第5節　サイバーセキュリティ政策の動向

1 概要

1 これまでの取組

世界的規模で深刻化するサイバーセキュリティ上の脅威の増大を背景として、我が国におけるサイバーセキュリティ政策の基本理念等を定めたサイバーセキュリティ基本法（平成26年法律第104号）が2014年（平成26年）に成立し、2015年（平成27年）、同法に基づき、サイバーセキュリティ政策に係る政府の司令塔として、内閣の下にサイバーセキュリティ戦略本部が新たに設置された。それ以降、経済社会の変化やサイバーセキュリティ上の脅威の増大などの状況変化も踏まえつつ、諸施策の目標及び実施方針を定める「サイバーセキュリティ戦略」が3年ごとに累次決定されており、2021年（令和3年）9月には新しい「サイバーセキュリティ戦略[*1]」が閣議決定された。これに基づきサイバーセキュリティ政策が推進されてきている。

重要インフラ防護に係る基本的な枠組を定めた「重要インフラのサイバーセキュリティに係る行動計画[*2]」（2022年（令和4年）6月サイバーセキュリティ戦略本部決定）において、情報通信分野（電気通信、放送及びケーブルテレビ）は、その機能が停止、又は利用不可能となった場合に国民生活・社会経済活動に多大なる影響を及ぼしかねないものとして重要インフラ14分野の一つに指定されている。重要インフラ所管省庁として、総務省において、引き続き情報通信ネットワークの安全性・信頼性の確保に向けた取組を推進することが必要とされている。

総務省では、2017年（平成29年）から、セキュリティ分野の有識者で構成される「サイバーセキュリティタスクフォース」を開催している。同タスクフォースでは、これまで、様々な状況変化や東京オリンピック・パラリンピック競技大会、新型コロナウイルス感染症への対応等も踏まえつつ、総務省として取り組むべき課題や施策を累次取りまとめてきたところであり、直近では、情報通信ネットワークの安全性・信頼性の確保やサイバー攻撃への自律的な対処能力の向上に向けた対策を盛り込んだ「ICTサイバーセキュリティ総合対策2022[*3]」を2022年（令和4年）8月に策定した。また、IoT機器を狙ったサイバー攻撃が多く発生している状況等に対応するため、2023年（令和5年）1月から、同タスクフォースの下に「情報通信ネットワークにおけるサイバーセキュリティ対策分科会」を開催し、現在の取組状況や課題を踏まえた上で、端末側（IoT機器）、ネットワーク側の双方から必要となる総合的な対策について検討している。これらを踏まえ、ICT分野におけるサイバーセキュリティ対策の推進に向け、諸施策に取り組んでいるところである。

2 今後の課題と方向性

新型コロナウイルス感染症の感染拡大防止のために人の移動が制限され、テレワーク活用などが進展するなど、国民による社会経済活動全般のデジタル化の推進、すなわち、社会全体のデジタル・トランスフォーメーション（DX）の推進が、より一層重要な政策課題と認識されるようになった。

＊1　サイバーセキュリティ戦略：https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021.pdf
＊2　重要インフラのサイバーセキュリティに係る行動計画：https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf
＊3　ICTサイバーセキュリティ総合対策2022：https://www.soumu.go.jp/main_content/000829941.pdf

また、近年、サイバー空間は、厳しい安全保障環境や地政学的緊張も反映しつつ国家間の争いの場となっており、各国では政府機関や重要インフラを狙ったサイバー攻撃が多く発生している。経済社会のデジタル化が広範かつ急速に進展する中、こうしたサイバー攻撃の増大により、情報通信ネットワークの機能停止や情報の漏洩等が生じると、国民の生活や我が国の経済社会活動に甚大な被害が発生するおそれがある。2022年（令和4年）12月には、我が国の国家安全保障戦略が改定され、サイバー安全保障分野における対応能力の向上のため「能動的サイバー防御」の導入が盛り込まれるなど、我が国のサイバーセキュリティ政策の転換点を迎えている。

サイバー空間が公共空間化する中で、IoTや5Gを含むICT（情報通信技術）に係るインフラやサービスは、その基盤となるものであり、社会全体のデジタル改革・DXを推進するためには、国民一人ひとりがその基盤となるICTを安心して活用できるよう、サイバーセキュリティを確保することが、いわば不可欠の前提としてますます重要になっている。

