資料19－1

前回までの御議論と今後の進め方等について

サイバーセキュリティタスクフォース事務局

令和元年12月25日

第16回、第17回、第18回で頂いた主な御意見について

【総論・その他】

- 東京2020大会まで間に合うものは実行するべきであり、総務省が採るべき具体的なアクションについて、早期に実施するためのとりまとめやリストアップを行うことが重要。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。
- 東京2020大会の組織委員会の準備状況を報告してもらってはどうか。
- 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。
- 通信インフラ事業者（ISP）だけでなく巨大IT企業など上位レイヤーが有する情報にも意識して対策を考える必要がある。

【IoTのセキュリティ対策】

- 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。
- 「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。
- 短期的な取組と長期的な取組に分けて、短期的な重要IoT機器に対する対策はできれば東京2020大会までに実施すべき。
- 動的IPアドレスにつながる機器が外からのアクセスを期待してポートを開けることはあまりないので、対策について中長期的に取り組んでいくべき。
- 中長期的な課題として、C&Cサーバと通信しているIoT機器への対処について、制度面も含めて検討すべき。
- 大規模停電からの復電時などにIoT機器が一斉に通信を行うことで障害とならないよう十分な検討を行うべき。
- オープン情報を集約して脅威検知を行う仕組みや、攻撃側が有する情報を陳腐化するような技術が必要。
- 重要IoT機器の脆弱性調査が実施できるよう、予算化を含む必要な対応を行うべき。

【クラウドサービスのセキュリティ対策】

- 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。

【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】

- 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。
- 未然防止だけでなく、事後の対処についても、特に重要インフラの１つである自治体では重要。
- インシデント情報の共有が大事だが、EUでも通信や放送の報告制度が義務づけられており、窓口を統一しているので参考になるのではないか。

【研究開発の推進】

- ソフトウェアとハードウェアの両方のぜい弱性、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。
- 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。

【人材育成・普及啓発の推進】

- 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。
- 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。
- そもそもセキュリティに興味を持ってもらうための入口の取組が必要。
- 理工系以外の組織を含め社会全体でマインドを育成していくことが重要。
- 重要インフラ事業者について、CYDERへ参加を促す必要がある。

【情報共有・情報開示の促進】

- 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。
- 既存の情報共有の取組をもっとPRすることが重要。

（※）項目は総合対策の想定箇所又は関連箇所、赤字は第17回で頂いた御意見、青字は第18回で頂いた御意見

第18回で御議論いただいた内容と今後の方向性について①

- 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）

主な現状と課題

- Wi-Fiについては、①端末－アクセスポイント(AP)間が**暗号化されていない**場合、②**なりすましAP**（詐称されたAP）を利用してしまう場合などで、通信を**盗聴されるリスク**が存在している。
- セキュリティを強化した、WPA3-Personal、WPA3-Enterprise、Enhanced Openといった新しい規格が策定されている。
- 公衆無線LANのように多数の利用者で共用する場合、盗聴リスクに対応するためにはWPA3-Enterprise等を利用することが適当だが、事業者・利用者双方に相応のコスト負担が発生する。
- **公衆無線LANの利用者**が、リスクを適切に認知した上でサービスを利用できるように、公衆無線LANの**セキュリティ対策の状況や自ら講じるべきセキュリティ対策を理解**してもらうことが重要。

今後の方向性（案）

- 公衆無線LANの利用者に、公衆無線LANのセキュリティ対策の状況や自ら講じるべきセキュリティ対策を理解してもらうべく、**引き続きより一層の周知を行っていくべき**ではないか。
- その際、ただ単にリスクを伝えるだけではなく、通信経路が暗号化されていない状況でID・パスワードを入力しないといった**適切な利用方法を情報提供していくことが必要**ではないか。
- また、**https**で正規のサイトにアクセスしていることの見分け方といった、無線LANより上位レイヤーにおけるセキュリティ対策についても**周知啓発**を進めていくべきではないか。

第18回で御議論いただいた内容と今後の方向性について②

● 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）

主な現状と課題

- 通信・放送分野においては、サイバーセキュリティ対策の実効性を確保するため、**事業法において、サイバーセキュリティ対策や設備が故障した際の報告の義務付けに関する取組**がなされている。

- また、通信・放送**業界で定められたガイドライン・基準やベストプラクティス**なども参照しつつ、各社でルールを策定・運用し、セキュリティを確保している。

【参照されているガイドライン・基準等】

✓ 情報通信ネットワーク安全・信頼性基準
✓ 電気通信分野における情報セキュリティ確保に係る安全基準（TCA）
✓ 電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン（TCAほか）
✓ 放送設備サイバー攻撃対策ガイドライン（ICT-ISAC）

- 他方、**中小事業者は、人材や資金などのリソース不足**から十分な対策をとるのが難しい現状にある。

今後の方向性（案）

- 左記のような、サイバーセキュリティ対策や事故報告についての法令への位置づけ、業界ごとのガイドラインや基準の策定を通じてサイバーセキュリティ対策を実効的に進めていく取組について、我が国のサイバーセキュリティの強化のため、**通信・放送業界の取組を国内で積極的に周知するべき**ではないか。

- 他方、通信・放送業界においても、**中小事業者**はリソース不足で十分な対策をとるのが難しいことが想定されることから、これらの事業者に対する**支援施策を検討すべき**ではないか。

