別紙２

ICT サイバーセキュリティ総合対策 2023
（案）

2023 年６月

総務省　サイバーセキュリティタスクフォース

目次

はじめに

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）は、サイバー攻撃の複雑化・巧妙化や脆弱性の拡大などの動向に対応したサイバーセキュリティに係る課題の整理や、情報通信分野において講ずべき対策や既存の取組の改善などについて幅広い観点から検討を行っている。「サイバーセキュリティ戦略」（2021 年 9 月 28 日閣議決定）等も踏まえつつ、2022 年８月には「ICT サイバーセキュリティ総合対策 2022」（以下、「総合対策 2022」という。）を取りまとめた。

「総合対策 2022」の策定後、本タスクフォースにおいて、国際情勢の緊迫化を含めたサイバー攻撃リスクの拡大等の状況変化を踏まえた議論を行うとともに、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１月から「情報通信ネットワークにおけるサイバーセキュリティ対策分科会」を設置して議論を行ってきた。

本文書は、これらの議論を経て、「ICT サイバーセキュリティ総合対策 2023」として、必要な改定を行ったものである。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を期待する。

Ⅰ　サイバーセキュリティを巡る最近の動向

１．サイバーセキュリティに関する政策動向

「総合対策 2022」においても記載されているとおり、政府においては、2021年９月に策定された「サイバーセキュリティ戦略」に基づき、社会全体のデジタル・トランスフォーメーション(DX) や、サイバー空間の公共空間化に伴う「誰一人取り残さない」サイバーセキュリティの確保(“Cybersecurity for All”)に向けた取組が継続的に推進されている。

「総合対策 2022」策定後の政府内での主な動向は以下のとおりである。

・　国家安全保障戦略の策定

2022 年 12 月に、「国家安全保障戦略」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ついて検討が進められている。

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。

2023 年１月末には、内閣官房にサイバー安全保障体制整備準備室が設置され、具体化に向けた議論が進められている。

・　経済安全保障推進法に基づく基幹インフラ役務の安定的な提供の確保に係る基本方針の策定

2023 年４月、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和４年法律第 43 号）に基づき「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本方針」[1]が閣議決定された。同法では通信・放送を含む基幹インフラ１４分野が規定されており、同基本方針において、①規制対象となる事業者等を定める際には、事業者の負担に配慮しつつ規制対象を適切に定めていくこと、②近年サイバー空間においては、特に国家の関与が疑われるサイバー活動も行われるものもみ

[1] https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin2.pdf

られており、国民生活及び経済活動の基盤となる役務の安定的な提供が妨害され、社会的に大きな混乱が生ずる事案も発生している中で、我が国の外部にある主体から強い影響を受けている事業者からの設備の導入等について慎重な審査を行う必要があるなど、サイバーセキュリティの観点を含め、審査にあたって考慮する要素などが定められている。

2024 年春頃の制度運用開始に向けて、今年夏頃に特定社会基盤事業者の指定基準、特定重要設備を定める政省令が策定される予定である。

２．サイバーセキュリティ全般を巡る動向

「総合対策 2022」策定後のサイバーセキュリティ全般を巡る動向は以下のとおりである。

・　サイバー攻撃リスクの拡大

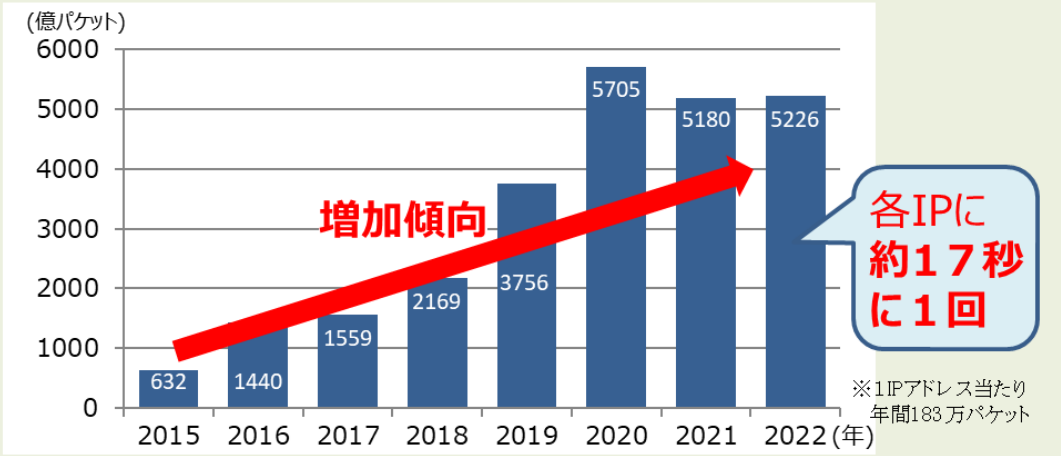
国内では、大規模サイバー攻撃観測網である NICTER において観測されたサイバー攻撃関連の通信数[2]は引き続き増加傾向（各 IP アドレスに約 17 秒に１回の通信）にある。また、2022 年のランサムウェア被害の報告件数[3]については、2020 年下半期と比較して５倍以上に増加している他、フィッシングメール及びフィッシングサイトの報告件数[4]についても、３年前の 2019 年と比較してそれぞれ約 17.4 倍、約 14.7 倍に急増している。

また、マルウェア Emotet の感染再拡大についても引き続き累次にわたって注意喚起が行われている他、新たな感染手法も確認されている[5]。

[2] NICTER 観測レポート 2022（2023 年2月 14 日　国立研究開発法人情報通信研究機構）
https://www.nict.go.jp/press/2023/02/14-1.html
[3] 令和4年におけるサイバー空間をめぐる脅威の情勢等について（2023 年3月 14 日　警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf
[4] 2022/12 フィッシング報告状況（2023 年1月6日　フィッシング対策協議会）
https://www.antiphishing.jp/report/monthly/202212.html
[5] マルウェア Emotet の感染再拡大に関する注意喚起（2023 年3月 20 日　一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC））
https://www.jpcert.or.jp/at/2022/at220006.html

（図表）

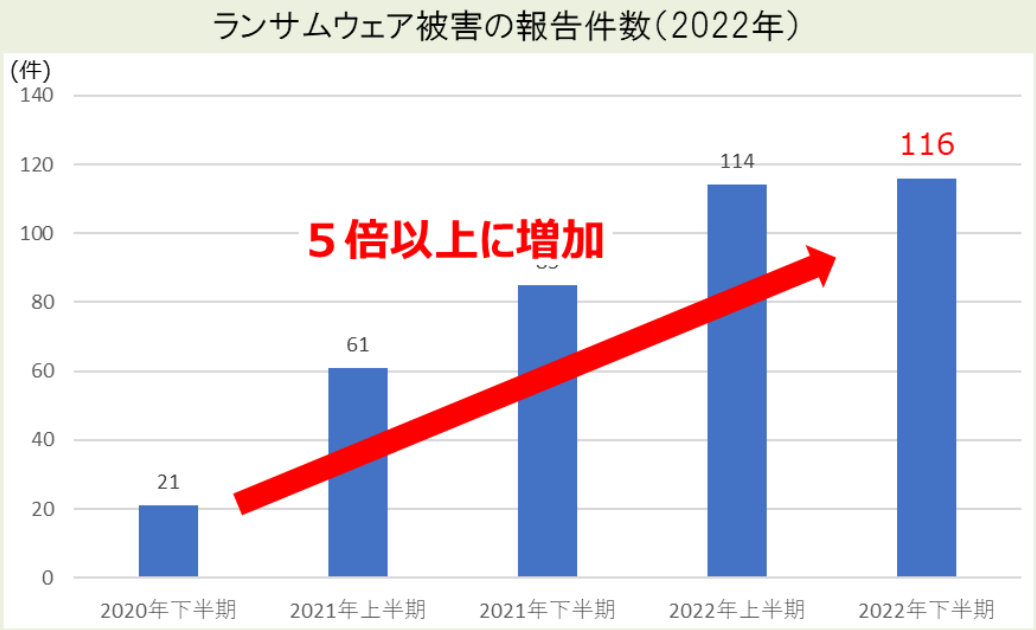
NICTERで1年間に観測されたサイバー攻撃関連の通信数



※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。

ランサムウェア被害の報告件数

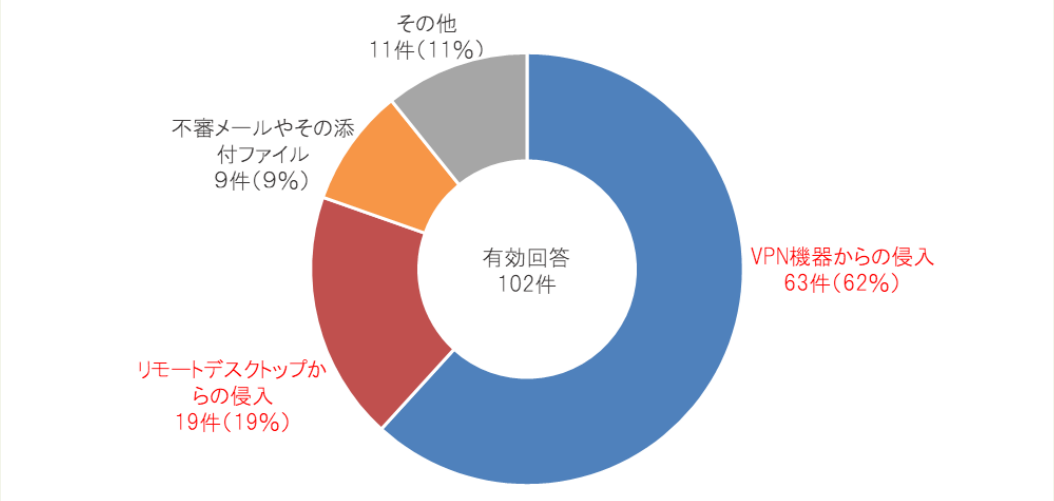
出典：「令和4年におけるサイバー空間をめぐる脅威の情報等について」（令和5年3月　警察庁）より作成



ランサムウェアの感染経路

出典:「令和4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5年3月　警察庁)より作成

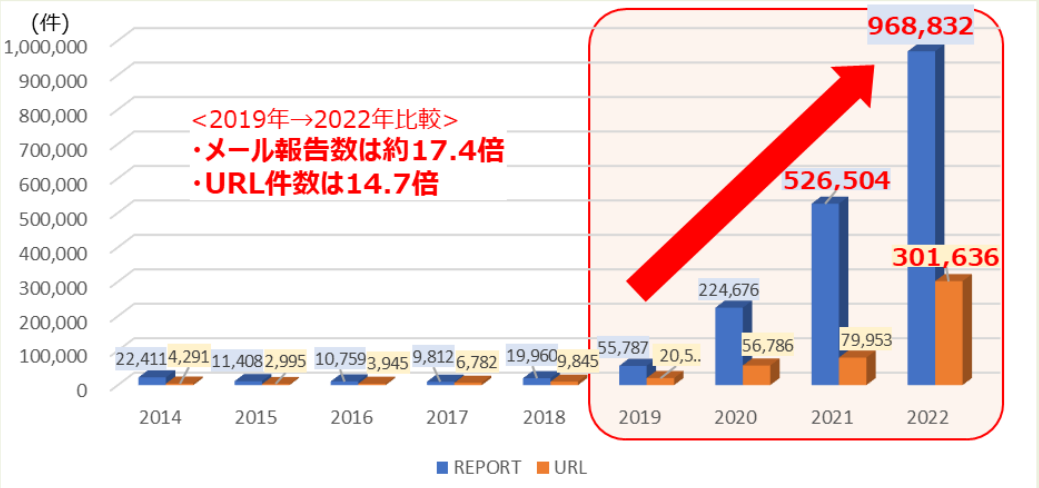
ランサムウェアの感染経路(2022年)



フィッシングメールとフィッシングサイトの報告件数

フィッシングメールの報告数とフィッシングサイトURL数

出典:「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



社会に大きな影響を与えたサイバー攻撃事例としては、2022 年 10 月に公立病院の電子カルテを含む総合情報システムが、給食事業者のシステムに設置された脆弱性のある VPN 機器からランサムウェアに感染し、長期間にわたり診療体制に大きな影響を及ぼした事例や、2022 年秋以降、一部の政府機関・地方公共団体や企業のホームページ等が標的となり、DDoS 攻撃により閲覧障害が断続的に発生した事例等があり、我が国全体として、地域や業種、事業規模を問わず、サイバー攻撃のリスクは引き続き高い状況にあると言える。

世界全体でも、ロシアによるウクライナ侵略等の国際社会における安全保障を巡る状況が引き続き緊迫している他、ランサムウェアをはじめ、各国で政府機関や重要インフラを狙ったサイバー攻撃も引き続き発生している。

こうした状況も踏まえ、直近では、総務省を含む関係省庁において、大型連休がサイバーセキュリティに与えるリスクを考慮し、2023 年４月に春の大型連休に向けて実施いただきたい対策について注意喚起を行った。

政府機関や重要インフラ事業者、地方公共団体をはじめとする企業・団体等においては、引き続き、サイバー攻撃の脅威に対する認識を深めるとともに、適切な対策を講じることが求められる。

・　情報通信ネットワークへの依存度の更なる高まり

新型コロナウイルス感染症の感染拡大等を機に、テレワークやクラウドサービスの利用が進み[6]、我が国のインターネット上を流通するトラヒックの推定量もここ５年で約３倍に増加しており[7]、社会全体のデジタル活用がますます進展している。

そして、社会全体のデジタル化の進展に伴い、必要不可欠な基盤としての情報通信ネットワークへの依存度は更に高まっている。2022 年７月に大手携帯キャリアにおいて通信サービス障害が発生した際には、延べ約 3,091 万人以上の利用者が影響を受け、物流や金融等の様々な分野において広範な影響を及ぼしたこと等を踏まえれば、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場合には、国民生活や社会経済活動に多大な影響が及ぶ状況となっている。

---

[6] 令和4年通信利用動向調査の結果（2023 年5月 29 日 総務省）
https://www.soumu.go.jp/johotsusintokei/statistics/data/230529_1.pdf

[7] 我が国のインターネットにおけるトラヒックの集計・試算 2022 年 11 月のトラヒックの集計結果（2023 年2月 15 日 総務省）
https://www.soumu.go.jp/main_content/000861552.pdf

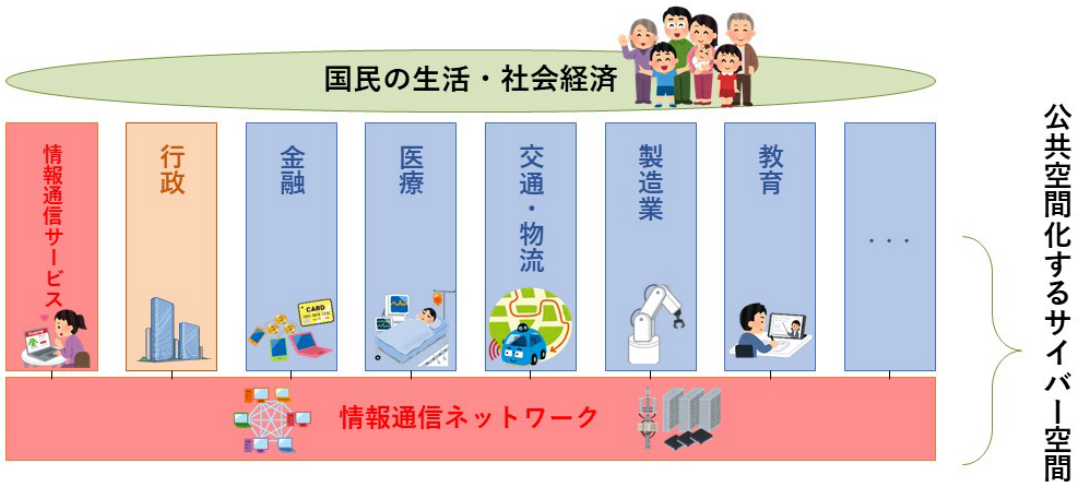
また、国際情勢の変化に伴い、サイバー空間自体が、国家間の競争・衝突の場となる中で、情報通信ネットワークは、サイバー攻撃の標的や経路、偽情報（Disinformation）を流布する場にもなり得るとともに、市民の間でリアルタイムに情報を共有するためのツールにもなり得るものである。

このような状況のもと、情報通信ネットワークの安全性・信頼性を確保することは一層重要となっている。

サイバーセキュリティと総務省の役割

✓ サイバー空間は、あらゆる主体が利用する公共空間であり、その根幹は情報通信ネットワーク。
✓ サイバー攻撃等により、情報通信ネットワークの機能停止や情報の漏えい等が生ずれば、国民の生活や我が国の経済社会に甚大な影響が発生するおそれ。

⇒ 総務省の役割：社会経済活動を支える情報通信ネットワークの安全を確保し、サイバー空間を利用する全ての国民のサイバーセキュリティの向上を図ること。



Ⅱ　「ICT サイバーセキュリティ総合対策 2023」として今後取り組むべき施策

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とを踏まえれば、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ると考えられる。

特に、Ⅰで示した状況変化及び認識を踏まえ、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・信頼性の確保及び利用者が安全・安心に利用できる情報通信サービスの実現に向けた施策を推進することが引き続き求められている。

なお、Ⅰで述べたように、政府においては、国家安全保障戦略に基づき、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に取り組むこととしているが、平時から我が国全体としてサイバーセキュリティ対策の強化を図ることは、こうした取組にも資するものと考えられる。

これらを踏まえ、総務省が今後重点的に取り組むべき施策について、「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」及び「普及啓発の推進」の４点を柱に、「ICT サイバーセキュリティ総合対策 2023」として示していくこととする。

１．情報通信ネットワークの安全性・信頼性の確保

Ⅰで述べたように、サイバー空間を支える情報通信ネットワークは国民生活や経済活動の基盤となるものであり、デジタル活用の進展とともにその重要性が増す中で、情報通信ネットワークの安全性・信頼性を確保することは一層重要となっている。

総務省では、これまでも、情報通信ネットワークのサイバーセキュリティ対策を推進してきたが、サイバー攻撃の複雑化・巧妙化・も踏まえ、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対応するため、攻撃インフラの拡大を防ぐ端末（IoT 機器）側の対策、IoT ボットネットに対して指令を出す C&C サーバへの対処を行う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ていくことが必要である。

また、広く普及が進むクラウドサービスや 5G サービスのセキュリティ確保、国内各地域において取組が進んでいるスマートシティのセキュリティ確保、放送設備のセキュリティの確保に加えて、これらを横断する課題であるサプライチェーンリスク対策等の取組を強化することが必要である。

更に、データを安心・安全に流通できる基盤の構築が不可欠であり、トラストサービスの普及に取り組む必要がある。

（１）総合的な IoT ボットネット対策の推進

本年１月に、サイバーセキュリティタスクフォースの下に、「情報通信ネットワークにおけるサイバーセキュリティ対策分科会」（主査 情報セキュリティ大学院大学学長 後藤厚宏）を設置し、総合的な IoT ボットネット対策の実現に向けて、端末（IoT 機器）側、ネットワーク側各々について今後取り組むべき対応策について検討を実施した。そのとりまとめは付録４（60～93 ページ）のとおりである。

端末（IoT 機器）側の今後の対応策（NOTICE（ノーティス））として、
①脆弱性等のある IoT 機器の調査の延長・拡充
②利用者への注意喚起等の実効性向上
③メーカーや SIer 等の幅広い関係者との連携による総合的な対処
④①～③を効果的に実施するための NOTICE の運営体制の強化

ネットワーク側その他の今後の対応策として、
①C&C サーバの検知精度の向上・検知情報の共有・利活用等の推進
②IoT ボットネットの全体像の可視化

が示されており、これらを総合的に進めて対策を強化することが必要である。

（２）その他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の推進

ア. 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

【現状】

2023 年度は、電気通信事業者による積極的なサイバーセキュリティ対策に関する総合実証として、以下の実証等[8]を実施している。

- ISP をはじめとするサービス提供者側による継続的な対策を確保するための必要事項の整理を目的とした、自動巡回による機械的処理を活用した悪性 Web サイト（フィッシングサイト等）の検知技術・共有手法の検討・実証
- 現在のインターネットを構成する根幹技術である BGP や DNS、電子メールに関する効果的な脆弱性対策の手法として標準化されており、国際的にも実装が進みつつあるにも関わらず、我が国では導入が進んでいない RPKI[9]や DNSSEC[10]、DMARC[11]等のネットワークセキュリティ技術について、技術的な課題等にとどまらない普及方策の検討

【今後の取組】

2023 年度の実証の成果を踏まえ、2024 年度においては、得られた知見を活用した普及啓発等を行うことが適当である。

- 悪性 Web サイトの検知技術・共有手法については、悪性 Web サイト情報の収集・分析を継続し、収集・分析結果を実際のセキュリティサービス等に活用した際の効果検証を行うとともに、検証結果をもとに悪性 Web サイト対策に係るガイダンスを作成し、対策の普及啓発に取り組む。

---

[8] この他、(1)で述べた、ネットワーク側の対策としての平時におけるフロー情報の収集・蓄積・分析によるC＆Cサーバの検知に係る技術実証を実施

[9] 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

[10] 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

[11] 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

・ RPKI、DNSSEC、DMARC 等のネットワークセキュリティ技術については、国内 ISP 等における導入状況や各ネットワークセキュリティ技術導入に係る技術的課題の調査・分析を継続するとともに、得られた知見を踏まえたネットワークセキュリティ技術等の普及促進に向けたガイドライン案を作成し、技術導入の普及啓発に取り組む。また、2024 年度の実証終了後も、インターネットコミュニティとの官民連携により、継続的に普及を促していく。

イ. 情報通信分野におけるサプライチェーンリスク対策

【現状】

（5G の脆弱性の検証手法等の確立と体制整備）

総務省において、2019 年度より 2021 年度にかけ、5G ネットワークにおけるセキュリティ確保に向けた調査検討を実施した。

具体的には、5G セキュリティに関する標準化機関や海外政府当局等の検討動向を調査するとともに、5G ネットワークのセキュリティに係る技術的検証を行うため、検証環境として、国立研究開発法人情報通信研究機構（以下「NICT」という。）において、5G ネットワークをエミュレート可能な仮想化基盤を構築し、同検証環境上での 5G ネットワークに対する脅威や脆弱性等の技術的検証を実施した。検証結果については対策要件等を整理し、2022 年４月、事業の成果文書として「5G セキュリティガイドライン第１版」[12]を公表し、普及啓発を図っているところである。

