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2章
情報セキュリティを支える基盤の動向

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

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

2.1 国内の情報セキュリティ政策の状況

本節では、政府が推進する情報セキュリティ対策の状況を述べる。

2.1.1 政府全体の政策動向

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

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

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

(1) 次期「サイバーセキュリティ戦略」の検討

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

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

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

(2) 「サイバーセキュリティ 2020」の主な取り組み状況

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

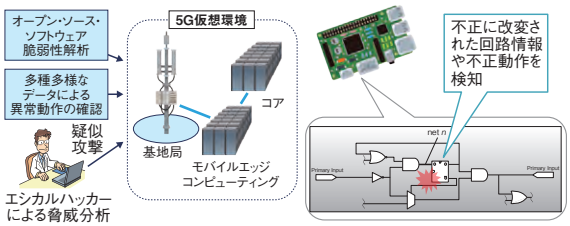
れた事業の継続や策定された指針・ガイドライン等の普及が計画された。以下、2018 年戦略の目的達成の施策として示されている四つの観点について、サイバーセキュリティ 2020 の計画に基づき実施された取り組みの中から注目すべきものを取り挙げる。

- 経済社会の活力の向上及び持続的発展

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

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

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



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

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

- 国民が安全で安心して暮らせる社会の実現

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

- 国際社会の平和・安定及び我が国の安全保障への寄与

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

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

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

名が参加した※15。

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

- 横断的政策

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

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

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

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

(3) 重要インフラの情報セキュリティ対策強化

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

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

なお、第5次行動計画は2022年内に決定されるものと見られる※25。

以下、2020年度における主な活動について述べる。

(a) 重要インフラ専門調査会における取り組み

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

(b)「分野横断的演習」の実施

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

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

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

(4) デジタル庁の設置

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

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

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

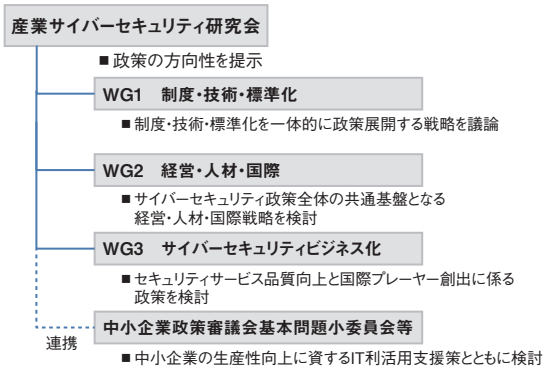
今後、デジタル庁設置に関しては、サイバーセキュリティ面での検証や議論も本格化するものと見られる。

2.1.2 経済産業省の政策

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

(1) 産業サイバーセキュリティ研究会

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



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

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

- サプライチェーンサイバーセキュリティ強化パッケージ

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

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

(a) WG1(制度・技術・標準化)

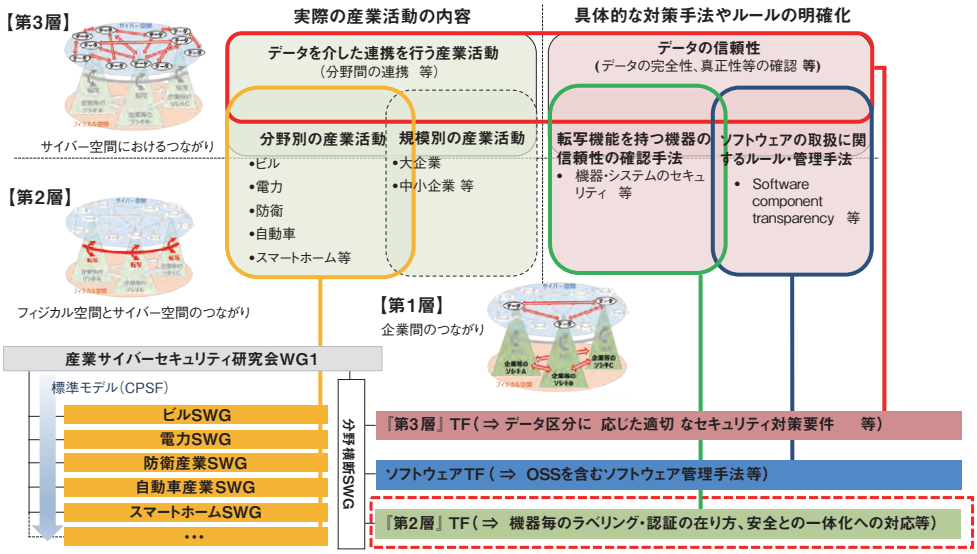
「サプライチェーンサイバーセキュリティ強化パッケージ」の活動を主に実施する WG1 では、産業サイバーセキュリティに関する制度・技術・標準化を一体として政策に展開する戦略を議論している。その前提として、サイバー空間とフィジカル空間の融合により、柔軟かつ動的なサプライチェーンが生まれるとし、これを価値創造過程(バリュークリエイションプロセス)と定義した。また、バリュークリエイションプロセス全体の業界横断的な標準モデルである「サイバー・フィジカル・セキュリティ対策フレームワーク※42(The Cyber/Physical Security Framework)Version 1.0」(以下、CPSF)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

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

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

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

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



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

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

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

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

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

(b) WG2（経営・人材・国際）

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

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

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

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

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

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

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

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

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

(c) WG3（サイバーセキュリティビジネス化）

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

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

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

(2) その他の検討会等における活動

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

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

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

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

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

（3）技術等情報管理認証制度の開始

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

（4）情報セキュリティサービス審査登録制度

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

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

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

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

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

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

（5）J-CSIP（サイバー情報共有イニシアティブ）

経済産業省の協力のもと、IPAでは2011年10月から、官民連携による標的型攻撃への対策を目的として、J-CSIP（Initiative for Cyber Security Information Sharing Partnership of Japan：サイバー情報共有イニシアティブ）を運用している。

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

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

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

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

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

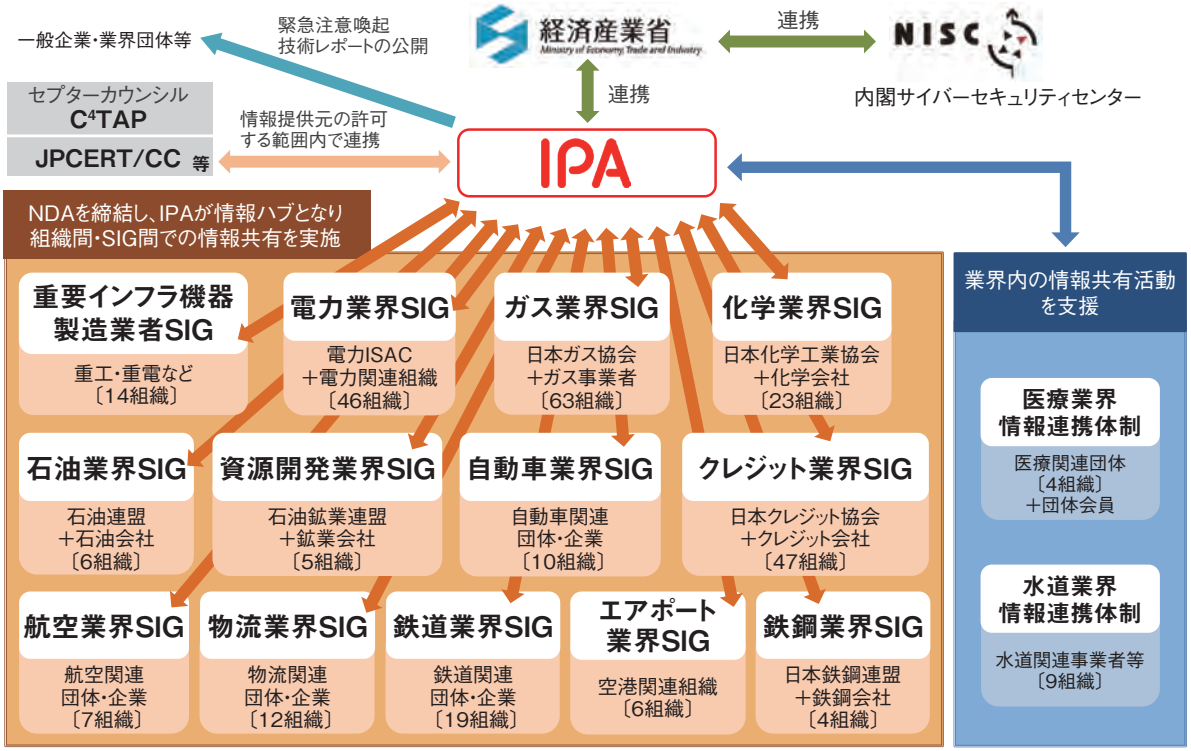
参加組織から提供された、不審なメール、ウイルス※80、攻撃の痕跡等の件数（情報提供件数）、提供を受けた情報のうち標的型攻撃メールと見なした件数（攻撃メール件数）、及びそれらを基に J-CSIP 内で情報共有を行った件数（情報共有件数）を表 2-1-1 に示す。年度により件数の増減はあるものの、継続して情報提供や共有が行われていることが分かる。

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

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

■表 2-1-1　J-CSIP の運用実績

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



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

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

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

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

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

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

(6) J-CRAT（サイバーレスキュー隊）

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

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

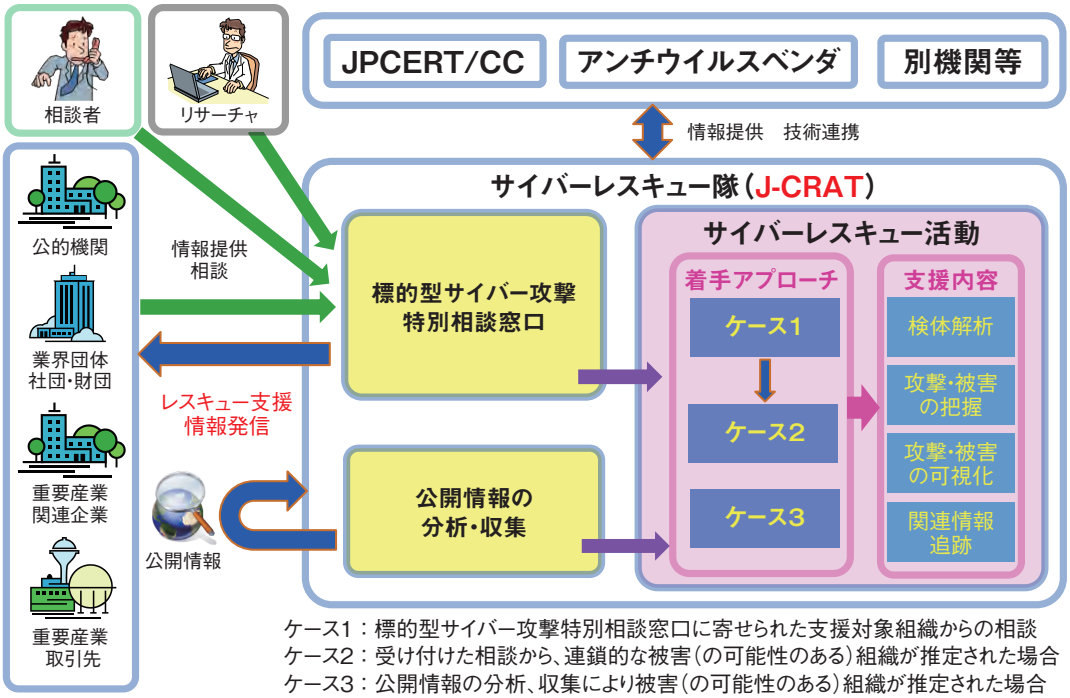
J-CRAT では、常時「標的型サイバー攻撃特別相談窓口」（以下、窓口）の運営と「公開情報の分析・収集」の二つの活動を実施している。

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

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

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

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



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

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

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

■表 2-1-2　J-CRAT の活動実績

2.1.3 総務省の政策

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

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

(1)「IoT・5G セキュリティ総合対策 2020」の概要

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

(a) クラウドのセキュリティ対策強化

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

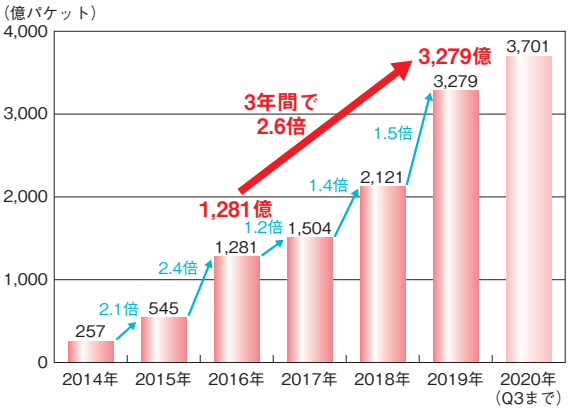
テレワーク中の情報共有や Web 会議システムの利用のため、クラウドサービスの利用も増加した※87。総合対策 2020 では、今後も組織における情報システムの構築や運用においてクラウドサービスの活用が進むことを指摘している。政府においても「政府情報システムにおけるクラウドサービスの利用に係る基本方針※88」を定め、情報システム調達に際しては、コスト削減や柔軟なリソースの増減等の観点から、クラウドサービスの利用を第一候補として検討を行う旨の方向性が示されている。

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

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

(b) IoT のセキュリティ対策

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



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

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

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

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

(c) 5G の本格開始に伴うセキュリティ対策の強化

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

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

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

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

(d)研究開発や人材育成等の横断的施策

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

- 研究開発の推進

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

- 人材育成オープンプラットフォームの構築

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

- 地域のセキュリティ人材育成

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

- 国際連携の推進

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

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

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

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

(2) テレワークにおけるセキュリティ確保

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

(a)「テレワークのセキュリティ あんしん無料相談窓口」の開設

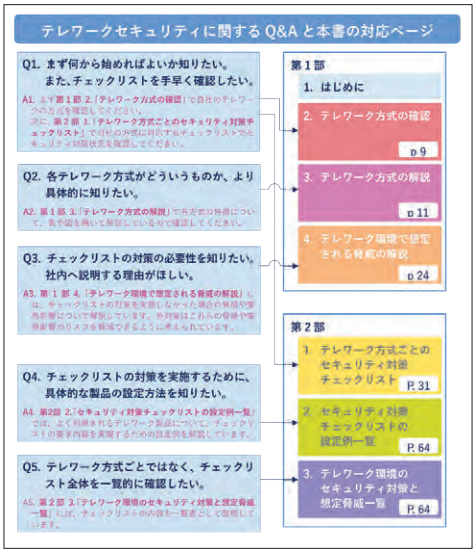
総務省はテレワーク導入の無料相談ができる「テレワークマネージャー派遣事業」（現、テレワークマネージャー相談事業）を2016年8月から実施してきた※104。2020年はテレワークの導入企業が増えたため、テレワークセキュリティについて相談対応体制を強化する目的で、同年7月に「テレワークのセキュリティ あんしん無料相談窓口」を開設した※105。セキュリティに関する不安、具体的なセキュリティ対策方法、ルール作りや自社の実施状況の適切性のコンサルティング等を、セキュリティの専門家がWebオンライン会議等でアドバイスする。

(b)「テレワークセキュリティガイドライン」の改訂

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

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

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

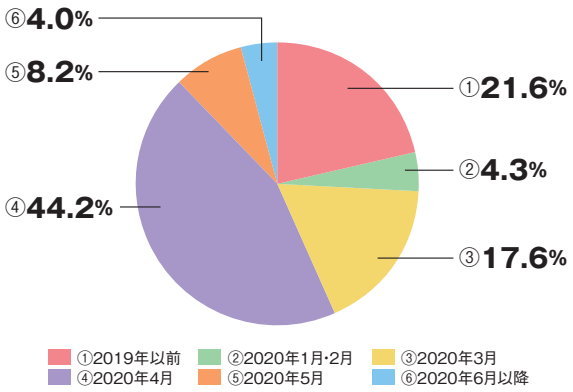


■図2-1-8　テレワークセキュリティに関するQ&Aと対応ページ
（出典）総務省「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（初版）」

(d)「テレワークセキュリティに係る実態調査」の実施

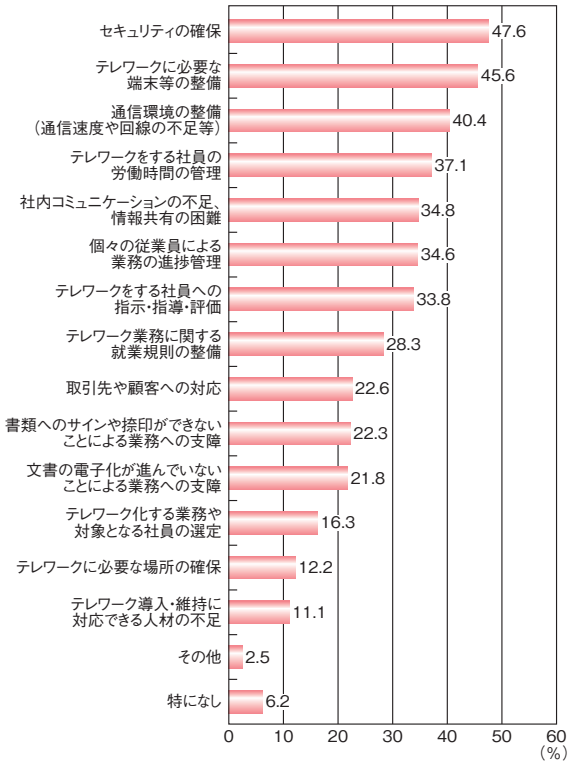
総務省は、2020年7～8月及び2020年12月～2021年1月の2度にわたり、テレワークを導入する企業等におけるセキュリティ対策状況の実態を把握するため「テレワークセキュリティに係る実態調査」を実施した（以下、それぞれを1次実態調査及び2次実態調査と呼ぶ）※110。1次実態調査の結果によると、テレワーク導入企業の過半が1回目の緊急事態宣言前後（2020年3～4月）に導入していることが分かった（次ページ図2-1-9）。また、テレワークを導入しない理由として、業務都合を除くとセキュリティに関する懸念がトップであった。総務省の「テレワークセキュリティガイドライン」について

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



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

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



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

(3) その他の取り組み

総務省のその他の取り組みについて述べる。

(a) 自治体情報セキュリティ対策

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

(b) トラストサービス制度

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

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

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

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

(c) スマートシティのセキュリティ対策

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

(d) インターネット上の違法・有害情報への対応

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

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

2.1.4 警察によるサイバー犯罪対策

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

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

(1) 警察における主な取り組み

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

(a) サイバー空間の脅威への対応の強化

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

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

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

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

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

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

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

(b) 警察における組織基盤の更なる強化

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

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

(c) 国際連携及び産学官連携の推進

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

また警察での産学官連携の推進については、一般財団法人日本サイバー犯罪対策センター（JC3：Japan Cybercrime Control Center）等と連携し、産学官の情報や知見をサイバー犯罪・サイバー攻撃の取り締り等に活用している。具体的には、総務省を装った偽の特別定額給付金の申請サイトへ誘導するメールに関する注意喚起※139、山形県警察によるサポート詐欺サイトでの被害発生を受けての注意喚起※140、愛知県警察、埼玉県警察によるネットショッピングに関する詐欺サイトの被害防止対策等の活動に取り組んでいる。

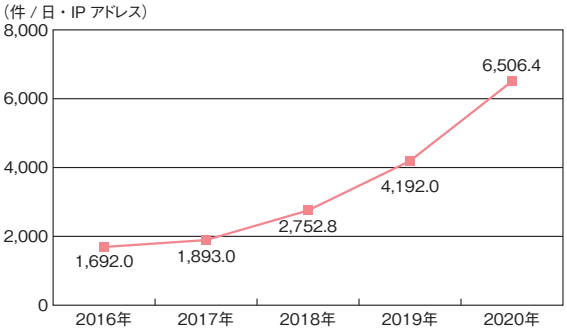
また警察庁のサイバーセキュリティ・情報化審議官主催の私的懇談会として、法務、技術、ITの各分野及びJC3等の官民有識者で構成されるサイバーセキュリティ政策会議が例年開催されている。2020年度の同会議では、警察が、政府全体の力を結集するための施策に安全・安心の観点から積極的・主体的に参画していく必要がある、との提言を含む報告書※141が取りまとめられ、2021年3月、警察庁より公開された。同報告書では「コロナ禍が顕在化させるサイバー空間の新たな脅威」「犯行手口等の悪質化と被害の深刻化」「国家の関与が疑われるサイバー攻撃被害の深刻化」といった生活様式の変化等によるサイバー空間の新たな脅威に対して、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

(2) 2020年のサイバー攻撃の情勢

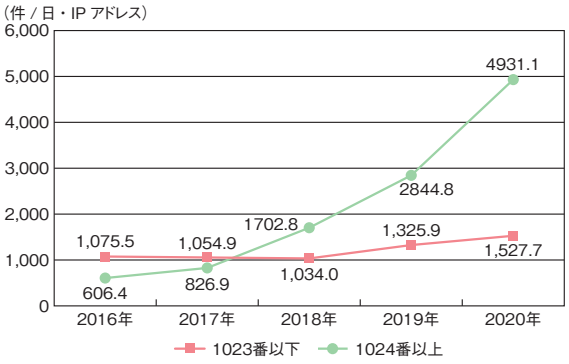
警察が把握する2020年のサイバー攻撃の情勢について述べる。

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

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



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



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

脆弱なIoT 機器とウイルス感染の実態」を参照されたい。

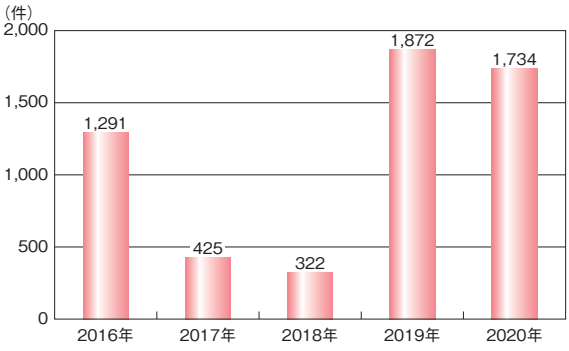
(3) 2020 年のサイバー犯罪の情勢等

警察が 2020 年に認知したサイバー犯罪の情勢等について述べる。

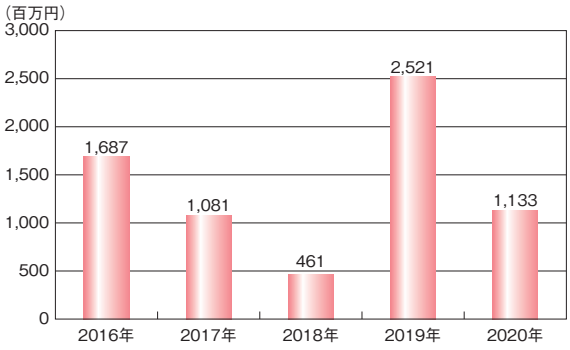
(a) サイバー犯罪の情勢

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

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



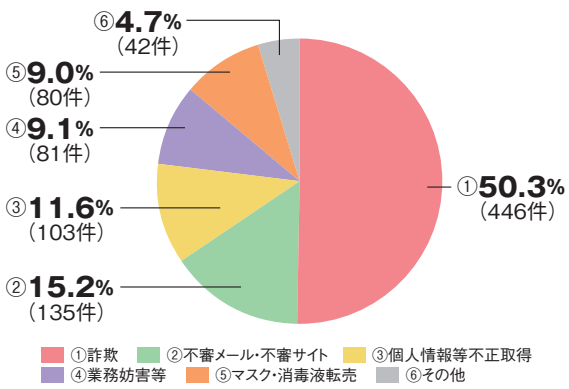
■図 2-1-13　インターネットバンキングに係る不正送金事犯の発生件数の推移
(出典)警察庁「令和２年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集



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

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

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



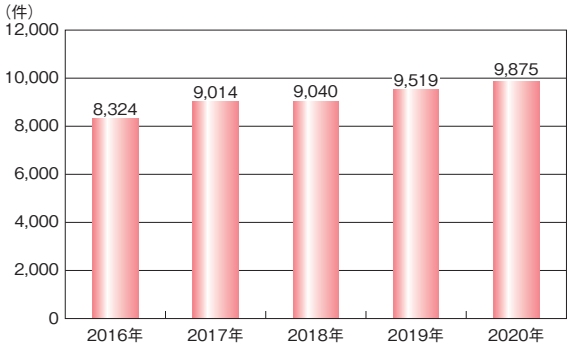
■図 2-1-15　新型コロナウイルスに関連するサイバー犯罪が疑われる事案の報告件数（n=887）
(出典)警察庁「令和２年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

(b) 検挙件数

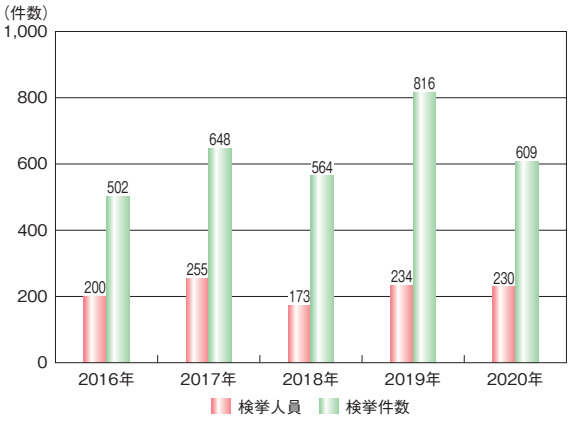
サイバー犯罪の検挙件数と主な事案事例について述べる。警察によれば、サイバー犯罪の検挙件数は増加傾向にあり、2020 年の検挙件数は 9,875 件と過去最多となった（次ページ図 2-1-16）。

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

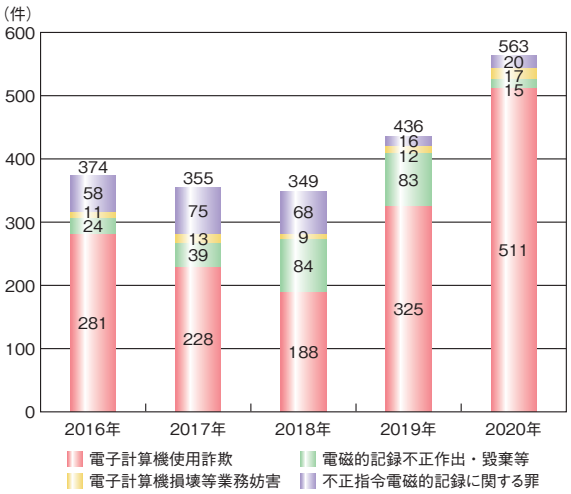
の 436 件を上回り、563 件と過去 5 年間で最多となった。そのうち「電子計算機使用詐欺」が 511 件と最も多く、全体の 90.8% を占めている（図 2-1-18）。



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



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



■図 2-1-18　コンピュータ・電磁的記録対象犯罪の検挙件数の推移
（出典）警察庁「令和 2 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

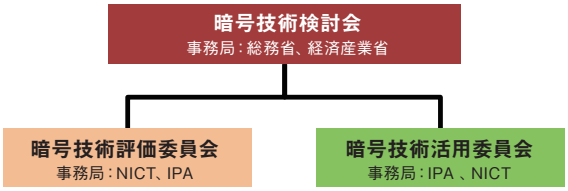
2.1.5 CRYPTRECの動向

電子政府の情報セキュリティを確保するため、総務省と経済産業省、NICT、及び IPA は安全性と実用性に優れた暗号技術を選び出すことを目的に、CRYPTREC（Cryptography Research and Evaluation Committees）を組織している。CRYPTREC では、電子政府システムでの利用を推奨する暗号アルゴリズム（CRYPTREC 暗号リスト※144）の安全性を評価、監視し、暗号技術の適切な実装法や運用法を調査、検討している。

(1) 2020 年度の体制

CRYPTREC は、総務省と経済産業省が運営し、政策的な判断を含む総合的な観点から電子政府の安全性及び信頼性を確保する活動を推進する「暗号技術検討会」、及び NICT と IPA が共同で運営し、主に技術的な評価を実施する委員会とで構成されている。

委員会には、暗号技術の安全性評価を中心とした技術課題を主に担当する「暗号技術評価委員会」と、セキュリティ対策の推進、暗号技術の利用促進に向けた環境整備を主に担当する「暗号技術活用委員会」が設置されている（図 2-1-19）。



■図 2-1-19　CRYPTREC の体制

暗号技術検討会と両委員会の主な役割は以下のとおりである。

- 暗号技術検討会

  CRYPTREC 活動計画の承認、委員会が作成する各種成果物の承認等、政策的な判断を含む総合的な観点から電子政府の安全性及び信頼性を確保する活動を推進する。量子コンピュータが実用化されても安全性が保てると期待される暗号「耐量子計算機暗号（PQC：Post-Quantum Cryptography）」を含む新たな暗号技術の動向等を踏まえ、次期 CRYPTREC 暗号リストに求められる要件や課題等を整理するため、傘下に「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」（以下、暗号の在り方 TF）が設置されている。

- 暗号技術評価委員会
  暗号技術に対する攻撃技術動向の調査や安全性評価等、暗号技術における技術的信頼に関する検討を担当する。傘下には、公開鍵暗号の中長期的な安全性の検証や新世代暗号に係る調査等を行う「暗号技術調査ワーキンググループ」が設置されている。
- 暗号技術活用委員会
  セキュリティ対策の推進、暗号技術の利用促進等に寄与する運用ガイドラインの整備を中心とした、暗号利用に関する課題の検討を担当する。

(2) 2020 年度の主な活動

2020 年度の暗号技術検討会及び各委員会の主な活動内容・成果について以下に述べる。

(a) 暗号技術検討会

2020 年度には、各委員会の 2019 年度活動報告、2020 年度活動計画、及び 2020 年度の活動報告の審議が行われ、承認された。

また、CRYPTREC 暗号リスト改定に向けた暗号の在り方 TF での検討内容が報告され※145、承認された。具体的には、検討継続課題となっていた CRYPTREC 暗号リストの取り扱いについて、以下のとおりの結論となった。

- CRYPTREC 暗号リストの構成は変更しない（「電子政府推奨暗号リスト」「推奨候補暗号リスト」「運用監視暗号リスト」の 3 リスト構成を維持する）。
- リスト間の移行ルールを整理し、特に「推奨候補暗号リスト」からの削除条件を明確化した。その条件とは、「安全性維持が困難（危殆化した）と判断した場合」と「CRYPTREC 暗号リスト（旧電子政府推奨暗号リストを含む）への掲載から 20 年を超えた後に実施する最初の利用実績調査までに、十分な利用実績を確認できなかった場合」であり、どちらかの条件に該当した場合に「推奨候補暗号リスト」から削除されることとなった。

(b) 暗号技術評価委員会

CRYPTREC 暗号リストに掲載されている暗号技術の安全性と実装性に関わる監視活動のほか、2020 年度の主な活動内容・成果は以下のとおりである。

- EdDSA の安全性評価
  TLS1.3 で採用され、次期米国政府標準デジタル署名方式（FIPS 186-5）でも追加予定となっている新しいデジタル署名 EdDSA※146 について、今後の利用拡大が見込まれることから、CRYPTREC 暗号リスト（推奨候補暗号リスト）への追加を視野に入れ、安全性評価を行った。その結果、EdDSA の曲線（Ed25519 と Ed448）及び方式の構成いずれについても安全性に問題は見つからなかったことから、引き続き、実装性能評価を行うこととなった。
- 暗号技術調査ワーキンググループの活動
  最近進展が著しい量子コンピュータによる暗号技術の安全性への懸念が提起されているため、2020 年度は、PQC を導入するための技術に関する動向、及び Shor の量子アルゴリズム※147 による現代暗号への脅威に関する調査を行った。本調査で注目すべきことは、「現状の量子コンピュータでは暗号で用いる程大きなパラメータの合成数を素因数分解することは困難であり、量子ビット数やゲート計算のエラー率等量子コンピュータの性能の大幅な向上がない限りは現代暗号の脅威にはならないと考えることができる」との見解をまとめたことである。また、主要な公開鍵暗号（RSA 暗号、楕円曲線暗号）の安全性の根拠となる「素因数分解問題」と「離散対数問題」の困難性に関して、CRYPTREC が公開している「予測図」の改訂も行った※146。

(c) 暗号技術活用委員会

2020 年度には、安全な暗号利用に関する運用ガイドラインを整備する観点から、「暗号鍵管理システム設計指針（基本編）※148」及び「TLS 暗号設定ガイドライン※149」を 2020 年 7 月に公開した。以下に概要を紹介する。

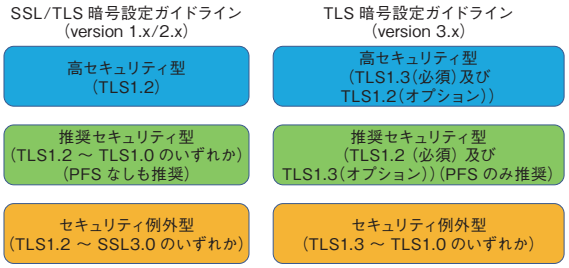
- 暗号鍵管理システム設計指針（基本編）
  本設計指針は、暗号鍵管理の必要性を認識するための「暗号鍵管理の在り方」についての解説部分と、鍵管理ガイドラインである NIST SP800-130 の解説書・利用手引書として活用できる「暗号鍵管理についての技術的内容」を取りまとめた部分とで構成される。具体的には、解説部分では暗号鍵管理の考え方や枠組み、暗号鍵管理において重要な「時間管理」の概念を説明している。
  また、技術的内容では、暗号鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき事項一覧（Framework Requirements）として NIST SP800-130 の内容を再整理して、暗号鍵管理システムのプロファイルや設計仕様書、運用マニュアル等の中で明示的に記載すべき要求事項を示している。
  ただし、本設計指針では具体的な特定のセキュリティ

機能の採用を義務付けていない。そのため、どのようにそれらの要求事項に対応するかは設計者や運用責任者に委ねられ、それらの対応方針をプロファイルや設計仕様書、運用マニュアル等に記載する必要がある。そこで、2021 年度以降、それらの作業を支援するためのプロファイル等の作成マニュアルを準備する計画である。まずは作成方法を整理する作業から始め、2022 年度に完成させる予定である。

- TLS 暗号設定ガイドライン

  本ガイドラインは、サーバの構築者･管理者向けにサーバでの適切な TLS 暗号設定方法を解説したもので、SSL/TLS 通信の規格化や技術環境の変化に対応するため、TLS1.3 の採用や SSL3.0 の禁止に伴って一段高い安全性を求める等、従来の暗号設定ガイドラインから全面的に内容を見直したものである（図 2-1-20）。2020 年 3 月時点における、TLS 通信で実現すべき安全性と、必要となる相互接続性とのバランスを考慮した三つの設定基準を提示している。また、これまでの必ず満たさなければならない「遵守項目」に加え、より良い安全性を実現するために満たすことが望ましい「推奨項目」を追加することで、より現実的かつ実効性･柔軟性が高い要求設定を可能にしている（表 2-1-3）。

また、今まで CRYPTREC 暗号リストに掲載されたアルゴリズムや鍵長の選定方法についてのガイダンスがなかったため、新たな取り組みとして、「鍵長設定要件（仮）」と「鍵長設定ガイダンス（仮）（一般用）」を作成することとし、作成方針を取りまとめた。これらのガイダンスは、2021 年度末に完成させる予定である。



■図 2-1-20　従来の暗号設定ガイドラインとの比較

要求設定	遵守項目	プロトコルバージョン	利用禁止プロトコルバージョンを利用不可にする設定
		サーバ証明書	利用する暗号アルゴリズムと鍵長の設定
			発行・更新時の鍵情報の生成方法の明確化
			警告表示の回避方法の明確化
		暗号スイート	利用禁止暗号アルゴリズムを利用不可にする設定
			公開鍵暗号の鍵長の設定
	推奨項目	プロトコルバージョン	利用プロトコルバージョンの優先順位付け
		暗号スイート	利用推奨暗号アルゴリズムのみでの設定
			推奨暗号スイートの優先順位付け

■表 2-1-3　要求設定における遵守項目と推奨項目

COLUMN

暗号の安全性を最終的に決めるものは？　ー各国の暗号政策調査からー

「暗号の安全性」といったとき、どんなことを思い浮かべますか？　この質問に対して、多くの場合は、「暗号アルゴリズムの安全性」を前提に話がされるのではないでしょうか。例えば、この暗号は安全である、今の公開鍵暗号は量子コンピュータで簡単に解読される、量子暗号は解読不可能な究極の暗号である、等々。

このこと自体は間違いではないのですが、注意する必要があるのは、システム全体から見れば、暗号アルゴリズムはあくまでも暗号処理を行うツールであって、「暗号システムの安全性」について何ら言及するものではない、ということです。もちろん、暗号アルゴリズム自体の安全性に問題があれば暗号システムの安全性にも直接的な悪影響を及ぼします。ところがその逆は成り立たず、暗号アルゴリズムが安全だからといって暗号システムが安全であるかどうかは分かりません。

では、暗号アルゴリズムの安全性以外に暗号システムの安全性に影響を与えるものにどんなものがあるでしょうか？　これには、暗号鍵の管理、ユーザに対する認証と権限管理、脆弱性がない製品の利用等といったものが考えられます。これら暗号システムの安全性に影響を与えるものの中には、相反する要求が出されることもあります。例えば、通信経路上を完全に暗号化する End-To-End 暗号化。確かに、ネットワークサービスの安全性確保や個人のプライバシー保護のことを考えれば End-To-End 暗号化は望ましい対策です。しかし一方で、内部不正による情報持出やサイバー攻撃による情報漏えい、ウイルスの流入等を管理部門がチェックできないということにつながることを考慮するなら End-To-End 暗号化はむしろ望ましくない対策であると言うこともできます。

つまり、暗号システムの安全性は、技術だけで決まるものではなく、暗号を使って何を達成したいのか、相反する要求をどのように調整するのかという「ポリシー」に大きく依存することになります。

実際、これが国家として（とりわけ、安全保障や重要インフラ保護、治安に関わるケース）の話となるとより鮮明に表れてきます。そのことを確かめるために、IPA では、米国、英国、フランス、ドイツ、エストニア、ロシア、中国、韓国、オーストラリア、EU の暗号に関わるセキュリティ政策に関する実施体制、法制度及び認証制度についての最新動向調査を実施してみました。

この調査で確認できたことは、これらの国々では国家における暗号に関わるセキュリティ政策に関する組織の指示・責任担当が一元化され、トップダウン型の強い権限が与えられていること、しかも近年その権限が強化されつつあることでした。例えば、中国では暗号法（2020年 1 月施行）を根拠法として、共産党中央委員会下に国家暗号管理局を設置しています。こうした、国家としての方針の徹底が図られているあたりは、暗号アルゴリズムと暗号システムの違いをよく理解していると感じられます。

なお、この調査報告書は以下の URL から入手できます。

https://www.ipa.go.jp/security/fy2021/reports/crypto_survey/index.html

2.2 国外の情報セキュリティ政策の状況

サイバー脅威・サイバー犯罪は国境を問わず、あらゆる国・地域の脆弱性を突き、ターゲットに攻撃を仕掛けてくる。また、IT 化した社会サービスやそれを支えるサプライチェーンは国境を越えてつながり合い、他国におけるサイバー脅威が自国に深刻な影響を与える可能性がある。更に近年、国家の支援を受けた攻撃者による他国へのサイバー脅威が現実になりつつある。こうした状況に国や地域が単独で対処することは難しく、国際連携が不可避である。本節では、国際連携に向けた状況理解のために、各国・各地域における情報セキュリティ政策について述べる。

2.2.1 国際社会と連携した取り組み

2019 年度に引き続き、日本政府は 2020 年度も米国、欧州、インド、ASEAN 諸国等とのサイバーセキュリティに関する連携協議や演習を実施した。それらの活動から主な取り組みを紹介する。2020 年度の全体的な傾向として、新型コロナウイルス感染拡大対策に関する国際連携が最重要課題となり、サイバーセキュリティに関する連携は現状維持とし、討議は縮小されたものが多い。

(1) 各国首脳・国際機関との連携

新型コロナウイルス感染は 2020 年 1 月以降世界的に広まり、中国、米国、欧州等各国で緊急事態が宣言された。これに伴い、2020 年 3 月 24 日、安倍晋三首相は東京 2020 オリンピック・パラリンピック競技大会の 1 年延期を Thomas Bach 国際オリンピック委員会（IOC：International Olympic Committee）会長と合意した、と発表した※150。この結果オリンピック大会は 2021 年 7 月 23 日開幕、パラリンピック大会は同年 8 月 24 日開幕と延期が決定した。

上記のように世界的な大規模イベント開催は延期等が相次ぎ、イベント対応のセキュリティ対策連携は継続の形になった。また各国首脳会談の多くもオンライン開催となり、政策課題については新型コロナウイルス対策が優先され、サイバーセキュリティに関する協議は安全保障等、限定的なものであった。

(a) G7 首脳会合・外相会合

G7 首脳は、新型コロナウイルス感染拡大への対処を協議すべく、2020 年 3 月 16 日、4 月 16 日にテレビ会議を行った。このうち 3 月 16 日の会議では、首脳声明として、新型コロナウイルス感染拡大対策の加速化、新型コロナウイルス流行の経済的影響への対応、経済成長を回復させることを表明した※151。また安倍首相は東京 2020 オリンピック・パラリンピック競技大会について、人類が新型コロナウイルスに打ち勝った証として完全な形で実施したいと述べ、各国の支持を得た。同会議に続き 3 月 25 日、G7 外相会合もオンラインで行われ、外務大臣間での連携が確認された。同会合では地域情勢も議論され、茂木敏充外務大臣は北朝鮮の弾道ミサイル発射実験等への抗議と各国の緊密な連携を呼びかけた※152。更に 4 月 16 日の G7 首脳テレビ会議では、各国の新型コロナウイルス感染拡大対策の取り組みが討議された。安倍首相は 4 月 7 日に発表した緊急事態宣言※153 と経済対策の紹介に加え、治療薬の開発、医療体制の脆弱な国の支援、情報の共有、世界の新型感染症予防体制の強化等を訴え、各国首脳の賛同を得た。

2020 年 8 月に予定されていた G7 米国サミットは、新型コロナウイルス感染拡大対応と米国大統領選挙によりいったん 11 月に延期されたが、開催が見送られた。G7 サミットでは例年、自由でオープンなサイバー空間の維持に関連する合意文書が出され、2019 年 8 月のフランス・ビアリッツサミットでは「開かれた自由で安全なデジタル化による変革のための戦略」が発表された※154 が、2020 年度はこの合意についても見送られた。

(b) 日米豪印外相会合

G7 の枠組みとは別に、2019 年以降、日米豪印（インド）4 ヵ国による協議が重ねられている。中国の東シナ海・南シナ海・インド洋への進出政策が各国共通の重要課題となっており、連携を強化する狙いがあると思われる。

2020 年 10 月 6 日、第 2 回日米豪印外相会合が東京で開催され、茂木外務大臣、Mike Pompeo 米国国務長官（Secretary of State of the United States）、Marise Payne オーストラリア連邦外務大臣（Minister for Foreign Affairs of the Commonwealth of Australia）、Subrahmanyam Jaishankar インド外務大臣（External Affairs Minister of India）が出席した※155。同会合でも新型コロナウイルス感染拡大対策での連携が確認されたほか、主要議題であるインド太平

洋地域の安全保障については、「自由で開かれたインド太平洋」ビジョンの重要性を再確認し、実現に向けた連携を広げること、特に「インド太平洋に関するASEANアウトルック※156」を通じてASEAN地域を支援すること、同ビジョン推進のために海洋安全保障、テロ対策、サイバーセキュリティ、人道・災害支援、人材教育等多方面で協力することで合意した。

更に2021年2月18日、米国Joe Biden大統領就任を受けた形で日米豪印外相電話会談が行われ、米国からはAntony Blinken国務長官が参加した※157。同会談では各国の実務レベルの協議・協力の進展を歓迎し、ASEAN、欧州との連携推進を確認したほか、茂木外務大臣からミャンマー情勢や中国海警法※158の成立に対する深刻な懸念が示され、力による現状変更の試みに対して強く反対することで合意した。

(c)国連によるサイバー脅威対策推進

国際連合(以下、国連)のサイバーセキュリティに関する国連オープン・エンド作業部会(OEWG:Open-ended Working Group)は、2018年12月の第73回国連総会決議(A/RES/73/27)に基づき、国際安全保障の文脈における情報、及び電気通信分野の発展に関して国連全加盟国が参加可能な議論の場として、2019年に設置された部会である※159。同年9月に第1回会合を開催して以来、サイバー空間における脅威認識、規範、国際法の適用、信頼醸成、能力構築等について検討が続けられ、日本もメンバーとして貢献してきた。2021年3月8～12日にOEWGの最終会合が開催され、検討成果の報告書が採択された※13。2021年の第75回国連総会に提出される見通しである。

同報告書はサイバー空間における脅威認識、責任ある国家の行動規範、サイバー空間で国際法がどのように適用されるか、信頼醸成、能力構築等について国連加盟国の共通認識を示し、サイバー空間の紛争防止・解決における国際法の適用を改めて確認したものである※160。承認されれば、サイバー空間上の紛争の抑止に一定の効力を持つことが期待される。

(2)2国間連携の取り組み

2019年度まで例年開催されてきた2国間のサイバー対話は、2020年4月以降、以下に示す日英サイバー対話以外ほとんど開催されていない(2021年4月現在)。以下ではスコープを広げ、日米安全保障協議委員会、日米首脳会談、日EU首脳テレビ会議についても紹介する。

(a)日英サイバー協議

2021年1月31日、東京において第5回日英サイバー協議が開催された※161。日本からは赤堀毅外務省総合外交政策局参事官兼サイバー政策担当大使を始めとする関係機関の代表者が、英国からはAlexander Evance外務省サイバー政策部長(Director Cyber, National Security Directorate, Foreign and Commonwealth Office)を始めとする関係機関の代表者が出席した。協議においては両国の最新のサイバーセキュリティ戦略と取り組みのほか、能力構築支援、国連を含む国際機関における双方向の連携等について意見を交換した。

(b)日米安全保障協議委員会

2021年3月16日、東京において日米安全保障協議委員会(日米「2+2」)が開催され、日本から茂木外務大臣と岸信夫防衛大臣、米国からAntony Blinken国務長官、Lloyd Austin国防長官(Secretary of Defense of the United States)が参加した※162。同委員会は、米国Biden政権との最初の閣僚級協議としてどのような合意になるかが注目された。

地域安全保障においては、2019年に懸念された北朝鮮の非核化に加え、中国の東シナ海・南シナ海への進出、海警法成立による中国国内法の外洋警備への適用、香港・新疆ウイグル自治区における人権問題等が深刻な懸念として共有され、日米豪印4ヵ国及びASEAN諸国との協力が再確認された。また防衛体制については、宇宙・サイバー領域における協力と情報保全の強化が強調された。

(c)日米首脳会談

日米「2+2」に引き続き、同年4月15～18日に菅義偉首相は米国を訪問、16日にワシントンDCにてJoe Biden大統領との日米首脳会談が行われた※163。同会談の共同声明「新たな時代における日米グローバル・パートナーシップ※164」においては、両国はパンデミックを終わらせ、「持続可能な、包摂的で、健康で、グリーンな世界経済の復興」を主導するために、デジタル経済の促進、気候変動に対応する脱炭素化、健康安全保障等において協力することが明記された。また、「自由で開かれたインド太平洋と包摂的な経済的繁栄の推進」のために両国の同盟を強化するとし、中国の「東シナ海における一方的な現状変更の試み」や「南シナ海における不

法な海洋権益に関する主張及び活動」に反対し、「台湾海峡の平和と安定」を重視することが明記された。

このように日米両国が共同声明で中国を非難することは異例であり、安全保障分野における中国との対立姿勢が鮮明となった。

(d)日 EU 首脳テレビ会議

2020 年 5 月 26 日、新型コロナウイルス感染拡大対策を主要議題として日 EU 首脳テレビ会議が開催された。日本からは安倍首相、EU からは Charles Michel 欧州理事会議長（President of the European Council）及び Ursula von der Leyen 欧州委員会委員長（President of the European Commission）が参加した※165。

同会議では、新型コロナウイルス感染終息後の経済復興について意見が交換され、高信頼通信インフラの整備拡充、強靭なサプライチェーンの構築、海外投資に対する安全保障上の観点からの適切な対応等、明らかに中国を意識した討議が行われた。また、新型コロナウイルス感染拡大の検証を公平で独立した形で行うこと、将来的な感染流行を防ぐために世界保健機関（WHO：World Health Organization）を含む国際機関の改革・効率化が重要であること等が確認された。

(3)アジア太平洋地域のサイバー連携

アジア太平洋地域における政府レベルの連携施策について述べる。CSIRT に関する連携施策については、「2.2.4 アジア太平洋地域での CSIRT の動向」を参照されたい。

(a)日・ASEAN サイバーセキュリティ政策会議

2020 年 10 月 20 日、第 13 回日・ASEAN サイバーセキュリティ政策会議（以下、政策会議）がオンラインで開催された※101。本会議は、サイバーセキュリティ分野における ASEAN 諸国との連携強化を目的として 2009 年より開催されている。

第 13 回政策会議は日本・カンボジアが議長国となり、日本から NISC、総務省、経済産業省の審議官、ASEAN 加盟国からサイバーセキュリティ・情報通信関係政府機関の局長・審議官等が参加した。同会議では、第 12 回政策会議で協力が合意された 9 項目（サイバー演習、重要インフラ保護、能力構築、インシデント相互通知、オンラインコミュニティ等）の活動状況を確認するとともに、今後の重点活動項目として、情報共有体制・インシデント対処体制の強化、能力構築・意識啓発分野の協力推進、産学官連携の事例共有等が議論され、活動の継続が確認された。

(b)ASEAN 地域フォーラム

ASEAN 地域フォーラム（ARF：ASEAN Regional Forum※166）は、ASEAN 地域の安全保障環境の向上を目的としたフォーラムで、日本政府は連携を継続している。サイバーセキュリティに関しては、シンガポール・マレーシアと共同で「サイバーセキュリティに関する会期間会合（ARF-ISM on ICTs Security）」を立ち上げ、2018 年 4 月より活動が始まっている。

2021 年 1 月 26 日、サイバーセキュリティに関する ARF 会期間会合のための第 6 回専門家会合※167 がオンラインで開催された。2020 年 1 月の第 5 回専門家会合と同様、日本・マレーシア・シンガポールが共同議長を務め、日本からは佐藤大輔外務省総合外交政策局経済安全保障政策室長が参加した。第 5 回に引き続き、国際的なサイバーセキュリティ環境や各国・地域の取り組み、今後取り組むべき信頼醸成措置について議論が行われた。また、サイバーセキュリティに関する国連政府専門家グループであるサイバー GGE（Group of Governmental Experts）※168 やオープン・エンド作業部会 OEWG（「2.2.1(1)(c)国連によるサイバー脅威対策推進」参照）等への参画を含め、世界的なサイバーセキュリティに関する議論に積極的に貢献することを確認した。

(c)インド太平洋地域に向けたサイバー演習

前出のように、インド太平洋地域のサイバーセキュリティ連携においてサイバー演習、能力構築は重要課題である。この状況のもとで 2021 年 3 月 8 ～ 12 日、経済産業省と IPA は米国政府と連携し、ASEAN を含むインド太平洋地域諸国を対象に、制御システムのサイバーセキュリティに関する演習をオンラインで実施した※169。また演習の一環としてポスト・コロナにおけるサイバーセキュリティに関する日米欧セミナーを開催した。本演習は制御システム等の重要インフラ防御に関するもので、ASEAN 及びインド太平洋地域から 40 名が参加した（演習内容は「2.3.2(1)中核人材育成プログラム」参照）。

(4)セキュリティ連携に関する国際会議

サイバーセキュリティの国際連携に関する主な会議として、2020 年度は、2019 年度に引き続き「サイバーセキュリティ国際シンポジウム」「サイバー・イニシアチブ東京」が開催された。

(a) 第 10 回サイバーセキュリティ国際シンポジウム

本シンポジウムは、サイバー脅威対応に向けた国際間の信頼構築を討議する場として、2016 年から日本で開催されている。2020 年は慶應義塾大学、同大学が主導する研究機関の国際連携組織 INCS-CoE（InterNational Cyber Security Center of Excellence）、米国 The MITRE Corporation[※170] の共催の形をとり、10 月 5 ～ 9 日にオンラインで開催された[※171]。また米国・英国・オーストラリア・イスラエル大使館及び駐日欧州連合代表部を始め、関係国の省庁が後援し、各国の有識者が参加した。会期中午後は国内向けの Japan Session、夜は Global Session という構成であった。

Global Session では、日本政府から河野太郎行政改革担当大臣が前防衛大臣の立場で講演し、基調パネルではパンデミック状況下のグローバルトラストをテーマとして、中満泉国際連合事務次長・軍縮担当上級代表（Under-Secretary-General and High Representative for Disarmament Affairs, United Nations）、Jeremy Jurgens 世界経済フォーラムマネージングディレクター・サイバーセキュリティセンター長（Managing Director & Head of the Centre for Cybersecurity, World Economic Forum）等が登壇、信頼構築について討議を行った。他の全体パネルでは、サイバーに関する規範、産学官のサイバー訓練、新型コロナウイルスの教訓、マルチステークホルダーによる国際トラスト等が議論された。産学官が連携した信頼構築に関する国際会議としてユニークなものと考えられる。

(b) サイバー・イニシアチブ東京 2020

世界各国の産学官のセキュリティ専門家を招いたサイバー・イシアチブ東京 2020 が、2020 年 11 月 24 ～ 25 日にオンラインで開催された[※172]。前出のサイバーセキュリティ国際シンポジウムと比較して、デジタルとリアルの融合に伴う脅威にフォーカスを当てた構成であった。

日本政府からは武田良太総務大臣、梶山弘志経済産業大臣、宇都隆史外務副大臣、岸信夫防衛大臣がそれぞれ講演したのを始め、関係省庁のセキュリティ関係者、国内・海外の民間有識者が参加し、ナショナルセキュリティ、ニューノーマルの安全保障、サプライチェーンリスク、医療セキュリティ、データ利活用等の多岐にわたる課題について議論が行われた。

2.2.2 米国の政策

2020 年度は米国にとり、新型コロナウイルスによるパンデミックへの対応、大統領選挙における世論の分断、Joe Biden 新大統領への政権移行、中国との継続的な関係悪化等が立て続けに起こる年となった。

米国のサイバーセキュリティ政策は、2019 年以降、サイバー空間の敵対的行動を監視し対抗する、という安全保障重視の姿勢を取り、サプライチェーンセキュリティの強化を進めている。しかし、SolarWinds Worldwide, LLC.（以下、SolarWinds 社）のネットワーク管理システムの脆弱性を突いたサプライチェーン攻撃、Colonial Pipeline Company（以下、Colonial 社）のパイプラインシステムを狙ったランサムウェア攻撃等が相次ぎ、米国政府・重要インフラへのサイバー脅威が深刻であることが改めて鮮明となった。

中国との関係においては、新型コロナウイルス対策における情報開示、海洋進出等の Trump 政権時からの課題に加え、香港・新疆ウイグル自治区における人権問題、台湾の主権帰属問題等から Biden 政権も中国に対して厳しい姿勢を取り、中国 IT 製品のサプライチェーンからの締め出し、及びグローバルサプライチェーンの再構築が継続される情勢である。

本項では、このような状況下で推進された米国政府のサイバーセキュリティ政策について述べる。

(1) 新型コロナウイルス対策とセキュリティリスク対応

新型コロナウイルスの蔓延と対策に関するセキュリティリスクの状況について述べる。

(a) 非常事態宣言

Donald Trump 大統領は 2020 年 3 月 13 日、新型コロナウイルス感染拡大について国家非常事態を宣言した[※173]。この宣言では、以下のような施策が盛り込まれた。

- 感染検査・治療対策に最大 500 億ドル（約 5 兆 4,000 億円）の連邦政府予算をあてる。
- 医療従事者に対する規制を緩和し、治療における最大限の柔軟性を与える。
- 病院に緊急対応計画の発動を要請する。
- PCR 検査を迅速に拡大する。
- 大学等が休校となった学生のローン返済を猶予する。

一方で、ニューヨーク州、カリフォルニア州等が独自

の緊急事態宣言を発動し、都市部のロックダウン等の厳しい措置をとったのとは対照的に、外出・旅行・マスク着用等に関する要請はなかった。

Biden 政権は 2021 年 2 月 24 日、パンデミックに対して引き続き警戒が必要であるとして、非常事態宣言の継続を宣言した※174。

(b) サプライチェーンリスクと中国との関係悪化

米中政府間では 2020 年 2 月初旬の中国滞在者の米国渡航制限以来、新型コロナウイルス感染原因の特定をめぐって相互に非難が続いた。Trump 大統領は同年 4 月、感染拡大防止でやるべきことをしていない、として中国を正面から批判※175、5 月には新型コロナウイルスが中国湖北省武漢にあるウイルス研究施設から流出したものか調査中であるとした※176。これらの発言はパンデミックと緊急事態宣言による経済停滞に苦しむ米国国民の支持を得て、2019 年秋の経済摩擦交渉で一時修復に向かった米中関係は急激に悪化した。一方、新型コロナウイルスの発生源とされ、また中国製造業の拠点でもある武漢市は 2020 年 1 月 23 日より 4 月 8 日まで完全にロックダウンされ※177、中国を起点とするグローバルサプライチェーンは甚大な影響を受けることとなった。

米国では既に、Huawei Technologies Co. Ltd. を始めとする中国 IT ベンダの製品が連邦政府システムや民間の重要インフラシステムにおいて調達されることが懸念され、サプライチェーンからの締め出し施策が実施されている（「情報セキュリティ白書 2020※178」の「2.2.2 米国の政策」参照）。加えて、パンデミックによりサプライチェーンリスクは更に深刻化し、これまで中国を起点としていたグローバルサプライチェーンの分散化・国内回帰の機運が米国・欧州・日本で高まりつつある。

Biden 大統領は選挙公約にサプライチェーンの米国回帰を掲げていたが、2021 年 2 月 24 日、サプライチェーン頑健化に関する大統領令に署名した※179。同大統領令では、頑健化の方針として安全、分散化、国産製品活用、冗長性、国内人材活用等が挙げられ、国家安全保障担当補佐官（APNSA：the Assistant to the President for National Security Affairs）、経済政策担当補佐官（APEP：the Assistant to the President for Economic Policy）が関係機関と協調してこれを実装するとし、施策として 100 日以内のサプライチェーンリスクレビュー、1 年以内の各政府機関のサプライチェーンアセスメント、及び過去 1 年にとられた対策の報告と提言を求めている。Biden 政権としては、パンデミック終息後の経済再建において環境問題・脱炭素を重視し、関連産業のサプライチェーン構築で脱中国を果たし、優位に立つ戦略があるものと思われる※180。

(c) CISA の新型コロナウイルス関連リスク対応

新型コロナウイルス関連のサイバーリスク対策は、国土安全保障省（DHS：Department of Homeland Security）配下でサイバーセキュリティと重要インフラセキュリティを統括する CISA（Cybersecurity and Infrastructure Security Agency）が中心となって推進している。2020 年 3 月 6 日、CISA はいち早く新型コロナウイルス関連詐欺メール・詐欺サイトに関する注意喚起を、また 3 月 18 日には重要インフラ保護、サプライチェーンの維持、リモート業務の保護、新型コロナウイルス関連詐欺対策を含むリスク管理ガイダンスを公開した※181。詐欺被害に関しては連邦捜査局（FBI：Federal Bureau of Investigation）も別途注意を呼びかけた※182。

また CISA は、英国国家サイバーセキュリティセンター（NCSC：National Cyber Security Centre）と共同で、新型コロナウイルスを話題とする標的型攻撃が急増する中、セキュリティ的に脆弱な環境でテレワークが行われている、として同年 4 月 8 日に注意喚起を行い※183、4 月 24 日にはテレワークのセキュリティガイダンスを公開した※184。また 4 月 17 日、コロナ禍における重要インフラ基盤の運用と従業員の安全に関するガイダンス（第 3 版）を公開した※185。更に 5 月 5 日、CISA と NCSC は新型コロナウイルス関連の医療研究機関・製薬企業の研究データや知的財産データが窃取される恐れがある、と警告した。続く 5 月 13 日における FBI と共同の注意喚起※186 では、「中国と関係するサイバーアクターが情報を狙っている」と初めて中国が名指しされた。

更に CISA は同年 8 月 12 日、中小企業庁（SBA：Small Business Administration）の新型コロナウイルス救済融資をかたるメールについて注意喚起を行った※187が、この後、新型コロナウイルス関連の詐欺攻撃は一段落した模様で、2021 年 4 月時点まで CISA から注意喚起は行われていない。

(d) 新型コロナウイルスをめぐるインフォデミック

2020 年 1 月以降、米国国務省の官僚が「SNS 上で反米的な偽情報を拡散している」としてロシアを非難する※188 等、新型コロナウイルス感染拡大をめぐり、インターネット上で国家間の非難の応酬が続いた。

同年 3 月以降は感染源や対策、ワクチン等をめぐる

誤情報や偽情報（フェイクニュース）がネット上にあふれ、社会に悪影響を及ぼすインフォデミック（infodemic）の状況が各国で現出した。これに対しWHOは同年9月、国連や国際連合児童基金（UNICEF：United Nations International Children's Emergency Fund）等の国際機関と共同して、正確で信頼できる情報を提供し、誤情報・偽情報の拡散を防ぐ対策を講じることを加盟国に呼びかけた※189。

米国においては、CISAが詐欺攻撃への注意喚起のほか、誤情報・偽情報に対する注意喚起も行っている※190。CISAは注意喚起の中で、信頼できる情報源として米国疾病予防管理センター（CDC：Center for Disease Control and Prevention）、連邦緊急事態管理庁（FEMA：Federal Emergency Management Agency）のRumor controlサイト、WHOを挙げている。

