別紙２

IoT・5G セキュリティ総合対策 2020

令和２年７月

サイバーセキュリティタスクフォース

目次

はじめに

Society5.0 の実現に向けて IoT や 5G をはじめとする ICT の利活用が一層進展していく中で、サイバーセキュリティリスクへの対策の一層の強化は急務となっている。

これまで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、IoT・5G の時代にふさわしいサイバーセキュリティ政策の在り方について検討を行ってきた。

折しも 2020 年（令和２年）に入ってからは、新型コロナウイルス感染症（以下「COVID-19」という。）への対応を官民で連携して取り組んでいる状況であるが、まさに未曾有の国難ともいえるこの状況において、テレワークシステムや Web 会議システムがビジネスやプライベートなど様々な分野で活用され、SNS アプリによるアンケートを通じたデータ収集が COVID-19 への対策の立案に活用されるなど、経済活動や国民生活において ICT の有用性が再認識されている状況である。

本文書は、2019 年（令和元年）８月に策定・公表した「IoT・5G セキュリティ総合対策」について、同総合対策の策定後の議論等を踏まえ、必要な改定を行ったものである。ICT は我が国の社会・経済、そして国民生活の重要な基盤として機能しており、サイバー空間のセキュリティ、すなわちサイバーセキュリティの確保は極めて重要な政策課題である。本文書を羅針盤として、総務省が関係府省庁や地方公共団体及び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が期待される。

Ⅰ　背景

（１）IoT・5G セキュリティ総合対策以降の状況変化と改定

本タスクフォースでは、2019 年（令和元年）８月に、「IoT・5G セキュリティ総合対策」を公表したところであるが、その際、直近で特に対策が必要となるサイバーセキュリティ上の留意事項として以下の６点を掲げたところである。

① 5G の開始に伴う新たなセキュリティ上の懸念
② サプライチェーンリスクの管理の重要性
③ Society5.0 の実現に向けた適切なデータの流通・管理の重要性
④ サイバーセキュリティにおける AI の利活用の重要性
⑤ 大規模な量子コンピュータの実用化の可能性
⑥ 大規模な国際イベント等の開催

本タスクフォースにおいて、同総合対策の公表後も、2020 年東京オリンピック・パラリンピック競技大会（以下「東京大会」という。）を控える中、取り組むべき施策の総点検を行うとともに、新たな課題への対応や施策展開の加速化を図るため、議論を継続して実施した。

その中で、2020 年（令和２年）７月より開催される予定であった東京大会に向けた対処として、2020 年（令和２年）１月に「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項 ［緊急提言］」（以下「緊急提言」という。）をとりまとめ、公表したところである。また、緊急提言の公表後は、「IoT・5G セキュリティ総合対策」の進捗状況等の確認を行いつつ、主に中長期的な取組について議論を実施した。

以上のような「IoT・5G セキュリティ総合対策」の策定・公表後の議論や状況変化を踏まえつつ、本タスクフォースでの検討の結果、「IoT・5G セキュリティ総合対策」を改編し、新たな施策を盛り込む形で「IoT・5G セキュリティ総合対策 2020」を策定することとしたものである。

（２）改定に当たっての主要な政策課題

「IoT・5G セキュリティ総合対策 2020」の策定に当たり、本タスクフォースでは、以下の４つを主要な政策課題として捉えている。

① COVID-19 への対応を受けたセキュリティ対策の推進

COVID-19 については、2020 年（令和２年）７月４日 15 時時点で感染者数が世界全体で約 1,103 万人、うち死亡者数が約 52 万 4,000 人にも及んでいる状

況であり、まさに世界全体として未曾有の事態に直面しているといっても過言ではない。

我が国においては、2020 年（令和２年）２月 25 日には新型コロナウイルス感染症対策本部において、「新型コロナウイルス感染症対策の基本方針」が決定され、当該基本方針において「患者・感染者との接触機会を減らす観点から、企業に対して発熱等の風邪症状が見られる職員等への休暇取得の勧奨、テレワークや時差出勤の推進等を強力に呼びかける。」とするなど、早期からテレワークの積極的な活用を図ってきた。その結果、様々な組織において、テレワークシステムを活用した在宅勤務やクラウド型の Web 会議システムを活用したミーティングなどの実施が進んでいるところである。

また、上記のような COVID-19 への対応における行動変容は、感染拡大が終息に向かい又は終息を迎えた後も維持され、その結果、生き方・住み方・働き方をはじめとする人々の価値観や社会・コミュニティ・経済の在り方が大きく変わるパラダイムシフトが今後まさに起きようとしていると考えられる。

その際、時間や距離の壁を越えることを可能にする ICT の役割はこれまで以上に大きくなっていくと考えられ、同時にそのような ICT を安全・安心に利用するためのサイバーセキュリティの重要性が益々高まることが想定される。

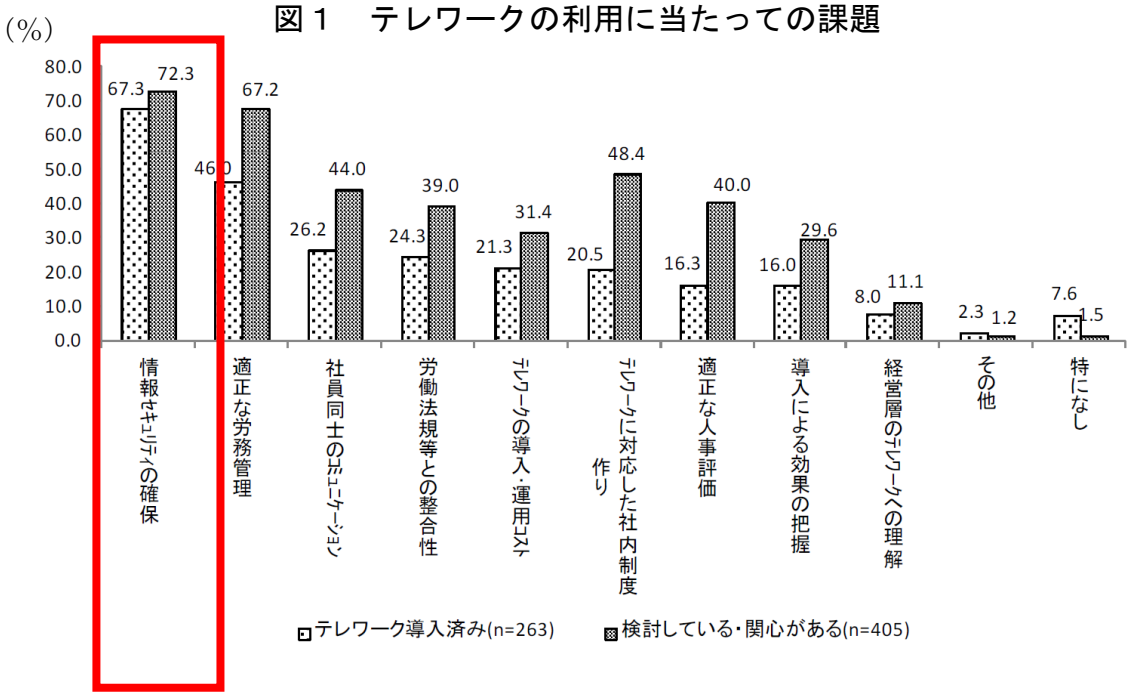
以上を踏まえつつ、COVID-19 への対応を踏まえ、本タスクフォースとしては、現時点において、以下の２点について課題認識を共有するに至った。

１）テレワークの利用の増加への対応

COVID-19 の感染拡大防止に当たっては、前述のとおり早期からテレワークの活用を呼びかけており、特に緊急事態宣言の発出後は、人と人との接触機会を８割程度低減することと併せ、テレワークが強力に推進されてきた。

他方、テレワークの実施に当たっては、職場環境に閉じた LAN ではなくインターネット経由での業務を前提とする必要があることや、通常と異なる勤務環境やシステムを利用する場合も多いことから、適切なセキュリティ対策を取ることが求められることとなる。実際にテレワークを導入するに当たっては、約７割の企業が「情報セキュリティの確保」が課題と感じているという調査結果もあり、より一層のテレワークを普及させる観点からも、セキュリティの確保が必要である。

図１　テレワークの利用に当たっての課題



（出典）地方創生と企業における ICT 利活用に関する調査研究
（2015 年３月 三菱 UFJ リサーチ&コンサルティング）

特に中小企業等においては十分なセキュリティ知識を有した担当者がいない場合が多いことが想定されるほか、COVID-19 への対応等のため、準備期間が十分とれずにテレワークを導入することとなった企業も多いことが想定される。テレワークのセキュリティ確保については、総務省にて 2018 年（平成 30 年）４月に「テレワークセキュリティガイドライン（第４版）」[1]を作成しているほか、今般の COVID-19 への対応に関連して、各政府機関等において注意喚起が行われている[2,3]ところであるが、中小企業等がテレワーク環境下におけるセキュリティ対策をより容易に強化できるようにするため、テレワークシステムのセキュリティに関するチェックリストの作成や相談窓口の拡充などの実践的な支援に取り組んでいくことが必要である。また、

[1] 2004 年（平成 16 年）12 月に初版を策定し、2006 年（平成 18 年）４月に第２版改定、2013 年（平成 25 年）３月に第３版改定を実施している。

[2] 2020 年（令和２年）３月 16 日、警視庁より、テレワークに関し端末の OS やウイルス対策ソフトは常に最新の状態に更新し、定期的なウイルススキャンを実施するよう呼び掛けを実施。

[3] 2020 年（令和２年）３月 27 日、内閣官房内閣サイバーセキュリティセンターより、パスワードの複雑化、多要素認証、アップデートの励行、通信の暗号化などテレワーク実施に当たっての注意喚起を実施。

そのような取組に当たっては、テレワークシステム等に関する実態調査を行い、実際の業務やシステム構成に応じた活用しやすいものにしていく必要がある。

また、テレワークが実施又は推奨されている企業においても、急遽テレワーク実施中に出社する必要が発生するケースが存在し、具体的な理由として請求書や押印手続、印刷など紙の書類の処理の必要性が挙げられている[4]。この点で、テレワークの普及の促進の観点からも、紙の書類のデジタル化や業務そのもののデジタル化の更なる促進が必要である。

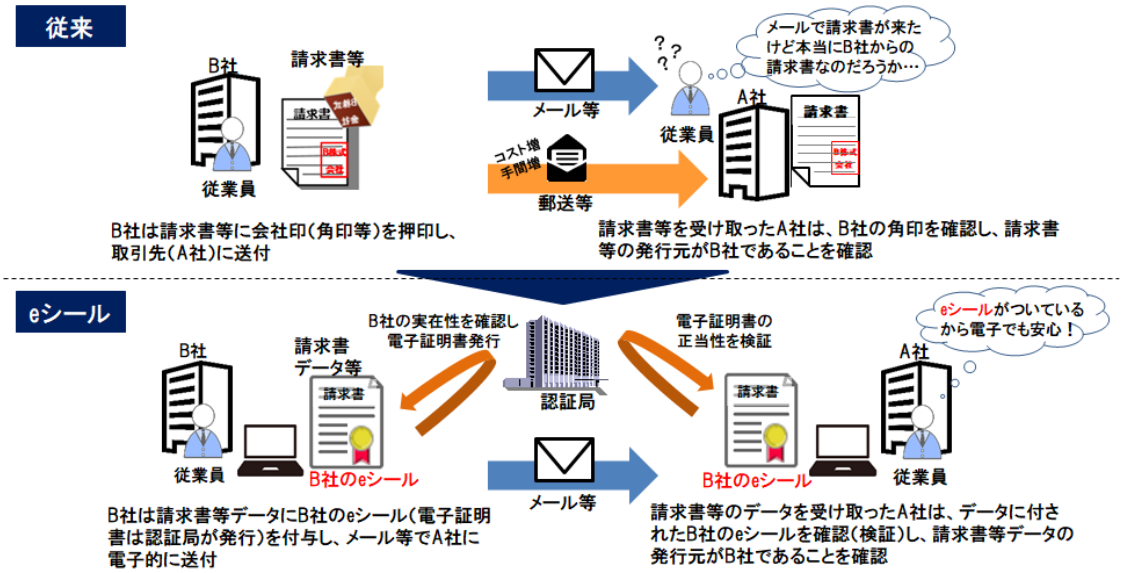
他方、デジタル化の促進のためには、業務上作成又は保管等を行っている書類の真正性を電子的に確保できる手段が必要不可欠であり、例えば、電子署名やｅシール[5]などのトラストサービスの活用を促進することが考えられる。併せて、一定の信用度のあるトラストサービスを認定するような公的な枠組みを構築することで、一層その普及を加速していくことが重要である。

---

[4] 一般社団法人日本 CFO 協会によれば、同協会会員を主体とした日本企業の CFO 及び経理・財務幹部へのアンケート調査の結果、テレワークを実施または推奨した約 70%のうち、41%が「テレワーク実施中に出社する必要が発生した」という回答となっている。また、「紙の書類、紙の証憑証跡がほとんどない、又はデジタル化している」に対応していないという回答が 77%であった。

[5] 電子文書の発信元の組織を示す目的で行われる暗号化等の措置で、企業の角印の電子版に相当する。個人名の電子署名とは異なり、使用する個人の本人確認が不要であり、領収書や請求書等の経理関係書類等のような迅速かつ大量に処理するような場面において、簡便にデータの発行元を保証することが可能。データ発行元の組織を簡便に確認できるようになり、これまで紙で行われていた書類等の企業間のやり取りを電子的に安全に行えるようになり、従来の郵送の手間やコストの削減による業務効率化や生産性向上が期待される。

図２　ｅシールの仕組み



（出典）組織が発行するデータの信頼性を確保する制度に関する検討会（第１回）事務局作成資料より抜粋

２）クラウドサービスの利用の進展を踏まえた対応

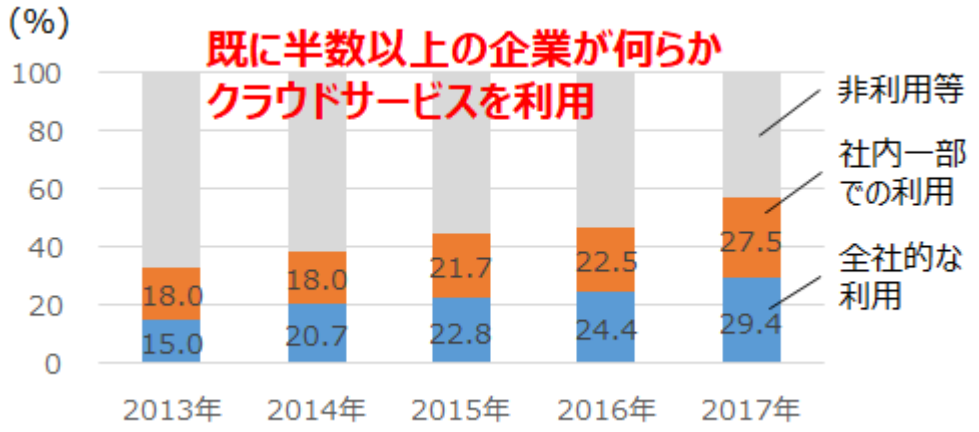
組織における情報システムの構築や運用においてクラウドサービスを活用する場合、正しい選択を行えば、コスト削減に加えて、情報システムの迅速な整備、柔軟なリソースの増減、自動化された運用による高度な信頼性、災害対策、テレワーク環境の実現等に寄与する可能性が大きい[6]。

