2021

情報セキュリティ白書

序章

2020年度の情報セキュリティの概況

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

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

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

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

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

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

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

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

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

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

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

2020 年度の情報セキュリティの概況

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

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

第3章
個別テーマ

本章では個別テーマとして、制御システム、IoT、そして2020年に新型コロナウイルス感染症の影響により急速に普及したテレワークの情報セキュリティについて、報告されたインシデントや攻撃の実態、脆弱性や脅威の動向、国の施策や企業の対策の状況等を解説する。

また、企業・組織のサイバーセキュリティ対策の検討や、政府機関のセキュリティ規格の策定・改訂の際に参照されることが多くなった米国NISTのセキュリティに関する活動やSP 800シリーズ等の規格策定の動向等について紹介する。

3.1 制御システムの情報セキュリティ

制御システム（ICS：Industrial Control System）は、電力、ガス、水道、輸送・物流、製造ライン等、我々の生活を支える重要インフラサービス※1を提供するシステムである。従来、制御システムは独立したネットワーク、固有のプロトコル、事業者ごとに異なる仕様で構築・運用されることが多く、外部からサイバー攻撃を行うことは困難と考えられていた。しかし、近年ネットワーク化やオープン化（標準プロトコル・汎用製品の利用）が進んだこと、また、10～20年に及ぶライフサイクルの長さ故に、外部との接続やサイバー攻撃を想定していないシステムが今なお多数稼働していることから、制御システムに対するサイバー脅威が高まっている。実際に、サイバー攻撃による浄水施設における薬液注入量の改ざん、大規模停電等のインシデントも発生している。

本節では、制御システムのセキュリティの動向と主な取り組みについて述べる。

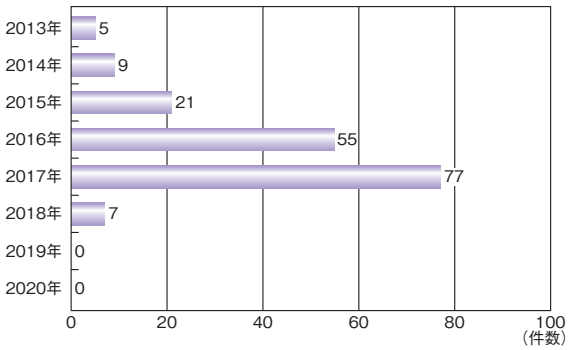
3.1.1 インシデントの発生状況と動向

国内においては、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC：Japan Computer Emergency Response Team Coordination Center）に2020年に報告された制御システムのインシデント件数は、2019年に引き続き0件であった（図3-1-1）。

しかし海外では、調査会社による制御システムユーザ等へのアンケート調査において、2019年同様、制御システムへの侵入や運用障害が発生したという回答が一定数以上あった。

例えば、製造事業者内のセキュリティ戦略、制御、運用に直接関与するサイバー及びITの専門家150名を対象とした調査結果では、調査対象者が所属する組織の53%が、過去12～24ヵ月の間に何らかのサイバー攻撃やその他のセキュリティインシデントに見舞われ、運用・制御技術（OT：Operational Technology）のインフラに影響があったと回答している※3。また、北米、欧州、アジアの重要インフラ組織の経営幹部400名以上を対象とした調査結果では、セキュリティ侵害があったという回答の85%のケースでOTネットワークまで侵入されており、そのうち36%がITシステムからの侵入であった※4。

2020年に公になったインシデントには、水道や電力等の重要インフラの制御システムを標的とした攻撃、ITシステムのウイルス※5感染による生産や重要サービスの停止、制御システムを標的としたランサムウェアによる攻撃、ネットワーク管理ソフトウェアの脆弱性に端を発する大規模な感染、USBメモリやパソコンを接続することによるウイルス感染の増加、という五つの特徴が見られた。



■図3-1-1　国内における制御システムのインシデント報告件数（2013～2020年）
（出典）JPCERT/CCのインシデント報告対応レポート※2を基にIPAが作成

(1) 水道や電力等の重要インフラの制御システムが標的となった事例

海外では、水道や電力等の重要インフラの制御システムが標的となったインシデントが報告された。

イスラエルの水道関連施設が、2020 年 4 月、6 月の 2 度攻撃された。4 月の攻撃は、廃水処理プラント、ポンプ場、下水処理場等 6 ヵ所の施設の SCADA（Supervisory Control And Data Acquisition：監視制御及びデータ収集）システムが標的となったが、イスラエル国家サイバー総局（INCD：Israel National Cyber Directorate）がリアルタイムで攻撃を検知し、阻止した[※6]。ある施設では、ポンプが連続運転状態となり、オペレータが自動運転モードを解除した[※7]。また、攻撃を阻止される前に攻撃者は浄水場の水の塩素レベルを変更しようとしたとの情報もあり、塩素または他の化学物質が誤った比率で水源に混入され、有害な状態のまま供給される恐れがあった[※8]。6 月の攻撃は、二つの農村地域の送水ポンプと農業用水ポンプが標的となったが、被害はなかった[※9]。

両方の攻撃はともに、イランによるものと考えられている。2020 年 5 月には、イラン最大の港であるシャヒード・ラジャーイー港の船舶、トラック、商品の流れを管理するコンピュータがサイバー攻撃を受けてシャットダウンする事態が発生した。これはイスラエルによる報復攻撃とされている[※10]。更に 12 月には、イランのハッキンググループが、イスラエルの再生水貯水池の監視制御システムの HMI（Human-Machine Interface）にアクセスするハッキング動画を公開した。ハッキングによる影響は明らかになっていないが、攻撃者は、貯水池の制御システムに簡単にアクセスし、水圧や温度等のシステム内の値を任意に変更することができた[※11、12]。これらの攻撃の応酬は、イスラエルとイランの国家間のサイバー戦争の様相を呈している。

2020 年 10 月 12 日、インドのムンバイで大規模停電が発生した。停電はムンバイ都市圏に影響を与え、交通管理システムや列車の運行に大きな混乱をもたらし、必要不可欠なサービスの復旧には 2 時間を要した。電力会社や送電会社のサーバへの複数の不審なログインが発見され、これらのサーバが操作されたことが、停電の引き金になったと考えられている。また、電力網の運用を監視、スケジューリングして配電する負荷分散センターの調査員がウイルスを発見したとも報じられている[※13]。

2021 年 2 月 5 日、米国フロリダ州ピネラス郡オールズマー市の浄水場がサイバー攻撃を受けた。攻撃者はリモートアクセスソフトウェアである TeamViewer を介して、SCADA システムにアクセスしたと考えられる。約 5 分間のアクセス中に、攻撃者は水酸化ナトリウムの投入設定値を約 100ppm から 1 万 1,100ppm に変更したが、監視していたオペレータが操作されていることに気付き、すぐに正常な値に戻した。水酸化ナトリウムは液体排水管クリーナーの主成分で、浄水場では水の酸性度をコントロールしたり、飲料水から金属を除去したりするために使用されている。浄水場のすべてのコンピュータの OS は、2020 年 1 月にサポートが終了した Windows 7 で、リモートアクセスに共有パスワードが使われていた[※14]。

(2) IT システムのウイルス感染によって生産や重要サービスが停止した事例

IT と OT の統合が進んでいることから、メールや Web サイト経由の IT システムのウイルス感染が制御システムまで拡大する例や、IT システムの感染から間接的に制御システムが影響を受け、生産ラインや重要サービスが停止する事例が増えている。

表 3-1-1（次ページ）に、2020 年に公にされた、IT システムのウイルス感染によって生産や重要サービスが停止したインシデント事例を示す。

「制御システムは IT システムの影響を受けない」という認識を見直し、攻撃や感染が IT から OT へ広がらないか等、IT、OT 個別の縦割りのリスク管理体制を越えた横断的なリスクの見直しが推奨される。

(3) 制御システムを標的としたランサムウェアによる攻撃事例

2019 年 12 月中旬、制御システムをも標的としたランサムウェア「SNAKE」（別名、EKANS）が新たに出現したが[※24]、ロシアのセキュリティベンダによると、2020 年には多くの企業が同ランサムウェアによる標的型攻撃を受けた[※25]。

2020 年 6 月、本田技研工業株式会社が SNAKE によるものと思われるサイバー攻撃を受けた。社内サーバが攻撃され、同社ネットワークを介してウイルスが拡散し、サーバ、メール、その他のシステムへのアクセスができなくなり、国内外の生産拠点の操業に影響が出た[※26]。

また、同日アルゼンチンの電力会社 Edesur SA（イタリアの多国籍エネルギー企業 Enel SPA の子会社）も、同様の攻撃を受けた。Enel SPA は、同年 10 月にもランサムウェア NetWalker による二度目の攻撃を受け、約 5T バイトのデータを攻撃者に窃取された[※27]。

SNAKE 等、一部のランサムウェアは、ファイルの暗号化といったランサムウェアの機能、データの削除といっ

事例名	発生国	発生年月（報道年月）	影響・被害	内容（原因等）
紡織機械製造企業の生産停止※15	ベルギー	2020年1月	紡織機械製造企業Picanolのベルギー、ルーマニア、中国の工場が約1週間生産停止した。ブリュッセル証券取引所の同社株式が、約3週間売買停止された。	ランサムウェアによる攻撃
天然ガス圧縮施設の停止※16	米国	2020年2月	天然ガス圧縮施設のITシステム及び制御システムがランサムウェアに感染し、2日間停止した。	不正なリンクを含むフィッシングメールによって、ITネットワークがウイルスに感染。制御システムを狙った攻撃ではなかったが、被害に遭った施設のITネットワークとOTネットワークの分離が不十分であったため、OTネットワークのWindowsベースの機器が感染
大手鉄鋼企業の生産停止※17	米国 カナダ	2020年3月	鉄鋼企業Evraz PLCの米国、カナダの複数の鉄鋼生産工場が稼働停止した。	ランサムウェアRyukによる攻撃を受け、ITシステムをシャットダウン
大手鉄鋼企業の製造システムの停止※18	オーストラリア	2020年5月	鉄鋼企業BlueScope Steel Limitedの全社の製造システムが停止した。手動操作に切り替えられた溶鉱炉も停止した。	従業員がメールの添付ファイルを開いたことでウイルスに感染
家電メーカの工場の稼働停止※19	ニュージーランド	2020年6月	家電メーカFisher & Paykel Appliances Holdings Limitedの製造及び流通に影響した。工場が稼働を停止した。	ランサムウェアNefilimによる攻撃。発覚後、すぐにITシステムをシャットダウン
半導体製造企業の生産停止※20	ドイツ	2020年7月	半導体製造企業X-FABの六つの製造拠点（ドイツ3拠点、米国、フランス、マレーシア）の生産が停止した。	ランサムウェアMazeによる攻撃
半導体製造企業の生産停止※21	イスラエル	2020年9月	半導体製造企業Tower Semiconductor Ltd.の一部の製造施設の操業が停止した。	ランサムウェアによる攻撃
大手鉄鋼企業の生産停止※22	カナダ	2020年10月	攻撃の範囲は限定的だったが、鉄鋼企業Stelco Holdings Inc.は予防措置として鉄鋼生産等、一部の業務を一時的に停止した。	ITシステムを標的としたランサムウェアによる攻撃
オフィス家具メーカの生産停止※23	米国	2020年10月	オフィス家具メーカSteelcase Inc.で攻撃の影響を受けたすべてのシステムと関連業務が約2週間、停止した。工場での製品の生産はすべて停止した。	ITシステムを標的としたランサムウェアRyukによる攻撃

■表3-1-1　2020年に公にされたITシステムのウイルス感染によって生産や重要サービスが停止したインシデント事例

た破壊型（ワイパー型）ウイルスの機能に加えて、特定の制御システムのプロセスを強制停止するように設計されている。従って、制御システムの所有者及び運用者は、こうした破壊型ウイルスの攻撃対象や感染する仕組みを理解した上で、防御策を講じることが強く推奨される（ランサムウェアの巧妙化については「1.2.2 新たなランサムウェア攻撃」参照）。

(4) ネットワーク管理用のソフトウェアの脆弱性に端を発する大規模な感染事例

2020年12月、ロシアが関連していると見られるハッキンググループが、米国のSolarWinds Worldwide, LLC.（以下、SolarWinds社）を攻撃し、同社のネットワーク集中監視・管理用のソフトウェアプラットフォームOrionの更新版に「Sunburst」（別名、Solorigate）と呼ばれるウイルスを混入させたことによって、世界中の多くの企業や政府機関のネットワークが感染したことが明らかとなった※28。その後の調査によると、最初の不正アクセスは2019年9月に発生し、Orionの10月の更新版で攻撃コードのテストが実施され、2020年2月からSunburstが仕込まれた更新版が展開されていた※29。そして5月から、「Teardrop」及び「Raindrop」と呼ばれるウイルス※30を使った本格的な攻撃が開始された。この間、SolarWinds社のOrionを使用していた政府機関や大手企業、セキュリティ企業は不正な挙動を検出することができなかったが※31、サイバーセキュリティ企業FireEye, Inc.が2020年12月に不正アクセスを受け、同社の多要素認証ソリューションに不正な端末登録が行われたという警告がきっかけで、この侵害が発覚した※32。

約1万8,000の同製品ユーザが、ウイルスが混入したバージョンをインストールしており、ロシアのセキュリティベンダの調査結果によると、20以上の産業部門の組織が攻撃を受けた可能性がある。その内訳は、製造業8、輸送及びロジスティクス6、ユーティリティ（電力・ガス・

水道等の公共サービス提供組織）4、建設 4、鉱業 3、エネルギー 2、で、地理的な分布は、北米からアジア太平洋まで、ほぼ全世界に及んでいた※33。米国国土安全保障省（DHS：Department of Homeland Security）のサイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA：Cybersecurity and Infrastructure Security Agency）の警告によると、米国の重要インフラ組織への侵害も確認されている※34。また、その後、同ソフトウェアのバグを悪用して、中国との関係が疑われるハッキンググループが、米国政府のコンピュータに侵入していたことも明らかになっている※35。

事業者は所有するソフトウェア及びハードウェア資産を常に正確に把握・管理し、所有資産の脆弱性に関する情報を収集して、新たな脅威に備える必要がある。

(5) USB メモリやパソコンを接続することによるウイルス感染の増加

業務用に持ち込んだ USB メモリやパソコンを接続することによるウイルス感染も、継続して発生している。Honeywell International, Inc. のレポート「Honeywell Industrial Cybersecurity USB Threat Report 2020※36」によると、同社が調査した全脅威のうち、制御システムに大きな混乱を引き起こす可能性のある、USB メモリを媒介とするウイルスの脅威は、2018 年の 26%から 59% へと 2 倍以上増加している。

制御システム運用者は、外部から持ち込む情報端末・機器や媒体の管理、及び接続前のウイルスチェックを今一度徹底させることが重要である。また、内部関係者の不正やヒューマンエラーによるリスクを軽減するために、セキュリティ教育や意識啓発等を通じて、従業員の情報リテラシーや情報モラルを向上させることも重要である。

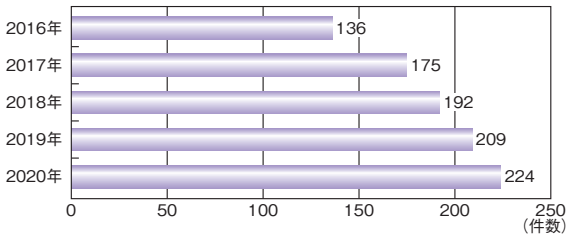
3.1.2 脆弱性及び脅威の動向

本項では、2020 年に見られた、制御システムの脆弱性及び脅威の動向について述べる。

(1) 脆弱性の動向

2020 年も、制御システムの脆弱性が多く公開された。制御システムの脆弱性情報を収集・公開している代表的な組織である米国 DHS の NCCIC（National Cybersecurity and Communications Integration Center）が、2020 年に公開したアドバイザリは 224 件であった。図 3-1-2 に示すように、増加傾向にある。

2020 年に NCCIC から公開された脆弱性で特に目立った傾向は、遠隔から攻撃可能な（Exploitable remotely）脆弱性が 174 件で、77.7%を占めた点である。IIoT（Industrial Internet of Things）機器の導入、クラウドとの接続、新型コロナウイルス感染症（以下、新型コロナウイルス）の感染拡大による遠隔アクセス等の利用拡大に伴い、これらの脆弱性によるリスクが高まっているため、インターネットに直接接続された機器を保護する等の脆弱性対策が重要である。



■図 3-1-2　NCCIC が公開した脆弱性アドバイザリの件数（2016 ～ 2020 年）
（出典）NCCIC の公開情報※37 を基に IPA が作成

非常に影響の大きい脆弱性も発見されている。イスラエルのセキュリティ企業 JSOF Ltd. が、多くの IoT 機器で利用されている米国 Treck, Inc. 製の TCP/IP ソフトウェアライブラリに、リモートでコードが実行可能な複数の脆弱性を発見した※38。「Ripple20」と名付けられたこれらの脆弱性が悪用されると、プリンタからデータが盗まれたり、輸液ポンプの動作が変更されたり、産業用制御機器が誤作動したりと、重要インフラを含む様々な業界で使用される数億個以上もの機器に影響を与える（Ripple20 の詳細については「3.2.2（1）Ripple20」参照）。

また、スペインの産業用サイバーセキュリティ企業 Titanium Industrial Security S.L. は、米 National Instruments Corporation の計測制御システム「CompactRIO」について、攻撃者が遠隔操作によって生産プロセスを混乱させることが可能な脆弱性（CVE-2020-25191※39）を発見した※40。同製品は、重機、製造業、輸送、発電、石油及びガス等の産業分野で使用されており、この脆弱性が悪用されると、生産プロセスが突然停止する可能性がある。米国の CISA は、この脆弱性についてのアドバイザリを発表した※41。

内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）は 2020 年 12 月 3 日、重要インフラ事業者に対し、米国 Fortinet, Inc. の製品の VPN 機能に存

在する脆弱性について、改めて注意を呼びかけた※42。Fortinet, Inc. 製の FortiOS の VPN 機能には、悪用されると、遠隔の第三者が当該製品から任意のファイルを読み込む可能性がある脆弱性（CVE-2018-13379※43）が存在していた。この脆弱性については 2019 年夏ごろより知られていたが、2020 年に入って、この脆弱性の影響を受ける機器や URL のリストがインターネットで公開され、悪用の危険度が増していた。NISC は、公開情報を基に情報収集・分析を行い、重要インフラ事業者等 218 社の VPN 装置、4,954 の IP アドレスが当該脆弱性の影響を受けることを確認し、所管省庁に対して注意喚起を行った（FortiOS の脆弱性を悪用した攻撃については「1.2.5(1)(a)攻撃事例」参照）。

脆弱性が公表された機器の所有者は、脆弱性の影響及び対応の可否を確認し、速やかに必要な対策を実施することが推奨される。

(2) 脅威の動向

2020 年の脅威の動向としては、「3.1.1 (3) 制御システムを標的としたランサムウェアによる攻撃事例」に示したようなランサムウェア攻撃の進化が挙げられる。

産業組織へのランサムウェア攻撃は、2018 年 1 月から 2020 年 10 月までの間に 6 倍に増加している※44。攻撃手法は、無差別にランサムウェアをばらまく攻撃から、特定の企業・組織を狙った「標的型」のランサムウェアへと劇的に進化した。更に、より確実に金銭的な利益を得るために、暗号化したデータの解読の脅迫に加え、標的企業から機密データを窃取し、それを公開すると脅迫して、身代金の支払いを強制する「二重の脅迫」（double extortion）が増えており、2020 年は、ランサムウェア Maze、RagnarLocker、Netwalker、Revil/Sodinokibi 等を使用する攻撃グループがこうした手法を使用していた※45（手口の詳細は「1.2.2 新たなランサムウェア攻撃」参照）。また、ランサムウェア Maze と Revil/Sodinokibi を使用する攻撃グループは、RaaS（Ransomware as a Service）モデルを使用しており、利益の一部を得る見返りにランサムウェアを複数の攻撃グループに提供していた。これによって、経験の浅い攻撃グループが、高度なツールを入手することができた※46。

「二重の脅迫」の事例としては、2020 年 3 月、米国の航空機メンテナンス専門企業 VT San Antonio Aerospace, Inc. が、ランサムウェア Maze を使った攻撃を受けた。攻撃者はサーバを暗号化する前に、1.5T バイト相当のファイルを窃取し、身代金を要求した。また、攻撃の証拠として財務スプレッドシート、サイバー保険契約等の 100 を超えるドキュメントを 4 月に公開した。攻撃者が公開したメモによると、まず侵害した管理者アカウントを使用して、同社のサーバにリモートデスクトップ接続し、次にデフォルトのドメイン管理者アカウントを侵害して、同社の二つのドメインにおいて、ドメインコントローラ、イントラネットサーバ、及びファイルサーバを攻撃した※47。

また、2020 年 5 月には、米国の半導体メーカ MaxLinear, Inc. が、ランサムウェア Maze による攻撃を受けた。同社コンピュータシステムの一部が暗号化され、1T バイト以上のデータが窃取された。その後同社が身代金を支払わなかったことから、攻撃者は 6 月 15 日に、窃取したデータのうち、10.3G バイトの会計・財務情報を公開した。同社が 6 月 16 日に米証券取引委員会に提出した文書によると、出荷、受注処理、及び生産には影響はなかった※48。

ランサムウェアへの対策として、基本的なウイルス対策、通信制御による対策、重要なデータのバックアップが適切に実施されているかの確認、等の感染や脅迫に備えたリスク管理対策を徹底することが推奨される（「1.2.2 (4) 新たなランサムウェア攻撃への対策」参照）。

3.1.3 海外の制御システムのセキュリティ強化の取り組み

本項では、海外における制御システムのセキュリティ強化に関する取り組みについて述べる。

(1) 米国政府の取り組み

米国 DHS の CISA は、2020 年 7 月、制御システムのサイバーセキュリティを強化するための新戦略「Securing Industrial Control Systems: A Unified Initiative※49」を発表した。この戦略の目的は、制御システムコミュニティである事業計画立案者、事業オーナー、オペレータ、ベンダ、インテグレータ、研究者等の、よりセキュアな制御システム運用につながる能力開発の支援であり、最終的には、CISA と制御システムコミュニティが、受動的な ICS セキュリティ対策から、より積極的な対策をとるようになることを目指している。

米国国立標準技術研究所（NIST：National Institute of Standards and Technology）は、製造業界向けのサイバーセキュリティフレームワーク「Cybersecurity Framework Version 1.1 Manufacturing Profile: NISTIR 8183 Revision 1※50」を 2020 年 10 月に公開した（「3.4.2 (4) フレームワーク」参照）。本文書は、製造

業の事業目標と業界のベストプラクティスに沿ってサイバーセキュリティリスクを軽減するためのロードマップとして使用できる。また、サイバーセキュリティ活動を管理し、製造システムに対するサイバーリスクを軽減するためのリスクベースのアプローチを提供している。

(2) 海事業界のセキュリティ

近年デジタル化が進んでいる海事業界でも、VSAT（Very Small Aperture Terminal）衛星通信技術の発達による船舶のインターネット常時接続の普及、船舶の運行データを陸上でモニタリングする等の船舶・陸上間のデータ共有の増加、船舶用機器のコンピュータ化や通信接続に伴い、船舶システムがウイルス感染や不正アクセスといったサイバー攻撃に晒されるリスクが高まっている。サイバーセキュリティ企業のレポートによると、海事業界の OT システムに対するサイバー攻撃は、過去 3 年間で 10 倍増加している※51。

2017 年 6 月の国際海事機関（IMO：International Maritime Organization）の第 98 回海上安全委員会において決議された「安全管理システムにおける海事サイバーリスクマネジメント（Res. MSC.428(98)）※52」では、2021 年 1 月以降、船舶のサイバーリスク対策は、船主・運航者の安全管理システム（SMS:Safety Management Systems）で対応することが強く推奨されている。

2020 年 12 月には、海運業界団体等から、海事サイバーセキュリティに関するガイドラインも公開された。これは、ボルチック国際海運協議会（BIMCO：Baltic and International Maritime Council）、国際海運会議所（ICS：International Chamber of Shipping）、国際乾貨物船主協会（INTERCARGO：International Association of Dry Cargo Shipowners）等の主要な海運業界団体が協力して策定した業界向けサイバーセキュリティガイドライン「The Guidelines on Cyber Security Onboard Ships」の第 4 版である※53。主な特徴として、サイバーリスク管理のベストプラクティスが更新され、リスクとリスク管理の概念が改善されている。

また同年 12 月に、欧州ネットワーク・情報セキュリティ機関（ENISA：EU Agency for Cybersecurity）が、DX（デジタルトランスフォーメーション）と規制強化の中で、欧州の港湾事業者のサイバーリスク管理を支援するためのサイバーセキュリティガイドライン「Guidelines - Cyber Risk Management for Port」を公開した※54。本ガイドラインは、2019 年のレポート「Port Cybersecurity※55」をベースに、欧州の海事部門が直面しているサイバーセキュリティの脅威とデジタル環境の変化に対応した実用的なプラクティスを提供している。

3.1.4 国内の制御システムのセキュリティ強化の取り組み

本項では、制御システムを含む、重要インフラサービスのセキュリティ強化に関する国内の主な取り組みの概要を紹介する。

(1) 日本政府の取り組み

包括的な重要インフラのセキュリティ政策については、「2.1.1 政府全体の政策動向」及び「2.1.2 経済産業省の政策」を参照されたい。ここでは特に、制御システムのセキュリティ強化に関連する取り組みについて触れる。

NISC が、2018 年度の我が国を取り巻くサイバーセキュリティの情勢、及び 2018 年 7 月に発表した「サイバーセキュリティ 2018」に掲げられた具体的な施策の実施状況等をまとめた「サイバーセキュリティ 2020※56」（2019 年度報告・2020 年度計画）を 2020 年 7 月に発表した。本報告の中から、代表的な取り組みを紹介する。

2020 年 4 月、国土交通省の支援のもと、交通機関へのサイバー攻撃に対抗するために、重要インフラ事業者等（航空、空港、鉄道、物流）が情報共有・分析及び対策を連携して行う組織として、一般社団法人交通 ISAC※57 が創設された。

経済産業省は、2020 年 11 月に、IoT や AI によって実現される「Society 5.0※58」及び「Connected Industries※59」における、フィジカル空間とサイバー空間のつながりの信頼性の確保の考え方を整理した「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」を策定した※60。IoT-SSF を活用することにより、フィジカル・サイバー間をつなぐ IoT 機器・システムに潜むリスクを踏まえて、機器・システムのカテゴライズを行い、カテゴリごとに求められるセキュリティ・セーフティ要求の観点を把握し、カテゴリ間で比較することが可能となる。

また、2021 年 2 月、経済産業省の「産業サイバーセキュリティ研究会 WG1」の電力 SWG は、小売電気事業者が各々の事業モデルに適したサイバーセキュリティ対策を実践していくための指針となる「小売電気事業者のためのサイバーセキュリティ対策ガイドライン Ver.1.0※61」を公開した。

(2) IPA の取り組み

2020 年、IPA では制御システムのセキュリティに関し

て、大きく二つの取り組みを行った。

(a) 制御システムのセキュリティリスクアセスメント普及活動

制御システムに対するセキュリティリスクアセスメントの普及を目的として、「制御システムのセキュリティリスク分析ガイド※62」(以下、リスク分析ガイド) を用いてリスク分析手法を解説するオンラインセミナーを 2020 年 9 月と 2020 年 12 月～ 2021 年 1 月の 2 回開催※63 した。同セミナーでは、約 350 社・団体からの受講者が、リスク分析ガイドを解説した合計約 3 時間の講義動画の視聴や、電子メールによる質疑応答を行った。また、過去数年間にわたって実施している重要インフラのリスク分析支援事業を、2020 年度は新電力分野及び物流分野に対して実施した。

また、「制御システム関連のサイバーインシデント事例シリーズ」を 2019 年 7 月以降、順次公開しており、2020 年は、事例 4 ～事例 7 を公開した※64 (表 3-1-2)。本シリーズでは、過去のインシデント事例の概要と攻撃の流れ (攻撃ツリー) を紹介しており、制御システム保有事業者は、リスク分析ガイドで提唱している「事業被害ベースのリスク分析※65」を実施する際に、事例に相当する攻撃ツリーの作成、セキュリティ対策の策定に活用することができる。

