

IoT セキュリティ総合対策 プログレスレポート 2019

令和元年 5 月

サイバーセキュリティタスクフォース

目次

はじめに	1
I 具体的施策	3
(1) 脆弱性対策に係る体制の整備	3
① セキュリティ・バイ・デザイン等の意識啓発・支援の実施	3
② 認証マークの付与及び比較サイト等を通じた推奨	5
③ IoT セキュアゲートウェイ	6
④ セキュリティ検査の仕組み作り	8
⑤ 簡易な脆弱性チェックソフトの開発等	9
⑥ 利用者に対する意識啓発の実施や相談窓口等の設置	10
⑦ 重要 IoT 機器に係る脆弱性調査	11
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	13
⑨ 被害拡大を防止するための取組の推進	16
⑩ IoT 機器に関する脆弱性対策に関する実施体制の整備	18
(2) 研究開発の推進	19
① 基礎的・基盤的な研究開発等の推進	19
② 広域ネットワークスキャンの軽量化	21
③ ハードウェア脆弱性への対応	23
④ スマートシティのセキュリティ対策の強化	24
⑤ 衛星通信におけるセキュリティ技術の研究開発	26
⑥ AI を活用したサイバー攻撃検知・解析技術の研究開発	28
(3) 民間企業等におけるセキュリティ対策の促進	29
① 民間企業のセキュリティ投資等の促進	29
② セキュリティ対策に係る情報開示の促進	31
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	33
④ 情報共有時の匿名化処理に関する検討	35
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	36
(4) 人材育成の強化	37
① 実践的サイバー防御演習 (CYDER) の充実	37
② 2020 年東京大会に向けたサイバー演習の実施	38
③ 若手セキュリティ人材の育成の促進	39
④ IoT セキュリティ人材の育成	40

(5) 国際連携の推進.....	42
① ASEAN 各国との連携	42
② 国際的な ISAC 間連携.....	44
③ 国際標準化の推進	45
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.....	47
II 今後の進め方.....	49

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。【資料1】

センサーの小型軽量化、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（システムックリスク）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。

2018年（平成30年）7月には、政府全体の新たな「サイバーセキュリティ戦略」が策定されたところであるが、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。【資料2、3】

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機器メーカー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）。【資料4】

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。【資料5】

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た「IoT分野共通セキュリティ要件ガイドライン（2018年度版）」を策定・公開し、2019年（平成31年）4月には当該ガイドラインを踏まえた認証プログラムが一部の会員企業向けに試行的に開始されたところである。

【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、機器メーカー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。

また、一般社団法人重要生活機器連携セキュリティ協議会の実施する認証プログラムについては、その2019年（令和元年）10月以降に広く一般企業も対象とするための準備が行われている。

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。

【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 6】

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。【資料 7】

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った特性上、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】

「IoT サービス創出支援事業（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、組み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。2019 年（平成 31 年）2 月から、当該ガイドラインに基づいた民間の検査事業が実施されている。

【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、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ける上述のガイドラインに基づく検査事業の実施状況や、改正端末設備等規則（項目（1）①参照）の施行状況等を踏まえつつ、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。

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「IoT 分野共通セキュリティ要件ガイドライン（2018 年度版）」を踏まえたセキュリティ評価・検証ツールが公開され、当協議会の会員企業への提供が行われる等、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】

民間企業に対してセキュリティ対策の実施状況に係る情報開示を促す等の取組を通じて、脆弱性を調査する民間サービス等の普及促進を図る。

(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。

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必要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。【資料 8】

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 9】

- 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、2018 年 (平成 30 年) に観測されたサイバー攻撃関連通信は 3 年前と比べて 3.9 倍の増加となっている。また、2018 年 (平成 30 年) に NICTER で観測したサイバー攻撃関連通信の約半数が IoT 機器を狙った通信であることが確認された³。【資料 10】

³ 「NICTER 観測レポート 2018 の公開」 (2019 年 2 月 NICT)
<https://www.nict.go.jp/press/2019/02/06-1.html>

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。【資料 11】

- 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」、「Gensys」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。【資料 12】

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。

【資料13、14】

【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。【資料 15】

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。【資料 16】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。【資料 17】

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】

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、NOTICE（項目（1）⑧参照）等の取組において、パスワード設定等に不備等のある利用者への注意喚起の実施に当たっては、ISP のみならず、IoT 機器製造業者や流通業者等の協力を得ながら効果的な注意喚起を図るなど、各主体で連携しながら、引き続き IoT 機器のセキュリティの強化を図る。

(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。【資料 18】

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。【資料 19】

IoT システムを支える第 5 世代携帯電話システム（5 G）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、2020 年（令和 2）を目途に開始される 5 G については、IoT システムの基盤技術であるため、5 G 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、5 G を活用する重要インフラ事業者等への周知・啓発を図る。【資料 20】

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。【資料 21】

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。【資料 22】

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への対応については、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 を活用し、ハードウェアの動作特性の把握による不正機能検出等の研究開発に取り組む。

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」に関する公募を行い、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）から取り組んでいる。

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・プライバシー保護の検討を進めているところである。【資料23】

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】

「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、初年度に得られた日欧の技術的な成果を、今後の実証実験での活用や個々の技術要素間の連携により、さらに洗練、進化させ、実用化を目指した取り組みを行う。

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。【資料24】

【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・解析に必要な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。【資料 25】

【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。【資料26】

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）4 月 26 日現在の認定事業社数 58 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実施し、「サイバーセキュリティ対策に係る情報開示の手引き」の案について 2019 年（令和元年）5 月にパブリックコメントを実施しているところである。（項目（3）②を参照）

【今後の取組】

上記のネクテッド・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、「サイバーセキュリティ対策情報開示の手引き」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。【資料27】

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（第三者開示）」、「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（第三者開示）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実施し、「サイバーセキュリティ対策に係る情報開示の手引き」の案について2019年（令和元年）5月にパブリックコメントを実施しているところである。【資料28】

【今後の取組】

情報開示の促進については、「サイバーセキュリティ対策情報開示の手引き」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。【資料 29、30】

このほか、日米の ISAC 間の情報共有、連携を進めており、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。（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。【資料 31】

【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。【資料 32、33】

また、演習プログラムについては、2018 年度 (平成 30 年度) より、重要インフラ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、重要インフラ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。【資料34】

【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。【資料 35】

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 SXSWS（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、SXSWS 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 SXSWS（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。【資料 36】

【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（平成 31 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。【資料37】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。【資料38】

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。【資料 39】

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 10 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。【資料 40】

【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。【資料 41、42】

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。【資料 43】

- 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

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GRESS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GRESSレポートの結果も適切に反映させていく。

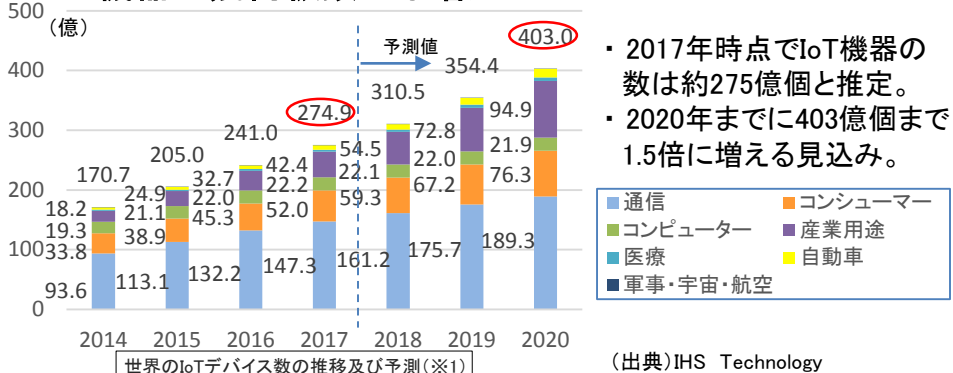
さらに、2018年（平成30年）7月に新たに策定された「サイバーセキュリティ戦略」も踏まえつつ、NISCや経済産業省をはじめ、関係府省庁との連携の下、IoTセキュリティ対策の強化を進めていく。

參考資料

現状

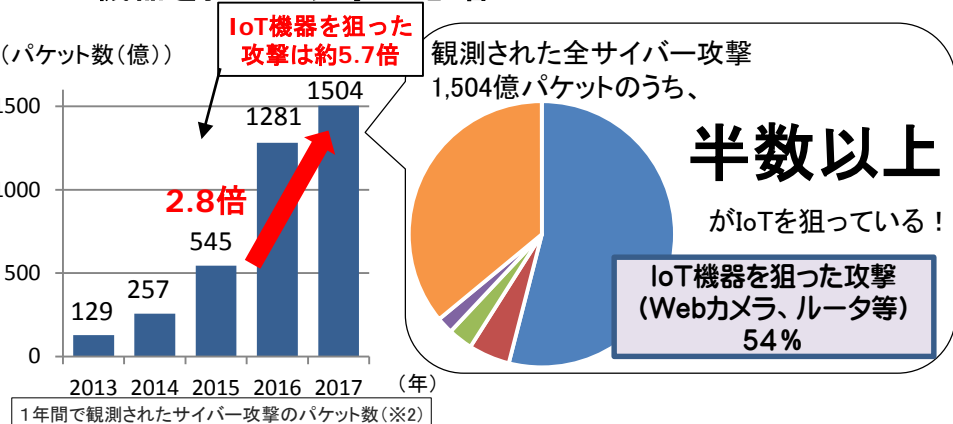
対策

○IoT機器の幾何級数的な増加

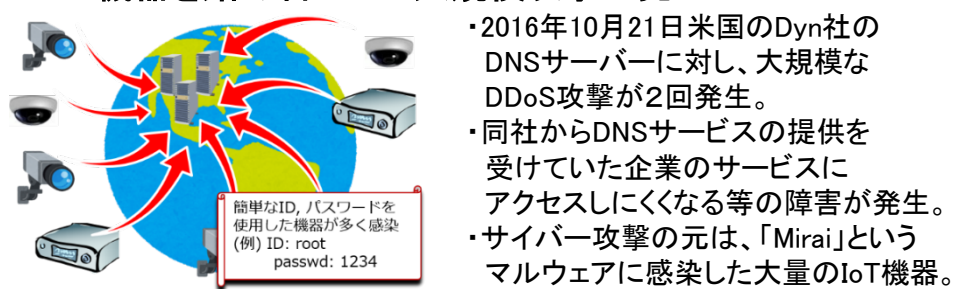


- ・ 2017年時点でIoT機器の数は約275億個と推定。
- ・ 2020年までに403億個まで1.5倍に増える見込み。

○IoT機器を狙った攻撃が急増



○IoT機器を踏み台にした大規模攻撃が発生



(※1)及び(※2)・・・総合対策公表時から数値を現行化。

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)

総合対策の進捗状況や今後の取組方針を整理し、「プログレスレポート」として公表

中長期的

1 策定の趣旨・背景

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）
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

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. 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

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）
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＞・**国家の強靱性の確保**
 - ①任務保証、②我が国の先端技術・防衛関連技術の防護、③サイバー空間を悪用したテロ組織の活動への対策
 - ・サイバー攻撃に対する**抑止力の向上**
 - ①実効的な抑止のための対応、②信頼醸成措置
 - ・サイバー空間の**状況把握の強化**
 - ①関係機関の能力向上、②脅威情報連携
 3. 国際協力・連携
 - ＜施策例＞・**知見の共有・政策調整**
 - ・事故対応等に係る国際連携の強化
 - ・能力構築支援
- 等

横断的施策

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

5 推進体制

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

戦略期間

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

- 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
- 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】
- 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

- 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
- 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
- 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
- 大学等における安全・安心な教育・研究環境の確保
- 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】
- 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
- 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

- 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
- 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】
- 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

- 今後製品化されるIoT機器がパスワード設定の不備等により悪用されないようにする対策として、IoT機器の技術基準※にセキュリティ対策を追加するための省令改正を行う。

※ 電気通信事業法では、電気通信事業者のネットワークに接続して使用する端末設備は、総務省令(端末設備等規則)で定める技術基準に適合しなければならないこととされている。

【端末設備等規則(省令)の改正概要】

- インターネットプロトコルを使用し、電気通信回線設備を介して接続することにより、電気通信の送受信に係る機能を操作することが可能な端末設備について、最低限のセキュリティ対策として、以下の機能を具備することを技術基準(端末設備等規則)に追加する。

