資料１０－２

IoT セキュリティ総合対策
プログレスレポート 2018（案）

平成 30 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 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。【資料１】

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。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 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、この方針に沿って、本文書では、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ている。また、本文書の中で言及された実証実験等の成果については参考資料として付されている。さらに、政府が 2018 年７月に決定予定の新たな「サイバーセキュリティ戦略」と総合対策の関係についても参考資料において整理している。【資料２、３】

---

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

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。

【進捗状況】

2017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た。2018年６月に開催された右会合において、「IoT機器のセキュリティ対策に関する検討の方向性」がまとめられた。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。【資料４】

また、情報通信審議会IPネットワーク設備委員会において、情報通信ネットワークの安全･信頼性を確保するため、DDoS攻撃の原因となるIoT機器がマルウェアに大量感染する事態を防止すること等を目的として、IoT機器を含む端末設備の技術基準に最低限のセキュリティ対策を追加することについて、2018年６月に第１次報告案をとりまとめた（意見招請手続を実施中）。

【今後の取組】

IoT機器のセキュリティ対策に係る認証制度については、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他、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。こうした点については、引き続き上記の WG において情報共有等を図るとともに、本タスクフォースにおいても注視し、必要に応じて提言を行うこととする。

また、情報通信審議会における検討については、意見募集の結果を踏まえ、IoT 機器等の端末設備の最低限のセキュリティ対策（アクセス制御機能、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、ファームウェアの更新機能等）について取りまとめた上、関係省令等の改正など所要の手続を進める。

（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 において、検討が進められてきた（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ところであり、その取組の一環として平成 30 年度戦略的情報通信研究開発推進事業（SCOPE）のプロジェクトとして採択されたところである。

【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。【資料５】

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を検証した。

【今後の取組】

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。【資料６】

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。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。

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も求められる。

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

（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】

上記事業の実施結果等も踏まえ、引き続き、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についての検討を行う。

その際、認証の仕組みの議論（項目（１）①参照）を踏まえつつ、IoT 機器のセキュリティ検査（単独の機器の検査に加え、IoT 機器を組み込んだ情報システムとしての検査を含む）を行う地域拠点を整備することについても検討を行う。当該拠点においては IoT 機器のセキュリティ確保のための関連人材の育成等の場として活用することを併せて検討する。

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、総務省としても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。その際、ツールによって検証すべき事項について、一定の共通要件（基本的な検証項目として盛り込むことが望ましい事項）を整理してガイドラインとして整理することも考えられる。その検討においては、IoT 機器を取り巻くセキュリティ環境が動的かつ急速に変化していくことが見込まれることから、例えば、脆弱性データベースに登録されている脆弱性のうち影響度の高いものに係る対策が講じられているかどうかをツールで検証可能とすること等が考えられ、こうした仕組みを実現するための関係者の連携のあり方等についても検討することが適当である。

（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。

【今後の取組】

上記の取組を継続するほか、IoT 機器の脆弱性に係る調査（項目（１）⑧参照）において、情報通信研究機構（以下「NICT」という。）による脆弱性調査の結果を踏まえ、電気通信事業者が脆弱性を有する IoT 機器の利用者を特定して注意喚起を行う取組を年度内に開始することとしている。その際、本調査の内容に関する問い合わせやパスワード設定の変更等に係る相談を受け付けるサポートセンターを設置することとしており、IoT 機器に係るセキュリティ対策について利用者を支援する体制を整備する。その際、消費者庁などの関係政府機関とも連携していく。

なお、総務省においては 2018 年夏を目途に各総合通信局等においてセキュリティ対策を担当する体制を強化することとしており、地方におけるサイバーセキュリティに関する支援組織の拡充や人材の育成にも取り組んでいく。

（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】

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６月、その結果を公表した。【資料７】

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。【資料８】

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】

今回の調査結果で得られた知見も踏まえつつ、今後 NICT を主体とする IoT 機器の脆弱性調査（項目（１）⑧参照）等を実施していくこととする。

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]。【資料９】

脆弱性を有する IoT 機器に関する注意喚起については、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。【資料 10】

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。【資料 11】

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、これを第三者機関（項目（１）⑨参照）を通じ

[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

て通信事業者に提供し、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発出することとしている。【資料 12】

【今後の取組】

「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」は公布の日から起算して９ヶ月以内に施行されることから、関係省令の整備を行うとともに、NICT の中期計画等の改正を行うほか、NICT が当該業務を行う際の実施計画を関係府省と協議の上で認可する等の諸準備を進め、2018 年度内に当該業務を開始することとしている。

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 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。【資料 13】

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。【資料 14】

【今後の取組】

「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」は公布の日から起算して９ヶ月以内に施行されることから、関係省令等の整備を行うとともに、改正法に基づき行われることが期待される情報共有の

[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

枠組について電気通信事業者等に周知を行っていく。

また、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、有識者等からなる研究会を開催し、実施できる範囲、手法等について検討を行い、具体的な実施に向けた留意点を整理するとともに、必要に応じて民間ガイドラインの改定を促す等により、実施に向けた体制を整える。

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。

【今後の取組】

上記の改正法を踏まえ、所要の規定等の整備を進める（項目（１）⑧及び⑨参照)。また、こうした制度の整備・運用とともに、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。具体的には、以下の研究開発を行っている。

まず、サイバーセキュリティ分野については、

１）　可視化ドリブンなセキュリティオペレーション技術の実現に向けたサイバー攻撃統合分析プラットフォーム「NIRVANA 改」の機能強化（大量のアラートの中から緊急性の高い事象の抽出を行うことによる防御策の迅速な展開の実現、「アラート・フィルタ機能」の強化及び時系列グラフの形に整理する「アラート・リプレイ機能」の開発）と技術移転

２）　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）【資料 15】

等を行っている。

また、暗号技術分野については、

３）　新たなニーズに応える機能を備えた機能性暗号技術の研究開発及び成果展開（高い安全性と相互接続性を有する群構造維持デジタル署名方式の開発、リソースに制約のある IoT 機器にも実装可能な軽量暗号に関する「CRYPTREC 暗号技術ガイドライン（軽量暗号）」の策定・公表）
４）　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及び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
５）　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の研究開発

等を行っている。

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（平成 27～31 年度（予定））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。

【今後の取組】

平成 30 年度予算において、「国立研究開発法人情報通信研究機構運営費交付金」として計上している 280.3 億円の内数を措置しており、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を行う。

特に、サイバー攻撃誘引基盤「STARDUST」については、平成 29 年度補正予算において「サイバー攻撃対策高度化研究開発環境の整備」として 10.0 億円を措置しており、サイバー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研究開発環境の整備を加速する。

また、SIP 第１期の研究開発課題については、研究開発成果の社会実装に向けて継続して実施する。加えて、平成 30 年度から５年間実施予定の SIP 第２期では、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むこととしている。本課題では、IoT 機器やサプライチェーンの各構成要素についてセキュリティの確保（信頼の創出）とその確認（信頼の証明）を繰り返し行い、信頼のチェーンを構築・維持することで、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行い、実サービスや各産業分野において実証を行うこととしている。

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、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 16】

【今後の取組】
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、平成 30～32 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ている。
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」

の開発を行うこととしている。
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」

の開発を行うこととしている。

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）に随時適用し、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)」（平成 29 年度予算　15.3 億円）の中で、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２月に外部有識者による継続評価を実施し、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。【資料 17】

【今後の取組】

引き続き、「戦略的情報通信研究開発推進事業（SCOPE)」（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」を進める。最終年度である平成 30 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する。

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」（平成 29 年度予算　5.1 億円の内数）を平成 29 年度から実施[5]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 年度から第２弾、2016 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 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 10 月から 2018 年１月にかけて、2018 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８月に「GCTC EXPO 2017」が開催され、2017 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ている。

[5]平成 29 年度は６地域（北海道札幌市、神奈川県横浜市、兵庫県加古川市、香川県高松市、福島県会津若松市及び埼玉県さいたま市浦和美園地区）で実施した。

【今後の取組】

「データ利活用型スマートシティ推進事業」については、平成30年度予算で2.5億円を計上しており、引き続き、面的拡大を図るとともに、多様な主体の参画支援や、グリーンフィールド（埋立地や工場移転跡地などの更地）への導入を促進するプロジェクトを実施することとしている。

また、「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」については、上記公募に係る審査・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」(平成30年度予算　280.3億円)の中で、2018年度から取り組む。

さらに、スマートシティの展開にあたっては、流通するデータが窃取されたり、改ざんされたりすることのないよう、そのプラットフォームにおけるセキュリティ対策（情報の機密性、真正性及び可用性の確保）が極めて重要となる。このため、EUの研究開発プロジェクトHorizon 2020や米国NISTが主導するGCTCプロジェクト等の国際的な動向も踏まえ、上記事業で得られた知見も活かしつつ、スマートシティにおけるセキュリティ確保策について検討を開始し、年内を目途に一定の結論を得る。

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。【資料 18】

【今後の取組】

平成 30 年度予算において、「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、平成 34 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）　量子暗号装置を超小型衛星に搭載するための小型化・軽量化を可能にする実装技術

２）　稼働率及びユーザビリティの向上とサービス拡大を図るための光地上局用空間光通信機器の小型化・軽量化及び光地上局の可搬化技術

３）　衛星から出射された光ビームを可能な限り細く絞り光地上局の望遠鏡に結合させるための高精度捕捉追尾技術

を開発するとともに、上記１）～３）で開発した技術を集約・統合し、航空機等による実証実験を行うこととしている。

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 技術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。具体的には機械学習を活用し、

１）　ダークネットへのトラフィックデータを基に DDoS 攻撃の発生を早期検知する研究開発
２）　マルウェアの分析を妨げる難読化ツール（パッカー）を特定する作業の自動化に関する研究開発
３）　オンラインマーケットにて配布される Android アプリがマルウェアであるかどうかを分析する研究開発

を行っている。【資料 19】

【今後の取組】

平成 30 年度予算において、「国立研究開発法人情報通信研究機構運営費交付金」として計上している 280.3 億円の内数を措置しており、引き続き、NICT において、機械学習等を応用した通信分析技術の高度化と試験運用を行うなど、AI を活用したサイバー攻撃の検知・解析を自動化する研究開発を推進する。

（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、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６月に関係法令が施行された。【資料 20】

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[6]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

6 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。

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 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６月に情報開示分科会報告書[7]として公表した。

【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平成 32 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、セキュリティ対策の情報開示・共有の促進については、上記報告書において、今後の取組として、社内の情報共有に向けた橋渡し人材等の育成、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いる。（項目（３）②を参照）

7 「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 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６月に情報開示分科会報告書として公表した。【資料 21】

同分科会における検討の結果、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「橋渡し人材」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[8]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。

当該報告書を踏まえ、民間企業におけるセキュリティ対策の情報開示を推進することにより、情報開示による「セキュリティ対策の見える化」を通じて、民間企業の経営層が自社のセキュリティ対策の現状を認識し、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し、導入する「セキュリティ対策の好循環」が起こる環境の実現等が期待される。

【今後の取組】

当該報告書においては、今後の取組として以下の５項目の取組を中心に産学官が連携しつつ進めていくこととしている。

（社内の情報共有に向けた橋渡し人材等の育成）

１．人材のスキルの具体化、スキル取得のための教育コンテンツの開発・普及、スキル認定を行う仕組みを産学官により構築するための検討。（平成 30 年度中を目途に方向性を整理）

（関係者間の情報共有促進のための仕組みづくりの検討）

２．米国等における ISAO（Information Sharing and Analysis Organization）等の動向等について調査するとともに、公的支援のあり方について検討。（平成 30 年度中を目途に検討結果を取りまとめ）

３．セキュリティベンダー、損害保険会社、その他の関連する企業によるサイバーセキュリティ保険を含む総合サービスの開発に向けたモデル事業を推進し、標準仕様化に向けて検討。また、企業のセキュリティ対策の強度を簡易に診断できるツールキットを評価する仕組みづくりを検討。（モデル事業については平成 30 年度に検討）

（第三者開示の促進に向けたガイドラインの策定）

４．「セキュリティ対策情報開示ガイドライン」（仮称）を策定・公表。（平成 30

---

[8] 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）

年秋を目途にガイドラインを策定）

５．「コネクテッド・インダストリーズ税制」の活用状況を分析するとともに、企業のニーズ等を反映した投資促進のための政策支援のあり方について検討。（支援税制の運用にあわせて適宜実施）（項目（３）①参照）

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。【資料 22、23】

このほか、2017 年 11 月に東京で「第２回 ISAC 間連携国際ワークショップ」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（項目（５）③参照）。

【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のほか、脆弱性情報を活用することによる早期対策の促進を可能とする仕組みの検討を行うとともに、人工知能（AI）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。

このほか、日米 ISAC 間のサイバーセキュリティ連携対策を更に促進するため、2018 年 11 月頃を目処に「第３回 ISAC 間連携国際ワークショップ」を開催する。

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）[9]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。

[9] 「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 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３月、公衆無線 LAN セキュリティ分科会報告書[10]として公表した。【資料 24】

同報告書では公衆無線 LAN サービスの普及に当たっては、提供者は多様な方式を提供するなどサービスの選択肢を増やし、利用者がそれらのサービスを適切に選択できる環境を整備することが必要である旨が示されている。

あわせて、「セキュアな公衆無線 LAN 環境の実現に向けた行動計画」を策定し、セキュリティに配慮した公衆無線 LAN の普及に向けて、「利用者・提供者の意識向上」、「データ利活用施策との連携」及び「優良事例の普及」を図ることとしている。

【今後の取組】

当該行動計画においては、今後の取組として以下の３項目の取組を中心に産官学が連携しつつ進めていくこととしている。

１　利用者・提供者の意識向上

（国における取組）

■　Wi-Fi 利用者・提供者向けマニュアル（手引き）の改定（2018 年夏頃を目途）

10 「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

■　オンライン教育等の教育コンテンツを活用した周知・啓発（2018 年秋頃を目途に開始）

■　e-ネットキャラバン等の活動を通じた青少年・高齢者向けの公衆無線 LAN の利用に関する周知・啓発（2018 年度以降に実施）

■　「公衆無線 LAN 版安全・安心マーク」に関する周知活動の実施（今後も継続的に実施）

（民間事業者における取組）

■　暗号化の有無を識別可能な公衆無線 LAN サービスの提供（接続アプリの提供等）（民間事業者の取組に期待）

２　データ利活用施策との連携

（国・民間事業者における取組）

■　公衆無線 LAN サービスと IoT おもてなしクラウドとの連携推進（2019 年中を目途に実用化）

３　優良事例の普及

（国・民間事業者等における取組）

■　自治体に対する公衆無線 LAN 環境整備支援事業の継続的推進（2019 年度まで継続）及び優良事例の普及促進（優良事例の調査・公表及びこれを踏まえた所要の政策支援については 2018 年夏以降に実施）

