Security Management in the U.S. and Japan
～ An Organizational Perspective ～

カリフォルニア大学バークレー校名誉教授　**Robert E. Cole**
三菱電機株式会社　シニアアドバイザー　**伏見信也**

初めに

本稿では、日本と米国の大～中規模企業の情報セキュリティ対策及び実践状況を、組織論の観点から比較する。言うまでもなく、米国は世界最大のソフトウェア産業国であり、日本もまたソフトウェア大国の一つである。この両国の企業が、情報セキュリティの課題にどのように対処しているか、を組織論の視点から比較し、日本企業のセキュリティマネジメントを考える上での一助としたい。

セキュリティマネジメントの組織論的課題

後に見るように、日本と米国では企業の情報セキュリティのパフォーマンスに違いがある。技術的観点から見れば、日米両国の企業が利用している情報セキュリティ対策のソフトウェアは大半が同じものである。一方、これらソフトウェアを、いつ、どこで、どのように利用しているか、の点では両国は異なるであろう。つまり、日米企業の情報セキュリティのパフォーマンスの違いは、技術力に限らず、組織的能力から生じていると考えられる。本稿ではこの点の検証を進める。

Facebook の情報セキュリティ責任者である Nathan Gleicher は、情報セキュリティの組織論的課題について「企業の組織を構成する従業員が、誤りなく指示に従い、相互連携することは期待できない。一方、情報セキュリティに対しては、社内のすべての従業員が、日常の細かな作業に至るまで社内規則や指示に忠実に従い、論理的に考え行動することが必要なのである」と指摘している[1]。

情報セキュリティが組織論的課題であることを、以下の二つの例で見てみよう。

A. ソフトウェア脆弱性対策（業務プロセス管理の課題）

企業は、ベンダ各社からの更新パッチを漏れなく把握し、遅滞なくシステムに適用し、記録に残すことが必要であるが、これを確実に実行できているのだろうか。これは企業の業務プロセス管理に関する課題である。

米国ではこのパッチ管理は大きな問題である。MIT Sloan School の Daniel Goldsmith と Michael Siegel は、Verizon 社 の Data Breach Investigations Report のデータ（対象企業の 83% が米国企業）を基に分析を行い、情報漏えい事案の 80% 以上は、攻撃に用いられた脆弱性に対するパッチが 1 年以上前にリリースされているにも関わらず、そのパッチが適用されていなかったために発生した、と報告している[2]。

パッチの適用遅れは、ハッカーに対して絶好の攻撃機会を与える。近年の米国での被害者数最大の情報セキュリティ事案は 2017 年に発生した Equifax（米国の個人信用情報の格付け企業）からの情報漏えいである。この事件では、米国国民の約半数に上る 1 億人以上の個

人情報が漏えいした。2020 年の米国法務省の起訴内容によれば、この攻撃は中国軍の部隊により実施され、Adobe 社の Web アプリケーション開発フレームワーク Apache Struts の脆弱性が利用されていた。Adobe 社はこの脆弱性に対するパッチを提供していたが、Equifax はこれを適用せず、侵入を許す結果となった[3]。

B. 標的型メール・詐欺メール対策（従業員、組織文化の課題）

どのようにすれば、従業員が詐欺メールやなりすましメールに騙されないようにできるのだろうか。これは企業の従業員の能力向上やセキュリティに関する組織文化に関わる課題である。

この問題に対しては、社内ネットワークで業務を行うすべての従業員が、細かな作業に至るまで社内規則に忠実に従い、行動する必要があるが、実際には実現困難である。加えて、ハッカーは、従業員を騙すための、いわゆる「ソーシャルエンジニアリング」技術を磨き上げており、攻撃メールを見破ることはますます難しくなっている。

従業員が、攻撃メールに騙され、悪意もないのにセキュリティの問題を起こしてしまうことは日米両国で大きな問題になっており、深刻な被害に至った例も少なくない。FBI によれば、2014 年のソニー・ピクチャーズ・エンタテインメントへのサイバー攻撃では、標的型メールがシステム技術者、ネットワーク管理者等に送られ、自身の Apple ID を確認するように誘導し、侵入に必要な情報を入手していた[4]。また 2015 年に発生した日本年金機構への攻撃では、厚生労働省の文書に見せかけたなりすましメールが送られ、従業員がウイルスの仕込まれた添付文書を開封した。加えて、社内の個人情報管理規則の違反、事故の報告や情報共有の遅延等の組織レベルの問題があり、被害が拡大した。個々の従業員の攻撃メールへの対応能力とともに、組織としての規則遵守の徹底や攻撃メール開封時の対応能力の向上が求められる。

経営層の認識とセキュリティ対策の現状

両国の経営層は、情報漏えいの影響や情報セキュリティ対策の必要性についてどのような認識を持っているのだろうか？　PwC は、70ヵ国 1,379 社の大企業の CEO（日本 110 人、米国 152 人）の意識調査を行った[5]。この調査によれば、「今後 5 年間で情報漏えい事故がステークホルダーの信頼にどの程度悪影響を及ぼすか」という質問に対し、「大きな影響がある」と回答した日本企業の CEO は全体の 70% に上り、米国企業の CEO の 49% に比べて大きな数字になっている。

にもかかわらず、日本の企業は米国に比べ、情報セキュリティ対策に対する投資が少ない傾向がみられる。NRI セキュアテクノロジーズ（以下、NRI セキュア）による調査[6]では、「情報セキュリティ対策に情報システム総費用の 10% 以上を投資しているか」との問いに対し、「はい」と答えた日本企業は約 20% で、米国企業の約 65% に比べて大幅に少ない。また CISO（Chief Information Security Officer）の設置状況について、情報セキュリティ担当の役員を配置している企業は、米国では回答企業の 71.2% であるのに対し、日本では 35.5% にとどまっている。

つまり、日本企業は、米国企業よりもセキュリティインシデント発生時の信頼喪失を恐れる一方、その対策への投資や専任役員の配置には消極的であることがうかがわれる。この矛盾はどのように説明できるだろうか?

コンテンツ配信大手の Akamai は、同社顧客企業（130 以上の国の 21 万 8,391 社）へのサイバー攻撃の監視結果を公表している。同社によれば、2017 年における米国企業の Web アプリケーションに対する攻撃は 10 億件、日本企業に対する攻撃は 4,400 万件であった[7]。このデータからも、米国企業は日本企業よりも圧倒的に多くの攻撃を受けていることが分かる。このため日本企業は、自社が攻撃に晒されている、との認識が相対的に低いことが推測される。すなわち、日本企業においては、攻撃による被害への心配は大きいものの、実際に攻撃を受ける可能性は低いとの認識で、情報セキュリティ対策への投資にふみきれないでいる、と考えられる。

文化、制度、従業員

NRI セキュアが 2017 年に行ったビジネス E メール詐欺に関する調査[6]では、日本の回答企業の 57.9% で詐欺のインシデントがあった（詐欺メールを受け取った）が、金銭的な損失を被った企業はなかった。このことから、従業員がそのようなメールを開封しなかったか、あるいは開封したが詐欺を見抜いたか、あるいは情報システム部門により適切な対応が取られた可能性が高い。同じ調査で、米国では 70.0% の企業で情報セキュリティのインシデントがあり、31.6%が金銭的損失を被った。日本へのなりすましメールは日本人以外が作成し、メールの文章に不自然さがあった可能性があるものの、それを考慮しても、日本の従業員がフィッシングやなりすましメールに対し、より注意深く対応したことが示唆される。

日本企業は、終身雇用制度を背景とした従業員性善説に支えられてきた。すなわち、日本企業において、従業員は長期間当該企業で就業し、規律を順守し、米国

企業に比べ、会社に対して強い帰属意識を持つ存在である。彼らは、フィッシングやなりすましメールに対する教育や訓練も社内規則に従って受講し、訓練内容を忠実に実践し、フィッシングやなりすましメールへの意識づけも一定程度できている、と考えられる。またNRIセキュアの調査によれば、サイバー攻撃における内部犯罪と外部攻撃の比率を比較しても、日本(5.1%)は米国(52.2%)に比べて圧倒的に内部犯罪が少ない[8]。情報セキュリティ対策においては、組織全体が忠実に対策指示を実行することが重要であるとすれば、日本企業のこれら組織風土は大きな強みとなる。

この分析に対し、日本の終身雇用制度も変化してきており、終身雇用の従業員は大きく減少し、会社への忠誠心も変化している、との批判もあるだろう。実際、日本の政府統計を見ると、2017年において、全従業員のうち、終身雇用される正社員は62.7%で、「失われた10年間」只中の1994年の79%から大きく減少し、代わってパートや派遣社員等の非正規雇用者が急増している[9]。これら非正規雇用者は、社内規則や指示の順守の点で、終身雇用者と同じレベルが期待できない可能性がある。ただし、企業内の機密情報へのアクセスはより制限されている可能性も高い。

米国企業側を見ると、従業員の規律順守の弱さに加え、もう一つ大きな問題がある。それは米国のIT産業を牽引する起業家やスタートアップ企業である。ITは近年の経済成長のエンジンであり、米国の最大の強みであるが、情報セキュリティにおいては同時に弱点にもなる。すなわち、米国のスタートアップ企業は、画期的なイノベーションを掲げた市場参入を最優先し、費用がかかり、短期効果も見えづらい情報セキュリティを後回しにしてきたのである。

これら米国のIT企業においては、セキュリティ対策を完了するまでは新しいソフトウェア技術をリリースしない、との判断ができるかが課題である。経営層は、市場への早期参入による利得と、セキュリティ対策により生じる参入遅れとのトレードオフを適切に評価する必要があるが、企業が置かれている競争環境や業界の慣行(ベータ版の市場投入等)、短期的成果・長期的成果のどちらを優先するか、にも大きく左右されることとなろう。

業務プロセス管理

日本企業のもう一つの強みは、業務改善活動を実現する業務プロセス管理と、その根幹にある品質指向の文化である。歴史的に見ても、日本企業は業務プロセス管理に優れており、またそれを支えてきたのは、企業内の規則や施策、業務プロセスを忠実に実行する従業員である[10]。

先に、米国企業では情報漏えいの80%以上が、1年以上パッチが適用されていなかったシステムで発生した点を指摘した。日本の大企業におけるパッチ管理はかなり異なっている。日本の大学研究者や企業の実務者へのヒアリングによれば、多くの日本の大企業では、全社レベルでパッチ管理と適用の業務プロセスを定め、その実行は集中化、自動化されている。すなわち、PCに関しては、中央の管理サーバが会社内のすべてのPCにパッチを適用する。サーバに関しては、パッチ適用が必要なサーバを特定し、社内のユーザの業務を妨げないように、サーバの停止・パッチ適用・再起動のスケジュールが計画され、実行される。ベンダが保守を打ち切るソフトウェアは、事前にリプレースされる。

これら日本企業の状況を考えると、脆弱性に対するパッチがリリースされてから、パッチが適用されるまでの平均時間は日本企業の方が短いことが予想される。実際、トレンドマイクロ社が2014年に行った調査によると、パッチを全サーバに適用した日本企業は半数程度ではあったが、パッチを適用している企業の54.5%が1週間以内にパッチを適用し、8.5%が半月以内、20%が1ヵ月以上であった[11]。先の米国企業に対するパッチ管理の調査結果とこの数字は直接比較できないが、日本企業は、パッチ管理をより効果的に実行していることが示唆される。このことは、日本企業の業務プロセス管理の能力が情報セキュリティ対策において活用されている例であると考えられる。

情報セキュリティ人材と情報システム部門

情報セキュリティ対策における日本企業の最大の弱みは、情報セキュリティ人材の不足と、その育成が進まない状況にある。逆に、情報セキュリティ人材は米国の強みであり、大学で多くの高度IT技術者が育成され、企業や研究機関に就職している。米国のトップクラスの大学でコンピュータサイエンス専攻者は依然として増加しており、情報セキュリティの講義やカリキュラムも強化されている。2018年には米国家安全保障局(National Security Agency)が137の教育機関を「サイバーセキュリティ教育・研究の中核的研究拠点」に指定し、育成を強化している。米国企業においても情報セキュリティ技術者への需要は大きいが、日本と比較して、米国の情報セキュリティ技術者には、高い役職とキャリアパスが提供され、事業に直接関わる機会も数多く与えられる。

NRIセキュアの日米の大企業の情報システム部門を

対象とした調査[8]では、情報セキュリティの最大の課題として、日本の回答者の43.2%が技術者の確保を上げており、全体で最多となっている。米国の回答ではこれが11.4%に過ぎず、全体でも4番目の位置付けである。Raytheonが2018年に実施した12ヵ国の3,800人の若者(18～26歳)を対象とした調査[12](Zogby Analyticsにより実施)では、日本の回答者の情報セキュリティに関わる職業に対する興味は全体平均よりも低く、米国に比べて圧倒的に低かった。具体的には、日本の回答者のうち、情報セキュリティ技術者の仕事の内容を理解しているのは31.6%で、米国の39.5%よりも低く、情報セキュリティ技術者と話をしたことがあるのは9.7%で、米国の24.3%より大幅に少なかった。

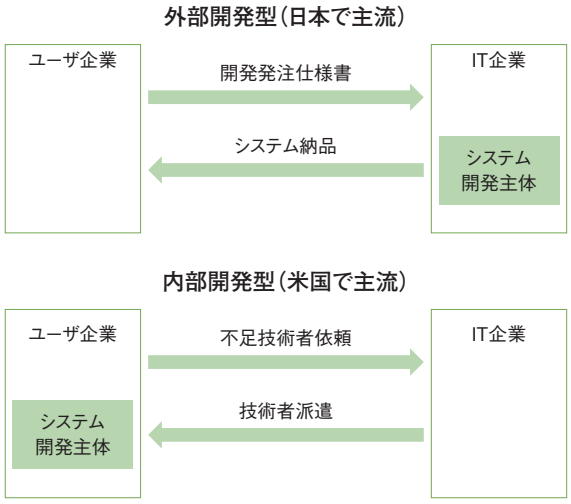
このように、日本においては、情報セキュリティ技術者は人気の職業ではない。この背景には、日本の企業が情報セキュリティ技術者の採用や、昇進について消極的だったことがあると考えられる。伝統的に日本企業の人材育成は幅広い業務経験を持つジェネラリストを育成することが中心であり、専門技術者は奨励されなかった。ジェネラリスト優先の環境では、情報セキュリティ技術者に高給を支払い、キャリアパスを提供することは行われない。NRIセキュアの調査によると、情報セキュリティ技術者に対してキャリアパスを提示しているのは、日本の大企業のうち3.8%であり、一方、米国企業のそれは36.4%である[8]。

技術者の不足に対する解決策の一つは、情報セキュリティ対策を外注することである。米国の26.6%、日本の29.3%の企業が少なくとも対策の一部を外部委託しているとの調査があるが[8]、この外部委託方式は、人材不足が深刻な日本では今後急速に増加するであろう。一方、企業の事業はデジタル技術が核となりつつあり、情報セキュリティはそのコアコンピタンスの一つである。システムインテグレータや専門会社はインセンティブも異なり、企業の業務理解にも限界がある。デジタル化の戦略は企業が判断すべきものであり、セキュリティ対策で何を優先すべきかをすべて外部委託することはできない。

日本企業の情報システム部門の考え方や情報システムのウォータフォール型の開発スタイルも、情報セキュリティの新しい手法導入の妨げになっている。米国では、DevSecOpsと呼ばれる新しいソフトウェア開発手法が普及し、開発の短期化とセキュリティ担保という相反する目標を同時に実現している。DevSecOpsは、ソフトウェア開発、セキュリティの開発、システム運用を一体化し、短期間でリリースを繰り返す手法である。

日本企業では、DevSecOps、更にはその元となっているアジャイルやDevOpsの開発方式の採用が進まないが、この理由は何だろうか? その一つは、ソフトウェア開発の組織論的な違いにある。日本の製造業やサービス業の大企業は、1990年代に子会社化やシステムインテグレータへの外注化を進めて、情報システム部門を縮小した。背景には、専門子会社の方が新技術や市場動向をうまく活用し、また子会社化や開発の外注化によりIT人員のコスト削減ができると考えたことがある。当時、日本企業は海外市場でも競争力を持ち、一方でIT技術が将来の事業の中核となるデジタル化時代は予想していなかった[13]。

この結果、図に示すように、日本のユーザ企業は情報システムをIT企業(システムインテグレータ)に外注して開発することが一般的となっている。IT企業は完成責任を持つから、原則として、システム仕様が確定した後に受注に応じる。このような日本企業の外注構造や小規模IT部門の体制では、開始時点で仕様が必ずしも明確でないDevOpsやDevSecOpsを取り入れるのは難しいのである。一方、米国企業の大半は、ユーザ企業が自身で情報システムを開発し、技術者が不足している場合にのみ、IT企業から派遣を受けることが一般的である。この場合、ユーザ企業が自身で完成責任を負うため、開発開始時点で仕様が確定していることは必ずしも必要はなく、ユーザ企業の責任で試作を繰り返してシステムを完成させて行くDevSecOpsのような開発手法が可能となる。また、日本企業は、事前に仕様が確定しないまま開発すると、品質問題が生じると考えがちである。伝統的な強みである品質指向の考えにより、新しいIT技術への取り組みに慎重になり、後追いになっている可能性がある。



■図　日米のソフトウェア開発形態の違い

おわりに

これらの日米比較から何が学べるだろうか。

これまでを振り返れば、米国企業は、日本企業に比べて遥かに大きなサイバー攻撃対象であった。この結果、米国企業は情報セキュリティへの取り組み意識が高く、情報セキュリティへの投資意欲も日本企業のそれに比べて大きい。一方、日本企業は、これまでは攻撃対象となることが少なく、現状対策で十分との認識を持っていた可能性がある。しかし、攻撃側の能力が急拡大している現状においては、その認識を改める必要がある。

