参考資料１

巧妙化・複雑化するサイバー攻撃への対策の在り方に関する検討会
（第２回）議事要旨

１．日時）令和８年６月 12 日（金）10：00～12：00

２．場所）web 会議

３．出席者）

【構成員】

鎮目座長、宍戸座長代理、上沼構成員、木村構成員、クロサカ構成員、篠田構成員、蔦構成員

【オブザーバー】

一般社団法人日本インターネットプロバイダー協会、一般社団法人電気通信事業者協会、一般社団法人テレコムサービス協会、一般社団法人日本ケーブルテレビ連盟、一般社団法人 ICT-ISAC、内閣官房国家サイバー統括室

【ヒアリング事業者】

NTT 株式会社、NTT ドコモビジネス株式会社、KDDI 株式会社、株式会社ラック、ソフトバンク株式会社

【総務省】

（サイバーセキュリティ統括官室）

三田サイバーセキュリティ統括官、赤阪大臣官房総括審議官（広報、政策企画（主）担当）、水間サイバーセキュリティ統括官室参事官（総括担当）、道方サイバーセキュリティ統括官室参事官（政策担当）、神谷サイバーセキュリティ統括官室企画官、中村サイバーセキュリティ統括官室参事官補佐

（総合通信基盤局）

吉田電気通信事業部長、大内利用環境課長、栗原利用環境課企画官

４．配付資料）

資料２－１　ヒアリング対象者一覧及びヒアリング事項（非公開資料）
資料２－２　NTT 株式会社ヒアリング資料（非公開資料）
資料２－３　NTT ドコモビジネス株式会社ヒアリング資料（非公開資料）
資料２－４　KDDI 株式会社ヒアリング資料（非公開資料）
資料２－５　株式会社ラックヒアリング資料（非公開資料）
資料２－６　ソフトバンク株式会社ヒアリング資料（非公開資料）
参考資料１　「巧妙化・複雑化するサイバー攻撃への対策の在り方に関する検討会」開催要綱
参考資料２　巧妙化・複雑化するサイバー攻撃への対策の在り方に関する検討会第１回　議事要旨

５．議事概要）

（１）開会

（２）議題

◆議題（１）「ヒアリング及び質疑応答」について

事務局から資料２－１を説明。

NTT 株式会社から資料２－２、NTT ドコモビジネス株式会社から資料２－３に基づく説明後、質疑応答が行われた。

KDDI 株式会社から資料２－４、株式会社ラックから資料２－５に基づく説明後、質疑応答が行われた。

ソフトバンク株式会社から資料２－６に基づく説明後、質疑応答が行われた。

ヒアリング対象事業者からの主な説明内容は以下のとおり。

- 電気通信事業者は、攻撃通信を観測して異常を検知して通信設備への影響を抑えることができる、利用者との接点があるといった強みがある。
- 電気通信事業者の事業用設備に対しても不正アクセス等の攻撃の試行が増加している。また、社会インフラを守る電気通信事業者として、重要なインフラ企業なども含め、利用者をしっかりと守りたい。場面に応じてできることが明確だとありがたい。
- 電気通信事業者の対応の高度化に当たっては、電気通信事業者を単にデータを運搬するものと捉えるか、社会のデジタルインフラを支えるものと捉えるかで、整理の方向が変わって来るのではないか。後者の場合、電気通信の安定的なサービスの提供から更に踏み込み、観測だけでなく予兆に踏み込んだり、自社だけでなく社会全体を守る取組ができないか、ということになるのではないか。
- 高度な対策環境を企業、産業界が作ることは難しい場合もあるため、セキュリティ機能を備えたネットワークサービスを展開している。また、セキュリティ対策ができていない IoT 機器が存在し、利用者がそれに気付けていない場合も、こうしたサービスは利用者をサポートできると考えている。利用者の設備をしっかり保護していくことが重要である。
- 総務省の実証実験を通じ、自社の設備保護を目的にフロー情報分析を実施している。得られる C2 サーバリストを自社設備の保護だけでなく、セキュリティ機能を備えたネットワークサービスで活用したり、連携先としてセキュリティベンダ等に提供することによって、利用者の保護、ひいては我が国のセキュリティ向上にも寄与できると考えている。様々な対策ができれば、海外プレーヤーとの協力にも繋がる。
- 高度化するサイバー攻撃に対応するためには、AI も活用しながら攻撃を早く正確に検知し、対応につなげることが必要。そのためにも、外部からの情報も含め、情報の質と量を上げていく必要がある。
- SOC 事業者ではインターネット全体における広範な脅威動向については把握が限定的であり、通信レイヤーで観測される情報を一定程度活用できる場合、利用者に対する注意喚起や監視強化など、限定的ではあるが予防的な対応の高度化につながる可能性がある。ただし、現状では、どの範囲・粒度の情報が活用可能であり、実際の対策に寄与するかについては、費用対効果も含め、必ずしも明確ではないため、実務的な観点から、情報連携の在り方や活用の可能性について検討していくことは一定の意義がある。
- 脆弱な IoT 機器は、踏み台になって利用者自身が被害を受けるかもしれず、電気通信事業者も何かしらの悪影響を受けるかもしれないが、利用者に「脆弱な IoT 機器がありますよ」とお知らせしても、なかなか対応していただけないところがあり、どうすれば良いのか非常に難しい。

◆議題（２）「自由討議」について

ヒアリング事業者からの説明を踏まえ、自由討議が行われた。構成員による主な意見は以下のとおり。

- インターネットのアーキテクチャとして、電気通信事業者と利用者の責任分界点の向こう側である利用者の領域は、基本的に利用者が自分で管理するものであり、それに準じて制度設計もされているが、利用者にやってもらうしかないという点に限界が見えつつあるのではないか。利用者と電気通信事業者の二者間の問題だけでなく、踏み台にされることで更なる被害が拡大していく可能性もある。こうした問題意識を踏まえ、引き続き検討していくべきではないか。
- 電気通信事業者による利用者の保護には制度上の制約があるところだと思う。利用者の保護について検討の俎上に載せるべきではないか。
- 利用者が安全なネットワーク環境を求めることは自然な期待であり、そのために電気通信事業者が果たせる役割は大きい。制度やガイドラインを含め、電気通信事業者が安心してサイバー防御や脅威情報の共有に取り組める環境を整備していくことが重要ではないか。
- 利用者が知らないうちにサイバー攻撃の加害者になってしまうことを防ぐためにも、セキュリティに関する知識が不足している利用者も守ってもらえるようなシステムを構築してほしい。

（３）閉会

以上