■　デジタルスタジアムの実現に向けたセキュアな公衆無線 LAN 環境の整備及び公衆無線 LAN サービスの SSID 等の情報や接続アプリを、オリンピック・パラリンピック公式サイトといった信頼できるサイトにおいて提供する仕組みの構築（2018 年度以降に実施）

（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、2017 年度、全国 47 都道府県で 100 回の演習を実施し、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）が受講している。また、NICT は、サイバー演習の運営に係るコストの削減と、受講者のプロファイルに合わせた効果的な演習プログラムの提供を行うためのサイバー演習自動化システム「CYDERANGE」（サイダーレンジ）を開発した。【資料 25、26、27】

【今後の取組】

実践的サイバー防御演習（CYDER）を実施しているナショナルサイバートレーニングセンターについては、平成 30 年度予算において「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 15.1 億円計上している。

実践的サイバー防御演習（CYDER）では、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する演習を実施している。具体的には、2018 年度においては全組織共通の A コース（初級・全 60 回）、地方公共団体向けの B-1 コース（中級・全 20 回）、国の行政機関向けの B-2 コース（中級・全 10 回）に加え、重要インフラ事業者向けの B-3 コース（中級・全 10 回）を新設し、さらなる内容の充実を図ることとしている。引き続き、演習プログラム・教育コンテンツの開発を継続的に行いつつ、「CYDERANGE」を活用した受講者のニーズに応じた演習を実施する。

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、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、計 74 名が受講した。【資料 25、28】

【今後の取組】

「サイバーコロッセオ」を実施しているナショナルサイバートレーニングセンターについては、平成 30 年度予算において「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 15.1 億円計上している。

2018 年度以降も、さらなる演習規模の拡大、演習内容の拡充を図りつつ、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し、最終的には約 220 人のセキュリティ担当者等を育成する予定である。

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】

若年層の 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」については、2017 年度、39 名がプログラムを修了した。【資料 25、29】

「SecHack365」は、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、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。具体的には、受講者は NICT の有する遠隔開発環境「NONSTOP」を活用し、常時どこからでも遠隔開発実習を行うことができ、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している。また、2018 年３月には４名の受講生を SXSW（South by Southwest）[11]に海外派遣し、SXSW Hackathon スポンサー賞を受賞した。

【今後の取組】

「SecHack365」を実施しているナショナルサイバートレーニングセンターについては、平成 30 年度予算において「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 15.1 億円計上している。

2018 年度は受講者として 50 名を選定し、受講生の特性に合った３つのコース（表現駆動コース、思索駆動コース、開発駆動コース）を設置している。今後も引き続き、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

[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。

一の育成に取り組む。

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、「IoT 機器等の適正利用のための ICT 人材育成」事業（平成 29 年度予算 2.5 億円の内数）を 2017 年度から実施している。

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。

【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、マルウェア等のデータの共有、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について、産学官による具体的な連携体制を含め検討するとともに、民間団体等のこうした取組を積極的に支援する。

（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 10 月にフィリピンにおいて実践的サイバー防御演習（CYDER）を実施するとともに、同年 11 月にはタイにおいて「Cyber SEA Games」を開催した。また、2017 年 12 月の「第 12 回日 ASEAN 情報通信大臣会合」において、ASEAN とのサイバーセキュリティ分野での人材育成協力の強化を目指すプロジェクト「日 ASEAN サイバーセキュリティ能力構築センター」についてタイで４年間実施することが、日 ASEAN 間で合意された。本センターは JAIF（日・ASEAN 統合基金）の資金供与により実現し、2018 年７月から本格的に稼働することとしており、実践的サイバー防御演習（CYDER）、デジタルフォレンジック、マルウェア解析からなるサイバーセキュリティ演習等を ASEAN 各国からの参加者に提供する予定である。【資料 30、31】

また、2017 年 10 月にシンガポールで開催された「第 10 回日 ASEAN 情報セキュリティ政策会議」では、我が国のサイバーセキュリティに関する取組について情報を共有し、相互理解を深めた。【資料 32】

さらに、2018 年２月に東京で開催された、日本及び ASEAN の ISP 間の情報共有を促進する「第８回日 ISP 向け ASEAN 情報セキュリティワークショップ」においては、日 ASEAN の ISP の取組の共有及び DDoS 対策などの連携可能性について議論を行うとともに、机上で合同サイバー攻撃対応演習を実施した。【資料 33】

【今後の取組】

「日 ASEAN サイバーセキュリティ能力構築センター」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・助言を行う。

また、2018 年度の我が国のサイバーセキュリティに関する取組を共有し、今後の連携強化について議論するため、2018 年 10 月に東京で開催される「第 11 回日 ASEAN サイバーセキュリティ政策会議」に参加する。

さらに、日 ASEAN の ISP 間の具体的な連携方策の議論及び信頼関係の更なる強化のため、2019 年２月にシンガポールで「第９回 ISP 向け日 ASEAN 情報セキュリティワークショップ」を情報通信メディア開発庁（IMDA）と共催する。

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】

2017 年 11 月に東京で「第２回 ISAC 間連携国際ワークショップ」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（項目（３）③参照）。脅威情報の自動共有に向けたステップとして、米国の IT-ISAC が利用中の情報共有プラットフォームに、日本の ICT-ISAC が試行的に参加することを合意した。また日本の ICT-ISAC と米国の National Council of ISAC(NCI) の協力を継続・深化させることについても合意した。【資料 34】

【今後の取組】

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、2018 年 11 月頃を目処に「第３回 ISAC 間連携国際ワークショップ」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。【資料 35、36】

2018 年４月の ISO/IEC JTC1 SC27 武漢会合において、ISO/IEC 27030 (Guidelines for security and privacy in Internet of Things (IoT))が新規標準化課題として承認された。

【今後の取組】

ITU-T SG17 においても、「IoT セキュリティガイドライン」の重要性が認識されており、今後は ISO/IEC との共同文書としての国際標準化を目指した取組を進める。

また、サイバー空間における認証にはトラストが不可欠である。EU において、トラストを担保する仕組みである eIDAS（電子識別・認証サービス）規則が運用されていることを踏まえ、我が国も EU の標準であるトラストリスト（適格トラストサービス・プロバイダーのリスト）との相互認証を目指した実証試験に取り組む。

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】

2017 年９月にイタリアで開催された「G7 情報通信・産業大臣会合」において、オープンで自由なインターネットを支持し、次世代生産革命における投資と信頼性を促進し、グローバルなデジタル経済の成長を下支えするための 14 の原則を確認している。【資料 37】

また、二国間協議については、2017 年 10 月に東京で行われた「第 23 回日 EU ICT 政策対話」、2018 年３月にフランスで行われた「第 20 回日仏 ICT 政策対話」、同年６月にドイツで行われた「第３回日独 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実施し、関係強化及び信頼醸成に取り組んだ。

【今後の取組】

デジタルエコノミー実現のため、基盤となるサイバーセキュリティの確保が不可欠である。その認識のもと、デジタルエコノミー実現において重要な会議である「G20 デジタル経済大臣会合」（2018 年８月にアルゼンチンで開催予定）の議論に積極的に参画する。特に G20 については、我が国が 2019 年の主催国であることから、サイバー空間における国際ルールを巡る議論についても主導的役割を果たしていくことが求められる。

Ⅱ　今後の進め方

総合対策においては、その推進にあたって、必要に応じて検証を行い、進捗状況を把握するとともに、本分野における技術革新や最新のサイバー攻撃の態様を踏まえ、必要に応じて随時見直しを行っていくことが望ましいとされており、引き続き、タスクフォースにおいて、プログレスレポートによる各施策の進捗の管理及び検証を行うこととする。また、必要に応じて総合対策の改定等の見直しを行う。

さらに、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。

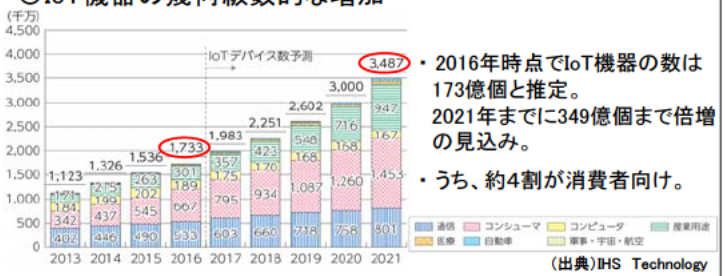
参考資料

【資料1】

IoTセキュリティ総合対策（平成29年10月公表）

現状

○IoT機器の幾何級数的な増加

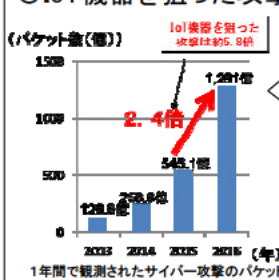


・2016年時点でIoT機器の数は173億個と推定。
2021年までに349億個まで倍増の見込み。

・うち、約4割が消費者向け。

（出典）IHS Technology

○IoT機器を狙った攻撃が急増

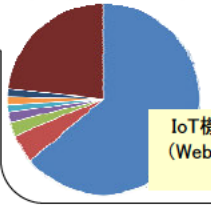


1年間で観測されたサイバー攻撃のパケット数

観測された全サイバー攻撃
1,281億パケットのうち、

$\frac{2}{3}$

がIoTを狙っている！



IoT機器を狙った攻撃
（Webカメラ、ルータ等）
64%

○IoT機器を踏み台にした大規模攻撃が発生

・2016年10月21日米国のDyn社のDNSサーバーに対し、大規模なDDoS攻撃が2回発生。

・同社からDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生。

・サイバー攻撃の元は、「Mirai」というマルウェアに感染した大量のIoT機器。

対策

IoTセキュリティ総合対策

脆弱性対策に係る体制の整備

・IoT機器の脆弱性についてライフサイクル全体（設計・製造、販売、設置、運用・保守、利用）を見通した対策が必要。

・脆弱性調査の実施等のための体制整備が必要。

研究開発の推進

・セキュリティ運用の知見を情報共有し、ニーズにあった研究開発を促進。

民間企業等におけるセキュリティ対策の促進

・民間企業等のサイバーセキュリティに係る投資を促進。

・サイバー攻撃の被害及びその拡大防止のための、攻撃・脅威情報の共有の促進。

人材育成の強化

・圧倒的にセキュリティ人材が不足する中、実践的サイバー防御演習等を推進。

国際連携の推進

・二国間及び多国間の枠組みの中での情報共有やルール作り、人材育成、研究開発を推進。

半年に1度を目途としつつ、必要に応じて検証
（関係府省と連携）

「サイバーセキュリティ戦略（案）」の全体概要

【資料2】

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。また、危機管理対応についても一層の強化 等

新「サイバーセキュリティ戦略」と「IoTセキュリティ総合対策」の関係

【資料3】

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
（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
②セキュリティ対策に係る情報開示の促進

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
（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【再掲】
②セキュリティ対策に係る情報開示の促進【再掲】

3．安全なIoTシステムの構築
（1）脆弱性対策に係る体制の整備
①セキュリティ・バイ・デザイン等の意識啓発・支援の実施
②認証マークの付与及び比較サイト等を通じた推奨
③IoTセキュアゲートウェイ
④セキュリティ検査の仕組み作り
⑤簡易な脆弱性チェックソフトの開発等
⑥利用者に対する意識啓発の実施や相談窓口等の設置
⑦重要IoT機器に係る脆弱性調査
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
⑩IoT機器に関する脆弱性対策に関する実施体制の整備
（5）国際連携の推進
③ 国際標準化の推進

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
（1）脆弱性対策に係る体制の整備
⑨被害拡大を防止するための取組の推進
⑩IoT機器に関する脆弱性対策に関する実施体制の整備【再掲】
（3）民間企業等におけるセキュリティ対策の促進
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

2．官民一体となった重要インフラの防護
（3）民間企業等におけるセキュリティ対策の促進
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【再掲】
④情報共有時の匿名化処理に関する検討
（4）人材育成の強化
①実践的サイバー防御演習（CYDER）の充実

3．政府機関等におけるセキュリティ強化・充実
（2）研究開発の推進
①基礎的・基盤的な研究開発等の推進
（4）人材育成の強化
①実践的サイバー防御演習（CYDER）の充実【再掲】
②2020年東京大会に向けたサイバー演習の実施

4．大学等における安全・安心な教育・研究環境の確保

5．2020年東京大会とその後を見据えた取組
（4）人材育成の強化
②2020年東京大会に向けたサイバー演習の実施【再掲】

6．従来の枠を超えた情報共有・連携体制の構築
（3）民間企業等におけるセキュリティ対策の促進
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【再掲】
④情報共有時の匿名化処理に関する検討【再掲】
（5）国際連携の推進
②国際的なISAC間連携

7．大規模サイバー攻撃事態等への対処態勢の強化

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
（5）国際連携の推進
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

2．我が国の防御力・抑止力・状況把握力の強化
（5）国際連携の推進
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【再掲】

3．国際協力・連携
（5）国際連携の推進
①ASEAN各国との連携
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【再掲】

横断的施策

人材育成・確保
（4）人材育成の強化
①実践的サイバー防御演習（CYDER）の充実【再掲】 ②2020年東京大会に向けたサイバー演習の実施【再掲】 ③若手セキュリティ人材の育成の促進 ④IoTセキュリティ人材の育成

研究開発の推進
（2）研究開発の推進
①基礎的・基盤的な研究開発等の推進【再掲】 ②広域ネットワークスキャンの軽量化 ③ハードウェア脆弱性への対応
④スマートシティのセキュリティ対策の強化 ⑤衛星通信におけるセキュリティ技術の研究開発 ⑥AIを活用したサイバー攻撃検知・解析技術の研究開発

全員参加による協働
（1）脆弱性対策に係る体制の整備
⑥利用者に対する意識啓発の実施や相談窓口等の設置【再掲】
（3）民間企業等におけるセキュリティ対策の促進
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

※ 赤字は「IoTセキュリティ総合対策」における具体的施策の項目。

IoT推進コンソーシアム

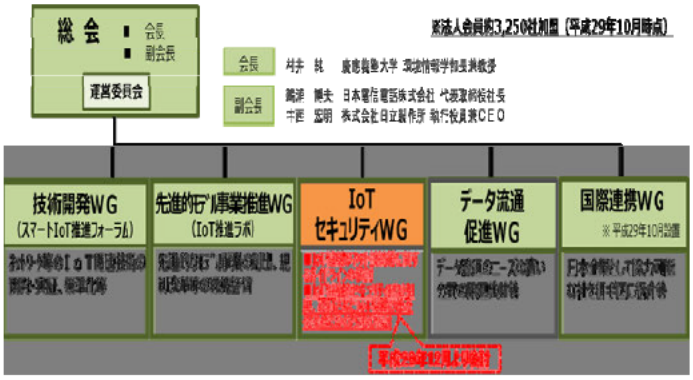
【資料4】

○ 概要：
　IoTセキュリティ総合対策（平成29年10月3日　サイバーセキュリティタスクフォース）において、セキュリティ・バイ・デザインの考え方を踏まえて設計された機器に認証マークを付与することや、比較サイト等を通じてセキュアな機器の使用が推奨される（利用者が容易にセキュアなIoT機器を確認できる）仕組みの構築について、具体的な検討を進める必要性が指摘されている。
　このことを受けて、IoT推進コンソーシアム IoTセキュリティワーキンググループにおいて、「IoTセキュリティガイドラインver1.0」の普及啓発やIoT機器のセキュリティ確保策等について検討を行う。