（5G の脆弱性情報や脅威情報等の共有の枠組み）

一般社団法人 ICT-ISAC（ISAC は Information Sharing and Analysis Center の略。以下「ICT-ISAC」という。）の 5G セキュリティ推進グループにおいて、ローカル 5G を提供する事業者やローカル 5G を利用する主体にとって参考となる、ローカル 5G のセキュリティガイドラインを 2022 年３月に策定・公表した。

（5G のセキュリティ対策の促進のための政策的措置）

総務省では、特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律[13]（令和２年法律第 37 号）に基づき、サイバーセキュリティ上のサプライチェーンリスク対策や機器や設備の供給安定性等の観点を

[12] https://www.soumu.go.jp/main_content/000812253.pdf

[13] https://elaws.e-gov.go.jp/document?lawid=502AC0000000037

含む指針に沿って、5G システムの開発供給計画及びその導入計画を認定し、税制上の優遇措置を講じている。また、全国 5G の特定基地局の開設計画の認定時及びローカル 5G の免許取得時に、サプライチェーンリスク対応を含む十分なサイバーセキュリティ対策を講ずることを条件として付しており、産業振興的な枠組み、規制的な枠組みの両面から 5G のセキュリティ確保を推進している。

（情報通信分野における SBOM 導入の可能性の検討等）

ソフトウェア分野におけるオープンソースソフトウェア（以下「OSS」という。）の急速な普及拡大によってソフトウェア・サプライチェーンが複雑化する中、通信事業者において、OSS を使用しているシステム内のソフトウェア部品の構成を把握することが重要であり、通信分野における SBOM（Software Bill of Materials)の導入の可能性を検討している。

また、スマートフォンに蓄積された利用者情報がスマートフォンアプリによって不正に外部送信されることへの懸念が高まる中、アプリ事業者以外の第三者によるスマートフォンアプリの挙動の技術的な解析可能性について検証を行っている。

【今後の取組】

（5G セキュリティガイドラインの普及等）

2022 年４月に公表した「5G セキュリティガイドライン第１版」について、国内の 5G オペレータへの普及を図り、5G ネットワークのセキュリティの確保を進めるとともに、ITU-T SG17 における標準化対象の一つとして、同ガイドラインをベースとした勧告化に向けた作業を進めていくことが適当である。

さらに、NICT に構築された 5G セキュリティ検証環境については、引き続き活用を推進するとともに、各ユースケースのグループに共通のアーキテクチャモデルに応じた具体的な脅威シナリオの検討を行うことが適当である。

これらの推進に当たっては、国際的にも進展の見られる基地局設備のインターフェースのオープン化や基地局設備自体の仮想化（いわゆる OpenRAN や vRAN)、コアや MEC を含めたクラウド（IaaS）利用も念頭に置くことが適当である。

特に、国際的に安心・安全な 5G ネットワークの重要性が議論される中で、オープンでセキュアなネットワークを実現する技術として注目される「Open RAN」やそれを活用したシステムの海外展開を推進することが求められる。

具体的には、2025 年までにチリ、タイ、ベトナム、フィリピン等の 10 か国程度で実証事業を実施し、米国とも連携しながら、いわゆる「グローバル・サウス」と呼ばれる国・地域を中心に世界シェア獲得を図ることが期待される。

（5G のセキュリティの促進のための政策的措置）

引き続き 5G の制度面において、サイバーセキュリティ上のサプライチェーンリスク対策等の安全性・信頼性等が確保された 5G の導入促進を行うことが適当である。

（情報通信分野における SBOM 導入の可能性の検討等）

引き続き、情報通信分野における SBOM 導入に当たっての課題等を整理するとともに、アプリ事業者以外の第三者によるスマートフォンアプリの挙動の技術的な解析可能性についての検証を行うことが適当である。

ウ. Beyond 5G・6G に向けたサイバーセキュリティの検討

【現状】

Beyond 5G・6G[14]に向けては、国際標準化機関等を舞台に、将来のサイバー空間のガバナンスやルール形成に大きな影響を与え得る情報通信アーキテクチャを左右しうる議論が行われているところ、その一部においては、我が国が掲げる「自由、公正かつ安全なサイバー空間」の在り方と必ずしも整合的ではないと考えられる提案も行われている。

【今後の取組】

5G に関しては、イに挙げた既存施策を着実に実施する。その上で、来る Beyond 5G・6G において開発・採用される技術について、多様な通信サービスを安全かつ安定的に信頼して利用できるよう、セキュリティ・バイ・デザインの考え方が反映されることが重要である。サイバー空間に関する将来動向を把握し、新たな研究開発要素も含め、国として推進すべきセキュリティ面での取組を検討することが適当である。この点、特に、情報通信アーキテクチャに関する国際的な議論の動向の主体的把握に努めるとともに、将来のサイバー空間のガバナンスやルールに、我が国が掲げる価値観が反映されるよう積極的に関与していくことが適当である。こうした観点から、インター

[14] 5G の特長の更なる高度化に加えて、あらゆる機器が自律的に連携し、最適なネットワークを構築する自律性、地球上のどこでも通信を可能とする拡張性、セキュリティ・プライバシーが常に確保される超安全・信頼性、データ処理量の激増に対応できる超低消費電力、といった機能を実装した次世代の移動通信システム。

ネット・コミュニティとの連携等を進め、主要な国際標準化団体等における関連する議論の動向を把握するとともに、そうした議論への我が国からの参加や国内における議論の活性化を促進していくべきである。また、標準化活動には蓄積されたノウハウが必要となることから、当該ノウハウの普及や継承のために、標準化活動に参加しやすくなるような方策を検討する必要がある。

なお、我が国が掲げる「自由、公正かつ安全なサイバー空間」の在り方と必ずしも整合的ではないと考えられる国際標準の提案は、既存のインターネットの TCP/IP 等のアーキテクチャに内在する脆弱性の存在を強調し、それを解決するための案として主張される場合もある。その一方、アの実証事業でも念頭に置く RPKI や DNSSEC、DMARC のように、既存のインターネットのアーキテクチャを前提に、そこに内在する脆弱性を緩和するための技術の標準化も進んでいる。国際場裡における議論に効果的に対応していくためには、これら技術のメカニズムや効果、国内外の普及状況等を踏まえた関与が求められる。

エ. クラウドサービスにおけるサイバーセキュリティの確保

【現状】

（提供事業者向けガイドラインの改定等）

クラウドサービスにおけるサイバーセキュリティの確保に関しては、2014 年に策定した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」[15]について、SaaS や IaaS の特性を踏まえた全体の構成見直しや責任共有モデルの考え方、管理策の見直しなどを行い、2021 年９月に第３版として改定した。

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[16]ことから、過去の情報漏えい等の事故の原因や、クラウドサービス利用者及び提供者において実施されている設定ミスを防止するための取組について調査・分析を行った上で、クラウドサービス利用者及

[15] https://www.soumu.go.jp/main_content/000771515.pdf

[16] 国内では、2023 年 5 月に、大手自動車メーカーが利用する SaaS サービスにおいて、公開設定の誤りによって情報が第三者からアクセス可能な状態であった事例が判明した。なお、IBM の調査（2020 年）では、2019 年に発生した情報漏えい事案のうち 85%以上はクラウドサービスの設定ミス等によるものであったとされている。
https://newsroom.ibm.com/2020-02-11-IBM-X-Force-Stolen-Credentials-and-Vulnerabilities-Weaponized-Against-Businesses-in-2019

び提供者において実施することが望ましい取組として、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」[17]を策定・公表した。

（ISMAP の運用）

政府機関が利用するクラウドサービスの安全性評価の仕組みとして、内閣官房（NISC・IT 室（現在のデジタル庁））、総務省及び経済産業省において、2020 年６月に「政府情報システムのためのセキュリティ評価制度」（ISMAP（イスマップ））を立ち上げた。2021 年３月に 10 サービスが初めて登録されて以降、2023 年５月 11 日現在、あわせて 44 サービスが登録されている[18]。

また、ISMAP において、セキュリティ上のリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組みとして、影響度が低いと評価される業務・情報に用いられる SaaS を対象とする ISMAP for Low-Impact Use（ISMAP-LIU）を 2022 年 11 月に運用開始した。

【今後の取組】

策定済みのガイドラインである、「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」及び「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」の普及促進を図るとともに、今後、特に後者について、利用者に向けた分かりやすい普及啓発のための方策を検討することが適当である。

また、ISMAP についてはクラウドサービスリストへの追加登録を実施しつつ、制度運用の合理化に向けた検討を行うとともに、ISMAP-LIU の普及・活用を促進するための施策に取り組む必要がある。

また、サイバー空間におけるクラウドサービス事業者の存在感がますます高まっていることから、総務省として、国内外の事業者との連携を深めていくことが求められる。

オ. スマートシティにおけるサイバーセキュリティの確保

【現状】

我が国では、関係省庁の連携の下、Society5.0 の先行的実現の場として、補助事業等を通じてスマートシティを推進している。2020 年には、内閣府の戦略イノベーション創造プログラム（SIP）において定義されたスマートシ

[17] https://www.soumu.go.jp/main_content/000843318.pdf
[18] 最新のクラウドサービスリストは ISMAP ポータルサイトを参照。
https://www.ismap.go.jp/

ティリファレンスアーキテクチャに基づいて、総務省がスマートシティのセキュリティ対策の指針として策定した「スマートシティセキュリティガイドライン」について、多様な主体の関与、多様なデータの連携などのスマートシティの特徴を踏まえ、2021 年６月に第 2.0 版として改定した[19]。政府のスマートシティ関連事業においては、2022 年度から全ての事業において、同ガイドラインに基づいて作成した「スマートシティセキュリティ導入チェックシート」を応募書類の一部として位置付け[20]、セキュリティ対策について意識させるきっかけを作ることで、各地域における積極的なセキュリティ対策を促進している。また、各国における類似の取組との整合を図るため、海外の政府機関との意見交換の取組を行っている。

加えて、スマートシティ官民連携プラットフォーム（事務局：国土交通省）のスマートシティのセキュリティ・セーフティ分科会の活動において、セキュリティ対策の先進事例について官民で情報共有を行った。

【今後の取組】

「スマートシティセキュリティガイドライン（第 2.0 版）」について、引き続き、国内における普及促進及び国際的な制度調和に向けた海外の政府機関との意見交換の取組を行うことが求められる。また、「スマートシティリファレンスアーキテクチャ」の改訂案の検討も踏まえつつ、スマートシティの先進自治体や都市 OS ベンダー等の関係者との意見交換を通じて、国内外のスマートシティセキュリティに関するベストプラクティスなども参考としながら、より関係者にとって活用しやすいガイドラインとするために、必要な見直しを行っていくことが適当である。

カ. ICT-ISAC を通じた情報共有

【現状】

サイバーセキュリティ上の脅威が複雑化・巧妙化している中、ISP を含む通信事業者や放送事業者のみならずソフトウェアベンダーや情報関連機器製造事業者などの幅広い分野から構成される ICT-ISAC を通じた分野横断的な情報共有が重要である。

2019 年度から 2021 年度にかけては、総務省は、ICT-ISAC と連携し、刻々と公表される脆弱性情報について、様々な情報ソースと機械学習を用いることによって、その深刻度を自動的に判断する技術の有効性や、情報共有基盤

[19] https://www.soumu.go.jp/main_content/000757799.pdf
[20] https://www8.cao.go.jp/cstp/stmain/r4_smartcity.html

との連携可能性などを実証した。

また、ICT-ISAC では、平時から DDoS 攻撃の監視や ISP 間の情報共有等を行うとともに、2020 年東京オリンピック・パラリンピック競技大会や 2023 年の G7 サミットの開催期間等の際には、NISC や関係機関等とも情報共有を行っている。

１（１）の総合的な IoT ボットネット対策の端末側の対策においては、NOTICE の参加 ISP への注意喚起対象リストの通知や連絡調整等を行っている他、ネットワーク側の対策においては、2022 年度には電気通信事業者におけるフロー情報分析による C&C サーバ検知に関する実証事業の一環として C&C サーバリストの共有等に係る検討を行った。

【今後の取組】

引き続き、ICT-ISAC を通じて、情報通信分野における情報共有を促進することが適当である。また、ICT-ISAC は、国内で初めて設立された ISAC として、他分野の ISAC の支援や ISAC 間の情報共有のために積極的な役割を果たすことが期待される。

ICT-ISAC が運用する観測・調査システムや高度化された情報共有基盤の有効活用により、より迅速なサイバーセキュリティ対策が取られるよう、関係者による取組や利用の普及を促進することが適当である。

また、IoT ボットネット対策の推進に向けて、NOTICE 参加 ISP の拡大や C&C サーバリストや C&C サーバの検知手法の効果的な共有等に取り組むことが必要である。

キ. 放送設備におけるサイバーセキュリティ対策

【現状】

2019 年２月の情報通信審議会答申を踏まえ、放送設備に関するサイバーセキュリティ対策の確保を技術基準に位置づけるとともに、放送設備に関する定期状況報告の際、サイバー事案に起因する事故報告を明記して報告を求めることを内容として、放送法施行規則[21]（昭和 25 年電波監理委員会規則第 10 号）等を改正し、2020 年３月に施行した。

また、今後は放送分野においても、利便性向上、運用効率化及びコスト低減等の観点から、放送設備の IP 化・クラウド化等集約化が進むものと想定されており、「デジタル時代における放送の将来像と制度の在り方に関する

[21] https://elaws.e-gov.go.jp/document?lawid=325M50080000010

取りまとめ」（デジタル時代における放送制度の在り方に関する検討会2022年８月５日公表）において、「マスター設備の集約化・IP化・クラウド化は、放送事業者の経営の選択肢であることに留意しつつ、その要求条件を総務省において検討・整理すべきである」と提言されている。これらを受けて、2022年12月より、情報通信審議会放送設備安全信頼性検討作業班において、放送設備のIP化・クラウド化等に伴い新たに措置すべき安全信頼対策等、安全・信頼性に関する技術的条件の検討を実施している。

なお、これまでに国内でサイバー攻撃に起因する放送停止事故は報告されていない。

【今後の取組】

今後とも、放送法施行規則等の制度を着実に運用していくとともに、放送設備のIP化・クラウド化等の技術動向も踏まえ、放送における可用性確保の重要性を考慮した上で更なるサイバーセキュリティ対策の必要性を検討することが必要である。

（３）トラストサービスの普及

サイバー空間と実空間が高度に融合したSociety5.0の実現のためには、「誰が」、「何を」、「いつ」という実空間の構成要素を正しくサイバー空間でも再現することが必要であり、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みであるトラストサービスの重要性が高まっている。また、新型コロナウイルス感染症の感染拡大に伴い、あらゆるやりとりをデジタル完結する要請が高まる中、データを安心・安全に流通できる基盤の構築が不可欠であり、トラストサービスが重要な役割を果たすことがより一層期待されているところである。

【現状】

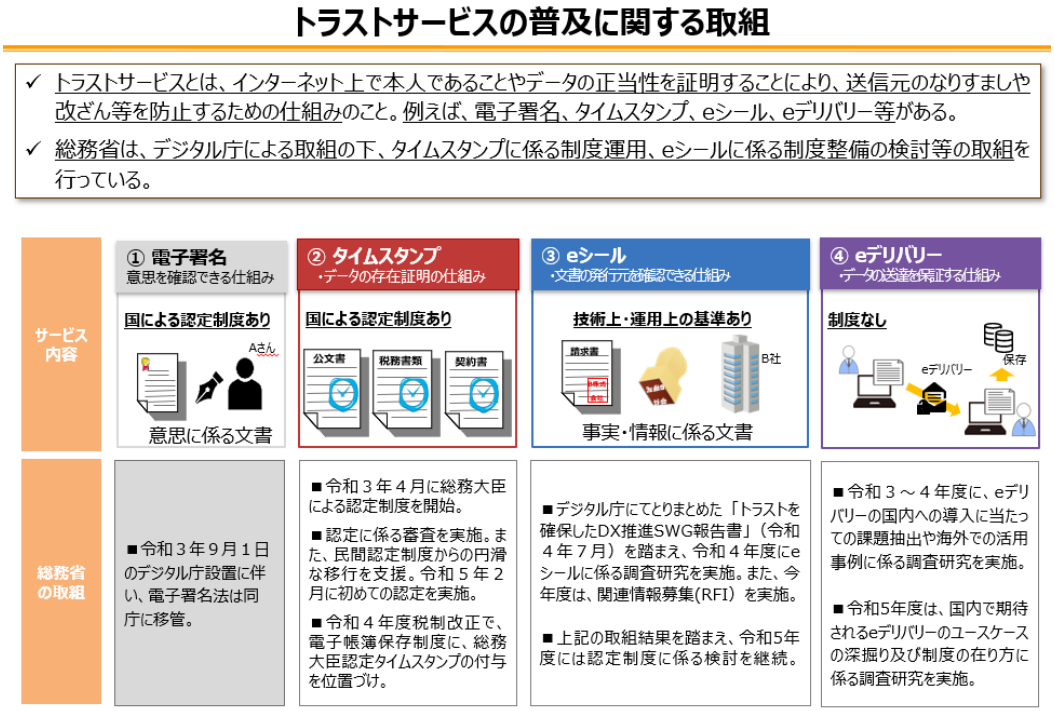
「サイバーセキュリティ戦略」において、「送信元のなりすましやデータの改ざん等を防止する仕組み（略）については、その利活用に向けて実効的な仕組みとする必要がある。」とされたことを踏まえ、総務省においては、タイムスタンプ・eシール等について取組を進めている。

タイムスタンプについては、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）」[22]を公布し、国によるタイムスタンプの

[22] 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）
https://www.soumu.go.jp/main_content/000742664.pdf

認定制度を整備したところ、2023 年２月には同認定制度に基づく最初の認定がなされており、制度の適切な運用に取り組んでいる。

また、e シールについては、「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」（2022 年７月 29 日デジタル庁）において、「e シールに係る指針」[23]（2021 年６月総務省）に基づき 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て取り組んでいくという方向性が示されたところである。総務省においては、その検討に当たり、我が国の e シールサービスの状況等を把握する目的で、令和４年度予算で「e シールに関する調査研究」を実施するとともに、2023 年４月には e シールサービスの状況等に関する情報提供依頼を発出するなど、必要な取組を進めている。



【今後の取組】

今後とも、政府におけるデータ戦略、とりわけトラストを確保する枠組みの実現に向けた検討の動向を踏まえながら、各種トラストサービスの普及に向けた取組を推進することが求められる。具体的には、タイムスタンプについて、国による認定制度を適切に運用するとともに、必要に応じて制度の見直し等を

[23] e シールに係る指針
https://www.soumu.go.jp/main_content/000756907.pdf

検討する必要がある。

また、e シールについて、引き続き、我が国の e シールサービスの状況等に関する情報収集を行いつつ、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、国による認定制度の創設を含めて検討を進めていくことが適当である。

さらに、e デリバリー等データ流通の信頼性の確保に向けた検討を行うことが適当である。

２．サイバー攻撃への自律的な対処能力の向上

（１）CYNEX（サイバーセキュリティ統合知的・人材育成基盤）、CYXROSS 等の推進

サイバーセキュリティは国家の基幹を守るもので、国際競争力の強化のほか、経済安全保障の観点からもサイバーセキュリティ産業の強化・育成は必須である。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、国内のサイバー攻撃情報等の収集・分析等が十分にできていない[24]。そのため、製品・サービスの開発に必要なノウハウや知見の蓄積が困難となっている。

また、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、人材育成を全て国で実施することは困難である[25]ため、民間事業者や教育機関等における自立的な人材育成が求められるものの、演習用の環境構築やシナリオ開発には高度な知識や技術力、そして基盤となる計算機環境が必要であり、民間企業・教育機関のみでは十分に対応できていない。

これらについては、「サイバーセキュリティ戦略」においても、「こうした状況を打破する取組の一環として、サイバーセキュリティに関する情報を国内で収集・蓄積・分析・提供していくための知的基盤を構築」、「社会全体でサイバーセキュリティ人材を育成するための共通基盤を構築し（中略）産学に開放する」と記載がなされている。これらの状況を踏まえ、我が国の企業を支えるセキュリティ技術が過度に海外に依存する状況を回避・脱却し、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。

【現状】

情報通信技術を専門とする我が国唯一の国立研究開発法人である NICT においては、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等を実施しており、NICT が有するこれらの技術・ノウハウ[26]や情報を中核として、我が

---

[24] 令和 4 年版情報通信白書第 3 章第 7 節「2我が国におけるサイバーセキュリティの現状」によれば、2020 年の国内企業シェアは 12%となっている。
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/pdf/n3700000.pdf

[25] NRI セキュアテクノロジーズの調査によれば、セキュリティ人材について、どちらかといえば不足している、あるいは不足していると回答した割合が米国 12.9%、英国 11.6%であるのに対して、我が国では 90.4%となっている。https://www.nri.com/-/media/Corporate/jp/Files/PDF/news/newsrelease/cc/2022/220208_1.pdf

[26] 世界的にも有数の規模を誇るサイバー攻撃観測網（NICTER）や、模擬的な企業ネットワーク上でマルウェア解析が可能なシステム（STARDUST）を保有し、また、研究開発だけでなく、実践的サイバー防御演習（CYDER）により NICT による人材育成を実施している。

国のサイバーセキュリティ情報の収集・分析とサイバーセキュリティ人材の育成における産学の結節点（サイバーセキュリティ統合知的・人材育成基盤）となる「CYNEX（サイネックス）」を 2020 年度３次補正予算及び 2021 年度予算で構築した。2022 年から試験運用を開始し、情報分析、製品検証、人材育成等を実施することで、CYNEX の更なる高度化に取り組んでいる。

