資料13－１

IoTセキュリティ総合対策の見直しの方向性（事務局作成資料）

総務省　サイバーセキュリティ統括官室

（１）脆弱性対策の推進について

● 「脆弱性対策の体制整備」に関するこれまでの主な進捗状況と今後の取組

①　現在使用されている機器への対策

- ✓ 2017年度（平成29年度）、重要IoT機器を中心にIoT機器の脆弱性調査を行い、脆弱なIoT機器の所有者等に対して注意喚起を実施。
- ✓ NICTの業務に、パスワード設定等に不備のあるIoT機器の調査を追加するNICT法改正法案を2018年（平成30年）３月に国会へ提出し、同年５月に成立。2019年（平成31年）２月より、NICTがサイバー攻撃に悪用されるおそれのある機器を調査し、電気通信事業者を通じた利用者への注意喚起を行う取組「NOTICE」を開始。
- ✓ 「NOTICE」の実施にあたり、専用の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を案内。また、IoT機器のセキュリティ対策の必要性や、本取組の内容の広報のため、家電量販店、公共機関等でのポスター掲示や新聞広告、交通広告等の周知広報活動を実施。

（１）脆弱性対策の推進について

● 「脆弱性対策の体制整備」に関するこれまでの主な進捗状況と今後の取組

② 今後製造される機器への対策

- ✓ 2019年３月、IoT機器を含む端末設備に対するセキュリティ対策として、端末設備の技術基準に、①アクセス制御機能、②適切なパスワード設定を促す機能、③ファームウェアの更新機能などのセキュリティ要件を追加することを内容とする端末設備等規則の改正を実施。
- ✓ 今後は2020年（令和２年）４月の改正省令の施行に向けて関係者と連携して取り組む。
- ✓ 2018年（平成30年）７月、IoT推進コンソーシアムのIoTセキュリティWGにおいて、セキュアなIoT機器の認証について、民間主体の自発的な取組により論点の具体化を図ることなどを内容とする、「IoT機器のセキュリティ対策に関する検討の方向性」をとりまとめ。今後は引き続き官民で連携して、と取組みを推進。

（１）脆弱性対策の推進について

● 「脆弱性対策の体制整備」に関するこれまでの主な進捗状況と今後の取組

③　電気通信事業者間の情報共有等の促進

✓ 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（認定送信型対電気通信設備サイバー攻撃対処協会）の制度創設等を内容とする電気通信事業法改正法案を2018年（平成30年）３月に国会へ提出し、同年５月に成立。2019年（平成31年）１月、改正法に基づき一般社団法人ICT-ISACを第三者機関として認定。今後は、第三者機関、電気通信事業者が行う対策について、円滑な実施のための支援を行うなど、取組を促進。

（１）脆弱性対策の推進について

■ 脆弱性対策の体制整備が一定程度完了したことを踏まえ、引き続き、ライフサイクル全体を通じたIoT機器のセキュリティ対策について推進する。

● 新たな総合対策の「脆弱性対策の推進」の項目（案）

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調査
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
⑪「日本版SHODAN/Censys」の実現（資料13－２の②）

御意見例

- NOTICEにおける調査等で得られた信頼できる情報を、検索可能なデータベースとして構築し、企業等が自社のIPアドレスレンジを検索して対策に役立てる「日本版SHODAN/Censysの実現」が有効である。
- IoT端末の脆弱性情報について、海外メーカー等の脆弱な機器などの情報についても、ユーザ企業やセキュリティ対策を行う組織で共有できる仕組みの構築をお願いしたい。

（２）研究開発の推進について

● 「研究開発の推進」に関するこれまでの主な進捗状況と今後の取組

① 基礎的・基盤的な研究開発等の推進

- ✓ サイバー攻撃誘引基盤「STARDUST」の高度化の実施。
- ✓ 現在利用されている暗号技術及び今後の利用が想定される暗号技術の安全性評価。
- ✓ 量子コンピュータ時代に向けた格子理論に基づく新たな公開鍵暗号の開発。
- ✓ プライバシーの保護に資する暗号化したままデータを解析する技術等の研究開発。
- ✓ SIP第1期課題「重要インフラ等におけるサイバーセキュリティ確保」において、制御・通信機器の真贋判定技術及び動作監視・解析技術等の開発に取り組んでいる。
- ✓ SIP第2期課題「IoT社会に対応したサイバー・フィジカル・セキュリティ」において、IoT機器のセキュリティを保証する技術、トラストリストを構築・確認する技術、トレーサビリティ確保技術等の開発に取り組んでおり、今後研究開発を本格化するとともに、実証実験の準備を進める。**（資料13－２の③）**

御意見例
- サービスサプライチェーンにおけるデータセキュリティ確保の研究開発が必要
- データセットの認証やデータのサプライチェーンの保護を促進する仕組みが必要

