参考資料１

総務省におけるこれまでの取組

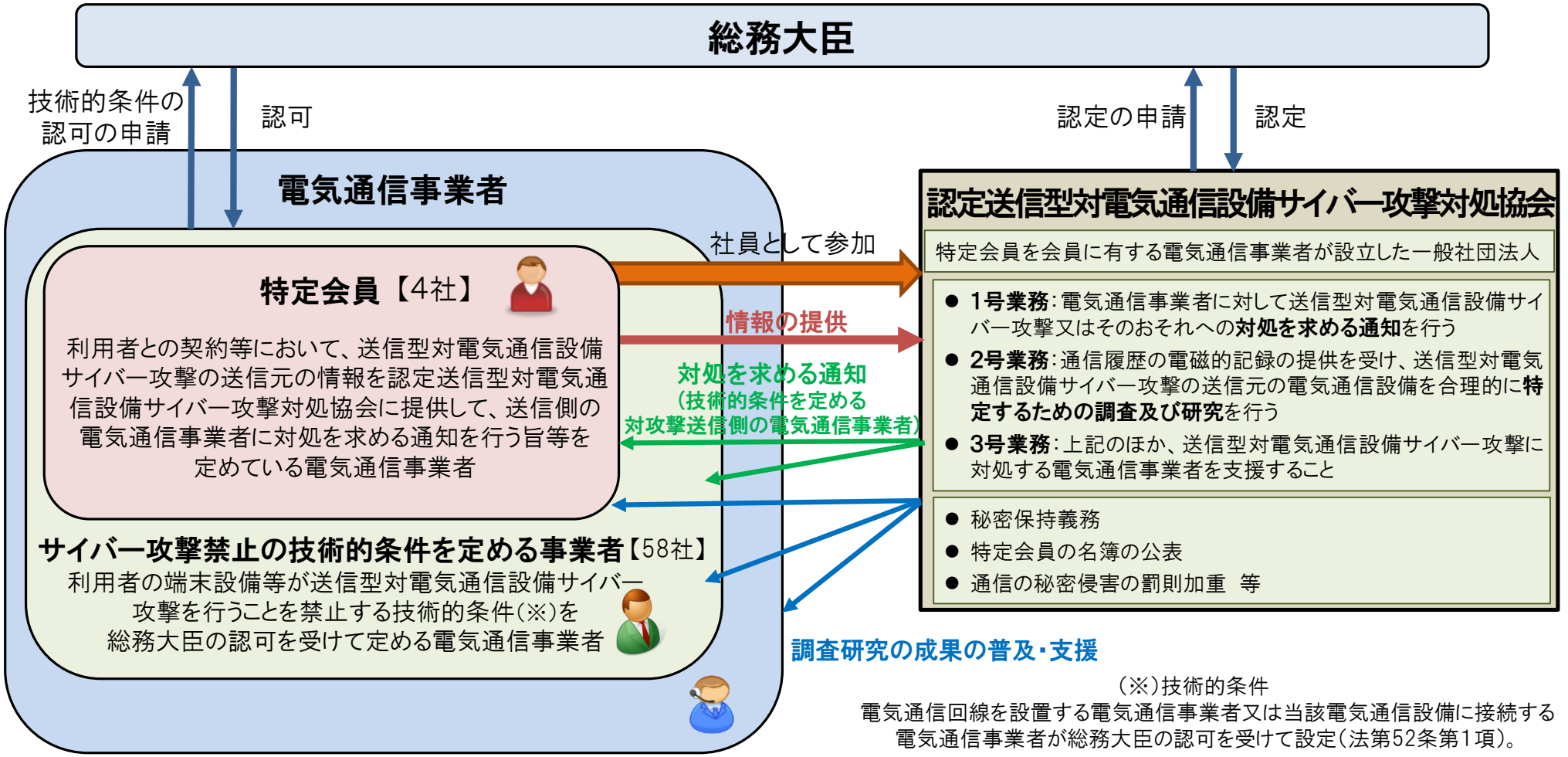
令和４年１月

サイバーセキュリティタスクフォース事務局

【１】情報通信ネットワークの安全性・信頼性の確保

認定送信型対電気通信設備サイバー攻撃対処協会（認定協会）の概要

- 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**。



（※）技術的条件
電気通信回線を設置する電気通信事業者又は当該電気通信設備に接続する電気通信事業者が総務大臣の認可を受けて設定（法第52条第1項）。

電気通信事業者による積極的セキュリティ対策

➢ 大規模化・巧妙化・複雑化するサイバー攻撃・脅威に、電気通信事業者が積極的に対処できるようにするため、フロー情報(注1)の分析を通じて、サイバー攻撃の指令元であるC&Cサーバ(注2)を検知する技術の実証等を行う。

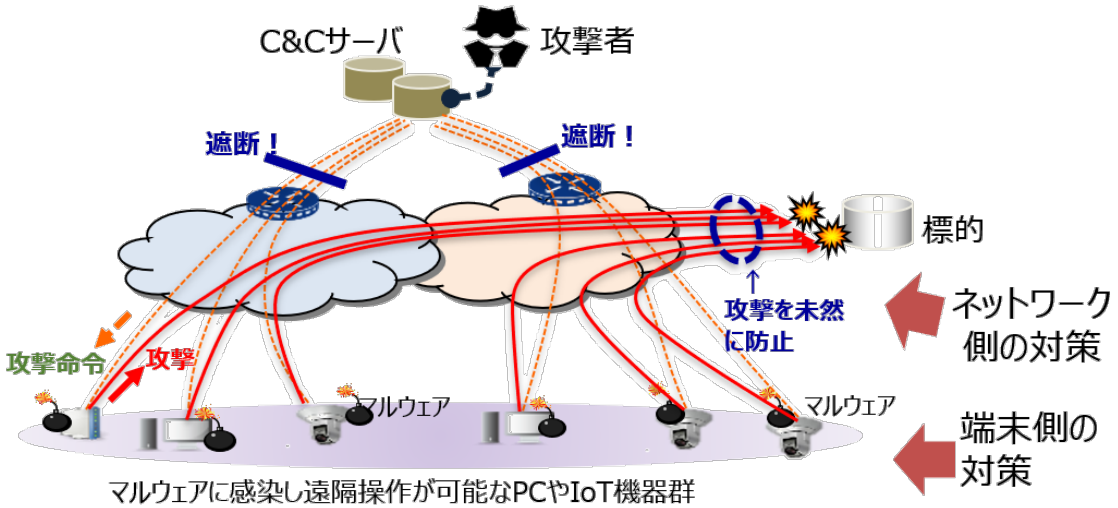
（1）通信の秘密に係る法的整理

有識者による研究会において、電気通信事業者における、インターネット利用者のトラヒックのうち必要最小限の範囲で収集するフロー情報の統計的・相関的な分析によるC&Cサーバである可能性が高い機器の検知について、通信の秘密に係る法的整理を実施。

※「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」（座長：鎮目征樹学習院大学法学部教授）の第四次とりまとめ（令和3年11月24日公表）において、正当業務行為（通信の秘密の侵害に該当しない）として整理。

（2）実証事業（令和3年度補正予算）　※「サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証」（18.0億円）

令和3年度補正予算に、電気通信事業者におけるフロー情報分析によるC&Cサーバ検知技術の有効性の検証や、事業者間の共有に当たっての運用面の課題整理のための実証事業を盛り込んでいる。



注１　フロー情報
通信トラフィックに係るデータのうち、IPアドレス及びポート番号等のヘッダ情報並びにルータでヘッダ情報を抽出する際に付与されるタイムスタンプ等の情報（通信の内容は含まない）

注２　C&Cサーバ
Command and Controlサーバの略で、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に対して攻撃者から指令を送り、制御を行うサーバコンピュータのこと

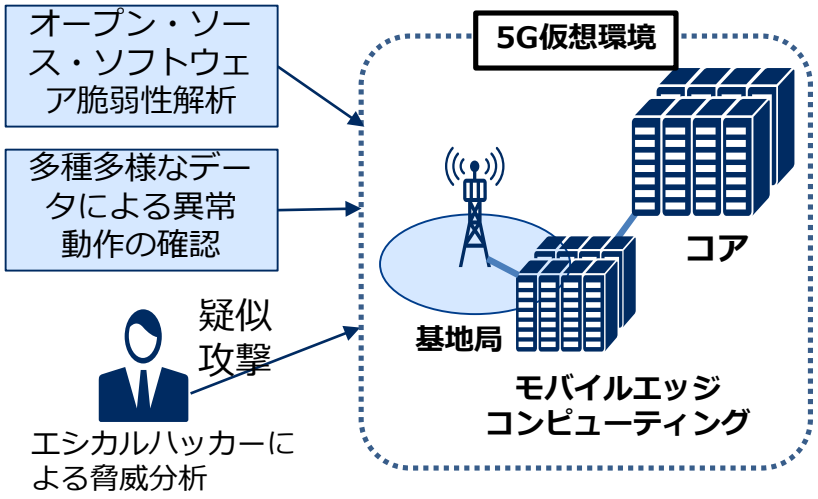
5Gネットワークのセキュリティ確保に向けた体制整備

- 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。また、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31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2年度版)」にて5Gセキュリティガイドライン(γ版)公開中。）

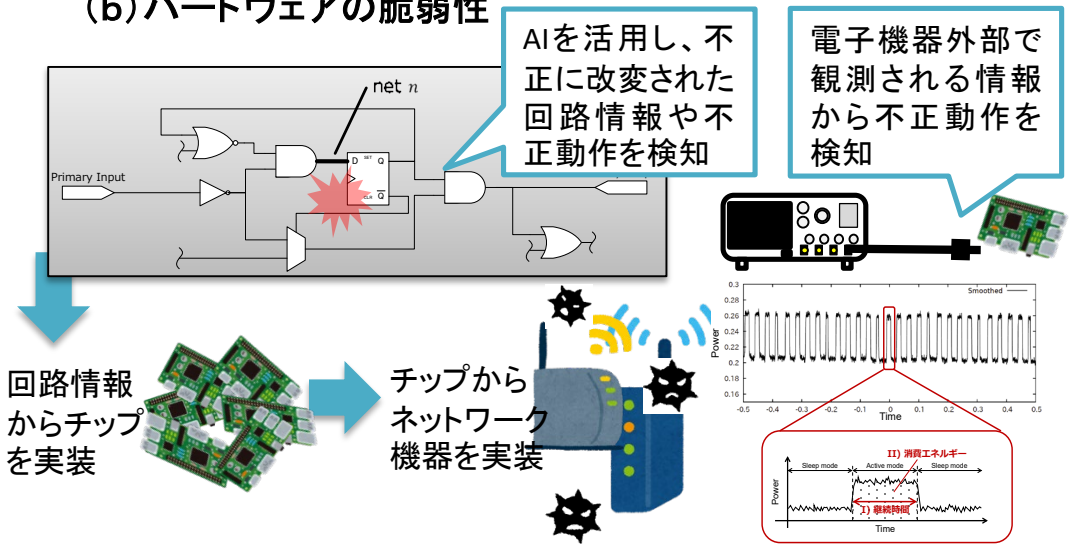
(a) ソフトウェアを中心としたネットワークの脆弱性: 5Gの通信インフラとしての機能保証のため、ソフトウェアにより構成される部分を含め、ネットワーク全体のセキュリティを確保する必要があるため、5G仮想環境を構築し、①オープンソースソフトウェア等の解析、②多種多様なパターンのデータ入力による異常動作確認（ファジング）、③エシカルハッカーによる脆弱性調査、脅威分析を実施・対策を検討。

(b) ハードウェアの脆弱性：5Gネットワークを構成するハードウェア上に故意に組み込まれた不正なチップのリスクに対応するため、①AIを活用し回路情報から不正に改変された回路を検知する技術や、②電子機器外部で観測される情報から不正動作を検知する技術を開発・対策を検証。また、③5Gネットワーク上での運用面の課題等について検討。

