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、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、現在、2021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6月サイバーセキュリティ戦略本部決定。2024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12月に閣議決定された国家安全保障戦略に基づき、「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」べく、当該分野における新たな取組の実現のために必要となる法制度等について検討するため、内閣官房において2024年6月から有識者会議を開催した。同年11月には「サイバー安全保障分野での対応能力の向上に向けた提言」がとりまとめられ、これを踏まえ、2025年の第217回国会（常会）に「重要電子計算機に対する不正な行為による被害の防止に関する法律」及び「重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律」の両法案が提出され、原案修正の上、2025年5月に可決・成立するなど、サイバー安全保障分野での政府の取組が進んでいる。

総務省では、2017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、2024年2月から、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・複雑化の動向を踏まえ、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する「ICTサイバーセキュリティ政策分科会」を開催し、「ICTサイバーセキュリティ政策の中期重点方針」を2024年7月に公表した。

2　今後の課題と方向性

近年、我が国を取り巻くサイバーセキュリティ情勢は年々複雑化・高度化しており、大手事業者のデータセンターを狙ったランサムウェア攻撃により事業に支障を与える事例や、生成AIを利用することで、技術的な知識なしにランサムウェアを作成した事例も発生している。また、デジタル化の急速な進展に伴うIoT機器の増加や、サプライチェーンの多様化により、攻撃対象は拡大し続ける一方、国際関係の変化は加速し、安全保障情勢も厳しさを増している。

このように、サイバー攻撃の複雑化・巧妙化が進んでいるなかで、その攻撃対象は重要インフラ等に

＊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

も及び、国民生活や経済活動に影響を与えかねないというように、サイバー空間を取り巻くセキュリティリスクは深刻化している。

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、総務省が関係機関や民間企業等と連携し、我が国のサイバーセキュリティ政策に率先して取り組むことにより、サイバー空間における安全・安心の確保に貢献していく。

2 重要インフラ等におけるサイバーセキュリティ

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。こうしたDDoS攻撃の典型的な手法には、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2024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、総務省、NICT及びインターネット・サービス・プロバイダ（ISP）と連携し、2019年2月から「NOTICE（National Operation Towards IoT Clean Environment）」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の調査を行い、利用者への注意喚起を行うための取組を実施し、一定の成果をあげたところである。

しかし、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、これまでの取組に加えて、2024年度より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済みの端末を調査し機器の利用者やIoT機器メーカー等に助言等を行うことをNICTの業務として位置付け、能力の強化を図ることとした。

さらに、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、総務省は2022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、2025年度からは、端末側の対策とも連携しながら、IoTボットネットの全体像を可視化した上で、各ボットネットの特性に応じた効果的な対処を実現することにより、IoTボットネットの縮小を目指していく。

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[*3]。

2021年度より、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、2024年5月にリファレンスの概要を公開した。「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、国際的にも実装が標準的になりつつあるにも関わらず、我が国では普及が十分ではないRPKI[*4]、DNSSEC[*5]、DMARC[*6]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した。2024年度には本ガイドライン案をもとに、一般社団法人日本ネットワークインフォメーションセンターから「RPKI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[*7]」が、一般社団法人日本データ通信協会から「送信ドメイン認証技術 DMARC導入ガイドライン[*8]」が公表された。2025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年度から2021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、2024年9月にITU-T SG17[*10]において、国際標準として承認された。

また、通信分野においては、機能の高度化等に伴いシステム構成が複雑化しており、OSS[*11]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等が発生しているが、ソフトウェアの構成を把握できていない場合、攻撃に対する迅速な対応が困難となる。

このような状況を踏まえ、総務省では、SBOM[*12]の活用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、SBOMを作成及び活用するに当たっての留意点をまとめた留意事項（案）を作成した。

さらに、2023年度からは、スマートフォンアプリを対象に、第三者によるアプリ挙動に関する技術的解析等を実施し、我が国の解析能力の水準や利用者情報の取扱慣行等を把握する実証事業を実施し

＊3　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
＊4　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。
＊5　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。
＊6　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。
＊7　RPKI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
https://www.nic.ad.jp/doc/jpnic-01324.html
＊8　送信ドメイン認証技術 DMARC 導入ガイドライン
https://www.dekyo.or.jp/soudan/data/anti_spam/dmarc_guideline.pdf
＊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　国際電気通信連合 電気通信標準化部門Study Group17
＊11　オープンソースソフトウェアを指し、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。
＊12　Software Bill of Materials. ソフトウェア部品表。

