資料 13－ 3

IoT セキュリティ総合対策
プログレスレポート 2019

（5/10 時点版）

令和元年〇月

サイバーセキュリティタスクフォース

目次

はじめに

本文書は、2017 年（平成 29 年）10 月に総務省のサイバーセキュリティタスクフォース（以下「タスクフォース」という。）が策定・公表した「IoT セキュリティ総合対策」（以下「総合対策」という。）[1]の進捗状況について、プログレスレポートとして整理したものである。

センサの小型軽量化、低廉化が進み、全てのモノがネットワークにつながる IoT の爆発的な普及が進んでおり、冷蔵庫やテレビといった家電、自動車、ロボット、スマートメーター等のモノの活用だけでなく、IoT 機器で得られるデータを利活用した新たなビジネスやサービスが創出されつつある。また、IoT 化の進展は、これまで個別領域ごとに進められてきた ICT 化を越え、異なるシステムの連携による仮想的な統合システム（System of Systems）となって異なる領域のデータ連携を実現する。その結果、IoT システムはリアルな現実空間とサイバー空間を緊密に連携させたデータの生成・収集・蓄積・連携・解析を通じ、社会的課題の解決をもたらす社会基盤として機能していくことが期待される。

他方、社会基盤としての IoT 化が進展すると、IoT システムのセキュリティ対策が十分でない場合、その影響として広範囲に及ぶ連鎖のリスク（システミックリスク）が顕在化する可能性がある。実際に、IoT を狙った攻撃等により、従来の情報漏えいに加えて、直接的な金銭被害、業務・サービス障害が国内外で生じ、経済社会の持続的な発展や国民生活の安全・安心等を脅かす事例が生じている。このため、IoT システムのセキュリティ対策に関しては、部分最適ではなく、システム全体を俯瞰した全体最適を実現する観点から総合的な対策を講じていく必要がある。

総合対策は、上記の問題意識を踏まえ、IoT システムのセキュリティ対策の総合的な推進に向けて取り組むべき課題を整理している。これを踏まえ、総務省においては、2016（平成 28 年）年８月に内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）が公表した「安全な IoT システムのためのセキュリティに関する一般的枠組み」[2]を踏まえつつ、総合対策において整理した５つの柱（施策群）、すなわち、（１）脆弱性対策に係る体制の整備、（２）研究開発の推進、（３）民間企業等におけるセキュリティ対策の促進、（４）人材育成の強化、（５）国際連携の推進に沿って各施策を展開してきた。

総合対策においては、その進め方として、「半年に１度を目途としつつ、必要

---

1 「IoT セキュリティ総合対策」（2017 年 10 月　サイバーセキュリティタスクフォース）
http://www.soumu.go.jp/main_content/000510701.pdf

2 「安全な IoT システムのためのセキュリティに関する一般的枠組み」（2016 年８月 NISC）
https://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf

に応じて検証を行い、進捗状況を把握する」とされたところであり、2018 年（平成 30 年）７月には、総合対策の項目ごとにその進捗状況及び今後の取組について整理した「IoT セキュリティ総合対策 プログレスレポート 2018」を公表した。本文書はこれに引き続いて総合対策の進捗状況と今後の取組について整理を行ったものである。なお、総合対策については、2017 年（平成 29 年）10 月の策定後にサイバーセキュリティを巡る様々な状況変化等があったことを踏まえ、現在、タスクフォースにて見直しに向けた検討を行っているところである。

総務省においては、今般の総合対策の検証結果を踏まえ、引き続き、NISC や経済産業省をはじめとする関係府省庁と連携しつつ、所要の施策を推進していくことが求められる。

Ⅰ　具体的施策

（１）脆弱性対策に係る体制の整備

（設計・製造段階）

①　セキュリティ・バイ・デザイン等の意識啓発・支援の実施

【本文】

設計・製造段階においては、所有者・運用者・利用者による安全な設定が行われるよう、ID/パスワード設定、ファームウェアのアップデート及びWi-Fi設定の仕様を設計時に盛り込むなど、製造業者におけるセキュリティ・バイ・デザインの考え方をいかに浸透させるかが重要となる。このような考え方を踏まえて設計された機器に認証マークを付与し、当該認証マークの付された機器の使用を推奨すること等について検討を行い、セキュリティ・バイ・デザイン等の意識啓発・支援を実施する必要がある。その際、認証を行った後に脆弱性等が発見される場合が想定されることから、認証は定期的に行い、最新の認証を受けているかどうかを利用者等が確認できる仕組みとすることが望ましい。

平成 30 年９月に、総務省情報通信審議会情報通信技術分科会において、IoT機器を含む端末設備に対するセキュリティ対策として、電気通信事業法の枠組みの中で、電気通信事業者の電気通信回線設備の機能に障害を与えない、他の利用者に迷惑を及ぼさないといった端末設備の接続の技術基準の原則の範囲内において、その技術基準にセキュリティ要件を追加することが適当との答申がなされたところである。これを受け、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、端末設備等規則（昭和 60 年郵政省令第 31 号）の一部改正を実施した（2019 年（平成 31 年）3 月 1 日公布）。同改正省令は、IoT 機器メーカや登録認定機関等の対応を考慮し、2020 年（令和２年）４月に施行される。また、当該改正後の端末設備等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、総務省において関係者の意見を考慮しながら検討を行い、「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・公表した（平成 31 年 4 月 22 日）。

なお、新たに技術基準に位置づけられた具体的な内容については、インターネットプロトコルを使用し、電気通信回線設備を介して接続することにより、電気通信の送受信に係る機能を操作することが可能な端末設備について、最低限のセキュリティ対策として、①アクセス制御機能、②アクセス制御の際に使用するID/パスワードの適切な設定を促す等の機能、③ファームウェアの更新機能、又は①～③と同等以上の機能を具備することである。なお、PC やスマートフォン

等、利用者が随時かつ容易に任意のソフトウェアを導入することが可能な機器については本セキュリティ対策の対象外とされている。

一方、民間主導の取組については、2017 年（平成 29 年）12 月より、IoT 推進コンソーシアムの IoT セキュリティ WG において、IoT 機器のセキュリティ対策のあり方について検討を開始し、平成 30 年７月に「IoT 機器のセキュリティ対策に関する検討の方向性」が取りまとめられた。この文書では、セキュアな IoT 機器の認証については「IoT 機器の多様性や技術革新の進展等に鑑み、基本的には民間団体主体の自発的な取組に委ねることが望ましい」とした上で、求めるセキュリティ要件（デフォルトパスワード使用の禁止、各分野の特性に応じた要件など）、認証手段（ツール検証、開発プロセス認証など）、基準・規格に適合している旨の表示（ラベリング）の仕組み、一定期間経過後の認証の更新の必要性、認証取得手段（要件適合の自己確認、第三者認証など）等の論点の具体化を図ることとしている。

また、2018 年（平成 30 年）11 月には、一般社団法人重要生活機器連携セキュリティ協議会が、IoT 機器・サービスのセキュリティ認証プログラムの実施に向けて、IoT 分野共通のセキュリティ要件の素案を策定・公開し、当該素案を踏まえて認証スキームの検証トライアルを行っており、民間団体・事業者等を中心に認証の開始に向けた準備が進められているところである（Ｐ）

【今後の取組】

2020 年（令和２年）４月の改正端末設備等規則の施行について、機器メーカ等の関係者と連携して円滑に実施できるよう取り組む。

民間主導の IoT 機器のセキュリティ対策の取組については、引き続き上記の WG において議論の動向をフォローしていくこととする。その検討に際しては分野ごとの認証の仕組みについて、各分野の特性を踏まえたセキュリティ水準の要求条件を何段階かにクラス分けして設定するほか、IoT 機器は分野を越えて接続されるものであることから、各分野に共通する事項を整理し、ベースライン要件として共通化を図り、段階的に底上げを図っていくことを併せて検討していく必要がある。