(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



電気通信事業ガバナンス検討会について

1．背景・目的

- 「デジタル社会」の実現のためには、その中枢基盤として、サイバー空間とフィジカル空間を繋ぐ神経網である通信サービス・ネットワークが安心・安全で信頼され、継続的・安定的かつ確実に提供されることが不可欠。
- 最近、通信サービス・ネットワークを司る電気通信事業者において、利用者の個人情報や通信の秘密の漏えい事案が発生し、海外の委託先等を通じ、これらのデータにアクセス可能な状態にあることに関するリスク等が顕在化。
- 更に、電気通信事業者に対するサイバー攻撃により、通信サービスの提供の停止に至る事案や、通信設備に関するデータが外部に漏えいした恐れのある事案など、サイバー攻撃のリスク等が深刻化。
- デジタル時代における安心・安全で信頼できる通信サービス・ネットワークの確保を図るため、電気通信事業者におけるサイバーセキュリティ対策とデータの取扱い等に係るガバナンス確保の在り方を検証し、今後の対策を検討。

2．主な検討事項

① 電気通信事業者におけるサイバーセキュリティ対策とデータの取扱い等に係るガバナンス確保の今後の在り方

② 上記①を踏まえた、政策的な対応の在り方

③ その他

3．体制

- データ、サイバーセキュリティ及びガバナンスに関する有識者から構成される検討会（座長：大橋教授）を設置。構成員は右図のとおり。
- オブザーバとして、IT総合戦略室、内閣サイバーセキュリティセンター（NISC）、個人情報保護委員会事務局及び内閣官房国家安全保障局（NSS）が参加。

相田　仁	東京大学大学院工学系研究科教授
石井　夏生利	中央大学国際情報学部教授
上沼　紫野	虎ノ門南法律事務所弁護士
大橋　弘	東京大学公共政策大学院院長
後藤　厚宏	情報セキュリティ大学院大学学長
中尾　康二	（一社）ICT-ISAC顧問 （国研）NICTサイバーセキュリティ研究所主管研究員
中村　修	慶應義塾大学環境情報学部教授
古谷　由紀子	（公社）日本消費生活アドバイザー・コンサルタント・相談員協会監事
森　亮二	英知法律事務所弁護士
山本　龍彦	慶應義塾大学大学院法務研究科教授

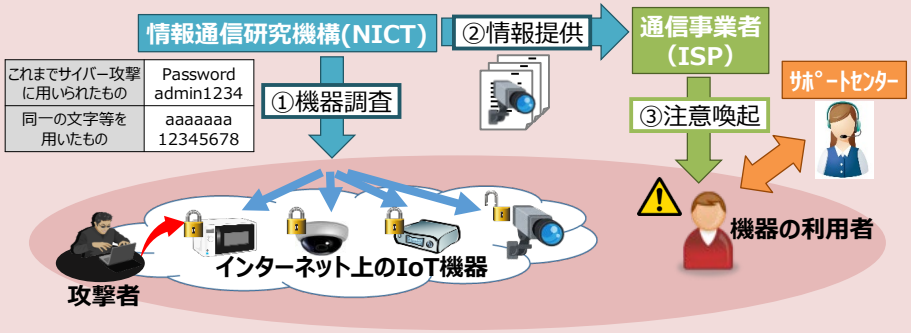
※第34回サイバーセキュリティTF資料34－1より抜粋

IoT機器調査及び利用者への注意喚起

- 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】

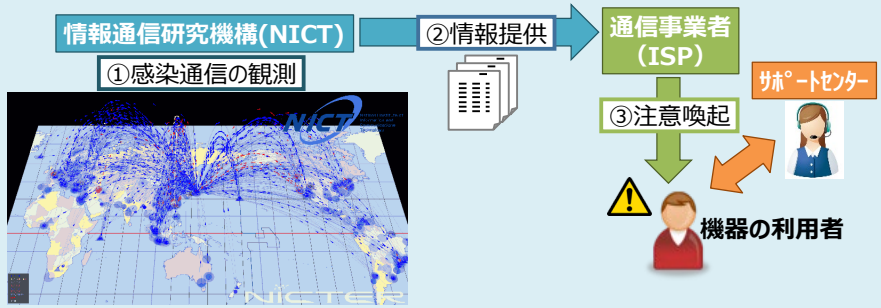


調査対象：パスワード設定等に不備があり、**サイバー攻撃に悪用されるおそれのある**IoT機器

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

IoT機器調査及び利用者への注意喚起の実施状況（2021年11月度）

- 参加手続きが完了している**ISP**（インターネット・サービス・プロバイダ）は**66社**。
  当該ISPの**約1.12億IPアドレス**に対して調査を実施。
- **NOTICE**による注意喚起は、**１，７３９件の対象を検知**しISPへ通知。
- **NICTER**による注意喚起は、１日平均**３７３件の対象を検知**しISPへ通知。

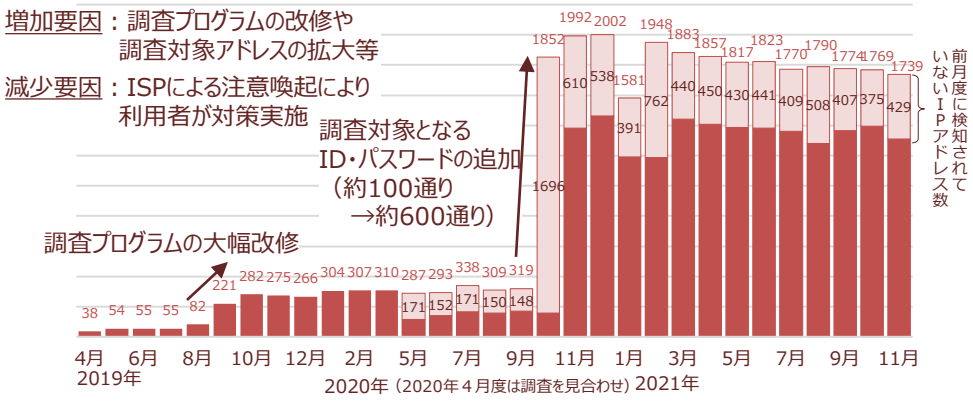
NOTICE注意喚起の取組結果

注意喚起対象としてISPへ通知したもの*

１，７３９件（10月度:1,769件）

（参考） 2019年度からの累積件数：29,392件
ID・パスワードが入力可能だったもの：9.5万件

*) 特定のID・パスワードによりログインできるかという調査をおおむね月に1回実施し、ログインでき、注意喚起対象となったもの（ユニークIPアドレス数）



NICTER注意喚起※の取組結果

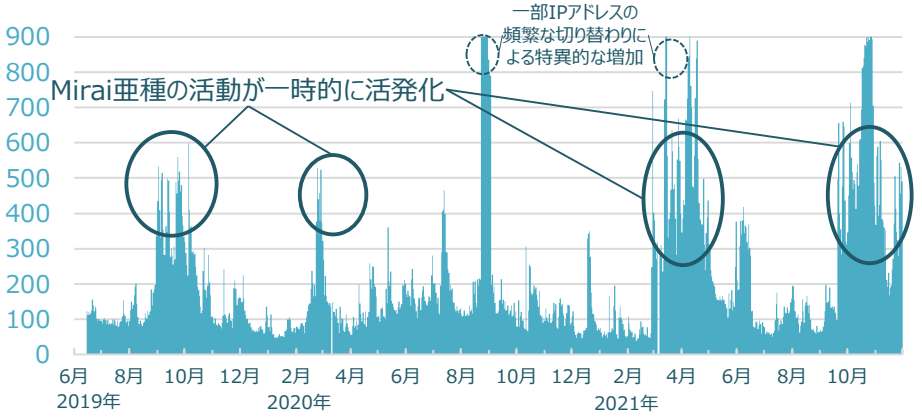
※マルウェアに感染しているIoT機器の利用者への注意喚起

注意喚起対象としてISPへ通知したもの**

１日平均３７３件（10月度:681件）

（参考） 期間全体での値： １日平均222件
最小：40件(2021/2/10)／最大：3,227件(2020/8/24)

**) NICTERプロジェクトによりマルウェアに感染していることが検知され、注意喚起対象となったもの（ユニークIPアドレス数）



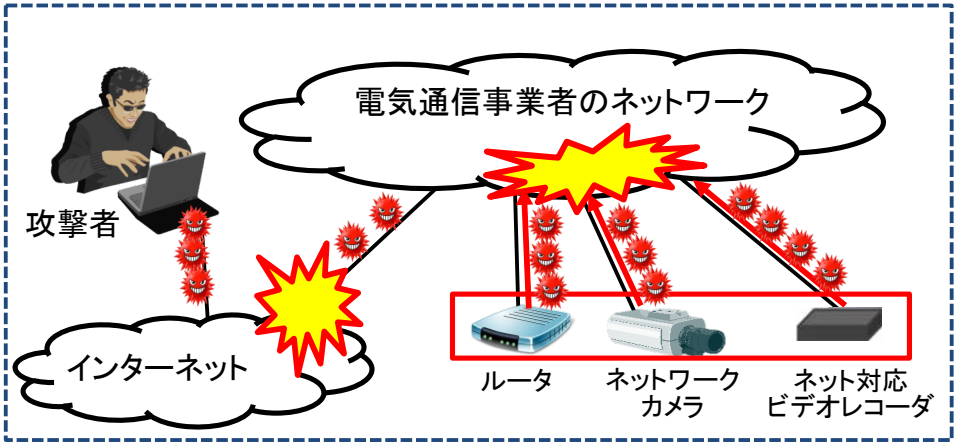
IoT機器のセキュリティ対策に関する技術基準の改正

【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。

【改正省令施行までの動き】

- 2020年４月１日の改正省令施行に向けて、2019年３月１日に改正省令公布、同年４月22日に改正省令の運用方法や解釈等を示したガイドラインを公表。これに加え、随時、周知や問合せ等に対応。

（一社）重要生活機器連携セキュリティ協議会（CCDS）認証プログラム

- 一般社団法人重要生活機器連携セキュリティ協議会（CCDS）は、**IoT機器のセキュリティ要件**を定め、2019年10月から認証プログラム（**民間の任意認証**）を開始。
- 認証の対象はソフトウェアを含むIoT機器で、認証されたものにはCCDS**マーク**（レベル１～３の３段階）を付与。
- マーク付与製品には**サイバー保険**が自動付帯され、インシデント発生時の原因調査等の費用を保険で保証。

IoTセキュリティ要件

✓IoT機器のセキュリティ要件を定義（適宜見直し）

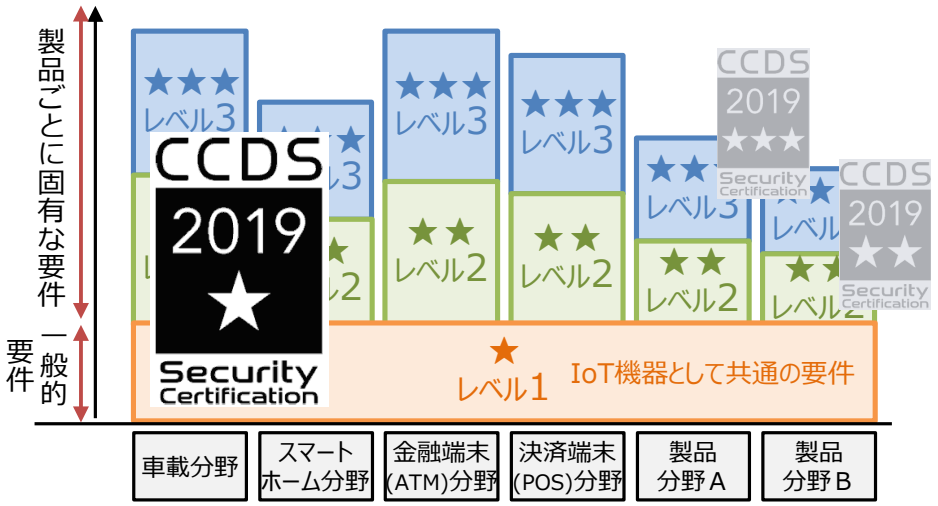
1 SQLインジェクション対応
2 クロスサイトサイトリクエストフォージェリ対応
3 パストラバーサル対応
4 不要なポートの閉塞
5 適切な認証・アクセス制御
（機器毎にユニークなID/パスワードでの管理等）
6 認証情報の設定変更が可能
（ID/パスワードをハードコーディングしない等）
7 廃棄やリユースを想定した機能実装
8 Wi-Fi Alliance推奨の最新の認証方式の実装
9 Bluetooth SIG推奨の最新のペアリング方式の実装
10 USBの不要なクラスを認識しない
11 ソフトウェアの更新が可能
12 脆弱性連絡窓口やサポートサイトの開設

