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

我が国では、サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、サイバーセキュリティ基本法（平成26年法律第104号）において、我が国のサイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、サイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定めるとともに、同法に基づき、内閣にサイバーセキュリティ戦略本部を設置し、同本部の下で、重要インフラ防護をはじめとする各種施策を推進することで、政府一体となってサイバーセキュリティの強化に取り組んできた。

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、内閣官房の有識者会議において2024年11月に取りまとめられた「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」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」（以下「サイバー対処能力強化法等」という。）の両法案が提出され、2025年5月に可決・成立したところである。これらを踏まえ、2025年7月、サイバーセキュリティ戦略本部が改組され、内閣総理大臣が本部長、内閣官房長官及びサイバー安全保障担当大臣が副本部長、すべての国務大臣が構成員となる新体制となり、併せて内閣サイバーセキュリティセンターが改組され、「国家サイバー統括室（NCO）」が設置された。さらに、2025年12月には、サイバー対処能力強化法等に基づく取組を含め、新たな「サイバーセキュリティ戦略」[*1]が閣議決定されるなど、巧妙化・複雑化するサイバー攻撃に対し、基幹インフラ・重要インフラのサイバーセキュリティの確保をはじめ、政府は取組の強化を進めている。

2　今後の課題と方向性

近年、国民生活、経済活動及び社会活動のあらゆる場面においてデジタル技術の利用が進展し、サイバー空間は各種サービス及び産業の基盤としての機能に加え、公共空間としての性格を一層強めつつ、その役割を拡大している。これに伴い、サイバー空間を取り巻く情勢は年々複雑化しており、ランサムウェア攻撃に起因して企業活動やインフラが停止した事例や、生成AIの悪用によってサイバー攻撃が実行された事例も確認されている。

このように、サイバー攻撃の脅威は拡大し、その対象は企業や個人にとどまらずインフラへと及び、重要システムの停止、機微情報の漏えい等の被害が相次ぐ等、経済・社会のみならず国家の安全保障に重大な影響を及ぼすに至っており、サイバーセキュリティ対策の強化は喫緊の課題となっている。また、近年のAI技術の急速な発展は、AIをサイバーセキュリティ対策に活用することで、ソフトウェアの脆弱性の発見・修正やサイバー攻撃の検知・対応等を通じ、我が国のサイバー対処能力の強化につながることが期待される一方で、攻撃者に悪用された場合には、サイバー攻撃の高速化・大規模化を招くおそれがあるなど、サイバーセキュリティ上の潜在的リスクの増大も懸念されている。

総務省は、こうした情勢の変化を認識しつつ、関係省庁及び関係機関と緊密に連携し、基幹インフ

＊1　サイバーセキュリティ戦略：https://www.cyber.go.jp/pdf/policy/kihon-s/cs_strategy2025.pdf

ラ・重要インフラの防護をはじめ、研究開発、人材育成、情報分析、周知啓発、国際連携の各施策を推進し、これらの取組を通じ、我が国のサイバーセキュリティ基盤の強化を図り、もって誰もが安全・安心にサイバー空間を利用できる環境の実現を目指している。

2　サイバー空間の安全性の確保

1 総合的なIoTボットネット対策の推進

DDoS攻撃等の大規模サイバー攻撃は、サイバー空間の基盤である情報通信ネットワークに重大な支障を生じさせるものであり、当該空間の安全性を確保する上で、その対策強化は引き続き重要な課題である。DDoS攻撃は、一般に、①多数のIoT機器をマルウェアに感染させてIoTボットネットを構築し、②当該ボットネットを攻撃インフラとして標的へ攻撃を実行する二段階で行われ、ネットワークに常時接続されるIoT機器の増加に伴い、攻撃の件数・規模は増加傾向にある。実際に、NICTのサイバー攻撃観測網（NICTER）が2025年に観測したサイバー攻撃関連通信は、引き続きIoT機器を対象とする通信が上位を占めている。

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）サーバー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講じ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）が連携し、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、「password」や「123456」のように容易に推測されるパスワードを設定している機器を調査し、利用者への注意喚起を実施し、一定の成果をあげてきたところである。

また、IoT機器のソフトウェアの脆弱性を狙ったサイバー攻撃等、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ることを踏まえ、これまでの取組に加えて、2024年度からは、新たにソフトウェア等に脆弱性を有するIoT機器やすでにマルウェアに感染済みの端末を調査し、当該機器の利用者への注意喚起や、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、取組を強化してきたところである。