(b) 制御システムのサイバーセキュリティ人材の育成

2017 年 4 月に発足した産業サイバーセキュリティセンター (ICSCoE : Industrial Cyber Security Center of Excellence) では、模擬プラントを用いた演習や、攻撃防御の実践経験、最新のサイバー攻撃情報の調査・分析等を通じて、社会インフラ・産業基盤のサイバーセキュリティリスクに対応する人材の育成を支援している (「2.3.2 産業サイバーセキュリティセンター」参照)。2020 年は、リスク分析ガイドの演習付き講義 (3 日間) を、中核人材育成プログラム 4 期生に対して実施した。

No.	表題	内容	被害
1	2015 年ウクライナ大規模停電	制御端末の外部からの遠隔操作	大規模長時間停電
2	2016 年ウクライナマルウェアによる停電	マルウェアによる遮断器の操作	大規模停電
3	2017 年安全計装システムを標的とするマルウェア	安全計装機器への攻撃スクリプト送信	制御システムの停止
4	Stuxnet : 制御システムを標的とする初めてのマルウェア	USB メモリとゼロデイ脆弱性を利用した破壊工作	遠心分離機の破壊
5	2019 年ランサムウェアによる操業停止	情報系を中心としたシステム破壊	生産量の激減
6	2018 年 半導体製造企業のランサムウェアによる操業停止	ランサムウェアに感染した新規導入機器からの感染拡大と暗号化	製造システムの操業停止
7	2020 年 医療関連企業のランサムウェアによる業務停止	電子カルテサーバからのデータ窃取	業務停止と患者の個人情報の漏えい

■表 3-1-2 「制御システム関連のサイバーインシデント事例」シリーズ

COLUMN

自動車が守るべきセキュリティ基準

自動車は非常によくできた工業製品で、自動車に備わる機能そのものの問題で深刻な事故につながることは、滅多にないものです。これは自動車産業界挙げて技術の蓄積や安全基準遵守に取り組み、危険の芽をことごとく摘み取り、改善してきた賜物ですが、近年は潮目が変わってきました。「悪意のサイバー攻撃」により、自動車のセキュリティが脅かされ、自動車の機能そのものに悪影響を与えて安全が脅かされる事態が現実になってきたためです。

最近の自動車は、ソフトウェアで制御されている車載部品や通信経路が非常に多く、サイバー攻撃を受ける可能性が高まっています。外部と情報通信を行うコネクテッドカーや高度な自動運転を目指す流れともあいまって、自動車を制御する車載システムのセキュリティは、今どきの自動車のいわば「アキレス腱」になりました。こうした背景により、業界全体で自動車のセキュリティを確保するための検討を行う機運が高まり、この際、世界の英知を集め、国際的なセキュリティの標準や規格を定め、みんなでセキュリティをしっかりと確保していこう、という動きが盛んになっています。

主な動きの一つが、国連の欧州経済委員会（UNECE）のもとに組織された自動車基準調和世界フォーラム（WP29）の自動運転専門分科会（GRVA）の専門家会議による国際的なサイバーセキュリティ規則（UNR）の策定です。2020 年 6 月、WP29 により自動車へのサイバー攻撃対策を義務付ける指針が採択されました。我が国における自動車の開発や販売に際しても、今後、自動車メーカ・自動車部品メーカが遵守すべきサイバーセキュリティの法規の指針となるもので、これを遵守していかないと世界各地で車両の型式認定の相互承認がうまくいかず、自動車を販売することが難しくなりそうです。

動きをもう一つ挙げるなら、国際標準化機構（ISO）と自動車技術者協会（SAE）のジョイントビジネスによる自動車セキュリティの国際標準規格 ISO/SAE 21434 の策定でしょうか。こちらは、車載システムだけでなく、ネットワークでつながる外部のシステムまでも対象とした幅広いサイバーセキュリティ対策全般についての規格で、WP29 の規則でも具体的な実施要件としてこの規格を参照することになっています。この国際規格は、自動車製造時のセキュリティへの配慮だけでなく、サプライヤーを含めたサプライチェーン全体の組織としての認証や、車両のライフサイクル全般の活動にも言及し、ソフトウェアアップデート等、運用フェーズのシステムの脆弱性管理等についても対策が要求されています。

今後も、いろいろなアップデートが予想される自動車のセキュリティ基準の動向に注目しましょう。

3.2 IoTの情報セキュリティ

IoT（Internet of Things）技術の普及とともに、インターネット接続機能を有するコンピュータ以外の機器（IoT 機器）がサイバー攻撃の対象となり、10 年以上が経過した。新型コロナウイルス感染拡大に伴い、2020 年は新しい生活様式やテレワークを狙うサイバー攻撃が目立った反面、IoT のセキュリティ脅威に関する報道や情報公開は減少傾向にあった。しかしながら、IoT に対する脅威は継続的に存在しており、ゼロデイ脆弱性を感染手段に取り入れる等、攻撃手法の悪質化が進んでおり、脅威の深刻さを正しく理解して対策を推進する必要がある。

本節では、IoT に対する脅威の動向、IoT セキュリティのサプライチェーンリスク、脆弱な機器とウイルス感染の実態、セキュリティ対策強化の取り組みについて述べる。

なお、本節中で記載されている脆弱性のうち、脆弱性データベースの登録 ID を記載しているものについては、表 3-2-1 に記載の各データベースで検索することによって、概要、詳細情報、関連情報へのリンク等を確認できる。

登録 ID の表記例	登録先データベース
CVE-20xx-xxxxx	NVD※66
JVNDB-20xx-xxxxxx	JVN iPedia※67
EDB-ID: xxxxx	Exploit Database※68

■表 3-2-1　脆弱性の登録 ID の表記例と登録先データベース

3.2.1 継続するIoTのセキュリティ脅威

「情報セキュリティ白書 2020」の本節では、IoT 機器に感染するウイルスを「機器乗っ取り型ウイルス」「機器保護型ウイルス」「機器破壊型ウイルス」の 3 種類に分類し、各分類のウイルスの状況を解説した。2020 年は、機器保護型ウイルスと機器破壊型ウイルスについて、目立った活動は見られなかった。一方、Mirai 及び Gafgyt に代表される機器乗っ取り型ウイルス※69 に関しては、新たな脆弱性の攻撃コード（PoC※70）を取り込み、様々な亜種・新種が発生している。

本項では、2020 年に発生した機器乗っ取り型ウイルスに関して、以下の報告について、時系列（一部例外を除き情報公開順）に沿って紹介する。

- IoT 機器に感染するウイルスや、ウイルスに感染した IoT 機器で構成されたボットネットの検知・検出
- 特定の IoT 機器の脆弱性を狙う攻撃活動・感染拡大活動の観測
- 上記サイバー攻撃に悪用可能な IoT 機器の脆弱性の発見

(1) TVT 社製 NVMS-9000 の脆弱性を狙う Mirai の亜種

2019 年 12 月 28 日から 2020 年 2 月 5 日にかけて、Mirai の亜種と考えられるウイルスによる TCP ポート番号 4567 へのアクセスの増加が観測された※71。アクセスの中には、Shenzhen TVT Digital Technology Co., Ltd.（深圳市同为数码科技股份有限公司。以下、TVT 社）製のデジタルビデオレコーダー（DVR：Digital Video Recorder）である NVMS-9000 及びその OEM 製品が有する脆弱性に対する攻撃コード※72 が含まれていた。攻撃コードに示す手順に従ってリモートから文字列を送信すると、ID とパスワードを含む設定ファイルを返す脆弱性が存在しており、認証情報を窃取しようと試みる攻撃であった。同機種には、リバースシェル※73 を用いてリモートコードを実行可能な脆弱性も存在しており、2019 年 10 月以降、この脆弱性の悪用を試みるアクセスが観測されていた※74。TVT 社は、2018 年 4 月にファームウェアの更新を呼びかけていた※75 が、適用せずにウイルス感染した機器が確認された。TVT 社製 DVR には 70 社以上の OEM 先が存在しており※76、世界中に感染対象機器が散在していると考えられる。

(2) PixelStor5000 の脆弱性を狙う Mirai の亜種「SORA」「UNSTABLE」

2020 年 2 月 5 日、Rasilient Systems Inc. 製の監視ビデオカメラ用ストレージシステム PixelStor5000 の非認証リモートコード実行の脆弱性（CVE-2020-6756（JVNDB-2020-001330））の悪用を試みる Mirai の亜種が発見され、「SORA」「UNSTABLE」と名付けられた※77。これらの新しい亜種は、従来の亜種と同様に、以下の脆弱性の悪用を試みる。

- CVE-2017-17215（JVNDB-2017-013014）：Huawei Technologies Co., Ltd 製ホームルータ HG532 の任意のコード実行の脆弱性
- CVE-2018-10561（JVNDB-2018-004885）：DASAN

Networks, Inc. 製 GPON ルータの認証回避の脆弱性

更に、「UNSTABLE」は、以下の脆弱性の悪用を試みるとともに、UPX 圧縮を用いて実行バイナリのサイズを縮小し、検出を回避することを試みていた。

- EDB-ID: 45978：Web アプリケーションフレームワーク「ThinkPHP 5.0.23/5.1.31」を用いた各機器の任意のコード実行の脆弱性

(3) Zyxel 社製 NAS の脆弱性を狙う Mirai の亜種「Mukashi」

2020 年 3 月 19 日、Zyxel Networks Corporation（合勤科技股份有限公司。以下、Zyxel 社）製 NAS（Network Attached Storage）のコマンドインジェクションの脆弱性（CVE-2020-9054（JVNDB-2020-001758））を狙う Mirai の亜種が発見され、「Mukashi」と名付けられた※78。悪用が極めて容易な脆弱性であり、同年 2 月 24 日から 3 月 11 日にかけて、Zyxel 社からアドバイザリが公開・更新されている※79。

(4) LILIN 社製 DVR のゼロデイ脆弱性を狙う攻撃

2020 年 3 月 20 日、Merit LILIN Ent. Co., Ltd.（利凌企業股份有限公司。以下、LILIN 社）製 DVR のゼロデイ脆弱性の悪用を試みるボットネットの情報が公開された※80。このゼロデイ脆弱性は、以下に示す 3 種類の脆弱性からなる。

- ハードコーディングされた認証情報（root/icatch99、report/8Jg0SE8K50）
- NTP 時刻同期コマンド NTPUpdate におけるコマンドインジェクションの脆弱性
- 設定ファイル中の FTP パラメータ及び NTP パラメータ改ざんによるコマンドインジェクションの脆弱性

2019 年 8 月 30 日、Mirai の亜種「Chalubo※81」による悪用で存在が認識されたこの脆弱性は、2020 年 1 月 11 日に Mirai の亜種「fbot※82」、同月 26 日に Mirai の亜種「Moobot※83」による悪用が確認され、LILIN 社に報告された。2020 年 2 月 13 日、LILIN 社は脆弱性を解消した更新ファームウェアを公開した※84。

(5) Xiongmai 社製 DVR/NVR のゼロデイ脆弱性を狙う攻撃

2020 年 2 月 11 日以降、Mirai の亜種と考えられるウイルスによる TCP ポート番号 9530 へのアクセスの増加が観測された※85。アクセスの中には、HiSilicon Technology Co., Ltd.（海思半导体有限公司）製 SOC チップセットと Hangzhou Xiongmai Technology Co., Ltd.（杭州雄迈信息技术有限公司。以下、Xiongmai 社）製ファームウェアを用いた DVR ／ネットワークビデオレコーダー（NVR：Network Video Recorder）及びその OEM 製品が有する脆弱性に対する攻撃が含まれていた。TCP ポート番号 9530 宛に「OpenTelnet:OpenOnce」という文字列を送信し、所定の応答を行うことで telnet を起動して外部からバックドアとして悪用可能となっており、2 月 4 日にゼロデイ脆弱性として公開されていた※86。2 月 20 日、Xiongmai 社は脆弱性情報を含むアドバイザリを公開した※87。インターネット接続機器検索サービス Shodan※88 を用いて当該機器を調査したところ、2020 年 3 月 23 日時点で全世界に約 26 万台が存在しており、うち約 1,900 台は日本国内であると報告されている※89。当該機器は、telnet を有効化した後、既知の認証情報の初期値（表 3-2-2）を用いたブルートフォース攻撃でログインし、外部から DVR/NVR に記録された映像データに不正アクセス可能となっていた。

ユーザ名	パスワード
root	xmhdipc
root	klv123
root	xc3511
root	123456
root	jvbzd
root	hi3518

■表 3-2-2　Xiongmai 社製 DVR/NVR の認証情報の初期値
（出典）Habr「Full disclosure: 0day vulnerability (backdoor) in firmware for Xiaongmai-based DVRs, NVRs and IP cameras※86」を基に IPA が編集

(6) DrayTek 社製ルータのゼロデイ脆弱性を狙う攻撃

2020 年 3 月 27 日、DrayTek Corporation（居易科技中国分公司。以下、DrayTek 社）製ブロードバンドルータの 2 種類のゼロデイ脆弱性の悪用を試みるボットネットの情報が公開された※90。これに先立ち、2019 年 12 月 4 日、DrayTek 社製 Vigor エンタープライズルータのコマンドインジェクションの脆弱性（認証処理において暗号化されたユーザ名とパスワードを復号する際のパラメータのフィルタリング漏れ）を狙う攻撃が検出され、同月 25 日、ゼロデイ脆弱性に対する攻撃として情報公開された。2020 年 1 月 28 日、同ルータのもう一つのコマンドインジェ

クションの脆弱性を狙う攻撃が検出された。2月1日、NVDにおいてCVE-2020-8515として脆弱性情報が公開された。2月6日、DrayTek社は脆弱性を解消した更新ファームウェアを、同月10日、本脆弱性に関するアドバイザリを公開した※91。

当該ルータには、その後も新たな脆弱性が発見されており、DrayTek社は4月8日、6月24日、2021年1月8日にアドバイザリを公開している※92。

(7) Gafgytの亜種「Hoaxcalls/XTC」

2020年4月3日、Gafgytの新たな亜種が発見され、C&Cサーバ※93との通信に用いるIRC※94チャネル名から「Hoaxcalls」と名付けられた※95。Hoaxcallsは、3月31日に攻撃コード※96が公開されたDrayTek社製ルータの脆弱性（CVE-2020-8515（JVNDB-2020-001735）、(6)参照）や、Grandstream Networks, Inc.製IP電話交換機Grandstream UCM6200のSQLインジェクションの脆弱性（CVE-2020-5722（JVNDB-2020-003190））を感染拡大に悪用する。

2020年4月20日、Hoaxcallsの亜種が発見された※97。この亜種は、3月9日に公開された※98、Zyxel社製Cloud CNM SecuManagerにおける非認証リモートコード実行の脆弱性（CVE-2020-15348（JVNDB-2020-007350）、CNVD-2020-16839※99）を攻撃対象に追加していることが判明した。Zyxel社は3月13日に本脆弱性を含む複数の脆弱性の存在を認めた※100が、日本国内においても4月12日以降、本脆弱性を狙ったTCPポート番号9673へのアクセスが観測されている※101。

2020年4月24日、Hoaxcallsの更なる亜種が発見された※102。3月26日に詳細が公開されたSymantec Corporation（現、Broadcom Ltd.）製Symantec Secure Web Gateway 5.0.2.8（ライフサイクル及びサポートの終了した旧製品）の認証後リモートコード実行の脆弱性※103を攻撃対象として追加するとともに、感染機器のリモートコントロール機能が強化されている。

なお、Hoaxcallsは、攻撃時のHTTP通信で用いるUser-Agentの値から「XTC」とも命名されており※104、5月以降も引き続き活発な活動が観測されている※105。

(8) Netlink社製GPONルータのゼロデイ脆弱性を狙う攻撃

2020年4月15日、Netlink ICT Pvt Ltd.（以下、Netlink社）製GPONルータのゼロデイ脆弱性の悪用を試みるMiraiの亜種Moobot及びGafgytの亜種によって構成されたボットネットの情報が公開された※106。これに先立ち、2020年2月28日、Moobotによる未知のエクスプロイトを用いた感染拡大の試みが検出され、3月17日、Netlink社製ルータのゼロデイ脆弱性を狙った攻撃であると認識された後、翌18日、Exploit Databaseにおいて、リモートコード実行の脆弱性（EDB-ID: 48225）として、攻撃コードとともに公開された。その後、3月19日には同攻撃コードのGafgytの亜種への取り込み、同月26日、Gafgytボットネットによるスキャン活動も検出されている。この時点において、Netlink社及び9社のOEM製品が感染対象となることが確認されている。

また、3月25日、公開後の同脆弱性を狙うMiraiの新たな亜種が発見され、亜種の命名に用いられるウイルスのファイル名には「rispek」の文字列が含まれていた※107。

(9) Moobotの亜種「LeetHozer」

2020年4月27日、Miraiの亜種Moobotを更に発展させたと考えられる新たなウイルス「LeetHozer」の情報が公開された※108。3月26日に発見されたLeetHozerは、Xiongmai社製ファームウェアを持つDVR/NVR等を攻撃対象としており、独自の暗号化方式や接続経路を匿名化するTor（The Onion Router）ネットワーク上のC&Cサーバとの通信機能を有する。

(10) D-Link社製ルータDIR-865Lの脆弱性

2020年2月28日、D-Link Corporation（友讯科技股份有限公司。以下、D-Link社）製ルータDIR-865Lの以下に示す6種類の脆弱性が発見されてD-Link社に報告された後、同年6月12日に情報が公開された※109。

- CVE-2020-13782（JVNDB-2020-006052）：コマンドインジェクションの脆弱性
- CVE-2020-13783（JVNDB-2020-006053）：情報漏えい（管理者パスワードの平文保存）の脆弱性
- CVE-2020-13784（JVNDB-2020-006054）：予測可能なseedを用いた疑似乱数生成の脆弱性
- CVE-2020-13785（JVNDB-2020-006038）：不十分な暗号強度（パスワードのブルートフォース攻撃に悪用可能な情報を平文のまま送信）の脆弱性
- CVE-2020-13786（JVNDB-2020-006039）：クロスサイトリクエストフォージェリの脆弱性
- CVE-2020-13787（JVNDB-2020-006040）：情報漏えい（パスワードを平文のまま送信するWEP（Wireless

Equivalent Privacy）を実装）の脆弱性

DIR-865L は 2016 年 1 月にライフサイクル及びサポート終了となっていたが、2020 年 5 月 26 日、D-Link 社は脆弱性を解消する更新ファームウェアを公開した※110。

（11）DrayTek 社製ルータを狙う新種「Bigviktor」

2020 年 6 月 17 日、DrayTek 社製 Vigor ルータの脆弱性（（6）参照）を狙う新たなウイルスが発見された※111。ファイル名に用いられた文字列「viktor」と検体中の特別な文字列「big boobs」から「Bigviktor」と名付けられた。Bigviktor は、ドメイン生成アルゴリズム（DGA：Domain Generation Algorithm）を用いて毎月 1,000 個の C&C サーバのドメイン名を生成してドメインを切り替え、C&C サーバの検出を困難とする。また、電子署名を付与したペイロードを JPEG 画像ファイルに偽装して、C&C サーバとの間で通信を行う。

（12）Comtrend 社製ルータ VR-3033 の脆弱性を狙う Mirai の亜種

2020 年 7 月 8 日、Comtrend Corporation（康全電訊股份有限公司。以下、Comtrend 社）製ルータ VR-3033 の OS コマンドインジェクションの脆弱性（CVE-2020-10173（JVNDB-2020-002596））の悪用を試みる Mirai の亜種が発見された※112。この脆弱性は、同年 2 月 27 日に脆弱性情報とともに攻撃コードが公開されていた（EDB-ID: 48142）が、今回初めて悪用が観測された。この亜種は、典型的な認証情報を用いた telnet と Secure Shell（SSH）に対するブルートフォース攻撃に加えて、以下の脆弱性の悪用も確認されている。

- EDB-ID: 48225（（8）参照）
- CVE-2018-17173（JVNDB-2018-010306）：LG SuperSign CMS のリモートコード実行の脆弱性
- EDB-ID: 31683：Linksys E-Series ルータのリモートコード実行の脆弱性
- EDB-ID: 40500：AVTECH Corporation（以下、AVTECH 社）製ネットワークカメラ／ NVR ／ DVR の複数の脆弱性
- EDB-ID: 27044：D-Link デバイスの UPnP SOAP コマンド実行の脆弱性
- EDB-ID: 41471：MVPower DVR のシェルコマンド実行の脆弱性
- CVE-2020-15348（（7）参照）
- EDB-ID: 45978：ThinkPHP 5.0.23/5.1.31 のリモートコード実行の脆弱性

（13）Tenda 社製 AC1900 ルータ AC15 の脆弱性

2020 年 7 月 11 日、Shenzhen Tenda Technology Co.,Ltd.（深圳市吉祥腾达科技有限公司。以下、Tenda 社）製 AC1900 ワイヤレスルータ AC15 の脆弱性についての情報が公開された※113。これに先立ち、同年 1 月 2 日、発見者は Tenda 社に連絡した後、同月 17 日、以下に示す 5 種類の脆弱性の詳細を報告した。

- CVE-2020-10986（JVNDB-2020-007725）：クロスサイトリクエストフォージェリの脆弱性
- CVE-2020-10987（JVNDB-2020-007726）：インジェクションの脆弱性
- CVE-2020-10988（JVNDB-2020-007727）：ハードコーディングされた認証情報の脆弱性
- CVE-2020-10989（JVNDB-2020-007728）：クロスサイトスクリプティングの脆弱性
- CVE-2020-15916（JVNDB-2020-008663）：OS コマンドインジェクションの脆弱性

Tenda 社が報告を無視したため、発見者は半年後に脆弱性の詳細を公開した。

（14）F5 社製ロードバランサ BIG-IP の脆弱性を狙う「SORA」の亜種

2020 年 7 月 11 日、F5, Inc.（以下、F5 社）製ロードバランサ BIG-IP の脆弱性（CVE-2020-5902（JVNDB-2020-007318））を悪用して感染を試みるウイルスが発見された※114。ウイルスのファイル名から「SORA」（（2）参照）の亜種と考えられる。7 月 1 日に BIG-IP の管理インタフェース TMUI（Traffic Management User Interface）に存在するリモートコード実行の脆弱性が公開されており、F5 社はソフトウェア更新の呼びかけを含むアドバイザリを公開していた※115。この亜種では、以下の脆弱性の悪用も確認されている。

- CVE-2020-1956（JVNDB-2020-008140）：Apache Kylin の OS コマンドインジェクションの脆弱性
- CVE-2020-7115（JVNDB-2020-006059）：Aruba ClearPass Policy Manager の非認証リモートコード実行の脆弱性
- CVE-2020-10173（（12）参照）
- CVE-2020-7209（JVNDB-2020-002007）：HP LinuxKI

のリモートコマンドインジェクションの脆弱性

- CVE-2020-10987（（13）参照）
- CVE-2020-10204（JVNDB-2020-003570）：Sonatype Nexus Repository Manager のリモートコード実行の脆弱性
- EDB-ID: 48225（（8）参照）
- Netgear R7000 ルータのリモートコード実行の脆弱性※116
- EDB-ID: 48646：Sickbeard のリモートコマンドインジェクションの脆弱性

（15）ZeroShell の脆弱性を狙う攻撃

2020 年 7 月 16 日以降、Linux ディストリビューションの一つであり、サーバや組み込み機器用ネットワークサービスとしてルータやファイアウォール機能を提供する ZeroShell の脆弱性を狙う攻撃が観測された※117。以下に示す脆弱性を攻撃対象としており、Mirai の亜種による感染活動と考えられる。

- CVE-2019-12725（JVNDB-2019-006591）：ZeroShell 3.9.0 の OS コマンドインジェクションの脆弱性
- CVE-2009-0545（JVNDB-2009-005813）：ZeroShell 1.0beta11 及びそれ以前の任意のコマンド実行の脆弱性

（16）ADB ポートを狙う Mirai の亜種

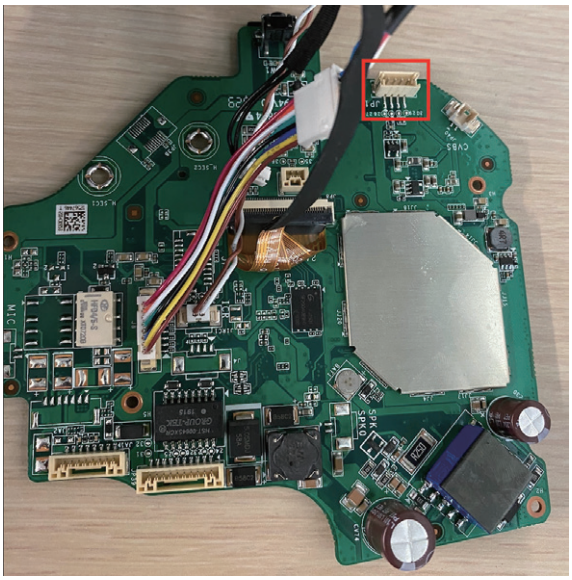
2020 年 7 月 16 日以降、TCP ポート番号 5555 を用いて Android 端末上のコマンド操作を行う ADB（Android Debug Bridge）に対して、特定のコマンドにより外部サーバからシェルスクリプトをダウンロードして実行を試みるアクセスの増加が観測された※118。Mirai またはその亜種と考えられる。ADB ポートを狙った攻撃は 2018 年 2 月 3 日以降観測されるようになった※119 が、再び攻撃が活性化している。

（17）AvertX 社製ネットワークカメラの脆弱性

2020 年 7 月 17 日、AvertX Systems（以下、AvertX 社）製ネットワークカメラ HD838 及び 438IR の脆弱性についての情報が公開された※120。これに先立ち、同年 2 月 24 日、以下に示す 3 種類の脆弱性が発見され、AvertX 社に報告されていた。

- CVE-2020-11623（JVNDB-2020-008740）：公開された危険な機能（UART インタフェースのコネクタが基板上に存在）の脆弱性
- CVE-2020-11624（JVNDB-2020-008828）：脆弱なパスワード要件（管理者アカウントのデフォルトパスワードからの変更が不要）の脆弱性
- CVE-2020-11625（JVNDB-2020-008827）：アカウントの有無によりログイン失敗時の応答が変化し、ユーザアカウントの存在が漏えいする（ユーザ列挙）脆弱性

HD838 及び 438IR は、Hangzhou Hikvision Digital Technology Co., Ltd.（杭州海康威视数字技术股份有限公司）製カメラに変更を加えてブランド名を付け替えた製品であり、AvertX 社は更新ファームウェアを公開した。また、最新製造ロットでは、悪用防止のため基板上から UART コネクタ（図 3-2-1 の赤枠部分）を削除した。



■図 3-2-1　ネットワークカメラの基盤上に設置された UART インタフェースのコネクタ（赤枠部分）
（出典）Palo Alto Networks, Inc.「3 Vulnerabilities Found on AvertX IP Cameras※120」

（18）IoT を狙い始めた「Ngioweb」の亜種

2020 年 8 月 4 日、Ngioweb の亜種が発見された。同月 16 日、x 86（32 ビット／ 64 ビット）、ARM（32 ビット／ 64 ビット）、MIPS（MIPS32 ／ MIPS- Ⅲ）、PPC 等の様々な CPU アーキテクチャ対応に拡張され、IoT 機器も攻撃対象となっていることが確認された※121。Ngioweb は 2019 年 5 月 27 日に初めて発見されたウイルスで、当時は Linux 上で動作する Web サーバを感染対象としていた※122。バージョン V2 と見なされる亜種は、従来のウイルスと比較して、①設定情報の AES 暗号化、② DGA を用いた C&C サーバのドメイン名生成、③ C&C サーバと接続するためのボットネットの入口名を設定ファイル中の記述から選択する、等の特徴を有する。

(19) AVTECH 社製 IP カメラ／ NVR ／ DVR を狙う「Specter」

2020 年 8 月 20 日、AVTECH 社製の IP カメラ／ NVR ／ DVR の複数の脆弱性（EDB-ID: 40500）の悪用を試みる新しいボットネットが発見され、ファイル名に含まれる文字列から「Specter」と命名された※123。Linux 上で動作する IoT 機器を狙ったこのウイルスは、C&C サーバとの通信に TLS 1.2（暗号化アルゴリズム ChaCha20、ハッシュアルゴリズム lz4）を用いて、認証及び暗号化を行う。攻撃手法として高度とは思えない側面（ランタイムライブラリとの動的リンク、メモリへの直接ロード、2016 年 10 月に公開された古い脆弱性の悪用）と、高度な側面（レイヤ設計、複雑なネットワーク通信等）を併せ持っており、開発途中の試験運用ではないかと考えられている。