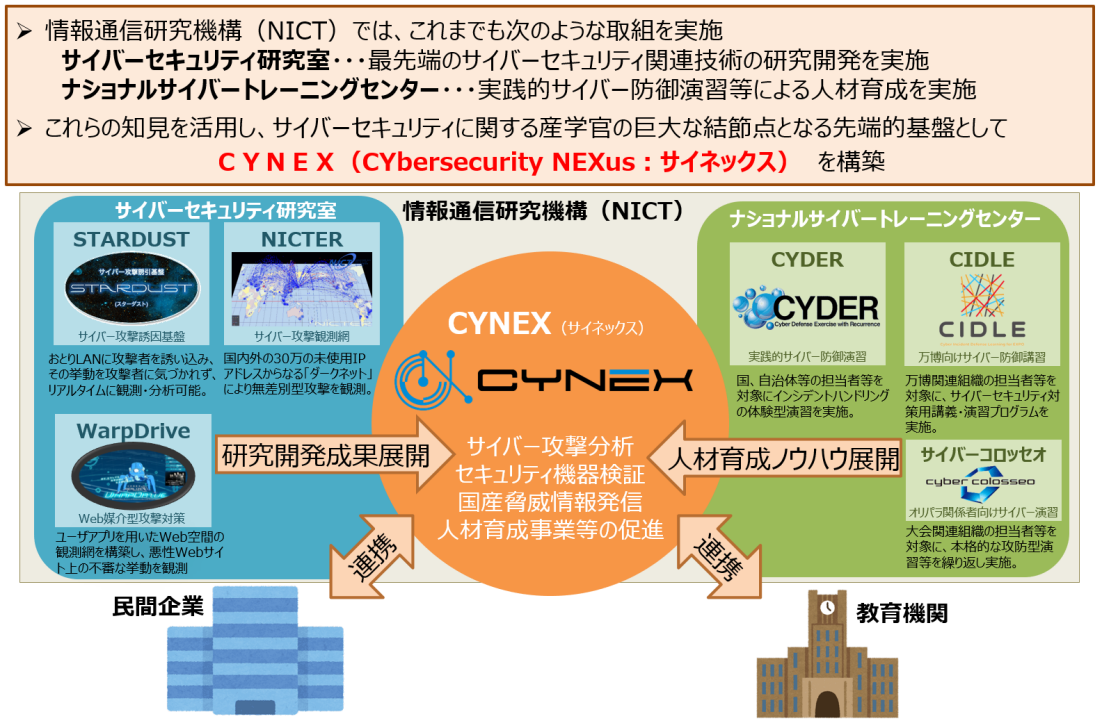
2023 年度から本格運用を開始するとともに、サイバーセキュリティに係る製品開発や人材育成等を進める大学、企業等の組織に事業連携の声掛けを行うことで、参画組織を 55 組織まで拡大した。

【今後の取組】

（情報収集・分析）

CYNEX では、得られた情報の効果的な共有と適切な管理、育成人材の質の担保等にも留意しつつ、システム基盤構築・運営環境整備を引き続き進めることが求められ、その計画・進捗については、本タスクフォースに適宜報告をし、方向性について最新のセキュリティ動向等を踏まえた議論を深めていく必要がある。

サイバーセキュリティに関する産学官の結節点『CYNEX』



また、NICT は、CYNEX が産学官の組織にとって利用したいと思える環境となるよう関係者との密な意見交換を行い必要な改善を施すとともに、利用する全

ての組織にとっての拠り所となるコミュニティの形成を積極的に図ることが求められるほか、産学官の参画組織がサイバー攻撃の収集・分析等に関してより深い関係性と信頼性が築ける運営が期待される。

なお、CYNEX 等では、利用者が自身で構築しているネットワーク内の機器にはアプローチできておらず、未知のマルウェア等を様々なネットワーク利用者の実利用環境から察知・収集することは、迅速な対処の分析につながる重要かつ有効な手段である。このことから、利用者参加型の Web 媒介型攻撃大規模観測プロジェクト（WarpDrive）を拡張開発することで、国内のマルウェア感染状況を利用者等からもリアルタイムかつ横断的な集約を可能とし、その分析結果を当該利用者等に対して迅速に通知する仕組みを 2023 年度中に CYNEX で実現することが期待される。

また、一部の府省庁に国産セキュリティソフトを導入し、得られたマルウェア情報等を CYNEX へ集約・分析することで、海外製品のみに頼らずに我が国独自のサイバーセキュリティ脅威情勢分析能力を強化する取組である「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（サイクロス））」を一層推進すべきである。さらに、生成した情報を国産セキュリティソフトの導入府省庁のみでなく、政府全体のサイバーセキュリティを統括する NISC、行政各部の情報システムの監視・分析を担う GSOC 及び常時診断・対応型のセキュリティアーキテクチャの実装等を行っているデジタル庁等へ共有することで、政府全体のサイバーセキュリティの向上が期待される。

（人材育成）

社会全体でのサイバーセキュリティ人材の育成を推進するため、サイバーセキュリティの人材育成に関し、演習の実施に必要となる幅広い要素（データセット、演習用ミドルウェア、計算機リソース等）を総合的にカバーする、オープン型の新たな人材育成プラットフォームを引き続き運用し、最新の技術動向・脅威動向からのインプットや利用者からのフィードバックを踏まえて改善していくことが求められる。

また、当該プラットフォーム上で利用可能な、産学官連携で作成する演習用教材等の共用コンテンツの拡充を図るとともに、これらのコンテンツを利用して当該プラットフォーム上で演習を提供可能な講師・チューターの育成に取り組む必要がある。

さらに、当該プラットフォームが積極的に活用されるようにするためのコミュニティの支援に取り組む必要がある。

（２）研究開発の推進

複雑化・巧妙化したサイバー攻撃の増大、サプライチェーンの複雑化・グローバル化に伴うリスクの増大による様々な脆弱性を対象とする攻撃の発生等について、適切に検知・対処するため、新たな脅威の発生可能性など、安全保障の観点を含め我が国をとりまく現下の課題認識に基づき、我が国において、サイバーセキュリティに係る実践的な研究開発の推進が求められる。

また、研究開発の推進に当たっては Beyond 5G をはじめとするネットワーク技術の高度化、機械学習等の AI 技術を駆使した自動分析・自動対策技術の確立・高度化などデジタル技術の進展に応じた観点や、サイバーセキュリティの基盤技術を維持・発展させる観点、人の誤認識につけ込むサイバー攻撃手法の高度化を踏まえ、人の認識や行動特性に応じたユーザブルセキュリティの見地も重要であり、中長期的な技術トレンドを視野に入れた柔軟な対応が求められる。

ア. CRYPTREC の取組の推進

社会全体のデジタル化の進展により、あらゆる主体が参画して社会経済活動が営まれる公共空間となったサイバー空間の安全性・信頼性を確保することが求められている中で、情報の秘匿や改ざんの防止、認証等に用いられる暗号技術は既に様々な製品やサービスに組み込まれ、セキュリティを支える基盤技術として欠かせないものとなっている。また、サイバー空間の拡大に伴う大量のデータの流通・連携を支える上でも、暗号技術の重要性は一層増していくと考えられる。

このような状況の下、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・検討するプロジェクトである CRYPTREC（クリプトレック）[27]に求められる役割は大きく、その取組を一層推進していくことが求められる。

【現状】

デジタル庁、総務省及び経済産業省は、CRYPTREC の活動を通じて暗号技術の評価等を行い、「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

[27] Cryptography Research and Evaluation Committees の略。デジタル庁、総務省及び経済産業省が共同で運営する「暗号技術検討会」と、NICT 及び IPA が共同で運営する「暗号技術評価委員会」及び「暗号技術活用委員会」で構成される。

（CRYPTREC 暗号リスト）」[28]を策定しており、2023 年３月、暗号アルゴリズム利用実績調査等の結果を踏まえた CRYPTREC 暗号リストの改定版[29]を策定した。

また、NICT 及び独立行政法人情報処理振興機構（IPA）は、CRYPTREC の活動を通じて、大規模な量子コンピュータが実用化されても安全性を保つことができると期待されている耐量子計算機暗号（PQC）や、従来の暗号技術に対して高機能性を有する高機能暗号に係る調査を行い、2023 年３月、「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」[30]及び「CRYPTREC 暗号技術ガイドライン（高機能暗号）」[31]を策定した。併せて、2023 年３月、「暗号鍵管理システム設計指針（基本編）」[32]の内容を詳説した「暗号鍵管理ガイダンス」[33]を策定した。

【今後の取組】

暗号技術に対する解析・攻撃手法は日々高度化していることから、電子政府システムでの利用に際して安全な暗号技術を選択することが可能となるように、CRYPTREC の活動を通じて今後も継続的に CRYPTREC 暗号リストに掲載されている暗号技術等を監視し、必要な場合には都度、CRYPTREC 暗号リストを改定していくことが必要である。

また、暗号技術の適切な利用に資するように、CRYPTREC の活動を通じて、暗号技術の動向と社会のニーズを踏まえ、ガイドライン類の整備を進めるとともに、量子コンピュータの発展が現代暗号に及ぼす影響を引き続き分析・予測することが必要である。

イ. NICT における研究開発の推進

【現状】

NICT において、観測データの拡充と有効活用を目指し、無差別型攻撃観測技術や標的型攻撃観測技術の高度化、機械学習等の AI 技術を用いたマルウェア感染活動の早期検知技術やセキュリティアラートの自動グルーピング等によるトリアージ技術等に関する高度化を実施した。

---

[28] https://www.cryptrec.go.jp/list.html
[29] https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022.pdf
[30] https://www.cryptrec.go.jp/report/cryptrec-gl-2004-2022.pdf
[31] https://www.cryptrec.go.jp/report/cryptrec-gl-2005-2022.pdf
[32] https://www.ipa.go.jp/security/crypto/guideline/gmcbt80000005u7d-att/ipa-cryptrec-gl-3002-1.0.pdf
[33] https://www.ipa.go.jp/security/crypto/guideline/gmcbt80000005u7d-att/ipa-cryptrec-gl-3004-1.0.pdf

また、パーソナルデータなど機密性の高いデータを複数組織間で互いに開示することなく安全に解析することができるプライバシー保護連合学習技術について、金融機関を対象に社会実装を進めたプライバシー保護技術について、クレジットカード分野における不正取引検知への応用を進めている。さらに差分プライバシーなどを用いたセキュリティ強化手法の研究開発を引き続き実施している他、あらゆる計算機で解読不可能な安全性を実現する量子暗号を活用した量子セキュアネットワーク技術等の研究開発を実施している。

これらの研究開発の成果については、例えば、標的型攻撃観測技術の高度化では、並行ネットワーク構築機能の強化を進めたサイバー攻撃誘引基盤（STARDUST）の外部利用を推進し、10 以上の機関に利活用されるなど社会実装および成果展開を推進した。

【今後の取組】

NICT においては、第５期中長期目標・計画にしたがって、研究開発を着実に推進し、ICT を取り巻く諸課題やサイバー攻撃の状況を常に踏まえながら、情報通信関連では国内唯一の国立研究開発法人として産学との連携のもと研究開発を更に牽引することが求められる。

サイバー攻撃対処能力の絶え間ない向上と多様化するサイバー攻撃の対処に貢献するため、複雑化・巧妙化するサイバー攻撃に対応した攻撃観測・分析・可視化・対策技術、大規模集約された多種多様なサイバー攻撃に関する情報の横断分析技術、新たなネットワーク環境等のセキュリティ向上のための検証技術の研究開発を実施していく必要がある。

また、社会の持続的発展において欠くことの出来ない情報のセキュリティやプライバシーの確保を確かなものとするため、耐量子計算機暗号等を含む新たな暗号・認証技術やプライバシー保護技術の研究開発を実施し、その安全性評価を行うとともに、安全な情報利活用を推進し、国民生活を支える様々なシステムへの普及を図ることが求められる。加えて、量子暗号をはじめとする量子セキュアネットワーク技術や、ノード内の信号処理も量子的に行う完全な量子ネットワークの実現を目指した量子ノード技術の研究開発を推進する必要がある。

ウ. 大学や民間企業における研究開発の支援等

【現状】

NICT による研究開発のほか、大学や民間企業において、国の研究開発プロ

ジェクトとして、以下の研究開発を実施している。

- 2020～2024 年度「グローバル量子暗号通信網構築のための研究開発」
- 2018～2023 年度「衛星通信における量子暗号技術の研究開発」
- 2021～2025 年度「グローバル量子暗号通信網構築のための衛星量子暗号通信の研究開発」
- 2021～2024 年度「安全な無線通信サービスのための新世代暗号技術に関する研究開発」

【今後の取組】

安全な衛星通信ネットワークの構築を可能とし、盗聴や改ざんが極めて困難な量子暗号通信を超小型衛星に活用するための技術の確立に向け、「衛星通信における量子暗号技術の研究開発」や、量子コンピュータ時代において国家・重要機関間の機密情報を安全にやりとりするための、距離に依らない堅牢な量子暗号通信網の実現に資する、地上系の量子暗号通信の更なる長距離化技術の確立に向けた「グローバル量子暗号通信網構築のための研究開発」について、継続的に取り組む必要がある。

加えて、数百～数千 km といった大陸間スケールでの量子暗号通信網を構築できる機能を検証する衛星系と地上系を統合した量子暗号通信網実現のための技術の確立に向けた「グローバル量子暗号通信網構築のための衛星量子暗号通信の研究開発」も継続が求められる他、暗号技術に関する研究開発として、「安全な無線通信サービスのための新世代暗号技術に関する研究開発」において、5G 等のための超高速・大容量に対応した共通鍵暗号方式技術や耐量子計算機暗号の機能付加技術等の研究開発に取り組むことが重要である。

これらについて、国及び国民の安全・安心の確保、産業競争力の強化等の観点から、重要な情報を安全に保管する手段として、機密性・完全性等を有し、かつ市場化を見据えて国際競争力の高い、量子通信・暗号に関する研究開発を引き続き実施する必要がある。

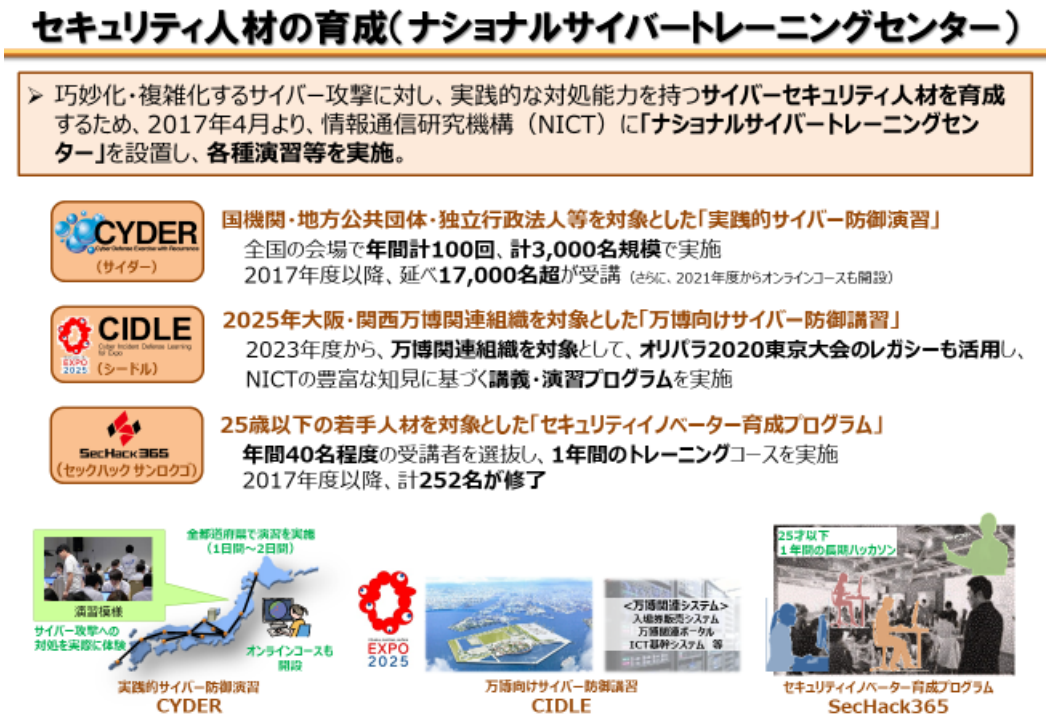
さらに、近年、顕在化している IoT 機器を様々な方法で悪用するサイバー攻撃等、変性する脅威に柔軟に対抗するための取り組みが重要であり、1（1）の NOTICE の取組等も通じて脅威観測を行い、研究・レポートの発表等を通じて観測データの有効活用を図ることで、関係機関等とも連携しつつ、全般的なサイバー攻撃の動向や脅威等についての状況把握や情報共有を進めることが期待される。

（３）人材育成の推進

サイバー攻撃が複雑化・巧妙化している一方で、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た状況が継続している。実際、人材不足に起因したインシデントの発生や被害の拡大が相次ぐ中、サイバーセキュリティ人材の育成は喫緊の課題となっており、「サイバーセキュリティ戦略」においても、「「質」・「量」両面での官民の取組を、一層継続・深化させていくことが必要」とされている。

このため、総務省は、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（サイダー）、CIDLE（シードル）、SecHack365（セックハックサンロクゴ））を積極的に推進している。また、地域のコミュニティや企業、教育機関等と連携して、サイバーセキュリティ人材を自立的に育成していくためのエコシステムの確立に向けた実証を行っている。

サイバーセキュリティ人材に対する社会のニーズ拡大に応えるため、こうした取組を引き続き実施・拡充することが求められる。



ア．実践的サイバー防御演習（CYDER）の実施

【現状】

総務省は、NICT のナショナルサイバートレーニングセンターにおいて、2017 年度から、行政機関等の実際のネットワーク環境を模した大規模仮想

LAN 環境を構築の上、国の機関等、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体験型の実践的サイバー防御演習（CYDER）を実施（全都道府県で集合演習を年間 100 回、計 3,000 名規模）しており、2022 年度は、集合演習を 108 回実施し、計 3,327 名が受講した（2017 年度からの合計で 17,194 名が受講）。

また、2021 年度から開始した CYDER のオンライン演習について、2022 年度は、集合演習の受講に必要な知識を習得するためのオンライン入門コースを新たに開講し、オンライン標準コースと合わせて 705 名が受講した。

【今後の取組】

組織を標的としたサイバー攻撃の複雑化・巧妙化が進み、被害を受ける組織が相次ぐ中、攻撃に対して迅速かつ的確に対応するためには、その対応を担う各組織の情報システム担当者等の能力強化を、広範かつ継続的に実施することが重要である。そのため、CYDER が果たすべき役割は大きく、演習に必要となるリソース（資機材や教材、講師・チューター等）を確保し、CYNEX の基盤も活用して、CYDER の実施に係る取組を一層推進していくことが求められる。

CYDER を受講した地方公共団体の数は順調に拡大しているものの、未受講の団体が依然として存在することから、未受講団体がサイバーセキュリティを確保する上での弱点とならないように、引き続き、地方公共団体に対し、CYDER の受講促進を図ることが必要である。

また、サイバー攻撃に対する対応能力を組織として維持できるようにするため、その目的に適った演習コースを開設するとともに、組織内の CSIRT[34] 等のチーム内に、当該演習コースの受講者が常に在籍している状況の実現を目指すべきである。地方公共団体をはじめとする各組織に対しては、この観点も踏まえ、CYDER の受講促進を図ることが必要である。

オンライン演習は、集合演習と比べて、受講に係る負担を軽減するために有用な方法であり、今後も積極的に活用を進めるべきである。その際、十分な演習効果を得られるように、演習内容に応じて集合演習とオンライン演習を適切に使い分けることが必要である。併せて、集合演習と同等の演習効果を得られるように、オンライン演習の改良を進めることも必要である。

CYDER は、これまで、主に国の機関等及び地方公共団体を対象として実施されてきた。他方、近年、病院等の重要インフラ事業者がサイバー攻撃を受

[34] Computer Security Incident Response Team の略。セキュリティインシデントに対して対処するためのチームのこと。

け、その運営に大きな支障を生じさせる事案が相次いでおり、その要因として、当該事業者の人的能力の不足も挙げられている。重要インフラ事業者の機能不全が社会経済活動に与える影響を踏まえ、こうした事案に対応するため、重要インフラ事業者に対する CYDER の提供を拡大することが求められる。

さらに、我が国の安全保障環境が厳しさを増す中、政府の国家安全保障戦略において、「Ⅳ２（４）ア　サイバー安全保障分野での対応能力の向上」では「政府内外の人材の育成・活用の促進等を引き続き図る。」とされているところ、これまでの CYDER による人材育成の実績を踏まえ、サイバー安全保障分野における人材育成に CYDER やその知見等を活用することも視野に入れて関係省庁と調整すべきである。

イ．万博向けサイバー防御講習（CIDLE）の実施

【現状】

2020 年東京オリンピック・パラリンピック競技大会での経験からも明らかなように、国際的に知名度の高いイベントはサイバー攻撃の標的とされるおそれがある。こうした背景から、2025 年日本国際博覧会（大阪・関西万博）の開催に当たり、サイバー攻撃に対する備えを万全なものとするため、大阪・関西万博主催者（公益社団法人 2025 年日本国際博覧会協会）及び関係自治体（大阪府及び大阪市）から総務省に対して、サイバーセキュリティ人材の育成に係る支援要望が寄せられた。

当該要望を踏まえ、総務省は NICT のナショナルサイバートレーニングセンターにおいて、2023 年度中に、大阪・関西万博関連組織を対象とした万博向けサイバー防御講習（CIDLE）を開始する予定としている。

【今後の取組】

サイバー攻撃の複雑化・巧妙化が進む中、大阪・関西万博の安全な開催に資するように、総務省は、大阪・関西万博主催者等からの要請を踏まえ、同主催者等と緊密に連携し、CIDLE を実施することが必要である。

CIDLE の実施に当たっては、総務省が 2020 年東京オリンピック・パラリンピック競技大会に向けて 2017 年度から 2020 年度まで実施し、同大会の安全な開催に貢献したサイバーコロッセオのレガシーを活用するとともに、最新のサイバー攻撃動向に対応して演習内容をアップデートしている CYDER の知見を踏まえ、実践的な人材を育成することが重要である。

ウ. SecHack365 の実施

【現状】

NICT のナショナルサイバートレーニングセンターにおいて、2017 年度から、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「SecHack365」を実施している。2022 年度は 40 名が修了し、2017 年度からの合計で 252 名が修了した。

【今後の取組】

本取組の特徴は、NICT の持つサイバーセキュリティの研究資産を活用しながら、実際のサイバー攻撃関連データに基づいたセキュリティ技術の研究・開発を、第一線で活躍する研究者・技術者が１年かけて継続的かつ本格的に指導する点にある。我が国における高度セキュリティ人材の育成のため、引き続き本取組を実施するとともに、本取組を修了した人材のネットワークを強化し、社会への効果的な定着を促進する必要がある。

