情報セキュリティ白書

Information Security White Paper

2022

ゆらぐ常識、強まる脅威：想定外にたちむかえ

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

「情報セキュリティ白書2022」の刊行にあたって

2021 年も新型コロナウイルス変異株による感染拡大が継続しました。米欧では対策緩和の方針がとられましたが、ワクチン接種やそれに基づく移動許可等の可否について多くの議論を呼びました。日本は、厳しい規制の中で東京 2020 オリンピック・パラリンピック競技大会を無観客で開催、成功させましたが、その後も規制はゆるまず、テレワーク等の新しい業務形態が定着していきました。

この間、重要な組織やインフラを狙った攻撃も続きました。特に目立ったのがランサムウェア被害です。米国では 2021 年 5 月にエネルギー事業者が攻撃を受け、米国東部の石油供給が一時ストップしました。国内では 7 月に食品事業者がバックアップデータまで暗号化され、事業再開が遅れました。10 月には病院が攻撃を受けて診療に支障が出ました。2022 年 2 月には製造事業者が攻撃を受け、納入先の事業者の生産に影響が出ました。昨年の巻頭言で申し上げたとおり、こうした攻撃は巧妙化しており、システムの脆弱性やサプライチェーンを介して侵入し、情報を盗んで二重の脅迫を行う等、深刻な脅威となっています。一方脆弱性については、テレワークで活用が進んだ VPN 等の対策がまだ十分でなく、12 月には広範囲の Web システムに影響を及ぼす Log4j の脆弱性が報告されました。こうした懸念もあり、2022 年の 10 大脅威では修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）が初めてランクインしました。テレワークや DX 推進等によって生活や業務の各場面でデジタル化が進む中、安全で信頼できると思っていた機器やシステムに脆弱性が見つかり、ゼロデイ攻撃され、生活の一部が突然立ち行かなくなるかもしれない、そういう時代を私達は迎えつつあります。

更に 2021 年後半以降のウクライナ危機は、「まさかこのような事態が起こるとは」を私達に痛切に感じさせました。ロシアとウクライナの紛争は、情報セキュリティの視点からは、三つの点が特に注目されます。一つ目は、紛争が武力とサイバー空間上の攻防が組み合わされたハイブリッドな戦いであること。二つ目は、ネット等で配信される紛争関連情報が急増し、その信頼性の見極めが難しいこと。最後は、サイバー空間の攻防において、民間組織や個人が簡単に当事者になってしまうこと。私達は国家間の分断や物的な流通分断のリスクに加え、虚偽の情報に誘導される、サイバー攻撃の対象になる、等のリスクに直面することとなりました。

半年前まで想定できなかったこうした状況に私達はどう対応すればよいでしょうか。申し上げてきたことの繰り返しになりますが、リスク対応の基本が大切であると思います。情報セキュリティに関しては、機器やシステムの脆弱性をなくすこと、このサービスが止まったときにどうするか、の想像力を持つことは大変重要です。また虚偽の情報に惑わされないために、様々なソースの情報を参照し、視野を広く持つことも大切になるでしょう。本白書が、多くの方々に広く利用され、新しい生活や働き方のリスクに対する意識を高め、備えを実践するための一助となることを祈念します。

2022年7月

独立行政法人情報処理推進機構（IPA）

理事長　富田達夫

目次

コラム

情報セキュリティ白書

序章

2021年度の情報セキュリティの概況

2020年から世界中で流行した新型コロナウイルス感染症については、日本・米国・欧州ではワクチン接種が進み、感染者の増減はあるものの、経済活動は徐々に以前の状態に戻りつつある。国内では、感染拡大防止対策として実施されたテレワークやオンライン会議等が新しい働き方として定着しつつある。こうした業務の見直し、デジタル化は、組織におけるDX（デジタルトランスフォーメーション）の推進を後押しする形となっている。

2021年はランサムウェアの手口が巧妙化して被害が拡大し、サプライチェーンに関連したインシデントや脆弱性を狙った攻撃も引き続き発生した。警察庁によれば、2021年下期の被害報告件数は2020年下期の4倍となった。また、2021年7月の製粉会社、10月の病院の事案では、バックアップデータも暗号化されたために早期復旧が困難であった。データ保管方法の見直しや復旧計画の重要性が再確認された。

攻撃経路として、海外拠点、海外子会社、取引先が攻撃され、被害を受ける事案も多くみられた。2021年10月の医薬品メーカの情報漏えい事案は海外拠点が攻撃対象であった。2022年2月の自動車部品会社へのランサムウェア攻撃では、部品供給先の自動車メーカの工場が1日停止した。サプライチェーン全体のセキュリティ強化が求められている。情報漏えい事案としては、マッチングアプリや大手製菓製造会社への不正アクセスにより合わせて300万件以上の大量の個人情報が流出した。

ソフトウェアの脆弱性を悪用した攻撃も継続して報告された。2021年に報告された脆弱性としては、VPN製品、Microsoft Exchange Serverの脆弱性、多くの製品やソフトウェアで使用されるJavaベースのロギングライブラリApache Log4jの脆弱性等、影響範囲が広く、攻撃により大きな被害が予想されるものが目立った。このほか、2021年初頭に欧州司法機関の一斉テイクダウンにより沈静化したウイルス「Emotet（エモテット）」の感染が再拡大し、2022年に入り注意喚起された。

セキュリティ政策面では、国内では2021年9月に「サイバーセキュリティ戦略」が閣議決定された。同戦略では「DX with Cybersecurity」として、デジタル社会の進展と併せてサイバーセキュリティ確保の取り組み推進が重要とされた。また同月にデジタル庁が発足、政府のIT基盤とセキュリティの整備を統括することとなった。サプライチェーンセキュリティについては、経済産業省がサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）等を継続的に推進した。

米国では、重要インフラやライフラインに関わる制御システムへの攻撃が相次ぎ、水道や浄水場等の制御システムへの攻撃、石油供給事業者へのランサムウェア攻撃が報告された。米国Biden政権は重要インフラのセキュリティ対策強化を打ち出し、これを受けた米国国立標準技術研究所（NIST）は、重要ソフトウェア調達におけるセキュリティガイドライン策定、消費者向けIoT製品のラベリング制度の検討等を実施した。NISTはまたサプライチェーンセキュリティに関する官民連携イニシアティブ（NIICS）の設置、サプライチェーンリスク管理の標準ガイド（NIST SP800-161）の改訂を進めた。今後の動向が注目される。

欧州では、欧州ネットワーク・情報セキュリティ機関（ENISA）が主導し、重要インフラに関するサイバーセキュリティ準拠法の改訂案（NIS2 Directive）審議、あるいは域内の製品・サービスのセキュリティを担保するサイバーセキュリティ認証スキーム（EUCC scheme V1.1.1）の構築等を中心としてセキュリティ政策を推進した。また欧州委員会は2021年4月、AI利用リスクへの対処に関する法案を公表した。同法は罰則を伴う初のAI利用規格として注目される。

このように、各国とも重要インフラやサプライチェーンへのセキュリティ対策強化を進めてきたが、2021年後半以降はウクライナ情勢が悪化、2022年2月のロシアのウクライナ侵攻により、世界は新たな緊張に直面している。この紛争は、武力とサイバー攻撃・防御あるいはサイバー空間での情報戦が組み合わさったハイブリッドな戦いが特徴であり、サイバー空間上では政府に加えて民間組織・個人が参画する、というまったく新たな状況が生まれている。政府の安全保障政策・サイバーセキュリティ政策は言うまでもなく、企業や個人がこのリスクへの対応、例えば、親ロシア系ハッカーの攻撃への備え、紛争に関連する情報の信頼度の見極め等をどうするべきか、が問われている。

2021 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
2021 年　4 月	● VPN 製品「Pulse Connect Secure」ゼロデイ攻撃発生（1.2.5） ● ファーストフードチェーン店でランサムウェア被害（1.2.8） ● マッチングアプリが不正アクセスを受け約 171 万件の個人情報流出（1.2.8、3.3.2）	■ 経済産業省「サイバーセキュリティ体制構築・人材確保の手引き」（第 1.1 版）改訂（2.1.2、2.3.1） ■ 欧州委員会「Artificial Intelligence Act」（AI 法）提出（3.4.2）
5 月	● 米石油供給事業者へのサイバー攻撃、身代金 500 万ドル相当を支払いか（3.4.1）	■ サプライチェーンセキュリティ強化を目指した米国大統領令 EO 14028 発表（3.4.1） ■ EU 域内のセキュリティ認証スキーム（EUCC scheme V1.1.1）公開（3.4.2）
6 月	● 無線通信機器メーカ、2017 年に不正アクセス確認から 3 年以上報告せず（1.2.8） ● 電子部品メーカの再委託先社員が取引先情報約 3 万件、従業員関連情報約 4 万件を不正持ち出し（1.2.8）	■ 総務省「スマートシティセキュリティガイドライン（第 2.0 版）」公開（2.1.3）
7 月	● 大手製粉会社がサイバー攻撃を受けシステム障害（1.2.2） ● IT 管理ツールをランサムウェア攻撃に悪用（1.1.1）	■ NISC「政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）」公開（2.1.1） ■ 総務省「ICT サイバーセキュリティ総合対策 2021」公開（2.1.3）
8 月	● ProxyShell の脆弱性を公表(1.2.5)	■ IPA「サイバーセキュリティ経営可視化ツール」公開（2.1.1） ■ NIST が「サプライチェーンセキュリティに関する官民を推進する国家イニシアティブ」を設置（3.4.1）
9 月		■ デジタル庁発足（2.1.1） ■ NISC「サイバーセキュリティ戦略」「サイバーセキュリティ 2021」決定（2.1.1）
10 月	● 徳島の町立病院でランサムウェアの被害発生（1.2.2） ● 医薬品メーカの国内外の拠点に不正アクセス（1.2.8）	■ NISC、第 14 回「日・ASEAN サイバーセキュリティ政策会議」開催（2.2.1） ■ Ransom Disclosure Act 米国議会に提出（3.4.1）
11 月	● 大手眼鏡販売チェーン持株会社で約 1 億円のビジネスメール詐欺被害（1.2.3） ● Emotet（エモテット）の攻撃活動再開（1.2.6）	■ NISC「クラウドを利用したシステム運用に関するガイダンス」公開（2.1.1、3.3.4） ■ CISA が既知の脆弱性悪用に関する重大リスクの削減に関する運用指令を公開（3.4.1）
12 月	● ロギングライブラリ Apache Log4j の任意のコード実行の脆弱性に関する注意喚起（1.1.1、1.3.2） ● スマホ決済のキャンペーン関係識別情報 13 万 3,484 件が GitHub 上で閲覧可能になっていたと発表（1.2.8）	■ 米 Biden 大統領が国防授権法に署名、アジア大平洋地域やウクライナ・NATO への関与を強化（3.4.1）
2022 年　1 月	● 決済サービス事業者不正アクセスによる情報漏えい公表（1.2.8）	
2 月	● ロシアがウクライナに侵攻（3.4.1） ● CISA、FBI がウクライナで使用された破壊的ウイルスに関し注意喚起（3.4.1）	■ NIST「ソフトウェアサプライチェーンセキュリティガイダンス」、NIST SP800-218 Ver.1.1 公開（3.4.1）
3 月	● 自動車部品会社がサイバー攻撃を受け、自動車メーカが国内工場停止（1.2.2） ● 大手製菓製造会社への不正アクセス（1.2.8） ● 複数の自治体で利用するクラウドが踏み台となり約 91 万件の迷惑メール発信（3.3.2）	■ CISA がウクライナ関連攻撃対策サイト「SHIELDS UP」を公開（3.4.1） ■ 総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」改訂版等公開（2.1.3）

※ 2021年度の主な情報セキュリティインシデント・事件、及び主な情報セキュリティ政策・イベントを示している。標的型攻撃、ランサムウェア被害、ビジネスメール詐欺、DDoS 攻撃、Web 改ざん、フィッシング等の攻撃や被害は通年で発生している。表中の数字は本白書中に掲載している項目番号である。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

2021 年度も、新型コロナウイルス感染症の蔓延が続いたが、日本･米国･欧州ではワクチン接種が進み、徐々に経済活動は戻りつつある。一方、2022 年 2 月にはロシアによるウクライナ侵攻が発生し、ウクライナ支援国家に対するサイバー攻撃や安全保障面の懸念が高まっている。

国内ではテレワークやオンライン会議が定着し、業務のデジタル化が進んでいる。政府ではデジタル庁が発足し、政府の IT 基盤整備とセキュリティを統括することとなった。

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、各種認証制度、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政策の状況を述べる。

2.1.1 政府全体の政策動向

政府全体のサイバーセキュリティに関する政策は、3 年ごとに改訂されている「サイバーセキュリティ戦略」に基づいている。更に、具体的な施策については各年度の年次計画として策定される。本項では、2021 年 9 月に改訂･閣議決定された「サイバーセキュリティ戦略※1」（以下、戦略）で挙げられている四つの施策項目の概要と、各施策項目に基づいて策定された 2021 年度の年次計画「サイバーセキュリティ 2021※2」（以下、年次計画）の主な内容について述べる。

(1) 経済社会の活力の向上及び持続的発展～DX with Cybersecurity の推進～

戦略では、経済社会のデジタル化や DX 推進の動きに併せてサイバーセキュリティ確保に向けた取り組みを同時に推進すること（DX with Cybersecurity）が重要であるとしている。

(a) 経営層の意識改革

企業にとって、DX（デジタルトランスフォーメーション）の必要性が高まり、付加価値の高いデジタルサービスを生み出せることが重要な競争力になり、サイバーセキュリティ対策を前提とした DX の推進が経営者に求められている。

年次計画では、「サイバーセキュリティ経営ガイドライン」「グループ・ガバナンス・システムに関する実務指針」等の普及・啓発、「取締役会の実効性評価」におけるサイバーセキュリティの重要性周知等によるサイバーセキュリティ経営の普及・実践を促進するとしている。

このうちサイバーセキュリティ経営ガイドラインの実践について、経済産業省は IPA を通じ、2021 年 8 月に「サイバーセキュリティ経営可視化ツール」を公開した※3。また、2022 年 3 月に「サイバーセキュリティ 経営ガイドライン Ver2.0 実践のためのプラクティス集 第 3 版※4」を公開した（「2.4.1 (2) セキュリティリスクマネジメント」参照）。

また、IT やセキュリティの専門知識や業務経験を持たない経営層が、セキュリティ専門家と協働するための「プラス・セキュリティ」知識を習得できる環境整備を推進するため、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、特に経営層や DX を推進する部課長向けのプログラムの普及の参考となるカリキュラムを作成・公開した※5（「2.3.1 (3) 人材育成の取り組み」参照）。

(b) 地域・中小企業における DX with Cybersecurity の推進

地域・中小企業、あるいはこれまで IT 化が進んでいなかった業種・業態の企業でも、デジタル化や DX 推進への対応が求められ、サイバーセキュリティ対策の必

要性も増している。ところが、こうした企業ではサイバーセキュリティの知見や人材等の不足、予算の確保が困難等の課題がある。

これに対する年次計画の取り組みとして、経済産業省はIPAを通じ、中小企業向けにサイバーセキュリティ対策を安価に提供する民間のサービスのうち一定の基準を満たすものに「サイバーセキュリティお助け隊サービス」の商標使用権を付与する制度を構築し（「2.4.2（3）(a) サイバーセキュリティお助け隊サービス制度」参照）、同サービスの普及を推進した。この制度には、2022年4月1日時点で12件のサービスが登録された※6。

(c) 新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

デジタルサービスの連携が進み、サプライチェーンが複雑化してサイバー攻撃のリスクポイントが増大することから、サプライチェーン全体を見通したリスク管理の重要性が増している。また、サイバーセキュリティ対策の推進のためには、セキュリティ製品・サービスの信頼性確保も課題である。

サイバーフィジカルシステムのサプライチェーンセキュリティ実装を目的に、内閣府は、戦略的イノベーション創造プログラム（SIP）第2期「IoT社会に対応したサイバー・フィジカル・セキュリティ」を実施し、「サイバー・フィジカル・セキュリティ対策基盤」の研究開発を推進している。2021年10月22日、「IoT社会に対応したサイバー・フィジカル・セキュリティONLINEシンポジウム2021※7」を開催し、成果を公開するとともに「Society 5.0におけるサプライチェーンの信頼性を築くデジタルトラスト」等のプレゼンテーションを行った。

セキュリティ製品・サービスの信頼性確保について、経済産業省は、「情報セキュリティサービス審査登録制度」に基づき、同制度のセキュリティサービス基準を満たすサービスリストを、IPAを通じて公開している。2021年度は、サービスリストの利用促進のため、「情報セキュリティサービス普及促進に関する検討会※8」を設置し、3回にわたり検討会を開催した（「2.1.2（4）情報セキュリティサービス審査登録制度」参照）。

(d) 誰も取り残さないデジタル／セキュリティリテラシーの向上と定着

社会のデジタル化に伴って、すべての国民がサイバーセキュリティ上の脅威から自らを守れるようにする必要がある。従って、サイバーセキュリティに関する基本的な知識・能力を習得できる環境の整備が重要となり、官民による普及啓発活動が求められる。

NISCは、サイバーセキュリティの普及啓発や人材育成に関する公的機関等の施策・取り組みを紹介することを目的として、2021年9月に、「みんなで使おうサイバーセキュリティ・ポータルサイト※9」の正式運用を開始した。このサイトは、ニーズ事例から適切な施策を選択できる「目的から選ぶ!施策一覧」と、利用者属性から適切な施策を選択できる「自身の年齢層や所属から選ぶ!施策一覧」とで構成されている。

総務省は文部科学省と協力し、青少年やその保護者のインターネットリテラシー向上を図るため、「e-ネットキャラバン」（「2.1.3（5）(c) 人材育成・普及啓発の推進」参照）等の青少年や保護者等に向けた啓発講座等の実施や、情報教育の中核的な役割を担う教員等を対象とした研修を実施し、サイバーセキュリティを含む情報モラルに関する指導力の向上を図る取り組みを行っている。2021年度は、「インターネットトラブル事例集（2021年度版）※10」を公開し、インターネットトラブルの実例と予防法を紹介した。

なお文部科学省は、学校における「一人一台端末」の実現を目指すGIGAスクール構想を推進している。同構想におけるセキュリティリテラシーの向上については「2.5.1（2）GIGAスクール構想」を参照されたい。

(2) 国民が安全で安心して暮らせるデジタル社会の実現

戦略では、政府は安心して暮らせるデジタル社会を実現するために、自助・共助による自律的なリスクマネジメントの環境づくりに努めるとしている。また公助としては、国民の安全・安心に関わる経済社会基盤について包括的なサイバー防御に取り組み、かつ先進的な取り組みの導入を率先するとしている。

(a) 国民・社会を守るためのサイバーセキュリティ環境の提供

戦略では、サプライチェーンの複雑化を踏まえ、サイバー空間のリスクの可視化、新しい技術・サービスのセキュリティ確保に取り組むとしている。このうち後者について、NISCは2021年11月、クラウドサービスの安全な運用やインシデント発生時の円滑な対応に重点を置いた利用者向けのガイダンスとして「クラウドを利用したシステム運用に関するガイダンス」を公表した※11。

また、内閣官房、デジタル庁、総務省及び経済産業

省は、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスの「政府情報システムのためのセキュリティ評価制度（ISMAP）」への追加登録や更新審査を行った。ISMAP クラウドサービスリスト※12 には、2022 年 6 月 1 日現在で 34 件のサービスが登録されている（「2.7.3 政府情報システムのためのセキュリティ評価制度（ISMAP）」参照）。

(b) デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

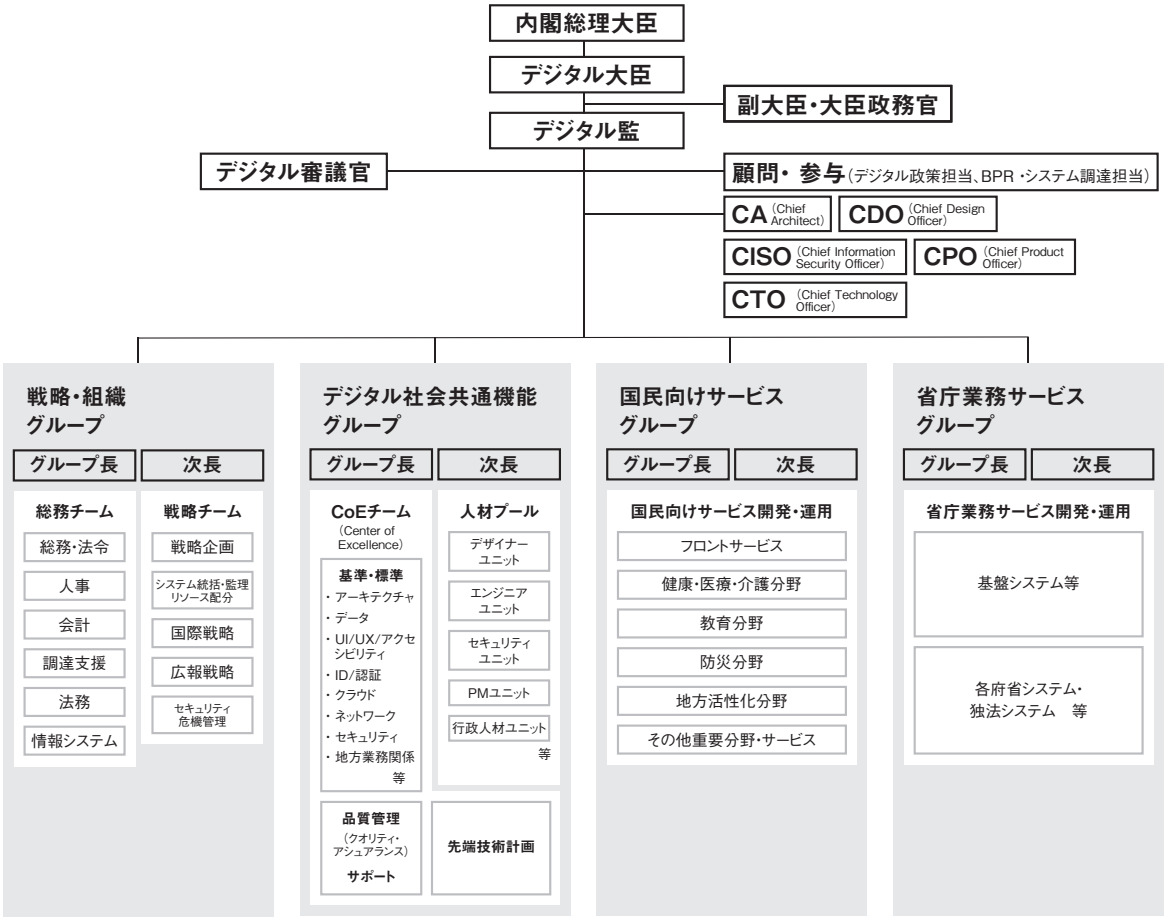
戦略では、国、地方公共団体や公的機関の情報システムの整備・管理の方針をデジタル庁が策定する際に、サイバーセキュリティの基本方針も盛り込み、実装を推進するとしている。デジタル庁において、サイバーセキュリティはデジタル社会共通機能グループの CoE チームが統括する（図 2-1-1）。

また戦略では、マイナンバーカードによる本人確認を前提として、マイナポータルを活用した官民の認証連携やデータ連携を推進する等としている。これを受けてデジタル庁は、「マイナンバー制度及び国と地方のデジタル基盤抜本改善ワーキンググループ」を設置※14して、2021 年度に 3 回開催した。

(c) 経済社会基盤を支える各主体における取り組み

戦略では、各政府機関は、統一的な基準に基づくサイバーセキュリティ対策を施すこととしている。NISC は 2021 年 7 月に、「政府機関等のサイバーセキュリティ対策のための統一基準（令和 3 年度版）※15」及び「政府機関等の対策基準策定のためのガイドライン（令和 3 年度版）※16」を公開した。これらにより、クラウドサービスの利用拡大を見据えた記載や、境界型防御だけでは十分なセキュリティを担保できなくなっている状況を踏まえて、ゼロトラストアーキテクチャの導入を検討すること等が追加された。

また戦略では、政府が共通で利用するシステムはデジタル庁が各府省庁と連携して整備・運用し、サイバーセキュリティも含めて安定的・継続的な稼働を確保するとしており、そのためのクラウドサービス（「ガバメントクラウド」）



■図 2-1-1　デジタル庁の組織体制（2021 年 9 月 1 日現在）
（出典）デジタル庁「組織情報※13」

を2021年度に整備し、翌年度以降は、原則として各府省庁等が活用を検討するとした※17。デジタル庁はこれを受けて、クラウドサービス移行に係る課題の検証を行う先行事業を2021年度から開始するために、協力する自治体を公募した。2021年10月、基幹業務システムは神戸市、倉敷市等8市町村が、セキュリティシステムは青森県、岩手県等7県258市町村が参加するグループ、及び鳥取県、岡山県の46市町村が参加するグループが採択された※18。

このほか、経済・社会を支える重要インフラ等について、政府は各主体の取り組みを促し、支援を行うとしている。これに基づき、NISCは「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」の改定に先立ってパブリックコメントを募集する目的で、その改訂案※19を2022年1月28日に公開した。

更にNISCは、「多様な主体によるシームレスな情報共有・連携と東京大会に向けた取り組みから得られた知見等の活用」に取り組むとして、2021年12月に「東京オリンピック・パラリンピック競技大会等の大規模国際イベントにおけるサイバーセキュリティの確保に向けた取組の今後の活用方策に関する有識者会議 最終報告※20」をまとめ、公表した。

(3) 国際社会の平和・安定及び我が国の安全保障への寄与

我が国の安全保障環境は厳しさを増し、オープンで自由なサイバー空間を確保するために国際社会との連携を強化する重要性が認識されている。戦略では、サイバー空間の安全・安定の確保のため、法の支配の推進、サイバー攻撃に対する防御力・抑止力・状況把握力の向上、国際協力・連携を一層強化するとしている。

NISCは2021年6月24日、ASEAN（Association of Southeast Asian Nations：東南アジア諸国連合）各国と日本のサイバーセキュリティインシデントへの対応能力向上、国際連携強化を目的に、サイバー情報連絡演習を開催した※21。ASEAN加盟国及び日本の政府機関のサイバー関連業務担当者等308名が参加し、事前に準備したシナリオ（政府に導入されているVPN装置へのサイバー攻撃、医療機関へのランサムウェア攻撃）のもとで、インシデント対応に関する情報共有の演習を実施した。

2021年10月21日には、オンラインにて第14回日本・ASEANサイバーセキュリティ政策会議が開かれた※22。前年の第13回会合で協力が合意された活動（重要インフラ防護、意識啓発、能力構築等）について実施状況を確認し、今後の日・ASEANの連携・協力が検討された。その主な内容は以下のとおりである。

- 情報共有体制及びサイバーインシデント発生時の対処体制の強化
- 重要インフラ防護に関する取り組みの推進、能力構築及び意識啓発における協力の推進
- 産学官連携の推進

なお、日・ASEANの政府間連携については「2.2.1(3) アジア太平洋地域のサイバー連携」を参照されたい。

(4) 横断的施策

戦略では、前述の(1)～(3)に示した施策項目を実行する上で、横断的・中長期的な視点で、研究開発や人材育成等に取り組んでいくことが重要であるとしている。

(a) 研究開発の推進

戦略では、サイバーセキュリティの研究開発においては、脅威情報やユーザニーズを踏まえ、実践的に進めることが重要であるとし、研究開発の国際競争力強化と産学官エコシステムの構築に向けた関係府省庁の振興施策を促進し強化を図るとしている。また、実践的な研究開発の推進においては、サプライチェーンリスクに対応するための技術検証体制の整備、国内産業の育成・発展支援策の推進、攻撃把握・分析・共有基盤の強化、暗号等の研究を推進するとしている。中長期的な対応については、特にAI（Artificial Intelligence：人工知能）技術・量子暗号技術等に関する取り組みを推進するとしている。

サイバーセキュリティ戦略本部は、2021年5月に「サイバーセキュリティ研究開発戦略（改訂）※23」を決定した。これは、2018年7月改訂の「サイバーセキュリティ戦略」を基に、研究開発の進捗と、環境の変化を踏まえた上で、研究・産学官連携の推進方策と産学官エコシステムの構築戦略を示したものである。

2021年度は、国立研究開発法人情報通信研究機構（NICT：National Institute of Information and Communications Technology）等が共同で、AIを用いたプライバシー保護連合学習技術による不正送金検知の実証実験を実施し、その結果を公表した※24。データの機密性を保ったまま機械学習を行う技術等を活用し、金融機関と連携して不正送金等を自動検知するシステムの実現を目指すとしている。

(b) 人材の確保、育成、活躍促進

戦略では、サイバー攻撃が複雑化・巧妙化する環境において新たな価値を創出していくために、サイバーセキュリティ確保に向けた人材の育成・確保が必要であるとしている。

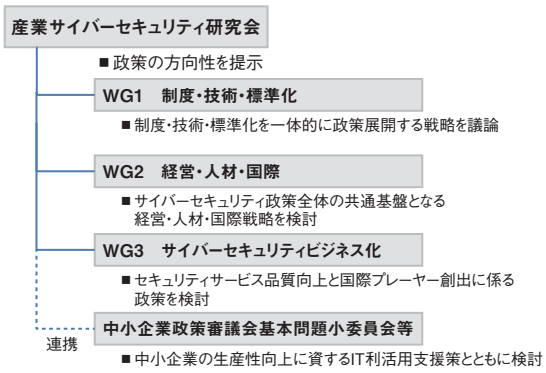
サイバーセキュリティ戦略本部は 2021 年 7 月に、「政府機関におけるデジタル改革に必要な IT・セキュリティ知識を有する人材の確保・育成総合強化方針」を公表した※25。情報システムの開発・運用及びサイバーセキュリティ対策と一体の業務改革に取り組むには、その担い手となる人材の充実が不可欠であるとして、各府省庁の内部人材の育成及び外部登用による確保を図るとしている。

2.1.2 経済産業省の政策

経済産業省は、サイバー空間、フィジカル空間を統合したサプラ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。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※26」

同研究会では 2021 年 4 月に第 6 回会合を開催し、「産業サイバーセキュリティ強化へ向けたアクションプラン※27」(2018 年 5 月発表) で示されたサプライチェーン、経営、人材、ビジネスの 4 パッケージを持続的に発展させるため、以下の三つの課題にチャレンジするとした※28。

- Cyber New Normal における 5 つ※29 の処方箋
  - ①「開発のための投資」から「検証のための投資」へのシフト
  - ②サイバー空間における価値創造を支えるデータマネジメントの枠組みの策定
  - ③セキュリティとセーフティの融合への対応
  - ④サプライチェーンセキュリティ確保のための産業界一丸となった対応
  - ⑤ Like-minded の関係強化
- 国としての対処能力の強化
- For the future infrastructure

以下では、本研究会で合意された取り組み方針に基づいた各 WG の 2021 年度の活動について述べる。

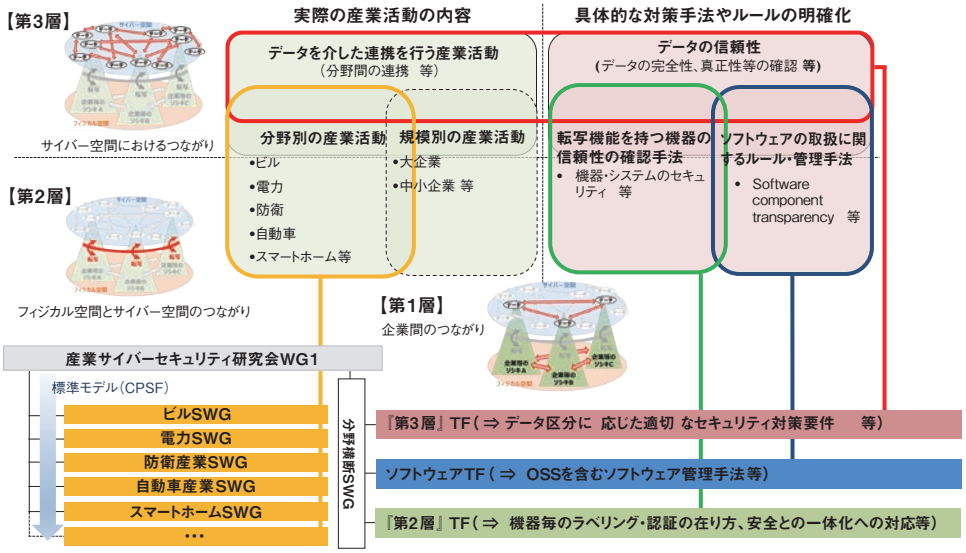
(a) WG1 (制度・技術・標準化)

WG1 では、「サプライチェーンサイバーセキュリティ強化パッケージ」の活動を主に実施しており、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※30 (The Cyber/Physical Security Framework) Version 1.0」(以下、CPSF)を 2019 年 4 月に策定した。

2021 年度は、CPSF をサイバー・フィジカル・システム(CPS)をとらえるモデルの一つとして位置付け、これを日本案として国際規格の策定を推進している。具体的には、ISO/IEC JTC 1/SC 27 WG 4 に Technical Specification (TS)として提案している(「2.6.2 (4) WG 4 (セキュリティコントロールとサービス)」参照)。

CPSF の具体化や実装、分野横断の共通課題を検討するため、WG1 には産業分野別サブワーキンググループ (SWG) と分野横断 SWG が設置されている (次ページ図 2-1-3)。2021 年度の活動の主な成果について述べる。

産業分野別 SWG は、ビル、電力、防衛産業、自動車産業、スマートホーム、宇宙産業、工場の七つの産業分野で活動している。ビル SWG は、ビルシステム全般に共通的な要件をまとめた共通編※31 に続く個別編として「空調システム」を作成中である。防衛産業 SWG は、



■図 2-1-3　タスクフォースの構成
（出典）経済産業省「サプワーキンググループ、タスクフォース等の検討状況※36」

2022 年 4 月に契約企業が保護すべき情報を取り扱う際に適用される情報セキュリティ基準を、米国連邦政府のセキュリティ標準（NIST SP800-171）と同程度まで強化した新情報セキュリティ基準を公開※32した。電力 SWG は、2021 年 2 月に「小売電気事業者のためのサイバーセキュリティ対策ガイドライン Ver1.0※33」を公開した。自動車産業 SWG は、2022 年 4 月に対策項目を拡充した「自工会／部工会・サイバーセキュリティガイドライン 2.0 版※34」を公開した。スマートホーム SWG は、2021 年 4 月に「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン Ver1.0※35」を公開した。宇宙産業 SWG は、2022 年 2 月から 3 月に「民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインβ版」に対するパブリックコメントを実施した。工場 SWG は、2022 年 4 ～ 6 月に「工場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（案）」に対するパブリックコメントを実施した。

分野横断 SWG は、2020 年度に引き続き CPSF の実装を促進するべく、第 2 層（フィジカル空間とサイバー空間のつながり）及び第 3 層（サイバー空間におけるつながり）に焦点を絞った層別タスクフォース（以下、TF）や、オープンソースソフトウェア（OSS：Open Source Software）等のソフトウェアの活用・脆弱性管理手法を検討するソフトウェア TF で議論を進めた。

第 2 層 TF では、2022 年 4 月に「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」を活用するための「IoT セキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集※37」を公開した。

第 3 層 TF では、2022 年 4 月にデータマネジメントに関する共通の考え方を整理した「協調的なデータ利活用に向けたデータマネジメント・フレームワーク ～データによる価値創造の信頼性確保に向けた新たなアプローチ」を公開した※38。

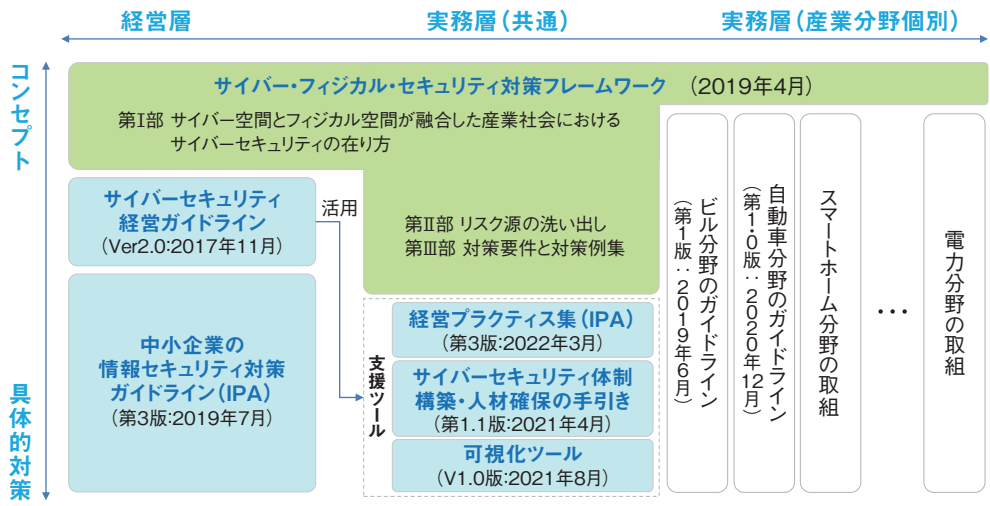
ソフトウェア TF では、2021 年 4 月に「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」を公開した※39。またソフトウェア管理手法としての Software Bill of Materials（SBOM：ソフトウェア部品表）の活用促進に向けて、自動運転システム検証基盤ソフトウェア「GARDEN ScenarioPlatform」を対象にした実証事業を実施した※40。

(b) WG2（経営・人材・国際）

「サイバーセキュリティ経営強化パッケージ」と「サイバーセキュリティ人材育成・活躍促進パッケージ」の活動を主に実践する WG2 では、サイバーセキュリティ対策における経営者の参画と人材育成、中小企業の対策、国際連携に関する政策を議論している。各種取り組みは CPSF を軸として整備している（次ページ図 2-1-4）。

経営に関しては、「サイバーセキュリティ経営ガイドライン※42」について、CPSF のコンセプトの反映やサプライチェーンの再整理等の検討を含め、2022 年度中に改訂を実施予定である。

「サイバーセキュリティ経営ガイドライン」の普及・定着については、IPA を通じて 2022 年 3 月に「サイバーセキュリティ経営ガイドライン Ver2.0 実践のためのプラクティス集第 3 版※4」及び経営ガイドラインの「重要 10 項目」の実



■図 2-1-4　CPSF を軸とした各種取り組みの大まかな関係
（出典）経済産業省「事務局説明資料※41」（第 7 回 産業サイバーセキュリティ研究会 ワーキンググループ 2（経営・人材・国際）資料 3）を基に IPA が編集

践をサポートする事例検索ツール「プラクティス・ナビ※43」を公開した。また、2021 年 8 月に「サイバーセキュリティ経営可視化ツール」（Web 版）を公開している（「2.4.1（2）セキュリティリスクマネジメント」参照）。

中小企業のセキュリティ対策の支援に関しては、IPA を通じて、2021 年 2 月には「サイバーセキュリティお助け隊サービス基準（1.0 版）」及び「サイバーセキュリティお助け隊サービス審査登録機関基準（1.0 版）」を、2021 年 7 月には「サイバーセキュリティお助け隊サービス基準」改訂版として 1.1 版を公開した。また、サービス審査登録機関により、サービス基準を満たすことが確認されたサービスに対して「サイバーセキュリティお助け隊マーク」の使用権を付与する事業を開始した。2022 年 4 月 1 日時点で 12 の民間事業者が登録されている※6（「2.4.2（3）（a）サイバーセキュリティお助け隊サービス制度」参照）。

地域に関しては、地域のセキュリティ・コミュニティ（地域 SECUNITY）の取り組みを更に促進するため、2021 年 6 月に「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3：Supply Chain Cybersecurity Consortium）」において地域 SECUNITY 形成促進 WG を設置した。また各地域における活動にあたって必要となる情報の共有、ベストプラクティスの展開、共通課題に対する解決策の検討等を目的としたワークショップを実施した（「2.4.2（2）（b）地域 SECUNITY 形成促進事業」参照）。

人材に関しては、セキュリティ人材の育成とプラス・セキュリティの普及が取り組みの柱となった。組織における人材確保や体制構築については、2021 年 4 月に「サイバーセキュリティ経営ガイドライン Ver2.0」の付録文書「サイバーセキュリティ体制構築・人材確保の手引き」の改訂第 1.1 版※44 を公開した（「2.3.1（2）セキュリティ業務・役割の広がり」参照）。

更に 2021 年 9 月から、「セキュリティ経営・人材確保の在り方検討 TF」を 9 回開催した（「2.1.2（2）（b）セキュリティ経営・人材確保の在り方検討 TF」参照）。

プラス・セキュリティについては、SC3 の産学官連携 WG において必要なスキルの整理等を行うこととした「2.3.1（3）（b）SC3 産学官連携 WG」参照）。今後、プラス・セキュリティの取り組みを普及させるため、デジタル人材育成プラットフォーム（「2.3.1（3）（a）デジタル人材育成プラットフォーム」参照）、地域 SECUNITY との連携による取り組みの推進等が検討される。

（c）WG3（サイバーセキュリティビジネス化）

「セキュリティビジネスエコシステム創造パッケージ」の活動を主に実践する WG3 では、セキュリティ製品・サービスの品質向上と国際プレイヤー創出に関わる政策として、サイバーセキュリティ製品の有効性を検証する検証基盤の整備を進めている。

セキュリティ製品の有効性検証／実環境における試行検証に関しては、IPA を通じて、製品選定から有効性検証の仕組み（手順・基準等）に基づいた製品検証や実環境での試行を実施し、これを通じ「試行導入・実績公表の手引き※45」の評価を実施した。また、更なるマッチング機会創出に向け、検証結果を活用した表彰制度の立案に向けた検討を行った。

模擬攻撃を含めたハイレベルな検証サービスに関しては、成果として 2021 年 4 月にセキュリティ検証サービス

の高度化を目的に「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」の公開等を実施した※46。本手引きは、「機器のセキュリティ検証において検証サービス事業者が実施すべき事項」「より良い検証サービスを受けるために検証依頼者が実施すべき事項及び持つべき知識」「検証サービス事業者・検証依頼者間の適切なコミュニケーションのために二者間で共有すべき情報や留意すべき事項」を整理したものである。本手引きが検証サービス事業者及び依頼者に活用されることで、国内の検証サービスの水準向上や、適切な検証体制の構築が期待される。

中小企業向けセキュリティ製品・サービスの検証事業に関しては、セキュリティ情報提供プラットフォーム仮検証サイトを立ち上げ、有効性検証を実施した。

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であるコラボレーション・プラットフォームに関しては、2021 年度はオンライン開催で計 6 回実施し、計約 800 人が参加した（表 2-1-1）。2021 年度は、新型コロナウイルス感染症（以下、新型コロナウイルス）対策のため聴講主体のオンラインセミナー形式で実施されたが、今後は少人数参加型でのオンラインワーキンググループ形式での開催が検討される。

開催回	テーマ
第 17 回	サイバーセキュリティ検証基盤事業
第 18 回	フェイクデータなど企業価値を毀損する新たな脅威
第 19 回	K 字型（二分化）経済環境下でのセキュリティ投資のあり方
第 20 回	ESG 視点でサイバーリスクマネジメントのあり方を探る
第 21 回	サプライチェーンを標的とするサイバーセキュリティリスクへの課題と対応策
第 22 回	事業変革“DX”の成功を支えるセキュリティ

■表 2-1-1　2021 年度の議論のテーマ

(2) その他の検討会の活動

他の検討会等における活動について述べる。

(a) 企業のプライバシーガバナンスモデル検討会

経済産業省と総務省は、DX における円滑なデータ利活用のためにプライバシーガバナンスの構築を目指している。2021 年度は、IoT 推進コンソーシアムのデータ流通促進 WG のもとに設置された「企業のプライバシーガバナンスモデル検討会」において、2022 年 2 月に「DX 時代における企業のプライバシーガバナンスガイドブック」の改訂版として、実践的な企業の具体例を充実させた ver1.2※47 を公開した。企業が本ガイドブックを参考にすることで、顧客や消費者からの信頼獲得、企業価値向上につながることが期待される。

(b) セキュリティ経営・人材確保の在り方検討 TF

経済産業省は「サイバーセキュリティ経営ガイドラインの見直し」と「セキュリティ人材活躍モデルの構築及び普及啓発」をテーマとして、セキュリティ経営・人材確保の在り方検討 TF を設置、2021 年 9 月から会合を 9 回開催した。「サイバーセキュリティ経営ガイドラインの見直し」については、経営層が自社にどのようなセキュリティ機能が必要かを考える際に、CPSF の枠組みで影響範囲をとらえることが容易となるよう CPSF の内容反映等を議論し、サイバーセキュリティ経営ガイドラインの改訂方針案を策定した。また「セキュリティ人材活躍モデルの構築及び普及啓発」については、2021 年 4 月に公開した「サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版」について、サプライチェーンや OT（Operational Technology）の観点から体制面での取り組みの強化等を議論した。

(3) 技術等情報管理認証制度

経済産業省は「産業競争力強化法等の一部を改正する法律」に基づき、2018 年 9 月から「技術等情報管理認証制度」を開始した※48。これは、事業者の技術等の情報管理について、国が示す認証基準に適合していることを、事業所管大臣及び経済産業大臣が認定した認証機関が認証を付与する制度である。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、2022 年 6 月現在 7 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・団体等に対しては、経済産業省が専門家を派遣して認証取得申請の支援を行う事業を行っており、2021 年度は 2021 年 8 月～ 2022 年 3 月の期間に実施した※49。また 2021 年度は、本制度の改善点・普及啓発方策等について検討会を 4 回実施した。機密性の高い技術情報等を保持する中小企業や業界団体等の制度活用が期待される。

(4) 情報セキュリティサービス審査登録制度

情報セキュリティサービスを安心して活用できる環境を醸成するべく、経済産業省は「情報セキュリティサービス基準」（以下、本サービス基準）及び「情報セキュリティサービスに関する審査登録機関基準」を策定し、2018

年2月に公表した※8。2022年1月31日には、両基準に基づく情報セキュリティサービス審査登録制度の一層の普及を図るべく、両基準の第2版を公表し、併せて、初版で「附則」としていた見直し需要の高い項目を「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示」として新たに公開した※50。

情報セキュリティサービス審査登録制度は、本サービス基準に照らして、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。

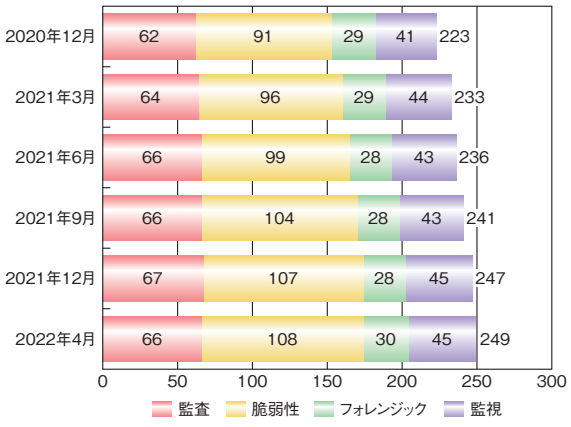
IPAはこの枠組みに基づき、2018年7月から、審査登録機関※51による審査の結果、本サービス基準に適合すると認められ、当該機関の登録台帳に登録され、かつIPAに誓約書を提出した事業者の情報セキュリティサービスを「情報セキュリティサービス基準適合サービスリスト」（以下、本リスト）として公開している※52。また、2021年2月からは、本リスト利用者がサービスを選定する際の参考となるよう、サービスのホームページへのリンク、サービスの概要、主たる対象顧客の分野・業種、対象とする地域の情報を本リストに追加し、提供している。

本サービス基準では、情報セキュリティサービスを以下の四つに分類しており、これらのサービス登録数の合計は2022年4月に249件に達した。登録数の推移としては、ゆるやかな上昇傾向にある（図2-1-5）。

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

なお、本リストは、NISCの「政府機関等の対策基準策定のためのガイドライン（令和3年度版）※16」において、以下のケースにおける外部委託先選定の際に活用できるように参照されている。

- 監査業務の外部委託先選定
- 脆弱性診断の外部委託先選定
- インシデントレスポンス業務の外部委託先選定
- セキュリティ監視業務の外部委託先選定



■図2-1-5　情報セキュリティサービス登録数の推移

また、本リストの「情報セキュリティ監査サービス」に掲載されているサービスを提供する監査機関であることは、「政府情報システムのためのセキュリティ評価制度（ISMAP）」において、評価を実施する監査機関の登録申請における要求事項の一つとなっている（「2.7.3 政府情報システムのためのセキュリティ評価制度（ISMAP）」参照）。

今後、本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の品質の維持・向上に加え、情報セキュリティサービス市場の活性化にもつながることが期待される。

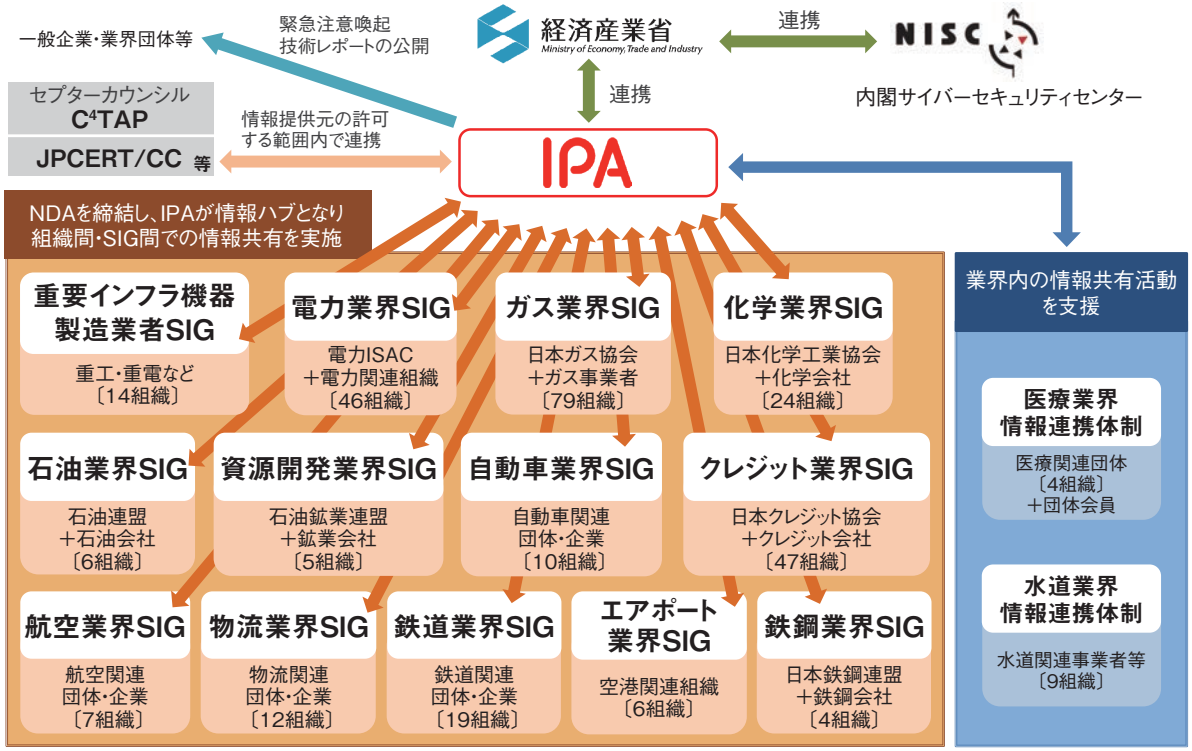
(5) J-CSIP（サイバー情報共有イニシアティブ）

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

J-CSIPは、日本の基幹産業を担う企業を中心に、サイバー攻撃等に関する情報を相互に共有し、サイバー攻撃の防御とその被害の低減を目指している。2022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292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※53）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（次ページ図2-1-6）。

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※54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



■図 2-1-6　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［2022 年 1 月～ 3 月］※55」

される情報は、提供元が明らかにならないよう、情報提供者の固有の情報を除去するルールがある。

参加組織から提供された、不審なメール、ウイルス※56、攻撃の痕跡等の件数（情報提供件数）、提供を受けた情報のうち標的型攻撃メール等と見なした件数（標的型攻撃件数）、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 2-1-2 に示す。年度により件数の増減はあるものの、継続して情報提供や共有が行われていることが分かる。

	2018 年度	2019 年度	2020 年度	2021 年度
参加組織からの情報提供件数	2,020	2,303	6,202	843
標的型攻撃件数（メール、検体等）	213	401	125	35
情報共有件数	195	225	147	118

■表 2-1-2　J-CSIP の運用実績

2021 年度は直近の 3 年間と比較して件数が減っている。これは「Ursnif」やその亜種である「Dreambot」、また「Emotet」と呼ばれるウイルスへの感染を狙う日本語の攻撃メールが大量にばらまかれ続けていたが、2021 年度はそれらの攻撃が減少あるいは停止していた時期が長かったことが影響している。

