資料12－１

IoTセキュリティ総合対策の主な取組の進捗状況等について

総務省　サイバーセキュリティ統括官室

IoTセキュリティ総合対策の具体的な施策について

(1) 脆弱性対策に係る体制の整備

① セキュリティ・バイ・デザイン等の意識啓発・支援の実施
② 認証マークの付与及び比較サイト等を通じた推奨
③ IoTセキュアゲートウェイ
④ セキュリティ検査の仕組み作り
⑤ 簡易な脆弱性チェックソフトの開発等
⑥ 利用者に対する意識啓発の実施や相談窓口等の設置
⑦ 重要IoT機器に係る脆弱性調査
⑧ サイバー攻撃の踏み台となるおそれがある機器に係る脆弱性
⑨ 被害拡大を防止するための取組の推進
⑩ IoT機器に関する脆弱性対策に関する実施体制の整備

スライド４
スライド２、３

(2) 研究開発の推進

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

スライド５

(3) 民間企業等におけるセキュリティ対策の促進

① 民間企業のセキュリティ投資等の促進
② セキュリティ対策に係る情報開示の促進
③ 事業者間での情報共有を促進するための仕組みの構築
④ 情報共有時の匿名化処理に関する検討
⑤ 公衆無線LANのサイバーセキュリティ確保に関する検討

スライド６

(4) 人材育成の強化

① 実践的サイバー防御演習（CYDER）の充実
② 2020年東京大会に向けたサイバー演習の実施
③ 若手セキュリティ人材の育成の促進
④ IoTセキュリティ人材の育成

スライド７

(5) 国際連携の推進

① ASEAN各国との連携
② 国際的なISAC間連携
③ 国際標準化の推進
④ サイバー空間における国際ルールを巡る議論への積極的参画

スライド９
スライド８
スライド１０
スライド８

（１）⑥⑦⑧⑨⑩ IoT機器調査及び利用者への注意喚起の取組

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

※National Operation Towards IoT Clean Environment

＜本取組の概要＞

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

（イメージ図）

※ 利用者からの問合せ対応等を行うサポートセンターを設置

（１）⑥⑦⑧⑨⑩　NOTICEに係る周知広報

- サポートセンターを設置し、ウェブサイトや電話による問合せ対応を通じて利用者に適切なセキュリティ対策等を案内。消費生活センター等と連携し対応。
- IoT機器のセキュリティ対策の必要性、本取組の内容の広報のため、公共機関等でのポスター掲示に加え、新聞広告、交通広告等を2月中旬から実施。

＜周知ポスター＞

＜サポートセンター＞

（ウェブサイト）

- 専用ホームページ（https://notice.go.jp）を開設
- コールセンターにより電話での問合せ対応
  受付時間：10:00～18:00（年末年始除く）
  0120－769－318（無料・固定電話のみ）
  03－4346－3318（有料）

＜駅構内サイネージ広告＞

（全国主要39駅）

＜駅構内ポスター掲示＞

（東京メトロ10駅）

＜電車中吊広告＞

（JR山手線等・東京メトロ全線）

＜新聞広告＞

＜テレビニュースでの報道＞

（１）① IoT機器のセキュリティ対策に関する技術基準の改正

- 今後製品化されるIoT機器がパスワード設定の不備等により悪用されないようにする対策として、IoT機器の技術基準※1にセキュリティ対策を追加するための省令改正を行う※2。