明らかに、日本の大～中規模企業は情報セキュリティにおける強みを持つ。すなわち、日本企業は、業務プロセス管理の能力やルール順守の組織文化を持ち、従業員は情報漏えいにつながるようなヒューマンエラーを最小化しようと行動する。しかしながら、攻撃側の能力（ソーシャルエンジニアリング等）は進化し続けており、日本企業は上記の強みを更に強化する必要がある。

一方、米国企業は、日本企業に比べ、業務プロセスとしてのセキュリティ対策遂行やルールの順守の風土に弱みがあるものの、能力の高い情報セキュリティ技術者を豊富に有する。更に情報セキュリティ技術者に対し、事業部門と連携し事業貢献する機会やその先のキャリアパスも提供しており、結果として情報セキュリティ技術者の能力を幅広く活用している。また、DevSecOps 等の新しい取り組みも進めている。

サイバー攻撃は、攻撃のコストが防御のコストより小さく、攻撃成功時のリターンが、防御成功時のリターンより大きい限り、今後も止むことはない。また、これからの情報セキュリティは、ソフトウェアのシステムやアプリケーション製品だけではなく、ハードウェア製品にも必要となる。近年のハードウェア製品にはソフトウェアが組み込まれ、ユーザのネットワークやインターネットにも接続されることで巨大な IoT システムを構成し、大きな攻撃対象になりつつある。

これらを踏まえ、今後、日本企業はどうすべきだろうか。

第一に、経営層は、情報セキュリティにおいては「改善」と「戦略」の双方が必要である点を認識すべきである。日本企業は、業務プロセス管理の能力が高く、情報セキュリティに必要な業務改善においても強みを発揮してきたが、それに加えて戦略が必要である。ここで、情報セキュリティ管理の戦略とは、よく知られている「競争戦略[14]」とは異なり、当該企業における情報セキュリティ管理の達成目標とアクションプランである。先に述べた Gleicher の組織的課題を考えれば、プロセス管理の充実や部門レベルの断片的な施策だけでは不十分なことは明らかである。全社レベルの戦略とその実行、例えば、情報セキュリティ技術の評価・導入、部門間・階層間・取引先にわたる指揮系統の確立、等が必要である。また、情報セキュリティに関する情報共有の戦略も必要である。情報セキュリティに関する情報は企業で秘匿しがちであるが、むしろ、他の企業、取引先、政府組織等と情報を共有し、ベストプラクティスとして有効な対策確立を加速する戦略も考えられる。

第二に、企業の経営層は、情報セキュリティに関しては、セキュリティ投資のリターンだけでなく、トータルなリスク管理の視点で意思決定しなければならない。

最後に、日本企業の経営層は、過去において自社に成功をもたらしたやり方（IT 部門の縮小、過度の外注化、ジェネラリスト優先の人材育成等）が、情報セキュリティ対策の新しい取り組み（DevSecOps 等）や人材確保を阻害している可能性を認識し、これまでの情報セキュリティへの取り組みを見直し、強化すべきである。

ここで、日本企業の情報セキュリティにおける弱みのほとんどは、これまで成功をもたらしたやり方故の結果であることに気付く。しかし、企業が従来の成功要因を否定して新しい取り組みを進めることは容易ではない。企業が過去辿ってきた道の上に企業の現在があるのであり、新しい取り組みへの道がこれまでと大きく異なれば、企業はこれまでの道の延長にある現状維持や現状改善を選ぶ。いわゆる、経路依存性（Path Dependency）である。このため、歴史を振り返れば、このような軌道修正に失敗してきた企業は数多い[15]。日本企業の情報セキュリティの今後においては、過去の成功にとらわれず、将来に取り組むことができる経営能力が最も重要となるのである。

執筆者略歴

Robert E. Cole
米国カリフォルニア大学バークレー校ハース経営大学院、社会学部名誉教授。ミシガン大学教授、カリフォルニア大学バークレー校ハース・ビジネススクール、社会学部教授を経て、現職。日本企業の研究、特に自動車、IT 分野の日本企業の組織論的研究、日米比較研究等に従事。日本においては、慶応大学、東京大学の客員教授、同志社大学大学院ビジネス研究科教授を歴任。イリノイ大学 Ph.D（社会学）。

伏見信也
三菱電機株式会社シニアアドバイザー。三菱電機株式会社技術企画部長、情報技術総合研究所所長、常務執行役インフォメーションシステム事業推進本部長を経て、現職。IT 分野の研究開発、事業経営に従事。東京大学工学博士（情報工学）、スタンフォード大学経営大学院修士（スローン・フェロー）。

1 McKinsey & Company, "Finding a Strategic Cybersecurity Model, Interview with Nathan Gleicher," 2017. [Online]. Available: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/finding-a-strategic-cybersecurity-model.
2 D. Goldsmith and M. Siegel, "Systemic Approaches to Cyber Security," Office of Naval Research, no. N00014-09-1-0597, 2010.
3 C. Warzel, “Brokers are Like Hackers but Legal,” New York Times, 11 Feb. 2020.
4 FBI National Press Office, “Update on Sony Investigation,” 2014.
5 PwC, “20th CEO Survey - Japan Territory Cut,” 2017.
6 NRI セキュアテクノロジーズ , “NRI Secure Insight 2018 企業にける情報セキュリティ実態調査 ,” 2018.
7 Akamai, “State of the internet / security, Q1-Q4 2017 Report,” 2017.
8 NRI Secure Technologies, Ltd., “NRI Secure Insight 2017 International Information Security Survey,” 2017.
9 総務省統計局 , “労働力調査 2018 年 ,” 2018.
10 M. Porter and T. Hirotaka, Can Japan Compete?, Palgrave MacMillan, 1990.
11 トレンドマイクロ , “企業におけるサーバ脆弱性対策に関する実態調査 2014,” 2014.
12 Raytheon, “Securing Our Future: Closing the Cybersecurity Talent Gap,” 2018.
13 R. Cole and Y. Nakata, "The Japanese Software Industry: What Went Wrong and What Can we Learn From it?," California Management Review, vol. Fall, pp. 16-43, 2014.
14 M. Porter, What is Strategy, Vols. November-December, Harvard Business Review, 1996, pp. 61-78.
15 D. Teece, G. Pisano and A. Shuen, "The Nature and Dynamics of Organizational Capabilities," G. Dosi, R. Nelson and S. Winter, Eds., Oxford University Press, 2000, pp. 346-347.

※ 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〔2020/6/11 確認〕
※ 2　DEF CON Communications：DEF CON　https://www.defcon.org/〔2020/6/11 確認〕
CODE BLUE 2019@TOKYO：ICS Cyber hacking Challenge　https://codeblue.jp/2019/contests/detail_02/〔2020/6/11 確認〕
※ 3　DOE：ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT　https://assets.documentcloud.org/documents/6535023/sPower-FOIA.pdf〔2020/6/11 確認〕
NERC：Lesson Learned　https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf〔2020/6/11 確認〕
※ 4　SECURITYWEEK：DoS Attack Blamed for U.S. Grid Disruptions: Report　https://www.securityweek.com/dos-attack-blamed-us-grid-disruptions-report〔2020/6/11 確認〕
ZDNet：Cyber-security incident at US power grid entity linked to unpatched firewalls　https://www.zdnet.com/article/cyber-security-incident-at-us-power-grid-entity-linked-to-unpatched-firewalls/〔2020/6/11 確認〕
cyberscoop：Utah renewables company was hit by rare cyberattack in March　https://www.cyberscoop.com/spower-power-grid-cyberattack-foia/〔2020/6/11 確認〕
※ 5　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 [2019 年 10 月 1 日～ 2019 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〔2020/6/11 確認〕）を参照した。
※ 6　infosecurityMAGAZINE：Nine in 10 CNI Providers Damaged by Cyber-Attacks　https://www.infosecurity-magazine.com/news/nine-10-cni-providers-hit-damaging-1/〔2020/6/11 確認〕
※ 7　infosecurityMAGAZINE：Security by Sector: Study Explores Cyber-Threats Impacting the Utility Industry　https://www.infosecurity-magazine.com/blogs/cyberthreats-impacting-utility/〔2020/6/11 確認〕
※ 8　「マルウェア」等の用語を混在して使用すると、読者を混乱させる可能性があるため、本白書では特に断りのない限り、または文献引用上の正確性を期す必要のない限り、総称して「ウイルス」と表現する。
※ 9　ASIA TIMES：Cyberattack scare dogs India's nuclear plants　https://www.asiatimes.com/2019/10/article/cyberattack-scare-dogs-indias-nuclear-plants/〔2020/6/11 確認〕
THE WIRE：Along With Kudankulam, ISRO Also Warned About Cyber Security Breach: Report　https://thewire.in/tech/isro-kudankulam-cyber-security〔2020/6/11 確認〕
NPCIL：Press Release　https://npcil.nic.in/writereaddata/Orders/20191030123734696017 1News_30102019_01.pdf〔2020/6/11 確認〕
※ 10　SANS Institute：SANS 2019 State of OT/ICS Cybersecurity Survey　https://www.nozominetworks.com/downloads/US/SANS-2019-OT-ICS-Security-Survey-from-Nozomi-Networks.pdf〔2020/6/11 確認〕
※ 11　HELPNETSECURITY：Employees are aware of USB drive security risks, but don't follow best practices　https://www.helpnetsecurity.com/2019/05/15/usb-drive-security-risks/〔2020/6/11 確認〕
※ 12　MINIGDOTCOM：Cyber attack hits operations at aluminum maker Norsk Hydro　https://www.mining.com/web/cyber-attack-hits-operations-aluminum-maker-norsk-hydro〔2020/6/11 確認〕
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 5 ～ 2019 年ランサムウェアによる操業停止～　https://www.ipa.go.jp/files/000080702.pdf
※ 13　InsuranceBUSINESS AMERICA：Norsk Hydro gets more cyber insurance compensation　https://www.insurancebusinessmag.com/us/news/cyber/norsk-hydro-gets-more-cyber-insurance-compensation-213096.aspx〔2020/6/11 確認〕
※ 14　BLEEPINGCOMPUTER：Cyber Attack Shuts Down Hoya Corp's Thailand Plant for Three Days　https://www.bleepingcomputer.com/news/security/cyber-attack-shuts-down-hoya-corps-thailand-plant-for-three-days/〔2020/6/11 確認〕
※ 15　The Register：South Africans shivering in the dark after file-scrambling nasty hits Johannesburg power biz　https://www.theregister.co.uk/2019/07/25/johannesburg_ransomware_infection/〔2020/6/11 確認〕
TechRadar：Ransomware attack leaves Johannesburg without power　https://www.techradar.com/news/johannesburg-ransomware-attack-leaves-city-without-power〔2020/6/11 確認〕
※ 16　Positive Technologies：Industrial companies: attack vectors　https://www.ptsecurity.com/ww-en/analytics/ics-attacks-2018/〔2020/6/11 確認〕
※ 17　ICS-CERT のウェブサイトで暦年（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 2019 年なら、採番年度が 2018（ICSA-2018-xxx-x）でも 2019 年でカウント）。NCCIC：ICS-CERT Advisories　https://www.us-cert.gov/ics/advisories〔2020/6/11 確認〕
※ 18　HELPNETSECURITY：200 million enterprise, industrial, and medical devices affected by RCE flaws in VxWorks RTOS　https://www.helpnetsecurity.com/2019/07/29/vxworks-rtos-vulnerabilities/〔2020/6/11 確認〕
※ 19　Armis Inc.：UPDATE：URGENT/11 affects additional RTOSs - Highlights Risks on Medical Devices　https://www.armis.com/urgent11/〔2020/6/11 確認〕
※ 20　WIRED：Inside the World's Highest-Stakes Industrial Hacking Contest　https://www.wired.com/story/pwn2own-industrial-hacking-contest/〔2020/6/11 確認〕
※ 21　ICS-CERT Annual Vulnerability Coordination Report の Figure 1.（p.3）の「Advisories - FY」の数字を採用した。ただし、Figure 1. の 2016 年には暦年（CY）の件数があるが、件数が 185 件と、実際に Web サイト上で公開されている件数（140 件）と大きく乖離しており、カウント方法の詳細が不明なため、2017 年、2018 年、2019 年と同様に ICSCERT 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て図 3-1-3 に掲載した。
NCCIC：ICS-CERT Annual Vulnerability Coordination Report　https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf〔2020/6/11 確認〕
※ 22　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 2019 年なら、採番年度が 2018（ICSA-2018-xxx-x）でも 2019 年でカウント）。
NCCIC：ICS-CERT Advisories　https://ics-cert.us-cert.gov/advisories〔2020/6/11 確認〕
※ 23　https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_005E.pdf?__blob=publicationFile&v=7〔2020/6/11 確認〕
※ 24　IPA：[ドイツ BSI] 産業用制御システム（ICS）のセキュリティ -10 大脅威と対策 2019-　https://www.ipa.go.jp/security/controlsystem/bsi2019.html〔2020/6/11 確認〕
※ 25　https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019〔2020/6/11 確認〕
※ 26　The Day Swig：Ransomware still dominates the cyber threat landscape in 2019 – Europol report　https://portswigger.net/daily-swig/ransomware-still-dominates-the-cyber-threat-landscape-in-2019-europol-report〔2020/6/11 確認〕
※ 27　TechCrunch：Arizona Beverages knocked offline by ransomware attack　https://techcrunch.com/2019/04/02/arizona-beverages-ransomware/〔2020/6/11 確認〕
※ 28　トレンドマイクロ株式会社：Account With Admin Privileges Abused to Install BitPaymer Ransomware via PsExec　https://blog.trendmicro.com/trendlabs-security-intelligence/account-with-admin-privileges-abused-to-install-bitpaymer-ransomware-via-psexec/〔2020/6/11 確認〕
※ 29　ATLANTA BUSINESS CHRONICLE：Cybersecurity incident at metro Atlanta's 4th-largest private company disrupts manufacturing, shipping　https://www.bizjournals.com/atlanta/news/2019/12/11/cybersecurity-incident-at-metro-atlantas-4th.html〔2020/6/11 確認〕BLEEPINGCOMPUTER：Maze Ransomware Demands $6 Million Ransom From Southwire　https://www.bleepingcomputer.com/news/security/maze-ransomware-demands-6-million-ransom-from-southwire/〔2020/6/11 確認〕
※ 30　DARKReading：Ransomware Victim Southwire Sues Maze Operators　https://www.darkreading.com/threat-intelligence/ransomware-victim-southwire-sues-maze-operators/d/d-id/1336719〔2020/6/11 確認〕
infosecurityMAGAZINE：US Biz Wins Court Case Against