（「IoT分野共通セキュリティ要件ガイドライン 2021 年版 Ver.1.0」より総務省作成）

認証プログラムのマーク（CCDSマーク）

✓利用者にも分かりやすいよう、★の数で対策レベルを表示

✓レベル１はIoT機器共通の要件、レベル２・３は分野別に策定



（CCDS記者発表会(2019年10月30日)資料より総務省作成）

【(一社)重要生活機器連携セキュリティ協議会（CCDS：Connected Consumer Device Security council について】

一般社団法人 重要生活機器連携セキュリティ協議会
Connected Consumer Device Security Council

- 民生機器を中心としたIoT機器やサービスのセキュリティ向上を目指す産学連携の協議会
- 生活機器に関する国内外の動向調査や、セキュリティ設計プロセスの開発等を実施
- 2014年に設立され、大学・企業・団体等の217会員（2021年2月時点）

放送設備に関するサイバーセキュリティ確保

■ 総務省において、令和2年3月に放送設備のサイバーセキュリティ確保に関する省令改正等を実施。

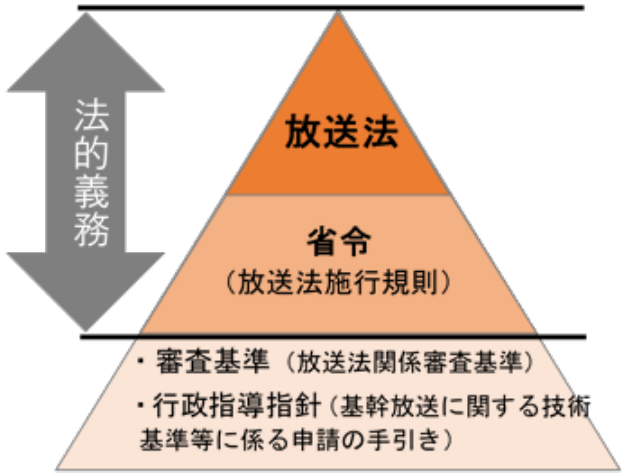
- 放送法第121条等において、放送設備の技術基準への適合を義務付け。
- 技術基準は、その発生を未然に防止するための措置及び発生した際の復旧を目指した措置として、設備故障、自然災害、停電その他の措置事項を省令（放送法施行規則）で規定。

・予備機器等
・故障検出
・試験機器及び応急復旧機材の配備
・機能確認
・誘導対策（アンテナからの電磁誘導影響への対策）
・耐震対策
・耐雷対策
・防火対策
・屋外設備
・収容する建築物
・停電対策
・宇宙線対策
・サイバーセキュリティの確保【追加】

- 令和2年3月に、放送法施行規則にサイバーセキュリティの確保の規定を追加。
（省令で規定される措置事項は計13項目となった）

（サイバーセキュリティの確保）
第百十五条の二　放送設備及び当該放送設備を維持又は運用するために必要な設備は、当該放送設備によつて行われる放送の業務に著しい支障を及ぼすおそれがないよう、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。以下同じ。）の確保のために必要な措置が講じられていなければならない。

※ 措置の具体的な内容については、放送法関係審査基準にその具体的措置を例示し、事業者ごとの対策内容を確認。



クラウドサービス提供における情報セキュリティ対策ガイドラインについて

■総務省では、安全・安心なクラウドサービスの利活用推進のため、2014年に「クラウドサービス提供における情報セキュリティ対策ガイドライン」を策定し、2018年に改定（第2版）。

■クラウドサービスを取り巻く環境の変化を踏まえ、クラウドサービスにおける責任分界のあり方や国際規格等との整合性の観点から、当ガイドラインの改定を検討し、2021年9月に「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」としてとりまとめた。

改定のポイント①

SaaS/PaaS/IaaSの特性や、クラウドサービス提供におけるクラウドサービス同士の相関性を踏まえた責任分界のあり方について追記

改定のポイント②

上述の責任分界に関する整理を踏まえ、

- ✓ SaaS/PaaS/IaaSを提供するクラウドサービス事業者で共通的に実施が求められる情報セキュリティ対策
- ✓ SaaSを提供するクラウドサービス事業者に実施が求められる情報セキュリティ対策
- ✓ PaaS/IaaSを提供するクラウドサービス事業者に実施が求められる情報セキュリティ対策

の3つのパターンに整理する形で当ガイドラインの章構成を見直し

改定のポイント③

国際規格（ISO/IEC27017:2016）やNIST SP800-53 rev.5において記載されているセキュリティ対策と整合性をとる形で、当ガイドラインに記載されているセキュリティ対策の内容を見直し

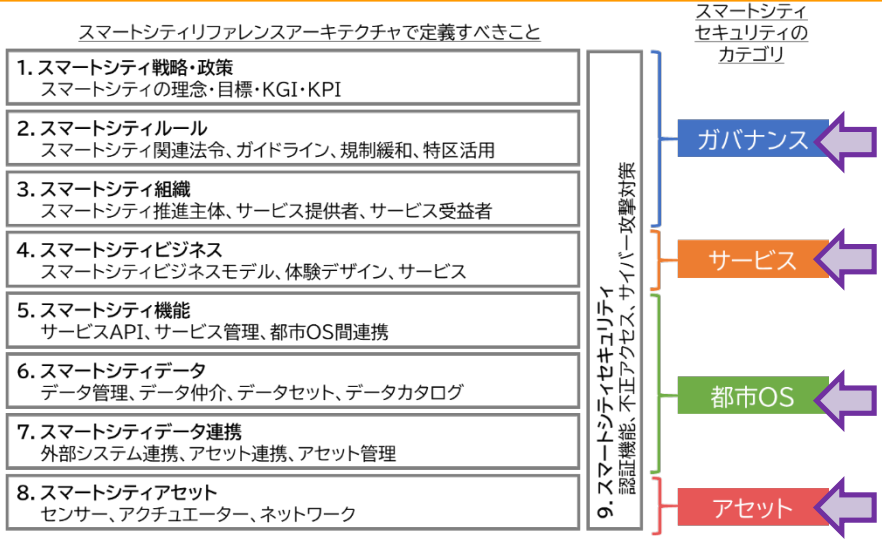
その他、上述の改定に伴い、読み手における読みやすさの観点で全体の構成を見直し

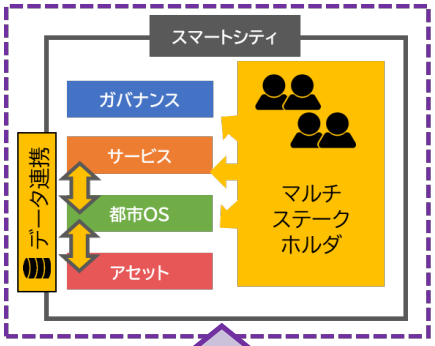
スマートシティセキュリティガイドライン（第2.0版）の概要

■「スマートシティセキュリティガイドライン」は、スマートシティの推進のための指針として、多様な関係主体が講じるべきセキュリティ対策や留意事項等を示したもの。令和２年10月に第1.0版を公表した後、内容のブラッシュアップを進め、令和３年６月に改定した第2.0版を公表。

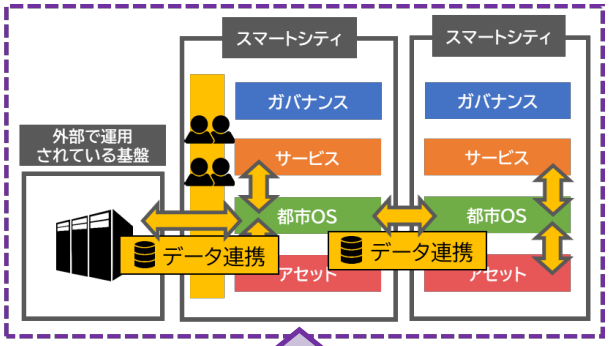
■ガイドラインでは、スマートシティの構成要素(※)をセキュリティの観点から４つのカテゴリ（＝ガバナンス、サービス、都市OS、アセット）に分類し、各カテゴリごとに想定されるセキュリティ上のリスクやセキュリティ対策を記載。（※:「スマートシティリファレンスアーキテクチャ」で定義されている各階層）

■また、「マルチステークホルダが複雑に関与」「多様なデータの連携」といったスマートシティの特徴を踏まえ、スマートシティ特有のセキュリティ対策を３つに分類して（＝適切なサプライチェーン管理、インシデント対応時の連携、データ連携時のセキュリティ確保）、リスクや具体的な対策を記載。





単体のスマートシティに着目した
セキュリティ検討



他のスマートシティや基盤との連携に着目した
セキュリティ検討

上述の４つのカテゴリそれぞれにおけるリスクやセキュリティ対策を記載

ガバナンス
- ✓ セキュリティに関するポリシー策定
- ✓ マルチステークホルダへのポリシー浸透
- ✓ ガバナンス維持のための取組

都市OS
- ✓ 外部からの攻撃等を防ぐセキュリティ対策
- ✓ インシデント発生防止のためのセキュリティ対策
- ✓ インシデント発生時に備えたセキュリティ対策
- ✓ 適切なクラウドサービスの利用

サービス
- ✓ それぞれのサービスにおけるリスクアセスメント
- ✓ 外部からの攻撃等を防ぐセキュリティ対策
- ✓ インシデント発生防止のためのセキュリティ対策
- ✓ インシデント発生時に備えたセキュリティ対策

アセット
- ✓ アセットの監視・管理
- ✓ アセットそのものへのセキュリティ対策

スマートシティの特徴を踏まえ、スマートシティ特有のセキュリティ対策として以下の３つに分類し、それぞれにおけるリスクやセキュリティ対策を記載

適切なサプライチェーン管理
- ✓ サプライチェーン全体のリスク・脆弱性情報の管理・把握
- ✓ 委託先のセキュリティ管理体制評価

インシデント対応時の連携
- ✓ インシデント対応体制の構築
- ✓ インシデント対応手順の整備
- ✓ インシデント対応訓練・演習の実施

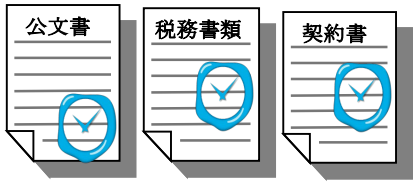
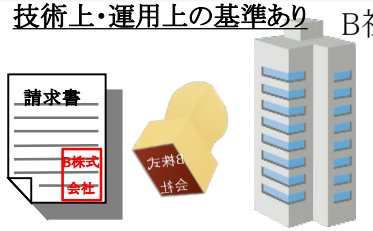
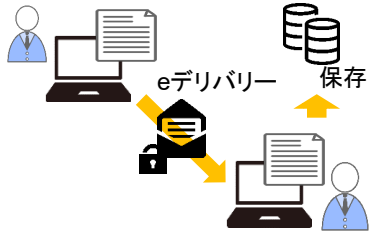
データ連携時のセキュリティ
- ✓ データ連携元・連携先のセキュリティ管理体制評価
- ✓ 認証とアクセス制御の実施
- ✓ データ利用時の透明性、信頼性の担保、匿名化・秘匿化
- ✓ APIのセキュリティ確保

■ その他、補助コンテンツとしてスマートシティセキュリティ導入チェックシートやリスク一覧、セキュリティ対策一覧などを掲載

■ 本ガイドラインをさらに読みやすくした「スマートシティセキュリティガイドブック」も本ガイドラインと同時に公表

トラストサービスの推進

- ✓ トラストサービスとは、インターネット上で本人であることやデータの正当性を証明することにより、送信元のなりすましや改ざん等を防止するための仕組みのこと。例えば、電子署名、タイムスタンプ、eシール、eデリバリー等がある。
- ✓ 各種トラストサービスの制度整備及びその普及に向けた取組を行うとともに、包括的データ戦略（令和3年6月18日閣議決定）において示された、トラスト基盤の検討（民間の保存書類の電子化を含む）の動向についてフォローを行い、連携を図る。