これらを踏まえ、以下で述べるとおり、情報通信ネットワークの安全性・信頼性の確保、サイバー攻撃への自律的な対処能力の向上、国際連携の推進、普及啓発の推進を行う必要がある。

2 情報通信ネットワークの安全性・信頼性の確保

1 IoTのセキュリティに関する取組

IoT化が進展し、社会・経済活動を支える様々なモノがインターネットにつながるなか、IoT機器は管理が行き届きにくい、機器の性能が限られ適切なセキュリティ対策ができないなどの理由から、サイバー攻撃の脅威にさらされることが多く、その対策強化の必要性が指摘されている。実際にIoT機器を悪用したサイバー攻撃が発生しているほか、NICTが運用するサイバー攻撃観測網（NICTER）が2022年（令和4年）に観測したサイバー攻撃関連通信についても、依然としてIoT機器（特にDVR/NVR）を狙ったものが最も多かったという結果が示されている。

こうした状況を踏まえ、IoT機器に対するサイバーセキュリティ対策を強化するため、2018年（平成30年）に情報通信研究機構法[*4]の一部改正を行った上で、総務省及びNICTでは、インターネット・サービス・プロバイダ（ISP）と連携し、2019年（平成31年）2月から「NOTICE（National Operation Towards IoT Clean Environment）」と呼ばれる取組を実施している。現行の取組では、①NICTがインターネット上のIoT機器に対して、例えば「password」や「123456」等の容易に推測されるパスワードを入力することなどにより、サイバー攻撃に悪用されるおそれのある機器を特定し、②特定した機器の情報をNICTからISPに通知し、③通知を受けたISPがその機器の利用者を特定し注意喚起を行う、という一連の取組を行っている。

また、NOTICEと並行して、2019年（令和元年）6月から、総務省、NICT、一般社団法人ICT-ISAC及びISP各社が連携して、既にマルウェアに感染しているIoT機器の利用者に対し、ISPが注意喚起を行う取組を実施している。この取組は、NICTが前述のNICTERで得られた情報を基にマルウェア感染を原因とする通信を行っている機器を検知し、ISPで当該機器の利用者を特定することにより行っている。

NOTICEの取組が2024年（令和6年）3月に期限を迎えることを踏まえ、情報通信ネットワークにおけるサイバーセキュリティ対策分科会において、NOTICEの現状や課題等について整理し、

＊4　国立研究開発法人情報通信研究機構法（平成11年法律第162号）

IoT機器を悪用したサイバー攻撃の脅威に対する観測能力の強化や効果的な対処の推進を含めた、今後のNOTICEの方向性について検討している。

関連データ

NOTICE及びNICTERに関する注意喚起の概要

URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/datashu.html#f00375（データ集）

2 電気通信事業者による積極的セキュリティ対策に関する取組

今後、5Gの進展により様々な産業でIoT機器の利用が更に拡大することが予想される中で、IoT機器のセキュリティ対策をより実効的なものにするためには、これまでの端末機器側の対策に加え、通信トラヒックが通過するネットワーク側でもより機動的な対処を行う環境整備が必要と考えられる*5。

このため、2022年度（令和4年度）からは、大規模化・巧妙化・複雑化するサイバー攻撃・脅威に電気通信事業者がより効率的・積極的に対処できるようにするため実施している、①C&Cサーバ検知技術の実証、②フィッシングサイト等の悪性Webサイトの検知技術・共有手法の実証、③ネットワークセキュリティ対策手法の導入に係る実証を2023年度（令和5年度）も引き続き実施するとともに、C&Cサーバの検知精度の向上・検知情報の共有・利活用等の推進や、IoTボットネットの全体像の可視化を含む、情報通信ネットワークにおけるサイバーセキュリティ対策分科会における議論も踏まえて、電気通信事業者等と連携しながら、持続可能な仕組を検討する。

そのほか、DDoS攻撃等のサイバー攻撃の送信元情報のISP間での共有や調査研究等の業務を行う第三者機関である「認定送信型対電気通信設備サイバー攻撃対処協会」*6における情報共有や分析について、その対象が、これまではサイバー攻撃が発生した場合にのみ限られていたが、攻撃の発生前になされる一定の予兆行為（ポートスキャン）が発生した場合も含まれることを内容とする電気通信事業法の一部を改正する法律が2022年（令和4年）6月に成立するなど、DDoS攻撃等のサイバー攻撃への対処における電気通信事業者間の連携促進を図っている*7。