我が国においては、既に半数以上の企業が何らかのクラウドサービスを利用する状況であったが、COVID-19 への対応を受け、Web 会議システム等の爆発的に利用が進んでいるサービスも存在[7]するなど、今後クラウドサービスの利用の動きが加速していくことが想定される。

[6]「政府情報システムにおけるクラウドサービスの利用に係る基本方針」(平成 30 年６月７日 各府省情報化統括責任者（CIO）連絡会議決定）によれば、クラウドサービスの利用のメリットとして、①効率性の向上、②セキュリティ水準の向上、③技術革新対応力、④柔軟性の向上、⑤可用性の向上の５つが挙げられている。

[7] 例えば、米国の Microsoft 社の発表によれば、同社の提供するチームコラボレーションサービス「Microsoft Teams」で実施される１日当たりの会議実行時間が 2020 年（令和２年） ３月 31 日時点で、同年３月 16 日の９億分から 200%増（３倍）の 27 億分（4,500 万時間）に至ったとのことである。

図３　クラウドサービスを利用している企業の割合



（出典）平成 30 年版　情報通信白書

他方、クラウドサービスが重要な社会基盤となりつつある現在においても、セキュリティに対する不安やセキュリティ上の課題は依然として存在する。例えば、2019 年（令和元年）８月には、大手クラウドサービスの東京リージョンの１つのアベイラビリティゾーン（AZ）において、空調設備の管理システムの障害が原因で長時間にわたってサービス障害が発生した。また、2019 年（令和元年）12 月には、自治体専用 IaaS サービスにおいてストレージ障害やデータアクセス障害が発生し、大多数の仮想 OS に影響が発生し、結果、多数の自治体の業務システムなどに長期間影響が出た。一方、クラウドサービス利用者・調達者側の設定ミスが原因とされる情報漏えい等も相次いで発生しており、こうした事故の損害については提供者側は責任を負わず、その多くが利用者・調達者側の責任とされている。

また、特に、昨今では基幹的な業務システムでクラウドサービスを活用するなど、高い可用性を求められるユースケースも存在しており、クラウドサービスの提供者において着実なセキュリティ対策を取ることが期待される。

現在、政府機関等が調達するクラウドサービスのセキュリティに関しては、「政府情報システムのためのセキュリティ評価制度」（通称　ISMAP: Information system Security Management and Assessment Program）の制度立ち上げに向けた準備が進められている。また、従前より民間団体等においては、クラウドサービスのセキュリティに関する認証等の取組もなされているところであり、このようなクラウドサービスのセキュリティの可視化の取組が着実に進んでいくことが望ましい。

一方、クラウドサービスのセキュリティは一般的に「責任共有モデル」が

採用されており、クラウドサービス提供者と利用者・調達者の共通の認識の下、それぞれの管理権限に応じた責任分担を行うものである。そのため、クラウドサービス提供者と利用者・調達者は、それぞれの役割を適切に果たすことで、クラウドサービスに関するセキュリティリスクを最小化するために、共に協力することが望ましい。この点で、利用者・調達者は、自らの責任の下で、必要に応じてクラウド環境におけるセキュアなアプリケーション開発や、サービス提供者から供給されるツールや対応策も活用し、セキュリティリスクを最小化することが求められる。したがって、クラウドサービス提供者のみならず、クラウドサービス利用者・調達者のリテラシーの向上も重要であり、クラウドサービス提供者においては、利用者・調達者がリスクを適切に判断できるような情報を開示するとともに、必要に応じ、セキュリティに関する啓発活動や研修等を通じて、その役割を果たしていくことが期待される。

なお、付言すれば、クラウドサービスの利用の進展や、先述のテレワークの利用促進に伴って、これまで以上にそれぞれの組織においてオフィスの内外にまたがる通信やアクセスが増加し、境界の概念がなくなっていくなど、ネットワーク維持・管理の在り方や対応するセキュリティ対策の在り方も変化していくことが想定される。このような ICT 利活用の進展に合わせ、新たなネットワークセキュリティモデル[8,9]も考案されている。

以上のように、COVID-19 への対応の後には、これまでとは異なったシステム・ネットワークの在り方が求められ、普及していく可能性がある。従来のク

---

[8] 米国標準技術研究所（NIST：National Institute of Standards and Technology）は「Draft（2nd）NIST Special Publication 800-207」において、「Zero Trust」のネットワークインフラについて、以下の前提を置いている。
・企業のプライベートネットワークは信頼できない
・ネットワーク上のデバイスは企業によって所有又は設定可能でない可能性がある
・内在的に信頼されているデバイスは存在しない
・全ての企業のリソースが企業の所有するインフラストラクチャ上に存在するわけではない
・企業の遠隔ユーザはローカルのネットワーク接続を信頼できない

その上で、「Zero Trust Architecture」が踏まえるべきコンセプトとして、
・あらゆる通信はネットワークの場所に関係なく保護される
・個々の企業のリソースへのアクセスは、接続単位で保証される
・ユーザ認証はアクセスが許可される前に動的かつ厳格に実施される
などを上げている。

[9] Gartner 社はネットワーク機能とネットワークセキュリティ機能を１つのクラウドプラットフォームに統合し、各機能をサービスとしてエッジに提供するモデル（Secure Service Access Edge）を提唱しており、これにより、複雑性やコストの削減、遅延の改善などが期待されている。

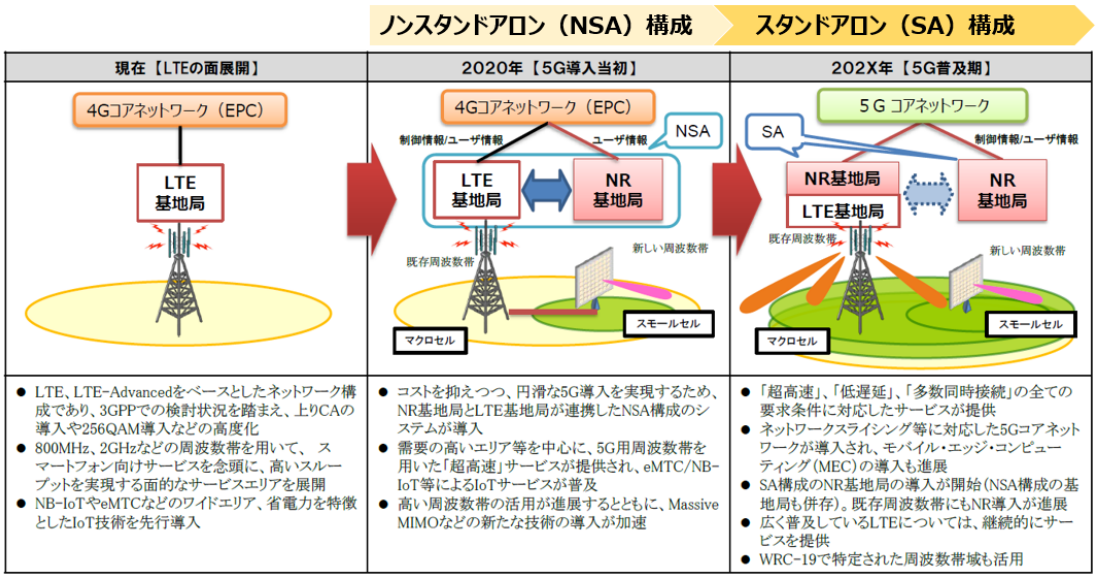
ラウド・バイ・デフォルト原則[10]や働き方改革などの流れを受けた、システム・ネットワークの在り方の変化なども踏まえつつ、新たな時代に対応したセキュリティ対策を引き続き検討していくことが求められる。

② 5G の本格開始に伴うセキュリティ対策の強化

5G は、4G など従来の移動通信システムと比較して、「超高速」、「超低遅延」、「多数同時接続」であるという特長を有しており、IoT 時代の基盤技術として、様々な産業分野での利活用が期待されている。

5G については、携帯電話事業者による全国 5G に加え、地域の企業や自治体等の様々な主体が自らの建物や敷地内でスポット的に柔軟に構築し利用することのできるローカル 5G の導入が進んでいる 5G サービス開始当初は 4G のコアネットワークを活用したノンスタンドアロン（NSA）構成での運用がなされるが、将来的には 5G のコアネットワークを使用したスタンドアロン（SA）構成での運用が進んでいくと見込まれている。

図４ 5G のノンスタンドアロン構成とスタンドアロン構成



（出典）総務省作成資料

他方、サイバーセキュリティの観点からは、5G のネットワークでは、モバイルエッジコンピューティング（MEC）[11]の活用に加え、ネットワーク機能の仮想化・ソフトウェア化などが一層進んでいくことが想定されるため、ソフトウ

[10] 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（平成 30 年６月７日各府省情報化統括責任者（CIO）連絡会議決定）により、政府情報システムは、「クラウドサービスの利用を第一候補として、その検討を行うものとする」とされた。
[11] ネットワークのエッジ（ユーザの近く）でなされる通信処理や高度な演算・データ処理。

ェアをはじめとするサプライチェーンリスクへの対応が不可欠である。

また、5G のネットワークは、ネットワークのリソースを動的に管理、制御することができるようになるなど、従来のネットワークとは構造等の点において異なる特徴を有することが想定されるほか、様々な産業用途での利用が想定されるなど、まさに社会基盤として、これまでとは異なる多岐にわたるユースケースが想定される。

5G については、2020 年（令和２年）より、携帯電話事業者が一般向け 5G サービスを提供開始しているほか、ローカル 5G についても免許交付が始まっているところであり、将来の社会基盤としての 5G の安全性や信頼性の確保のため、5G 黎明期の現段階から、セキュリティ・バイ・デザインの観点で、官民で連携して対策を取る必要がある。具体的には、以下のような対策が想定される。

・脆弱性[12]及び脅威の検証・分析のための手法や体制の確立

5G のネットワークのセキュリティ確保の観点からは、サプライチェーンリスクへの対応を念頭に置きつつ、ハードウェア・ソフトウェアの両面において脆弱性の検証手法等を確立することが必要である。その上で、脆弱性検出技術の成果について、技術移転などの形で活用するとともに、関連する脅威の分析の視点を踏まえつつ、システムや利用者に対するインパクト分析を実施し、必要なセキュリティ対策を検討することが必要である。また、このような検証・分析の取組においては、5G の事業者・運用者やベンダー等が協力して実施する体制を構築することが必要である。

なお、「Beyond 5G 推進戦略 －6G へのロードマップ－」（令和２年６月 30 日総務省）でも謳われているように、将来の移動通信システムのネットワークにおいては、サイバーセキュリティ常時確保機能の実現が期待されている。そのため、将来的には、リアルタイムの改ざんの検知や脆弱性の検出等を自動的に行うために必要となる技術の開発なども想定され、これらの取組を促進していくことも必要である。

・情報共有の促進

5G のネットワークの運用又は利用については、多様なプレイヤーによる多様な用途が想定されることから、その脆弱性や脅威について、5G の事業

[12] ここでいう脆弱性とは、ソフトウェアやハードウェアにおいて、コンピュータ不正アクセスやコンピュータウイルスの攻撃等により、その機能や性能を損なう原因となりうるセキュリティ上の問題箇所のことを指す。

者・運用者やベンダー等との間で適切に情報共有が図られることが必要である。特に 5G が利用されているインフラのハード・ソフトの脆弱性情報や脅威情報、さらにこれらの対処の在り方に関する情報については、速やかにベンダーから事業者・運用者に提供されることが求められる。

・セキュリティ対策の実装の促進

セキュリティ対策の実装の促進の観点からは、セキュリティ・バイ・デザインの観点から、5G の事業者や運用者に対し、実際に対策の実施を促すための制度的な措置や産業振興的な措置を取ることが必要である。

5G のセキュリティの確保に当たっては、上記のように多面的なアプローチで対策が進んでいくことが必要である。

③　サイバー攻撃に対する電気通信事業者のアクティブな対策の実現

サイバー攻撃がますます巧妙化・多様化し、また今般の COVID-19 への対応のためのテレワークの普及拡大等によりインターネットに接続される機器が急激に増加し、脆弱でそのセキュリティ対策が困難な機器が増加する中、端末側と通信ネットワーク側の双方から総合的なセキュリティ対策を実施することが求められている。

端末側の対策としては、これまで電気通信事業法（昭和 59 年法律第 86 号）における端末設備等規則（昭和 60 年郵政省令第 31 号）へのセキュリティ要件の導入や、脆弱な状態にある機器の利用者への注意喚起等の取組、IoT 機器の不正検知等のためのゲートウェイの設置といった取組を実施してきた。

これらに加えて、ネットワーク側での対策として、電気通信事業者が、適切な自社ネットワーク保護やユーザの保護のために、機器の利用者への注意喚起等の取組と併せて、電気通信事業者が個々の感染端末に指示を出す C&C サーバに直接対処するなど、より効率的にセキュリティ対策を実施することが求められており、サイバー攻撃が経由する電気通信事業者の果たす役割は大きい。例えば、IoT のセキュリティに対する対策は、これまで IoT 機器の対策を中心にとられてきたところであるが、IoT を狙った攻撃は依然として多く、今後、様々な産業で IoT 機器の利用が拡大することが予想される中、これまでの対策だけでは必ずしも十分ではないおそれがある。