J-CSIP では、無作為に送信される不審メールやウイルスメール（ばらまき型メール）については、一般的に脅威の度合いが低いと考えられることから、原則として情報の提供依頼や共有の対象とはしていない。しかし、Emotet については、無作為に近い攻撃でありながらも、窃取した正規メールの文面の流用、パスワード付き ZIP ファイルの悪用といった手口が駆使され、多数の企業・組織にとって深刻な脅威であると見なせる状況であった（「1.2.6 ばらまき型メールによる攻撃」参照）。このことから、特に攻撃手口等に大きな変化が確認できた際は、情報共有の対象とし、各組織に対応を促してきた※57。なお、2017 年頃には Ursnif や Dreambot が巧妙な日本語の件名のメールで観測されたことから、同様に一部情報共有を行ってきた。ばらまき型メールと見なせる攻撃であっても、かつて標的型攻撃で使われていたような巧妙な手口が取り入れられている傾向があり、状況に応じ、今後も情報共有を図っていく必要があると思われる。

ビジネスメール詐欺に関しては、2020 年度までと同様、複数の情報提供を受けた。実被害に至る前に偽のメールであることに気付けた事例もあれば、攻撃者の口座へ送金してしまった事例もあった。企業間の取り引きのメールに介入したり、CEO（Chief Executive Officer：最高経営責任者）になりすましたりする等、基本的な騙しの

手口は変わらない（「1.2.3 ビジネスメール詐欺（BEC）」参照）。ただし細かい点では、送金先の変更を依頼する際、新型コロナウイルスの影響であるという嘘をつく等、時流に沿った騙しの手口の変化が見られた。これらの詳しい情報を J-CSIP 内で共有するとともに、情報提供元の許可が得られた範囲で、事例の一般公開も行った。

このほか、ウイルスに感染させる仕掛けが施された PowerPoint や Excel のアドインファイルが添付された攻撃メール、自衛隊の大規模接種センターをかたったフィッシングメール等の情報提供があり、それぞれ共有を行った。

全体的には、2016 年度まで観測されてきた、諜報活動が目的と思われる、日本国内の特定の業界や組織に向けて多数のメールが送信されるような標的型攻撃は減少傾向にある。これは、攻撃者がより慎重に、目立たないように攻撃を行うようになったためであると考えられる。また、発端が標的型攻撃メールであるのか、別の方法であるのか特定できないが、長期に渡って組織内ネットワークへ侵入されていたという情報提供もあった。ひそかに攻撃を行う攻撃者に一層の注意が必要と思われる。

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

(6) J-CRAT（サイバーレスキュー隊）

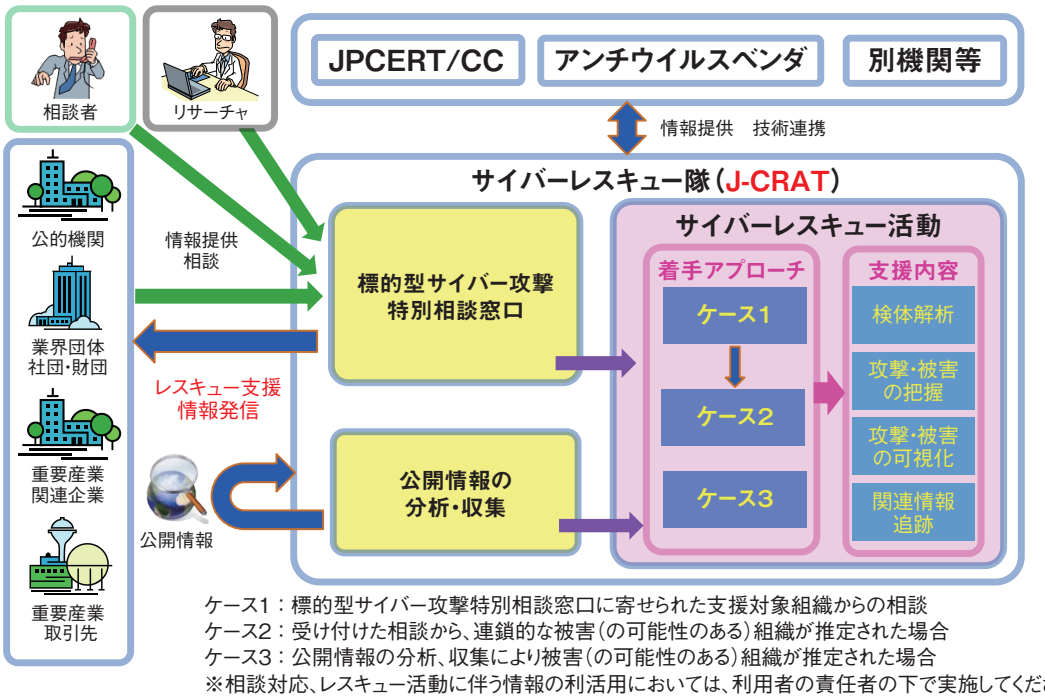
経済産業省の協力のもと、IPA は 2014 年 7 月に J-CRAT（Cyber Rescue and Advice Team against targeted attack of Japan：サイバーレスキュー隊）を発足させた。J-CRAT の目的を以下に示す。

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

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

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

標的型サイバー攻撃の被害に遭っている、または遭っている可能性が高い組織のうち、特に公的機関や業界団体、重要インフラ関連企業や取引先等サプライチェーンを構成する組織に対して、被害実態の確認と認知の支援、被害緩和の暫定対応に関する助言を「サイバーレスキュー活動」として実施している[※58]。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



ケース1：標的型サイバー攻撃特別相談窓口に寄せられた支援対象組織からの相談
ケース2：受け付けた相談から、連鎖的な被害（の可能性のある）組織が推定された場合
ケース3：公開情報の分析、収集により被害（の可能性のある）組織が推定された場合
※相談対応、レスキュー活動に伴う情報の利活用においては、利用者の責任者の下で実施してください。

■図 2-1-7　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）[※59]」

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（前ページ図 2-1-7）。

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 2-1-3 に示す。2021 年度の活動実績を 2020 年度と比較すると、「相談件数」は 7.6% 減少しており、内訳を見ると「レスキュー支援件数」が 7.8% 減少、「オンサイト支援件数」も 47.1% 減少している。

	2018 年度	2019 年度	2020 年度	2021 年度
相談件数	413 件	392 件	406 件	375 件
レスキュー支援件数	127 件	139 件	102 件	94 件
オンサイト支援件数	31 件	20 件	17 件	9 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 2-1-3　J-CRAT の活動実績

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

2.1.3 総務省の政策

総務省は、IoT・5G 機器に対するサイバー脅威が深刻化している状況を踏まえて 2020 年 7 月に取りまとめた提言「IoT・5G セキュリティ総合対策 2020[※60]」の改訂版として、2021 年 7 月に「ICT サイバーセキュリティ総合対策 2021[※61]」（以下、総合対策 2021）を策定・公表した。総合対策 2021 には、デジタル庁の発足、DX の進展等の環境変化も踏まえ、IoT・5G にとどまらない ICT インフラサービスに対するセキュリティ対策が広く盛り込まれている。

本項では、総合対策 2021 の流れに沿った総務省のセキュリティへの取り組み状況、及び地方自治体のセキュリティへの取り組み状況を述べる。

(1)「ICT サイバーセキュリティ総合対策 2021」の概要

2021 年 7 月、総務省は ICT サービス・インフラにおけるサイバーセキュリティを確保するための具体的な施策について、総合対策 2021 に取りまとめた。以下の方針や考え方に準拠している。

- 2020 年 12 月に閣議決定した「デジタル社会の実現に向けた改革の基本方針[※62]」に基づく社会全体のデジタル改革・DX の推進
- 2021 年 5 月にサイバーセキュリティ戦略本部が発表した「次期サイバーセキュリティ戦略（骨子）[※63]」に基づく「自由、公正、かつ安全なサイバー空間」の確保
- IoT、5G を含む ICT サービス・インフラは、デジタル改革・DX 推進の基盤であり、国民一人ひとりが安心して ICT を活用できるようなサイバーセキュリティの確保が不可欠であるという考え方

総合対策 2021 では、具体的施策として、「電気通信事業者における安全かつ信頼性の高いネットワークの確保」「COVID-19 への対応を受けたセキュリティ対策の推進」「デジタル改革・DX 推進の基盤となるサービス等のセキュリティ対策」「サイバーセキュリティ情報に関する産学官での連携・共有等の促進」を挙げている。また、横断的施策として、「サイバーセキュリティ情報に関する産学官での連携・共有等の促進」「ICT サイバーセキュリティに係る横断的施策」を挙げている。以下では、2021 年度の各施策の実施状況について述べる。

(2) 電気通信事業者における安全でかつ高信頼なネットワーク確保のための対策推進

総合対策 2021 では、5G インフラ構築の進展や IoT 機器の普及、社会のデジタル化進展等によって高まるサイバーリスクに対し、電気通信事業者がセキュリティ対策を講じ、安全で高信頼なネットワークを確保することが重要であるとし、以下の三つの重点施策を挙げている。

(a) 安全かつ信頼性の高いネットワーク確保

総合対策 2021 では、安全かつ信頼性の高いネットワーク確保のため、ガバナンスの確保、及び通信事故の報告・検証に注目している。

- ガバナンスの確保

  総務省は 2021 年 4 月に通信事業者にサイバーセキュリティの実態に関しヒアリングを行うとともに、同年 5 月に「電気通信事業ガバナンス検討会」を立ち上げ、セ

キュリティ対策とデータの取り扱いに対する事業者のガバナンスの在り方を協議した。

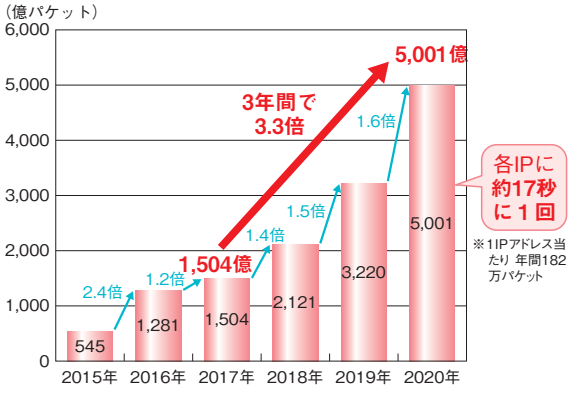
上記検討会では、ネットワークサービス利用者情報の保護の強化が焦点となっていた。具体的には、ネットワークサービス事業者が収集するクッキー・タグ等の取り扱いに関して国内外の施策を調査し、これらの情報を保護するべきとし、事業法である電気通信事業法を改正する方向で議論が進められた。一方で、討議終盤に経済団体から、議論のプロセスが不透明である、電気通信事業法改正による方式は慎重に検討すべき、等の意見が提示された※64。これらの経済団体の意見、及び意見募集を調整した結果は2022年2月18日に公開された※65。利用者情報の保護強化は盛り込まれたが、当初想定されたクッキー利用に関するオプトアウト義務化等は見送られ、事業者の更なるガバナンス強化は今後の検討を待つこととなった。

- 通信事故の報告・検証

総務省は2020年以来、情報通信審議会情報通信技術分科会 IPネットワーク設備委員会にて、IoT導入、マルチステークホルダー等で複雑化する通信事故の報告・原因検証を通じたリスクマネジメントに関するガバナンスを検討している※66。2021年度は、同委員会に事故報告・検証制度等タスクフォースを設置して事業者ヒアリングを実施した。また、事故対応で事業者・官庁・自治体が即応連携する際に課題となるマルチステークホルダーの拡散（増大）について、リスクマネジメント（PDCA、OODA※67ループ等）の強化が重要であるとし、この視点から、サイバー攻撃を原因とする通信事故報告制度や検証制度の在り方、個人情報保護法への対応、事故検証に基づくリスクアセスメント機能の強化等を検討した。これらの検討結果は報告にまとめられ※68、同報告に対する意見募集の結果が2021年9月22日に公表された※69。

(b) 電気通信事業者の積極的なサイバー攻撃対策

総合対策2021では、IoT機器へのサイバー攻撃が急増している状況（図2-1-8）を鑑み、端末側の脆弱性対策だけでなく、ネットワーク側での機動的な対策が必要、としている。具体的に総務省は、情報フロー分析によるC&C（Command and Control）サーバ検知手法の実証施策を検討し、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」にて、通信の秘密に抵触しない範囲で事業者が共有できるサーバ情報について整理した。またこの内容を「第四次とりまとめ案」として意見募集を実施※70し、2021年11月24日に結果を公表した※71。結果は、C&Cサーバである疑いの高い機器の検知行為、及びC&Cサーバ検知に関する情報の共有はいずれも適法、というものであった。



■図2-1-8　IoT機器を狙った攻撃の増加
（出典）総務省「ICTサイバーセキュリティ総合対策2021」を基にIPAが編集

(c) 5Gセキュリティの強化

総務省は、制度、技術、情報共有、市場、振興等の各分野で総合的な5Gセキュリティの施策を推進している。2021年時点で注目されるのは、2020年5月に施行、2021年9月にデジタル庁発足を受けて一部改正された「特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律※72」の運用である。

同法は、5Gの全国基地局やローカル5Gに関わる高度情報通信システムの開発導入を税制面で優遇するもので、導入においてはサプライチェーンセキュリティを含むセキュリティ対策を求めている。税制優遇措置は当初施行後2年であったが、2021年12月、3年間の延長が閣議決定された※73。

上記のサプライチェーンセキュリティには、5G関連機器調達における海外（特に中国）ベンダへの依存リスク対応が含まれる。海外ベンダ依存リスクを低減するため、総務省は、5G製品の相互接続規格化推進、5G市場のオープン化施策を推進している。ベンダに向けた施策としては、相互接続規格O-RAN（Open Radio Access Network）※74の普及、国内のO-RAN相互接続検証拠点の具体化に取り組んでいる。また5G事業者に対しては、周波数帯域割り当てにおいて、オープン化規格に基づく機器の採用計画を必須とし、これを含む特定基地局向け周波数割り当て指針に関して2021年12月に意見募集を行った※75。

このほか、2020年2月にICT-ISACに設置された「5G

セキュリティ推進グループ」は、ローカル 5G のセキュリティ対策調査活動等を実施※76している。具体的には 5G 関連機器ベンダ、通信事業者、ユーザ企業を対象としたアンケート調査結果を 2021 年 3 月に公開し、参照すべきガイドライン策定の必要性を指摘している。今後のガイドラインの整備が期待される。

(3) 新型コロナウイルスへの対応に関するセキュリティ対策の推進

新型コロナウイルスの感染防止対策のため、2020 年 2 月以降、人の移動を抑制し、患者・感染者との接触機会を減らす観点から、テレワークや時差出勤が推進されている。総合対策 2021 では、新型コロナウイルスへの対応に関するセキュリティ対策として、以下の二つの対策を挙げている。

(a) テレワークセキュリティの確保

総務省では、企業等がテレワークを実施する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針として「テレワークセキュリティガイドライン」の初版を 2004 年 12 月に策定した。その後、状況の変化に対応して改定を行い、2021 年 5 月に第 5 版※77を公表した。また、セキュリティの専任担当がいない中小企業等のシステム管理担当者を対象として、テレワークを実施する際に最低限のセキュリティを確実に確保してもらうため「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」等を 2020 年 9 月に策定し、2021 年 5 月に最新のセキュリティ動向等を踏まえて改定を実施した※78。総務省はまた、テレワークを導入する企業等のセキュリティ対策状況の実態調査を実施した。2022 年 3 月に公表された報告書によると、テレワーク導入の課題として、最も多かったのは「テレワークに必要な端末等の整備」(51.9%)、次いで「セキュリティの確保」(51.6%)、「通信環境の整備」(44.3%)という結果で、セキュリティの確保は大きな課題の一つであることがうかがえる※79。

(b) トラストサービスの制度化と普及促進

新型コロナウイルス感染防止のため、対面を前提としない手続きの整備が進んだが、その際、データの改ざんや送信元のなりすまし等を防止する仕組みとしてトラストサービスの必要性が高まった。

総務省では、「プラットフォームサービスに関する研究会」のもとに「トラストサービス検討ワーキンググループ」を立ち上げ、我が国のトラストサービスの在り方に関する検討を行い、2020 年 2 月にトラストサービスの取り組みの方向性について提言した※80。この提言を踏まえ、タイムスタンプ認定制度の適切な運用、電子文書の発行元の真正性を証明する e シール等トラストサービスの普及方策の検討を行った。

タイムスタンプについては、2020 年に「タイムスタンプ認定制度に関する検討会」を立ち上げ、現行の民間の認定制度である「タイムビジネス信頼・安心認定制度」の課題や EU（European Union：欧州連合）等の国際的な制度との整合性等の観点から議論を行い、2021 年 4 月に「時刻認証業務の認定に関する規程（令和 3 年総務省告示第 146 号）」を公布し、国によるタイムスタンプの認定制度を整備した※81。

e シールについては、2020 年 4 月に「組織が発行するデータの信頼性を確保する制度に関する検討会」を立ち上げ、e シールの利用が有効なユースケースや、我が国の e シールの在り方等について検討を行い、2021 年 6 月に「e シールに係る指針」を公表※82し、今後、我が国の e シールの信頼性を担保するために利用者、認証局、e シールサービスの提供事業者、e シールを活用するアプリケーションの提供事業者等に求められる技術上・運用上の基準等について整理した。

電子署名については、2020 年 7 月に「電子署名法 2 条 1 項に関する Q&A※83」を、9 月には「電子署名法 3 条に関する Q&A※84」を公表する等、電子署名法上の電子署名の利便性を改善した。

(4) デジタル改革・DX 推進の基盤となるサービス等のセキュリティ対策の推進

総合対策 2021 では、デジタル改革や DX 推進の基盤として IoT やクラウドサービス、そしてそれらのサービスを組み合わせたユースケースであるスマートシティ等を安全に安心して利用できる環境を整備していくことが重要であるとし、セキュリティ対策として以下の三つの重点施策を挙げている。

(a) IoT のセキュリティ対策

総合対策 2021 では、IoT 機器の設計・製造・販売段階と運用段階のセキュリティ対策強化を並行して行うとしている。

- 設計・製造・販売段階の対策
  製造事業者に対して IoT 機器のセキュリティ・バイ・デザインの考え方を十分に浸透させるとともに、対策

がとられた機器の市場への展開を促進させるために、総務省は「電気通信事業法に基づく端末機器の基準認証に関するガイドライン」（以下、技術基準）を策定し、2020年9月に第2版※85を公表した。一般社団法人重要生活機器連携セキュリティ協議会（CCDS：Connected Consumer Device Security Council）は、この技術基準に加え、製品分野ごとのセキュリティ要件のガイドライン※86を策定し、当該要件に適合したIoT機器に対して適合していることを示すマークを付す認証の仕組み（CCDSサーティフィケーションプログラム）を構築し、運用している※87。2021年10月には、現金自動預け払い機（ATM）関連システムの物理・サイバー攻撃対策に関するCCDSサーティフィケーションプログラムの運用を開始した※88。

- 運用段階の対策

既に運用されているIoT機器のセキュリティを高める対策が必要であるとして、2019年2月よりNICTが脆弱性等のあるIoT機器を調査し、電気通信事業者（ISP: Internet Service Provider）を通じて利用者へ注意喚起を行う取り組み「NOTICE」を実施している※89。2021年度は、総務省のロゴ入り封筒による郵送の注意喚起の実施、注意喚起への対応ができていない利用者（法人）に対する電話ヒアリング等を実施した※90。更に、これまではTelnet及びSSH（パスワード認証）のみを調査対象としてきたが、対象をhttp/httpsプロトコルに広げ、2022年3月から予備調査を開始した※91。

また、2019年6月からは既にウイルスに感染しているIoT機器をNICTの「NICTER」プロジェクトで得られた情報を基に特定し、IPAを通じて利用者へ注意喚起を行う取り組みも実施している。2021年は1IPアドレスあたりで約175万パケットが観測され、2012年以降続いていた増加傾向が減少（約6%減）に転じたが、2019年と比較すると約1.4倍の値であり、依然多くのサイバー攻撃関連パケットが観測されている状況が続いているとのことである※92（2021年度の注意喚起数については「3.2.3(1)国内における実態」参照）。

(b) クラウドサービスの利用の進展を踏まえた対応

総合対策2021では、クラウドサービス利用時の設定ミスを防止・軽減するため、発生している設定ミスやそれに起因する事故、クラウドサービス事業者における取り組み状況等を把握し、当該事業者のセキュリティ対策を促す方策を検討することが適当であるとしている。総務省は、2014年に策定したクラウドサービス事業者向けの「クラウドサービス提供における情報セキュリティ対策ガイドライン」について、全体の構成や責任共有モデルの考え方・管理策の見直し等を行い、2021年10月に改定した※93。改定内容については「3.3.4 クラウドの情報セキュリティに対する政府の取り組み」を参照されたい。

(c) スマートシティのセキュリティ対策

総務省は2021年6月に、安全・安心なスマートシティの実現に資するため、「スマートシティセキュリティガイドライン（第2.0版）※94」を公表した。2020年10月に公表した第1.0版を、よりスマートシティの運用の実態に沿った、スマートシティ構築・運営主体が利用しやすいガイドラインとする改定である。本ガイドラインでは、スマートシティの構成要素を「ガバナンス」「サービス」「都市OS」「アセット」の四つのカテゴリに分け、各カテゴリにおけるセキュリティと、スマートシティ全体としてのセキュリティそれぞれの観点から考慮すべきリスクや対策について整理している。添付のセキュリティ対策一覧表やチェックシートは、スマートシティの分野や特性を踏まえたセキュリティ対策の検討に活用されることが期待される。

また、2021年6月に、上記ガイドラインを活用しようとするスマートシティ推進主体やサービス提供者等に向けた導入ガイドブックとして、「スマートシティセキュリティガイドブック※95」を公表した。上記ガイドラインと同様に活用が期待される。

(5) ICTサイバーセキュリティに係る横断的施策

総合対策2021では、ICTサイバーセキュリティに係る横断的施策として、国際連携の推進、研究開発の推進、人材育成・普及啓発の推進が掲げられている。以下にそれぞれの概要を述べる。

(a) 国際連携の推進

サイバー空間は国境を越えて利用される領域であることから、情報共有、国際的なルール作り、研究開発、人材育成等の多様な取り組みが必要である。アジア地域においてはASEAN各国との関係強化のため、日ASEANサイバーセキュリティ能力構築センター（AJCCBC：ASEAN-Japan Cybersecurity Capacity Building Centre）において、CYDER等を通じて、ASEANのセキュリティ人材の育成支援を実施し、4年間で734名が参加している（2021年12月現在）。また、オンライン環境で受講可能なプログラムの拡充、有志国

との第三者連携、国内企業により開発された演習の提供等を実施している。なお、ASEAN 諸国との包括的な連携については「2.2.1（3）アジア太平洋地域のサイバー連携」を参照されたい。

更に 5G・ポスト 5G 推進とセキュリティ確保、知財権・プライバシー保護を含む安全なデジタルデータ流通について、欧州諸国・EU とも定期的に協議やワークショップを実施している。2021 年度は以下の通り行われた。

- 2021 年 6 月 17 日：日仏 ICT 政策協議（第 21 回）※96
- 2022 年 2 月 3 日：日 EU･ICT 政策対話（第 27 回）※97
- 2022 年 3 月 23 日～ 24 日：日独 ICT 政策対話（第 6 回）※98

(b) 研究開発の推進

NICT は中長期計画に基づき、サイバーセキュリティ分野の基礎的、基盤的な研究開発等を実施している。具体的には、2022 年度までの 3 年間は「電波の有効利用のための IoT マルウェアの無害化、無機能化技術等に関する研究開発」等に取り組んでいる。本研究では、AI 技術を駆使した IoT マルウェアの挙動検知及び駆除、感染した IoT 機器の無害化、無機能化の技術開発に取り組むとしている。

(c) 人材育成・普及啓発の推進

2021 年 4 月に発足したサイバーセキュリティ統合知的・人材育成基盤「CYNEX（Cybersecurity Nexus：サイネックス）」は、我が国のサイバーセキュリティの対応力向上を目指すための共通基盤である※99。CYNEX では、NICT がこれまで取り組んできた、「STARDUST」「NICTER」「CYDER」「ナショナルサイバートレーニングセンター」等の知見、成果を産学官に開放する。更に配下に四つのサブプロジェクト「Co-Nexus」を設け、サイバーセキュリティに関する攻撃分析、データ収集・蓄積、製品検証、人材育成等の活動を行う。2022 年 2 月にはサブプロジェクトの一つであり、演習教材と実機の演習環境からなる「CYROP（サイロップ）※100」のトライアル利用を期間限定で実施した（「2.3.4(7)CYNEX」参照）。

他方、インターネットの安心･安全な利用のため、児童・生徒とその保護者等を対象にした啓発事業「e-ネットキャラバン」を官民連携で実施している。2021 年度の実施件数は 2,559 件、開催場所は 47 都道府県で、全国まんべんなく開催されている。

(6) 地方自治体の情報セキュリティ

本項では、自治体等の情報セキュリティ対策の見直しについて、総務省が 2021 年 9 月より開始した「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会」からの公表情報等を参照して述べる。

(a) 2021 年度の動向

2021 年 7 月、NISC の「政府機関等のサイバーセキュリティ対策のための統一基準群※15」が改定された。これを踏まえ、総務省は「地方公共団体における情報セキュリティポリシーに関するガイドライン」について、2020 年 12 月に改定した内容を維持しつつ、2021 年 9 月から 12 月にかけて 3 回の検討会を実施※101、2022 年 3 月 25 日に改定版を公開した※102。

主な改定内容は次の 4 点となる※103。

①業務委託・外部サービス利用時の情報資産の取り扱いについて

- 外部サービスを「業務委託」と「外部サービス」に再定義した上で、「機密性 2 以上の情報を取り扱う場合」と「機密性 2 以上の情報を取り扱わない場合」に区分し、取り扱う情報に応じたセキュリティ対策を追記
- 機密性 2 以上の情報を取り扱う外部サービスの利用ライフサイクルに渡るセキュリティ要件の追加、及びシャドー IT 対策となる組織内のサービス利用規定整備の要請を追記
- クラウドサービス選定の指標・基準等として ISMAP や ISO/IEC 27017 等の第三者認証の活用を推奨

②未知の不正プログラム対策製品やソフトウェア等の導入に加え、監視体制や CSIRT との連携を留意点として追記

③多様な働き方を前提としたセキュリティ対策として

- テレワークで職員が確認すべきチェック項目やショルダーハッキング防止等のテレワークの運用面に関するセキュリティ対策を追記
- BYOD（Bring Your Own Device）利用時のセキュリティ対策として IP アドレス、MAC アドレス等による端末認証や端末利用申請手続きの遵守、端末に情報を保存できないようにする機能を設ける等の対策を追記
- Web 会議サービス利用時のセキュリティ対策として Web 会議に無関係な者が参加できないようにする対策等を追記

④マイナンバー利用事務系から外部接続先（eLTAX、ぴったりサービス）へのデータのアップロードについて、地方公共団体に対してリスク分析と情報セキュリティ対策の徹底を条件に認めることを追記

(b) 今後の予定

地方自治体の基幹業務システムの統一・標準化に関しては、「デジタル社会の実現に向けた重点計画」（2021年6月及び12月に閣議決定[※104]。以下、重点計画）において、基幹業務システムを利用する原則すべての地方公共団体が、目標時期である2025年度までに、ガバメントクラウド上に構築された標準準拠システムへ移行できるよう、環境を国が整備する、としている[※105]。また、地方自治体が活用するクラウド環境のセキュリティ対策については「適切に講じる予定[※104]」としており、セキュリティについては、各自治体が個別にセキュリティ対策や運用監視を行う必要がなく、また個別の対応が難しかった最新のセキュリティ対策も導入可能になる、としている[※104]。重点計画は、「自治体の三層の対策」の抜本的見直しを含め、2022年の夏を目途に地方公共団体のガバメントクラウド活用に関するセキュリティ対策の方針を決定していくとし、また先の総務省検討会では「ガバメントクラウド活用に関する新たなセキュリティ対策の在り方については、デジタル庁における検討と連携し、随時検討を行う[※103]」としている。

2021年6月、ガバメントクラウドの先行事業の公募が開始された[※106]。次期自治体情報セキュリティクラウドの一部として活用を希望する都道府県を対象に、ガバメントクラウド等を通じてセキュリティ機能を国が提供する先行事業となる。検証予定とするセキュリティシステムをCDN（Content Delivery Network）及びWAF（Web Application Firewall）とし、サイバー攻撃やシステム障害時の国・地方の役割・連携方法を含め、効果的なセキュリティ対策の実施手法や運用に係る経費の削減等導入効果を検証する予定となっている[※107]（図2-1-9）。

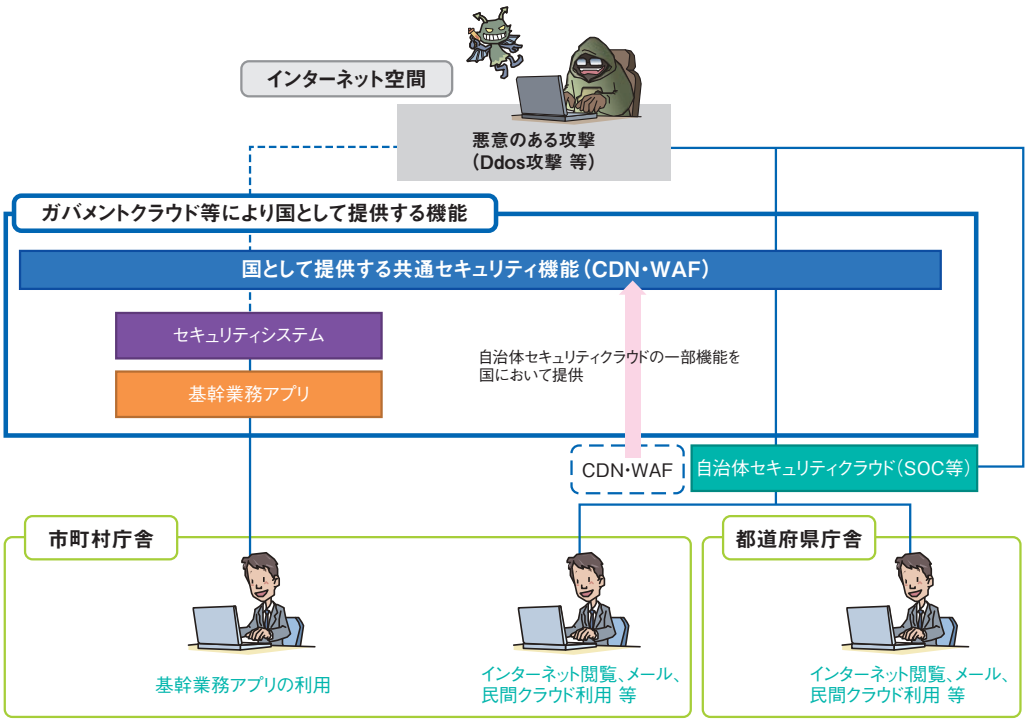
2021年10月、ガバメントクラウド先行事業のうちセキュリティシステムを対象とする自治体について、2グループが採択された[※108]（「2.1.1 (2) (c) 経済社会基盤を支える各主体における取り組み」参照）。

(7) 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) 無線LANセキュリティ

総務省では、無線LANの利用者・提供者のそれぞれに向けたセキュリティ確保に関するガイドラインとして「Wi-Fi利用者向け簡易マニュアル」及び「Wi-Fi提供者向けセキュリティ対策の手引き」を作成し[※109]、2020年



■図2-1-9　先行事業（セキュリティシステム）について
（出典）内閣官房「地方自治体によるガバメントクラウドの活用（先行事業）について[※107]」を基にIPAが編集

■図 2-1-10　無線 LAN 利用者・提供者向けガイドライン
（出典）総務省「無線 LAN（Wi-Fi）の安全な利用（セキュリティ確保）について※109」

5 月にこれらの改訂を行っている（図 2-1-10）。

「Wi-Fi 利用者向け簡易マニュアル」では、以下のセキュリティ対策の三つのポイントを示し、解説している。

- 接続するアクセスポイントの確認
- https 通信の際の URL の確認
- 自宅に設置している機器の設定の確認

「Wi-Fi 提供者向けセキュリティ対策の手引き」では、利用者を守るための対策や、Wi-Fi を安全に提供するための対策等について解説している。

2021 年度の活動として、無線 LAN のセキュリティ対策に関する周知啓発を目的として、オンライン講座を開講した※110。

(b) 不正アクセス対策

総務省は、「不正アクセス行為の禁止等に関する法律※111」に基づく取り締り等から得た不正アクセスの手口に関する最新情報の提供や、「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」を公表すること等を通じ※112、不正アクセスの防御に関する啓発及び知識の普及を図る等により、官民で連携した不正アクセス防止対策を推進している。なお、上記の「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」は 2022 年 4 月 7 日に更新された。2021 年 1 月 1 日～ 12 月 31 日の不正アクセス行為発生状況については「2.1.4 (1) (a) サイバー空間の脅威への対応の強化」を参照されたい。

(c) ログ保存の在り方

安全・安心なサイバー空間を構築するための通信履歴等に関するログの保存の在り方について、「電気通信事業における個人情報保護に関するガイドライン※113」の解説を踏まえ、関係事業者における適切な取り組みを推進する等の対応を行っている。同ガイドラインは 2022 年 3 月 31 日に改訂された。

2.1.4 警察によるサイバー犯罪対策

警察庁では、「警察におけるサイバーセキュリティ戦略※114」及び「サイバーセキュリティ重点施策※115」に従い、サイバー空間の脅威への対処に関する取り組みを推進している。

本項では、2021 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とサイバー犯罪の情勢等について、警察庁が公開している「令和 3 年上半期におけるサイバー空間をめぐる脅威の情勢等について※116」及び「令和 3 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※117」等に基づいて述べる。

(1) 警察における主な取り組み

「サイバーセキュリティ重点施策」は、「サイバー空間の脅威への対応の強化」「警察における組織基盤の更なる強化」及び「国際連携及び産学官連携の推進」を主な柱としている。これらを踏まえ、2021 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

サイバー空間が社会活動を営む重要かつ公共性の高い場へと変貌を遂げつつある中で 2021 年のサイバー犯罪の検挙件数は 1 万 2,209 件と過去最多を記録した。ランサムウェアによる被害の拡大、不正アクセスによる情報流出、国家を背景に持つ集団によるサイバー攻撃等、サイバー空間をめぐる脅威は、極めて深刻な情勢が続いているという。

- ランサムウェアの傾向と対応

  2020 年下期の企業・団体等におけるランサムウェア被害の報告件数が 21 件であったものが、2021 年上期は 61 件、同年下期は 85 件と急増した（警察庁によるランサムウェア被害の調査結果については「1.1.2 (4) 国内被害が拡大したランサムウェアについて」参照）。

  ランサムウェアへの対策として、警察庁 Web サイトでの注意喚起（2021 年 9 月）※118、一般社団法人日本損害保険協会等との連携による警察への通報促進に向けた取り組み※119、ダーク Web 上のサイトに掲載された「VPN 製品の認証情報」に関係する企業等への

注意喚起、医療機関を標的としたランサムウェアの被害に関する厚生労働省への情報提供等、関係機関と連携した対策を行った。

- 不正アクセスによる政府機関等からの情報流出
  サイバー攻撃による情報窃取事案については、国内において政府機関や研究機関等が外部からの不正アクセスを受け、個人情報等が流出した可能性がある事案が相次いで確認されている。
  具体的な事例としては、国立研究開発法人海洋研究開発機構からの不正アクセス被害の発表（2021年3月）、内閣府からの内閣府、内閣官房、復興庁及び個人情報保護委員会が使用するファイル共有ストレージへの不正アクセス被害の公表（同年4月）、原子力規制庁からの原子力規制委員会ネットワークシステムへの不正アクセス被害の中間報告（同年5月）等がある。
  また警察庁が実施した企業、行政機関等における不正アクセスの実態調査報告（同年12月公開）によると、回答総数716社・団体のうち、過去1年間に不正アクセス等の攻撃・被害に遭ったと回答したのは95団体（13.3%）であった※120。
- 国家を背景に持つ集団によるサイバー攻撃
  警察の捜査により国家レベルの関与の可能性が明らかになったサイバー攻撃の事案がある。
  具体的には、レンタルサーバ不正契約事件の捜査から国立研究開発法人宇宙航空研究開発機構（JAXA：Japan Aerospace Exploration Agency）を始めとする国内企業等へのサイバー攻撃に中国人民解放軍が関与している可能性が高いとした事案※121や、日本製法人版セキュリティソフトの年間使用権の不正取得に係る捜査から、中国人民解放軍が日本国内の各種情報を収集している可能性が高いとした事案がある。
  また2021年7月、外務省はサイバー攻撃集団「APT40」等について中国政府を背景に持つ可能性が高いとする談話を発表※122した。このとき警察はNISCと連携し、情報収集や対策等を進めていく旨を発表※123、被害企業に対し、不正プログラムへの感染の可能性や有効な対応策等の情報を提供する等、被害防止の取り組みも併せて実施している。
- 東京オリンピック・パラリンピック競技大会
  その他、東京2020オリンピック・パラリンピック競技大会では、大会関係機関と協力し、官民一体の共同対処訓練や、大会関係事業者や重要インフラ事業者等に対する注意喚起等を継続的に実施した。大会期間中、24時間体制で臨んだ結果、大会の運営に影響を及ぼすようなサイバー攻撃は見受けられなかった※124（「2.2.1（1）（c）オリンピック開催と期間中の首脳・外相会談」参照）。

（b）警察における組織基盤の更なる強化

警察のサイバー犯罪対応体制としては、警察庁のサイバー攻撃対策室が、都道府県警察が行う捜査に対する指導・調整、官民連携や外国治安情報機関との情報交換に当たっている。また、サイバー攻撃対策室長を長とする「サイバー攻撃分析センター」でサイバー攻撃に係る情報の集約・分析を実施、14都道府県警察には「サイバー攻撃特別捜査隊」を設置している。更に技術面での支援部隊として警察庁の「サイバーフォースセンター」を司令塔に、全国の地方機関の情報通信部に「サイバーフォース」を設置、24時間体制でのサイバー攻撃の予兆・実態把握、標的型メールに添付された不正プログラムの解析等を行っている※121。

2021年、警察庁の私的懇談会であるサイバーセキュリティ政策会議※125において「サイバー局等新組織において取り組む政策パッケージ」が議論され、サイバー空間を取り巻く情勢とリスク、新組織に求められる役割、その役割を果たす上での政策課題及び解決のための具体策等の提言を含む報告書が取りまとめられ、12月に公開された※126。

並行して、警察法の一部を改正する法律案が2022年1月に国会に提出された※127。国会では、サイバー事案に関する政策を一元的に担うサイバー警察局とともに、重大サイバー事案の捜査、実態解明の責を担う捜査部隊を警察庁に設置すること等が審議された。この結果、2022年4月、警察庁にサイバー局、関東管区警察局にサイバー特別捜査隊が発足した。

（c）国際連携及び産学官連携の推進

国境を越えるサイバー犯罪・サイバー攻撃に対処するためには外国捜査機関との協力が必要になる。警察庁では、国際捜査共助の枠組みの活用や、国際会議、専門家会合、国際刑事警察機構（ICPO：International Criminal Police Organization、INTERPOLとも呼ばれる）等が主催するワークショップへの参加をとおして、外国捜査機関等との情報交換、協力関係の確立に積極的に取り組んでいる。また、情報技術解析に関する事案対処に資する技術情報の収集についても、ICPOデジタル・フォレンジック専門家会合に参加している※121。

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

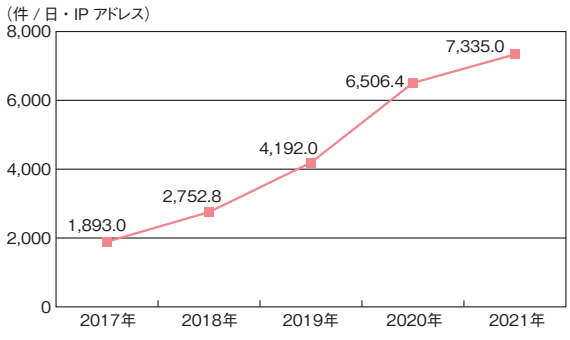
具体的には、2020 年度に引き続き、総務省を装った偽の特別定額給付金申請サイトへの誘導メールに関する注意喚起※128、ワクチン接種予約を装ったフィッシングに関する注意喚起※129、ネット通販サイトの e コマース、通信事業者、クレジット会社等を装ったフィッシングサイトが多数観測されたことへの注意喚起等を JC3 の Web サイト等で実施した※130。

(2) 2021 年のサイバー攻撃の情勢

警察が把握する 2021 年のサイバー攻撃の情勢について述べる。

(a) リアルタイム検知ネットワーク

警察庁では、インターネットとの接続点にセンサーを設置してリアルタイム検知ネットワークシステム※131 を 24 時間体制で運用し、通常のインターネット利用では想定されない接続情報等を検知、集約・分析している。本システムが検知するアクセスの大半は、不特定多数の IP アドレスを対象とするサイバー攻撃やネットワークに接続された機器の脆弱性を探索するサイバー攻撃の準備行為とみられている。2021 年に本システムで検知した不審なアクセス件数は、1 日・1IP アドレス当たり 7,335.0 件（前年比 12.7% 増）で、右肩上がりで増加している（図 2-1-11）。検知したアクセスの送信元は大半が海外であり、海外からのサイバー攻撃等の脅威が高くなっていることが分かる。



■図 2-1-11　サイバー空間における探索行為等とみられるアクセス件数
（出典）警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

また検知したアクセスの宛先ポートも、主として IoT 機器が標準設定で使用するポート番号 1024 以上のポートへのアクセス件数が特に増加しており、2017 年比で 7.1 倍となっている。普及する IoT 機器の脆弱性に対する探索行為であるとみられている※132。

(b) サイバー攻撃への警察の取り組み

サイバー攻撃に対して警察は以下の取り組み等を実施した。

- 海外の捜査当局からの警察庁への情報提供に基づき、総務省と連携し、国内の Emotet に感染している機器の情報をインターネットサービスプロバイダ（ISP：Internet Service Provider）に提供した。また ISP 経由で機器の利用者への注意喚起を実施した。
- 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警察が把握した国内 C&C サーバの機能停止（テイクダウン）を、サーバの運営事業者等に働きかけた。運営事業者に対し、不正な蔵置ファイルの削除を依頼する等により無害化措置を実施した結果、27 件の C&C サーバの機能が停止した。
- 電力事業者、自治体、金融機関等重要インフラ事業者等とのサイバー攻撃の発生を想定した共同対処訓練を継続的に実施した。

(3) 2021 年のサイバー犯罪の情勢等

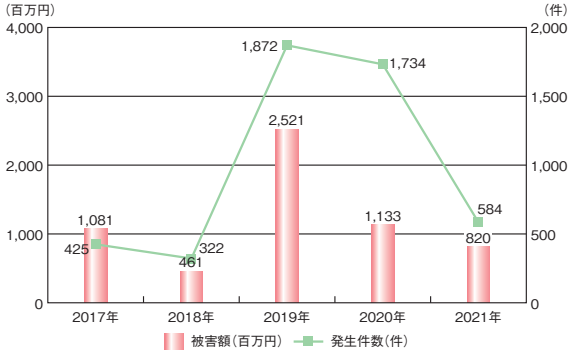
警察が 2021 年に認知したサイバー犯罪の情勢等について述べる。

(a) サイバー犯罪の情勢

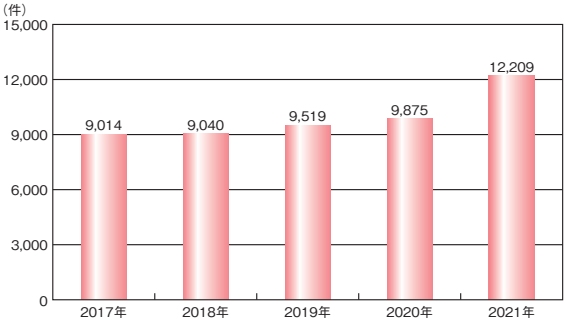
主なサイバー犯罪の情勢について以下に述べる。

- フィッシング等に伴う不正送金・不正利用

「インターネットバンキングに係る不正送金事犯」としては、SMS 等を用いて金融機関等を装ったフィッシングサイトへ誘導する手口のほか、インターネット上のメモアプリ等に保存していたネットバンキングの ID、パスワード等が、同アプリ等への不正アクセスから窃取され不正送金に使用されたと思われるケースが確認されている。インターネットバンキングに係る不正送金事犯による被害が集中している金融機関に対して、警察からはモニタリングの強化、認証手続きに関するセキュリティの強化、利用者への注意喚起の強化等を重点的に実施してきた。2019 年に増加した発生件数、被害額はともに 2 年連続で大きく減少した（次ページ図 2-1-12）。他方、既述の JC3 の注意喚起では、フィッシングのターゲットが従来の銀行等の金融機関から、クレジットカード情報や各種 EC サイトのアカウント情報へと変化して



■図 2-1-12　インターネットバンキングに係る不正送金事犯
(出典)警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集



■図 2-1-13　サイバー犯罪の検挙件数
(出典)警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

いる、と分析している。

これらに対し警察は、不正送金組織、口座売買組織の検挙等のほか、金融機関とのサイバー犯罪防犯情報連絡会議等の連携強化、メモアプリ提供事業者に対する被害防止対策の要請や各種注意喚起を実施している。

- 不正商品購入事犯

  2020 年 9 月に確認されたスマートフォン決済サービスを使った不正商品購入の事犯では、2021 年 6 月までに男女 8 人を詐欺等で検挙した。不正に使われたスマートフォン決済サービスに関して、サービス事業者と業務提携する金融機関に開設された口座情報を不正に入手し、振替を行う手口について、金融庁及び関係団体に情報提供するとともに不正防止対策強化の要請を実施した。

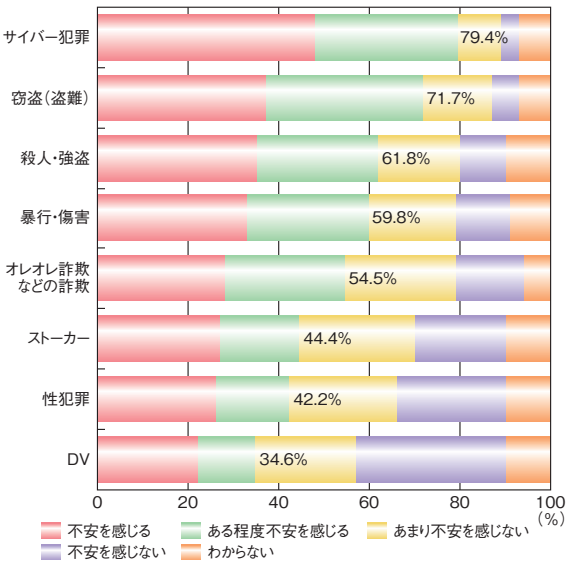
- SMS 認証代行

  二要素認証等において本人確認として使われている SMS 認証を不正に代行する「SMS 認証代行」について、特殊詐欺等に必要な犯行ツールを提供する犯罪インフラにもなりうる懸念から、総務省と連携し、業界団体に対して SMS 機能付きデータ SIM 契約時の本人確認の強化を要請した。併せて都道府県警察に対し、法令に違反する悪質事業者の取り締り強化を図った[※133]。

(b) 検挙件数

警察庁長官官房が公開している「令和 3 年の犯罪情勢[※132]」によると、国内の犯罪情勢を測る指標のうち、刑法犯認知件数の総数は、2003 年以降一貫して減少しており、2021 年は戦後最少を更新している。一方で、サイバー犯罪の検挙件数は 2020 年まで 1 万件弱で推移していたが、2021 年は 1 万 2,209 件に上り、前年から大きく増加した(図 2-1-13)。

2021 年 11 月に警察庁長官官房が実施した犯罪情勢に関するアンケート調査(全国の 15 歳以上の男女 5,000 人を対象)によると、サイバー犯罪に遭うことへの不安感をもっているとの回答が 79.4%(2020 年は 75.3%[※134])となり、その他の犯罪(窃盗、暴行、殺人、詐欺等)を抑え、第一位となっている(図 2-1-14)。同調査で過去 1 年間にサイバー犯罪の被害に遭った、または遭う恐れのある経験をしたとの回答は 35.9% に上る。また、ここ 10 年で日本の治安が悪くなったと思うとした回答が 64.1%、その要因として 57.1% の方がサイバー犯罪を上げている[※132]。国民のサイバー空間に対する不安感は年々高まっている。警察等の公的な機関が必要な役割を果たし、サイバー空間において実空間と同じく安全・安心の確保を図っていくことが求められている。



■図 2-1-14　犯罪に遭うことに関する不安感
(出典)警察庁「令和 3 年の犯罪情勢」を基に IPA が編集

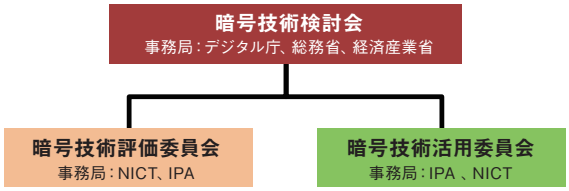
2.1.5 CRYPTRECの動向

電子政府の情報セキュリティを確保するため、デジタル庁、総務省、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※135）の安全性を評価、監視し、暗号技術の適切な実装法や運用法を調査、検討している。

(1) 2021年度の体制

CRYPTRECは、デジタル庁と総務省、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2-1-15）。



■図2-1-15　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。
- 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、暗号技術の技術的信頼に関する検討を担当する。傘下には、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「耐量子計算機暗号（PQC：Post-Quantum Cryptography）」に関するガイドラインを作成する「暗号技術調査ワーキンググループ（耐量子計算機暗号）」と、従来の暗号技術では実現できないような機能を持つ「高機能暗号」に関するガイドラインを作成する「暗号技術調査ワーキンググループ（高機能暗号）」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。傘下には、2020年度に公開した「暗号鍵管理システム設計指針（基本編）※136」のガイダンスを作成する「暗号鍵管理ガイダンスワーキンググループ」が設置されている。

(2) 2021年度の主な活動

2021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

2021年度には、各委員会の2021年度活動計画、及び活動報告の審議が行われ、承認された。更に、以下の項目についても審議が行われ、承認された。

- 推奨候補暗号リストから電子政府推奨暗号リストへの昇格基準となる「暗号利用実績に関する選定基準」
- 電子政府システムの調達・開発にあたって、調達要件や開発要件として採用すべき「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」
- 鍵長の選択方法や暗号鍵の設定に関する一般的なガイダンスを提供する「暗号鍵設定ガイダンス」
- デジタル署名EdDSA（Edwards-curve Digital Signature Algorithm）※137の推奨候補暗号リストへの追加

(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、2021年度の主な活動内容・成果は以下のとおりである。

- デジタル署名EdDSAの実装性能調査
  デジタル署名EdDSAについて、2020年度の安全性評価に引き続き、2021年度は実装性能評価を実施した。その結果、EdDSAの実装上の特徴は、いずれも実装性能として有益であると考えられ、楕円曲線DSA（ECDSA：Elliptic Curve Digital Signature Algorithm）と比較しても遜色ない十分な実装性能を有していると判断した。

- 軽量暗号に関する技術動向調査
  2020 年度第 2 回暗号技術検討会での了承に基づき、2021 年度は、2016 年度に作成した「CRYPTREC 暗号技術ガイドライン（軽量暗号）」の更新のため、2017 年度以降の技術動向調査を実施した。特に、2016 年度ガイドラインで紹介された暗号方式を中心とした代表的な軽量暗号に対して、2021 年 9 月時点で脅威につながる脆弱性が指摘されているか否かを 3 段階で分類した。今後は、NIST Lightweight Cryptography コンペティションファイナリスト※138 を対象とした安全性及び実装性能に関わる調査・評価を実施し、新規情報を追加・更新した文書を 2023 年度版ガイドラインとして公開する予定である。
- 暗号技術調査ワーキンググループの活動
  2020 年度第 2 回暗号技術検討会での了承に基づき、2021 年度は、耐量子計算機暗号に関するガイドライン、及び高機能暗号に関するガイドラインを作成するために、耐量子計算機暗号を検討するワーキンググループと高機能暗号を検討するワーキンググループを設置し、それぞれの研究動向を調査している。2022 年秋まで調査を継続し、その結果を踏まえ、2022 年度中にこれらのガイドラインを作成する予定である。この活動に加え、主要な公開鍵暗号（RSA 暗号、楕円曲線暗号）の安全性の根拠となる「素因数分解問題」と「離散対数問題」の困難性に関して、CRYPTREC が公開している「予測図」の改訂も行った※139。

(c) 暗号技術活用委員会

2021 年度の主な活動内容・成果は以下のとおりである。

- 暗号利用実績に関する選定基準の検討
  暗号利用実績に基づく選定基準（選定ルール）は、2012 年度の CRYPTREC 暗号リスト改定の際に初めて導入されたものである。2021 年度の委員会では、2012 年以降の暗号アルゴリズムをめぐる状況変化を踏まえて選定基準の見直しを行った。その結果、電子政府推奨暗号リストへの昇格のための明確な選定基準・閾値は設けず、本基準で示す考慮項目を参考に実際の昇格判断は個々の状況を鑑みて個別に行うものとする基準案を取りまとめた。
- 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準の検討
  暗号の安全性は暗号アルゴリズムと鍵長の組み合せにより決まるものであるが、今までの CRYPTREC 暗号リストでは鍵長の取り扱いは規定していなかった。そのため、今回、CRYPTREC 暗号リストに掲載されている暗号技術を利用する際に、適切なセキュリティ強度を実現するためのアルゴリズム及び鍵長の選択方法を規定するものとして本基準を作成した。具体的には、電子政府システムを調達または開発する際は、そのシステムの運用寿命全体と、その期間に実現するセキュリティ強度の関係を考慮してセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズムと鍵長の組み合せを調達・開発要件とするように定めている。
- 暗号鍵設定ガイダンスの検討
  暗号技術を利用する際の鍵長の選択方法に関する一般的な考え方のガイダンスとして作成した。具体的には、暗号鍵を安全に設定し、運用していくために考慮すべき項目として、暗号鍵の鍵長についての考え方、暗号鍵のライフサイクル等について解説している。なお、本ガイダンスでは、実際の利用用途や利用期間、環境、コスト、その他様々な制約条件を踏まえて、読者が必要なセキュリティ強度を決めるスタイルを採用している。
- 暗号鍵管理ガイダンスワーキンググループの活動
  情報を安全に取り扱うためには、通信データや保管情報の暗号化に使う暗号アルゴリズムのみに注意を払うだけでは不十分であり、その暗号アルゴリズムに用いられる暗号鍵の管理が適切に行われる必要がある。そこで、2020 年に公開した「暗号鍵管理システム設計指針（基本編）」に引き続き、暗号鍵管理についてのガイダンスを作成するため、暗号鍵管理ガイダンスワーキンググループを設置した。具体的には、情報システム設計者やシステム調達者が暗号鍵管理を適切に扱えることを目的とし、暗号鍵管理で必要となる項目について、シンプルなモデルを例示しつつ、鍵管理における要求や思想が理解できるような記載を目指している。2021 年度は、ガイダンス作成に向けた執筆方針の方向性を取りまとめ、2022 年度中に暗号鍵管理ガイダンスとして完成させる予定である。

COLUMN

デジタル庁が進めるシステム検証とは?