3 サプライチェーンリスク対策に関する取組

総務省では、2019年度（平成31年度）から2021年度（令和3年度）にかけて5Gネットワークにおけるセキュリティ確保に向けた調査検討を実施している。仮想化基盤・管理系を含む5Gネットワーク全体を考慮した技術的検証を通じて、オペレータが留意すべきセキュリティ課題やその対策を整理し、2022年（令和4年）4月、その成果の一部として「5Gセキュリティガイドライン第1版*8」を公表した。同ガイドラインは、2022年（令和4年）9月、ITU-T SG17において新規作業項目として採用され、現在、専門機関と連携して国際標準化に向けた取組を推進している。

また、通信分野においては、システムに求められる機能の高度化、多様化に伴いシステムの構成が複雑化しており、多様な商用ソフトウェアやオープンソースソフトウェア（OSS）*9がソフト

＊5　2021年（令和3年）に策定した「ICTサイバーセキュリティ総合対策2021」では、「サイバー攻撃に対する電気通信事業者の積極的な対策の実現」として、「インターネット上でISPが管理する情報通信ネットワークにおいても高度かつ機動的な対処を実現するための方策の検討が必要」としている。（https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00192.html）
＊6　電気通信事業法第116の2条第1項に基づき、認定送信型対電気通信設備サイバー攻撃対処協会として、2019年（平成31年）1月に一般社団法人ICT-ISACが認定されている。
＊7　電気通信事業法の一部を改正する法律（令和4年法律第70号）は2023年（令和5年）6月16日に施行。
＊8　5Gセキュリティガイドライン第1版：https://www.soumu.go.jp/main_content/000812253.pdf
＊9　ソースコードが無償で公開され、誰でも利用や改良、再配布が可能なソフトウェア。

ウェア部品として利用されるようになっている。このようなソフトウェア・サプライチェーンの変化に伴い、ソフトウェア部品への悪意のあるコードの混入やソフトウェア部品の脆弱性を標的としたサイバー攻撃が発生しているが、システム内のソフトウェア部品の構成を把握できていない場合、攻撃に対して迅速に対応することが困難となる。

このような状況を踏まえ、総務省では、SBOM[*10]を活用したソフトウェア・サプライチェーンの把握によるサイバーセキュリティの強化に資するように、2023年度（令和5年度）から、通信分野におけるSBOMの導入に向けた実証事業を実施している。

さらに、2023年度（令和5年度）からは、スマートフォンが広く普及している一方で、スマートフォンアプリがユーザーの意図に反してユーザー情報を送信しているのではないかなどの懸念が生じた場合にその実態を確認する手法が限られている現状を踏まえ、第三者によるアプリの技術的解析等を通じたアプリ挙動の実態把握に係る実証事業を実施している。

4 トラストサービスに関する取組

Society5.0においては、実空間とサイバー空間が高度に融合することから、実空間における様々なやりとりをサイバー空間においても円滑に実現することが求められる。その実現のためには、データを安全・安心に流通できる基盤の構築が不可欠であり、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であるトラストサービス（**図表5-5-2-1**）の重要性が高まっている。

政府全体としては、デジタル社会推進会議令（令和3年政令第193号）に基づく「データ戦略推進ワーキンググループ」の下で、官民の様々な手続や取引についてデジタル化のニーズや必要なアシュアランスレベルの検討を行う「トラストを確保したDX推進サブワーキンググループ」が2021年（令和3年）11月に立ち上げられ、2022年（令和4年）7月に「トラストを確保したDX推進サブワーキンググループ報告書[*11]」を公表した。

総務省においては、2020年（令和2年）2月に公表された「トラストサービス検討ワーキンググループ」の最終取りまとめ[*12]を踏まえ、タイムスタンプとeシールについて、必要な制度整備や指針策定に向けた検討を進めている。