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

② 初期設定のパスワードの変更を促す等の機能

③ ソフトウェアの更新機能※¹

又は ①～③と同等以上の機能※²

※¹ ①と③の機能は、端末が電源オフになった後、再び電源オンに戻った際に、出荷時の初期状態に戻らず電源オフになる直前の状態を維持できることが必要。

※² 同等以上の機能を持つものとしては、国際標準ISO/IEC15408に基づくセキュリティ認証(CC認証)を受けた複合機等が含まれる。

- PCやスマートフォン等、利用者が随時かつ容易に任意のソフトウェアを導入することが可能な機器については本セキュリティ対策の対象外とする。

【スケジュール】

- 2019年3月1日に改正省令を公布。2020年4月1日に改正省令を施行。
- 2019年4月22日に改正省令の運用方法や解釈等を定めるガイドラインを策定。

IoT推進コンソーシアム

○ 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。

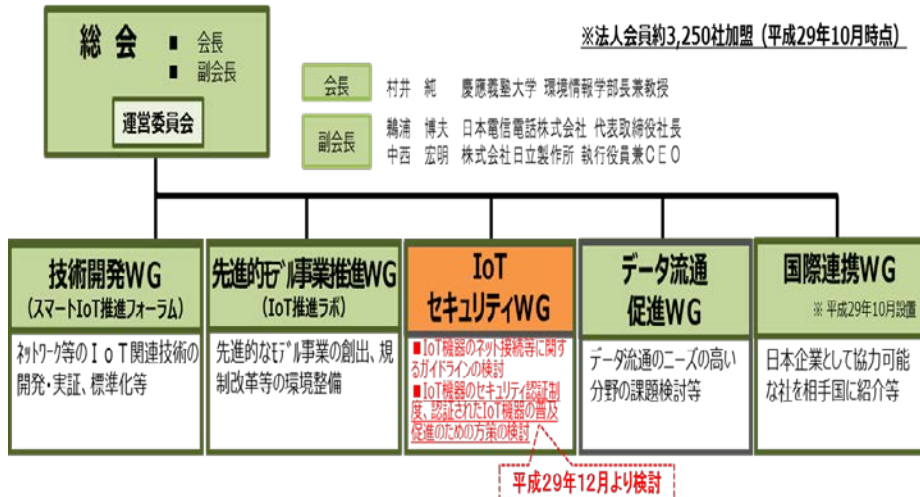
このことを受けて、IoT推進コンソーシアム IoTセキュリティワーキンググループにおいて、「IoTセキュリティガイドラインver1.0」の普及啓発やIoT機器のセキュリティ確保策等について検討を行う。

○ 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】

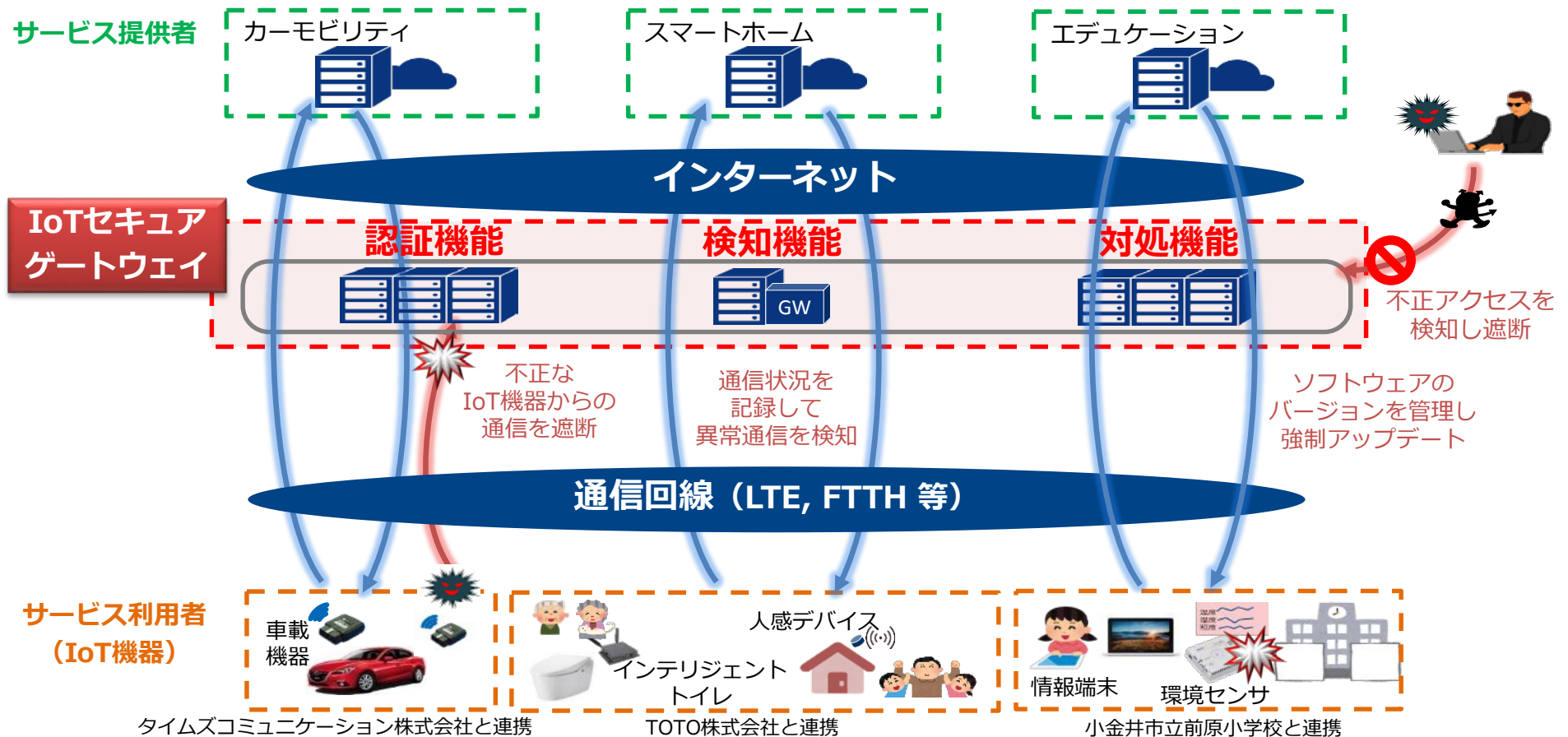
有村 浩一	一般社団法人JPCERTコーディネーションセンター 常務理事
出雲 秀一	在日米商工会議所 サイバーセキュリティタスクフォース共同委員長
鶴飼 裕司	株式会社FFRI 代表取締役社長
大矢 隆一郎	一般社団法人 ビジネス機械・情報システム産業協会 委員
小川 武史	青山学院大学工学部機械創造工学科 教授
荻野 司	一般社団法人 重要生活機器連携セキュリティ協議会 代表理事
金子 健一	一般社団法人日本電機工業会 家電部 技術課
川上 景一	一般社団法人電子情報技術産業協会 常務理事
小山 覚	一般社団法人 日本経済団体連合会 情報通信委員会 企画部会長代行・サイバーセキュリティに関する懇談会座長
(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)
塚原 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ー センター長
向殿 政男	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

- 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））



- **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

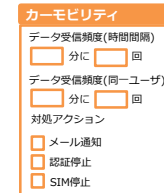
検知機能の向上

(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值を自動的に設定することが必要（※）。

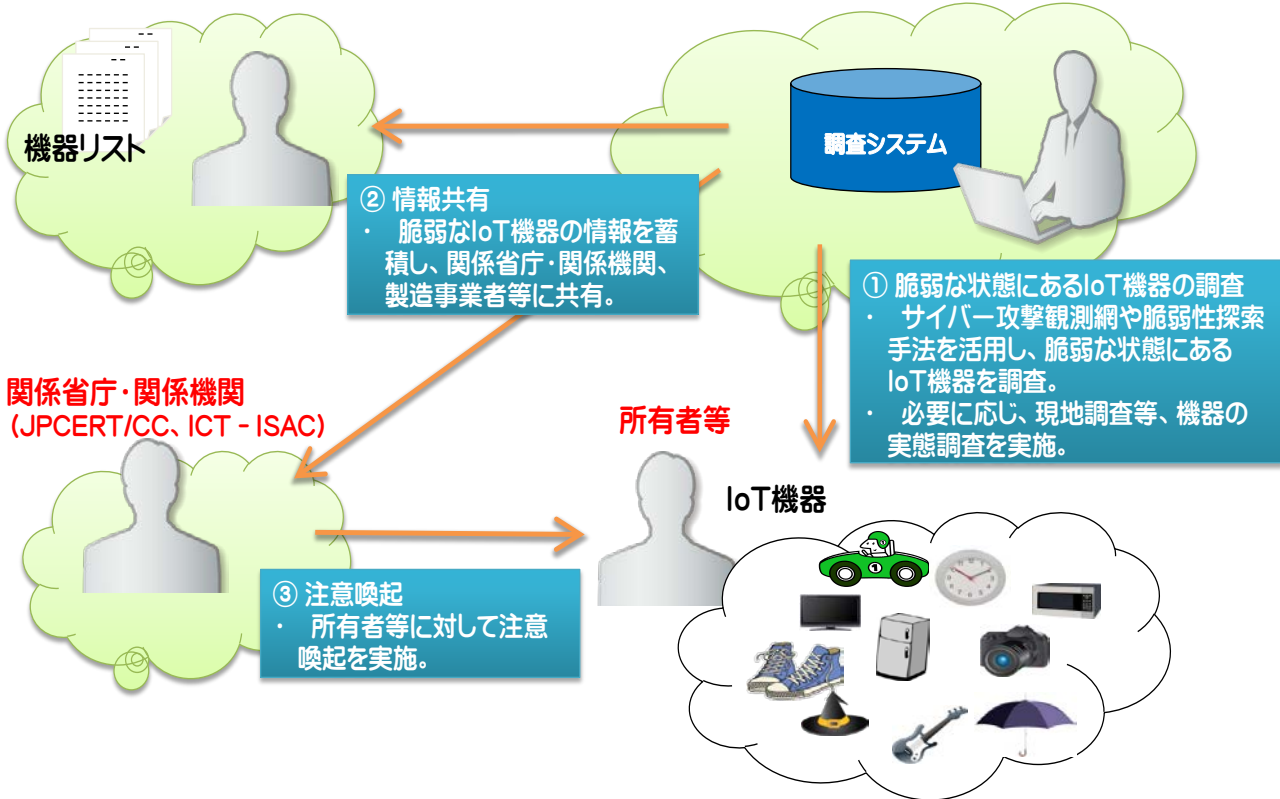
※ AIを用いたデータ分析の活用も考えられる。

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8】

- 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。

製造事業者等 (IoT機器メーカー・ベンダ)

総務省、ICT-ISAC、横浜国立大学



【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時代が到来し、それらに対す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28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: [別紙添付](#))

【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)

<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/tcp1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】

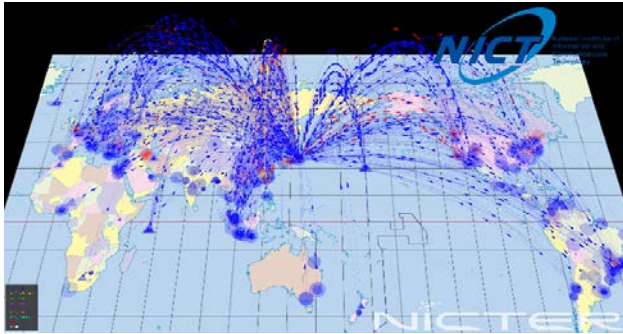
- 本件調査により検出した脆弱な重要IoT機器は150件、そのうちWebインタフェースに記載されている情報から利用者等に関する情報が得られたものが77件、そのうち実際に利用者等にコンタクトが取れて、注意喚起等を行ったものが36件であった。
- 検出した重要IoT機器(工場、工事現場等)は、消費電力監視装置、水位監視装置、防災設備制御装置、ガス観測警報通知装置等であった。
- 36件の内訳は、パスワード設定が適切になされていないものが27件、パスワード設定はなされているが認証画面がインターネット上で公開されていたものが9件であった。

