参考資料１

第１回分科会における構成員等からの主なご意見

令和５年２月

構成員等からの主なご意見①

情報通信ネットワークにおけるサイバー攻撃の脅威の認識

- 現状国内のIoTボットネットは海外に攻撃を発していたとしても、攻撃者次第でDDoS攻撃が国内に向けられる可能性もあることから、継続的な対策が必要。【小山構成員、吉岡構成員】

調査対象の拡大・利用者への注意喚起以外の対処方法の在り方

- パスワード設定等の不備以外の脆弱性も含めて、NOTICEの調査対象や機器所有者への注意喚起対象を検討していくべき。【吉岡構成員、井上構成員】
- リスクの高いボットネットから対策を進め、通信フロー分析等によるボットネットの把握、メーカーと連携したマルウェア感染・脆弱性診断（am I infected?）の取組、通信の瞬断やテイクダウン等、複合的な対策と効果測定をやってはどうか。【小山構成員】

参加ISPの拡大・既に参加しているISPのインセンティブの確保に向けた方策

- ISPとしては、注意喚起の対象拡大は、運営体制や注意喚起手法の検討と同時に進める必要があると考える。【齋藤構成員】

利用者側におけるIoT機器の適切な管理など、注意喚起の実効性を向上させていくための方策

- マルウェアの感染によって消費者自身が直接被害を受けないケースも多いが、それによって不正なサイトに誘導されるような事例もある。【吉岡構成員】
- 「am I infected?」のような、IoT機器の感染状況を調査する取組をどんどん周知すべき。事業者がIoT機器を提供する際、保守運用の一環として、こうした取組を活用して感染状況を確認することを推奨するなど、普及啓発したい。【小山構成員】
- 利用者の関心や理解に留意しつつ、NOTICEの注意喚起の意味（対象のサイバー攻撃の危険性、利用者自身が攻撃に加担して見える場合がある旨等）や対処方法等を分かりやすく伝えていくことが必要。【ICT-ISAC、吉岡構成員、河村構成員】

メーカー側の適切なサポートの在り方

- 「am I infected?」のような、IoT機器の感染状況を調査する取組をどんどん周知すべき。事業者がIoT機器を提供する際、保守運用の一環として、こうした取組を活用して感染状況を確認することを推奨するなど、普及啓発したい。【小山構成員　再掲】
- 消費者への注意喚起には限度があり、メーカーの対策により消費者が思い悩まなくても済むような仕組みを作っていく必要がある。【河村構成員】

構成員等からの主なご意見②

前述の課題等に効果的に対応していくための今後のNOTICEの枠組みと運営の在り方

- NOTICEで用いる識別符号の追加には、実施計画書の変更について総務大臣認可が必要だが、手続に半年程度要し、タイムリーな対応の一つのハードルでもある。また、調査実施機関のNICTとしては、調査体制の維持、人員確保も大きな課題となっている。【井上構成員】
- ISPとしては、注意喚起の対象拡大は、運営体制や注意喚起手法の検討と同時に進める必要があると考える。【齋藤構成員再掲】
- サイバー攻撃対策全体としてのNOTICEの位置づけを行った上で、NOTICEによって出来上がった注意喚起の枠組みを上手く活用し活動の幅を広げていくべき。【吉岡構成員】

ネットワーク側の対策（フロー情報分析の可能性）

- 少数の攻撃サーバから攻撃を行う場合は、大規模感染していてもダークネットやハニーポットで観測できない可能性があり，フローデータの分析など別の観測方法が必要となる。【吉岡構成員】
- リスクの高いボットネットから対策を進め、通信フロー分析等によるボットネットの把握、メーカーと連携したマルウェア感染・脆弱性診断（am I infected?）の取組、通信の瞬断やテイクダウン等、複合的な対策と効果測定をやってはどうか。【小山構成員再掲】

その他

- 日本の中で考えても収まらない部分がたくさんあり、国という単位では解決しない部分は増えていく。何が制約になっていて、どのような解決手段があるのかもぜひ議論したい。【後藤主査】