ア　国によるタイムスタンプ認定制度の整備

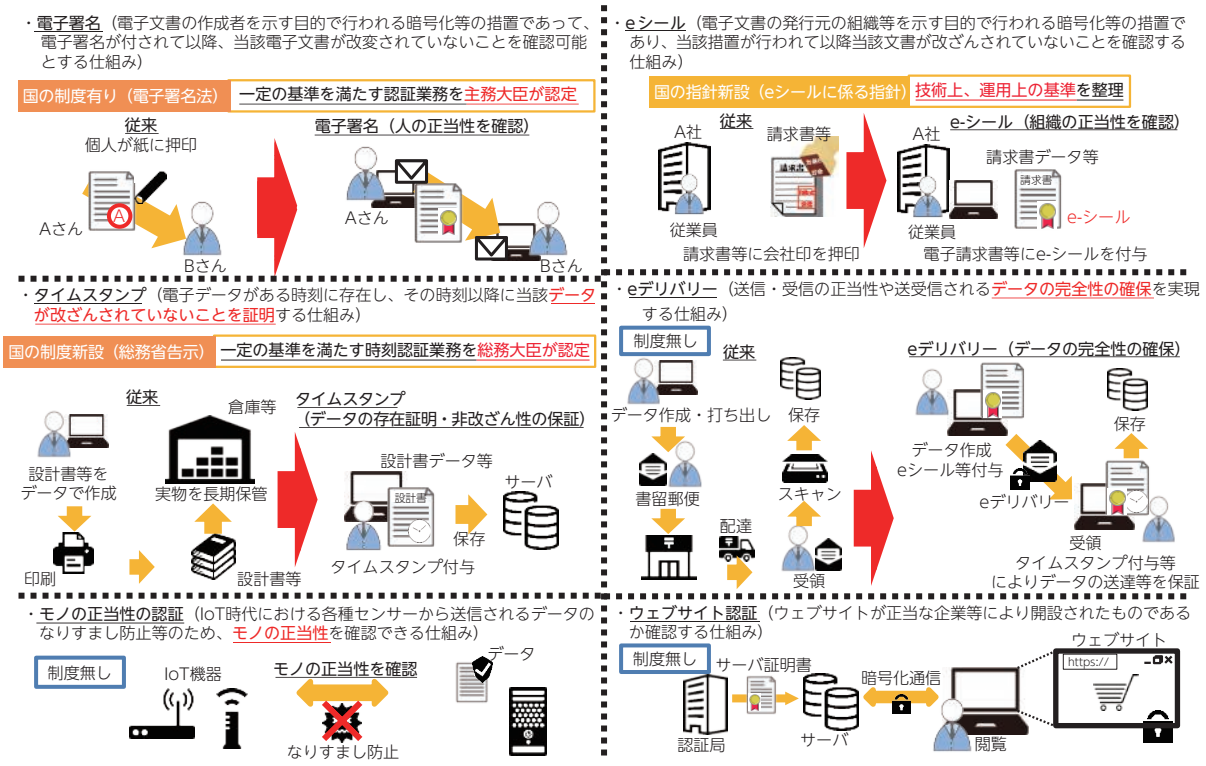
タイムスタンプについては、2020年（令和2年）3月に立ち上げた「タイムスタンプ認定制度に関する検討会」で更なる検討を行い、2021年（令和3年）4月に、時刻認証業務の認定に関する規程（令和3年総務省告示第146号）を制定し、国（総務大臣）による認定制度を整備した。さらに、2022年度（令和4年度）の税制改正により、税務関係書類に係るスキャナ保存制度等について、民間（一般財団法人日本データ通信協会）による認定制度に基づくタイムスタンプに代わり、国による認定制度に基づくタイムスタンプを位置付けることとされた[*13]。その後、2023年（令和5年）2月、初めての国による時刻認証業務の認定を行った。今後も引き続き、国による認定制度を適切かつ確実に運用するとともに、タイムスタンプの利用の一層の拡大に向け、必要な取組を行う。

＊10 Software Bill of Materials. ソフトウェア部品構成表。
＊11 トラストを確保したDX推進サブワーキンググループ報告書（https://www.digital.go.jp/councils/trust-dx-sub-wg/）
＊12 トラストサービス検討ワーキンググループ最終とりまとめ https://www.soumu.go.jp/main_content/000668595.pdf
＊13 2022年（令和4年）4月1日から2023年（令和5年）7月29日までの間は、従前どおり一般財団法人日本データ通信協会が認定する業務に係るタイムスタンプを付すことを可能とする経過措置が講じられる。