一方、国防総省（DoD:Department of Defense）は、2020年4月の時点で中国、ロシアのコロナウイルスに関する情報発信が虚偽であり、特にロシアの情報（手洗いの効果はない）は対策を誤らせるとして非難していた※191。インフォデミックについても軍への波及の観点から警戒し、軍関係の情報で事実でないものを公開している※192。またコロナワクチン接種を控えさせかねない誤情報についてもこれを否定し※193、軍関係者に接種を促している。

民間組織もコロナ関連情報の監視を行っている。例えば情報監視サイトPOLYGRAPH.infoはSNS上で流通するコロナ情報のファクトチェックを行い、誤り（Misinformation）あるいはミスリーディングなもの（Disinformation）を根拠とともに公開している※194。言うまでもなく、こうした組織はパンデミック関連情報に限らず、政治・軍事・人権等様々なカテゴリのファクトチェックを行っている。

こうした努力にもかかわらず、インフォデミックの影響は米国では深刻と考えられる。2021年2月の民間調査によれば、民主党支持者の8割以上がパンデミックを深刻な脅威としたのに対し、共和党支持者で深刻な脅威とした人は半数に満たないことが確認された※195。このような分断状況が、事実を受け入れず偽の情報を流通させてしまう、場合によっては感染し死に至る、等の問題につながっている可能性がある。

(2) Trump政権下のセキュリティ施策

2021年1月までのTrump政権のもとで、各政府機関により推進されたセキュリティ施策について述べる。

(a) Trump政権の政策

2020年はTrump政権4年目であり、2018年9月に米国大統領として初めて発表したサイバーセキュリティ戦略を実装するべく、各政府機関が施策を推進してきた。この戦略は前述のように、国家安全保障の観点から敵対的勢力に対抗する施策・体制を盛り込んでいるが、同時に外交・経済制裁等を含め、同盟国・民間との連携を重視した協調的な姿勢も示してきた。

2018年9月にTrump大統領が公表した国家サイバーセキュリティ戦略を拡張する形で、同政権は2020年3月、セキュア5Gに関する国家戦略を発表した。CISAとNRMC（National Risk Management Center）はこれに基づき、2020年8月14日、セキュアで頑健な重要インフラのための5G戦略を発表した※196。大統領選挙前にセキュリティ関連戦略として具体化されたものは、これが最後となった。

一方で、サプライチェーンリスク対応には大統領任期満了までこだわり、2021年1月5日、Trump大統領はAnt Group Co., Ltd.の「Alipay（支付宝）」を含む八つの中国デジタル決済プラットフォームとの取り引きを禁止する大統領令に署名した※197。また1月20日、自身最後のサプライチェーンセキュリティ施策として、米国のIaaSプラットフォーム事業者に外国人利用者の記録を残すことを要請する大統領令に署名した※198。ただし、これらの施策の実施可否はBiden政権に委ねられた。

(b) DHSの施策

DHSでは、2018年11月にサイバーセキュリティと重要インフラセキュリティを統括する組織として改組されたCISAの活動が本格化している。活動のうち、新型コロナウイルス対策については既に記したが、このほかの重点項目として重要インフラセキュリティ、サプライチェーンセキュリティがある。このうち重要インフラセキュリティ、特に制御システムに対する脅威とその対策については「3.1 制御システムの情報セキュリティ」を参照されたい。

サプライチェーンセキュリティについては、2019年に設置したICT Supply Chain Risk Management（SCRM）Task Force（以下、Task Force）が中心となり、2020年2月に、IT製品・サービスの供給者視点でまとめたサプライチェーン脅威シナリオ第1版を、また2021年2月には脅威シナリオのインパクトと緩和策（mitigation）を分析した第2版を公開した※199。脅威シナリオは偽造、攻撃、内部不正、開発環境への攻撃、供給者の財務体質を含む包括的なもので、米国のサプライチェーンリ

スクのとらえ方がよく現れている。

これに続き2020年5月、Task Forceは企業のサプライチェーンリスク管理指針となるガイダンスとファクトシートを公開した※200。更に具体的なリスク管理ツールとして、米国標準技術研究所（NIST：National Institute of Standards and Technology）の規格群をベースとする製品・供給者・入札者に関する有資格リストの検討を進め、2021年4月に報告書を公開した※201。このリストがどの程度政治的な意味を持つかは未知数である。

一方でTask Forceは2020年11月、パンデミックで中国依存のリスクが顕在化したグローバルサプライチェーンの脆弱性、及びサプライチェーンを頑健化するための指針をまとめた※202。これには必ずしもITサプライチェーンにとどまらない課題と対応策が示されている。

(c) DoDのサプライチェーンセキュリティ施策

2020年1月31日、DoDは、新たなサイバーサプライチェーンセキュリティ規格として、サイバーセキュリティ成熟度モデル認証（CMMC：Cybersecurity Maturity Model Certification）の初版を公開した。また同年3月18日に改訂版Version1.02を公開した※203。「情報セキュリティ白書2020」の「2.2.2 米国の政策」で述べたとおり、調達者に対するセキュリティ規格NIST SP800-171の管理策徹底が厳しすぎる等で不評であったことから、5段階の成熟度モデル、5個のセキュリティマネジメントプロセス、171個のプラクティスで構成されるCMMCがより有効であるとして適用に踏み切ったものである。DoDは2020年3月に認証機関CMMC Accreditation Body（CMMC-AB）※204を設立、調達事業者認証に向けた準備を開始した。また、国防総省調達規則補足（DFARS: Defense Federal Acquisition Regulation Supplement）を改正し、2020年11月30日から2025年9月30日（会計年度終了）までのCMMCによる調達を暫定的に有効にする、とした※205。

このようにCMMCによる防衛調達制度が整備される一方で、認証のコスト、連邦政府とCMMC-ABとの責任分担等の問題が指摘され、2021年3月、DoDは制度の見直しにはいった※206。CMMCに限らず、高度なセキュリティ認証は高コストになりがちであるが、防衛サプライチェーンのセキュリティは米国の最重要課題ともいえる。DoDやBiden政権がどのような制度設計を行うか注目される。

(3) SolarWinds事案とその対応

2020年、連邦政府機関及びフォーチュン500に掲載される企業等を一斉に狙った過去最大規模のサプライチェーン攻撃が発覚した。同年12月13日、セキュリティベンダFireEye, Inc.は、ネットワーク管理ツールベンダSolarWinds社のネットワーク管理システムOrionへの大規模攻撃キャンペーン（UNC2452）を確認した、と発表した※207。これは、Orionのサードパーティサーバとのバックドアからトロイの木馬型プラグインを仕込み、Orionソフトウェアのアップデートにより管理対象機器にウイルスを感染させるというもので、2020年3月から始まったという。SolarWinds社は同13日にこの攻撃を認め、同社の顧客1万8,000社に影響した可能性がある、とした。CISAも同13日、連邦政府機関に対して緊急指令（Emergency Directive21-01）を発令し、サプライチェーン上で他者により利用・運用されている情報システムを保護し、脅威を緩和するための対策を求め※208、具体的な行動計画も明示した。

UNC2452の目標は情報窃取と考えられたが、調査の進展につれ、攻撃キャンペーンの広がりが深刻であることが明らかになった。FireEye, Inc.は、攻撃の水平展開の一環として、オンプレミスネットワークからOffice 365への不正アクセスが行われたとしている※209。少なくとも250の官民のネットワークが侵害され、これまで米国国家安全保障局（NSA：National Security Agency）が進めてきたインサイダー監視のための法規、DHSの防御施策、DoDのサイバーコマンド部隊が早期警戒のため海外ネットワークに設置した監視センサー等の対策がことごとく無効であったという※210。CISAは「連邦政府、州政府、自治体から重要インフラ企業のネットワークに至るまで影響は甚大である」とした※211。サイバーセキュリティやサプライチェーン関係各部門は、これまでの施策について大幅な見直しを迫られることになる。他の追跡調査については、「3.1.1(4)ネットワーク管理用のソフトウェアの脆弱性に端を発する大規模な感染事例」を参照されたい。

攻撃者については、米国大統領選挙に対するロシア政府の妨害工作が懸念されていた経緯から、ロシア情報機関とつながりのあるハッカー集団APT29による選挙妨害工作の一環である、と疑われた※212。2021年1月5日、FBI、CISA、国家情報長官室（ODNI：Office of the Director of National Intelligence）、NSAはサイバー統合調整グループUCG（Cyber Unified Coordination Group）を設置し、連邦政府ネットワーク

侵害等の重大事案に関する調査・脅威緩和を協力して行うこととした※213。この体制は言うまでもなくロシアへの対抗を意識したもので、関係4機関は翌6日、合同でSolarWinds社へのハッキングはロシアが主導した可能性が高い、と公式にロシアを非難した。これに先立ちTrump大統領は、選挙妨害は民主党の意を受けた中国による可能性もある、とSNSで発言したが、これは明確に否定された。

2021年4月15日、Biden大統領は調査結果を受け、ロシアに対する制裁措置に関する大統領令に署名した※214。同大統領令では、SolarWinds事案を含む米国に対する選挙妨害活動が、ロシア対外情報庁（SVR: Sluzhba vneshney razvedki Rossiyskoy Federatsii）によるものと断定、活動に協力したロシア企業6社を特定し、またロシア政府と米国金融機関の取り引きを一部停止するとした。当然ながらロシア政府はハッキングへの関与を否定し、制裁には報復措置を講ずるとしている※215。

(4) Microsoft Exchange事案とその対応

2021年3月2日、Microsoft Corporation（以下、Microsoft社）は、オンプレミス用メールサーバソフトウェアExchange Server 2010、2013、2016、2019の各バージョンに対する緊急セキュリティ更新プログラムをリリースした。対象となる脆弱性はExchangeサーバ上でリモートコード実行が可能になるもので、至急のパッチ適用と攻撃の調査が求められた※216。同社はまた、中国に支援された攻撃者グループHAFNIUMが高い確度でこの脆弱性を突いた限定的標的型攻撃を行っているとした※217。

セキュリティ専門家によれば、この攻撃は同年1月6日（一部Trump支持者の連邦議会占拠当日）に発見されていたが、Microsoft社の情報開示直後、パッチ未適用のExchangeサーバを持つ中小企業、自治体、学校等少なくとも3万の組織がHAFNIUMと目される中国ハッカー集団の攻撃を受け、メール通信の窃取が行われた可能性があるという※218。

これに対しCISAは3月3日に注意喚起を実施、政府機関に対しても緊急指令（Emergency Directive21-02）を発令してパッチ適用を指示した※219。Biden政権は15日に新たなUCGを招集、Microsoft社と連携して特に支援が必要な中小企業の対策・調査にあたるとともに、サイバー防御の一新のために民間との連携を強化するとした※220。民間との連携によるサイバー防御強化はTrump政権でも重点としていたが、これを踏襲した形である。

事案発覚後1ヵ月あまりで、この事案の深刻さが浮き彫りになってきた。中国のハッカーによるこれまでの不正な情報収集活動が今回の大規模な攻撃につながったといわれる※221。またMicrosoft社によれば、不正に収集されたメールアカウントの認証情報は特権昇格等の攻撃にこれからも悪用される恐れがあり、2021年4月時点においても被害の全貌が明らかになっていない可能性がある※222。同社は管理者権限の最小化等によって被害を低減するように呼びかけている。

本事案とSolarWinds事案との直接的な関係は見つかっていない。しかし、ネットワーク管理、メールサーバ等の基幹システムの脆弱性対策が機能せず、国家の支援による攻撃があれば甚大な被害となるという事態は米国を始め、欧州、日本等にも深刻な問題であり、Biden政権にとっても重要課題となると考えられる。

(5) Colonial Pipeline事案とその対応

SolarWinds、Microsoft Exchangeの各事案が収束しない2021年5月7日、石油パイプライン事業最大手のColonial社は、サイバー攻撃を受け、パイプラインの操業を停止したと発表し※223、翌8日にはネットワークへのランサムウェア攻撃を認めた。同社のパイプラインはテキサス州からニュージャージー州に及ぶ石油供給の45%を担う大動脈であり、米国東部の燃料不足が懸念される事態となった。連邦政府は直ちに対応し、10日、Biden大統領は「影響を緩和する措置をとり、攻撃を阻止し、攻撃者を訴追する」と言明し、FBIはRaaS（Ransomware as a Service）をビジネスとする東欧系ハッカー集団DarkSideによる攻撃であることを確認した※224。ロシアの関与の証拠はないとされたが、Biden大統領は「ロシアが一定の責任を負う」とコメントした。名指しされたDarkSideは、「攻撃の目的は金銭であり政治的混乱を起こす意図はない」とする声明を発表した※225。11日、FBIとCISAは更なるランサムウェア攻撃への対処について注意喚起を行った※226。

Colonial社は停止したパイプラインの再稼働を12日から始めるとし※227、フル稼働までに時間がかかるとしたが、燃料不足の懸念はひとまず沈静化した。一方、身代金については約75ビットコイン（500万ドル相当）の支払いがあったと報じられ※228、Colonial社のCEOも「早期復旧のために支払った」ことを認めた※229。

Biden政権は5月12日、サイバーセキュリティに関する大統領令※230を公表するところであったが、図らずも同時期に、重要インフラの防御が脆弱であり、被害の影

響が深刻であることが露呈してしまった。なお、大統領令については「2.2.2(7)Biden 政権の政策」で言及する。

(6) 大統領選挙とフェイクニュースの混乱

2020 年 11 月 3 日、第 59 回米国大統領選挙が実施され、共和党 Donald Trump 大統領、民主党 Joe Biden 候補が接戦を演じたが、鍵となるジョージア州、ペンシルベニア州等で優位に立った Biden 候補が 11 月 7 日に勝利を宣言した※231。選挙結果の確定は遅れ、11 月 23 日、Trump 大統領は政権移管手続きを認めた※232 ものの、慣例の敗北宣言をしなかった。同大統領は同年 9 月の時点で郵送による選挙に不正の危険があると SNS で発言、また開票中も「選挙は盗まれた」と不正を訴え、州政府に多くの訴訟を起こしたが、提出された証拠は薄弱であるとして却下された。連邦最高裁判所に提訴された 2 件についても 12 月 8 日、11 日に却下された※233。

こうした Trump 政権の「不正選挙」キャンペーンがフェイクニュースの氾濫、一部 Trump 支持者の過激な行動を誘発した。2021 年 1 月 6 日、連邦議会は Biden 候補の当選を承認する予定であったが、一部 Trump 支持者は力によりこれを防ぐとしてワシントン DC に集結した。Trump 大統領は彼らを扇動する発言を SNS で続け、更に 6 日午後、ホワイトハウス前で同様の演説を行った。これに乗じた支持者は警戒を破って連邦議会に侵入、占拠し、排除において死者 4 名が出る異常事態となった※234。翌 7 日、議会はあわただしく Biden 候補の当選を承認し、Pence 副大統領も Biden 候補の勝利を公式に認めた。また Trump 大統領は選挙の不正を主張し続けたものの「政権の秩序ある移行を行う」と SNS で表明した※235。1 月 20 日、Biden 次期大統領は大統領に就任したが、共和党員の支持はほとんどなく、分断状態となった米国の再統合という難しいかじ取りを迫られることとなった。

以上の経緯により、フェイクニュースの氾濫・誘導が世論を分断し、国家の安定を揺るがしかねないという深刻な課題が浮き彫りとなった。フェイクニュースのリスクはパンデミックで既に顕在化し、SNS ベンダは対策を強化していた。例えば Facebook, Inc.(以下、Facebook 社)は 2020 年 2 月、大統領選挙に向けたファクトチェック強化のため、Thomson Reuters Corp との提携を開始した※236。Twitter, Inc.(以下、Twitter 社)は、危害を加える、または誤解を招く可能性のあるツイートに対する警告ラベルの適用を強化した。2020 年 5 月 26 日、Trump 大統領のツイートに初めて警告し※237、同年 11 月 5 日の時点では、同大統領の「不正選挙」に関する 29 個のツイートのうち 11 個に警告したという※238。こうした警告とそれに伴う SNS サービスの利用制限は、一方で SNS ベンダの越権行為だと批判する声もあったが、フェイクニュースの混乱は加熱し、暴徒による議会占拠が起こってしまった。

ここに至り、Facebook 社は 1 月 6 日、Trump 大統領の Facebook アカウントを無期限に停止した。Twitter 社は同大統領のアカウントを凍結し、支持者応援演説の映像等を削除した上で凍結をいったん解除したが、同月 12 日、「さらなる暴力扇動のリスクを除く」として恒久的に Trump 大統領の Twitter 利用を禁止した※239。

上記 2 社はこれまで「表現の自由」を標榜し、政治家が SNS 上で行う発言には終始寛容であった。しかし 1 月以降、2 社は態度を 180 度転換し、Google LLC(傘下の Instagram 等へのアクセスを制限)とともに利用者に対する最も厳しい措置を取った。この結果、氾濫していたフェイクニュースが劇的に減少し、扇動による混乱が収まったことは事実である。

しかし一方で、この措置は「IT プラットフォーム事業者は個人の言論発表の機会に対して圧倒的な力を持ち得るが、その力の根拠は不明である」という新たな問題を提起し、様々な議論がおこった。例えば利用停止の直後、ドイツの Angela Merkel 首相は「言論の規制は法律に基づくべき」として、SNS ベンダの対応に疑問を呈した。「他に表現手段のない弱い立場の人が投稿を削除されることへの懸念」も表明された※240。特に EU 諸国は、米国の巨大プラットフォーム事業者による EU 域内の私権の制限に対する懸念が強いが、同じ問題は日本にも起こり得る。今後も注視すべき課題であるといえる※241。

なお大統領選挙に関して、AI 技術を悪用した Deep fake によりフェイク動画を作成し、選挙活動に干渉する攻撃が懸念されていたが、重大事案は報告されず、結果的には大きな問題とならなかった※242。

(7) Biden 政権の政策

Biden 政権は、SolarWinds、Microsoft Exchange、Colonial Pipeline の各事案のただ中で発足した。同政権はこれらの事案の収束とサイバーサプライチェーンリスク対応、基幹サービスのセキュリティ強化を中心として、セキュリティ政策を見直していくものと思われる。サプライチェーン再構築について、Biden 政権は「2.2.2. (1) (b)

サプライチェーンリスクと中国との関係悪化」で述べたとおり、2021 年 2 月 24 日に大統領令を発表し、連邦政府機関と連携して 100 日以内に各機関のサプライチェーンリスクレビューを実施するとした。更に 5 月 12 日、Biden 政権は前述のサイバーセキュリティに関する大統領令を発表した。主にサプライチェーンセキュリティ強化を意図したもので、以下の点が注目される。

- 官民の脅威情報共有の障壁除去
  政府システムにおける民間プラットフォーム・サービスの活用が拡大する中で、調達契約で記載するべきセキュリティリスク・対策等の要件とそれを表現する契約用語を明確にすることを求めている。ISACs、ISAOs（Information Sharing and Analysis Organizations）による現体制では IT/OT 事業者、クラウド事業者等が持つ脅威・インシデント情報を関係政府機関が共有できていないとの危機意識があると思われる。
- 連邦政府セキュリティの現代化（Modernization）
  政府システムのセキュリティ刷新は Trump 政権からの継続事項となる。本大統領令では多要素認証を含むゼロトラストアーキテクチャの実装、政府共通のクラウドセキュリティ戦略等を新たに求め、政府調達クラウド認証制度 FedRAMP（Federal Risk and Authorization Management Program）の現代化にも言及している。
- ソフトウェアサプライチェーンセキュリティの強化
  重要（Critical）なソフトウェアのセキュア開発・調達に関して、NIST を中心とした新たなガイドラインの 1 年以内の策定を求めている。検討項目にはコードチェック等の自動化、SBOM（Software Bill of Materials、ソフトウェア部品表）の採用等、懸案となってきたものも含まれる。ソフトウェア調達においてはこのガイドラインの遵守状況が審査されるため、どの程度厳しい内容になるか注目される。
  このほか、IoT 機器のセキュリティに関する情報を利用者に提供する（Consumer labelling）パイロットプログラムの実施が求められている。

上記大統領令はサプライチェーンセキュリティに関しては包括的で歓迎の声もあるが、どこまで実装可能かは未知数である。また、Colonial Pipeline 事案のような重要インフラの脆弱性対策等は含まれていない。Trump 政権も発足当初にこのようなレビューと対策立案を実施したが、Biden 政権は更に待ったなしの状況で、国家のサイバーセキュリティの火急の見直し・再構築が求められる。

人材面では、Trump 政権末期には、不正選挙キャンペーンへの反発から、CISA の Chris Krebs 長官が更迭される等、セキュリティ人材が政府機関から流出していたが、2021 年 4 月、Biden 大統領は CISA 新長官に元 NSA の Jen Easterly 氏を、2021 年の国防予算大綱である国防権限法（National Defense Authorization Act for Fiscal Year 2021）※243 により新設された国家サイバー長官（National Cyber Director）に、同じく元 NSA の John Chris Inglis 氏を指名し、立て直しを図っている※244。

対外的には、Trump 政権と同様に中国に対する厳しい姿勢をとりながら、SolarWinds 事案で再燃したロシアへの対抗政策が求められる。中国、ロシアはともに米国にとってサイバーセキュリティ上の敵対勢力とみなされる国であるが、両国と同時に衝突することは得策ではなく、Biden 政権がどのような交渉を行うか注目される。

2.2.3 欧州の政策

2020 年 2 月 1 日、英国は正式に EU を離脱※245 し、同年 12 月 31 日までを移行期間として EU 法制の適用を継続し、その間に EU・英国間の新しい自由貿易協定（FTA：Free Trade Agreement）等を締結することとなった。FTA をめぐる交渉は難航したが、時間切れ直前の 12 月 24 日、双方は合意に達した※246。合意文書「EU・英国の通商と協力に関する協定（TCA：EU-UK Trade and Cooperation Agreement）」※247 は 2021 年 1 月 1 日に暫定的に発効し、英国は完全に EU から離脱した。同年 4 月 27 日、欧州議会（European Parliament）は TCA、及び付随する「EU・英国の情報セキュリティ協定（EU-UK Security of Information Agreement）」（以下、セキュリティ協定）を承認、翌 28 日に欧州理事会（European Council）がこれを批准し、合意は 2021 年 5 月 1 日から正式に有効となった※248。

一方で、2020 年度は欧州各国も新型コロナウイルスによるパンデミック対応に追われ、セキュリティ面では米国同様にインフォデミックやサプライチェーンリスクへの対応が課題となった。以下では、英国を含む EU 諸国のセキュリティ・データ保護に関する動向について述べる。

(1) EU・英国の交渉

2020 年 3 月 2 日、ブリュッセルにて EU と英国の「将来関係交渉（EU-UK future partnership negotiations）」が開始され、11 の分科会に分かれて討議（ラウンド）が

行われた※249。なお防衛に関しては、英国の意向で将来関係交渉には含めないこととなった。将来関係交渉の第2ラウンド～第4ラウンドは新型コロナウイルスの影響で主にビデオ会議の形式で行われた。交渉は当初予定の9月では決着せず、7回の延長交渉の末、「合意なき離脱」を避けるための最低限の合意に至った。主要な合意点は以下のようになる※250。

- EU・英国間で関税をゼロとするが、通関手続きは復活する。
- 鉄道・航空・海上輸送等は現状を維持する。
- 英国はEUの統一ルールや欧州司法裁判所の影響から外れ、金融等の規制・監督は独自に行う。
- 英国は公正な競争のためにEUルールを尊重する。
- 公正な競争がゆがめられた場合には必要な措置を取る。

以下では、争点となった課題・セキュリティ関連課題の合意内容について紹介する。

なお、以下の(a)(b)(c)は最後まで難航したが、形の上では英国が粘ってEUの統制をある程度弱めることに成功した点である。その一方、EU・英国間の貿易は煩雑・高コストとなり、英国からのEU単一市場へのアクセスは明らかにハードルが上がっている。

(a)漁業

漁業においては、英国が自国海域の漁獲枠を自国が決めるとしたのに対し、EUは保持している漁業権の維持を主張し、難航した。双方が歩み寄った結果、当面EU漁船の英国海域での操業は許可するが、今後5年間で現行のEUの漁獲割り当ての25%を英国に移行する、2026年6月以降、英国は自国海域でのEU漁船の操業を制限できるが、EU側も対抗策を実施できる等で合意した※251。

(b)公正な競争

公正な競争(Level playing field)とは、EU・英国間で企業の競争が同じ条件で行われることの保証である。EUは、域内企業に対する課税や環境対策・労働環境等の規制、及び補助金制度等について英国が独自に緩和し、域内企業が不利になることを警戒し、例えば英国政府が日産自動車株式会社に示したEU離脱後の保証が懸念材料となった※252。EUは同等の競争環境維持について英国に規則化を要求したが英国はこれを嫌い、交渉は難航した。

最終的には双方が歩み寄り、補助金制度は別々とする一方で双方の制度設計の原則を規定する、労働条件・環境対策の水準を低下させない互恵的約束を規定する、公平性の評価・修正の仕組みを作る等で合意した※253。

(c)ガバナンス

ガバナンスとは、EU・英国間のTCA違反等における紛争解決の統制のことである。EUは欧州司法裁判所による一律の統制を要求したと思われるが、英国はEUの法制度を適用されることに強く反発、国別に締結する経済連携協定（EPA：Economic Partnership Agreement)、FTA等により調停するべき、として難航した。最終的にはEUの法制適用は見送られ、双方がまず協議し、不調なら独立の仲裁パネルが調停を行うことで合意した。

(d)データの妥当性

データの妥当性(Data adequacy)は、EU・英国間の自由なデータ移転のための保護施策を保証することであり、特にGDPR(General Data Protection Regulation)に相当する英国の個人データ保護施策の認定（十分性の認定)が重要である。

英国は、GDPR施行に合わせて同規則遵守の体制を整えていたが、EU離脱前後の政治的混乱等から十分性認定の手続きが遅れ、2021年1月以降のEU・英国間のデータ移転に支障が出ることが危ぶまれていた。TCAではこれに対し、十分性認定が確定するまで最大6ヵ月間、欧州経済領域（EEA：European Economic Area。EUとノルウェー、リヒテンシュタイン、アイスランド等のEU非加盟国で構成）からの英国への個人データ移転を暫定的に認めることとした※254。続いて2021年2月19日、欧州委員会（European Commission）は英国の個人データ保護のレベルがEUの保護レベルと比較して妥当であるとの評価(Adequacy Decision)ドラフトを公表した※255。この評価は、欧州データ保護委員会（EDPB：European Data Protection Board）の助言のもとにEU加盟国、欧州委員会が承認する必要がある。4月16日、EDPBは同評価について、「評価を支持するが、今後の英国の動向を注視する」との意見を表明した※256。具体的な懸念として、移民の入国統制への意図しない個人データ利用、英国のデータ保護方針の変更、法執行機関からのアクセス等に言及している※257が、承認は問題なく行われると思われる。

(e) セキュリティ

EU は、国際犯罪や外交等における共通の安全上の脅威に関し、EU の機密情報を第三者と共有する場合は、個別事案に特化した情報セキュリティ合意（Security of Information Agreement）を求めている。しかし将来関係交渉においては、事案ごとの交渉が煩雑となり得ること等から、機密情報の格付け、保護、第三者開示、相互協力等に関して包括的な規定が作成された（前出のセキュリティ協定※258）。本セキュリティ協定の内容は非常に基本的なもので、TCA の改廃に連動する等、あくまで TCA に付随する扱いである。2020 年 12 月 24 日の最終討議で TCA とともに合意された。

一方、サイバーセキュリティは将来関係交渉の議題とならなかった。「情報セキュリティ白書 2020」の「2.2.3 欧州の政策」で述べたとおり、英国は EU の NIS 指令（Network and Information Security Directive）に対応する国内法も整備済みであり、EU 加盟国との連携も既存の枠組みでできていることから、従来どおりの連携が進むものと思われる。

(2) 新型コロナウイルスへの対応

欧州においても、2020 年 1 月以降、新型コロナウイルス感染が拡大し、各国は対策に追われた。

(a) 感染状況

欧州でのパンデミックはまず 2020 年 1 月末に中国からの渡航者が滞在したイタリア北部地域で発生、3 月 9 日にはイタリア全土にわたるロックダウンが開始された※259。フランスでも同年 2 月後半から感染者が急増し、同年 3 月 16 日、Emmanuel Macron 大統領は少なくとも 15 日間の全国的なロックダウンを要請した※260。

ドイツでも 1 月下旬の感染発覚以来感染者が急増し、3 月 13 日には各州の学校・幼稚園が閉鎖、16 日には国境管理の厳格化とともに各州におけるロックダウンの強化※261、17 日には EU 委員会提案に基づく EU 域内への 30 日間の入域制限が実施された。

英国政府は、2020 年 3 月初旬の時点では「科学に基づき、国民に免疫をつけさせることが有効」とし、ロックダウン等の強い施策を行わない方針であったが、医療専門家の批判を受けてこれを撤回、3 月 23 日に Boris Johnson 首相が「Stay at home」を要請した※262。

上記以外の欧州諸国も同様な対応を余儀なくされた。欧州各国は上記のパンデミック第 1 波の後、10 ～ 12 月の第 2 波、2021 年 3 ～ 4 月の第 3 波に襲われ、それぞれロックダウン等を迫られている。

なおこの間、英国では 2021 年 1 月からのワクチン接種が急速に進み、2021 年 4 月末時点で少なくとも 1 回接種した人は 3,436 万人を超えた。また 2021 年 1 月初旬に 6 万人超であった 1 日の感染者数が 4 月末時点で 2,300 人弱に減少している※263。

パンデミックの原因について、米国・欧州は 2020 年 1 月末時点から中国武漢市が起点であったとし、中国の情報開示の不十分さや自国のビジネスを優位にするかに見える対策支援の姿勢に不審感を抱いた。EU と中国は 2019 年までは 5G 関連の IT インフラ導入等で親密といえる関係にあったが、パンデミックによる中国への不信、グローバルサプライチェーンの中国依存体質の見直し、更には香港や新疆ウイグル自治区における人権問題により中国との関係は冷却し、英国と EU 諸国はこれを見直そうとしている。

(b) セキュリティ対策

パンデミックの影響で在宅勤務が増加し、詐欺情報やデマ情報が蔓延した状況は欧州も米国と同様である。欧州ネットワーク・情報セキュリティ機関（ENISA：The European Union Agency for Cybersecurity）は、各国のロックダウンが本格化した 2020 年 3 月 24 日、テレワークのセキュリティと新型コロナウイルス関連のフィッシングに注意喚起を※264、同月 31 日にはネットショッピングの急増に対し、フィッシングや決済の不正等に対する注意喚起を※265 行った。しかし 3 月以降、欧州のフィッシングメールによる攻撃件数は 1 ～ 2 月の 6 倍以上に急増し、5 月 6 日、再度注意喚起をせざるを得なくなった※266。ENISA はまた、4 月 24 日にオンライン会議ツール選択に関する注意喚起を行った※267。注意喚起では、欧州らしい特徴として、セキュリティに加え個人情報保護への配慮が注意点に含まれている。

(c) インフォデミック対策

フィッシングへの対処の一方、新型コロナウイルスの感染対策やワクチン接種、更には米国大統領選挙に関する虚偽情報・悪意の情報（フェイクニュース）による混乱・扇動（インフォデミック）に対し、欧州は厳しい態度をとり続けている。2020 年 12 月 3 日、欧州委員会はフェイクニュースによる政治活動過激化への対策として「欧州民主主義行動計画（European Democracy Action Plan）」（以下、行動計画）を発表した※268。行動計画は、「デジタル空間において、虚偽や悪意を排した事実に基づき、

自由でオープンな意見表明と討議を可能にし、欧州の民主主義を強化する」として、以下の3点について施策を講ずるとしている。
①自由で公正な選挙の推進
②メディアの自由と多元主義の強化
③虚偽・有害情報対策

①については、2016年、マイクロターゲティング技術を用いる選挙コンサルティング会社Cambridge Analytica Ltd.が英国の国民投票や米国大統領選挙に干渉したとされる事案や、英国のEU離脱国民投票をめぐる扇動、米国大統領選挙をめぐる扇動等の苦い経験から、政治広告への規制を行う、としている。

②については、加盟国においてジャーナリストの物理・サイバー両面の活動に対する外部の圧力が高まっているとし、ジャーナリスト（特に女性）の安全を確保し、メディアの多元性の強化を加盟国と推進する、としている。ここでいう外部の圧力・多元性の強化には、明言されないが、中国・ロシアの言論封殺や干渉に対する警戒があり、中国・ロシア資本によるメディアの所有や政治広告等に対する監視を強めるものと考えられる。

③については、欧州委員会が2019年に策定し、米国のプラットフォーム事業者が合意したSNS、ネット広告等における虚偽・有害情報に関する行動規範※269（Code of Practice on Disinformation、以下、行動規範）を強化するもので、欧州のデジタル市場戦略と重なる点で①②とは別の意味を持っている。行動計画では、現在義務化されていない行動規範を準規則化（co-regulatory framework）し、プラットフォーム事業者の監視を強める、としている。また行動規範の強化は、現在欧州委員会が策定中のデジタルプラットフォーム規制法「デジタルサービス法（Digital Services Act）」と整合させる、としている。同法法案は2020年12月15日、欧州議会に提出された※270。

「2.2.2（6）大統領選挙とフェイクニュースの混乱」で述べたように、2021年1月にTwitter社やFacebook社がTrump大統領（当時）のSNS利用を停止したことは、個人の言論を封じるような制裁を、法的権限を持たないプラットフォーム事業者が実施できるのかについて議論をまき起こした。これについて欧州は、消費者保護（域内市民保護）と競争確保の点から一貫してプラットフォーム事業者規制の立場をとっている。上記の行動計画やデジタルサービス法、及び並行して策定されているデジタル市場法（Digital Markets Act）※271により、欧州の描く公平・公正なデジタル市場の統制の形が見えてくると考えられる。

（3）GDPRの運用状況

GDPRの運用を行うEDPBや、各国のデータ保護委員会（DPA：Data Protection Authority）にとって、新型コロナウイルス感染対策は2020年度の重要課題となった。

（a）新型コロナウイルス対応

新型コロナウイルス対応における個人データ管理についてEDPBは2020年3月16日に声明を発表し、企業・医療機関における同意なしの個人データ取得等の例外はGDPRが包括的に規定していること、位置情報は匿名化を基本とするが、例外処理が必要な場合は策定中のeプライバシー法（ePrivacy Directive）に準拠すべきこと、を明記した※272。EDPBは続けて5月9日、位置情報及び接触追跡ツールに関するガイドライン※273、研究目的の健康情報処理に関するガイドライン※274を公開した。その後欧州各国も、個人の行動や新型コロナウイルス感染の有無等のデータ管理に関するガイドラインを相次いで公開した。

2020年後半以降は、新型コロナウイルスに対するワクチン開発への期待から、移動制限・入国制限を緩和するための「ワクチン接種証明」が注目され、議論が継続している。海外渡航に必要なワクチン接種証明書の発行はWHOの管轄であるが、WHOは新型コロナウイルスに対するワクチン接種証明書には慎重であるといわれる※275。理由としては、疫学的エビデンスの不足、ワクチン供給に関する不公平、関係法制の不備、個人情報保護やデータ管理等の規格の共通化等の課題が挙げられている。

こうした懸念をよそに、欧州委員会はEU域内の自由で安全な移動を保証するワクチン接種証明書（Digital Green Certificate）の検討を進め、2021年3月17日、関連法案を発表した※276。同法案では、この証明がワクチン非接種者への差別要因とならないように、感染していないことの証明、感染から回復したことの証明を含める、記録する個人情報は最小限にする等としている。また接種証明は、EUが承認したワクチンが対象となるが、加盟国が独自にワクチンを追加してもよいとしている。

その一方、接種証明を政府がどのように使うのか、例えばある国のワクチンは承認しないとした場合（実質的なEU域内入国制限になる）の政治リスク、接種しない人

が差別される倫理面のリスク、ワクチンの効果に差があった場合の対応、証明書発行手続きにおけるプライバシー保護の合意等、様々な懸念が表明されている※277。

またイタリア政府は、国内の新型コロナウイルス感染の高リスク地域への移動を緩和するため、独自の「ワクチンパスポート」の導入法案を準備している※278。2021年5月4日、イタリアのDPAであるGaranteが同法案について、個人データ処理に伴う人権、プライバシー保護上の検討不備があるとして懸念を表明した※279。

こうした懸念に対し、欧州評議会(Council of Europe)は2021年4月14日、加盟国政府の接種証明導入における人権保護ガイダンスを公開した※280。

(b)GDPRの運用

GDPRの実際の運用は2018年5月の発効から2年半以上を経過し、厳格さを増している。2020年7月16日、欧州司法裁判所は、2016年以来米国とEUの間の包括的データ移転の枠組みであった「プライバシーシールド」が無効である、すなわち、米国に移転された個人データの保護はGDPRと同等のレベルにない、との判断を示した※281。これはFacebookからの個人情報流出に反発したEU域内利用者の訴訟に対する判決である。同判決ではGDPRの標準契約条項(SCC:Standard Contractual Clauses)による代替策は有効である、とされたものの煩雑となり、EU域内のデータを米国のAIで分析する等のサービスに影響が出ると思われる。

GDPR違反の摘発については、調査によれば2020年1月28日から2021年1月28日までの制裁金総額(1億5,850万ユーロ、約206億円)は、それ以前の20ヵ月の総額に比べ40%増加した。その一方、違反届け出件数等は国により開きがあり、パンデミックで経営が厳しくなったBritish Airways Plcの制裁金(2018年に1億8,300万ポンド、約245億円を課された)が2020年10月、2,000万ポンド(約27億円)に減額される※282等、画一的な運用はされていないという※283。このほか、2020年度に高額の制裁金が課された事例としては以下のものがある。

2020年7月13日、前出のGaranteは電話事業者Wind Tre S.p.A.に対し、ダイレクトマーケティングに関する利用者の同意のとり方についてGDPR違反があったとし、1,670万ユーロ(約21.7億円)の制裁金を課すと公表した※284。

同年10月2日、ハンブルク市のDPAであるThe Hamburg Commissioner for Data Protection and Freedom of Informationは、衣料小売企業H&M Hennes & Mauritz Online Shop A.B. & Co. KGに対し、従業員数百人の病歴等を含むプライベートな情報の登録を少なくとも2014年以来強制し、同社マネージャー50人がこの情報にアクセス、評価に利用していたとし、3,526万ユーロ(約45億8,300万円)の制裁金を課した※285。2019年にフランスのDPAであるCNIL(Commission nationalede l'informatique et des libertes)がGDPR発効直後、Google LLCに課した制裁金5,000万ユーロ(約65億円)に次ぐ高額となった※286。

更に10月30日、英国のDPAであるICO(Information Commissioner's Office)はMarriotto International Inc.(以下、Marriotto社)に対し、傘下のStarwood Hotels and Resorts Worldwide Inc.(以下、Starwood社)における延べ3億3,900万人に及ぶ顧客情報流出について、1,840万ポンド(約25億円)の制裁金を課した※287。本事案は英国のEU離脱前の2018年に発覚してGDPR違反の査察対象となり、ICOの調査の結果、Marriotto社が2015～2016年にStarwood社を買収した時点のセキュリティ体制整備に問題があったとしたが、Marriotto社による申し立てやパンデミックによる経営悪化の影響も加味して、当初9,920万ポンド(約135億円)とされた制裁金は減額された。この経緯は前述のBritish Airways Plcの事案でも同様である。

(4)新たなサイバーセキュリティ戦略

欧州委員会は2020年12月10日、「誰もが安全なデジタル生活を送る」ために、以下を柱とする「デジタル時代のサイバーセキュリティ戦略」を発表した※288。

- 基盤サービスとつながるモノのセキュリティ確保
- 主要なサイバー攻撃への対応能力強化
- 世界のパートナーとの連携

大方針としては従来の戦略と大きな差があるように感じられないが、基盤サービスとしての医療、エネルギー、交通等の重視、つながる機器を守るためのサプライチェーン重視、それに関わる海外パートナーとの連携、コロナ禍からのリカバリー施策としてのセキュリティ投資強化が主眼であると思われる※289。

更に欧州委員会は翌11日、欧州議会の承認を受け、上記戦略を推進する組織Cybersecurity Competence Center and Networkをブカレストに設置することを発表した※290。同組織はENISAとは別に、EUのデジタル投

資・研究投資ファンドである Digital Europe Programme、Horizon Europe を財源として中長期的なサイバーセキュリティ投資を行うとしている。同組織の提案は 2018 年時点で行われており[※291]、EU 域内産業のデジタル化・技術革新におけるサイバーセキュリティ重視の姿勢が感じられる。

(5) 重要インフラに関するセキュリティの状況

2016 年に発効し、ENISA が実践を統括する NIS 指令は、重要インフラセクターの共通なセキュリティ指針となっているが、以下では医療セクター・通信セクターに向けた ENISA の活動、及び関連する関係諸国の動向を紹介する。

(a) 医療セクターのセキュリティ

医療セクターのセキュリティ確保は 2020 年、大きな焦点となったが、ENISA は同年 2 月、医療機器・システム調達におけるセキュリティ確保のガイドラインを公開した[※292]。機器調達の計画・実施・運用におけるセキュリティについて、29 個のプラクティスが紹介されている。また 2021 年 1 月 18 日、医療クラウドのセキュリティに関する報告書が公開された[※293]。同報告書では、医療のクラウド化で対応すべき電子健康データ（EHR：Electronic Health Record）の収集と管理、遠隔治療、医療機器操作に対するセキュリティリスクアセスメント結果が示されている。

欧州における医療のデジタル化（eHealth）は、エストニアで先進サービスが試みられる一方、ドイツ・フランスでは EHR の扱いに慎重であり、対応は一様ではないが、コロナ禍や医療への AI 利用等により、今後デジタル化が加速する可能性がある[※294]。なお、ENISA は 2020 年 12 月 15 日、AI のセキュリティに関するエコシステムと脅威に関する報告書を公開した[※295]。機械学習を用いる AI の設計・開発・運用のライフサイクルに沿って、関係するエコシステム・サプライチェーンで生じ得る脅威の分析を行っている。

(b) 通信セクターのセキュリティ

2020 年 12 月 14 日、ENISA は 5G ネットワークに関する脅威分析の改訂を行った[※296]。公開された脆弱性情報等に基づき、2019 年 11 月発行のレポートを改訂したものである。続いて 2021 年 2 月 24 日、3GPP[※297] が規定した 5G のセキュリティ管理策に関する報告書を公開した[※298]。5G 機器ベンダ・サービス事業者（通信キャリア）・政府機関への規格実装のプラクティスを示し、5G 規格の複雑さへの対処に注意を促している。

「2.2.3 (2) (a) 感染状況」や「情報セキュリティ白書 2020」の「2.2.3 欧州の政策」で述べたとおり、2020 年、パンデミックに関する情報開示や人権侵害等の問題により欧州各国と中国との関係は冷却し、米国の制裁措置にならい、キャリア通信網からの中国ベンダ機器排除の動きが加速した。ただし、2021 年 4 月の時点では、各国の対応に濃淡が見える。

最も厳しい対応をしたのが英国である。英国政府は 2020 年 7 月 14 日、Huawei Technologies Co., Ltd.（以下、Huawei 社）、ZTE Corporation の 5G 機器の新規調達を同年 12 月末から禁じ、既存の中国製機器も 2027 年までに撤去することとした[※299]。更に政府は 11 月 24 日、通信事業者が調達する機器やベンダに対するセキュリティ要件を厳格化する法案（Telecommunication Security Bill）を議会に提出した[※300]。同法案では「ハイリスクベンダ」の排除、通信事業者のセキュリティ監査の強化、違反時のペナルティ等が明記されている。スウェーデン・フランスもこのような排除を前提とする対応を行っている。

一方ドイツは、どのベンダも 5G 機器調達から排除しないという方針を維持している。2020 年 12 月 16 日、ドイツ政府は、国内の IT セキュリティ基本法である「IT セキュリティ法 2.0」を閣議決定した[※301]。同法案には、重要インフラ事業者の調達における監督官庁の認可制度等、セキュリティ規制の強化が盛り込まれる一方、ハイリスクベンダの排除は含めず、調達可否は監督官庁の査閲に委ねられた。過去においてドイツの通信事業者が Huawei 社の機器を運用してきた経緯によると思われるが、排除を前提とする同盟国等とのデジタルプラットフォーム統合に関する軋轢、あるいは EU が希望する北大西洋条約機構（NATO：North Atlantic Treaty Organization）への米国のコミットメント強化に対する影響が懸念されている[※302]。

2.2.4 アジア太平洋地域でのCSIRTの動向

アジア太平洋地域の多くの国で、各国のインシデント対応連携の窓口となる National CSIRT が既に設立され運用されている。ここ数年は、サイバーセキュリティ戦略や新たな法律によって、National CSIRT 及び所管省庁の権限を強化したり、役割を明文化したりする動きが継続している。本項では、アジア太平洋地域におけ

るCSIRTの機能強化やインシデント対応の新たな取り組みに関する動き、CSIRT間の相互連携の実態について述べる。

(1) CSIRTの機能強化の動き

アジア太平洋地域における各国・地域のCSIRTの機能強化の動きについて述べる。

(a) オーストラリア

2020年8月6日、オーストラリアの内務省(Department of Home Affairs)から2020年版のサイバーセキュリティ戦略[※303]が発表された。これは2016年に発表された同戦略の更新版である。国民生活や企業活動のために安心安全に利用できるサイバー空間を創造するため、向こう10年間で16億7,000万豪ドル(約1,300億円余り)を計上することが盛り込まれている。National CSIRTの機能を担うACSC(Australian Cyber Security Centre)[※304]にも、そこから多くの予算が割り当てられ、機能が更に拡充される計画である。例えば、海外から同国を狙うサイバー犯罪の対策強化、重要インフラ事業者におけるセキュリティアセスメント及び対策の徹底、主に女性を対象としたサイバーセキュリティ教育やトレーニング機会の創設等にACSCが取り組むとされている。

(b) シンガポール

National CSIRTであるSingCERT[※305]を管轄するCSA(Cyber Security Agency:サイバーセキュリティ庁)[※306]は、2020年10月6日に「Singapore's Safer Cyberspace Masterplan 2020[※307]」を公開した。この文書には、「核となるデジタルインフラの保護」「サイバー空間での活動の安全性の確保」及び「サイバーセキュリティについて知識を持つ人たちの活躍」という三つの大目標と、それに付随する計11項目の取り組みが記載されている。例えば、「サイバー空間での活動の安全性の確保」の中では、AI(人工知能)を活用し、サイバー空間での不正な行為を迅速に検知し対応することが挙げられている。具体的には、AIを活用して情報を集約分析し、より重要度の高いインシデントをトリアージする機能を備えたサイバー・フュージョン・プラットフォームをCSAが創設する計画である。またIoTの分野では、グローバルな脅威動向や脆弱性の情報をモニタリングし攻撃の早期検知及び対応を行うために、CSAがIoTの脅威情報を関係組織と共有し分析するIoT脅威分析プラットフォームの運営が計画されている。関係組織と協同して分析することで、IoT機器に対する大規模な攻撃を事前に検知し、影響を把握することが可能になるという。それらに加えて、サイバー衛生[※308]に関するポータルサイトの作成、国内の中小企業に対するサイバーセキュリティ対策の支援、啓発活動の充実、5Gセキュリティの推進等にCSAが取り組むとされている。

(c) マレーシア

2020年10月、マレーシアのNACSA(National Cyber Security Agency:国家サイバーセキュリティ庁)[※309]は2020年から2024年にかけてのサイバーセキュリティ戦略[※310]を公開した。この戦略には、サイバーセキュリティに関する「ガバナンスとマネジメントの効率化」「法制度設計と施行の強化」「世界に通用するイノベーション、技術、研究、産業の促進」「能力開発、啓発、教育の促進」及び「国際連携」という五つの柱が掲げられている。「国際連携」の項では、国際連合やASEAN等の多国間のサイバーセキュリティに関する連携に積極的に参加し貢献を続けると明記している。この中には、National CSIRTの役割を担うCyberSecurity Malaysia[※311]が2020年現在議長を務めるAPCERTや、事務局を務めるOIC-CERT(Organisation of The Islamic Cooperation – Computer Emergency Response Teams)[※312]での活動も明記されており、今後もこれらのコミュニティにおける同組織のリーダーシップが期待される。

(d) 韓国

韓国のKrCERT/CC[※313]は、毎年国内のセキュリティ関連企業と協力し、今後猛威を振るう脅威を予測して「7大サイバー脅威」として公開している。2020年は、初めての試みとしてアジア太平洋地域のCSIRTに協力を募り、呼びかけに応じたAusCERT(オーストラリア)[※314]、CERT-In(インド)[※315]、Sri Lanka CERT|CC(スリランカ)[※316]と共同で、12月に「Cyber Threat Signal 2021[※317]」を公開した。この中で、AusCERTはEmotetを中心としたウイルスのばらまきキャンペーンを脅威の一つに挙げ、CERT-InはVPN機器等リモートワーク環境に対する攻撃が増える可能性を指摘している。またKrCERT/CCは企業から流出した情報のダークウェブ上での売買について、Sri Lanka CERT|CCは巧妙化するビジネスメール詐欺(BEC:Business Email Compromise)について警鐘を鳴らしている。

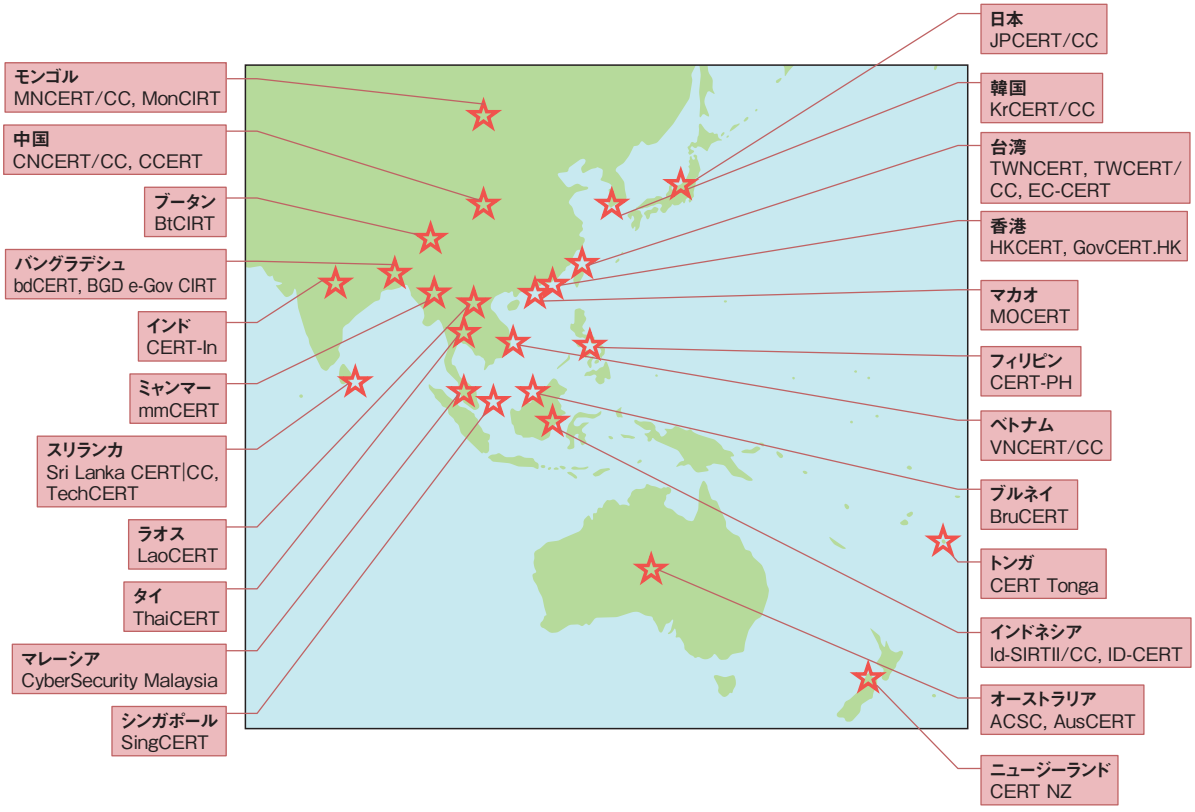
(2) アジア太平洋地域の CSIRT 間連携

アジア太平洋地域全体の CSIRT からなるコミュニティとして、APCERT（Asia Pacific Computer Emergency Response Team：アジア太平洋コンピュータ緊急対応チーム）[※318] があり、地域内で発生したインシデント対応における連携の円滑化や、サイバー脅威等に関する情報共有・技術交流の推進を目的に活動している。2003年の設立当初、参加メンバーは 12 の国・経済地域の 15 チームだったが、地域内で National CSIRT の立ち上げが進んだことや、CSIRT コミュニティへの参加を通じた情報共有等の重要性が高まったことから年々メンバーが増え、2020 年には南太平洋地域から初めてトンガの CERT Tonga [※319]、並びにフィリピンの CERT-PH [※320] 等が新たに加わった。2021 年 3 月末現在、23 の国･経済地域の 33 チームが、オペレーショナルメンバーとなっている（図 2-2-1）。

JPCERT/CC は、2003 年の APCERT 設立当初から事務局を務め、運営委員会の一員として組織運営を支えている。また、JPCERT/CC が主導するネットワーク定点観測共同プロジェクト「TSUBAME」に参加する APCERT メンバーも多く、APCERT 内にワーキンググループを設けて、センサーを用いたサイバー脅威動向の観測や情報共有を推進している。2021 年 3 月末現在、TSUBAME には APCERT メンバーを中心に 19 の国･経済地域から 24 チームが参加し、観測結果を共有している[※321]。

APCERT の主な活動は、年次サイバー演習の実施、年次報告書の発行及び年次会合の開催である。2020 年のサイバー演習は、「Banker Doubles Down on Miner（仮想通貨と金融機関）」をテーマに実施された[※322]。同演習には、APCERT のオペレーショナルメンバーのうち合計 19 の国・経済地域から 25 チームが参加した。年次報告書は、APCERT 全体の活動に加えて各チームの組織概要や、対応したインシデント統計等をまとめた文書で、Web サイトで公開されている[※323]。2020 年の年次会合は、新型コロナウイルス感染拡大の影響により、9 月に初めてオンラインで開催された。2019 年から議長を務めるマレーシアの CyberSecurity Malaysia が議長に、中国の CNCERT/CC [※324] が副議長にそれぞれ再選された。

このほか、APCERT では能力開発の取り組みとして、電話会議システムを利用してインシデント対応に関するノウハウを教えるオンライントレーニングを 2014 年以来継続している。新型コロナウイルス感染拡大が続き、対面で



■図 2-2-1　APCERT オペレーショナルメンバー（2021 年 3 月末現在）

のトレーニング開催が困難な中でも、こうしたオンラインで連携する取り組みを継続している。

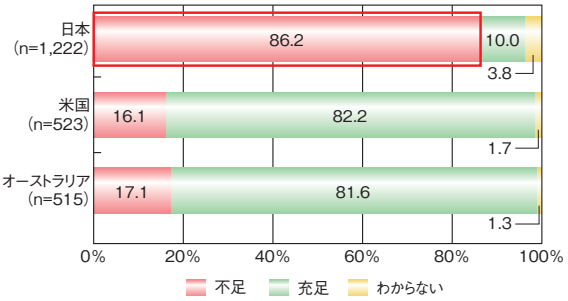
また、日本政府が出資してタイのバンコクに設立された AJCCBC（ASEAN Japan Cybersecurity Capacity Building Center：日 ASEAN サイバーセキュリティ能力構築センター）※325 は、2020 年 12 月に「Cyber SEA Game」と呼ばれる CTF イベントをオンラインで開催した※326。

その他のアジア太平洋地域のサイバーセキュリティ関連イベントの多くが、各国の National CSIRT が主催するカンファレンスを含め、2020 年はオンライン形式に移行して実施された。対面の会議や情報交換の機会が制限されている状況下でも、こうした場をとおして CSIRT 間の連携は継続して行われている。

2020 年中に JPCERT/CC に寄せられたインシデント報告件数は、特にフィッシングサイトに関するものを中心として、前年より高い水準で推移した。また、その内訳を見ると、インシデント拡大防止を目的とした調整のため、海外の CSIRT 等に通知を行ったケースも多かった※327。このようなインシデントへの対応を効果的に進めていくためには、諸外国や特に近隣地域の CSIRT と結束力を高めて連携していくことが必要であり、CSIRT コミュニティをとおした協力が更に推進されることが期待される。

2.3 情報セキュリティ人材の現状と育成

国内のサイバーセキュリティに関わる人材は質的にも量的にも不足しており、人材育成は各界が協力して解決すべき問題である。教育の充実、高度な人材の育成・確保、セキュリティ人材が将来にわたって活躍できる社会環境の整備等、様々な課題が挙げられている。本節では、セキュリティ人材の現状と、産学官における人材育成の取り組みについて述べる。



■図 2-3-1　セキュリティ対策に従事する人材の過不足感
(出典)NRI セキュアテクノロジーズ株式会社「NRI Secure Insight 2020※329」を基に IPA が編集

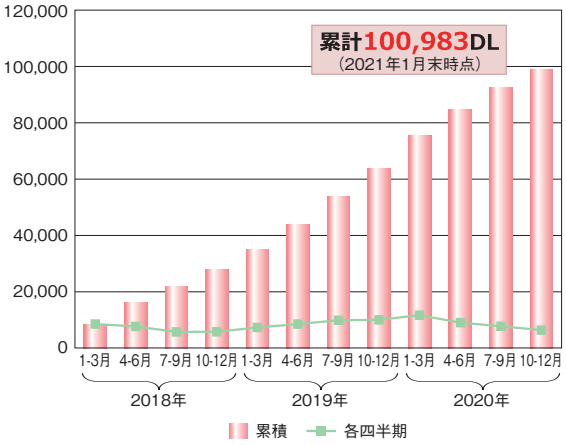
2.3.1 情報セキュリティ人材の状況

ここ数年来、政府や民間の組織において国内のセキュリティ人材育成のための活動が行われてきた。ユーザ企業、IT ベンダ・セキュリティベンダによりセキュリティ関連タスクの概念整理が行われ、ユーザ企業におけるセキュリティ体制については、経営層、戦略マネジメント層、実務者層・技術者層等に整理された。

2018 年度から、実際に人材育成を進める活動として、セキュリティ人材の役割定義に紐付くタスク・スキルの洗い出しを行うとともに、具体的に人材育成を行う試みの有効性に関する検討が行われてきている。

2020 年度においては、コロナ禍によるテレワークや DX の推進に拍車がかかる中、求められるセキュリティ人材の状況にも変化があり、ビジネスあるいは経営の観点でセキュリティ対策を理解し、実践する能力を持った人材への関心が高まりつつある。

このような背景を踏まえて、各所で計画・実施されている活動の概要を紹介する。



【参考】上場企業数　第一部　2,157社　第二部　488社　(日本取引所グループ公表 2019年12月17日時点)

■図 2-3-2　サイバーセキュリティ経営ガイドライン V2.0 のダウンロード数推移
(出典)経済産業省「事務局説明資料※331」(第 7 回 産業サイバーセキュリティ研究会 ワーキンググループ 2(経営・人材・国際) 資料 3)を基に IPA が編集

(1) セキュリティ人材不足に関する認識

米国 NIST の NICE(National Initiative for Cybersecurity Education)において発行されたニュースレターによると、セキュリティ関連職種の雇用需要は、2018 年から 2020 年にかけて、約 71 万 6,000 人から 92 万 3,000 人と、約 29% も増加しており、セキュリティ人材の供給は順調に成長しているにも関わらず、充足できていない雇用は 62% にまで達している状況である※328。日本はそのような状況にある米国と比較しても、セキュリティ人材の不足感が更に大きく、セキュリティ人材が不足している状況である(図 2-3-1)。

「サイバーセキュリティ経営ガイドライン」の普及(図 2-3-2)や、一般社団法人日本経済団体連合会(以下、経団連)の「経団連サイバーセキュリティ経営宣言※330」等により、サイバーセキュリティが経営課題であることが徐々に浸透していることから、様々な組織においてセキュリティ関連の役割を担う人材への需要は更に増えていると推定される。

NISC のまとめによれば、どのような種別の人材が不足しているかについて、2018 年では、1 位は「ログを監視・分析して、危険な兆候をいち早く察知できる」、2 位が「セキュリティ戦略・企画を策定する人」であったが、2019 年、2020 年は、1 位が「セキュリティ戦略・企画を策定する人」となっており、不足する人材の分野が、実務者層・技術者層から戦略・企画を担当する人材に変わってきている(次ページ表 2-3-1)。

	2018 年	2019 年	2020 年
1 位	ログを監視・分析して、危険な兆候をいち早く察知できる 57.0%	セキュリティ戦略・企画を策定する人 47.2%	セキュリティ戦略・企画を策定する人
2 位	セキュリティ戦略・企画を策定する 52.7%	セキュリティリスクを評価・監査する人 34.1%	セキュリティリスクを評価・監査する人
3 位	セキュリティインシデントへの対応・指揮ができる 44.1%	ログを監視・分析する人 34.1%	ログを監視・分析する人

セキュリティ対策にあたる実務者層・技術者層
戦略・企画を担当する人材
(データ出所)NRI セキュアテクノロジーズ㈱「企業における情報セキュリティ実態調査」より NISC 作成

■表 2-3-1　不足している人材の種別
(出典)NISC「人材の確保、育成、活躍促進に向けた今後の検討の方向性について(全体像)※332」を基に IPA が編集