た。2025年度からは、「スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律」（令和6年法律第58号）の施行により、我が国においてスマートフォンのOS事業者が運営する公式ストア以外のアプリ代替流通経路の利用が進むと見込まれるため、アプリ代替流通経路の事業者等がSPSI[*13]に準拠して、セキュリティ等の確保に向けた取組が実施されているかについての調査を実施している。

4 クラウドサービスの安全性確保に関する取組

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」を策定した。2024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。

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」（2024年6月21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[*15]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て取り組んでいる。

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3月に総務省が立ち上げた「タイムスタンプ認定制度に関する検討会」で検討を行い、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年度の税制改正により、電子帳簿保存法[*16]（平成10年法律第25号）による税務関係書類に係るスキャナ保存制度等で使用されるタイムスタンプについては、総務大臣認定制度に基づくタイムスタンプを使うこととされた。2025年5月時点では4社がタイムスタンプ事業者として認定されている。今後も、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取り組む。

＊13　スマートフォン プライバシー セキュリティ イニシアティブ（SPSI）（https://www.soumu.go.jp/main_content/000981875.pdf）
＊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-b989-2bcaabffe870/6329b727/20240621_policies_priority_outline_03.pdf）
＊15　eシールとは、電磁的記録に記録された情報（以下「電子データ」という。）に付与された又は論理的に関連付けられた電子データであって、「当該情報の出所又は起源を示すためのものであること」及び「当該情報について改変が行われていないかどうか確認することができるものであること」のいずれの要件にも該当するものをいう。
＊16　電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律（平成10年法律第25号）

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4月に総務省が立ち上げた「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。2023年9月には「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4月に検討会の最終取りまとめ[*17]とともに、「eシールに係る指針（第2版）[*18]」を公表した。さらに、2024年6月には、eシールに係る認定制度創設に向けて、制度運用に必要な関係規程の策定に資する検討を行うことを目的に「eシールに係る関係規程策定のための有識者会議」を開催し、2025年3月に「eシールに係る認証業務の認定に関する規程」（令和7年総務省告示第113号）により国（総務大臣）による認定制度を創設した。今後は本格的な運用に向けて、指定調査機関の指定等に取り組んでいく。

図表Ⅱ-2-5-1　トラストサービスのイメージ

3　サイバー攻撃対処能力の向上と新技術への対応

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（CYber Defense Exercise with Recurrence）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、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

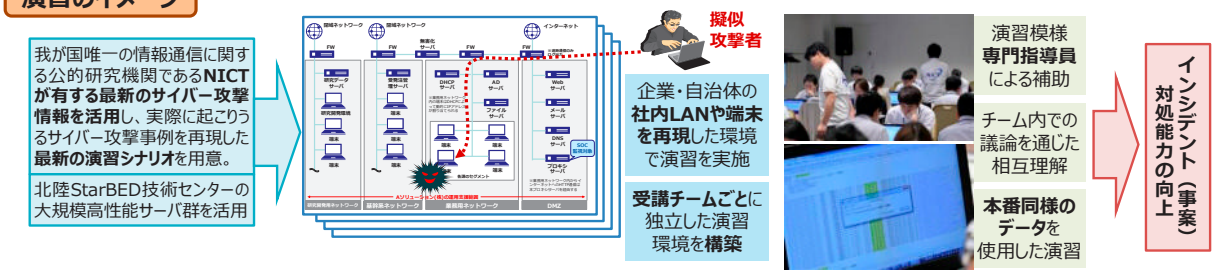
＊17　eシールに係る検討会　最終取りまとめ（https://www.soumu.go.jp/main_content/000942601.pdf）
＊18　eシールに係る指針（第2版）（https://www.soumu.go.jp/main_content/000942602.pdf）

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）。

2024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」を本格実施した（図表Ⅱ-2-5-3）。

CYDER集合演習の受講者は、2024年度は4,225人で、2017年度からの合計で2万5千人超となった。

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　2024年度CYDER実施状況

コース名		実施方法	レベル	受講想定者（習得内容）	受講想定組織	実施地	実施期間
CYDER	A	集合形式	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	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	10月～翌年1月
	B-2				地方公共団体以外	東京・大阪・名古屋	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・大阪	11月～翌年1月
プレCYDER		オンライン形式	-	全ての情報システム担当者（最低限必要となる知識の習得と最新化）	全組織共通	（受講者職場等）	前半：5月～7月 後半：10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が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年度から2024年度まで講義・演習プログラムを提供した。