【ヒアリング調査等の結果(ポイント)】

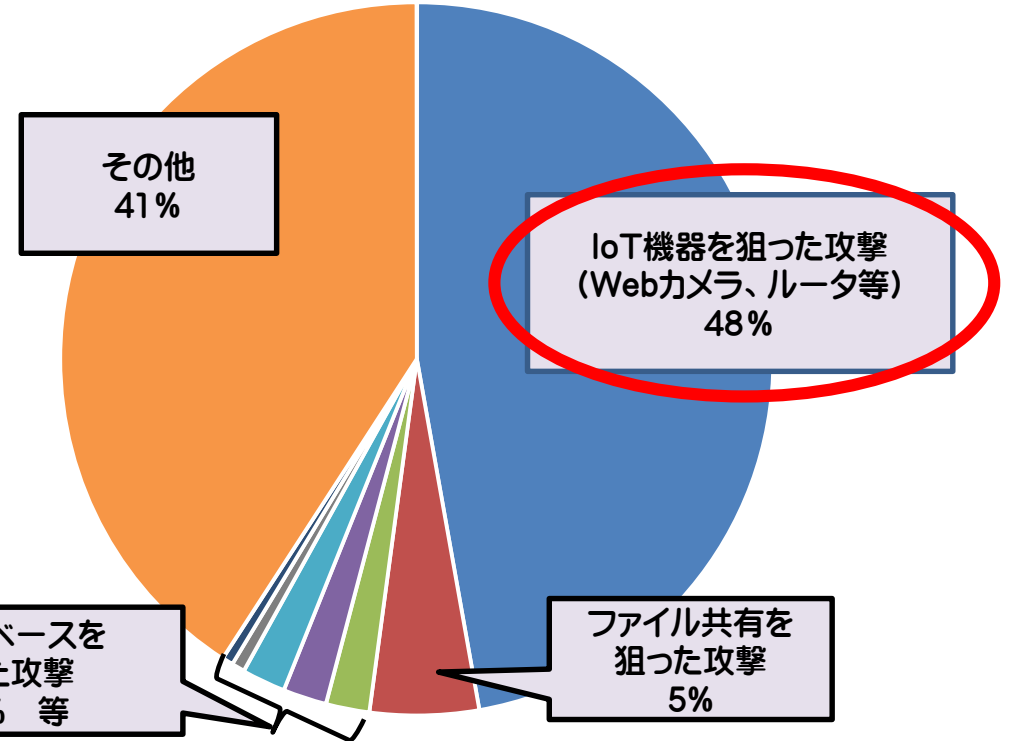
- 関係者(所有者、利用者、運用者、導入者、製造者)の脅威に対する認識が十分でない、または、認識の共有が十分にできていない。
- 多様な関係者間の責任の所在が明確になっていない。

○ 国立研究開発法人情報通信研究機構(NICT)では、大規模サイバー攻撃観測網であるNICTERにおいて、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。

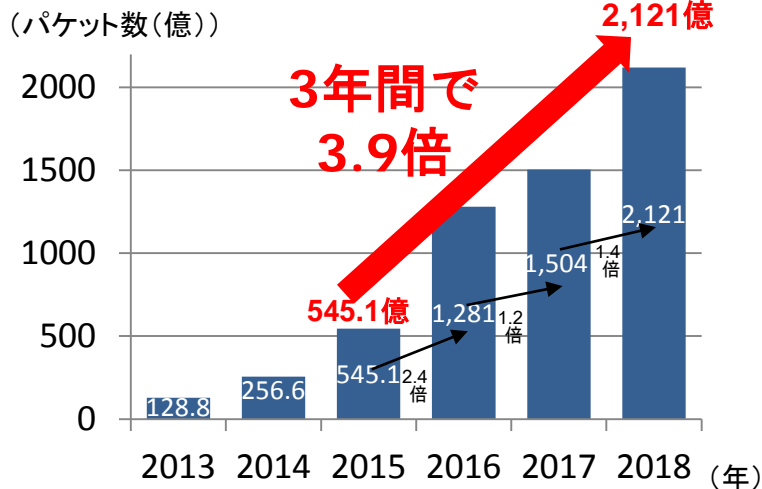
NICTERにより観測されるサイバー攻撃の様子



約半数がIoT機器を狙った攻撃



NICTERで1年間に観測されたサイバー攻撃回数



(注1) NICTERで観測されたパケットのうち、サービスの種類(ポート番号)ごとに割合の多い上位から30位までを分析したもの。
(注2) IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。

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11】

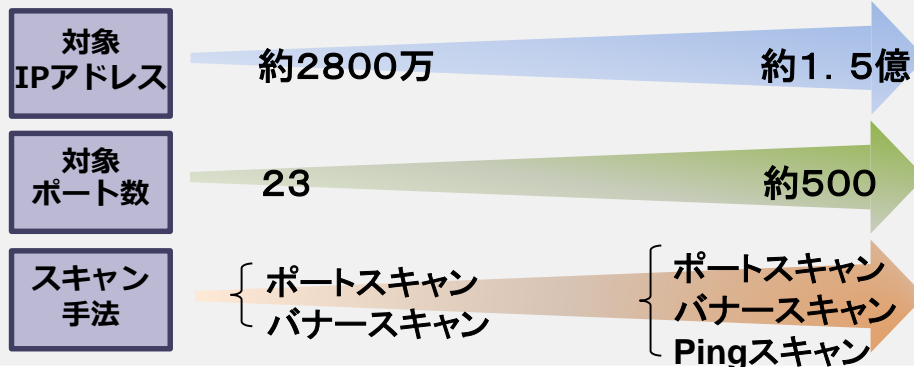
<実施内容>

- 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。

【実施工程】 Phase1 >> Phase2 >> Phase3 >> Phase4



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】

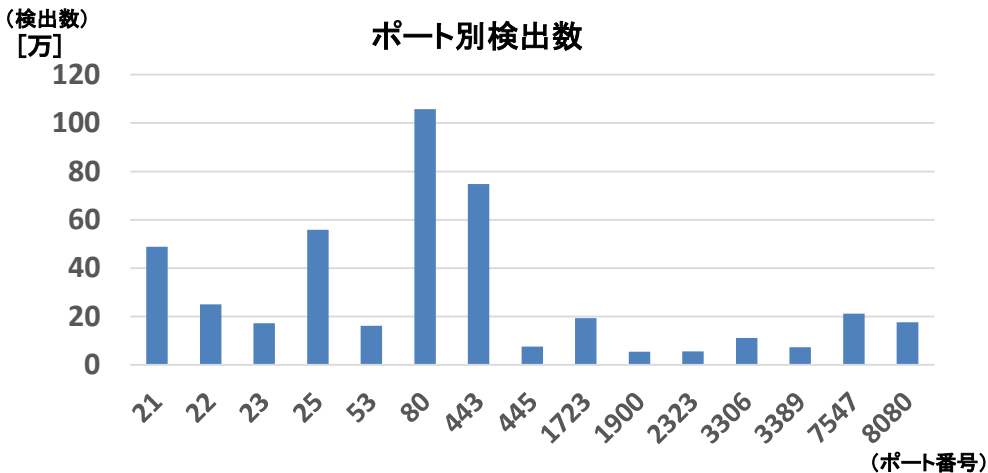
- オープンソースのツールをベースとして、設定、チューニング、機能追加し、独自のスキャンシステムを構築。
- 構築したスキャンシステムの機能については、「SHODAN」、「Censys」の情報と比較しても、遜色なく、十分な調査能力を有していることを確認。これにより、信憑性を確保した正確なスキャン結果の蓄積が可能となった。

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。



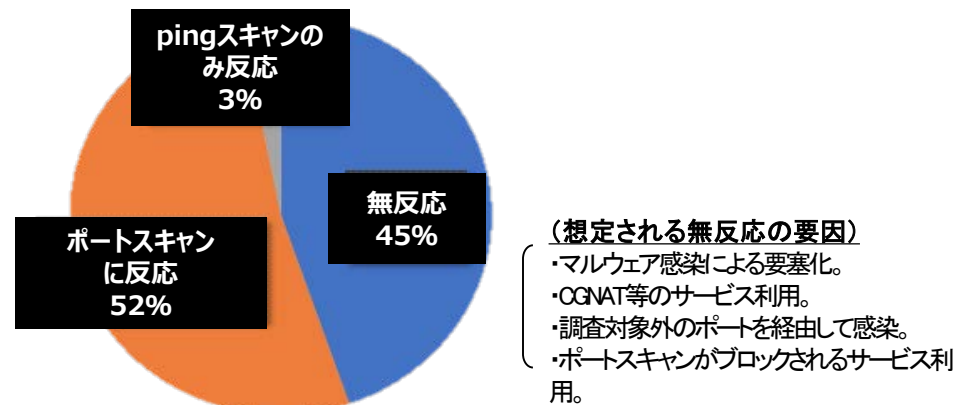
【バナー情報等をもとにした機種特定の実現性検証】

- 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



- 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12】

- 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)する等の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った。

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)。

情報通信研究機構法の改正

サイバーセキュリティ
戦略本部

(中長期計画)
意見聴取

総務大臣

(中長期計画認可)

情報通信研究機構

- ・パスワード設定に不備のある機器に係るIPアドレス等を提供

②情報提供

第三者
機関

※ 改正後の電気通信事業法に規定する第三者機関に委託

電気通信事業者

①機器調査

- ・パスワード設定に不備のある機器(その機器に係るIPアドレス)を特定

※ 総務大臣が調査の実施計画を認可

③注意喚起

- ・パスワード設定に不備のある機器に係る利用者を特定し、設定変更の注意喚起



※ 平成30年度予算を活用しつつ、サポート体制整備等を実施

インターネット上のIoT機器

機器の利用者

攻撃者

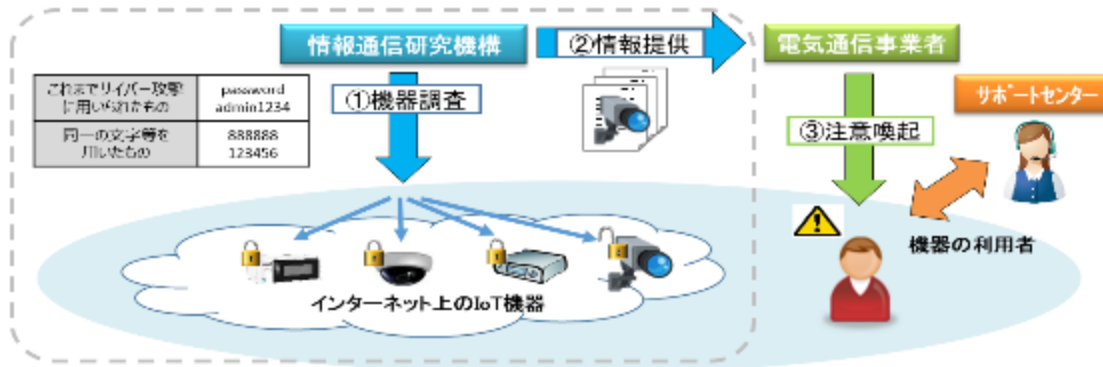
- IoT機器等を悪用したサイバー攻撃の深刻化を踏まえ、国立研究開発法人情報通信研究機構（NICT）の業務に、パスワード設定等に不備のあるIoT機器の調査等を追加するため、国立研究開発法人情報通信研究機構法を平成30年5月に改正。
- 平成31年2月20日（水）より、同法に基づきNICTがサイバー攻撃に悪用されるおそれのある機器を調査し、電気通信事業者を通じた利用者への注意喚起を行う取組「NOTICE※」を実施。