今後の検討項目とスケジュールについて【第17回資料再掲】

■ 「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でどうか。

■ 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でどうか。

← 短期的な検討項目 →

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）

← **中長期的な検討項目** →

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。

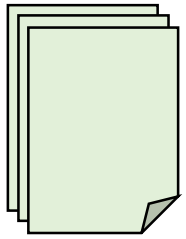
（※）太字は「IoT・5Gセキュリティ総合対策」の項目

今後の会合の進め方（案）

■ 「IoT・5Gセキュリティ総合対策」の主要な項目レベルで議論を実施。

■ ただし、総合対策の柱立てに明示的に含まれない項目についても必要に応じて議論を行う。

IoT・5Gセキュリティ総合対策



【具体的に取り組むべき課題・施策の項目】

Ⅲ 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のセキュリティ対策
（２）5Gのセキュリティ対策
（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
（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の確保

Ⅳ 横断的施策

（１）研究開発の推進
（２）人材育成・普及啓発の推進
（３）国際連携の推進
（４）情報共有・情報開示の促進

第16回 ～ 第18回

短期的に速やかに検討すべき課題について検討

第19回

第20回

第21回

第22回

⋮

中長期的な検討項目について、各回ごとに、IoT・5Gセキュリティ総合対策の主要な項目について議論を実施

- 東京2020大会までに早急に取り組むべき事項について、現在事務局にて整理を行っているところ。
- IoT・5Gセキュリティ総合対策の主要な項目に対応して、①「IoT・5Gセキュリティ総合対策」の個別施策の進捗状況等のレビューを実施しつつ、②今後取り組むべき内容について御議論いただく。
- 「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項目についても必要に応じて議論を行う。

令和2年度以降に取り組むべき課題や施策について春～夏頃を目途に最終的な取りまとめを行う。

中長期的な検討項目について（現時点での例）

項目	検討内容（案）	（参考）TFで頂いた御意見
スマートシティのセキュリティ対策（Ⅲ-(4)）	● スマートシティのセキュリティの確保に、クラウド化などを念頭に、現状の取組についてレビューしつつ、今後の方向性等について検討する。	
地域の情報通信サービスのセキュリティの確保（Ⅲ-(8)）	● いわゆるセキュリティ弱者への啓蒙啓発や、戦略マネジメント層などへの啓蒙啓発も念頭に、総合通信局等を中心とした地域単位の情報共有体制の構築に向けた取組について、現状の取組についてレビューしつつ、今後の方向性等について検討する。	● 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。 ● 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。 ● そもそもセキュリティに興味を持ってもらうための入口の取組が必要。 ● 理工系以外の組織を含め社会全体でマインドを育成していくことが重要。
研究開発の推進（Ⅳ-(1)）	● 特に5Gのネットワークや機器を念頭に、ソフトウェアとハードウェアの双方のセキュリティ確保に向けた取組の在り方について引き続き検討する。 ● サイバーセキュリティ分野における研究開発の方向性について、AIや5G、量子など先進的な技術動向も踏まえつつ整理を行う。	● ソフトウェアとハードウェアの両方のぜい弱性、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。 ● 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。

（※）その他の検討項目については現在事務局において検討中であり、次回以降改めて提示予定。

検討に当たっての留意点①

- サイバーセキュリティ対策は広範な政策分野であり、その推進に当たっては**各主体の適切な役割分担の下での連携・協働**が必要である。この点、総務省に期待される役割は、まず情報通信サービス・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、**関係府省庁や地方公共団体及び民間企業と連携**しつつ、政策を実効的に推進していくことである。

- 当該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**や、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**、**国際連携の推進**、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**の観点からの取組を並行して進めていく必要がある。

（IoT・5Gセキュリティ総合対策の「Ⅱ　施策展開の枠組み」より抜粋）

個別分野のサイバーセキュリティ施策を実施する前提として、サイバー空間を支える情報通信サービス・ネットワークの全体像を意識しておくことが重要ではないか。

Ex.) IoT、5G、クラウド、スマートシティなど、それぞれの技術、カテゴリ、概念などが情報通信サービス・ネットワークの全体像の中で、どのように位置づけられるかを意識しておく必要があるのではないか。

左記の全体像を念頭に置いた上で、Society5.0の実現に向け、様々な関係主体と連携してサイバーセキュリティの確保に取り組むべきではないか。

Ex.) 官民の様々な主体が連携して取り組むことにより、サイバー空間全体のサイバーセキュリティが確保されるよう意識しておく必要があるのではないか。

検討に当たっての留意点②

IoT・5Gセキュリティ総合対策の「Ⅱ 施策展開の枠組み」より抜粋

① 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・ネットワーク全体の安全性や信頼性を確保するためには、ネットワーク側とユーザ側の双方の視点でサイバーセキュリティ対策を推進するための施策を検討する必要がある。

② 情報通信サービス・ネットワークのレイヤー構造

- 情報通信サービス・ネットワークについては、機能に着目して構造的にサービス（データ流通）層、プラットフォーム層、ネットワーク層、機器層と分類が可能であるが、それぞれの層において留意すべき脅威とセキュリティ要件の在り方について検討する必要がある。

③ 時間軸を意識した施策展開

- IoT機器のライフサイクル、人材育成のスパンなど、施策の効果の発現に関する時間軸を意識した政策立案を行う必要がある。

④ 政策バリューチェーンの構築

- 例えば、研究開発の成果を情報通信サービス・ネットワークの個別分野の施策に反映しつつ、その成果について国際的な展開を図る、また、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施策と人材育成の施策を連携させて、地域のサイバーセキュリティ確保を一体的に推進するなど、個別施策を有機的に連携させ、横断的で一貫性のある施策展開を図る必要がある。