図５　IoT 機器を狙った攻撃の増加
（NICTER により１年間に観測されたサイバー攻撃回数）

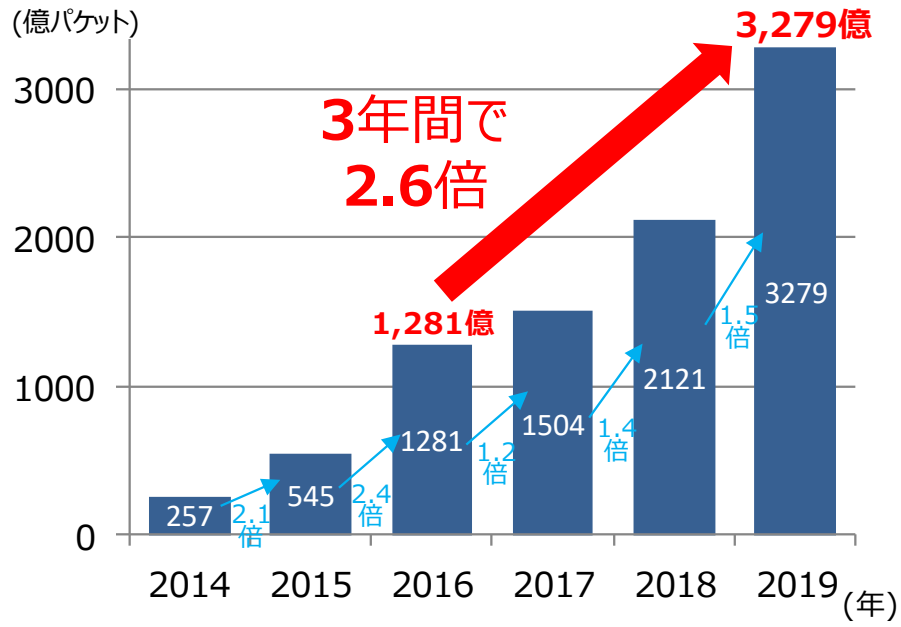
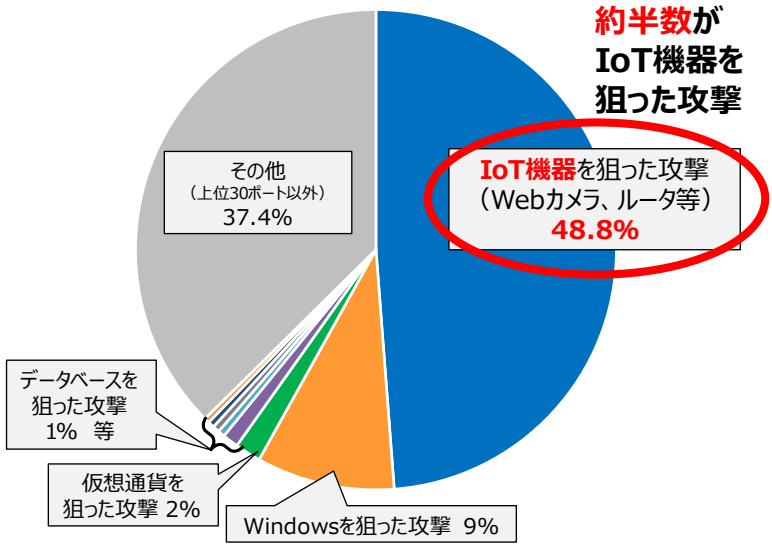
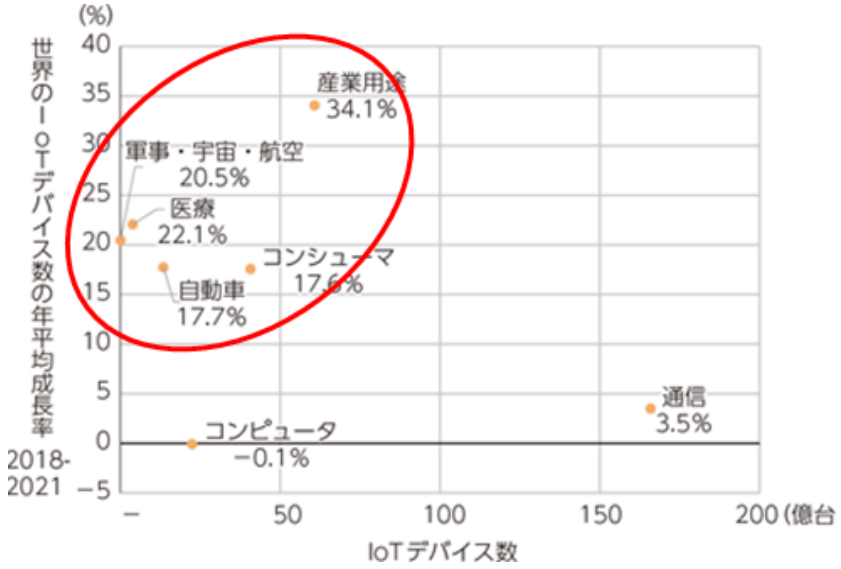


図６　IoT 機器を狙った攻撃の割合



※　NICTERで2019年に観測されたパケットのうち、調査目的パケット以外についてサービス種類（ポート番号）ごとに上位30ポートまでを分析したもの。なお、IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。

図７　IoT 機器の数と年平均成長率

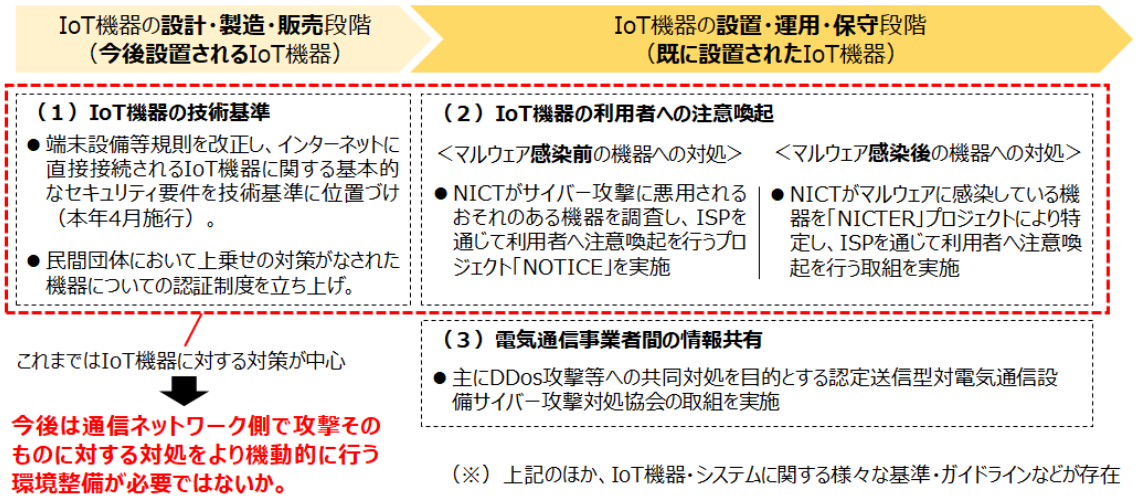


（出典）IHS Technology

これまでの IoT のセキュリティ対策は、IoT 機器の機能要件の設定や、パスワードの設定等に不備のある IoT 機器等の調査及び注意喚起の実施など、IoT 機器に対する対策が中心であった。

一方で、IoT のセキュリティ対策をより実効的なものにするためには、サイバー攻撃が通過するネットワーク側でより機動的な対処を行う環境整備が必要と考えられる。

図８　IoT の対策のイメージ



（出典）サイバーセキュリティタスクフォース（第 23 回）事務局作成資料

このため、IoT をはじめ、情報通信システム全般において、海外における動

向（制度、実施状況等）も参考としながら、ユーザ側で運用している情報通信機器や情報システムのセキュリティ対策と連動する形で、インターネット上でインターネットサービスプロバイダ（以下「ISP」という。）が管理する情報通信ネットワークにおいても高度かつ機動的な対処を実現するための方策の検討が必要である。

具体的には、ISP が自ら C&C サーバ[13]を検知し、サイバー攻撃の指令通信の遮断等の対策を実施するための方策や、新技術を活用した対策の高度化を促進するための方策について、制度的・技術的な観点から検討等を行う必要がある。

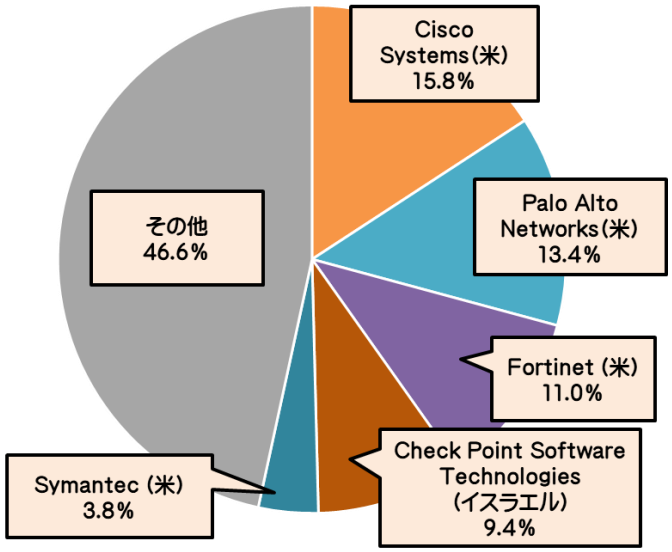
④　我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

我が国のセキュリティ事業者は、海外のセキュリティ製品を導入・運用する形態が主流である。そのため、我が国のサイバーセキュリティ対策は、海外製品や海外由来の情報に大きく依存しており、国内のサイバー攻撃情報等の収集・分析等が十分にできていない状況である。

例えば、2019 年（令和元年）第４四半期時点における世界のセキュリティ製品市場では、上位５者が約半数のシェアを占めており、いずれも米国やイスラエルなどの海外事業者である。

13 ボットネットや感染コンピュータのネットワークに対し、不正なコマンドを遠隔で頻繁に送信するために利用されるサーバのこと。Command and Control サーバの略。

図９　世界セキュリティアプライアンス製品市場ベンダー別シェア（売上額）（2019 年（令和元年）第４四半期））

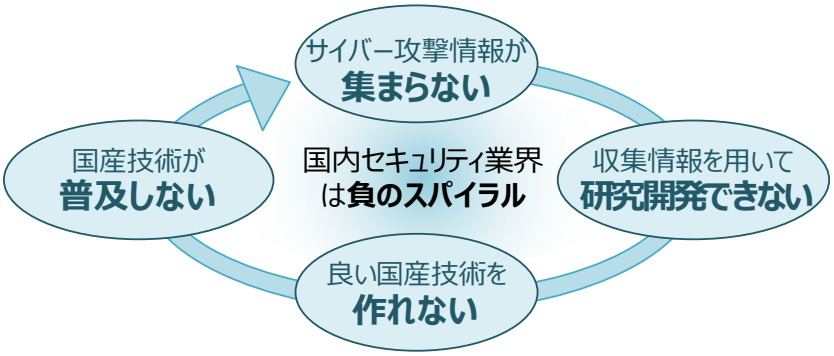


（出典）IDC プレスリリース ″ Top 5 Companies, Worldwide Security Appliance Revenue, Market Share, and Growth, Fourth Quarter of 2019 (revenue in US$ millions)″より作成

こうした海外事業者の製品の使用により、国内のデータが海外事業者に流れ、我が国のセキュリティ関連の情報が海外で分析される一方、分析の結果得られる脅威情報を海外事業者から購入する状況が継続している。

また、この状況を別側面から見ると、(a)国内でのサイバー攻撃関連の実データが集まらず、(b)実データが集まらないため実データを使った研究開発ができず、(c)研究開発ができないため良い国産セキュリティ技術を作れず、(d)良い技術を作れないため国産技術が普及せず、(a')国産技術が普及しないからサイバー攻撃関連の実データも集まらない、という「データ負けのスパイラル」に陥っている状況である。

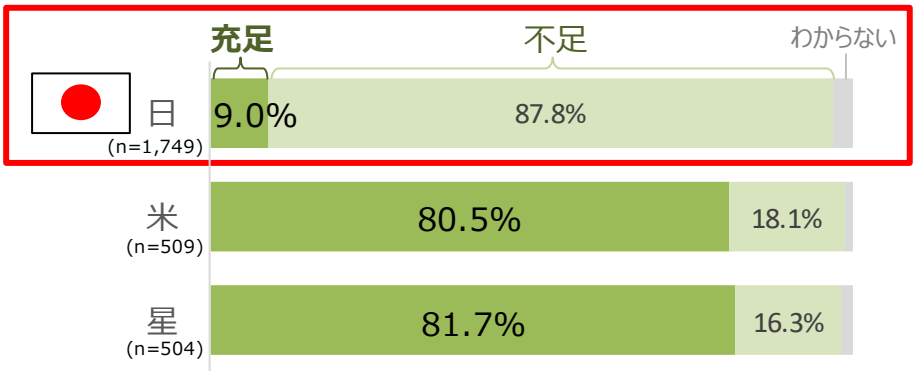
図 10　データ負けのスパイラル



（出典）サイバーセキュリティタスクフォース（第 23 回）資料 23-1 より作成

このように国内のセキュリティ事業者においては、実データが集まらないためコア部分のノウハウや知見を蓄積することができず、我が国がグローバルレベルの情報共有において一層の貢献を果たし、国際的に通用するエンジニアの育成をより効果的に実施することが難しくなっている。一方で、利用者側企業においても、セキュリティ製品やセキュリティ情報を適切に取り扱える人材が不足している状況がある。我が国においてセキュリティ人材が充足しているとの回答は１割を切っており、人材不足は深刻な状況である。

図 11　セキュリティ対策に従事する人材の充足状況



（出典）企業における情報セキュリティ実態調査 2019
（NRI セキュアテクノロジーズ）より作成

サイバーセキュリティ人材については、幅広い層において不足しているが、従来から人材育成のための対策を講じているシステム担当者等に加え、戦略を立てシステムベンダと共働しつつ組織のセキュリティ対策を先導できる人材が求められている状況にある。また、環境構築技術者・開発者層のセキュリティ知識の不足により、本来防げるはずのセキュリティインシデントが発生していることから、こうした人材についても不足を解消していく必要がある。

このような人材不足の一因としては、人材育成の仕組みや基盤が不十分であることが挙げられる。特に演習用の環境構築や演習シナリオ開発には高度な知識や技術力、基盤となる計算機環境が必要であり、個々の企業では十分に対応できない。また、国内では対応する基盤が十分でないため、基盤が整備されている海外の演習教材に依存することとなり、結果として日本特有の事例が十分に反映できない状況がある。

以上を踏まえ、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、サイバーセキュリティ人材の育成を含めて我が国のサイバー攻撃への自律的な対処能力を高めるとともに、我が国としてグローバルレベルの情報共有において一層の貢献を実現していくためには、オープン型の研究開発や人材育成の基盤を構築・運用して産業界等に開放し、産学官の英知を結集して、取組を進めていく必要がある。

Ⅱ　施策展開の枠組み

サイバーセキュリティ対策は広範な政策分野であり、その推進に当たっては各主体の適切な役割分担の下での連携・協働が必要である。この点、総務省に期待される役割は、まず情報通信サービス・ネットワークの、特に重点的に対応すべき個別分野のセキュリティの在り方について包括的な検討の上、関係府省庁や地方公共団体及び民間企業と連携しつつ、政策を実効的に推進していくことである。

さらに、当該分野での政策をより効果的に実施するための研究開発の推進や、情報通信サービス・ネットワークのユーザも含めた人材育成・普及啓発の推進、国際連携の推進、サイバーセキュリティに関する情報共有・情報開示の促進の観点からの取組を並行して進めていく必要がある。