2021年9月1日に、日本のデジタル社会実現の司令塔としてデジタル庁が発足し、注目されています。2021年12月24日には、目指すべきデジタル社会の実現に向けて、政府が重点的に実施すべき施策として、「デジタル社会の実現に向けた重点計画[i]」が閣議決定されました。これは、各府省庁が構造改革や個別の施策に取り組み、それを世界に発信・提言する際の羅針盤となるものです。

この計画では、デジタル社会を形成するための基本原則として、「オープン・透明」「公平・倫理」等10原則を掲げていますが、その中の一つが「安全・安心」です。デジタル改革を進めるに当たって、政府機関・独立行政法人等のサービスにおける国民目線に立った利便性の向上の徹底と、国民への行政サービス等を安定して安全に提供するためのサイバーセキュリティの確保の両立が不可欠であることから、サイバーセキュリティ戦略に基づき、政府全体として同戦略を踏まえた施策を着実に講じていくことにより、サイバーセキュリティの強化に努めることを宣言しています。

その具体的な施策の一つとして、デジタル庁が整備・運用するシステム等の安定的・継続的な稼働の確保等の観点から「システム検証・監査」を実施することとし、その実施体制をデジタル庁とIPAが共同して構築することが記されています。「システム検証」という言葉は、「システム監査」と比べて少し聞きなれないかもしれません。あえて「検証」という言葉を使っているのは、各情報システムがデジタル庁の示す情報システム整備方針に沿った整備・運用を行っているかどうか、という適合性を確認することを主眼としているからです。もちろん確認手段等は「監査」と重なる部分も多いのですが、方針への適合性というより広い視野からの確認を行うことになります。また、この「システム検証」は、NISC・IPAによる府省庁・独立行政法人等へのセキュリティ監査のような第三者による外部監査ではなく、あくまでデジタル庁の内部監査的な位置付けとして実施される予定であることも特徴の一つです。新型コロナウイルス接触確認アプリ「COCOA」における不具合は記憶に新しいところですが、開発チームと独立した検証チームを内部に持つことによって、外部監査よりも迅速かつ柔軟な対応が可能となることが期待されます。

この「システム検証」は、まず2022年度以降、「①デジタル庁システム」(各府省庁が共通で利用する基盤を含む)を中心にスタートし、更に、2023年度以降は、「②デジタル庁・各府省共同プロジェクト型システム」も対象とする予定で、IPAもその一翼を担う組織として取り組みます。

i https://www.digital.go.jp/policies/priority-policy-program/〔2022/5/23確認〕

2.2 国外の情報セキュリティ政策の状況

サイバー脅威は国境を問わず、あらゆる国・地域の脆弱なシステムに対して攻撃が仕掛けられる。また、IT化した社会サービスやそれを支えるサプライチェーンは国境を越えてつながり合い、他国におけるサイバー脅威が自国に深刻な影響を与える可能性がある。更に近年、国家の支援を受けた攻撃者による他国へのサイバー攻撃・虚偽情報流布等の脅威が現実になっている。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。なお、米国・欧州については「3.4 米国・欧州の情報セキュリティ政策」を参照されたい。

2.2.1 国際社会と連携した取り組み

2020 年度に引き続き、日本政府は 2021 年度も米国、欧州、インド、ASEAN 諸国等とのサイバーセキュリティに関する連携協議や演習を実施した。それらの活動から主な取り組みを紹介する。2021 年度の傾向として、新型コロナウイルス感染対策に関する国際連携が引き続き重要課題となったが、2022 年 2 月 24 日、ロシアのウクライナ侵攻が勃発、侵攻拡大阻止、ウクライナ政府・避難民の支援、対ロシア経済制裁等に関する国際連携が日本政府にとっても大きな課題となった。サイバーセキュリティの観点では、サイバー戦への対策・ウクライナ支援も国際的な課題となった。

(1) 各国首脳・国際機関との連携

新型コロナウイルスは 2021 年に入っても猛威を振るい、2021 年 6 月以降は感染力の強い変異種デルタ株、同年 11 月以降は更に感染力の強いオミクロン株が世界的に流行した。日本・米国・欧州諸国等は 3 回にわたるワクチン接種や数度のロックダウン等、対応に追われた。

(a) 2021 年 6 月の G7 首脳会合

2020 年度にオンライン形式で開催された G7 首脳会合は 2021 年 6 月 11 ～ 13 日、英国コーンウォール州カービス・ベイにて対面形式で開催された※140。全体テーマはコロナ禍からの「より良い回復」とされ、経済面の回復では、開かれた世界におけるデジタル化、グリーン化、ジェンダー平等、サプライチェーン脆弱性への対処等の方向性が示された。また「より強靭な回復」に向けた議論において、2020 年に引き続き中国に対する懸念が示され、市場の公平性・透明性の担保、人権・自由の尊重、領土問題に関する力による現状変更への反対等も、盛り込まれた。また 2020 年に引き続きワクチン接種等に関する途上国支援が、更に 2021 年の新提案として地球温暖化対策（エネルギーイノベーション）の推進が合意された。

G7 首脳会合で例年議論され、声明が出される「自由でオープンなサイバー空間」の維持に関しては、上記の議論を反映し、2021 年度はより広範な「開かれた社会」を目指す声明が出された※141。同声明には、デジタル、人権、ジェンダー、自由、オープン性・透明性を持つ多国間システム等に加え、ワクチン接種を含む課題への協働、持続可能な開発目標（SDGs：Sustainable Development Goals）の達成支援等が含まれている。

なお、菅義偉首相（当時）は、東京 2020 オリンピック・パラリンピック競技大会の安全・安心な開催の決意を示し、G7 首脳の同意を得た。

(b) 2022 年 3 月の G7 首脳会合・外相会合

2022 年 2 月 24 日、ロシアのウクライナ侵攻が開始された。これに対し G7 首脳は同日に緊急のテレビ会議※142を実施、3 月 12 日に首脳声明を発表し、Vladimir Putin ロシア大統領への非難、侵攻の即時停止と被害者の救済、ロシアへの制裁、ウクライナの支援について団結し合意したことを示した※143。具体的な制裁として、ロシアの最恵国待遇はく奪、多国籍金融機関のロシア融資停止、Putin 政権関係者の資産凍結支援、重要物品・技術の輸出入制限、侵攻関係組織の資金調達制限等が明記された。

更に 2022 年 3 月 24 日、緊急の G7 首脳会合がベルギー・ブリュッセルで開催され、Volodymyr Zelenskyy ウクライナ大統領がオンラインで参加、更なる支援を呼びかけた※144。同会合の首脳声明では、3 月 12 日の首脳声明で明記された金融・経済制裁の強化・ウクライナ支援に加え、原子力施設の安全や核兵器・生物化学兵器使用への懸念、ウクライナのサイバー防御支援・難民支援、ロシア政府の欺瞞的情報統制への非難、エネルギー・食料サプライチェーンの脱ロシアに向けた再

構築、等が盛り込まれた。

侵攻開始1ヵ月のうちに、G7首脳レベルでこのような一枚岩の団結がなされたことは大きなインパクトがあったと思われる。日本政府は、天然ガスや小麦等の供給をロシア・ウクライナに依存しているという課題を抱えながらも、侵攻に対して断固とした態度を取ることを決定している※145。

(c)オリンピック開催と期間中の首脳・外相会談

東京2020オリンピック・パラリンピック競技大会は、デルタ株流行の厳しい状況下となったが、2021年7月23日～9月5日、無観客・感染対策徹底という厳戒態勢のもとに開催された。期間中のセキュリティに関しては、NISCが運用した対処調整センターが観測情報75件、脅威情報32件を関係組織に提供したほか※146、協力通信事業者が4.5億回に上る不審イベントを検知・遮断し、大会運営に影響するインシデントは発生せず、全競技を無事終了した※147。

オリンピック期間中は各国首脳・外相との会談が集中的に行われた。菅首相は11ヵ国（米国・エストニア・フランス・アルメニア・スイス・コソボ・ポーランド・モンテネグロ・トルクメニスタン・モンゴル・南スーダン）の首脳と会談（電話会談を含む）、法の支配に基づく自由で開かれたインド太平洋地域や通商・デジタル化に向けた連携を強化すること等を合意した。また、茂木敏充外相（当時）も6ヵ国（フィンランド・カナダ・アゼルバイジャン・アンティグア-バーブーダ・コソボ・米国）の外相・大統領と会談（電話会談を含む）、上記課題のほかコロナ対策・人権等についても連携を確認した※148。

(d)日米豪印4ヵ国の連携

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

2021年9月24日、第2回日米豪印首脳会合がワシントンD.C.で開催され、菅首相、Scott Morrisonオーストラリア連邦首相（Prime Minister of the Commonwealth of Australia）、Narendra Modiインド首相（Prime Minister of India）、Joseph Biden米国大統領が出席した※149。同会談では。2020年の4ヵ国外相会談に引き続き、法の支配に基づく「自由で開かれたインド太平洋」の実現に向けた連携で合意するとともに、ASEAN諸国による取り組みである「インド太平洋に関するASEANアウトルック」を支持し、EUの「インド太平洋における協力のための戦略」も歓迎した。また、ワクチンを含むコロナ対策、気候変動、海洋安全保障、テロ対策、サイバーセキュリティ、人道支援・災害救援等の分野での4ヵ国の協力進展を歓迎し、宇宙、サイバーの分野で作業部会等を立ち上げるとともに、クリーン・エネルギー、人的交流の分野でも協力を強化することで一致した。

(e)国際連合によるサイバー脅威対策推進

2021年5月24～28日、サイバーセキュリティに関する第6会期国連政府専門家会合（GGE：the Group of Governmental Experts）最終会合が開催され、日本から赤堀毅国連・サイバー政策担当大使（総合外交政策局審議官）ほかがオンラインで出席した※150。同会合では、サイバー空間における責任ある国家の行動に関し、2015年のGGE報告書に記載された11個の規範への拘束力のある義務追加の可能性、サイバー空間への国際法、国連憲章の適用、紛争解決のための信頼醸成、能力構築等に関する共通認識を取りまとめた。この結果は報告書として2021年9月の第76回国連総会に提出された。

同報告はサイバー空間の各国の行動に国際法や国連憲章が適用されることとし、違反行為に対する加盟国の責任ある行動を求めた点が特徴である。なお日本政府はサイバー行動に適用される国際法に関する基本的な立場を公表している※151。

続いて2021年11月13～17日、サイバーセキュリティに関する国連オープン・エンド作業部会（OEWG 2021-2025：the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025）第1回会合が開催された。OEWGは全加盟国のサイバーセキュリティに関する協議の場として2019年に設置され、2021年3月に報告書を採択していた（「情報セキュリティ白書2021」の「2.2.1(1)(c)国連によるサイバー脅威対策推進」参照）。第75回国連総会決議により、改めて2025年までの活動が決まったものである。同会議では、日本から有馬裕サイバー政策担当大使（総合外交政策局審議官）がビデオメッセージで参加、前述のGGE報告に記載された国際法の適用等の重要性を強調した。

(2)2国間連携の取り組み

「2.2.1(1)(c)オリンピック開催と期間中の首脳・外相会談」で見たとおり、2021年の2国間首脳協議・閣僚

級協議は東京 2020 オリンピック・パラリンピック競技大会期間中に集中的に行われた。以下では、それ以外で行われたサイバーセキュリティ、及びサイバーを含む安全保障に関する 2 国間協議について述べる。

(a)日英サイバー協議

2021 年 6 月 29 日、第 6 回日英サイバー協議がオンライン形式で開催された※ 152。日本からは赤堀審議官、英国からは William Middleton 外務連邦開発省サイバー政策部長（Director Cyber, National Security Directorate, Foreign, Commonwealth and Development Office）を始めとする両国関係省庁の代表者が出席した。

協議においては、2020 年開催の第 5 回に引き続き、サイバー分野における脅威と施策の共有、国際連携、能力構築支援、サイバー強靭性等について議論を行った。

(b)日エストニア・サイバー協議

2021 年 12 月 22 日、第 4 回日エストニア・サイバー協議がオンライン形式で開催された※ 153。日本からは有馬審議官、エストニアからティルマー・クラール外務省サイバー外交担当大使を始めとする両国関係省庁の代表者が出席した。

協議においては、最近のサイバー環境やサイバー分野における両国の施策について意見を交換するとともに、国連の GGE、OEWG の活動等に関する 2 国間連携について討議を行った。

(c)日米安全保障協議委員会

2021 年 3 月 16 日、東京において日米安全保障協議委員会（日米「2 + 2」）が開催され、日本から茂木外務大臣と岸信夫防衛大臣、米国から Antony Blinken 国務長官（Secretary of State of the United States）、Lloyd Austin 国防長官（Secretary of Defense of the United States）が参加した※ 154。同委員会では、中国・北朝鮮情勢に関する地域安全保障及び人権上の懸念と日米豪印 4 ヵ国による連携強化、宇宙・サイバー領域の協力を含む防衛体制強化が議論された。

同委員会は更に 2022 年 1 月 7 日、オンライン形式で開催され、日本からは第 2 次岸田内閣で着任した林芳正外務大臣、岸防衛大臣が出席した※ 155。同会議では、地域安全保障に関しては引き続き中国・北朝鮮対応が最重点となったが、新たにウクライナ情勢の注視が盛り込まれた。また防衛体制については、サイバー領域における自衛隊の体制強化、宇宙における「責任ある行動」の確保に関する両国の連携強化等が議論された。

「責任ある行動」の重視は、国連 GGE や OEWG の活動（サイバー空間における国際法の適用）と連動したものと考えられる。

(d)日米首脳会談

2021 年度は日米首脳会談が 2 回開催された。1 回目は 2021 年 4 月 16 日、ワシントン D.C. にて菅首相と Biden 大統領との会談が行われた※ 156。同会談で、両国は「持続可能な、包摂的で、健康で、グリーンな世界経済の復興」のため、デジタル経済の促進、脱炭素化、健康安全保障等において協力することで合意したほか、「自由で開かれたインド太平洋と包摂的な経済的繁栄の推進」のために同盟を強化するとし、「台湾海峡の平和と安定」を重視することが明記された。

更に 2022 年 1 月 21 日、岸田文雄首相が Biden 大統領とテレビ会談を行った※ 157。同会議では、2021 年 4 月の首脳会談、及び 2022 年 1 月の日米「2+2」会議の合意が再確認されたほか、ウクライナへのロシアの侵攻抑止に関する連携が日米間で初めて言及された。また、経済連携強化のための日米経済政策協議委員会（経済版「2+2」）の設置が合意された。

(e)日 EU 定期首脳協議

2021 年 5 月 27 日、第 27 回日 EU 定期首脳協議がテレビ会議形式で開催された。日本からは菅首相、EU からは Charles Michel 欧州理事会議長（President of the European Council）及び Ursula von der Leyen 欧州委員会委員長（President of the European Commission）が参加した※ 158。

同会議では、新型コロナウイルス終息後の経済復興、高信頼通信インフラの整備、強靭なサプライチェーン構築、安全保障上の観点からの海外投資等、中国の台頭を意識した討議が行われた。

(3)アジア太平洋地域のサイバー連携

アジア太平洋地域における政府レベルの連携施策について述べる。CSIRT に関する連携施策については、「2.2.2 アジア太平洋地域での CSIRT の動向」を参照されたい。

(a)日 ASEAN 首脳会議

2021 年 10 月 27 日、第 24 回日 ASEAN 首脳会議

がオンラインで開催された。Haji Hassanal Bolkiah ブルネイ国王陛下（His Majesty Sultan）が議長を務め、日本からは岸田首相がオンライン形式で参加した※159。岸田首相は「自由で開かれたインド太平洋」の推進を強調し、新型コロナ対策支援、及びASEAN独自の構想「インド太平洋に関するASEANアウトルック」（AOIP：ASEAN Outlook on the Indo-Pacific）の推進等について説明を行った。また、2020年の第23回首脳会議に引き続き、サイバーセキュリティに関する連携強化が議長声明に盛り込まれた。

(b) ASEAN地域フォーラム

ASEAN地域フォーラム（ARF：ASEAN Regional Forum※160）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、2021年4月28日、サイバーセキュリティに関する第3回ARF会期間会合がオンライン形式で開催され、日本からは赤堀審議官が参加した※161。同年1月に行われた第6回専門家会合に引き続き、国際的なサイバーセキュリティ環境や各国・地域の取り組み、今後取り組むべき信頼醸成措置について議論が行われた。また、その結果を信頼醸成と予防外交に関する会期間グループ会合（ISG on CBMs and PD）で報告することを確認した。

(c) 日・ASEANサイバーセキュリティ政策会議

2021年10月21日、第14回日・ASEANサイバーセキュリティ政策会議がオンライン形式で開催された※162。議長国は日本、ラオスが務め、日本、ASEANのサイバーセキュリティ・情報通信所管省庁の代表が参加した。同会議では、第13回会議で合意された10項目の協力活動（演習、重要インフラ防護、意識啓発、能力構築、インシデント時情報共有、産学連携等）の状況を確認し、今後の協力を検討した。また、メール等の情報連絡演習や、オンライン会議時のインシデント対応演習等についても活発な意見がかわされた。更に能力構築については、AJCCBCや、次項で述べる「インド太平洋地域向け日米EU産業制御システムサイバーセキュリティウィーク」の研修・演習内容が紹介された。

(d) インド太平洋地域に向けたサイバー演習

日本政府はサイバーセキュリティ能力構築支援の一貫として、インド太平洋地域のサイバー演習を推進している。2021年10月25～29日、経済産業省とIPAは米国政府及び欧州委員会（European Commission）と連携し、インド太平洋地域の重要インフラ事業者、National CSIRT等のIT/OTセキュリティ担当者等を対象に、「インド太平洋地域向け日米EU産業制御システムサイバーセキュリティウィーク」を実施した※163。同演習は、リモートによる模擬プラント操作、日米EUの専門家によるワークショップ・セミナー等により参加者の能力向上を目指す内容である。なお、2021年3月の演習については「3.1.4 (1) 日本政府の取り組み」を参照されたい。

(4) セキュリティ連携に関する国際会議

サイバーセキュリティの国際連携に関する主な会議として、2021年度は、2020年度に引き続き「サイバーセキュリティ国際シンポジウム」「サイバー・イニシアチブ東京」が開催された。

(a) 第11回サイバーセキュリティ国際シンポジウム

本シンポジウムは、サイバー脅威対応に向けた国際間の信頼構築を討議する場として、2016年から日本で開催されている。2021年は慶應義塾大学、大学間の国際連携組織INCS-CoE（InterNational Cyber Security Center of Excellence）、The MITRE Corporation※164の共催の形を取り、10月25～29日にオンラインで開催された※165。米国・英国・オーストラリア・イスラエル大使館及び駐日欧州連合代表部を始め、関係国の省庁が後援し、各国の有識者が参加した。

Global sessionでは、日本政府から平井卓也前デジタル大臣がビデオにより講演し、基調パネルでは、多国間サイバーセキュリティ行動委員会（MCAC：Multilateral Cybersecurity Action Committee）によるナショナルセキュリティにおける国際連携、あるいは相互承認（Mutual Recognition）や信頼性のある自由なデータ流通（DFFT: Data Free Flow with Trust）による社会セキュリティ等がテーマとなり、参加各国の有識者が討議を行った。2020年度に引き続き、産学主導による国際間の信頼構築討議の場となり、政府主導のイベントでありがちな「オープンで自由なサイバー空間」のキャンペーンとは一線を画したものとなった。

(b) サイバー・イニシアチブ東京2021

国内外のセキュリティ・IT専門家を招いたサイバー・イニシアチブ東京2021が、2021年11月29～30日にオンラインで開催された※166。第4回となる同イベントの主

要議題は、社会のデジタル変革におけるセキュリティの実装（デジタル・セキュア社会の実現）とされ、日本政府からは金子恭之総務大臣、萩生田光一経済産業大臣、小田原潔外務副大臣、岸防衛大臣が、台湾政府からはAudrey Tangソーシャルイノベーション担当デジタル大臣（Digital Minister in charge of Social Innovation）が講演したほか、各国の閣僚・有識者が講演・パネル討議に参加した。

また、東京2020オリンピック・パラリンピック競技大会のセキュリティ対策の成果について、坂明デジタル庁CISO（Chief Information Security Officer：最高情報セキュリティ責任者）他の有識者がパネル討議を行ったことも注目された。

2.2.2 アジア太平洋地域でのCSIRTの動向

2021年、ランサムウェアを用いたサイバー攻撃が世界各地で相次ぎ、またEmotetの感染再拡大が確認され、これらの動向はアジア太平洋地域においても深刻な脅威となっている。こうした攻撃による被害拡大を防ぐための対策情報の共有や、被害を受けた後の復旧支援等、インシデント対応連携の窓口となるCSIRTが果たす役割は大きくなっており、各国ではCSIRTの体制や情報連携の強化が進んでいる。本項では、主にアジア太平洋地域におけるCSIRTの設立や機能強化に関する動き、CSIRT間の相互連携の実態について述べる。

(1) CSIRTの設立・機能強化の動き

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

(a) オーストラリア

2021年4月21日、オーストラリア政府は「国際サイバー・重要技術エンゲージメント戦略（International Cyber and Critical Technology Engagement Strategy）」を発表した※167。本戦略は、オーストラリア、インド太平洋地域及び世界の安全と繁栄を、サイバー空間と重要技術の強化推進によって実現することを目指し策定されたものである。また本戦略は、サイバーと重要技術の諸問題に関して、オーストラリア政府が信頼のおける影響力のあるリーダーとして国際的な評価を得るための戦略的アプローチを示しており、より厳しさを増す国際環境を乗り切るために、サイバー能力の向上及び重要技術の開発や活用を促進するような外交を強化しなければならないと述べている。本戦略における重要技術とは、オーストラリアの繁栄、社会的結束、国家安全保障等の国益を大幅に向上させる、あるいは損なう可能性のある技術と定義されており、人工知能（AI）、5G、IoT、量子コンピューティング、サイバーセキュリティ等が含まれる。サイバーセキュリティに関しては、National CSIRTの機能を担うACSC（Australian Cyber Security Centre）がPaCSON（Pacific Cyber Security Operational Network）や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）等の地域のパートナーと協力し、信頼できるサイバー脅威情報共有ネットワークの構築に取り組んできたことを踏まえて、運用面及び技術面から深刻なサイバーセキュリティの課題に効果的に対処できるよう、ガイダンスや脅威に関するアドバイスを提供していくとしている。また、近隣国であるトンガやバヌアツ、サモア、フィジー、ソロモン諸島のCSIRTやセキュリティ運用センターへのインシデント対応支援を行うことで、地域の集合的なサイバーセキュリティを強化していくとしている。

(b) ニュージーランド

2021年8月16日、ニュージーランド首相内閣府に設置された国家セキュリティグループ（NSG：National Security Group）が「サイバーセキュリティ緊急対応計画（CSERP：Cyber Security Emergency Response Plan）」の第5版を発行した※168。2013年に第1版が発行された後、変化する情勢に応じて、またインシデントからの教訓を反映する形で更新されている。本計画は、サイバーセキュリティに関する緊急事態が起きた際の、政府の対応の枠組みを定めたガイダンスである。緊急を要するインシデントが起きた際は、CERT NZ（Computer Emergency Response Team New Zealand：ニュージーランドコンピュータ緊急対応チーム）及びNCSC（National Cyber Security Centre）がインシデントの重大性を評価し、「深刻」や「重大」等4段階に分類するよう定めている。「深刻」とされたインシデントの場合には、ODESC（Officials Committee for Domestic and External Security Coordination：国内外のセキュリティ調整のための政府委員会）等の設置を含む国家安全保障システムが発動される。「重大」とされたインシデントの場合には、状況に応じてCERT NZ、首相内閣府、NCSC、警察等が、サイバーセキュリティ緊急調整グループを構成して対応にあたることを定めている。

(c)シンガポール

2021年10月5日、National CSIRTであるSingCERT（Singapore Computer Emergency Response Team）を管轄するCSA（Cyber Security Agency：サイバーセキュリティ庁）が「サイバーセキュリティ戦略2021（The Singapore Cybersecurity Strategy 2021）※169」を発表した。同戦略では、「レジリエントなインフラの構築」「より安全なサイバースペースの実現」「国際的なサイバー協力の強化」の三本の戦略的柱を掲げ、それぞれの柱が詳細に述べられている。また、サイバーセキュリティの基礎として「活発なサイバーセキュリティエコシステムの構築」と「強固なサイバー人材供給力の育成」を挙げている。国際的なサイバー協力の強化の項目では、CSIRTネットワークへの積極的な参加と緊密な連携等を通じて、地域及び国際的なパートナーとの多国間協力を強化するとしている。CSAは、毎年ASEANを対象としたサイバーインシデント演習（ACID：ASEAN CERT Incident Drill）を開催し、情報共有メカニズムの強化を行う等、国境を越えたサイバー脅威に立ち向かうために、地域のパートナーとの連携に取り組んでいる。

(d)サモア

2021年5月にSamCERT（Samoa National Computer Emergency Response Team：サモア国家コンピュータ緊急対応チーム）がMCIT（Ministry of Communications and Information Technology：通信情報技術省）の傘下に設立された※170。サイバー攻撃やインシデントに際しては、これまでSMPP（Samoa Ministry of Police and Prisons:サモア警察刑務所省）が報告を受け付け、MCITが支援を行う体制であったが、今後はSamCERTが窓口となってすべてのインシデントに関して報告を受け付け、インシデントが起きた民間企業や非政府組織（NGO：Non-Governmental Organization）、政府機関、及び学術機関と連携して対応するとしている※171。

(e)タイ

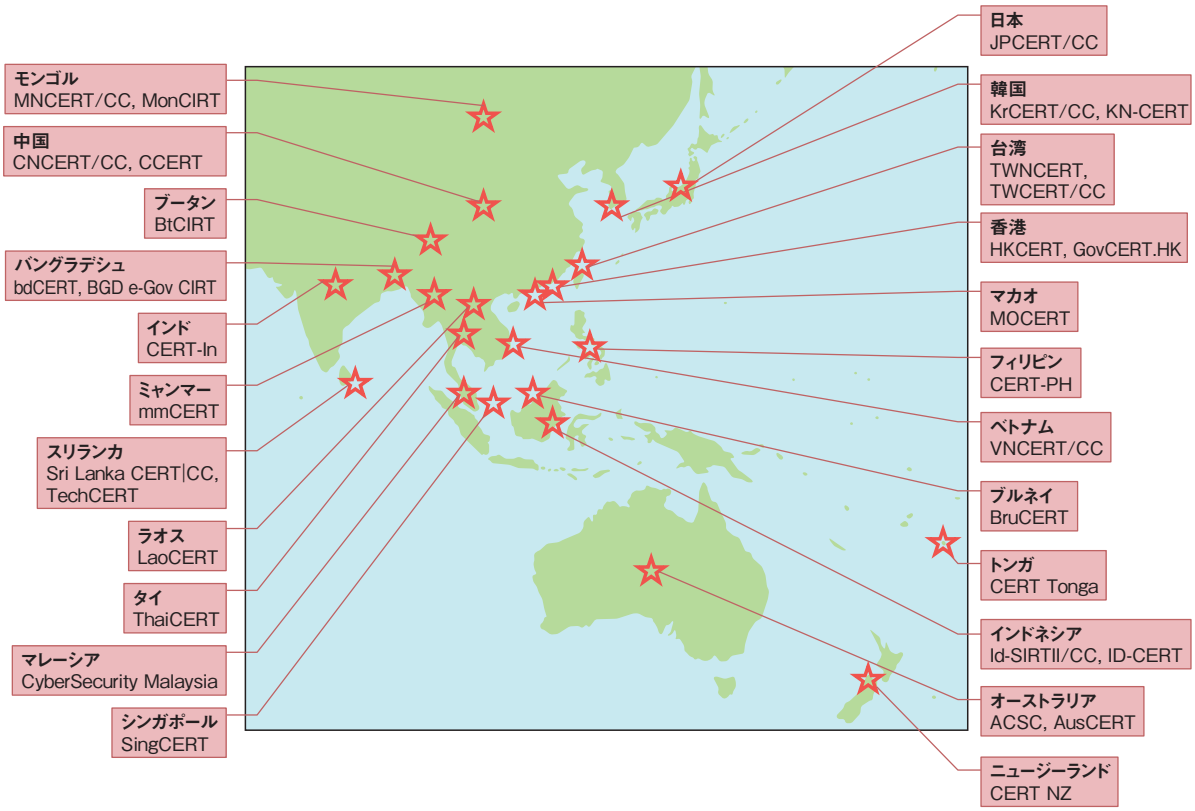
2021年8月18日、タイのMDES（Ministry of Digital Economy and Society:デジタル経済社会省）がNCSA（National Cyber Security Agency：国家サイバーセキュリティ機関）を新設したことを発表した※172。NCSAは、経済及び社会に影響を及ぼす深刻なサイバー脅威に対処する機関として設立され、官民のサイバーセキュリティ関連セクターのセキュリティに関する知識や理解を深め、サイバー脅威の状況認識を高めていくとしている。また、世界中で深刻なサイバー攻撃が増加していることを踏まえ、サイバーセキュリティ能力開発プログラムの提供を通じて、国家安全保障機関、金融、エネルギー、医療分野等を含む七つの主要な重要インフラセクターで働く要員のサイバーセキュリティ能力を高めていく取り組みも行うとしている※173。

(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）※174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、2022年3月末現在、23の国・経済地域の32チームが、オペレーショナルメンバーとなっている（次ページ図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。2022年4月末現在、TSUBAMEにはAPCERTメンバーを中心に18の国・経済地域から21チームが参加し、観測結果を共有している※175。

APCERTの主な活動は、年次サイバー演習の実施、及び年次会合の開催であり、年次報告書を公表している。2021年のサイバー演習は、「Supply Chain Attack Through Spear-Phishing - Beware of Working from Home -（スピアフィッシングを発端とするサプライチェーン攻撃）」をテーマに実施された※176。同演習には、APCERTのオペレーショナルメンバーのうち合計19の国・経済地域から25チームが参加した。年次報告書は、APCERT全体の活動に加えて各チームの組織概要や、対応したインシデントの統計等をまとめた文書で、Webサイトで公開されている※177。2021年の年次会合は、新型コロナウイルス感染拡大の影響により、前回に引き



■図 2-2-1　APCERT オペレーショナルメンバー（2022 年 3 月末現在）

続き 9 月にオンライン形式で開催された。マレーシアの CyberSecurity Malaysia[※178] が議長に、中国の CNCERT/CC[※179] が副議長にそれぞれ再選された。また、JPCERT/CC が事務局に再選された。

このほか、APCERT では能力開発の取り組みとして、2014 年以来継続して、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実施している。新型コロナウイルス禍で、対面でのトレーニング開催が困難な中でも、こうしたオンラインで連携する取り組みを継続している。

また、2021 年 10 月には、シンガポールの CSA が立ち上げた ASEAN-Singapore Cybersecurity Centre of Excellence（ASCCE）のキャンパス（活動拠点）が正式にオープンした[※169]。ASCCE は、2019 年に立ち上げられたサイバー能力向上プログラムで、政策及び技術を担当する ASEAN 地域の上級実務者向けにサイバーセキュリティのトレーニング等を提供し、地域のサイバーセキュリティ能力向上の促進や情報連携の強化に取り組んでいる。ASCCE においても、新型コロナウイルス感染拡大の影響により、対面式のキャパシティビルディング（能力向上）等の取り組みが停止したが、状況の変化とニーズに応じてオンライン形式のプログラム提供を行っている。

その他のアジア太平洋地域のサイバーセキュリティ関連イベントの多くが、各国の National CSIRT が主催するカンファレンスを含め、2021 年も前年同様にオンライン形式で実施された。対面の会議や情報交換の機会が制限されている状況下でも、こうした場をとおして CSIRT 間の連携が継続して行われている。

インシデントへの対応を効果的に進めていくためには、諸外国や特に近隣地域との CSIRT 連携が重要となる。CSIRT コミュニティをとおした協力が更に推進されることで、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・進展が期待される。

2.3 情報セキュリティ人材の現状と育成

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

2.3.1 情報セキュリティ人材の状況

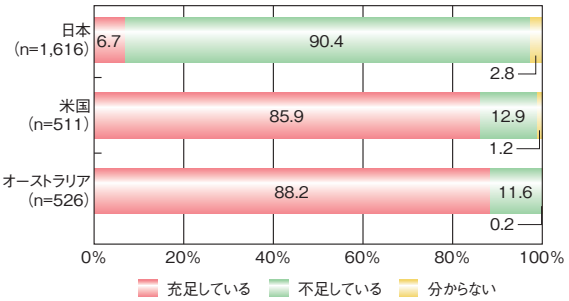
コロナ禍によるテレワークが続き、また、企業におけるDX推進が強く進められるようになってきている。2021年9月に策定された「サイバーセキュリティ戦略」では、セキュリティに関わる人材育成に関して、「DX with Cybersecurityの推進」として「プラス・セキュリティ」知識を補充できる環境整備や「巧妙化・複雑化する脅威への対処」として人材教育プログラムの強化や人材育成共有基盤の構築が盛り込まれた（「2.1.1 (1) 経済社会の活力の向上及び持続的発展～DX with Cybersecurityの推進～」参照）。

情報セキュリティ専門人材への需要は更に伸びるとともに、DX推進によりセキュリティ関連業務を主とする職種以外においてセキュリティ能力を持った人材への需要が高まっている。

(1) セキュリティ人材不足に関する認識

米国（ISC）^{2}（International Information Systems Security Certification Consortium）が発行した「2021 (ISC)^{2} Cybersecurity Workforce Study[※180]」によると、全世界で419万人のセキュリティの専門家がサイバーセキュリティの業務に従事していると推定され、これは前年と比較して70万人以上増加している。また、サイバーセキュリティ人材の不足数は北米、南米、欧州で増加、アジア太平洋地域では減少している。全体としてはサイバーセキュリティ分野の人材不足は2年連続で減少しており、2021年は前年の312万人から272万人に減少しているが、不足数を補うためには世界のサイバーセキュリティ人材を65%増加させる必要があるとし、依然としてセキュリティの人材が不足している状況である。

日米の比較をすると同調査では米国では約38万人、日本では4万人が不足しているとしており、絶対数では日本の方が不足数は低いが、NRIセキュアテクノロジーズ株式会社の「NRI Secure Insight 2021[※181]」では、米国と比較して充足できていない企業が非常に多くなっている（図2-3-1）。その要因として、セキュリティ業務システム化の標準化・自動化が進んでいないことが挙げられる（表2-3-1）。また、DX推進が強く進められている中、



※充足している：「人材が過剰な状態」「充足している（最適な状態）」「どちらかといえば充足している」のいずれかを回答
※不足している：「どちらかといえば不足している」「不足している」のいずれかを回答

■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株式会社「NRI Secure Insight 2021」を基にIPAが編集

	日本 (n=109)	米国 (n=439)	オーストラリア (n=464)
1位	33.9% セキュリティ業務が標準化されており、役割分担が明確化されているため	35.8% セキュリティ業務がシステム等により自動化・省力化されているため	35.3% セキュリティ業務がシステム等により自動化・省力化されているため
2位	32.1% 想定していたほどの有事が少ないため	33.3% セキュリティ業務が標準化されており、役割分担が明確化されているため	32.8% 想定していたほどの有事が少ないため
3位	31.2% セキュリティ業務の量が少ないため	33.0% 想定していたほどの有事が少ないため	31.3% セキュリティ業務は経験豊富な一部のメンバーで対応しているため
4位	19.3% セキュリティ業務は経験豊富な一部のメンバーで対応しているため	31.4% セキュリティ業務の量が少ないため	28.9% セキュリティ業務の量が少ないため
5位	14.7% セキュリティ業務がシステム等により自動化・省力化されているため	29.8% セキュリティ業務は経験豊富な一部のメンバーで対応しているため	21.6% セキュリティ業務を外部委託しているため

■表2-3-1 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株式会社「NRI Secure Insight 2021」を基にIPAが編集

企業で求められるセキュリティに関する業務が変化してきていることも影響している。

(2) セキュリティ業務・役割の広がり

企業でビジネスのIT利用が浸透し、更にDX化が進むにつれて事業部門が自ら様々なITを駆使してビジネス環境を構築することが必要になり、事業部門の中にもITやセキュリティの知識を有する技術者が在籍することが広まりつつある[※182]。

サイバーセキュリティ戦略では、このような状況をとらえて、デジタル化の進展と併せてサイバーセキュリティ確保に向けた取り組みを同時に推進すること（DX with cybersecurity）が盛り込まれた。そして、DXを推進する事業部門の人材を始め、ITやセキュリティの専門知識や業務経験を必ずしも持たない場合にも、セキュリティ専門家と協働できる能力「プラス・セキュリティ」を補充できる環境整備を推進している。

セキュリティに関連する役割・人材を表現する用語について、「サイバーセキュリティ体制構築・人材確保の手引き 第1.1版[※183]」のITSS+（セキュリティ領域）を基に整理すると図2-3-2のようになる。

「戦略マネジメント層」は青枠で示すように、DX推進におけるセキュリティをリードする役割を広く表現しているととらえることができる。「プラス・セキュリティ人材」は緑枠で示すように事業遂行するにあたり、事業部門でセキュリティに関連する業務を担当している役割をセキュリティの観点で表現しているととらえることができる[※184]。「セキュリティ人材」は赤枠で示すように、セキュリティ経営（CISO）、脆弱性診断・ペネトレーション等のセキュリティ対策に関する業務を主とする役割を表現している。特に、その中で中心的な役割を果たすのが「セキュリティ統括」（紫枠）となる。

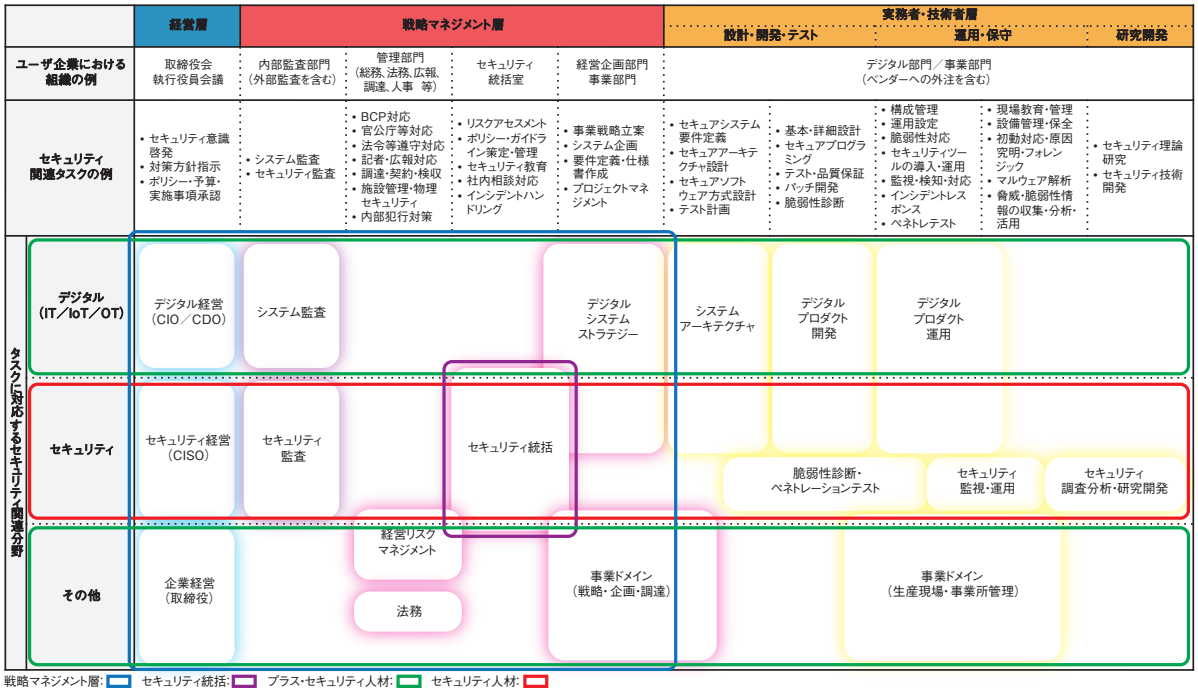
個々の事業責任は推進する事業部門が持っているが、事業で使用するシステム等のセキュリティに関しても、第一義的には事業部門が責任を負う。CISO及び情報システム部門は共通化、標準化すべきインフラ等の整備に加え、事業部門のDX化支援により、企業全体としてのセキュリティ状況を把握し、統括管理する体制に変わりつつある。

企業におけるセキュリティ関連業務が広がっていることを踏まえて、セキュリティ人材育成の取り組みが行われている。

(3) 人材育成の取り組み

経済産業省では人材施策として「サイバーセキュリティ体制構築・人材確保の手引き」（「サイバーセキュリティ経営ガイドライン」付録F）を改訂するとともに、プラス・セキュリティの取り組みを推進するとしている（次ページ図2-3-3）（「2.1.2(1)産業サイバーセキュリティ研究会」参照）。

セキュリティ人材の育成については、中核人材育成プ



■図2-3-2　ITSS+（セキュリティ領域）と人材分類
（出典）経済産業省・IPA「サイバーセキュリティ体制構築・人材確保の手引き 第1.1版」（「サイバーセキュリティ経営ガイドライン」付録F）を基に編集

●昨年度は、「セキュリティ体制構築・人材確保の手引き」の改訂を行うとともに、セキュリティ人材育成の既存施策を進めつつ、特に、セキュリティを本務としない者が自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につける「プラス・セキュリティ」の取組を推進するため、SC3での検討や地域での具体的な取組を推進。

取組の全体像

セキュリティ対策を進めるための体制・人材の考え方

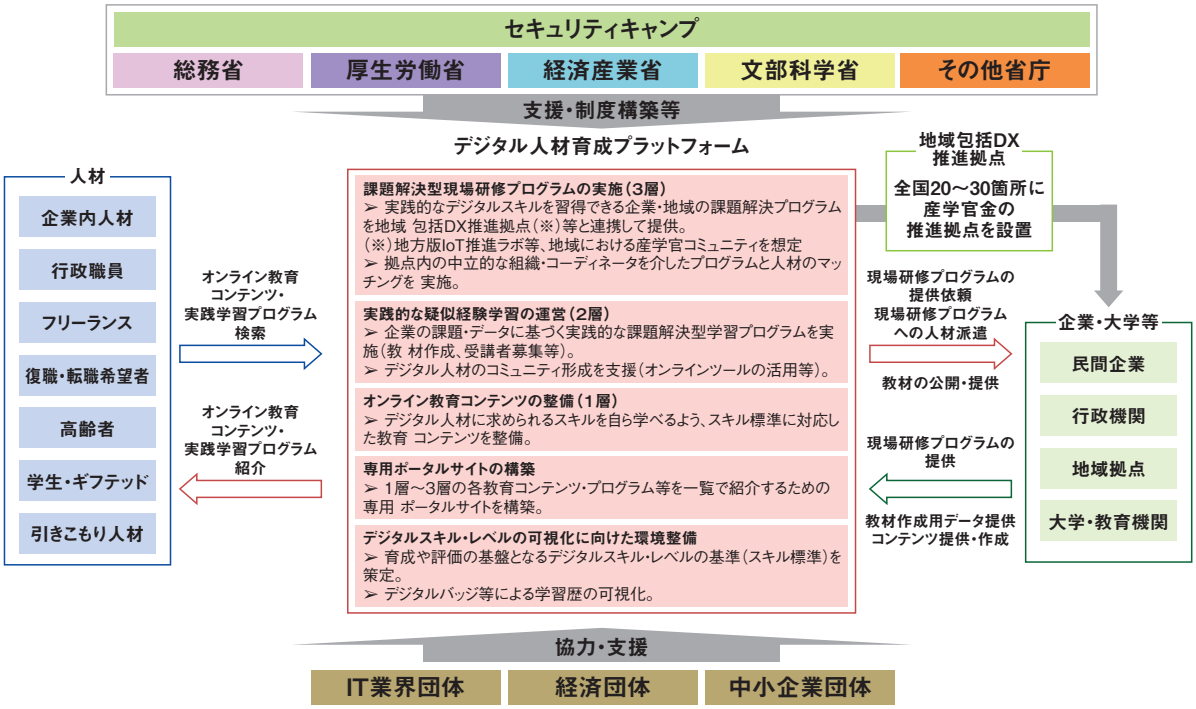
セキュリティ体制構築・人材確保の手引き（「サイバーセキュリティ経営ガイドライン」付録F）

セキュリティ人材の育成	プラス・セキュリティの普及
ICSCoE中核人材育成プログラム	SC3産学官連携WGでのプラス・セキュリティ具体化
情報処理安全確保支援士	NISCにおけるモデルカリキュラム策定
セキュリティキャンプ	地域SECUNITYにおける人材育成
デジタル人材育成プラットフォームにおけるスキル標準の整理・教育コンテンツ・実践型教育	
大学・高専等と産業界の連携	

今後の方向性

●手引きの普及による各企業での体制構築の促進と各種セキュリティ人材育成施策を引き続き実施するとともに、プラス・セキュリティの取組を普及させるため、SC3産学官連携WG、デジタル人材育成プラットフォーム、各地域における産学官連携の取組（地域SECUNITY）との連携による取組の具体化・拡大を進めていく。

■図 2-3-3　サイバーセキュリティ人材施策の全体像
（出典）経済産業省「第７回 産業サイバーセキュリティ研究会 事務局説明資料※185」（資料３）



■図 2-3-4　デジタル人材育成プラットフォーム 概要イメージ
（出典）経済産業省「実践的な学びの場ワーキンググループ活動結果報告※187」（第５回 デジタル時代の人材政策に関する検討会 資料 3-1）を基に IPA が編集

ログラム（「2.3.2（1）中核人材育成プログラム」参照）、セキュリティ・キャンプ（「2.3.4（1）セキュリティ・キャンプ」参照）等の活動が既に実施され継続されている。また、プラス・セキュリティの普及については、NISCにより、経営層・部課長級向けの知識補充のモデルカリキュラム策定等が実施されてきた※186。

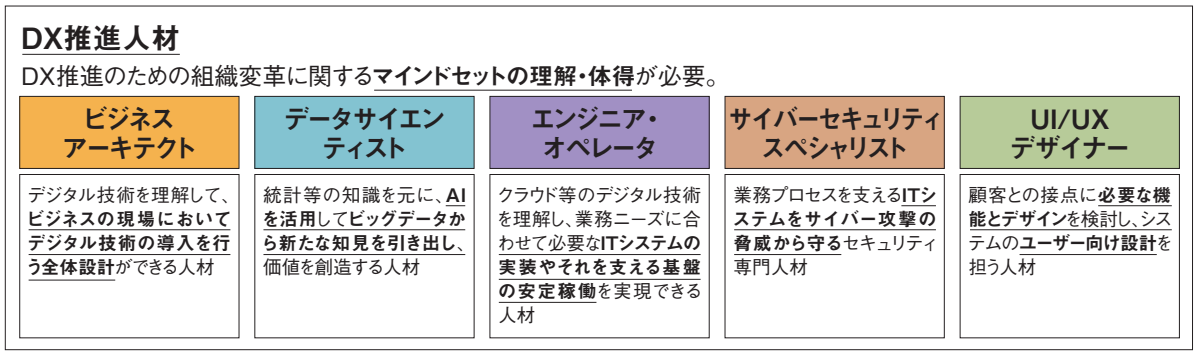
それらに加えて、SC3産学官連携WGにおいて、産学官間でのセキュリティ人材育成をいかに行うべきかの検討が進められている（後述）。また、セキュリティ人材、プラス・セキュリティ人材の基盤として活用可能なプラットフォームとして、「デジタル人材育成プラットフォーム」の構築に向けての検討が進められている。

(a) デジタル人材育成プラットフォーム

本プラットフォームは、ビジネスに求められるデジタルリテラシーとデジタル専門知識の学習機会を提供し、DXを推進できる実践的なDX推進人材の育成手法を確立することを目標としている（前ページ図2-3-4）。

育成するDX推進人材像（仮説）として図2-3-5に示す五つが想定されており、サイバーセキュリティスペシャリストとしてセキュリティ専門人材も含まれている。

プラットフォームで提供される教育コンテンツの整備並

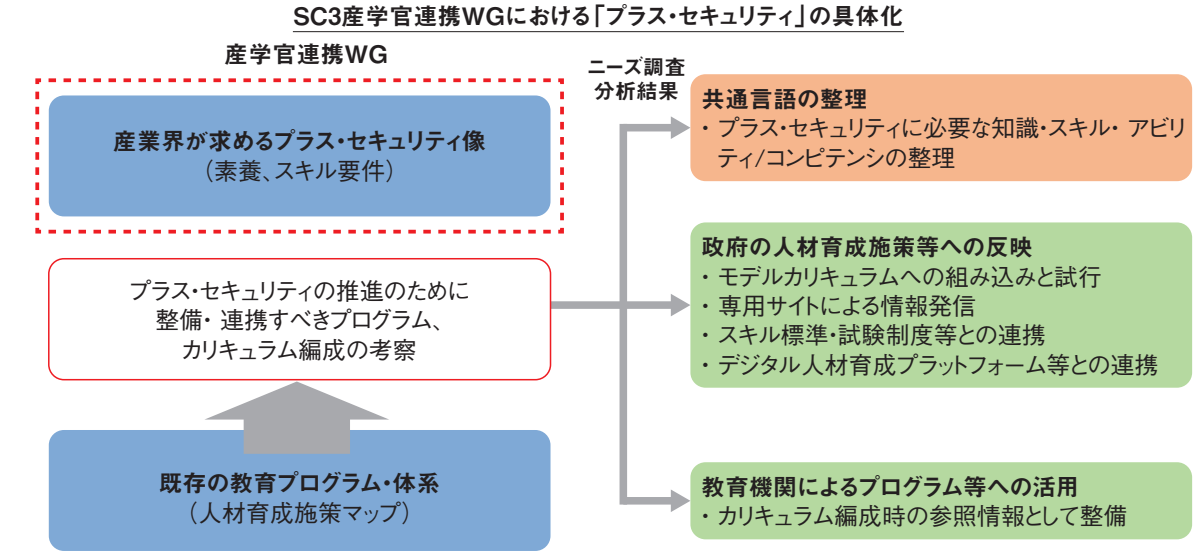


■図2-3-5　DXを進める企業等におけるビジネスパーソンの人材像（仮説）
（出典）経済産業省「実践的な学びの場ワーキンググループ活動結果報告」（第5回 デジタル時代の人材政策に関する検討会 資料3-1）を基にIPAが編集

