くらしの中に
総務省
MIC Ministry of Internal Affairs and Communications

総務省におけるサイバーセキュリティ政策

令 和 ３ 年 ２ 月 ２５ 日

総務省サイバーセキュリティ統括官付参事官
海野　敦史　(Atsushi Umino)

１．最近のセキュリティ動向

２．政府全体の取組

３．「IoT・5Gセキュリティ総合対策2020」

（１）COVID-19への対応を受けたセキュリティ対策の推進

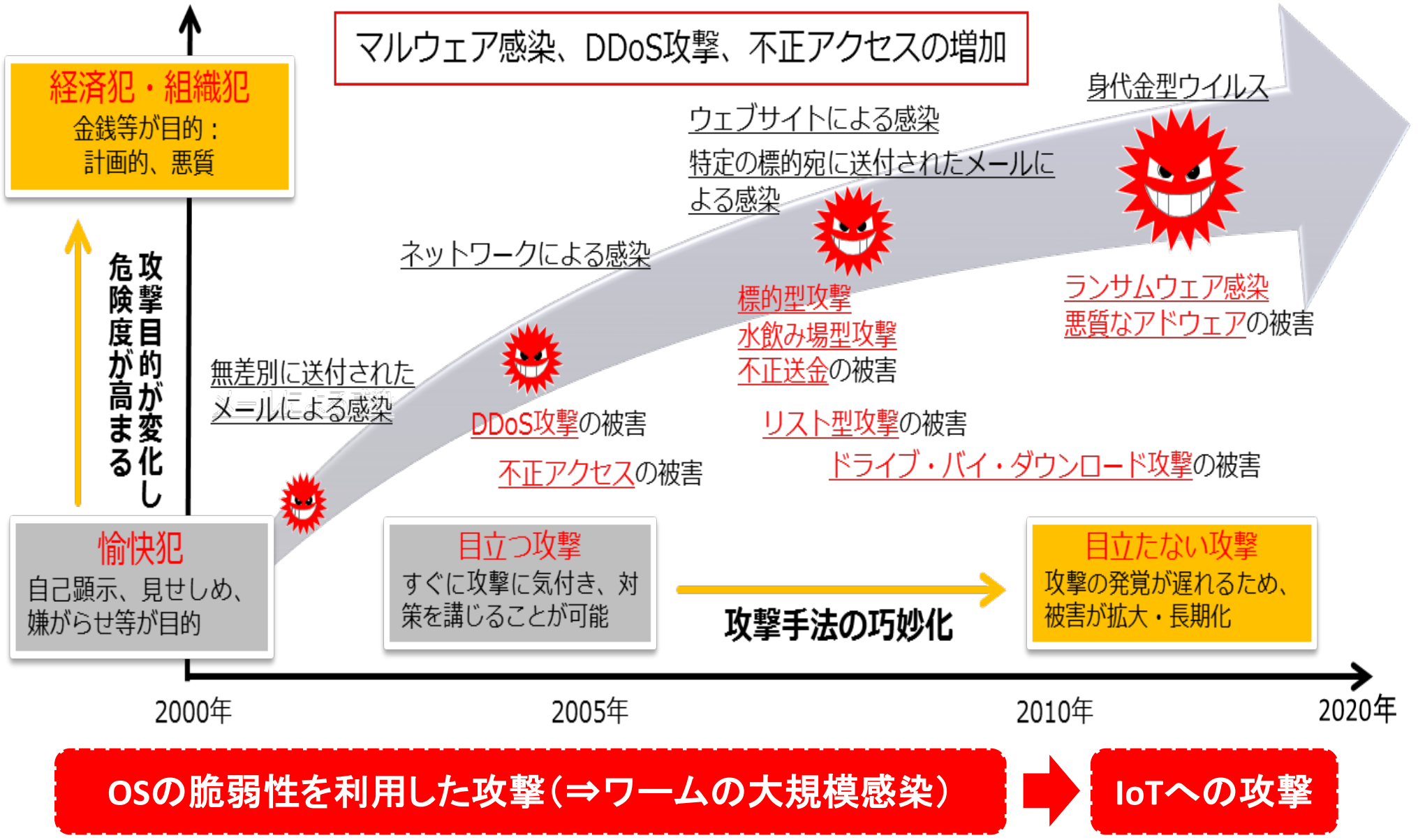
（２）5Gの本格開始に伴うセキュリティ対策の強化

（３）サイバー攻撃に対する電気通信事業者のアクティブな対策の実現

（４）我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

（５）その他のトピックス（暗号、スマートシティ、国際連携）

サイバーセキュリティ上の脅威の増大



昨今のサイバー攻撃の事例

出典：各種公開資料等より総務省作成

国内事例

2015年６月	日本年金機構の職員が利用する端末がマルウェアに感染し、年金加入者の情報約125万件が流出（標的型攻撃）
2015年11月	東京五輪組織委員会のホームページにサイバー攻撃、約12時間閲覧不能（DDoS攻撃）
2016年６月	i.JTB（JTBのグループ会社）の職員が利用する端末が、マルウェアに感染し、パスポート番号を含む個人情報が流出した可能性（標的型攻撃）
2017年５月	国内（行政、民間企業、病院等）において、WannaCryによる被害が確認。企業内のシステム停止などの障害が発生（ランサムウェア）
2018年１月	コインチェック社が保有していた暗号資産（仮想通貨）が外部へ送信され、顧客資産が流出（不正アクセス）
2020年	三菱電機やNEC等において防衛関連情報を含む情報が外部へ流出した可能性が判明（不正アクセス）

海外事例

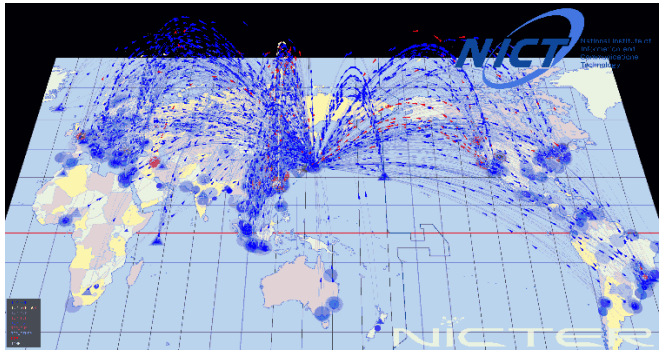
2015年６月	米国の人事管理局（OPM）が不正にアクセスされ、政府職員の個人情報が流出（不正アクセス）
2015年12月	ウクライナの電力会社のシステムがマルウェアに感染し、停電が発生（標的型攻撃）
2016年10月	米国のDyn社のDNSサーバが大規模なDDoS攻撃を受け、同社のDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生（DDoS攻撃）
2017年５月	世界各国（アメリカ、イギリス、中国、ロシア等）でWannaCryの感染被害が発生。行政、民間企業、医療等の多くの組織に影響（ランサムウェア）
2017年10月	米Yahoo社で約30億件の個人情報が流出していたことが判明（不正アクセス）
2019年９月	エクアドルで国民ほぼ全員を含む約2000万人分の個人情報が海外に流出（不正アクセス）
2020年12月	ソフトウェア更新を悪用した複数の米政府機関への大規模サイバー攻撃が判明（不正アクセス）