さらに、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、NOTICEのウェブサイト[*2]等を通じてIoT機器のセキュリティ対策の意識啓発も併せて行うことで、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サーバーを検知する技術の有効性の検証や、検知したC&Cサーバーリストの事業者間の情報共有や利活用の在り方の検討等を実施している。これまでの取組により、一定数のC&Cサーバーの検知に成功するなど、フロー情報分析の有効性を確認しており、2026年度も引き続き、端末側の対策とも連携しながら、C&Cサーバーの検知・評価・共有等の一連の仕組みの改善・検証に取り組むことにより、IoTボットネット対策を推進していく。

＊2　NOTICEウェブサイト：https://notice.go.jp/

2 電気通信事業者による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、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]。

このため、総務省では、2021年度から、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。

また、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、総務省では、ガイドラインの策定支援やハンズオン勉強会の開催等を通じて導入を後押ししている。特に、なりすましメール対策として有効なDMARCの普及は、フィッシングによる不正送金等の被害が拡大している中で重要な課題となっている。2025年7月に策定された政府の「国民を詐欺から守るための総合対策2.0」[*7]では、「DMARC等への更なる対応促進」のため関係省庁が連携して取り組むこととされている。総務省では、これを踏まえて、2025年9月に、関係業界団体に対して、DMARCの導入やDMARCポリシーの設定（隔離、拒否）について要請を実施した[*8]。また、総務省においても、2025年7月には、soumu.go.jpドメインやそのサブドメインについて、サブドメインを含めて、DMARCポリシーを「隔離」に設定変更したほか、2025年11月からは、BIMI[*9]にも対応するなど、なりすましメール対策を積極的に進めている。

3 クラウドサービスのセキュリティ対策の推進

総務省では、安全・安心なクラウドサービスの利活用を推進するため、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」を策定している。

また、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、クラウドサービス利用者向けに、「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」を策定するとともに、同ガイドラインの内容をわかりやすく解説する「クラウドの設定ミス対策ガイドブック」を公表している。

3 サイバー空間を支える基盤技術の高度化と信頼性の確保

1 量子計算機時代に対応した暗号技術の高度化

暗号技術は、インターネット利用をはじめとした様々な場面で使われている。一方で、量子計算機（量子コンピュータ）に関する研究開発が加速しており、将来的に実用的で大規模な量子計算機が実現した場合、現在利用されている暗号技術の安全性が低下（危殆化）することが懸念されている。また、

＊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、サーバー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　犯罪対策閣僚会議Webサイトに掲載 https://www.cas.go.jp/jp/seisakukaigi/hanzai/index.html
＊8　フィッシングメール対策の強化に関する要請 https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000260.html
＊9　Brand Indicators for Message Identificationの略。DMARCで認証が成功したメールにロゴを表示させる技術。

現時点では解読できない暗号化データを収集・保存し、将来、量子計算機の発展後に解読を試みる、いわゆる「Harvest Now, Decrypt Later（HNDL）」攻撃も想定されており、情報の機密性や長期的な保護の観点から、耐量子計算機暗号（Post-Quantum Cryptography：PQC）への移行を見据えた検討が重要な課題となっている。

こうした状況を踏まえ、政府機関等における耐量子計算機暗号の利用に関する検討を進めるため、2025年6月に関係府省庁連絡会議[*10]を設置した。同連絡会議では、量子計算機の進展が暗号技術に与える影響を整理するとともに、政府機関等におけるPQC移行の考え方や対象、進め方について検討を行い、同年11月に中間とりまとめを公表した。今後は、この中間とりまとめを踏まえ、2026年度中に工程表（ロードマップ）を策定し、政府機関等における計画的なPQC移行に向けた取組を進めていくこととしている。

また、政府の情報システムで利用される暗号技術については、CRYPTREC[*11]において「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）」としてまとめられており、これについてもPQCへの対応が求められている。そのため、一部のPQCについて安全性等の評価を実施した上で、2026年3月にPQCに対応するためのCRYPTREC暗号リストの改定を行った。PQCの安全性等の評価は順次実施しており、今後もCRYPTREC暗号リストの継続的な改定を通じて、政府情報システムにおける暗号技術の安全性確保に取り組んでいく。