プラス・セキュリティの普及促進

プラス・セキュリティ

- **プラス・セキュリティ＝（セキュリティが本務ではないが）自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のこと。**
- プラス・セキュリティの取組普及のため、SC3産学官連携WGにおいて必要なスキルの整理等が行われているほか、NISCにおいても「プラス・セキュリティ」のモデルカリキュラムの策定や官民のコンテンツのポータルサイトへの掲載などを実施中。デジタル人材育成プラットフォーム事業等の関連施策とも連携し、取組を普及させていく。



■図2-3-6　SC3産学官連携WG「プラス・セキュリティの普及促進」
（出典）経済産業省「事務局説明資料※189」（第8回 産業サイバーセキュリティ研究会 ワーキンググループ2（経営・人材・国際）資料3）

びに教育コンテンツが提供する具体的な学習項目については、DX リテラシー標準として今後検討される。

経済産業省と IPA は、デジタル人材の育成を推進するため、デジタル知識・能力を身に付けるための実践的な学びの場として、デジタル人材育成プラットフォームポータルサイト「マナビ DX（デラックス）」を 2022 年 3 月に開設した※188。ポータルサイトでは、デジタルスキルを学ぶことができる学習コンテンツを紹介するとともに、すべての社会人が身に付けるべきデジタルスキルを示した「DX リテラシー標準」も掲載しており、これまでデジタルスキルを学ぶ機会がなかった人にも新たな学習を始めるきっかけとなることが期待される。

(b) SC3 産学官連携 WG

SC3 産学官連携 WG では、プラス・セキュリティ人材育成の具体化として、産業界が求めるプラス・セキュリティ像と既存の教育プログラム・体系の摺り合わせを行うとしている（前ページ図 2-3-6）。

現時点では、プラス・セキュリティ向けの教育カリキュラムは整備されておらず、SC3 産学官連携 WG ではそれらのセキュリティ教育プログラムで身に付けるべき知識・スキル及びその他の能力を明確にし、共通化する作業も行うとしている。

今後、教育機関、教育ベンダ等がプラス・セキュリティに関する人材育成として具体的な教育プログラムを整備することが期待される。

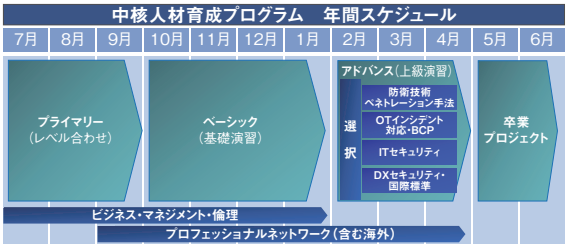
2.3.2 産業サイバーセキュリティセンター

我が国の経済・社会を支える重要インフラ※190 や産業基盤のサイバー攻撃に対する防御力を強化するため、IPA は 2017 年 4 月に産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）を発足させた。

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

(1) 中核人材育成プログラム

ICSCoE は、2017 年 7 月、制御技術（OT：Operational Technology）と情報技術（IT）、マネジメント、ビジネス分野を総合的に学び、サイバーセキュリティ対策の中核となる人材を育成する「中核人材育成プログラム」を開始した。本プログラムでは、OT 及び IT 知識のレベル合わせからハイレベルな演習までを 1 年間のフルタイムで実施する（図 2-3-7）。第 1 期は 76 名、第 2 期は 83 名、第 3 期は 69 名、第 4 期は 47 名が参加し、2021 年 7 月に開講した第 5 期では、電力・鉄鋼・石油・化学・自動車・鉄道・放送・通信・産業ベンダ等の幅広い業界から 48 名が参加した。



■図 2-3-7　第 5 期中核人材育成プログラムの年間スケジュール

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

2021 年 10 月には米国政府・EU と連携した制御システムのサイバーセキュリティ対策に関するキャパシティビルディングプログラム「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク※191」を経済産業省と共催した（「2.2.1 (3) (d) インド太平洋地域に向けたサイバー演習」参照）。本演習には第 5 期の受講者及びインド太平洋地域から招聘した外国人受講者 40 名がオンラインで参加し、米国、EU 及び日本の専門家によるエネルギー分野を含むサイバーセキュリティに関するワークショップ、リモートでのハンズオン演習等を実施した。

同年 12 月の海外派遣演習では、英国政府によるサイバーセキュリティ政策の紹介や英国企業によるサプライチェーンサイバーセキュリティについてのケーススタディ等をオンラインで実施した。2022 年 2 月には、2017 年 5 月に合意された「日イスラエル・イノベーション・パートナシップ」等に基づき、イスラエルのテルアビブ大学やイスラエ

ル国家サイバー総局によるサイバーセキュリティ対策に関する講義をオンラインで実施した。

2022 年 5 月の海外派遣演習では、フランスを訪問し、サイバーセキュリティの国際標準や先進的な取り組みの理解、現地トップレベル機関の人材とのネットワーク構築を目的に学術研究機関や産学官連携による研究施設の講義を受講し、自動運転等の模擬システムを見学した。

2018 年 7 月、中核人材育成プログラムの修了者コミュニティとして「叶会※192」が発足し、2019 年夏以降、本プログラムを通じて培った人脈の活用、知見やノウハウの共有を目指し、地域活動や技術をテーマにする複数の部会が設置された。また修了年次をまたがる縦のつながりの形成、最新情報及びノウハウ収集を目的とした叶会総会の第 4 回が 2021 年 11 月に開催された。叶会には第 1 期から第 4 期までの修了者に加え、2022 年 6 月に修了した第 5 期生も参加しており、今後もコミュニティとしての規模を拡大しながら、お互いの顔が見える縦横の人的つながりを形成し、産業サイバーセキュリティに関する適時、適切な情報共有活動を継続することが期待される。

なお、同プログラムの修了者は、「情報処理の促進に関する法律」の規定に基づき、後述する情報処理安全確保支援士試験の全部免除を受けることができる※193。

(2) 短期プログラム

ICSCoE では、セキュリティに関連するスキルの習得機会が充分でない部門責任者や現場責任者、及びセキュリティ実務担当者に向けて、数日間で学ぶ短期演習形式の「サイバー危機対応机上演習（CyberCREST）」「業界別サイバーレジリエンス強化演習（CyberREX）」「戦略マネジメント系セミナー」「制御システム向けサイバーセキュリティ演習」及び「ERAB サイバーセキュリティトレーニング」を提供している。対面形式での実施のほか、新型コロナウイルス対策の一環として、オンライン形式、または対面とオンラインを併用したハイブリッド形式での実施とした。

(a) サイバー危機対応机上演習（CyberCREST）

「サイバー危機対応机上演習（CyberCREST：Cyber Crisis RESponse Table top exercise）※194」は、制御システムを有する企業・団体においてサイバーセキュリティ対策を統括する責任者やセキュリティ・オペレーション・センター（SOC）の責任者、サイバーセキュリティ対策部門の管理職を対象にしたプログラムである。

2021 年 9 月に本演習をオンライン（ライブ配信）で実施した。本演習では、組織を守るために必要なスキルとメソッドを身に付けるため、最新のサイバー脅威の動向や米国の先進的なサイバーセキュリティ戦略である「コレクティブ・ディフェンス」、近年重要性が説かれている「任務保証」等について、米国サイバーコマンド出身の専門家や CISO、セキュリティアーキテクト等が講師となって講演、講義及びロールプレイング演習を行った。受講者からは、多種多様な経験を積んできた講師陣の話をリアルタイムの対話形式で聴くことができたことは有益であった、との反応があった。

(b) 業界別サイバーレジリエンス強化演習（CyberREX）

「業界別サイバーレジリエンス強化演習（CyberREX：Cyber Resilience Enhancement eXercise by industry）※195」は、電力、鉄道、ビル、ガス、金属、石油・化学、自動車（製造）、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たプログラムである。

2021 年 10 月にはオンライン（ライブ配信）で、11 月には大阪で本演習を実施した。本演習は、部署・部門のサイバーセキュリティに関するインシデント対応力・回復力を強化するため、仮想企業を想定し、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、グループ演習を行った。受講者からは、実務で起こりうる事例がシナリオで挙げられており興味深い、外部組織との連携や事業への影響等、高い視座でインシデントを見ることができ有意義であったとの反応があった。

(c) 戦略マネジメント系セミナー

「戦略マネジメント系セミナー※196」は、経営層を補佐し、実務者・技術者を指揮することでセキュリティ対策を進める戦略マネジメント層、及び今後戦略マネジメント層になることが期待される層を対象としたプログラムである。

2022 年 1 月から 2 月にかけて、本セミナーを対面（東京）とオンラインのハイブリッド形式で実施した。本セミナーは、ビジネスのデジタル化・DX 推進に伴うリスクの変化に対応して、セキュリティ対策を組織横断的に統括できる責任者を育成することを目的としている。具体的には、政府の動向やサイバーセキュリティの事故や対策につい

ての先進事例の講演、責任者の役割等を理解するための講義のほか、事例を用いてインシデント発生時に必要な意思決定における課題を発見し、対策ガイドを作成するために、グループワーク（ディスカッション）を行った。受講者からは、どのような視点で経営層と現場をつなげばいいかが理解できた、他社の方と意見交換することで自分の中にはなかった視点を学べたとの反応があった。

(d) 制御システム向けサイバーセキュリティ演習

「制御システム向けサイバーセキュリティ演習[※197]」は、制御システムのサイバーセキュリティを担当する、または今後担当予定の技術者を対象としたプログラムである。

2022 年 2 月に福岡で本演習を実施した。本演習は制御システムのサイバーセキュリティを理解するための導入的な演習に位置付けられ、制御システムの攻撃手法、及び制御システムのサイバーセキュリティ対策の基礎を、簡易模擬システムを用いた実機演習（ハンズオン演習）で体験し、制御システムのセキュリティについて実践的に理解することを目的としている。受講者からは、ハンズオン研修は身に付きやすいと感じた、OT-IT 連携の重要性について腹落ちしたとの反応があった。

(e) ERAB サイバーセキュリティトレーニング

「ERAB サイバーセキュリティトレーニング[※198]」は、電力小売事業に関わる ERAB（Energy Resource Aggregation Business）事業者において、セキュリティ対策を検討し、立案・実施する実務者及び対策の導入・実施を判断する責任者を対象としたプログラムである。

2022 年 2 月にはオンライン（ライブ配信）で、3 月には東京で本トレーニングを実施した。本トレーニングは、経済産業省の「エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン Ver2.0[※199]」における ERAB 事業者に求められるサイバーセキュリティ対策に関する学習を目的としている。具体的には、本ガイドラインの解説やリスク分析・対策事例の解説やグループワーク、実機を用いた実演（デモ）を中心とした演習を実施した。受講者からは具体的なデモを目の当たりにすることでリスクや事象についてイメージを持つことができた、実機を用いて不正アクセス・制御が実施できることを理解でき対策の必要性を実感できたとの反応があった。

2.3.3 情報セキュリティ人材育成のための国家試験、国家資格制度

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

(1) 情報セキュリティマネジメント試験

企業・組織においては、組織が定めた情報セキュリティポリシーを部門内に周知して遵守を促し、部門の情報管理を実施する等、情報セキュリティ対策を推進する人材（情報セキュリティマネジメント人材）が必須である。こうした人材を育成するために、2016 年度春期より「情報処理技術者試験」の新たな試験区分として「情報セキュリティマネジメント試験」が実施されている。2019 年度までは、試験を筆記方式で年 2 回実施していたが、2020 年度から CBT（Computer Based Testing）方式[※200]に移行した。CBT 方式への移行により、受験者は、自身で試験日、試験会場を選択することが可能となった。2021 年度は、CBT 方式による試験が年 2 回（上期 7 月 1 ～ 31 日、下期 12 月 1 ～ 26 日）実施され、応募者数 3 万 1,672 人（前年比約 3.3 倍）、合格者数 1 万 5,325 人（前年比約 2.5 倍）であった[※201]。2022 年度も CBT 方式での実施を継続する。

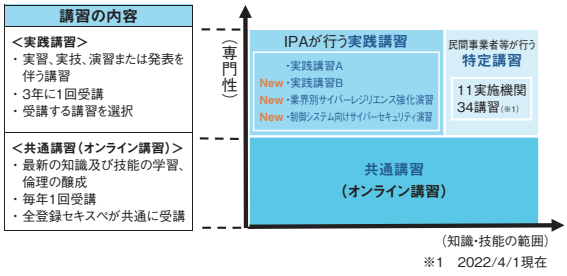
(2) 情報処理安全確保支援士制度

サイバー攻撃の増加・高度化に加え、社会全般に IT が広く普及・活用されていることから、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 月に「情報処理の促進に関する法律」の改正法が施行され、国家資格「情報処理安全確保支援士」制度が創設された。

情報処理安全確保支援士（以下、登録セキスペ）はサイバーセキュリティ分野初の国家資格であり、情報処理安全確保支援士試験合格者等が登録申請後、登録簿に登録されることにより資格を取得できる。試験は年 2 回実施され、2021 年度は応募者数 3 万 2,627 人、合格者数 4,665 人であった[※201]。登録セキスペは 2022 年 4 月 1 日時点で 2 万 253 人[※202]となった。

登録セキスペには、法定講習の受講と、3 年に 1 度



■図 2-3-8 法定講習の全体像
(出典)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※203」

の登録更新が義務付けられている※203。

法定講習の全体像を図 2-3-8 に示す。

「共通講習(オンライン講習)」は、登録セキスペとして期待される情報セキュリティ実践のために必要な知識・技能・倫理について学習することを目的として、すべての登録セキスペが毎年 1 回受講する。

「実践講習」は、実習、実技、演習または発表等を通じて具体的な技術や手法を学ぶことを目的として、3 年に 1 回「IPA が行う実践講習」あるいは「民間事業者等が行う特定講習」から任意の講習を選択して受講する。

「IPA が行う実践講習」のうち「実践講習 A」は主に登録後 3 年目までの登録セキスペを対象とし、情報セキュリティインシデント対応等の演習を通じて情報セキュリティ実践のための具体的な技術や手法を習得することができる。Web 会議ツールを活用したオンライン形式で実施し、2021 年度は全国より 3,016 名が受講した。更に、2022 年 3 月より、主に登録後 4 年目以降の登録セキスペを対象とし、新規事業を立ち上げる際のセキュリティ上の助言を検討する「実践講習 B」を開始した。また専門的な分野の知識・技術修得を望む登録セキスペを対象として、「業界別サイバーレジリエンス強化演習(CyberREX)」と「制御システム向けサイバーセキュリティ演習」が追加され、より選択肢が広がった(演習内容については「2.3.2(2)(b)業界別サイバーレジリエンス強化演習(CyberREX)」「2.3.2 (2)(d) 制御システム向けサイバーセキュリティ演習」参照)。

「民間事業者等が行う特定講習」は、「IPA が行う実践講習」と同等以上の効果を有する講習として経済産業大臣が定める講習※204 であり、2022 年度は、11 実施機関 34 講習が経済産業省より特定講習として定められている。

なお登録セキスペの利便性向上等を目的とし、2021 年度に登録セキスペ専用の「情報処理安全確保支援士ポータルサイト」を開設し、「共通講習(オンライン講習)」受講、資格更新オンライン申請、その他登録セキスペの業務に役立つ情報の掲載等も開始された。

情報処理安全確保支援士制度全体に対して、登録セキスペからは「国家資格保持者である登録セキスペとなることで、単なる情報部門の公務員ではなく、信頼できる情報技術の専門家とみなされるようになった」(地方自治体所属)、「情報処理安全確保支援士の講習で得られる最新の知識・スキルが業務で役立つ重要なツールになっている」(IT ベンダ企業所属)、等の声が聞かれ、今後一層、企業・組織のセキュリティ対策推進に登録セキスペの活躍が期待され、大きな役割を果たしていくと考えられる。

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 により運営されている。本項では、一般社団法人セキュリティ・キャンプ協議会と IPA が開催しているプログラム・イベントについて紹介する。

(a) セキュリティ・キャンプ全国大会

年 1 回、主に夏休み期間中に 4 泊 5 日の合宿形式の勉強会としてセキュリティ・キャンプのメインイベントである「セキュリティ・キャンプ全国大会」(以下、全国大会)が実施されてきた。18 回目となる 2021 年度の「全国大会 2021 オンライン」は、2020 年に引き続き新型コロナウイルス感染防止のためオンライン形式による開催となった。過去 3 番目の多さとなる 317 名の応募があり、選考を通過した 81 名が参加した※205。

(b) セキュリティ・ネクストキャンプ

過去の全国大会を修了した、または同等以上のスキルを持つ 25 歳以下の学生等を対象に、さらなる育成の場として「セキュリティ・ネクストキャンプ 2021 オンライン」が全国大会と同時にオンライン形式で開催された。3 回

目の開催となる本プログラムでは選考を通過した 10 名が参加した※206。

(c) セキュリティ・キャンプ地方大会（セキュリティ・ミニキャンプ）

これまで地方において小規模で開催してきた「セキュリティ・ミニキャンプ」も、2020 年に引き続き一部オンライン形式を取り入れて開催された※207。

参加資格を限定しない一般講座は山梨（2021 年 9 月）、広島（2021 年 11 月）、大阪（2022 年 3 月）にて開催し、最新のサイバーセキュリティ脅威の動向や対応策、これからの IT 人材のキャリア等をテーマに、産学官の有識者による講演やディスカッションが行われた※208。

また、2021 年 10 ～ 11 月に行われた「セキュリティ・ミニキャンプ オンライン 2021」は、従来のミニキャンプの特徴を踏襲しつつ、地域ごとのグループによる助け合いと、グループワークによる盛んな交流を取り入れて開催された※207。参加者は、25 歳以下の学生・生徒・児童で、北海道、東北、関東、中部、近畿、中国、四国、九州、沖縄の地域ごとに 4 名程度を選考して実施された。

(d) セキュリティ・キャンプフォーラム 2022

セキュリティ・キャンプ修了生相互の年度を超えた交流と意見交換の場の提供、及び同修了生の認知度向上と現在の活動状況紹介による産業界での活動の機会提供の 2 点を目的として 2022 年 3 月に「セキュリティ・キャンプフォーラム 2022」が開催された。本フォーラムでは講師、チューター、修了生がパネリストとなり、「プログラミングの教育者になるとしたら、何から教えるか」をテーマにパネルディスカッションや修了生による講演が行われた。また、フォーラム終了後には「セキュリティ・キャンプ交流会 2022 春オンライン」が開催され、LT（Lightning Talk）会等、セキュリティ・キャンプ修了生同士の交流が行われた。

(e) Global Cybersecurity Camp

「Global Cybersecurity Camp（GCC）」は「国籍・人種を超えた専門知識のあるグローバル人材の育成」と「国境を超えた友情とゆるやかなコミュニティの形成」を目的として、セキュリティに興味を持つ 25 歳以下の若者がともに学び、友好を深める場として 2018 年度から日本を含むアジア太平洋地域 8 ヵ国の関連団体・大学により開催されている。4 回目となる 2021 年度の「GCC 2022 Taiwan」は台湾で開催され、日本からも選考を通過した数名が参加した※209。

(f) Asian Cyber Security Challenge

「Asian Cyber Security Challenge（ACSC）」はアジアトップの Capture The Flag（CTF）プレイヤーを選出するための CTF 大会である。2021 年 1 月 1 日時点で 25 歳以下のアジア圏在住者を対象とし、成績優秀者はアジア代表チームとして「International Cybersecurity Challenge（ICC）」に参加できる。ファイナリストには 3 名の日本人※210 が選ばれ、2022 年 6 月※211 に開催される ICC にアジア代表のチームメンバーとして参加が予定されている。

(2) enPiT

「enPiT（Education Network for Practical Information Technologies：成長分野を支える情報技術人材の育成拠点の形成）」は、情報技術を高度に活用して社会の具体的な課題を解決できる人材を育成するために、2012 年 4 月から開始された文部科学省の事業である。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ている。2021 年度 4 月以降は、セキュリティを含む 4 分野において大学により自主展開されている※212。本項では、セキュリティ分野で提供されている三つのプログラムについて紹介する。

(a) SecCap

2012 ～ 2016 年度までは大学院生を対象とした事業「第 1 期 enPiT」が実施された。この活動を継承した教育プログラム「enPiT1」のセキュリティ分野では、五つの大学※213（情報セキュリティ大学院大学、北陸先端科学技術大学院大学、奈良先端科学技術大学院大学、慶應義塾大学、東北大学）が協力して開講する実践セキュリティ人材育成コース「SecCap」が設けられ、産業界が求める「セキュリティ実践力のある IT 人材」を育成するプログラムとなっている。

(b) Basic SecCap

「第 1 期 enPiT」を踏まえて 2016 年度から、学部生を対象とした「第 2 期 enPiT」（以下、enPiT2）が実施されている。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。enPiT2 のセ

キュリティ分野では、14の大学※214が協力して開講する情報セキュリティ分野の実践的人材育成コース「Basic SecCap」が設けられ、幅広いセキュリティ分野の最新技術や知識を取得可能なプログラムとなっている※215。

(c) enPiT Pro Security

「enPiT Pro Security（情報セキュリティプロ人材育成短期集中プログラム）」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、慶應義塾大学、長崎県立大学の7大学院※216が連携し、文部科学省「情報セキュリティ人材育成に関する調査研究」で提唱されたモデル・コア・プログラムに基づき、社会人の学び直しを支援する高等教育の体制を整え、様々な分野で活躍する情報セキュリティ分野のリーダー人材を育成する短期集中プログラムである。数学・アルゴリズム・暗号理論等のセキュリティの基盤技術から、サイバーセキュリティ・リスクマネジメント・法制度・暗号技術の応用・ビットコイン・ブロックチェーン・IoT等の最新技術までを幅広くカバーしており、社会システムにセキュリティ技術を安全に適用できる知識の獲得を目的としている※217。

(3) SECCON

「SECCON」（SECURITY CONTEST）は、情報セキュリティをテーマに多様な競技を開催する情報セキュリティコンテストイベントとして、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）内のSECCON実行委員会により運営されている※218。本イベントは、世界の情報セキュリティ分野で通用する実践的情報セキュリティ人材の発掘・育成を目的とし、日本の情報セキュリティレベルを世界トップレベルに引き上げることを目標としている。競技種目としては、CTFが採用されている※219。本項では、SECCON実行委員会が開催している三つのイベントについて紹介する。

(a) SECCON CTF 2021

世界各国のセキュリティ専門家がCTFの技量を競う「SECCON CTF 2021」は、2021年12月11～12日にオンライン形式で開催され、世界各国から506のチームが参加し、そのうち日本からは312のチームが参加した※220。

その他、コンテストの結果発表やワークショップを行うイベントとして「SECCON 2021 電脳会議」が同年12月18日に開催された※221。

(b) SECCON Beginners CTF

若手のCTFプレイヤーにより運営されている「SECCON Beginners」は、日本国内のCTF参加者を増やし、セキュリティ人材の底上げすることを目的とした勉強会である。CTF初心者・中級者を対象とした「SECCON Beginners CTF」をオンライン形式で2021年5月22～23日に開催した※222。

(c) CTF for GIRLS

「CTF for GIRLS」は、情報セキュリティ技術に興味がある女性（女性と自認されている方を含む）を対象に、気軽に技術的な質問や何気ない悩みを話し合うことができるコミュニティを作ることを目的とした団体である。コミュニティ形成の一環として、2021年6月30日にはExploit※223、2021年9月22日にはフォレンジック※224、2021年12月22日にはWebセキュリティ※225に焦点を当てたワークショップが開催された。

(4) 産学情報セキュリティ人材育成交流会

「産学情報セキュリティ人材育成交流会」は、今後の情報セキュリティ業界を支える人材育成を目的としたJNSAのインターンシップ支援活動である。将来情報セキュリティ業界で活躍したいと考える学生に対し、本交流会を介して2021年度は8社の企業がインターンシップを実施した※226。

(5) サイバーセキュリティ経営戦略コース

東京工業大学社会人アカデミーでは2021年11月11日、MOT（Management of Technology：技術経営）に関する社会人向けプログラムとして「キャリアアップMOT『サイバーセキュリティ経営戦略コース』」を開講した。本コースは2020年に引き続きオンライン講義形式となった。

本コースでは、サイバーセキュリティが企業・組織の経営に及ぼす影響を理解し、サイバーセキュリティ経営及びその戦略立案に求められる知識・能力を備え、企業・組織を先導する人材の育成を目指しており、経営企画、CISO相当業務等の実務者、サイバーセキュリティ経営を学びたい方等、多様な立場の社会人の受講を想定している。本コースは、週1回、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18回の講義で構成される※227。

(6) KOSEN Security Educational Community

「KOSEN Security Educational Community（K-SEC）」は、サイバーセキュリティ専門技術者として必要となる高度な技術を持つ人材だけでなく、工学分野（機械・建築・土木・電気／電子・材料・生命等）の技術者が持つべきセキュリティ技術を身に付けた人材の輩出を目的とした独立行政法人国立高等専門学校機構（以下、国立高専機構）による事業である。セキュリティ知識を身に付けた国立高等専門学校生（以下、高専生）、また高度なセキュリティ技術を身に付けた人材の育成のために、企業、大学、公的機関等の外部組織と連携し、講習会やコンテストの開催、インターンシップの実施等を行っている。

関連するイベントとして、2021 年 12 月 27 ～ 28 日に「K-SEC セキュリティウィンタースクール 2021」がオンライン形式で開催された。本開催で 8 回目となり、全国から 40 名の高専生が参加した。JNSA やトレンドマイクロ株式会社、株式会社日本総合研究所等の様々な講師による講義や演習を通じて、参加者はセキュリティのスキルを学んだ※ 228。

(7) CYNEX

NICT は、保有しているサイバー攻撃に関連した大量のデータや、人材育成の知見を活用し、サイバーセキュリティ分野の産学官の「結節点」となることを目指し、「CYNEX（Cybersecurity Nexus：サイネックス）」を 2021 年 4 月 1 日に設立した※ 99。本組織は、サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するとともに、人材育成の基盤としてサイバーセキュリティ演習に必要となる演習環境や教材を提供することで、日本のサイバーセキュリティの対応能力向上を目的としている（「2.1.3 (5) (c) 人材育成・普及啓発の推進」参照）。

CYNEX の人材育成プロジェクトの一つである「CYDERANGE as an Open Platform（CYROP）」では、国内における民間事業者や教育機関におけるセキュリティ人材育成事業の促進を目的に、NICT の演習プラットフォームをオープン化するための検証を 2022 年度末までの期間限定で実施している。この検証によって演習を実施する組織からフィードバックを得て、演習教材の拡充や演習環境の高度化等を行い、2023 年度には CYROP の本格運用開始が予定されている※ 100。

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

2.4.1 企業等における対策状況

情報セキュリティに対する企業等の対策状況及びセキュリティリスクマネジメントの取り組みについて述べる。

(1) 情報セキュリティに対する企業等の対策状況

近年、DX の推進に伴うサイバーセキュリティの重要性が注目されている。一方で、海外拠点を含むサプライチェーンのセキュリティ脅威が増しており、ランサムウェア等の攻撃により事業継続に影響する被害も出ている。このような背景を踏まえ、企業のセキュリティ対策・統制状況について、NRI セキュアテクノロジーズ株式会社（以下、NRI セキュア社）の「NRI Secure Insight 2021[※181]」(日本 1,616 社、米国 511 社、オーストラリア 526 社の企業を対象に調査。以下、NRI セキュア社調査）を基に述べる。

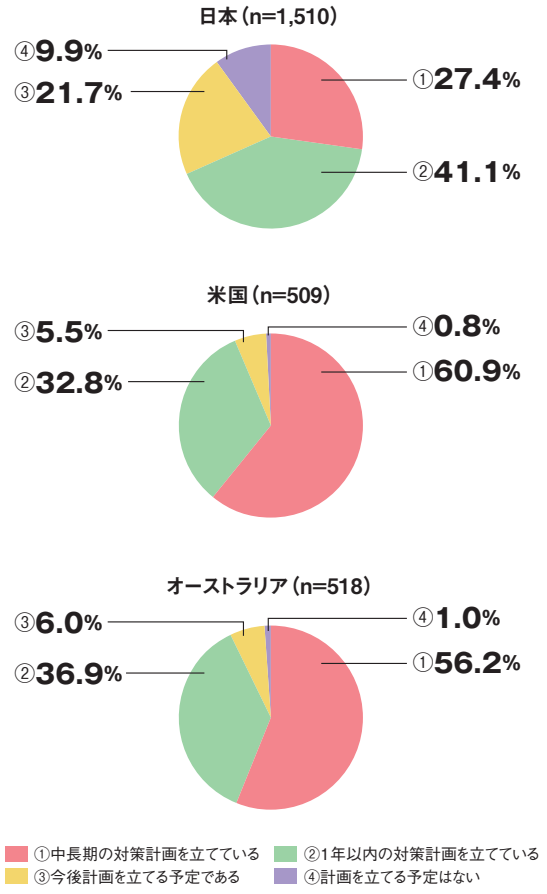
(a) セキュリティ対策計画の策定状況

NRI セキュア社調査（図 2-4-1）によると、 3 年程度の「中長期の対策計画を立てている」企業の割合は日本が 27.4% である一方、米国とオーストラリアは 60% 前後と日本の約 2 倍であった。また、「計画を立てる予定はない」企業の割合は日本が 9.9% である一方、米国とオーストラリアは約 1% であった。

回答企業のうち、1,000 人未満の企業の割合は日本 70.3%、米国 34.3%、オーストラリア 34.8% となっており、日本と米国・オーストラリアの違いは企業規模の構成比が影響している可能性がある。中堅企業、中小企業においても、「サイバーセキュリティ経営ガイドライン[※229]」等を参照して、セキュリティ対策計画を立案し、対策を実施していくことが望まれる。

(b) サプライチェーンのセキュリティ対策状況の把握

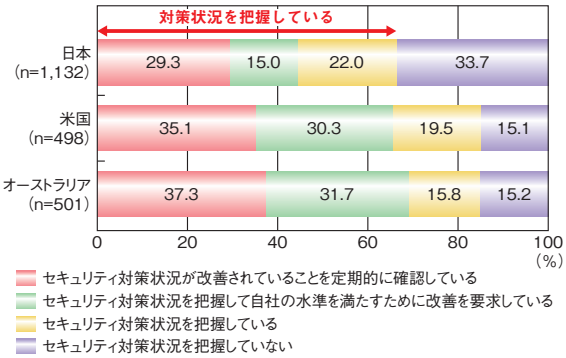
NRI セキュア社調査（図 2-4-2）によると、企業が国内関連子会社のセキュリティ対策状況を把握している割合は、日本では 66.3% で、米国とオーストラリアでは 80%



■図 2-4-1　セキュリティ対策計画の策定状況
(出典)NRI セキュア社「NRI Secure Insight 2021」を基に IPA が作成

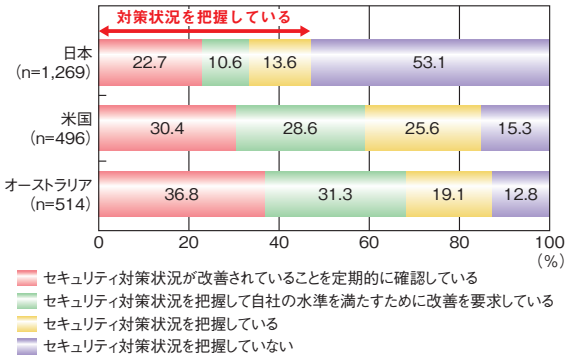
以上であった。また、自社の水準を満たすために関連子会社へ改善要求まで実施している割合は、日本では約 44.3% で、米国とオーストラリアでは 65% 以上であった。

国内パートナー／委託先への統制状況を調査した結果が図 2-4-3 (次ページ) である。国内パートナー／委託先のセキュリティ対策状況を把握している割合は、日本



■図 2-4-2　国内関連子会社に対するセキュリティ統制状況
(出典)NRI セキュア社「NRI Secure Insight 2021」を基に IPA が編集

では 46.9% で、米国とオーストラリアでは 85% 以上であった。また、自社の水準を満たすためにパートナー／委託先へ改善要求まで実施している割合は、日本では 33.3% で、米国とオーストラリアでは 60% 前後であった。



■図 2-4-3　国内パートナー／委託先に対するセキュリティ統制状況
(出典)NRI セキュア社「NRI Secure Insight 2021」を基に IPA が編集

日本でも、サプライチェーン上でのインシデントの増加や政府機関による注意喚起もあったためか、国内関連子会社に対するセキュリティ統制状況（前ページ図 2-4-2）では「セキュリティ状況を把握していない」割合は 33.7% であり、7 割弱の企業が何らかの取り組みを実施していた。しかし、統制対象が国内パートナー／委託先の場合（図 2-4-3）、「セキュリティ状況を把握していない」割合は 53.1% と約半数であった。子会社とは違って統制は容易ではないと推察されるが、米国、オーストラリアでは統制が進んでいることから、国内でも状況の改善が望まれる。2022 年 1 月に IPA が発表した「情報セキュリティ 10 大脅威 2022[※230]」によると、「サプライチェーンの弱点を悪用した攻撃」が 3 位となり、無視できない脅威になっている。業種・業態・事業規模に関係なく、サプライチェーンを構成するすべての事業者が対策を検討し、協力することが重要である。

(c) セキュリティ管理体制の構築状況

NRI セキュア社調査（表 2-4-1）によると、CISO を設置している企業の割合は、米国とオーストラリアが 90% 以上であるのに対し、日本は 46.1% にとどまっている。これは、同社が前年に行った同様の調査[※231]とおおむね同じ結果であり、CISO の設置は進んでいない。

	日本 (n=1,509)	米国 (n=503)	オーストラリア (n=511)
CISO	46.1%	94.8%	91.4%

■表 2-4-1　CISO の設置状況
(出典)NRI セキュア社「NRI Secure Insight 2021」を基に IPA が編集

(d) セキュリティ人材の充足状況

NRI セキュア社調査（表 2-4-2）によると、セキュリティ対策に従事する人材が不足しているとする企業における、不足している人材の種別として、日本では「セキュリティ戦略・企画を策定する人」が 1 位であり、米国とオーストラリアでは「経営層に対して適切な表現で、現状や対策内容等を説明・報告できる人」が 1 位であった。

	日本 (n=1,461)	米国 (n=66)	オーストラリア (n=61)
1 位	54.3% セキュリティ戦略・企画を策定する人	51.5% 経営層に対して適切な表現で、現状や対策内容等を説明・報告できる人	41.0% 経営層に対して適切な表現で、現状や対策内容等を説明・報告できる人
2 位	39.3% セキュリティリスクを評価・監査する人	33.3% セキュリティリスクを評価・監査する人	31.1% 関係部署との調整をしながら、セキュリティ対策を推進・統括できる人
3 位	38.4% ログを監視・分析して、危険な兆候をいち早く察知できる人	28.8% セキュリティ戦略・企画を策定する人	29.5% セキュアなシステム設計ができる人

■表 2-4-2　セキュリティ対策に従事する人材が不足していると考えている企業における、不足している人材種別
(出典)NRI セキュア社「NRI Secure Insight 2021」を基に IPA が編集

「2.4.1 (1) (a) セキュリティ対策計画の策定状況」で述べたとおり、日本では、「中長期の対策計画を立てている」企業の割合が少ない。表 2-4-2 の結果から、その背景として、セキュリティ戦略・企画を策定する人材が不足していることがうかがえる。

一方で、米国及びオーストラリアで「経営層に対して適切な表現で、現状や対策内容を説明・報告できる人」が求められる状況は、CISO 設置率の高さ（表 2-4-1）とも整合し、経営層がセキュリティに関与し、事業継続性やサイバー攻撃に対する防御力向上の観点で適切な経営判断を行うことを重要視していると推察される。

(2) セキュリティリスクマネジメント

国内の企業・組織は、「2.4.1 (1) 情報セキュリティに対する企業等の対策状況」で述べたようなセキュリティリスクに直面している。組織のセキュリティリスクを把握・管理するリスクマネジメントは、企業にとって経営・事業を守るための重要課題の一つである。リスクマネジメントには経営層のリーダーシップが欠かせないため、経済産

業省とIPAは、経営層のセキュリティリスクマネジメント向上を目的として、2017年に「サイバーセキュリティ経営ガイドライン Ver2.0[※232]」（以下、経営ガイドライン）を発行した。またIPAは、経営ガイドラインの実践には、対策状況の可視化や、参考となる実践事例（プラクティス）の提示が重要であることから、それらに関する取り組みを行ってきた。

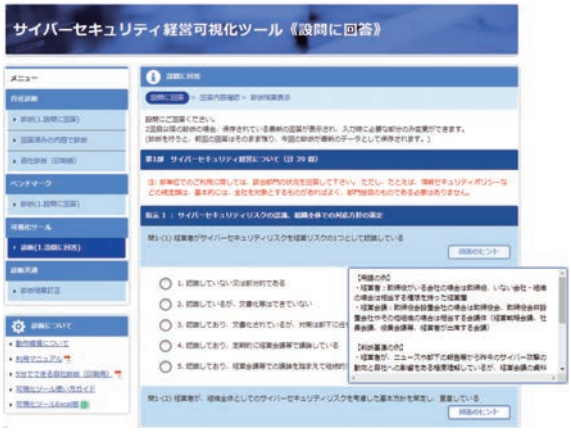
本項では、上記の取り組みを基にしたセキュリティリスクマネジメントについて述べる。

(a) サイバーセキュリティの対策状況

組織のセキュリティリスクマネジメントにおいては、経営層とCISO等のセキュリティマネジメントを統括する部門が情報共有できるように、自組織の対策状況を可視化することが重要である。IPAは、経営ガイドラインに基づく質問に回答することで、サイバーセキュリティ対策状況のレーダーチャート表示や業種平均との比較ができる「サイバーセキュリティ経営可視化ツール[※3]」（以下、可視化ツール）を提供している（図2-4-4）。回答方法は成熟度モデルに基づく5段階（最高5ポイント、最低1ポイント）の選択式（表2-4-3）で、回答者がなるべく客観的に判断できるようなヒントの提示（表2-4-4）により、利用者がより正確に回答できるよう工夫されている。

可視化ツールでは、回答に基づき、対策実施状況を経営ガイドラインで示された「重要10項目」ごとにレーダーチャート表示する。図2-4-5に2021年8～12月に利用者登録された企業全体と業種別（製造業、情報通信業）の回答の平均値を示す。

全回答の総計である「全体」では重要10項目の中で、指示1（サイバーセキュリティリスクの認識、組織全体での対応方針の策定）が3.1ポイントと最も高い。文書化まではできているものの、その見直し体制までは構築できていないことがうかがえる。一方、指示8（インシデントによる被害に備えた復旧体制の整備）、指示9（ビジネスパートナーや委託先を含めたサプライチェーン全体の対策及び状況把握）、指示10（情報共有活動への参加を通じ



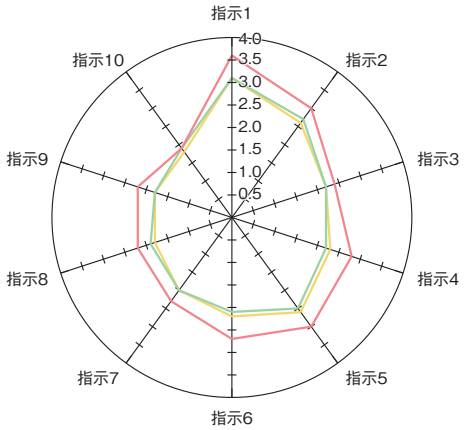
■図2-4-4　サイバーセキュリティ経営可視化ツール画面

問1-(1)	成熟度	企業の対応状況
経営者がサイバーセキュリティリスクを経営リスクの1つとして認識している	レベル1	認識していない又は部分的である
	レベル2	認識しているが、文書化等はできていない
	レベル3	認識しており、文書化されているが、対策は部下に任せている
	レベル4	認識しており、定期的に経営会議等で議論している
	レベル5	認識しており、経営会議等での議論を踏まえて継続的に改善している

■表2-4-3　5段階の成熟度モデルによる回答選択肢の例

問1-(1) の判断基準の例
・経営者が、ニュースや部下の報告等から昨今のサイバー攻撃の動向と自社への影響をある程度理解しているが、経営会議の資料等の形にしていなければレベル2。 ・経営会議の議題に入っているが、資料は付録、情シス責任者の報告を聞き流すだけ等であればレベル3以下。（経営者が自分の言葉で考え、語っているかがポイント。） ・経営会議の議題に入っており、かつ経営者が自分の考え、自分の言葉で議論していればレベル4。 ・経営会議で議論されたことが現場に展開され、その結果がまた経営会議に報告・議論されるというプロセスが回っていればレベル5。

■表2-4-4　問1-(1)の判断のためのヒント



指示1:サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示2:サイバーセキュリティリスク管理体制の構築
指示3:サイバーセキュリティ対策のための資源（予算、人材等）確保
指示4:サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示5:サイバーセキュリティリスクに対応するための仕組みの構築
指示6:サイバーセキュリティ対策におけるPDCAサイクルの実施
指示7:インシデント発生時の緊急対応体制の整備
指示8:インシデントによる被害に備えた復旧体制の整備
指示9:ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
指示10:情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

■図2-4-5　可視化ツールに利用者登録した企業のサイバーセキュリティ対策状況（2021年8～12月）

た攻撃情報の入手とその有効活用及び提供）は、1.8 ポイントと最も低い。対応方針の策定はできているものの、インシデント復旧体制の整備、サプライチェーンの状況把握、情報共有活動までは十分できていない実態がうかがえる。

個別の業種については、回答数の多かった二つを掲載している。「製造業」は「全体」とほぼ同様の傾向である。一方、「情報通信業」は指示 1 ～ 9 で「全体」を 0.2 ～ 0.5 ポイント上回り、取り組みが進んでいる業種であることがうかがわれる。その「情報通信業」においても指示 10 のポイントは低く、情報共有活動の実践は業種横断的な課題である可能性がある。

(b) セキュリティリスクマネジメントの実践事例

他社のセキュリティリスクマネジメント実践事例は、自社の同様なセキュリティ課題について対策を行う上で、有用な情報である。IPA は、企業へのアンケート及びインタビューを通じて収集した、実際に行われている施策に基づく「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 3 版※4」（以下、プラクティス集）を提供している。プラクティス集は、事例ごとに仮想的な企業を想定し、その企業が置かれている事業状況やセキュリティ等の状況、CISO 等及び関係者の役割、対策に関する意思決定、実際の作業について具体的に記載している。

プラクティス集では、二つのタイプ（重要 10 項目の実践に紐づくものと、重要 10 項目を横断する課題の解決に紐づくもの）を掲載している。ここでは、そのうち前者のタイプで重要 10 項目の指示 1 の実践に紐づく事例を紹介する。

従業員数 1 万名規模の精密機器メーカである C 社では、ある拠点で製品サポートを提供した顧客情報の管理不備が見つかった。意図しない漏えいリスクに危機感を抱いた経営層は本社の CISO を中心に対応を指示した。CISO が各拠点の事情を踏まえ実践した手順は次のとおりである。

①専門家の助言を基に、拠点立地国の個人情報やプライバシー情報の保護に関する要求事項（例：EU の GDPR（General Data Protection Regulation：一般データ保護規則））を整理した上、現地に対策を委ねることが困難な拠点を洗い出した。

②当該拠点ごとのチェックリスト（例：個人情報を定められた場所に保存しているか、保管期限を経過した情報を削除しているか等）を作成した。

③各拠点担当者が、本社の支援のもとチェックリストを用いて定期的な自己点検を実施した。

④情報セキュリティ対策に関する内部監査で、上記の自己点検結果を監査することで現地法規制の遵守状況を確認し、必要に応じて是正を指示した。

CISO は①～④のプロセスを統括し、②のチェックリスト作成にあたっては、正確性を担保しつつ現地の商習慣、スタッフの役割等を考慮し各業務内容に沿った記載とすることで、現地スタッフにとって分かりやすい内容となるよう努めた。

なお、上記のような他社のプラクティスを参考にする際は、実践内容をそのまま受け入れるのではなく、自社の問題に置き換えて取り得る対策、重点化する対策等を柔軟に考えることが重要である。

(c) まとめ

セキュリティリスクマネジメントについて、経済産業省はサイバーセキュリティ経営ガイドラインの実践を通じた経営層のコミットメント強化を推進しており、そのための重要な支援ツールとして可視化ツールとプラクティス集が位置付けられている（「2.1.2 (1) (b) WG2（経営・人材・国際）」参照）。企業の経営層や CISO 等を含むリスクマネジメント統括部門はこれらの支援ツールを有効に活用し、セキュリティリスクマネジメントの向上に取り組むことが望まれる。

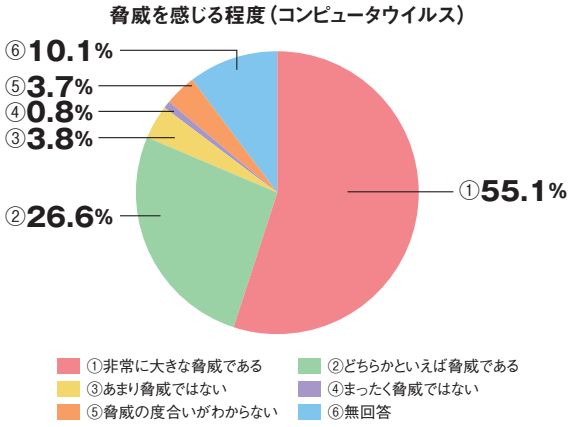
2.4.2 中小企業に向けた情報セキュリティ支援策

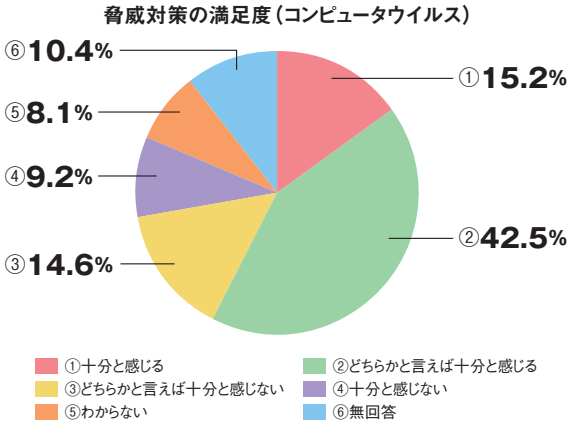
本項では、中小企業における情報セキュリティ、対策支援、及び普及啓発・対策ツールの現状について紹介する。

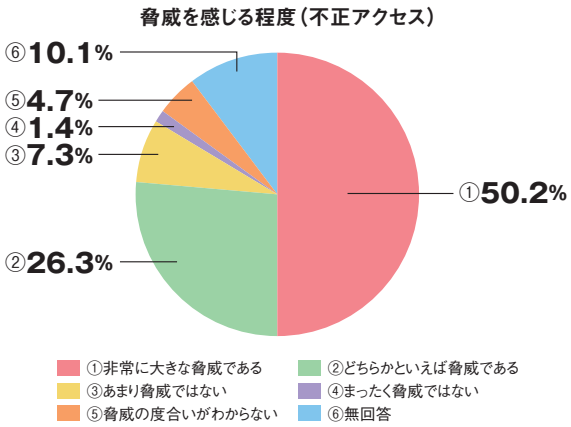
(1) 中小企業の情報セキュリティの現状

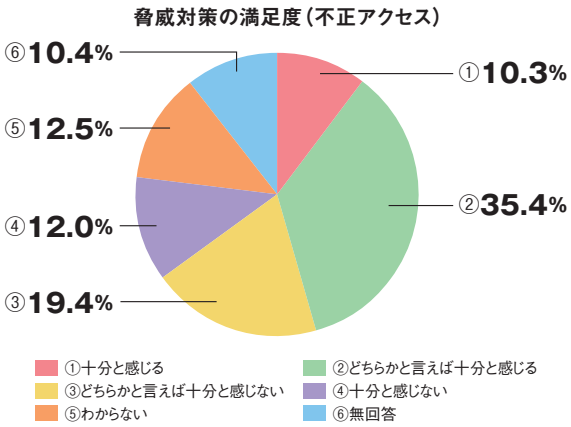
IPA が 2022 年 3 月 31 日に発表した「2021 年度 中小企業における情報セキュリティ対策に関する実態調査報告書※233」によると、情報セキュリティに関する脅威について、コンピュータウイルスを「非常に大きな脅威である」または「どちらかといえば脅威である」と認識している企業の割合は 81.7% であった。また、不正アクセスを「非常に大きな脅威である」または「どちらかといえば脅威である」と認識している企業は 76.5% であった（次ページ図 2-4-6）。

一方で、脅威対策の満足度について、ウイルス対策を









■図 2-4-6　情報セキュリティに関する脅威
（出典）IPA「2021 年度中小企業における情報セキュリティ対策の実態調査報告書」を基に編集

■図 2-4-7　脅威対策の満足度
（出典）IPA「2021 年度中小企業における情報セキュリティ対策の実態調査報告書」を基に編集

「十分と感じる」または「どちらかと言えば十分と感じる」という企業の割合は 57.7% であった。また、不正アクセス対策を「十分と感じる」または「どちらかと言えば十分と感じる」という企業の割合は 45.7% であった（図 2-4-7）。

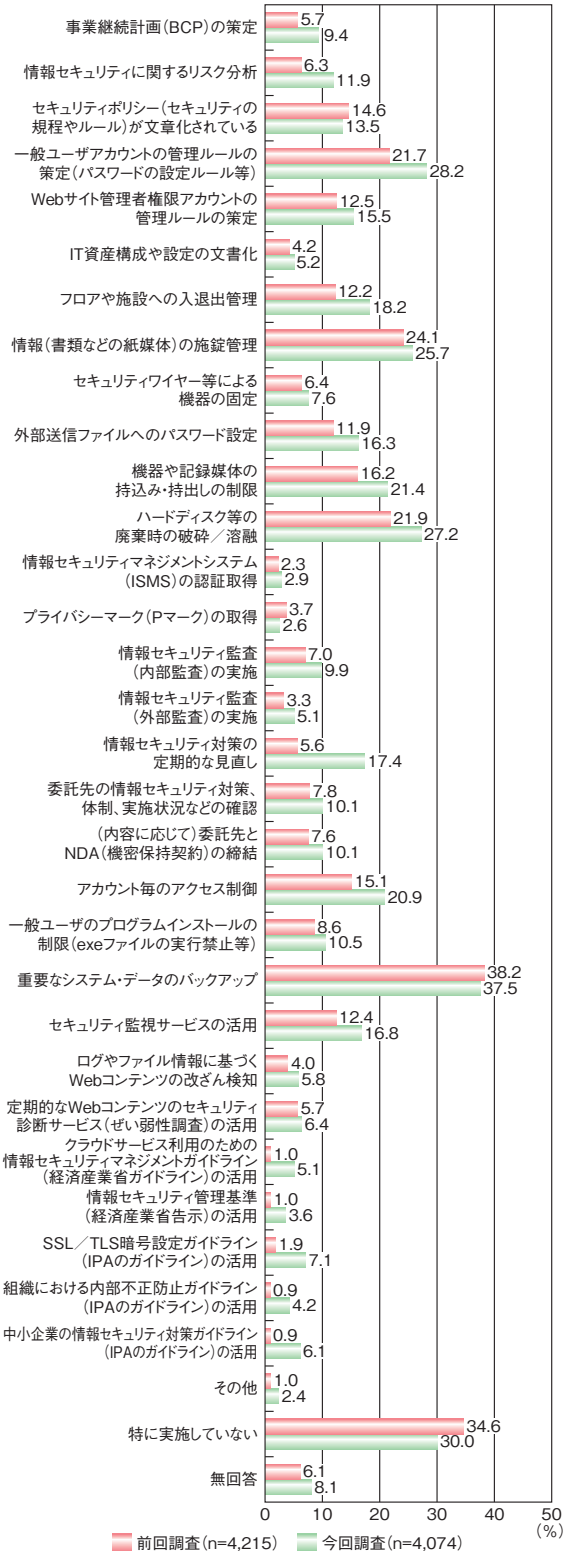
被害防止のための組織面・運用面の対策の実施状況については、「重要なシステム・データのバックアップ」の割合が最も高く 37.5% となっている。次いで、「特に実施していない」（30.0%）、「一般ユーザアカウントの管理ルールの策定（パスワードの設定ルール等）」（28.2%）となっている。2016 年度に実施した同調査の結果と比較すると、「特に実施していない」の割合が 34.6% から 30.0% へ減少し、大半の項目で実施割合がわずかながら増加している（次ページ図 2-4-8）。

情報セキュリティ関連製品やサービスの導入状況については、「ウイルス対策ソフト・サービスの導入」の割合が最も高く 77.2% となっている。次いで、「ファイアウォール」（35.6%）、「VPN」（17.1%）となっている。2016 年度調査の結果と比較すると、「VPN」の導入割合が 11.9% から 17.1% に増加しているものの、その他の選択肢については大きな差はない（次ページ図 2-4-9）。