そのため、本文書では、総務省として取り組むべき具体的な施策について、「Ⅲ情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策」と「Ⅳ　横断的施策」の「（１）研究開発の推進」、「（２）人材育成・普及啓発の推進」、「（３）国際連携の推進」、「（４）情報共有・情報開示の促進」という項目で整理を行っている。

なお、施策の検討・展開の際には、それぞれの取組において、例えば以下のような観点について留意しつつ、施策の有効性を確保する必要がある。

①　ネットワーク側とユーザ側の双方の観点からの施策展開

情報通信サービス・ネットワーク全体の安全性や信頼性を確保するためには、ネットワーク側とユーザ側の双方の視点でサイバーセキュリティ対策を推進するための施策を検討する必要がある。

②　情報通信サービス・ネットワークのレイヤー構造

情報通信サービス・ネットワークについては、機能に着目して構造的にサービス（データ流通）層、プラットフォーム層、ネットワーク層、機器層と分類が可能であるが、それぞれの層において留意すべき脅威とセキュリティ要件の在り方について検討する必要がある。

③　時間軸を意識した施策展開

施策の対象の時間軸（例：機器やシステムのライフサイクル）や、施策の効果の発現に関する時間軸（例：短期的又は長期的な人材育成）など、動学的な政策立案を行う必要がある。

④　政策バリューチェーンの構築

サイバーセキュリティ政策の効果をより高めるには、本総合対策に盛り込まれている施策間のみならず、関係府省庁の実施する個別施策との有機的な連携を図り、横断的で一貫性のある施策展開を図る必要がある。

Ⅲ　情報通信サービス・ネットワークの個別分野に関する具体的施策

Ⅰ、Ⅱを踏まえつつ、総務省において、サイバーセキュリティの確保に取り組むべき情報通信サービス・ネットワークの個別分野としては、以下のような分野が考えられる。なお、施策の検討に当たっては、「IoT・5G セキュリティ総合対策」に盛り込まれた取組の内容や進捗状況や、2020 年（令和２年）１月に策定・公表した緊急提言も踏まえることとした。

また、具体的施策の検討・実施に当たっては、前述（Ⅱ）の①～④の観点などに留意する必要がある。

（１）IoT のセキュリティ対策

①　IoT 機器の設計・製造・販売段階での対策

IoT 機器の設計・製造・販売段階においては、製造業者における IoT 機器のセキュリティ・バイ・デザインの考え方を十分に浸透させるとともに、対策がとられた機器の市場への展開を促進させることが重要となる。

この点、IoT 機器に関する基本的なセキュリティ対策については、電気通信事業法の枠組みにおいて端末設備等規則を改正し、強制規格としての技術基準が策定[14]されている（2019 年（平成 31 年）３月１日公布、2020 年（令和２年）４月１日施行）。また、当該改正後の同規則の各規定等に係る端末機器の基準認証に関する運用について明確化を図る観点から、総務省において 2019 年（平成 31 年）４月に「電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第１版）」を策定・公表している。今後は、当該技術基準の適切な運用を行っていくことが必要である。

また、こうした技術基準に加え、民間団体がセキュリティ要件のガイドラインを策定し、当該要件に適合した IoT 機器に対して適合していることを示すマークを付す認証（Certification）の仕組みを構築している。このような任意の認証（Certification）がより広範に普及するなど民間においても自主的な取組が進むことが期待される。

②　脆弱性等を有する IoT 機器の調査及び注意喚起

[14] インターネットプロトコルを使用し、電気通信回線設備を介して接続することにより、電気通信の送受信に係る機能を操作することが可能な端末設備について、最低限のセキュリティ対策として、①アクセス制御機能、②アクセス制御の際に使用する ID/パスワードの適切な設定を促す等の機能、③ファームウェアの更新機能、又は①～③と同等以上の機能を具備することを求めている。なお、PC やスマートフォン等、利用者が随時かつ容易に任意のソフトウェアを導入することが可能な機器については本対策の対象外とされている。

①の対策については、実効性を発揮するまでに一定程度の時間を要することから、既に設置されている IoT 機器のセキュリティ対策に関しては別に対応を行う必要がある。

この対策については、国立研究開発法人情報通信研究機構（以下「NICT」という。）の業務に、パスワード設定等に不備のある IoT 機器の調査等を５年間の時限措置として追加すること等を内容とする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）の改正を実施し、2019 年（平成 31 年）２月より、NICT が IoT 機器を調査し、電気通信事業者（ISP）を通じて利用者への注意喚起を行うプロジェクト「NOTICE[15]」を実施している。

また、2019 年（令和元年）６月より、既にマルウェアに感染している IoT 機器を NICT の「NICTER」プロジェクトで得られた情報を基に特定し、ISP を通じて利用者へ注意喚起を行う取組も実施している。

これらの注意喚起の取組について引き続き実施し、取組に参加する ISP の拡大を図っていくとともに、各 ISP において架電や往訪も含めた有効な注意喚起手法についてベストプラクティスの共有を行っていくことが必要である。また、総務省においても専用のサポートセンターを設置し、行政相談窓口や消費生活センター等と連携しつつ、Web サイトや電話による問合せ対応を通じて利用者に適切な IoT 機器のセキュリティ対策を案内することが必要である。そして、こうした IoT 機器の利用者に対する注意喚起に加えて、IoT 機器の製造事業者や、法人向け IoT 機器を念頭として IoT 機器を設置・運用する事業者（SIer 等）に対しても、脆弱な状態にある IoT 機器を増やさないような注意喚起等を行っていく必要がある。

さらに、緊急提言にもあるように、国内の重要施設に設置されている IoT 機器について、利用事業者名や用途がインターネット上から容易に判別できることなどによって攻撃を受けやすい状態に置かれていないか調査を行い、問題のある機器の所有者・運用者等に対策の実施を促していく取組を、東京大会までに実施する必要がある。

なお、これらの取組については、IoT 機器のセキュリティ対策のベストプラクティスとして、Ⅳ－（３）の国際連携の推進などの取組を通じ、海外各国に対して発信し、各国の取組につながるよう働きかけることが重要である。

③　サイバー攻撃に関する電気通信事業者間の情報共有

[15] National Operation Towards IoT Clean Environment の略。

脆弱性を有する IoT 機器が踏み台となったことが確認された際、被害の拡大を防止するため、ISP による、当該 ISP の利用者の端末と C&C サーバの間の通信を遮断するなどの取組が必要である。

この点、総務省では、2018 年（平成 30 年）５月の改正電気通信事業法において、電気通信事業者が「送信型対電気通信設備サイバー攻撃」への対応を共同して行うため、攻撃の送信元情報の共有や C&C サーバの調査研究等の業務を行う第三者機関(認定送信型対電気通信設備サイバー攻撃対処協会。以下「認定協会」という。）を総務大臣が認定する制度を創設し、2019 年（平成 31 年）１月に一般社団法人 ICT-ISAC[16]が認定されたところである。

今後は認定協会の活動について、マルウェアに感染している可能性の高い IoT 端末等や C&C サーバであると疑われる機器の検知や利用者への注意喚起等の電気通信事業者が行う対策に向け、円滑な実施のための支援を行うなどの取組を促進することが重要である。

また、こうした認定協会の活動や「NOTICE」の実施状況も踏まえ、電気通信事業者等が協力してサイバー攻撃への対処を行う際の基盤となる効果的な情報共有の在り方について引き続き検討することが重要である。

（２）5G のセキュリティ対策

①　脆弱性の検証手法等の確立と体制整備

5G のネットワークに関しては、仮想化・ソフトウェア化が進むことから、サプライチェーンリスクを含む新たなサイバーセキュリティ上の課題が懸念される。そのため、5G のネットワークやその構成要素及びサービスについて、ソフトウェア・ハードウェアの両面から技術的検証を行うことを通じ、5G のネットワークのセキュリティを確保する仕組みや体制を整備することが必要である。

具体的には、まず、ソフトウェアを中心としたネットワークの脆弱性については、5G の通信インフラとしての機能保証のため、ソフトウェアにより構成される部分を含め、ネットワーク全体のセキュリティを確保する必要がある。

---

[16] ISAC は Information Sharing and Analysis Center の略で、サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織を指し、分析した情報は ISAC に参加する会員間で共有され、各々のセキュリティ対策等に役立てられる。通信分野では、2002 年（平成 14 年）に他分野に先立ち、「Telecom-ISAC」が設立され、その後、会員企業を ISP 事業者、放送事業者、ICT ベンダー及びセキュリティベンダー等に拡大する形で、一般財団法人日本データ通信協会から独立し、「ICT-ISAC」として一般社団法人化。

そのため、5G の仮想環境を構築し、(a)オープンソースソフトウェア等の解析、(b)多種多様なパターンのデータ入力による異常動作確認（ファジング）、(c)エシカルハッカーによる脆弱性調査・脅威分析を実施し、対策を検討することが必要である。

一方、ハードウェアの脆弱性については、5G 等のネットワークを構成するハードウェア上に故意に組み込まれた不正なチップによって生じるセキュリティ上の課題に対応するため、AI を活用し(a)回路情報から不正に改変された回路を検知する技術や、(b)電子機器外部で観測される情報から不正動作を検知する技術を開発し、対策を検証することが必要である。

また、上記の検証結果を踏まえつつ、5G 等のネットワーク上での運用面の課題等についても検討する必要がある。

その上で、技術移転などを含めて前述のような脆弱性検出技術の成果を活用し、関連する脅威の分析の視点を踏まえつつ、システムや利用者に対するインパクト分析を実施し、必要なセキュリティ対策を検討することが必要である。また、このような検証・分析の取組において、5G の事業者・運用者やベンダー等が協力して実施する体制を構築することが必要である。

② 5G の脆弱性情報や脅威情報等の共有の枠組みの構築

4G までの従来の移動通信システムでは電気通信事業者がネットワークの運用を行っていたが、5G の時代では、ローカル 5G について、従来は通信サービスのユーザとしての位置づけであった様々な企業や自治体等がネットワークの運用者として関わっていくこととなる。

また、ネットワークの用途も、超低遅延や多数同時接続などの特長を活かした様々な産業用途が期待されているため、リスクや脅威の在り方も多様なものが想定される。

このため、5G のセキュリティを確保していく上では、①の脆弱性の検証と合わせ、5G のネットワークを運用している事業者・運用者やベンダー、利用者等の間での脆弱性情報や脅威情報、さらにこれらの対処の在り方に関する情報の共有の取組が重要である。

この点、5G とそのセキュリティに関する情報共有などを定期的に実施して 5G のセキュリティの啓発を進めるとともに、ローカル 5G を含む 5G の運用者が 5G サービスを提供する場合のサイバーセキュリティ上の懸念や脅威に関する問い合わせに対して助言を行うことを目的とし、2020 年（令和２年）２月

に一般社団法人 ICT-ISAC において「5G セキュリティ推進グループ」が設立されたところである。

上記のような民間での取組を踏まえつつ、引き続き、5G のセキュリティの確保に向け、情報共有の取組を促進することが必要である。

③ 5G のセキュリティ対策の促進のための政策的措置

5G のセキュリティ確保のためには、①、②の取組に加え、実際のネットワークにおいて対策の実装が進むことが必要である。この点、5G のセキュリティの確保については、サイバーセキュリティ基本法（平成 26 年法律第 104 号）第６条及び第７条の趣旨を踏まえ、電気通信事業者その他の 5G のネットワークの運用者が自ら積極的かつ自主的に確保すべきものであり、国としてはこのような自主的な取組を支援するような振興的措置を取ることが望ましい。その上で、特に必要な部分については、法令等に基づき規律が課されることが望ましい。

この点、5G の安全性・信頼性を確保しつつその適切な開発供給及び導入を促進するため、全国 5G 及びローカル 5G の導入事業者に対する税制優遇措置や導入事業者及び開発供給事業者に対する金融支援の実施を盛り込んだ「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」が 2020 年（令和２年）５月に成立したところであり、今後、税制優遇及び金融支援措置が積極的に活用されるよう、その早期施行に向け必要な準備を進めることが必要である。

また、5G のセキュリティを確保するため、全国 5G では、携帯電話事業者に対して第５世代移動通信システムの導入のための特定基地局の開設計画の認定の際に、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いるほか、ローカル 5G では、ローカル 5G 導入に関するガイドラインにおいて、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じる旨を明記するとともに、ローカル 5G の免許時の条件として付すこととしている。

このような産業振興的な枠組み、制度的な枠組みの両面から 5G のセキュリティ確保に向けた取組を進める必要がある。

（３）クラウドサービスのセキュリティ対策

ICT の利活用が社会全体として進展する中、インターネット上のリソースを臨機応変に活用するクラウドサービスは、サービスアプリケーションから多様な

IoT プラットフォームまで、様々な ICT ソリューションを支えており、データの利活用・管理における中核のサービスとなりつつある。また、COVID-19 への対応において、クラウド型の Web 会議システムなどの利用も増大しており、今後社会・経済の様々な分野で利用が加速していくことが想定される。

その中で、我が国の政府においても「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（平成 30 年６月７日 CIO 連絡会議決定）を定め、情報システム調達に際しては、コスト削減や柔軟なリソースの増減等の観点から、クラウドサービスの利用を第一候補として検討を行う旨の方向性が示されているところである。

このような状況を踏まえ、現在、政府機関等の情報システムにおけるクラウドサービスの調達に関しては、「政府情報システムのためのセキュリティ評価制度」（通称 ISMAP: Information system Security Management and Assessment Program）について、2020 年度（令和２年度）中に各省庁において制度の利用開始ができるよう立ち上げが進められているが、本取組を着実に実施する必要がある。

また、クラウドサービスのセキュリティについては、既存の様々な認証・認定制度が存在し、サービスにおける対策の可視化の取組がなされており、クラウドが普及していく時代においては、利用者・調達者の側においてこのような既存の認証・認定制度を参照していくことが期待される。他方、クラウドサービスを活用した情報システムについては、クラウドサービスの提供者と利用者・調達者による「責任共有モデル」が採用されることが一般的であることを念頭に、利用者・調達者が自ら採るべき対策についても認識をした上でサービス利用を行う必要があることから、利用者・調達者の側のリテラシー向上に向けた取組を進めることが重要である。

なお、付言すれば、クラウドサービスの利用やテレワークの普及の進展などを念頭に、それぞれの組織においてオフィスの内外をまたがるアクセスが増加し、境界の概念がなくなっていくなど、ネットワーク維持・管理の在り方や対応するセキュリティ対策の在り方も今後徐々に変化していくことが想定される。このような新たな時代のネットワークセキュリティの在り方について、継続的に調査・検討し、必要に応じて政策に反映していくことが重要である。

（４）スマートシティのセキュリティ対策

スマートシティは、先進的技術の活用により、都市や地域の機能やサービスを効率化・高度化し、各種の課題の解決を図るとともに、快適性や利便性を含めた

新たな価値を創出する取組であり、「Society 5.0の先行実現の場」[17]である。

この点、総務省では、都市や地域が抱える様々な課題の解決や地域活性化・地方創生を目的として、ICTを活用した分野横断的なスマートシティ型の街づくりに取り組む「データ利活用型スマートシティ推進事業」を2017年度（平成29年度）から実施しているところである。なお、今後は政府のスマートシティに係る各事業の連携や分野間のデータ連携等を協力推進していくため、関係本部・省庁で連携[18]していくこととされている。