2 トラストサービスによる信頼性の確保

サイバー空間における安全・安心なデータ流通を実現するためには、暗号技術によりデータを暗号化して通信時の安全性を確保することが基本となる。一方で、暗号技術のみでは、データが「いつ存在していたか」や「組織として正当に発行されたものであるか」といった点について、後から第三者が確認できる形で示すことは困難である。このため、暗号技術を基盤としつつ、データの時刻や発行主体の真正性等を客観的に証明する仕組みとして、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。

このため、総務省では、タイムスタンプ及びeシールについて、国による認定制度を整備することで、これらトラストサービスを通じたデータの信頼性の確保に取り組んでいる。

ア　タイムスタンプ認定制度

タイムスタンプは、ある時刻にその電子データが存在していたことと、その時刻以後に改ざんされていないことを証明する仕組みである。

総務省では、タイムスタンプサービスの信頼性を確保するため、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。認定制度では、時刻の正確性、設備の安全性・冗長性、業務運用体制等について一定の基準に適合したタイムスタンプサービスを認定している。

2026年5月時点で6サービスを認定しており、認定を受けたタイムスタンプの年間総発行件数は10億件以上である。これらは、官報[*12]、電子帳簿保存[*13]、電子契約、知的財産保護等の様々な分野で活用されている。

＊10　政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議 https://www.cas.go.jp/jp/seisaku/pqc/
＊11　Cryptography Research and Evaluation Committeesの略。デジタル庁、総務省、経済産業省、国立研究開発法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）により共同運営されているプロジェクト。https://www.cryptrec.go.jp/
＊12　官報の発行に関する内閣府令（令和6年内閣府令第80号）により、認定を受けたタイムスタンプを利用することとされている。
＊13　2022年度の税制改正により、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）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ている。

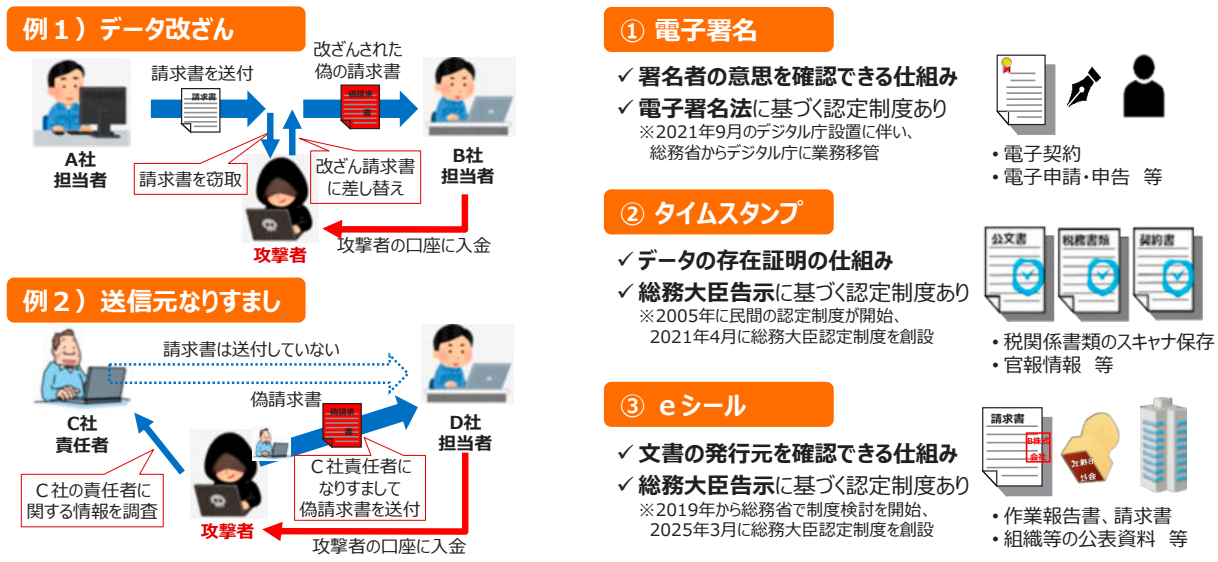
イ　eシール認定制度

eシールは、企業等が発行する電子データの発行元を証明し、また、電子データに改ざんがないことを証明する仕組みである。

総務省では、組織が発行する電子データの信頼性確保に向け、2020年4月から「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[*14]」、2023年9月から「eシールに係る検討会[*15]」、2024年6月から「eシールに係る認定制度の関係規程策定のための有識者会議[*16]」を順次開催し、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ってきた。これらの検討結果を踏まえ、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）を制定し、国（総務大臣）による認定制度を整備した。

