別紙２

ＩＣＴサイバーセキュリティ政策の中期重点方針

2024 年７月

ＩＣＴサイバーセキュリティ政策分科会

目次

はじめに

社会全体のデジタル化が進展し、人々のデジタル技術の活用が加速する中で、サイバー空間は我々の日常生活や社会経済活動におけるある種の「公共空間」として必要不可欠なものとなっている。2030 年代に向けて、我が国の経済社会が、サイバー空間と実空間が高度に融合した Society 5.0 の実現が進んでいくことが期待され、サイバー空間の重要性が更に高まっていくことが想定される。一方で、サイバー空間上におけるサイバー攻撃の巧妙化・深刻化・組織化が進み、セキュリティリスクが引き続き高まっている状況にあり、さらに、厳しさを増す安全保障情勢や国際関係の変化の加速、生成 AI 等の新たな技術・サービスの急速な普及やサプライチェーンの多様化・複雑化等の動向を踏まえ、我が国のサイバーセキュリティを巡る環境は今後大きく変化していくことが見込まれる。

これらの動向を踏まえ、サイバーセキュリティタスクフォース（座長 情報セキュリティ大学院大学学長 後藤厚宏）では、ICT サイバーセキュリティ政策分科会（主査 情報セキュリティ大学院大学学長 後藤厚宏）を新たに設置し、

- 重要インフラ分野におけるサイバーセキュリティ対策強化
- サイバーセキュリティの基盤となる人材育成及び研究開発
- サイバーセキュリティの確保に向けた国際連携及び普及啓発

に関し、総務省が今後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集中的に検討を行ってきた。

本文書は、これらの検討を経て、「ICT サイバーセキュリティ政策の中期重点方針」として取りまとめたものである。本文書を羅針盤として、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ことを期待する。

第１章　サイバーセキュリティを巡る情勢と対応の方向性

１．サイバーセキュリティを巡る情勢

今やサイバー空間は、あらゆる主体が利用する公共空間となっている。2023 年６月に公表された「2030 年頃を見据えた情報通信政策の在り方」最終答申[1]によれば、2030 年頃には、AI と人間の協働、サイバーとフィジカルの高度な融合、新たな生活・経済活動の場（メタバース）の実現等が期待されている。情報通信技術の進化と普及により、サイバー空間での活動範囲が拡大し、サイバー空間とフィジカル空間が高度に融合・一体化し、サイバー空間が新たな「社会」の一形態となり、これまでの生活空間が拡張される未来が予想される。例えば、AI、ロボットなどや情報通信技術の進化と普及により、多様な分野における省力化・自動化・遠隔化が図られ、物理的制約から解放され効率化・高度化・利便性の向上が図られ、Society5.0 が実現していくことが期待される。

一方で、このようにサイバー空間の重要性が高まり、社会経済活動がこの安定的提供に依存する中で、サイバー攻撃も政府機関や重要インフラのみならず、あらゆる主体が標的となっている。これを踏まえ、平時から官民挙げて我が国全体としてサイバーセキュリティ対策を強化していくことが何よりも重要であり、こうした平時からの取組が、政府全体の方針である我が国におけるサイバー安全保障分野での対応能力の向上や経済安全保障の推進に資するものと考えられる。

特に、サイバー空間の利用はネットワークを通じて行われており、安全・安心な安定的なネットワーク接続を確保していくことは極めて重要である。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政策については、こうしたデジタル化が更に進展する社会を見据えながら、検討を進めていく必要がある。

（１）サイバー攻撃の最近の動向

ア　NICTER の観測等に基づくサイバー攻撃の状況

我が国へのサイバー攻撃の状況を継続的に観測していくことは、適切に状況を把握し官民連携した対策を実施していくことための礎としても重要である。

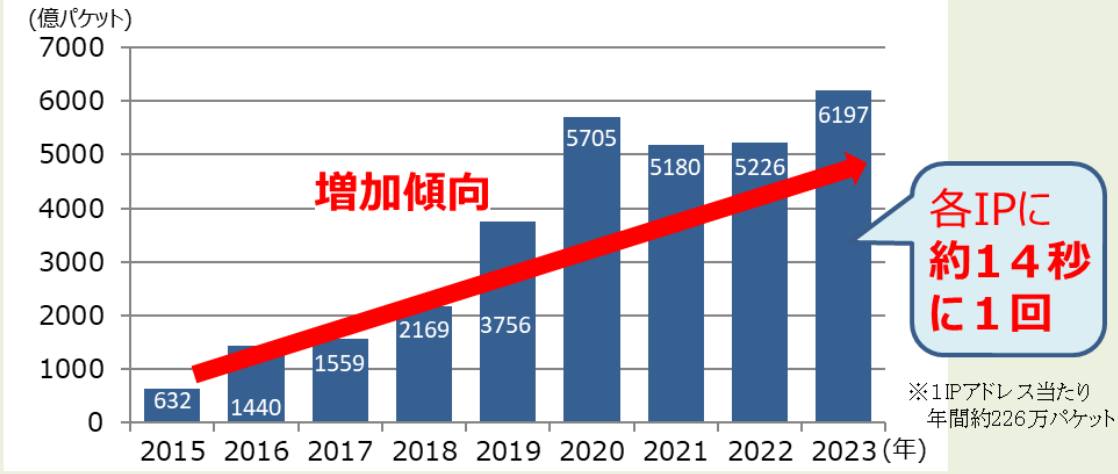
国立研究開発法人情報通信研究機構（NICT）が、「NICTER プロジェクト」で運用している大規模サイバー攻撃観測網（ダークネット観測網）によれば、サイバー攻撃関連通信の観測数は年々増加しており、2023 年は過去最高の約 6,197 億

[1] 「2030 年頃を見据えた情報通信政策の在り方」最終答申（情報通信審議会、2023 年６月）（https://www.soumu.go.jp/main_content/000888370.pdf）

パケット（１IP アドレス当たり約 226 万パケット）を観測した[2]。（図１）この観測パケットのうち、調査目的とみられるスキャンの割合が年々増加している。既に感染した IoT 機器等が新たな攻撃目的を探すための調査を行うものなどを含む未知組織によるスキャンが調査目的のスキャンの中の５割以上を占めている。また、攻撃のターゲットとしては依然としてルーターやネットワークカメラといった IoT 機器を狙ったものが最も多く、特に 2023 年にはモバイル回線に接続された LTE ルーターの感染等も多く観測されている。

IoT 機器へのサイバー攻撃については、公開された脆弱性情報を悪用した攻撃の他、脆弱性に対する修正プログラムの公開前を狙ったゼロデイ攻撃の脅威も依然として高い状況にある。特に脆弱性情報を悪用した攻撃については、最近では IoT 機器だけではなく、多数のクラウドサーバを踏み台とした大規模なサイバー攻撃も観測されており、こうしたクラウドサーバは IoT 機器と比較して１台当たりのリソースが大きいため、より強力なサイバー攻撃を行うことが出来るとの分析[3]もある。

（図１）NICTER で１年間に観測されたサイバー攻撃関連の通信数



※2020年は特異的な事象（大規模なバックスキャッタや大量の調査スキャン）が観測されており、例外的にパケット数が多い。

NICTER 観測レポート 2023 より作成

[2] 「NICTER 観測レポート 2023」（https://csl.nict.go.jp/report/NICTER_report_2023.pdf）

[3] 「Cloudflare Names OVH and Hetzner as Origins of DDOS Attack」（Search Engine Journal）（https://www.searchenginejournal.com/cloudflare-names-ovh-hetzner-origins-of-ddosattack/447991/）

イ　その他のサイバー攻撃の状況

不正アクセス行為については、2023 年における認知件数は 6,312 件であり、前年比で 4,112 件（約 186.9%）増と急増している。不正アクセス後の行為別に内訳を見ると「インターネットバンキングでの不正送金等」（5,598 件）が最も多い[4]。（図２）

ランサムウェアについては、2023 年における被害件数は 197 件と高水準で推移しており、データを暗号化することなくデータを窃取し、対価を要求する手口による被害も新たに 30 件確認されている。その感染経路は、引き続き VPN 機器からの侵入が最も多く、次いでリモートデスクトップからの侵入となっている[5]。（図３・４）

フィッシングについては、2023 年度の報告件数は約 126 万件であり、3 年前の 2021 年度から比べて約 2.1 倍増の過去最多となっている[6]。「フィッシングレポート 2024」[7]によれば、EC サイト大手、クレジットカード会社の他、マイナポイント事務局等の公共サービス、交通系サービスのなりすましが報告されている。また、観測しているメールアドレスで受信したフィッシングメールのうち、平均約 74.9%、最大で 91.9%が「なりすまし」送信メールであった。（図５）

---

[4] 「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」（警察庁・総務省・経済産業省、2024 年３月）（https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00279.html）

[5] 「令和５年におけるサイバー空間をめぐる脅威の情報等について」（警察庁、2024 年３月）（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf）

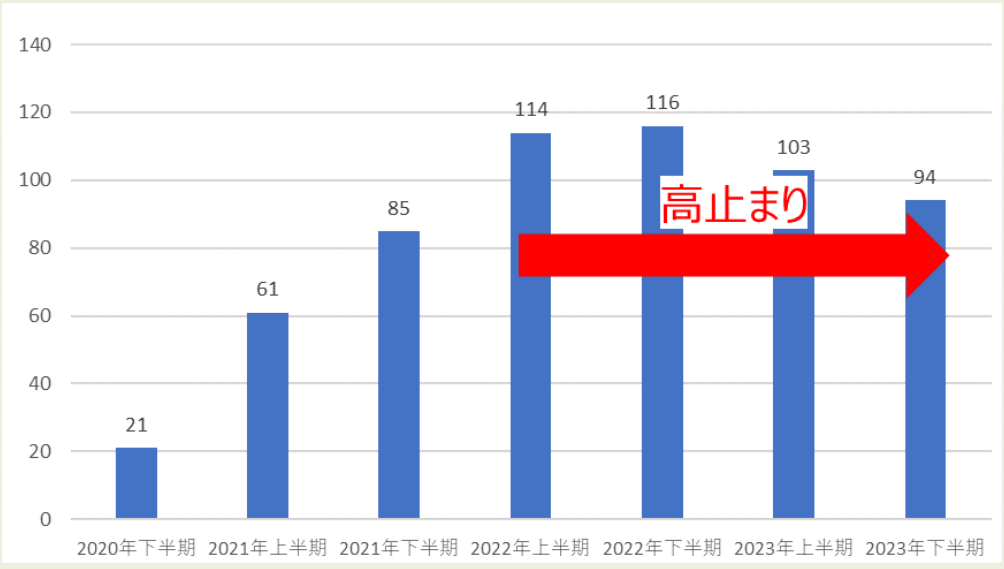
[6] フィッシング対策協議会__HP（https://www.antiphishing.jp/）

[7] 「フィッシングレポート 2024」（フィッシング対策協議会、技術・制度検討ワーキンググループ、2024 年６月）（https://www.antiphishing.jp/report/phishing_report_2024.pdf）

（図２）不正アクセス行為の認知件数

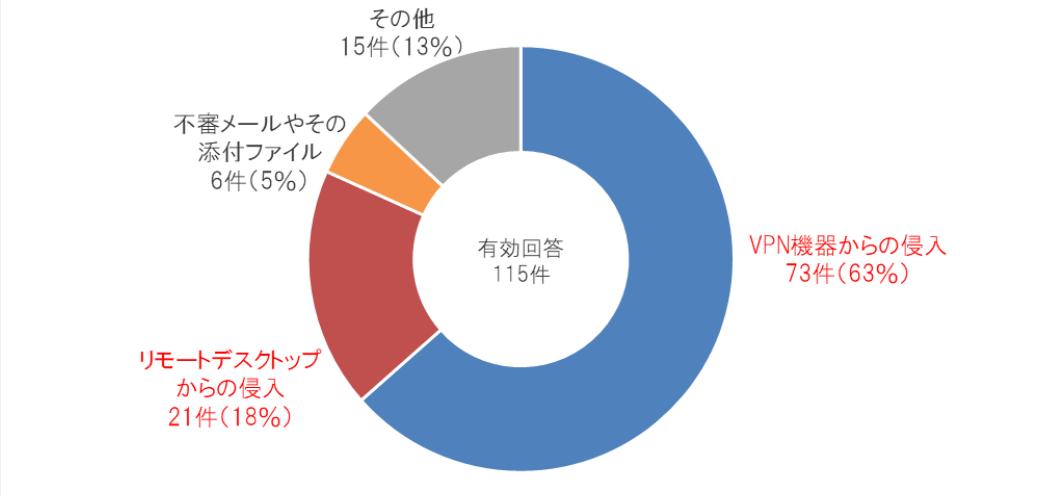
不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況より作成

（図３）ランサムウェア被害の報告件数



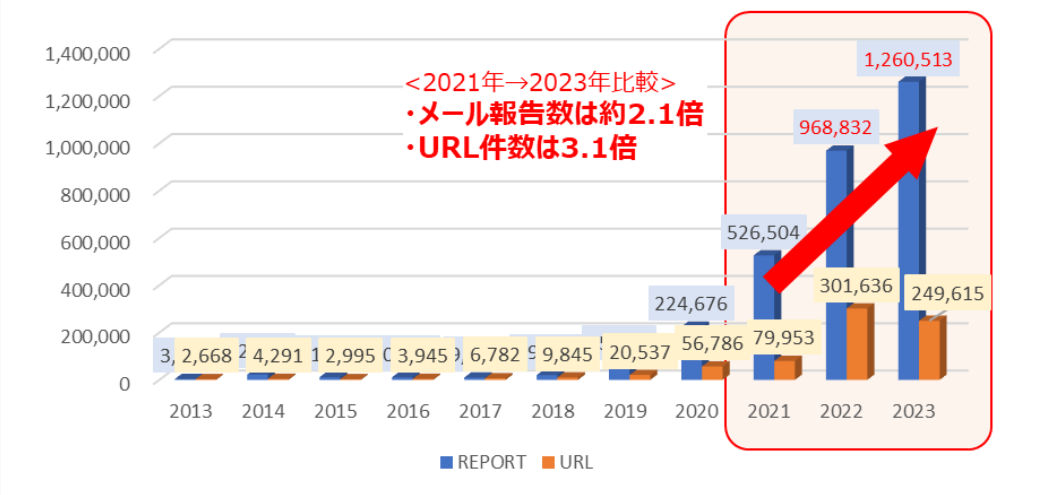
「令和５年におけるサイバー空間をめぐる脅威の情報等について」（令和６年３月　警察庁）より作成

（図４）ランサムウェアの感染経路



「令和５年におけるサイバー空間をめぐる脅威の情報等について」（令和６年３月　警察庁）より作成

（図５）フィッシングメールとフィッシングサイトの報告件数



「フィッシング報告状況」（フィッシング対策協議会）より作成

ウ　最近の国内外における主なサイバー攻撃事案

重要インフラ分野については、2023 年７月に、名古屋港のすべてのコンテナターミナルにおけるコンテナの積卸し作業、搬入・搬出等を一元的に管理する名古屋港統一ターミナルシステムが、ランサムウェアに感染したことにより、約３日間、同ターミナルからのコンテナの搬入・搬出が停止し、物流に大きな影響を与えることとなった。

