IoT・5G セキュリティ総合対策
プログレスレポート 2020

令和２年５月

サイバーセキュリティタスクフォース

目次

Ⅰ　はじめに

IoT をはじめとする ICT の利活用が一層進展していく中で、今後、5G のサービスが開始することが予定されているほか、Society5.0 に向けた適切なデータ管理・流通の重要性やサプライチェーンリスクへの対応の必要性が増大するなど、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。

そのため、サイバーセキュリティタスクフォースでは、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し、2019年（令和元年）８月に「IoT・5Gセキュリティ総合対策」（以下「総合対策」という。）として策定・公表した。【資料１】

また、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「2020年東京大会」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、議論を継続してきたところである。その中で、本年７月より開催される予定であった2020年東京大会に向けた対処として、本年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。【資料２】

緊急提言の公表後は主に中長期的な取組について議論を行ってきたところである。総合対策においては、その内容等について、「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」とされたところであり、本文書は総合対策の進捗状況と今後の取組の方向性について、プログレスレポートとして整理したものである。本レポートを踏まえ、今後、必要に応じて総合対策の見直しを行っていくものとする。

2018年（平成30年）７月には、政府全体の新たな「サイバーセキュリティ戦略」が策定されている。また、現在、内閣官房を中心として、2020年東京大会関連のサイバーセキュリティの取組を政府一丸となって進めている。総務省においても、本レポートの内容も踏まえつつ、このような関係府省庁等との緊密な連携によって政府全体の取組に貢献し、サイバーセキュリティ政策に継続的に取り組んでいくことが必要である。【資料３】

Ⅱ　総合対策の進捗状況と今後の取組（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）

（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

【本文】

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（昭和 59 年法律第 86 号）の枠組みにおいて端末設備等規則（昭和 60 年郵政省令第 31 号）を改正し、強制規格としての技術基準が策定されている（2019 年（平成 31 年）３月１日公布、2020（令和２年）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、当該技術基準の運用開始に向けた準備を進めることが必要である。

また、IoT 機器に関するセキュリティ対策の上乗せ部分については、民間団体がセキュリティ要件のガイドラインを策定し、さらに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)制度の構築の準備を進めていることから、このような民間の任意の認証（Certification）制度の普及が期待される。

【進捗状況】

2018 年（平成 30 年）９月の情報通信審議会及び 2019 年（平成 31 年）１月の情報通信行政・郵政行政審議会からの答申を受け、IoT 機器を含む端末設備のセキュリティ対策に関する技術基準の整備等を行うことを目的として一部改正された端末設備等規則（昭和 60 年郵政省令第 31 号）が 2020 年（令和２年）４月に施行された。

本改正に関して、総務省において、関係団体等との打合せ・意見交換や 2019 年（平成 31 年）４月に公表した「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）」を活用し、技術基準適合認定に関するセミナーでの周知等を実施するとともに、機器の製造業者等からの個別の問合せ等対

応するなど円滑な施行に向けた対応を実施した。【資料４】

また、民間の任意の認証（Certification）制度として、一般社団法人重要生活機器連携セキュリティ協議会（CCDS）において、IoT 機器のセキュリティ要件を定め、2019 年（令和元年）10 月から認証プログラムを開始している。このプログラムでは、消費者にも分かりやすいよう「★」の数でセキュリティ対策のレベル（レベル１～３）を示すこととしており、2019 年度（令和元年度）時点ではレベル１について実施している。【資料５】

さらに、民間団体における IoT セキュリティに関する任意の取組として、ルーター等のメーカー団体である一般社団法人デジタルライフ推進協会（DLPA）において、家庭内ネットワークの中心となる Wi-Fi ルーターについて、「自動ファームウェア更新機能」と「管理画面へログインするための ID 又はパスワードの固有化」を備えたものを「DLPA 推奨 Wi-Fi ルーター」としてメーカーから周知していく旨が 2019 年（令和元年）12 月に発表された。【資料６】

【今後の取組】

2020 年（令和２年）４月に施行された改正端末設備等規則について、総務省において、機器の製造業者等の関係者と連携して円滑に実施できるよう引き続き取り組むとともに、問合せへの対応を含め、適切な運用がなされるようフォローしていく。

また、民間団体における IoT セキュリティに関する任意の取組についても、より広範に広がっていくようフォローしていく。また、このような取組が実際のネットワークにおいてどの程度浸透しているのか、③に記載する取組との関連性も含め検討を進めていく必要がある。

② IoT 機器の設置・運用・保守段階での対策

【本文】

機器の性格上セキュリティ対策を取ることが困難なものや海外製品など、流通する IoT 機器の中から、脆弱性を有する IoT 機器を完全に排除することは困難であることから、機器の設置・運用・保守段階（ネットワークへの接続時又は接続後）において、脆弱性を有する機器が存在することを前提として、セキュアな IoT システム構築を実現する仕組みが重要である。

また、IoT 機器は広範な利用者が利用することが想定されており、利用者によっては、IoT 機器やセキュリティに関する知識が十分に無いことが想定さ

れる。したがって、例えば、IoT 機器の設置後に新たな脆弱性が発見された場合に、当該 IoT 機器の製造業者によって脆弱性のパッチがユーザサポートの一環として提供されるなど、各種事業者の側において対策が実施される仕組みの構築が重要である。

IoT システム・サービス全体としてのセキュリティの確保に関しては、IoT 機器だけでなく、ネットワークやプラットフォーム側での対処の在り方についても検討が必要である。この点で、IoT 機器の不正検知等のため、IoT 機器とインターネットの境界上にセキュアゲートウェイ（IoT セキュアゲートウェイ）を設置・運用し、ネットワークやプラットフォーム等での防御に活用する取組が考えられる。本取組について、Ⅲ－（４）のスマートシティのセキュリティ対策の取組等を通じ、実際の導入を進める仕組みや方策について検討することが重要である。

【進捗状況】

セキュアゲートウェイを活用した IoT 機器の監視については、Ⅲ－（４）のスマートシティのセキュリティ対策の取組において、その在り方の検討が行われている。具体的には、総務省において、内閣府で検討中のスマートシティのアーキテクチャを踏まえつつ、スマートシティのセキュリティの要件について検討する調査研究を実施しているほか、スマートシティ官民連携プラットフォーム（事務局：内閣府、国土交通省、総務省、経済産業省）のスマートシティセキュリティ・セーフティ分科会（事務局：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）においても IoT 機器を含むスマートシティのセキュリティ・セーフティの確保の在り方について検討を行っており、これらの取組において、合わせてスマートシティにおける IoT セキュアゲートウェイの必要性などについても検討を行っている。【資料７】

また、民間における IoT 機器の運用段階の取組として、2019 年 12 月に、TRON フォーラムにおいて、IoT 分野と関連した脆弱性情報の収集や情報共有等を目的として「TRON IoT 脆弱性センター」が立ち上げられ、活動を開始している。

【今後の取組】

IoT 機器の設置・運用・保守段階での対策として、総務省において、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の認証画面等から容易に判別できることなどにより攻撃を受けやすい状態に置かれていないかどうかについて、2020 年東京大会までに緊急的に調査を行い、問題のある機器の所有者・運用者等に対して注意喚起や対策の実施を促す

取組を実施予定である。【資料８】

また、IoT のセキュアゲートウェイについては、総務省において、スマートシティのセキュリティ確保の観点から、引き続き、上述の枠組みにおいて官民でその在り方について検討を行う。

③　脆弱性等を有する IoT 機器の調査と注意喚起

【本文】

前述の①、②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有することから、まずは既に設置されている IoT 機器に関する脆弱性等の有無の調査を実施し、必要な対応を速やかに実施する必要がある。

この点、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、電気通信事業者を通じて利用者への注意喚起を行うプロジェクト「NOTICE」を開始したところであり、引き続き、本プロジェクトの着実な実施を通じ、既に現在設置されている IoT 機器のセキュリティ対策を進めることが必要である。

また、「NOTICE」の取組に加えて、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、電気通信事業者を通じて利用者へ注意喚起を行う取組を実施することも必要である。

さらに上述の取組の実施にあたり、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、ウェブ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も必要である。

加えて、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。

【進捗状況】

総務省及び国立研究開発法人情報通信研究機構（以下「NICT」という。）は、インターネットサービスプロバイダ（以下「ISP」という。）と連携し、2019 年（平成 31 年）２月から、ID・パスワード設定等が脆弱なためサイバー攻撃に悪用されるおそれのある IoT 機器の調査及び当該機器の利用者への注意喚起を行

う取組「NOTICE」を開始している。具体的には、NICT がインターネット上の IoT 機器に、容易に推測されるパスワード（「password」や「123456」等）を入力すること等により、サイバー攻撃に悪用されるおそれのある機器を調査し、当該機器の情報について ISP へ通知を行い、当該通知を受けた ISP が、当該機器の利用者を特定し、注意喚起を実施している。

また、2019 年（令和元年）６月からは、NICT の NICTER プロジェクトで得られた情報を基に、既にマルウェアに感染している IoT 機器の利用者に対し、ISP が注意喚起を行う取組（以下「NICTER 注意喚起」という。）を実施している。

2020 年（令和２年）３月時点で、これらの注意喚起の取組に対して、50 社の ISP が参加しており、当該 ISP に係る約 1.1 億 IP アドレスを対象に NOTICE の調査を実施している。このうち ID・パスワードが入力可能であったものが約 100,000 件[1]であり、更に ID・パスワードによりログインでき、注意喚起の対象となったものは延べ 2,249 件[2]である。また、NICTER 注意喚起については、ISP に対する通知の対象となったものは、１日当たり平均 162 件[3]である。【資料９】

なお、これらの取組のために、専用のサポートセンターを設置するとともにウェブサイト（https://notice.go.jp）による情報提供を行っている。

また、ISP において実施する注意喚起において、より有効な手法について共有するため、2020 年（令和２年）２月に取組に参加する ISP と総務省との意見交換会を実施した。

【今後の取組】

総務省において、引き続き、NOTICE 及び NICTER 注意喚起の取組を継続するとともに、注意喚起に協力する ISP の増加を図る。また、利用者に対する有効な注意喚起については、各 ISP における架電や往訪を含めたベストプラクティスについて ISP 間で引き続き情報共有を行うとともに、新たな注意喚起手法等について検討等を行い、脆弱な状態にある IoT 機器への対策を進めていく。

---

[1] NOTICE の調査はおおむね月に１回程度実施しており、2020 年（令和２年）３月調査の数字。

[2] 2019 年（平成 31 年）４月から 2020 年（令和２年）３月までの延べ数。

[3] NICTER により検知した情報を日ごとに共有しており、日により変動があるもの。NICTER における長期的な観測傾向から見るとこの変動幅は、大きな変化ではない。

④　サイバー攻撃に関する電気通信事業者間の情報共有

【本文】

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等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 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。

【進捗状況】

2019 年（平成 31 年）２月より、「NOTICE」プロジェクトにおいて、電気通信事業者間の情報共有の結節点となる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。）の機能を活用し、認定協会経由でパスワード設定等に不備のある IoT 機器に関する情報を ISP に通知しているところであり、更に、5G のサービス開始も見据え、認定協会の活動の活性化に向けた取組を推進しているところである。【資料 10】

また、2020 年度（令和２年度）から全国 5G とローカル 5G が本格的に導入されるが、社会インフラ・産業インフラとしての活用が期待される 5G は、高いセキュリティが要求されるものであり、また、ICT 利活用の裾野が大きく広がることによるサイバーセキュリティリスクの増大が予想される。そのため、5G のリスク情報や脅威情報などについては、個々の事業者又は運用者に閉じるのではなく、相互に情報共有を行い、情報通信ネットワーク・サービス全体のレジリエンスを強化する必要がある。【資料 11】

この点、2020 年（令和２年）２月に、一般社団法人 ICT-ISAC において広く 5G

セキュリティに係る情報共有を進めることを目的とした「5G セキュリティ推進グループ」が立ち上げられたところであり、今後、5G 運用者の間で 5G を提供する場合のサイバーセキュリティのリスクや脅威に関する情報などについて情報共有を行っていくこととしている。

【今後の取組】

総務省において、IoT 機器のセキュリティに関し、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ついて、円滑な実施のための支援を行うなど、取組を促進していく。

また、今後 5G の利活用が進んでいくにつれ、5G に関するセキュリティ対策も重要な取組になってくることから、総務省において、上記の「5G セキュリティ推進グループ」などの情報共有の枠組みを促進していく。

（２）5G のセキュリティ対策

①　ソフトウェア脆弱性への対応

【本文】

今後サービスが開始される予定の 5G については、従来までの移動通信システムと比較して、①超高速、②超低遅延、③多数同時接続であるという特徴を有しており、IoT システムの基盤技術として、電気通信事業者のみならず、様々な主体や産業分野での利活用が期待されている。

一方、5G のネットワークに関しては、ネットワーク機能の仮想化・ソフトウェア化が進むことから、新たなサイバーセキュリティ上の課題が懸念される。また、新たにネットワークのエッジ（ユーザの近く）で通信処理や高度な演算・データ処理がなされる MEC が利用されることから、ネットワークインフラとしての機能維持のためには、基地局やコア網のみならず、MEC も含めた各構成要素（デバイス、クラウド、アプリケーション等）全体を考慮したセキュリティの確保が必要不可欠である。

そのため、5G を利用したシステム全体の各構成要素におけるソフトウェアを含むセキュリティを総合的かつ継続的に担保する仕組みを整備し、ガイドライン等によって対策の共有等を図ることを通じ、5G を構築・活用する重要インフラ事業者等への周知・啓発を図ることが必要である。

また、5G のセキュリティの確保は、国際的にも重要な政策課題であること

から、作成したガイドライン等について国際機関等への提案も視野に入れるなど、諸外国との連携を図ることが期待される。

【進捗状況】

5G については、2020 年度（令和２年度）以降、携帯電話事業者による全国向け 5G サービスと、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ネットワークを構築し利用可能とするローカル 5G の取組が開始することが想定されている。【資料 12】

我が国においては、5G の導入の初期段階では 4G 対応のコアネットワークを活用したノンスタンドアロン 5G の導入が予定されているが、他方、5G の普及期に導入が想定されるスタンドアロン 5G については、仮想化・ソフトウェア化がより一層進展し、ネットワークそのもののリスクや脆弱性がこれまでと大きく変わる可能性もあることから、セキュリティ・バイ・デザインの観点から、現段階でそのセキュリティの在り方についても検討を始めることが必要である。

そのため、総務省において、2019 年度（令和元年度）より、5G ネットワークにおけるソフトウェアの脆弱性に対応するための調査検討を実施している。具体的には、2019 年度（令和元年度）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ことから、5G 仮想環境（コアネットワーク）を構築し、オープンソースソフトウェア等の解析、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）、エシカルハッカー[4]による脆弱性調査、脅威分析の実施に向けて取り組んでいる。【資料 13】

【今後の取組】

2020 年度（令和２年度）は、総務省において、2019 年度（令和元年度）に構築した 5G 仮想環境を仮想化通信プラットフォーム、MEC まで拡張し、引き続き①オープンソースソフトウェア等の解析、②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）、③エシカルハッカーによる脆弱性調査、脅威分析の実施と、それに対する対策の検討を行う。

[4] 高い倫理感、技術力を持ち合わせたハッカーをエシカルハッカーと呼ぶ。

② ハードウェア脆弱性への対応

【本文】

機器のセキュリティについては、機器にインストールされているソフトウェアだけでなく、集積回路の設計工程において、ハードウェア脆弱性が存在する可能性が指摘されている。

そのため、総務省では、2017 年度（平成 29 年度）より、戦略的情報通信研究開発推進事業（SCOPE）において、ハードウェア脆弱性の検知技術の研究開発を実施し、膨大な数の回路設計図をビッグデータとして収集・蓄積しつつ、脆弱性が存在する可能性のあるチップを、AI を活用して類型化し、ハードウェア脆弱性を発見するための研究開発を実施してきたところである。

5G の時代を見据え、サプライチェーンリスクへの対応の観点から、ソフトウェアやファームウェアに対する対策と合わせて、引き続き、ビッグデータや AI を活用しつつハードウェアに組み込まれるおそれのある脆弱性を検出する技術の研究開発等を推進することが必要である。

【進捗状況】

総務省において、ハードウェア脆弱性への対応として、設計・製造におけるチップの脆弱性検知手法の研究開発を実施しており、2019 年度（令和元年度）においては、外部から調達した設計ツールや設計部品を用いたチップの安全性を担保するために、標準的なベンチマーク回路等を用いて、不正回路の種類及びその機能を明確化し、不正回路を検知する技術の開発を行った。加えて、回路情報が入手できないチップの安全性を担保するために、市販の組込みマイコン等、比較的簡易な電子機器の動作のもと、電子機器の外部から観測される情報を用いて、不正動作を検知する技術の開発を行った。【資料 13】

【今後の取組】

総務省において、引き続き、ハードウェアチップの脆弱性検知手法の確立を目的として、ハードウェアチップの回路情報を用いて不正回路を検知する技術及び電子機器の外部から観測される情報を用いて不正動作を検知する技術の改良及び基礎的な検証を実施する。

③　制度的/産業振興的対応（総合対策公表後の対応等）

【進捗状況】

5G のサイバー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[5]を講ずることを条件として付した。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。

また、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、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を行うことを目的とした「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案」が 2020 年（令和２年）２月に閣議決定された。

このような制度的な枠組み、産業振興的な枠組みの両面から 5G のセキュリティ確保を推し進めている。

【今後の取組】

総務省において、開設計画の認定や免許の附款において付与したサイバーセキュリティ対策の条件について、その履行状況のフォローアップを行う。

また、総務省において、経済産業省と連携し、「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案」の成立に向け尽力するとともに、成立後、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。

---

[5] 「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）、「政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版）」及び「ＩＴ調達に係る国の物品等又は役務の調達方針及び調達手続きに関する申合せ」（平成 30 年 12 月 10 日関係省庁申合せ）に留意し、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。

（３）クラウドサービスのセキュリティ対策

【本文】

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っている。

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」（2018 年（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。

この点、諸外国では、2010 年代に政府が情報システム調達においてクラウドファーストを掲げ、その後間もなく、政府が主導してクラウドサービスの安全性を評価する制度を構築・運用している事例があり、2018 年（平成 30 年）に上述のクラウド・バイ・デフォルト原則を採用した我が国においても、安全性評価の制度の検討が必要な段階に到達している。

そのため、総務省と経済産業省において、クラウドサービスの安全性評価に関する検討を行うことを目的として、2018 年（平成 30 年）８月より、「クラウドサービスの安全性評価に関する検討会」を開催し、2019 年（平成 31 年）３月に制度の枠組みが示されたところである。

本枠組みを踏まえつつ、官民双方が一層安全・安心にクラウドサービスを採用し、継続的に利用していくため、クラウドサービスの安全性評価制度について、引き続き、総務省において、経済産業省と連携しつつ、2020 年（令和２年）の制度の開始を目指して、評価基準や制度の確立に向けた検討を進めることが必要である。

【進捗状況】

政府の情報システムにおけるクラウドサービスの安全性評価については、2018 年（平成 30 年）８月より、総務省と経済産業省が事務局となって「クラウドサービスの安全性評価に関する検討会」を開催し、2020 年（令和２年）１月に取りまとめを公表した。

また、本取りまとめも踏まえ、2020 年（令和２年）１月のサイバーセキュリティ戦略本部において、政府情報システムにおけるクラウドサービスの安全性評価制度の基本的枠組みが本部決定されたところである。【資料 14】

本制度は、制度所管省庁（内閣官房、総務省、経済産業省）と有識者で構成される制度運営委員会を最高意思決定機関とした上で、共通の情報セキュリティ管理の基準に適合していることが監査によって確認されたクラウドサービスをリストに登録し、調達府省庁等は当該リストに掲載されているクラウドサービスの中から原則調達を行うものとしている。現在は、制度所管省庁において、各種基準やガイドラインの作成を含む制度の立ち上げ準備を実施しているところである。

【今後の取組】

これまでの検討を踏まえ、2020 年度（令和２年度）内に、全政府機関において、上記の仕組みを活用して安全性が評価され、セキュリティ水準の確保が図られたクラウドサービスの利用を開始できるよう、総務省において、内閣官房及び経済産業省と連携し、引き続き、環境整備等について検討を進める。

（４）スマートシティのセキュリティ対策

【本文】

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、Society5.0 の先行的な実現の場である。

この点、総務省では、都市に設置されたセンサーから収集・生成・蓄積・解析されるデータを活用し、その解析結果を都市経営の課題解決などに活用するデータ利活用型スマートシティ事業を 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しているため、常にサイバー攻撃のリスクにさらされるおそれがある。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等も必要である。さらに、システムとしてのスマートシティの構築・運用には多様な主体が関わることから、システム全体としてのセキュリティ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。

そのため、スマートシティ上の様々なユースケース（分野）やアーキテクチ

ャ、相互運用性などを踏まえつつ、スマートシティに求められるセキュリティ要件について検討を行い、明確化を図る必要がある。

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）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。

さらに、スマートシティのシステムでは、多種多様な IoT 機器が活用されることが想定されることから、そのセキュリティの確保に当たっては、IoT 機器そのもののセキュリティの強化だけでなく、ネットワークの側で IoT 機器の不正検知等を実施するための仕組みが有効であり、実際の運用に関して、Ⅲ－（１）－②の IoT 機器とインターネットの境界上にセキュアゲートウェイを設置し、適切に運用する取組との連携の在り方も検討することが重要である。

【進捗状況】

総務省では、スマートシティを推進する施策として、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）から実施してきたところである。【資料 15】

他方、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、「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、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。

この点、スマートシティのセキュリティについては、総務省において、内閣府作成のスマートシティのアーキテクチャを踏まえつつ、スマートシティのセキュリティの要件について検討する調査研究を実施しているほか、2020 年（令和２年）１月より、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・セーフティ分科会においてもスマートシティのセキュリティ・セ

ーフティの確保の在り方について検討を実施している。【資料７】

また、戦略的情報通信研究開発推進事業（国際標準獲得型）の取組として、総務省において EU と連携した日 EU 共同研究を実施している。スマートシティ分野については、2018 年（平成 30 年）７月から「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)」を開始し、Fed4IoT のユースケースとその要求条件の選定等を行った。これを踏まえ、IoT サービスのセキュリティ・プライバシ保護の検討を進めているところである。【資料 16】

【今後の取組】

スマートシティについては、現時点では我が国における取組は実証段階が大半であり、今後取組が拡大していくことが期待されるものである。そのため、そのセキュリティの在り方については、スマートシティの取組の推進を妨げないよう、過度な要件とならないことが必要である。他方、セキュリティ・バイ・デザインの観点から、多様な主体が関わることが想定されるスマートシティの企画・設計・構築の段階において、セキュリティ確保のための体制・方策・ルールなどの検討がなされ、実装されていくことが重要である。そのため、スマートシティのセキュリティに関し、関係者間での協議などを通じてセキュリティの PDCA サイクルや SOC 又は CSIRT の設置の必要性についての共通認識が醸成されることが必要であり、国としてそのための環境整備に取り組む必要がある。

以上を踏まえ、総務省において、スマートシティ官民連携プラットフォームなどの場も活用し、スマートシティの普及や高度化の取組と合わせ、例えばセキュリティに関する一定の考え方をスマートシティ推進主体に示すことなどを通じ、セキュリティの確保の視点を浸透させる。また、その際には、IoT、5G、クラウドに関するセキュリティ、人材育成の取組など、既存の施策のシナジーが生まれるよう、有機的に連携させることが重要であることに留意が必要である。

戦略的情報通信研究開発推進事業（国際標準獲得型）で実施している Fed4IoT については、総務省において、欧州も含めたサービスも考慮し、IoT サービスにおいて個人情報を保護した上でユーザ認証・属性認証サービスを提供するスキームの実証を行う。

（５）トラストサービスの在り方の検討

【本文】

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」を設置し、2019 年（平成 31 年）１月から、以下のようなトラストサービスに関する現状や課題について検討を行っている。

１）人の正当性を確認できる仕組み（電子署名）

２）組織の正当性を確認できる仕組み（組織を対象とする認証、ウェブサイト認証）

３）IoT 機器等のモノの正当性を確認できる仕組み

４）データの存在証明・非改ざんの保証の仕組み（タイムスタンプ）

５）データの送達等を保証する仕組み（e デリバリー）

一方、EU においては 2016 年（平成 28 年）７月に発効した eIDAS（electronic Identification and Authentication Services）規則により、電子署名、タイムスタンプ、e シール等のトラストサービスについて包括的に規定している状況である。

