資料９－１

「IoTセキュリティ総合対策」の取組状況について

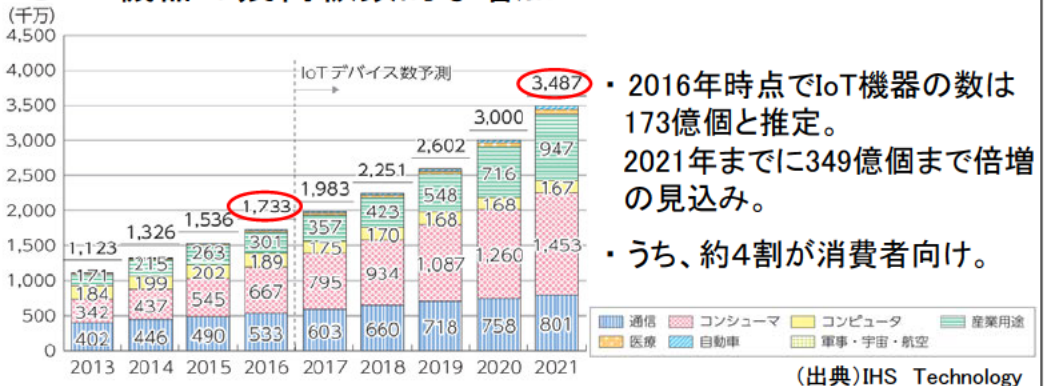
平成３０年４月１１日

事務局

IoTセキュリティ総合対策

現状

○IoT機器の幾何級数的な増加

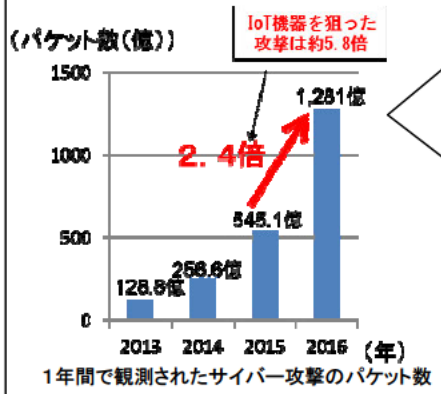


・2016年時点でIoT機器の数は173億個と推定。
2021年までに349億個まで倍増の見込み。

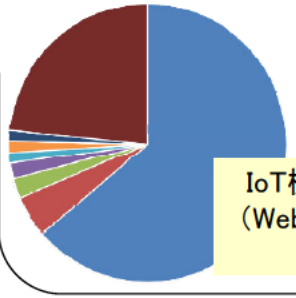
・うち、約4割が消費者向け。

(出典)IHS Technology

○IoT機器を狙った攻撃が急増



観測された全サイバー攻撃
1,281億パケットのうち、

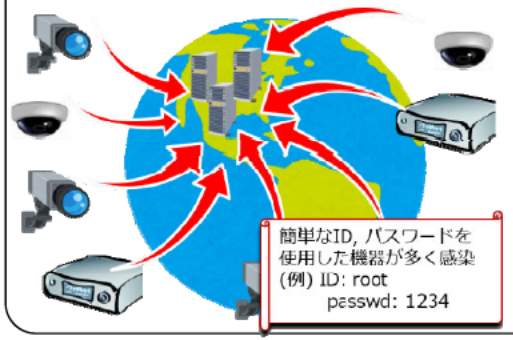


2/3

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)

「脆弱性対策に係る体制の整備」に係る取組状況

脆弱性対策に係る体制の整備

「IoTセキュリティ総合対策」における項目	取組状況
■　**セキュリティ・バイ・デザイン等の意識啓発・支援の実施** セキュリティ・バイ・デザインの考え方を踏まえ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、意識啓発・支援を実施。	・「IoT推進コンソーシアム IoTセキュリティWG」で検討 （平成29年12月～） 【参考資料　p. 8】
■　**IoTセキュアゲートウェイ** 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の検討。	・平成28年度補正予算　2．5億円 （サイバーセキュリティの強化　5．0億円の内数） 【参考資料　p. 9】
■　**重要IoT機器に係る脆弱性調査** ■　**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** IoT機器の調査を実施し、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実施。また、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ため、IoT機器の脆弱性情報を関係事業者間で共有する仕組みを構築。 ■　**IoT機器に関する脆弱性対策に関する実施体制の整備** 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））のあり方について検討（年度内を目途に結論）。	・平成28年度補正予算　1．1億円 （サイバーセキュリティの強化　5．0億円の内数） （平成29年秋から試行実施） 【参考資料　p. 10】 ・平成30年度予算 IoTセキュリティ総合対策の推進　6．0億円 （平成30～34年度） 【参考資料　p. 11】 ・平成30年3月6日、「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改正案」を国会提出 【参考資料　p. 12～14】
■　**被害拡大を防止するための取組の推進** 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、ISPによるC&Cサーバとの通信制御の実施を推進するとともに、当該取組を促進するための方策について検討（年度内を目途に方向性）。	・「円滑なインターネット利用環境の確保に関する検討会」において議論（平成29年10月～平成30年2月）。平成30年2月20日、「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」を公表。 【参考資料　p. 15】

「研究開発の推進」に係る取組状況

研究開発の推進

「IoTセキュリティ総合対策」における項目	取組状況
■基礎的・基盤的な研究開発等の推進 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（STARDUST）を構築。	・ 平成29年度補正予算 サイバー攻撃対策高度化研究開発環境の整備　10．0億円 ・ 平成30年度予算 国立研究開発法人情報通信研究機構運営費交付金　280．3億円の内数 （「サイバー攻撃誘引基盤の構築」（平成30～34年度）） 【参考資料　p．16】
■広域ネットワークスキャンの軽量化 膨大なIoT機器に対する広域的なネットワークスキャンを効率的に実施するため、その軽量化などの必要な技術開発を推進。	・ 平成30年度予算　（電波利用料財源） 電波資源拡大のための研究開発等　165．1億円の内数 （「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」（平成30～32年度）） 【参考資料　p．17】
■ハードウェア脆弱性への対応 ビッグデータやAIを活用しつつ、ハードウェアに組み込まれるおそれのあるハードウェア脆弱性を検出する技術の研究開発を推進。	・ 平成30年度予算 戦略的情報通信研究開発推進事業（SCOPE）　15．5億円の内数 （平成29年度採択案件「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」（平成29～30年度）） 【参考資料　p．18】
■スマートシティのセキュリティ対策の強化 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推進。	・ 平成30年度予算 国立研究開発法人情報通信研究機構運営費交付金　280．3億円の内数 （「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」（平成28～30年度））
■衛星通信におけるセキュリティ技術の研究開発 安全性を備えた衛星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を実施。	・ 平成30年度予算 衛星通信における量子暗号技術の研究開発　　3．1億円 （平成30～34年度） 【参考資料　p．19】

「民間企業等におけるセキュリティ対策の促進」に係る取組状況

民間企業等におけるセキュリティ対策の促進

「IoTセキュリティ総合対策」における項目	取組状況
■民間企業のセキュリティ投資等の促進 経済産業省と連携して、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する税制優遇措置を検討。	・ 平成30年度税制要望 コネクテッド・インダストリーズ税制の創設（経済産業省と共同要望） 【参考資料　p. 20】
■セキュリティ対策に係る情報開示の促進 任意の情報開示であることを前提としつつ、関係府省と連携しながら、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検討（年度内を目途に結論）。	・ タスクフォースのもとに「情報開示分科会」を設置し、検討（平成29年12月～）。第4回（平成30年4月6日）に報告書（案）を議論し、今後、意見募集を経て、公表予定。 【参考資料　p. 21】
■公衆無線LANのサイバーセキュリティ確保に関する検討 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検討（年度内を目途に結論）。	・ タスクフォースのもとに「公衆無線LANセキュリティ分科会」を設置し、検討（平成29年11月～）。平成30年3月22日、「公衆無線LANセキュリティ分科会報告書」を公表。 【参考資料　p. 21】