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

※2 IoT機器のセキュリティ対策の内容は、情報通信審議会等に諮問して検討を実施（2018年2月～2019年1月）。

【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。

【スケジュール】

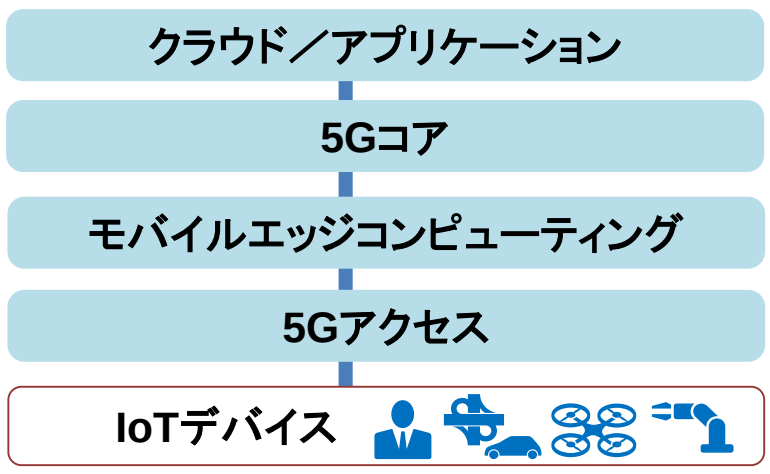
- 本年３月１日に改正省令を公布。来年（2020年）４月１日に改正省令を施行。
- 改正省令の運用方法や解釈等を定めるガイドラインも策定予定（本年４月目途）。

（２）①　5Gネットワークのセキュリティ確保に向けた体制整備と周知・啓発

第５世代移動通信システム（５G）は、IoTシステムの基盤技術であるため、５Gに係る各構成要素（デバイス、クラウド、アプリ等）におけるセキュリティを総合的かつ継続的に担保する仕組みを整備し、対策の共有等を図ることを通じ、５Gを活用する重要インフラ事業者等への周知・啓発を図る。

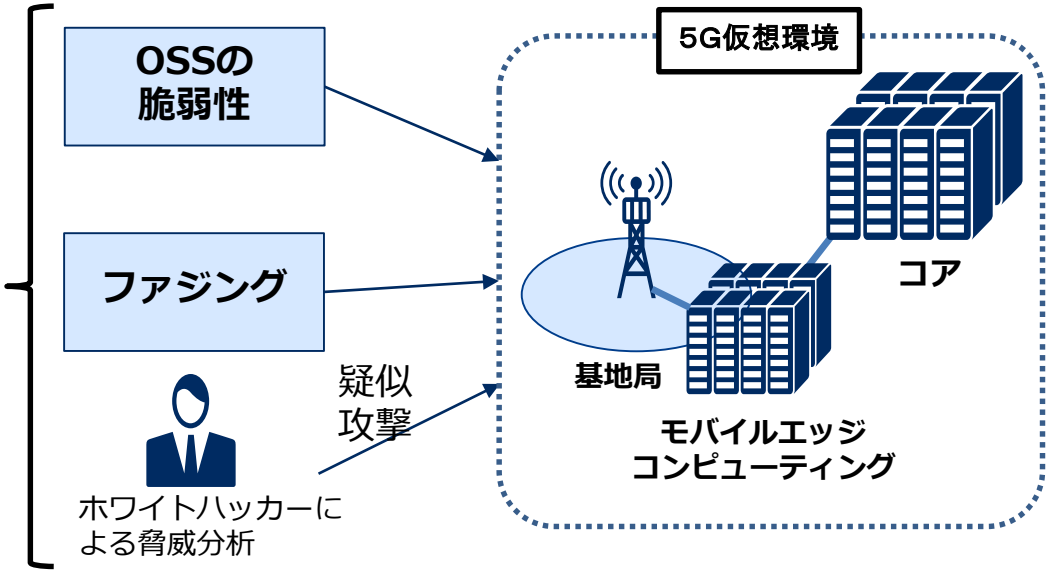
＜基本的考え方＞

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



＜平成31年度実施内容＞

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



（３）② サイバーセキュリティ対策情報開示の手引きについて（案）

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

目的

- ✓ 民間企業による**サイバーセキュリティ対策**やその対策の**情報開示の重要性**の認識を促進する。
- ✓ 他方、サイバーセキュリティ対策の具体的な実施状況の開示がサイバー攻撃を誘発するリスクがあることに鑑み、民間企業にとって参考になり得るような**既存の開示の実例**を**事例集として**示す。

活用主体

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

対象とする情報開示

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

内容

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

（４）④　地域におけるサイバーセキュリティ人材育成に関する取組

■ 平成30年12月より、タスクフォースの下のサイバーセキュリティ人材育成分科会において、地方におけるサイバーセキュリティ人材の育成に関する課題を整理し、その在り方について検討を実施してきたところ。