最近では、新型コロナウィルスの感染拡大に乗じたサイバー攻撃の事例を多数確認

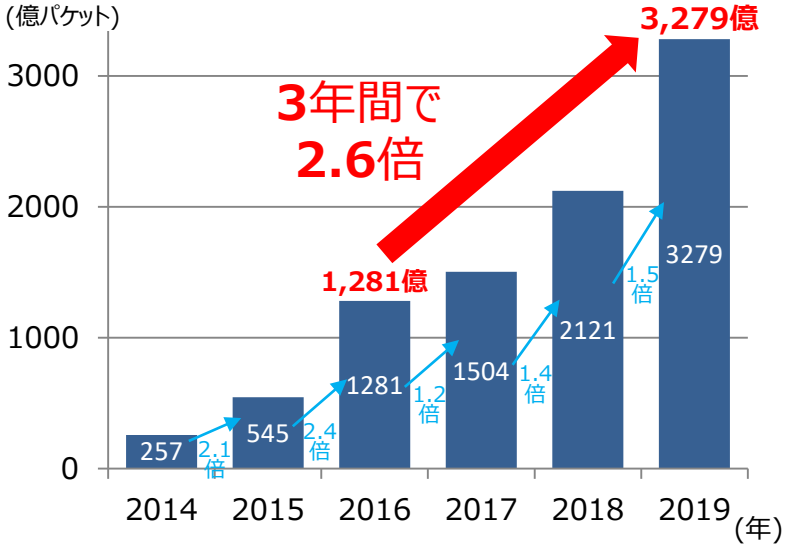
IoT機器を狙った攻撃の急増（NICTERによる観測）

○　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。

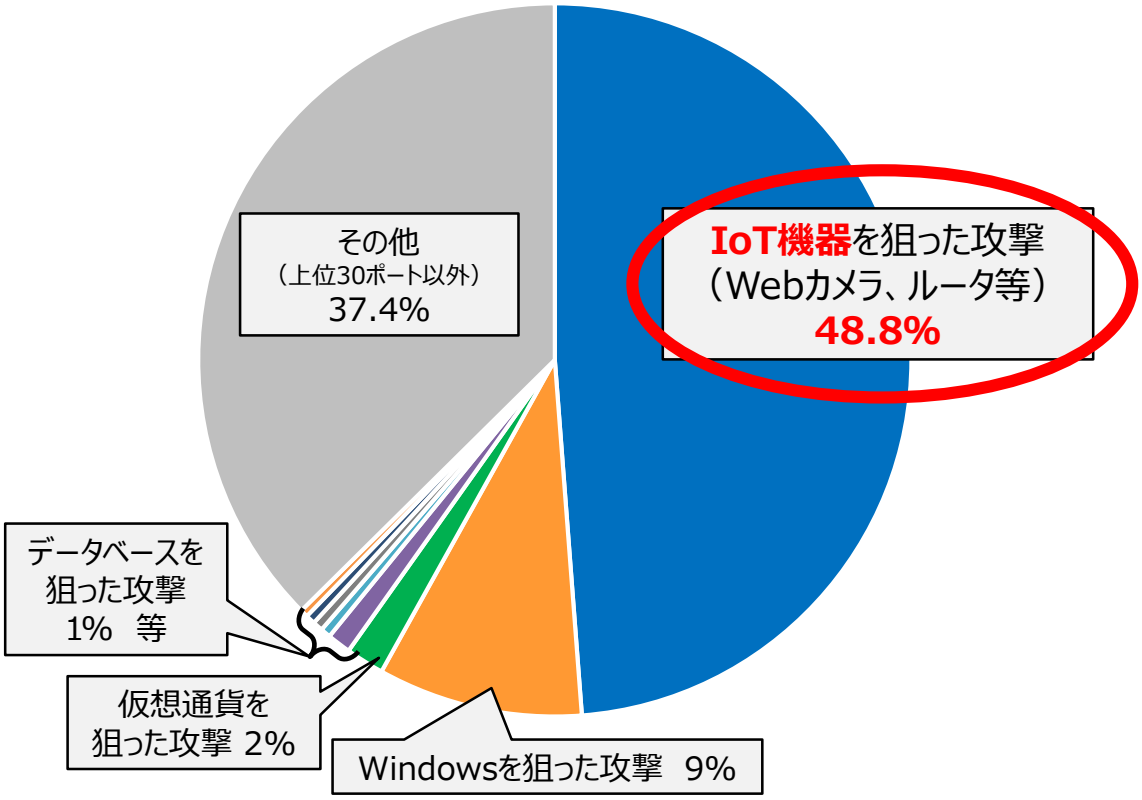
NICTERにより観測されるサイバー攻撃の様子



NICTERで１年間に観測されたサイバー攻撃関連パケット



約半数がIoT機器を狙った攻撃



※　NICTERで2019年に観測されたパケットのうち、調査目的パケット以外についてサービス種類（ポート番号）ごとに上位30ポートまでを分析したもの。

※　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。

IoT機器がサイバー攻撃の対象として狙われやすい理由

➢ IoTの進展が企業活動や製品・サービスのイノベーションを加速する一方で、IoT特有の性質と想定されるリスクをもつことから、これらの性質とリスクを踏まえたセキュリティ対策を行うことが必要。

1）脅威の影響範囲・影響度合いが大きい

攻撃を受けると、ネットワークを介してシステム・サービス全体へその影響が波及（自動車・医療等における致命的影響等も存在）

2）IoT機器のライフサイクルが長い

工場の制御機器等をはじめ10年以上の長期にわたって使用され、構築・接続時に適用したセキュリティ対策が危殆化

3）IoT機器に対する監視が行き届きにくい

画面がなく問題の発生がわかりづらい上に、人目が行き届きにくく勝手なネットワーク接続をされかねない

4）IoT機器側とネットワーク側の環境や特性の相互理解が不十分である

IoT機器と接続ネットワークの双方でセキュリティ要件の整合をとらなければ、必要な安全性等をみたせない

5）IoT機器の機能・性能が限られている

適切な暗号等のセキュリティ対策を適用できない場合が存在

6）開発者が想定していなかった接続が行われる可能性がある

これまで外部につながっていなかったモノがネットワークに接続され、当初想定していなかった影響が発生

（出展：IoTセキュリティガイドラインver1.0　平成28年7月　IoT推進コンソーシアム・総務省・経済産業省）

１．最近のセキュリティ動向

２．政府全体の取組

３．「IoT・5Gセキュリティ総合対策2020」

（１）COVID-19への対応を受けたセキュリティ対策の推進

（２）5Gの本格開始に伴うセキュリティ対策の強化

（３）サイバー攻撃に対する電気通信事業者のアクティブな対策の実現

（４）我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

（５）その他のトピックス（暗号、スマートシティ、国際連携）

「サイバーセキュリティ基本法」の概要

（平成26年11月、第187回国会（臨時会）において成立。平成28年、平成30年改正後）

第Ⅰ章．総則

■**目的（第1条）**

■**定義（第2条）**

⇒「サイバーセキュリティ」について定義

■**基本理念（第3条）**

⇒ サイバーセキュリティに関する施策の推進にあたっての基本理念について次を規定

① 情報の自由な流通の確保を基本として、官民の連携により積極的に対応

② 国民１人１人の認識を深め、自発的な対応の促進等、強靱な体制の構築

③ 高度情報通信ネットワークの整備及びITの活用による活力ある経済社会の構築

④ 国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施

⑤ IT基本法の基本理念に配慮して実施

⑥ 国民の権利を不当に侵害しないよう留意

■**関係者の責務等（第4条～第9条）**

⇒ 国、地方公共団体、重要社会基盤事業者（重要インフラ事業者）、サイバー関連事業者、教育研究機関等の責務等について規定

■**法制上の措置等（第10条）**

■**行政組織の整備等（第11条）**

第Ⅱ章．サイバーセキュリティ戦略

■**サイバーセキュリティ戦略（第12条）**

⇒ 次の事項を規定

① サイバーセキュリティに関する施策の基本的な方針

② 国の行政機関等におけるサイバーセキュリティの確保

③ 重要インフラ事業者等におけるサイバーセキュリティの確保の促進

④ その他、必要な事項

⇒ その他、総理は、本戦略の案につき閣議決定を求めなければならないこと等を規定

第Ⅲ章．基本的施策

■**国の行政機関等におけるサイバーセキュリティの確保（第13条）**

■**重要インフラ事業者等におけるサイバーセキュリティの確保の促進（第14条）**

■**民間事業者及び教育研究機関等の自発的な取組の促進（第15条）**

■**多様な主体の連携等（第16条）**

■**サイバーセキュリティ協議会を組織（第17条）**

■**犯罪の取締り及び被害の拡大の防止（第18条）**

■**我が国の安全に重大な影響を及ぼすおそれのある事象への対応（第19条）**

■**産業の振興及び国際競争力の強化　（第20条）**

■**研究開発の推進等（第21条）**

■**人材の確保等（第22条）**

第Ⅲ章．基本的施策（つづき）

■**教育及び学習の振興、普及啓発等（第23条）**

■**国際協力の推進等（第24条）**

第Ⅳ章．サイバーセキュリティ戦略本部

■**設置（第25条）**

■**所掌事務等（第26条）**

⇒サイバーセキュリティ戦略案の作成、国の行政機関、独立行政法人・指定法人に対する監査・原因究明調査等の実施

■**組織等（第27条～第30条）**

⇒内閣官房長官を本部長として、副本部長（国務大臣）、国家公安委員会委員長、総務大臣、外務大臣、経済産業大臣、防衛大臣、総理が指定する国務大臣、有識者本部員で構成

■**事務の委託（第31条）**

⇒独立行政法人・指定法人に対する監査・原因究明調査の事務の一部をIPAその他政令で定める法人に委託（秘密保持義務を規定）

■**資料提供等（第32条～第37条）**

第Ⅴ章．罰則

■**罰則（第38条）**

⇒戦略本部からの事務の委託を受けた者が秘密保持義務に反した場合。1年以下の懲役又は50万円以下の罰金

我が国におけるサイバーセキュリティ推進体制

平成26年11月に成立した「サイバーセキュリティ基本法」に基づき、平成27年1月、内閣にサイバーセキュリティ戦略本部が設置され、同年9月、日本年金機構の年金情報流出の事案も踏まえた新たな「サイバーセキュリティ戦略」を閣議決定。同本部を司令塔として、事務局を担う内閣サイバーセキュリティセンター（NISC）の調整の下、関係省庁が連携した政府横断的サイバーセキュリティ推進体制を整備し、本戦略を推進。

内閣

内閣総理大臣

高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）

高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進

緊密連携

サイバーセキュリティ戦略本部（2015.1.9 ｻｲﾊﾞｰｾｷｭﾘﾃｨ基本法により設置）

本部長　内閣官房長官
副本部長　サイバーセキュリティ戦略本部に関する事務を担当する国務大臣
本部員　国家公安委員会委員長
総務大臣
外務大臣
経済産業大臣
防衛大臣
情報通信技術（ＩＴ）政策担当大臣
東京オリンピック競技大会・パラリンピック競技大会担当大臣
有識者（８名；10名以下）

閣僚が参画

遠藤　信博	日本電気株式会社代表取締役会長
小野寺　正	ＫＤＤＩ株式会社代表取締役相談役
後藤　厚宏	情報セキュリティ大学院大学学長
中谷　和弘	東京大学大学院法学政治学研究科教授
野原佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
前田　雅英	東京都立大学法科大学院兼任教授
宮澤　英一	株式会社デジタルハーツホールディングス取締役会長
村井　純	慶應義塾大学環境情報学部教授　大学院政策・メディア研究科委員長

（令和２年４月１日現在）

- 重要インフラ専門調査会
- 研究開発戦略専門調査会
- 普及啓発・人材育成専門調査会
- ｻｲﾊﾞｰｾｷｭﾘﾃｨ対策推進会議（CISO等連絡会議）

国家安全保障会議（NSC）

我が国の安全保障に関する重要事項を審議

緊密連携

連携

サイバーセキュリティ協議会

官民の多様な主体が相互に連携した、より早期の段階での、サイバーセキュリティの確保に資する情報の迅速な共有等

内閣官房　内閣サイバーセキュリティセンター（2015.1.9 内閣官房組織令により設置）

（事務局）

内閣サイバーセキュリティセンター長
（内閣官房副長官補(事態対処・危機管理)が兼務）
副センター長（内閣審議官）
上席サイバーセキュリティ分析官
サイバーセキュリティ参与

- 政府機関・情報セキュリティ横断監視・即応調整チーム（ＧＳＯＣ）
- 情報セキュリティ緊急支援チーム（CYMAT）

協力

協力

＜重要インフラ所管省庁＞

金融庁（金融機関）
総務省（地方公共団体、情報通信）
厚生労働省（医療、水道）
経済産業省（電力、ガス、化学、クレジット、石油）
国土交通省（鉄道、航空、物流、空港）

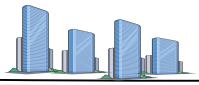
＜その他関係省庁＞

文部科学省（セキュリティ教育）等

閣僚本部員５省庁

- 警察庁（サイバー犯罪・攻撃の取締り）
- 総務省（通信・ネットワーク政策）
- 外務省（外交・安全保障）
- 経済産業省（情報政策）
- 防衛省（国の防衛）


重要インフラ事業者等


政府機関（各府省庁）

企業


個人

「サイバーセキュリティ戦略」（平成30年7月27日 閣議決定）の全体概要

中長期的

戦略期間（2018～2021年（3年間））

1 策定の趣旨・背景

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

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

2 サイバー空間に係る認識

2．1． サイバー空間がもたらす恩恵

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

※：Internet of Thingsの略

2．2． サイバー空間における脅威の深刻化

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

3 本戦略の目的

3．1． **基本的な立場の堅持**

（1）基本法の目的（2）基本的な理念（「自由、公正かつ安全なサイバー空間」）（3）基本原則（情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携）