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。2024年度は39名が修了し、2017年度からの合計で328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（サイネックス：CYbersecurity NEXus）を2021年度より推進している。2023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。2025年度も引き続き、官公庁及び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官公庁及び民間企業・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/r07/html/datashu.html#f00393（データ集）

また2023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へ集約し、NICTの能力を活用して分析することで、我が国のセキュリティ対策を強化する取組を開始した。2025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/r07/html/datashu.html#f00394（データ集）

3 サイバーセキュリティにおける生成AI等に関する取組

近年、あらゆる分野において生成AIの実装が急速に進んでいる一方で、生成AIを巡るリスクとして、偽・誤情報の拡散、プライバシーの侵害、知的財産権の侵害等に加えて、サイバー攻撃への悪用等によるサイバーセキュリティのリスクが新たに指摘されている。他方、サイバー攻撃の大規模化・複雑化・巧妙化に伴い、サイバーセキュリティ対策の業務負荷が課題となっている中、サイバー攻撃対策への生成AI等の利活用が期待されている。

こうした背景を踏まえ、生成AI等のAI技術を巡る最新動向を把握しつつ、AIに起因するセキュリティリスクを可能な限り回避・低減するための「Security for AI」に取り組むとともに、AIをセキュリティ対策に効果的に活用するための「AI for Security」に取り組むことが必要である。

「Security for AI」の取組については、AIの安全かつ効果的な開発・提供に向けたセキュリティガイドラインの策定等のほか、NICTと米国等の様々な専門機関との連携によるAI安全性の研究開発を実施することで、生成AIの安心安全な利用を促進していく。

「AI for Security」の取組については、サイバー脅威情報の収集・分析や生成AI等を活用した攻撃インフラの検知の精緻化・迅速化を行うことで、生成AIのサイバーセキュリティ対策への積極的な活用を促進していく。

関連データ サイバーセキュリティにおける生成AI等に関する取組
URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html#f00395（データ集）

4 地域をはじめとするサイバーセキュリティの底上げに向けた取り組み

1 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。2024年度にはセミナー等20件、インシデント対応演習14件、若年層向けCTF（Capture The Flag）3件を実施した他、7会場同時開催の全国型CTFイベントも開催した。地域SECUNITYの取組拡大に向けて、2025年も引き続き、イベント開催などの支援を実施していく。

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/main_sosiki/cybersecurity/localsecunity/index.html

2 テレワーク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[*19]では、セキュリティ確保がテレワーク導入の最大の課題になっている。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、2004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。

テレワークは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。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5月にガイドラインを改訂し、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した。

また、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に専門的な知識が不足している場合が想定されるため、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）」を2020年から策定・公表している。チェックリストに従ってセキュリティ対策を実施する際に、テレワークで利用する製品をどのように設定するか解説した「設定解説資料」も公表しており、2024年7月に「設定解説資料」を更新した。

＊19 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/

3 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。ただし、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の被害を受けるおそれがある。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、2025年2月に、最新のセキュリティ動向や技術動向に対応させた改定を行った*20。

公衆無線LANサービスを利用する者に向けた「公衆Wi-Fi利用者向け簡易マニュアル」と、自宅に無線LANを設置し利用する者に向けた「自宅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ポイントを解説している。飲食店や小売店をはじめとする無線LANの提供者に向けた「公衆Wi-Fi提供者向け セキュリティ対策の手引き」では、利用者と提供者自身のための2つの観点から、必要な対策を解説している。

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、最新のセキュリティ対策等を学べる無料のオンライン講座をサイバーセキュリティ月間（2/1～3/18）に合わせて毎年度開講している。2024年度は、2025年2月5日から3月18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。

4 国民のためのサイバーセキュリティサイト

インターネット利用者がサイバー攻撃の被害を受けないよう自衛し、また意図せず他人に迷惑をかけることを防ぐため、総務省では「国民のためのサイバーセキュリティサイト」*21を開設し、広く国民に対してサイバーセキュリティに関する普及啓発をしている。

2024年5月には、サイバー攻撃による被害事例とその対処法、予防策を整理し、最新のセキュリティ動向を踏まえ記事内容を更新した。

5 国際連携のさらなる推進

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対話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*22。2023年度からは、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・地域向けに新たに能力構築支援の演習を実施するなど、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や、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。

＊20　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/
＊21　国民のためのサイバーセキュリティサイト：https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/
＊22　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