2026年3月から認定申請の受付を開始しており、今後、eシールサービスの認定を通じ、組織が発行する電子データの真正性・信頼性を確保する基盤として、eシールの普及・活用を推進していく。

図表Ⅱ-2-5-1　トラストサービスのイメージ



4　サイバー攻撃対処能力の向上と新技術への対応

1　サイバーセキュリティ人材の育成

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、サイバーセキュリティ人材育成（CYDER、SecHack365及びCYROP）に取り組んでいる。

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）

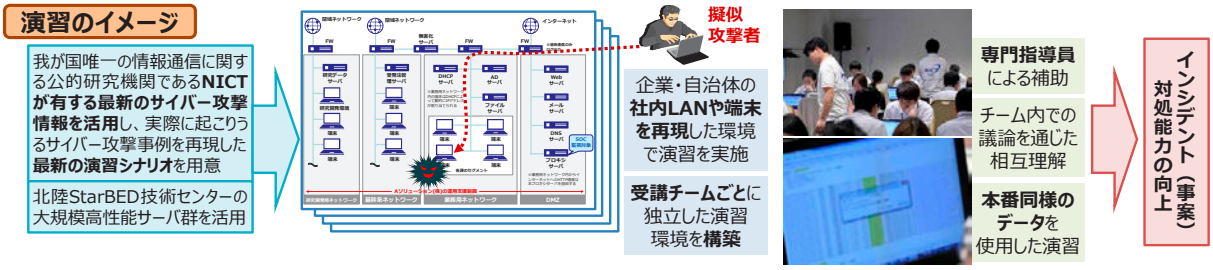
CYDER（CYber Defense Exercise with Recurrence）は、国の機関、地方公共団体、独立行政法人、重要インフラ事業者等の情報システム担当者等を対象とした実践的サイバー防御演習である。受講者は、組織のネットワーク環境を模した大規模仮想LAN環境下で、実機を操作し、インシデントの検

＊14　https://www.soumu.go.jp/main_sosiki/kenkyu/data_organization/
＊15　https://www.soumu.go.jp/main_sosiki/kenkyu/e_seal/
＊16　https://www.soumu.go.jp/main_sosiki/kenkyu/e_seal_yushikisha/

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）ことが可能であり、2025年度は3,989人、2017年度からの合計では29,000人超が受講した。

また、2025年度は、従来実施している初級・中級・準上級の集合演習や、最低限のセキュリティ知識を学べる「プレCYDER」に加え、オンラインで集合演習と同等の受講効果を得られる「オンライン実践コース」を地方公共団体向けに試行的に実施した（図表Ⅱ-2-5-3）。

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　2025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	実施回数	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	78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8地域	10回	10月～11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（初動分析を含む主体的な事案対応）	全組織共通	東京・大阪	5回	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）	–	1期：5月～8月 2期：9月～11月 3期：11月～翌年1月