3．2． 目指すサイバーセキュリティの基本的な在り方

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

4 目的達成のための施策

経済社会の活力の向上及び持続的発展

1．新たな価値創出を支えるサイバーセキュリティの推進

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

2．多様なつながりから価値を生み出すサプライチェーンの実現

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

3．安全なIoTシステムの構築

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

等

国民が安全で安心して暮らせる社会の実現

1．国民・社会を守るための取組

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

2．官民一体となった重要インフラの防護

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

3．政府機関等におけるセキュリティ強化・充実

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

4．大学等における安全・安心な教育・研究環境の確保

＜施策例＞・**大学等**の多様性を踏まえた対策の推進

5．2020年東京大会とその後を見据えた取組

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

6．従来の枠を超えた情報共有・連携体制の構築

＜施策例＞・**多様な主体の情報共有・連携の推進**

7．大規模サイバー攻撃事態等への対処態勢の強化

＜施策例＞・**サイバー空間と実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への寄与

1．自由、公正かつ安全なサイバー空間の堅持

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

2．我が国の防御力・抑止力・状況把握力の強化

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

3．国際協力・連携

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

等

横断的施策

人材育成・確保 ＜施策例＞**戦略マネジメント層の育成・定着**、実務者層・技術者層の育成（**高度人材**含む）、人材育成基盤の整備、**政府人材**の確保・育成の強化、国際連携の推進

研究開発の推進 ＜施策例＞実践的な研究開発の推進（**検知・防御等の能力向上、不正プログラム等の技術的検証**を行うための体制整備）、**AI等**中長期的な技術・社会の進化を視野に入れた対応

全員参加による協働 ＜施策例＞サイバーセキュリティの普及啓発に向けた**アクションプランの策定、国民への情報発信**（サイバーセキュリティ月間の充実等）、サイバーセキュリティ教育の推進

5 推進体制

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

１．最近のセキュリティ動向

２．政府全体の取組

３．「IoT・5Gセキュリティ総合対策2020」

（１）COVID-19への対応を受けたセキュリティ対策の推進

（２）5Gの本格開始に伴うセキュリティ対策の強化

（３）サイバー攻撃に対する電気通信事業者のアクティブな対策の実現

（４）我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

（５）その他のトピックス（暗号、スマートシティ、国際連携）

IoT・5Gセキュリティ総合対策2020（2020年7月公表） 全体概要

■ サイバーセキュリティタスクフォースにおけるこれまでの短期的・中長期的な観点の議論、「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項 [緊急提言]」※1の内容、さらには新型コロナウイルス感染症への対応等を踏まえつつ、「IoT・5Gセキュリティ総合対策」※2について、必要な改定を行い、「IoT・5Gセキュリティ総合対策2020」として2020年７月に公表。 https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00126.html

● 改定に当たっての主要な政策課題

1 COVID-19 への対応を受けたセキュリティ対策の推進

① テレワークシステムのセキュリティに関するチェックリストの作成や相談対応体制の拡充など、特に中小企業を念頭においたテレワークセキュリティの確保のための実践的な対策を推進する。

② ネット上で業務・手続を完結可能とするため、電子署名やeシールなどのトラストサービスの制度化や普及促進を図るとともに、制度・手続・慣習の見直しを進める。

2 5G の本格開始に伴うセキュリティ対策の強化

① 5Gネットワークの脆弱性及び脅威の検証・分析のための手法や体制の確立

② 関係者間のリスク・脅威情報の共有の促進

③ 規制・振興両面でのセキュリティ対策の実装の促進など

（セキュリティ・バイ・デザインの観点で推進）

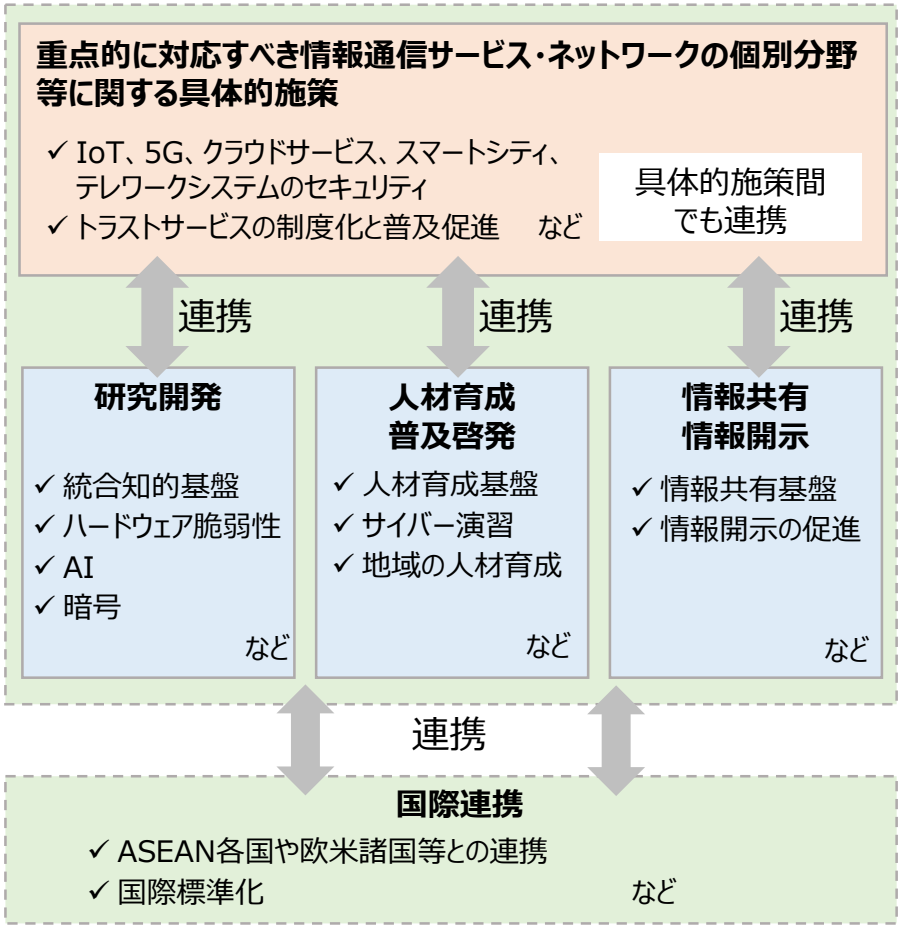
3 サイバー攻撃に対する電気通信事業者のアクティブな対策の実現

巧妙化・多様化するサイバー攻撃に対処するため、電気通信事業者における積極的なサイバーセキュリティ対策（C&Cサーバの能動的な検知や攻撃指令通信の遮断等）を迅速かつ効果的に実施可能とするため、通信の秘密の保護を図りつつ、一層のサイバーセキュリティを確保する方策について検討を行う。

4 我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

我が国におけるセキュリティ製品・サービスの海外依存や慢性的な人材不足から脱却するため、サイバーセキュリティ情報を国内で収集・蓄積(生成)・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤を構築し、産学官連携の結節点とするための体制の構築を図る。

● IoT・5Gセキュリティ総合対策2020の枠組み



※1 2020年東京大会に向けた対処として短期的な観点から早急に取り組むべき事項を整理した結果を「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項 [緊急提言]」として 2020年１月に公表。

※2 IoT・5G時代にふさわしいサイバーセキュリティ政策の在り方について検討した結果を「IoT・5Gセキュリティ総合対策」として2019年8月に公表。

１．最近のセキュリティ動向

２．政府全体の取組

３．「IoT・5Gセキュリティ総合対策2020」

（１）COVID-19への対応を受けたセキュリティ対策の推進

（２）5Gの本格開始に伴うセキュリティ対策の強化

（３）サイバー攻撃に対する電気通信事業者のアクティブな対策の実現

（４）我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

（５）その他のトピックス（暗号、スマートシティ、国際連携）

テレワークにおけるセキュリティ対策の強化

- 総務省では従来から「**テレワークセキュリティガイドライン**」を**策定**し、**セキュリティ対策の考え方**を示している。
- 新型コロナウイルスの影響により、これまで未導入だった中小企業等においてもテレワークの導入が広まる中で、**実践的かつ具体的で分かりやすい内容のチェックリスト**を作成し、2020年９月に公表。
- またチェックリスト策定と併せ、**セキュリティ対策**に関する**実態調査**と**専門的な相談対応**を実施中。

チェックリストの策定

テレワークセキュリティガイドライン

（2018年４月　第４版）

2004年12月初版
2006年４月第２版
2013年３月第３版

【想定読者像】

- ✓ システム管理者のほか経営層や利用者を幅広く対象
- ✓ 専任の担当や部門が存在
- ✓ 基本的なIT用語は仕組みとして理解しているレベル
- ✓ 基本的なシステム設定作業は、補助解説なく実施可能

2020年度内に改定予定

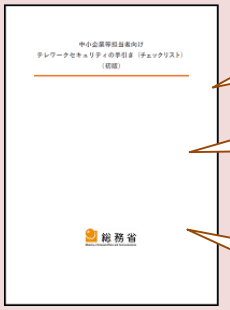
追加

中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)

（2020年９月　初版）

【想定読者像】

- ✓ システム管理担当者向け
- ✓ 専任の担当・部門は存在しない
- ✓ 基本的なIT用語は聞いたことがあるレベル
- ✓ 基本的なシステム設定作業は検索しながら実施可能



テレワーク方式を特定し、その方式に**対応するチェックリストを確認**

チェックリストは**最低限のセキュリティを確実に確保**してもらうためのものに限定

テレワーク用ソフトについて、**設定解説資料を作成**し具体的設定を解説

2020年度内を目途に実態調査の結果等を踏まえて**改定**予定

公表先

実態調査／専門相談対応

テレワーク導入企業が拡大しており、セキュリティ等の実態や課題について調査
（結果はチェックリスト策定にもフィードバック）

テレワーク導入企業

相談申込先

テレワーク導入時・導入後における
セキュリティ対策の専門的な相談

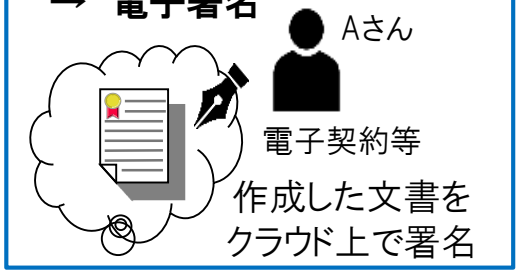
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