「人材育成の強化」に係る取組状況

人材育成の強化

「IoTセキュリティ総合対策」における項目	取組状況
■実践的サイバー防御演習（CYDER）の充実 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た実践的サイバー防御演習を引き続き推進するとともに、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実施。 **■2020年東京大会に向けたサイバー演習の実施** 2020年東京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た事業について、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とともに、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。 **■若手セキュリティ人材の育成の促進** 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。	・ 平成30年度予算　ナショナルサイバートレーニングセンターの構築 15．1億円（平成26～32年度） 【参考資料　p. 22～24】

「国際連携の推進」に係る取組状況

国際連携の推進

「IoTセキュリティ総合対策」における項目	取組状況
■ASEAN各国との連携 実践的サイバー防御演習「CYDER」等の海外展開を通じたセキュリティ人材の育成支援を推進するとともに、各種会議等を通じて、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（平成29年～平成31年の3年間で500人を目標）。	・ 日ASEAN情報セキュリティ政策会議を開催＠シンガポール（平成29年10月10日～11日） ・ ASEAN CYDERを実施＠フィリピン（平成29年10月26日～27日） ・ Cyber SEA Gamesを開催＠タイ（平成29年11月22日） 【参考資料 p. 25】 ・ 日ASEAN情報通信大臣会合＠カンボジア（平成29年12月1日）において、日ASEANサイバーセキュリティキャパシティビルディングセンターをタイで運営することが決定（「日ASEANサイバーセキュリティ協力ハブ」プロジェクト） 【参考資料 p. 26】 ・ ISP向け日ASEAN情報セキュリティワークショップを開催＠東京（平成30年2月1日～2日） 【参考資料 p. 27】
■国際的なISAC間連携 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（Automated Indicator Sharing）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を促進。	・ 国際連携ワークショップを開催＠東京（平成29年11月6日～7日） 【参考資料 p. 28】
■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 様々なチャネルを通じて進められている、サイバー空間における国際ルール等に関する議論へ積極的に参画。	・ G7情報通信・産業大臣会合開催＠イタリア（平成29年9月25日～26日） 【参考資料 p. 29】

（参考資料）

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。

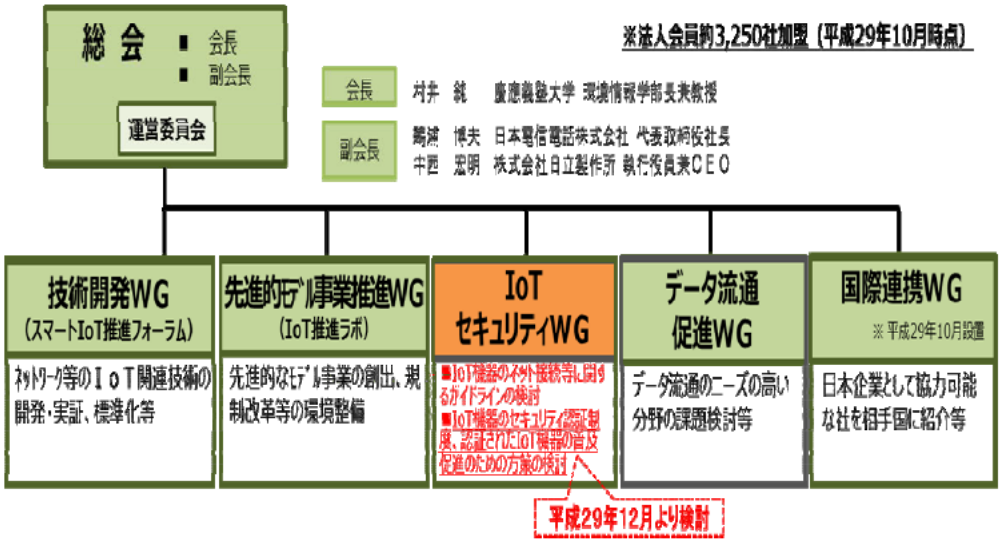
このことを受けて、IoT推進コンソーシアム IoTセキュリティワーキンググループにおいて、「IoTセキュリティガイドラインver1.0」の普及啓発やIoT機器のセキュリティ確保策等について検討を行う。

○ スケジュール：

平成29年12月11日（月）に今年度第１回会合を開催。以降、随時開催予定。

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】

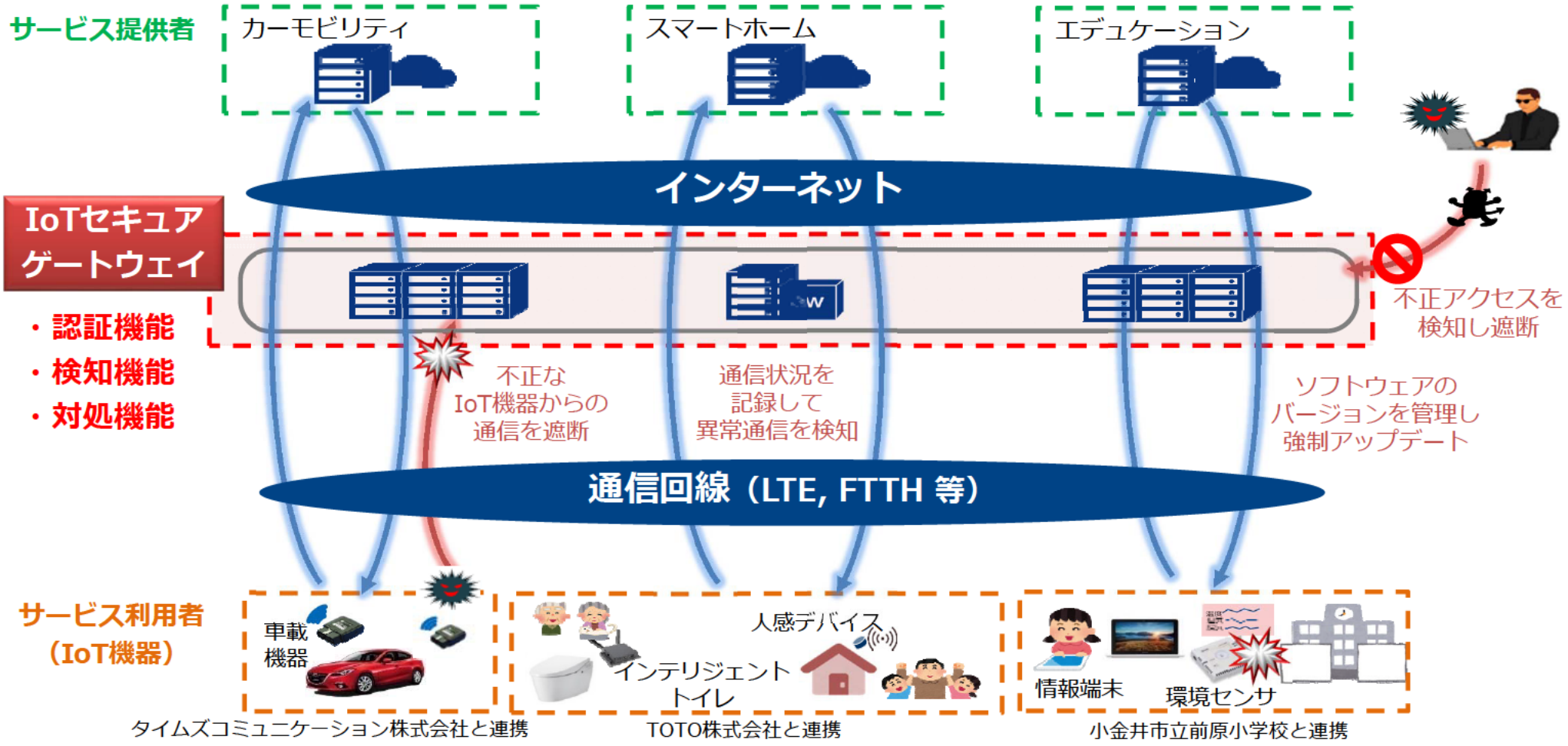
	有村　浩一	一般社団法人JPCERTコーディネーションセンター　常務理事
	出雲　秀一	在日米国商工会議所　サイバーセキュリティタスクフォース共同委員長
	鵜飼　裕司	株式会社FFRI　代表取締役社長
	大矢　隆一郎	一般社団法人 ビジネス機械・情報システム産業協会　委員
	小川　武史	青山学院大学理工学部機械創造工学科　教授
	荻野　司	一般社団法人 重要生活機器連携セキュリティ協議会　代表理事
	金子　健一	一般社団法人日本電機工業会　家電部　技術課
	川上　景一	一般社団法人電子情報技術産業協会　常務理事
	小山　覚	一般社団法人　日本経済団体連合会　情報通信委員会 企画部会長代行・サイ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