(20) QNAP 社製 NAS の非公開の脆弱性を狙う攻撃

2020 年 8 月 31 日、QNAP Systems, Inc.（威聯通科技股份有限公司。以下、QNAP 社）製 NAS の非公開の脆弱性の悪用を試みるウイルスの情報が公開された※124。これに先立ち、同年 4 月 21 日以降、非公開の脆弱性（非認証のリモートコマンド実行）を狙う攻撃が観測された後、5 月 13 日に QNAP 社に攻撃コードが報告された。8 月 12 日、QNAP PSIRT（Product Security Incident Response Team）からは「最新版のアップデートで脆弱性は解決済みであるが、未適用機器のインターネット上の存在を確認」との回答が得られた。2017 年 7 月 21 日に脆弱性を解消したファームウェア QTS 4.3.3 が公開されているが、未適用の機器が世界中に散在していると考えられる。

(21) Tenda 社製ルータのゼロデイ脆弱性を狙う「Ttint」

2020 年 10 月 1 日、Tenda 社製ルータのゼロデイ脆弱性の悪用を試みる Mirai の亜種の情報が公開された※125。

これに先立ち、2019 年 11 月 9 日、Tenda 社製ルータのゼロデイ脆弱性を攻撃するウイルスが発見された。感染した IoT 機器を DDoS 攻撃の踏み台に悪用する機能に加えて、ルータの Socket5 プロキシ化、DNS 改ざん、iptables 設定、カスタムシステムコマンド実行等、12 種類の RAT（Remote Access Trojan）機能を実装していた。発見者はこのウイルスによるボットネットを「Ttint」と名付けた。当該のゼロデイ脆弱性は、2020 年 7 月に CVE-2020-10987 として公開された（(13) 参照）。

2020 年 8 月 21 日、Tenda 社製ルータの別のゼロデイ脆弱性（詳細非公開）を攻撃する Ttint の新しい版（v2）が発見された。C&C サーバとの通信に WSS（WebSocket over TLS）プロトコルを用いて、Mirai 型のトラフィック検知を回避しつつ、通信内容を暗号化する機能が拡張されていた。影響を受ける機種は、Tenda 社製ルータ AC9、AC10U、AC15、AC18 等である。脆弱性を有したままインターネットに接続された当該ルータの国別分布を、表 3-2-3 に示す。発見者は 8 月 28 日に脆弱性を攻撃コードとともに報告したが、Tenda 社からは回答は得られていない。

国名	台数
ブラジル	37,967
米国	9,271
南アフリカ	8,847
インド	8,195
ロシア	3,462
中国	3,265
イタリア	2,942

■表 3-2-3　Tenda 社製ルータのゼロデイ脆弱性を有する国別分布
（出典）Qihoo 360 Technology Co., Ltd.「Ttint: An IoT Remote Access Trojan spread through 2 0-day vulnerabilities※125」を基に IPA が作成

(22) P2P プロトコルを用いる自爆機能付き「HEH」

2020 年 10 月 6 日、最近発見された、IoT 機器を狙う未知のウイルスに関する情報が公開された※126。x86（32 ビット／ 64 ビット）、ARM（32 ビット／ 64 ビット）、MIPS（MIPS32 ／ MIPS- Ⅲ）といった様々な CPU アーキテクチャに対応し、ポート番号 23 または 2323 の telnet に対するブルートフォース攻撃を用いて感染拡大を図る。Go 言語で記述されており、独自仕様の P2P プロトコルを用いる。ソースファイルのパス名（プロジェクト名）に「heh」の文字列が用いられていることから、「HEH」と名付けられた。自爆コマンド（コード番号 8）を受信すると、すべてのディスク上の全データを消去する機能が実装されており、証拠隠滅を目的としていると考えられる。

(23) 新しい脆弱性を狙う Mirai の亜種

2020 年 10 月 14 日、IoT 機器の新しい 2 種類の脆弱性と、各々の脆弱性を攻撃する 2 種類ずつ（合計 4 種類）の Mirai の亜種の情報が公開された※127。第一

の脆弱性は、NTP サーバ設定機能を有する Web サービスにおけるコマンドインジェクションの脆弱性（HTTP リクエストのパラメータ NTP_SERVER の値における不十分なサニタイズ※128 処理）で、同年 7 月 23 日から 9 月 23 日にかけて攻撃が観測されていた。

第二の脆弱性は、ある種のリモート管理ツールにおけるコマンドインジェクションの脆弱性（HTTPリクエストのパラメータ pid における不十分なサニタイズ処理）で、8 月 16 日のみ攻撃が観測されていた。

(24) TCP ポート 5501 を狙う Mirai の亜種

2020 年 10 月 20 日以降、TCP ポート番号 5501 への攻撃を試みる Mirai の亜種の活動が観測された※129。海外製 DVR 等への感染を試みる Mirai の亜種と考えられる。

(25) UNIX CCTV 社製 DVR/NVR の脆弱性を狙う「Moobot」の亜種

2020 年 11 月 20 日、UNIX CCTV Corp.（以下、UNIX CCTV 社）製 DVR/NVR のゼロデイ脆弱性（リモートコマンドインジェクション）の悪用を試みる Moobot の亜種に関する情報が公開された※130。これに先立ち、同年 6 月 9 日、ゼロデイ脆弱性を狙うスキャン活動が初めて発見され、同月 24 日、この脆弱性を感染拡大に悪用する Moobot の検体が採取された。感染対象となる DVR/NVR では、ポート番号 8000 でリモート管理機能が有効となっており、システム時間を遠隔更新する際に NTP サーバ名を指定するパラメータのチェック漏れにより、不正なコマンドが実行可能となっていた。インターネット上に約 8,000 台の接続が発見されており、その大半は米国であった。国別分布を表 3-2-4 に示す。8 月 24 日、UNIX CCTV 社は、脆弱性を解消した更新ファームウェアを公開した。

(26) 既知の脆弱性を狙う攻撃の再活性化

2020 年の終わりには、以下のように既知の IoT 機器の脆弱性を狙う攻撃が再活性化した※131。

- 11 月 21 日以降、Huawei Technologies Co., Ltd. 製ルータ HG532 における任意のコード実行の脆弱性（CVE-2017-17215（JVNDB-2017-013014））を狙う Mirai の亜種のアクセスの増加が観測された。
- 12 月 20 日以降、Realtek SDK を用いた IoT 機器における UPnP miniigd SOAP サービスの任意のコード実行の脆弱性（CVE-2014-8361（JVNDB-2014-008039））を狙う Mirai の亜種のアクセスの増加が観測された。
- 12 月 15 日以降、SIA Mikrotīkls 製ルータにおける MikroTik RouterOS の認証に関する脆弱性（CVE-2018-14847（JVNDB-2018-008866））を狙うウイルス Glupteba※132 のアクセス増加が観測された。

国名	台数
米国	4,529
韓国	789
カナダ	84
日本	73
オランダ	66
オーストラリア	56
ドイツ	55
英国	31
ベトナム	23
マレーシア	19
サウジアラビア	15
チェコ	15
スイス	14
中国	11

■表 3-2-4　UNIX CCTV 社製 DVR/NVR のゼロデイ脆弱性を有する国別分布
（出典）Qihoo 360 Technology Co., Ltd.「MooBot on the run using another 0 day targeting UNIX CCTV DVR※130」を基に IPA が作成

3.2.2 IoTセキュリティのサプライチェーンリスク

IoT のセキュリティ対策、特に脆弱性対策を困難としている理由の一つに、IoT 機器のサプライチェーンリスクがある。本項では、2020 年に発生したサプライチェーンに起因する脆弱な IoT 機器の流通事例を紹介する。

(1) Ripple20

2020 年 6 月 16 日、多くの IoT 機器において組み込みソフトウェアとして採用されている Treck, Inc.（以下、Treck 社）製ライブラリの TCP/IP スタックにおいて発見された 19 種類のゼロデイ脆弱性（次ページ表 3-2-5）が報告されるとともに、「Ripple20」と名付けられた※38。脆弱性を有する Treck 社のライブラリは、過去 20 年以上の間、直接的あるいは間接的に世界中で広く利用されており、複数のリモートコード実行の脆弱性を有する IoT 機器が数億台以上存在すると考えられる。脆弱性を発見した JSOF Ltd. は、Treck 社のライブラリを用いた UPS（無停電電源装置）を乗っ取り、UPS に接続され

た輸液ポンプ、プリンタ、照明器具等を誤動作させるデモ動画を公開し、潜在的なリスクの一例を示した※133。

JSOF Ltd. の報告と同日の16日に、DHS傘下のICS-CERTはアドバイザリを公開し、その後も随時情報を更新している※134。

Treck社は、アドバイザリを公開し、最新版への更新を推奨した※135。

1990年代にTreck社と提携していたエルミックシステム株式会社（現、図研エルミック株式会社）製TCP/IPライブラリ「KASAGO」においても、同等の脆弱性が分岐する形で存在しており、6月17日、図研エルミック株式会社は回避策の適用及び修正プログラムの適用を呼びかけた※136。

6月24日、NISCは、ネットワーク製品に組み込まれているライブラリに深刻な脆弱性が発見され、影響範囲が広い反面、特定・対応が容易でないことから、重要インフラ事業者等に向けて、対象製品と対応を含む参考情報を公開した※137。

2020年10月25日の時点で以下の31社の製品に影響が及ぶことが確認されている※38。

- ABB Ltd.
- Aruba Networks（Hewlett Packard Enterprise Co. の一部門）
- AudioCodes Limited
- B. Braun Medical Inc.
- Baxter International Inc.
- Becton, Dickinson and Company（BD）
- ブラザー工業株式会社※138
- Carestream Health, Inc.
- Caterpillar Inc.
- Cisco Systems Inc.
- Dell Inc.※139
- Digi International Inc.
- Eaton Corporation
- Green Hills Software, Inc.
- HCL Technologies Limited
- HP Inc.
- Hewlett Packard Enterprise Co.
- Intel Corporation
- Johnson Controls, Inc.
- MaxLinear, Inc.
- Miele & Cie. KG
- 三菱電機株式会社※140
- Opto 22
- 株式会社リコー※141
- Rockwell Automation, Inc.
- Schneider Electric SE
- Smiths Medical（Smiths Group plc の一部門）
- Telit
- Teradici Corporation
- Xerox Corporation
- 図研エルミック株式会社※136

更に、当該各社の製品をOEM販売している会社や

脆弱性ID	概要
CVE-2020-11896※142 （JVNDB-2020-006776）	リモートコード実行の脆弱性 （CVSS v3 基本値：10）
CVE-2020-11897 （JVNDB-2020-006777）	境界外書き込みの脆弱性 （CVSS v3 基本値：10）
CVE-2020-11898※142 （JVNDB-2020-006778）	情報漏えいの脆弱性 （CVSS v3 基本値：9.1）
CVE-2020-11899 （JVNDB-2020-006779）	境界外読み取りの脆弱性 （CVSS v3 基本値：5.4）
CVE-2020-11900 （JVNDB-2020-006766）	二重解放の脆弱性 （CVSS v3 基本値：8.2）
CVE-2020-11901※143 （JVNDB-2020-006767）	リモートコード実行の脆弱性 （CVSS v3 基本値：9.0）
CVE-2020-11902 （JVNDB-2020-006768）	境界外読み取りの脆弱性 （CVSS v3 基本値：7.3）
CVE-2020-11903 （JVNDB-2020-006763）	境界外読み取りの脆弱性 （CVSS v3 基本値：6.5）
CVE-2020-11904 （JVNDB-2020-006764）	境界外書き込みの脆弱性 （CVSS v3 基本値：7.3）
CVE-2020-11905 （JVNDB-2020-006765）	境界外読み取りの脆弱性 （CVSS v3 基本値：6.5）
CVE-2020-11906 （JVNDB-2020-006758）	整数アンダーフローの脆弱性 （CVSS v3 基本値：6.3）
CVE-2020-11907 （JVNDB-2020-006759）	不特定の脆弱性 （CVSS v3 基本値：6.3）
CVE-2020-11908 （JVNDB-2020-006760）	不特定の脆弱性 （CVSS v3 基本値：4.3）
CVE-2020-11909 （JVNDB-2020-006761）	整数アンダーフローの脆弱性 （CVSS v3 基本値：5.3）
CVE-2020-11910 （JVNDB-2020-006755）	境界外読み取りの脆弱性 （CVSS v3 基本値：5.3）
CVE-2020-11911 （JVNDB-2020-006756）	認証の欠如に関する脆弱性 （CVSS v3 基本値：5.3）
CVE-2020-11912 （JVNDB-2020-006757）	境界外読み取りの脆弱性 （CVSS v3 基本値：5.3）
CVE-2020-11913 （JVNDB-2020-006753）	境界外読み取りの脆弱性 （CVSS v3 基本値：5.3）
CVE-2020-11914 （JVNDB-2020-006754）	境界外読み取りの脆弱性 （CVSS v3 基本値：4.3）

■表3-2-5　Treck社製TCP/IP Stackのゼロデイ脆弱性
（出典）JSOF Ltd.「Ripple20※38」、NVD※66、JVN iPedia※67を基にIPAが作成

自社製品の一部に組み込んでいる会社も含めて、世界中で多くの企業が対応策等の情報公開に追われた。

2020年12月18日、Treck社のTCP/IPスタックにおける4種類の新たな脆弱性が公表された※135。同日、ICS-CERTからアドバイザリが公開されている※145。国内で販売される家電製品等が影響を受け、回避策が公開されている※146。

(2) AMNESIA:33

2020年12月8日、オープンソースとして公開されている4種類のTCP/IPスタック(uIP、FNET、picoTCP、Nut/Net)において発見された33種類の脆弱性が報告されるとともに、「AMNESIA:33」と名付けられた※147。4種類の深刻な脆弱性を含み、150社以上のベンダ、100万台以上のIoT機器に影響を与えるとされている。同日、ICS-CERTはアドバイザリを公開している※148。

(3) サプライチェーンによる影響範囲の拡大

「3.2.1 継続するIoTのセキュリティ脅威」にて紹介した、2020年に発生したIoTのセキュリティ脅威においても、サプライチェーンにより影響範囲が拡大した事例が多く含まれている。

- 複数の会社経由でOEM製品として販売されているIoT機器に脆弱性が発見された例
  該当製品が世界中に拡散している上、エンドユーザは自分が使用している機器がOEM製品であるか否か気付くことが困難である(「3.2.1 (1) TVT社製NVMS-9000の脆弱性を狙うMiraiの亜種」「3.2.1(8) Netlink社製GPONルータのゼロデイ脆弱性を狙う攻撃」「3.2.1 (17) AvertX社製ネットワークカメラの脆弱性」参照)。
- 複数のIoT機器の開発に利用されているハードウェア部品やソフトウェア部品に脆弱性が発見された例
  当該部品を用いた機器が世界中に拡散している上、エンドユーザは自分が使用している機器が該当するか否か気付くことが極めて困難である(「3.2.1 (5) Xiongmai社製DVR/NVRのゼロデイ脆弱性を狙う攻撃」「3.2.1(9)Moobotの亜種『LeetHozer』」「3.2.1(15)ZeroShellの脆弱性を狙う攻撃」参照)。

世界中に同一機種や同等機種が多数散在するIoT機器をウイルス感染対象とすることは、サイバー攻撃者にとっては、容易に多数の機器を侵害することを可能にする。2020年には、このような条件を満たす機器のゼロデイを含む脆弱性を攻撃する傾向が目立った。

サプライチェーンに関わるIoTの脅威として、以下に示す事例も報告されている※149。

- 2020年7月15日、IT企業で発見されたCisco Systems Inc.製ネットワークスイッチCatalyst 2960-Xシリーズの偽物に関する情報が公開された※150。ソフトウェアのアップグレード後に障害が発生したことから、偽造品であることが判明した。明確なバックドア機能は発見されなかったが、偽造品の動作を排除するための検証プロセスを回避するためのアドオン回路が組み込まれていた。
- 2020年3月26日、ファームウェア更新機能を容易に提供可能なため、ネットワーク機器の開発に使用されている組み込み用Linuxディストリビューションのオープンソース OpenWrtに、リモートコード実行の脆弱性(CVE-2020-7982 (JVNDB-2020-003125))が発見された※151。悪用されると不正なファームウェアへの更新に誘導される恐れがあった。

3.2.3 脆弱なIoT機器とウイルス感染の実態

IoT機器を狙うサイバー攻撃が継続する中、ウイルス感染の恐れがある脆弱なIoT機器や実際にウイルス感染したIoT機器は、国内外にどれだけ存在しているのか。本項では、セキュリティ対策強化の取り組みの公開情報等から、脆弱なまま運用されているIoT機器とウイルス感染の実態を考察する。

(1) 国内における実態

総務省及びNICTは、2019年2月以降、インターネット接続事業者と連携し、サイバー攻撃に悪用される恐れのあるIoT機器の調査及び当該機器の利用者への注意喚起を行う取り組み「NOTICE (National Operation Towards IoT Clean Environment)※152」を継続してきた。

2020年6月17日、実施状況の定期的な公表が開始された※153。2020年5月以降の取り組み結果を、表3-2-6(次ページ)に示す(同年4月の調査は新型コロナウイルス拡大防止のため未実施)。

- 「NOTICE注意喚起」(ログイン可能機器利用者への注意喚起)は、2020年10月以降大幅に増加しているが、調査強化(「3.2.4(2)IoT機器調査及び利用者への注意喚起の取り組みの強化」参照)の成果であり、実態としては大きな変化はないと考えられる。

- 「NICTER 注意喚起」（ウイルス感染機器利用者への注意喚起）は、2020 年 8 月のみ大幅に急増しているが、同一機器の IP アドレスが頻繁に切り替わったことによる多重計上の影響であり、実態としては大きな変化はないと考えられる。

	NOTICE 注意喚起（ログイン可能機器）	NICTER 注意喚起（ウイルス感染機器）
2020 年 5 月	287 件	平均 154 件／日
2020 年 6 月	293 件	平均 167 件／日
2020 年 7 月	338 件	平均 209 件／日
2020 年 8 月	309 件	平均 700 件／日
2020 年 9 月	319 件	平均 186 件／日
2020 年 10 月	1,852 件	平均 138 件／日
2020 年 11 月	1,992 件	平均 114 件／日
2020 年 12 月	2,002 件	平均 113 件／日
2021 年 1 月	1,581 件	平均 79 件／日
2021 年 2 月	1,948 件	平均 94 件／日
2021 年 3 月	1,883 件	平均 469 件／日

■表 3-2-6　国内における注意喚起の取り組みの実施結果
（出典）NOTICE サポートセンター「実施状況[※153]」を基に IPA が作成

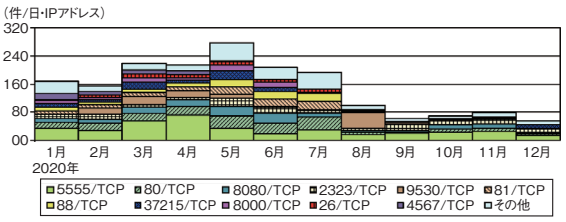
(2) 国内の IoT 機器を狙ったアクセスの観測

警察庁が国内の IoT 機器を狙ったアクセスについて、2020 年 1 ～ 12 月の通年観測状況を公開した[※154]。

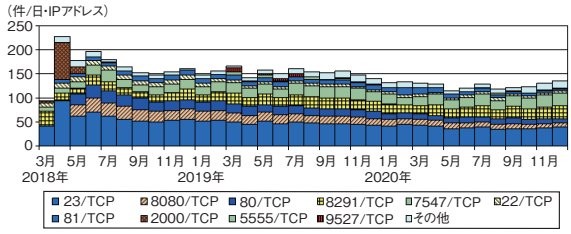
- 機器乗っ取り型ウイルス「Mirai」及びその亜種に感染した IoT 機器で構成されるボットネットによると思われるアクセスは、通年で継続的に観測された（図 3-2-2）。「Mirai」及びその亜種は、特定の IoT 機器の脆弱性を感染拡大手段として随時取り込んでおり、宛先ポートを攻撃の流行に応じて変化させながら、活動を継続していることが分かる。
- 機器保護型ウイルス「Hajime[※155]」に感染した IoT 機器で構成されるボットネットによると思われるアクセスは、通年で継続的に観測された（図 3-2-3）。

(3) DDoS 攻撃の対象国分布

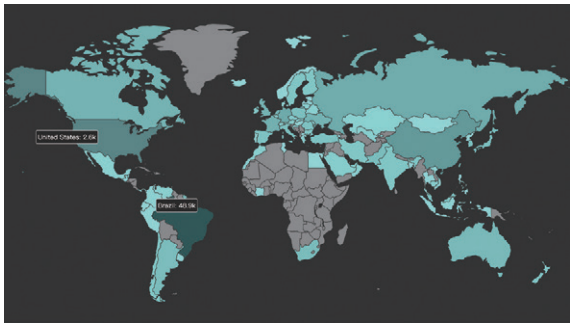
Mirai の亜種 Moobot の活動を観察しているセキュリティベンダが 2020 年 3 月末から 5 月初旬にかけて、数百から 2 万へ急増した DDoS 攻撃について報告している[※156]。図 3-2-4 は攻撃対象の国別分布であり、地図上の濃淡は攻撃数の大小を示す。それによると、攻撃対象国は世界中に分布しているが、ブラジル（約 4 万 8,900）と米国（約 2,600）に集中しており、中国とロシアがそれに続いていることが分かる。



■図 3-2-2　Mirai 及びその亜種と思われるアクセス件数の推移
（出典）警察庁「インターネット観測結果等（令和2年）[※154]」を基に IPA が編集



■図 3-2-3　Hajime と思われるアクセス件数の推移
（出典）警察庁「インターネット観測結果等（令和2年）」を基に IPA が編集



■図 3-2-4　DDoS 攻撃の対象国分布例
（出典）Qihoo 360 Technology Co. Ltd.「An Update for a Very Active DDos Botnet: Moobot[※156]」

3.2.4 セキュリティ対策強化の取り組み

これまで述べたように、IoT に対する脅威は継続しており、世界中に存在する IoT 機器に対して、ゼロデイ対策を含む脆弱性対応やセキュリティ対策を継続的に実施していくことが急務となっている。本項では、対策を検討・推進する上で参考となるセキュリティガイド等の発行状況や、政府の取り組みとしての法規制の強化、民間の取り組みについて紹介する。

(1) IoT 関連セキュリティガイド等の改訂・新規発行

これまでに公開された IoT のセキュリティに関するガイドラインや手引き等の改訂版、新たに発行されたガイドライン等が引き続き公開されている。2020 年以降に国内及び海外で公開された資料を、表 3-2-7（次ページ）と表

3-2-8（次ページ）に示す。

(2) IoT 機器調査及び利用者への注意喚起の取り組みの強化

NOTICE（「3.2.3 (1) 国内における実態」参照）では、IoT 機器を狙う新たなウイルスが継続的に出現し、感染時に悪用される認証情報が増加していることから、2020 年 10 月以降、調査に用いる ID とパスワードの組み合わせを大幅に追加した。また、調査に必要となる通信量が増加することから、調査のための特定アクセス行為の送信元として使用する IP アドレスを増強した（次ページ表 3-2-9）[※157]。

また、国内の重要施設に設置されている IoT 機器において、利用事業者名や用途がインターネット上から容易に判別可能である等、サイバー攻撃を受けやすい状態にある機器が一定数存在することが確認されたため、2020 年 7 月 28 日、一般社団法人 ICT-ISAC は、実態調査、及び該当機器を使用している法人の所有者・運用者等への注意喚起や対策実施の促進を開始した[※158]。

(3) 米国内で拡がる規制の強化

2020 年 1 月 1 日以降、米国カリフォルニア州において IoT 機器の製造業者にセキュリティ対策強化を義務付ける「IoT セキュリティ法[※159]」の施行が開始されたが、米国内の他の州においても規制が強化されている[※160]。

カリフォルニア州に続いて可決されたオレゴン州の IoT

公開機関・団体	公開資料名	対象読者	主な内容	公開年月
経済産業省	IoT セキュリティ・セーフティ・フレームワーク[※60]	設計者、開発者、運用者、利用者	IoT 機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有するための基本的共通基盤（「2.1.2（1）(a) WG1（制度・技術・標準化）」参照）	2020 年 11 月
	機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き[※168]	IoT 機器のセキュリティ検証サービス事業者、検証依頼者（機器製造者）	検証サービス事業者の実施事項、検証依頼者の準備情報、二者間コミュニケーションにおける留意事項、信頼できる事業者の判断基準	2021 年 4 月
総務省	IoT・5G セキュリティ総合対策 プログレスレポート 2020[※169]	IoT セキュリティ関係者	「IoT・5G セキュリティ総合対策」の進捗状況及び今後の取り組み	2020 年 5 月
	IoT・5G セキュリティ総合対策 2020[※170]	IoT セキュリティ関係者	IoT・5G に関するセキュリティ対策の総合的な推進に向けて取り組むべき課題（「2.1.3 (1)『IoT・5G セキュリティ総合対策 2020』の概要」参照）	2020 年 7 月
	電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第 2 版）[※171]	IoT 機器の製造者	インターネットに直接接続する機能を有する IoT 機器に対する規制の強化点	2020 年 9 月
IPA	脆弱性対処に向けた製品開発者向けガイド[※172]	一般消費者が利用するネットワーク接続機器の開発事業者	実施すべき脆弱性対処とその開示方法	2020 年 8 月
一般社団法人 重要生活機器連携セキュリティ協議会（CCDS：Connected Consumer Device Security Council）	IoT 分野共通セキュリティ要件ガイドライン 2021 年版 Ver.1.0[※173]	IoT 機器のサーティフィケーションプログラム（「3.2.4（4）民間における取り組み」参照）申請者	IoT 機器の最低限のセキュリティ要件	2020 年 11 月
	IoT 機器セキュリティ実装ガイドライン ソフトウェア更新機能[※174]	IoT 機器の製造者	ソフトウェア更新機能の実装に関する具体的なセキュリティ要件	2020 年 12 月
一般社団法人日本スマートフォンセキュリティ協会（JSSEC：Japan Smartphone Security Association）	IoT セキュリティチェックシート 第 2.1 版[※175]	IoT を利用・導入する一般企業	IoT 利用・導入時に検討・考慮すべき項目	2020 年 2 月

■表 3-2-7　2020 年以降に国内で新規公開・改訂された IoT 関連のガイドライン等
（出典）各団体の公開情報を基に IPA が作成

公開機関・団体	公開資料名	対象読者	主な内容	公開年月
NIST（National Institute of Standards and Technology：米国国立標準技術研究所）（NISTの成果公開については「3.4.2 成果紹介」参照）	NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers※176	IoT機器の製造者	販売前に（主に設計工程で）考慮すべき推奨事項	2020年5月
	NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline※177	IoT機器の製造者	IoT機器のセキュリティ機能のコアとなるベースライン	2020年5月
	Draft NIST Special Publication 800-213: IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements※178	米国政府機関職員	IoT機器の視点からシステムセキュリティを検討するためのガイダンス	2020年12月
	Draft NISTIR 8259B: IoT Non-Technical Supporting Capability Core Baseline※179	IoT機器の製造者	製造者が導入を検討すべき四つの非技術的サポート機能	2020年12月
	Draft NISTIR 8259C: Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline※180	IoT機器の製造者	特定の顧客またはアプリケーション向けにカスタマイズしたプロファイルの作成方法	2020年12月
	Draft NISTIR 8259D: Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government※181	IoT機器の製造者	8259C記載の方法を用いて作成した米国政府向けプロファイル	2020年12月
ENISA（European Union Agency for Cybersecurity/ European Network and Information Security Agency：欧州ネットワーク・情報セキュリティ機関）	Guidelines for Securing the Internet of Things - Secure Supply Chain for IoT※182	IoTソフトウェアの開発者・製造者、プロジェクトマネージャ、調達チーム	IoTサプライチェーンのセキュリティ脅威、考慮事項、グッドプラクティス	2020年11月
	Cybersecurity Stocktaking in the CAM - Stakeholder mapping and stocktaking of connected and automated mobility (CAM) cyber-security※183	コネクテッドカー／自動運転車のすべての関係者	コネクテッドカー／自動運転車のセキュリティ	2020年11月
ETSI（European Telecommunications Standards Institute：欧州電気通信標準化機構）	ETSI TS 303 645 v2.1.1 (2020-06): CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements※184	コンシューマ向けIoT製品の開発者・製造者	すべてのコンシューマ向けIoT製品に適用可能なベースライン規定	2020年6月

■表 3-2-8　2020年以降に海外で新規公開・改訂されたIoT関連のガイドライン等
（出典）各団体の公開情報を基にIPAが作成

調査時期	ID・パスワード	IPアドレス
～2020年9月	約100通り	41個
2020年10月～	約600通り	54個

■表 3-2-9　NOTICEの取り組み強化
（出典）総務省「サイバー攻撃に悪用されるおそれのあるIoT機器の調査（NOTICE）の取組強化※157」を基にIPAが作成

法（House Bill 2395）も2020年1月1日に施行されており、主に個人・家族・家庭で使用するIoT機器の製造者や販売者に対して、合理的なセキュリティ機能の装備を義務付けている※161。

また、イリノイ州※162、メリーランド州※163、バーモント州、マサチューセッツ州※164、ワシントン州※165においてもIoT法案が提出されている。

(4) 民間における取り組み

民間団体及び民間企業においても、IoTセキュリティ向上のための取り組みが行われている。

- 2020年9月1日、一般社団法人日本スマートフォンセキュリティ協会（JSSEC：Japan Smartphone Security Association）は、「IoTセキュリティチェックシート」（前ページ表3-2-7）をオンラインで解説するセミナー動画「IoTセキュリティチェックシート入門」を公開した※166。
- 2020年11月24日、一般社団法人重要生活機器連携セキュリティ協議会（CCDS：Connected Consumer Device Security Council）は、2019年11月から実施している「IoT機器向けサーティフィケーションプログラム」を拡張し、スマートホーム分野サービス向けプログラムを実施すると発表した※167。

COLUMN

リモート監査が主流となる時代の幕開け!!