	① 電子署名 （意思を確認できる仕組み）	② タイムスタンプ （データの存在証明の仕組み）	③ eシール （文書の起源を確認できる仕組み）	④ eデリバリー （データの送達を保証する仕組み）
サービス内容	国の制度（電子署名法）有り  意思に係る文書	国の認定制度あり 	技術上・運用上の基準あり  事実・情報に係る文書	制度無し 
総務省の取組	令和3年9月1日のデジタル庁設置に伴い、電子署名法は同庁に移管。	**令和3年4月1日より国の認定制度が開始**。電子文書の送受信・保存において有効な手段になるよう、利用の拡大に向けた施策を実施。	技術上・運用上の基準等を整理した**「eシールに係る指針」を公表済**。利用の拡大に向けた検討。	日本での導入に当たっての**法的・技術的課題について検討**。

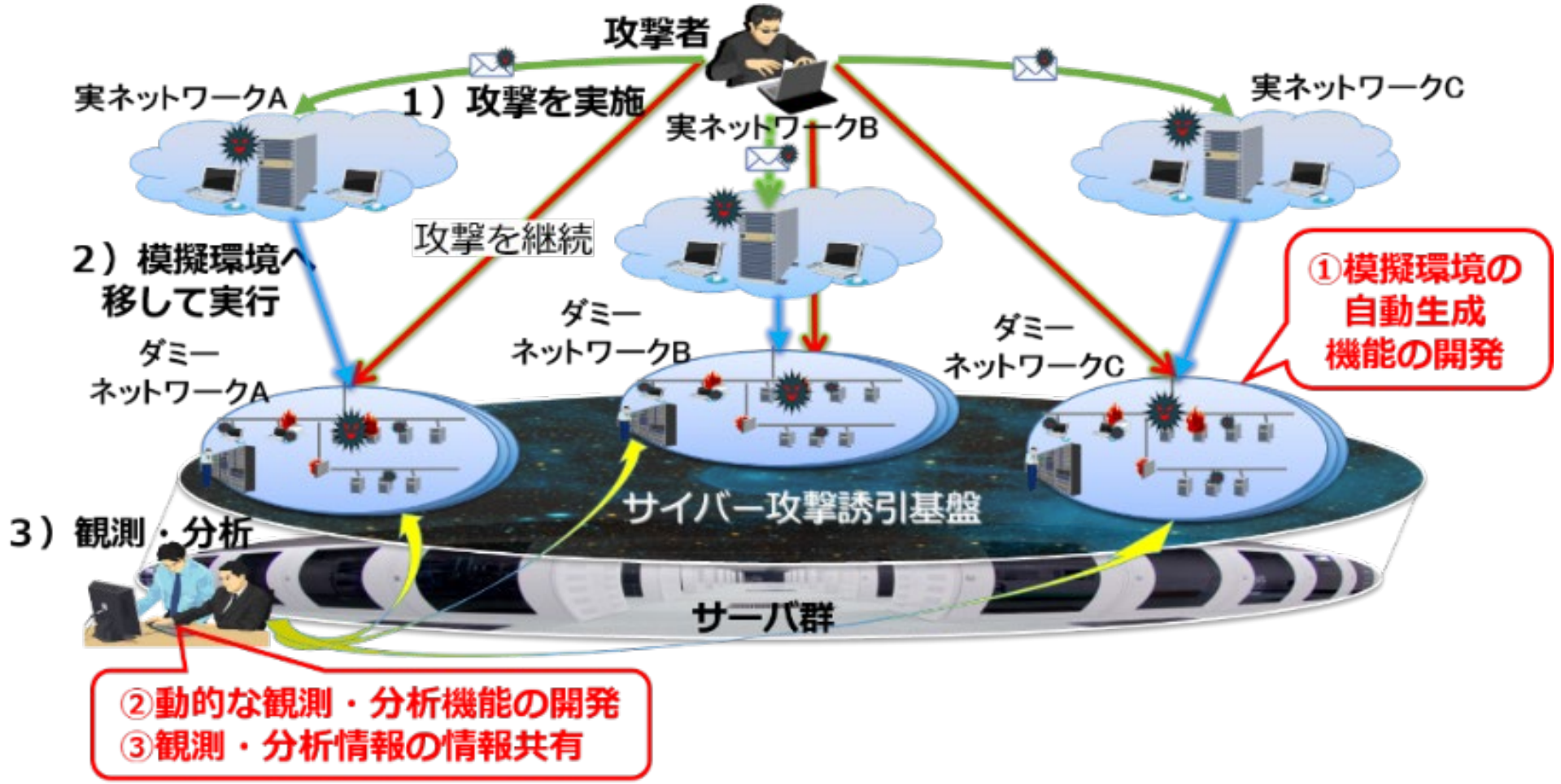
政府全体の取組

トラスト基盤の検討（民間の保存書類の電子化を含む）
＠デジタル社会推進会議　データ戦略推進ワーキンググループ

【２】研究開発

STARDUST（スターダスト） ～標的型攻撃対策～

- NICTでは、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（STARDUST）を構築。



電波の有効利用のためのIoTマルウェア無害化/無機能化技術等に関する研究開発

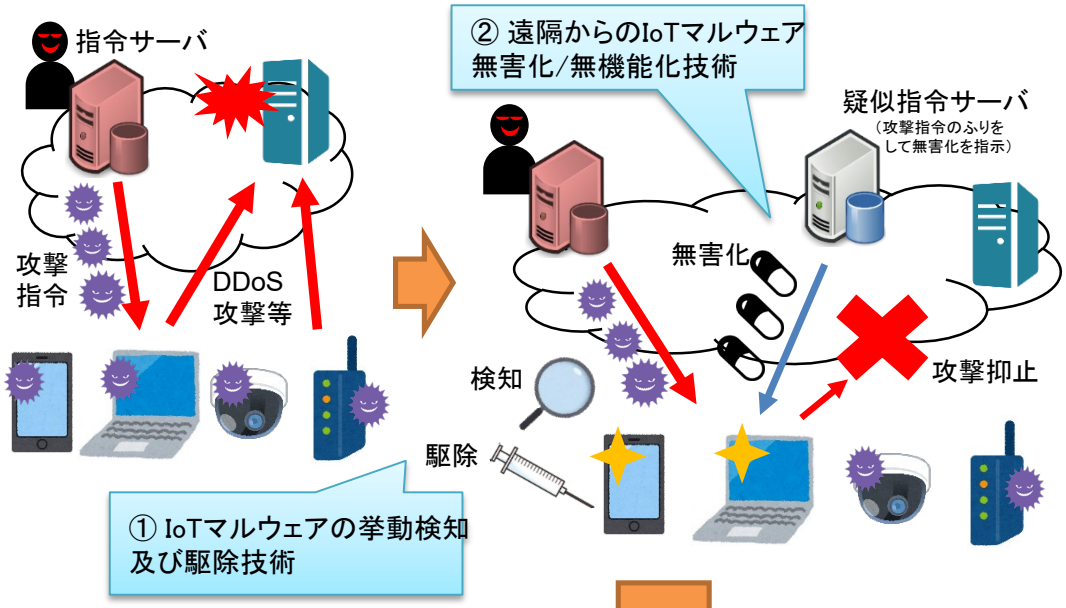
IoTの普及により、無線ネットワークに接続されるIoT機器が急速に増加している。これらがマルウェアに感染すると、大量の不要な電波を発生させ、無線リソースをひっ迫させるおそれがある。そのため、IoT機器に感染するマルウェアを検知し、遠隔から無害化/無機能化する技術等の研究開発を行い、マルウェア感染に起因する不要な電波の発射を抑制することにより、電波の有効活用を図る。

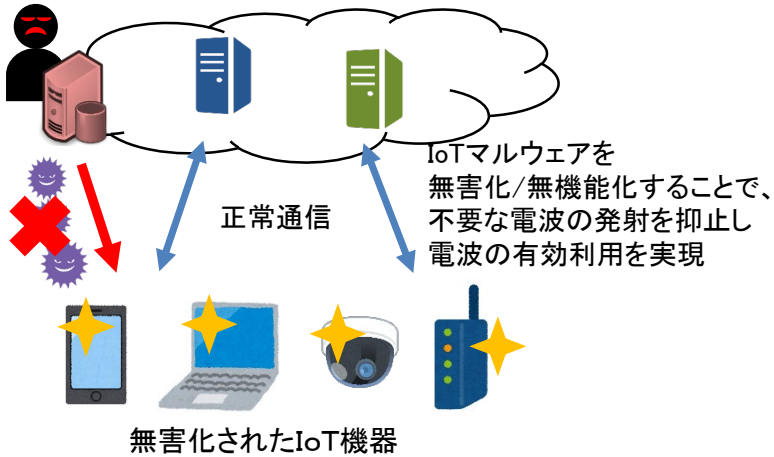
【背景・課題】

- 近年、センサーなどのIoT機器が急速に増加しており、これらがマルウェアに感染すると無線ネットワークに大量の不要な電波を発生させることから、無線リソースのひっ迫が懸念される。
- 多くのIoT機器は、メモリー等のリソースの制約等により十分なセキュリティ対策が行われないまま運用されている中、マルウェアに感染したIoT機器による不要な電波の発射を抑止することが喫緊の課題となっている。

【実施内容】

マルウェアに感染した不要な無線通信を抑止するため、①IoTマルウェアの挙動検知及び駆除技術、②遠隔からのIoTマルウェア無害化及び無機能化技術の研究開発を実施する。令和4年度は、これまでに開発した方式の改良を行った上で、社会実装に向けた実証を行う。





目標	マルウェアの攻撃挙動の解析を自動化し早期警戒情報として導出する技術、IoT機器に感染したマルウェアを無害化/無機能化する技術を令和4年度までに開発し、令和5年度までの実用化を目指す。マルウェアに感染したIoT機器からの不要な電波を抑止し、無線リソースひっ迫を低減することで、電波の有効活用を図る。
対象周波数帯	IoT機器の通信として利用される無線システムの周波数帯 （700MHz/800MHz帯、900MHz帯、920MHz帯、1.5MHz帯、1.7MHz帯、2GHz帯、2.3GHz帯、2.4GHz帯、2.5GHz帯、2.6GHz帯、3.4GHz帯、4GHz帯、4.5GHz帯、5GHz帯）
実施期間	令和2年度～令和4年度 （3か年）

安全な無線通信サービスのための新世代暗号技術に関する研究開発

5G等の高度化において、大規模量子コンピュータ等に解読されないよう、①LTEと同等の安全性を確保しつつ、超高速・大容量に対応した共通鍵暗号方式、②5G等の特性を損なわないよう、5G等のユースケースに応じた耐量子計算機暗号（PQC）への機能付加技術等を確立することで、無線通信リソースの効率的な利用環境を提供することにより、無線リソースのひっ迫を抑止し電波の有効利用を図る。

【背景・課題】

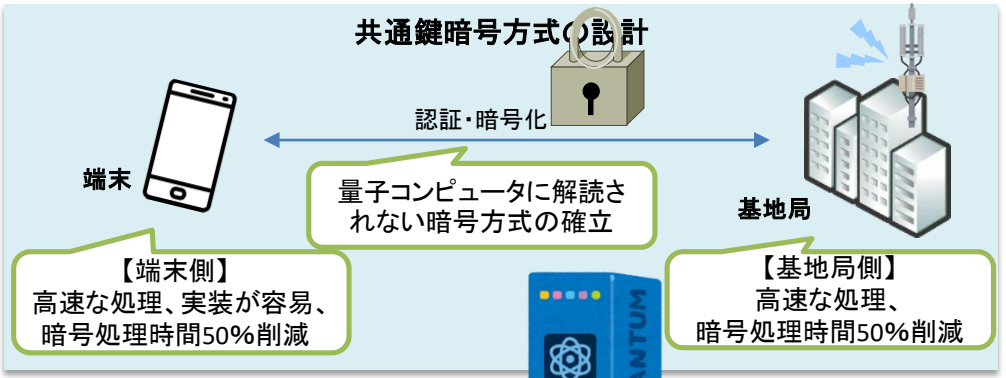
・大規模量子コンピュータ等が実用化されると、共通鍵暗号方式においては、LTEと同等の安全性を確保するためには鍵長を増加する必要があるが、スマートフォン等の限られた情報処理能力の中で5G等が求める高速・大容量に対応した暗号方式の設計が課題である。