○ 開催実績（平成29年12月以降）：
　平成29年12月11日（取組状況の共有等）、平成30年6月14日（今後の検討の方向性の議論等）

検討体制（IoT推進コンソーシアム）

- IoT／ビッグデータ／人工知能時代に対応し、企業・業種の枠を超えて産学官で利活用を促進するため、総務省及び経済産業省の共同の呼びかけのもと、民主導の組織として「IoT推進コンソーシアム」を設立。（平成27年10月23日（金）に設立総会を開催。）
- 技術開発、利活用、政策課題の解決に向けた提言等を実施。



【IoTセキュリティWG　構成員】

	有村　浩一	一般社団法人JPCERTコーディネーションセンター　専務理事
	出縄　秀一	在日米国商工会議所　サイバーセキュリティタスクフォース共同委員長
	鵜飼　結可	株式会社FFRI　代表取締役社長
	大矢　晴一郎	一般社団法人 ビジネス機械・情報システム産業協会　委員
	小川　真史	青山学院大学理工学部機械創造工学科　教授
	荻野　司	一般社団法人 重要生活機器連携セキュリティ協議会　代表理事
	金子　優一	一般社団法人日本電機工業会　専電部　技術課
	川上　晨一	一般社団法人電子情報技術産業協会　常務理事
	小山　覚	一般社団法人　日本経済団体連合会　情報通信委員会 企画部会長代行・サイバーセキュリティに関する懇談会委員
（座長）	佐々木　良一	東京電機大学　教授
	四ノ宮　大輔	一般社団法人情報通信ネットワーク産業協会 通信ネットワーク機器セキュリティ分科会主査
	新　誠一	横浜国立大学 大学院 環境情報研究院　教授
	高田　広章	名古屋大学大学院情報科学研究科教授 （附属　組込みシステム研究センター　センター長）
	寺原　哲史	株式会社NTTドコモ　情報セキュリティ部
	徳田　英幸	国立研究開発法人情報通信研究機構　理事長
	中尾　康二	国立研究開発法人情報通信研究機構／KDDI株式会社　顧問
	中野　利彦	株式会社日立製作所　インフラシステム社　制御セキュリティセンタ　センター長
	西原　政勇	明治大学　名誉教授
	森　亮二	弁護士法人　英知法律事務所　弁護士／ニューヨーク州弁護士
	吉岡　克成	横浜国立大学大学院　環境情報研究院　准教授

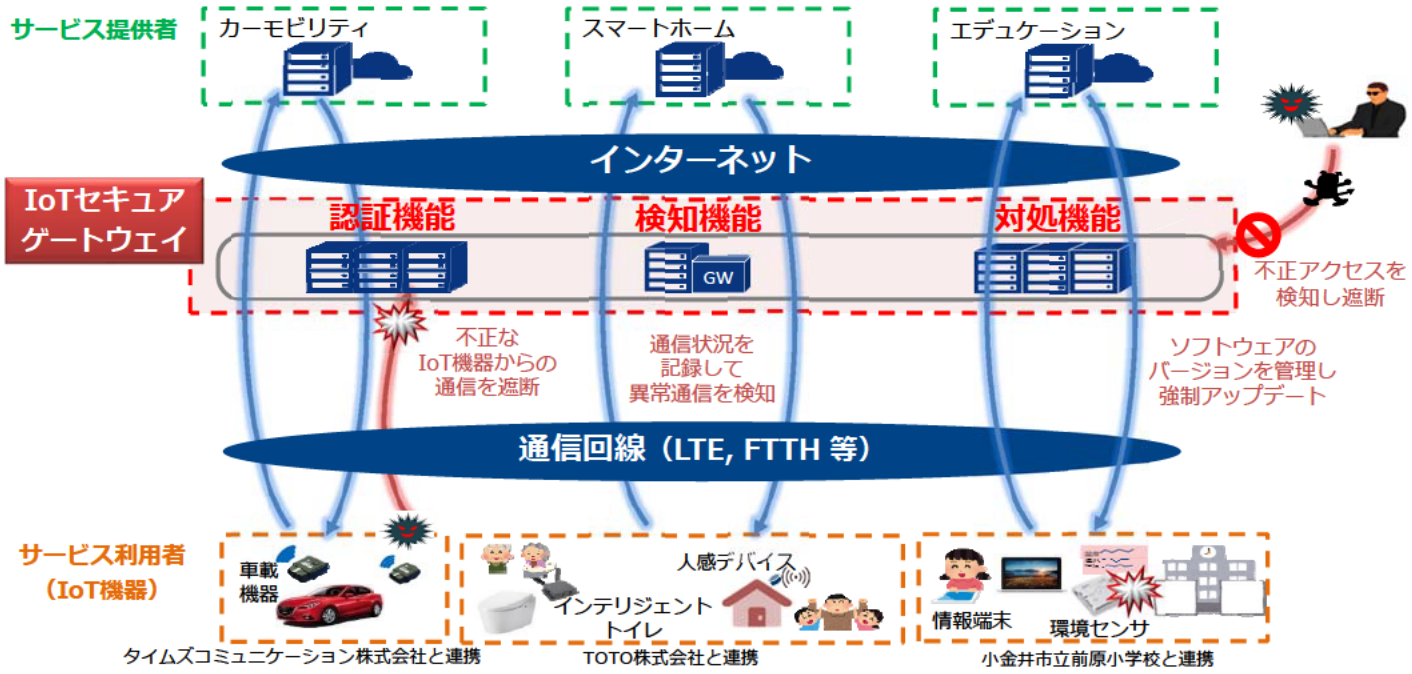
IoTセキュアゲートウェイの実証実験

【資料5】

○ IoT機器とインターネットの境界にIoTセキュアゲートウェイを設置し、その有用性に関する実証実験を実施。
○ 様々なセキュリティ脅威に対して、認証、検知、対処といった一連のセキュリティ対策ができるかを試行。

実証実験のイメージ

実施主体：NTTコミュニケーションズ株式会社、平成29年12月より実証実験を開始（平成28年度補正（2.5億円））



IoTセキュアゲートウェイの実証実験結果について

【資料6】

○　**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、良好な運用が行えた**。IoTセキュアゲートウェイは認証、検知、対処といった機能は十分提供できており、**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。その課題を解決するために、**異常な通信を検知する機能を向上させる必要がある**。

運用上の課題の例

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**に以下の誤検知が発生。

・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**

・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**

改善

検知機能の向上

（1）機能改善

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が必要。

テンプレート無し　　テンプレート利用

（2）動的検知

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必要（※）。

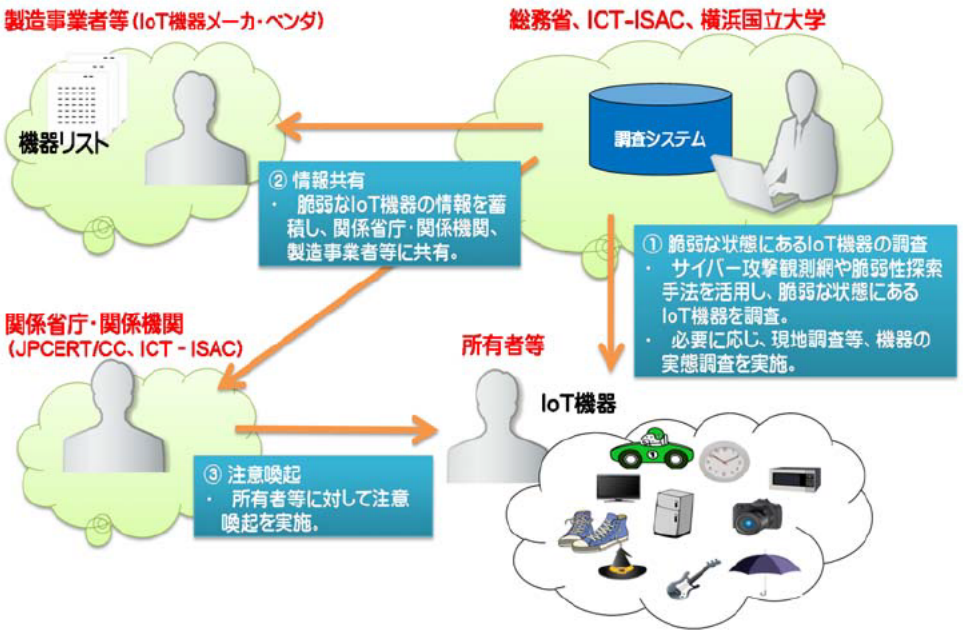
※　AIを用いたデータ分析の活用も考えられる。

IoT機器に関する脆弱性調査等の実施（平成29年9月5日 報道発表）

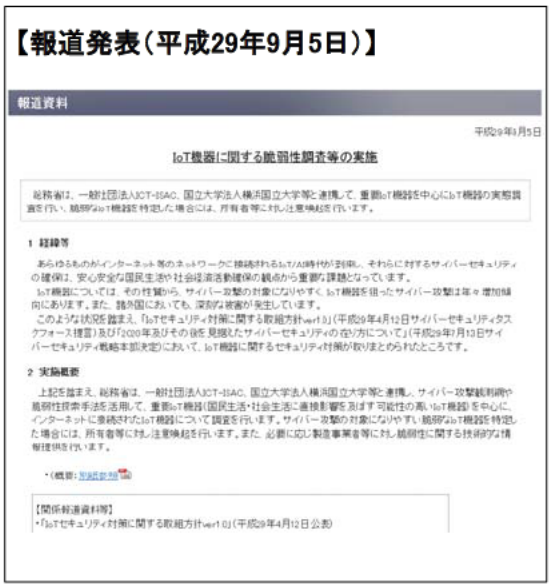
【資料7】

○　サイバー攻撃観測網や脆弱性探索手法を活用して、重要IoT機器（国民生活・社会生活に直接影響を及ぼす可能性の高いIoT機器）を中心に、インターネットに接続されたIoT機器について調査を実施。

○　サイバー攻撃の対象になりやすい脆弱な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実施。また、必要に応じて製造事業者等に対して脆弱性に関する技術的な情報提供を実施。



【報道発表（平成29年9月5日）】



報道資料

平成29年9月5日

IoT機器に関する脆弱性調査等の実施

総務省は、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て、重要IoT機器を中心にIoT機器の実態調査を行い、脆弱なIoT機器を特定した場合には、所有者等に対し注意喚起を行います。

1 経緯等

あらゆるものがインターネット等のネットワークに接続されるIoT/AI時代が到来。それらにおけるサイバーセキュリティの確保は、安心安全な国民生活や社会経済活動確保の観点から重要な課題となっています。

IoT機器については、その性質から、サイバー攻撃の対象になりやすく、IoT機器を狙ったサイバー攻撃は年々増加傾向にあります。また、諸外国においても、深刻な被害が発生しています。

このような状況を踏まえ、「IoTセキュリティ対策に関する取組方針（ver1.0）」（平成28年4月12日サイバーセキュリティタスクフォース提言）及び「2020年及びその後を見据えたサイバーセキュリティの在り方について」（平成29年7月13日サイバーセキュリティ戦略本部決定）において、IoT機器に関するセキュリティ対策が取りまとめられたところです。

2 実施概要

上記を踏まえ、総務省は、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、サイバー攻撃観測網や脆弱性探索手法を活用して、重要IoT機器（国民生活・社会生活に直接影響を及ぼす可能性の高いIoT機器）を中心に、インターネットに接続されたIoT機器について調査を行います。サイバー攻撃の対象になりやすい脆弱なIoT機器を特定した場合には、所有者等に対し注意喚起を行います。また、必要に応じ製造事業者等に対し脆弱性に関する技術的な情報提供を行います。

・（概要）別紙参照

【関係報道資料等】

・「IoTセキュリティ対策に関する取組方針（ver1.0）」（平成28年4月12日公表）

重要インフラ等で利用されるIoT機器の調査

【資料8】

＜実施内容＞

○ サイバー攻撃観測網やネットワークスキャンを活用して、重要インフラ等で利用される脆弱な重要IoT機器※を調査。

○ Webインタフェースに記載されている情報等から当該機器の所有者等を特定し、所有者等に当該機器の設置状況、システム構成等をヒアリングした上で、想定されるリスク、対策の必要性の説明などの注意喚起を実施。

○ また、必要に応じて製造事業者等に対しリスクに関する技術的な情報提供を実施。

※ 重要インフラ等で利用される機器は、国民生活等に直接影響を及ぼす可能性があることを踏まえ、脆弱な重要IoT機器とは、パスワード設定が適切になされていないものに加え、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るものも含むこととした。

調査・注意喚起の流れ

①重要IoT機器の探索

日本国内のグローバルIPアドレス（IPv4）について、主に80/tcpに対してアクティブスキャン等を行い脆弱な状態にある機器を検出。

②利用事業者などの特定、コンタクト

Webインタフェースに記載されている情報等から、所有者・運用者・利用者等の特定を試みる。

③設置環境や設定状況等を現地でヒアリング（実地調査）、電話や電子メールで調査（類似事例調査）

所有者等にコンタクトをとり、必要な者から同意を得た上で、当該機器の設置環境、設定状況、システム構成等を現地調査
※ 類似案件については、電話又は電子メールでヒアリング

④脆弱性解消のための注意喚起、対策例の提示

所有者等に想定されるリスクを伝え、対策の必要性を説明。
（対策例：推測されにくいパスワードの設定、アクセス制御の実施、VPNの導入）

⑤対策状況の確認

調査結果（概要）

【調査結果概況】

- 本件調査により検出した脆弱な重要IoT機器は150件、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。
- 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。
- 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。