リモート監査は、オンサイト監査と同じ、ドキュメント及び記録のレビュー、監査対象の施設の見学、担当者へのインタビュー、監査結果のプレゼンテーション等を、ICT ツールを介して行います。ICT ツールを用いて遠隔から監査を実施する手法は、既に 2008 年に IAF（国際認定フォーラム）の基準文書 MD 4 で公開されていましたが、日本ではそれほど実施されているという印象はありませんでした。しかし、新型コロナウイルスの感染拡大に伴って、日本では多くの監査法人や認証機関、企業で監査／審査が延期されるという事態が発生し、急に利用が拡大していきました。

海外諸国では離れた拠点でリモート監査を実施することに慣れていましたが、日本では対面で話を伺う、直接ドキュメントを確認することが一般的な監査の進め方だったので、リモート監査を実施するための環境を構築することから始めなければなりませんでした。

第一段階として、自宅でテレワークを行うためのインフラ環境として普及した Web 会議サービスを利用した監査の検討が進みました。そして、証跡として文書確認は事前にできるものの現場観察が不足していたことから、デバイス（スマートフォン、タブレット PC）、書画カメラ等を用いて現場確認を行うことで証跡を補うことができるようになりました。第二段階でビデオ機能を搭載したスマートフォンやタブレット等のモバイルテクノロジーと組み合わせたライブストリーミング、更に第三段階でスマートグラス技術とビデオヘッドセットを組み合わせたライブストリーミング等の利用が検討されています。

このように、観る、聴く、伺うといったことはリモート監査でもできるようになりつつありますが、監査員が現場で直接感じ、経験として蓄積してきたノウハウ、例えばインタビュー相手の態度（表情以外）や職場の雰囲気、日常的に使用されている文書かを知る紙質、古さ加減、データセンター、サーバルーム、情報機器等の異常（温度、異音、異臭等）等からリスクを認識することは困難です。

リモート監査をより効果的なものとしていくためには、データに注目した確認が重要です。どのようなデータがどこ（クラウド、業務システム、部門サーバ等）にあるのか、そのデータ項目の存在意義は何か等を把握し、更には、ワークフローや業務システムではどのようなログが取得され、どの程度の期間保存されているのかを把握する必要もあります。そして、これらのデータを活用している AI、ビッグデータ、IoT、RPA 等、様々な ICT にどのようなリスクがあるのかを認識し、その大きさを評価するような監査が求められています。

このようにリモート監査では、過去のみが監査の対象ではなく、未来を見て組織の予測を行い、改善提案を行うことが重要となります。これからの組織はリスクに対する想像力を高めるようなリモート監査を要件として取り組むことが重要ではないでしょうか。

3.3 テレワークの情報セキュリティ

2020 年 4 月 7 日、新型コロナウイルス拡大防止のために緊急事態宣言が発出され、外出自粛が求められたことにより、多くの企業・組織で、オフィス以外の場所から勤務を行う形態での業務（以下、テレワーク）が実施されるようになった。

テレワークを行うために必要な IT 製品・サービスの利用拡大に伴い、脆弱性の発見や、テレワーク端末が原因となったウイルス感染や情報漏えい等の被害の発生が確認されている。

本節ではテレワーク普及の経緯やテレワークのセキュリティ脅威と対策について、IPA が実施した調査結果を踏まえて述べる。

3.3.1 テレワークの広がりと推進活動

テレワークの利用状況の変化と利用拡大、セキュリティ対策の強化のための推進活動について述べる。

(1) テレワーク利用状況の変化

テレワークとは、情報通信技術（ICT：Information and Communication Technology）を活用した、場所や時間にとらわれない柔軟な働き方のことである。テレワークの形態には、表 3-3-1 に示すように、在宅勤務、モバイルワーク、サテライト／コワーキング、ワーケーションがある。

在宅勤務	自宅を就業場所とする働き方。通勤時間の削減、移動による身体的負担の軽減が図れ、時間の有効活用ができる。
モバイルワーク	電車や新幹線、飛行機の中等で行うもの、移動の合間に喫茶店などで行うものも含み、業務の効率化に繋がる。
サテライト／コワーキング	企業のサテライトオフィスや一般的なコワーキングスペースで行うもの。企業が就業場所を規定する場合も、個人で選択する場合も含む。
ワーケーション	リゾートなどバケーションも楽しめる地域でテレワークを行うもの。ビジネスの前後に出張先などで休暇を楽しむブレジャーも含む。

■表 3-3-1　テレワークとは
（出典）一般社団法人日本テレワーク協会「テレワークとは※185」を基に IPA が編集

(a) 2019 年までの経緯

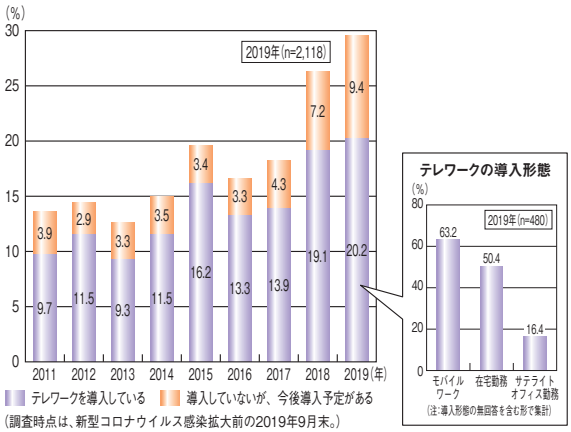
「テレワーク」が生まれたのは、1970 年代の米国である※186。当時の米国では、大気汚染やオイルショック等への危機感から、一部の企業を中心に自宅で仕事をするスタイルが導入された。2001 年 9 月 11 日の米国同時多発テロ事件をきっかけに危機管理の方策としてテレワークが認識され、2010 年にはテレワーク強化法が施行された。この法律は連邦政府職員がテレワークを推進するための様々な義務を定めている。

日本では、1984 年に日本電気株式会社によりサテライトオフィスが作られ、これが日本で初めて「テレワーク」が導入された事例とされている※187。

その後、テレワークは、育児・介護、障がい等により、恒常的または一時的に通勤が困難な人でも在宅で勤務することにより、雇用を継続するために有効であるとして導入の検討が進められた。また、モバイルワークは、営業や SE 等接客機会の多い人が、外出先や移動中でも社内システムへのアクセスや、書類の作成を可能にすることで業務効率化が図れるとして注目された。更に 2011 年 3 月 11 日の東日本大震災以降、自然災害等により通勤が困難になる事態においても事業継続の手段としてテレワークが効果的であると考えられるようになった。他にも図 3-3-1 に示すように社会的な効果が期待されている。

■図 3-3-1　テレワークの効果
（出典）一般社団法人日本テレワーク協会「テレワークを導入する効果※188」を基に IPA が編集

更に、安価で安定した通信インフラの普及と働き方改革への関心の高まりや、東京 2020 オリンピック・パラリンピック競技大会期間中の交通渋滞緩和策として、政府がテレワークによる外出者の削減を奨励したこともあり、テレワークを導入する企業・組織は増加した。図 3-3-2（次ページ）にテレワーク導入状況の推移を示す。



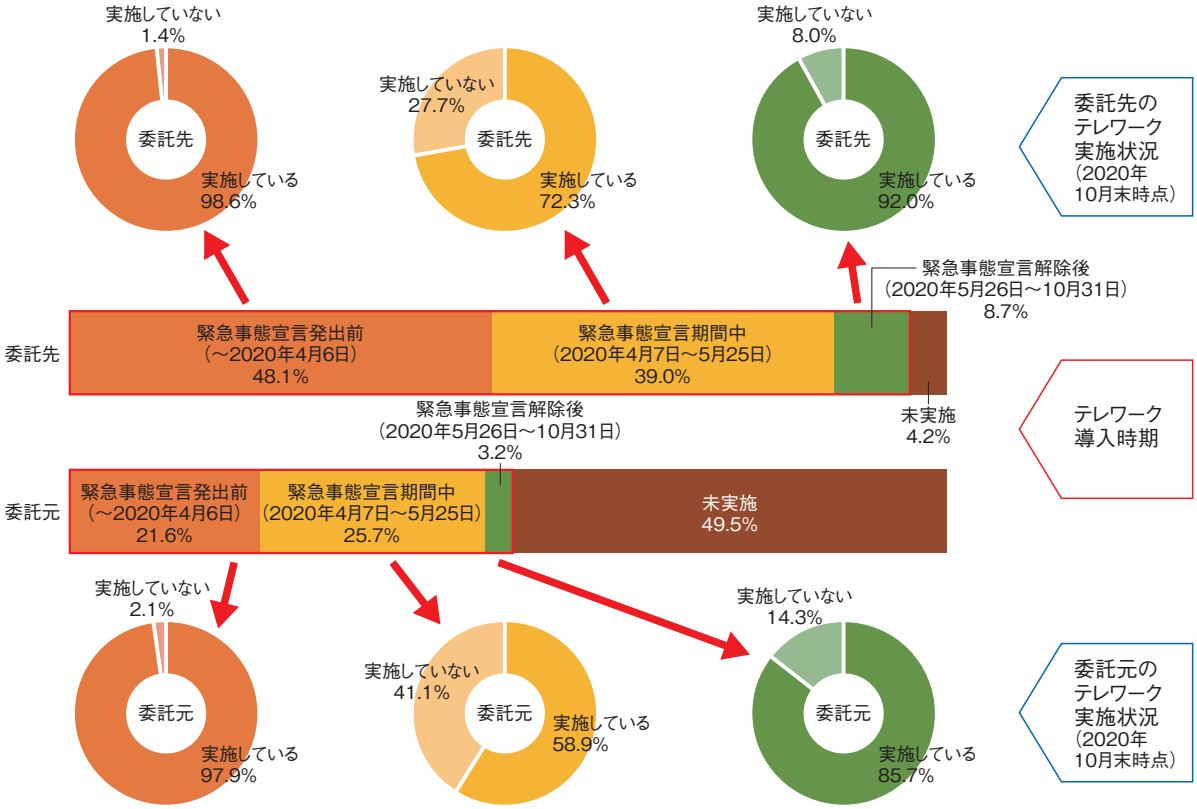
■図 3-3-2　テレワークの導入状況
(出典)総務省「令和元年通信利用動向調査※189」を基に IPA が編集

(b) 2020 年以降の経緯

2019 年 12 月に中国武漢市から広まったとされる新型コロナウイルスの感染拡大が深刻化し、2020 年 4 月 7 日、日本政府は 1 回目の「新型コロナウイルス感染症緊急事態宣言※190」(以下、緊急事態宣言)を発出し、不要不急の外出を控えることを強く求めた。このため多くの企業・組織は、テレワークを導入し、在宅勤務により、出社しなければならない人を最小限にした。以前よりテレワークを推進していた一部の企業では、在宅勤務の期間や回数が増える程度のことで済んだが、それ以外の企業・組織は可用性確保のためネットワークや端末の増強に追われた。

5 月 25 日に「新型コロナウイルス感染症緊急事態解除宣言※191」(以下、緊急事態宣言解除)が発出されたが、職場への出勤等については慎重な意見が多く、政府もテレワーク、時差出勤、自転車通勤等、人との接触を低減する取り組みを呼びかけた※192。その後も 2021 年 1 月 7 日に 2 回目の緊急事態宣言が発出される等、感染者の増減が繰り返され、多くの企業・組織が 1 年以上にわたり、テレワークを継続している。このような、オフィス以外の場所で業務を行う働き方は不可逆的な変化として定着しつつあり、「新常態(ニューノーマル)」と呼ばれている。

IPA は 2021 年 4 月、「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査※193」の結果を公開した(図 3-3-3)。ユーザ企業から業務委託を受ける IT 企業やベンダ(以下、委託先)と業務委託するユーザ企業(以下、委託元)を対象に、テレワークの導入時期と継続状況を 2020 年 11 月に調査したものである。この調査では、10 月 31 日時点で委託先の 95.8%、委託元の 50.5% の組織がテレワークを実施した



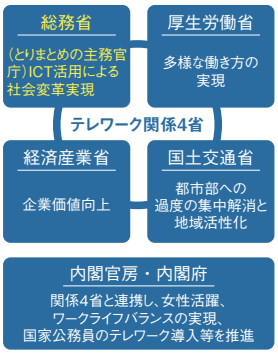
■図 3-3-3　テレワーク導入時期と継続状況(n=505)
(出典)IPA「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」を基に編集

ことがあると回答した。1回目の緊急事態宣言発出前からテレワークを実施していた委託先は48.1%、委託元は21.6%となっており、IT企業の多い委託先では、テレワークの導入が進んでいた。一方、1回目の緊急事態宣言期間中にテレワークを導入した委託先は39.0%、委託元は25.7%となっており、短期間に多くの企業・組織で導入されたことが分かる。一時はパソコン、ネットワークのリソース不足※194等が発生し、企業・組織は応答遅延等、厳しい環境での業務を迫られた。

更に、前述の緊急事態宣言期間中にテレワークを導入したと回答した組織のうち、委託先の27.7%、委託元の41.1%が、2020年10月31日時点でテレワークを実施していないと回答しており、テレワークが一時的な対応にとどまっていたことがうかがえる。しかし、緊急事態宣言発出前、あるいは緊急事態宣言解除後から実施・導入していた組織の9割はテレワークを継続しており、今後も組織の勤務形態としてテレワークが定着することが予想される（そのほかの調査結果については「3.3.3 テレワークのセキュリティ実態調査」参照）。

(2) テレワークとセキュリティ対策の推進

テレワークは、ワークライフバランスの実現、人口減少時代における労働力の確保、地域の活性化、非常時における業務継続等に有効と考えられ、関係府省が連携して普及・推進を図ってきた。2016年7月からは内閣官房長官指示により関係府省連絡会議が開催され、テレワーク推進に向けた取り組みの共有や連携施策の検討・推進がなされている（図3-3-4）。



構成員（政務）	
総務省	総務副大臣（議長）
厚生労働省	厚生労働副大臣
経済産業省	経済産業副大臣
国土交通省	国土交通副大臣

構成員（事務）	
内閣官房	内閣審議官（IT総合戦略室 室長代理）
内閣府	官房審議官（男女共同参画局担当）
総務省	官房総括審議官（情報通信担当）
厚生労働省	雇用環境・均等局長
経済産業省	官房審議官（商務情報政策局担当）
国土交通省	官房審議官（都市担当）

■図3-3-4　テレワーク関係府省連絡会議
（出典）厚生労働省「テレワーク総合ポータルサイト　政府のテレワークへの取り組み※195」

この中で、テレワークの導入支援を目的とした情報提供手段として、総務省が「テレワーク総合情報サイト※196」を、厚生労働省が「テレワーク総合ポータルサイト※197」を開設し、テレワークの導入事例や導入にあたって活用可能な支援策等が示された。また、総務省は2018年

テレワーク関連ガイドライン・情報サイト名	発行元・運用者	概要
みんなでしっかりサイバーセキュリティ※201	NISC	テレワーク実施者を対象とし、情報セキュリティを確保するための対策や注意点を簡易に説明している。
テレワークセキュリティガイドライン第5版※202	総務省	テレワークにおける情報セキュリティ対策の考え方、ポイント、テレワークトラブル事例と対策一覧等をまとめている。2021年5月に全面的に改定された。
中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）※202	総務省	テレワークセキュリティガイドラインを補完する。セキュリティの専任担当がいない中小企業等がテレワークを実施する際に最低限のセキュリティを確保するためのチェックリスト。
テレワーク時における秘密情報管理のポイント（Q&A解説）※203	経済産業省	テレワークに対応した規程の整備等について、Q&A形式でまとめている。
テレワークモデル就業規則～作成の手引き～※204	厚生労働省	テレワーク導入の際に検討が必要な就業規則についての考え方や、参考とすべき規定例、組織におけるセキュリティガイドライン策定の必要性等をまとめている。
テレワークの適切な導入及び実施の推進のためのガイドライン※205	厚生労働省	テレワークの導入・実施にあたり、労務管理を中心に、労使双方の留意点、望ましい取り組み等を明らかにしている。
テレワークを行う際のセキュリティ上の注意事項※206	IPA	テレワーク環境提供の有無、使用場所の違い、テレワーク環境から職場に戻る際の注意点等、テレワーク実施時のセキュリティ上の注意を促している。
Web会議サービスを使用する際のセキュリティ上の注意事項※207	IPA	組織のWeb会議主催者、情報システム部門を対象に、Web会議サービス選定時に考慮すべきセキュリティ上のポイントを挙げている。
テレワークのガイド・事例等※208	一般社団法人日本テレワーク協会	テレワーク導入の際に参考となる各種ガイドラインや事例集等を掲載している。

■表3-3-2　テレワーク関連ガイドライン・情報サイト概要
（出典）各組織の公開情報を基にIPAが作成

4月に、企業等が情報セキュリティ上の不安を払拭してテレワークを導入・活用するための指針「テレワークセキュリティガイドライン 第4版[※198]」を、厚生労働省は2018年2月に、テレワークにおける労務管理の留意点を記載した「情報通信技術を利用した事業場外勤務の適切な導入及び実施のためのガイドライン[※199]」や、自営型テレワークの実施に向けた「自営型テレワークの適切な実施のためのガイドライン[※200]」を公表した。2020年には情報サイトが更に増え、テレワークセキュリティガイドライン等既存のガイドラインも改版・拡充された。表3-3-2（前ページ）に主なガイドライン、情報サイトとその概要を示す。

2020年は更に、「新型コロナウイルス感染症緊急経済対策」（2020年4月7日閣議決定）や2020年度第一次・二次補正予算において、税制措置としてテレワーク等のための設備投資が中小企業経営強化税制の対象とされたほか、経済産業省、総務省、厚生労働省からテレワーク促進のため助成金等、各種予算措置が取られることとなり、テレワーク導入企業の裾野を広げる機運が高まっている。

3.3.2 テレワークに関連した問題

2020年に報告された脅威や実際に発生した被害の中には、テレワーク環境に関わる脆弱性や攻撃が存在した。以下はその解説である。

(1) 2020年に発生したインシデント事例

2020年に報告されたテレワーク環境に起因するインシデント事例を紹介する。

(a) Web会議サービス利用時の問題

テレワークの普及に伴い、Web会議サービスを利用する組織が増加した。しかし、これらのサービスのクライアントアプリケーション（以下、アプリ）に脆弱性が発見されたり、利用者の不注意により被害が生じたりしている。

2020年3月、Web会議サービス「Zoom」のWindows向けアプリに脆弱性が発見された。この脆弱性を悪用された場合、認証情報を窃取されたり任意の実行可能ファイルを起動されたりする可能性があった。この脆弱性は製品開発者により速やかに修正され、発見の翌日に修正バージョンが公表された[※209]。Zoomに関してはその後、セキュリティについて大幅な修正が行われ、通信内容のエンドツーエンドでの暗号化機能等が実装された。

上記のようなWeb会議サービスの脆弱性は、Zoomのみではなく、TeamsやWebex等のアプリにおいても報告されており、随時修正が行われている。

また、Zoomについては Zoom 爆弾という荒らし行為による被害が確認されている。Zoomでは会議を設定すると会議参加用のURLが発行される。このURLには会議のIDが含まれており、攻撃者が総当たり攻撃を行うことでIDが推測される。このとき、会議への参加にパスワードが設定されていないと、意図しない参加者が会議に参加できてしまう。実際に攻撃者によって、IDを推測され、会議に侵入された際に不適切な画像を画面共有される等の被害が発生した。Zoom爆弾の被害が報告された後、会議にパスワードを設定する等の対策が呼びかけられている[※210]。

これまでに紹介した被害の発生に伴い、IPAではWeb会議サービスを安全に利用するための注意事項として、「Web会議サービスを使用する際のセキュリティ上の注意事項[※207]」を公開し、Web会議サービス選定時に考慮すべきポイントや会議準備、会議実施のタイミングでの注意すべきポイントについて、解説を行っている。

(b) VPN製品の脆弱性

2020年には、Fortinet, Inc.製FortiOSのSSL VPN機能の脆弱性「CVE-2018-13379」について、修正バージョンへのアップデートが未実施である機器のIPアドレス情報が、インターネット上で公開された。この脆弱性は2019年に公表され、同年11月に修正バージョンのファームウェアが公表されていた。しかし、何らかの理由により、アップデートが行われなかった機器のIPアドレス情報が2020年になって公開されたものである。この中には日本企業や警視庁、大学等のホストも存在したとの報道もあり、脆弱性を悪用されたことによる被害が国内でも報告されている[※211]（FortiOSの脆弱性を悪用した攻撃については「1.2.5(1)(a)攻撃事例」参照）。

Fortinet, Inc.の製品に加え、2019年にはPalo Alto Networks, Inc.やPulse Secure, LLC.のSSL VPN製品でも脆弱性が公表され、JPCERT/CCから注意喚起が行われている[※212]。また、2021年4月にもPulse Secure, LLC.のSSL VPN製品について、任意のコマンド実行につながる脆弱性「CVE-2021-22893[※213]」が発表されている。このようにVPN製品等のテレワークで用いる通信機器にも脆弱性が発見・報告されており、各組織のネットワーク管理者は常に情報を収集することが求められている。

(c) テレワーク端末や個人を標的とした攻撃

2020 年 8 月、三菱重工グループにおいて、不正アクセスがあったことが報告された。この事案では、グループ内のネットワークにおいてウイルス感染が発生し、ウイルスに感染した端末が悪用されて不正アクセスが生じたとされている。三菱重工グループの報告によれば、テレワーク中の従業員が自宅に持ち帰っていた社用パソコンを使用し SNS を参照した際、ウイルスをダウンロードしてしまい感染、その後オフィスに出社した際にウイルスに感染したパソコンをグループ内のネットワークに接続したことで、ウイルスが持ち込まれたとしている※214(「1.2.1 (3) (d) SNS を悪用した攻撃」参照)。

オフィス等組織内で業務を行う形態では、組織が管理するファイアウォールやセキュリティ製品により各従業員が利用する端末やネットワークは保護されている。しかし、テレワーク環境では、各従業員の端末は、自宅のルータや各端末に導入したセキュリティソフトによる対策で守る必要があり、組織内と同様のセキュリティ強度を維持することが困難となっている。また、業務端末の管理が各従業員に一任される状態となっており、OS やソフトウェア製品のアップデートが実施されているのかを管理することが、オフィス勤務よりも難しくなっている。

加えて、自然災害が発生したとき等と同様に、新型コロナウイルスへの不安に便乗したフィッシング等も発生している※215(個人を対象とした同様なフィッシングについては「1.2.7 個人をターゲットにした騙しの手口」参照)。これについても、オフィス勤務であれば気が付いた従業員が周囲に簡単に注意喚起を行うことができたが、テレワーク環境では注意喚起が容易ではなくなっており、フィッシング等の被害が発生する危険性が高まっていると考えられる。

(2) テレワーク環境を取り巻く脅威

オフィスでは物理的な隔離等の対策が組織で可能であったが、テレワーク環境では個人でパソコンの管理やソフトウェアの更新、ネットワークの安全性等に責任を持たなければならず、オフィス程堅牢な対策はとれないため、攻撃者に狙われる可能性は高い。テレワーク環境を取り巻く脅威を、テレワーク環境で働く従業員（個人）を狙ったものと、テレワークを実施する組織を狙ったものに大別して解説する（対策については「3.3.4 テレワークのセキュリティ対策」参照)。

(a) 個人が注意すべき脅威

テレワークの実施に際し、個人を標的として予想される脅威の代表例を以下に示す。

① 不正アクセス
② ウイルス感染
③ フリー Wi-Fi からの盗聴
④ ソーシャルハッキング
⑤ 端末や業務資料の紛失

不正アクセスやウイルス感染が発生する原因としては、業務用パソコンで使用しているソフトウェアや自宅のルータのファームウェア、セキュリティソフト等の更新が行われず、脆弱性を狙った攻撃や最新のウイルスへの対応が行われないことが想定される。

また、自宅やオフィス以外で仕事をする際、Wi-Fi のフリースポットを使用して通信内容を盗聴される被害や、社外秘の資料を開いた画面を覗かれ、情報が盗まれるソーシャルハッキングによる被害の発生が予想される。特に、ソーシャルハッキングについては自宅においても、家族が社外秘の資料を見て、悪意を持たず第三者に話してしまうといった事態も想定される。

組織がテレワークを主とした業務形態に移行しても、必要に応じて出勤する場合や、オフィスから業務用パソコンや業務上必要な書類を自宅へ持ち帰る場合等が考えられる。このような場合、通勤経路や自宅で端末や業務資料の紛失が生じる可能性がある。公共交通機関におけるカバン等の置き引きや置き忘れは、以前から注意喚起されており、従業員も警戒していると考えられる。しかし自宅内において、重要書類を誤って廃棄し、廃棄した書類が第三者に拾われる、あるいは空き巣被害によって重要書類や業務用パソコンが盗まれるといった被害も想定される。

(b) 組織が注意すべき脅威

組織が直面する脅威として、以下が予想される。

① 規則違反
② ソフトウェア等の資産管理不備
③ サーバ等の ID 漏えいによる不正アクセス
④ 問い合わせ・報告先の不備

まず、テレワークを実施するに際し、組織が定めたテレワーク規則について従業員が重要性を理解していないため、規則に違反してしまいウイルス感染や盗聴、端末の紛失といった被害が発生することが想定される。

また、各従業員が使用する業務端末や端末上のソフトウェアがオフィス外にあるため資産管理ができず、アップデート状況やライセンスの継続状況が把握できなくなることが想定される。

加えて従業員が各自宅等から、組織のサーバ等の資産にアクセスするため、ID やパスワードのメモを持ち帰った後に紛失したり、フィッシング等により窃取されたりすることで、ID やパスワードの漏えい被害の発生が想定される。