（２）研究開発の推進について

● 「研究開発の推進」に関するこれまでの主な進捗状況と今後の取組

① 基礎的・基盤的な研究開発等の推進

✓ 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。**（資料13－２の③）**

御意見例
- 5Gの本格化を迎え、これを悪用したサイバー攻撃がさらに強力となる可能性があることから、これを想定した対策技術の検討が必要。

✓ 大規模な量子コンピュータの実用化による暗号危殆化の可能性を踏まえた検討が必要のため、暗号技術検討会の下に「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」を設置し、次期電子政府推奨暗号リストの要件の他、新たな暗号技術の動向を踏まえた検討を加速する。**（資料13－２の⑦）**

御意見例
- 暗号基盤の危殆化に備えた基盤技術の研究開発

（２）研究開発の推進について

● 「研究開発の推進」に関するこれまでの主な進捗状況と今後の取組

② 広域ネットワークスキャンの軽量化

✓ 2018年度（平成30年度）からの３年間、「周波数有効利用のためのIoTワイヤレス高効率広域ネットワークスキャン技術の研究開発」において、周波数の利用状況の自動推定による広域ネットワークスキャン技術の開発と、広域ネットワークスキャンの無線通信量軽減技術の開発を行う。

✓ 引き続き、通信量の抑制と制度の向上を実現する効率的な広域ネットワークスキャンの実現を目指して研究開発を進め、詳細な技術仕様の検討と性能評価を行う。また本研究開発の成果をIoT機器の脆弱性調査に活用するための連携を進め、調査の効率化に取り組む。**（資料13－２の⑧）**

御意見例 ● ネットワーク探索と連動した攻撃の検知、分析技術などを高度化する必要がある。

③ ハードウェア脆弱性への対応 **（資料13－２の⑤）**

✓ 「戦略的情報通信研究開発推進事業（SCOPE）」において、2017年度（平成29年度）は、IoT機器の回路部品を検知する技術の確立を検討し、2018年度（平成30年度）は、IoT機器及びIoTネットワークにおいて、不正動作を検出した後高速にIoTネットワークを正常回復する仕組みを構築することを目標として研究開発を実施した。引き続き、本分野においても継続的に取り組む。

御意見例 ● ハードウェアセキュリティあるいはチップセキュリティについて、比較的早期の研究開発が必要。

（２）研究開発の推進について

● 「研究開発の推進」に関するこれまでの主な進捗状況と今後の取組

④ スマートシティのセキュリティ対策の強化

- ✓ 戦略的情報通信研究開発推進事業（国際標準獲得型）の取組において、EUとの研究を実施。2018年（平成30年）７月から「スマートシティアプリケーションに拡張性と相互運用性をもたらす仮想IoTクラウド連携基盤の研究開発（Fed4IoT）」を開始し、Fed4IoTのユースケースと要求条件の選定等を行った。
- ✓ 今後は、欧州も含めたサービスも考慮し、IoTサービスにおいて個人情報を保護した上でユーザ認証・属性認証サービスを提供するスキームの実証を行う。

（２）研究開発の推進について

● 「研究開発の推進」に関するこれまでの主な進捗状況と今後の取組

⑤ 衛星通信におけるセキュリティ技術の研究開発

- ✓ 安全な衛星通信ネットワークの構築を可能とし、盗聴や改ざんが極めて困難な量子暗号通信を超小型衛星に活用するための技術の確立に向け、2018年度（平成30年度）から５年間、「衛星通信における量子暗号技術の研究開発」に取り組む。
- ✓ 2018年度（平成30年度）は量子暗号通信を超小型衛星に活用するために、（１）超小型衛星に搭載可能な量子暗号装置の小型化・軽量化技術、（２）衛星への照準を精微に合わせるための空間光通信・高精度捕捉追尾技術、（３）衛星から送信された光信号を地上局において高感度に受信する技術の開発に向けた装置の設計及び試作等を実施した。
- ✓ 2020年度（令和2年度）末までに装置の政策及び機能検証等を終え、上記の技術を集約・統合し、2021年度（令和３年度）から2022年度（令和４年度）にかけて航空機等による実証実験を行う。

（２）研究開発の推進について

● 「研究開発の推進」に関するこれまでの主な進捗状況と今後の取組

御意見例　● セキュリティ対策自動化技術の研究開発が必要

⑥ AIを活用したサイバー攻撃検知・解析技術の研究開発（資料13－２の⑥）

- ✓ NICTにおいて、サイバー攻撃に対して機械学習をはじめとするAIを活用したサイバーセキュリティの研究開発を実施中。
- ✓ 現段階の成果例として、（１）ダークネットデータに基づいてDDoS攻撃を早期検知する研究開発、（２）マルウェアの解析を妨げる難読化ツール（パッカー）の特定の自動化に関する研究開発、（３）オンラインマーケットにおいて配布されるAndroidアプリのマルウェア判別分析に関する研究開発、を実施。
- ✓ 引き続き、AIのサイバーセキュリティ対策の活用に向けた研究開発に取り組む。

（２）研究開発の推進について

■ 従来の研究開発に加え、暗号基盤の危胎化に向けた基礎技術の研究開発や5Gのセキュリティ対策など、重要な政策テーマについて、新たに取り組む。

● 新たな総合対策の「研究開発の推進」において追加することが考えられる項目（案）

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
⑦ 暗号基盤の危胎化に向けた基礎技術の研究開発（資料13－２の⑦）
⑧ 5Gのセキュリティ対策（資料13－２の③）