上述の調査検討で得られた知見や、民間団体・事業者による認証スキーム立ち上げの動きがあることを踏まえ、引き続き、官民で連携して IoT 機器のセキュリティの確保に努めていく。

（販売段階）

② 認証マークの付与及び比較サイト等を通じた推奨

【本文】

販売段階においては、脆弱性を有する機器の流通を防止することが重要となる。そのため、一定のセキュリティ要件を満たしている IoT 機器に上記の認証マークを付与することや、比較サイト等を通じて認証マークが付与された機器が推奨される（利用者が容易に認証取得の有無等を確認できる）仕組みの構築について、具体的な検討を進める必要がある。

なお、IoT 機器の中でも国民生活や社会経済活動への影響が大きい機器については、市場への流通後も管理が可能となるよう管理番号を付与できる仕組みが考えられる。これに関して、例えば、民間団体では、IC チップ内に電子証明書を格納することにより、製造元等を識別する取組が開始されている。

【進捗状況】

IoT 機器を含む端末設備に対するセキュリティ対策については、端末設備等規則の一部改正を行った（項目（１）①参照）。民間主導の IoT 機器のセキュリティ対策に係る認証の仕組みについては、IoT 推進コンソーシアムの IoT セキュリティ WG や民間団体等において検討が進められてきたほか、民間団体等による認証スキーム構築の動きもある（項目（１）①参照）。

また、民間組織において、機器製造段階で IC チップに証明書や鍵情報を書き込み、デバイスのトレーサビリティを確保するような取組が行われている。さらに、2018 年度（平成 30 年度）戦略的情報通信研究開発推進事業（SCOPE）においては、IoT 機器そのものと IoT ネットワークに焦点を当て、不正動作を検出した後、高速に IoT ネットワークを正常回復する仕組みを構築することを目標として研究開発を実施した（項目（２）③参照）。

【今後の取組】

前項①の取組の中で、認証マークの付与の方法等についても検討を進める。なお、民間におけるセキュア IoT プラットフォームを確立するための取組等については、海外においても様々な観点から同様のトラストチェーンを構築しようとする動きが出てきていることを踏まえ、こうした国際動向を分析するとともに、相互連携の可能性の検討を含め、引き続き積極的に支援していくこととする。

（設置段階）

③　IoT セキュアゲートウェイ

【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、流通している機器の中から、脆弱性を有する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(ネットワークへの接続)段階において、脆弱性を有する機器が存在することを前提として、セキュアなシステム構築を実現する仕組みが重要となる。また、IoT 機器単体では必要なセキュリティ対策の実現が困難な場合や IoT 機器に精通していない利用者についてはセキュリティ対策が十分講じられない場合が想定される。このため、IoT システム・サービス全体としてセキュリティを確保する観点から、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する取組について、総務省において実証を進めるとともに、セキュリティ評価や実際の導入を進める仕組みについて検討する必要がある。

【進捗状況】

総務省では、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する取組について、平成 28 年度補正予算の「サイバーセキュリティの強化」の 5.0 億円の内数（2.5 億円）により、３つの IoT サービス（カーモビリティ分野、スマートホーム分野、エデュケーション分野）で実証実験を実施した。

具体的には様々なセキュリティ脅威に対して、

１）　認証（IoT サービスに接続しようとする IoT 機器が正当なものであるかを IoT セキュアゲートウェイにおいて認証）
２）　検知（データ受信頻度や通信量等を基に、異常な通信を検知）
３）　対処（異常な通信を行う IoT 機器の遮断や、脆弱性を有する IoT 機器の自動ソフトウェアアップデート）

といった一連のセキュリティ対策が実現できるかについて検証を行った。

検証を行った結果、総じて通信の遅延や IoT セキュアゲートウェイを起因とする IoT サービスの停止等は発生せず、良好に運用することができた。IoT セキュアゲートウェイは認証、検知、対処といった機能も提供できており、通信暗号化機能や秘匿性の高いデータ管理機能を有した堅牢なシステムであることも確認された。

ただし、IoT サービスの特性に基づく運用上の課題があり、機能が十分に発揮できないケースがあった。例えば、カーモビリティ分野において、車両に IoT 機

器を取り付けるという特性上、地下駐車場に入り電波の届かない場所で通信が途絶えた場合に、IoT セキュアゲートウェイが IoT 機器の状態を把握できず盗難があったと誤検知したケースや、IoT セキュアゲートウェイが IoT 機器との通信を再開した際に一気に送信されたデータを受信してしまい、乗っ取りがあったと誤検知したケースがあった。こうした運用上の課題を解決するために、検知機能の向上が求められることが明らかになった。具体的には、サービス提供者が利用シーンに応じて検知条件を設定することができるテンプレート（条件設定画面）を用意するといった機能改善や、サービス利用者の利用状況等の統計的なデータを収集・分析した結果に基づき、サービス利用者・IoT 機器ごとに脅威検知に関する適正値を自動的に設定することが求められることとされた。

その上で、今後、IoT セキュアゲートウェイの普及に向け、以下３点の実用的なサービスモデルの提示の取組が必要とされた。

１） サービス提供者が迅速かつ適切な行動をとれるよう、サービス提供者に対する脅威検知のレベルや攻撃状況の詳細情報等の提示

２） IoT セキュアゲートウェイを利用しやすくなるよう、各種 IoT サービスに応じた多様なテンプレートの作成

３） 効率的なシステム運用が行えるよう、SOC（Security Operation Center）のシステムと IoT セキュアゲートウェイの連携等

【今後の取組】

上述の実証実験において、個々の IoT サービスの特性に基づく個別の運用上の課題等が明らかになっていることから、引き続き、個別のユースケース等に応じた運用ルールとそのルールを踏まえた機能改善の在り方等について検討を行う。

（運用・保守段階）

④　セキュリティ検査の仕組み作り

【本文】

IoT 機器が実際に利用されている状況においても、運用・保守段階において、継続的に安全安心な状態を維持することが求められる。そのため、継続的な安全性を確保するためのセキュリティ検査の仕組み作り（機器の脆弱性に係る接続試験を行うテストベッドの構築を含む。）と対策が不十分な IoT 機器への対応について検討する必要がある。ただし、この検査の仕組みについては、家庭用の IoT 機器から重要インフラで利用される IoT 機器まで様々な IoT 機器がある中で、どの機器を対象とするか慎重に検討する必要がある。

【進捗状況】

「身近な IoT プロジェクト（平成 27 年度補正予算）」の「スマートホームを想定した連携 IoT 機器のセキュリティ検証用テストベッドの構築」事業において、組込み機器向け検証基盤システムと連携したスマートホームのテストベッド環境を構築し、日常生活で使用する情報家電（IoT 機器）におけるセキュリティ上の安全性を検証する事業が行われた。この事業では、スマートホーム内で IoT 機器が連携するユースケースを作成して、実機での脆弱性検証を実施し、評価・検証のスキームを確立するとともに、具体的な検証プロセスをガイドラインとして取りまとめた。

【今後の取組】

IoT 機器の継続的な安全性を確保するためのセキュリティ検査については、民間団体等において、上述のガイドライン等を踏まえつつ実施されているところであり、引き続き実施状況を注視する。（Ｐ）

⑤　簡易な脆弱性チェックソフトの開発等

【本文】

利用している IoT 機器に脆弱性が有するか確認したい利用者に対して、簡易に脆弱性をチェックできるソフトを開発して配布する取組や、脆弱性を調査する民間サービスの実施を促進する取組を検討する必要がある。

【進捗状況】

例えば、一般社団法人重要生活機器連携セキュリティ協議会において製品分野別セキュリティ評価・検証ツールが公開される等、民間団体において IoT 機器のソフトウェア、ハードウェア、ネットワーク等の脆弱性の有無を診断する各種サービスが提供されている。