通信分野においても、2022 年３月～11 月にかけて企業向けネットワークサービスを提供する事業者において、外部からの不正侵入による情報漏洩事案が発生した他、2023 年 11 月に、多くの国民が利用するメッセージサービスを提供する事業者において、業務の再委託先の従業員のＰＣがマルウェア感染が生じたこと等を契機とした不正アクセス等による情報漏洩事案が発生した。

この他、重要インフラ等を対象としたサイバー攻撃については、2023 年以降も、DDoS 攻撃とみられる被害により、政府機関、自治体や民間企業の Web サイトの閲覧障害が累次にわたって発生しており、その中には、緊迫化する国際情勢を背景として、親ロシア系ハッカー集団や反イスラエルを掲げるハクティビストから犯行をほのめかす投稿も SNS 上で確認されている。さらに、DNS 権威サーバを狙ったランダムサブドメイン攻撃によるものとみられる多数のウェブサイトの閲覧障害が断続的に発生した他、2024 年５月には、鉄道事業者の IC 乗車券システムがサイバー攻撃を受け、一時的に当該システムに繋がりにくくなった事案も発生している。

諸外国においても、引き続きランサムウェア攻撃により、行政や医療等の重要インフラ分野においてサービスの提供に重大な支障を及ぼした事案等が発生している。

（２）サイバーセキュリティを巡る主な課題

ア　厳しさを増す国際情勢とサイバー攻撃リスクの高まり

昨今の国家間のパワーバランスと安全保障環境の変化を背景に、国家間競争は激しさと複雑さを増している。そのような中、2022 年２月にロシアがウクライナ侵略を開始し、2023 年 10 月に発生したハマスによるイスラエルに対するテロ攻撃以降、イスラエル・パレスチナ情勢が悪化しており、国際社会の対立構造はより複雑化している。

このような情勢を背景に、安全保障の裾野は半導体や重要鉱物などのサプライチェーンの強靱性確保、重要・新興技術の育成と保護、サイバーセキュリティ、偽情報対策等にまで広がりを見せている。特にサイバーセキュリティに関しては、例えば、トレンドマイクロは、ウクライナへの侵攻に伴うサイバー攻撃について、重要インフラ・システムの破壊攻撃（Sabotage）、機密情報の窃取（Espionage）、世論に影響を与える活動（Influence Operation）、サイバー上のコミュニティによる敵対国への DDoS 攻撃や情報窃取・暴露攻撃（ハクティビストによる活動）の４つの分類に分けて調査を実施している[8]。こうしたサイバー攻撃は、軍事と非軍事の境界を意図的に曖昧にした現状変更の手法である「ハイブリッド戦」の手段の１つとされている。

こうした中で、国家を背景とするグループからの攻撃をはじめとするサイバー攻撃の深刻化・巧妙化が一層進展しており、2023 年５月に、ファイブ・アイズ５ヶ国及びマイクロソフトが、中国を背景とするサイバー攻撃グループ「Volt Typhoon」（ボルトタイフーン）について注意喚起を発出[9]した他、2023 年９月には、警察庁及び NISC が、米国家安全保障局（NSA）、米連邦捜査局（FBI）及び米国土安全保障省サイバーセキュリティ・インフラ庁（CISA）とともに、中国を背景とするサイバー攻撃グループ「BlackTech」（ブラックテック）によるサイバー攻撃に関する合同の注意喚起を発出[10]している。

このように厳しさを増す国際情勢をしっかりと念頭に置きつつ、重要インフラをはじめとするサイバーセキュリティ対策の強化に取り組むとともに、国際連携を更に推進していくことが喫緊の課題となっている。

---

[8] 「ウクライナ侵攻開始から１年間のサイバー攻撃を振り返る」（トレンドマイクロ、2023 年３月）（https://www.trendmicro.com/ja_jp/jp-security/23/c/securitytrend-20230322-01.html）

[9] 「People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection」（American's Cyber Defense Agency、2023 年５月）（https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a）

[10] 「中国を背景とするサイバー攻撃グループ BlackTech によるサイバー攻撃について（注意喚起）」（警察庁・内閣サイバーセキュリティセンター、2023 年９月）（https://www.npa.go.jp/bureau/cyber/pdf/20230927press.pdf）

イ　多様化・複雑化するサプライチェーンとアタックサーフェス（攻撃対象領域）の増加

現在では、グローバルバリューチェーンと呼ばれる世界規模での分業体制が多くの分野で見られる。この分業体制により、様々な製品が安く生産できるというメリットがある一方で、様々な地域の多くの企業が生産等に関与することから、新たなリスクの要因ともなり得る。

このようなリスクの例として、委託等の契約関係がある関係者のうち、サイバーセキュリティ対策が不十分な者が踏み台とされ得ることが挙げられており、実際に、（１）ウで述べたように、2023 年 11 月に、多くの国民が利用するメッセージサービスを提供する事業者において、業務の再委託先の従業員のＰＣがマルウェア感染が生じたこと等を契機とした不正アクセス等による情報漏洩事案が発生している。

また、あらゆる分野において、汎用的な機器でハードウェア・システムを構築した上で、ソフトウェアにより多様な機能を持たせることが主流となる中、通信分野においても、5G 等の新たな通信技術の普及とともに、マルチベンダ化やネットワークの仮想化が進展することによりオープンソースソフトウェア（OSS）の利用が急速に拡大している。

さらに、このようなサプライチェーンの多様化・複雑化に加え、クラウドやテレワークの利用拡大等をはじめとするデジタル化の進展に伴って、防御側から見たサイバー攻撃の経路や起点となり得るアタックサーフェス（攻撃対象領域）が増加しており、こうしたリスクに適切に対応するためのセキュリティ対策が求められている。

ウ　セキュリティ人材の確保

サイバー攻撃が大規模化・複雑化・巧妙化し、SOC 等のセキュリティ対策業務の負荷が増大する中で、それを担うセキュリティ人材の確保は極めて重要である。他方、我が国については、約９割の企業でセキュリティ人材が不足しており、その割合は諸外国よりも高いという調査結果[11]もある。また、ISC2（国際情報システムセキュリティ認証コンソーシアム）の調査によれば、我が国のセキュリティ人材は約 11 万人不足[12]していると推計されている。人材育成の取組を更に拡

---

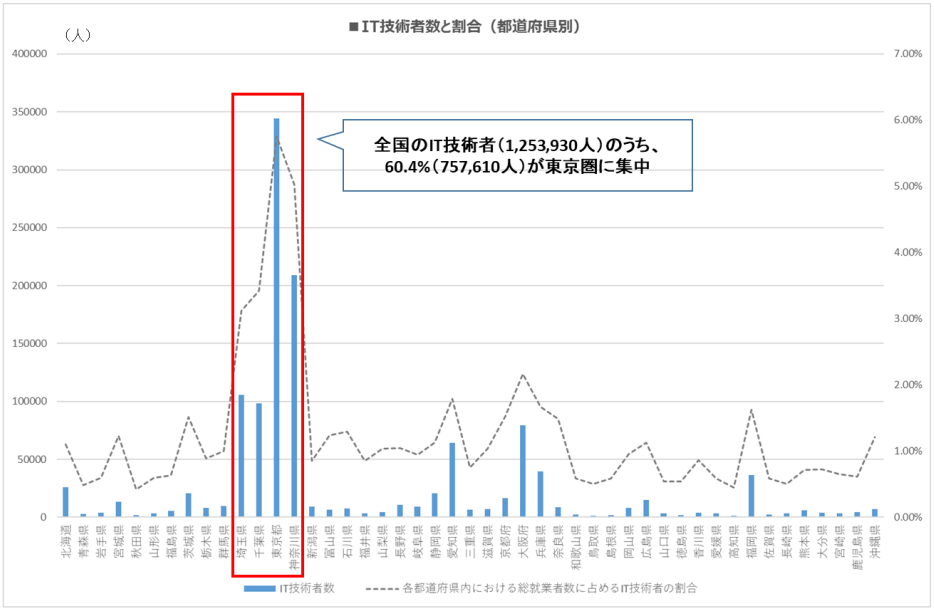
[11] 「NRI Secure Insight 2023　～企業における情報セキュリティ実態調査～」によれば、セキュリティ人材が不足していると回答した企業の割合は、米国が 8.5%、豪州が 8.2%、日本が 91.7%であった。（https://www.nri-secure.co.jp/download/insight2023-report）

[12] 「How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce」（ISC2 CYBERSECURITY WORKFORCE STUDY）（https://3sgplus.com/wp-content/uploads/2024/02/ISC2_Cybersecurity_Workforce_Study_2023.pdf）

充する等により、我が国の自律的なセキュリティ対処能力を強化することが喫緊の課題となっている。

さらに、DX を担うデジタル人材については、数の不足とともに、大都市（特に東京圏）への偏在が指摘されている（図６）ことから[13]、セキュリティ人材の偏在についても同様の傾向にあると考えられる。このため、特に地域を対象としたセキュリティ人材育成や、その裾野を広げていくための普及啓発活動についてもあわせて取組を強化していく必要がある。

（図６）デジタル人材の都道府県別の割合



資料：総務省「国勢調査」（令和２年）により作成。
IT技術者＝職業（小分類）における「システムコンサルタント・設計者」及び「ソフトウェア作成者」及び「その他の情報処理・通信技術者」の数を合算。
就業者総数＝15歳以上就業者数

活力ある地域社会の実現に向けた情報通信基盤と利活用の在り方に関する懇談会 資料 3-1（事務局資料）より抜粋

エ　生成 AI 等の新たな技術への対応

サイバーセキュリティを中長期的な視点で見た場合、新技術への対応は極めて重要な課題である。特に AI 技術については、2022 年 11 月に ChatGPT が公開されて以降、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、サイバーセキュリティのリスクが新たに指摘されている。

[13] 活力ある地域社会の実現に向けた情報通信基盤と利活用の在り方に関する懇談会（第３回）資料３－１（2024 年３月）（https://www.soumu.go.jp/main_content/000934671.pdf）

また、量子コンピュータも今後急速に発展することが見込まれる中で、従来型の暗号が解読されるリスク（危殆化）が顕在化することが指摘されている[14]。こうした新技術の進展に対して、セキュリティ確保の観点から的確に対応することが求められている。

[14] 「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」（国立研究開発法人情報通信研究機構、独立行政法人情報処理推進機構、2023 年３月）（https://www.cryptrec.go.jp/report/cryptrec-gl-2004-2022.pdf）

２．政府の主な動きと総務省としての対応の基本的な方向性

（１）政府の最近の主な動き

ア　国家安全保障戦略

2022 年 12 月に「国家安全保障戦略[15]」が閣議決定された。同戦略に基づき、我が国の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、国や重要インフラ等の安全を確保するため、重要インフラ事業者等との情報共有、政府による対処調整、支援の強化をはじめとする「能動的サイバー防御」に必要な措置の実施や、総合調整の司令塔となる新たな組織の立ち上げ、それらに必要となる法整備等に向けた検討を進めることとされている。

特に、「能動的サイバー防御」については、武力攻撃に至らないものの、国や重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合に、可能な限りこれを未然に排除するとともに、そのようなサイバー攻撃が発生した場合の被害の拡大を防止するために導入するものであるとされている。

2024 年６月からは、「サイバー安全保障分野での対応能力の向上に向けた有識者会議」において、「能動的サイバー防御」の導入をはじめとする我が国のサイバー安全保障分野での対応能力の向上を実現するための方策について検討が進められている。

イ　重要インフラのサイバーセキュリティに係る行動計画の改定

2023 年７月に発生した名古屋港コンテナターミナルのシステム障害を踏まえ、国土交通省における検討[16]を経て、2024 年３月８日に「重要インフラのサイバーセキュリティに係る行動計画」を改定し、新たに「港湾」が重要インフラとして追加された[17][18]。

---

[15] 「国家安全保障戦略」（国家安全保障会議決定、2022 年 12 月）（https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf）

[16] コンテナターミナルにおける情報セキュリティ対策等検討委員会（https://www.mlit.go.jp/kowan/kowan_mn2_000006.html）

[17] 「重要インフラのサイバーセキュリティに係る行動計画」（2024 年３月サイバーセキュリティ戦略本部改定）（https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2024.pdf）

[18] 2024 年５月に成立した改正経済安全保障推進法に基づき、基幹インフラ事業として「港湾運送」が追加された。

ウ　経済安全保障推進法の施行

2022 年５月に経済安全保障推進法[19]が成立し、基幹インフラ役務の安定的な提供の確保に関しては、特定社会基盤事業者は特定重要設備の導入等に当たって事前に計画書を届け出なければならないこととされ、主務大臣はその審査等を行うこととされている。総務省においても 2023 年 11 月に電気通信・放送・郵便分野における特定社会基盤事業者をそれぞれ指定[20]した上で、2024 年５月から制度運用を開始した。

エ　AI 事業者ガイドラインの策定や AISI の設立

2024 年４月、政府は、AI 開発・提供・利用にあたって必要な取組についての基本的な考え方を示す「AI 事業者ガイドライン[21]」を策定・公表した。同ガイドラインは、近年の生成 AI の普及を踏まえ、既存のガイドラインに必要な改訂を行ったものである。

同ガイドラインにおける 10 の共通指針の１つに「セキュリティの確保」があり、AI の振る舞いについて、不正操作によって意図せぬ変更や停止が生じることのないよう、セキュリティを確保することが重要との方針の下、開発者・提供者・利用者向けに遵守すべき事項を定めている。（図７）

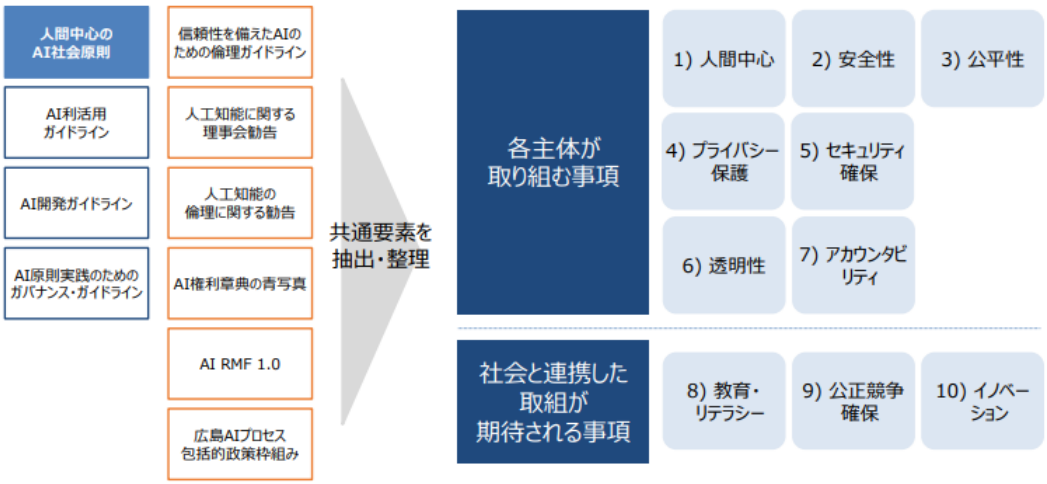
また、政府は、AI の安全性に対する国際的な関心の高まりを踏まえ、AI の安全性の評価手法の検討や、それに係る国際連携等を担う機関として、2024 年２月に「AI セーフティ・インスティテュート（AISI）」を設立した。

