資料27－４

今後の検討課題について

サイバーセキュリティタスクフォース事務局

令和2年 12月3日

今後の検討課題（例）

■ 「IoT・5Gセキュリティ総合対策2020」で提言された施策を着実に進めつつも、昨今のサイバー攻撃事案、なりすましによるオンライン・サービスの不正利用事案、サイバー空間をめぐる国際的な動向等を踏まえて、例えば、以下のような論点について今後議論が必要ではないか。

1 巧妙化・多様化するサイバー攻撃への対策

【最近のサイバー攻撃事案を踏まえた対策】

- 最近のサイバー攻撃事案を踏まえてどのような対策が必要か？
- 「ゼロトラスト」のコンセプトを取り入れたサイバー攻撃対策の必要性について、どのように考えるか？

【IoT端末等を踏み台にしたサイバー攻撃への対策の強化】

- NOTICEやNICTER注意喚起を通じたIoT端末等の保有者への注意喚起について、より効果的に進める方策はないか？
- IoT機器の設計・製造・販売段階での対策として、更に取り組むべき点はないか？
- このほか、IoT機器のセキュリティ対策を更に強化するにはどのような取組が必要か？

（端末側における対策のみで十分な効果が上がっているか？／海外のIoT端末等が注意喚起の対象になっていないことに課題はないか？ 等）

【クラウドサービスのセキュリティ対策】

- クラウドサービスの利用が浸透する中で、クラウド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？

今後の検討課題（例）

2 グローバル化するサイバー空間への対応の強化

【通信ネットワークの高度化・多様化に対応したサイバーセキュリティの確保、強靭なサイバー空間の実現】

- 国際動向が激動する中で、情報通信サービスや機器におけるサプライチェーンリスクへの対策として、更に取り組むべき事項は何かあるか？
- 我が国のサイバーセキュリティ情報の収集・産学官の連携による分析のためにNICTに構築する「サイバーセキュリティ統合知的・人材育成基盤」について、効果的な活用のために期待することは何か？
- ５G／ローカル５Gがスタートし、５Gの高度化、B5Gに向けた検討が今後進展していく中で、より強靭なサイバー空間の実現を図る観点から、将来にわたってどのような取組（研究開発、標準化等）を具体的に進めていくべきか？

（静止・非静止の衛星通信網の高度化、５G／B5G等地上網との融合、ネットワークの仮想化／オープン化／グローバル化 等）

【国際連携の推進】

- 民間組織の連携を通じたサイバーセキュリティ上の脅威等に対する情報共有をいかに推進すべきか？

（米国・ASEAN以外の国・地域（欧州、豪州等）について、民間組織の連携をどのように推進すべきか？）

- 発展途上国等へのサイバーセキュリティに係る能力構築支援や二国間・多国間連携をいかに実施すべきか？

（AJCCBCと他国主導の能力構築支援組織との連携の余地もあるが、我が国のプレゼンス維持・向上の必要も踏まえ、かかる連携は積極的に実施すべきか？／情報通信研究機構（NICT）運営のNICTER、DAEDALUS等の取組について、リソース上の課題等もある中、どのように国際連携を図るべきか？ ）

今後の検討課題（例）

3 安全で信頼できるサイバー空間の実現による、安心なICT利活用の確保

【トラストサービスの推進】

- 電子署名、タイムスタンプ、eシールなどのトラストサービスの普及に向けて取り組むべき事項は何か？

【オンライン・サービスにおける本人確認・認証の強化】

- なりすましによるオンライン・サービスの不正利用事案を受けて、セキュリティ強化に向けて取り組むべき事項は何か？

（本人確認・認証の強化？／そのほか、なりすましによる被害を防止し、ユーザーが安心かつ信頼してネットを利用できる環境を構築する観点から、何に取り組むべきか？）

【ユーザの被害防止、ユーザに対する周知啓発の推進】

- なりすまし等によってユーザが被害を被ることを防止するための対策として、何に取り組む必要があるか？

（利用者に対する費用対効果の高い周知啓発・注意喚起？／フィッシングによる被害を防止するための取組？）

本日以降に構成員の皆様に頂いた御意見やコメントを踏まえながら、検討課題を設定し、「IoT・5Gセキュリティ総合対策2020」の改定も見据えつつ、議論を進めていただくことでどうか。