情報セキュリティ白書

序章

2019年度の情報セキュリティの概況

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

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

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

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

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

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

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

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

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

2019 年度の情報セキュリティの概況

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

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

第2章
情報セキュリティを支える基盤の動向

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

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

2.1 国内の情報セキュリティ政策の状況

本節では、政府が推進する情報セキュリティ対策の状況を述べる。

2.1.1 政府全体の政策動向

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

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

(1)「サイバーセキュリティ戦略」の見直し

サイバーセキュリティ戦略とは、サイバーセキュリティ基本法に基づき策定された、我が国のサイバーセキュリティにおける基本的な立場等と策定後 3 年間の施策目標や実施方針を示した行動計画を指す。2015 年 9 月に初めてサイバーセキュリティ戦略（以下、2015 年戦略）が閣議決定され、2018 年 7 月に 2 回目となる新たなサイバーセキュリティ戦略（以下、2018 年戦略）が閣議決定された（図 2-1-1）。

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

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

- サービス提供者の任務保証

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

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

- 参加・連携・協働

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

また、2018年戦略の目的達成の施策として、「経済社会の活力の向上及び持続的発展」「国民が安全で安心して暮らせる社会の実現」「国際社会の平和・安定及び我が国の安全保障への寄与」「横断的施策」の四つの観点が示されている。これらに関して2019年度に実行された施策について、次項で述べる。

(2)「サイバーセキュリティ2019」の主な取り組み状況

「サイバーセキュリティ2019[※2]」は、2018年戦略に基づく初めての年次報告とそれを反映した2019年度の年次計画を統合したもので、関連府省庁はこれに基づき施策を実施する。以下、2018年戦略の目的達成の施策として示されている四つの観点について、サイバーセキュリティ2019で計画し実施された取り組みについて述べる。

- 経済社会の活力の向上及び持続的発展

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

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

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

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

また経済産業省とIPAは、サイバーセキュリティの政策・課題に関する官民の情報共有や企業同士の連携を図るため、メンバーを限定しない情報交流の場「コラボレーション・プラットフォーム※8」を開催した（コラボレーション・プラットフォームについては「2.1.2（1）（c）WG3（サイバーセキュリティビジネス化）参照」）。

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

- 国民が安全で安心して暮らせる社会の実現

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

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

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

- 国際社会の平和・安定及び我が国の安全保障への寄与

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

- 横断的施策

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

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

（3）重要インフラの情報セキュリティ対策強化

我が国の重要インフラの防護に係る基本的な枠組みとして、サイバーセキュリティ戦略本部は2017年4月に「重

要インフラの情報セキュリティ対策に係る第 4 次行動計画※19」（以下、第 4 次行動計画）を決定した。続いて 2018 年 7 月、新たな重要インフラ分野として「空港」分野を追加する形で同計画を改定した※20。

また、各重要インフラ分野に共通して求められる情報セキュリティ対策の実施を訴求するため、2018 年 4 月に、サイバーセキュリティ戦略本部が「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第 5 版）※21」を、重要インフラ専門調査会が「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第 1 版）※22」を発行した。以下、2019 年度における主な活動について述べる。

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

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

同調査会はこれに基づき、2019 年 10 月に「『重要インフラの情報セキュリティ対策に係る第 4 次行動計画』に基づく情報共有の手引書（試行版）※24」（以下、試行版）を策定した。2019 年 11 月に実施された後述の「分野横断的演習」において、同演習参加者（事業者）は試行版を参照し、情報連絡様式を実際に用いて情報連絡を実施した。事業者等から内容の修正を要するコメントはなかったため、同調査会は 2020 年 3 月を目途に正式版として制定するとしている。

(b)「分野横断的演習」の実施

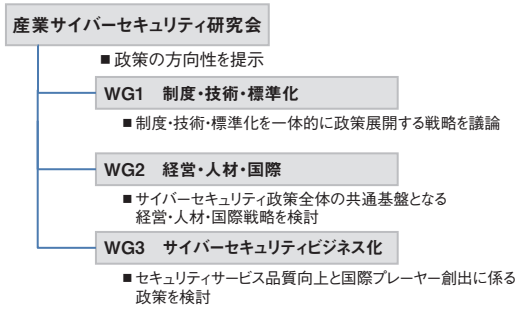
NISC は、重要インフラ事業者の事業継続計画や官民・分野横断的な情報共有体制に関する検証及び課題の抽出を行うことにより、障害対応体制の強化を図ることを目的とした分野横断的演習を 2019 年 11 月に実施した※25。重要インフラ 14 分野を対象に、重要インフラ事業者や所管省庁、情報セキュリティ関係機関等から、過去最大となる 4,967 名（717 組織）が参加した。同演習では東京 2020 オリンピック・パラリンピック競技大会開催期間中を想定した演習シナリオのもと、重要インフラ事業者等は事業継続計画等に基づいて、状況整理、所管省庁への情報連絡、対応方針検討、関係機関、他事業者等との情報共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

2.1.2 経済産業省の政策

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

(1) 産業サイバーセキュリティ研究会

2017 年 12 月、経済産業省は我が国の産業界が直面するサイバーセキュリティの課題を洗い出し、関連政策を推進するため、産業界を代表する経営者、インターネット関連の学識経験者等から構成される「産業サイバーセキュリティ研究会」を設置した※26。図 2-1-2 に同研究会の構成を示す。



■図 2-1-2　産業サイバーセキュリティ研究会の構成
（出典）経済産業省「産業分野におけるサイバーセキュリティ政策※27」を基に IPA が編集

また、同研究会では 2018 年 5 月に発表した「産業サイバーセキュリティ強化へ向けたアクションプラン※28」を中心とした取り組みを更に加速して行くために、以下の三つの視点から重点施策を強化するとしている※29。

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

各 WG の概要と活動状況は以下のとおりである。

(a) WG1（制度・技術・標準化）

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

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

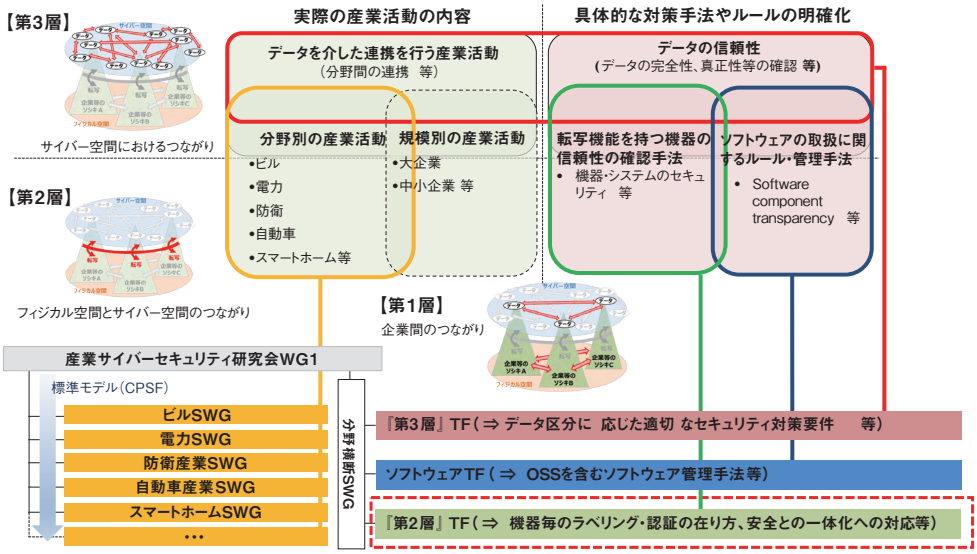
CPSFでは、産業社会を三つの層で整理した「3層構造モデル」ととらえることでセキュリティ確保のための信頼性の基点を明確化するとともに、バリュークリエイションプロセスに関与する、セキュリティ対策を講じる最小単位となる「六つの構成要素」を提示している。これらに基づいて、リスク源を洗い出し、その対策要件※30を特定できるとしている（リスクベースアプローチ）。

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

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

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

また、WG1ではCPSFを参考にしつつ、各産業分



■図2-1-3　タスクフォースの構成
（出典）経済産業省「『第2層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性※32」

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

（b）WG2（経営・人材・国際）

WG2 では、サイバーセキュリティ対策における経営者の参画と人材育成、国際連携に関する政策を議論している。

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

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

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

国際連携活動としては、IPA を通じて、2019 年 9 月 9～12 日に「インド太平洋地域向け日米サイバー演習※15」を実施した（「2.3.2（1）中核人材育成プログラム」参照）。また、国際会議等で各国のステークホルダと CPSF を軸とした議論を行い、サイバー・フィジカル・セキュリティに関する共通認識を醸成した※39。

（c）WG3（サイバーセキュリティビジネス化）

WG3 では、セキュリティ製品・サービスの品質向上と国際プレーヤー創出に関わる政策として、サイバーセキュリティ製品の有効性を検証する検証基盤の整備による、国内セキュリティビジネスの競争力創出等の議論を行った※40。

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

また WG3 は IPA を通じて、2018 年 6 月から、サイバー・フィジカル・セキュリティに関する情報交流の場として「コラボレーション・プラットフォーム」を設置し、2019 年度も継続した※8。ここでは参加資格を限定せず、議論を通じてサイバーセキュリティ対策のニーズを明確化・具体化するとともに、シーズに関する情報提供・情報収集等を行うことで、政策等への意見反映や企業間のマッチングを図っている。2019 年度は 6 回実施し、計 567 人が参加した。

（2）政府情報システムのためのセキュリティ評価制度（ISMAP）

各府省情報化統括責任者（CIO）連絡会議において決定され、2018 年 6 月に公開された「政府情報システ

ムにおけるクラウドサービスの利用に係る基本方針※43」では、「クラウド・バイ・デフォルト原則」が掲げられた。一方で、クラウドサービスプロバイダに要求する統一的なセキュリティ要求基準は存在せず、各政府機関等が調達の際に、個別のプロバイダのセキュリティ対策を確認し調達を行っている。こうした現状を踏まえ、経済産業省と総務省は、2018年8月から「クラウドサービスの安全性評価に関する検討会※44」を発足させた。

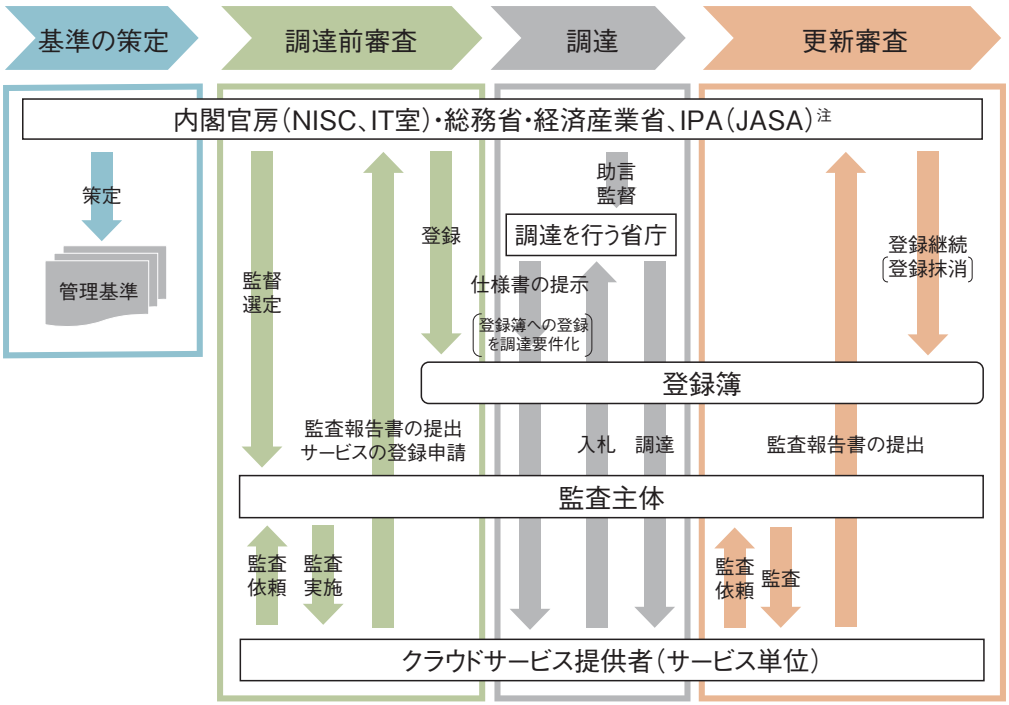
本検討会では、日本経済再生本部による「未来投資戦略2018※45」を踏まえ、クラウドサービスに関する既存のガイドラインや国内外の認証制度、監査制度等を整理するとともに、適切なセキュリティを満たすクラウドサービスを導入するために必要な評価方法等を検討し、2020年1月に「クラウドサービスの安全性評価に関する検討会とりまとめ※46」(以下、検討会取りまとめ)が公開された。また、同月のサイバーセキュリティ戦略本部会合において「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて※47」が決定された。

本制度においては、まず、政府機関等が調達するクラウドサービスに対して要求するべき基本的な情報セキュリティ管理・運用の基準を定めることとした。その上で、本制度で定められた情報セキュリティ監査の枠組みを活用した評価プロセスに基づき、上記の基準を満たすセキュリティ対策を実施していることが確認されたクラウドサービスを、本制度が公表するクラウドサービスリストに登録することとした。

また、本制度における監査を行うことができる監査機関は、あらかじめ本制度で定める要求事項を満たすことが確認され、本制度が公表する監査機関リストに登録されるものとした。以上の制度のフローを図2-1-4に示す。図において、クラウドサービス提供者は監査機関リストに登録された機関による監査を受け、所管政府機関に申請の上、登録簿にのせてもらう。省庁の調達者は登録簿を使って調達先候補を選ぶ。所管政府機関は監査者認定と監査結果に基づく登録簿管理を行う。

従来、政府調達に当たっては、個々のクラウドサービスが実施していると表明する情報セキュリティ対策の実施状況を、調達者が直接確認することが必要であったが、本制度により、この確認負荷が省略できるとともに、本制度が要求する情報セキュリティ対策基準を満たすことが確認されたクラウドサービスを効率的に調達することができる。

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



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

■図2-1-4　クラウドサービスの安全性評価の制度のフロー
(出典)内閣官房・総務省・経済産業省「政府情報システムのためのセキュリティ評価制度(ISMAP)について※48」

ISMAPに関する規則、基準等は、以下のとおりである。

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

クラウドサービス事業者が遵守すべきISMAP管理基準は、国際規格をベースに「政府機関等の情報セキュリティ対策のための統一基準群（平成30年度版）※50」「NIST SP800-53 rev.4」を参照して作成されている。国際規格としては、情報セキュリティに関してはJIS Q 27001（ISO/IEC 27001）、JIS Q 27002（ISO/IEC 27002）とクラウドサービスの情報セキュリティに関するJIS Q 27017（ISO/IEC 27017）を参考としている。また、これらの国際規格に準拠して編成された「クラウド情報セキュリティ管理基準（平成28年度版）」を参考とし、そこに含まれるガバナンス基準についてはJIS Q 27014（ISO/IEC 27014）を参考としている。

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

ISMAPの所管はNISC、情報通信技術（IT）総合戦略室、総務省、経済産業省であり、最高意思決定機関としてISMAP運営委員会を設置し、事務局はNISCに置かれる。またISMAPの実施時期については、2019年12月の「デジタルガバメント実行計画※53」において、「2020年度（令和2年度）内に、全政府機関において（中略）利用の開始」が目標として掲げられていたが、2020年6月3日、ISMAPの運用開始が正式に発表され※54、運用実務はIPAが担当することとなった※55。

なお、ISMAPで公開される情報等については、重要産業分野等を始めとする民間においても参照することで、クラウドサービスの適切な活用の推進が期待される。これに関連して、重要インフラにおけるクラウドサービスの利用について、2019年5月23日に改定されたNISCの「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）※56」においては「事業環境の変化を捉え、インターネットを介したサービス（クラウドサービス等）を活用するなど新しい技術を利用する際には、国内外の法令や評価制度等の存在について留意する。」と位置付けられている。

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

(3) AI・データの利用に関する契約ガイドライン

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

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

(4) 産業競争力強化法等の一部改正

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

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

報等の管理について、国が示す認証基準に適合していることを、事業所管大臣及び経済産業大臣が認定した認証機関から認証を受けられる制度である。認証機関に対する支援措置として、独立行政法人中小企業基盤整備機構やIPAからの情報提供支援があり、2020年2月現在3事業者が認定を受けている。認証を取得しようとする企業・団体に対しては、経済産業省が専門家を派遣して認証取得申請の支援を行う事業を行っている。更に、自社の情報管理状況を把握できる「セルフチェックシート」の一部（全事業者共通の必須事項のみ）を2019年12月に先行公開している。

(5) 情報セキュリティサービス基準適合サービス

情報セキュリティサービスを安心して活用できる環境を醸成するべく、経済産業省は「セキュリティサービス認定検討会」を開催し、「情報セキュリティサービス基準」及び「情報セキュリティサービスに関する審査登録機関基準」を策定し、2018年2月に公表した※64。本サービス基準は、情報セキュリティサービスについて一定の品質の維持向上が図られているか否かを第三者が客観的に判断し、結果を公開することで、利用者が必要なセキュリティサービスを容易に選定できるようにする枠組みである。

IPAはこの枠組みに基づき、2018年7月から、審査登録機関※65による審査の結果サービス基準に適合すると認められ、当該機関の登録台帳に登録され、かつIPAに誓約書を提出した事業者の情報セキュリティサービスを掲載した「情報セキュリティサービス基準適合サービスリスト」を公開している※66。本サービス基準では、情報セキュリティサービスを以下の四つに分類しており、これらのサービス登録数の合計が2020年7月時点で192件に達した。

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

なお、本リストの「情報セキュリティ監査サービス」に掲載されているサービスは、「政府機関等の対策基準策定のためのガイドライン」から参照されている。また、本リストの「情報セキュリティ監査サービス」に掲載されているサービスを提供する監査機関であることは、前述の「ISMAP監査機関登録規則」において、監査機関登録の申請者への要求事項の一つとなっている。

今後、本サービスリストの活用が進むことで、情報セキュリティサービス市場の活性化にもつながることが期待される。

(6) J-CSIP（サイバー情報共有イニシアティブ）

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

J-CSIPは、日本の基幹産業を担う企業を中心に、サイバー攻撃等に関する情報を相互に共有し、サイバー攻撃の防御とその被害の低減を目指している。2020年3月末日現在、IPAを情報の中継・集約点（情報ハブ）として15の業界から262の企業や業界団体（以下、組織）がJ-CSIPに参加している。

参加の形態としては、IPAと各組織との間で個別にNDA（Non-Disclosure Agreement：秘密保持契約）を締結して情報共有を行う業界単位のグループ（SIG※67）と、規約を基に業界の情報共有活動を支援するための枠組みである「情報連携体制」が存在する（図2-1-5）。

また、J-CSIPはIPAを通じて、経済産業省やセプターカウンシルのC4TAP、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC：Japan Computer Emergency Response Team Coordination Center）等とも連携している。

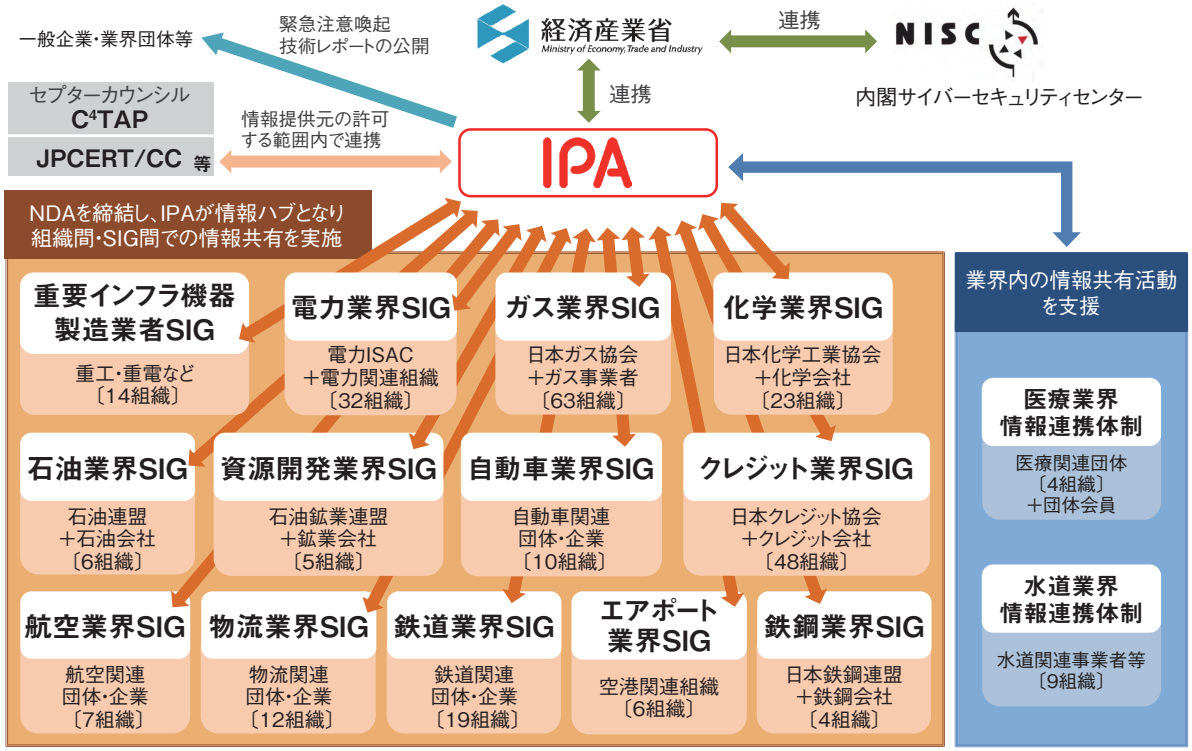
J-CSIPでは、IPAと参加組織との間でサイバー攻撃に関する手口や被害の情報、標的型攻撃メール等に関する情報共有を行っている。なお、J-CSIPの中で共有される情報は、提供元が明らかにならないよう、情報提供者の固有の情報を除去するルールがある。

参加組織からの情報提供件数、提供を受けた情報のうち標的型攻撃メールと見なした件数（攻撃メール件数）、及びそれらを基にJ-CSIP内で情報共有を行った件数（情報共有件数）を表2-1-1に示す。時期により件数の上下はあるものの、継続して情報提供や共有が行われていることが分かる。

2019年度は、2018年度までと同様、ビジネスメール

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

■表2-1-1　J-CSIPの運用実績



■図 2-1-5　J-CSIP の体制全体図
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2020 年 1 月～ 3 月］※68」

詐欺の事例に関する情報提供が多く寄せられた。偽のメールを駆使し、金銭の詐取を試みるという点は従来の事例と変わらないが、新たな騙しの手口が確認されている（「1.2.2 ビジネスメール詐欺（BEC）」参照）。詳しい情報を J-CSIP 内で共有するとともに、情報提供元の許可が得られた範囲で、事例の一般公開も行っている。

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

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

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

全体的には、2016 年度まで観測されてきた、諜報活動が目的と思われる、日本国内の特定の業界や組織に向けて多数のメールが送信されるような標的型攻撃は減少傾向にある。これは、攻撃者がより慎重に、目立たないように攻撃を行うようになったためであると考えられる。

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

(7) J-CRAT（サイバーレスキュー隊）

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

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

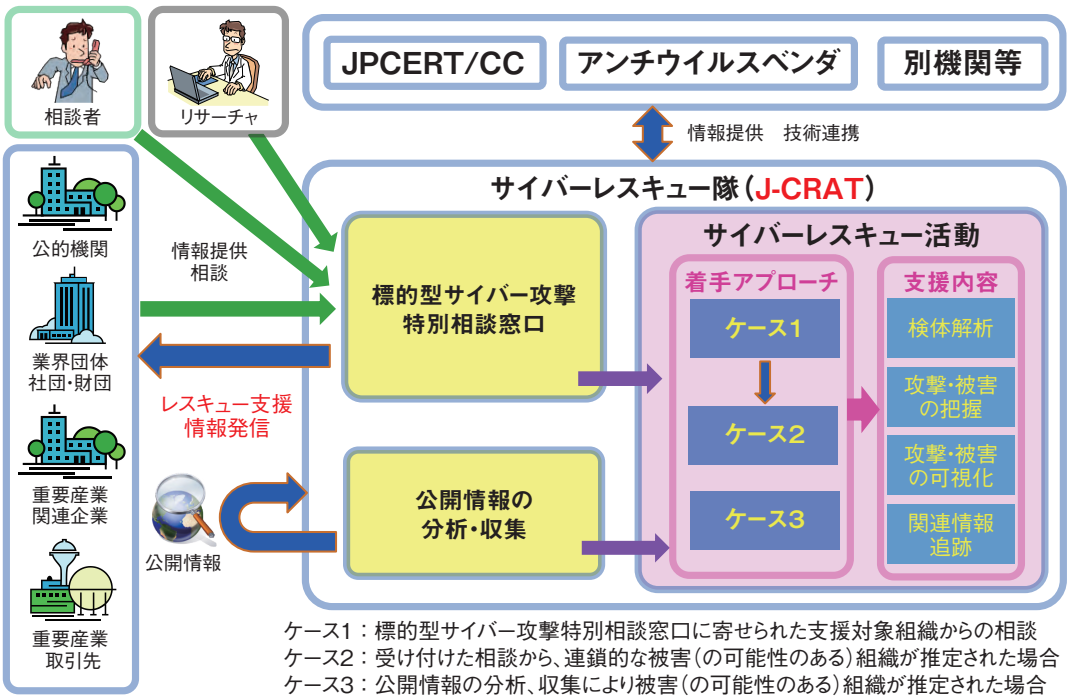
J-CRAT では、常時「標的型サイバー攻撃特別相談窓口」（以下、窓口）の運営と「公開情報の分析・収集」の二つの活動を実施している。

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

標的型サイバー攻撃の被害に遭っている、または遭っている可能性が高い組織のうち、特に公的機関や業界団体、重要インフラ関連企業や取引先等サプライチェーンを構成する組織に対して、被害実態の確認と認知の支援、被害緩和の暫定対応における助言を「サイバーレスキュー活動」として実施している※73。また、窓口における対応の結果、必要があると判断した組織に対して、攻撃の期間・内容、感染範囲、想定被害等をヒアリングし、早急な対策着手が行えるよう、民間セキュリティ事業者への移行を前提とした助言を行っている（図 2-1-6）。

相談を受けた案件のうち、緊急を要する事案に対しては、「レスキュー支援」を行い、更に当該組織での対応が必要な場合は、隊員を派遣する「オンサイト支援」を行っている。それぞれの支援件数を表 2-1-2 に示す。2019 年度の活動実績を 2018 年度と比較すると、「相談件数」は 5.1% 減少しており、内訳を見ると「レスキュー支援件数」が 9.4% 増加している一方、「オンサイト支援件数」は 35.5% 減少している。

J-CRAT では、定期的に活動状況を公開するほか、情報収集活動や支援活動から得られた結果を技術レポートとして随時公開している。これらの取り組み等を通じ、被害組織におけるセキュリティインシデントに対する



■図 2-1-6　J-CRAT の活動の全体像とスキーム
（出典）IPA「サイバーレスキュー隊 J-CRAT（ジェイ・クラート）※74」

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

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

■表 2-1-2　J-CRAT の活動実績

速やかな対応力向上や、平時における標的型攻撃への対策力向上に資する活動を行っている。また、活動を通じて組織のセキュリティ人材の育成、標的型サイバー攻撃の連鎖の解明、及び攻撃の連鎖を遮断することによる被害の低減を推進していく。

2.1.3 総務省の政策

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

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

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

以下では本レポートに基づき、総務省の主な取り組みの状況を述べる。

(1)「IoT・5G セキュリティ総合対策」に基づく主な取り組み

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

(a) 脆弱性対策に関わる体制の整備に向けた主な取り組み

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

- 脆弱な IoT 機器の調査の実施

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

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

- IoT 機器のセキュリティ対策に関する技術基準の改正

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

(b) 5G のセキュリティ対策

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

- 全国 5G のセキュリティ対策
  5G のサイバーセキュリティを確保するため、第 5 世代移動通信システムの導入のための特定基地局の開設に関する指針は、携帯電話事業者に対して、5G 導入に向けた特定基地局の開設計画の認定の際に、品質や普及等に関する条件並びにサプライチェーンリスクを含む十分なサイバーセキュリティ対策を講ずることを条件として付与した※83。
- ローカル 5G のセキュリティ対策
  ローカル 5G 導入に関するガイドラインにおいて、サプライチェーンリスク対応を含む十分なサイバーセキュリティ対策を講じる旨を明記するとともに、ローカル 5G の免許申請時の条件として付与した※84。
- 5G ネットワークの脆弱性対策
  総務省は 2019 年度から、5G ネットワークやその構成要素及びサービスについて、ソフトウェア・ハードウェアの両面から技術的検証を実施している。ソフトウェアを中心としたネットワークの脆弱性については、5G の通信インフラとしての機能保証のため、オープンソースソフトウェア等の解析、多種多様なパターンのデータ入力による異常動作確認（ファジング）、エシカルハッカー※85 による脆弱性調査、脅威分析の実施を検討した。またハードウェアの脆弱性については 5G ネットワークを構成するハードウェア上に故意に組み込まれた不正なチップのリスクに対応するため、AI を活用し回路情報から不正に改変された回路を検知する技術や、電子機器外部で観測される情報から不正動作を検知する技術を開発した。2020 年度以降は検知技術の改良、改変や不正動作への対策の検証を行い、また、5G ネットワーク上での運用面の課題等について検討する予定である。

(c) 研究開発の推進の状況

「IoT・5G セキュリティ総合対策」に基づく研究開発の推進状況を述べる。

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

(d) 民間企業等におけるセキュリティ対策の促進

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

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

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

(e) 人材育成の強化

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

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

(2) その他の取り組み

総務省のその他の取り組みについて述べる。

(a) クラウドサービスのセキュリティ対策

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

価制度（ISMAP）」参照）。

（b）「自治体情報セキュリティ対策の見直しについて」の公表

総務省は、2019 年 12 月より、「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会」を開催し、2020 年 5 月「自治体情報セキュリティ対策の見直しについて」を公表した※93。これは自治体情報セキュリティ対策見直しに関わる具体的な施策を取りまとめたものであり、総務省に対して、次期自治体情報セキュリティクラウドの在り方についての自治体への助言や、「地方公共団体における情報セキュリティポリシーに関するガイドライン※94」の改定等を提言している。

（c）トラストサービスの在り方の検討

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

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

2.1.4 警察によるサイバー犯罪対策

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

2019 年度の警察におけるサイバーセキュリティ重点施策への取り組み状況及びサイバー犯罪の情勢等について述べる。

（1）警察における主な取り組み

「サイバーセキュリティ重点施策」は、「サイバー空間の脅威への対応の強化」「警察における組織基盤の更なる強化」及び「国際連携及び産学官連携の推進」を主な柱としている。この戦略を踏まえ、2019 年度の警察におけるサイバー犯罪対策の主な取り組みについて述べる。

（a）サイバー空間の脅威への対応の強化

警察は先端技術を有する全国約 8,100 の事業者等（2020 年 1 月現在）との間で、情報窃取を企図したとみられるサイバー攻撃に関する情報共有を行う枠組みとして「サイバーインテリジェンス情報共有ネットワーク」を構築している。2019 年中のサイバーインテリジェンス情報共有ネットワークを通じて把握した標的型攻撃の件数は 5,301 件であった※100。標的型攻撃のうち、同じ文面や不正プログラムが 10 ヵ所以上に送付される「ばらまき型」攻撃が多発し、全体の 90% を占め、引き続き高い割合となった。

警察では、サイバー攻撃事案で使用された不正プログラムの解析等を通じて把握した国内の C&C（Command and Control）サーバの機能停止（テイクダウン）を、サーバを運営する事業者等に働きかけることで促進している。警察が把握した C&C サーバを運営する事業者に対し、不正な蔵置ファイルの削除を依頼する等して C&C サーバの無害化措置が執られた結果、2019 年中に 16 台の機能停止が実施された。

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

（b）警察における組織基盤の更なる強化

警察では、サイバー空間の脅威への対処に関する人

材基盤を強化するため、サイバー犯罪・サイバー攻撃の捜査及び情報通信技術に関する知識等を有する人材の育成を推進している。2019 年 4 月、警察におけるサイバーセキュリティ戦略の改定を踏まえ「サイバー空間の脅威への対処に係る人材育成方針」を改定し、サイバー空間の脅威に対する対処能力の強化を図ることとした。更に、警察全体で計画的な人材育成を推進するために 2011 年より行われているサイバー犯罪等対処能力検定の初級に全警察官を合格させる、等を含む「サイバー空間の脅威への対処に関する人材の育成計画」を策定し、都道府県警察もこの計画や各都道府県警察の実情を踏まえた計画を策定または見直すことが指示された[※101]。

(c) 国際連携及び産学官連携の推進

警察は、一般社団法人日本サイバー犯罪対策センター（JC3：Japan Cybercrime Control Center）等と連携し、産学官の情報や知見をサイバー犯罪・サイバー攻撃の取締り等に活用している。

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

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

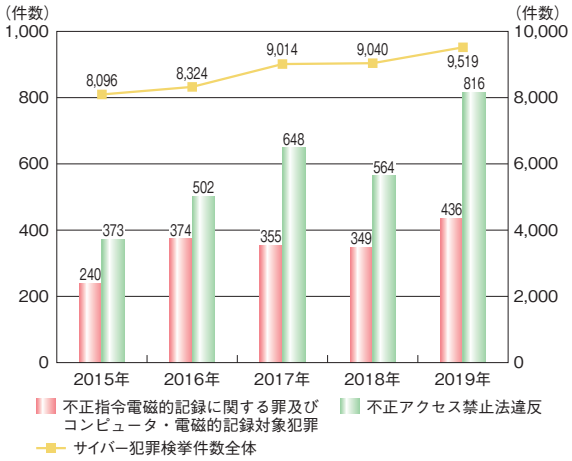
その他、2019 年 10 月フランスで開催された G7 ローマ／リヨングループに設置されたハイテク犯罪サブグループ会合、2019 年 11 月タイ・バンコクで開催された ASEAN + 3 国際犯罪閣僚会議及び日・ASEAN 国際犯罪閣僚会議等に警察庁から幹部・担当者が出席し、テロや国際犯罪への対策について各国代表と協議した[※104]（サイバーセキュリティに関する政府間連携については「2.2.1 国際社会と連携した取り組み」参照）。

(2) サイバー犯罪の検挙件数等

2019 年におけるサイバー犯罪の検挙件数、主な検挙事例について述べる。

(a) 2019 年のサイバー犯罪の情勢、検挙件数

警察によれば、サイバー犯罪の検挙件数は増加傾向

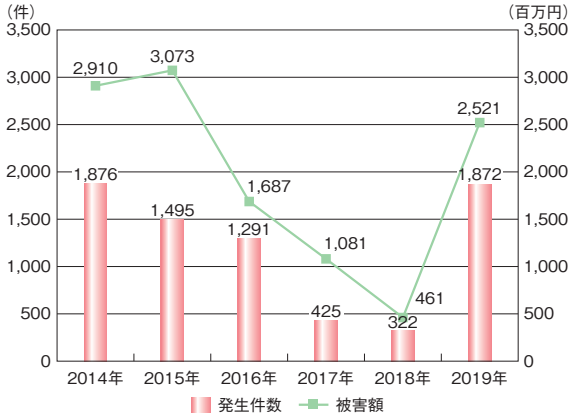


■図 2-1-7　サイバー犯罪検挙件数推移
（出典）警察庁「令和元年におけるサイバー空間をめぐる脅威の情勢等について[※100]」を基に IPA が作成

にあり、2019 年の検挙件数は 9,519 件と過去最多であった（図 2-1-7）。その中で「不正アクセス禁止法違反」の検挙件数は 816 件、「不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪」の検挙件数は 436 件であり、いずれも過去 5 年間では最多であった。

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

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



■図 2-1-8　インターネットバンキングに係る不正送金事犯の発生件数と被害額の推移
（出典）警察庁「平成 30 年におけるサイバー空間をめぐる脅威の情勢等について[※105]」「令和元年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

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

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

(b) 主なサイバー犯罪の検挙事例

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

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

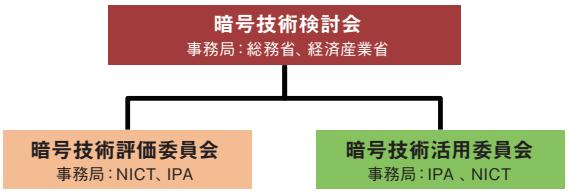
2.1.5 CRYPTRECの動向

電子政府の情報セキュリティを確保するため、総務省と経済産業省、NICT、及び IPA は安全性と実用性に優れた暗号技術を選び出すことを目的に、CRYPTREC（Cryptography Research and Evaluation Committees）を組織している。CRYPTREC では、電子政府システムでの利用を推奨する暗号アルゴリズム（CRYPTREC 暗号リスト※110）の安全性を評価、監視し、暗号技術の適切な実装や運用法を調査、検討している。

(1) 2019 年度の体制

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

委員会には、暗号技術の安全性評価を中心とした技術課題を主に担当する「暗号技術評価委員会」と、セキュリティ対策の推進、暗号技術の利用促進に向けた環境整備を主に担当する「暗号技術活用委員会」が設置されている（図 2-1-9）。



■図 2-1-9　CRYPTREC の体制

暗号技術検討会と両委員会の主な役割は以下のとおりである。

- 暗号技術検討会
  CRYPTREC 活動計画の承認、委員会が作成する各種成果物の承認等、政策的な判断を含む総合的な観点から電子政府の安全性及び信頼性を確保する活動を推進する。2019 年度には、量子コンピュータが実用化されても安全性が保てると期待される暗号（耐量子計算機暗号）を含む新たな暗号技術の動向等を踏まえ、次期 CRYPTREC 暗号リストに求められ

る要件や課題等を整理するため、傘下に「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」（以下、暗号の在り方 TF）が設置された。

- 暗号技術評価委員会
  暗号技術に対する攻撃技術動向の調査や安全性評価等、暗号技術における技術的信頼に関する検討を担当する。傘下には、公開鍵暗号の中長期的な安全性の検証や新世代暗号に係る調査等を行う「暗号技術調査ワーキンググループ」が設置されている。
- 暗号技術活用委員会
  セキュリティ対策の推進、暗号技術の利用促進等に寄与する運用ガイドラインの整備を中心とした、暗号利用に関する課題の検討を担当する。2018 年 5 月に一部改訂した「SSL/TLS 暗号設定ガイドライン」を大幅に見直すため、2019 年度には傘下に「TLS 暗号設定ガイドライン WG」が設置された。

(2) 2019 年度の主な活動

2019 年度の暗号技術検討会及び各委員会の主な活動内容・成果について以下に述べる。

(a) 暗号技術検討会

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

また、CRYPTREC 暗号リスト改定に向けた暗号の在り方 TF での検討内容が報告され、審議の結果、承認された。承認された内容は以下のとおりである。

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

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

(b) 暗号技術評価委員会

CRYPTREC 暗号リストに掲載されている暗号技術の安全性と実装性に関わる監視活動のほか、2019 年度の主な活動内容・成果は以下のとおりである。

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

(c) 暗号技術活用委員会

2019 年度には、安全な暗号利用に関する運用ガイドラインを整備する観点から、「暗号鍵管理システム設計指針（基本編）」及び「TLS 暗号設定ガイドライン」の作成を行った。

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

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

2.2 国外の情報セキュリティ政策の状況

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

2.2.1 国際社会と連携した取り組み

2018 年度に引き続き、日本政府は 2019 年度も米国、欧州、ASEAN 等の諸国とのサイバーセキュリティに関する連携協議や演習を実施した。それらの活動から主な取り組みを紹介する。

(1) G20 大阪サミット

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

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

(2) 日米のサイバー連携

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

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

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

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

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

(3) EU諸国とのサイバー連携

2019年は、EU、フランス、英国とのサイバー協議が行われた。

(a) 日EUサイバー対話

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

(b) フランスとのサイバー協議

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

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

(c) 英国とのサイバー協議

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

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

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

(4) ウクライナ・ロシアとのサイバー協議

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

(a) 日露サイバー協議

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

(b) 日ウクライナサイバー協議

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

(5) ASEAN とのサイバー連携

ASEAN 地域における政府レベルの連携施策について紹介する。

(a) 日・ASEAN 情報セキュリティ政策会議

2019 年 10 月 29 ～ 30 日、タイ・バンコクにて第 12 回日･ASEAN 情報セキュリティ政策会議（以下、政策会議）が開催された※129。本会議は、サイバーセキュリティ分野における ASEAN 諸国との連携強化を目的として 2009 年より開催されている。

第 12 回政策会議は日本・タイが議長国となり、日本から NISC、総務省、経済産業省の審議官、ASEAN 加盟国からサイバーセキュリティ・情報通信関係政府機関の局長・審議官等が参加した。同協議では、第 11 回政策会議で合意された 8 項目（サイバー演習、重要インフラ保護、能力構築、インシデント相互通知等）の活動状況を確認するとともに、今後の活動として情報共有体制、インシデント対処体制確立に向けた演習、重要インフラ保護に関するワークショップ実施の取り組み、能力構築・意識啓発に関する協力の推進等が議論され、活動の継続が確認された。

(b) ASEAN 地域フォーラム

ASEAN 地域フォーラム（ARF：ASEAN Regional Forum※130）は、ASEAN 地域の安全保障環境の向上を目的としたフォーラムで、日本政府は連携を継続している。サイバーセキュリティに関しては、シンガポール・マレーシアと共同で「サイバーセキュリティに関する ARF 会期間会合（ARF-ISM on ICTs Security）」（以下、会期間会合）を立ち上げ、2018 年 4 月より活動が始まっている。

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

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

(c) ASEAN 諸国向けの演習・インドとの連携

2019 年 9 月 9 ～ 12 日、経済産業省と IPA は米国政府と連携し、ASEAN 加盟国を含むインド太平洋地域諸国を対象とする「インド太平洋地域向け日米サイバー演習」を東京にて実施した※15。同演習は制御システム等の重要インフラ防御に関するもので、ASEAN 及びインド太平洋地域から政府関係者・重要インフラ事業者等 35 名が参加した（演習の内容は「2.3.2 (1) 中核人