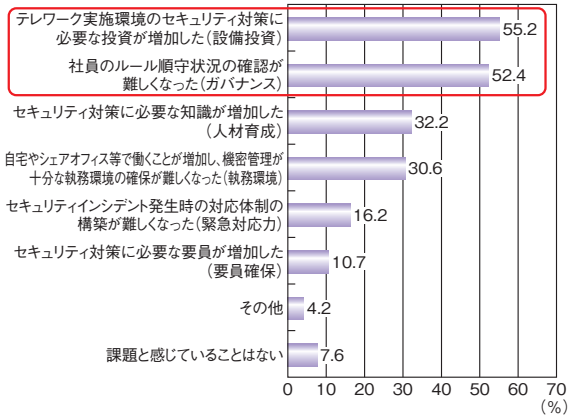
上記のような被害やトラブルが発生した際に、組織内の連絡先となる窓口が整備されていなかったり、従業員に展開されていなかったりする場合、対応の遅れが生じ被害の拡大につながると想定される。

3.3.3 テレワークのセキュリティ実態調査

コロナ禍での事業継続のため利用が拡大したテレワークやオンラインによるコミュニケーションといった変化に対して、組織のセキュリティ対策は十分なのか、リスクは顕在化していないのか、等の実態を把握するため IPA では 2020 年度に「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」を実施した。以降にその結果を述べる。なお、調査時期は、2020 年 11 月、調査対象は企業データベース等から抽出した企業・組織の情報システム・IT 企画関連業務の担当者である。

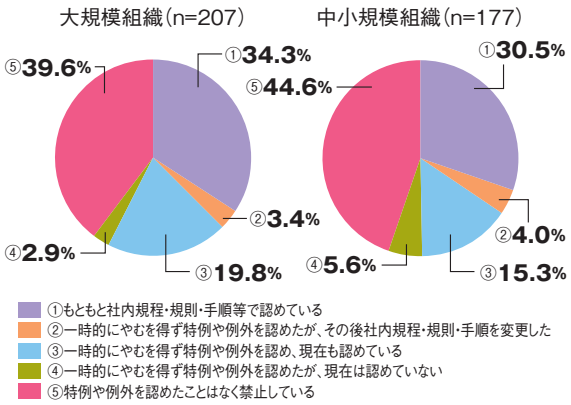
(1) テレワーク実施時のセキュリティ上の課題

テレワークを実施する上でのセキュリティ上の課題について調査した結果を図 3-3-5 に示す。「テレワーク実施環境のセキュリティ対策に必要な投資が増加した」という回答が最も多く（55.2%）、「社員のルール順守状況の確認が難しくなった（ガバナンス）」が 52.4% で続いた。



■図 3-3-5　テレワーク実施時のセキュリティ上の課題（複数回答）
（出典）IPA「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」を基に編集

緊急事態宣言中またはコロナ禍の影響により、例外として個人が所有する端末（パソコン・スマートフォン等）の業務利用を認めたかを調査した結果を図 3-3-6 に示す。「一時的にやむを得ず特例や例外を認め、現在も認めている」という回答が大規模組織で 19.8%、中小規模組織で 15.3% であった。



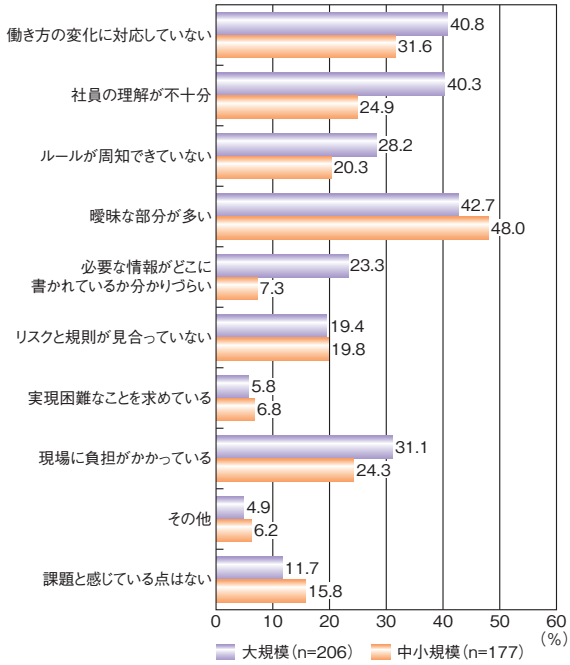
■図 3-3-6　緊急事態宣言中またはコロナ禍の影響により特例や例外を認めたセキュリティ対策の社内規定・規則（個人が所有する端末（パソコン・スマートフォン等）の業務利用）
（出典）IPA「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」を基に編集

緊急事態により一時的に例外や特例を認めることは、業務継続を優先するという観点からやむを得ないと判断されたと思われる。しかし、例外や特例で規則が緩和されることにより脆弱性が増し、セキュリティリスクは大きくなる。緩和された状態が常態化することによって、セキュリティインシデントの発生が懸念される。組織は、緩和によるリスクと事業継続の状況等を総合的に判断し、リスク低減のための対策（規定・規則の見直し、対象範囲の縮小、ツールの導入等）の検討、あるいは、例外や特例の撤廃により、リスクを受容可能なレベルまで小さくすることが望ましい。なお、IPA ではテレワークを行う際のセキュリティ上の注意事項を公開している※206。テレワークを行う際の規定の見直しと制定の参考としていただきたい。

(2) 社内規定・規則・手順の課題

テレワークに関する社内規定・規則・手順についての課題について調査した結果を図 3-3-7（次ページ）に示す。企業規模に関わらず「曖昧な部分が多い」という回答が最も多く、「働き方の変化に対応していない」「社員の理解が不十分」が続いた。

「働き方の変化に対応していない」という課題は新型コ



■図 3-3-7　社内規定・規則・手順の課題
(出典)IPA「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」を基に編集

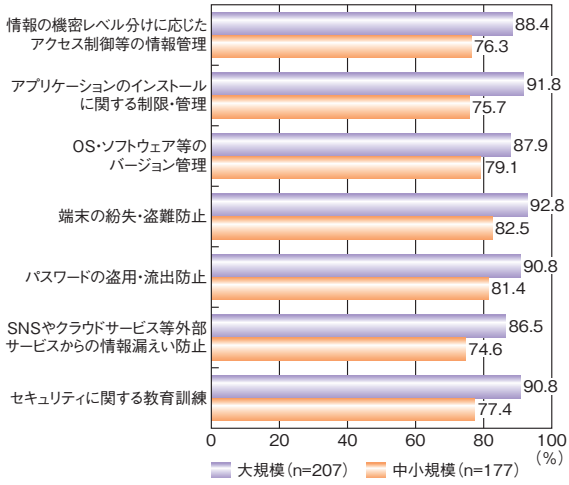
ロナウイルス対策としてテレワークの導入や利用が急増したことに対して、社内規定・規則・手順の作成や見直しが追い付いていないことが理由であると考えられる。

中小規模企業と大規模企業の違いとして、「社員の理解が不十分」という回答において中小規模企業では 24.9%、大企業では 40.3% と 15.4 ポイントの差が見られ、「必要な情報がどこに書かれているのかわかりにくい」という回答において中小規模企業では 7.3%、大規模企業では 23.3% と 16 ポイントの差が見られた。この結果から、大規模企業の場合、多くの規定・規則・手順が定められてはいるが管理・周知や理解が十分できていないことが推測できる。どのような場合にどの規定に従えばよいのか、またその規定はどこに記載されているのかを従業員が理解していないことがインシデントの発生等につながる恐れがある。

(3) テレワーク実施に関するセキュリティ対策規則の制定状況

テレワークに関するセキュリティ対策規定の制定状況について調査した結果を図 3-3-8 に示す。中小規模企業の 75% 以上、大規模企業の 85% 以上がテレワークに関するセキュリティ対策規則を制定しているという結果となった。

企業規模による規定制定状況のばらつきは見られず、全体的に高い割合で制定されていることがうかがえる

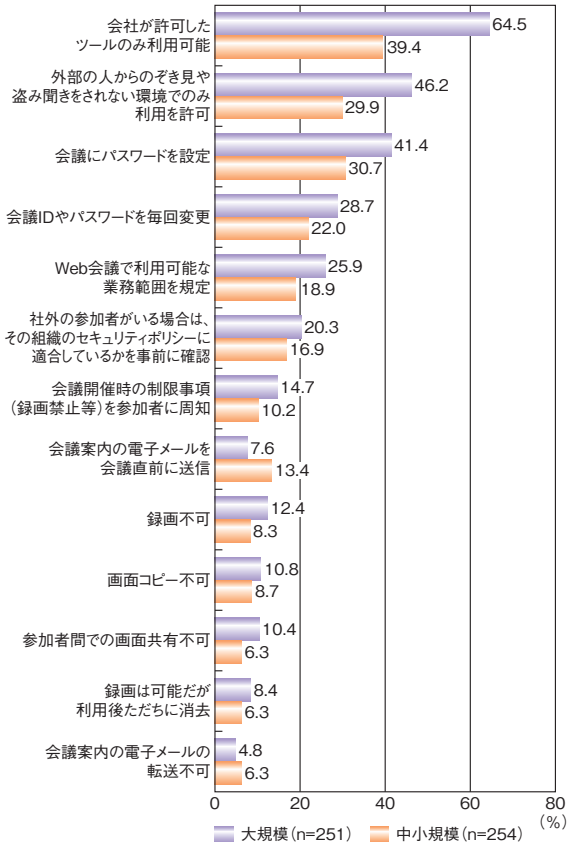


■図 3-3-8　テレワーク実施に関するセキュリティ対策規則の制定状況
(出典)IPA「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」を基に編集

が、規定がない状況でテレワークを実施している企業も一定数存在することが確認された。

(4) Web 会議サービス利用時の規則制定状況

Web 会議サービス利用時の規則制定状況について調査した結果を図 3-3-9 に示す。企業規模に関わらず、「会社が許可したツールのみ利用可能」という回答が最も

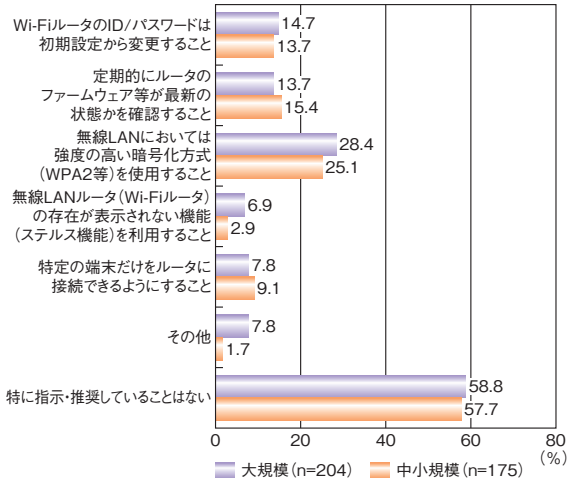


■図 3-3-9　Web 会議サービス利用時の規則制定状況
(出典)IPA「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」を基に編集

多く、「外部の人からのぞき見や盗み聞きをされない環境でのみ利用を許可」「会議にパスワードを設定」が続いた。

規則を制定している割合について企業規模による偏りは見られないが、最も回答が多かった「会社が許可したツールのみ利用可能」では、大規模企業の 64.5% に対し、中小規模企業は 39.4% であり、25.1 ポイントの差が見られた。大規模企業では離れた拠点間の会議等でコロナ禍以前から Web 会議サービスを利用していた企業が多く、規則が決まっていたのに対して、中小規模企業ではコロナ禍以降に Web 会議サービスを導入したため、規則が間に合っていない企業が多かったことが影響していると考えられる。また、「会社が許可したツールのみ利用可能」以外の規則の制定状況はいずれも 50% 以下であり、図 3-3-8（前ページ）のテレワーク実施に関する規則と比較すると、「Web 会議サービス利用時の規則」はテレワークの規則に比べ制定の割合が低いことが分かった。

規則がない状態で Web 会議サービスを利用すると、使い方を誤り、気付かないうちに情報を漏えいさせてしまう恐れがある。また、規定を決めても Web 会議の相手に同様の規定がなければ Web 会議サービスの設定や情報の取り扱いが異なることによって、セキュリティリスクが高まる恐れがあるため、Web 会議で機密情報を扱う場合は、情報の管理方法や参加者の限定・表記等のルール等を双方で確認することが重要である。IPA では Web 会議サービスを利用する際のセキュリティ上の注意事項を公開している※207。Web 会議サービスの規定の見直しと制定の参考としていただきたい。



■図 3-3-10　テレワークで自宅のホームネットワークを利用する際の指示、推奨事項（複数回答）
（出典）IPA「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」を基に編集

(5) テレワークで自宅のホームネットワークを利用する際の指示、推奨事項

テレワークで自宅のホームネットワークを利用する際の指示、推奨事項について調査した結果を図 3-3-10 に示す。約 6 割が「特に指示・推奨していることはない」と回答しているが、残りの企業・組織では何らかの指示・推奨をしていると回答した。

テレワークにおいて自宅のホームネットワークを利用するケースも増加していることが考えられるが、ホームネットワークに関する指示や推奨事項を決めている企業は少ないことが分かった。ホームネットワークは新たなリスクになることが想定されるため、安全な使い方の指示や推奨事項についての検討が急務である。

3.3.4 テレワークのセキュリティ対策

テレワーク実施時のインシデントの被害やトラブルの発生原因が個人と組織で異なるため、対策についてもそれぞれの立場で検討する必要がある。

(1) 個人が実施すべき対策

テレワークの実施に際し、個人を標的とする脅威の代表例を再掲し、それぞれについて実施すべき対策を述べる。

① 不正アクセス
② ウイルス感染
③ フリー Wi-Fi からの盗聴
④ ソーシャルハッキング
⑤ 端末や業務資料の紛失

①と②に対しては、脆弱性対策、ウイルス対策が必要である。使用するパソコンの OS やソフトウェア、自宅のルータのファームウェア、セキュリティソフトのパターンファイルを最新の状態に保つことが第一の対策となる。また、脆弱性を悪用した不正アクセスやウイルス感染等の早期検知の方法として、近年はホームルータにも UTM や類似の機能が組み込まれているものがあるため、必要に応じてセキュリティ設定を有効にすることも検討すべきである。

③と④に対しては、各組織のテレワークに関するルールを順守しつつ、業務を実施する環境を見直す必要がある。

例えば、自宅以外の場所で業務を行う際にインターネットを利用する場合は、フリー Wi-Fi を利用せず、会社貸与のモバイルルータを利用することや、フリー Wi-Fi を利

用する場合は、各組織のネットワークに VPN 接続して組織のファイアウォールを経由して通信する、等の対策を検討すべきである。

また、ソーシャルハッキングへの対策としては、第三者の出入りが多いカフェやレストラン等での業務を避けるほか、自宅内においても個室で業務を行い、席を離れる際はパソコンを必ずロックし、業務書類や手帳等も引き出し等にしまい、放置しないといった対策を徹底することが重要である。

⑤に対しては、ワイヤーロック等の盗難対策や片付けの徹底が第一の対策となる。特に第三者が出入りするカフェやホテル等では、パソコンや資料から目を離さないようにし、もし目の届かない状態になる場合は、鍵付きのカバン等に確実に収納し、ワイヤーロック等を使い盗難を防止する等の対策が必要である。

また、自宅においても書類がチラシ等に紛れてしまい、誤って廃棄される等の事態を防ぐために、専用のファイルに収納する等の対策を検討すべきである。その他、空き巣等による業務用パソコンの盗難を防止するため、自宅内でもワイヤーロックを使用し、パソコンを使用しない場合は鍵のかかる引き出し等に保管するといった対策が必要である。

(2) 組織が実施すべき対策

組織が直面すると予想される脅威を再掲し、それぞれについて実施すべき対策を述べる。

① 規則違反
② ソフトウェア等の資産管理不備
③ サーバ等の ID 漏えいによる不正アクセス
④ 問い合わせ・報告先の不備

①に対しては、各組織において、業務内容に応じた規則を設定、あるいは見直しを行い、従業員に徹底する必要がある。規則の徹底においては、業務内容から想定される被害の大きさを認識させ、被害防止のために実施すべきことを従業員に理解してもらう必要がある。

②に対しては、各従業員の作業端末や組織のサーバ等で使用するソフトウェアが常に最新の状態に保たれるようにテレワーク環境でどのようにメンテナンスを行うか、作業手順を整備する必要がある。必要に応じて、資産管理ソフトウェア等を新規に導入する等、管理体制の見直しが必要である。

③に対しては、サーバ等へのログイン情報の管理を行う。各従業員が自宅等から日常的に組織のサーバを利用するため、不正アクセスには特に注意が必要となる。ワンタイムパスワードを使用した認証や、多要素認証等を用いて ID やパスワードが漏えいした際への対策を進めることを検討すべきである。

また、各従業員の通信内容の盗聴を避けるため、組織のネットワークと VPN による接続を行うことも検討すべきである。

④に対しては、情報提供窓口やインシデント発生時の通報窓口の再確認、整備が必要である。一般向けの窓口は、通常の問い合わせとインシデント報告先の窓口が識別しやすい名称でないと、適切な窓口に連絡されず、スムーズな対応ができないことが想定される。

テレワーク業務では、オフィス等に従業員が集まっていないため、インシデント発生時の連絡先が通常と異なる。インシデント発生時の連絡先や対応担当者が適切に整備されず、通報者が連絡先を確認できない場合、報告・初動対応が遅れてしまい、被害の拡大につながるリスクがある。

従業員が適切な連絡先をスムーズに確認できない場合、業務を優先してしまうことで、重大事象の通報を後回しにしたり、通報自体を放棄したり、失念したりすることで被害の発生を見過ごす事態も想定される。

特にテレワーク業務では、インシデントや不審な事象の発生時に各従業員が発生事象について周囲に相談や報告を行うことが難しいため、誤って報告すべき事象を過小評価し、報告しないことも想定される。結果として、組織内のインシデントの発生が見過ごされてしまう危険がある。

また、テレワーク環境ではトラブルが発生した場合の連絡手段が限られ、担当部署の従業員が直接端末等を確認することもできないため、事象の調査にはオフィス勤務の場合以上に時間を要すると考えられる。このため、問い合わせ・報告先とともに、事象発生時にどのような情報を取得し、どのような形式で担当部署へ展開すべきかを整備しておくことも、迅速な対応のために重要である。

3.3.5 今後のテレワークのセキュリティ

勤務場所の多様化、業務のデジタル化・オンライン化といった働き方の変化は、試行錯誤が続きつつもニューノーマルとして定着すると想定される。2020 年は業務継続のため、十分な準備ができないままテレワークや Web 会議を導入した企業・組織が多く、サービスの利用や、情報の取り扱いに関するルールの緩和等で急場しのぎせ

ざるを得なかった。しかし、このようなセキュリティ対策の特例や例外を認め、リスクの低減策が検討されない状態が常態化することによって、インシデントの発生、被害の拡大を招くことが懸念される。具体的には、組織が管理できない機器の増加、新サービスの脆弱性、自宅で利用する機器のメンテナンス不備等により、従来の組織統制のもとでの働き方に比べ、攻撃のリスクが増えている。またテレワークという新しい環境に便乗したフィッシング、ウイルス感染や自宅での管理不備による情報流出等、人的要因による被害リスクも増えている。

テレワークでは固定的なセキュリティ境界はなくなり、自宅やクラウドといった、組織のガバナンスでは統制しにくい状況でセキュリティのレベルを保つことが求められる。テレワークで利用する端末・ネットワーク・サービスの特定とそれに基づくリスクアセスメント、可用性重視で暫定的に作成したルールの再整備と周知徹底、インシデント対応の見直し、機器や人の認証の強化を含むゼロトラストの考え方の導入、最新の攻撃やフィッシング等の脅威に関する情報の共有等について、できることから検討していただきたい。

COLUMN

情報セキュリティをテレワークができない理由にしないで

新型コロナウイルス対応で、民間企業だけでなく多くの組織でこれまでの働き方を変える必要に迫られました。そんな中で自宅等オフィス以外の場所で働くいわゆるテレワークやリモートワークが急速に広まりました。しかし新型コロナウイルス禍前までは、正直言ってテレワークの普及は遅々として進まなかったというのが実情でした。

なぜテレワークが普及しないのかという理由について、各種調査や専門家による分析が行われましたが、労務管理や業績評価の難しさ、社内ルールや IT インフラの未整備、上司と部下・社員同士のコミュニケーションの難しさと並んで必ず上位に挙げられるのが情報セキュリティの問題です。もちろん、テレワークの実施にあたっては、オフィス外で機密性の高い情報を扱うことになるケースもあるわけですから、情報セキュリティ対策に十分配慮することが求められるのは確かです。しかし、情報セキュリティが心配だからテレワークを導入できないというのは単なる言いわけだと思われても仕方ありません。

新型コロナウイルス禍という困難な状況において求められているのは働き方の「変革」です。従来の働き方や情報の取り扱い方法を改善して業務を改革していくというだけではこの状況を変えることは難しいのではないでしょうか。いったん、「いままではこうだった」という考え方を置いて、業務のやり方、IT インフラの在り方、情報の取り扱い方法等、まずは大胆な発想で働き方を変えていくということが大切ではないでしょうか。想像してください。人口の減少や高齢化による労働人口の減少、今後予想されている大規模災害、新たなウイルスの出現等、今ここで変わっておかないと、後々大変なことになるかもしれません。

もちろん、詳細を検討していくと、経営者や中間管理職の皆さんにとっては、「そうは言っても」とか「現実的には」と言いたくなる場面があるかもしれません。そこを社員の皆さんの変わろうとする勇気と知恵で、一つでも二つでも乗り越えていこうというパワーこそが変革につながっていくのではないでしょうか。そして経営者や中間管理職の皆さんは、そういう社員の変革への意欲・提案を受け止めていただき、テレワークができない理由を考えるのではなく、どうしたらできるのかについて、公表されている他社事例や専門家のアドバイス等を参考にして、組織一丸となって検討をしていただきたいと思います。

特にテレワークにおける情報セキュリティは、業務に携わる人達の責任と自覚、そして技術によって、十分に解決可能な問題だと考えます。比較的安価なクラウドサービス、Web 会議システムやシンクライアントシステム等の提供がテレワークの推進を後押ししてくれるでしょう。こういった技術を安全に利用するための情報を IPA は提供していきます。情報セキュリティをテレワークができない理由にしないで、この困難な状況を乗り越えるべく、働き方の「変革」を実現しましょう。

3.4 NISTのセキュリティ関連活動

組織のサイバーセキュリティ対策を検討する場合、自らの対策がグローバルなセキュリティ基準と整合しているか、グローバルな基準のどのレベルに相当するか、等を考える際によく参照される規格として、国際標準化機構（ISO:International Organization for Standardization）のSC 27専門委員会※216が策定するISO/IEC 27000シリーズ、及び米国国立標準技術研究所（NIST：National Institute of Standards and Technology）※217の策定するNIST SP 800シリーズがある。

ISO/IEC 27000シリーズは、国内では日本産業規格（JIS：Japanese Industrial Standards）として日本語化され、活用されている。また本白書では、SC 27専門委員会等の最新標準化動向を紹介している（「2.5.2 情報セキュリティ、サイバーセキュリティ、プライバシー保護関係の規格の標準化（ISO/IEC JTC 1/SC 27）」参照）。これに対し、NISTの活動は国内で十分に紹介され、理解されているとはいえないが、その規格やガイドラインへの注目度は高い。

例えば、国内政府機関のセキュリティ規格の策定・改訂において、米国連邦政府機関が採用すべき管理策を定めたNIST SP 800-53やNIST SP 800-171は頻繁に参照される。またNISTが策定したCybersecurity Framework※218は、経営層とセキュリティ担当部門がコミュニケーションをとるための共通言語として、連邦政府機関・民間企業のみならず各国から注目されている。経済産業省とIPAも、国内施策であるサイバーセキュリティ経営ガイドライン※219やサイバー・フィジカル・セキュリティ対策フレームワーク※220の活動をNISTのCybersecurity Framework、あるいはSP 800-160※221等の関連規格に整合させ、国内の施策が容易にグローバル展開できるように努めている。

本項では、NISTのセキュリティに関する活動の概要と規格策定の最新動向について紹介する。

3.4.1 NISTの活動概要

NISTは米国の産業競争力に関わるあらゆる標準規格・ガイドライン策定、計測技術の開発を担っている組織であり、活動も多様な形態をとっている。

(1) 組織の沿革と体制

NISTの沿革と組織体制について述べる。

(a) 沿革とミッション

NISTは、産業競争力のベースとなる計測技術基盤を強化するために、議会が1901年に設立した国立規格基準局（NBS：National Bureau of Standards）を前身とし、現在は米国商務省（DoC：Department of Commerce）の傘下で「経済的安全保障を高め、生活を向上させるように科学的測定手法、標準、技術を進歩させ、米国の技術革新、及び産業競争力を促進すること」をミッションに掲げている。計測や標準化の対象はナノスケールの材料やコンピュータチップ、サイバー空間から巨大建造物・ネットワークまで多岐にわたり、「重要な測定ソリューション、公平な基準の作成・推進により世界をリードし、イノベーションを刺激し、産業競争力を促進し、生活の質を改善すること」をビジョンとしている。

(b) 組織

組織は以下の五つの研究所と二つのユーザ用施設で構成される。

- 通信技術研究所（CTL：Communications Technology Laboratory）
- エンジニアリング研究所（EL：Engineering Laboratory）
- 情報技術研究所（ITL：Information Technology Laboratory）
- 材料計測研究所（MML：Material Measurement Laboratory）
- 物理計測研究所（PML：Physical Measurement Laboratory）
- NISTニューロン研究センター（NCNR：NIST Center for Neutron Research）
- ナノスケール科学技術センター（Center for Nanoscale Science & Technology）

このうち情報技術研究所は、情報システム技術に関する標準、測定、相互運用性のテスト、セキュリティ、有用性、及び情報システムの信頼性に関する技術を開発し、普及させるミッションを持ち、下記の6部門で構成される。このうちセキュリティに関する活動を担当するのは、高度ネットワーク技術部（ルーティング等のネットワーク

セキュリティ）、応用サイバーセキュリティ部、コンピュータセキュリティ部、情報アクセス部の 4 部門である。

- 高度ネットワーク技術部（Advanced Network Technologies Division）
- 応用計算数学部（Applied and Computational Mathematics Division）
- 応用サイバーセキュリティ部（Applied Cybersecurity Division）
- コンピュータセキュリティ部（Computer Security Division）
- 情報アクセス部（Information Access Division）
- ソフトウェア・システム部（Software and Systems Division）

(2) 活動と成果公開

NIST の活動の特徴、及び成果公開の形式について述べる。

(a) 活動

NIST の活動の中心は、産業競争力強化の基盤となる度量衡の計測技術開発とその規格化であり、高度な計測サービス等により、民間における技術の発展を支援している※222。一方で情報技術研究所はこうした規格に基づき、連邦政府が遵守すべき調達規格やガイドラインを策定しているが、この規格には IT システムの運用が含まれ、結果として連邦政府機関のセキュリティ対策を主導している。規格策定における NIST の活動の特徴は、産学の専門家と連携する、あるいはドラフト段階から内容を公開したりワークショップを開催したりして積極的に外部のフィードバックを求める、等のオープン性にあると考えられる。

更に NIST は、策定した規格の機器・ツール等への実装を産学官連携の枠組みで支援し、成果の民間移管を促している。セキュリティ分野では情報技術研究所内の NCCoE（National Cybersecurity Center of Excellence）がこれを担当する※223。NCCoE では例えば、サプライチェーンリスク管理プラクティス SP 1800-34 ドラフト版に基づく「調達コンピュータ機器の検証」の方式実装に向けたプロジェクトを実施中である（2021 年 4 月現在）※224。SP 1800-34 がまだドラフト段階でありながら実装プロジェクトを立ち上げ、パブリックコメント募集もその中で実施する点は非常に機動的であると感じられる。

NIST はまた、連邦資金研究開発センター（FFRDCs: Federally Funded Research and Development Centers）の一つである非営利組織 MITRE Corporation※225（以下、MITRE 社）のスポンサーとなっている。サイバーセキュリティ分野では、MITRE 社は脆弱性を登録するための共通識別子である CVE（Common Vulnerabilities and Exposures）、サイバー攻撃のライフサイクルに基づく攻撃手法・対策知識ベース MITRE ATT&CK※226 等の活動で近年注目されているが、NIST はこのような民間で利用されるツールの実装を視野に入れつつ、規格を策定することが可能である。