他方、スマートシティでは、インターネットに接続するセンサー・カメラ等が散在し、多様なデータが流通することが想定され、常にサイバー攻撃の脅威にさらされるおそれがあるため、IoT機器の監視を行うセキュアゲートウェイの在り方についての検討が重要である。また、様々なデータが共通プラットフォーム上で流通する中で、データの真正性の確保や適切なデータ流通の管理の仕組みの構築が必要となることが想定される。また、スマートシティには多様な主体が関わることが想定されるため、システム全体としてのセキュリティのPDCAサイクルや、平時・有事のセキュリティ確保の体制としてのSOC又はCSIRTの在り方についても検討が必要となることが想定される。

以上を踏まえ、スマートシティのセキュリティ確保の在り方について、多様な関係者間で一定の共通認識の醸成が必要である。具体的には、スマートシティ官民連携プラットフォーム[19]のスマートシティセキュリティ・セーフティ分科会[20]

---

[17] スマートシティについては、「統合イノベーション戦略2019」（令和元年６月21日閣議決定）において、「Society 5.0の先行実現の場としてのスマートシティの拡大・発展を図っていく必要がある」されている。

[18] スマートシティについては、「統合イノベーション戦略2019」において、「各府省は、共通の基本方針を踏まえて事業を実施するとともに、アーキテクチャ構築の検討会議（以下「検討会議」という。）を設置し、同会議での検討結果を各府省の具体の事業に反映させていく旨を合意したところであり、今後は、本合意に沿って、各府省の事業連携や分野間のデータ連携等を強力に推進」していくこととされている。

[19] 「統合イノベーション戦略2019」等において、スマートシティの事業推進に当たり、官民の連携プラットフォームの構築を行うことが明記されたことを受け、内閣府、総務省、経済産業省、国土交通省が事務局となり、スマートシティの取組を官民連携で加速するため、企業、大学・研究機関、地方公共団体、関係府省等を会員とする「スマートシティ官民連携プラットフォーム」を設立。会員サポートとして、①事業支援、②分科会、③マッチング支援、④普及促進活動等を実施。2020年（令和２年）４月末時点で598団体（オブザーバを含む）が参加。

[20] スマートシティ官民連携プラットフォームの下部の分科会の１つで、総務省、株式会社ラック、一般社団法人オープンガバメント・コンソーシアムが事務局となり、スマートシティにおいて実現される様々な機能・サービス・機器などについて、セキュリティやセーフティを確保

など、官民の検討の場において、スマートシティのセキュリティ確保の観点から留意すべき要件やチェックすべき事項などについて検討を行い、明確化を図ることが必要である。またその際は、スマートシティを推進する取組との連携を図り、セキュリティ対策の実装を促進していくことが重要である。

なお、スマートシティは、地域における IoT や 5G、クラウドサービスのユースケースとしての側面もあり、（１）の IoT のセキュリティ対策や、（２）の 5G のセキュリティ対策、（３）のクラウドサービスのセキュリティ対策の取組等の連携を図ることが重要であるほか、（８）の地域の情報通信サービスのセキュリティの確保やⅣ－（２）－⑤の地域のセキュリティ人材育成の取組など、地域のセキュリティ強化の取組と連携を図ることも重要である。

また、スマートシティの取組は国際的にも EU の研究開発プロジェクト Horizon 2020 や NIST が主導する GCTC（Global City Teams Challenge）プロジェクトでも展開されており、総務省では EU と連携した、スマートシティ分野のセキュリティ・プライバシ保護を含む日 EU 共同研究（Fed4IoT）[21]を 2018 年（平成 30 年）から実施している。

そのため、上述の成果については諸外国と連携の上、国際標準化や必要に応じた国際的な議論の場への提案を検討するなど、諸外国との調和を意識して展開を図ることが重要である。

（５）トラストサービスの制度化と普及促進

Society5.0 の実現に向けて、サイバー空間の自由で安心・安全なデータの流通を実現するためには、データの信頼性を確保する仕組みとして、データの改ざんや送信元のなりすまし等を防止するトラストサービスが不可欠である。

そのため、総務省では、「プラットフォームサービスに関する研究会」の下に「トラストサービス検討ワーキンググループ」を開催し、2019 年（平成 31 年）１月から、トラストサービスに関する現状や課題について検討を実施し、2020 年（令和２年）２月に同研究会最終報告書の取りまとめがなされ、一定のサービス提供の実態又は具体的なニーズの見込みがあり、利用者がより安心して利用できる環境の構築に向けた課題が顕在化しているタイムスタンプ、ｅシール及びリモート署名について、以下のとおり、今後の取組の方向性が示された。

１）タイムスタンプについては、技術やサービス内容が確立されており、一般

しつつ、実装していくための方策について検討するために立ち上げたもの。

[21] スマートシティアプリケーションに拡張性と相互運用性をもたらす仮想 IoT-クラウド連携基盤の研究開発

財団法人日本データ通信協会による民間の認定制度が 14 年間運用されてきたが、国の信頼性の裏付けがないことや、国際的な通用性への懸念が更なる普及を妨げている一因となっていることを踏まえ、国が信頼の置けるタイムスタンプサービス・事業者を認定する制度を創設することが適当である。

２）ｅシールについては、新しいサービスであり、その導入促進のためには利用者が安心して利用するため、信頼のおけるサービス・事業者に求められる技術上・運用上の基準の提示や、それを満たすサービス・事業者について利用者に情報提供する仕組みが重要である一方、サービス内容や提供するための技術などが確立されていないことから、国が一定程度関与しつつ、信頼の置けるサービス・事業者に求められる技術上・運用上の基準を策定し、これに基づく民間の認定制度を創設することが適当である。

３）今後利用拡大が期待されるリモート署名については、ガイドラインが民間団体において策定されたことを踏まえ、利用者によるリモート署名の円滑な利用を図るため、当該民間のガイドラインの策定・公表や自主的な適合性評価の仕組みの整備を受け、主務省（総務省、経済産業省、法務省）において、当該ガイドライン等の精査や当該ガイドライン及び適合性評価の仕組みの運用状況のモニタリングなどの取組を進めながら、リモート署名の電子署名法上の位置づけについて速やかに明確化することが適当である。

これを受け、上述の方向性に合わせ、トラストサービスの制度的な枠組みの形成に向けた取組を一層加速する必要がある。

- タイムスタンプについて、2020 年度（令和２年度）中に国による認定制度の整備を行う。
- ｅシールについて、国が関与して策定した基準に基づく民間の認定制度の創設に向け、2021 年度（令和３年度）までに認定基準等の整備を行う。
- リモート署名について、技術や運用の動向も踏まえ検討を行い、2021 年度（令和３年度）までに電子署名法上の位置づけを明確化する。

また、COVID-19 への対応において、請求書や押印手続、印刷など紙の書類の処理の必要性がテレワークの実施の阻害要因になっているケースがあり、企業間の様々なやり取りの電子化やオンラインでの完結が求められる中、トラストサービスはその実現に必要不可欠なものであるため、可能な限り前倒しを検討することが求められる。

なお、これら制度の具体化と併せて、実際の利用の場面でトラストサービスの

各種業法等における位置づけを明確化していくことが重要であることを踏まえ、各種法令・ガイドライン等との関係で有効な手段として認められるトラストサービスの要件を明示するよう、法令・制度を所管する関係府省庁への働きかけを行っていくことも重要である。

（６）無線 LAN のセキュリティ対策

無線 LAN は通信料等を気にすることなく高速な通信が利用可能な手段として家庭をはじめとして幅広く使われているほか、外出先で利用可能な公衆無線 LAN 環境についても、観光や防災などの観点から有効であることから官民を問わずその整備が進んでいる。一方で無線 LAN の利用に当たっては、適切なセキュリティ対策をとらなければ、無線 LAN 機器を踏み台にした攻撃や情報窃取が行われるおそれがある。

総務省においては、無線 LAN のセキュリティ対策に関して、利用者・提供者のそれぞれに向けたガイドラインを策定し、緊急提言を踏まえ、2020 年（令和２年）５月に改定を行っている。東京大会に向けて多くの利用が見込まれるホテル・観光機関や病院、そして ICT の利活用が急速に進んでいる学校等に対してガイドラインの内容を周知していくなど、安全・安心に無線 LAN を利用できる環境の整備に向けて、利用者・提供者の双方に対するセキュリティ対策に関する周知啓発を図っていく必要がある。

（７）重要インフラとしての情報通信分野等のセキュリティ対策

情報通信分野及び地方公共団体分野は、「重要インフラの情報セキュリティに係る第４次行動計画」（平成 29 年４月 18 日サイバーセキュリティ戦略本部決定 令和２年１月 30 日サイバーセキュリティ戦略本部最終改定。以下「第４次行動計画」という。）において、特にその機能が停止、又は利用不可能となった場合に国民生活・社会経済活動に多大なる影響を及ぼしかねないものとして重要インフラに指定されている。

第４次行動計画を踏まえ、重要インフラ各分野の横断的な指針として「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」（平成 30 年４月４日サイバーセキュリティ戦略本部決定　令和元年５月 23 日サイバーセキュリティ戦略本部改定）が定められており、同指針を踏まえ、官民で連携して、安全基準等の整備及び浸透に向けた取組が進められている。

この点、まず情報通信分野のうち、電気通信分野においては、事故再発防止のため、「電気通信事故検証会議」等の枠組みを通じ、電気通信事故の分析・検証等を行うとともに、「情報通信ネットワーク・安全信頼性基準（昭和 62 年郵政省

告示第 73 号)」等の見直しの必要性について検討を行っている。

さらに、情報通信審議会情報通信技術分科会 IP ネットワーク設備委員会においては、2019 年（令和元年）６月から 2020 年（令和２年）３月にかけて「IoT の普及に対応した電気通信設備に係る技術的条件」について検討が行われた。具体的には、通信ネットワークの本格的なソフトウェア化・仮想化の進展に対応した技術基準等の在り方や災害に強い通信インフラの維持・管理方策について検討が行われ、その検討結果については、2020 年（令和２年）３月に情報通信審議会から一部答申を受けたところである。

当該答申を踏まえ、総務省においては、令和元年房総半島台風等による通信被害を踏まえ市町村役場をカバーする固定通信局舎及び携帯電話基地局について 24 時間以上の停電を考慮した予備電源を確保することなど電気通信事業者における停電対策の強化等に関する制度整備を行うため、情報通信ネットワーク安全・信頼性基準の改正に向けた手続を行っており、2020 年（令和２年）６月末までの制度化を予定している。今後は、改正後の制度を着実に運用していくとともに、引き続き委員会を開催し、電気通信設備の安全・信頼性確保に向け必要な検討が進められていくことが期待される。

また、2018 年度（平成 30 年度）には、前述の（１）－③のとおり、「送信型対電気通信設備サイバー攻撃」に関する送信元情報の共有や C&C サーバの調査研究等を行う第三者機関として認定協会を総務大臣が認定する制度を創設した。さらに本制度改正に関連して、「送信型対電気通信設備サイバー攻撃」が原因である電気通信事故の発生状況を把握する観点から当該事故の報告を求めるため、電気通信事業報告規則（昭和 63 年郵政省令第 46 号）を改正する制度整備が行われている。

今後は、当該事故に関する情報を含むサイバー攻撃を起因とする電気通信事故に関する情報、それらの情報を踏まえた再発防止に向けた教訓等及び情報通信ネットワーク安全・信頼性基準等に関する内閣官房内閣サイバーセキュリティセンターや電気通信事業者との間の情報共有の在り方等、情報通信ネットワークの安全・信頼性対策とサイバーセキュリティ対策との更なる連携強化を図ることが期待される。

加えて、放送分野においては、2020 年（令和２年）１月に公表した緊急提言において、「放送分野において、放送設備のサイバーセキュリティ確保に関する省令改正を速やかに実施することが必要」としているところであるが、2019 年（令和元年）７月より情報通信審議会情報通信技術分科会放送システム委員会で放送設備のサイバーセキュリティ確保に関する検討を開始し、同年 12 月に情

報通信審議会から答申を受けたところである。

当該答申を踏まえ、放送設備等のサイバーセキュリティ確保のため、放送法施行規則（昭和 25 年電波監理委員会規則第 10 号）等を改正する制度整備を実施し、2020 年（令和２年）３月に施行されたところである[22]。本制度改正によって、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としており、今後は改正した制度を着実に運用していく必要がある。

また、地方公共団体分野においては、2015 年（平成 27 年）のいわゆる「三層の対策」により、インシデント数の大幅な減少を実現するなど、短期間で自治体の情報セキュリティ対策の抜本的強化したところであるが、2019 年（令和元年）12 月より、三層の対策の効果や課題、新たな時代の要請を踏まえ、効率性・利便性を向上させた新たな自治体情報セキュリティ対策について検討を開始したところである。

なお、緊急提言においては、情報通信分野の取組に関し、サイバーセキュリティ対策や事故報告についての法令への位置づけ、分野ごとの所管省庁や業界団体によるガイドラインや基準の策定を通じてサイバーセキュリティ対策を実効的に進めていく取組について、あらゆる機会を通じて周知し、対応の強化を呼びかけていくことが必要としたところであり、今後も安全基準等の整備及び浸透の取組などを積極的に推進していくことが期待される。

（８）地域の情報通信サービスのセキュリティの確保

我が国の情報通信サービス・ネットワークの安全性や信頼性の確保の観点からは、全国規模や首都圏でサービスを提供している事業者だけでなく、地域単位

---

[22] 具体的には、放送法施行規則において、放送設備等に対し、サイバーセキュリティの確保のために必要な措置が講じられていなければならない旨を新たに規定するとともに、放送法関係審査基準（平成 23 年総務省訓令第 30 号）において、以下の項目を審査項目として追加する制度改正を実施。

①放送本線系入力となる番組送出設備について、外部ネットワークから隔離するための措置
②放送設備に接続される監視・制御及び保守に使用される回線について、外部ネットワークからの不正接続対策を行うための措置
③設備の導入時及び運用・保守時におけるソフトウェアの点検について、不正プログラムによる被害を防止するため、放送設備のネットワークからの分離・遮断の措置及び不正プログラムの感染防止の措置
④放送設備に対する物理的なアクセス管理について、機密性が適切に配慮させるための措置
⑤放送設備の運用・保守に際して、業務を確実に実施するための組織体制の構築及び業務の実施に係る規程若しくは手順書の整備に関する措置