そのため、国際的な相互運用性の確保の観点からも、引き続き、同ワーキンググループにおいて、制度的課題等について整理を行い、トラストサービスの在り方について 2019 年（令和元年）中を目途に結論が得られるよう、検討を進めることが必要である。

【進捗状況】

データの改ざんや送信元のなりすましを防止し、データの信頼性を確保する仕組みであるトラストサービスについては、Society5.0 時代において、社会全体のデジタル化に貢献するものとして、「プラットフォームサービスに関する研究会」の下に設置した「トラストサービス検討ワーキンググループ」において、2019 年（平成 31 年）１月の第１回会合以来、同年 11 月まで合計 15 回にわたり、事業者やユーザ企業等からユースケース等のヒアリング等を行いつつ、トラストサービスの制度化の在り方に関する詳細な検討を行ってきた。【資料 17】

2020 年（令和２年）２月にプラットフォーム研究会の最終報告書が取りまとめられ、トラストサービスに関しては、上記ワーキンググループの議論を基に、

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。【資料 18】

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、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ることを踏まえ、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付けについて検討を行うことが適当である。

【今後の取組】

上記「プラットフォームサービスに関する研究会」の最終報告書を踏まえ、総務省において、タイムスタンプについては 2020 年（令和２年）３月に「タイムスタンプ認定制度に関する検討会」を、e シールについても４月に「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」を立ち上げ、これらの会合において、国際的な相互運用の観点も踏まえながら、具体的な認定基準等の制度の詳細について検討を行うこととしている。

さらに、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が各種業法等に位置づけられることが重要であることに鑑み、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、総務省において、法令・制度を所管する関係省庁への働きかけを行っていくこととしている。

（６）公衆無線 LAN のセキュリティ対策

【本文】
公衆無線 LAN については、2020 年東京大会に向けて、観光や防災の観点から、その普及が進んでいるところである。他方、多くの公衆無線 LAN のサービスにおいて、依然としてサイバーセキュリティに対する配慮に欠けるものも多く、これらのサービスを踏み台にした攻撃や情報漏洩などのインシデントが発生するおそれもある。
そのため、公衆無線 LAN の利用者や提供者向けの公衆無線 LAN の利用の手引きの普及を図るなど、利用者・提供者において必要となるセキュリティ対策に関する周知啓発の充実を図ることが重要である。
その際、Ⅲ－（８）の地域の情報通信サービスのセキュリティの確保の取組で構築する連絡体制を活用し、効果的な周知啓発を図ることが重要である。

【進捗状況】

総務省では、公衆無線 LAN の提供者・利用者向けに、それぞれ「Wi-Fi 提供者向け　セキュリティ対策の手引き（平成 28 年８月版）」及び「Wi-Fi 利用者向け簡易マニュアル(平成 27 年３月 10 日版)」としてガイドラインを作成している。当該ガイドラインは総務省 HP に掲載しており年間約３万件の閲覧があるなど周知啓発に活用しているが、新たな無線 LAN 規格の登場等を踏まえ、現在、当該ガイドラインの見直しを行っている。ガイドラインの改定に当たっては、新技術動向（WPA3、Enhanced Open 等）の反映のほか、ガイドライン対象者の明確化や、なりすましアクセスポイント（詐称されたアクセスポイント）対策について追記することを予定している。【資料 19】

また、公衆無線 LAN の利用者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 2020 年（令和２年）２月 10 日から同年３月 23 日にかけて開講した。これは、大規模オンライン講座プラットフォーム「gacco」を活用し、有識者が公衆無線 LAN 利用時のリスクや適切なセキュリティ対策等を動画(全 10 回)により紹介するもので、3,164 名が受講登録を行った。

また、若年層を含む利用者への周知を目的として、無線 LAN のセキュリティ対策に関して 20 秒程度の動画コンテンツ（全３種）を作成し、SNS を通じて、

2020 年（令和２年）３月２日から同月 22 日にかけて約 102 万インプレッション[6]の動画配信（広告）を行っている。【資料 20】

【今後の取組】

公衆無線 LAN サービスの利用に当たっては、総務省において、訪日外国人の利用も念頭に置きつつ、提供者・利用者双方におけるセキュリティ対策を進めるほか、ガイドラインについて 2020 年度（令和２年度）の早期に改訂を行うとともに、2020 年東京大会に向けて多くの利用が見込まれるホテル・観光関係機関や病院、また GIGA スクール構想をはじめ ICT の利活用の進む学校等を含めて周知を実施していくなど、引き続き、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・提供者において必要となるセキュリティ対策に関する周知啓発の充実を図る。

（７）重要インフラとしての情報通信分野のセキュリティ対策

【本文】

情報通信分野は、「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　平成 30 年７月 25 日サイバーセキュリティ戦略本部改定。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低下した場合に国民生活・社会経済活動に多大なる影響を及ぼしかねないサービスとして重要インフラの 14 分野の１つに指定されている。

第４次行動計画を踏まえ、重要インフラ各分野に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月サイバーセキュリティ戦略本部決定　令和元年５月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の取組が進められている。

この点、電気通信においては、各年の取組として、「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、事故再発防止のため、「情報通信ネットワーク・安全信頼性基準」等の見直しの必要性について検討を行っている。

また、2018 年度（平成 30 年度）には、前述のⅢ－（１）－④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

[6] 動画コンテンツをクリックした場合には、gacco 上で開講しているオンライン動画講座の登録ページに誘導するようにしており、3,525 ユニーククリックであった。

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を改正する制度整備が行われている。

以上のような取組も踏まえつつ、引き続き、必要に応じて情報通信分野のセキュリティ対策に関する制度的枠組みの改善等に向けた取組が行われることが期待される。

【進捗状況】

本タスクフォースでは、１月に公表した緊急提言において、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、総務省において、緊急提言や第４次行動計画なども踏まえ、所管の情報通信分野において、安全基準等の整備及び浸透の取組などを進めてきているところである。

情報通信分野については、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、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[7]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（昭和 62 年郵政省告示第 73 号）の改正に向けた手続きを行っており、2020 年（令和２年）６月末までの制度化を予定している。

さらに、放送分野については、緊急提言においても、「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

7 「IoT の普及に対応した電気通信設備に係る技術的条件」に関する情報通信審議会からの一部答申（令和２年３月 31 日）
https://www.soumu.go.jp/menu_news/s-news/01kiban05_02000201.html

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、総務省において、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）などを改正する制度整備の作業を進め、パブリックコメント（2020 年（令和２年）１月 22 日（水）～2020 年（令和２年）２月 20 日（木））を実施した。このパブリックコメントを踏まえて、同年３月 11 日（水）に電波監理審議会に放送法施行規則の改正案を諮問し、同日原案を適当とする旨の答申を受け、同年３月末までに制度整備を実施した。

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行った。【資料 21】

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

合わせて、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いる。【資料 22】

【今後の取組】

先述のとおり、情報通信分野では制度的枠組みの改善の取組を積極的に実施

してきたところであり、総務省において、引き続き、これらの取組を先導的に進めていくとともに、我が国の重要インフラ事業者のセキュリティ確保に向け、他の分野においても積極的に周知をしていくことが重要である。

その上で、放送分野では、総務省において、先述の制度改正を踏まえつつ、引き続き、各放送事業者の安全信頼性対策の意識向上に向けた周知・啓発を行う。

（８）地域の情報通信サービスのセキュリティの確保

【本文】

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、セキュリティ対策が十分でないケースが存在するおそれがある。

そのため、業界団体やセキュリティ関係機関等と連携しつつ、地域の事業者のサイバーセキュリティ対策の質の向上に向けた連絡体制を構築することが必要である。

なお、当該施策の展開に当たっては、Ⅲ－（６）の公衆無線 LAN のセキュリティの確保やⅣ－（２）－①の実践的サイバー防御演習（CYDER）の実施、Ⅳ－（２）－④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、効果的に地域の情報通信サービス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。

【進捗状況】

地域の情報通信サービスのセキュリティの確保のためには、国の行政機関の地方支分部局、産業界、大学等の教育機関、都道府県警、地方公共団体など様々な主体によるコミュニティ形成が一つの重要な取組である。

この点で、北海道地方や近畿地方では、地方単位で産学官が連携したセキュリティ確保の体制が既に構築され、継続的な活動を行っている。

例えば、北海道では 2014 年（平成 26 年）９月に北海道地域情報セキュリティ連絡会（HAISL）が北海道総合通信局・北海道経済産業局・北海道警察を共同事

務局として立ち上げられており、参画機関・団体が実施する情報セキュリティ関連行事の告知や相互協力依頼、人材育成に係る環境整備など連絡会員間での連携を図り、各事業の効果的かつ効率的な実施につなげることを目的として、情報セキュリティに関する定期的な勉強会や注意喚起等の情報発信を継続的に行っている。【資料 23】

また、近畿では、2018 年（平成 30 年）10 月より、近畿総合通信局・近畿経済産業局・一般財団法人関西情報センター（KIIS）が共同事務局となり、サイバーセキュリティに関する関西の産学官等の相互協力を促進し、関西におけるセキュリティの推進基盤として人材発掘・育成、情報交換、機運醸成の場を提供することを目的として、関西サイバーセキュリティ・ネットワーク（関西 SEC-net）が活動を開始している。本体制については、産学官個で 65 機関（2020 年（令和２年）２月時点）が参加しており、サイバーセキュリティ人材の産学交流イベントや企業担当者向けのサイバーセキュリティ・リレー講座、企業経営者層向けセミナーやイベントなどを継続的に実施している。【資料 24】

また中国地方では、既に都道府県単位で産学官の連携の枠組みが構築されていることから、2019 年度（令和元年度）は、中国総合通信局において、当面の取組として通信・放送事業者の経営層向けにサイバーセキュリティに関する講演を行う機会を増やし、通信・放送事業者への啓蒙・啓発の取組を開始した。

このほか、2019 年度（令和元年度）には、北海道、中国、近畿において、経営層及び戦略マネジメント層を対象とし、有事のインシデント対応について学ぶ演習又はセミナーを予定していたが、新型コロナウイルス感染症（以下「COVID-19」という。）の影響で中止となった。

なお、これらの活動[8]及びサイバーセキュリティタスクフォースでの議論により、例えば以下のような課題が明らかになっている。

・インシデント演習等の専門的な活動を実施する場合には、域内のリソースだけでは実施が難しいことから、域外の専門家などと継続的な関係作りをしつつ、うまく活動に巻き込んでいくことが必要。

・人事異動などで人脈が途切れてしまう可能性があることから、安定的な運用のためにも平時、有事の信頼関係の構築を含め、信頼できるキーマンの存在が必要。

8 上記のほか、東北地方においては、東北経済産業局、独立行政法人情報処理推進機構、地方公共団体等の連携により、各県でサイバーセキュリティセミナーが開催されている。

・地域では優秀な専門人材が東京に引き抜かれていっており、コミュニティの構築の先のゴールについての検討が必要。

・有事の情報共有は難しいため、まずは平時における情報共有の体制を構築していくことが重要。また、新しいコミュニティではなく、既存のコミュニティの活用をするのが望ましい。

・コミュニティの構築はコミュニティの色や参加したい人に強く依存する一方、情報発信に課題を抱えているコミュニティが多いため、国としては横から暖かく見守るプロモーションに取り組むのが望ましい。

【今後の取組】

地域に根付いたセキュリティコミュニティの構築については、コミュニティの単位について、地方レベル、都道府県レベル、市町村レベルなど様々な単位が想定されるが、いずれのケースにおいても大前提として、各地域における自発的な取組として実施される必要があり、国は自立性を尊重しつつ、そのような取組の側面支援を行っていくことが必要である。

その上で、総務省において、経済産業省などと連携し、インシデント演習等の高度に専門的な知見やスキルを必要とする取組の実施に当たっての人的・予算的支援や、コミュニティ作りの事例の積極的な周知、既存のコミュニティを活用した活動の支援などを念頭におきつつ、地域に根付いたセキュリティコミュニティの形成の取組を引き続き促進する。

Ⅲ　総合対策の進捗状況と今後の取組（横断的施策）

（１）研究開発の推進

①　基礎的・基盤的な研究開発等の推進

【本文】

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格子理論に基づく新たな公開鍵暗号の開発、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）－③の脆弱性等を有するIoT機器の調査と注意喚起と連携し、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。

【進捗状況】

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。

特に、サイバーセキュリティ技術については、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・模擬情報を用いたサイバー攻撃誘引基盤「STARDUST」の高度化を進めるとともに、標的型攻撃の解析結果について、

関係機関との情報共有を行った。【資料 25】

加えて、サイバーセキュリティ関連情報を大規模集約し、安全かつ利便性の高いリモート情報共有を可能とする「CURE」（キュア）を開発・実装するとともに、NICT 内における集約データ間の突合分析を含む試験運用を行った。【資料 26】

また、暗号技術分野については、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格子理論に基づく新たな公開鍵暗号の開発、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を行っており、2019 年度（令和元年度）においては、多変数多項式暗号の安全性評価において世界記録を達成した。【資料 27】

また、2019 年（令和元年）６月からは、NICT の NICTER プロジェクトで得られた情報を基に、既にマルウェアに感染している IoT 機器の利用者に対し、ISP が注意喚起を行う取組を実施している。

【今後の取組】

NICT では、引き続き、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くとともに、NICTER 注意喚起を通じた IoT 機器のセキュリティ対策を推進していく。

② 広域ネットワークスキャンの軽量化

【本文】

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。他方、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。

他方、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）－③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。

【進捗状況】

既存の広域ネットワークスキャン技術は、IoT機器が接続されたネットワークに対して網羅的に行うものであるため、IoT機器が増加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。

このため、総務省において、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指して、2018年度（平成30年度）から「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」に取り組んでいる。【資料28】

2019年度（令和元年度）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技術を確立するため、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、広域ネットワークスキャンの無線通信量軽減技術に関する詳細な技術仕様の検討と性能評価を行うとともに、研究開発成果の活用を目的として、項目Ⅱ－（１）－③のIoT機器の脆弱性調査を実施するNICT等に対し、本研究で収集した広域スキャンデータや機器情報を提供した。

【今後の取組】

総務省において、引き続き、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指して、研究開発を進め、詳細な技術仕様の検討と性能評価を行い、技術を確立する。

また、本研究開発の成果を脆弱性等を有するIoT機器の調査（項目Ⅱ－（１）－③参照）に活用するための連携を引き続き進め、調査の効率化に取り組む。

③　ハードウェア脆弱性への対応【再掲】

【本文】

機器のセキュリティについては、機器にインストールされているソフトウェアだけでなく、集積回路の設計工程において、ハードウェア脆弱性が存在する可能性が指摘されている。

そのため、総務省では、2017 年度（平成 29 年度）より、戦略的情報通信研究開発推進事業（SCOPE）において、ハードウェア脆弱性の検知技術の研究開発を実施し、膨大な数の回路設計図をビッグデータとして収集・蓄積しつつ、脆弱性が存在する可能性のあるチップを、AI を活用して類型化し、ハードウェア脆弱性を発見するための研究開発を実施してきたところである。

5G の時代を見据え、サプライチェーンリスクへの対応の観点から、ソフトウェアやファームウェアに対する対策と合わせて、引き続き、ビッグデータや AI を活用しつつハードウェアに組み込まれるおそれのある脆弱性を検出する技術の研究開発等を推進する必要がある。

【進捗状況】

総務省において、ハードウェア脆弱性への対応として、設計・製造におけるチップの脆弱性検知手法の研究開発を実施しており、2019 年度（令和元年度）においては、外部から調達した設計ツールや設計部品を用いたチップの安全性を担保するために、標準的なベンチマーク回路等を用いて、不正回路の種類及びその機能を明確化し、不正回路を検知する技術の開発を行った。加えて、回路情報が入手できないチップの安全性を担保するために、市販の組込みマイコン等、比較的簡易な電子機器の動作のもと、電子機器の外部から観測される情報を用いて、不正動作を検知する技術の開発を行った。【資料 13】

【今後の取組】

総務省において、引き続き、ハードウェアチップの脆弱性検知手法の確立を目的として、ハードウェアチップの回路情報を用いて不正回路を検知する技術及び電子機器の外部から観測される情報を用いて不正動作を検知する技術の改良及び基礎的な検証を実施する。

④　スマートシティのセキュリティ対策【再掲】

【本文】

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、Society5.0 の先行的な実現の場である。

この点、総務省では、都市に設置されたセンサーから収集・生成・蓄積・解析されるデータを活用し、その解析結果を都市経営の課題解決などに活用するデータ利活用型スマートシティ事業を 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しているため、常にサイバー攻撃のリスクにさらされるおそれがある。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等も必要である。さらに、システムとしてのスマートシティの構築・運用には多様な主体が関わることから、システム全体としてのセキュリティ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。

そのため、スマートシティ上の様々なユースケース（分野）やアーキテクチャ、相互運用性などを踏まえつつ、スマートシティに求められるセキュリティ要件について検討を行い、明確化を図る必要がある。

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）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。

さらに、スマートシティのシステムでは、多種多様な IoT 機器が活用されることが想定されることから、そのセキュリティの確保に当たっては、IoT 機器そのもののセキュリティの強化だけでなく、ネットワークの側で IoT 機器の不正検知等を実施するための仕組みが有効であり、実際の運用に関して、Ⅱ－（１）－②の IoT 機器とインターネットの境界上にセキュアゲートウェイを

設置し、適切に運用する取組との連携の在り方も検討することが重要である。

【進捗状況】

総務省では、スマートシティを推進する施策として、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）から実施してきたところである。

他方、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、「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、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。

この点、スマートシティのセキュリティについては、総務省において、内閣府の検討会議での議論を踏まえたスマートシティのアーキテクチャを踏まえつつ、スマートシティのセキュリティの要件について検討する調査研究を実施しているほか、2020 年（令和２年）１月より、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・セーフティ分科会においてもスマートシティのセキュリティ・セーフティの確保の在り方について検討を実施している。【資料７】

また、戦略的情報通信研究開発推進事業（国際標準獲得型）の取組として、総務省において EU と連携した日 EU 共同研究を実施している。スマートシティ分野については、2018 年（平成 30 年）７月から「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）」を開始し、Fed4IoT のユースケースとその要求条件の選定等を行った。これを踏まえ、IoT サービスのセキュリティ・プライバシ保護の検討を進めているところである。【資料 16】

【今後の取組】

スマートシティについては、現時点では我が国における取組は実証段階が大半であり、今後取組が拡大していくことが期待されるものである。そのため、そのセキュリティの在り方については、スマートシティの取組の推進を妨げないよう、過度な要件とならないことが必要である。他方、セキュリティ・バイ・デ

ザインの観点から、多様な主体が関わることが想定されるスマートシティの企画・設計・構築の段階において、セキュリティ確保のための体制・方策・ルールなどの検討がなされ、実装されていくことが重要である。そのため、スマートシティのセキュリティに関し、関係者間での協議などを通じてセキュリティのPDCA サイクルや SOC 又は CSIRT の考え方などについての共通認識が醸成されることが必要であり、国としてそのための環境整備に取り組む必要がある。

以上を踏まえ、総務省において、スマートシティ官民連携プラットフォームなどの場も活用し、スマートシティの普及や高度化の取組と合わせ、例えばセキュリティに関する一定の考え方をスマートシティ推進主体に示すことなどを通じ、セキュリティの確保の視点を浸透させる。また、その際には、IoT、5G、クラウドに関するセキュリティ、人材育成の取組など、既存の施策のシナジーが生まれるよう、有機的に連携させることが重要であることに留意が必要である。

戦略的情報通信研究開発推進事業（国際標準獲得型）で実施しているFed4IoTについては、総務省において、欧州も含めたサービスも考慮し、IoT サービスにおいて個人情報を保護した上でユーザ認証・属性認証サービスを提供するスキームの実証を行う。

⑤　衛星通信におけるセキュリティ技術の研究開発

【本文】

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。

【進捗状況】

総務省において、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「衛星通信における量子暗号技術の研究開発」に取り組んでいる。

2019 年度（令和元年度）予算では、「衛星通信における量子暗号技術の研究開発」として 3.6 億円を計上しており、2022 年度（令和４年度）までの研究開発期間の中で、量子暗号通信を超小型衛星に活用するために、

１）超小型衛星に搭載可能な量子暗号装置の小型化・軽量化技術
２）衛星への照準を精微に合わせるための空間光通信・高精度捕捉追尾技術
３）衛星から送信された光信号を地上局において、高感度に受信する技術の開発に向けた、装置の設計及び試作等を実施した。【資料 29】

【今後の取組】

総務省において、2020 年度（令和２年度）末までに小型化・軽量化した量子暗号装置や高精度捕捉追尾、高感度受信可能な送受信機の製作及び機能検証等を終え、上記１）～３）の技術を集約・統合し、2021 年度（令和３年度）から 2022 年度（令和４年度）にかけて実証実験を行う。

⑥ AI を活用したサイバー攻撃検知・解析技術の研究開発

【本文】
日々、数多く発生するサイバー攻撃に対して、AI を活用することにより、サイバー攻撃の検知・解析を自動化し、多様なサイバー攻撃に対する迅速なサイバーセキュリティ対策を講ずることが可能となる。
そのため、今後、AI を活用したサイバー攻撃検知・解析技術の研究開発にも取り組む必要がある。具体的には、様々な手法により収集したサイバー攻撃情報を、機械学習を用いて分析することにより、マルウェアの攻撃挙動の解析を自動化するとともに、攻撃の初期挙動の特徴分析や影響度評価を行い、関連組織で共有できる早期警戒情報を導出する技術等を開発する必要がある。

【進捗状況】

NICT では、巧妙化・高度化するサイバー攻撃に対して、機械学習を始めとす

るAIを活用したサイバーセキュリティの研究開発に取り組んでいる。

具体的には、ダークネット、ハニーポット、サンドボックス、クローリング等を用いて、マルウェア感染IPアドレス、スキャン等の攻撃挙動情報、C&Cサーバとの通信に関する情報、悪性URL等を収集し、これらをデータベース化したデータセットを用いて、攻撃の影響度分析、攻撃相関分析、攻撃パターン分析等を機械学習等によって自動化する試みを行っている。

2019年度（令和元年度）においては、

１） 多種多様な観測手段から得られるサイバー攻撃情報に対し、各種機械学習のエンジンを用いて、多角的なマルウェア挙動に関連する特徴量を抽出する技術
２） 抽出された多角的なマルウェア挙動に関連する特徴量を用いて、サイバー攻撃の初期挙動の検出及び影響度分析を行い、早期警戒情報を導出する技術の確立を目的とし、ダークネット、ハニーポット等の多くの手段により収集したデータに基づき、AI技術を駆使することで、IoTマルウェアの挙動検知技術の基本方式の設計を実施した。【資料30】

【今後の取組】

NICTにおいて、サイバー攻撃の巧妙化、多様化が進む中で、AIを効果的にサイバーセキュリティ対策に活用することが求められていることから、引き続き、AIのサイバーセキュリティ対策の活用に向けた研究開発に取り組む。

⑦ 量子コンピュータ時代に向けた暗号の在り方の検討

【本文】
①のとおり、暗号技術分野については、NICTにおいて、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格子理論に基づく新たな公開鍵暗号の開発、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を行っている。
その上で、今後、大規模な量子コンピュータの実用化による暗号の危殆化の可能性を踏まえた検討が必要であることから、CRYPTRECの「暗号技術検討会」の下に「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、次期電子政府推奨暗号リストの要件、その他新たな暗号技術の動向を踏まえた検討を行う必要がある。

【進捗状況】

総務省及び経済産業省は、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（Cryptography Research and Evaluation Committees)」を実施しており、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行うため、CRYPTREC の暗号技術検討会の下に「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」(以下「検討 TF」という。）を 2019 年（令和元年）６月に設置した。【資料 27】

検討 TF として３回の会合を実施し、まず、量子コンピュータの開発動向等について検討を行った。その結果、現状の量子コンピュータの規模（量子ビット数）は 50 程度だが、暗号解読には数千程度以上が必要である上、現状の量子コンピュータではノイズ（誤り）があり、規模だけ拡大しても暗号解読に活用できる水準ではないため、暗号解読ができるような（大規模でノイズの少ない）量子コンピュータの実現時期が見えていないことが確認された。

なお、ゲート型の量子コンピュータが量子超越を実現したという報告があり、暗号技術の危殆化が一部で懸念されたことから、検討 TF で検討を行った量子コンピュータの動向を周知するため、2020 年（令和２年）２月 17 日に、CRYPTREC として「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」という注意喚起情報を発出している。当該情報において、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ため、CRYPTREC としては、CRYPTREC 暗号リスト記載の暗号技術が近い将来に危殆化する可能性は低いと考えていることを明らかにしている。