---

[19] 令和４年法律第 43 号。
[20] 総務省告示第 388 号。
[21] 「AI 事業者ガイドライン（第 1.0 版）」（総務省・経済産業省、2024 年４月）（https://www.soumu.go.jp/main_content/000943079.pdf）

（図７）ＡＩ事業者ガイドラインにおける「共通の指針」

- AIの活用による目指すべき社会の実現のために各主体が連携して取り組む内容を原則としてまとめた上で、「共通の指針」として整理する
- 「共通の指針」は、「人間中心のAI社会原則」を土台としつつ、諸外国における議論状況や、新技術の台頭に伴い生じるリスクへの対応等を反映している
- その結果、各主体が取り組む事項、及び社会と連携して取り組むことが期待される事項に分類される



「AI 事業者ガイドライン（1.0 版）概要」より抜粋

（２）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政策の基本的な方向性

今やサイバー空間は、あらゆる主体が利用する公共空間となっており、サイバー攻撃も政府機関や重要インフラのみならず、あらゆる主体が標的となっている。これを踏まえ、平時から官民挙げて我が国全体としてサイバーセキュリティ対策を強化していくことが何よりも重要であり、こうした平時からの取組が、政府全体の方針である我が国におけるサイバー安全保障分野での対応能力の向上や経済安全保障の推進に資するものと考えられる。

総務省においては、サイバー空間の基盤となる情報通信ネットワークの安全性・信頼性の確保に加え、通信分野と同様に重要インフラであり、情報伝達手段としての重要な役割を担う放送分野や、地域住民に必要不可欠な行政サービスの提供を担う地方公共団体分野において、セキュリティ確保に向けた施策を推進することが求められている。

また、１．で述べたように、2030 年頃には、AI と人間の協働、サイバーとフィジカルの高度な融合、新たな生活・経済活動の場（メタバース）の実現等が期待されている。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政策については、こうしたデジタル化が更に進展する社会を見据えながら、検討を進めていく必要がある。

これらの視点を踏まえ、2030 年頃に想定される社会も見据えつつ、１で述べたようなサイバー攻撃の動向やサイバーセキュリティを巡る環境の変化に的確に対応するため、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政策について、

１．重要インフラ等におけるサイバーセキュリティの確保
２．サイバー攻撃対処能力の向上と新技術への対応
３．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
４．国際連携の更なる推進

の４つを重点事項とした上で、「ＩＣＴサイバーセキュリティ政策の中期重点方針」として示していくこととする。

第２章　ＩＣＴサイバーセキュリティ政策の中期重点方針

１．重要インフラ分野等におけるサイバーセキュリティの確保

（１）通信

サイバー空間があらゆる主体が利用する公共空間となり、デジタル化を支える情報通信ネットワークは今や国民生活や経済活動の重要かつ不可欠な基盤となっている。第１章で述べたように、国際情勢が厳しさを増し、サイバーセキュリティの脅威が高まる中で、サイバー攻撃により情報通信ネットワークの機能に支障が生じたり、もしくはその機能が停止した場合には、社会・経済や安全保障の面で多大な影響を及ぼすおそれがあり、そのセキュリティの確保は喫緊の課題である。

これを踏まえ、情報通信ネットワークに大きな影響を及ぼすようなサイバー攻撃に悪用される IoT ボットネットについて総合的な対策を進めるとともに、安全・安心な通信サービスの利用に向けたセキュリティ対策やサプライチェーン対策、通信事業者におけるサイバー攻撃による情報漏洩等の事案への対応等について的確な取組を進めていくことが必要である。

ア　総合的な IoT ボットネット対策

DDoS 攻撃をはじめとする情報通信ネットワークの機能に支障を及ぼしうるサイバー攻撃については、マルウェアに感染した多数の IoT 機器等が踏み台となり、「攻撃インフラ」となって悪用されていることが問題となっている。

こうした大規模サイバー攻撃は、主に①IoT 機器にマルウェアを感染させ、攻撃の踏み台として悪用できるようにした攻撃インフラ（IoT ボットネット）の拡大と、②C&C サーバからネットワークを通じて IoT ボットネットに指令を出し、攻撃先への大量通信の送信により攻撃を実行、という２つの段階がある。（図８）

このようなサイバー攻撃に十分に対応するためには、脆弱性のある IoT 機器を減らしていくための端末側の対策及び、IoT ボットネットに対して指令を出す C&C サーバを検知・対処するためのネットワーク側の対策を双方から実施し、IoT ボットネットを縮小させていくことを目指す総合的な対策を推進していくことが必要である。

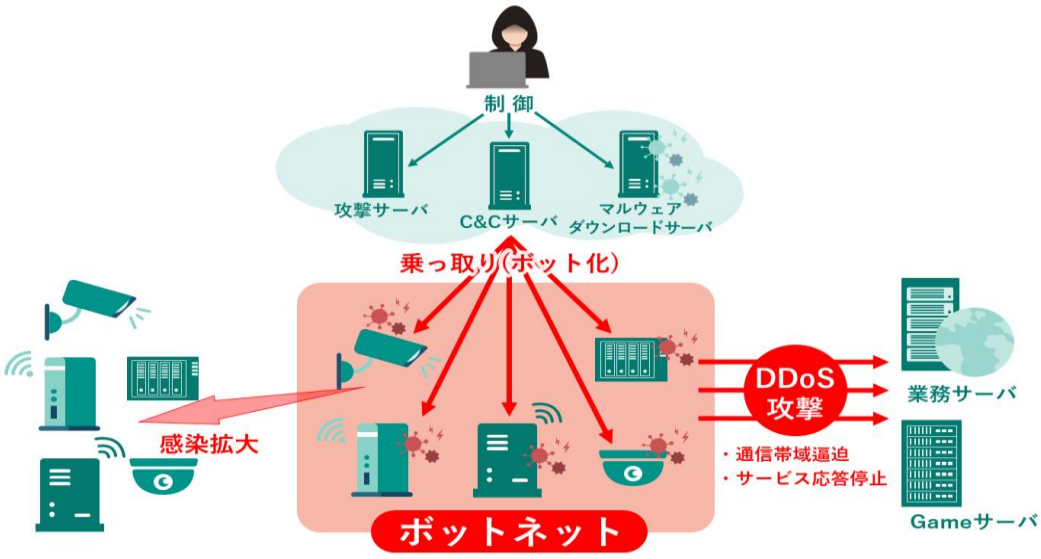
・新 NOTICE（端末側の対策）

【現状】

2018 年に NICT 法を改正[22]し、５年間の時限措置（不正アクセス禁止法の例外）として、NICT が、ID・パスワードに脆弱性のある IoT 機器を調査して ISP に通知を行い、ISP が個別の利用者への注意喚起を行う取組（NOTICE）を 2019 年２月に開始した。こうした NOTICE の取組により、IoT 機器の脆弱性解消に一定の成果はあったものの、依然として ID・パスワードに脆弱性のある IoT 機器を標的としたサイバー攻撃が発生している他、最近ではファームウェアの脆弱性を狙ったサイバー攻撃も増加している。

これを踏まえ、2023 年 12 月に NICT 法を改正[23]し、NICT が行う IoT 機器の調査について継続して実施可能とするとともに対象の拡充を行った。この法改正等を踏まえて、NOTICE をルータ等の IoT 機器のセキュリティ向上を推進し、IoT 機器を悪用したサイバー攻撃の発生等を防ぐためのプロジェクトとして再定義し、2024 年４月から、従来の取組に加え、ファームウェア脆弱性の調査と対処要請を新たに開始している。また、IoT 機器の適正な管理に関する周知啓発活動を強化するとともに、IoT 機器メーカや SIer 等との連携により、利用者への注意喚起のみに依らない多様な関係者による対処を推進している。（図８・９）

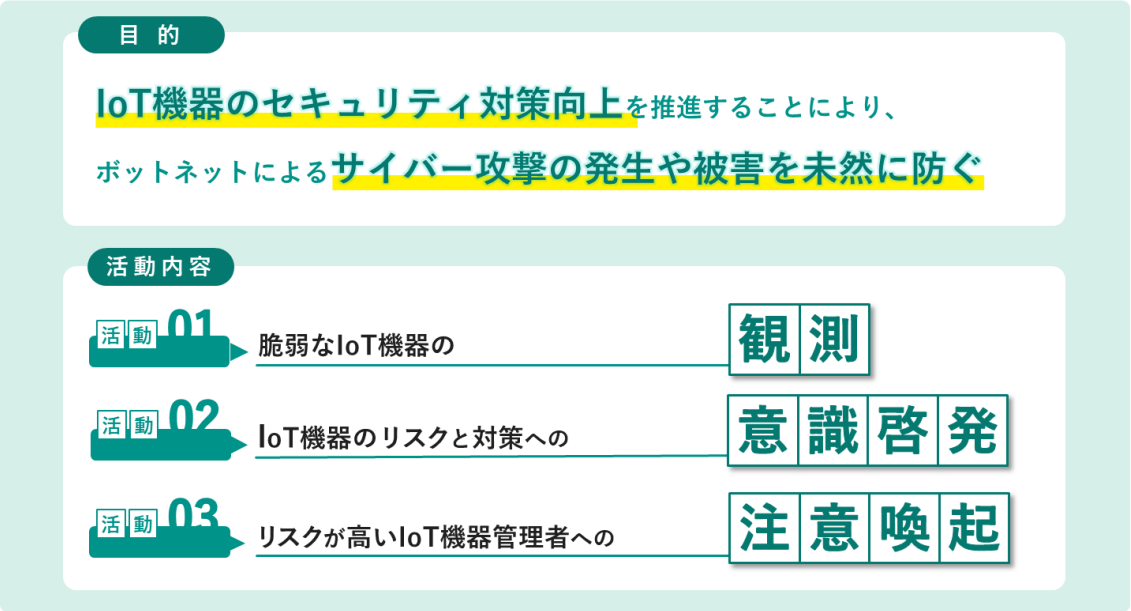
（図８）ボットネットについて



ICT サイバーセキュリティ政策分科会 資料 7-2（事務局資料）より抜粋

[22] 平成 30 年法律第 24 号。
[23] 令和５年法律第 87 号。

（図９）新 NOTICE の活動の３本柱



ICT サイバーセキュリティ政策分科会 資料 7-2（事務局資料）より抜粋

【今後の取組の方向性】

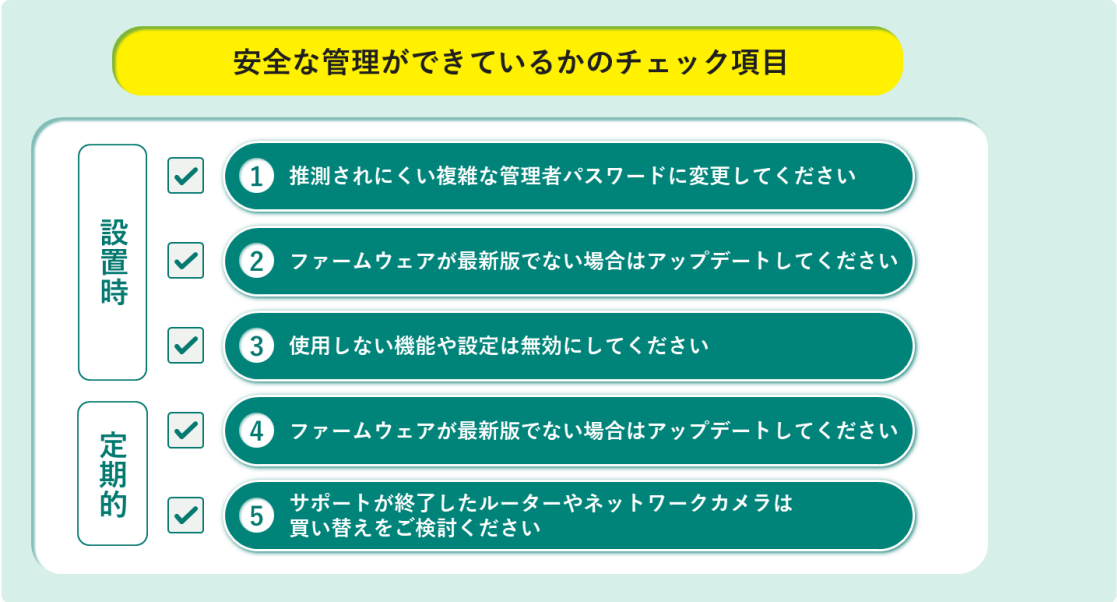
IoT 機器メーカ等の多様な関係者と更に連携を深めつつ、以下の取組を継続して実施し、ルーター等の乗っ取りの予防対策及び乗っ取られたルーター等のセキュリティ対策の見直しを推進することにより、IoT ボットネットの活動を抑制し、これに起因するサイバー攻撃の発生と被害の軽減を目指していくことが求められる。

- ルーター等の管理者向けに、ルーター等の乗っ取りリスクと基本的な安全対策の周知啓発の実施（図 10）
- ルーター等を悪用したサイバー攻撃や、高リスク脆弱性を有するルーター等の調査（図 11）
- 高リスク脆弱性を有するルーター等については、関係者の連携による対処を推進

さらに、NOTICE で得られた NICT の IoT 機器調査に係る知見・ノウハウを活用することにより、高度な分析情報の提供や重要インフラを対象としたアタックサーフェス調査に取り組む等、NOTICE のみならず我が国のセキュリティ対処能力の向上に広く貢献していくことを目指すことが重要である。

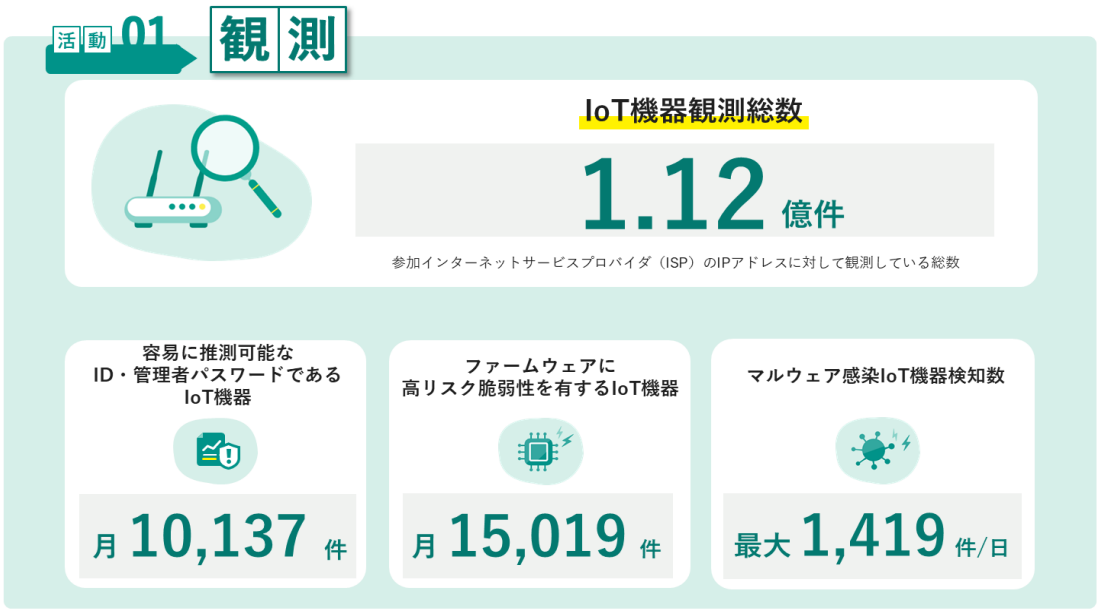
これらの取組に加え、IoT 機器のセキュリティ対策においては、「セキュリティ・バイ・デザイン」・「セキュリティ・バイ・デフォルト」の重要性が高まっていることも踏まえ、適切な IoT 機器のセキュリティ基準の在り方について、NOTICE の取組や経済産業省で検討を進めている IoT 製品に対するセキュリティ適合性評価制度の動向等を踏まえつつ不断に検討することが必要である。