エ. 地域人材エコシステムの形成

【現状】

サイバーセキュリティ事業者が都市部に集中し、地域においては、サイバーセキュリティに関する雇用の受け皿が無いことから、若年層がサイバーセキュリティ関連業界を目指さず、地域におけるサイバーセキュリティ人材が更に不足するといった悪循環が生じている。他方で、都市部に集中するサイバーセキュリティ事業者が過度に集中する業務の一部をアウトソーシング（外部発注）する動きがある。このため、セキュリティ人材のエコシステムの自走に必要となる研修カリキュラム等を構築し、沖縄県において、就業の場の確保と就業につながる研修を一体的に行い、地域における人材エコシステムの形成を図るモデル事業を実施した。加えて、沖縄県内でエコシステムを自走していくための支援を行うとともに、他地域におけるエコシステム確立に向けて調査検討を行った。

【今後の取組】

これまでに作成した研修カリキュラム等をパッケージ化した上で、他地域に横展開して研修を行い、エコシステムの形成に向けた課題整理を行うとともに、モデル事業対象地域（沖縄県）におけるエコシステム自走に対する支援を継続し、セキュリティ人材のエコシステムの確立を図ることが必要である。

３．国際連携の推進

サイバー空間は国境を越えて利用される領域であることから、サイバーセキュリティの確保のためには国際連携の推進が必要不可欠である。そのため、各国政府・民間レベルでの本分野における情報共有や国際標準化活動への積極的な関与を進めていく必要がある。

また、国際的なサイバーセキュリティ上の弱点を減らし、日本を含む世界全体のリスクを低減させる等の観点から、インド太平洋地域をはじめとする地域の開発途上国に対する能力構築支援を行い国際的な人材育成への貢献を図るほか、国内企業のサイバーセキュリティ分野における国際競争力の持続的な向上を図る取組も推進することが重要である。

（１）有志国との二国間連携の強化

【現状】

総務省が主催する ICT 分野の政策対話や外務省が主催するサイバー協議等において、米国をはじめとする G7 各国を中心に総務省のサイバーセキュリティ政策（IoT セキュリティ、5G セキュリティ）の積極的な発信や意見交換を実施したほか、各会合を通じて日 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）への教材提供を呼びかけた。また有志国とは、インド太平洋地域での開発途上国に対する能力構築支援活動の現状や今後の展開について意見交換を行った。

【今後の取組】

引き続き、情報の自由な流通の確保を基本とする考えの下、当該理念を共有する国を中心に、能力構築支援や国際標準化の分野における連携強化のための関係性構築に取り組むことが必要である。

（２）多国間会合を通じた有志国との連携の強化

【現状】

G7 デジタル技術大臣宣言及び安全で強靭なデジタルインフラの構築に向けた G7 アクションプランにおいて、世界銀行等の国際機関と連携し、発展途上

国における安全で強靱なデジタルインフラを支援することが確認された。[35]

OECD（経済協力開発機構）では、主にWPSDE（デジタル経済セキュリティ作業部会）における政策議論に参加しているほか、日ASEANサイバーセキュリティ政策会議等、多国間の枠組みにおけるセキュリティ関係の議論に積極的に参画した。また、2021 年９月の第２回日米豪印首脳会合において日米豪印サイバー上級会合を設立することで合意し、定期的に開催されている。

WPSDEでは、日本の意見を発言・提出するとともに、副議長として会合の進行に寄与するなど、プレゼンスを発揮した。また我が国は、2023年3月に「The Global Forum on Digital Security for Prosperity」[36]をOECD事務局とともに主催し、IoTやAIに関するデジタルセキュリティの議論や政策立案コミュニティと技術者コミュニティの連携に関する議論が行われ、デジタルセキュリティを取り巻く課題が多様化・複雑化・高度化していく中で、マルチステークホルダーを巻き込んだ政策立案・政策実施が重要であるという点が様々な見地から語られる意義深い会合となった。

日 ASEAN サイバーセキュリティ政策会議においては、「総合対策 2022」やNOTICEやNICTERの取組、及びAJCCBCにおける演習コンテンツ等の紹介を行い、各国との連携の更なる強化を図った。

また、2022年5月の日米豪印首脳会合共同声明[37]において、「日米豪印サイバーセキュリティ・パートナーシップ」[38] が公表された。2023 年５月の首脳会合[39]では、サイバーへの意識向上を目的とした「サイバー・チャレンジ」[40]を歓迎するとともに、「ソフトウェア・セキュリティに関する共同原則」[41]及び「重要インフラのサイバーセキュリティに関する共同原則」を歓迎した。

さらに、同時に日米豪印重要・新興技術作業部会の成果として「Open RANセキュリティ報告書」が公表された。[42]

【今後の取組】

---

[35] G7群馬高崎デジタル・技術大臣会合の開催結果 https://www.soumu.go.jp/menu_news/s-news/01tsushin06_02000268.html

[36] https://www.oecd.org/digital/digital-security/

[37] https://www.mofa.go.jp/mofaj/fp/nsp/page1_001188.html

[38] https://www.mofa.go.jp/mofaj/files/100347900.pdf

[39] https://www.mofa.go.jp/mofaj/fp/nsp/page1_001702.html

[40] https://www.cyberchallenge.tech/

[41] (原文)https://www.mofa.go.jp/mofaj/files/100509254.pdf
(仮訳)https://www.mofa.go.jp/mofaj/files/100509255.pdf

[42] https://www.soumu.go.jp/menu_news/s-news/01tsushin06_02000270.html

G7 デジタル技術大臣宣言[43]、安全で強靱なデジタルインフラの構築に向けた G7 アクションプラン[44]及び 2023 年５月の日米豪印首脳会合共同声明を踏まえ、途上国への能力構築支援を国際機関と連携しつつ着実に実現することが求められる。

また、日米豪印においては、2022 年 5 月の日米豪印首脳会合の機会に当局間で署名した協力覚書（ＭＯＣ）に基づき、Open RAN の検証、相互運用性、セキュリティに関する情報共有や試験環境の共有の可能性の検討等について、引続き協力・活動を実施することが適切である。

その他、2023 年 10 月に京都で開催予定の IGF（インターネットガバナンスフォーラム）における議論、Quad を通じた日米豪印の連携や、日 ASEAN サイバーセキュリティ政策会議等を通して今年友好協力 50 周年を迎える ASEAN との関係強化を図る等、情報の自由な流通の確保を基本とする考えの下、当該理念を共有する国を中心に、連携強化のための関係性構築に取り組むことが必要である。

（３）ISAC 間を通じた民間分野での国際連携の促進

【現状】

サイバー攻撃は国境を越えて行われるため、サイバーセキュリティ対策においては、脅威情報（攻撃情報）等の国際的な共有を行うことにより、国際レベルでの早期の攻撃挙動等の把握が必要不可欠である。そのため、国内の産業分野ごとに設立されるサイバーセキュリティに関する脅威情報等を共有・分析する組織である ISAC において、国際的な ISAC 間等の連携を促進していく必要がある。

ICT 分野では、ICT-ISAC と 2019 年に協力覚書を締結した米国 IT-ISAC 及びその関係機関との連携について、定期会合の開催等を通じて強化している。また、米国以外の国・地域等との連携も促進しており、2021 年度に続き、2022 年度にも EU との ISAC 関連団体との意見交換会を開催した。

また、ASEAN 各国を対象とした ISP 向け日 ASEAN 情報セキュリティワークショップを開催し、2022 年度には 3 年ぶりとなる対面会合を東京で実施した。

---

[43] （原文）https://www.soumu.go.jp/main_content/000879099.pdf
（仮訳）https://www.soumu.go.jp/main_content/000879093.pdf

[44] （原文）https://www.soumu.go.jp/main_content/000879102.pdf
（仮訳）https://www.soumu.go.jp/main_content/000879096.pdf

【今後の取組】

ICT-ISAC と米国 IT-ISAC 間における連携を更に促進するため、日本側及び米国側関係者との議論を重ね、情報共有の自動化、共有する情報の種類、情報の活用方策等、情報共有のあり方について検討を進めることが重要である。加えて、EU をはじめとする他の国・地域の ISAC 関連組織との連携を引き続き促進することが求められる。

また、ASEAN 各国の ISP との間では、信頼醸成の構築のためのイベントを実施することに加え、民間レベルにおいてより実感的に情報共有を行うことの重要性を意識し、サイバーセキュリティに関する脅威情報の共有を促進できるよう検討を進めることが必要である。

（４）インド太平洋地域等における開発途上国に対する能力構築支援

ア. AJCCBC

【現状】

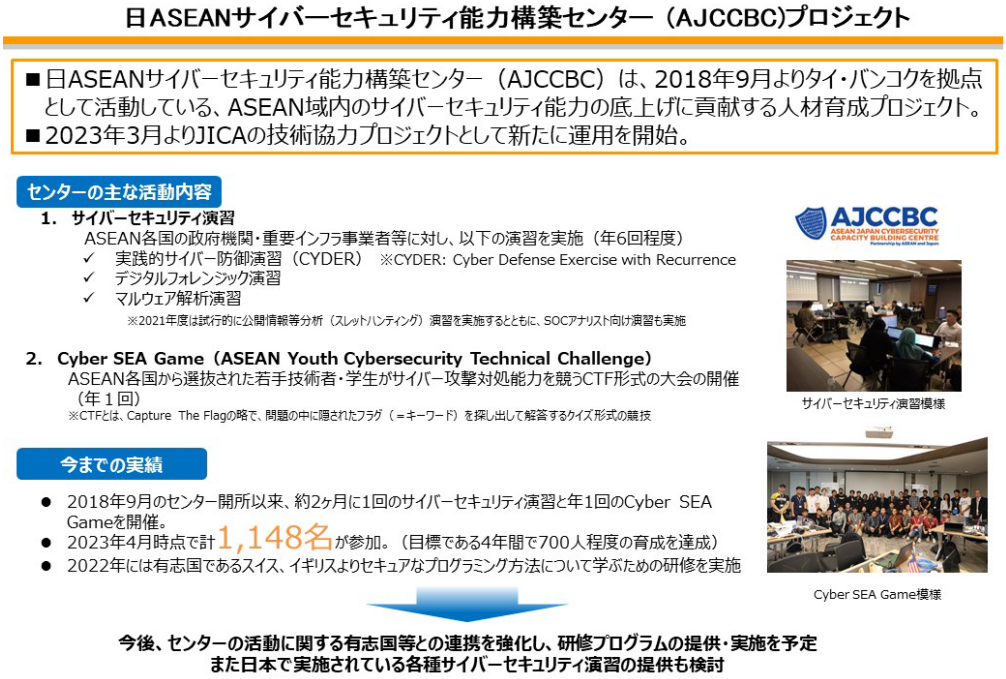
ASEAN 各国との協力関係を強化するため、2018 年９月にタイのバンコクに設立した AJCCBC において、CYDER[45]等を通じて、ASEAN 各国のセキュリティ人材の育成支援を実施した（AJCCBC において日本が提供する演習プログラムには、2023 年４月現在 1,148 名が参加）。また、オンライン環境で受講可能なプログラムの拡充や、第三者との連携による新たな演習提供に向けた調整等を実施した。

【今後の取組】

引き続き、ASEAN 各国との協力関係強化の観点から、AJCCBC の活動を拡大していくことが必要である。

[45] 「CYDER」の詳細は P31～33 参照。

具体的には、今年度からは JICA の技術協力プロジェクトの活用等により、プロジェクト運営体制の強化を図っていく他、AJCCBC の更なる活性化や ASEAN 域内への貢献に向けて、第三者（有志国）との更なる連携等による受講可能な演習プログラムの拡充、学術機関等への演習対象の拡大等に取り組むことが求められる。



イ. 大洋州島しょ国への展開

【現状】

2021 年 12 月にサイバーセキュリティ戦略本部が決定した「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」[46]に則り、AJCCBC の運営を通じて得られた知見やノウハウを活用し、新たにインド太平洋地域でのサイバーセキュリティ能力の向上に資するため、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プロジェクトの検討を進めている。

2022 年度に対象地域におけるニーズ等を把握するための実地調査を実施したところ、サイバーセキュリティ人材育成に関する日本からの支援のニーズが高く、初級から上級レベルまで学習することができる網羅的な演習プログラムの提供等に対して大きな期待が寄せられていることが判明している。

[46] https://www.nisc.go.jp/pdf/policy/kokusai/cs-tojyokokushien2021.pdf

【今後の取組】

2022 年度の調査結果を踏まえ、対象地域のニーズに合ったサイバーセキュリティ能力構築支援の最適な方法を検討するため、2023 年度は AJCCBC で提供している演習プログラムを基にトライアル演習を実施するとともに、この結果を踏まえ、可能な限り早期の本格的な演習の立ち上げに向けて検討を加速することが求められる。

ウ. 国際機関との連携

【現状】

世界銀行のデジタル開発パートナーシップ（DDP）プロジェクトに係る取組の一環として、総務省は、2019 年に開発途上国のサイバーセキュリティ能力構築支援を行うプロジェクトを世界銀行と連携して実施した。

2021 年には、低・中所得国のサイバーセキュリティ問題の解決についてのグローバルな知見、世界銀行のクライアント国における国別評価、技術支援、サイバーセキュリティ従事者のための研修、能力開発支援を提供するため、DDP 傘下に新たにサイバーセキュリティマルチ・ドナー信託基金が設立された。

【今後の取組】

開発途上国の様々なニーズに応えるため、国内の関係省庁及びサイバーセキュリティ関連企業と連携し、サイバーセキュリティマルチ・ドナー信託基金の下における世界銀行との連携の具体化に向けた検討を行う。

また、その他の国際機関との連携についても積極的に検討を行う。

（５）国際標準化機関における日本の取組の発信及び各国からの提案への対処

【現状】

2016 年７月に IoT 推進コンソーシアムにおいて策定された「IoT セキュリティガイドライン」[47]の国際標準への反映等に向けて、ITU-T SG17 及び ISO/IEC JTC1 SC27 における IoT セキュリティに係る国際標準化の議論に積極的に貢献している。なお、同ガイドラインは、ISO/IEC JTC1 SC27 では、2022 年 6 月に ISO/IEC 27400[48]として発行された。

[47] https://www.soumu.go.jp/main_content/000428393.pdf
[48] https://www.iso.org/standard/44373.html

2021 年 10 月には、ITU-T SG17 において、日本発のサイバーセキュリティのノウハウが、ITU-T 勧告 X.1060[49]「Framework for the creation and operation of a cyber defence centre」として発行された。2022 年度は発展途上国からのフィードバックも踏まえ、補足的な解説文書の作成が進められた。

2022 年８～９月の SG17 会合では、Ⅱ1.（２）イで言及された「5G セキュリティガイドライン第１版」[50]をベースとした勧告案の作成を提案し、作業項目の設立が合意された。

また、「自由、公正かつ安全なサイバー空間」という基本的な理念に必ずしも整合的でない動きが見られる現状も踏まえつつ、必要な調査や連携強化の取組を実施している。

【今後の取組】

IoT セキュリティに係る国際標準化が ITU-T で議論されているところであり、関係府省庁と連携し、こうした活動に積極的に貢献していくことが重要である。また、5G セキュリティをはじめとしたⅡ１.(2)イの「情報通信分野におけるサプライチェーンリスク対策」に係る分野の具体的施策について、必要に応じて国際連携の場で共有するとともに、国際標準化等の可能性について継続的に検討することが重要である。

また、サイバーセキュリティ分野の国際標準化動向について、前述の「自由、公正かつ安全なサイバー空間」という基本的な理念に必ずしも整合的でない動きが見られる現状も踏まえつつ、我が国として注力すべき分野や具体的な課題等について調査を行うとともに、積極的な対処のために必要な連携強化に向けて継続的に取り組んでいく必要がある。

加えて、標準化活動には蓄積されたノウハウが必要となることから、当該ノウハウの普及や継承のために、標準化活動に参加しやすくなるような方策を検討する必要がある。

（６）国内企業の国際展開への支援

【現状】

国内企業のサイバーセキュリティ製品・ソリューションの海外への展開を支援するための調査等を実施している。

---

[49] https://www.itu.int/rec/T-REC-X.1060-202106-I

[50]「5G セキュリティガイドライン第1版」の詳細は P14 参照。

2022 年度は、主にアフリカ地域での普及啓発を図ることを目的として、ITU-T 勧告 X.1060 の展開・普及に係る課題を整理するための調査を実施した。加えて、動画の公開[51]やグッズ配布等、ITU-T 勧告 X.1060 の周知広報活動を行った。他、ISP 向け日 ASEAN 情報セキュリティワークショップにおいて、日本国内のサイバーセキュリティ製品・サービスの展示会を行い、ASEAN からの参加者に製品・サービスについて知ってもらう機会を提供した。

過去の実証事業の結果によれば、現地法人を持つ大企業においてはサイバーセキュリティ製品・ソリューションの受注実績がある一方、現地法人を持たない中小企業からは、海外展開を単独で行うことは困難との声も多い。

【今後の取組】

我が国におけるサイバーセキュリティの知見を元に策定された ITU-T 勧告 X.1060 の普及展開に向けた取組を引き続き実施し、本勧告の普及を通して、我が国の取組と整合的なサイバーセキュリティ体制の整備を支援すること等により、日本の製品・サービスを海外に展開しやすい環境を構築するほか、引き続き中小企業の海外展開を含めた効果的な支援の在り方の検討を行うことが必要である。その際、情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携といったサイバーセキュリティ戦略上の基本原則の実現・浸透を図ることが重要である。

[51]「5 分でわかる X.1060 CDC / Cyber Defence Centre in 5 minutes」: https://www.youtube.com/watch?v=2qkS7NPTHWs

４．普及啓発の推進

我が国全体としてサイバー攻撃のリスクが高まるとともに、サイバー空間に参加する層が広がる中で、「サイバーセキュリティ戦略」がコンセプトとして掲げている”Cybersecurity for ALL”（誰も取り残さないサイバーセキュリティ）の観点からは、事業者であれば地域や業種、事業規模を問わず、個人であれば世代を問わず、サイバーセキュリティ対策の穴を作らないことが重要である。Ⅰに述べたように、政府としては、特に事業者や地方公共団体に対して、累次にわたりサイバーセキュリティ対策の強化を求める注意喚起を行っているが、引き続き、事業者向け、個人向けそれぞれについて、ターゲットの課題と特性に合わせた普及啓発を推進することが求められる。

（１）事業者向けの普及啓発

事業者向けの普及啓発については、サイバーセキュリティに関する予算、人材、知見が不足する傾向がある「中小企業等」や、都市部と比べサイバーセキュリティに係る人材育成や情報共有の機会が少ないと考えられる「地域」を主なターゲットとして、テレワークにおけるサイバーセキュリティの確保の推進や、地域におけるセキュリティコミュニティの強化を進める必要がある。

また、サイバー攻撃被害を受けた組織における適切な情報の取扱いに資するため、サイバー攻撃被害に係る情報の共有・公表に関して、実務上の参考となるガイダンスの策定を踏まえた取組等を引き続き推進することが求められる。

ア．テレワークにおけるサイバーセキュリティの確保

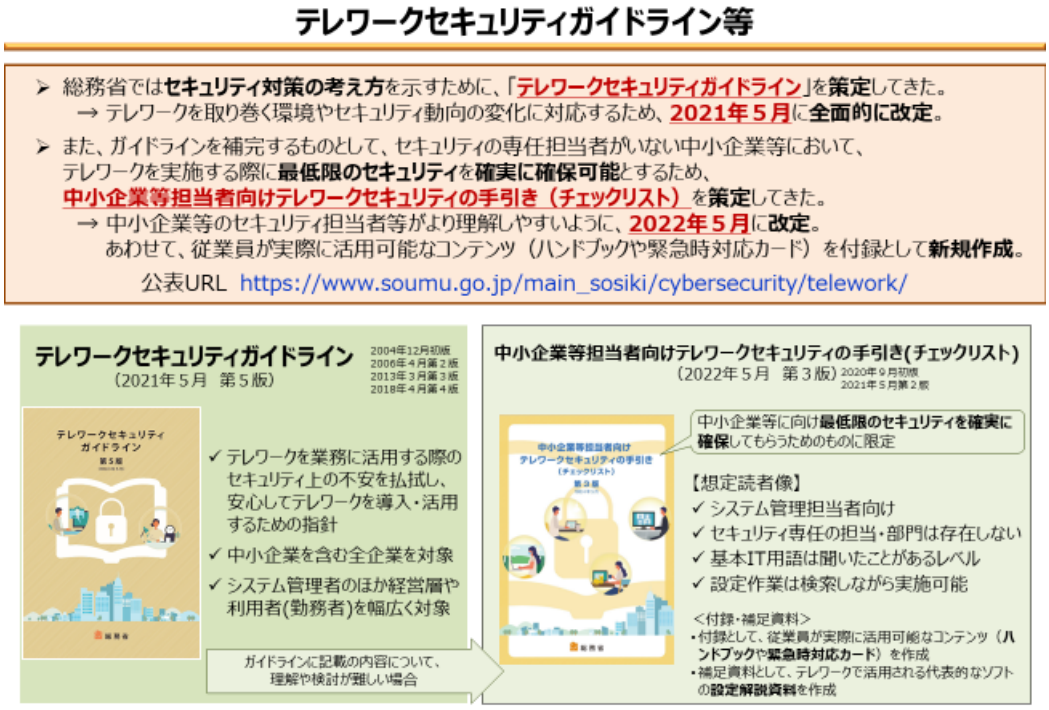
【現状】

「テレワークセキュリティガイドライン」[52]について、テレワークを取り巻く環境やセキュリティ動向の変化に対応するため、 2021 年５月に改定し第５版を策定した。また、専任のセキュリティ担当者が存在しないような中小企業等においても、最低限のセキュリティを確実に確保可能とするための「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）」[52] について、2022 年５月に改定し第３版を策定した。さらに、テレワークで利用される製品・サービスの設定にチェックリストの内容を反映させるための参考資料である「設定解説資料」について、対象製品・サービスの

[52] ガイドライン類及び実態調査の結果は、次の URL にて公表している。
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

拡充を進めている。

これらの取組に加えて、2022 年 11 月から 2023 年１月にかけて、テレワークセキュリティに関する今後の政策立案等に活用することを目的として、テレワークを導入する企業等におけるセキュリティ対策の実施状況を調査し、その結果を公表した[52]。



【今後の取組】

テレワークセキュリティガイドライン及びチェックリスト（設定解説資料を含む。）について、関係省庁や関係団体・企業等とも連携し、テレワークを実施または検討する企業に対して、一層広く周知していく必要がある。