Ransomware Data Thieves https://www.infosecurity-magazine.com/news/us-biz-court-case-ransomware-data/〔2020/6/11 確認〕
※ 31 ComputerWeekly.com：Cyber gangsters publish staff passwords following 'Sodinokibi' attack on car parts group Gedia https://www.computerweekly.com/news/252477341/Cyber-gangsters-publish-staff-passwords-following-Sodinokibi-attack-on-car-parts-group-Gedia〔2020/6/11 確認〕
※ 32 IBM 社：Combating Destructive Malware: Lessons from the Front Line https://www.ibm.com/account/reg/il-en/signup?formid=urx-40087〔2020/6/11 確認〕
※ 33 ZDNet：Cyberattacks against industrial targets have doubled over the last 6 months https://www.zdnet.com/article/cyberattacks-against-industrial-targets-double-over-the-last-6-months/〔2020/6/11 確認〕
SecurityIntelligence：From State-Sponsored Attackers to Common Cybercriminals: Destructive Attacks on the Rise https://securityintelligence.com/posts/from-state-sponsored-attackers-to-common-cybercriminals-destructive-attacks-on-the-rise/〔2020/6/11 確認〕
※ 34 Dragos, Inc：CRASHOVERRIDE：Reassessing the 2016 Ukraine Power Event as a Protection-Focused Attack https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf〔2020/6/11 確認〕
※ 35 Dragos, Inc：EKANS Ransomware and ICS Operations https://dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/〔2020/6/11 確認〕
※ 36 MeriTalk：DHS Sets List of National Critical Functions, Marking Shift from CI Sectors https://www.meritalk.com/articles/dhs-sets-list-of-national-critical-functions-marking-shift-from-ci-sectors/〔2020/6/11 確認〕
CISA：National Critical Functions Set https://www.cisa.gov/national-critical-functions-set〔2020/6/11 確認〕
※ 37 SECURITYWEEK：NIST Working on Industrial IoT Security Guide for Energy Companies https://www.securityweek.com/nist-working-industrial-iot-security-guide-energy-companies〔2020/6/11 確認〕
※ 38 NIST CSRC：Draft NISTIR 8183A is Available for Comment: Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide https://csrc.nist.gov/News/2019/nist-releases-draft-nistir-8183a-for-comment〔2020/6/11 確認〕
※ 39 THE HILL：Legislation to protect electric grid from cyberattacks added to massive defense bill https://thehill.com/policy/cybersecurity/474160-legislation-to-protect-electric-grid-from-cyber-attacks-added-to-massive〔2020/6/11 確認〕
※ 40 ISA：New ISA Global Cybersecurity Alliance Accelerates Education, Readiness, and Knowledge Sharing https://www.isa.org/news-and-press-releases/isa-press-releases/2019/july/new-isa-global-cybersecurity-alliance-accelerates-education-readiness-and-knowledge-sharing/〔2020/6/11 確認〕
ISA：ISA Announces First Founding Members of Global Cybersecurity Alliance https://www.isa.org/news-and-press-releases/isa-press-releases/2019/july/isa-announces-first-founding-members-of-global-cybersecurity-alliance/〔2020/6/11 確認〕
ISA：GLOBAL CYBERSECURITY ALLIANCE https://isaautomation.isa.org/isa-global-cybersecurity-alliance-news-releases/〔2020/6/11 確認〕
※ 41 Reed Exhibitions Ltd.：ISA Global Cybersecurity Alliance Triples Membership https://www.infosecurity-magazine.com/news/isagca-triples-membership/〔2020/6/11 確認〕
※ 42 SMART ENERGY INTERNATIONAL：Global alliance to enhance cybersecurity capabilities launched https://www.smart-energy.com/industry-sectors/cybersecurity/global-alliance-to-enhance-cybersecurity-capabilities-launched/〔2020/6/11 確認〕
※ 43 DailyEnergyInsider：Fortress, AEP team up to help protect power grid from cyber threats https://dailyenergyinsider.com/news/22814-fortress-aep-team-up-to-help-protect-power-grid-from-cyber-threats/〔2020/6/11 確認〕
Forbes：New Platform Aims To Help Protect Power Grid From Cyber Threats https://www.forbes.com/sites/tonybradley/2019/11/10/new-platform-aims-to-help-protect-power-grid-from-cyber-threats/#78ebb9762614 〔2020/6/11 確認〕
※ 44 HELPNETSECURITY：ATT&CK for ICS: Knowledge base of techniques used by cyber adversaries https://www.helpnetsecurity.com/2020/01/08/attck-for-ics/〔2020/6/11 確認〕
MITRE：ATT&CK for Industrial Control Systems https://collaborate.mitre.org/attackics/index.php/Main_Page〔2020/6/11 確認〕
※ 45 CHATHAM HOUSE：Cybersecurity of NATO's Space-based Strategic Assets https://www.chathamhouse.org/publication/cybersecurity-nato-s-space-based-strategic-assets〔2020/6/11 確認〕
※ 46 SPACENEWS：Air Force to require cybersecurity audits of commercial satellite communications providers https://spacenews.com/air-force-to-require-cybersecurity-audits-of-commercial-satellite-communications-providers/〔2020/6/11 確認〕
※ 47 WIRED：The Air Force Will Let Hackers Try to Hijack an Orbiting Satellite https://www.wired.com/story/air-force-defcon-satellite-hacking/〔2020/6/11 確認〕
AvionicsINTERNATIONAL：Air Force to Decide Which Satellite to Offer for Test at Defcon Hacker Conference https://www.aviationtoday.com/2019/12/12/air-force-decide-satellite-offer-test-defcon-hacker-conference/〔2020/6/11 確認〕
※ 48 AFCEA：DHS Builds Position, Navigation and Timing Framework https://www.afcea.org/content/dhs-builds-position-navigation-and-timing-framework〔2020/6/11 確認〕
※ 49 https://www.nisc.go.jp/active/kihon/pdf/cs2019.pdf〔2020/6/11 確認〕
※ 50 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〔2020/6/11 確認〕
※ 51 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 版を策定しました https://www.meti.go.jp/press/2019/06/20190617005/20190617005.html〔2020/6/11 確認〕
※ 52 e-Gov：ガス事業法の保安規制におけるサイバーセキュリティ対策の強化について（省令改正省令改正） https://search.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000180277〔2020/6/11 確認〕
※ 53 経済産業省：「エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン」を改定しました https://www.meti.go.jp/press/2019/12/20191227004/20191227004.html〔2020/6/11 確認〕
※ 54 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〔2020/6/11 確認〕
※ 55 IPA：制御システムのセキュリティリスク分析ガイド：過去のセミナー https://www.ipa.go.jp/security/controlsystem/pastseminar.html〔2020/6/11 確認〕
※ 56 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〔2020/6/11 確認〕
※ 57 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。
※ 58 IPA：米国発のセキュリティマネジメント成熟度の評価モデル「ES-C2M2」の解説書およびチェックシートの公開 https://www.ipa.go.jp/security/controlsystem/usenergy.html〔2020/6/11 確認〕
※ 59 IPA：JVN iPedia 脆弱性対策情報データベース https://jvndb.jvn.jp/〔2020/6/11 確認〕
※ 60 ウイルス内部に保持する、特定の IoT 機器の初期設定値やその後の変更値として用いられやすい、典型的で類推可能なログイン名とパスワードの組み合わせ。
※ 61 悪用方法の多様化の詳細に関しては、「情報セキュリティ白書 2019」の「3.2.1（2）悪用方法の多様化と被害対象の範囲拡大」（p.166）を参照。
※ 62 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。
※ 63 VPNFilter の詳細に関しては、「情報セキュリティ白書 2019」の「3.2.1（3）VPNFilter」（p.168）を参照。
※ 64 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。
※ 65 BrickerBot の詳細に関しては、「情報セキュリティ白書 2018」の「3.1.1（2）IoT 機器を破壊するウイルス「BrickerBot」」（p.163）を参照。
※ 66 Palo Alto Networks, Inc.：New Mirai Variant Targets Enterprise Wireless Presentation & Display Systems https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/〔2020/6/11 確認〕
パロアルトネットワークス株式会社：新しい Mirai 亜種、エンタープライズワイヤレスプレゼンテーションとディスプレイシステムを標的に https://unit42.paloaltonetworks.jp/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/〔2020/6/11 確認〕

※ 67 エクスプロイト：脆弱性を悪用して攻撃するためのプログラム。
※ 68 Exploit Database：WePresent WiPG-1000 - Command Injection (Metasploit) https://www.exploit-db.com/exploits/41935〔2020/6/11 確認〕
※ 69 Exploit Database：D-Link DCS-930L - (Authenticated) Remote Command Execution (Metasploit) https://www.exploit-db.com/exploits/39437〔2020/6/11 確認〕
※ 70 Exploit Database：D-Link DIR-645 / DIR-815 - 'diagnostic.php' Command Execution (Metasploit) https://www.exploit-db.com/exploits/24956〔2020/6/11 確認〕
※ 71 タイ True Corporation Public Company Limited 社が運営する ISP。
※ 72 SecLists.Org：Multiple RCE in ZyXEL / Billion / TrueOnline routers https://seclists.org/fulldisclosure/2017/Jan/40〔2020/6/11 確認〕
※ 73 Threat9 Inc.：routersploit / routersploit / modules / exploits / routers / netgear / prosafe_rce.py https://github.com/threat9/routersploit/blob/master/routersploit/modules/exploits/routers/netgear/prosafe_rce.py〔2020/6/11 確認〕
※ 74 Websec Canada：Backdoors in Zhone GPON 2520 and Alcatel Lucent I240Q https://www.websec.ca/publication/Blog/backdoors-in-Zhone-GPON-2520-and-Alcatel-Lucent-I240Q〔2020/6/11 確認〕
※ 75 Exploit Database：VideoFlow Digital Video Protection (DVP) 2.10 - Hard-Coded Credentials https://www.exploit-db.com/exploits/44387〔2020/6/11 確認〕
※ 76 Qihoo 360 Technology Co. Ltd.：The new developments Of the Fbot https://blog.netlab.360.com/the-new-developments-of-the-fbot-en/〔2020/6/11 確認〕
※ 77 Satori の詳細に関しては、「情報セキュリティ白書 2018」の「3.1.1 (3) (d) Satori ／ Okiru」(p.164) を、国内における感染急増に関しては、「情報セキュリティ白書 2018」の「3.1.2 (1) 国内における IoT 機器のウイルス感染の急増」(p.165) を参照。
※ 78 Qihoo 360 Technology Co. Ltd.：Fbot, A Satori Related Botnet Using Blockchain DNS System https://blog.netlab.360.com/threat-alert-a-new-worm-fbot-cleaning-adbminer-is-using-a-blockchain-based-dns-en/〔2020/6/11 確認〕
※ 79 Sophos Ltd.：Author of record-setting IoT botnets pleads guilty https://nakedsecurity.sophos.com/2019/09/05/author-of-record-setting-iot-botnets-pleads-guilty/〔2020/6/11 確認〕
※ 80 Trend Micro Incorporated：Mirai Variant Spotted Using Multiple Exploits, Targets Various Routers https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mirai-variant-spotted-using-multiple-exploits-targets-various-routers/〔2020/6/11 確認〕
※ 81 Palo Alto Networks, Inc.：New Mirai Variant Adds 8 New Exploits, Targets Additional IoT Devices https://unit42.paloaltonetworks.com/new-mirai-variant-adds-8-new-exploits-targets-additional-iot-devices/〔2020/6/11 確認〕
パロアルトネットワークス株式会社：新たな Mirai 亜種 8 つのエクスプロイトを追加 新たな IoT デバイスを標的化 https://www.paloaltonetworks.jp/company/in-the-news/2019/new-mirai-variant-adds-8-new-exploits-targets-additional-iot-devices〔2020/6/11 確認〕
※ 82 Palo Alto Networks, Inc.：iocs / mirai / ECHOBOT_6thAug2019.md https://github.com/pan-unit42/iocs/blob/master/mirai/ECHOBOT_6thAug2019.md〔2020/6/11 確認〕
※ 83 Palo Alto Networks, Inc.：Mirai Variant ECHOBOT Resurfaces with 13 Previously Unexploited Vulnerabilities https://unit42.paloaltonetworks.com/mirai-variant-echobot-resurfaces-with-13-previously-unexploited-vulnerabilities/〔2020/6/11 確認〕
パロアルトネットワークス株式会社：Mirai 亜種 ECHOBOT がこれまで悪用されたことのない 13 件の脆弱性を悪用 https://unit42.paloaltonetworks.jp/mirai-variant-echobot-resurfaces-with-13-previously-unexploited-vulnerabilities/〔2020/6/11 確認〕
※ 84 Exploit Database：MiCasaVerde VeraLite - Remote Code Execution https://www.exploit-db.com/exploits/40589〔2020/6/11 確認〕
※ 85 vuldb.com：VULDB 94801 ZyXEL P660HN-T v1 ViewLog.asp remote_host privilege escalation https://vuldb.com/?id.94801〔2020/6/11 確認〕
※ 86 Exploit Database：Linksys E-series - Remote Code Execution https://www.exploit-db.com/exploits/31683〔2020/6/11 確認〕
※ 87 Exploit Database：ThinkPHP 5.0.23/5.1.31 - Remote Code Execution https://www.exploit-db.com/exploits/45978〔2020/6/11 確認〕
※ 88 W Box Technologies：IP Cameras/NVRs/DVRs Secure Activation Procedure https://www.wboxtech.com/content/files/product_categories/ip_cameras/IPC-NVR-DVR-secure-activation.pdf〔2020/6/11 確認〕
※ 89 Exploit Database：OpenDreamBox 2.0.0 Plugin WebAdmin - Remote Code Execution https://www.exploit-db.com/exploits/42293〔2020/6/11 確認〕
※ 90 VMware, Inc：VMware Security Advisories VMSA-2018-0011.2 Unauthenticated Command Injection vulnerability in VMware SD-WAN Edge by VeloCloud https://www.vmware.com/security/advisories/VMSA-2018-0011.html〔2020/6/11 確認〕
※ 91 Exploit Database：Dell KACE Systems Management Appliance (K1000) 6.4.120756 - Unauthenticated Remote Code Execution https://www.exploit-db.com/exploits/46684
※ 92 Exploit Database：Hootoo HT-05 - Remote Code Execution (Metasploit) https://www.exploit-db.com/exploits/46143〔2020/6/11 確認〕
※ 93 Exploit Database：ASUS DSL-N12E_C1 1.1.2.3_345 - Remote Command Execution https://www.exploit-db.com/exploits/45135〔2020/6/11 確認〕
※ 94 Exploit Database：Belkin Wemo UPnP - Remote Code Execution (Metasploit) https://www.exploit-db.com/exploits/46436〔2020/6/11 確認〕
※ 95 Exploit Database：NETGEAR ReadyNAS Surveillance 1.4.3-16 - Remote Command Execution https://www.exploit-db.com/exploits/42956〔2020/6/11 確認〕
※ 96 Exploit Database：NUUO NVRmini - 'upgrade_handle.php' Remote Command Execution https://www.exploit-db.com/exploits/45070〔2020/6/11 確認〕
※ 97 IT Security Research by Pierre：Multiple vulnerabilities found in Wireless IP Camera (P2P) WIFICAM cameras and vulnerabilities in custom http server https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html〔2020/6/11 確認〕
※ 98 Exploit Database：Blue Angel Software Suite - Command Execution https://www.exploit-db.com/exploits/46792〔2020/6/11 確認〕
※ 99 Rubicon Communications, LLC：pfSense Default Username and Password https://docs.netgate.com/pfsense/en/latest/usermanager/pfsense-default-username-and-password.html〔2020/6/11 確認〕
※ 100 Aerohive Networks, Inc.：Default username and password https://thehivecommunity.aerohive.com/s/question/0D50c00006da0wW/default-username-and-password?language=en_US〔2020/4/14 確認〕
※ 101 Exploit Database：Crestron AM-100 - Multiple Vulnerabilities https://www.exploit-db.com/exploits/40813〔2020/6/11 確認〕
※ 102 Exploit Database：EyeLock nano NXT 3.5 - Remote Code Execution https://www.exploit-db.com/exploits/40228〔2020/6/11 確認〕
※ 103 Exploit Database：Iris ID IrisAccess ICU 7000-2 - Remote Command Execution https://www.exploit-db.com/exploits/40166〔2020/6/11 確認〕
※ 104 Exploit Database：Xfinity Gateway - Remote Code Execution https://www.exploit-db.com/exploits/40856〔2020/6/11 確認〕
※ 105 Exploit Database：BEWARD N100 H.264 VGA IP Camera M2.1.6 - Remote Code Execution https://www.exploit-db.com/exploits/46319〔2020/6/11 確認〕
※ 106 Exploit Database：Fritz!Box Webcm - Command Injection (Metasploit) https://www.exploit-db.com/exploits/32753〔2020/6/11 確認〕
※ 107 Exploit Database：FLIR Thermal Camera FC-S/PT - Command Injection https://www.exploit-db.com/exploits/42788〔2020/6/11 確認〕
※ 108 Exploit Database：SAPIDO RB-1732 - Remote Command Execution https://www.exploit-db.com/exploits/47031〔2020/6/11 確認〕
※ 109 Exploit Database：AVCON6 systems management platform - OGNL Remote Command Execution https://www.exploit-db.com/exploits/47379〔2020/6/11 確認〕
※ 110 Exploit Database：Sar2HTML 3.2.1 - Remote Command Execution https://www.exploit-db.com/exploits/47204〔2020/6/11 確認〕
※ 111 Exploit Database：ACTi ASOC 2200 Web Configurator 2.6 - Remote Command Execution https://www.exploit-db.com/