（図 10）IoT 機器の管理者向けのチェック項目



ICT サイバーセキュリティ政策分科会 資料 7-2（事務局資料）より抜粋

（図 11）IoT 機器の観測状況



ICT サイバーセキュリティ政策分科会 資料 7-2（事務局資料）より抜粋

・C&C サーバの検知・対処の推進（ネットワーク側の対策）

【現状】

フロー情報の分析による C&C サーバである可能性が高い機器の検知について、正当業務行為として法的整理を実施した上で、2022～2023 年度の 2 年間のプロジェクトとして、電気通信事業者におけるフロー情報[24]の分析による C&C サーバ[25]検知技術の有効性の検証や、事業者間の情報共有に当たっての課題整理のための実証事業を実施してきた。（図 12・13）

同事業によって、分析機能の強化や、能動的分析等の新たな手法の導入により、技術的に信頼度の極めて高い C&C サーバリストの作成に成功している。また、この分析の結果として、C&C サーバの挙動状況、国別やマルウェアファミリ等の属性も把握できている。また、分析結果の中には、オープン情報よりも早く検知された C&C サーバが数多く確認されており、フロー情報分析によって迅速な対処につながる可能性が期待される。さらに、フロー情報分析事業者の検出共通性は高くないことが判明しており、多くの事業者が分析に参画することで、より多くの C&C サーバが検知できる可能性がある。

【今後の取組の方向性】

C&C サーバの生存期間が短いこと等も踏まえ、シード情報の拡充、AI 技術の更なる活用、分析作業の自動化、能動的分析機能の拡充や外部プロジェクトとの連携等を進め、分析機能の強化や分析オペレーションの高度化を図り、引き続きより迅速かつ精緻な C&C サーバリストの作成を目指すとともに、分析事業者の拡大に一層取り組み、統合的な分析を進めることで C&C サーバの検出網羅性の向上を目指していくことが必要である。

C&C サーバリストに基づく対策については、まずは対策トライアルから始め、効果を検証しつつ、必要に応じて制度改正も視野に入れながら、対策手法の改善を図っていくことが必要である。

また、分析事業者が検知した C&C サーバ情報の収集・精査・事業者への共有等、ハブ的な機能を担う統合分析対策センターについては、持続的な運用が可能となるように体制面等も含めて検討を進めることが必要である。

これらの事項について中長期的に取組を進めることにより、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

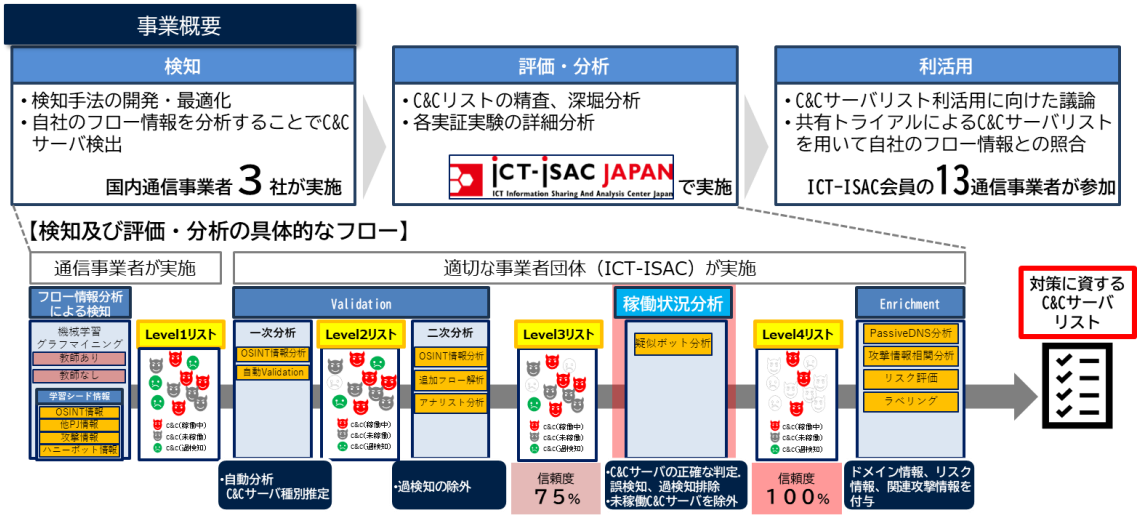
---

[24] 通信トラヒックに係るデータのうち、IP アドレス及びポート番号等のヘッダ情報並びにルーターでヘッダ情報を抽出する際に付与されるタイムスタンプ等の情報（通信内容は含まない）。

[25] マルウェアに感染した端末に攻撃指令通信を送信する Command and Control サーバの略。

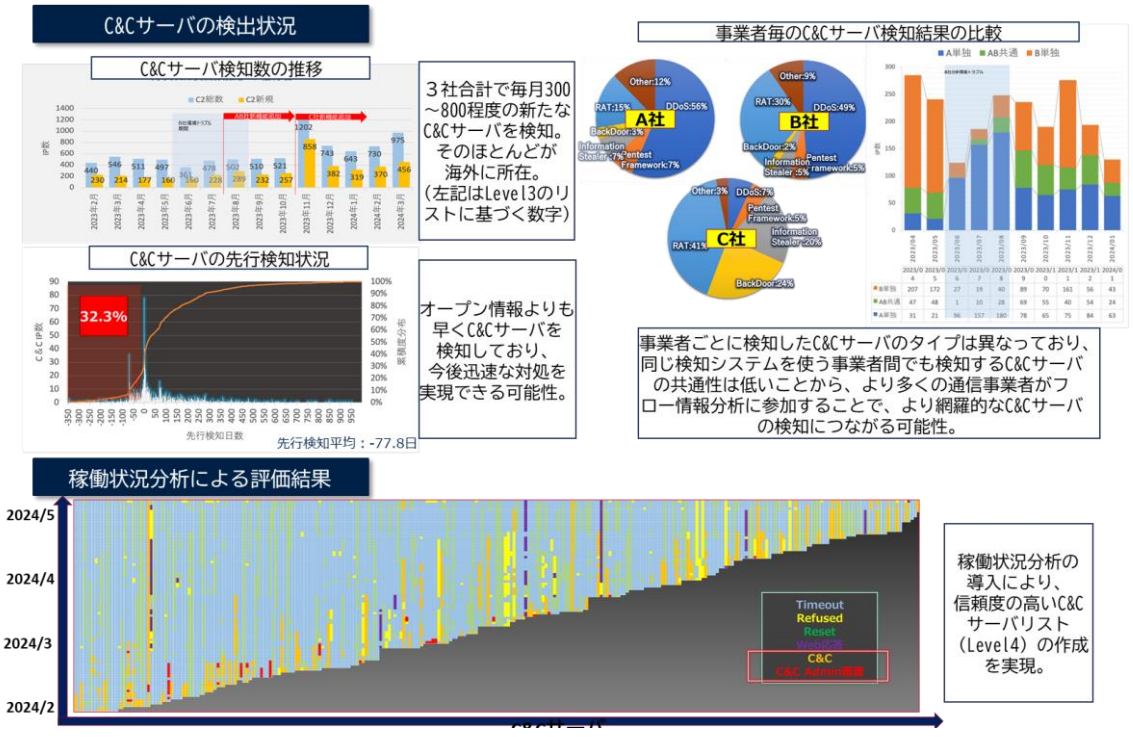
現することで、ボットネットの縮小を目指していくことが求められている。

（図 12）フロー情報分析による C&C サーバ検知の取組の概要



ICT サイバーセキュリティ政策分科会 資料 7-4（NTT コミュニケーションズ資料）等より事務局作成

（図 13）フロー情報分析による C&C サーバ検知の成果



ICT サイバーセキュリティ政策分科会 資料 7-4（NTT コミュニケーションズ資料）等より事務局作成

イ　安全・安心な通信サービスの利用に向けたセキュリティ対策の推進

・スマートフォンアプリのセキュリティ対策の推進

【現状】

スマートフォン等のモバイルサービスは、あらゆる社会・経済活動を支えるインフラとして、また、国民生活に不可欠なライフラインとして重要な役割を果たしている。他方で、スマートフォンに搭載されているアプリについては、利用者の意図しない利用者情報の取扱いが生じ得るものとして、透明性が不十分なアプリ、脆弱性があるアプリ及び不正なアプリが指摘されており、このようなアプリに起因するセキュリティリスク等に的確に対応する必要がある。

これまで、利用者が安心・安全にアプリを利用できるように、総務省においてスマートフォン利用者情報取扱指針等を含む「スマートフォンプライバシーイニシアティブ（SPI）[26]」を策定している他、民間団体もガイドライン等を策定しているが、アプリによる利用者情報の取扱いの実態を把握することには課題がある。

こうしたことを踏まえ、2023 年度より、人気アプリ等を対象に利用者の意図に反したスマートフォンアプリによる情報送信等について技術的な解析を実施することで、我が国のアプリ解析能力水準に係る課題等の整理に取り組んでいる。

【今後の取組の方向性】

SPI について、アプリケーション提供サイト運営事業者等による脆弱性があるアプリや不正なアプリへの対応等、セキュリティの観点を新たに盛り込んでいくとともに、スマートフォンアプリにおけるセキュリティ対策の実態把握等に取り組むことにより、モバイルサービスの提供に不可欠な役割を果たしているスマートフォンアプリについて、利用者情報が適切に保護される環境を目指していくことが必要である。

---

[26] 「スマートフォン プライバシー イニシアティブ Ⅲ」（総務省、2017 年７月）（https://www.soumu.go.jp/main_content/000532174.pdf）

・ネットワークセキュリティ認証技術の導入促進

【現状】

RPKI[27]や DNSSEC[28]、DMARC[29]等のネットワークセキュリティ認証技術については、情報の窃取・改ざん、不正アクセス、なりすましやフィッシング等、インターネットの脆弱性を悪用し、通信サービスの安全・安心な利用を脅かすようなサイバー攻撃に対する有効な対策技術であり、国際標準化もされているものの、諸外国と比較して我が国の導入率が低いことが課題となっている。

このため、2022 年度より、RPKI や DNSSEC、DMARC 等のネットワークセキュリティ認証技術の導入における技術的な課題に関する調査・実証を実施し、その結果を踏まえ、今年度の出来るだけ早い時期に各認証技術を適切かつ円滑に導入・運用するためのガイドラインを新たに策定することとしている。

【今後の取組の方向性】

RPKI や DNSSEC、DMARC 等のネットワークセキュリティ認証技術について、技術動向や企業の導入状況を踏まえつつ、関連ガイドラインの周知啓発に取り組むとともに、ISP をはじめとする企業の対策状況の可視化を進めることにより、各認証技術の導入を持続的に促進する枠組の検討に取り組んでいくことが必要である。

ウ　通信分野におけるサプライチェーン対策の推進

・SBOM の導入促進

【現状】

通信分野においては、仮想化等のネットワーク技術の進展に伴い、オープンソースソフトウェア（OSS）の利用が急速に拡大しており、ソフトウェア・サプライチェーンは、自社開発の専用ソフトウェアの単純な組合せから、多数の OSS 等の複雑な組合せへと変化し、ソフトウェアの構成管理が複雑化している。このため、ソフトウェア部品の脆弱性が確認された場合の対応の迅速化を図る観点から、ソフトウェアを構成する部品名等を一覧化した SBOM（Software Bill of Materials）を導入する必要性が増している。

---

[27] RPKI（Resource Public-Key Infrastructure）：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。

[28] DNSSEC（DNS Security Extensions）：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。

[29] DMARC（Domain-based Message Authentication Reporting and Conformance）：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。

これを踏まえ、通信機器を対象としたSBOMを実際に作成することにより、我が国の通信分野におけるSBOMを導入する上での課題等を整理するとともに、諸外国におけるSBOMに係る動向を調査している。

【今後の取組の方向性】

我が国の通信分野へのSBOM導入に向けた留意事項等を取りまとめる等、経済産業省における取組とも連携しつつ、セキュリティ・バイ・デザインの考え方の下、サプライチェーン全体におけるSBOMの普及やSBOMの効果的なセキュリティ対策への活用の促進に取り組むことで、ソフトウェアの透明性を確保するとともに、OSS等のソフトウェア部品に含まれ得る脆弱性への対応の迅速化を目指していくことが必要である。

・5Gネットワークのセキュリティ確保

【現状】

普及が進む5Gネットワークについては、サプライチェーンリスクにも対応したセキュリティ確保を図るため、2022年に「5Gセキュリティガイドライン」（第１版）[30]を策定・公表し、本ガイドラインをベースにITUにおける勧告化に取り組んでいる。

【今後の取組の方向性】

5Gセキュリティについては、国際標準化に関する議論の最新動向等も踏まえつつ、O-RANの海外展開にも貢献する観点から、継続してガイドラインのアップデートに取り組むとともに、Beyond5G/6Gについて、国際標準化も含めて我が国が先導的な役割を果たせるようセキュリティ分野においても貢献をしていくことが必要である。

エ　最近の通信事業者における情報漏洩などの事案を踏まえた対応

【現状】

2022年３月～11月にかけて企業向けネットワークサービスを提供する事業者において、外部からの不正侵入による情報漏洩事案が発生したことを受け、2023年６月に再発防止のための行政指導を実施した。また、2023年11月に、多くの国民が利用するメッセージサービスを提供する事業者において、不正ア

[30] 「5Gセキュリティガイドライン（第１版）」（総務省、2022年４月）（https://www.soumu.go.jp/main_content/000812253.pdf）

クセス等による情報漏洩事案が発生したことを受け、2024 年 3 月及び４月に再発防止のための行政指導を実施した。

【今後の取組の方向性】

デジタル化の進展に伴い、サイバー攻撃による情報漏洩やサービス停止のリスクや社会的影響はますます増大しているところ、社会基盤を担う通信事業者において、企業全体としてのサイバーセキュリティ対策の向上が図られるよう、国として必要な支援及び指導を行っていくことが重要である。

