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制定された、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）により、2015年（平成27年）、内閣の下にサイバーセキュリティ戦略本部が設置された。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、現在、2021年（令和3年）9月に閣議決定された「サイバーセキュリティ戦略[*1]」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。

また、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。2024年（令和6年）3月同本部改定。）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15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。

さらに、2022年（令和4年）12月に閣議決定された国家安全保障戦略においては、「国や重要インフラ等の安全等を確保するために、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる」ことが掲げられており、同戦略に基づく取組の実現に向けた検討が政府全体で進められている。

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、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。直近では、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で開催した「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」での議論も踏まえ、総合的なIoTボットネット対策の推進をはじめとした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等を盛り込んだ「ICTサイバーセキュリティ総合対策2023[*3]」を2023年（令和5年）8月に策定した。また、生成AIなどの新たな技術・サービスの急速な普及やサプライチェーンの多様化・複雑化などにより、今後ますます大きく変化していくサイバーセキュリティを巡る環境の変化を見込み、2024年（令和6年）2月からは、「ICTサイバーセキュリティ政策分科会」を開催し、総務省が中長期的に取り組むべきサイバーセキュリティ施策の方向性について検討を行っている。

＊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_2024.pdf
＊3　ICTサイバーセキュリティ総合対策2023：https://www.soumu.go.jp/main_content/000895981.pdf

② 今後の課題と方向性

社会全体のデジタル・トランスフォーメーション（DX）の推進により、サイバー空間は誰もが日常的に利用するようになってきている一方で、フィッシング詐欺やランサムウェア被害の報告件数が年々深刻化するなど、サイバー空間を取り巻くリスクは時代や環境とともに変化してきている。

特に、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ほか、我が国でも港湾や医療機関、政府機関等を狙った深刻なサイバー事案が発生している状況にある。さらに、生成AI等の新しい技術が登場し、利便性が増す一方で、それらの悪用によるリスクの拡大も指摘されている。

サイバー空間が公共空間化する中で、これらの情勢変化を認識しつつ、その基盤となるIoTや5Gを含むICT（情報通信技術）を国民一人ひとりが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 総合的なIoTボットネット対策の推進

サイバー空間を支える情報通信ネットワークの安全性・信頼性を確保する上で、DDoS攻撃のように情報通信ネットワークの機能に支障を生じさせるような大規模サイバー攻撃による影響も懸念される。大規模サイバー攻撃の典型例であるDDoS攻撃では、①多数のIoT機器にマルウェアを感染させ攻撃者の支配下に置く段階（攻撃インフラの拡大）と、②これらの攻撃インフラを利用しネットワークを通じた攻撃を実行する段階の2つの段階が存在する。実際に、IoT機器の数の増加や機能向上に伴い、IoT機器を悪用したサイバー攻撃も件数・規模は増加傾向にあり、NICTが運用するサイバー攻撃観測網（NICTER）が2023年（令和5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。

こうした大規模なサイバー攻撃に対応していくためには、攻撃インフラの拡大を防ぐ端末側（IoT機器）の対策、攻撃インフラに対して指令を出すC&C（Command and Control）サーバに対処するネットワーク側の対策の双方から、総合的なIoTボットネット対策を推進することが必要となる。

端末側の対策としては、総務省及びNICTにおいて、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きた。この取組では、国立研究開発法人情報通信研究機構法（以下「NICT法」という。）に基づき、令和5年度までのNICTの時限的な業務として、インターネット上のIoT機器に対して、「password」や「123456」等の容易に推測されるパスワードを設定している機器やマルウェア感染を原因とする通信をおこなっている機器を調査し、これらがサイバー攻撃に悪用されないよう、機器の利用者への注意喚起等の対処を推進し、一定の成果をあげている。

しかしながら、最近では、IoT機器のソフトウェアの脆弱性を狙ったサイバー攻撃も増加している等、IoT機器を悪用したサイバー攻撃のリスクは引き続き高い状況にあり、依然としてIoT機器を悪用したサイバー攻撃が発生している。これを踏まえ、2023年（令和5年）の第212回国会（臨時国会）において、NICT法の改正を行い、ID・パスワードの設定に脆弱性があるIoT機器の調査を2024年度（令和6年度）以降も継続して実施するとともに、新たにソフトウェア等の脆弱性を有するIoT機器やすでにマルウェアに感染しているIoT機器にも調査対象を拡充した。また、これまでのIoT機器管理者への注意喚起に加え、メーカーやシステムベンダーなどと連携したIoT機器のセキュリティ対策の推進や、動画配信やネット広告などを活用したIoT機器のセキュリティ対策の意識啓発も行うことで、総合的な対処を推進することとしている。