【サイバーセキュリティ人材育成分科会第一次とりまとめ骨子案の概要】

現状と課題	取組の方向性
	① 地域におけるセキュリティファシリテータの育成
○　中小企業のセキュリティ意識が低く、サプライチェーンの一端を担う地域の中小企業がリスクとなるおそれがあり、セキュリティ意識の向上が必要。 ○　地方では研修機会が少なく、機会があっても参加しない。	○　地方でのサイバーセキュリティ研修機会の拡大やインセンティブの創出。 ○　地域単位での共助の仕組みを構築し、地域のセキュリティファシリテーターを育成。 ⇒　候補者向けカリキュラムやテキスト、ツール等の作成
	② 地域でのセキュリティ人材のシェアリング
○　セキュリティ担当者がいる中小企業は全体の半数弱で、また、存在する場合もその大半は兼任。 ○　サイバーセキュリティ体制がない組織では対策が進まない傾向にある。	○　自社の状況に合わせて、地域の情報化やセキュリティのスキルを有する人材をマッチングする仕組みを構築。 ○　複数の企業・組織で必要なスキルを有する人材をシェアする仕組みを構築。 ⇒　地域単位でスキルごとに人材をデータベース化
	③ 地域における人材エコシステムの形成
○　地域にセキュリティ人材の受け皿がなく、地域で若手人材が育たない・定着しないといった悪循環が存在。 ○　国全体のサイバーセキュリティ人材不足から、地域の中小企業のペネトレーションテスト等の一部の業務にまでセキュリティベンダの手が回らない。	○　雇用の受け皿と研修・演習機会の創出による地域での人材エコシステムの形成。 ○　民間等と連携した実践的な人材の育成。 ⇒　地域単位でスキルごとに人材をデータベース化 ○　大学（院）や高専等と連携することで、ハイエンドな業務も含めて地場産業化し、沖縄をはじめとする地域の高度な人材エコシステム形成も期待。

（５）①④　サイバーセキュリティに関する国際連携の推進

サイバー空間には国境がないため、サイバー攻撃への対処については、各国間での情報共有や人材育成等の連携が重要。

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

● 日ASEAN統合基金を活用したASEAN域内のセキュリティ人材育成プロジェクト（４年間で650人程度）。2018年9月にタイで開所。

■ プロジェクト概要

1. サイバーセキュリティ演習

政府機関・重要インフラ事業者等に対し、以下の演習プログラムを実施（年6回）

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（年１回）

イスラエルとのサイバーセキュリティ分野における協力覚書締結

● 2018年11月29日、総務省はイスラエル国家サイバー総局との間にサイバーセキュリティ分野における協力覚書を締結。

■ 協力分野

（1）サイバーセキュリティ政策に関する情報交換
（2）研究開発
（3）人材育成

ベンアリ駐日イスラエル大使と石田総務大臣による覚書締結式（2018.11）

（５）② 日米のISAC連携について

複雑化・高度化が進むサイバー空間の脅威に対応するためには、官民での情報共有や国際連携の強化が重要。
総務省では、サイバー脅威に対する国内通信インフラ事業者の対処能力向上を目的として、日米の情報通信分野ISAC(*)組織間における情報共有・連携の促進を支援。