イ　「eシールに関する指針」の策定

eシールについては、2020年（令和2年）4月に立ち上げた「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」において、我が国におけるeシールの在り方などについて検討を行った。その後、2021年（令和3年）6月に検討会の取りまとめを公表するとともに、我が国のeシールにおける信頼の置けるサービス・事業者に求められる技術上・運用上の基準などについて整理した「eシールに係る指針[*14]」を策定した。

図表5-5-2-1　トラストサービスのイメージ



5　クラウドサービスの安全性確保に関する取組

ア　政府情報システムにおけるクラウドサービスの安全性評価

政府では、クラウド・バイ・デフォルト原則の下、クラウドサービスの安全性評価について、「クラウドサービスの安全性評価に関する検討会」で検討を行い、「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」（令和2年1月30日サイバーセキュリティ戦略本部決定）で、制度の①基本的枠組、②各政府機関等における利用の考え方、③所管と運用体制が決定された。

基本的枠組を受け、2020年（令和2年）6月、有識者と制度所管省庁（内閣サイバーセキュリティセンター・デジタル庁・総務省・経済産業省）を構成員とするISMAP運営委員会で決定した各種規程等に基づき、「政府情報システムのためのセキュリティ評価制度」（英語名：Information system Security Management and Assessment Program（ISMAP））が立ち上げられた。2021年（令和3年）3月から、この制度で定められた基準に基づいた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の登録が始まり、2023年（令和5年）5月11日現在、

＊14　eシールに係る指針（https://www.soumu.go.jp/main_content/000756907.pdf）

合計44サービスがISMAPクラウドサービスリスト[*15]として公開されている。

2022年（令和4年）11月には、主に機密性2情報を扱うSaaSのうち、セキュリティ上のリスクの小さな業務・情報の処理に用いるものに対する仕組として、ISMAP for Low-Impact Use（通称：ISMAP-LIU）の運用を開始した。ISMAP-LIUは、SaaSのうち用途や機能が極めて限定的なサービスや、比較的重要度が低い情報のみを取り扱うサービスについて、監査全体として現行ISMAPよりも緩やかな設計とした仕組であり、ISMAPとともに、クラウド・バイ・デフォルトの更なる拡大を推進していく。

イ　クラウドセキュリティに関するガイドラインの策定

総務省では、安全・安心なクラウドサービスの利活用推進のための取組として、クラウドサービス事業者における情報セキュリティ対策を取りまとめた「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」を策定しており、2021年（令和3年）9月には、クラウドサービスの提供・利用実態等を踏まえた改定版（第3版）を公表している。また、昨今では、クラウドサービス利用者が適切にクラウドサービスを利用できていないことに起因し、結果的に情報流出のおそれに至る事案も発生していることから、利用者の適切なクラウドサービスの利用促進について、提供者・利用者を含む幅広い主体で検討した上で、2022年（令和4年）10月、「クラウドサービス利用・提供における適切な設定のためのガイドライン」として策定・公表した。

3　サイバー攻撃への自律的な対処能力の向上

1　セキュリティ人材の育成に関する取組

サイバー攻撃が巧妙化・複雑化している一方で、我が国のサイバーセキュリティ人材は質的にも量的にも不足しており、その育成は喫緊の課題である。このため、総務省では、NICTの「ナショナルサイバートレーニングセンター」を通じて、サイバーセキュリティ人材育成の取組（CYDER、CIDLE及びSecHack365）を積極的に推進している。

ア　情報システム担当者等を対象とした実践的サイバー防御演習（CYDER）

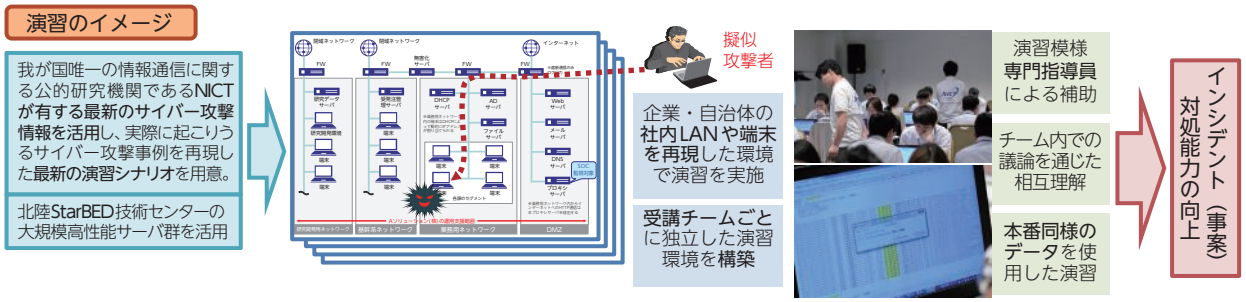
CYDERは、国の機関、地方公共団体、独立行政法人及び重要インフラ事業者などの情報システム担当者等を対象とした実践的サイバー防御演習である。受講者は、チーム単位で演習に参加し、組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って、インシデントの検知から対応、報告、回復まで、サイバー攻撃への一連の対処方法を体験する（図表5-5-3-1）。