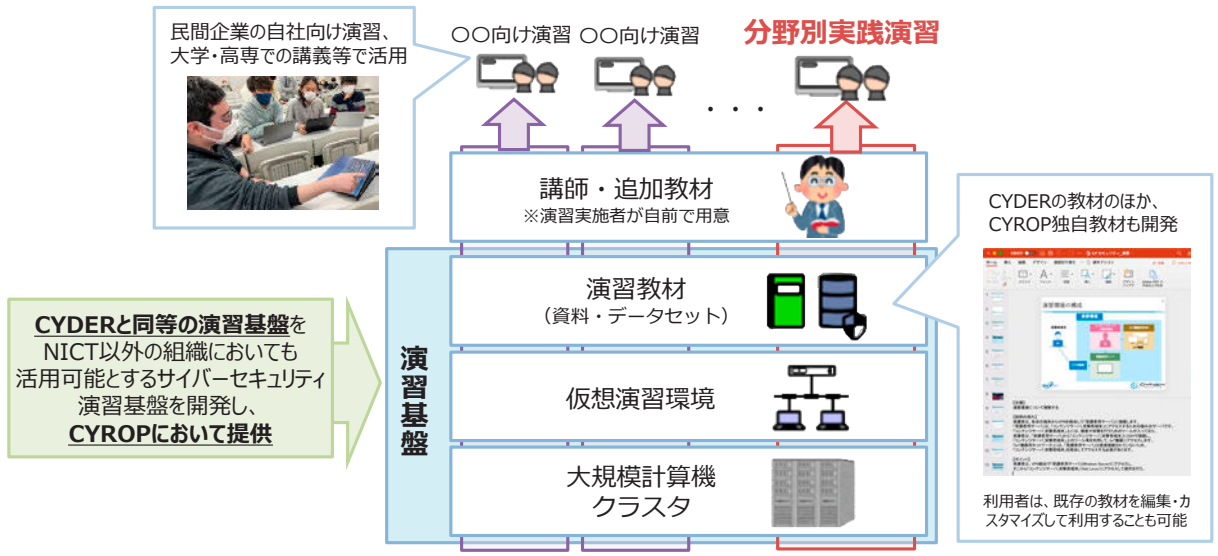
イ　若手セキュリティ人材の育成プログラム（SecHack365）

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、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が有する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・開発等を1年かけて継続的かつ本格的に指導する。2025年度は36名が修了し、2017年度からの合計で300名超が修了している。

ウ　分野別実践演習の開発・実施基盤（CYROP）

CYROP（CYber Range Open Platform）は、分野に応じた実践的演習を容易に開発・実施可能とする演習基盤である。NICTが有する人材育成ノウハウを民間企業・教育機関等に横展開するため、後述するCYNEXの一環として、2023年度からサイバーセキュリティ演習の実施に必要となる演習環境・演習教材を提供している（図表Ⅱ-2-5-4）。

図表Ⅱ-2-5-4　分野別実践演習の開発・実施基盤（CYROP）



2 新たな技術・サービスを生み出すためのエコシステムの形成

我が国のサイバーセキュリティ対策は、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り、情報についても海外由来のものに大きく依存している。海外のセキュリティ製品のベンダーは、世界中から集めた一次情報を基に新たな技術・サービスを生み出す一方、相対的にシェアの小さい国内のベンダーは、十分なセキュリティ情報を収集できておらず、製品の開発が進んでいないためである。

こうした海外製品への依存構造は、日本特有のサイバー攻撃への対応の遅れや国際競争力の低下といったサイバー安全保障や経済安全保障上の様々な問題につながることが懸念されている（図表Ⅱ-2-5-5）。

図表Ⅱ-2-5-5　国産セキュリティ技術の必要性

総務省では、これらの構造的な課題に対応するため、NICTと連携し、NICTが培ってきた技術・ノウハウを中核として、産官学連携を促進する取組であるCYNEX（サイネックス：CYbersecurity NEXus）を2021年度から実施している。CYNEXには、2025年度末時点で107組織が参画しており、2026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、サイバー脅威情報の収集・分析・共有や国産セキュリティ技術の開発を支援し、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していく。

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/r08/html/datashu.html#f00383（データ集）

また、特に、サイバー脅威情報の収集・分析を強化する取組として、CYXROSS（サイクロス：CYNEX XROSS organ observatory project）を実施している。これは、政府機関等の端末にNICTが開発したセンサーを導入し、収集した情報の分析を実施するものであり、サイバーセキュリティ対策に必要な様々な技術・情報・ノウハウを得ることを目的としている。2023年度から実証事業として実施してきたところであり、2025年にサイバー対処能力強化法等が成立し、同年に改正サイバーセキュリティ基本法が施行されたことを受け、2025年12月から本格的に事業を開始した。

総務省では、CYXROSSによる脅威情報の収集・分析の強化を含め、国産技術を核とした産官学連携のエコシステムを強化し、我が国自らの力によるサイバー対応能力の確保に取り組んでいく。

関連データ　国産技術を核としたサイバー対処能力向上エコシステム

URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r08/html/datashu.html#f00384（データ集）

3 AIのセキュリティ対策の推進

生成AIをはじめとするAI技術は急速に発展しており、あらゆる領域で社会実装が急速に進んでいる。このような中、AI自体へのサイバー攻撃によって、例えば、AIから不正な出力が行われたり、AIを組み込んだシステムが停止したりすれば、社会経済活動に多大な影響を生じさせかねない。

こうしたことを背景に、総務省では、2025年9月から、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」の下に「AIセキュリティ分科会」を設置し、AI開発者及びAI提供者におけるAIへの脅威に対する技術的対策の検討を行った。2026年3月には、当該分科会の取りまとめ（2025年12月公表）を踏まえ、「AIのセキュリティ確保のための技術的対策に係るガイドライン」[*17]を策定・公表した。

また、総務省では、NICTの「AIセキュリティ研究センター（CREATE）」を通じて、北米の5組織との共同研究を実施しており、サイバー攻撃に対するAI自身のセキュリティ検証の研究開発を推進していくことで、生成AIの安心安全な利用を促進していく。