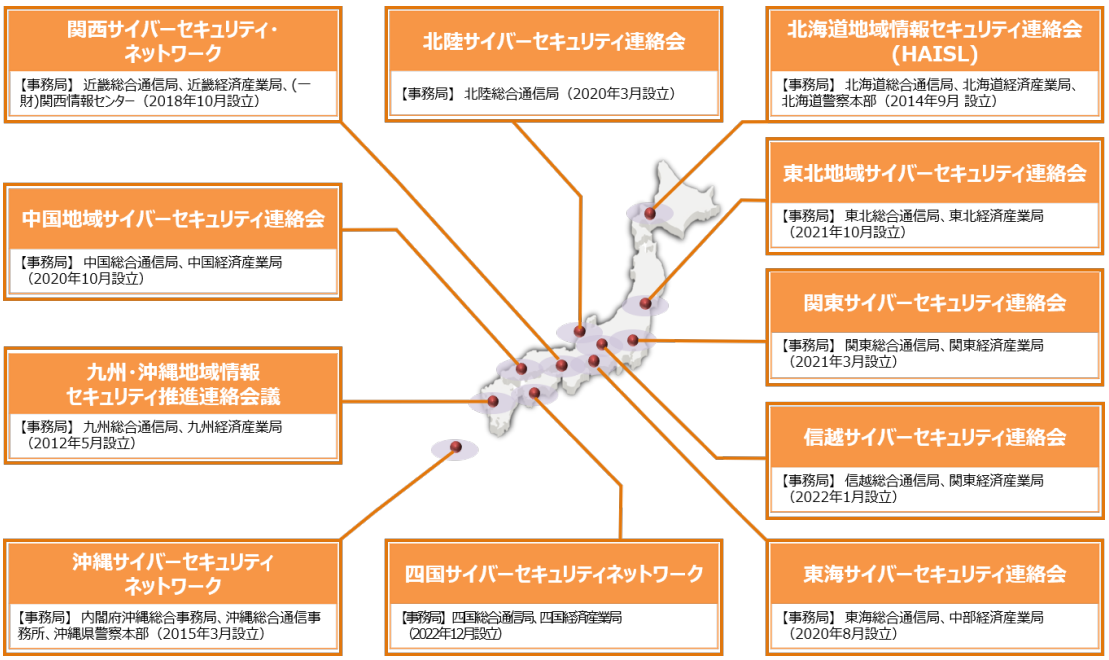
また、コロナ禍でのテレワーク導入企業等の増加に伴う影響を把握するためにも、テレワーク導入企業等におけるセキュリティ対策の実施状況の調査を継続するとともに、当該調査結果やセキュリティ動向等を踏まえ、必要に応じてテレワークセキュリティガイドライン等の改定について検討を実施することが必要である。

イ．地域セキュリティコミュニティの強化

【現状】

サイバーセキュリティのリスクが地域や企業・団体の規模を問わず高まっているが、地域においては、有効なサイバーセキュリティ対策をとるための

人材育成・普及啓発の機会や情報共有の枠組みが不足しているおそれがあり、地域レベルのコミュニティを設けることで、情報共有等を強化することが重要である。2022 年度末までに、全 11 総合通信局等の管轄地域で地域に根付いたセキュリティコミュニティ（地域 SECUNITY（セキュニティ））に当たる組織が設立され、これらのコミュニティを通じ、セキュリティ意識啓発・対応能力向上のためのセミナーやサイバーインシデント対応演習、若年層のサイバーセキュリティ人材育成に向けた CTF（Capture The Flag）などを実施することで、地域全体としてのサイバーセキュリティの向上を図っている（2022 年度は全 33 回（本省支援分）のイベントに、情報通信関連を中心とする幅広い業種の企業・団体の実務者層や戦略マネジメント層など約 1800 人が参加）。



【今後の取組】

引き続き、地域 SECUNITY の強化支援を通じてサイバーセキュリティを向上するため、関係機関と連携しつつ、各地域でのセミナーやサイバーインシデント対応演習などの開催を支援することが必要である。

また、若年層向け CTF については、地域を横断した大規模なイベントを行い、コミュニティの一層の拡大を図る。加えて、セミナーや演習には情報通信関連以外を含む幅広い業種の企業・団体からの参加を、CTF には大学、高専生などの若年層の参加を促進する。

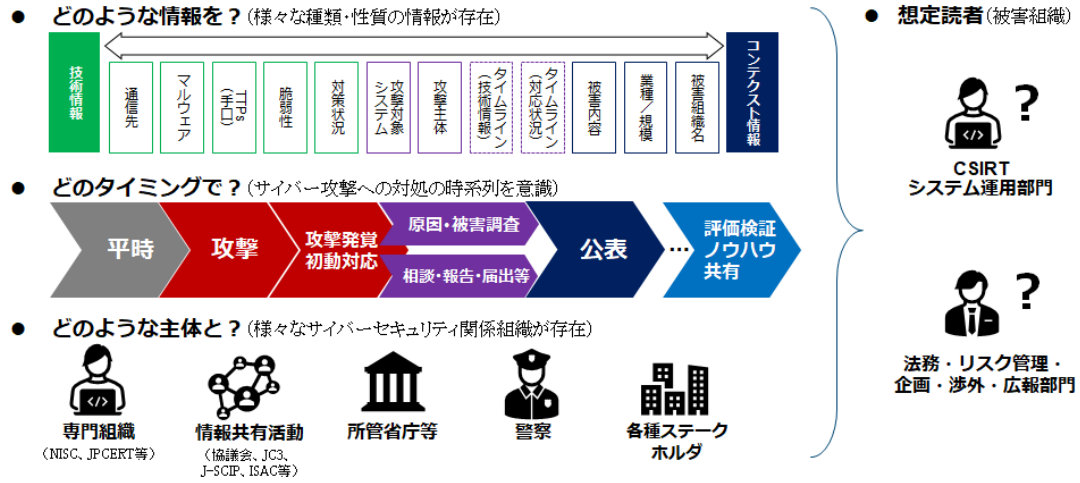
さらに、将来に向けて地域 SECUNITY のより自発的な活動を促すための方策を検討することが必要である。

ウ. サイバー攻撃被害に係る情報の共有・公表の適切な推進

【現状】

大手民間企業やそのサプライチェーンを担う中小企業等を対象としたサイバー攻撃が多発している中、攻撃被害を受けた組織が、サイバー攻撃に関する情報を外部専門機関等に共有することは、攻撃者の手口の分析等により発生したサイバー攻撃の全容を解明し、対策強化や第三者における新たな被害の発生を未然に防止することができるため、サイバー攻撃の被害に遭った組織にとっても社会的全体にとっても非常に有益である。しかし、被害を受けた組織の現場にとっては、自組織のレピュテーションに影響しかねない情報共有等には慎重であるケースも多い。現場からは、被害に係る情報のうち、どのような情報をどのタイミングで、どのような主体と共有すればよいかを検討するに当たっての実務上の参考とすべきものがないため、適切に判断することが難しいとの声も聞かれる。

こうした問題意識に基づく 2020 年度の総務省調査研究事業（JPCERT/CC 実施）の成果を踏まえ、総務省を含む関係省庁等では、2022 年４月、サイバーセキュリティ協議会運営委員会の下に、有識者からなる「サイバー攻撃被害に係る情報の共有・公表ガイダンス」検討会を設置し、６回にわたる検討会とパブリックコメントを経て、2023 年 3 月に同ガイダンスを策定した。



【今後の取組】

「サイバー攻撃被害に係る情報の共有・公表ガイダンス」について、関係省庁と連携しつつ、所管事業者等に対して、普及啓発を進めていくことが適当である。

エ. サイバーセキュリティ対策に係る情報開示の促進

【現状】

総務省では、民間企業によるサイバーセキュリティ対策の情報開示の重要性について、認識を促進するため、2019 年６月に、民間企業の実際の開示事例等を盛り込んだ「サイバーセキュリティ対策情報開示の手引き」[53]を公表した。その後、手引きを踏まえ、企業のサイバーセキュリティ対策情報の開示状況を調査・公表したほか、それを踏まえて一定の企業を表彰する取組（サイバー・インデックス・アワーズ）[54]が登場している。

【今後の取組】

引き続き、サイバーセキュリティを巡る状況変化を踏まえながら、企業のサイバーセキュリティ対策情報の開示状況の調査・公表等の取組への必要な支援を行うことなどにより、適切な情報開示を促すことが重要である。

オ. サイバーセキュリティに関する功績の表彰を通じたモチベーション向上策

【現状】

総務省では、2017 年度より、サイバーセキュリティ対応の現場において優れた功績を挙げ、今後も更なる活躍が期待される個人又は団体を自薦又は他薦により募集し、その中から実績等を踏まえ、「サイバーセキュリティに関する総務大臣奨励賞」として毎年表彰している[55]。

【今後の取組】

情報共有、事案対処、人材育成、研究、国際標準化、普及啓発、コミュニティ形成等のサイバーセキュリティに係る様々な現場で活躍する現役世代は、我が国のサイバー強靱性の基盤である。こうした個人や団体を顕彰していくことで、現場のサイバーセキュリティ人材のモチベーションの向上を更に図るべく、「サイバーセキュリティに関する総務大臣奨励賞」を引き続き実施する必要がある。

---

[53] https://www.soumu.go.jp/main_content/000630516.pdf

[54] 日本経済新聞社が主催する国際会議「サイバー・イニシアチブ東京」において、日本 IT 団体連盟の調査に基づいて、サイバーセキュリティで優れた成果を上げる企業や取り組みを表彰するもの。

[55] 2023 年の表彰者は以下のとおり報道発表を行っている（2023 年2月 28 日）。
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00158.html

（２）個人向けの普及啓発

サイバー空間と実空間との融合の進展により、あらゆる主体がサイバー空間に参画する一方、サイバー攻撃は複雑化・巧妙化しているため、デジタル化の動きと呼応し「誰一人取り残さない」サイバーセキュリティの確保に向け、こどもや高齢者を含む国民全体に向けた普及啓発を通じて、社会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、利用者が安全に情報通信サービスを利用するためには、利用者一人ひとりがサイバーセキュリティ上の脅威を認識し、それを回避するための適切な対策を把握し、実践することが重要であり、このため、利用者層に応じた普及啓発施策に取り組んでいく必要がある。

ア．無線 LAN におけるサイバーセキュリティの確保

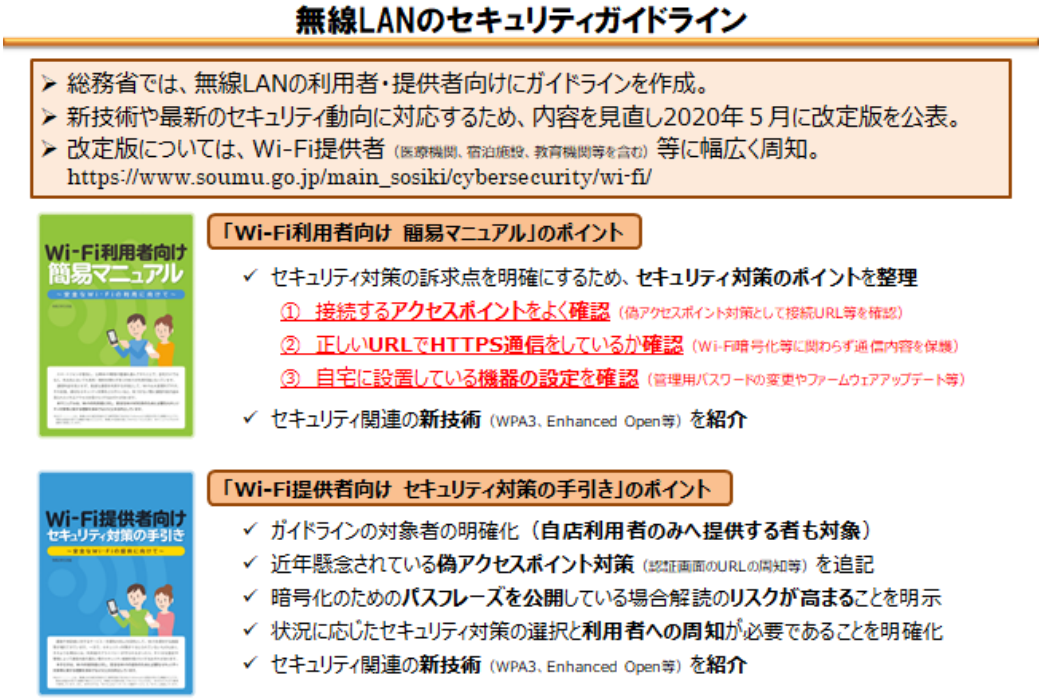
【現状】

無線 LAN の利用者・提供者向けのセキュリティ対策に関するガイドラインである 「Wi-Fi 利用者向け簡易マニュアル」[56]及び「Wi-Fi 提供者向けセキュリティ対策の手引き」[56]について、セキュリティ動向の変化等に対応するため、2020 年５月に改定した。

また、無線 LAN のセキュリティ対策に関する周知啓発の一環として、オンライン動画講座を 2023 年３月１日～26 日にかけて開講した。これは、無線 LAN を安全に利用・提供するためのセキュリティ対策を、アニメや講義形式の動画（全 12 回）により解説するもので、1,924 名が受講登録を行った。

さらに、2022 年 10 月～11 月にかけて、無線 LAN の利用者のセキュリティ意識や、無線 LAN の提供者のセキュリティ対策実施状況等を把握するための調査を実施し、その結果を公表した[56]。

[56] ガイドライン類及び実態調査の結果は、次の URL にて公表している。
https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/



【今後の取組】

総務省では、無線 LAN のセキュリティ対策に関して、利用者・提供者の各々に向けたガイドラインを策定しているところ、安全な無線 LAN 環境の実現のためには利用者・提供者双方の取組が重要であることを踏まえ、両ガイドラインの内容を、オンラインメディア等も活用して継続的に周知する必要がある。

また、無線 LAN の利用者のセキュリティ意識や、無線 LAN の提供者のセキュリティ対策実施状況等を把握するための調査を継続し、セキュリティ対策の浸透状況を確認するとともに、当該調査結果やセキュリティ動向等を踏まえ、ガイドラインの改定について検討を進める必要がある。

イ. 国民のためのサイバーセキュリティサイトを通じた普及啓発

【現状】

総務省では、サイバーセキュリティに関する知識の習得に役立ち、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するための Web サイトである「国民のためのサイバーセキュリティサイト」[57]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実施している。

[57] https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html

【今後の取組】

広く国民に対して普及啓発を実施するに当たっては、サイバーセキュリティを取り巻く状況の変化に対応し、かつ国民のニーズに沿った形でサイバーセキュリティに関する情報を発信していく必要がある。これを踏まえ、「国民のためのサイバーセキュリティサイト」について、必要に応じてWebサイトの構成を見直すとともに、セキュリティ動向等を踏まえた内容の更新を実施し、同サイトを通じてサイバーセキュリティに関する普及啓発を継続していくことが重要である。

ウ. こどもや高齢者等に向けた普及啓発

【現状】

総務省では、誰もが安心・安全にインターネットを利用して、デジタルの恩恵を享受できるように、様々な取組を実施している。

こども向けの取組としては、「e-ネットキャラバン」として、インターネットの安全な利用に係る普及啓発を目的に、児童・生徒、保護者・教職員等

に対する学校等の現場での無料の出前講座を、情報通信分野等の企業・団体と総務省・文部科学省が協力して全国で開催している（実施主体は一般財団法人マルチメディア振興センター（FMMC）。2022 年度は、2226 件の講座を実施し、約 36 万人が受講）。

また、高齢者向けの取組としては、現在、総務省で実施している「デジタル活用支援推進事業」（民間企業や地方公共団体等と連携し、デジタル活用に不安のある高齢者等向けに、スマートフォンを利用したオンライン行政手続等に対する助言・相談等を行う取組）について、総務省・内閣官房で連携し、サイバーセキュリティの普及啓発の観点から講座教材を作成し、講習会を行った。

【今後の取組】

スマートフォンの保有割合やインターネットの利用割合が全世代で上昇しており[58]、これに伴い、サイバーセキュリティ上のリスクも高まっていることから、こども、高齢者といった特に注力すべきターゲットに向けて普及啓発を強化する必要がある。

具体的には、こども向けの「e-ネットキャラバン」、高齢者向けの「デジタル活用支援推進事業」の実施において、“Cybersecurity for ALL”の観点を考慮し、2022 年 10 月にサイバーセキュリティ戦略本部において策定された「サイバーセキュリティ意識・行動強化プログラム」に基づき、「e-ネットキャラバン」については、サイバーセキュリティの普及啓発に資する取組内容の充実を検討し、「デジタル活用支援推進事業」については、サイバーセキュリティに関する講座の利活用に向けて検討することが適当である。

[58] 令和 3 年通信利用動向調査の結果(2022 年 5 月 27 日 総務省)
https://www.soumu.go.jp/menu_news/s-news/01tsushin02_02000158.html

Ⅲ　今後の進め方

「ICT サイバーセキュリティ総合対策 2023」は、サイバー攻撃の複雑化・巧妙化や脆弱性の拡大等の動向や国際情勢の変化等を踏まえて、社会全体のデジタル化や安全保障の観点からも、平時から官民挙げて我が国全体のサイバーセキュリティの強化が最重要課題であるとの認識の下で、当該課題への対処のために講じるべき施策を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」をはじめとする政府方針に基づき、関係省庁と連携しつつ、今後、「ICT サイバーセキュリティ総合対策 2023」を踏まえ、「自由、公正、かつ安全なサイバー空間」の実現を下支えする情報通信ネットワークのサイバーセキュリティの確保等を図る観点から、各施策を具体的に推進していくことが求められる。なお、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必要である。

特に、DDoS 攻撃等の情報通信ネットワークの機能に支障を及ぼし得るサイバー攻撃に対応していくため、付録４の「情報通信ネットワークにおけるサイバーセキュリティ分科会とりまとめ　－総合的な IoT ボットネット対策の実現に向けて－」を踏まえ、制度的措置を講じるとともに、関係団体、関係事業者と官民連携した取組を進めていくことが必要である。

また、「ICT サイバーセキュリティ総合対策 2023」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。こうした観点から、関係するステークホルダーとの間で、本提言及び提言の目的・狙い、ビジョンの共有を図り、取組の強化を図っていくことが望ましい。

付録１　「サイバーセキュリティタスクフォース」開催要綱

「サイバーセキュリティタスクフォース」開催要綱

１　目的

サイバー空間は、あらゆる主体が利用する公共空間として、今後の経済社会の持続的な発展の基盤であるとともに、自由主義、民主主義、文化発展を支える基盤である。これを支える情報通信ネットワークのサイバーセキュリティを確保し、国民一人ひとりが安心してサイバー空間を利用できるようにすることは、いわば不可欠の前提としてますます重要になっている。

そこで、2020年東京オリンピック・パラリンピック競技大会における成果や「サイバーセキュリティ戦略」（2021年９月28日閣議決定）を踏まえつつ、サイバー攻撃の複雑化・巧妙化や脆弱性の拡大などの動向に対応したサイバーセキュリティに係る課題を整理するとともに、情報通信分野において講ずべき対策や既存の取組の改善など幅広い観点から検討を行い、必要な方策を推進することを目的として、本タスクフォースを開催する。

２　名称

本タスクフォースは、「サイバーセキュリティタスクフォース」と称する。

３　主な検討・推進事項

（１）サイバーセキュリティに係る動向把握
（２）サイバーセキュリティを支える基盤・制度の在り方
（３）サイバーセキュリティを担う人材育成や普及啓発の在り方
（４）サイバーセキュリティ確保に向けた国際連携の在り方

４　構成及び運営

（１）本タスクフォースは、総務省サイバーセキュリティ統括官のタスクフォースとして開催する。
（２）本タスクフォースの構成員は、別添のとおりとする。
（３）本タスクフォースには、座長及び座長代理を置く。
（４）座長は、構成員による互選とし、座長代理は座長が指名する。
（５）座長は、本タスクフォースを招集し、主宰する。また、座長代理は、座長を補佐し、座長不在のときは、座長に代わって本タスクフォースを招集し、主宰する。
（６）本タスクフォースの構成員は、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）座長は、必要に応じ、臨時構成員を指名又はオブザーバを招聘することができる。
（８）座長は、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）座長は、検討を促進するため、必要に応じ、分科会を開催することができる。
（１０）分科会の主査は、座長が指名する。
（１１）その他、タスクフォースの運営に必要な事項は、座長が定める。

５　議事・資料等の扱い

（１）本タスクフォースは、原則として公開とする。ただし、座長が必要と認める場合については、非公開とする。
（２）タスクフォース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、当事者又は第三者の利益を害するおそれがある場合若しくは座長が必要と認める場合については、非公開とする。
（３）本タスクフォースの議事要旨は、原則として公開とする。ただし、座長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

本タスクフォースは、平成29年１月から開催する。

７　その他

本タスクフォースの事務局は、サイバーセキュリティ統括官室が行う。

（別添）

「サイバーセキュリティタスクフォース」構成員名簿

（敬称略、五十音順）

鵜飼（うかい） 裕司（ゆうじ）	株式会社 FFRI セキュリティ 代表取締役社長
岡村（おかむら） 久道（ひさみち）	英知法律事務所 弁護士、京都大学大学院医学研究科講師
後藤（ごとう） 厚宏（あつひろ）	情報セキュリティ大学院大学　学長
小山（こやま） 覚（さとる）	NTT コミュニケーションズ株式会社情報セキュリティ部 部長 ICT-ISAC　ステアリング・コミッティ運営委員長
篠田（しのだ） 佳奈（かな）	株式会社 BLUE　代表取締役
園田（そのだ） 道夫（みちお）	国立研究開発法人情報通信研究機構（NICT） サイバーセキュリティ研究所 ナショナルサイバートレーニングセンター センター長
辻（つじ） 伸弘（のぶひろ）	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
戸川（とがわ） 望（のぞむ）	早稲田大学理工学術院 教授
徳田（とくだ） 英幸（ひでゆき）	国立研究開発法人情報通信研究機構（NICT） 理事長、 慶應義塾大学 名誉教授