「トラストサービス」とは

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

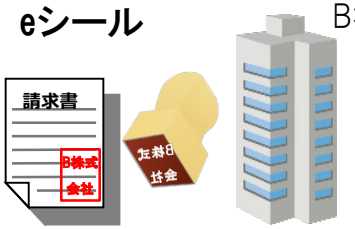
国の制度（電子署名法）有り

①意思を確認
→ 電子署名



制度無し

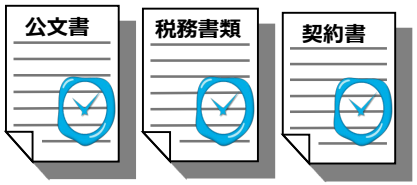
②文書の起源を確認
→ eシール



組織が発行する文書

民間の認定スキーム有り

④データの存在証明
→ タイムスタンプ



制度無し

③データの送信元（モノ）の正当性を確認

IoT機器（センサー等）から
発せられるデータ

制度無し

⑤データの送達等の保証（①～④の組合せによるサービス）

トラストサービスにより期待される効果の例

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

※ 利用者がサーバにリモートでログインし、サーバ上で行う電子署名のこと

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

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

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

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

電子署名法の概要

内容

※　「電子署名及び認証業務に関する法律」（平成12年法律第102号）
総務省、法務省及び経済産業省の共管（平成13年4月施行）

電子署名とは、電磁的記録に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するもの（法第２条第１項）。

一　当該情報が**当該措置を行った者の作成に係るもの**であることを示すためのものであること。

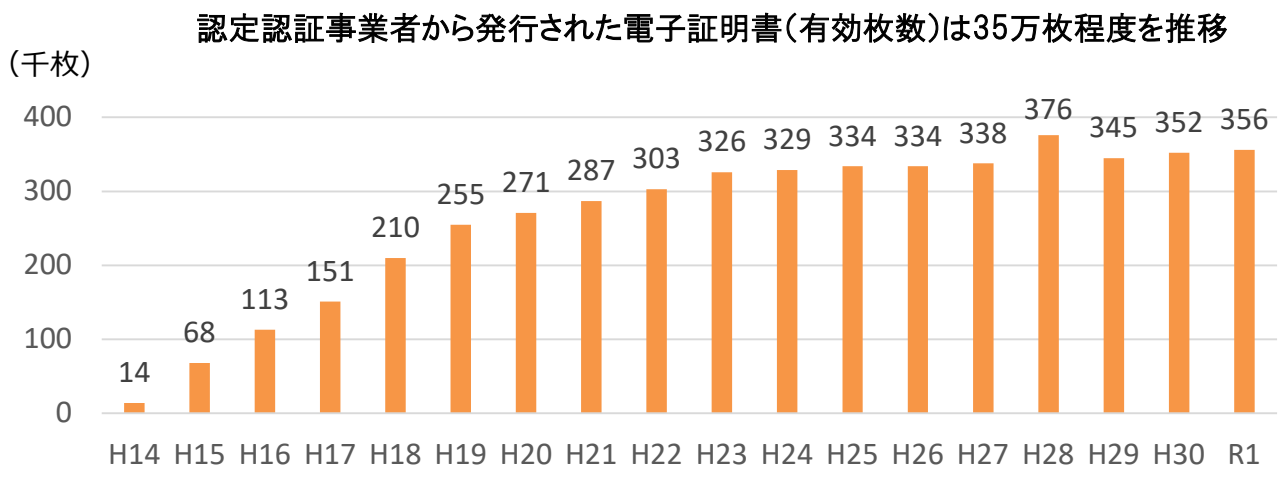
二　当該情報について**改変が行われていないかどうかを確認することができるもの**であること。

（１）電磁的記録の真正な成立の推定

本人による一定の条件を満たす電子署名が付されている電子文書等の真正な成立の推定（法第３条）

（２）認証業務に関する認定制度

主務大臣は、主務省令で定める基準等に適合する認証業務を認定（法第６条）



認定認証事業者：７事業者

- （株）日本電子公証機構
- セコムトラストシステムズ（株）
- 日本電子認証（株）
- 東北インフォメーション・システムズ（株）
- （株）帝国データバンク
- （株）エヌ・ティ・ティネオメイト
- 三菱電機インフォメーションネットワーク（株）

（令和２年10月1日時点）

タイムスタンプの概要

○　一般財団法人日本データ通信協会による民間の認定スキーム（タイムビジネス信頼・安心認定制度）により、タイムスタンプ事業者がサービスを提供

一般財団法人
日本データ通信協会

認定

時刻認証業務
認定事業者（TSA）

5事業者

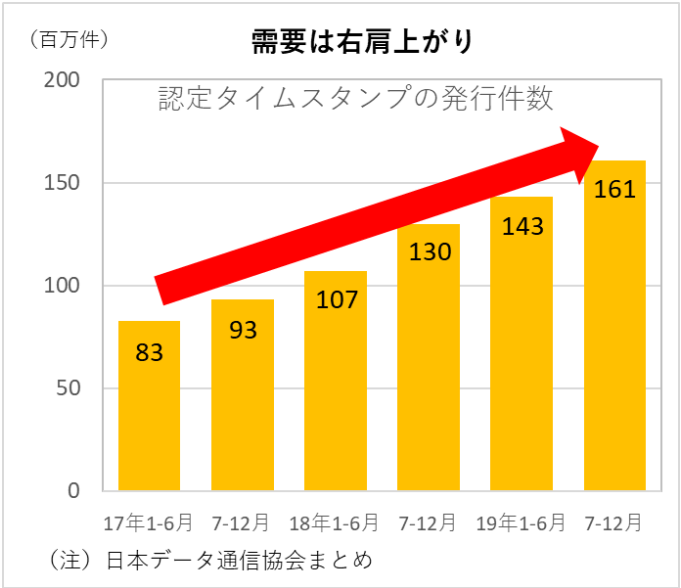
- アマノ（株）
- セイコーソリューションズ（株）
- （株）TKC
- （株）サイバーリンクス
- 三菱電機インフォメーションネットワーク（株）

（令和2年10月1日時点）

タイムスタンプを発行

利用者

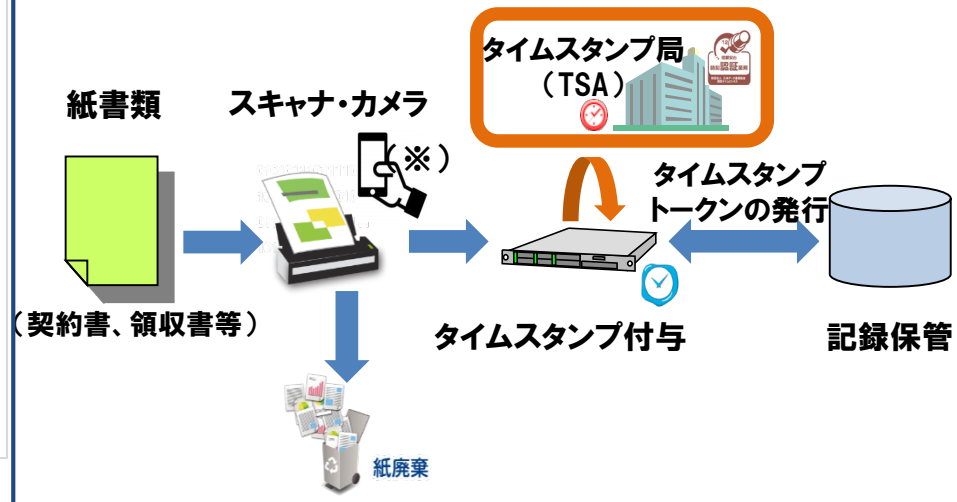
平成17年（2005年）2月
タイムスタンプの認定業務を開始



（注）日本データ通信協会まとめ

活用事例

電子帳簿保存法（国税庁）に基づく取引関係書類の電子データ化



※　平成28年の制度改正により、スマホ等のカメラによる画像保存が認められた。

トラストサービス検討WG取りまとめ

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

現状・課題	取組の方向性
〇データの存在証明の仕組み（タイムスタンプ） • **民間の認定スキームの下で、一部の分野を除き、利用が十分に広がっていない**。 → 電子データと紙による保存を併存している実態があり、保存コストを要している。	• タイムスタンプ事業者に対する**国としての認定制度を創設**。
〇文書の起源を確認できる仕組み（eシール） • 請求書や領収書等について、企業が電子的に発行したことを**簡便に保証する仕組みがない**。 → 企業内の業務や企業間の取引における**電子化が進まず、業務効率化の妨げ**となっている。	• 企業間の書類のやり取りの現状を把握しつつ、**eシールが有効なユースケースについて、幅広く検討。**
〇意思を確認できる仕組み（電子署名） • クラウドを活用した**リモート署名など最新の技術に制度が十分に対応しきれていない**部分が存在。 → 電子署名の利用が伸びていない。 • リモート環境で本人だけが安全に署名できるための**技術的な要件について民間団体で検討中**。	• リモート署名の**電子署名法上の位置づけについて検討**。

■ 上記に加え、電子文書の送受信・保存について規定している**法令との関係で有効な手段として認められるトラストサービスの要件を明示するよう、所管省庁への働きかけ**を行う。

タイムスタンプの国による認定制度の全体像

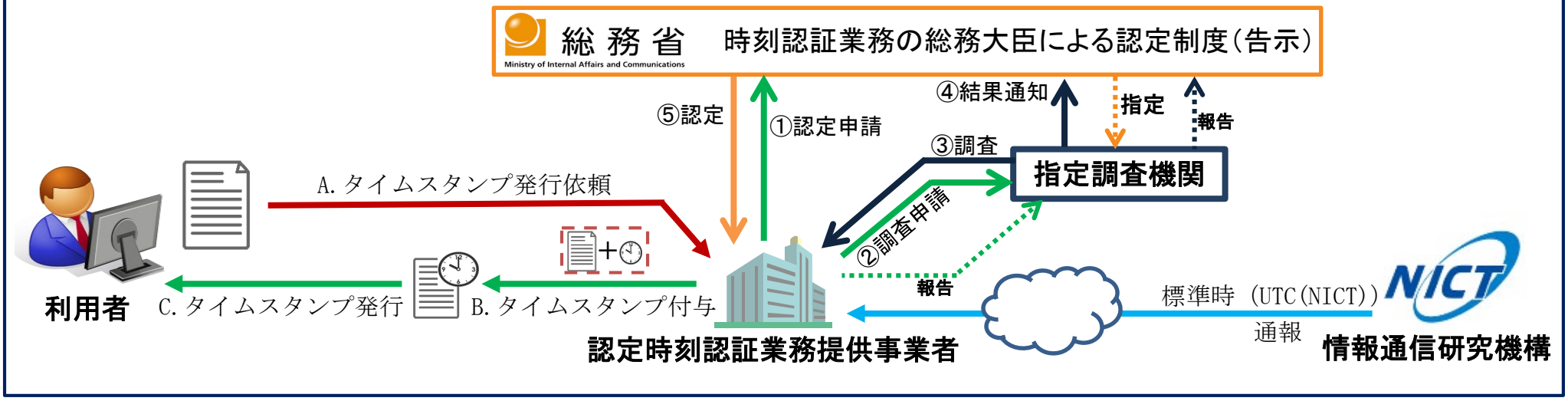
タイムスタンプの国による認定制度（告示）の概要

- **電子データがある時点に存在していたこと**及び**当該電子データがその時点から改ざんされていないこと**を証明する情報である「タイムスタンプ」を、電子データに係る情報に付与する役務を提供する業務を**「時刻認証業務」**とする。
- 時刻認証業務の中で、**確実かつ安定的にタイムスタンプを発行するための要件を満たすもの**を、**「認定時刻認証業務」**とする。