4 AIの高度化を踏まえたサイバーセキュリティ対策の推進

近年、AI技術は急速な発展を続けており、その活用によりサイバー対処能力の向上が期待される一方、悪用された場合には、サイバー攻撃の規模や頻度が飛躍的に増大するおそれが指摘されるなど、サイバーセキュリティ上の脅威は一層高まっている。特に、米国Anthropic社のClaude Mythos

＊17　AIのセキュリティ確保のための技術的対策に係るガイドライン本編（https://www.soumu.go.jp/main_content/001064122.pdf）
AIのセキュリティ確保のための技術的対策に係るガイドライン別添（付属資料）（https://www.soumu.go.jp/main_content/001064123.pdf）

Previewをはじめとするフロンティア AI モデルでは、脆弱性の発見等のサイバーセキュリティ性能がこれまでの AI モデルを大きく上回っている。

こうした状況を受け、政府は、2026年5月に、AI性能の高度化に対応したサイバーセキュリティ対策を、重要インフラへの対応と脆弱性の発見・修正時の対応の双方の観点から検討するため、関係省庁会議を開催し、政府全体としての対策パッケージ「Project YATA-Shield」[*18]を取りまとめた。また、総務省においても、これを踏まえ、情報通信・地方行政・郵便分野のサイバーセキュリティ確保に関する会合を開催し、林総務大臣から各分野の代表[*19]に対し、経営層のリーダーシップの下、脆弱性の評価や修正パッチの迅速な適用を含むリスクに応じた対応方針を検討し、必要な予算や人員の割当などを行うことなどについて、要請を行った。

今後、AI技術の更なる高度化が見込まれる中、AIの安全かつ適切な活用を推進するとともに、AIを悪用したサイバー攻撃への対処能力の強化を図っていくことが重要である。

5　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組

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

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を十分に得られる機会がない、人材等の経営リソースは不足しているなどの理由により、単独で十分なセキュリティ対策を取ることが困難であったり、また、そもそも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地域でコミュニティが設立されたところである。2025年度は、地域SECUNITYの取組として、セミナー等21件、インシデント対応演習14件、若年層向けCTF（Capture The Flag）2件を実施したほか、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、2026年度も引き続きイベント開催等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：（データ集）https://www.soumu.go.jp/main_sosiki/cybersecurity/localsecunity/index.html

2　テレワークのセキュリティ対策の推進

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。一方で、テレワーク導入企業に対して実施したアンケート[*20]では、テレワーク導入の最大の課題としてセキュリティの確保があげられている。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。2021年5月には、クラウド活用の進展、サイバー攻撃の高度化等、取り巻く環境の変化を踏まえてガイドラインを改定し、実施すべきセキュリティ対策や具体的なトラブル事例等を全面的に見直した。

＊18　https://www.cyber.go.jp/pdf/press/20260518_AI_CS_gaiyou.pdf
＊19　参加団体：一般社団法人ICT-ISAC、一般社団法人電気通信事業者協会、日本放送協会、一般社団法人日本民間放送連盟、一般社団法人日本ケーブルテレビ連盟、全国知事会、全国市長会、全国町村会、地方公共団体情報システム機構、日本郵便株式会社及び国立研究開発法人情報通信研究機構
＊20　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/

また、中小企業等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。

3 無線LANのセキュリティ対策の推進

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サービス等幅広く利用されている。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等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月には、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[*21]。

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」、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。また、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二つの観点から、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おり、2025年度は、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 サイバーセキュリティに関する普及啓発

国民生活や社会・経済活動のあらゆる場面においてインターネットの利用が広がる中、誰もがインターネットを安全に利用できるよう、総務省では「国民のためのサイバーセキュリティサイト」[*22]を開設し、インターネットとサイバーセキュリティの知識や、利用方法に応じたサイバーセキュリティ対策を講じるための基本となる情報を提供している。特に、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てコンテンツを掲載しており、環境の変化に応じて情報の更新を行っている。

6 国際連携の更なる推進

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等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、サイバー攻撃等の脅威は国境を越えて及ぶため、世界全体のサイバーセキュリティのリスクを低減するためには、開発途上国に対する能力構築支援も重要である。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[*23]。さらに、2023年度からは、AJCCBC

＊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/
＊22　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/
＊23　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

の活動で培ったノウハウ等を活用し、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、通信事業者等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）との意見交換会等を開催している。