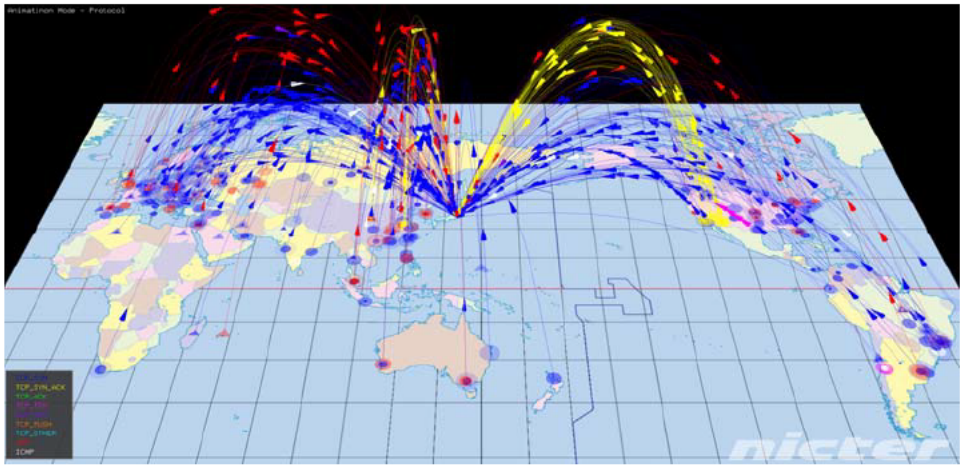
【ヒアリング調査等の結果（ポイント）】

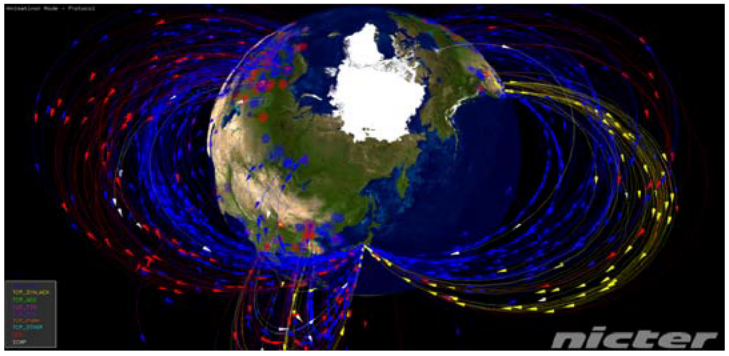
- 関係者（所有者、利用者、運用者、導入者、製造者）の脅威に対する認識が十分でない、または、認識の共有が十分にできていない。
- 多様な関係者間の責任の所在が明確になっていない。

NICTERによる観測

【資料9】

○ 国立研究開発法人 情報通信研究機構（NICT）では、未使用のIPアドレス30万個（ダークネット）を活用し、グローバルにサイバー攻撃の状況を観測。





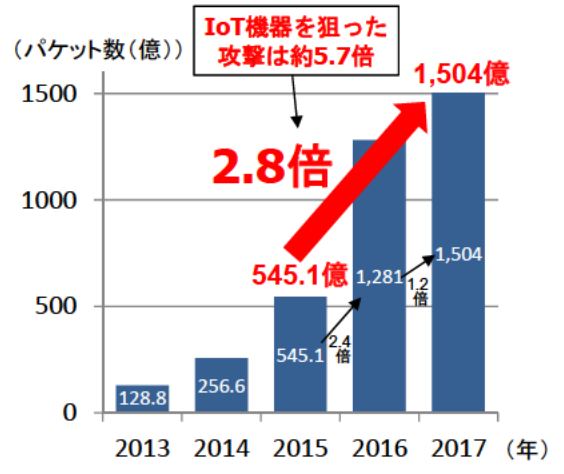
- TCP SYN
- TCP SYN/ACK
- TCP ACK
- TCP FIN
- TCP RESET
- TCP PUSH
- TCP Other
- UDP
- ICMP

・ダークネットに飛来するパケットの送信元アドレスから緯度・経度を推定し、世界地図上で可視化

・色：パケットごとにプロトコル等を表現

NITCERで１年間に観測されたサイバー攻撃回数

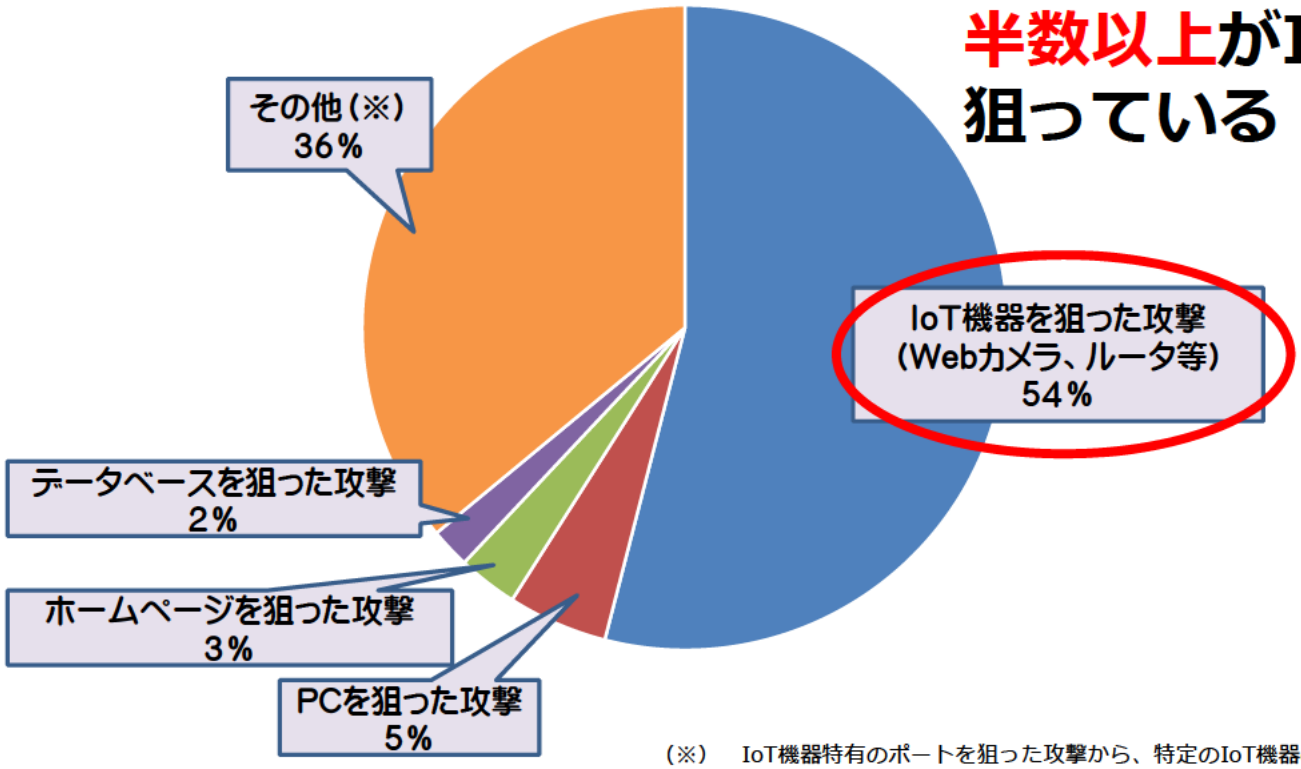
・2年間で2．8倍
（2015年→2016年：2．4倍、2016年→2017年：1．2倍）



サイバー攻撃の内訳（2017年、NICTERによる観測）

観測された全サイバー攻撃1,504億パケットのうち、

半数以上がIoTを狙っている！



（※） IoT機器特有のポートを狙った攻撃から、特定のIoT機器の脆弱性を狙ったより高度な攻撃も観測されるようになっており、単純にポート番号だけから分類することが難しいIoT機器を狙った攻撃が「その他」に含まれている。

家庭用ルータ、防犯カメラ等の一般利用者向けIoT機器の調査①【資料10】

＜実施内容＞

○ 日本国内のグローバルIPアドレス（IPv4）で接続されたIoT機器に広くネットワークスキャンを行うためのシステムを構築

○ 上記システムを用いてネットワークスキャンを行い、開放ポート（稼働しているサービス）の調査等を実施。

○ ネットワークスキャンによって得られるバナー情報等をもとにした機種特定について検証を実施。

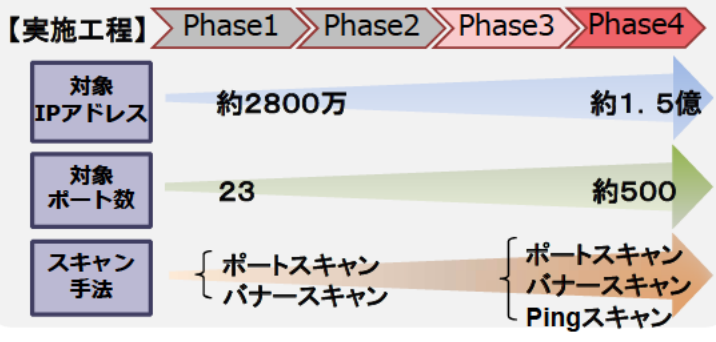
※ ネットワークスキャンで発見した脆弱な機器の所有者等への注意喚起にあたっては、IoT機器の機種を特定できれば、それぞれの製品毎の設定変更やファームウェアの適用、サポート等を行うことが可能となる。

○ NICTERで観測したマルウェア感染機器に関する情報と連携した分析を実施。

※ ネットワークスキャンの結果から、マルウェア感染機器の特定、感染の可能性がある機器の事前把握などができれば、マルウェア対策に有益な情報となる。

＜ネットワークスキャン実施条件等＞

- 本調査で対象としたIPアドレスは、日本へ割り当てられているもののうち、海外で利用されている可能性があるものや到達性のないものなどを除外した約1．5億個。
- 調査対象ポートは、約500ポート（TCPポート）。
- 調査対象やネットワークへの影響を考慮し、またシステム稼動状態の確認を行いつつ調査規模を段階的に拡大。



調査結果（概要）

【ネットワークスキャンを行うシステムの構築】

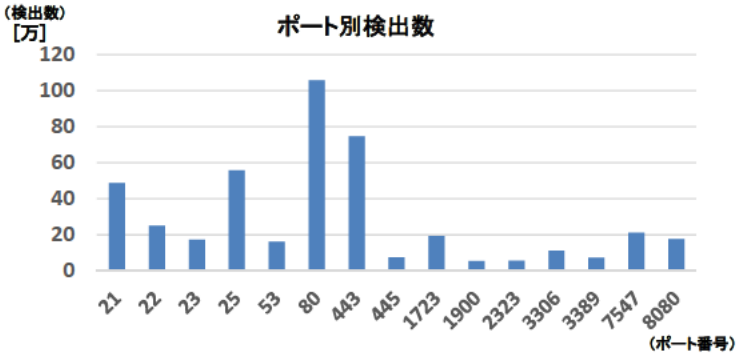
- オープンソースのツールをベースとして、設定、チューニング、機能追加し、独自のスキャンシステムを構築。
- 構築したスキャンシステムの機能については、「SHODAN」、「Censys」の情報と比較しても、遜色なく、十分な調査能力を有していることを確認。これにより、信憑性を確保した正確なスキャン結果の蓄積が可能となった。

家庭用ルータ、防犯カメラ等の一般利用者向けIoT機器の調査②

調査結果（概要）

【ネットワークスキャンに対する応答】

- 調査対象IPアドレスに対して、ネットワークスキャン（pingスキャン、ポートスキャン、バナースキャン）を行ったところ、その約6%で何らかの応答を確認。
- ポートスキャンの結果からは、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。



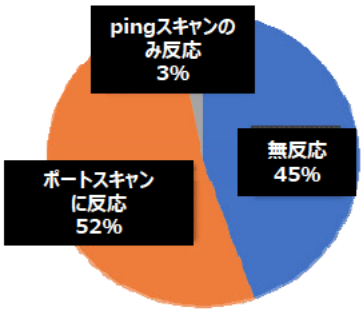
【バナー情報等をもとにした機種特定の実現性検証】

- バナー情報の分析等により、一部機種特定が可能であることを確認。また、機種は特定できない場合であっても、製造事業者名や機器類型（カメラ、ルータなど）などの機種特定につながる情報が多く得られることを確認。
- より精度を上げるために、別の手法との組み合わせを考慮するなど、分析手法の高度化が必要。

【NICTER観測データと連携した分析】

- 情報通信研究機構がNICTER※で捉えたマルウェア感染機器（TCP23又はTCP2323に対して感染拡大パケットを発信していた機器）に対してネットワークスキャンを実施。
- Mirai亜種が感染に用いたポート、Mirai亜種に対する脆弱性を持つ機器に固有のポート等から反応があった。全体の45%からは反応がなかった。

※ ダークネット（未使用IPアドレス）への通信をセンサーで観測し、サイバー攻撃の地理的情報や攻撃量、攻撃手法等を可視化するシステム



（想定される無反応の要因）
・マルウェア感染による要塞化。
・CGNAT等のサービス利用。
・調査対象外のポートを経由して感染。
・ポートスキャンがブロックされるサービス利用。

- NICTER観測データと連携することで、マルウェア感染機器のより詳細な分析が可能となるなど、分析結果の正確性向上に寄与することを確認。
- 技術開発等も含めて、分析能力の向上を図ることが重要。

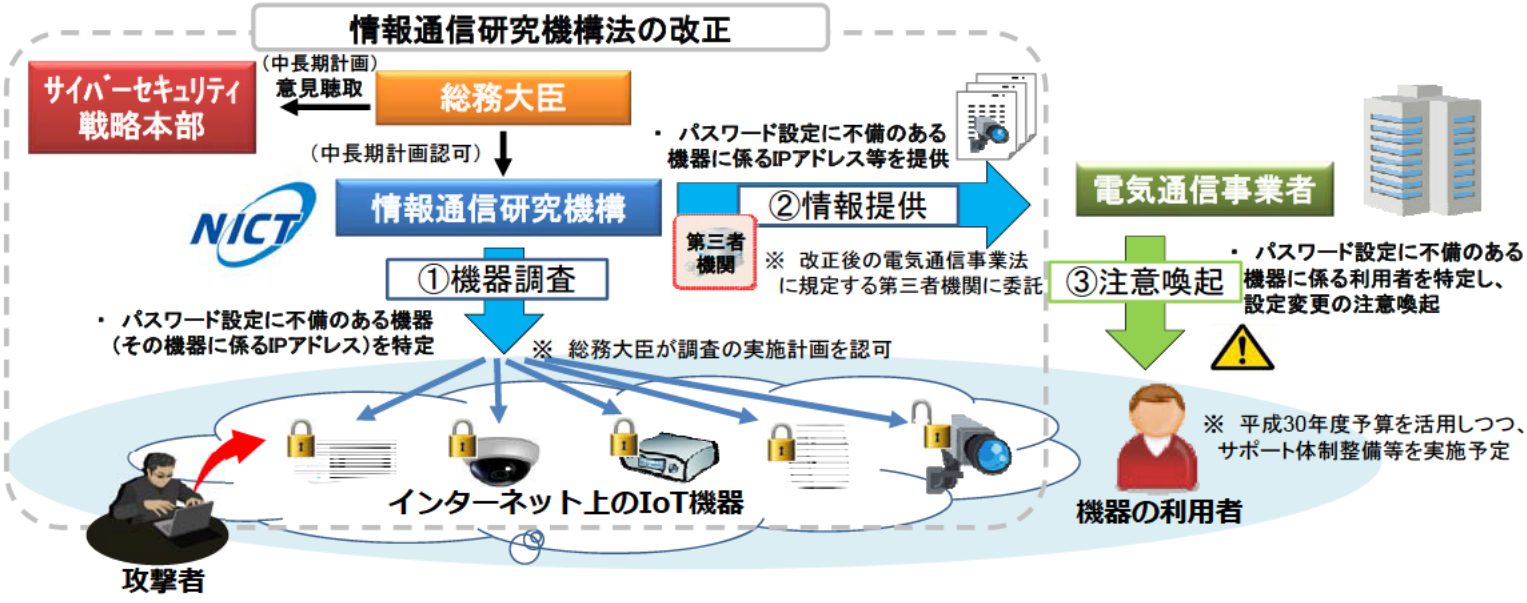
国立研究開発法人情報通信研究機構法の改正について 【資料11】

○ IoT機器などを悪用した**サイバー攻撃の深刻化**を踏まえ、国立研究開発法人情報通信研究機構（NICT）の業務に、**パスワード設定に不備のあるIoT機器の調査**等を追加（**5年間の時限措置**）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の改正**を行うもの。