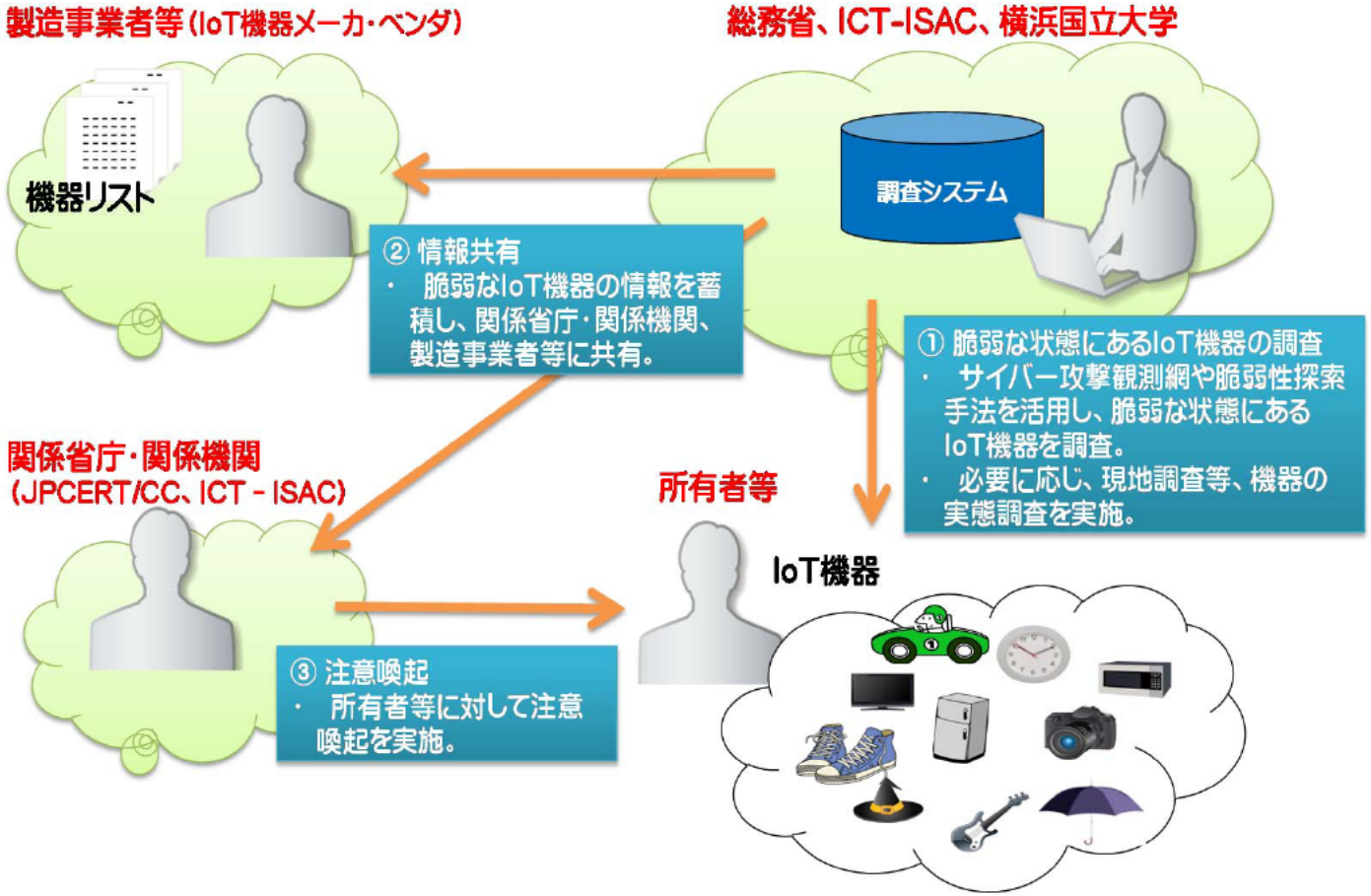
実施主体：NTTコミュニケーションズ株式会社、平成29年12月より実証実験を開始（平成28年度補正（2.5億円））



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）

○ 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29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29年4月12日公表）