こうした動向を踏まえた上で、CRYPTREC 暗号リストにおける耐量子計算機暗号の扱いについて検討を行った。その結果、CRYPTREC 暗号リストは、安全性等の評価に加え、利用実績や普及見込みも考慮して作成しているところ、耐量子計算機暗号は、多数の方式が提案され安全性等の検討が行われている状況であり、その利用実績や普及見込みを考慮できる段階にないことから、CRYPTREC 暗号リストとは別に、耐量子計算機暗号に関するガイドラインを作成することが適当とされた。

また、検討 TF において、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、CRYPTREC 暗号リストにおいてどのように取り扱うべきか検討が行われ、これらの暗号は、利用環境やアプリケーションが限定され、従来暗号とは取り扱いが異

なることから、CRYPTREC 暗号リストとは別に、軽量暗号及び高機能暗号に関するガイドラインを作成することが適当とされた。

【今後の取組】

総務省及び経済産業省において、量子コンピュータや耐量子計算機暗号の状況をフォローし、CRYPTREC 暗号リスト改定の在り方を引き続き議論するため、2020 年度（令和２年度）以降も検討 TF を継続設置することを予定している。

また、耐量子計算機暗号等に関するガイドラインの検討は、暗号技術の安全性評価を実施している CRYPTREC の暗号技術評価委員会にて、CRYPTREC 暗号リストの改定作業（2022 年度（令和４年度）末目途）と並行して実施することを予定している。

⑧　重要インフラ等におけるサイバーセキュリティの確保

【本文】

戦略的イノベーション創造プログラム（以下「SIP」という。）の第１期課題（2015 年度（平成 27 年度）～2019 年度（令和元年度））である「重要インフラ等におけるサイバーセキュリティの確保」について、内閣府、経済産業省等と連携して研究開発と実証を進めている。

本課題では、2020 東京大会の安心・安全な開催に向けて重要インフラ等におけるサイバーセキュリティを確保するため、制御・通信機器の真贋判定技術及び動作監視・解析技術等の開発に取り組んでおり、最終年度である 2019 年度（令和元年度）において、幅広い分野に横展開するための技術開発及び社会実装を進める必要がある。

【進捗状況】

総務省において、内閣府、経済産業省等と連携して、2020 年東京大会の安心・安全な開催に向けて重要インフラ等におけるサイバーセキュリティを確保するため、制御・通信機器の真贋判定技術及び動作監視・解析技術等の開発に取り組んでいる。2019 年度（令和元年度）においては、５年間のプロジェクトの最終年度として、幅広い分野に横展開のために必要な技術開発を行うとともに、開発技術の商用サービス化及び重要インフラ事業者による実装を進めた。

⑨　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

【本文】
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、実証実験に向けた準備を着実に進めることが重要である。

【進捗状況】

総務省において、内閣府、経済産業省等と連携して、セキュアな Society 5.0 の実現に向けて、様々な IoT 機器を守り、社会全体の安全・安心を確立するため、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。2019 年度（令和元年度）においては、５年間のプロジェクトの２年目として、各技術において、基本方式の設計とデモシステム（PoC）の開発を行うとともに、2020 年度（令和２年度）の実証実験に向けた準備を行った。

【今後の取組】

総務省において、引き続き、内閣府、経済産業省等と連携し、IoT システム・サービス及びサプライチェーン全体のセキュリティを確保するために必要な研究開発を本格化するとともに、特定分野での実証実験を開始する。

（２）人材育成・普及啓発の推進

①　実践的サイバー防御演習（CYDER）の実施

【本文】

総務省はNICTを通じ、NICTの北陸StarBED技術センターに設置された大規模高性能サーバ群を活用し、行政機関等の実際のネットワークを模した大規模仮想LAN環境を構築の上、国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者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、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シナリオを提供している。

そのため、演習の取組を継続的に進めつつ、NICTが実施している基礎的・基盤的な研究開発の研究成果も活用しつつ、新たな手法のサイバー攻撃にも対応できる演習プログラム・教育コンテンツの開発を継続的に行う必要がある。

また、特に受講実績の少ない地方公共団体の受講機会拡大を図るため、開催方法等の工夫を行うなど、運営方法についても継続的に見直しを進めることが重要である。

その上で、Ⅲ－（８）の地域の情報通信サービスのセキュリティの確保の取組と連携し、CYDERの適切な周知広報がなされることが期待される。

【進捗状況】

実践的サイバー防御演習（CYDER）は、2017年度（平成29年度）から、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、年間100回、計3,000名規模で実施している。具体的には、2017年度（平成29年度）は100回の演習で計3,009名、2018年度（平成30年度）は107回の演習で計2,666名、2019年度（令和元年度）は105回の演習で計3,090名が受講した。【資料31】

2019年度（令和元年度）のCYDERの実施に当たっては、未受講となる地方公共団体の参加を促す観点から、開催場所及び開催日程といった開催方法の見直しを総合通信局等とも連携して実施した。具体的には、開催場所については、従来、都道府県庁所在地での開催を原則としていたが、これまでの参加実績を踏まえ変更や追加を実施した[9]。また、開催日程については、同一地域での開催日を

[9] 例えば北海道においては、2018年度（平成30年度）は札幌市及び旭川市で実施していたが、2019年度（令和元年度）は札幌市、函館市及び釧路市で実施した。

分散化することにより、受講機会を拡大した[10]。この結果、2017 年度（平成 29 年度）及び 2018 年度（平成 30 年度）に未受講であった地方公共団体 1,019 団体のうち 175 団体が新たに受講し、2019 年度（令和元年度）までの未受講団体数は 844 団体となった。これは、全地方公共団体（1,788 団体）の過半が受講済の状況である。

また、独立行政法人及び指定法人は全 96 機関のうち 30 機関が 2017 年度（平成 29 年度）及び 2018 年度（平成 30 年度）に未受講であったことから、所管省庁を通じた CYDER 演習に関する周知を実施した結果、30 機関中 27 機関が新たに受講した。

演習シナリオについては、①各コースで異なるシナリオとする、②最新のサイバー攻撃の事例を踏まえて実際の組織で発生し得る現実的なシナリオとする、③前年度と異なるシナリオの提供を通じて受講者へ CYDER 再受講を促せるようにする、との方針の下で 2019 年度（令和元年度）についても新たな演習シナリオを作成した上で演習を実施している。

周知については、地域の ICT 振興のために総務省としてとりまとめ作成している地域情報通信振興関連施策集に掲載したり、新たにポスターを作成し都道府県等に送付したりといった対応を実施している。

【今後の取組】

2020 年東京大会の開催に向け、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。この観点から NICT において、CYDER による人材育成を引き続き実施するとともに、依然として半数近くが未受講である地方公共団体の受講促進の取組を早急に実施する必要がある。

具体的には、都道府県ごとに CYDER 未受講の市区町村等を対象とした受講計画の作成を進めており、各都道府県と緊密に連携しながら地方公共団体における CYDER 受講の促進を図ることとする。

また、地理的な要因等により未受講である地方公共団体について、開催場所の変更による対応だけでは限界があることから、NICT において、2021 年（令和３

[10] 例えば四国においては、2018 年度（平成 30 年度）は４件とも７月上中旬に実施していたが、2019 年度（令和元年度）は７月（徳島県）・８月（愛媛県）・９月（香川県）・10 月（高知県）と分散開催を実施した。

年）初頭を目途にオンラインでの受講を可能とする演習実施環境の整備を実施する予定である。

② 2020 年東京大会に向けたサイバー演習の実施

【本文】
総務省は NICT を通じ、2020 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 2016 年（平成 28 年）より実施している。
本演習においては、大規模クラウド環境を用いて、公式サイト、大会運営システムや、社会インフラの情報システム等を模擬したシステムを構築し、当該システムを活用して、大会開催時を想定したサイバー攻撃を模擬し、大会組織委員会のサイバーセキュリティの担当者を中心に、攻撃側と防御側の手法の検証及び訓練を行っている。
また、2018 年（平成 30 年）より講義形式でサイバー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たほか、実機演習についても演習シナリオのレベル分けを増やすなど、必要に応じて見直しを実施している。
来年に開催される 2020 東京大会の円滑な実施に向け、大会事務局等と連携しつつ、引き続き本演習の取組を着実に実施する必要がある。

【進捗状況】

2020 年東京大会に向けた実践的サイバー演習「サイバーコロッセオ」は、2017 年度（平成 29 年度）から、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施している。具体的には、実機演習を行う「コロッセオ演習」を実施しているほか、2018 年度（平成 30 年度）からは講義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」も併せて実施している。

2017 年度（平成 29 年度）は、コロッセオ演習として初・中級コースと準上級コースを各１回ずつ（計２回）開催し、延べ 74 名（初・中級コース 34 名／準上級コース 40 名）が受講した。2018 年度（平成 30 年度）はコロッセオ演習として初級コース、中級コース及び準上級コースを各２回ずつ（計６回）開催し、延べ 137 名（初級コース 38 名／中級コース 51 名／準上級コース 48 名）が受講したほか、コロッセオカレッジを 16 回開催し、延べ 347 名が受講した。2019 年度（令和元年度）はコロッセオ演習として初級コース４回、中級コース５回及び準上級コース６回の計 15 回開催し、延べ 193 名（初級コース 72 名／中級コース

67 名／準上級コース 54 名）が受講したほか、コロッセオカレッジを 59 回開催し、延べ 992 名が受講した。【資料 32】

【今後の取組】

2020 年度（令和２年度）についても、NICT において、2020 年東京大会の実施延期及び COVID-19 の状況を鑑みた上で、大会組織委員会と緊密な連携を図りながら、コロッセオ演習及びコロッセオカレッジを実施する予定である。

③　若手セキュリティ人材の育成の促進

【本文】
総務省では NICT を通じ、未来のサイバーセキュリティ研究者・起業家の創出に向けて、サイバーセキュリティ分野の第一線で活躍する研究者・技術者が 25 歳以下の若手 ICT 人材に対し、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・開発について、１年かけて継続的かつ本格的に指導する「SecHack365」を 2017 年（平成 29 年）から実施している。
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。

【進捗状況】

25 歳以下の ICT 人材を対象にセキュリティイノベーターの育成に取り組む「SecHack365」は、2017 年度（平成 29 年度）から、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施している。具体的には、NICT の有する演習開発環境「NONSTOP」を活用した遠隔開発実習や、集合イベントとして座学講座（研究倫理）やハッカソン等により構成されている。【資料 33】

2017 年度（平成 29 年度）は 10 歳から 24 歳までの 39 名がプログラムを修了した。2018 年度（平成 30 年度）は受講生の興味関心に合わせられるよう３つのコースを設け、12 歳から 24 歳までの 46 名が 修了した。2019 年度（令和元年度）は更に２つのコースを追加して５つのコースとし、15 歳から 24 歳までの 45 名が修了した。

一部の受講生は海外のイベントに派遣することとしており、2017 年度（平成

29 年度）と 2018 年度（平成 30 年度）は SXSW（South by Southwest）[11]への派遣を実施し、スタートアップ・ベンチャー企業等との交流を図るとともに、ハッカソンに参加し、SXSW Hackathon スポンサー賞を受賞するなどの成果を挙げた。なお、2019 年度（令和元年度）については、イスラエル国家サイバー総局との間で締結したサイバーセキュリティ分野における協力覚書に基づき、修了生がイスラエル関連国際会合へ参画した（項目（３）－④参照）が、COVID-19 の影響により SXSW は中止となっている。

【今後の取組】

NICT において、引き続き、遠隔開発実習、集合イベントにおける座学講座（研究倫理、起業家を招いた講義等）やハッカソンの開催、先端科学技術企業の見学、全国の一流の研究者・技術者との交流、海外派遣、修了生コミュニティの形成等のプログラム内容の充実を図りつつ、継続的にセキュリティイノベーターの育成に取り組む。

④　地域のセキュリティ人材育成

【本文】

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。昨今のサイバー攻撃は地理的な距離に関係なく、弱いところをターゲットとす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。

そのため、本タスクフォースの下に、サイバーセキュリティ人材の育成に関する課題を整理し、その在り方について検討を行うことを目的とする「サイバーセキュリティ人材育成分科会」を 2018 年（平成 30 年）12 月に設置し、2019 年（平成 31 年）６月に第一次取りまとめがなされたところである。

具体的には、地域のサイバーセキュリティに関し、以下の三つの課題が存在する。

１）研修機会の不足

サイバーセキュリティに関する研修や気づきを得る機会は、都市部に集中し

[11] SXSW（South by Southwest）は、毎年３月にアメリカ合衆国テキサス州オースティンで行われる、音楽祭・映画祭・インタラクティブフェスティバルなどを組み合わせた大規模イベントであり、音楽や映画からサイバーセキュリティまで、様々な分野のイベントが開催され、ハッカソンも行われる。

ており、地域での研修機会が少ない状況にある。

２）組織体制の不足

地域の中小企業等では、CISO や CSIRT 等の体制が整っていない場合が多く、特に規模が小さい組織ほど、サイバーセキュリティ体制が整っていない状況にある。

３）就業機会の不足

サイバーセキュリティ関連企業においても人材は不足しており、地域や中小企業向けのビジネスには十分に手が回っていない状況にある。また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なく、地域の人材が地元に根付かない状況にある。

上記の課題認識を踏まえ、以下の施策に取り組む必要がある。

１）地域のセキュリティリーダーの育成

地域の中小企業等にサイバーセキュリティに関する気づきを与えるためのコミュニティ活動を活性化するため、地域でリーダーとなる人材を育成するためのカリキュラムの体系化や研修コンテンツの作成を行うモデル事業を実施する必要がある。

なお、カリキュラムや研修コンテンツの検討にあたっては、サイバーセキュリティだけでなく、中小企業等の経営層の関心を惹く内容を含め、地域の多様なステークホルダーを巻き込むためのノウハウも盛り込むことが必要である。

２）地域でのセキュリティ人材のシェアリング

サイバーセキュリティの専門家や専門組織を、得意分野や知識レベルで細分化してデータベース化した上で、必要とする中小企業等とのマッチングや複数の中小企業等間でのシェアリングのモデル事業を実施することが必要である。

その際、監査やリスクマネジメント経験のあるシニア人材、U・I ターン人材、セカンドキャリアを地域への貢献に活かそうとする人材、産休・育休からキャリア復帰を目指す女性人材などの活用が期待される。

３）地域における人材エコシステムの形成

地域の民間企業等と連携し、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ためのモデル事業を実施することが必

要である。
　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サイバー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。

【進捗状況】

2019 年度（令和元年度）は、総務省において、「地域のセキュリティリーダーの育成」、「地域でのセキュリティ人材のシェアリング」及び「地域における人材エコシステムの形成」について、それぞれ対象地域を特定した上でその有効性を確認するための実証的調査を実施した。【資料 34】

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）の育成については、東海地方を対象地域として実証を行った。具体的には、セキュリティファシリテーターの人材像や求められるスキルといった要件等について検討を行い、当該検討結果に基づき、必要となる研修カリキュラムや研修コンテンツを作成した。また、実際にセキュリティファシリテーターに対する研修を実施し、検討結果や研修コンテンツ等の有効性を確認した。

地域でのセキュリティ人材のシェアリングについては、関西地方を対象地域として実証を行った。具体的には、セキュリティに対する支援を必要とする中小企業等の「利用者」とセキュリティ専門家等の「支援者」を一定数集めた上で、実際にシェアリングシステムを構築し、当該システムを利用したシェアリングについて実証を行った。実証の結果、利用者が求める分野としては、脆弱性診断といった専門的な内容よりも、セキュリティ上の課題抽出や分析等を行うコンサルタント支援が求められていることが判明した。また、中小企業等の多くはそもそもセキュリティ対策に関する問題意識が強くなく、そのようなニーズ自体を自ら把握できていないという状況であり、シェアリングに先んじて前述のセキュリティファシリテーターにより地域の中小企業等にサイバーセキュリティに関する気づきを与えることを優先的に行うことが必要であることを確認した。

地域における人材エコシステムの形成については、沖縄を対象地域として実証を行った。具体的には、都市部で需要が受けきれずに機会逸失しており、かつ遠隔地となる地域でも業務受託が可能な業務である Web アプリケーション診断を対象とし、サイバーセキュリティ人材の入門職でもある Web アプリケーション診断士を育成するための研修カリキュラム・研修コンテンツを作成した。また、Web アプリケーション診断士のスキルバランスを可視化する手法を確立するとともに、実際に研修を行った結果について、当該可視化手法によりその有効性を

確認した。

【今後の取組】

総務省において、2019 年度（令和元年度）の取組結果を踏まえ、地域で自立したサイバーセキュリティ人材の育成が行われる仕組みとなるよう実証的調査を継続するとともに、調査成果を調査対象地域以外でも活用できるよう横展開を進めていく。また、人材の育成に当たっては、セキュリティに知見・関心のある人材の能力を伸ばすだけでなく、地域の中小企業の経営課題、監査やマネジメントに精通している人材にセキュリティに関する知識を身につけてもらうなど、地域の実情に応じた多面的な取組を進めていく。

（３）国際連携の推進

① ASEAN 各国との連携

【本文】

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）～2021 年（令和３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 情報通信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 IoT 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 IoT 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。

【進捗状況】

ASEAN におけるセキュリティ人材の育成支援については、「第 12 回日 ASEAN 情報通信大臣会合」（2017 年（平成 29 年）12 月開催）において、我が国の支援により、ASEAN のサイバーセキュリティ分野の人材育成の強化に向けたプロジェク

トをタイで実施することに合意し、これを受けて 2018 年（平成 30 年）９月に「日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC：ASEAN Japan Cybersecurity Capacity Building Centre)」をタイ・バンコクに設立した。【資料 35】

同センターにおいて ASEAN 各国の政府機関及び重要インフラ事業者のサイバーセキュリティ担当者を対象に実践的サイバー防御演習（CYDER）等を継続的に実施しており、これまでに 300 名以上が参加した。また、同センターでは ASEAN 各国から選抜された若手技術者･学生がサイバー攻撃対処能力を競う「Cyber SEA Game」も開催しており、2019 年（令和元年）11 月に実施した。さらに、AJCCBC の取組を円滑に進めるため、プロジェクト・ステアリング・コミッティーの構成員として必要な支援・助言を行っている。

また、2019 年（令和元年）10 月にタイ・バンコクで開催された「第 12 回日・ASEAN サイバーセキュリティ政策会議」では、この一年間の各国のセキュリティ政策について意見交換を行ったほか、サイバーインシデントへの対処協力、重要インフラ防護の実践事例の共有及びサイバーセキュリティ人材の育成などの協力活動の確認・評価を行った。【資料 36】

2019 年（令和元年）10 月にラオス・ビエンチャンで開催された「第 14 回日 ASEAN 情報通信大臣会合及び第 15 回日 ASEAN 情報通信高級実務者会合」では、今後１年間の日 ASEAN 間の協力・連携施策について、サイバーセキュリティを含めた ICT 分野における更なる連携の実現に向けた「日 ASEAN ICT ワークプラン 2020」がとりまとめられた。

2019 年（令和元年）12 月にタイ・バンコクで開催された「第 10 回 ISP 向け日 ASEAN 情報セキュリティワークショップ」では、日本及び ASEAN の ISP 間で、サイバーセキュリティに関する最新動向、自組織の課題、取組や計画等についての情報共有等を行った。【資料 37】

また、マレーシアにおいて、柔軟なネットワーク制御によりセキュリティ対策をより安価に実施できる SD-WAN 技術とマルウェア検知技術を組み合わせた国産の標的型攻撃対策ソリューションの有効性に関する実証実験をクアラルンプール大学と協力して実施した。

さらに、ミャンマーでは運輸・通信省と連携し、サイバーセキュリティに関するワークショップを開催するなど、ASEAN 加盟国におけるサイバーセキュリティ能力の向上に取り組んでいる。

このほか、インドについては、2020 年（令和２年）３月にデリーにて同国政

府職員向けに CYDER を実施した。

【今後の取組】

AJCCBC におけるサイバーセキュリティ能力構築支援、2020 年（令和２年）10 月に東京で開催される「第 13 回日 ASEAN サイバーセキュリティ政策会議」、同年内にマレーシアで開催予定の「日 ASEAN デジタル大臣会合及び関連会合」及び同年度内に東京で開催予定の、「第 11 回 ISP 向け日 ASEAN 情報セキュリティワークショップ」等を通じて、引き続き ASEAN 加盟国との情報交換・人材育成等における協力関係を強化していく。

② 国際的な ISAC 間連携

【本文】

サイバー攻撃には国境が存在しないため、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、国際連携ワークショップの開催等を通じて、日本の ICT-ISAC と米国の ICT 分野の ISAC との連携をさらに強化し、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。

【進捗状況】

2019 年（令和元年）11 月に東京で開催された「第４回 ISAC 国際連携ワークショップ」では、日米 ISAC 間での情報共有を促進するための具体的方策について議論した。

なお、本ワークショップの開催に合わせて、「サイバーセキュリティ国際シンポジウム」を開催し、総務省、米国国土安全保障省、日米の ISAC 代表者及び米国 NCI（National Council of ISACs）らが、事業者間での情報共有の仕組みや先進的取組事例などを紹介するとともに、より効率的な情報共有の在り方についてパネルディスカッションを実施した。また、本シンポジウムの機会を活用し、

日本の ICT-ISAC と米国の IT-ISAC は、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た覚書に署名した。【資料 38】

【今後の取組】

日米 ISAC 間の脅威情報の効率的な共有をはじめとするサイバーセキュリティ連携対策を更に促進するため、2020 年度（令和２年度）内を目処に「第５回 ISAC 国際連携ワークショップ」を開催する。

③　国際標準化の推進

【本文】

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等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。

【進捗状況】

国内関係機関と連携し、我が国から ISO/IEC JTC1 SC27 及び ITU-T SG17 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」をベースとした勧告・標準の策定に向けて寄与文書を入力するなど、国際標準化の議論に参加・貢献した。

2019 年（令和元年）８月から９月にかけてスイスで開催された ITU-T SG17 会合では、IoT システムのためのセキュリティ管理策に関する勧告案について議論が実施された。

また、2019 年（令和元年）10 月にパリで開催された ISO/IEC JTC1 SC27 会合では、IoT におけるセキュリティ及びプライバシーのためのガイドラインの策定

に向けた議論が実施された。

【今後の取組】

ITU-T SG17 において、引き続き「IoT セキュリティガイドライン」の国際標準化に向けた取組を進める。本ガイドラインの勧告化は 2021 年（令和３年）に完了予定である。

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

【本文】

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、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をし、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。

【進捗状況】

二国間協議については、2019 年（令和元年）9 月にブラジリアで行われた「日ブラジル ICT 共同作業部会」、同年 10 月に東京で行われた「インターネットエコノミーに関する日米政策協力対話」、「日米サイバー対話」、同年 11 月に東京

（遠隔）で行われた「日エクアドル ICT 共同作業部会」、東京で行われた「日露サイバー協議」、ハノイで行われた「日ベトナム ICT 共同作業部会」、同年 12 月に東京で行われた「日 EU・ICT 政策対話」、「日 EU・ICT 戦略ワークショップ」、2020 年（令和２年）１月に東京で行われた「日ウクライナサイバー協議」、「日英サイバー協議」、同年２月に東京で行われた「日独 ICT 政策対話」などを通じて、各国とサイバーセキュリティ政策の共有等を行い、関係強化及び信頼醸成に取り組んだ。

また、2018 年（平成 30 年）11 月にイスラエル国家サイバー総局との間で締結したサイバーセキュリティ分野における協力覚書に基づき、両国間で政策の情報交換を継続するとともに、人材育成に関して SecHack365 修了生がイスラエル関連国際会合へ参画するなど、協力を深化させた。

その他、2019 年（令和元年）11 月にベルリンで開催された IGF への参加など、サイバー空間における国際ルールを巡る議論に積極的に貢献した。

【今後の取組】

政府が主体となる二国間・多国間会合の場や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サイバー空間における国際ルール等のあり方に関する議論に引き続き積極的に参画する。

（４）情報共有・情報開示の促進

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】

【本文】

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等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 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、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。

【進捗状況】

2019 年（平成 31 年）２月より、「NOTICE」プロジェクトにおいて、電気通信事業者間の情報共有の結節点となる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。）の機能を活用し、認定協会経由でパスワード設定等に不備のある IoT 機器に関する情報を ISP に通知しているところであり、更に、5G のサービス開始も見据え、認定協会の活動の活性化に向けた取組を推進しているところである。【資料 10】