サイバー脅威の深刻化
・IoT機器の急激な増加に伴い、IoT機器を踏み台とするサイバー攻撃の脅威が顕在化。
※IoT機器を狙った攻撃は全体の3分の2（2016年）

対策の必要性
・パスワード設定に不備のあるIoT機器の実態を把握するため、調査機能の強化が急務。

体制の整備
・NICTに機器調査に係る業務を追加し、電気通信事業者と連携しつつ対策を推進（下図）。



IoT機器に関する脆弱性調査

【資料12】

○ IoTサービスの普及に伴い、インターネットに接続されているIoT機器の種類・台数は年々増加している。昨年10月には、IoT機器を踏み台にした世界規模のサイバー攻撃が発生するなど、サイバー攻撃の脅威は今後も増大すると予測されており、セキュリティ対策の強化が急務。

○ 関係省庁、研究機関、業界団体等と連携しつつ下記の取組を実施し、IoT機器に関する脆弱性対策を推進。

IoT機器に関する脆弱性対策の概要

① 脆弱なIoT機器の実態調査、所有者等への注意喚起

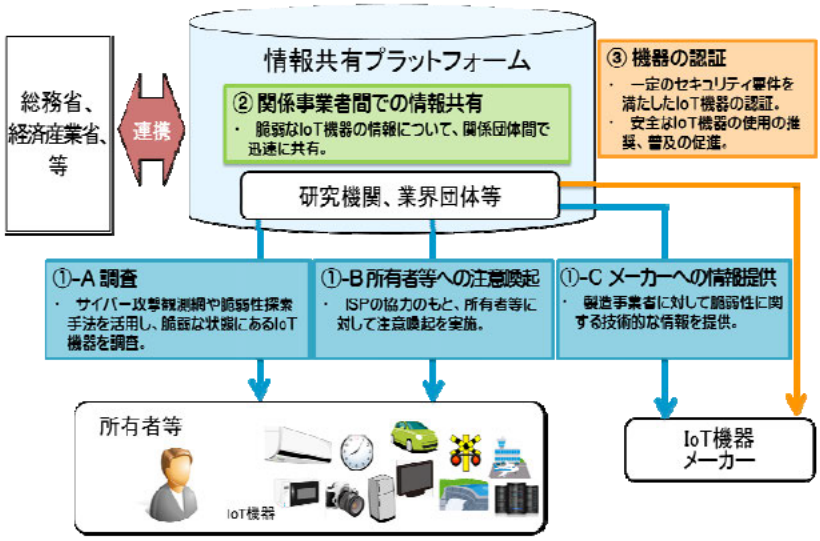
広域ネットワーク探索手法、サイバー攻撃観測網等を活用し、インターネットに接続されているIoT機器の調査を実施。脆弱性を持つIoT機器が発見された場合は、インターネットサービスプロバイダ(ISP)等の協力のもと、当該機器の所有者・運用者・利用者へ注意喚起を行う。

② IoT機器の脆弱性情報の関係事業者間での共有

①の取組等により収集した脆弱なIoT機器の情報について、関係事業者間で共有する仕組みを構築し、IoT機器の製造事業者等が脆弱性に迅速に対応することを可能とする。

③ 一定のセキュリティを確保したIoT機器の認証

一定のセキュリティ要件を満たしたIoT機器を認証し、安全なIoT機器の使用の推奨、普及を促進する。



期間 平成30年度～平成34年度

平成30年度予算 6億円（5年間の総額では18億円を想定）

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」（平成30年2月）の概要等

【資料13】

1. 電気通信事業者による攻撃通信の発生の防止

・マルウェア感染の疑われる利用者に対する注意喚起、指令サーバとの通信遮断、未知のマルウェア感染端末等を検知。

※ 事業者が、利用者の同意なく、注意喚起、検知等のために利用者の通信に係るIPアドレスやタイムスタンプ等を利用することは、通信の秘密の窃用に該当し得る。

→ 通信の秘密に配慮した実施方法等を整理し、民間のガイドラインに反映。

2. 情報共有、分析基盤の構築

・1. の対策の実効性を高めるため、第三者機関が指令サーバ等に関する情報を集約し、分析・検証した上で電気通信事業者との間で情報共有。

※ 本取組においては、第三者機関が、通信の秘密を集約、分析 検証、共有することとなる。

→ 第三者機関が通信の秘密に該当する情報を扱うことから、裏付けとなる法制度を整備。

3. IoT機器を含む脆弱な端末設備への対策の検討

・DDoS攻撃等の発生源となりうる脆弱なIoT機器について、基本的なセキュリティ対策を実施。

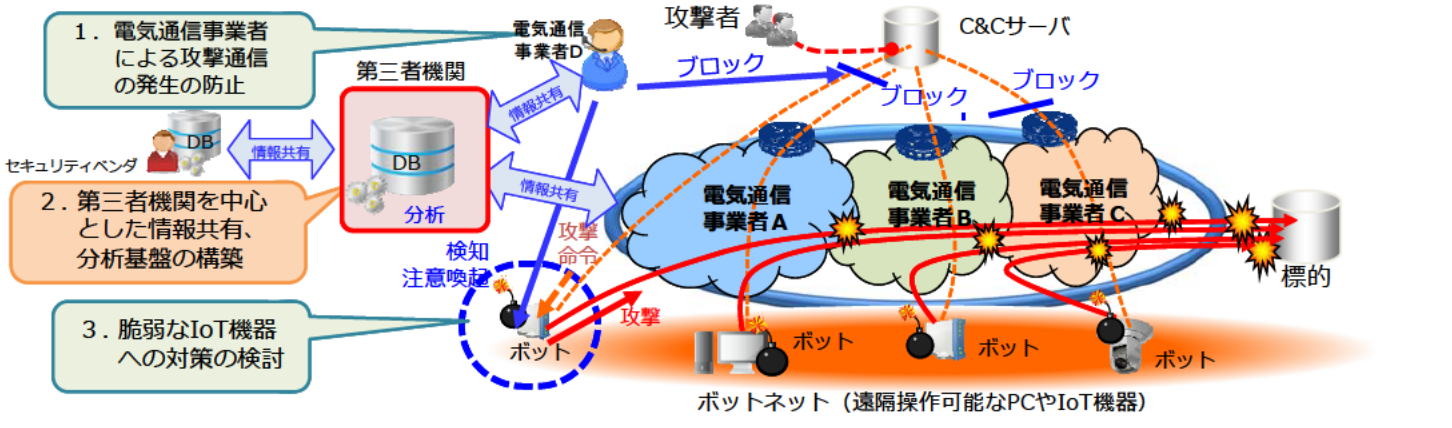
※ 事業者のネットワークに接続される端末設備の技術基準には、現時点ではサイバー攻撃等によるインターネットの障害に関する規定はない。

→ ネットワークの安全・信頼性を確保するための端末のセキュリティ対策について、国際動向等を踏まえ、情報通信審議会で検討。

4. 昨年8月に発生した大規模なインターネット障害の検証を踏まえた対策の検討

・事業者においてインターネットの経路情報を適切に制御する技術的対策を実施するともに、事業者間でインターネット障害に関する情報を共有。

→ 情報通信ネットワーク安全・信頼性基準（ガイドライン）の改訂や、事業者から総務省へのインターネット障害の報告の在り方について検討。



電気通信事業法の一部改正について

【資料14】

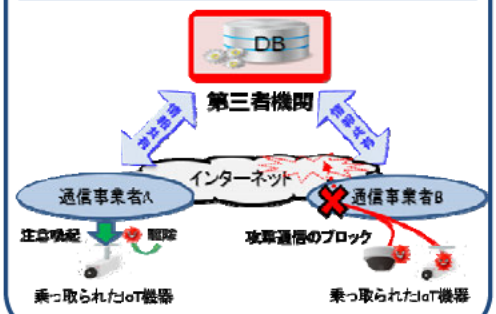
○　IoT化に伴うサイバー攻撃の深刻化やネットワークのIP網への移行に対応するため、電気通信事業法の改正を行うもの。

①深刻化するサイバー攻撃への通信事業者の対処の促進

- IoT機器を悪用したサイバー攻撃によるインターネット障害の深刻化

- サイバー攻撃の送信元となるマルウェア感染機器などの情報を共有するための制度を整備し、通信事業者による利用者への注意喚起・攻撃通信のブロック等を促進

第三者機関を通じた情報共有による対処



②電気通信番号に関する制度整備

- モバイル化・IoT化に伴う番号ニーズの増大による番号の逼迫やIP網移行に対応した全ての事業者による番号管理の必要性

- 番号の公平・効率的な使用と電話サービスの円滑な提供のため、使用条件を付して事業者に番号を割り当てるための制度を整備

番号の逼迫状況や効率的な使用

■ 番号の逼迫状況

番号	用途	指定率（指定数/全番号）	使用率（使用数/指定数）
070/080/090	携帯電話・PHS	90.4%	70.3%
0120	着信課金	99.2%	55.3%

※　その他、固定電話（0AB~J番号）の市外局番は、全国（582地域）のうち138地域で指定率が80%以上（平均使用率が18.6%）

■ 番号ポータビリティ（電話番号の持ち運び）

固定電話は現在、NTT東西から他事業者への片方向のみ。今後、携帯電話と同様、双方向番号ポータビリティを実現

③電気通信業務等の休廃止に係る利用者保護

- IP網移行や通信設備の更改等を背景として利用者への影響が大きい業務等の終了が予定

- 事業者が業務の休廃止に伴い行う利用者周知について、行政が予め確認するための制度を整備

例：廃止予定のINSサービスの用途

コンビニのPOS

銀行取引（EB）　企業間取引（EDI）

電気通信事業におけるサイバー攻撃への対処の促進について

○　サイバー攻撃を行うマルウェア※感染機器やそれらに指令を出すサーバへの対処を促進するため、第三者機関を中心として通信事業者が必要な情報共有をするための制度を整備。

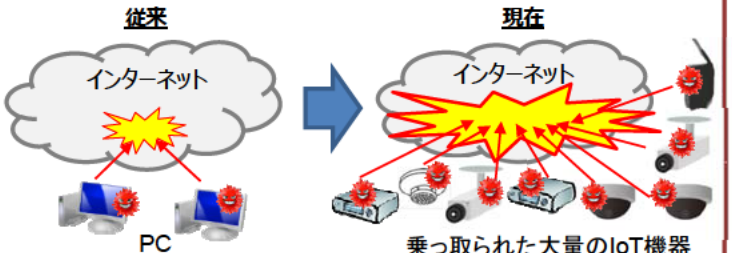
※悪意あるソフトウェアの総称であり、コンピュータに感染することによって、サイバー攻撃などの遠隔操作を自動的に実行するプログラムのこと。

現　状

インターネットの障害の深刻化

- サイバー攻撃によるインターネットの障害が発生し、国民生活や社会経済活動に影響
- 増加するIoT機器※を悪用したサイバー攻撃によりインターネットに重大な障害が発生
- 2020年の東京オリンピック・パラリンピック競技大会に際して、日本に対する大規模なサイバー攻撃の発生の懸念