IoT機器に関する脆弱性調査

○ 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

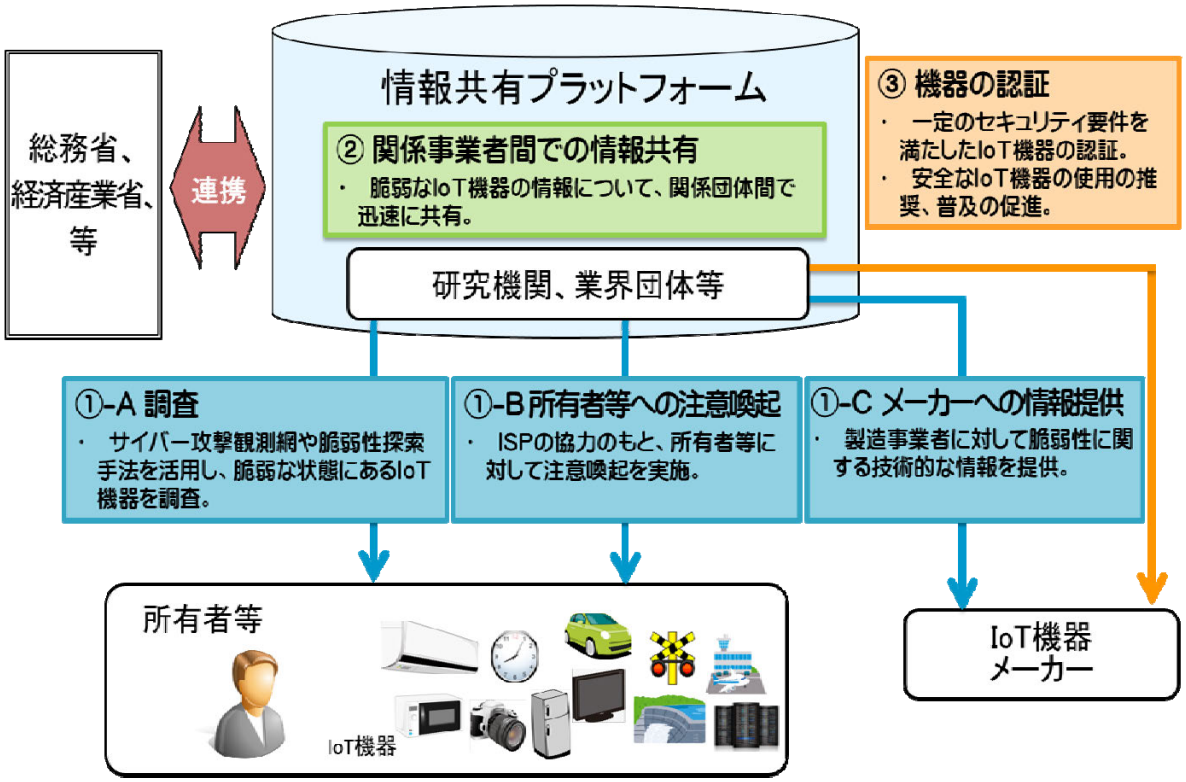
広域ネットワーク探索手法、サイバー攻撃観測網等を活用し、インターネットに接続されているIoT機器の調査を実施。脆弱性を持つIoT機器が発見された場合は、インターネットサービスプロバイダ(ISP)等の協力のもと、当該機器の所有者・運用者・利用者へ注意喚起を行う。

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）

電気通信事業法の一部改正案について

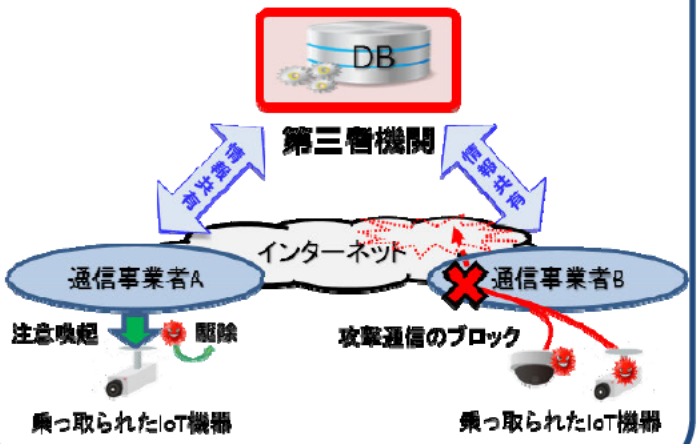
○　**IoT化に伴うサイバー攻撃の深刻化**やネットワークの**IP網への移行**に対応するため、**電気通信事業法の改正**を行うもの。

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

カード決済端末

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。

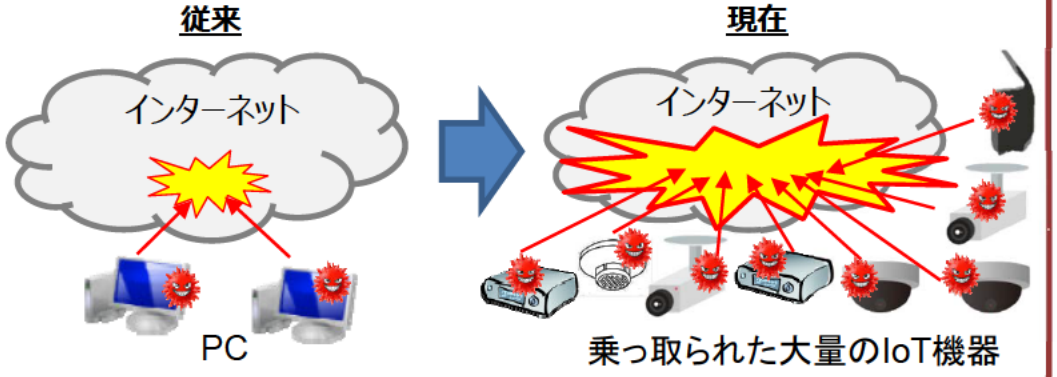
※悪意あるソフトウェアの総称であり、コンピュータに感染することによって、サイバー攻撃などの遠隔操作を自動的に実行するプログラムのこと。

現　状

インターネットの障害の深刻化

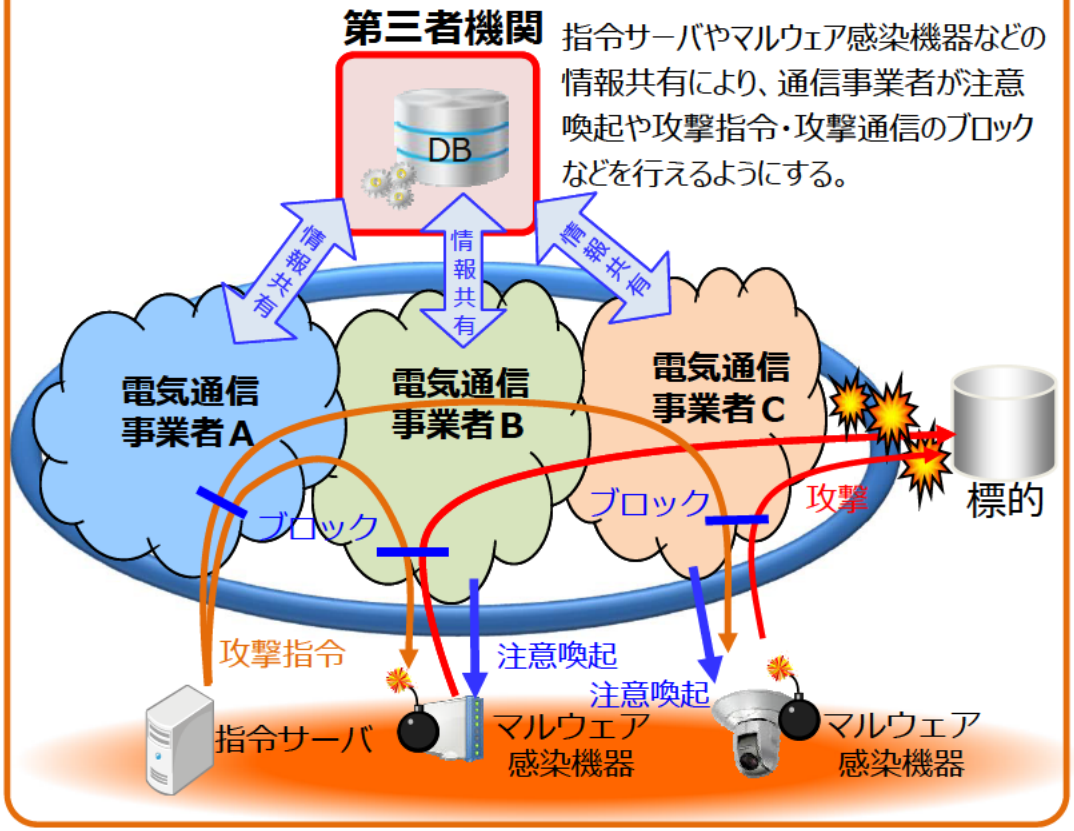
- サイバー攻撃によるインターネットの障害が発生し、国民生活や社会経済活動に影響
- 増加するＩｏＴ機器※を悪用したサイバー攻撃によりインターネットに重大な障害が発生
- 2020年の東京オリンピック・パラリンピック競技大会に際して、日本に対する大規模なサイバー攻撃の発生の懸念