また、2020 年度（令和２年度）から全国 5G とローカル 5G が本格的に導入されるが、社会インフラ・産業インフラとしての活用が期待される 5G は、高いセキュリティが要求されるものであり、また、ICT 利活用の裾野が大きく広がることによるサイバーセキュリティリスクの増大が予想される。そのため、5G のリスク情報や脅威情報などについては、個々の事業者又は運用者に閉じるのではなく、相互に情報共有を行い、情報通信ネットワーク・サービス全体のレジリエンスを強化する必要がある。【資料 11】

この点、2020 年（令和２年）２月に、ICT-ISAC において広く 5G セキュリティに係る情報共有を進めることを目的とした「5G セキュリティ推進グループ」が立ち上げられたところであり、今後、5G の事業者や運用者の間で 5G のリスク情報や脅威情報などについて情報共有を行っていくこととしている。

【今後の取組】

総務省において、IoT 機器のセキュリティに関し、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ついて、円滑な実施のための支援を行うなど、取組を促進していく。

また、今後 5G の利活用が進んでいくにつれ、5G に関するセキュリティ対策も重要な取組になってくることから、総務省において、上記の「5G セキュリティ推進グループ」などの情報共有の枠組みを促進していく。

② 事業者間での情報共有を促進するための基盤の構築

【本文】

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、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。

【進捗状況】

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のため、総務省において、2019 年度（令和元年度）から、脆弱性情報をその影響を受けるソフトウェアと紐付けた形で配布する仕組みの検討を実施するとともに、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している。【資料 39】

具体的には、2019 年度（令和元年度）は、IPA にて公表される脆弱性情報を STIX 形式にて情報共有基盤上で共有し資産管理ツール上で紐付けを行う実証を実施するとともに、脆弱性情報を機械学習によって評価する際に必要となる学

習データの生成や利用する機械学習技術の選定を行った上で実証試験を行った。

このほか、日米の ISAC 間の情報共有、連携を進めており、2019 年（令和元年）11 月に東京で開催された「第４回 ISAC 国際連携ワークショップ」では、日米 ISAC 間での情報共有を促進するための具体的方策について議論した。なお、本ワークショップの開催に合わせて、「サイバーセキュリティ国際シンポジウム」を開催し、総務省、米国国土安全保障省、日米の ISAC 関係者及び米国 NCI（National Council of ISACs）らが、事業者間での情報共有の仕組みや先進的取組事例などを紹介するとともに、より効率的な情報共有の在り方についてパネルディスカッションを実施した。また、本シンポジウムの機会を活用し、日本の ICT-ISAC と米国の IT-ISAC は、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た覚書に署名した。【資料 38】

【今後の取組】

これまでの取組の成果を踏まえ、総務省において、引き続き、ICT-ISAC による情報共有に係る取組を促進する。また、情報共有基盤の高度化を図るため、サイバー攻撃に関する情報に加え、脆弱性情報を活用することで早期対策を促進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行う。

③　サイバーセキュリティ対策に係る情報開示の促進

【本文】

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、こうした取組をさら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。

このような状況を踏まえ、2017 年（平成 29 年）12 月より本タスクフォースの下に「情報開示分科会」を設置し、民間企業の情報開示の促進に向けた議論を実施してきたところであり、2018 年（平成 30 年）６月に報告書を公表したところである。

当該報告書を受け、まずは、民間企業のサイバーセキュリティ対策の自主的な情報開示を促進する観点から、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。

今後は民間企業の情報開示を促進するため、本手引きを策定して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。

【進捗状況】

2019 年度（令和元年度）においては、上記の「サイバーセキュリティ対策情報開示の手引き」の公表後も企業等において様々なインシデントが発生しているところであり、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。【資料 40】

そのため、今後は、各企業のみならず、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においても情報開示の取組が進んでいくことが期待される。この点、例えば、一般社団法人日本 IT 団体連盟においては、サイバーセキュリティに関する第三者評価や自己評価などの公開情報などを基に企業のサイバーセキュリティ対策の総合評価などを行う取組が始まっているところである。こうした取組を通じ、企業のサイバーセキュリティ対策について、ステークホルダーへ咀嚼された情報の伝達と比較可能性の提供がなされ、ステークホルダーからの評価を受ける企業のセキュリティレベルの向上に資することが期待される。

【今後の取組】

総務省において、引き続き、「サイバーセキュリティ対策情報開示の手引き」の普及等に努める。

④　サイバーセキュリティ対策に係る投資の促進

【本文】

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、一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により、生産性を向上させる取組について、それに必要となるシステムや、センサー・ロボット等の導入を支援する税制措置（コネクテッド・インダストリーズ税制）が 2018 年（平成 30 年）に創設され、2020 年（令和２年）までの

３年間の適用期間で運用されているところである。
そのため、当該税制措置の活用状況を把握・分析しつつ、必要に応じ、企業のニーズ等を反映したサイバーセキュリティ対策に係る投資の促進のための政策支援の在り方について検討を行うことが期待される。

【進捗状況】

本税制措置について、2020 年（令和２年）２月末時点の認定事業社数は 154 社である。なお、本税制措置は 2019 年度（令和元年度）で終了となっている。

また、5G 及びローカル 5G について、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、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を行うことを目的とした「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案」が 2020 年（令和２年）２月に閣議決定された。

【今後の取組】

5G 及びローカル 5G については、総務省において、経済産業省と連携し、「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案」の成立に向け尽力するとともに、成立後には、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。

⑤　国際的な ISAC 間連携【再掲】

【本文】
アジアサイバー攻撃には国境が存在しないため、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、国際連携ワークショップの開催等を通じて、日本の ICT-ISAC と米国の ICT 分野の ISAC との連携をさらに強化し、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。

【進捗状況】

2019 年（令和元年）11 月に東京で開催された「第４回 ISAC 国際連携ワークショップ」では、日米 ISAC 間での情報共有を促進するための具体的方策について議論した。

なお、本ワークショップの開催に合わせて、「サイバーセキュリティ国際シンポジウム」を開催し、総務省、米国国土安全保障省、日米の ISAC 代表者及び米国 NCI（National Council of ISACs）らが、事業者間での情報共有の仕組みや先進的取組事例などを紹介するとともに、より効率的な情報共有の在り方についてパネルディスカッションを実施した。また、本シンポジウムの機会を活用し、日本の ICT-ISAC と米国の IT-ISAC は、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た覚書に署名した。【資料 38】

【今後の取組】

日米 ISAC 間の脅威情報の効率的な共有をはじめとするサイバーセキュリティ連携対策を更に促進するため、2020 年度（令和２年度）内を目処に「第５回 ISAC 国際連携ワークショップ」を開催する。

Ⅳ　今後の進め方

本プログレスレポートにおいて総合政策の各施策の進捗の管理及び検証を行ったが、現在、タスクフォースにおいてもサイバーセキュリティ政策の在り方に関する議論を行っており、本プログレスレポートの結果も適切に反映させていくこととする。

その上で、総務省において、2018 年（平成 30 年）7 月に新たに策定された「サイバーセキュリティ戦略」も踏まえつつ、NISC や経済産業省をはじめ、関係府省庁との連携の下、IoT・5G などのセキュリティ対策の強化を進めていくこととを期待する。

参考資料

IoT・5Gセキュリティ総合対策（令和元年8月公表）

■ ICTの利活用が一層進展していく中で、5Gのサービスの開始、データ管理・流通の重要性やサプライチェーンリスクへの対応などの必要性が増大していること等を踏まえ、IoT・5G時代にふさわしいサイバーセキュリティ対策の在り方について検討し、総務省として取り組むべき課題を「IoT・5Gセキュリティ総合対策」として策定し令和元年8月に公表（※）。

● 直近で留意すべき事項

1 5Gのサービス開始に伴う新たなリスク
- ✓ 仮想化、ソフトウェア化、モバイルエッジコンピューティング
- ✓ 産業用途でのIoT機器の設置・運用

2 サプライチェーンリスクの管理の重要性
- ✓ ICTの製品・サービスの製造・流通過程でのリスク
- ✓ 委託先が踏み台となって攻撃を受けるケース

3 Society5.0の実現に向けたデータの流通・管理の重要性
- ✓ クラウドサービスやスマートシティなどのセキュリティの確保の重要性
- ✓ トラストサービスの必要性

4 サイバーセキュリティにおけるAI利活用の重要性
- ✓ AIの活用が進展する中で、特にAIを利活用したサイバーセキュリティ対策を促進することが必要

5 大規模な量子コンピュータの実用化の可能性
- ✓ 将来の大規模な量子コンピュータの実用化の可能性を踏まえ、現時点から新たな推奨暗号の在り方について検討の必要性

6 大規模な国際イベント等の開催
- ✓ ラグビーワールドカップや東京オリンピック・パラリンピック大会の円滑な実施、及びその後も見据え、対策の着実な実施が必要

● IoT・5Gセキュリティ総合対策の枠組み

重点的に対応すべき情報通信サービス・ネットワークの個別分野等に関する具体的施策
- ✓ IoT、5G、クラウドサービス、スマートシティのセキュリティ　など
- ✓ トラストサービスの在り方の検討　など

具体的施策間でも連携

連携 ↕ 連携 ↕ 連携 ↕ 連携 ↓

研究開発	人材育成 普及啓発	情報共有 情報開示	国際連携
✓ ハードウェア脆弱性 ✓ AI ✓ 暗号 など	✓ 2020東京大会向け人材育成 ✓ 地域の人材育成 など	✓ 情報共有基盤 ✓ 情報開示の促進 など	✓ ASEAN各国との連携 ✓ 国際標準化 など

（※）これに先立ち、2017年（平成29年）には、IoT機器・システムのセキュリティ等の確保を主眼においた「IoTセキュリティ総合対策」を策定・公表

我が国のサイバーセキュリティ強化に向け早期に取り組むべき事項［緊急提言］【資料2】

■ サイバーセキュリティタスクフォースにおける「IoT・5Gセキュリティ総合対策」の策定・公表後の議論を踏まえ、2020年７月より開催される予定であった2020年東京大会に向けた対処として早急に取り組むべき事項を整理・公表（2020年１月28日）

1 IoT機器のセキュリティ対策の拡充

- ✓ 脆弱な状態にあるIoT機器について注意喚起方法の一層の改善を図ることが必要
- ✓ 重要施設に設置されているIoT機器に対して新たに注意喚起を実施することが必要

2 地方公共団体向け実践的サイバー防御演習（CYDER）の繰り上げ実施等

- ✓ 2020年東京大会前に未受講の地方公共団体を中心としてCYDERの集中的な受講機会を設けることが必要
- ✓ CYDERのオンライン受講を早期に開始することが必要

3 サイバーセキュリティに関する情報共有体制の強化

- ✓ 個人情報などの流出が疑われる時点で、速やかにインシデントに関する情報の公表を検討することが望ましい
- ✓ 類似の被害の拡大を防ぐ観点から、インシデントに関する情報の共有を速やかに行うことが求められる
- ✓ 先行的に始まったISACの知見やノウハウの展開を通じて、重要インフラ分野等におけるISACの立ち上げを促進することが必要

4 公衆無線LANのセキュリティ対策

- ✓ 公衆無線LANサービスの利用者及び提供者に対し、公衆無線LANのセキュリティ対策の状況や自ら講じるべきセキュリティ対策の周知を強化するため、ガイドラインを年度内に改定し、ホテル、病院、学校等への周知を強化することが必要

5 制度的枠組みの改善

- ✓ サイバーセキュリティ対策等の法令への位置づけや、官民のガイドラインや基準について周知し、対応の強化を呼びかけていくことが必要
- ✓ 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
- ✓ 各地方公共団体における情報セキュリティ対策及び緊急時連絡体制の確保等の徹底を図ることが必要

「サイバーセキュリティ戦略」の全体概要

【資料3】

中長期的

戦略期間

1　策定の趣旨・背景

1．1．　サイバー空間がもたらすパラダイムシフト（サイバー空間では、創意工夫で活動を飛躍的に拡張できる。人類がこれまでに経験したことのないSociety5.0へのパラダイムシフト）

1．2．　2015年以降の状況変化（サイバー空間と実空間の一体化の進展に伴う脅威の深刻化、2020年東京大会等を見据えた新たな戦略の必要性）

2　サイバー空間に係る認識

2．1．　サイバー空間がもたらす恩恵

・人工知能（AI）、IoT※などサイバー空間における知見や技術、サービスが社会に定着し、既存構造を覆すイノベーションを牽引。**様々な分野で当然に利用**され、人々に豊かさをもたらしている。

※：Internet of Thingsの略

2．2．　サイバー空間における脅威の深刻化

・技術等を**制御できなくなるおそれは常に内在**。IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、多大な経済的・社会的な損失が生ずる可能性は拡大

3　本戦略の目的

3．1．　**基本的な立場の堅持**

（1）基本法の目的（2）基本的な理念（「自由、公正かつ安全なサイバー空間」）（3）基本原則（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）

3．2．　目指すサイバーセキュリティの基本的な在り方

（1）目指す姿（**持続的発展のためのサイバーセキュリティ（「サイバーセキュリティエコシステム」）の推進**）（2）主な観点（①サービス提供者の**任務保証**、②**リスクマネジメント**、③**参加・連携・協働**）

4　目的達成のための施策

経済社会の活力の向上及び持続的発展

1．新たな価値創出を支えるサイバーセキュリティの推進

＜施策例＞・**経営層の意識改革の促進（「費用」から「投資」へ）**
・投資に向けたインセンティブ創出（情報発信・開示による市場の評価、保険の活用）
・セキュリティ・バイ・デザインに基づくサイバーセキュリティビジネスの強化

2．多様なつながりから価値を生み出すサプライチェーンの実現

＜施策例＞・**中小企業を含めたサプライチェーン（機器・データ・サービス等の供給網）におけるサイバーセキュリティ対策指針の策定**

3．安全なIoTシステムの構築

＜施策例＞・IoTシステムにおけるセキュリティの体系の整備と国際標準化
・**IoT機器の脆弱性対策モデルの構築・国際発信**

等

国民が安全で安心して暮らせる社会の実現

1．国民・社会を守るための取組

＜施策例＞・脅威に対する事前の防御（**積極的サイバー防御**）策の構築
・サイバー犯罪への対策

2．官民一体となった重要インフラの防護

＜施策例＞・安全基準等の改善・浸透（サイバーセキュリティ対策の**関係法令等における保安規制としての位置付け**）
・地方公共団体のセキュリティ強化・充実

3．政府機関等におけるセキュリティ強化・充実

＜施策例＞・**情報システムの状態のリアルタイム管理の強化**
・先端技術の活用による先取り対応への挑戦

4．大学等における安全・安心な教育・研究環境の確保

＜施策例＞・**大学等**の多様性を踏まえた対策の推進

5．2020年東京大会とその後を見据えた取組

＜施策例＞・**サイバーセキュリティ対処調整センターの構築の推進**
・成果のレガシーとしての活用

6．従来の枠を超えた情報共有・連携体制の構築

＜施策例＞・**多様な主体の情報共有・連携の推進**

7．大規模サイバー攻撃事態等への対処態勢の強化

＜施策例＞・**実空間とサイバー空間の双方の危機管理に臨むための大規模サイバー攻撃事態等への対処態勢の強化**

等

国際社会の平和・安定及び我が国の安全保障

1．自由、公正かつ安全なサイバー空間の堅持

＜施策例＞・**自由、公正かつ安全なサイバー空間**の理念の発信
・サイバー空間における法の支配の推進

2．我が国の防御力・抑止力・状況把握力の強化

＜施策例＞・国家の**強靭性の確保**（①任務保証、②我が国の先端技術・防衛関連技術の防護、③サイバー空間を悪用したテロ組織の活動への対策）
・サイバー攻撃に対する**抑止力の向上**（①実効的な抑止のための対応、②信頼醸成措置）
・サイバー空間の**状況把握の強化**（①関係機関の能力向上、②脅威情報連携）

3．国際協力・連携

＜施策例＞・**知見の共有・政策調整**
・事故対応等に係る国際連携の強化
・能力構築支援

等

横断的施策

人材育成・確保	＜施策例＞**戦略マネジメント層の育成・定着**、実務者層・技術者層の育成（**高度人材**含む）、人材育成基盤の整備、**政府人材**の確保・育成の強化、国際連携の推進
研究開発の推進	＜施策例＞実践的な研究開発の推進（**検知・防御等の能力向上、不正プログラム等の技術的検証**を行うための体制整備）、**AI等**中長期的な技術・社会の進化を視野に入れた対応
全員参加による協働	＜施策例＞サイバーセキュリティの普及啓発に向けた**アクションプランの策定、国民への情報発信**（サイバーセキュリティ月間の充実等）、サイバーセキュリティ教育の推進

5　推進体制

本戦略の実現に向け、サイバーセキュリティ戦略本部の下、**内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化**を図るとともに、同センターが、各府省庁間の総合調整、産学官民連携の促進の要となる主導的役割を担う。**施策が着実かつ効果的に実施されるよう必要な予算の確保と執行を図る。**　等

IoT機器のセキュリティ対策に関する技術基準の改正

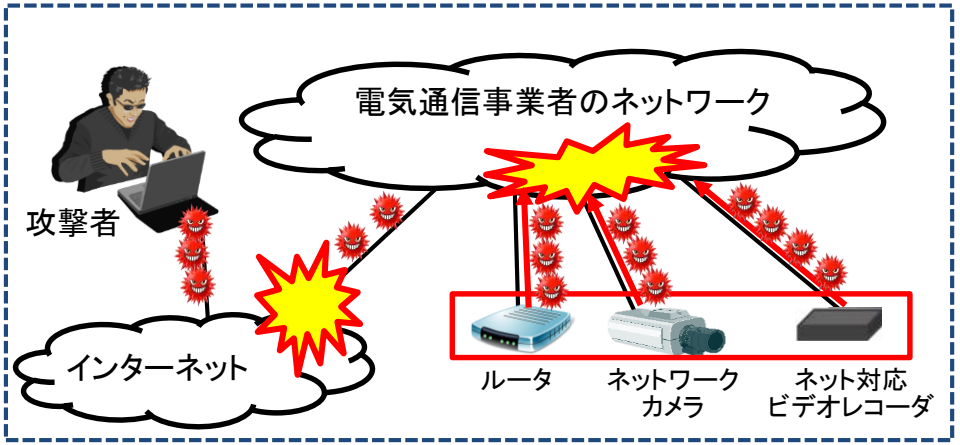
【資料4】

【背景・課題】

- 近年、インターネットにつながるWebカメラやルータ等のIoT機器を悪用したサイバー攻撃により、通信網に深刻な障害を及ぼす事案※1が発生。
- その原因としては、パスワード設定の不備などによりIoT機器を悪用されるケースが多く、その対策が重要な課題。

※1　2016年10月、「Mirai」というマルウェアに感染した10万台を超えるIoT機器が、米国のDyn(ダイン)社のシステムを攻撃し、Dyn社のサーバーを利用していた数多くの大手インターネットサービスやニュースサイトに障害が発生。

＜IoT機器が乗っ取られてサイバー攻撃に悪用される事案のイメージ＞



【端末設備等規則（省令）の改正概要】

- 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、以下の機能を具備することを技術基準（端末設備等規則）に追加する。

  ①アクセス制御機能※1（例えばアクセス制限をかけてパスワード入力を求め、正しいパスワードの入力時のみ制限を解除する機能のこと）

  ②初期設定のパスワードの変更を促す等の機能

  ③ソフトウェアの更新機能※1

  又は①～③と同等以上の機能※2

  ※1 ①と③の機能は、端末が電源オフになった後、再び電源オンに戻った際に、出荷時の初期状態に戻らず電源オフになる直前の状態を維持できることが必要。
  ※2 同等以上の機能を持つものとしては、国際標準ISO/IEC15408に基づくセキュリティ認証(CC認証)を受けた複合機等が含まれる。

- 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セキュリティ対策の対象外とする。

【改正省令施行までの動き】

- 2020年４月１日の改正省令施行に向けて、2019年３月１日に改正省令公布、同年４月22日に改正省令の運用方法や解釈等を示したガイドラインを公表。これに加え、随時、周知や問合せ等に対応。

（一社）重要生活機器連携セキュリティ協議会（CCDS）認証プログラム 【資料5】

- 一般社団法人重要生活機器連携セキュリティ協議会（CCDS）は、**IoT機器のセキュリティ要件**を定め、2019年10月から認証プログラム（**民間の任意認証**）を開始。
- 認証の対象はソフトウェアを含むIoT機器で、認証されたものにはCCDS**マーク**（レベル１～３の３段階）を付与。
- マーク付与製品には**サイバー保険**が自動付帯され、インシデント発生時の原因調査等の費用を保険で保証。

IoTセキュリティ要件

✓11のセキュリティ要件を定め、脆弱性に対応

1 SQLインジェクション
2 クロスサイトサイトリクエストフォージェリ
3 パストラバーサル
4 不要サービスポートの解放
5 オープンサービスポートの不適切なアクセス管理（機器毎にユニークなID/パスワードでの管理等）
6 アクセスコードの不適切な実装（ID/パスワードのハードコーディングや変更不可等）
7 廃棄やリユースを想定した機能実装不備
8 Wi-Fiアライアンス推奨の最新の認証方式が不備
9 BluetoothSIG推奨の最新のペアリング方式が不備
10 USBの不要なクラスの利用
11 ソフトウェアアップデートできない

認証プログラムのマーク（CCDSマーク）

✓消費者にも分かりやすいよう、★の数で対策レベルを表示

✓レベル１はIoT機器共通の要件、レベル２・３は分野別に策定
（2020年３月時点で、レベル１について実施しており、レベル２・３は準備中）

（出典：CCDS記者発表会(2019年10月30日)資料

【(一社)重要生活機器連携セキュリティ協議会（CCDS：Connected Consumer Device Security council について】

一般社団法人 重要生活機器連携セキュリティ協議会
CCDS Connected Consumer Device Security Council

- 民生機器を中心としたIoT機器やサービスのセキュリティ向上を目指す産学連携の協議会
- 生活機器に関する国内外の動向調査や、セキュリティ設計プロセスの開発等を実施
- 2014年に設立され、大学・企業・団体等の209会員（2020年4月時点）

（一社）デジタルライフ推進協会（DLPA）推奨Wi-Fiルータ

- 一般社団法人デジタルライフ推進協会（DLPA）は、出荷時からセキュリティ対策機能が搭載されている家庭用Wi-Fiルーターを「**DLPA推奨Wi-Fiルータ**」として推奨。
- DLPA加盟社のうち４社※がDLPA推奨Wi-Fiルーターを販売中。

※(株)アイ・オー・データ機器、NECプラットフォームズ(株)、エレコム(株)、(株)バッファロー

DLPA推奨Wi-Fiルータ

以下の２つのセキュリティ対策機能を出荷時から搭載。

① ファームウェアの自動更新

② １台ごとに固有の管理画面用ログインID又はパスワードを設定

（出典：DLPAウェブサイト https://dlpa.jp/wifi_support/）

【(一社)デジタルライフ推進協会（DLPA：Digital Life Promotion Association）について】

一般社団法人 デジタルライフ推進協会 Digital Life Promotion Association

- デジタル技術の進歩により可能となる新たなデジタル技術の活用形態＝「デジタルライフ」における利用者の利便性を守り、その健全な発展に寄与することを目的として、2010年に設立
- デジタルライフの普及・啓発活動や業界共通仕様の策定等を実施
- Wi-Fiルータや外付けハードディスク等のデジタル機器のメーカが加盟

スマートシティにおけるセキュリティの検討の枠組み

【資料7】

■　政府全体のスマートシティの取組と連動する形でスマートシティのセキュリティの在り方について検討を実施。

政府全体の取組

アーキテクチャ検討会議【官】

（事務局：内閣府、座長：越塚登　東京大学教授）

目的：分野・企業横断のデータ連携、他都市・地域への展開、国際標準化等に資する**アーキテクチャ**を検討

検討の内容を共有　⇩　⇧　事務局オブザーバ出席

スマートシティ官民連携プラットフォーム【官民】

（令和元年８月８日設置）

（事務局：内閣府、国土交通省、**総務省**、経済産業省）

目的：官民が一体となって全国各地のスマートシティの取組を推進

会員：スマートシティ関連事業実施団体　等
（コンソーシアム・協議会(78)、地方公共団体(113)、企業・大学・研究機関等(356)、関係府省(11)、経済団体(2)）
（数字は令和元年12月末時点）

＜活動内容＞

スマートシティ関連事業の効果的な推進・重点支援	**分科会（※）の開催**（令和元年11月時点で８個）
企業、大学・研究機関、地方公共団体等の間のマッチング等支援	国内外への普及促進活動