材育成プログラム」参照）。

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

(6) セキュリティ連携に関する国際会議

サイバーセキュリティの国際連携に関する主な会議として、2019 年度は慶應義塾大学主催のサイバーセキュリティ国際シンポジウム等が開催された。

(a) 第 9 回サイバーセキュリティ国際シンポジウム

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

(b) 情報セキュリティ国際シンポジウム

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

(c) サイバー・イニシアチブ東京 2019

世界各国の民間のセキュリティ専門家を招いたサイバー・イシアチブ東京 2019 が、2019 年 12 月 12 ～ 13 日に開催された※139。日本からは高市早苗総務大臣、梶山弘志経済産業大臣、河野太郎防衛大臣、鈴木馨祐外務副大臣等が講演したのを始め、関係省庁のセキュリティ関係者、国内・海外の民間有識者が参加して安全保障、大規模国際イベント・重要インフラの防衛、5G、AI 等のデジタル化革新技術の課題について議論を行った。

2.2.2 米国の政策

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

(1) 米中貿易摩擦交渉の推移

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

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

(2) 新型コロナウイルス対策をめぐる米中関係悪化

2020 年 3 月以降の新型コロナウイルスの国内感染拡

大と景気後退は米国を大きく揺さぶっている。トランプ大統領は同年1月、中国発の新型コロナウイルスの蔓延について経済アドバイザー等から警告を受けていたが、当初はこれを無視したといわれる※143。世界保健機構（WHO：World Health Organization）のパンデミック宣言後、トランプ大統領は3月13日に国家非常事態を宣言※144、感染検査・治療対策に最大500億ドル（約5兆4,000億円）の連邦政府予算をあてるとした。しかし、ニューヨーク州を筆頭に被害が激増、経済的な影響も甚大となり、初動対策の遅れに対する批判が相次いだ。

米中政府間では、2月初旬の中国滞在者の米国渡航制限以来、感染拡大の責任について非難の応酬が始まっていたが、トランプ大統領は4月に入り、WHOに対してパンデミックへの警告が不十分で、中国の影響を小さく見せていると批判、資金拠出の停止を発表した※145。同大統領は更に、中国がパンデミックについて「故意の責任があるなら報いを受けるべき」と中国を正面から批判※146、5月には新型コロナウイルスが中国湖北省武漢にあるウイルス研究施設から流出したものか調査中であるとした※147。これらの発言は自身への批判をかわすためとも見られるが、中国への厳しい姿勢はパンデミックに苦しむ米国の世論となっており、欧州からも中国が情報を隠ぺいしたとの批判の声があがっている※148。米国政府は習近平主席への直接的な批判を避けてはいるものの、一時修復に向かった米中関係は急激に悪化している。

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

(3) 国防権限法

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

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

(4) 議会におけるサイバーセキュリティ戦略検討

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

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

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

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

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

(5) DoD の政策

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

(a) 抑止的なサイバー軍の活動

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

(b) 防衛調達における新しいフレームワークの採用

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

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

(c) 民間 IT 基盤の活用

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

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

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

(d) AI 倫理原則の採用

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

のである。

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

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

(6) DHS 及び商務省の政策

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

(a) サプライチェーンセキュリティ対策の推進

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

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

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

(b) 敵対的勢力からのサイバー攻撃の監視

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

(c) 新型コロナウイルス対策としてのセキュリティ

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

国ではCISAがいち早く新型コロナウイルス封じ込めと緩和のための情報共有を支援すると宣言し、同年3月6日に新型コロナウイルス関連詐欺メール・詐欺サイトに関する注意喚起[※176]を、また3月18日に重要インフラ保護、サプライチェーンの維持、リモート業務の保護、新型コロナウイルス関連詐欺対策を含むリスク管理ガイダンスを公開した[※177]。詐欺被害に関してはFBIも別途注意をよびかけた[※178]。

また、CISAは英国国家サイバーセキュリティセンター（NCSC：National Cyber Security Centre）と共同で、新型コロナウイルスを話題とする標的型攻撃が急増する中、セキュリティ的に脆弱な環境でテレワークが行われている、として同年4月8日に注意喚起を行った[※179]。更に同年5月5日、CISAとNCSCは続報として、医療・ヘルスケア関連組織が攻撃対象になっており、特に製薬企業・医療研究機関に対し研究データや知的財産データの窃取を狙っている、と警告した[※180]。更にCISAは4月24日、遠隔会議システム等のテレワークのツールに対する攻撃が急増しているとして、テレワーキングのセキュリティに関するガイダンスを公開した[※181]。

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

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

2.2.3 欧州の政策

2020年2月1日、英国は正式にEUを離脱した[※183]。アイルランドと北アイルランドの国境問題等で懸念されていた合意なしの離脱はかろうじて避けられ、2020年12月31日までを移行期間としてEU法制の適用を継続し、その間に英国・EU間の新しい自由貿易協定（FTA：Free Trade Agreement）等を締結することとなった。ただし、本当に厳しい交渉は移行期間が始まってからであり、難航するという見方もある[※184]。以下では、英国を含むEU諸国のセキュリティ・データ保護に関する動向について述べる。

(1) 英国・EUの連携交渉に関する論点

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

(a) 国内の法執行

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

(b) 国外の防衛

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

(c) データの妥当性

データの妥当性とは、英国・EU間の自由なデータ移

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

(d) サイバーセキュリティ

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

(2) GDPR実施の状況

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

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

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

このほか、2019年度に高額の制裁金が課された事例としては以下のものがある。

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

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

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

(3) EUサイバーセキュリティ法の施行状況

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

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

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

(a) 認証フレームワークの構築状況

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

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

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

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

(b) プライベート認証に関する議論

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

(4) 5G導入に関するセキュリティ検討の状況

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

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

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

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

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

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

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

2.2.4 アジア太平洋地域でのCSIRTの動向

アジア地域の多くの国では各国の窓口となる National CSIRT が既に設立され、運用が進んでいる。ここ数年は、サイバーセキュリティ戦略や、新たな法律によって、National CSIRT 及び所管省庁の権限を強化したり、役割を明文化したりする動きが継続している。一方、南太平洋地域では National CSIRT がまだ存在しない国が多いが、新規設立に向けた動きが近年活発になっている。本項では、アジア太平洋地域における CSIRT の機能強化や新規設立に関する動きと、CSIRT 間の相互連携の実態について述べる。

(1) CSIRT の設立・機能強化の動き

各国・地域の CSIRT の設立、機能強化の動きについて述べる。

(a) 台湾

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

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

(b) 韓国

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

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

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

(c)ニュージーランド

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

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

(d)南太平洋地域の国々

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

(2)アジア太平洋地域のCSIRT間連携

アジア太平洋地域全体のCSIRTからなるコミュニティとして、APCERT（Asia Pacific Computer Emergency Response Team：アジア太平洋コンピュータ緊急対応チーム）※236があり、地域内で発生したインシデント対応における連携の円滑化や、サイバー脅威等に関する情報共有・技術交流の推進を目的に活動している。2003年の設立当初、参加メンバーは12の国・経済地域の15チームだったが、地域内でNational CSIRTの立ち上げが進んだことや、CSIRTコミュニティへの参加を通じた情報共有等の重要性が高まったことから年々メンバーが増え、2020年5月末現在22の国・経済地域の31チームが、オペレーショナルメンバーとなっている（図2-2-1）。

JPCERT/CCは、2003年のAPCERT設立当初から事務局を務め、運営委員会の一員として組織運営を支えている。また、JPCERT/CCが主導するネットワーク定点観測共同プロジェクト「TSUBAME」に参加するAPCERTメンバーも多く、APCERT内にワーキンググループを設けて、センサーを用いたサイバー脅威動向の観測や情報共有を推進している。2020年5月現在、TSUBAMEにはAPCERTメンバーを中心に18の国・経済地域から23チームが参加し、観測結果を共有している※237。

APCERTの主な活動は、年次サイバー演習の実施、年次報告書の発行及び年次会合の開催である。2019

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

年のサイバー演習は、「企業ネットワークからの情報漏えい」をテーマに実施された※238。同演習には、APCERT のオペレーショナルメンバーのうち合計 20 の国・経済地域から 26 チームが参加した。年次報告書は、APCERT 全体としての活動に加えて各チームの組織概要や、対応したインシデント統計等をまとめた文書で、Web サイトで公開されている※239。

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

このほか、APCERT では能力開発のための取り組みとして、電話会議システムを利用してインシデント対応に関するノウハウを教えるオンライントレーニングを 2014 年以来継続しているほか、年次会合の場を利用して技術的なトレーニングのワークショップも開催されている。

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

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

のサイバーセキュリティ能力の向上や、組織間の連携促進を目指している。

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

COLUMN

5Gがもたらす恩恵とプライバシーリスク

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

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

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

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

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

2.3 情報セキュリティ人材の現状と育成

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

2.3.1 情報セキュリティ人材の状況

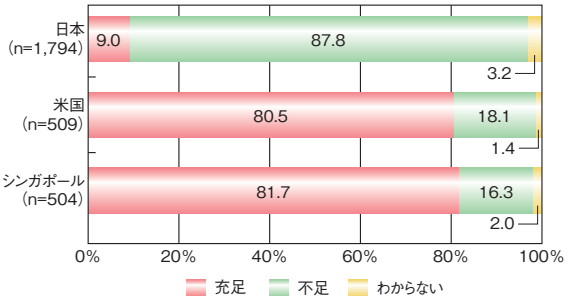
ここ数年来、政府や民間の組織等において国内のセキュリティ人材育成のための活動が行われてきた。経済産業省の 2016 年の調査で「2020 年に国内で 19 万人不足」という予想が発表され※250、その後、セキュリティ人材不足を解消するために、企業においてセキュリティに関わる役割定義や持つべきスキルに関する議論が行われた。また、ユーザ企業、IT ベンダ／セキュリティベンダでセキュリティ関連タスクの概念整理が行われ、ユーザ企業におけるセキュリティ体制については、経営層、戦略マネジメント層、実務者層・技術者層等に整理された。

2018 年度から政府や民間の組織等において、より実際的に人材育成を進める活動として、セキュリティ人材の役割定義に紐付くタスク・スキルの洗い出しを行うとともに、具体的な施策として人材育成を行う試みの有効性に関する検証が行われている。以下にセキュリティ人材に関する課題の現状と、各所で行われている活動の概要を紹介する。

(1) セキュリティ人材不足に関する認識

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

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



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

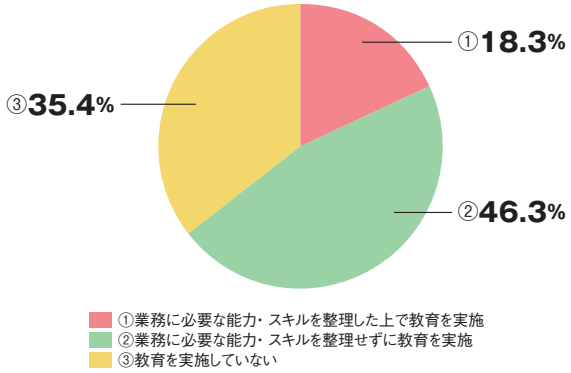
また、日本においては、6 割以上の企業がセキュリティ人材の育成を実施しているが、業務に必要な能力・スキルを整理した上でセキュリティ教育を実施しているのは全体の 2 割弱しかなく（次ページ図 2-3-2）、セキュリティ人材の育成・教育における課題として、適切なキャリアパスの不足を一番の課題として挙げている（次ページ図 2-3-3）。

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

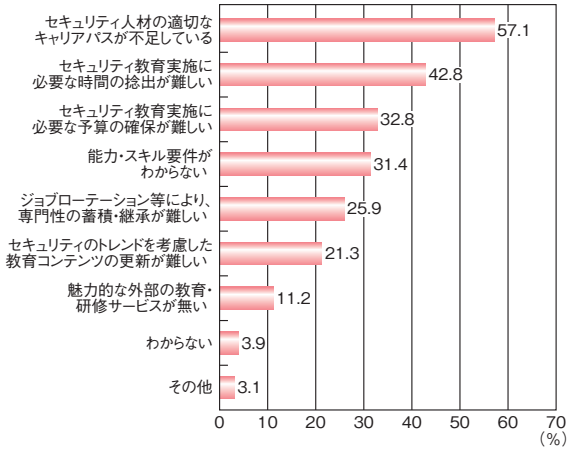
	日本 (n=161)	米国 (n=410)	シンガポール (n=412)
1 位	想定よりも有事対応が少ない	セキュリティ業務が標準化され、役割分担が明確	セキュリティ業務が自動化・省力化されている
2 位	セキュリティ業務の量が少ない	想定よりも有事対応が少ないため	想定よりも有事対応が少ない
3 位	セキュリティ業務が標準化され、役割分担が明確	経験豊富なメンバーで対応	セキュリティ業務が標準化され、役割分担が明確
4 位	経験豊富なメンバーで対応	セキュリティ業務が自動化・省力化されている	セキュリティ業務の量が少ない
5 位	セキュリティ業務を外部委託している	外部から経験豊富な人材を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

※その他の選択肢：社内・グループ内の異動で人員を補充／その他／わからない

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



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



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

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

(2) 経済産業省及び関連省庁等の取り組み

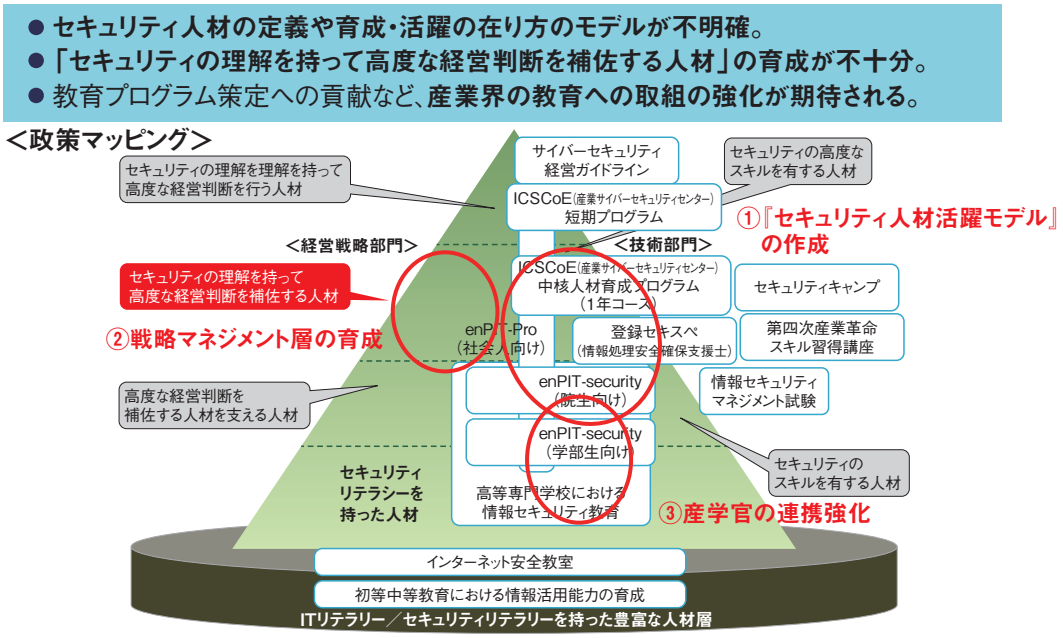
経済産業省は、産業サイバーセキュリティ研究会 WG2 においてサイバーセキュリティ人材育成・活躍促進パッケージとして、セキュリティ人材育成に関わる活動を検討している（図 2-3-4）。

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

(a) セキュリティ人材活躍モデル

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

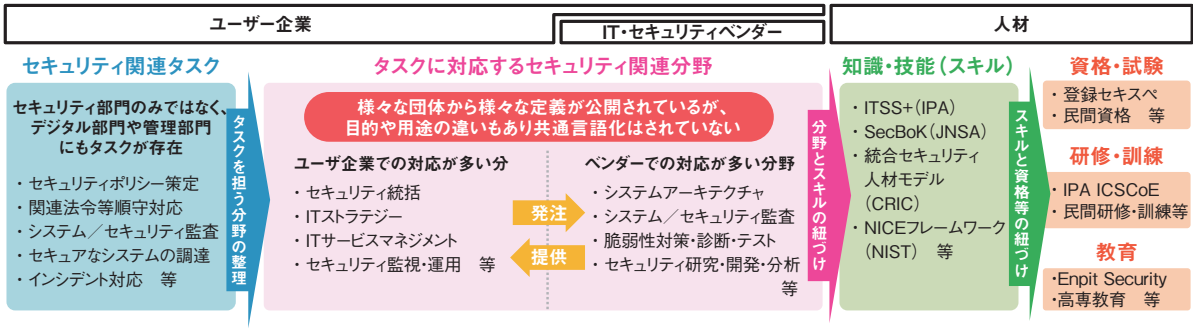
また、「セキュリティ人材活躍モデル」として企業におけるセキュリティ関連分野の概観についても検討している。図 2-3-6 に示すのは、2018 年度に行ったユーザ企業におけるセキュリティ体制・人材に関する概念整理を基に、人材を経営層、戦略マネジメント層、実務者・技術者層に分け、更に典型的な組織例とそれらに紐付けられるタスク例を挙げるとともに、ユーザ企業全体のセキュリティ関連分野を整理したものである（ただし、検討



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

セキュリティ人材の全体像の可視化や育成・活躍促進のためのモデルの構築

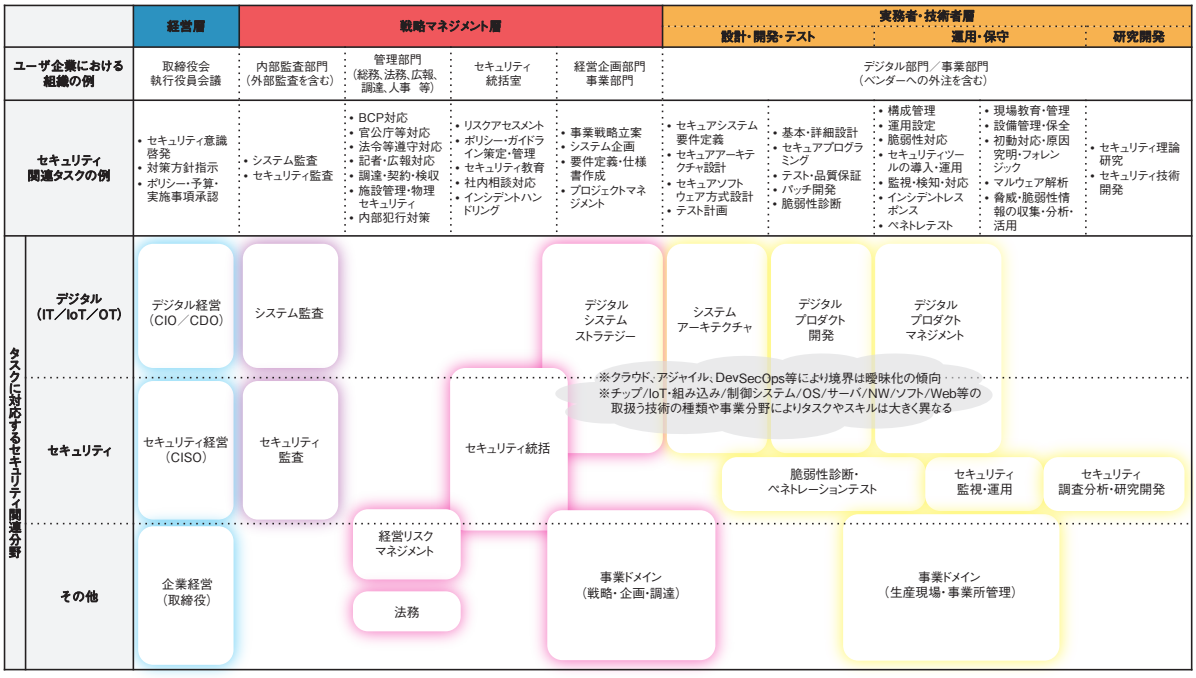
- ITSS+(セキュリティ領域)改定により、各分野に紐づくセキュリティ関連タスク等を整理中。
- その後、各分野に関するキャリアパス事例集や、ユーザ企業における体制・人材確保のプラクティス集等を開発。



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

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

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



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

途中であり、最終的なものではない)。

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

(b) 人材育成プログラム

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

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

産学官が協力してセキュリティ人材を育成する活動として、独立行政法人国立高等専門学校機構に対して、IPA、一般社団法人サイバーリスク情報センター 産業横断サイバーセキュリティ人材育成検討会（CRIC CSF）、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA：Japan Network Security Association）といった業界団体や企業が 2018 年度に引き続き協力している。具体的には、キャリア教育、講師派遣や教材開発等の活動を行っており、例えば、CRIC CSF は高等専門学校に在籍する非情報系学科の学生に向けたキャリア教育として、ユーザ企業におけるセキュリティや IT の活用を知ってもらうためのビデオ教材の作成を、また、JNSA は情報系学科の学生に向けて、ゲーム形式の教材製作やセキュリティ関連イベント・講習への講師派遣を行っている。

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

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

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

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

(3) 一般社団法人日本経済団体連合会の取り組み

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

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

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

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

- CRIC CSF：
  「人材定義リファレンス※259」

「OT セキュリティ人材スキル定義リファレンス※260」

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

(4) まとめ

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

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

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

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

2.3.2 産業サイバーセキュリティセンター

我が国の経済・社会を支える重要インフラ※262 や産業基盤のサイバー攻撃に対する防御力を強化するため、IPA は 2017 年 4 月に産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）を発足させた。

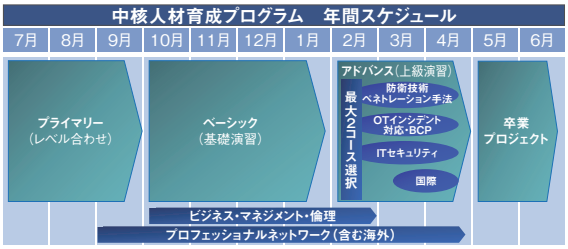
ICSCoE では、重要インフラや産業基盤のサイバーセキュリティリスクに対応する人材・組織・システム・技術を生み出していくため、「人材育成事業」「制御システムの安全性・信頼性検証事業」「攻撃情報の調査・分析事業」の三つを事業の柱としている。本項では、「人材育成事業」について述べる。

(1) 中核人材育成プログラム

ICSCoE は、2017 年 7 月、制御技術（OT：Operational Technology）と情報技術（IT）、マネジメント、ビジネス分野を総合的に学び、サイバーセキュリティ対策の中核となる人材を育成する「中核人材育成プログラム」を開始した。本プログラムでは、OT 及び IT 知識のレベル合わせからハイレベルな演習までを 1 年間のフルタイムで実施する。第 1 期は 76 名、第 2 期は 83 名が参加し、2019 年 7 月に開講した第 3 期では、電力・自動車・鉄道・化学・放送・通信・産業ベンダ等の幅広い業界から 69 名が参加した。

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

本プログラムは、過去の実施結果を踏まえて毎年カリキュラム及びスケジュールの改善を図っている。3 年目となる 2019 年度は、「アドバンス（上級演習）」において選択可能な演習を追加して複数コースを選択できるように見直しを実施した（図 2-3-7）。



■図 2-3-7　第 3 期中核人材育成プログラムの年間スケジュール

2019 年 9 月の海外派遣演習では、フランスにてセキュリティ専門家によるサイバーレジリエンスの強化を目的とした研究の講義を受講し、自動運転や鉄道制御の模擬システムを見学した。同年 12 月の海外派遣演習では、英国にて政府・自動車業界・海運業界及び起業家の代表者によるサイバーセキュリティの取り組みに関する講義を受講した。

また 2019 年 9 月には、米国政府と連携して制御システムのサイバーセキュリティ対策に関する「インド太平洋地域向け日米サイバー演習」を経済産業省と共催した※15。本演習には第 3 期の受講者及びインド太平洋地域から招聘した外国人受講者 35 名が参加し、米国の有識者による講演に加え、各国での制御システムセキュリティに関する課題や対策を参加者間で共有するワークショップ

を実施し、国境を越えた積極的な意見交換がなされた（ASEAN・インドとのサイバー連携については「2.2.1 (5) (c) ASEAN 諸国向けの演習・インドとの連携」参照）。

2018 年 7 月、中核人材育成プログラムの OB 会として、修了者コミュニティ「叶会※263」が発足し、2019 年夏以降、本プログラムを通じて培った人脈の活用、知見やノウハウの共有を目指し、地域活動や技術をテーマにする複数の部会が設置された。また 2019 年 11 月には、修了年次をまたがる縦のつながりの形成、最新情報及びノウハウ収集を目的とした叶会総会が開催された。第 1 期及び第 2 期の修了者に加え、2020 年 6 月に修了した第 3 期生も叶会へ参加しており、今後もコミュニティとしての規模を拡大しながら、お互いの顔が見える縦横の人的つながりを形成し、産業サイバーセキュリティに関する適時、適切な情報共有活動を継続することが期待される。

なお、中核人材育成プログラムの修了者は、情報処理の促進に関する法律の規定に基づき、後述する情報処理安全確保支援士試験の全部免除を受けることができる※264。

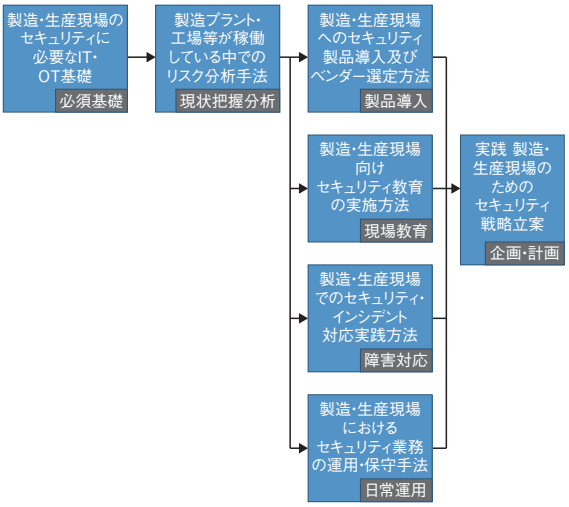
(2) 短期プログラム

ICSCoE では、セキュリティに関連するスキルの習得機会が十分でない部門責任者や現場責任者、及びセキュリティ実務担当者に向けて、数日間で学ぶ短期演習形式の「製造・生産分野の管理監督者層向けプログラム」「サイバー危機対応机上演習（旧名称、国際トレーニング）」「業界別サイバーレジリエンス強化演習（旧名称、業界別トレーニング）」「戦略マネジメント系セミナー」及び「制御システム向けサイバーセキュリティ演習」を実施している。

(a) 製造・生産分野の管理監督者層向けプログラム

制御系システムの企画・導入・運用・保守を行う部署や、製造・生産に使用する設備を担う部署の管理監督者向けのトレーニングとして、「製造・生産分野の管理監督者層向けプログラム※265」を 2019 年度に新設した。

具体的には、ICSCoE が第 2 期中核人材育成プログラム受講者とともに、セキュリティ向上における組織の課題を調査・分析した結果に基づき、上記の部署、及び現場の QC（Quality Control：品質管理）、カイゼン、KY（Kiken Yochi：危険予知）活動に取り組む部署等の管理監督者の能力育成のため、7 種の研修コースを実施した（図 2-3-8）。



■図 2-3-8　製造・生産分野の管理監督者層向けコース体系図

本プログラムを通じて、製造・生産現場のセキュリティに必要な IT・OT の基礎知識からセキュリティ戦略立案まで、現場が主体的に取り組むためのマネジメントスキルを身に着けることが期待される。

(b) サイバー危機対応机上演習（CyberCREST）

2019 年 11 月及び 2020 年 2 月に「サイバー危機対応机上演習（CyberCREST：Cyber Crisis RESponse Table top exercise）※266」を実施した。本演習では、制御システムを有する企業・団体のサイバーセキュリティ対策の統括責任者を対象とし、米国サイバー軍の退役軍人や重要インフラ関連企業のサイバーセキュリティ対策責任者等が講師やファシリテーターとなり、講義や演習を行った。

演習においては、東京 2020 オリンピック・パラリンピック競技大会を想定したサイバー攻撃のシナリオを基に、受講者は CISO（Chief Information Security Officer）や広報担当、事業部門長等の役割に扮して経営判断まで含めたプロセスを疑似体験した。講師が扮するステークホルダとの対話を通じて実践的なインシデント対応のフレームワークを学習するとともに、参加企業に合わせたインシデント対応（IR：Incident Response）計画や机上演習（TTX：Table Top Exercise）シナリオの作成方法についても理解を深めた。

本演習を通じて、経営者の判断をサポートするためのリスク分析、迅速かつ適切な対策の提示、政府機関やマスメディアを含む様々なステークホルダとのコミュニケーション等、CISO 等がインシデント対応時に求められる役割について理解を深め、実践につなげることが期待さ

れる。

(c) 業界別サイバーレジリエンス強化演習（CyberREX）

2019 年 8 月及び 9 月に電力、鉄道、ビル、自動車（製造部門）、ファクトリーオートメーション業界において CISO に相当する役割を担う人材や IT 部門、生産部門等の責任者・マネージャークラスの人材を対象として、「業界別サイバーレジリエンス強化演習（CyberREX：Cyber Resilience Enhancement eXercise by industry）※267」を実施した。

本演習は、部署・部門のサイバーセキュリティに関する対応力・回復力を強化するため、業界の最新動向、業界別に考慮すべきセキュリティ要件、安全性要件を織り込んだ構成とし、仮想企業を想定したシナリオ形式による実践演習を中心に進められた。受講者に加え、サイバーセキュリティの専門家や監督省庁の関係者も参加した形式でのグループ演習を行った。

(d) 戦略マネジメント系セミナー

2020 年 2 月に、セキュリティに関する方針・戦略・計画及び組織体制を策定する管理職向け、及びセキュリティ対策の実装・運用やセキュリティ体制の構築を担当する実務者向けの 2 コース構成で「戦略マネジメント系セミナー※268」を実施した。

NISC が提唱する「戦略マネジメント層」、及び経済産業省において示された「セキュリティ統括機能」の考えに基づき、サイバーセキュリティは経営課題であること、及び経営層を始めとする関係者が認知しておくべきセキュリティ機能の重要性を理解することを目指し、サイバーセキュリティ有識者の実務経験に基づく講演や、Society 5.0、DX 等の環境変化を踏まえた上で事業継続及び発展を実現するためのサイバーセキュリティ対策について講義を実施した。

(e) 制御システム向けサイバーセキュリティ演習

制御システムのサイバーセキュリティを担当する、または今後担当予定の人材を対象とした実務者向けプログラムとして、「制御システム向けサイバーセキュリティ演習※269」を 2019 年度に新設し、東京、名古屋、大阪で開催した。

本演習は制御システムのサイバーセキュリティを理解するための導入的な位置付けであり、制御システムへの攻撃の契機や手法、及び制御システムのサイバーセキュリティ対策の基礎を、簡易模擬システムを用いた実機演習（ハンズオン演習）で体験し、制御システムのセキュリティについて実践的に理解することを目的として実施した。

2.3.3 情報セキュリティ人材育成のための国家試験、国家資格制度

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

(1) 情報セキュリティマネジメント試験

企業・組織においては、組織が定めた情報セキュリティポリシーを部門内に周知して遵守を促し、部門の情報管理を実施する等、情報セキュリティ対策を推進する人材（情報セキュリティマネジメント人材）が必須である。こうした人材を育成するために、2016 年度春期より「情報処理技術者試験」の新たな試験区分として「情報セキュリティマネジメント試験」が実施されている。試験は年 2 回実施され、2019 年度の応募者数は 3 万 6,679 人であった※270。

同試験は、業種や組織を問わず、部門内で個人情報を取り扱う担当者や外部委託担当者、情報システム担当者等を主な対象者としている。2019 年度の受験者のうち 85.5%を社会人が占めている。更に業種別に見ると、IT 系企業が 52.6%、非 IT 系企業が 47.4%と、非 IT 系企業が半数近くを占めている。非 IT 系企業の業種も、製造業、サービス業等、幅広い業種の人が受験していることから、広く組織の情報セキュリティを推進する人材の強化に有効な試験と考えられていることがうかがえる※271。

(2) 情報処理安全確保支援士制度

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

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

情報処理安全確保支援士は、試験合格者が登録簿に登録されることにより資格を取得する、サイバーセキュリティ分野初の名称独占資格である。試験は年 2 回実

■図 2-3-9　登録セキスペのロゴマーク

施され、2019 年度の応募者数は 4 万 3,412 人であった。また、情報処理安全確保支援士の登録人数は、2020 年 4 月 1 日時点で 2 万 413 人となった※272。図 2-3-9 は、情報処理安全確保支援士の資格保有者（以下、登録セキスペ）、またはその所属企業・組織のみが使えるロゴマークである。

登録セキスペには法定講習の受講が義務付けられており、最新知識や実践的な能力の維持が求められる。法定講習は毎年 1 回のオンライン講習と 3 年に 1 回の実践講習からなり※273、受講者からは、「資料での学びに加え、経験者の意見を聞きながら、インシデント対応を体験できた」「登録セキスペとしての倫理面での責任を改めて感じた」等の声が上がっている※274。

ユーザ企業においては、事業とのバランスを取りながら、セキュリティを担保する役割を登録セキスペに担わせることで、IT を活用した事業促進をセキュアに進めることができる。IT ベンダ企業においては、登録セキスペが在籍することで、提供する機能やサービスの信頼性向上、社会的評価・信頼の向上、入札要件の充足等によるビジネスチャンスの拡大等のメリットが期待できる。本制度を活用している企業・組織へのインタビューでは、「セキュリティを任せたいとお客様に考えていただくには、信頼が必須であり、情報処理安全確保支援士制度は信頼を頂く枠組みの 1 つとして活用している」「情報セキュリティにおける社員の共通言語や、共通の認識・理解・レベルを作るために、情報処理技術者試験・情報処理安全確保支援士制度を活用している」といった声が上がっている※275。

なお、2020 年 5 月に「情報処理の促進に関する法律」の改正法が施行され、次の 2 点が変更になった※276。

・更新制の導入
・義務講習の実施事業者の追加

「更新制の導入」により、更新手続きを通じて、登録セキスペの登録情報の変更や、欠格事由に該当していないことを確認することができ、本制度の信頼性が向上する。また、これまで義務講習の対象は IPA が実施するものに限られていたが、一定の条件を満たした民間事業者等が実施する講習も対象に追加されたことで、登録セキスペの多様なニーズに応じることができる。

2.3.4 情報セキュリティ人材育成のための活動

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

(1) セキュリティ・キャンプ

セキュリティ・キャンプは、若年層の情報セキュリティ意識の向上、並びに将来第一線で活躍できる高度な情報セキュリティ人材を発掘・育成する場として、一般社団法人セキュリティ・キャンプ協議会と IPA が運営している。

2019 年 8 月 13 ～ 17 日に東京で 16 回目となる全国大会が開催され、76 名が参加した※277。また、主に若年層を対象としたセキュリティ・ミニキャンプも、セキュリティ人材育成に関心の高い地域（福岡／山形／山梨／愛知／北海道／広島／石川／沖縄／長崎）で開催された※278。更に、中学生を対象としたジュニアキャンプが高知で開催された※279。

その他、過去のセキュリティ・キャンプ全国大会を修了、または同等以上のスキルを持つ 25 歳以下の学生を対象に、更なる育成の場として、セキュリティ・ネクストキャンプが全国大会と同時に開催された※280。

一般社団法人セキュリティ・キャンプ協議会は、キャンプ修了生の情報セキュリティに関連する取り組みをテーマとしてプレゼンテーションを行う場を設け、優れた成果を上げた人や価値ある取り組みを表彰するセキュリティ・キャンプアワードも例年開催している※281 が、2020 年 3 月に予定されていた最終選考及び表彰式は新型コロナウイルスの影響で延期となった※282。また、2019 年 1 月に始まった Global Cybersecurity Camp の第 2 回が 2020 年 2 月 10 日～ 14 日に千葉県で開催され、日本を含めて七つの国・経済地域から 29 名が参加した※283。

(2) enPiT

enPiT（Education Network for Practical Information Technologies：成長分野を支える情報技術人材の育成

拠点の形成）は、情報技術を高度に活用して社会の具体的な課題を解決できる人材を育成するため、産学協働の教育ネットワークを形成し、PBL（Problem Based Learning:課題解決型学習）等の実践的な教育を推進・普及することを目的とした文部科学省の事業である。2012 ～ 2016 年度までは大学院生を対象とした事業「第 1 期 enPiT」が実施され、これを踏まえ 2016 年度（同年度は準備期間の位置付け）から、学部生を対象とした事業「第 2 期 enPiT」（以下、enPiT2）を開始している。

enPiT2 は、ビッグデータ・AI、セキュリティ、組み込みシステム、ビジネスシステムデザインの 4 分野を対象として教育プログラムを提供している。セキュリティ分野では、2019 年度は大学等 41 校、連携企業等 43 社・団体が参加した。このうち、東北大学を中核とした 14 の大学が、高度化する情報セキュリティの脅威を理解し、リスクマネジメントに必要な知識、基本技術、実践力を備えた人材を育成する Basic SecCap コースを運営しており、323 名が修了認定を取得した※284。

上記以外では、社会人を対象に情報科学技術分野を中心とする体系的かつ高度で短期の実践教育プログラムとして、enPiT-Pro が 2017 年度に開始されている※285。セキュリティ分野では、情報セキュリティ大学院大学、東北大学、大阪大学、和歌山大学、九州大学、長崎県立大学、慶應義塾大学の 7 大学が、enPiT-Pro Security※286 というプロ人材育成のための教育コースを幅広く展開している。

(3) SECCON 2019

JNSA は、日本における最大規模の CTF※287 大会である「SECCON 2019※288」を開催した。

2019 年 12 月 21 ～ 22 日の国際決勝大会では、64 ヵ国 799 チームの中からオンライン予選を勝ち抜いた 11 チームと、特別招待枠 3 チームの計 14 チーム（日本 4、韓国 2、中国 2、ロシア 1、ウクライナ 1、ポーランド 1、台湾 1、タイ 1、EAST ASIA チーム（東アジア連合チーム）1）が集まり、実力を競い合った。第 1 位（経済産業大臣賞）を獲得したのは日本チーム「NaruseJun」、第 2 位が韓国チーム「CodeRed」、第 3 位が中国チーム「Blue-Lotus」であった※289。

SECCON ではその他、CTF 未経験者でも参加可能な「SECCON Beginners※290」や、情報セキュリティに興味がある女性を対象とした「CTF for GIRLS※291」等のイベントを定期的に開催しており、実践的情報セキュリティ人材の発掘・育成、技術の実践の場の提供に取り組んでいる。

(4) 産学情報セキュリティ人材育成交流会

JNSA の産学情報セキュリティ人材育成交流会は、2012 年 2 月に発足し、今後の情報セキュリティ業界を支える人材を育成するためのインターンシップの支援活動を実施している。2019 年度も昨年度に引き続き、将来情報セキュリティ業界で活躍したいと考える学生に対し、インターンシップの受け入れを検討している企業との交流の場を提供する「産学情報セキュリティ人材育成交流会～これからの IT 人材のキャリアを考える－サイバーセキュリティの視点から－」を 2019 年 4 月 27 日に開催した。2019 年度は企業 17 社がインターンシップを実施した※292。

(5) サイバーセキュリティ経営戦略コース

東京工業大学社会人アカデミーでは 2020 年 1 月、MOT（技術経営）に関する社会人向けプログラムとして、キャリアアップ MOT「サイバーセキュリティ経営戦略コース」を開講した※293。ここで育成を目指すのは、サイバーセキュリティが企業・組織の経営に及ぼす影響を理解し、サイバーセキュリティ経営及びその戦略立案に求められる知識・能力を備え、企業・組織を先導する人材であり、多様な業界・業種から、経営者、マネージャー、若手等、多くの社会人が受講することを想定している。

本コースは、週 1 回、サイバーセキュリティ経営の経験を持つ産学官の有識者による関連技術・法制・世界情勢等の解説や、事例に基づく演習、討議等を含む全 14 回の講義で構成される。

2.4 組織・個人における情報セキュリティの取り組み

企業や政府、地方公共団体、教育機関、一般利用者の情報セキュリティの対策状況について、IPA による調査結果及び公表されている資料等を基に述べる。

2.4.1 企業における対策状況

情報セキュリティへの企業等の対策状況、経営層の課題認識、CISO 等の役割やセキュリティリスクマネジメントへの取り組みについて述べる。

(1) 情報セキュリティに対する経営層・CISO 等の取り組み状況

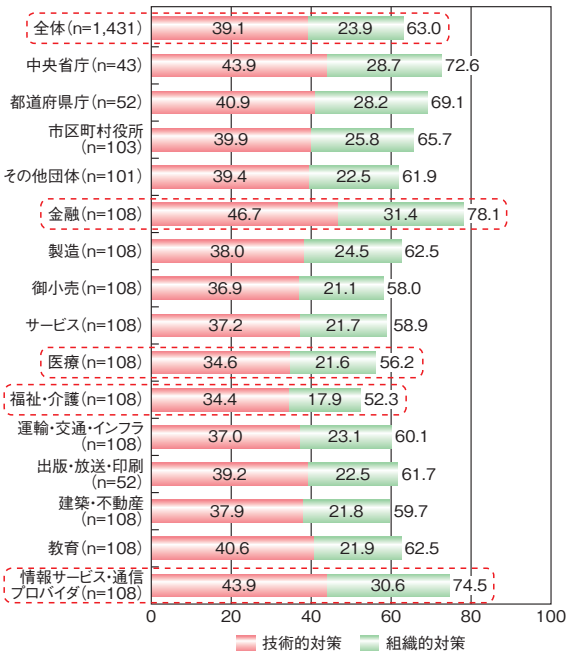
近年、企業経営においては、IT を活用した「攻めの経営」と情報資産やシステムを保護する「守りの経営」とを高いレベルで両立することが求められている。このためには、経営方針に基づき、セキュリティに関して企業内の調整や実務者層をリードする人材（CISO 等）、及び同方針に基づいた技術的・組織的なセキュリティ対策の実践が必要とされている。このような背景を踏まえ、企業の情報セキュリティ対策状況について、以下の資料を基に述べる。