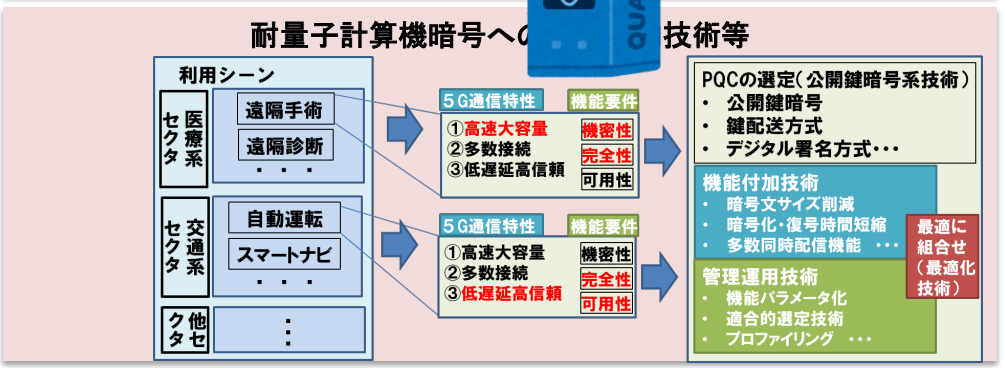
・また、公開鍵暗号方式においては、高速な解読が可能となるため、PQCへの移行が必要である。今後、複数の暗号方式が採用される予定であるが、5G等のユースケースに応じて最適化し、スマートフォン等の計算資源や通信量を抑えるようにPQCへの機能付加等が必要である。

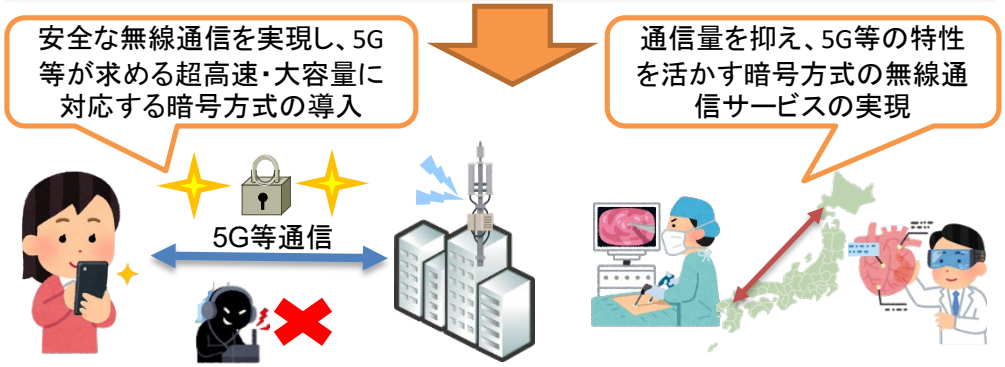
【実施内容】

大規模量子コンピュータ等に解読されないよう、①LTEと同等の安全性を確保するために鍵長を倍にしつつ、超高速・大容量に対応できる共通鍵暗号方式、②5G等のユースケースに応じ、通信データ量を抑え、PQCへの機能付加技術等を確立し、無線通信の効率的な利用環境を提供することにより、電波の有効利用を図る。

目標	超高速・大容量に対応する共通鍵暗号方式及びPQCへの機能付加技術等を令和6年までに開発するとともに、ISOや3GPP等の標準化団体に提案し、標準化策定に寄与することを目指す。
対象周波数帯	5G等のバンド：3.6GHz～4.6GHz、27.0GHz～29.5GHz、100GHz越の高い周波数帯
実施期間	令和3年度～令和6年度 （4か年）







【３】人材育成

実践的サイバー防御演習（CYDER）

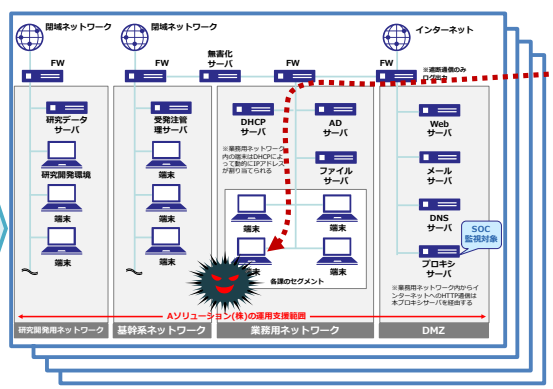
CYDER: CYber Defense Exercise with Recurrence

- 総務省は、情報通信研究機構(NICT)を通じ、**国の機関**、**指定法人**、**独立行政法人**、**地方公共団体**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**実践的サイバー防御演習(CYDER)**を実施。
- 受講者は、**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。**
- **全都道府県**において、年間**100回・計3,000名規模**で実施。 参加申込 → https://cyder.nict.go.jp
  ※2017年度：100回・3,009名／2018年度：107回・2,666名／2019年度：105回・3,090名／2020年度：106回・2,648名

演習のイメージ

我が国唯一の情報通信に関する公的研究機関である**NICTが有する最新のサイバー攻撃情報を活用**し、実際に起こりうる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。

北陸StarBED技術センターの大規模高性能サーバ群を活用



擬似攻撃者

企業・自治体の**社内LANや端末を再現**した環境で演習を実施

受講チームごとに独立した演習環境を**構築**

演習模様 **専門指導員**による補助

チーム内での議論を通じた相互理解

本番同様のデータを使用した演習

インシデント（事案）対処能力の向上

令和３年度の実施計画

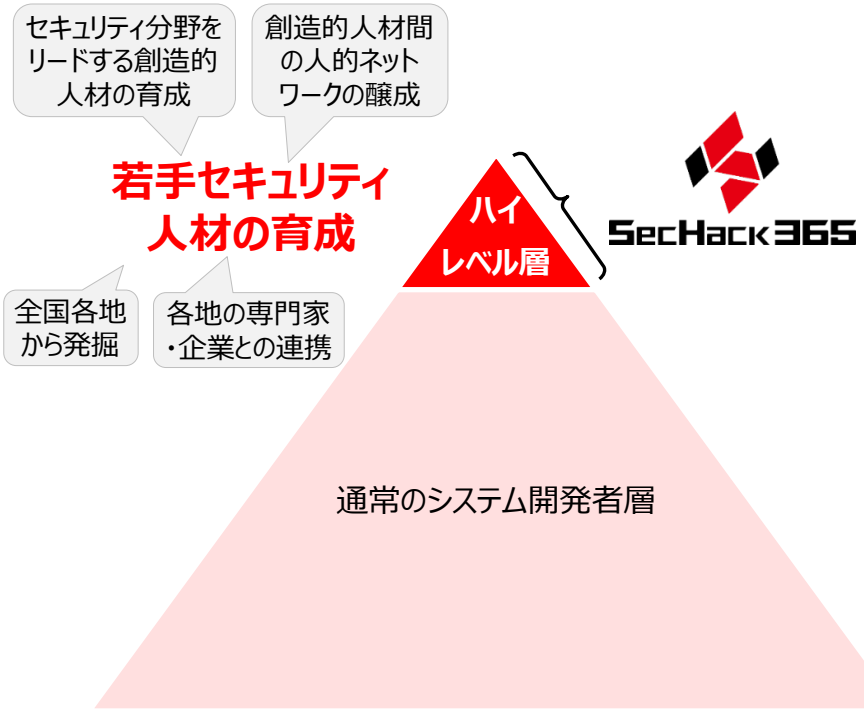
コース名	演習方法	レベル	受講想定者（習得内容）	受講想定組織	開催地	開催回数	実施時期
A	集合演習	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	４７都道府県	６５回	７月～翌年２月
B-1		中級	システム管理者・運用者 (主体的な事案対応・ｾｷｭﾘﾃｨ管理)	地方公共団体	全国１１地域	２１回	10月～翌年２月
B-2				地方公共団体以外	東京・大阪・名古屋・福岡	１３回	翌年１月～２月
C		準上級	セキュリティ専門担当者 (高度なセキュリティ技術)	全組織共通	東京	２回	翌年１月～２月
オンラインA	ｵﾝﾗｲﾝ演習	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	（受講者職場等）	随時	11月～翌年３月 （６～８月に試験提供）

令和３年度から**新規**開設

SecHack365

- 日本国内に居住する**25歳以下の若手ICT人材を対象**として、新たなセキュリティ対処技術を生み出しうる**最先端のセキュリティ人材（セキュリティイノベーター）**を育成。
- NICTの持つサイバーセキュリティの研究資産を活用し、実際のサイバー攻撃関連データに基づいたセキュリティ技術の研究・開発を、**第一線で活躍する研究者・技術者が１年かけて継続的かつ本格的に指導。**
  （2017年度:39名、2018年度:46名、2019年度:45名、2020年度:41名、合計171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。

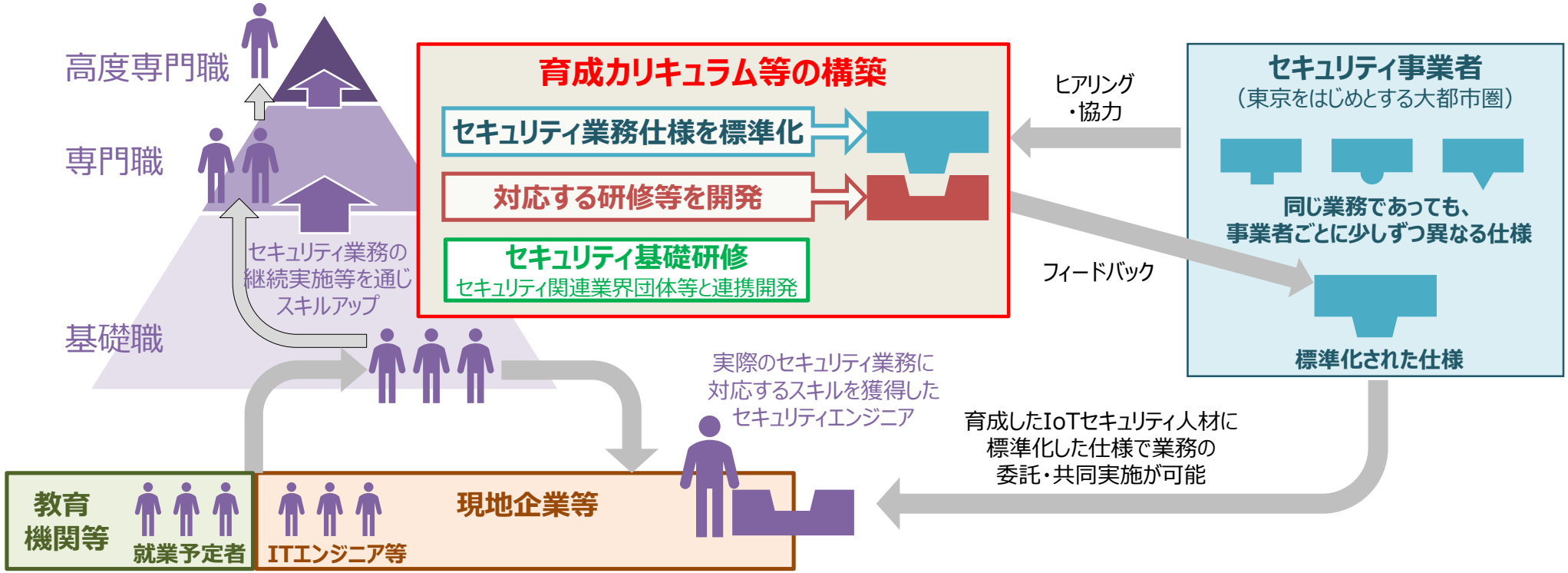
※ NONSTOP（NICTER Open Network Security Test-out Platform）では、NICTの長年にわたるサイバーセキュリティ研究によって得られた膨大なセキュリティ関連データを活用することができ、NONSTOP内に整備された様々な研究開発・解析用ツール類と、他では触れることのできない貴重なデータを用いて研究・開発に取り組むことが可能。