※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



国立研究開発法人情報通信研究機構法の一部改正案について

○　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）

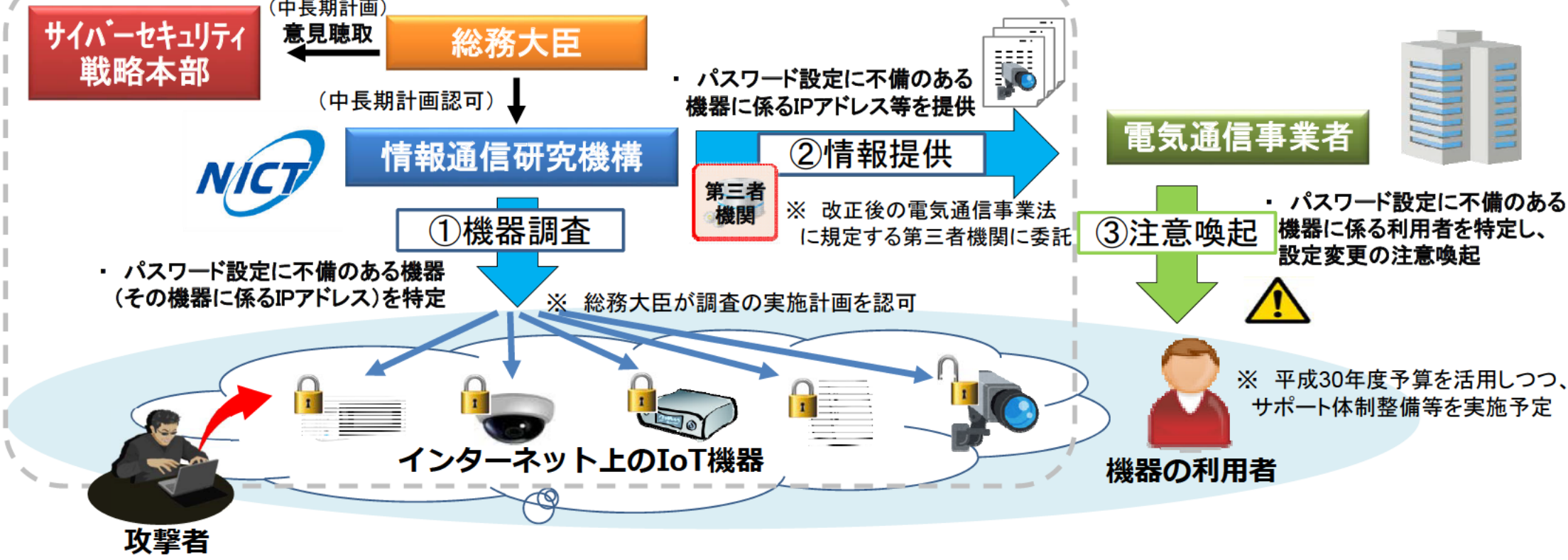
対策の必要性

・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）。

情報通信研究機構法の改正



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

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。

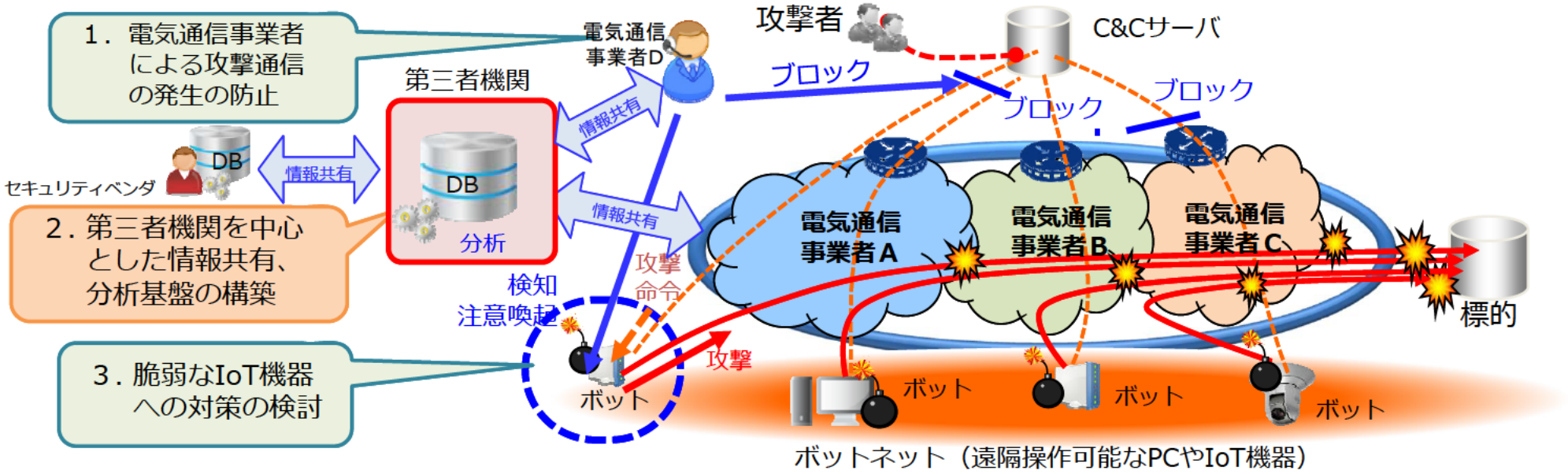
※ 事業者のネットワークに接続される端末設備の技術基準には、現時点ではサイバー攻撃等によるインターネットの障害に関する規定はない。