（３）民間企業等におけるセキュリティ対策の促進について

● 「民間企業等におけるセキュリティ対策の促進」に関するこれまでの主な進捗状況と今後の取組

① 民間企業のセキュリティ投資等の促進

- ✓ 2018年度（平成30年度）よりコネクテッド・インダストリーズ税制が開始。今後、その活用状況を把握・分析するとともに、セキュリティ投資促進のための政策支援の在り方について引き続き検討を行う。

② セキュリティ対策に係る情報開示の促進

- ✓ 経営層のセキュリティ対策の重要性の認識の促進をするため、2017年（平成29年）12月より情報開示分科会を開催し、民間企業のセキュリティ対策の情報開示に関する課題を整理し、普及に必要な方策の検討結果を報告書として公表。
- ✓ 同報告書を受け、現在、サイバーセキュリティ対策に関する民間企業の情報開示の手引きの策定に向けた議論を実施。策定後、同手引きの普及促進を図る。

（３）民間企業等におけるセキュリティ対策の促進について

● 「民間企業等におけるセキュリティ対策の促進」に関するこれまでの主な進捗状況と今後の取組

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

- ✓ ICT-ISACと連携してサイバー攻撃に関する情報を収集・分析・共有するための情報共有基盤の運用の実証を実施し、2018年（平成30年）３月にはICT-ISACにおいて、「脅威情報の情報共有基盤利用ガイドライン（事業者向け）」を策定。
- ✓ 今後は脆弱性情報を活用した早期対策を促進するためのし仕組みの検討や機械学習を活用した情報の分析や対策の自動化に向けた検討を行う。
- ✓ 日米のISAC間の情報共有、連携のためのワークショップを随時実施（第2回：2017年（平成29年）11月、第3回：2019年（平成31年）２月）。

④ 情報共有時の匿名化処理に関する検討

- ✓ 情報共有時の匿名化に関する既存の仕組み等として、「重要インフラの情報セキュリティ対策に係る第４次行動計画」）や上述のガイドラインが存在。
- ✓ 引き続き、事業者等による積極的な情報共有を促進するための取組について、機微情報等の匿名化処理を含めた検討を行う。

（３）民間企業等におけるセキュリティ対策の促進について

● 「民間企業等におけるセキュリティ対策の促進」に関するこれまでの主な進捗状況と今後の取組

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

- ✓ 2017年（平成29年）11月に公衆無線LANセキュリティ分科会を設置し、公衆無線LANのセキュリティ対策の在り方と、セキュリティに配慮した公衆無線LANサービスの普及策について検討を実施し、2018年（平成30年）３月に報告書として公表。
- ✓ 周知・啓発の一環として、（株）ドコモの運営する大規模オンライン講座プラットフォーム「gacco」において、公衆無線LANのリスクやセキュリティ対策等を解説するオンライン教育コンテンツを2019年（平成31年）２月から同年３月まで開講・配信し、3,837名の受講登録があった。
- ✓ 引き続き、安全に無線LANを利用できる環境の整備に向けて、利用者・提供者において必要となるセキュリティ対策に関する周知啓発の充実を図る。

（３）民間企業等におけるセキュリティ対策の促進について

■ 構成員の御意見等を踏まえ、新たに以下の項目を追加することを検討。

● 新たな総合対策の「民間企業等におけるセキュリティ対策の促進」において追加することが考えられる項目（案）

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
⑥ 5Gのセキュリティ対策【再掲】（資料13－２の③）
⑦ トラストサービスの在り方の検討（資料13－２の③）

④人材育成の強化について

■ 人材育成は今後も重要な取組であり、これまでと同様、NICTのナショナルサイバートレーニングセンターでの取組を継続する。

■ また、新たに地域の企業向けの対策を強化する。

● 新たな総合対策の「人材育成の強化」の項目（案）

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 地域のセキュリティ人材の育成（資料13－２の①）

御意見例 ● 地域における戦略マネジメント層人材の育成が課題

御意見例 ● 専任のセキュリティ担当者を持つのが難しい小規模企業等について、いかにして経営層の皆様に関心をもっていただくかについて、十分な議論と実践が喫緊の課題

・地域におけるセキュリティファシリテータの育成（資料13－２の④）
・地域でのセキュリティ人材のシェアリング
・地域における人材エコシステムの形成（資料13－２の⑨）

御意見例
● 長期的な人材育成の仕組み作りが必要
● セキュリティマネジメント人材とセキュリティ技術人材の融合化の推進

⑤国際連携の推進について

■ サイバーセキュリティ対策に関しては、国際連携が重要であることから、今後も引き続きASEAN各国との連携や国際的なISAC間連携、国際標準化の取組、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を通じ、各国との連携を強化する。

● 新たな総合対策の「国際連携の推進」の項目（案）

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

ただし、**「トラストサービスの在り方の検討」**については、**「民間企業等におけるセキュリティ対策の促進」**に項目を移動