認定要件のポイント（抜粋）

- ○ デジタル署名方式を用いること。
- ○ 時刻源は国立研究開発法人情報通信研究機構のUTC（NICT）とすること。
- ○ 発行する（した）タイムスタンプと当該時刻源との時刻差が1秒以内となるよう、時刻の品質を管理及び証明する措置を講じること。
- ○ タイムスタンプは十分な安全性を有する暗号技術や装置等を用いて生成・管理すること。

認定制度の仕組み



１．最近のセキュリティ動向

２．政府全体の取組

３．「IoT・5Gセキュリティ総合対策2020」

（１）COVID-19への対応を受けたセキュリティ対策の推進

（２）5Gの本格開始に伴うセキュリティ対策の強化

（３）サイバー攻撃に対する電気通信事業者のアクティブな対策の実現

（４）我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

（５）その他のトピックス（暗号、スマートシティ、国際連携）

5Gの本格開始に伴うセキュリティ対策の強化

5Gのセキュリティについて、セキュリティ・バイ・デザインの観点から、総合的な対応を推進。

①脆弱性・脅威の検証・分析のための手法・体制の確立

- サプライチェーンリスクへの対応を念頭に置きつつ、**ハードウェア・ソフトウェアの両面において脆弱性の検証手法等を確立**。
- 脆弱性検出技術の成果を活用（技術移転を含む）し、関連する脅威の分析の視点を踏まえた**5Gシステムや利用者に対するインパクト分析を実施し、必要なセキュリティ対策に反映**。
- 上記の検証・分析の取組に関し、**5Gの事業者・運用者やベンダー、研究機関等が協力して実施する体制を構築**。

※Beyond 5Gを見据えた技術開発も促進。

②脆弱性の情報共有の促進

- （一社）ICT-ISACの「5Gセキュリティ推進グループ」において、事業者・運用者・ベンダー間で**5Gのリスク情報や脅威情報などの共有を推進**。

③対策の促進

制度的措置

- サプライチェーンリスク対応を含む十分なサイバーセキュリティ対策を講じることを全国5Gの開設計画の認定及びローカル5Gの**免許の条件**とし、対策の実施状況について定期的にフォローアップ。

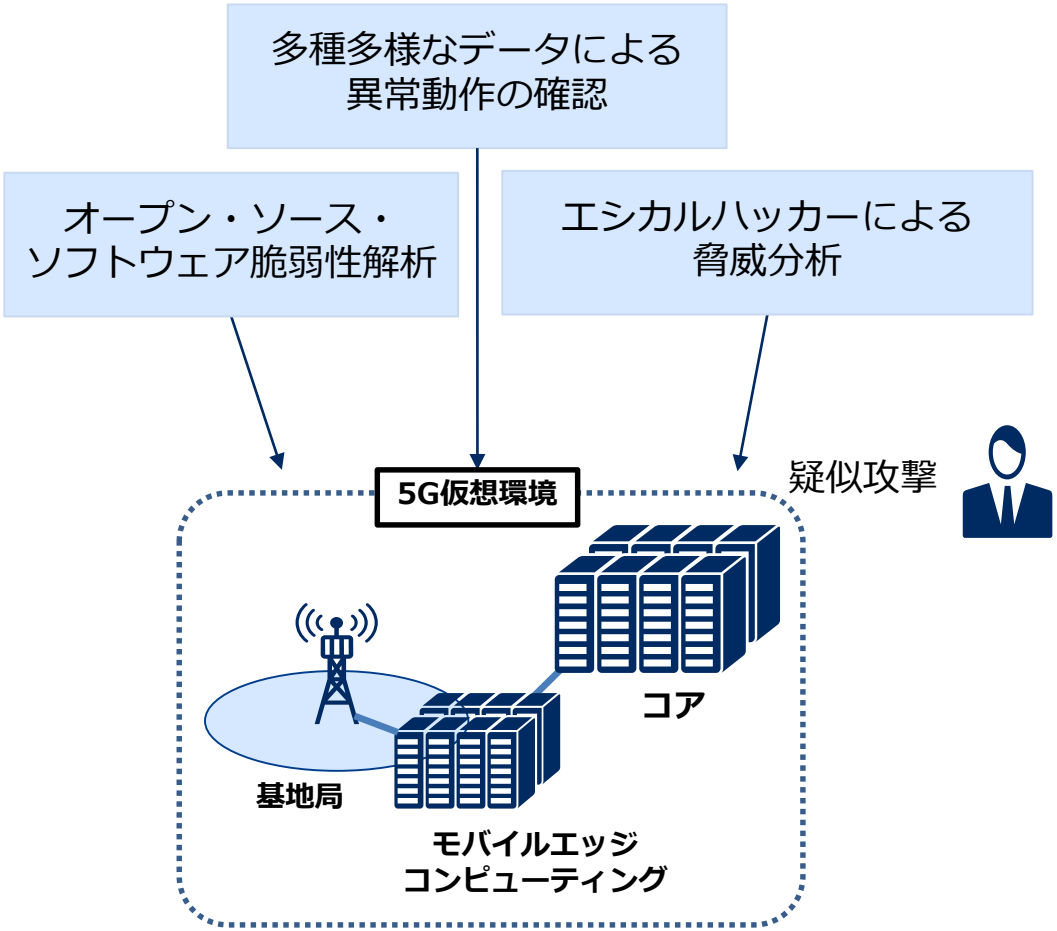
振興的措置

- 全国５G及びローカル５Gの導入事業者に対する**税制優遇措置等**により、安全・安心な５Gシステムの普及を支援。

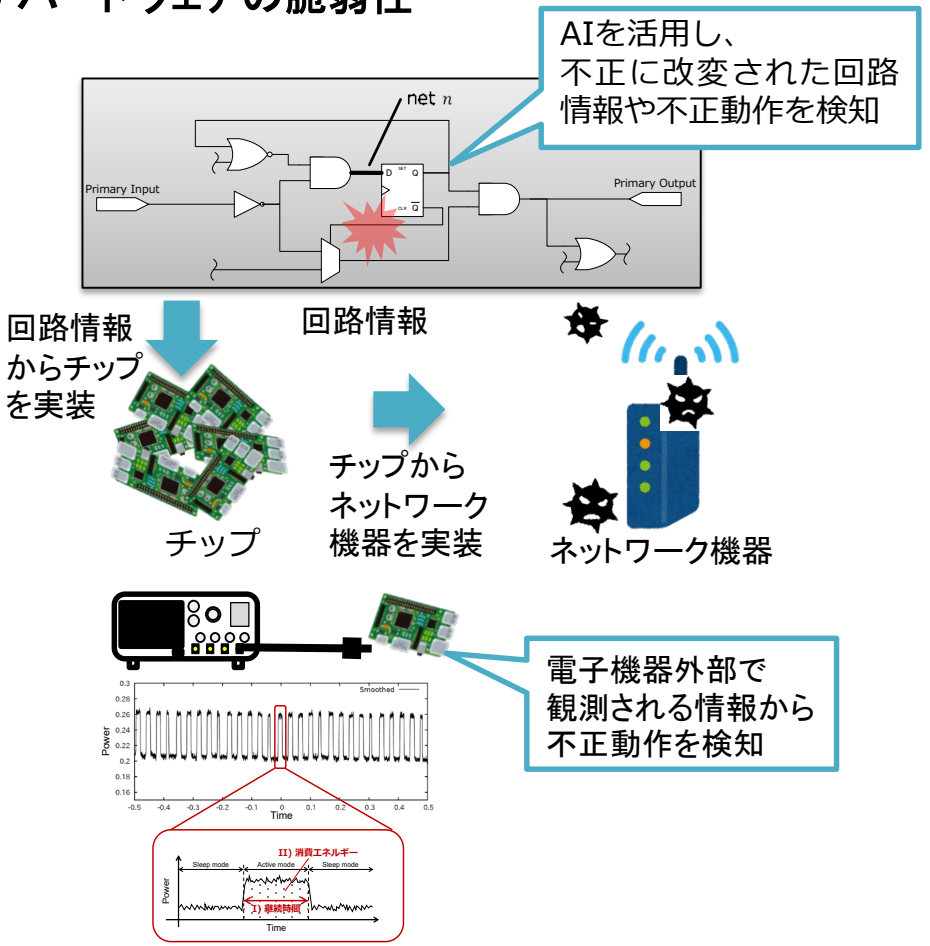
5Gネットワークの脆弱性対策

- 国民の安全・安心の確保に向け、5Gネットワークやその構成要素及びサービスについて、ソフトウェア・ハードウェアの両面から技術的検証を行うことを通じ、5Gネットワークのセキュリティを総合的かつ継続的に担保できる仕組みを整備。事業の成果は関係者へ共有のうえ、周知・啓発と実際の対策の推進を図る。
（サイバーセキュリティタスクフォース（第25回）資料「5Gネットワーク構築におけるセキュリティに関する対策等の留意点（令和元年度版）」にて5Gセキュリティガイドライン（β版）公開中。）