NIST の活動のもう一方の特徴として、将来を見据えた研究と評価がある。NIST には個々の技術分野の専門家が集まっており、将来的な技術の方向性を明らかにする研究や技術評価が行われる。セキュリティ分野においては例えば、耐量子暗号アルゴリズムの提案評価プロジェクト（PQC：Post-Quantum Cryptography）を主導している※227。技術革新と将来的な規格化を視野に入れたものと考えられる。なお、PQC の最新動向は「2.8.2 (2) 公開鍵暗号に関する研究及び標準化の動向」を参照されたい。

以上のように NIST の活動は、企業の産業競争力強化と連邦政府機関の技術導入の双方を支援する、機器や部品の計測から IT システムの運用まで、及び研究開発から産学官連携による成果移管までを行う等、非常に多面的、重層的である。計測等の基盤技術を把握し、産学と連携した実装までをスコープとしていることが、NIST の規格・ガイドラインへの信頼を生み出しているものと考えられる。

(b) 成果公開

NIST の活動成果は主に出版物として公開される。ドラフト段階にある文書も公開され、自由に意見を提出できる。前述のミッションに基づき、NIST は産業競争力強化のための測定技術研究、及び技術規格の標準・ガイドライン策定の二つの活動を行うが、公開文書はそれに従い、以下のような分類となっている。

- 連邦情報処理標準（FIPS：Federal Information Processing Standards）
  連邦政府機関が利用する情報通信機器に法令で求められるセキュリティ技術標準。
- SP（Special Publication）
  FIPS の実践に役立つ勧告やベストプラクティスを記載した文書。このうち SP 800 シリーズは具体的なセキュリティ要件、管理策、ガイドライン等がまとめられている。

- NISTIR（NIST Interagency/Internal Report）
  FIPS や SP 策定に関する技術研究や仕様検討等の報告。中間成果も公開される。

各シリーズは別々に策定されるが、特定トピックの要件・管理策・プラクティス・技術報告のように、相互に関連し合う文書群として利用されることもある。

3.4.2 成果紹介

以下では、2020 年度に公開された成果を中心に、文書シリーズごとに紹介する。

(1) FIPS

NIST は、連邦情報セキュリティマネジメント法（FISMA：Federal Information Security Management Act of 2002）に基づき、連邦政府に求められるセキュリティ要件を策定する責務を負う。この要件に関する規格文書が連邦情報処理標準（FIPS：Federal Information Processing Standards）である。代表的な規格として、連邦政府が扱う情報や情報システムのセキュリティレベル、及びセキュリティ脅威の影響度に関する分類規格 FIPS 199、連邦政府の情報や情報システムに対する最低限のセキュリティ要件を定めた規格 FIPS 200 がある[※228]。2020 年 11 月には、連邦政府職員・契約事業者のアイデンティティ情報の検証に関する FIPS 201-3ドラフト版が公開され、2021 年 2 月 11 日まで意見募集が行われた[※229]。2020 年度に発行された FIPS の出版物は表 3-4-1 のとおりである。

(2) SP 800 シリーズ

SP 800 シリーズは情報セキュリティ全般にわたるガイド、推奨、技術仕様、NIST 活動報告に関する文書[※230]である。2020 年度に発行された主な SP 800 シリーズの出版物は表 3-4-1 のとおりである。

(3) SP 1800 シリーズ

実用的で使用可能なサイバーセキュリティソリューションに関する文書である。ベストプラクティスが記載される等、実践的であり、SP 800-53 や Cybersecurity Framework 等との対応も記載される。コンプライアンス対応状況も把握しやすい。2020 年度に発行された SP 1800 シリーズの出版物は表 3-4-1 のとおりである。

識別子	タイトル	ステータス	公開日	概要	関連規格・IR
連邦情報処理標準（FIPS）					
FIPS 201-3 (Draft)	Personal Identity Verification (PIV) of Federal Employees and Contractors	Draft	2020 年 11 月 2 日	連邦職員・契約者の身分証明	—
ガイド・管理策（SP 800 シリーズ）					
SP 800-213	IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements	Draft	2020 年 12 月 15 日	IoT 機器のセキュリティガイド	NISTIR 8259B NISTIR 8259C NISTIR 8259D
SP 800-210	General Access Control Guidance for Cloud Systems	Final	2020 年 7 月 31 日	クラウドのアクセス制御ガイド	—
SP 800-209	Security Guidelines for Storage Infrastructure	Final	2020 年 10 月 26 日	ストレージ基盤アーキテクチャのセキュリティガイド	—
SP 800-208	Recommendation for Stateful Hash-Based Signature Schemes	Final	2020 年 10 月 29 日	ハッシュベース署名スキームの推奨アルゴリズム	—
SP 800-207	Zero Trust Architecture	Final	2020 年 8 月 11 日	ゼロトラストアーキテクチャ（日本語版発行）	—
SP 800-181 Rev. 1	Workforce Framework for Cybersecurity (NICE Framework)	Final	2020 年 11 月 16 日	セキュリティ人材育成フレームワーク	NISTIR 8355

■表 3-4-1　2020 年に発行された出版物（FIPS、SP 800 シリーズ、SP 1800 シリーズ）(1/3)

識別子	タイトル	ステータス	公開日	概要	関連規格・IR
SP 800-172	Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171	Final	2021 年 2 月 2 日	SP 800-171 Rev. 2 の追補	SP 800-171 Rev. 2
SP 800-171 Rev. 2	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	Final	2021 年 1 月 28 日	政府調達事業者の CUI 保護規定（日本語版発行）	SP 800-172 SP 800-161 Rev. 1
SP 800-161 Rev. 1	Cyber Supply Chain Risk Management Practices for Systems and Organizations	Draft	2021 年 4 月 29 日	サイバーサプライチェーンリスク管理プラクティス	SP 800-171 Rev. 2 NISTIR 8276
SP 800-140	FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759	Final	2020 年 3 月 20 日	暗号モジュール検証プログラム（CMVP）の FIPS 140-3 発行に伴う改訂（「2.6.2 暗号モジュール試験及び認証制度」参照）	SP 800-140A SP 800-140B SP 800-140C SP 800-140D SP 800-140E SP 800-140F
SP 800-137A	Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment	Final	2020 年 5 月 21 日	情報セキュリティ継続モニタリング（ISCM）のアセスメント	SP 800-137 NISTIR 8212
SP 800-124 Rev. 2	Guidelines for Managing the Security of Mobile Devices in the Enterprise	Draft	2020 年 3 月 24 日	企業のモバイルセキュリティガイドライン	—
SP 800-77 Rev. 1	Guide to IPsec VPNs	Final	2020 年 6 月 30 日	IPsec 利用ガイド	—
SP 800-57 Part1 Rev. 5	Recommendation for Key Management: Part 1 – General	Final	2020 年 5 月 4 日	鍵管理ガイドの改訂	SP 800-57 Part2 Rev. 1 SP 800-57 Part3 Rev. 1
SP 800-56C Rev. 2	Recommendation for Key-Derivation Methods in Key-Establishment Schemes	Final	2020 年 8 月 18 日	秘密分散の鍵生成に関する推奨	SP 800-56A Rev. 3 SP 800-56B Rev. 2
SP 800-53 Rev. 5	Security and Privacy Controls for Information Systems and Organizations	Final	2020 年 9 月 23 日（2020 年 12 月 10 日更新）	組織のセキュリティ・プライバシー管理策（民間組織を含む）	SP 800-53A Rev. 4（Rev. 4 は日本語版発行） SP 800-53B
SP 800-53B	Control Baselines for Information Systems and Organizations	Final	2020 年 12 月 10 日	政府システムのベースライン管理策	SP 800-53 Rev. 5
プラクティス（SP 1800 シリーズ）					
SP 1800-34	Validating the Integrity of Computing Devices (Preliminary Draft)	Draft	2021 年 3 月 17 日	コンピュータデバイスの検証（サプライチェーンリスク管理）	—
SP 1800-33	5G Cybersecurity (Preliminary Draft)	Draft	2021 年 2 月 1 日	5G セキュリティ	—
SP 1800-31	Improving Enterprise Patching for General IT Systems: Utilizing Existing Tools and Performing Processes in Better Ways (Preliminary Draft)	Draft	2020 年 9 月 10 日	企業システムパッチ強化：ツール利用・プロセスの改善	—
SP 1800-30	Securing Telehealth Remote Patient Monitoring Ecosystem (2nd Draft)	Draft	2021 年 5 月 6 日	遠隔医療モニタリング	—

■表 3-4-1　2020 年に発行された出版物（FIPS、SP 800 シリーズ、SP 1800 シリーズ）(2/3)

識別子	タイトル	ステータス	公開日	概要	関連規格・IR
SP 1800-27	Securing Property Management Systems	Final	2021 年 3 月 30 日	資産管理	—
SP 1800-26	Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events	Final	2020 年 12 月 8 日	データ保護：ランサムウェア検知・対応	SP 1800-11 SP 1800-25
SP 1800-25	Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events	Final	2020 年 12 月 8 日	データ保護：ランサムウェアからの資産保護	SP 1800-11 SP 800-26
SP 1800-24	Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector	Final	2020 年 12 月 21 日	医療画像保護	—
SP 1800-23	Energy Sector Asset Management: For Electric Utilities, Oil & Gas Industry	Final	2020 年 5 月 20 日	エネルギー産業の資産保護	—
SP 1800-21	Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)	Final	2020 年 9 月 15 日	業務用モバイル機器のセキュリティ	—
SP 1800-19	Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments	Draft	2020 年 4 月 13 日	トラステッドクラウド	
SP 1800-16	Securing Web Transactions: TLS Server Certificate Management	Final	2020 年 6 月 16 日	TLS サーバ証明書管理	—
SP 1800-15	Securing Small Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)	Final	2021 年 5 月 26 日	中小企業・ホーム IoT 機器の保護	—
SP 1800-11	Data Integrity: Recovering from Ransomware and Other Destructive Events	Final	2020 年 9 月 22 日	データ保護：ランサムウェア事故復旧	SP 1800-25 SP 1800-26

※年次報告、ドラフト未公開のものは記載していない。

■表 3-4-1　2020 年に発行された出版物（FIPS、SP 800 シリーズ、SP 1800 シリーズ）(3/3)

(4) フレームワーク

「3.4.1 (2)(b) 成果公開」で記載したシリーズ以外の文書で重要なものに Cybersecurity Framework、Privacy Framework がある。このほか、包括的なリスクマネジメントの枠組みとして Risk Management Framework（RMF）がある。SP シリーズ（SP 800-37 Rev.2）として文書化され、Rev.1 は日本語化されている（p.231 表 3-4-3）。これらは連邦政府機関だけでなく、重要インフラ企業を含む民間企業のセキュリティマネジメント、プライバシーマネジメントに関して、経営層とセキュリティ部門のコミュニケーションツールとして策定されている。

2020 年に公開された NISTIR 文書、フレームワークは表 3-4-2（次ページ）のとおりである。

(5) 注目される規格・プロジェクト

2020 年度で注目された規格・プロジェクトについて紹介する。

(a) SP 800-53 Rev. 5 の発行

SP 800-53 は連邦政府機関のセキュリティ管理策標準であるが、近年は ISO/IEC 27001、27002 と並び各国のセキュリティ規格策定において参照され、影響を与え続けている。第 5 版は、2014 年 1 月の第 4 版更新以来 7 年ぶりの改訂となり、クラウド・モバイル・IoT 等の管理対象範囲の拡大、プライバシー保護等への要請を踏まえ、2020 年 9 月 23 日に公開、同年 12 月 10 日に更新された。管理対象を政府組織から民間組織に拡張し、20 のカテゴリーにおいて 1,000 を越える多様な管理

識別子	タイトル	ステータス	公開日	概要	関連規格・IR、法令
組織横断・内部報告（NISTIR シリーズ）					
NISTIR 8323	Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services	Final	2021 年 2 月 11 日	測位サービスのセキュリティプロファイル	大統領令 13905（2020 年 2 月 12 日）
NISTIR 8320A	Hardware-Enabled Security: Container Platform Security Prototype	Draft	2020 年 12 月 7 日	ハードウェアセキュリティ：コンテナ基盤セキュリティ	NISTIR 8320
NISTIR 8312	Four Principles of Explainable Artificial Intelligence (Draft)	Draft	2020 年 8 月 18 日	説明可能な AI に関する 4 原則	—
NISTIR 8309	Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process	Final	2020 年 7 月 22 日	NIST の耐量子暗号標準化状況報告	NISTIR 8240
NISTIR 8301	Blockchain Networks: Token Design and Management Overview	Final	2021 年 2 月 9 日	ブロックチェーンネットワーク：トークン設計と管理	NISTIR 8202
NISTIR 8294	Symposium on Federally Funded Research on Cybersecurity of Electric Vehicle Supply Equipment (EVSE)	Final	2020 年 4 月 29 日	電気自動車充電装置（EVSE）のセキュリティシンポジウム	—
NISTIR 8287	A Roadmap for Successful Regional Alliances and Multistakeholder Partnerships to Build the Cybersecurity Workforce	Final	2020 年 2 月 20 日	セキュリティ人材育成の地域連携プログラム	—
NISTIR 8286A	Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)	Draft	2020 年 12 月 14 日	企業リスク管理におけるセキュリティリスク評価	NISTIR 8286
NISTIR 8286	Integrating Cybersecurity and Enterprise Risk Management (ERM)	Final	2020 年 10 月 13 日	企業リスク管理へのサイバーセキュリティの統合	NISTIR 8286A NISTIR 8170
NISTIR 8278A	National Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers	Final	2020 年 11 月 20 日	OLIR（NIST 規格と他規格のリファレンス）：標準リファレンス作成ガイド	NISTIR 8278
NISTIR 8278	National Online Informative References (OLIR) Program: Program Overview and OLIR Uses	Final	2020 年 11 月 20 日	OLIR：プログラム概要と利用	大統領令 13636
NISTIR 8276	Key Practices in Cyber Supply Chain Risk Management: Observations from Industry	Final	2021 年 2 月 11 日	産業界のサプライチェーンリスク管理プラクティス	SP 800-161 Rev. 1
NISTIR 8259D	Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government	Draft	2020 年 12 月 15 日	IoT コアベースライン、非技術ベースラインの連邦政府機関プロファイル	SP 800-213 NISTIR 8259 NISTIR 8259A NISTIR 8259B NISTIR 8259C
NISTIR 8259C	Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline	Draft	2020 年 12 月 15 日	IoT コアベースライン、非技術ベースラインの作成	SP 800-213 NISTIR 8259 NISTIR 8259A NISTIR 8259B NISTIR 8259D

■表 3-4-2　2020 年に発行された出版物（NISTIR シリーズ、フレームワーク）（1/2）

識別子	タイトル	ステータス	公開日	概要	関連規格・IR、法令
NISTIR 8259B	IoT Non-Technical Supporting Capability Core Baseline	Draft	2020 年 12 月 15 日	IoT 機器製造者の非技術（共通）セキュリティ実践能力	SP 800-213 NISTIR 8259 NISTIR 8259A NISTIR 8259C NISTIR 8259D
NISTIR 8259	Foundational Cybersecurity Activities for IoT Device Manufacturers	Final	2020 年 5 月 29 日	IoT 機器製造者の基本的セキュリティ対策	SP 800-213 NISTIR 8228
NISTIR 8246	Collaborative Vulnerability Metadata Acceptance Process (CVMAP) for CVE Numbering Authorities (CNAs) and Authorized Data Publishers	Final	2020 年 12 月 15 日	CVMAP（脆弱性メタデータ共同受容プロセス）	—
NISTIR 8235	Security Guidance for First Responder Mobile and Wearable Devices	Draft	2020 年 9 月 28 日	救急モバイル・ウェアラブル機器のセキュリティガイド	—
NISTIR 8219	Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection	Final	2020 年 7 月 16 日	製造制御システムの保護：動作異常検知	—
NISTIR 8214A	NIST Roadmap Toward Criteria for Threshold Schemes for Cryptographic Primitives	Final	2020 年 7 月 7 日	秘密分散のしきい値法に関する基準策定ロードマップ	NISTIR 8214
NISTIR 8212	ISCMA: An Information Security Continuous Monitoring Program Assessment	Final	2021 年 3 月 31 日	ISCMA（セキュリティ継続モニタリングプログラム）の評価	SP 800-137 SP 800-137A
NISTIR 8183 Rev. 1	Cybersecurity Framework Version 1.1 Manufacturing Profile	Final	2020 年 10 月 7 日	製造業向けサイバーセキュリティフレームワーク V1.1 プロファイル	NISTIR 8183
NISTIR 8170	Approaches for Federal Agencies to Use the Cybersecurity Framework	Final	2020 年 3 月 19 日	連邦政府機関のサイバーセキュリティフレームワーク実践事例	NISTIR 8286 SP 800-53 Rev. 5
NISTIR 8006	NIST Cloud Computing Forensic Science Challenges	Final	2020 年 8 月 25 日	クラウドフォレンジックの課題	—
フレームワーク					
Privacy Framework Version 1.0	The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0	Final	2020 年 1 月 16 日	プライバシーフレームワーク	Cybersecurity Framework Version 1.1

■表 3-4-2　2020 年に発行された出版物（NISTIR シリーズ、フレームワーク）（2/2）

策が記載されている。主な改訂のポイントは以下のとおりである。

- 情報セキュリティ管理策とプライバシー管理策の統合
- サプライチェーンリスク管理の統合
- 最新の脅威インテリジェンスとサイバー攻撃データに基づく管理策の追加
- 管理策を成果ベースで構成
- コンテンツ関係の記述改善
- 管理策の選択プロセスの管理策からの分離
- 情報システム・組織の管理策ベースラインの SP 800-53B への移行

なお、同時に公開された SP 800-53B は連邦政府のベースラインとなる管理策をまとめている。

(b) サプライチェーンセキュリティ関連規格・プラクティス

2020 年 2 月 21 日、政府調達事業者に連邦政府機関が提供する情報（CUI：Controlled and Unclassified

Information）の保護規定の改訂第2版SP 800-171 Rev. 2が公開され、2021年1月28日に更新された。続いて2021年2月11日、サイバーサプライチェーンリスク管理について、4年にわたり産業界のキープラクティスを収集してきた結果をまとめたNISTIR 8276確定版が公開された。更に同年4月29日、サイバーサプライチェーンリスク管理プラクティスの改訂版SP 800-161 Rev. 1ドラフト版が公開され、コメントが募集された。

こうした規格群が整備される一方で、2020年12月のSolarWinds事案は米国政府・企業のサプライチェーンセキュリティに深刻な課題があることを示し、2021年5月12日、Biden政権はサプライチェーンセキュリティ対策強化を主眼とする大統領令（以下、大統領令）を発表した（「2.2.2（3）SolarWinds事案とその対応」「2.2.2（7）Biden政権の政策」参照）。この中で、NISTには関係部門と協力し、ソフトウェア開発委託に関するガイドラインの暫定版を180日以内に、完全版を360日以内に発行することが求められた。これまでのNISTによるリスクマネジメントやデータ保護の規格化だけではサプライチェーンセキュリティ対策は不十分とされたと考えられる。ソフトウェア調達分野でNISTがどのようなガイドラインを提示するか、注目される。

（c）IoTセキュリティ関連の規格・ガイダンス

2020年12月15日、NISTは連邦政府機関向けのIoT機器調達におけるデバイスセキュリティガイダンスSP 800-213ドラフト版、及びIoTセキュリティに関する非技術支援機能のベースライン、応用別プロファイル作成、実践事例に関する3件のNISTIR（NISTIR 8259B、8259C、8259D）のドラフト版を公開した。同年12月4日に成立したIoT Cybersecurity Improvement Act of 2020[※231]に呼応したものである。NISTはまた、上記ドラフト版と関連文書群の関連をブログで公開した[※232]。このブログではSP 800-213で定めるセキュリティ要件に対して、NISTIR 8259シリーズで提供されるツールを用いて、SP 800-53等の管理策のカタログから具体的なプラクティスを作ってもらう、という構想が説明されている。

（d）ゼロトラストアーキテクチャ関連ガイド

ゼロトラストアーキテクチャへの関心が高まる中、NISTは2020年8月11日、ゼロトラストアーキテクチャのガイドラインSP 800-207を公開した。ゼロトラストの定義や七つの理念、論理アーキテクチャを記載している。また、リソースの認証・認可・アクセス制御が動的なポリシーによって実施されること等を記載している。

更に2021年5月12日、前述の大統領令において、連邦政府システムのサイバーセキュリティ現代化（Modernization）が重要課題とされ、その施策の筆頭にゼロトラストアーキテクチャが明記された。具体的には、各省庁は既存のNISTの規格・ガイダンスに合わせ、ゼロトラストアーキテクチャを段階的に埋め込む（Migration）計画を60日以内に策定することが求められ、連邦政府において同アーキテクチャの実装が火急の課題となった。

（e）人材育成フレームワーク

2020年11月16日、NISTはサイバーセキュリティ教育・人材育成の国家イニシアティブ（NICE：National Initiative for Cybersecurity Education）に基づく枠組みNICE Frameworkを改訂、SP 800-181 Rev. 1として公開した（「2.3.1（4）NICE Frameworkの改訂」参照）。NICE Frameworkは、各職務で行うセキュリティに関するタスクとそれに必要な知識・スキルを示したリファレンスである。

今回の改訂では、煩雑となっていた用語とその関係が簡易化され、Work Role、Tasks、及びKnowledge、Skillsの各用語が残された。また、セキュリティ人材の呼称をより包括なLearnersとする一方、Learnersの評価の記述を示す用語としてCompetenciesが再導入された。NISTは、Cybersecurity Frameworkの成功にならい、NICE Frameworkもサイバーセキュリティ業務・能力記述の共通言語とし、セキュリティ教育・人材育成のエコシステムを構築したいとしている[※233]。

（f）ランサムウェア対策関連プラクティス

世界的に被害が拡大しているランサムウェア対策について、NISTは前掲のNCCoEにおいて、企業のセキュリティ専門家と対策事例（プラクティス）集の策定を進めてきたが、2020年9月22日にランサムウェア事故からの復旧のプラクティス集SP 1800-11を、12月8日に資産管理・防御のプラクティス集SP 1800-25、及び攻撃検知・対処のプラクティス集SP 1800-26を公開した。これらに記載されたプラクティスは「破壊的イベント」におけるデータ一貫性の維持と事業継続に主眼が置かれ、身代金支払い等の経営判断には言及していない。

2021年5月のColonial Pipeline Companyの石油パイプライン停止により、米国重要インフラ企業のランサムウェア対策は喫緊の課題となった（「2.2.2（5）Colonial Pipeline事案とその対応」参照）。上記プラクティス集の

普及に加え、NISTには更なる事例やガイドラインの策定が求められる可能性がある。

(g)その他の規格

NISTは、2008年に発行した情報セキュリティの性能指標ガイドの改訂版発行(SP 800-55 Rev. 2)を計画し、2020年9月から12月10日まで事前意見募集(Pre-draft Call for Comments)を行った※234。2021年5月時点でRev. 2のドラフト版は発行されていない(表3-4-1には未記載)。今後どのような性能指標ガイドが提示されるか、注目される。

Trump政権は2019年2月、頑健で信頼できるAI利用システム開発の技術標準とツールに関する計画の策定をNISTに命じた※235。NISTはこれを受けて計画を発表、意見募集とワークショップを重ねてきたが、2020年8月18日、説明可能なAI(Explainable AI)の4原則をNISTIR 8312としてドラフト版を公開した。AIの判断結果に関する説明性の担保は、特に統計的機械学習技術の信頼性の課題として広く議論されているが、上記NISTIRはNISTの最初の検討成果として注目された。今後も継続的な成果の公開が期待される。

(6)日本のセキュリティ規格・対策との関係

NISTの規格・活動が日本に与える影響について述べる。

(a)NISTシリーズのインパクト

NISTの策定する要件・管理策は国内政府機関のセキュリティ仕様策定において、ISO/IEC 27000シリーズと並び、参照されることが多くなっている。例えば2020年に運用を開始した「政府情報システムのためのセキュリティ評価制度(ISMAP)※236」の管理基準策定においては、グローバル規格としてISO/IEC 27001、27002とともにSP 800-53 Rev. 4がレビューされた(ISMAPの運用については「2.6.3 政府情報システムのためのセキュリティ評価制度(ISMAP)」参照)。また、政府調達事業者が遵守すべきセキュリティ要件については、SP 800-171が注目され、国内政府機関、国内の調達事業者にレビューされてきた※237。サイバーセキュリティ規格が国内に限定されることは効果的でなく、海外規格との整合・海外との連携が必須であるとの認識が政府にも強まっている。

企業においても、米国政府調達に関わる場合はもちろん、グローバルに事業を展開するためには海外規格への対応は必須である。実効的に米国のセキュリティ規格を牽引するNISTの文書を参照する企業が増えている。

(b)規格の日本語化

NIST出版物の分析、国内への展開は主にIPAがその任を担っている。IPAはNIST出版物の概要を紹介するとともに、重要な規格等について日本語版を公開している※238。主として2011年以降に日本語化されたNIST出版物のうち、IPAのWebサイトで掲載しているものを表3-4-3(次ページ)に示す。なお、日本語化はタイムラグが発生する作業であるため、公開版は必ずしも最新バージョンではない(公開後改訂されたものは表中に明記している)。また、仕様の正しい意味を確認する際には原文を参照していただきたい。

(c)NIST事業との連携

IPAは前述したNIST出版物の展開のほか、政府調達暗号(CRYPTREC)に関する技術討議、脆弱性データベースNVD(National Vulnerability Database)※239、NIST Cybersecurity Frameworkと経済産業省のサイバーセキュリティ経営ガイドラインとの整合等で情報共有・連携を行っている。IPAはまた脆弱性管理について、MITRE社の採番するCVEを活用している。IPA以外では、例えば一般社団法人サイバーリスク情報センター産業横断サイバーセキュリティ検討会(CRIC CSF)※240は、Cybersecurity Frameworkの活用を含むサイバーセキュリティマネジメント強化に取り組み、2018年9月にNISTのワークショップで事例を報告している※241。更に、前掲のPQC等の暗号化アルゴリズムプロジェクトでは、日本の研究者も参画、貢献している。

(7)まとめ

NISTは本来米国企業の産業競争力を強化するための連邦政府機関であり、規格や標準化も米国企業、あるいは連邦政府のために策定される。しかし、これまで見たようにその影響力は大きく、策定される標準やガイドライン・フレームワークは世界から参照されるに足る品質と水準を持っている。日本国内のセキュリティ規格、ガイドライン、対策もNISTの活動と整合を保ち、ときにはNISTと協力して推進していくことが望まれる。

識別子	発行日	タイトル	IPA 掲載日	補足
FIPS				
FIPS 199	2004 年 2 月	連邦政府の情報および情報システムに対するセキュリティ分類規格 Standards for Security Categorization of Federal Information and Information Systems	2006 年 8 月	セキュリティ目的と潜在的影響レベルの定義、セキュリティ分類
FIPS 200	2006 年 2 月	連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項 Minimum Security Requirements for Federal Information and Information Systems	2006 年 9 月	最低限のセキュリティ要求事項と影響レベルに合わせた管理策の選択
FIPS 201-1	2006 年 3 月	連邦職員および委託業者のアイデンティティの検証 Personal Identity Verification (PIV) of Federal Employees and Contractors	2011 年 3 月	―
SP 800 シリーズ				
SP 800-30 Rev. 1	2012 年 9 月	リスクアセスメントの実施の手引き Guide for Conducting Risk Assessments	2013 年 2 月	リスクアセスメントの基礎
SP 800-37 Rev. 1	2010 年 2 月	連邦政府情報システムに対するリスクマネジメントフレームワーク適用ガイド：セキュリティライフサイクルによるアプローチ Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach	2011 年 3 月	2018 年 12 月 20 日 Rev. 2 発行（未訳）
SP 800-40 Rev. 2	2005 年 11 月	パッチおよび脆弱性管理プログラムの策定 Creating a Patch and Vulnerability Management Program	2007 年 12 月	2013 年 7 月 22 日 Rev. 3 発行（未訳）
SP 800-52 Rev. 1	2014 年 4 月	トランスポート層セキュリティ(TLS)実装の選択、設定、および使用のためのガイドライン Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations	2017 年 1 月	2019 年 8 月 29 日 Rev. 2 発行（未訳）
SP 800-53 Rev. 4	2013 年 4 月	連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策 Recommended Security Controls for Federal Information Systems	2017 年 1 月	2020 年 12 月 10 日 Rev. 5 更新（未訳）
SP 800-57 Part 1 Rev. 5	2020 年 5 月	鍵管理における推奨事項　第一部：一般事項 Recommendation for Key Management Part 1: General	2021 年 5 月	―
SP 800-57 Part 3 Rev. 1	2015 年 1 月	鍵管理における推奨事項　第三部：アプリケーション特有の鍵管理ガイダンス Recommendation for Key Management Part 3: Application-Specific Key Management Guidance	2016 年 11 月	―
SP 800-61 Rev. 1	2008 年 3 月	コンピュータインシデント対応ガイド Computer Security Incident Handling Guide	2009 年 1 月	2012 年 8 月 6 日 Rev. 2 発行（未訳）
SP 800-63	2006 年 4 月	電子的認証に関するガイドライン Electronic Authentication Guideline	2007 年 8 月	2017 年 12 月 1 日 63-3 発行（未訳） 2020 年 6 月 8 日 63-4 ドラフト版発行（未訳）
SP 800-70	2005 年 5 月	IT 製品のためのセキュリティ設定チェックリストプログラム - チェックリスト利用者と開発者のための手引き Security Configuration Checklists Program for IT Products - Guidance for Checklists Users and Developers	2007 年 3 月	2018 年 2 月 15 日 Rev. 4 発行（未訳）
SP 800-73 Rev. 1	2005 年 4 月	個人識別情報の検証インタフェース Interfaces for Personal Identity Verification	2006 年 10 月	2016 年 2 月 12 日 73-4 発行（未訳）