※National Operation Towards IoT Clean Environment

＜本取組の概要＞

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

（イメージ図）



※ 利用者からの問合せ対応等を行うサポートセンターを設置

- 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

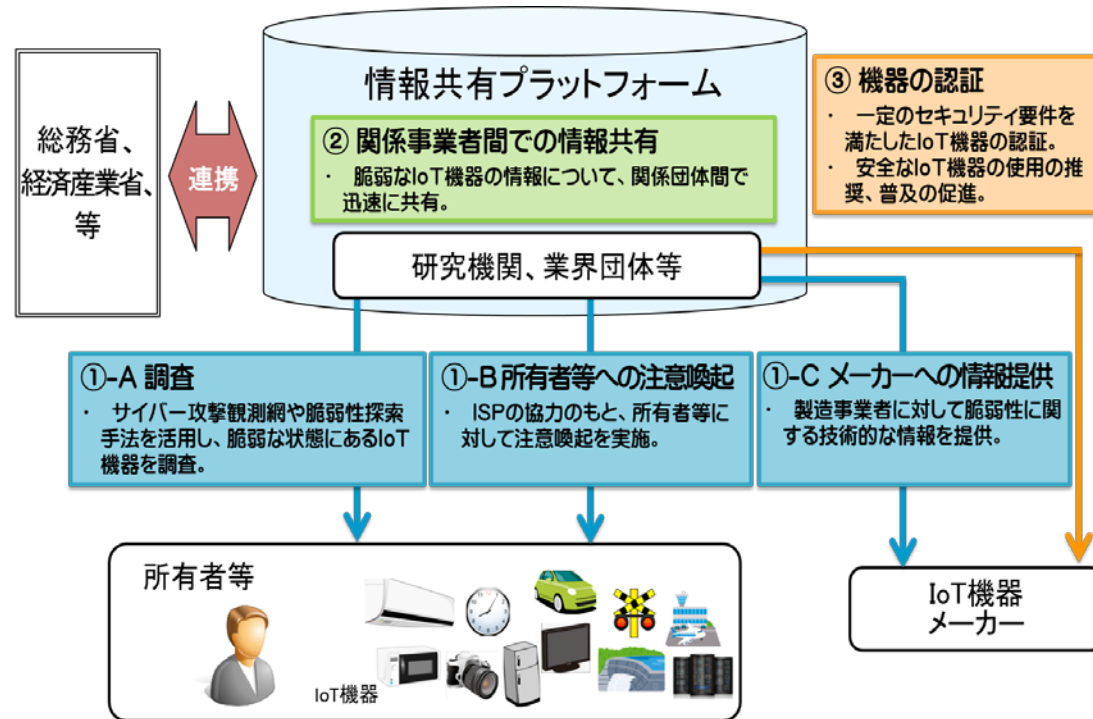
広域ネットワーク探索手法、サイバー攻撃観測網等を活用し、インターネットに接続されているIoT機器の調査を実施。脆弱性を持つIoT機器が発見された場合は、インターネットサービスプロバイダ(ISP)等の協力のもと、当該機器の所有者・運用者・利用者へ注意喚起を行う。

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)

1. 電気通信事業者による攻撃通信の発生防止

- ・ 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

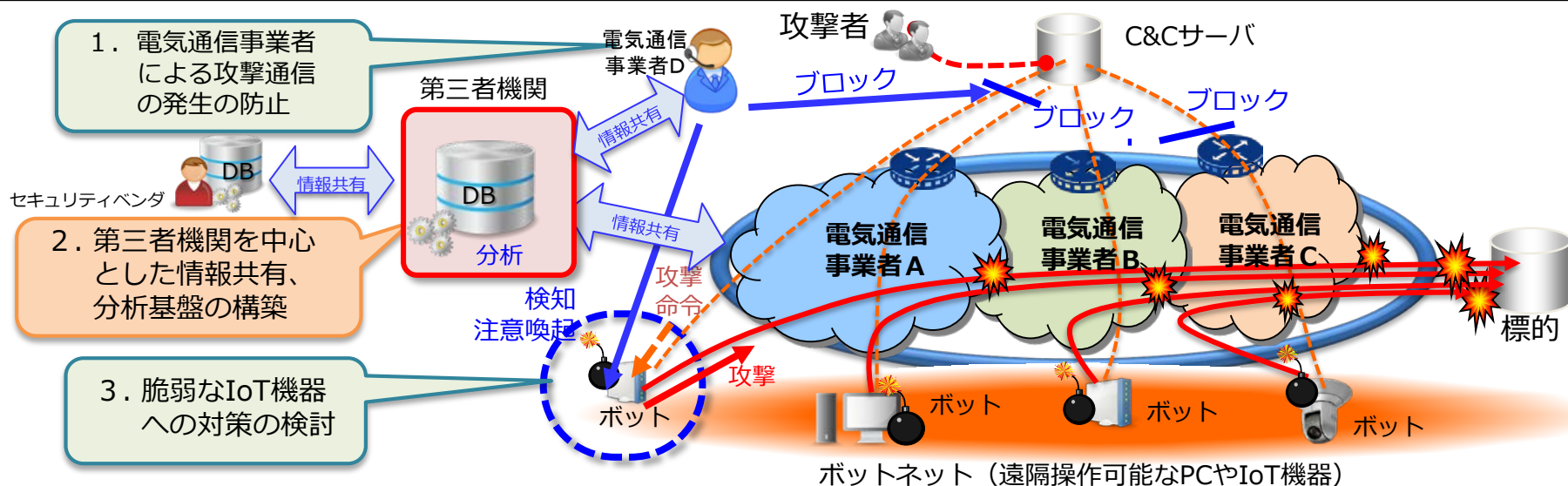
- ・ 1. の対策の実効性を高めるため、第三者機関が指令サーバ等に関する情報を集約し、分析・検証した上で電気通信事業者との間で情報共有。
 ※ 本取組においては、第三者機関が、通信の秘密を集約、分析・検証、共有することとなる。
 → **第三者機関が通信の秘密に該当する情報を扱うことから、裏付けとなる法制度を整備。**

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。**

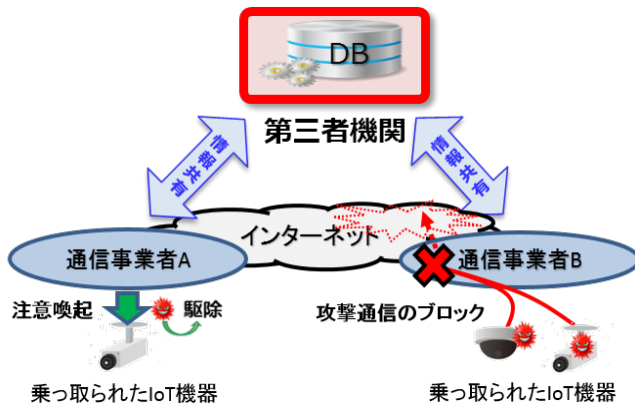


○ IoT化に伴うサイバー攻撃の深刻化やネットワークのIP網への移行に対応するため、電気通信事業法の改正を行った。

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**。

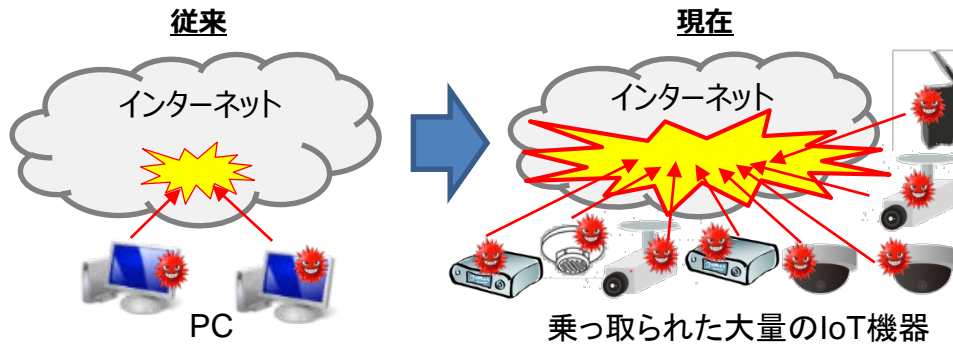
※悪意あるソフトウェアの総称であり、コンピュータに感染することによって、サイバー攻撃などの遠隔操作を自動的に実行するプログラムのこと。

現 状

インターネットの障害の深刻化

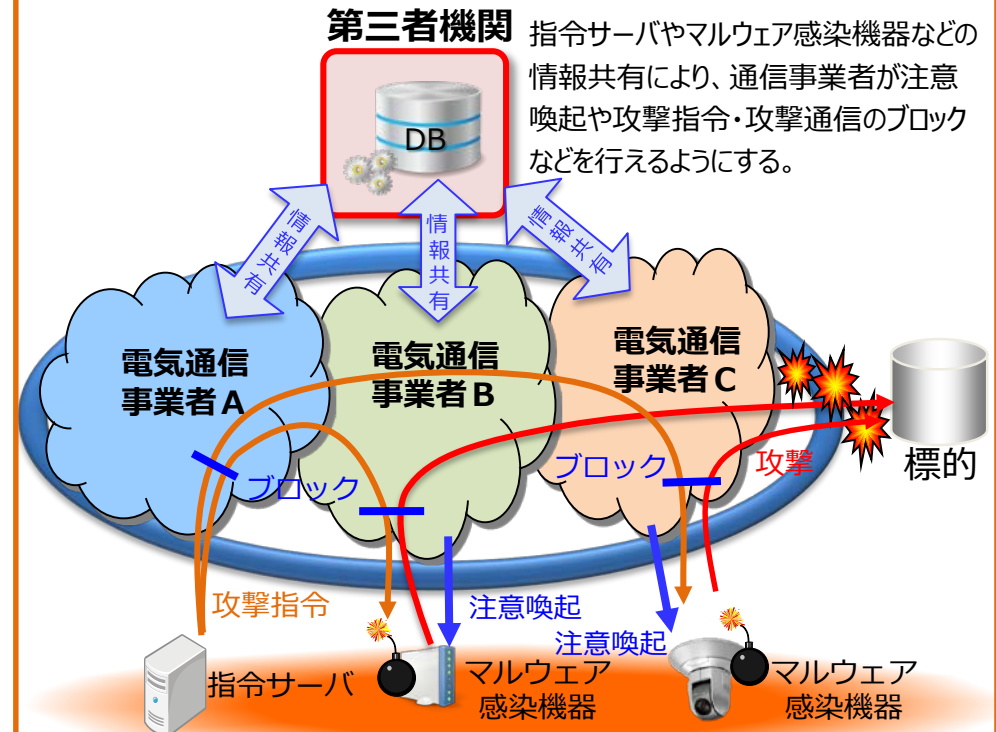
- サイバー攻撃によるインターネットの障害が発生し、国民生活や社会経済活動に影響
- 増加するIoT機器※を悪用したサイバー攻撃によりインターネットに重大な障害が発生
- 2020年の東京オリンピック・パラリンピック競技大会に際して、日本に対する大規模なサイバー攻撃の発生の懸念

※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



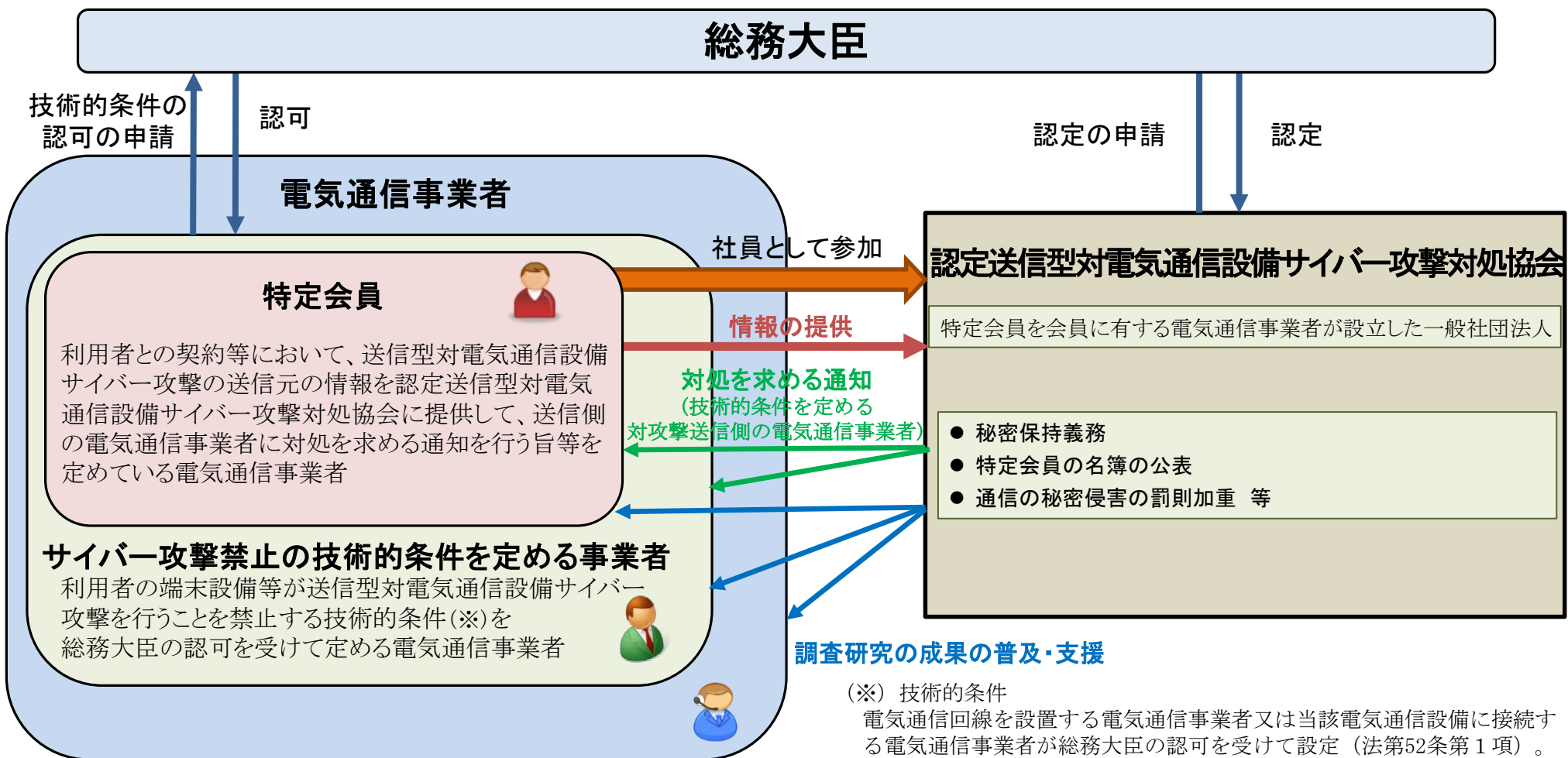
制度整備(イメージ)