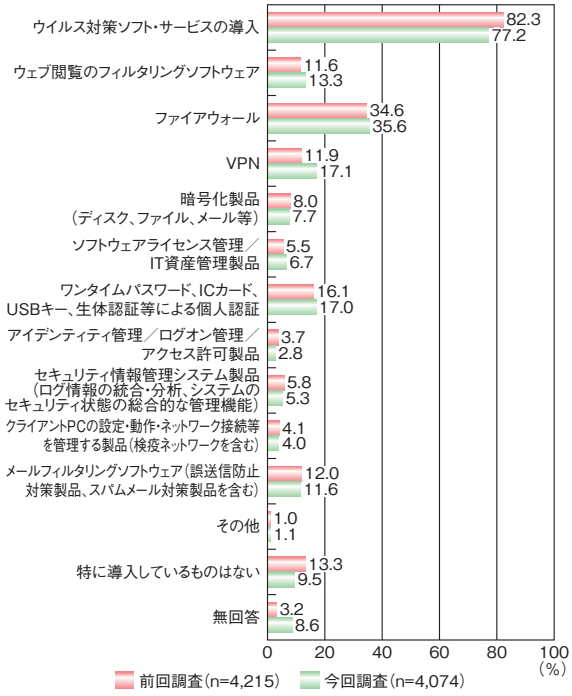
販売先・仕入先との契約締結時における情報セキュリティに関する条項・取引上の義務・要請については、「義務・要請はない」の割合が高く 63.2% となっている。「義務・要請がある」の割合は、26.1% である（次ページ図 2-4-10）。

また、「義務・要請がある」と回答した企業のうち、契約時における情報セキュリティに関する要請について、「秘密保持」の割合が最も高く 93.8% となっている。次いで、「契約終了後の情報資産の扱い（返却、消去、廃棄等）」（36.3%）、「情報セキュリティに関する契約内容に違反した場合の措置」（32.4%）となっている（次ページ図 2-4-11）。

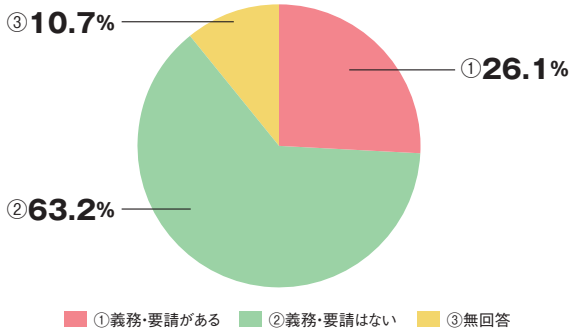
このような調査結果から、中小企業では情報セキュリティに関する脅威を認識しているものの、十分な対策がとられているとは言えない状況にあることが分かった。また、サプライチェーン上の販売先・仕入先等からの情報セキュリティに関する義務・要請も十分に行われていない。しかし、「サイバーセキュリティお助け隊事業（令和 2 年度中小企業向けサイバーセキュリティ対策支援体制構築事業）成果報告書※234」では、業種や事業規模を問わずサイバー攻撃や不審なアクセス等の脅威に晒されて



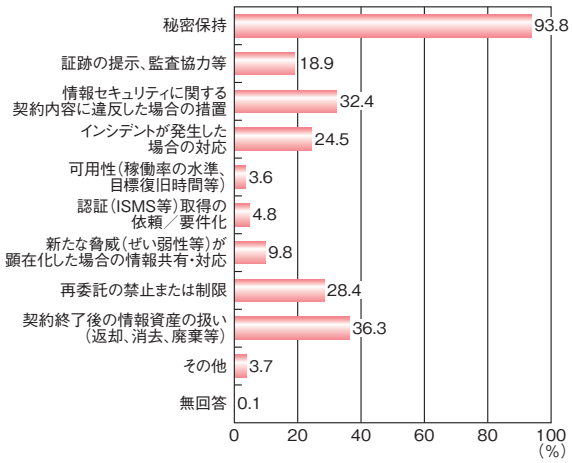
■図 2-4-8　被害防止のための組織面・運用面の対策(複数回答)
(出典)IPA「2021 年度中小企業における情報セキュリティ対策の実態調査報告書」を基に編集



■図 2-4-9　情報セキュリティ関連製品やサービスの導入状況(複数回答)
(出典)IPA「2021 年度中小企業における情報セキュリティ対策の実態調査報告書」を基に編集



■図 2-4-10　販売先・仕入先からの情報セキュリティに関する条項・取引上の義務・要請
(出典)IPA「2021 年度中小企業における情報セキュリティ対策の実態調査報告書」を基に編集



■図 2-4-11　契約時における情報セキュリティに関する要請(販売先(発注元企業)との契約時)(複数回答)
(出典)IPA「2021 年度中小企業における情報セキュリティ対策の実態調査報告書」を基に編集

いる状況が明らかになっている。中小企業を含むサプライチェーン全体でのセキュリティの確保が望まれる。

(2) 中小企業向け情報セキュリティ対策支援施策

政府が 2021 年度に新たに実施した中小企業向け情報セキュリティ対策支援施策を紹介する。

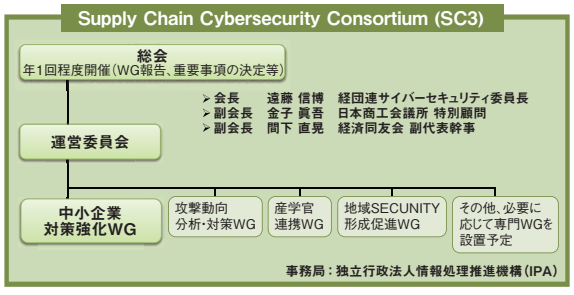
(a) サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)

経済産業省は 2020 年度に引き続き 2021 年度、IPA を通じて、産業界が一体となって中小企業を含むサプライチェーン全体のサイバーセキュリティ対策を推進する運動「サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)※235」の支援を行った。

具体的には、中小企業対策強化 WG では、サイバーセキュリティお助け隊サービスの普及に向けた議論や中小企業を対象としたウェビナーの開催等を行った。

また、2021 年 6 月の運営委員会において、攻撃動向分析・対策 WG 及び地域 SECUNITY 形成促進 WG、産学官連携 WG が新たに設置された(図 2-4-12)。このうち地域 SECUNITY 形成促進 WG は、全国各地で活動する地域のセキュリティコミュニティ(通称、地域 SECUNITY)を対象に地域間の情報共有や共通課題の解決に向けた取り組みを検討・推進することを目的としたワークショップを開催した。

今後、各 WG の活動を通じて、地域や業界に閉じない横断的な活動を展開していくことが期待される。



■図 2-4-12　SC3 の組織体制
(出典)IPA「サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)とは※236」

(b) 地域 SECUNITY 形成促進事業

経済産業省は 2021 年度、地域に根差したセキュリティコミュニティの形成促進のため「地域 SECUNITY 形成促進事業」を実施した。

本事業では、地域のセキュリティ関係者(公的機関、教育機関、地元企業、地元ベンダ等)が集まり、セキュリティについての相談や意見交換を行う地域 SECUNITY の形成を促進するために、地域ごとの形成状況に応じて、調査やセミナー、ワークショップ、専門家派遣、有識者会議等の取り組みを行った。

今後、地域の中でセキュリティに関する情報の収集や相談が行える「共助」の取り組みが、全国各地で展開されることが期待される。

(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) サイバーセキュリティお助け隊サービス制度

IPA は 2021 年度、中小企業に対するサイバー攻撃への対処として不可欠なサービスの要件をまとめた「サイバーセキュリティお助け隊サービス基準※237」を満たした民間セキュリティ事業者のサービスを「サイバーセキュリティお助け隊サービス※6」として登録・公表した。

サイバーセキュリティお助け隊サービス基準は、相談窓口、異常の監視、緊急時の対応支援、簡易サイバー保険等の各種サービスをワンパッケージで安価に提供することを要件としている(表 2-4-5)。同基準を満たすサービスには、「サイバーセキュリティお助け隊マーク」の利用が許諾される(次ページ図 2-4-13)。

2022 年 3 月末時点で 12 のサービスが登録されている。中小企業が無理なくサイバーセキュリティ対策を導入・運用できる具体的なサービスが明示されることで、サ

主な要件	概要
相談窓口	ユーザからの相談を受け付ける窓口を設置／案内
異常の監視の仕組み	ネットワーク及び／または端末を 24 時間見守る仕組みを提供
緊急時の対応支援	インシデント発生等の緊急時には駆け付け支援
中小企業でも導入・運用できる簡単さ	専門知識がなくても導入・運用できるような工夫
簡易サイバー保険	突発的に発生する駆付け費用等を補償するサイバー保険
中小企業でも導入・維持できる価格	・ネットワーク一括監視型:月額 1 万円以下(税抜き) ・端末監視型:月額 2,000 円以下／台(税抜き) ・併用型:これらの和に相当する価格を超えないこと ※端末 1 台から契約可能であることが条件

■表 2-4-5　サイバーセキュリティお助け隊サービス基準の主な内容
(出典)IPA「サイバーセキュリティお助け隊サービス基準」を基に作成

■図 2-4-13　サイバーセキュリティお助け隊マーク

■図 2-4-14　SECURITY ACTION ロゴマーク

プライチェーン全体のセキュリティの強化が期待される。

(b) 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※238」を運営し、中小企業と関連の深い中小企業支援機関、士業団体、IT 関連団体と連携して SECURITY ACTION を通じた情報セキュリティの普及啓発を行っている(図 2-4-14)。

SECURITY ACTION に基づく自己宣言は、経済産業省が実施するものづくり・商業・サービス生産性向上促進補助金のデジタル枠の申請要件になっているほか、公的な補助金制度の申請要件としても活用されている。

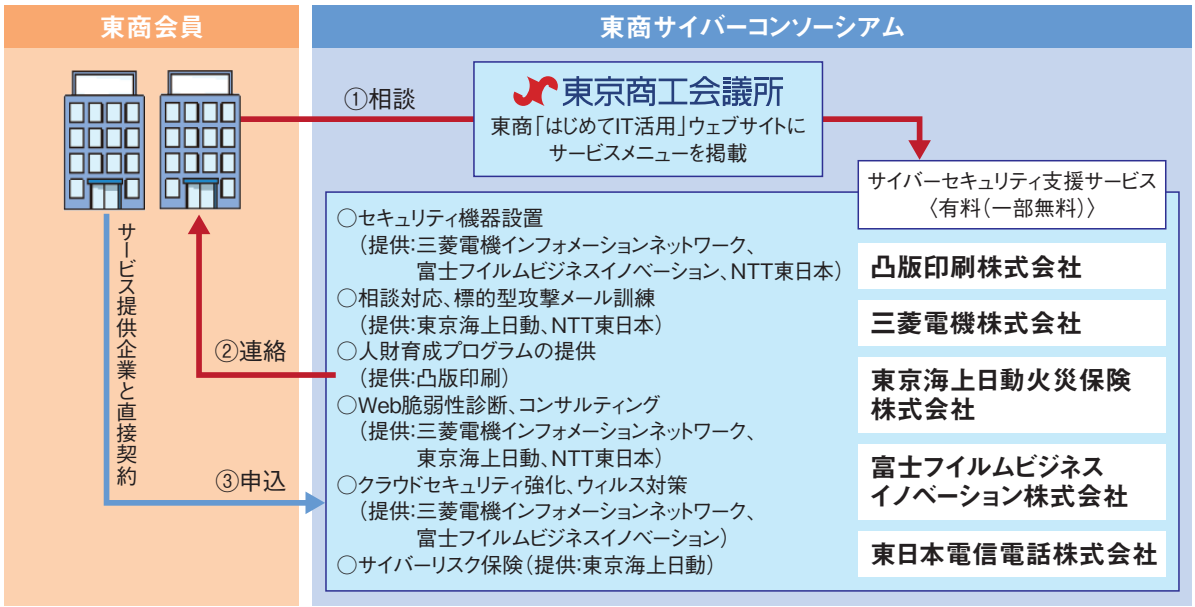
2022 年 1 月末時点の宣言数は 18 万件(個人事業主を含む)を超えている。今後、より多くの中小企業が SECURITY ACTION を宣言し、社内の意識付けや社外への信頼性のアピール等に活用し、対策を推進することが望まれる。

(c) 東商サイバーセキュリティコンソーシアム

東京商工会議所は 2021 年 7 月 30 日、会員企業のサイバーセキュリティ対策支援を目的とした「東商サイバーセキュリティコンソーシアム※239」を設立した(図 2-4-15)。

東京商工会議所では、従前より展開している「『はじめて IT 活用』1 万社プロジェクト」において、中小・小規模事業者の IT 活用を総合的に支援してきた。この枠組みの中でコンソーシアムを設立し、東京商工会議所と参画企業 5 社が連携し、専用 Web サイトを通じて、中小企業向けサイバーセキュリティ支援サービスを提供している。

地域の総合経済団体による中小企業へのサイバーセキュリティ対策支援の取り組みの一つのモデルとして、今後全国へと拡大していくことが期待される。



■図 2-4-15　東商サイバーセキュリティコンソーシアムの連携スキーム図
(出典)東京商工会議所「『東商サイバーセキュリティコンソーシアム』が本日発足　～東商とサイバーセキュリティ対策のノウハウを持つ大手 5 社が業界を横断し、初連携! 増大するサイバーリスクにさらされる中小企業を総合的に支援～※240」を基に編集

2.4.3 教育機関・政府及び地方公共団体等法人における対策状況

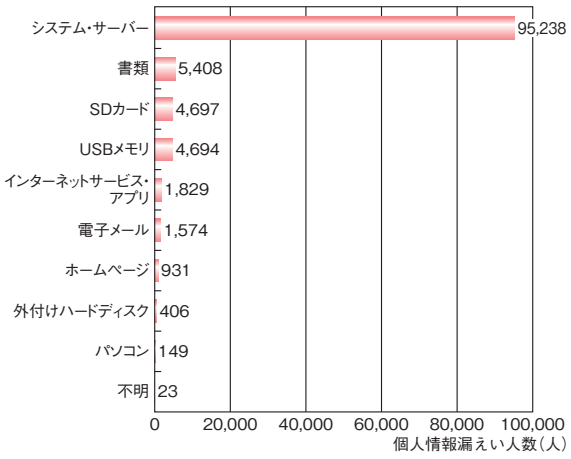
教育機関・政府及び地方公共団体等法人における対策状況について、公表されている資料に基づいて述べる。

(1) 教育機関における個人情報紛失・漏えいの現状

教育ネットワーク情報セキュリティ推進委員会（ISEN：Information Security for Education Network）は、毎年、学校等教育関連機関で発生した個人情報の紛失・漏えい事故について公開情報を調査し、公表している。2021 年 11 月、「令和 2 年度（2020 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※241」（以下、ISEN 報告書）を公表した。本項では、ISEN 報告書に基づいて、2020 年 4 月 1 日～ 2021 年 3 月 31 日の間の事故の傾向について述べる。

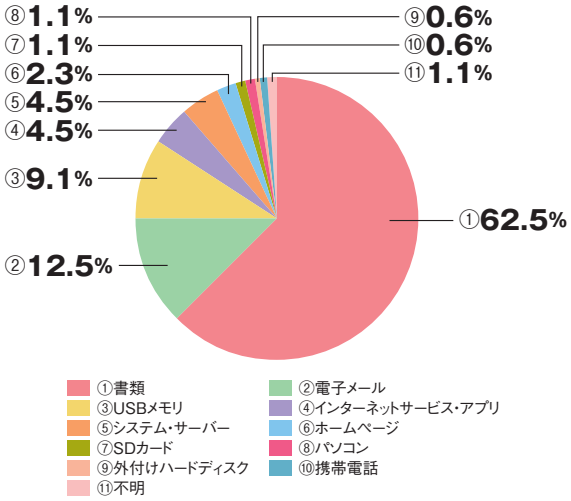
ISEN 報告書によると、2020 年度は 170 件（2019 年度 226 件）の個人情報漏えい事故が発生し、11 万 4,232 人分（2019 年度 23 万 6,185 人分）の個人情報が漏えいした。2019 年度と比較すると、発生件数は約 25% 減少し、漏えい人数は半減した。

漏えいした個人情報の人数を経路・媒体ごとに比較すると、図 2-4-16 に示すように、2020 年度は学校、教育委員会が管理する「システム・サーバー」が 9 万 5,238 人と最も多く、2 位の「書類」以下を大きく引き離している。



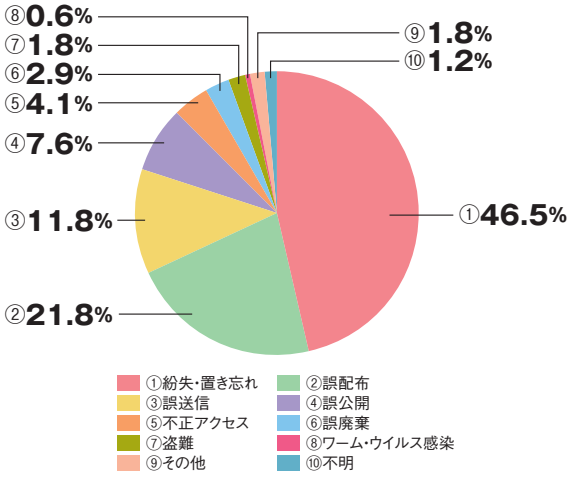
■図 2-4-16　漏えい経路・媒体別個人情報漏えい人数※242
（出典）ISEN 報告書を基に IPA が作成

一方で、漏えいした個人情報の漏えい経路・媒体ごとの事故発生件数は、図 2-4-17 に示すように「書類」の 62.5% が最も多く、次いで「電子メール」の 12.5% となっている。これに対し「システム・サーバー」を起因とする事故発生件数は全体の 4.5% と少なく、1 件あたりの個人情報の漏えい人数が顕著に大きいことが分かる。



■図 2-4-17　漏えい経路・媒体別事故発生件数
（出典）ISEN 報告書を基に IPA が作成

漏えい人数とは別に、事故の種類ごとの発生件数を調べると、「紛失・置き忘れ」「誤配布」「誤送信」「誤公開」「誤廃棄」のように「不注意」による事故が全体の 90.6% に上っている（図 2-4-18）。



■図 2-4-18　漏えい事故種別発生割合
（出典）ISEN 報告書を基に IPA が作成

このように教育機関等においては、個人情報が記録された書類や USB メモリの紛失・置き忘れ、誤配布等の不注意による事故が後を絶たない。学校における安全安心な ICT 活用に向け情報セキュリティ対策を講じることが求められる中、情報管理不備（不注意）対策と「システム・サーバー」等からの情報漏えい対策の徹底が、ますます重要になっている。

(2) 文部科学省における対策

文部科学省における情報セキュリティの取り組みを「『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 4 年 3 月)改定について※243」に基づき述べる。

2017 年 10 月、教育委員会・学校が情報セキュリティポリシーの作成や見直しを行う際の参考となる「教育情報セキュリティポリシーに関するガイドライン」が策定され、その後、順次改定されてきた。

まず 2019 年 12 月、「多様な子供たちを誰一人取り残すことなく、公正に個別最適化され、資質・能力が一層確実に育成できる教育 ICT 環境」の実現を目指す、とする GIGA スクール構想※244 の始動に合わせて 1 回目の改定が実施された。

その後、新型コロナウイルス感染拡大に伴い、学びの環境を保障するために GIGA スクール構想計画は前倒しされた。すなわち、当初「教育の ICT 化に向けた環境整備」については「5 か年計画(2018 ～ 2022 年)※245」とされていたが、1 人 1 台の端末整備や高速大容量の校内通信ネットワークの整備等の GIGA スクール構想計画は、3 度の補正予算によって 2020 年度内に完了した※246。

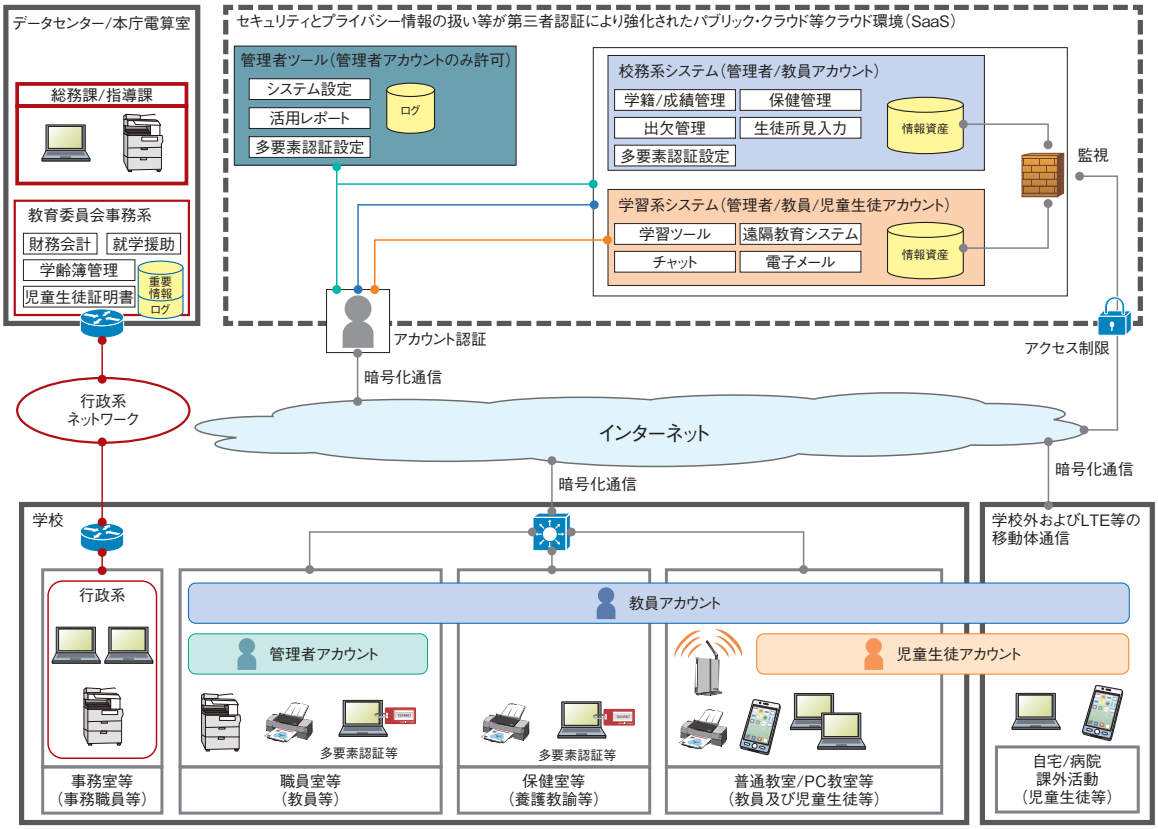
このような環境整備に併せて必要となるセキュリティ対策やクラウドサービスの活用に向けたネットワーク構成等の課題に対応するため、2021 年 5 月に 2 回目の改訂が実施され※247、「『教育情報セキュリティポリシーに関するガイドライン』(令和 3 年 5 月版) ハンドブック※248」も公表された。

2021 年 5 月の改定では、学校内外での学習者用端末の活用や、クラウドサービス活用に向けた ID 管理等に関するセキュリティ対策が多く追記された。また、過渡期としてのローカルブレイクアウト※249 構成や、校務系／学習系のネットワーク分離を必要としない教育情報ネットワークの構成等についても記載された。

更に 2021 年 12 月、「デジタル社会の実現に向けた重点計画」が閣議決定され※250、今後、各地方公共団体においてもクラウドの利用を念頭にセキュリティを検討していくことが方向付けられた。

2022 年 3 月には、その方針を踏まえ、デジタル庁の支援のもと、3 回目となる改定が実施され※251、「『教育情報セキュリティポリシーに関するガイドライン』ハンドブック(令和 4 年 3 月)※252」も公開された。

同ガイドラインで提示された、1 人 1 台端末を活用するために必要なネットワーク構成のイメージ (アクセス制御による対策を講じたシステム構成)を図 2-4-19 に示す。



■図 2-4-19　1 人 1 台端末を活用するために必要なネットワーク構成例
(出典)文部科学省「『教育情報セキュリティポリシーに関するガイドライン』ハンドブック(令和 4 年 3 月)」を基に IPA が編集

2022 年 3 月の改定では、今後の推奨ネットワーク構成となる、校務系／学習系のネットワーク分離を必要としない教育情報ネットワーク構成としての「アクセス制御による対策を講じたシステム構成」と、これまでの「ネットワーク分離による対策を講じたシステム構成」を明確に区分し、その上で「アクセス制御による対策を講じたシステム構成」について、特に校務用端末における「リスクベース認証[※253]」「ふるまい検知[※254]」「マルウェア対策」「暗号化」「SSO（シングルサインオン）の有効性」等の詳細な技術的対策が追記された。

また、上記それぞれの構成における「校務用端末の使い分け」についての記述の適正化や、「校務用端末の持ち出し」に関する記述の適正化が図られた。

今後の GIGA スクール構想の進展において、セキュリティが担保されることで、「これまでの我が国の教育実践と最先端の ICT のベストミックスを図ることにより、教師・児童生徒の力を最大限に引き出す[※244]」環境が整備されることが期待される。

(3) 地方自治体等における対策状況

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 2021 年 8 月に公表した「地方自治情報管理概要～電子自治体の推進状況（令和 2 年度）～[※255]」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 2-4-6 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。2019 年度[※256]と 2020 年度との実施率の差も併せて記載している。

2019 年度に都道府県では 10 項目、市区町村では全項目について 100%の実施率を達成できていなかったが、2020 年度に都道府県では「重要なデータへのアクセス制限（権限設定、認証）を実施」「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」の 2 項目について新たに 100% の実施率を達成した。しかしながら、都道府県では全 22 項目中 8 項目が、市区町村では依然として全項目が 100% の

対策実施率（都道府県は 47、市区町村は 1,741）							
	対象項目	都道府県	市区町村		対象項目	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)	99.9% (+0.1ポイント)	(B)	緊急時対応訓練を実施している	87.2% (0.0ポイント)	40.1% (+7.1ポイント)
(A)	緊急時対応計画を整備	100.0% (0.0ポイント)	72.8% (+3.2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% (+0.0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)	95.5% (+2.6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)	99.7% (0.4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	85.1% (+10.6ポイント)	72.9% (+9.1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	100.0% (+2.1ポイント)	99.8% (+0.1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	80.9% (+6.4ポイント)	55.2% (+7.4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)	98.6% (+0.7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)	99.5% (+0.2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% (+0.0ポイント)	93.3% (1.6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)	98.1% (+0.7ポイント)		重要なデータを暗号化し保存	89.4% (+2.2ポイント)	56.7% (+6.7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)	99.1% (+0.5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% (+0.0ポイント)	97.8% (+1.5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)	98.9% (+0.6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	100.0% (+2.1ポイント)	80.0% (+8.9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	97.9% (4.3ポイント)	93.7% (+2.5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	74.5% (+6.4ポイント)	58.5% (+9.0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)	94.1% (+1.2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	70.2% (+10.6ポイント)	49.1% (+10.4ポイント)

■表 2-4-6　地方公共団体における主な情報セキュリティ対策状況（2020 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２年度）～」「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）～[※256]」を基に IPA が作成

実施となっていない。

基本的な個別対策の中で「情報資産について、機密性、完全性及び可用性により分類」については都道府県、市区町村ともに前年度からの改善ポイントは高いものの達成率そのものは都道府県 85.1%、市区町村 72.9% にとどまっている。

また、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、今後の改善が求められる。都道府県においても「緊急時対応訓練を実施している」の項目については前年度からの改善が見られていないことから、併せて今後の改善が求められる。

2.4.4 一般利用者における対策状況

IPA では、2005 年から情報セキュリティの脅威に対する意識調査を、2013 年から倫理に対する意識調査を継続して実施しており、標的型攻撃やランサムウェア等の脅威に対する認知度、インターネットを利用する上で利用者に求められる各種対策、SNS 利用における意識、経験等を調査している。2020 年度に調査仕様を見直し、2021 年度調査は仕様変更後 2 回目の調査となった。本項では、同調査※257 のうち、情報セキュリティの脅威に対する意識調査について、主に追加分析を行った結果を紹介する。

(1) 使用機器の違いによる対策状況の差

脅威に対する意識調査はパソコン利用者とスマートフォン利用者※258 を対象に、それぞれの機器の特性や使用環境に応じた質問を設定し、実施している。調査結果では、総じてスマートフォン利用者のセキュリティ対策実施率※259（以下、対策実施率）が低い。具体的には、セキュリティ対策実施の有無を問う全 17 問中、スマートフォン利用者の対策実施率が 50% を超えるのは 3 問のみであった（表 2-4-7 の「A：全体」）。一方、パソコン利用者は全 20 問中、対策実施率が 50% を超える質問は 8 問※260 であった。そこでスマートフォン利用者の対策実施率の低さの要因を探るため、回答者属性等の追加分析を行った。

(2) スマートフォン利用者の対策実施状況

追加分析の結果を以下に示す。

スマートフォン利用者のセキュリティ対策実施状況	A: 全体（n=5,000）	B: スマートフォンのみを利用（n=1,749）	C: スマートフォンでの利用時間が長い（n=3,251）	B-C 差
（可能な機種の場合）OS のアップデート	51.6%	41.3%	57.2%	-15.9%
信頼できる場所（公式サイト、公式ストア等）からアプリをインストールする	56.4%	48.2%	60.8%	-12.6%
アプリをインストールする前または実行時に要求される権限を確認する	46.1%	38.8%	50.0%	-11.2%
端末内のアプリのアップデート	59.2%	53.0%	62.5%	-9.5%
紛失時などに備えたデバイス捜索対策	29.6%	22.4%	33.4%	-11.0%
リモートロックなどの不正利用防止機能	26.1%	20.0%	29.4%	-9.5%
パスワードや PIN、パターンなどによる画面ロック機能	46.4%	39.5%	50.1%	-10.7%
指紋認証・顔認証など、生体認証による画面ロック機能	42.9%	34.4%	47.5%	-13.1%
アプリをインストールする前にレビューやコメントなどを確認する	46.8%	40.3%	50.3%	-10.1%
デバイス内データ（写真、動画、個人情報など）のバックアップ	43.3%	35.8%	47.4%	-11.6%
セキュリティソフト・サービスの導入・活用	38.5%	26.4%	44.9%	-18.5%
重要な情報を扱うアプリの個別ロック機能の活用	24.9%	17.2%	29.1%	-11.9%
パスワード、指紋、ワンタイムパスワード等から 2 種類以上を組合わせる多要素認証の積極的な利用	39.3%	30.8%	43.8%	-13.0%
IoT 機器にアカウント設定があれば、購入後すぐにパスワードの変更等セキュリティ設定を実施	29.1%	22.1%	32.8%	-10.7%
セキュリティのサポートが終了した IoT 機器等の利用を止めている	27.3%	20.6%	30.9%	-10.3%
使わなくなった IoT 機器は、ネットから切り離している	30.1%	22.9%	34.0%	-11.0%
IoT 機器を廃棄する場合には購入時の状態に初期化している	29.6%	22.4%	33.6%	-11.2%

■表 2-4-7　スマートフォン利用者のセキュリティ対策実施状況比較

(a) インターネットを利用する機器の違いによる対策実施率

スマートフォン利用者向け調査は、事前調査の回答から、インターネットの利用をパソコンではなくスマートフォンのみで行う回答者※261と、パソコンも使っているがスマートフォンの方が利用時間が長い※262（以下、スマートフォンでの利用時間が長い）回答者を対象としている。サンプル総数 5,000 人のうち、2021 年度調査では「スマートフォンのみを利用」している人が 1,749 人、「スマートフォンでの利用時間が長い」人が 3,251 人であった。

スマートフォン利用者の対策実施率について、「全体」（以下、A 群）と「スマートフォンのみを利用している人」（以下、B 群）、「スマートフォンでの利用時間が長い人」（以下、C 群）、及び「B 群」「C 群」の実施率の差分を表 2-4-7（前ページ）に示す。

「A 群」の対策実施率が 50% を超えるのは「（可能な機種の場合）OS のアップデート」「信頼できる場所（公式サイト、公式ストア等）からアプリをインストール」「端末内のアプリのアップデート」の 3 問である。そして「B 群」「C 群」と「A 群」を比較すると、「B 群」の対策実施率が全設問で「A 群」より低く、逆に「C 群」は「A 群」より高い。「B 群」と「C 群」では、後者の方がおおむね 10% 程度対策実施率が高かった。表 2-4-7（前ページ）にあるスマートフォン利用者向けの設問の選択肢は、パソコンの使用経験から得られる知見等ではなく、ほとんどがスマートフォンに特化した対策事項である。にもかかわらず、「B 群」の対策実施率が低かった。この要因について以降で考察する。

(b) パスワード設定におけるセキュリティ対策実施率

パスワード設定における対策状況を比較した。パスワードのセキュリティ対策においても「B 群」の実施率が低いことが分かる（表 2-4-8）。「A 群」の母数 4,661 人は、事前質問においてインターネットサービスのアカウントを持っている人（パスワード設定の必要がある人）、また 3,930 人はインターネットのサービスアカウントを 2 個以上保有する人である。

表中の四つの対策のうち、最も実施率が低いのは「使いまわさない」であるが、「B 群」の対策実施率は 41.5%、初期パスワードを変更していない割合も 41.4% と少ない。「A 群」も 36.3% が、例えば Web サービスや IoT 機器等で提供される初期パスワードを変更しないまま、利用していることになる。

表 2-4-7（前ページ）及び表 2-4-8 のとおり、「B 群」は

	A: 全体（n=4,661）	B：スマートフォンのみを利用（n=1,578）	C:スマートフォンでの利用時間が長い（n=3,083）	B-C 差
推測されにくい	70.9%	67.1%	72.8%	-5.7%
出来るだけ長い	59.7%	54.4%	62.4%	-8.0%
初期パスワードを変更	63.7%	58.6%	66.3%	-7.8%
	（n=3,930）	（n=1,264）	（n=2,666）	B-C 差
使いまわさない	45.7%	41.5%	47.7%	-6.2%

■表 2-4-8　パスワード設定におけるセキュリティ対策実施状況

セキュリティ対策全般について、対策実施率が「A 群」より低い。「B 群」は事前アンケートで「現在はパソコンでインターネットを使っていない」を選択しており、調査時点で私物のパソコンを使わない、あるいは所有していない状況だったと考えられる。

このことから、現在、パソコンでインターネットを使っていないことと、セキュリティ対策の学びの少なさに関係があるのではないかとの仮説を立て、セキュリティ教育の受講経験の割合について調べた。

(c) セキュリティ教育の受講経験割合

「スマートフォン利用者」（以下、A 群）及び「パソコン利用者」（以下、D 群）のセキュリティ教育の受講経験割合を確認した（表 2-4-9）。「A 群」と「D 群」で比較すると前者が 1.8% 低いが大きな差ではない。次に「A 群」の中で、前節の「B 群」と「C 群」を比較すると「B 群」の受講経験が 6.6% 低かった。

昨今、パソコンを多用する職場では、社員教育の一環としてセキュリティ教育が進み、教育機会はある程度確保されていると考えられる。上記結果からも、パソコンの利用経験（所有）があることによって、情報セキュリティ教育の受講機会が得られ、セキュリティ対策やリテラシーの向上につながっている可能性がある。その一方で、「B 群」は、受講機会が得られにくく、対策の必要性への理

A 群：スマートフォン利用者（n = 5,000）	15.1%
B 群：スマートフォンのみでインターネットを利用（n = 1,749）	10.8%
C 群：スマートフォンでの利用時間が長い（n = 3,251）	17.4%
D 群：パソコン利用者（n = 5,000）	16.9%
B 群と C 群の差	-6.6%

■表 2-4-9　セキュリティ教育の受講経験割合の比較

解や対策実施率の低さにつながっている可能性が考えられる。セキュリティ教育の受講機会が「D 群」程ないと想定される「B 群」にとって自主的に受講機会を得るのは難しい。「B 群」に対し、どのようなセキュリティの学習（教育）機会をどうやって提供するかが課題と考えられる。

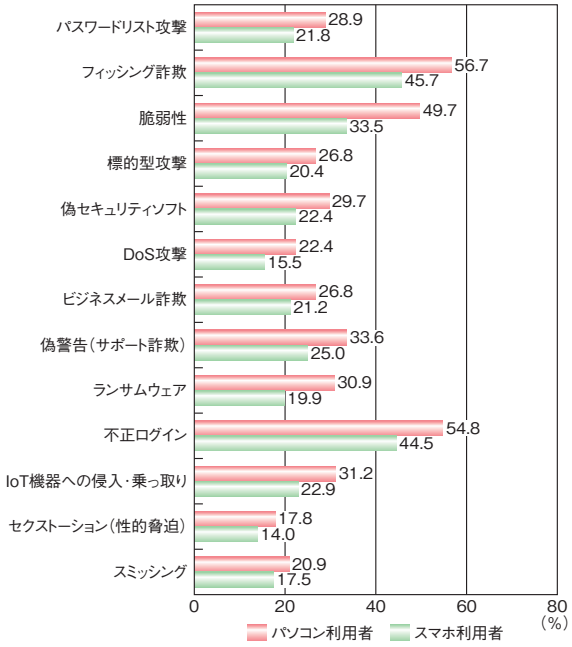
次に、受講経験の割合の低さと、回答者の属性との関係を確認するために「B 群」（1,749 人）のうち、受講経験のない 89.2%（1,560 人）の属性を調べた（表 2-4-10）。属性の分類においては職種によって回答が分かれることを想定し、会社員等職業従事者について、「情報システムや通信関係など IT 関連業務に従事、関与」している人とそうでない人とを分けて集計した。結果は、「パート、アルバイト」（20.8%）、「専業主婦・主夫」（20.0%）、「IT 業務に従事、関与※263していない会社員」（15.9%）、「無職」（14.4%）の順で割合が高かった。

この結果をまとめると B 群の職業に従事していない属性では「専業主婦・主夫」「無職」の割合が高かった。職業に従事する属性では「パート・アルバイト」「IT 業務に従事、関与していない会社員」の割合が高い一方で、「IT 業務に従事、関与している会社員」も一定程度の割合（7.1%）で存在した。こうした属性が混在する職場では、セキュリティ対策が十分にできていない可能性がある。

(3) 脅威名の認知度

各種セキュリティ脅威の認知度についてパソコン利用者とスマートフォン利用者の割合を比較した（図 2-4-20）。

総じて、パソコン利用者における認知度の方がスマートフォン利用者より高いが、認知度が過半数を超えるものは 2021 年度調査では「フィッシング詐欺」（56.7%）、「不正ログイン」（54.8%）の 2 点のみである。その他、社会人には比較的馴染みがあると思われる脅威名であっても、「ビジネスメール詐欺」（26.8%）、「標的型攻撃」（26.8%）、「DoS 攻撃」（22.4%）等の認知度は決して高くない。また、昨今国内でも深刻な被害が発生している「ランサムウェア」も 30.9% である。なお、各種脅威の認知度は過去の調査においても変動があまりなく、おおよそ上記と同様の割合、傾向である。



■図 2-4-20　パソコン及びスマートフォン利用者における各種脅威名の認知度比較

	属性	人数	受講経験割合		属性	人数	受講経験割合
IT 業務に従事・関与している	会社員	111	7.1%	IT 業務に従事・関与していない	会社員	248	15.9%
	公務員・団体職員	21	1.3%		公務員・団体職員	17	1.1%
	教職員	3	0.2%		教職員	2	0.1%
	契約・派遣社員	37	2.4%		契約・派遣社員	52	3.3%
	自営業・自由業・フリーランス	23	1.5%		自営業・自由業・フリーランス	37	2.4%
	経営者・役員	8	0.5%		専業主婦・主夫	312	20.0%
	医者	0	0.0%		無職（定年退職・家事手伝い含）	225	14.4%
	弁護士	0	0.0%		パート・アルバイト	325	20.8%
	医師・弁護士以外の専門職	26	1.7%		短大生・高専生	2	0.1%
	中学生	7	0.4%		大学生	7	0.4%
	高校生	50	3.2%		大学院生	2	0.1%
	専門学校生	4	0.3%		その他	41	2.6%

■表 2-4-10 「B 群：スマートフォンのみを利用」する人で受講経験のない人の属性別割合（n=1,560）

パソコン利用者とスマートフォン利用者とで認知度の差は、「脆弱性」が 16.2 ポイントと最も大きく、「フィッシング詐欺」「ランサムウェア」が 11.0 ポイント、「不正ログイン」が 10.3 ポイントと続いている。スマートフォン利用者がパソコン利用者と比べ、セキュリティ脅威の基本である「脆弱性」の認知度が低いのは、セキュリティ知識の不足の一端を表しているといえる。

(4) まとめ

これらの調査結果全体をとおし、セキュリティの対策実施率、教育の受講経験割合、脅威名の認知度、いずれにおいても、スマートフォン利用者がパソコン利用者に比べ低い傾向にあった。また属性でみると職業に従事していない「専業主婦・主夫」「無職」や、「パート・アルバイト」といった非正規雇用者において低い傾向にあった。こうした属性のスマートフォン利用者に対する教育機会の創出、提供が望まれる。

COLUMN

高齢者層の情報セキュリティ

2021 年 9 月 1 日に日本のデジタル社会実現の司令塔としてデジタル庁が発足しました。デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会を目指し、安全・安心を前提とした「誰一人取り残されない、人に優しいデジタル化」を進めることを目標としています[i]。そのようなデジタル社会において、行政手続きや暮らしに関わるオンラインサービス等の恩恵を社会全体で享受するためには、インターネットやスマートフォンの積極的な活用が広まっていない高齢者層にも、今後はその活用が求められます。

デジタル社会の利便性を向上させていく一方で、情報セキュリティの確保は両立しなくてはならない課題です。特にインターネットやデジタル機器の扱いに慣れていない高齢者層の情報セキュリティの現状には、様々な課題があると考えられます。

具体的には、フィッシングや、偽サイト等のネット詐欺の被害事例が高齢者層で多く確認されています。例えば、独立行政法人国民生活センターが 2022 年 2 月 24 日に発表[ii]した、いわゆる「サポート詐欺」に関する相談における契約当事者の年齢は 60 歳以上が 5 割を超えていて、特に 70 歳以上が被害に遭っているとされています。パソコンやスマートフォン等の端末操作に不慣れで、セキュリティの知識がないことにつけ込まれているとのことです。このような状況からも、高齢者層の情報セキュリティに課題があることが分かります。

IPA は地域での普及啓発活動の一環として、2021 年度は高齢者層向けを意識した「インターネット安全教室[iii]」の開催に力を入れました。この教室では、「パスワードの作り方が分からない」「フィッシングの見分け方を教えて欲しい」「SNS、SMS、二段階認証などの言葉の意味が分からない」といった不安に対して説明を行っています。また、「情報セキュリティ安心相談窓口[iv]」においても、高齢者の方々から数多くの様々なご相談をいただき、それに対してアドバイスを提供しています。

「誰一人取り残されない、人に優しいデジタル社会」を実現するために、社会全体の取り組みとして、高齢者層の情報セキュリティリテラシー向上を目指していく必要があります。

i　デジタル庁：デジタル社会の実現に向けた重点計画　https://www.digital.go.jp/policies/priority-policy-program〔2022/5/23 確認〕
ii　独立行政法人国民生活センター：そのセキュリティ警告画面・警告音は偽物です!「サポート詐欺」にご注意!!　https://www.kokusen.go.jp/pdf/n-20220224_2.pdf〔2022/5/23 確認〕
iii　https://www.ipa.go.jp/security/keihatsu/net-anzen.html〔2022/5/23 確認〕
iv　https://www.ipa.go.jp/security/anshin/〔2022/5/23 確認〕

2.5 情報セキュリティの普及啓発活動

新型コロナウイルスの感染が収まらず、新型コロナウイルスに常に注意を向ける「with コロナ」の生活が続いている。

2020 年から急速な移行を求められたテレワークや、リモート授業・会議は今や日常のものとなり、「オンライン状態」にいる人が多くなっている。

このようにオンライン化が急激に進む中で、必要とされるネットリテラシーと様々な組織による普及啓発活動について述べる。

2.5.1 ネットリテラシーの重要性

新型コロナウイルスの感染拡大に伴い、インターネットを介した非接触のコミュニケーションが推奨され、リモートツール・サービスが我々の生活に浸透してきている。

(1) オンライン取引／契約の注意点

コロナ禍以降は外出の自粛により「おうち時間」が増え、自宅にいながら買い物を楽しんだり、外食の代替として料理の宅配サービスを利用したりと、通信販売の利用が増加した※264。65 歳以上のシニア層世帯でも利用が進んでいる※265 が、通信販売に不慣れだったシニア層がトラブルに巻き込まれるケースも増加している。

独立行政法人国民生活センターは、60 歳代以上から受けた通信販売に関する相談件数が、2020 年度に初めて 10 万件を超え、過去最高となったと発表した※266。60 歳代から 80 歳代以上のいずれの年代も、相談件数の上位は通信販売に関するものとなり、特に 70 歳代及び 80 歳代以上では、過去 5 年間で最も多くなった。

中でも、定額を支払う音楽や動画等の配信サービス利用や、サプリメント等の購入ができる「サブスクリプション」についての相談が多く、そのほとんどがインターネットで契約したものであった※267。具体的には「動画配信サービスの解約を忘れ、利用していないにもかかわらず代金を請求された」等の事例が報告されている。

このサブスクリプション契約に関する対策として、消費者庁は特定商取引に関する法律の通達改正（2022 年 2 月 9 日）において、「通信販売の申込み段階における表示についてのガイドライン※268」を公表した。この中で、「サブスクリプションに見受けられる、無償または割引価格の対象期間後、自動的に価格が変わる契約内容に移行するような場合には、あらかじめ支払い金額を明示する必要がある」としており、表示方法の改善が期待される。

また、政府は消費者契約法改正案を提出するとしており、改正されれば、利用者にとって契約内容や解約方法が分かりやすくなり、トラブルの減少につながることが予想される。

通信販売トラブルはシニア層だけのものではない。若年層の定期購入に関する相談も増加している※269。

1 回だけの「お試し」のつもりで申し込んだが、2 回目の商品が届き定期購入になっていたことに気づいた、等のトラブルが発生しており 10 ～ 20 歳代の若者が巻き込まれるケースも少なくない。このため、独立行政法人国民生活センターは「通信販売にはクーリング・オフ制度がない」「注文する前に販売サイトを隅々まで確認する」等、トラブル防止のポイントをまとめ、公表している※270。また、政府広報オンライン※271 や京都府消費生活安全センター等の公的機関が、定期購入に関する注意喚起動画（図 2-5-1）を公開しており、手軽に学べる機会が提供されている。

■図 2-5-1　定期購入に関する注意喚起動画
（出典）京都府「あなたも気をつけよう!～身近な消費者トラブル～お試し購入編※272」

SNS を介した「個人間融資」にも注意が必要である。コロナ禍による失業や収入の低下によって金銭面で困難な状態にある人が巻き込まれやすいとされる「個人間融資」では、法外な利息を要求されるトラブルが発生している。また、保証金としてお金をとられたり、個人情報が悪用され、さらなる犯罪被害に巻き込まれたりする恐れもある※273。

金融庁は、SNS 等で勧誘し、お金の貸し借りを行う「個人間融資」は、貸金業法の規程に抵触する場合があるとして注意を呼びかけている※274。また、神奈川県もヤミ

金融情報のページを開設[※275]し、成年年齢の引き下げを受け、啓発キャラクタを使用したリーフレットを公開する等して「絶対に借りないこと!」等のアドバイスを行っている。

(2) GIGA スクール構想

文部科学省が推進する GIGA スクール構想は、児童生徒に 1 台ずつ端末を提供し、個別最適化された学びや創造性を育む学びの実現を目指している(「2.4.3(2) 文部科学省における対策」参照)。「端末利活用状況等の実態調査(令和 3 年 7 月末時点)(確定値)[※276]」は、公立の義務教育段階の学校を設置する 1,812 の自治体の 96.2% において、児童生徒がタブレットやノートパソコンを活用できる環境が整ったことを示した。残る自治体でも、その 7 割は 2021 年度内に整備が完了するという。

端末を利用したオンライン授業は、通学の必要がなく、自分のペースで学習できる等のメリットがあるが、教員がそばで操作等について指導ができないため、児童生徒個々のネットリテラシーがより重要になる。

小学 1 年生～中学 3 年生の子どもを持つ保護者と、教員を対象とした「GIGA スクールにおけるセキュリティ実態調査 2021[※277]」を実施したトレンドマイクロ株式会社は、端末を受け取った児童生徒のうち、約 2 割が何かしらのトラブルを経験していると発表した。トラブルのうちセキュリティに関する主な項目は「アカウント(IDとパスワード)情報を盗まれる・悪用される(アカウントのっとり、不正アクセスの被害者となる)」(9.2%)、「不正アプリ(ウイルス)への感染」(7.8%)、「アカウント(ID とパスワード)情報を盗む・悪用する(アカウントのっとり、不正アクセスの加害者となる)」(7.1%)だった。また、「ネットの長時間利用による依存や、学業、健康への悪影響」(9.2%)、「不適切な Web サイトの閲覧」(5.0%)、「ネット上での見知らぬ人との出会い」(5.0%)等、情報モラル・リテラシーに関連する回答も挙がった。

文部科学省は「GIGA スクール構想の下で整備された 1 人 1 台端末の積極的な利活用等について(通知)[※278]」の中で、「情報モラル教育の一層の充実を図ること」を通知しており、「1 人 1 台端末の利用に当たり、保護者等との間で事前に確認・共有しておくことが望ましい主なポイント」として、「端末・アカウント(ID)・パスワードを適切に取り扱う」「就寝 1 時間前からは ICT 機器の利用を控える」「他人を傷つけたり、嫌な思いをさせることをネット上に書き込まない」等の項目を紹介している。また、「はじめてのパスワード指導」や「他人の情報の取り扱い方を考えよう」等、全国の自治体や学校による先進的な実践事例を紹介する Web サイト「StuDX Style[※279]」(図 2-5-2)を公開し、子ども達への指導の際の参考となる情報をまとめている。

■図 2-5-2 「StuDX Style」のホームページ抜粋
(出典)文部科学省「StuDX Style」

心身ともに成長段階にある子ども達は、様々なことを柔軟に吸収する。そして、その柔軟さ故にトラブルの経験は深い傷を残すことがあり、周囲の大人はトラブル回避に奔走する。しかし、当の大人はネット上のトラブルを回避できているだろうか。

IPA が公表した「2020 年度情報セキュリティの倫理と脅威に対する意識調査 -【脅威編】報告書 -[※280]」では、パソコンを利用する回答者のうち「脅威との遭遇経験が過去 1 年間にはなかった」とした人は 28.5% に過ぎず、10 代が最も遭遇経験が少ないとの結果となった。多くのパソコン利用者が何らかのトラブルを経験しており、大人にとっても脅威は身近にあるといえる。

子ども達の端末利用が進む中、大人もネット上の社会倫理や情報セキュリティについてともに学びながら被害を食い止めていかなければならない。

(3) ネット上の誹謗中傷への対策

SNS 等を介したコロナ感染者に対する差別的な発言は後を絶たない。感染者のみならず、医療従事者やその家族までがターゲットとなり、心ない書き込みによって苦しめられている。

法務省人権擁護局は TikTok と連携し、インターネット上の人権侵害防止のキャンペーンを展開した(次ページ図 2-5-3)。TikTok アプリ内に特設ページを開設し、「誹謗中傷」「SNS いじめ」及び「個人情報の取扱い」に関する啓発動画を計 7 本公開している。動画は、人気のクリエイターの協力により制作され、TikTok を利用する若者に向けて人権尊重を訴えた。また、中傷被害を受けている人が相談する窓口の情報も掲載された。

■図 2-5-3 「#誰かのことじゃない～ネットの誹謗中傷・SNS いじめ・個人情報の取扱い～」キャンペーン
（出典）法務省人権擁護局の Tweet※281

コロナ差別への取り組みは、地方自治体でも独自に展開されている。

例えば石川県は「Stop! コロナ差別！」と題した啓発活動を行うとともに、AI を活用して SNS や掲示板を始めとする閲覧可能な Web サービス全般をチェックし、差別的な書き込みを収集している※282。収集した情報は、被害者が訴訟を起こす際の証拠資料として活用できるよう県が保管している。同様の取り組みは、福井県、愛知県、和歌山県、岡山県等でも実施されており、このうち、和歌山県※283 では、条例でプロバイダの責務を規定し、誹謗中傷等の削除や、投稿の抑止のための広報活動等を依頼している。

(4) 新型コロナウイルスに関するフィッシング

2021 年 6 月、「自衛隊大規模接種センター」をかたる新型コロナワクチン接種の予約サイトの案内メールを送信し、フィッシングサイトに誘導する手口が発覚した※284。メールに記載されている URL をクリックするとワクチン接種に関するポータルサイトのようなページに辿りつき、氏名や住所、更にはクレジットカードの情報を入力する画面が表示される。独立行政法人国民生活センターは送信元やメールのタイトルに心当たりがない場合は、クリックやタップをせず、「新型コロナ関連詐欺 消費者ホットライン※285」に相談してほしいと呼びかけている。

また、「新型コロナウイルス特別定額支援金」という偽サイトに誘導する手口も報告されており、厚生労働省は注意を呼びかけている※286。

コロナ禍の不安につけ込んだ同様の手口は、今後も発生する危険がある。受信したメールを鵜呑みにしてメール内のリンクをクリック／タップすることのないよう注意したい（「1.2.7 (3) 世の中の関心に乗じる手口」参照）。