exploits/16993〔2020/6/11 確認〕
※ 112 Exploit Database：3Com OfficeConnect - Code Execution https://www.exploit-db.com/exploits/9862〔2020/6/11 確認〕
※ 113 Exploit Database：CCBILL CGI - 'ccbillx.c' 'whereami.cgi' Remote Code Execution https://www.exploit-db.com/exploits/53〔2020/6/11 確認〕
※ 114 Trend Micro Incorporated：New Mirai Variant Uses Multiple Exploits to Target Routers and Other Devices https://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-variant-uses-multiple-exploits-to-target-routers-and-other-devices/〔2020/6/11 確認〕
※ 115 RCE（Remote Code Execution）：リモートコード実行。
※ 116 SSD Secure Disclosure：SSD Advisory – Vacron NVR Remote Command Execution https://ssd-disclosure.com/ssd-advisory-vacron-nvr-remote-command-execution/〔2020/6/11 確認〕
※ 117 Mirai の亜種の一つで、多くの脆弱性を取り込んだ 2018 年に発見された代表的なウイルスの一つ。Omni とその亜種の詳細に関しては、「情報セキュリティ白書 2019」の「3.2.1 (1) (d) Omni」「3.2.1 (1) (g) Omni の亜種」(p.164)を参照。
※ 118 Hakai の詳細に関しては、「情報セキュリティ白書 2019」の「3.2.1 (1) (k) Hakai」(p.166)を参照。
※ 119 Exploit Database：Multiple CCTV-DVR Vendors - Remote Code Execution https://www.exploit-db.com/exploits/39596〔2020/6/11 確認〕
※ 120 Yowai の詳細に関しては、「情報セキュリティ白書 2019」の「3.2.1 (1) (j) Yowai」(p.166)を参照。
※ 121 Exploit Database：D-Link Devices - UPnP SOAP TelnetD Command Execution (Metasploit) https://www.exploit-db.com/exploits/28333〔2020/6/11 確認〕
※ 122 Exploit Database：Eir D1000 Wireless Router - WAN Side Remote Command Injection (Metasploit) https://www.exploit-db.com/exploits/40740〔2020/6/11 確認〕
※ 123 Exploit Database：Netgear DGN1000 1.1.00.48 - 'Setup.cgi' Remote Code Execution (Metasploit) https://www.exploit-db.com/exploits/43055〔2020/6/11 確認〕
※ 124 Exploit Database：NETGEAR R7000 / R6400 - 'cgi-bin' Command Injection (Metasploit) https://www.exploit-db.com/exploits/41598〔2020/6/11 確認〕
※ 125 Exploit Database：MVPower DVR TV-7104HE 1.8.4 115215B9 - Shell Command Execution (Metasploit) https://www.exploit-db.com/exploits/41471〔2020/6/11 確認〕
※ 126 Miori の詳細に関しては、「情報セキュリティ白書 2019」の「3.2.1 (1) (i) Miori ／ IZ1H9 ／ APEP」(p.165)を参照。
※ 127 Trend Micro Incorporated：The Reigning King of IP Camera Botnets and its Challengers https://blog.trendmicro.com/trendlabs-security-intelligence/reigning-king-ip-camera-botnets-challengers/
※ 128 Trend Micro Incorporated：New Miori Variant Uses Unique Protocol to Communicate with C&C https://blog.trendmicro.com/trendlabs-security-intelligence/new-miori-variant-uses-unique-protocol-to-communicate-with-cc/〔2020/6/11 確認〕
※ 129 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。
※ 130 トレンドマイクロ株式会社：Tor ネットワークを利用する「Mirai」亜種 IoT マルウェアを発見 https://blog.trendmicro.co.jp/archives/21920〔2020/6/11 確認〕
※ 131 Trend Micro Incorporated：Back-to-Back Campaigns: Neko, Mirai, and Bashlite Malware Variants Use Various Exploits to Target Several Routers, Devices https://blog.trendmicro.com/trendlabs-security-intelligence/back-to-back-campaigns-neko-mirai-and-bashlite-malware-variants-use-various-exploits-to-target-several-routers-devices/〔2020/6/11 確認〕
※ 132 Wikimedia Foundation：Malicious attack on Wikipedia—What we know, and what we're doing https://wikimediafoundation.org/news/2019/09/07/malicious-attack-on-wikipedia-what-we-know-and-what-were-doing/〔2020/6/11 確認〕
Blizzard Entertainment, Inc.：Recent DDoS Attacks Impacting Game Service https://us.forums.blizzard.com/en/wow/t/recent-ddos-attacks-impacting-game-service/290063〔2020/6/11 確認〕
※ 133 Twitch の動画配信者が使用可能な同名のボット（ツール）「Moobot」(https://moo.bot/)とは別物である。
※ 134 株式会社インターネットイニシアティブ：Wikipedia, Twitch, Blizzard への DDoS 攻撃 https://sect.iij.ad.jp/d/2019/09/175257.html〔2020/6/11 確認〕
※ 135 Exploit Database：HiSilicon DVR Devices - Remote Code Execution https://www.exploit-db.com/exploits/44004〔2020/6/11 確認〕
※ 136 Qihoo 360 Technology Co. Ltd.：The Botnet Cluster on the 185.244.25.0/24 https://blog.netlab.360.com/the-botnet-cluster-on-185-244-25-0-24-en/〔2020/6/11 確認〕
※ 137 Trend Micro Incorporated：DDoS Attacks and IoT Exploits: New Activity from Momentum Botnet https://blog.trendmicro.com/trendlabs-security-intelligence/ddos-attacks-and-iot-exploits-new-activity-from-momentum-botnet/〔2020/6/11 確認〕
※ 138 SourceSec Security Research：Hacking D-Link Routers With HNAP https://regmedia.co.uk/2016/11/07/dlink_hnap_captcha.pdf〔2020/6/11 確認〕
※ 139 Exploit Database：ThinkPHP 5.X - Remote Command Execution https://www.exploit-db.com/exploits/46150〔2020/6/11 確認〕
※ 140 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/〔2020/6/11 確認〕
※ 141 Palo Alto Networks, Inc.：New Mirai Variant Targets Zyxel Network-Attached Storage Devices https://unit42.paloaltonetworks.com/new-mirai-variant-mukashi/〔2020/6/11 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/〔2020/6/11 確認〕
※ 142 Exploit Database：Netlink GPON Router 1.0.11 - Remote Code Execution https://www.exploit-db.com/exploits/48225〔2020/6/11 確認〕
※ 143 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〔2020/6/11 確認〕
※ 144 Trend Micro Incorporated：Bashlite IoT Malware Updated with Mining and Backdoor Commands, Targets WeMo Devices https://blog.trendmicro.com/trendlabs-security-intelligence/bashlite-iot-malware-updated-with-mining-and-backdoor-commands-targets-wemo-devices/〔2020/6/11 確認〕
※ 145 Palo Alto Networks, Inc.：Home & Small Office Wireless Routers Exploited to Attack Gaming Servers https://unit42.paloaltonetworks.com/home-small-office-wireless-routers-exploited-to-attack-gaming-servers/〔2020/6/11 確認〕
パロアルトネットワークス株式会社：Gafgyt: 小規模オフィス / ホーム無線 LAN ルーターに感染しゲームサーバーを攻撃するボットネット https://unit42.paloaltonetworks.jp/home-small-office-wireless-routers-exploited-to-attack-gaming-servers/〔2020/6/11 確認〕
※ 146 JenX／Jennifer の詳細に関しては、「情報セキュリティ白書 2019」の「3.2.1 (1) (b) JenX ／ Jennifer」(p.163)を参照。
※ 147 S.C. Bitdefender S.R.L.：New Hide 'N Seek IoT Botnet using custom-built Peer-to-Peer communication spotted in the wild https://labs.bitdefender.com/2018/01/new-hide-n-seek-iot-botnet-using-custom-built-peer-to-peer-communication-spotted-in-the-wild/〔2020/6/11 確認〕
※ 148 Palo Alto Networks, Inc.：Hide 'N Seek Botnet Updates Arsenal with Exploits Against Nexus Repository Manager & ThinkPHP https://unit42.paloaltonetworks.com/hide-n-seek-botnet-updates-arsenal-with-exploits-against-nexus-repository-manager-thinkphp/〔2020/6/11 確認〕
パロアルトネットワークス株式会社：Hide 'N Seek ボットネット さらなるエクスプロイト追加で攻撃力を増強 https://unit42.paloaltonetworks.jp/hide-n-seek-botnet-updates-arsenal-with-exploits-against-nexus-repository-manager-thinkphp/〔2020/6/11 確認〕
※ 149 Exploit Database：Apache CouchDB < 2.1.0 - Remote Code Execution https://www.exploit-db.com/exploits/44913〔2020/6/11 確認〕
※ 150 Exploit Database：OrientDB 2.2.2 < 2.2.22 - Remote Code Execution (Metasploit) https://www.exploit-db.com/exploits/42965〔2020/6/11 確認〕
※ 151 Exploit Database：AVTECH IP Camera / NVR / DVR Devices - Multiple Vulnerabilities https://www.exploit-db.com/exploits/40500〔2020/6/11 確認〕

※ 152 Sekurak：TP-Link http/tftp backdoor　https://sekurak.pl/tp-link-httptftp-backdoor/〔2020/6/11 確認〕
※ 153 Exploit Database：NETGEAR DGN1000 / DGN2200 - Multiple Vulnerabilities　https://www.exploit-db.com/exploits/25978〔2020/6/11 確認〕
※ 154 SecLists.Org：IS-2010-002 - Linksys WAP54Gv3 Remote Debug Root Shell　https://seclists.org/bugtraq/2010/Jun/93〔2020/6/11 確認〕
※ 155 Qihoo 360 Technology Co. Ltd.：Mozi, Another Botnet Using DHT　https://blog.netlab.360.com/mozi-another-botnet-using-dht/〔2020/6/11 確認〕
※ 156 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〔2020/6/11 確認〕
※ 157 S.C. Bitdefender S.R.L.：Hold My Beer Mirai - Spinoff Named 'LiquorBot' Incorporates Cryptomining　https://labs.bitdefender.com/2020/01/hold-my-beer-mirai-spinoff-named-liquorbot-incorporates-cryptomining/〔2020/6/11 確認〕
※ 158 Palo Alto Networks, Inc.：Muhstik Botnet Attacks Tomato Routers to Harvest New IoT Devices　https://unit42.paloaltonetworks.com/muhstik-botnet-attacks-tomato-routers-to-harvest-new-iot-devices/〔2020/6/11 確認〕
パロアルトネットワークス株式会社：Muhstik ボットネットが Tomato ルータを攻撃 新しい IoT デバイスを「収穫」　https://unit42.paloaltonetworks.jp/muhstik-botnet-attacks-tomato-routers-to-harvest-new-iot-devices/〔2020/6/11 確認〕
※ 159 https://www.shodan.io/〔2020/6/11 確認〕
※ 160 Just an independent security researcher.（個人ブログ）：Hajime: A follow-up　https://x86.re/blog/hajime-a-follow-up/〔2020/6/11 確認〕
※ 161 株式会社インターネットイニシアティブ：2018 年の IoT ボット観測状況と最近の動向　https://sect.iij.ad.jp/d/2019/01/288147.html〔2020/6/11 確認〕
※ 162 Kaspersky Lab：Hajime, the mysterious evolving botnet　https://securelist.com/hajime-the-mysterious-evolving-botnet/78160/〔2020/6/11 確認〕
※ 163 Exploit Database：MikroTik RouterOS < 6.38.4 (MIPSBE) - 'Chimay Red' Stack Clash Remote Code Execution　https://www.exploit-db.com/exploits/44283〔2020/6/11 確認〕
※ 164 株式会社インターネットイニシアティブ：Hajime ボットの観測状況　https://sect.iij.ad.jp/d/2017/09/293589.html〔2020/6/11 確認〕
※ 165 株式会社インターネットイニシアティブ：Hajime ボットによる 8291/tcp へのスキャン活動　https://sect.iij.ad.jp/d/2018/03/293998.html〔2020/6/11 確認〕
※ 166 DarkReading（Informa PLC）：Why Bricking Vulnerable IoT Devices Comes with Unintended Consequences　https://www.darkreading.com/iot/why-bricking-vulnerable-iot-devices-comes-with-unintended-consequences-/a/d-id/1336009〔2020/6/11 確認〕
※ 167 ZDNet（CBS Interactive Inc.）：New Silex malware is bricking IoT devices, has scary plans　https://www.zdnet.com/article/new-silex-malware-is-bricking-iot-devices-has-scary-plans/〔2020/6/11 確認〕
※ 168 https://twitter.com/_larry0/status/1143532888538984448〔2020/6/11 確認〕
※ 169 https://notice.go.jp/
※ 170 総務省・NICT：IoT 機器調査及び利用者への注意喚起の取組「NOTICE」の実施　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00011.html〔2020/6/11 確認〕
※ 171 インターネット上で起こる大規模攻撃への迅速な対応を目指したサイバー攻撃観測・分析・対策システムを用いて、ダークネットや各種ハニーポットによるサイバー攻撃の大規模観測及びその原因（マルウェア）等の分析を実施するプロジェクト。　https://www.nicter.jp/〔2020/6/11 確認〕
※ 172 総務省・NICT・一般社団法人 ICT-ISAC：マルウェアに感染している IoT 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_00025.html〔2020/6/11 確認〕
※ 173 総務省・NICT・一般社団法人 ICT-ISAC：脆弱な IoT 機器及びマルウェアに感染している IoT 機器の利用者への注意喚起の実施状況　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00033.html〔2020/6/11 確認〕
総務省・NICT・一般社団法人 ICT-ISAC：脆弱な IoT 機器及びマルウェアに感染している IoT 機器の利用者への注意喚起の実施状況（2019 年度第 2 四半期）　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00043.html〔2020/6/11 確認〕
総務省・NICT・一般社団法人 ICT-ISAC：脆弱な IoT 機器及びマルウェアに感染している IoT 機器の利用者への注意喚起の実施状況（2019 年度第 3 四半期）　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00058.html〔2020/6/11 確認〕
総務省・NICT・一般社団法人 ICT-ISAC：脆弱な IoT 機器及びマルウェアに感染している IoT 機器の利用者への注意喚起の実施状況（2019 年度）　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00067.html〔2020/6/11 確認〕
※ 174 株式会社インターネットイニシアティブ：2019 年の IoT ボット観測状況　https://sect.iij.ad.jp/d/2020/02/030029.html〔2020/6/11 確認〕
※ 175 IPA：入退管理システム　チェックリスト　https://www.ipa.go.jp/security/jisec/choutatsu/ecs/index.html〔2020/6/11 確認〕
※ 176 IPA：情報システム等の脆弱性情報の取扱いにおける報告書を公開　https://www.ipa.go.jp/security/fy2019/reports/vuln_handling/index.html〔2020/6/11 確認〕
※ 177 JPCERT/CC：IoT セキュリティチェックリスト　https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html〔2020/6/11 確認〕
※ 178 CCDS：協議会・研究会公開資料　https://www.ccds.or.jp/public_document/index.html〔2020/6/11 確認〕
※ 179 https://www.ccds.or.jp/certification/document/IoT 分野共通セキュリティ要件ガイドライン 2019 年版 _ver2.0.pdf〔2020/6/11 確認〕
※ 180 https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2019/11/Guide_to_theCSA_IoT_Controls_Framework_J-1.pdf〔2020/6/11 確認〕
※ 181 https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2019/11/CSA_IoT_Controls_Framework_Final_J.pdf〔2020/6/11 確認〕
※ 182 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〔2020/6/11 確認〕
※ 183 DLPA：ご家庭で Wi-Fi ルーターをより安全にお使い頂くために　https://dlpa.jp/wifi_support/〔2020/6/11 確認〕
※ 184 NIST：Considerations for a Core IoT Cybersecurity Capabilities Baseline　https://www.nist.gov/system/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf〔2020/6/11 確認〕
※ 185 NIST：NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks　https://csrc.nist.gov/publications/detail/nistir/8228/final〔2020/6/11 確認〕
※ 186 NIST：NISTIR 8267(Draft) Security Review of Consumer Home Internet of Things (IoT) Products　https://csrc.nist.gov/publications/detail/nistir/8267/draft〔2020/6/11 確認〕
※ 187-1　NIST：NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers　https://csrc.nist.gov/publications/detail/nistir/8259/final〔2020/6/26 確認〕
※ 187-2　NIST：NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline　https://csrc.nist.gov/publications/detail/nistir/8259a/final〔2020/6/26 確認〕
※ 188 ENISA：IoT Security Standards Gap Analysis　https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis〔2020/6/11 確認〕
※ 189 IPA：欧州ネットワーク情報セキュリティ機関（ENISA）「IoT のセキュリティ標準のギャップ分析」　https://www.ipa.go.jp/files/000076742.pdf〔2020/6/11 確認〕
※ 190 ENISA：Good Practices for Security of IoT - Secure Software Development Lifecycle　https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1〔2020/6/11 確認〕
※ 191 ENISA：ENISA good practices for security of Smart Cars　https://www.enisa.europa.eu/publications/smart-cars〔2020/6/11 確認〕
※ 192 ETSI：ETSI EN 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〔2020/7/3 確認〕
※ 193 総務省：端末設備等規則及び電気通信主任技術者規則の一部を改正する省令（平成 31 年総務省令第 12 号）　https://www.soumu.go.jp/main_content/000611859.pdf〔2020/6/11 確認〕
※ 194 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 1 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_02000179.html〔2020/6/11 確認〕
※ 195 California Legislative Information：SB-327 Information privacy: connected devices.(2017-2018)　https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327〔2020/6/11 確認〕