総務省の取組（セキュリティ関連）

スマートシティのセキュリティの検討

- 内閣府で検討中（SIP事業）の**スマートシティのアーキテクチャを踏まえ**、関係省庁等と連携し、**スマートシティのセキュリティの在り方**について検討する調査研究を実施中

検討の内容を共有　⇩　⇧　フィードバック

スマートシティセキュリティ・セーフティ分科会

（令和２年１月活動開始）

（事務局：**総務省**、(株)ラック、(一社)オープンガバメント・コンソーシアム）

目的：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しつつ、実装していくための方策について検討する。

メンバー：13者（令和２年２月時点）

総務省、(株)ラック、(一社)オープンガバメント・コンソーシアムのほか、地方公共団体、印刷会社、機器メーカ、損害保険会社、不動産デベロッパー、セキュリティベンダー　など

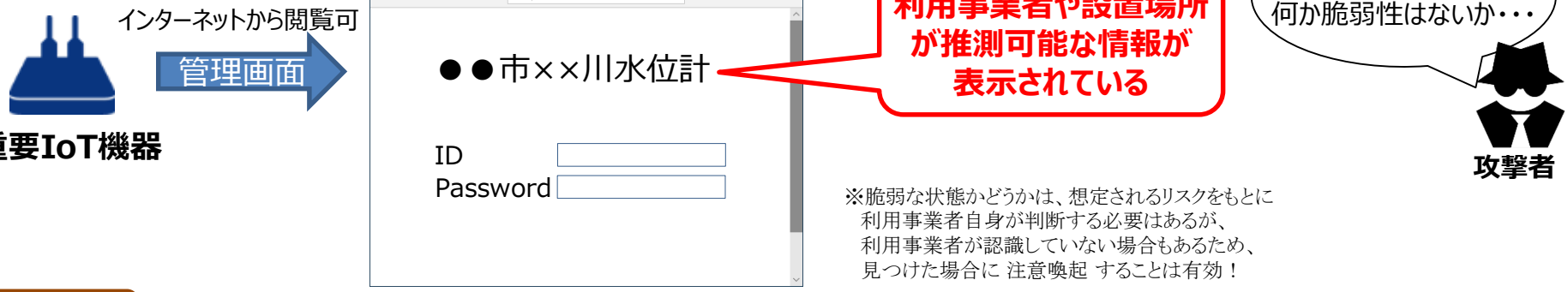
（参考）スマートシティビジョンの検討および地域へのスマートシティ普及促進分科会

（事務局：内閣府）

重要IoT機器のセキュリティ対策

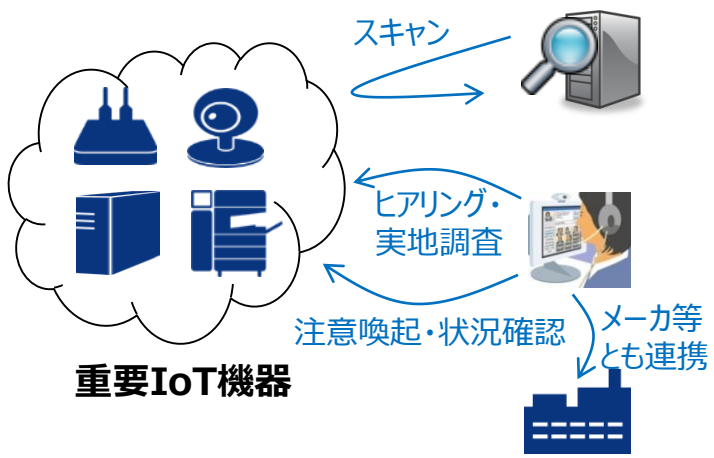
- 重要インフラ等の社会的に影響を及ぼすリスクを伴った使用をしているIoT機器（**重要IoT機器**）について、**公開する必要のない情報が公開されている**など、攻撃を受けやすい**脆弱な状態**にあるものを**検出**する。
- 検出した重要IoT機器について、利用事業者に対して**設定状況等のヒアリング**を行った上で、脆弱な状態を解消するための**注意喚起**や**対策手法の提示**を行い、**対策の完了までのトレース**を行う。

脆弱な状態の例



※脆弱な状態かどうかは、想定されるリスクをもとに利用事業者自身が判断する必要はあるが、利用事業者が認識していない場合もあるため、見つけた場合に 注意喚起 することは有効！

対策スキーム



重要IoT機器探索	重要IoT機器？ Web画面が見える？
利用者特定	画面の事業者名は？
利用環境調査	どのような用途か？ どのような設定・管理をしているか？ どのようなネットワーク環境で使っているか？
注意喚起実施	想定されるリスクはどのようなものか 対策にはどのようなものが有効か
対策状況確認	対策の実施に当たり問題はないか？

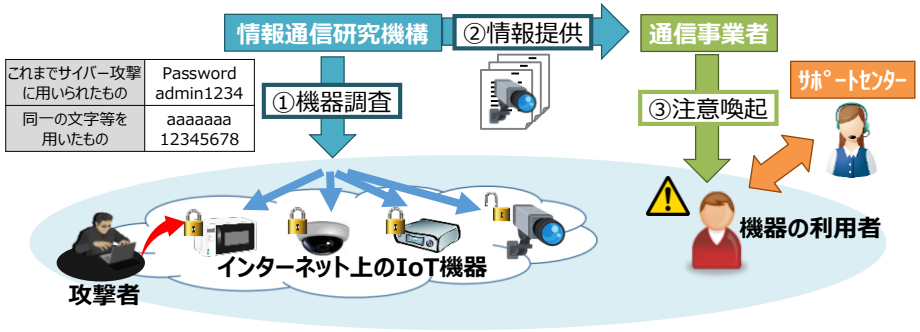
IoT機器調査及び利用者への注意喚起（NOTICE等）

- 情報通信研究機構（NICT）が**サイバー攻撃に悪用されるおそれのあるIoT機器**を調査し、インターネットプロバイダを通じた利用者への注意喚起を行う取組「**NOTICE**」を2019年２月より実施。
- NOTICEの取組に加え、**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、インターネットプロバイダから利用者へ注意喚起を行う取組を2019年６月より開始。

（１）NOTICEプロジェクトの推進

（調査対象）パスワード設定等に不備があり、サイバー攻撃に悪用されるおそれのあるIoT機器

① NICTがインターネット上のIoT機器に、容易に推測されるパスワードを入力することなどにより、サイバー攻撃に悪用されるおそれのある機器を特定。
② 当該機器の情報をインターネットプロバイダ（ISP）に通知。
③ ISPが当該機器の利用者を特定し、注意喚起を実施。



2020年３月までの取組結果

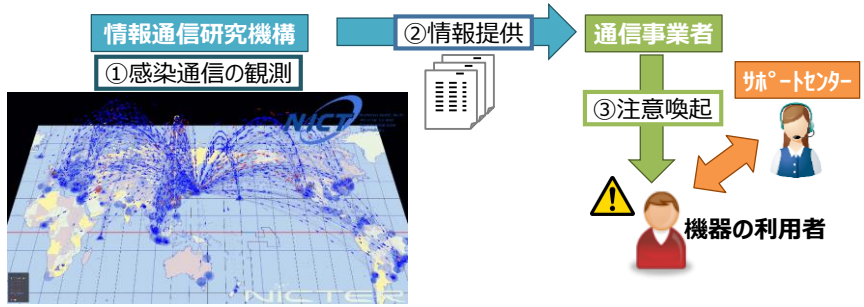
ID・パスワードが入力可能であったもの　約100,000件（直近での調査）

上記の内、ID・パスワードによりログインでき、注意喚起の対象となったもの　延べ2,249件

（２）マルウェアに感染しているIoT機器の利用者への注意喚起の推進

（調査対象）既にMirai等のマルウェアに感染しているIoT機器

① NICTが「NICTER」プロジェクトにおけるダークネット※に向けて送信された通信を分析することでマルウェアに感染したIoT機器を特定。
※NICTがサイバー攻撃の大規模観測に利用しているIPアドレス群
② 当該機器の情報をインターネットプロバイダ（ISP）に通知。
③ ISPが当該機器の利用者を特定し、注意喚起を実施



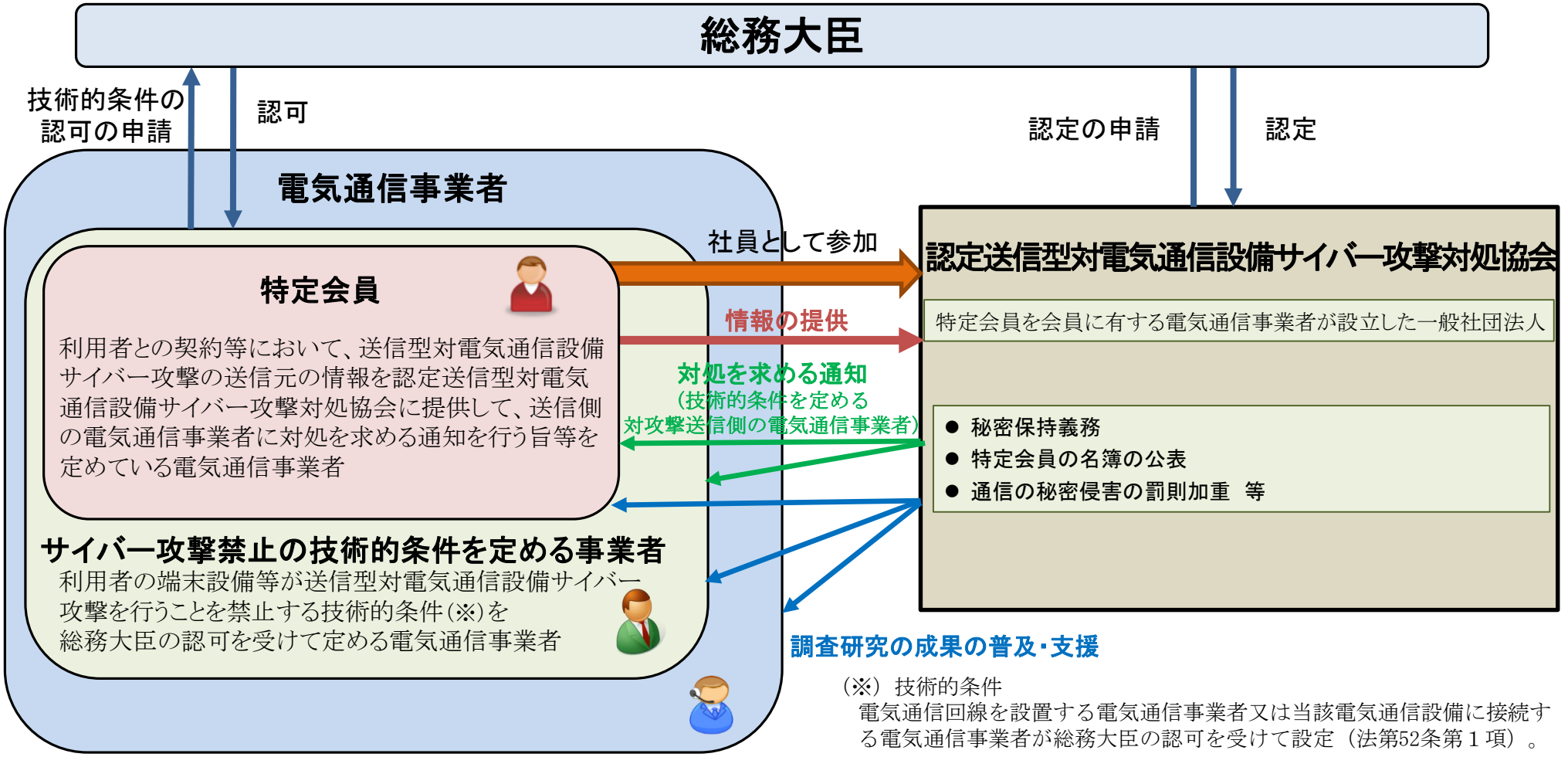
2020年３月までの取組結果

ISPに対する通知の対象となったもの　平均162件（１日当たり）

※50社（約1.1億IPアドレス）を対象に調査

認定送信型対電気通信設備サイバー攻撃対処協会制度の概要【資料10】

- 2018年（平成30年）5月23日に公布された改正電気通信事業法において、電気通信事業者がDDoS攻撃等のサイバー攻撃への対応を共同して行うため、サイバー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を総務大臣が認定する制度を創設。
- 当該第三者機関である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）については2019年（平成31年）1月に、総務大臣により一般社団法人ICT-ISACが認定。



（※）技術的条件
電気通信回線を設置する電気通信事業者又は当該電気通信設備に接続する電気通信事業者が総務大臣の認可を受けて設定（法第52条第１項）。

第5世代移動通信システム（5G）について

■ 第5世代移動通信システム（5G）は、超高速、超低遅延、多数同時接続を実現する新たな社会インフラとして期待されている一方、そのセキュリティの在り方についても引き続き検討していくことが必要。

5Gは、AI/IoT時代のICT基盤

低遅延

移動体無線技術の
高速・大容量化路線

2G　3G　4G

同時接続

5G

超高速

現在の移動通信システムより100倍速いブロードバンドサービスを提供

⇒ **２時間の映画を３秒でダウンロード**

超低遅延

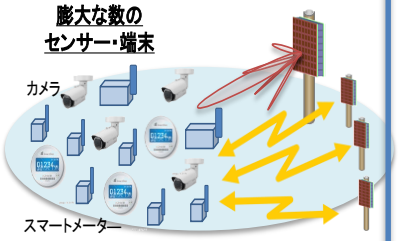
利用者が遅延（タイムラグ）を意識することなく、リアルタイムに遠隔地のロボット等を操作・制御

ロボットを遠隔制御

⇒ **ロボット等の精緻な操作をリアルタイム通信で実現**

多数同時接続

スマホ、PCをはじめ、身の回りのあらゆる機器がネットに接続



⇒ **自宅部屋内の約100個の端末・センサーがネットに接続**
（現行技術では、スマホ、PCなど数個）

社会的なインパクト大

新たな社会インフラへ

ローカル5Gの概要

- ローカル5Gは、地域や産業の個別のニーズに応じて**地域の企業や自治体等の様々な主体が、自らの建物内や敷地内でスポット的に柔軟に構築**できる5Gシステム。
  一部の周波数帯で先行して**2019年12月に制度化**。

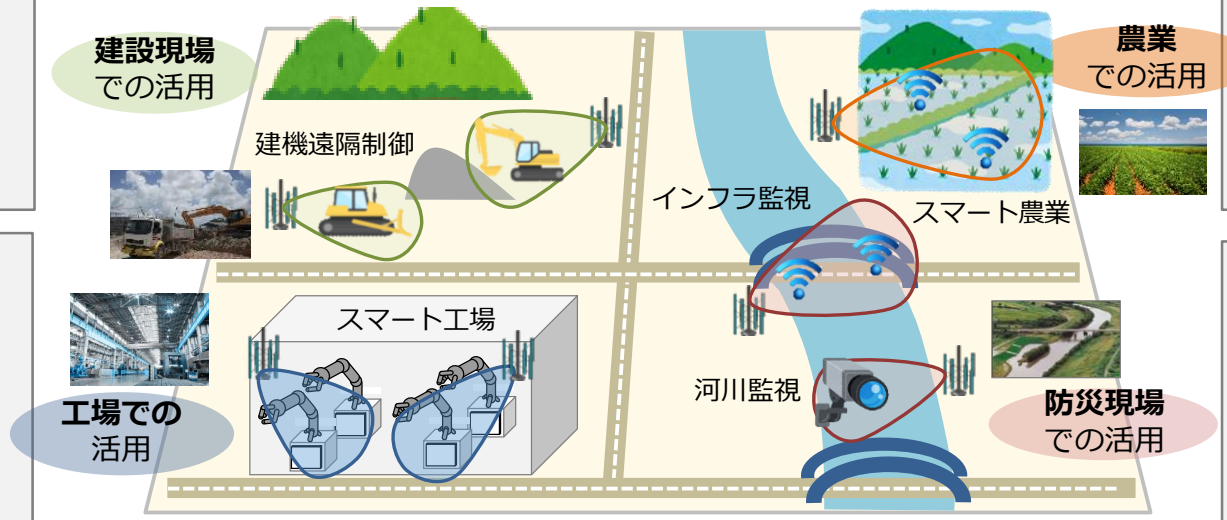
<他のシステムと比較した特徴>

- 携帯事業者の５Ｇサービスと異なり、
  - 携帯事業者によるエリア展開が遅れる地域において５Ｇシステムを**先行して構築**可能。
  - 使用用途に応じて**必要となる性能を柔軟に設定**することが可能。
  - **他の場所の通信障害や災害などの影響を受けにくい。**
- Wi-Fiと比較して、**無線局免許に基づく安定的な利用が可能。**

ゼネコンが建設現場で導入
建機遠隔制御

事業主が工場へ導入
スマートファクトリ

建物内や敷地内で自営の5Gネットワークとして活用



農家が農業を高度化する
自動農場管理

自治体等が導入
河川等の監視

5Gネットワークのセキュリティ確保に向けた体制整備

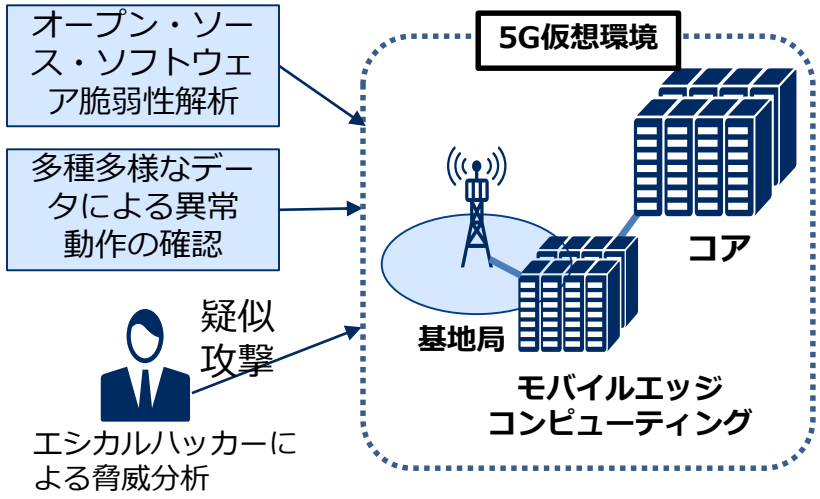
【資料13】

- 国民の安全・安心の確保に向け、5G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（2019年度開始）を行うことを通じ、5Gネットワークのセキュリティを総合的かつ継続的に担保できる仕組みを整備。また、事業の成果は関係者へ共有のうえ、周知・啓発と実際の対策の推進を図る。

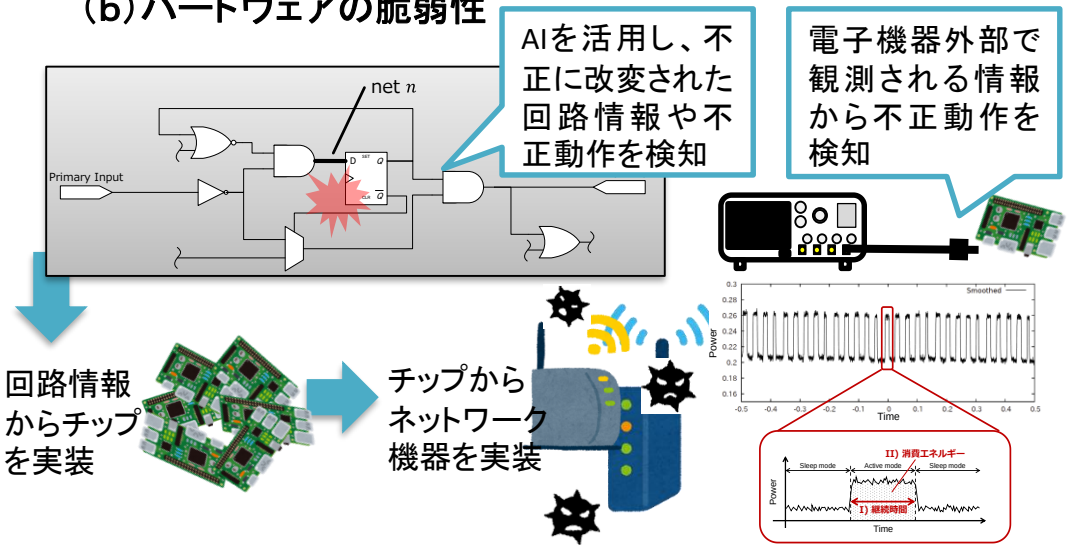
(a) ソフトウェアを中心としたネットワークの脆弱性: 5Gの通信インフラとしての機能保証のため、ソフトウェアにより構成される部分を含め、ネットワーク全体のセキュリティを確保する必要があるため、5G仮想環境を構築し、①オープンソースソフトウェア等の解析、②多種多様なパターンのデータ入力による異常動作確認（ファジング）、③エシカルハッカーによる脆弱性調査、脅威分析を実施・対策を検討。

(b) ハードウェアの脆弱性：5G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のリスクに対応するため、①AIを活用し回路情報から不正に改変された回路を検知する技術や、②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・対策を検証。また、③5Gネットワーク上での運用面の課題等について検討。

(a)ソフトウェアを中心としたネットワークの脆弱性



(b)ハードウェアの脆弱性



政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組み【資料14】

■ サイバーセキュリティ戦略本部第23回会合において、①本制度の基本的な枠組み、②本制度の利用の考え方、③本制度の所管と運営体制を決定。

令和２年１月３０日　サイバーセキュリティ戦略本部決定

１．本制度の基本的な枠組み

本制度で定められた評価プロセスに基づいて、要求する基準に基づいたセキュリティ対策を実施していることが確認されたクラウドサービスを、本制度が公表するクラウドサービスリストに登録。

２．各政府機関等における本制度の利用の考え方

各政府機関は、クラウドサービスを調達する際は本制度において登録されたサービスから調達することを原則とし、本制度における登録がないクラウドサービスの調達や、経過措置の詳細は、サイバーセキュリティ対策推進会議、各府省情報化統括責任者（CIO）連絡会議において定める。

３．本制度の所管と運用体制

本制度の所管は内閣官房（NISC、IT室）・総務省・経済産業省とし、本制度の最高意思決定機関として、有識者と所管省庁を構成員とした制度運営委員会を設置し、事務局をNISCに置く。

事務局は、本制度の運用状況について、サイバーセキュリティ戦略本部に報告を行う。

本制度の運用に当たっては、（中略）独立行政法人情報処理推進機構（以下「IPA」という。）において、制度運用係る実務及び評価に係る技術的な支援を行うものとする。ただし、IPAは制度運用のうち、監査機関の評価及び管理に関する業務については、（中略）情報セキュリティ監査制度及び監査機関の質の確保に精通した民間団体に、（中略）委託すること。

データ利活用型スマートシティ推進事業

（総務省の事業内容）

○　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地方公共団体等の初期投資・継続的な体制整備等にかかる経費の一部を補助する。

（政府一体となった推進）

○　統合イノベーション戦略推進会議の下に設置されたスマートシティ・タスクフォースにおいて、基本原則（共通アーキテクチャ等）を取りまとめ、関係府省はそれを踏まえて事業を推進。

○　地方公共団体等からの補助金の公募や交付先に対する実地支援などを関係府省と共同で実施する。

○補助対象:地方公共団体等
○補助率:1／2
○平成29年度から開始
○予算額:5.1億円の内数（平成29年度）
　　2.5億円（平成30年度）
　　2.2億円（令和元年度）
　　2.2億円（令和2年度予算）

国内の事例:

○札幌市（分野:観光、交通、健康）
人流情報と購買情報を活用したマーケティング、走行情報を活用した除排雪最適化、行動情報から健康増進情報のpush配信等を実施。

○高松市（分野:防災、観光）
水位情報の可視化による行政の災害対応の効率化、動態データの活用による観光マーケティング等を実施

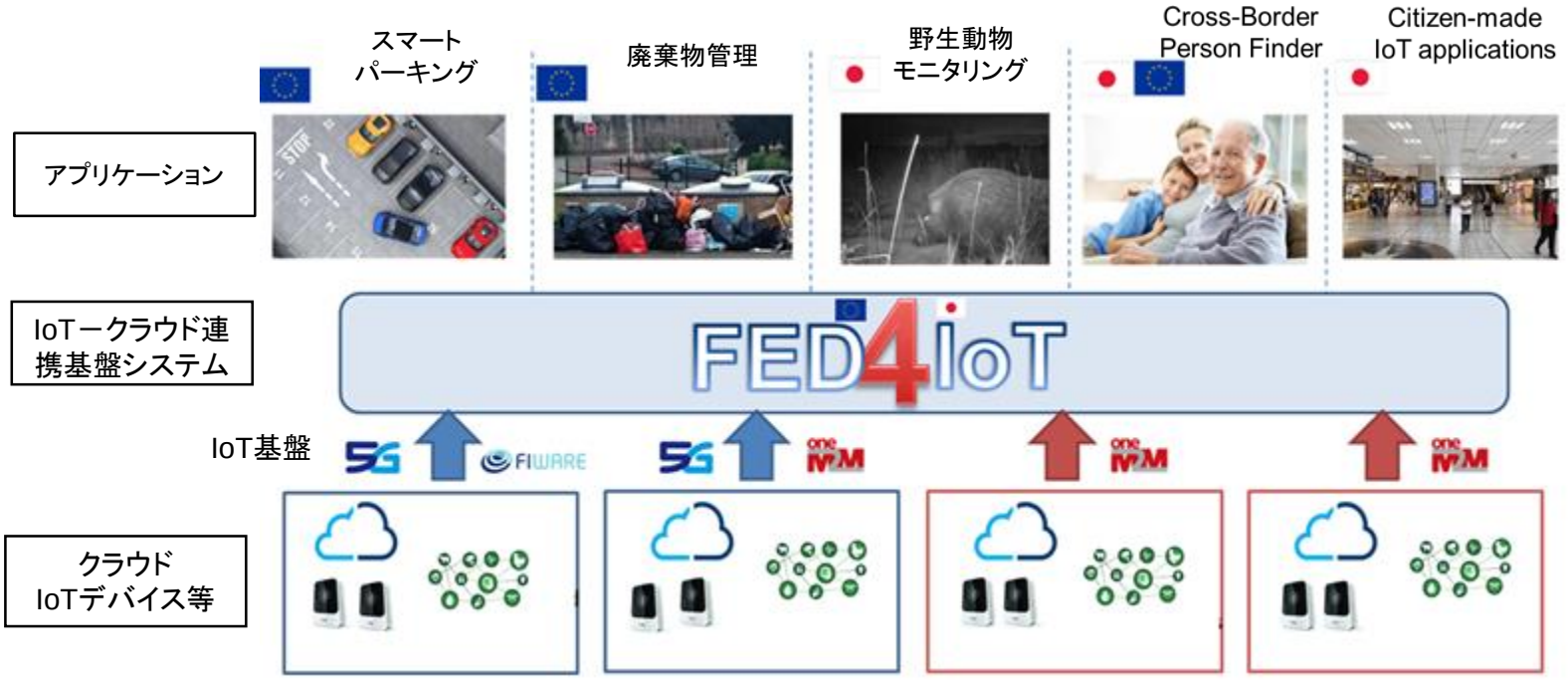
Fed4IoTの概要　日EU共同研究（SCOPE（国際標準獲得型）第4次公募）【資料16】

■ 多様なIoTデバイスの導入等が進む中、より効率的な処理基盤の実現のため、IoTデバイス、クラウド基盤、アプリケーションの相互運用と連携が必要になっていることから、より大きなシナジー効果を生み出す相互運用性に必要とされる要求条件を明確化し、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-クラウド連携基盤を研究開発する。［2018年度～2021年度（36ヶ月）］

プロジェクト名：　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）

実証実験

- プロジェクト内でスマートシティに関する5つのユースケースを想定
- 日EU共同で研究開発を実施するとともに、日本・EUそれぞれで実証実験を予定（個人情報を保護した上でユーザ認証・属性認証サービスを提供するスキームの実証を含む）



日本の研究機関
早稲田大学 株式会社 IIJイノベーションインスティテュート パナソニック株式会社 金沢工業大学
欧州の研究機関
Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT)（イタリア） Easy Global Market (EGM)（フランス） Odin Solutions S.L.（OdinS）（スペイン） NEC Laboratories Europe GmbH (NEC)（ドイツ）

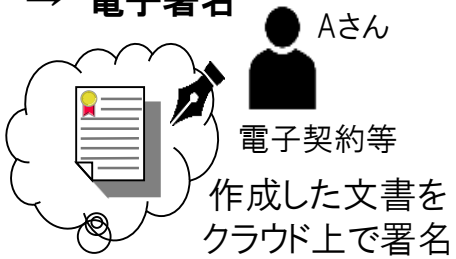
「トラストサービス」の制度化に向けた検討

【資料17】

○ データの自由な流通（Data Free Flow with Trust）は、これからの成長のエンジン。
○ Society5.0の実現に向けて、サイバー空間と実空間の一体化が進展し、社会全体のデジタル化を進める中、その有効性を担保する基盤として、ネット利用者の本人確認やデータの改ざん防止等の仕組みである**トラストサービス**が必要。

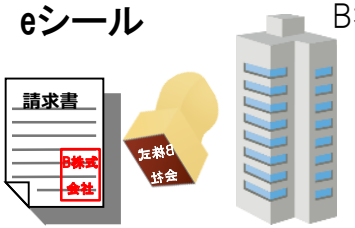
国の制度（電子署名法）有り

①人の正当性を確認
→ 電子署名



制度無し

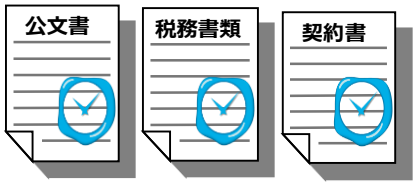
②組織の正当性を確認
→ eシール



組織が発行する文書

民間の認定スキーム有り

④データの存在証明・非改ざんの保証
→ タイムスタンプ



制度無し

③データの送信元（モノ）の正当性を確認

IoT機器（センサー等）から発せられるデータ

制度無し

⑤データの送達等の保証（①～④の組合せによるサービス）

トラストサービスにより期待される効果の例

① 電子署名のクラウド利用への適用（リモート署名※）により、ICカード携行が不要となり、**テレワークや出張の際でも、速やかに電子契約が締結可能となることで、ビジネスの迅速化に寄与**

※ 利用者がサーバにリモートでログインし、サーバ上で行う電子署名のこと

② 組織の正当性を簡便に確認できることにより、企業の文書等の電子化を推進し、**社内業務や企業間取引を効率化**

③ ビッグデータの発信元である**IoT機器等からのデータの真正性を確保し、なりすましを防止**

④ いつ作成された電子データであるか保証されることで、**電子データのみで長期保存が可能となり文書の保存コストが低減**

⑤ **トラストサービスを活用した新たなサービスの創出**
（例：”書留”の電子版）

（参考）「成長戦略フォローアップ」（令和元年６月２１日閣議決定）

サイバー空間での自由で安心・安全なデータ流通を支える基盤として、データの改ざんや送信元のなりすまし等を防止する仕組み（トラストサービス）の在り方について、国際的な相互運用性の観点も踏まえ、2019年中を目途に結論を得て、速やかに制度化を目指す。

プラットフォームサービスに関する研究会
トラストサービス検討WG取りまとめのポイント

【資料18】

※ パブリックコメントを2020年1月20日まで実施。2月7日、最終報告書を公表

具体的なニーズと課題が顕在化している**タイムスタンプ、eシール、リモート署名について取組の方向性を提示。**

現状・課題	取組の方向性
〇データの存在証明・非改ざんの保証の仕組み（タイムスタンプ） • **民間の認定スキームの下で、一部の分野を除き、利用が十分に広がっていない**。 → 電子データと紙による保存を併存している実態があり、保存コストを要している。	• タイムスタンプ事業者に対する**国としての認定制度を創設**。
〇組織の正当性を確認できる仕組み（eシール） • 請求書や領収書等について、企業が電子的に発行したことを**簡便に保証する仕組みがない**。 → 企業内の業務や企業間の取引における**電子化が進まず、業務効率化の妨げ**となっている。	• eシールの認証事業者に対する**国の基準に基づく民間の認定制度を創設**。
〇人の正当性を確認できる仕組み（電子署名） • クラウドを活用した**リモート署名など最新の技術に制度が十分に対応しきれていない**部分が存在。 → 電子署名の利用が伸びていない。 • リモート環境で本人だけが安全に署名できるための**技術的な要件について民間団体で検討中**。	• リモート署名の**電子署名法上の位置づけについて検討。**

■ 上記に加え、電子文書の送受信・保存について規定している**法令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、所管省庁への働きかけ**を行う。

無線LANのセキュリティガイドラインの見直しについて

【資料19】

- 総務省では、無線LANの提供者・利用者向けにガイドラインを作成しており、周知啓発に活用。
- 新技術や最新のセキュリティ動向に対応するため、内容を見直し予定。

「Wi-Fi利用者向け 簡易マニュアル」（2015年３月版）の見見直しポイント

- ✓ セキュリティ対策の訴求点を明確にするため、**セキュリティ対策のポイント**を**整理**
  - ① 接続する**アクセスポイントをよく確認**（偽アクセスポイント対策として接続URL等を確認）
  - ② **原則HTTPS通信**の利用を（Wi-Fi暗号化等に関わらず通信内容を保護）
  - ③ 自宅に設置する**Wi-Fi機器の設定**に注意（管理用パスワードの変更等）
- ✓ セキュリティ関連の**新技術**（WPA3、Enhanced Open等）を**紹介**

「Wi-Fi提供者向け セキュリティ対策の手引き」（2016年８月版）の見直しポイント

- ✓ ガイドラインの対象者の明確化（**自店利用者のみへの提供する者も対象**）
- ✓ 近年懸念されている**偽アクセスポイント対策**（認証画面のURLの周知等）を追記
- ✓ 暗号化のための**パスフレーズを公開**している場合解読の**リスクが高まる**ことを明示
- ✓ 状況に応じたセキュリティ対策の選択と**利用者への周知**が必要であることを明確化
- ✓ セキュリティ関連の**新技術**（WPA3、Enhanced Open等）を**紹介**

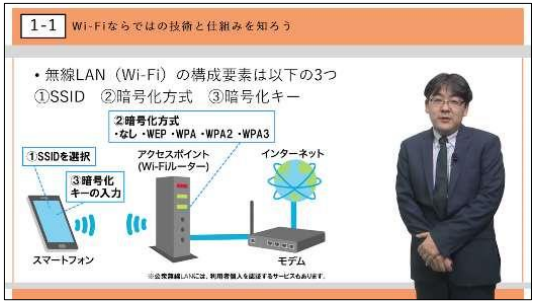
➡ **改定後はWi-Fi提供者（医療機関、宿泊施設、教育機関等を含む）等に改めて周知予定。**

公衆無線LAN(Wi-Fi)の利用に関する周知啓発

- 総務省では、公衆無線LANの利用者のセキュリティ対策に関する周知啓発を実施している。
- 令和元年度は、**オンライン動画講座**を開講するとともに、**ショートムービー**を作成し**SNSを通じて周知**。

オンライン動画講座

- ✓有識者が、公衆無線LAN利用時のリスクや、適切なセキュリティ対策を動画(全10回)により紹介
- ✓オンライン講座プラットフォーム「gacco」にて配信
  https://gacco.org/wifi-security/
- ✓2020年２月10日～３月23日に実施し、3,164名が受講登録。



第１回：もっとつながる・使える公衆無線LAN＜Wi-Fiの技術＞
第２回：とっても危険！「野良Wi-Fi」
第３回：そのWi-Fi、本物ですか？
第４回：さまざまな公衆無線LANサービスを知ろう
第５回：Wi-Fiの接続と暗号化の仕組み
第６回：安全なWeb利用の方法
第７回：自分で重要な通信内容を守る
第８回：より安全・安心にWi-Fiを使うために
第９回(追加講義)：Wi-Fi規格の最新動向
第10回(追加講義)：自宅や外出先で行う最新のセキュリティ対策とは

SNSを用いた周知啓発

- ✓無線LANのセキュリティ対策に関し、20秒程度の動画コンテンツを作成（全３種）
- ✓若年層を含む利用者への周知のため、SNSを通じて作成動画を周知
- ✓動画から上記オンライン動画講座にリンクを張ることで相乗効果を期待
- ✓2020年３月２日～22日に配信し、約102万インプレッション（3,525ユニーククリック）

＜動画① 知らない接続先を使わない＞

その他、＜動画② HTTPSの利用・確認＞ ＜動画③ 管理用パスワード等の適切な設定＞を配信

放送設備の現状とサイバーセキュリティの確保のための措置項目【資料21】

- 放送設備及び有線放送設備の構成は、①放送番組を視聴者に届ける放送ネットワーク系統（放送本線系）と②各放送設備の故障検出や設備切替等を行う監視・制御ネットワーク系統（監視・制御系）に大別。
- 放送本線系は、映像や音声伝送のための専用方式による片方向の中継伝送と、直接受信のための放送方式による一対多の片方向の送信で構成されており、外部のネットワークと直接接続されていない。したがって、送信の起点となる箇所について対策を行うことで、効率的・効果的に他のネットワークから分離することが可能。
- 放送本線系の予備回線や監視・制御及び保守等のために電気通信事業者回線を使用する場合は、専用回線の使用、VPN化、ポート制限、ID・パスワードによる使用者の権限・アクセスの管理に加え、その管理に係る規程・マニュアルの整備など、セキュリティの確保のための措置が重要。

（サイバーセキュリティ確保のための具体的措置項目）

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次の措置又はこれと同等と認められる措置

- 原則として、第三者が接続可能な外部ネットワークとの接続を行わない措置
- やむを得ず接続を行う場合には、ファイアーウォールの設置又は不正接続対策等の措置

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次の措置又はこれと同等と認められる措置

- 専用回線又はＶＰＮ回線の使用、ポート番号若しくはＩＰアドレスによる接続制限又はＩＤ及びパスワードにより権限を有する者だけが接続できるようにする措置
- 未使用時は回線を通じた接続を遮断する等の措置

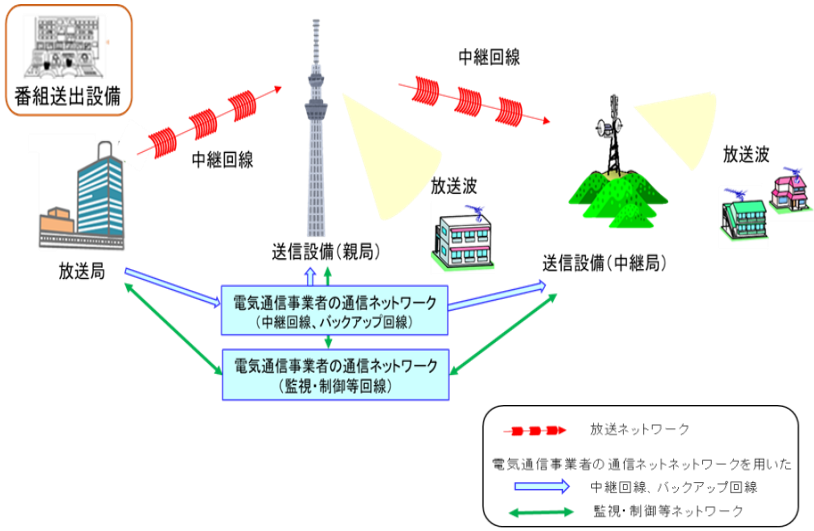
3　設備の導入時及び運用・保守時におけるソフトウェアの点検について、不正プログラムによる被害を防止するため、放送設備のネットワークからの分離・遮断の措置及び不正プログラムの感染防止の措置

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れるための次の措置又はこれと同等と認められる措置

- 番組送出設備に対しＩＤカード、テンキー錠又は有人による入退室の管理等を行う措置及び監視・制御回線、保守回線に係る機器の設置場所に対し公衆が容易に立ち入ることができないよう施錠その他の必要な措置
- 外部記録メディア等を介した不正プログラムへの感染防止の措置

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次の措置又はこれと同等と認められる措置

- 事故報告を含む事後対応を、迅速かつ確実に実施するための規程を整備する措置
- 放送設備のソフトウェアの更新等設備の運用・保守等について、実施方法を定める規程を整備する措置



放送設備の構成のイメージ（地上デジタル放送の例）

放送分野における設備に関する報告様式の変更

放送法令において、各放送事業者は設備の状況を定期的（※）に総務大臣に報告することとされている。

当該報告に関し、放送事故の発生区分に『サイバー事案』を追加し、『サイバー事案』に起因する事故報告を明記するよう、報告様式を変更。

（※）認定基幹放送事業者、特定地上基幹放送事業者及び基幹放送局提供事業者は半年ごと、登録一般放送事業者は１年ごと

別表第二十九号（第127条関係）

特定地上基幹放送局等設備の状況報告書

年　月　日

総務大臣 殿

郵 便 番 号
住　　所
（ふりがな）
氏　　名　（法人又は団体にあつては、名称及び代表者の氏名。記名押印又は署名）
電 話 番 号
免 許 番 号　（親局の免許番号を記載すること。）

放送法施行規則第127条の規定により、　年　月　日から　年　月　日までの特定地上基幹放送局等設備の状況を、次のとおり報告します。

発生年月日（発生時刻）	復旧年月日（復旧時間）	発生区分	発生原因	故障設備	措置模様	影響があつた下位の放送局	備考
		□設備故障 □回線障害 □自然災害 □停電 □ｻｲﾊﾞｰ事案 □その他					
		□設備故障 □回線障害 □自然災害 □停電 □ｻｲﾊﾞｰ事案 □その他					
		□設備故障 □回線障害 □自然災害 □停電 □ｻｲﾊﾞｰ事案 □その他					
		□設備故障 □回線障害 □自然災害 □停電 □ｻｲﾊﾞｰ事案 □その他					
		□設備故障 □回線障害 □自然災害 □停電 □ｻｲﾊﾞｰ事案 □その他					

北海道地域情報セキュリティ連絡会（HAISL）

■　平成26年９月、インターネットが広く普及し、サイバー攻撃や情報漏洩等のリスクへの情報セキュリティ対策が重要となっている中、国、地方公共団体、企業、団体及び教育関係者等が連携や協力を進めやすい環境を整え、関係者が情報セキュリティに関する情報を共有するとともに、情報交換や勉強会を通じた交流を深めることで北海道地域の情報セキュリティ向上することを目的に設立。

＜連絡会の概要＞

■運営体制

会長　　北海道大学　情報基盤センター長　高井　昌彰　教授
副会長　北海道情報セキュリティ勉強会　会長代理　三谷　公美（道警関係）
　　一般社団法人北海道IT推進協会　副会長　河瀬　恭弘　（経済産業局関係）
　　一般社団法人テレコムサービス協会　北海道支部長　佐々木　浩一　（総合通信局関係）
事務局　**北海道総合通信局**、北海道経済産業局、北海道警察本部

■取り組み

１　相互協力

参画機関・団体が実施する情報セキュリティ関連行事の告知や相互協力依頼、人材育成に係る環境整備など、連絡会会員間での連携を図り、各事業の効果的かつ効率的な実施に繋げる。

２　勉強会

参画機関から講師を招き、情報セキュリティインシデントのトレンドやその対策等について勉強会を行う。

３　情報発信

情報セキュリティに関する注意喚起や連絡会会員が実施する情報セキュリティ関連行事等を随時メール等により、広く情報発信する。

■参加機関

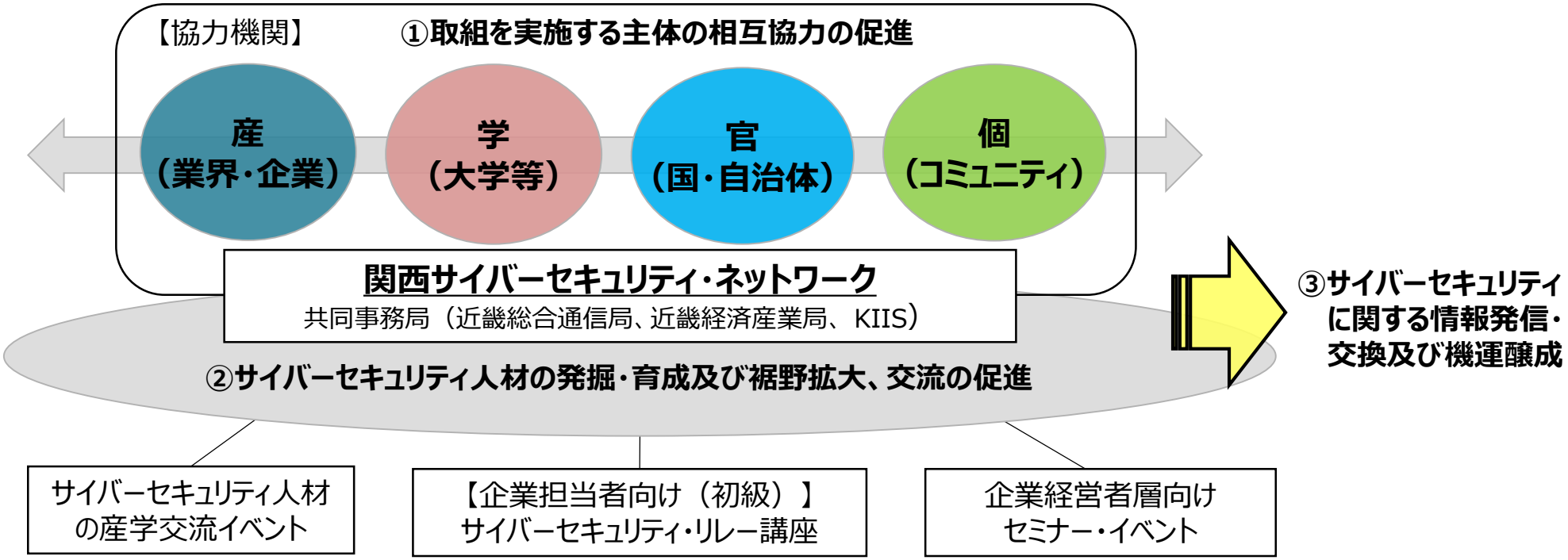
道内の情報セキュリティ関係機関（産学官）３９機関、事務局３機関

関西サイバーセキュリティ・ネットワーク（関西SEC-net）

【資料24】

■ 2018年10月、近畿総合通信局、近畿経済産業局、（一財)関西情報センター(KIIS)が共同事務局となり、サイバーセキュリティ分野における関西の産学官等の相互協力を促進するため、「関西サイバーセキュリティ・ネットワーク」（関西SEC-net）を発足。