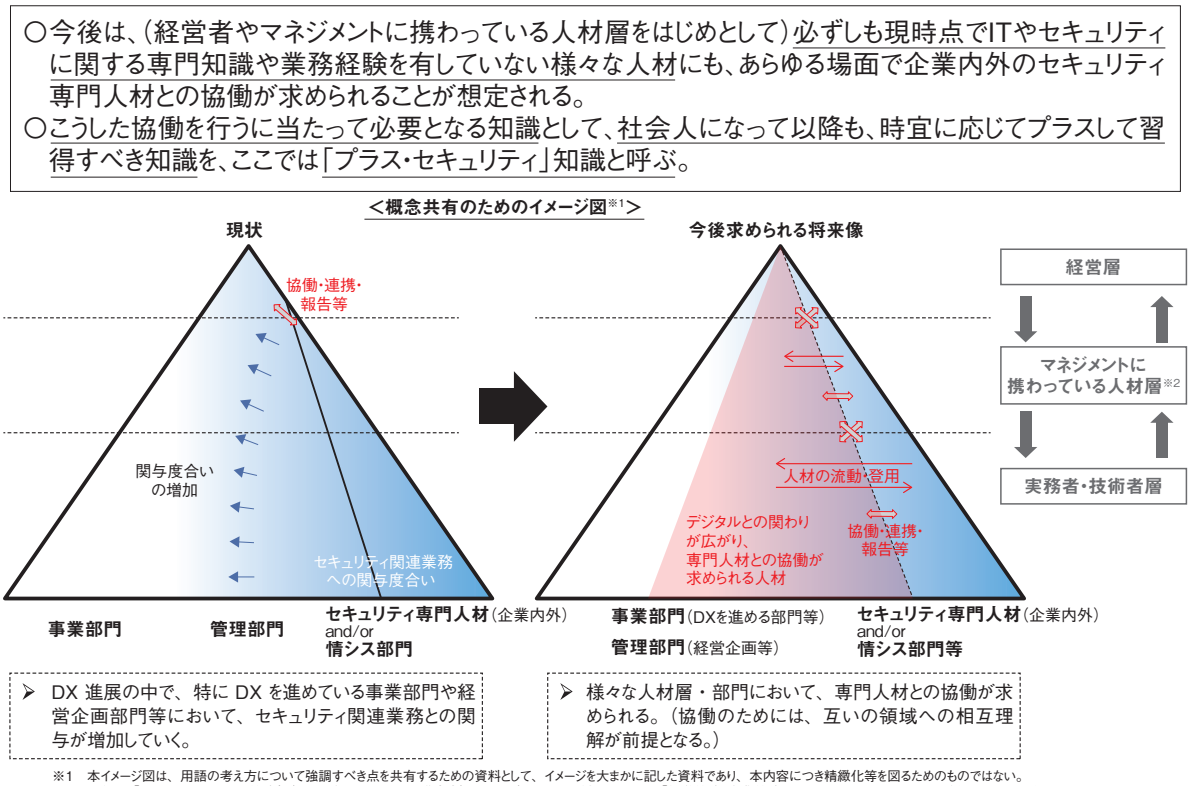
経済産業省の「デジタルトランスフォーメーションに向けた研究会」による「DX レポート※333」では、レポート中の「2025 年の崖」を克服する DX 実現シナリオにより変革された際の展望として、ユーザ企業とベンダ企業間の IT 人材分布は現在の 3:7 から、欧州並みの 5:5 になるとしている。

実際、株式会社デンソー※334、大和総研グループ※335、住友化学株式会社※336 等先進的なユーザ企業では、従来、情報システム部門を本社機構から切り離し情報子会社としていた体制を変更し、本社へ吸収・合併する事例が出始めている。

DX 推進とともに IT 人材の所属が変わり、IT ベンダ、情報子会社から、ユーザ企業へのシフトが起こりつつある。今後はユーザ企業も含め、セキュリティ人材の育成を考慮すべきである。

(2) NISC の取り組み

NISC では、2020 年 7 月に「普及啓発・人材育成専門調査会(第 13 回会合)」を開催し、DX 時代におけるサイバーセキュリティ人材の確保、育成、活躍の促進に係る政策課題について検討を始めた。DX の進展が予想される中、DX と同時にサイバーセキュリティ対策を組み込んでいくこと(DX with Cybersecurity)が求められているとしている。検討すべき三つの政策課題の一つとして、「DX に必要な『プラス・セキュリティ』知識を補充できる環境・人材育成の推進」を掲げており、2018 年の「サイバーセキュリティ戦略※337」で提言した戦略マネジメント層の確保・育成の一つのアプローチと考えられるとし



※1　本イメージ図は、用語の考え方について強調すべき点を共有するための資料として、イメージを大まかに記した資料であり、本内容につき精緻化等を図るためのものではない。
※2　現行の「サイバーセキュリティ戦略」(2018 年 7 月 27 日閣議決定)によれば、こうした人材層において、「経営戦略、事業戦略におけるサイバーセキュリティに係るリスクを認識し、経営層の方針を踏まえた対策を立案し、実務者・技術者を指導できる人材」が「戦略マネジメント層」と定義されている。

■図 2-3-3　「プラス・セキュリティ」知識の考え方
(出典)NISC「政策課題2 DX に必要な『プラス・セキュリティ』知識を補充できる環境・人材育成の推進※338」

ている。

NISC はまた、「プラス・セキュリティ」の考え方の概念的な表現として、セキュリティ専門人材と事業部門においてセキュリティ関連業務に関わるプラス・セキュリティの知識・役割を持つ人材の関係を示しており、相互に協働が必要であるとしている（前ページ図 2-3-3）。

NISC では、DX with cybersecurity を進めていく上で必要なプラス・セキュリティ知識を持った人材を育成するために必要な教育カリキュラムの検討を進めモデル化するとしている。また、企業において DX に対応した体制構築を行う際の参考となるように、ITSS+（セキュリティ領域）[※339] で定義されているセキュリティ関連タスクを担う分野において、どのようなプラス・セキュリティ知識が必要となり得るかを示している（図 2-3-4）。

これらの検討結果は、次期サイバーセキュリティ戦略に盛り込まれ、推進されるものと思われる。

(3) 経済産業省の取り組み

経済産業省のセキュリティ人材育成の取り組みについて述べる。

(a) 産業サイバーセキュリティ研究会 WG2（経営・人材・国際）

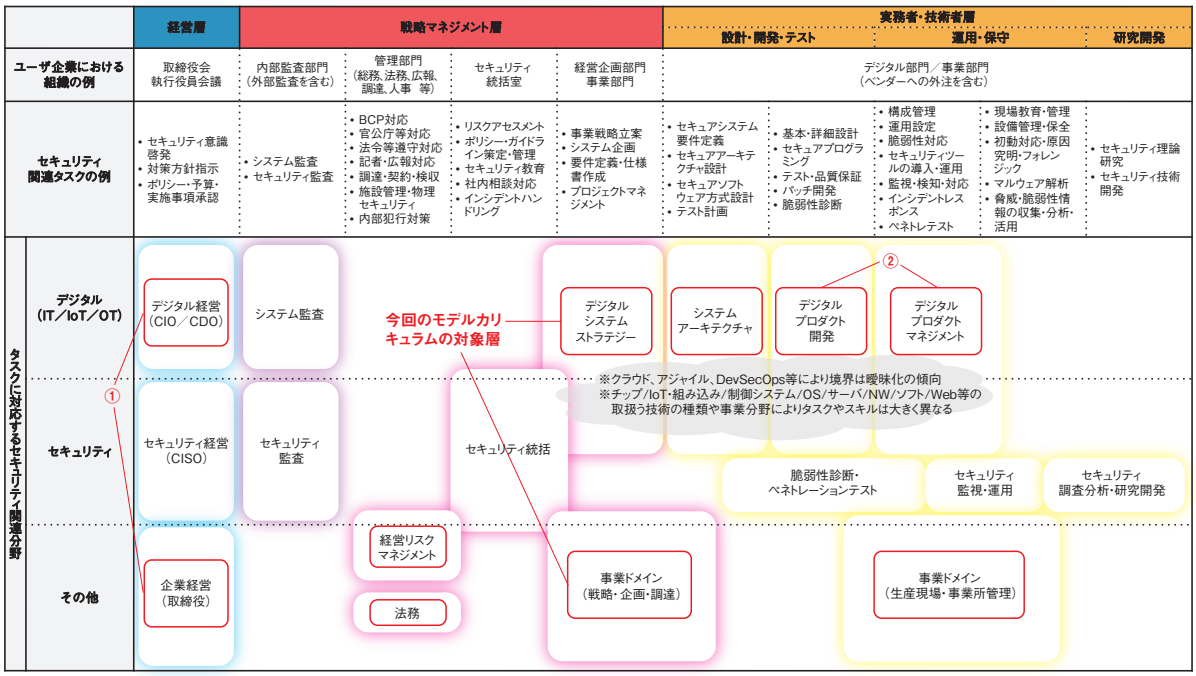
経済産業省では、産業サイバーセキュリティ研究会において、サイバー・フィジカル・セキュリティ対策フレームワークを軸として、各種取り組みを整理している（次ページ図 2-3-5）。

人材育成に関わる対策として、「サイバーセキュリティ経営ガイドライン」をより具体的に活用するための支援ツールの拡充並びに、産学官連携を推し進める取り組みが行われており、「サイバーセキュリティ人材育成・活躍促進パッケージ」として、以下の三つの施策が進められている。

①「セキュリティ人材活躍モデル」の作成
②戦略マネジメント層の育成
③産学官の連携強化

「セキュリティ人材活躍モデル」の作成に関しては、経済産業省では、2018 年より関連有識者会合にて検討を重ね、2020 年 4 月以降は「セキュリティ経営・人材確保の在り方検討タスクフォース」において継続して検討が進められている。その成果として、2020 年 9 月「サイバーセキュリティ経営ガイドライン Ver2.0」の付録 F として「サイバーセキュリティ体制構築・人材確保の手引き 第 1 版」が、2021 年 4 月にはその改訂版として第 1.1 版が公開されている[※58]（「2.3.1 (3) (b)『サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版』の概要」参照）。

戦略マネジメント層の育成に関しては、2018 年より

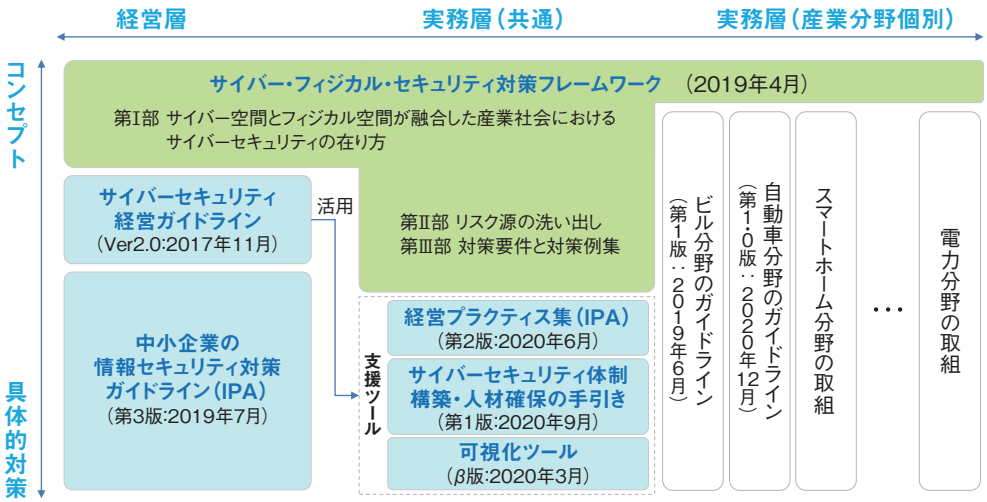


■図 2-3-4　プラス・セキュリティ知識が必要となり得る分野
（出典）NISC「政策課題2 DX に必要な『プラス・セキュリティ』知識を補充できる環境・人材育成の推進」

サイバー・フィジカル・セキュリティ対策フレームワークを軸とした各種取組

●「サイバー・フィジカル・セキュリティ対策フレームワーク」では、Society5.0における産業社会でのセキュリティ対策の全体枠組みを提示。
●全体の枠組みに沿って、対象者や具体的な対策を整理し、『サイバーセキュリティ経営ガイドライン』や産業分野別のガイドラインなどの実践的なガイドラインを整備。

＜各種取組の大まかな関係＞



■図 2-3-5 サイバー・フィジカル・セキュリティ対策フレームワークを軸とした各種取り組み
（出典）経済産業省「事務局説明資料」（第７回 産業サイバーセキュリティ研究会 ワーキンググループ２（経営・人材・国際）資料３）

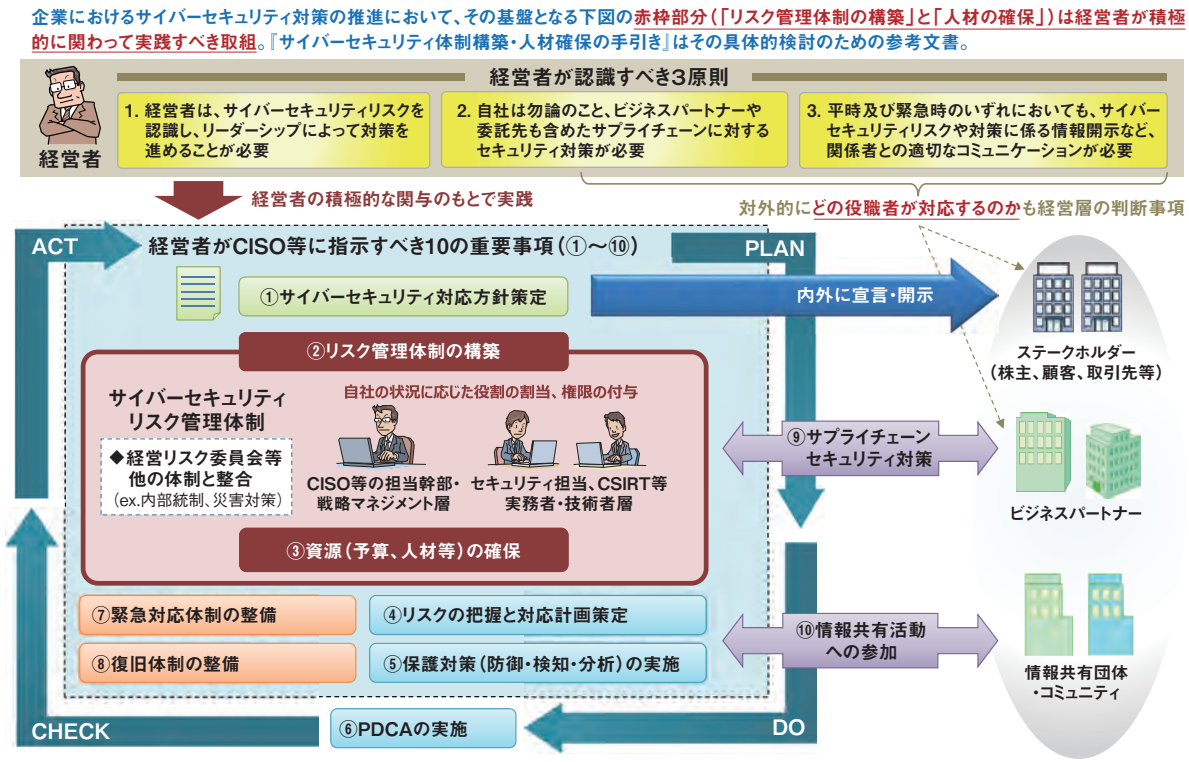
IPA ICSCoEにおいて「戦略マネジメント系セミナー※340」を毎年開催している（「2.3.2 産業サイバーセキュリティセンター」参照）。また、東京工業大学 CUMOT において「サイバーセキュリティ経営戦略コース※341」が開講されている（「2.3.4 (5) サイバーセキュリティ経営戦略コース」参照）。更に、NISC では、情報セキュリティ大学院大学の協力により、「DX を推進する部門の責任者あるいは主要な役割を担う管理職」を対象層としてモデルカリキュラム開発を試行している。情報セキュリティ大学院大学では、開発カリキュラムをベースとし、DX 推進者を対象とした「DX with Cybersecurity 3日間教育コース※342」を実施した。2021 年度も同様に開催されるとともに、更にモデルカリキュラムをベースとして強化が進められる。

産学官の連携強化に関しては、経済産業省、IPA、JPCERT/CC 及び業界団体が国立高専機構と連携し、高専生の専攻（セキュリティ、IT、その他（機械、電気等））に応じた教育コンテンツの提供や講師の派遣等、産学官連携の具体化を進めている（「2.3.4 情報セキュリティ人材育成のための活動」参照）。また、地域におけるセキュリティ人材育成については、地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ活動（地域 SECUNITY）の中で、地域ごとに普及活動、人材育成を実施している（「2.4.2 中小企業に向けた情報セキュリティ支援策」参照）。

(b)「サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版」の概要

「サイバーセキュリティ経営ガイドライン」では、サイバーセキュリティについて経営者が認識すべき3原則を提示し、経営者が CISO 等に指示すべき重要 10 項目を説明している。その付属書である「サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版」（以下、手引き）では、重要 10 項目のうち、以下の二つの項目にフォーカスし、解説を行っている（次ページ図 2-3-6）。
②リスク管理体制の構築（以下、指示 2）
③資源（予算、人材等）の確保（以下、指示 3）

これは、サイバーセキュリティが経営課題であるという意識が浸透し、多くの企業が「サイバーセキュリティ経営ガイドライン」の実践に取り組む中で、管理体制の構築をどのように行えばよいか、また、資源人材の確保をどうすれば良いかが分からないという意見が多く寄せられたことによる。また、この二つの重要事項は、経営者の意思決定が求められる項目だからである。



■図 2-3-6 「サイバーセキュリティ体制構築・人材確保の手引き」のサイバーセキュリティ経営ガイドラインにおける位置付け
（出典）経済産業省・IPA「付録 F（概要版）サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版※343」

手引きにおける検討のポイントでは、指示 2 について、以下が挙げられている。

- 経営者のリーダーシップのもとでのセキュリティ機能と体制の検討
- セキュリティ統括機能の検討
- セキュリティ関連タスクを担う部門・関係会社の特定・責任明瞭化（ITSS+（セキュリティ領域）を参考にし、外部委託先の選定では情報セキュリティサービス基準適合サービスリスト等を活用）

指示 3 については、以下が挙げられている。

- 「セキュリティ人材」の確保（まずは、セキュリティ統括人材の確保を目指す。）
- 「プラス・セキュリティ」の取組推進
- 教育プログラム・試験・資格等の活用と人材育成計画の検討

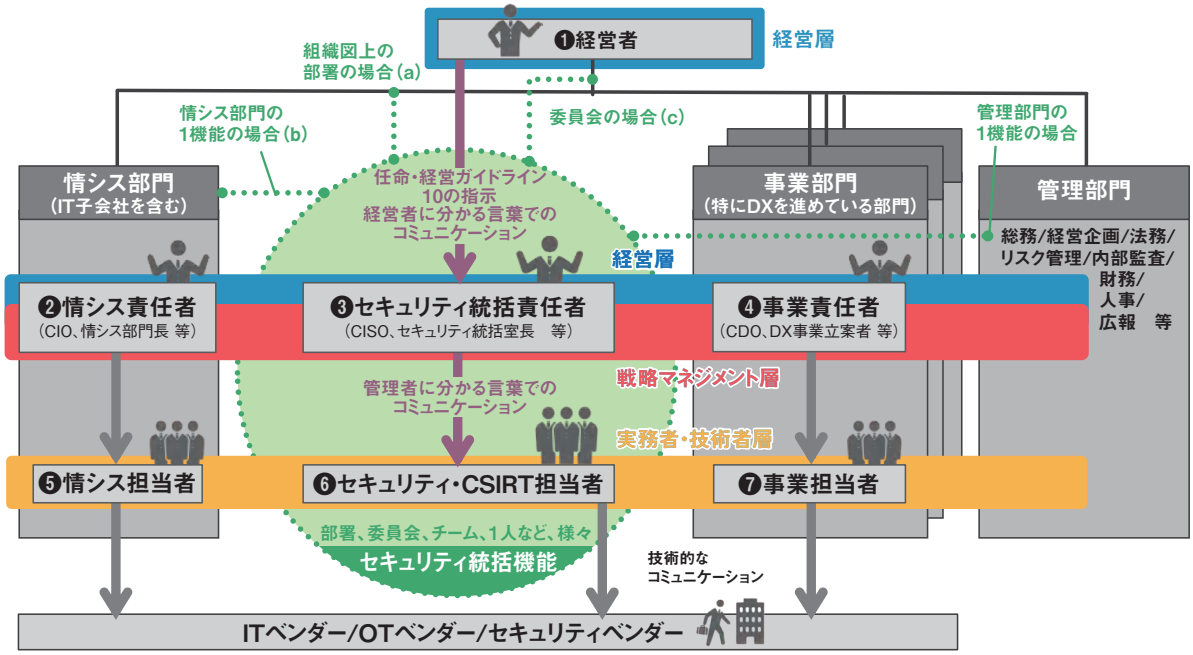
それらのポイントを理解し、利用する上で大事な概念として以下がある。

- セキュリティ統括機能
- ITSS+（セキュリティ領域）
- プラス・セキュリティ

セキュリティ統括機能は、セキュリティ対策及びインシデント対応において、CISO や経営層を補佐してセキュリティ対策を組織横断的に統括することにより、企業におけるリスクマネジメント活動の一部を担うとしている。2018 年ごろから「セキュリティ統括室」といった名称を明示した部署を設ける企業が出てきているが、手引きでは、セキュリティ統括は、「機能」であって「組織」として設置しなくてもよく、状況に応じて、組織に最適な形態を取るべきだとしている（次ページ図 2-3-7）。

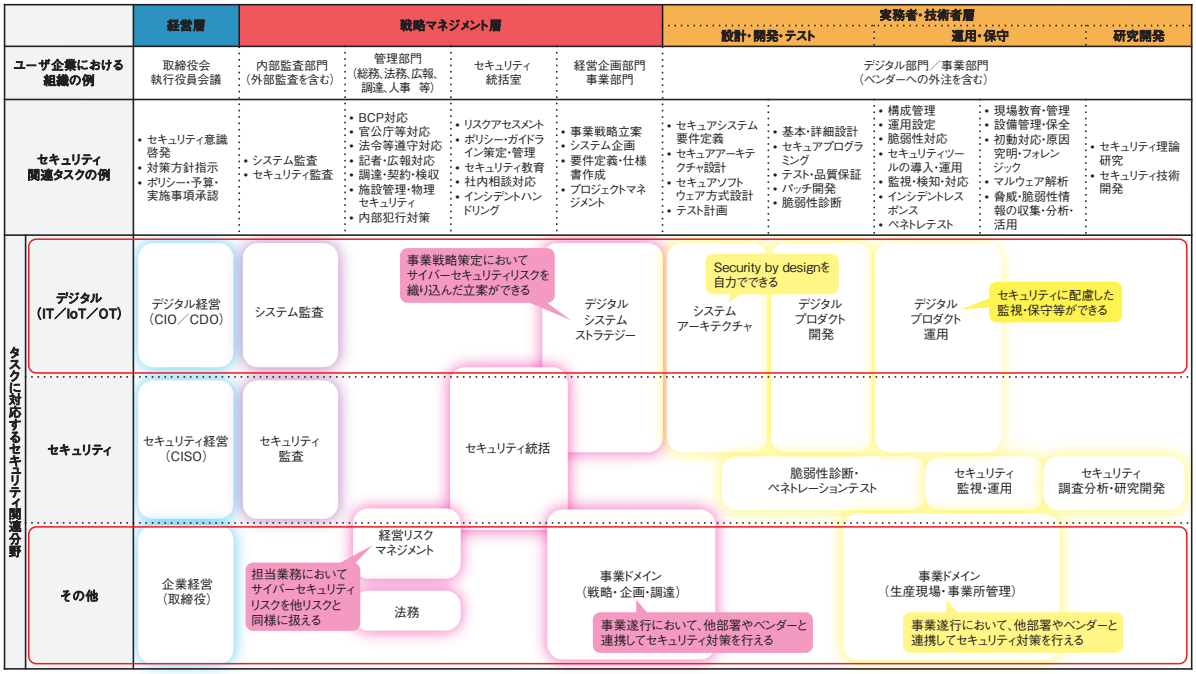
ITSS+（セキュリティ領域）は、企業のセキュリティ対策に必要となる関連業務を 17 分野に整理しており、それぞれの分野に求められるセキュリティ知識・スキルの概念をまとめることで、企業でセキュリティ体制を構築する際の業務役割を検討する際に利用できる。セキュリティの専門性の高い分野だけでなく、経営層や法務部門、事業ドメインまで、サイバーセキュリティ対策に関わる幅広い領域を網羅している（次ページ図 2-3-8）。

手引きでは、プラス・セキュリティを、「（セキュリティ対策を本務としていないが）自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態」と定義している。また、「プラス・セキュリティ」人材を業務担当者と別に確保する必要はなく、既存の



■図 2-3-7　セキュリティ統括機能のイメージ
(出典)経済産業省・IPA「付録 F(概要版)サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版」

ITSS+(セキュリティ領域)(赤枠が「プラス・セキュリティ」の分野)



■図 2-3-8　ITSS+(セキュリティ領域)
(出典)経済産業省・IPA「付録 F(概要版)サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版」

業務担当者がサイバーセキュリティの知識・スキルを習得し、実践することを通じて役割を担うとしている。また、プラス・セキュリティは、DX の取り組みの有無に関わりなく、IT を活用するすべての企業に必要であるとしている。

今回、手引きにおいて、指示 2 及び指示 3 の実践を担当する戦略マネジメント層が、セキュリティ統括人材とプラス・セキュリティ人材という二つの類型で整理された。この方針は、DX の活用・推進において必要なセキュリティを推進することを NISC で「DX with Cybersecurity」と呼称し、プラス・セキュリティ知識が必要としていることとも整合が取れている。

(4) NICE Framework の改訂

NIST のサイバーセキュリティ人材育成イニシアティブ NICE（National Initiative for Cybersecurity Education）では、米国のセキュリティ人材育成のため枠組として、Workforce Framework for Cybersecurity（以下、NICE Framework）を 2012 年から発行しており、第 3 版は 2017 年 8 月に NIST SP800-181[※344] として発行された。それが 2020 年 11 月に改訂され、最新版として NIST SP800-181 Revision 1[※345] が発行された（NIST の規格については「3.4 NIST のセキュリティ関連活動」参照）。

NICE Framework は、その時々の組織におけるサイバーセキュリティの要求や必要性に合う形で、サイバーセキュリティに関連する仕事や関わる人材の能力を記述する共通言語として機能することを目的としている。

日本の方向性との関連では、NICE Framework が目指している様々な関係者間での共通言語化は、日本において経済産業省や NISC が示している「役割定義の共通言語化等」と共通している[※346]。また、NICE Framework における「Cybersecurity Workforce」から「Learners」への変更は、日本において NISC 等が示しているプラス・セキュリティ、DX with Cybersecurity への取り組みとも同じ方向である。

(5) 総務省・NICT の取り組み

総務省の人材育成に関わる取り組みは、NICT を中心に行われており、ナショナルサイバートレーニングセンターで実施されている実践的サイバー防御演習「CYDER」、サイバーコロッセオや若手セキュリティ人材育成のための SecHack365 等の人材育成プログラムを展開している。

2021 年からは、「サイバーセキュリティ統合知的・人材育成基盤 CYNEX」構築を計画している（「2.1.3 総務省の政策」参照）。

(6) まとめ

DX の推進では、デジタル化を前提としたビジネスを考え実行する際にセキュリティを担う人が必要となってくる。

セキュリティ担当部門のみならず、事業部門にもセキュリティが分かり、必要なセキュリティ業務をこなすことが求められてきており、セキュリティに特化した能力だけではなく、デジタル化を前提とした事業を推進するために必要なセキュリティを確保できる能力が求められ、プラス・セキュリティ知識を持った人材育成が重要となっている。

一方で、組織全体での情報セキュリティ統制（ガバナンス）を考えて実行する機能・役割も必要である。自組織のビジネス・業務への深い知識と理解を持った上で、組織全体として統制の取れたセキュリティ対策を実施するセキュリティ統括の役割を担うセキュリティ専門人材が必要である。手引き書作成等の活動により、いままでの戦略マネジメント層は、DX with Cybersecurity を推進する人材像として以下のように整理された。

- セキュリティ統括：組織全体のセキュリティを統括的に担う人材
- プラス・セキュリティ：事業におけるセキュリティを担当する人材

今後、NISC、経済産業省、総務省等の官による施策は、2021 年に改定される次期「サイバーセキュリティ戦略」に盛り込まれ、計画、実施されていくものと思われる。それに加えて、SC3 等による民間での協調体制が徐々に構築され、相互に連携しながら、セキュリティ人材育成環境が整備されていくことが期待される。

2.3.2 産業サイバーセキュリティセンター

我が国の経済・社会を支える重要インフラ[※347] や産業基盤のサイバー攻撃に対する防御力を強化するため、IPA は 2017 年 4 月に産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）を発足させた。

ICSCoE は、重要インフラや産業基盤のサイバーセキュリティリスクに対応する人材・組織・システム・技術を生み出していくため、「人材育成事業」「制御システムの安全性・信頼性検証事業」「攻撃情報の調査・分析事業」の三つを事業の柱としている。本項では、「人材育成事業」について述べる。

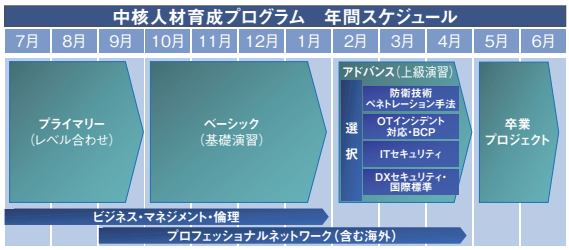
(1) 中核人材育成プログラム

ICSCoE は、2017 年 7 月、制御技術（OT：Operational Technology）と情報技術（IT）、マネジメント、ビジネス分野を総合的に学び、サイバーセキュリティ対策の中核となる人材を育成する「中核人材育成プログラム」を開始した。本プログラムでは、OT 及び IT 知識のレベル合わせからハイレベルな演習までを 1 年間のフルタイムで実施する。第 1 期は 76 名、第 2 期は 83 名、第 3 期は 69 名が参加し、2020 年 7 月に開講した第 4 期では、電力・鉄鋼・石油・化学・自動車・鉄道・放送・

通信・産業ベンダ等の幅広い業界から47名が参加した。

カリキュラムはOT分野の「防衛技術・ペネトレーション手法」（制御システム固有のセキュリティリスク、攻撃に対する防御技術の理解等）、「OTインシデント対応・BCP」（安全性と事業継続性を両立するOTインシデント対応、制御システムBCP対応の演習等）、IT分野の「ITセキュリティ」（制御システムセキュリティ実現のためのIT設計、ITインシデント対応、体制整備等）の3領域を基軸として、ビジネスマネジメントに関する実務家による講義や米国・欧州等の先進事例を学ぶ海外派遣演習等を含む構成となっている。

本プログラムは、過去の実施結果を踏まえて毎年カリキュラム及びスケジュールの改善を図っている。4年目となる2020年度は、「アドバンス（上級演習）」において選択可能な演習として、AI、IIoT（Industrial Internet of Things：産業分野向けIoT）、商用クラウド、DLT（Distributed Ledger Technology：分散台帳技術）のセキュリティ応用及びセキュリティ課題の講習等を実施する「DXセキュリティ・国際標準」を追加した（図2-3-9）。



■図2-3-9　第4期中核人材育成プログラムの年間スケジュール

2020年12月の海外派遣演習では、英国の政府機関・航空業界及び起業家の代表者によるサイバーセキュリティの取り組みや5Gのポリシーに関する講義をオンラインで実施した。2021年1月には、フランスのセキュリティ専門家による海運業界のサイバーセキュリティやデータ処理のセキュリティに関する講義をオンラインで実施した。

同年1月には、2017年5月に合意された「日イスラエル・イノベーション・パートナーシップ」等に基づき、イスラエルの重要インフラ企業やサイバーセキュリティ企業の担当者によるサイバーセキュリティ対策に関する講義をオンラインで実施した。

また同年3月には、米国政府・EUと連携した制御システムのサイバーセキュリティ対策に関するキャパシティビルディングプログラム「インド太平洋地域向け日米産業制御システムサイバーセキュリティウィーク※169」（「2.2.1（3）（c）インド太平洋地域に向けたサイバー演習」参照）を経済産業省と共催した。本演習には第4期の受講者及びインド太平洋地域から招聘した外国人受講者40名がオンラインで参加し、米国、EU及び日本の専門家によるエネルギー分野を含むサイバーセキュリティに関するワークショップ、リモートでのハンズオン演習等を実施した。

2018年7月、中核人材育成プログラムのOB会として、修了者コミュニティ「叶会※348」が発足し、2019年夏以降、本プログラムを通じて培った人脈の活用、知見やノウハウの共有を目指し、地域活動や技術をテーマにする複数の部会が設置された。また修了年次をまたがる縦のつながりの形成、最新情報及びノウハウ収集を目的とした叶会総会があり、2020年11月に第3回総会が開催された。叶会には第1期から第3期までの修了者に加え、2021年6月に修了した第4期生も参加しており、今後もコミュニティとしての規模を拡大しながら、お互いの顔が見える縦横の人的つながりを形成し、産業サイバーセキュリティに関する適時、適切な情報共有活動を継続することが期待される。

なお、同プログラムの修了者は、情報処理の促進に関する法律の規定に基づき、後述する情報処理安全確保支援士試験の全部免除を受けることができる※349。

（2）短期プログラム

ICSCoEでは、セキュリティに関連するスキルの習得機会が充分でない部門責任者や現場責任者、及びセキュリティ実務担当者に向けて、数日間で学ぶ短期演習形式の「製造・生産分野向けセキュリティ教育プログラム」「業界別サイバーレジリエンス強化演習」「戦略マネジメント系セミナー」及び「制御システム向けサイバーセキュリティ演習」を提供している。新型コロナウイルスへの対応の一環として、オンライン実施が可能なものはライブ配信または事前収録した動画のオンデマンド配信とした。

（a）製造・生産分野向けセキュリティ教育プログラム

「製造・生産分野向けセキュリティ教育プログラム※350」（旧称、製造・生産分野の管理監督者層向けプログラム）は、製造・生産のための制御系システムを日夜運用する管理監督者の方で、サイバー攻撃に対する防護力の強化に関心を持つ方を対象としたプログラムである。

2020年11～12月には「製造・生産現場のセキュリティに必要なIT・OT基礎コース」をオンライン（オンデマンド配信）と神戸での講習を組み合わせて実施した。本コースは製造・生産現場のセキュリティ対策に必要なIT・OTの基礎知識を理解すること、IT部門とOT部門が

連携してセキュリティを推進するための共通目線を獲得し相互理解を深めること等を目的としている。受講者からは、「理解度に応じて動画を繰り返し視聴できる点が良かった」「体系的に構成されており理解しやすかった」との反応があった。

また2021年1～2月には「製造・生産現場でのセキュリティ・インシデント対応実践方法コース」をオンライン（ライブ配信）で実施した。本コースは異常が発生した際、サイバー攻撃の可能性も考慮した初動対処を行い、障害の切り分けができること、社内外の関連組織と連携し、影響を最小化しながら、原因究明、事業継続等の対応ができること等を目的としている。受講者からは、「オンラインでもしっかり学べた」「座学で学んだ上で実践するスタイルが良かった」「サイバーセキュリティに精通していなくても理解できる内容であった」との反応があった。

(b) 業界別サイバーレジリエンス強化演習（CyberREX）

「業界別サイバーレジリエンス強化演習（CyberREX：Cyber Resilience Enhancement eXercise by industry）※351」は、電力、鉄道、ビル・物流、自動車（製造系）、ファクトリーオートメーション業界においてCISO（Chief Information Security Officer：最高情報セキュリティ責任者）に相当する役割を担う人材やIT部門、生産部門等の責任者・マネージャークラスの人材を対象としたプログラムである。

2020年11月に本演習をオンライン（ライブ配信）で実施した。本演習は、部署・部門のサイバーセキュリティに関する対応力・回復力を強化するため、業界の最新動向、業界別に考慮すべきセキュリティ要件、安全性要件を織り込んだ構成とし、仮想企業を想定したシナリオ形式による実践演習を中心に進められた。受講者に加え、サイバーセキュリティの専門家や監督省庁の関係者も参加した形式でのグループ演習を行った。受講者からは、「オンラインでの受講に問題なかった」「演習の内容が非常によく練られておりまるで訓練中かのような雰囲気で学べた」との反応があった。

(c) 戦略マネジメント系セミナー

「戦略マネジメント系セミナー※352」は、セキュリティ及びリスクマネジメントに係る方針や戦略を策定し、推進することを期待される管理職を対象としたプログラムである。

2021年2月に、本セミナーをオンライン（オンデマンド配信）で実施した。本セミナーでは、2019年度に実施した同セミナーの「セキュリティ組織管理」コースを発展させ、組織のセキュリティ体制を統括・推進するための考え方、セキュリティ対策の実践に向けたマネジメント手法等を習得することを目的とした。

具体的には、政府動向や先進事例の講演、セキュリティ対策のあるべき姿や対策推進時の悩み・解決策を有識者が議論するパネルディスカッション、現場でセキュリティ対策を実践するための体系的なノウハウの講演を動画で配信した。受講者からは、「オンデマンド配信は受講時間の自由度が高くなり良かった」「政府動向の要点をつかめる貴重な機会であった」「他社のセキュリティの取り組み状況や課題認識を知ることができて大変参考になった」との反応があった。

(d) 制御システム向けサイバーセキュリティ演習

「制御システム向けサイバーセキュリティ演習※353」は、制御システムのサイバーセキュリティを担当する、または今後担当予定の技術者を対象としたプログラムである。

2020年12月に東京で本演習を実施した。本演習は制御システムのサイバーセキュリティを理解するための導入的な位置付けであり、制御システムへの攻撃手法、及び制御システムのサイバーセキュリティ対策の基礎を、簡易模擬システムを用いた実機演習（ハンズオン演習）で体験し、制御システムのセキュリティについて実践的に理解することを目的としている。受講者からは、「非常に有益な研修であった」「これまで攻撃方法の実機演習の機会がなかったため今回深く学ぶことができた」との反応があった。

2.3.3 情報セキュリティ人材育成のための国家試験、国家資格制度

本項では、情報セキュリティ人材の育成や確保を目的とした国家試験や国家資格制度に関する動向を紹介する。

(1) 情報セキュリティマネジメント試験

企業・組織においては、組織が定めた情報セキュリティポリシーを部門内に周知して遵守を促し、部門の情報管理を実施する等、情報セキュリティ対策を推進する人材（情報セキュリティマネジメント人材）が必須である。こうした人材を育成するために、2016年度春期より「情報処理技術者試験」の新たな試験区分として「情報セキュリティマネジメント試験」が実施されている。2019年度までは、試験を年2回実施していたが、2020年度は、新型コロナウイルス感染拡大防止の観点から春期試験

(4 月)が中止となった。また、秋期試験(10 月)についても、新型コロナウイルスの影響により試験会場を十分に確保できないことから、試験の実施方式を、同一日に全国の試験会場で一斉実施する従来の紙試験から、複数日で実施する CBT（Computer Based Testing）方式※354 に移行した。CBT 方式への移行により、受験者は、自身で試験日、試験会場を選択することが可能となった。2020 年度は、CBT 方式による試験を 12 月 1 ～ 27 日の期間で実施し、応募者数 9,694 人、合格者数 6,071 人であった※355。2021 年度も CBT 方式での実施を継続する。

(2) 情報処理安全確保支援士制度

サイバー攻撃の増加・高度化に加え、社会的な IT 依存度の高まりから、企業・組織におけるサイバーセキュリティ対策の重要性が高まっている。それに伴い、企業・組織での安全なセキュリティ対策を高度なスキルを活かして推進できる人材が求められている。

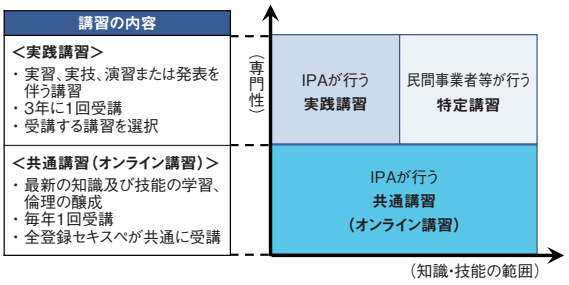
そこで、最新の知識・技能を備え、サイバーセキュリティ対策を推進する人材の育成と確保を目指し、2016 年 10 月、「情報処理の促進に関する法律」の改正法が施行され、新たな国家資格「情報処理安全確保支援士」制度が創設された。

情報処理安全確保支援士（以下、登録セキスペ）は、情報処理安全確保支援士試験合格者が登録簿に登録されることにより資格を取得する、サイバーセキュリティ分野初の国家資格である。試験は例年、年 2 回実施されているが、2020 年度は新型コロナウイルス感染拡大防止の観点から春期試験（4 月）が中止となり、実施された秋期試験（10 月）の応募者数は 1 万 6,597 人、合格者数は 2,253 人であった※356。

また、2020 年 5 月に「情報処理の促進に関する法律」が改正され、新たに更新制及び特定講習の制度が導入された。更新制とは登録から 3 年ごとに資格の更新を義務付けるものであり、サイバーセキュリティに関する最新の知識・技能の維持のみならず、欠格事由に該当していないか等、登録セキスペとしての資格を有しているかを改めて確認することで、情報処理安全確保支援士制度の信頼性向上を目的としている。2020 年 10 月 1 日に 5,865 人、2021 年 4 月 1 日に 1,847 人が登録セキスペ資格の更新を行った。2020 年度の新規登録者 1,111 人と合わせ、登録セキスペの登録人数は、2021 年 4 月 1 日時点で 2 万 178 人である※357。

登録セキスペには法定講習として、共通講習と実践講習の受講が義務付けられている。2021 年度から実践講習は、IPA が行う実践講習と民間事業者等が行う特定講習から選択できるようになった。特定講習は、一定の条件を満たした民間事業者等が実施する講習を経済産業大臣が法定講習として定める制度である※358。2021 年 3 月に 8 実施機関 23 講座が 2021 年度の特定講習として経済産業省より公開された※359。これにより、登録セキスペの多様なニーズに対応できるようになった。

登録セキスペに受講が義務付けられている法定講習の全体像を図 2-3-10 に示す※360。



■図 2-3-10　法定講習の全体像

IPA の行う実践講習は、グループディスカッションを中心とした内容で従来は集合形式で実施していたが、新型コロナウイルス感染拡大防止の観点から、2020 年 11 月からは Web 会議ツールを利用したリモート形式で実施しており、2021 年度も継続する。2020 年度には 1,243 名が受講し、集合形式と同等の満足度を実現している。受講者からは、「自分が普段携わっていないインシデント対応や CSIRT 構築・運用や経営目線等、様々な視点の考え方を学ぶことができた」「登録セキスペとしての倫理面での責任を改めて感じた」等の声が上がっている。また、「ディスカッションの内容をファイル共有ツールを介して即時にテキスト化でき、自分自身の考えが整理されるとともに他者の意見も理解しやすかった」「地域で集まるのではなく、全国の方と意見交換できるのはリモート講習ならではの貴重な場だと感じた」といったリモート形式ならではのメリットも挙がった※361。

2.3.4 情報セキュリティ人材育成のための活動

情報セキュリティに関する情報共有や情報セキュリティ人材育成の場として、様々なイベントが開催されている。また、複数の大学と産業界がネットワークを形成し、セキュリティ分野の人材を育成する事業が行われている。

(1) セキュリティ・キャンプ

「セキュリティ・キャンプ」は、若年層の情報セキュリティ意識の向上、並びに将来第一線で活躍できる高度な情報セキュリティ人材を発掘・育成する場として、一般社団法人セキュリティ・キャンプ協議会（以下、セキュリティ・キャンプ協議会）とIPAにより運営されている。

17回目となる2020年度の全国大会は、新型コロナウイルスの影響により2020年10月18日～12月6日にオンライン形式で開催され、選考を通過した85名が参加した※362。

また、過去のセキュリティ・キャンプ全国大会を修了、または同等以上のスキルを持つ25歳以下の学生を対象とした育成の場である「セキュリティ・ネクストキャンプ2020オンライン」も、全国大会と同期間に併催され、7名が参加した※363。

主に若年層を対象とした「セキュリティ・ミニキャンプ」については、新型コロナウイルスの影響により東京開催は中止となったが、北海道、青森、山梨、広島、福岡、沖縄は現地で開催され、大阪は3月にオンラインで開催された※364。

セキュリティ・キャンプ協議会が単独で主催するイベントである「Global Cybersecurity Camp」については、第3回が2021年1月16日～2月7日にオンライン開催された※365。このトレーニングキャンプは、「国籍・人種を越えた専門知識のあるグローバル人材の育成」「国境を越えた友情とゆるやかなコミュニティの形成」を目的として、セキュリティに興味を持つ、異なる国の若者がともに学び、友好を深める場を提供するものである。

セキュリティ・キャンプ協議会が実施するその他の活動として、2021年3月13日に「セキュリティ・キャンプフォーラム2021」がオンライン開催された。本フォーラムの目的は、セキュリティ・キャンプ修了生相互の年次を超えた交流と意見交換の場の提供、同修了生の認知度向上と現在の活動紹介による産業界での活躍支援のきっかけの提供、の2点である。当日は、セキュリティ・キャンプ修了生が情報セキュリティに関連する取り組みをテーマとしたプレゼンテーションを行った。また、優れた成果を上げた人や価値ある取り組みを表彰する「セキュリティ・キャンプアワード2021」の表彰を実施した。表彰後には、「セキュリティ・キャンプ交友会2021春オンライン版」が併せて開催された※4。

(2) enPiT

「enPiT（Education Network for Practical Information Technologies：成長分野を支える情報技術人材の育成拠点の形成）」は、情報技術を高度に活用して社会の具体的な課題を解決できる人材を育成するために、産学協働の教育ネットワークを形成し、PBL（Problem Based Learning：課題解決型学習）等の実践的な教育を推進・普及することを目的とした文部科学省の事業である。2012～2016年度までは大学院生を対象とした事業「第1期enPiT」が実施され、これを踏まえて2016年度から、学部生を対象とした「第2期enPiT」（以下、enPiT2）を実施している。enPiT2は、ビッグデータ・AI、セキュリティ、組み込みシステム、ビジネスシステムデザインの4分野を対象として教育プログラムを提供している。

このうちセキュリティ分野（enPiT-Security）では、2020年度は大学等31校、連携企業51社・団体が参加した（2021年3月現在）。東北大学を中核とした14の大学が連携して、高度化する情報セキュリティの脅威を理解し、リスクマネジメントに必要な知識、基本技術、実践力を備えた人材を育成する「Basic SecCapコース※366」を提供しており、210名が修了認定を取得した※367。

また、社会人を対象とした情報科学技術分野に関する体系的かつ高度で短期の実践教育プログラムとして「enPiT-Pro※368」がある。セキュリティ分野では、情報セキュリティ大学院大学、東北大学、大阪大学、和歌山大学、九州大学、長崎県立大学、慶應義塾大学の7大学が、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA：Japan Network Security Association）、一般社団法人サイバーリスク情報センター（CRIC）、及び地域の団体・官庁・企業（2021年2月時点で37社・団体）と連携し、多様な産業ニーズに即したプロ人材育成のための教育コース「enPiT-Pro Security※369」を展開している。

(3) SECCON 2020

SECCONは実践的情報セキュリティ人材の発掘・育成、技術の実践の場の提供を目的とする日本最大の情報セキュリティコンテストイベントである。

世界各国のセキュリティ専門家がCTF※370の技量を競うSECCON CTF 2020は、新型コロナウイルスの影響で例年の予選・決勝の形式をとらず、2020年10月10～11日にオンライン形式で開催された。世界88ヵ国から982チーム、1,862人の参加があった※371。

関連するイベントとして、新しいコンテストの企画案・

設計案をCFC（Call for Contest）として2020年10月に募集した（「Contest of Contest」）。またコンテストに関する講演・ワークショップのイベントとして、同年12月19日に「SECCON 2020電脳会議」を開催した。主催者、CTF参加者の講演等のほか、「Contest of Contest」の結果も発表された※372。

また、日本国内のCTF参加者を増やし、セキュリティ人材の底上げを図るためのワークショップ「SECCON Beginners※373」も開催した。まず2020年5月23～24日にはCTF初級者～中級者を対象とする「オンラインCTF」を開催し、1,070チームが参加した。10月17日には講演形式の「SECCON Beginners Live※374」を開催し、オンラインCTFの結果を解説した。

更に、情報セキュリティに興味がある女性を対象としたワークショップ「CTF for GIRLS※375」では、2020年9月18日にネットワーク、12月11日に暗号に関するオンラインワークショップを開催した。

JNSAは、このようにSECCONをとおして、専門家向けのCTFだけでなく、初級者・中級者を含めた様々なセグメントに対して実践的情報セキュリティ人材の発掘・育成の機会を提供している。

(4) 産学情報セキュリティ人材育成交流会

JNSAの産学情報セキュリティ人材育成交流会は、2012年2月に発足し、今後の情報セキュリティ業界を支える人材を育成するためのインターンシップの支援活動を実施している。将来情報セキュリティ業界で活躍したいと考える学生に対し、本交流会を介して、2020年度は6社の企業がインターンシップを実施した。CTF形式を取り入れたセキュリティ業務体験イベントや特別セミナーを開催した企業もあった※376。

(5) サイバーセキュリティ経営戦略コース

東京工業大学社会人アカデミーでは2021年2月18日、MOT（Management of Technology：技術経営）に関する社会人向けプログラムとして「キャリアアップMOT『サイバーセキュリティ経営戦略コース』」を開講した。本コースは新型コロナウイルス対策のため、オンライン講義形式となった※377。

本コースでは、サイバーセキュリティが企業・組織の経営に及ぼす影響を理解し、サイバーセキュリティ経営※378及びその戦略立案に求められる知識・能力を備え、企業・組織を先導する人材の育成を目指しており、多様な業界･業種から、経営者、マネージャー、若手等、多くの社会人が受講することを想定している。本コースは、週1回、産学官の実務経験豊富な有識者による関連技術・法制・世界情勢等の解説や、事例に基づく演習、討議等を含む全20回の講義で構成される。

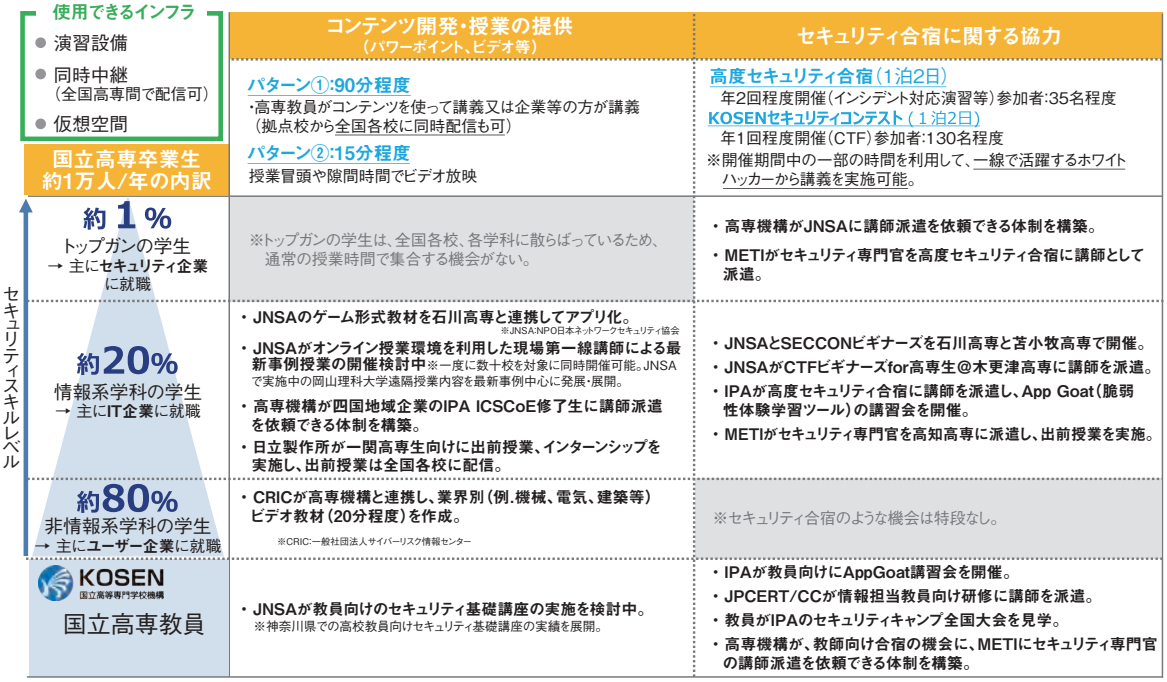
(6) 産学官で連携した国立高等専門学校での取り組み

国立高等専門学校（以下、高専）のセキュリティ教育において、産業界が求めるセキュリティ人材を育成・輩出する支援として、経済産業省、IPA、JPCERT/CC及びJNSA等の業界団体が、独立行政法人国立高等専門学校機構（以下、国立高専機構）と連携し、教育コンテンツの提供や講師の派遣等に取り組んでいる。

高専生の専攻（セキュリティ、IT、その他（機械、電気等））により、卒業後の就職先の業界に傾向があることに着目し、将来を見据えたセキュリティ人材育成を、2019年より産学官連携で行っている。約20%の人材（情報系の学生）への教育コンテンツ提供や講師派遣、80%の人材（非情報系学科の学生）に向けた一般社団法人サイバーリスク情報センター（CRIC）による業界別ビデオ教材の作成等を行っている。図2-3-11（次ページ）に具体的な取り組みを示す。

2020年は、JNSAによるオンライン授業環境を利用した最新事例授業や教員向けセキュリティ基礎講座等、これまでの実績をより広く展開する検討を行った。また、四国地域企業のIPA ICSCoE修了生を地域の高専に、経済産業省のセキュリティ専門官をセキュリティ合宿や教師向け合宿に講師派遣できる体制を構築した。

● METI、IPA、JPCERT及び業界団体が国立高専機構と連携し、高専生の専攻（セキュリティ、IT、その他（機械、電気等））に応じた教育コンテンツの提供や講師の派遣等、産学官連携の具体化を推進中。



■図 2-3-11　国立高専機構と産・官との連携促進・具体化
（出典）経済産業省「事務局説明資料」（第 7 回 産業サイバーセキュリティ研究会 ワーキンググループ 2（経営・人材・国際）資料 3）を基に IPA が編集

2.4 組織・個人における情報セキュリティの取り組み

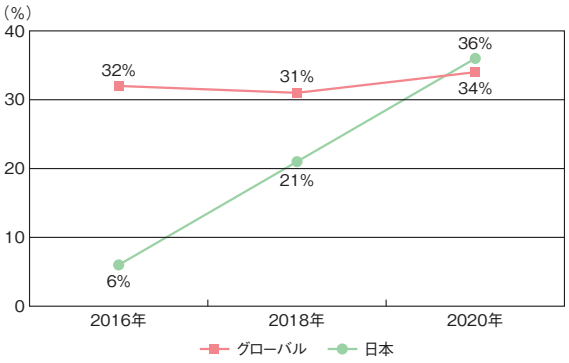
企業、教育機関、地方自治体、一般利用者の情報セキュリティの対策状況及び課題について、政府、IPA 等による取り組み及び公表されている資料等を基に述べる。

2.4.1 企業における対策状況

情報セキュリティに対する企業の対策状況、及びセキュリティマネジメントの取り組みについて述べる。

(1) 情報セキュリティに対する企業の対策状況

PwC が 2 年に 1 度実施している世界規模のアンケート調査※379 によると、日本の組織がサイバー攻撃の被害に遭った割合は上昇傾向にあり、2020 年には「グローバル」とほぼ同じ割合となっている（図 2-4-1）。この増加傾向は、「グローバル」の傾向とも異なって急激であり、これまで以上に国内企業・組織のセキュリティ対策が求められる。



■図 2-4-1「サイバー犯罪」の被害にあったと回答した組織の比率の推移
（出典）PwC Japan グループ「経済犯罪実態調査 2020 日本分析版※380」を基に IPA が編集

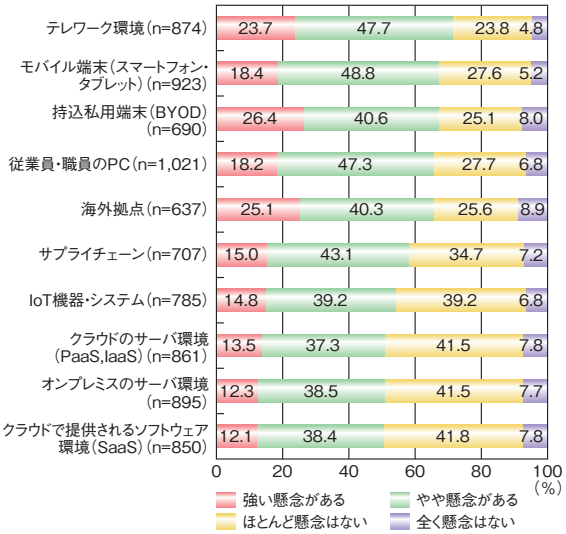
このような背景を踏まえ、企業のセキュリティ対策状況について、以下の資料を基に述べる。

- トレンドマイクロ株式会社（以下、トレンドマイクロ社）：2020 年度 法人組織のセキュリティ動向調査※381（民間企業 980 社及び官公庁自治体 106 団体を対象に調査。以下、トレンドマイクロ社調査）
- NRI セキュアテクノロジーズ株式会社（以下、NRI セキュア社）：NRI Secure Insight 2020※382（国内・海外企業 2,260 社を対象に調査。以下、NRI セキュア社調査）
- IPA：2020 年度サイバーセキュリティ経営ガイドライン実践のためのプラクティスの在り方に関する調査※383（国内企業 930 社を対象に調査。以下、プラクティス調査）

(a) セキュリティ対策の検討状況

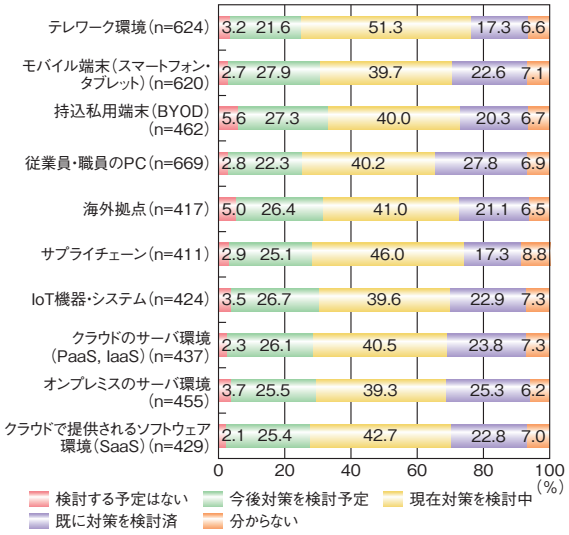
トレンドマイクロ社調査（図 2-4-2）によると、現在利用または今後利用予定がある IT 環境やシステムについて、「強い懸念がある」及び「やや懸念がある」を合わせた割合は、「テレワーク環境」（71.4%）が最も高く、「モバイル端末（スマートフォン・タブレット）」（67.2%）、「持込私用端末（BYOD）」（67.0%）、「従業員・職員の PC」（65.5%）と続く。テレワークの普及によって、これらの懸念が高まっている可能性がある。

また、「強い懸念がある」割合に着目すると、「持込私用端末（BYOD）」（26.4%）に次いで、「海外拠点」（25.1%）が高い。海外に拠点を持つ企業において、国内と比較して海外拠点のセキュリティ対策が課題になっている。

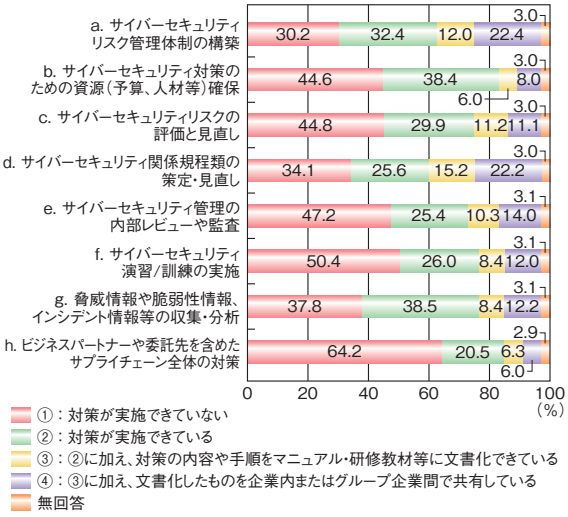


■図 2-4-2　IT 環境やシステムへの今後の懸念
（出典）トレンドマイクロ社「2020 年度 法人組織のセキュリティ動向調査」を基に IPA が編集

図 2-4-3（次ページ）に示すように、懸念がある IT 環境やシステム※384 に対する対策の検討状況について、「既に対策を検討済」の割合が最も低いのは「テレワーク環境」と「サプライチェーン」（ともに 17.3%）である。「テレワーク環境」及び「サプライチェーン」のセキュリティ対策を懸念している企業であっても、検討が不十分なまま導入・



■図 2-4-3　懸念がある IT 環境やシステムに対する対策の検討状況
（出典）トレンドマイクロ社「2020 年度 法人組織のセキュリティ動向調査」を基に IPA が編集



■図 2-4-4　サイバーセキュリティ対策の状況
（出典）IPA「2020 年度サイバーセキュリティ経営ガイドライン実践のためのプラクティスの在り方に関する調査」を基に作成

運用している状況がうかがえる（テレワークの脅威と対策については「3.3 テレワークの情報セキュリティ」参照）。

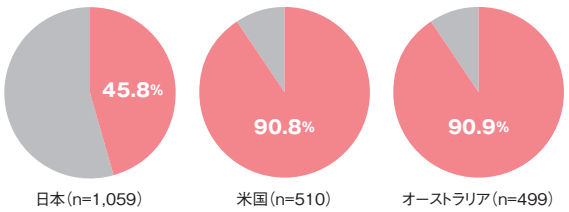
プラクティス調査（図 2-4-4）によると、個々のサイバーセキュリティ対策の実施状況に関して、対策が実施できている（②、③、④の合計）割合が高いのは、「a. サイバーセキュリティリスク管理体制の構築」（66.8%）、「d. サイバーセキュリティ関係規程類の策定・見直し」（63.0%）、及び「g. 脅威情報や脆弱性情報、インシデント情報等の収集・分析」（59.1%）である。このうち、文書化・共有化までできている（③と④の合計）割合が高いのは、「a. サイバーセキュリティリスク管理体制の構築」（34.4%）と「d. サイバーセキュリティ関係規程類の策定・見直し」（37.4%）である。