- IPA：企業の CISO 等やセキュリティ対策推進に関する実態調査※294（国内の CISO 等を任命している企業 534 社を対象に調査。以下、IPA 実態調査）
- トレンドマイクロ株式会社（以下、トレンドマイクロ社）：法人組織におけるセキュリティ実態調査 2019 年版※295（国内企業 1,132 社及び官公庁自治体 299 団体を対象に調査。以下、トレンドマイクロ社調査）
- NRI セキュアテクノロジーズ社：NRI Secure Insight 2019（国内・海外企業 2,807 社を対象に調査。以下、NRI セキュアテクノロジーズ社調査）

(a) 業界ごとのセキュリティ対策状況

トレンドマイクロ社調査（図 2-4-1）によると、調査対象全体のセキュリティ対策包括度スコア※296 は 63.0 点となっており、業種別で見ると、「金融」が 78.1 点でトップ、「情報サービス・通信プロバイダ」が 74.5 点で続く。金融情報を扱う金融業界では技術的対策・組織的対策の両軸で対策が進んでいることが分かる。また、「情報サービス・通信プロバイダ」においても様々な情報をオンラインで取り扱うことから、セキュリティ対策が進んでいることがうかがえる。

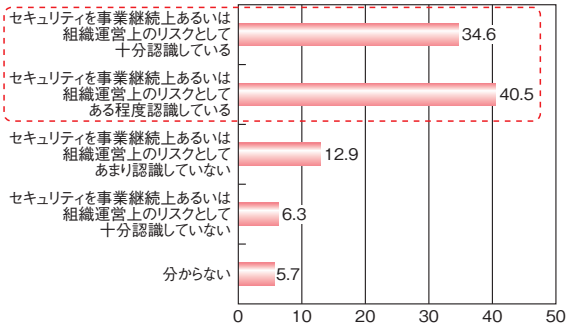
一方、スコアが最も低かったのは「福祉・介護」の 52.3 点で、「医療」が 56.2 点で続く。いずれも患者の医療情報や要介護者の機微情報等を取り扱っており、本来であれば高いセキュリティが求められる業種にもかかわらず、情報セキュリティの観点では他業種に遅れをとっている状況が浮き彫りとなっている。



■図 2-4-1　セキュリティ対策包括度スコア（業種別）
（出典）トレンドマイクロ社「法人組織におけるセキュリティ実態調査 2019 年版」を基に IPA が編集

(b) 経営層のセキュリティに対する意識

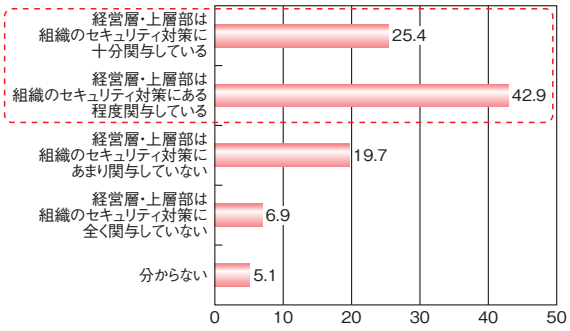
情報セキュリティに関する経営層・上層部のリスク認識について、トレンドマイクロ社調査（図 2-4-2）によると、



■図 2-4-2　情報セキュリティに関する経営層・上層部のリスク認識（n=1,431）
（出典）トレンドマイクロ社「法人組織におけるセキュリティ実態調査 2019 年版」を基に IPA が編集

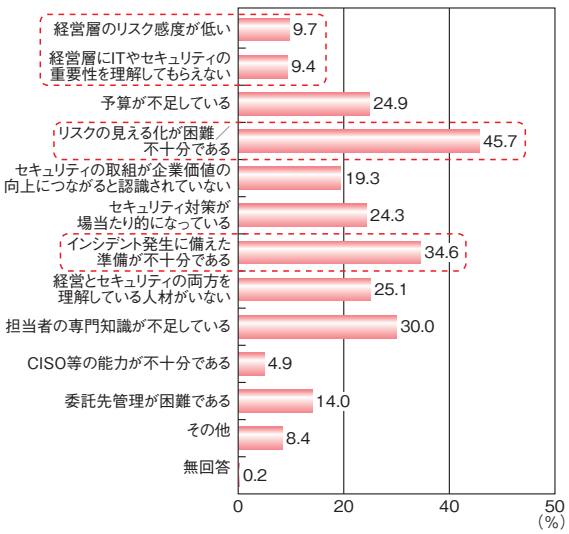
セキュリティを事業継続上あるいは組織運営上のリスクとして認識している経営者の割合は 75.1% と高い割合となり、昨年調査の 70.2% から 4.9 ポイント増加した。

また、図 2-4-3 に示すように、経営層・上層部のセキュリティ対策への関与について「十分関与している」「ある程度関与している」と答えた割合は合わせて 68.3% となっており、図 2-4-2 のリスク認識に比べてやや割合は低いものの、経営層の約 7 割がセキュリティに関与している状況がうかがえる。



■図 2-4-3　セキュリティ対策に関する経営層・上層部の関与度（n=1,431）
（出典）トレンドマイクロ社「法人組織におけるセキュリティ実態調査 2019 年版」を基に IPA が編集

企業の課題認識について、IPA 実態調査（図 2-4-4）によると、CISO 等を任命している企業では、「リスクの見える化が困難／不十分である」（45.7%）が最も多く、次いで「インシデント発生に備えた準備が不十分である」（34.6%）が多かった。これらの課題解決、対策強化の取り組み事例としては「2.4.1 (2) (a) スモールスタートでのリスク把握」「2.4.1 (2) (b) 業務に即したインシデント対応

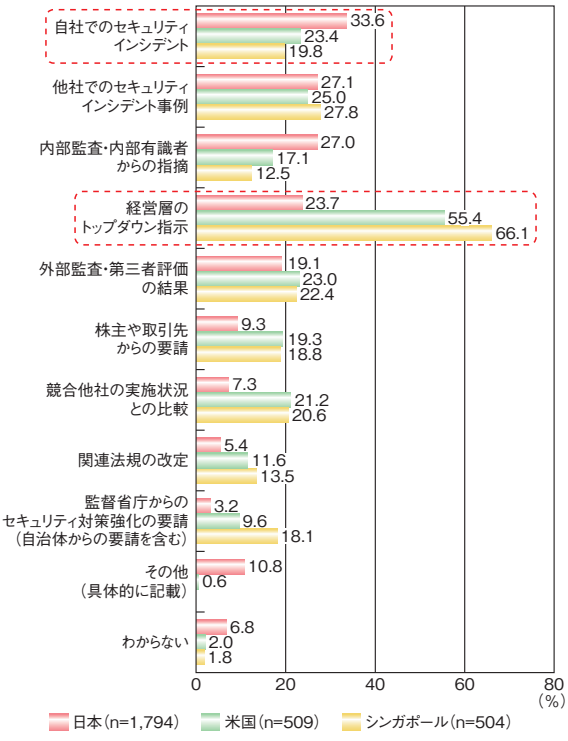


■図 2-4-4　サイバーセキュリティに関する企業の課題認識（n=534）
（出典）IPA「企業の CISO 等やセキュリティ対策推進に関する実態調査」を基に IPA が編集

演習や訓練」を参照いただきたい。

一方、「経営層のリスク感度が低い」や「経営層に IT やセキュリティの重要性を理解してもらえない」と回答した企業はそれぞれ約 10%にとどまり、当該企業の多くの経営層は、リスク把握やセキュリティの重要性を認知・理解していることがうかがえる結果であった。

過去 1 年間で実施したセキュリティ対策のきっかけや理由について、NRI 社が日本・米国・シンガポールにおいて同時期に実施した調査（図 2-4-5）によると、日本企業では「自社でのセキュリティインシデント（事件・事故）」（33.6%）がトップであったのに対して、米国とシンガポールの企業では「経営層のトップダウン指示」（米国企業 55.4%、シンガポール企業 66.1%）がトップであった。日本企業は、インシデントの発生をきっかけにセキュリティ対策を実施するという、後手に回った対応が多いとみられる。本調査では、デジタルトランスフォーメーション（通称、DX）やサイバーセキュリティ等、企業を取り巻く環境が目まぐるしく変化する中で、今後は、セキュリティ分野における経営のリーダーシップを向上させ、先を見据えた対策を打っていく必要があるとしている。

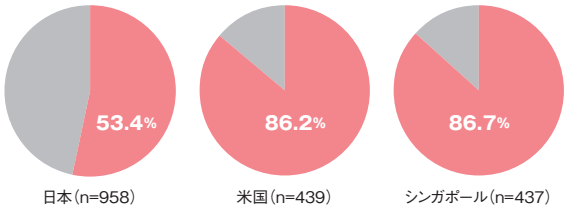


■図 2-4-5　過去 1 年間で実施したセキュリティ対策のきっかけ
（出典）NRI セキュアテクノロジーズ社「NRI セキュア、『企業における情報セキュリティ実態調査 2019』を実施～ DX の推進に向けて、セキュリティ対応の意識・行動改革が求められる日本企業～※297」を基に IPA が編集

(c) 企業のセキュリティ体制

企業におけるセキュリティ関連役職者の設置状況につ

いて、NRI セキュアテクノロジーズ社調査（図 2-4-6）によると、CISO を「設置している」と答えた企業が日本は 53.4% だったのに対して、米国は 86.2%、シンガポールは 86.7%であった。

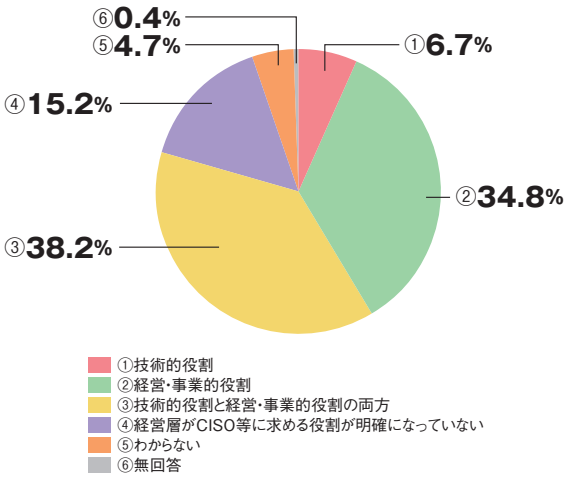


CISOの属性とその割合

	経営層	非経営層	社外有識者
日本（n=958）	70.3%	28.7%	1.0%
米国（n=439）	68.1%	26.2%	5.7%
シンガポール（n=437）	57.2%	34.1%	8.7%

■図 2-4-6　CISO を設置している企業
（出典）NRI セキュアテクノロジーズ社「NRI Secure Insight 2019」を基に IPA が編集

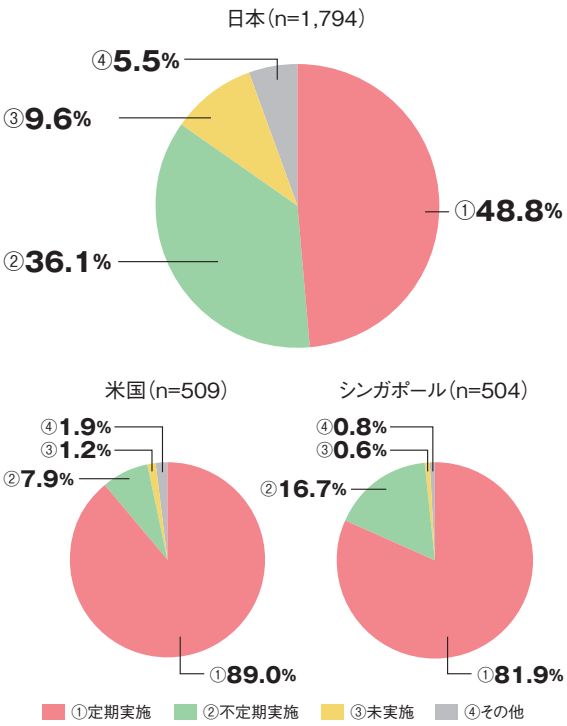
IPA では経営層が CISO 等に対して「経営・事業的役割」と「技術的役割」のどちらを求めているかを調査した（図 2-4-7）。その結果、「技術的役割」のみを求める割合は最も低く 6.7% であったのに対して、「経営・事業的役割」（34.8%）、「技術的役割と経営・事業的役割の両方」（38.2%）と「経営・事業的役割」を重視していることが分かった。日本企業において、CISO 等には技術的役割に加え、経営・事業的役割が求められていることがうかがえる。



■図 2-4-7　経営層が CISO 等に求める役割（n=534）
（出典）IPA「企業の CISO 等やセキュリティ対策推進に関する実態調査」を基に編集

(d) 企業のセキュリティ対策評価実施状況

NRI セキュアテクノロジーズ社調査（図 2-4-8）によると、セキュリティ対策評価（リスク評価）を定期的に実施する企業の割合は、米国が約 90%、シンガポールが約 80% である一方、日本は 50% に満たない結果となった。NRI セキュアテクノロジーズ社調査では、海外ではリスク評価を徹底し、評価結果に応じた合理的・効率的な対策を重視する考え方が根付いていると分析している。



■図 2-4-8　セキュリティ対策評価の実施状況
（出典）NRI セキュアテクノロジーズ社「NRI Secure Insight 2019」を基に IPA が編集

(e) まとめ

以上のように、国内企業における経営層のセキュリティリスク認識やセキュリティ対策への関与の度合いは高く、セキュリティに対する課題認識も持っているが、海外と比較すると経営層のセキュリティへの課題認識はあるものの、リスク評価等の具体的な取り組みに対応できていない状況である。

一方、企業のセキュリティ体制については、CISO 等に対してセキュリティ専門家としての技術的役割のみを期待する企業等は少なく、技術と経営・事業的な役割を合わせ持つことが期待されている。

今後は、企業の経営層はこれまで以上に CISO 等と連携してセキュリティリスクマネジメントを強化することが求められる。

(2) セキュリティリスクマネジメント

本項では、リスクマネジメントにおいて重要なリスクの把握、インシデント対応、情報共有、及びセキュリティ対策状況の可視化について述べる。リスクの把握、インシデント対応、及び情報共有については、IPA 実態調査、「サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集 第 2 版※298」(以下、IPA プラクティス集)、「IT システム・サービスの業務委託契約書見直しに関する調査※299」から、セキュリティ対策の取り組みについての調査結果を紹介する。また、対策状況の可視化については、「サイバーセキュリティ経営ガイドライン実践状況の可視化ツールβ版※36」を紹介する。

(a) スモールスタートでのリスク把握

セキュリティへの経営者の取り組み姿勢は重要であり、自社のリスクを数値化しセキュリティの重要性の理解を深めていくことはセキュリティ対策強化に有効である※300。しかし、IPA 実態調査では、CISO 等がいる組織においてもセキュリティに関する事業リスク評価が未実施である割合は 53.4% であり、リスク評価の実施に何らかの難しさがあると推察される。IPA 実態調査で行った有識者ヒアリングでは、「初めから網羅性を目指さず、重要度の高い領域からスモールスタートで取り組みを始めることが肝要である」との知見が得られ、企業ヒアリングにおいても「リスクベースアプローチでリスクが高い領域から優先的に対策を実装する」等の取り組み事例が見られた。

リスクの把握のためには、守るべきシステムや情報資産を特定することが必要であるが、自社の IT システムについて網羅的な情報資産の洗い出しが困難な場合がある。こうした場合、スモールスタートの取り組みとして、リスクが高い攻撃手法とシステムの組み合わせを特定し、優先的に対策することが考えられる。IPA プラクティス集にまとめられた手順は以下のとおりである。

①重要度が高い情報資産に対して身近・手軽なツールを用いて、リスクアセスメントを実施する※301。
②同業他社等で発生したインシデントをリストアップし、自社の情報資産への被害発生可能性を特定※302 する。
③情報資産の重要度と攻撃手法の被害発生可能性からリスク値を算定し、リスク値の高い攻撃手法とシステムの組み合わせを決定する。

なお、①及び②の情報資産に対するリスク分析には、IPA の「中小企業の情報セキュリティ対策ガイドライン 第 3 版※302」及び付録 7「リスク分析シート※301」(図 2-4-9) も活用できる。

媒体・保存先	個人情報の種類			評価値			重要度	保存期限	登録日	現状から想定されるリスク（入力不要・自動表示）				
	個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性				脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性 ※「対策状況チェック」シートに入力すると表示		被害発生可能性	リスク値
事務所PC	有			2	0	0	2		2016/7/1	3 通常の状態で脅威が発生する（いつ発生してもおかしくない）	2 部分的に対策を実施している	2	可能性：中	4 リスク大
書類	有			2	2	2	2		2016/7/1	2 特定の状況で脅威が発生する（年に数回程度）	2 部分的に対策を実施している	1	可能性：低	2 リスク中
書類		有		2	2	1	2	5年	2016/7/1	2 特定の状況で脅威が発生する（年に数回程度）	1 部分的に対策を実施している	1	可能性：低	2 リスク中
事務所PC			有	2	2	1	2	7年	2016/7/1	3 通常の状態で脅威が発生する（いつ発生してもおかしくない）	2 部分的に対策を実施している	2	可能性：中	4 リスク大

■図 2-4-9　リスク分析シート
(出典) IPA「中小企業の情報セキュリティ対策ガイドライン 第 3 版」の付録7「リスク分析シート」

(b) 業務に即したインシデント対応演習や訓練

IPA 実態調査で行った有識者ヒアリングにおいて、PDCA サイクルの「Check」の取り組みの一つとして、業務に即したインシデント対応演習や訓練が考えられる、という意見が出された。演習シナリオは、必ずしも完成度が高いものである必要はなく、事業部門等関係者の意見を取り入れ、実際のヒヤリハット体験を生かす等により、参加者の関心を高めることができて効果的である。またインシデントについて顧客等、外部に説明するための材料を揃える、インシデント対応経験の豊富なベンダと連携する、等をシナリオに入れることも有効である。業務の実態に即したシナリオによる演習は、参加者の主体性を高め、当事者意識を醸成する効果が期待できる。

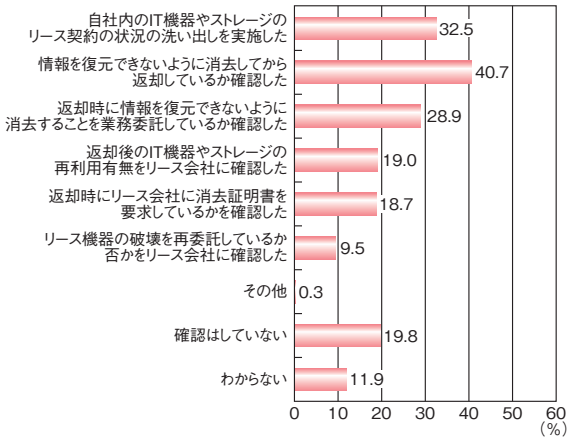
また、演習を通じて、インシデントが自社で生じた場合にどう対応するか考えることにより、「(システム停止等を) 判断する人がわからない」「連絡手段が定まっていない」等の課題点を明らかにしたり、演習で対応に手間取った部門には追加の教育を実施したりすることによって、組織としての対応力強化が期待できる。

(c) 情報の収集・共有活動

同業他社等で発生したサイバー攻撃の手口や利用された脆弱性等インシデントに関する情報を収集するためには、一方的な収集ではなく、コミュニティに参加して情報を共有しあうことも効果的である。IPA 実態調査で行った企業ヒアリングでは、外部のコミュニティ参加者と信頼関係を構築するためには、Give and Take の考え方が重要、という意見が出された。ただし、有益な情報を得るためには必ずしも高度な情報を提供する必要があるわけではない。情報提供は自分の課題を正直に話すという形でもよい。課題の共有でかえって信頼され、情報を得られることもある。それ以外にも、コミュニティ運営の支援やオフライン会議への参加等の貢献が考えられる。また、セキュリティベンダのユーザ会や、同業者以外のコミュニティでの情報共有も有用である。

(d) インシデント情報共有による改善活動

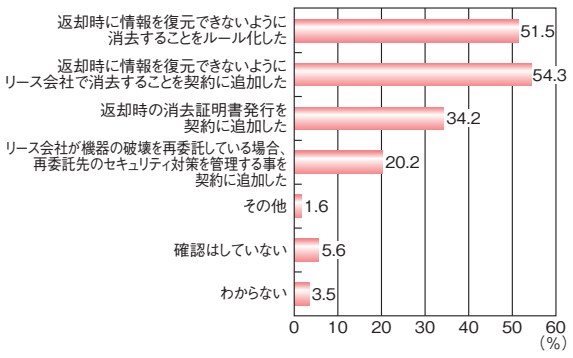
インシデント情報の共有により、セキュリティ対策の見直しを行うことも重要である。2019 年 12 月、リース契約満了により返却されたハードディスクの廃棄を再委託された会社の社員が窃盗・転売し、消去予定であった県の情報が漏えいするというインシデントが発生した※303（「1.2.7 (3) 内部者の不正による情報漏えい」参照）。多くの企業で IT 機器やストレージのリース契約が行われており、データ消去を委託する場合もあることから注目された。IPA による調査では、調査した企業の約 7 割で上記インシデントをきっかけに IT 機器やストレージに関するリース契約内容や情報の取り扱いについて何らかの確認作業が行われていた（図 2-4-10）。



■図 2-4-10　IT 機器やストレージに関するリース契約内容や情報の取り扱いの確認状況（n=911）
（出典）IPA「IT システム・サービスの業務委託契約書見直しに関する調査」を基に作成

更に、何らかの確認作業を行った企業のうち、半数以上がルール化や契約への追加等、管理を強化していた（図 2-4-11）。

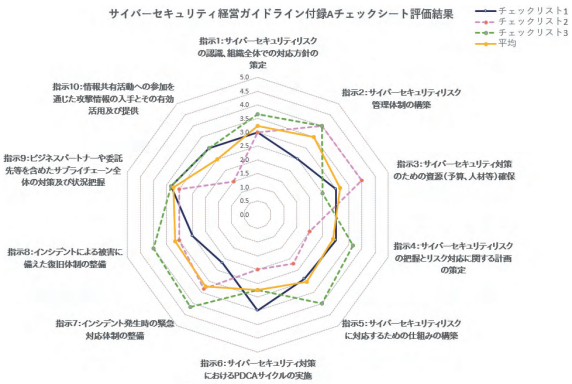
本インシデントはメディアで注目されたこともあり、調査した企業の約 7 割で見直しが実施されたが、メディアに大きく取り上げられないインシデントについても、自社に関係のあるインシデントが発生している場合は、セキュリティ対策の見直しを実施していくことが望ましい。



■図 2-4-11　IT 機器やストレージのリースの契約書の確認や見直し、情報の取り扱いの見直し状況（n=623）
（出典）IPA「IT システム・サービスの業務委託契約書見直しに関する調査」を基に作成

(e) セキュリティ対策実践状況の可視化

リスクマネジメントには、経営層と情報共有できるように状況を可視化することが重要である。経営層がリスクを評価し、最終的な判断ができることを目的とし、IPA と経済産業省は企業のセキュリティ対策実践状況を可視化するためのツールを作成した（図 2-4-12）。本ツールは「サイバーセキュリティ経営ガイドライン」を基にして構成され、経営層に向けたセキュリティマネジメント実施状況の可視化を志向している。企業によるセルフチェックを想定し、質問数は 50 問に満たない簡易な形式となっている。セルフチェックでは回答の信頼度に問題がある可能性があるが、役職・部門等の異なる複数人がチェックすることで精度を上げる、等の工夫も考えられる。回答の評価が実態に比べて高い、あるいは回答が一致しない等の項目はマネジメントに課題がある可能性があり、優先度を高めて調査・検討対象とする使い方も有効である。



■図 2-4-12　評価結果イメージ
（出典）IPA「サイバーセキュリティ経営ガイドライン実践状況の可視化ツール β版」

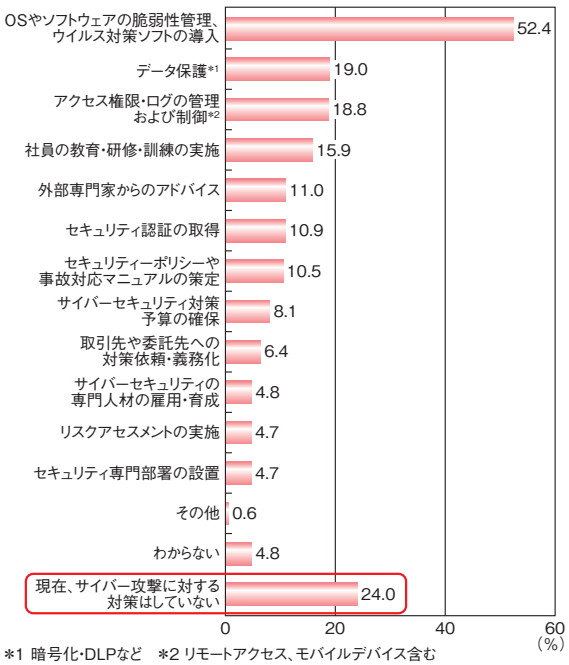
2.4.2 中小企業における情報セキュリティの取り組み

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

(1) 中小企業の情報セキュリティの現状

一般社団法人日本損害保険協会が 2020 年 1 月 28 日に発表した「中小企業の経営者のサイバーリスク意識調査 2019※304」によると、サイバー攻撃への対策状況につ

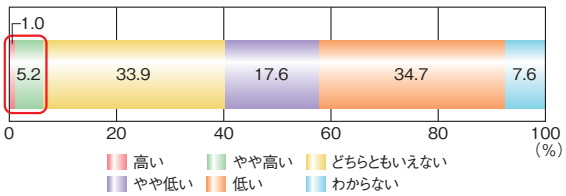
いて、中小企業の 4 社に 1 社は、今もなおサイバー攻撃への対策を実施していないと回答している（図 2-4-13）。



*1 暗号化・DLPなど　*2 リモートアクセス、モバイルデバイス含む

■図 2-4-13　サイバー攻撃への対策内容（n=825）
（出典）一般社団法人日本損害保険協会「中小企業の経営者のサイバーリスク意識調査 2019」を基に IPA が編集

サイバー攻撃の対象となる可能性については、自社がサイバー攻撃の対象となる可能性を認識している中小企業は 1 割未満であった（図 2-4-14）。

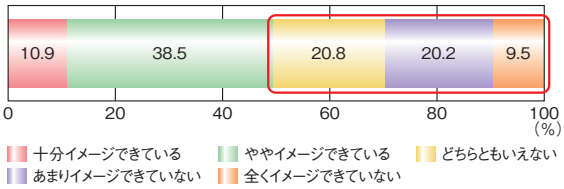


■図 2-4-14　サイバー攻撃の対象となる可能性（n=825）
（出典）一般社団法人日本損害保険協会「中小企業の経営者のサイバーリスク意識調査 2019」を基に IPA が編集

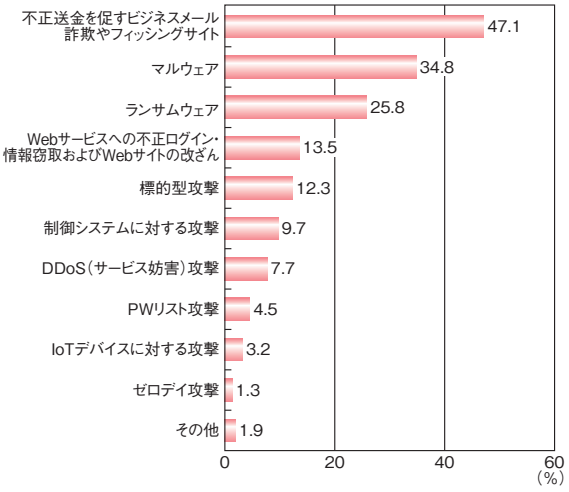
サイバー攻撃によって自社が被る被害については、中小企業の約半数が十分イメージできていないという結果であった（図 2-4-15）。

サイバー攻撃の被害経験については、825 社中 155 社が被害に遭っており、中小企業の約 2 割は何らかのサイバー攻撃の被害に遭っている。その被害内容を図 2-4-16 に示す。また、サイバー攻撃による被害総額は、図 2-4-17 に示すように、半数以上の企業で 50 万円を超えている。

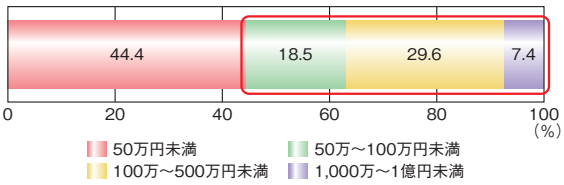
このような調査結果から、中小企業のサイバー攻撃対策は未対応の企業が四分の一である等、十分ではない。背景に、自社が攻撃対象になりうるという認識や攻撃被害のイメージの不足があると思われる。その一方で、サイバー攻撃の被害経験がある企業は少なくはなく、中小企業においても、経営課題の一つとして優先度を高め、サイバー攻撃対策を推進していくことが必要であると考えられる。



■図 2-4-15　サイバー攻撃の被害イメージ有無（n=825）
（出典）一般社団法人日本損害保険協会「中小企業の経営者のサイバーリスク意識調査 2019」を基に IPA が編集



■図 2-4-16　サイバー攻撃の被害内容（n=155）
（出典）一般社団法人日本損害保険協会「中小企業の経営者のサイバーリスク意識調査 2019」を基に IPA が編集



■図 2-4-17　サイバー攻撃による被害額（n=27）
（出典）一般社団法人日本損害保険協会「中小企業の経営者のサイバーリスク意識調査 2019」を基に IPA が編集

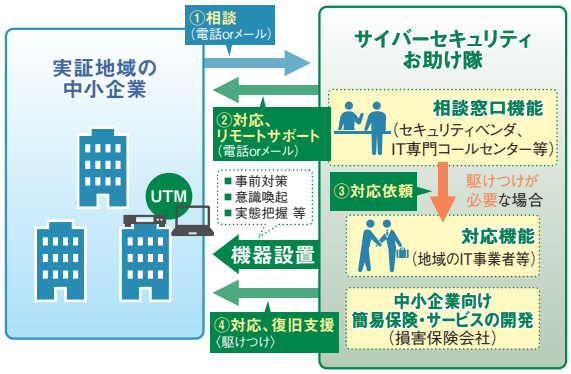
(2) 中小企業向け情報セキュリティ対策支援施策

政府が 2019 年度に新たに実施した中小企業向け情報セキュリティ対策支援施策を紹介する。

(a) 中小企業向けサイバーセキュリティ事後対応支援実証事業

経済産業省は2019年度、IPAを通じて、「中小企業向けサイバーセキュリティ事後対応支援実証事業」（通称、サイバーセキュリティお助け隊）を実施した（図2-4-18）。本事業では、全国8地域の中小企業を対象として、サイバーセキュリティに関する悩みや、対策のニーズ、サイバー攻撃被害の実態等を把握するとともに、サイバーインシデントが発生した際の地域における支援体制の構築等に向けた実証を行った。

本事業には、19府県8地域（①岩手、宮城、福島、②新潟、③長野、群馬、栃木、茨城、埼玉、④神奈川、⑤石川、福井、富山、⑥愛知、⑦大阪、京都、兵庫、⑧広島、山口）の中小企業1,064社が参加した。このうち、727社にUTM（Unified Threat Management：統合脅威管理）等の機器を設置し、サイバー攻撃を観測した場合は地域のITベンダ等で構成されるサイバーセキュリティお助け隊が駆けつけ、対応、復旧支援等を行った。その結果、合計で128件のインシデントが発生しており、そのうち駆けつけ対応が18件発生している。本事業を通じて、中小企業においても業種や規模を問わず例外なくサイバー攻撃を受けているが、検知及び防御のための対策や社内体制の構築ができていない企業が多いことが明らかになった。本事業の報告書[※305]では、人的リソースの不足やコストに制約がある中小企業に、必要なセキュリティ対策を促すためには、「継続的な意識啓発」「導入・運用しやすい対策機器やサイバー保険の開発」「専門家の伴走型支援を含むワンパッケージ化」「コスト低廉化」が重要であり、これらを効果的に推進するため地域コミュニティとの連携促進やビジネス化に向けた情報共有の仕組みの構築が有効であるとまとめている。



■図2-4-18　サイバーセキュリティお助け隊の事業イメージ
（出典）IPA「中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊）[※37]」を基に編集

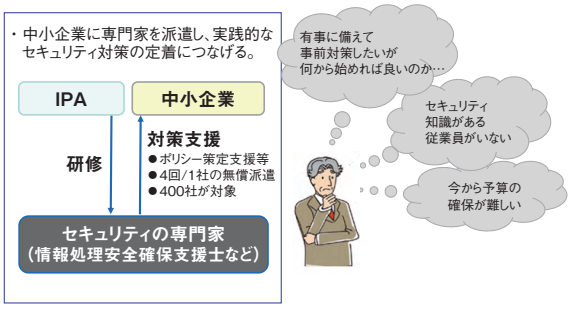
本事業において大阪府、京都府、兵庫県での実証を担当した大阪商工会議所は2020年4月、「サイバーセキュリティお助け隊」を中小企業向けサービス事業として、大阪府内を中心に京阪神でのサービス提供を開始した[※306]。今後、実証事業を踏まえた中小企業向けサービスの提供事業者の増加、提供地域の拡大が期待される。

(b) 中小企業の情報セキュリティマネジメント指導業務

経済産業省は2019年度、IPAを通じて、「中小企業の情報セキュリティマネジメント指導業務」を実施した（図2-4-19）。本事業では、全国の中小企業を対象として、情報処理安全確保支援士等の専門家が訪問し、中小企業の現場に応じたリスクの洗い出しからマネジメントに必要なセキュリティ基本方針や関連規定の策定に向けて以下の指導を実施した。

- 1回目：情報セキュリティ診断等による潜在的リスクの洗い出し
- 2回目：診断結果に基づく重点領域の可視化、基本方針の策定、対策の決定
- 3回目：関連規定の策定に向けた検討
- 4回目：関連規定のレビューと専門家指導全体のまとめ

本事業には、全国の中小企業382社が参加した。その結果、96.4%の企業が成果を得られたと回答し、指導した専門家も92.0%が指導先企業のセキュリティレベルが上がったと回答した。また、今後実施すべきと考える取り組みについて、「体制整備・運用ルールの策定・継続的な改善」と回答した企業は79.9%であった。本事業を通じて、多くの企業がセキュリティレベルや継続的改善の意識の向上を果たした。



■図2-4-19　情報セキュリティマネジメント指導業務のイメージ
（出典）IPA「中小企業の情報セキュリティマネジメント指導業務[※307]」を基に編集

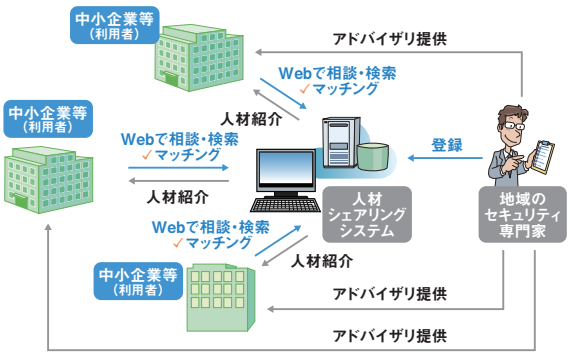
(c) 中小企業向けサイバーセキュリティ製品・サービスのプラットフォーム構築事業

経済産業省では 2019 年度、IPA を通じて、「中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築事業※308」を実施した。本事業は、中小企業でも扱いやすいセキュリティ製品・サービスを導入・運用することで得られる効果や費用、利用のし易さ、課題等を分かりやすく提示する枠組み（プラットフォーム）の実現可能性を調査するものである。具体的には、中小企業向けセキュリティ製品･サービスについて、「導入のし易さ」「運用のし易さ」「導入や運用に要する費用」「製品・サービスのセキュリティ性能」等の評価項目を仮設定した後、セキュリティ製品・サービスをユーザ企業に導入してもらい、ヒアリング調査にて評価項目の有効性を検証し、有識者委員会にて評価項目の設定を見直した。また、有識者委員会にて中小企業向けセキュリティ製品・サービスの情報提供プラットフォームのあるべき姿の検討等を行った。

本事業を通じて、情報提供プラットフォームのあるべき姿が明確となり、必要となる機能や運営方法の方向性が打ち出された。今後、本プラットフォームが構築されることで、中小企業におけるセキュリティ製品・サービスの選定が容易になり、導入や対策の実践が促進することが期待される。

(d) セキュリティ人材シェアリングモデル事業

総務省は2019年度、グローバルセキュリティエキスパート株式会社を通じて、「セキュリティ人材シェアリングモデル事業」を実施した（図 2-4-20）。本事業では、関西地域の中小企業 50 社を対象として、クラウド上の人材シェアリングシステム（人材登録やマッチング等を行う）を使用し、地域の中小企業が抱えるサイバーセキュリティの課題と、地域のサイバーセキュリティ専門家のセキュリティスキルをマッチングした。マッチングが成立した場合は、サイバーセキュリティ専門家が当該中小企業を訪問し、セキュリティに関する助言を行い、企業が抱えるサイバーセキュリティ上の課題解決を支援した。



■図 2-4-20　セキュリティ人材シェアリングモデル事業のイメージ
（出典）グローバルセキュリティエキスパート株式会社「セキュリティ人材シェアリングモデル事業※309」を基に IPA が編集

(3) 普及啓発・対策ツール

中小企業に向けた情報セキュリティの普及啓発活動や対策ツールを紹介する。

(a) SECURITY ACTION

IPA では、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度「SECURITY ACTION」を運営し、中小企業と関連の深い中小企業支援機関、士業団体、IT 関連団体と連携して SECURITY ACTION を通じた情報セキュリティの普及啓発を行っている※310。

SECURITY ACTION に基づく自己宣言は、一般社団法人クラウド活用・地域 ICT 投資促進協議会が実施する「全国中小企業クラウド実践大賞※311」の参加条件になるほか、公的な補助金制度の申請要件としても活用されている。

2020 年 3 月末時点の宣言数は 9 万件（個人事業主を含む）を超えている。今後より多くの中小企業が SECURITY ACTION を宣言し、社内の意識付けや社外への信頼性のアピール等に活用し、対策を推進することが望まれる。

(b) 小さな中小企業と NPO 向け情報セキュリティハンドブック

NISC は、2019 年 4 月に「小さな中小企業と NPO 向け情報セキュリティハンドブック※312」を公開した（次ページ図 2-4-21）。

本ハンドブックは、特に小規模事業者やセキュリティ担当者の設置が困難な中小企業及び NPO 等に向けて、サイバーセキュリティに関する脅威とその対策についてイラストを交えながら解説している。

本ハンドブックの著作権は NISC に留保されているが、自由な活用を目的に制作されており、企業内のサイバーセキュリティに関する社員研修等で利用したい場合は、印刷用の版下データや、イラスト単位で活用できるように画像データ等も提供されている。

■図 2-4-21　小さな中小企業と NPO 向け情報セキュリティハンドブック
(出典)NISC「小さな中小企業と NPO 向け情報セキュリティハンドブック」

(c) MY CISO ハンドブック・テンプレート

JNSA は、2019 年 9 月に「MY CISO ハンドブック・テンプレート」を公開した※313。

「MY CISO ハンドブック・テンプレート」は、2018 年 5 月に公開した「MY CISO ハンドブック」を中小企業向けに使いやすくしたものであり、中小企業の CISO やセキュリティ担当者が、セキュリティに関わる業務を執行し、経営陣と適切なコミュニケーションを進める上で明確にすべき項目と内容を例示している。例示されたものを自社に則した内容にカスタマイズし、独自の「MY CISO ハンドブック」を整備することで、日常的な業務の中にセキュリティ業務を組み込むことが期待できる。

2.4.3 教育機関・政府及び地方公共団体等法人における対策状況

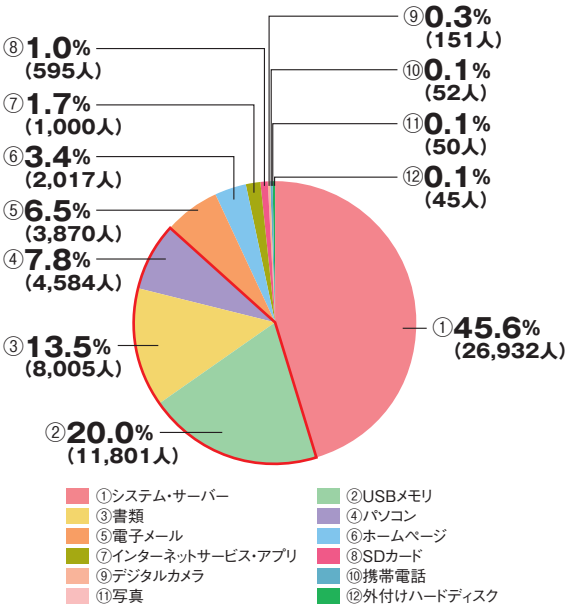
教育機関・政府及び地方公共団体等法人における対策状況について、公表されている資料に基づいて述べる。

(1) 教育機関における個人情報漏えいと政府による対策、インシデント事例

教育ネットワーク情報セキュリティ推進委員会（ISEN：Information Security for Education Network）では、学校、公的教育機関、関連組織で発生した、児童・生徒・保護者等の個人情報を含む情報の紛失・漏えい事故について、公開情報を調査・集計した結果を「学校教育機関における個人情報漏えい事故の発生状況－調査報告書－」（以下、ISEN 調査報告書）として毎年公表している。

ISEN 調査報告書※314 によると、2018 年度は 198 件の個人情報漏えい事故が発生しており、漏えいした件数は延べ 5 万 7,628 人分である。2017 年度の 187 件、2016 年度の 207 件と比べ※315、過去三年間の発生件数に大きな改善はない。