■ 関西におけるセキュリティの推進基盤として、人材発掘・育成、情報交換、機運醸成の場を提供。サイバーセキュリティで重要な、「知る」ための取組を進める。

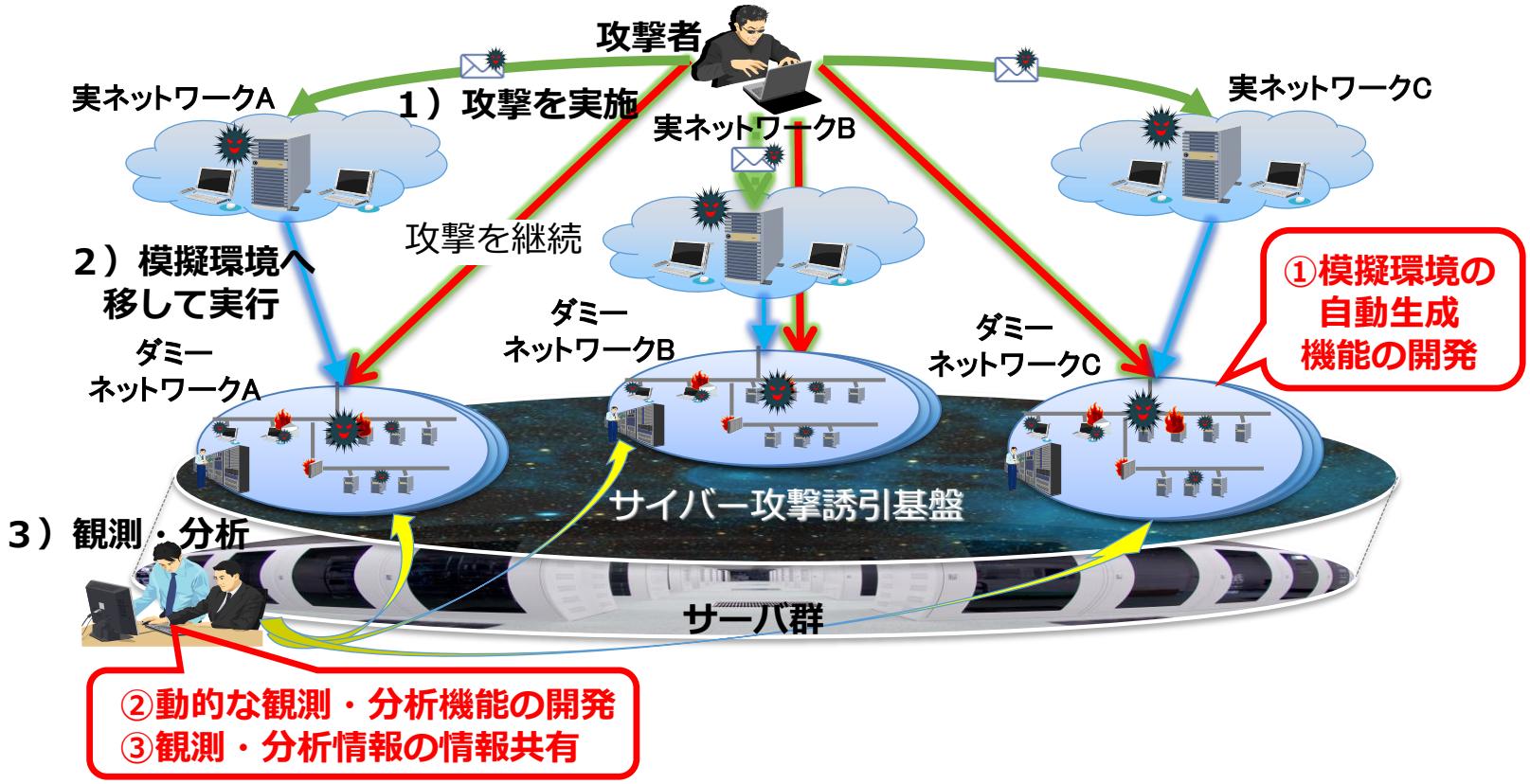


※原則として、産学官個の各主体が実施していない領域の取組を補完的に実施する

サイバー攻撃誘引基盤の構築（STARDUST）

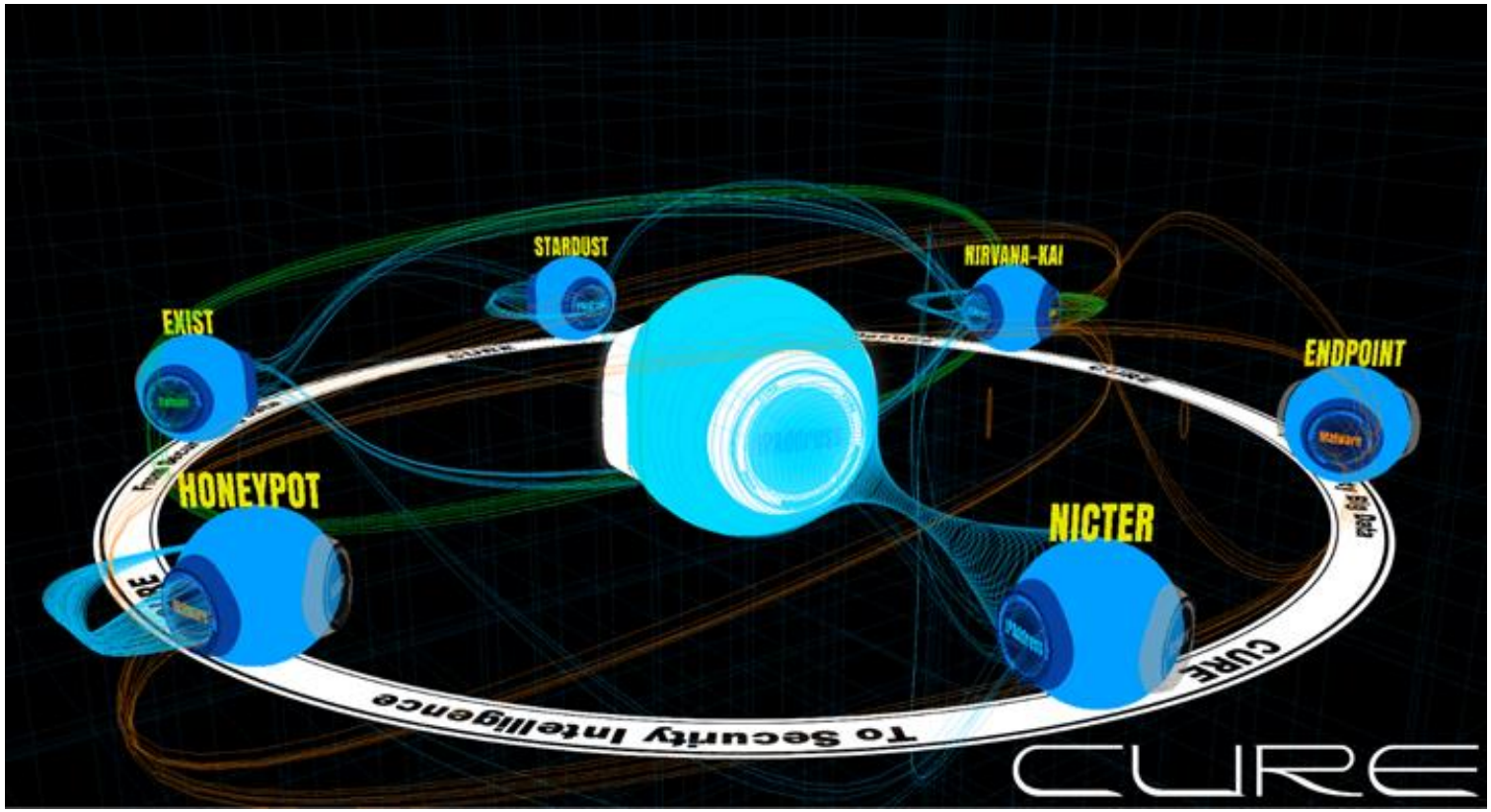
○　高度かつ複雑なサイバー攻撃に対処するため、政府や企業等の組織を模擬したネットワークに攻撃者を誘い込み、攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握することが可能な、高度で効率的なサイバー攻撃誘引基盤を構築。

○　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実証を行うための研究開発環境を、情報通信研究機構（NICT）に整備。分析結果は、セキュリティ対策機関等と連携して情報共有を図り、安全なサイバー空間を実現。



CURE ～サイバーセキュリティ関連情報の大規模集約・横断分析～

- NICTでは、サイバー攻撃の観測情報や脅威情報等、異なる情報源から得られるサイバーセキュリティ関連情報を一元的に集約してつなぎ合わせることで、これまで把握が困難であったサイバー攻撃の隠れた構造を解明し、リアルタイムに可視化。
- 例えば、自組織内のアラートと外部の脅威情報とを関連付けることで、最新の脅威が組織に及ぼす影響について迅速な把握を可能とし、組織のセキュリティ・オペレーションを効率化。



※ CURE（**C**ybersecurity **U**niversal **RE**pository）

量子コンピュータ時代に向けた暗号の在り方の検討

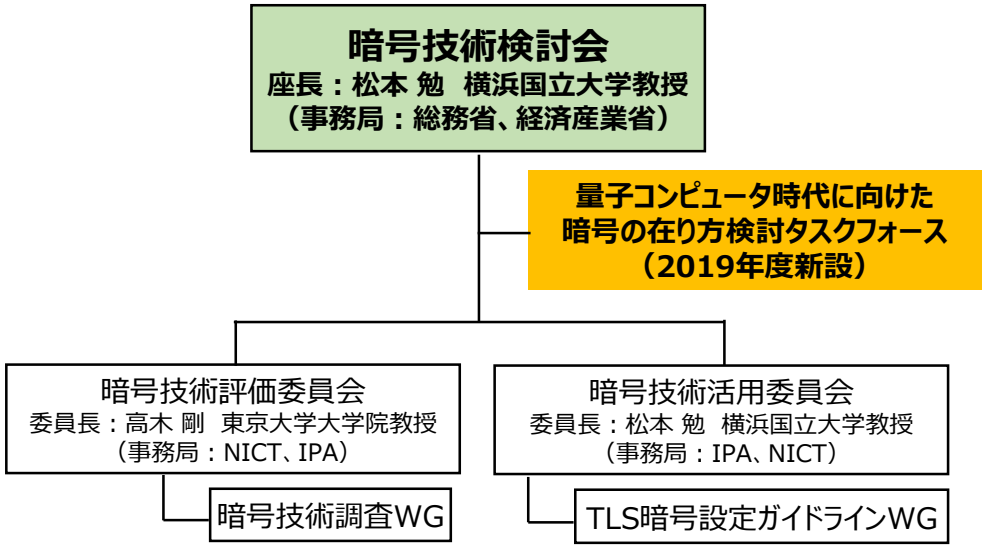
- 総務省等※は、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト「**CRYPTREC**（Cryptography Research and Evaluation Committees）」を実施。
  ※総務省、経済産業省、国立研究開発法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）
- CRYPTRECの暗号技術検討会の下に「**量子コンピュータ時代に向けた暗号の在り方検討タスクフォース**」を設置し、量子コンピュータ時代の推奨暗号の検討（2019年６月～）。

CRYPTRECの概要

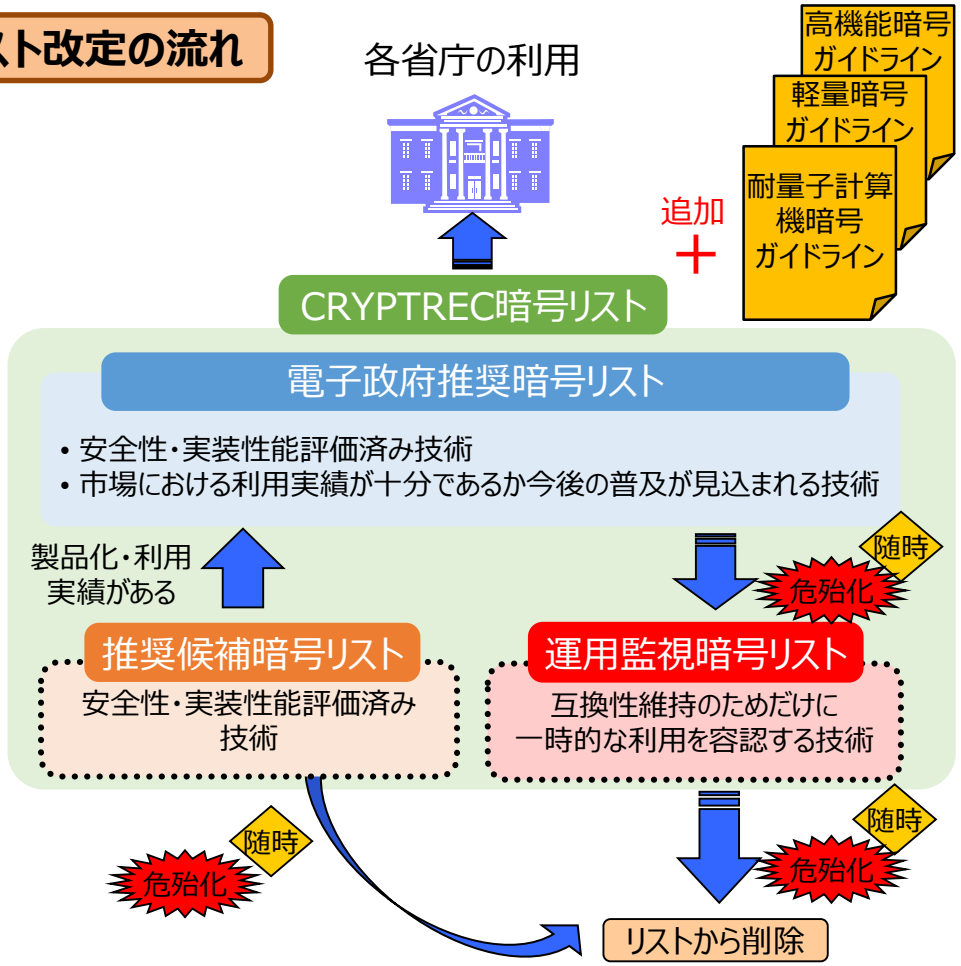
○ 活動内容
- 「CRYPTREC暗号リスト」（※）の公表
- 暗号技術の安全性等の監視及び評価を実施

（※）CRYPTREC暗号リストは、「電子政府推奨暗号リスト」、「推奨候補暗号リスト」、「運用監視暗号リスト」から構成される。

CRYPTRECの体制



リスト改定の流れ



広域ネットワークスキャンの軽量化

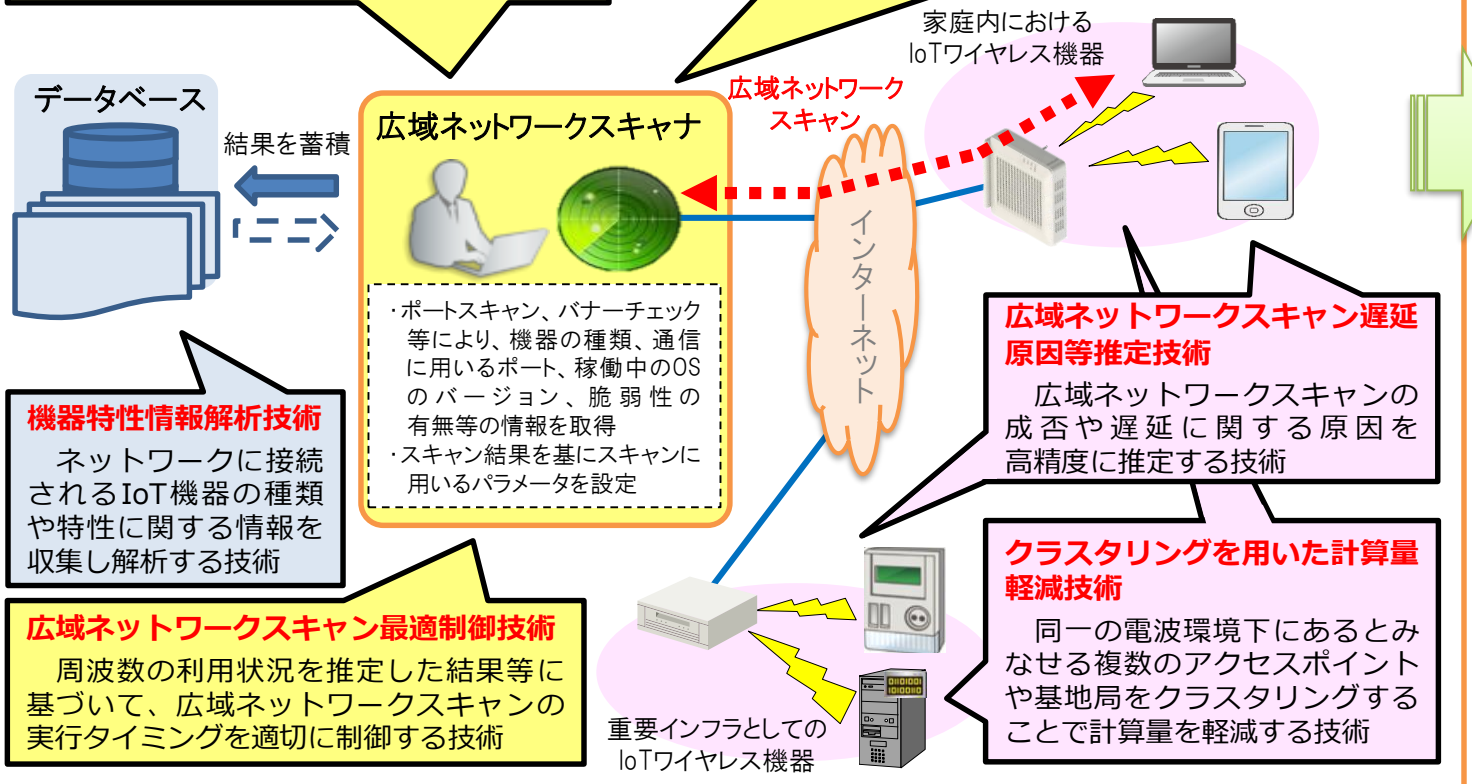
○ 近年、IoT機器を狙ったサイバー攻撃は増加傾向にあり、脆弱なIoT機器への対策は喫緊の課題。

○ 今後、無線通信を利用するIoT機器の割合は増加するものと見込まれているため、「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」に取り組み、効率的な広域ネットワークスキャンの実現を目指す。

広域ネットワークスキャンを実現する要素技術

広域ネットワークスキャン頻度最適化技術
広域ネットワークスキャンの頻度を最適化する技術

広域ネットワークスキャン対象ポート選定技術
広域ネットワークスキャンを実施するポートを選定する技術



機器特性情報解析技術
ネットワークに接続されるIoT機器の種類や特性に関する情報を収集し解析する技術

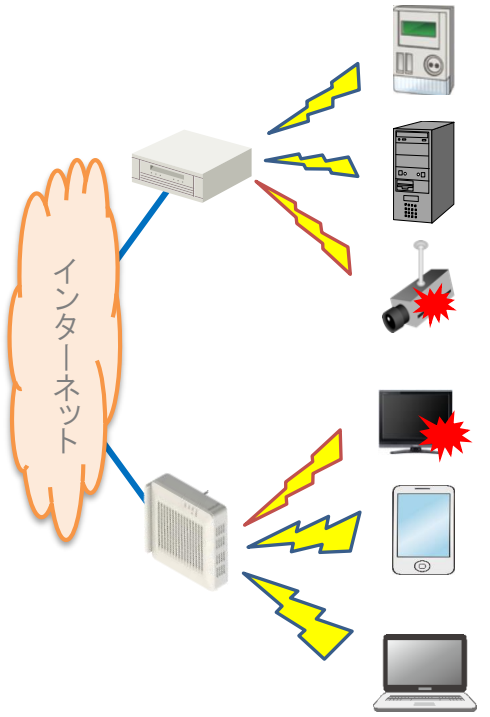
広域ネットワークスキャン遅延原因等推定技術
広域ネットワークスキャンの成否や遅延に関する原因を高精度に推定する技術

広域ネットワークスキャン最適制御技術
周波数の利用状況を推定した結果等に基づいて、広域ネットワークスキャンの実行タイミングを適切に制御する技術

クラスタリングを用いた計算量軽減技術
同一の電波環境下にあるとみなせる複数のアクセスポイントや基地局をクラスタリングすることで計算量を軽減する技術

研究開発の成果

正常な通信を阻害することなく、セキュリティ対策が必要な脆弱なIoT機器を特定することで、安全なICT基盤を実現



衛星通信における量子暗号技術の研究開発

- 近年の世界的な宇宙分野における人工衛星の産業利用に向けた活動の活発化により、今後一層の衛星利用の需要拡大が見込まれる状況。
- 他方、衛星通信に対するサイバー攻撃が脅威となりつつあり、安全な衛星通信ネットワークの構築を可能とする高秘匿な衛星通信技術の確立が急務。
- 小型衛星にも搭載可能であり、盗聴や改ざんが極めて困難な衛星通信を実現する量子暗号技術の開発を平成30年度より開始。本研究成果を活かした衛星ビジネスや移動通信ネットワーク等の事業化を目指す。

研究開発内容

（1）小型衛星に搭載可能な量子暗号通信技術の開発

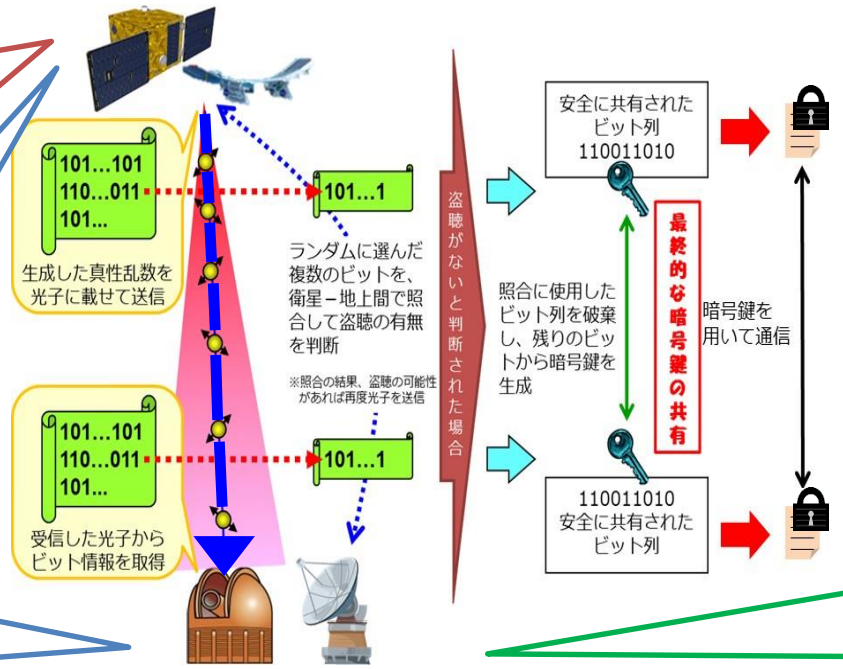
・小型衛星に搭載可能な装置の小型軽量化・省電力化

・宇宙空間という電子機器には劣悪な環境下において動作

・鍵生成の高速化技術の開発

（2）空間光通信・高精度捕捉追尾技術の開発

・衛星への照準を精微に合わせるための高精度な捕捉追尾技術の開発



（3）光地上局の高感度受信技術の開発

・衛星から送信された光信号を地上局において、高感度に受信する技術の開発

（4）インテグレーション・航空機等による実証実験

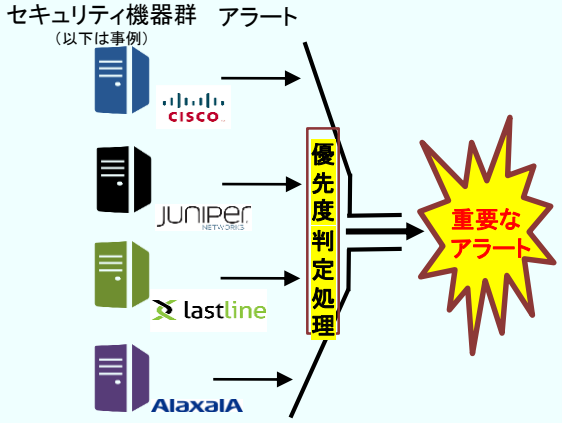
・開発機器を統合し、航空機等を用いた実証実験を行う。

AI x Cybersecurity ～AIを活用したサイバーセキュリティの高度化に関する研究～【資料30】

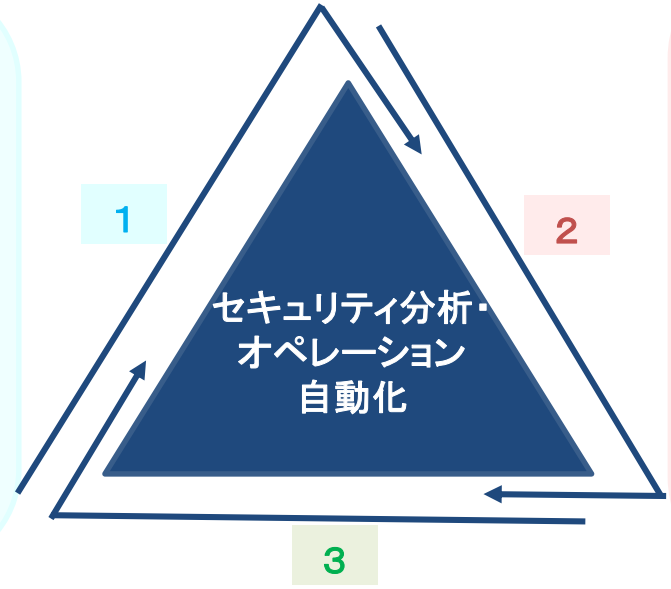
- NICTでは、ダークネット、ハニーポット等の攻撃観測環境を用いて得られた、マルウェアやサイバー攻撃手口などのサイバー攻撃に関連する多種多様かつ大量な情報を保有。
- これらの情報に基づく各種自動分析技術やセキュリティオペレーションの自動化・高精度化に向けて、AI技術を最大限に活用した研究開発を推進。