※ 196 英国政府（GOV.UK）：Government to strengthen security of internet-connected products https://www.gov.uk/government/news/government-to-strengthen-security-of-internet-connected-products〔2020/6/11 確認〕
※ 197 CCDS：CCDS サーティフィケーションプログラムの概要 https://www.ccds.or.jp/certification/index.html〔2020/6/11 確認〕
※ 198 トレンドマイクロ株式会社：家庭内ネットワークに繋がるスマート家電の安全性を診断する無料アプリ「スマートホームスキャナー™」を提供開始 https://www.trendmicro.com/ja_jp/about/press-release/2020/pr-20200302-03.html〔2020/6/11 確認〕
※ 199 警視庁：遺失物取扱状況（令和元年中） https://www.keishicho.metro.tokyo.jp/about_mpd/jokyo_tokei/kakushu/kaikei.html〔2020/6/11 確認〕
※ 200 IPA: パスワードと安全な付き合い方を優しくご紹介! https://www.ipa.go.jp/security/keihatsu/munekyun-pw/password/index.html〔2020/6/11 確認〕
※ 201 https://www.is702.jp/special/3533/partner/12_t/〔2020/6/11 確認〕
※ 202 https://www.mcafee.com/consumer/ja-jp/store/m0/securitynews/news-086.html〔2020/6/11 確認〕
※ 203 PIO-NET（Practical Living Information Online Network System：全国消費生活情報ネットワークシステム）：国民生活センターと全国の消費生活センターが受付けた消費生活に関する相談の情報が蓄積されたデータベース。
※ 204 http://www.kokusen.go.jp/pdf/n-20190808_1.pdf〔2020/6/11 確認〕
※ 205 一般社団法人日本クレジット協会：学校等への教材提供 https://www.j-credit.or.jp/education/school/provide.html〔2020/6/11 確認〕
※ 206 https://www.soumu.go.jp/main_content/000225177.pdf〔2020/6/11 確認〕
※ 207 警察庁：令和元年における特殊詐欺認知・検挙状況等について https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2019.pdf〔2020/6/11 確認〕
※ 208 毎日新聞：特殊詐欺 実行犯役募集に警告返信 愛知県警、ツイッターで「人生台無しに」 https://mainichi.jp/articles/20190802/ddm/012/040/094000c〔2020/6/11 確認〕
※ 209 http://www.pref.osaka.lg.jp/chiantaisaku/furikome2607/ukekohen.html〔2020/6/11 確認〕
※ 210 公益財団法人東京オリンピック・パラリンピック競技大会組織委員会：東京 2020 大会の新開催日程を発表 https://tokyo2020.org/ja/news/news-20200330-04-ja〔2020/6/11 確認〕
※ 211 総務省：情報通信白書平成 30 年版 （1）インターネット利用の広がり https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd142110.html〔2020/6/11 確認〕
※ 212 産経新聞：「自首して」「あなたも指名手配」…あおり運転同乗女と間違われた女性が会見 https://www.sankei.com/affairs/news/190823/afr1908230024-n1.html〔2020/6/11 確認〕
※ 213 https://www.keishicho.metro.tokyo.jp/smph/kurashi/cyber/joho/truth.html〔2020/6/11 確認〕
※ 214 https://www.it-saga.jp/kyouzai/sns-seigikan/〔2020/6/11 確認〕
※ 215 https://fij.info/coronavirus-feature〔2020/6/11 確認〕
※ 216 公益財団法人日本ユニセフ協会：新型肺炎 世界で広がる誤情報 ユニセフ、注意呼びかけ https://www.unicef.or.jp/news/2020/0039.html〔2020/6/11 確認〕
※ 217 株式会社 JTB 総合研究所:世界中の若者が熱狂する「e スポーツ」の魅力について https://www.tourism.jp/tourism-database/column/2019/05/esports-attraction/〔2020/6/11 確認〕
※ 218 2020 年以降の数値は、2020 年 2 月時点での予測。
株式会社 KADOKAWA Game Linkage：2019 年 日本 e スポーツ市場規模は 60 億円を突破。 https://kadokawagamelinkage.jp/news/pdf/news200213.pdf〔2020/6/11 確認〕
※ 219 https://www.ibaraki-esports.com/e-47/index.html〔2020/6/11 確認〕
※ 220 経済産業省：「e スポーツを活性化させるための方策に関する検討会」の報告書が公表されました https://www.meti.go.jp/press/2019/03/20200313003/20200313003.html〔2020/6/11 確認〕
※ 221 Newsweek：e スポーツは賞金 300 万ドルの巨大市場に成長中 https://www.newsweekjapan.jp/stories/world/2019/09/e300.php〔2020/6/11 確認〕
※ 222 https://www.is702.jp/manga/3567/partner/200_k/〔2020/6/11 確認〕
※ 223 WHO：Gaming disorder https://www.who.int/features/qa/gaming-disorder/en/〔2020/6/11 確認〕
※ 224 独立行政法人国民生活センター：病気認定されたゲーム障害の現状と今後 http://www.kokusen.go.jp/wko/pdf/wko-201910_02.pdf〔2020/6/11 確認〕
※ 225 IPA：活動事例 https://www.ipa.go.jp/security/event/hyogo/2019/awd_katsudo.html〔2020/6/11 確認〕
※ 226 警察庁サイバー犯罪対策プロジェクト：サイバー防犯ボランティア活動事例 https://www.npa.go.jp/cyber/policy/volunteer/fukuoka.html〔2020/6/11 確認〕
※ 227 明治大学：明大 SNS スタイル（SNS 利用時の注意） https://www.meiji.ac.jp/koho/social_media/sns.html〔2020/6/11 確認〕
※ 228 総務省統計局：人口推計（2019 年（令和元年）10 月 1 日現在）結果の要約 https://www.stat.go.jp/data/jinsui/2019np/index.html〔2020/6/11 確認〕
※ 229 https://www.ipa.go.jp/security/event/hyogo/2018/sakuhin_hyogo.html〔2020/6/11 確認〕
※ 230 朝日新聞デジタル：JAL、パンプス強制を撤廃 「ジェンダー平等に配慮」 https://www.asahi.com/articles/ASN3R67D6N3RULFA03D.html〔2020/6/11 確認〕
※ 231 毎日新聞：SNS で誹謗中傷する人に共通する意識 木村花さん急死の危うい背景 https://mainichi.jp/articles/20200529/k00/00m/040/177000c〔2020/6/11 確認〕
※ 232 https://juas.or.jp/cms/media/2020/05/JUAS_IT2020_original.pdf?20200522〔2020/7/18 確認〕
※ 233 総務省：令和元年通信利用動向調査の結果 https://www.soumu.go.jp/johotsusintokei/statistics/data/200529_1.pdf〔2020/7/18 確認〕
※ 234 各府省情報化統括責任者（CIO）連絡会議：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 https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf〔2020/7/18 確認〕
※ 235 https://www.ipa.go.jp/security/ismap/index.html〔2020/7/18 確認〕
※ 236 piyolog：AWS 東京リージョンで発生した大規模障害についてまとめてみた https://piyolog.hatenadiary.jp/entry/2019/08/23/174801〔2020/7/18 確認〕
PayPay 株式会社：PayPay でお支払いやチャージができない（復旧済み） https://paypay.ne.jp/notice/20190823/01/〔2020/7/18 確認〕
株式会社ミクシィ：mixi（公式） https://twitter.com/mixi_official/status/1164754947142868993〔2020/7/18 確認〕
株式会社サイバーエージェント：ピグパーティ［ピグパ］ https://twitter.com/PiggPARTY/status/1164811966856085504〔2020/7/18 確認〕
株式会社ユニクロ：接続障害のお知らせ https://twitter.com/UNIQLO_JP/status/1164792224267157505〔2020/7/18 確認〕
株式会社東急ハンズ：復旧のお知らせ https://twitter.com/TokyuHands/status/1164841868569407488〔2020/7/18 確認〕
楽天株式会社：【復旧済み】ラクマの機能がご利用できない不具合が発生していました https://news.fril.jp/entry/2019/08/23/150607〔2020/7/18 確認〕
スターバックスコーヒージャパン株式会社：システム障害のお知らせ https://www.starbucks.co.jp/notice/20193149.php〔2020/7/18 確認〕
※ 237 Amazon Web Services, Inc.:東京リージョン（AP-NORTHEAST-1）で発生した Amazon EC2 と Amazon EBS の事象概要 https://aws.amazon.com/jp/message/56489/〔2020/7/18 確認〕
※ 238 Publickey：Microsoft Azure、DNS の設定変更に失敗して全世界的にサービス障害。日本は十連休中だったのが不幸中の幸いか https://www.publickey1.jp/blog/19/microsoft_azuredns.html〔2020/7/18 確認〕
※ 239 Google 社：An update on Sunday's service disruption https://cloud.google.com/blog/topics/inside-google-cloud/an-update-on-sundays-service-disruption〔2020/7/18 確認〕
Google 社：Google Cloud Networking Incident #19009 https://status.cloud.google.com/incident/cloud-networking/19009〔2020/7/18 確認〕
※ 240 Publickey：Google Cloud や YouTube の障害は「数台のサーバへの設定変更のつもりが、誤って複数リージョンの多数のサーバに適用されてしまった」。Google が説明 https://www.publickey1.jp/blog/19/google_cloudyoutubegoogle.html〔2020/7/18 確認〕
※ 241 piyolog：Office 365 のメール受信障害についてまとめてみた https://piyolog.hatenadiary.jp/entry/2019/11/20/063815〔2020/7/18 確認〕
※ 242 日本電子計算株式会社：「Jip-Base」の障害における復旧状況のご報告（第 3 報） https://www.jip.co.jp/news/20200110〔2020/7/18 確認〕

INTERNET Watch：53 自治体でシステム障害、7 割復旧も全面復旧の見通し立たず――日本電子計算が謝罪　https://internet.watch.impress.co.jp/docs/news/1224846.html〔2020/7/18 確認〕
piyolog：類例報告過去 4 件の不具合で発生した自治体専用 IaaS のシステム障害についてまとめてみた　https://piyolog.hatenadiary.jp/entry/2019/12/11/063826〔2020/7/18 確認〕
※ 243 Server Side Request Forgery（SSRF）：公開サーバ等の権限を悪用してイントラネット内のサーバに不正なコマンドを送る攻撃。
※ 244 Capital One 社：Capital One Announces Data Security Incident Pres　https://www.capitalone.com/about/newsroom/capital-one-announces-data-security-incident/〔2020/7/18 確認〕
piyolog：SSRF 攻撃による Capital One の個人情報流出についてまとめてみた　https://piyolog.hatenadiary.jp/entry/2019/08/06/062154〔2020/7/18 確認〕
※ 245 https://www.lac.co.jp/lacwatch/pdf/20200130_cecreport_vol8.pdf〔2020/7/18 確認〕
※ 246 日本経済新聞:FB のデータ、アプリ開発会社が 5 億件超を「放置」　https://www.nikkei.com/article/DGXMZO43311990U9A400C1000000/〔2020/7/18 確認〕
UpGuard, Inc.：Losing Face: Two More Cases of Third-Party Facebook App Data Exposure　https://www.upguard.com/breaches/facebook-user-data-leak〔2020/7/18 確認〕
※ 247 株式会社オージス総研：「宅ふぁいる便」サービスにおける不正アクセスについて　～お客さま情報の漏洩について（お詫びとご報告）～　https://www.ogis-ri.co.jp/news/1272165_6734.html〔2020/7/18 確認〕
※ 248 ビジネス＋ IT：宅ふぁいる便の衝撃的漏えい、しかしパスワードの平文保存は「超レア」と言えない現実　https://www.sbbit.jp/article/cont1/36041〔2020/7/18 確認〕
※ 249 株式会社オージス総研：「宅ふぁいる便」サービス終了のお知らせ（2020 年 1 月 14 日）　https://www.ogis-ri.co.jp/news/20200114_001.html〔2020/7/18 確認〕
※ 250 NIST：SP 800-207(Draft) Zero Trust Architecture (2nd Draft)　https://csrc.nist.gov/publications/detail/sp/800-207/draft〔2020/7/18 確認〕
※ 251 例えば Microsoft Azuri の Active Directory に基づく ID ベース認証強化対策等。
Microsoft 社：Zero Trust part 1: Identity and access management　https://www.microsoft.com/security/blog/2018/12/17/zero-trust-part-1-identity-and-access-management/〔2020/7/18 確認〕
※ 252 CSA ジャパン：クラウド時代に求められる最新の認証方式　https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2018/12/SDP_guide_160408_2.pdf〔2020/7/18 確認〕
※ 253 https://cloudsecurityalliance.org/〔2020/7/18 確認〕
※ 254 CSA ジャパン：Software Defined Perimeter アーキテクチャガイド　https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2020/03/sdp_architecture_guide_v2_J_FINAL.pdf〔2020/7/18 確認〕
※ 255 クラウドネイティブソフトウェア：クラウドネイティブとは、クラウド環境でスケーラブルなアプリケーションを構築するためのソフトウェア実装・運用手法を指す。代表的な手法としてコンテナがある。
※ 256 https://www.cncf.io/〔2020/7/18 確認〕
※ 257 IDC Japan 株式会社：2020 年 国内コンテナ／ Kubernetes に関するユーザー導入調査結果を発表　https://www.idc.com/getdoc.jsp?containerId=prJPJ46289720〔2020/7/18 確認〕
※ 258 NIST：NIST SP800-190 Application Container Security Guide　https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf〔2020/7/18 確認〕
※ 259 Palo Alto Networks, Inc.：Cloudy with a Chance of Entropy　https://www.paloaltonetworks.com/resources/research/unit42-cloud-with-a-chance-of-entropy〔2020/7/18 確認〕
※ 260 神奈川県：リース契約満了により返却したハードディスクの盗難及び再発防止策等について　https://www.pref.kanagawa.jp/docs/fz7/cnt/p0273317.html?pk_campaign=top&pk_kwd=hdd〔2020/7/18 確認〕
※ 261 https://www.ipa.go.jp/files/000082277.pdf〔2020/7/18 確認〕
※ 262 IPA：Zoom の脆弱性対策について　https://www.ipa.go.jp/security/ciadr/vul/alert20200403.html〔2020/7/18 確認〕
※ 263 Fortune：Zoom meetings keep getting hacked. Here's how to prevent 'Zoom bombing' on your video chats　https://fortune.com/2020/04/02/zoom-bombing-what-is-meeting-hacked-how-to-prevent-vulnerability-is-zoom-safe-video-chats/〔2020/7/18 確認〕
※ 264 Zoom 社：Zoom Product Updates: New Security Toolbar Icon for Hosts, Meeting ID No Longer Displayed　https://blog.zoom.us/zoom-product-updates-new-security-toolbar-icon-for-hosts-meeting-id-hidden/〔2020/7/18 確認〕
※ 265 Zoom 社：Webinar Recap – 90-Day Security Plan Progress Report: July 1st　https://blog.zoom.us/webinar-recap-90-day-security-plan-progress-report-july-1st/〔2020/7/18 確認〕
※ 266 ITmedia：Zoom、中国政府の要請で米国で開催の天安門関連 Web 会議を閉鎖　改善を約束　https://www.itmedia.co.jp/news/articles/2006/13/news023.html〔2020/7/18 確認〕
※ 267 Cisco Systems G.K.：Cisco Webex Meetings Suite と Cisco Webex Meetings Online における未認証会議参加の脆弱性　https://www.cisco.com/c/ja_jp/support/docs/csa/2020/cisco-sa-20200124-webex-unauthjoin.html〔2020/7/18 確認〕
※ 268 Cisco Systems G.K.：Cisco Webex ネットワーク録画プレーヤーおよび Cisco Webex プレーヤーの任意のコード実行における脆弱性　https://www.cisco.com/c/ja_jp/support/docs/csa/2020/cisco-sa-webex-player-Q7Rtgvby.html〔2020/7/18 確認〕
※ 269 Cisco Systems G.K.：Cisco Webex Meetings デスクトップアプリの URL フィルタリングの任意プログラム実行に対する脆弱性　https://www.cisco.com/c/ja_jp/support/docs/csa/2020/cisco-sa-webex-client-url-fcmpdfVY.html〔2020/7/18 確認〕
※ 270 CyberArc Software, Inc.：Beware of the GIF: Account Takeover Vulnerability in Microsoft Teams　https://www.cyberark.com/resources/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams〔2020/7/18 確認〕
※ 271 https://www.ipa.go.jp/security/fy2019/reports/scrm/index.html〔2020/7/18 確認〕
※ 272 キヤノンマーケティングジャパン株式会社：情報セキュリティ意識に関する実態調査レポート～把握しておくべき『シャドー IT』の実態について～　https://eset-info.canon-its.jp/malware_info/trend/detail/200313.html〔2020/7/18 確認〕
※ 273 JCISPA：JASA - クラウドセキュリティ推進協議会　https://jcispa.jasa.jp/〔2020/7/18 確認〕
※ 274 一般社団法人情報マネジメントシステム認定センター：ISMS 適合性評価制度　https://isms.jp/isms.html〔2020/7/18 確認〕
※ 275 https://www.ipa.go.jp/files/000083955.pdf〔2020/7/18 確認〕

付録

資料･ツール

資料A　2019年のコンピュータウイルス届出状況

IPA が 2019 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届出の集計結果について述べる。

A.1　集計方法の変更について

近年、コンピュータウイルス（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-1 のとおり変更した。

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-1　ウイルス届出の集計方法の変更点

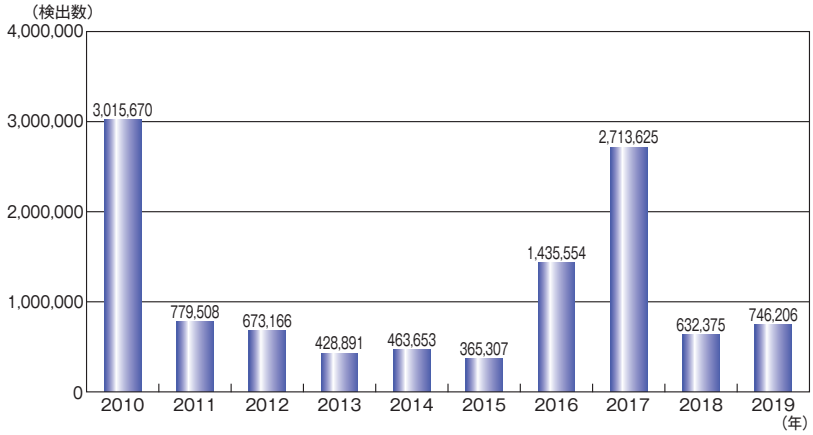
A.2　届出件数

新たな集計方法に基づく 2019 年の年間届出件数は、259 件となった。そのうち、ウイルス感染被害があった届出は 18 件であった。ウイルス感染被害の内訳のうち、主なものは Emotet 感染被害 5 件、ランサムウェア感染被害 5 件であった。本白書の「1.2.5 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 年以前の年間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。

A.3　届出ウイルス等

2019 年に寄せられたウイルス等検出数は、前年の 632,375 個より 113,831 個（18.0%）多い 746,206 個であった（図 A-1）。



■図 A-1　ウイルス等検出数推移（2010 ～ 2019 年）

参照

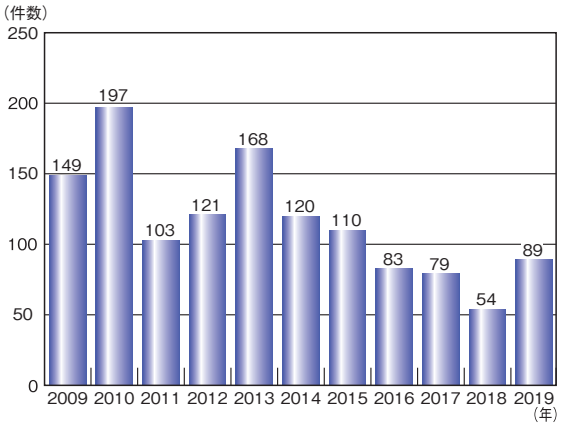
■コンピュータウイルス・不正アクセスの届出状況［2019年（1月～12月）］
https://www.ipa.go.jp/security/outline/todokede-j.html

資料B　2019年のコンピュータ不正アクセス届出状況

IPA が 2019 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届出の集計結果について述べる。

B.1　届出件数

2019 年の年間届出件数は 89 件となり、2018 年の届出件数 54 件から 35 件（64.8%）増加した（図 B-1）。



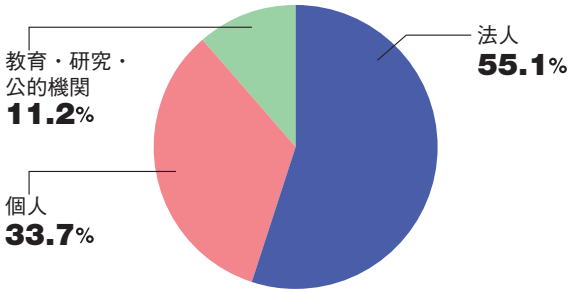
■図 B-1　不正アクセス届出件数の年別推移（2009 年～ 2019 年）

B.2　届出者別件数

2018 年と比較すると、届出者別の内訳は「法人」「個人」「教育・研究・公的機関」からの届出件数について、いずれも前年より増加した。2019 年の届出者別件数の比率では「法人」が 49 件（55.1%）と最も多かった（表 B-1、図 B-2）。

届出者別	2017 年	2018 年	2019 年
法人	46	35	49
個人	23	14	30
教育・研究・公的機関	10	5	10
合計（件）	79	54	89