中尾（なかお）　康二（こうじ）　ICT-ISAC　顧問、

国立研究開発法人情報通信研究機構（NICT）

サイバーセキュリティ研究所　主管研究員

名和（なわ）　利男（としお）　サイバーディフェンス研究所 専務理事/上級分析官

林（はやし）　紘一郎（こういちろう）　情報セキュリティ大学院大学 元学長・名誉教授

藤本（ふじもと）　正代（まさよ）　情報セキュリティ大学院大学 教授

安田（やすだ）　元（げん）　株式会社テレビ朝日 技術局 技術業務部 設備統制担当部長

吉岡（よしおか）　克成（かつなり）　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

若江（わかえ）　雅子（まさこ）　株式会社読売新聞東京本社　編集委員

※ その他、議題に応じて、座長は臨時構成員を指名

付録２ これまでのサイバーセキュリティタスクフォースにおける検討状況

回次	議事内容
第 41 回 （2022 年 12 月 13 日）	✓ 「ICT サイバーセキュリテイ総合対策 2022」に基づく取組 ✓ 最近の無差別型サイバー攻撃の動向と対策 ✓ 国際的なサイバーセキュリティ・ボットネット対策 ✓ サイバーセキュリティタスクフォースの今後の進め方
第 42 回 （2023 年 2 月 1 日）	✓ 国際連携に関する取組状況と課題について ✓ 普及啓発・人材育成に関する取組状況と課題について
第 43 回 （2023 年 4 月 28 日）	✓ 情報通信ネットワークの安全性・信頼性の確保に関する取組状況と課題について ✓ サイバー攻撃への自律的な対処能力の向上に関する取組状況と ✓ 課題について ✓ 分科会の検討状況について ✓ 総合対策骨子（案）について
第 44 回 （2023 年 6 月 29 日）	✓ 「ICT サイバーセキュリテイ総合対策 2023」（案）について

付録３ 本文に記載した総務省作成ガイドラインの一覧

ガイドライン名	URL
5G セキュリティガイドライン第１版(2022 年４月)	https://www.soumu.go.jp/main_content/000812253.pdf
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）（2021 年９月）	https://www.soumu.go.jp/main_content/000771515.pdf
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（2022 年 10 月）	https://www.soumu.go.jp/main_content/000843318.pdf
ASP・SaaS の安全・信頼性に係る情報開示指針（ASP・SaaS 編）第３版	https://www.soumu.go.jp/main_content/000843320.pdf
スマートシティセキュリティガイドライン（第 2.0 版）（2021 年６月）	https://www.soumu.go.jp/main_content/000757799.pdf
e シールに係る指針（2021 年６月）	https://www.soumu.go.jp/main_content/000756907.pdf
IoT セキュリティガイドライン ver1.0（2016 年７月）	https://www.soumu.go.jp/main_content/000428393.pdf
テレワークセキュリティガイドライン（第５版）（2021 年５月）	https://www.soumu.go.jp/main_content/000752925.pdf
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）（第３版）(2022 年５月)	https://www.soumu.go.jp/main_content/000816096.pdf
サイバーセキュリティ対策情報開示の手引き（2019 年６月）	https://www.soumu.go.jp/main_content/000630516.pdf
Wi-Fi 利用者向け簡易マニュアル（2020 年５月版）	https://www.soumu.go.jp/main_content/000690266.pdf
Wi-Fi 提供者向けセキュリティ対策の手引き（2020 年５月版）	https://www.soumu.go.jp/main_content/000690267.pdf

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３月）	https://www.soumu.go.jp/main_content/000867112.pdf

付録４　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とりまとめ（案）

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
とりまとめ（案）

－総合的な IoT ボットネット対策の実現に向けて－

2023 年６月

総務省　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

目次

はじめに

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。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場合には、社会・経済に多大な影響を及ぼすおそれがあり、その安全性・信頼性の確保は喫緊の課題である。

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」となって利用されていることが問題となっている。

「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」は、依然として 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、2019 年から開始された脆弱性のある IoT 機器の調査及び注意喚起を行う NOTICE（National Operation Towards IoT Clean Environment）や、2022 年から開始された「電気通信事業者におけるフロー情報分析による C&C サーバ検知及び共有に関する調査」等の取組を含め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について検討を行うことを目的として、「サイバーセキュリティタスクフォース」の下に本年１月に設置されたものである。

分科会において、多くの関係団体、関係事業者や有識者から貴重な発表をいただき、活発な議論が行なわれた。本とりまとめは、この分科会における議論を踏まえたものであり、現状・成果及び課題等を踏まえ、端末（IoT 機器）側、ネットワーク側各々について今後取り組むべき対応策を「総合的な IoT ボットネット対策」として示したものである。情報通信ネットワークの安全性・信頼性を確保していくため、本とりまとめを踏まえ、総務省、関係団体、関係事業者、利用者等の関係者が適切に役割分担を図りながら、「総合的な IoT ボットネット対策」の実現に向けて取組を加速することを期待する。

１．　情報通信ネットワークにおけるサイバーセキュリティを巡る現状

（１）国民の日常生活や社会経済活動に必要不可欠な情報通信ネットワーク

社会全体のデジタル化の進展に伴い、必要不可欠な基盤としての情報通信ネットワークへの依存度は更に高まっている。2022 年７月に大手携帯キャリアにおいて通信サービス障害が発生した際には、延べ約 3,091 万人以上の利用者が影響を受け、物流や金融等の様々な分野において広範な影響を及ぼしたこと等を踏まえれば、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場合には、国民生活や社会経済活動に多大な影響が及ぶ状況となっている。

このような状況のもと、情報通信ネットワークの安全性・信頼性を確保することは一層重要となっている。

（２）情報通信ネットワークの機能に支障を及ぼし得るサイバー攻撃や IoT ボットネットの現状

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得るサイバー攻撃の発生数や規模等については、世界全体においても引き続き増大しており、2022 年第３四半期のネットワーク層で発生した DDoS 攻撃の数は、前年比 97%増[1]となっている他、攻撃対象の拡大及び攻撃継続時間の増加もみられている。また、こうしたサイバー攻撃が踏み台として利用する IoT 機器、サーバ、コンピュータ等のいわゆる「攻撃インフラ」も拡大している。

国立研究開発法人情報通信研究機構（NICT）においては、ダークネット（未使用の IP アドレス）を活用したサイバー攻撃の観測網（NICTER）を構築し、国内外で発生している無差別型サイバー攻撃の状況を観測しているが、この観測結果によれば、IoT 機器を狙った攻撃が最も大きな割合を占めている（図１）。

さらに昨年春以降、国内において Mirai 系マルウェアの活動が活発化しており、特に脆弱性のあるネットワークカメラの感染による影響が大きい（図２）。こうしたネットワークカメラは、１台当たり数十 Mbps のトラフィックを発生させることも可能であり、強力な DDoS 攻撃の踏み台となるおそれがある[2]。

こうしたネットワークカメラを含む IoT 機器については、社会全体のデジタ

---

[1] Cloudflare DDoS 脅威レポート 2022 年第 3 四半期
https://blog.cloudflare.com/ja-jp/cloudflare-ddos-threat-report-2022-q3-ja-jp/

[2] 第 41 回サイバーセキュリティタスクフォース NICT プレゼン資料
https://www.soumu.go.jp/main_content/000854031.pdf

ル化を促進する大きな役割を果たしている一方で、機器のライフサイクル（製品寿命）が長い、監視が行き届きにくい、開発者が想定していなかった接続が行われる等の特性から、サイバー攻撃の対象として狙われやすくなっている。

実際に、国内の IoT 機器を踏み台として海外に向けた大規模な DDoS 攻撃が発生し、情報通信サービスの安定的な提供に大きな支障を及ぼしかねない事案も起きており、こうした大規模サイバー攻撃が国内に向けられた場合のリスクも想定した対策を実施する必要がある。また、大規模サイバー攻撃に至らないものの、政府機関や重要インフラ事業者等のウェブサイトを狙った DDoS 攻撃により、閲覧が困難になる等の事象が断続的に発生している他、家庭用ルーターがサイバー攻撃に悪用されていることが判明し、本年春に警察庁等から注意喚起が発出[3]されている。

さらに最近では、ID・パスワードの脆弱性を狙ったログインによる侵入だけではなく、リモートコード実行やコマンドインジェクション等、ファームウェア[4]をはじめとする様々なソフトウェアの脆弱性を狙ったマルウェアが増えており、こうした脆弱性に対する攻撃コードがプラットフォーム上で公開されると、それを悪用したサイバー攻撃のリスクが急増する傾向にある[5]。

この他、少数のサーバから直接サイバー攻撃を行うケースも発生しているが、こうした攻撃は感染機器を観測しているダークネットやハニーポットといった従来の手法では観測できない可能性がある他、機器の再起動といった簡易な手法では駆除できないマルウェアも新たに観測される等、サイバー攻撃の手法も多様化している[6]。

---

[3] https://www.npa.go.jp/bureau/cyber/pdf/20230328_press.pdf

[4] 機器の内部に組み込まれた、機器を制御するためのソフトウェア

[5] 第1回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 吉岡構成員プレゼン資料
https://www.soumu.go.jp/main_content/000856810.pdf

[6] 脚注5参照。

図１　増加・多様化する無差別型サイバー攻撃～NICTER による観測～

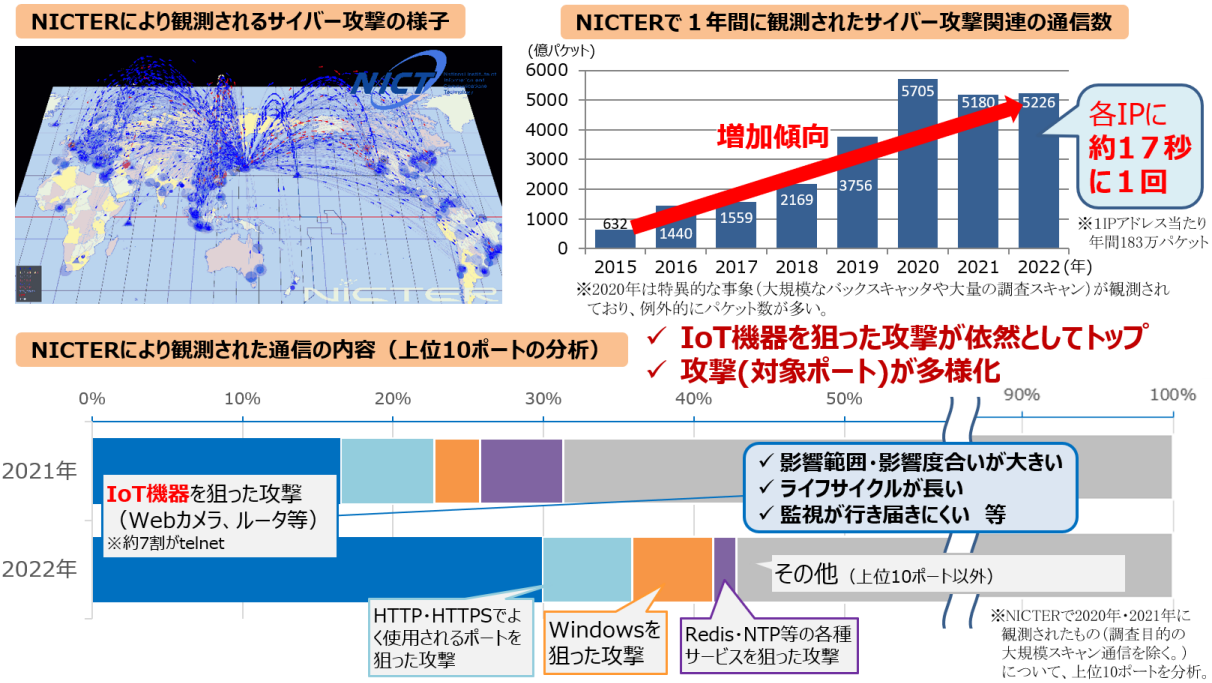
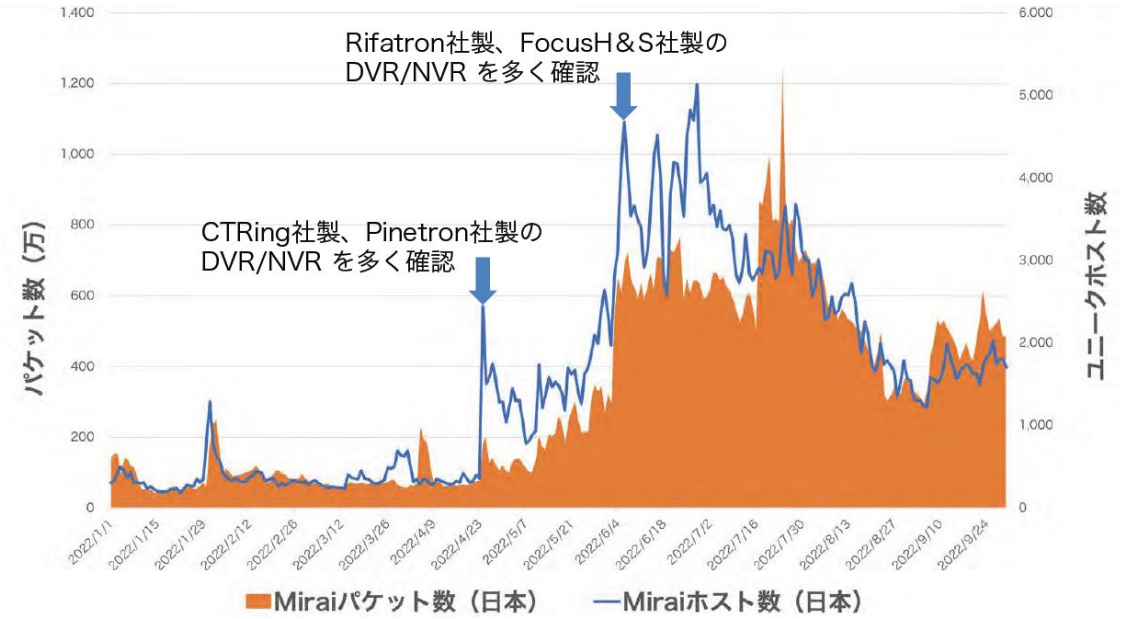


図２　日本を送信元とする Mirai の特長を持つパケット数とユニークホスト数（日毎）



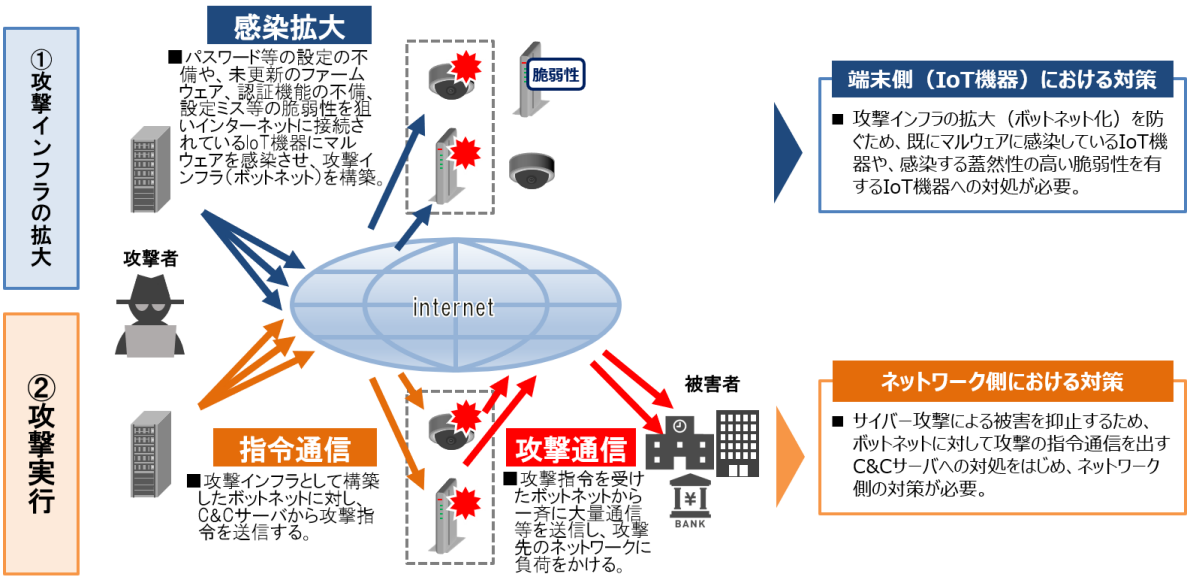
（３）情報通信ネットワークにおけるサイバーセキュリティ対策の強化に向けて

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[7]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３）。

このような大規模サイバー攻撃への対策として、攻撃インフラの拡大を防ぐための端末（IoT 機器）側の対策、IoT ボットネットに対して指令を出す C&C サーバへの対処のための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ていくことが必要[8]である。

その際、端末（IoT 機器）側の対策については、開発・製造といった段階でも適切なセキュリティ対策が講じられることが望ましいものの、IoT 機器は裾野が非常に広く様々な種類があり、メーカーも多数存在していることや、ライフサイクルが長い等の IoT 機器の特性も十分踏まえ、PC やスマートフォンにおける OS のアップデート等や、クラウドサービス（SaaS）等の事例を参考にしつつ、ISP、メーカー、SIer[9]、流通業者、利用者等のステークホルダー各々が適切に役割分担をしながら、必要な対策を講じていくことが求められる。

図３　DDoS 攻撃の段階と対応策



[7] Command and Control サーバの略であり、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に対して攻撃者から指令を送り、制御を行うサーバコンピュータのこと。

[8] 総合的な IoT ボットネット対策には、IoT 機器がマルウェアに感染し IoT ボットネットになることを未然に防ぐための IoT セキュリティ対策も含まれる。

[9] IoT 機器等の設置からそれに関わるシステムの開発・保守・運用までを請け負う事業者のこと。

２．端末側における対策（NOTICE）

（１）これまでの取組

2015 年～2016 年頃、「Mirai」と呼ばれるマルウェアの感染が急速に拡大し、多数の IoT 機器を踏み台とした大規模な DDoS 攻撃が国内外において発生した。

こうした多数の IoT 機器が DDoS 攻撃の踏み台となる事態を未然に防止するため、当時主流であった ID・パスワードの脆弱性を狙った感染手法に着目し、2018 年 11 月に国立研究開発法人情報通信研究機構法（平成 11 年法律第 162 号）を改正し、2024 年３月末までの５年間の時限措置（不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）の例外）として、NICT が、同様の手法（特定アクセス行為[10]）により、ID・パスワードに脆弱性のある IoT 機器を調査して電気通信事業者（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を 2019 年２月に開始した。

なお、NICT から ISP への通知については、認定送信型対電気通信設備サイバー攻撃対処協会（認定協会）である（一社）ICT-ISAC を通じて実施している。

調査を開始した当初は、ID・パスワードは 100 通り、通信プロトコルは telnet／ssh のみ、ポートも１つのみが調査対象であったが、サイバー攻撃の手法の変化等も踏まえ、ID・パスワードについては 2020 年 10 月に 600 通りに拡大した他、通信プロトコルについては 2022 年６月に http／https を追加するとともに、ポートも順次追加し、現在は 39 のポートを対象に調査を実施している。

また、上記の取組に加えて、NICT が、NICTER によりマルウェアの感染通信を出している IoT 機器を調査し、NOTICE の枠組みを活用して個別の利用者への注意喚起を行う取組を 2019 年６月から開始している。

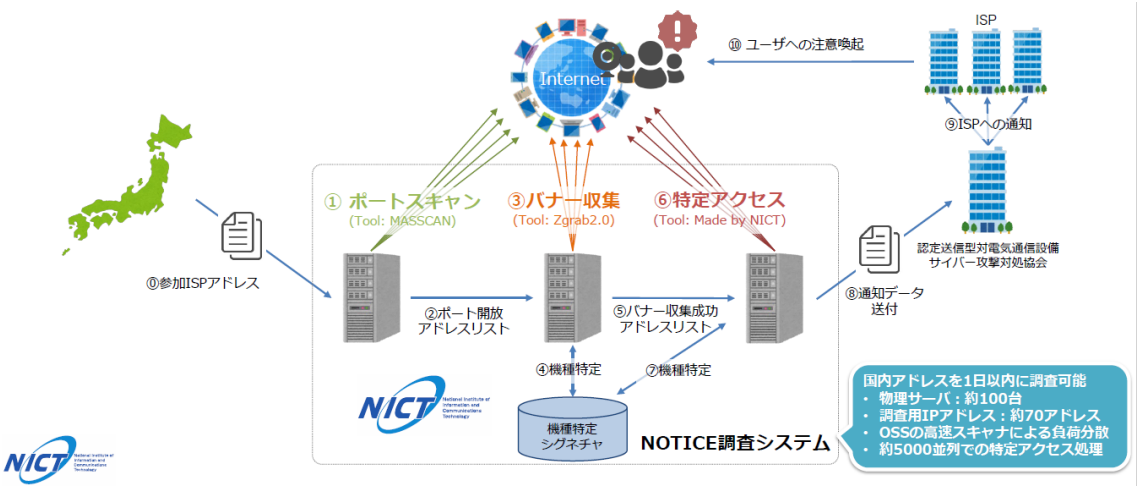
こうした NOTICE の取組は、ISP の自主的な協力を基本としており、2019 年の開始当初の参加 ISP は 24 社であったが、その後参加数は徐々に拡大し、2023 年６月時点で 78 社の ISP が NOTICE に参加しており、NOTICE の調査対象となる IP アドレスの総数も 1.12 億アドレス[11]となっている。

---

[10] 国立研究開発法人情報通信研究機構法附則第8条第4項第1号。

[11] JPNIC が管理する日本国内の IP アドレスは約 1.9 億あるが、このうち NOTICE に参加している ISP が管理している IP アドレスを調査対象としている。

図４　ID・パスワードに脆弱性がある IoT 機器の調査の概要



（２）現状・成果と課題

①脆弱性等がある IoT 機器の調査

【現状・成果】

NOTICE の取組により、ID・パスワードに脆弱性がある IoT 機器については、国内の 1.12 億 IP アドレスを対象に、NICT が法律に基づいて調査を実施し、全体的な動向を把握できるようになった。その結果、ID・パスワードに脆弱性があるとして ISP に通知した IoT 機器の数は、直近では月平均 4,000 件程度で推移しており、現在までの累計で８万件以上の通知を実施している（図５）。

また、NICTER により検知され、注意喚起対象として ISP に通知した感染通信を出している IoT 機器の数は、直近では 1 日平均 400～700 件程度で推移しており、現在までの累計で 62 万件以上の通知を実施している（図６）。

注意喚起対象となった機種については、ID・パスワードに脆弱性がある IoT 機器及び感染通信を出している IoT 機器双方ともルーターが最も多くを占めており、次いでネットワークカメラとなっている（図１及び図７）。

