資料14－１

IoTセキュリティ総合対策改定版（仮称）（案）について
（事務局作成資料）

サイバーセキュリティタスクフォース事務局

令和元年　６月１４日

「IoTセキュリティ総合対策」（2017年10月公表）

①脆弱性対策に係る体制の整備

- 脆弱性調査の実施。
- 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。

②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。

③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。

④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。

⑤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）

総合対策の進捗状況や今後の取組方針を整理し、「プログレスレポート」として公表（平成30年７月、令和元年５月）

「IoTセキュリティ総合対策」策定後の状況変化

■ 総合対策の策定後の様々な状況変化を踏まえ、今般、新たにIoTセキュリティ総合対策を改定する方向で検討。

●「IoTセキュリティ総合対策」策定後の状況変化（資料14-2のP5～P8）

1 5Gのサービス開始

- ✓ 仮想化、ソフトウェア化、モバイルエッジコンピューティングなど、構造面で従来と異なる特徴
- ✓ 産業用途でのIoT機器の設置・運用

2 サプライチェーンリスクの重要性

- ✓ ソフトウェア・ハードウェアのサプライチェーンなどICTの製品・サービスの製造・流通過程でのリスク
- ✓ 委託先が踏み台となって攻撃を受けるケース

3 Society5.0の実現に向けたデータの流通・管理の重要性

- ✓ クラウドサービスやスマートシティなどのセキュリティの確保の重要性
- ✓ トラストサービスの必要性

4 サイバーセキュリティ×AIの重要性

- ✓ AIの活用が進展する中で、特にAIを利用したセキュリティ対策を促進することが必要

5 大規模な量子コンピュータの実用化の可能性

- ✓ 将来の大規模な並列演算が可能な量子コンピュータの実用化に向け、現時点から新たな推奨暗号の在り方について検討の必要性

6 大規模な国際イベント等の開催

- ✓ 2019年ラグビーワールドカップや2020年東京オリンピック・パラリンピック大会の円滑な実施、及びその後も見据え、対策の着実な実施が必要

これら直近で特に対応すべきリスクの増大要因に対応する施策を新たに盛り込んで総合対策を改定。

「IoTセキュリティ総合対策改定版」（仮称）のポイント（案）①

■ 施策展開の枠組みとして、情報通信サービス・ネットワークの、特に重点的に対応すべき個別分野のサイバーセキュリティについて政策を推進しつつ、研究開発や人材育成・普及啓発、国際連携、情報共通・情報開示の促進に取り組む必要がある。

● **施策展開の枠組み（資料14-2のP8～P9）**

✓ 情報通信サービス・ネットワークの、特に重点的に対応すべき個別分野のサイバーセキュリティの在り方について包括的な検討の上、関係府省庁や民間企業と連携しつつ、政策を実効的に推進。

✓ さらに以下の観点からの取組を並行して実施。

（１） 上記の分野での政策をより効果的に実施するための研究開発の推進

（２） 情報通信サービス・ネットワークのユーザも含めた人材育成・普及啓発の推進

（３） 国際連携の推進

（４） サイバーセキュリティに関する情報共有・情報開示の促進

✓ なお、施策の検討・展開に当たっては、ネットワーク側とユーザ側の双方の観点からの施策展開、情報通信サービス・ネットワークのレイヤー構造や時間軸を意識した施策展開、政策バリューチェーンの構築などの観点に留意しつつ、施策の有効性を確保する。

「IoTセキュリティ総合対策改定版」（仮称）のポイント（案）②

■ 施策の実施に当たっては、個々の取組の成果などを有機的に連携させて取り組む必要がある。

● **施策展開の枠組み（資料14-2のP8～P9）**

特に重点的に対応すべき情報通信サービス・ネットワークの個別分野等に関する具体的施策

- ✓ IoT、5G、クラウド、スマートシティのセキュリティ　など
- ✓ トラストサービスの在り方の検討　など

具体的施策間でも連携

連携　連携　連携　連携

研究開発

- ✓ ハードウェア脆弱性
- ✓ 暗号
- ✓ AI

など

人材育成 普及啓発

- ✓ CYDER
- ✓ 地域の人材育成

など

情報共有 情報開示

- ✓ 認定協会
- ✓ 情報共有基盤
- ✓ 情報開示

など

国際連携

- ✓ ISAC連携
- ✓ 国際標準化
- ✓ サイバー対話

など

「IoTセキュリティ総合対策改定版」（仮称）のポイント（案）③

■ 情報通信サービス・ネットワークでは、IoTや5Gのセキュリティ対策などに重点的に取り組む必要がある。

● 情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策

（１）IoTのサイバーセキュリティ対策（資料14-2のP10～P13）

① IoT機器の設計・製造・販売段階での対策

② IoT機器の設置・運用・保守段階での対策

③ 脆弱性等を有するIoT機器の調査と注意喚起

④ サイバー攻撃に関する電気通信事業者間の情報共有

（２）5Gのセキュリティ対策（資料14-2のP13～P14）

① ソフトウェア脆弱性への対応

② ハードウェア脆弱性への対応

（３）クラウドサービスのセキュリティ対策

（４）スマートシティのセキュリティ対策

（５）トラストサービスの在り方の検討（資料14-2のP16～P17）

（６）公衆無線LANのセキュリティ対策

（７）重要インフラとしての情報通信分野のセキュリティ対策

（８）地域の情報通信サービスのセキュリティ対策の確保

「IoTセキュリティ総合対策改定版」（仮称）のポイント（案）④

■ 研究開発では、ハードウェア脆弱性やAIを活用したサイバー攻撃対策に加え、量子コンピュータ時代に向けた暗号の在り方の検討を行う必要がある。

● 横断的施策

（１）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【再掲】（資料14-2のP21）

④ スマートシティのセキュリティ対策【再掲】

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（資料14-2のP23）

⑦ 量子コンピュータ時代に向けた暗号の在り方の検討（資料14-2のP23）

⑧ 重要インフラ等におけるサイバーセキュリティの確保

⑨ IoT 社会に対応したサイバー・フィジカル・セキュリティ対策

「IoTセキュリティ総合対策改定版」（仮称）のポイント（案）⑤

■ 人材育成・普及啓発に関しては、従来の取組に加え、地域のセキュリティ人材育成に重点的に取り組む必要がある。

■ 国際連携に関しては、ASEAN各国との連携を中心に、引き続き様々な取組を進める必要がある。

● 横断的施策

（２）人材育成・普及啓発の推進

① 実践的サイバー防御演習（CYDER）の実施

② 2020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育成（資料14-2のP26～P27）

（３）国際連携の推進

① ASEAN各国との連携（資料14-2のP28）

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

「IoTセキュリティ総合対策改定版」（仮称）のポイント（案）⑥

■ 情報共有・情報開示については、事業者間での情報共有を促進するための基盤の構築や、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を中心に、民間企業の自主的な情報開示・情報共有を促進する必要がある。

● 横断的施策

（４）情報共有・情報開示の促進

① サイバー攻撃に関する電気通信事業者間の情報共有【再掲】

② 事業者間での情報共有を促進するための基盤の構築（資料14-2のP31～P32）

③ サイバーセキュリティ対策に係る情報開示の促進（資料14-2のP32）

④ サイバーセキュリティ対策に係る投資の促進

⑤ 国際的なISAC間連携