→ 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。



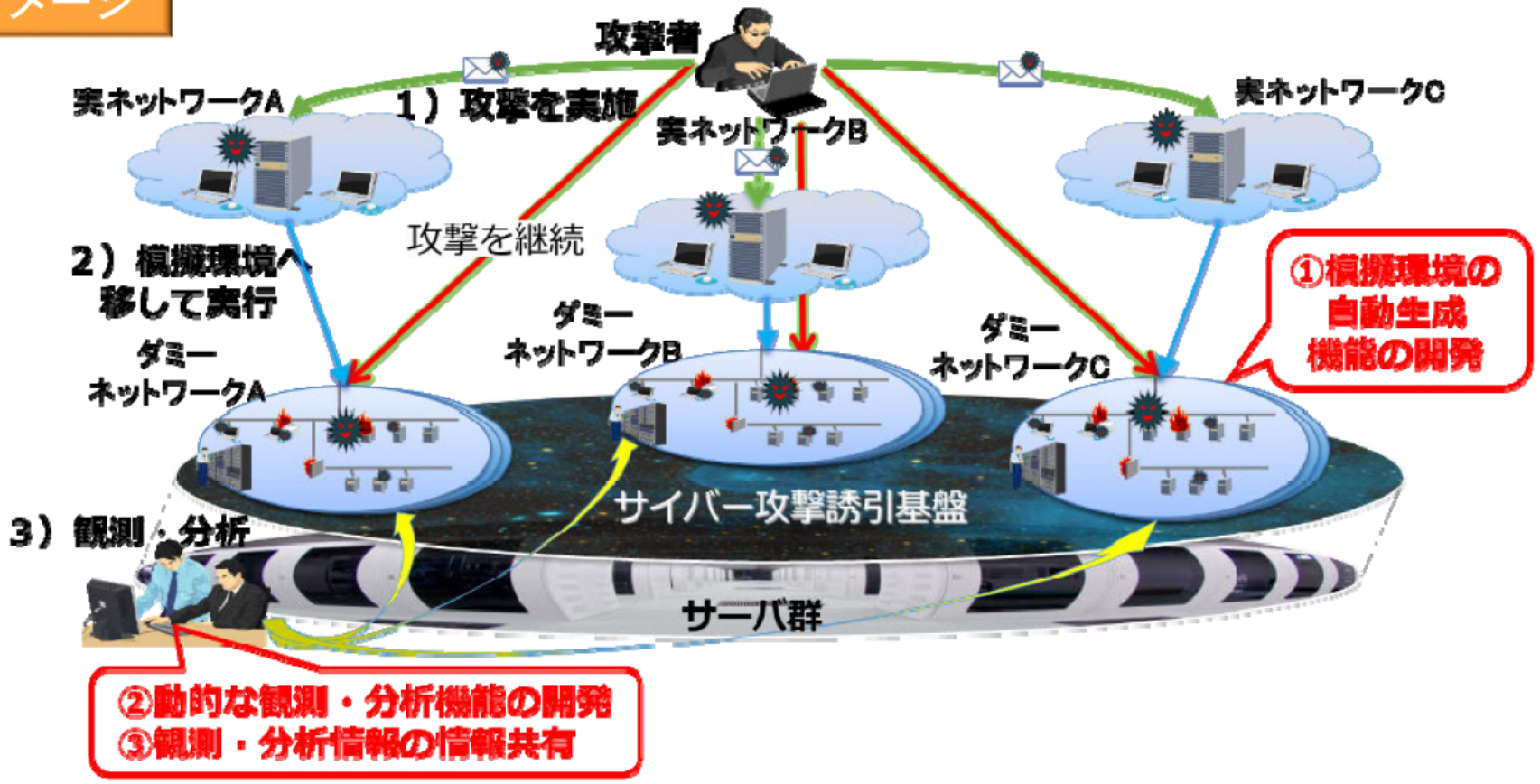
サイバー攻撃誘引基盤

○　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。

【平成29年度補正予算：10億円、平成30年度予算：NICT交付金の内数】

システムイメージ



広域ネットワークスキャンの軽量化

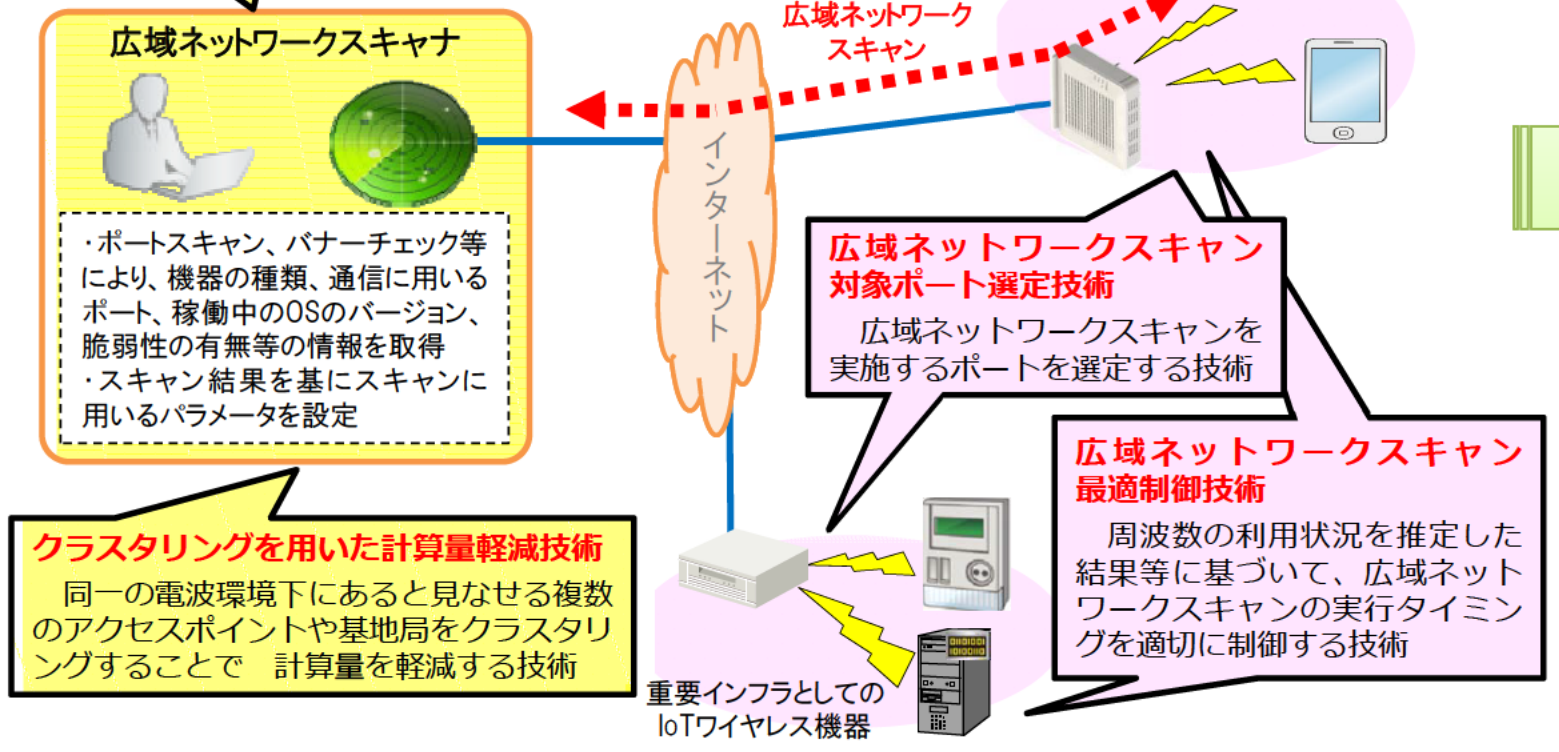
○ 近年、IoT機器を狙ったサイバー攻撃は増加傾向にあり、脆弱なIoT機器への対策は喫緊の課題。

○ 今後、無線通信を利用するIoT機器の割合は増加するものと見込まれているため、「IoTワイヤレス高効率広域ネットワークスキャン技術」の研究開発を実施。

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

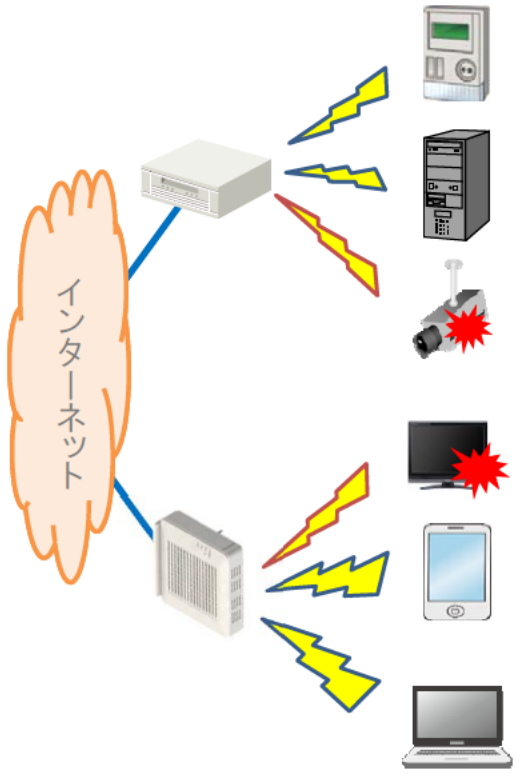
広域ネットワークスキャン遅延原因等推定技術
広域ネットワークスキャンの成否や遅延に関する原因を高精度に推定する技術