■表 B-1　不正アクセス届出者別件数の推移（2017 ～ 2019 年）



■図 B-2　不正アクセス届出者別件数の比率（2019 年）

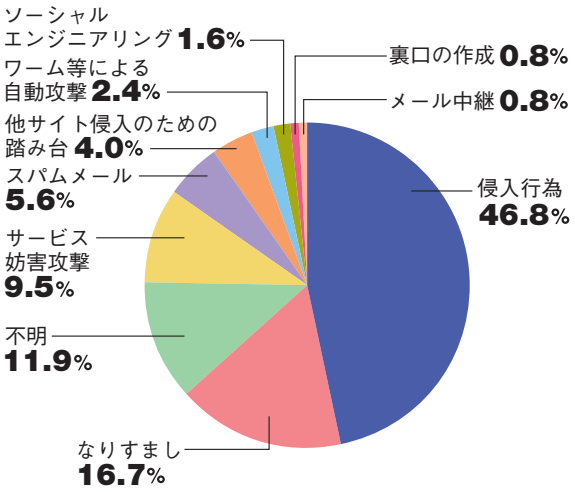
B.3　手口別件数

届出を攻撃行為（手口）により分類した件数について述べる。合計件数は 126 件で 2018 年から 53 件（72.6%）増加した。2019 年の主な手口の内訳は、「侵入行為」が 59 件（46.8%）と最も多く、次いで「なりすまし」が 21 件（16.7%）であった（表 B-2、次ページ図 B-3）。

手口種別	2017 年	2018 年	2019 年
侵入行為	55	33	59
なりすまし	10	18	21
不明	2	1	15
サービス妨害攻撃	12	11	12
スパムメール	1	8	7
他サイト侵入のための踏み台	0	0	5
ワーム等による自動攻撃	0	0	3
ソーシャルエンジニアリング	0	0	2
裏口の作成	0	0	1
メール中継	3	0	1
証拠の隠滅	0	1	0
メールアドレス詐称	0	1	0
その他	4	0	0
合計（件）	87※	73※	126※

※届出 1 件に複数の攻撃行為を受けているケースもあるため、届出件数合計と一致していない。

■表 B-2　不正アクセス手口別件数の推移（2017 ～ 2019 年）



■図 B-3　不正アクセス手口別件数の比率（2019 年）

B.4 被害内容別件数

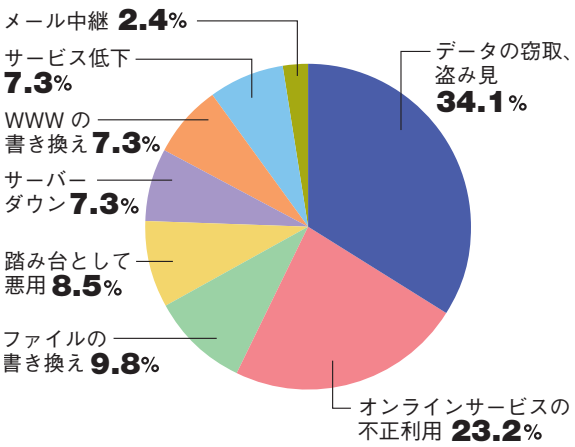
届出のうち被害未遂の届出を除いた、実際に被害に遭った届出について、被害内容で分類した件数について述べる。合計件数は82件で2018年から35件(74.5%)増加した。被害内容の内訳は2018年と傾向が異なり、「データの窃取、盗み見」が28件（34.1%）と最も多く、次いで「オンラインサービスの不正利用」が19件(23.2%)であった(表 B-3、図 B-4)。

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[2019年下半期(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［2019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。

被害内容	2017年	2018年	2019年
データの窃取、盗み見	11	9	28
オンラインサービスの不正利用	0	10	19
ファイルの書き換え	6	3	8
踏み台として悪用	7	13	7
サーバーダウン	0	1	6
WWW の書き換え	12	5	6
サービス低下	9	5	6
メール中継	5	0	2
不正アカウントの作成	2	1	0
合計（件）	52※	47※	82※

※届出 1 件に複数の被害内容が存在するケースもあるため、届出件数合計と一致していない。

■表 B-3　不正アクセス被害内容別件数の推移（2017 ～ 2019 年）



■図 B-4　不正アクセス被害内容別件数の比率（2019 年）

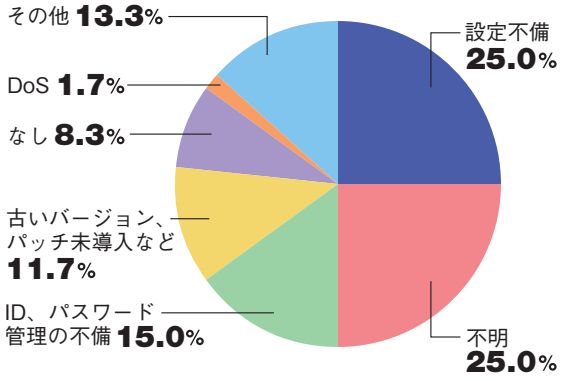
B.5 原因別件数

届出のうち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について述べる。合計件数は60件で2018年から17件(39.5%)増加した。原因の内訳は2018年と傾向が異なり、「設定不備」と「不明」がそれぞれ15件(25.0%)と最も多かった(表 B-4、図 B-5)。

被害原因	2017年	2018年	2019年
設定不備	7	7	15
不明	11	8	15
ID、パスワード管理の不備	20	23	9
古いバージョン、パッチ未導入など	11	1	7
なし	0	0	5
DoS	5	4	1
その他	0	0	8
合計（件）	54※	43※	60※

※届出 1 件に複数の原因内容が存在するケースもあるため、届出件数合計と一致していない。

■表 B-4　不正アクセス原因別件数



■図 B-5　不正アクセス原因別件数の比率（2019 年）

B.6 対策情報

2019 年は、なりすましによるオンラインサービスの不正利用、情報窃取の被害の届出が依然として多く見られた。一方で、Web サーバへの不正アクセスによる情報の窃取や、DB サーバへの不正アクセスによるファイルの書き換えといったサーバに対する被害の届出も見られた。これらサーバに対する不正アクセスの原因は、Web サイトの構築・運用に用いられるコンテンツマネジメントシステム（CMS：Contents Management System）の設定不備や古いバージョンの利用等であった。

なりすましによるオンラインサービスの不正利用に対しては、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」「二段階認証等のセキュリティ機能を積極的に活用する」等、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望ましい。また、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「Web アプリケーションの定期的な脆弱性対策の実施」「Web サーバ上の不要なサービスの停止」等、Web サイトのセキュリティホールをなくしていくことが推奨される。

参照

■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）］
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、2019 年末までに 1 万 5,224 件に達した。

C.1　脆弱性の届出概況

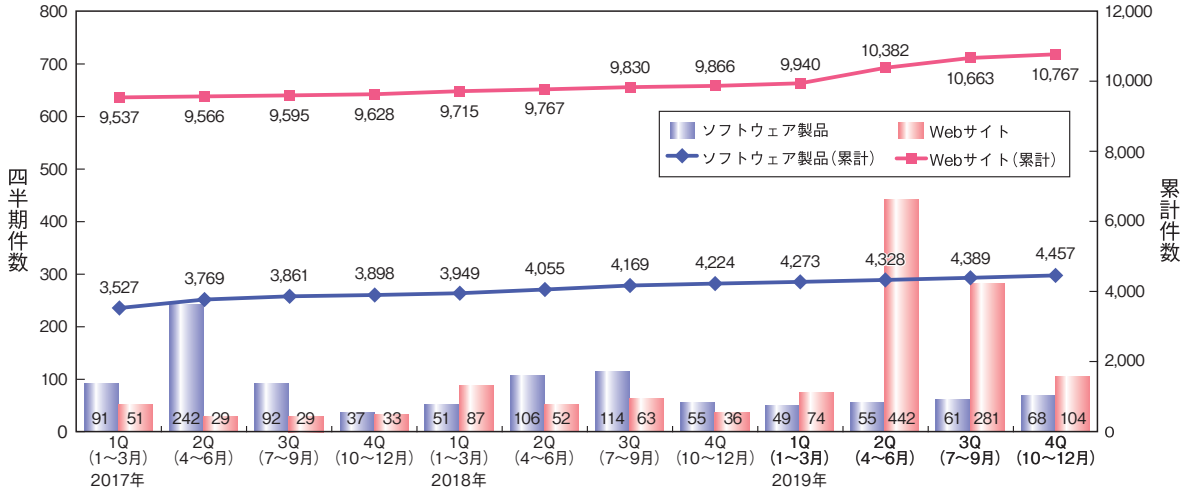
2019 年末時点で、届出受付開始（2004 年 7 月 8 日）からの累計は、ソフトウェア製品に関するもの 4,457 件、Web サイトに関するもの 10,767 件、合計 1 万 5,224 件で、Web サイトに関する届出が全体の 70.7% を占めている。

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、2019 年第 4 四半期末時点で 4.03 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。

2018 年 1Q（1～3 月）	2018 年 2Q（4～6 月）	2018 年 3Q（7～9 月）	2018 年 4Q（10～12 月）	2019 年 1Q（1～3 月）	2019 年 2Q（4～6 月）	2019 年 3Q（7～9 月）	2019 年 4Q（10～12 月）
4.08	4.06	4.03	3.99	3.96	4.03	4.06	4.03

■表 C-1　脆弱性関連情報の届出件数の四半期別推移



■図 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）

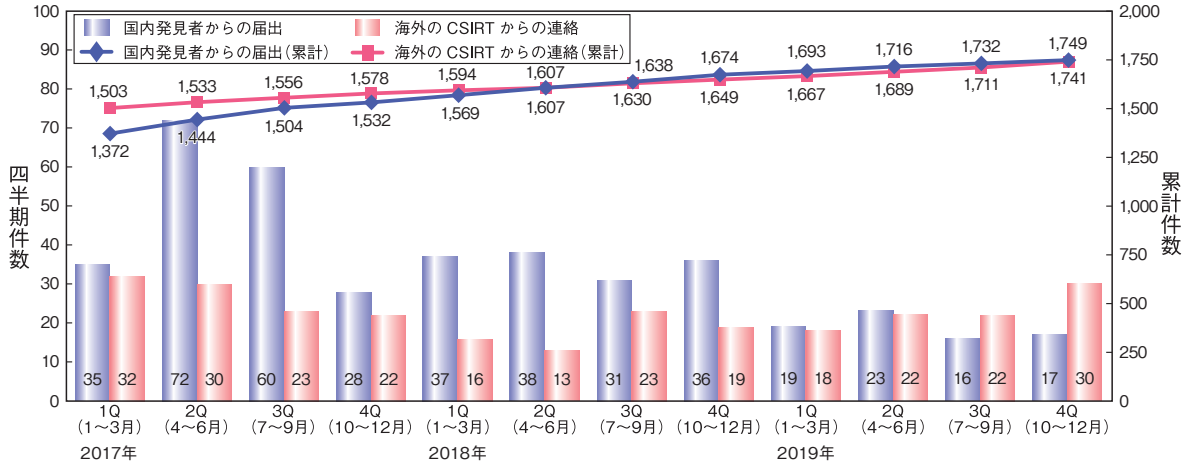
C.2　ソフトウェア製品の脆弱性の処理状況届出種別

2019 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 2,034 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 39 件、製品開発者が脆弱性ではないと判断したものは 97 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 488 件で、これらの取り扱いを終了したものの合計は 2,658 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 1,741 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	2,034件
	個別対応	39件
脆弱性ではない		97件
不受理		488件
合計		2,658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

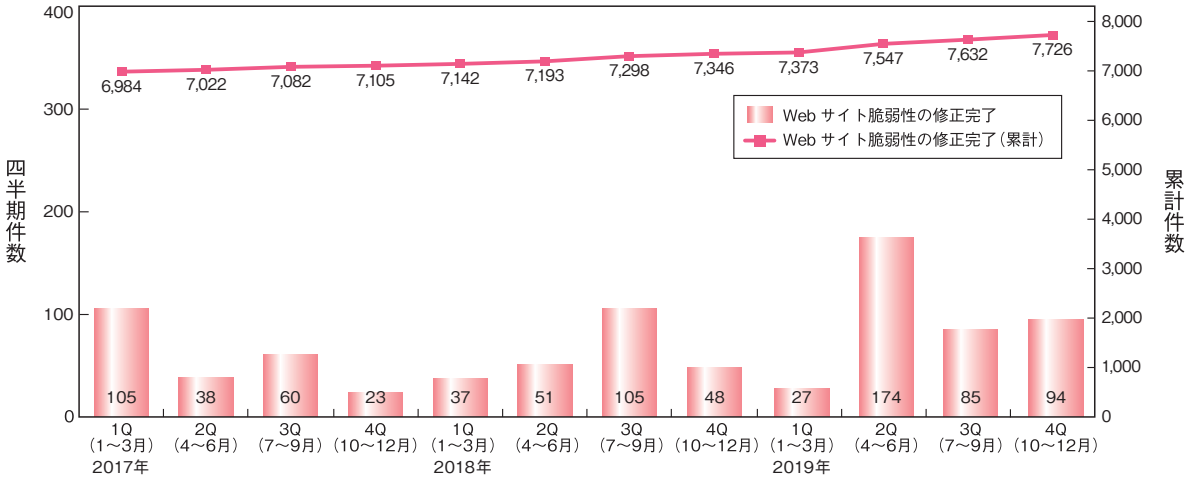
C.3 Webサイトの脆弱性の処理状況

2019 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 7,726 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 655 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 210 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 271 件で、これらの取り扱いを終了したものの合計は 9,992 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	7,726件
注意喚起	1,130件
脆弱性ではない	655件
取扱不能	210件
不受理	271件
合計	9,992件

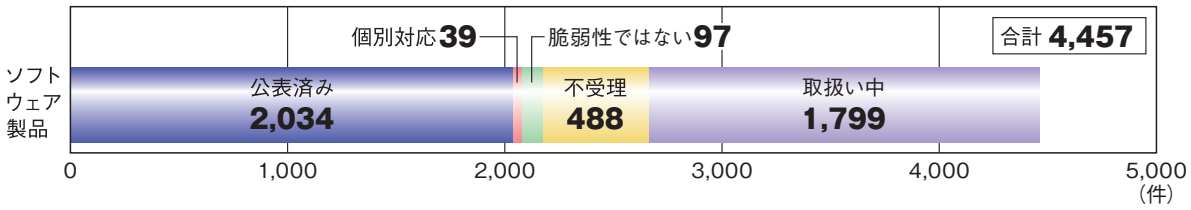
■表 C-3　Web サイトの脆弱性の終了件数



■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

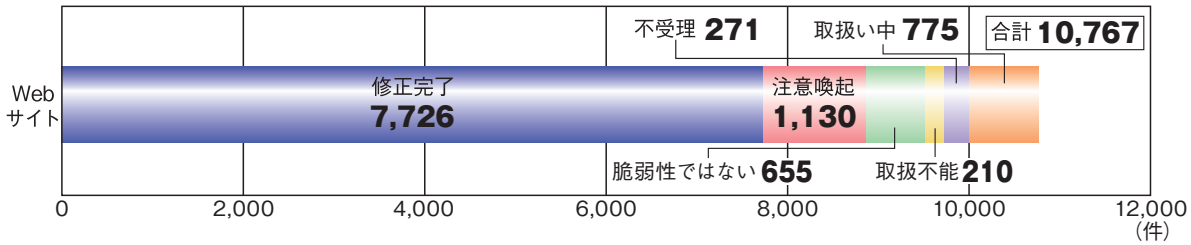
ソフトウェア製品の脆弱性関連情報の届出について処理状況を図 C-4 に示す。



■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[2019年第4四半期(10月～12月)]
https://www.ipa.go.jp/files/000080025.pdf

脆弱性対処を促進するための二つのガイド
（製品開発者向け／消費者向け）

近年、ネットワークに接続する製品（インターネット家電、ルータ、ネットワークカメラ、玩具やゲーム等。以下、製品）が一般家庭に広く普及しています。その結果、脆弱性対処が行われていない製品を悪用されることによって一般家庭でもコンピュータウイルスに感染させられる等の被害が増加しています。IPA では、このようなネットワークに接続する製品を開発・販売している製品開発者へ脆弱性対処の必要性について普及啓発に取り組んでいますが、多くの製品に脆弱性が発見されているのが現状です。

その一方で、脆弱性対処に積極的に取り組んでいる製品開発者が存在していることも事実です。しかし、積極的な取り組みを行っていることが、製品を購入する消費者に伝わらず消費者が安全な製品が選定できないという状況や、購入時に安全な製品であっても購入後の消費者の不適切な運用により、危険な状態のまま利用されてしまうという問題も存在しています。

そこで、IPA では、製品開発者向けに脆弱性対処として実施すべき項目や実施内容をまとめたガイドと、消費者向けに脆弱性対処が行われた安全な製品の購入・利用に関する注意事項をまとめたガイドを作成して公表しました。

脆弱性対処に向けた製品開発者向けガイド	
内容	・脆弱性対処として実施が求められる項目（12 項目）と、その意義 ・各実施項目について自組織のレベルに応じた実施内容 ・消費者に脆弱性対処していることをアピールするための、各実施項目について、消費者へのアピール方法（開示方法）

ネット接続製品の安全な選定 / 利用ガイド	
内容	・購入前（安全な選定）に、脆弱性対処された製品を選定するための確認ポイント（アップデート機能の有無等）や、確認方法 ・購入後（安全な利用）に、安全に製品を利用するための確認ポイント（適切なセキュリティ設定や定期的なセキュリティ更新等）や、確認方法

これらのガイドは、以下の URL からダウンロードできます。

https://www.ipa.go.jp/security/vuln/report/index.html#section9

ネットワークに接続する製品に関する脆弱性対処の促進、及び安全な製品の選定、製品の安全を保つことに役立てるため、製品開発者、及び消費者の方々はぜひこれらのガイドをご活用ください。

IPA動画コンテンツ「脆弱性発見・報告のみちしるべ」

近年、若年層からプログラミング教育が実施されています。これに伴い、脆弱性を見付けることができるIT技術初学者が増え、脆弱性を見付ける機会も増加しています。IPAでも、学生に対して情報セキュリティに関する技術教育を実施し、次代を担う情報セキュリティ人材を発掘・育成する「セキュリティキャンプ」事業に取り組んでおり、セキュリティキャンプ修了生からもIPAが運営する「脆弱性届出制度」(2004年7月から「情報セキュリティ早期警戒パートナーシップガイドライン」に則り運用)へ脆弱性の報告が寄せられています。