【今後の取組】

IoT 機器の脆弱性をチェックするためのツールの開発については、民間主導で行うことが基本であり、これらの活動を積極的に支援していくことが求められる。（Ｐ）

（利用段階）

⑥　利用者に対する意識啓発の実施や相談窓口等の設置

【本文】

IoT システムの運用に際しては従来の端末機器以上に利用者による十分な対応が重要となることを踏まえ、利用者に対する意識啓発を推進していくことが求められる。このため、セキュリティに適合している IoT 機器の使用を推奨する取組を進めるとともに、ID/パスワード設定、ファームウェアのアップデート、Wi-Fi 設定の３点を中心とした利用者への意識啓発を行う必要がある。また、利用者からの相談窓口や、脆弱性が見つかった場合の関係機関との調整窓口を設置することが適当であり、関係府省等と連携して具体化を図る必要がある。

【進捗状況】

IoT セキュリティの重要性や総合対策の内容について、サイバーセキュリティ月間における各種イベントのほか、総合通信局等が開催するセミナー等において講演等を行い、普及啓発活動に努めた。また、総務省「国民のための情報セキュリティサイト」を通じて、情報セキュリティ関連の情報提供などを実施した。

国立研究開発法人情報通信研究機構（以下「NICT」という。）がサイバー攻撃に悪用されるおそれのある機器を調査し、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」（項目（１）⑧参照）の実施にあたっては、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セキュリティ対策を案内している。また、IoT 機器のセキュリティ対策の必要性や、本取組の内容の広報のため、家電量販店、公共機関等でのポスター掲示や新聞広告、交通広告等の周知広報活動を実施している。

なお、総務省においては、地方におけるサイバーセキュリティに関する支援組織や人材育成の取組等を拡充するため、平成 30 年７月に各総合通信局等にサイバーセキュリティ室を設置し、地域においてサイバーセキュリティ対策を担当する体制を強化したところである。

【今後の取組】

引き続き、上記の普及啓発活動や「NOTICE」の取組を中心に利用者に対する意識啓発等に努める。

（脆弱性調査の実施）

⑦　重要 IoT 機器に係る脆弱性調査

【本文】

重要 IoT 機器は、サイバー攻撃の対象となった場合に国民生活や社会経済活動に深刻な被害が生じることが想定されるため、特に迅速な対策が求められる。総務省においては、平成 29 年９月から以下の事業を実施しているところであるが、この事業により得られたデータ、ノウハウ等を活用し、調査範囲の拡大、データベースの蓄積等を図る必要がある。

１）重要 IoT 機器の脆弱性調査の実施（現地の設置環境や施工面の状況調査を含む。）。
２）調査結果から脆弱性のある重要 IoT 機器のデータベースの作成。
３）特定された重要 IoT 機器の所有者・運用者・利用者に対して注意喚起を行い、各者による対策を促進。
４）特定された重要 IoT 機器の製造業者に対して情報提供を行い、今後製造する機器への対策を促進。

【進捗状況】

2016 年度（平成 28 年度）補正予算の「サイバーセキュリティの強化」5.0 億円の内数により、2017 年（平成 29 年）９月から、一般社団法人 ICT-ISAC、国立大学法人横浜国立大学等と連携し、重要 IoT 機器を中心に IoT 機器の脆弱性調査を行い、脆弱な IoT 機器を特定した場合には、所有者等に対して注意喚起を行う取組などを行い、2018 年（平成 30 年）７月、その結果を公表した。

このうち、重要 IoT 機器に関する脆弱性調査においては、以下の結果が得られた。

１）　当該調査で検出した脆弱な重要 IoT 機器は 150 件で、そのうち Web インタフェースに記載されている情報から利用者等に関する情報が得られたものが 77 件、そのうち実際に利用者等にコンタクトが取れて、注意喚起等を行ったものが 36 件であった。
２）　検出した重要 IoT 機器（工場、工事現場等）は、消費電力監視装置、水位監視装置、防災設備制御装置、ガス観測警報通知装置等であった。
３）　36 件の内訳は、パスワード設定が適切になされていないものが 27 件、パスワード設定はなされているが認証画面がインターネット上で公開されていたものが９件であった。
４）　今回の調査を通じ、関係者（所有者、利用者、運用者、導入者、製造者）

の重要 IoT 機器に係る脆弱性がもたらし得る脅威の認識が十分でなく認識の共有が十分にできていないことや、多様な関係者間の責任の所在が明確になっていないという課題が明らかとなった。

【今後の取組】

調査結果で得られた知見も踏まえつつ、今後、NOTICE（項目（１）⑧参照）等の取組において対策を進めていくこととする。

⑧　サイバー攻撃の踏み台となるおそれがある機器に係る脆弱性調査

【本文】

家庭用 IoT 機器など、サイバー攻撃の踏み台となってネットワークに悪影響を与えるおそれがある機器については、幅広く調査を行い、脆弱性を有する機器を特定する必要がある。しかし、SHODAN や Censys といった海外の公開データベースに頼った調査では、詳細な仕様が公開されていないため、そのデータベースの信頼性が疑わしく、また把握できる機器にも限りがあることから、脆弱性を有する機器を特定するため、以下の取組を実施する必要がある。

１）サイバー攻撃観測網（NICTER、ハニーポット等）による感染機器の把握。
２）広域の脆弱性スキャンの実施（必要に応じて、調査の研究開発）。
３）上述のサイバー攻撃観測網や脆弱性スキャンを活用し、特定のポートが開いている IoT 機器等についてデータベースを作成。

また、脆弱性を有する IoT 機器を特定した場合には、それらの機器がサイバー攻撃の踏み台となってネットワークに悪影響を与えることとならないよう、以下の取組を実施することを検討する必要がある。

４）特定された脆弱性を有する IoT 機器が踏み台となることを防止するため、所有者・運用者・利用者に対して脆弱な機器の注意喚起を行い、各者による対策を促進。また、製造業者に対して情報提供を行い、今後製造する機器への対策を促進。

なお、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場合の対応として、以下の取組の推進を検討する必要がある。

５）被害拡大を防止するため、ISP による C&C サーバとの通信制御の実施。

【進捗状況】

NICT が運用するサイバー攻撃観測網 NICTER において、2017 年（平成 29 年）に観測されたサイバー攻撃関連通信は２年前と比べて 2.8 倍、また IoT 機器を対象とした攻撃は同期間で 5.7 倍の増加となっている。また、2017 年（平成 29 年）に NICTER で観測したサイバー攻撃関連通信の 54%以上が IoT 機器を狙った

通信であることが確認された[3]。（Ｐ）

脆弱性を有する IoT 機器に関する注意喚起については、2017 年（平成 29 年）９月から実施した重要 IoT 機器に係る脆弱性調査（項目（１）⑦参照）において、脆弱な IoT 機器を特定した場合には所有者等に対して注意喚起を行う取組などを実施した。

上記の調査の一環として、重要 IoT 機器に係る脆弱性調査の他、一般利用者向け IoT 機器の調査を広域スキャンにより実施した。その調査結果から、以下の点の結果が得られた。

１） 本調査において IoT 機器を検索するために構築したスキャンシステムは、「SHODAN」、「Censys」と比較して遜色のない十分な調査能力を有していることが確認された。なお、本調査では国内約 1.5 億個の IP アドレスを対象とし、ネットワークスキャンの結果として何らかの応答を確認したものが約６％であった。また、ポートスキャンの結果から、ウェブサービス（TCP80/443）、メールサービス（TCP25）、テルネットサービス（TCP23）、DNS サービス（TCP53）など、多様なサービスの稼働を確認した。今後、調査手段の改善を図ることで国内における IoT 機器の利用実態などについて、より詳細な調査の実施が可能になることが期待される。