また、ネットワーク側の対策としては、2022年度（令和4年度）から、電気通信事業者において通信トラヒックに係るフロー情報（IPアドレス、ポート番号、タイムスタンプ等）を分析し、サイバー攻撃の指令元であるC&Cサーバを検知する技術の有効性の検証や、検知したC&Cサーバリストの事業者間の情報共有や利活用の在り方の検討などを実施している。これまでの取組の成果として、一定数のC&Cサーバの検知に成功するなど、フロー情報分析の有効性は確認されており、2024年度（令和6年度）からは、フロー情報分析を行う電気通信事業者の拡大、検知されたC&Cサーバに対する能動的分析の実施等により、更なる検知精度の向上に取り組んでいく。

関連データ　動画配信を活用したIoTセキュリティ対策の意識啓発

URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/html/datashu.html#f00399（データ集）

2 電気通信事業者による積極的サイバーセキュリティ対策の推進

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、前述の総合的なIoTボットネット対策に加え、通信トラヒックが通過するネットワーク側におけるより機動的な対処を行う環境整備が必要と考えられる[*4]。

2023年度（令和5年度）は、2022年度（令和4年度）に引き続き、大規模化・巧妙化・複雑化するサイバー攻撃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のサイバーセキュリティ対策に関する総合実証を実施した。「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」においては、Webサービス提供者向けのフィッシング対応実務リファレンスを作成するとともに一般国民向けの普及啓発を実施した。「ネットワークセキュリティ対策手法の導入に係る実証」においては、国際的にも実装が進みつつあるにも関わらず、我が国では普及が進んでいないRPKI[*5]、DNSSEC[*6]、DMARC[*7]等のネットワークセキュリティ技術について、技術実証等を通じて得られた知見を踏まえて導入・運用に係るガイドライン案を作成[*8]し、2024

＊4　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

＊5　Resource Public-Key Infrastructureの略。自律ネットワークのIPアドレスやAS番号を電子証明書で検証し、通信経路の乗っ取り等を防止する技術。

＊6　DNS Security Extensionsの略。ドメインネームとIPアドレスの紐付けを電子証明書で検証し、サーバのなりすまし等を防止する技術。

＊7　Domain-based Message Authentication Reporting and Conformanceの略。電子メールの送信元ドメインの正しさを検証し、なりすまし等の場合は自動的に処理する技術。

＊8　第5回ICTサイバーセキュリティ政策分科会参考資料2〜4（①RPKIのROAを使ったインターネットにおける不正経路への対策ガイドライン案、②DNSSECによるDNS応答の認証技術ガイドライン案、③電子メールのなりすまし対策、迷惑メール対策技術であるDMARC等（SPF、DKIMを含む）のメール認証技術ガイドライン案）https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00286.html

年度（令和6年度）においても継続的に普及促進に向けた取組を推進している。

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行い、2022年（令和4年）4月、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た「5Gセキュリティガイドライン第1版[*9]」を公表した。同ガイドラインは、2022年（令和4年）9月、ITU-T SG17において標準化のための新規作業項目として承認され、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）[*10]がソフト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[*11]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 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、2024年（令和6年）5月1日現在、合計68サービスがISMAPクラウドサービスリスト[*12]として公開されている。

＊9　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
＊10　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。
＊11　Software Bill of Materials. ソフトウェア部品構成表。
＊12　ISMAPクラウドサービスリスト：https://www.ismap.go.jp/csm?id=cloud_service_list

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みである。

また、ISMAPの信頼性・安定性の保持を前提としつつ、制度運用を合理化・明確化するため、2022年（令和4年）10月より「ISMAP制度改善の取組み」を継続して実施している。その一環として、2023年（令和5年）10月より、「外部監査の負担軽減」や「審査の迅速化・効率化」などについて改善した枠組みによる本格運用を開始した。今後も制度改善の取組等を通じてクラウド・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」として策定し、2024年（令和6年）4月には、クラウドサービス利用者向けに、ガイドラインの内容をわかりやすく解説するための「クラウドの設定ミス対策ガイドブック」を公表した。

5 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Ⅱ-2-5-1）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[*13]」を公表した。

総務省においては、「デジタル社会の実現に向けた重点計画」（2023年（令和5年）6月9日閣議決定）[*14]を踏まえ、タイムスタンプの的確な制度運用とeシールの民間サービスの信頼性を評価する基準策定及び適合性評価の実現に向けた検討等を進めている。

＊13　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/
＊14　デジタル社会の実現に向けた重点計画：https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609_policies_priority_outline_05.pdf