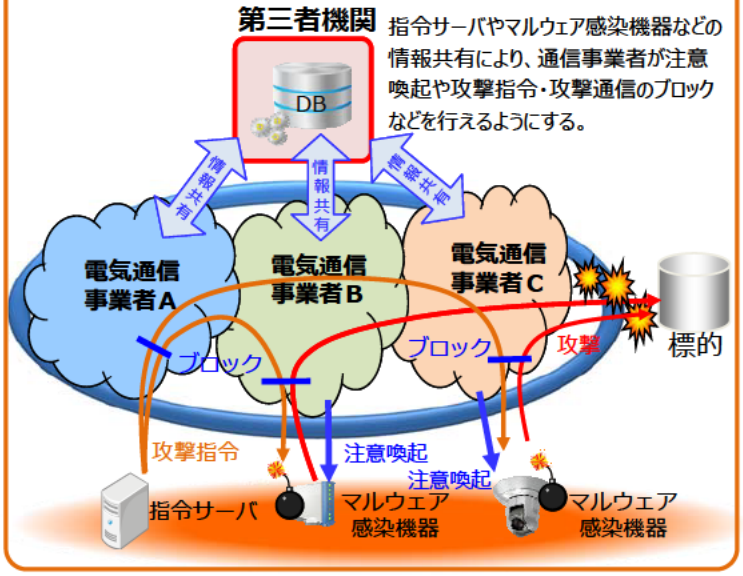
※インターネットに接続される家庭用機器や業務用センサーなどの機器



制度整備（イメージ）

第三者機関を中心とした情報共有基盤の構築

第三者機関　指令サーバやマルウェア感染機器などの情報共有により、通信事業者が注意喚起や攻撃指令・攻撃通信のブロックなどを行えるようにする。



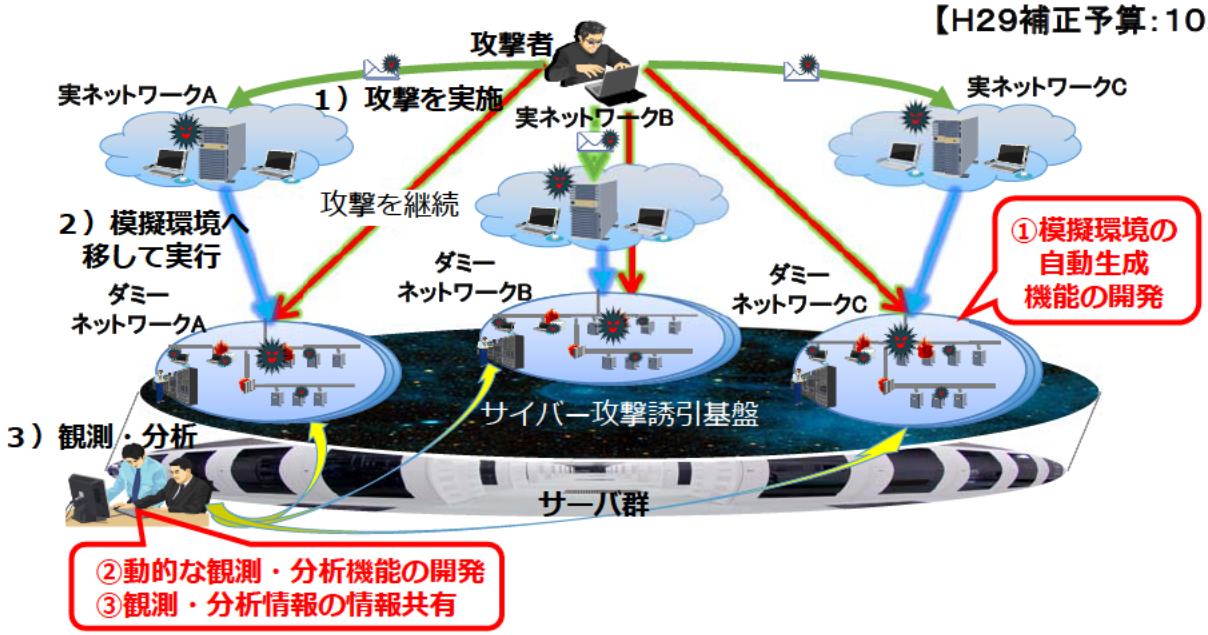
サイバー攻撃誘引基盤の構築（STARDUST）

【資料15】

○　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。

【H29補正予算：10.0億円】



広域ネットワークスキャンの軽量化

【資料16】

○　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

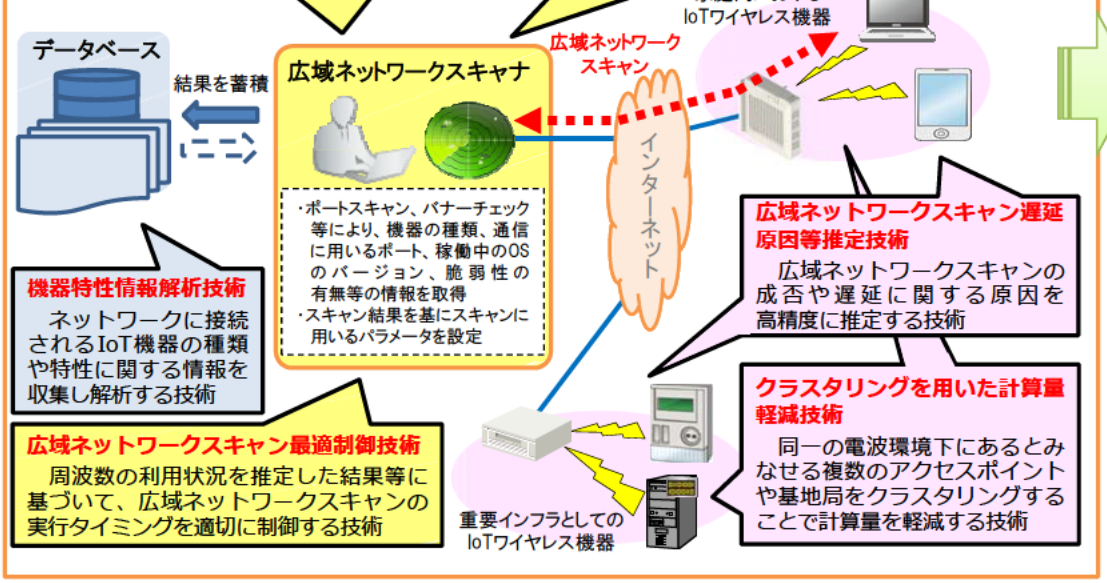
広域ネットワークスキャン対象ポート選定技術
広域ネットワークスキャンを実施するポートを選定する技術

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

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

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

AIを利用してIoT部品のハードウェアのセキュリティの確保を目指した研究 【資料17】

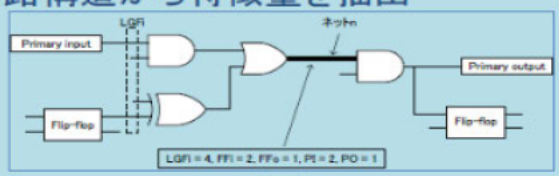
戦略的情報通信研究開発推進事業（SCOPE）：総務省公募研究事業
【平成29年度採択案件：早稲田大学基幹理工学部　戸川望教授】

IoT機器に悪意ある回路（ハードウェアトロイ）が組み込まれると・・・

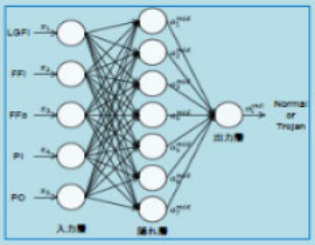
2013年10月（BBC）
ロシアの公営放送局（Rossiya 24）によると、サイバー犯罪者が、アイロンや湯沸かし器の中に、スパムアタックを行うチップを埋め込んでいることが判明。このチップは、勝手にWi-Fiネットワークに繋がってウイルスをばらまく電子回路が組み込まれていた。

http://www.bbc.com/news/blogs-news-from-elsewhere-24707337

回路構造から特徴量を抽出



AIによる学習と判断でハードウェアトロイの検知



→未知のハードウェアトロイを誤りなく検知することが目標！

SCOPE課題「設計工程に侵入したハードウェアトロイの検出と耐ハードウェアトロイ設計技術の研究開発」(H26～H28，代表：戸川望)の成果を活用して発展的に研究

衛星通信における量子暗号技術の研究開発の概要 【資料18】

事業の背景と課題

○衛星通信ネットワークを盗聴、改竄、乗っ取り等のサイバー攻撃から防御することにより、安心安全なインフラとしての発展を促進。

○今後、普及・発展が見込まれる、コンステレーション衛星網を構成する超小型衛星にも搭載可能な衛星ネットワークセキュリティ技術を実現。

○衛星通信回線への攻撃は実際に確認されている状況であり、衛星のマルチコンステレーション化が進むことで、一つのセキュリティホールへの攻撃から、多数の衛星や地上網に影響が広がる可能性。

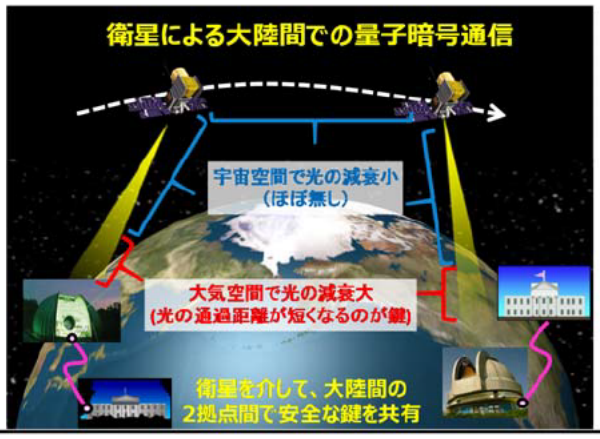
○将来的に量子コンピュータのような計算機技術の発展によって、従来の暗号技術を搭載した衛星通信も危殆化するおそれ。

○従来の光ファイバーによる量子暗号通信技術では、光ファイバー内における光の減衰の影響から遠距離（例えば大陸間など）での量子暗号通信は不可能な状況。

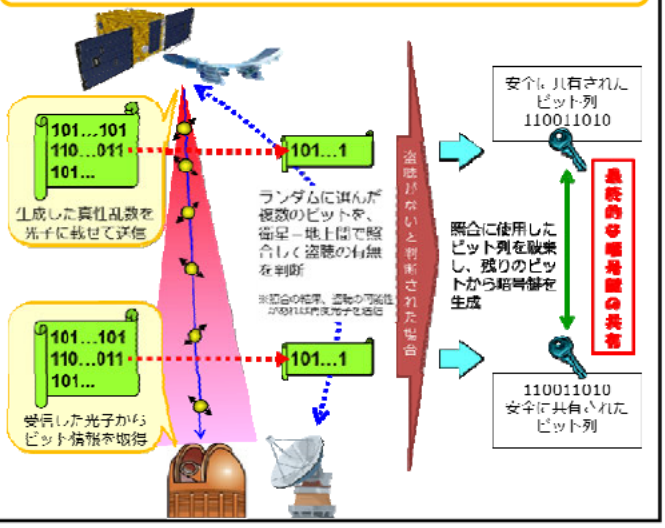
事業イメージ

◆ 人工衛星に適した情報セキュリティ技術を開発することにより、人工衛星を標的にしたサイバー攻撃を大幅に低減。

◆ 人工衛星を介した量子暗号通信ネットワークを実現することにより、量子暗号通信網の広域化を実現。



①超小型衛星にも搭載可能な宇宙仕様の暗号技術
②暗号鍵を光衛星通信回線上で配送する量子暗号鍵配送技術



AIを活用したサイバー攻撃検知・解析技術の研究開発

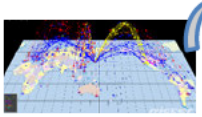
【資料19】

○　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技術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。

データセットの構築（例）

■ダークネット関連データ

未使用IPアドレスへの攻撃関連通信データ等

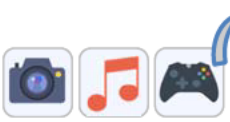


■マルウェア関連データ

マルウェア検体等、静的・動的解析結果等

■Android APK関連データ

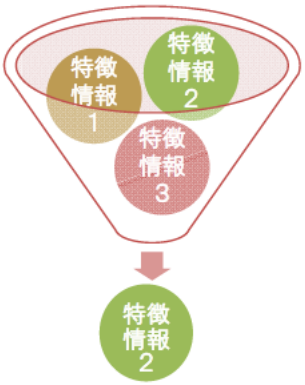
アプリのカテゴリ情報や説明文等



機械学習の活用（例）

■特徴選択

多様な特徴情報から最も影響力の強い特徴情報を特定



■SVM（サポートベクタマシン）

特徴情報に基づき、機械学習（SVM等）を用いて、データを分類

研究開発成果

攻撃パターンの分析やマルウェアの動作・影響分析等を自動化

（事例１）DDoS攻撃の発生検知

ダークネットトラフィックにおける特徴情報を効果的に特定することで、DDoS攻撃の発生を早期に検知

（事例２）パッカーの特定

マルウェアがどのようなパッカー（難読化ツール（※））を利用しているかを特定

（事例３）Androidアプリ分析

オンラインマーケットで配布されているアプリがマルウェアであるかどうかを判定

（※）難読化ツールとは、実行形式ファイルの機能を損なうことなく、そのソースコードの解析を困難にするツール。

コネクテッド・インダストリーズ税制の創設

【資料20】

○　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・ロボット等の導入に対して、特別償却30%又は税額控除3%（賃上げを伴う場合は5%）を措置。

○ 事業者は当該取組内容に関する事業計画を作成し、主務大臣が認定。認定計画に含まれる設備に対して、税制措置を適用（適用期限は、平成32年度末まで）。

※　経済産業省との共管

【計画認定の要件】

①データ連携・利活用の内容

・社外データやこれまで取得したことのないデータを社内データと連携

・企業の競争力における重要データをグループ企業間や事業所間で連携

②セキュリティ面

必要なセキュリティ対策が講じられていることをセキュリティの専門家(登録セキスペ等)が担保

③生産性向上目標

投資年度から一定期間において、以下のいずれも達成見込みがあること

・労働生産性：年平均伸率２%以上

・投資利益率：年平均15%以上

課税の特例の内容

➢ 認定された事業計画に基づいて行う設備投資について、以下の措置を講じる。

対象設備	特別償却	税額控除
ソフトウェア 器具備品 機械装置	30%	3% （法人税額の15%を限度）
		5％ ※ （法人税額の20%を限度）

【対象設備の例】

データ収集機器（センサー等）、データ分析により自動化するロボット・工作機械、データ連携・分析に必要なシステム（サーバ、ＡＩ、ソフトウェア等）、サイバーセキュリティ対策製品　　等

最低投資合計額：5,000万円

※ 計画の認定に加え、平均給与等支給額の対前年度増加率≧３％を満たした場合。

情報開示分科会報告書　概要

【資料21】

○　民間企業における**セキュリティ対策の情報開示による「セキュリティ対策の見える化」を通じて**、民間企業の経営層が自社のセキュリティ対策の現状を認識し、また、他社の状況と比較することにより、さらに必要な具体的な　対策を検討し、導入する**「セキュリティ対策の好循環」が起こる環境の実現**が期待される。

○　情報を開示するにあたっては、開示の対象者によってその考え方、取組が異なることから、報告書（案）においては、**①社内の情報共有（第一者開示）**、**②契約者間等の情報開示（第二者開示）**、**③社会に対する情報開示（第三者開示）**の3つの側面に分けて整理している。

社内の情報共有（第一者開示）

・　経営層の理解を深め、気づきを与えるとともに、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「橋渡し人材」等の育成に向けた取組を進める必要がある。

（社内の情報共有に向けた橋渡し人材等の育成）

1. **人材のスキルの具体化**、スキル取得のための**教育コンテンツの開発・普及**、**スキル認定を行う仕組みを産学官により構築するための検討**。

【平成30年度中を目途に方向性を整理】

契約者間等の情報開示（第二者開示）

…契約の相手方等、対象を限定して自社のセキュリティ対策を開示すること。

・　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また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。

・　サイバーセキュリティ保険について、対策の実施及び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・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。

（関係者間の情報共有促進のための仕組みづくりの検討）

2. **米国等におけるISAO(※)等の動向等について調査**するとともに、**公的支援のあり方について検討**。　【平成30年度中を目途に検討結果を取りまとめ】

(※)ISAO：Information Sharing and Analysis Organization

3. **セキュリティベンダー、損害保険会社、その他の関連する企業によるサイバーセキュリティ保険を含む総合サービスの開発に向けたモデル事業を推進**し、標準仕様化に向けて検討。また、**企業のセキュリティ対策の強度を簡易に診断できるツールキットを評価する仕組みづくりを検討**。

【モデル事業については平成30年度に検討】

社会に対する情報開示（第三者開示）

…社会の幅広い対象に向けて、自社のセキュリティ対策を開示すること。

・　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（※）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。