２） バナー情報の分析等により、一部の機種特定が可能であることに加え、機種特定ができない場合においても、製造事業者名や機器類型（カメラ、ルータなど）の機種特定につながる情報が得られることを確認した。今後、他の手法と組み合わせる等の分析手法の高度化によって機種特定の精度を上げることが必要である。

３） 今回の調査では NICTER との連携を試みた。具体的には、NICTER で捉えたマルウェアに感染したと考えられる機器に対してネットワークスキャンを実施したところ、約 55%が反応したものの、依然として反応が見られないケースも多いことが確認された。今後、技術開発等も含めて、分析能力の向上を図ることが重要である。

また、IoT 機器の脆弱性調査については、本総合対策を踏まえ、NICT の業務にパスワード設定に脆弱性がある IoT 機器の調査を行う業務を追加すること等を盛り込んだ「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律案」を 2018 年（平成 30 年）３月に国会へ提出し、同改正法は同年５月に成立し、公布された。

---

[3] 「NICTER 観測レポート 2017 の公開」（2018 年２月　NICT）
http://www.nict.go.jp/press/2018/02/27-1.html

本法においてNICTはIoT機器についてのパスワード設定に脆弱性があるIoT機器に関する技術情報を取得し、これを認定協会（項目（１）⑨参照）を通じて通信事業者に提供することとされており、当該事業者はこの情報をもとに利用者を特定し、パスワード設定の変更を求める注意喚起を行う。2019年（平成31年）２月より、NICTがサイバー攻撃に悪用されるおそれのある機器を調査し、電気通信事業者を通じた利用者への注意喚起を行う取組「NOTICE」を開始した。

【今後の取組】

引き続き、NICT、認定協会、電気通信事業者等と連携した「NOTICE」の取組（項目（１）⑧参照）を通じて、既に設置・運用されているIoT機器の脆弱性への対策を着実に実施する。

⑨　被害拡大を防止するための取組の推進

【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を促進するための方策について、年度内を目途に方向性が得られるよう検討する必要がある。

【進捗状況】

2017 年（平成 29 年）10 月から、総務省において「円滑なインターネット利用環境の確保に関する検討会」を開催し、2018 年（平成 30 年）２月に当該検討会における議論を取りまとめた「対応の方向性」[4]を公表した。

当該検討会においては、DDoS 攻撃等への対策として、DDoS 攻撃等に係る通信の分析を行うことにより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を検知し、利用者等への注意喚起や C&C サーバであると疑われる機器に係る通信の遮断等を行うことが効果的であり、これらの対策を通信の秘密やプライバシーの保護等との調整を図りながら実施していくことが必要であるとされた。

また、精度の高い C&C サーバのレピュテーション情報を得るためには、電気通信事業者が連携して DDoS 攻撃等に関する通信や C&C サーバとの通信等に係る通信を集積した上で、集中的に情報の分析や検証を行い、その結果を広く共有することが必要であることから、電気通信事業者等における情報共有の結節点として電気通信事業者の通信ネットワークを保護する目的で行われる情報共有を促進するため第三者機関を法律上に位置づけ、当該第三者機関における通信の秘密を含む情報の収集、分析、共有等の枠組みを明確化する必要があるとされた。

これらを受け、総務省においては、電気通信事業者間のサイバー攻撃に関する情報の結節点となる第三者機関に係る認定制度等を盛り込んだ「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律案」を 2018 年（平成 30 年）３月に国会へ提出し、同改正法は同年５月に成立し、公布された。なお、同改正法によって新たに位置づけられた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 が認定されており、電気通信事業者への対処を求める通知も認定協会を通じて行われている。

---

[4] 「円滑なインターネット利用環境の確保に関する検討会　対応の方向性」（2018 年２月 円滑なインターネット利用環境の確保に関する検討会）
http://www.soumu.go.jp/main_content/000534017.pdf

【今後の取組】

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。

⑩　IoT 機器に関する脆弱性対策に関する実施体制の整備

【本文】

IoT セキュリティ対策は、例えば、IoT 機器を利用したサービス全体としてのセキュリティを考えれば、機器のライフサイクルの各段階にとどまらず、IoT 機器製造業者、流通業者、保守ベンダー、ISP 及び利用者といった各主体が補完し合いながら対応していくことが求められる。これらの各主体と相互に連携し、ネットワーク全体のセキュリティを確保するため、情報共有のあり方を含め、IoT 機器に対する脆弱性対策を実施する体制（IoT セキュリティ対策センター（仮称））のあり方について、年度内を目途に結論が得られるよう検討する必要がある。

【進捗状況】

IoT 機器に対する脆弱性対策を実施する体制整備については、「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律案」に盛り込み、2018 年（平成 30 年）３月に国会へ提出し、同改正法は同年５月に成立し、公布された。

また同改正法を受け 2019 年（平成 31 年）２月より、同法に基づき NICT がサイバー攻撃に悪用されるおそれのある機器を調査し、電気通信事業者を通じた利用者への注意喚起を行う取組「NOTICE」を開始した。

【今後の取組】

上記の改正法を踏まえ、今後、NOTICE（項目（１）⑧参照）等の取組において対策を進めていくとともに、上述の調査検討で得られた知見も踏まえつつ、IoT 機器製造者、流通業者、保守ベンダー等を含む情報共有のあり方について継続的に検討を進める。

（２）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り、引き続き、サイバーセキュリティ技術、セキュリティ検証プラットフォーム構築活用技術、暗号技術の研究開発等に取り組むとともに、研究開発成果の普及や社会実装を目指すことが求められる。

特に、サイバー攻撃は巧妙化・複雑化しており、特定の組織の情報をターゲットとする標的型攻撃は、近年、特に大きな脅威となっていることから、標的型攻撃への対策に向けた研究開発を重点的に行うことが求められる。

NICT は、平成 29 年５月、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、その攻撃活動を長期観測することで、従来では収集が困難であった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）を開発したことを公表した。

こうした研究開発を基に、今後、早期の社会実装を目指し、新たに出現する未知の標的型攻撃の挙動を早い段階で明らかにするとともに、分析結果をセキュリティ対策機関等と連携して情報共有を図ることが可能な、高度で効率的なサイバー攻撃誘引基盤を構築する必要がある。

【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（ステルス性のより高い観測技術や模擬環境構築の自動化手法の開発等）を図り、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いる。

上記に加え、戦略的イノベーション創造プログラム（SIP）の第１期課題（2015 年度（平成 27 年度）～2019 年度（平成 31 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、東京 2020 オリンピック・パラリンピック競技大会の安心・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。

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り組みを開始した。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。

IoT システムを支える第５世代携帯電話システム（5G）の導入を念頭に置きつつ、SDN/NFV 等のネットワーク制御技術のセキュリティ関連技術の研究開発を推進している。

【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、暗号技術分野については、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。

SIP 第２期においては、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、実証実験に向けた準備を着実に進める。

また、2019 年（平成 31 年）を目途に開始される 5G については、IoT システムの基盤技術であるため、５Ｇに係る各構成要素（デバイス、クラウド、アプリ等）における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、対策の共有等を図ることを通じ、５Ｇを活用する重要インフラ事業者等への周知・啓発を図る。

② 広域ネットワークスキャンの軽量化

【本文】

近年、IoT 機器を狙ったサイバー攻撃は著しく増加傾向にあり、脆弱な IoT 機器への対策は喫緊の課題である。脆弱な IoT 機器のセキュリティ対策のため、膨大な 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。このため、広域ネットワークスキャンの軽量化など、その効率的な実施のために必要な技術開発を推進する必要がある。

【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、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。

2018 年度（平成 30 年度）予算において、「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」として 5.8 億円を計上しており、2018 年度（平成 30 年度）～2020 年度（令和２年度）の３年間を実施期間として、２つの研究開発を行うこととした。