2022年度（令和4年度）は、従来から実施している初級・中級・準上級の集合演習コース及びオンライン標準コースに加え、インシデント対応の「はじめの一歩」を学べるオンライン入門コースを新たに実施するとともに、地理的・時間的要因による地方公共団体の未受講解消のためにNICTが現地まで赴く「出前CYDER」、複数会場を結んで同時開催することで講師・スタッフの効率化を図る「CYDERサテライト」を実施した（図表5-5-3-2）。

CYDER集合演習の受講者は、2017年度（平成29年度）からの合計で1万7千人超となった。

＊15 ISMAPクラウドサービスリスト：https://www.ismap.go.jp/csm?id=cloud_service_list

図表5-5-3-1　実践的サイバー防御演習（CYDER：CYber Defense Exercise with Recurrence）



図表5-5-3-2　2022年度CYDER実施状況

コース名	演習方法	レベル	受講想定者（習得内容）	受講想定組織	開催地	開催回数	実施時期
A	集合演習	初級	システムに携わり始めた者（事案発生時の対応の流れ）	全組織共通	47都道府県 ※出前、サテライト形式も試行	72回	7月～翌年2月
B-1		中級	システム管理者・運用者（主体的な事案対応・セキュリティ管理）	地方公共団体	全国11地域	20回	10月～翌年1月
B-2				地方公共団体以外	東京・大阪・名古屋・つくば	13回	翌年1月～2月
C		準上級	セキュリティ専門担当者（高度なセキュリティ技術）	全組織共通	東京	3回	10月～翌年2月
オンライン標準	オンライン演習	初級相当	システムに携わり始めた者（事案発生時の対応の流れ）	全組織共通	（受講者職場等）	随時	5/24～7/19
オンライン入門		入門					翌年1/17～2/24

イ　万博向けサイバー防御講習（CIDLE）

CIDLEは、2025年日本国際博覧会（大阪・関西万博）に向けて万全のセキュリティ体制を確保することを目的とした、公益社団法人2025年日本国際博覧会協会の情報システム担当者等対象のサイバー防御講習である。東京2020オリンピック・パラリンピック競技大会のレガシーを活用し、2023年度（令和5年度）中に講義・演習プログラムの提供を予定している。

ウ　若手セキュリティ人材の育成プログラム（SecHack365）

SecHack365は、日本国内に居住する25歳以下の若手ICT人材を対象として、新たなセキュリティ対処技術を生み出しうる最先端のセキュリティ人材（セキュリティイノベーター）を育成するプログラムである。NICTの持つ実際のサイバー攻撃関連データを活用しつつ、第一線で活躍する研究者・技術者が、セキュリティ技術の研究・開発などを1年かけて継続的かつ本格的に指導する。2022年度（令和4年度）は40名が修了し、2017年度（平成29年度）からの合計で252名が修了している。

2　サイバーセキュリティ統合知的・人材育成基盤（CYNEX）の構築

我が国のセキュリティ事業者は、海外のセキュリティ製品を導入・運用する形態が主流である。このため、我が国のサイバーセキュリティ対策は、海外製品や海外由来の情報に大きく依存しており、国内のサイバー攻撃情報などの収集・分析などが十分にできていない。また、海外のセキュリティ製品を使用することで、国内のデータが海外事業者に流れ、我が国のセキュリティ関連の情報が海外で分析される一方で、分析の結果として得られる脅威情報を海外事業者から購入する状況が継続している。