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見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

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

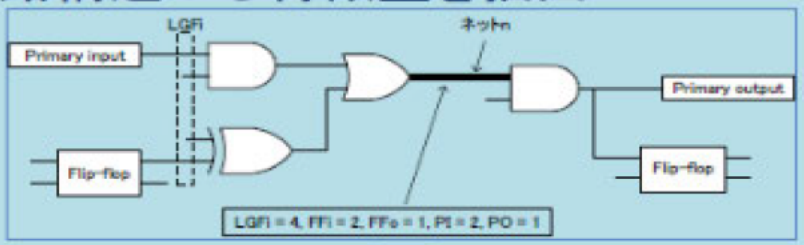
【平成29年度採択案件 ：早稲田大学基幹理工学部　戸川望教授】

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・・・

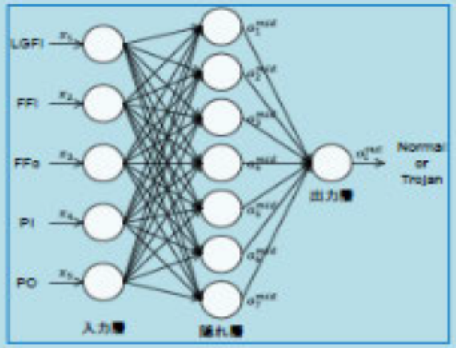
2013年10月（BBC）
ロシアの公営放送局（Rossiya 24）によると、サイバー犯罪者が、アイロンや湯沸かし器の中に、スパムアタックを行うチップを埋め込んでいることが判明。
このチップは、勝手にWi-Fiネットワークに繋がってウイルスをばらまく電子回路が組み込まれていた。

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（事業期間：平成30年～平成34年）

事業の内容

背景と課題

○衛星通信ネットワークを盗聴、改ざん、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。

条件（対象者、対象行為、補助率等）

国 → 委託 → 民間企業等

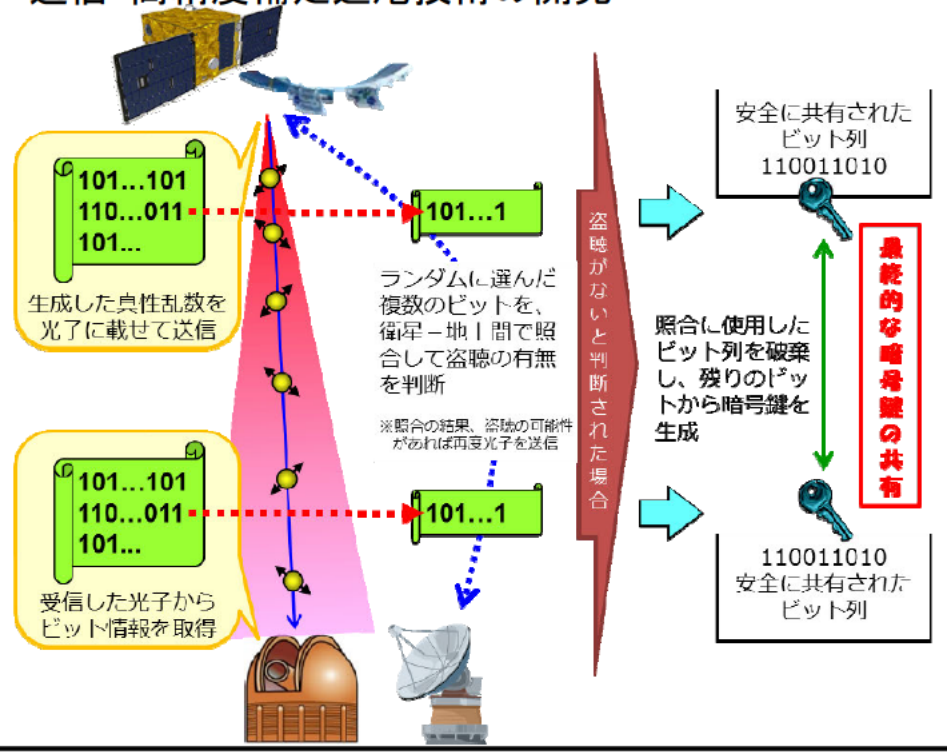
事業イメージ

衛星通信における量子暗号技術の研究開発

◆ 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鍵配送を可能とすることにより、大陸間のような量子暗号網の広域化を実現。

① 小型衛星にも搭載可能な量子暗号通信技術を開発
② 空間光通信用の光地上局の高感度受信技術及び空間光通信・高精度補足追尾技術の開発



コネクテッド・インダストリーズ税制の創設

○　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。

公衆無線LANセキュリティ分科会及び情報開示分科会の開催

公衆無線LANセキュリティ分科会

○ 概要

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に向けて、観光や防災の観点から、その普及が進んでいる。しかし、公衆無線LANサービスの中には、セキュリティへの対策が十分でないものも多く、公衆無線LANサービスを踏み台にした攻撃や情報漏洩等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におけるセキュリティ上の課題を整理し、必要な対策について、検討を行う。

○ 主な検討事項

・公衆無線LANのセキュリティ対策について
・セキュリティに配慮した公衆無線LANサービスの普及について

○ スケジュール

平成29年11月24日～平成30年３月16日に計５回開催。平成30年３月22日に報告書を公表。

情報開示分科会

○ 概要

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適切に評価される仕組みを構築していくことが求められている。

このため、あくまで任意の取組であることを前提としつつ、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う。

○ 主な検討事項

・情報開示する具体的な項目やその方法
・情報開示の普及の方策

○ スケジュール

平成29年12月～平成30年４月６日に計４回開催。第４回（平成30年４月６日）における議論を踏まえ、今後、報告書（案）について意見募集を実施。第５回（５月中下旬開催予定）において、報告書（案）に対する意見募集の結果を報告するとともに、報告書をとりまとめる予定。

実践的サイバー防御演習（CYDER）の概要

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

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）

○　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**。

○　サイバーコロッセオは、**国立研究開発法人情報通信研究機構（NICT）が実施主体となり**、NICTが有する大規模演習環境及び長年のサイバーセキュリティ研究による知見を活かした、**実際の機器やソフトウエアの操作を伴う「実践的なトレーニング」を実施**。

