資料35－3

今後検討いただきたい論点（案）

令和４年１月

サイバーセキュリティタスクフォース事務局

今後検討いただきたい論点（案）①

【全体】

○ 本タスクフォースは2017年に、東京2020大会を控えてサイバーセキュリティの課題を整理し、必要な方策を推進することを目的として設置された。引き続き、本タスクフォースでは、東京2020大会における成果や「サイバーセキュリティ戦略」（2021年９月28日閣議決定）を踏まえ、社会経済活動を支える情報通信ネットワークの安全性・信頼性を確保することを目的として議論していくことが重要ではないか。

（参考）「サイバーセキュリティタスクフォース」開催要綱（抄）

１　目的

あらゆるものがインターネット等のネットワークに接続されるIoT/AI時代が到来し、それらに対するサイバーセキュリティの確保は、安心安全な国民生活や、社会経済活動確保の観点から極めて重要な課題である。

2020年東京オリンピック・パラリンピック競技大会を3年半後に控え、IoT/AI時代を見据えたサイバーセキュリティに係る課題を整理するとともに、情報通信分野において講ずべき対策や既存の取組の改善など幅広い観点から検討を行い、必要な方策を推進することを目的として、本タスクフォースを開催する。

今後検討いただきたい論点（案）②

【１】情報通信ネットワークの安全性・信頼性の確保

○ 最近のサイバー攻撃の動向や「サイバーセキュリティ戦略」に盛り込まれた積極的サイバー防御の議論を踏まえて、既存の事業者・利用者による対策に加えて、端末側、ネットワーク側でそれぞれ、例えば以下の点について、今後どのような更なる対策を講ずる必要があると考えられるか。

・２年後に実施期限を迎えるIoT機器などの脆弱性調査・注意喚起（NOTICE）の在り方

・明らかに脆弱性があるメーカー保証期間を終えた機器や中古機器を使用しない（使用中止させる）方法

・クラウド、CDN、DNSなどの通信ネットワークそのものではないインフラでの障害の発生への対策

・利用者保護の観点でのフィッシング攻撃対策（例：DMARCの普及等）やランサムウェア攻撃対策

○ サイバーセキュリティやサプライチェーンリスク対応の重要性の高まりや経済安全保障の議論などを受けた電気通信事業者のガバナンス強化に向けた検討や、今後サイバーセキュリティ戦略本部において改定予定の重要インフラのサイバーセキュリティに係る行動計画を踏まえ、総務省として取組を見直すべき点はあるか。

○ 海外における政策やサイバー攻撃の動向から留意すべきことはあるか。

【２】研究開発

○ Beyond5G、6Gや衛星通信などの今後発展する分野や技術を含めサイバーセキュリティ対策に向けてどのような施策が考えられるか。

○ 現状観測している情報に加えて、NICTにおいて観測対象として追加すべき情報の分野・観点があるか。

今後検討いただきたい論点（案）③

【３】人材育成

○ 総務省としてどのターゲットを重視して取組を行うべきか。
（若年層～社会人、実務者・技術者～戦略マネジメント層～経営層、オペレーター～トップエンジニア等）

○ 他省庁や民間における人材育成の取組とどのように連携していくべきか。

○ サイバーセキュリティ関係の若手研究者やスタートアップの支援のためにどのような施策が考えられるか。

【４】「統合知的・人材育成基盤（CYNEX）」の構築

○ 令和２年度３次補正予算及び３年度予算で構築している「サイバーセキュリティ統合知的・人材育成基盤」（CYNEX）が産学官の組織にとって利用したいと思える環境となるよう、早期の本格稼働に向けてシステム基盤構築・運営環境整備をいかに進めるべきか。

【５】普及啓発

○ 「サイバーセキュリティ戦略」を踏まえた「Cybersecurity for ALL」に向けて総務省としてどう貢献すべきか。

○ 他省庁や民間における普及啓発の取組とどのように連携していくべきか。

○ 地域セキュリティコミュニティについて、現在は、セミナーやインシデント対応演習を開催する役割を担っているが、今後どのような役割の拡大を期待するか。

今後検討いただきたい論点（案）④

【６】国際連携

○ 現在実施している二国間・多国間の国際連携をどのように発展させていくべきか。

○「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」（2021年12月14日サイバーセキュリティ戦略本部決定）を踏まえ、総務省としてASEAN地域やインド太平洋地域における能力構築支援をどのように推進すべきか。

○ 国内企業のサイバーセキュリティ製品・ソリューションの国際展開を支援していくうえで、どのような領域・地域に注力していくべきか。

【７】情報の開示・共有等

○ サイバー攻撃の被害を受けた企業が適切なタイミングで情報の共有や公表を行うことを促進するために、どのような取組が必要か。

○ 一般社団法人ICT-ISACの役割として何を期待するか。

今後の進め方（案）

■ 本タスクフォースにおいて、本日の御意見を踏まえ、今後、「ICTサイバーセキュリティ総合対策2021」の改定に向けて議論することとしてはどうか。

■ 今後は、２月～５月に３回程度会合を開催して、事務局から関連の御報告を行いつつ、議論を深めることとしてはどうか。

（イメージ）

・３月：個別論点①（IoT対策、人材育成、CYNEX）
・４月：個別論点②（国際連携など）
・５月：個別論点③（普及啓発など）、全体（骨子）
・６月：全体（原案）