(a) ソフトウェアを中心としたネットワークの脆弱性



(b) ハードウェアの脆弱性



規制・振興両面でのセキュリティ対策の実装促進

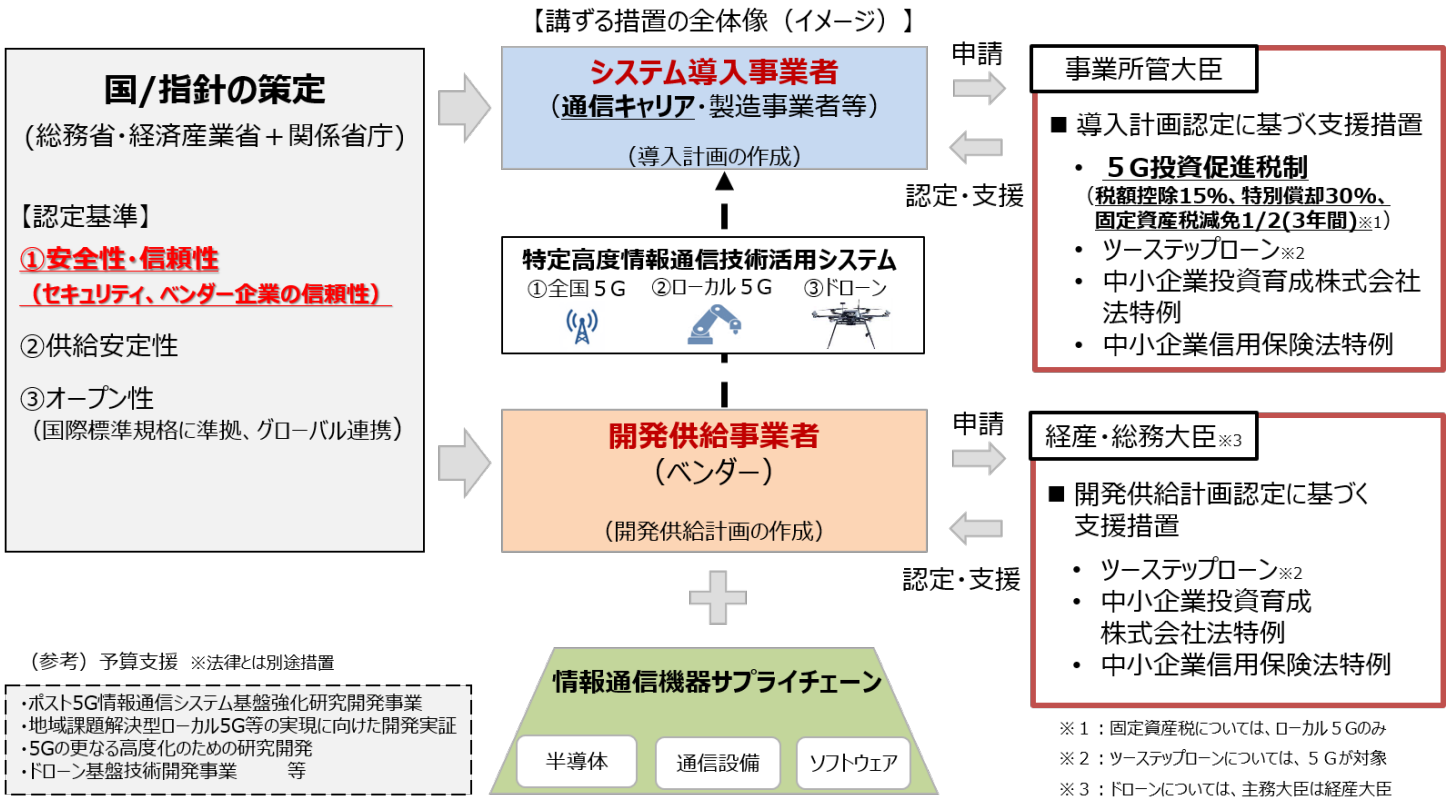
規制的措置

5G（全国5G）用周波数の割当て（開設計画の認定）及びローカル5Gの免許にあたり、サプライチェーンリスクを含む十分なサイバーセキュリティ対策を講ずるよう条件を付し、その対策状況を定期的にフォローアップ。

振興的措置

新法（特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律）により、特定高度情報通信技術活用システム（全国5G及びローカル5G、ドローン）の開発供給及び導入に係る認定制度と税制等の支援措置を講ずることにより、サイバーセキュリティ等を確保しつつ、5G／ローカル5Gの普及を図る。

「特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律」の概要



1. 最近のセキュリティ動向

2. 政府全体の取組

3.「IoT・5Gセキュリティ総合対策2020」

（１）COVID-19への対応を受けたセキュリティ対策の推進

（２）5Gの本格開始に伴うセキュリティ対策の強化

（３）サイバー攻撃に対する電気通信事業者のアクティブな対策の実現

（４）我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

（５）その他のトピックス（暗号、スマートシティ、国際連携）

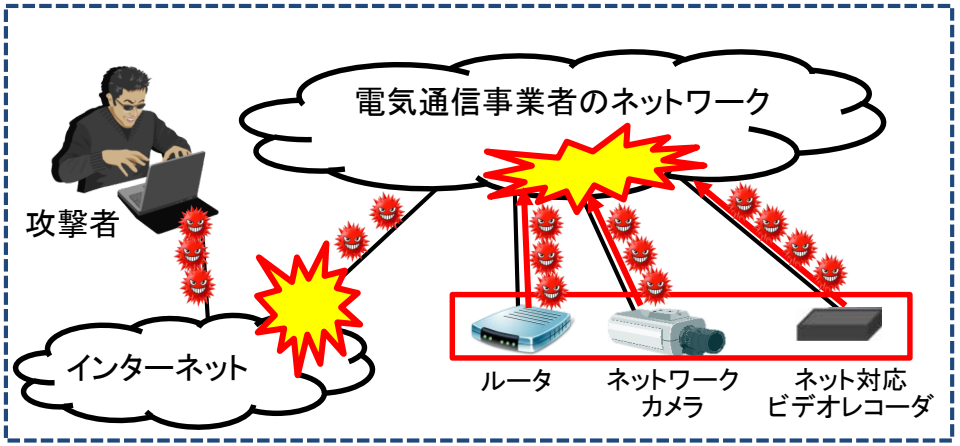
IoT機器のセキュリティ対策に関する技術基準の改正

【背景・課題】

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

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

＜IoT機器が乗っ取られてサイバー攻撃に悪用される事案のイメージ＞



【端末設備等規則（省令）の改正概要】

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

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

  ②初期設定のパスワードの変更を促す等の機能

  ③ソフトウェアの更新機能※1

  又は①～③と同等以上の機能※2

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

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

【その他】

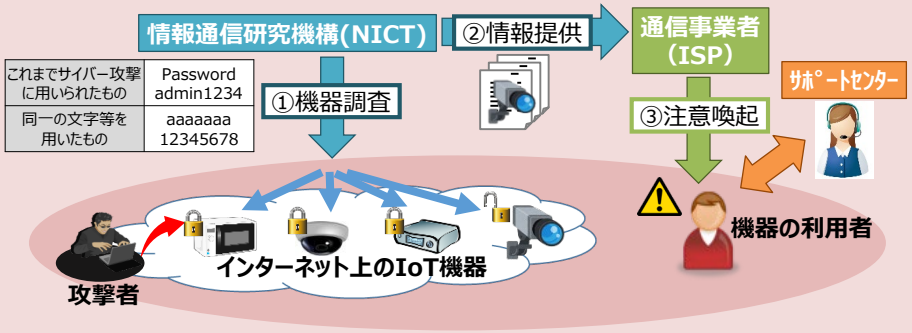
- 2020年４月１日に改正省令を施行。
- 改正省令の運用方法や解釈等を定めるガイドラインも策定。

IoT機器調査及び利用者への注意喚起（NOTICE/NICTER）

- 情報通信研究機構(NICT)が**サイバー攻撃に悪用されるおそれのあるIoT機器**を調査し、インターネット・サービス・プロバイダ(ISP)を通じた利用者への注意喚起を行う取組「**NOTICE**」を2019年２月より実施。
- NOTICEの取組に加え、**マルウェアに感染しているIoT機器**をNICTの「**NICTER**」プロジェクト※で得られた情報を基に特定し、ISPから利用者へ注意喚起を行う取組を2019年６月より開始。

※NICTが、インターネット上で起こる大規模攻撃への迅速な対応を目指したサイバー攻撃観測・分析・対策システムを用いて、ダークネットや各種ハニーポットによるサイバー攻撃の大規模観測及びその原因（マルウェア）等の分析を実施。

【NOTICE注意喚起の概要】

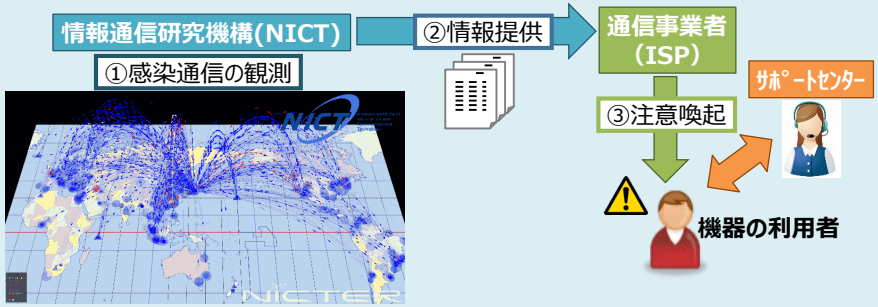


調査対象：パスワード設定等に不備があり、**サイバー攻撃に悪用されるおそれのある**IoT機器

① NICTがインターネット上のIoT機器に、容易に推測されるパスワードを入力するなどして、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ISPに通知。
③ ISPが当該機器の利用者を特定し、注意喚起を実施。

【NICTER注意喚起※の概要】

※マルウェアに感染しているIoT機器の利用者への注意喚起



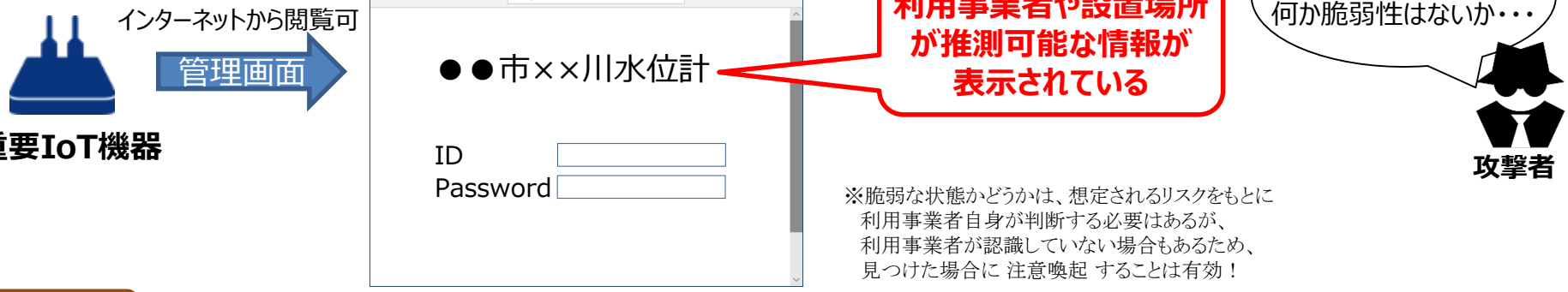
調査対象：既にMirai等の**マルウェアに感染している**IoT機器

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

重要IoT機器のセキュリティ対策

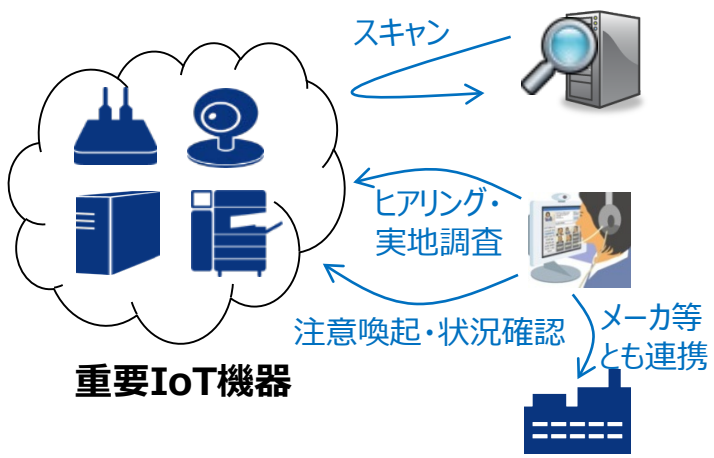
- 重要インフラ等の社会的に影響を及ぼすリスクを伴った使用をしているIoT機器（**重要IoT機器**）について、**公開する必要のない情報が公開されている**など、攻撃を受けやすい**脆弱な状態**にあるものを**検出**する。
- 検出した重要IoT機器について、利用事業者に対して**設定状況等のヒアリング**を行った上で、脆弱な状態を解消するための**注意喚起**や**対策手法の提示**を行い、**対策の完了までのトレース**を行う。