（２）放送

【現状】

放送は、国民生活にとって重要な情報伝達手段であり、極めて高い公共性を有する社会基盤であることから、重要インフラサービスの１つとして位置づけられている。

デジタル化の進展に伴い、今後、放送分野においても、マスター設備（番組送出設備）を中心に放送設備の IP 化・クラウド化・集約化が進むことが想定されている。これを踏まえ、サイバーセキュリティ対策をその内容に含む地上テレビジョン放送等の安全・信頼性に関する技術的条件の見直しに向けた検討を実施し、導入計画が具体化している IP 化について、2023 年 11 月に情報通信審議会から一部答申[31]を受け、2024 年４月に関連規定を整備した。

また、ICT-ISAC 放送 WG において、放送設備サイバー攻撃対策ガイドラインの策定・普及、教育・訓練ツールの作成・配布等に取り組んでいる他、ケーブルテレビについても、中小規模事業者等におけるサイバーセキュリティ対策を推進するため、日本ケーブルラボにおいて、技術者向けのセキュリティに関する情報提供や人材育成支援等を実施しているなど、業界団体の主導による取組が進められている。

【今後の取組の方向性】

放送設備の IP 化を図る場合には、放送事業者において安全・信頼性に関する新たな技術基準に基づくサイバーセキュリティ対策を着実に進めるとともに、放送分野における IP 化・クラウド化・集約化の動向を引き続き注視しながら、必要に応じて技術基準の見直しに向けて検討を不断に行っていくことが必要である。

また、放送分野のサイバーセキュリティ対策を支える人材育成・普及啓発については、民間や業界団体による取組とともに、CYDER や地域 SECUNITY 等の政府の支援策の効果的な活用も進めていくことが必要である。

[31] 地上デジタルテレビジョン放送等の安全・信頼性に関する技術的条件－情報通信審議会からの一部答申－（総務省、2023 年 11 月）（https://www.soumu.go.jp/menu_news/s-news/01ryutsu08_02000298.html）

（３）自治体

【現状】

自治体分野においては、複雑・巧妙化しているサイバー攻撃の脅威により、地方公共団体の行政に重大な影響を与えるリスクが想定されるため、それを担う情報システムにおいては、機密性はもとより、可用性や完全性の確保にも十分配慮した、情報システム全体の強靭性の向上が求められている。地方公共団体の情報システム・ネットワークについても、クラウドサービスの普及を踏まえ、「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[32]」において、クラウドサービスの利用等に対応した必要なセキュリティ対策を示している。

なお、システムの標準化については、2023 年９月に閣議決定された「地方公共団体情報システム標準化基本方針[33]」に基づき、原則として 2025 年度までに基幹業務システムを標準準拠システムに移行することとされている。

また、自治体分野における最も重要なセキュリティ対策の１つが、サイバー攻撃事案への対処及び情報セキュリティの統一的な窓口の役割を担う CSIRT の体制整備であり、さらに CSIRT 機能を継続して維持していくことが必要である。

これを踏まえ、地方公共団体情報システム機構（J-LIS）では、自治体 CSIRT 協議会を運営する立場から、CSIRT の構築・運用支援、対応訓練や分野横断的演習等を実施している他、自治体職員向けにセキュリティも含むデジタル人材育成のための研修プログラムを提供している。また、NICT が実施する実践的サイバー防御演習「CYDER」及び「プレ CYDER」についても、各自治体の受講が進み、未受講自治体数も前年度比で約４割減少している。

【今後の取組の方向性】

今夏以降に改定予定の「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」に基づくセキュリティ対策を着実に推進する。

その際、自治体が利用するクラウドサービスについて、特に SaaS は自治体ごとに多種多様であることを踏まえ、第三者認証を取得したクラウドサービスの利用を推奨する同ガイドラインの趣旨にも鑑み、関係省庁と連携しつつ、ISMAP-LIU 登録サービスを増やしていく取組等により、クラウドサービスを安全・安心

---

[32] 「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（令和５年３月版）」（総務省）（https://www.soumu.go.jp/main_content/000873096.pdf）

[33] 「地方公共団体情報システム標準化基本方針」（総務省、2023 年９月）（https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/c58162cb-92e5-4a43-9ad5-095b7c45100c/f6ea9ca6/20230908_policies_local_governments_outline_03.pdf）

に利用できる環境整備を進めることが必要である。

また、クラウド化や標準化等、自治体の情報システム・ネットワークを巡る今後の大きな環境変化に備えるため、セキュリティ人材育成や CSIRT の体制強化が必要不可欠である。このため、J-LIS や地域 SECUNITY の取組の他、CYDER 等を通じて自治体の CSIRT の能力・成熟度の強化に貢献していくことが必要である。

（４）データ流通基盤

安心・安全なサイバー空間を確保するためには、通信等の重要インフラ分野ではないものの、サイバー空間を支える重要なデータ流通基盤であるクラウドサービスのセキュリティ対策やトラストサービスの推進が求められている。

・　クラウドサービスにおけるセキュリティ対策の推進

【現状】

昨今では、官民問わずクラウドサービスの利用が急速に進み、それに伴うセキュリティ対策の重要性は引き続き高まっている状況にあり、これを踏まえ、2021年９月にクラウドサービス提供事業者向けの「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（第３版）[34]」を策定・公表した。

また、クラウドサービスの設定ミスに起因する情報漏えいや障害といった事故が多発していることを踏まえ、2022 年 10 月に「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[35]」を策定・公表した他、2024 年４月には、利用者向けに本ガイドラインの内容をわかりやすく解説した「クラウドの設定ミス対策ガイドブック[36]」を公表し、クラウドサービスのセキュリティ確保に向けた普及啓発を推進している。

さらに、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るための評価制度である ISMAP については、2021 年より制度の運用を開始し、2024 年５月末日現在、68 サービスが ISMAP クラウドサービスリストとして公開されている。また、2022 年には、リスクの小さな業務・情報の処理に用いる SaaS を対象とした ISMAP for Low Impact Use（ISMAP-LIU）の運用を開始している。

【今後の取組の方向性】

クラウドサービスに係る各種ガイドラインについては引き続き普及啓発に取り組むとともに、必要に応じてガイドラインの見直し等を行うことにより、安心・安全なクラウドサービスの利用を促進することが必要である。

ISMAP については、NISC、デジタル庁、経済産業省と連携しつつ、外部監査の負担軽減、審査の迅速化・明確化及び ISMAP 利用層の拡大等の様々な改善策に

---

[34] 「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）」（総務省、2021 年９月）（https://www.soumu.go.jp/main_content/000771515.pdf）

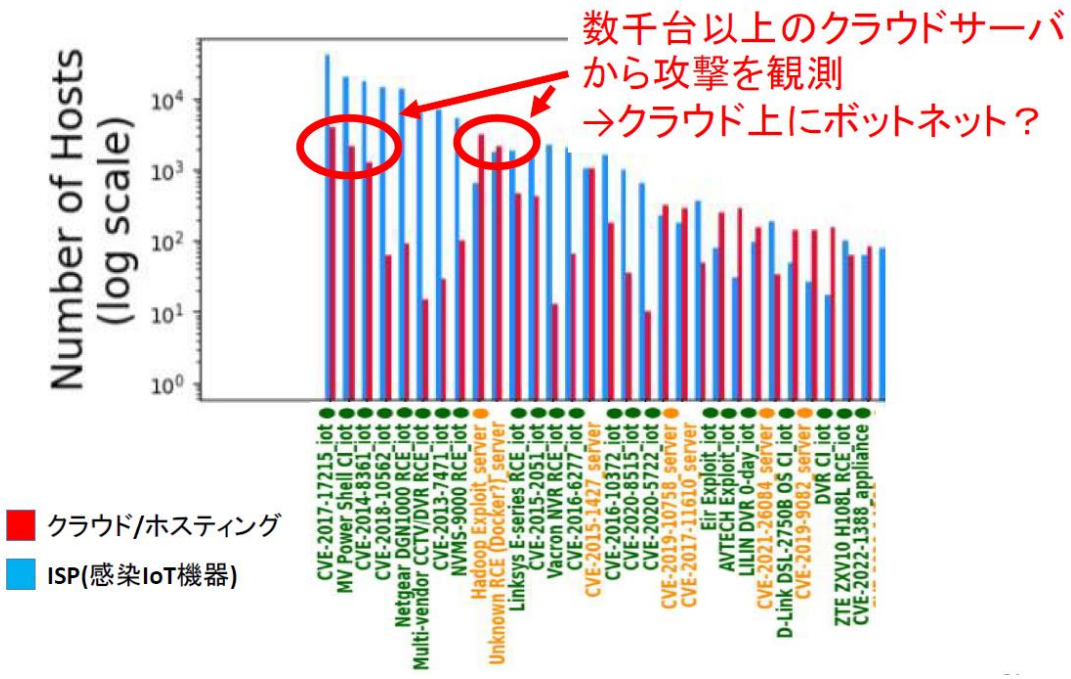
[35] 「クラウドサービス利用・提供における適切な設定のためのガイドライン」（総務省、2022 年 10 月）（https://www.soumu.go.jp/main_content/000843318.pdf）

[36] 「クラウドの設定ミス対策ガイドブック」（総務省、2024 年４月）（https://www.soumu.go.jp/main_content/000944467.pdf）

取り組むことにより、ISMAP・ISMAP-LIU へのクラウドサービス登録を促進し、政府や自治体等において安心・安全なクラウドサービスの利用を推進していくことが必要である。

さらに、クラウドボットネットを利用したサイバー攻撃の増加等、クラウドサービスを取り巻く国内外のセキュリティの最新動向の把握に継続して取り組み必要に応じて対策を講じていくことが求められる。（図 14）

（図 14）クラウドボットネットの実態



ICT サイバーセキュリティ政策分科会 資料 7-1（吉岡構成員資料）より抜粋

・トラストサービス

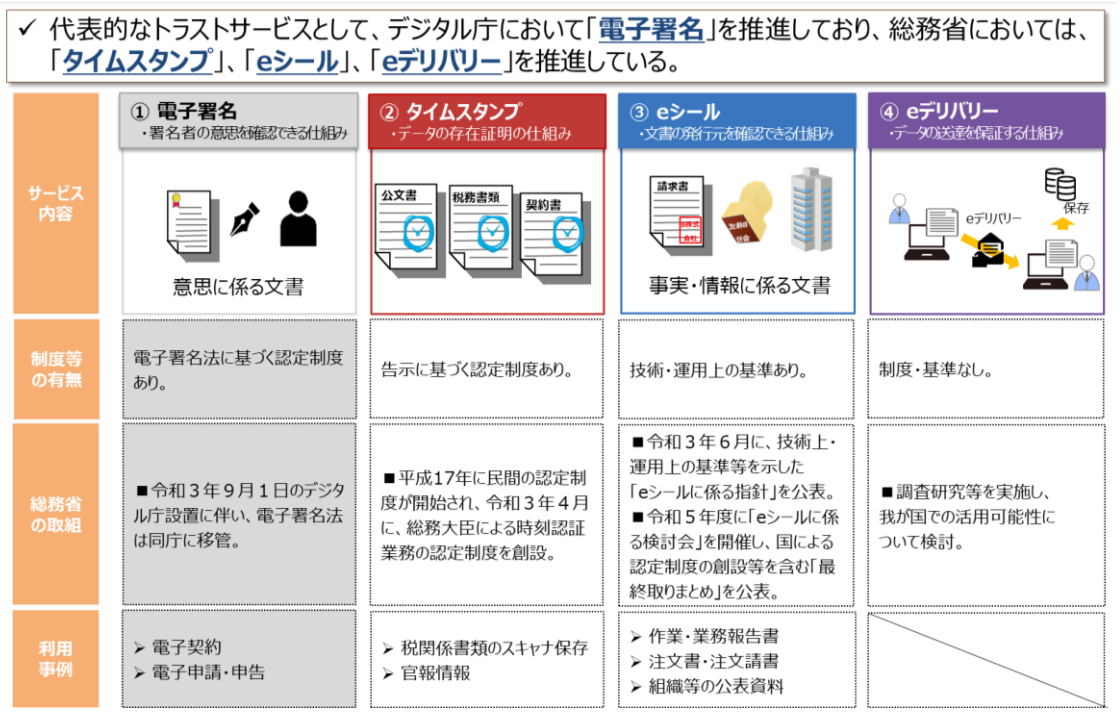
【現状】

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であるトラストサービスは、我が国が推進する「信頼のあるデータ流通（DFFT）」の実現に向けて、データの安全・安心な流通を確保するための基盤として、重要な役割を担うことが期待されている。（図 15）

電子データの発行元を確認できる仕組みである e シールについては、「e シールに係る検討会」を開催し（図 16）、2024 年 4 月に、国による e シールに係る認

定制度の創設等を内容とする「最終取りまとめ」を公表するとともに、技術・運用上の一定の基準を示した「e シールに係る指針（第２版）[37]」を策定した。また、タイムスタンプについては、時刻認証業務（電子データに係る情報にタイムスタンプを付与する役務を提供する業務）に対する認定制度を運用している。

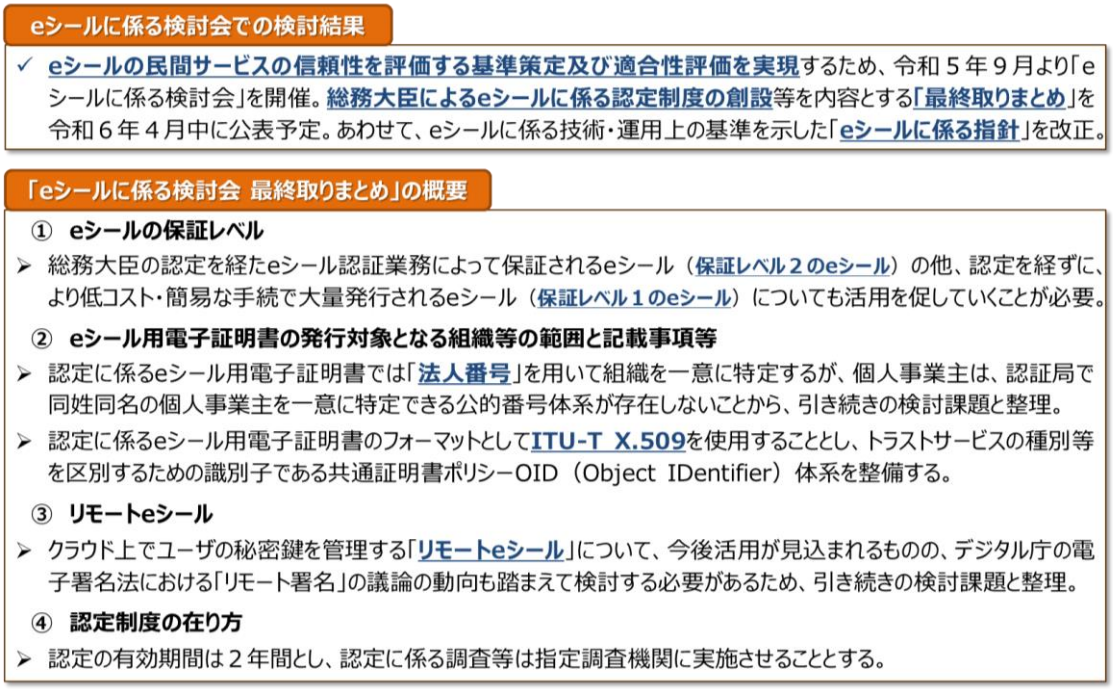
（図 15）代表的なトラストサービス



ICT サイバーセキュリティ政策分科会 資料 5-4（事務局資料）より抜粋

[37] 「e シールに係る指針（第２版）」（総務省、2024 年４月）（https://www.soumu.go.jp/main_content/000942602.pdf）