漏えいした個人情報の件数を経路・媒体ごとに比較すると、「システム・サーバー」が約半数の 45.6%（2 万 6,932 人）と最も多く、次いで「USB メモリ」が 20.0%（1 万 1,801 人）、「書類」が 13.5%（8,005 人）、「パソコン」が 7.8%（4,584 人）と続く。4 位までの経路・媒体を合計すると、漏えい件数の約 9 割を占める（図 2-4-22）。



■図 2-4-22　情報漏えいの経路・媒体別の事故発生比率※316
(出典)ISEN 調査報告書を基に IPA が作成

従って、これらの経路・媒体の利用に関する対策を徹底することによって、大幅な改善が見込める。なお、人数が 2 位～4 位の経路・媒体は、合計すると 41.3%（図 2-4-22 の赤枠部分）となり、1 位の「システム・サーバー」に匹敵する漏えい人数であるが、これらはいずれも、紛失したり置き忘れたりする人的ミスが漏えいの原因となる媒体であり、後述するように共通した対策が考えられる。

学校における個人情報漏えい事故に関する政府の取り組みとして、文部科学省は、学校を対象として「教育情報セキュリティポリシーに関するガイドライン（令和元年 12 月版）※317」を公表している。この中で、前述の「システム・サーバー」及び紛失・置き忘れの対象となる漏えい経路・媒体に関する対策等の考え方が示されている。

(a)「システム・サーバー」からの漏えいに対する施策

「システム・サーバー」については技術的な対策が主になるが、① Web 閲覧やメール等外部からアクセスが容易なシステムと、個人情報等機微な情報を扱う校務系システムとを論理的あるいは物理的に分離すること、②児童生徒による機微情報へのアクセスリスクを回避するために、校務系システムと学習系システムを分離すること、③学習系システムには機微な情報を保管しないことを原則とすること、等が対策として挙げられている。また、効率的にこうした対策を実現する上では、「システム・サーバー」の管理を学校現場等で行うのではなく、セキュリティ水準が第三者認証等によって確保されるクラウド事業者に任せる選択も効果的としている（クラウドについては「3.4 クラウドの情報セキュリティ」参照）。

(b) 人的ミスによる媒体からの漏えいに対する施策

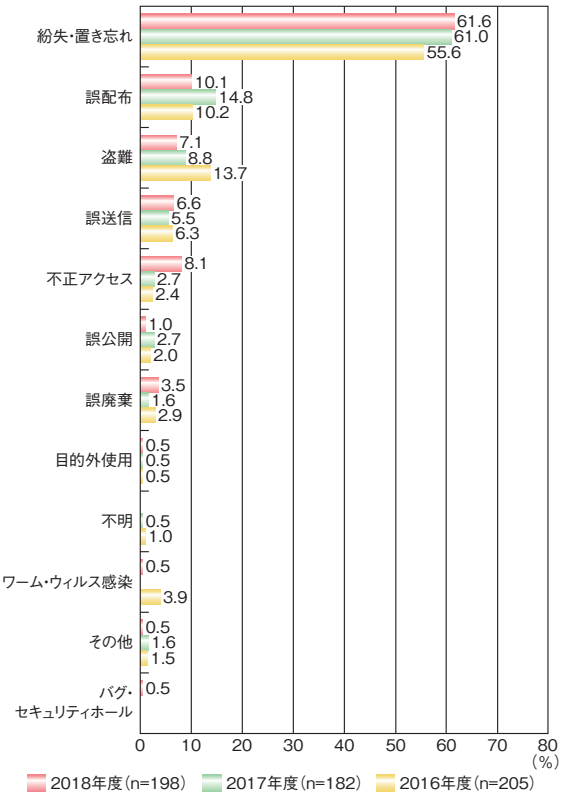
媒体の紛失・置き忘れの対策としては、管理されたUSB メモリやパソコン以外の使用を禁止し、適切なパスワード設定や個人情報等の暗号化を徹底すること等が挙げられている。ただし「書類」については、こうした技術的対策では保護が難しいため、人的・制度的なセキュリティ対策にも併せて取り組む必要がある。例えば、個人情報の外部持出しには教育情報セキュリティ管理者（ガイドラインでは、校長等を想定）の許可を得なければならないとする規則の制定・施行等である。

個人情報漏えい事故の原因別の統計を見ると、紛失・置き忘れは、発生件数の 61.6% を占めており、しかもこの状況が 2017 年度 61.0%、2016 年度 55.6% と過去 3 年間続いていることが分かる（図 2-4-23）。紛失・置き忘れによる情報漏えい事故の対策徹底は、依然として不十分であったことがうかがわれる。

紛失・置き忘れが原因とみられるインシデントの実例を以下に示す。

2019 年 8 月 30 日、富山大学で、学生 320 人の個人情報を格納した USB メモリの紛失が判明した。この大学では個人情報の持ち出しが原則禁止されており、持ち出しの場合は保護管理者の許可を得ることが定められていたが、この規則が守られていなかった上、USB メモリにはパスワード設定がされていなかった※318。

2019 年 9 月 12 日、静岡県立袋井商業高等学校で、生徒 64 人の個人情報を保存した教師の私物 USB メモリの紛失が判明した。校長の許可を得ずに USB メモリに個人情報を保存した上、パスワードを設定する等のセキュリティ対策もしていなかった。この高校では 4 月にも



■図 2-4-23　学校における個人情報漏えい事故
（出典）ISEN 調査報告書を基に IPA が作成

USB メモリの紛失が発生しているが、その際も、個人情報保護管理の徹底が不十分だったとみられる※319。

このように、前述の「教育情報セキュリティポリシーに関するガイドライン（令和元年 12 月版）」等において適切な技術的対策（パスワード等の適切な設定、機微な情報の暗号化等）や人的・制度的対策（個人情報持ち出しに確認・許可を必要とする規則の制定等）が示されていても、それが周知徹底されない、あるいは周知されても実践のスキルや時間的余裕がない状況が続いては、効果が発揮できない。上位の組織（地方自治体の教育委員会、私立の学校法人等）において標準的な施策を決め、対策予算やセキュリティ技術に詳しい人的リソースを用意し、実施状況の改善進捗を把握・管理する等、適切な支援が求められる。

(2) 地方公共団体における対策状況

総務省は、継続的に地方公共団体の情報セキュリティ対策の実施状況を調査している。ここでは総務省が公表している「地方自治情報管理概要～電子自治体の推進状況（令和元年度）～※320」に基づき、地方公共団体の情報セキュリティ対策の実施状況の変化について述べる。

表 2-4-1（次ページ）は、対策項目に関して、都道府

県及び市区町村の実施率をまとめたものである。2018年度と2019年度の実施率の差も併せて記載している。

2018年度に比べ2019年度は、多くの項目で実施率が向上した。特に市区町村では、10ポイント以上実施率が向上した項目が四つある。

基本的な個別対策（「情報セキュリティ責任者や管理者等の任命の有無」「情報資産の重要度に応じて保管やアクセス、持ち出しについて規定」「サーバ室等の入退室管理を行っている」等）は、都道府県・市区町村ともに高い実施率となっている。他方、調査・分析・計画等の項目（表中の（A）の項目）や監査・評価に関する項目（表中の（B）の項目）は、特に市区町村において、今後の改善が期待される。

2.4.4 一般利用者における対策状況

IPAが実施した「2019年度情報セキュリティに対する意識調査[※322]」の結果を基に、一般利用者の情報セキュリティ対策の実施状況について述べる。

(1) パソコン利用者のセキュリティ対策実施状況

パソコン利用者のセキュリティ対策実施状況の調査結果によると、「Windows Updateなどによるセキュリティパッチの更新」をしている割合が50.8%（2018年度から4.9ポイント減）、「セキュリティソフト・サービスの導入・活用」をしている割合が55.1%（2018年度から5.8ポイント減）で、どちらも半数以上が実施しているが、2018年度よりも減少している（図2-4-24）。また、「不審な電子メー

対象項目		対策実施率	
		都道府県	市区町村
	情報セキュリティの責任者や管理者等の任命の有無	100.0% (0.0ポイント)	99.8% (+1.1ポイント)
(A)	緊急時対応計画を整備	100.0% (+2.1ポイント)	69.6% (+14.5ポイント)
	情報資産の重要度に応じて、保管やアクセス、持ち出しについて規定	100.0% (0.0ポイント)	92.9% (+4.6ポイント)
	情報資産について、機密性、完全性及び可用性により分類	74.5% (+4.3ポイント)	63.8% (+14.1ポイント)
(A)	主要な情報資産について調査及びリスク分析を行っている	74.5% (+6.4ポイント)	47.8% (+9.5ポイント)
	サーバ室等の入退室管理を行っている	100.0% (0.0ポイント)	99.3% (+0.2ポイント)
	サーバ等への停電や免振対策を実施している	100.0% (0.0ポイント)	97.4% (-1.2ポイント)
	重要情報を含む紙媒体を適切に管理している	100.0% (0.0ポイント)	98.6% (+1.2ポイント)
	CD-R、USBメモリ等によるデータの持ち出し、持ち込みを制限している	97.9% (0.0ポイント)	98.3% (+1.5ポイント)
	クラウドサービスやデータセンターを利用している	93.6% (0.0ポイント)	91.2% (+6.8ポイント)
	情報セキュリティ研修を職員に対して実施している	100.0% (0.0ポイント)	92.9% (+3.3ポイント)

対象項目		対策実施率	
		都道府県	市区町村
(B)	緊急時対応訓練を実施している	87.2% (+12.7ポイント)	33.0% (+6.8ポイント)
	重要なデータのバックアップを取得	100.0% (0.0ポイント)	99.9% (+0.2ポイント)
	機器や外部記録媒体を廃棄する際、重要なデータを抹消	100.0% (0.0ポイント)	99.3% (0.0ポイント)
	重要なデータへのアクセス制限（権限設定、認証）を実施	97.9% (−2.1ポイント)	99.7% (+0.7ポイント)
	許可されていないソフトウェアの導入を禁止	100.0% (0.0ポイント)	97.9% (+1.2ポイント)
	重要な情報システムのアクセスログを保存し、検査	100.0% (+2.1ポイント)	91.7% (0.0ポイント)
	重要なデータを暗号化し保存	87.2% (+6.3ポイント)	50.0% (+4.9ポイント)
	委託事業者に対し、情報漏えい防止策を契約等により義務付けている	100.0% (+2.1ポイント)	96.3% (+5.7ポイント)
	情報資産の調達の際、仕様書等に情報セキュリティポリシーに基づいた要件を記載している	97.9% (+6.4ポイント)	71.1% (+12.4ポイント)
(B)	情報システムの運用等の委託事業者に対する指導・監査を実施している	68.1% (+8.5ポイント)	49.5% (+9.9ポイント)
(B)	機密性、完全性及び可用性等についてサービス契約（SLA）に定め、委託事業者に対し定期的に報告することを定めている	59.6% (+8.5ポイント)	38.7% (+12.6ポイント)

（A）の項目は対策実施手順・ポリシーの策定や調査・分析・計画等の項目。（B）の項目は監査や評価に関する項目（本文参照）。各セルの1行目の値は2019年度の値。2行目の括弧付きの値は2018年度の値との差。

■表2-4-1　地方公共団体における主な情報セキュリティ対策状況（2019年度、47都道府県、1,741市区町村）
（出典）総務省「地方自治情報管理概要～電子自治体の推進状況（令和元年度）～」「地方自治情報管理概要～電子自治体の推進状況（平成30年度）～[※321]」を基にIPAが作成

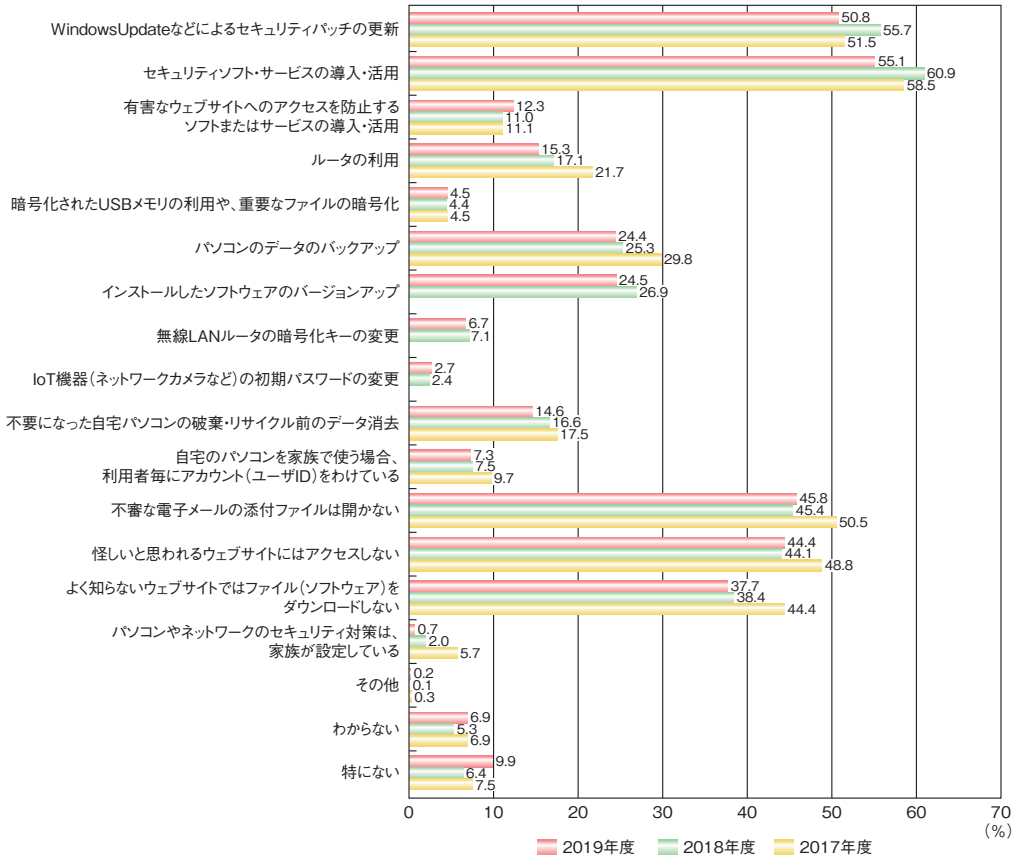
ルの添付ファイルは開かない」割合は 45.8%（2018 年度から 0.4 ポイント上昇）、「怪しいと思われるウェブサイトにはアクセスしない」割合は 44.4%（2018 年度から 0.3 ポイント上昇）である等、若干上昇している項目もあるものの、いずれも過半数には届かず伸び悩んでいる。

近年の OS（オペレーティングシステム）は利用者が意識しなくても初期設定でセキュリティパッチが自動更新されるものが増えており、Windows Defender ウイルス対策※323 のように、パソコンの購入時点でインストール済みのセキュリティソフトも存在する。そのため、本調査で各対策を「実施している」と回答しなかった利用者の中には、意識せずに対策を実施している人が含まれる可能性もある。しかし、利用しているパソコンで実施されている対策や設定を把握していないことは、偽警告や偽セキュリティソフト（「1.2.6 個人をターゲットにした騙しの手口」参照）等、別の被害につながる可能性がある。パソコンを購入した販売店にセキュリティソフトウェアについて相談する、あるいは OS 開発元のサイト※324 等を参考に設定を確認する、等の対応が望まれる。

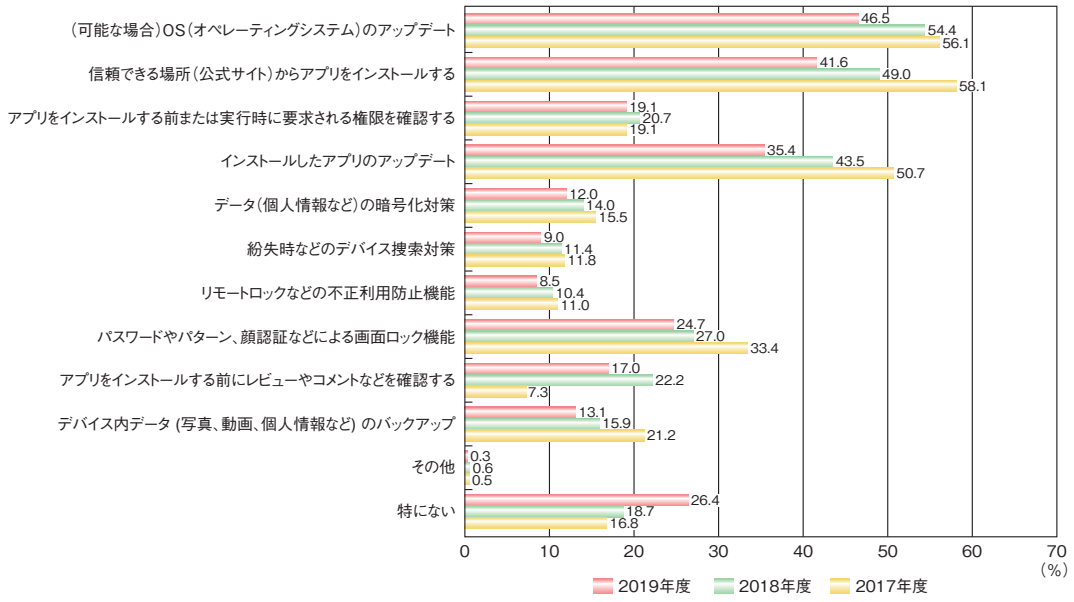
(2) スマートデバイス利用者のセキュリティ対策実施状況

スマートフォンやタブレット端末等のスマートデバイスのセキュリティ対策実施状況の調査結果によると、以前は半数が実施していた「（可能な場合）OS（オペレーティングシステム）のアップデート」（46.5%）、「信頼できる場所（公式サイト）からアプリをインストールする」（41.6%）、「インストールしたアプリのアップデート」（35.4%）の割合がいずれも 4 割前後まで低下している（次ページ図 2-4-25）。また、スマートデバイス紛失時の捜索や不正利用防止等、他の対策の実施割合も 2018 年度より低下している。

2019 年に急速に普及したスマートフォン決済サービス（スマホ決済）では、アカウント、あるいはアカウント情報の不正利用が大きな問題となっている。不正利用の原因としては、フィッシングや情報漏えいによって窃取された ID・パスワードを使った不正ログインの他に、決済アプリや決済のための情報が入ったスマホ自体を盗まれることや、アプリやサービスの脆弱性を悪用されること等が挙げられている※325-1。図 2-4-25（次ページ）の結果を見ると、スマホ決済を利用する人の多くがこのリスクに対処できていないことが懸念される。



■図 2-4-24　パソコン利用者のセキュリティ対策実施状況（n=5,000）
（出典）IPA「2019 年度情報セキュリティの脅威に対する意識調査※325-2」を基に作成



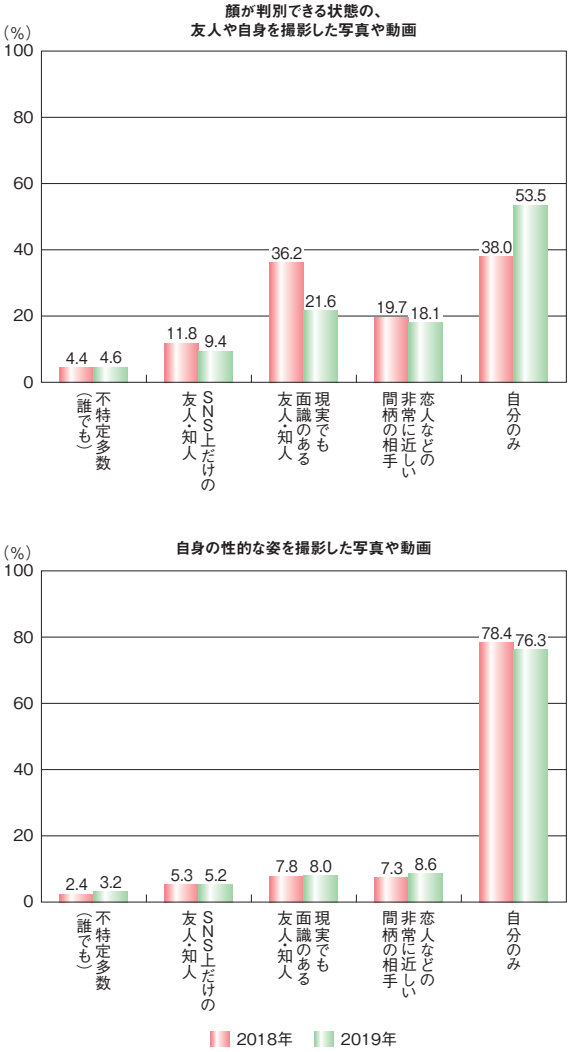
■図 2-4-25　スマートデバイス利用者のセキュリティ対策実施状況（n=5,000）
（出典）IPA「2019 年度情報セキュリティの脅威に対する意識調査」を基に作成

スマホ決済の不正利用による金銭被害を防ぐ意味でも、画面ロック機能を始めとする他者による不正操作の防止策を講じておくことや、スマホ決済アプリを公式マーケット等の信頼できるサイトからインストールし、通知があったら迅速にアップデートを実施することが推奨される。また、不正利用につながる個人情報を詐取されないよう、「1.2.6 個人をターゲットにした騙しの手口」を参考に対策を実施することも有効である。

(3) SNS 利用におけるリスクの認識状況

SNS の利用により、個人が簡単に情報を発信し、著名人や共通の興味・趣味を持つ人と立場を越えて交流することが可能となった。しかし同時に、コミュニケーション不備による炎上や情報の意図しない拡散、悪意の人物との接触のリスクも大きくなり、実際に犯罪被害が発生している（「1.2.6 個人をターゲットにした騙しの手口」「3.3 次代を担う青少年を取り巻くネット環境」参照）。犯罪に巻き込まれないためには、SNS 利用におけるリスクを認識し、慎重に行動することが重要である。

スマートデバイス利用者を対象とした SNS での写真・動画の共有相手に関する意識の調査結果（図2-4-26）によると、顔が判別できる状態の、友人や自身を撮影した写真や動画について、「恋人などの非常に近しい間柄の相手に共有してよい」と回答した割合は 18.1%、「現実でも面識のある友人・知人に共有してよい」と回答した割合は 21.6%、「SNS 上だけの友人・知人に共有してよい」と回答した割合は 9.4% であった。SNS 上に投



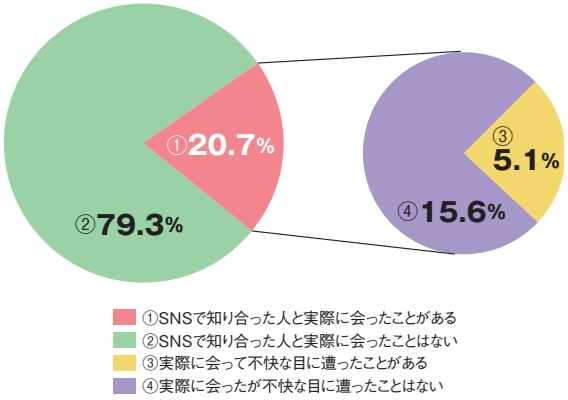
■図 2-4-26　SNSでの写真・動画の共有相手に関する意識（n=5,000）
（出典）IPA「2019 年度情報セキュリティの倫理に対する意識調査[※325-3]」を基に作成

稿した顔写真はストーカー行為等に悪用される可能性があるため、身元の分からない相手に送信するリスクはもとより、知人に送信する際にも、知人の端末から漏えいする、知人が勝手に公開する等のリスクがあることを認識しておきたい。

また、自身の性的な姿を撮影した写真や動画について、「恋人などの非常に近しい間柄の相手に共有してよい」と回答した割合は 8.6%、「現実でも面識のある友人・知人に共有してよい」と回答した割合は 8.0%、「SNS 上だけの友人・知人に共有してよい」と回答した割合は 5.2% であった。性的な映像はセクストーションやリベンジポルノといった犯罪に悪用されるリスクがあるため、SNS への投稿はもちろん、撮影することも控えるべきである。

更に、スマートデバイス利用者の中で、「SNS 上で交流がある人と実際に会ったことがある人」の割合は 20.7%、「実際に会って不快な目に遭ったことがある人」は 5.1% と、SNS 上で交流がある人と実際に会ったことのある人のうちおよそ 4 人に 1 人が実際に会った結果、不快な目に遭ったことがあると回答した（図 2-4-27）。SNS で知り合った人と実際に会ったことをきっかけとする意図しない特殊詐欺への加担や、誘拐等の被害が発生している昨今、SNS 上での交流の中で実際に会うという話題が出た際には、相手の目的、会う場所や時間等について慎重に判断すべきである。

以上のようなリスクを認識の上、SNS は慎重に利用することが望ましい。



■図 2-4-27　SNS 上で交流がある人と実際に会った経験（n=5,000）
（出典）IPA「2019 年度情報セキュリティの倫理に対する意識調査」を基に作成

COLUMN

サイバーの中心で、愛をさけぶ

皆さんは「セキュリティって何?」って考えたことがありますか? 堅苦しい定義で言えば、「機密性」「完全性」「可用性」を守ることになると思いますが、もう少し柔らかい言い方をすると、「私たちがインターネットやコンピュータ、スマートフォンを安心して使い続けられるように、大切な情報が流出したり、ウイルスなどに感染することから守ること」だと言えます。私たちの大切なものや大切な人の生活を、それらを脅かすもの者から守ること、これってまさに「愛」だと思いませんか? 突然何を言い出すのかと思われるかもしれませんが、私たちの生活にたくさんの「愛」が溢れているように、サイバーな世界にもたくさんの「愛」が必要で、それこそが「セキュリティ」なのです。

愛し愛されるためには努力が必要なように、セキュリティにも努力が必要です。愛を維持するために必要な努力の多くは、そのままセキュリティの維持にも必要なものです。

1. 愛(セキュリティ)とは、手間(時間)をかけること
   長いパスワードや、多要素認証など、ちょっと面倒だけどひと手間かけてください。
2. 愛(セキュリティ)とは、共有すること
   都合の悪い出来事(インシデント)こそ、隠さずに共有しましょう。組織内だけでなく、社会全体と共有することも大切です。
3. 愛(セキュリティ)とは、信頼すること
   サイバー空間では信頼できる相手(信頼点)の確保が重要です。信頼があるからこそ、確認(監査)ができるのです。
4. 愛(セキュリティ)とは、許すこと
   インシデントが発生した組織をあまり責めないでください。本当に悪いのは、悪意を持ってウイルスをばらまいたり、情報を流出させる人(集団)です。
5. 愛(セキュリティ)とは、忘れてはならない約束だということ
   職場で、家庭で、これだけは守ろうというルールを決めることが大切です。そして、それを忘れないように。
6. 愛(セキュリティ)とは、見返りを求めないこと
   セキュリティを強化したからといって直接的に利益が増えないばかりか、利用者に面倒がられるかもしれませんが、確かにそこに愛はあります!
7. 愛(セキュリティ)とは、楽しむこと
   人もいない、予算もつかない、平常時には褒められないなど、愚痴や文句のひとつも言いたくなるかもしれませんが、あなたはひとりではありません。一緒に楽しみましょう!

いかがですか? 「セキュリティ=愛」だということがおわかりいただけたのではないでしょうか。一緒にサイバーの世界を愛で満たしましょう!

2.5 国際標準化活動

国際標準とは、製品や技術を、国境を越えて利用するために制定される国際的な共通規格であり、国際規格とも呼ばれる。国際標準化は第4次産業革命時代の鍵を握る※326として、日本も積極的に活動に参画している。

本節では、セキュリティ分野に関わる国際標準化活動の動向を紹介する。

2.5.1 様々な標準化団体の活動

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

(1) 日本の国際標準化活動への取り組み

1995年にWTOにより、貿易の技術的障害に関する協定（WTO/TBT協定）が発効し、加盟国が製品や技術に適用する強制規格や適合性評価手続きの作成の際には、原則として国際規格（ISO/IEC等）を基礎とすることが義務付けられた※327。翌1996年、WTO政府調達協定が発効し、政府調達における技術仕様等には国際規格を基礎とすることが各国に義務付けられた。欧米各国は、国際競争力強化のために国際標準化活動を重要と考えて取り組んできたが、日本でも「知的財産推進計画2010※328」において国際標準化を知的財産政策の第1項に掲げ取り組んできた。

標準化は製品の仕様や性能等の実体物の形態や機能を対象として進展してきたが、徐々に対象が拡大し、サービスや社会システム・環境等の形のないものや仕組みを対象とするようになってきた。また、技術開発スピードの高まりや国際社会における新興国の存在感の高まり等により、標準化検討プロセスの加速や標準化活動を担う人材の育成が強く求められるようになった。このような環境変化に対応するため、日本における標準化活動の基盤となっている工業標準化法が2018年5月に改正され、2019年7月に施行された。これに伴い、「工業標準化法」は「産業標準化法」に、「日本工業規格（JIS: Japanese Industrial Standards）」は「日本産業規格（JIS）」に変わった。また、法目的に国際標準化の促進を追加するとともに、産業標準化及び国際標準化に関する国、国立研究開発法人・大学、事業者等の努力義務規定が設けられた※329。

(2) 標準の分類

国際標準には、公的な標準化団体により所定の手続きを経て制定される「デジュール標準（de jure standard）」、いくつかの団体（企業等）が協力して自主的に作成する「フォーラム標準（forum standard）※330」、公的な標準化団体を介さず、市場や業界において広く採用された結果として事実上標準化される「デファクト標準（de facto standard）」がある。

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

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

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

(3) 情報セキュリティ分野に関する標準化団体

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

- ISO（International Organization for Standardization: 国際標準化機構）/IEC（International Electrotechnical Commission：国際電気標準会議）JTC 1（Joint Technical Committee 1：第一合同技術委員会）※331：情報セキュリティを含む情報技術の国際規格を策定している。コンピュータや情報分野を扱う国際標準化団

体としてISO、IECはそれぞれ独立に存在しているが、扱う領域の競合を避けるために双方が連携し、JTC1が設立された。日本国内の標準化団体としては、日本産業標準調査会（Japanese Industrial Standards Committee：JISC）がISO、IEC双方のメンバーであり、JTC 1でも活動している※332。

- ITU-T（International Telecommunication Union Telecommunication Standardization Sector：国際電気通信連合 電気通信標準化部門）：
  電気通信技術に関わる国際規格を策定している。情報セキュリティに関してはSG（Study Group）17が設置され※333、ISOや後述するIETFとともにネットワークやID管理等に関する標準化活動を行っている。策定した標準はITU勧告として定められる。

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

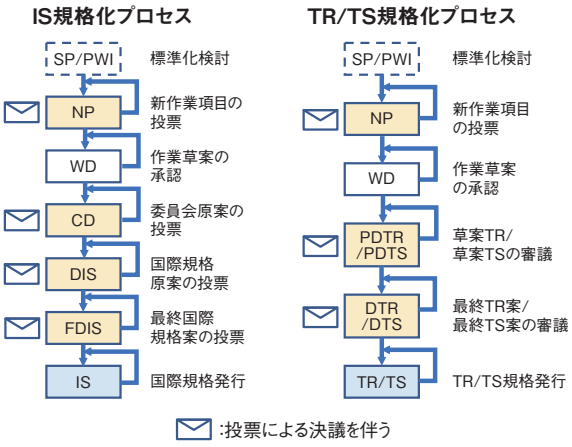
- IEEE（The Institute of Electrical and Electronics Engineers, Inc.）：
  電気工学・電子工学技術に関する国際学会である。標準化活動は内部組織であるIEEE-SA（Standards Association）が行っている。情報セキュリティについては、サイバーセキュリティ、ネットワークセキュリティ、IoTセキュリティ等の広範な領域で標準化を行っている。
- IETF（Internet Engineering Task Force）：
  インターネット技術の国際標準化を行う任意団体である。非常にオープンな組織であり、作業部会のメーリングリストに登録することで誰でも議論に参加することができる。情報セキュリティについては、インターネット上のセキュアなプロトコル、暗号、署名、認証、セキュリティ情報連携（セキュリティオートメーション）等の方式の標準化を行っている※334。標準化した技術文書はRFC（Request For Comments）として参照することができる。
- TCG（Trusted Computing Group）：
  信頼できるコンピューティング環境（埋め込み機器、パソコン／サーバ、ネットワーク等）に関するセキュリティ技術の標準化を行う業界団体である。ハードウェア、ソフトウェア等のベンダやシステムインテグレータがメンバーとなり、中国、日本にregional forumがある※335。

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

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

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

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



■図2-5-1　ISO/IEC JTC 1/SC 27における文書のステータス
（出典）JISC「ISO規格の策定手順※336-1」を基にIPAが作成

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

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

PDTS：予備技術仕様書原案（Preliminary Draft Technical Specification）
DTR：技術報告書原案（Draft Technical Report）
DTS：技術仕様書原案（Draft Technical Specification）
TR：技術報告書（Technical Report）
TS：技術仕様書（Technical Specification）

2019年度は、4月にWG会議と総会がテルアビブ（イスラエル）、10月にWG会議がパリ及びサンドニ（フランス）で開催された（以下、テルアビブ会議、パリ会議）。

なお、SC27のタイトルについて、活動範囲が広がっていることから見直しがされ、総会において「Information security, cybersecurity and privacy protection」とすることが承認された※336-2。

以下に、各WGの活動概要を述べる。

（1）WG 1（情報セキュリティマネジメントシステム）

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

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

2013年の改訂から5年を経たISO/IEC 27002:2013については、2018年3月までの1年間のSPにおいて、次期改訂の設計仕様（Design Specification）が決定され、改訂作業が開始されている。2018年4月及び10月、並びに2019年4月に、それぞれWDを発行し、エキスパートレベルでの審議を進めてきたが、2018年11月にはCDの初版を発行、国レベルでの審議にステージを移した。2020年4月現在、管理策の全体構成については、大枠が固まり、今後は管理策の具体的な内容を決める段階となっている。

ISO/IEC 27001:2013については、2019年に実施された、改訂の必要性を各国に問う定期レビューの結果、Confirm（改訂しない）という結論となり、改訂作業は開始されていない。これは、ISO/IEC専門業務用指針、第1部において規定されたマネジメントシステム規格の共通フォーマットが改訂中の状況を考慮し、並行してISO/IEC 27001を改訂することは、改訂作業を複雑にすると考えての結論である。ただし、今回の定期レビューの結論は改訂しないこととなったが、SC 27/WG 1では、共通フォーマット及びISO/IEC 27002の改訂がISO/IEC 27001に与える影響評価を継続して行っており、この評価結果によっては、次の定期レビューを待たずに、ISO/IEC 27001改訂を検討することも想定されている。

(b) 分野別規格の国際標準化活動

分野別規格作成に関する要求事項を示す規格であるISO/IEC 27009は2016年に発行された後、2017年から早期改訂が行われ、2020年4月に改訂版が発行された。

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

一方、ISO/IEC 27009は、ISO/IEC 27001を特定分野に適用した規格を作成する際の、規格の記述方法や様式等を定めた規格であり、ISO/IEC 27002だけの拡張は適用範囲としていない。ISO/IEC 27009に適合する規格としては、エネルギー分野に関する規格としてISO/IEC 27019:2017、プライバシー情報マネジメントに関する規格としてISO/IEC 27701:2019※337が発行済みである。なお、ISO/IEC 27701については、これに基づく認証に対する市場ニーズが高いことから、ISO/IEC 27701の認証機関に対する認定基準となるISO/IEC TS 27006-2を早期に策定するWG 1とWG 5の共同プロジェクトを開始した（「2.5.2（5）（b）プライバシー」参照）。ISO/IEC 27002を拡張した分野別規格については、次期改訂において、ISO/IEC 27002の改訂への対応に加えて、ISO/IEC 27009への適合、すなわち、ISO/IEC 27001の要求事項の拡張についても検討される可能性がある。ISO/IEC 27011については、これら2点を主たる目的として、既に改訂が開始されている。

(c) サイバーセキュリティ関連の国際標準化活動

新たなトピックである、サイバーセキュリティに関する規格化については、まず、サイバーセキュリティの既存のフレームワークとISO及びIEC規格類との対応関係を示した技術報告書ISO/IEC TR 27103が2018年に発行された。次いで、サイバー保険に関する規格ISO/IEC 27102が2019年に発行された。サイバーセキュリティのフレームワーク構築に関する技術仕様書ISO/IEC TS 27101は、DTS審議中の状況にある。また、サイバーセキュリティの概念やコンセプトに関する規格についても検討が進められており、これはWD審議中の状況である。ただし、サイバーセキュリティに関する解釈は各国、各組織で多様化しているため、対象範囲の決定や用語定義等を行うことは難しく、規格化に向けた課題はまだ多い。

(d) その他のISO/IEC 27000ファミリー規格の国際標準化活動

ISO/IEC 27001:2013への本格的対応を積み残している情報セキュリティリスクマネジメントに関するガイドライン規格ISO/IEC 27005については、2020年4月時点でも改訂中でWDを検討中である。引用規格※338の改訂に伴う改訂も行われている。ISO/IEC 27007:2017は、ISO 19011にISMS固有のガイダンスを加えた規格であるが、ISO 19011:2018の発行に対応し、2020年に改訂版が発行された。ISO/IEC 27013:2015はISO/IEC 20000-1及びISO/IEC 27001の統合実践に関するガイドライン規格であるが、ISO/IEC 20000-1:2018の発行を受けて、2020年4月時点で改訂中である。

また、ISO/IEC 27009の発行、及びこれに適合した分野別規格の発行に伴い、分野別に拡張されたISMSを認証するニーズが生じてきている。ISO/IEC 27006は、ISMS認証を希望する組織の審査・認証を行う認証機関に対する要求事項を規定した規格であるが、分野別ISMS規格に対する認定のための要求事項について、ISO/IEC 27006に相当する規格の発行等の検討が開始されている。前述(b)のISO/IEC TS 27006-2の検討はこの取り組みの一つである。

(2) WG 2(暗号とセキュリティメカニズム)

WG 2では、暗号プリミティブ(暗号アルゴリズム)や、デジタル署名技術、鍵共有のような汎用的かつ基本的な暗号プロトコル等の標準化を行っている。WG 2の国際主査、副主査ともに日本人が選出され、WG 2での活動をリードしている。2019年度は、新しい規格3件(「暗号アルゴリズム　第6部:準同型暗号(ISO/IEC 18033-6)」「軽量暗号　第6部:メッセージ認証コード(MAC)(ISO/IEC 29192-6)」「軽量暗号　第7部:放送型認証プロトコル(ISO/IEC 29192-7)」)、及び既存規格3件の改訂版が発行された。このほかの主な活動内容について以下に示す。

(a) ブロック暗号Kuznyechikの標準化中止

「暗号アルゴリズム　第3部:ブロック暗号(ISO/IEC 18033-3)」へロシアからブロック暗号Kuznyechikの提案があり、追補として規格化作業が行われていた。一方、中国から同規格へブロック暗号SM4の提案があり、追補として規格化作業が並行して行われていた。両暗号がそれぞれ最終国際追補案(FDAM:Final Draft Amendment)へ到達したため、両暗号を盛り込んだ改訂版のFDISを準備していた。

しかし、2019年1月にフランスの研究者から、Kuznyechikに使用されているSボックス(入力・出力変換関数)は、設計者が主張するようなランダム性を持つようには生成されていないとの論文が発表された。このため、WG 2内でもKuznyechikの扱いが議論になった。解読はされていないので問題ないとのロシアの主張に対し、多くの国が安全性に疑義を持つことになったため標準化すべきではないとの意見が出された。

その後、ブロック暗号Kuznyechikの標準化中止(FDISのキャンセル)の提案が行われ、いくつかの投票を経て、最終的に標準化の中止が決まった。なお、中国のSM4には問題がないため、追補原案(DAM:Draft Amendment)から標準化作業を再開する。

(b) 安全なマルチパーティ計算の新規標準化

データを暗号化したままで処理することを可能にする秘密計算は、強固な情報漏えい対策技術として期待されている。秘密計算の中でもデータを複数のマシンに秘密分散したまま処理する技術がマルチパーティ計算である。

日本からマルチパーティ計算の標準化提案を行い、「安全なマルチパーティ計算　第1部:概要(ISO/IEC 4922-1)」「安全なマルチパーティ計算　第2部:秘密分散に基づく機構(ISO/IEC 4922-2)」の2部構成で標準化することが2020年4月に承認された。エディタは日本とオーストリアが務め、2023年の規格の発行を目指している。

(3) WG 3(セキュリティの評価・試験・仕様)

WG 3 は 2019 年 4 月にテルアビブ（イスラエル）、10 月にサンドニ（フランス）にて定期会議を開催した。2020 年 4 月にサンクトペテルブルグ(ロシア)で予定された会議は新型コロナウイルスのためキャンセルされ、Zoom 会議にてオンライン開催された。それらの会議の議論内容を以下に概説する。

(a) ISO/IEC 20897 の開発

ISO/IEC 20897（Security requirements, test and evaluation methods for physically unclonable functions for generating nonstored security parameters） で は、PUF（Physically Unclonable Function）と呼ばれる技術のセキュリティ要件、及びそのテスト手法に関する標準化が行われている。PUF は半導体チップ固有の物理特性から識別 ID や暗号鍵を生成し、IoT 機器等の認証やデータ秘匿等に用いる技術である。

本規格はパート 1、パート 2 に分かれており、パート 1 では PUF のセキュリティ要件(例えば、PUF から生成される識別 ID や暗号鍵は、予測不可能なランダムな値でなければならない等）を規定している。このパート 1 はテルアビブ会議にて DIS のための投票に進むことが合意され、その投票結果は Zoom 会議にて議論され、FDIS に進むことが合意された。パート 2 は、パート 1 のセキュリティ要件が正しく製品に実装されていることを検証するための手法を定めているが、その検証手法の大枠が定まったこともあり、サンドニ会議にて CD に進むことが合意され、Zoom 会議では更なる技術的な議論を行うため、CD2 に進むことが合意された。なお本標準化に関しては、昨年度より引き続き PUF の研究プロジェクト※339 の成果を反映すべく、日本の技術者が積極的に標準化に貢献している。