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

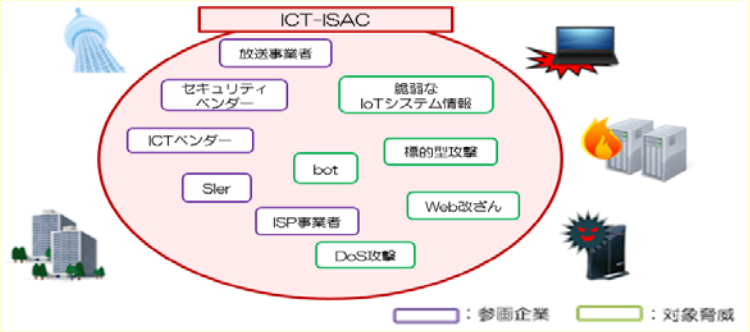
■ 日米ISAC連携の取組

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

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

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

「ICT-ISAC Japan」の概要



ICT-ISAC JAPAN
ICT Information Sharing and Analysis Center Japan

〈正式名称〉（一社）ICT-ISAC
〈 理事長 〉 齊藤忠夫
〈会員企業〉通信事業者、放送事業者、ICTベンダー、セキュリティベンダー等を含む計40社

（５）③ トラストサービスに関する検討

■ 総合通信基盤局長とサイバーセキュリティ統括官の共同開催による「プラットフォームサービスに関する研究会」の下に「トラストサービス検討ワーキンググループ」を設置し、**ネットワークにつながる人・組織・モノの正当性を確認できる仕組みの確保やデータの完全性の確保等を実現するためのトラストサービスの制度化に向けた検討**を実施。

トラストサービスのイメージ

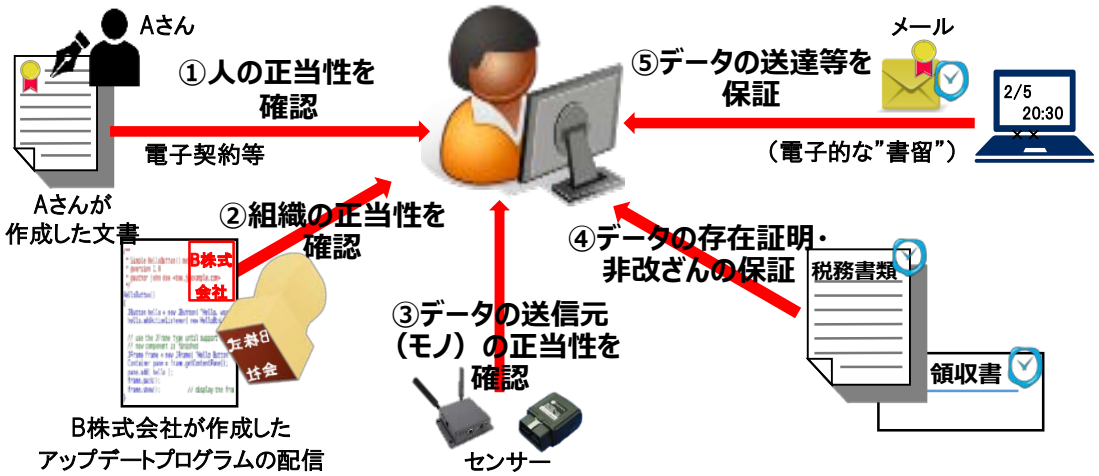
① **人の正当性**を確認（利用者認証、リモート署名）

② **組織の正当性**を確認
（組織を対象とする認証、ウェブサイト認証）

③ IoT機器等の**モノの正当性**を確認

④ **データの存在証明・非改ざんを保証**
（タイムスタンプ）

⑤ **データの送達等を保証**（eデリバリー）



現状と課題の例

➤ 我が国には、EUのeIDAS規則に相当する**トラストサービスを包括的に規定する法令が存在しない**（電子署名法のみ存在）。

⇒ **電子署名のクラウド環境下での利用への対応**

・ 近年のクラウドの急速な普及に伴い、電子署名に関してもクラウドを介して電子証明書（鍵）を利用するリモート署名へのニーズが高まっており、その実現のための制度設計が求められている。

⇒ **長期にわたって電子的な記録の真正性を確保するための仕組みの構築**

・ 住宅ローンの契約書の保存（最大35年）等、長期にわたって文書の保存が求められる場合には、真正性の確保のためにタイムスタンプの活用が有効。一方、タイムスタンプについては、法的な裏付けがないことからユーザが採用を見送り、紙による文書保存を継続して、業務の電子化・効率化が進展しないケースが多数存在。タイムスタンプの制度化が求められている。

⇒ **Society5.0に対応した組織やモノを認証する仕組みの構築**

・ 電子署名法等に基づく電子認証制度は、ヒト（法人の代表者等）に対して電子証明書を発行する仕組みであり、Society5.0の時代では、組織やモノの正当性、また、それらから発信される情報の完全性をも確認できる仕組みの構築が必要。