（図 16）e シールに係る検討会について



ICT サイバーセキュリティ政策分科会 資料 5-4（事務局資料）より抜粋

【今後の取組の方向性】

2024 年度中の e シールに係る認定制度の創設を目指すとともに、タイムスタンプに係る認定制度の的確な運用に取り組む他、欧州の eIDAS2.0 等の諸外国の動向を把握しつつ、各種トラストサービスを普及させることにより、電子データを安心・安全に流通させることができる基盤を整え、DX を推進することが必要である。

２．サイバー攻撃対処能力の向上と新技術への対応

（１）我が国のサイバー攻撃対処能力の向上

サイバーセキュリティは国家の基幹を守るものであり、国際競争力の強化のみならず安全保障上の観点からも、サイバー攻撃対処能力の向上は極めて重要である。他方、我が国のサイバーセキュリティ製品・サービスは、海外製品や海外由来の情報に大きく依存しており、国内でサイバー攻撃情報の収集・分析等を必ずしも十分に行えているわけではない。さらに、こうしたデータ不足は新たな製品・サービスの開発を困難なものとしており、データ不足がサイバー攻撃対処能力向上の足枷となっている。

また、第１章でも述べたように我が国のセキュリティ人材は不足しており、その育成が大きな課題となっている。セキュリティ人材を育成するための演習には、演習シナリオの開発や演習用の環境構築が必要となるものの、シナリオ開発の前提となるサイバー攻撃情報が上述のとおり不足しており、環境構築には高度な技術力と相応の費用を要するに加え、民間企業・教育機関等のみでは十分に対応できないため、政府としてもセキュリティ人材育成支援に引き続きしっかりと取り組むことが求められている。

これらの課題に対して、我が国のサイバー攻撃対処能力を向上させ、我が国におけるサイバーセキュリティの確保を過度に海外に依存する状況を回避・脱却するためには、国内でのサイバーセキュリティ情報の生成や、人材育成を加速するエコシステムの構築が必要である。

ア　CYNEX・CYXROSS

【現状】

国内でのサイバーセキュリティ情報の生成や人材育成を加速するエコシステムの構築を目指す「CYNEX（サイネックス）」については、NICT が開発したサイバー攻撃観測システムの供用等を通じて、産学官で連携してサイバー攻撃情報の収集・分析等を実施するとともに、その結果を活用して、国産サイバーセキュリティ製品の開発支援やセキュリティ人材育成支援を実施している。また、2023 年 10 月には、国内の産学官の組織が参画する「CYNEX アライアンス」が新たに発足した。（図 17・18）

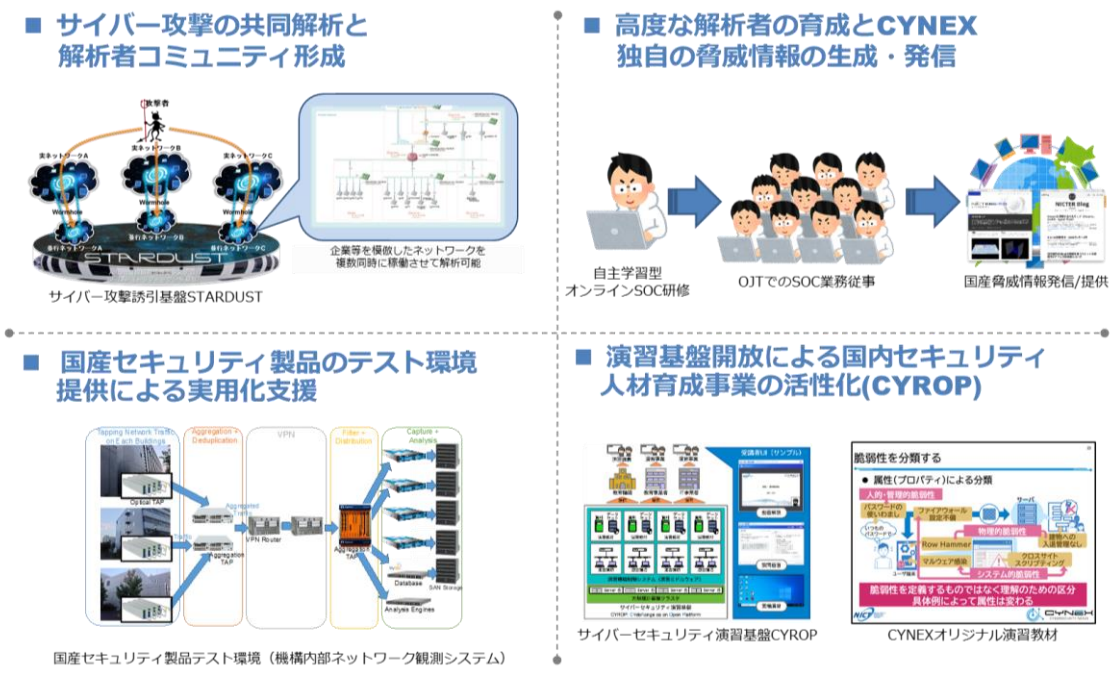
また、NICT が開発した透明性の検証が可能なセキュリティセンサーを政府端末に導入し、NICT において端末情報を収集・分析するプロジェクトである「CYXROSS（サイクロス）」については、センサー及び情報収集・分析システムの

開発を完了し、2023 年度から一部府省庁の端末にセンサーを導入して端末情報の収集・分析を開始している。（図 19）

（図 17）CYNEX アライアンスの発足

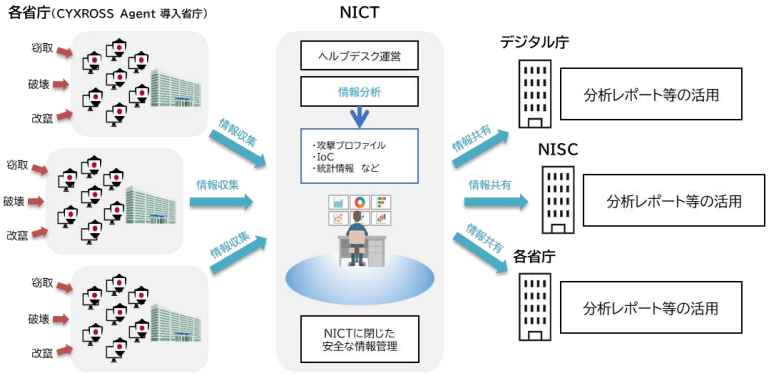
ICT サイバーセキュリティ政策分科会 資料 9-1（NICT 資料）より抜粋

（図 18）CYNEX における具体的な取組領域（４つの Co-Nexus）



ICT サイバーセキュリティ政策分科会 資料 1-2（事務局資料）より抜粋

（図 19）CYXROSS の取組



✓ NICT開発のセンサー『CYXROSS Agent』を政府端末に導入し情報収集
✓ NICT CYNEXで組織横断的情報分析を行い、デジタル庁やNISC等に情報共有、今後GSOCとも連携予定

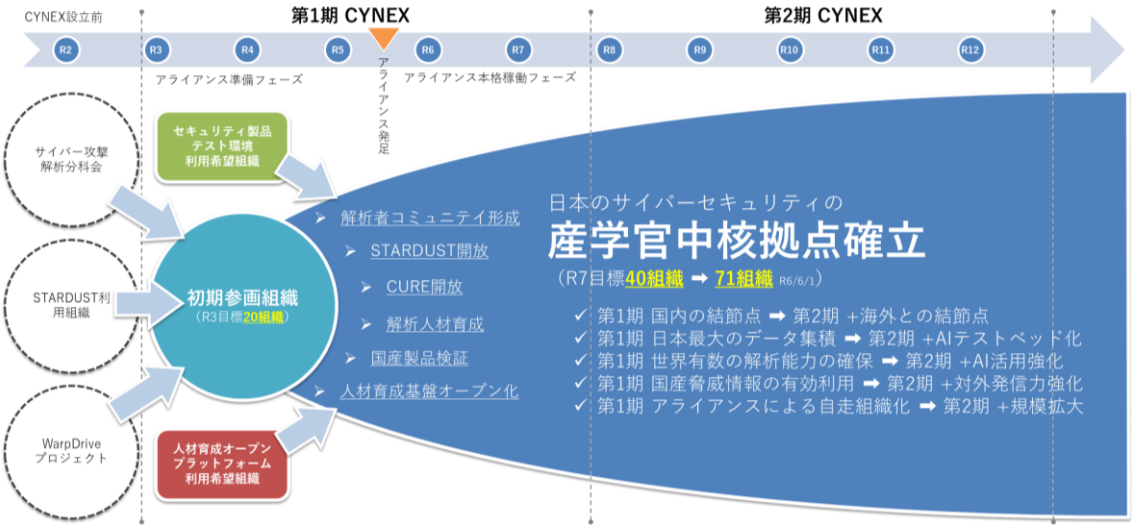
ICT サイバーセキュリティ政策分科会 資料 9-1（NICT 資料）より抜粋

【今後の取組の方向性】

CYNEX・CYXROSS の取組を通じて、国産のサイバーセキュリティ情報・技術による我が国のサイバー攻撃対処能力の向上を目指すとともに、我が国の安全保障の強化にも貢献していくため、主に以下の事項について取り組むことが必要である。（図 20）

- CYNEX については、産学官の連携により我が国におけるサイバーセキュリティ情報の収集・分析等の活動を抜本的に強化し、当該情報がセキュリティ分野を取り巻く様々な課題の解決に有効活用されるよう、それを利用する政府機関やセキュリティ関係団体、セキュリティベンダ、研究機関等のセキュリティ関係組織に対して必要な情報が提供される体制を構築する。
- CYNEX で収集・分析した情報に基づく演習シナリオや構築した演習環境の供用等を通じて、民間事業者や教育機関等によるセキュリティ演習の実施を促進することにより、我が国で不足するセキュリティ人材を幅広く育成する。これらの取組を CYNEX アライアンスにおいて自律的に推進する。
- CYXROSS については、センサー導入府省庁を拡大し、端末情報をより広範に収集し、NICT のデータ及び技術も活用して独自で分析することにより、我が国独自のサイバーセキュリティ脅威情報を生成し、政府システムのセキュリティ対策を強化するために当該情報を NISC やデジタル庁等の関係機関に提供する。さらに、CYXROSS を GSOC と連携させ、これを NICT の継続的な実務として取り組むことで、エンドポイントを含む政府システムの一元的な監視体制の構築に貢献する。

（図 20）CYNEX の事業展開のタイムライン



ICT サイバーセキュリティ政策分科会 資料 9-1（NICT 資料）より抜粋

イ　人材育成

【現状】

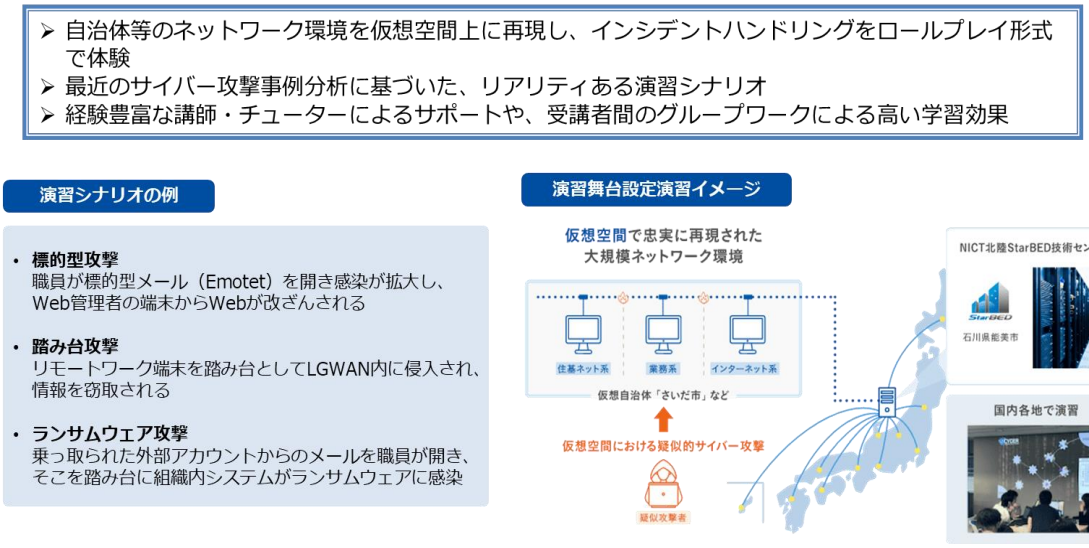
総務省・NICT では、NICT の技術的知見や研究設備等を最大限に活用し、実践的なサイバートレーニングを企画・推進するため、2017 年４月に「ナショナルサイバートレーニングセンター」を設置し、インシデント対応の実務に携わるシステム運用者や革新的なセキュリティサービス等を生み出すハイレベル層の開発者を対象として主に以下のプロジェクトに取り組んでいる。（図 21）

- 国の機関、地方公共団体及び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「CYDER」を実施しており、2023 年度は 3,742 名が受講した他、CSIRT 担当者が知っておくべき基礎的な事項を短時間で習得できる「プレ CYDER」を、国の機関及び地方公共団体向けに新たに試行的に実施した。（図 22・23）
- 2025 年の大阪・関西万博の安全な開催に資するよう、 2023 年度から万博関連組織の情報システム担当者等を対象として万博向けサイバー防御講習「CIDLE（シードル）」を実施している。
- 若手デジタル人材を対象として、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）の育成プログラム「SecHack365」を実施しており、2023 年度は 38 名が修了している。