(b) ISO/IEC 23837 の開発

ISO/IEC 23837（Security requirements, test and evaluation methods for quantum key distribution）では、量子鍵配信(QKD：Quantum Key Distribution)のセキュリティ要件、及びそのテスト手法に関する標準化が行われている。QKD とは、暗号鍵を光子に乗せ伝送する技術であるが、この QKD による暗号鍵配送方式は、第三者による鍵の盗聴を確実に検知することが、量子力学の理論上保証されている。QKD を利用することにより、情報漏えいを完全に防げるとされる暗号技術、量子暗号通信が実現可能となる。

QKD では、光子の送受信は QKD 送信機及び受信機により行われるが、理論どおり鍵の盗聴を検知するためには、それら送受信機は所定のセキュリティ要件を満たす必要がある。例えば、送受信機には一般の IT 製品と同様に管理機能が存在するが、管理機能を悪用した攻撃が想定される。また、QKD 送受信機自体も、理論上セキュアであると保証された QKD プロトコルに従い光子を送受信しなければならない。本規格は、QKD 送受信機等が満たすべきセキュリティ要件及びその検証手法を定めることを目的にしており、テルアビブ会議にて規格開発が承認され、パリ会議、Zoom 会議にて WD1、WD2 に基づく議論が実施された。日本からも 2019 年に設立された一般社団法人量子 ICT フォーラム※340 のメンバーがこの WD1、WD2 に対し数多くのコメントを提出し、本規格開発に大きく貢献している。

(c) ISO/IEC 15408、ISO/IEC 18045 の改訂

ISO/IEC 15408（Evaluation Criteria for IT security）及び ISO/IEC 18045（Methodology for IT security evaluation）は WG 3 の主要規格の一つであり、IT 製品のセキュリティ機能を評価する手続きを定めた国際標準である。本規格をより柔軟に適用可能にするため、数々の新たな評価の枠組みが導入されたことを「情報セキュリティ白書 2019」にて概説※341 したが、CD の成熟度が高まったことからパリ会議にて DIS に進むことが合意され、早ければ 2020 年度中の出版が見込まれる状況にある。

(d) 研究期間による規格開発

2019 年、WG 3 においては、コネクテッドカーのセキュリティ評価やハードウェアトロイ等、計九つの SP を開始することが、中国、フランス、米国、英国等から提案され WG 3 総会で承認された。コネクテッドカーに関しては、現在 ISO/SAE 21434(Road vehicles — Cybersecurity engineering)を開発中の ISO/TC 22/SC 32/WG 11 議長等をパリ会議、Zoom 会議に招き、今後の規格開発の方向性を検討している。またハードウェアトロイに関しては、日本でも 2019 年度に研究プロジェクト※342 が立ち上がっており、そのプロジェクトメンバーも Zoom 会議に参加し、研究期間の副ラポータになることが承認された。

(4) WG 4(セキュリティコントロールとサービス)

WG 4 では、WG 1 が対象とする ISMS を実施・運

用する際に必要となる具体的なセキュリティ対策、及びセキュリティサービスの標準化を行っている。以下に、WG 4における2019年度の主な成果、活動を紹介する。

(a) IoT セキュリティ／プライバシーのための標準化活動

WG 4では、IoT セキュリティ／プライバシーに関わる標準化として、以下の三つの活動を進めている。

- ISO/IEC 27030: Cybersecurity – IoT security and privacy – Guideline
- ISO/IEC 24391: Security techniques – Guidelines for IoT-domotics security and privacy
- ISO/IEC 27402: Cybersecurity – IoT security and privacy – Device baseline requirements

(ア) ISO/IEC 27030: Cybersecurity – IoT security and privacy – Guideline

我が国は、IoT 関連の製品・システム開発の競争力を強化し、またIoTの国際的なセキュリティレベル向上に寄与するために、IoT 推進コンソーシアムが策定した「IoT セキュリティガイドライン※343」の国際標準化を提案した。具体的には、本ガイドラインに基づき、ISO/IEC 27030（IoT のセキュリティとプライバシー）、ISO/IEC 30147（IoT システム／サービスの信頼性のための方法論）の二つの規格案がそれぞれ SC 27/WG 4、及び SC 41/WG 3で審議されている。以下にISO/IEC 27030の規格について概説する。

ISO/IEC 27030の具体的内容に当たる第5章以降では、第5～6章で参照モデル、各ステークホルダーの役割、IoT ライフサイクルに触れ、IoT システムにおけるリスクについて言及する。第7章では、セキュリティ対策、及びプライバシー対策が、開発者／サービスプロバイダ、ユーザのそれぞれの立場での対策内容、目的、導入ガイドといったガイドライン的表現で記載されている。

パリ会議において、ISO/IEC 27030は、CD1となり、規格案としての完成度が一定のレベルとなった。本規格に対するコメントは、日本、フランス、カナダ、ドイツ、米国、インド、中国等の多くの専門家から大量に提出されており、審議は極めて活発である。本規格はIoT セキュリティ及びプライバシーのための規範となるガイドラインであるため、IoT ステークホルダーにおける認証等への活用が期待されている。

(イ) ISO/IEC 24391: Security techniques – Guidelines for IoT-domotics security and privacy

本規格は、テルアビブ会議において、中国からNPとして提案され、パリ会議では、NPの承認がなされ、WD1が作成された。「IoT-Domotics」とは、娯楽、機器制御、監視等の用途として、居住環境で利用するIoT サービスをいう。本規格は、ISO/IEC 27030との棲み分けが難しい部分が多いものの、IoT-Domoticsの特性を抽出し、ISO/IEC 27030と整合を取る形で規格化を進めるとしている。

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

本NPは、米国から強く提案されたもので、IoT 機器が備えるべきセキュリティメカニズムのベースラインとなる要件の規定を目指している。ISO/IEC 27030とは異なるスコープを掲げ、IoT 機器に特化した要件化を視野に入れ、NIST 及び ETSI（European Telecommunications Standards Institute：欧州電気通信標準化機構）の既存のガイドラインを下敷きに標準化することを想定している。NP案に添付されたベースライン的要件としては、以下が例示されている。

- Device Identification（機器の識別）
- Device Reset（機器のリセット）
- Configuration（構成）
- Data Protection/Security（データ保護とセキュリティ）
- Software and Firmware updates（ソフトウェア、ファームウェアのアップデート）
- Interface access（インタフェースアクセス）
- Telemetry（テレメトリ）
- Vulnerability Disclosure（脆弱性情報の開示）
- Secure Storage（セキュリティの確保されたストレージ）

上記の要件は、あるレベルでISO/IEC 27030においても記載されているため、今後の規格策定においては、ISO/IEC 27030との棲み分け、役割分担に注視する必要がある。

(b) ビッグデータセキュリティ／プライバシーのための標準化活動

ビッグデータとは、主にボリューム、多様性、速度、及び／または変動性の特性を有し、効率的な保管、操作、分析のためにスケーラブルなアーキテクチャを必要と

する広範なデータセットのことを指す。ビッグデータを用いた分析により、より優れた意思決定や戦略的なビジネス行動につながる洞察等を導き出すことができるため、近年注目を浴びている。WG 4 では、ビッグデータのセキュリティ／プライバシーに関わる標準化として、以下の三つの活動を進めている。

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

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

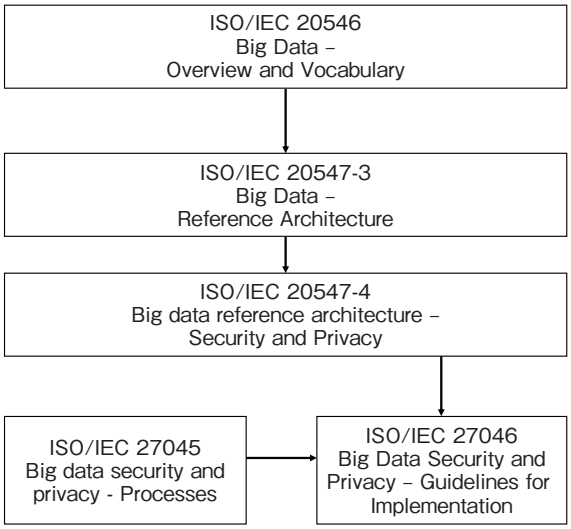
ISO/IEC JTC 1/SC 42 で審議されている、ISO/IEC 20547（ビッグデータ参照体系）は四つのパートから成り立っている。そのうちパート 4 は、SC 42 の依頼により SC 27/WG 4 で審議されており、セキュリティ及びプライバシーに関わる参照体系を規定している。本規格は、パリ会議において CD2 をベースにコメント審議を行った。日本は、品質や ISO/IEC 20547-3 との整合性の課題等の理由で DIS に進むことを反対し、米国、フランス、スウェーデン、スイスも同様に反対したものの、結果的には DIS に進むこととなった。

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

本規格は、組織のビッグデータのセキュリティとプライバシーを評価及び改善するためのプロセスの参照モデル、評価・成熟度モデルを規定する。プロセスには、プロセスパフォーマンスとプロセス機能の一連のインジケーターが含まれ、評価者が評価の良し悪しを決めるための客観的証拠の基礎として使用される。現在の規格内容は、ISO/IEC JTC 1/SC 7 で規格化されている ISO/IEC 33004、ISO/IEC 33002 等を参照する形で記載されている。パリ会議において、WD2 が審議され、次回の会議においては、WD3 に進めることとなった。

(ウ) ISO/IEC 27046: Big data security and privacy – Guidelines for implementation

本規格は、ビッグデータのセキュリティとプライバシーの主要な課題とリスクを分析し、ビッグデータのリソース、組織化、分散化、計算能力及び破壊等の視点から、ビッグデータのセキュリティとプライバシーの実装のためのガイドラインを記述することを狙っている。パリ会議においては、前述の(ア)と(イ)の規格との差別化について審議され、図 2-5-2 のように整理された。



■図 2-5-2　ビッグデータセキュリティ／プライバシー関連規格間の関係性

本課題は、テルアビブ会議にて NP 提案がなされ、パリ会議ではその承認と WD1 に進むことの合意がなされた。

(c) WG 4 に関連するその他の規格群

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

- ビジネス継続のための ICT 準備技術（27031）：PWI から仕切り直し
- インターネットセキュリテイガイドライン（27032）：WD3 に進むことが決定
- ネットワークセキュリティ（27033）：改版作業なし
- アプリケーションセキュリティ（27034）：パート 4 が DIS に移行、他パートは規格化完了
- インシデントマネジメント（27035）：パート 3 が DIS に移行
- サプライヤー関連セキュリティ（27036）：全パートを視野に入れた改版作業の検討中
- デジタルエビデンスの識別、収集、確保、保全（27037）：改版作業なし
- リダクション（墨消し技術）（27038）：改版作業なし
- IDPS（侵入検知システム）（27039）：改版作業なし
- ストレージセキュリティ（27040）：大規模な改版を視野に入れ NP として仕切り直し

- 仮想化サーバの設計／実装のためのセキュリティガイドライン(21878):改版作業なし
- 産業用インターネット基盤のためのセキュリティ参照体系(24392):WD1に進む
- 仮想化された信頼のルートのためのセキュリティ要件(27070):CD1に進む
- 公開鍵基盤における実践とポリシーの枠組み(27099):CD1に進む
- 機器とサービス間の信頼接続の構築のためのセキュリティ推奨(27071):WD2に進む
- 安全な配備、アップデート、及びアップグレード(4983):NPの審議に進む
- データの起源―参照モデル（データ追跡のため):PWIとして審議継続
- 情報セキュリティインシデント対応の調整:PWIとして審議継続
- セキュリティオペレーションセンター（SOC）のガイドライン:PWIとして審議継続

(5) WG 5(アイデンティティ管理とプライバシー技術)

WG 5では、アイデンティティ管理、プライバシー、バイオメトリクスの標準化を行っている。2019年度の主な活動を紹介する。

(a) アイデンティティ管理

2013年4月に発行されたユーザ認証についてのフレームワーク規格であるISO/IEC 29115について、アイデンティティ管理全般についての規格であるISO/IEC 24760との整合性を確保したり、複数要素認証等の技術動向に合わせたりする改訂作業が進められている。

(b) プライバシー

プライバシー対策に関わる規格であるISO/IEC 27701:2019は、2019年8月にISとして発行された。本規格は、ISMSの要求事項を規定したISO/IEC 27001及びISMSを実施するためのプラクティスをまとめたISO/IEC 27002に、プライバシー対策に関する要求事項及びプラクティスを追加することにより、プライバシー対策に関するマネジメントシステム構築を支援することを目的としている。本規格はこれまで、ISO/IEC 27552として規格策定作業が行われていたが、マネジメントシステム規格（MSS:Management System Standard）※344の番号付けルールに従い、IS発行時に番号がISO/IEC 27701と改められた。2019年12月には、本規格を基にして認証や審査を行う組織に対する要求事項を定める新たな規格提案があり、WG 1とWG 5合同のプロジェクトとして作業が開始された(「2.5.2(1)(b)分野別規格の国際標準化活動」参照)。

日本提案の規格としては、経済産業省が2014年10月に公開した「消費者向けオンラインサービスにおける通知と同意・選択に関するガイドライン」に基づく国際規格であるISO/IEC 29184が、2020年6月にISとして発行された。また、同じく日本提案である「ユーザのプライバシープリファレンスに基づくユーザ主導によるPII処理のためのフレームワーク」は、2019年5月に新たな規格策定プロジェクトとして承認された。2020年4月現在、CD投票に向けて規格案の内容を精査しているところである。

(c) バイオメトリクス

バイオメトリック認証をリモート環境でも使用可能にするためのデータ構造を定義するISO/IEC 24761:2019は、改訂が進められ、2019年10月にISとして発行された。バイオメトリックデータの保護技術を扱うISO/IEC 24745は、2011年に発行されたが、その後の新技術を反映するための改訂が進み、CD段階にある。また、モバイル機器上でのバイオメトリクスを使った認証に対するセキュリティ要件を定めるプロジェクトISO/IEC 27553は、WD段階にある。スマートフォンへのバイオメトリクスの適用が進みつつある中、このプロジェクトは関心を集めている。

2.5.3 信頼性の高いコンピューティング環境の実現に向けたセキュリティ標準(TCG)

TCG（Trusted Computing Group）※345は、高い信頼性を持つコンピューティング環境実現のため、多様な機器やネットワーク、あるいは異なるレベルに対応するセキュリティ技術に関して統一的な標準仕様を開発、策定、普及させることを目的とし、2003年に発足した国際的非営利団体（NPO:Non-Profit Organization）である。TCGは、2020年2月現在、世界各国77の企業、30以上の政府機関、業界団体、大学、専門家で構成されている。

日本からはIPA、NICTを始めとする多数の機関、企業、専門家が参加している。前身のTCPA(Trusted Computing Platform Alliance）発足が1999年であったことから、2019年に設立20周年を迎え、記念イベン

トの開催等のキャンペーンを行った。

セキュリティチップTrusted Platform Module（TPM）を信頼の基点（Root of Trust）とし、自己暗号化ドライブ、高信頼ネットワーク、高信頼なパソコン／スマートフォン／自動車／ IoT ／産業機器等を実現する多種の仕様策定、公開を進めている。

TPM は 2004 年に世界各社のパソコンに搭載が開始された。その仕様は 2009 年に ISO/IEC 11889：2009 として公開、更に 2015 年に改訂版 TPM2.0 仕様（TPM Library Specification）が ISO/IEC 11889：2015 として公開されている※346。

TCG 初となる地域支部は日本に 2008 年に設立された※347。この日本支部（JRF：Japan Regional Forum）では、国内に向けて、ストレージ、サーバ、ネットワーク等での TCG 標準仕様の普及を目指し、種々の活動を行っている。2019 年には勉強会やワークショップ※348 を開いており、その実績と経験を日本から世界へ発信している。

2020 年 2 月現在、20 あるワークグループが、2019 年 2 月から 2020 年 2 月の間に公開した活動※349 の中から、以下では三つのワークグループ、及び JRF のワークショップについて紹介する。

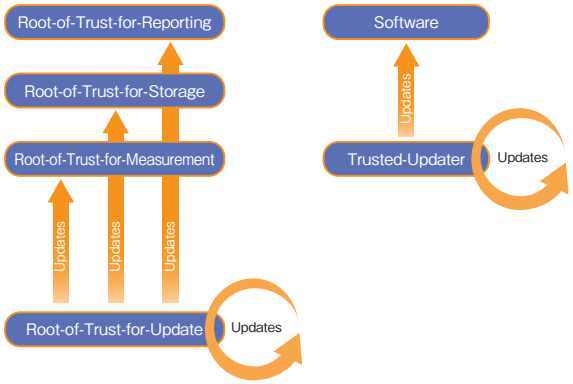
（1）組み込み機器ワークグループ（Embedded Systems WG）

パソコンへの実装から始まった TPM を、組み込み機器に幅広く展開する目的で活動している※350。

本 WG 配下の自動車サービスサブグループでは、TPM 仕様を自動車向けに最適化し、2015 年に初版公開、2018 年に Version 1.01 Revision 15 を改訂公開した※351。この版に合わせたセキュリティ要件（Protection Profile）に関しては、「Protection profile Automotive-Thin Specific TPM for TCG TPM 2.0 Automotive Thin Profile Family “2.0” Level 0」として 2019 年 2 月に確定版を公開した※352。自動車向けユースケースとしては、車載機器リモートメンテナンス、近年話題の自動運転用情報転送及びドライブレコーダ内データ保証等があり、これらについても検討を続けている。

同じく本 WG 配下の IoT サブグループでは、IoT 機器での TPM 活用による遠隔ソフト／ファームウェア更新のガイドラインとして「TCG Guidance for Secure Update of Software and Firmware on Embedded Systems※353」を 2020 年 2 月に公開した。本ガイドラインに記載されている「信頼されるプラットフォームに基づくアップデートの流れ」を図 2-5-3 に示す。作業の出発点として、TPM を主とする「Root-of-Trust-for-Update」を置き、そこでアップデート内容の信頼性を確認した後に順に上位層を動かしてアップデートを行う仕組みである（図 2-5-3 の左）。

また、IoT 機器の制約から簡略化した実装方式も用意されている。「Trusted-Updater」も、「Root-of-Trust-for-Update」と同様、作業の出発点として機能し、そこでアップデート内容の信頼性を確認した後に上位のソフトウェアのアップデートを行う仕組みである（図 2-5-3 の右）。



■図 2-5-3　信頼されるプラットフォームに基づくアップデートの流れ
（出典）TCG「TCG Guidance for Secure Update of Software and Firmware on Embedded Systems」を基に IPA が編集

（2）Device Identifier Composition Engine Architectures ワークグループ（DICE WG）

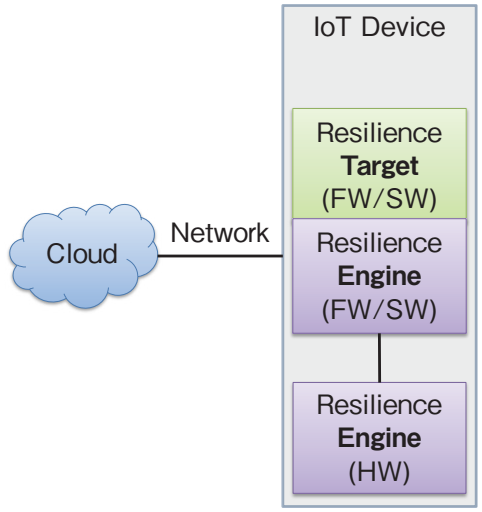
DICE WG は、前述の Embedded Systems WG から 2017 年に独立し、RIoT（Robust IoT）の Core 仕様上で動作するソフトウェア群の策定を目指している。特に TPM 利用システムだけでなく、TPM を使わないシステムでもデバイス ID を最小のシリコンリソースで実現できる新しい ID 管理アーキテクチャの開発を目指している。本 WG は 2020 年 1 月に「Symmetric Identity Based Device Attestation」を仕様として公開した※354。

（3）Cyber Resilient Technologies ワークグループ（CyRes WG）

2018 年 5 月に NIST が公開したファームウェアの攻撃耐性（レジリエンス）に関するセキュリティ規格である文書 SP800-193 を補完する（NIST の Requirement に対する実現可能な Solution を提供する）ことを目的の一つとして、2018 年 6 月に設立された WG である。NIST は TCG のリエゾンの一つであり、両者は密接に交流している。

2019 年 6 月の公開セミナーでは、本 WG の議長であ

る Microsoft 社のメンバーが「TCG Cyber Resilient Technologies - Trusted Computing Group」と題する講演を行った。この中で、本 WG と NIST SP800-193 の関係が説明された。図 2-5-4 は、その講演資料に記載されている「IoT を例とする遠隔からのリカバリーの流れ」である。この図で IoT Device の最下辺に位置する「Resilience Engine (HW)」は、図 2-5-3（前ページ）で説明した TPM を主とする「Root-of-Trust-for-Update」と同じ位置付けである。ここを信頼の基点として作業を進め、上位層を動かす仕掛けである。



■図 2-5-4　IoT を例とする遠隔からのリカバリーの流れ
（出典）TCG「TCG Cyber Resilient Technologies※355」を基に IPA が編集

(4) JRF の活動

JRF は 2008 年に発足して以来毎年イベントを開催している。2019 年 12 月には、FIDO Alliance※356-1、JPCERT/CC、IPA、NICT の協力／後援を受け、「IOT 時代に求められる Security by design のその先へ」をテーマに公開ワークショップを開催した。ワークショップでは、「TCG 最新動向の紹介」等の講演、パネルディスカッションのほか、多数のデモ展示が行われた※348。

COLUMN

セーフティ&セキュリティ

セーフティの英単語である Safety の意味は、安全、無事[i]等であり、セキュリティの英単語である Security の意味は、安全、安心、防衛[ii]等を意味します。どちらも「安全」の意味を持つので、違いがあまり分からないという方も多いかもしれません。

ISO や IEC 等の国際標準では、セーフティは、「許容不可能なリスクがないこと[iii]」、「許容できないリスクから免れている状態[iv]」、「安全（safety）とは，事故や損失がないことである。[v]」等と定義されます。一方、セキュリティとは、「攻撃により情報が漏えいする等の被害が起きないようシステムを守ること[vi]」等とされます。

また、両者の違いを「何を守るのか」という保護対象の観点で考えると、セーフティは人命、財産（家屋等）ですが、情報セキュリティでは情報の「機密性，完全性、可用性等[vii]」になります。そして「何から守るのか」という原因の観点で考えると、セーフティは偶発的なミス、故障等の確率的に発生する危険に対する安全を指すのに対し、セキュリティは、主に人為的に行われる脅威に対する安全を指します。つまり、原因に悪意があるかどうかが大きな違いになります。

モノづくりの国、日本において、自動車、家電、医療機器等の開発・生産とセーフティの関わりは深く、人の生命や健康に影響を及ぼすため、セーフティが重要視されてきたという長い歴史があります。セーフティは人のミス対応にはじまり、機械の故障対応、人と機械の協調対応へと対応の幅をひろげてきました。

一方、セキュリティはインターネットが一般に普及してきた 2000 年前後から注目され始め、インターネットを通じた攻撃の目的が、いたずらから金銭的利益へと変化するにつれて急速に重要分野となりました。サイバー犯罪のブラックマーケットは巨大化してきており、IoT をターゲットにした攻撃や AI を悪用した攻撃によって、更に社会に深刻な影響を与えることも想定されます。例えば、インターネットとつながる自動車や医療機器等も遠隔操作による攻撃を受け、人命を脅かすようなセキュリティの脅威に晒されることが分かり、各メーカも対応を進めています。

あらゆる機器・システムが複雑に影響を及ぼし合う AI と IoT の時代の到来に備えて、安全安心にシステムを利用できるように、セーフティ&セキュリティの実現が求められています。

i　株式会社研究社：新英和中辞典　https://ejje.weblio.jp/content/Safety〔2020/6/30 確認〕
ii　株式会社研究社：新英和中辞典　https://ejje.weblio.jp/content/security〔2020/6/30 確認〕
iii　ISO：ISO/IEC Guide 51:2014　https://www.iso.org/standard/53940.html〔2020/6/30 確認〕
iv　IEC：IEC 61508-4 Edition 2.0　https://www.iec.ch/functionalsafety/standards/page2.htm〔2020/6/30 確認〕
v　ナンシー・G・レブソン著、松原友夫監訳・訳、片平真史、吉岡律夫、西康晴、青木美津江訳：セーフウェア　安全・安心なシステムとソフトウェアを目指して、2009 年 10 月、p.175
vi　SQuBOK 策定部会編：ソフトウェア品質知識体系ガイド（第 2 版）－ SQuBOK Guide V2 －、2014 年 11 月、p.38
vii　ISO：ISO/IEC 27000:2018　https://www.iso.org/standard/73906.html〔2020/6/30 確認〕

2.6 安全な政府調達に向けて

IPA では、国民に向けた情報セキュリティに関する啓発活動のほか、政府機関や独立行政法人が安全に IT 製品等を調達するために活用できる制度の運営や利活用のための普及活動を行っている。

本節では、IT 製品のセキュリティ機能の適切性と妥当性を評価する「IT セキュリティ評価及び認証制度」の動向や安全な IT 調達に向けた新たな取り組み、及び暗号アルゴリズムの適切な実装を確認する「暗号モジュール試験及び認証制度」の動向について報告する。

2.6.1 ITセキュリティ評価及び認証制度

サイバーセキュリティ戦略本部の発行した「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」（以下、政府統一基準）では、府省庁及び独立行政法人が遵守すべき情報セキュリティ対策の基準を示しており、例えば公的なサービスにおいて国民の情報等を扱うシステムを構築する場合、そのシステムを構成する市販の IT 製品のセキュリティ要件を策定することを調達者に求めている。

このようなセキュリティ要件を確保する手段として、多くの国々では第三者が IT 製品の情報セキュリティを評価し、公的機関がその評価結果に基づき評価された IT 製品に認証を与える制度が用いられている。日本でも「IT セキュリティ評価及び認証制度（JISEC：Japan Information Technology Security Evaluation and Certification Scheme）」を IPA が運営し、政府機関等の調達に活用されている。

(1) 政府調達のセキュリティ要件

政府統一基準では、特にセキュリティ要件を策定すべき IT 製品として、経済産業省が発行している「IT 製品の調達におけるセキュリティ要件リスト」（以下、要件リスト）を参照している。この要件リストには、情報システムの基盤となり、攻撃の対象となり得る以下の 11 の製品分野が指定されている。

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

府省庁や独立行政法人の情報システムセキュリティ責任者は、これらの製品分野の IT 製品を調達する場合、想定されるセキュリティ上の脅威にそれらの製品が対抗できていることを確認することが義務付けられている。

要件リストには、これら対象製品において想定されるセキュリティ上の脅威が記載されている。例えば、ファイアウォールであれば、以下の脅威が想定されている。

- 管理機能等への不正アクセスによる不正な通信の発生
- ネットワーク処理の残存情報からの情報漏えい
- リモートで管理する場合の通信データの盗聴、改ざん
- 監査ログの改ざん・不正な削除

製品調達において、各組織の情報システムセキュリティ責任者は、これらの想定される脅威に対するセキュリティ要件を製品が満たしていることを、納品時に検査し確認することが求められる。

要件リストでは、セキュリティ要件の納品時検査の代替として、国際標準に基づく第三者認証製品の活用も認めている。日本における JISEC も、セキュリティ評価基準である ISO/IEC 15408 に基づく第三者認証の制度である。例えば、JISEC において先の四つの脅威に対抗できることが確認されたファイアウォール認証製品を購入することで、セキュリティ要件に関する納品時検査をしたものとみなされる。ただし、認証製品が想定していない個別のセキュリティ要件を調達に課した場合は、認証製品においても情報システムセキュリティ責任者は個別にその要件を確認しなければならない。

JISEC は、要件リストの中でも特に日本のベンダが世界的シェアを持つ製品分野である「デジタル複合機」、国策としてセキュリティが必要な旅券やマイナンバーカードといった「スマートカード」の調達に活用されている。

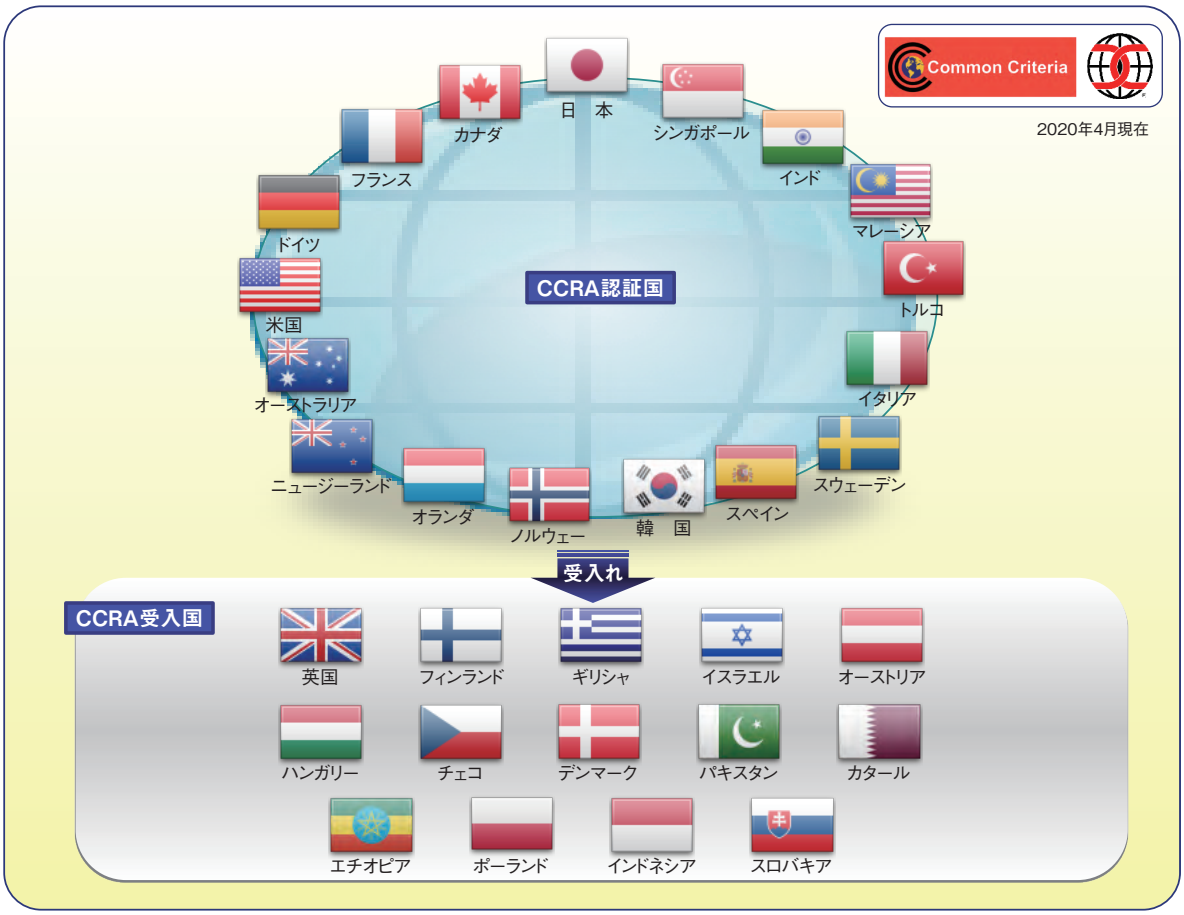
(2) 認証制度の国際連携

セキュリティ評価のための国際標準である ISO/IEC

15408は、欧米6ヵ国によるコモンクライテリア（共通基準）プロジェクトとして開発された。更に同じ評価基準であるコモンクライテリアにより評価された結果を相互に認め合うことで、調達国ごとに重複的な評価を行うコストを低減することを目的とした相互承認が締結された。この相互承認の枠組みはCCRA（Common Criteria Recognition Arrangement）と呼ばれ、その後多くの国が加盟した。日本もコモンクライテリアに基づく認証制度であるJISECの運用を2001年に始め、2003年にCCRAへ加盟している。これにより、日本のベンダが日本語の開発資料をそのまま利用しJISECで認証を取得した製品を、CCRA加盟国の政府調達の対象とすることができるようになった。

CCRAでは、自国で認証制度を運営している「認証国」と、認証制度を有しないが政府調達要件として認証結果を受け入れる「受入国」があり、近年は東南アジアや東ヨーロッパ諸国の受入国としての加盟が増加している。2019年9月にはスロバキアが受入国として加盟した。また、コモンクライテリアプロジェクトの初期メンバーである英国は、自国に認証を必要とする国際的な市場を持つセキュリティ製品ベンダがなく、2019年10月、制度維持のコスト削減を理由に認証国から受入国に移行した。2020年4月現在、CCRA加盟国は認証国17ヵ国、受入国14ヵ国の計31ヵ国に上る（図2-6-1）。

CCRAでは、共通的なセキュリティ評価基準の策定や評価結果の相互承認に加えて、政府調達時の製品分野ごとの共通的なセキュリティ要件の策定も行っている。「2.6.1（1）政府調達のセキュリティ要件」で述べたように、各国政府はIT製品を調達する際に想定されるセキュリティ上の脅威に対抗できることを要件とし、その確認を行ってきた。この調達のためのセキュリティ要件をコモンクライテリアで規定された形式に従って記述したものを「プロテクションプロファイル」と呼び、各国の調達担当者は、IT製品の調達要件として多くのプロテクションプロファイルを策定し公開してきた。同一製品分野に対し国ごとに異なるプロテクションプロファイルへの適合を求めることによる製品ベンダの負荷を軽減するため、CCRAでは、製品分野ごとの共通のプロテクションプロファイルの策定を始めた。現在までに、ファイアウォール、ドライブ全暗号化、ネットワークデバイスについて共通プロテクションプ



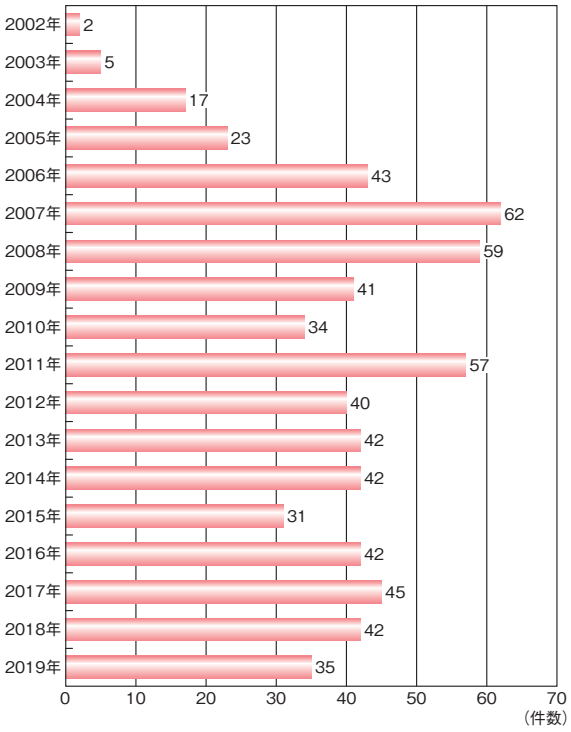
■図2-6-1　CCRA加盟国

ロファイルをCCRAのWebサイト※356-2で公開しており、要件リストにおいてもこれらの共通のプロテクションプロファイルに適合した製品を調達することで、確認すべき要件を満たすことが記載されている。

更に、日本が多くの製品ベンダを有するデジタル複合機についても、日本と韓国が発起人となり、関連するベンダや評価機関をメンバーとする技術コミュニティが発足し、共通のプロテクションプロファイルの策定を行っている。

(3) 認証の状況

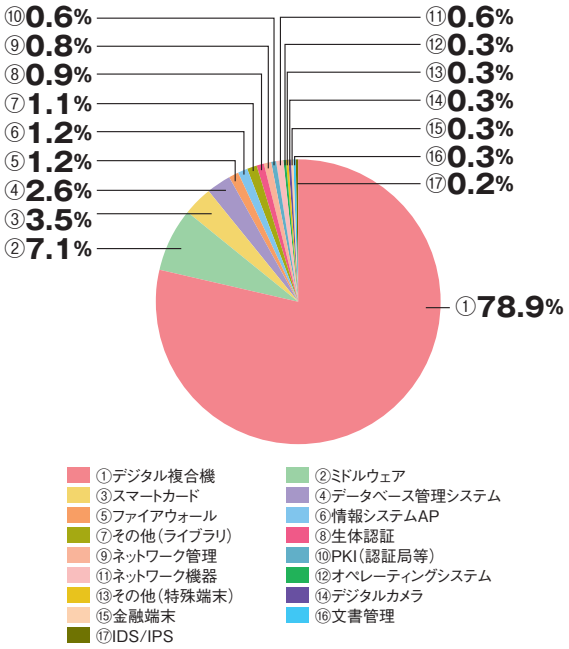
2019年度までのJISECでの認証発行件数の推移を図2-6-2に示す。制度設立当時は、製品のプロモーションを目的とし、政府調達に係ることのない多様な分野の製品の認証を発行していたが、2008年のリーマンショック以後は、申請される製品分野が政府調達の対象に絞られている。



■図2-6-2　JISECの認証発行件数の推移

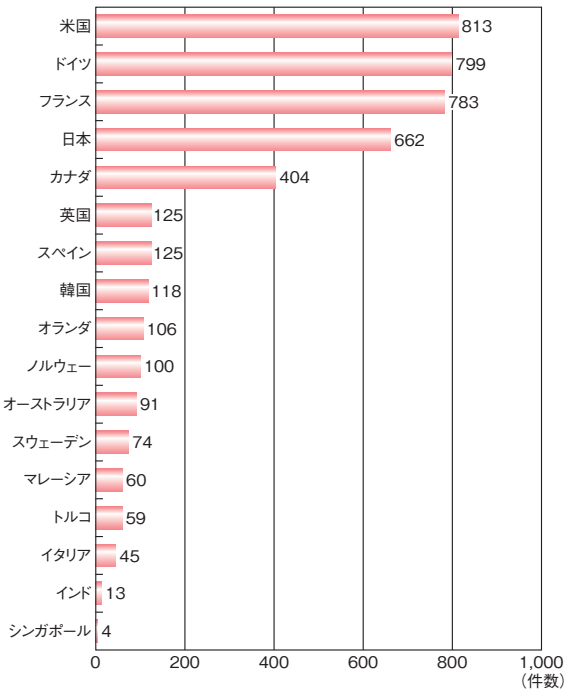
日本における認証発行製品分野の内訳は、図2-6-3に示すように圧倒的にデジタル複合機が多い。これは前述のように、多くの日本のベンダが国際的なシェアを有し、かつ政府調達の対象となる唯一のITセキュリティ製品だからである。デジタル複合機のような国際競争力を持つIT製品が新たに要件リストに追加されない限り、今後もこのような状況は続くと考えられる。

CCRA加盟各国が公開している認証製品の2019年



■図2-6-3　JISECの認証発行の製品分野内訳

度までの累計を図2-6-4に示す。日本は米国、ドイツ、フランスに次いで認証した製品が多い。米国とドイツは政府調達におけるプロテクションプロファイルの活用が活発であり、多くの情報サービス産業分野の製品が認証されている。一方で、フランスは認証製品の85%以上がスマートカード及び集積回路関連である。フランスでは1984年に設立された銀行カード協会が世界に先駆け銀



■図2-6-4　CCRA加盟国の認証数累計

行カードのスマートカード化を推進した結果、金融分野での利用を中心としたプロテクションプロファイルが策定され、高度な保証レベルの評価が数多く実施された。このような実績を背景に、日本のベンダを含め各国のスマートカード関連製品の評価がフランスで行われている。

(4) 2019 年度のトピック

まだ数は少ないが、日本の政府調達においても、調達部門が調達要件として自らプロテクションプロファイルを策定し、調達を実施している。要件リストに掲載されている JISEC で認証を取得したプロテクションプロファイルを表 2-6-1 に示す※357。

申請者	プロテクションプロファイルの名称	認証年月日
IPA	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015※358	2017 年 5 月 29 日
外務省領事局旅券課	旅券冊子用 IC のためのプロテクションプロファイル ― SAC 対応（BAC+PACE） 及び能動認証対応 ― 第 1.00 版※359	2016 年 3 月 22 日
外務省領事局旅券課	旅券冊子用 IC のためのプロテクションプロファイル ― SAC 対応（PACE） 及び能動認証対応 ― 第 1.00 版※360	2016 年 3 月 22 日
地方公共団体情報システム機構	個人番号カードプロテクションプロファイル 第 1.00 版※361	2014 年 5 月 15 日

■表 2-6-1　要件リストに掲載されている JISEC で認証を取得したプロテクションプロファイル

2019 年度には、外務省領事局旅券課が発行した「旅券冊子用 IC のためのプロテクションプロファイル SAC 対応（PACE）及び能動認証対応 - 第 1.00 版」並びに「旅券冊子用 IC のためのプロテクションプロファイル -SAC 対応（BAC+PACE）及び能動認証対応 - 第 1.00 版」にそれぞれ適合する 2 製品の旅券冊子用 IC が認証された※362。これらは、2015 年に国際民間航空機関（ICAO: International Civil Aviation Organization）が発行した、個人の生体情報を認証に利用した IC 旅券に関する規格「ICAO Doc 9309 Part 11」に対応したものである。これらの旅券冊子用 IC を搭載した IC シートが旅券冊子の製造を請け負う独立行政法人国立印刷局に約 92 万枚納入される予定である※363。

政府統一基準では、要件リストとは別に、近年政府においても活用される IoT 製品を含む情報システムについても、その調達や利用におけるセキュリティ対策を求めている。JISEC では、安全な政府調達を推進する立場から 2017 年度にネットワークカメラシステムのセキュリティ要件を調達者が自ら確認できるチェックリストを公開した※364。これに続き 2019 年度は、入退管理システムのチェックリストを策定し公開した※365。本チェックリストでは、入退管理システムの利用形態モデル（スタンドアローン、統合管理、クラウド）ごとに調達時に考慮すべき設定や運用、及びそれらを可能とするセキュリティ機能の要件を記載しており、調達者は本チェックリストを参照することにより、調達する入退管理システムの情報セキュリティ要件を確認できる。本チェックリストは、産業サイバーセキュリティ研究会が発行した「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン 第 1 版※366」で参考文献として参照されている（産業サイバーセキュリティ研究会については「2.1.2（1）産業サイバーセキュリティ研究会」「3.1.4(1)日本政府の取り組み」参照）。