1. インシデントの優先順位判定

・アラートスクリーニング※
・脆弱性のインパクト分析

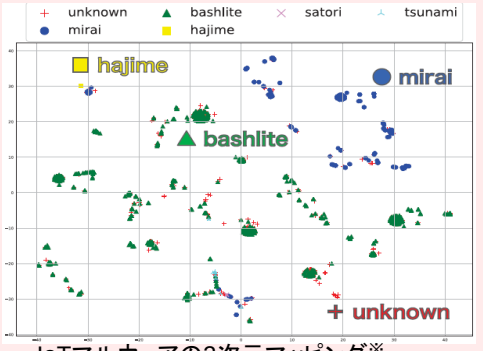


※各種警報を需要度等に応じて選別



2. マルウェア機能分析自動化

・Androidアプリおよびマーケット分析
・IoTマルウェア分析、自動分類
・マルウェア自動分析ツール化

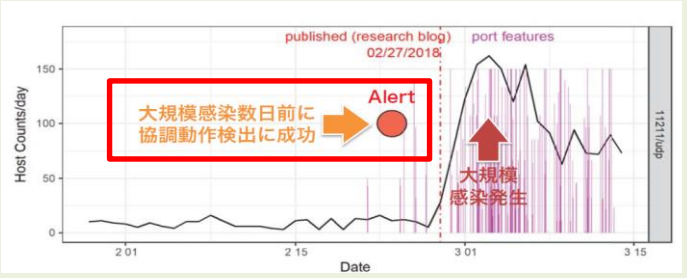


IoTマルウェアの2次元マッピング※

※あるマルウェアを捕獲したときに、Miraiなのかhajimeなのかといった情報がすぐに分かれば、その後のマルウェア解析を効率的に行うことが可能。その類似度を表している。

3. 攻撃の検知・脅威予測・予兆把握

・攻撃初期挙動検知
・ユーザトラフィックの異常検出
・脅威予測
・予兆検知
・影響度評価（攻撃インパクト分析）
・早期警戒情報の導出



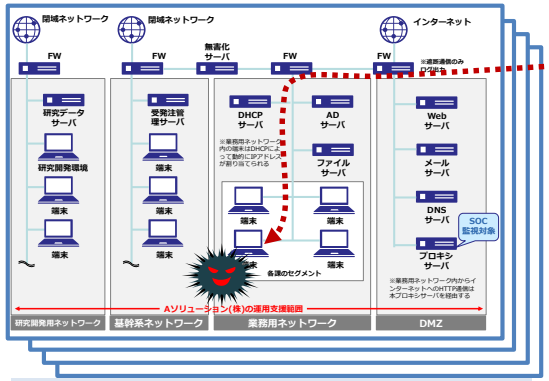
実践的サイバー防御演習（CYDER）

CYDER：CYber Defense Exercise with Recurrence

- 総務省は、情報通信研究機構(NICT)を通じ、**国の機関**、**指定法人**、**独立行政法人**、**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。
- 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って**サイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- **全都道府県**において、年間**100回・計3,000名規模**で実施。
  ※平成29年度：年間100回・3,009名受講／平成30年度：年間107回・2,666名受講／令和元年度：年間105回・3,090名受講

演習のイメージ

NICTの有する技術的知見を活用し、サイバー攻撃に係る我が国固有の傾向等を徹底分析し、現実のサイバー攻撃事例を再現した**最新の演習シナリオ**をコースごとに用意。



実際の**大規模LANを模した環境**を、**受講チームごと**に専用環境として**構築**

擬似攻撃者

NICT北陸StarBED技術センターに設置された大規模高性能サーバー群を活用

演習実施模様
専門の指導員による補助

機材・データを使用して**本番同様の作業**を実施

インシデント（事案）対処能力の向上

令和元年度の実施状況

コース	受講対象組織	対象者	開催地	開催回数	開催時期
Aコース（初級）	全組織共通	システムの運用担当者（システムの利用者レベルを含む）	４７都道府県	６６回	６月～2月
B-1コース（中級）	地方公共団体	セキュリティ管理業務を主導する立場の者	全国１１地域	２０回	９月～11月
B-2コース（中級）	国の機関等、重要インフラ事業者等		東京・大阪・名古屋	１９回	11月～２月

東京2020オリンピック・パラリンピック競技大会に向けた実践的サイバー演習（サイバーコロッセオ）【資料32】

- 近年さらに高度化・多様化するサイバー攻撃に備え、2020年東京オリンピック・パラリンピック競技大会の適切な運営を確保することを目的として、**大会関連組織のセキュリティ担当者等を対象**とした、**高度な攻撃に対処可能な人材の育成**を行う実践的サイバー演習「**サイバーコロッセオ**」を平成30年２月から本格的に実施。
- 実機演習を伴う**コロッセオ演習**を補完する形で、演習時以外にも学習可能な**学習コンテンツ**を提供するとともに、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。

※コロッセオ演習・・・平成29年度：年間２回・74名受講／平成30年度：年間6回・137名受講／令和元年度：年間15回・193名受講
※コロッセオカレッジ・・・平成30年度：年間16回・347名受講／令和元年度：年間59回・992名受講

イメージ図

コロッセオ演習

実機演習を伴っての演習
（攻防型演習を含む）

- 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忠実に再現した、仮想のネットワーク環境を構築。
- 仮想のネットワーク環境上で、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、攻撃・防御手法の検証及び訓練を実施。

学習コンテンツ

コロッセオ演習当日
以外でも学習可能な
コンテンツを提供

コロッセオカレッジ

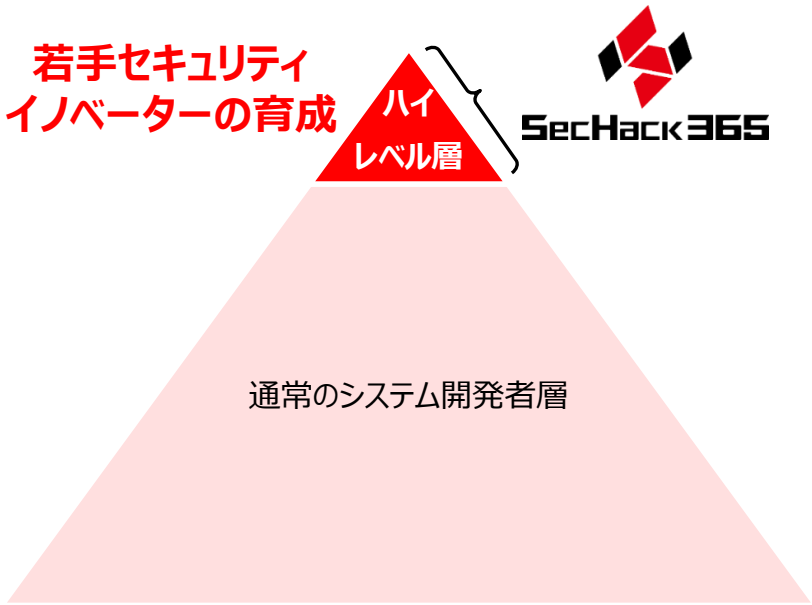
講義演習形式により
セキュリティ関係の
知識や技能を学習

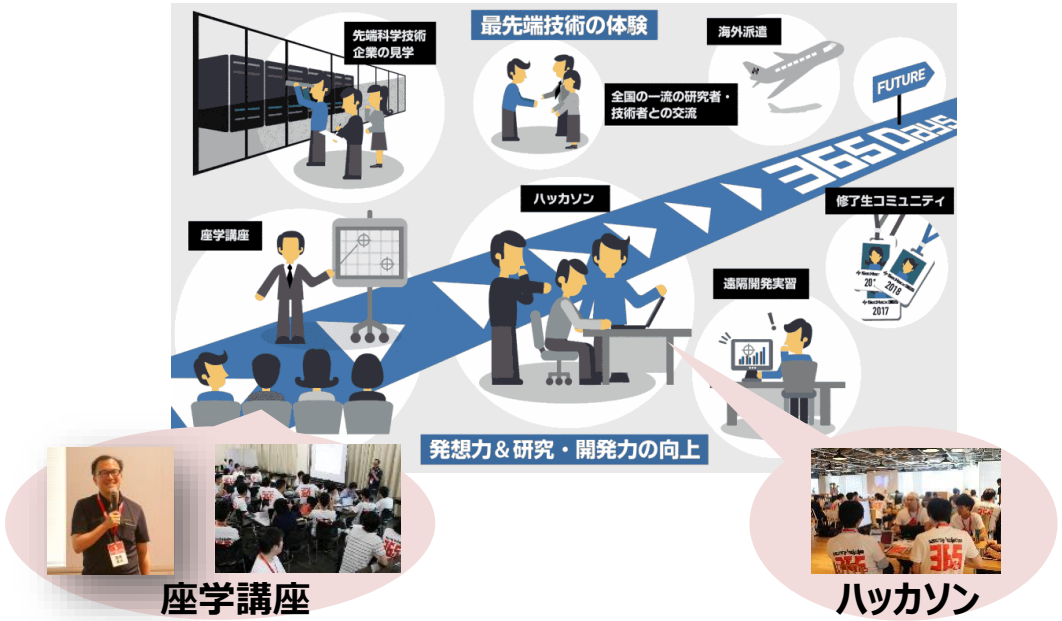
東京2020オリンピック・パラリンピック競技大会のサイバーセキュリティを確保

若手セキュリティイノベータの育成（SecHack365）

- **未来のサイバーセキュリティ研究者・技術者等の創出**に向けて、NICTの持つサイバーセキュリティの研究資産を活用し、**若年層のICT人材を対象**に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**。
- 対象者は、日本国内に居住する**25歳以下の若手ICT人材**（2017年度:39名、2018年度:46名、2019年度:45名が修了）。
- 受講者は、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**。また、集合イベントとして、**座学講座（研究倫理）**や**ハッカソン等**を実施。

※ NONSTOP（NICTER Open Network Security Test-out Platform）では、NICTの長年にわたるサイバーセキュリティ研究によって得られた膨大なセキュリティ関連データを活用することができ、NONSTOP内に整備された様々な研究開発・解析用ツール類と、他では触れることのできない貴重なデータを用いて研究・開発に取り組むことが可能。





通年の遠隔開発実習＋年６回の集合研修（座学講座・ハッカソン等）の組合せによる総合的な人材育成プログラム

地域におけるセキュリティ人材の育成

- サイバーセキュリティ人材は、地方においては首都圏以上に不足している状況。これを踏まえ、総務省では、「サイバーセキュリティタスクフォース・人材育成分科会」において課題と対応方策の検討を実施。
- 2019年６月に「第１次取りまとめ」を公表するとともに、地域のコミュニティや企業、教育機関等と連携して新たなスキームによる人材育成の方策を実証するためのモデル事業を2019年10月から実施。

１．研修リーダーの不在

気付きの機会がない → 研修があっても参加者が少ない → 地方で研修が開催されない → 気付きの機会がない

悪循環

２．組織体制の不足

何をすればよいかわからない → 専門人材を雇用できない → 対策が進まない → 何をすればよいかわからない

悪循環

３．就業機会の不足

雇用の受け皿がない → 地域の若年層がセキュリティ人材を目指さない → 地域におけるセキュリティ人材が更に不足 → 雇用の受け皿がない

悪循環

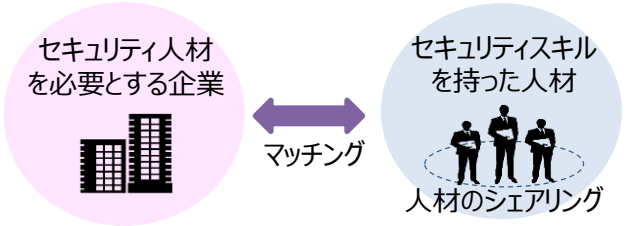
１．地域のセキュリティリーダーの育成

中部地方にて実施（日立製作所）

○ **地域のコミュニティ活動を活性化し、中核としてリードする人材を育成**。

２．地域でのセキュリティ人材のシェアリング

関西地方にて実施（GSX）



○ 県や広域エリアにおいて、複数の中小企業等が**セキュリティ専門家をシェアできるようにマッチング**。

３．地域におけるセキュリティ人材のエコシステムの形成

沖縄にて実施（NRIｾｷｭｱ）

○ 地域の企業や教育機関と連携し、就業の場の確保と**就業につながる研修を行うことで、地域のセキュリティ人材のエコシステムを形成**。

「日ASEANサイバーセキュリティ能力構築センター（AJCCBC）」プロジェクトの概要【資料35】

- JAIF（日ASEAN統合基金）を活用した、ASEAN域内のサイバーセキュリティ能力の底上げに貢献する人材育成プロジェクト。
- 2017年12月の日ASEAN情報通信大臣会合にて総務省が議論をリードし、タイのETDA（電子取引開発機構）がセンターを運用することで合意。2018年9月にセンター開所。

実施時期

STEP1：2017年～
　事前調査を実施
STEP2：2018年～
　センターを活用し以下の活動を実施

STEP2の主な活動内容

1．サイバーセキュリティ演習（CYDER※等）

ASEAN各国の政府機関・重要インフラ事業者等に対し、以下の演習プログラムを実施。

・実践的サイバー防御演習（CYDER）※CYDER：Cyber Defense Exercise with Recurrence

・証拠保全・解析等のためのデジタルフォレンジック演習

・マルウェアの挙動解析演習

2．ASEAN Youth Cybersecurity Technical Challenge (Cyber SEA Game)

ASEAN各国から選抜された若手技術者・学生がサイバー攻撃対処能力を競うCTF形式※の大会の開催（年1回）

※CTFとは、Capture The Flagの略で、問題の中に隠されたフラグ（＝キーワード）を探し出して解答するクイズ形式の競技

日ASEAN情報通信大臣会合（2017年12月）

サイバーセキュリティ演習

第12回 日・ASEANサイバーセキュリティ政策会議の結果

【資料36】

1. 開催概要

日時: 2019年10月29日（火）及び30日（水）

場所: タイ・バンコク

主催: 内閣官房（内閣サイバーセキュリティセンター）、総務省、経済産業省

目的: サイバーセキュリティ分野における我が国とASEAN諸国との国際的な連携・取組の強化

参加者: ASEAN加盟国のサイバーセキュリティ関係省庁及び情報通信関係省庁の局長・審議官等
ASEAN事務局
我が国の内閣官房・総務省・外務省・経済産業省の審議官等

2. 主な成果

2018年10月に東京で開催された第11回会合において協力することが合意された8つの協力活動（サイバー演習、重要インフラ防護、意識啓発、能力構築、インシデント相互通知、オンラインコミュニティ、リファレンス（便覧）、ワーキンググループ運営）について実施状況を確認するとともに、今後の日・ASEANの連携・協力についての検討を実施。

（1）情報共有体制及びサイバーインシデント発生時の対処体制の強化

日・ASEANにおけるサイバーセキュリティ脅威情報共有体制の維持と、インシデント発生時の国際連携手順の確認を目的とした、情報連絡演習及び机上演習について、2019年度の成果が報告された。さらに、インシデントを検知した際に相互通知を行う取組について、2019年度の成果が報告され、2020年度以降も引き続き実施することが承認された。また、オンラインで利用可能な新たなコミュニケーションツールについて、利用ガイドライン案が承認された。また、ASEAN諸国及び我が国のサイバーセキュリティに関する政策及び体制整備の動向をとりまとめたリファレンス（便覧）が作成され、承認された。

（2）重要インフラ防護に関する取組の推進

重要インフラ防護の実践的な取組や、先進的・先導的な取組に関する情報交換を行うため、2018年に引き続き「重要インフラ防護ワークショップ」が開催されたことが報告された。また、2020年度以降も継続的に実施することが確認された。

（3）能力構築及び意識啓発における協力の推進

我が国が実施しているサイバー分野の能力構築（人材育成）事業の実施状況が報告されるとともに、日本とASEAN各国の意識啓発活動の実施状況が報告された。また、2020年度以降も継続的に実施することが確認された。

第10回 ISP向け日ASEAN情報セキュリティワークショップの開催結果 【資料37】

1. ワークショップの概要

日時: 2019年12月17日（火）及び18日（水）

場所: タイ・バンコク

主催: 総務省及びタイ電子取引開発機構（ETDA）

目的: 日本及びASEAN各国のサイバー攻撃の現状やサイバーセキュリティに関する取組の情報共有を通じて、各国のISP連携を維持・強化する。

参加者: ASEAN各国のISP事業者及び政府機関

日本より総務省、NICT、ICT-ISAC等

傍聴者を含み計40名程度

ワークショップの模様

2. 主な内容

- ○ 総務省から、IoTセキュリティ対策の取組及びASEAN諸国に対する能力構築支援の取組等について発表
- ○ NICTから、サイバーセキュリティ対策に関する最新の研究開発動向について発表
- ○ ICT-ISACから、ICT-ISAC Japanの概要、各WGの活動状況、脅威情報の共有の取組等について発表
- ○ ASEANの参加者から、各国におけるサイバー攻撃の現状やサイバーセキュリティの取組について発表
- ○ サイバー攻撃対応机上演習を実施。DDoS攻撃等への対処を題材としたシナリオへの対処を議論

3. 成果

- ○ 各国のISP事業者におけるサイバーセキュリティ分野の取組状況の共有と意見交換
- ○ ASEAN各国（主にISP事業者）との人的ネットワークの維持・強化
- ○ 各事業者による脅威情報の共有、顧客を対象とした意識啓発施策について、継続して検討・協力していくことを確認

日米のISAC連携に関する取組

複雑化・高度化が進むサイバー空間の脅威に対応するためには、官民での情報共有や国際連携の強化が重要。
総務省では、サイバー脅威に対する国内通信インフラ事業者の対処能力向上を目的として、日米の情報通信分野ISAC(*)組織間における情報共有・連携の促進を支援。

(*) ISACとは、Information Sharing and Analysis Center(情報共有分析センター)の略で、特定の産業界において、サイバー攻撃のインシデント情報等を収集・分析し、業界内で共有することを目的として、事業分野ごとに設立される組織。

■ 日米ISAC連携ワークショップのこれまでの開催実績

- 2016年11月: 日米ISAC関係者による初めての国際連携会合を開催。日米のサイバー脅威動向や取組状況等を意見交換。
- 2017年11月: 第2回会合を開催。米国IT-ISACの保有するサイバー脅威関連情報のICT-ISACへの提供等について合意。
- 2019年2月: 第3回会合を開催。各ISACが情報共有を推進する上での懸念事項を共有し、その解決策等を議論。あわせて、公開シンポジウムも開催。
- 2019年11月: 第4回会合を開催。ICT-ISACと米国IT-ISACが協力に係る覚書に署名。
  (1) サイバー脅威とインシデント情報の共有
  (2) 脅威情報の共有を自動化する仕組みの構築に向けた協力
  (3) 両ISAC会員企業間での協力の促進
- 2020年1月: 2020年1月のPTC(太平洋電気通信協議会)においてフォローアップ会合を実施。

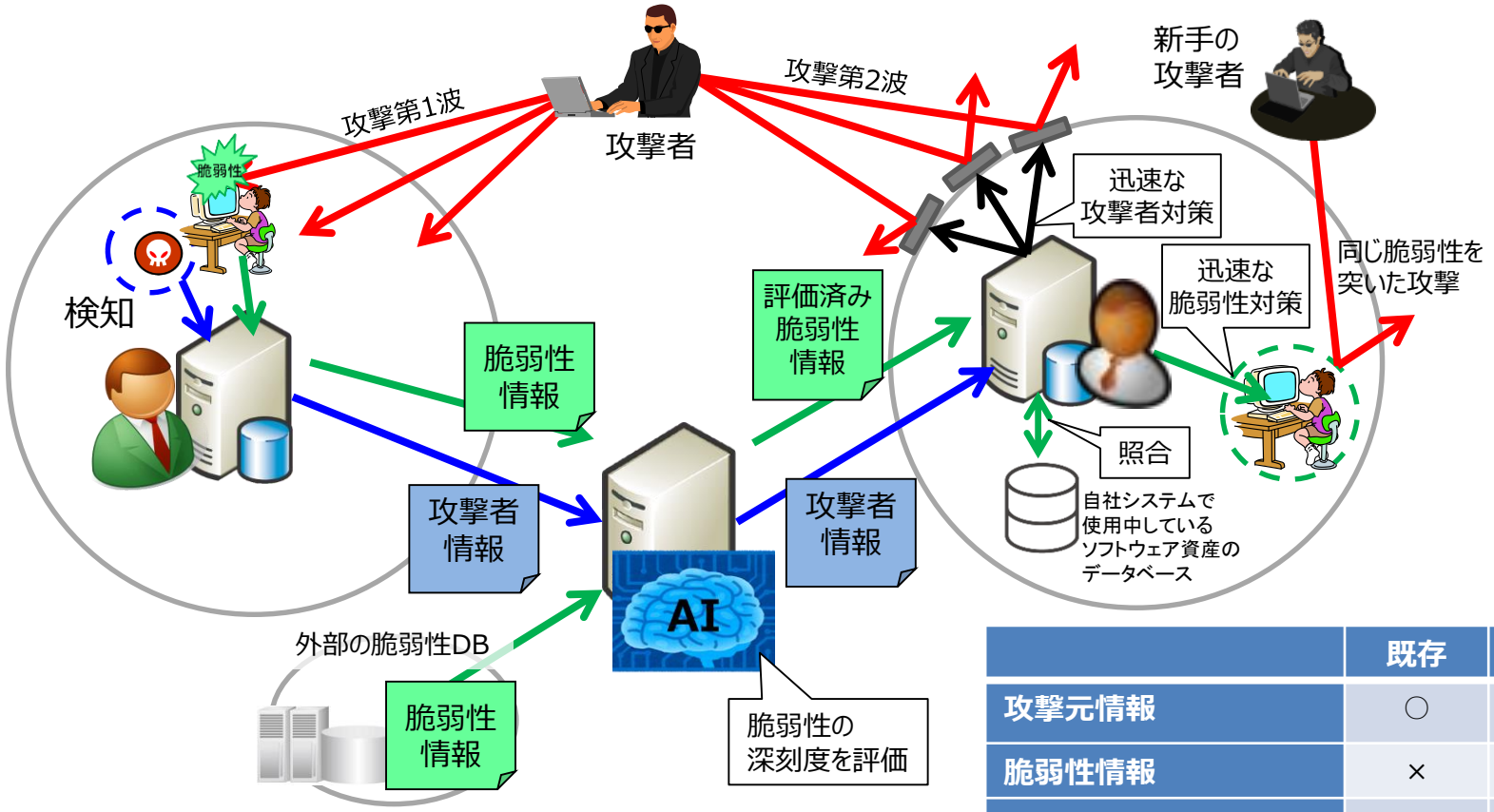
ICT-ISACと米国IT-ISACによる
覚書署名式の様子(2019年11月)

第4回公開シンポジウム
パネルディスカッション(2019年11月)

情報共有基盤の高度化 ～脆弱性情報の共有による対策の更なる迅速化～【資料39】

○ 既存モデルでは、攻撃元の情報は共有されていたが、防御側の弱点である脆弱性情報は機械的な速度で共有できておらず、各組織のセキュリティ担当者が手作業で情報の収集や深刻度の評価、セキュリティパッチ適用の判断を行っている状態。

○ サイバーセキュリティ人材が不足している中、サイバー攻撃による被害が多発・深刻化している状況では、攻撃元情報に加え、脆弱性情報についても機械的速度で情報を共有し、深刻度の正確な把握と迅速な対処を行う、新たなモデルを確立する必要。



	既存	高度化
攻撃元情報	○	○
脆弱性情報	×	○+評価
ソフトウェア情報 紐付け	×	○

サイバーセキュリティ対策情報開示の手引きの趣旨・目的

【資料40】

■総務省では、平成29年12月より、サイバーセキュリティタスクフォース（座長：安田　浩　東京電機大学　学長）の下で「情報開示分科会」（主査：岡村久道　英知法律事務所 弁護士）を開催。同分科会において、民間企業のサイバーセキュリティ対策の情報開示に関する課題を整理し、民間企業における サイバーセキュリティ対策の情報開示を促進するために必要な方策等について検討。

■今般、検討結果を踏まえ総務省において民間企業にとって参考となり得る情報開示の事例等をまとめた「サイバーセキュリティ対策情報開示の手引き」（案）を作成し、意見公募を経て令和元年6月に公表。

背景

✓ サイバー攻撃が深刻化する中、民間企業においてサイバーセキュリティ対策は重要な経営課題となっているが、企業としての社会的責任を果たしステークホルダーからの信頼を得るためには、**サイバーセキュリティ対策の実施のみならずその内容について適切な情報開示が重要。**

目的

✓ 民間企業による**サイバーセキュリティ対策**やその対策の**情報開示の重要性**の認識を促進。

✓ 民間企業にとって参考になり得るような**既存の情報開示の実例**を**事例集として**示す。

活用主体

✓ **サイバーセキュリティ対策の情報開示**に一定の関心のある民間企業の開示の実務担当者等を想定。

対象とする情報開示

✓ **開示書類**を通じた情報開示を取り扱う。

✓ 開示書類の読み手は、**投資家、融資元、顧客・契約者・取引先、従業員、競合他社等を含む、社会全体の広範なステークホルダー**を想定。