※　①基本方針等の策定状況　②管理体制　③教育・人材育成　④社外との情報共有体制　⑤第三者評価・認証

（第三者開示の促進に向けたガイドラインの策定）

4. **「セキュリティ対策情報開示ガイドライン」（仮称）を策定・公表**。

【平成30年秋を目途にガイドラインを策定】

5. 導入予定の「コネクティッド・インダストリー税制」の活用状況を分析するとともに、**企業のニーズ等を反映した投資促進のための政策支援のあり方について検討**。

【支援税制の運用にあわせて適宜実施】

情報共有基盤に関する実証事業の概要

【資料22】

＜目的＞

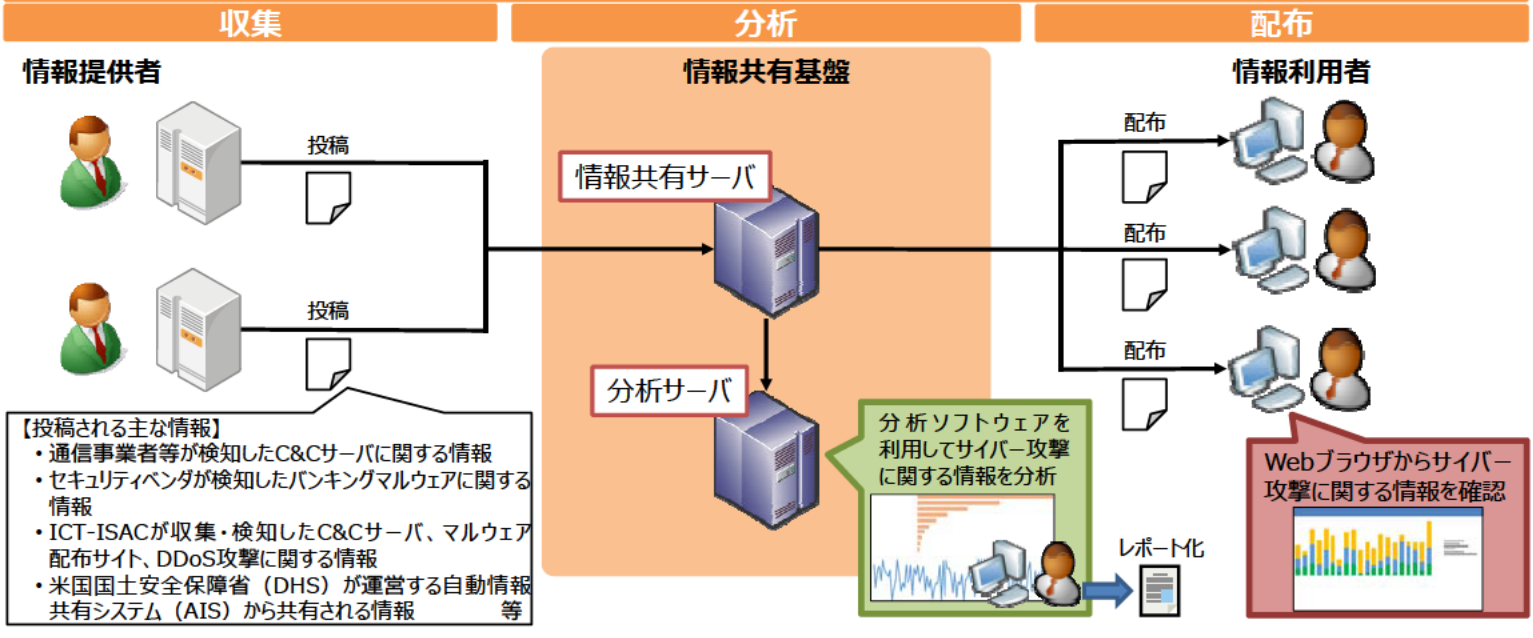
○　サイバー攻撃の被害状況、原因、対策等の情報をいち早く把握し、複数組織間で情報を共有する仕組みの構築。

※　機械処理を前提としてコンピュータが直接読み込むことが可能な形式（STIX/TAXII）で情報共有を行うことにより、手間をかけることなく、共有された情報をデータベース化・分析し、対策に活用することを可能とする。

＜実施内容＞

○　サイバー攻撃に関する情報の収集・分析・配布を行う情報共有基盤の運用における課題の抽出及び情報共有の有効性の検証。

○　事業者が情報共有基盤を利用する方法を示すガイドラインの策定。



利用ガイドラインの策定

【資料23】

○ ICT-ISACにおいて、情報共有基盤の利用方法を記載した「脅威情報の情報共有基盤　利用ガイドライン」を策定。
○ 利用ガイドラインには、利用方法のほか、情報共有基盤の利用に当たり事前に対応すべき事項や情報共有基盤の運営に係る取組が記載。
○ 利用ガイドラインは、今後、ICT-ISACにおいて、情報共有基盤の普及に活用していく予定。

【ガイドラインの全体構成】

Ⅰ：情報共有基盤の概要
情報共有の重要性や課題、情報共有基盤の仕組み等について解説

Ⅱ：情報共有基盤の活用
情報共有基盤の利用に当たり事前に対応すべき事項、情報共有基盤の利用方法について解説

Ⅲ：情報共有基盤の運営
情報共有基盤の利用者の不安を取り除き、利用を促進するための、情報共有基盤の運営に係る取組を紹介

付録
情報利用者及び情報提供者としての情報共有基盤の運用方針に記載すべき事項、情報共有基盤を運営する団体が作成する規則例を提示

『Ⅱ：情報共有基盤の活用』

○ **情報共有基盤の利用に当たり事前に対応すべき事項（情報利用者、情報提供者）**
- 情報共有基盤を利用する目的や、情報共有基盤の利用により達成したい目標の設定
- 情報共有に当たり利用可能なセキュリティ機器の確認
- サイバー攻撃に関する情報を収集する範囲や、当該情報を適用するセキュリティ機器の範囲の設定
- 情報利用者及び情報提供者としての情報共有基盤の運用方針の策定

○ **情報共有基盤の利用方法（情報利用者）**
- 情報共有基盤の利用方法について、以下の６つの手順に沿って解説
- 幅広い対象の情報利用者を想定し、取得したサイバー攻撃に関する情報を手動処理及び機械処理する場合の利用方法を記載

1. サイバー攻撃に関する情報を取得
2. サイバー攻撃に関する情報の信頼度を確認
3. サイバー攻撃の脅威種別、IPアドレス等の情報（インディケーター）を抽出し、サイバー攻撃に関する情報の重要度を確認
4. インディケーターを基に、実施するセキュリティ対策を適用するシステムの範囲を決定
5. ４で対象となったシステムに用いられるセキュリティ機器にインディケーターを提供
6. セキュリティ対策を十分に講じた上で、サイバー攻撃に関する情報を保管

○ **情報共有基盤への情報提供（情報提供者）**
- 自組織内で発見したサイバー攻撃に関する情報を情報共有基盤に提供する方法について、以下の３つの手順に沿って解説

1. 自組織内のサーバ等から、サイバー攻撃に関する情報を取得
2. １で取得した情報のうち、自組織のシステムのIPアドレス、メールアドレス等の機微情報を除外
3. サイバー攻撃に関する情報をSTIX形式に加工して投稿

公衆無線LANセキュリティ分科会報告書　概要

【資料24】

○　利便性と安全性のバランスに配慮しつつ、必要なセキュリティ対策について基本的考え方を示すとともに、セキュリティに配慮した公衆無線LAN環境の普及策として、①利用者・提供者の意識向上、②データ利活用施策との連携、③優良事例の普及を図ること等を報告書として取りまとめ。

今後の取組　（セキュアな公衆無線LAN環境の実現に向けた行動計画）

1. 利用者・提供者の意識向上

（国における取組）

① Wi-Fi利用者・提供者向けマニュアル（手引き）の改定（2018年夏頃を目途）
② オンライン教育等の教育コンテンツを活用した周知・啓発（2018年秋頃を目途に開始）
③ e-ネットキャラバン等の活動を通じた青少年・高齢者向けの周知・啓発（2018年度以降に実施）
④ 「公衆無線LAN版安全・安心マーク」に関する周知活動の実施（今後も継続的に実施）

（民間事業者における取組）

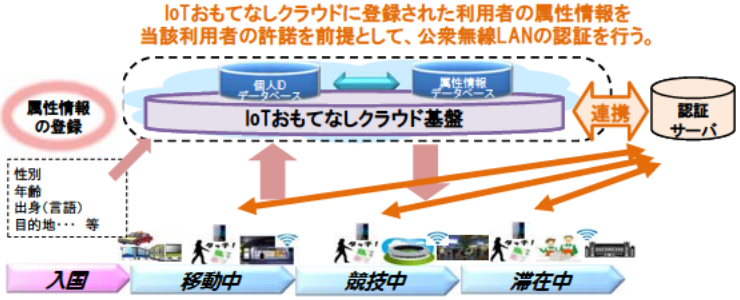
⑤ 暗号化の有無を識別可能な公衆無線LANサービスの提供（接続アプリの提供等）（民間事業者の取組に期待）

Secured Wi-Fi　公衆無線LAN版 安全・安心マーク

2. データ利活用施策との連携

（国・民間事業者における取組）

① 公衆無線LANサービスとIoTおもてなしクラウドとの連携推進（2019年中を目途に実用化）



3. 優良事例の普及

（国・民間事業者等における取組）

① 自治体に対する公衆無線LAN環境整備支援事業の継続的推進（2019年度まで継続）及び優良事例の普及促進（優良事例の調査・公表及びこれを踏まえた所要の政策支援については、2018年夏以降に実施）

② デジタルスタジアムの実現に向けたセキュアな公衆無線LAN環境の整備及び公衆無線LANサービスのSSID等の情報や接続アプリを、オリンピック・パラリンピック公式サイトといった信頼できるサイトにおいて提供する仕組みの構築（2018年度以降に実施）

セキュリティ人材の育成（ナショナルサイバートレーニングセンター）

【資料25】

○　巧妙化・複合化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材を育成するため、平成29年4月にNICTに組織した「ナショナルサイバートレーニングセンター」において、下記取組を実施。

① 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を対象とした実践的サイバー防御演習 （CYDER）

② 東京2020オリンピック・パラリンピック競技大会に向けた大会関連組織のセキュリティ担当者等を対象者とした実践的サイバー演習（サイバーコロッセオ）

③ 若手セキュリティイノベーターの育成 （SecHack365）

CYDER

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・教育コンテンツを開発

サイバーコロッセオ

SecHack365

平成30年度予算　15．1億円

実践的サイバー防御演習（CYDER）の概要

【資料26】

CYDER: CYber Defense Exercise with Recurrence

○　総務省は、情報通信研究機構（NICT）を通じて、**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**実践的なサイバー防御演習（CYDER）**を実施。

○　**受講者は**、組織の情報システム担当職員として、**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**。

○　平成29年度については、**全国で100回開催**され、**計3,009名が受講**。

演習のイメージ

CYDER演習風景

- 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。
- 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用意。

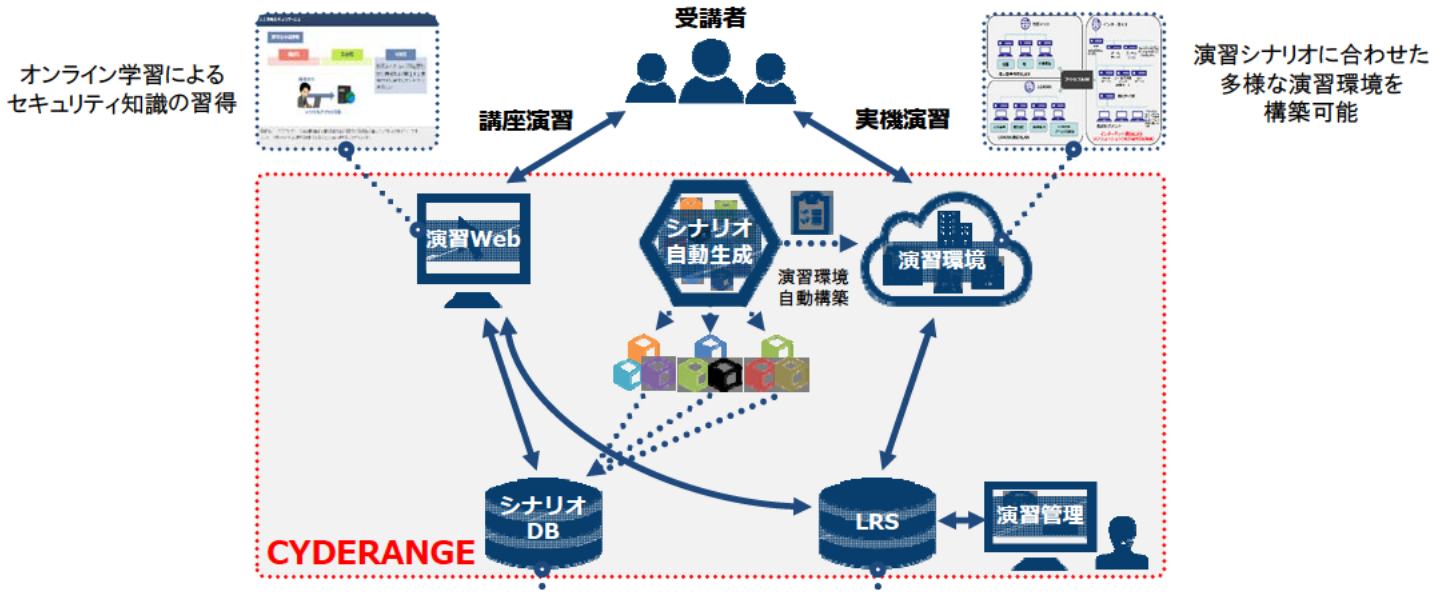
平成30年度の実施計画

コース	受講対象組織	開催地	開催回数
Aコース（初級）	（全組織共通）	47都道府県	60回
B-1コース（中級）	地方公共団体向け	全国11地域	20回
B-2コース（中級）	国の行政機関等向け	東京	10回
B-3コース（中級）	重要インフラ事業者向け	東京	10回

CYDERRANGEの概要

【資料27】

○　CYDERANGE（サイダーレンジ）は、サイバー演習の運営に係るコストの削減と、受講者のプロファイルに合わせた効果的な演習プログラムの提供を行うためのサイバー演習自動化システム（NICTが開発、2018年４月より実運用開始）。



◆ 各フェーズ（インシデント発見、初動対応等）の要素を組み合わせ、受講者のプロフィール（スキルレベル等）に応じた演習シナリオを自動生成

◆ シナリオ自動生成機能によって生成された環境構築情報に基づき、演習環境も自動で構築可能

◆ 教育・演習データ記録方式の世界規格であるExperience API（xAPI）を用いたLRS（Learning Record Store）を構築

◆ 演習時の受講者の行動（キー入力、マウス操作、ウィンドウ操作等）を収集し、行動分析が可能

◆ LRSを利用した統一的な演習受講管理を実現

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28】

○　近年さらに高度化・多様化するサイバー攻撃に備え、東京2020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**。