図５　パスワード設定等に不備がある IoT 機器に対する注意喚起対象件数の推移（2023 年４月）

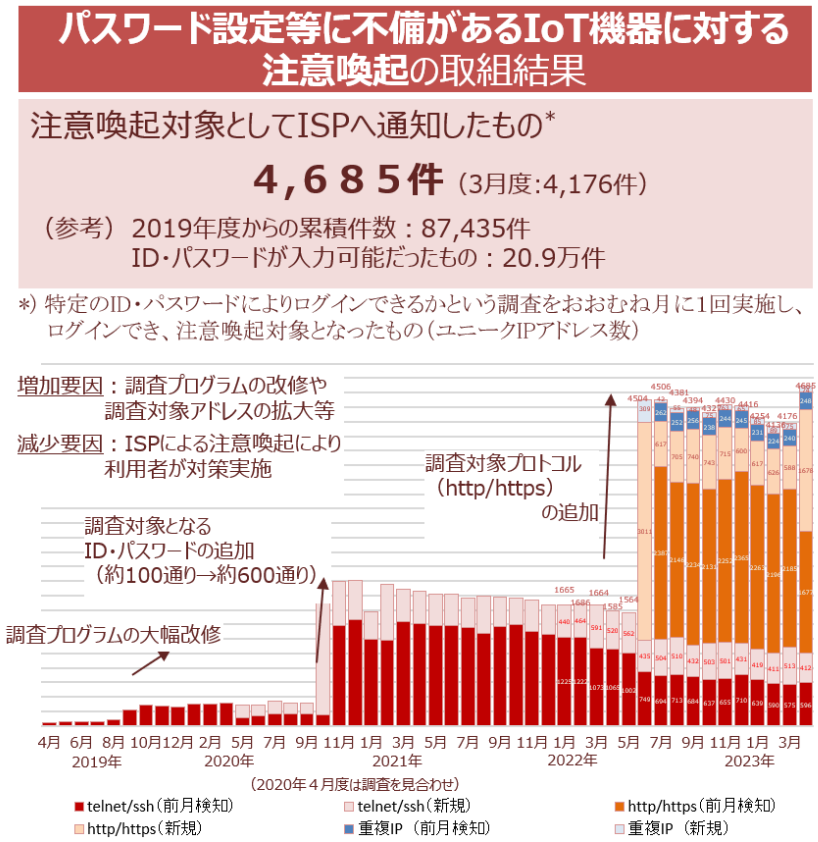


図６　感染通信を出しているIoT機器に対する注意喚起対象件数の推移（2023年４月）

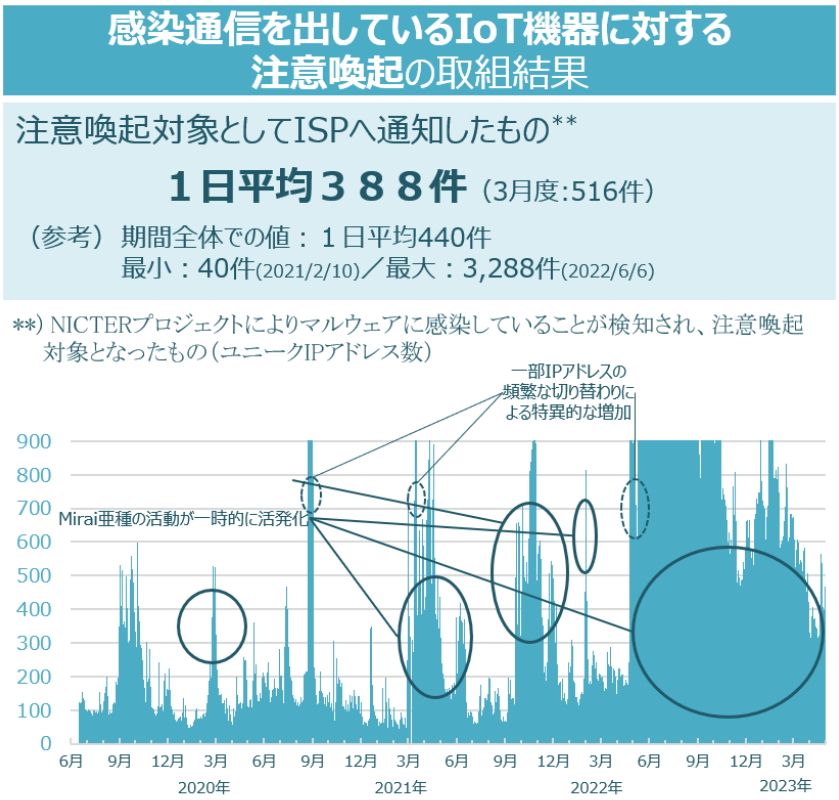
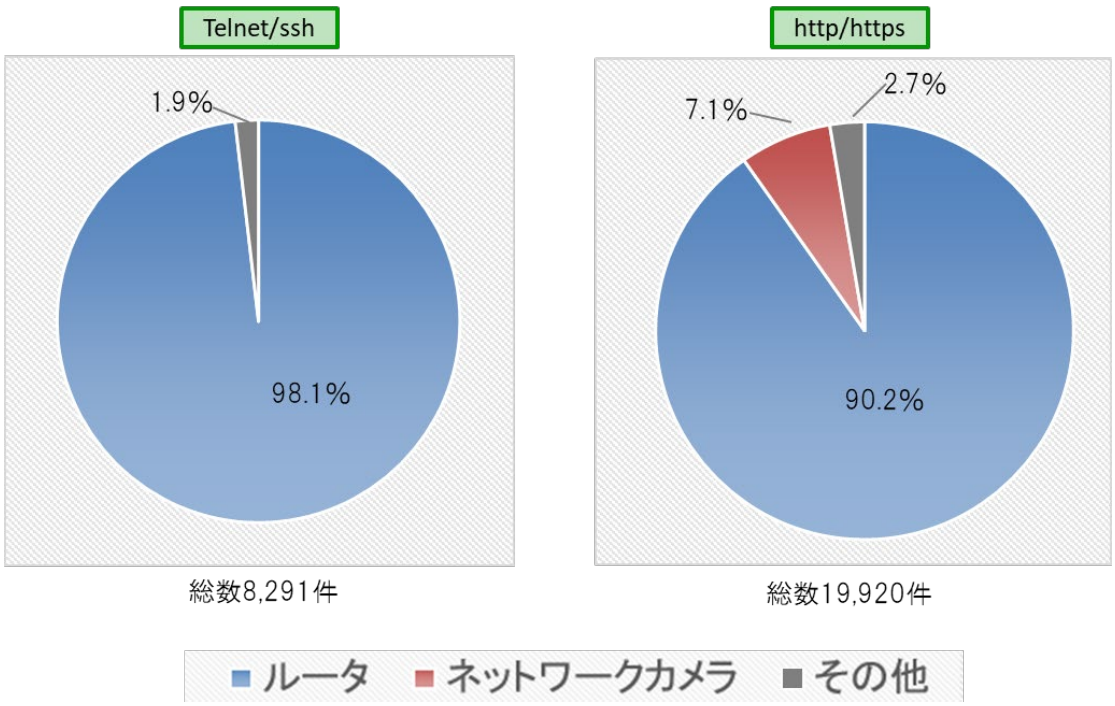


図７　注意喚起対象となったIoT機器の機種の内訳（2022年11月～2023年４月）



【課題】

１（２）で述べたように、情報通信ネットワークの機能に支障を及ぼし得るサイバー攻撃の発生数や規模等は増大しており、こうした攻撃の踏み台となる可能性のある IoT 機器の数も、デジタル化を背景に引き続き増加していくことが見込まれる。

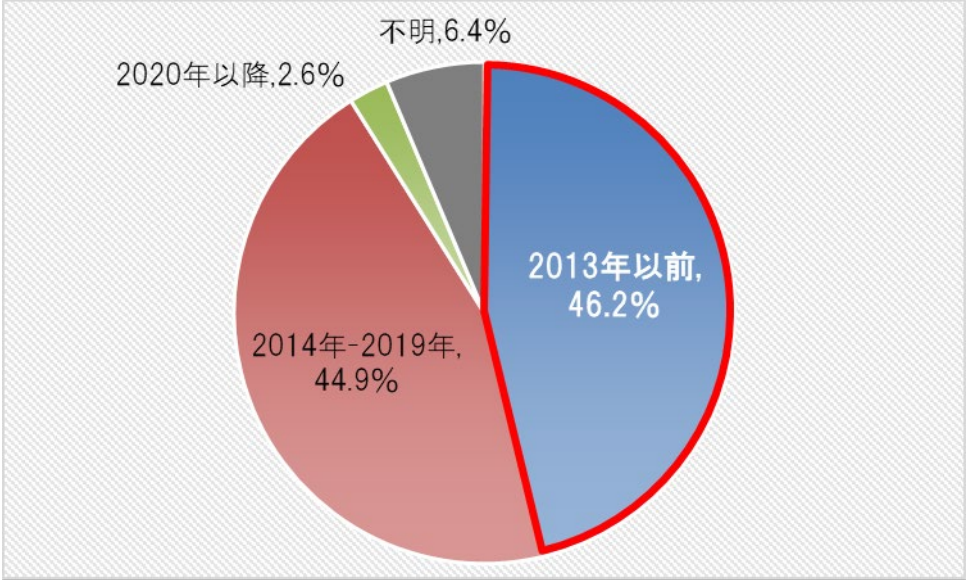
また、ISP にとっては、外から自網へ向けて送信される攻撃通信よりも、自網内の IoT ボットネットから外へ送信される攻撃通信の方が、正常な通信も遮断するおそれがある等の理由により、一般的に対策が困難とされている。そのため、こうした IoT 機器を踏み台としたサイバー攻撃を未然に防ぐためには、IoT ボットネットと、ボットネット化する可能性がある IoT 機器を可能な限り減らしていく取組が必要である。

この点、NOTICE の取組によって、IoT ボットネット対策は一定の成果を上げているものの、ID・パスワードに脆弱性がある IoT 機器は現在でも一定数残存している。特に、注意喚起対象となった機器のうち、10 年以上前に発売された古い機器が４割以上を占めており、IoT 機器のライフサイクルの長さが明らかとなっている（図８）[12]。また、１（２）で述べたように、NICTER により検知され、注意喚起対象となった感染通信を出している IoT 機器の数は、昨年春以降、マルウェア活動の活発化等を背景に高止まっている。

この他、同じく１（２）で述べたように、ファームウェア等の ID・パスワード以外の脆弱性がある IoT 機器を狙ったサイバー攻撃が増えている。こうした機器については、NOTICE 調査の過程で検知できる場合があり、メーカー等に情報提供した事例はあるものの、アドホック的な対応にとどまっており、現行の NOTICE の枠組みにおいては十分対処ができていない状況にある。

[12] 脚注 15 参照。2020 年4月の IoT セキュリティ基準施行後の新しい機器については、ID・パスワードの脆弱性等、一定の対策が進んでいる。

図８　注意喚起対象となったIoT機器の発売年の割合（2022年11月～2023年４月）



②利用者への注意喚起

【現状・成果】

NOTICE の枠組みを通じて個別の利用者への注意喚起を実施するとともに、「NOTICE サポートセンター」を設置し、問合せ対応や機器別の脆弱性解消マニュアルの作成等、注意喚起を受けた利用者のサポートを行う等の取組により、ID・パスワードに脆弱性のあるIoT機器は一定数減少している他、あるISPにおいては、注意喚起の進捗状況を適切に管理することで、注意喚起対象件数がゼロになった事例もある[13]。

また、一部のISPにおいては、一般家庭向けにルーター等のIoT機器のレンタルサービスを提供しており、最新のファームウェアの提供や機器の監視といったセキュリティ対策をISP側で一括して行っている事例がある。

さらに2020年４月に、インターネット等に接続される端末について、初期設定のパスワードの変更を促す等の機能やソフトウェア更新機能等の要件を定め

[13] 検知されたIoT機器の利用者が全て法人利用者であり、ISPによる通知データを顧客単位で紐付け、歴月管理を行い対処状況を把握しながら、メールでの注意喚起を実施したもの。

た IoT セキュリティ基準を端末等設備規則において新たに定める[14]とともに、当該要件を満たさない場合等において、ISP が端末の接続を拒否できる制度を措置している。

【課題】

IoT 機器の適切なセキュリティ対策に対する利用者の意識が十分でないことに加え、ルーターのパスワード変更等といった対策方法も一般の利用者にとって難しいものとなっている[15]。

特に法人利用者については、所有者・設置者・利用者各々が異なり、管理責任の所在が曖昧である等適切な IoT 機器の管理体制がないため、適切に注意喚起が届かないケースや、コストがかかるため、実害がない限りはファームウェアの更新や設定変更等の対処が行われないケースもある。

また、こうした利用者側の課題に加え、注意喚起を受けた利用者について、実際に対処を完了したかどうか確認が出来ていない等、注意喚起による効果測定が十分に行われていないことが課題となっている。

一方、IoT セキュリティ基準を満たさない端末やマルウェアに感染している端末等、サイバー攻撃に悪用されるおそれのある端末を接続拒否する約款については、利用者の理解が得られにくいことも課題となっている。

③メーカーの対応

【現状・成果】

メーカーにおいては、IoT 機器の適切な管理に関する利用者への周知啓発、機

---

[14] 電気通信事業法（昭和 59 年法律第 86 号）において、電気通信事業者が、技術基準を満たさない端末設備からの自社の電気通信回線設備への接続の請求を拒否することができることとされており、当該技術基準を具体的に定めた端末設備等規則（昭和 60 年郵政省令第 31 号）において、ネットワークに係る攻撃は電気通信回線設備の機能に障害を与え又は他の利用者に迷惑を及ぼしうるものであることを踏まえ、電気通信回線設備に直接接続される端末機器を対象に、IoT 機器の特性を踏まえた最低限の技術基準として、①アクセス制御機能、②アクセス制御の際に使用する ID／パスワードの初期設定の変更を促す等の機能、③ファームウェアの更新機能、④変更した ID／パスワードを維持する機能を具備することを追加で定めている。

[15] （一社）デジタルライフ推進協会（DLPA）が 2023 年3月に実施した Wi-Fi ルーター利用者向けアンケートの結果は以下のとおり。

- 57.8%の利用者が Wi-Fi ルーターのセキュリティを意識したことがない
- 81.7%の利用者が自宅の Wi-Fi ルーターがサイバー攻撃されると考えたことがない
- 購入時のパスワードをそのまま利用している利用者が 42.7%

器のサポート期間終了やファームウェアの更新等に関する情報提供に取り組んでいる。

特に、（一社）デジタルライフ推進協会（DLPA）に加盟しているメーカーにおいては、個体毎に異なる ID・パスワードが設定されており、ファームウェアの自動更新機能を有しているルーターを「DLPA 推奨 Wi-Fi ルーター」として販売しており、当該ルーターについては NOTICE の調査においてこれまで 1 台も検知されていない。

さらに、NOTICE の調査で検知した機器について、メーカーとの連携により、脆弱性のあるファームウェアの改修や新製品のセキュリティ機能の改善につながった事例もある。

【課題】

国内のインターネットに接続されている IoT 機器のうち、メーカーのサポート期間が終了している EOL（End Of Life の略）を迎えた古い機器や、ファームウェアが更新されずに古いままになっている機器が一定数残存している[16]。

IoT 機器はライフサイクルが一般的に長く、特に中小企業の場合、定期的に設備更改が行われる大企業と比較すると、コストを抑えるため、壊れるまで機器を利用する傾向が強く、10～15 年利用される事例もある。

また、前述のとおり、現行の NOTICE においては事案に応じて個別にメーカーとコミュニケーションを取っているが、アドホック的な対応にとどまっているため、今後恒常的に連携を図っていくような取組も必要となっている。

④NOTICE の運営

【現状・成果】

NOTICE の取組により、利用者からサイバー攻撃の被害の申告を受けて対処するのではなく、あらかじめ脆弱性等の問題のある IoT 機器を特定して利用者へ注意喚起を実施することにより、未然に「プッシュ型」で対処につなげる枠組みができたことは成果の１つと言える。

---

[16] 第3回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 (株)ゼロゼロワンプレゼン資料
https://www.soumu.go.jp/main_content/000868984.pdf

また、NOTICE 調査の過程で ISP が管理している IoT 機器に脆弱性があることが判明し、ISP と連携してパスワードを変更したケースや、ISP やメーカーと連携してファームウェアの更新・適用を行ったケース等、利用者への注意喚起を実施せずに対処に成功した事例もある。

さらに、海外の捜査当局から警察庁に国内の「Emotet」[17]感染端末の情報提供があり、警察庁と連携して利用者への注意喚起を実施した事案や、IoT 機器の検知数の急変により不正アクセスを検知した事案等、NOTICE の枠組みを活用して当初想定していなかったサイバー攻撃のリスクに対処した事例もある。

【課題】

NOTICE に参加している ISP にとっては、NICT から注意喚起対象となる IoT 機器の通知を受けた後、利用者の特定から注意喚起、問合せ対応までの一連の業務に係る負担が大きく、効率性も踏まえて取り組むことが必要となっている。

脆弱性等のある IoT 機器の調査を担う NICT においても、サイバー攻撃の手法の変化等に対応した十分な調査を実施していくため、関係団体や関係事業者とも連携して体制や人員を充実することが課題となっている。

また、NOTICE の調査対象として未参加の ISP が管理する IP アドレスは対象外となっているとともに、参加 ISP の卸先 ISP が NOTICE に参加していない場合、脆弱性等のある IoT 機器が検知されたとしても個別の利用者への注意喚起を行うことができない等の課題がある。

更に、NICT においては、2019 年以降の NOTICE の調査を通じて国内の IoT 機器の脆弱性等に関する様々なデータが蓄積されてきていることから、国内のネットワークの状況の可視化や関係団体との協調等に取り組むとともに、研究・レポートの公表等を通じて積極的に情報公開を図ることにより、更なるサイバー攻撃への対策に向けて、これを有効活用していくことが必要である。

[17] 情報の窃取や他のマルウェアへの感染のために悪用されるマルウェアであり、現在においても攻撃活動が断続的に発生している。

（３）今後の対応に向けた基本的な考え方

これまでの現状・成果及び課題を踏まえ、今後の NOTICE をはじめとする端末側における対策については、国民の日常生活・社会経済活動に必要不可欠な情報通信サービスの安定的な提供を確保するため、IoT 機器を踏み台としたサイバー攻撃の脅威に対する観測能力を強化し、攻撃の脅威に応じた効果的な対処の促進に向けて、以下のような方向性で取り組むべきである。

サイバー攻撃の踏み台となり得る IoT 機器に対する観測能力の維持・強化

情報通信ネットワークの機能に支障を及ぼし得るサイバー攻撃については、発生数・規模ともに増大しており、攻撃の踏み台となる可能性のある IoT 機器の数も、デジタル化を背景に引き続き増加することが見込まれる中、こうした攻撃に効果的に対応していくためには、脅威を観測した上でリスク評価を行っていくことが必要不可欠であることから、これを NOTICE の役割として明確に位置づけ、脆弱性等のある IoT 機器に対する観測能力の維持・強化を図る。

幅広い関係者との連携や対処手段の多様化等による「プッシュ型支援」の強化

脆弱性等のある IoT 機器への対処をより効果的に促していくため、利用者への注意喚起の実効性向上を図るとともに、注意喚起のみに依存するのではなく、幅広い関係者との連携により状況に応じた多様な手段を講じる。

（４）今後の対応策

①脆弱性等のあるIoT機器の調査の延長・拡充

サイバー攻撃の踏み台となり得る脆弱性のあるIoT機器に対する観測能力を維持・強化する観点から、今年度末までの時限措置となっている特定アクセス行為によるID・パスワードに脆弱性があるIoT機器の調査について、NICTERによる感染通信を出しているIoT機器の調査も含め、NICTが来年度以降も継続して取り組む必要がある。

また、サイバー攻撃手法の多様化に対応するため、ファームウェア等のID・パスワード以外の脆弱性のあるIoT機器についても、機器の脆弱性、攻撃コードの公開状況及び国内における普及状況等、脅威度に応じて個別に判断しつつ、NOTICEの枠組みを活用して必要な調査及び対処を実施することが求められる。

これらの取組を継続的に実施することを可能とするため、早急に制度的措置を講じることが必要である。

②利用者への注意喚起等の実効性向上

利用者への注意喚起等の実効性を向上させるため、ホームページの充実等を含めNOTICEの情報発信を強化するとともに、メーカーやSIer等の関係者との連携により、一般利用者・法人利用者それぞれに向けて、ID・パスワードの変更、ファームウェアの更新、新しい機器への買い替え等を含めて利用者によるIoT機器の適切な管理を推進するための周知啓発を更に強化する。その際、脆弱性等のあるIoT機器が、利用者本人やネットワーク全体に対して、どのような不利益・リスクを生じさせるのか、また、その対応策について分かりやすく伝わるよう工夫する。

また、IoT機器の管理状況等に関する利用者への実態調査や「am I infected?」[18]との連携等を進めることにより、注意喚起による効果のより詳細な把握に取り組む。

更に、感染通信を出している端末やサイバー攻撃の踏み台となり得る脆弱性のある端末について、累次にわたって注意喚起に利用者が応じない場合等について、ISPが接続拒否できる具体的な要件や手続等の妥当性についてあらかじめ

[18] 横浜国立大学が実施している、利用者の申請に基づいてIoT機器のマルウェア感染と脆弱性を確かめる検査サービス。https://amii.ynu.codes/

示すため、「端末設備の接続に関するガイドライン（仮称）」を策定する。

③メーカーや SIer 等の幅広い関係者との連携による総合的な対処

脆弱性等のある IoT 機器への対応を進める際に ISP やメーカーとの連携により効果的に成果を上げている事例があることを踏まえ、②の利用者への注意喚起のみに依存するのではなく、ケースバイケースで様々な手段を活用しつつ総合的に対処（※）を行うことができるように、関係団体、ISP、メーカー、SIer 等の関係事業者等と連携を進めることが必要である。

（※）脆弱性等のある IoT 機器に対する利用者への注意喚起以外の対処例

連携例	対処例
ISP との連携	レンタルサービス等を通じて機器が ISP によって管理されている場合、利用者に直接対処を求めることなく ISP 側で一括して対処する。
メーカーとの連携	注意喚起対象となった製品について、利用者への情報提供、ファームウェアの改修・更新や新製品の機能改善等必要な対処を促す。
SIer との連携	法人利用者等、機器の設置・管理に SIer が関与している場合、SIer を通じて機器の ID・パスワードの設定等やファームウェアの更新等必要な対処を促す。