第三者機関を中心とした情報共有基盤の構築



認定送信型対電気通信設備サイバー攻撃対処協会制度の概要【資料17】

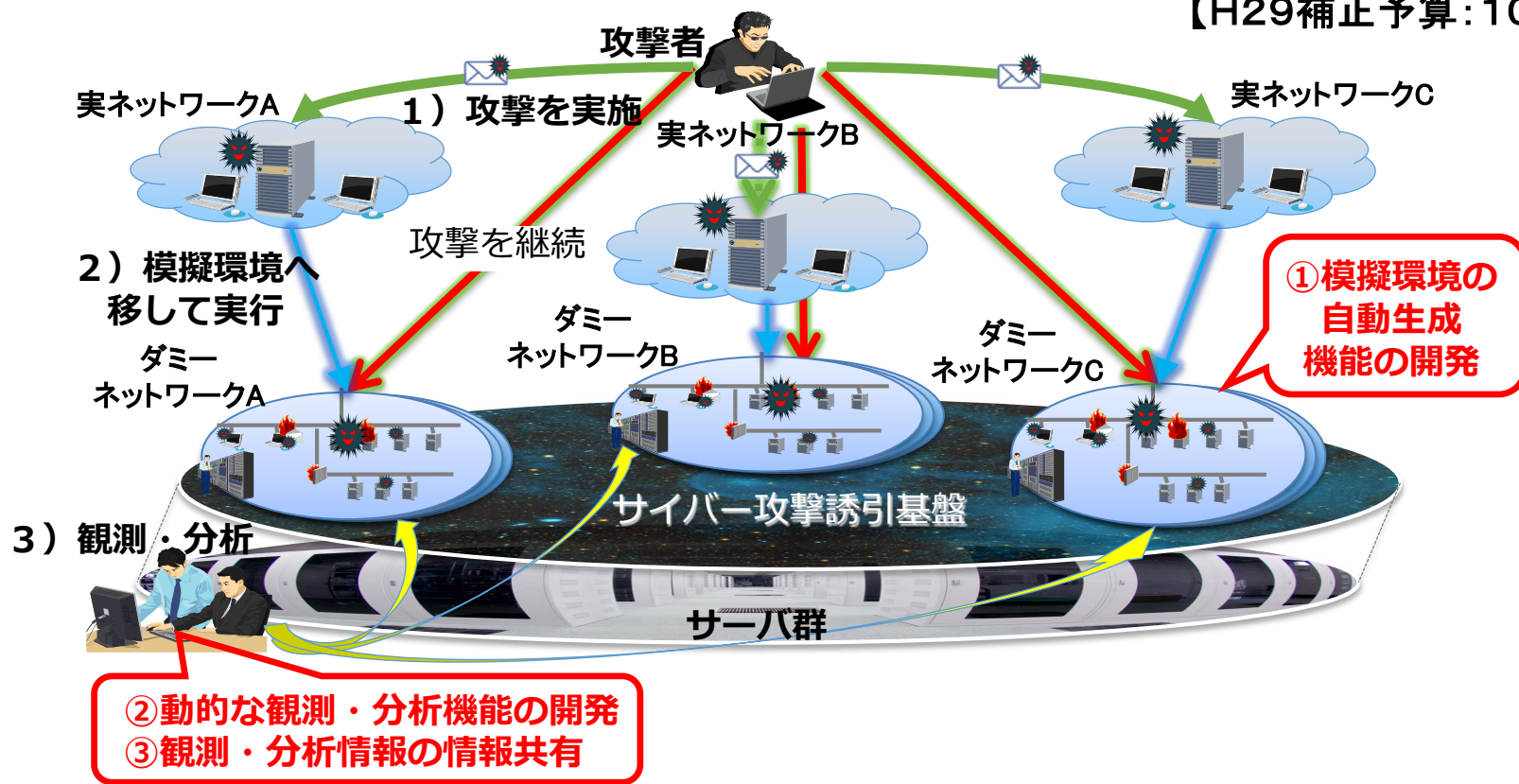
- 2018年(平成30年)5月23日に公布された改正電気通信事業法において、電気通信事業者がDDoS攻撃等のサイバー攻撃への対応を共同して行うため、サイバー攻撃の送信元情報の共有やC&Cサーバの調査研究等の業務を行う第三者機関を総務大臣が認定する制度を創設。
- 当該第三者機関である認定送信型対電気通信設備サイバー攻撃対処協会(以下、認定協会)については2019年(平成31年)1月に、総務大臣により一般社団法人ICT-ISACが認定。



サイバー攻撃誘引基盤の構築(STARDUST)

- 高度かつ複雑なサイバー攻撃に対処するため、政府や企業等の組織を模擬したネットワークに攻撃者を誘い込み、攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握することが可能な、高度で効率的なサイバー攻撃誘引基盤を構築。
- 攻撃活動の早期収集や未知の標的型攻撃等を迅速に検知する技術等の実証を行うための研究開発環境を、情報通信研究機構（NICT）に整備。分析結果は、セキュリティ対策機関等と連携して情報共有を図り、安全なサイバー空間を実現。

【H29補正予算:10.0億円】



目指す姿

概要

セキュアな Society 5.0 の実現に向け、様々なIoT機器を守り社会全体の安全・安心を確立するため、IoTシステム・サービス及び中小企業を含む大規模サプライチェーン*1全体を守ることに活用できる『サイバー・フィジカル・セキュリティ対策基盤』の開発と実証を行う。多様な社会インフラやサービス、幅広いサプライチェーンを有する製造・流通・ビル等の各産業分野への社会実装を推進する*2。

目標

*1: 自動車産業の延べサプライヤー数は100万社超(2012年)

*2: 「未来投資戦略 2017」閣議決定(2017年6月)

スマート家電等の一般消費者向けの機器から産業用システムまで、多様なIoT機器・システム・サービスのセキュリティを確保できる『サイバー・フィジカル・セキュリティ対策基盤』を確立する。実証を通じて有効性を確認し、実稼働するサプライチェーンに組み込み実用化する。本基盤の社会実装を他国に先駆けて推進することで、サイバー脅威に対するIoT社会の強靱化を図り、我が国のセキュアなSociety5.0実現に寄与する。

出口戦略

当初から課題認識のある製造・流通・ビル等のユーザ企業と連携した研究開発と実証実験を進め、参画企業が主体的に製品化・事業化。欧米の基準とすり合わせながら府省による制度整備と連携してIoTシステム・サービスやサプライチェーンへの導入を促進し、2030年までにサプライチェーン対策が求められる中小企業の50%に成果の導入を目指す。

社会経済インパクト

IoT社会の強靱化（サイバー犯罪による経済損失回避）により、Society5.0の実現がもたらす約90兆円の価値創出を支える。さらにグローバルなサプライチェーンに参画する要件*3となるセキュリティ確保を適切なコストで実現することにより、日本の製品・サービスの国際競争力を強化（輸出主体の製造業の参入機会の確保）する。

*3: 米国のNIST SP800-171や、欧州のサイバーセキュリティ認証フレームワーク等の動き

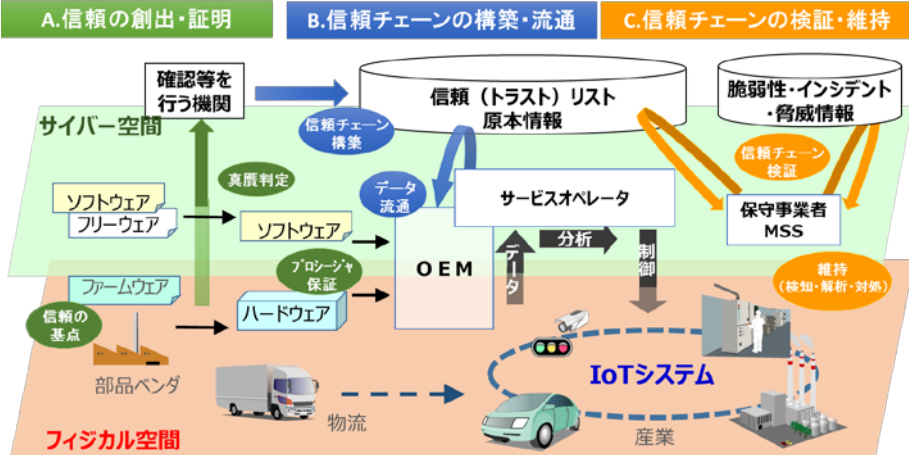
達成に向けて

研究開発内容

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、

- A. 信頼の創出・証明 (IoT機器向け真贋判定技術 等)
- B. 信頼チェーンの構築・流通 (トラストリストを用いた信頼チェーン構築技術 等)
- C. 信頼チェーンの検証・維持 (インシデントの検知・解析・対処など信頼チェーンの維持技術 等)

及び、その他、必要な研究開発・動向調査を行い、実サービスや各産業分野において実証を行う。



5Gネットワークのセキュリティ確保に向けた体制整備と周知・啓発(令和元年度予算)【資料20】

第5世代移動通信システム(5G)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。

<基本的考え方>

- ネットワークインフラとしての機能維持のためには、コア網の機器調達のみには留意すれば良いわけではない。ネットワークのエッジ(基地局の直前)に位置するモバイルエッジコンピューティングのセキュリティが確保されない限り、機能停止/不正動作等のおそれあり。
- 重要通信については、SDN/NFV/スライス等のネットワーク制御技術のセキュリティ対策に加え、5G環境下でのネットワークサービスの各構成要素(デバイス、クラウド、アプリ等)全体を考慮することが必要。

クラウド／アプリケーション

5Gコア

モバイルエッジコンピューティング

5Gアクセス

IoTデバイス



<令和元年度予算>

- 5Gの仮想環境を構築し、以下の手法により、ネットワークに潜在する脆弱性調査及びセキュリティ課題の洗い出しを実施。
 - ①5Gに実装されるオープンソースソフトウェア等の解析
 - ②多種多様なパターンのデータ送付(ファジング)による異常動作の確認
 - ③ホワイトハッカーによる脆弱性調査、脅威分析
- その結果を踏まえた対応策の策定とその周知・啓発を図る。