脆弱な状態の例



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

対策スキーム



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

１．最近のセキュリティ動向

２．政府全体の取組

３．「IoT・5Gセキュリティ総合対策2020」

（１）COVID-19への対応を受けたセキュリティ対策の推進

（２）5Gの本格開始に伴うセキュリティ対策の強化

（３）サイバー攻撃に対する電気通信事業者のアクティブな対策の実現

（４）我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

（５）その他のトピックス（暗号、スマートシティ、国際連携）

セキュリティ人材の育成（ナショナルサイバートレーニングセンター）

➢ 巧妙化・複雑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」において演習等を実施。

CYDER Cyber Defense Exercise with Recurrence（サイダー）

国・地方公共団体・独法・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

⇒ **年間100回、計3,000名規模**で実施（**１日**コース＆**全都道府県**で開催）
2019年度は延べ**3,090名**が受講（2017年度は延べ3,009名、2018度は延べ2,666名が受講）
※2021年からオンライン受講を新設予定

cyber colosseo（サイバーコロッセオ）

2020年東京大会関連組織のセキュリティ担当者等を対象とした実践的サイバー演習

⇒ 2017年度から開始し、2020年12月で事業完了
期間中に、**演習形式**で延べ**571**名、**講義形式**で延べ**1,717名**の人材を育成

SecHack365（セックハック365）

25歳以下の若手セキュリティイノベーターの育成

⇒ **年間50名程度**の受講者を選定し、**１年間のトレーニング**コースを実施
2019年度は**45名**が修了（2017年度は39名、2018年度は46名が修了）

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

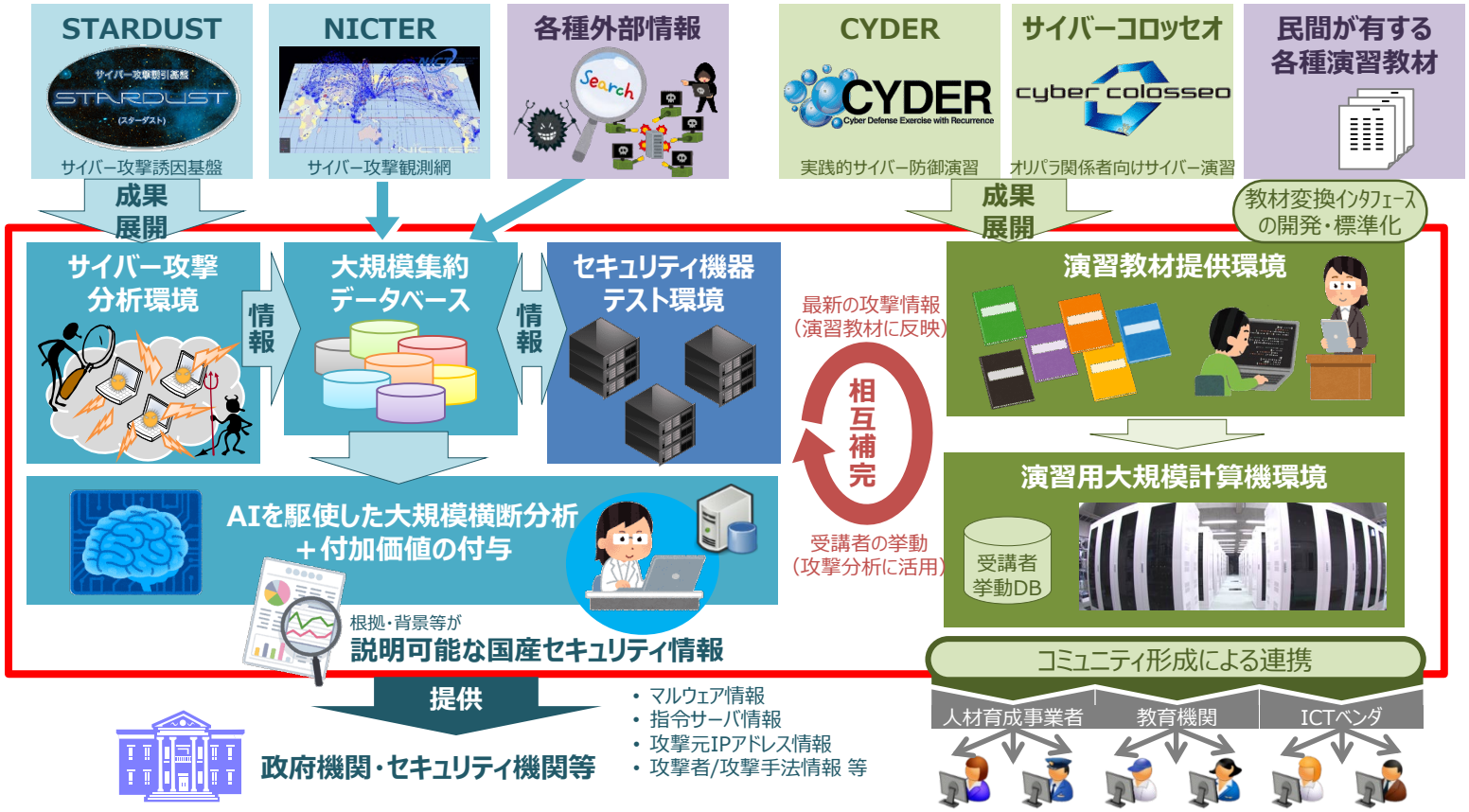
実事案に対処可能な人材育成
CYDER

高度な攻撃に対処可能な人材育成
サイバーコロッセオ

ハイレベル層の人材育成
SecHack365

サイバーセキュリティ統合知的・人材育成基盤

➢ サイバーセキュリティ情報を**国内で収集・蓄積・分析・提供**するとともに、**社会全体でサイバーセキュリティ人材を育成する**ための共通基盤をNICTに構築し、産学の結節点として開放することで、サイバーセキュリティ対応能力の向上を図る。



次のとおり活用可能な基盤をNICTに構築。

➢ **国産セキュリティ情報の収集・蓄積・分析・提供**
幅広くサイバーセキュリティ情報を収集・蓄積し、AIを駆使して横断的に分析することで、高信頼で即時的なセキュリティ情報を生成し、政府・セキュリティ機関等に提供。

➢ **セキュリティ機器テスト環境**
セキュリティ製品・サービスの開発を推進するため、最新のサイバー攻撃情報を活用し、その対応状況をセキュリティ事業者がテストできる環境を提供。

➢ **高度解析人材の育成**
収集したセキュリティ情報を活用し高度なサイバー攻撃を迅速に検知・分析できる卓越した人材を育成。

➢ **人材育成のための基盤提供**
NICTが有する人材育成に関する環境・知見を民間・教育機関等に開放し、自律的な人材育成を推進。

１．最近のセキュリティ動向

２．政府全体の取組

３．「IoT・5Gセキュリティ総合対策2020」

（１）COVID-19への対応を受けたセキュリティ対策の推進

（２）5Gの本格開始に伴うセキュリティ対策の強化

（３）サイバー攻撃に対する電気通信事業者のアクティブな対策の実現

（４）我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

（５）その他のトピックス（暗号、スマートシティ、国際連携）

量子コンピュータ時代に向けた暗号の在り方の検討

➢ CRYPTRECの暗号技術検討会*の下に「**量子コンピュータ時代に向けた暗号の在り方検討タスクフォース**」を設置し、量子コンピュータ時代の推奨暗号の在り方について検討（2019年６月～）。

＜検討事項＞
- 大規模な量子コンピュータの動向を踏まえた次期CRYPTREC暗号リストに求められる要件等の検討
- その他新たな暗号技術の動向等（軽量暗号や秘密計算に利用される準同型暗号等）を踏まえた検討等

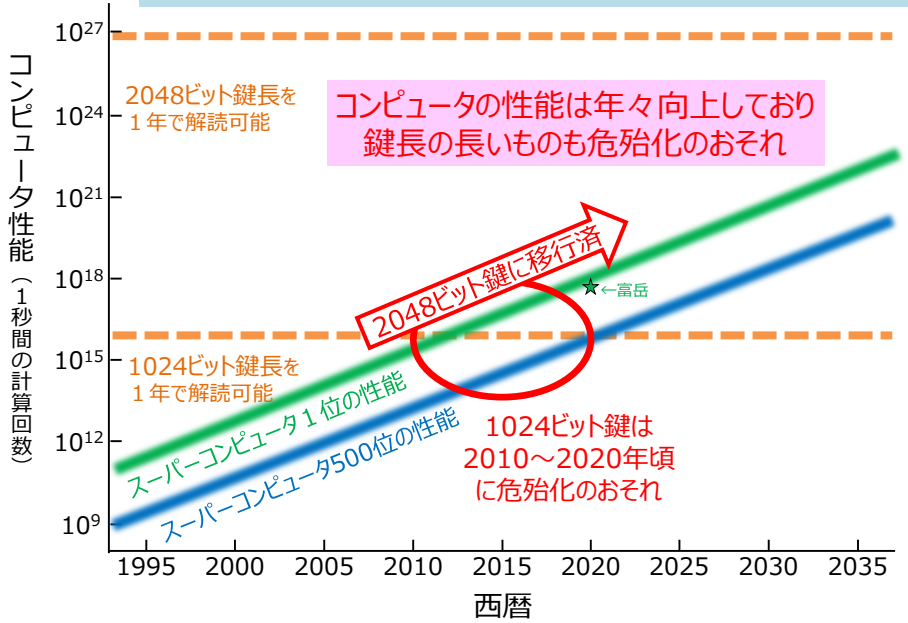
＊ **CRYPTREC**（Cryptography Research and Evaluation Committees）は、**電子政府推奨暗号**の**安全性を評価・監視**し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。総務省及び経済産業省が共同運営する**暗号技術検討会**と、NICT及びIPAが共同運営する**暗号技術評価委員会**で構成。

