

# 今後の検討課題とスケジュールについて

---

サイバーセキュリティタスクフォース事務局

令和元年 11月22日

# 今後の検討項目とスケジュールについて

- 「IoT・5Gセキュリティ総合対策」の柱立てに沿って、①できるだけ早期に検討を始めて実施に着手すべき短期的な検討項目、②中長期的な検討項目について整理して議論をしつつ、前回頂いた御意見なども踏まえ、必要に応じて新たな検討項目を追加して議論を行うことどうか。
- また、各回の議論は構成員や臨時のプレゼンター等による論点ごとのプレゼンテーションと自由討議を基本とすることどうか。

## ← 短期的な検討項目 →

## ← 中長期的な検討項目 →

### 第17回 (11/22)

- 重要インフラ事業者等が設置するIoT機器のセキュリティ確保に向けて取り組むべき事項はないか？  
(Ⅲ(1)IoTのセキュリティ対策)
- 地方公共団体や重要インフラ事業者等の人材育成を強化する必要はないか？  
(Ⅳ(2)人材育成・普及啓発の推進)
- サイバーセキュリティの質の向上のため実効的な情報共有体制が構築・運営されているか？  
(Ⅳ(4)情報共有・情報開示の促進)

### 第18回 (12/5)

- Wi-Fiの安全な利用のための周知を徹底する必要はないか？  
(Ⅲ(6)公衆無線LANのセキュリティ対策)
- 重要インフラ事業者等のサイバーセキュリティ対策などは実効的に行われているのか？  
(Ⅲ(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)

### 第19回以降 (12/25～)

- その他「Ⅲ 具体的施策」や、「Ⅳ(1)研究開発の推進」、「Ⅳ(3)国際連携の推進」
- などの中から論点を抽出し、議論を実施。
- なお、「IoT・5Gセキュリティ総合対策」の柱立てに明示的に含まれない課題についても必要に応じて議論を行う。
  - また、平行して「IoT・5Gセキュリティ総合対策」の実施状況についてのレビューも行う。

(※) 太字は「IoT・5Gセキュリティ総合対策」の項目

- 人材育成については、インシデントなどの積極的な情報共有や情報発信が重要。
- 人材育成については、技術と制度を掛け合わせたハイブリッドな人材の育成が必要。
- 中小企業に係るサプライチェーンリスクの問題については、クラウド化・アウトソーシングによって端末管理にリソースを集中する仕組みの導入が必要。
- 大規模災害に対する通信設備の可用性について点検が必要。
- セキュリティの知識の全体的な底上げのため、戦略マネジメント層人材の育成が非常に重要。
- IoT機器の調査結果を、ユーザーの啓発や、これから重要になる端末の安全性確保などに活用すべき。
- サイバー対策はネットの安全性を高めるので通信の秘密を強める、保護レベルを高める可能性があることを踏まえ、（通信の秘密について）議論をすべきではないか。
- オリンピックまで間に合うものは実行すべきである。また、中長期的に法制度を含めて見直さねばならないものは何なのか、この場で認識の共有を行うとよい。
- 東京オリンピックパラリンピック大会に向けて大会組織委員会の準備状況を報告してもらってはどうか。
- ソフトウェアとハードウェアの両方にせい弱性があるということ、及びそれらの課題について産学が連携して研究開発で取り組んでいるということを広く周知すべき。
- 「NOTICE」の取組について、技術的知識が十分でない一般の利用者に対してIoTセキュリティの重要性の周知啓発のための検討が必要。
- 広域ネットワークスキャンの研究開発の成果を、「NOTICE」を含めた様々な分野で活用することが重要。