OSSの脆弱性

ファジング

疑似攻撃

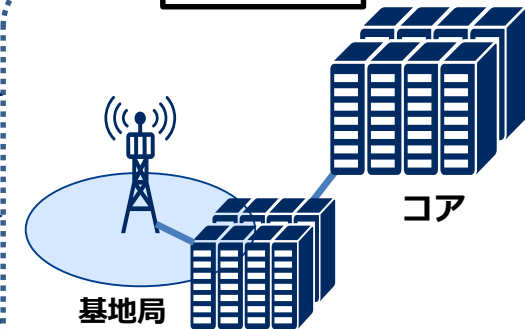
ホワイトハッカーによる脅威分析

5G仮想環境

基地局

モバイルエッジコンピューティング

コア

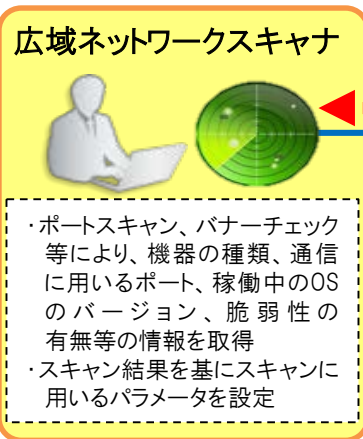
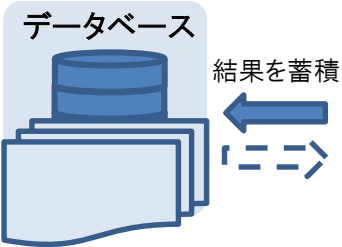


- 近年、IoT機器を狙ったサイバー攻撃は増加傾向にあり、脆弱なIoT機器への対策は喫緊の課題。
- 今後、無線通信を利用するIoT機器の割合は増加するものと見込まれているため、「周波数有効利用のためのIoTワイヤレス高効率広域ネットワークスキャン技術の研究開発」に取り組み、効率的な広域ネットワークスキャンの実現を目指す。

広域ネットワークスキャンを実現する要素技術

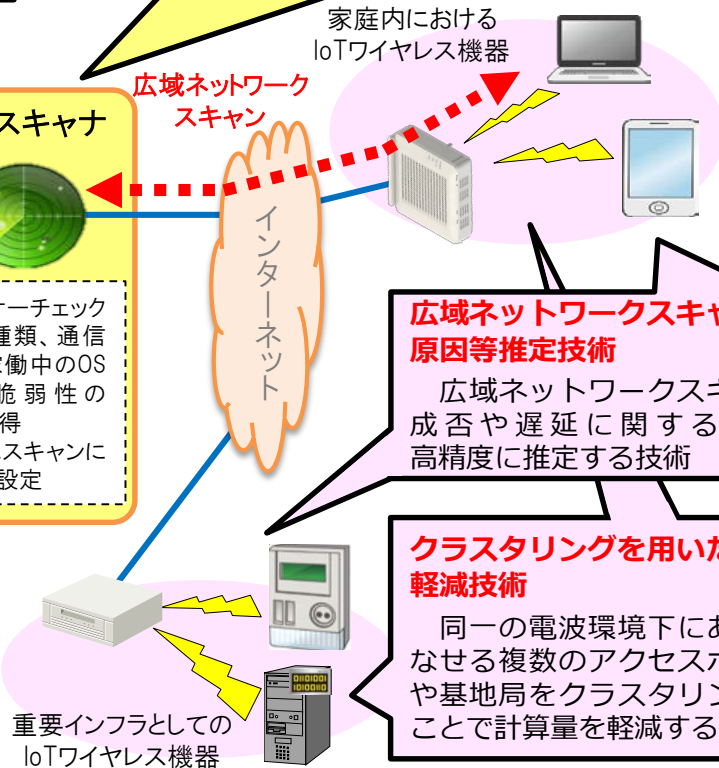
広域ネットワークスキャン頻度最適化技術
広域ネットワークスキャンの頻度を最適化する技術

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

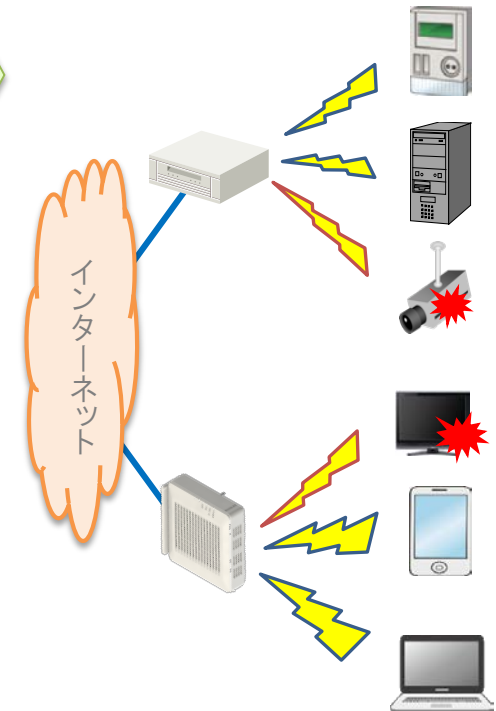


広域ネットワークスキャン遅延原因等推定技術
広域ネットワークスキャンの成否や遅延に関する原因を高精度に推定する技術

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



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、スパム攻撃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。

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

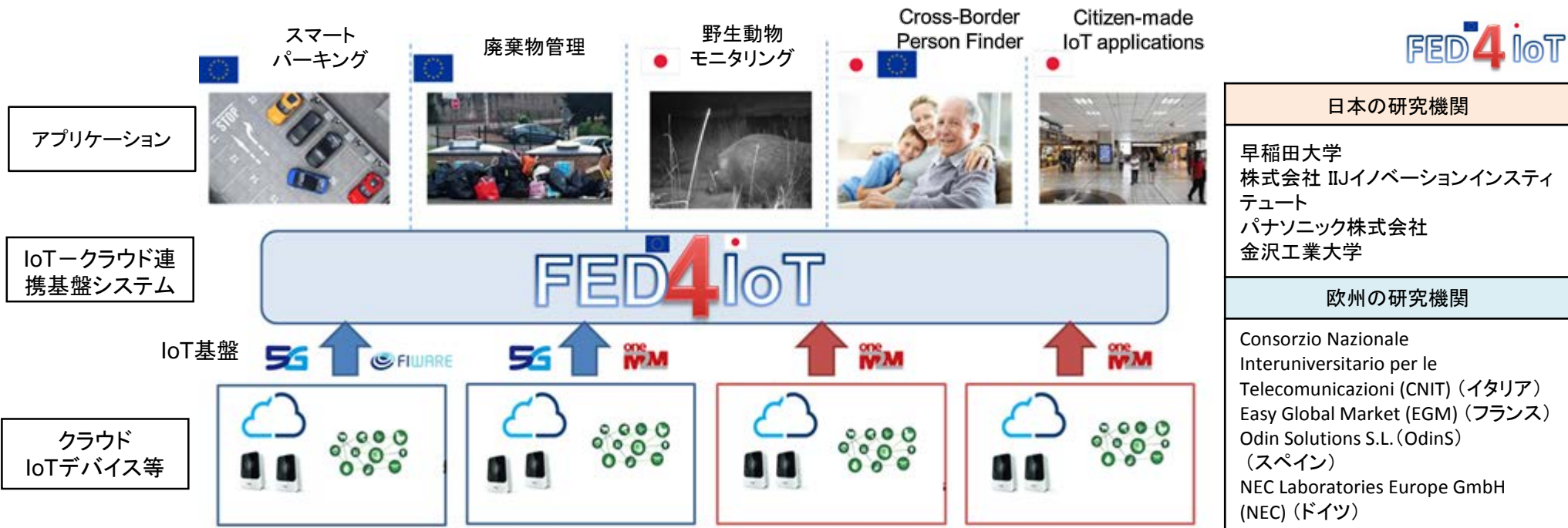
Fed4IoTの概要 日EU共同研究(SCOPE(国際標準獲得型)第4次公募)【資料23】

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

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

実証実験

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



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

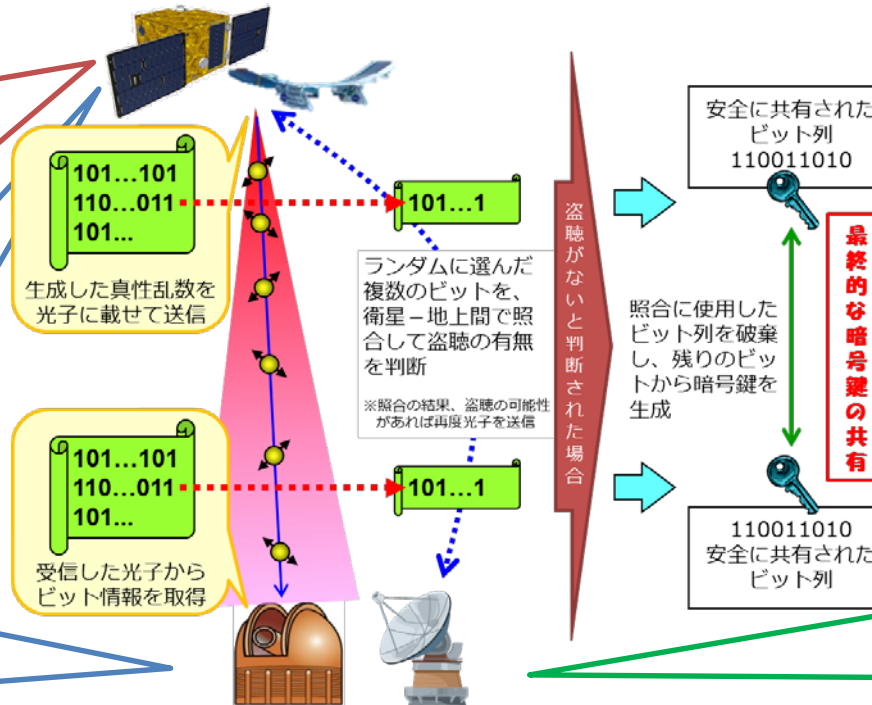
研究開発内容

(1) 小型衛星に搭載可能な量子暗号通信技術の開発

- ・小型衛星に搭載可能な装置の小型軽量化・省電力化
- ・宇宙空間という電子機器には劣悪な環境下において動作
- ・鍵生成の高速化技術の開発

(2) 空間光通信・高精度捕捉追尾技術の開発

- ・衛星への照準を精微に合わせるための高精度な捕捉追尾技術の開発



(4) インテグレーション・航空機等による実証実験

- ・開発機器を統合し、航空機等を用いた実証実験を行う。

(3) 光地上局の高感度受信技術の開発

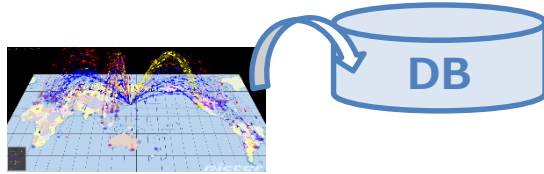
- ・衛星から送信された光信号を地上局において、高感度に受信する技術の開発

- 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。

データセットの構築（例）

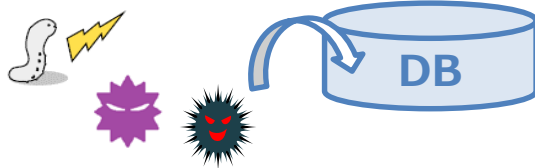
■ ダークネット関連データ

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

マルウェア検体や静的・動的解析結果等



■ Android APK関連データ

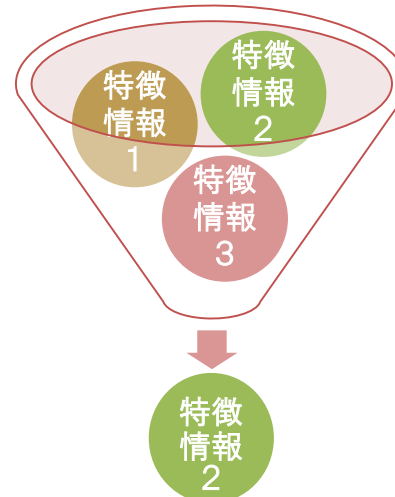
アプリのカテゴリ情報や説明文等



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

**攻撃の影響度分析や
攻撃相関分析、攻撃
パターン分析等を自動化**

（事例1）DDoS攻撃の早期検知

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において配布され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。

- 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、A I、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 $\geq 3\%$ を満たした場合。

- 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（第三者開示）、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（第三者開示） ……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。

（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ISA0(※)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】