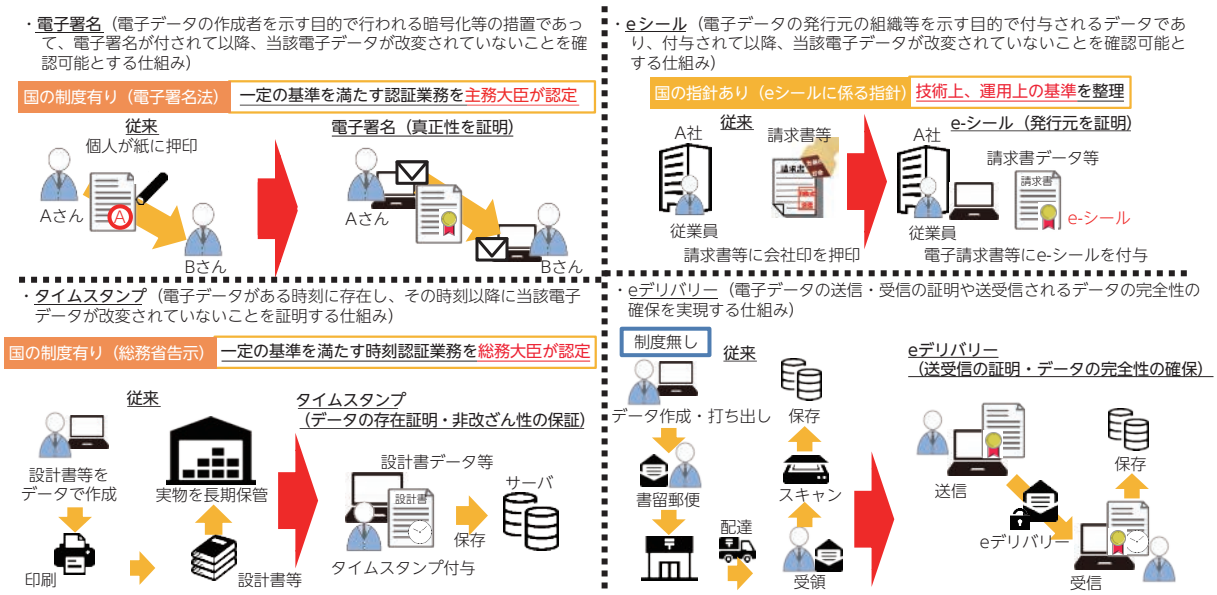
ア　国によるタイムスタンプ認定制度の整備

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。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。

イ　eシールの制度化に向けた取組

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い、2021年（令和3年）6月に、我が国におけるeシールに係る技術や運用等に関する一定の基準を示した「eシールに係る指針」を策定した。さらに、2023年（令和5年）9月に「eシールに係る検討会」を立ち上げ、eシールの民間サービスの信頼性を評価する基準策定及び適合性評価の実現に向けた検討を行い、2024年（令和6年）4月に検討会の最終取りまとめ[*15]とともに、「eシールに係る指針（第2版）[*16]」を公表した。これらの検討結果を踏まえながら、国によるeシールに係る認定制度の運用開始に向けた取組を行う。

図表Ⅱ-2-5-1　トラストサービスのイメージ



*15 eシールに係る検討会　最終取りまとめ：https://www.soumu.go.jp/main_content/000942601.pdf
*16 eシールに係る指針（第2版）：https://www.soumu.go.jp/main_content/000942602.pdf

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。

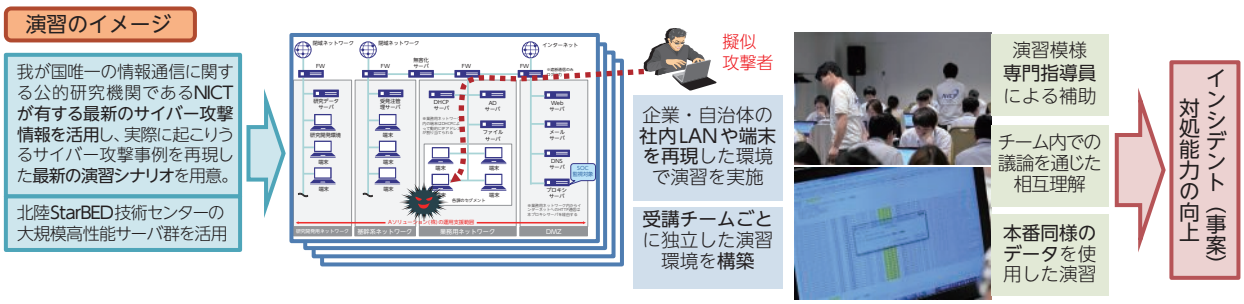
ア　情報システム担当者等を対象とした実践的サイバー防御演習（CYDER）

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Ⅱ-2-5-2）。

2023年度（令和5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入門コースに加え、サイバー攻撃の仕組みやトレンド、インシデントハンドリングの基礎を学べる「プレCYDER」を試行実施した（図表Ⅱ-2-5-3）。