イメージ図

■　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。

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）

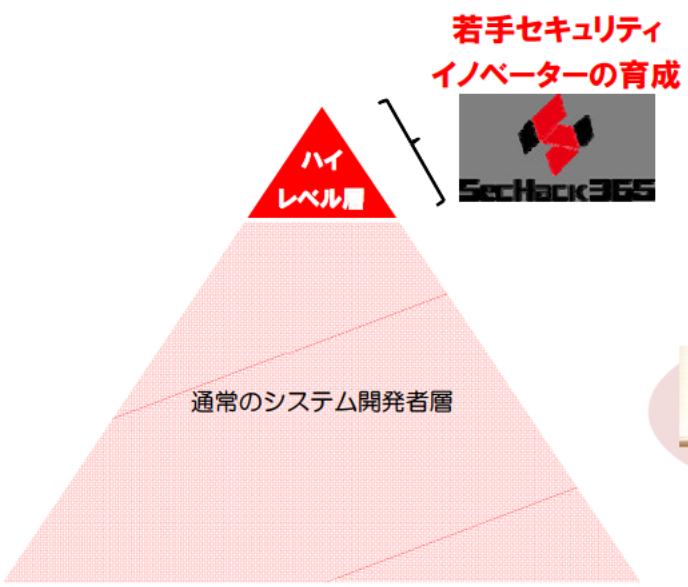
【資料29】

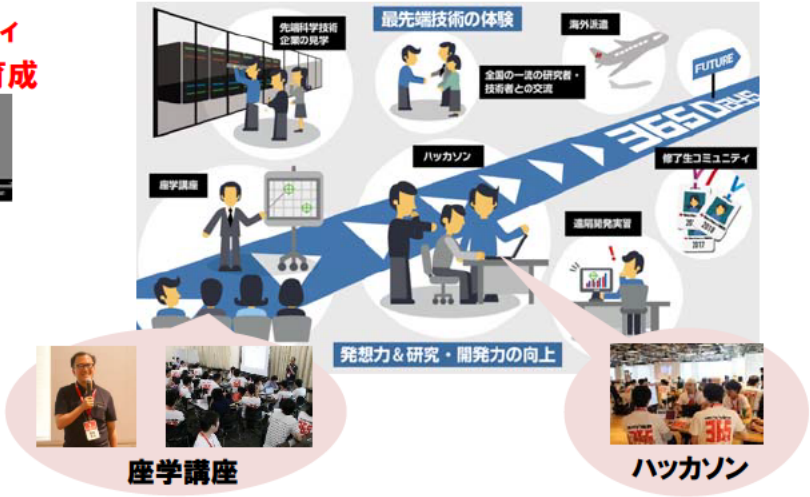
○ **未来のサイバーセキュリティ研究者・起業家の創出に向けて**、NICTの持つサイバーセキュリティの研究資産を活用し、**若年層のICT人材を対象に**実際のサイバー攻撃関連データに基づいた**セキュリティ技術の研究・開発を、第一線で活躍する研究者・技術者が1年かけて継続的かつ本格的に指導**。

○ 対象者は、日本国内に居住する**25歳以下の若手ICT人材**（平成29年度は39名が一年間のプログラムを修了。）

○ 受講者は、NICTの有する遠隔開発環境（NONSTOP（※））を活用し、**年中どこからでも遠隔開発実習を行うことが可能**。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。





■ 遠隔開発実習、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。

Cyber SEA Game 概要

【資料30】

ASEAN Youth Cybersecurity Technical Challenge (Cyber SEA Game)

- 実践的情報セキュリティ人材の発掘・育成をするため、ASEAN各国の若者向けにCTF形式の競技を実施
- 優勝チームを2018年2月に日本で行われるSECCON決勝大会に招待

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
- パケット解析、リバースエンジニアリング、フォレンジック、その他情報セキュリティに関連したあらゆる知識・技術が必要であり、チームメンバー同士の協力も重要

開催概要

- 日時　：2017年11月22日(水)
- 開催場所　：スイスホテル　ル　コンコルド　バンコク
- 参加者　：ASEAN10ヶ国の代表チーム（各国4名、計40名）
  （30歳以下の技術者、学生）

「日ASEANサイバーセキュリティ能力構築センター」プロジェクトの概要【資料31】

JAIF（日ASEAN統合基金）を活用して2017年から実施。
ASEAN域内のサイバーセキュリティ能力向上を支援する人材育成プロジェクトで、4年間で700人以上の参加をめざす。従来ハブと称していたが、2018年に”ASEAN-Japan Cybersecurity Capacity Building Centre”に改称。

○ 実施時期

STEP1（2017年2月-2017年12月） STEP2（2018年5月から4年間）

○ これまでの動向

- STEP1で実施されたF/Sの結果を踏まえ、2017年12月に開催された日ASEAN情報通信大臣会合において、STEP2としてタイETDA（電子取引開発機構）が、センターを運営することで合意
- STEP2の2018年7月からの演習開始に向け、タイ側と継続的に協議を実施

○ 主な活動内容

1. サイバー演習（インシデントレスポンス、デジタルフォレンジック、マルウェア解析）

政府機関・重要インフラ事業者等に対して、実践的なインシデントレスポンス演習（CYDER）、証拠の保全・解析等のためのデジタルフォレンジック演習、及びマルウェアの挙動解析演習を年6回程度実施

2. セキュリティコンテスト(Cyber SEA Games)

ASEAN各国から選抜された30歳以下の若手技術者・学生がサイバー攻撃対処能力を競う大会を毎年開催

3. その他

セキュリティワークショップを開催

第10回「日・ASEAN情報セキュリティ政策会議」の開催結果【資料32】

1. 開催概要

日時　：平成29年10月10日（火）及び11日（水）

場所　：グランド コプソーン ウォーター フロント ホテル（シンガポール）

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加盟国の経済・投資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. 内容

(1)重要インフラ防護、(2)サイバー攻撃による事態発生時の連絡体制、及び(3)サイバー分野における人材育成に関する前回会議からの一年間の取組みの確認・評価とともに、これまでの活動の包括的な振返りと評価を行い、これを踏まえ今後の協力について議論。

3. 成果

日・ASEANの政策担当者間の各レベルでの信頼醸成と協力関係の進展が確認されたとともに、これまで共同して実施してきた意識啓発活動や政府間の情報連絡演習等の継続に加え、日常的な情報共有の一層の促進に向けた連携・協力体制強化の検討や、重要インフラ防護に向けた先進的・先導的取組の共有等、日・ASEANの今後の取組みについて合意。

あわせて、政策会議の名称を「日・ASEANサイバーセキュリティ政策会議」に変更すること、並びに、10周年記念事業として、「日・ASEANサイバーセキュリティ政策ハンドブック（仮称）」を編纂することに合意。

第8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33】

1. ワークショップの概要

日時: 平成30年2月1日（木）、2日（金）の2日間

場所: 京王プラザホテル（東京）

主催: 総務省

目的: 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、日本及びASEAN各国のISP連携を維持・強化する。

参加者: 全体で48名
ASEAN10か国のISP事業者又は政府機関 （計21名）
総務省、ICT-ISAC （計27名）

2. 主な内容

○日本(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。

○前回に引き続き、サイバー攻撃対処演習を実施。国境を越えた協力が必要な脅威を想定したシナリオ（IoT機器を踏み台としたリフレクション攻撃）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。

○IoTセキュリティ対策をより高度化するために、セキュリティ対策に関する情報共有を引き続き実施することで合意。

○脅威情報の共有体制、方法について継続的な意見交換をメール等で実施していくことで合意。

第2回ISAC国際連携ワークショップの結果概要 【資料34】

- **2016年からISAC国際連携ワークショップを開催し、サイバーセキュリティに関する国際的な情報共有等について意見交換**
- **第2回ワークショップは、総務省主催で日米のISACが参加して2017年11月に東京で開催**
- **米国のIT-ISACが利用中の情報共有プラットフォームへのICT-ISACの試行接続などの協力強化で一致**

1. 経緯・目的

○サイバーセキュリティに関する情報収集・調査・分析を行うISAC(Information Sharing and Analysis Center)間の国際的な連携を強化するため、2016年からISAC国際連携ワークショップを開催

○サイバーセキュリティに関する両国の最新状況の共有、脅威情報の共有対象や共有方法に関する意見交換を実施

2. 開催日時、開催場所、参加者

○日時 :2017年11月6日, 7日

○場所 :京王プラザホテル（東京）

○参加者: 日本 ICT-ISAC, 総務省
米国 Comm-ISAC, IT-ISAC, Auto-ISAC

3. 結果

脅威情報やベストプラクティスの共有、サイバー演習の協力等について幅広く議論し、米国のIT-ISACが利用中のwebベースの情報共有プラットフォームにICT-ISACが試行的に接続するなど、更なる協力強化で一致した。

2018年のCyberstorm VI演習（DHS主催）へのICT-ISACの参加について検討することとした。また米国のNational Council of ISAC(NCI)とICT-ISACの協力の継続・深化についても合意した。

IoTセキュリティガイドラインの国際標準化

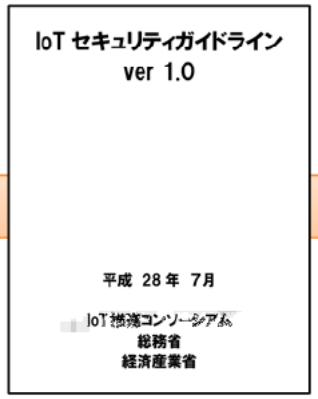
【資料35】

○我が国が主体となり、ITU-T及びISO/IECにおいて、IoTセキュリティガイドラインの国際標準化に向けた活動を推進中

これまでの取組

IoT Acceleration Consortium

総務省　経済産業省



ITU

ISO JTC1 IEC
INFORMATION TECHNOLOGY STANDARDS

○2016年7月、IoT推進コンソーシアム・総務省・経済産業省により、「IoTセキュリティガイドラインver1.0」を公表

○本ガイドラインをベースに国際標準化を目指し、ITU-T及びISO/IECに提案中

○2018年4月、ISO/IEC JTC1 SC27において、本ガイドラインをベースとしたIoTセキュリティ規格案(ISO/IEC 27030)が、新規標準化課題として承認

IoTセキュリティガイドライン　概要

【資料36】

- 平成28年1月より、「IoT推進コンソーシアム」において、IoT機器の設計・製造及びネットワークの接続等に関するセキュリティガイドラインを検討。
- 本ガイドラインは、IoTのセキュリティを確保するための「機器メーカ、サービス提供者などを対象にした5つの指針」及び「一般利用者を対象にしたルール」を分野横断的に定めたものであり、「IoT推進コンソーシアム、総務省及び経産省」の3者連名で、平成28年7月5日に公表。

	指針	主な要点
方針	IoTの性質を考慮した基本方針を定める	・経営者がIoTセキュリティにコミットする ・内部不正やミスに備える
分析	IoTのリスクを認識する	・守るべきものを特定する ・つながることによるリスクを想定する
設計	守るべきものを守る設計を考える	・つながる相手に迷惑をかけない設計をする ・不特定の相手とつなげられても安全安心を確保できる設計をする ・安全安心を実現する設計の評価・検証を行う
構築・接続	ネットワーク上での対策を考える	・機能及び用途に応じて適切にネットワーク接続する ・初期設定に留意する ・認証機能を導入する
運用・保守	安全安心な状態を維持し、情報発信・共有を行う	・出荷・リリース後も安全安心な状態を維持する ・IoTシステム・サービスにおける関係者の役割を認識する ・脆弱な機器を把握し、適切に注意喚起を行う
一般利用者のためのルール		・問合せ窓口やサポートがない機器やサービスの購入・利用を控える ・初期設定に気をつける ・使用しなくなった機器については電源を切る

セキュリティ対策の困難なIoT機器をネットワークに接続する場合、インターネットへつながる手前でセキュアなゲートウェイを経由させる等、セキュリティを確保する手段を講じる。

G7 情報通信・産業大臣会合 結果概要

【資料37】

1. 会合概要

（1）日程・場所　２０１７年９月２５日（月）～２６日（火） トリノ（イタリア）

（2）参加者　議長・イタリア：カレンダ　経済振興大臣、
日本：奥野総務副大臣、平木経産大臣政務官、
米国：クラティオス　大統領副補佐官・副CTO、
カナダ：ベインズ　イノベーション・科学・経済発展大臣、
英国：ハンコック　デジタル担当大臣、
フランス：マジュビ　デジタル担当大臣、
ドイツ：マハニック　経済エネルギー省事務次官、
EU：アンシップ　欧州委員会副委員長

2. 結果概要

○ 社会経済のデジタル化による「次世代生産革命（Next Production Revolution）」の推進を主題として、①包摂性(Inclusiveness)、②開放性(Openness)、③セキュリティ(Security)の３つのテーマにつき討議。

○ **「G7情報通信・産業大臣宣言」及び3つの付属文書**「Annex1　次世代生産革命における**中小企業の競争力及び包摂性**のためのG7共通の政策アプローチ」、「Annex2　我々の社会のための**人間中心のAI**に関するG7マルチステークホルダーの交流」、「Annex3　ビジネスのための**サイバーセキュリティ**を強化するためのG7の行動」を採択。

- **オープンで自由なインターネットを支持し、次世代生産革命における投資と信頼性を促進し、グローバルなデジタル経済の成長を下支えするための１４の原則を確認。**
  - ・国境を越えた**情報の自由な流通の促進と保護**、　**・インターネット及び高速ブロードバンドサービスへのアクセスの重要性**、
  - **・データローカライゼーション要求への反対**、　**・ソースコードについてのアクセス又は移転を要求するような政策への反対**、
  - **・市場の開放性を維持し、保護主義と戦うことへのコミット**、
  - **・持続可能な開発目標（ＳＤＧｓ）への対処に貢献するための**、世界中における**より一層のＩＣＴの利用**への支持
- ＡＩの進歩が社会・経済にもたらす便益を認識し、デジタル経済におけるイノベーション及び成長を主導する**人間中心のＡＩというビジョンを共有**。
- **セキュリティ・バイ・デザインのアプローチの促進に基づく企業（特に中小企業）におけるサイバーセキュリティの重要性**、及び**知的財産権の効率的な保護及び執行を強調**。
- **2018年のカナダ議長国のＧ７において、引き続き対話及び協力が促進されることを期待**。

○ 我が国が昨年、21年ぶりに高松において開催したG7情報通信大臣会合の流れを維持。
同会合において**我が国が提唱したAIに関する国際的な議論の重要性**、マルチステークホルダーアプローチの重要性を確認。