第１に、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を行うため、

１）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「広域ネットワークスキャン遅延原因等推定技術」

２）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「クラスタリングを用いた計算量軽減技術」

３）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「広域ネットワークスキャン最適制御技術」

の開発を行う。

第２に、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を行うため、

１）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「機器特性情報解析技術」
２）広域ネットワークスキャンの頻度を最適化する「広域ネットワークスキャン頻度最適化技術」
３）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「広域ネットワークスキャン対象ポート選定技術」
の開発を行う。

なお、2018 年度（平成 30 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基礎技術の開発を行った。

【今後の取組】
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う。
今後、本研究開発の成果を IoT 機器の脆弱性調査（項目（１）⑧参照）に活用するための連携を進め、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

【本文】

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おり、平成 29 年度から、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が行われている。具体的には、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、これを元に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ことを目指すものである。

今後、IoT 端末はさらなる増加が見込まれており、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、ハードウェアに組み込まれるおそれのあるハードウェア脆弱性を検出する技術の研究開発について、ビッグデータや AI を活用しつつ推進していく必要がある。

【進捗状況】

ハードウェア脆弱性への対応については、「戦略的情報通信研究開発推進事業（SCOPE)」（2017 年度（平成 29 年度）予算　15.3 億円）の中で、2017 年度（平成 29 年度）に採択した「IoT 部品・機器・ネットワークの階層横断セキュリティ技術の研究開発」として進めている。平成 29 年度には、IoT 機器の回路部品において、ハードウェアトロイがない（不正部品の侵入がない）IoT 回路部品を検知する技術の確立を検討した。

2018 年（平成 30 年）２月に外部有識者による継続評価を実施し、2018 年度（平成 30 年度)も引き続き、研究開発を進めていくことになったことを踏まえ、引き続き、「戦略的情報通信研究開発推進事業（SCOPE)」（2018 年度（平成 30 年度）予算　15.5 億円）の中で、「IoT 部品・機器・ネットワークの階層横断セキュリティ技術の研究開発」を実施した。最終年度である同年度には、IoT 機器そのものと IoT ネットワークに焦点を当て、不正動作を検出した後、高速に IoT ネットワークを正常回復する仕組みを構築することを目標として研究開発を実施した。

【今後の取組】

ハードウェア脆弱性については、現状においても IoT 機器の設計・製造工程において不正な回路や部品を仕込まれるリスクが格段に増大しており、サプライチェーン全体のセキュリティの確保の観点からも重要である。今後は AI により、既知・未知の不正回路を検知する技術開発が急務となっていることから、総務省において、回路情報を用いて AI 技術により悪性回路を検知するプロトタイプ技術の研究開発や、電力波形などのシステムの外部情報を用いて、AI 技術に

より悪性機能を検知する技術の研究開発などに取り組む。

④　スマートシティのセキュリティ対策の強化

【本文】

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平成 29 年度から開始している。同様の取組は EU の研究開発プロジェクト Horizon 2020 や米国国立標準技術研究所（NIST）が主導する GCTC（Global City Team Challenge）プロジェクトでも展開されている。スマートシティにおいてデータの連携・解析などを行うプラットフォームのセキュリティ対策はデータの真正性を確保し、かつスマートシティの機能をサイバー攻撃から防御するためにも極めて重要である。

このため、スマートシティのプラットフォームに係るセキュリティ要件の具体化や所要の技術開発を推進するとともに、その成果を国際的な標準化プロセスに提案する等の取組を一体的に進めていく必要がある。

【進捗状況】

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）から実施している。

また、NICT では、欧州連合（EU）との連携により研究開発の促進が期待できる領域について、2013 年度（平成 25 年度）から欧州委員会（EC）と連携して共同で公募を実施しており、2014 年度（平成 26 年度）から第２弾、2016 年度（平成 28 年度)から第３弾の公募を行い､継続して日欧の共同研究を実施してきた。2016 年（平成 28 年）10 月、総務省、NICT 及び欧州委員会は､「第６回日欧国際共同研究シンポジウム」を開催し､その中で今後の研究開発公募に向けた技術ニーズ・シーズ等を議論し情報共有を行った。このシンポジウムを経て、2017 年（平成 29 年）10 月から 2018 年（平成 30 年）１月にかけて、2018 年度（平成 30 年度）から開始する「欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発」に関する公募を行ったところであり、審査・採択を経て､「国立研究開発法人情報通信研究機構運営費交付金」(2018 年度（平成 30 年度）予算　280.3 億円）の中で、2018 年度（平成 30 年度）から取り組んだ。

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、総務省でも 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。

米国国立標準技術研究所(NIST)が主導する GCTC(Global City Team Challenge)プロジェクトについては、2017 年（平成 29 年）８月に「GCTC EXPO 2017」が開催され、2017 年（平成 29 年）秋以降の新たな取組として、サイバーセキュリティ上の課題に焦点を当てる「GCTC-SC3（Smart and Secure Cities and Communities Challenge)」を主催者である NIST と国土安全保障省（DHS）が共同で実施することが発表されたところである。

【今後の取組】

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、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】

宇宙産業の急速な発展に伴い、今後、衛星へのサイバー攻撃（衛星回線の傍受やデータの窃取など）が増加することが懸念される。しかし、衛星の実装スペースの制約等により、マルウェア対策ソフトや暗号仕様を更新するのは容易ではない。

こうした問題意識の下、「宇宙×ＩＣＴに関する懇談会報告書」（平成 29 年８月　宇宙×ＩＣＴに関する懇談会）においても指摘しているように、どれ程の計算力をもってしても解読できない安全性を備えた通信を実現するために、量子暗号技術の研究開発や高秘匿衛星光通信技術の実証を行うとともに、衛星のバックアップや高高度での中継を行うための航空機等による移動体光通信技術の研究開発などに取り組む必要がある。

【進捗状況】

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、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、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。

2018 年度（平成 30 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 3.1 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。

【今後の取組】

2020 年度（令和２年度）末までに装置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）にかけて航空機等による実証実験を行う。

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（人工知能）を活用することにより、サイバー攻撃の検知・解析を自動化することができ、また、機械学習により、サイバー攻撃のパターンを抽象化することで、多様なサイバー攻撃に対する迅速なセキュリティ対策を講ずることが可能となる。

したがって、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。その際、研究開発に有用な各種調査のデータの情報共有の仕組み、検知・解析の対象となるインシデント情報の収集・集約体制、検知･解析に必要となる十分な計算処理能力やシミュレーション能力を有するサイバー攻撃検知・解析環境の整備が求められる。

【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。

現段階の成果例としては、

１）　ダークネットデータに基づいて DDoS 攻撃を早期検知する研究開発
２）　マルウェアの解析を妨げる難読化ツール（パッカー）の特定の自動化に関する研究開発
３）　オンラインマーケットにおいて配布される Android アプリのマルウェア判別分析に関する研究開発

などが挙げられる。

【今後の取組】

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。

（３）民間企業等におけるセキュリティ対策の促進

①　民間企業のセキュリティ投資等の促進

【本文】

民間企業においては、１社がサイバー攻撃の被害を受けた場合に、被害がサプライチェーン全体に広がる懸念が増すことになるため、企業間の取引においても、取引条件としてサイバーセキュリティに関する要求がなされつつある状況にある。しかしながら、コスト等が原因でセキュリティサービスの導入が進んでおらず、また、サイバーセキュリティ製品の効果的な活用もできていない状況にある。

そこで、経済産業省と連携して、IoT 産業等の関連産業等の成長を見据え、企業におけるセキュリティ投資を促進するため、高レベルのサイバーセキュリティ対策に必要なシステムの構築やサービスの利用に対して、税制優遇措置を講ずる方向で検討していく必要がある。

【進捗状況】

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 IoT 税制（コネクテッド・インダストリーズ税制）について、2018 年度（平成 30 年度）の税制改正に向けて経済産業省と共同で要望し、2018 年（平成 30 年）６月に関係法令が施行された。