その結果、国内のセキュリティ事業者では、コア部分のノウハウや知見の蓄積ができず、また、グローバルレベルの情報共有における貢献や国際的に通用するエンジニアの育成を効果的に実施することが難しくなっている。利用者側企業でも、セキュリティ製品やセキュリティ情報を適切に取

り扱える人材が不足している。サイバーセキュリティ人材の育成を含めて我が国のサイバー攻撃への自律的な対処能力を高めるためには、国内でのサイバーセキュリティ情報生成や人材育成を加速するエコシステムの構築が必要である。

総務省では、サイバーセキュリティに関する国内トップレベルの研究開発を実施しているNICTと連携し、NICTが培ってきた技術・ノウハウを中核として、サイバーセキュリティに関する産学官の巨大な結節点となる先端的基盤「サイバーセキュリティ統合知的・人材育成基盤」（通称CYNEX（サイネックス））の試験運用を2022年度（令和4年度）から開始しており、2023年度（令和5年度）からは、大学や民間企業等との連携を拡大しながら、情報分析、製品検証、人材育成事業の本格運用を開始する予定である。

関連データ

サイバーセキュリティ統合知的・人材育成基盤（CYNEX）

URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/datashu.html#f00380（データ集）

また2023年度（令和5年度）より、「政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証事業（CYXROSS）」について、一部の府省庁に国産セキュリティソフトを導入し、得られたマルウェア情報等をNICTのCYNEXへ集約・分析することで、我が国のセキュリティ対策を強化する取組を開始する予定である。

関連データ

政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証事業（CYXROSS）

URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/datashu.html#f00381（データ集）

この先端的基盤の構築により、我が国のサイバーセキュリティ情報を幅広く収集・分析し、更にその情報を活用して国産セキュリティ製品の開発を推進するとともに、高度なセキュリティ人材の育成や民間・教育機関などでの人材育成支援を行うことが可能となる。これにより、我が国におけるサイバーセキュリティ対策のより一層の強化を目指している。

4 国際連携の推進

サイバー空間はグローバルな広がりをもつことから、サイバーセキュリティの確立のためには諸外国との連携が不可欠である。このため、総務省では、サイバーセキュリティに関する国際的合意形成への寄与を目的として、各種国際会議やサイバー協議などでの議論や情報発信・情報収集を積極的に実施している。

また、世界全体のサイバーセキュリティのリスクを減らすためには、開発途上国に対するサイバーセキュリティ分野における能力構築支援の取組も重要である。総務省では、ASEAN地域において、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）を通じた人材育成プロジェクトを推進するなど、ASEAN地域を中心に、サイバーセキュリティ能力の向上に資する取組を行っている[*16]。

加えて、通信事業者などによる民間レベルでの国際的なサイバーセキュリティに関する情報共有

＊16 日ASEANサイバーセキュリティ能力構築センターでの取組については、第5章第8節「ICT国際戦略の推進」も参照。

を推進するために、ASEAN各国のISPが参加するワークショップ、日米・日EU間でのISAC（Information Sharing and Analysis Center）との意見交換会などを開催している。

5 普及啓発の推進

1 テレワークのセキュリティに関する取組

テレワーク導入企業に対して実施したアンケート[*17]では、セキュリティ確保がテレワーク導入に当たっての最大の課題とされており、総務省では、こうしたセキュリティ上の不安を払拭し、企業が安心してテレワークを導入・活用できるようにするため、2004年（平成16年）から「テレワークセキュリティガイドライン」を策定・公表している。

新型コロナウイルス感染症の感染拡大を契機として、テレワークを取り巻く環境が大きく変化しているほか、クラウド活用の進展やサイバー攻撃の高度化などセキュリティ動向の変化も生じていることから、総務省では、2021年（令和3年）5月に、実施すべきセキュリティ対策や具体的なトラブル事例などを全面的に見直すガイドライン改定を行った。

併せて、中小企業などではセキュリティの専任担当がいない場合や担当が専門的な仕組を理解していない場合も想定されるため、最低限のセキュリティを確実に確保することに焦点を絞った「中小企業など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）」を策定したが、2022年（令和4年）5月に、ユニバーサルデザインを意識して読みやすいデザイン・文言となるよう改定を行うとともに、従業員が実際に活用可能な「従業員向けハンドブック」等を付録として新たに作成した。