(※)ISA0: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。

（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】

※ 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

- 民間企業のサイバーセキュリティ対策の情報開示の促進のため、民間企業にとって参考となり得る事例等をまとめた手引きを策定する。

目的

- ✓ 民間企業によるサイバーセキュリティ対策やその対策の情報開示の重要性の認識を促進する。
- ✓ 民間企業にとって参考になり得るような既存の開示の実例を事例集として示す。

活用主体

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

対象とする 情報開示

- ✓ 開示書類を通じた情報開示を取り扱う。
- ✓ 開示書類の読み手は、投資家、融資元、顧客・契約者・取引先、従業員、競合他社等を含む、社会全体の広範なステークホルダーを想定。

内容

- ✓ 企業が取ることが望ましい対策項目を記載した上で、その開示に当たっての留意事項等について記載。
- ✓ 既に存在する開示の実例について、対策項目との関係性を明示して掲載する。

情報共有基盤に関する実証事業の概要

<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。

収集

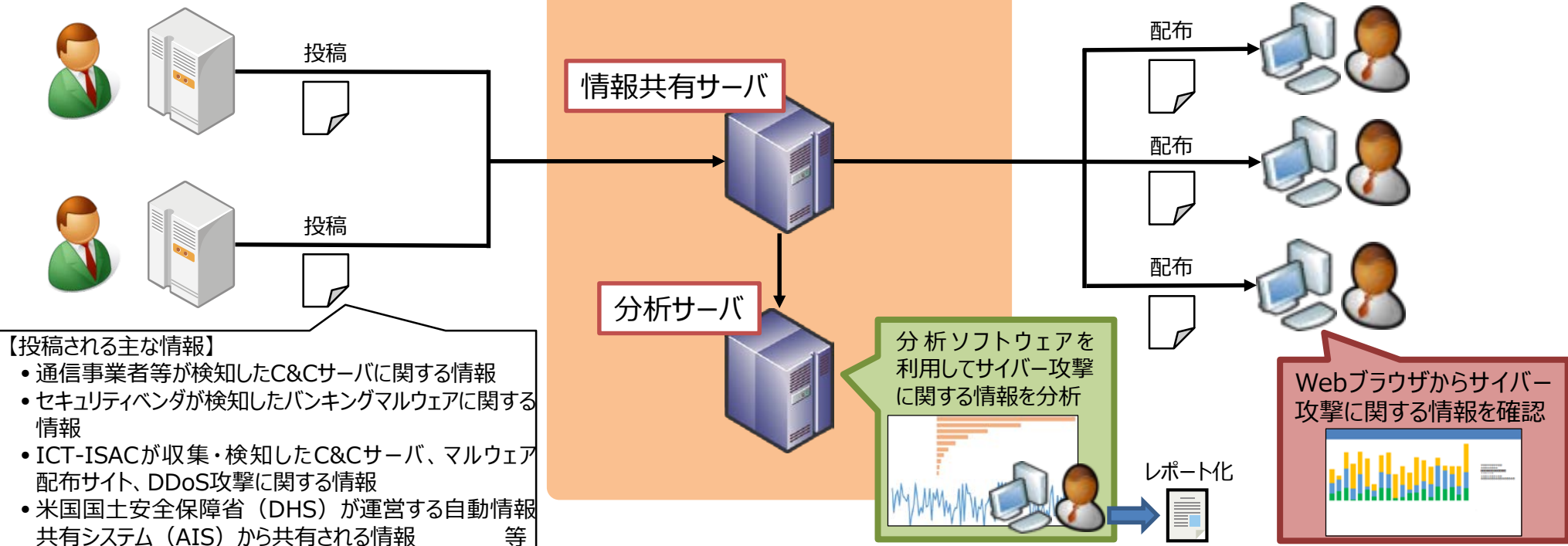
分析

配布

情報提供者

情報共有基盤

情報利用者



利用ガイドラインの策定

- 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）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の利用者のセキュリティ対策に係る周知・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。

<講座の概要>

全8回の動画コンテンツから構成され、有識者が公衆無線LANを利用する際のリスクを事例を通じて紹介するとともに、適切なセキュリティ対策の方法をわかりやすく紹介。

The screenshot shows the gacco website interface. At the top, there is a navigation bar with 'ログイン' (Login) and '新規会員登録' (New Member Registration) buttons. The main header features the title 'これだけは知っておきたい公衆無線LANセキュリティ対策' (Essential Public Wi-Fi Security Measures) and a red '受講登録する(無料)' (Register for Course (Free)) button. Below the header, there is a '講座概要' (Course Overview) section. The '講座内容' (Course Content) section describes the course's focus on security risks in various scenarios and provides details such as the course number (pt023), start date (February 27, 2019), and duration (1 hour). A note indicates that user information is shared with the provider. The bottom part of the page mentions that the course consists of 8 video lessons, with the first 4 covering general risks and the last 4 providing specific security measures.

The infographic is titled '第2回 とっても危険! 「野良Wi-Fi」' (Lesson 2: Super Dangerous! 'Stray Wi-Fi'). It features a large Wi-Fi symbol in the top right corner. The text identifies the instructor as '猪俣 敦夫' (Ikumaru Atsuo) from the Department of Future Science, Tokyo University of Science. A warning box labeled '2-3' states: 'そのメール、悪意のある第三者に見られてしまうかも <盗聴の危険>' (Your email may be seen by a malicious third party <Risk of eavesdropping>). Below this, two bullet points highlight risks: 1) Connecting to unencrypted access points can lead to eavesdropping on content, and 2) Unauthorized access can lead to information leakage or theft. An illustration at the bottom shows a man with a suitcase and a Wi-Fi symbol, and a thief with a Wi-Fi symbol and a 'PASS' label. A callout box explains that '野良Wi-Fiとは、身元不明、誰が提供しているかわからないアクセスポイントのこと' (Stray Wi-Fi is an access point where the identity is unknown and the provider is unknown). A final warning states: '重要な情報を盗み取られる危険性' (Risk of important information being stolen).

○ 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月より、情報通信研究機構(NICT)の「ナショナルサイバートレーニングセンター」において、以下の実践的サイバー演習等を積極的に推進。

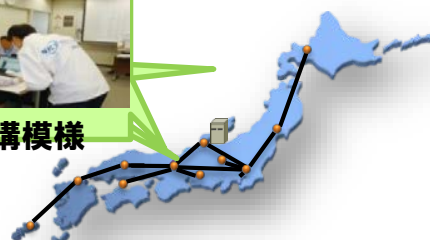
- ① 国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等を対象とした実践的サイバー防御演習(CYDER)
⇒ 年間100回、3,000名規模で実施(1日コース、全都道府県で開催)。
- ② 2020年東京オリンピック・パラリンピック競技大会に向けた等大会関連組織のセキュリティ担当者を対象者とした実践的サイバー演習(サイバーコロッセオ)
⇒ 平成29年度は延べ74名、平成30年度は延べ137名が受講。
- ③ 25歳以下の若手セキュリティイノベーターの育成(SecHack365)
⇒ 平成29年度は39名、平成30年度は46名が1年間のコースを終了。

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

サイバー攻撃への
対処方法を体得



演習受講模様



CYDER

チケット販売

社会インフラ

公式HP

擬似オリンピック
パラリンピック
システム

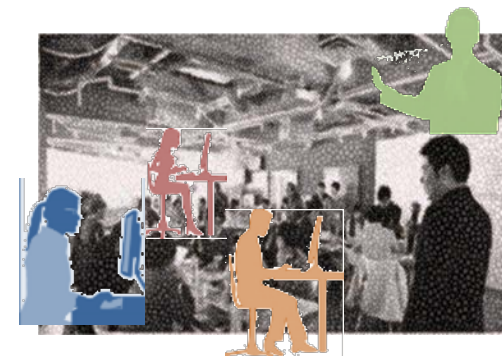
避難・誘導

放送環境

WiFi・通信環境



サイバーコロッセオ

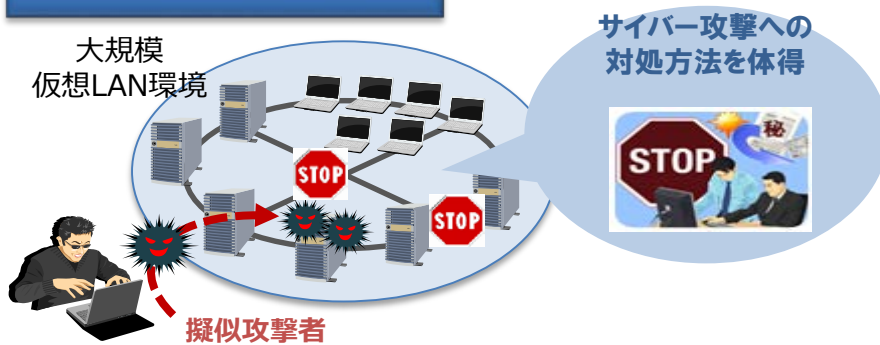


SecHack365

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。平成30年度は、全国で107回開催し、計2,666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。

令和元年度の実施計画

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、重要社会基盤事業者、民間企業等向け	東京ほか	20回

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34】

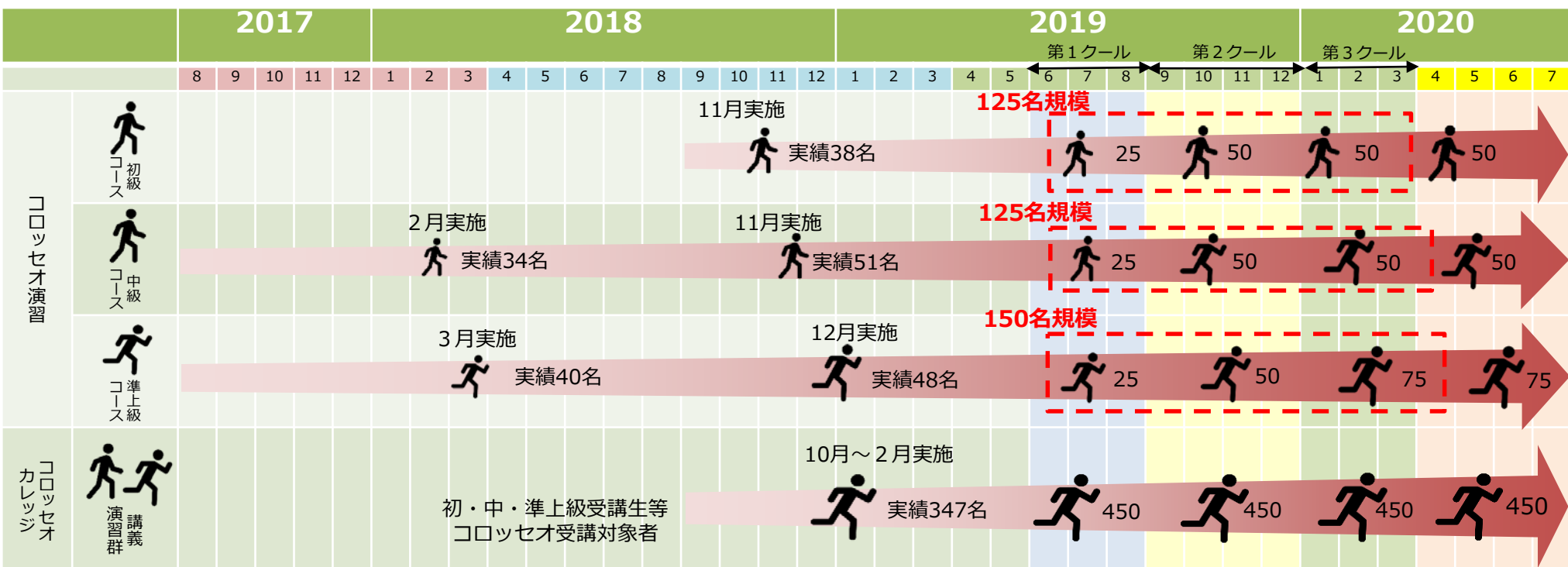
○近年さらに高度化・多様化するサイバー攻撃に備え、東京2020オリンピック・パラリンピック競技大会の適切な運営を確保することを目的として、大会関連組織のセキュリティ担当者等を対象とした、高度な攻撃に対処可能な人材の育成を行う実践的サイバー演習「サイバーコロッセオ」を平成30年2月から本格的に実施。