で情報通信サービスを提供している事業者におけるサイバーセキュリティの確保も重要な課題である。

他方、地域においては、首都圏と比較してサイバーセキュリティに関する情報格差が存在するほか、経営リソースの不足等の理由により、単独で十分なセキュリティ対策を取ることが難しかったり、セキュリティ対策の必要性を認識するに至らなかったりするケースが存在するおそれがある。したがって、地域レベルのセキュリティの質を向上させるためには、関係者間でのセキュリティに関する「共助」の関係が構築されることが望ましい。

このため、地域で情報通信サービスを提供している事業者を含む各種民間企業、行政機関、教育機関、関係団体等が、顔の見える関係の中で、セキュリティについて相互に啓発を行う体制やコミュニティを構築していくことが重要である。その上で、このような体制等において、イベント等の継続開催による地域のセキュリティ意識向上・人材育成や、国や専門家を招へいした情報提供が持続的・自発的に実施されることが望ましい。このような関係者間でのセキュリティに関する「共助」の関係を構築されたコミュニティ（以下「地域 SECUNITY」という。）が形成されることで、地域におけるセキュリティ対策の質の向上が持続的に図られることが期待される。

また、このような自律的に活動している「地域 SECUNITY」が発展していく中で、「地域 SECUNITY」同士が地域の枠を越えて情報共有や連携を行うことで、コミュニティとしての活動の活性化や新たな価値創造につながることが期待される。また、将来的には、各地域におけるセキュリティのニーズとシーズのビジネスマッチング、共同研究による地域発のセキュリティソリューションの開発など地域一体となった課題解決がなされていくことも期待される。

そのため、まずは、「地域 SECUNITY」の構築に向け、関係府省庁と連携し、各地において地域単位でのコミュニティ構築を支援することが必要である。その際、国においては、地域の自主性を尊重しつつ、例えばコミュニティの成功事例のプロモーションや、セミナー・演習の実施に当たっての専門家の斡旋などの側面支援に注力していくことが重要である。

なお、当該施策の展開に当たっては、（６）の無線 LAN のセキュリティ対策やⅣ－（２）－②の実践的サイバー防御演習（CYDER）の実施、Ⅳ－（２）－⑤の地域のセキュリティ人材育成の取組等との連携を図り、効果的に地域のセキュリティ対策の質の向上を図ることが重要である。

（９）テレワークシステムのセキュリティ対策

テレワークは、時間や場所を有効に活用でき柔軟な働き方を実現するものであるとともに、COVID-19 への対応という観点や、災害発生時も含めた業務継続という観点からも有効かつ重要なものである。中長期的な観点から、我が国においては少子高齢化に伴う生産年齢人口の減少への対処が要請されており、そのためにもテレワークの利活用を検討する必要がある。一方で、テレワークの実施に当たっては、職場環境に閉じた LAN ではなくインターネット経由での業務を前提とする必要があること、また、通常と異なる勤務環境やシステムを利用する場合も多いことから、適切なセキュリティ対策を採ることが必要である。また、企業間において Web 会議システムを利用するケースにおいても同様に適切なセキュリティ対策を採ることが必要である。

このため総務省では、企業等がテレワークを実施する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針として、2018 年（平成 30 年）４月に「テレワークセキュリティガイドライン（第４版）」を作成している。さらに、COVID-19 への対応等のため中小企業等においてもテレワークの導入が拡大する中で、当該ガイドラインをより具体的で分かりやすくした、実践的な内容のチェックリスト等が有用であり、総務省において早期に策定を行う必要がある。企業等においては、このようなガイドラインやチェックリスト等を活用することで、これからテレワーク環境を導入しようとする場合には適切なセキュリティ対策を採り、既にテレワーク環境を導入している場合にはセキュリティ対策の自己点検等を行うことが重要である。

また、COVID-19 への緊急対応のため多くの企業では準備期間が十分とれずにテレワークを導入・導入検討していると想定されるが、特に中小企業等においては十分なセキュリティ知識を有した担当者がいない場合が多いと想定されるため、テレワーク導入時及び導入後においてセキュリティ対策の専門家が相談を受け付ける体制を提供する必要がある。

こうした取組と併せて、中小企業等のテレワークセキュリティに関する実態把握のための調査を行い、実際の業務やシステム構成に応じた活用しやすい取組としていくなど、セキュリティを確保したテレワーク環境を実現するための適切な支援策を講じていく必要がある。

（10）電気通信事業者による高度かつ機動的なサイバー攻撃対策の実現

サイバー攻撃はその定義からして、電気通信事業者のネットワークを経由し、ユーザに対してなされるものであり、サイバー攻撃の検知や防御等に関して電

気通信事業者の果たす役割が大きい。

例えば、これまで IoT 機器のセキュリティ対策については、IoT 機器の技術基準の策定・運用や IoT 機器の利用者向けの注意喚起など、端末側でのセキュリティ対策が中心であったが、今後は、より効率的かつ総合的なセキュリティ対策の実現のため、注意喚起等の取組と併せて、電気通信事業者が、個々の感染端末に指示を出す C&C サーバに直接対処するといった、通信ネットワーク側における積極的なサイバー攻撃対策を推進することが期待される。

このため、IoT のセキュリティ対策を含め、様々な分野において、海外における動向（制度、実施状況等）も参考としながら、ユーザ側で運用している情報通信機器や情報システムのセキュリティ対策と連動する形で、インターネット上で ISP が管理する情報通信ネットワークにおいても高度かつ機動的な対処を実現するための方策の検討が必要である。

具体的には、電気通信事業者が自ら C&C サーバを検知し、サイバー攻撃の指令通信の遮断等の対策を実施できるような環境整備に向け、通信の秘密に配慮した適切な対応を電気通信事業者が円滑に行うことが求められるところ、制度的な観点から対策の検討を行うことが重要である。なお、中長期的な課題として、通信の秘密の保護を図りつつ、より迅速なセキュリティ対策を実現するために、必要に応じ新たな視点からも検討を行うことが適当と考えられる。

また、技術的な課題解決のための取組も重要である。例えば、利用者の PC や IoT 機器などがマルウェアに感染した場合に当該 PC や機器に対して指令を与える C&C サーバの探索については、通信の秘密等の制度的観点に配慮しつつ、AI を活用して検知の高度化を図るなど、新技術を活用した対策の高度化を促進する必要がある。

さらに、これらの取組について、実際に通信ネットワークを活用して情報システムを運用しているユーザ企業向けの対策との連携を含め、関係府省庁とも連携して取組を推進していくことが重要である。

Ⅳ　横断的施策

（１）研究開発の推進

サイバー空間における攻撃の態様は常に変化しており、インターネットをはじめとするネットワークに接続される機器の更なる増加に伴い、サイバー攻撃の対象が拡大するとともに、AI の進展やサプライチェーンの複雑化等により、攻撃手法・能力が巧妙化・大規模化していくことが想定される。そのため、これに対応するには、政府が支援する産学官連携による研究開発の成果を即座に反映した最新のサイバーセキュリティ対策を実施していくことが有効である。

この点、サイバーセキュリティに関する研究開発は重要な政策課題とされており、サイバーセキュリティ戦略において、高いレベルのセキュリティ品質を備えた安全・安心な製品やサービスを提供していくことは、我が国の産業の成長、国際競争力の向上を目指していく上で不可欠である旨や、実践的なサイバーセキュリティの研究開発が必要である旨が示されている。

また、同戦略期間中における政府の取組の具体化及び強化を図る目的で策定された「サイバーセキュリティ研究・技術開発取組方針」（令和元年５月 23 日サイバーセキュリティ戦略本部報告）によれば、我が国のサイバーセキュリティの研究・技術開発において取り組むべき課題として、「サプライチェーンリスクの増大」、「サイバーセキュリティ自給率の低迷」、「研究・技術開発に資するデータの活用」、「先端技術開発に伴う新たなリスクの出現」、「産学官連携強化の必要」、「国際標準化強化の必要」の６点が指摘されているところである。

したがって、総務省においても、上述の課題認識の下、NICT や民間企業等と連携しつつ、研究開発の成果が民間企業等への技術移転によって広く普及し、社会実装が進むことを視野に入れながら、サイバーセキュリティ対策に係る研究開発を効果的に推進する必要がある。特に、膨大化するサイバー攻撃に関する情報を高効率かつ有効に活用するためのサイバー攻撃観測技術等の高度化やサイバーセキュリティ情報を国内で収集・蓄積（生成）・提供するためのシステム基盤の構築、量子計算機時代等を見据えた安全に利用できる暗号基盤技術の確立、5G 等の新たなネットワーク環境の進展を踏まえたセキュリティ検証技術の確立等について重点的に取り組む必要がある。

なお、サイバーセキュリティが社会経済活動のインフラとなりつつある現状を考慮し、研究開発を進めるに際して、サイバーセキュリティ技術の研究者だけでなく、法制度や AI 等の専門家も取り込む形で、社会システム全体の中での位置づけを踏まえた実証等の取組を進めていく必要がある。また、国際標準化や国

際連携についても積極的に進めることが求められる。

① サイバーセキュリティ統合知的基盤の構築

我が国のサイバーセキュリティは、海外製品や海外サービスへの依存度が高い状況にある。そのため、国内のデータが海外に流出して分析される一方、我が国は海外で生成された脅威情報を高額で購入することでセキュリティ対策を講じてきた状況である。この状況を別の側面から見ると、実データの不足が、良質な国産のセキュリティ技術の創出・普及を阻害し、それが更に実データの不足をもたらすという「データ負けのスパイラル」に陥っていることが考えられる。

このため、我が国の企業の国際競争力強化はもちろんのこと、グローバルレベルの情報共有へのより一層の貢献や国際的に通用するエンジニアの効果的な育成、政府機関や重要インフラ事業者等のサービス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の回避・脱却などの観点から、コア技術の開発・運用を中心に、国産技術・産業の育成を進めていくことが重要であり、我が国において、以下の取組を進める必要がある。なお、その際、我が国において必要なサイバーセキュリティ関連情報の収集・分析等を実施できるように仕組みを整えながらも、グローバルな協力・連携も含め、国際的なサイバーセキュリティの向上に貢献するという視点が重要である。

１）実データを大規模に集約・蓄積する仕組み

具体的には産学官が連携して、各種公的機関等が観測した情報やインターネット上の公開情報（OSINT）を大規模に集約して蓄積する仕組みが考えられる。

２）実データを定常的・組織的に分析する仕組み

具体的には攻撃ツールや手法を並列かつリアルタイムに観測・解析する環境を構築するとともに、本環境を活用した高度解析者の結集・育成を行う仕組みが考えられる。

３）実データで国産製品を運用・検証する仕組み

具体的には国産製品のプロトタイプ群を長期運用・機能検証できる環境を構築するとともに、本環境を活用したSOC人材の育成を行う仕組みが考えられる。

４）実データから脅威情報を生成・共有する仕組み

具体的には１）～３）で収集した実データを用い、AI を駆使した大規模横断分析を行い、日本独自の脅威情報を生成し、信頼性の高い、説明可能かつ即時的なセキュリティ情報を関連機関で共有することが考えられる。

以上の取組を自律的に実施する仕組み・体制を構築し、国内でサイバーセキュリティ情報を収集・蓄積（生成）・提供する環境が必要である。

② 基礎的・基盤的な研究開発等の推進

これまで NICT では、中長期計画に基づき、サイバーセキュリティ分野の基礎的・基盤的な研究開発等を実施しているところである。

例えば、巧妙化・複雑化するサイバー攻撃や標的型攻撃に対応するため、模擬環境や模擬情報を用いて攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握することを可能にするサイバー攻撃誘引基盤「STARDUST」（スターダスト）を活用し、攻撃活動の早期収集や未知の標的型攻撃等を迅速に検知する技術等の研究開発を行っている。

また、暗号技術分野においては、現在利用されている暗号技術及び今後の利用が想定される暗号技術の安全性評価、量子コンピュータ時代に向けた機能的な公開鍵暗号の研究開発、プライバシーの保護に資する暗号化したままデータを解析する技術等の研究開発が行われている。

その中で、インターネット上で起こる大規模攻撃への迅速な対応を目指したサイバー攻撃観測・分析・対策システムを用いて、ダークネットや各種ハニーポットによるサイバー攻撃の大規模観測及びその原因（マルウェア）等の分析を実施する「NICTER」プロジェクトが実施されている。同プロジェクトで得られるマルウェアに感染している機器に係る情報を、電気通信事業者に提供することで、Ⅲ－（１）－②の脆弱性等を有する IoT 機器の調査及び注意喚起と連携し、IoT 機器のセキュリティ対策を推進することが必要である。

このような基礎的・基盤的な研究開発については、その研究開発の成果が民間企業等への技術移転によって広く普及し、社会実装が進むことが求められることから、引き続き、社会全体のサイバーセキュリティ対策の質の向上に資するよう、基礎的・基盤的な研究開発等を推進することが必要である。

③ IoT 機器のセキュリティ対策技術の研究開発の推進

IoT 機器を狙ったサイバー攻撃は依然として多く、脆弱な IoT 機器のセキュリティ対策は喫緊の課題である。

IoT 機器の対策のためには、インターネットに接続している IoT 機器に対して広域的なネットワークスキャンを実施する必要がある。一方で、IoT 機器が増大している中で広域ネットワークスキャンを行うと、それに係る通信量も膨大になるおそれがあることから、通信量の抑制と精度の向上を両立するような効率的な広域ネットワークスキャンの実現が必要となる。

そのため、総務省では、通信量の抑制と精度の向上を実現する効率的な広域ネットワークスキャンの実現を目的として、2018 年度（平成 30 年度）～2020 年度（令和２年度）までの３年間を実施期間とし、「周波数有効利用のための IoT ワイヤレス高効率広域ネットワークスキャン技術の研究開発」に取り組むこととしている。

本研究開発を通じ、周波数の利用状況の自動推定による広域ネットワークスキャン技術の開発と広域ネットワークスキャンの無線通信量軽減技術の開発に取り組む必要がある。

また、本研究開発の成果については、Ⅲ－（１）－②の IoT 機器の脆弱性調査に活用し、当該調査の効率化を図ることが重要である。

さらに、増加し続ける IoT マルウェアを無害化・無機能化する技術を確立すべく、2020 年度（令和２年度）～2022 年度（令和４年度）までの３年間を実施期間とし、「電波の有効利用のための IoT マルウェアの無害化/無機能化技術等に関する研究開発」に取り組むこととしている。

本研究開発を通じ、AI 技術を駆使した IoT マルウェアの挙動検知及び駆除技術、マルウェアに感染した IoT 機器を無害化・無機能化する技術の開発に取り組む必要がある。

④　脆弱性の検証手法等の確立と体制整備【再掲】

5G のネットワークに関しては、仮想化・ソフトウェア化が進むことから、サプライチェーンリスクを含む新たなサイバーセキュリティ上の課題が懸念される。そのため、5G のネットワークやその構成要素及びサービスについて、ソフトウェア・ハードウェアの両面から技術的検証を行うことを通じ、5G のネットワークのセキュリティを確保する仕組みや体制を整備することが必要である。