■表 3-4-3　日本語化された主な NIST 出版物（FIPS、SP 800 シリーズ、フレームワーク）（2021 年 5 月時点）（1/2）

識別子	発行日	タイトル	IPA 掲載日	補足
SP 800-76-1	2007 年 1 月	個人識別情報の検証における生体認証データ仕様（改訂版） Biometric Data Specification for Personal Identity Verification (Rev. 1)	2009 年 10 月	2013 年 7 月 11 日 76-2 発行（未訳）
SP 800-81	2006 年 5 月	セキュアなドメインネームシステム（DNS）の配備ガイド Secure Domain Name System (DNS) Deployment Guide	2009 年 9 月	2013 年 9 月 18 日 81-2 発行（未訳）
SP 800-82 Rev. 2	2015 年 5 月	産業制御システム (ICS) セキュリティ Guide to Industrial Control Systems (ICS) Security	2016 年 3 月	―
SP 800-83	2005 年 11 月	マルウェアによるインシデントの防止と対応のためのガイド Guide to Malware Incident Prevention and Handling	2008 年 9 月	2013 年 7 月 22 日 Rev. 1 発行（未訳）
SP 800-88	2006 年 9 月	媒体のサニタイズに関するガイドライン Guidelines for Media Sanitization	2009 年 9 月	2014 年 12 月 17 日 Rev. 1 発行（未訳）
SP 800-94	2007 年 2 月	侵入検知および侵入防止システム（IDPS）に関するガイド Guide to Intrusion Detection and Prevention Systems (IDPS)	2011 年 3 月	―
SP 800-130	2013 年 8 月	暗号鍵管理システム設計のフレームワーク A Framework for Designing Cryptographic Key Management Systems	2020 年 7 月	―
SP 800-144	2011 年 12 月	パブリッククラウドコンピューティングのセキュリティとプライバシーに関するガイドライン Guidelines on Security and Privacy in Public Cloud Computing	2014 年 3 月	―
SP 800-145	2011 年 9 月	NIST によるクラウドコンピューティングの定義 The NIST Definition of Cloud Computing	2011 年 12 月	NIST によるクラウド定義
SP 800-146	2012 年 5 月	クラウドコンピューティングの概要と推奨事項 Cloud Computing Synopsis and Recommendations	2012 年 8 月	―
SP 800-171 Rev. 2	2020 年 2 月	非連邦政府組織およびシステムにおける管理対象非機密情報 CUI の保護 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	2021 年 2 月	―
SP 800-175A	2016 年 8 月	米国連邦政府での暗号標準利用のためのガイドライン：指令、命令、及び方針 Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies	2021 年 5 月	―
SP 800-175B Rev. 1	2020 年 3 月	米国連邦政府での暗号標準利用のためのガイドライン：暗号メカニズム Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	2021 年 5 月	―
SP 800-190 Rev. 1	2017 年 9 月	アプリケーションコンテナセキュリティガイド Application Container Security Guide	2020 年 9 月	―
SP 800-207	2020 年 8 月	ゼロトラスト・アーキテクチャ Zero Trust Architecture	2020 年 12 月	アーキテクチャ解説
フレームワーク				
Cybersecurity Framework Version 1.1	2018 年 4 月	重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1 版 Framework for Improving Critical Infrastructure Cybersecurity Version 1.1	2019 年 1 月	―

■表 3-4-3　日本語化された主な NIST 出版物（FIPS、SP 800 シリーズ、フレームワーク）（2021 年 5 月時点）（2/2）

※1　NISC が重要インフラの運営を担う事業者と、そこで行われるセキュリティ対策を支援する所管省庁が参照すべき指針として公表している「重要インフラの情報セキュリティ対策に係る行動計画」では、「重要インフラ」として 14 分野が定義されている。
NISC：活動内容　https://www.nisc.go.jp/active/infra/outline.html〔2021/4/27 確認〕
※2　インシデント件数については「JPCERT/CC インシデント報告対応レポート［2013 年 1 月 1 日～ 2013 年 3 月 31 日］」～「JPCERT/CC インシデント報告対応レポート［2020 年 10 月 1 日～ 2020 年 12 月 31 日］」（JPCERT/CC：インシデント報告対応レポート　https://www.jpcert.or.jp/ir/report.html〔2021/4/27 確認〕）を参照した。
※3　TrapX Security Inc.：53% of Manufacturing Organizations Say Operational Technology is Vulnerable to Cyber Attacks　https://trapx.com/53-of-manufacturing-organizations-say-operational-technology-is-vulnerable-to-cyber-attacks/〔2021/4/27 確認〕
※4　Scoop News：Survey Shows Staff Bigger Threat To Cyber And Physical Security Than Cyber Criminals　https://www.scoop.co.nz/stories/BU2003/S00430/survey-shows-staff-bigger-threat-to-cyber-and-physical-security-than-cyber-criminals.htm〔2021/4/27 確認〕
※5　「マルウェア」等の用語を混在して使用すると、読者を混乱させる可能性があるため、本白書では特に断りのない限り、または文献引用上の正確性を期す必要のない限り、総称して「ウイルス」と表現する。
※6　American Military University Edge：Israeli cyber chief: Major attack on water systems thwarted　https://amuedge.com/israeli-cyber-chief-major-attack-on-water-systems-thwarted/〔2021/4/27 確認〕
※7　The Times of Israel：6 facilities said hit in Iran's cyberattack on Israel's water system in April　https://www.timesofisrael.com/6-facilities-said-hit-in-irans-cyberattack-on-israels-water-system-in-april/〔2021/4/27 確認〕
SecurityWeek：Israel Says Hackers Targeted SCADA Systems at Water Facilities　https://www.securityweek.com/israel-says-hackers-targeted-scada-systems-water-facilities〔2021/4/27 確認〕
※8　ZDNet：Two more cyber-attacks hit Israel's water system　https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/〔2021/4/27 確認〕
※9　The Times of Israel：Cyber attacks again hit Israel's water system, shutting agricultural pumps　https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/〔2021/4/27 確認〕
※10　The Washington Post：Officials: Israel linked to a disruptive cyberattack on Iranian port facility　https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html〔2021/4/27 確認〕
※11　Industrial Cyber：OTORIO confirms Iranian hackers gained access to ICS at an Israeli water reservoir　https://industrialcyber.co/threats-attacks/industrial-cyber-attacks/otorio-confirms-iranian-hackers-gained-access-to-ics-at-an-israeli-water-reservoir/〔2021/4/27 確認〕
※12　OTORIO Ltd.：What We've Learned from the December 1st Attack on an Israeli Water Reservoir?　https://www.otorio.com/blog/what-we-ve-learned-from-the-december-1st-attack-on-an-israeli-water-reservoir/〔2021/4/27 確認〕
※13　SecurityWeek：Major Power Outage in India Possibly Caused by Hackers: Reports　https://www.securityweek.com/major-power-outage-india-possibly-caused-hackers-reports〔2021/4/27 確認〕
※14　ZDNet：Hacker modified drinking water chemical levels in a US city　https://www.zdnet.com/article/hacker-modified-drinking-water-chemical-levels-in-a-us-city/〔2021/4/27 確認〕
ZDNet：Following Oldsmar attack, FBI warns about using TeamViewer and Windows 7
https://www.zdnet.com/article/following-oldsmar-attack-fbi-warns-about-using-teamviewer-and-windows-7/〔2021/4/27 確認〕
CyberScoop：Investigators suggest hackers exploited weak password security to breach Florida water facility　https://www.cyberscoop.com/florida-water-facility-hack-password/〔2021/4/27 確認〕
※15　The Brussels Times：Cyber attack sees Picanol shares suspended　https://www.brusselstimes.com/news-contents/economic/89253/cyber-attack-sees-picanol-shares-suspended/〔2021/4/27 確認〕
Picanol：Press release: cyber attack - update January 31, 2020
https://www.picanol.be/news/press-release-cyber-attack-update-january-31-2020〔2021/4/27 確認〕
※16　Dragos, Inc.：Assessment of Ransomware Event at U.S. Pipeline Operator　https://www.dragos.com/blog/industry-news/assessment-of-ransomware-event-at-u-s-pipeline-operator/〔2021/4/27 確認〕
CISA：Alert (AA20-049A)Ransomware Impacting Pipeline Operations　https://us-cert.cisa.gov/ncas/alerts/aa20-049a〔2021/4/27 確認〕
※17　ZDNet：One of Roman Abramovich's companies got hit by ransomware　https://www.zdnet.com/article/one-of-roman-abramovichs-companies-got-hit-by-ransomware/〔2021/4/27 確認〕
※18　iTnews：BlueScope IT 'disruption' feared to be ransomware attack　https://www.itnews.com.au/news/bluescope-it-disruption-feared-to-be-ransomware-attack-548127〔2021/4/27 確認〕
BlueScope Steel Limited：BLUESCOPE RESPONSE TO CYBER INCIDENT　https://secure.weblink.com.au/clients/WebChartClient/clients/BlueScopeSteel2/article.asp?view=3541284〔2021/4/27 確認〕
※19　iTnews：Fisher & Paykel Appliances struck by Nefilim ransomware　https://www.itnews.com.au/news/fisher-paykel-appliances-struck-by-nefilim-ransomware-549102〔2021/4/27 確認〕
※20　Business Wire：X-FAB Affected by Cyber Attack　https://www.businesswire.com/news/home/20200705005045/en/X-FAB-Affected-Cyber-Attack〔2021/4/27 確認〕
Business Wire：X-FAB on Track to Resume Production After Cyber Attack　https://www.businesswire.com/news/home/20200712005045/en/X-FAB-Track-Resume-Production-Cyber-Attack〔2021/4/27 確認〕
※21　The Times of Israel：Israeli chip manufacturer Tower says it was targeted in cyberattack　https://www.timesofisrael.com/israeli-chip-manufacturer-tower-says-it-was-targeted-in-cyberattack/〔2021/4/27 確認〕
eeNews Europe：Cyberattack is resolved but will hit Tower's results　https://www.eenewseurope.com/news/cyberattack-resolved-will-hit-towers-results〔2021/4/27 確認〕
※22　NorfolkToday.ca：A Ransomware Attack Temporarily Shut Down Steel Production At Stelco　https://www.norfolktoday.ca/2020/10/28/a-ransomware-attack-temporarily-shut-down-steel-production-at-stelco/〔2021/4/27 確認〕
※23　BleepingComputer：Steelcase furniture giant down for 2 weeks after ransomware attack　https://www.bleepingcomputer.com/news/security/steelcase-furniture-giant-down-for-2-weeks-after-ransomware-attack/〔2021/4/27 確認〕
※24　Dragos, Inc.：EKANS Ransomware and ICS Operations　https://dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/〔2021/4/27 確認〕
※25　AO Kaspersky Lab：Targeted attacks on industrial companies using Snake ransomware　https://ics-cert.kaspersky.com/alerts/2020/06/17/targeted-attacks-on-industrial-companies-using-snake-ransomware/〔2021/4/27 確認〕
※26　BANK INFO SECURITY：Honda Confirms Hack Attack Disrupted Global Production　https://www.bankinfosecurity.com/honda-confirms-cyberattack-affecting-global-production-a-14410〔2021/4/27 確認〕
※27　BleepingComputer：Enel Group hit by ransomware again, Netwalker demands $14 million　https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million/〔2021/4/27 確認〕
※28　ZDNet：Microsoft, FireEye confirm SolarWinds supply chain attack　https://www.zdnet.com/article/microsoft-fireeye-confirm-solarwinds-supply-chain-attack/〔2021/4/27 確認〕
※29　ChannelE2E：SolarWinds Orion Security Breach: Cyberattack Timeline and Hacking Incident Details　https://www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details/〔2021/4/27 確認〕
※30　ITmedia エンタープライズ：第 4 のマルウェア「Raindrop」発見 続く SolarWinds サイバー攻撃の解析　https://www.itmedia.co.jp/enterprise/articles/2101/20/news118.html〔2021/4/27 確認〕
※31　ITmedia NEWS：1 年以上も検出できなかった「史上最大級の高度な攻撃」、同じ弱点は世界中に　https://www.itmedia.co.jp/news/articles/2101/25/news064.html〔2021/4/27 確認〕
※32　POLITICO：How suspected Russian hackers outed their massive cyberattack　https://www.politico.com/news/2020/12/

16/russian-hackers-fireeye-cyberattack-447226〔2021/4/27 確認〕
FireEye, Inc.：Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html〔2021/4/27 確認〕
※ 33 AO Kaspersky Lab：SunBurst industrial victims https://ics-cert.kaspersky.com/reports/2021/01/26/sunburst-industrial-victims/〔2021/4/27 確認〕
※ 34 CISA：Alert (AA20-352A)：Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations https://us-cert.cisa.gov/ncas/alerts/aa20-352a〔2021/4/27 確認〕
※ 35 Reuters：Exclusive: Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency – sources https://www.reuters.com/article/us-cyber-solarwinds-china/exclusive-suspected-chinese-hackers-used-solarwinds-bug-to-spy-on-u-s-payroll-agency-sources-idUSKBN2A22K8〔2021/4/27 確認〕
※ 36 https://discover.honeywell.com/USBThreatReport-8156-Registrationpage.html〔2021/4/27 確認〕
※ 37 ICS-CERT の Web サイトで暦年（1/1 ～ 12/31）ごとに公開された ICSA Advisories の件数をカウントした。ただし、ICSMA（医療機器の脆弱性）は除く。カウントは公表日ベースとした（公表日が 2020 年なら、採番年度が 2019（ICSA-2019-xxx-x）でも 2020 年でカウント）。
NCCIC：ICS-CERT Advisories https://ics-cert.us-cert.gov/advisories〔2021/4/27 確認〕
※ 38 JSOF Ltd.：Ripple20 https://www.jsof-tech.com/disclosures/ripple20/〔2021/4/27 確認〕
※ 39 https://nvd.nist.gov/vuln/detail/CVE-2020-25191〔2021/4/27 確認〕
※ 40 SecurityWeek：Vulnerability in NI Controller Can Allow Hackers to Remotely Disrupt Production https://www.securityweek.com/vulnerability-ni-controller-can-allow-hackers-remotely-disrupt-production〔2021/5/27 確認〕
※ 41 CISA：ICS Advisory (ICSA-20-338-01) National Instruments CompactRIO https://us-cert.cisa.gov/ics/advisories/icsa-20-338-01〔2021/4/27 確認〕
※ 42 NISC：Fortinet 製 VPN の脆弱性 (CVE-2018-13379) に関する重要インフラ事業者等についての注意喚起の発出について https://www.nisc.go.jp/active/infra/pdf/fortinet20201203.pdf〔2021/4/27 確認〕
※ 43 NIST：CVE-2018-13379 Detail https://nvd.nist.gov/vuln/detail/CVE-2018-13379〔2021/4/27 確認〕
※ 44 Dragos, Inc.：Ransomware in ICS Environments https://www.dragos.com/resource/ransomware-in-ics-environments/〔2021/4/27 確認〕
※ 45 Back End News：Sophos releases cyber attack trends to shape IT security in 2020 https://backendnews.net/sophos-releases-cyber-attack-trends-to-shape-it-security-in-2020/〔2021/4/27 確認〕
※ 46 PhishLabs：Year In Review: Ransomware https://info.phishlabs.com/blog/year-in-review-ransomware〔2021/4/27 確認〕
※ 47 BleepingComputer：US aerospace services provider breached by Maze Ransomware https://www.bleepingcomputer.com/news/security/us-aerospace-services-provider-breached-by-maze-ransomware/〔2021/4/27 確認〕
※ 48 BleepingComputer：Chipmaker MaxLinear reports data breach after Maze Ransomware attack https://www.bleepingcomputer.com/news/security/chipmaker-maxlinear-reports-data-breach-after-maze-ransomware-attack/〔2021/4/27 確認〕
※ 49 https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_Control_Systems_S508C.pdf〔2021/4/27 確認〕
※ 50 NIST：NISTIR 8183 Rev. 1 https://csrc.nist.gov/publications/detail/nistir/8183/rev-1/final〔2021/4/27 確認〕
※ 51 Marine Log：Cybersecurity: Attacks on OT systems are on the increase https://www.marinelog.com/news/cybersecurity-attacks-on-ot-systems-are-on-the-increase/〔2021/4/27 確認〕
※ 52 IMO：RESOLUTION MSC.428(98) https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428(98).pdf〔2021/4/27 確認〕
※ 53 https://www.intercargo.org/wp-content/uploads/2020/05/2021-12-23-Guidelines-on-Cyber-Security-Onboard-Ships-v.4.pdf〔2021/4/27 確認〕
※ 54 ENISA：Cybersecurity in the Maritime Sector: ENISA Releases New Guidelines for Navigating Cyber Risk https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-maritime-sector-enisa-releases-new-guidelines-for-navigating-cyber-risk〔2021/4/27 確認〕
※ 55 ENISA：Port Cybersecurity - Good practices for cybersecurity in the maritime sector https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector〔2021/4/27 確認〕
※ 56 サイバーセキュリティ戦略本部：サイバーセキュリティ 2020（2019 年度年次報告・2020 年度年次計画） https://www.nisc.go.jp/active/kihon/pdf/cs2020.pdf〔2021/4/27 確認〕
※ 57 https://t-isac.or.jp/〔2021/4/27 確認〕
※ 58 内閣府：Society 5.0 https://www8.cao.go.jp/cstp/society5_0/〔2021/4/27 確認〕
※ 59 経済産業省：Connected Industries https://www.meti.go.jp/policy/mono_info_service/connected_industries/index.html〔2021/4/27 確認〕
※ 60 経済産業省：IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）を策定しました https://www.meti.go.jp/press/2020/11/20201105003/20201105003.html〔2021/4/27 確認〕
※ 61 https://www.meti.go.jp/press/2020/02/20210222004/20210222004-1.pdf〔2021/6/10 確認〕
※ 62 IPA：「制御システムのセキュリティリスク分析ガイド 第 2 版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～」を公開 https://www.ipa.go.jp/security/controlsystem/riskanalysis.html〔2021/4/27 確認〕
※ 63 IPA：制御システムのセキュリティリスク分析ガイド：セミナー https://www.ipa.go.jp/security/controlsystem/seminar.html〔2021/4/27 確認〕
※ 64 IPA：制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ https://www.ipa.go.jp/security/controlsystem/incident.html〔2021/4/27 確認〕
※ 65 詳細リスク分析手法の一つで、サイバー攻撃で想定される事業被害に基づいてリスク分析を行う。
※ 66 NIST：National Vulnerability Database（NVD） https://nvd.nist.gov/〔2021/4/28 確認〕
※ 67 IPA：JVN iPedia 脆弱性対策情報データベース https://jvndb.jvn.jp/〔2021/4/28 確認〕
※ 68 OffSec Services Limited：Exploit Database https://www.exploit-db.com/〔2021/4/28 確認〕
※ 69 感染した IoT 機器上で不正なプログラムを実行し、ボットネットを構成するとともに、DDoS 攻撃の踏み台等のサイバー攻撃への悪用を試みるウイルス。典型例である「Mirai」や「Gafgyt（別名、Bashlite、QBot 等）」は、それぞれソースコードが公開されており、様々な亜種が出現している。Mirai の詳細に関しては、「情報セキュリティ白書 2017」の「3.2.1（1）Mirai による DDoS 攻撃の脅威」（p.174）を参照。
※ 70 PoC（Proof of Concept）：発見された脆弱性を実証するために公開されたプログラムコード。IoT 機器を狙うサイバー攻撃において、不正侵入やウイルス感染を試みる悪意のプログラムの一部として悪用されることがある。
※ 71 警察庁：宛先ポート 4567/TCP に対する Mirai ボットの特徴を有するアクセスの増加等について https://www.npa.go.jp/cyberpolice/detect/pdf/20200226.pdf〔2021/4/28 確認〕
※ 72 mcw0：PoC / TVT_and_OEM_IPC_NVR_DVR_RCE_Backdoor_and_Information_Disclosure.txt https://github.com/mcw0/PoC/blob/master/TVT_and_OEM_IPC_NVR_DVR_RCE_Backdoor_and_Information_Disclosure.txt〔2021/4/28 確認〕
※ 73 リバースシェル：ウイルス感染させた IoT 機器から攻撃者がインターネット上に用意したサーバにアクセスさせることによって、感染 IoT 機器の遠隔操作を試みる攻撃手法。
※ 74 警察庁：複数の IoT 機器等の脆弱性を標的としたアクセスの増加等について https://www.npa.go.jp/cyberpolice/detect/pdf/20200130.pdf〔2021/4/28 確認〕
※ 75 TVT 社：Notification of Critical Vulnerabilities http://en.tvt.net.cn/news/227.html〔2021/4/28 確認〕
※ 76 IPVM：A List Of TVT's 79 DVR OEMs https://ipvm.com/forums/video-surveillance/topics/a-list-of-tvt-s-79-dvr-oems〔2021/4/28 確認〕
※ 77 Trend Micro Incorporated：SORA and UNSTABLE: 2 Mirai Variants Target Video Surveillance Storage Systems https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/sora-and-unstable-2-mirai-variants-target-video-surveillance-storage-systems/〔2021/4/28 確認〕
※ 78 Palo Alto Networks, Inc.：New Mirai Variant Targets Zyxel Network-Attached Storage Devices https://unit42.paloaltonetworks.

com/new-mirai-variant-mukashi/〔2021/4/28 確認〕
パロアルトネットワークス株式会社：Zyxel の NAS の脆弱性（CVE-2020-9054）を標的にした新しい Mirai 亜種、Mukashi が発見される https://unit42.paloaltonetworks.jp/new-mirai-variant-mukashi/〔2021/4/28 確認〕
※ 79 Zyxel 社：Zyxel security advisory for the remote code execution vulnerability of NAS and firewall products https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml〔2021/4/28 確認〕
※ 80 Qihoo 360 Technology Co., Ltd.：Multiple botnets are spreading using LILIN DVR 0-day https://blog.netlab.360.com/multiple-botnets-are-spreading-using-lilin-dvr-0-day-en/〔2021/4/28 確認〕
※ 81 Sophos Ltd.：Chalubo botnet wants to DDoS from your server or IoT device https://news.sophos.com/en-us/2018/10/22/chalubo-botnet-wants-to-ddos-from-your-server-or-iot-device/〔2021/4/28 確認〕
※ 82 fbotの詳細に関しては、「情報セキュリティ白書2020」の「3.2.1（1）（b）fbot」（p.167）を参照。
※ 83 Moobotの詳細に関しては、「情報セキュリティ白書2020」の「3.2.1（1）（h）Moobot」（p.172）を参照。
※ 84 LILIN 社：利凌企業股份有限公司網路商品資安漏洞修正通知／Merit LILIN Network Product Vulnerability Notification https://www.meritlilin.com/assets/uploads/support/file/M00158-TW.pdf〔2021/4/28 確認〕
※ 85 警察庁：Apache Tomcat の脆弱性 (CVE-2020-1938) を標的としたアクセスの観測等について https://www.npa.go.jp/cyberpolice/detect/pdf/20200325.pdf〔2021/4/28 確認〕
※ 86 Habr：Full disclosure: 0day vulnerability (backdoor) in firmware for Xiaongmai-based DVRs, NVRs and IP cameras https://habr.com/en/post/486856/〔2021/4/28 確認〕
※ 87 Xiongmai 社：Security Advisory – Vulnerability of some XM product before year 2017 https://www.xiongmaitech.com/en/index.php/news/info/12/68〔2021/4/28 確認〕
※ 88 https://www.shodan.io/〔2021/4/28 確認〕
※ 89 国立研究開発法人情報通信研究機構 NICTER Blog:ビデオレコーダを狙った 9530/tcp 宛通信の増加について https://blog.nicter.jp/2020/04/nvr-9530/〔2021/4/28 確認〕
※ 90 Qihoo 360 Technology Co., Ltd.：Two zero days are Targeting DrayTek Broadband CPE Devices https://blog.netlab.360.com/two-zero-days-are-targeting-draytek-broadband-cpe-devices-en/〔2021/4/28 確認〕
※ 91 DrayTek 社：Vigor3900 / Vigor2960 / Vigor300B Router Web Management Page Vulnerability (CVE-2020-8515) https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-router-web-management-page-vulnerability-(cve-2020-8515)/〔2021/4/28 確認〕
※ 92 DrayTek 社：DrayTek Security Advisory https://www.draytek.com/about/security-advisory〔2021/4/28 確認〕
※ 93 C&C サーバ：Command and Control サーバの略。ウイルス等により乗っ取ったコンピュータ等（ここでは IoT 機器）に対し、遠隔から命令を送り制御するサーバ。
※ 94 IRC（Internet Relay Chat）：サーバを介してクライアント同士がテキストベースの通信を行うプロトコル。サイバー攻撃において、C&C サーバと乗っ取った IoT 機器との間の通信に悪用される。
※ 95 Palo Alto Networks, Inc.：Grandstream and DrayTek Devices Exploited to Power New Hoaxcalls DDoS Botnet https://unit42.paloaltonetworks.com/new-hoaxcalls-ddos-botnet/〔2021/4/28 確認〕
パロアルトネットワークス株式会社：Grandstream および DrayTek デバイスのエクスプロイトで拡大する新たな Hoaxcalls DDoS ボットネット https://unit42.paloaltonetworks.jp/new-hoaxcalls-ddos-botnet/〔2021/4/28 確認〕
※ 96 Packet Strom：DrayTek Vigor2960 / Vigor3900 / Vigor300B Remote Command Execution https://packetstormsecurity.com/files/156979/DrayTek-Vigor2960-Vigor3900-Vigor300B-Remote-Command-Execution.html〔2021/4/28 確認〕
※ 97 Radware Ltd.：Evolution of Hoaxcalls https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/hoaxcalls-evolution/〔2021/4/28 確認〕
※ 98 IT Security Research by Pierre：Multiple vulnerabilities found in Zyxel CNM SecuManager https://pierrekim.github.io/blog/2020-03-09-zyxel-secumanager-0day-vulnerabilities.html〔2021/4/28 確認〕
※ 99 国家信息安全漏洞共享平台（CNVD：China National Vulnerability Database）：ZyXEL Cloud CNM SecuManager 未授权远程代码执行漏洞 https://www.cnvd.org.cn/flaw/show/CNVD-2020-16839〔2021/4/28 確認〕
※ 100 Zyxel 社：Zyxel security advisory for vulnerabilities of CloudCNM SecuManager https://www.zyxel.com/support/vulnerabilities-of-CloudCNM-SecuManager.shtml〔2021/4/28 確認〕
※ 101 警察庁：Zyxel CNM SecuManager の脆弱性を標的としたアクセスの観測等について https://www.npa.go.jp/cyberpolice/detect/pdf/20200605.pdf〔2021/4/28 確認〕
※ 102 Palo Alto Networks, Inc.：Mirai and Hoaxcalls Botnets Target Legacy Symantec Web Gateways https://unit42.paloaltonetworks.com/hoaxcalls-mirai-target-legacy-symantec-web-gateways/〔2021/4/28 確認〕
パロアルトネットワークス株式会社:Mirai、Hoaxcalls が標的を拡大 サポート終了バージョンの Symantec Web Gateway を狙う https://unit42.paloaltonetworks.jp/hoaxcalls-mirai-target-legacy-symantec-web-gateways/〔2021/4/28 確認〕
※ 103 code16（cody sixteen）：HUNTING 0DAYS with Symantec Web Gateway 5.0.2.8 https://dl.packetstormsecurity.net/2004-exploits/symantecwg5028-exec.pdf〔2021/4/28 確認〕
※ 104 Internet Initiative Japan Inc.：Mirai 亜種（XTC）による感染活動の観測 https://wizsafe.iij.ad.jp/2020/05/967/〔2021/4/28 確認〕
※ 105 Internet Initiative Japan Inc.：wizSafe Security Signal 2020 年 5 月 観測レポート https://wizsafe.iij.ad.jp/2020/06/1004/〔2021/4/28 確認〕
※ 106 Qihoo 360 Technology Co., Ltd.：Multiple fiber routers are being compromised by botnets using 0-day https://blog.netlab.360.com/multiple-fiber-routers-are-being-compromised-by-botnets-using-0-day-en/〔2021/4/28 確認〕
※ 107 Trend Micro Incorporated：Mirai Updates: New Variant Mukashi Targets NAS Devices, New Vulnerability Exploited in GPON Routers, UPX-Packed FBot https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mirai-updates-new-variant-mukashi-targets-nas-devices-new-vulnerability-exploited-in-gpon-routers-upx-packed-fbot〔2021/4/28 確認〕
※ 108 Qihoo 360 Technology Co., Ltd.：The LeetHozer botnet https://blog.netlab.360.com/the-leethozer-botnet-en/〔2021/4/28 確認〕
※ 109 Palo Alto Networks, Inc.：6 New Vulnerabilities Found on D-Link Home Routers https://unit42.paloaltonetworks.com/6-new-d-link-vulnerabilities-found-on-home-routers/〔2021/4/28 確認〕
パロアルトネットワークス株式会社：D-Link ホームルーターで発見された 6 つの新たな脆弱性 https://unit42.paloaltonetworks.jp/6-new-d-link-vulnerabilities-found-on-home-routers/〔2021/4/28 確認〕
※ 110 D-Link 社：DIR-865L :: Rev. Ax :: End of Support / End of Life Product :: Reporting Multiple Vulnerabilities https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10174〔2021/4/28 確認〕
※ 111 Qihoo 360 Technology Co., Ltd.：The new Bigviktor Botnet is Targeting DrayTek Vigor Router https://blog.netlab.360.com/bigviktor-dga-botnet/〔2021/4/28 確認〕
※ 112 Trend Micro Incorporated：New Mirai Variant Expands, Exploits CVE-2020-10173 https://www.trendmicro.com/en_us/research/20/g/new-mirai-variant-expands-arsenal-exploits-cve-2020-10173.html〔2021/4/28 確認〕
トレンドマイクロ株式会社：ルータの脆弱性「CVE-2020-10173」を利用する IoT マルウェア https://blog.trendmicro.co.jp/archives/25896〔2021/4/28 確認〕
※ 113 Medium：Tenda AC15 AC1900 Vulnerabilities Discovered and Exploited https://blog.securityevaluators.com/tenda-ac1900-vulnerabilities-discovered-and-exploited-e8e26aa0bc68〔2021/4/28 確認〕
※ 114 Trend Micro Incorporated：Mirai Botnet Attack IoT Devices via CVE-2020-5902 https://www.trendmicro.com/en_us/research/20/g/mirai-botnet-attack-iot-devices-via-cve-2020-5902.html〔2021/4/28 確認〕
トレンドマイクロ株式会社：「BIG-IP」の脆弱性「CVE-2020-5902」を利用する IoT マルウェアを確認 https://blog.trendmicro.co.jp/archives/26197〔2021/4/28 確認〕
※ 115 F5 社：K52145254: TMUI RCE vulnerability CVE-2020-5902 https://support.f5.com/csp/article/K52145254〔2021/4/28 確認〕
※ 116 GRIMM Blog（SMFS, Inc.）：SOHO Device Exploitation https://blog.grimm-co.com/2020/06/soho-device-exploitation.html〔2021/4/28 確認〕

