資料６－３

構成員等からの主なご意見

令和５年６月

前回分科会における主なご意見①（端末側における対策（NOTICE））

【1. 情報通信ネットワークにおけるサイバーセキュリティを巡る現状】

- 情報通信ネットワークへの依存性が毎年高まる一方であるという前提については強調すべき。【後藤主査】
- メーカー、通信事業者、NOTICEと色々な主体それぞれの取組が重要であり、全体としてどのような方向性となるのかを、本文の前段で示し、各施策が今後成功するかの見通しを立てるためにも、過去の成功事例について記載すべき。【齋藤構成員】

【2. 端末側における対策（NOTICE） ①脆弱性があるIoT機器の調査の延長・拡充】

- 新しい脆弱性や外部に公開すべきではないポートについて注意喚起することは重要。【辻構成員、井上構成員】
- 2019年のNOTICE開始時はメディアの反応を踏まえて、かなり慎重な実施に舵を切ったという経緯がある。次期NOTICEの検討にあたっては、本分科会で透明性をもって検討を進めているため、メディアとコミュニケーションを取りながら十分な情報展開及び広報活動をしていく必要がある。【井上構成員】
- 端末側の対策として、従来の利用者への脆弱性の通知に終始するのではなく、NOTICEを端末側に関する対策の在り方と位置づけ、広く踏み込んだ対策を実施していく方向性が見えるように、「2. 端末側に対する対策（NOTICE）」という見出しや本文で明確に示すべき。【小塚構成員】

【2. 端末側における対策（NOTICE） ②利用者への注意喚起の実効性向上】

- 注意喚起の認知度が上がって、何か対応しなければと思ったときに参照されるNOTICEサポートセンター等のホームページの拡充が非常に重要。様々な方々に感心を持ってもらうためのリーチの手法も大切。【藤本構成員、辻構成員】
- NOTICEの取組で脆弱性が確認できたとき、それが意図されたものか判別できないケースが多く、どこまで踏み込んで注意喚起をするかの判別が難しいため、今後は技術的にも考えていかなければならない。【吉岡構成員】
- 端末設備の接続に関するガイドラインについて、感染機器の利用者は被害者でもあるため、関係者と丁寧に議論することや、累次にわたって注意喚起に応じない利用者の中には、注意喚起が全く届いてない場合もあり得るため、慎重な検討が必要。感染機器が社会に悪影響を与えるという認識を持たせる機会を設けることも必要。【田中構成員、河村構成員】
- 対消費者契約と対事業者契約ではこの点規制の強さが違うため、その点も踏まえながらガイドラインを策定する必要がある。【小塚構成員】
- 注意喚起をするときは、脆弱性だけでなく、どういった不利益があるのか、どういった対応が必要かもセットで伝えることで、ユーザーへの動機付けを強めることも大切。【辻構成員】

前回分科会における主なご意見②（端末側における対策（NOTICE））

【2. 端末側における対策（NOTICE） ③メーカーやSIer等の幅広い関係者との連携による総合的な対処】

- NOTICEの活動について、過去の取組ではメーカーやSIerを巻き込むことができず、注意喚起が活動の中心となり、注意喚起疲れが生じた。従前の注意喚起に頼った対策から脱却するために、メーカーやSIerとの連携が重要。【小山構成員、吉岡構成員】
- 「安全な機器やサービスを選ぶといった利用者に求められる役割」との記載について、利用者が安全なものを選ぶことができるための情報が豊富にあることが重要。製品そのものへの表示だけではなく、売場やWebサイトへの表示も効果的かと思うため、ネットショッピングの提供事業者や量販店などもステークホルダーに含めるべきではないか。【河村構成員】
- 現状の注意喚起に対して対策の精度を上げていくために、販売店やSIer等の役割や利用者側の役割等、他のステークホルダーに関しても期待する対応を記載するのはどうか。【齋藤構成員】

【2. 端末側における対策（NOTICE） ④①～③を効果的に実施するためのNOTICEの運営体制の強化】

- 実施計画の改訂に係る手続に時間がかかり、危険なポート番号が判明しても即時対応できない場合があるため、調査の柔軟性や機動性を確保する仕組みが必要。また、人員の確保も重要。【井上構成員】
- 攻撃の発生原因を追究し、攻撃が起こる前に通知が出来ると良いと思うが、実際の脆弱性の多くは個々の機器の脆弱性にとどまらず、根本原因が機器のハードウェアやチップなどの、ベンダーが出しているBSP（ボードサポートパッケージ）や、オープンソースソフトウェアに起因している場合も多くあり、NOTICEでは脅威の氷山の一角しか見ていないこともある。個々の機器以外の脆弱性についてもしっかりと分析し、問題の程度や影響度等を調査し、世界的に発信できると、日本の活動として注意喚起の価値が高くなる。【吉岡構成員】
- 従来のマルウェア感染事案においても、ISP毎のIPアドレスレンジにより違いがあると知られており、今回のフロー分析においてもISP毎に分析結果に違いが出ることを再確認できた。得られた情報の利活用は整理すべき課題であり、C&Cサーバ調査プロジェクトとNOTICEステアリングコッミティの取組が上手くすり合っていくように、情報共有の検討が重要。【小山構成員】

前回分科会における主なご意見③（ネットワーク側その他における対策）

【3. ネットワーク側その他における対策】

- IoTボットネットの全体像の可視化について、可視化は一つの手段であって目的ではないため、可視化を進めることで最終的にボットネットの縮小などに取り組むというところまで記載を進めて良いのではないか。【田中構成員】
- 国内で見つかったC&Cサーバにどう対処していくか、対処について可能となる取組も検討すべき。【辻構成員】
- C&Cサーバは海外で発見されているという話もあり、取得した情報を国際的にも共有した上でさらに連携が先にあると思うところ、検知技術や取得する情報自体も始めから海外の取組と協調していく必要もあるのではないか。【小塚構成員】
- 情報共有の重要性と課題について、各ステークホルダー間でのデータをオープン化すると周知広報にもつながるかもしれないが、他方で機微な情報があると課題も多い。海外との共有になるとさらに難しいところもあると思う。【後藤主査】
- 省庁間の情報共有にも課題があるのではないか。C&Cサーバの検知に関し得られた情報はISPや総務省の範囲内だけではなく、官民の情報も広く共有し相互に対応能力を上げることも検討すべき。【辻構成員】
- 端末とネットワークの対策と、IoTボットネット可視化により最終的にボットネット縮小を目指していくといった全体像を絵のような形で示していただいた方が、本施策全体に対する関係者の理解も深まる。現状、文字のみの報告書案となっているので、次回以降、その部分などを構成に追加するとより読みやすい。【田中構成員】