一方、対策が実施できていない（①）割合は、「h. ビジネスパートナーや委託先を含めたサプライチェーン全体の対策」（64.2%）が最も高く、「f. サイバーセキュリティ演習 / 訓練の実施」（50.4%）、「e. サイバーセキュリティ管理の内部レビューや監査」（47.2%）と続く。このうちサプライチェーン（h.）や演習／訓練（f.）は、サイバーセキュリティ対策を推進する部門以外を巻き込んだ活動であり、高コストやノウハウ・意識付けの不足等により実施が進んでいないことがうかがえる。これは、トレンドマイクロ社調査（前ページ図 2-4-2）において、サプライチェーンに関しては、そこで利用する IT 環境やシステムに対する懸念は比較的少ないことからも推察される。

体制の構築（a.）や規程類の策定・見直し（d.）では、文書化・共有化まではある程度実施できているものの、情報収集・分析（g.）に関しては、文書化・共有化まではできていない実態がうかがわれる。

(b) セキュリティ管理体制の構築状況

NRI セキュア社調査（図 2-4-5）によると、CISO を設置している企業の割合は、米国とオーストラリアが 90% 以上であるのに対し、日本は 45.8% にとどまっている。また、米国とオーストラリアに比べて、「経営層の兼務」の割合（75.2%）が高く、「社外有識者」の割合（1.8%）が低い。



CISOの属性とその割合

	経営層	非経営層	社外有識者
日本（n=1,059）	75.2%	23.0%	1.8%
米国（n=510）	49.8%	38.6%	11.6%
オーストラリア（n=499）	55.9%	33.6%	10.5%

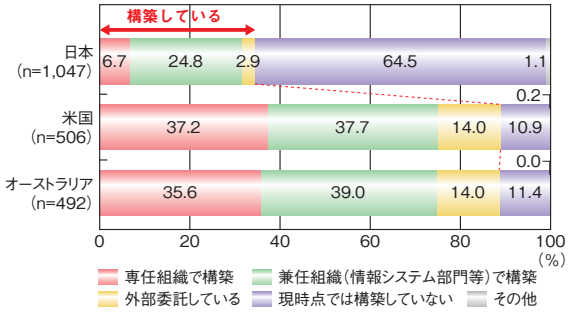
※わからないを除く

■図 2-4-5　CISO を設置している企業
（出典）NRI セキュア社「NRI Secure Insight 2020」を基に IPA が編集

図 2-4-6（次ページ）によると、CSIRT を構築している企業の割合は、米国とオーストラリアが約 90% であるのに対し、日本は 34.4% にとどまっている。また、CSIRT の構築形態では、米国とオーストラリアに比べて「専任組織で構築」の割合が 6.7%、「外部委託している」の割

合が 2.9% とともに低い。

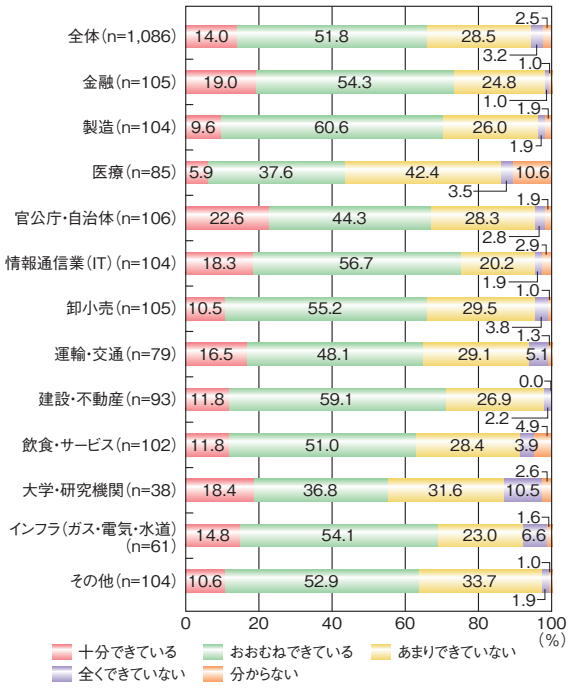
日本の企業では、CISO は経営者の兼務、また CSIRT は情報システム部門等の兼務が多く、専門家の不足、専門知識を持った外部人材の活用不足が推察される（セキュリティ人材に関する政府の施策については「2.3.1 情報セキュリティ人材の状況」参照）。



■図 2-4-6　CSIRT の構築状況
（出典）NRI セキュア社「NRI Secure Insight 2020」を基に IPA が編集

(c) セキュリティリスク管理の業種別実施状況

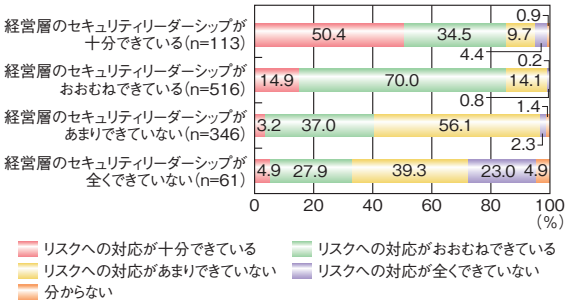
トレンドマイクロ社調査（図 2-4-7）によると、顕在化したリスクを適切に対処する事後のリスク対応の実施状況について、「十分できている」及び「おおむねできている」を合わせた割合は、全体で 65.8% となっており、業種別では「情報通信業（IT）」（75.0%）が最も高く、次いで「金融」（73.3%）が高い。一方、低かったのは、「医療」



■図 2-4-7　リスクへの対応の実施状況（業種別）
（出典）トレンドマイクロ社「2020 年度 法人組織のセキュリティ動向調査」を基に IPA が編集

（43.5%）、次いで「大学・研究機関」（55.2%）である。「医療」や「大学・研究機関」は、近年攻撃対象となることが増え、情報漏えい対策等の強化が望まれていながら、リスク対応が十分できていない業種であることがうかがわれる。

図 2-4-8 によると、「経営層のセキュリティリーダーシップ※385 が十分できている」企業は、「リスクへの対応が十分できている」の割合が 50.4% である。一方、「経営層のセキュリティリーダーシップが全くできていない」企業は、「リスクへの対応が十分できている」の割合はわずか 4.9% である。経営層のリーダーシップの重要性がうかがわれる。



■図 2-4-8　経営層のセキュリティリーダーシップとリスクへの対応の実施状況
（出典）トレンドマイクロ社「2020 年度 法人組織のセキュリティ動向調査」を基に IPA が編集

(d) まとめ

以上のように、国内企業が直面するセキュリティリスクとしては、テレワーク等の新しく常態化する IT 環境への対応、及びガバナンスが弱い海外拠点・業務委託先等のサプライチェーン対策等が懸念される。また対策実施面では、サプライチェーン対策や演習のコストとノウハウ・意識の不足、リスクに関する情報共有の不備、人材不足等による CISO/CSIRT 等の体制の不備等が懸念される状況である。

今後、企業の経営層は、これまで以上にリーダーシップを発揮し、業務アウトソース・人事を含む資源配分の最適化、新しい業務形態への対応、海外事業のガバナンス、サプライチェーンパートナーを含む情報共有等を推進することが求められる。

(2) セキュリティリスクマネジメント

国内の企業・組織は、前項「2.4.1 (1) 情報セキュリティに対する企業の対策状況」で述べたようなセキュリティリスクに直面している。組織のセキュリティリスクを把握・管理するリスクマネジメントは、企業にとって経営・事業

を守るための重要な課題の一つである。また前項で見たとおり、リスクマネジメントには経営層のリーダーシップが欠かせない。このため、経済産業省とIPAは、経営層のセキュリティリスクマネジメント向上のため、2017年に「サイバーセキュリティ経営ガイドライン Ver2.0[※386]」を発行した。また同ガイドラインの実践には対策状況の可視化や、参考となる実践事例（プラクティス）の提示が重要であると考え、それらに関する取り組みを行ってきた。

本項では、上記の活動を踏まえたセキュリティリスクマネジメントについて以下の資料を基に述べる。

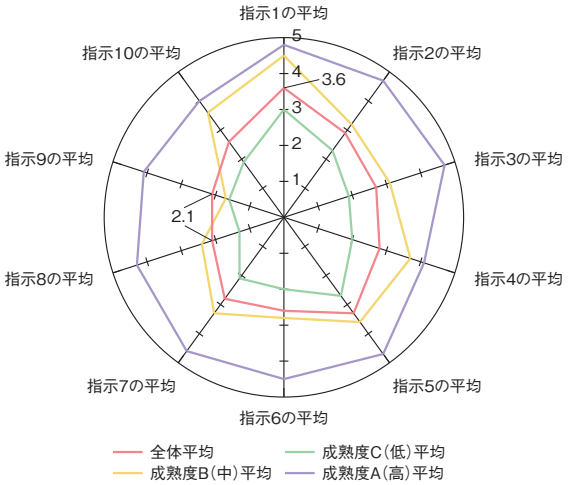
- 「可視化ツールβ版[※387]」の試用に関するJUAS（Japan Users Association of Information Systems：一般社団法人日本情報システム・ユーザー協会）調査（以下、可視化ツール調査、非公開）
- IPA：サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集 第2版[※388]（以下、プラクティス集）
- IPA：2020年度サイバーセキュリティ経営ガイドライン実践のためのプラクティスの在り方に関する調査（以下、プラクティス調査）

(a) 可視化ツールβ版の試用調査結果

本項の可視化ツールとは、サイバーセキュリティ経営ガイドラインにおいて経営層が指示すべき「重要10項目」に関する実施状況を、企業のCISO等がセルフチェックするツールであり、2020年3月にExcel形式によるβ版がリリースされた。またリリース直後、JUASがメンバー企業の協力を得て本ツールの試行を行った。

2020年9月に実施したJUASの可視化ツール調査では、可視化ツールβ版の試行を25社に対して行い、評価結果に基づいて企業を3グループに分け、グループごとの重要10項目の実施状況（以下、セキュリティ成熟度）の平均値を図示した（図2-4-9）。この図によれば、参加25社の全体平均（図2-4-9の赤線部）において、重要10項目の指示のうち、指示1（サイバーセキュリティリスクの認識、組織全体での対応方針の策定）へのセキュリティ成熟度が平均3.6ポイント（最高は5.0ポイント）で最も高い値となった。

一方、セキュリティ成熟度の全体平均において、指示8（インシデントによる被害に備えた復旧体制の整備）、指示9（ビジネスパートナーや委託先を含めたサプライチェーン全体の対策及び状況把握）のセキュリティ成熟度は、ともに2.1ポイントと低く、強化が必要であるとしている。

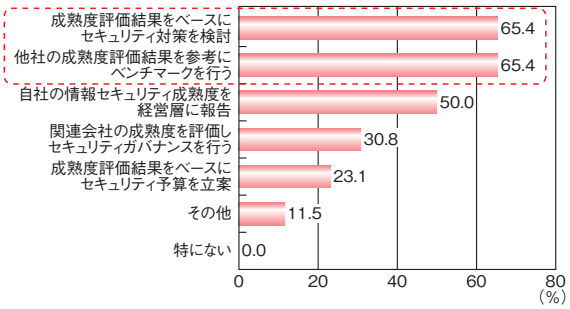


■図2-4-9　重要10項目の実施状況の平均値（n=25）
（出典）JUASの可視化ツール調査を基にIPAが編集

また、同調査において、可視化ツールβ版の利用場面について尋ねた結果、回答の65.4%がセキュリティ対策の検討やベンチマークの利用を想定していた（図2-4-10）。更に、経営層への報告の際のコミュニケーションツールとして可視化ツールを使いたい意図があると考えられる。

プラクティス調査において、セキュリティ対策実施状況の可視化は、対策検討・ベンチマークとしての利用が重要であること、そのためには現状の可視化結果と対策との紐付けが重要であること、が企業や有識者へのインタビューにより示唆された。

これらの結果から、可視化ツールβ版は、企業のセキュリティ成熟度を可視化してベンチマークを行い、具体的な対策を検討するために有効であると考えられる。このような可視化の手法を用いることでセキュリティリスクマネジメントの促進が期待される。



■図2-4-10　可視化ツールβ版の利用場面（n=26）
（出典）JUASの可視化ツール調査を基にIPAが編集

(b) プラクティス集への要望等に関する調査結果

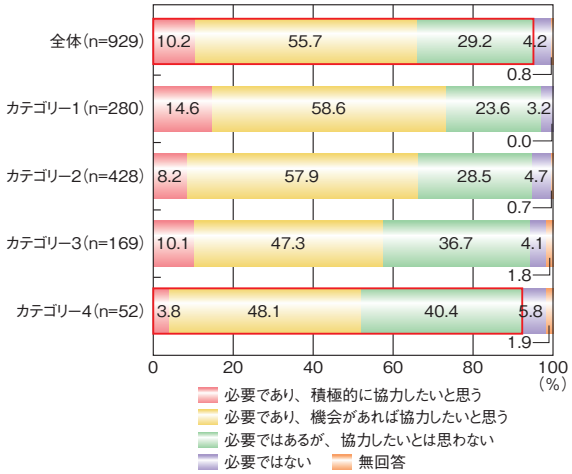
他社のセキュリティマネジメント実践事例を参考にして自社のセキュリティ課題を明らかにし、対策を行うことは

有効と考えられる。IPA は、これからサイバーセキュリティ対策に取り組む企業が重要 10 項目を実施するにあたっての考え方、ヒント、対策事例をまとめたプラクティス集を公開している。2020 年度は、プラクティス集の利用実態を把握し、その作成・共有のプロセスを含めたプラクティス集自体の在り方を検討することを目的に、企業の要望等の調査を実施した。本調査では、プラクティスに対するニーズが企業規模、IT 依存度により変化するとの仮説のもとに、それらに基づく企業の類型（以下、企業像）を定義し、企業像ごとのニーズを調査した。更にこの結果を基に、企業像をセキュリティ対策の成熟度に関して 3 グループに分類し、各グループのニーズを整理した。表 2-4-1 に各グループの特性と、ニーズから導いたセキュリティマネジメントの課題及び有効と思われるプラクティスを示す。

企業の特性	課題・有効なプラクティス
IT 依存度が低く、セキュリティのリソースが十分でない企業	自社の課題や取り組みが必要な領域・テーマが把握できていないため、サイバーセキュリティ体制構築の課題と実現のためのファーストステップを整理したプラクティスが有効。
IT 依存度が中程度以上で IT 化がある程度進んでいる企業	自社の課題や取り組みが必要な領域・テーマもある程度把握している。難度の高いサプライチェーン対策、インシデント対応力の強化や財務面のリスクヘッジ（サイバー保険）等のプラクティスが有効。
IT 依存度が高く、先進的な IT を導入している企業	自社の課題や取り組みが必要な領域・テーマを広く把握している。最新の技術・脅威に関する事例、解決策に関するプラクティスが有効。

■表 2-4-1　IT 依存度による企業分類と課題・対応策

IPA のプラクティス集利用者がコンスタントに増えている等、プラクティスの利用に対する期待はあると考えられる。一方で、プラクティスの収集や共有は一般には容易でない。そこで、プラクティス調査でプラクティスの効果的な収集や共有について尋ねたところ、プラクティスを共同で作成・共有する枠組みについて、「必要である※389-1」と回答した企業は、全体の 95.1% に上る（図 2-4-11）。この図において、カテゴリーとは前述の企業像を表し、カテゴリーの数値が小さい程、IT 依存度が高い（成熟度が高い）。最も IT 依存度の低いカテゴリー 4 の企業においても、作成・共有の枠組みが必要だとする回答は 90% を越えていることから、プラクティスに関する情報共有は、どのカテゴリーの企業にとっても重要と考えられる。



■図 2-4-11　プラクティスを共同で作成・共有する枠組みについて
（出典）IPA「2020 年度サイバーセキュリティガイドライン実践のためのプラクティスの在り方に関する調査」を基に編集

(c) セキュリティリスクマネジメントのフレームワーク

2021 年 2 月 18 日の経済産業省主催の第 7 回産業サイバーセキュリティ研究会 WG2 において、サイバーセキュリティ対策に関する取り組みのフレームワークが整理された。これによると、前掲のプラクティス集や可視化ツールはサイバーセキュリティ経営ガイドライン活用の支援ツールとして位置付けられる※389-2。今後は産業分野別等の実践的なガイドラインを整備するとしている。企業はこのフレームワークを活用してセキュリティリスクマネジメントの可視化・実践に取り組むことが期待される。

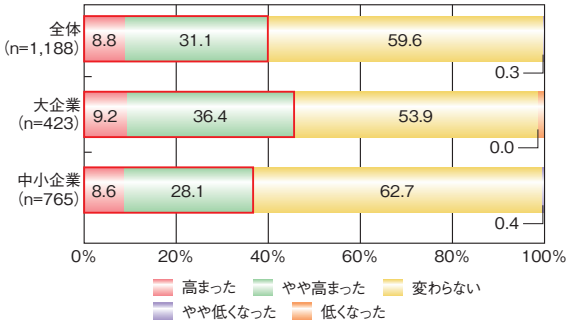
2.4.2 中小企業に向けた情報セキュリティ支援策

本項では、中小企業における情報セキュリティ、対策支援、及び普及啓発・対策ツールの現状について紹介する。

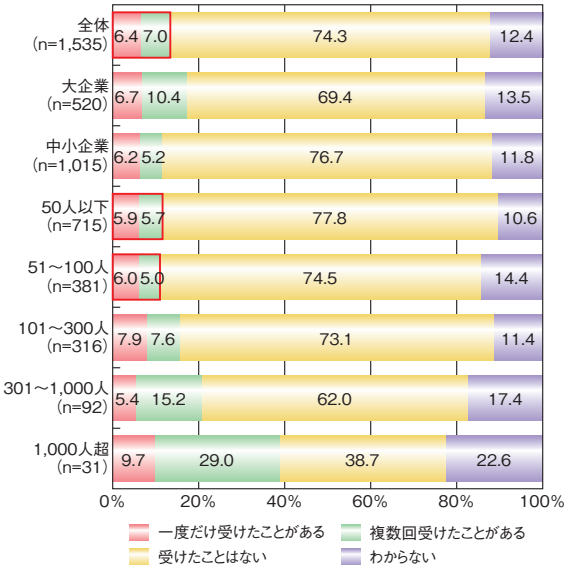
(1) 中小企業の情報セキュリティの現状

一般社団法人日本損害保険協会が 2020 年 12 月 9 日に発表した「国内企業のサイバーリスク意識・対策実態調査 2020 集計報告書※390」によると、新型コロナウイルスの感染拡大前と比べてサイバー攻撃を受ける可能性が「高まった」または「やや高まった」（次ページ図 2-4-12 の赤枠部分）と認識している企業の割合は 39.9% であった。企業規模別に見ると、大企業（45.6%）と比べて、中小企業では 36.7% と低くなっている。

サイバーリスク対策における課題については、「現在行っている対策が十分なのかわからない」と回答した割合が全体で 43.8% と最も高くなっている。「対策をする



■図 2-4-12　新型コロナウイルスの拡大以前と比べたサイバー攻撃を受ける可能性
(出典)一般社団法人日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020 集計報告書」を基に IPA が編集



■図 2-4-14　サイバー被害状況
(出典)一般社団法人日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020 集計報告書」を基に IPA が編集

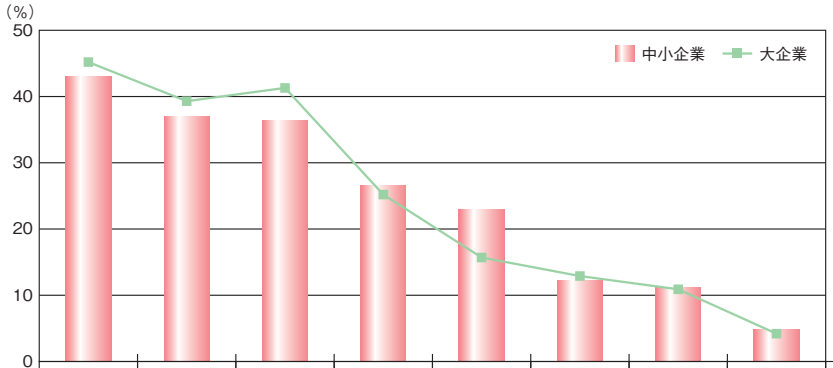
費用が足りない」と回答した企業の割合を企業規模別に見ると、大企業(15.7%)と比べて、中小企業では 23.0%と高くなっている(図 2-4-13)。

サイバー被害状況について、全体では 13.4% の企業がこれまでにサイバー被害を受けたことがあると回答しており、企業規模別に見ると、規模の小さい従業員 100 人以下の企業でも 1 割超がサイバー被害を経験している(図 2-4-14)。

また、サイバー被害を受けたことがある企業のうち、サイバー被害を受けた時期について、全体では 18.5%が「直近半年以内」と回答している。その割合を企業規模別に見ると、大企業 (16.9%) と比べて、中小企業では 19.8%と高くなっている(次ページ図 2-4-15)。

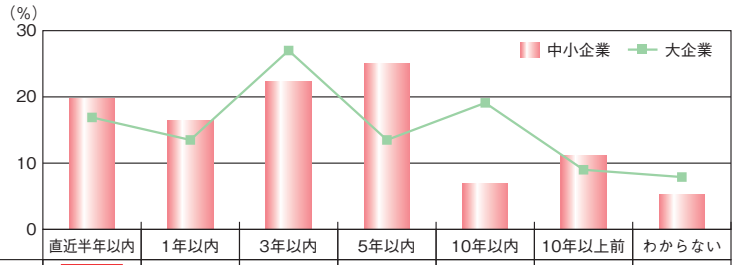
サイバー被害を受けた際の攻撃の種類としては、全体では「マルウェア」や「ランサムウェア」(いずれも31.7%)の割合が最も高く、「不正送金を促すビジネスメール詐欺やフィッシングサイト」(24.4%)、「標的型攻撃」(13.7%)と続いている。それらの割合を企業規模別に見ると、大企業と比べて、いずれも中小企業で割合が高くなっている(次ページ図 2-4-16)。

中小企業ではサイバーセキュリティ対策に十分な予算を割くことができていないため、サイバー攻撃を検知できていないという指摘がある。サイバーセキュリティ対策が強固とはいえない中小企業を標的としたサイバー攻撃やそれに起因する大企業等への被害が顕在化しているこ



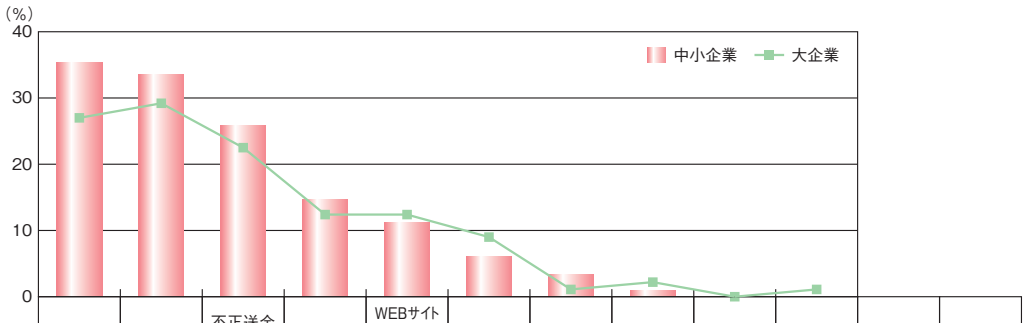
		現在行っている対策が十分なのか分からない	対策の効果測定が難しい	対策をする人手が足りない	社内や周囲に専門の人材がいない	対策をする費用が足りない	対策をする時間が足りない	特に課題はない	対策の必要性について社内の理解が得られず、十分な予算を獲得・確保できない	その他	わからない
全体(n=1,442)		43.8%	37.8%	38.1%	26.1%	20.5%	12.4%	11.1%	4.6%	0.6%	3.6%
企業規模別	大企業(n=496)	45.2%	39.3%	41.3%	25.2%	15.7%	12.9%	10.9%	4.2%	0.4%	4.6%
	中小企業(n=946)	43.0%	37.0%	36.4%	26.6%	23.0%	12.2%	11.2%	4.8%	0.6%	3.1%

■図 2-4-13　サイバーリスク対策における課題(複数回答)
(出典)一般社団法人日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020 集計報告書」を基に IPA が編集



		直近半年以内	1年以内	3年以内	5年以内	10年以内	10年以上前	わからない
全体(n=205)		18.5%	15.1%	24.4%	20.0%	12.2%	10.2%	6.3%
企業規模別	大企業(n=89)	16.9%	13.5%	27.0%	13.5%	19.1%	9.0%	7.9%
	中小企業(n=116)	19.8%	16.4%	22.4%	25.0%	6.9%	11.2%	5.2%

■図 2-4-15　サイバー被害を受けた時期(複数回答)
(出典)一般社団法人日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020 集計報告書」を基に IPA が編集



		マルウェア	ランサムウェア	不正送金を促すビジネスメール詐欺やフィッシングサイト	標的型攻撃	WEBサイトへの不正ログイン・情報窃取およびWEBサイトの改ざん	DDoS(サービス妨害)攻撃	制御システムに対する攻撃	PWリスト攻撃	IoTデバイスに対する攻撃	ゼロデイ攻撃	その他	わからない
全体(n=205)		31.7%	31.7%	24.4%	13.7%	11.7%	7.3%	2.4%	1.5%	0.0%	0.5%	4.9%	10.7%
企業規模別	大企業(n=89)	27.0%	29.2%	22.5%	12.4%	12.4%	9.0%	1.1%	2.2%	0.0%	1.1%	2.2%	14.6%
	中小企業(n=116)	35.3%	33.6%	25.9%	14.7%	11.2%	6.0%	3.4%	0.9%	0.0%	0.0%	6.9%	7.8%

■図 2-4-16　サイバー被害を受けた際の攻撃の種類(複数回答)
(出典)一般社団法人日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020 集計報告書」を基に IPA が編集

ともあり、中小企業を含むサプライチェーン全体でのセキュリティの確保が望まれている。

(2) 中小企業向け情報セキュリティ対策支援施策

政府が 2020 年度に新たに実施した中小企業向け情報セキュリティ対策支援施策を紹介する。

(a) サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)

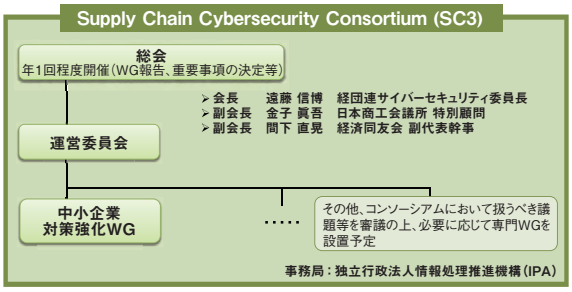
IPA による「情報セキュリティ 10 大脅威 2021[※391]」において、組織への脅威として第 4 位に「サプライチェーンの弱点を悪用した攻撃」が位置付けられているとおり、製造から販売までを含む一連の商流(サプライチェーン)において、セキュリティ対策が強固でない中小企業が攻撃の標的となることで、サプライチェーンに関わる組織が連鎖的に被害を受けるケースが懸念されている。

このような背景のもと、経済産業省は、2020 年 6 月、産業を巡るサイバーセキュリティの状況認識と、今後の取り組みの方向性を取りまとめた報告書[※56]を公表した。本報告書では、企業のリスクマネジメント強化のための基本行動指針として、以下の三つが提示された。

①共有:サプライチェーンを共有する企業間における高密度な情報共有
②報告:機微技術情報の流出懸念がある場合の報告
③公表:多数の関係者に影響する恐れがある場合の公表

そして 2020 年 11 月、この基本行動指針へのコミットメントとともに、産業界を挙げて中小企業を含むサプライチェーン全体のサイバーセキュリティ対策強化を目指す枠組みとして「サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3:Supply Chain Cybersecurity Consortium)[※392]」が設立された(次ページ図 2-4-17)。

SC3 中小企業対策強化 WG では、サイバー攻撃に



■図 2-4-17　SC3 の組織体制
(出典)IPA「サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)」

遭った際の事後支援を中心とした中小企業向けサイバーセキュリティ対策支援の仕組みである「サイバーセキュリティお助け隊サービス」の民間によるサービス展開に向けた検討が行われた(「2.4.2 (2) (b) 中小企業向けサイバーセキュリティ対策支援体制構築事業」参照)。

本検討に基づき、IPA は、2021 年 2 月に「サイバーセキュリティお助け隊サービス」の内容を明確化、同サービスとして充足すべき基準を「サイバーセキュリティお助け隊サービス基準 (1.0 版)※393」として策定・公表した。そして、同基準を充足するサービスのブランド化を通じて普及を図り、中小企業における無理のないサイバーセキュリティ対策の導入・運用について支援を進めることとした。

今後 SC3 では、サイバー攻撃の実態や官民における取り組み等についての情報共有、取引先企業が求める中小企業のセキュリティ水準についての検討等を予定しており、中小企業を含むサプライチェーン全体のサイバーセキュリティ対策について業界横断的な活動を展開していくことが期待される。

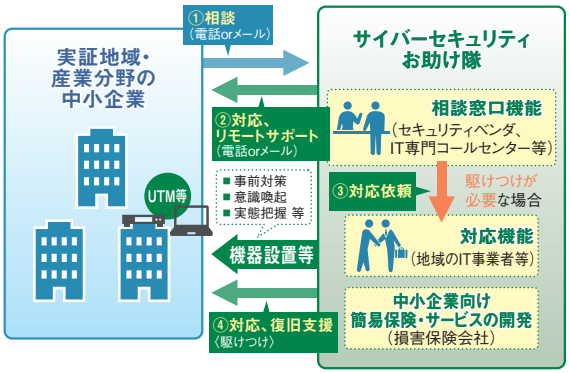
(b) 中小企業向けサイバーセキュリティ対策支援体制構築事業

経済産業省は 2020 年度、IPA を通じて「中小企業向けサイバーセキュリティ対策支援体制構築事業※54」(サイバーセキュリティお助け隊)を実施した(図 2-4-18)。本事業では、全国 24 道県 13 地域(①北海道、②宮城、山形、秋田、青森、③岩手、④岩手、宮城、福島、⑤千葉、埼玉、⑥千葉、⑦岐阜を中心とする中部エリア、⑧愛知、岐阜、三重、⑨滋賀、奈良、和歌山、⑩香川、⑪福岡、佐賀、長崎、熊本、大分、宮崎、⑫熊本、⑬沖縄)と 2 産業分野(⑭防衛・航空宇宙産業及び⑮自動車産業)の中小企業を対象として、サイバーインシデントが発生した際の事後対策支援を中心に実環境における実証を行い、合計 1,117 社の中小企業が参加した。

本実証においては、EDR (Endpoint Detection and Response) サービスにおける不正プログラム (ブラウザ・ハイジャッカー) の検知と駆除や、ウイルス感染の疑いのある通信の UTM (Unified Threat Management) による検知と駆除等の対応を行った。2020 年度は、新型コロナウイルスの影響もあり、リモートで管理可能な支援サービスの提供が多く行われ、インシデント発生に際してもおおむねリモートでの支援対応が実施された。また、UTM 機器等により、18 万件超の社内システムへの侵入等を試みる不審なアクセスが検知される等、2019 年度実証結果と同様に、業種や規模を問わず中小企業においても例外なくサイバー攻撃の危険に晒されていることが明らかとなった。本実証に参加した中小企業からは「サイバー攻撃が可視化され実際に攻撃を受けていることが認識できてよかった」「サイバーセキュリティ対策を実施していることは取引先に対する PR 材料にもなり、良いきっかけをもらえた」等の声が寄せられた。

このようなサイバー攻撃の危険があっても、人材・コスト面での制約もある中でセキュリティ対策に取り組むことができる中小企業は多くない。「サイバーセキュリティお助け隊サービス」の今後の民間でのサービス展開に際しては、個別の細やかなサポートと同時に、サービス内容のスリム化や導入・運用負荷を下げることが必要と考えられる。

2021 年度以降は、2 年間の実証事業で得られた知見、及び SC3 中小企業対策強化 WG の議論を踏まえた「サイバーセキュリティお助け隊サービス」のブランド化・普及により、中小企業において無理なくサイバーセキュリティ対策の導入・運用が可能となることが期待される。



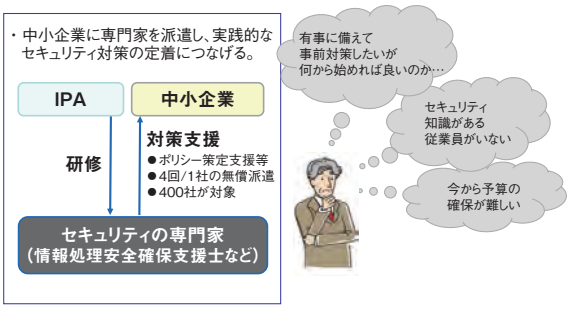
■図 2-4-18　サイバーセキュリティお助け隊の事業イメージ
(出典)IPA「サイバーセキュリティお助け隊(令和 2 年度中小企業向けサイバーセキュリティ対策支援体制構築事業)※54」を基に編集

(c) 中小企業の情報セキュリティマネジメント指導業務

経済産業省は 2020 年度、IPA を通じて、「中小企業の情報セキュリティマネジメント指導業務※394」を実施

した（図 2-4-19）。本事業では、全国の中小企業を対象として、情報処理安全確保支援士等の専門家が訪問し、セキュリティリスクの診断、情報セキュリティマネジメントに必要な基本方針・規程の策定支援等を実施した。

本事業には、全国の中小企業 395 社が参加した。このうち 97.6% の企業が成果を得られたと回答し、指導した専門家も 84.4% が指導先企業の経営層の意識が向上したと回答した。また、63.8% の企業が今後も専門家による指導・支援を希望すると回答した。本事業で作成し有効性が確認された指導要領等を、指導ツールとして専門家へ提供すること等が計画されており、今後の中小企業支援に活用されることが期待される。



■図 2-4-19　情報セキュリティマネジメント指導業務の事業イメージ
（出典）IPA「令和２年度中小企業の情報セキュリティマネジメント指導業務」を基に編集

(d) 中小企業サイバーセキュリティ対策促進事業

経済産業省は 2020 年度、「中小企業サイバーセキュリティ対策促進事業（地域 SECUNITY 形成促進事業）」を実施した。本事業では、地域の企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ（地域 SECUNITY）の形成、及びセキュリティ対策の実態把握のための調査やセミナー等を行った。将来的には、地域のニーズとシーズのマッチングによる課題解決・付加価値創出の場（コラボレーション・プラットフォーム）へと発展することを目指している（コラボレーション・プラットフォームについては「2.1.2 (1) (c) WG3（サイバーセキュリティビジネス化）」参照）。

また、2021 年 2 月 17 日、地域のセキュリティコミュニティの活動事例調査を踏まえ、「地域セキュリティコミュニティ【地域 SECUNITY】形成・運営のためのプラクティス集第 1 版[※395]」を公開した（図 2-4-20）。本資料では、コミュニティ形成の際に参考となる事例とポイント、地域のセキュリティコミュニティが主催するイベント等で活用できるセキュリティ講師派遣制度等の情報・問い合わせ先リストがまとめられている。

■図 2-4-20　地域セキュリティコミュニティ【地域 SECUNITY】形成・運営のためのプラクティス集のイメージ
（出典）経済産業省「地域セキュリティコミュニティ【地域 SECUNITY】形成・運営のためのプラクティス集」

(3) 普及啓発・対策ツール

中小企業に向けた情報セキュリティの普及啓発活動や対策ツールを紹介する。

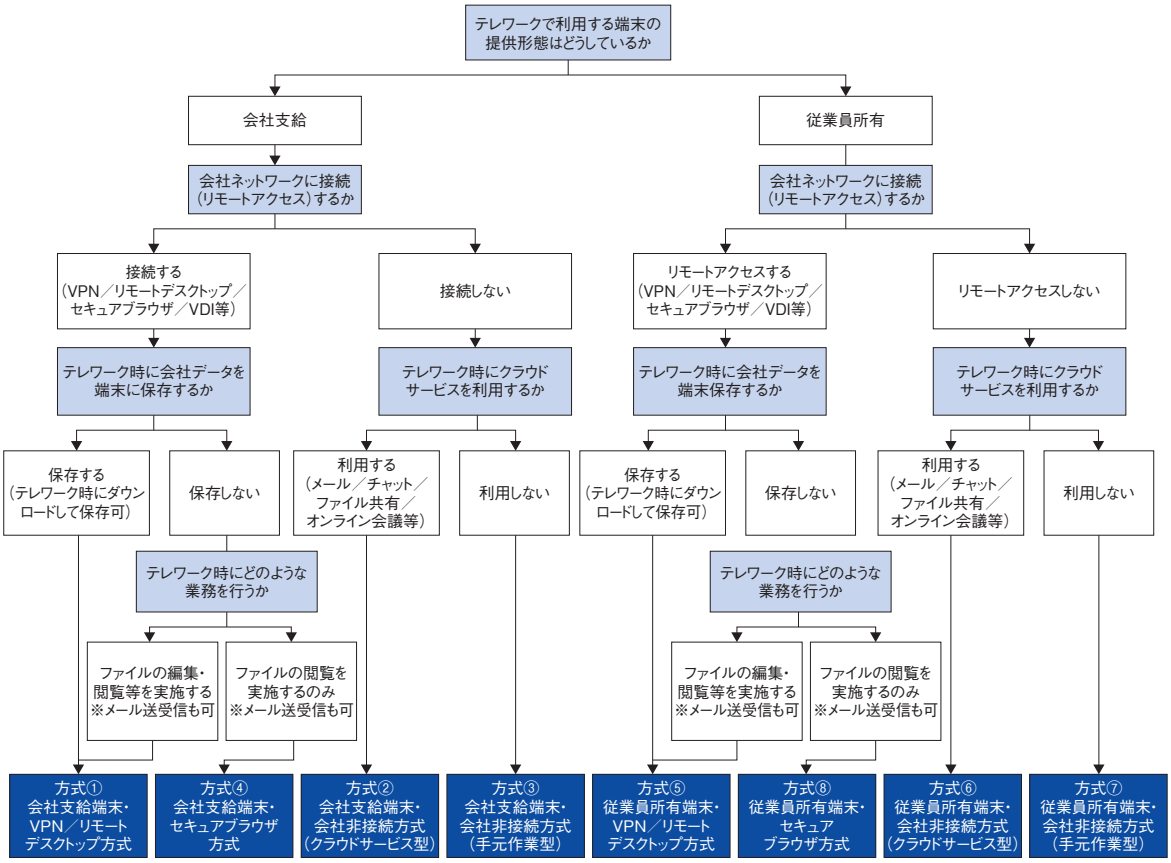
(a) 中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）

総務省は 2020 年 9 月 11 日、「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（初版）」を公表した。本手引きは、セキュリティの専任担当がいないような中小企業等におけるシステム管理担当者を対象として、テレワークを実施する際に最低限のセキュリティを確保するためのチェックリストを提供している。また、テレワークでよく利用されるオンライン会議ツール等の製品（Cisco Webex Meetings、Microsoft Teams、Zoom）の設定解説資料を同時公開している[※396]。

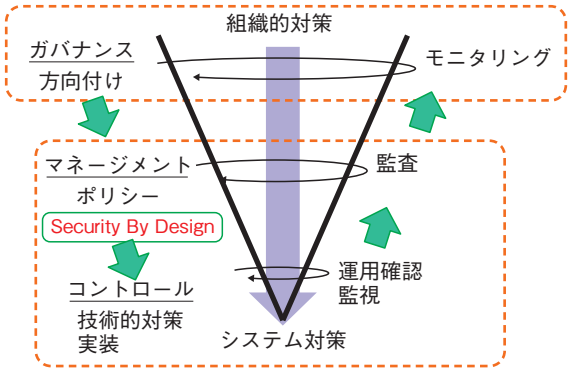
2021 年 5 月 31 日、「テレワークセキュリティガイドライン」の改定を受けて「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（第 2 版）[※397]」を公表した（次ページ図 2-4-21）。今後、設定解説資料への対象製品の追加が予定されている。

(b) 中小企業において目指す Security By Design

JNSA は 2020 年 11 月 5 日、「中小企業において目指す Security By Design[※398]」を公開した（次ページ図 2-4-22）。IT システムの開発・導入においては、機能要件の定義が主になり、セキュリティ機能は非機能要件として、重要視されず、後回しにされることが多々ある。しかし、一般に IT システムの開発・導入においては、後工程での修正程、コストが増加する傾向にあり、IT システム導入後、十分なセキュリティ対策を行うことは、



■図 2-4-21　テレワーク方式確認のフローチャート
(出典)総務省「中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)(第２版)」



■図 2-4-22　V 字モデルにおける「Security By Design」の位置付けのイメージ
(出典)JNSA「中小企業において目指す Security By Design」

困難となる。従って、IT システムの企画･設計段階から、セキュリティを考慮した設計(Security by Design)の導入が重要となる。本資料では、中小企業の情報システム部門が考えるべき IT システムの導入、運用、廃止までのライフサイクルを考慮した情報セキュリティのあるべき姿の検討結果をまとめている。

(c) SECURITY ACTION

IPA では、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度「SECURITY ACTION[※399]」を運営し、中小企業と関連の深い中小企業支援機関、士業団体、IT 関連団体と連携して SECURITY ACTION を通じた情報セキュリティの普及啓発を行っている(図 2-4-23)。

SECURITY ACTION に基づく自己宣言は、秋田県リモートワーク環境整備支援事業費補助金や堺市テレワーク導入支援補助金の申請要件になっていたほか、公的な補助金制度の申請要件としても活用されている。

2021 年 3 月末時点の宣言数は 14 万件(個人事業主を含む)を超えている。今後より多くの中小企業が SECURITY ACTION を宣言し、社内の意識付けや

■図 2-4-23　SECURITY ACTION のロゴマーク

社外への信頼性のアピール等に活用し、対策を推進することが望まれる。

2.4.3 教育機関・政府及び地方公共団体等法人における対策状況

教育機関・政府及び地方公共団体等法人における対策状況について、公表されている資料に基づいて述べる。

(1) 教育機関における個人情報紛失・漏えいの現状、文部科学省の対策、事故の事例

教育ネットワーク情報セキュリティ推進委員会（ISEN：Information Security for Education Network）は、毎年、学校等教育関連機関で発生した個人情報の紛失・漏えい事故について公開情報を調査し、公表している。2020年11月には、「令和元年度（2019年度）学校・教育機関における個人情報漏えい事故の発生状況 −調査報告書− 第2版※400」（以下、ISEN報告書）を公表した。本項では、ISEN報告書に基づいて、2019年4月1日～2020年3月31日の事故の傾向について述べる。次いで、政府が示している対策を紹介した後、事故事例について述べる。

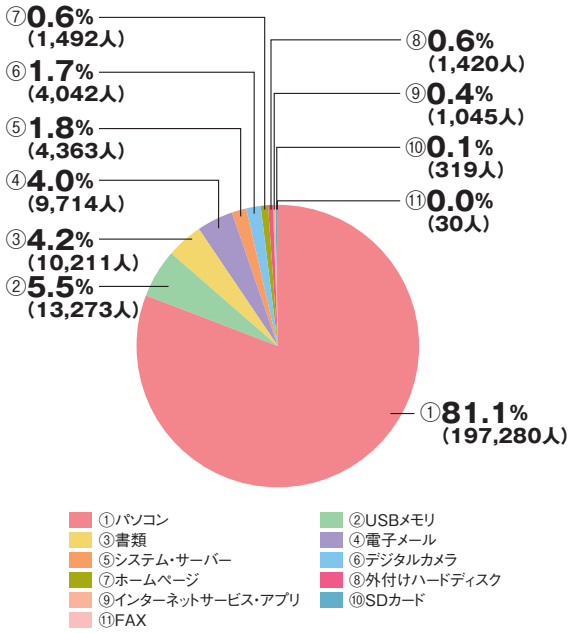
ISEN報告書によると、2019年度は226件の個人情報漏えい事故が発生し、合わせて23万2,857人分の個人情報が漏えいした。過去2年（2018年度5万7,629人、2017年度12万7,278人）に比べ急増しており、過去15年のうちで2番目に多い年度であった。

漏えいした個人情報の人数を経路・媒体ごとに比較すると、図2-4-24に示すように、2019年度は「パソコン」が全体の81.1%を占めており、2位の「USBメモリ」（5.5%）以下を大きく引き離している。

また事故の種類ごとの発生件数を調べると、「紛失・置き忘れ」「盗難」「誤廃棄」のように「意図せず失くす」事故が全体の約67%に上ることが分かる（図2-4-25）。

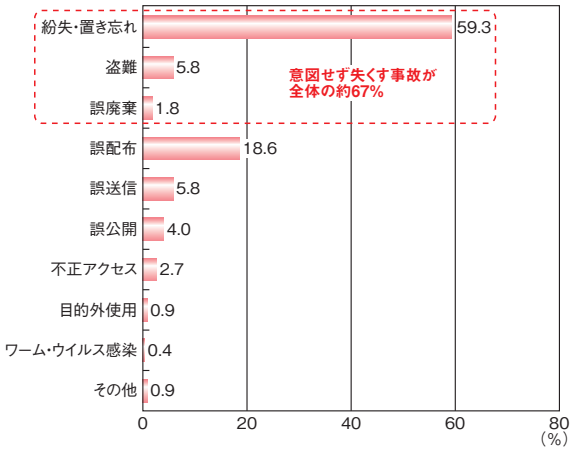
これらのことから、ノートパソコンやUSBメモリ等可搬性のある媒体を失くすことによる個人情報漏えいの対策に取り組むことで、大きな改善が見込めると推察される。

これらに有効な対策として、文部科学省の「教育情報セキュリティポリシーに関するガイドライン※401」では、ログインパスワード、起動時のBIOS・ハードディスク等のパスワード、多要素認証、セキュリティチップの暗号化機能、遠隔消去機能（リモートワイプ）等の利用を挙げている。また同ガイドラインでは、モバイル端末の持ち出しや外部での作業の実施は許可制とするのが適切であるとしており、情報セキュリティポリシーの例文に、端末や電子媒体の持ち出し・外部での作業の制限に関する事項を含めている。



※1件の事故で複数の経路・媒体から漏えいした場合は、それぞれの経路・媒体に含まれていた個人情報漏えい人数を合算

■図2-4-24 漏えい経路・媒体別個人情報漏えい人数
（出典）ISEN報告書を基にIPAが作成



■図2-4-25 漏えい事故種別発生割合
（出典）ISEN報告書を基にIPAが作成

次に、教育機関等における個人情報紛失の事故事例を取り上げる。2020年2月29日、金沢大学の教員が海外出張中にノートパソコンの盗難に遭い、教職員と学生の個人情報2万件以上を含むデータファイルを紛失した。これらの個人情報は、持ち出すにあたって保護管理者の許可を得ておらず、またパスワード設定等の対策も施されていなかった※402。2021年2月8日、東京藝術大学は、受験関係書類等個人情報115件が入った教員のノートパソコンが、学内の研究室から盗まれた

と発表した。これらの情報を格納したファイルには、パスワード設定が施されていなかった※403。2021年3月5日、立教大学は、91名分の一般選抜に関する個人情報が入ったUSBメモリを紛失したと発表した。USBメモリとファイルには、パスワードロック等の対策が施されていなかった※404。

このように、パソコンやUSB等個人情報を保存した媒体を意図せずに失くし、かつ有効な対策が施されていない事例が後を絶たない。前述のガイドライン等を参考に、対策の徹底が望まれる。

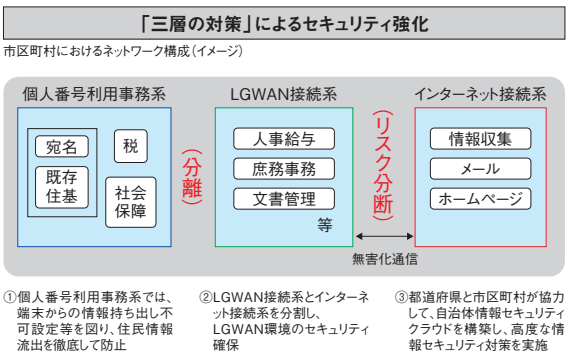
(2) 地方自治体等における対策状況

本項では、自治体等の情報セキュリティ対策とその課題、及び課題解決・改善のための対策見直しについて、総務省が2020年5月に公表した「自治体情報セキュリティ対策の見直しについて※405」(以下、「対策見直し」)に基づき、一部に他の公的機関や地方自治体から公表された資料を参照して述べる。

(a) 地方自治体等の従来対策

2015年5月、日本年金機構において、標的型攻撃による約125万件の個人情報流出が起きた。これを受け総務省は、同年12月に総務大臣通知「新たな自治体情報セキュリティ対策の抜本的強化について」を出し、自治体に「三層の対策」を講じるよう要請した。この対策は、自治体のネットワークを、住民情報等の特に機密性の高い情報を扱う「マイナンバー利用事務系」、職員に関する機微情報や非公開情報等の機密性の高い情報を扱う「LGWAN※406接続系」、インターネットメールや機密性の低い情報を扱う「インターネット接続系」の三つのセグメントに分離・分割するものである(図2-4-26)。

特に「マイナンバー利用事務系」(図2-4-26では「個人番号利用事務系」)をセグメントに分離することにより、



■図2-4-26 「三層の対策」によるセキュリティ強化
(出典)総務省「自治体情報セキュリティ対策の見直しのポイント※407」

住民情報の徹底した流出防止を図っている。この要請を受け、自治体は「三層の対策」への対応を2017年7月までに完了した。

更に、自治体では総務省の指導のもと、「自治体情報セキュリティクラウド」を構築した。それまで自治体ごとに行われていたインターネット接続と情報セキュリティ対策を、原則、都道府県単位に集約することで、セキュリティ対策の水準引き上げを図る施策である。

(b) 課題

前項で述べた対策の課題、発生したインシデントにより見えてきた課題について述べる。

- 従来対策の課題

  「対策見直し」によれば、これらの従来の対策により、インシデントやウイルスへの感染は、短期間で大幅に減少したという。その一方で、ネットワークを分離・分割したことでユーザビリティが下がり、自治体の事務効率に影響していると指摘された。具体的には、住民等によるオンラインの行政手続きデータをマイナンバー利用事務系に取り込んだり、メールの添付ファイルを取得したりすることが制限されているとの指摘である。加えて、働き方改革に伴うテレワーク実施やWeb会議、グループウェア等コミュニケーションツールの利用に制約がある等の課題も浮き彫りになった。

  また、自治体情報セキュリティクラウドについても、自治体へのアンケート調査の結果等から、個々のクラウドによって導入している機能や運営事業者のレベルに差異があることが判明した。また次に述べるインシデント等により、機器故障時や災害発生時の可用性等に課題があることが判明した。

- 重大インシデントにより判明した課題

  2019年12月、日本電子計算株式会社による自治体向けクラウドサービスに障害が発生、全国53団体の業務に影響し、自治体事務の一部には長期の支障が残った。直接の原因は、故障したストレージに依存しているシステムが利用できなくなったこと、データバックアップが不十分だったこと等であり、障害時の可用性の確保に課題があることが判明した。

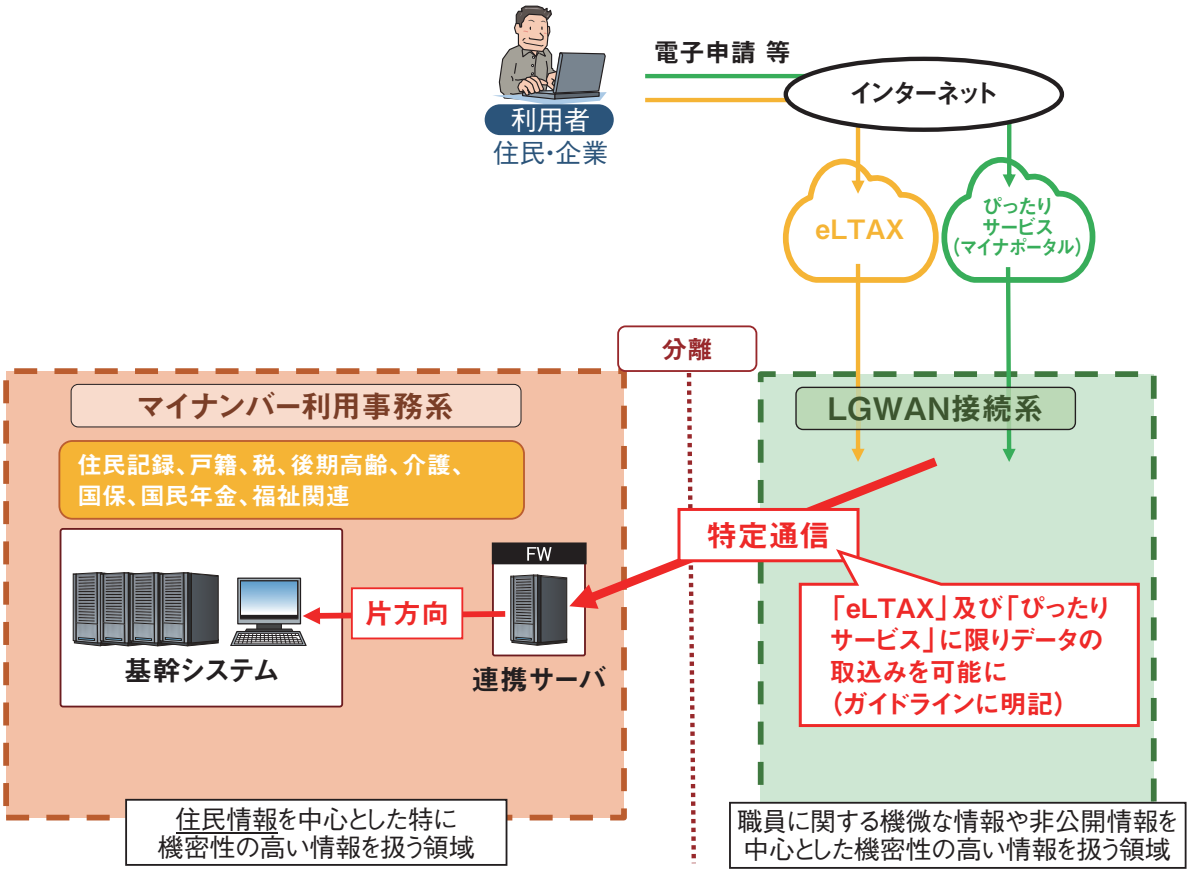
  また同月、神奈川県において、契約満了でリース事業者に返却され廃棄予定だったハードディスクが、不正に売却されたことによる情報流出のインシデントが発生し、対策の不備が判明した。当面の対応として、重要な情報を格納する記憶装置の廃棄にあたっては、物理的・磁気的に破壊すること、これらの処置

の完了まで自治体職員が立ち会うこと等の要請が行われた。

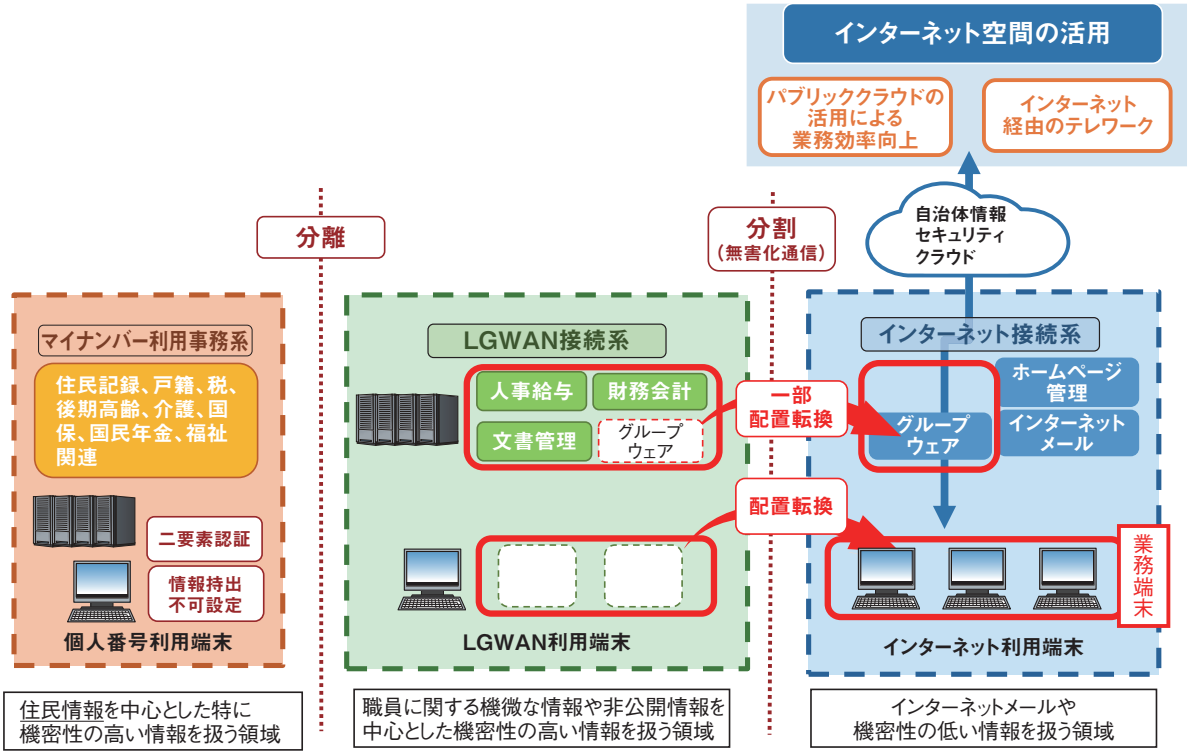
(c) 課題解決・改善のための対策見直し及び関連する動き

前述の課題を解決・改善する対策について、「対策見直し」に記載された主な事項とそれに関連した地方自治体・公的機関の動きについて述べる。

- 「三層の対策」におけるマイナンバー事務処理系の分離の見直し
  住民情報の流出防止徹底を重視し、マイナンバー事務処理系の他セグメントからの分離は、従来どおり維持した上で、住民等からのインターネット経由の申請データ等をこのセグメントに取り込めるように見直すとしている。具体的には、十分なセキュリティが確保されていることを国が確認した特定の通信(「eLTAX※408」と「ぴったりサービス※409」)を経由する場合に限って、データを取り込めるようにする(図 2-4-27)。
- 「三層の対策」における LGWAN 接続系とインターネット接続系の分割の見直し
  自治体内部の業務端末や、人事給与、財務会計等内部管理のシステムは、これまで LGWAN 接続系のセグメントに配置されていた。この一部については、業務効率改善を目的として、インターネット接続系に移動する新たなモデルが示された(次ページ図 2-4-28)。ただし、自治体がこのモデルを採用するには、セキュリティを維持するための条件を満たすことが求められる。具体的には情報資産単位でのアクセス制御、セキュリティ監視やセキュリティインシデントへの即応体制(CSIRT)の整備、職員のセキュリティリテラシーの向上等である。
- 自治体向けのテレワークの仕組みの検討
  本見直しまで、セキュリティ確保の観点からリモートアクセスの利用は限定的であったが、働き方改革等の動きを受け、テレワークの導入検討が検討会※410で行われた。まず、インターネットを介さずに LGWAN 接続系へリモートアクセスするための技術要件等が検討され、2020 年 1 月に中間報告が取りまとめられた。また、地方公共団体情報システム機構(J-LIS:Japan Agency for Local Authority Information Systems)は 2020 年 10 月、IPA と共同で、自治体職員が自宅から LGWAN 接続系のパソコンに接続する仕組み

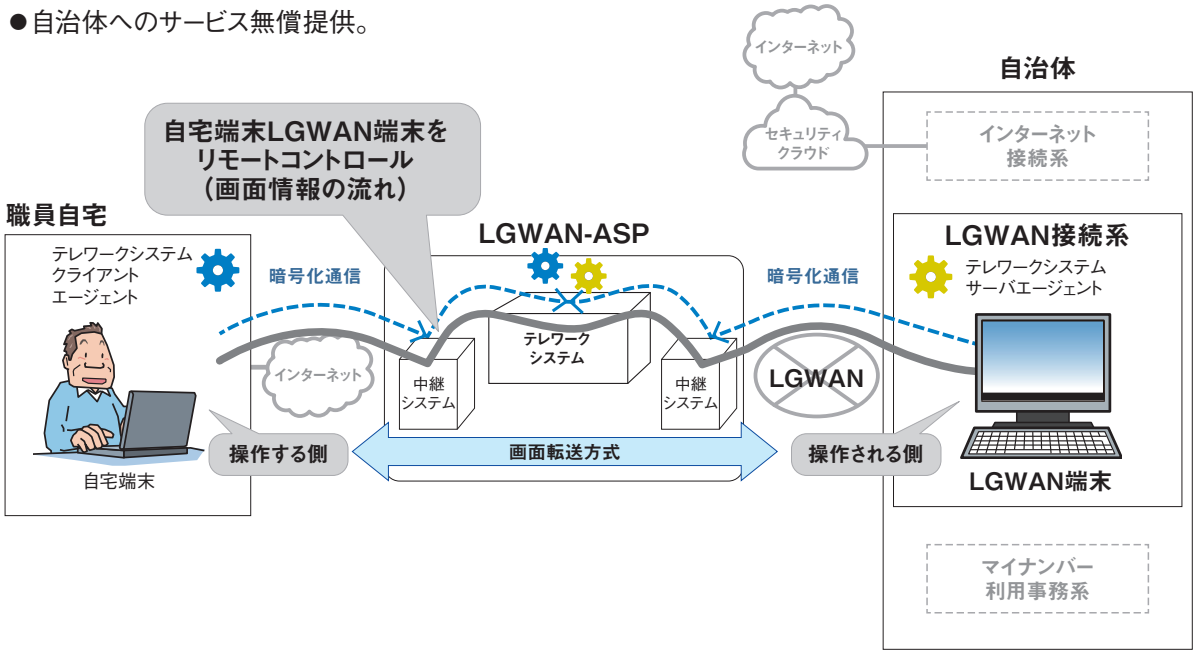


■図 2-4-27　マイナンバー利用事務系の分離に係る見直し
(出典)総務省「自治体情報セキュリティ対策の見直しのポイント」を基に IPA が編集



■図 2-4-28　LGWAN 接続系とインターネット接続系の分割の見直し
（出典）総務省「自治体情報セキュリティ対策の見直しのポイント」を基に IPA が編集

●職員宅から自治体LGWAN接続系へのテレワークを可能とするサービス提供。（リモートコントロール方式）
●LGWAN-ASPを介した職員自宅と自治体庁内の接続。
●自治体へのサービス無償提供。