（図 21）ナショナルサイバートレーニングセンターの概要

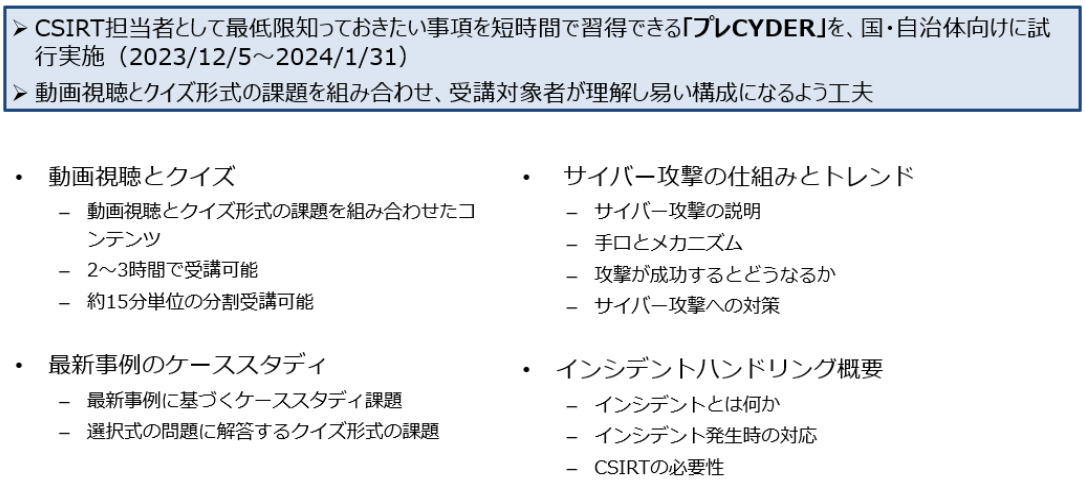
ICT サイバーセキュリティ政策分科会 資料 4-1（NICT 資料）より抜粋

（図 22）CYDER のトレーニング内容



ICT サイバーセキュリティ政策分科会 資料 4-1（NICT 資料）より抜粋

（図 23）プレ CYDER の新規実施



ICT サイバーセキュリティ政策分科会 資料 4-1（NICT 資料）を基に作成

【今後の取組の方向性】

国の機関や地方公共団体等のネットワーク構成を仮想環境上に再現し、NICT が収集・分析したサイバーセキュリティ情報を活用した実践的なインシデント対応のトレーニングを提供する実践的サイバー防御演習「CYDER」や、CSIRT 活動の基礎となるインシデント対応の最初の一歩と最新のサイバー攻撃動向に関する知識をコンパクトに提供する「プレ CYDER」については、コース内容の充実やトップダウンも含めた周知啓発の強化、オンライン方式を活用した受講利便性の向上等を図りながら、これらを継続的に提供することで、複雑化・巧妙化するサイバー攻撃に対する国の機関や地方公共団体等における CSIRT のベースラインとなる基本的な対処能力の抜本的な強化に貢献していくことが必要である。

また、国の機関や地方公共団体等における CSIRT 以外にも大きく拡大しているセキュリティ人材育成ニーズに対応できるように、CYDER で培った演習基盤の産学官への展開・技術移転を推進していくことが重要である。

多くの優秀な修了生を輩出してきた我が国で唯一の長期ハッカソン形式による若手セキュリティ人材育成プログラム「SecHack365」については、自ら課題を発見し新たな発想で解決策を生み出すことのできるセキュリティイノベーターの育成を継続するとともに、「SecHack365 Returns」等の機会を通じて、修了生の社会での活躍を一層促進するために修了生によるコミュニティ活動を活性化させ、修了生が講師等としてプログラムに戻ってくるようなセキュリティ人材育成のエコシステム確立を目指していくことが必要である。

ウ　研究開発等を担うNICTの取組・体制強化

【現状】

NICT サイバーセキュリティ研究所は、サイバーセキュリティ分野における基礎から応用に至る幅広い技術の研究開発を実施するとともに、同研究所の強みを活かして、セキュリティ強化に係る社会的要請に応えるための各種サービス（例：ナショナルサイバートレーニングセンターにおける公的機関 CSIRT 等の能力強化、ナショナルサイバーオブザベーションセンターにおけるインターネットに接続された IoT 機器の脆弱性調査及び対処方法の助言等）を提供している。

【今後の取組の方向性】

NICT サイバーセキュリティ研究所が提供する上述の各種サービスについて、同研究所の強みを活かしつつ、サービス利用者の実態とニーズを精緻に把握して、これらに一層寄り添った形でサービス提供を行えるよう、同研究所の事業推進体制を強化することが重要である。

また、サイバーセキュリティ分野における我が国の研究開発能力の強化に向けて、当該分野で豊富なデータ・技術・人材を有するとともに標準化や成果発信等においても大きな影響力を有する米国との連携を深化させるため、NICT 内に米国の政府機関や研究組織とのサイバーセキュリティ技術に関する国際的な結節点を形成し、共同研究や人材交流、情報の共有や発信等を戦略的に活性化させる必要がある。

これらの取組も含め、NICTは、今後策定されるNICTの第６期中長期計画（2026年度～2030年度）に基づき、AI、量子技術、Beyond5G/6G等の将来的な技術動向を十分踏まえながら、我が国唯一の情報通信分野を専門とする国立研究開発法人として、我が国の自律的なサイバー攻撃対処能力の向上に向けて、サイバーセキュリティ分野において一層重要な役割を果たしていくべきである。

（２）新技術への対応

ア　AI とセキュリティ

【現状】

第１章においても述べたように、生成 AI をはじめとする AI 技術の急速な普及に伴い、サイバーセキュリティ分野においても、AI を起因とした新たなリスク（AI の脆弱性を狙ったサイバー攻撃、AI の不適切な利用によるセキュリティリスクや AI を悪用したサイバー攻撃等）が指摘されている。

特に生成 AI の脆弱性を狙ったサイバー攻撃の脅威については、2023 年に OWASP[38]が LLM アプリケーションの 10 大脅威[39]を公表しており、悪意のあるプロンプト注入による LLM の不正操作（プロンプト・インジェクション）等が指摘されている。また、生成 AI を悪用したサイバー攻撃の脅威については、フィッシングの増加・高度化やマルウェア生成の容易化等が指摘されている。

AI の脆弱性を狙ったサイバー攻撃に対しては、既存のセキュリティ対策と組み合わせた多層防御の対策、AI の不適切な利用によるセキュリティリスクや AI を悪用したサイバー攻撃に対しては、利用者リテラシーの向上や、AI の提供者等による悪意のある AI の検知・削除等の対策が挙げられている。

一方で、AI は効果的なセキュリティ対策手段として活用が進んでおり、特に昨今、サイバー攻撃の大規模化・複雑化・巧妙化に伴い、SOC や CSIRT 等のセキュリティ対策業務負荷の増加が課題となっている中、サイバー防御の自動化や調査レポート作成支援等において、今後、生成 AI の利活用が期待されている。

【今後の取組の方向性】

生成 AI 等の AI 技術を巡る動向の変化はスピードが速いことも踏まえ、その最新動向を継続的に把握した上で、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。

AI に起因するセキュリティリスクについては、諸外国の動向調査や実際のセキュリティリスクに関する検証等を実施した上で、国内外の関係省庁・機関と連

---

[38] The Open Worldwide Application Security Project の略であり、世界中のセキュリティ専門家が参加するオープンソースのセキュリティコミュニティ。Web やモバイルアプリ等のセキュリティに関する様々な資料やツールを提供している。

[39] 「OWASP Top 10 for LLM Applications(Version1.1)」（OWASP、2023 年 10 月）（https://owasp.org/www-project-top-10-for-large-language-model-applications/assets/PDF/OWASP-Top-10-for-LLMs-2023-v1_1.pdf）

携しつつ、本年４月に公表した「AI 事業者ガイドライン」に基づき、セキュリティリスクの回避・低減を目的とした「開発者」「提供者」「利用者」等の各ステークホルダー向けのガイドライン策定を目指すとともに、AI に対する攻撃に対策を講じる際に参照可能な当該攻撃に係るナレッジベース（例えば MITRE ATLAS[40] 等）の拡充を図ることが求められる。

また、AI 利用者のリテラシー向上等を図る観点から、「AI セキュリティ情報発信ポータル[41]」の更新等を通じて、AI セキュリティに関する情報の的確かつ分かりやすい発信に取り組むことが必要である。

生成 AI を含む AI のセキュリティ対策への効果的な活用については、その促進を図るため、迅速かつ的確なサイバー脅威情報の収集、通信等の重要インフラ分野におけるサイバー攻撃検知・対処オペレーション業務の高度化等の具体的なプロジェクトを通じて、セキュリティ分野における AI 活用の有効性やその手法を示していくことが重要である。

イ　耐量子計算機暗号等の暗号技術

【現状】

サイバー空間の安全性・信頼性は、情報の秘匿や改ざんの防止、認証等のために用いられる暗号技術の基盤の上で成立しており、サイバー空間の拡大に伴い、暗号技術の重要性も増大している。

今日、広く利用されている現代暗号は、従来型コンピュータでは、効率的な求解が困難な数学問題に基づき安全性を担保しているものの、今後の量子コンピュータの大規模化による計算機能力の向上に伴い、多くの現代暗号において危殆化リスクの増大が見込まれている。特に、公開鍵暗号は、大規模量子コンピュータにより、鍵長を伸長したとしても現実的な時間での解読が可能となることから、大規模量子コンピュータでも解読困難な耐量子計算機暗号（PQC）への移行が必要とされている。

こうした課題を踏まえ、CRYPTREC[42]において、各種現代暗号の安全性監視を実施している他、NICT においても PQC を含む現代暗号の安全性評価に関する研究

---

[40] 米国連邦政府や各州・自治体などの公共機関に対して研究開発等の支援を行う米国の非営利団体（MITRE）が公開している、人工知能・機械学習に対する攻撃者の TTP（戦術（Tactics）・技術（Techniques）・手順（Procedures））を集約したナレッジベース。（MITRE ATLAS_HP）（https://atlas.mitre.org/）

[41] 「AI セキュリティ情報発信ポータル」（総務省委託事業）（https://www.mbsd.jp/aisec_portal/）

[42] Cryptography Research and Evaluation Committees の略であり、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討する政府のプロジェクト。

開発を実施している。2023 年３月、CRYPTREC における検討を踏まえ、NICT 及び IPA は「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）[43]」を策定している。

また、今後、無線サービスにおいても PQC 等への移行が必要となることを見据え、5G 等でのユースケースに合わせた PQC への機能付加技術等の研究開発を実施している。

【今後の取組の方向性】

NICT における暗号安全性評価に関する研究開発の取組を充実させるとともに、その成果も活用して、CRYPTREC における現代暗号に対する安全性監視能力を維持・強化し、我が国として、PQC を含む形で、現代暗号の安全性評価・監視を主体的に実施することが必要である。

現代暗号の安全性評価・監視については、従来型コンピュータの計算機能力向上に加えて、量子コンピュータの計算機能力向上を考慮に入れて実施する必要があることから、これらの技術の進展を的確に把握することが重要である。

また、CRYPTREC における現代暗号の安全性評価・監視で得られる知見も踏まえ、「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」や「CRYPTREC 暗号リスト[44]」の改定を含め、PQC 等への移行に向けて必要となる技術的検討及び情報発信を実施することが必要である。

さらに、量子コンピュータの計算機能力向上に伴う現代暗号の危殆化リスクに対しては、各分野において適切にリスクを把握した上で、 暗号移行には一定の期間を要することも考慮に入れつつ、PQC 等への移行に向けて必要な対応を進めることが重要である。

これらの取組とあわせて、PQC 等への円滑な移行に向けて、PQC や鍵長を伸長した共通鍵暗号の性能向上技術やクリプト・アジリティ[45]技術等の研究開発を推進することが求められる。

---

[43] 前掲注 14）

[44] 「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」（デジタル庁・総務省・経済産業省、2023 年３月）（https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022.pdf）

[45] NIST により提唱された「暗号の俊敏性」を表す概念。IT システムで利用されている暗号方式が危殆化した場合などに、暗号方式を素早く別の暗号方式に切り替えられるようにするための設計・実装・運用における各種工夫を指す。

３．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

社会全体のデジタル化が進み、我々の日常生活や社会経済活動におけるサイバー空間への依存度が上昇する中、地域・業種等を問わず発生し得るサイバー攻撃リスクに対応するためには、地に足のついた日々のセキュリティ対策が極めて有効であり、それを支える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普及啓発等がますます重要になっている。

（１）地域 SECUNITY

【現状】

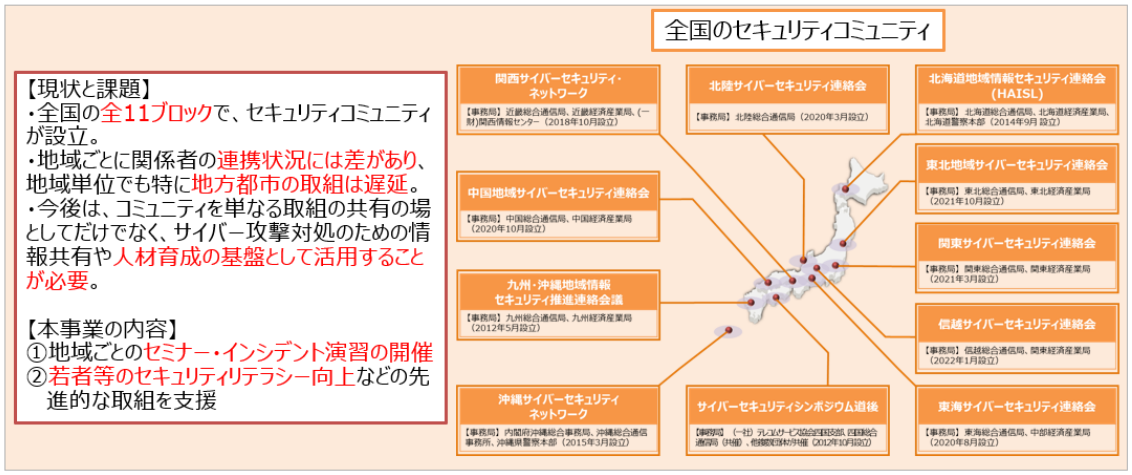
官民の関係者による「共助」の関係の下で、セキュリティに関する情報共有や普及啓発等を促進することを目的とした地域に根付いたセキュリティコミュニティである「地域 SECUNITY」については、全国 11 か所の総合通信局等の管区においてコミュニティの設立が完了し、各地域において、セミナーやインシデント演習を継続的に実施している他、セキュリティに関心のある層の裾野を拡大するため、若年層向け CTF を実施している。（図 24）

【今後の取組の方向性】

地域におけるセキュリティ対策の状況を継続的に調査し、各地域の実情を把握しつつ、地域向けの普及啓発活動を行う機関との更なる連携の拡大や、特定の業界・参加者向けといったターゲットを明確にしたイベントの拡充を図っていくことが必要である。

さらに、地域 SECUNITY を通じた普及啓発活動が持続的なものとなるよう、それを担う地域の人材・体制の整備に取り組むことより、より効果的な取組としていくことを目指すことが求められる。

（図 24）地域セキュリティコミュニティ強化支援事業の概要



サイバーセキュリティタスクフォース 資料 46-1（事務局資料）より抜粋

（２）ガイドラインその他普及啓発に向けた取組

【現状】

「サイバーセキュリティ対策情報開示の手引き[46]」「サイバー攻撃被害に係る情報の共有・公表ガイダンス[47]」「スマートシティセキュリティガイドライン（第3.0版）[48]」「テレワークセキュティガイドライン（第５版）[49]」「無線 LAN（Wi-Fi）のセキュリティに関するガイドライン[50]」を策定・公表しており、各ガイドラインの周知啓発に取り組むとともに必要に応じて改定を実施している。

一般国民向けのセキュリティ対策に関する情報発信を目的とした「国民のためのサイバーセキュリティサイト[51]」については、最新の技術動向や社会環境を踏まえて内容の更新を行うとともに、デザインの大幅な見直しを行い、2024 年５月にリニューアルを行っている。

【今後の取組の方向性】

既存のガイドラインについては、引き続き周知啓発、必要に応じた改定を実施するとともに、セキュリティの最新動向を踏まえながら、ガイドライン等を通じたセキュリティ対策の促進に貢献していくことが重要である。