更に、JISEC では、2017 年度に作成したネットワークカメラシステムのチェックリストをセキュリティ要件とし、実際の製品に対するコモンクライテリアを用いた評価の実効性調査を 2019 年度に開始した※367。2020 年度は、この調査結果から、コモンクライテリアでの IoT 機器評価にかかる工数やコストと脆弱性評定効果とのバランスを調達者、ベンダ及び有識者で構成される委員会で検討し、プロテクションプロファイルを策定することで、IoT 製品分野での安全な政府調達を推進していく。

2.6.2 暗号モジュール試験及び認証制度

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

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

JCMVP では、2018 年 6 月から、暗号モジュールが満たすべきセキュリティ要求事項（アクセス制御、物理的

セキュリティ等）を定めた規格として、ISO/IEC 19790：2012 を採用している※368。これと並行して、JCMVP は、既存の承認された暗号モジュール試験機関について、ISO/IEC 19790：2012 に基づく暗号モジュール試験を実施する力量を有しているかを確認するための技能試験を実施し、1 社について力量を有していることを確認した※369。

関連する北米 CMVP の動向として、暗号モジュールのセキュリティ要求事項として NIST が策定中であった FIPS 140-3※370 が 2019 年 3 月 22 日に承認され、2019 年 5 月 1 日に米国連邦政府の官報に公示された※371。FIPS 140-3 は、その技術的内容について ISO/IEC 19790：2012 に準拠することを求めている。更に、FIPS 140-3 に適合するかどうか判断するにあたっての試験方法を定める NIST SP 800-140 シリーズのドラフトが 2019 年 10 月に公開され※372、2019 年 12 月までのパブリックコメントが実施された。

JCMVP は、このパブリックコメントを通じて、暗号モジュール認証を行う上での解釈の画一化等を目的として、ISO/IEC 19790:2012 を採用するにあたって得た知見のフィードバックを行った。NIST SP 800-140 シリーズの最終版は 2020 年 3 月に公開された※373。

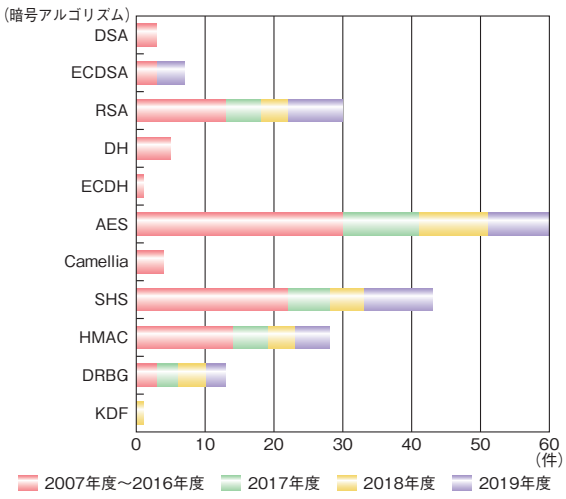
(2) 政府機関等における認証製品の活用

各府省情報化統括責任者（CIO）連絡会議が決定した「デジタル・ガバメント推進標準ガイドライン※374」に関連して、「行政手続におけるオンラインによる本人確認の手法に関するガイドライン※375」が 2019 年 2 月に公開された。本ガイドラインでは、JCMVP によって耐タンパ※376 性※377 が確認されたハードウェアトークンは、当人認証保証レベルとして最高のレベル 3 に位置付けられている。

(3) IT セキュリティ評価及び認証制度との連携

IPA が運営する評価認証制度には、JISEC と JCMVP の二つがある。JISEC が 2016 年に発行、2019 年に改定したガイドライン※378 によって、JCMVP の活用方針が示されている（JISEC の活動については「2.6.1 IT セキュリティ評価及び認証制度」参照）。

2019 年度は、JISEC のもとで、この活用方針に関連する「Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015※379」に基づくデジタル複合機の認証が 8 件完了している※380。このプロテクションプロファイルでは、信頼できるツールを用いた暗号アルゴリズム実装のテストを求めている。このテストに、JCMVP の暗号アルゴリズム実装試験ツール（JCATT：Japan Cryptographic Algorithm implementation Testing Tool）が活用され、認証に貢献している。具体的には、図 2-6-5 に示すように、JCATT を使って確認された暗号アルゴリズム実装の実績が、2017 年度、2018 年度及び 2019 年度において堅調に増加している。また、2019 年度は楕円曲線暗号の一つである ECDSA（Elliptic Curve Digital Signature Algorithm）の実績が増えており、楕円曲線暗号のニーズが反映されていると考えられる。



■図 2-6-5　JCATT により確認された暗号アルゴリズム実装の実績

(4) 承認されたセキュリティ機能の見直し

2019 年度に、JCMVP の下部組織である技術審議委員会において、暗号モジュールのセキュリティ要求事項に組み合わせることのできる暗号の一覧である「承認されたセキュリティ機能」の見直しに関して、以下の二点の審議が実施された。

- GCM-AES-XPN の追加
- 3-key Triple DES の削除

GCM-AES-XPN については 2019 年 7 月に承認されたセキュリティ機能に追加された。3-key Triple DES については、2019 年 12 月末を以て、承認されたセキュリティ機能から削除された※381。

また、2019 年度から次の事項について検討を進めている。

- RSA 1024 の署名検証機能の削除
- TLS version 1.0 及び 1.1 の鍵導出関数の削除
- TLS version 1.3 の鍵導出関数の追加

(a) RSA 1024 の署名検証機能の削除

公開鍵暗号方式の一つで、暗号アルゴリズムが RSA、鍵の長さを 1,024 ビットとしたものを RSA 1024 と呼んでいる。JCMVP では RSA 1024 の署名検証機能に限って承認されたセキュリティ機能に含めている。この RSA 1024 の政府機関等における使用の根拠となっている、「電子署名及び認証業務に関する法律施行規則」及び「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針」の見直しが進められている※382。これを受けて、RSA 1024 の署名検証機能についても、承認されたセキュリティ機能からの削除について、技術審議委員会配下の暗号アルゴリズム実装試験要件検討 WG において検討を行った。同 WG における検討の結果、削除時期は「電子署名法及び認証業務に関する法律施行規則」の改正の後とするという条件付きで、RSA 1024 の署名検証機能を削除する方針を技術審議委員会に答申することが決まった。なお、2020 年 3 月 30 日に「電子署名及び認証業務に関する法律施行規則」が改正されている※383。

(b) TLS version 1.0 及び 1.1 の鍵導出関数の削除

TLS（Transport Layer Security）version 1.0 及び 1.1 の使用を非推奨とするドラフトが IETF で検討されている※384。また、TLS のバージョン別のトラフィックに関するデータも公開されており※385、2020 年 2 月時点では TLS version 1.2 が主に使用されている。主要なブラウザにおいても、TLS version 1.0 及び 1.1 をサポートしない方向に舵を切る動きがある※386。これらに加え、米国※387、ドイツ※388、フランス※389 の動向を踏まえて、承認されたセキュリティ機能から TLS version 1.0 及び 1.1 の鍵導出関数を削除するスケジュールについて、暗号アルゴリズム実装試験要件検討 WG で検討を行った。同 WG において、CRYPTREC の動向を踏まえ、TLS version 1.0 及び 1.1 の鍵導出関数を削除する方針を技術審議委員会に答申することが決まった（2020 年 3 月末時点）。

(c) TLS version 1.3 の鍵導出関数の追加

前述の TLS version 1.0 及び 1.1 の鍵導出関数の削除の議論と並行して、承認されたセキュリティ機能に TLS version 1.3 の鍵導出関数を追加するための検討についても、暗号アルゴリズム実装試験要件検討 WG で開始した。TLS version 1.3 の鍵導出関数は、JCMVP の承認されたセキュリティ機能のうち、NIST SP 800-56C Rev.1※390 で規定された extraction-then-expansion 形式の鍵導出関数の expansion 部分に、NIST SP 800-108※391 で規定された Feedback Mode を用いた鍵導出関数を組み合わせた形を取っている。すなわち、TLS version 1.3 の鍵導出関数は、JCMVP の承認されたセキュリティ機能に含まれている鍵導出関数から構成されているとみなすことができるため、新たな安全性評価を行うことなく承認されたセキュリティ機能への追加を行うことが検討されている。この方向性は、同 WG において了承され、2020 年度から、TLS version 1.3 の鍵導出関数に対する試験仕様の検討を行うこととなった。

2.7 その他の情報セキュリティ動向

情報セキュリティ市場の規模と成長の動向、データ利活用の動向、及び暗号技術の動向、個人情報保護法の改訂について述べる。

2.7.1 情報セキュリティ市場の動向

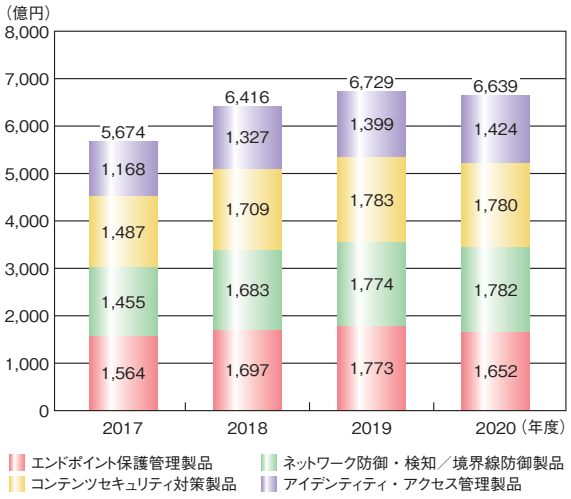
JNSA が発表した「2019 年度 国内情報セキュリティ市場調査報告書[※392]」によると、2019 年度の情報セキュリティ市場規模（ツールとサービスを合わせた数値）は、2018 年度より 5.0% の伸びとなる見込みである。

情報セキュリティのツールとサービスそれぞれの市場規模の推移を図 2-7-1 と図 2-7-2 に示す。図中の 2017 年度、2018 年度については推定実績値で、2019 年度については推定見込値、2020 年度については予測値である。

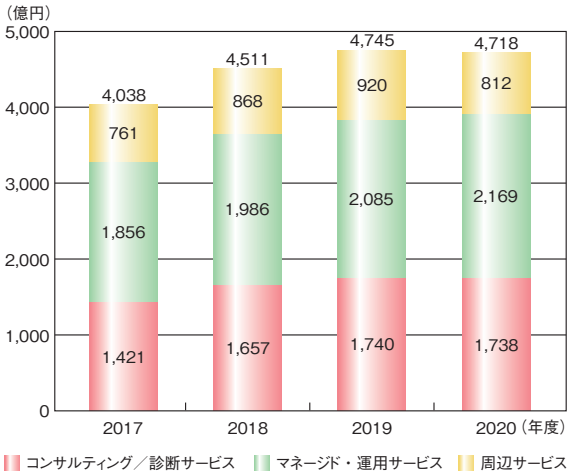
なお、JNSA では「2019 年度 国内情報セキュリティ市場調査報告書」から集計する際の市場区分を変更している[※393]（表 2-7-1、表 2-7-2）。

情報セキュリティツールの市場規模全体では、2018 年度から 2019 年度は 4.9% 伸びている。ツールの区分別に見ても、「エンドポイント保護管理製品」の 2018 年度比 4.5% 増、「ネットワーク防御・検知／境界線防御製品」の 2018 年度比 5.4% 増等、すべての区分で増加傾向が続いている。

情報セキュリティサービスの市場規模全体では、2018 年度から 2019 年度は 5.2% 伸びている。サービスの区分別に見ると、「コンサルティング／診断サービス」の 2018 年度比 5.0% 増、「マネージド・運用サービス」の 2018 年度比 5.0% 増を始め、すべての区分で増加傾向が続いている。



■図 2-7-1　国内情報セキュリティツール市場規模の推移
（出典）JNSA「2019 年度 国内情報セキュリティ市場調査報告書」を基に IPA が編集



■図 2-7-2　国内情報セキュリティサービス市場規模の推移
（出典）JNSA「2019 年度 国内情報セキュリティ市場調査報告書」を基に IPA が編集

分類		説明
旧セキュリティツール	統合型アプライアンス	FW、IDS、ウイルス対策等複数機能を持ったアプライアンス
	ネットワーク脅威対策製品	FW、IDS ／ IPS、VPN、アプリケーションファイアウォール
	コンテンツセキュリティ対策製品	ウイルス対策、スパム対策、URL フィルタ、メールフィルタ、DLP 等
	アイデンティティ・アクセス管理製品	認証、ログオン管理・アクセス許可、PKI 製品
	システムセキュリティ管理製品	セキュリティ情報統合管理、ポリシー・アクティビティ管理ツール、脆弱性検査ツール　等
	暗号製品	暗号化製品、暗号モジュール
新セキュリティツール	エンドポイント保護管理製品	ウイルス対策製品、EDR 製品、ポリシー管理・設定管理・動作監視制御製品
	ネットワーク防御・検知／境界線防御製品	FW、VPN 接続、IDS／IPS、WAF、UTM、セキュリティ情報管理、物理セキュリティ
	コンテンツセキュリティ対策製品	情報漏えい対策 :DLP ／ DRM、暗号化製品、メール・セキュリティ対策、URL フィルタリング、脆弱性検査製品
	アイデンティティ・アクセス管理製品	個人認証用・生体認証デバイス及びその認証システム、アイデンティティ管理、ログオン管理／アクセス許可、PKI

■表 2-7-1　情報セキュリティツールの市場区分（新旧対照）
（出典）JNSA「2019 年度 国内情報セキュリティ市場調査報告書」を基に IPA が編集

分類		説明
旧セキュリティサービス	情報セキュリティコンサルテーション	ポリシー構築、監査・診断等セキュリティ管理全般コンサルティング、規格認証取得支援サービス
	セキュアシステム構築サービス	IT セキュリティの設計、導入、製品選定支援　等
	セキュリティ運用・管理サービス	脆弱性検査、マネージドサービス（IT セキュリティの監視、運用支援）、プロフェッショナルサービス、電子認証サービス　等
	情報セキュリティ教育	教育実施、コンテンツ提供、教育 ASP、資格認定　等
	情報セキュリティ保険	情報セキュリティ及び IT セキュリティ保険
新セキュリティサービス	コンサルティング／診断サービス	コンサルティング、監査・評価、診断、規格認証
	マネージド・運用サービス	SOC、インシデント対応・フォレンジック、インテリジェンス情報提供
	周辺サービス	電子証明書発行・PK 型認証、リテラシー教育、資格取得支援、保険

■表 2-7-2　情報セキュリティサービスの市場区分（新旧対照）
（出典）JNSA「2019 年度 国内情報セキュリティ市場調査報告書」を基に IPA が編集

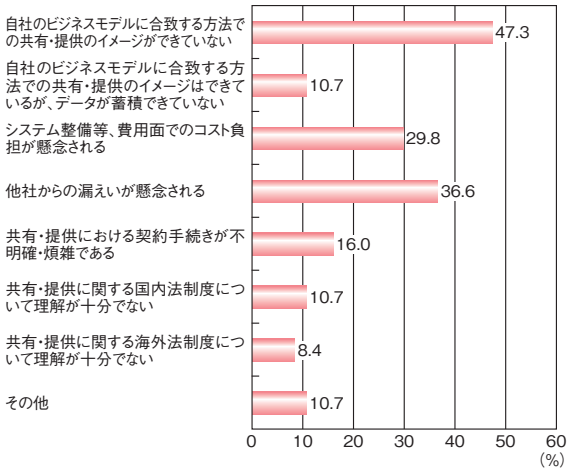
以上のように、情報セキュリティ市場の規模は 2019 年度まで拡大傾向が続いていたが、2020 年度以降については世界的な経済活動の縮小が予測されており※394、先行きが不透明である。

2.7.2 データ利活用の動向

近年、日本が目指す産業の在り方として、産業活動で生成されるデータを利活用することで技術革新や生産性向上等の新たな付加価値の創出や課題解決を目指す「Connected Industries」が提唱されている※395。データ利活用にあたり、AI、IoT 等の技術を背景とした DX を推し進め、新たな付加価値を創出することで競争力を高めていくことが各企業で重要なテーマとなっている。

データの利活用を自社内に限定せず、サプライチェーン上の関係会社や取引先企業にも展開すれば、既存製品・サービスの付加価値向上、新製品・サービスの開発、マーケティング戦略策定、不正防止等の様々な活用の可能性が広がる。ただし、自社の持つデータのみでは十分な活用ができない場合も多く、他社が保有しているデータも含めて効果的に活用していくことは、経営戦略・事業戦略上重要である。

一方で、データの提供を求められる側もデータを使用する側も、課題や懸念を抱える企業は少なくない。各企業は、データを活用したビジネス戦略を模索していることも多く、IPA が 2018 年度に実施した実態調査※396 では、「データ利活用による事業への効果が不透明」「他社からのデータ漏えいが懸念される」といった理由でデータの提供・共有が進んでいない企業が多く存在することが明らかとなった（図 2-7-3）。



■図 2-7-3　データを共有・提供しない理由（複数選択、n=131）
（出典）IPA「安全なデータ利活用に向けた準備状況及び課題認識に関する調査 調査実施報告書※397」を基に作成

こうした社会的状況を踏まえ、データ利活用の更なる推進に向けたビジネス、制度、セキュリティ等の施策を明らかにするため、IPA は、2019 年度に企業におけるデータ利活用・保護の戦略立案に関する調査を行った※398。本調査は、データ利活用に関する先進的な取り組みを行う企業及びデータ利活用に豊富な知見を持つ有識者 24 者に対するインタビュー調査が中心である。以下に、本調査で得られた、企業におけるデータ利活用のポイントを紹介する。

(1) データ利活用のポイント

調査の結果を、データ利活用を推進するために必要な四つの観点（「ビジネス開発」「データの共有における合意」「人材・組織」「リスクマネジメント」）に分類した。個々の観点からポイントを整理する。

(a) ビジネス開発

データを活用したビジネスモデルを構築し、事業の目標を設定する際、着目しておくべきポイントとして以下の 3 点が挙げられる。

- ビジネスの類型と価値創造の明確化

  データを活用して価値を創造するビジネスには、AI によるビッグデータ分析等の技術革新により新しいサービスを志向するものと、以前からあるデータを利用した

サービスの付加価値を向上させるものの二つの類型がある。企図するビジネスモデルの類型と、着地点となる価値創造が何か、をあらかじめ明確にしなければならない。

- 目的の具体化とデータの絞り込み
  必要となるデータはデータ利活用の目的に応じて決まるが、そのためには活用目的を具体化する必要がある。データ利活用の検討当初は何がどこまでできるかが不明瞭な場合もある。その際、小規模な PoC[※399] を繰り返しながら徐々に活用目的を明らかにし、必要となるデータを絞り込むことも重要である。
- データ利活用ビジネスに対する経営層の理解
  ビジネスモデルの構築段階から、PoC 等の試行による活用目的の明確化が必要となる等、既存の事業と異なる新たな取り組みとなることが多く、経営層の理解と判断が必要となる。

まずはこうしたデータ利活用ビジネスの特徴を理解し、適切なビジネス開発を行うことが、有効なデータ利活用の第一歩につながる。

(b) データの共有における合意

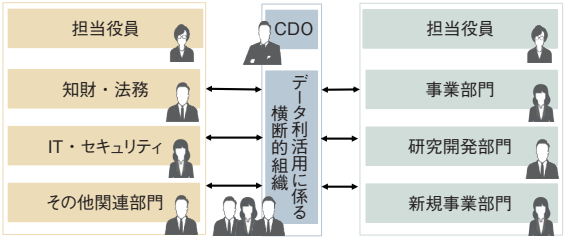
データを共有することで、自社のデータを自社のみで利用する場合と比べ、大きな価値が生まれる可能性が高まる一方で、情報漏えいリスク・法的リスク等のリスクも高まる。データ共有にあたり、こうしたリスクの把握と適切な管理が必要となる。共有するケースに応じて検討すべき事項を確認し、あらかじめ共有先と合意しておくことが重要である。

合意においては、リスクを過大にとらえて一律に広範な利用制限やアクセス制限を課すのではなく、共有相手の目的に応じて適切な利用範囲を設定し、合意することが、データ共有の効果を最大化するポイントである。試行用のデータを提供する場合は品質の保証をしないかわりに利用制限を緩和する、等の合意形成の工夫が一例である。

(c) 人材・組織

データ利活用の実務では、データに関する知識に加えて法的、経営的知見も用いて意思決定を行う必要がある。データ利活用ビジネスを行う組織には、そうした点も加味した組織のマネジメントが求められる。

- CDO 等の設置
  データ利活用に求められる知見を有し、データによるビジネス革新を推進する「データ人材」を最高データ責任者（CDO：Chief Data Officer）として設置する動きが進んでいる。CDO 等の設置により全社的なデータ利活用戦略に関する責任の所在を明確化し、経営層のコミットメントを強化することが求められる。
- 組織横断的な統括機能
  データの処理・管理・分析等のデータ利活用技術に精通したエンジニアを有する組織体制は必須である。一方、技術に限らない多様な機能（事業、IT セキュリティ、知財、法務等）との連携も求められることから、部門横断的にデータ利活用を統括する機能がポイントとなる。具体的には、機能別の組織に対して横串を通すような組織を設置することで、全社的な連携を図る等である（図 2-7-4）。



■図 2-7-4　データ利活用に係る横断的組織の機能例
（出典）IPA「企業におけるデータ利活用・保護の戦略立案のための手引書（案）の作成[※398]」を基に編集

なお、知財・法務部門は以前よりデータを企業が保有する情報資産として管理してきた部門であり、データの戦略的な保護・活用の観点から、更に横断的な機能を持たせることも一案である。

(d) リスクマネジメント

データ利活用のリスクに対する考え方として、全体最適の視点が大切である。洗い出したリスクをすべて回避するばかりでなく、適切にコントロールしてリスクを低減させること、及びデータ利活用を行わないことで逆に発生しうるビジネス上のリスク（事業機会の損失等）を考慮することが求められる。一般的にリスクはゼロにすることはできないため、最終的には意思決定権者による判断でリスク受容を行わなければならない。

(2) データ利活用の課題

データ利活用を行うビジネスを展開していく上での課題について以下に整理する。

- データ利活用ビジネス開発に特有の課題
  － 試行的な PoC の課題

データ利活用ビジネスの開始段階においては、データの価値やビジネス上のリスクをあらかじめ測ることが困難であることから、試行的な PoC の実施が有益である。一方、PoC からサービス化への次の段階へ進むケースは必ずしも多くなく、一般に相当の試行錯誤が必要であること、共同開発契約等で定めるべき事項の把握が困難であること、PoC ごとに異なる個別対応による工数がかさむこと、等の課題が挙げられる。

- 組織的課題
  - データ利活用を推進する組織づくり

    部門横断的な統括組織を設置することの重要性は認識されても、機能ごとにそれぞれ高い専門性を求められるため、一度にすべての機能を備えて組織化することは困難である。
  - 中小・ベンチャー企業や大学等との連携

    中小・ベンチャー企業や大学等と共同開発等の形でビジネスモデルの検討を行う場合、連携を支援する IT 投資や知財、法務面での支援機能が充実していないケースが多い。そうした場合、これらの課題を解決しながらデータ利活用を推進することが困難である。
- データの価値・品質・リスクの測定
  - データの価値の測り方

    自社の複数の部門間、あるいは他社とのデータの共有にあたり、データの価値（対価）を測る共通指標が必ずしも確立されていない。これはビジネスモデル策定の障害となりうる。
  - データの品質の測り方

    データをビジネスに利用するには満足できる「データの品質」を規定しておくことが必要となるが、その定義がデータ利活用を行う当事者間で必ずしも定まっていない。データの品質に関する基準を明らかにするためには、当事者間で PoC 段階やサービスのリリース段階において都度契約で定める、あるいは事前調整により品質指標を策定する、等の複合的な施策が必要と想定される。
  - リスクの測り方

    データ利活用に伴うビジネス上のリスクを総合的に測ることが困難である。特に、データの不適切な使用や情報漏えい等に起因するレピュテーションリスクに関しては、予測することが極めて困難となる。これらを明確に把握できないことが、経営層がデータ利活用ビジネスにおけるリスクテイクを行えない要因の一つとなっている。

(3) データ利活用ビジネスと情報セキュリティの課題

データ利活用を行うビジネスに関するセキュリティ視点からの課題をまとめる。

前述のとおり、ビジネスモデルの開発が重要であり、ビジネスモデルを確立し、必要な精度で目的を実現するための試行が必須である。このとき、セキュリティやプライバシーに十分に配慮しながら、試行が容易に行えるような利用範囲・データ保護ルールを作ることが重要である。例えば、一部個人情報を含むデータによる試行においてはセキュリティ・プライバシー保護対策を厳しくルール化する一方、個人を特定できる情報を含まないテスト用データを別途作成して自由な流通や複製を許容し、より簡易に試行を行えるようにする、等の方策が考えられる。

同時に、データの漏えい、あるいは不正な転用によるビジネスリスク評価はセキュリティ観点からも大きな課題であり、漏えい防止・不正転用に関するルールの整備とともに、万一そのような事態が起きた場合のリスク評価や計測の手法が求められる。海外においては、データの価値・品質・リスクの測り方等に関し、定量的に分析する方法が報告されている※400 が、前述のレピュテーションリスクの評価・計測の検討は進んでおらず、対応は容易ではないと考えられる。一方で、インシデントに関するレピュテーションリスクは、情報開示を適切に行う、等のリスクマネジメント体制の整備により小さく抑えられる可能性がある。このように、データ利活用ビジネスの経営判断には、組織のリスクマネジメント体制を含めたリスク評価手法の充実が重要である。

2.7.3 暗号技術の動向

本項では 2019 年度における、共通鍵暗号、公開鍵暗号、軽量暗号及び実装攻撃に関する研究及び標準化の動向についてそれぞれ解説する。

(1) 共通鍵暗号に関する研究動向

共通鍵暗号に対する攻撃に関する研究として、2019 年度の大きなトピックは、「CRYPTREC 暗号リスト」の「運用監視暗号リスト」に掲載されているハッシュ関数 SHA-1 に対する攻撃が更に進展し、chosen-prefix collision attack と呼ばれる攻撃に成功したことを述べた論文※401 が Eurocrypt2019 で発表されたことである。本攻撃手

法は後述する collision attack より強力で、実環境における証明書やアプリケーション等の偽造につながり、ひいては TLS 等のインターネットプロトコルの安全性を揺るがす可能性がある。実際、過去にはハッシュ関数 MD5 に対する chosen-prefix collision attack が発表された翌年（2008 年）の年末に TLS で利用される中間 CA 証明書の偽造攻撃に成功したことが公表[※402]され、MD5 を使った証明書が一掃される契機ともなった。

(a) chosen-prefix collision attack とは

ハッシュ関数の攻撃には三つの段階がある。

第一段階は free-start collision attack と呼ばれるもので、本来は固定値である初期ベクトルの値を攻撃者が自由に設定した上で衝突するメッセージ組を見つける攻撃手法である。メッセージだけでなく、初期ベクトルも攻撃者が調整できるので衝突を見つけやすい。

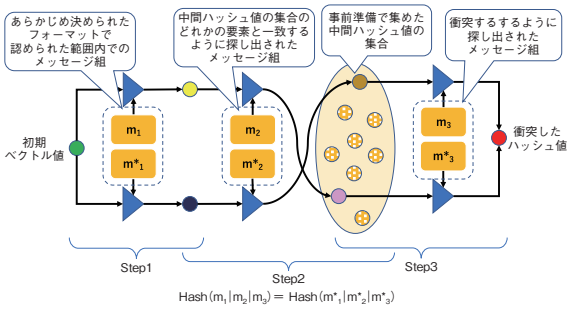
次の段階が collision attack と呼ばれるもので、メッセージだけを調整して衝突するメッセージ組を見つける攻撃手法である。一般に「ハッシュ関数の衝突」という場合はこの段階のことを言う。しかし、この攻撃手法では攻撃者がメッセージを制約なく調整できることが前提であるため、実環境の中では取りえない値のメッセージになる可能性もある。そういった場合には、アプリケーション側でのエラーチェック等で不正を検知できる可能性がある。

最後の段階が chosen-prefix collision attack である。これは、攻撃者が調整できるメッセージにある種の制約を加えた上で衝突するメッセージ組を見つける攻撃手法である。例えば、証明書の発行番号や発行者情報、有効期間等の部分はフォーマットがあらかじめ決まっていることから、そのフォーマットで認められる範囲内に収まるようにメッセージを調整した上で衝突するメッセージ組を見つける。こうすることによって、アプリケーション側でのエラーチェック等もすり抜けることが可能になる。

(b) 攻撃手法の概要

本攻撃手法は、MD5 や SHA-1、SHA-2 のような Merkle-Damgård 型のハッシュ関数を攻撃対象としている。攻撃は以下の事前準備と 3 ステップで行われる。Step1 から Step3 までで求めたメッセージ組（のブロック）を連結したものが衝突するメッセージ組となる（図 2-7-5）。

- ［事前準備］　Step3 で衝突するようなメッセージ組を作り出せる可能性が高い中間ハッシュ値の集合を集めておく。
- ［Step1］　あらかじめ決められたフォーマットで認められる範囲内に収まるような同じ長さのメッセージ組（のブロック）を作る。この部分が chosen-prefix に相当し、攻撃者にとっての制約条件となる。
- ［Step2］　Step1 で求めたメッセージ組に対して計算したハッシュ値それぞれを初期ベクトルとみなして、それぞれが事前準備で用意した集合中のどれかの要素と同じ中間ハッシュ値になるようなメッセージ組（のブロック）を探す。
- ［Step3］　Step2 で求めたメッセージ組に対して計算した中間ハッシュ値（事前準備で用意した集合のなかのある要素）から衝突するようなメッセージ組（のブロック）を探す。



■図 2-7-5　Eurocrypt2019 で発表された攻撃手法のイメージ

(c) 攻撃論文のインパクト

SHA-1 に対する chosen-prefix collision attack が可能であることが示されたものの、MD5 に対する場合と比較すると約 100 万～ 1 億倍以上の計算量が必要と見積もられている。このため、MD5 のときのような中間 CA 証明書の偽造攻撃が成功する、等の事態が直ちに発生する可能性は低いと考えられる。しかしながら、chosen-prefix collision attack が可能と示されたこと自体がハッシュ関数の安全性にとって従来とは違うステージに入ったことを意味しており、SHA-1 の寿命が尽きるところにまた一歩近づいたことになる。

(2) 公開鍵暗号に関する研究及び標準化の動向

NIST による「量子コンピュータに耐性を持つ暗号（耐量子計算機暗号、PQC：Post-Quantum Cryptography）」の標準化は、2019 年 1 月 30 日に候補暗号を 64 件から 26 件に絞って第 2 ラウンドに入り、PQC を対象とする公開鍵暗号の研究はますます盛んになっている。直前に行われた暗号国際会議 CRYPTO と併催される形で、2019 年 8 月 24 ～ 26 日に米国カリフォルニア州サンタバーバラにて第 2 回 NIST PQC 標準化会議が開催された。同会議では各候補暗号の前回からの変更点の紹介、

及び安全性・処理性能・消費電力等、様々な観点からの評価結果が発表された。第1ラウンドから第2ラウンドへの応募暗号数の変化の内訳を表2-7-3に示す。

	署名	鍵確立／暗号化	合計
格子ベース	5→3	21→9	26→12
符号ベース	2→0	17→7	19→7
多変数	7→4	2→0	9→4
対称／ハッシュベース	3→2	0→0	3→2
その他	2→0	5→1	7→1
合計	19→9	45→17	64→26

■表2-7-3　NIST PQCコンペティション応募暗号数（第1ラウンド→第2ラウンド）
（出典）Dustin Moody（NIST）「The 2nd Round of the NIST PQC Standardization Process※403」を基にIPAが編集

会議冒頭にNISTのDustin Moody氏から開会挨拶があり、①候補暗号間の統合（マージ）はまだ許容されること、②第2ラウンドは12ヵ月～18ヵ月かかり、その後第3ラウンドに入ると予想していること、③ドラフト標準は2022年ごろを期待していること、④第2ラウンドは処理性能が大きな役割を果たすであろうこと等が述べられた。

今後は2020年7月ごろに候補を絞り込んだ後、第3ラウンドに入ることが予想される。2022～2024年ごろのドラフト標準作成やその後の標準化を通じて、2030年ごろを目指して移行を進めていく予定である。

(3) 軽量暗号に関する研究及び標準化の動向

NISTは、IoTやセンサーネットワーク、ヘルスケア等の制約のある環境で用いる暗号の標準化のため、2015年に「軽量暗号」のプロジェクトを開始した。候補暗号は公募され、2019年4月に応募された57件のうち56件を第1ラウンドの候補として発表、2019年8月に第2ラウンドとして更に32件に絞った※404。この32件中、日本人研究者が関与する候補暗号は11件である。

今後は、2020年9月ごろに第3ラウンドとして更に候補数を絞り、2021年に最終的に選抜したアルゴリズムを発表する予定である。

(4) 実装攻撃に関する研究の動向

暗号実装に対する攻撃には、消費電力や処理時間等のサイドチャネル情報から暗号鍵等の秘密情報の復元を試みるサイドチャネル攻撃や、ICチップに一時的な誤動作を起こさせることによって暗号鍵等の秘密情報の暴露を試みる故障利用攻撃等が存在する。

サイドチャネル攻撃に関しては、暗号のソフトウェア実装のキャッシュタイミングを利用したサイドチャネル攻撃（タイミング攻撃）に対して脆弱なソースコードを分析する手法を提案し、具体例としてOpenSSLに対する新たな脆弱性を指摘する論文が発表された※405。これはRSA鍵生成時に、キャッシュのヒット／ヒットミスの状況による実行時間の差を利用したサイドチャネル攻撃によって、生成された鍵が復元される可能性を示すものである。この脆弱性は、CVE-2018-0737として報告されている。

DSA（Digital Signature Algorithm）及びECDSAの署名生成処理において、剰余演算時の処理時間の差を利用したタイミング攻撃を提案する論文も発表された※406。その中でDSAやECDSAを実装している既存のオープンソースソフトウェアの約半数にこの脆弱性が存在していることも示された。この脆弱性が実際に悪用可能かどうかについては研究の進展を待つ必要があるが、暗号の実装にあたっては処理時間がパラメータによらず一定時間になることを、計算過程のあらゆる場面で注意深く確認してソースコードを記述する必要があるといえる。

故障利用攻撃に関しては、ICの側面からレーザ光を照射する攻撃に関する論文が発表された※407。レーザ攻撃は、ICの背面から照射する方法が最も効果的で多く使用されるが、最近のICのパッケージ技術ではICが3次元的に複雑な構造を持つことが多くなり、背面からの攻撃が困難であるケースが増えている。そのようなICに対しても、側面からのレーザ照射が効果的であることが示された。側面からの照射は、攻撃対象の回路への距離が背面からの照射に比較して遠いため、背面からの照射より効果は劣るが、現実的な脅威になり得る程の成功率が得られることが示されたことから、この攻撃の研究の進展に注意が必要と考えられる。

2.7.4 個人情報保護法の改正

2019年12月、個人情報保護委員会は、2020年の個人情報保護法の改正に向けて、「個人情報保護法いわゆる3年ごと見直し 制度改正大綱※408（以下、大綱）」を公表した。

大綱では、利用停止等の権利の拡充、開示のデジタル化推進、6ヵ月以内に消去するデータも保有個人データに包含すること、漏えい等報告の義務化、個人データの提供先基準の明確化等の新たな規定が盛り込まれているほか、ペナルティについては重科（重い罰則）の導入

を含め、必要に応じて見直すとしている。また、データ利活用を推進するために、「仮名化情報（仮称）」を導入するとしている。

(1) 大綱の概要

公表された大綱の骨子を表 2-7-4 に示す。

	合計
I. 個人データに関する個人の権利の在り方	利用の停止、消去、第三者提供の停止の請求に係る要件の緩和
	開示のデジタル化の推進
	開示等の対象となる保有個人データの範囲の拡大
	オプトアウト規制の強化
II. 事業者の守るべき責務の在り方	漏えい等報告及び本人通知の義務化
	適正な利用義務の明確化
III. 事業者における自主的な取組を促す仕組みの在り方	認定個人情報保護団体制度の多様化
	保有個人データに関する公表事項の充実
IV. データ利活用に関する施策の在り方	「仮名化情報」の創設
	提供先において個人データとなる場合の規律の明確化
	公益目的による個人情報の取扱いに係る例外規定の運用の明確化
	個人情報の保護と有用性に配慮した利活用相談の充実
V. ペナルティの在り方	法人処罰規定に係る重科の導入など
VI. 法の域外適用の在り方及び越境移転の在り方	域外適用の範囲の拡大
	外国にある第三者への個人データの提供制限の強化
VII. 官民を通じた個人情報の取扱い	行政機関、独立行政法人等に係る法制と民間部門に係る法制との一元化
	地方公共団体の個人情報保護制度

■表 2-7-4　大綱の改訂項目
（出典）個人情報保護委員会「個人情報保護法 いわゆる 3 年ごと見直し制度改正大綱（骨子）[※409]」を基に IPA が作成

以下では、特徴的な改訂項目について述べる。

(a) 開示のデジタル化推進（骨子 I）

自己データの開示について、電磁的形式による提供を求められるようになる。これにより業者をまたいだデータの移動、すなわちポータビリティが実現可能になるものと思われる。また、現行法では 6 ヵ月以内しか保有しない短期データは開示請求の対象外であるが、これも開示対象に含まれることとなる。

(b) オプトアウト規制の強化（骨子 I）

本人が積極的に反対しない限り個人情報の利用に同意したものとみなすオプトアウトへの規制が更に強化される。具体的には、オプトアウト規定に基づき本人同意なく第三者提供できる個人データの範囲がより限定されるほか、届出事項にも追加が行われる。一方で、現行の Web サービス等においてオプトアウトの手続きが必ずしも簡易でない、という課題は残っている。

(c) 漏えい等報告の義務化（骨子 II）

個人データ漏えいが発生した場合、現行法規において、当局への通知は努力義務とされているのが改められ、件数が多い場合や要配慮個人情報の漏えい等、一定の条件を満たす場合については報告が義務化される（罰則がある）。また報告先は、個人情報保護委員会または権限委任官庁に一本化される。一方で、報告時期の限定や個人への通知等については例外規定等を設けることで、事業者にも配慮している。

(d)「仮名化情報（仮称）」の創設（骨子 IV）

現行法では、個人情報を第三者に提供する際に「個人を特定できてはならない」という厳しい要件を付加し、この要件を満たすべく匿名加工処理を義務付けている。しかし同一事業者内での利用であれば、ここまで厳しい措置をしなくてもプライバシー等への影響は小さいと考えられる。仮名化情報はこれを考慮し、同一事業者内利用における利便性を高めるため、それ単体では個人は特定できないものの「他の情報と組み合わせれば個人が特定できる」ものについて、個人の開示等請求への対応義務を緩和し、様々な分析への活用を認めるものである。一方、仮名化情報は、匿名加工情報とは異なり、それ自体が個人情報であるため、第三者への提供にあたっては原則として本人同意が必要となる。仮名化情報の導入は、EU 等での仮名化情報の利用と整合をとることも目的と考えられる。

(e) 個人データの提供先基準の明確化（骨子 IV）

現行法制では、提供における個人情報の定義を「提供元で個人が特定されうる情報」としているため、提供した情報と提供先が保有する情報とを組み合わせて個人を特定してしまうことに対応できない。特に、提供先で他の情報と照合すれば個人と紐づけされることを認識しながら、クッキー（cookie）等の識別子を含んだ情報を提供する事業形態が問題となってきている。大綱では、提供

先が上記の手段で個人を特定できることが明らかな場合、個人を特定した利用はできないことが明確化される。ただし、「明らかな」をどのように定義するかは不透明であり、個々のケースで慎重な判断が必要と考えられる。

(f) 域外適用の範囲の拡大(骨子Ⅵ)

現行法では報告徴収や立ち入り検査等の強制力のある規定は外国の事業者に適用されず、事業者に違反行為があった場合の法執行が問題となっていた。これについては、外国にある事業者への矯正法執行を認めるべきか、外国の主権を尊重して法執行すべきでないか、意見が分かれていた。大綱では、法執行できる立場に立つことを明確にし、外国事業者も報告徴収や立ち入り検査の対象とする。ただし当該国の主権も尊重し、必要に応じてその国と執行について協力する、としている。

(2) 意見聴取と改正法案の提出

大綱について、2020 年 1 月 14 日まで意見募集が行われた。個人情報保護委員会は寄せられた意見を踏まえて「個人情報の保護に関する法律等の一部を改正する法律案」を策定、同法案は 2020 年 3 月 10 日に閣議決定され※410、第 201 回通常国会に提出された。

COLUMN

情報セキュリティ活動と法整備のジレンマ

仮想通貨のマイニングをする「Coinhive（コインハイブ）」を Web サイトに設置したことで、不正指令電磁的記録保管罪でサイト運営者が検挙された「Coinhive 事件」。2019 年 1 月から開かれた Coinhive 事件の裁判では、開廷前から傍聴希望者の列ができる等、世間の興味、関心の高さがうかがえました。約 1 年後となる 2020 年 2 月には、控訴審判決で 1 審の無罪判決が破棄され、逆転有罪となったことで再び注目を集めました[i]。

2017 年 10 月には、情報セキュリティ企業の社員が不正指令電磁的記録保管容疑で逮捕された事案（2018 年に地方検察庁によって不起訴が決定）[ii]、2019 年 3 月には、ポップアップが繰り返し表示されるサイトの URL を掲示板に書き込んだとして、不正指令電磁的記録供用未遂の疑いで摘発された「アラートループ事件[iii]」等がありました。