■図 2-4-29　自治体テレワークシステム for LGWAN
（出典）J-LIS「緊急事態宣言（令和3年1月）の発出に伴う『自治体テレワークシステム for LGWAN』の一時提供について※412」を基に IPA が編集

「自治体テレワークシステム for LGWAN」（図 2-4-29）を提供し、テレワークの実証実験を行うとした※411。更に、新型インフルエンザ等対策特別措置法の規定に基づく緊急事態宣言の発出に伴い、自治体事務の業務継続の観点からテレワークの必要性が高まったことを受けて、2021 年 1 月、宣言の対象区域となった都道府県の自治体に対して、上記システムを一時的に提供することとなった※412。

- 自治体情報セキュリティクラウドの見直し

  自治体情報セキュリティクラウドは更新の時期が近づいており、前述の「対策見直し」は、サイバー攻撃の増加等の変化を踏まえた次期クラウドの在り方の検討が必要であるとしている。

  また現行の自治体情報セキュリティクラウドは、機能や運営事業者のレベルにばらつきが見られるが、次期クラウドではこうしたばらつきを抑え一定の水準を確保するため、総務省が標準的な要件を整備・提示することが望ましいとしている。2020年8月、総務省はこれを受けて、次期自治体情報セキュリティクラウドに係る標準要件※413を取りまとめ、公表した。

  また「対策見直し」は、新たなセキュリティ脅威に対抗するために、SOC※414の強化も必要であるとしている。加えて、災害発生時等に住民からのアクセスが輻輳した場合でも情報発信機能の可用性を維持するため、CDN※415が必要であるとしている。これらの要件は、前述の標準要件に盛り込まれた。

  こうした動きを背景に、各自治体では、それぞれが運営する自治体情報セキュリティクラウドの更新に向けて、具体的な取り組みが進められている。例えば、三重県では現行のセキュリティクラウドが2022年3月に保守期限を迎えることから、システム全体のクラウド化を前提としたシステム構築の検討を始める※416としており、茨城県でも同様の検討が始まっている※417。

- その他の対策見直し

  「対策見直し」では、自治体におけるクラウドサービスの選定にあたっては、クラウド上で運用するシステムごとに必要な可用性が提供されることを確認したり、SLA※418を含む契約を推進したりすることが必要としている。また、リース満了等による機器の廃棄に際しては、格納情報の機密性に応じた適切な廃棄の手法等を採用することも必要としている。

  総務省は、2020年12月に、本項で述べた検討内容を踏まえて「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改訂を行った（「2.1.3(3)(a)自治体情報セキュリティ対策」参照）。

2.4.4 一般利用者における対策状況

IPAが実施した「2020年度情報セキュリティに対する意識調査【倫理編】【脅威編】※419」の報告書の内容、及び追加分析の結果を基に、一般利用者におけるセキュリティ対策状況とその背景等を考察する。

2020年度調査では、対策の実施状況の設問において、パソコン利用者向けに20項目、スマートデバイス利用者向けに17項目の小問を設け調査した。図2-4-30（次ページ）と図2-4-33（次々ページ）は、それらの項目について、対策の実施率※420を高い順から並べたものである。なお、本項ではグラフの項目名を本文中で省略して記載する場合がある。

(1) パソコン利用者の対策状況

対策の実施率が高かった上位3位は、「怪しいと思ったウェブサイトに行き着いたら先に進まない、情報を入力しない」（76.9%）、「メールの添付や本文中のURLを不用意にクリックしない」（69.6%）、「ファイルのダウンロード時に安全性や信頼性を判断」（69.5%）であった。また上位8位までの実施率が50%を超えており、一般利用者において、基本的なセキュリティ対策がある程度定着していることがうかがえる（次ページ図2-4-30）。

下位3位は、「重要なファイルはパスワード付USBメモリでの持ち出し、パスワードをかけてメールを送信する」「無線LANルータの暗号化キーの変更」「HDDなど外部記憶装置全体の暗号化」であり、いずれも2割強の実施率であった。これら対策の実施率は例年最も低い傾向である。

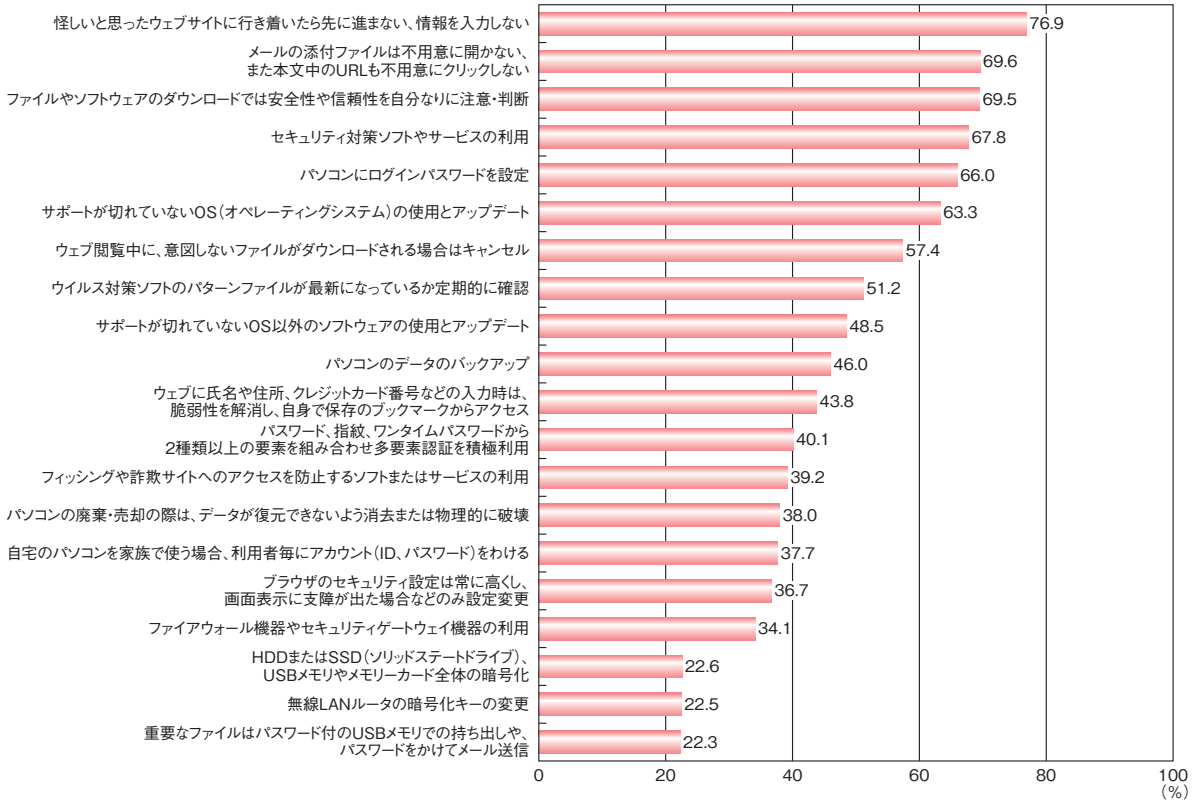
基本的なセキュリティ対策の一つとして挙げられる「サポートの切れていないOSの使用とアップデート」の実施率が全体では63.3%であったが、性別で実施率に差があり、男性が69.4%、女性が55.0%と約15%の開きがあった（次ページ図2-4-31）。

一方、男女で実施率がほぼ同程度となった対策は三つあった。それらは専用のソフトウェアや機器を使う必要がなく、自身の知識や注意等、意識次第で実施可能な対策で、「家族で自宅のパソコンを使う場合、利用者ごとにアカウントを分けている」「怪しいと思ったウェブサイトに行きついたら先に進まない、情報を入力しない」「パソコンにはログインパスワードを設定している」であった（次ページ図2-4-32）。

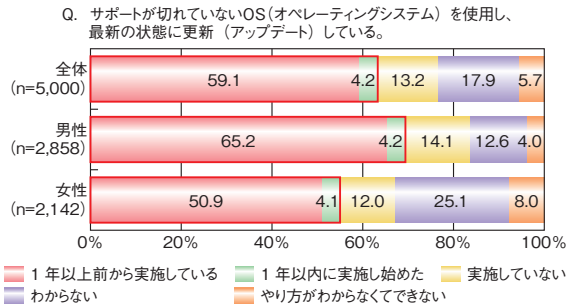
(2) スマートデバイス利用者の対策状況

2019年度以前の同調査では、スマートフォンやタブレットの利用を念頭に置いた対策の実施状況を調査していたが、本年はスマートスピーカーやネットワークカメラ等に対する対策の項目も新たに設けた。

対策の実施率が高かった上位3位は、「端末内のアプリのアップデート」（63.6%）、「公式サイト、マーケットか



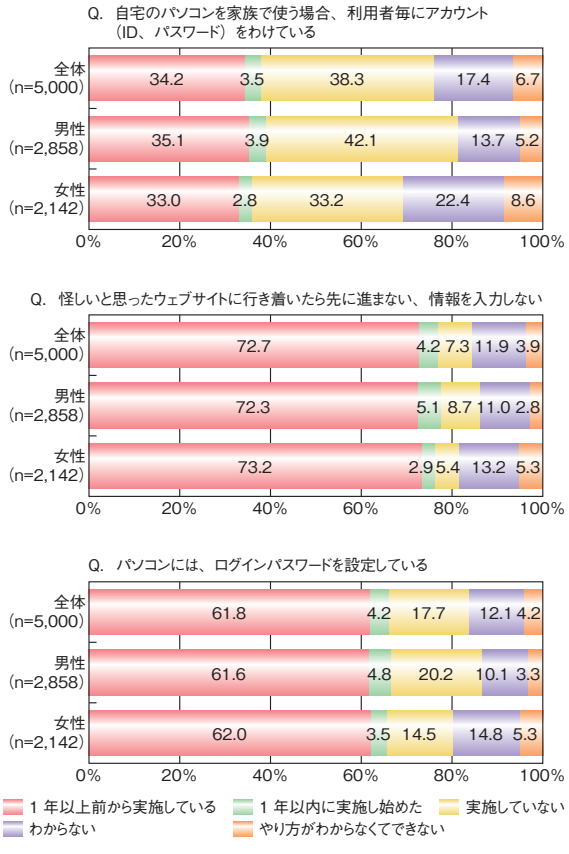
■図 2-4-30　パソコン利用者の対策実施状況



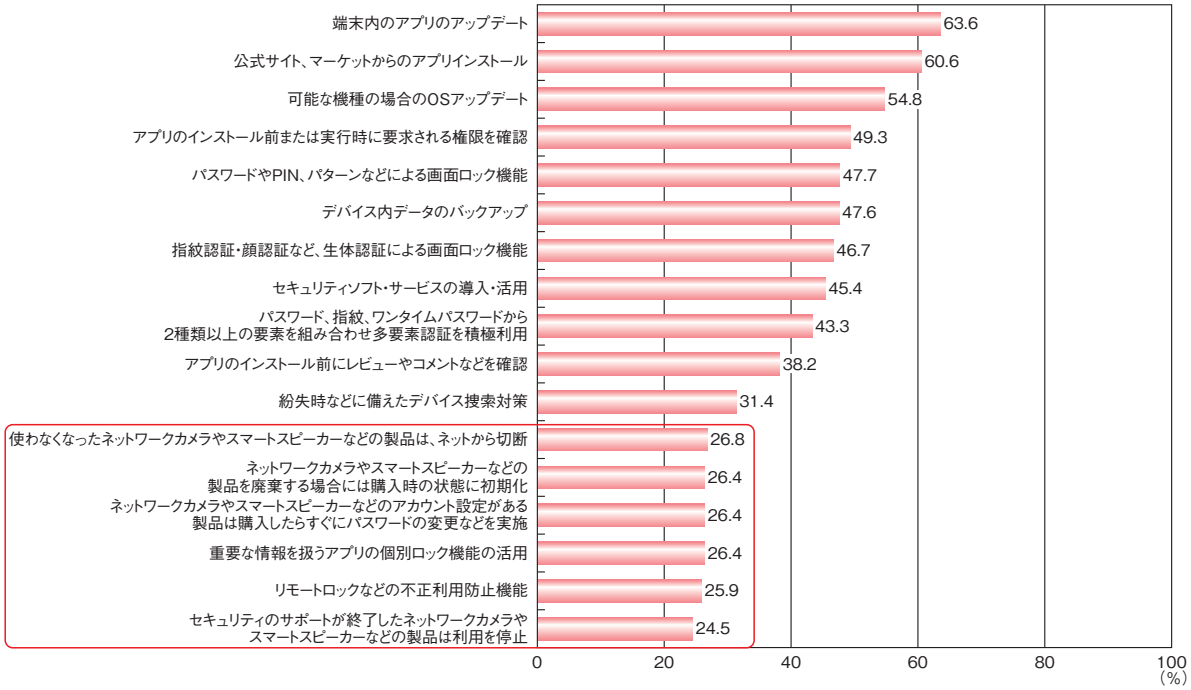
■図 2-4-31　パソコン利用者の OS アップデートに関する対策実施状況

らのアプリのインストール」（60.6%）、「OS のアップデート」（54.8%）であり、スマートフォンに求められる基本的な対策が並んだ（次ページ図 2-4-33）。反対に実施率が低かったのは、今回の調査で新たに設けた四つの項目と、スマートフォンのリモートロック設定及びアプリの個別ロック機能の活用に関する項目、の計六つ（次ページ図 2-4-33 の赤枠部分）で、いずれも 25% 前後の実施率であった。

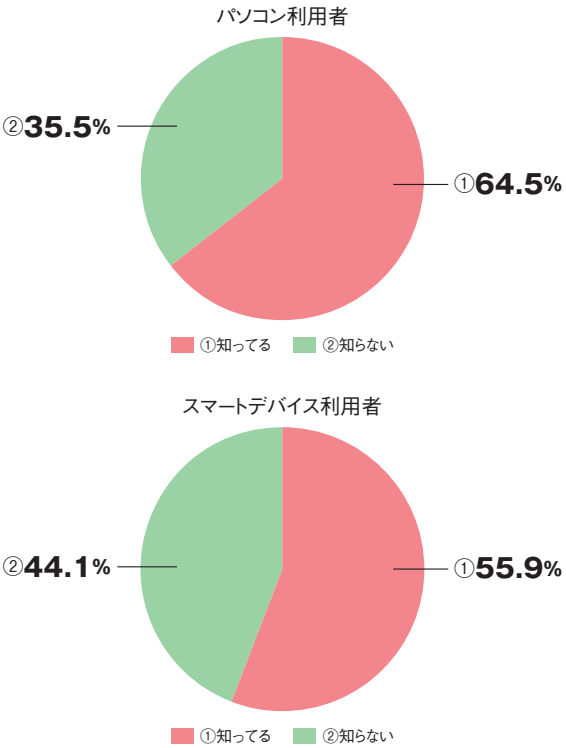
今回の調査結果から、IoT 機器のセキュリティ対策の実施状況はまだ途上で、対策の必要性及び方法について一層の普及啓発が必要と考えられる。



■図 2-4-32　パソコン利用者で男女の実施率が同程度の対策実施状況



■図 2-4-33　スマートデバイス利用者の対策実施状況



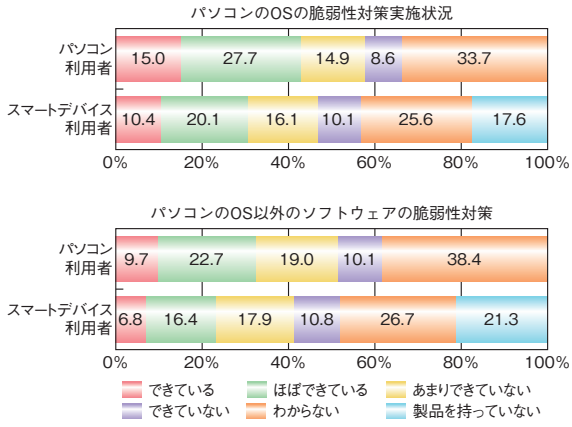
■図 2-4-34　パソコン利用者とスマートデバイス利用者の脆弱性対策に関する認識

(3) パソコン利用者とスマートデバイス利用者の比較

図 2-4-30（前ページ）と図 2-4-33 を比較すると、設問が一部異なるものの、全体的にスマートデバイス利用者の方が対策の実施率が低かった。

共通の設問としてセキュリティ対策の基本である脆弱性対策について尋ねており、その結果を紹介する。ソフトウェアに脆弱性対策が必要なことを「知っている」と回答した割合はスマートデバイス利用者の方が低いが、半数以上は対策が必要であることを認識していた（図 2-4-34）。

具体的なパソコン利用時の脆弱性対策の実施状況を尋ねた結果を図 2-4-35 に示す。スマートデバイス利用



■図 2-4-35　パソコン利用者とスマートデバイス利用者の脆弱性対策実施状況

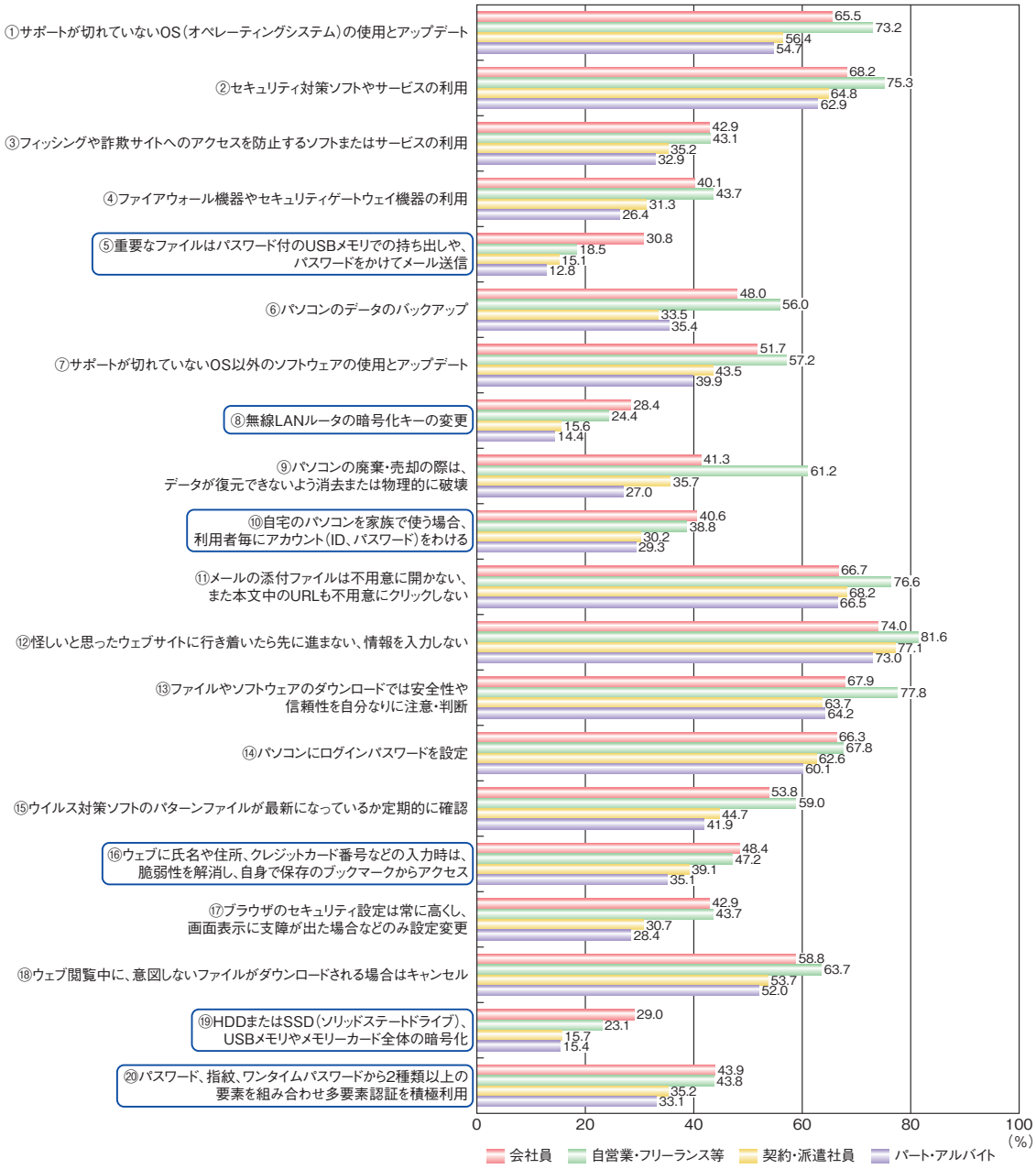
者の中には2割前後、パソコンを所有していないという回答が含まれるが、スマートデバイス利用者の「パソコンのOSの脆弱性対策」の実施率は30.5%、「パソコンのOS以外のソフトウェアの脆弱性対策」の実施率は23.2%であった。OSの場合、昨今は自動アップデートされることも多く、回答者の自覚と対策実施率が必ずしも同期しないと考えられる。しかし、あらゆる脅威への基本対策である脆弱性の解消は、その実施状況を利用者自身が自覚しておく必要がある。

回答者は今後もテレワークを奨励され、私物パソコン、あるいはスマートデバイスを業務に使用する等の可能性がある。テレワーク環境では職場の堅牢なセキュリティ対策は通用しないため、個人の意識と対策が一層問われることになる。なお、包括的なテレワークのセキュリティ対策については「3.3 テレワークの情報セキュリティ」を参照されたい。

(4) 回答者属性別の対策状況の特徴

パソコン利用者の調査結果に基づき、本白書では、情報システム・通信関係の業務に従事・関与しない利用者（会社員、自営業・フリーランス等、契約・派遣社員、パート・アルバイト）に対象を絞り、雇用形態別に回答者の対策状況のグラフを作成した（図2-4-36）。

自営業・フリーランス等と会社員[※421]を比較すると、



■図2-4-36　パソコン利用者の対策実施状況（雇用形態別）

自営業・フリーランス等の方が対策の実施状況が高い傾向にあった。例外は図中の六つの青枠で、これらの項目についてのみ会社員の対策実施率が高かった。

所属組織にもよるが、一般に会社員の方が、情報セキュリティに関する教育機会が多く、対策への認識、実施率は向上していると考えられる。しかし、情報セキュリティ教育が必ずしも提供されていない、自営業・フリーランス等の対策状況が高い結果となった。この理由について考察する。

項目別に見ると、まず「⑨パソコンの廃棄・売却時はデータが復元できないよう消去または物理的に破壊」では会社員よりも自営業・フリーランス等の実施率が約 20 ポイント高い。会社員が職場で使用するパソコンは通常、自身で廃棄処理を行う必要はほぼないと思われる。一方、自営業・フリーランス等は業務用パソコンの購入から廃棄までを自身で行うと考えられる。そのため、会社員が私物パソコンを所有していたとしても、廃棄における対策の必要性については、自営業・フリーランス等より認識が高くない可能性がある。

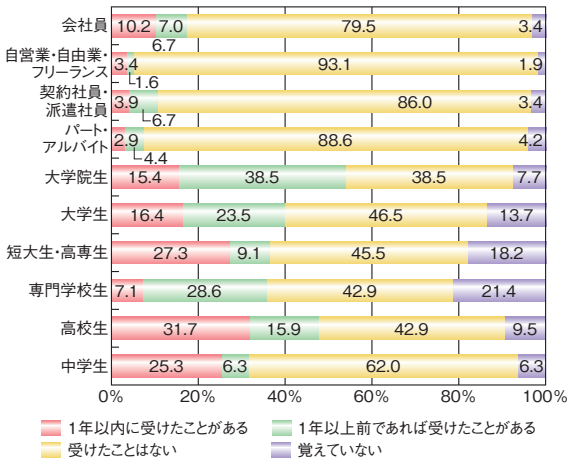
次に「⑪メールの添付ファイルや本文にある URL を不用意にクリックしない」「⑬ファイルなどのダウンロードでは安全性や信頼性を注意・判断する」では、自営業・フリーランス等が会社員より約 10 ポイント、対策実施率が高い結果であった。具体的な割合は⑪が 76.6%、⑬が 77.8% で、全体ではいずれも 69% 程度であるので、それと比較しても高い※422。自営業・フリーランス等は取引先とデータやファイルのやり取りをするために各種 Web サービスの利用頻度が高いと考えられる。そのため、セキュリティ対策への意識を高く持ち、対策を徹底していると考えられる。

続いて「⑤重要なファイルはパスワード付 USB で持ち出しや、メールはパスワードをかけて送信」について比較する。この項目では、自営業・フリーランス等の対策実施率が会社員に比べ 12.3 ポイント低い結果であった。加えて「⑲ HDD、USB メモリーカード全体の暗号化」の実施率も約 6 ポイント低い結果であった。

この 2 点について会社員の実施率が高いのは、勤務先のルールや対策の徹底が功を奏している可能性が考えられる。外部記憶媒体はデータの授受や持ち運びに便利なツールであるが、ひとたび紛失すれば、個人情報や営業秘密等の漏えいインシデントにつながり得る。そのため、多くの企業は情報持ち出し規則の周知やセキュリティ教育、暗号化機能が付いた媒体の利用等を徹底している。一方、自営業・フリーランス等は時にセキュリティ対策が十分といえない相手との仕事も避けられないと思われる。このような環境の違いが数値の差に表れていると考えられる。

一方で、契約・派遣社員の対策の実施率は、⑪、⑫を除きすべての項目で自営業・フリーランス等及び会社員と比較して低くなっている。例えば「⑩自宅のパソコンを家族で使う場合、利用者毎にアカウントをわける」については、契約・派遣社員及びパート・アルバイトの実施率は会社員及び自営業・フリーランス等と比べ 10 ポイント程度低い結果が見られた。

そこで、セキュリティに関する教育機会について尋ねた結果を見ると（図 2-4-37）、学生と社会人とで顕著な差が見られた。社会人の中で最も受講経験のある人の割合が高い会社員であっても、「過去に受講経験がある」とする回答は 17.2% と学生に比べ極めて低い。社会人には、雇用形態に合わせた多様な教育機会が提供されることが必要である。教育機関との連携や地域のコミュニティ等、職場以外でも学べる場を充実させていくことが望まれる。



■図 2-4-37　セキュリティ教育の受講経験

COLUMN

コロナ禍で「インターネット安全教室」はどのように変わったか

コロナ禍により人々の生活は様々な場面で大きな変化を求められることになりましたが、その一つに多くの組織で実施をしている「集合研修」が挙げられます。集合研修という知識や情報を共有する有効な手段がストップしたことは大きな痛手だったのではないでしょうか。

IPA でも集合研修形式で「インターネット安全教室」を全国各地で開催していました。インターネット安全教室は、家庭や学校等からインターネットにアクセスする一般利用者に向けた基本的な情報モラル・セキュリティの普及啓発の場、また、情報モラル・セキュリティ教育の指導者を育成する場となるものです。

2020 年度のインターネット安全教室では、集合研修形式に加えて、新型コロナウイルス感染症対策の一環として、初めてオンライン形式を導入しました。オンライン形式での開催は、依頼者の要望に合わせ、①講師及び参加者全員が Web 会議サービスを用いて開催するケース、②講師または参加者のどちらかがオンラインで接続し開催するケースの 2 種類の形式で行いました。

オンライン形式の導入により、交通アクセス等の事情で例年は受講がかなわなかった方も参加が可能になり、より広範囲での普及啓発が実現した一方で、課題や工夫を要する点も見えてきました。以下、開催にあたって必要となる対応や今後の課題についてご紹介します。併せて、IPA の「Web 会議サービスを利用する際のセキュリティ上の注意事項」（https://www.ipa.go.jp/security/announce/webmeeting.html）もご参照ください。

①事前準備について

インターネット安全教室では Web 会議サービスを利用する環境が整っていない参加者が多くいるため、タブレット端末、モバイル Wi-Fi ルータ、接続ケーブル等の機器の貸出しを行いました。また、オンライン講演の開催経験が浅い団体向けには事前に機器や Web 会議サービスの利用方法について、事務局からのレクチャーや入念な接続テストを行いました。オンライン形式では、開催者側はオフラインの場合と比較して、より入念な事前準備が必要であるといえます。

②講演中の対応について

インターネット安全教室では、参加者の反応を講演者が把握するため、ネット環境や個人情報の問題がなければ可能な限りビデオをオンにした状態で行いました。ビデオをオンにした状態で Web 会議を行う際は周囲の映り込みに注意を促すことが必要です。

チャット機能の使用やグループワーク等で参加者が発言する機会を用意すると、講演者側からの一方通行を防ぐことができます。また、オンラインでの講演に際して、意図しない第三者からのいたずらを防ぐため、参加者の制限を行う等の注意が必要です。

③講演後の対応について

講演後に行うアンケートの回収率は、集合形式の場合と比較して下がることが課題として挙げられます。オンライン形式では講演中の回収が難しく、現在は講演後、参加者にアンケートフォームにアクセスして回答していただく形をとる等、受講者側の手間を一つ増やす形を取っていますが、受講者の自発性に頼ることも限界があるため、改善の余地があるといえます。

2.5 国際標準化活動

国際標準とは、製品や技術を、国境を越えて利用するために制定される国際的な共通規格であり、国際規格とも呼ばれる。国際標準化は第4次産業革命時代の鍵を握る※423として、日本も積極的に活動に参画している。本節では、セキュリティ分野に関わる国際標準化活動の動向を紹介する。

2.5.1 様々な標準化団体の活動

日本の国際標準化活動への取り組みと、作成プロセスや作成組織の違いから見た標準の分類、及び情報セキュリティ分野の主な標準化団体の概要を示す。

(1) 日本の国際標準化活動への取り組み

企業が培ってきた技術や知的財産の秘匿化や、それらを知財として権利化する「クローズ戦略」に対して、標準化は「オープン戦略」に位置付けられている。クローズ戦略により企業のコア領域を守り、他社との差別化を図ることは重要であるが、その技術を利用する市場が広がらなければ、企業としては事業を拡大することが困難である。コア領域を守りつつ、市場を拡大する「オープン&クローズ戦略」が必要である。技術の発展、市場のグローバル化が進み、このオープン&クローズ戦略の考え方は企業にとどまらず、国の政策として位置付けられるようになった。知的財産戦略本部による「知的財産推進計画2020※424」では、デジタル技術を活用した社会的課題解決の取り組みを、複数の主体による協働・共創を通じて、持続可能なビジネスとして定着・拡大させていく上で、標準を戦略的に活用することも重要であるとしている。

2020年7月、国立研究開発法人産業技術総合研究所は「標準化推進センター」を設置した※425。政策的ニーズや産業界のニーズに基づく業界・領域横断的な分野の標準化を主導するとしている。また、標準化の専門人材として「標準化オフィサー」を新設し、標準化の専門知識と経験を活かして、ステークホルダー間の調整や標準の普及策検討等、標準化を一貫して推進するとしている。

(2) 標準の分類

国際標準には、公的な標準化団体により所定の手続きを経て行われる「デジュール標準(de jure standard)」、いくつかの団体(企業等)が協力して自主的に作成する「フォーラム標準(forum standard)※426」、公的な標準化団体を介さず、市場や業界において広く採用された結果として事実上標準化される「デファクト標準(de facto standard)」がある。

デジュール標準では、幅広くステークホルダーを集めて議論をとおして合意形成を行う。次項で紹介するISO、IEC、ITUが作成する国際規格やJIS等の国家規格が該当し、策定プロセスが規定されており、様々な規制等に用いられることも多い。合意形成のために複数の検討段階が設定されており、正式に発行するまでに時間がかかる(ISO/IECは約3年)。

フォーラム標準は業界団体等、共通の関心を持つ企業等が集まって議論し、業界ルール等限定的な範囲で合意される標準である。作成スピードは速く、業界の特性が反映されていることから該当する業界内では利用が促進されやすい。次項で紹介するIEEE、IETF、TCGが発行する標準が該当する。コンソーシアム標準と呼ばれることもある。業界のフォーラム標準が、その後、国際標準化団体に提案され、時間をかけてデジュール標準となる場合もある。

電気製品やIT製品等、開発サイクルの短い分野では、その時点の市場で一般的な規格としてデファクト標準が採用される傾向にある。例えばWindowsのようなOSやGoogleのような検索エンジン等、グローバルなIT企業の製品・サービスが事実上の国際標準となる傾向があり、合意形成プロセスは存在しない。

(3) 情報セキュリティ分野に関する標準化団体

情報セキュリティに関連するデジュール標準やフォーラム標準の策定を行っている主な国際標準化団体を以下に示す。

- ISO(International Organization for Standardization:国際標準化機構)/IEC(International Electrotechnical Commission:国際電気標準会議)JTC 1(Joint Technical Committee 1:第一合同技術委員会)※427:情報セキュリティを含む情報技術の国際規格を策定している。コンピュータや情報分野を扱う国際標準化団体としてISO、IECはそれぞれ独立に存在しているが、扱う領域の競合を避けるために双方が連携し、JTC 1が設立された。日本国内の標準化団体としては、日

本産業標準調査会（Japanese Industrial Standards Committee：JISC）がISO、IEC双方のメンバーであり、JTC 1でも活動している※428。

- ITU-T（International Telecommunication Union Telecommunication Standardization Sector：国際電気通信連合 電気通信標準化部門）：
  電気通信技術に関わる国際規格を策定している。情報セキュリティに関してはSG（Study Group）17が設置され※429、ISOや後述するIETFとともにネットワークやID管理等に関する標準化活動を行っている。策定した標準はITU勧告として定められる。

また、情報セキュリティ分野に関するフォーラム標準を策定する代表的な組織として、以下のようなものがある。

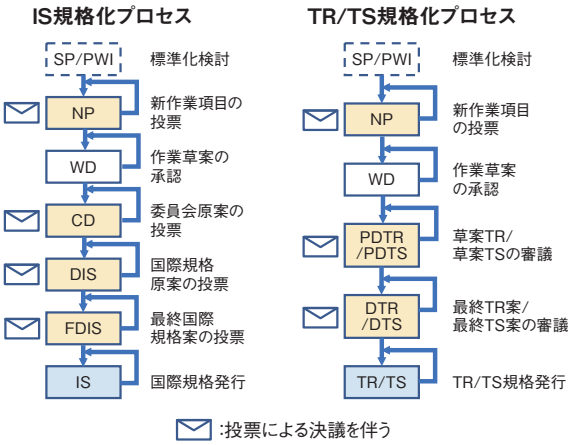
- IEEE（The Institute of Electrical and Electronics Engineers, Inc.）：
  電気工学・電子工学技術に関する国際学会である。標準化活動は内部組織であるIEEE-SA（Standards Association）が行っている。情報セキュリティについては、サイバーセキュリティ、ネットワークセキュリティ、IoTセキュリティ等の広範な領域で標準化を行っている。
- IETF（Internet Engineering Task Force）：
  インターネット技術の国際標準化を行う任意団体である。非常にオープンな組織であり、作業部会のメーリングリストに登録することで誰でも議論に参加することができる。情報セキュリティについては、インターネット上のセキュアなプロトコル、暗号、署名、認証、セキュリティ情報連携（セキュリティオートメーション）等の方式の標準化を行っている※430。標準化した技術文書はRFC（Request For Comments）として参照することができる。
- TCG（Trusted Computing Group）：
  信頼できるコンピューティング環境（組み込み機器、パソコン／サーバ、ネットワーク等）に関するセキュリティ技術の標準化を行う業界団体である。ハードウェア、ソフトウェア等のベンダやシステムインテグレータがメンバーとなり、中国、日本にregional forumがある※431。

2.5.2 情報セキュリティ、サイバーセキュリティ、プライバシー保護関係の規格の標準化（ISO/IEC JTC 1/SC 27）

ISO/IEC JTC 1/SC 27（以下、SC 27）は、ISO及びIECの合同専門委員会（ISO/IEC JTC 1）において、情報セキュリティに関する国際標準化を行う分科委員会（SC）である。SC 27は、テーマ別に以下の五つのWGで構成される。

WG 1：情報セキュリティマネジメントシステム
WG 2：暗号とセキュリティメカニズム
WG 3：セキュリティの評価・試験・仕様
WG 4：セキュリティコントロールとサービス
WG 5：アイデンティティ管理とプライバシー技術

ISO/IECにおける標準化作業は、策定する仕様の完成度によって図2-5-1のような状態があり、それぞれ各国の投票によって次の段階へ進む。なお、ISOにおいて、技術が未成熟である、またはガイダンス等の標準仕様ではないが重要であるとされたものは、技術報告書または技術仕様書として出版する。



■図2-5-1　ISO/IEC JTC 1/SC 27における文書のステータス
（出典）JISC「ISO規格の策定手順※432」を基にIPAが作成

図2-5-1の各文書のステータスと略号は以下のとおりである。なお本文中では、略号を使用する。

SP：研究期間（Study Period）
PWI：予備業務項目（Preliminary Work Item）
※SPとPWIのどちらを実施するかはWGによって異なる。
NP：新作業項目（New work item Proposal）
WD：作業原案（Working Draft）
CD：委員会原案（Committee Draft）
DIS：国際規格原案（Draft International Standard）
FDIS：最終国際規格案（Final Draft International Standard）
IS：国際規格（International Standard）
PDTR：予備技術報告原案（Preliminary Draft Technical Report）
PDTS：予備技術仕様書原案（Preliminary Draft Technical Specification）
DTR：技術報告書原案（Draft Technical Report）

DTS：技術仕様書原案（Draft Technical Specification）
TR：技術報告書（Technical Report）
TS：技術仕様書（Technical Specification）

以下に、各 WG の活動概要を述べる。

（1）WG 1（情報セキュリティマネジメントシステム）

WG 1 では、情報セキュリティマネジメントシステム（ISMS：Information Security Management System）に関する国際規格として、ISO/IEC 27001（ISMS 要求事項を示す規格）及び ISO/IEC 27002（情報セキュリティ管理策及び実施の手引きを示す規格）を中心に、ISO/IEC 27001 が示す ISMS 要求事項に関する手引きや指針を提供する規格、ISO/IEC 27001 及び ISO/IEC 27002 を土台とする分野別規格、及びその他トピックスに関する ISO/IEC 27000 ファミリー規格の国際標準化活動を実施している。

(a) ISO/IEC 27001 及び ISO/IEC 27002 の改訂に関する状況

2013 年の改訂から 5 年を経ている ISO/IEC 27002:2013 については、2018 年 3 月までの 1 年間の SP において、次期改訂の設計仕様（Design Specification）が決定され、改訂作業が開始された。2018 年 4 月に WD の初版を発行、エキスパートレベルでの審議を行い、2018 年 11 月には CD の初版を発行、国レベルでの審議にステージを移した。2021 年 4 月現在は、DIS 投票中の状況にある。管理策の全体構成も固まり、管理策の具体的な内容を決める最終段階となっている。2021 年 4 月の投票結果、及び 6 月に予定されている国際会合の結果によって FDIS 発行となるかが決定される。

ISO/IEC 27001:2013 については、2019 年に実施された、改訂の必要性を各国に問う定期レビューの結果、Confirm（改訂しない）という結論となり、改訂作業は開始されていない。これは、ISO/IEC 専門業務用指針、第 1 部において規定されたマネジメントシステム規格の共通フォーマットが改訂中である状況を考慮し、並行して ISO/IEC 27001 を改訂することは、改訂作業を複雑にすると考えての結論であった。しかし、2021 年 4 月現在、ISO/IEC 27002 の改訂が最終段階となったこと、また、管理策の構成等が現版から大きく変わることを受け、ISO/IEC 27001: 2013 の Annex A のみを改訂版 ISO/IEC 27002 と整合するように変更することを決定した。

(b) 分野別規格の国際標準化活動

分野別規格作成に関する要求事項を示す規格である ISO/IEC 27009 は 2016 年に発行された後、2017 年から早期改訂が行われ、2020 年 4 月に改訂版が発行された。2021 年 4 月現在は、ISO/IEC 27002 の改訂が最終段階になったことを受けて、それに伴う ISO/IEC 27009 の早期改訂についての検討を予定している。

分野別規格そのものについては、通信事業者のためのガイドライン規格 ISO/IEC 27011:2016、セクター間及び組織間コミュニケーションのためのガイドライン規格 ISO/IEC 27010:2015、クラウドサービスカスタマ及びプロバイダ向けのガイドライン規格 ISO/IEC 27017:2015 が発行済みである。これらは、いずれも ISO/IEC 27002 を拡張した分野別規格であるため、現在進行中の ISO/IEC 27002 の改訂が完了すれば、それに伴って改訂が行われる見込みである。実際、ISO/IEC 27011:2016 については、既に改訂を開始しており、WD を発行、エキスパートレベルの審議を行っている。

一方、ISO/IEC 27009 は、ISO/IEC 27001 を特定分野に適用した規格を作成する際の、規格の記述方法や様式等を定めた規格であり、ISO/IEC 27002 だけを対象に、特定分野に特化して修正することは適用範囲としていない。ISO/IEC 27009 に適合する規格としては、エネルギー分野に関する規格として ISO/IEC 27019:2017、プライバシー情報マネジメントに関する規格として ISO/IEC 27701:2019[※433] が発行済みである。なお、ISO/IEC 27701 については、これに基づく認証に対する市場ニーズが高いことから、ISO/IEC 27701 の認証機関に対する認定基準となる ISO/IEC TS 27006-2 を早期に策定するため、WG 1 と WG 5 の共同プロジェクトを開始、2020 年 2 月に発行に至った。また、ISO/IEC TS 27006-2 の発行に伴い、ISO/IEC 27001 の認証機関に対する認定基準 ISO/IEC 27006 についても、ISO/IEC 27006-1 への改番が必要となり、これに対応した改訂が予定されている。

(c) サイバーセキュリティ関連の国際標準化活動

サイバーセキュリティに関する規格化については、まず、サイバーセキュリティの既存のフレームワークと ISO 及び IEC 規格類との対応関係を示した技術報告書 ISO/IEC TR 27103 が 2018 年に発行された。次いで、サイバー保険に関する規格 ISO/IEC 27102 が 2019 年に発行された。サイバーセキュリティのフレームワーク構築に関する技術仕様書 ISO/IEC TS 27110 は 2021 年

2月に発行された。本規格は規格番号を27101として検討を進めてきたが、27110に変更しての発行となった。また、サイバーセキュリティの概念やコンセプトに関する技術仕様書ISO/IEC TS 27100についても2020年12月に発行された。

(d)その他のISO/IEC 27000ファミリー規格の国際標準化活動

ISO/IEC 27001:2013への本格的対応を積み残している情報セキュリティリスクマネジメントに関するガイドライン規格ISO/IEC 27005:2018については、2021年4月時点も改訂中でCDを審議中である。ISO/IEC 20000-1及びISO/IEC 27001の統合実践に関するガイドライン規格であるISO/IEC 27013:2015は、ISO/IEC 20000-1:2018の発行を受けて、2021年4月時点で改訂中であり、DIS投票を終え、結果に基づく国際会議の場での審議を予定している。情報セキュリティガバナンスの原則、及びプロセスの手引きを提供するISO/IEC 27014については、改訂を終えて2020年12月に発行された。

(2)WG 2(暗号とセキュリティメカニズム)

WG 2では、暗号プリミティブ(暗号アルゴリズム)や、デジタル署名技術、鍵共有のような汎用的かつ基本的な暗号プロトコル等の標準化を行っている。WG 2の国際主査、副主査ともに日本人が選出され、WG 2での活動をリードしている。2020年度は、新しい規格の発行はなかったが、既存規格10件の改訂版が発行された。このほかの主な活動内容について以下に示す。

(a)完全準同型暗号の規格化検討

完全準同型暗号は、暗号化したままで加算や乗算の両方が計算可能な公開鍵暗号である。完全準同型暗号を使用すれば、計算のためにデータの復号を行う必要がないため、守秘性の高いデータ処理を外部業者に委託する場合においても、負担をかけずにリスクを抑えることが可能となる。

2020年4月に米国より、この完全準同型暗号の規格化が提案され、議論を重ねた結果、2021年4月にISO/IEC 18033(暗号アルゴリズム)の第8部として規格化提案の投票にかけることが合意された(2021年6月現在投票中)。

(b)耐量子計算機暗号の文書を一般公開

耐量子計算機暗号[※434]の文書を2年程かけ作成してきたが、文書作成作業がいったん完了し、「ISO/IEC JTC 1/ SC 27/WG 2 Standing Document 8(SD8) Post-Quantum Cryptography[※435]」として2020年6月に一般公開された。

(3)WG 3(セキュリティの評価・試験・仕様)

WG 3は2020年4月、9月にZoomにて定期会合を開催した。なお、定期会合はサンクトペテルブルグ(ロシア)、ワルシャワ(ポーランド)での開催が予定されていたが、新型コロナウイルスのためキャンセルされ、オンライン開催となった。それらの会合の議論内容、特に新しい規格を開発するためにPWI[※436]でなされた議論に焦点を当てて以下に概説する。

(a)PWI“Evaluation criteria for connected vehicle information security based on ISO/IEC 15408”

自動車がネットワークにつながることで利便性が向上したと同時に、自動車に対するサイバー攻撃の脅威も高まっている。米国では、研究者がChryslerブランドの車両のエンジンを切る、ワイパーを動かす等のリモートハッキングを行って見せた[※437]。これに先立ち、事前通知を受けていたFCA US LLC(旧Chrysler Group LLC)は2015年7月にハッキング対象機種140万台のリコールを発表した[※438]。

そのような背景もあり、2020年6月にUNECE[※439]の自動車基準調和世界フォーラムWP.29にて自動車のサイバーセキュリティ基準が採択された。またISO/TC 22/SC 32/WG 11では、車載機器製造時に順守すべきサイバーセキュリティ要件やガイドラインを定めた「ISO/SAE 21434 Road vehicles — Cybersecurity engineering」の策定が進められている[※440]。しかしながら、自動車へのリモートハッキングの対象となっている車載エンターテインメントシステムや、エンジンやブレーキを制御する電子制御ユニット(ECU:Electronic Control Unit)に対し、具体的にどのような脆弱性分析や侵入テストを実施すべきかを定めた規格や指針は存在せず、WP.29のサイバーセキュリティ基準やISO/SAE 21434においてもその技術的詳細には一切触れられていない。

そのため、WG 3では2019年4月のテルアビブ会合から車載機器のセキュリティ評価基準に関する議論を行っていたが、2021年4月のZoom会議において、今までの議論結果をベースに新たな規格を開発するための新業務項目提案を行うことが合意された。なお、本PWIでは日本エキスパートがPWIのメンバーとして議論

に参加している。

(b) PWI “A general framework for runtime hardware security assessment”

半導体チップに集積されるトランジスターの数は、「ムーアの法則」に従い着実に増加し、最新のマイクロプロセッサーには、10 億個を軽く超える膨大な数のトランジスターが集積されている。また、その設計・製造には様々な企業が関わっており、ハードウェアトロイの脅威が高まっている。ハードウェアトロイとは、半導体チップに不正に仕込まれ、トリガーとなる事象（例えば、特定の入力等）が生じた場合に不正な活動を行う、悪意を持つ回路である。現在、マイクロプロセッサー等のハードウェアコンポーネントの稼働状況をモニタリングすることにより、ハードウェアの異常な振る舞いを検出する技術に関する研究が各国の研究者により進められている。

日本においても同様なテーマを題材にした総務省の「設計・製造におけるチップの脆弱性検知手法の研究開発」が立ち上がっており、そのプロジェクトメンバーも本 PWI の一員として議論に参加している。今後日本は、本プロジェクトの成果をベースに、ハードウェアトロイを検知するハードウェアモニタリング回路の評価手法に関し、その知見を本 PWI にインプットしていく予定である。

(c) PWI “Multi-party coordinated vulnerability disclosure and handling”

WG 3 では、IT 製品の脆弱性の開示・取り扱いに関する以下の二つの標準を既に出版している。

- ISO/IEC 29147：脆弱性情報の開示に向けて開発者に必要となるやり取り（外部からの脆弱性に関する情報の受領等）に関わる要件を規定
- ISO/IEC 30111：脆弱性取り扱いのプロセス（脆弱性の検証等）の要件を規定

しかしこれら二つの規格では、脆弱性を取り扱う関係者が多岐に渡るような場合に誰がどのような対応をすべきであるかに関する詳細な説明がされていない。例えば CPU に脆弱性が検出された場合、その脆弱性を修正するためには、CPU のみでなく CPU 上で稼働するファームウェア、オペレーティングシステムや各種ソフトウェアの更新が要求されるケースがある。また、複数の製品に共通して使用されているソフトウェアライブラリに脆弱性が発見されるといったケースも多々存在する。

本 PWI では、そのような多数の開発者が関わる脆弱性の取り扱いに際し、関係者間で協業、また時には分業しながら、脆弱性に関する情報を利用者に適切なタイミングで提供し、速やかに更新プログラムを開発し、利用者に更新プログラムを確実に提供するための指針を提供することを目指している。なお、本 PWI においても日本から脆弱性の取り扱いに関わるエキスパートが参加し、その知見を本活動に生かしている。

(d) 2020 年出版規格

2020 年には、日本のエキスパートがエディタとして多大な貢献をした以下の規格が出版された。なお、ISO/IEC 19989 に関しては、産業界にインパクトがある標準として、ISO よりプレスリリースが配信されている※441。

- ISO/IEC 19989-1 “Criteria and methodology for security evaluation of biometric systems – Part 1: Framework”
- ISO/IEC 19989-2 “Criteria and methodology for security evaluation of biometric systems – Part 2: Biometric recognition performance”
- ISO/IEC 19989-3 “Criteria and methodology for security evaluation of biometric systems – Part 3: Presentation attack detection”
- ISO/IEC 20897-1 “Physically unclonable functions – Part 1: Security requirements”

(4) WG 4（セキュリティコントロールとサービス）

WG 4 では、WG 1 が対象とする ISMS を実施・運用する際に必要となる具体的なセキュリティ対策、及びセキュリティサービスの標準化を行っている。以下に、WG 4 における 2020 年度の主な成果、活動を紹介する。

(a) IoT セキュリティ／プライバシーのための標準化活動

WG 4 では、IoT セキュリティ／プライバシーに関わる標準化として、以下の三つの活動を継続的に進めている。当初は、ばらばらの三つの規格としての位置付けだったが、2020 年に体系的な検討がなされ、Cybersecurity – IoT security and privacy と名付けられたプロジェクト群（ISO/IEC 27400 シリーズ）として規格番号の見直しを行い、規格間でも適切な参照を行うように修正された。

- ISO/IEC 27400（旧 27030）: Cybersecurity – IoT security and privacy – Guidelines
- ISO/IEC 27402: Cybersecurity – IoT security and privacy – Device baseline requirements
- ISO/IEC 27403（旧 24391）: Cybersecurity – IoT

security and privacy –Guidelines for IoT-domotics

（ア）ISO/IEC 27400: Cybersecurity – IoT security and privacy – Guidelines

日本は、IoT 関連の製品・システム開発の競争力を強化し、また IoT の国際的なセキュリティレベル向上に寄与するために、IoT 推進コンソーシアムが策定した「IoT セキュリティガイドライン※442」の国際標準化を提案した。具体的には、本ガイドラインに基づき、ISO/IEC 27400（IoT のセキュリティとプライバシー）、ISO/IEC 30147（IoT システム／サービスの信頼性のための方法論）の二つの規格案がそれぞれ SC 27/WG 4、及び SC 41/WG 3 で審議されている。以下に ISO/IEC 27400 の規格について概説する。

ISO/IEC 27400 の具体的内容にあたる第 5 章以降では、第 5 章で参照モデル、各利害関係者の役割、IoT ライフサイクルに触れ、第 6 章では IoT システムにおけるリスクマネジメントについて言及している。第 7 章では、セキュリティ対策及びプライバシー対策が、サービス開発者／サービスプロバイダ、ユーザのそれぞれの立場での対策内容、目的、導入ガイドといったガイドライン的な表現で記載されている。ここで、IoT 機器製造業者は IoT サービス開発者の中に含まれる。2020 年 9 月の SC 27/WG 4 オンライン会議（以下、2020 年 9 月オンライン会議）にて策定されたドキュメントの枠組みは以下のとおりである。

第 1 章～ 4 章：スコープ、文献、用語定義等
第 5 章：IoT 概念と参照モデル
　5.1 概要
　5.2 IoT システムの特徴
　5.3 IoT システムの利害関係者（利用者、サービス提供者、サービス開発者）
　5.4 IoT エコシステム
　5.5 IoT ライフサイクル
　5.6 ドメインに基づく参照モデル
第 6 章：IoT システムのリスクマネジメント
　6.1 導入
　6.2 リスク源（リスクソース）
　6.3 リスクシナリオと IoT システムのリスク
第 7 章：セキュリティ／プライバシーのための管理策
　7.1 セキュリティ管理策
　7.2 プライバシー管理策

2020 年 9 月オンライン会議において、ISO/IEC 27400 は CD3 となっており、次の段階では DIS への移行が想定できる完成度となっている。本規格に対するコメントは、日本、スイス、フランス、カナダ、ドイツ、インド、中国等の多くの機関から大量に提出されており、審議は継続的に極めて活発である。本規格は IoT セキュリティ及びプライバシーの規範となるガイドラインであるため、IoT 利害関係者における認証等への活用が期待されている。

（イ）ISO/IEC 27402: Cybersecurity – IoT security and privacy – Device baseline requirements

本規格は、米国が主導で進めており、IoT 機器が備えるべきセキュリティメカニズムのベースラインとなる要求条件の規定を目指している。ISO/IEC 27400 とは異なるスコープを掲げ、IoT 機器に特化した要件化を視野に入れ、NIST 及び ETSI（European Telecommunications Standards Institute：欧州電気通信標準化機構）の既存のガイドラインを下敷きに標準化を進めている。2020 年 4 月に WD1 が審議されたものの、NIST や ETSI の既存規格に基づいているため、一定の完成度と判断され、2020 年 9 月オンライン会議では、CD1 として進むことが決定された。通常の SC 27/WG 4 における規格策定の進め方としては考えられないスピードで規格策定が推進されている。2020 年 9 月オンライン会議にて策定されたドキュメントの枠組みは以下のとおりであり、IoT 機器製造者、及び IoT 機器のための要求事項がそれぞれ盛り込まれた。

第 1 章～ 4 章：スコープ、文献、用語定義、概要
第 5 章 要求事項
　5.1 IoT 機器製造者のための要求事項
　　5.1.1 リスクアセスメント
　　5.1.2 ユーザへのコミュニケーション
　　5.1.3 脆弱性の開示と処理プロセス
　5.2 IoT 機器のための要求事項
　　5.2.1 識別
　　5.2.2 構成
　　5.2.3 リセット
　　5.2.4 ユーザデータの削除
　　5.2.5 データの保護
　　5.2.6 インタフェースアクセス（Interface access）
　　5.2.7 ソフトウェアとファームウェアのアップデート
　　5.2.8 サイバーセキュリティイベント
　　5.2.9 安全な保存（Secure Storage）
　　5.2.10 データ検証

なお、インタフェースアクセスは、IoT デバイスにおいて、秘密鍵やパスワード等の重要なセキュリティパラメータを共有または再利用するためのインタフェースへのアクセスを許可された権限者に限定することに言及している。また、安全な保存は、ユーザにより IoT 機器で扱われる重要なデータの機器への保存に関するセキュリティ要求事項について述べている。

上記の要求事項に近い内容は、ハイレベルなセキュリティ対策として ISO/IEC 27400 においても触れられており、ISO/IEC 27400 と ISO/IEC 27402 は、ISO/IEC 27400 シリーズ規格として一貫性を確保する形で規格策定が進められている。

(ウ) ISO/IEC 27403: Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics

本規格は、2019 年 4 月テルアビブ会議において、中国から NP として提案され、同年 10 月のパリ会議では、NP の承認がなされ、2021 年 3 月までに WD4 に進んでいる状況にある。「IoT-Domotics」とは、娯楽、機器制御、監視等の用途として、居住環境で利用する IoT サービスをいう。本規格は、ISO/IEC 27400 との棲み分けが難しい部分が多いものの、IoT-Domotics の特性を抽出し、ISO/IEC 27400 とは異なる視点でセキュリティとプライバシーに関するガイドラインとして整理している。具体的には、IoT-Domotics のためのリスクアセスメントの実施を、①アプリケーション、②ネットワーク、③ハードウェアの三点から評価しており、それらの結果を受ける形で、IoT-Domotics を構成するサブシステムや IoT ゲートウェイのためのセキュリティ、及びプライバシーのガイドラインを整理する方向としている。

(b) ビッグデータセキュリティ／プライバシーのための標準化活動

ビッグデータとは、主にボリューム、多様性、速度、及び／または変動性の特性を有し、効率的な保管、操作、分析のためにスケーラブルなアーキテクチャを必要とする広範なデータセットのことを指す。ビッグデータを用いた分析により、より優れた意思決定や戦略的なビジネス行動につながる洞察等を導き出すことができるため、近年注目を浴びている。WG 4 では、ビッグデータのセキュリティ／プライバシーに関わる標準化として、以下の三つの活動を進めている。

- ISO/IEC 20547-4: Big data reference architecture – Part4: Security and privacy
- ISO/IEC 27045: Big data security and privacy – Processes
- ISO/IEC 27046: Big data security and privacy – Implementation guidelines

(ア) ISO/IEC 20547-4: Big data reference architecture – Part4: Security and privacy

ISO/IEC JTC 1/SC 42 で審議されている、ISO/IEC 20547（ビッグデータ参照体系）は四つのパートから成り立っている。そのうちパート 4 は、SC 42 の依頼により SC 27/WG 4 で審議されており、セキュリティ及びプライバシーに関わる参照体系を規定している。本規格は、2019 年パリ会議において DIS に進み、2020 年 4 月オンライン会議で FDIS に進むことが決定し、既に発行されている。

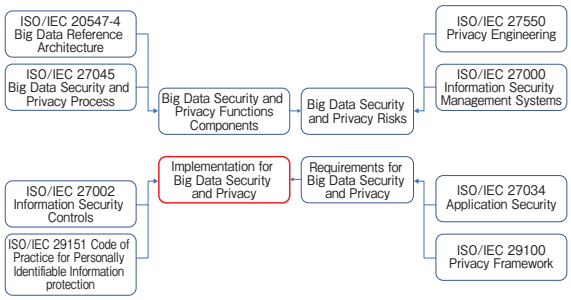
(イ) ISO/IEC 27045: Big data security and privacy – Processes

本規格は、組織のビッグデータのセキュリティとプライバシーを評価及び改善するためのプロセスの参照モデル、評価・成熟度モデルを規定する。プロセスには、プロセスパフォーマンスとプロセス機能の一連のインジケーターが含まれ、評価者が評価の良し悪しを決めるための客観的証拠の基礎として使用される。現在の規格内容は、ISO/IEC JTC 1/SC 7 で規格化されている ISO/IEC 33004、ISO/IEC 33002 等を参照する形で記載されており、2020 年度は数回のオンライン会議を開催して WD3 から WD6 まで規格の改善を進めた。WD6 においては、プロセスの参照モデルを策定し、組織としてのプロセス、マネジメントで必要となるプロセス、技術的なプロセスに分類し、整理を進めた。しかしながら、何度も大きな方針レベルの見直しをこれまで行っているため、規格として安定したものには未だ到達していない状況である。

(ウ) ISO/IEC 27046: Big data security and privacy – Implementation guidelines

本規格は、ビッグデータのセキュリティとプライバシーの主要な課題とリスクを分析し、ビッグデータのリソース、組織化、分散化、計算能力及び破壊等の視点から、ビッグデータのセキュリティとプライバシーの実装のためのガイドラインを記述することを狙っている。2020 年 9 月オンライン会議においては、WD3 への移行が決議され、本規格と他規格との関係については、図 2-5-2 （次ページ）

のように整理された。赤枠部分が本規格に対応する。なお、本図は、規格案（ISO/IEC 27046 WD3）の図 1 として利用されている。



■図 2-5-2　ビッグデータセキュリティ／プライバシーの関連規格間の関係性

（c）WG 4 に関連するその他の規格群

WG 4 では、上記の IoT 及びビッグデータ以外の課題についても、多数の重要な審議を進めている。以下にその審議課題項目、規格の番号、及び審議状況を示す。

- ビジネス継続のための ICT 準備技術（27031）：PWI、NWI の審議を経て、WD1 に進む
- インターネットセキュリティガイドライン（27032）：WD4 に進むことが決定
- ネットワークセキュリティ（27033-7）：ネットワーク仮想化セキュリティのガイドラインとして NP が成立し、WD1 に進む
- アプリケーションセキュリティ（27034）：パート 4 が FDIS に移行、他パートは規格化完了
- インシデントマネジメント（27035）：パート 3 が発行された
- サプライヤー関連セキュリティ（27036）：パート 1 から改版作業を開始
- デジタルエビデンスの識別、収集、確保、保全（27037）：改版作業なし
- リダクション（墨消し技術）（27038）：改版作業なし
- IDPS（侵入検知システム）（27039）：改版作業なし
- ストレージセキュリティ（27040）：大規模な改修を視野に入れ改版作業を開始、現在 WD1
- 仮想化サーバの設計／実装のためのセキュリティガイドライン（21878）：改版作業なし
- 産業用インターネット基盤のためのセキュリティ参照体系（24392）：WD5 に進む
- 仮想化された信頼のルートのためのセキュリティ要件（27070）：DIS に進む
- 公開鍵基盤における実践とポリシーの枠組み（27099）：CD3 に進む
- 機器とサービス間の信頼接続の構築のためのセキュリティ推奨（27071）：WD4 に進む
- 安全な配備、アップデート、及びアップグレード（4983）：NWI 審議を経て、WD1 に進む
- データの起源―参照モデル（データ追跡のため）（5158）：PWI として審議継続
- 情報セキュリティインシデント対応の調整（5189）：PWI として審議継続
- サイバーフィジカルシステムのためのセキュリティ参照体系：PWI として審議（日本提案）

（5）WG 5（アイデンティティ管理とプライバシー技術）

WG 5 では、アイデンティティ管理、プライバシー、バイオメトリクスの標準化を行っている。2020 年度の主な活動を紹介する。

（a）アイデンティティ管理

2013 年 4 月に発行されたユーザ認証についてのフレームワーク規格である ISO/IEC 29115（エンティティ認証保証フレームワーク）は、2020 年秋に改定プロジェクトがキャンセルとなり、複数要素認証等についての技術の状況や他の規格文書との整合性の観点から対象範囲を再検討している PWI 段階にある。

2015 年 6 月に発行された ISO/IEC 24760-2（アイデンティティ管理のフレームワーク パート 2：リファレンスアーキテクチャと要件）の定期見直しにおいては、確認（Confirmation）への投票が最も多く（9 ヵ国）、日本を含む 6 ヵ国が改訂または追補（Revision/Amend）に投票していたが、2020 年 4 月の WG 5 定期会合（オンライン会議）後、日本、フランス、ベルギー、ドイツ、米国、フィリピン、ルクセンブルク、カナダから構成されるアドホックグループが複数回にわたるオンライン会議を行った結果、コンテキストや機能面の改訂の必要性が認められた。現在、WD 段階にある。

2016 年 8 月に発行された ISO/IEC 24760-3（アイデンティティ管理のフレームワーク パート 3：実践）は改訂のための WD 段階にある。

（b）プライバシー

プライバシー対策に関わる ISO/IEC 27701: 2019 は、ISMS の要求事項を規定した ISO/IEC 27001 及び

ISMS を実施するためのプラクティスをまとめた ISO/IEC 27002 に、プライバシー対策に関する要求事項及びプラクティスを加えて拡張することにより、組織による PIMS（Privacy Information Management System：プライバシー情報マネジメントシステム）の構築を支援することを目的としている。2019 年 8 月に IS として発行され、日本語対訳書が 2020 年 3 月に出版された。

ISO/IEC 27701 は、PIMS を構築するためのものであるが、独立したマネジメントシステムではなく、ISMS によるマネジメントシステムの拡張として規定されている。このため ISO/IEC 27701 を基にして ISMS の審査及び認証を行う機関に対する要求事項が 2019 年 12 月に提案され、ISO/IEC 27006（Requirements for bodies providing audit and certification of information security management systems）の Part 2（Privacy information management systems） が TS として 2021 年 2 月に発行され、日本語対訳書が同年 3 月に出版された。

国内では、ISO/IEC 27701 を基にした ISMS 認定が 2020 年 12 月から開始されている。ISO/IEC 27006-2 については、更に内容を充実させるための IS 化の審議が継続されている。

日本提案の規格としては、経済産業省が 2014 年 10 月に公開した「消費者向けオンラインサービスにおける通知と同意・選択に関するガイドライン」に基づく国際規格である ISO/IEC 29184（オンラインにおけるプライバシーに関する通知と同意）が 2020 年 6 月に発行され、日本語対訳書が同年 11 月に出版されている。

また、同じく日本提案である ISO/IEC 27556（プライバシープリファレンスに基づいたユーザ主体の PII 処理）は、2019 年 5 月に新たな規格策定プロジェクトとして承認され、2021 年 4 月現在、CD 段階にある。

(c) バイオメトリクス

バイオメトリックデータの保護技術を扱う ISO/IEC 24745 は、2011 年に発行されたが、その後の新技術を反映するための改訂が進み、2021 年 4 月会合で FDIS 段階に進んだ。また、モバイル機器上でのバイオメトリクスを使った認証に対するセキュリティ要件を定めるプロジェクト ISO/IEC 27553 は、CD 段階にあったが、2021 年 4 月会合で適用範囲が問題となり、Part 1（Local modes）、Part 2（Remote modes）に分け、Part 1 は CD 段階の審議を継続、Part 2 は PWI から検討を開始することとなった。スマートフォンへのバイオメトリクスの適用が進みつつある中、ISO/IEC 27553 は関心を集めている。

COLUMN

2021年1月から「ISMS-PIMS認証」の審査始動!