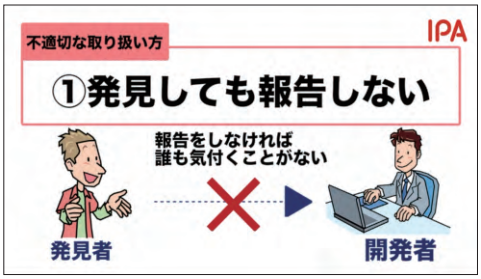
一方、以下のような誤った方法で脆弱性の発見や取り扱い等をした場合、製品開発者やWebサイト運営者とトラブルに発展する、またはWebサービスや製品利用者へ被害を及ぼす恐れがあります。

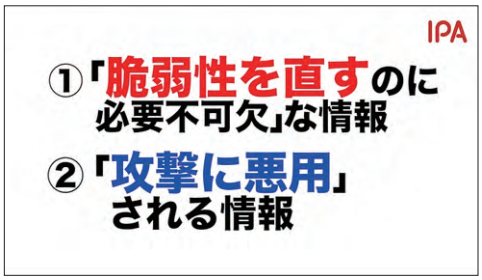
・脆弱性の誤った発見方法によっては、意図せずWebサイトを停止させてしまう。
・脆弱性情報の誤った取り扱い方法によっては、攻撃者による攻撃を誘発してしまう。
・脆弱性情報の誤った報告方法によっては、脆弱性が修正されない。

そこで、脆弱性を見付ける可能性のあるIT技術初学者向けに、正しい脆弱性情報の発見・取り扱い方、報告方法を理解していただくため、IPAでは動画コンテンツ「脆弱性発見・報告のみちしるべ～発見者に知っておいて欲しいこと～」を公開しました。

この動画は、8編で構成され、各動画の再生時間は2～3分程度のため、すきま時間に視聴できます。また、全8編を1編に纏めた動画もあります。個人学習や教育機関での教育教材として、以下のURLにアクセスしてご活用ください。

https://www.ipa.go.jp/about/press/20200406.html





No.	動画タイトル	No.	動画タイトル
1	脆弱性という言葉　知っていますか？	5	脆弱性の発見から対策実施までの流れ
2	脆弱性情報とは？	6	発見時の注意点 ～発見者に求められる心構え～
3	実は諸刃の剣？ 脆弱性情報の２つの側面	7	報告時の注意点 ～発見者が知っておくべきこと～
4	やってはいけない！ 脆弱性情報の取扱い	8	情報セキュリティ早期警戒パートナーシップ

IPAの便利なセキュリティツール

IPA では、企業や個人がセキュリティ対策状況の診断、セキュリティに関する情報収集、教育等を実施するための便利なツールを提供しています。以下の表の URL からご利用ください。

情報セキュリティ対策ベンチマーク 診断

46 問の設問に回答すると、規模、業種、情報資産数等が近い他社と比較した自社のセキュリティレベルがグラフで表示されます。 [https://www.ipa.go.jp/security/benchmark/]

脆弱性体験学習ツール「AppGoat」 ― 突いてみますか？ 脆弱性！ ― 教育

脆弱性の概要や対策方法等の脆弱性に関する基礎的な知識を実習形式で体系的に学ぶことができます。
[https://www.ipa.go.jp/security/vuln/appgoat/]

脆弱性対策情報データベース「JVN iPedia」 情報検索 情報配信

10 万件超の脆弱性対策情報を収集、蓄積しており、キーワードやベンダ名、製品名等で検索できます。RSS 配信機能によって定期的に情報を取得することもできます。 [https://jvndb.jvn.jp/]

MyJVN 脆弱性対策情報収集ツール 情報検索

フィルタリング条件を設定することで、JVN iPedia の中から自社システムに関連する脆弱性情報を効率よく収集できます。 [https://jvndb.jvn.jp/apis/myjvn/mjcheck3.html]

MyJVN バージョンチェッカ 診断

パソコンにインストールされているソフトウェア製品が最新バージョンであるかを簡単な操作で確認できます。
[https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html]

サイバーセキュリティ注意喚起サービス「icat for JSON」 情報配信

IPA の Web サイトに掲載している「重要なセキュリティ情報」をリアルタイムで配信して自社のイントラサイト等に一覧として表示します。 [https://www.ipa.go.jp/security/vuln/icat.html]

注意警戒情報サービス 情報配信

「重要なセキュリティ情報」及びサーバ用オープンソースソフトウェア製品のリリース情報を「緊急」「注意」等に分類して発信しています。 [https://jvndb.jvn.jp/alert/]

Webサイトの攻撃兆候検出ツール「iLogScanner」 診断

Web サーバのログを解析して SQL インジェクション等の脆弱性を狙った攻撃や不正アクセス等の兆候を検出できます。 [https://www.ipa.go.jp/security/vuln/iLogScanner/]

知っていますか？ 脆弱性 教育

Web サイトにおける代表的な 10 種類の脆弱性について理解できます。
[https://www.ipa.go.jp/security/vuln/vuln_contents/]

情報セキュリティ対策支援サイト 診断 情報検索 教育

中小企業における情報セキュリティ対策の「知りたい」「学びたい」「始めたい」「続けたい」を支援します。セキュリティに取り組むことを宣言する SECURITY ACTION の申し込みも行えます。 [https://security-shien.ipa.go.jp/]

セキュリティ要件確認支援ツール 診断

情報システムの調達担当者等がシステムの機能・サービスを入力すると、政府機関の統一基準等を基に必要なセキュリティ要件を提供します。 [https://www.ipa.go.jp/security/isec-sras/]

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！」 情報検索

官・民が保有する情報セキュリティのコンテンツを集約し、「対策する」「教育・学習」等のニーズ別に分類して掲載しています。 [https://www.ipa.go.jp/security/kokokara/]

IPAコンクール応援隊長「まもるくん」

第15回 IPA「ひろげよう情報モラル・セキュリティコンクール」2019 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、優秀な情報モラル・情報セキュリティをテーマに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。

「ひろげよう情報モラル・セキュリティコンクール」（https://www.ipa.go.jp/security/event/hyogo/）

最優秀賞

〈標語部門〉

「とくめい」が
自分の良心
まどわせる

青森県 つがる市立森田中学校 2年
成田 優碧さん

〈ポスター部門〉

岐阜県 土岐市立泉中学校 2年
伴 里来さん

〈4コマ漫画部門〉

昔話が始まらない ～依存ゆえに～

愛知県 愛知県立豊田東高等学校 1年
中 智奈望さん

優秀賞

〈独立行政法人情報処理推進機構〉

〈標語部門〉

きれいだよ　スマホをおいて　みるはなび

鹿児島県　鹿児島市立広木小学校　1年
竹之内 俐勇さん

1枚の　写真に百もの　情報が

北海道　札幌市立西野中学校　3年
中田 瑞音さん

同意します　何に同意か　わかってる?

大阪府　大阪府立三国丘高等学校　1年
宮原 明日香さん

〈ポスター部門〉

佐賀県 小城市立晴田小学校 3年
森永 美紀さん

群馬県 高崎市立吉井西中学校 2年
時澤 のぞみさん

大阪府 帝塚山学院高等学校 1年
佐藤 綾菜さん

〈4コマ漫画部門〉

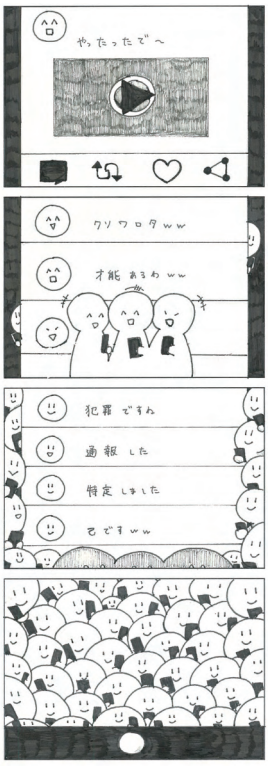
送る前に考えよう

長野県 上田市立浦里小学校 6年
片田 千尋さん

うっかり桃太郎

東京都 国立大学法人筑波大学附属中学校 1年
金子 真央さん

不特定多数のむこう側



岡山県 岡山県立津山工業高等学校 3年
今井 優花さん

〈警察庁〉
きをつけよう　ネットで話すの　どこのだれ
茨城県　筑西市立上野小学校　1年
武井 明香里さん

〈一般社団法人コンピュータソフトウェア著作権協会〉
「拾い画像」?　その絵は　落とし物じゃない
大阪府　桃山学院高等学校　2年
粕野 哲さん

〈一般社団法人コンピュータソフトウェア協会〉
パスワード　文字数ふやせば　自己防衛
鹿児島県　鹿児島市立松原小学校　4年
森田 麗市さん

〈一般社団法人JPCERTコーディネーションセンター〉
忘れたい　あの日に書いた　メッセージ
鹿児島県　鹿児島市立伊敷小学校　6年
中友 結さん

〈一般社団法人情報サービス産業協会〉
大じょうぶ?　ネットにのせる　そのじょうほう
鹿児島県　鹿児島市立山下小学校　2年
内藤 蓮温さん

〈一般社団法人全国地域情報産業団体連合会〉
大切に　個人情報と未来の自分
福島県　会津若松市立第五中学校　1年
岩澤 佑磨さん

〈一般社団法人日本教育情報化振興会〉
スマホデビュー　忘れないで　家族の時間
兵庫県　市川町立市川中学校　1年
利根川 准菜さん

〈一般社団法人日本情報システム・ユーザー協会〉
スマートフォン　軽い気持ちが　おおごとに
山梨県　山梨学院小学校　5年
千葉 叶惺さん

〈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　あなたの笑顔を　守るため
長崎県　諫早市立西諫早中学校　3年
髙瀬 紋花さん