年６回の集合研修（座学講座等）、
成果発表会・OB交流会＋通年の遠隔開発実習
の組合せによる総合的な人材育成プログラム

地域におけるIoTセキュリティ人材の確保

- **地域コミュニティにおいてIoTセキュリティに関して活躍可能な人材を自立的に育成するエコシステムを構築。**
  - ✓ セキュリティ事業者ごとに異なる業務仕様を、業務ごとに標準化し、対応する研修等を開発。
  - ✓ 地方を拠点に、現地のITエンジニアや若年層に集中的に研修等を提供し、業務遂行できるスキルを身につけたIoTセキュリティエンジニアを育成。
  - ✓ セキュリティ事業者は、標準化した業務仕様に基づき業務委託が可能。
- **エコシステム構築に必要となる、育成カリキュラム等の育成モデルを構築する。**



【４】CYNEXの構築

サイバーセキュリティに関する産学官の結節点『CYNEX』

- 情報通信研究機構（NICT）では、これまでも次のような取組を実施
  サイバーセキュリティ研究室・・・最先端のサイバーセキュリティ関連技術の研究開発を実施
  ナショナルサイバートレーニングセンター・・・実践的サイバー防御演習等による人材育成を実施
- これらの知見を活用し、サイバーセキュリティに関する産学官の巨大な結節点となる先端的基盤として
  ＣＹＮＥＸ（CYbersecurity NEXus：サイネックス） を構築

【５】普及啓発

テレワークにおけるセキュリティ対策の推進

- 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**を示してきた。
  → テレワークを取り巻く環境やセキュリティ動向の変化に対応するため**2021年５月**に**全面的に改定**
- ガイドラインを補完するものとして、セキュリティの専任担当がいないような中小企業等においても、テレワークを実施する際に**最低限のセキュリティ**を**確実に確保**してもらうための**チェックリスト**についても策定。

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

テレワークセキュリティガイドライン
（2021年５月　第５版）

2004年12月初版
2006年４月第２版
2013年３月第３版
2018年４月第４版

- ✓ テレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針
- ✓ 中小企業を含む全企業を対象
- ✓ システム管理者のほか経営層や利用者(勤務者)を幅広く対象

ガイドラインに記載の内容について、
理解や検討が難しい場合

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)
（2021年５月　第２版）　2020年９月初版

中小企業等に向け**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

【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IT用語は聞いたことがあるレベル
- ✓ 設定作業は検索しながら実施可能

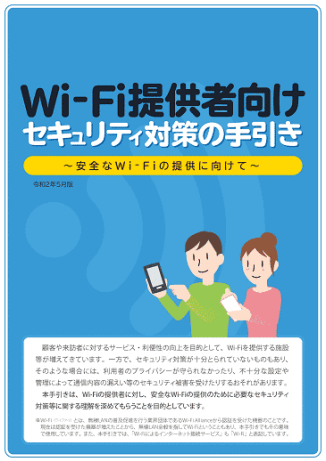
テレワークで活用される代表的なソフトについて、**設定解説資料**を作成し、具体的な設定を解説
【設定解説資料の対象】
CiscoWebexMeetings／Microsoft Teams／Zoom／Windows／Mac／iOS／Android／LanScope An／Exchange Online／Gmail／Teams_chat／LINE／OneDrive／Googleドライブ／Dropbox／YAMAHA VPNルータ／CiscoASA／Windowsリモートデスクトップ接続／Chromeリモートデスクトップ／Microsoft Defender／ウイルスバスター ビジネスセキュリティサービス

無線LANのセキュリティガイドライン

- 総務省では、無線LANの利用者・提供者向けにガイドラインを作成しており、周知啓発に活用。
- 新技術や最新のセキュリティ動向に対応するため、内容を見直し2020年５月に改定版を公表。
- 改定版については、Wi-Fi提供者（医療機関、宿泊施設、教育機関等を含む）等に幅広く周知。
  https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

「Wi-Fi利用者向け 簡易マニュアル」のポイント

- ✓ セキュリティ対策の訴求点を明確にするため、**セキュリティ対策のポイント**を**整理**
  - ① 接続する**アクセスポイント**を**よく確認**（偽アクセスポイント対策として接続URL等を確認）
  - ② 正しい**URL**で**HTTPS通信**をしているか**確認**（Wi-Fi暗号化等に関わらず通信内容を保護）
  - ③ 自宅に設置している**機器の設定**を**確認**（管理用パスワードの変更やファームウェアアップデート等）
- ✓ セキュリティ関連の**新技術**（WPA3、Enhanced Open等）を**紹介**



「Wi-Fi提供者向け セキュリティ対策の手引き」のポイント

- ✓ ガイドラインの対象者の明確化（**自店利用者のみへ提供する者も対象**）
- ✓ 近年懸念されている**偽アクセスポイント対策**（認証画面のURLの周知等）を追記
- ✓ 暗号化のための**パスフレーズを公開**している場合解読の**リスクが高まる**ことを明示
- ✓ 状況に応じたセキュリティ対策の選択と**利用者への周知**が必要であることを明確化
- ✓ セキュリティ関連の**新技術**（WPA3、Enhanced Open等）を**紹介**

地域に根付いたセキュリティコミュニティ（地域SECUNITY）の形成促進

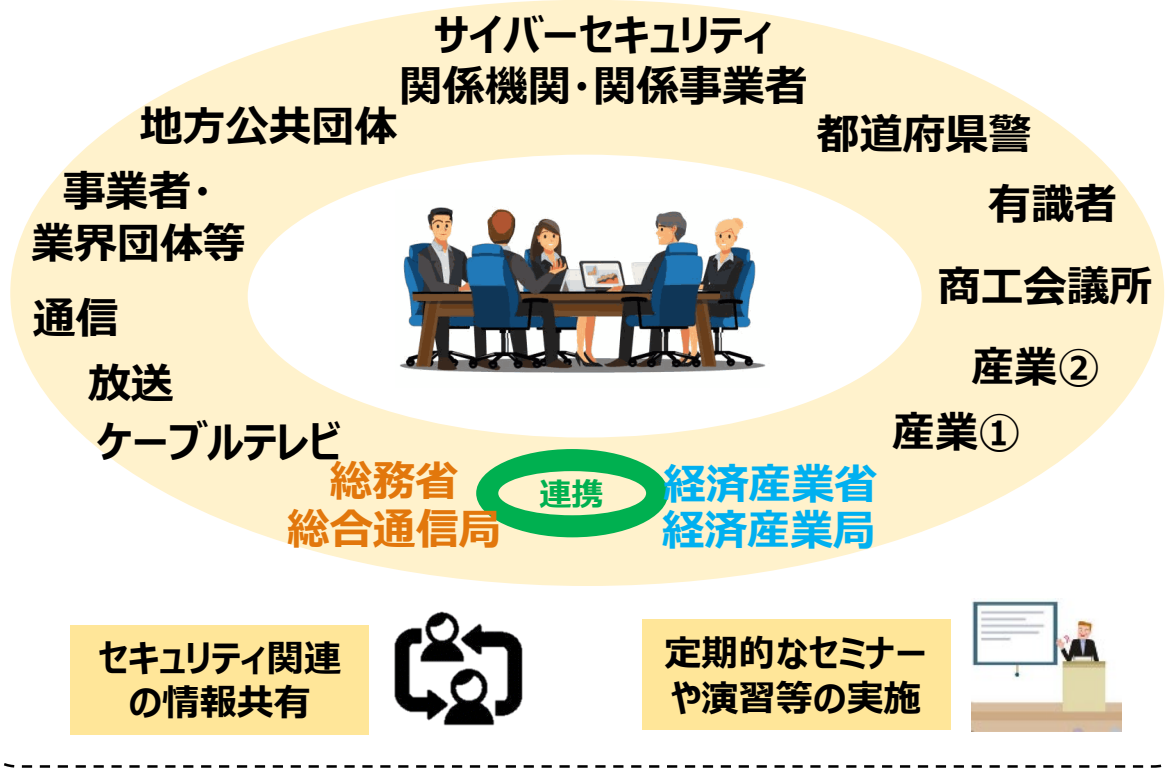
■ 総務省、経済産業省が互いに連携しつつ、地域単位の事業者のセキュリティ対策の強化のため、地域に根付いたセキュリティコミュニティ(地域SECUNITY)の形成の促進を図る。

● 全国規模で事業展開する企業に比べ、地域の企業や地方公共団体などについては、有効なサイバーセキュリティ対策をとるための人材育成・普及啓発の機会や情報共有の枠組みなどが不足しているおそれ。

➡

● 地域の企業や地方公共団体については、各者とも単独で有効なサイバーセキュリティ対策をとることは困難であり、地域レベルでの**<u>コミュニティを形成</u>**して情報共有等を強化する必要がある。

地域に根付いたセキュリティコミュニティ



セキュリティコミュニティの形成の促進

● ①当該地域における大手事業者、②業界団体（地方支部など）、③都道府県警、④サイバーセキュリティ関係事業者・機関、⑤地方公共団体、⑥有識者などによる地域のサイバーセキュリティ向上のための推進体制を構築する。なお、情報共有体制がすでに存在している地域においては、既存の体制を活用していくことが望ましい。

● 地域の企業等向けに①定期的なセミナーやインシデント演習※の実施、②セキュリティ関連の情報共有の枠組みなどを構築。

【６】国際連携

二国間連携

■ 現在、総務省が主催する各国とのICTに関する政策対話や外務省が主催するサイバー協議等において、総務省の主要なサイバーセキュリティ政策（IoTセキュリティ、５Gセキュリティ、能力構築支援等）について発信する一方、相手国におけるサイバーセキュリティ政策に関する説明を聴取しつつ、意見交換を行いながら、相手国政府との間での信頼醸成を推進。

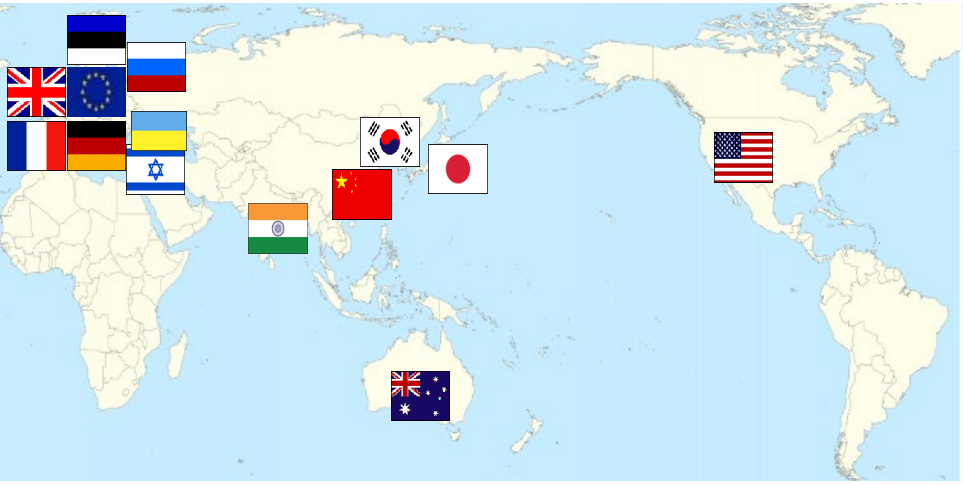
総務省が主催する主な国際会議

- 米国との「インターネットエコノミーに関する日米政策協力対話」、EUとの「日EU・ICT政策対話」及び「日EU・ICT戦略ワークショップ」等の二国間対話の場において、サイバーセキュリティに係る政策に関する意見交換を実施。
- 途上国地域を含むその他の二国間での対話の場においても、総務省の関連施策の紹介や民間情報共有活動に係る連携の促進等、具体的な協調関係を構築。