2021年1月から、日本でもISO/IEC 27701:2019規格に基づいた「ISMS-PIMS（アイエスエムエスピムス）認証」の審査が開始しました。本認証では、PII（Personally Identifiable Information）の保護への対応が行えているかを確認する審査が行われます。PIIには、氏名等の「個人情報」だけでなく、免許証番号や住所、性別、年齢等と組み合わせることで「個人を特定できる情報」、例えば、位置情報、画像識別情報、遺伝子情報も含んでいます。個人情報保護法やGDPR等による規制はますます厳格になっており、企業・組織にとってPIIの適正な管理は重要課題です。

日本では、ISMS認証やプライバシーマークといった制度を活用している企業・組織がたくさんあります。ISMS-PIMS認証は、ISMS認証の基準となったISO/IEC 27001を拡張し、より具体的で実践的な個人情報やプライバシー保護のための情報マネジメントシステムであるISO/IEC 27701を基準としています。それ故、ISMS認証と親和性が高く、ISMS認証に付加する形でISMS-PIMS認証されます。プライバシーマークはJIS Q 15001に基づく国内制度ですが、ISMS-PIMS認証は国際標準を基にしているので、世界各国の個人情報、プライバシー保護の法律や規制との関係も整理しやすいです。ISO/IEC 27701の別添資料Annex DにはEU一般データ保護規則（GDPR）との対応表が提供されています。日本企業がGDPR等の海外の個人情報、プライバシー保護の法律や規制にも適合していく必要がでてきたことに応える認証制度として、ISMS-PIMS認証は注目され、大きな期待が寄せられています。

ISMS-PIMS認証の大きな特徴としては、「PII管理者」と「PII処理者」という2種類の振る舞いをする組織が定義しており、適用範囲がどちらに該当しているかで個別の要件が確認されることです。ISO/IEC 27701では、どんな情報をどんな目的、手段で収集・利用するのかを決めるPII管理者と実際のデータを保管・加工するPII処理者の各々が何に責任を持つのかが明確に規定されています。PII管理者とPII処理者は、同一組織内のこともあれば、委託元と委託先という関係のこともあります。パブリッククラウドを利用する場合も考慮されているので、PIIを扱う多くの組織でセキュリティ対策の検討に利用できます。

ISO/IEC 27701を委託先との個人情報に関する取り扱いの取り決め等で活用し、ISMS-PIMS認証を自社のセキュリティ対策強化・改善のきっかけにしてはいかがでしょうか。

2.6 安全な政府調達に向けて

IPA では情報セキュリティ対策の実現を目指し、国民に向けた情報提供や啓発活動、企業・組織に対するセキュリティ施策の促進とともに、政府機関や独立行政法人が安全に IT 製品やクラウドサービス等を調達するために活用できるいくつかの制度の運営を行っている。

本節では、政府機関等で使用される IT 製品のセキュリティ機能を評価する「IT セキュリティ評価及び認証制度」、及び政府機関等のシステムに組み込まれる暗号のアルゴリズムを確認する「暗号モジュール試験及び認証制度」の動向について報告する。また 2020 年度に開始した、政府が求めるセキュリティ要求を満たしているクラウドサービスを評価・登録する「政府情報システムのためのセキュリティ評価制度（ISMAP）」の概要を紹介する。

2.6.1 ITセキュリティ評価及び認証制度

サイバーセキュリティ戦略本部は、府省庁及び独立行政法人が遵守すべき情報セキュリティ対策を定めた「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）[※443]」（以下、政府統一基準）を発行した。この中では、国民の情報等を扱う公的なサービスを提供するシステムを構築する場合、そのシステムを構成する市販の IT 製品についてもセキュリティ要件を策定することを調達者に求めている。

IT 製品の調達において、セキュリティ要件を確認するための仕組みとして、セキュリティ評価の制度が先進国を中心に発展し、セキュリティ評価基準が国際規格として策定された。日本でも、このセキュリティ評価基準を用いて IT 製品を評価する「IT セキュリティ評価及び認証制度（JISEC：Japan Information Technology Security Evaluation and Certification Scheme）」を IPA が運営し、政府機関等の IT 製品調達に活用されている。

(1) 政府の IT 製品調達セキュリティ要件

政府統一基準では、調達及び運用において特にセキュリティ要件を策定すべき IT 製品分野として、経済産業省が発行している「IT 製品の調達におけるセキュリティ要件リスト[※444]」（以下、調達要件リスト）を参照している。調達要件リストには、利用者情報を扱うシステムの基盤となり、攻撃の対象となり得る以下の 11 の製品分野が指定されている。今後も対象製品分野は、拡大される予定である。

- デジタル複合機
- ファイアウォール
- 不正検知・防止システム
- サーバ OS
- データベース管理システム
- スマートカード
- 暗号化 USB メモリ
- ルータ／レイヤ 3 スイッチ
- ドライブ全体暗号化システム
- モバイル端末管理システム
- 仮想プライベートネットワークゲートウェイ

府省庁や独立行政法人の情報システムセキュリティ責任者は、これらの製品分野の IT 製品を調達する場合、想定されるセキュリティ上の脅威にそれらの製品が対抗できていることを確認することが義務付けられている。各組織が調達する IT 製品が、想定するセキュリティ要件を満たしていることを個別に確認する方法に加え、調達要件リストでは、国際標準に基づく第三者認証製品の活用も認めている。

JISEC は、IT 製品のセキュリティ評価の国際標準である ISO/IEC 15408 に基づく第三者認証制度を運営している。組織の調達責任者は、想定する脅威に対抗していることが評価され、JISEC で認証された IT 製品を購入することで、政府統一基準の要求を満たすことができる。

特に、システム構築とは独立して調達されることの多い「デジタル複合機」、国策としてセキュリティ対策が重要となる旅券やマイナンバー等の「スマートカード」の調達で JISEC の認証制度は活用されている。

(2) 認証制度の国際連携

JISEC でも採用しているセキュリティ評価基準である ISO/IEC 15408 は、欧米 6 ヵ国によるコモンクライテリア（共通基準）プロジェクトとして開発された。これらの国々では、同じセキュリティ評価基準であるコモンクライテリアを用いて、その国を代表する公的機関が運営する制度で評価された結果については相互に認め合うことで、調達国ごとに重複的な評価を行うコストを低減することを目的とした相互承認が締結された。この相互承認の

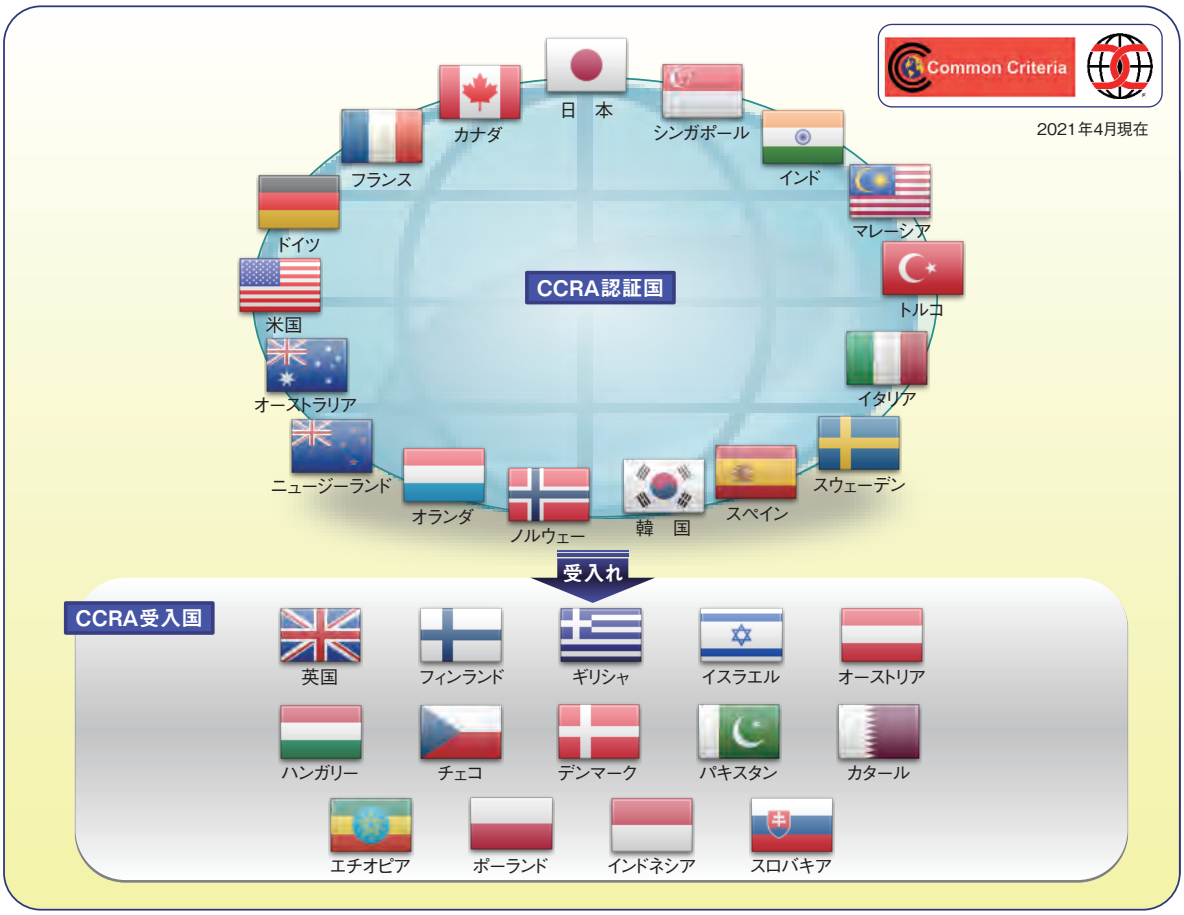
枠組みは、CCRA（Common Criteria Recognition Arrangement）と呼ばれ、その後多くの国が加盟し、JISEC を運営する日本も 2003 年に加盟している。これにより、日本のベンダは日本語の開発資料をそのまま利用し、JISEC で認証を取得した製品を CCRA 加盟国の政府調達の対象とすることができるようになった。

CCRA では、自国で認証制度を運営している「認証国」と、認証制度をまだ有しないが政府調達要件として認証結果を受け入れる「受入国」があり、近年は東ヨーロッパやアフリカの国が受入国として加盟している。2021 年 4 月現在、CCRA 加盟国は認証国 17 ヵ国、受入国 14 ヵ国の計 31 ヵ国に上る（図 2-6-1）。

(3) セキュリティ要件の共通化

コモンクライテリアでは、IT 製品が具備すべきセキュリティ要件を、規定された形式に従って記述する。例えば、アクセス制御機能においては、対象となるオブジェクトやサブジェクトのリスト、セキュリティ属性、それらを用いたアクセス方針をコモンクライテリアで規定された形式で記述する。これにより、調達者が必要としている IT 製品のセキュリティ要件仕様を、あいまいさを排除して製品開発者に伝えることを可能とする。このコモンクライテリア形式で表された調達要件仕様書を「プロテクションプロファイル」と呼び、CCRA 加盟国での IT 製品の政府調達に利用されている。加盟国の調達部門は、調達する IT 製品のセキュリティ要件をプロテクションプロファイルとして作成し、調達要件として公開している。これらのプロテクションプロファイルのうち汎用的なものは、CCRA のポータルサイト※445 にも掲載され、他の機関も同様の分野の製品を調達する際に用いることができる。日本においても、調達要件リストでは製品分野ごとにこれらのプロテクションプロファイルを指定している。また、独自の製品を調達する機関は、プロテクションプロファイルを自ら作成し※446、調達を実施している。

CCRA では、これまで調達者ごとに作成していたプロテクションプロファイルを、製品分野ごとに共通化する作業を行っている。同じ製品分野の IT 製品調達で、似たような調達仕様が調達者ごとに提示されることは、開発者にとっては負荷となる。そこで CCRA 加盟国の認証機関が中心となり、いくつかの製品分野で共通的に

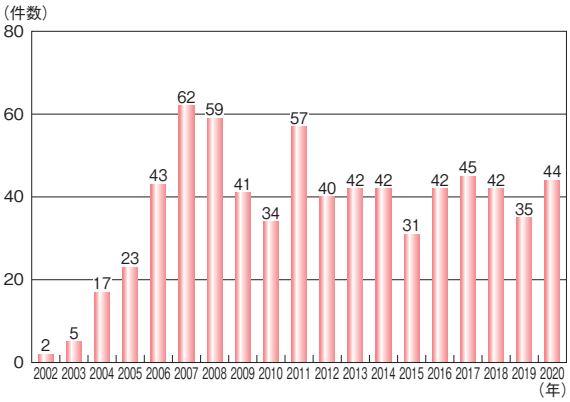


■図 2-6-1　CCRA 加盟国

用いるプロテクションプロファイルの策定を行っている。このプロテクションプロファイルは、cPP（collaborative Protection Profile）と呼ばれ、CCRA 加盟国は、該当する製品分野の調達には、このcPPを用いてセキュリティ要件を指定することとしている。既にファイアウォール、ディスク暗号ドライブ、ネットワークデバイスの製品分野について cPP が策定され、CCRA ポータルサイトで公開されている。現在も、バイオメトリクス認証やデータベースについて cPP の策定が進行中である。日本も、国内に多くの製品ベンダを有するデジタル複合機について、韓国の認証機関とともに発起人となり、各国のベンダや評価機関をメンバーとする技術コミュニティを発足し、2021 年内の公開を目指し cPP の策定を行っている。

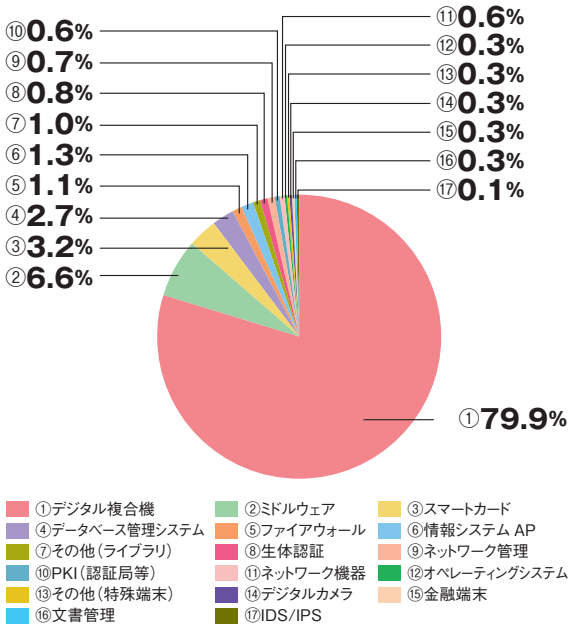
(4) 認証の状況

2020 年度までの JISEC における認証発行件数の推移を図 2-6-2 に示す。リーマンショックの影響による 2009 年の申請数の減少とそのリバウンド（2011 年度）以降、毎年 40 件前後の認証発行を行っている。



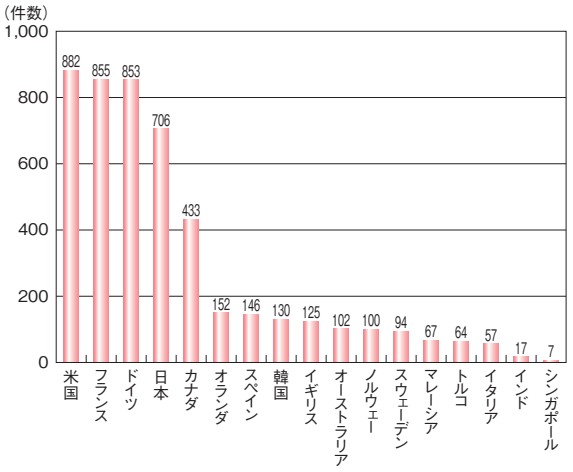
■図 2-6-2　JISEC の認証発行件数の推移

JISEC が認証発行した製品の分野の内訳を、図 2-6-3 に示す。認証製品分野としては、デジタル複合機が圧倒的に多い。これは前述のように、日本のベンダが国際的にもシェアを有し、CCRA 加盟国においても政府調達の対象となっているからである。また、その他の製品分野の認証が JISEC で少ないのは、セキュリティ製品全般において日本ベンダの国際的な競争力が弱く、デジタル複合機以外の認証申請取得がなされないこと、ファイアウォールやネットワーク管理製品のようにシステム構築の中で組み込まれてテストされ納入されることが多いため、製品単品での調達要件の対象とならないこと等が理由である。JISEC が毎年認証発行している 40 件前後は、ほとんどがデジタル複合機の新機種リリースによるものである。



■図 2-6-3　JISEC 認証発行の製品分野内訳

CCRA 加盟各国の認証機関が公開している認証発行件数の 2020 年度における累計を図 2-6-4 に示す。日本の認証発行件数は、米国、フランス、ドイツに次いで 4 番目に多い。これらの国は、政府調達に認証製品を活用しているのに加えて、国内に IT 製品の製造業者を多く持つ国々である。英国は、セキュリティ評価の歴史は長いにもかかわらず、国内の製造業者の減少により、2019 年に制度維持コストの削減を理由に認証国から受入国に移行している。韓国では、国際的に大きな市場を持つ製造業者が、製品仕向地によりモバイル製品は米国で、スマートカード関連製品はヨーロッパで認証を取得しているため、国内制度の認証発行件数は低い。



■図 2-6-4　CCRA 各国の認証件数

(5) 2020 年度のトピック

JISEC では IT 製品の認証実施のほか、国内やアジア地域における認証制度の活用や普及に向けた取り組みを行っている。

(a) IoT 製品分野セキュリティへの対応

政府統一基準では、調達要件リストとは別に、近年政府において活用されている IoT 製品についてもセキュリティ対策を求めている。更に 2020 年 4 月に施行された「電気通信事業法に基づく端末機器の基準認証」では、IoT 機器の技術基準にセキュリティ対策が追加された。このような背景を踏まえ JISEC では、IoT 製品分野に係る国内ベンダが多く存在することから、安全な政府調達の推進と国際的な市場競争力の確保を目的に、IoT 製品分野への認証制度活用に向けた取り組みを実施している。これまでにネットワークカメラシステム及び入退管理システムについて、調達者自身が調達時に必要なセキュリティ要件を確認できるようにチェックリストを公開している。2020 年度には、このうちネットワークカメラシステムのチェックリストの基本的なセキュリティ要件について、コモンクライテリアによる評価の検証を実施している。具体的には、脆弱性診断サービスを提供する民間機関 3 社により、市販のネットワークカメラシステム 3 製品を対象に、コモンクライテリアの評価手法に従った機能テスト及び脆弱性評定を実施した。この結果、短期間にいくつかの脆弱性が発見され、IoT 製品に対するコモンクライテリア適用の有効性が確認された。2021 年は IoT 機器の基本的セキュリティ要件についてプロテクションプロファイルを策定し、今後 IoT 製品分野の政府調達への活用を推進していく。

(b) ASEAN 諸国への協力

欧米諸国を中心として発足した CCRA にも、マレーシア、シンガポール、インドネシアのような東南アジアの国々が参加するようになった。JISEC は制度運営の経験を基に、セキュリティ評価制度の概要について、例年、独立行政法人国際協力機構（JICA：Japan International Cooperation Agency）が主催する ASEAN 各国の政府機関関係者に向けたセミナーを通じて情報共有を行ってきた。このセミナー参加国の一つであるベトナムから、コモンクライテリアを評価基準とするセキュリティ認証制度の確立に向けた検討のため、JICA を通じて協力依頼があった。JISEC では 2021 年 2 月及び 3 月に IT セキュリティ評価に関するオンラインセミナーを開催した。ベトナム政府の関係部門に対し、制度設立の経緯や現状及び CCRA 加盟に向けた手続きについて説明と質疑応答を行い、今後もベトナムのセキュリティ認証制度の設立と CCRA 加盟に向けた協力を継続的に行うことを約束した。

2.6.2 暗号モジュール試験及び認証制度

暗号モジュール試験及び認証制度（JCMVP：Japan Cryptographic Module Validation Program）とは、利用者が暗号モジュールの信頼性を客観的に把握できるように設けられた第三者適合性評価認証制度である。本制度に基づく認証を取得することにより、暗号アルゴリズムが適切に実装され、暗号鍵等の重要情報を適切に保護している暗号モジュールであることをアピールできる。本制度は、米国の NIST とカナダの CCCS（Canadian Centre for Cyber Security）により運営されている CMVP（Cryptographic Module Validation Program）と同等の制度であり、IPA が認証機関として運営している。本項では、JCMVP の最新動向、及び関連する CMVP の動向について述べる。

(1) 暗号モジュールのセキュリティ要求事項の新規格への移行及び CMVP の動向

JCMVP では、2018 年 6 月から、暗号モジュールが満たすべきセキュリティ要求事項（アクセス制御、物理的セキュリティ等）を定めた規格として、ISO/IEC 19790: 2012 を採用している※447。2020 年 10 月、JCMVP は ISO/IEC 19790: 2012 に基づいて、既存の承認された暗号モジュール試験機関 1 社の技能試験を実施した。

関連する CMVP の動向としては、FIPS 140-3（2019 年 9 月改訂）の暗号モジュールセキュリティ要件が ISO/IEC 19790 及び ISO/IEC 24759 の要件を参照するように変更された。これに伴い、FIPS 140-2 から FIPS 140-3 に移行するための計画※448 が公開され、2020 年 3 月に FIPS 140-3 の試験要件が SP 800-140x シリーズとして規定※449 された。その後の FIPS 140-3 への移行スケジュールは、以下のとおりである（⑤、⑥は予定）。

①2020 年 5 月 20 日：CMVP FIPS 140-2 Management Manual 改訂※450
②2020 年 7 月 1 日：Tester competency exam 改訂※451
③2020 年 9 月 21 日：FIPS 140-3 IG 公開※452、CMVP FIPS 140-3 Management Manual 改訂※453
④2020 年 9 月 22 日：FIPS 140-3 での申請受付開始

⑤2021 年 9 月 21 日：FIPS 140-2 新規申請停止
⑥2026 年 9 月 21 日：FIPS 140-2 認証は Historical List へ移動

JCMVP は、ISO/IEC 19790:2012 の採用にあたって得た知見を2019年12月にCMVPに対してフィードバックした。その概要及び FIPS 140-3 との差異について 2020 年 9 月 21 ～ 24 日に開催された暗号モジュールに関する国際会議 ICMC20※454 において報告した。

(2) 政府機関等における JCMVP・CMVP の活用

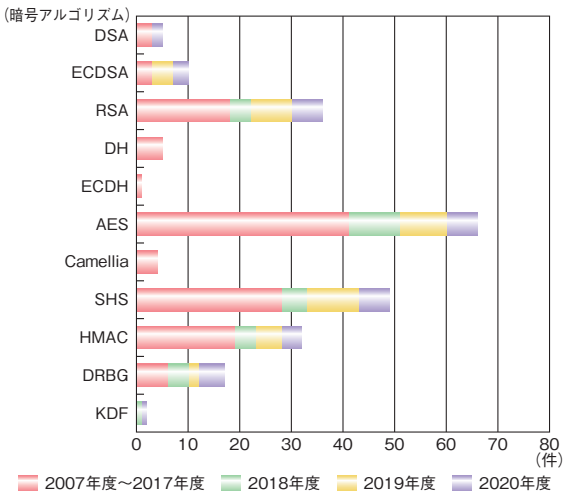
CMVP では、CMVP 認証を取得していない暗号モジュールについて、「認証されていない暗号は情報及びデータを保護しないとみなす。省庁が情報及びデータを暗号的に保護すべきであると指定した場合には、FIPS 140-2 (2026 年 9 月 22 日まで) または FIPS 140-3 (2020 年 9 月 22 日より)に準拠した保護が該当する。すなわち、暗号が必要であれば認証されたものでなければならず、認証が取り消されれば、その暗号モジュールを使用してはならない。※455」と規定している。

日本においては、各府省情報化統括責任者（CIO）連絡会議が決定し、2019 年 2 月に公開された「行政手続におけるオンラインによる本人確認の手法に関するガイドライン※456」において、JCMVP 認証されたハードウェアトークンに対して当人認証保証の最高レベル 3 を与えるとされた。

(3) IT セキュリティ評価及び認証制度（JISEC）との連携

IPA が運営する評価認証制度には、JISEC と JCMVP の二つがある。JISEC が 2016 年に発行、2020 年に改定したガイドライン※457 によって、JCMVP の活用方針が示されている（JISEC の活動については「2.6.1 IT セキュリティ評価及び認証制度」参照）。

2020 年度は、JISEC のもとで、この活用方針に関連する「Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015※458」に基づくデジタル複合機の認証が 28 件完了している※459。このプロテクションプロファイルでは、信頼できるツールを用いた暗号アルゴリズム実装のテストを求めている。このテストに、JCMVP の暗号アルゴリズム実装試験ツール（JCATT：Japan Cryptographic Algorithm implementation Testing Tool）が活用され、認証に貢献している。具体的には、図 2-6-5 に示すように、JCATT を使って確認された暗号アルゴリズム実装の実績が、2018 年度、2019 年度及び 2020 年度において堅調に増加している。また、2019 年度より楕円曲線暗号の一つである ECDSA（Elliptic Curve Digital Signature Algorithm）の実績が増えており、楕円曲線暗号のニーズが反映されていると考えられる。



■図 2-6-5　JCATT により確認された暗号アルゴリズム実装の実績
(出典)IPA の公開情報※460 を基に作成

(4) 承認されたセキュリティ機能等の見直し

2020 年度に JCMVP の下部組織である技術審議委員会において、暗号モジュールのセキュリティ要求事項に組み合わせることのできる暗号の一覧である「承認されたセキュリティ機能※461」の見直しに関して、以下の審議が実施された。

①RSA 1024 の署名検証の削除
②SHA-1 の署名検証の削除
③署名検証のパラメータ改正
④TLS version 1.0 及び 1.1 の鍵導出関数の削除
⑤TLS version 1.3 の鍵導出関数の NIST SP800-56C※462 への適合性

①②③は 2020 年 12 月施行の「電子署名及び認証業務に関する法律施行規則※463」の改正に対応したものである。同規則の改正内容は、署名検証においても、先行してセキュリティ上の条件（鍵長の制約や使用可能なハッシュ関数のアルゴリズム）が強化されていた署名生成と同じ条件に揃えるものであった。技術審議委員会では、同様の主旨の改正を「承認されたセキュリティ機能」に対して行うことの可否を審議した。その結果、「削除されるセキュリティ機能を実装した認証済みの製品の扱いや、

同セキュリティ機能を使い続けることが必須（例えば、長期署名の検証）の製品の認証について、認証機関として方針を定める」ことを条件として承認を得た。2021年5月現在、認証機関としての方針を策定中である。

④では、TLS（Transport Layer Security）version 1.0及び1.1の使用を非推奨とする国内外の動向や、実際のサポート状況を踏まえ、これらのTLSのバージョンで定められた鍵導出関数を「承認されたセキュリティ機能」から削除することについて審議し、技術審議委員会の承認を得た。

⑤では、TLSの新たなバージョンであるTLS version 1.3の鍵導出関数がNIST SP800-56Cに適合するかどうかを審議し、技術審議委員会は適合すると判断した。また同文書に適合する鍵導出関数は「承認されたセキュリティ機能」に含まれるため、新たにTLS version 1.3の鍵導出関数の実装試験仕様を整備していくことについて、技術審議委員会の承認を得た。

更に、2020年度から以下の事項について検討を進めることについても技術審議委員会の承認を得た。

- ECDSAの仕様変更への対応
- TLS version 1.3の鍵導出関数の実装試験仕様

前者は、「承認されたセキュリティ機能」におけるECDSAの仕様の参照先の一つであるANS X9.62-2005が2020年9月に廃止され、新たにANSI X9.142-2020がリリースされたことを受け、両規格の差分や既存の製品への影響を調査し、JCMVPとしての対応を検討するものである。後者は、TLS version 1.3の鍵導出関数の実装試験仕様を整備する方針を受け、対応する試験方法や内容を検討するものである。

(5) JCMVP規程類の改正

JCMVPの下部組織である運営審議委員会では、認証業務運営の方針に関する事項及びマネジメントシステムの維持に関する事項等の審議を行い、統括責任者に対する助言を行う役割を担っている。2020年度に運営審議委員会を開催し、JCMVP規程類の大規模な改正について審議を実施した。

今回の改正目的は、サプライチェーンリスクが重大なセキュリティ課題として認識されるようになってきている現状に鑑み、JCMVPの規程類では以下の事項についての取り扱い方法が明確化されていなかったため、規程として取り扱い方法を明確化することであった。

- サプライチェーンリスク等への対応方針
  - JCMVP認証制度の目的の明確化
  - 運営審議委員会の役割の追加
  - 暗号モジュール認証及び暗号アルゴリズム確認の申請の制限
  - 暗号モジュール認証及び暗号アルゴリズム確認の認証作業の中止、及び認証許諾拒否の新設
  - 日本または輸出貿易管理令別表第3の地域に本社を有しない企業等への暗号モジュール認証及び暗号アルゴリズム確認の譲渡に対する対策
- 認証済暗号モジュール及び確認済暗号アルゴリズムに対する認証効力の一時停止及び取り消しに関する条件
- 規程類が改正されたときの認証済及び認証中の暗号モジュール及び暗号アルゴリズムへの改正規程類の適用方針

改正の大きなポイントは、JCMVP認証制度の目的に「日本国内におけるセキュアな暗号モジュールの調達、購入及び利用に資する」と追加することで、サプライチェーンリスクへの対応を考慮し、必要に応じて適切な措置を講じることができることを明確にした点と、中立性・客観性の観点から、必要に応じて運営審議委員会から、申請の受付可否、認証の許諾、拒否または取り消し等に関する事項等の助言を得ることができることを明文化したことである。

なお、規程類の改正は2020年10月に行われ、同11月から適用開始となった※464。

2.6.3 政府情報システムのためのセキュリティ評価制度（ISMAP）

2020年6月3日、内閣官房、総務省、経済産業省は政府情報システムのためのセキュリティ評価制度（ISMAP）の開始をアナウンスした※465。本項では、ISMAPの概要について紹介する。

(1) ISMAPの概要

政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program:通称、ISMAP（イスマップ））は、政府が求めるセキュリティ要求を満たしているクラウドサービスをあらかじめ評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスの円滑な導入に資することを目的とした制度である。

従来、政府調達にあたっては、個々のクラウドサービスが実施していると表明する情報セキュリティ対策の実施状況を、調達者が直接確認することが必要であったが、本制度により、確認を省略でき負担を軽減できる。

(2) ISMAP 制定の経緯

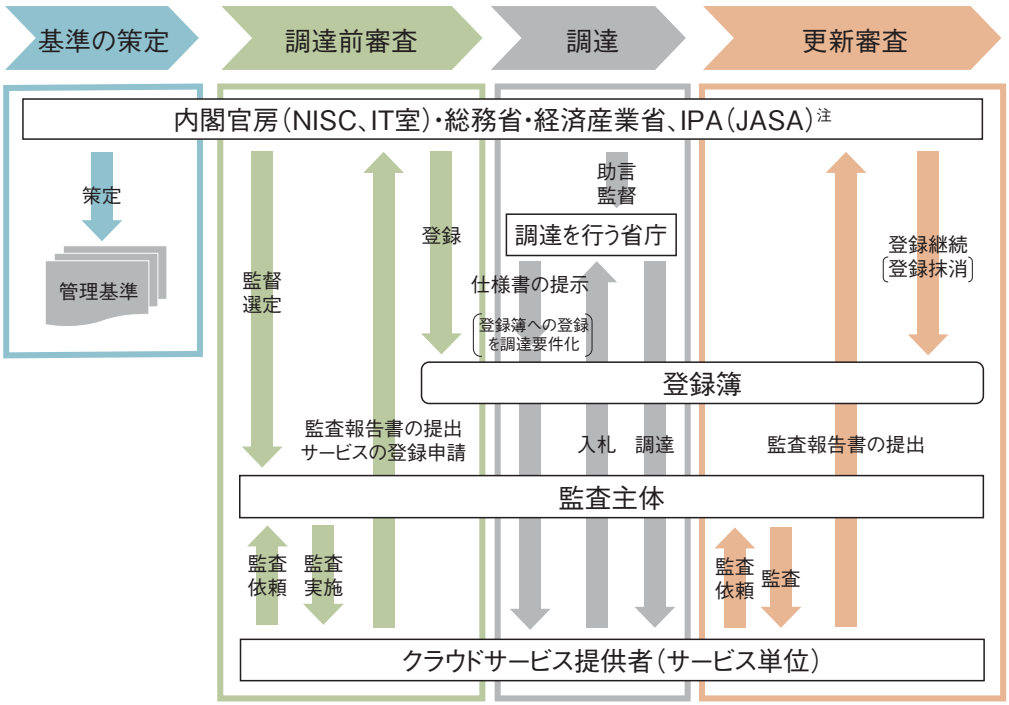
各府省情報化統括責任者（CIO）連絡会議において決定され、2018 年 6 月に公開された「政府情報システムにおけるクラウドサービスの利用に係る基本方針※466」（2021 年 3 月 30 日付けで ISMAP に関する記述が追記されている）では、「クラウド・バイ・デフォルト原則」が掲げられた。これを踏まえ、経済産業省と総務省は、2018 年 8 月から「クラウドサービスの安全性評価に関する検討会※467」を発足させ、適切なセキュリティ要件を満たすクラウドサービスを導入するために必要な評価方法等を検討し、2020 年 1 月に「クラウドサービスの安全性評価に関する検討会とりまとめ※468」が公開された。また、同月のサイバーセキュリティ戦略本部会合において「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて※469」が決定された。

また上記検討会において、2019 年 6 月から、政府情報システム調達に応募するクラウド事業者が遵守すべきセキュリティ管理基準（以下、ISMAP 管理基準）の検討が行われた。ISMAP 管理基準は、国際規格をベースに「政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版）」「NIST SP800-53 rev.4」を参照して作成された。国際規格としては、情報セキュリティに関しては JIS Q 27001（ISO/IEC 27001）、JIS Q 27002（ISO/IEC 27002）とクラウドサービスの情報セキュリティに関する JIS Q 27017（ISO/IEC 27017）が参考にされた。また、これらの国際規格に準拠して編成された「クラウド情報セキュリティ管理基準（平成 28 年度版）」が参考にされ、そこに含まれるガバナンス基準については JIS Q 27014（ISO/IEC 27014）が参考にされた。

(3) ISMAP の運用

本制度においては、まず、政府機関等が調達するクラウドサービスに対して要求するべき基本的な情報セキュリティ管理・運用の基準が後述する NISC 他の所管政府機関にて定められる。また、本制度で定められた情報セキュリティ監査の枠組みを活用した評価プロセスに基づき、上記の基準を満たすセキュリティ対策を実施していることが確認されたクラウドサービスが ISMAP クラウドサービスリスト（以下、サービスリスト）に登録される。政府機関がクラウドサービスを調達する場合、上記リストに登録されたサービスを選定候補とする。

また、本制度における監査を実施できる監査機関は、あらかじめ本制度で定める要求事項を満たすことが確認



（注）制度運用に係る実務及び評価に係る技術的な支援をIPAが行い、うち、監査機関の評価及び管理に関する業務についてJASAに再委託する。

■図 2-6-6　クラウドサービスの安全性評価の制度のフロー
（出典）内閣官房・総務省・経済産業省「政府情報システムのためのセキュリティ評価制度（ISMAP）について※470」

され、本制度が公表するISMAP監査機関リスト（以下、監査機関リスト）に登録される。

本制度のフローを図2-6-6（前ページ）に示す。図において、クラウドサービス提供者は監査機関リストに登録された機関による監査を受け、所管政府機関にサービス登録申請を行う。所管政府機関は審査を行い、承認されたサービスがサービスリスト（図では登録簿と表記）に掲載される。府省庁の調達者はサービスリストを使って調達先候補を選ぶ。所管政府機関は監査者認定と監査結果に基づくサービスリスト管理を行う。

（4）セキュアなクラウド利用に向けて

本制度は2020年6月、運用が開始された。

ISMAPの所管は2021年5月現在、NISC、内閣官房情報通信技術（IT）総合戦略室、総務省、経済産業省であり、最高意思決定機関としてISMAP運営委員会を設置し、事務局はNISCに置き、運用実務はIPAが担当している。

制度の概要、基準規程類、監査機関リスト、及びサービスリストは、ISMAPポータルサイト※471で公開されている。2021年4月時点で登録されている監査機関は4機関、また、クラウドサービスは10サービスである。

なお、IPAは総務省からの受託事業として、クラウドサービス事業者がサービスリストへの登録を行うにあたり、セキュリティ対策の進め方及び管理基準の理解の一助となることを目的として、管理基準マニュアルの検討を行っている。

また、ISMAPで公開される情報は、重要インフラ分野等を始めとする民間企業においても参照されることで、クラウドサービスの適切な活用の推進が期待される。これに関連して、2019年5月23日に改定されたNISCの「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）※472」においては、「事業環境の変化を捉え、インターネットを介したサービス（クラウドサービス等）を活用するなど新しい技術を利用する際には、国内外の法令や評価制度等の存在について留意する。」とされており、国内の評価制度としてはISMAPが該当すると考えられる。

「クラウドサービスの安全性評価に関する検討会とりまとめ」にも記載されたように、情報システムのセキュリティ確保の責任は、一義的に当該システムの調達者／利用者が負うものである。本制度に登録されたクラウドサービスを利用したとしても、それだけでは情報システム全体のセキュリティが十分に確保されることにはならない。情報システムの調達者／利用者は、利用するクラウドサービスについて適切な設定を行うことに加えて、情報システム全体のセキュリティリスクを分析し、適切な対策を行うことが求められる。

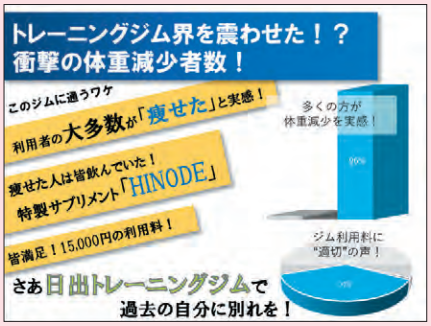
COLUMN

噂を信じてしまう法則って?
～日出学園中学・高等学校の取り組み～

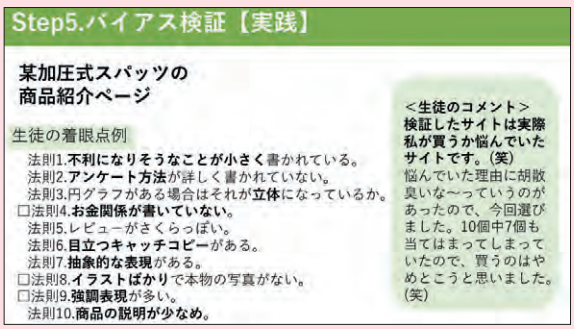
インターネットの普及により、私達は知りたいと思った情報をすぐその場で調べることができるようになりました。しかし、その情報は、誰かが悪意を持って流した偽の噂(デマ)である危険性をはらみます。スマートフォンを通じて、SNS や Web サイトに触れる機会の多い中高生にとって、ネット上に溢れる情報に対し、高い情報モラルをもって接することは特に重要です。ここでは、第 16 回 IPA「ひろげよう情報モラル・セキュリティコンクール」2020 で文部科学大臣賞を受賞した、日出学園中学校・高等学校[i]の活動事例[ii]をご紹介します。

同校では、①「他人に相談せずに、自分だけで判断してしまうこと」、②「深く考えずに何となく行動してしまうこと」の二つを防ぐことを課題とした情報モラル教育に取り組みました。

まず、①を防ぐため、オンライン授業ツールの使い方や Web サイトの信頼性について、生徒同士で意見を交換することで、「対話的に」学び、他者に相談する意義を学びました。次に、②を防ぐため、普段何となく判断している基準を明文化することで、ネット上に溢れる情報を「深く」読み解くきっかけを作りました。噂を信じてしまう法則を身の回りの噂から考えてみたところ、生徒からは、「自分自身に関わること」「完全に否定できないこと」「具体的な人物や場所が出てくること」等が挙がりました。その後の実習では、これらの法則に基づいた「新しい噂」を作りました。また、隠れたバイアスを吟味する能力を養うべく、あえてバイアスを含んだ「怪しい広告」(図 1)を作成し、それを基に、広告を眺める際のチェックリスト(図 2)をまとめました。更にそのチェックリストを、実際の広告に照らし合わせ考察することで、日常においても都度触れる情報を「深く」考える習慣を身に付けています。



■図 1　生徒が制作した広告
(出典)日出学園中学校・高等学校より提供



■図 2　生徒による広告の検証例と感想
(出典)日出学園中学校・高等学校より提供

新型コロナウイルスの影響により、急速なオンライン化が進む中、情報モラル･セキュリティ教育の重要性はますます高まっています。本コンクールで受賞した学校の取り組みをぜひご覧いただき[ii]、今後の教育に活かしていただければ幸いです。学校関係者の皆様、ご家族に小・中・高校生がいらっしゃる皆様には、本コンクールへのご応募もお待ちしております。

i　https://high.hinode.ed.jp/〔2021/6/16 確認〕
ii　IPA：活動事例　https://www.ipa.go.jp/security/event/hyogo/2020/awd_katsudo.html〔2021/6/16 確認〕

2.7 情報セキュリティの普及啓発活動

2020 年は、これまで「当たり前」とされてきたことが新型コロナウイルスの感染拡大により、大きく覆された年となった。毎日の出勤はテレワークに切り替わり、対面での会議や授業はオンラインによる実施が推進された。

このように生活の中の IT 利用機会が大きく増え、それに伴うセキュリティ対策はこれまで以上に重要になっている。また情報セキュリティを含む IT 利用スキル（IT リテラシー）の向上も重要性を増している。

本節では、様々な組織・団体が各々の視点で実施した普及啓発活動について述べる。

2.7.1 恒常的な対策等に関する普及啓発活動

インターネットの利便性が広く知られる一方で、その危険性や利用上の注意に対する理解の深化は遅く、利用者への啓発が継続的に行われている。

(1) 多様なツールを活用した普及啓発活動

インターネットが生活の多くの場面で使用される中、未だインターネットを悪用した詐欺被害や SNS を介した未成年者誘拐、誹謗中傷等、事件や事故は後を絶たず、利用者の情報セキュリティ対策の実施状況も、情報セキュリティ意識の定着もまだ十分とはいえない。

ここでは、普段情報セキュリティを意識していない人でも意識を向けやすいよう工夫が施された資料やツールを紹介する。

NISC によるサイバーセキュリティ月間（2021 年 2 月 1 日～ 3 月 18 日）では、「ラブライブ!サンシャイン !!」とのタイアップによる短編アニメーションを公開した※ 473。「ラブライブ!」シリーズは、過去には紅白歌合戦に出場する等、若年層だけでなく広く国民の認知度を得ていることから、幅広い層への意識付けが期待された。

動画による啓発は、文字を読むよりも視聴者へのメッセージが伝わりやすく、興味を引きやすいため、他にも多数公開されている。山形県警察本部は、「『サポート詐欺』に騙されないで!※ 140」と題した 3 本の動画を公開した。これは、実際の偽の警告画面を基に、警察官が犯人とやり取りをした様子を記録したものである。文章だけでは伝わりにくい犯人の発語の特徴や画面の内容について理解することができる。埼玉県警察本部は、「ポッポくん、ポポ美ちゃんのサイバーセキュリティ教室」のシリーズとして「安全なパスワードの管理※ 474」や「システム・アプリのアップデート※ 475」の動画を公開し、手口や対策方法についてイラストを用いて解説している。

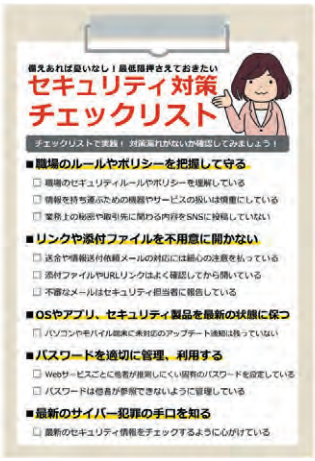
動画以外にも、様々なツールが公開された。警視庁は、サイバーセキュリティ学習用ボードゲームとして「サイバー迷宮脱出ゲーム」を公開した（図 2-7-1）。「オンラインゲームの課金」や「SNS への写真投稿」等、日常的に行っている行為が、どのような問題につながっていくのかをコマを進めることで学べるものとなっている。

■図 2-7-1　サイバー迷宮脱出ゲーム
（出典）警視庁「サイバーセキュリティ学習用ボードゲーム※ 476」

鳥取県警察本部は「インターネット安全利用啓発まんが※ 477」と題し、偽サイトや偽警告サイト・偽サポート請求、スマートフォンのセキュリティ対策等をテーマにした漫画を作成した。県民にとって読みやすい漫画というツールによって注意点が分かりやすく描かれている。

また、JNSA が「みんなの『サイバーセキュリティコミック』」プロジェクトを開始し、クラウドのセキュリティや情報漏えい対策等をテーマに、全 8 話の漫画による解説を公開した※ 478。

更に、社会人が身に付けるべき基本的な対策をまとめた「働く大人なら最低限知っておきたいネットセキュリティの基本 2021※ 479」がトレンドマイクロ株式会社から無償で提供されている（次ページ図 2-7-2）。新型コロナウイルスの影響で、新入社員等の集合研修が困難な中でも、Web サイトから資料をダウンロードし、各自で学習することができる。巻末には情報セキュリティ対策のチェックリストが掲載されており、これを活用した対策状況の確認が推奨される。



■図 2-7-2　セキュリティ対策チェックリスト
（出典）トレンドマイクロ株式会社「働く大人なら最低限知っておきたいネットセキュリティの基本 2021」

(2) ネット上の誹謗中傷への対策

2020 年 5 月、当時人気だったリアリティ番組の出演者の一人が自ら命を絶った。番組内での言動を端緒として中傷投稿が SNS 上にあふれ、それが一因となったと報道された※480。

このような状況のもと、総務省は 2020 年 8 月、「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（以下、プロバイダ責任制限法）の第 4 条第 1 項の発信者情報を定める省令に、発信者の電話番号を開示の対象として追加した※481。

誹謗中傷の投稿は匿名で行われることが多く、投稿の削除請求のためには、まず、投稿者を特定する必要がある※482。プロバイダ責任制限法では「情報の流通によって自己の権利を侵害された」場合、SNS 事業者等に投稿者の IP アドレスや投稿時間の開示を請求することができるとしている。次に、その情報を基に、プロバイダに対して氏名や住所の開示請求を行うことで、投稿者の特定ができる。しかし、SNS 事業者等が、IP アドレスを保存していないケースや、プロバイダが保有する接続記録が一定期間を経過すると消去されてしまうケース等、投稿者の特定に結びつかないことがあった。

今回の法改正により、投稿者の電話番号が開示されれば、電話会社に発信者の氏名や住所を照会することで投稿者の特定につながり、これが抑止効果となることが期待される。

2020 年 12 月、群馬県では全国に先駆けて「インターネット上の誹謗中傷等の被害者支援等に関する条例」を制定した。これは、誹謗中傷やプライバシー侵害により命に関わる事件が発生していることを背景に、県民が被害者にも加害者にもなることがないよう、正しくインターネットを活用する知識と能力を習得することを目的としたものである。本条例に関する知事のメッセージは YouTube で公開されている※483。

2020 年 4 月に ByteDance 株式会社、Facebook Japan 株式会社、LINE 株式会社、Twitter Japan 株式会社を中心とした SNS 事業者等によって設立された一般社団法人ソーシャルメディア利用環境整備機構は、SNS 等に起因する児童被害防止を強化し、ソーシャルメディアの健全な発展と、信頼される環境構築を目指すとしている（図 2-7-3）。同年 7 月には、法務省人権擁護局、総務省とともに「#NoHeartNoSNS※484」というスローガンを発表し、「誰かを傷つけてしまいそうなら」「あなたが傷ついたら」どうすればよいのか等について紹介する特設ページを公開した。特設ページでは、人権相談の窓口や、誹謗中傷等、ネット上で公開された情報を削除するにはどうすれば良いのか、相談員がアドバイスを行っていることも案内し、「あなたは一人ではありません。みんながあなたの力になります。」と締めくくっている。

■図 2-7-3　参加事業者が運営するサービス（2021 年 2 月現在）
（出典）一般社団法人ソーシャルメディア利用環境整備機構のホームページ※485 から抜粋

また、SNS 事業者等はルール改正等による課題の解決にも努めている。

Twitter Japan 株式会社は 2020 年 3 月、年齢、障がいや病気に基づいて人間性を否定する言葉を削除の対象に加えた※486。また、同年 8 月には投稿者が自分の投稿にリプライが可能なアカウントを選択できる機能※487を追加したこと等から、攻撃的なリプライの減少が期待されている。

TikTok 運営会社の日本法人である ByteDance 株式会社は、青少年を保護する対策の一環として 2021 年 1 月、16 歳未満の利用者については、初期設定を「非

公開」にした※488ほか、同年2月からは起動時に生年月日の入力を求める画面を表示し、利用者の年齢確認を開始している※489。

また、多くの投稿系サービスを提供するヤフー株式会社は、2020年6月「プラットフォームサービスの運営の在り方検討会」を設置し、AI等を利用した誹謗中傷等の投稿抑止と削減を進めるとともに、各サービスのポリシーや削除基準を明確化し、透明性の高いレポートを公表していくことを発表した※490。

まだまだ向上の余地はあるものの、公的機関、SNS事業者等は新たな誹謗中傷の被害者を出さないよう活動を行っている。一方、SNSの投稿者も自らの言動に責任を持ち、加害者とならないよう意識の変革が求められる。

2019年に行方不明になった小学生の母親に対し、「殺すぞ」等のメッセージをSNS上に投稿して脅迫した被告の初公判が2020年10月に開かれた。被告の男は、逮捕後に自分自身もインターネット上で誹謗中傷を受けており、初公判の場で「被害者の気持ちが身にしみて分かった」と謝罪を述べた※491。この言葉が一つの教訓となるのではないだろうか。

2.7.2 Withコロナにおける普及啓発活動

新型コロナウイルスの蔓延防止策の一つとして、一層利活用が進むインターネットを、安全に使用するための新たな取り組みについて考察する。

(1)テレワーク・オンライン授業

内閣府が発表した「新型コロナウイルス感染症の影響下における生活意識・行動の変化に関する調査※492」によると、国内のテレワーク実施率は2020年5月時点では全国平均で27.7%、同年12月には21.5%であった。テレワークは働き方改革の切り札の一つでもあることから、導入・実施の継続に対する期待が続いている。

2020年12月、厚生労働省はテレワークについて、実施の際の留意点や関連情報をまとめたリーフレット「テレワークを有効に活用しましょう※493」を公開した。テレワークを実施するまでの流れや労務管理はもちろん、情報セキュリティの必要性についても言及されており、テレワークの開始前に一読することが望まれる。また、総務省では、情報セキュリティの担当者が選任されていない中小企業においても、テレワークを実施する際に必要最低限の対策が行えるよう「テレワークセキュリティに関する手引き(チェックリスト)」を公開している※108。

IPAは、「不正アクセス防止対策に関する官民意見集約委員会(官民ボード)」の活動の一環として運営する情報セキュリティ・ポータルサイト「ここからセキュリティ!※494」上に、テレワークに関するセキュリティ情報を集約し公開した(図2-7-4)。このページでは、官民ボードメンバーが各々公開する情報の中から、テレワークを導入する際に参考となるガイドラインや、Web会議システムの利用時に必要な対策等30以上のコンテンツが紹介されている。

■図2-7-4　テレワークのセキュリティコンテンツ(一部)
(出典)IPA「ここからセキュリティ!」

2020年3月、政府の要請を受け、新型コロナウイルスの感染拡大防止策として多くの学校が休校となった。休校が長引くにつれて、オンライン授業の必要性が急浮上し、文部科学省は「新型コロナウイルスによる緊急事態宣言を受けた家庭での学習や校務継続のためのICTの積極的活用について※495」と題した事務連絡を各都道府県教育委員会に対して行った。この中で、家庭におけるICT機器利用の留意点として、情報セキュリティの確保の必要性が明記されている。また、付属のタブレット活用のルールのサンプルには、端末を使用する際に子ども達が注意すべき点が記載されており、安心・安全な利用のために必要な行動を学べる資料となっている。

更に、オンライン授業を早期に実現するため、2020年度第3次補正予算が成立しGIGAスクール構想が加速し始めた。GIGAスクール構想は、子ども達に1人1台の端末と通信ネットワークを提供し、個別最適化された学びを実現すること等を目的として2019年12月に文部科学省が打ち出した計画である※496。学校は計画を急ピッチで進めるだけではなく、2019年10月に文部科学省が改訂した「教育情報セキュリティポリシーに関するガイドライン※497」を実践することが不可欠である。

一部の学校では、インターネットを利用するために身に

付けるべき事項について、オンラインで学べるツールを開発し、臨時休業中も積極的な指導を行った。

立教新座中学校・高等学校では、インターネットを利用した授業は、「多くの情報から必要な情報を取捨選択する力の育成」「情報社会に積極的に参画する機会」であるととらえ、オンラインで視聴できる動画やオンライン確認テストを開発した（図 2-7-5）。

オンライン授業が推進される中、インターネットを利用する児童生徒が、インターネットを利用する前、または利用しながら情報モラルや情報セキュリティの知識を習得することは、今後一層重視されると予想される。

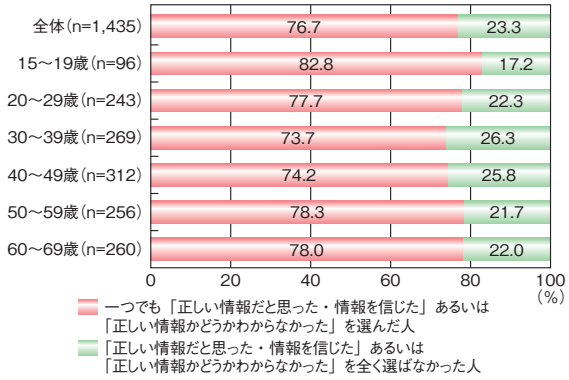
■図 2-7-5　オンライン教材（確認テスト）
（出典）立教新座中学校・高等学校提供

(2) フェイクニュースやデマへの対応

2020 年 4 月に出された緊急事態宣言下において、テレビのニュース番組では、スーパーマーケットのトイレットペーパー売り場に品物がなくなっている映像を繰り返し映し出した。「買いだめはしないでください」「紙はなくなっていません」というアナウンスよりも、映像のインパクトは大きかった。トイレットペーパーが品薄になるというデマは、SNS 上での発言が端緒ともいわれている※498。

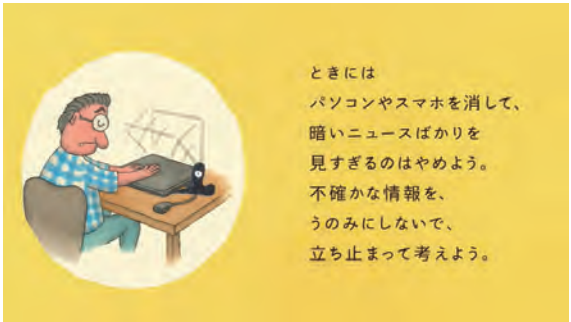
総務省が公表した「新型コロナウイルス感染症に関する情報流通調査※499」では、新型コロナウイルスに関するフェイクニュースやデマを見聞きした人は 72.0% に上った。そのうち、フェイクニュースやデマを「正しい情報だと思った・情報を信じた」あるいは「正しい情報かどうかわからなかった」人は 76.7% であった（図 2-7-6）。このうちの 35.5% は、その情報をほかの人と共有・拡散したと回答しており、少なくない人が偽の情報を広める側に回ってしまったことが分かる。

台湾においてもトイレットペーパーの在庫が切れるというデマがネット上で拡散されたが、お尻を振るマンガ絵の行政院長が「お尻はみんなひとつしかないよ」と語り、「マスクの原料は台湾産、ティッシュペーパーは南米産」と説明したポスターを投稿した。このユーモアのある投稿のおかげで正しい情報の方が、デマや誤情報よりも拡散されたため、台湾では事態の悪化が防げた※500。ユーモアのある投稿が拡散され、デマの力を弱めたと考えられており、学べることがありそうだ。



■図 2-7-6　新型コロナウイルスに関する間違った情報や誤解を招く情報への接触状況
（出典）総務省「新型コロナウイルス感染症に関する情報流通調査」を基に IPA が編集

人から人へと広がる玉石混交な情報に振り回され、新たな問題を引き起こしてしまうことがないよう、日本赤十字社が動画「ウイルスの次にやってくるもの※501」を公開している（図 2-7-7）。この中では、「誰にもまだわからないことは、誰にもまだわからないことでしかない。そのままを受け止めよう」と、情報を冷静に取り扱うことの重要性が訴えられている。



■図 2-7-7　心や社会を守る心構えを伝える動画コンテンツ
（出典）日本赤十字社「ウイルスの次にやってくるもの」

(3) コロナ差別への対応

新型コロナウイルスの患者や、医療従事者への偏見や差別が問題となっている。インターネット上で感染者やその家族を特定する動きや、感染者と思しき人に対する差別的な書き込みが行われ、ある被害者は「ウイルスより

恐ろしかった」としている※502。

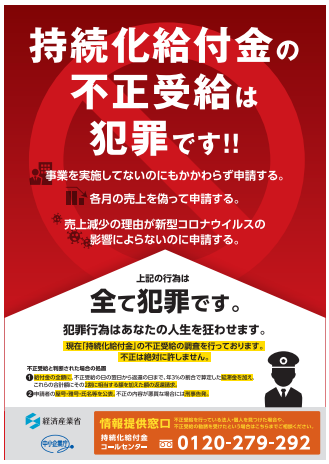
宮城県は、2020年12月、新型コロナウイルスの感染者やその関係者に対する誹謗中傷や偏見、差別の根絶を訴える決議案を可決した。これを受けて、行政、医療、学校等が連携し「ストップ!コロナ差別」の共同宣言が行われチラシが作成される等、啓発活動が行われた※503。

2021年2月、厚生労働省は新型コロナウイルスに関する偏見や差別を防止するための規定が設けられた「新型インフルエンザ等対策特別措置法等の一部を改正する法律」を公布した※504。この法律の改正により、感染者の個人名等を特定し、SNS等で公表・非難するような行為は許されない事例であることが示された。

(4) SNSによる悪質な勧誘への対応

特殊詐欺の「受け子」等に代表される「闇バイト」の勧誘は、SNSによって発信されるものが依然として少なくない。2020年は新型コロナウイルスの感染拡大防止のため、営業自粛等の影響を受ける事業者に対する支援策として持続化給付金が支給された。しかし、この制度を悪用した不正受給の勧誘が行われ、SNSもその手段の一つとなった。独立行政法人国民生活センターは「新型コロナウイルスに便乗した悪質商法にご注意!※505」と題した報道発表を行い、犯罪に加担しないよう注意を促した。また、経済産業省と中小企業庁は「犯罪行為はあなたの人生を狂わせます」と、犯罪抑止のメッセージを発信した(図2-7-8)。

また、犯罪被害につながるアルバイトにも注意が必要である。「荷物転送バイト」の勧誘は、新型コロナウイルスが蔓延する中、「自宅にいながら安全に稼ぐ方法」としてSNS上に広がっている。このアルバイトに登録する際には、写真付きの身分証明書等の個人情報の提示を求められ、この情報が携帯電話等の契約に悪用されている。知らぬ間に契約された登録者は、携帯電話の料金を請求されるほか、自分名義の携帯電話が特殊詐欺等に利用されてしまうことから、神奈川県と埼玉県は注意を呼びかけた※507。



■図2-7-8　持続化給付金の不正受給を抑止するためのチラシ
(出典)経済産業省・中小企業庁「持続化給付金の不正受給は犯罪です!!※506」

2.7.3 今後の課題

「2.7.2 Withコロナにおける普及啓発活動」に記したとおり、国内の多くの学校が新型コロナウイルスの感染予防対策による休校を余儀なくされた。教育委員会等から休校中に活用できる資料やツールが公開されている。

しかし、インターネットにアクセスする術を持たない子どもと、自由に通信機器を使用してインターネットにアクセスできる環境にある子どもとでは、その活用に大きな開きがあったことが推測される。また、保護者が傍らにいて、操作方法等について指導を受けた子どもとそうでない子どもとでは、インターネットの危険性を知る機会に差ができたことも推測される。

2021年2月、新型コロナウイルスのワクチン接種が開始され、日常を取り戻す兆しが見え始めた。ワクチン接種後の副反応が懸念される中、厚生労働省は接種を受けた後の健康状況についてSNSを利用した調査を行うこととした。また、同省は、新型コロナウイルスのワクチンに関する相談窓口等の情報や、新型コロナウイルスにより、家計に影響を受けたひとり親世帯に対する「ひとり親世帯臨時特別給付金」の受け取りの呼びかけ等、SNSを通じて様々な情報を発信している。

これらは、SNSで情報の収集や送信をしなければ、自分の行動や、更には生活にまで影響する重要な情報を得られない状況となりつつあることを示している。

インターネットのみならずSNSも生活の「インフラ」になったというのはたやすい。しかし、スマートフォンやタブレットを所有しない人や、新型コロナウイルスの影響で、ITサービスへの出費が困難になった人に、SNSを使った情報が届くのかどうか、課題は少なくない。

スマートフォン等のアプリケーションやサービスが多数提供されたことにより、メディアの種類は格段に増加しているといえる。様々な環境下にある人にどのようなメディアを使って平等に情報を伝えるのか、平等性が求められる学習や健康、生活等に関連する情報をすべての人に届ける手段について、情報発信者は十分に検討する必要があるだろう。

COLUMN

みんなバラバラにならないで!