このような、近年の不正指令電磁的記録保管罪や不正指令電磁的記録供用罪での検挙に対して、情報セキュリティに関連する活動の萎縮を懸念する声が度々挙がっていました。実際、「アラートループ事件」の直後には、参加者が逮捕される可能性があるとして Web セキュリティの勉強会を自粛するといった萎縮の動きがありました[iv]。冒頭の Coinhive 事件でも、逆転有罪の判決を受け、弁護人は活動萎縮への懸念を強めているようです[v]。

情報セキュリティやソフトウェア開発の現場から懸念の声が挙がる要因として、新しい技術の進歩のスピードと、その技術を利用する際のルールを定める法整備を含めた世の中の動きに差があることが考えられます。

これまでの技術の進歩は、例えば、活版印刷や自動車等を見ても、世に初めて登場してから長い時間をかけ少しずつ進歩していったことで、紆余曲折がありながらも、世の中の動きもその変化に対応できていたものと思われます。しかし、インターネットやスマートフォン等は、その登場から進歩のスピードが著しく早く、結果的に変化に追いついていけるものと、いけないものとの二極化が発生する状況となっているようです。

急速な技術の進歩により、昨日はできなかったことが今日はできるといった便利な世の中が実現することは喜ばしいですが、それらは皆が安心・安全に利用できるという前提があってこそとなります。情報セキュリティやソフトウェア開発においても、その活動の安心・安全を担保できるよう、迅速な法整備やガイドライン等の整備が望まれます。

i　日経クロステック：Coinhive 設置で 1 審無罪の控訴審、東京高裁がサイト運営者に逆転有罪　https://xtech.nikkei.com/atcl/nxt/news/18/07046/?i_cid=nbpnxt_reco_atype〔2020/7/10 確認〕
ITmedia NEWS：「ウイルス罪」めぐる事件、セキュリティ事業者に余波　「活動の萎縮につながる」「指針が必要」　https://www.itmedia.co.jp/news/articles/1906/28/news088.html〔2020/7/10 確認〕
ii　株式会社ディアイティ：当社社員の不正指令電磁的記録（ウイルス）保管容疑で逮捕された件について　https://www.dit.co.jp/news/archive/2017/1101.html〔2020/3/16 確認〕
iii　ITmedia NEWS：「何回閉じても無駄ですよ〜」ブラクラ URL を掲示板に貼っただけで補導、「やり過ぎ」と物議　https://www.itmedia.co.jp/news/articles/1903/05/news080.html〔2020/7/10 確認〕
iv　ITmedia NEWS：セキュリティ勉強会休止、「攻撃コードの研究発表でも逮捕されかねない」と懸念　いたずら URL 事件受け　https://www.itmedia.co.jp/news/articles/1903/20/news079.html〔2020/7/10 確認〕
v　ITmedia NEWS：Coinhive 裁判、弁護側が IT 業界から意見書募集　Web 上の声をくみあげ、最高裁に提出　https://www.itmedia.co.jp/news/articles/2002/18/news108.html〔2020/7/10 確認〕

※1　政府機関等の情報セキュリティ対策のための統一基準群：国の行政機関及び独立行政法人等の情報セキュリティ水準を向上させるための統一的な枠組みを指す。国の行政機関及び独立行政法人等の情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項を規定している。
NISC：「政府機関等の情報セキュリティ対策のための統一基準群（平成30年度版）」について　https://www.nisc.go.jp/active/general/kijun30.html〔2020/6/30 確認〕
※2　NISC：サイバーセキュリティ2019　https://www.nisc.go.jp/active/kihon/pdf/cs2019.pdf〔2020/6/30 確認〕
※3　経済産業省：CGS（第2期）取りまとめ　https://www.meti.go.jp/shingikai/economy/cgs_kenkyukai/20190628_report.html〔2020/6/30 確認〕
※4　経済産業省：「グループ・ガバナンス・システムに関する実務指針」を策定しました　https://www.meti.go.jp/press/2019/06/20190628003/20190628003.html〔2020/6/30 確認〕
※5　NISC：サイバーセキュリティ戦略・サイバーセキュリティ2019の概要　https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-cs2019-gaiyou.pdf〔2020/6/30 確認〕
※6　サイバーセキュリティタスクフォース：総務省が2017年1月に設置した、IoT/AI時代を見据えたサイバーセキュリティに係る課題を整理するとともに、情報通信分野において講ずべき対策や既存の取り組みの改善等幅広い観点から検討を行い、必要な方策を推進することを目的とした組織。
※7　総務省：サイバーセキュリティ対策情報開示の手引き　https://www.soumu.go.jp/main_content/000630516.pdf〔2020/6/30 確認〕
※8　IPA：コラボレーション・プラットフォームについて　https://www.ipa.go.jp/security/announce/collapla_index.html〔2020/6/30 確認〕
※9　経済産業省：サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を策定しました　https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html〔2020/7/29 確認〕
※10　経済産業省：クラウドサービスの安全性評価に関する検討会　とりまとめ　https://www.meti.go.jp/shingikai/mono_info_service/cloud_services/pdf/20200130_report.pdf〔2020/6/30 確認〕
※11　NISC：2020年東京オリンピック・パラリンピック競技大会に向けての取組状況　https://www.nisc.go.jp/conference/cs/dai23/pdf/23shiryou06.pdf〔2020/6/30 確認〕
※12　NISC：サイバーセキュリティ対処調整センターについて　https://www.nisc.go.jp/conference/cs/ciip/dai18/pdf/18shiryou11.pdf〔2020/6/30 確認〕
東京都：東京2020大会の安全・安心の確保のための対処要領（第二版）　http://www.metro.tokyo.jp/tosei/hodohappyo/press/2019/04/16/documents/13_02.pdf〔2020/6/30 確認〕
※13　ASEAN加盟国（ブルネイ、カンボジア、インドネシア、ラオス、ミャンマー、フィリピン、シンガポール、タイ、ベトナム）、インド、バングラディッシュ、スリランカ、ニュージーランド、台湾。
※14　IPA：中核人材育成プログラム　https://www.ipa.go.jp/icscoe/program/core_human_resource/index.html〔2020/6/30 確認〕
※15　経済産業省：「インド太平洋地域向け日米サイバー演習」を実施しました　https://www.meti.go.jp/press/2019/09/20190912009/20190912009.html〔2020/6/30 確認〕
※16　NISC：サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ 報告書 ～「戦略マネジメント層」の育成・定着に向けて～　https://www.nisc.go.jp/conference/cs/pdf/jinzai-sesaku2018set.pdf〔2020/6/30 確認〕
※17　総務省：IoT機器調査及び利用者への注意喚起の取組「NOTICE」の実施　https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00011.html〔2020/6/30 確認〕
※18　NICT：NICTER観測レポート2019　https://www.nict.go.jp/cyber/report.html〔2020/6/30 確認〕
※19　NISC：重要インフラの情報セキュリティ対策に係る第4次行動計画　https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf〔2020/6/30 確認〕
※20　NISC：重要インフラの情報セキュリティ対策に係る第4次行動計画（改定）　https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r1.pdf〔2020/6/30 確認〕
※21　NISC：重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）　https://www.nisc.go.jp/active/infra/pdf/shishin5.pdf〔2020/6/30 確認〕
※22　NISC：活動内容　https://www.nisc.go.jp/active/infra/shisaku1.html〔2020/6/30 確認〕
※23　政府内において第4次行動計画に基づく情報共有の実施に必要な事項を定めた「重要インフラ所管省庁との情報共有に関する実施細目」。
※24　https://www.nisc.go.jp/conference/cs/ciip/dai20/pdf/20shiryou07-2.pdf〔2020/6/30 確認〕
※25　NISC：重要インフラ専門調査会第21回会合（令和2年1月29日）　資料3　分野横断的演習（2019年度）の実施結果について　https://www.nisc.go.jp/conference/cs/ciip/dai21/pdf/21shiryou03.pdf〔2020/6/30 確認〕
※26　経済産業省：「産業サイバーセキュリティ研究会」を開催します　https://www.meti.go.jp/press/2017/12/20171226004/20171226004.html〔2020/6/30 確認〕
※27　経済産業省：産業分野におけるサイバーセキュリティ政策　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/001_05_00.pdf〔2020/6/30 確認〕
※28　経済産業省：産業サイバーセキュリティ強化へ向けたアクションプラン　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/002_03_00.pdf〔2020/6/30 確認〕
※29　経済産業省：産業サイバーセキュリティの加速化指針 ~ アクションプランの深化・拡大 ~　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/003_04_00.pdf〔2020/6/30 確認〕
※30　対策要件のカテゴリはNISTの「Cybersecurity Framework Version 1.1」に対応する形で整理している。
※31　転写：CPSFにおいては、温度や距離等の物理事象をデータに変換するといった、サイバー空間とフィジカル空間の境界において行われる情報の変換を意味する。
※32　経済産業省：『第2層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/dainiso/pdf/002_03_00.pdf〔2020/6/30 確認〕
※33　経済産業省：『第3層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/daisanso/pdf/002_03_00.pdf〔2020/6/30 確認〕
※34-1　経済産業省：サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/003_03_00.pdf〔2020/6/30 確認〕
※34-2　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/pdf/20190617_01.pdf〔2020/7/27 確認〕
※35　経済産業省：サイバーセキュリティ経営ガイドライン　https://www.meti.go.jp/policy/netsecurity/mng_guide.html〔2020/6/30 確認〕
※36　IPA：サイバーセキュリティ経営ガイドライン実践状況の可視化ツールβ版　https://www.ipa.go.jp/security/economics/checktool/index.html〔2020/6/30 確認〕
※37　IPA：中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊）　https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html〔2020/6/30 確認〕
※38　「サイバーセキュリティ戦略」（https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf〔2020/6/30 確認〕）では、「経営戦略、事業戦略におけるサイバーセキュリティに係るリスクを認識し、経営層の方針を踏まえた対策を立案し、実務者・技術者を指導できる人材」と定義している。
※39　経済産業省：事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/005_03_00.pdf〔2020/6/30 確認〕
※40　経済産業省：事務局説明資料（産業サイバーセキュリティ研究会WG3（サイバーセキュリティビジネス化）第3回）　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/pdf/003_03_00.pdf〔2020/6/30 確認〕
※41　IPA：サイバーセキュリティ検証基盤構築に向けた有識者会議　https://www.ipa.go.jp/security/economics/kensyokiban2019.html〔2020/6/30 確認〕
※42　IPA：セキュリティ製品の有効性検証の試行について　https://www.ipa.go.jp/security/economics/shikoukekka2019.html〔2020/6/30 確認〕
※43　https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf〔2020/6/30 確認〕
※44　経済産業省：クラウドサービスの安全性評価に関する検討会について　https://www.meti.go.jp/shingikai/mono_info_service/cloud_services/pdf/001_02_00.pdf〔2020/6/30 確認〕
※45　https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2018_zentai.pdf〔2020/6/30 確認〕
※46　https://www.meti.go.jp/press/2019/01/20200130002/20200130002-1.pdf〔2020/6/30 確認〕
※47　サイバーセキュリティ戦略本部：「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」　https://www.nisc.go.jp/active/general/pdf/wakugumi2020.pdf〔2020/6/30 確認〕
※48　https://www.ipa.go.jp/files/000082669.pdf〔2020/6/30

確認〕
※ 49 経済産業省：政府情報システムのためのセキュリティ評価制度（ISMAP）における各種基準（案）の意見公募手続（パブリックコメント）を開始しました https://www.meti.go.jp/press/2019/03/20200327017/20200327017.html
※ 50 https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf〔2020/6/30 確認〕
※ 51 https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex04.pdf〔2020/6/30 確認〕
※ 52 https://www.ipa.go.jp/files/000082279.pdf〔2020/6/30 確認〕
※ 53 https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20191220/siryou.pdf〔2020/6/30 確認〕
※ 54 経済産業省：「政府情報システムのためのセキュリティ評価制度（ISMAP）」の運用を開始しました https://www.meti.go.jp/press/2020/06/20200603001/20200603001.html
※ 55 IPA：政府情報システムのためのセキュリティ評価制度（ISMAP） https://www.ipa.go.jp/security/ismap/index.html〔2020/6/30 確認〕
※ 56 https://www.nisc.go.jp/active/infra/pdf/shishin5rev.pdf〔2020/6/30 確認〕
※ 57 経済産業省：データの利用権限に関する契約ガイドライン ver1.0 https://www.meti.go.jp/press/2017/05/20170530003/20170530003-1.pdf〔2020/6/30 確認〕
※ 58 経済産業省：「AI・データの利用に関する契約ガイドライン」を策定しました https://www.meti.go.jp/press/2018/06/20180615001/20180615001.html〔2020/6/30 確認〕
※ 59 経済産業省：「不正競争防止法等の一部を改正する法律案」が閣議決定されました https://www.meti.go.jp/press/2017/02/20180227001/20180227001.html〔2020/6/30 確認〕
※ 60 経済産業省：限定提供データに関する指針 https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31pd.pdf〔2020/6/30 確認〕
※ 61 経済産業省：「AI・データの利用に関する契約ガイドライン 1.1 版」を策定しました https://www.meti.go.jp/press/2019/12/20191209001/20191209001.html〔2020/6/30 確認〕
※ 62 衆議院：議案名「産業競争力強化法等の一部を改正する法律案」の審議経過情報 http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/keika/1DC7D8E.htm〔2020/6/30 確認〕
経済産業省：「産業競争力強化法」の一部改正が施行されました https://www.meti.go.jp/press/2018/07/20180709006/20180709006.html〔2020/6/30 確認〕
※ 63 経済産業省：重要技術マネジメント https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html〔2020/6/30 確認〕
※ 64 経済産業省：情報セキュリティサービス基準及び情報セキュリティサービスに関する審査登録機関基準を策定しました https://www.meti.go.jp/press/2017/02/20180228002/20180228002.html〔2020/6/30 確認〕
※ 65 審査登録機関：「情報セキュリティサービスに関する審査登録機関基準」に適合するとIPAが確認した機関。なお、申請事業者が「情報セキュリティサービス基準」に適合するか否かの審査・判定は、各審査登録機関がその責任において実施する。
※ 66 IPA：情報セキュリティサービス基準適合サービスリストの公開 https://www.ipa.go.jp/security/it-service/service_list.html〔2020/6/30 確認〕
※ 67 SIG（Special Interest Group）：「特定の分野（各業界におけるサイバー攻撃に関する情報）について、情報を交換するグループ」という意味で、J-CSIP では各業界の参加組織の集合体を SIG と呼んでいる。
※ 68 https://www.ipa.go.jp/files/000081877.pdf〔2020/6/30 確認〕
※ 69 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019年 7 月～ 9 月］ https://www.ipa.go.jp/files/000078200.pdf〔2020/6/30 確認〕
※ 70 「マルウェア」等の用語を混在して使用すると、読者を混乱させる可能性があるため、本白書では特に断りのない限り、または文献引用上の正確性を期す必要のない限り、総称して「ウイルス」と表現する。
※ 71 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2019年 10 月～ 12 月］ https://www.ipa.go.jp/files/000080133.pdf〔2020/6/30 確認〕
※ 72 トレンドマイクロ株式会社：サイバー攻撃集団「TICK」による「Operation ENDTRADE」 https://blog.trendmicro.co.jp/archives/23107〔2020/6/30 確認〕
※ 73 IPA：サイバーレスキュー隊 J-CRAT（ジェイ・クラート） https://www.ipa.go.jp/security/J-CRAT/index.html〔2020/6/30 確認〕
IPA：J-CRAT ／標的型サイバー攻撃特別相談窓口 https://www.ipa.go.jp/security/tokubetsu/index.html〔2020/6/30 確認〕
※ 74 IPA：サイバーレスキュー隊 J-CRAT（ジェイ・クラート） https://www.ipa.go.jp/security/J-CRAT/index.html〔2020/6/30 確認〕
※ 75 総務省：サイバーセキュリティタスクフォースの開催 https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000116.html〔2020/7/7 確認〕
※ 76 https://www.soumu.go.jp/main_content/000641510.pdf〔2020/7/7 確認〕
※ 77 総務省：「IoT・5G セキュリティ総合対策プログレスレポート 2020」の公表 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00068.html〔2020/7/7 確認〕
※ 78 総務省：新規制定・改正法令・告示 法律 https://www.soumu.go.jp/menu_hourei/s_houritsu.html〔2020/7/7 確認〕
上記 Web ページの「電気通信事業法及び国立開発研究法人情報通信研究機構法の一部を改正する法律（平成 30 年法律第 24 号）」を参照。
※ 79 https://notice.go.jp/〔2020/7/7 確認〕
※ 80 NISC：IoT機器調査及び利用者への注意喚起プロジェクト https://www.nisc.go.jp/conference/cs/dai21/pdf/21sankou.pdf〔2020/7/7 確認〕
Security NEXT：政府の脆弱 IoT 機器調査「NOTICE」、2 月 20 日から - イメージキャラクターにカンニング竹山さん http://www.security-next.com/102208〔2020/7/7 確認〕
※ 81 総務省・NICT・一般社団法人 ICT-ISAC：脆弱な IoT 機器及びマルウェアに感染している IoT 機器の利用者への注意喚起の実施状況 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00033.html〔2020/7/7 確認〕
※ 82 総務省：端末設備等規則等の一部改正について https://www.soumu.go.jp/main_content/000581187.pdf〔2020/7/7 確認〕
※ 83 総務省：第5世代移動通信システム（5G）の導入のための特定基地局の開設計画の認定（概要） https://www.soumu.go.jp/main_content/000613734.pdf〔2020/7/7 確認〕
※ 84 総務省：ローカル5G導入に関するガイドライン https://www.soumu.go.jp/main_content/000659870.pdf〔2020/7/7 確認〕
※ 85 高い倫理感、技術力を持ち合わせたハッカーをエシカルハッカーと呼ぶ。
※ 86 国立研究開発法人情報通信研究機構、公立大学法人首都大学東京：耐量子計算機暗号の安全性評価で世界記録を達成 https://www.nict.go.jp/press/2019/06/27-1.html〔2020/7/7 確認〕
※ 87 総務省：総務省におけるサイバーセキュリティ研究開発の取組み https://www.nisc.go.jp/conference/cs/kenkyu/dai10/pdf/10shiryou05.pdf〔2020/7/7 確認〕
※ 88 https://www.soumu.go.jp/main_content/000555901.pdf〔2020/7/7 確認〕
※ 89 総務省：サイバー攻撃の防御に向けた情報共有基盤に関する実証事業の成果の公表 https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000153.html〔2020/7/7 確認〕
※ 90 IPA：脅威情報構造化記述形式 STIX 概説 https://www.ipa.go.jp/security/vuln/STIX.html〔2020/7/7 確認〕
※ 91 NICT：実践的サイバー防御演習「CYDER」 https://cyder.nict.go.jp/〔2020/7/7 確認〕
※ 92 NICT：cyber colosseo https://colosseo.nict.go.jp/〔2020/7/7 確認〕
※ 93 総務省：「自治体情報セキュリティ対策の見直しについて」の公表 https://www.soumu.go.jp/menu_news/s-news/01gyosei07_02000098.html〔2020/7/7 確認〕
※ 94 https://www.soumu.go.jp/main_content/000575052.pdf〔2020/7/7 確認〕
※ 95 総務省：プラットフォームサービスに関する研究会の開催 https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000050.html〔2020/7/7 確認〕
※ 96 総務省：トラストサービス検討ワーキンググループ（第 1 回） https://www.soumu.go.jp/main_sosiki/kenkyu/platform_service/02cyber01_04000001_00016.html〔2020/7/7 確認〕
※ 97 総務省：プラットフォームサービスに関する研究会最終報告書 https://www.soumu.go.jp/main_content/000668595.pdf〔2020/7/7 確認〕
※ 98 NISC：サイバーセキュリティ戦略の変更について https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf〔2020/7/6 確認〕
※ 99 警察庁：サイバーセキュリティ戦略の改定について（依命通達） https://www.npa.go.jp/cybersecurity/pdf/300906_senryaku.pdf〔2020/7/6 確認〕
警察庁：サイバーセキュリティ重点施策の改定について（通達） https://www.npa.go.jp/cybersecurity/pdf/300906_juutensesaku.pdf〔2020/7/6 確認〕
※ 100 警察庁：令和元年におけるサイバー空間をめぐる脅威の情勢等について https://www.npa.go.jp/publications/statistics/cybersecurity/data/R01_cyber_jousei.pdf〔2020/7/6 確認〕

※ 101 警察庁：サイバー空間の脅威への対処に係る人材育成方針の改定について（通達） https://www.npa.go.jp/laws/notification/kanbou/kikaku/2019kikaku-h4.pdf〔2020/7/6 確認〕
※ 102 警察庁：フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（全銀協等と連携した注意喚起） http://www.npa.go.jp/cyber/policy/caution1910.html〔2020/7/6 確認〕
※ 103 JC3：クレジットカード情報窃取の手口に注意 https://www.jc3.or.jp/topics/credit_card.html〔2020/7/6 確認〕
※ 104 警察庁：令和元年の国際協力等の状況 https://www.npa.go.jp/about/overview/kokusai/kyouryoku/R01.pdf〔2020/7/6 確認〕
※ 105 https://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_cyber_jousei.pdf〔2020/7/6 確認〕
※ 106 サイバーセキュリティ.com：人事情報など167万件を不正閲覧、男性職員を停職及び降任処分｜長崎県 https://cybersecurity-jp.com/news/34706〔2020/7/6 確認〕
※ 107 産経新聞：7pay詐欺容疑で逮捕 熊本県警 https://www.sankei.com/region/news/191004/rgn1910040021-n1.html〔2020/7/6 確認〕
※ 108 産経新聞：ゲームアプリ不正使用の疑い https://www.sankei.com/region/news/191102/rgn1911020020-n1.html〔2020/7/6 確認〕
※ 109 日本経済新聞：元漫画村運営者「責任ある」、起訴内容認める 福岡 https://www.nikkei.com/article/DGXMZO53408570W9A211C1ACYZ00/〔2020/7/20 確認〕
※ 110 正式名称は「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r4.pdf〔2020/6/30 確認〕）。現在は、「電子政府推奨暗号リスト」「推奨候補暗号リスト」「運用監視暗号リスト」の三つのリストから構成される。
※ 111-1 NIST:FIPS 186-5(Draft) Digital Signature Standard (DSS) https://csrc.nist.gov/publications/detail/fips/186/5/draft〔2020/6/30 確認〕
※ 111-2 IPA：暗号鍵管理ガイドライン https://www.ipa.go.jp/security/vuln/ckms.html〔2020/7/22 確認〕
※ 111-3 IPA:TLS 暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～ https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html〔2020/7/22 確認〕
※ 112 外務省：G20 大阪サミット https://www.mofa.go.jp/mofaj/gaiko/g20/osaka19/jp/〔2020/6/30 確認〕
※ 113 World Economic Forum 2019 https://www.weforum.org/events/world-economic-forum-annual-meeting-2019〔2020/6/30 確認〕
※ 114 外務省：大阪トラック https://www.mofa.go.jp/mofaj/ecm/it/page25_001989.html〔2020/6/30 確認〕
※ 115 外務省：河野外務大臣の G20 貿易・デジタル経済大臣会合（茨城県つくば市）への出席（結果） https://www.mofa.go.jp/mofaj/ecm/it/page4_005041.html〔2020/6/30 確認〕
※ 116 外務省：G20 AI 原則 https://www.mofa.go.jp/mofaj/gaiko/g20/osaka19/pdf/documents/jp/annex_08.pdf〔2020/6/30 確認〕
※ 117 U.S. Department of State：The Seventh U.S.-Japan Cyber Dialogue https://www.state.gov/the-seventh-u-s-japan-cyber-dialogue/〔2020/6/30 確認〕
※ 118 外務省：日米首脳会談 https://www.mofa.go.jp/mofaj/na/na1/us/page4_005001.html〔2020/6/30 確認〕
※ 119 防衛省：日米サイバー防衛政策ワーキンググループ（CDPWG）第7回会合について https://www.mod.go.jp/j/press/news/2019/10/25b.html〔2020/6/30 確認〕
※ 120 外務省：第4回日 EU サイバー対話 https://www.mofa.go.jp/mofaj/erp/ep/page23_003018.html〔2020/6/30 確認〕
※ 121 外務省：サイバー犯罪に関する条約（略称：サイバー犯罪条約） https://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html
※ 122 外務省：第5回日仏サイバー協議の開催 https://www.mofa.go.jp/mofaj/fp/cp/page22_003266.html〔2020/6/30 確認〕
※ 123 外務省：サイバー規範イニシアティブに関するディナール宣言 https://www.mofa.go.jp/mofaj/files/000466471.pdf〔2020/6/30 確認〕
※ 124 外務省：第5回日英サイバー協議の開催 https://www.mofa.go.jp/mofaj/press/release/press4_008287.html〔2020/6/30 確認〕
※ 125 外務省：日英首脳会談 https://www.mofa.go.jp/mofaj/area/uk/page6_000372.html〔2020/6/30 確認〕
※ 126 BBC：What is the transition period? https://www.bbc.com/news/uk-politics-50838994〔2020/6/30 確認〕
※ 127 外務省：第3回日露サイバー協議の開催 https://www.mofa.go.jp/mofaj/press/release/press4_008022.html〔2020/6/30 確認〕
※ 128 外務省：第2回日ウクライナサイバー協議 https://www.mofa.go.jp/mofaj/erp/c_see/ua/page25_002085.html〔2020/6/30 確認〕
※ 129 総務省：第12回日・ASEAN サイバーセキュリティ政策会議の結果 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00049.html〔2020/6/30 確認〕
※ 130 http://aseanregionalforum.asean.org/〔2020/6/30 確認〕
※ 131 外務省：サイバーセキュリティに関する ARF 会期間会合のための第3回専門家会合の開催 https://www.mofa.go.jp/mofaj/press/release/press4_007030.html〔2020/6/30 確認〕
※ 132 外務省：サイバーセキュリティに関する第2回 ARF 会期間会合等の開催 https://www.mofa.go.jp/mofaj/press/release/press4_007262.html〔2020/6/30 確認〕
※ 133 外務省：サイバーセキュリティに関する ARF 会期間会合のための第5回専門家会合の開催 https://www.mofa.go.jp/mofaj/press/release/press4_008249.html〔2020/6/30 確認〕
※ 134 2018 年 12 月、第 73 回国連総会決議（A／RES／73／266）に基づき、国際安全保障の文脈におけるサイバー空間での責任ある国家の行動の進展に関して 25 ヵ国からの専門家（25 名）による専門的な議論の場として、国連のもとに立ち上がる会合。GGE は過去 5 会期にわたり実施されている。2019 年 12 月に第 1 回会合を開催し、全部で 4 回の本会合を経て 2021 年の国連総会において報告書を提出することとなっている。
※ 135 正式名称は「国際安全保障の文脈における情報及び電気通信分野での発展に関するオープン・エンド作業部会」。2018 年 12 月、第 73 回国連総会決議（A／RES／73／27）に基づき、国際安全保障の文脈における情報、及び電気通信分野の発展に関して国連全加盟国参加可能な議論の場として、2019 年より国連のもとに初めて立ち上がる会合。2019 年 9 月に第 1 回会合を開催し、全部で 3 回の本会合を経て 2020 年の国連総会において報告書を提出することとなっている。
※ 136 外務省：第3回日・インドサイバー対話の開催 https://www.mofa.go.jp/mofaj/press/release/press1_000330.html〔2020/6/30 確認〕
「情報セキュリティ白書 2019」の「2.2.1（6）インドとのサイバー連携」（p.82）を参照。
※ 137 慶應義塾大学：第9回サイバーセキュリティ国際シンポジウム https://cysec-lab.keio.ac.jp/sympo1912/index-j.html〔2020/6/30 確認〕
※ 138 ICT ISAC Japan：サイバーセキュリティ国際シンポジウム https://www.ict-isac.jp/news/news20191008.html〔2020/6/30 確認〕
※ 139 日本経済新聞／株式会社日経 BP：サイバー・イニシアチブ東京 2019 https://project.nikkeibp.co.jp/event/19z1212cit/〔2020/6/30 確認〕
※ 140 時事通信社：米中、貿易協議「第1段階」合意 追加関税の発動見送り―来月めど署名 https://www.jiji.com/jc/article?k=2019121400242&g=int〔2020/6/30 確認〕
※ 141 時事通信社：米中「第1段階」合意発効 初の関税下げ―摩擦緩和も火種残る https://www.jiji.com/jc/article?k=2020021400772&g=int〔2020/6/30 確認〕
※ 142 時事通信社：米政府、中国製マスクの制裁関税免除 新型コロナ配慮か https://www.jiji.com/jc/article?k=2020030700350&g=int〔2020/6/30 確認〕
※ 143 The Washington Post：Apparently, Trump ignored early coronavirus warnings. That has consequences https://www.washingtonpost.com/politics/2020/03/23/apparently-trump-ignored-early-coronavirus-warnings-that-has-consequences/〔2020/6/30 確認〕
※ 144 BBC：Trump declares national emergency over coronavirus https://www.bbc.com/news/world-us-canada-51882381〔2020/6/30 確認〕
※ 145 BBC：Coronavirus: US to halt funding to WHO, says Trump https://www.bbc.com/news/world-us-canada-52289056〔2020/6/30 確認〕
※ 146 AFP：トランプ氏が中国批判、故意ならパンデミックの「報いを受けるべき」 https://www.afpbb.com/articles/-/3279279〔2020/6/30 確認〕
※ 147 AFP：新型コロナ、武漢の研究所が発生源の可能性確信=トランプ米大統 https://jp.reuters.com/article/health-coronavirus-usa-idJPKBN22C3ZE〔2020/6/30 確認〕
※ 148 時事通信社：偽ニュース拡散、中国非難 警戒強めるEU―新型コロナ https://www.jiji.com/jc/article?k=2020061100867&g=int〔2020/6/30 確認〕
※ 149 Bloomberg：Trump Says U.S. Must Reopen Even If More Americans Get Sick, Die https://www.bloomberg.com/news/articles/2020-05-05/trump-says-u-s-must-reopen-even-if-more-americans-get-sick〔2020/6/30 確認〕
※ 150 CONGRESS.GOV：H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019 https://www.

congress.gov/bill/115th-congress/house-bill/5515/text〔2020/6/30 確認〕
※ 151 5 社とは、Huawei Technologies Co. Ltd.（ネットワーク機器）、ZTE Corporation（通信機器）、Hangzhou Hikvision Digital Technology Co., Ltd.（監視カメラ）、Dahua Technology Co. Ltd.（防犯カメラ）、Hytera Communications Co. Ltd.（無線機）。
※ 152 CONGRESS.GOV：H.R.2500 - National Defense Authorization Act for Fiscal Year 2020 https://www.congress.gov/bill/116th-congress/house-bill/2500〔2020/6/30 確認〕
※ 153 Cyberspace Solarium Commission：https://www.solarium.gov/home〔2020/6/30 確認〕
※ 154 BUSINESS INSIDER：A senate report says the US government's current plan to prepare for cyber doomsday isn't nearly strong enough https://www.businessinsider.com/senate-report-says-us-government-needs-stronger-cyber-doomsday-plan-2020-3〔2020/6/30 確認〕
※ 155 DoD：SUMMARY DEPARTMENT OF DEFENSE CYBER STRATEGY 2018 https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF〔2020/6/30 確認〕
※ 156 COUNCIL ON FOREIGN RELATIONS：U.S. Cyber Command's Malware Inoculation: Linking Offense and Defense in Cyberspace https://www.cfr.org/blog/us-cyber-commands-malware-inoculation-linking-offense-and-defense-cyberspace〔2020/6/30 確認〕
※ 157 U.S. Cyber Command：https://www.cybercom.mil/〔2020/6/30 確認〕
※ 158 DoD：DOD to Require Cybersecurity Certification in Some Contract Bids https://www.defense.gov/Explore/News/Article/Article/2071434/dod-to-require-cybersecurity-certification-in-some-contract-bids/〔2020/6/30 確認〕
※ 159 NIST：SP 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final〔2020/6/30 確認〕
※ 160 Defense Federal Acquisition Regulation Supplement：DFARS 252.204-7012 Defense Industrial Base Compliance Information https://www.acq.osd.mil/eie/Downloads/IE/DFARS%207012%20Information%20Paper.pdf〔2020/6/30 確認〕
※ 161 DoD：DOD Announces Enterprise General Purpose Cloud Contract Award https://www.defense.gov/Newsroom/Releases/Release/Article/1999651/dod-announces-enterprise-general-purpose-cloud-contract-award/〔2020/6/30 確認〕
※ 162 ZDNet：US Federal Court judge grants AWS request to temporarily block JEDI contract work https://www.zdnet.com/article/u-s-federal-court-judge-grants-aws-request-to-temporarily-block-jedi-contract-work/〔2020/6/30 確認〕
※ 163 WIRED：Microsoft Is the Surprise Winner of a $10B Pentagon Contract https://www.wired.com/story/microsoft-surprise-winner-dollar10b-pentagon-contract/〔2020/6/30 確認〕
※ 164 DoD：DOD Adopts Ethical Principles for Artificial Intelligence https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/source/GovDelivery/〔2020/6/30 確認〕
※ 165 The White House：Artificial Intelligence for the American People https://www.whitehouse.gov/ai/〔2020/6/30 確認〕
※ 166 DHS：CISA https://www.cisa.gov/〔2020/6/30 確認〕
※ 167 Task Forceについては「情報セキュリティ白書2019」の「2.2.2(2)(c)戦略の分析」(p.86)を参照。
※ 168 CISA：CISA'S ICT SUPPLY CHAIN RISK MANAGEMENT TASK FORCE APPROVES NEW WORKING GROUP FOR SECOND PHASE https://www.cisa.gov/news/2019/12/18/cisas-ict-supply-chain-risk-management-task-force-approves-new-working-group-second〔2020/6/30 確認〕
※ 169 COVINGTON：CISA Information and Communications Technology Supply Chain Risk Management Task Force Releases New Guidance on Security Resiliency https://www.globalpolicywatch.com/2020/05/cisa-information-and-communications-technology-supply-chain-risk-management-task-force-releases-new-guidance-on-security-resiliency/〔2020/6/30 確認〕
※ 170 The White House：Executive Order on Securing the Information and Communications Technology and Services Supply Chain https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/〔2020/6/30 確認〕
※ 171 Federal Register：Securing the Information and Communications Technology and Services Supply Chain https://www.federalregister.gov/documents/2019/12/23/2019-27596/securing-the-information-and-communications-technology-and-services-supply-chain〔2020/6/30 確認〕
※ 172 Business Roundtable：Business Roundtable Comments to the Proposed Rule on Securing the Information and Communications Technology and Services Supply Chain https://www.businessroundtable.org/business-roundtable-comments-to-the-proposed-rule-on-securing-the-information-and-communications-technology-and-services-supply-chain〔2020/6/30 確認〕
※ 173 CISA：EXECUTIVE ORDER 13873 RESPONSE https://www.cisa.gov/sites/default/files/publications/eo-response-methodology-for-assessing-ict_v2_508.pdf〔2020/6/30 確認〕
※ 174 BBC：Qasem Soleimani: US kills top Iranian general in Baghdad air strike https://www.bbc.com/news/world-middle-east-50979463〔2020/6/30 確認〕
※ 175 CISA：CISA INSIGHTS Increased Geopolitical Tensions and Threats https://www.cisa.gov/sites/default/files/publications/CISA-Insights-Increased-Geopolitical-Tensions-and-Threats-S508C.pdf〔2020/6/30 確認〕
※ 176 CISA：Defending Against COVID-19 Cyber Scams https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams〔2020/6/30 確認〕
※ 177 CISA：CISA INSIGHTS Risk Management for Novel Coronavirus (COVID-19) https://www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf〔2020/6/30 確認〕
※ 178 FBI：Protect Your Wallet—and Your Health—from Pandemic Scammers https://www.fbi.gov/news/stories/protect-yourself-from-covid-19-scams-040620
※ 179 CISA：Alert (AA20-099A) https://www.us-cert.gov/ncas/alerts/aa20-099a〔2020/6/30 確認〕
※ 180 CISA：Alert (AA20-126A) https://www.us-cert.gov/ncas/alerts/AA20126A〔2020/6/30 確認〕
※ 181 CISA：Telework Guidance and Resources https://www.cisa.gov/telework〔2020/6/30 確認〕
※ 182 BUSINESS INSIDER：US accuses Russia of spreading conspiracies about the Wuhan coronavirus, including that it's a CIA biological weapon https://www.businessinsider.com/us-officials-claim-russian-coronavirus-disinformation-campaign-2020-2?r=US&IR=T〔2020/6/30 確認〕
※ 183 BBC：Brexit: UK leaves the European Union https://www.bbc.com/news/uk-politics-51333314〔2020/6/30 確認〕
※ 184 Bloomberg：U.K. and EU Draw Battle Lines as the Hard Part of Brexit Begins https://www.bloomberg.com/news/articles/2020-01-20/u-k-eu-draw-battle-lines-as-the-hard-part-of-brexit-begins〔2020/6/30 確認〕
※ 185 House of Commons Library：The UK-EU future relationship negotiations: process and issues https://commonslibrary.parliament.uk/research-briefings/cbp-8834/〔2020/6/30 確認〕
※ 186 欧州逮捕状（EAW）：EU 加盟国が、犯罪組織への参加、テロ行為、サイバー犯罪、殺人等の犯罪に加担したとして他の EU 加盟国が発行する逮捕状を自国で執行するシステム。
※ 187 European Court of Human Rights/Council of Europe:ヨーロッパにおける人権および基本的自由の保護のための条約 https://www.echr.coe.int/Documents/Convention_JPN.pdf〔2020/6/30 確認〕
※ 188 European Union External Action：The Common Security and Defence Policy (CSDP) https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/431/common-security-and-defence-policy-csdp_en〔2020/6/30 確認〕
※ 189 legislation.gov.uk：Investigatory Powers Act 2016 http://www.legislation.gov.uk/ukpga/2016/25/section/1/enacted〔2020/6/30 確認〕
※ 190 GOV.UK：The NIS Regulations 2018 https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018〔2020/6/30 確認〕
※ 191 Taylor & Francis Online: Brexit and Cyber Security https://www.tandfonline.com/doi/full/10.1080/03071847.2019.1643256〔2020/6/30 確認〕
※ 192 ZDNET：After Brexit, Europe wants cybersecurity pact with UK https://www.zdnet.com/article/after-brexit-europe-wants-cybersecurity-pact-with-uk/〔2020/6/30 確認〕
※ 193 ICO：Intention to fine British Airways £183.39m under GDPR for data breach https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-

british-airways/〔2020/6/30 確認〕
※ 194 ICO: Statement：Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach〔2020/6/30 確認〕
※ 195 DIGIDAY：250 億円!：GDPR 違反で、初の大型制裁金が科せられる https://digiday.jp/brands/2019-is-the-year-of-enforcement-gdpr-fines-have-begun/〔2020/6/30 確認〕
※ 196 European Data Protection Board：Administrative criminal proceedings of the Austrian data protection authority against Österreichische Post AG (Austrian Postal Service) https://edpb.europa.eu/news/national-news/2019/administrative-criminal-proceedings-austrian-data-protection-authority_en〔2020/6/30 確認〕
※ 197 LEXOLOGY：Austria：Data Protection Authority imposes EUR 18 million fine on Austrian Post https://www.lexology.com/library/detail.aspx?g=7865633f-6ad1-4919-911f-81c11ec65567〔2020/6/30 確認〕
※ 198 European Data Protection Board：Berlin Commissioner for Data Protection Imposes Fine on Real Estate Company https://edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_en〔2020/6/30 確認〕
※ 199 European Data Protection Board：MARKETING: THE ITALIAN SA FINES TIM EUR 27.8 MILLION https://edpb.europa.eu/news/national-news/2020/marketing-italian-sa-fines-tim-eur-278-million_en〔2020/6/30 確認〕
GARANTE：Provvedimento correttivo e sanzionatorio nei confronti di TIM S.p.A. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9256486〔2020/6/30 確認〕
※ 200 EC：The Cybersecurity Act strengthens Europe's cybersecurity https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity〔2020/6/30 確認〕
※ 201 EU：REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&qid=1579157494056&from=EN〔2020/6/30 確認〕
※ 202 Jones Day：INSIGHTS The EU Cybersecurity Act is Now Applicable https://www.jonesday.com/en/insights/2019/06/the-eu-cybersecurity-act-is-now-applicable〔2020/6/30 確認〕
※ 203 CEN-CENELEC Management Centre：Cybersecurity Act - Establishing the link between Srandardization and Certification https://www.cencenelec.eu/News/Events/Pages/EV-2018-001.aspx〔2020/6/30 確認〕
※ 204 EU サイバーセキュリティ庁：Conference: Towards the EU Cybersecurity Certification Framework https://www.enisa.europa.eu/events/towards_security_framework/towards_security_framework〔2020/6/30 確認〕
※ 205 EU サイバーセキュリティ庁：Conference: Towards the EU Cybersecurity Certification Framework https://www.enisa.europa.eu/events/towards_certification_framework/towards_security_framework〔2020/6/30 確認〕
※ 206 Ad hoc WG の設立は、EU サイバーセキュリティ法の Article 49 に規定されている。
※ 207 ECSO：About the cPPP https://ecs-org.eu/cppp〔2020/6/30 確認〕
※ 208 https://ecs-org.eu/〔2020/6/30 確認〕
※ 209 Dr. Martin Schaffer：European Cyber Security Certification: ECSO Meta-scheme Approach https://www.enisa.europa.eu/events/towards_security_framework/Presentation%20-%20Schaffer〔2020/6/30 確認〕
※ 210 https://eucyberact.org/〔2020/6/8 確認〕
※ 211 ECCG の設立は、EU サイバーセキュリティ法の Article 62 に規定されている。
※ 212 Common Criteria：https://www.commoncriteriaportal.org/〔2020/6/30 確認〕
SOG-IS（Senior Officials Group Information Systems Security）：https://www.sogis.eu/〔2020/7/22 確認〕
※ 213 GlobalPlatform：Security Certification https://globalplatform.org/certifications/security-certification/〔2020/6/30 確認〕
※ 214 TrustCB B.V.：IoT Evaluation and Certification https://www.trustcb.com/blog/iot-evaluation-and-certification/〔2020/6/30 確認〕
※ 215 European Commission:COMMISSION RECOMMENDATION (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0534&from=GA〔2020/6/30 確認〕
勧告の詳細については「情報セキュリティ 2019」の「2.2.3（4）(b) 5G ネットワークに関するリスクアセスメント指針」(p.89)を参照。
※ 216 European Commission：NIS Cooperation Group https://ec.europa.eu/digital-single-market/en/nis-cooperation-group〔2020/6/30 確認〕
※ 217 European Commission：Member States publish a report on EU coordinated risk assessment of 5G networks security https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049〔2020/6/30 確認〕
※ 218 EU サイバーセキュリティ庁：ENISA threat landscape for 5G networks https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks〔2020/6/30 確認〕
※ 219 European Commission：Secure 5G networks: Commission endorses EU toolbox and sets out next steps https://ec.europa.eu/commission/presscorner/detail/en/IP_20_123〔2020/6/30 確認〕
※ 220 The Japan Times：Huawei wins contract to develop German 5G network, subject to approval from Berlin https://www.japantimes.co.jp/news/2019/12/12/business/huawei-wins-contract-develop-german-5g-network-subject-berlins-nod/#.XtO-JTr7RPZ〔2020/6/30 確認〕
※ 221 独立行政法人日本貿易振興機構：英国政府、5G 通信網へのファーウェイの一部参入を容認 https://www.jetro.go.jp/biznews/2020/01/af47ec419f1668da.html〔2020/6/30 確認〕
※ 222 The Guardian：Boris Johnson forced to reduce Huawei's role in UK's 5G networks https://www.theguardian.com/technology/2020/may/22/boris-johnson-forced-to-reduce-huaweis-role-in-uks-5g-networks〔2020/6/30 確認〕
※ 223 South China Morning Post：Germany's Telefonica Deutschland picks Ericsson for 5G core network over Huawei https://www.scmp.com/tech/policy/article/3087184/germanys-telefonica-deutschland-picks-ericsson-5g-core-network-over〔2020/6/30 確認〕
※ 224 BBC：Hong Kong：US and allies defend 'bastion of freedom' https://www.bbc.com/news/world-asia-china-52837229〔2020/6/30 確認〕
※ 225 TWNCERT:https://www.twncert.org.tw/〔2020/6/30 確認〕
※ 226 全國法規資料庫：Cyber Security Management Act https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030297〔2020/6/30 確認〕
※ 227 National Security Office：National Cybersecurity Strategy https://www.krcert.or.kr/filedownload.do?attach_file_seq=2162&attach_file_id=EpF2162.pdf〔2020/6/30 確認〕
※ 228 KrCERT/CC：https://www.krcert.or.kr/krcert/intro.do〔2020/6/30 確認〕
※ 229 Department of the Prime Minister and Cabinet：New Zealand's Cyber Security Strategy 2019 https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2019〔2020/6/30 確認〕
※ 230 https://www.cert.govt.nz/〔2020/6/30 確認〕
※ 231 CERT NZ：Advisories https://www.cert.govt.nz/it-specialists/advisories/〔2020/6/30 確認〕
※ 232 CERT NZ：Alerts https://www.cert.govt.nz/individuals/alerts/〔2020/6/30 確認〕
※ 233 APNIC：https://www.apnic.net/〔2020/6/30 確認〕
※ 234 APNIC：Hands-on training seeks to secure Nauru' s future networks https://blog.apnic.net/2019/09/30/hands-on-training-seeks-to-secure-naurus-future-networks/〔2020/6/30 確認〕
APNIC：Register now for Information Security intermediate workshop in Vanuatu https://blog.apnic.net/2019/05/17/register-now-for-information-security-intermediate-workshop-in-vanuatu/〔2020/6/30 確認〕
※ 235 APNIC：Cybersecurity training series builds skills and regional cooperation https://blog.apnic.net/2019/06/13/cybersecurity-training-series-builds-skills-and-regional-cooperation/〔2020/6/30 確認〕
※ 236 APCERT：https://www.apcert.org/〔2020/6/30 確認〕
※ 237 APCERT：TSUBAME Working Group https://www.apcert.org/about/structure/tsubame-wg/index.html〔2020/6/30 確認〕
※ 238 APCERT：APCERT CYBER DRILL 2019“CATASTROPHIC SILENT DRAINING IN ENTERPRISE NETWORK” https://www.