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

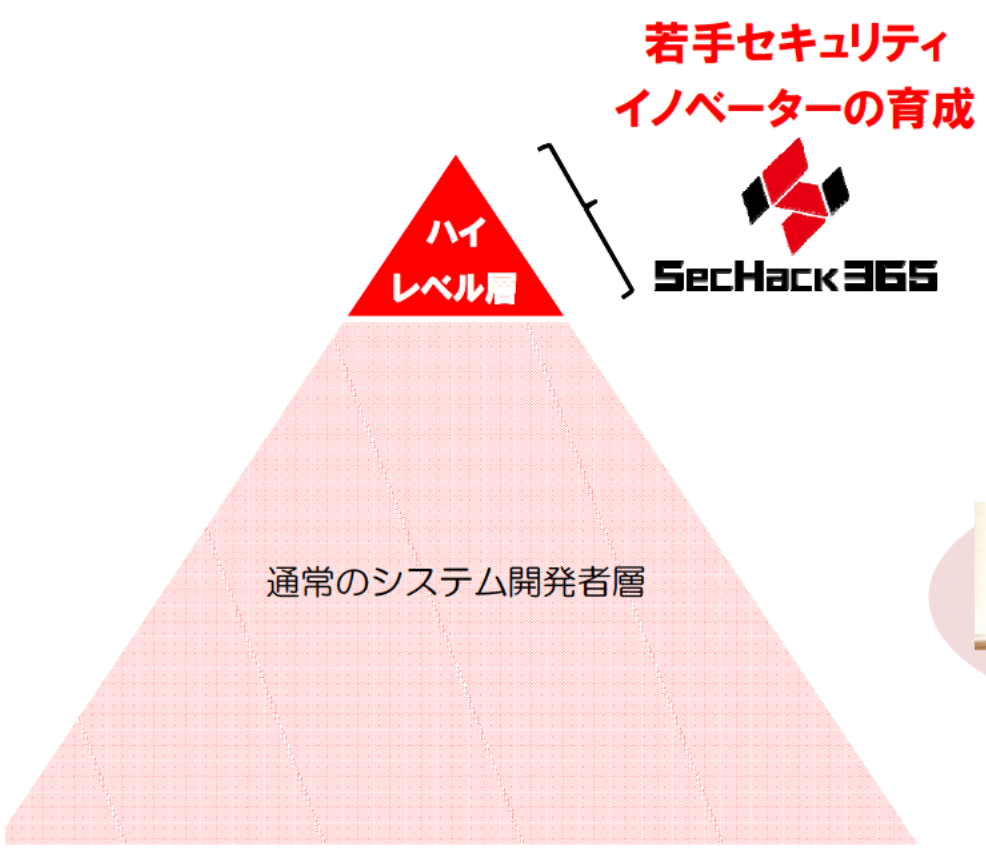
若手セキュリティイノベータの育成（SecHack365）

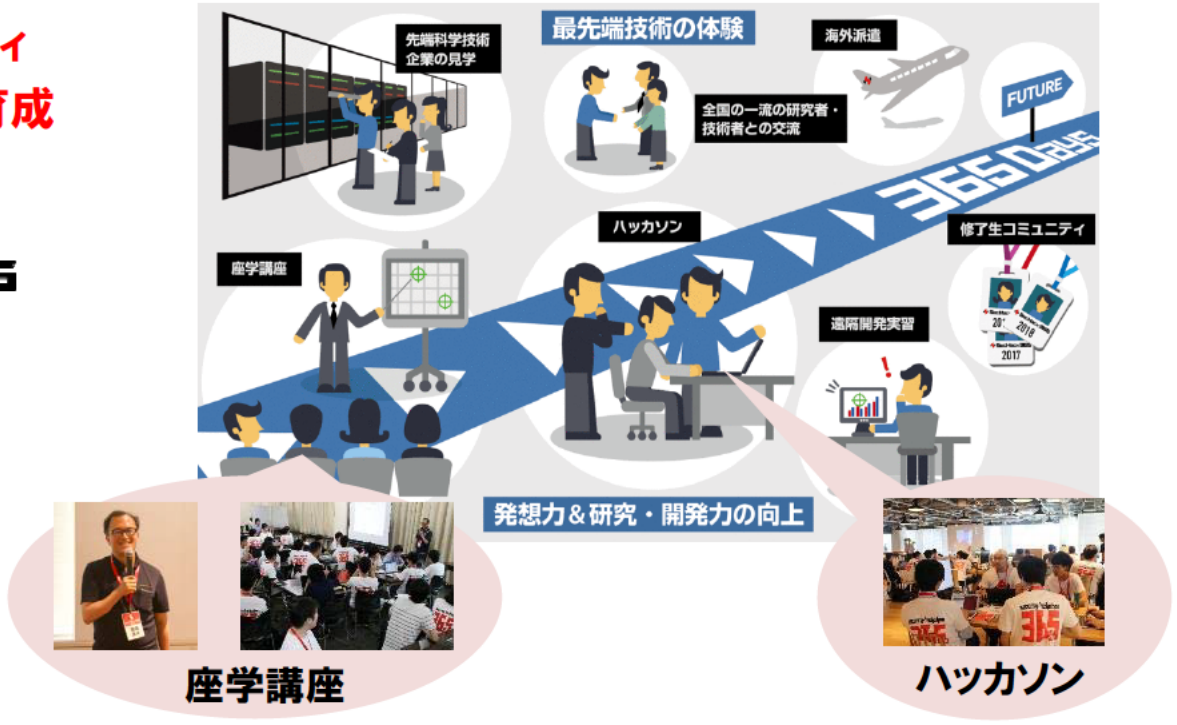
○ **未来のサイバーセキュリティ研究者・起業家の創出に向けて**、NICTの持つサイバーセキュリティの研究資産を活用し、**若年層のICT人材を対象に**実際のサイバー攻撃関連データに基づいた**セキュリティ技術の研究・開発を、第一線で活躍する研究者・技術者が1年かけて継続的かつ本格的に指導**。

○ 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年度は受講者として47名を選定。）

○ 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（2017年11月） 概要

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形式の競技を実施しました。
- 優勝チームを2018年2月に日本で行われるSECCON決勝大会に招待しました。

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です。
- 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、チームメンバー同士の協力も重要となります。

開催概要

- 日時　　：2017年11月22日(水)
- 開催場所：Swissotel Le Concorde Bangkok, Thailand
- 参加者　：30歳以下の学生、および技術者
  ASEAN10か国、計40名

「日ASEANサイバーセキュリティ協力ハブ」プロジェクトの概要

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。
正式名称は、”ASEAN-Japan Cybersecurity Capacity Building Centre” project。

○ 実施時期

STEP1（2017年4月～ ）、STEP2（2018年前半～（4年間を予定））

○ 実施体制

- STEP1で実施されたF/Sの結果を踏まえ、2017年12月の日ASEAN情報通信大臣会合にて、タイETDA（電子取引開発機構）がSTEP2を実施することで合意。
- STEP2は、PSC（Project Steering Committee）を設置し、実施する予定。以降、4月からのSTEP2開始に向け、タイ側と継続的に協議を実施。PSCメンバーは、MDES（デジタル経済社会省）、ETDA、ASEAN事務局、外務省、総務省を予定。

○ 主な活動内容（予定）

1. 演習（CYDER演習）※ CYDER：CYber Defense Exercise with Recurrence

最新のサイバー攻撃に基づく政府機関・重要インフラ事業者におけるLAN管理者向けの実践的なサイバー防御演習の実施（年6回程度）

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大会の開催

3. その他

重要インフラ防護セミナー／ワークショップの開催等

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

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

〇日本(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。

〇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。

〇前回に引き続き、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

〇各国の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。

〇ASEAN各国（主にISP事業者）との人的ネットワークの維持・強化。

〇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。

〇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

- 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。

G7 情報通信・産業大臣会合 結果概要

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、
米国：クラティオス　大統領副補佐官・副CTO、
英国：ハンコック　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、
日本：奥野総務副大臣、平木経産大臣政務官、
カナダ：ベインズ　イノベーション・科学・経済発展大臣、
フランス：マジュビ　デジタル担当大臣、
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。