こんにちは! ぼくは、IPA「ひろげよう情報モラル・セキュリティコンクール」応援隊長のまもるです。新型コロナウイルスの影響で、学校に行けなくなったり、家族がお家で仕事するようになったり、いろんなことが変わったね。頑張って変化に対応しながらも、みんなが元気でいてくれるといいな、と思っているよ!

さて、この新型コロナの発生によって、悲しい出来事がネットでもたくさん起きてしまいました。例えば、一生懸命患者さんを治療しているお医者さんや看護師さんに対して SNS で意地悪を言ったり、感染したお友達が通っている学校に「学校をなくしてしまえ」なんて悲しいメールを送ったり。コロナだけでもとても大変な状況なのに、どうしてこんなことになってしまうのかな。ぼくは、家族で話し合ったりネットで調べたりして、こう考えてみたよ。

世の中は「感染している人」と「感染していない人」だけがいると考えると、そこにはどうしても大きな溝ができてしまう。例えば「感染していない人」は感染したくないから「感染している人」とは距離を置きたくなる。もちろん、感染を拡大させないためには物理的な距離を置く必要はあるのだけれど、でも、心まで離れてしまう必要はないよね。

誰だって(もちろん、感染してしまった人だって!)コロナにかかりたくない。でも、目に見えないウイルスは、いつの間にか忍び寄って来て体を蝕む。それは、「感染した人」だって「感染していない人」だって気がつかないうちに起きていることなんだ。それに、自分は感染していないと思っている人も、本当は今「感染している」かもしれないし、「過去に感染していた」かもしれない。今感染していなくても、いつかかるかわからないから「感染していない人」は「まだ感染してない人」と言い換えることもできるよね。そう考えると「感染していない人」は、「感染している人」を攻撃できなくなるはずだよ!

東京都では「戦うべき本当の相手は人ではなくウイルスです[i]」というメッセージを出したよ。ほんとだね。誰だって新型コロナにかかりたくはないけれど、戦う相手が見えないから混乱して、本当に大切なことを見失ってしまっているのかもしれないね。

「コロナはとても嫌なウイルスで、この地球に来なければよかったのに」と思うけど、コロナはもう来てしまって、ぼくたちの健康を脅かしている。それにぼくたちを「感染している人」と「感染していない人」に分けて心の健康にまで影響してきているよ。心も体もコロナに負けちゃいけない。そして、ぼくたち自らが「分断」しちゃいけない。こんなときだからこそネットのコミュニケーションツールを良いほうに使おうよ。心を通わせたメッセージを発信しよう。みんなが、力を合わせられるように。

i 東京都:東京都総務局人権部 じんけんのとびら https://www.soumu.metro.tokyo.lg.jp/10jinken/〔2021/6/16 確認〕

2.8 その他の情報セキュリティ動向

営業秘密保護の動向、暗号技術の動向、及び情報セキュリティ市場の規模と成長の動向について述べる。

2.8.1 営業秘密保護の動向

企業の技術情報や顧客情報等、営業秘密の活用は企業の競争力の強化に重要な役割を果たす一方、ひとたび営業秘密が漏えいすると、事業に深刻な影響を及ぼすことから、その保護は喫緊の課題である。

営業秘密の保護については、業務のデジタル化を背景としたビッグデータの利活用や AI 等の解析技術の進展等を踏まえ、政府による環境整備が進められている。

法整備の面では、不正競争防止法※508 第五条の二（推定規定）の「技術上の秘密」として「情報の評価又は分析の方法」を対象とし、「技術上の秘密を使用したことが明らかな行為」として「情報の評価又は分析の方法を使用して評価し、又は分析する役務の提供」を対象とすること等を規定した不正競争防止法施行令が 2018 年 11 月に施行された※509。また、2019 年 7 月には「限定提供データ」の不正取得等を不正競争行為として追加した規定も施行された※510。

更に、クラウド等、情報の管理形態の多様化等を踏まえた営業秘密管理指針の改訂※511 も 2019 年 1 月に行われている。

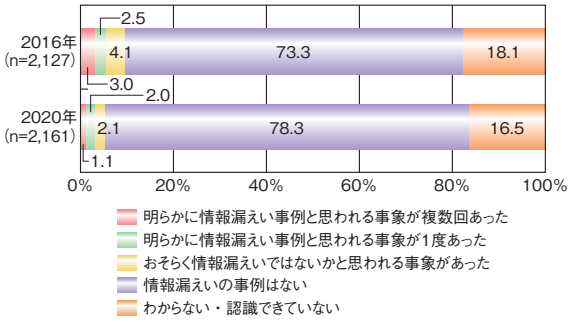
企業もこれらの動きに合わせ、営業秘密の保護に向けた情報セキュリティ対策等を強化していく必要がある。こうした状況を踏まえ、IPA は 2020 年度、「企業における営業秘密管理に関する実態調査 2020」を実施した※512。本調査では、2016 年に行った同一目的の調査※513（以下、前回調査）以降の情報漏えい発生状況、管理実態や対策の変化、法改正の影響等を企業アンケートやインタビューにより確認したほか、文献・裁判例の最新動向を調査した。その調査結果から、いくつかのポイントを紹介する。

(1) 営業秘密情報漏えいの実態

営業秘密情報の漏えいの実態としてインシデント発生状況とその原因について述べる。

(a) 情報漏えいインシデント発生状況

「明らかに情報漏えいと思われる事象が 1 回以上発生した」と回答した割合は 3.1% で、前回調査時の 5.5% より減少したが、この要因としては企業の対策が実際に進展した効果のほか、攻撃の巧妙化により事象そのものを認知しにくくなっている可能性等、複数の要因が作用しての結果と考えられる。また、「情報漏えいの事例はない」の割合が 78.3% で、前回の 73.3% から増加しており、情報漏えいの監視・検知は課題となっている（図 2-8-1）。



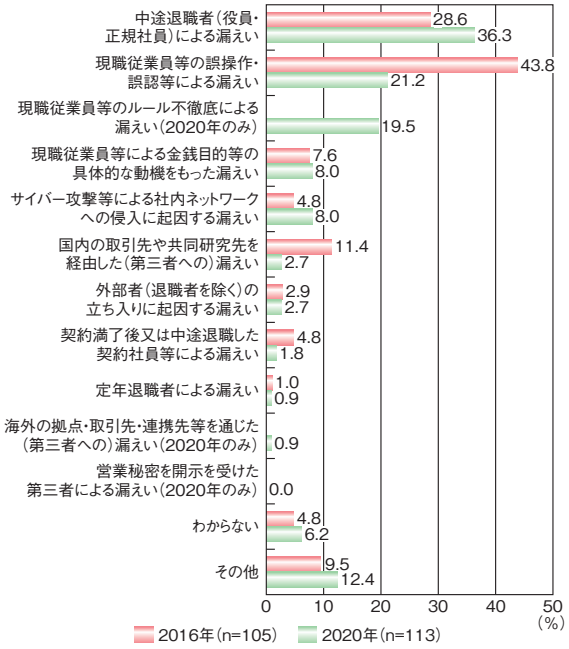
■図 2-8-1　営業秘密漏えいの発生状況（複数選択）
（出典）IPA「企業における営業秘密管理の実態調査 2020」を基に作成

(b) 秘密保持契約締結状況・情報漏えいの原因等

情報漏えいがあったと回答した企業の中で、役員を対象に秘密保持契約を締結している企業は前回調査の 36.3% から 44.6% へ増加した。また、従業員を対象に秘密保持契約を締結している企業も 46.1% から 56.6% へと増加した。ただし、秘密保持契約を締結していない企業のうち、「特に理由はない」と回答した比率が 37.4% とかなり高く、今後の改善の余地があることがうかがえる。

情報漏えいがあった場合の原因については、「誤操作、誤認等」が 21.2% と前回調査時と比べて約半減した一方、「中途退職者」が前回調査時より増加し、36.3% と項目の中で最多となった（次ページ図 2-8-2）。中途退職者による情報漏えいは技術的に防ぐことが難しく、状況の改善が容易ではないことがうかがえる。

情報漏えいが判明した場合に実施したアクションは、「行為者（と疑われる者）に対するヒアリング」や「ログ等の確認」の割合がそれぞれ 50.5%、43.2% と高かったものの、デジタルフォレンジック調査まで踏み込んで実施した比率は 10% に満たなかった。従業員 300 名以下の製造業では、「何をすべきかわからなかったので何もしなかった」割合が 17.2% と突出して高かった。



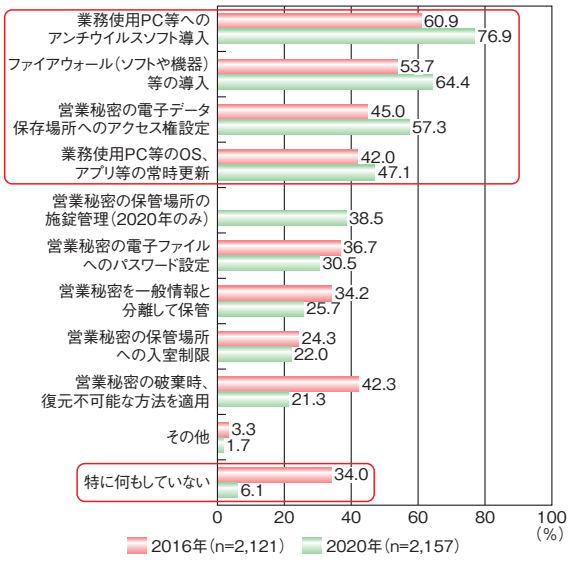
■図 2-8-2　営業秘密の漏えい原因
（出典）IPA「企業における営業秘密管理の実態調査 2020」を基に作成

(2) 漏えい対策・情報管理状況

営業秘密情報の漏えい対策や、情報管理状況のポイントについて述べる。

(a) 不正アクセスの防止対策状況

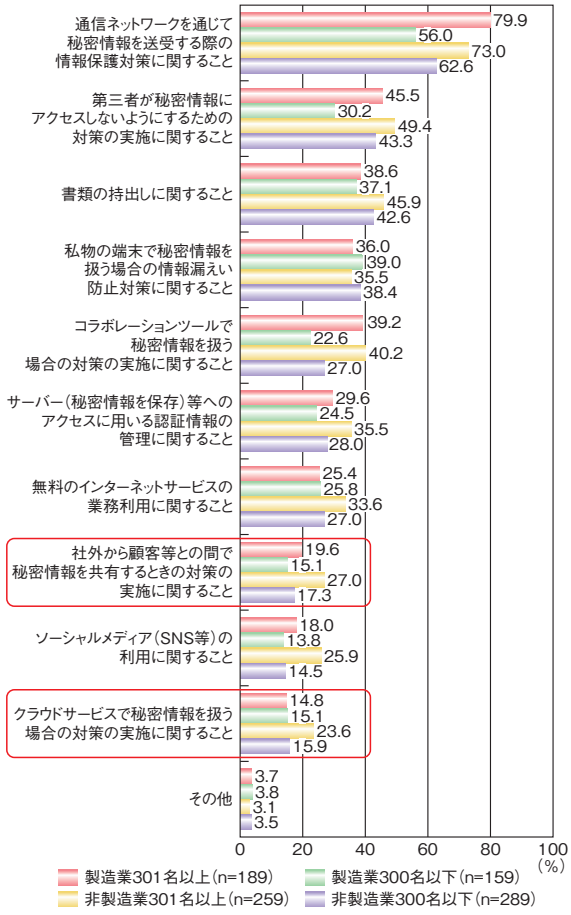
営業秘密情報への不正なアクセスの防止対策としては、「特に何もしていない」割合は 6.1% で、前回調査時の 34.0% と比較して大幅減となった。また、アンチウイルスソフト導入やファイアウォール等の導入、アクセス権の設定等、基礎的な対策の伸びが見られた（図 2-8-3）。



■図 2-8-3　営業秘密情報への不正なアクセスを防ぐための対策の実施状況
（出典）IPA「企業における営業秘密管理の実態調査 2020」を基に作成

(b) テレワーク（在宅勤務等）における管理規定の状況

テレワーク等に関して何らかの情報管理ルール等を整備している、と回答した企業に具体的な内容を尋ねた結果、「秘密情報を社外から取引先と共有する際のルール」や「クラウドサービスで扱う場合のルール」を取り決めている割合が低い（回答企業の各カテゴリーで 30% 未満）ことが分かった（図 2-8-4）。



■図 2-8-4　テレワークで営業秘密を扱う場合に規定したルール（企業規模・業種別）
（出典）IPA「企業における営業秘密管理の実態調査 2020」を基に作成

(3) 営業秘密管理の傾向と課題のまとめ

インタビューを含む調査結果を踏まえ、2020 年度調査による営業秘密保護状況の傾向と課題をまとめる。

- 情報漏えいインシデントの発生は減少したものの、攻撃側の手口の巧妙化等の複数の要因が作用し、減少したように見えている可能性もある。また、テレワーク・クラウド利用等の増加により、組織内に情報を保管して業務を行うよりも漏えい経路が増えていることに注意しなければならない。
- 企業の情報持ち出し規則の整備や普及啓発等により、従業員のミスによる漏えい割合は減少し、漏えい

原因の多くが中途退職者であった。この結果、内部不正による漏えいの割合は相対的に増加した。ますます進展すると想定される雇用の流動化に備え、中途退職者の不正防止対策を強化することが必要である。

- 漏えいが判明したときの対応として、ログの確認等は既に広く実施されているが、情報の廃棄状況の確認や漏えい時の証跡確保で重要となるデジタルフォレンジック調査等は、実施に困難が伴うこともあってまだ浸透していない。
- 基本的な対策として、従業員と秘密保持契約を締結する企業は増えた。不正アクセス防止についても、アクセス権設定等の基本的な対策を中心に進んだ。一方で、対策を従業員に周知していない企業が増加しており、心理的な抑止効果・啓発の観点からは周知が望まれる。
- テレワークの急速な普及により、これまで想定されていなかった環境下で営業秘密を扱う体制やルールの整備が求められており、特にテレワーク環境での他社との情報共有ルールやクラウドサービスでの秘密情報の扱い等について、体制やルールの整備を含む対策が求められている。

情報管理に従事する情報システムや知的財産管理の担当者は、これらの調査結果を自組織の状況と比較し、規程の整備や漏えい対策の強化等の活動の一助としていただきたい。

2.8.2 暗号技術の動向

本項では2020年度における、共通鍵暗号、公開鍵暗号、軽量暗号及び実装攻撃に関する研究及び標準化の動向についてそれぞれ解説する。

(1) 共通鍵暗号に関する研究動向

共通鍵暗号技術に対する攻撃としては、既存の暗号アルゴリズムへの攻撃について、攻撃に必要な計算量の削減等の進展があった。ここでは主な発表を紹介する。

差分攻撃[※514]の拡張であるBoomerang Attackの改良版が発表され[※515]、ラウンド数5のAES[※516]に適用した結果は計算量が$2^{16.5}$(すなわち、全鍵復元において9万回の暗号化と復号の操作しか要求しない)にまで改良した。AESに対する攻撃は2020年度も進展は見られたが、安全性マージンはまだあり、AESの安全性に直ちに影響を与えるものではない。

その他の暗号については、ARX(Addition, Rotation, and XOR)ベースの暗号に対する差分線形解析[※517]の改良が発表された[※518]。ストリーム暗号の一種であるChaCha[※519]がこのタイプに属する。ラウンド数6のChaChaでは時間計算量が$2^{77.4}$、データ計算量が2^{58}、ラウンド数7のChaChaでは時間計算量が$2^{230.86}$、データ計算量が$2^{48.83}$という結果になっており、これまでの記録を上回っているが、ChaCha20のラウンド数20にはまだ安全性マージンがあり、早急な対策が必要となるものではない。

(2) 公開鍵暗号に関する研究及び標準化の動向

公開鍵暗号に関しては、Crypto 2020においてフランス・リモージュ大学のFabrice Boudotらにより、795ビットの素因数分解(RSA-240)及び離散対数計算(DLP-240)に対する新記録が報告され[※520]、前者は約1,000コア年、後者は約3,200コア年の計算量であった。これまでの記録はいずれも768ビット(2009年のRSA-768と2016年の768ビット離散対数)であったが、例えば離散対数の関係探索においては前回時間よりも25%少ない時間で済む等、両計算においてかなりの高速化が実現された。また離散対数計算の素因数分解に対する計算量比率も約3倍と、これまで考えられていた程差があるわけではないことが判明した。更に、別の記録となるRSA-250に対する素因数分解の結果も報告され、本分野において多大な貢献があり、2020年に亡くなったPeter L. Montgomery氏に捧げられた。

NISTによる、量子コンピュータに耐性を持つ暗号「耐量子計算機暗号(PQC:Post-Quantum Cryptography)」の標準化は、2020年7月22日に候補を26件から15件に絞って第3ラウンドに入り、七つの最終候補(Finalist)及び八つの代替候補(Alternate)の評価が進められている。第3ラウンド候補数及び暗号名を表2-8-1(次ページ)に示す。2021年1月22日、PQC Forumメーリングリストにおいて、NISTは「最近の暗号解析が多変数署名Rainbow及びGeMSSに影響を与えたため、セキュリティ及びアプリケーションの観点から多様性欠如の懸念を持っている」旨のメールを投稿した。更にNISTは、第2ラウンド時のレポートから、SPHINCS+が第3ラウンドの終わりの時点で標準のアルゴリズムになる可能性について言及した部分、及び標準化プロセスにないスキームを採用する可能性について言及した部分を議論のスタートポイントとして提示し、意見を募った。今後の予断を許さない状況となり、第3回標

準化会議を2021年6月7～9日に開催する予定で論文募集が行われた（投稿締切り：4月23日、採録通知：5月7日）。

(3) 軽量暗号に関する標準化の動向

NISTのLightweight Cryptographyプロジェクトにおいて、軽量暗号の標準化が行われており、応募された57のアルゴリズムから32のアルゴリズムが残っていたが、2021年3月末にファイナリストとして、10のアルゴリズム（ASCON、Elephant、GIFT-COFB、Grain128-AEAD、ISAP、Photon-Beetle、Romulus、Sparkle、TinyJambu、Xoodyak）が選出された※522。

今後約1年かけて標準化するアルゴリズムが選出される予定である。

(4) 実装攻撃に関する研究動向

暗号実装に対する攻撃には、消費電力や処理時間等のサイドチャネル情報から暗号鍵等の秘密情報の復元を試みるサイドチャネル攻撃や、ICチップに一時的な誤動作を起こさせることによって暗号鍵等の秘密情報の暴露を試みる故障利用攻撃等が存在する。

具体的な暗号実装に対する攻撃として、ECDSA※523の実装に対するタイミング攻撃が発表された※524。この論文では、発表時において、数個のソフトウェア暗号ライブラリとハードウェア実装に対してこの攻撃が有効であることを示している。ECDSA署名の計算時に使用するnonce※525のビット長が、処理時間の差という形で漏えいする場合、数千個の署名生成の電力波形から秘密鍵が復元される可能性がある。この脆弱性に関するCVE※526も発行されている。この結果は、ECDSAを実装するにあたって、nonceの扱いに注意が必要であることを示している。別の種類の楕円曲線を使用する署名アルゴリズムであるEdDSAは、nonceの生成方法に違いがあることからこの攻撃に対しては耐性がある。

その他、具体的な実装に対する攻撃として、ECDSAとRSAの実装に対する、暗号演算に含まれるbinary GCDアルゴリズム※527のサイドチャネル攻撃に関する脆弱性の発表※528、楕円曲線演算における点の射影座標表現でのZ座標のリークを利用した攻撃の発表※529もあり、暗号演算の様々な箇所に対する実装攻撃が研究されている。

2.8.3 情報セキュリティ市場の動向

JNSAが発表した「2020年度 国内情報セキュリティ市場調査報告書※530」によると、2020年度の情報セキュリティ市場規模（ツールとサービスを合わせた数値）は、2019年度より3.5%の伸びとなる見込みである。

情報セキュリティのツールとサービスそれぞれの市場規模の推移を図2-8-5と図2-8-6（次ページ）に、調査市場区分を表2-8-2（次ページ）に示す。図中の2018年度、2019年度については売上高推定実績値で、2020年度については売上高推定見込値、2021年度については売上高予測値である。

情報セキュリティツールの市場規模全体では、2019年度に比べ2020年度は3.3%伸びている。ツールの区分別に見ても、「エンドポイント保護管理製品」の2019年度比9.5%増、「ネットワーク防御・検知／境界線防御製品」の2019年度比2.1%増等、すべての区分で増加傾向が続いている。

情報セキュリティサービスの市場規模全体では、2019年度に比べ2020年度は3.9%伸びている。サービスの区分別に見ても、「コンサルティング／診断サービス」の2019年度比3.7%増、「マネージド・運用サービス」の

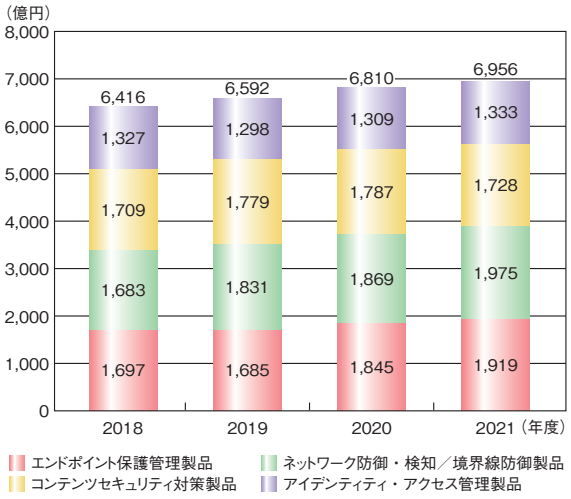
	電子署名		鍵カプセル化機構／暗号化		合計
	暗号名	候補数	暗号名	候補数	
格子ベース	Crystals-Dilithium (F), Falcon (F)	2	Crystals-Kyber (F), FrodoKEM (A), NTRU (F), NTRU Prime (A), Saber (F)	5	7
符号ベース	—	0	ClassicMcEliece (F), BIKE (A), HQC (A)	3	3
多変数	Rainbow (F), GeMSS (A)	2	—	0	2
ハッシュベース	SPHINCS+ (A), Picnic (A)	2	—	0	2
その他	—	0	SIKE (A)	1	1
合計	6 (F:3, A:3)		9 (F:4, A:5)		15

F：Finalist（最終候補）、A：Alternate（代替候補）

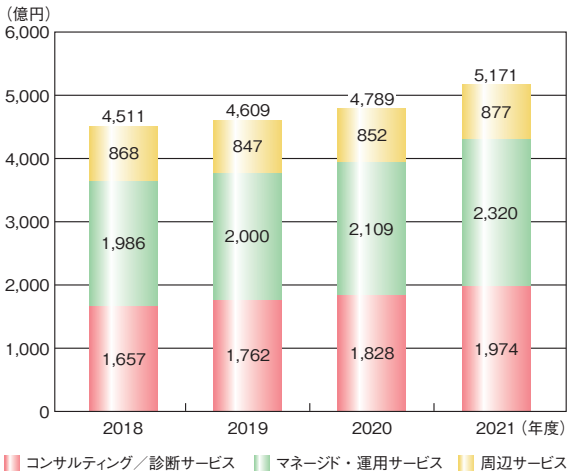
■表2-8-1 NIST PQCコンペティション応募暗号数及び暗号名（第3ラウンド）
（出典）Dustin Moody（NIST）「NIST PQC Standardization Update – Round 2 and Beyond※521」を基にIPAが編集

2019 年度比 5.5% 増等、すべての区分で増加傾向が続いている。

以上のように、情報セキュリティ市場の規模は拡大傾向が続いている。2020 年度は新型コロナウイルスにより経済活動には大きな影響があったが、テレワークやオンライン会議等の普及や DX の推進、クラウドサービスの利用拡大に伴い、これらに対するサイバー攻撃へのセキュリティ対策等が促進されたと考えられる。2020 年度以降においても引き続き国内情報セキュリティ市場は堅調に推移することが予測される。



■図 2-8-5　国内情報セキュリティツール市場規模の推移
（出典）JNSA「2020 年度 国内情報セキュリティ市場調査報告書」を基に IPA が編集



■図 2-8-6　国内情報セキュリティサービス市場規模の推移
（出典）JNSA「2020 年度 国内情報セキュリティ市場調査報告書」を基に IPA が編集

大分類	中分類	小分類
情報セキュリティツール	エンドポイント保護管理製品	ウイルス対策、EDR、ポリシー管理・設定管理・動作監視制御製品
	ネットワーク防御・検知／境界線防御製品	FW、VPN 接続、IDS ／ IPS、WAF、UTM、セキュリティ情報管理システム、物理セキュリティシステム
	コンテンツセキュリティ対策製品	DLP（情報漏えい対策）、DRM、暗号化、メール・セキュリティ対策、URL フィルタリング、脆弱性検査
	アイデンティティ・アクセス管理製品	個人認証用デバイス及びその認証システム、個人認証用生体認証デバイス及びその認証システム、アイデンティティ（ID）管理、ログオン管理／アクセス許可、PKI システム及びそのコンポーネント
情報セキュリティサービス	コンサルティング／診断サービス	コンサルティング、監査・評価、診断、規格認証
	マネージド・運用サービス	SOC、インシデント対応・フォレンジック、インテリジェンス情報提供
	周辺サービス	電子証明書発行・PK 型認証、リテラシー教育、資格取得支援、保険

■表 2-8-2　情報セキュリティツール・サービスの調査市場区分
（出典）JNSA「2020 年度 国内情報セキュリティ市場調査報告書」を基に IPA が編集

※1　政府機関等の情報セキュリティ対策のための統一基準群：国の行政機関及び独立行政法人等の情報セキュリティ水準を向上させるための統一的な枠組みを指す。国の行政機関及び独立行政法人等の情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項を規定している。
NISC：「政府機関等の情報セキュリティ対策のための統一基準群（平成30年度版）」について　https://www.nisc.go.jp/active/general/kijun30.html〔2021/5/31 確認〕
※2　首相官邸：サイバーセキュリティ戦略本部について　https://www.kantei.go.jp/jp/tyoukanpress/202102/10_a.html〔2021/5/31 確認〕
NISC：次期サイバーセキュリティ戦略の検討について　https://www.nisc.go.jp/conference/cs/dai26/pdf/26shiryou01.pdf〔2021/5/31 確認〕
※3　NISC：次期サイバーセキュリティ戦略の骨子について　https://www.nisc.go.jp/conference/cs/dai28/pdf/28shiryou01.pdf〔2021/5/31 確認〕
※4　NISC：サイバーセキュリティ2020　https://www.nisc.go.jp/active/kihon/pdf/cs2020.pdf〔2021/5/31 確認〕
※5　NEDO：戦略的イノベーション創造プログラム（SIP）第2期／IoT社会に対応したサイバー・フィジカル・セキュリティ　https://www.nedo.go.jp/activities/ZZJP2_100123.html〔2021/5/31 確認〕
※6　NEDO：「SIP『IoT社会に対応したサイバー・フィジカル・セキュリティ』ONLINEシンポジウム2020」の開催　https://www.nedo.go.jp/events/IT_100060.html〔2021/5/31 確認〕
※7　https://www.soumu.go.jp/main_content/000750257.pdf〔2021/5/31 確認〕
※8　https://www.soumu.go.jp/main_content/000711459.pdf〔2021/5/31 確認〕
※9　NISC：サイバーセキュリティ対策推進会議（CISO等連絡会議）https://www.nisc.go.jp/conference/cs/taisaku/index.html〔2021/5/31 確認〕
※10 https://www.nisc.go.jp/active/general/pdf/itakusaki_moshiawase.pdf〔2021/5/31 確認〕
※11 https://www.nisc.go.jp/active/general/pdf/choutatsu_moshiawase_kaisei.pdf〔2021/5/31 確認〕
※12 外務省：国連安保理アリア・フォーミュラ会合（サイバー空間の安定化，紛争予防，能力構築）　https://www.mofa.go.jp/mofaj/fp/cp/page24_001098.html〔2021/5/31 確認〕
※13 外務省：サイバーセキュリティに関する国連オープン・エンド作業部会最終会合における報告書の採択　https://www.mofa.go.jp/mofaj/press/release/press3_000453.html〔2021/5/31 確認〕
※14 NISC：第13回　日・ASEANサイバーセキュリティ政策会議の結果　https://www.nisc.go.jp/press/pdf/aseanj_meeting20201106.pdf〔2021/5/31 確認〕
※15 NISC：国際サイバーセキュリティワークショップ・演習の開催　https://www.nisc.go.jp/active/kokusai/pdf/international_ws_ttx_20210305.pdf〔2021/5/31 確認〕
※16 NISC：サイバーセキュリティウェビナー「Control Cybersecurity Risk」の開催　https://www.nisc.go.jp/active/kokusai/pdf/seminar_thai_20210226.pdf〔2021/5/31 確認〕
※17 NISC：サイバーセキュリティウェビナー「Control Cybersecurity Risk」の開催（インドネシア）　https://www.nisc.go.jp/active/kokusai/pdf/seminar_indonesia_20210329.pdf〔2021/5/31 確認〕
※18 https://www.nisc.go.jp/conference/cs/kenkyu/wg/dai09/pdf/kenkyuwg-saishu.pdf〔2021/5/31 確認〕
※19 NISC：サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ 報告書 ～「戦略マネジメント層」の育成・定着に向けて～ https://www.nisc.go.jp/conference/cs/pdf/jinzai-sesaku2018set.pdf〔2021/5/31 確認〕
※20 https://www.nisc.go.jp/security-site/month/event/nisc-cs-seminar.html〔2021/5/31 確認〕
※21 https://cyder.nict.go.jp/index.html〔2021/5/31 確認〕
※22 NICT：2020年度 実践的サイバー防御演習「CYDER」の受講申込受付を開始　https://www.nict.go.jp/press/2020/07/01-3.html〔2021/5/31 確認〕
※23 NISC：重要インフラの情報セキュリティ対策に係る第4次行動計画　https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf〔2021/5/31 確認〕
※24 NISC：重要インフラの情報セキュリティ対策に係る第4次行動計画　https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r2.pdf〔2021/5/31 確認〕
※25 NISC：次期重要インフラ行動計画の検討について　https://www.nisc.go.jp/conference/cs/dai26/pdf/26shiryou06.pdf〔2021/5/31 確認〕
※26 NISC：重要インフラ専門調査会　https://www.nisc.go.jp/conference/cs/ciip/index.html〔2021/5/31 確認〕
※27 NISC：2020年度分野横断的演習について　https://www.nisc.go.jp/conference/cs/ciip/dai24/pdf/24shiryou04.pdf〔2021/5/31 確認〕
※28 日経クロステック：NCA初の「オンライン」サイバー攻撃演習、静寂の中で得た収穫と課題　https://xtech.nikkei.com/atcl/nxt/column/18/00001/04986/〔2021/5/31 確認〕
※29 金融庁：「金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅴ）」について　https://www.fsa.go.jp/news/r2/20201013.html〔2021/5/31 確認〕
※30 首相官邸：令和2年9月16日菅内閣総理大臣記者会見　https://www.kantei.go.jp/jp/99_suga/statement/2020/0916kaiken.html〔2021/5/31 確認〕
※31 日経クロステック：菅新政権の「デジタル庁」構想、焦点は人事権と内製化に　https://xtech.nikkei.com/atcl/nxt/column/18/01426/091700003/〔2021/5/31 確認〕
※32 首相官邸：デジタル・ガバメント閣僚会議　https://www.kantei.go.jp/jp/singi/it2/egov/〔2021/5/31 確認〕
※33 https://www.kantei.go.jp/jp/singi/it2/dgov/201225/siryou1.pdf〔2021/5/31 確認〕
※34 内閣官房：デジタル改革関連法案について　https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/dejigaba/dai14/siryou1.pdf〔2021/5/31 確認〕
※35 デジタル庁：https://www.digital.go.jp〔2021/5/31 確認〕
※36 デジタル庁：デジタル庁は「行政の透明化」を掲げ、noteでの発信を始めます。　https://note.digital.go.jp/n/n3690482b9676〔2021/5/31 確認〕
※37 経済産業省：産業サイバーセキュリティ研究会　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/〔2021/5/26 確認〕
※38 経済産業省：産業分野におけるサイバーセキュリティ政策　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/001_05_00.pdf〔2021/5/26 確認〕
※39 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20200417.pdf〔2021/5/26 確認〕
※40 経済産業省：産業サイバーセキュリティ強化へ向けたアクションプラン　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/002_03_00.pdf〔2021/5/26 確認〕
※41 経済産業省：第5回 産業サイバーセキュリティ研究会 事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/005_03_00.pdf〔2021/5/26 確認〕
※42 CPSFの詳細に関しては、「情報セキュリティ白書2020」の「2.1.2(1)(a)WG1（制度・技術・標準化）」(p.69)を参照。
※43 経済産業省：ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第1版　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/20190617_report.html〔2021/5/26 確認〕
※44 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/20210222_1.pdf〔2021/5/26 確認〕
※45 https://www.jama.or.jp/it/cyb_sec/download/cyb_sec_guideline_V01_00.pdf〔2021/5/26 確認〕
※46 https://www.meti.go.jp/press/2021/04/20210401005/20210401005-1.pdf〔2021/5/26 確認〕
※47 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/dainiso/pdf/004_03_00.pdf〔2021/5/26 確認〕
※48 経済産業省：IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）を策定しました　https://www.meti.go.jp/press/2020/11/20201105003/20201105003.html〔2021/5/26 確認〕
※49 経済産業省：『第3層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/daisanso/pdf/003_03_00.pdf〔2021/5/26 確認〕
※50 Software Bill of Material（SBOM）：ソフト部品構成表、ソフトウェア部品表等と呼ばれる、様々なソフトウェア部品の名称とそのライセンス等で構成される一覧表。米国商務省電気通信情報局（NTIA：National Telecommunications and Information Administration）が設立した「Software Component Transparency」において2018年から議論されている。
※51 経済産業省：サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/004_03_00.pdf〔2021/5/26 確認〕

※ 52 https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf〔2021/5/26 確認〕
※ 53 IPA：中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊）の報告書について https://www.ipa.go.jp/security/fy2019/reports/sme/otasuketai_houkoku.html〔2021/5/26 確認〕
※ 54 IPA：サイバーセキュリティお助け隊（令和２年度中小企業向けサイバーセキュリティ対策支援体制構築事業）https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index2020.html〔2021/5/26 確認〕
※ 55 IPA：サイバーセキュリティお助け隊サービス　https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html〔2021/5/26 確認〕
※ 56 経済産業省：昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性についての報告書を取りまとめました https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html〔2021/5/26 確認〕
※ 57 https://www.meti.go.jp/policy/netsecurity/downloadfiles/tebiki.pdf〔2021/5/26 確認〕
※ 58 経済産業省：「サイバーセキュリティ体制構築・人材確保の手引き」（第 1.1 版）を取りまとめました　https://www.meti.go.jp/press/2021/04/20210426002/20210426002.html〔2021/5/26 確認〕
※ 59 経済産業省：事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/006_03_00.pdf〔2021/5/26 確認〕
経済産業省：事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/007_03_00.pdf〔2021/5/26 確認〕
※ 60 経済産業省：事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/pdf/006_03_00.pdf〔2021/5/26 確認〕
※ 61 https://www.ipa.go.jp/files/000081564.pdf〔2021/5/26 確認〕
※ 62 IPA：2020 年度 セキュリティ製品の有効性検証の試行について　https://www.ipa.go.jp/security/economics/shikoukekka2021.html〔2021/5/26 確認〕
※ 63 経済産業省：機器のサイバーセキュリティ確保のためのセキュリティ検証の手引きを取りまとめました　https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html〔2021/5/26 確認〕
※ 64 IPA：コラボレーション・プラットフォームについて　https://www.ipa.go.jp/security/announce/collapla_index.html〔2021/5/26 確認〕
※ 65 https://www.meti.go.jp/press/2020/03/20210301004/20210301004-1.pdf〔2021/5/26 確認〕
※ 66 https://www.meti.go.jp/press/2020/09/20200930006/20200930006-2.pdf〔2021/5/26 確認〕
※ 67 https://www.meti.go.jp/shingikai/mono_info_service/dgs5/pdf/20201109_01.pdf〔2021/5/26 確認〕
※ 68 IPA：DX 認定制度　Web 申請受付開始のご案内　https://www.ipa.go.jp/ikc/info/dxcp.html〔2021/5/26 確認〕
※ 69 https://www.meti.go.jp/press/2020/08/20200828012/20200828012-1.pdf〔2021/5/26 確認〕
※ 70 IPA：「情報システム・モデル取引・契約書」第二版を公開 https://www.ipa.go.jp/ikc/reports/20201222.html〔2021/5/26 確認〕
※ 71 IPA：セキュリティ仕様策定プロセス　https://www.ipa.go.jp/files/000087454.docx〔2021/5/26 確認〕
IPA：情報システム開発契約のセキュリティ仕様作成のためのガイドライン ～ Windows Active Directory 編～　https://www.ipa.go.jp/files/000087453.docx〔2021/5/26 確認〕
※ 72 経済産業省：重要技術マネジメント　https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html〔2021/5/26 確認〕
※ 73 株式会社三菱総合研究所：「技術等情報管理認証制度に係る指導支援等の専門家派遣及び調査・広報事業」（経済産業省事業）において専門家の派遣を希望する事業者・団体の公募のご案内について https://www.mri.co.jp/news/public_offering/20201008.html〔2021/5/26 確認〕
※ 74 経済産業省：情報セキュリティサービス審査登録制度　https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html〔2021/5/20 確認〕
※ 75 審査登録機関：「情報セキュリティサービスに関する審査登録機関基準」に適合するとIPAが確認した機関。なお、申請事業者が「情報セキュリティサービス基準」に適合するか否かの審査・判定は、各審査登録機関がその責任において実施する。
※ 76 IPA：情報セキュリティサービス基準適合サービスリストの公開 https://www.ipa.go.jp/security/it-service/service_list.html〔2021/5/20 確認〕
※ 77 NISC：政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）　https://www.nisc.go.jp/active/general/pdf/guide30.pdf〔2021/5/20 確認〕
※ 78 SIG（Special Interest Group）：「特定の分野（各業界におけるサイバー攻撃に関する情報）について、情報を交換するグループ」という意味で、J-CSIP では各業界の参加組織の集合体を SIG と呼んでいる。
※ 79 https://www.ipa.go.jp/files/000090633.pdf〔2021/5/26 確認〕
※ 80 「マルウェア」等の用語を混在して使用すると、読者を混乱させる可能性があるため、本白書では特に断りのない限り、または文献引用上の正確性を期す必要のない限り、総称して「ウイルス」と表現する。
※ 81 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2020 年 7 月～ 9 月］　https://www.ipa.go.jp/files/000086549.pdf〔2021/5/26 確認〕
※ 82 IPA：サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））https://www.ipa.go.jp/security/J-CSIP/〔2021/5/26 確認〕
※事例については、上記 Web ページの「公開レポート」を参照。
※ 83 IPA：サイバーレスキュー隊 J-CRAT（ジェイ・クラート）　https://www.ipa.go.jp/security/J-CRAT/index.html〔2021/5/26 確認〕
IPA：J-CRAT ／標的型サイバー攻撃特別相談窓口　https://www.ipa.go.jp/security/tokubetsu/index.html〔2021/5/26 確認〕
※ 84 総務省：サイバーセキュリティタスクフォースの開催　https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000116.html〔2021/5/20 確認〕
※ 85 https://www.soumu.go.jp/main_content/000641510.pdf〔2021/5/20 確認〕
※ 86 https://www.soumu.go.jp/main_content/000698567.pdf〔2021/5/20 確認〕
※ 87 ITmedia NEWS：Microsoft のクラウドサービス、新型コロナ外出禁止地域での利用が 775％増　https://www.itmedia.co.jp/news/articles/2003/30/news075.html〔2021/5/20 確認〕
※ 88 https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf〔2021/5/20 確認〕
※ 89 総務省：「政府情報システムのためのセキュリティ評価制度（ISMAP）」の運用開始　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00071.html〔2021/5/20 確認〕
※ 90 https://www.soumu.go.jp/main_content/000722477.pdf〔2021/5/20 確認〕
※ 91 https://notice.go.jp/〔2021/5/20 確認〕
※ 92 総務省：サイバー攻撃に悪用されるおそれのある IoT 機器の調査（NOTICE）の取り組み強化　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00079.html〔2021/5/20 確認〕
※ 93 NICT：NICTER 観測レポート 2020 の公開　https://www.nict.go.jp/press/2021/02/16-1.html〔2021/5/20 確認〕
※ 94 MEC（Multi-access Edge Computing）：端末により近い場所にサーバを分散配置して処理するアーキテクチャ。
※ 95 一般社団法人 ICT-ISAC：5G セキュリティ推進グループの立ち上げについて　https://www.ict-isac.jp/news/news20200219.html〔2021/5/20 確認〕
※ 96 ローカル 5G：通信事業者ではない企業や自治体が、自らの建物内や敷地内でスポット的に柔軟に構築できる 5G システムのこと。
※ 97 参議院：議案情報　https://www.sangiin.go.jp/japanese/joho1/kousei/gian/201/meisai/m201080201022.htm〔2021/5/20 確認〕
※ 98 https://www.soumu.go.jp/main_content/000722596.pdf〔2021/5/20 確認〕
※ 99 NICT：量子コンピュータ実機を用いた離散対数問題の求解実験に成功　https://www.nict.go.jp/press/2020/12/09-1.html〔2021/5/20 確認〕
※ 100 https://www.soumu.go.jp/main_content/000733733.pdf〔2021/5/26 確認〕
※ 101 総務省：第 13 回 日・ASEAN サイバーセキュリティ政策会議の結果　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00083.html〔2021/5/20 確認〕
※ 102 総務省：テレワークの推進　https://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/index.htm〔2021/5/20 確認〕
※ 103 総務省：新型コロナウイルス感染症対策としてのテレワークの積極的な活用について　https://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/02ryutsu02_04000341.html〔2021/5/20 確認〕
※ 104 総務省：「テレワークマネージャー相談事業」について　https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000400.html〔2021/5/20 確認〕
※ 105 総務省：テレワークのセキュリティ安心無料相談窓口　https://www.soumu.go.jp/main_content/000697737.pdf〔2021/5/20 確認〕
※ 106 総務省：「テレワークセキュリティガイドライン（第 5 版）」（案）に対す

る意見募集 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00094.html〔2021/5/20 確認〕
※ 107 https://www.soumu.go.jp/main_content/000706649.pdf〔2021/5/20 確認〕
※ 108 総務省：テレワークセキュリティに関する手引き（チェックリスト）等の公表 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00080.html〔2021/5/20 確認〕
※ 109 設定解説資料は、手引き（チェックリスト）の内容を具体的な環境で実施する際の参考となるよう、テレワークで多く利用される製品を対象として補足的に作成している資料である。
※ 110 総務省：テレワークにおけるセキュリティ確保 https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/〔2021/5/20 確認〕
※ 111 https://www.soumu.go.jp/main_content/000711713.pdf〔2021/5/20 確認〕
※ 112 総務省：テレワークセキュリティに係る実態調査（2次実態調査）報告書 https://www.soumu.go.jp/main_content/000744643.pdf〔2021/5/20 確認〕
※ 113 総務省：「自治体情報セキュリティ対策の見直しについて」の公表 https://www.soumu.go.jp/menu_news/s-news/01gyosei07_02000098.html〔2021/5/20 確認〕
※ 114 https://www.soumu.go.jp/main_content/000727474.pdf〔2021/5/20 確認〕
※ 115 https://www.soumu.go.jp/main_content/000726080.pdf〔2021/5/20 確認〕
※ 116 トラストサービス：タイムスタンプ、eシール、リモート署名、eデリバリー、Webサイト認証等のサービスの総称で、日本が提唱する自由で信頼できるデータ流通（DFFT：Data Free Flow with Trust）の基盤である。トラストサービス検討WGにて各サービスの現状・課題・あるべき制度等の検討を行った。
※ 117 総務省：プラットフォームサービスに関する研究会における最終報告書（案）に対する意見募集の結果及び最終報告書の公表 https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000075.html〔2021/5/20 確認〕
※ 118 総務省：組織が発行するデータの信頼性を確保する制度に関する検討会 https://www.soumu.go.jp/main_sosiki/kenkyu/data_organization/index.html〔2021/5/20 確認〕
※ 119 総務省：タイムスタンプの国による認定制度 https://www.soumu.go.jp/main_content/000742673.pdf〔2021/5/20 確認〕
※ 120 https://www.soumu.go.jp/main_content/000710778.pdf〔2021/5/20 確認〕
※ 121 総務省：インターネット上の違法・有害情報に対する対応（プロバイダ責任制限法） https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/ihoyugai.html〔2021/5/26 確認〕
※ 122 総務省：インターネット上のフェイクニュースや偽情報への対策 https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/ihoyugai_05.html〔2021/5/26 確認〕
※ 123 総務省：インターネット上の誹謗中傷への対策 https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/hiboutyusyou.html〔2021/5/26 確認〕
※ 124 NISC：サイバーセキュリティ戦略 https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf〔2021/5/19 確認〕
※ 125 警察庁：サイバーセキュリティ重点施策の改定について（通達） https://www.npa.go.jp/cybersecurity/pdf/300906_juutensesaku.pdf〔2021/5/19 確認〕
※ 126 警察庁：サイバーセキュリティ戦略の改定について（依命通達） https://www.npa.go.jp/cybersecurity/pdf/300906_senryaku.pdf〔2021/5/19 確認〕
※ 127 警察庁：令和2年におけるサイバー空間をめぐる脅威の情勢等について https://www.npa.go.jp/publications/statistics/cybersecurity/data/R02_cyber_jousei.pdf〔2021/5/19 確認〕
※ 128 警察庁：治安の回顧と展望（令和2年版） https://www.npa.go.jp/bureau/security/publications/kaiko_to_tenbou/R2/kaitenR2.pdf〔2021/5/19 確認〕
※ 129 滋賀県警察：滋賀大学におけるサイバー攻撃共同対処訓練の実施 https://www.pref.shiga.lg.jp/police/seikatu/304024/terotaisaku/313411.html〔2021/5/19 確認〕
※ 130 日刊警察ニュース：富山県警察と愛知県警察でサイバー攻撃の共同対処訓練を実施 https://nikkankeisatsu.co.jp/news/201210-1.html〔2021/5/19 確認〕
※ 131 青森県警察：サイバーテロ対策担当者向け「共同対処訓練」 https://www.pi.jtua.or.jp/aomori/wp-content/uploads/sites/14/2020/12/8b34e36a9092699cbdaa4a4056090908.pdf〔2021/5/19 確認〕
※ 132 警察庁：情報セキュリティ対策ビデオ https://www.npa.go.jp/cyber/video/index.html〔2021/5/19 確認〕
※ 133 警察庁：スマートフォン決済サービスを利用した不正振替事犯に係る対策について https://www.npa.go.jp/cyber/policy/pdf/210318publicrelations.pdf〔2021/5/19 確認〕
※ 134 宮城県警察：宮城県サイバーセキュリティ協議会 https://www.police.pref.miyagi.jp/hp/cyber/kyougikai.html〔2021/5/19 確認〕
※ 135 警察庁：サイバー空間の脅威への対処に係る人材育成方針の改定について（通達） https://www.npa.go.jp/laws/notification/kanbou/kikaku/2019kikaku-h4.pdf〔2021/5/19 確認〕
※ 136 警察庁：令和2年度予算の概要 https://www.npa.go.jp/policies/budget/r2/r2tousyoyosan2.pdf〔2021/5/19 確認〕
※ 137 警察庁：電磁的記録の解析 https://www.npa.go.jp/joutuu/011.htm〔2021/5/19 確認〕
※ 138 警察庁：国際連携・協力 https://www.npa.go.jp/joutuu/013.htm〔2021/5/19 確認〕
※ 139 総務省・消費者庁・警察庁：給付金のサギ（詐欺）に注意!! https://www.npa.go.jp/bureau/soumu/corona/sagihigaibousi.pdf〔2021/5/19 確認〕
※ 140 山形県警察：山形県警察広報動画「サポート詐欺」にだまされないで!（その1）警告画面に表示された番号に電話をかけると https://www.youtube.com/watch?v=sWftPO_I3r8〔2021/5/19 確認〕
※ 141 サイバーセキュリティ政策会議：生活様式の変化等に伴うサイバー空間の新たな脅威に対処するための官民連携の更なる推進 https://www.npa.go.jp/cybersecurity/pdf/20210308_2.pdf〔2021/5/19 確認〕
※ 142 警察庁では、市販のウイルス対策ソフトでは検知できない不正プログラムを添付して、業務に関連した正当なものであるかのように装った電子メールを送信し、これを受信したコンピュータを不正プログラムに感染させる等して、情報の窃取を図るものを「標的型メール攻撃」として集計している。
※ 143 警察庁：サイバー攻撃に対する技術的対応 https://www.npa.go.jp/joutuu/012.htm〔2021/5/19 確認〕
※ 144 正式名称は「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」（https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r5.pdf〔2021/5/31 確認〕）。現在は、「電子政府推奨暗号リスト」「推奨候補暗号リスト」「運用監視暗号リスト」の三つのリストから構成される。
※ 145 CRYPTREC：2020年度 第2回 暗号技術検討会 資料3別添3 2020年度 暗号技術調査WG（暗号解析評価）活動報告 https://www.cryptrec.go.jp/report/cryptrec-mt-1021-2020.pdf〔2021/5/31 確認〕
※ 146 EdDSA（Edwards-curve Digital Signature Algorithm）：楕円曲線の一種であるエドワーズ曲線を用いたデジタル署名アルゴリズム。
※ 147 Shorの量子アルゴリズム：現代暗号の基盤である素因数分解や離散対数問題等を量子コンピュータによって効率的に解くアルゴリズム。
※ 148 IPA：暗号鍵管理ガイドライン https://www.ipa.go.jp/security/vuln/ckms.html〔2021/5/31 確認〕
※ 149 IPA：TLS暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～ https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html〔2021/5/31 確認〕
※ 150 Kyodo：Tokyo Olympics postponed until 2021 due to coronavirus pandemic https://english.kyodonews.net/news/2020/03/529743138975-breaking-news-japan-pm-abe-plans-talks-with-ioc-chief-bach-over-phone-tues-source.html〔2021/5/12 確認〕
※ 151 外務省：G7首脳テレビ会議 https://www.mofa.go.jp/mofaj/ecm/ec/page6_000378.html〔2021/5/12 確認〕
※ 152 外務省：G7外相会合の実施 https://www.mofa.go.jp/mofaj/press/release/press4_008389.html〔2021/5/12 確認〕
※ 153 首相官邸：新型コロナウイルス感染症に関する安倍内閣総理大臣記者会見 https://www.kantei.go.jp/jp/98_abe/statement/2020/0407kaiken.html〔2021/5/12 確認〕
※ 154 外務省：Biarritz Strategy for an Open, Free and Secure Digital Transformation https://www.mofa.go.jp/mofaj/files/000512682.pdf〔2021/5/12 確認〕
※ 155 外務省：第2回日米豪印外相会合 https://www.mofa.go.jp/mofaj/press/release/press6_000682.html〔2021/5/12 確認〕
※ 156 外務省：第23回日・ASEAN首脳会議「インド太平洋に関するASEAN・アウトルック（AOIP）協力についての第23回日アセアン首脳会議共同首脳声明」の発出 https://www.mofa.go.jp/mofaj/a_o/rp/page3_002923.html〔2021/5/12 確認〕
※ 157 外務省：日米豪印外相電話会談 https://www.mofa.go.jp/mofaj/press/release/press3_000427.html〔2021/5/12 確認〕
※ 158 LAWFARE：China's New Coast Guard Law and Implications for Maritime Security in the East and South China Seas https://www.lawfareblog.com/

chinas-new-coast-guard-law-and-implications-maritime-security-east-and-south-china-seas〔2021/5/12 確認〕
※ 159 United Nations: Open-ended working group https://www.un.org/disarmament/open-ended-working-group/〔2021/5/12 確認〕
※ 160 United Nations：Open-ended working group on developments in the field of information and telecommunications in the context of international security Final Substantive Report https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf〔2021/5/12 確認〕
※ 161 外務省：第 5 回日英サイバー協議の開催 https://www.mofa.go.jp/mofaj/press/release/press4_008287.html〔2021/5/12 確認〕
※ 162 外務省：日米安全保障委員会 https://www.mofa.go.jp/mofaj/na/st/page1_000942.html〔2021/5/12 確認〕
※ 163 外務省：日米首脳会談 https://www.mofa.go.jp/mofaj/na/na1/us/page1_000951.html〔2021/5/13 確認〕
※ 164 https://www.mofa.go.jp/mofaj/files/100181507.pdf〔2021/5/13 確認〕
※ 165 外務省：日 EU 首脳テレビ会議の開催 https://www.mofa.go.jp/mofaj/erp/ep/page4_005157.html〔2021/5/12 確認〕
※ 166 https://aseanregionalforum.asean.org/〔2021/5/12 確認〕
※ 167 外務省：サイバーセキュリティに関する ARF 会期間会合のための第 6 回専門家会合の開催（結果） https://www.mofa.go.jp/mofaj/press/release/press3_000409.html〔2021/5/12 確認〕
※ 168 2018 年 12 月、第 73 回国連総会決議（A/RES/73/266）に基づき、国際安全保障の文脈におけるサイバー空間での責任ある国家の行動の進展に関して 25 ヵ国からの専門家（25 名）による専門的な議論の場として、国連のもとに立ち上がった会合。2019 年 12 月に第 1 回会合を開催し、全部で 4 回の本会合を経て 2021 年の国連総会において報告書を提出することとなっている。
※ 169 経済産業省：「インド太平洋地域向け日米産業制御システムサイバーセキュリティウィーク」を実施しました https://www.meti.go.jp/press/2020/03/20210315001/20210315001.html〔2021/5/12 確認〕
※ 170 The MITRE Corporation は 1958 年創立の非営利民間企業で、米国連邦政府機関の出資を受けた研究開発、及び成果の民間移転を推進している。 https://www.mitre.org/〔2021/5/12 確認〕
※ 171 慶應義塾大学：第 10 回サイバーセキュリティ国際シンポジウム https://symp.cysec-lab.keio.ac.jp/2020oct/program-j.html〔2021/5/12 確認〕
※ 172 日本経済新聞／株式会社日経 BP：サイバー・イニシアチブ東京 2020 https://project.nikkeibp.co.jp/event/2020z1124cit/〔2021/5/12 確認〕
※ 173 BBC：Trump declares national emergency over coronavirus https://www.bbc.com/news/world-us-canada-51882381〔2021/5/13 確認〕
※ 174 THE WHITE HOUSE：A Letter on the Continuation of the National Emergency Concerning the Coronavirus Disease 2019 (COVID-19) Pandemic https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/24/a-letter-on-the-continuation-of-the-national-emergency-concerning-the-coronavirus-disease-2019-covid-19-pandemic〔2021/5/13 確認〕
※ 175 AFP：トランプ氏が中国批判、故意ならパンデミックの「報いを受けるべき」 https://www.afpbb.com/articles/-/3279279〔2021/5/13 確認〕
※ 176 AFP：新型コロナ、武漢の研究所が発生源の可能性確信＝トランプ米大統領 https://jp.reuters.com/article/health-coronavirus-usa-idJPKBN22C3ZE〔2021/5/13 確認〕
※ 177 The New York Times：Wuhan, Center of Coronavirus Outbreak, Is Being Cut Off by Chinese Authorities https://www.nytimes.com/2020/01/22/world/asia/china-coronavirus-travel.html〔2021/5/13 確認〕
※ 178 IPA：情報セキュリティ白書 2020 https://www.ipa.go.jp/security/publications/hakusyo/2020.html〔2021/5/13 確認〕
※ 179 THE WHITE HOUSE：Executive Order on America's Supply Chains https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/〔2021/5/13 確認〕
※ 180 時事ドットコム：米、供給網で脱中国依存 日本など同盟国と連携 https://www.jiji.com/jc/article?k=2021022400885&g=int〔2021/5/13 確認〕
※ 181 CISA：CISA INSIGHTS Risk Management for Novel Coronavirus (COVID-19) https://www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf〔2021/5/13 確認〕
※ 182 FBI：Protect Your Wallet—and Your Health—from Pandemic Scammers https://www.fbi.gov/news/stories/protect-yourself-from-covid-19-scams-040620〔2021/5/13 確認〕
※ 183 CISA：Alert (AA20-099A) COVID-19 Exploited by Malicious Cyber Actors https://us-cert.cisa.gov/ncas/alerts/aa20-099a〔2021/5/13 確認〕
※ 184 CISA：Telework Guidance and Resources https://www.cisa.gov/telework〔2021/5/13 確認〕
※ 185 CISA：CISA RELEASES VERSION 3.0 OF GUIDANCE ON ESSENTIAL CRITICAL INFRASTRUCTURE WORKERS DURING COVID-19 https://www.cisa.gov/news/2020/04/17/cisa-releases-version-30-guidance-essential-critical-infrastructure-workers-during〔2021/5/13 確認〕
なお、同ガイダンスは同年 10 月に第 4 版が公開された。
※ 186 CISA&FBI：People's Republic of China (PRC) Targeting of COVID-19 Research Organizations https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf〔2021/5/13 確認〕
※ 187 CISA：Alert (AA20-225A) Malicious Cyber Actor Spoofing COVID-19 Loan Relief Webpage via Phishing Emails https://us-cert.cisa.gov/ncas/alerts/aa20-225a〔2021/5/13 確認〕
※ 188 BUSINESS INSIDER：US accuses Russia of spreading conspiracies about the Wuhan coronavirus, including that it's a CIA biological weapon https://www.businessinsider.com/us-officials-claim-russian-coronavirus-disinformation-campaign-2020-2?r=US&IR=T〔2021/5/13 確認〕
※ 189 WHO：Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation〔2021/5/13 確認〕
※ 190 CISA：COVID 19 DISINFORMATION TOOLKIT https://www.cisa.gov/publication/covid-19-disinformation-toolkit〔2021/5/13 確認〕
※ 191 Military.com：Russia and China Are Spreading Lies About Coronavirus, Pentagon Says https://www.military.com/daily-news/2020/04/10/russia-and-china-are-spreading-lies-about-coronavirus-pentagon-says.html〔2021/5/13 確認〕
※ 192 DoD：CORONAVIRUS:RUMOR CONTROL https://www.defense.gov/explore/spotlight/coronavirus/rumor-control/〔2021/5/13 確認〕
※ 193 Military.com：Navy Debunks Top 10 COVID-19 Vaccine Myths https://www.military.com/daily-news/2021/03/04/navy-debunks-top-10-covid-19-vaccine-myths.html〔2021/5/13 確認〕
※ 194 以下は 2021 年 4 月 2 日の事例である。
POLYGRAPH.info：Coronavirus: The Infodemic - April 2 https://www.polygraph.info/a/31183802.html〔2021/5/13 確認〕
※ 195 Pew Research Center：A Year of U.S. Public Opinion on the Coronavirus Pandemic https://www.pewresearch.org/2021/03/05/a-year-of-u-s-public-opinion-on-the-coronavirus-pandemic/〔2021/5/13 確認〕
※ 196 CISA：CISA RELEASES 5G STRATEGY FOR SECURE AND RESILIENT CRITICAL INFRASTRUCTURE https://www.cisa.gov/news/2020/08/24/cisa-releases-5g-strategy-secure-and-resilient-critical-infrastructure〔2021/5/13 確認〕
※ 197 Bloomberg：Trump Targets Ant's Alipay, WeChat Pay in Latest App Bans https://www.bloomberg.com/news/articles/2021-01-05/trump-order-would-ban-transactions-with-chinese-payment-apps〔2021/5/13 確認〕
※ 198 ZDNet：Trump decrees American cloud providers need to maintain records on foreign clients https://www.zdnet.com/article/trump-decrees-american-cloud-providers-need-to-maintain-records-on-foreign-clients/〔2021/5/13 確認〕
※ 199 CISA：ICT SCRM TASK FORCE: THREAT SCENARIOS REPORT https://www.cisa.gov/publication/ict-scrm-task-force-threat-scenarios-report〔2021/5/13 確認〕
※ 200 COVINGTON：CISA Information and Communications Technology Supply Chain Risk Management Task Force Releases New Guidance on Security Resiliency https://www.globalpolicywatch.com/2020/05/cisa-information-and-communications-technology-supply-chain-risk-management-task-force-releases-new-guidance-on-security-resiliency/〔2021/5/13 確認〕
※ 201 CISA：MITIGATING ICT SUPPLY CHAIN RISKS WITH QUALIFIED BIDDER AND MANUFACTURER LISTS https://