○ 2018年度、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、347名が受講。実機演習では、初級コースを開設し、初級38名、中級51名、準上級48名の計137名が受講。

○ 2019年3月、サイバーコロッセオ実施計画を改定し、2019年度以降の対象者の受講機会を拡大。

- ① 3クール制(第1クール(2019年6月～8月)・第2クール(2019年9月～12月)・第3クール(2020年1月～3月))により受講機会を分散。
- 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加し、内容を充実。
- ③ 中級・準上級の演習シナリオを追加。

※受講人数は延べ人数



※ 目標人数は現時点において公益財団法人東京オリンピック・パラリンピック競技大会組織委員会(以下「組織委」という。)が想定する延べ人数であり、今後、組織委側のニーズを踏まえつつ、必要に応じて見直しを行う予定。
 「東京2020オリンピック・パラリンピック競技大会に向けたサイバーコロッセオ実施計画」(2019年3月12日時点)を基に作成

- **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、平成30年度は46名が修了）。
- 受講者は、NICTの有する遠隔開発環境を活用し、**年中どこからでも遠隔開発実習を行うことが可能。**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。**

若手セキュリティイノベータの育成



通常システム開発者層



■ 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。

- サイバーセキュリティ人材は首都圏等に偏在し、地方においては不足していることから、組織の壁を越えて、人材育成のリーダーを育成するとともに、専門家のシェアリングを行って、地域のセキュリティ対策を支援。
- 地域の企業や教育機関と連携し、セキュリティ人材が地域に根付くエコシステムを形成。

1. 研修リーダーの不在

気づきの機会がない

悪循環

研修があっても参加者が少ない

地方で研修が開催されない

2. 組織体制の不足

何をすればよいかわからない

悪循環

専門人材を雇用できない

対策が進まない

3. 就業機会の不足

雇用の受け皿がない

悪循環

地域の若年層がセキュリティ人材を目指さない

地域におけるセキュリティ人材がさらに不足

1. 地域のセキュリティリーダーの育成



- 地域のコミュニティ活動を活性化し、中核としてリードする人材を育成。

2. 地域でのセキュリティ人材のシェアリング

セキュリティ人材を必要とする企業



マッチング

セキュリティスキルを持った人材



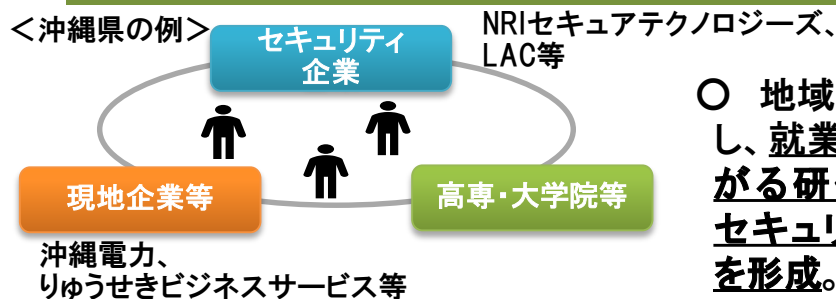
人材のシェアリング

- 県や広域的なエリアにおいて、複数の中小企業等がセキュリティの専門家をシェアできるようにマッチング。

※ 地域情報化アドバイザーとも連携

3. 地域におけるセキュリティ人材のエコシステムの形成

<沖縄県の例>



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

「日ASEANサイバーセキュリティ能力構築センター(AJCCBC)」プロジェクトの概要【資料37】

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

実施時期

STEP1: 2017年～

事前調査を実施

STEP2: 2018年～

センターを活用し以下の活動を実施

STEP2の主な活動内容

1. サイバーセキュリティ演習(CYDER※等)

政府機関・重要インフラ事業者等に対し、以下の演習プログラムを実施。

- ・実践的サイバー防御演習(CYDER)※CYDER: Cyber Defense Exercise with Recurrence
- ・証拠保全・解析等のためのデジタルフォレンジック演習
- ・マルウェアの挙動解析演習

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

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

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



日ASEAN情報通信大臣会合(2017.12)



サイバーセキュリティ演習

1. 開催概要

- 日時 : 平成30年10月16日(火)及び17日(水)
- 場所 : 京王プラザホテル(東京)
- 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. 主な成果

2017年10月にシンガポールで開催された第10回会合において協力することが合意された、サイバー演習、重要インフラ防護、人材育成等に関する協力活動について実施状況を確認。また、今後の日・ASEANの連携・協力についての検討を実施。

(1) 情報共有体制及びサイバーインシデント発生時の対処体制の強化

日・ASEANにおけるサイバーセキュリティ脅威情報共有体制の維持と、インシデント発生時の国際連携手順の確認を目的とした、情報連絡演習及び机上演習について、今年度の成果が報告された。また、来年度以降も継続的に実施することが確認された。

また、日常的な情報共有を一層充実させるために、新たなコミュニケーションツールを試験導入することに合意。

(2) 重要インフラ防護に関する取り組みの推進

重要インフラ防護の実践的な取り組みや、先進的・先導的な取り組みに関する情報交換を行うため、昨年引き続き「重要インフラ防護ワークショップ」が開催されたことが報告された。また、来年度以降も継続的に実施することを確認。

(3) 人材育成における協力の推進

日本が実施しているサイバー分野の人材育成事業の実施状況が報告されるとともに、日本とASEAN各国の意識啓発活動の実施状況が報告された。また、来年度以降も継続的に実施することを確認。

第9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39】

1. ワークショップの概要

日時： 平成31年1月23日(水)及び24日(木)

場所： Singapore Marriott Tang Plaza Hotel(シンガポール)

主催： 総務省及びシンガポール情報通信メディア開発庁(IMDA)

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

参加者：傍聴者を含み全体で50名程度

ASEAN10か国のISP事業者又は政府機関(計35名)

総務省、在シンガポール日本大使館、ICT-ISAC(計9名)



ワークショップ集合写真

2. 主な内容

- 総務省から、IoTセキュリティ対策の取組及びASEAN諸国に対する能力構築支援の取組等について発表
- ICT-ISACから、ICT-ISAC Japanの概要、各WGの活動状況、脅威情報の共有の取組等について発表
- ASEANの参加者から、各国におけるサイバー攻撃の現状やサイバーセキュリティの取組について発表
- サイバー攻撃対応机上演習を実施。国境を越えた連携が必要な脅威(DDoS攻撃やフィッシングサイト対策等)を想定したシナリオへの対処を議論

3. 成果

- 各国のISP事業者におけるサイバーセキュリティ分野の取組状況の共有と意見交換
- ASEAN各国(主にISP事業者)との人的ネットワークの維持・強化
- 各国より課題として多く挙げられたDDoS攻撃対策やIoTセキュリティ対策に関する情報共有を今後も継続することを確認
- 脅威情報の共有体制、方法について継続的な意見交換を実施していくことを確認

複雑化・高度化が進むサイバー空間の脅威に対応するためには、官民での情報共有や国際連携の強化が重要。

総務省では、サイバー脅威に対する国内通信インフラ事業者の対処能力向上を目的として、日米の情報通信分野ISAC(*)組織間における情報共有・連携の促進を支援。

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

■ 日米ISAC連携の取組

日米の情報通信分野のISAC組織間における情報共有・連携の促進を目的として、日本のICT-ISAC Japan、米国のIT-ISAC及びComm-ISACを中心とした組織間で情報共有のあり方を議論するワークショップを開催。

- 2016年11月：日米ISAC関係者による初めての国際連携会合を開催。日米のサイバー脅威動向や取組状況等を意見交換。
- 2017年11月：第2回会合を開催。米国IT-ISACの保有するサイバー脅威関連情報のICT-ISACへの提供等について合意。
- 2019年2月：第3回会合を開催。各ISACが情報共有を推進する上での懸念事項を共有し、その解決策等を議論。あわせて、公開シンポジウムも開催。

今後も、日米ISAC間での効率的なサイバー脅威情報の共有が進むよう総務省としてもサポート。



公開シンポジウム 講演の様相



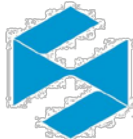
公開シンポジウム パネルディスカッション

IoTセキュリティガイドラインの国際標準化

○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

IoT セキュリティガイドライン
ver 1.0

平成 28 年 7 月

IoT 推進コンソーシアム
総務省
経済産業省



○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

○2018年9月、ITU-T SG17において、本ガイドラインをベースとして、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(X.sc-IoT)として承認

- 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「機器メーカー、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。

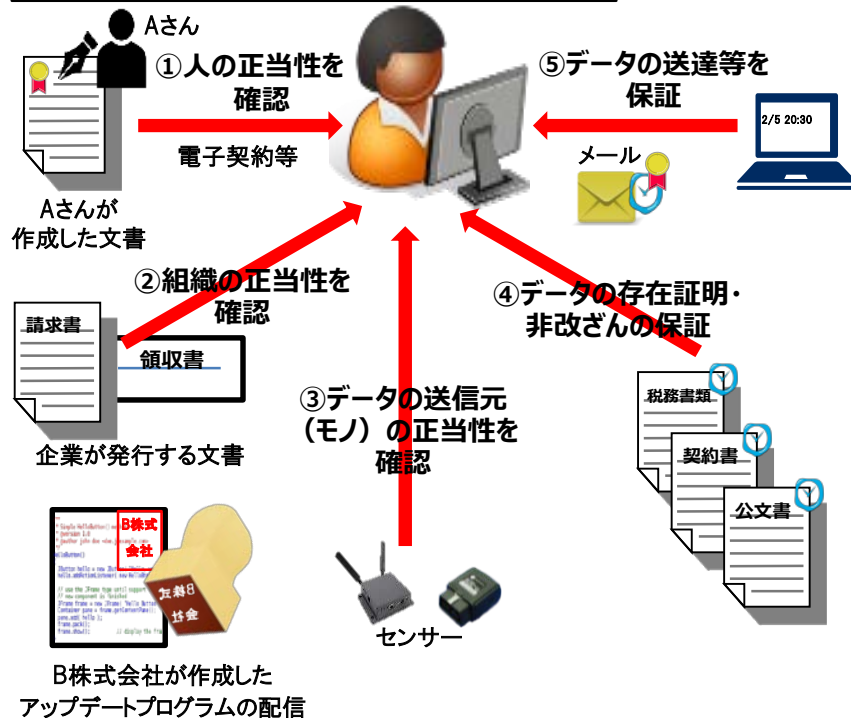
	指針	主な要点
方針	<u>IoTの性質を考慮した基本方針を定める</u>	<ul style="list-style-type: none"> 経営者がIoTセキュリティにコミットする 内部不正やミスに備える
分析	<u>IoTのリスクを認識する</u>	<ul style="list-style-type: none"> 守るべきものを特定する つながることによるリスクを想定する
設計	<u>守るべきものを守る設計を考える</u>	<ul style="list-style-type: none"> つながる相手に迷惑をかけない設計をする 不特定の相手とつなげられても安全安心を確保できる設計をする 安全安心を実現する設計の評価・検証を行う
構築・接続	<u>ネットワーク上での対策を考える</u>	<ul style="list-style-type: none"> 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	<u>安全安心な状態を維持し、情報発信・共有を行う</u>	<ul style="list-style-type: none"> 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		<ul style="list-style-type: none"> 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。

トラストサービスの制度化に向けた検討

- Society5.0の実現に向けて、サイバー空間と実空間の一体化が加速的に進展し、実空間での様々な活動がサイバー空間に置き換わる中、その有効性を担保するための基盤として、ネット利用者の本人確認やデータの改ざん防止等の仕組みであるトラストサービスが必要。

トラストサービスのイメージ



- ① **人の正当性**を確認できる仕組み(電子署名)
- ② **組織の正当性**を確認できる仕組み(組織を対象とする認証、ウェブサイト認証)
- ③ IoT機器等の**モノの正当性**を確認できる仕組み
- ④ **データの存在証明・非改ざんの保証**の仕組み(タイムスタンプ)
- ⑤ **データの送達等を保証**する仕組み(電子的な”書留”)

ネットワークにつながる人・組織・モノの正当性を確認できる仕組みの確保やデータの完全性の確保等を実現するためのトラストサービスについて、EUにおけるeIDAS規則の制定等の動きも踏まえつつ、国際的なサービスの進展を視野に入れた相互運用性の確保の観点からも、我が国としての在り方について検討。