具体的には、当該税制を利用しようとする事業者は、生産性向上特別措置法（平成 30 年法律第 25 号）に基づき、データの安全管理の方法[5]や、その内容の適正性及びその運用について担保する情報処理安全確保支援士（登録セキスペ）等を記載することとしている「革新的データ産業活用計画」を作成し、主務大臣に提出し、「生産性向上特別措置法第二十九条の規定に基づく生産性の向上に特に資するものとして主務大臣が定める基準」（平成 30 年内閣府、総務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省告示第２号）に適合することについてその確認を受け、その認定を受けることによ

[5] 生産性向上特別措置法施行規則（平成 30 年内閣府、公正取引委員会、個人情報保護委員会、総務省、法務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省、原子力規制委員会令第１号）で定められている様式第 19「革新的データ産業活用計画の認定申請書」においては、データの安全管理の方法として、①データにアクセスできる組織又は個人を必要最小限に制限する機能、②データ連携を行うシステム間の通信経路から盗取されないような機能、③データに対する外部からの不正なアクセスに対する防御に必要な機能、④データを連携させるシステムに対する不正なアクセス等を検知する体制、⑤不正なアクセス等により被害が生じた場合の対処方針、⑥データの提供を受ける法人又は個人における安全確保対策、⑦データを連携させるシステムについての定期的な脆弱性確認の方法を記載することとされている。

り、同計画に基づき取得又は制作するソフトウェア、器具用品、機械装置に対して特別償却 30%又は税額控除３％（平均給与等支給額の対前年度増加率が３％以上となる場合は５％）を措置することとしている。（2019 年（平成 31 年）２月 28 日現在の認定事業社数 33 社）

また、民間企業においてセキュリティ対策を進めるためには、特に経営層の中で、セキュリティ対策が企業経営において重要な課題であるとの認識が深まることが重要である。

そのため、企業の経営層が自社のセキュリティ対策の現状を正しく認識し、また、他社の状況と比較することを通じて、さらに必要な具体的な対策を検討・導入できるような環境が実現することに加えて、こうした取組を積極的に進めている企業が、市場を含む第三者から適切に評価されることが必要である。こうした環境を実現するためには、自社のセキュリティ対策に係る情報について、経営層に限らず、社内全体で共有するとともに、関係企業及び社会全体に対して適切な方法・範囲で開示（共有）されることが必要であると考えられる。

こういった課題意識から、2017 年（平成 29 年）12 月に、タスクフォースのもとに「情報開示分科会」を設置し、民間企業のセキュリティ対策の情報開示に関する課題を整理し、その普及に必要な方策について検討を行い、その結果をとりまとめ、2018 年（平成 30 年）６月に情報開示分科会報告書[6]として公表した。同報告書においては今後の取組として、社内の情報共有に向けた戦略マネジメント層等の育成、関係者間の情報共有促進のための仕組みづくりの検討、第三者開示の促進に向けたガイドラインの策定等を進めていくこととしており、2019 年（平成 31 年）１月より同分科会において、サイバーセキュリティ対策に関する民間企業の情報開示の手引きの策定に向けた議論を進めている。（項目（３）②を参照）

【今後の取組】

上記のコネクテッド・インダストリーズ税制は 2020 年度（令和２年度）末を適用期限としていることから、今後、その活用状況を把握・分析するとともに、企業のニーズ等を反映したセキュリティ投資促進のための政策支援のあり方について、引き続き検討していく。また、情報開示の促進については、民間企業のサイバーセキュリティ対策に係る情報開示の手引きを 2019 年度（令和元年）度早期に策定し、公表する。（項目（３）②を参照）

---

6 「情報開示分科会　報告書」（2018 年６月　サイバーセキュリティタスクフォース　情報開示分科会）
http://www.soumu.go.jp/main_content/000555901.pdf

② 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、セキュリティ対策を講じている企業が市場を含む第三者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。

米国においては、日本の有価証券報告書にあたる 10－K 報告書において記載することが推奨されるセキュリティ対策について証券取引委員会（SEC）がガイドラインを策定・公表している。こうした情報開示はあくまで任意のものであるが、企業の対策促進の観点からみて有益な取組であると考えられる。

このため、我が国においても、あくまで任意の情報開示であることを前提としつつ、企業のセキュリティ対策に係る情報開示に関するガイドラインの策定について、関係府省と連携しつつ、年度内を目途に一定の結論が得られるよう検討する必要がある。その際、開示する情報の粒度については情報開示が新たな攻撃を誘発しないよう十分に配慮するとともに、こうした情報開示とサイバーセキュリティ保険の普及の在り方について併せて検討する必要がある。

【進捗状況】

前述のとおり、2017 年（平成 29 年）12 月に、タスクフォースの下に「情報開示分科会」を設置し、民間企業のセキュリティ対策の情報開示に関する課題を整理し、その普及に必要な方策について検討を行い、その結果をとりまとめ、2018 年（平成 30 年）６月に情報開示分科会報告書として公表した。

同分科会における検討の結果、サイバーセキュリティ対策の情報開示については、開示の対象者によって目的、方法、項目、その粒度等に違いがあることから、「社内の情報共有（第一者開示）」、「契約者間等の情報開示（第二者開示）」、「社会に対する情報開示（第三者開示）」の３つの側面に分けて議論を整理することとされた。

このうち、社内の情報共有（第一者開示）については、引き続き、経営層の理解を深め、セキュリティ対策の担当部署の現場と経営層の間を繋ぐ、いわゆる「戦略マネジメント層」等の育成に向けた取組を進める必要があるとされた。

また、契約者間等の情報開示（第二者開示）については、契約者間等で確認すべき事項や必要な対策の整理、サプライチェーン全体又はグループ全体における情報共有体制の構築の促進が必要であるとされた。さらに、サイバーセキュリティ保険の活用に向けて、セキュリティ対策及びその開示のインセンティブとなるような割引制度の普及や、グループ全体又はサプライチェーン全体で一括して加入するような保険商品の展開が期待されるとした。

加えて、社会に対する情報開示（第三者開示）については、事業者の規模や取組状況に応じて、セキュリティ対策の自己宣言制度や主要５項目[7]の開示、「情報セキュリティ報告書」の作成など、段階的に対策を講じていくことが望ましいとされた。

その後、2019 年（平成 31 年）１月より上記の分科会において、社会に対する情報開示（第三者開示）の促進のため、サイバーセキュリティ対策に関する民間企業の情報開示の手引きの策定に向けた議論を進めているところである。

【今後の取組】

情報開示の促進については、民間企業のサイバーセキュリティ対策に係る情報開示の手引きを 2019 年度（令和元年）度早期に策定し、公表する。

7 ①セキュリティに関する基本方針等の策定状況（情報セキュリティ基本方針、情報セキュリティポリシーの策定等）、②セキュリティに関する管理体制（情報セキュリティマネジメント体制、CSIRT の設置等）、③社員に対する教育・人材育成（従業員に対する研修の実施等）、④社外との情報共有体制（ＩＳＡＣや日本シーサート協議会への加盟等）、⑤第三者評価・認証の取得状況（情報セキュリティマネジメントシステム（ISMS）の国際規格「ISO/IEC27001:2005」及び「JISQ27001:2006」の認証を取得等）

③　事業者間での情報共有を促進するための仕組みの構築

【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・非常時などの状況に応じた提供すべき情報の範囲及び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。

そのため、事業者間での情報共有を促進するための仕組みを検討する必要がある。具体的には、新たに情報共有を開始する事業者との間でも安全・安心な情報共有ができるよう、情報提供元及び共有される情報自体の信頼性を担保する仕組みや、様々な事業者から提供された大量の情報の分析、情報の重複の排除、情報の重み付け、サイバー攻撃の全体像の把握を行った上で、入力フォーマットの標準化などの情報共有を実施する仕組みを検討する必要がある。また、国内の民間団体においては、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）との連携を開始しており、こういった取組を支援することも重要である。