www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Qualified-Bidders-Lists_508.pdf〔2021/5/13 確認〕
※ 202 CISA：ICT SCRM TASK FORCE: LESSONS LEARNED DURING THE COVID-19 PANDEMIC REPORT https://www.cisa.gov/publication/ict-supply-chain-lessons-learned-covid-19〔2021/5/13 確認〕
※ 203 Office of the Under Secretary of Defense for Acquisition & Sustainment：CYBERESECURITY MATURITY MODDEL CERTIFICATION (CMMC) https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf〔2021/5/13 確認〕
※ 204 CMMC-AB：https://cmmcab.org/〔2021/5/13 確認〕
※ 205 OUSD A&S：Cybersecurity Maturity Model Certification Pilots for Fiscal Year 2021 https://www.acq.osd.mil/news/archive/2020/cybersecurity-maturity-model-certification-pilots-for-fiscal-year-2021.html〔2021/5/13 確認〕
※ 206 FEDSCOOP：CMMC is under an internal DOD review https://www.fedscoop.com/dod-cmmc-review-new-administration/〔2021/5/13 確認〕
※ 207 FireEye, Inc.：Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html〔2021/5/13 確認〕
※ 208 cyber.dhc.org：Emergency Directive 21-01 https://cyber.dhs.gov/ed/21-01/#supplemental-guidance-v3〔2021/5/13 確認〕
※ 209 FIREEYE：Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452 https://www.fireeye.com/blog/threat-research/2021/01/remediation-and-hardening-strategies-for-microsoft-365-to-defend-against-unc2452.html〔2021/5/13 確認〕
※ 210 The New York Times：As Understanding of Russian Hacking Grows, So Does Alarm https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html〔2021/5/13 確認〕
※ 211 arstechnica：SolarWinds hack that breached gov networks poses a “grave risk” to the nation https://arstechnica.com/information-technology/2020/12/feds-warn-that-solarwinds-hackers-likely-used-other-ways-to-breach-networks/〔2021/5/13 確認〕
※ 212 ITMediaビジネスオンライン：大手企業が次々と被害に ソーラーウィンズから連鎖した「サプライチェーン攻撃」の脅威 https://www.itmedia.co.jp/business/articles/2012/24/news031_3.html〔2021/5/13 確認〕
※ 213 CISA：JOINT STATEMENT BY THE FEDERAL BUREAU OF INVESTIGATION (FBI), THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), AND THE NATIONAL SECURITY AGENCY (NSA) https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure〔2021/5/13確認〕
※ 214 The White House：FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/〔2021/5/13 確認〕
※ 215 FCW：White House sanctions Russia over SolarWinds campaign, election interference https://fcw.com/articles/2021/04/15/katz-russia-cyber-sanctions.aspx〔2021/5/13 確認〕
※ 216 Microsoft Security Response Center：On-Premises Exchange Server Vulnerabilities Resource Center – updated March 25, 2021 https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/〔2021/5/13 確認〕
※ 217 Microsoft Security Response Center：HAFNIUM targeting Exchange Servers with 0-day exploits https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/〔2021/5/13 確認〕
※ 218 KrebsonSecurity：At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft’s Email Software https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/〔2021/5/13 確認〕
※ 219 CISA：CISA Issues Emergency Directive and Alert on Microsoft Exchange Vulnerabilities https://us-cert.cisa.gov/ncas/current-activity/2021/03/03/cisa-issues-emergency-directive-and-alert-microsoft-exchange〔2021/5/13 確認〕
※ 220 The White House：Statements by Press Secretary Jen Psaki & Deputy National Security Advisor for Cyber Anne Neuberger on Microsoft Exchange Vulnerabilities UCG https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/17/statements-by-press-secretary-jen-psaki-deputy-national-security-advisor-for-cyber-anne-neuberger-on-microsoft-exchange-vulnerabilities-ucg/〔2021/5/13 確認〕
※ 221 The Wall Street Journal：Suspected China Hack of Microsoft Shows Signs of Prior Reconnaissance https://www.wsj.com/articles/suspected-china-hack-of-microsoft-shows-signs-of-prior-reconnaissance-11617800400〔2021/5/13 確認〕
※ 222 ZDNet：Exchange Server attacks: Microsoft shares intelligence on post-compromise activities https://www.zdnet.com/article/exchange-server-attacks-microsoft-shares-intelligence-on-post-compromise-activities/〔2021/5/13 確認〕
※ 223 The New York Times：Cyberattack Forces a Shutdown of a Top U.S. Pipeline https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html〔2021/5/26 確認〕
※ 224 The New York Times：The F.B.I. confirms that DarkSide, a ransomware group, was behind the hack of a major U.S. pipeline. https://www.nytimes.com/2021/05/10/us/politics/dark-side-hack.html〔2021/5/26 確認〕
※ 225 WIRED：DarkSide Ransomware Hit Colonial Pipeline—and Created an Unholy Mess https://www.wired.com/story/darkside-ransomware-colonial-pipeline-response/〔2021/5/26 確認〕
※ 226 CISA：DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks https://us-cert.cisa.gov/ncas/alerts/aa21-131a〔2021/5/26 確認〕
※ 227 Forbes：Colonial Pipeline Restarts Operations As Biden Seeks To Protect Government From Cyber Attacks https://www.forbes.com/sites/edwardsegal/2021/05/12/colonial-pipeline-restarts-operations-as-biden-seeks-to-protect-government-from-cyber-attacks/?sh=17093d217814〔2021/5/26 確認〕
※ 228 The New York Times：Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html〔2021/5/26 確認〕
※ 229 The Wall Street Journal：Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636〔2021/5/26 確認〕
※ 230 The White House：Executive Order on Improving the Nation’s Cybersecurity https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/〔2021/5/26 確認〕
※ 231 The New York Times：Biden Wins Presidency, Ending Four Tumultuous Years Under Trump https://www.nytimes.com/2020/11/07/us/politics/biden-election.html〔2021/5/13 確認〕
※ 232 日本経済新聞：米、政権移行へ本格始動 トランプ氏が引き継ぎ容認 https://www.nikkei.com/article/DGXMZO66600380U0A121C2MM8000/〔2021/5/13 確認〕
※ 233 朝日新聞：トランプ氏側、最高裁で２度目の敗訴 大統領選不正訴訟 https://www.asahi.com/articles/ASNDD5HP6NDDUHBI00K.html〔2021/5/13 確認〕
最終的には 2021 年３月８日の連邦最高裁判決で Wisconsin 州の選挙に関する提訴が却下され、Trump 陣営の完全敗訴が確定した。
Reuters：U.S. Supreme Court dumps last of Trump's election appeals https://www.reuters.com/article/us-usa-court-election-idUSKBN2B01LE〔2021/5/13 確認〕
※ 234 The Washington Post：How one of America’s ugliest days unraveled inside and outside the Capitol https://www.washingtonpost.com/nation/interactive/2021/capitol-insurrection-visual-timeline/?utm_campaign=wp_graphics&utm_medium=social&utm_source=twitter〔2021/5/13 確認〕
※ 235 The New York Times：After Pro-Trump Mob Storms Capitol, Congress Confirms Biden’s Win https://www.nytimes.com/2021/01/06/us/politics/congress-gop-subvert-election.html〔2021/5/13 確認〕
※ 236 REUTERS：Reuters launches fact-checking initiative to identify misinformation, in partnership with Facebook https://www.reuters.com/article/rpb-fbfactchecking/reuters-launches-fact-checking-initiative-to-identify-misinformation-in-partnership-with-facebook-idUSKBN2061TG〔2021/5/13 確認〕
※ 237 REUTERS：Twitter fact-checks Trump tweet for the first

time https://www.reuters.com/article/us-twitter-trump-idUSKBN232389〔2021/5/13 確認〕
※ 238 The New York Times：Twitter Has Labeled 38% of Trump's Tweets Since Tuesday https://www.nytimes.com/2020/11/05/technology/donald-trump-twitter.html〔2021/5/13 確認〕
※ 239 The Washington Post: Twitter bans Trump's account, citing risk of further violence https://www.washingtonpost.com/technology/2021/01/08/twitter-trump-dorsey/〔2021/5/13 確認〕
※ 240 NHK：ツイッター アカウント永久停止の波紋 https://www.nhk.or.jp/ohayou/biz/20210128/index.html〔2021/5/13 確認〕
※ 241 Newsweek:Donald Trump's Twitter Ban Concerns World Leaders, Officials https://www.newsweek.com/donald-trump-twitter-ban-concerns-world-leaders-officials-1560771〔2021/5/13 確認〕
※ 242 WIRED：What happened to the deepfake threat to the US election? https://wired.me/business/what-happened-to-the-deepfake-threat-to-the-us-election/〔2021/5/13 確認〕
※ 243 GovTrack.us：S. 1790 (116th):National Defense Authorization Act for Fiscal Year 2020 https://www.govtrack.us/congress/bills/116/s1790〔2021/5/13 確認〕
※ 244 TechCrunch：Biden's cybersecurity dream team takes shape https://techcrunch.com/2021/04/12/bidens-cybersecurity-dream-team-takes-shape/〔2021/5/13 確認〕
※ 245 BBC：Brexit:UK leaves the European Union https://www.bbc.com/news/uk-politics-51333314〔2021/5/17 確認〕
※ 246 日本経済新聞：英国との FTA 暫定適用、EU 加盟国が承認 大使級会合 https://www.nikkei.com/article/DGXZQODB289LU0Y0A221C2000000/〔2021/5/17 確認〕
※ 247 The EU-UK Trade and Cooperation Agreement：TRADE AND COOPERATION AGREEMENT BETWEEN THE EUROPEAN UNION AND THE EUROPEAN ATOMIC ENERGY COMMUNITY, OF THE ONE PART, AND THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND, OF THE OTHER PART https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948119/EU-UK_Trade_and_Cooperation_Agreement_24.12.2020.pdf〔2021/5/17 確認〕
※ 248 POLITICO：European Parliament ratifies post-Brexit trade deal https://www.politico.eu/article/european-parliament-post-brexit-trade-deal-ratification/〔2021/5/17 確認〕
※ 249 European Council：EU-UK negotiations on the future relationship https://www.consilium.europa.eu/en/policies/eu-uk-negotiations-on-the-future-relationship/#:~:text=Negotiations%20on%20the%20future%20partnership,provisionally%20from%201%20January%202021.〔2021/5/17 確認〕
※ 250 日本経済新聞：英 EU、通商協定で合意 関税ゼロ維持へ https://www.nikkei.com/article/DGXZQOGM00090_09122020000000/〔2021/5/17 確認〕
※ 251 BBC：Brexit trade deal: What does it mean for fishing? https://www.bbc.com/news/46401558〔2021/5/17 確認〕
※ 252 Institute for Government：UK–EU future relationship: level playing field https://www.instituteforgovernment.org.uk/explainers/future-relationship-level-playing-field〔2021/5/17 確認〕
※ 253 JETRO：英国の EU 離脱後の通商・協力協定交渉の争点と進捗状況 https://www.jetro.go.jp/ext_images/world/europe/uk/referendum/brexit_outline_20210104.pdf〔2021/5/17 確認〕
※ 254 The Law Society：Personal data flows from the EU/EEA to the UK after Brexit https://www.lawsociety.org.uk/topics/brexit/eu-data-flows-after-brexit〔2021/5/17 確認〕
※ 255 European Commission：COMMISSION IMPLEMENTING DECISION of XXX pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom https://ec.europa.eu/info/sites/default/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_19_feb_2020.pdf〔2021/5/17 確認〕
※ 256 Data Protection Report：EDPB cautiously welcomes UK adequacy finding https://www.dataprotectionreport.com/2021/04/edpb-cautiously-welcomes-uk-adequacy-finding/〔2021/5/17 確認〕
※ 257 European Data Protection Board：EDPB Opinions on draft UK adequacy decisions https://edpb.europa.eu/news/news/2021/edpb-opinions-draft-uk-adequacy-decisions_en〔2021/5/17 確認〕
※ 258 European Commission：The EU-UK Security of Information Agreement https://ec.europa.eu/info/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement/eu-uk-security-information-agreement_en#:~:text=If%20a%20joint%20security%20threat,EU%20and%20a%20third%20country.〔2021/5/17 確認〕
※ 259 BBC：Coronavirus: Italy extends emergency measures nationwide https://www.bbc.com/news/world-europe-51810673〔2021/5/17 確認〕
※ 260 France24：Macron announces 15-day lockdown in French 'war' on coronavirus https://www.france24.com/en/20200316-live-france-s-macron-addresses-nation-amid-worsening-coronavirus-outbreak〔2021/5/17 確認〕
※ 261 France24：Germany closes public spaces, bans religious gatherings in virus clampdown https://www.france24.com/en/20200316-germany-closes-public-spaces-bans-religious-gatherings-in-virus-clampdown〔2021/5/17 確認〕
※ 262 The Guardian：UK coronavirus: Boris Johnson announces strict lockdown across country – as it happened https://www.theguardian.com/politics/live/2020/mar/23/uk-coronavirus-live-news-latest-boris-johnson-minister-condemns-people-ignoring-two-metre-distance-rule-in-parks-as-very-selfish〔2021/5/17 確認〕
※ 263 GOV.UK：Coronavirus（Covid-19）in the UK https://coronavirus.data.gov.uk/〔2021/5/17 確認〕
※ 264 ENISA：Tips for cybersecurity when working from home https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home〔2021/5/17 確認〕
※ 265 ENISA：Tips for cybersecurity when buying and selling online https://www.enisa.europa.eu/news/enisa-news/tips-for-cybersecurity-when-buying-and-selling-online〔2021/5/17 確認〕
※ 266 ENISA：Understanding and dealing with phishing during the COVID-19 pandemic https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic〔2021/5/17 確認〕
※ 267 ENISA：Tips for selecting and using online communication tools https://www.enisa.europa.eu/news/enisa-news/tips-for-selecting-and-using-online-communication-tools〔2021/5/17 確認〕
※ 268 European Commission：European Democracy Action Plan: making EU democracies stronger https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250〔2021/5/17 確認〕
※ 269 European Commission：Code of Practice on Disinformation https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation〔2021/5/17 確認〕
※ 270 European Commission：Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital〔2021/5/17 確認〕
※ 271 European Commission：The Digital Markets Act: ensuring fair and open digital markets https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en〔2021/5/17 確認〕
※ 272 European Data Protection Board：Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en〔2021/5/17 確認〕
※ 273 European Data Protection Board：Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf〔2021/5/17 確認〕
※ 274 European Data Protection Board：Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf〔2021/5/17 確認〕
※ 275 東洋経済：話題の「ワクチン接種証明書」とはいったい何か https://toyokeizai.net/articles/-/426924〔2021/5/17 確認〕
※ 276 European Commission：Coronavirus: Commission proposes a Digital Green Certificate https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1181〔2021/5/17 確認〕
※ 277 The Office of Privacy Commissioner：Covid-19 vaccine passports not immune to privacy concerns https://privacy.org.nz/blog/covid-19-vaccine-passports-not-immune-to-privacy-

concerns/〔2021/5/17 確認〕
※ 278 The Local：Italy to introduce new Covid 'pass' for travel in high-risk zones https://www.thelocal.it/20210420/covid-19-italy-to-introduce-new-vaccine-pass-for-travel-in-high-risk-zones/〔2021/5/17 確認〕
※ 279 European Data Protection Board：Italian DPA：Major Critical Issues for Vaccination Pass https://edpb.europa.eu/news/national-news/2021/italian-dpa-major-critical-issues-vaccination-pass_en〔2021/5/17 確認〕
※ 280 Council of Europe：Vaccine passports：Council of Europe issues guidance to governments to safeguard human rights https://www.coe.int/en/web/portal/-/vaccine-passports-council-of-europe-issues-guidance-to-governments-to-safeguard-human-rights〔2021/5/17 確認〕
※ 281 The New York Times：E.U. Court Strikes Down Trans-Atlantic Data Transfer Pact https://www.nytimes.com/2020/07/16/business/eu-data-transfer-pact-rejected.html〔2021/5/17 確認〕
※ 282 日本経済新聞：BA に GDPR 制裁金 27 億円　顧客情報流出、コロナで減 額 https://www.nikkei.com/article/DGXMZO065136230X11C20A0000000/〔2021/5/17 確認〕
ICO：ICO fines British Airways £20m for data breach affecting more than 400,000 customers https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/〔2021/5/17 確認〕
※ 283 DLA Piper：Privacy Matters DLA Piper's Global Privacy and Data Protection Resource https://blogs.dlapiper.com/privacymatters/dla-piper-gdpr-fines-and-data-breach-survey-january-2021/〔2021/5/17 確認〕
ZDNet：GDPR 制裁金、前年比で 39%増 -- さらに高額化する可能性も https://japan.zdnet.com/article/35165383/〔2021/5/17 確認〕
※ 284 GARANTE：Operatori telefonici: continua l' attività di controllo del Garante privacy, sanzione a Wind per 17 milioni di euro e a Iliad per 800 mila euro https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9435901#english〔2021/5/17 確認〕
DataGuidance：Italy: Garante fines Wind Tre €16.7M for unlawful direct marketing practices, highlights consent violations https://www.dataguidance.com/news/italy-garante-fines-wind-tre-%E2%82%AC167m-unlawful-direct-marketing-practices-highlights-consent〔2021/5/17 確認〕
※ 285 European Data Protection Board：Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en〔2021/5/17 確認〕
※ 286 TESSIAN：14 Biggest GDPR Fines of 2020 and 2021 (So Far) https://www.tessian.com/blog/biggest-gdpr-fines-2020/〔2021/5/17 確認〕
※ 287 ICO：ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/〔2021/5/17 確認〕
※ 288 European Commission：Shaping Europe's digital future https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade〔2021/5/17 確認〕
※ 289 European Commission：Shaping Europe's digital future https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies〔2021/5/17 確認〕
※ 290 European Commission：Commission welcomes political agreement on the Cybersecurity Competence Centre and Network https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2384〔2021/5/17 確認〕
※ 291 ENISA：ENISA welcomes the European Commission proposal to create a network of Cybersecurity Competence Centres https://www.enisa.europa.eu/news/enisa-news/enisa-welcomes-the-european-commission-proposal-to-create-a-network-of-cybersecurity-competence-centres〔2021/5/17 確認〕
※ 292 ENISA：Procurement Guidelines for Cybersecurity in Hospitals https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services〔2021/5/17 確認〕
※ 293 ENISA：Securing Cloud Services for Health https://www.enisa.europa.eu/news/enisa-news/securing-cloud-services-for-health〔2021/5/17 確認〕
※ 294 Health Advances, LLC：Reflections on Healthcare & Life Sciences Innovation https://healthadvancesblog.com/2020/03/24/e-health-in-france/〔2021/5/17 確認〕
※ 295 ENISA：Artificial Intelligence Cybersecurity Challenges https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges〔2021/5/17 確認〕
※ 296 ENISA：Updated ENISA 5G Threat Landscape Report to Enhance 5G Security https://www.enisa.europa.eu/news/enisa-news/updated-enisa-5g-threat-landscape-report-to-enhance-5g-security〔2021/5/17 確認〕
※ 297 https://www.3gpp.org/〔2021/5/17 確認〕
※ 298 ENISA：Cybersecurity for 5G: ENISA Releases Report on Security Controls in 3GPP https://www.enisa.europa.eu/news/enisa-news/cybersecurity-for-5g-enisa-releases-report-on-security-controls-in-3gpp〔2021/5/17 確認〕
※ 299 TechCrunch：UK U-turns on Huawei and 5G, giving operators until 2027 to rip out existing kit https://techcrunch.com/2020/07/14/uk-u-turns-on-huawei-and-5g-giving-operators-until-2027-to-rip-out-existing-kit/〔2021/5/17 確認〕
※ 300 GOV.UK：New telecoms security law to protect UK from cyber threats https://www.gov.uk/government/news/new-telecoms-security-law-to-protect-uk-from-cyber-threats〔2021/5/17 確認〕
※ 301 JETRO：IT セキュリティー法 2.0 を閣議決定、特定企業の排除は明示せず https://www.jetro.go.jp/biznews/2020/12/947abab1c5dedc9d.html〔2021/5/17 確認〕
※ 302 European Council on Foreign Relations：What Germany's new cyber security law means for Huawei, Europe, and NATO https://ecfr.eu/article/what-germanys-new-cyber-security-law-means-for-huawei-europe-and-nato/〔2021/5/17 確認〕
※ 303 Department of Home Affairs：Australia's Cyber Security Strategy 2020 https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy〔2021/5/19 確認〕
※ 304 https://www.cyber.gov.au/〔2021/5/19 確認〕
※ 305 https://www.csa.gov.sg/singcert〔2021/5/19 確認〕
※ 306 https://www.csa.gov.sg/〔2021/5/19 確認〕
※ 307 https://www.csa.gov.sg/news/publications/safer-cyberspace-masterplan〔2021/5/19 確認〕
※ 308 サイバー衛生：サイバー攻撃の原因となり得る問題を取り除くため、ソフトウェアや OS へのパッチ適用、ネットワーク設定の見直し、パスワード設定の強化等の予防的な対策を推進し、サイバー空間をセキュアに保つこと。
※ 309 https://www.nacsa.gov.my/〔2021/5/19 確認〕
※ 310 NACSA：Malaysia Cyber Security Strategy 2020-2024 https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf〔2021/5/19 確認〕
※ 311 https://www.cybersecurity.my/en/index.html〔2021/5/19 確認〕
※ 312 https://www.oic-cert.org/en/〔2021/5/19 確認〕
※ 313 https://www.boho.or.kr/krcert/intro.do〔2021/5/19 確認〕
※ 314 https://www.auscert.org.au/〔2021/5/19 確認〕
※ 315 https://www.cert-in.org.in/〔2021/5/19 確認〕
※ 316 https://www.cert.gov.lk/〔2021/5/19 確認〕
※ 317 KrCERT/CC：[INFORMATION] Cyber Threat Signal 2021 https://www.boho.or.kr/krcert/publicationView.do?bulletin_writing_sequence=35833〔2021/5/19 確認〕
※ 318 https://www.apcert.org/〔2021/5/19 確認〕
※ 319 https://www.cert.gov.to/〔2021/5/19 確認〕
※ 320 https://www.ncert.gov.ph/〔2021/5/19 確認〕
※ 321 APCERT：About TSUBAME Working Group https://www.apcert.org/about/structure/tsubame-wg/index.html〔2021/5/19 確認〕
※ 322 APCERT：APCERT CYBER DRILL 2020 "BANKER DOUBLES DOWN ON MINER" https://www.apcert.org/documents/pdf/APCERT_Drill2020_Press%20Release.pdf〔2021/5/19 確認〕
※ 323 APCERT：Documents https://www.apcert.org/documents/index.html〔2021/5/19 確認〕
※ 324 https://www.cert.org.cn/publish/english/index.html〔2021/5/19 確認〕
※ 325 https://ajccbc.org/index.html〔2021/5/19 確認〕
※ 326 AJCCBC：ASEAN-Japan Cybersecurity Capacity Building Centre https://www.facebook.com/permalink.php?story_fbid=209846830824990&id=107358564407151〔2021/5/19 確認〕
※ 327 JPCERT/CC：JPCERT/CC インシデント報告対応レポート

2020 年 7 月 1 日～ 2020 年 9 月 30 日　https://www.jpcert.or.jp/pr/2020/IR_Report20201015.pdf〔2021/5/19 確認〕
※ 328 NIST：NICE eNewsletter Winter 2020-21 Industry Spotlight　https://www.nist.gov/itl/applied-cybersecurity/nice/nice-enewsletter-winter-2020-21-industry-spotlight〔2021/5/11 確認〕
※ 329 https://www.nri-secure.co.jp/download/insight2020-report〔2021/5/11 確認〕
※ 330 経団連：経団連サイバーセキュリティ経営宣言　https://www.keidanren.or.jp/policy/2018/018.html〔2021/5/11 確認〕
※ 331 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/007_03_00.pdf〔2021/5/11 確認〕
※ 332 https://www.nisc.go.jp/conference/cs/jinzai/dai14/pdf/14shiryou02.pdf〔2021/5/11 確認〕
※ 333 経済産業省：DX レポート ～ IT システム「2025 年の崖」克服と DX の本格的な展開～　https://www.meti.go.jp/shingikai/mono_info_service/digital_transformation/20180907_report.html〔2021/5/11 確認〕
※ 334 株式会社デンソー：完全子会社 (株式会社デンソー IT ソリューションズ) との吸収合併 (簡易合併・略式合併) に関するお知らせ　https://www.denso.com/jp/ja/news/newsroom/2020/20200706-02/〔2021/5/11 確認〕
※ 335 株式会社大和証券グループ本社・株式会社大和総研ホールディングス・株式会社大和総研・株式会社大和総研ビジネス・イノベーション：株式会社大和総研ホールディングス、株式会社大和総研及び株式会社大和総研ビジネス・イノベーションの合併について　https://www.dir.co.jp/release/2020/2020122201.html〔2021/5/11 確認〕
※ 336 住友化学株式会社：完全子会社の吸収合併（簡易合併・略式合併）に関するお知らせ　https://www.sumitomo-chem.co.jp/news/files/docs/20210226_5.pdf〔2021/5/11 確認〕
※ 337 https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf
※ 338 https://www.nisc.go.jp/conference/cs/jinzai/dai14/pdf/14shiryou0105.pdf〔2021/5/11 確認〕
※ 339 IPA:ITSS+（プラス）・IT スキル標準（ITSS）・情報システムユーザースキル標準（UISS）関連情報　https://www.ipa.go.jp/jinzai/itss/itssplus.html
※ 340 https://www.ipa.go.jp/icscoe/program/middle/strategic_management/index.html〔2021/5/11 確認〕
※ 341 東京工業大学：サイバーセキュリティ経営戦略コース受講生募集のご案内　https://www.titech.ac.jp/company/news/pdf/info-26604.pdf〔2021/5/11 確認〕
※ 342 情報セキュリティ大学院大学：DX 推進者対象 DX with Cybersecurity 3 日間教育コース　https://www.iisec.ac.jp/event/pdf/20201118seminar_pamp.pdf〔2021/5/11 確認〕
※ 343 https://www.meti.go.jp/policy/netsecurity/downloadfiles/tebikigaiyou1.1.pdf〔2021/5/11 確認〕
※ 344 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf〔2021/5/11 確認〕
※ 345 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf〔2021/5/11 確認〕
※ 346 NISC：（事務局資料）政策議論のための補助フレームワーク　https://www.nisc.go.jp/conference/cs/jinzai/dai14/pdf/14sankou01.pdf〔2021/5/11 確認〕
※ 347 重要インフラ：他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもので、重要インフラ分野として指定する分野。具体的には、「情報通信」「金融」「航空」「空港」「鉄道」「電力」「ガス」「政府・行政サービス（地方公共団体を含む）」「医療」「水道」「物流」「化学」「クレジット」及び「石油」の 14 分野。
NISC：重要インフラの情報セキュリティ対策に係る第 4 次行動計画　https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r2.pdf〔2021/05/19 確認〕
※ 348 IPA：中核人材育成プログラム修了者コミュニティ「叶会（かなえかい）」　https://www.ipa.go.jp/icscoe/program/core_human_resource/icscoe_alumni.html〔2021/05/19 確認〕
※ 349 IPA：情報処理安全確保支援士（登録セキスペ）になるには　https://www.ipa.go.jp/siensi/toberiss/index.html〔2021/05/19 確認〕
※ 350 IPA:管理監督者向けプログラム　製造・生産分野向けセキュリティ教育プログラム　https://www.ipa.go.jp/icscoe/program/middle/seizo-seisan/2020.html〔2021/05/19 確認〕
※ 351 IPA：責任者向けプログラム 業界別サイバーレジリエンス強化演習（CyberREX）　https://www.ipa.go.jp/icscoe/program/short/specific_industries/2020.html〔2021/05/19 確認〕
※ 352 IPA：戦略マネジメント系セミナー　https://www.ipa.go.jp/icscoe/program/middle/strategic_management/2020.html〔2021/05/19 確認〕
※ 353 IPA：実務者向けプログラム 制御システム向けサイバーセキュリティ演習　https://www.ipa.go.jp/icscoe/program/short/icssec/2020.html〔2021/05/19 確認〕
※ 354 CBT（Computer Based Testing）方式：試験会場に設置されたコンピュータを利用して実施する試験方式のこと。受験者はコンピュータに表示された試験問題に対して、マウスやキーボードを用いて解答する。
※ 355 IPA：情報処理技術者試験 情報処理安全確保支援士試験 統計資料 令和 2 年度試験全試験区分版　https://www.jitec.ipa.go.jp/1_07toukei/toukei_r02o.pdf〔2021/6/21 確認〕
※ 356 IPA：情報処理技術者試験 情報処理安全確保支援士試験 統計資料 令和 2 年度試験全試験区分版　https://www.jitec.ipa.go.jp/1_07toukei/toukei_r02o.pdf〔2021/6/21 確認〕
※ 357 IPA：国家資格「情報処理安全確保支援士」2021 年 4 月 1 日付登録者 804 名の内訳を公開しました　https://www.ipa.go.jp/siensi/data/20210401newriss.html〔2021/5/19 確認〕
※ 358 経済産業省：情報処理安全確保支援士特定講習　https://www.meti.go.jp/policy/it_policy/jinzai/tokutei.html〔2021/5/19 確認〕
※ 359 経済産業省：情報処理安全確保支援士特定講習一覧　https://www.meti.go.jp/press/2020/03/20210331004/20210331004-1.pdf〔2021/5/19 確認〕
※ 360 IPA：情報処理安全確保支援士（登録セキスペ）の受講する講習について　https://www.ipa.go.jp/siensi/lecture/index.html〔2021/5/19 確認〕
※ 361 IPA：国家資格「情報処理安全確保支援士」制度の仕組み　https://www.ipa.go.jp/files/000088283.pdf〔2021/5/19 確認〕
※ 362 IPA：セキュリティ・キャンプ全国大会 2020 オンライン　ホーム　https://www.ipa.go.jp/jinzai/camp/2020/zenkoku2020_index.html〔2021/5/19 確認〕
※ 363 IPA：セキュリティ・ネクストキャンプ 2020 オンライン　ホーム　https://www.ipa.go.jp/jinzai/camp/2020/next2020_index.html〔2021/5/19 確認〕
※ 364 IPA：セキュリティ・キャンプ　https://www.ipa.go.jp/jinzai/camp/index.html#section5〔2021/5/19 確認〕
※ 365 一般社団法人セキュリティ・キャンプ協議会事務局：セキュリティ・キャンプ　https://www.security-camp.or.jp/event/index.html〔2021/5/19 確認〕
※ 366 enPiT2：連携校によるネットワークで特徴ある講義・演習を相互に提供　https://www.seccap.jp/basic/seccap.html〔2021/5/19 確認〕
※ 367 大阪大学大学院情報科学研究科 enPiT 事務局：enPiT［文部科学省］成長分野を支える情報技術人材の育成拠点の形成 2020 年度 成果報告書　https://www.enpit.jp/files/enPiT_annualreport_uni_2020.pdf〔2021/5/19 確認〕
※ 368 https://enpit-pro.jp〔2021/5/19 確認〕
※ 369 https://www.seccap.pro/〔2021/5/19 確認〕
※ 370 CTF（Capture The Flag）：互いに相手陣地にある旗を奪い合う野外ゲームを情報セキュリティに適用したもので、例えば自分のホストを守りながら、相手チームのホストを攻撃する競技等がある。
※ 371 Security NEXT：SECCON 初のオンライン決勝、約 1000 チームが参戦 - 一時開催危ぶまれるも若手奮闘　https://www.security-next.com/120376〔2021/5/19 確認〕
※ 372 SECCON：SECCON 2020 電脳会議 2020.12.19(sat)　https://www.seccon.jp/2020/ep201219.html〔2021/5/19 確認〕
※ 373 SECCON：SECCON Beginners とは　https://www.seccon.jp/2020/beginners/about-seccon-beginners.html〔2021/5/19 確認〕
※ 374 SECCON：SECCON Beginners Live 開催のお知らせ　https://www.seccon.jp/2020/seccon_beginners/seccon_beginners_live.html〔2021/5/19 確認〕
※ 375 http://girls.seccon.jp/〔2021/5/19 確認〕
※ 376 JNSA：JNSA インターンシップ　https://www.jnsa.org/internship/index.html〔2021/5/19 確認〕
※ 377 東京工業大学：キャリアアップ MOT「2020 年度 サイバーセキュリティ経営戦略コース」受講生募集のご案内　https://www.titech.ac.jp/alumni/news/2020/048570.html〔2021/5/19 確認〕
※ 378 サイバーセキュリティ経営：経営戦略や事業リスク管理の一貫としてサイバーセキュリティリスク管理を実践すること。
※ 379 PwC Japan グループ：経済犯罪実態調査 2020 日本分析版　https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2020/assets/pdf/economic-crime-survey.pdf〔2021/5/26 確認〕
※ 380 https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2020/assets/pdf/economic-crime-survey.pdf〔2021/5/26 確認〕

※ 381 トレンドマイクロ社：法人組織のセキュリティ動向調査 2020 年版を発表 https://www.trendmicro.com/ja_jp/about/press-release/2020/pr-20201002-01.html〔2021/5/26 確認〕
※ 382 NRI セキュア社：NRI セキュア、「企業における情報セキュリティ実態調査 2020」を実施 https://www.nri.com/jp/news/newsrelease/lst/2020/cc/1215_1〔2021/5/26 確認〕
※ 383 IPA：「2020 年度サイバーセキュリティ経営ガイドライン実践のためのプラクティスの在り方に関する調査」報告書 https://www.ipa.go.jp/security/fy2020/reports/practice/index.html〔2021/5/26 確認〕
※ 384 「強い懸念がある」及び「やや懸念がある」を合わせた回答。
※ 385 情報セキュリティリスクの管理体制構築や情報セキュリティ対策の実装等を率先して指示することを指す。
※ 386 https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf〔2021/5/26 確認〕
※ 387 IPA：サイバーセキュリティ経営ガイドライン実践状況の可視化ツールβ版 https://www.ipa.go.jp/security/economics/checktool/index.html〔2021/5/26 確認〕
※ 388 https://www.ipa.go.jp/security/fy30/reports/ciso/index.html〔2021/5/26 確認〕
※ 389-1 「必要であり、積極的に協力したいと思う」「必要であり、機会があれば協力したいと思う」「必要ではあるが、協力したいとは思わない」の合計。
※ 389-2 経済産業省：事務局説明資料 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/007_03_00.pdf〔2021/6/25 確認〕
※ 390 https://www.sonpo.or.jp/cyber-hoken/data/2020-01/pdf/cyber_report2020.pdf〔2021/5/19 確認〕
※ 391 https://www.ipa.go.jp/files/000088835.pdf〔2021/5/19 確認〕
※ 392 https://www.ipa.go.jp/security/keihatsu/sme/sc3/〔2021/5/19 確認〕
※ 393 https://www.ipa.go.jp/files/000088836.pdf〔2021/5/19 確認〕
※ 394 IPA：令和 2 年度中小企業の情報セキュリティマネジメント指導業務 https://www.ipa.go.jp/security/keihatsu/sme/management/index.html〔2021/5/19 確認〕
※ 395 経済産業省：「地域セキュリティコミュニティ【地域 SECUNITY】形成・運営のためのプラクティス集」（第 1 版）を取りまとめました https://www.meti.go.jp/press/2020/02/20210217001/20210217001.html〔2021/5/19 確認〕
※ 396 経済産業省：テレワークにおけるセキュリティ確保 https://www.soumu.go.jp/main_sosiki/cybersecurity/telework〔2021/6/2 確認〕
※ 397 https://www.soumu.go.jp/main_content/000753141.pdf〔2021/6/2 確認〕
※ 398 https://www.jnsa.org/result/west/data/SecurityByDesign.pdf〔2021/5/19 確認〕
※ 399 https://www.ipa.go.jp/security/security-action/〔2021/5/19 確認〕
※ 400 https://school-security.jp/pdf/2019.pdf〔2021/5/25 確認〕
※ 401 文部科学省：教育情報セキュリティポリシーに関するガイドライン（令和元年 12 月版） https://www.mext.go.jp/content/20200219-mxt_jogai02-000003278_409.pdf〔2021/6/1 確認〕
※ 402 国立大学法人金沢大学：個人情報を保存したノートパソコンの窃盗による紛失について（事実報告とお詫び） https://www.kanazawa-u.ac.jp/news/83181〔2021/5/25 確認〕
※ 403 国立大学法人東京芸術大学：ノート PC 及び受験関係書類の盗難にかかる個人情報の紛失について https://www.geidai.ac.jp/news/2021021998422.html〔2021/5/25 確認〕
※ 404 学校法人立教大学：個人情報を含む USB メモリ紛失のお詫びとお知らせ https://www.rikkyo.ac.jp/news/2021/03/mknpps000001j46o.html〔2021/5/25 確認〕
※ 405 総務省：自治体情報セキュリティ対策の見直しについて https://www.soumu.go.jp/main_content/000688754.pdf〔2021/5/25 確認〕
※ 406 LGWAN（Local Government Wide Area Network）：総合行政ネットワークのこと。地方公共団体を相互に接続する行政専用のネットワークであり、地方公共団体相互間のコミュニケーションの円滑化、情報の共有による情報の高度利用を図るための基盤として整備され、全国の地方公共団体の組織内ネットワークを相互に接続している。
※ 407 https://www.soumu.go.jp/main_content/000688753.pdf〔2021/5/25 確認〕
※ 408 eLTAX:地方税ポータルシステムのこと。地方税における手続きを、インターネットを利用して行うためのシステムで、地方税共同機構が開発・運営。読み方は「エルタックス」。
※ 409 ぴったりサービス：地方公共団体が提供する行政サービスを、検索したりオンライン申請したりできるサービスの総称。内閣府番号制度担当室が運営。
※ 410 総務省：地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会 https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security/index.html〔2021/6/3 確認〕
※ 411 J-LIS：（全体運用の開始）「自治体テレワーク推進実証実験」について https://www.j-lis.go.jp/lgwan/news/lgwan-koubo_telework.html〔2021/5/25 確認〕
※ 412 J-LIS：緊急事態宣言（令和 3 年 1 月）の発出に伴う「自治体テレワークシステム for LGWAN」の一時提供について https://www.j-lis.go.jp/lgwan/news/lgwan-koubo_telework_1.html〔2021/5/25 確認〕
※ 413 総務省：次期自治体情報セキュリティクラウドの標準要件の決定について https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security/index_00001.html〔2021/5/25 確認〕
※ 414 SOC（Security Operation Center）：セキュリティ攻撃の検出・分析のため、システムやデバイス、ネットワーク等を監視するセキュリティ専門人材による組織。
※ 415 CDN（Content Delivery Network）：Web コンテンツを配信するために最適化されたネットワーク。オリジナルの Web コンテンツを格納するサーバである「オリジンサーバ」、代理で Web コンテンツを配信する「キャッシュサーバ」などから構成される。
※ 416 三重県：三重県自治体情報セキュリティクラウドの更改に関する情報提供依頼（RFI） https://www.pref.mie.lg.jp/IT/HP/m0009800059_00004.htm〔2021/5/25 確認〕
※ 417 茨城県：いばらき情報セキュリティクラウド導入にかかる情報提供依頼（RFI）の実施について https://www.pref.ibaraki.jp/kikaku/joho/denshi/20210308.html〔2021/5/25 確認〕
※ 418 SLA（Service Level Agreement）：サービス事業者と利用者の間で結ばれるサービスのレベル（定義、範囲、内容、達成目標等）に関する合意サービス水準、サービス品質保証のこと。
※ 419 IPA:「2020 年度情報セキュリティに対する意識調査【倫理編】【脅威編】」報告書 https://www.ipa.go.jp/security/economics/ishikichousa2020.html〔2021/6/4 確認〕
※ 420 選択肢「1 年以上前から実施している」「1 年以内に実施し始めた」の合計。
※ 421 IPA の「2020 年度情報セキュリティに対する意識調査【脅威編】」では、調査対象者のうち社会人を「情報システムおよび通信関係以外の業務」及び「情報システムおよび通信関係の業務」に分類し分析している。本白書用に実施した追加分析では前者の「情報システムおよび通信関係以外の業務」の従事者を対象とした。また、本調査では、情報システム・通信関係の業務に従事・関与しない対象者として「公務員」「教職員」の分類が存在する。しかし、サンプル数が少なく参考値扱いとなったため、追加分析の対象から除外した。
※ 422 IPA の「2020 年度 情報セキュリティに対する意識調査【脅威編】」の「職業軸 _ 脅威調査 PC」（https://www.ipa.go.jp/files/000088918.pdf〔2021/6/4 確認〕）では「電子メールにある添付ファイルは不用意に開かない、また本文中の URL も不用意にクリックしない」を「1 年以上前から実施している」「1 年以内に実施し始めた」の合計が 69.6%（p.81）、「ネットでファイルやソフトウェアをダウンロードする場合、安全性や信頼性を自分なりに注意・判断している」を「1 年前から実施している」「1 年以内に実施し始めた」割合が 69.5%（p.83）。
※ 423 経済産業省：知的財産と標準化によるビジネス戦略 https://www.jpo.go.jp/news/shinchaku/event/seminer/text/document/h30_jitsumusya_txt/34_pp.pdf〔2021/6/4 確認〕
※ 424 https://www.kantei.go.jp/jp/singi/titeki2/kettei/chizaikeikaku20200527.pdf〔2021/6/4 確認〕
※ 425 国立研究開発法人産業技術総合研究所：産業界の標準化活動をサポートする産総研標準化推進センターが始動 https://www.aist.go.jp/aist_j/news/pr20200701.html〔2021/6/4 確認〕
※ 426 フォーラム標準の定義については、「JIS Z 8002:2006」の「JA.1」の「100.5」を参照。
※ 427 ISO：ISO/IEC JTC 1 https://www.iso.org/committee/45020.html〔2021/6/4 確認〕
※ 428 日本産業標準調査会：JISC について https://www.jisc.go.jp/jisc/index.html〔2021/6/4 確認〕
※ 429 ITU：SG17: Security https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx〔2021/6/4 確認〕
※ 430 IETF：The IETF Security Area https://trac.ietf.org/trac/sec/wiki〔2021/6/4 確認〕
※ 431 TCG：Welcome to Trusted Computing Group https://trustedcomputinggroup.org/work-groups/regional-forums/japan〔2021/6/4 確認〕
※ 432 https://www.jisc.go.jp/international/iso-prcs.html〔2021/6/4 確認〕
※ 433 ISO/IEC 27701 は SC 27/WG 5 で検討、発行された規格である。
※ 434 耐量子計算機暗号：量子計算機が実用化されても安全性が保てると期待される暗号。

※ 435 ドイツ規格協会：Downloads　https://www.din.de/en/meta/jtc1sc27/downloads〔2021/6/4 確認〕
上記 Web ページの「SC27WG2 SD8 Post-Quantum Cryptography」をクリックすることでダウンロードできる。
※ 436 Preliminary Work Item（予備業務項目）：新しい標準を作成するための検討期間を指す。2020 年 9 月まで WG 3 内では研究期間（Study Period）と呼ばれていた。
※ 437 Black Hat：Remote Exploitation Of An Unaltered Passenger Vehicle　https://www.youtube.com/watch?reload=9&v=MAcHkASmXEc〔2021/5/19 確認〕
※ 438 日本経済新聞：クライスラー、ハッキング対策で 140 万台リコール　https://www.nikkei.com/article/DGXLASGM25H19_V20C15A7MM0000/〔2021/5/19 確認〕
※ 439 United Nations Economic Commission for Europe（国際連合欧州経済委員会）：国際連合の経済社会理事会の地域経済委員会の一つ。
※ 440 ISO：ISO/SAE FDIS 21434 Road vehicles — Cybersecurity engineering　https://www.iso.org/standard/70918.html〔2021/5/19 確認〕
※ 441 ISO：Biometric security　https://www.iso.org/contents/news/2021/01/Ref2613.html〔2021/5/19 確認〕
※ 442 IoT 推進コンソーシアム・総務省・経済産業省：IoT セキュリティガイドライン Ver1.0　https://www.soumu.go.jp/main_content/000428393.pdf〔2021/5/26 確認〕
※ 443 https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf〔2021/6/2 確認〕
※ 444 https://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf〔2021/6/2 確認〕
※ 445 https://www.commoncriteriaportal.org/〔2021/6/2 確認〕
※ 446 IPA：認証プロテクションプロファイルリスト　https://www.ipa.go.jp/security/jisec/certified_pps/pp_list.html〔2021/6/2 確認〕
※ 447 IPA：本制度に関連する ISO/IEC 規格　https://www.ipa.go.jp/security/jcmvp/topics.html〔2021/6/3 確認〕
※ 448 NIST：FIPS 140-3 Transition Effort　https://csrc.nist.gov/Projects/fips-140-3-transition-effort/fips-140-3-docs〔2021/6/3 確認〕
※ 449 NIST：Supporting Documents for FIPS 140-3 and the Cryptographic Module Validation Program (CMVP) Now Available: NIST Special Publication 800-140x Subseries　https://csrc.nist.gov/news/2020/nist-publishes-sp-800-140x-subseries-for-the-cmvp〔2021/6/3 確認〕
※ 450 NIST：FIPS 140-2 Cryptographic Module Validation Program Management Manual　https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Module-Validation-Program/documents/CMVPMM.pdf〔2021/6/3 確認〕
※ 451 NIST：FIPS 140-3 Transition Effort　https://csrc.nist.gov/projects/fips-140-3-transition-effort〔2021/6/3 確認〕
※ 452 NIST：FIPS 140-3 IG Announcements　https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements〔2021/6/3 確認〕
※ 453 NIST：FIPS 140-3 Management Manual　https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-140-3-management-manual〔2021/6/3 確認〕
※ 454 International Cryptographic Module Conference：https://icmconference.org/〔2021/6/3 確認〕
※ 455 NIST：Use of Unvalidated Cryptographic Modules by Federal Agencies and Departments　https://csrc.nist.gov/projects/cryptographic-module-validation-program〔2021/6/3 確認〕
※ 456 https://www.kantei.go.jp/jp/singi/it2/cio/kettei/20190225kettei1-1.pdf〔2021/6/3 確認〕
※ 457 IPA/JISEC：「ハードコピーデバイスのプロテクションプロファイル」適合の申請案件についてのガイドライン 第 1.8 版　https://www.ipa.go.jp/security/jisec/mfp/guidelineforHCD-PP_1.8.pdf〔2021/6/3 確認〕
※ 458 https://www.ipa.go.jp/security/jisec/certified_pps/c0553/c0553_pp.pdf〔2021/6/3 確認〕
※ 459 IPA/JISEC：認証製品リスト　https://www.ipa.go.jp/security/jisec/certified_products/cert_listv31.html〔2021/6/3 確認〕
※ 460 IPA：暗号アルゴリズム確認登録簿　https://www.ipa.go.jp/security/jcmvp/avallists.html〔2021/6/3 確認〕
※ 461 IPA/JCMVP：暗号モジュール試験及び認証制度（JCMVP）：承認されたセキュリティ機能　https://www.ipa.go.jp/security/jcmvp/algorithm.html〔2021/6/3 確認〕
※ 462 NIST：Recommendation for Key-Derivation Methods in Key-Establishment Schemes　https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr1.pdf〔2021/6/3 確認〕
※ 463 e-Gov 法令検索：電子署名及び認証業務に関する法律施行規則　https://elaws.e-gov.go.jp/document?lawid=413M60000418002〔2021/6/3 確認〕
※ 464 IPA：暗号モジュール試験及び認証制度（JCMVP）：規程集　https://www.ipa.go.jp/security/jcmvp/kitei.html〔2021/6/3 確認〕
※ 465 経済産業省：「政府情報システムのためのセキュリティ評価制度（ISMAP）」の運用を開始しました　https://www.meti.go.jp/press/2020/06/20200603001/20200603001.html〔2021/6/4 確認〕
※ 466 https://cio.go.jp/sites/default/files/uploads/documents/cloud_policy_20210330.pdf〔2021/6/4 確認〕
※ 467 経済産業省：クラウドサービスの安全性評価に関する検討会について　https://www.meti.go.jp/shingikai/mono_info_service/cloud_services/pdf/001_02_00.pdf〔2021/6/4 確認〕
※ 468 https://www.meti.go.jp/press/2019/01/20200130002/20200130002-1.pdf〔2021/6/4 確認〕
※ 469 https://www.nisc.go.jp/active/general/pdf/wakugumi2020.pdf〔2021/6/4 確認〕
※ 470 https://www.ismap.go.jp/sys_attachment.do?sys_id=c0b4525fdb53a4107766044cd3961942〔2021/6/4 確認〕
※ 471 https://www.ismap.go.jp〔2021/6/4 確認〕
※ 472 https://www.nisc.go.jp/active/infra/pdf/shishin5rev.pdf〔2021/6/4 確認〕
※ 473 NISC：『ラブライブ!サンシャイン !!』とのタイアップについて　https://www.nisc.go.jp/security-site/month/lovelive.html〔2021/5/19 確認〕
※ 474 https://www.youtube.com/watch?v=L7FQboNt9RI〔2021/5/19 確認〕
※ 475 https://www.youtube.com/watch?v=Cghzzqh33JA〔2021/5/19 確認〕
※ 476 https://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/csboardgame.html〔2021/5/19 確認〕
※ 477 https://www.itct-net.com/siryou#h.kaes1k95c2bs〔2021/5/19 確認〕
※ 478 JNSA：みんなの「サイバーセキュリティコミック」プロジェクト　https://www.jnsa.org/comic/〔2021/5/19 確認〕
※ 479 トレンドマイクロ株式会社：法人向けガイドブック「働く大人なら最低限知っておきたいネットセキュリティの基本」2021 年度版公開　https://www.is702.jp/news/3835/〔2021/5/19 確認〕
※ 480 NHK：木村花さんの死が問いかけるもの　https://www3.nhk.or.jp/news/html/20200604/k10012457591000.html〔2021/5/19 確認〕
※ 481 総務省：特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律第 4 条第 1 項の発信者情報を定める省令の一部を改正する省令の制定　https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000095.html〔2021/5/19 確認〕
※ 482 違法・有害情報相談センター：削除依頼の流れについて　https://ihaho.jp/guide/reqdelflow.html〔2021/5/19 確認〕
※ 483 https://www.pref.gunma.jp/07/cl01_00048.html〔2021/5/19 確認〕
※ 484 https://no-heart-no-sns.smaj.or.jp/〔2021/5/19 確認〕
※ 485 https://smaj.or.jp/〔2021/5/19 確認〕
※ 486 Twitter Japan 株式会社：https://twitter.com/twitterjp/status/1235685197959639042〔2021/5/19 確認〕
※ 487 Twitter Japan 株式会社：Twitter での会話について　https://help.twitter.com/ja/using-twitter/twitter-conversations#controls〔2021/5/19 確認〕
※ 488 ByteDance 株式会社：TikTok、青少年のオンライン上でのプライバシー保護に関する安全性を強化　https://newsroom.tiktok.com/ja-jp/strengthening-privacy-and-safety〔2021/5/19 確認〕
※ 489 ByteDance 株式会社：TikTok、青少年保護強化のために年齢認証システムを全ユーザー向けに変更　https://newsroom.tiktok.com/ja-jp/tiktok-changes-the-age-verification-system-to-be-applicable-for-all-users〔2021/5/19 確認〕
※ 490 ヤフー株式会社：ユーザーに安心してご利用いただくための自主ルール策定を目的とした「プラットフォームサービスの運営の在り方検討会」を開催　https://about.yahoo.co.jp/pr/release/2020/07/01a/〔2021/5/19 確認〕
※ 491 千葉日報：被告「被害者の気持ち分かった」　成田不明女児の母を脅迫　検察、懲役6月求刑　https://www.chibanippo.co.jp/news/national/731442〔2021/5/19 確認〕
※ 492 https://www5.cao.go.jp/keizai2/manzoku/pdf/result2_covid.pdf〔2021/5/19 確認〕
※ 493 https://www.mhlw.go.jp/content/000777425.pdf〔2021/5/19 確認〕
※ 494 https://www.ipa.go.jp/security/kokokara/〔2021/5/19 確認〕

※ 495 https://www.mext.go.jp/content/20200427-mxt_kouhou01-000004520_1.pdf〔2021/5/19 確認〕
※ 496 文部科学省：GIGA スクール構想について　https://www.mext.go.jp/a_menu/other/index_0001111.htm〔2021/5/19 確認〕
※ 497 文部科学省：「教育情報セキュリティポリシーに関するガイドライン」公表について　https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm〔2021/5/19 確認〕
※ 498 NHK：トイレットペーパー“品薄はデマ”も不安に歯止めかからず　https://www3.nhk.or.jp/news/html/20200302/k10012309761000.html〔2021/5/19 確認〕
※ 499 https://www.soumu.go.jp/main_content/000693280.pdf〔2021/5/19 確認〕
※ 500 ASCII.jp：オードリー・タン氏「台湾のデジタル社会イノベーションはどう実現したか」　https://ascii.jp/elem/000/004/033/4033626/2/〔2021/5/19 確認〕
※ 501 https://www.youtube.com/watch?v=rbNuikVDrN4〔2021/5/19 確認〕
※ 502 読売新聞オンライン：［STOP　ネット暴力］「うちの県にコロナ持ってきた」…「感染者狩り」横行、実名特定・中傷エスカレート　https://www.yomiuri.co.jp/national/20200804-OYT1T50069/〔2021/5/19 確認〕
※ 503 宮城県：「ストップ!コロナ差別」 啓発活動にご協力ください　https://www.pref.miyagi.jp/site/covid-19/corona-stopsenngenn.html〔2021/5/19 確認〕
※ 504 内閣官房：新型コロナウイルス感染症に関する偏見や差別を防止するための規定が設けられました!　https://corona.go.jp/emergency/pdf/henken_sabetu_20210212.pdf〔2021/5/19 確認〕
※ 505 http://www.kokusen.go.jp/pdf/n-20200710_1.pdf〔2021/5/19 確認〕
※ 506 https://www.meti.go.jp/covid-19/pdf/jizokuka-kyufukin_fusei.pdf〔2021/5/19 確認〕
※ 507 神奈川県：荷受代行や荷物転送のアルバイトにご注意!　https://www.pref.kanagawa.jp/docs/r7b/cnt/f370214/p1057013.html〔2021/5/19 確認〕
埼玉県：「荷受代行」「荷物転送」のアルバイトに気をつけて!　https://www.pref.saitama.lg.jp/b0304/soudanjirei/161125.html〔2021/5/19 確認〕
※ 508 経済産業省：不正競争防止法　https://www.meti.go.jp/policy/economy/chizai/chiteki/h30jyoubunn.pdf〔2021/5/19 確認〕
※ 509 経済産業省：「不正競争防止法第十八条第二項第三号の外国公務員等で政令で定める者を定める政令の一部を改正する政令」が閣議決定されました　https://www.meti.go.jp/press/2018/09/20180904001/20180904001.html〔2021/5/19 確認〕
※ 510 BUSINESS LAWYERS:第 1 回 2019 年 7 月施行、ビッグデータの保護に関する改正不正競争防止法の概要と保護の対象となるデータ　https://www.businesslawyers.jp/articles/583〔2021/5/19 確認〕
※ 511 経済産業省：営業秘密管理指針　https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf〔2021/5/19 確認〕
※ 512 IPA：「企業における営業秘密管理に関する実態調査 2020」報告書について　https://www.ipa.go.jp/security/fy2020/reports/ts_kanri/index.html〔2021/5/19 確認〕
※ 513 IPA：「企業における営業秘密管理に関する実態調査」報告書について　https://www.ipa.go.jp/security/fy28/reports/ts_kanri/index.html〔2021/5/19 確認〕
※ 514 差分攻撃：入力平文と出力暗号文の差分を用いる暗号攻撃手法。
※ 515 Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir：The Retracing Boomerang Attack　https://link.springer.com/chapter/10.1007%2F978-3-030-45721-1_11〔2021/5/19 確認〕
※ 516 AES（Advanced Encryption Standard）：米国で NIST により標準化された共通鍵暗号。
※ 517 差分線形解析：差分と線型近似とを組み合せた暗号攻撃手法。
※ 518 Christof Beierle, Gregor Leander, and Yosuke Todo：Improved Differential-Linear Attacks with Applications to ARX Ciphers　https://link.springer.com/chapter/10.1007/978-3-030-56877-1_12〔2021/5/19 確認〕
※ 519 ChaCha:Daniel J. Bernstein によって開発されたストリーム暗号。Chacha20 は ChaCha を基にした暗号であり、これとメッセージ認証子である Poly1305 とを組み合わせた ChaCha20-Poly1305 は、CRYPTREC の推奨候補暗号リストに入っている。
※ 520 Comparing the Difficulty of Factorization and Discrete Logarithm: A 240-Digit Experiment [Crypto2020] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann　https://link.springer.com/chapter/10.1007%2F978-3-030-56880-1_3〔2021/5/19 確認〕
※ 521 NIST：NIST PQC Standardization Update-Round 2 and Beyond　https://csrc.nist.gov/CSRC/media/Presentations/pqc-update-round-2-and-beyond/images-media/pqcrypto-sept2020-moody.pdf〔2021/5/19 確認〕
※ 522 NIST：Lightweight Cryptography Standardization: Finalists Announced　https://csrc.nist.gov/News/2021/lightweight-crypto-finalists-announced〔2021/5/19 確認〕
※ 523 ECDSA（Elliptic Curve Digital Signature Algorithm）：楕円曲線暗号を用いたデジタル署名アルゴリズム。
※ 524 Jan Jancar, Vladimir Sedlacek, Petr Svenda, and Marek Sys：Minerva: The curse of ECDSA nonces　https://tches.iacr.org/index.php/TCHES/article/view/8684〔2021/5/19 確認〕
※ 525 nonce：ある種の暗号演算において、1 度だけ使用される使い捨ての値。
※ 526 CVE（Common Vulnerabilities and Exposures）：個別製品中の脆弱性を対象として採番されている識別子。本件については実装ごとに CVE-2019-2894、CVE-2019-13627、CVE-2019-13628、CVE-2019-13629、CVE-2019-14318、CVE-2019-15819 が発行されている。
※ 527 binary GCD アルゴリズム：2 数の最大公約数を求めるアルゴリズムの一つ。ユークリッドの互除法と比較して、計算機に向くような単純な算術演算（シフト、比較、減算）のみを使用することで、高速に計算できるようにしている。
※ 528 Alejandro Cabrera Aldaya, and Billy Bob Brumley：When one vulnerable primitive turns viral: Novel single-trace attacks on ECDSA and RSA　https://tches.iacr.org/index.php/TCHES/article/view/8549〔2021/5/19 確認〕
※ 529 Alejandro Cabrera Aldaya, Cesar Pereida García and Billy Bob Brumley：From A to Z: Projective coordinates leakage in the wild　https://tches.iacr.org/index.php/TCHES/article/view/8596〔2021/5/19 確認〕
※ 530 https://www.jnsa.org/result/surv_mrk/2021/index.html〔2021/6/30 確認〕