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３回）議事要旨

１．日時）令和８年７月３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、中尾構成員、吉岡構成員

【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

【ヒアリング対象者】

株式会社 FFRI セキュリティ、SBI ホールディングス株式会社、一般社団法人 ICT-ISAC、一般社団法人デジタルライフ推進協会

【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）

湯本総合通信基盤局長、栗原利用環境課企画官

４．配付資料）

資料３－１　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３－２　株式会社 FFRI セキュリティヒアリング資料（非公開資料）
資料３－３　SBI ホールディングス株式会社ヒアリング資料（非公開資料）
資料３－４　一般社団法人 ICT-ISAC ヒアリング資料（非公開資料）
資料３－５　一般社団法人デジタルライフ推進協会ヒアリング資料（非公開資料）

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３－１を説明。

株式会社 FFRI セキュリティから資料３－２に基づく説明後、質疑応答が行われた。

SBI ホールディングス株式会社から資料３－３に基づく説明後、質疑応答が行われた。

一般社団法人 ICT-ISAC から資料３－４に基づく説明後、質疑応答が行われた。

一般社団法人デジタルライフ推進協会資料３－５に基づく説明後、質疑応答が行われた。

ヒアリング対象者からの主な説明内容は以下のとおり。

- AI の劇的な進歩もある中で、エンドポイントとネットワークが素早く連携できると有用と考えられるが、制度面やビジネス面での課題がある。例えば、フロー情報から抽出された脅威情報を利用者のシステムと連携したり、エンドポイント側で得られる脅威情報をネットワーク側と連携させることが考えられる。また、こうした情報が集約できれば研究開発にも有用であり、そのためには、電気通信事業者、セキュリティベンダ、公的機関のほか、利用者側の協力も必要である。国内である程度強力なセキュリティ対策手段を持っておくことが、海外との交渉においても重要である。
- AI が劇的に進化する中にあって、対策の本質は基本の徹底と対応の超高速化である。この観点からは、攻撃が届く前の対処など、いかに早く Bot に対処できるかが重要であり、フロー情報分析による C2 サーバ検知の実証事業等の知見や、それを用いたネットワーク側での対処が有用ではないか。
- エンドポイント側での対策費用はエンドポイントのサービスの利用料に反映されていくように、電気通信事業者が講じる対策の費用は、当該事業者のサービスの提供に当たって考慮されていくものと考えている。
- C2 サーバに関する情報やフィッシングドメイン等の脅威情報の官民・業界横断での共有が有用ではないか。
- 踏み台化する脆弱な IoT 機器の観測・注意喚起を継続し、攻撃インフラそのものの母数を削減することは重要。
- 家庭内に設置された一部のストリーミングデバイスや帯域シェアアプリを利用したレジデンシャルプロキシ攻撃は、海外からのアクセスを国内 IP アドレスで中継するため、被害側では正常通信と見分けることが困難である。また、LAN 内にあるため、NOTICE の取組での検知も困難である。利用者自身は悪性通信を中継しているとは認識していないことが通常である。対策には、官民の様々な主体による協力・協働が不可欠である。具体的には、利用者の行動変容を促す社会的な啓発や効果的な警告を行う、流通経路の対策を講じる、C2 サーバとレジデンシャルプロキシ間の通信をフィルタリングすることの効果を検証するといったことが考えられる。
- 高度化するサイバー攻撃への対応について、生じるコストの適正負担も考慮の上で、官民・民民の連携を更に進めることが必要。
- IoT 機器の製造はサプライチェーンが多層的であり、その過程で、脆弱性の対応ができない又は追い付かないところが狙われると踏み台化する。対策としては、更新提供されない製品への対応や、感染端末の検知・利用者への通知などが考えられる。

◆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。

- ヒアリングにおいてネットワークからの脅威情報とエンドポイントから得られる脅威情報を収集・集約できれば有用との説明があったとおり、ネットワークで取得・収集可能な脅威情報が、適正かつトラストある形で共有されることは、具体的な対策として重要である。ここでいう適正とは関連法規の法解釈として矛盾なく成立すること、またトラストある形とは実際の運用に一定の制約を課すこと（例えば共有できる対象の特定とその理由、また廃棄やデータ加工を含めたデータ管理方法の規範の確立、対処の結果に関する透明性の一定程度の確保等）を意味する。こうした観点から検討を更に深めていただきたい。
- ネットワーク側が講じる対処の責任に関して、利用者において事前に、誤ってフィルタリングされる等のリスクの一部を引き受ける旨の意思表示や、対処の優先度の設定を行わなければ、迅速な対処は難しいのではないか。費用負担に関して、善意に支えられた仕組みは規模が大きくなるほど続かないのではないか。
- レジデンシャルプロキシ等の広がりは、「国内の IP アドレスからの通信は受信を拒否しづらい」という点を逆手に取っていると思われる。こうした攻撃の巧妙化も踏まえ、利用者自身による重層的なセキュリティ対策も必要ではないか。
- 利用者が知らないうちにサイバー攻撃に悪用され得る機器を購入・利用してしまうこともあり得るので、利用者がわかるように周知広報してほしい。

（３）閉会

以上