【進捗状況】

情報共有を実施する仕組みを検討するため、ICT-ISAC と連携して、サイバー攻撃に関する情報を収集・分析・共有するための情報共有基盤の試行環境を構築する取組を実施し、ICT-ISAC において、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）との連携を図りつつ、関係事業者等に情報共有を行った。また、情報共有基盤の普及を図るため、2018 年（平成 30 年）３月、ICT-ISAC において、情報共有基盤の仕組み、利用方法等を示す「脅威情報の情報共有基盤　利用ガイドライン（事業者向け）」を策定した。

このほか、日米の ISAC 間の情報共有、連携を進めており、2017 年（平成 29 年）11 月に東京で「第２回 ISAC 国際連携ワークショップ」を開催し、日本の ICT-ISAC、米国の Comm-ISAC、IT-ISAC 及び Auto-ISAC との間で、脅威情報の共有等に関する意見交換・議論を行った。また、日米 ISAC 間の脅威情報の自動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、2019 年（平成 31 年）２月に「第３回 ISAC 間連携国際ワークショップ」を開催した。（項目（５）②参照）

【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。

④　情報共有時の匿名化処理に関する検討

【本文】

情報を共有する際、当該情報に通信のネットワーク設備に係る情報などのセンシティブな情報や個人情報が含まれ得ることから、事業者によっては情報共有をすることに対して消極的になることが想定される。

そこで、情報共有に当たって、情報の秘匿性を担保する観点から、情報の匿名化処理の導入を検討する必要がある。その際、どのような方法で、どの程度まで情報を匿名化するべきかについての評価指標やガイドラインの整備を検討する必要がある。なお、これらの検討事項については、情報共有基盤等を活用した自動化処理の可能性に留意して検討する必要がある。

【進捗状況】

「重要インフラの情報セキュリティ対策に係る第４次行動計画」(2017 年４月サイバーセキュリティ戦略本部決定）[8]に基づき、重要インフラ事業者等において、インシデントが発生し、NISC へ報告する際、必要に応じて匿名化等を行った上で情報を共有する仕組みが構築されている。また、ICT-ISAC において策定した前述の「脅威情報の情報共有基盤　利用ガイドライン（事業者向け）」では、情報共有（項目（３）③参照）を行う際には、機微情報を適切に除外することが必要である旨が明記されている。

【今後の取組】

事業者等による積極的な情報共有を促進するための取組について、機微情報等の匿名化処理を含め、引き続き検討を行う。

8 「重要インフラの情報セキュリティ対策に係る第４次行動計画」（2017 年４月サイバーセキュリティ戦略本部決定）
https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf

⑤　公衆無線 LAN のサイバーセキュリティ確保に関する検討

【本文】

公衆無線 LAN については、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。）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。しかし、多くの公衆無線 LAN のサービスにおいて、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ことが考えられる。このため、公衆無線 LAN におけるサイバーセキュリティ上の課題を整理し、今後必要な対策について、年度内を目途に一定の結論が得られるよう検討する必要がある。

【進捗状況】

2017 年（平成 29 年）11 月に、「公衆無線 LAN セキュリティ分科会」をタスクフォースの下に設置し、公衆無線 LAN のセキュリティ対策のあり方とセキュリティに配慮した公衆無線 LAN サービスの普及策について検討を行い、その結果をとりまとめ、2018 年（平成 30 年）３月、公衆無線 LAN セキュリティ分科会報告書[9]として公表した。

同報告書では、公衆無線 LAN のセキュリティ対策に係る周知啓発について、わかりやすいツールの利用やコンテンツの充実を図ることが適当である旨などが示されている。

周知・啓発の一環として、（株）ドコモの運営する大規模オンライン講座プラットフォーム「gacco」において、公衆無線 LAN のリスクやセキュリティ対策等を解説するオンライン教育コンテンツを 2019 年（平成 31 年）２月から同年３月まで開講・配信し、3,837 名の受講登録があった。

【今後の取組】

引き続き、安全に無線 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。

9 「公衆無線 LAN セキュリティ分科会　報告書」（2018 年３月　サイバーセキュリティタスクフォース　公衆無線 LAN セキュリティ分科会）
http://www.soumu.go.jp/main_content/000539751.pdf

４）人材育成の強化

①　実践的サイバー防御演習（CYDER）の充実

【本文】

NICT は、大規模仮想 LAN 環境上に CYDER を構築し、平成 28 年度は全国 11 地域において約 1,500 名を対象に演習を実施し、平成 29 年度においては全国 47 都道府県において約 3,000 名を対象に演習を実施することとしている。引き続き、国の行政機関・地方自治体及び重要インフラ事業者などを対象としてこうした取組を進めるとともに、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よう努める必要がある。

【進捗状況】

実践的サイバー防御演習（CYDER）については、「ナショナルサイバートレーニングセンターの構築」として 2017 年度（平成 29 年度）予算において 15.0 億円、2018 年度（平成 30 年度）予算において 15.1 億円を計上し、全国 47 都道府県で開催した。2017 年度（平成 29 年度）は 100 回の演習で計 3,009 名（うち国の行政機関 316 名、地方公共団体 1,889 名、重要インフラ事業者 553 名、その他 251 名）、2018 年度（平成 30 年度）は 107 回の演習で計 2, 666 名（うち国の行政機関 386 名、地方公共団体 1,664 名、重要インフラ事業者 397 名、その他 219 名）が受講した。

また、演習プログラムについては、2018 年度（平成 30 年度）より、重要社会基盤事業者に対するサイバー攻撃への防護がますます重要になっていることから、重要社会基盤事業者に特化したシナリオと環境で演習を行うコースとして、金融・交通インフラ・医療・教育研究機関・一般向けに、B-3 コースを新設した。

【今後の取組】

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に対し、開催手法等の工夫を通じてより多くの受講機会を確保できるよう配慮する。

また、演習内容については、受講者のニーズやネットワーク環境等を踏まえたコースの再編等を行うなど、対象者のサイバー攻撃への対応能力向上に向けた柔軟な取組を推進する。

② 2020 年東京大会に向けたサイバー演習の実施

【本文】

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、大会組織委員会のセキュリティ担当者を中心に、攻撃側と防御側の手法の検証及び訓練を行う環境を整備している。平成 28 年度に開始した本事業について、更なる内容の拡充を図り、より実践的な環境の下でのサイバー演習の強化を図る必要がある。また、大会終了後に、同システムによる演習の実施により得られた知見、ノウハウを活用する方策について併せて検討する必要がある。

【進捗状況】

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」については、2017 年度（平成 29 年度）、東京オリンピック・パラリンピック競技大会組織委員会（以下「組織委員会」という。）のセキュリティ担当者等を対象に演習を実施し、初級・中級コース（２月）と準上級コース（３月）を各１回ずつ開催し、延べ 74 名が受講した。

2018 年度（平成 30 年度）においては新たに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を開設し、延べ 347 名が受講した。また、従来からのコロッセオ演習（実機演習）では、初級コース 38 名、中級コース 51 名、準上級コース 48 名の延べ 137 名が受講した。

【今後の取組】

NICT において、2019 年（平成 31 年）３月にサイバーコロッセオ実施計画を改定し、2019 年度（平成 31 年度）以降の対象者の受講機会を拡大することとしている。具体的には、①受講機会を３クール制（第１クール（2019 年（令和元年）６月～８月）、第２クール（2019 年（令和元年）９月～12 月）、第３クール（2020 年（令和２年）１月～３月）に分散、②コロッセオカレッジについて、より実践に即したスキルを習得できる科目を増やし、内容を充実化、③中級コース、準上級コースの演習シナリオを追加、などの改善を図ることとしている。