その他の主な国際会議

- 外務省が主催するサイバー協議・対話では、計13か国・地域との間で、年1回程度の頻度でサイバー空間に関する政府横断的な政策議論・対話を継続的に実施。

（参考）サイバー協議・対話の開催実績



開催国	英	印	米	EU	中・韓	イスラエル	仏	エストニア	豪	露	独	ウクライナ
2012年	○	○										
2013年			○									
2014年	○		○	○	○	○	○	○				
2015年			○		○			○	○	○		
2016年	○		○		○*	○	○		○	○	○	○
2017年		○	○	○	○	○	○	○	○			
2018年	○		○			○	○					
2019年		○	○	○	○		○		○	○		
2020年	○				○							○
2021年			○				○	○			○	

* 2016年は韓国との間での二国間協議を開催

多国間連携

- 多国間の枠組みであるOECD、国連GGE・OEWG、国連ITU-T、日米豪印首脳会議（Quad）等に積極的に参画し、サイバーセキュリティに関する政策的な協調や合意文書の作成等を実施している。

OECD/SDE

・経済協力開発機構 （OECD：Organisation for Economic Co-operation and Development）のデジタル経済政策委員会（CDEP）に設けられているデジタル経済セキュリティ作業部会（SDE：Working Party on Security in the Digital Economy)において、サイバーセキュリティ政策に関する議論を実施。2021年１月より、海野参事官がSDE副議長を務めている。

※2023年にセキュリティ関係のOECDイベントである「グローバルフォーラム」を日本（総務省）が事務局とともに主催する予定。

ITU-T/SG17

・ITU（国際電気通信連合）では、国際標準化を担うTセクタにおいてSG（Study Group）ごとに国際標準となる勧告を議論。SG17は「セキュリティ」を担当。

Quad

・日米豪印首脳会議における共同声明（2021年９月）に基づき、日米豪印シニアサイバーグループの立上げによるリーダーレベルの専門家の定期会合を実施。

日ASEANサイバーセキュリティ政策会議

経緯・目的

- 日本とASEAN諸国間の情報セキュリティ分野での連携・協力を進めるため、日本（NISC）主導で2009年2月に「日・ASEAN情報セキュリティ政策会議」を立ち上げ、以降毎年１回ペースで開催。（2017年10月の政策会議で「日・ASEANサイバーセキュリティ政策会議」に改称。）
- ASEAN 10か国、ASEAN事務局、日本が参加。NISC、総務省、経産省が主催。
- 2013年9月に「日・ASEANサイバーセキュリティ協力に関する閣僚政策会議」を開催。
- 2015年2月に政策会議下に「ワーキンググループ（WG）」を立ち上げ、「重要インフラ防護」、「サイバー演習」、「意識啓発」等をテーマとした協力活動を行っている。数次の体制変更を経て現在年に3回のWG会合を開催。

会議体

- **日・ASEANサイバーセキュリティ政策会議　（局長・審議官級）**
  - ✓ 情報セキュリティ分野におけるASEANとの協力枠組み等を議論・決定する。

※開催実績：
第１回(2009.2　東京)、第２回(2010.3　バンコク)、第３回(2011.3　東京)、
第４回(2011.11　クアラルンプール)、第５回(2012.10　東京)、第６回(2013.10　マニラ)、
第７回(2014.10　東京)、第８回(2015.10　ジャカルタ)、第９回(2016.10　東京)、
第10回(2017.10 シンガポール)、第11回(2018.10 東京)、第12回(2019.10 バンコク)
第13回(2020.10 オンライン)、第14回(2021.10 オンライン)、
第15回（2022.10　東京（予定））

第12回日ASEANサイバーセキュリティ政策会議模様

- **日・ASEANサイバーセキュリティWG会議　（課長級）**
  - ✓ 政府機関の情報セキュリティ対策についての具体的な協力活動を推進する。

※直近の開催実績・予定：
2020年：第1回(2020.2 シェムリアップ)、第2回(2020.6 オンライン)、第3回(2020.8 オンライン)
2021年：第1回(2021.2 オンライン)、第2回(2021.6 オンライン)、第3回(2021.9 オンライン)
2022年：第1回（2022･2マレーシア）、第2回（2022.3　ミャンマー）、第3回（2022.8　インドネシア）　※いずれも予定

日米のISAC連携の推進に関する取組

- 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、官民での情報共有に加え、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・連携を推進。

(*) 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連携ワークショップのこれまでの開催実績

- 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。併せて、公開シンポジウムも開催。
- 2019年11月： 第4回会合を開催。ICT-ISACと米国IT-ISACが協力に係る覚書に署名。
  (1) サイバー脅威とインシデント情報の共有
  (2) 脅威情報の共有を自動化する仕組みの構築に向けた協力
  (3) 両ISAC会員企業間での協力の促進
- 2020年１月： 2020年1月のPTC（太平洋電気通信協議会）においてフォローアップ会合を実施。
- 2021年4月： 第5回会合をリモートで開催。

（参考）2022年2月に第6回を開催予定。EUからの参加についても調整中。

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

第4回公開シンポジウム
パネルディスカッション（2019年11月）

米国以外の地域（EU等）との情報共有活動の促進

■ 民間情報共有組織におけるサイバーセキュリティ上の脅威情報や脆弱性情報の共有活動の一層の高度化等を図る観点から、米国以外の国・地域（EU等）との国際連携についても推進中。

■ 連携先として、ICT分野の民間情報共有組織が既に存在し、又は設立されつつある国・地域を選択し、総務省が相手国・地域の関係省庁を通じて調整を行っているところ。

目的

- 日本の民間情報共有組織における情報共有活動の高度化等に資する。
- 連携相手国との間でのサイバーセキュリティに関する協力関係の強化に資する。

これまでの主な取組

- 総務省が、EU等の関係機関に呼びかけ、官民参加型のワークショップを主催。先進的な取組ないし独自の取組を行っている海外のICT分野の民間情報共有組織と日本のICT-ISACとの間でのベストプラクティスの交換等による連携促進を図っている。

  -日EU International Workshop on Cybersecurity

  - 開催日：2021年９月14日（オンライン形式）
  - 出席者：日本側：総務省、NICT、ICT-ISAC、金融ISAC
    EU側　：DG-CONNECT、ENISA、FI-ISAC（金融ISAC）

今後の主な取組

- 今後、上記ワークショップを端緒としたEUとの連携（関係イベントへの相互参加の可能性等）を深める。

ISP向け日ASEAN情報セキュリティワークショップ

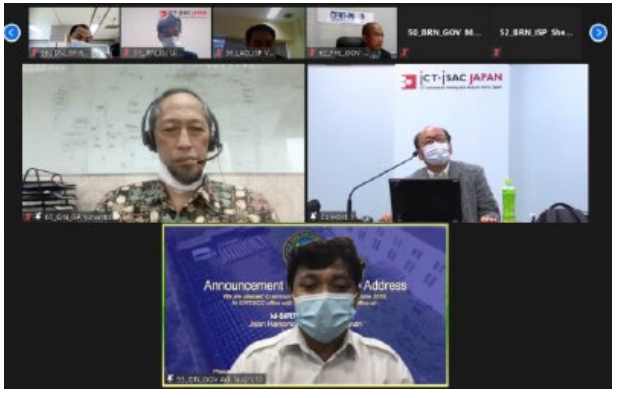
経緯・目的

- 日ASEAN情報セキュリティ政策会議（2010年3月）の結果を受け、総務省の主催により2011年1月に第1回を開催。基本的に年1回の頻度で開催しており、直近では2021年1月に第11回を開催。
- 日本とASEAN各国のISP事業者等におけるサイバーセキュリティ分野の取組状況の共有、意見交換及び人的ネットワークの維持・強化を目的としている。

開催実績・予定

#	開催時期	開催場所
第1回	2011年01月	日本（東京）
第2回	2012年03月	日本（東京）
第3回	2013年02月	タイ（バンコク）
第4回	2013年08月	日本（東京）
第5回	2014年10月	フィリピン（マニラ）
第6回	2015年12月	日本（東京）
第7回	2016年12月	タイ（バンコク）
第8回	2018年02月	日本（東京）
第9回	2019年01月	シンガポール
第10回	2019年12月	タイ（バンコク）
第11回	2021年1月	リモート
第12回	2022年1月	リモート

第10回ワークショップ模様



第11回ワークショップ(オンライン開催)の模様

AJCCBCにおけるASEANのセキュリティ人材育成

- AJCCBC（日ASEANサイバーセキュリティ能力構築センター）は、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（電子取引開発庁）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。

センターの主な活動内容

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

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

※2021年度は試行的に公開情報等分析（スレットハンティング）演習を実施するとともに、SOCアナリスト向け演習も実施予定

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

※これらに加えて、自主学習教材の開発・オンライン（eラーニング）提供も実施

日ASEAN情報通信大臣会合（2017年12月）

研修開催実績

- 2018年9月のセンター開所以来、約2ヶ月に1回のサイバーセキュリティ演習と年1回のCyber SEA Gameを開催。
- 2021年12月時点で計734名が参加。

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（2018-2022年の4年間で700人程度の育成を目標）

○今後、センターの活動に関する有志国等との連携（米国、英国、スイス等からの研修プログラムの提供・実施）を予定

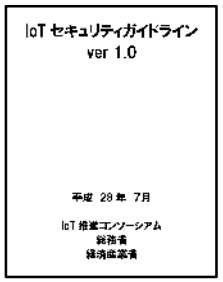
IoTセキュリティガイドラインの国際標準化

- IoT推進コンソーシアム・総務省・経済産業省が公表した「IoTセキュリティガイドラインver1.0（2016年7月）」の国際標準化に向け、ITU-T及びISO/IECにおける議論を継続中。

IoT Acceleration Consortium

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



ITU-T及びISO/IECに対して
国際標準化に向けた検討を提案

（主な標準化項目）
・IoTシステムのステークホルダー
・IoTシステムに係るリスク分析
・IoT機器のライフサイクル
・適切なセキュリティ管理手順　等

ITU

ISO JTC1 IEC
INFORMATION TECHNOLOGY STANDARDS

○2018年4月以降継続的にISO/IEC JTC1 SC27において議論されていた、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 27400）が、国際規格原案として承認され、現在最終勧告案化に向けた準備が行われている。

○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）として承認され、議論を継続中。

サイバーセキュリティソリューションの海外展開

実証事業概要

- 日本企業のサイバーセキュリティソリューション・製品等をASEAN諸国等に展開することを目的とした実証事業等を実施。
- 平成30年度事業：
  - ✓ セキュリティ対策に課題を抱えるASEAN諸国において、導入・運用が簡便かつ低コストであり、セキュリティ対策上の効果も高い技術の一つであるSD-WANを利用したセキュリティ共通基盤をクアラルンプール大学内に導入し、その効果を調査。
- 令和元年度事業：
  - ✓ 前度事業を契機に導入されたSD-WANセキュリティ共通基盤を活用し、アノマリー型エンドポイントセキュリティ製品と連携させた標的型攻撃対策ソリューションの導入効果を調査。
- 令和2年度事業：
  - ✓ マレーシア学術機関と連携し、BYOD端末の本人認証の強化及び本人認証に基づくネットワークアクセスポリシーとの自動連携による日本発のセキュリティ対策ソリューションの実証事業実施。
- 令和3年度事業：
  - ✓ ベトナム学術機関と連携し、セキュアなファイル授受によるセキュリティ対策ソリューションによる日本発のセキュリティ対策ソリューションの実証事業を実施中。