2 地域に根付いたセキュリティコミュニティ（地域SECUNITY）の形成促進

我が国の情報通信サービス・ネットワークの安全性や信頼性の確保の観点からは、全国規模や首都圏でサービスを提供している事業者だけでなく、地域単位で情報通信サービスを提供している事業者におけるサイバーセキュリティの確保も重要な課題である。他方、地域の企業や地方自治体では、首都圏や全国規模で展開する企業と比較してサイバーセキュリティに関する情報格差が存在するほか、経営リソースの不足などの理由により、単独で十分なセキュリティ対策を取ることが難しかったり、セキュリティ対策の必要性を認識するに至らなかったりするおそれがある。

総務省では、このような関係者間でのセキュリティに関する「共助」の関係を構築したコミュニティ（「地域SECUNITY」）について、2022年度（令和4年度）までに、総合通信局等の管区を基準とした全11地域での設立を完了した。今後は、大規模な地域横断的なイベントの開催や、幅広い層への普及啓発の取組の拡大に向けて、2023年度（令和5年度）も同様に引き続きイベント開催などの支援を実施していく[*18]。

関連データ

各地域におけるセキュリティコミュニティ

URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/datashu.html#f00382（データ集）

＊17 テレワークセキュリティに係る実態調査：https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
＊18 最新のイベントの詳細等は以下のURLに掲載している
https://www.soumu.go.jp/main_sosiki/cybersecurity/localsecunity/index.html

3 サイバー攻撃被害に係る情報の共有・公表の適切な推進

サイバー攻撃の脅威が高まる中、サイバー攻撃の被害を受けた組織がサイバーセキュリティ関係組織と被害に係る情報を共有・公表することは、攻撃の全容解明や対策強化を図る上で、被害組織・社会全体の双方にとって有益である一方、自組織に対する評判等の懸念から、被害組織は、情報の共有・公表に慎重であるケースが多い。

そこで、2022年（令和4年）4月、官民の多様な主体が連携する協議体である「サイバーセキュリティ協議会」の運営委員会の下に「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」を開催し、サイバー攻撃被害を受けた組織において実務上の参考となる「サイバー攻撃被害に係る情報の共有・公表ガイダンス」について検討を行った。同ガイダンスについては、パブリックコメントを経て、2023年（令和5年）3月に同検討会において取りまとめ、公表している[*19]。

今後、関係省庁が連携して同ガイダンスの普及啓発に努めるとともに、サイバー攻撃の被害を受けた組織が同ガイダンスを活用した際のフィードバック等を踏まえ、同ガイダンスの改定の必要性等について検討していく。

4 無線LANセキュリティに関する取組

無線LANは、自宅や職場での利用に加え、街なかの公衆無線LANサービスなど幅広く利用が進んでいるが、適切なセキュリティ対策をとらなければ、無線LAN機器を踏み台とした攻撃や情報窃取などが行われるおそれがある。このため、総務省では、無線LANのセキュリティ対策に関して、利用者・提供者のそれぞれに向けたガイドラインを策定しており、2020年（令和2年）5月に、最新のセキュリティ動向や技術動向に対応させるための改定を行った。

無線LANの利用者に向けた「Wi-Fi利用者向け 簡易マニュアル」では、利用者が留意すべきセキュリティ対策として、①接続するアクセスポイントをよく確認、②正しいURLでHTTPS通信をしているか確認、③自宅に設置している機器の設定を確認、の3つのポイントを示した上で、それぞれに解説を加えている。

無線LANの提供者に向けた「Wi-Fi提供者向け セキュリティ対策の手引き」では、飲食店や小売店をはじめとする幅広い無線LAN提供者が、提供に当たりどのようなセキュリティ上のリスクが存在し、どのようなセキュリティ対策を講じればよいかを確認できるようにしている。

また、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、サイバーセキュリティ月間（2/1～3/18）に合わせて、無線LANに関する最新のセキュリティ対策等を学ぶことが出来る無料のオンライン講座を、毎年度開講している[*20]。2022年度（令和4年度）は、2023年（令和5年）3月1日から同年3月26日までオンライン講座「今すぐ学ぼうWi-Fiセキュリティ対策」を開講した。

＊19 サイバー攻撃被害に係る情報の共有・公表ガイダンス（令和5年3月8日策定）：https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00160.html
＊20 無線LAN（Wi-Fi）のセキュリティ対策に係るオンライン講座：https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/index.html