引き続き、東京 2020 オリンピック・パラリンピック競技大会に向けて組織委員会と連携しつつ、より実践的なサイバー演習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】

我が国のサイバーセキュリティ技術は、世界のセキュリティソフトウェアの市場における存在感が決して大きくないなど、製品開発等における分野では遅れをとっている。サイバー攻撃は、日々刻々と変化しており、高度な技術力を支えるセキュリティ人材の育成に中長期的に取り組む必要がある。

具体的には、引き続き、若年層の ICT 人材に対し、集中的な研修を行うとともに、海外派遣による経験等を通じて、サイバーセキュリティのコア技術を開発できるような人材、あるいは、そのような技術力を生かしてリスクを許容し、積極的に起業ができるような人材の育成方策を検討し、そうした人材に対する支援の枠組みの構築を促進する必要がある。

【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、NICT の持つサイバーセキュリティの研究資産を活用し、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・開発等を、第一線で活躍する研究者・技術者が 1 年かけて継続的かつ本格的に指導するものである。2017 年度（平成 29 年度）は 10 歳から 24 歳の 39 名が、2018 年度（平成 30 年度）は 12 歳から 24 歳の 46 名がプログラムを修了した。

プログラムでは、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。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）[10]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。

【今後の取組】

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。

[10] 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。

④　IoT セキュリティ人材の育成

【本文】

IoT が社会に実装されていく中、従来の通信分野のみならず、製造、流通、サービスなど多岐にわたる分野で IoT システムが構築・運用されるものと見込まれる。このため、広く IoT セキュリティを担うことができる人材の育成が不可欠である。

そこで、IoT セキュリティに関するスキルを獲得するための教材作成や研修体制の整備、各種調査のデータの共有、機器の脆弱性に係る接続試験を行うテストベッドの構築等を行うための総合的な対策を産学官の連携により推進するための環境整備に向けた検討を行う必要がある。

【進捗状況】

多様な分野・業種において膨大な数の利活用が見込まれている IoT 機器を適正に利用できる人材を育成するため、2017 年度（平成 29 年度）から「IoT 機器等の適正利用のための ICT 人材育成」事業（2018 年度（平成 30 年度）予算 2.7 億円の内数）を実施している。

本事業では、

１）　IoT 機器等の電波利用システムの適正利用に関するテキストの作成
２）　ユーザ企業等を対象とした地域毎の講習会の開催
３）　開発者を目指す若者を対象とした講習会・ハッカソン体験の開催

を行っている。

2017 年度（平成 29 年度）においては、１）で作成したテキストを用いて、講習会を全国主要都市・地域で計 19 回開催するとともに、講習会の模様を e-ラーニング形式で公開し、講習会及び e-ラーニングに計約 1,000 名が参加した。

2018 年度（平成 30 年度）においては、技術の進展等を反映して１）で作成したテキスト及び講習内容を更新し、これに基づく講習会を全国各地で 27 回開催するとともに、講習の内容を e-ラーニング環境において公開し、計約 3,000 名の参加があった。

また、人口減少が急速に進む地方において、サイバーセキュリティ人材を確保することは大きな課題となっていることから、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」をタスクフォースの下に、2018 年（平成 30 年）12 月に設置した。

【今後の取組】

多様な分野における IoT セキュリティ人材の育成を加速化する観点から、IoT セキュリティに関するスキルを獲得するための教材作成や研修体制の整備を引き続き行う。

また、2019 年（令和元年）４月の分科会において議論された「サイバーセキュリティ人材育成分科会　第１次取りまとめ案」にて示された地域におけるセキュリティ人材育成に向けた以下の三つの方策を推進する。

１）地域のセキュリティファシリテーターの育成

地域のコミュニティ活動を活性化するため、中核としてリードするファシリテーター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。

２）地域でのセキュリティ人材のシェアリング

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。

３）地域における人材エコシステムの形成

就業につながる研修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。沖縄をはじめとする地域において、国際的に通用する人材も含めた様々なレベルのセキュリティ人材育成のエコシステムの構築を図る。

（５）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協力ハブの構築による実践的サイバー防御演習「CYDER」等の海外展開を通じ、３年間（平成 29 年～平成 31 年）で 500 人を目標として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 情報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、2017 年(平成 29 年) 12 月にカンボジアで開催された「第 12 回日 ASEAN 情報通信大臣会合」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。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 150 名以上が参加した。また、2018 年（平成 30 年）11 月には同センターにおいて、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」も開催された。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、2018 年（平成 30 年）10 月に東京で開催された「第 11 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。

2018 年（平成 30 年）12 月にインドネシアで開催された「第 13 回日 ASEAN 情報通信大臣会合及び第 14 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 2019」がとりまとめられた。

さらに、2019 年（平成 31 年）２月にシンガポールで開催された「第９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。

このほか、2018 年度（平成 30 年度）は、インドネシアにおいて標的型サイバー攻撃の検知、遮断、可視化及び侵入経路分析を行うソリューションの有効性に関する実証実験を、ID-SIRTII と協力して実施した他、マレーシアでは拠点間ネットワークをソフトウェア技術を用いて低コストに集中管理・制御可能な国産の SD-WAN 技術を活用したセキュリティ共通基盤導入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、カンボジアでは郵便電気通信省と連携し、それぞれ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

【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、2019 年（令和元年）10 月にタイで開催される「第 12 回日 ASEAN サイバーセキュリティ政策会議」、同年 11 月にラオスで開催される「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」、同年度内に東京で開催予定の「第 10 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】

国際的な ISAC（Information Sharing and Analysis Center）間連携を引き続き推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 との連携を強化し、通信事業者、IoT 機器ベンダー、セキュリティベンダー等が、AIS 等を介して脅威情報を自動的に共有し、サイバーセキュリティ対策に活用することを促す必要がある。

【進捗状況】

2019 年（平成 31 年）２月に東京で開催された「第３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。

【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、2019 年度（令和元年度）内を目処に「第４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 システムのセキュリティに係る国際標準化が ISO/IEC 及び ITU-T で開始されているところであり、関係する府省庁と連携しつつ、こうした活動に積極的に貢献していくことが求められる。その際、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ける議論等を通じ、産学官連携による検討結果を国際標準に反映すべく努める必要がある。

【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。

2018 年（平成 30 年）４月に中国で開催された 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が、新規標準化課題として承認された。

2018 年（平成 30 年）９月に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文書が勧告草案として承認された。

また、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ことから、「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、次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ところである。

①人の正当性を確認できる仕組み（リモート署名）
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）
③IoT 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）

【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。

また、トラストサービスの在り方については、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ことも踏まえ、国際的な相互運用性の確保の観点からも、引き続き、トラストサービス検討ワーキンググループにおいて、技術的課題や制度的課題等について整理を行い、トラストサービスの制度化に向けた検討を行う。

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。

【進捗状況】

二国間協議については、2018 年（平成 30 年）３月にフランスで行われた「日仏 ICT 政策協議」、同年６月にドイツで行われた「日独 ICT 政策対話」、同年７月に東京で行われた「日・シンガポール ICT 政策対話」、同月に米国で行われた「インターネットエコノミーに関する日米政策協力対話」、同年 12 月にオーストリアで行われた「日 EU・ICT 政策対話」において、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）に総務省はイスラエル国家サイバー総局との間でサイバーセキュリティ分野における協力覚書を締結した。

その他、2018 年（平成 30 年）11 月にパリで開催された IGF への参加や 2019 年（平成 31 年）３月の ICANN 神戸会合におけるローカルホストとしての参画など、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。特に G20 については、我が国が 2019 年（令和元年）の議長国であることから、サイバー空間における国際ルー

ルを巡る議論について主導的な役割を果たす。

Ⅱ　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総合対策の改定に向けた議論を行っており、本プログレスレポートの結果も適切に反映させていく。

さらに、2018 年（平成 30 年）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 セキュリティ対策の強化を進めていく。