2.5.2 恒常的な啓発活動

ここでは、コロナ禍以前から継続的に実施されている情報セキュリティ・情報リテラシーに関する啓発活動について述べる。

(1) SNS 事業者等による対策

2022 年 1 月、他人の SNS のアカウントに無断でログインした等により不正アクセス禁止法違反容疑で男が逮捕された※287。容疑者は、アカウント名から氏名や生年月日等を割り出し、パスワードを推測していたとされ、ID やパスワードの管理の重要性を改めて知らしめた。

SNS のセキュリティ強化として、Twitter Japan 株式会社は Twitter を安心して使うための「プレイブック日本語版」を 2021 年 12 月に公開した（図 2-5-4）。プレイブックは「安心して使う」「安全を確保する」及び「自分のデジタルフットプリントを管理する」という目的で、該当する機能の紹介を行うものである。シチュエーションごとに有効な機能をフローチャートで紹介し、アカウントの安全を確保するための設定方法等について記載しており、活用が望まれる。

■図 2-5-4 Twitter プレイブック日本語版
（出典）Twitter Japan 株式会社「Twitter の安全機能をまとめた「プレイブック」日本語版を発行※288」

Instagram も、「プロフィール情報の確認」や「ログイン情報を共有しているアカウントの特定」等の「セキュリティに関する確認」4 項目を通知して、アカウントを安全に管理するための設定を促す取り組みを開始している※289。

また、ネット上のハラスメントや権利侵害、若年層保護に対する対策も進んでいる。

Instagram は、急激に注目を集めた利用者を誹謗中傷等から守る機能として「抑制」機能を発表した※290。これは、自身をフォローしていないアカウントや、最近フォローしたばかりのアカウントから届くコメントや DM リクエストを自動的に非表示にするものである。また、若年層保護を

目的として、16 歳未満の全アカウントについて初期設定を「非公開」にすること、若年層のアカウントにブロックされた成人のアカウントは、若年層とやり取りすること等ができなくなる機能を加え、対策を強化した※291。

YouTube は、低評価の数を非表示にすると発表した※292。本来は、動画の内容の良し悪しを判断できるよう設けられた機能だが、動画の内容ではなく動画のクリエイターに対する悪意ある低評価や嫌がらせに使用されるケースが発生しており、このようなハラスメントからクリエイターを守るためとして、2021 年 11 月 10 日から順次展開している。

ヤフー株式会社は、「Yahoo! ニュース」の記事に対し、利用規約等に違反する投稿を繰り返す利用者への対策を始めたと発表した※293。不適切投稿の抑止を目的としたもので、「発信者情報開示請求等を受けた場合、法令上の手続きにのっとり開示を行う場合がある」といった違反投稿を続けた場合に起こり得る法的なリスクを画面に表示する。

このようにサービス事業者の取り組みが進んでおり、利用者側の意識の成熟も望まれる。

(2) 成年年齢引き下げに伴う啓発

2022 年 4 月より成年年齢が 18 歳に引き下げられた。これまで若者は、未成年者取消権によって守られ、親権者の同意を得ずに締結した契約は後から取り消しができた。しかし、成年年齢の引き下げにより、18 歳、19 歳の人はこの保護の対象外となる。

18 ～ 19 歳の新成人となる層から消費者庁、自治体等の消費生活相談に寄せられたトラブルでは、健康食品や化粧品に関するもののほか、デジタルコンテンツや出会い系サイトに関するものが多くみられた※294。これらのトラブルに巻き込まれるきっかけは SNS の広告や書き込み等に誘導されるケースや SNS 上の知り合いから誘われるケース等が挙げられている。

成人と言っても、経験したことのない事柄について判断するのは容易ではない。また、ネット上では、相手の顔が見えない状態で言葉巧みに言いくるめられ騙されることも考えられる。

消費者庁では、「『18 歳から大人』特設ページ※295」を開設して啓発動画を公開したり、Twitter による情報発信を行ったりしている。また、総務省も「インターネットトラブル事例集」の中で「成人年齢の引き下げにあたって学んでおきたいこと※296」をまとめた Web ページを公開している。

法務省も「大人への道しるべ※297」という漫画とクイズで学べるホームページを開設した（図 2-5-5）。「大人って何?」や「契約は人と人との約束」等の項目のほか、「SNS は便利で怖い」や「その動画、アップして大丈夫?」等、ネットにまつわるテーマの漫画とクイズが公開され、ネット上での振る舞いや責任について改めて考えることができる。

■図 2-5-5 「大人への道しるべ」のホームページ抜粋
（出典）法務省「大人への道しるべ」

また、公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会も「18 歳からのスマート通販学※298」という電子書籍を公開した。「インターネット通販のメリット / デメリット」や「投げ銭型ライブ配信サービス」の注意点等の事例と、トラブルに巻き込まれた際の相談窓口が分かりやすく紹介されている。新たに成人になる 18 ～ 19 歳のみならず、インターネット通販を利用するすべての人に有効な情報であり、活用が推奨される。

(3) オンラインゲームにおけるチート行為対策

2021 年 6 月、日本初のシニアによる e スポーツプロチームが発足した※299。高齢者の健康増進・維持としての活用だけでなく、世代や地域を超えるコミュニケーションを可能にする点でも e スポーツは注目されている。

2021 年 10 月には経済産業省が、社会人 e スポーツリーグ「AFTER 6 LEAGUE」を国の機関としては初めて後援する※300 等、国を挙げた盛り上がりを見せ始めている。

オンラインゲームを活用した e スポーツが競技として楽しまれている一方で、オンラインゲームを悪用した手口による事件も発生している。

京都府警察本部サイバー犯罪対策課はゲームを有利に進めるための「チート行為」を行ったとして 5 人を書類送検した※301。容疑は、ゲーム会社のサーバに不正なデータを送信し、ゲーム内のアイテムを不正に入手する

等した私電磁的記録不正作出・同供用にあたるとしている。過去には、チート行為が「著作者人格権侵害」や「電子計算機損壊等業務妨害罪」となった事例※302もあり、安易にチート行為を行わないよう啓発が必要である。

また、オンラインゲームの開発者にも不正防止の対策が必要である。株式会社ラックは、オンラインゲームのチート対策の知見を集めたホワイトペーパー「オンラインゲーム、スマートフォンゲームのセキュリティ～チートの脅威と対策について～」を開発者向けに公表した※303。

作り手側と使用者側双方の意識向上が望まれる。

(4) 誰も取り残さないセキュリティ・リテラシー

NISCは、セキュリティには「全員参加による共同、普及啓発」が重要だとしており、2022年サイバーセキュリティ月間（2月1日～3月18日）のキャッチフレーズを「#サイバーセキュリティは全員参加」として、国民全体の意識向上を目指す普及啓発活動を行っている。2022年の主なイベントとして「ランサムウェア攻撃対応・東京2020大会の対策から学ぶ※304」と題したセミナーがオンライン配信されたほか、チェコ、フランス、ドイツを始めとする海外のサイバーセキュリティ関係当局及び、日本のサイバーセキュリティ関係省庁が参加した国際サイバーセキュリティワークショップ・演習が開催され※305、インシデント発生時の対処能力の向上、知見の共有が行われた。

また、政府広報オンラインでも、サイバーセキュリティ月間の期間中「家族みんなで考えよう！安全・安心なインターネットの利用※306」という動画を公開し、進級・進学を機にスマートフォンを利用する子どもとその保護者に向けた啓発を行った。

2.5.3 インターネットがもたらす未来

株式会社オリィ研究所が2021年6月に開店した「分身ロボットカフェDAWN ver. β※307」では、筋萎縮性側索硬化症（ALS）等の重度の障害により外出が困難な人が、全国各地から分身ロボットを遠隔操作し接客を行っている（図2-5-6）。これは、健常者が行っているリモートワークの発展形という見方もあり、障害を持つ人の社会参加の場のみならず、コロナ禍において人と人との接触を減らす役割を果たすことも期待できる。

■図2-5-6　分身ロボットカフェ DAWN ver. β
（出典）株式会社オリィ研究所「分身ロボットカフェ DAWN ver. β」

このように、インターネットの技術及び関連するツールは、生活インフラであるという点での重要性のみならず、未来の生活に恩恵をもたらすものである。ただし、インターネットの利用場面が増えると、情報セキュリティ対策が必要な場面も増えていく。また、いかに有用であっても、それを使いこなす側に悪意があれば、一転して我々を脅かす武器になってしまう。悪意がなくても、無知や配慮の欠如によって他者への攻撃になってしまうこともあり得る。

一人ひとりが「有用なツールを正しく使いこなすことができているのか」と自らに問い続け、被害者にも加害者にもならないという意識と行動が一層必要とされている。

COLUMN

インターネット上の戦い

こんにちは！　ぼくは、IPA「ひろげよう情報モラル・セキュリティコンクール」応援隊長のまもるです。ぼくたちは今、新型コロナウイルスに負けないように、マスクを着け、手洗いと換気をして戦っているよ。

そして、地球上ではコロナとは別の戦いが二つ起きています。戦車や爆撃などによる「地上戦」、もうひとつは「サイバー戦争」。ぼくたちが住んでいるところからは遠い国同士の戦いだと思っていたのだけれど、インターネットには国境がないから、「よその国のお話」では済まされないんだと、お父さんが話してくれました。

サイバー戦争で何が起きるのかを調べてみたら、ぼくたちの生活に大きく影響することがわかりました。鉄道や電気、ガス、水道を管理するシステムが攻撃されると、生きるために必要なものを手に入れられなくなるよね。それに、原子力発電所が攻撃されて、制御ができなくなったとしたら……。

ほかにも、もし国に関係するWebサイトが改ざんされてしまうと、自分たちの国がどんな情報を発信しているのか、わからなくなってしまうね。何か嘘の情報を書かれていたとしても、改ざんされていることを知らなかったら、ぼくたちはその情報を信じて間違った行動を起こしてしまうかもしれない。

実際に、ある国の大統領の偽の動画がネットに公開されたことがあったよ。武器を捨てて降伏するよう市民に訴えるディープフェイクだったんだけど、大統領のお話なら信じてしまいそうだよね。

それから、サイバー戦争は、二つの国の間だけで起きているわけではなくて、「攻撃されている国」を助けるという目的で、「攻撃している国」にハッカー集団がサイバー攻撃をしかけているんだって。「攻撃している国」の国営テレビなどをハッキングして戦地の映像を放送した、とSNSに投稿したっていうよ。でも、本当に映像が流れたのかな?

そのハッカー集団はもともといろんな国の政府や企業にサイバー攻撃を繰り返している人たちで、いつもはみんなが怖がったり非難したりしている存在だから、信じて良いかどうかぼくには判断ができなかったよ。それなのに、世界中の多くの人が「良くやった!」とか「かっこいい!」と称賛する書き込みをしたりして、頭のなかがこんがらがってしまいました。こんなふうに、情報はぼくたちを混乱させ、時には間違った方向に導くこともあるんだね。だから、発信する内容も閲覧する内容もよく確認しなくてはいけないんだ。

それと、ショッキングな情報ほど目について誰かと共有したくなっちゃうんだけど、不確かな情報をむやみに拡散することを止めなくちゃね。安易な拡散によって、いつのまにか自分が誰かを「攻撃する側」に立っていた、なんてことにならないように。

2.6 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。本節では、日本の国際標準化活動への取り組み、及び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。

2.6.1 様々な標準化団体の活動

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

(1) 日本の国際標準化活動への取り組み

企業が培ってきた技術や知的財産の秘匿化や、それらを知財として権利化する「クローズ戦略」に対して、標準化は「オープン戦略」に位置付けられている。クローズ戦略により企業のコア領域を守り、他社との差別化を図ることは重要であるが、その技術を利用する市場が広がらなければ、企業としては事業を拡大することが困難である。コア領域を守りつつ、市場を拡大する「オープン&クローズ戦略」が必要である。技術の発展、市場のグローバル化が進み、このオープン&クローズ戦略の考え方は企業にとどまらず、国の政策として位置付けられるようになった。

既に、主要国では、自国に有利な標準化を目指し、官民を挙げて標準化活動に取り組んでおり、例えば、米国の国立標準技術研究所（NIST：National Institute of Standards and Technology）では、政府・国内企業向けの標準策定に関与し、技術的知見や評価結果の提供、民間利害関係者間の調整、政府からの指示を受けた標準化案の検討等を行っている。中国の中国標準化研究院や中国工程院、ドイツのフラウンフォーファー研究機構といった組織でも標準化の取り組みが行われている。日本でも公的機関が民間の標準活用戦略活動を支援することが望ましいとして、国立研究開発法人産業技術総合研究所、IPA、NICT、国立研究開発法人農業・食品産業技術総合研究機構、一般財団法人日本規格協会（JSA：Japanese Standards Association）等の関係機関をネットワーク化し、ワンストップで支援する協働体制「標準活用支援サービスプラットフォーム」を整備した※308。

(2) 標準の分類

国際標準には、公的な標準化団体により所定の手続きを経て行われる「デジュール標準（de jure standard）」、いくつかの団体（企業等）が協力して自主的に作成する「フォーラム標準（forum standard）」、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。フォーラム標準は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）※309：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（JISC：Japanese Industrial Standards Committee）がISO、IEC双方のメンバーであり、JTC 1でも活動している※310。

- 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※311、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。

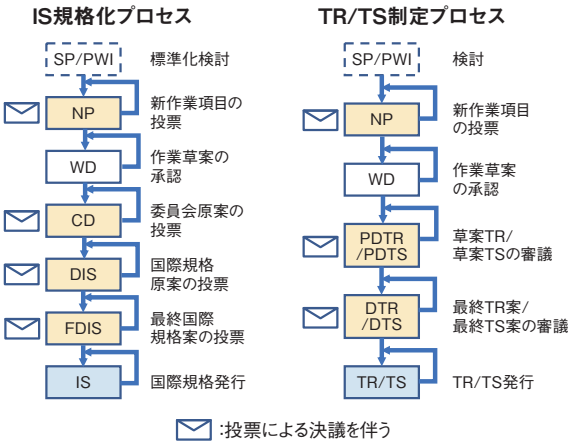
- IEEE（The Institute of Electrical and Electronics Engineers, Inc.）：
  電気工学・電子工学技術に関する国際学会である。標準化活動は内部組織であるIEEE-SA（Standards Association）が行っている。情報セキュリティについては、サイバーセキュリティ、ネットワークセキュリティ、IoTセキュリティ等の広範な領域で標準化を行っている。
- IETF（Internet Engineering Task Force）：
  インターネット技術の国際標準化を行う任意団体である。非常にオープンな組織であり、作業部会のメー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、デジタル署名、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※312。標準化した技術文書はRFC（Request For Comments）として参照できる。
- TCG（Trusted Computing Group）：
  信頼できるコンピューティング環境（組み込み機器、パソコン／サーバ、ネットワーク等）に関するセキュリティ技術の標準化を行う業界団体である。ハードウェア、ソフトウェア等のベンダやシステムインテグレータがメンバーとなり、中国、日本にregional forumがある※313。

2.6.2 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作業グループ（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2-6-1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2-6-1　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※314」を基にIPAが作成

図2-6-1の各文書のステータスと略号は以下のとおりである。

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

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

以下に、各 WG の活動概要を述べる。なお本文中では略号を使用する。

（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

ISO/IEC 27002:2013 は、1 年間の SP において、次期改訂の設計仕様（Design Specification）を決定後、2018 年 3 月より改訂作業が開始されていたが、2022 年 2 月に改訂版が発行となった。

本改訂では、管理策群の内容としては、基本的に 2013 年版を踏襲しており、それに新しい脅威や技術に合わせて、新規管理策が追加されている。一方で、管理策の構成については、2013 年版から大きく変更されている。ISO/IEC 27002:2022 には、2013 年版管理策との対応表も Annex として掲載されているので、旧管理策との対応や新規管理策を確認することができる。

ISO/IEC 27002:2022 の管理策の構成等が 2013 年版から大きく変わることを受け、ISO/IEC 27001：2013 Annex A との不整合が発生する状況が望ましくないことから、ISO/IEC 27001 を限定的に改訂することが合意された。具体的には、ISO/IEC 27001:2013 Annex A を ISO/IEC 27002:2022 と整合するように変更することに伴う改訂のみを実施する。手続きとしては、まず、Annex A の入れ替えに関連する内容を Amendment（追補）として発行し、先に発行済みの 2 件の Corrigendum（正誤表）の内容も含め、ISO/IEC 27001 の新たな版として 2022 年に発行予定である。

一方、ISO/IEC 27001:2013 の内容を見直す改訂の必要性も認識されており、上記の限定的な改訂を終えた後の次期改訂に向け PWI を設置、検討を開始している。

(b) ISO/IEC 27002:2022 発行の他規格への影響

ISO/IEC 27002:2022 発行に伴い、ISO/IEC 27002:2013 を年号付きで引用、参照している規格は参照元を失ったことになる。また、仮に年号付きで引用、参照していなくとも、今回の改訂で構成が大きく変わったこと等を考慮すると、ISO/IEC 27002 を引用、参照する規格はいずれも何らかの見直しが発生すると想定できる。

最も影響が大きいのは ISO/IEC 27001 であるが、これについては、前述のとおり Annex A を整合するための限定的改訂を現在実施中である。

次に影響が高いものとして、セクター規格がある。ISO/IEC 27011:2016 は、電気通信業界内の組織における、ISO/IEC 27002 に基づいた情報セキュリティマネジメント導入を支援するガイドライン規格であり、ISO/IEC 27002:2013 をベースに追加の管理策やガイダンスが記されている。SC 27 と ITU の共同文書でもある。本規格は、ISO/IEC 27002 改訂版発行を待たずに改訂作業を開始しており、現在 CD ステージである。ISO/IEC 27017:2015 は、クラウドサービスのための情報セキュリティ管理策実践の規範を提供する規格であり、同様に、ISO/IEC 27002:2013 をベースに追加の管理策やガイダンスを提供する。規格の普及状況等を考慮しても、ISO/IEC 27002:2022 発行の影響は大きいため、本規格についても改訂に向けた作業を開始、PWI を設置した。一方、ISO/IEC 27010:2015 は、ISO/IEC 27002 をベースにしたセクター規格でありながらも、改訂による影響は大きくないと判断され、改訂は見送られた。また、エネルギー業界向けセクター規格である ISO/IEC 27019:2017 については、改訂は今後の検討課題となっており、まだ決定していない。

また、ISO/IEC 27001 や ISMS についてのガイダンスを提供する他のガイドライン規格（ISO/IEC 27003:2017、ISO/IEC 27004:2016、ISO/IEC TS 27008:2019 等）についても、ISO/IEC 27002 による影響は想定されるが、セクター規格への対応が優先され、セクター規格に次いだ検討項目となっている。

(c) その他の ISO/IEC 27000 ファミリー規格の国際標準化活動

ISO/IEC 27002:2022 の改訂とは直接関係のない、その他の規格の動向として次がある。

情報セキュリティリスクマネジメントに関するガイドライン規格 ISO/IEC 27005:2018 は、ISO/IEC 27001:2013 への本格的対応を積み残していることから改訂作業中であるが、2022 年 4 月時点で DIS を審議中である。ISO/IEC 20000-1 及び ISO/IEC 27001 の統合実践に関するガイドライン規格である ISO/IEC 27013:2015 は、ISO/IEC 20000-1:2018 の発行を受けて、2021 年 11 月改訂版が発行された。ISMS 専門家の力量に関する要求事項を提供する ISO/IEC 27021:2017 は、2021 年に追補を発行した。

(2) WG 2 (暗号とセキュリティメカニズム)

WG 2 では、暗号プリミティブ (暗号アルゴリズム) や、デジタル署名技術、鍵共有のような汎用的かつ基本的な暗号プロトコル等の標準化を行っている。WG 2 の国際主査、副主査ともに日本人が選出され、WG 2 での活動をリードしている。2021 年度は、新しい規格である「鍵管理　第 7 部 : クロスドメイン・パスワードに基づく認証鍵交換 (ISO/IEC 11770-7)」と「暗号アルゴリズム　第 3 部 : ブロック暗号　追補 1 (ISO/IEC 18033-3/AMD1)」の 2 件、及び既存規格 6 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) PWI

2022 年 5 月時点の主な PWI は、以下のとおりである。個別に議論され、標準化すべきとの判断となった場合、標準化に着手する。なお、最後の項目については、日本から提案された。

- 調整値付き (tweakable) ブロック暗号の利用モード
- 算術演算暗号アルゴリズム (ハッシュ関数を含む)
- 安全なマルチパーティ計算 – 第 3 部 : ガーブル回路※315 を用いたメカニズム
- ID 情報に基づく認証鍵交換の追加メカニズム

(b) 新型コロナウイルス感染拡大の影響によるプロジェクト進捗遅延

WG 2 では、「匿名デジタル署名　第 3 部 : 複数の公開鍵を用いたメカニズム (ISO/IEC 20008-3)」のような、大学関係者がエディタをしているプロジェクトが多くあり、オンライン授業等の対応を優先しなければならなかったため、いくつかの規格作成のスケジュール遅延が目に付くようになっていた。2022 年度に入り、当該大学関係者も標準化作業に時間を割くことができるようになり、これから標準化作業の加速が期待される。

(3) WG 3 (セキュリティの評価・試験・仕様)

WG 3 は 2021 年 10 月、2022 年 4 月にオンライン会議にて定期会合を開催した。それらの会合の議論内容、特に 2021 年度に標準化が承認されたプロジェクトに焦点を当て以下に概説する。

(a) ISO/IEC 5888 "Information security, cybersecurity and privacy protection — Security requirements and evaluation activities for connected vehicle devices"

UNECE (United Nations Economic Commission for Europe : 国際連合欧州経済委員会) の自動車基準調和世界フォーラム WP.29 にて自動車のサイバーセキュリティ基準が採択されたことを受け、自動車業界はその基準への対応を迫られている。自動車の主要なコンポーネントである車載 Engine Control Unit (ECU) に関する技術的詳細を記したサイバーセキュリティ基準は存在していない一方で、多くの脆弱性が検出されている。そのため、WG 3 では 2019 年 4 月テルアビブ会合から車載 ECU のセキュリティ評価基準に関する議論を開始し、2022 年 3 月に ISO/IEC 5888 の開発が承認された。

ISO/IEC 5888 は、車載 ECU に対し具体的にどのようなセキュリティ要件 (例えば、暗号に対する要件や、データ保護に関する要件等) を課すべきか、そのセキュリティ要件を満たしていることを確認するため、どのような脆弱性分析やテストを実施すべきかを定める国際標準である。自動車業界が ISO/IEC 5888 に定義されたテスト等を実施することにより、WP.29 自動車サイバーセキュリティ基準や、その基準において参照されている、自動車のライフサイクル全般にわたるサイバーセキュリティ対策を定めた ISO/SAE 21434 "Road vehicles — Cybersecurity engineering" への適合を主張できることを念頭に置いている。

本国際標準は、情報セキュリティやサイバーセキュリティに関わる国際標準を開発する ISO/IEC JTC 1/SC 27 (Information security, cybersecurity and privacy protection)、及び車載の電気・電子コンポーネントに関わる国際標準を開発する ISO/TC 22/SC 32 (Electrical and electronic components and general

system aspects）の両方に関係するため、双方のSCのJWG（Joint Working Group）6をISO/IEC JTC 1/SC 27配下に設立し、そのJWG 6にて標準開発することで合意されている。共同議長や共同プロジェクトリーダーは双方のSCから既に選出されており、今後メンバー募集終了後、本JWG 6における国際標準活動が開始される予定である。なお、SC 27側の共同プロジェクトリーダーとして日本のエキスパートが指名され、今後ISO/IEC 5888の開発に深く関わることとなる。

(b) ISO/IEC TS※316 9569 “Information security, cybersecurity and privacy protection — Towards Creating an Extension for Patch Management for ISO/IEC 15408 and ISO/IEC 18045”

ISO/IEC 15408に基づくIT製品のセキュリティ評価・認証制度では、IT製品の特定のバージョン・リビジョンに対し評価・認証を実施し、合格したIT製品に認証書が付与される。しかしながら評価・認証が完了したバージョン・リビジョン（例えばIT製品V1R1）に更新プログラムが適用されると、その認証書は更新されたバージョン・リビジョンの製品（IT製品V1R2）に対しては有効ではない。それは、評価・認証を経ていない更新プログラムを適用することにより、新たな脆弱性が混入される可能性があるからである。IT製品に対する軽微な更新の場合は、保証継続と呼ばれる、評価・認証より簡易な仕組みによって、更新されたバージョン・リビジョンの製品に対し認証書を再発行することもできるが、修正量が多い場合は、再度評価・認証を実施し新規の認証書を更新製品に対し発行する必要がある。しかしながら更新が頻繁に発生するIT製品においては、その都度保証継続、あるいは再評価を実施するのは現実的ではない。

本ISO/IEC TS 9569は、上記の問題を解決するため、開発者がセキュアな更新プログラムを開発する際に順守すべき更新プログラムの管理要件や、攻撃者により改変された更新プログラムが適用されることを防ぐためにIT製品が満たすべきセキュリティ機能要件等を定める。現在EUで創設が進められているサイバーセキュリティ認証スキームEUCC※317においては、更新プログラムを適用した際に認証書を更新する仕組みを導入する予定である。EUCCの評価・認証フレームを記した規定文書※318が公開されているが、その認証書更新の際の参照文書としてISO/IEC TS 9569を指定しており、ISO/IEC TS 9569は将来的に欧州における認証書更新の指針となる可能性もある（EUのセキュリティ認証制度については「3.4.2 (3) (b) セキュリティ認証スキームとセキュリティ市場分析」参照）。

(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2021年度の主な成果、活動を紹介する。

(a) IoTのセキュリティとプライバシーのための標準化活動

WG 4では、IoTのセキュリティとプライバシーに関わる標準化として、以下の三つの活動を継続的に進めており、加えて今期は新しい課題の検討がPWI 27404: Cybersecurity Labelling for Consumer IoTとして始まった。これらの規格は、Cybersecurity – IoT security and privacyと名付けられたプロジェクト群（ISO/IEC 27400シリーズ）として規格番号が振られ、規格間でも適切な参照を行うような形で検討が進められている。

- ISO/IEC 27400: Cybersecurity – IoT security and privacy – Guideline
- ISO/IEC 27402: Cybersecurity – IoT security and privacy – Device baseline requirements
- ISO/IEC 27403: Cybersecurity – IoT security and privacy –Guidelines for IoT domotics
- PWI 27404: Cybersecurity Labelling for Consumer IoT

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

日本は、IoT関連の製品・システム開発の競争力を強化し、またIoTの国際的なセキュリティレベル向上に寄与するために、IoT推進コンソーシアムが策定した「IoTセキュリティガイドライン※319」の国際標準化を提案した。本ガイドラインに基づき、プライバシー関連の対策を含む形でISO/IEC 27400（IoTのセキュリティとプライバシー）の規格案がSC 27/WG 4で審議されている。以下にISO/IEC 27400の規格について概説する。

ISO/IEC 27400の具体的内容にあたる第5章以降では、第5章で参照モデル、各利害関係者の役割、IoTライフサイクルに言及し、第6章でIoTシステムにおけるリスク源（リスクソース）について言及している。第7章では、セキュリティ対策、及びプライバシー対策が、IoTサービス開発者及び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

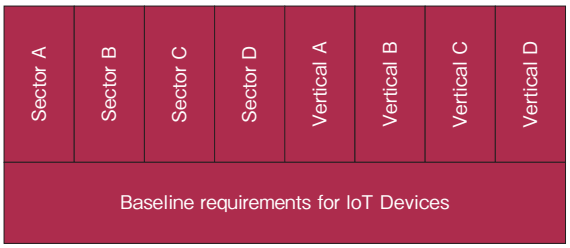
たガイドライン的表現で記載されている。ここで、IoT 機器製造業者は IoT サービス開発者の中に含まれる。現在策定されているドキュメントの枠組みは以下のとおりである。

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

2021 年 10 月にオンラインで開催された SC 27/WG 4 会議において、ISO/IEC 27400 は DIS となっていたが、DIS の投票を通過し、2021 年度末の段階では FDIS となっており、最終発行に近づいている。これまで、本規格に対するコメントは、日本、スイス、フランス、カナダ、ドイツ、インド、中国等の多くの機関から大量に提出されており、審議は極めて活発に行われた。本規格は IoT セキュリティ及びプライバシーの規範となるガイドラインであるため、IoT 利害関係者における認証等への活用が期待されている。

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

本規格は、米国が主導して進めており、IoT 機器が備えるべきセキュリティメカニズムのベースラインとなる要求条件の規定を目指している。ISO/IEC 27400 とは異なるスコープを掲げ、IoT 機器に特化した要件化を視野に入れ、NIST 及び ETSI（European Telecommunications Standards Institute：欧州電気通信標準化機構）の既存のガイドラインを下敷きに標準化を進めている。2020 年 4 月に WD 1 として審議が開始され、一定の完成度と判断され、2020 年 9 月会議では、CD1 に進むことが決定したが、内容の重要性や ISO/IEC 27400 との整合性等が議論され、2021 年 10 月会議で CD2 の状態となっている。本規格の位置付けは、図 2-6-2 にあるように、本規格の基本要求事項が水平方向の基本ベースラインとなり、その上に垂直市場（健康、金融サービス、産業、家電、輸送等）や様々なセクター（民間／工業、公共、防衛、国家安全保障等）のアプリケーションで想定される IoT デバイスの使用とリスクに対する追加要件を構築できるというものになっている。



■図 2-6-2　特定セクターや垂直市場による潜在的な追加要件との関係
（出典）ISO・IEC「ISO/IEC CD 27402.2 - Cybersecurity — IoT security and privacy — Device baseline requirements※320」

また、本規格は IoT 機器の適合性評価スキームの要件を提供することができる。具体的には、まず特定のセクター及び垂直市場の利害関係者が、この水平規格の「上」に構築される、それぞれのコンテキスト固有の要件に関する合意を形成することが期待され、その後、それらの特定のセクター及び垂直市場に関する適合性評価プログラムが開発され、本規格は、共通の基本要件セットを提供しながら、そのようなプログラムに効果的に統合されるといったイメージとなる。

現在策定されているドキュメント（CD2）の枠組みを以下に示す。

第 1 章～ 4 章：スコープ、文献、用語定義、概要
第 5 章 要求事項
　5.1 IoT 機器製造者のための要求事項
　5.1.1 リスクアセスメント
　5.1.2 ユーザへのコミュニケーション
　5.1.3 脆弱性の開示と処理プロセス
　5.2 IoT 機器のための要求事項
　5.2.1 一般事項
　5.2.2 IoT 機器の識別
　5.2.3 構成
　5.2.4 リセット
　5.2.5 ユーザデータの削除
　5.2.6 データの保護
　5.2.7 インタフェースアクセス（Interface access）

5.2.8 ソフトウェアとファームウェアのアップデート

なお、インタフェースアクセスは、IoT デバイスにおいて、秘密鍵やパスワード等の重要なセキュリティパラメータを共有または再利用するためのインタフェースへのアクセスを許可された権限者に限定することに言及している。

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

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

本規格は、2019 年 4 月テルアビブ会議において、中国から NP として提案され、同年 10 月のパリ会議では、NP の承認がなされ、2021 年 10 月に CD1 に進んでいる状況にある。「IoT-domotics」とは、娯楽、機器制御、監視等の用途として、居住環境で利用する IoT サービスをいう。本規格は、ISO/IEC 27400 との棲み分けが難しい部分が多いものの、IoT-domotics の特性を抽出し、ISO/IEC 27400 とは異なる視点でセキュリティとプライバシーに関するガイドラインとして整理している。具体的には、IoT-domotics のためのリスクアセスメントの実施を、アプリケーション、ネットワーク、ハードウェアの三点から評価しており、それらの結果を受ける形で、IoT-domotics を構成するサブシステムや IoT ゲートウェイのためのセキュリティ、及びプライバシーのガイドラインを整理する方向としている。

(エ) PWI 27404: Cybersecurity Labelling for Consumer IoT

本 PWI は、2021 年 10 月にシンガポールから提案されたもので、利用者が活用する IoT 機器にセキュリティラベルを付与し、機器にどの程度セキュリティ機能が装備されているかを、IoT 機器の利用者が把握できるようにする目的で検討が開始された。

現在、PWI として審議を継続しているが、ISO/IEC 27402 も IoT 機器に関する基本的な要求事項を規格化しようとしており、そこでも機器認証に関連した議論を行っていることから、簡単に本 PWI は NP とならない可能性が高いと考えられている。

(b) ビッグデータのセキュリティと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と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
- PWI 27045: Big data security and privacy — Guidelines for data security management framework
- 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、2019 年パリ会議において DIS に進み、2021 年に発行されている。

(イ) PWI 27045: Big data security and privacy — Guidelines for data security management framework

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プロセスの参照モデル、評価・成熟度モデルを規定するものであったが、内容的に規格化の方法が難しいことから、いったん規格化を断念し、PWI のステージに戻った形で議論が再開されている。

タイトルをビッグデータのセキュリティマネジメントのための枠組みを示すガイドラインとしており、多少これまでの検討を修正し、規格として成立しやすい形で審議を開始している。中国が主要なエディタとなり、オランダ、カナダが支援している。

(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。2021 年 9 月会議（リモート）においては、WD 5 への移行が決議され、本規格におけるビッグデータのソリューションのためのセキュリティとプライバシーのスコープを図 2-6-3 のように整理している。

(c) サイバーフィジカルシステムのためのセキュリティの枠組み

サプライチェーンに代表される多様な組織が連携するビジネススタイルの急速な進展、サイバー攻撃の出現と巧妙化、更に近年の IoT の利用拡大、IoT システムで収集されるデータの高度利用を考えると、サイバーフィジカルシステム（CPS：Cyber Physical System）という概念を重視し、サイバーフィジカルシステムにおけるセキュリティリスクを特定する必要がある。CPS の導入は、あらゆる社会システムの効率化、新しい産業の創出、知的生産性の向上等の目的に有用である。CPS は、現実世界（物理空間）で発生する膨大な観測データ等の情報を、サイバー空間の強力な計算能力と結びつけて定量化するための方法論を提供するものである。

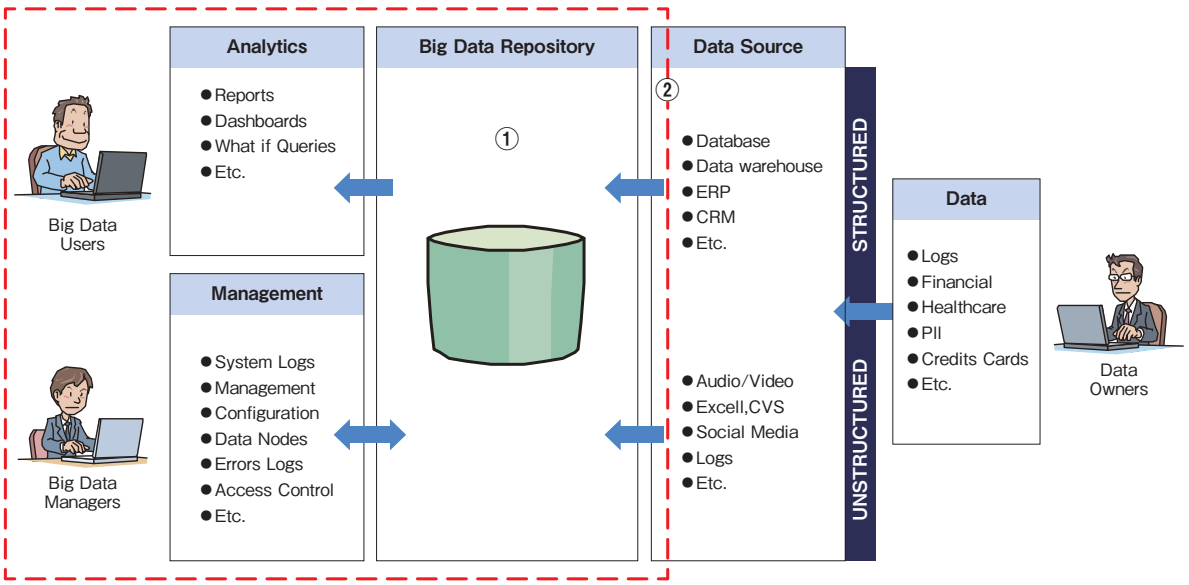
以上の背景から、日本の提案により 2020 年 4 月に PWI 5689 として「CPS のためのセキュリティフレームワーク」の議論が開始された。本フレームワークは経済産業省で構築した「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）[※322]」に基づいている（「2.1.2 (1) 産業サイバーセキュリティ研究会」参照）。現在のドラフトテキスト（N 5436）では、CPS の概念モデル、CPS 下でのセキュリティ懸念、ISO/IEC TS 27110 や NIST の文書と整合性のあるセキュリティフレームワークの記述がなされている。

規格案が一定のレベルに達したことにより、本 PWI を NP に移行するための投票が 2021 年 12 月 2 日から 2022 年 3 月 5 日まで実施され、規格に賛成した国は多かったものの、規格策定に貢献する国の数が不足していることが理由で投票は否決された。この結果、再審議を実施するため、再度 PWI に戻り、規格スコープを拡張して審議を継続する予定である。

(d) WG 4 に関連するその他の規格群

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

- ビジネス継続のための ICT 準備技術（27031）：PWI、NWI（New Work Item）の審議を経て、現在は WD3 の段階
- インターネットセキュリティガイドライン（27032）：現在は CD3 の段階



■図 2-6-3　ビッグデータソリューションにおけるセキュリティとプライバシーのスコープ
（出典）ISO・IEC「ISO/IEC WD 27046.4 - Information technology — Big data security and privacy — Implementation guidelines [※321]」を基に IPA が編集

- ネットワークセキュリティ（27033-7）：ネットワーク仮想化セキュリティのガイドラインとして NP が成立し、現在は WD4 の段階
- アプリケーションセキュリティ（27034）：パート 4 が FDIS に移行後、認証部分の記述の問題からキャンセルとなり、現在は PWI として審議を継続。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 は発行。パート 1、及びパート 2 については、見直しのフェーズ。なお、パート 4 が Coordination として提案され、現在 WD4 の段階
- サプライヤー関連セキュリティ（27036）：パート 1 から改版作業を開始
- デジタルエビデンスの識別、収集、確保、保全（27037）：改版作業なし
- リダクション（墨消し技術）（27038）：改版作業なし
- IDPS（不正検知・防止システム）（27039）：改版作業なし
- ストレージセキュリティ（27040）：大規模な改修を視野に入れ改版作業を開始、現在は CD1 の段階
- 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）：現在は CD2 の段階
- 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）：現在は FDIS の段階
- 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）：現在は CD2 の段階
- 公開鍵基盤における実践とポリシーの枠組み（27099）：現在は FDIS の段階
- 安全な配備、アップデート、及びアップグレード（4983）：NWI 審議を経て、現在は WD2 の段階
- データの起源―参照モデル（データ追跡のため）（5181）：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。2021 年度の主な活動を紹介する。

(a) アイデンティティ管理

2019 年 5 月に発行された ISO/IEC 24760-1（アイデンティティ管理のフレームワーク パート 1：用語と定義）は現在改訂中であり、2022 年 4 月のオンライン会議の結果、DIS に進むことになった。

2015 年 6 月に発行された ISO/IEC 24760-2（アイデンティティ管理のフレームワーク パート 2：リファレンスアーキテクチャと要件）も現在改訂中であり、4 月のオンライン会議の結果、アドホック（特設）グループが設立され、日本からもメンバーが参加し、改訂案を作成中である。

2016 年 8 月に発行された ISO/IEC 24760-3（アイデンティティ管理のフレームワーク パート 3：実践）は追補作成中であり、2022 年 3 月末から 4 月初旬のオンライン会議の結果、DIS に進むことになった。

(b) プライバシー

属性に基づく連結不能なエンティティ認証のためのフレームワークと要求事項を提供する ISO/IEC 27551 は 2021 年 9 月に発行された。

ユーザ主体でプライバシープリファレンス（プライバシー設定）を管理し、PII（Personally Identifiable Information）の提供を制御するフレームワークを規定する規格である ISO/IEC 27556 は、2022 年 5 月 24 日に DIS DoC（Disposition of Comments）オンライン会合を開催し、FDIS に進んだ。

再識別リスク及び非識別データのライフサイクルに関連するリスクを特定し、軽減するための枠組みを提供する ISO/IEC 27559 は、2022 年 5 月 30 日に DIS DoC オンライン会合を開催し、FDIS に進んだ。

中国から新規に提案された、組織とユーザの間で個人データを共有または伝送する際に、共有情報を最小限にしてリスクを低減し、プライバシーを向上させるゼロ知識証明（ZKP：Zero-Knowledge Proof）を利用するためのガイドラインの提供を目的とした ISO/IEC 27565 が、2022 年 2 月の投票の結果、NP から 1st WD へと進んだ。

ISO/IEC 27001 及び 27002 を拡張し、組織による PIMS（Privacy Information Management System：プライバシー情報マネジメントシステム）の構築を支援することを目的とする ISO/IEC 27701 は、発行から 3 年目を迎え pre-review 時期にあたることと、ISO/IEC 27002 の改訂版が 2022 年 2 月に発行されたことを受けて、2022 年 4 月の会合で改訂の必要があることが合意された。改訂範囲等の詳細を議論するアドホックグループが設置され、日本からもメンバーが参加し、議論する予定である。

(c) バイオメトリクス

バイオメトリックデータの保護技術を扱うISO/IEC 24745は、2011年に発行されたが、その後の新技術を反映するための改訂が行われ、2022年2月に第2版が発行された。

モバイル端末におけるバイオメトリック認証のセキュリティとプライバシーの要求事項を扱うISO/IEC 27553は、バイオメトリック処理のすべてをモバイル端末で行うローカルモードと、そうではないリモートモードを別パートで扱うように分割された。ローカルモードを扱うパート1は、2022年5月24～25日にDIS DoCオンライン会合を開催し、FDISに進んだ。リモートモードを扱うパート2は4月のオンライン会議の結果、NPとして登録されることとなった。

2.7 安全な政府調達に向けて

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

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

2.7.1 ITセキュリティ評価及び認証制度

サイバーセキュリティ戦略本部は、2021 年 7 月、府省庁及び独立行政法人が遵守すべき情報セキュリティ対策を定めた「政府機関等のサイバーセキュリティ対策のための統一基準（令和 3 年度版）」（以下、政府統一基準）を発行した。この中では、国民の情報等を扱う公的なサービスを提供するシステムを構築する場合、そのシステムを構成する市販の IT 製品についてもセキュリティ要件を策定することを調達者に求めている。

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

(1) 政府の IT 製品調達セキュリティ要件

政府統一基準では、調達及び運用において特にセキュリティ要件を策定すべき IT 製品分野として、経済産業省が発行している「IT 製品の調達におけるセキュリティ要件リスト※323」（以下、調達要件リスト）を参照している。調達要件リストには、利用者情報を扱うシステムの基盤となり、攻撃の対象となり得る以下の 11 の製品分野が指定されている。今後も対象製品分野は、拡大される予定である。

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

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

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

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

(2) 認証制度の国際連携

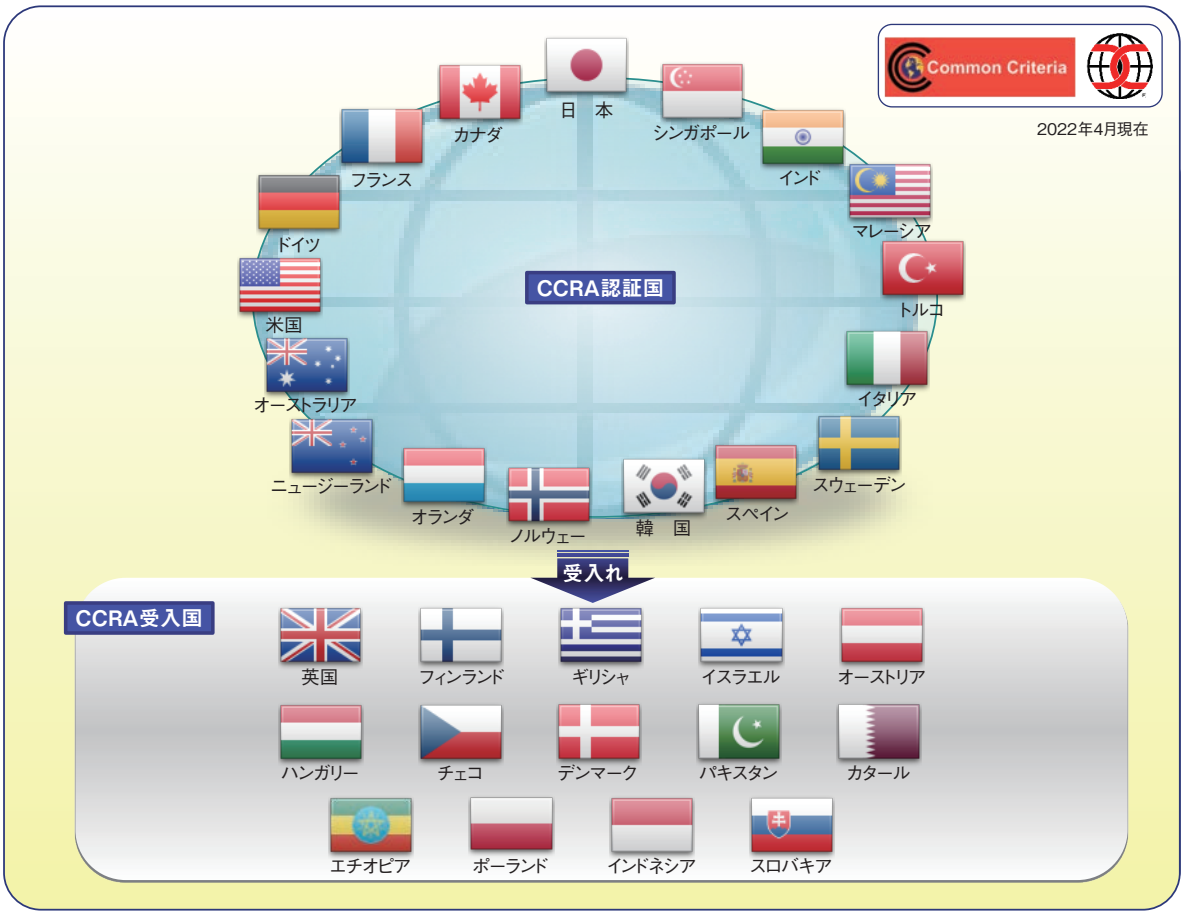
JISEC でも採用しているセキュリティ評価基準である ISO/IEC 15408 は、欧米 6 ヵ国によるコモンクライテリア（共通基準）プロジェクトとして開発された。これらの国々では、同じセキュリティ評価基準であるコモンクライテリアを用いて、その国を代表する公的機関が運営する制度で評価された結果については相互に認め合うことで、調達国ごとに重複する評価を行うコストを低減することを目的とした相互承認協定が締結された。この相互承認の

枠組みは、CCRA（Common Criteria Recognition Arrangement）と呼ばれ、その後多くの国が加盟し、JISEC を運営する日本も 2003 年に加盟している。これにより、日本のベンダは日本語の開発資料をそのまま利用し、JISEC で認証を取得した製品を CCRA 加盟国の政府調達の対象とすることができるようになった。CCRA では、自国で認証制度を運営している「認証国」と、認証制度をまだ有しないが政府調達要件として認証結果を受け入れる「受入国」があり、近年は東ヨーロッパやアフリカの国が受入国として加盟している。2022 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 2-7-1）。

(3) セキュリティ要件の共通化

コモンクライテリアでは、IT 製品が具備すべきセキュリティ要件を、規定された形式に従って記述する。例えば、アクセス制御機能においては、対象となるオブジェクトやサブジェクトのリスト、セキュリティ属性、それらを用いたアクセス方針をコモンクライテリアで規定された形式で記述する。これにより、調達者が必要としている IT 製品のセキュリティ要件仕様を、あいまいさを排除して製品開発者に伝えることを可能とする。このコモンクライテリア形式で表された調達要件仕様書を「プロテクションプロファイル」と呼び、CCRA 加盟国での IT 製品の政府調達に利用されている。加盟国の調達部門は、調達する IT 製品のセキュリティ要件をプロテクションプロファイルとして作成し、調達要件として公開している。これらのプロテクションプロファイルのうち汎用的なものは、CCRA のポータルサイト※324 にも掲載され、他の機関も同様の分野の製品を調達する際に用いることができる。日本においても、調達要件リストでは製品分野ごとにこれらのプロテクションプロファイルを指定している。また、独自の製品を調達する機関は、プロテクションプロファイルを自ら作成し※325、調達を実施している。

同じ製品分野の IT 製品調達で、似たような調達仕様が調達者ごとに提示されることは、開発者にとっては負荷となる。そこで CCRA では、加盟国の認証機関が中心となり、いくつかの製品分野で共通的に用いるプロテクションプロファイルの策定を行っている。このプロテクションプロファイルは、cPP（collaborative Protection

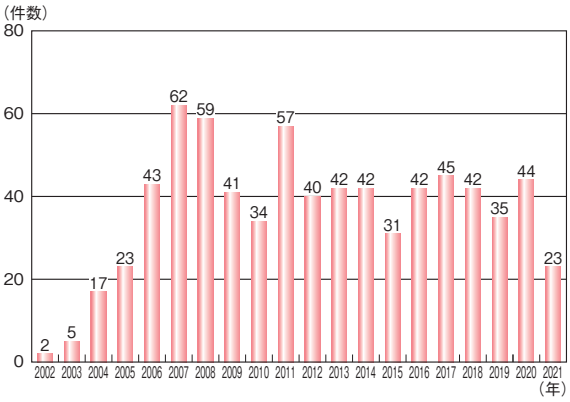


■図 2-7-1　CCRA 加盟国

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

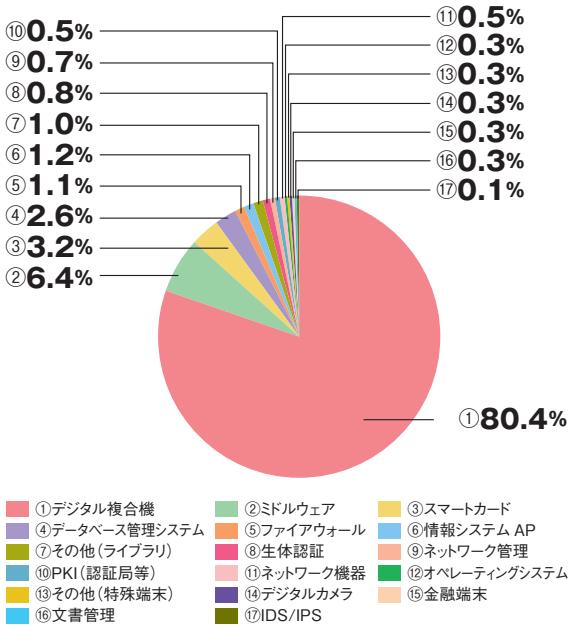
(4) 認証の状況

2021 年度までの JISEC における認証発行件数の推移を図 2-7-2 に示す。リーマンショックの影響による 2009 年の申請数の減少とそのリバウンド（2011 年）以降、毎年 40 件前後の認証発行を行ってきた。しかし、2021 年度の認証発行は前年度比約 48% 減となっている。これはコロナによる要員の配置や半導体調達の影響で、開発の遅延が発生したためである。

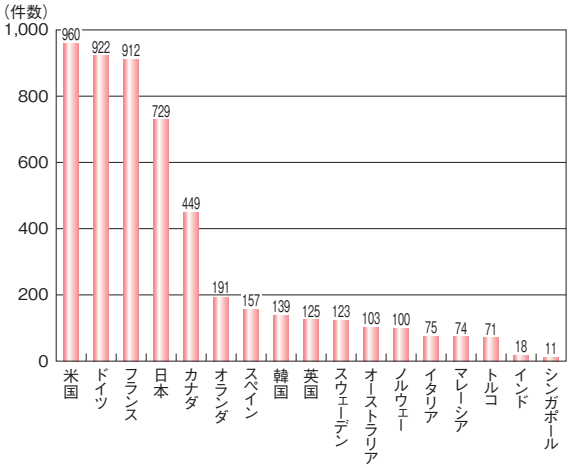


■図 2-7-2　JISEC の認証発行件数の推移

JISEC が認証発行した製品の分野の内訳を図 2-7-3 に示す。認証製品分野としては、デジタル複合機が圧倒的に多い。これは前述のように、日本のベンダが国際的にもシェアを有し、CCRA 加盟国においても政府調達の対象となっているからである。また、その他の製品分野の認証が JISEC で少ないのは、セキュリティ製品全般において日本ベンダの国際的な競争力が弱く、デジタル複合機以外の認証申請取得がなされないこと、ファイアウォールやネットワーク管理製品等はシステム構築の中で組み込まれてテストされ納入されることが多いため、製品単品での調達要件の対象とならないこと等が理由である。JISEC が毎年認証発行している 40 件前後は、ほとんどがデジタル複合機の新機種リリースによるものである。