具体的には、まず、ソフトウェアを中心としたネットワークの脆弱性については、5G の通信インフラとしての機能保証のため、ソフトウェアにより構成される部分を含め、ネットワーク全体のセキュリティを確保する必要がある。

そのため、5G の仮想環境を構築し、(a)オープンソースソフトウェア等の解析、(b)多種多様なパターンのデータ入力による異常動作確認（ファジング）、(c)エシカルハッカーによる脆弱性調査・脅威分析を実施し、対策を検討することが必要である。

一方、ハードウェアの脆弱性については、5G 等のネットワークを構成するハードウェア上に故意に組み込まれた不正なチップによって生じるセキュリティ上の課題に対応するため、AI を活用し(a)回路情報から不正に改変された回路を検知する技術や、(b)電子機器外部で観測される情報から不正動作を検知する技術を開発し、対策を検証することが必要である。

また、上記の検証結果を踏まえつつ、5G 等のネットワーク上での運用面の課題等についても検討する必要がある。

その上で、技術移転などを含めて前述のような脆弱性検出技術の成果を活用し、関連する脅威の分析の視点を踏まえつつ、システムや利用者に対するインパクト分析を実施し、必要なセキュリティ対策を検討することが必要である。また、このような検証・分析の取組において、5G の事業者・運用者やベンダー等が協力して実施する体制を構築することが必要である。

⑤　スマートシティのセキュリティ対策【再掲】

スマートシティは、先進的技術の活用により、都市や地域の機能やサービスを効率化・高度化し、各種の課題の解決を図るとともに、快適性や利便性を含めた新たな価値を創出する取組であり、「Society 5.0 の先行実現の場」である。

この点、総務省では、都市や地域が抱える様々な課題の解決や地域活性化・地方創生を目的として、ICT を活用した分野横断的なスマートシティ型の街づくりに取り組む「データ利活用型スマートシティ推進事業」を 2017 年度（平成 29 年度）から実施しているところである。なお、今後は政府のスマートシティに係る各事業の連携や分野間のデータ連携等を協力推進していくため、関係本部・省庁で連携していくこととされている。

他方、スマートシティでは、インターネットに接続するセンサー・カメラ等が散在し、多様なデータが流通することが想定され、常にサイバー攻撃の脅威にさらされるおそれがあるため、IoT 機器の監視を行うセキュアゲートウェイの在り方についての検討が重要である。また、様々なデータが共通プラットフォーム上で流通する中で、データの真正性の確保や適切なデータ流通の管理の仕組みの構築が必要となることが想定される。また、スマートシティには多様

な主体が関わることが想定されるため、システム全体としてのセキュリティのPDCAサイクルや、平時・有事のセキュリティ確保の体制としてのSOC又はCSIRTの在り方についても検討が必要となることが想定される。

以上を踏まえ、スマートシティのセキュリティ確保の在り方について、多様な関係者間で一定の共通認識の醸成が必要である。具体的には、スマートシティ官民連携プラットフォームのスマートシティセキュリティ・セーフティ分科会など、官民の検討の場において、スマートシティのセキュリティ確保の観点から留意すべき要件やチェックすべき事項などについて検討を行い、明確化を図ることが必要である。またその際は、スマートシティを推進する取組との連携を図り、セキュリティ対策の実装を促進していくことが重要である。

なお、スマートシティは、地域における IoT や 5G、クラウドサービスのユースケースとしての側面もあり、Ⅲ－（１）の IoT のセキュリティ対策や、Ⅲ－（２）の 5G のセキュリティ対策、Ⅲ－（３）のクラウドサービスのセキュリティ対策の取組等の連携を図ることが重要であるほか、Ⅲ－（８）の地域の情報通信サービスのセキュリティの確保や（２）－⑤の地域のセキュリティ人材育成の取組など、地域のセキュリティ強化の取組と連携を図ることも重要である。

また、スマートシティの取組は国際的にも EU の研究開発プロジェクト Horizon 2020 や NIST が主導する GCTC（Global City Teams Challenge）プロジェクトでも展開されており、総務省では EU と連携した、スマートシティ分野のセキュリティ・プライバシ保護を含む日 EU 共同研究（Fed4IoT[23]）を 2018 年（平成 30 年）から実施している。

そのため、上述の成果については諸外国と連携の上、国際標準化や必要に応じた国際的な議論の場への提案を検討するなど、諸外国との調和を意識して展開を図ることが重要である。

⑥　衛星通信におけるセキュリティ技術の研究開発

近年、世界的な宇宙分野における人工衛星等の産業利用に向けた活動が活発化しており、商社や自動車製造など、これまで宇宙ビジネスに関わったことがない非宇宙系であった業界がその動きを牽引している。また、衛星コンステレーションによるグローバルな地球観測や衛星通信網の構築に関する計画が進

[23] スマートシティアプリケーションに拡張性と相互運用性をもたらす仮想 IoT-クラウド連携基盤の研究開発（Fed4IoT）

められており、今後一層の衛星利用の需要拡大が見込まれる状況にある。

一方、衛星通信に対する第三者による通信内容の盗聴や改ざん、制御の乗っ取りといったサイバー攻撃が脅威となりつつあり、より一層の衛星通信のセキュリティ強化が求められる。

そのため、総務省では、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、2018 年度（平成 30 年度）から５年間の研究開発期間で「衛星通信における量子暗号技術の研究開発」に取り組んでおり、引き続き、本研究開発を継続して実施する必要がある。

⑦　量子コンピュータ時代に向けた暗号の在り方の検討

総務省及び経済産業省は共同で、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 CRYPTREC[24]を実施している。この中で、NICT は、現在利用されている暗号技術及び今後の利用が想定される暗号技術の安全性評価等の役割を担っており、2022 年度（令和４年度）末を目途とする電子政府推奨暗号リスト（CRYPTREC 暗号リスト）の改定の検討においても積極的にその役割を果たしていく必要がある。

また、今後、大規模な量子コンピュータの実用化により、現在の公開鍵暗号（RSA 暗号や楕円曲線暗号）が将来的に解読されるおそれがある[25]こと等を踏まえ、2019 年度（令和元年度）から CRYPTREC に「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」を設置し、量子コンピュータ時代の推奨暗号の在り方について検討を実施している。2019 年度（令和元年度）の検討においては、CRYPTREC 暗号リストとは別に「耐量子計算機暗号（PQC）」に関するガイドラインを作成することが適当とされているほか、今後利用が拡大すると想定される IoT 機器等に用いられる「軽量暗号」や、暗号状態で情報処理が可能な「高機能暗号」についてもガイドラインを作成することが適当とされたところである。

総務省等においては、量子コンピュータの開発状況や耐量子計算機暗号（PQC）

[24] Cryptography Research and Evaluation Committees の略。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。

[25] 現在の量子コンピュータによる暗号技術の安全性への影響については、CRYPTREC 暗号技術評価委員会が 2020 年（令和２年）２月 17 日に、現在の量子コンピュータの開発状況を踏まえると、暗号解読には規模の拡大だけでなく量子誤り訂正などの実現が必要であることから、現行の暗号技術が近い将来に危殆化する可能性は低い旨を公表している。

の標準化状況のフォロー等を行うため、引き続き同タスクフォースでの検討を継続するとともに、CRYPTREC 暗号リストの改定と並行して耐量子計算機暗号等に関するガイドラインの検討を行っていくことが重要である。

⑧ IoT 社会に対応したサイバー・フィジカル・セキュリティ対策

SIP の第２期（2018 年度（平成 30 年度）～2022 年度（令和４年度））では、新たな研究課題として「IoT 社会に対応したサイバー・フィジカル・セキュリティ」を設定し、内閣府、経済産業省等と連携して取組を開始している。

本課題では、IoT 機器のセキュリティを保証する技術、サプライチェーンの分野毎の要件を明確にしたうえでトラストリストを構築・確認する技術、業務データを安全に流通させるためのトレーサビリティ確保技術、サイバー・フィジカル空間を跨った不正なデータを検知・防御する技術等の開発に取り組んでいる。

そのため、上記の研究開発を本格化するとともに、製造・ビル等の分野における実証実験を開始し、本取組を着実に進めることが重要である。

（２）人材育成・普及啓発の推進

サイバーセキュリティ人材の育成は重要な政策課題とされており、サイバーセキュリティ戦略においては、組織における経営層、戦略マネジメント層、実務者層・技術者層といった各人材層の育成・確保や、若年層における教育の充実、中小企業関係の取組等について、具体的な方向性が示されているところである。

これまで、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、実務者層・技術者層及び若年層を対象とした次の人材育成施策を実施しており、引き続き取り組んでいく必要がある。

１） 国の機関、地方公共団体、重要インフラ事業者等を対象とした実践的サイバー防御演習（CYDER）
２） 東京大会の適切な運営に向けたセキュリティ人材の育成（サイバーコロッセオ）
３） 若手セキュリティイノベーターの育成（SecHack365）

また、これらの取組に加え、組織の戦略マネジメント層や ICT 環境構築技術者・開発者等も含む人材育成を産学官が連携して行うための仕組みや、地域におけるセキュリティ能力向上のための人材育成の仕組みについても検討を進める必要がある。

① 人材育成オープンプラットフォームの構築

②の実践的サイバー防御演習（CYDER）の実施等を通じた人材育成を行っているものの、我が国全体としてはサイバーセキュリティ人材のニーズはあるが育成が不十分な状況である。特に、戦略を立ててシステムベンダと共働しつつ組織のセキュリティ対策を先導できる人材が不足しているほか、環境構築技術者・開発者層のセキュリティ知識の不足により、本来防げるはずのセキュリティインシデントが発生している。

このような人材育成を全て国で実施することは困難であるため、特に民間事業者において大学等の教育機関を巻き込みながら自立的に育成を行うことが求められるが、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。また、このような不十分な国内基盤を背景として、既存の民間演習事業においても、海外の演習教材に依存し、日本特有の事例が反映できない状況である。

こうした課題に対応するため、サイバーセキュリティの人材育成に関し、演習の実施に関する様々な要素（データセット、教材、演習用ミドルウェア、計算機リソースなど）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や、産学官の連携によって当該プラットフォームを積極的に活用するためのコミュニティの支援が必要である。

② 実践的サイバー防御演習（CYDER）の実施

総務省は NICT を通じ、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[26]、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）を実施している。また、CYDER で使用する演習シナリオについては、NICT の有する技術的知見を活用し、サイバー攻撃の傾向を分析し、現実のサイバー攻撃事例を再現した最新のものを提供している。

サイバー攻撃は年々増加していることから、社会全体としてサイバーセキュリティ対応力を強化することは急務であり、実際のインシデント発生時に対応を行う情報システム担当者等に対する人材育成の取組は特に重要である。防災訓練と同様に定期的に演習を経験することで実対応時の能力向上を図るよう、CYDER による人材育成を引き続き実施する必要がある。

[26] 独立行政法人及びサイバーセキュリティ基本法第 13 条に基づく指定法人を含む。

また、地方公共団体には未受講の団体もあり、そのような団体が我が国におけるサイバーセキュリティ対策上の穴とならないよう、2020 年（令和２年）１月に公表した緊急提言を踏まえ、総務省と都道府県が緊密に連携し、都道府県ごとに受講計画を策定するなどの取組により受講の促進を図っていく必要がある。

NICT においても、開催日程や開催場所の工夫などの運営面の継続的見直しによって受講機会を拡大するとともに、地理的な要因等により未受講となっている地方公共団体を主な対象として、オンラインでの受講を可能とする演習環境の整備を早期に実施することが求められる。

③　東京大会に向けたサイバー演習の実施

総務省は NICT を通じ、東京大会の適切な運営の確保を目的として、大会関連組織のセキュリティ担当者等を対象とした、実践的サイバー演習「サイバーコロッセオ」を 2017 年度（平成 29 年度）から実施している。

本演習においては、大規模演習環境を用いて、東京大会の公式サイト、大会運営システム等ネットワーク環境を再現した、演習環境（仮想ネットワーク環境）を構築し、東京 2020 大会時に想定されるサイバー攻撃を擬似的に発生させ、本格的な攻防型演習等を実施している。さらに、実機演習を補完する形で、2018 年度（平成 30 年度）からは講義演習形式によりセキュリティ関係の知識や技能を学ぶコロッセオカレッジを開設している。

2021 年（令和３年）に延期された東京大会の円滑な実施に向け、大会組織委員会と緊密な連携を図りながら、引き続き本取組を着実に実施する必要がある。

④　若手セキュリティ人材の育成の促進

総務省は NICT を通じ、25 歳以下の若手 ICT 人材を対象として、既存ツールを単にユーザとして利用するだけではなく、自ら手を動かしてセキュリティに関わる新たなモノづくりができる人材（セキュリティイノベーター）の育成施策「SecHack365」を 2017 年度（平成 29 年度）から実施している。

この取組は、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ことが特徴である。NICT の有する遠隔開発環境を活用し、年中どこからでも遠隔開発実習が可能であり、こうしたオンライン環境に加え集合研修等を行うことで高度な人材育成を実施している。

我が国のサイバーセキュリティの確保に向け、セキュリティイノベーターの育成を推進するため、引き続き、本取組を進める必要がある。

⑤　地域のセキュリティ人材育成

サイバーセキュリティ人材の育成は重要な政策課題となっているが、特に地域においては人材の確保が一層厳しい状況にある。サイバー攻撃は地理的な距離に関係なく、弱いところがターゲットとなる傾向にあることから、セキュリティ人材の裾野を広げ、地域のセキュリティ人材を底上げすることが必要である。

2019 年度（令和元年度）に実施したモデル事業において、地域の中小企業等の多くは、セキュリティ対策に関する問題意識が強くなく、その必要性をそもそも認識していない場合が多いという結果が判明しており、地域の中小企業等においてサイバーセキュリティに関する気づきを得ていただくための活動が必要である。このような活動を地域において自立的かつ継続的に行うためには、地域のセキュリティリーダー（セキュリティファシリテーター）となる人材の育成や、自らセキュリティに関する問題意識を持って活躍しようとしている人材が必要となることから、総務省においてこうした人材の育成を支援する方法について検討していく必要がある。

また、地域においては、セキュリティに関する雇用の受け皿がないことから、若年層がセキュリティ人材を目指さず、地域におけるセキュリティ人材が更に不足するという悪循環がある。そのため、地域においてセキュリティを地場産業化しようとしている民間企業等と総務省が連携し、民間による雇用の受け皿創出の動きに合わせ、就業の場の確保と就業につながる研修を一体的に行うことを通じて、地域における人材エコシステムの形成を図ることについて、その有効性の検討を行う必要がある。さらに、高等教育機関と連携することにより、高度なセキュリティ人材の輩出や、下請的な業務にとどまらないハイエンドなセキュリティビジネスの地場産業化を通じて、より高次のエコシステムの形成が期待される。