〈フィッシング対策協議会「STOP. THINK.CONNECT.」〉
そのサイト　「危ないかも」と　一呼吸
高知県　高知商業高等学校　3年
窪内 まことさん

〈デジタルアーツ株式会社〉
いやなこと　書かない見ない　広げない
鹿児島県　鹿児島市立広木小学校　2年
迫田 蒼汰さん

〈株式会社ネットワールド〉
いいねより　自分のいいこと　いっぱいあるよ
兵庫県　雲雀丘学園小学校　3年
髙原 澪さん

〈LINE株式会社〉
見直そう　自分の投稿　載せる前
宮城県　大崎市立古川中学校　1年
會田 美歩さん

〈株式会社ラック〉
プログラム　パッチをあてて　バッチグー
広島県　広島商船高等専門学校　2年
三好 陸斗さん

〈北海道警察サイバーセキュリティ対策本部〉
顔見せて　同じ言葉が　言えますか?
北海道　北海道帯広柏葉高等学校　2年
佐藤　結愛乃さん

〈札幌市教育委員会〉
ちょっと待て!　安易な拡散、デマ情報?
北海道　札幌市立西野中学校　3年
大川 巧人さん

〈宮城県警察本部〉
セキュリティ　かければ自分が　守られる
宮城県　大崎市立古川中学校　2年
柏倉 暖さん

〈公益財団法人仙台応用情報学研究振興財団〉
思いやり　ネットの中での　守り神
宮城県　クラーク記念国際高等学校 仙台キャンパス　3年
荒木 進太郎さん

〈茨城県〉
おもしろさ　免罪符には　ならないよ
茨城県　茨城県立下妻第二高等学校　2年
根本　華蓮さん

〈茨城県教育庁学校教育部義務教育課〉
友達が　クリック1つで　消えてった
茨城県　北茨城市立磯原中学校　2年
小口 愛莉さん

〈茨城県メディア教育指導員連絡会〉
そのじょうほう　ひろがるひろがる　けせないよ
茨城県　筑西市立上野小学校　2年
吉原 洵さん

〈栃木県警察本部〉
自分をまもるため　正しいちしき　みにつけよう!
栃木県　那須烏山市立江川小学校　3年
相吉澤 駿さん

〈群馬県警察本部〉
冗談で　のせた写真が　もう消せない
群馬県　東吾妻町立岩島小学校　6年
一場 夢叶さん

〈埼玉県警察本部〉
映えるより　いいねの数より　モラルとルール
埼玉県　立教新座高等学校　2年
山内 太陽さん

〈東京情報大学〉
つぶやいた　言葉がむかう　全世界
千葉県　日出学園小学校　5年
志賀 亮太さん

〈警視庁〉
サギだった　気付いた時には　カモだった
東京都　錦城学園高等学校　1年
青木 千優さん

〈一般社団法人東京都情報産業協会〉
ちょっと待て 送るは一瞬 背負うは一生
東京都　東京都立三鷹中等教育学校　1年
三保 幸輝さん

〈福井県警察本部〉
パスワード　かけるは一時の面倒　かけぬは一生の後悔
福井県　北陸学園北陸高等学校　2年
小林 玄虎さん

〈一般社団法人山梨県情報通信業協会〉
大丈夫?　手洗いうがい　セキュリティ
山梨県　山梨学院小学校　5年
遠藤 幸歩さん

〈長野県警察本部〉
戻らない　書いた事実も　友達も
長野県　長野県岡谷東高等学校　1年
中澤 恋菜さん

〈一般社団法人長野県情報サービス振興協会〉
目の前で　言えない事は　書かないよ
長野県　松本市立丸ノ内中学校　1年
西尾 真さん

〈長野県青少年インターネット適正利用推進協議会〉
再確認　スマホのルールと　使い方
長野県　長野県松川高等学校　1年
西島 美幸さん

〈岐阜県警察本部〉
その発言　モラルとマナー　気にしてる?
岐阜県　岐阜県立各務原西高等学校　1年
直江 美里さん

〈特定非営利活動法人ふじのくに情報ネットワーク機構〉
命がけ　歩きスマホの　つなわたり
静岡県　日本大学三島高等学校　1年
島袋 紫月さん

〈愛知県警察本部〉
気をつけろ　消したつもりが　拡散中
愛知県　名古屋市立工芸高等学校　2年
大川 花菜さん

〈一般社団法人京都府情報産業協会〉
その画像　誰が見るのか　分からない
京都府　舞鶴市立若浦中学校　3年
森 美空さん

〈公益社団法人京都府防犯協会連合会〉
成りすまし?　相手のフェイス　フェイクかも
京都府　舞鶴市立青葉中学校　1年
竹田 芽生さん

〈京都府私立中学高等学校情報科研究会〉
そのトーク　切り取られても　大丈夫?
京都府　花園高等学校　1年
芦田 恵理さん

〈京都コンピュータ学院〉
個人情報　自分で守ろう　ネット社会
京都府　舞鶴市立青葉中学校　1年
林田 真太郎さん

〈大阪私学教育情報化研究会〉
そのことば　あいての画面で　どう見える
大阪府　泉佐野市立佐野中学校　1年
芝田 芽依さん

〈特定非営利活動法人奈良地域の学び推進機構〉
気を付けて　気づかぬうちに　人を傷つける
奈良県　奈良文化高等学校　1年
松岡 彩花さん

〈鳥取県警察本部生活安全部サイバー犯罪対策課〉
その画像　出回ってからでは　もう遅い
鳥取県　鳥取県立鳥取西高等学校　1年
前田 海透さん

〈鳥取県警察本部生活安全部少年課〉
友達は　追加じゃなくて　作るもの
鳥取県　鳥取県立鳥取西高等学校　1年
矢野 慧さん

〈島根県教育委員会〉
つなげよう　スマホじゃなくて　人と人
島根県　島根県立松江商業高等学校　1年
井上 敬翔さん

〈一般社団法人島根県情報産業協会〉
もう消せない一生残るよその書き込み
島根県　島根県立松江商業高等学校　1年
齋藤 愛依さん

〈岡山県警察本部〉
悪ふざけ　デジタルタトゥーが　いつまでも
岡山県　岡山大学教育学部附属中学校　1年
高見 真央さん

〈岡山県情報セキュリティ協議会〉
SNS　水をかけても　火は消えない
岡山県　岡山大学教育学部附属中学校　1年
渡辺 彩子さん

〈一般社団法人広島県情報産業協会〉
キケンだよ　知らない相手に　個人情報
広島県　熊野町立熊野東中学校　2年
門田 翼希さん

〈広島県インターネットセキュリティ対策推進協議会〉
情報を　見分ける力を　養おう
広島県　熊野町立熊野東中学校　2年
安永 渉さん

〈徳島県警察本部〉
気をつけよう　クリック1つじゃ　とり消せない
徳島県　阿南市立羽ノ浦中学校　1年
山下 蒼衣さん

〈徳島県教育委員会〉
その「いいね」ほんとにみんなの「いいね」なの?
徳島県　徳島県立城ノ内高等学校　1年
大城 楓彩さん

〈一般社団法人徳島県情報産業協会〉
改めて　考えてみよう　ネットの怖さ　その一言で　もどれなくなる
徳島県　美馬市立脇町中学校　1年
川西 太晴さん

〈公益財団法人e-とくしま推進財団〉
いいねより　大事にしよう　あなたのハート♥
徳島県　徳島県立城ノ内高等学校　1年
堀井 咲良さん

〈香川県教育委員会〉
こっちみて　画面じゃなくて　現実を
香川県　高松市立香東中学校　1年
鳥取 崇悟さん

〈情報通信交流館〉
狙ってる　さぎという名の　モンスター
香川県　高松市立香東中学校　2年
入江 凜太朗さん

〈愛媛県警察本部〉
何気ない　その書き込みは　もう消えない
愛媛県　新居浜市立角野中学校　3年
川口 蒼生さん

〈高知県警察本部〉
送信が　自分の未来を　左右する
高知県　明徳義塾高等学校　2年
新澤 颯真さん

〈一般社団法人高知県情報産業協会〉
ネットでは　怪しいサイトに　入らない
高知県　南国市立久礼田小学校　5年
弘瀬 青空さん

〈福岡県警察本部〉
消せないよ　載せたら一生　残るもの
福岡県　久留米市立久留米商業高等学校　2年
徳永 妃夏さん

〈一般社団法人長崎県情報産業協会〉
ちょっとまて　流していいの?　その情報
長崎県　諫早市立西諫早中学校　2年
熊野 暉さん

〈大分県警察本部〉
いいことと　思って拡散　加害者に
大分県　中津市立三光中学校　1年
塚元 仁菜さん

〈宮崎県警察本部〉
信じるの?　顔の見えない　お友達
宮崎県　都城聖ドミニコ学園高等学校　2年
酒井 悠衣さん

〈鹿児島県警察本部〉
個人情報　広まるスピード　SNSからSOS
鹿児島県　長島町立鷹巣中学校　3年
濵村 汐音さん

〈鹿児島県教育委員会〉
ネット社会　使い方しだいで　変わる世界
鹿児島県　鹿児島市立吉野小学校　6年
上別府 美空さん

〈鹿児島市教育委員会〉
いやだけど　みまもり設定　ぼくのため
鹿児島県　鹿児島市立草牟田小学校　4年
若松 亮佑さん

〈特定非営利活動法人ITかごしま支援隊〉
パソコンも　かぜをひかないように　よぼうしよう　ウイルスたいさく
鹿児島県　鹿児島市立谷山小学校　2年
山下 暖起さん

〈沖縄県情報通信関連産業団体連合会〉
その発言　ずっと残るよ　大丈夫?
沖縄県　昭和薬科大学附属中学校　2年
宮城 優奈さん

ポスター部門 優秀賞

〈一般社団法人組込みシステム技術協会〉

愛知県 刈谷市立雁が音中学校 2年

望月 香奈さん

〈株式会社カスペルスキー〉

東京都 東京都立葛飾総合高等学校 2年

須藤 愛子さん

〈実教出版株式会社〉

神奈川県 神奈川県立神奈川工業高等学校 3年

鈴木 孝実さん

〈株式会社シマンテック〉

鹿児島県 姶良市立帖佐中学校 1年

倉橋 知世さん

〈株式会社ディー・エヌ・エー〉

大阪府 大阪府立寝屋川高等学校 全日制課程 2年

中川 晃汰さん

〈マカフィー株式会社〉

群馬県 ぐんま国際アカデミー 中等部 1年

中塚 さくらさん

〈一般社団法人
北海道情報システム産業協会〉

北海道 市立札幌開成中等教育学校 1年

斎藤 美楽希さん

〈岩手県警察本部〉

岩手県 岩手県立一関第一高等学校附属中学校 1年

小池 碧さん

〈一般社団法人
宮城県情報サービス産業協会〉

宮城県 宮城県松島高等学校 3年

末永 ゆめさん

〈秋田県警察本部〉

秋田県 秋田県立矢島高等学校 1年

佐藤 彩花さん

〈福島県警察本部〉

福島県 福島県立会津農林高等学校 1年

渡部 悠羽さん

〈茨城県教育庁学校教育部高校教育課〉

茨城県 茨城県立下妻第二高等学校 2年

横島 璃子さん

〈茨城県警察本部〉

茨城県 塚原学園　青葉台中等学部 3年

菅原 凜南さん

〈茨城県情報通信
ネットワークセキュリティ協議会〉

茨城県 つくば市立吾妻中学校 1年

石丸 理緒さん

〈千葉県警察本部〉

千葉県 日出学園高等学校 2年

岩田 純佳さん

〈新潟県警察本部〉

新潟県 新潟県立新潟向陽高等学校 3年

長島　奏羽さん

〈長野県インターネットプロバイダ
防犯連絡協議会〉

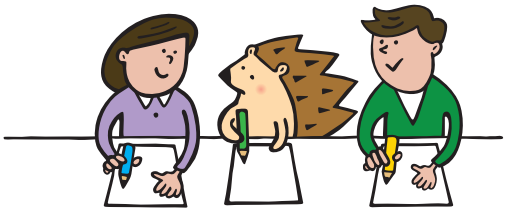
長野県 長野県駒ケ根工業高等学校 3年

竹下 魁音さん

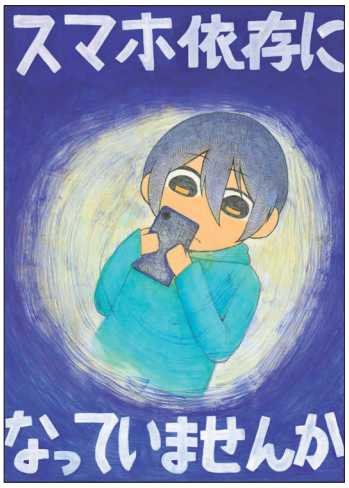
〈ネット安全・安心ぎふコンソーシアム〉

岐阜県 輪之内町立仁木小学校 6年

三浦 夢乃さん



〈静岡県警察本部〉



静岡県 静岡県立浜松工業高等学校 3年

池川 侑希さん

〈三重県警察本部〉

三重県 三重県立名張高等学校 2年

釘田 慈さん

〈滋賀県警察本部〉

滋賀県 大津市立北大路中学校 3年

鈴木 絹さん

〈京都府教育委員会〉

京都府 京都翔英高等学校 1年

堀 さやとさん

〈大阪府警察本部〉

大阪府 大阪府立布施高等学校 1年

米満 采さん

〈兵庫県警察本部〉

兵庫県 兵庫県立龍野北高等学校 2年

粕谷 友莉さん

〈奈良県警察本部〉

奈良県 奈良県立奈良北高等学校 2年

香野 華蓮さん

〈鳥取県警察本部生活安全部〉

鳥取県 鳥取県立鳥取湖陵高等学校 3年

森脇 妃菜さん

〈香川県プロバイダ等防犯連絡協議会〉

香川県 香川県立高松工芸高等学校 3年

池内 藍華さん

〈愛媛県情報サービス産業協議会〉

愛媛県 松山市立東雲小学校 5年

近藤 凛々子さん

〈高知県教育委員会〉

高知県 高知商業高等学校 3年

佐伯 奈津実さん

〈福岡県教育委員会〉

福岡県 福岡県立嘉穂東高等学校 1年

鳥居 穂花さん

〈佐賀県警察本部〉

佐賀県 佐賀県立有田工業高等学校 1年

緒方 悠季乃さん

〈特定非営利活動法人 IT サポートさが〉

佐賀県 上峰町立上峰中学校 1年

荒木 陽菜さん

〈長崎県警察本部〉

長崎県 長崎日本大学高等学校 2年

髙平 悠花さん

〈熊本県警察本部〉

熊本県 御船町立御船中学校 1年

村上 華さん

〈一般社団法人宮崎県情報産業協会〉

宮崎県 宮崎市立佐土原中学校 1年

鳥原 蘭さん

〈沖縄県警察本部〉

沖縄県 沖縄県立那覇商業高等学校 3年

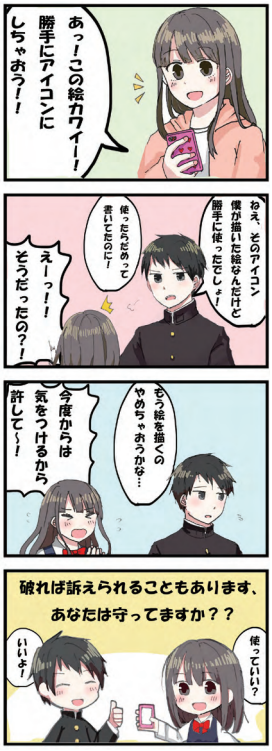
新城 はるかさん

4コマ漫画部門 優秀賞

モラル

破られがちな著作権

〈公益社団法人著作権情報センター〉

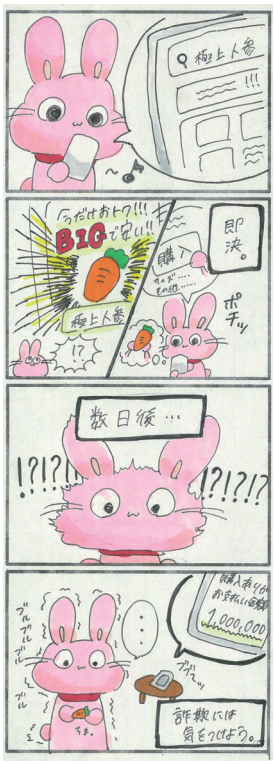


千葉県 学校法人市川学園市川高等学校 1年

粟屋 日菜さん

詐欺に気をつけて

〈モバイルコンピューティング推進コンソーシアム〉



北海道 北海道北見柏陽高等学校 1年

漆原 美月さん

許可はとった？

〈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〉

静岡県 静岡県立三島南高等学校 1年

仲原 叶人さん

無料アプリ、無料サイトのリスク

〈ソースネクスト株式会社〉

福島県 福島市立信陵中学校 1年

斎藤 奈々子さん

「小さなウソから…」

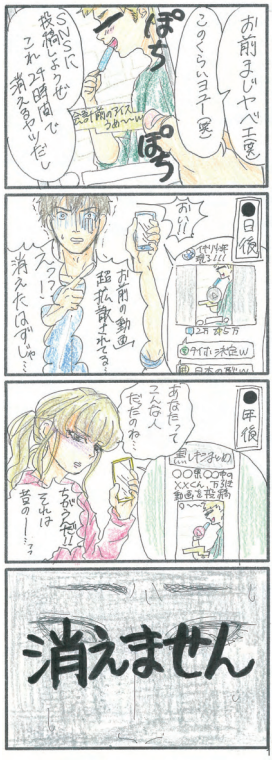
〈トレンドマイクロ株式会社〉

大阪府 帝塚山学院高等学校 1年

髙橋 恵さん

消えません

〈青森県警察本部〉

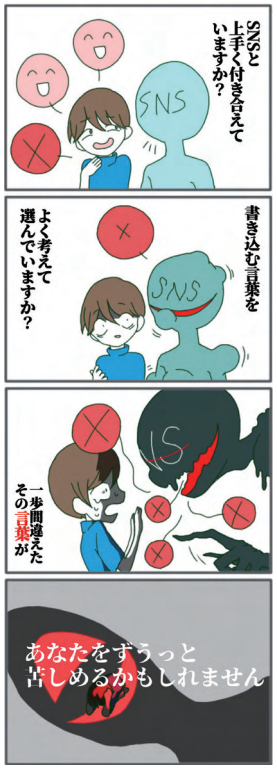


青森県 三沢市立第一中学校 3年

佐々木 花乃さん

言葉

〈山形県警察本部〉



山形県 山形県立酒田光陵高等学校 3年

後藤 莉穂さん

SNS の繋がり

〈公益社団法人埼玉県情報サービス産業協会〉

埼玉県 埼玉県立新座総合技術高等学校 2年

小田 花哉さん

ネット社会

〈神奈川県警察本部〉

なりすましシンデレラ

神奈川県 洗足学園中学校 1年

池田 夏埜さん

〈富山県警察本部〉

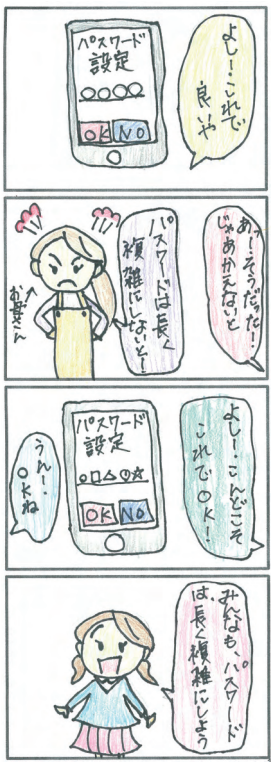
本当に大切な物は？

富山県 富山県立南砺福野高等学校 1年

田中 綾音さん

〈山梨県警察本部〉

パスワードは長く複雑に！



山梨県 山梨学院小学校 6年

小林 亜子さん

〈京都府警察本部〉

デジタルタトゥー

京都府 同志社高等学校 1年

後藤 詩さん

〈京都情報大学院大学〉

炎上するシチメンチョー

京都府 京都府立大江高等学校 2年

松岡 優佳さん

〈和歌山県警察本部〉

一生残る。

和歌山県 和歌山市立東和中学校 3年

長尾 美杏さん

〈島根県警察本部〉

失われた赤ずきんちゃん

島根県 島根大学教育学部附属義務教育学校 3年

佐々木 いづみさん

〈一般社団法人システムエンジニアリング岡山〉

なりすましにはご注意を。

岡山県 岡山県立津山工業高等学校 3年

福田 美咲さん

〈広島県警察本部〉

ウイルス入りリンゴに注意！

広島県 広島県立大門高等学校 2年

金子 葵さん

〈山口県警察本部〉

その通販サイト、大丈夫？

山口県 山口県立長府高等学校 2年

木下 朋香さん

〈かがわ情報化推進協議会〉

家族で夕食・・・？

香川県 東かがわ市立白鳥中学校 2年

岡本 沙津希さん

〈長崎県ネットワーク・セキュリティ連絡協議会〉

本当の顔は分からない

長崎県 諫早市立西諫早中学校 3年

髙橋 茉莉花さん

〈大分県情報サービス産業協会〉

河童の川流れ？

大分県 臼杵市立北中学校 3年

小坂 葵衣さん

〈一般社団法人鹿児島県情報サービス産業協会〉

パクリはダメ！

鹿児島県 湧水町立吉松中学校 2年

永野 未侑さん

〈特定非営利活動法人鹿児島インファーメーション〉

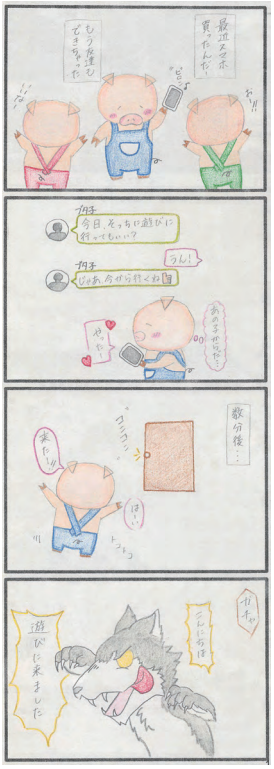
鬼ヶ島

鹿児島県 日置市立吹上中学校 3年

大寺 太郎さん

〈沖縄県〉

騙された子ブタ



沖縄県 沖縄県立北谷高等学校 1年

平田 菜奈弥さん

索引

さ

た

な

は

ま

ら

おわりに

「情報セキュリティ白書2020」では、初めての試みとして、セキュリティマネジメントの日米企業比較に関する特別寄稿を掲載し、青少年にフォーカスしたテーマとして「次代を担う青少年を取り巻くネット環境」を取り上げました。

2019年度は、サイバーセキュリティや個人情報保護に向けた政策の着実な実践が続いた一方、2020年に入ってからは、新型コロナウイルス感染症拡大により、生活や働き方の面での大きな変化を余儀なくされました。本白書も例外ではなく、試行錯誤しながらの執筆・編集となりました。

世界的な新型コロナウイルス感染症の拡大に伴い、感染対策をかたる詐欺メールや偽情報、医療機関やテレワークに使用するシステムを狙った攻撃等が急増しましたが、それらは既存の脅威と大きく変わるものではなく、騙されないための対策や脆弱性対策の重要性は変わりません。しかしながら、テレワーク等の新しい取り組みの中では、個々人が情報の管理や利用するシステムのセキュリティに対してより高い意識を持ち行動する必要があります。そのため今回のサブタイトルは、「変わる生活、変わらぬ脅威:自らリスクを考え新しい行動を」としました。

本白書は、IPAの職員を始めとする多くの関係者が、 多岐にわたる情報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、読者の方々に伝わるよう分かりやすい解説を心掛けて作成しました。皆様のサイバーセキュリティ対策の検討・実践の一助となれば幸いです。

編集子

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　小山 明美　山田 彩歌

執筆者　IPA
西尾 秀一　山里 拓己　佐藤 眞司　武智 洋　小川 隆一
神田 雅透　櫻井 玄弥　松坂 志　浅井 優子　猪城 明
板橋 博之　伊東 隆司　江島 将和　大友 更紗　岡下 博子
奥田 美幸　甲斐 成樹　亀山 友彦　唐亀 侑久　木内 直人
岸 和輝　木村 泰介　栗原 史泰　小暮 淳　小林 桂
小山 明美　近澤 武　佐川 陽一　柴田 直　島田 毅
ジリエ 陽子　竹内 智子　田村 百合子　辻 宏郷　土屋 昭治
中田 量子　名倉 裕介　橋本 徹　半貫 貴久　増田 亮太
松島 伸彰　森 淳子　山下 真吾　山田 彩歌　渡邉 祥樹
カリフォルニア大学バークレー校名誉教授　Robert E. Cole
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
お茶の水女子大学　リエゾン・URA センター　小谷 誠剛
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
三菱電機株式会社　伏見 信也
情報規格調査会 JTC 1/SC 27/WG 5 小委員会

協力者　IPA
加賀谷 伸一郎　桑名 利幸　松井 洋二　小沢 理康　白石 歩
伊藤 真一　田口 聡　前田 祐子　日向 英俊　本多 康弘
横山 尚人　渡辺 貴仁　石田 淳一　伊藤 彰朗　伊藤 博康
井上 勝浩　君島 知也　黒谷 欣史　竹腰 智　田村 智和
土屋 正　遠山 真　中原 和裕　畑野 元　福原 聡
宮本 一弘
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
宮内・水町 IT 法律事務所　宮内 宏
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

情報セキュリティ白書 2020

変わる生活、変わらぬ脅威：自らリスクを考え新しい行動を

2020 年 8 月 31 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
Fax　03-5978-7510
E-Mail spd-book@ipa.go.jp

表紙デザイン／本文 DTP・編集サポート　**伊藤 千絵、久磨 公治、涌田 明夫、北林 俊平、岩田 直也**