※ 117 警察庁：ZeroShell の脆弱性を標的としたアクセスの観測について https://www.npa.go.jp/cyberpolice/detect/pdf/20200811.pdf〔2021/4/28 確認〕
※ 118 警察庁：vBulletin の脆弱性（CVE-2020-17496）を標的としたアクセスの観測等について https://www.npa.go.jp/cyberpolice/detect/pdf/20201016.pdf〔2021/4/28 確認〕
※ 119 「情報セキュリティ白書 2019」の「3.2.1 (2) (c) 仮想通貨マイニングへの悪用（ADB.Miner）」（p.167）を参照。
※ 120 Palo Alto Networks, Inc.：3 Vulnerabilities Found on AvertX IP Cameras https://unit42.paloaltonetworks.com/avertx-ip-cameras-vulnerabilities/〔2021/4/28 確認〕
パロアルトネットワークス株式会社：AvertX 製 IP カメラで 3 つの脆弱性が見つかる https://unit42.paloaltonetworks.jp/avertx-ip-cameras-vulnerabilities/〔2021/4/28 確認〕
※ 121 Qihoo 360 Technology Co., Ltd.：Quick update on the Linux.Ngioweb botnet, now it is going after IoT devices https://blog.netlab.360.com/linux-ngioweb-v2-going-after-iot-devices-en/〔2021/4/28 確認〕
※ 122 Qihoo 360 Technology Co., Ltd.：An Analysis of Linux.Ngioweb Botnet https://blog.netlab.360.com/an-analysis-of-linux-ngioweb-botnet-en/〔2021/4/28 確認〕
※ 123 Qihoo 360 Technology Co., Ltd.：Ghost in action: the Specter botnet https://blog.netlab.360.com/ghost-in-action-the-specter-botnet/〔2021/4/28 確認〕
※ 124 Qihoo 360 Technology Co., Ltd.：In the wild QNAP NAS attacks https://blog.netlab.360.com/in-the-wild-qnap-nas-attacks-en/〔2021/4/28 確認〕
※ 125 Qihoo 360 Technology Co., Ltd.：Ttint: An IoT Remote Access Trojan spread through 2 0-day vulnerabilities https://blog.netlab.360.com/ttint-an-iot-remote-control-trojan-spread-through-2-0-day-vulnerabilities/〔2021/4/28 確認〕
※ 126 Qihoo 360 Technology Co., Ltd.：HEH, a new IoT P2P Botnet going after weak telnet services https://blog.netlab.360.com/heh-a-new-iot-p2p-botnet-going-after-weak-telnet-services/〔2021/5/27 確認〕
※ 127 Palo Alto Networks, Inc.：Two New IoT Vulnerabilities Identified with Mirai Payloads https://unit42.paloaltonetworks.com/iot-vulnerabilities-mirai-payloads/〔2021/4/28 確認〕
パロアルトネットワークス株式会社：Mirai 亜種のペイロードに 2 つの新しい IoT 脆弱性を特定 https://unit42.paloaltonetworks.jp/iot-vulnerabilities-mirai-payloads/〔2021/4/28 確認〕
※ 128 サニタイズ（無害化）：値をチェックして攻撃に使用されるコードが含まれていた場合は除去（無効化）すること。
※ 129 警察庁：Oracle WebLogic Server の脆弱性（CVE-2020-14882）を標的としたアクセスの観測等について https://www.npa.go.jp/cyberpolice/detect/pdf/20201224.pdf〔2021/4/28 確認〕
※ 130 Qihoo 360 Technology Co., Ltd.：MooBot on the run using another 0 day targeting UNIX CCTV DVR https://blog.netlab.360.com/moobot-0day-unixcctv-dvr-en/〔2021/4/28 確認〕
※ 131 警察庁：脆弱性が存在する複数の IoT 機器を標的としたアクセスの増加等について https://www.npa.go.jp/cyberpolice/detect/pdf/20210305.pdf〔2021/4/28 確認〕
※ 132 Sophos Ltd.：Glupteba: Hidden Malware Delivery in Plain Sight https://news.sophos.com/wp-content/uploads/2020/06/glupteba_final.pdf〔2021/4/28 確認〕
※ 133 YouTube JSOF Channel：JSOF Ripple20 Exploit UPS https://www.youtube.com/watch?v=jkfNE_Twa1s〔2021/4/28 確認〕
※ 134 ICS-CERT：ICS Advisory (ICSA-20-168-01) Treck TCP/IP Stack (Update G) https://us-cert.cisa.gov/ics/advisories/icsa-20-168-01〔2021/4/28 確認〕
※ 135 Treck 社：Vulnerability Response Information https://treck.com/vulnerability-response-information/〔2021/4/28 確認〕
※ 136 図研エルミック株式会社：KASAGO 製品における脆弱性に関するお知らせ https://www.elwsc.co.jp/wp-content/uploads/2020/06/KASAGO202006-1.pdf〔2021/4/28 確認〕
※ 137 NISC：多くのデバイスが影響を受ける複数の脆弱性「Ripple20」に関する参考情報 https://www.nisc.go.jp/active/infra/pdf/Ripple2020200624.pdf〔2021/4/28 確認〕
※ 138 ブラザー工業株式会社：セキュリティーデータベース脆弱性識別番号 CVE-2020-11896 等、複数の脆弱性の対応について https://support.brother.co.jp/j/b/faqend.aspx?c=jp&lang=ja&prod=group2&faqid=faq00100718_002〔2021/4/28 確認〕
※ 139 デル・テクノロジーズ株式会社：Ripple20 の脆弱性に対するデルの対応 https://www.dell.com/support/kbdoc/ja-jp/000126658〔2021/4/28 確認〕
※ 140 三菱電機株式会社：TCP/IP スタックにおける複数の脆弱性（Ripple20）の影響について https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2020-010.pdf〔2021/4/28 確認〕
※ 141 株式会社リコー：「Ripple20」によるリコー製品への影響について https://jp.ricoh.com/info/notice/2020/0731_1〔2021/4/28 確認〕
※ 142 JSOF Ltd.：CVE-2020-11896 RCE CVE-2020-11898 Info Leak https://www.jsof-tech.com/jsof_ripple20_technical_whitepaper_june20/〔2021/4/28 確認〕
※ 143 JSOF Ltd.：CVE-2020-11901 https://www.jsof-tech.com/ripple20_cve-2020-11901-august20/〔2021/4/28 確認〕
※ 144 JVN：JVNVU#94829658 Treck 社製 TCP/IP スタックに複数の脆弱性 https://jvn.jp/vu/JVNVU94829658/index.html〔2021/4/28 確認〕
※ 145 ICS-CERT：ICS Advisory (ICSA-20-353-01) Treck TCP/IP Stack (Update A) https://us-cert.cisa.gov/ics/advisories/icsa-20-353-01〔2021/4/28 確認〕
※ 146 三菱電機株式会社：当社製品の TCP プロトコルスタックにおける悪意のあるプログラムが実行される脆弱性 https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2020-022.pdf〔2021/4/28 確認〕
※ 147 Forescout Technologies Inc.：AMNESIA:33 https://www.forescout.com/research-labs/amnesia33/〔2021/4/28 確認〕
※ 148 ICS-CERT：ICS Advisory (ICSA-20-343-01) Multiple Embedded TCP/IP Stacks https://us-cert.cisa.gov/ics/advisories/icsa-20-343-01〔2021/4/28 確認〕
※ 149 Palo Alto Networks, Inc.：Risks in IoT Supply Chain https://unit42.paloaltonetworks.com/iot-supply-chain/〔2021/4/28 確認〕
パロアルトネットワークス株式会社：IoT サプライチェーンのリスク https://unit42.paloaltonetworks.jp/iot-supply-chain/〔2021/4/28 確認〕
※ 150 F-Secure Corporation：THE FAKE CISCO - Hunting for backdoors in Counterfeit Cisco devices https://labs.f-secure.com/assets/BlogFiles/2020-07-the-fake-cisco.pdf〔2021/4/28 確認〕
※ 151 ForAllSecure, Inc.：Uncovering OpenWRT Remote Code Execution (CVE-2020-7982) https://forallsecure.com/blog/uncovering-openwrt-remote-code-execution-cve-2020-7982〔2021/4/28 確認〕
※ 152 https://notice.go.jp/〔2021/4/28 確認〕
※ 153 NOTICE サポートセンター：実施状況 https://notice.go.jp/status〔2021/4/28 確認〕
※ 154 警察庁：インターネット観測結果等（令和2年） https://www.npa.go.jp/cyberpolice/detect/pdf/20210316.pdf〔2021/4/28 確認〕
※ 155 感染した IoT 機器上で不正なプログラムを実行し、ボットネットを構成するとともに、IoT 機器を狙った他のウイルスが感染に悪用する通信ポートの遮断等を実施して、結果的に機器を他のウイルス感染から防御するウイルス。Hajime の詳細に関しては、「情報セキュリティ白書 2018」の「3.1.1 (1) IoT 機器の Mirai 等の感染に対抗する『Hajime』」（p.162）を参照。
※ 156 Qihoo 360 Technology Co., Ltd.：An Update for a Very Active DDos Botnet: Moobot https://blog.netlab.360.com/ddos-botnet-moobot-en/〔2021/4/28 確認〕
※ 157 総務省：サイバー攻撃に悪用されるおそれのある IoT 機器の調査（NOTICE）の取組強化 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00079.html〔2021/4/28 確認〕
※ 158 一般社団法人 ICT-ISAC：脆弱な状態にある重要 IoT 機器の調査及び注意喚起について https://www.ict-isac.jp/news/news20200728.html〔2021/4/28 確認〕
※ 159 「IoT セキュリティ法」の詳細に関しては、「情報セキュリティ白書 2020」の「3.2.3 (2) (b) カリフォルニア州における法規制の施行開始」（p.180）を参照。
※ 160 Fox Rothschild LLP：The Internet of (Secure) Things: California Now Regulates Security of IoT Devices https://www.foxrothschild.com/publications/the-internet-of-secure-things-california-now-regulates-security-of-iot-devices/〔2021/4/28 確認〕
※ 161 Oregon State Legislature：Enrolled House Bill 2395 https://olis.leg.state.or.us/liz/2019R1/Downloads/MeasureDocument/HB2395/Enrolled〔2021/4/28 確認〕
※ 162 Illinois General Assembly：Bill Status of HB3391 101st General Assembly https://www.ilga.gov/legislation/BillStatus.asp?DocNum=3391&GAID=15&DocTypeID=HB&LegId=119982&SessionID=108&GA=101〔2021/4/28 確認〕
※ 163 Maryland General Assembly：Legislation - HB1276 https://mgaleg.maryland.gov/mgawebsite/legislation/details/hb1276?ys=2019rs〔2021/4/28 確認〕
※ 164 General Court of the Commonwealth of Massachusetts：Bill S.2056 191st(2019-2020) https://malegislature.gov/Bills/

191/S2056〔2021/4/28 確認〕
※ 165 Washington State Legislature：HOUSE BILL 2365 https://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/House%20Bills/2365.pdf〔2021/4/28 確認〕
※ 166 JSSEC：『IoT セキュリティチェックシート入門』を公開しました。https://www.jssec.org/report/20200901.html〔2021/4/28 確認〕
※ 167 CCDS：CCDS スマートホーム分野サービス向けサーティフィケーションプログラム実施に向けて https://www.ccds.or.jp/public/document/other/[CCDS]PressRelease_ スマートホーム分野サービス向けサーティフィケーションプログラム実施 .pdf〔2021/4/28 確認〕
※ 168 経済産業省：機器のサイバーセキュリティ確保のためのセキュリティ検証の手引きを取りまとめました https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html〔2021/4/28 確認〕
※ 169 総務省：「IoT・5G セキュリティ総合対策 プログレスレポート 2020」の公表 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00068.html〔2021/4/28 確認〕
※ 170 総務省：「IoT・5G セキュリティ総合対策 2020（案）」に対する意見募集の結果及び「IoT・5G セキュリティ総合対策 2020」の公表 https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00126.html〔2021/4/28 確認〕
※ 171 総務省：「電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第２版）」（案）についての意見募集の結果及びガイドラインの公表 https://www.soumu.go.jp/menu_news/s-news/01kiban05_02000209.html〔2021/4/28 確認〕
※ 172 IPA：脆弱性対処に向けた製品開発者向けガイド https://www.ipa.go.jp/security/vuln/report/notice/guideforvendor.html〔2021/4/28 確認〕
※ 173 https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTCommonReq_2021_v1.0_jpn.pdf〔2021/4/28 確認〕
※ 174 https://www.ccds.or.jp/public/document/other/CCDS_IoT 機器セキュリティ実装ガイドライン（ソフトウェア更新機能）_v1.0.pdf〔2021/4/28 確認〕
※ 175 JSSEC:『IoT セキュリティチェックシート』および、『IoT 利用アンケート』 https://www.jssec.org/iot〔2021/4/28 確認〕
※ 176 NIST：NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers https://csrc.nist.gov/publications/detail/nistir/8259/final〔2021/4/28 確認〕
※ 177 NIST：NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline https://csrc.nist.gov/publications/detail/nistir/8259a/final〔2021/4/28 確認〕
※ 178 NIST：Draft NIST Special Publication 800-213: IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements https://csrc.nist.gov/publications/detail/sp/800-213/draft〔2021/4/28 確認〕
※ 179 NIST：Draft NISTIR 8259B: IoT Non-Technical Supporting Capability Core Baseline https://csrc.nist.gov/publications/detail/nistir/8259b/draft〔2021/4/28 確認〕
※ 180 NIST：Draft NISTIR 8259C: Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline https://csrc.nist.gov/publications/detail/nistir/8259c/draft〔2021/4/28 確認〕
※ 181 NIST：Draft NISTIR 8259D: Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government https://csrc.nist.gov/publications/detail/nistir/8259d/draft〔2021/4/28 確認〕
※ 182 ENISA：Guidelines for Securing the Internet of Things https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things〔2021/4/28 確認〕
※ 183 ENISA：Cybersecurity Stocktaking in the CAM https://www.enisa.europa.eu/publications/cybersecurity-stocktaking-in-the-cam〔2021/4/28 確認〕
※ 184 ETSI：ETSI TS 303 645 v2.1.1 (2020-06): CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf〔2021/4/28 確認〕
※ 185 https://japan-telework.or.jp/tw_about/〔2021/6/8 確認〕
※ 186 従来は「テレコミューティング（telecommuting）」（遠隔通勤）という用語が用いられた。1973 年、米物理学者で当時、米航空宇宙局（NASA）の複雑な通信システム作業を自宅から行っていた Jack Nilles 氏が自身の勤務体制を「テレコミューティング（telecommuting）」と表現したのが始まりである。
※ 187 日本テレワーク学会：NECにおけるテレコミューティングへの取り組み http://www.telework-gakkai.jp/archive/IFF/newsletter-j/V3N10/nec.html〔2021/5/25 確認〕
※ 188 https://japan-telework.or.jp/tw_about/tw_effect/〔2021/6/8 確認〕
※ 189 総務省：令和元年通信利用動向調査の結果（概要） https://www.soumu.go.jp/main_content/000689455.pdf〔2021/5/25 確認〕
※ 190 https://corona.go.jp/news/pdf/kinkyujitai_sengen_0407.pdf〔2021/5/25 確認〕
※ 191 https://corona.go.jp/news/pdf/kinkyujitaisengen_gaiyou0525.pdf〔2021/5/25 確認〕
※ 192 内閣官房：新型コロナウイルス感染症緊急事態宣言・まん延防止等重点措置 https://corona.go.jp/emergency/〔2021/5/25 確認〕
※ 193 https://www.ipa.go.jp/security/fy2020/reports/scrm/index-final.html〔2021/5/25 確認〕
※ 194 日本経済新聞：パソコン供給追いつかず 在宅勤務で需要増 中国に生産偏り、部品調達遅れ https://www.nikkei.com/article/DGKKZO57950540Q0A410C2TJC000/〔2021/5/25 確認〕
日経クロステック：5700 人テレワークで VPN のリソース不足に直面、東京ガスの講じた混雑解消策 https://xtech.nikkei.com/atcl/nxt/column/18/01298/060200008/〔2021/5/25 確認〕
ITmedia NEWS：社内システム使えず「テレワークできない」→ 4000 人が VPN 同時接続 シオノギ製薬グループの“激動の５日間” https://www.itmedia.co.jp/news/articles/2009/23/news043.html〔2021/5/25 確認〕
株式会社アシスト：情報システム担当者の奮闘記～新型コロナで全社員がテレワークへ移行。緊急対応で学んだ危機管理～ https://www.ashisuto.co.jp/pr_blog/article/1211682_5736.html〔2021/5/25 確認〕
※ 195 厚生労働省：政府のテレワークへの取り組み https://telework.mhlw.go.jp/telework/gvm/〔2021/5/25 確認〕
※ 196 https://telework.soumu.go.jp/〔2021/5/25 確認〕
※ 197 https://telework.mhlw.go.jp/〔2021/5/25 確認〕
※ 198 https://www.soumu.go.jp/main_content/000545372.pdf〔2021/5/25 確認〕
※ 199 https://www.mhlw.go.jp/content/11911500/000690830.pdf〔2021/6/8 確認〕
※ 200 https://www.mhlw.go.jp/file/06-Seisakujouhou-11900000-Koyoukintoujidoukateikyoku/0000198641_1.pdf〔2021/5/25 確認〕
※ 201 https://www.nisc.go.jp/security-site/telework/index.html〔2021/5/25 確認〕
※ 202 総務省：テレワークにおけるセキュリティ確保 https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/〔2021/6/8 確認〕
※ 203 https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/teleworkqa_20200507.pdf〔2021/5/25 確認〕
※ 204 https://www.tw-sodan.jp/dl_pdf/16.pdf〔2021/5/25 確認〕
※ 205 https://www.mhlw.go.jp/content/000759469.pdf〔2021/6/8 確認〕
※ 206 IPA：テレワークを行う際のセキュリティ上の注意事項 https://www.ipa.go.jp/security/announce/telework.html〔2021/5/25 確認〕
※ 207 IPA：Web 会議サービスを使用する際のセキュリティ上の注意事項 https://www.ipa.go.jp/security/announce/webmeeting.html〔2021/5/25 確認〕
※ 208 https://japan-telework.or.jp/suguwakaru/guide/〔2021/5/25 確認〕
※ 209 IPA：Zoom の脆弱性対策について https://www.ipa.go.jp/security/ciadr/vul/alert20200403.html〔2021/5/25 確認〕
※ 210 NEC ネッツエスアイ株式会社：「Zoom-Bombing」と呼ばれる事象への対処方法について https://symphonict.nesic.co.jp/zoom/update-all/notification-002/〔2021/5/25 確認〕
※ 211 piyolog：警察庁内端末不正アクセスと５万件の脆弱な VPN ホストの公開についてまとめてみた https://piyolog.hatenadiary.jp/entry/2020/11/30/063636〔2021/5/25 確認〕
※ 212 JPCERT/CC：複数の SSL VPN 製品の脆弱性に関する注意喚起 https://www.jpcert.or.jp/at/2019/at190033.html〔2021/5/25 確認〕
※ 213 Pulse Security, LLC.：SA44784 - 2021-04: Out-of-Cycle Advisory: Multiple Vulnerabilities Resolved in Pulse Connect Secure 9.1R11.4 https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784〔2021/5/25 確認〕
※ 214 三菱重工業株式会社：当社グループ名古屋地区のネットワークに対する第三者からの不正アクセスに係る件 https://www.mhi.com/jp/notice/notice_200807.html〔2021/5/25 確認〕
※ 215 サービス & セキュリティ株式会社：新型コロナウイルスに便乗したフィッシング https://www.ssk-kan.co.jp/topics/?p=10717〔2021/5/25 確認〕
※ 216 ISO：ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection https://www.iso.org/committee/45306.html〔2021/6/7 確認〕
※ 217 https://www.nist.gov/〔2021/6/7 確認〕

※ 218 NIST：CYBERSECURITY FRAMEWORK　https://www.nist.gov/cyberframework〔2021/6/7 確認〕
※ 219 経済産業省：サイバーセキュリティ経営ガイドライン　https://www.meti.go.jp/policy/netsecurity/mng_guide.html〔2021/6/7 確認〕
※ 220 経済産業省：サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を策定しました　https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html〔2021/6/7 確認〕
※ 221 NIST：SP 800-160 Vol. 1 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems　https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final〔2021/6/7 確認〕
※ 222 NIST：Work with NIST　https://www.nist.gov/about-nist/work-nist〔2021/6/7 確認〕
※ 223 NIST：National Cybersecurity Center of Excellence　https://www.nccoe.nist.gov〔2021/6/7 確認〕
※ 224 NIST：Validating the Integrity of Computing Devices　https://www.nccoe.nist.gov/sites/default/files/library/sp1800/nist-sp1800-34a-tpm-sca-preliminary-draft.pdf〔2021/6/7 確認〕
※ 225 MITRE 社：We operate FFRDCs　https://www.mitre.org/centers/we-operate-ffrdcs〔2021/6/7 確認〕
※ 226 MITRE 社：MITRE ATT&CK　https://attack.mitre.org/〔2021/6/7 確認〕
※ 227 NIST：Post-Quantum Cryptography　https://csrc.nist.gov/projects/post-quantum-cryptography〔2021/6/7 確認〕
※ 228 NIST：FIPS 199 Standards for Security Categorization of Federal Information and Information Systems　https://csrc.nist.gov/publications/detail/fips/199/final〔2021/6/7 確認〕
NIST：FIPS 200 Minimum Security Requirements for Federal Information and Information Systems　https://csrc.nist.gov/publications/detail/fips/200/final〔2021/6/7 確認〕
※ 229 NIST:FIPS 201-3 (Draft) Personal Identity Verification (PIV) of Federal Employees and Contractors　https://csrc.nist.gov/publications/detail/fips/201/3/draft〔2021/6/7 確認〕
※ 230 NIST CSRC:Publications　https://csrc.nist.gov/publications〔2021/6/7 確認〕
※ 231 CONGRESS.GOV：H.R.1668 - IoT Cybersecurity Improvement Act of 2020　https://www.congress.gov/bill/116th-congress/house-bill/1668〔2021/6/7 確認〕
※ 232 NIST：Rounding Up Your IoT Security Requirements：Draft NIST Guidance for Federal Agencies　https://www.nist.gov/blogs/cybersecurity-insights/rounding-your-iot-security-requirements-draft-nist-guidance-federal〔2021/6/7 確認〕
※ 233 NIST：NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)　https://www.nist.gov/itl/applied-cybersecurity/nice〔2021/6/7 確認〕
※ 234 NIST：SP 800-55 Rev. 2 (Draft) PRE-DRAFT Call for Comments: Performance Measurement Guide for Information Security　https://csrc.nist.gov/publications/detail/sp/800-55/rev-2/draft〔2021/6/7 確認〕
※ 235 Federal Register：Maintaining American Leadership in Artificial Intelligence　https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence〔2021/6/7 確認〕
※ 236 https://www.ismap.go.jp/〔2021/6/7 確認〕
※ 237 2020 年に入り、DoD は調達事業者に対して、サイバーセキュリティ成熟度モデル認証（CMMC：Cyber security Maturity Model Certificate）への対応を義務化することを検討している。これによって SP 800-171 への対応が無用になることはないが、国内の防衛産業は CMMC にも注意が必要となる。CMMC 運用の動向については「2.2.2 米国の政策」を参照されたい。
※ 238 IPA：セキュリティ関連 NIST 文書　https://www.ipa.go.jp/security/publications/nist/〔2021/6/7 確認〕
※ 239 NIST：NATIONAL VULNERABILITY DATABASE　https://nvd.nist.gov/vuln〔2021/6/7 確認〕
※ 240 https://cyber-risk.or.jp/〔2021/6/7 確認〕
発表当時の団体名は「産業横断サイバーセキュリティ人材育成検討会」である。
※ 241 NIST：Success Story: Japanese Cross-Sector Forum　https://www.nist.gov/cyberframework/success-stories/japanese-cross-sector-forum〔2021/6/7 確認〕