CYDER集合演習の受講者は、2023年度（令和5年度）は3,742人で、2017年度（平成29年度）からの合計で2万人超となった。

図表Ⅱ-2-5-2　実践的サイバー防御演習（CYDER：CYber Defense Exercise with Recurrence）



図表Ⅱ-2-5-3　2023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	68回	7月～翌年1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	21回	10月～翌年1月
B-2				地方公共団体以外	東京・大阪・名古屋	13回	翌年1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	4回	11月～翌年1月
オンライン入門	オンライン演習	入門	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月～7月
プレCYDER		—	システムに携わり始めたばかりの者（前提知識、基礎的な事項）	国の機関等、地方公共団体			12月～翌年1月

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、大阪・関西万博関連組織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）から講義・演習プログラムを提供している。

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。2023年度（令和5年度）は38名が修了し、2017年度（平成29年度）からの合計で289名が修了している。

2 サイバーセキュリティ統合知的・人材育成基盤の構築（CYNEX）

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」の構築・運用を行うことで、我が国のサイバーセキュリティ対応能力を向上させる取組であるCYNEXを推進している。2023年(令和5年）10月には、CYNEXに参画する産学官の組織で構成する「CYNEXアライアンス」を発足させ、CYNEXの本格展開を開始した。2024年度（令和6年度）も引き続き、民間企業や教育機関等との連携を拡大しながら、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企業・教育機関等での人材育成支援を行うことで、我が国におけるサイバーセキュリティ対応能力のより一層の強化を目指す。

関連データ　サイバーセキュリティ統合知的・人材育成基盤の構築（CYNEX）

URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/html/datashu.html#f00403（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、一部の府省庁に安全性・透明性を検証可能な

センサーを導入し、得られたサイバーセキュリティ情報をNICTのCYNEXへ集約し分析することで、我が国のセキュリティ対策を強化する取組を開始した。2024年度（令和6年度）は、引き続きサイバーセキュリティ情報の集約・分析を拡充するとともに、センサー導入府省庁を拡大することで、我が国独自のサイバー攻撃分析能力を強化する。

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/r06/html/datashu.html#f00404（データ集）

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[*17]。2023年度（令和5年度）には、AJCCBCの活動で培ったノウハウ等を活用して、大洋州の島しょ国向けに新たに能力構築支援の試行的な演習を実施するなど、能力構築支援の活動地域の拡大を図っている。

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[*18]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広がり、働き方改革の中心にも据えられているテレワークについて、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を踏まえ、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の改定を行った。

＊17 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Ⅱ部第2章第8節「ICT国際戦略の推進」も参照
＊18 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/

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、セキュリティ対策の担当者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2020年（令和2年）から策定・公表している。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・文言となるようチェックリストの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。また、チェックリストに従ってセキュリティ対策を実施するにあたり、テレワークで使用される製品をどのように設定すべきか解説した「設定解説資料」も公表。2023年（令和5年）10月には「設定解説資料」の対象製品を拡充するとともに公開済みの製品についても内容の更新を行った。

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

我が国の安全・安心なサイバー空間の確保の観点からは、地域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、人材等の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、地域における関係者間での「共助」の関係を基本としたセキュリティ分野におけるコミュニティ（「地域SECUNITY」）の形成を促進しており、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。2023年度（令和5年度）にはセミナー等16件、インシデント対応演習10件、若年層向けCTF（Capture The Flag）7件を実施した他、大規模な地域横断的なイベントも開催した。地域SECUNITYの取組拡大に向けて、2024年度（令和6年度）も引き続き、イベント開催などの支援を実施していく[*19]。

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/r06/html/datashu.html#f00405（データ集）

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」2023年（令和5年）3月に取りまとめ、公表した[*20]。

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

＊19 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
＊20 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

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いる[*21]。

2024年（令和6年）3月には、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」の内容について更新を行うとともに細分化し、「公衆Wi-Fi利用者向け 簡易マニュアル」と、自宅に無線LANを設置する者に向けた「自宅Wi-Fi利用者向け 簡易マニュアル」に分けた。これにより、利用者が無線LANを使う状況に応じて適切な内容を確認できるようになった。

飲食店や小売店をはじめとする幅広い無線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」についても、記載内容の更新を行い、2024年（令和6年）3月に更新版を公開した。

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。2023年度（令和5年度）は、2024年（令和6年）3月1日から同年3月24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。

＊21 無線LAN（Wi-Fi）のセキュリティに関するガイドライン：https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/index.html