■図 2-7-3　JISEC の認証発行の製品分野内訳



■図 2-7-4　CCRA 各国の認証件数

CCRA 加盟各国の認証機関が公開している認証発行件数の 2021 年度における累計を図 2-7-4 に示す。日本の認証発行件数は、米国、フランス、ドイツに次いで 4 番目に多い。これらの国は、政府調達に認証製品を活用しているのに加えて、国内に IT 製品の製造業者を多く持つ国々である。英国は、セキュリティ評価の歴史は長いにもかかわらず、国内の製造業者の減少により、2019 年に制度維持コストの削減を理由に認証国から受入国に移行している。韓国では、国際的に大きな市場を持つ製造業者が、製品仕向地に応じてモバイル製品は米国で、スマートカード関連製品はヨーロッパで認証を取得しているため、国内制度の認証発行件数は少ない。

(5) 2021 年度のトピック

JISEC では、IT 製品に対してだけでなく、プロテクションプロファイルに対しての認証[※326]も実施している。2021 年度から 2022 年度にかけて JISEC が認証した 2 件のプロテクションプロファイルを以下に紹介する。

(a) 特定用途機器ー共通セキュリティプロテクションプロファイル

政府統一基準では、調達要件リストとは別に、近年政府において活用されている IoT 製品についてもセキュリティ対策を求めている。更に 2020 年 4 月に施行された「電気通信事業法に基づく端末機器の基準認証」では、IoT 機器の技術基準にセキュリティ対策が追加された。このような背景を踏まえ、IoT 製品分野に係る国内ベンダが多く存在することから、JISEC では、安全な政府調達の推進と国際的な市場競争力の確保を目的に、IoT 製品分野への認証制度活用に向けた取り組みを実施している。

これまでにネットワークカメラシステム及び入退管理システムについて、調達者自身が調達時に必要なセキュリティ要件を確認できるようにチェックリストを公開している。IPA は 2020 年度にネットワークカメラシステムのチェックリストの基本的なセキュリティ要件について、コモンクライテリアの評価手法に従った検証を実施し、コモンクライテリア適用の有効性を確認した。この結果を踏まえ、2021 年度はネットワークカメラシステム等の IoT 機器を含む特定用途機器の基本的セキュリティ要件についてプロテクションプロファイルを策定し、JISEC でのプロテクションプロファイル認証を進めており、2022 年度上期に認証取得できる見込みである。今後、認証を取得したプロテクションプロファイルを用いた特定用途機器分野の政府調達での活用を推進していく。

(b) 電子パスポートプロテクションプロファイル

偽変造防止や安全かつ迅速な空港手続きを目的とした電子パスポートへの移行が、ICAO（International Civil Aviation Organization：国際民間航空機関）での国際標準化策定により各国で進められている。

日本においても、2015 年度に電子パスポート用 IC チップのプロテクションプロファイルの認証を行っている。2021 年度は、ICAO 文書の改訂やコモンクライテリア文書の改訂、パスポート特有のライフサイクル期間（最長 10 年間）を考慮し、ハッシュ関数のハッシュ長拡大、主要暗号アルゴリズムの鍵長拡大、楕円曲線暗号に用いる曲線拡大等、主に暗号面の安全性強化を行った新しいプロテクションプロファイルの認証を行った。今後、本プロテクションプロファイルに基づき製品認証を取得した IC チップが電子パスポートに採用されることにより、更にセキュリティ機能が強化された電子パスポートの推進・普及が期待される。

2.7.2 暗号モジュール試験及び認証制度

暗号モジュール試験及び認証制度（JCMVP：Japan Cryptographic Module Validation Program）とは、利用者が暗号モジュールの信頼性を客観的に把握できるように設けられた第三者適合性評価認証制度である。本制度に基づく認証を取得することにより、暗号アルゴリズムが適切に実装され、暗号鍵等の重要情報を適切に保護している暗号モジュールであることをアピールできる。本制度は、米国の NIST とカナダの CCCS（Canadian Centre for Cyber Security）により運営されている CMVP（Cryptographic Module Validation Program）[※327]と同等の制度であり、IPA が認証機関として運営している。本項では、JCMVP の最新動向、及び関連する CMVP の動向について述べる。

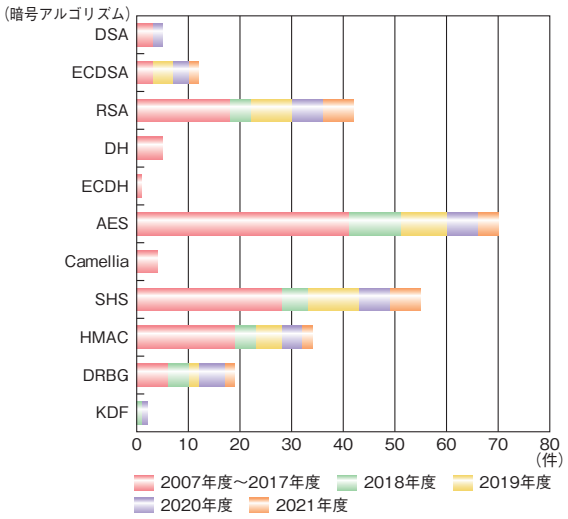
(1) 政府機関等における JCMVP の活用

政府統一基準における暗号・電子署名の遵守事項（6.1.5 節）に対する基本対策事項として、「政府機関等の対策基準策定のためのガイドライン（令和 3 年度版）」では「情報システムセキュリティ責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずること。」として、五つの例が挙げられている。その中の一つに、選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号または電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択することが挙げられている。また、各府省情報化統括責任者（CIO）連絡会議が決定し、2019 年 2 月に公開された「行政手続におけるオンラインによる本人確認の手法に関するガイドライン[※328]」において、JCMVP により認証されたハードウェアトークンに対して当人認証保証の最高レベル 3 を与えるとされている。

(2) IT セキュリティ評価及び認証制度（JISEC）との連携

IPA が運営する評価認証制度には、JISEC と JCMVP の二つがある。JISEC が 2016 年に発行、2020 年に改定したガイドライン※329 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「2.7.1 IT セキュリティ評価及び認証制度」参照）。

例えば、この活用方針に関連するデジタル複合機のプロテクションプロファイル「Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015※330」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。JISEC では、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）を活用して認証を行っている。2021 年度は、このプロテクションプロファイルに基づく認証が 8 件完了している※331。このような連携を通じて、図 2-7-5 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は、2018 年度から 2020 年度において堅調に増加してきた。2021 年度は 2020 年度よりも増加のペースが鈍ったが、それが新型コロナウイルス感染拡大の影響に起因する一時的なものかどうかは、現時点では不明である。また図 2-7-5 において、楕円曲線暗号の一つである ECDSA（Elliptic Curve Digital Signature Algorithm）は、2019 年度からは毎年実績が増えてきており、鍵長が比較的短くて済む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 2-7-5　JCATT により確認された暗号アルゴリズム実装の実績
（出典）IPA の公開情報を基に作成

(3) JIS X 19790 及び X 24759 の改正

JCMVP に関連する JIS 規格として、JIS X 19790（セキュリティ技術－暗号モジュールのセキュリティ要求事項）及び JIS X 24759（セキュリティ技術－暗号モジュールのセキュリティ試験要件）がある※332。JIS X 19790 は、コンピュータシステム及び通信システムの中のセキュリティシステムで使用される暗号モジュールに対するセキュリティ要求事項を規定したものである。JIS X 24759 は、暗号モジュールがその要求事項を満たしていることを試験機関が試験する方法等を規定したものである。これらは、それぞれ国際規格 ISO/IEC 19790 及び ISO/IEC 24759 の対応規格として作られている。

ISO/IEC 19790 は、2015 年 12 月に ISO/IEC 19790:2012/Cor.1:2015 として、暗号モジュールのソフトウェア及びファームウェア構成要素に対する誤り検出符号（EDC：Error-Detecting Code）の適用についての要求事項を追加する等、要求事項をより明確化した訂正版が発行されている。また、ISO/IEC 24759 は、2017 年 3 月に ISO/IEC 24759:2017 として、軽微な誤りの修正、技術的に正確な要件となるような修正を行い、ベンダ情報要件及び試験手順要件の一部を改正し、第 3 版が発行されている※333。

これに対し、JSA 及び IPA は、JIS X 19790 及び JIS X 24759 について、対応国際規格との乖離を解消するとともに技術の実態に即した内容にするための改正を進めることとした。IPA は、民間の有識者、学識経験者及び政府関係者からなる JIS X 19790 及び X 24759 原案作成委員会を組織し、JIS 改正原案を 2022 年 2 月に作成した。原案は JSA による校正を経て、2022 年 6 月に JSA から経済産業省へ提出された。

その後は、60 日間の WTO/TBT 意見受付公告※334 の後、JISC による審議を経て※335、2022 年末ごろに発行される見込みである。

(4) CMVP の動向

NIST と CCCS は、2019 年に CMVP の新しい規格となる FIPS 140-3※336 を発行したことを契機に 2020 年から FIPS 140-2 から FIPS 140-3 への移行を進めている。その移行スケジュールに則り、2021 年 9 月に FIPS 140-2 での新規申請が原則終了した（例外申請が認められた分も 2022 年 3 月で申請終了）。2026 年 9 月に FIPS 140-2 認証製品はすべて Historical List※337 へ移動する予定である。

2.7.3 政府情報システムのための セキュリティ評価制度（ISMAP）

2020 年 6 月 3 日、内閣官房、総務省、経済産業省は政府情報システムのためのセキュリティ評価制度（ISMAP）の開始をアナウンスした※338。本項では、ISMAP の概要について紹介する。

(1) ISMAP の概要

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

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

なお、ISMAP がクラウドサービスの申請受付を開始した 2020 年 10 月 1 日から 1 年間、現状やむを得ず ISMAP に登録されていないクラウドサービスを利用中、または利用予定の各政府機関等に対しては、当該サービスが申請されることを前提として、それらのサービスの利用を可能とする暫定措置期間が設けられていた。その暫定措置期間が 2021 年 9 月 30 日に期限を迎えることから、2021 年 7 月 6 日に開催された「サイバーセキュリティ対策推進会議・各府省情報化統括責任者（CIO）連絡会議」で、真にやむを得ないケースを対象に縮小した新規の暫定措置期間が設定された※339。

(2) ISMAP 制度制定の経緯

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※340」（2021 年 3 月 30 日付けで ISMAP に関する記述が追記されている）では、「クラウド・バイ・デフォルト原則」が掲げられた。これを踏まえ、経済産業省と総務省は、2018 年 8 月から「クラウドサービスの安全性評価に関する検討会※341」を発足させ、適切なセキュリティ要件を満たすクラウドサービスを導入するために必要な評価方法等を検討し、2020 年 1 月に「クラウドサービスの安全性評価に関する検討会とりまとめ※342」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※343」が決定された。

上記検討会において、2019 年 6 月から、政府情報システム調達に応募するクラウド事業者が遵守すべきセキュリティ管理基準（ISMAP 管理基準）の検討が行われた。ISMAP 管理基準は、国際規格をベースに「政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版）※344」「NIST SP800-53 rev.4」を参照して作成された。国際規格としては、情報セキュリティに関しては JIS Q 27001（ISO/IEC 27001）、JIS Q 27002（ISO/IEC 27002）とクラウドサービスの情報セキュリティに関する JIS Q 27017（ISO/IEC 27017）が参考にされた。また、これらの国際規格に準拠して編成された「クラウド情報セキュリティ管理基準（平成 28 年度版）」が参考にされ、そこに含まれるガバナンス基準について JIS Q 27014（ISO/IEC 27014）が参考にされた。

(3) ISMAP のフロー

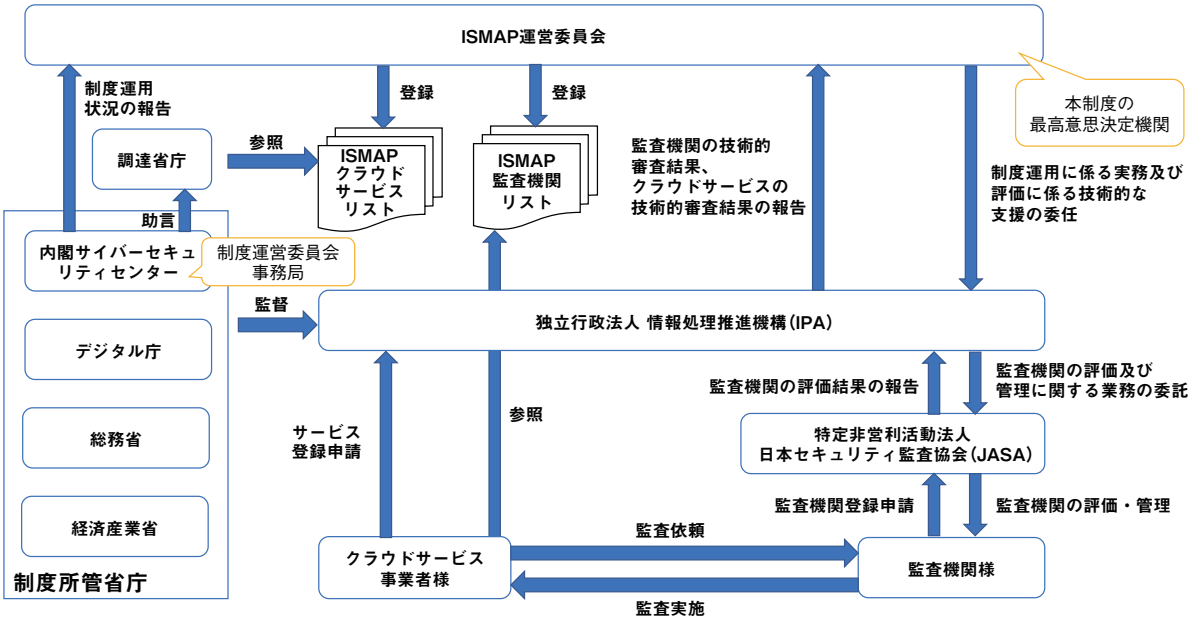
本制度においては、本制度で定められた情報セキュリティ監査の枠組みに基づき、政府機関等が調達するクラウドサービスに要求される基本的な情報セキュリティ管理・運用の基準を満たすセキュリティ対策を実施していることが確認されたクラウドサービスが、ISMAP クラウドサービスリスト（以下、サービスリスト）に登録される。政府機関がクラウドサービスを調達する場合、サービスリストに登録されたサービスを選定候補とする。

また、本制度における監査を実施できる監査機関は、あらかじめ本制度で定める要求事項を満たすことが確認され、本制度が公表する ISMAP 監査機関リスト（以下、監査機関リスト）に登録される。

本制度のフローを図 2-7-6（次ページ）に示す。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、ISMAP 運用支援機関である IPA を通じて ISMAP 運営委員会にサービス登録申請を行う。申請を受けた ISMAP 運営委員会は審査を行い、承認されたサービスがサービスリストに掲載される。府省庁の調達者はサービスリストを使って調達先候補を選ぶ。なお、本制度の運用に係る実務及び評価に係る技術的な支援は IPA が行い、そのうち、監査機関の評価及び管理に関する業務については、IPA から特定非営利活動法人日本セキュリティ監査協会（JASA）に委託している。

(4) ISMAP の運用

本制度は、2020 年 6 月に運用が開始された。



(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 2-7-6　クラウドサービスの安全性評価の制度のフロー
(出典)ISMAP「ISMAP 概要※345」

ISMAP の所管は 2022 年 1 月現在、NISC、デジタル庁、総務省、経済産業省であり、最高意思決定機関として ISMAP 運営委員会を設置し、事務局は NISC に置き、運用実務は IPA が担当している。

制度の概要、基準規程類、監査機関リスト、及びサービスリストは、2021 年 5 月に開設された ISMAP ポータルサイト※346 で公開されており、2022 年 1 月には本制度の登録について、ポータルサイトでの電子申請の受付を開始している。2022 年 6 月 1 日時点で登録されている監査機関は 5 機関、また、クラウドサービスは 34 サービスである。

(5) セキュアなクラウド利用に向けて

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

また、ISMAP で公開される情報は、重要インフラ分野等を始めとする民間においても参照されることで、クラウドサービスの適切な活用の推進が期待される。これに関連して、2019 年 5 月 23 日に改定された NISC の「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針(第 5 版)※347」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。」としており、国内の評価制度としては ISMAP が該当すると考えられる。

「クラウドサービスの安全性評価に関する検討会とりまとめ」にも記載されたように、情報システムのセキュリティ確保の責任は、一義的に当該システムの利用者である調達省庁が負うものである。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。情報システムの利用者である調達省庁は、利用するクラウドサービスについて適切な設定を行うことに加えて、情報システム全体のセキュリティリスクを分析し、適切な対策を行うことが求められる。

2.8 その他の情報セキュリティ動向

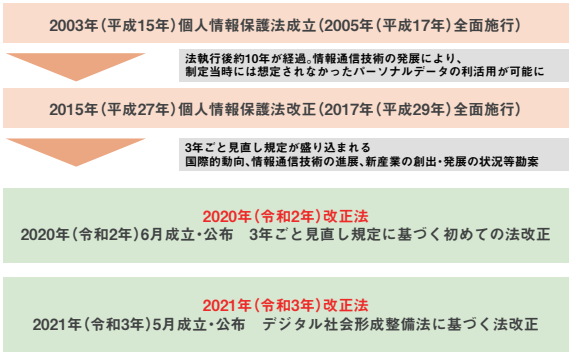
個人情報保護法改正、内部不正防止対策の動向、及び暗号技術の動向について述べる。

2.8.1 個人情報保護法改正

個人情報保護法※348は、情報流通や通信の高度な進展に伴う個人情報利活用の有用性に配慮しながら、個人の権利利益を保護することを目的とした、個人情報の取り扱いに関する法律である。個人情報保護に関する施策推進の基本的方向性や、国、地方公共団体、個人情報取扱事業者等が講ずべき措置の方向性が示されている。

(1) 個人情報保護法改正の経緯

個人情報保護法は2003年に成立、2005年に施行された。その後情報通信技術の進展や個人情報を利活用する要請の高まりに伴い、「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律※349」が2015年に成立、2017年に施行され、3年ごとの見直し規定が盛り込まれた。この見直し規定に基づき2020年に法改正され※350（2022年4月全面施行）、個人の権利の保護と活用の強化、越境データの流通増大に伴う新たなリスクへの対応、AI・ビッグデータ時代への対応等が盛り込まれた。更に2021年に「デジタル社会の形成を図るための関係法律の整備に関する法律※351」（デジタル社会形成整備法）に基づく法改正により※352、官民を通じた個人情報保護制度の見直し（官民一元化）が行われた。2021年改正法は2022年4月に政府関係機関・学術研究機関に対する部分が施行された。地方自治体関係機関に対する部分は2023年に施行予定である。



■図2-8-1　個人情報保護法改正の経緯

(2) 個人情報保護法改正の概要

2020年及び2021年の法改正の概要をまとめる。

(a) 2020年の個人情報保護法改正

個人情報に対する意識の高まり、技術革新を踏まえた保護と利活用のバランス、越境データの流通増大に伴う新たなリスクへの対応等の改正が実施された。2020年の改正の主な内容を挙げる。

①個人の権利の在り方

個人情報の利用停止・消去等の個人の請求権、個人データの開示方法、第三者提供記録の本人開示請求等が拡充された。

②事業者の守るべき責務の在り方

個人情報保護委員会への報告や本人への通知が義務化され、不適正な方法での個人情報利用が禁止された。

③事業者による自主的な取り組みを促す仕組みの在り方

認証個人情報保護団体制度で、企業の特定分野（部門）を対象とする団体を認定できるようになった。

④データ利活用の在り方

「仮名加工情報」が創設され、内部分析用途に限定し、開示・利用停止請求への対応義務が緩和された。

⑤ペナルティの在り方

命令違反・虚偽報告等の行為者への罰金が引き上げられ、法人は行為者より罰金刑最高額が引き上げられた（次ページ表2-8-1）。

⑥法の域外適用・越境移転の在り方

日本国内の個人情報等を取り扱う外国事業者を、罰則付きの報告徴収・命令の対象とした。また、外国の第三者への個人データ提供時、移転先での個人情報の取り扱いに関する本人への情報提供の充実が求められた。

なお、2020年の個人情報保護法改正については「情報セキュリティ白書2020※353」の「2.7.4 個人情報保護法の改正」も参照されたい。

		懲役刑		罰金刑	
		改正前	改正後	改正前	改正後
個人情報保護委員会からの命令への違反	行為者	6月以下	1年以下	30万円以下	100万円以下
	法人等	―	―	30万円以下	1億円以下
個人情報データベースなどの不正提供など	行為者	1年以下	1年以下	50万円以下	50万円以下
	法人等	―	―	50万円以下	1億円以下
個人情報保護委員会への虚偽報告等	行為者	―	―	30万円以下	50万円以下
	法人等	―	―	30万円以下	50万円以下

■表 2-8-1　2020 年改正前後の法定刑の比較
（出典）個人情報保護委員会「令和2年 改正個人情報保護法について※350」

(b) 2021 年の個人情報保護法改正

個人情報保護とデータ流通の両立・強化、国際的制度との調和を目的として 2021 年に法改正された。四つのポイントを以下に示す。

①個人情報保護法、行政機関個人情報保護法、独立行政法人等個人情報保護法の 3 本の法律を一つに統合し、地方公共団体の個人情報保護制度についても統合後の法律の中で全国的な共通ルールを規定し、全体の所管を個人情報保護委員会に一元化した（図 2-8-2 の①）。

②医療・学術分野の規律を官民で統一するため、国公立の病院、大学等には原則として民間の病院、大学等と同等の規律を適用した（図 2-8-2 の②）。

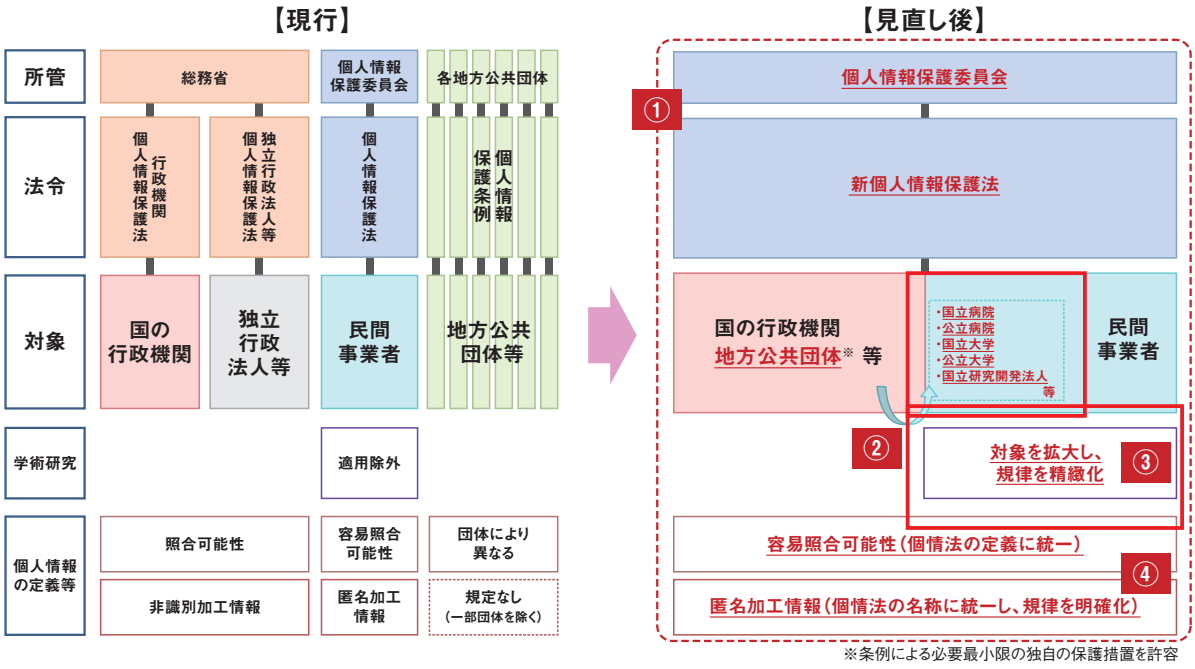
③学術研究分野を含めた GDPR の十分性認定への対応を目指し、学術研究に係る適用除外規定（学術研究目的の利用については本人同意を必須としない等）について、一律の適用除外ではなく、義務ごとの例外規定として精緻化した（図 2-8-2 の③）。

④個人情報の定義等を国・民間・地方で統一するとともに、行政機関等での匿名加工情報の取り扱いに関する規律を明確化した（図 2-8-2 の④）。

2021 年の改正法では、データの保有、利用目的、提供の適不適、例外適用の可否等の法解釈・運用に関する諸権限が、個人情報保護委員会に集約されることとなった。

また、多くのステークホルダーが関与し、全国広範囲で実施されるようなビジネスにおいて、しばしば「個人情報保護法制 2000 個問題※355」と呼ばれていた以下の諸問題について、同法が一律に適用される見込みであり、実効的解決が期待されることとなった。

- 個人情報関連法制が自治体ごとに異なるルール・解釈で運用されていた問題
- 個人情報を含むデータの利用を伴う新規案件の検討・実行の諸手続き解釈等の検討に長時間を要していた問題



■図 2-8-2　2021 年改正の概要
（出典）個人情報保護委員会「個人情報保護制度見直しの全体像※354」

- 効率を高め得る新技術導入が敬遠され、導入時に過度のカスタマイゼーションが求められがちであった問題

各自治体に改正法の統一的な条文が適用される一方、自治体ごとの条例で個別に定めることができるのは、統一的な部分に対するいわゆる上乗せ・横出し部分（条例要配慮個人情報等）になると考えられる。

更に、国公立大学・病院等、日常的活動そのものに官民の差があまりない領域においては、官民で規律を共通化することで連携が容易となり、データが適正に管理されているかの見極めも、個人情報保護委員会が一元的に判断可能となると期待される。

2.8.2 内部不正防止対策の動向

組織が保有する秘密情報の保護は重要な課題であり、内部不正が関係する情報漏えいは、組織において特に注意すべき脅威の一つである。2020 年度に IPA が実施した営業秘密管理に関する実態調査※356 の結果でも、情報漏えいインシデントの多くは内部不正により発生する傾向が高いことが示されている。また同調査によれば、近年のテレワーク等の働き方の変化、クラウド化等の IT プラットフォームの変化は、組織のセキュリティ対策実施のガバナンスを弱め、内部不正のリスクを高めている、との意識も強まっている。

これを受けて IPA は、2013 年に発行した「組織における内部不正防止ガイドライン」（以下、内部不正ガイドライン）を 2022 年 4 月に第 5 版に改訂した※357。本項では改訂にあたり、近年の社会的・技術的環境変化を整理し、インシデントや政策・対策の現状を調査した上で、重要な対策のポイントを整理した結果を紹介する。

(1) 内部不正によるインシデント事例

内部不正ガイドライン改訂に必要な情報収集の一環として、国内外の内部不正によるインシデント事例を報道や公知の文献情報等から調査した。具体的には、悪意による情報の漏えい、退職時の情報持ち出し、不適切に管理された情報の漏えい等に関係した事例を新たに収集した。第 5 版の改訂で内部不正ガイドラインに追記した事例の抜粋を表 2-8-2 に示す。

外部者からの働きかけによる営業秘密情報の漏えい、中途退職者による営業秘密情報の窃取、管理不備による営業秘密情報の外部への持ち出し等、以前から注意喚起され、現在も継続して発生している典型的事例が目を引く。

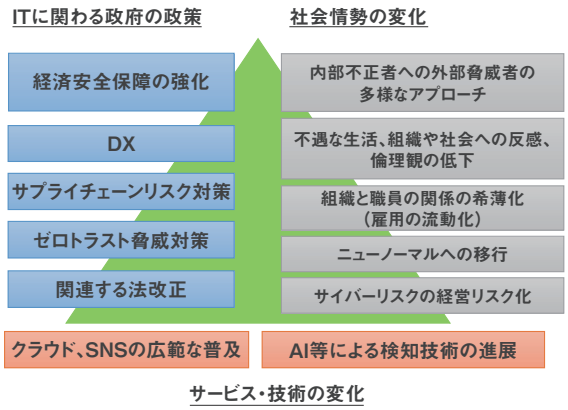
類型	内部不正の内容
技術情報の国外への漏えい	企業の防衛・宇宙部門に在籍していた職員が、防衛・宇宙関連の営業秘密にあたる技術情報を国外に漏えいさせた。 職員の出身国であった外国政府からのアプローチを受けたことによる。
営業秘密情報の漏えい	企業の職員が、退職後に企業のシステム内の機密情報に不正アクセスし営業秘密情報を窃取した。 業績不振を理由に解雇されることに不満があったこと、退職後に共有アカウントのパスワードが変更されていなかったことによる。
顧客情報（営業秘密）・個人情報の不正な持ち出し	企業の共同開発先として委託を受けた海外現地法人の職員が、業務用パソコンへ取引先情報及び個人情報を含むデータを許可なくダウンロードし、海外のクラウドストレージサービスの個人アカウントへアップロードした。 海外現地法人の職員に対する教育や内部不正対策の周知徹底が十分でなかったことによる。
個人情報の暴露	自治体の職員が、貸与パソコンから同自治体職員の個人情報を含むファイルを入手し、新聞社にファイル添付したメールを送信した。 貸与パソコンの中に、個人情報を含むファイルが残されていたこと、同職員には待遇への不満、自治体の情報管理不備をマスコミに告発することによる自己肯定欲求があったことによる。
システム・プログラムの破壊	企業の職員が、退職前に開発中のシステムのソースコードを社内で共有せず自分のパソコンから削除した。 処遇に不満があったこと、プログラム管理システムへのソースコード登録の手続き不備があったことによる。
システム・プログラムの改ざん	企業の職員が貸与されたコンピュータにハッキングツールをインストールし、他の職員の認証情報を盗み、外部の共犯者に渡した。共犯者は同社の Web サイトにその認証情報を用いて不正アクセスし、Web サイトを改ざんした。 支給されたコンピュータにハッキングツールをインストールすることが可能であったことによる。

■表 2-8-2　内部不正ガイドラインに掲載した内部不正事例（抜粋）

(2) 内部不正対策検討のポイント

内部不正のリスクを分析し、対策を検討する前提として、仕事や生活の IT 化・デジタル化に関する環境条件を整理することが有用であると考えられる。本改訂においては、それらの環境条件として IT に関わる政府の政策、社会情勢の変化、サービス・技術の変化の 3 点に注目した（次ページ図 2-8-3）。

IT に関わる政府の政策としては、サイバーセキュリティ戦略本部が公表している「サイバーセキュリティ 2021※2」等の IT セキュリティ戦略の観点から、経済安全保障の



■図 2-8-3　三つの環境条件から見た重要な変化

強化の必要性、DX 推進、サプライチェーンリスク対策、ゼロトラスト脅威対策、関連する法改正等が注目される。社会情勢の変化としては、内部不正者への外部脅威者の多様なアプローチ、不遇な生活・組織や社会への反感、倫理観の低下、組織と職員の関係の希薄化（雇用の流動化）、ニューノーマルへの移行、サイバーリスクの経営リスク化等が注目される。サービス・技術の変化については、クラウド・SNS の広範な普及、AI 等による検知技術の進展等が注目される。

内部不正防止ガイドラインの改訂においては、関連法制調査を含む文献調査の結果と、上記の三つの環境条件に関わる変化点を併せて整理し、新たな内部不正対策を検討するための七つの課題を抽出した。

①営業秘密、とりわけ重要技術情報の漏えいに対する社会的な危機感の拡大
②内部不正が事業経営に及ぼすリスクの増大
③テレワークに代表される働き方の変化、及びその常態化に伴う情報漏えいリスクの増大
④オンラインストレージやクラウド等の外部サービスの利用拡大
⑤セキュリティ技術（特にエンドポイントセキュリティやモニタリング技術）の急速な進展と個人情報に配慮した運用
⑥雇用の流動化による退職者（転職者）の急増
⑦法改正（個人情報保護法、不正競争防止法等）による漏えいの通報義務、重要データ保護等の強化

これらの課題のポイントは、以下として整理できる。

- 経営層のコミットメント
- 法制との整合
- 強化すべき対策

以下では強化すべき対策について、企業・有識者へのインタビュー調査を行い、収集した情報を踏まえた 3 点のポイントを示す。

(a) テレワーク・クラウドの普及に伴う対策

テレワークに代表される働き方の変化や、それに伴うオンラインストレージやクラウド等の外部サービスの利用拡大といった環境変化が顕著である。それらの変化に対応した技術的な対策・証拠保全等の事後対策等が重要であり、特に以下の対策に留意する。

- 個人情報・営業秘密情報等の重要情報が、テレワークやクラウド等の利用により広範囲に分散する傾向が強まるため、重要情報の棚卸しを行い、情報の保存場所・管理責任者等に関する管理ルールを定め、運用する。
- クラウドプロキシや CASB（Cloud Access Security Broker）の導入等により、クラウドの利用状況を把握し、管理されない「野良クラウド」の利用を認めない。
- クラウドサービスのアクセス権限の設定漏れや設定ミス等による意図しない相手への情報の曝露に注意する。
- クラウドサービスへのアクセスの認証ログ・アプリケーションの操作ログを取得し、ログに不正アクセスの痕跡が記録されていないかを定期的に確認する。
- データのダウンロードが制御できるクラウドサービスに限り使用許可を行う。
- テレワーク端末の内蔵記録装置（HDD・SSD 等）の暗号化やデータの遠隔消去等の対策を導入する。

(b) 退職者関連対策

IPA が 2021 年に公開した「企業における営業秘密管理に関する実態調査 2020[※356]」でも、営業秘密の漏えいルートは「中途退職者」による漏えいが 36.3% と最多であった。退職者の内部不正を防止する目的でシステムのモニタリングを行うことは抑止的な対策として有用である。

一方、プライバシーやコンプライアンスの観点からの注意点も存在する。退職予定者を含めた役職員をモニタリングするにあたり、その目的が、正しく業務を行っている役職員を保護するためであることを広く周知するべきである。経営者は、「モニタリングは不正アクセスの検知を目的とし、業績評価を目的としない」「モニタリングは正しい業務を行う職員を守るために行う」等の周知を就業規則等で明確に行い、役職員の理解を得ておくことが望ましい。

なお、退職後の秘密保持契約や誓約書の提出を退

職予定者に拒否されることもありえるため、雇用契約に退職時の禁忌事項を盛り込む等の対策も有効である。また、退職者が組織の外に重要情報を不正に開示するような事態を防ぐために、退職前の事前対策として、重要情報を組織の外に持ち出さないように本人に通知した上で技術的・物理的な情報漏えい対策を講じること等が有効である。

(c) ふるまい検知等の新技術対策

近年、急速に進展してきた新技術に、EDR（Endpoint Detection and Response）等のエンドポイントセキュリティ技術や、パソコン・システム上におけるふるまい検知を含む各種モニタリング技術がある。AI 等によるふるまい検知を行う製品・サービスも内部不正対策として実用レベルになってきている。

こうしたふるまい検知等の新技術を内部不正対策として適用することは効果的である一方、役職員の人権・プライバシーに配慮した運用が求められる。個人情報保護法・欧州の GDPR・米国のプライバシー関連法等のプライバシー保護規制に合わせた個人データの収集・分析や役職員の適切な保護が可能なシステムを選定すること、行動履歴を含む個人データの収集については労働規約等で周知しておくこと、分析を AI まかせにせず、「人間」による判断と「自動化・効率化」を組み合わせた運用を行う等、組織としてモニタリングの説明責任を果たせる運用体制の構築が対策のポイントとなる。

(d) 経営層へのメッセージ

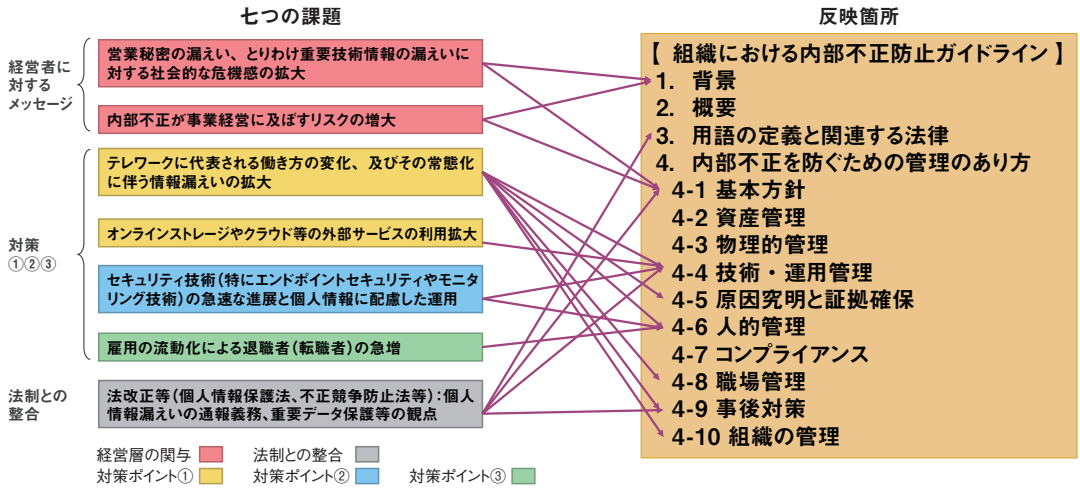
以上 3 点の対策ポイントに加えて、経営層の内部不正リスクに対する問題意識を高める施策はあらゆる対策の根幹として重要である。経営陣が内部不正インシデント発生時のリスクと責任を認識できるよう、インシデントにより引き起こされる事業への影響がどの程度なのか、BIA（Business Impact Analysis）等の分析により評価し、把握することが有用である。併せて、組織のリスクマネジメント体制の中に内部不正リスクを所管する責任者を明示的に置くことも経営リスクと責任の所在の明確化に役立つ。

(3) 内部不正ガイドラインの改訂内容

このように得られた知見に基づき、2022 年 4 月に内部不正ガイドラインを第 5 版に改訂した。検討した内部不正対策の七つの課題に対応する改訂箇所を特定し、前節で述べた対策強化ポイントを反映した（図 2-8-4）。

経営層への内部不正対策の重要性の訴求については、「1. 背景」「4-1 基本方針」部分の加筆を行った。テレワーク・クラウド・AI ／ふるまい検知技術の普及については、「4-4 技術・運用管理」に特に重点を置き加筆した。更に、モニタリング適用時の職員の人権・プライバシー保護等の必要性、雇用の流動化に伴う退職時の対策について「4-6 人的管理」の加筆・修正を行った。

更に、内部不正防止に関連する法制度の変化に対応するため、NISC の「サイバーセキュリティ関係法令 Q & A ハンドブック※359」等を参照し、各施策と個人情報保護法・改正不正競争防止法等の関係法制の対応を明示し、対策実施におけるコンプライアンスも重視した。内部不正ガイドライン第 5 版の今後の活用が望まれる。



■図 2-8-4　内部不正ガイドライン第 5 版の改訂箇所
（出典）株式会社エヌ・ティ・ティ・データ経営研究所「IPA『組織における内部不正防止ガイドライン』の改訂に係る調査等業務 概要説明資料※358」を基に IPA が編集

2.8.3 暗号技術の動向

本項では2021年度における、共通鍵暗号、公開鍵暗号及び実装攻撃に関する研究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

2021年度は、2020年度に引き続き、共通鍵暗号に関する解読について大きな進展はなかったものの、既存の暗号アルゴリズムへの攻撃について、攻撃に必要な計算量の削減等の進展があった。ここでは主な発表を紹介する。

AES※360については、二つの暗号解析論文が注目される。一つ目は、Eurocrypt 2021で、AES鍵スケジュールに対する新しい表現とそれを活用したAES-128に対する不能差分攻撃(impossible-differential attacks)の改善を報告した。INDOCRYPT 2010で報告された攻撃、及びその亜種が今までの最善の攻撃であったが、本提案手法はそれよりも約2.3倍計算量を改善している。この論文はEurocrypt 2021 Best paper awardを受賞した。二つ目は、同じくEurocrypt 2021にて、AES-128ハッシュモードの8段に対する最初の攻撃を報告した。これは、攻撃探索問題を混合整数線形計画法における制約条件のもとでの最適化問題に変換することで、攻撃の探索範囲を拡大し、より攻撃に有効な経路を発見できることを利用している。このように、AESに対する攻撃は2021年度も進展は見られたが、セキュリティマージンはまだ十分にあり、AESの安全性に直ちに影響を与えるものではない。

その他の暗号については、Eurocrypt 2021で、ARX(Addition, Rotation, and XOR)ベースの暗号に対する差分線形解析の改良が発表された。ストリーム暗号の一種であるChaCha※361がこのタイプに属し、研究結果として、時間計算量が2^{51}、データ計算量が2^{51}となるラウンド数6のChaChaに対する攻撃が発表された。この結果は、CRYPTO 2020で発表された今まで最良の攻撃計算量(時間計算量$2^{77.4}$、データ計算量2^{58})よりも大きく削減され、攻撃が進展したことを示している。ただ、ChaCha20のラウンド数20にはまだマージンがあり、早急な対策が必要となるものではない。

(2) 公開鍵暗号に関する研究及び標準化の動向

公開鍵暗号の一種であるRSA※362については、部分的に秘密鍵が分かっている場合の新規の素因数分解アルゴリズム(Partial Key Exposure Attack)がAsiacrypt 2021において提案された。素因数分解する数をNとして、今まではCRT-RSA指数※363のサイズが$N^{0.122}$以下のときの多項式時間攻撃が提案されていたが、本攻撃はCRT-RSA指数の最下位ビット(LSB:Least Significant Bit)の部分的な知識を仮定して、サイズが$N^{0.122}$以上$N^{0.5}$以下の場合の攻撃を実現している。

また、RSAへの攻撃方法を報告するSchnorr氏の査読前論文に関連して、格子理論を用いた素因数分解についての講演が、PKC 2021にて行われた。このSchnorr氏の攻撃方法は直ちにRSAの危殆化につながらないことは、既に専門家の間で暗黙の了解として共有されているものの、格子によるRSAの解析アプローチ自体は重要な研究であるため、今後も動向を注視すべきである。

NISTによる、量子計算機による解読に耐性を持つ暗号「耐量子計算機暗号(PQC:Post-Quantum Cryptography)」の標準化では、NIST PQC 3rd Standardization Conference※364において、NISTは「格子に基づかない汎用的電子署名スキームに関心がある」とした上で、第3ラウンド終了後、新たな提案募集を行う予定を明らかにした。応募期間は6ヵ月から1年の予定であり、特に構造付き格子(structured lattice)以外の汎用的電子署名スキームに興味を示している。第3ラウンドにおけるセレクションは未だ継続中であり、更に続く第4ラウンドもまた12～18ヵ月かけて行われる見通しである。最終的な標準化については、2024年に最終版を提出する予定であるという。

(3) 実装攻撃に関する研究動向

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

CPUの脆弱性を利用した具体的な暗号実装に対する攻撃として、RAS(Return Address Stack)を利用したサイドチャネル攻撃が発表された※365。

CPUには、処理速度を向上させるための様々な機構が実装されているが、その実装の脆弱性を突いた攻撃が近年注目されている。分岐予測※366や投機的実行※367の実装の脆弱性を突いた攻撃として2018年ごろに発見されたSpectre※368が有名である。最近のCPUには、分岐予測・投機的実行による処理速度向上を更に改善

するために、サブルーチンからのリターン命令における戻り先アドレスの予測機構も組み込まれ、そのためにリターンアドレスをCPU内のバッファに保存するRASという仕組みも実装されている。今回発表された攻撃は、このRASに注目し、悪意あるプロセスがRASのバッファを埋め尽くすことによってキャッシュミスを誘発し、タイミング攻撃※369を行うことで秘密鍵の推測につなげるものである。実際にOpenSSLによる楕円曲線P-256を使用したECDSA※370の署名生成に対する攻撃が有効であることも示している。この攻撃はCPUの様々な処理速度高速化手法が攻撃対象となり得ることを示しており、CPUのセキュリティには今後とも注視が必要である。

その他にも、ECDSAに対する攻撃として、テンプレート攻撃※371の一種であるOnline Template Attackに関する論文※372が発表されている。Online Template Attackは、テンプレート生成のための暗号演算の実行回数が少なくても実行できるように改良した攻撃である。以前の研究では理論的な攻撃可能性のみ検討されていたが、今回の発表では具体的な暗号実装であるlibgcrypt、mbedTLS、wolfTLSに対する適用可能性を示している。

※1 https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf〔2022/5/12 確認〕
※2 サイバーセキュリティ戦略本部：サイバーセキュリティ 2021（2020 年度年次報告・2021 年度年次計画） https://www.nisc.go.jp/pdf/policy/kihon-s/cs2021.pdf〔2022/5/12 確認〕
※3 IPA：サイバーセキュリティ経営可視化ツール https://www.ipa.go.jp/security/economics/checktool/index.html〔2022/5/12 確認〕
※4 IPA：サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集 https://www.ipa.go.jp/security/fy30/reports/ciso/index.html〔2022/5/12 確認〕
※5 NISC：プラス・セキュリティ知識補充講座 カリキュラム例 https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf〔2022/5/12 確認〕
※6 IPA：サイバーセキュリティお助け隊サービス制度 https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html〔2022/5/12 確認〕
※7 NEDO：戦略的イノベーション創造プログラム（SIP）第 2 期／ IoT 社会に対応したサイバー・フィジカル・セキュリティ https://www.nedo.go.jp/activities/ZZJP2_100123.html〔2022/5/12 確認〕
※8 経済産業省：情報セキュリティサービス審査登録制度 https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html〔2022/5/12 確認〕
※9 https://security-portal.nisc.go.jp/〔2022/5/12 確認〕
※10 総務省：インターネットトラブル事例集 https://www.soumu.go.jp/use_the_internet_wisely/trouble/〔2022/5/12 確認〕
※11 NISC：クラウドを利用したシステム運用に関するガイダンス（詳細版） https://www.nisc.go.jp/pdf/policy/infra/cloud_guidance.pdf〔2022/5/12 確認〕
※12 https://www.ismap.go.jp/csm?id=cloud_service_list〔2022/5/12 確認〕
※13 https://www.digital.go.jp/about/〔2022/5/12 確認〕
※14 デジタル庁：マイナンバー制度及び国と地方のデジタル基盤抜本改善ワーキンググループの開催について https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/658916e5-76ce-4d02-9377-1273577ffc88/20211021_meeting_my_number_wg_01.pdf〔2022/5/12 確認〕
※15 https://www.nisc.go.jp/pdf/policy/general/kijyunr3.pdf〔2022/5/12 確認〕
※16 https://www.nisc.go.jp/pdf/policy/general/guider3.pdf〔2022/5/12 確認〕
※17 政府 CIO ポータル：ガバメント・クラウド先行事業（市町村の基幹業務システム）の公募及びガバメントクラウド先行事業（地方自治体のセキュリティシステム）の公募について【地方自治体職員対象】 https://cio.go.jp/node/2778〔2022/5/12 確認〕
※18 デジタル庁：ガバメントクラウド先行事業（市町村の基幹業務システム等）の採択結果を公表しました https://www.digital.go.jp/news/ZYzU5DYY/〔2022/5/12 確認〕
※19 NISC：重要インフラのサイバーセキュリティに係る行動計画（案） https://www.nisc.go.jp/pdf/policy/infra/pubcom_keikakuan.pdf〔2022/5/12 確認〕
※20 https://www.nisc.go.jp/pdf/council/2020-meeting/2020-meeting-saisyuhoukoku.pdf〔2022/5/12 確認〕
※21 NISC：日・ASEAN 国際サイバー演習の開催 https://www.nisc.go.jp/pdf/press/international_asean_rcx_20210625_jp.pdf〔2022/5/12 確認〕
※22 NISC：第 14 回 日・ASEAN サイバーセキュリティ政策会議の結果 https://www.nisc.go.jp/pdf/press/AMSJ_CPM_20211021_r2.pdf〔2022/5/12 確認〕
※23 サイバーセキュリティ戦略本部：サイバーセキュリティ研究開発戦略（改訂） https://www.nisc.go.jp/pdf/policy/kihon-1/kenkyu2021-kettei.pdf〔2022/5/12 確認〕
※24 NICT：プライバシー保護連合学習技術を活用した不正送金検知の実証実験を実施 https://www.nict.go.jp/press/2022/03/10-1.html〔2022/5/12 確認〕
※25 サイバーセキュリティ対策推進会議等：政府機関におけるデジタル改革に必要なIT・セキュリティ知識を有する人材の確保・育成総合強化方針 https://www.nisc.go.jp/pdf/policy/materials/jinzai_kyoka_hoshin2021.pdf〔2022/5/12 確認〕
※26 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/001_05_00.pdf〔2022/5/12 確認〕
※27 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/002_03_00.pdf〔2022/5/12 確認〕
※28 経済産業省：第 6 回 産業サイバーセキュリティ研究会 事務局説明資料 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/006_03_00.pdf〔2022/5/12 確認〕
※29 2022 年 4 月の「第 7 回 産業サイバーセキュリティ研究会 事務局説明資料」（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/007_03_00.pdf〔2022/5/12 確認〕）では「6 つの処方箋」に増えた。
※30 CPSF の詳細については「情報セキュリティ白書 2020」の「2.1.2 (1) (a) WG1（制度・技術・標準化）」(p.69)を参照。
※31 経済産業省：ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第 1 版 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/20190617_report.html〔2022/5/12 確認〕
※32 防衛省：防衛産業サイバーセキュリティ基準の強化について https://www.mod.go.jp/atla/pinup/pinup040401.pdf〔2022/5/12 確認〕
※33 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/20210222_report.html〔2022/5/12 確認〕
※34 https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_guideline_V02_00.pdf〔2022/5/12 確認〕
※35 経済産業省：「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」を策定しました https://www.meti.go.jp/press/2021/04/20210401005/20210401005.html〔2022/5/12 確認〕
※36 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/pdf/006_05_00.pdf〔2022/5/12 確認〕
※37 https://www.meti.go.jp/policy/netsecurity/wg1/IoT-SSF_ver1.0_UseCase.pdf〔2022/5/12 確認〕
※38 経済産業省：協調的なデータ利活用に向けたデータマネジメント・フレームワークを策定しました https://www.meti.go.jp/press/2022/04/20220408005/20220408005.html〔2022/5/12 確認〕
※39 経済産業省：オープンソースソフトウェアの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集を取りまとめました https://www.meti.go.jp/press/2021/04/20210421001/20210421001.html〔2022/5/12 確認〕
※40 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/006_03_00.pdf〔2022/5/12 確認〕
※41 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/007_03_00.pdf〔2022/5/12 確認〕
※42 経済産業省：サイバーセキュリティ経営ガイドラインと支援ツール https://www.meti.go.jp/policy/netsecurity/mng_guide.html〔2022/5/12 確認〕
※43 IPA：プラクティス・ナビ https://www.ipa.go.jp/security/economics/practice/〔2022/5/12 確認〕
※44 経済産業省：サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版 https://www.meti.go.jp/policy/netsecurity/downloadfiles/tekibihontai1.1r.pdf〔2022/5/12 確認〕
※45 IPA：試行導入・導入実績公表の手引き https://www.ipa.go.jp/files/000090566.pdf〔2022/5/12 確認〕
※46 経済産業省：機器のサイバーセキュリティ確保のためのセキュリティ検証の手引きを取りまとめました https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html〔2022/5/12 確認〕
※47 総務省・経済産業省：DX 時代における企業のプライバシーガバナンスガイドブック ver1.2 https://www.meti.go.jp/policy/it_policy/privacy/guidebook12.pdf〔2022/5/12 確認〕
※48 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〔2022/5/12 確認〕
※49 株式会社三菱総合研究所：「産業競争力強化法に基づく技術情報管理認証制度の普及促進に向けた調査分析及び専門家派遣等事業」（経済産業省事業）において専門家の派遣を希望する事業者の公募のご案内について https://www.mri.co.jp/news/public_offering/20210805.html〔2022/5/12 確認〕
※50 経済産業省：「情報セキュリティサービス基準第 2 版」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第 2 版」を公表しました https://www.meti.go.jp/press/2021/01/20220131003/20220131003.html〔2022/5/17 確認〕
※51 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。
※52 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〔2022/5/17 確認〕