また、「国民のためのサイバーセキュリティサイト」については、一般国民がサイバーセキュリティの基本知識や日々行うべき望ましいセキュリティ対策（サイバーハイジーン）を学ぶことができるサイトとして情報のアップデートを継続的に実施するとともに、政府が発信する信頼できる情報源として認知度の向上に努めることが必要である。（図 25）

---

46 「サイバーセキュリティ対策情報開示の手引き」（総務省、2019 年６月）（https://www.soumu.go.jp/main_content/000630516.pdf）

47 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（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、2023 年３月）（https://www.soumu.go.jp/main_content/000867112.pdf）

48 「スマートシティセキュリティガイドライン（第 3.0 版）」（総務省、2024 年６月）（https://www.soumu.go.jp/main_content/000955126.pdf）

49 「テレワークセキュリティガイドライン（第５版）」（総務省、2021 年５月）（https://www.soumu.go.jp/main_content/000752925.pdf）

50 「自宅 Wi-Fi 利用者向け 簡易マニュアル」（総務省、令和６年３月版）、「公衆 Wi-Fi 利用者向け 簡易マニュアル」（令和６年３月版）、「公衆 Wi-Fi 提供者向け セキュリティ対策の手引き」（令和６年３月版）（https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/）

51 「国民のためのサイバーセキュリティサイト」（総務省）（https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/）

（図 25）国民のためのサイバーセキュリティサイト

「国民のためのサイバーセキュリティサイト」より抜粋

４．国際連携の更なる推進

（１）国際連携全般

【現状】

第１章で述べたように、国際情勢が緊迫化し、サイバー攻撃の脅威が高まっている中、サイバー空間の安全性確保のため、国際連携の更なる推進が必要不可欠な状況である。

このため、関係省庁・機関と連携しつつ、二国間・多国間における各国政府・民間レベルでの情報共有や ITU における国際標準化活動に積極的に関与している（主な実績：各国とのサイバー協議、クアッド上級サイバーグループ会合、日 ASEAN サイバーセキュリティ政策会議、ITU-T SG17、ISAC 連携ワークショップ等）。

【今後の取組の方向性】

引き続き、関係省庁・機関と連携しつつ国際連携を推進し、サイバー空間の安全性確保に貢献するとともに、ICT 分野における我が国のサイバーセキュリティ政策に関する取組の積極的な情報発信、国際機関等における標準化活動やその普及展開、米国や欧州等の ISAC 間における更なる情報共有・連携の促進等に取り組み、サイバーセキュリティ分野における我が国の国際的なプレゼンス向上を目指していくことが重要である。

（２）人材育成支援

【現状】

サイバーセキュリティ分野における国際的な人材育成支援については、我が国を含む世界全体のサイバーセキュリティリスクを低減させる等、安全保障上の観点からも極めて重要な取組となっている。

これを踏まえ、ASEAN 域内のサイバーセキュリティ能力の底上げに貢献するため、ASEAN 等と連携して、2018 年に日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）を開所した。2023 年３月以降は JICA の技術協力プロジェクトにより運営を支援している。

AJCCBC においては、CYDER 等の我が国発の演習コンテンツの他、第三者連携のスキームを活用して有志国の研修プログラムも提供しており、2024 年５月までの累計で、ASEAN 域内の政府機関及び通信セクター等の重要インフラ事業者から約 1,700 名が参加している。（図 26）

また、自由で開かれたインド太平洋（FOIP）の実現に向けた取組の一環として、AJCCBC における知見・ノウハウを活用し、2024 年２月に大洋州島しょ国を対象としたサイバーセキュリティ能力構築支援事業を試行的に実施した。

【今後の取組の方向性】

AJCCBC については、JICA をはじめとする国内関係機関や有志国等との連携推進により、我が国が提供する CYDER 等の演習コンテンツの拡充に加え、第三者提供によるプログラムの拡大や ICT 以外の重要インフラセクターへの対象拡大を図ること等により、幅広い関係者が参画する能力構築支援プラットフォームを目指すことで、引き続き ASEAN 域内のサイバーセキュリティ能力の向上に貢献することが求められる。

また、大洋州島しょ国向け支援事業については、大洋州島しょ国のニーズを踏まえ、関係各国・機関と連携しつつ、実施体制や運用拠点等の検討を進め、2025 年度以降の継続的かつ本格的な実施を目指していくべきである。（図 27）

さらに、AJCCBC や大洋州島しょ国向け支援事業で得られたノウハウ・知見を活用するとともに、有志国や世界銀行等の関係機関との連携を更に深めることにより、支援対象地域の拡大等、能力構築支援活動の更なる拡充に取り組むことが重要である。

（図 26）日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）プロジェクトの概要

■2017年12月の日ASEAN情報通信大臣会合にて総務省が議論をリードし、タイのETDA（電子取引開発機構）がセンターを運用することで合意。ASEAN域内のサイバーセキュリティ能力の底上げに貢献する事業として、2018年９月にセンター開所。（2023年3月以降は、JICA技術協力により支援中）

センターの主な活動内容

1. **サイバーセキュリティ演習**
   ASEAN各国の政府機関・重要インフラ事業者等に対し、以下の演習を実施（年6回程度）
   - ✓ 実践的サイバー防御演習（CYDER） ※CYDER: Cyber Defense Exercise with Recurrence
   - ✓ デジタルフォレンジック演習
   - ✓ マルウェア解析演習
   - ✓ デジタルフォレンジック・マルウェア解析に係るトレーナー向け演習
   - ✓ ASEANニーズ調査に基づく演習（2023年度はペネトレーションテストに関する演習を実施）
   - ✓ トラストデジタルサービス（Trusted Digital Service）に係る演習

2. **Cyber SEA Game（ASEAN Youth Cybersecurity Technical Challenge）**
   ASEAN各国から選抜された若手技術者・学生がサイバー攻撃対処能力を競うCTF形式の大会の開催（年１回）
   ※CTFとは、Capture The Flagの略で、問題の中に隠されたフラグ（＝キーワード）を探し出して解答するクイズ形式の競技

AJCCBC
ASEAN JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE


サイバーセキュリティ演習模様


Cyber SEA Game模様

今までの実績等

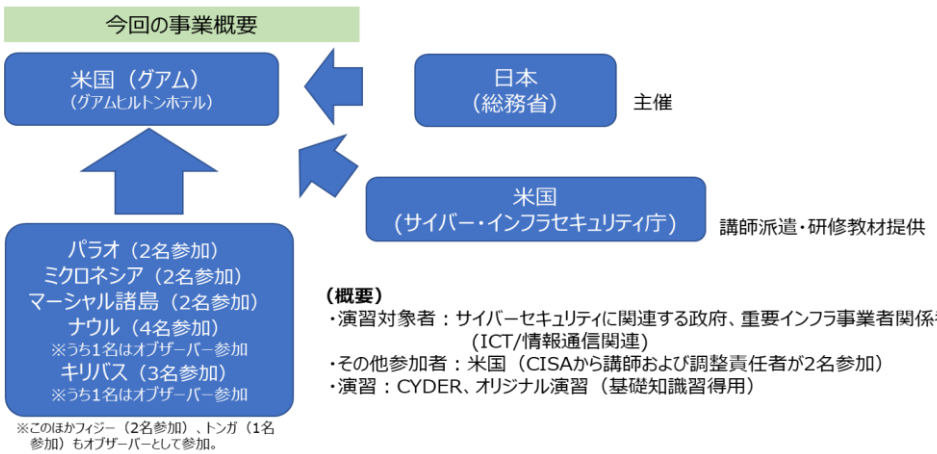
- 2018年9月のセンター開所以来、約2ヶ月に1回のサイバーセキュリティ演習と年1回のCyber SEA Gameを開催。
- 日本から提供しているサイバーセキュリティ演習には、2024年5月時点で約1,700名が参加。
- 第三者連携のスキームを活用することにより、有志国（米国、英国等）の研修プログラムも提供。

今後、センターの活動に関する有志国等との連携を強化し、研修プログラムの提供・実施を予定
また日本で実施されている各種サイバーセキュリティ演習の提供も検討

ICT サイバーセキュリティ政策分科会 資料 3-4（事務局資料）を基に更新

（図 27）大洋州島しょ国におけるサイバーセキュリティ能力構築支援の概要

■自由で開かれたインド太平洋（FOIP）の実現に向けた取組みの一環として、総務省では本年２月18日～26日の日程で米国（グアム）にてサイバーセキュリティに係る能力構築支援（演習事業）を実施。
■具体的には、ミクロネシア（パラオ、ミクロネシア、マーシャル諸島、ナウル、キリバス）のサイバーセキュリティに関する政府職員及び通信事業者等の重要インフラ事業者の職員13名が参加（※フィジー、トンガを含めた全体で16名）。
■演習教材には、既に**日ASEANサイバーセキュリティ能力構築センター(AJCCBC)**で途上国支援として採用されている実践的サイバー防御演習（CYDER）（NICTが開発）等を使用。
■今回の事業成果を踏まえ、来年度は更に効果的な事業を検討・実施する予定（※実施国は未定）。



ICT サイバーセキュリティ政策分科会 資料 3-4（事務局資料）より抜粋

おわりに

「ICT サイバーセキュリティ政策の中期重点方針」は、サイバー攻撃の巧妙化・深刻化が進み、我が国のサイバーセキュリティを巡る環境が今後大きく変化していくことが見込まれる中、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政策の方向性について取りまとめたものである。

総務省においては、「サイバーセキュリティ戦略」や「国家安全保障戦略」等をはじめとする政府全体の方針に基づき、関係省庁と連携しつつ、今後、同中期重点方針を踏まえ、我が国の安全保障にも貢献する観点から、平時から安全・安心なサイバー空間の確保を図るため、各施策を具体的に推進していくことが求められる。

また、同中期重点方針で示された各施策の推進に際しては、サイバー空間を取り巻く環境等が常に変化し続けていることを踏まえて、そうした変化に柔軟に対応しつつ、取り組んでいくことが重要である。こうした観点から、各施策の進捗状況について、定期的にフォローアップを行った上で、必要に応じて同中期重点方針の見直しを図っていくことが必要である。

なお、同中期重点方針の推進に当たっては、社会全体のデジタル化の主体となる多様なステークホルダーの理解と連携の下で効果的に進めていくことが必要である。このため、関係するステークホルダーとの間で、同中期重点方針の目的・狙いやビジョンの共有を進め、取組の強化を図っていくことが望ましい。

「ICTサイバーセキュリティ政策分科会」開催要綱

１　目的

社会全体のデジタル化が進展し、我々の日常生活や社会経済活動におけるサイバー空間への依存度はますます上昇する一方で、サイバー攻撃の巧妙化・深刻化が進み、セキュリティリスクが高まっている状況にある。さらに、厳しさを増す安全保障情勢、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・複雑化などを踏まえれば、我が国のサイバーセキュリティを巡る環境は今後大きく変化していくことが見込まれる。

これを踏まえ、本分科会は、「サイバーセキュリティタスクフォース」の下に開催される会合として、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うことを目的とする。

２　名称

本分科会は、「ICTサイバーセキュリティ政策分科会」と称する。

３　検討事項

（１）重要インフラ分野におけるサイバーセキュリティ対策強化の在り方
（２）サイバーセキュリティの基盤となる人材育成及び研究開発の在り方
（３）サイバーセキュリティの確保に向けた国際連携及び普及啓発の在り方

４　構成及び運営

（１）本分科会の主査は、サイバーセキュリティタスクフォースの座長が指名する。
（２）本分科会の構成員は、別添のとおりとする。
（３）主査は、本分科会を招集し、主宰する。
（４）主査は、必要があると認めるときは、主査代理を指名することができる。
（５）主査代理は、主査を補佐し、主査不在のときは主査に代わって本分科会を招集し、主宰する。
（６）本分科会の構成員は、やむを得ない事情により出席できない場合において、代理の者を指名し、出席させることができる。
（７）主査は、必要に応じ、オブザーバを招聘することができる。
（８）主査は、必要に応じ、外部の関係者の出席を求め、意見を聞くことができる。
（９）その他、分科会の運営に必要な事項は、主査が定める。

５　議事・資料等の扱い

（１）本分科会は、原則として公開とする。ただし、主査が必要と認める場合については、非公開とする。
（２）本分科会で使用した資料については、原則として、総務省のウェブサ

イトに掲載し、公開する。ただし、公開することにより、当事者若しくは第三者の利益を害するおそれがある場合又は主査が必要と認める場合については、非公開とする。

（３）本分科会の議事要旨は、原則として公開とする。ただし、主査が必要と認める場合については、非公開とする。

６　スケジュール

本分科会は、令和６年２月から開催する。

７　その他

本分科会の事務局は、サイバーセキュリティ統括官室が行う。

（別添）

「ICT サイバーセキュリティ政策分科会」構成員名簿

（敬称略、五十音順）

新　井　　悠	株式会社 NTT データグループ 技術革新統括本部システム技術本部 サイバーセキュリティ技術部　エグゼクティブ・セキュリティ・アナリスト
上原　哲太郎	立命館大学情報理工学部　教授
栗　原　　純	株式会社 TBS グロウディア デジタル技術事業本部 情報システム部　副部長
後藤　厚宏	情報セキュリティ大学院大学　学長
小　山　　覚	NTT コミュニケーションズ株式会社　情報セキュリティ部長 ICT-ISAC　ステアリング・コミッティ運営委員長
篠田　佳奈	株式会社 BLUE　代表取締役
辻　　伸弘	SB テクノロジー株式会社 プリンシパルセキュリティリサーチャー
蔦　　大輔	森・濱田松本法律事務所　弁護士
盛合　志帆	国立研究開発法人情報通信研究機構（NICT）　執行役 経営企画部長
吉岡　克成	横浜国立大学大学院環境情報研究院/先端科学高等研究院　教授

ＩＣＴサイバーセキュリティ政策分科会における検討状況

回次	議事内容
第１回 （2024 年２月９日）	✓ サイバーセキュリティの最近の状況及び ICT サイバーセキュリティ政策分科会について ✓ 我が国を取り巻くサイバーセキュリティの情勢 ✓ 通信分野におけるサイバーセキュリティ対策の取組について
第２回 （2024 年２月 27 日）	✓ 放送分野におけるサイバーセキュリティ対策の取組について
第３回 （2024 年３月 13 日）	✓ 国際連携に係る取組状況について ✓ 海外における人材育成に係る取組状況について
第４回 （2024 年３月 27 日）	✓ 地域における人材育成に係る取組状況 ✓ 地域の事業者等に向けた普及啓発に係る取組状況
第５回 （2024 年４月５日）	✓ スマートフォンのセキュリティ確保に向けた取組状況 ✓ 情報通信ネットーワークの安定性・信頼性の確保に向けた取組状況
第６回 （2024 年４月 26 日）	✓ 自治体におけるサイバーセキュリティ対策の取組について
第７回 （2024 年５月 10 日）	✓ 通信分野におけるサイバーセキュリティ対策の取組について
第８回 （2024 年５月 27 日）	✓ 量子計算機の進展に応じた耐量子計算機暗号の研究開発 ✓ AI の進展に応じたサイバーセキュリティ対策
第９回 （2024 年６月 14 日）	✓ CYNEX・CYXROSS 等について ✓ 論点整理
第 10 回 （2024 年６月 24 日）	✓ ICT サイバーセキュリティ政策の中期重点方針」（案）