センター設立の記念セレモニー（平成31年3月）
（中央はクアラルンプール大学学長）

実証事業中間報告会（令和元年年12月）

対外活動・受賞歴

- **PERISA ‘19 【シルバー受賞】、及び、PECIPTA '19 【シルバー受賞】**
  - ✓ マレーシア教育省及びマレーシア財閥MARAグループ主催の技術イノベーションコンペティションにて、本事業を含むセキュリティソリューションの紹介を行い、シルバー受賞。
  - ✓ マレーシア教育省及び高等教育機関であるInstitution of Higher Learning主催の国際展示会においても同様に本事業の紹介を行い、シルバー受賞。
- **MEF 3.0 Proof of Concept Showcase ’19 【SD-WAN Implementation部門アワード受賞】**
  - ✓ ネットワーク技術の標準団体であるMEF(Metro Ethernet Forum)主催のShowcaseにて、本事業で用いたSD-WANセキュリティ共通基盤のデモ展示及び紹介を行い、SD-WAN Implementation部門アワード受賞。
- **NACSA-MIC Webinar for ASEAN “Cybersecurity in the New Normal”（2021年度）**
  - ✓ マレーシア国家サイバーセキュリティ局（NACSA）とウェビナーを共催し、産学官から数百名の参加を得て、両国企業による最新のサイバー脅威や技術動向やR2年度の実証について紹介。

PERISA/PECIPTA シルバー受賞

MEFアワード受賞

DAEDALUSの国際展開

- サイバー空間における攻撃の実態把握のための情報源の拡大、国際連携の推進等を目的として、NICTが運用するDAEDALUSのアラート提供に係る連携を有志国に呼びかけた。
- 現在、DAEDALUSのアラート提供に関する有志国との試行的連携を実施中。

＊ DAEDALUS（Direct Alert Environment for Darknet And Livenet Unified Security）とは、情報通信研究機構（NICT）が運用している大規模ダークネット観測網（NICTER）を用いて、組織内から送出される異常な通信を検知し、当該組織に対して迅速にアラートを送信するシステム。

目的

- 二国間のサイバーセキュリティ分野での協調関係の醸成（脅威認識の共有及び情報共有のための枠組みの構築）

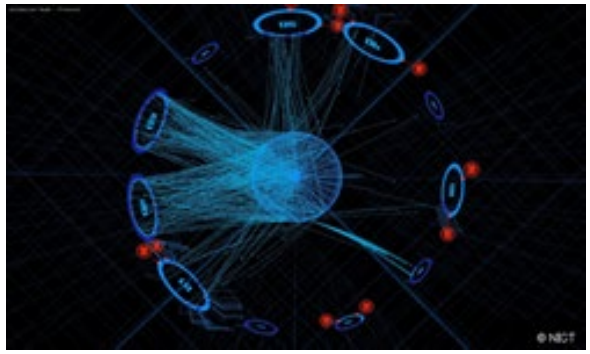
連携イメージ（案）

- 連携相手国においては、DAEDALUSに係る連携に必要な手続を行い、アラート情報をメールで適宜受信しつつ、既存のサイバーセキュリティ対策を強化させる。
- 日本側においては、連携相手国と情報交換を行い、サイバー空間の実態把握に役立てる。

日本側の体制・役割

総務省　：諸外国へのDAEDALUS提供の提案のための
　　協議の場の設置及び推進。
　　連携に関する問合せ窓口としても機能。
NICT　：DAEDALUSのシステム開発・運用を担当。

（参考）https://www.nict.go.jp/out-promotion/other/case-studies/itenweb/DAEDALUS.html



DAEDALUSの可視化エンジン

【７】情報の開示・共有等

サイバーセキュリティ対策情報開示の手引きの策定

■ 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情報開示の事例等をまとめた手引きを策定し、令和元年6月に公表。

背景

- ✓ サイバー攻撃が深刻化する中、民間企業においてサイバーセキュリティ対策は重要な経営課題となっているが、企業としての社会的責任を果たしステークホルダーからの信頼を得るためには、**サイバーセキュリティ対策の実施のみならず、その内容について適切な情報開示が重要。**

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。
- ✓ 民間企業にとって参考になり得るような**既存の情報開示の実例**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。

本編　サイバーセキュリティ対策情報開示の手引き

1．本手引きの趣旨・目的【内容】
- ✓ サイバーセキュリティリスクの増大と対策の必要性
- ✓ サイバーセキュリティ対策の情報開示の意義
- ✓ 本手引きの目的、想定参照主体、及び内容・構成等

2．情報開示の手段【内容】
- ✓ 代表的な開示書類の紹介

3．企業における情報開示の在り方【内容】
- ✓ 企業において実施されるのが望ましいサイバーセキュリティ対策
- ✓ 開示にあたってのポイントと記載例

4．今後の方向性について【内容】
- ✓ 手引きの改定の在り方等の今後の方向性

参考資料①　関連施策等の紹介

【内容】
- ✓ 本手引きに関連した様々な施策やガイドライン等について紹介

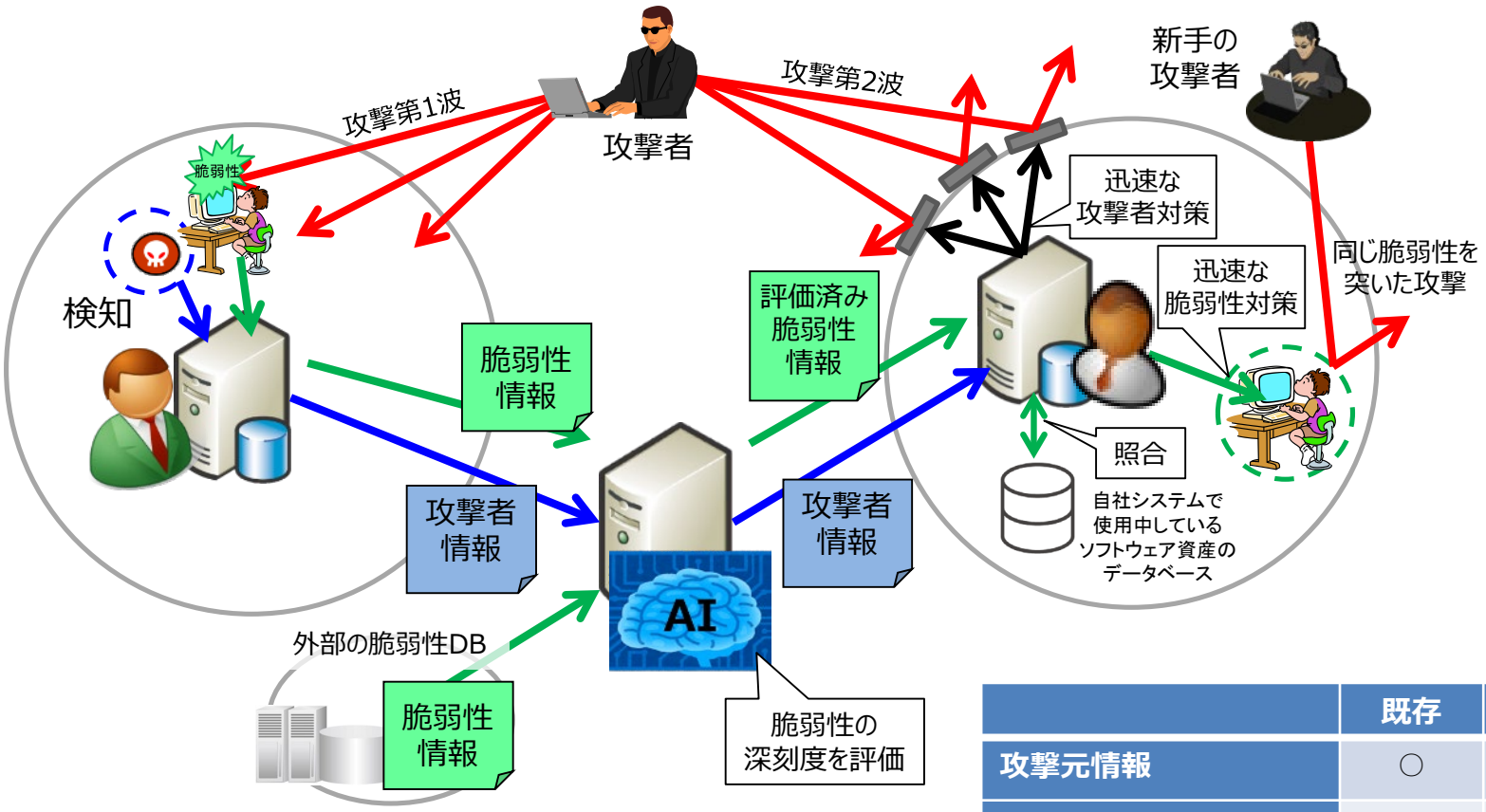
参考資料②　開示書類の事例集

【内容】
- ✓ サイバーセキュリティ対策の情報開示にかかる実際の開示書類の例について紹介

情報共有基盤の高度化～脆弱性情報の共有による対策の更なる迅速化～

○ 既存モデルでは、攻撃元の情報は共有されていたが、防御側の弱点である脆弱性情報は機械的な速度で共有できておらず、各組織のセキュリティ担当者が手作業で情報の収集や深刻度の評価、セキュリティパッチ適用の判断を行っている状態。

○ サイバーセキュリティ人材が不足している中、サイバー攻撃による被害が多発・深刻化している状況では、攻撃元情報に加え、脆弱性情報についても機械的速度で情報を共有し、深刻度の正確な把握と迅速な対処を行う、新たなモデルを確立する必要。



	既存	高度化
攻撃元情報	○	○
脆弱性情報	×	○+評価
ソフトウェア情報 紐付け	×	○

ICT-ISACの概要

概要

ICTに関わる幅広い企業・団体と協力連携し、安全なICT社会の形成に寄与するため、ICT分野全体のサイバーセキュリティに関する情報収集、分析及び対応について情報共有し、対処を実施。

活動内容

１．サイバーセキュリティに関する情報収集・調査・分析
ICTに関わる情報セキュリティ対策に資する情報（インシデント情報を含む。）を収集、調査、分析する活動

２．会員間の情報共有と共同対処
情報セキュリティに関する情報を目的に応じて共有し、それを活用しつつ会員企業間で相互協調する仕組みを整備しそれを促進する活動

３．セキュリティ人材の育成、セキュリティ啓発
会員企業のセキュリティ人材育成を促進する活動及びユーザが安全にICTを利用するための普及啓発活動

４．セキュリティガイドライン等の整備に関する活動
会員各社がセキュリティ対策を円滑に行う上で必要となるガイドラインの検討及び法制度に関する政府研究会等への参画活動

５．認定送信型対電気通信設備サイバー攻撃対処協会としての活動
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

役員

理事長：齊藤　忠夫（東京大学名誉教授）　　理事：澁谷　直樹（日本電信電話㈱）、田中　孝司（KDDI㈱）　　監事：向井　健太郎（富士通㈱）

会員企業

計43社（令和3年12月時点）

【通信系】日本電信電話㈱、KDDI㈱、エヌ・ティ・ティ・コミュニケーションズ㈱、㈱インターネットイニシアティブ、㈱NTTドコモ、㈱オプテージ、ソニーネットワークコミュニケーションズ㈱、ソフトバンク㈱、東日本電信電話㈱、西日本電信電話㈱、ニフティ㈱、ビッグローブ㈱、インターネットマルチフィード㈱、エヌ・ティ・ティ・データ先端技術㈱、㈱KDDI総合研究所、エヌ・ティ・ティ・エムイー㈱、㈱QTnet、㈱日本レジストリサービス、アルテリア・ネットワークス㈱、㈱朝日ネット、日本ネットワークイネイブラー㈱、楽天モバイル㈱、中部テレコミュニケーション㈱

【放送系】日本放送協会、㈱TBSテレビ、㈱テレビ朝日、㈱テレビ東京、㈱フジテレビジョン、日本テレビ放送網㈱、JCOM㈱

【SI･ベンダ系】沖電気工業㈱、㈱日立製作所、日本電気㈱、富士通㈱、㈱東陽テクニカ

【セキュリティベンダ系】NRIセキュアテクノロジーズ㈱、NTTセキュリティ・ジャパン㈱、㈱FFRI、㈱カスペルスキー、トレンドマイクロ㈱、㈱サイバーディフェンス研究所、パロアルトネットワークス㈱、KDDIデジタルセキュリティ㈱

※オブザーバ：総務省、（国研）情報通信研究機構（NICT）、（一社）日本インターネットプロバイダー協会（JAIPA）、（一社）テレコムサービス協会、（一社）電気通信事業者協会（TCA）、（一財）日本データ通信協会、（一社）日本民間放送連盟、（一社）日本ケーブルテレビ連盟