apcert.org/documents/pdf/APCERT_Drill2019_Press%20Release.pdf〔2020/6/30 確認〕
※ 239 APCERT：Documents　https://www.apcert.org/documents/index.html〔2020/6/30 確認〕
※ 240 SingCERT：https://www.csa.gov.sg/singcert〔2020/6/30 確認〕
※ 241 SingCERT：APCERT Conference 2019　https://www.apcert2019.sg/〔2020/2/12 確認〕
※ 242 Sri Lanka CERT|CC：https://www.cert.gov.lk/〔2020/6/30 確認〕
※ 243 Australian Cyber Security Centre：https://www.cyber.gov.au/〔2020/6/30 確認〕
※ 244 CyberSecurity Malaysia：https://www.cybersecurity.my/en/index.html〔2020/6/30 確認〕
※ 245 Singapore Cyber Security Agency：Singapore International Cyber Week 2019 - Highlights and Testimonials https://www.csa.gov.sg/news/press-releases/sicw-2019---highlights-and-testimonials〔2020/6/30 確認〕
※ 246 The Straits Times：New Asean cyber-security centre launched to train response teams to combat online threats https://www.straitstimes.com/tech/new-asean-cyber-security-centre-launched-to-train-response-teams-to-combat-online-threats〔2020/6/30 確認〕
※ 247 総務省：日 ASEAN サイバーセキュリティ能力構築センターの設立　https://www.soumu.go.jp/menu_news/s-news/01tsushin09_02000074.html〔2020/6/30 確認〕
※ 248 OpenGov Asia：ETDA holds training to boost cybersecurity knowledge　https://www.opengovasia.com/etda-holds-training-to-boost-cybersecurity-knowledge/〔2020/6/30 確認〕
※ 249 Australian Cyber Security Centre: Strengthening cyber security across the Pacific　https://www.cyber.gov.au/news/pacific-islands〔2020/6/30 確認〕
※ 250 経済産業省：IT 人材の最新動向と将来推計に関する調査結果 ～ 報告書概要版 ～　https://warp.da.ndl.go.jp/info:ndljp/pid/10159415/www.meti.go.jp/press/2016/06/20160610002/20160610002-7.pdf〔2020/6/30 確認〕
※ 251 NRI セキュアテクノロジーズ社：NRI Secure Insight 2019 ～企業における情報セキュリティ実態調査～　https://www.secure-sketch.com/ebook-download/insight2019-report〔2020/6/30 確認〕
※ 252 IPA:ITSS+（プラス）・IT スキル標準（ITSS）・情報システムユーザースキル標準（UISS）関連情報　https://www.ipa.go.jp/jinzai/itss/itssplus.html〔2020/6/30 確認〕
※ 253 経済産業省：理工系人材需給状況に関する調査結果概要 https://www.meti.go.jp/press/2018/04/20180420005/20180420005-1.pdf〔2020/6/30 確認〕
※ 254 経済産業省：理工系人材需給状況に関する調査結果を取りまとめました　https://www.meti.go.jp/press/2018/04/20180420005/20180420005.html〔2020/6/30 確認〕
※ 255 経済産業省：第四次産業革命スキル習得講座認定制度　https://www.meti.go.jp/policy/economy/jinzai/reskillprograms/index.html〔2020/6/30 確認〕
※ 256 経済産業省：第四次産業革命スキル習得講座 一覧　https://www.meti.go.jp/policy/economy/jinzai/reskillprograms/pdf/kouzaichiran.pdf〔2020/6/30 確認〕
※ 257 厚生労働省：教育訓練プログラムの開発　https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou_roudou/jinzaikaihatsu/program_development.html〔2020/6/30 確認〕
※ 258 https://www.keidanren.or.jp/policy/2020/025.html〔2020/6/30 確認〕
※ 259 https://cyber-risk.or.jp/cric-csf/jinzai_reference_2016.html〔2020/6/30 確認〕
※ 260 https://cyber-risk.or.jp/contents/CRICCSF_OT-Security_Skill-Reference_1.0_20190731.pdf〔2020/6/30 確認〕
※ 261 https://www.jnsa.org/isepa/images/outputs/JTAG_guideline-%CE%B2_190118.pdf〔2020/6/30 確認〕
※ 262 重要インフラ：他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもので、重要インフラ分野として指定する分野。具体的には、「情報通信」「金融」「航空」「空港」「鉄道」「電力」「ガス」「政府・行政サービス（地方公共団体を含む）」「医療」「水道」「物流」「化学」「クレジット」及び「石油」の 14 分野。
NSC:「重要インフラの情報セキュリティ対策に係る第4次行動計画（改定）」　https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r2.pdf〔2020/6/30 確認〕
※ 263 IPA：中核人材育成プログラム修了者コミュニティ「叶会（かなえかい）」　https://www.ipa.go.jp/icscoe/program/core_human_resource/icscoe_alumni.html〔2020/6/30 確認〕
※ 264 IPA：情報処理安全確保支援士（登録セキスペ）になるには https://www.ipa.go.jp/siensi/toberiss/index.html#section1〔2020/6/30 確認〕
※ 265 IPA：製造・生産分野の管理監督者層向けプログラム　https://www.ipa.go.jp/icscoe/program/seizo-seisan/index.html〔2020/6/30 確認〕
※ 266 IPA：責任者向けプログラム サイバー危機対応机上演習（CyberCREST）　https://www.ipa.go.jp/icscoe/program/short/all_industries/2019.html
※ 267 IPA：責任者向けプログラム 業界別サイバーレジリエンス強化演習（CyberREX）　https://www.ipa.go.jp/icscoe/program/short/specific_industries/2019.html〔2020/6/30 確認〕
※ 268 IPA：戦略マネジメント系セミナー　https://www.ipa.go.jp/icscoe/program/middle/strategic_management/2019.html〔2020/6/30 確認〕
※ 269 IPA：制御システム向けサイバーセキュリティ演習　https://www.ipa.go.jp/icscoe/program/short/icssec/index.html〔2020/6/30 確認〕
※ 270 IPA：情報処理技術者試験 情報処理安全確保支援士試験 統計資料 令和元年度秋期試験全試験区分版　https://www.jitec.ipa.go.jp/1_07toukei/toukei_r01a.pdf〔2020/6/30 確認〕
※ 271 IPA：プレス発表　平成 31 年度春期情報処理技術者試験（情報セキュリティマネジメント試験、基本情報技術者試験）の合格者を発表 https://www.ipa.go.jp/about/press/20190522.html〔2020/6/30 確認〕
IPA：令和元年度秋期情報処理技術者試験（情報セキュリティマネジメント試験、基本情報技術者試験）の合格者を発表　https://www.jitec.ipa.go.jp/1_00topic/topic_20191120.html〔2020/6/30 確認〕
※ 272 IPA：国家資格「情報処理安全確保支援士」2020 年 4 月 1 日付登録人数 1,096 人（総数 20,413 人）　https://www.ipa.go.jp/siensi/data/20200401newriss.html〔2020/6/30 確認〕
※ 273 IPA：情報処理安全確保支援士（登録セキスペ）の受講する講習について　https://www.ipa.go.jp/siensi/lecture/index.html〔2020/6/30 確認〕
※ 274 IPA：セキュリティの実態を踏まえた登録セキスペへの期待と役割　https://www.ipa.go.jp/files/000079909.pdf〔2020/6/30 確認〕
※ 275 IPA：活用企業・組織のインタビュー　https://www.ipa.go.jp/siensi/data/interview.html〔2020/6/30 確認〕
IPA：情報処理安全確保支援士（登録セキスペ）制度のご紹介　https://www.ipa.go.jp/files/000063331.pdf〔2020/6/30 確認〕
※ 276 IPA：プレス発表　12 月 6 日公布の法律改正に伴う情報処理安全確保支援士制度の見直し　https://www.ipa.go.jp/about/press/20191212_3.html〔2020/6/30 確認〕
IPA：情報処理安全確保支援士（登録セキスペ）制度の見直しについて https://www.ipa.go.jp/siensi/kaisei.html〔2020/6/30 確認〕
※ 277 IPA：セキュリティ・キャンプ全国大会 2019　ホーム　https://www.ipa.go.jp/jinzai/camp/2019/zenkoku2019_index.html〔2020/6/30 確認〕
※ 278 一般社団法人セキュリティ・キャンプ協議会：地方大会　実施状況　https://www.security-camp.or.jp/minicamp/index.html〔2020/6/30 確認〕
※ 279 一般社団法人セキュリティ・キャンプ協議会：セキュリティ・ジュニアキャンプ in 高知 2019　https://www.security-camp.or.jp/minicamp/kochi2019.html〔2020/6/30 確認〕
※ 280 IPA：セキュリティ・ネクストキャンプ 2019　ホーム　https://www.ipa.go.jp/jinzai/camp/2019/next2019_index.html〔2020/6/30 確認〕
※ 281 一般社団法人セキュリティ・キャンプ協議会：セキュリティ・キャンプアワード 2020　https://www.security-camp.or.jp/event/award2020.html〔2020/6/30 確認〕
※ 282 IPA：「セキュリティ・キャンプフォーラム 2020」開催のご案内 https://www.ipa.go.jp/jinzai/camp/2019/forum2020.html〔2020/6/30 確認〕
一般社団法人セキュリティ・キャンプ協議会：セキュリティ・キャンプ交友会 2020 春　https://www.security-camp.or.jp/event/friend2020spr.html〔2020/6/30 確認〕
※ 283 一般社団法人セキュリティ・キャンプ協議会：GCC Tokyo - Global Cybersecurity Camp　https://www.security-camp.or.jp/event/gcc_tokyo.html〔2020/6/30 確認〕
ScanNetSecurity：サイバーセキュリティの新鋭集結、アジア各国の若者が互いの国を知る ～ GCC Tokyo 2020　https://scan.netsecurity.ne.jp/article/2020/03/24/43854.html〔2020/6/30 確認〕
※ 284 enPiT：2019 年度 成果報告　http://www.enpit.jp/files/enPiT_annualreport_uni_2019.pdf〔2020/6/30 確認〕
※ 285 文部科学省：平成 29 年度「成長分野を支える情報技術人材の育成拠点の形成（enPiT）」enPiT-Pro の選定状況について　http://

www.mext.go.jp/a_menu/koutou/kaikaku/enpit/1395904.htm〔2020/6/30 確認〕
※ 286 http://www.seccap.pro/〔2020/6/30 確認〕
※ 287 CTF（Capture The Flag）：互いに相手陣地にある旗を奪い合う野外ゲームを情報セキュリティに適用したもので、例えば自分のホストを守りながら、相手チームのホストを攻撃する競技等がある。
※ 288 https://www.seccon.jp/2019/〔2020/6/30 確認〕
※ 289 NETIB-NEWS：CTF 国際大会第 1 位の栄冠を手にしたのは日本チーム! https://www.data-max.co.jp/article/34132/?rank〔2020/6/30 確認〕
※ 290 SECCON2019 運営事務局：SECCON Beginners とは https://www.seccon.jp/2019/beginners/about-seccon-beginners.html〔2020/6/30 確認〕
※ 291 SECCON2019 運営事務局：CTF for GIRLS とは https://www.seccon.jp/2019/girls/ctf-for-girls.html〔2020/6/30 確認〕
※ 292 JNSA：インターンシップ募集 https://www.jnsa.org/internship/2019/index.html〔2020/6/30 確認〕
※ 293 東京工業大学：キャリアアップ MOT「サイバーセキュリティ経営戦略コース（2019 年度）」開講のお知らせ https://www.titech.ac.jp/company/news/2019/045588.html〔2020/6/30 確認〕
東京工業大学：カリキュラム概要 https://www.academy.titech.ac.jp/cumot/cy/schedule.html〔2020/6/30 確認〕
※ 294 IPA：企業の CISO 等やセキュリティ対策推進に関する実態調査 https://www.ipa.go.jp/security/fy2019/reports/2019DL_index.html〔2020/6/30 確認〕
※ 295 トレンドマイクロ社：法人組織におけるセキュリティ実態調査 2019 年版を発表 https://www.trendmicro.com/ja_jp/about/press-release/2019/pr-20191015-01.html〔2020/6/30 確認〕
※ 296 法人組織で講じられている対策の度合い、定期的な実施や見直しの徹底といった観点を基に、回答内容に応じてスコアリングすることでセキュリティ対策包括度を算出したもの。
※ 297 https://www.nri-secure.co.jp/news/2019/0718〔2020/6/30 確認〕
※ 298 https://www.ipa.go.jp/security/fy30/reports/ciso/index.html〔2020/6/30 確認〕
※ 299 IPA：「IT システム・サービスの業務委託契約書見直しに関する実態調査報告」について https://www.ipa.go.jp/security/fy2019/reports/scrm/index.html〔2020/6/30 確認〕
※ 300 一般社団法人日本サイバーセキュリティ・イノベーション委員会：サイバーセキュリティ情報公開のポイント～経営者の取組み姿勢が重要～ https://www.j-cic.com/pdf/report/Disclosure-Report.pdf〔2020/6/30 確認〕
※ 301 IPA：リスク分析シート https://www.ipa.go.jp/files/000055518.xlsx〔2020/6/30 確認〕
※ 302 IPA：中小企業の情報セキュリティ対策ガイドライン 第 3 版 https://www.ipa.go.jp/files/000055520.pdf〔2020/6/30 確認〕
※ 303 神奈川県：リース契約満了により返却したハードディスクの盗難及び再発防止策等について https://www.pref.kanagawa.jp/docs/fz7/cnt/p0273317.html〔2020/6/30 確認〕
※ 304 https://www.sonpo.or.jp/cyber-hoken/data/2019-01/pdf/cyber_report2019.pdf〔2020/6/30 確認〕
※ 305 IPA：中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊）- 成果報告書（全体版）- https://www.ipa.go.jp/files/000082722.pdf
※ 306 大阪商工会議所：サイバーセキュリティお助け隊の本格サービス化について https://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/200221cyber.pdf〔2020/6/30 確認〕
※ 307 https://www.ipa.go.jp/security/keihatsu/sme/management.html〔2020/6/30 確認〕
※ 308 IPA：「中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築に向けた実現可能性調査」報告書について https://www.ipa.go.jp/security/fy2019/reports/sme/smesecinfopf.html〔2020/6/30 確認〕
※ 309 https://www.gsx.co.jp/informationsecurity/mic_2019.html〔2020/6/30 確認〕
※ 310 IPA：SECURITY ACTION セキュリティ対策自己宣言 https://www.ipa.go.jp/security/security-action/index.html〔2020/6/30 確認〕
※ 311 https://www.cloudil.jp/contest〔2020/6/30 確認〕
※ 312 https://www.nisc.go.jp/security-site/files/blue_handbook-all.pdf〔2020/6/30 確認〕
※ 313 JNSA：MY CISO ハンドブック https://www.jnsa.org/result/2019/act_ciso/index.html〔2020/6/30 確認〕
※ 314 ISEN：平成 30 年度 学校・教育機関における個人情報漏えい事故の発生状況－調査報告書－第 2 版 https://school-security.jp/pdf/2018.pdf〔2020/6/30 確認〕
ISEN：平成 29 年度 学校・教育機関における個人情報漏えい事故の発生状況－調査報告書－第 2 版 https://school-security.jp/pdf/2017.pdf〔2020/6/30 確認〕
ISEN：平成 28 年度 学校・教育機関における個人情報漏えい事故の発生状況－調査報告書－第 2 版 https://school-security.jp/pdf/2016.pdf〔2020/6/30 確認〕
※ 315 2017 年度と 2016 年度のセキュリティインシデント数は「平成 30 年度 学校教育機関における個人情報漏えい事故の発生状況－調査報告書－第 2 版－」に記載されているものである。図 2-4-23 は「平成 29 年度 学校教育機関における個人情報漏えい事故の発生状況－調査報告書－第 2 版－」及び「平成 28 年度 学校教育機関における個人情報漏えい事故の発生状況－調査報告書－第 2 版－」を基に作成しているため、本文のセキュリティインシデント数と図の標本数は異なった数になっている。
※ 316 1 件の事故で複数の経路・媒体から漏えいした場合は、それぞれの経路・媒体に含まれていた個人情報漏えい人数を合算している。
※ 317 https://www.mext.go.jp/content/20200225-mxt_jogai02-100003157_001.pdf〔2020/6/30 確認〕
※ 318 富山大学：個人情報を含む USB メモリの紛失について https://www.u-toyama.ac.jp/news/2019/0830.html〔2020/6/30 確認〕
※ 319 ISEN: 県立高等学校、生徒 64 人の個人情報を保存した私物の USB メモリを紛失 https://school-security.jp/leak/2019/09/%e7%9c%8c%e7%ab%8b%e9%ab%98%e7%ad%89%e5%ad%a6%e6%a0%a1%e3%80%81%e7%94%9f%e5%be%9264%e4%ba%ba%e3%81%ae%e5%80%8b%e4%ba%ba%e6%83%85%e5%a0%b1%e3%82%92%e4%bf%9d%e5%ad%98%e3%81%97%e3%81%9f%e7%a7%81%e7%89%a9/〔2020/6/30 確認〕
静岡県：生徒の個人情報が保存されたUSBメモリーの紛失 http://www2.pref.shizuoka.jp/all/kisha19.nsf/c3db48f94231df2e4925714700049a4e/225635949fa6c55a49258472002e4f2c?OpenDocument〔2020/6/30 確認〕
※ 320 https://www.soumu.go.jp/main_content/000679388.pdf〔2020/6/30 確認〕
※ 321 https://www.soumu.go.jp/main_content/000610588.pdf〔2020/6/30 確認〕
※ 322 IPA：「2019 年度情報セキュリティに対する意識調査」報告書について https://www.ipa.go.jp/security/economics/ishikichousa2019.html〔2020/6/30 確認〕
※ 323 Microsoft 社：Windows セキュリティによる保護 https://support.microsoft.com/ja-jp/help/4013263/windows-10-stay-protected-with-windows-security〔2020/6/30 確認〕
※ 324 Microsoft 社：Windows Update の利用手順 – Windows 10 の場合 https://msrc-blog.microsoft.com/2018/10/18/wumusteps_win10/〔2020/6/30 確認〕
Apple Inc.：Mac の「セキュリティとプライバシー」の「一般」環境設定を変更する https://support.apple.com/ja-jp/guide/mac-help/mh11784/mac〔2020/6/30 確認〕
Apple Inc.：Mac の「ソフトウェア・アップデート」環境設定を変更する https://support.apple.com/ja-jp/guide/mac-help/mchla7037245/10.15/mac/10.15〔2020/6/30 確認〕
※ 325-1 トレンドマイクロ株式会社：スマホ決済を安全に利用するために確認したい 7 つのポイント https://www.is702.jp/special/3533/partner/200_k/〔2020/6/30 確認〕
※ 325-2 https://www.ipa.go.jp/files/000080784.pdf〔2020/6/30 確認〕
※ 325-3 https://www.ipa.go.jp/files/000080783.pdf〔2020/6/30 確認〕
※ 326 経済産業省：知的財産と標準化によるビジネス戦略 https://www.jpo.go.jp/news/shinchaku/event/seminer/text/document/h30_jitsumusya_txt/34_pp.pdf〔2020/6/30 確認〕
※ 327 経済産業省：今後の基準認証の在り方ールール形成を通じたグローバル市場の獲得に向けてー答申 https://www.meti.go.jp/shingikai/sankoshin/sangyo_gijutsu/kijun_ninsho/pdf/20171011001_1.pdf〔2020/6/30 確認〕
※ 328 https://www.kantei.go.jp/jp/singi/titeki2/2010keikaku.pdf〔2020/6/30 確認〕
※ 329 経済産業省：JIS 法改正 https://www.meti.go.jp/policy/economy/hyojun-kijun/jisho/jis.html〔2020/6/30 確認〕
※ 330 フォーラム標準の定義については、「JIS Z 8002:2006」の「JA.1」の「100.5」を参照。
※ 331 ISO：ISO/IEC JTC 1 https://www.iso.org/committee/45020.html〔2020/6/30 確認〕
※ 332 日本工業標準調査会：JISC について http://www.jisc.go.jp/jisc/index.html〔2020/6/30 確認〕
※ 333 ITU：SG17: Security https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx〔2020/6/30 確認〕
※ 334 IETF：The IETF Security Area https://trac.ietf.org/trac/sec/wiki〔2020/6/30 確認〕

※ 335 TCG：Trusted Computing Group へようこそ https://trustedcomputinggroup.org/work-groups/regional-forums/japan〔2020/6/30 確認〕
※ 336-1 https://www.jisc.go.jp/international/iso-prcs.html〔2020/6/30 確認〕
※ 336-2 一般社団法人情報処理学会情報規格調査会：第 1 種専門委員会 https://www.itscj.ipsj.or.jp/hyojunka/h_sn_member/h_sn_katsudo/2019arfiles/SC27_2019R.pdf〔2020/6/30 確認〕
※ 337 ISO/IEC 27701 は SC 27/WG 5 で検討、発行された規格である。
※ 338 引用規格：ある規格から引用されることによって引用元の規格の一部を構成する規格。本項では ISO 19011、ISO 20000 が引用規格である。
※ 339 国立研究開発法人新エネルギー・産業技術総合開発機構による委託事業「高効率・高速処理を可能とする AI チップ・次世代コンピューティングの技術開発事業／高度な IoT 社会を実現する横断的技術開発／複製不可能デバイスを活用した IoT ハードウェアセキュリティ基盤の研究開発」を指す。
※ 340 https://qforum.org/〔2020/7/20 確認〕
産官学連携し、量子技術の標準化の支援等を目的に設立された一般社団法人。
※ 341 「情報セキュリティ白書 2019」の「2.5.2（3）（a）ISO/IEC 15408、ISO/IEC 18045 の改訂」(p.127)を参照。
※ 342 総務省が 2019 年度に実施した内閣府事業 PRISM（官民研究開発投資拡大プログラム）の対象研究開発課題「設計・製造におけるチップの脆弱性検知手法の研究開発」を指す。
※ 343 IoT 推進コンソーシアム：IoT セキュリティガイドライン Ver1.0 https://www.soumu.go.jp/main_content/000428393.pdf〔2020/6/30 確認〕
※ 344 JISC：マネジメントシステム規格とは https://www.jisc.go.jp/mss/〔2020/6/30 確認〕
※ 345 https://trustedcomputinggroup.org/〔2020/6/30 確認〕
※ 346 TCG：TPM 2.0 Library Specification https://trustedcomputinggroup.org/tpm-library-specification/〔2020/6/30 確認〕
※ 347 TCG：Trusted Computing Group へようこそ https://trustedcomputinggroup.org/work-groups/regional-forums/japan/〔2020/6/30 確認〕
※ 348 TCG：第 11 回 TCG 日本支部公開ワークショップ https://trustedcomputinggroup.org/work-groups/regional-forums/japan/jrfworkshop/〔2020/6/30 確認〕
※ 349 TCG：Resources Archive https://trustedcomputinggroup.org/resources/?〔2020/6/30 確認〕
※ 350 TCG：Embedded Systems https://trustedcomputinggroup.org/work-groups/embedded-systems/〔2020/6/30 確認〕
※ 351 TCG：TCG TPM 2.0 Automotive Thin Profile For TPM Family 2.0; Level 0 https://trustedcomputinggroup.org/resource/tcg-tpm-2-0-library-profile-for-automotive-thin/〔2020/6/30 確認〕
※ 352 TCG:Protection Profile Automotive-Thin Specific TPM for TCG TPM 2.0 Automotive Thin Profile Family “2.0” Level 0 https://trustedcomputinggroup.org/resource/protection-profile-automotive-thin-specific-tpm-for-tcg-tpm-2-0-automotive-thin-profile-family-2-0-level-0/〔2020/6/30 確認〕
※ 353 https://trustedcomputinggroup.org/resource/tcg-guidance-for-secure-update-of-software-and-firmware-on-embedded-systems/〔2020/6/30 確認〕
※ 354 TCG：Symmetric Identity Based Device Attestation https://trustedcomputinggroup.org/resource/symmetric-identity-based-device-attestation/〔2020/6/30 確認〕
※ 355 https://trustedcomputinggroup.org/wp-content/uploads/TCG-Cyber-Resilient-Technologies-%E2%80%93-Rob-Spiger-Microsoft.pdf〔2020/6/30 確認〕
※ 356-1 https://fidoalliance.org/〔2020/6/30 確認〕
※ 356-2 https://www.commoncriteriaportal.org/〔2020/7/20 確認〕
※ 357 JISEC：認証プロテクションプロファイルリスト https://www.ipa.go.jp/security/jisec/certified_pps/pp_list.html〔2020/6/30 確認〕
※ 358 https://www.ipa.go.jp/security/jisec/certified_pps/c0553/c0553_it7627.html〔2020/6/30 確認〕
※ 359 https://www.ipa.go.jp/security/jisec/certified_pps/c0500/c0500_it5575.html〔2020/6/30 確認〕
※ 360 https://www.ipa.go.jp/security/jisec/certified_pps/c0499/c0499_it5574.html〔2020/6/30 確認〕
※ 361 https://www.ipa.go.jp/security/jisec/certified_pps/c0431/c0431_it4485.html〔2020/6/30 確認〕
※ 362 JISEC：ID&Trust IDentity-J with SAC (PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G v1.0.7052 https://www.ipa.go.jp/security/jisec/hardware/hw_certified_products/c0648/c0648_it8678.html〔2020/6/30 確認〕
JISEC：ID&Trust IDentity-J with SAC (BAC+PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G v1.0.7052 https://www.ipa.go.jp/security/jisec/hardware/hw_certified_products/c0649/c0649_it8679.html〔2020/6/30 確認〕
※ 363 独立行政法人国立印刷局の入札情報公開システム（https://www.npb.go.jp/ja/guide/finance/nyusatu/rakusatu.html〔2020/6/30 確認〕）で 2019 年度の「旅券用ICシート（SAC 対応）B」の入札・見積結果情報を確認した。
※ 364 JISEC：ネットワークカメラシステム チェックリスト https://www.ipa.go.jp/security/jisec/choutatsu/nwcs/index.html〔2020/6/30 確認〕
※ 365 JISEC：入退管理システムチェックリスト https://www.ipa.go.jp/security/jisec/choutatsu/ecs/index.html〔2020/6/30 確認〕
※ 366 https://www.meti.go.jp/press/2019/06/20190617005/20190617005_01.pdf〔2020/6/30 確認〕
※ 367 IPA：「特定用途機器 PP を用いた認証の実効性調査」に係る企画競争 https://www.ipa.go.jp/about/kobo/kobo20191211.html〔2020/6/30 確認〕
※ 368 IPA：本制度に関連する ISO/IEC 規格 https://www.ipa.go.jp/security/jcmvp/topics.html〔2020/6/30 確認〕
※ 369 NITE：ASNITE 0002 Testing 一般社団法人 IT セキュリティセンター 評価部の認定範囲 https://www.nite.go.jp/data/000000804.pdf〔2020/6/30 確認〕
※ 370 NIST：FIPS 140-3 Security Requirements for Cryptographic Modules https://csrc.nist.gov/publications/detail/fips/140/3/final〔2020/6/30 確認〕
※ 371 NIST：FIPS 140-3 Development https://csrc.nist.gov/projects/fips-140-3-development〔2020/6/30 確認〕
※ 372 NIST：SP 800-140(Draft) FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759 https://csrc.nist.gov/publications/detail/sp/800-140/archive/2019-10-09〔2020/6/30 確認〕
NIST：SP 800-140A(Draft) CMVP Documentation Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 https://csrc.nist.gov/publications/detail/sp/800-140a/archive/2019-10-09〔2020/6/30 確認〕
NIST：SP 800-140B(Draft) CMVP Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B https://csrc.nist.gov/publications/detail/sp/800-140b/archive/2019-10-09〔2020/6/30 確認〕
NIST：SP 800-140C(Draft) CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759 https://csrc.nist.gov/publications/detail/sp/800-140c/archive/2019-10-09〔2020/6/30 確認〕
NIST：SP 800-140D(Draft) CMVP Approved Sensitive Parameter Generation and Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759:2014(E) https://csrc.nist.gov/publications/detail/sp/800-140d/archive/2019-10-09〔2020/6/30 確認〕
NIST：SP 800-140E(Draft) CMVP Approved Authentication Mechanisms: CMVP Validation Authority Requirements for ISO/IEC 19790:2012 Annex E and ISO/IEC 24579:2017 https://csrc.nist.gov/publications/detail/sp/800-140e/archive/2019-10-09〔2020/6/30 確認〕
NIST：SP 800-140F(Draft) CMVP Approved Non-Invasive Attack Mitigation Test Metrics: CMVP Validation Authority Updates to ISO/IEC 24759:2014(E) https://csrc.nist.gov/publications/detail/sp/800-140f/archive/2019-10-09〔2020/6/30 確認〕
※ 373 NIST：SP 800-140 FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759 https://csrc.nist.gov/publications/detail/sp/800-140/final〔2020/6/30 確認〕
NIST：SP 800-140A CMVP Documentation Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 https://csrc.nist.gov/publications/detail/sp/800-140a/final〔2020/6/30 確認〕
NIST：SP 800-140B CMVP Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B https://csrc.nist.gov/publications/detail/sp/800-140b/final〔2020/6/30 確認〕
NIST：SP 800-140C CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759 https://csrc.nist.gov/publications/detail/sp/800-140c/final〔2020/6/30 確認〕
NIST：SP 800-140D CMVP Approved Sensitive Parameter Generation and Establishment Methods: CMVP Validation

Authority Updates to ISO/IEC 24759 https://csrc.nist.gov/publications/detail/sp/800-140d/final〔2020/6/30 確認〕
NIST：CMVP Approved Authentication Mechanisms: CMVP Validation Authority Requirements for ISO/IEC 19790 Annex E and ISO/IEC 24579 Section 6.17 https://csrc.nist.gov/publications/detail/sp/800-140e/final〔2020/6/30 確認〕
NIST：SP 800-140F CMVP Approved Non-Invasive Attack Mitigation Test Metrics: CMVP Validation Authority Updates to ISO/IEC 24759 https://csrc.nist.gov/publications/detail/sp/800-140f/final〔2020/6/30 確認〕
※ 374 https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline_20190225.pdf〔2020/6/30 確認〕
※ 375 https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline_honninkakunin_20190225.pdf〔2020/6/30 確認〕
※ 376 日本産業規格 JIS X 19790「セキュリティ要求事項―暗号モジュールのセキュリティ要求事項」においては、用語として「タンパー」を用いている。
※ 377 耐タンパ性：モジュールがあらかじめ準備したインタフェース以外のアクセス手段を用いて、許可なくモジュールの内部情報を読み取ろうとする攻撃に対する耐性。
※ 378 IPA/JISEC：「ハードコピーデバイスのプロテクションプロファイル」適合の申請案件についてのガイドライン 第 1.6 版 https://www.ipa.go.jp/security/jisec/application/documents/guidelineforHCD-PP_1.6.pdf〔2020/6/30 確認〕
※ 379 https://www.ipa.go.jp/security/jisec/certified_pps/c0553/c0553_pp.pdf〔2020/6/30 確認〕
※ 380 IPA/JISEC：認証製品リスト https://www.ipa.go.jp/security/jisec/certified_products/cert_listv31.html〔2020/6/30 確認〕
※ 381 IPA/JCMVP：暗号モジュール試験及び認証制度（JCMVP）：承認されたセキュリティ機能 https://www.ipa.go.jp/security/jcmvp/algorithm.html〔2020/6/30 確認〕
※ 382 e-Gov：電子政府の総合窓口 電子署名及び認証業務に関する法律施行規則の改正案等に対する意見募集 https://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=145209452&Mode=0〔2020/6/30 確認〕
e-Gov：電子署名及び認証業務に関する法律施行規則の一部を改正する省令 https://search.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000197437〔2020/6/30 確認〕
e-Gov：電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針 https://search.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000197438〔2020/6/30 確認〕
※ 383 e-Gov：電子署名及び認証業務に関する法律施行規則 https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=413M60000418002〔2020/6/30 確認〕
※ 384 IETF：Deprecating TLSv1.0 and TLSv1.1 draft-ietf-tls-oldversions-deprecate-06 https://tools.ietf.org/id/draft-ietf-tls-oldversions-deprecate-06.html〔2020/6/30 確認〕
※ 385 Qualys SSL Labs：SSL Pulse https://www.ssllabs.com/ssl-pulse/〔2020/6/30 確認〕
※ 386 Microsoft Security Response Center https://msrc-blog.microsoft.com/2018/10/16/tlsdeprecation/〔2020/6/30 確認〕
※ 387 NIST：NIST Special Publication 800-52 Revision 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf〔2020/6/30 確認〕
※ 388 Federal Office for Information Security：BSI TR-02102-2：“Technical Guideline TR-02102-2Cryptographic Mechanisms: Recommendations and Key Lengths, Part 2 – Use of Transport Layer Security (TLS)” https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-2.pdf〔2020/6/30 確認〕
※ 389 Agence nationale de la sécurité des systèmes d’information：Security Recommendations for TLS https://www.ssi.gouv.fr/uploads/2017/02/security-recommendations-for-tls_v1.1.pdf〔2020/6/30 確認〕
※ 390 NIST：NIST Special Publication 800-56C Revision 1 Recommendation for Key-Derivation Methods in Key-Establishment Schemes https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr1.pdf〔2020/6/30 確認〕
Draft NIST Special Publication SP 800-56C Revision 2 Recommendation for Key-Derivation Methods in Key-Establishment Schemes https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2-draft.pdf〔2020/6/30 確認〕
※ 391 NIST：NIST Special Publication 800-108 Recommendation for Key Derivation Using Pseudorandom Functions https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf〔2020/6/30 確認〕
※ 392 https://www.jnsa.org/result/surv_mrk/2020/〔2020/6/30 確認〕
※ 393 「2019 年度 国内情報セキュリティ市場調査報告書」では、変更後の市場区分定義に沿って 2017 ～ 2020 年度の市場規模を新たに集計している。また、JNSA の「2019 年度 国内情報セキュリティ市場調査報告書」の Web ページ（https://www.jnsa.org/result/surv_mrk/2020/〔2020/6/30 確認〕）では、従来の市場区分の集計結果も公表している。
※ 394 公益社団法人日本経済研究センター：短期経済予測（第 181 回再改訂 /2020 年 1-3 月期～ 2022 年 1-3 月期）年内に自粛解除でも、20 年度マイナス 8%成長―新興国の感染拡大に懸念― https://www.jcer.or.jp/economic-forecast/20200424.html〔2020/7/10 確認〕
※ 395 経済産業省：Connected Industries https://www.meti.go.jp/policy/mono_info_service/connected_industries/index.html〔2020/7/1 確認〕
※ 396 IPA：「安全なデータ利活用に向けた準備状況及び課題認識に関する調査」報告書について https://www.ipa.go.jp/security/fy30/reports/ts_research/index.html〔2020/7/1 確認〕
※ 397 https://www.ipa.go.jp/files/000072809.pdf〔2020/7/1 確認〕
※ 398 IPA：「企業におけるデータ利活用・保護の戦略立案のための手引書（案）の作成」調査報告書 https://www.ipa.go.jp/security/fy2019/reports/ts_research/20200327.html〔2020/7/1 確認〕
※ 399 PoC（Proof of Concept：概念実証）：新しい概念や理論、原理、アイディアの実証を目的とした検証やデモンストレーション。
※ 400 研究の例としては、以下がある。
Batini, Carlo, and Monica Scannapieco. “Data Quality: Concepts, Methodologies and Techniques” Springer (2006)
Rajesh Jugulum, “Competing with High Quality Data: Concepts, Tools, and Techniques for Building a Successful Approach to Data Quality” Wiley (2014)
Aiken, Peter and Billings, “Monetizing Data Management” Technics Publishing, LLC (2014)
Aiken, Peter and Harbour, “Data Strategy and the Enterprise Data Executive” Technics Publishing, LLC (2017)
※ 401 G. Leurent, T. Peyrin, From Collision to Chosen-Prefix Collisions Application to Full SHA-1, EUROCRYPT 2019, LNCS 11478, pp. 527-555
※ 402 Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger：MD5 considered harmful today https://www.win.tue.nl/hashclash/rogue-ca/〔2020/6/30 確認〕
※ 403 NIST：The 2nd Round of the NIST PQC Standardization Process-Opening Remarks at PQC 2019: https://csrc.nist.gov/CSRC/media/Presentations/the-2nd-round-of-the-nist-pqc-standardization-proc/images-media/moody-opening-remarks.pdf〔2020/6/30 確認〕
※ 404 NIST：Lightweight Cryptography https://csrc.nist.gov/projects/lightweight-cryptography〔2020/6/30 確認〕
※ 405 A. C. Aldaya, C. P. García, L. M. A. Tapia, B. B. Brumley：Cache-Timing Attacks on RSA Key Generation https://tches.iacr.org/index.php/TCHES/article/view/8350〔2020/6/30 確認〕
※ 406 K. Ryan：Return of the Hidden Number Problem https://tches.iacr.org/index.php/TCHES/article/view/7337〔2020/6/30 確認〕
※ 407 J. Rodriguez, A. Baldomero, V. Montilla, J. Mujal：LLFI: Lateral Laser Fault Injection Attack https://fdtc.deib.polimi.it/FDTC19/shared/FDTC%202019%20-%20session%203.1.pdf〔2020/6/30 確認〕
※ 408 個人情報保護委員会：個人情報保護法 いわゆる3年ごと見直し制度改正大綱 https://www.ppc.go.jp/files/pdf/200110_seidokaiseitaiko.pdf〔2020/6/30 確認〕
※ 409 個人情報保護委員会：個人情報保護法 いわゆる3年ごと見直し制度改正大綱（骨子） https://www.ppc.go.jp/files/pdf/191129_houdou_koshi.pdf〔2020/6/30 確認〕
※ 410 個人情報保護委員会：「個人情報の保護に関する法律等の一部を改正する法律案」の閣議決定について https://www.ppc.go.jp/news/press/2019/20200310/〔2020/6/30 確認〕