総務省においては、モデル事業の実施等を通じてこれら地域人材の育成に関する取組を引き続き実施し、その成果はモデル事業対象地域以外でも横展開して活用できるように進めていく必要がある。

（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り、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、米国をはじ

めとする G7 各国を中心に、二国間及び多国間の枠組みの中で本分野における情報共有や国際的なルール作り（サイバー空間における国際法の適用関係の明確化や国際規範の具体化）を多様なルートで進めつつ、情報通信サービス・ネットワーク分野の具体的な施策、研究開発、人材育成・普及啓発、情報共有・情報開示の取組などを進めていく必要がある。

2019 年（令和元年）６月に開催された G20 大阪サミットでは、我が国主導の下デジタル経済に関する議論が行われ、データ・フリー・フロー・ウィズ・トラスト（DFFT：信頼性のある自由なデータ流通）の概念が合意された。データの自由な流通を促進するため、サイバーセキュリティをはじめとする課題に対処することが必要であり、我が国はサイバーセキュリティ分野における国際協調に向けて今後も主導的な役割を果たしていくことが求められる。その際、サイバーセキュリティの確保を理由とする情報の自由な流通を阻害する動きに対しては、データの越境流通の円滑化がサイバー空間の健全な発展に不可欠であることを踏まえて対応していく必要がある。

① ASEAN 各国をはじめとするインド太平洋地域等との連携

アジア地域においては引き続き ASEAN 各国との協力関係の強化が必要である。具体的には、日 ASEAN サイバーセキュリティ能力構築センターにおける実践的サイバー防御演習「CYDER」等の実施を通じ、４年間（2018 年（平成 30 年）～2022 年（令和４年））で 650 人程度を目標として ASEAN のセキュリティ人材の育成支援を進める必要がある。

また、日・ASEAN サイバーセキュリティ政策会議、日 ASEAN デジタル大臣会合及び高級実務者会合、ISP を対象とする日 ASEAN 情報セキュリティワークショップ等の定期的な開催により、我が国及び ASEAN におけるサイバーセキュリティの脅威をめぐる状況やサイバーセキュリティ対策に関する情報交換を行うほか、ASEAN 側のニーズを踏まえつつ、ASEAN におけるサイバーセキュリティ強化に向けた施策の導入・促進のための協力を推進することが重要である。

さらに、「ICT 国際競争力強化パッケージ支援事業」等の取組を通じ、我が国における ICT の知見やノウハウを含めた成功事例の海外展開の促進を図る必要がある。

加えて、「自由で開かれたインド太平洋（FOIP）」構想等の政府戦略を踏まえつつ、各国との連携を強化することが重要である。

② 国際的な ISAC 間連携

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（Information Sharing and Analysis Center）において、国際的な ISAC 間等の連携を引き続き促進していく必要がある。

具体的には、2019 年（令和元年）11 月に一般社団法人 ICT-ISAC と米国の IT-ISAC との間でサイバーセキュリティ上の脅威に対する情報共有体制の一層の強化を目的として締結された覚書に基づき、国際連携ワークショップの開催等を通じて、一般社団法人 ICT-ISAC と米国の ICT 分野の ISAC との連携を更に強化し、通信事業者、放送事業者、IoT 機器ベンダー、セキュリティベンダー等が、脅威情報やインシデント情報等を自動的に共有し、サイバーセキュリティ対策に活用することを促進することが重要である。また、こうした取組を国際的に拡大することも重要である。

③　国際標準化の推進

IoT セキュリティに係る国際標準化が ISO/IEC 及び ITU-T で議論されているところであり、関係府省庁の連携において、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。具体的には、2016 年（平成 28 年）７月に IoT 推進コンソーシアムの IoT セキュリティワーキンググループにおいて策定された IoT セキュリティガイドラインを国際標準に反映するなどの取組を進め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、現状を把握しつつ、我が国として注力すべき分野について調査を行う必要がある。

さらに、Ⅲの情報通信サービス・ネットワーク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。

④　サイバー空間における国際ルールを巡る議論への積極的参画

サイバー空間における国際ルール等のあり方については、国連をはじめ、G7 や G20、二国間協議等の政府が主体となる場だけでなく、ISOC（Internet Society）や ICANN（Internet Corporation for Assigned Names and Numbers）、IGF（Internet Governance Forum）等のマルチステークホルダーによる場を含め、様々なチャネルを通じて議論が進められてきている。

狭義のインターネットガバナンスのあり方について、物理的な伝送網の上に構築されたパケット伝送網については、「自律・分散・協調」を基本原則として民間主体のマルチステークホルダーによる運営が行われている。しかし、更にその上位に位置するデータ・情報流通層においては、情報の自由な流通（オープンエコノミーの確保）、個人データの越境流通、国際連携によるサイバーセキュリティの確保、サイバー空間における安全保障の確保などの様々な議論が行われているところであり、こうした議論に我が国として積極的に参画していく必要がある。

その際、サイバー空間におけるルール整備は基本的にリアル空間と同等の規制が適用されるものであり、かつ領域ごとの議論は既存の国際ルールに準拠することを基礎として議論が進められることが期待される。

さらに、NOTICE 等の IoT セキュリティ対策をはじめとしたⅢの情報通信サービス・ネットワーク分野の具体的施策について、相手国の状況に応じて国際連携の場で共有をし、各国の取組につながるよう働きかけるとともに、海外からのフィードバックを得て施策の改善につなげる取組を継続的に進めることが重要である。総務省は、イスラエル・国家サイバー総局との間で 2018 年（平成 30 年）11 月に締結した覚書に基づき人材育成協力を推進しており、引き続きこうした取組を拡大することが重要である。

（４）情報共有・情報開示の促進

ICT の利活用が進展した現在では、サイバー攻撃を行う側が圧倒的に優位な状況にあり、サイバー攻撃を受ける側はサイバーセキュリティを協調領域と捉え、平時・有事において協力をして取り組むことが求められる。

この点で、サイバーセキュリティ基本法の一部を改正する法律（2019 年（平成 31 年）４月施行）によって、新たにサイバーセキュリティ協議会が創設され、官民を含めた多様な主体がサイバーセキュリティに関する情報を迅速に共有することにより、サイバー攻撃による被害を予防し、被害の拡大を防ぐための体制が構築されているところである。さらに、民間の取組としては、サイバー攻撃や事故への事前の対処、及び、障害発生時の事案対処や復旧に関する情報などについて事業者間で共有することを目的とした ISAC がいくつかの業界で立ち上げられており、緊急提言おいて、他の重要インフラ分野等での ISAC の立ち上げの促進や国際間を含む ISAC 間の連携を促進することの必要性について指摘したところである。

以上を踏まえつつ、その他の情報共有体制も含め、脆弱性情報やサイバー攻

撃に関する脅威情報のほか、サイバーセキュリティ対策に関する情報等の共有を促進し、各主体のサイバーセキュリティ対策の質を向上させることが重要である。

また、企業や組織の活動においてICTの利活用が前提となっている現在、サイバーセキュリティリスクの認識やその対策についてステークホルダーに適切な開示を行うことは、ステークホルダーへの説明責任を果たし、円滑な関係を維持する上で重要な取組となっている。

さらに、サイバーセキュリティ対策の情報開示を促進することにより、民間企業の経営層が自社の対策について認識をし、更に他社との比較によって対策の質の向上に取り組むことが期待される。また、社内や取引先・委託先への啓発にも寄与するなど、情報開示は各主体のサイバーセキュリティ対策の質の向上に寄与することも期待される。

① サイバー攻撃に関する電気通信事業者間の情報共有【再掲】

脆弱性を有するIoT機器が踏み台となったことが確認された際、被害の拡大を防止するため、ISPによる、当該ISPの利用者の端末とC&Cサーバの間の通信を遮断するなどの取組が必要である。

この点、総務省では、2018年（平成30年）５月の改正電気通信事業法において、電気通信事業者が「送信型対電気通信設備サイバー攻撃」への対応を共同して行うため、攻撃の送信元情報の共有やC&Cサーバの調査研究等の業務を行う第三者機関（認定協会）を総務大臣が認定する制度を創設し、2019年（平成31年）１月に一般社団法人ICT-ISACが認定されたところである。

今後は認定協会の活動について、マルウェアに感染している可能性の高いIoT端末等やC&Cサーバであると疑われる機器の検知や利用者への注意喚起等の電気通信事業者が行う対策に向け、円滑な実施のための支援を行うなどの取組を促進することが重要である。

また、こうした認定協会の活動や「NOTICE」の実施状況も踏まえ、電気通信事業者等が協力してサイバー攻撃への対処を行う際の基盤となる効果的な情報共有の在り方について引き続き検討することが重要である。

② 事業者間での情報共有を促進するための基盤の構築

事業者間の情報共有を促進するためには、解析・対処能力が事業者間で一様ではないことを踏まえ、情報共有の目的・利点・手順、必要とされる情報を明確化するとともに、平時・有時などの状況に応じた提供すべき情報の範囲、提

供先の範囲等を明確化することが重要である。また、単に各事業者の情報を共有するだけではなく、効果的かつ効率的に実施することが重要であり、将来的には、共有された情報に基づき、サイバー攻撃に応じた自動防御を目指すことも考えられる。

総務省では、2016 年度（平成 28 年度）及び 2017 年度（平成 29 年度）に、ICT-ISAC と連携し、サイバー攻撃に関する情報を収集・分析・配布する情報共有基盤の試行運用を行う実証事業を行い、その成果として、ICT-ISAC において、「脅威情報の情報共有基盤　利用ガイドライン」を策定しており、引き続き、同ガイドラインの普及を図ることが重要である。

また、同情報共有基盤については、米国国土安全保障省（DHS）が運営する自動情報共有システム（AIS）と連携しており、情報共有の内容や範囲に配慮しつつ、このような海外との連携の取組も促進することが重要である。

さらに、事業者においてより迅速なサイバーセキュリティ対策を促進するため、サイバー攻撃に関する情報に加え、脆弱性情報を活用し、当該脆弱性の影響を受けるソフトウェアと紐付けた形で情報を配布する仕組みの検討を行うとともに、機械学習を活用したサイバー攻撃に関する情報の分析及び対策の自動化に向けた検討を実施するなど、サイバーセキュリティの更なる強化に資する情報共有基盤の構築を促進することが必要である。

③　サイバーセキュリティ対策に係る情報開示の促進

民間企業においては、複雑・巧妙化するサイバー攻撃に対する対策強化を進める動きが見られるようになってきており、こうした取組を更に促進するためには、サイバーセキュリティ対策を講じている企業が、その対策の在り様について適切に開示をし、様々なステークホルダーから評価される仕組みを構築していくことが求められる。

この点、2019 年（令和元年）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」が策定・公表されたところである。引き続き、民間企業の情報開示を促進するため、本手引きの普及を図るとともに、必要に応じて手引きの見直し等の検討を行うことが重要である。

なお、2019 年度（令和元年度）においては、企業等において様々なインシデントが発生していたところであり、発生後にどのように対応し公表をしていくかという点も含め、サイバーセキュリティ対策に関する情報開示は引き続き重要な課題である。

今後は、各企業に加え、マスメディア・格付機関など、企業による情報開示をステークホルダーに伝達する主体を含めた産業界全体における情報開示の取組を促進していくことが重要である。

④　サイバーセキュリティ対策に係る投資の促進

上述のとおり、情報開示の促進を通じて民間企業におけるサイバーセキュリティ対策の質の向上が進むことが期待されるが、併せて、民間企業のサイバーセキュリティ対策に関する投資が促進されるような環境整備（インセンティブの付与を含む）が必要である。

この点、全国 5G 及びローカル 5G については、サイバーセキュリティ等を確保しつつその適切な開発供給及び導入を促進するため、全国 5G 及びローカル 5G の導入事業者に対する税制優遇措置や導入事業者及び開発供給事業者に対する金融支援の実施を盛り込んだ「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」が 2020 年（令和２年）５月に成立したところであり、今後、税制優遇及び金融支援措置が積極的に活用されるよう、その早期施行に向け必要な準備を進めることが必要である。

⑤　国際的な ISAC 間連携【再掲】

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（Information Sharing and Analysis Center）において、国際的な ISAC 間等の連携を引き続き促進していく必要がある。

具体的には、2019 年（令和元年）11 月に一般社団法人 ICT-ISAC と米国の IT-ISAC との間でサイバーセキュリティ上の脅威に対する情報共有体制の一層の強化を目的として締結された覚書に基づき、国際連携ワークショップの開催等を通じて、一般社団法人 ICT-ISAC と米国の ICT 分野の ISAC との連携を更に強化し、通信事業者、放送事業者、IoT 機器ベンダー、セキュリティベンダー等が、脅威情報やインシデント情報等を自動的に共有し、サイバーセキュリティ対策に活用することを促進することが重要である。また、こうした取組を国際的に拡大することも重要である。

⑥　5G の脆弱性情報や脅威情報等の共有の枠組みの構築【再掲】

4G までの従来の移動通信システムでは電気通信事業者がネットワークの運

用を行っていたが、5G の時代では、ローカル 5G について、従来は通信サービスのユーザとしての位置づけであった様々な企業や自治体等がネットワークの運用者として関わっていくこととなる。

また、ネットワークの用途も、超低遅延や多数同時接続などの特長を活かした様々な産業用途が期待されているため、リスクや脅威の在り方も多様なものが想定される。

このため、5G のセキュリティを確保していく上では、Ⅲ－（２）－①の脆弱性の検証と合わせ、5G のネットワークを運用している事業者・運用者やベンダー、利用者等の間での脆弱性情報や脅威情報、さらにこれらの対処の在り方に関する情報の共有の取組が重要である。

この点、5G とそのセキュリティに関する情報共有などを定期的に実施して 5G のセキュリティの啓発を進めるとともに、ローカル 5G を含む 5G の運用者が 5G サービスを提供する場合のサイバーセキュリティ上の懸念や脅威に関する問い合わせに対して助言を行うことを目的とし、2020 年（令和２年）２月に一般社団法人 ICT-ISAC において「5G セキュリティ推進グループ」が設立されたところである。

上記のような民間での取組を踏まえつつ、引き続き、5G のセキュリティの確保に向け、情報共有の取組を促進することが必要である。

Ⅴ　今後の進め方

「IoT・5G セキュリティ総合対策 2020」の推進に際しては、定期的に検証を行い、進捗状況を把握するとともに、本分野における技術革新や最新のサイバー攻撃の態様を踏まえ、必要に応じて随時見直しを行っていくことが望ましい。また、対策の推進に際しては、内閣官房内閣サイバーセキュリティセンターや経済産業省をはじめとする関係府省庁や地方公共団体及び民間企業等との連携の下に進めていく必要がある。

「IoT・5G セキュリティ総合対策 2020」の推進は、COVID-19 への対応のみならず、その後に控えている東京大会の成功に向けても必須である。重要インフラの防御対策強化の観点を含め、関係するステークホルダーの連携によるビジョンの共有と取組の強化が不可欠である。