さらに、ISP 及びメーカー等の関係者が連携し、ファームウェアの自動更新等、利用者が意識せずに IoT 機器を適切に管理可能な製品・サービスの普及に取り組む。

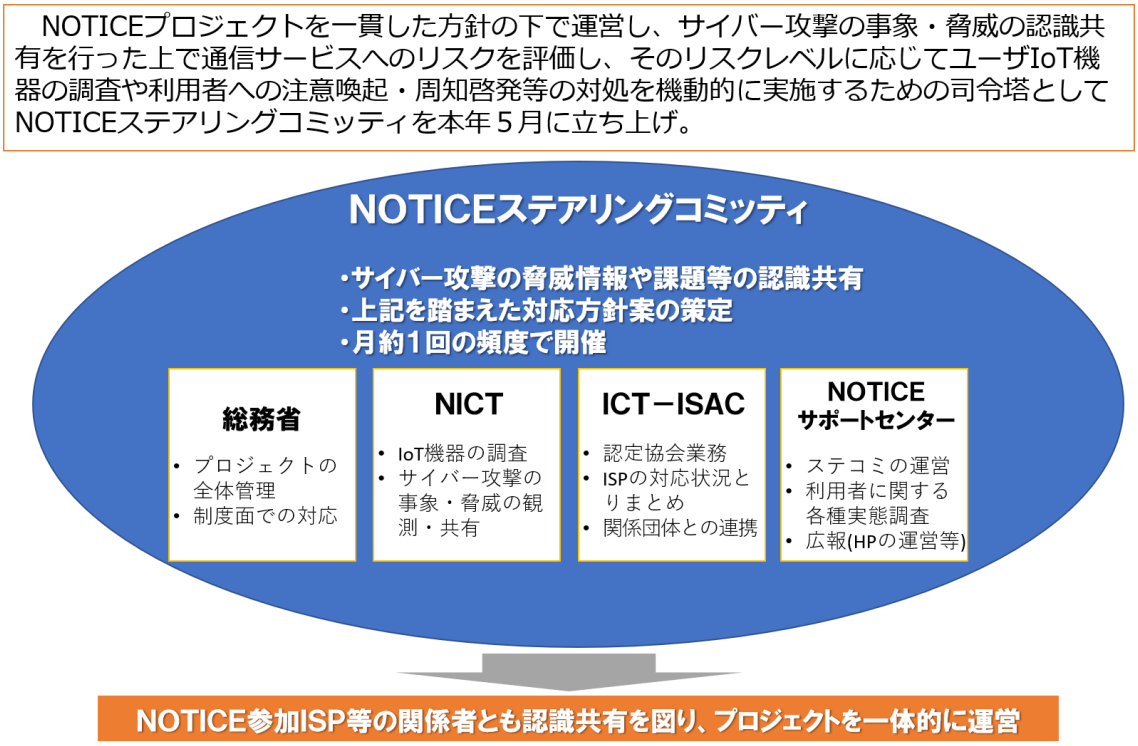
また、メーカーや流通業者と連携し、IoT 機器のサポート期間終了やファームウェアの更新等、利用者が安全な製品・サービスを選択する際に必要な情報の確実な提供、利用者にとって分かりやすい設定・操作が可能な機器やマニュアルの提供を進める。

④①～③を効果的に実施するための NOTICE の運営体制の強化

関係者間でサイバー攻撃の脅威を評価し、目指すべきゴールや必要な対策に

ついて認識の共有を図りつつ、PDCA サイクルを回しながら、NOTICE の柔軟かつ効率的な運営に取り組むため、司令塔としての役割を担う体制（NOTICE ステアリングコミッティ）を整備・確立する（図９）。

図９　NOTICE ステアリングコミッティの概要



その際、③にあるように総合的な対処を進める観点から、NOTICE の取組にメーカーや SIer 等も参画し、ファームウェアの更新や新製品への対応も含め脆弱性等のある IoT 機器への総合的・効果的な対処の推進に向けて、幅広い関係者が恒常的に情報共有・連携を図るような枠組み（図 10）をつくる。

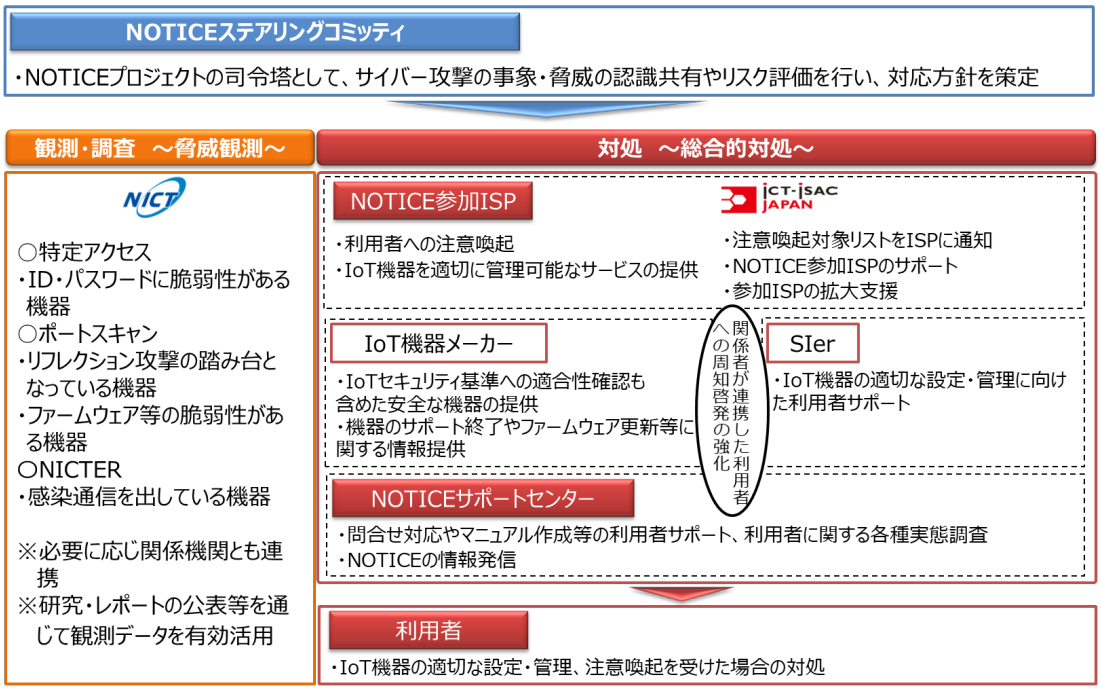
また、②にあるように NOTICE の情報発信を更に強化することにより、一般利用者の理解を得るとともに、参加 ISP の拡大を図る。

こうした取組の前提となる脆弱性等のある IoT 機器の調査について、①にもあるようにサイバー攻撃の変化に応じて十分に実施するため、主にこれを担う NICT の体制・人員の柔軟な確保が可能となるように必要な措置に取り組むとともに、必要に応じて IoT ボットネットの調査に係る関係者との連携を一層推進[19]する。

[19] IoT ボットネットの観測･調査等に関係する国内の主な観測･調査システムは参考 93 ページを参照。

さらに、このように調査体制や連携を強化することにより、例えば、外部から認証なしに管理画面にアクセスできる機器、脆弱性のある古いファームウェアのままの機器、外部に公開すべきではないポートの空き状況等、NOTICE の調査で得られた様々なデータについて、研究・レポートの発表等を通じた情報公開や、関係機関との共有を適切に進めることで、国内のインターネットに接続されている機器の脆弱性等に関する状況の可視化等を図り、サイバー攻撃の脅威に関する認識共有や対策の強化に資するよう更なる有効活用を進める。

図 10　今後の NOTICE の全体像



３．ネットワーク側その他における対策

（１）これまでの取組

大規模化・複雑化・巧妙化するサイバー攻撃に対して、あらかじめ電気通信事業者が積極的に対処できるようにする観点から、平時から電気通信事業者が自網内の通信トラフィックに係るデータを収集・蓄積・分析し、サイバー攻撃の指令元となっている C&C サーバである可能性の高い機器の検知等を行うことできるようにすることが重要である。

これを踏まえ、まず、2021 年 11 月に「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会　第四次とりまとめ」において、電気通信事業者におけるインターネット利用者のトラフィックのうち、必要最小限の範囲で収集するフローー情報 [20]の統計的・相関的な分析による 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（通信の秘密の侵害に該当しない）として法的整理を実施した。

この整理に基づき、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ー情報の分析による C&C サーバ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運用面の課題整理のための実証事業を実施している。

本実証事業については、電気通信事業者 3 社がグラフマイニングと機械学習の２つの手法によりフローー情報を分析して被疑 C&C サーバを検知し、(一社)ICT-ISAC において検知された被疑 C&C サーバの多面的な分析・評価を実施するとともに、事業者間の情報共有等に関する検討を行っている。

[20] 通信トラフィ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（通信の内容は含まない）

（２）現状・成果と課題

①C&C サーバの検知・検知情報の共有・利活用

【現状・成果】

本実証事業に参加した電気通信事業者３社それぞれにおいて、フロー情報の分析により多くの被疑 C&C サーバが検知され、当該手法の有効性が確認されるとともに、検知された C&C サーバの一部については既存の手法よりも早期に検知されたことから（図 11）、より迅速な対応につなげられる可能性も期待される。

また、特定の電気通信事業者のみが検知した被疑 C&C サーバが多く確認されたことから（図 12）、事業者間連携を更に進めることによって、より多くの C&C サーバを検知できる可能性や、より影響度の高い C&C サーバを特定できる可能性も期待される。

（一社）ICT-ISAC においては、新たに WG を立ち上げ、会員社のうち 15 社が WG に参画し、C&C サーバリストの情報共有・利活用の在り方や、C&C サーバの検知手法の共有について検討し、課題の整理を行っている。

図 11　C&C サーバの先行検知

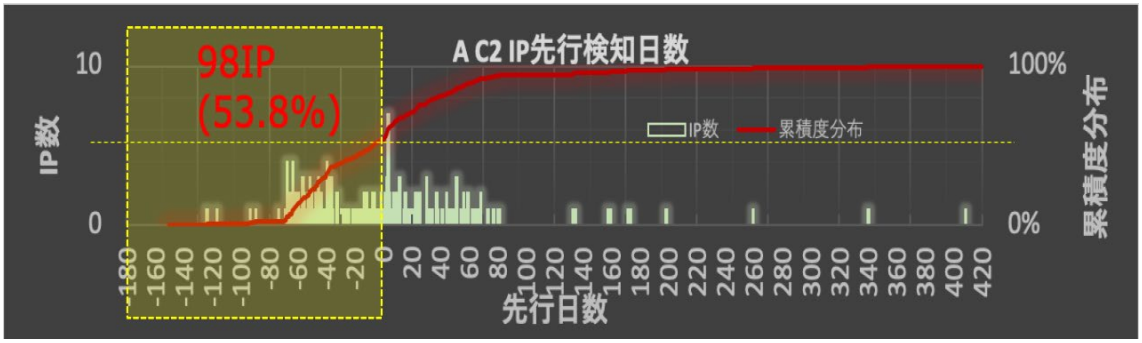


図 12　C&C サーバの検知結果と事業者間の相関性

事業者	C&Cサーバ	
	総IP数	主要な関連マルウェア
事業者A	183 (1.2/日)	Mirai系 116(61%)
事業者B	586 (12.3/日)	Mirai系 388(66%)
事業者C	160 (11.4/日)	Emotet系 86(53%)

【課題】

C&C サーバの検知精度の向上に向けて、検知手法や評価手法の更なる改善を図るとともに、関係機関との連携によるソース情報の拡充を図っていくことが必要である。

また、８割の C&C サーバは 10 日以内で接続できなくなるとの観測結果もある[21]等、C&C サーバの生存期間が限られていることも踏まえ、検知データのリアルタイム性を出来るだけ確保していくことが重要である。

検知データをセキュリティ対策に効果的に活用するため、円滑かつ迅速に C&C サーバリストが共有されるような仕組みや共有すべきデータの検討とあわせて、C&C サーバリストの具体的な利活用シーンについて更に整理が必要である。

さらに、前述のように、事業者間連携を更に進めることによって、より多くの C&C サーバを検知できる可能性が期待されているが、C&C サーバの検知のためにフロー情報を分析できる技術・リソースを有する事業者は一部に限られていることから、より多くの事業者が C&C サーバを検知するためには、検知手法の共有が必要不可欠である。

②IoT ボットネットの可視化

【現状・成果】

情報通信ネットワークの機能に支障を及ぼし得るサイバー攻撃に未然に対応するため、端末（IoT 機器）側の対策として NOTICE プロジェクト、ネットワーク側の対策として C&C サーバの検知等に関する実証を各々で実施している。

【課題】

C&C サーバの居場所は頻繁に変わる一方、ボットネット端末は変わらないため、ボットネット端末は次々異なる C&C サーバから攻撃指令を受けている状況であることを踏まえれば、「攻撃インフラ」としての IoT ボットネットの全体像の可視化を進めていくことが必要である。

---

[21] 脚注5参照。

また、多数の IoT 機器を踏み台とした大規模サイバー攻撃に効果的に対処していくためには、脆弱性のある IoT 機器、IoT ボットネット、C&C サーバ等全体を俯瞰した対応が必要であり、情報の適正な取扱いを確保した上で、様々な情報を重ね合わせていくことで精度を上げながら全体像を把握していくことが重要である。

さらに、恒久的な対策に向けて、対処が必要な IoT 機器の情報、マルウェアの情報、C&C サーバの情報、サイバー攻撃の発生に関する情報等、全ての情報がそろっていることが必要であるものの、個々の ISP にとってこれらの情報を総合的に収集・分析することが困難であるため、こうした取組を促進するような方策を検討していく必要がある。

（３）今後の対応策

①C&C サーバの検知精度の向上・検知情報の共有・利活用等の推進

NICT その他関係機関との連携等による C&C サーバの更なる検知精度の向上や、検知・評価に係る作業の短縮化に取り組むとともに、C&C サーバの死活監視を通じてその活動状況を逐次観測することにより、収集するデータのリアルタイム性の確保を目指す。

検知された C&C サーバリストについて ISP 間で試行的な共有・検証を行いながら、迅速かつ効果的な共有・利活用に関する具体的な枠組み・ルールの策定に向けて検討を加速する。

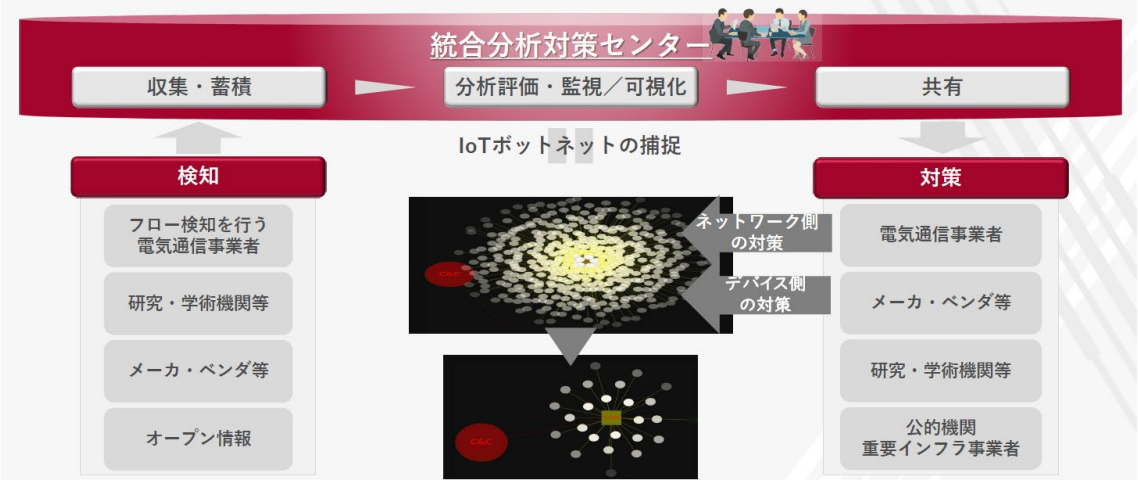
さらに、可能な限り多くの ISP が参加し、C&C サーバの幅広い検知ができるような環境を整備するため、C&C サーバの検知手法に関する ISP 間の情報共有の促進に取り組む。

②IoT ボットネットの全体像の可視化

NOTICE で検知された脆弱性等のある IoT 機器や、今般の実証で検知した C&C サーバリスト等、端末側・ネットワーク側両面から情報の収集・分析を行い、IoT ボットネットの全体像の可視化につなげていくための観測網である「統合分析対策センター（仮称）」を立ち上げる。

IoT ボットネットの全体像を可視化した上で、個々の IoT ボットネットの状況に応じて効果的な対策を講じられるよう、幅広い関係者が柔軟に役割分担をしつつ、NOTICE をはじめとする総合的な対策に取り組み、その対策の効果を確認しながら、最終的に IoT ボットネットを縮小することを目指す。（図 13）

図 13　統合分析対策センター（仮称）のイメージ



４．今後の進め方

本とりまとめは、総合的な IoT ボットネット対策の実現に向けて、端末（IoT 機器）側、ネットワーク側各々について今後取り組むべき対応策を示したものであるが、いずれの対策についても着手可能なものからスピード感を持って速やかに取り組むことが求められる。

また、IoT ボットネット対策は決して国内のみで完結するものではないことから、諸外国の動きや国際的な連携を常に視野に入れながら取組を進めることが必要不可欠である。

本とりまとめで示した対応策の進捗状況等については、必要に応じ、本分科会においてフォローアップを実施することとする。

「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」開催要綱

１ 目的

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中、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場合には、社会・経済に多大な影響を及ぼすおそれがあり、その安全性・信頼性の確保は喫緊の課題である。

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、依然として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、NOTICEや「電気通信事業者による積極的なサイバーセキュリティ対策に関する総合実証」等の取組みを含め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、「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」と称する。

３ 検討事項

（１）IoT におけるサイバーセキュリティの確保に向けた取組（NOTICE 等）の現状と課題

（２）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の現状と課題（総合実証の検討等）

（３）上記課題の解決に向けた必要な方策

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５年１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）

「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」
構成員名簿

（敬称略、五十音順）

井 上 大 介	国立研究開発法人情報通信研究機構(NICT) サイバーセキュリティ研究所サイバーセキュリティネクサス長
河 村 真 紀 子	主婦連合会 会長
小 塚 荘 一 郎	学習院大学法学部 教授
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
齋 藤 衛	株式会社インターネットイニシアティブ セキュリティ本部長
田 中 暁	KDDI 株式会社情報セキュリティ本部 セキュリティ管理部長
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
藤 本 正 代	情報セキュリティ大学院大学 教授
吉 岡 克 成	横浜国立大学大学院環境情報研究院 教授

情報通信ネットワークにおけるサイバーセキュリティ対策分科会

における検討状況

回次	議事内容
第１回 （2023 年 1 月 18 日）	✓ 情報通信ネットワークにおけるサイバーセキュリティ対策分科会について ✓ IoT ボットネットの現状について ✓ NOTICE の取組状況について
第２回 （2023 年 2 月 16 日）	✓ 通信事業者によるサイバーセキュリティ対策の取組状況と課題について
第３回 （2023 年 3 月 16 日）	✓ 国内の IoT 機器が踏み台となった最近のサイバー攻撃事案について ✓ 地域 ISP 等によるサイバーセキュリティ対策の取組状況と課題について ✓ メーカー等によるサイバーセキュリティ対策の取組状況と課題について
第４回 （2023 年 4 月 21 日）	✓ フロー情報分析による C&C サーバ検知に関する調査の報告 ✓ 効果的な利用者への周知啓発について ✓ 諸外国におけるサイバーセキュリティ対策の取組事例 ✓ 論点整理
第５回 （2023 年 5 月 18 日）	✓ NOTICE ステアリングコミッティの設置について ✓ 取りまとめ骨子（案）ついて
第６回 （2023 年 6 月 19 日）	✓ 「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とりまとめ～総合的な IoT ボットネット対策の実現に向けて～」（案）について

（参考）

主な観測・調査システム

主体	観測・調査システム	観測・調査内容
NICT	○特定アクセス ○ポートスキャン	・日本国内で弱いID・パスワードを使用している機器を調査 ・リフレクション攻撃の踏み台になりうる機器、管理機能への認証なし管理機能アクセス可能な機器、脆弱性を有するVPN機器等を調査
	●NICTER □DAEDALUSアラート	【ダークネット観測システム】 ・マルウェアに感染した機器からのスキャンを大規模観測し、アラート発報 ・バックスキャッタによるDDoS攻撃検知
	●AmpMon （AmpPot）	【リフレクション型DDoS観測システム】 ・DRDoS（Distributed Reflection Denial-Service）、DDoS攻撃を観測し、アラート発報
	●STARDUST	【サイバー攻撃誘引基盤】人間の攻撃者による攻撃の誘引・観測
	●□WarpDrive	【Web媒介型サイバー攻撃対策プロジェクト】プロジェクト参加ユーザのWebアクセスを観測（悪性サイトを検知し、アラート発報）
	●ライブネット	【機構内システム】機構内の実トラフィックおよびセキュリティ機器から発報されるアラートを観測（観測データはNIRVANA改で統合、CUREへ蓄積）
ICT-ISAC JAPAN	●無人くん ●無人ガーZ □PRACTICE Alert	・重要インフラ観測システム（重要インフラ1000団体、3000URLのレスポンス監視） ・レスポンス観測システム（複数センサーによる特定サイトレスポンス監視） ・DRDoS攻撃アラートシステム（DNSアンプ攻撃、DRDoS攻撃、 DNSランダムサブドメイン攻撃を観測、アラートとして配信）
	○Zakion	・広域スキャンシステム（毎週スキャン、2019年以降時系列データ検索可能）
	○Vuldate	・AIによる脆弱性の攻撃利用の危険度評価・予測システム
横浜国大	●DRDoSハニーポット ●IoTPOT ●IoTボットネットC2判定・監視システム □Am I Infected？	・DRDoS攻撃、DNSランダムサブドメイン攻撃の検知 ・IoT機器等への攻撃観測、悪用された脆弱性を判別すると共にIoTマルウェアの自動収集 ・IoTPOTで収集したマルウェア検体の自動解析、機械学習によりC&Cサーバを自動判定、判定したC&Cサーバに疑似マルウェアスクリプトで接続し、攻撃命令を収集 ・NICTER情報等と突合利用してアラート表示
JPCERT/CC	●TSUBAME	・インターネット上の攻撃動向観測システム（観測用センサーを分散配置） （ICMP、FTP、SSH、TELNET、SMTP、DNS、HTTP、POP3、NTP、IMAP4、HTTPS、MSSQL、RDP等を観測）

※　下線：東京オリンピック・パラリンピック競技大会や、G7広島サミットなどの際にも主に活用、○脆弱性調査、□アラート伝達、●感染・攻撃情報