検討の背景

✓ 遠くない将来に現在の公開鍵暗号（RSA暗号や楕円曲線暗号）が容易に解読されるおそれ
✓ 大規模システムの改修・更改には10年以上を要する

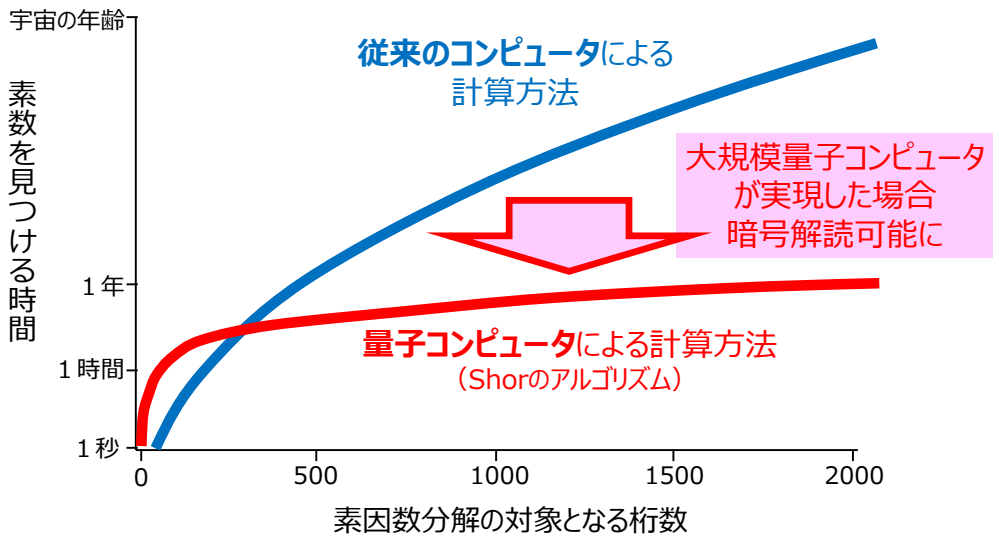
※RSA暗号：大きな桁数の素因数分解は困難なことを安全性の根拠とした公開鍵暗号

従来のコンピュータの性能向上による影響
例：RSA暗号の安全性評価



※CRYPTREC Report 2019 及び top500.org により作成

実用的な量子コンピュータによる影響
例：RSA暗号の安全性評価



※Quantum Computing (Stolze and Suter)により作成

スマートシティにおけるセキュリティ（検討の枠組み）

- スマートシティのセキュリティ確保の在り方について、多様な関係者間で一定の共通認識の醸成が必要。
- **官民の検討の場において、スマートシティのセキュリティ確保の観点から留意すべき要件やチェックすべき事項などについて検討を行い、明確化**を図る。またその際は、スマートシティを推進する取組との連携を図り、セキュリティ対策の実装を促進していくことが重要。

政府全体の取組

アーキテクチャ検討会議【官】

（事務局：内閣府、座長：越塚登　東京大学教授）

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

検討の内容を共有 ↓　↑ 事務局オブザーバ出席

スマートシティ官民連携プラットフォーム【官民】

（令和元年８月８日設置）

（事務局：内閣府、国土交通省、**総務省**、経済産業省）

目的：官民が一体となって全国各地のスマートシティの取組を推進

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

＜活動内容＞

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

総務省の取組（セキュリティ関連）

スマートシティのセキュリティの検討

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

検討の内容を共有 ↓　↑ フィードバック

スマートシティセキュリティ・セーフティ分科会

（令和２年１月活動開始）

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

目的：スマートシティにおいて実現される様々な機能・サービス・機器などについて、セキュリティやセーフティを確保しつつ、実装していくための方策について検討する。

メンバー：13者（令和２年２月時点）

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

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

（事務局：内閣府）

「スマートシティセキュリティガイドライン（第1.0版）」の公表

■ 内閣府SIPにおいて定義された、「スマートシティリファレンスアーキテクチャ」※の枠組みに基づき、スマートシティに求められるセキュリティ要件を整理した**「スマートシティセキュリティガイドライン（第1.0版）」を作成**、2020年10月に公表。

スマートシティリファレンスアーキテクチャで定義すべきこと

1. **スマートシティ戦略・政策**
   スマートシティの理念、目標、KGI、KPI
2. **スマートシティルール**
   スマートシティ関連法令、ガイドライン、規制緩和、特区活用
3. **スマートシティ組織**
   スマートシティ推進主体、サービス提供者、サービス受益者
4. **スマートシティビジネス**
   スマートシティビジネスモデル、体験デザイン、サービス
5. **スマートシティ機能**
   サービスAPI、サービス管理、都市OS間連携
6. **スマートシティデータ**
   データ管理、データ仲介、データセット、データカタログ
7. **スマートシティデータ連携**
   外部システム連携、アセット連携、アセット管理
8. **スマートシティアセット**
   センサ、アクチュエータ、ネットワーク

9. **スマートシティセキュリティ**
   認証機能、不正アクセス・サイバー攻撃対策

スマートシティセキュリティのカテゴリ

スマートシティセキュリティガイドライン（第1.0版）

- **ガバナンス**
  - ✓ セキュリティ基本方針の策定
  - ✓ セキュリティ対応のルール化
  - ✓ セキュリティ対応体制の構築
- **サービス**
  - ✓ サービスの特性を踏まえた守るべき機能や資産の特定
  - ✓ サービスを守るためのセキュリティ実装
    （脆弱性排除、多要素認証 等）
- **都市OS**
  - ✓ クラウド基盤の活用を前提とした都市OSセキュリティの実装
    （認証、アクセス制御、暗号化 等）
- **アセット**
  - ✓ アセット（機器や中継装置）に対するセキュリティの実装
    （機器の異常検知等）

※ スマートシティサービス構築の際のフレームワークを提示する等し、スマートシティの関連ステークホルダーがスマートシティサービスを構築する際に参考とすることができるアーキテクチャ。令和２年３月１８日に内閣府HPにてホワイトペーパーが公開された。

総務省のサイバーセキュリティ分野における国際連携の取組について

■ 総務省では、サイバーセキュリティに関する二国間・多国間の連携や対ASEAN諸国を中心とする能力構築支援の取組を実施するとともに、ISACやISP間の国際連携を推進している。

①二国間・多国間連携

総務省のサイバーセキュリティ政策について、積極的な対外発信と連携強化を実施。

・二国間連携
- インターネットエコノミーに関する日米政策協力対話
- 日EU・ICT政策対話・戦略ワークショップ
- その他、豪、中韓、英、仏を含む13か国等とのサイバー協議　等

・多国間連携
- OECD SDE
- ITU-T SG17
- 日・ASEANサイバーセキュリティ政策会議　等

＊　イスラエルとの連携
2018年11月、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。

②民間組織の国際連携の推進

・ISP向け日ASEAN情報セキュリティワークショップ

日本とASEAN各国のISP事業者等との情報共有等の推進

・日米ISAC連携ワークショップ

日米の情報通信分野ISAC(*)間における情報共有の推進。ICT-ISACと米国IT-ISACとは2019年11月に協力覚書を締結。

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

(*) ISACとは、Information Sharing and Analysis Center（情報共有分析センター）の略で、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。

③能力構築支援

・日ASEANサイバーセキュリティ能力構築センター（AJCCBC）

AJCCBC
ASEAN JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE
Partnership by ASEAN and Japan

・世界銀行との連携

マルチ基金「DDP（Digital Development Partnership）」による途上国への能力構築支援を実施。

■主なプロジェクト

1. 第1回Cybersecurity Study Tour in Tokyo
　ASEAN諸国及び南アジア政府関係者向けのスタディツアー
2. 第2回Cybersecurity Study Tour in Tokyo
　ASEAN諸国及びインド政府関係者向けのスタディツアー
3. 西アフリカ諸国経済共同体向けワークショップへの参画

第2回Cybersecurity Study Tour（2019年9月）

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

- 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。

実施フェーズ

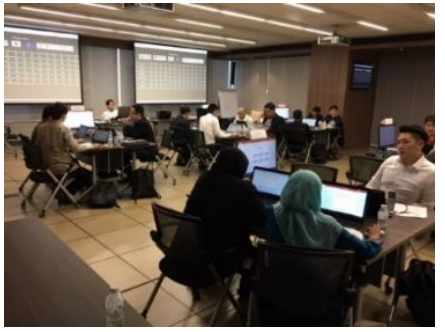
- STEP1：事前調査を実施（2017年）
- STEP2：センターを設立し研修等を実施（2018年～2022年）

AJCCBC
ASEAN JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE
Partnership by ASEAN and Japan

センターの主な活動内容

1. **サイバーセキュリティ演習**
   ASEAN各国の政府機関・重要インフラ事業者等に対し、以下の演習を実施（年6回程度）
   - ✓ 実践的サイバー防御演習（CYDER） ※CYDER: Cyber Defense Exercise with Recurrence
   - ✓ デジタルフォレンジック演習
   - ✓ マルウェア解析演習
2. **Cyber SEA Game（ASEAN Youth Cybersecurity Technical Challenge）**
   ASEAN各国から選抜された若手技術者・学生がサイバー攻撃対処能力を競うCTF形式の大会の開催（年１回）
   ※CTFとは、Capture The Flagの略で、問題の中に隠されたフラグ（＝キーワード）を探し出して解答するクイズ形式の競技

日ASEAN情報通信大臣会合（2017年12月）



サイバーセキュリティ演習

**ASEAN自らが域内の指導者となり得る人材の育成を目指すことで、
ASEANにおけるサイバーセキュリティ対処能力の底上げに貢献。（4年間で700人程度）**

新型コロナウイルスの影響を踏まえた取組

持続的な研修実施の観点から、総務省においてオンラインコース（eラーニング）の提供に取組中。また、2020年11月以降、一部の演習についてオンライン化。2021年４月には、現在実施中のすべての演習プログラムがオンラインで実施可能となる予定。

連絡先：a.umino@soumu.go.jp

総務省
Ministry of Internal Affairs and Communications