※ 53 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。
※ 54 セプターカウンシル：各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う、分野横断的な情報共有体制。
※ 55 https://www.ipa.go.jp/files/000098129.pdf〔2022/5/16 確認〕
※ 56 「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。
※ 57 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2021 年 10 月～ 12 月］ https://www.ipa.go.jp/files/000095766.pdf〔2022/5/16 確認〕
※ 58 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〔2022/5/16 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〔2022/5/16 確認〕
※ 59 https://www.ipa.go.jp/security/J-CRAT/index.html〔2022/5/16 確認〕
※ 60 https://www.soumu.go.jp/main_content/000698567.pdf〔2022/5/16 確認〕
※ 61 https://www.soumu.go.jp/main_content/000761893.pdf〔2022/5/16 確認〕
※ 62 https://warp.ndl.go.jp/info:ndljp/pid/11688280/www.kantei.go.jp/jp/singi/it2/dgov/201225/siryou1.pdf〔2022/5/16 確認〕
※ 63 https://www.nisc.go.jp/pdf/council/cs/dai17/17shiryou02.pdf〔2022/5/16 確認〕
※ 64 新経済連盟：電気通信事業法の改正の方向性に対する懸念について https://jane.or.jp/proposal/pressrelease/15987.html〔2022/5/16 確認〕
一般社団法人日本経済団体連合会：総務省『電気通信事業ガバナンス検討会報告書（案）』に対する意見 https://www.keidanren.or.jp/policy/2022/012.html〔2022/5/16 確認〕
※ 65 総務省：「電気通信事業ガバナンス検討会 報告書」及び意見募集の結果の公表 https://www.soumu.go.jp/menu_news/s-news/01kiban05_02000237.html〔2022/5/16 確認〕
※ 66 総務省：IP ネットワーク設備委員会 https://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/joho_tsusin/ipnet/ipnet.html〔2022/5/16 確認〕
※ 67 OODA：Observe, Orient, Decide, Act の略。
※ 68 総務省：情報通信審議会 情報通信技術分科会IPネットワーク設備委員会第五次報告（案）～ IoT の普及に対応した電気通信設備に係る技術的条件～ https://www.soumu.go.jp/main_content/000759203.pdf〔2022/5/16 確認〕
※ 69 総務省：情報通信審議会 情報通信技術分科会 IP ネットワーク設備委員会 第五次報告（案）に対する意見募集の結果 https://www.soumu.go.jp/menu_news/s-news/01kiban05_02000228.html〔2022/5/16 確認〕
※ 70 総務省：電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第四次とりまとめ（案）についての意見募集 https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000130.html〔2022/5/16 確認〕
※ 71 総務省：「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第四次とりまとめ」及び意見募集の結果の公表 https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000134.html〔2022/5/16 確認〕
※ 72 e-GOV 法令検索：特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律 https://elaws.e-gov.go.jp/document?lawid=502AC0000000037〔2022/5/16 確認〕
※ 73 総務省：令和 4 年度税制改正要望の結果 https://www.soumu.go.jp/menu_news/s-news/01kanbo05_02000157.html〔2022/5/16 確認〕
※ 74 O-RAN：https://www.o-ran.org〔2022/5/16 確認〕
※ 75 総務省：2.3GHz 帯における第 5 世代移動通信システムの普及のための周波数の割当てに関する意見募集 https://www.soumu.go.jp/menu_news/s-news/01kiban14_02000525.html〔2022/5/16 確認〕
※ 76 ICT-ISAC JAPAN:ローカル 5G セキュリティ対策に関するアンケート結果（概要版）の公開について https://www.ict-isac.jp/news/news20210315.html〔2022/5/16 確認〕
※ 77 総務省：テレワークセキュリティガイドライン 第5版 https://www.soumu.go.jp/main_content/000752925.pdf〔2022/5/16 確認〕
※ 78 総務省：中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）第2版 https://www.soumu.go.jp/main_content/000753141.pdf〔2022/5/16 確認〕
※ 79 株式会社東京商工リサーチ：「テレワークセキュリティに係る実態調査 調査報告書」 https://www.soumu.go.jp/main_content/000811682.pdf〔2022/5/16 確認〕
※ 80 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〔2022/5/16 確認〕
※ 81 総務省：タイムスタンプについて https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/timestamp.html〔2022/5/16 確認〕
※ 82 総務省：組織が発行するデータの信頼性を確保する制度に関する検討会取りまとめ（案）及び e シールに係る指針（案）に対する意見募集の結果 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00114.html〔2022/5/16 確認〕
※ 83 総務省・法務省・経済産業省：利用者の指示に基づきサービス提供事業者自身の署名鍵により 暗号化等を行う電子契約サービスに関する Q&A https://www.soumu.go.jp/main_content/000697715.pdf〔2022/5/16 確認〕
※ 84 総務省・法務省・経済産業省：利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関する Q&A（電子署名法第3条関係） https://www.soumu.go.jp/main_content/000705576.pdf〔2022/5/16 確認〕
※ 85 総務省：電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第２版） https://www.soumu.go.jp/main_content/000705080.pdf〔2022/5/16 確認〕
※ 86 CCDS：サーティフィケーションプログラムにおけるセキュリティ要件 https://www.ccds.or.jp/certification/requirements.html〔2022/5/16 確認〕
※ 87 CCDS：プログラム概要 https://www.ccds.or.jp/certification/index.html〔2022/5/16 確認〕
※ 88 CCDS：2021.10.15 [CCDS] 現金自動預け払い機 (ATM) 関連システムの物理・サイバー攻撃対策に関する CCDS サーティフィケーションプログラムの運用開始 https://www.ccds.or.jp/event/2021/20211015/20211015.html〔2022/5/16 確認〕
※ 89 総務省・NICT：IoT 機器調査及び利用者への注意喚起の取組「NOTICE」の実施 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00011.html〔2022/5/16 確認〕
※ 90 総務省：情報通信ネットワークの安全性・信頼性の確保に係るサイバーセキュリティ対策の現状と課題 https://www.soumu.go.jp/main_content/000812244.pdf〔2022/5/16 確認〕
※ 91 NICT：サイバー攻撃に悪用されるおそれのある IoT 機器の調査等（NOTICE）の取組内容の変更について https://notice.go.jp/news/topic/news20220121〔2022/5/16 確認〕
※ 92 NICT：NICTER 観測レポート 2021 https://www.nict.go.jp/cyber/report/NICTER_report_2021.pdf〔2022/5/16 確認〕
※ 93 総務省：「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）」（案）に対する意見募集の結果及び「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）」の公表 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00121.html〔2022/5/16 確認〕
※ 94 https://www.soumu.go.jp/main_content/000757799.pdf〔2022/5/16 確認〕
※ 95 https://www.soumu.go.jp/main_content/000757800.pdf〔2022/5/16 確認〕
※ 96 総務省：日仏 ICT 政策協議（第 21 回）の結果 https://www.soumu.go.jp/menu_news/s-news/01tsushin08_02000120.html〔2022/5/16 確認〕
※ 97 総務省：日 EU・ICT 政策対話（第 27 回）の結果 https://www.soumu.go.jp/menu_news/s-news/01tsushin08_02000128.html〔2022/5/16 確認〕
※ 98 総務省：日独 ICT 政策対話（第 6 回）の結果 https://www.soumu.go.jp/menu_news/s-news/01tsushin08_02000130.html〔2022/5/16 確認〕
※ 99 NICT：サイバーセキュリティネクサス https://www.nict.go.jp/cynex/〔2022/5/16 確認〕
※ 100 NICT：サイバーセキュリティ演習基盤 CYROP のオープン化トライアルを開始 https://www.nict.go.jp/press/2022/02/03-1.html〔2022/5/16 確認〕
※ 101 総務省：地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会 https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security_r03/index.html〔2022/5/16 確認〕
※ 102 総務省：「地方公共団体における情報セキュリティポリシーに関するガイドライン」等の公表及び意見募集の結果 https://www.soumu.go.jp/menu_news/s-news/01gyosei07_02000128.html〔2022/5/16 確認〕
※ 103 総務省：「地方公共団体における情報セキュリティポリシーに関するガイドライン」改定のポイントについて（案）」 https://www.soumu.

go.jp/main_content/000785574.pdf〔2022/5/16 確認〕
※ 104 閣議決定：デジタル社会の形成に関する重点計画・情報システム整備計画・官民データ活用推進基本計画について https://cio.go.jp/sites/default/files/uploads/documents/digital/20211224_policies_priority_package.pdf〔2022/5/16 確認〕
デジタル庁：デジタル社会の実現に向けた重点計画 https://www.digital.go.jp/policies/priority-policy-program〔2022/5/16 確認〕
※ 105 デジタル庁：地方自治体によるガバメントクラウドの活用について（案） https://cio.go.jp/sites/default/files/uploads/documents/digital/20211224_local_governments_02.pdf〔2022/5/16 確認〕
※ 106 内閣官房：ガバメントクラウド先行事業（セキュリティシステム）公募要項 https://cio.go.jp/sites/default/files/uploads/documents/koubosecurity20210604.pdf〔2022/5/16 確認〕
※ 107 内閣官房：地方自治体によるガバメントクラウドの活用（先行事業）について https://cio.go.jp/sites/default/files/uploads/documents/senkoujigyougaiyou20210831.pdf〔2022/5/16 確認〕
※ 108 デジタル庁：ガバメントクラウド先行事業（市町村の基幹業務システム等）の採択結果を公表しました https://www.digital.go.jp/posts/ZYzU5DYY〔2022/5/16 確認〕
※ 109 総務省：無線 LAN（Wi-Fi）の安全な利用（セキュリティ確保）について https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/〔2022/5/16 確認〕
※ 110 総務省：無線 LAN のセキュリティ対策に係るオンライン講座の開講 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00127.html〔2022/5/16 確認〕
※ 111 e-Gov 法令検索：不正アクセス行為の禁止等に関する法律 https://elaws.e-gov.go.jp/document?lawid=411AC0000000128〔2022/5/16 確認〕
※ 112 総務省：不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00128.html〔2022/5/16 確認〕
※ 113 https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html〔2022/5/16 確認〕
※ 114 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〔2022/5/10 確認〕
※ 115 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〔2022/5/10 確認〕
※ 116 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf〔2022/5/10 確認〕
※ 117 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf〔2022/5/10 確認〕
※ 118 警察庁：企業の皆様へ サイバー犯罪の被害は警察へ通報を! https://www.npa.go.jp/cyber/ransom/pdf/leaflet.pdf〔2022/5/10 確認〕
警察庁：ランサムウェア被害防止対策 https://www.npa.go.jp/cyber/ransom/index.html〔2022/5/10 確認〕
※ 119 一般社団法人日本損害保険協会：多様化するリスクとサイバー保険 https://www.sonpo.or.jp/cyber-hoken/risk/〔2022/5/10 確認〕
※ 120 警察庁：不正アクセス行為対策等の実態調査 アクセス制御機能に関する技術の研究開発の状況等に関する調査 調査報告書 https://www.npa.go.jp/cyber/research/r3/R3countermeasures.pdf〔2022/5/10 確認〕
※ 121 警察庁：令和 3 年版警察白書（特集 2 サイバー空間の安全の確保） https://www.npa.go.jp/hakusyo/r03/pdf/03_tokushu02.pdf〔2022/5/10 確認〕
※ 122 外務省：中国政府を背景に持つ APT40 といわれるサイバー攻撃グループによるサイバー攻撃等について（外務報道官談話） https://www.mofa.go.jp/mofaj/press/danwa/page6_000583.html〔2022/5/10 確認〕
※ 123 NISC・警察庁:中国政府を背景に持つ APT40 といわれるサイバー攻撃グループによるサイバー攻撃等について（注意喚起） https://www.npa.go.jp/cybersecurity/pdf/20210719pr.pdf〔2022/5/10 確認〕
※ 124 警察庁：治安の回顧と展望（令和3年版） https://www.npa.go.jp/bureau/security/publications/kaiko_to_tenbou/R3/kaitenR3.pdf〔2022/5/10 確認〕
※ 125 サイバーセキュリティ政策会議：サイバー空間の脅威への対処について法学・技術系学者、弁護士、ITベンダー、日本サイバー犯罪対策センター等多様な分野の有識者による検討を行うサイバーセキュリティ・情報化審議官主催の私的懇談会。
警察庁：サイバーセキュリティ政策会議 https://www.npa.go.jp/cybersecurity/CS.html〔2022/5/10 確認〕
※ 126 サイバーセキュリティ政策会議：実空間とサイバー空間とが融合したデジタル社会の安全・安心の確保 https://www.npa.go.jp/cybersecurity/pdf/20211217_2.pdf〔2022/5/10 確認〕
※ 127 警察庁：警察法の一部を改正する法律案要綱 https://www.npa.go.jp/laws/kokkai/220128/01_youkou.pdf〔2022/5/10 確認〕
※ 128 JC3：総務省を騙った特別定額給付金に関するフィッシングに注意 https://www.jc3.or.jp/threats/topics/article-42.html〔2022/5/10 確認〕
※ 129 警察庁：警察活動の回顧と展望 https://www.npa.go.jp/bureau/soumu/tenbou/kaikototenbou.pdf〔2022/5/10 確認〕
※ 130 JC3：フィッシングターゲットの変遷 https://www.jc3.or.jp/threats/topics/article-430.html〔2022/5/10 確認〕
※ 131 警察庁：サイバー攻撃に対する技術的対応 https://www.npa.go.jp/joutuu/012.htm〔2022/5/10 確認〕
※ 132 警察庁：令和３年の犯罪情勢 https://www.npa.go.jp/publications/statistics/crime/situation/r3_hanzaijyousei.pdf〔2022/5/10 確認〕
※ 133 警察庁：犯罪インフラ化するSMS認証代行への対策について https://www.npa.go.jp/cyber/policy/pdf/R030422_SMStaisaku.pdf〔2022/5/10 確認〕
※ 134 警察庁：令和２年の犯罪情勢 https://www.npa.go.jp/publications/statistics/crime/situation/r2_report_c.pdf〔2022/5/10 確認〕
※ 135 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-0001-2012r6.pdf〔2022/4/21 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。
※ 136 https://www.ipa.go.jp/security/ipg/documents/ipa-cryptrec-gl-3002-1.0.pdf〔2022/4/21 確認〕
※ 137 EdDSA（Edwards-curve Digital Signature Algorithm）：楕円曲線の一種であるエドワーズ曲線を用いたデジタル署名アルゴリズム。
※ 138 NIST Lightweight Cryptography コンペティションファイナリスト：NIST が主催する軽量暗号コンペティション（NIST：Lightweight Cryptography https://csrc.nist.gov/Projects/lightweight-cryptography〔2022/4/21 確認〕）の最終選考に残ったアルゴリズム。
※ 139 CRYPTREC：2021 年度 第1回 暗号技術検討会 https://www.cryptrec.go.jp/report/cryptrec-mt-1011-2021.pdf〔2022/4/21 確認〕
上記に含まれる「配付資料3−4 2021 年度暗号技術調査 WG（耐量子計算機暗号）活動報告」を参照。
※ 140 外務省：G7 コーンウォール・サミット（概要） https://www.mofa.go.jp/mofaj/ecm/ec/page4_005342.html〔2022/5/11 確認〕
※ 141 外務省：2021 年開かれた社会声明 https://www.mofa.go.jp/mofaj/files/100200087.pdf〔2022/5/11 確認〕
※ 142 外務省：G7 首脳テレビ会議 https://www.mofa.go.jp/mofaj/ecm/ec/page6_000665.html〔2022/5/11 確認〕
※ 143 外務省：G7 首脳声明 https://www.mofa.go.jp/mofaj/ecm/ec/page4_005524.html〔2022/5/11 確認〕
※ 144 外務省：G7 首脳会合 https://www.mofa.go.jp/mofaj/ecm/ec/page6_000680.html〔2022/5/11 確認〕
※ 145 首相官邸：ロシアによるウクライナ侵略を踏まえた対応について https://www.kantei.go.jp/jp/headline/ukraine2022/index.html〔2022/5/23 確認〕
※ 146 NISC：東京大会におけるサイバーセキュリティ対策と今後の取組方針 https://www.nisc.go.jp/pdf/policy/2020/Tokyo2020houkoku.pdf〔2022/5/11 確認〕
※ 147 日本電信電話株式会社：東京 2020 オリンピック・パラリンピック競技大会における NTT の貢献 https://group.ntt/jp/newsrelease/2021/10/21/211021a.html〔2022/5/11 確認〕
※ 148 外務省：2020 年東京オリンピック・パラリンピック競技大会に向けた外務省の取り組み https://www.mofa.go.jp/mofaj/p_pd/ep/page24_000800.html#section10〔2022/5/11 確認〕
※ 149 外務省：第２回日米豪印首脳会合 https://www.mofa.go.jp/mofaj/fp/nsp/page4_005424.html〔2022/5/11 確認〕
※ 150 外務省：サイバーセキュリティに関する国連政府専門家会合最終会合における報告書の採択 https://www.mofa.go.jp/mofaj/press/release/press24_000114.html〔2022/5/11 確認〕
※ 151 外務省：サイバー行動に適用される国際法に関する日本政府の基本的な立場について https://www.mofa.go.jp/mofaj/gaiko/page3_003059.html〔2022/5/11 確認〕
※ 152 外務省：第６回日英サイバー協議の開催 https://www.mofa.go.jp/mofaj/press/release/press3_000511.html〔2022/5/11 確認〕
※ 153 外務省：第４回日エストニア・サイバー協議の開催 https://www.mofa.go.jp/mofaj/erp/we/page24_001587.html〔2022/5/11 確認〕
※ 154 外務省：日米安全保障協議委員会（日米「２＋２」）（結果）

https://www.mofa.go.jp/mofaj/na/st/page1_000942.html〔2022/5/11 確認〕
※ 155 外務省：日米安全保障協議委員会（日米「2＋2」）（概要）https://www.mofa.go.jp/mofaj/na/st/page4_005483.html〔2022/5/11 確認〕
※ 156 外務省：日米首脳会談 https://www.mofa.go.jp/mofaj/na/na1/us/page1_000951.html〔2022/5/11 確認〕
※ 157 外務省：日米首脳テレビ会談 https://www.mofa.go.jp/mofaj/na/na1/page1_001086.html〔2022/5/11 確認〕
※ 158 外務省：第 27 回日 EU 定期首脳協議（概要） https://www.mofa.go.jp/mofaj/erp/ep/page6_000563.html〔2022/5/11 確認〕
※ 159 外務省：第 24 回日 ASEAN 首脳会議 https://www.mofa.go.jp/mofaj/area/asean/page3_003142.html〔2022/5/11 確認〕
※ 160 http://aseanregionalforum.asean.org/〔2022/5/11 確認〕
※ 161 外務省：サイバーセキュリティに関する第 3 回 ARF 会期間会合の開催（結果） https://www.mofa.go.jp/mofaj/press/release/press1_000518.html〔2022/5/11 確認〕
※ 162 経済産業省：第 14 回 日・ASEAN サイバーセキュリティ政策会議を開催しました https://www.meti.go.jp/press/2021/10/20211022006/20211022006.html〔2022/5/11 確認〕
※ 163 経産省：「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク」を実施しました https://www.meti.go.jp/press/2021/11/20211101001/20211101001.html〔2022/5/11 確認〕
※ 164 The MITRE Corporation（https://www.mitre.org/〔2022/5/11 確認〕）は 1958 年創立の非営利民間企業で、米国連邦政府機関の出資を受けた研究開発、及び成果の民間移転を推進している。
※ 165 サイバーセキュリティ国際シンポジウム事務局：第 11 回サイバーセキュリティ国際シンポジウム https://symp.cysec-lab.keio.ac.jp/2021oct/index-j.html〔2022/5/11 確認〕
※ 166 株式会社日本経済新聞社・株式会社日経ビーピー：サイバー・イニシアチブ東京 2021 https://project.nikkeibp.co.jp/event/2021z1129cit/〔2022/5/11 確認〕
※ 167 Australian Government：Launch of Australia's International Cyber and Critical Technology Engagement Strategy https://www.internationalcybertech.gov.au/launch-of-australias-international-cyber-critical-tech-strategy〔2022/5/10 確認〕
※ 168 DPMC：New Zealand's Cyber Security Emergency Response Plan https://dpmc.govt.nz/publications/new-zealands-cyber-security-emergency-response-plan〔2022/5/10 確認〕
※ 169 CSA：The Singapore Cybersecurity Strategy 2021 https://www.csa.gov.sg/sgcybersecuritystrategy2021〔2022/5/10 確認〕
※ 170 APNIC：How can organizations support cybersecurity in the Pacific? https://blog.apnic.net/2021/07/29/how-can-organizations-support-cybersecurity-in-the-pacific/〔2022/5/10 確認〕
※ 171 PaCSON：Annual Report 2020 https://pacson.org/sites/default/files/2021-12/PaCSON%202020%20Annual%20report.pdf〔2022/5/10 確認〕
※ 172 Ministry of Digital Economy and Society：https://www.mdes.go.th/news/detail/4583〔2022/5/10 確認〕
上記では、Web ページのタイトルがタイ語のため省略している。
※ 173 National News Bureau of Thailand：Thailand's Cyber Security Agency Will Develop Security Skills in 7 Sectors https://thainews.prd.go.th/en/news/detail/TCATG210917142334222〔2022/5/10 確認〕
※ 174 https://www.apcert.org/〔2022/5/10 確認〕
※ 175 APCERT：TSUBAME Working Group https://www.apcert.org/about/structure/tsubame-wg/index.html〔2022/5/10 確認〕
※ 176 APCERT：APCERT CYBER DRILL 2021 "SUPPLY CHAIN ATTACK THROUGH SPEAR-PHISHING - BEWARE OF WORKING FROM HOME -" https://www.apcert.org/documents/pdf/APCERT_Drill2021_Press%20Release.pdf〔2022/5/10 確認〕
※ 177 APCERT：Documents https://www.apcert.org/documents/index.html〔2022/5/10 確認〕
※ 178 https://www.cybersecurity.my/en/index.html〔2022/5/10 確認〕
※ 179 https://www.cert.org.cn/publish/english/index.html〔2022/5/10 確認〕
※ 180 (ISC)²：(ISC)² Cybersecurity Workforce Study Sheds New Light on Global Talent Demand Amid a Lingering Pandemic https://www.isc2.org/News-and-Events/Press-Room/Posts/2021/10/26/ISC2-Cybersecurity-Workforce-Study-Sheds-New-Light-on-Global-Talent-Demand〔2022/5/12 確認〕
※ 181 https://www.nri-secure.co.jp/download/insight2021-report〔2022/5/12 確認〕
※ 182 Gartner, Inc.：The Rise of Business Technologists https://www.gartner.com/en/articles/the-rise-of-business-technologists〔2022/5/12 確認〕
※ 183 https://www.meti.go.jp/press/2021/04/20210426002/20210426002-1.pdf〔2022/5/12 確認〕
※ 184 業務によりセキュリティ関連のタスクの占める割合は様々と考えられる。
※ 185 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/007_03_00.pdf〔2022/5/12 確認〕
※ 186 NISC：プラス・セキュリティ知識 https://security-portal.nisc.go.jp/dx/plussecurity.html〔2022/5/12 確認〕
※ 187 https://www.meti.go.jp/shingikai/mono_info_service/digital_jinzai/pdf/005_03_01.pdf〔2022/5/12 確認〕
※ 188 経済産業省：デジタル人材育成プラットフォーム「マナビ DX」を開設しました! https://www.meti.go.jp/press/2021/03/20220329002/20220329002.html〔2022/5/12 確認〕
※ 189 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/008_03_00.pdf〔2022/5/12 確認〕
※ 190 重要インフラ：他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもので、重要インフラ分野として指定する分野。具体的には、「情報通信」「金融」「航空」「空港」「鉄道」「電力」「ガス」「政府・行政サービス（地方公共団体を含む）」「医療」「水道」「物流」「化学」「クレジット」及び「石油」の 14 分野。
NISC：重要インフラの情報セキュリティ対策に係る第4次行動計画 https://www.nisc.go.jp/pdf/policy/infra/infra_rt4.pdf〔2022/5/10 確認〕
※ 191 IPA：「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク」を実施しました https://www.ipa.go.jp/icscoe/news_all/news20211101.html〔2022/5/10 確認〕
※ 192 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〔2022/5/10 確認〕
※ 193 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〔2022/5/10 確認〕
※ 194 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/2021.html〔2022/5/10 確認〕
※ 195 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/2021.html〔2022/5/10 確認〕
※ 196 IPA：戦略マネジメント系セミナー https://www.ipa.go.jp/icscoe/program/middle/strategic_management/2021.html〔2022/5/10 確認〕
※ 197 IPA：実務者向けプログラム 制御システム向けサイバーセキュリティ演習 https://www.ipa.go.jp/icscoe/program/short/icssec/2021.html〔2022/5/10 確認〕
※ 198 IPA：実務者向けプログラム ERAB サイバーセキュリティトレーニング https://www.ipa.go.jp/icscoe/program/short/erab/2021.html〔2022/5/10 確認〕
※ 199 https://www.meti.go.jp/press/2019/12/20191227004/20191227004-1.pdf〔2022/5/10 確認〕
※ 200 CBT（Computer Based Testing）方式：試験会場に設置されたコンピュータを利用して実施する試験方式のこと。受験者はコンピュータに表示された試験問題に対して、マウスやキーボードを用いて解答する。
※ 201 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 3 年度試験 全試験区分版 https://www.jitec.ipa.go.jp/1_07toukei/toukei_r03.pdf〔2022/5/17 確認〕
※ 202 IPA：国家資格「情報処理安全確保支援士」2022 年 4 月 1 日付登録者 1,016 名の内訳を公開しました https://www.ipa.go.jp/siensi/data/20220401newriss.html〔2022/5/17 確認〕
※ 203 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〔2022/5/17 確認〕
※ 204 経済産業省：情報処理安全確保支援士特定講習 https://www.meti.go.jp/policy/it_policy/jinzai/tokutei.html〔2022/5/17 確認〕
※ 205 IPA:セキュリティ・キャンプ全国大会 2022 オンライン 前回レポート https://www.ipa.go.jp/jinzai/camp/2022/zenkoku2022_report.html〔2022/5/12 確認〕
※ 206 IPA：セキュリティ・ネクストキャンプ 2021 オンライン 応募要項 https://www.ipa.go.jp/jinzai/camp/2021/next2021_vote.html〔2022/5/12 確認〕
※ 207 一般社団法人セキュリティ・キャンプ協議会事務局：セキュリティ・ミニキャンプ オンライン 2021 https://www.security-camp.or.jp/

minicamp/online2021.html〔2022/5/12 確認〕
※ 208 一般社団法人セキュリティ・キャンプ協議会事務局：セキュリティ・ミニキャンプ in 山梨 2021 https://www.security-camp.or.jp/minicamp/yamanashi2021.html〔2022/5/12 確認〕
一般社団法人セキュリティ・キャンプ協議会事務局：セキュリティ・ミニキャンプ in 広島 2021 https://www.security-camp.or.jp/minicamp/hiroshima2021.html〔2022/5/12 確認〕
一般社団法人セキュリティ・キャンプ協議会事務局：セキュリティ・ミニキャンプ in 大阪 2022 https://www.security-camp.or.jp/minicamp/osaka2022.html〔2022/5/12 確認〕
※ 209 一般社団法人セキュリティ・キャンプ協議会事務局（Twitter アカウント）：https://twitter.com/security_camp/status/1483243001359265794?cxt=HHwWhMDTudbpxJUpAAAA〔2022/5/12 確認〕
一般社団法人セキュリティ・キャンプ協議会事務局：GCC 2022 Taiwan - Global Cybersecurity Camp 2022 Taiwan https://www.security-camp.or.jp/event/gcc_online2022.html〔2022/5/12 確認〕
※ 210 Asian Cyber Security Challenge 2021：https://acsc.asia〔2022/5/12 確認〕
一般社団法人セキュリティ・キャンプ協議会事務局：ACSC 2021 - Asian Cyber Security Challenge 2021 https://www.security-camp.or.jp/event/acsc2021.html〔2022/5/12 確認〕
※ 211 International Cybersecurity Challenge：https://ecsc.eu/icc/〔2022/5/12 確認〕
※ 212 大阪大学大学院情報科学研究科 enPiT 事務局：［文部科学省］成長分野を支える情報技術人材の育成拠点の形成（enPiT） https://www.enpit.jp/〔2022/5/12 確認〕
※ 213 SecCap 事務局：SecCap について https://www.seccap.jp/gs/about/〔2022/5/12 確認〕
※ 214 大阪大学大学院情報科学研究科 enPiT 事務局：セキュリティ分野 https://www.enpit.jp/fields/security/index.html〔2022/5/12 確認〕
※ 215 Basic SecCap コンソーシアム：Basic SecCap コース https://www.seccap.jp/basic/pdf/BasicSecCap_pamph.pdf〔2022/5/12 確認〕
※ 216 enPiT Pro Security：https://www.seccap.pro〔2022/5/12 確認〕
※ 217 大阪大学：安全なデータ利活用のためのプロフェッショナル人材育成コース https://cy2sec.comm.eng.osaka-u.ac.jp/miyaji-lab/pro-sec/index-jp.html〔2022/5/12 確認〕
※ 218 SECCON：SECCON 実行委員会／WG メンバー https://www.seccon.jp/2021/seccon/executivecommittee.html〔2022/5/12 確認〕
※ 219 SECCON：SECCON と は https://www.seccon.jp/2021/seccon/about.html〔2022/5/12 確認〕
※ 220 SECCON：SECCON 2021 開催スケジュール https://www.seccon.jp/2021/seccon/schedule.html〔2022/5/12 確認〕
※ 221 SECCON：SECCON 2021 電脳会議 https://www.seccon.jp/2021/ep211218.html〔2022/5/12 確認〕
※ 222 SECCON：第 4 回 SECCON Beginners CTF（5 月 22 日）開催終了しました https://www.seccon.jp/2021/seccon_beginners/_seccon_beginners_ctf_2021.html〔2022/5/12 確認〕
※ 223 CTF for GIRLS：第 16 回 CTF for GIRLS ワークショップ開催レポート http://girls.seccon.jp/news24.html〔2022/5/12 確認〕
※ 224 CTF for GIRLS：第 17 回 CTF for GIRLS ワークショップ開催レポート http://girls.seccon.jp/news25.html〔2022/5/12 確認〕
※ 225 CTF for GIRLS：第 18 回 CTF for GIRLS（ワークショップ）開催のご案内 http://girls.seccon.jp/news0.html〔2022/5/12 確認〕
※ 226 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：インターンシップ募集 https://www.jnsa.org/internship/index.html#jnsainternship〔2022/5/12 確認〕
※ 227 東京工業大学：カリキュラム概要 https://www.academy.titech.ac.jp/cumot/cy/schedule.html〔2022/5/12 確認〕
※ 228 独立行政法人国立高等専門学校機構：TOPICS & NEWS https://k-sec.kochi-ct.ac.jp/topics-news/info-1.html〔2022/5/12 確認〕
※ 229 経済産業省：サイバーセキュリティ経営ガイドラインと支援ツール https://www.meti.go.jp/policy/netsecurity/mng_guide.html〔2022/5/12 確認〕
※ 230 https://www.ipa.go.jp/security/vuln/10threats2022.html〔2022/5/19 確認〕
※ 231 NRI セキュア社：NRI Secure Insight 2020 https://www.nri-secure.co.jp/download/insight2020-report〔2022/5/19 確認〕
※ 232 https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf〔2022/5/17 確認〕
※ 233 IPA：「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」について https://www.ipa.go.jp/security/fy2021/reports/sme/index.html〔2022/5/17 確認〕
※ 234 IPA：サイバーセキュリティお助け隊（令和 2 年度中小企業向けサイバーセキュリティ対策支援体制構築事業）の報告書について https://www.ipa.go.jp/security/fy2020/reports/sme/otasuketai_houkoku.html〔2022/5/17 確認〕
※ 235 https://www.ipa.go.jp/security/sc3/〔2022/5/17 確認〕
※ 236 https://www.ipa.go.jp/security/sc3/about/〔2022/5/17 確認〕
※ 237 https://www.ipa.go.jp/files/000092713.pdf〔2022/5/17 確認〕
※ 238 https://www.ipa.go.jp/security/security-action/〔2022/5/17 確認〕
※ 239 https://www.tokyo-cci.or.jp/hajimete-it/security/〔2022/5/17 確認〕
※ 240 https://www.tokyo-cci.or.jp/page.jsp?id=1025418〔2022/5/17 確認〕
※ 241 https://school-security.jp/pdf/2020.pdf〔2022/5/17 確認〕
※ 242 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。
※ 243 https://www.mext.go.jp/content/20220303-mxt_shuukyo01-100003157_005.pdf〔2022/5/17 確認〕
※ 244 文部科学省：GIGA スクール構想の実現へ https://www.mext.go.jp/content/20200625-mxt_syoto01-000003278_1.pdf〔2022/5/17 確認〕
※ 245 内閣府：GIGA スクール構想の実現ロードマップ https://www5.cao.go.jp/keizai-shimon/kaigi/special/reform/committee/20200323/shiryou3_1_1.pdf〔2022/5/17 確認〕
※ 246 文部科学省：GIGA スクール構想の実現 https://www.mext.go.jp/content/20210118-mxt_jogai01-000011648_001.pdf〔2022/5/17 確認〕
文部科学省：令和 2 年度第 3 次補正予算案への対応について https://www.mext.go.jp/content/000091784.pdf〔2022/5/17 確認〕
※ 247 文部科学省：「教育情報セキュリティポリシーガイドライン」の第 2 回改訂に関する説明資料 令和 3 年 5 月改訂 https://www.mext.go.jp/content/20210528-mxt_jogai02-000011648_001.pdf〔2022/5/17 確認〕
※ 248 https://www.mext.go.jp/content/20210630-mxt_jogai02-000011648_052.pdf〔2022/5/17 確認〕
※ 249 ローカルブレイクアウト：WAN のトラフィック負荷軽減のために各拠点のルータなどが特定クラウドサービスについて拠点間の回線網を迂回して直接インターネットへアクセスさせる仕組み。
※ 250 デジタル庁：「デジタル社会の実現に向けた重点計画」が閣議決定されました 公開日：2021 年 12 月 24 日 https://www.digital.go.jp/posts/79b7ZMv1〔2022/5/17 確認〕
※ 251 文部科学省：教育情報セキュリティポリシーに関するガイドライン（令和 4 年 3 月） https://www.mext.go.jp/content/20220304-mxt_shuukyo01-100003157_1.pdf〔2022/5/17 確認〕
※ 252 https://www.mext.go.jp/content/20220303-mxt_shuukyo01-100003157_003.pdf〔2022/5/17 確認〕
※ 253 リスクベース認証：システムへの接続において場所や時間等が通常と異なる場合等に ID・パスワードだけでなく追加の認証を行う方式。
※ 254 ふるまい検知：通信内容等の監視対象の「動き」を分析し、異常、あるいは不審な挙動を検知する仕組み。
※ 255 https://www.soumu.go.jp/main_content/000762715.pdf〔2022/5/17 確認〕
※ 256 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）～ https://www.soumu.go.jp/main_content/000768078.pdf〔2022/5/17 確認〕
※ 257 IPA:「2021 年度情報セキュリティに対する意識調査【倫理編】【脅威編】」報告書 https://www.ipa.go.jp/security/economics/ishikichousa2021.html〔2022/5/17 確認〕
※ 258 2020 年度調査まではスマートデバイス（タブレット及びスマートフォン）利用者を対象としていたが、2021 年度調査からスマートフォン利用者のみを対象にした。
※ 259 対策を「1 年以上前から実施している」「1 年以内に実施し始めた」の総和。
※ 260 IPA：2021 年度 情報セキュリティの倫理と脅威に対する意識調査 -【脅威編】- https://www.ipa.go.jp/files/000096683.pdf〔2022/5/17 確認〕
※ 261 事前調査において、プライベートにおけるパソコン、スマートフォンの利用状況を尋ね、インターネットでパソコンを使用していないと回答した者。
※ 262 事前調査において、プライベートにおいてパソコン、スマートフォンの両方を使用している場合、それぞれの機器の 1 日の利用時間を尋ね、利用時間が長い方の機器で回答者を分類した。
※ 263 「情報セキュリティに対する意識調査」では職業従事者の区分で

ある「会社員」「公務員・団体職員」「教職員」「契約・派遣社員」「自営業・自由業・フリーランス」について、同じ区分であっても職務の分野によって結果に差が出ると想定し、「情報システムや通信関係などIT関連業務に従事、関与」している人としていない人とを分類して集計している。
※264 総務省：オンライン消費の増加　https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd121310.html〔2022/5/17確認〕
※265 総務省統計局：新型コロナウイルス感染症で変わるネットショッピング―家計消費状況調査の結果から―　https://www.stat.go.jp/info/today/162.html〔2022/5/17確認〕
※266 独立行政法人国民生活センター：2020年度にみる60歳以上の消費者トラブル―コロナ禍で、通信販売の相談件数は過去最高に―　https://www.kokusen.go.jp/news/data/n-20210902_1.html〔2022/5/17確認〕
※267 独立行政法人国民生活センター：「解約したはず!」「契約してない!」と思い込んでいませんか?予期せぬ“サブスク”の請求トラブルに注意!　https://www.kokusen.go.jp/pdf/n-20211007_1.pdf〔2022/5/17確認〕
※268 https://www.caa.go.jp/policies/policy/consumer_transaction/specified_commercial_transactions/assets/consumer_transaction_cms202_220209_07.pdf〔2022/5/17確認〕
※269 独立行政法人国民生活センター：【若者向け注意喚起シリーズ<No.3>】健康食品等の「定期購入」のトラブル―「お試し」「1回限り」のつもりが定期購入に!?―　https://www.kokusen.go.jp/news/data/n-20210617_1.html〔2022/5/17確認〕
※270 独立行政法人国民生活センター：【若者向け注意喚起シリーズ<No.3>】健康食品等の「定期購入」のトラブル-「お試し」「1回限り」のつもりが定期購入に!?-　https://www.kokusen.go.jp/pdf/n-20210617_1.pdf〔2022/5/17確認〕
※271 内閣府：ネット通販でトラブル急増!「お試し」のつもりが定期購入に!?　https://www.gov-online.go.jp/useful/article/202012/2.html〔2022/5/17確認〕
※272 https://www.pref.kyoto.jp/net_tv/cm/219.html〔2022/5/17確認〕
※273 内閣府：新たな手口のヤミ金融に注意!「#個人間融資」「給与ファクタリング」　https://www.gov-online.go.jp/useful/article/202103/4.html〔2022/5/17確認〕
※274 金融庁：SNS等を利用した「個人間融資」にご注意ください!　https://www.fsa.go.jp/ordinary/chuui/kinyu_chuui.html〔2022/5/17確認〕
※275 神奈川県：ヤミ金融にご注意を（ヤミ金融情報のページ）　https://www.pref.kanagawa.jp/docs/m6c/cnt/f646/p7876.html〔2022/5/17確認〕
※276 https://www.mext.go.jp/content/20211125-mxt_shuukyo01-000009827_001.pdf〔2022/5/17確認〕
※277 https://www.trendmicro.com/ja_jp/about/press-release/2021/pr-20210729-01.html〔2022/5/17確認〕
※278 https://www.mext.go.jp/content/20210312-mxt_jogai01-000011649_002.pdf〔2022/5/17確認〕
※279 https://www.mext.go.jp/studxstyle/〔2022/5/17確認〕
※280 https://www.ipa.go.jp/files/000088916.pdf〔2022/5/17確認〕
※281 https://twitter.com/moj_jinken/status/1465938718393573378〔2022/5/17確認〕
※282 石川県：「Stop! コロナ差別!」～ネット上の誹謗中傷は許されません～　https://www.pref.ishikawa.lg.jp/soumu/jinken/corona_jinken_monitor.html〔2022/5/17確認〕
※283 和歌山県：新型コロナ誹謗中傷対策条例を施行しました　https://www.pref.wakayama.lg.jp/prefg/021400/d00206062_d/fil/leaflet.pdf〔2022/5/17確認〕
※284 防衛省・自衛隊（Twitterアカウント）：https://twitter.com/modjapan_jp/status/1402589334386008069〔2022/5/17確認〕
※285 独立行政法人国民生活センター：「新型コロナ関連詐欺　消費者ホットライン」をご利用ください　https://www.kokusen.go.jp/info/data/coronavirus_vshotline.html〔2022/5/17確認〕
※286 厚生労働省:新型コロナウイルス感染症に関して厚生労働省を装った詐欺にご注意ください。　https://www.mhlw.go.jp/stf/seisakunitsuite/newpage_00004.html〔2022/5/17確認〕
※287 時事ドットコムニュース：SNS「1500人のぞいた」　不正アクセス容疑で男逮捕―愛知県警　https://www.jiji.com/jc/article?k=2022010601107&g=soc〔2022/5/17確認〕
※288 https://blog.twitter.com/ja_jp/topics/company/2021/playbook-for-safety〔2022/5/17確認〕
※289 Meta Platforms, Inc.：Instagramの安全とセキュリティを確保する　https://about.instagram.com/ja-jp/blog/announcements/keeping-instagram-safe-and-secure〔2022/5/17確認〕
※290 Meta Platforms, Inc.：Instagramコミュニティを不適切なコンテンツから守るための新たな方法　https://about.instagram.com/ja-jp/blog/announcements/introducing-new-ways-to-protect-our-community-from-abuse〔2022/5/17確認〕
※291 Meta Platforms, Inc.:若い利用者のために、安全性とプライバシーを強化したエクスペリエンスを提供　https://about.instagram.com/ja-jp/blog/announcements/giving-young-people-a-safer-more-private-experience〔2022/5/17確認〕
※292 Google LLC：日本版YouTube公式ブログ　https://youtube-jp.googleblog.com/2021/11/youtube.html〔2022/5/17確認〕
※293 ヤフー株式会社：Yahoo! ニュース、コメント欄をより健全化するためユーザーからの違反コメント報告を促進　https://about.yahoo.co.jp/pr/release/2021/12/22b/〔2022/5/17確認〕
※294 独立行政法人国民生活センター：狙われる!? 18歳・19歳「金」と「美」の消費者トラブルに気をつけて!　https://www.kokusen.go.jp/pdf/n-20210408_1.pdf〔2022/5/17確認〕
※295 https://www.caa.go.jp/policies/policy/consumer_education/consumer_education/lower_the_age_of_adulthood/〔2022/5/17確認〕
※296 https://www.soumu.go.jp/use_the_internet_wisely/trouble/reference/reference02.html〔2022/5/17確認〕
※297 https://seinen.go.jp/〔2022/5/17確認〕
※298 https://smart18.info/files/smart18ebook.pdf〔2022/5/17確認〕
※299 MATAGI SNIPERS：https://matagi-snps.com/〔2022/5/17確認〕
※300 funglr Games：社会人eスポーツリーグ「AFTER 6 LEAGUE」を経済産業省が後援決定　https://funglr.games/ja/news/a6l-meti-support/〔2022/5/17確認〕
※301 京都新聞：チート行為で男女5人書類送検　京都府警、ゲーム内のアイテム不正入手疑い　https://www.kyoto-np.co.jp/articles/-/713337〔2022/5/17確認〕
※302 福井県：「チート行為」はやめましょう!～損害賠償請求や違法行為として処罰される可能性も～　http://www.fukui-city.ed.jp/na-fuji-e/moraru/R2%20mararu20.pdf〔2022/5/17確認〕
※303 株式会社ラック：東京ゲームショウ2021 オンラインに出展!チート対策ホワイトペーパーも公開　https://www.lac.co.jp/lacwatch/service/20210910_002704.html〔2022/5/17確認〕
※304 https://www.nisc.go.jp/pdf/policy/kihon-s/set_20220318_cswebinarboshu_r10.pdf〔2022/5/17確認〕
※305 NISC：国際サイバーセキュリティワークショップ・演習の開催　https://www.nisc.go.jp/eng/pdf/international_ws_ttx_2022_jp.pdf〔2022/5/17確認〕
※306 https://www.gov-online.go.jp/pr/media/tv/kasumigaseki/movie/20220218.html〔2022/5/17確認〕
※307 https://dawn2021.orylab.com〔2022/5/17確認〕
※308 知的財産戦略本部：知的財産推進計画2021　https://www.kantei.go.jp/jp/singi/titeki2/kettei/chizaikeikaku20210713.pdf〔2022/5/19確認〕
※309 ISO：ISO/IEC JTC 1　https://www.iso.org/committee/45020.html〔2022/5/19確認〕
※310 JISC：JISCについて　http://www.jisc.go.jp/jisc/index.html〔2022/5/19確認〕
※311 ITU：SG17: Security　https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx〔2022/5/19確認〕
※312 IETF：The IETF Security Area　https://trac.ietf.org/trac/sec/wiki〔2022/5/19確認〕
※313 TCG：Welcome to Trusted Computing Group　https://trustedcomputinggroup.org/work-groups/regional-forums/japan〔2022/5/19確認〕
※314 https://www.jisc.go.jp/international/iso-prcs.html〔2022/5/19確認〕
※315 ガーブル回路：暗号学においてスクランブルされた回路を意味し、2者間の秘密計算を可能とする暗号プロトコル。
※316 TS（Technical Specification：技術仕様書）：現時点では技術的に未成熟等の理由により、国際標準として発行するのは妥当ではない文書。
※317 EUCC（European Union Cybersecurity Certification）：欧州で創立が進められている、ISO/IEC 15408に基づくIT製品のセキュリティ評価・認証制度。
※318 ENISA：CYBERSECURITY CERTIFICATION　https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1〔2022/5/25確認〕
※319 IoT推進コンソーシアム・総務省・経済産業省：IoTセキュリティ

ガイドライン Ver1.0　http://www.soumu.go.jp/main_content/000428393.pdf〔2022/5/24 確認〕
※ 320 https://www.iso.org/standard/80136.html〔2022/5/24 確認〕
※ 321 https://www.iso.org/standard/78572.html〔2022/5/24 確認〕
※ 322 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〔2022/5/24 確認〕
※ 323 https://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf〔2022/5/17 確認〕
※ 324 https://www.commoncriteriaportal.org/〔2022/5/17 確認〕
※ 325 IPA：認証プロテクションプロファイルリスト　https://www.ipa.go.jp/security/jisec/certified_pps/pp_list.html〔2022/5/17 確認〕
※ 326 プロテクションプロファイルに対しての認証：プロテクションプロファイルがコモンクライテリア形式を満たしていることの認証。
※ 327 https://csrc.nist.gov/projects/cryptographic-module-validation-program〔2022/5/30 確認〕
※ 328 https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline_honninkakunin_20190225.pdf〔2022/5/17 確認〕
※ 329 IPA・JISEC：「ハードコピーデバイスのプロテクションプロファイル」適合の申請案件についてのガイドライン 第 1.8 版　https://www.ipa.go.jp/security/jisec/mfp/guidelineforHCD-PP_1.8.pdf〔2022/5/17 確認〕
※ 330 https://www.ipa.go.jp/security/jisec/certified_pps/c0553/c0553_pp.pdf〔2022/5/17 確認〕
※ 331 IPA・JISEC：認証製品リスト　https://www.ipa.go.jp/security/jisec/certified_products/cert_listv31.html〔2022/5/17 確認〕
※ 332 JCMVP の「トピックス」ページ（https://www.ipa.go.jp/security/jcmvp/topics.html〔2022/5/17 確認〕）の「本制度に関連する日本産業規格 (JIS)」参照。
※ 333 JCMVP の「トピックス」ページ（https://www.ipa.go.jp/security/jcmvp/topics.html〔2022/5/17 確認〕）の「本制度に関連する ISO/IEC 規格」参照。
※ 334 JISC：意見受付公告（JIS）　https://www.jisc.go.jp/app/jis/general/GnrOpinionReceptionNoticeList?show〔2022/5/17 確認〕
※ 335 JISC：JIS の制定等のプロセスについて　https://www.jisc.go.jp/jis-act/cap_process.html〔2022/5/17 確認〕
※ 336 「FIPS 140」は暗号モジュールに関するセキュリティ要件を規定する連邦情報処理規格。「-2」は第 2 版、「-3」は第 3 版であることを示す。
※ 337 Historical List：認証の有効期間が満了した製品であることを示すリスト。
※ 338 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〔2022/5/17 確認〕
※ 339 サイバーセキュリティ対策推進会議・各府省情報化統括責任者（CIO）連絡会議：政府情報システムのためのセキュリティ評価制度（ISMAP）の暫定措置の見直しについて　https://www.nisc.go.jp/pdf/policy/general/ismap_minaoshi.pdf〔2022/5/17 確認〕
※ 340 https://cio.go.jp/sites/default/files/uploads/documents/cloud_policy_20210330.pdf〔2022/5/17 確認〕
※ 341 総務省・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〔2022/5/17 確認〕
※ 342 https://www.meti.go.jp/press/2019/01/20200130002/20200130002-1.pdf〔2022/5/17 確認〕
※ 343 https://www.nisc.go.jp/pdf/policy/general/wakugumi2021.pdf〔2022/5/17 確認〕
※ 344 NISC：「政府機関等のサイバーセキュリティ対策のための統一基準群」　https://www.nisc.go.jp/policy/group/general/kijun.html〔2022/5/17 確認〕
※ 345 https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005〔2022/5/17 確認〕
※ 346 https://www.ismap.go.jp〔2022/5/17 確認〕
※ 347 https://www.nisc.go.jp/pdf/policy/infra/shishin5.pdf〔2022/5/17 確認〕
※ 348 e-Gov 法令検索：個人情報の保護に関する法律　https://elaws.e-gov.go.jp/document?lawid=415AC0000000057〔2022/5/17 確認〕
※ 349 https://www.ppc.go.jp/files/pdf/151112_kaiseian.pdf〔2022/5/17 確認〕
※ 350 個人情報保護委員会：令和2年 改正個人情報保護法について　https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/〔2022/5/17 確認〕
※ 351 デジタル庁：デジタル社会の形成を図るための関係法律の整備に関する法律　https://cio.go.jp/sites/default/files/uploads/documents/digital/20210901_laws_r3_37_article.pdf〔2022/5/17 確認〕
※ 352 個人情報保護委員会：令和3年 改正個人情報保護法について（官民を通じた個人情報保護制度の見直し）　https://www.ppc.go.jp/personalinfo/minaoshi/〔2022/5/17 確認〕
※ 353 https://www.ipa.go.jp/files/000087025.pdf〔2022/5/17 確認〕
※ 354 https://www.ppc.go.jp/files/pdf/seibihou_gaiyou.pdf〔2022/5/17 確認〕
※ 355 内閣府：個人情報保護法制 2000 個問題について　https://www8.cao.go.jp/kisei-kaikaku/suishin/meeting/wg/toushi/20161115/161115toushi01.pdf〔2022/5/17 確認〕
※ 356 IPA：「企業における営業秘密管理に関する実態調査 2020」報告書について　https://www.ipa.go.jp/security/fy2020/reports/ts_kanri/index.html〔2022/5/17 確認〕
※ 357 IPA：組織における内部不正防止ガイドライン　https://www.ipa.go.jp/security/fy24/reports/insider/〔2022/5/17 確認〕
※ 358 https://www.ipa.go.jp/files/000097371.pdf〔2022/5/17 確認〕
※ 359 https://security-portal.nisc.go.jp/law_handbook/law_handbook.pdf〔2022/5/17 確認〕
※ 360 AES（Advanced Encryption Standard）：米国で NIST により標準化された共通鍵暗号。
※ 361 ChaCha:Daniel J. Bernstein によって開発されたストリーム暗号。Chacha20 は ChaCha を基にした暗号であり、これとメッセージ認証子である Poly1305 とを組み合わせた ChaCha20-Poly1305 は、CRYPTREC の推奨候補暗号リストとなっている。
※ 362 RSA：素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号。
※ 363 CRT-RSA 指数：RSA 暗号の復号時の計算量を下げる際に用いられる、秘密鍵に付随する付加情報。
※ 364 NIST：Third PQC Standardization Conference　https://csrc.nist.gov/Events/2021/third-pqc-standardization-conference〔2022/4/21 確認〕
※ 365 Anirban Chakraborty, Sarani Bhattacharya, Manaar Alam, SikharPatranabis and Debdeep Mukhopadhyay：RASSLE: Return Address Stack based Side-channel LEakage　https://tches.iacr.org/index.php/TCHES/article/view/8795〔2022/4/21 確認〕
※ 366 分岐予測：CPU において、条件分岐命令で分岐するかしないかを予測することによって、パイプライン処理の乱れを極力避けて処理速度の低下を抑えるための機構。
※ 367 投機的実行：CPU において命令を、必要な処理であることが確定する前にパイプラインに投入して実行を始める処理。パイプラインの乱れを極力避けることを目的とする。分岐予測が外れて必要でない処理であることが確定すると、その実行結果は破棄され、正しい分岐先の命令を改めて実行する。
※ 368 Spectre-v1 については、以下を参照。
CVE:CVE-2017-5753 Detail　https://cve.org/CVERecord?id=CVE-2017-5753〔2022/4/21 確認〕
Spectre-v2 については、以下を参照。
CVE:CVE-2017-5715 Detail　https://cve.org/CVERecord?id=CVE-2017-5715〔2022/4/21 確認〕
※ 369 タイミング攻撃：サイドチャネル情報のうち、処理時間の差異を利用する攻撃。
※ 370 ECDSA（Elliptic Curve Digital Signature Algorithm）：楕円曲線暗号を用いたデジタル署名アルゴリズム。
※ 371 テンプレート攻撃：暗号実装に対し、異なる入力値に対するサイドチャネル情報（消費電力、電磁場など）をあらかじめ測定しておき、それをテンプレートとして利用して実際の暗号鍵復元のための攻撃を行う手法。
※ 372 Alejandro Cabrera Aldaya and Billy Bob Brumley：Online Template Attacks: Revisited　https://tches.iacr.org/index.php/TCHES/article/view/8967〔2022/4/21 確認〕