資料５－２

これまでの論点整理等に対する主なご意見

令和5年5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））

【脆弱性等のあるIoT機器の調査】

- NOTICEの取組については着実に成果を挙げていることを踏まえ、今後も継続していくべき。【後藤主査】
- IoT機器を狙う攻撃の脅威が多様化しており、NOTICEの効果を維持するためにも、ID・パスワードの設定不備以外の脆弱性の対応を検討すべき。【吉岡構成員】
- 脆弱性を狙う攻撃パターンが増加しているため、適切にフォローアップ及び調査対象を拡大することで、日本のネットワークの状況を把握することは重要。感染機器だけでなく脆弱性のある機器を潜在的なリスクとして認識し観測する必要がある。【NICT笠間氏】

【利用者への注意喚起】

- 利用者に何らかのアクションを求める情報伝達をする場合には、実際のリアクションに繋げるための伝達の仕方や、普段セキュリティの情報に触れない層にどう情報をリーチさせるか戦略的な検討が必要。【藤本構成員】
- 利用者による対処に頼るのは難しいため、利用者が意識しなくても機器の安全性を確保していく取組が重要。【河村構成員】
- 端末の接続拒否については慎重に行うべきではあるが、NOTICEの取組を加速させる観点でも接続拒否制度の利用者への啓発や、接続拒否のための要件及び手続の明確化による当該制度の活用を検討すべき。【吉岡構成員】

【メーカーの対応】

- 利用者、ISP及びメーカー等のステークホルダー各々がどれだけの事を実施するのか、関係者間で協議しながら全体的にバランスの取れた施策とすべき。【後藤主査、齋藤構成員】

【NOTICEの運営】

- NOTICEについては、一つの手段としてその効果を確認しながら、多数のステークホルダーが相互に協力しバランスの取れた対策とすることが重要。【後藤主査】
- IoT機器の調査対象の拡大にあたっては、人員や体制を柔軟に確保出来るような対応をお願いしたい。【NICT笠間氏】
- これまでのNOTICEの調査により、国内機器の機種・バージョン情報のデータも蓄積されているため、データの活用により国内の状況の可視化や関係団体との協調に繋げたい。【NICT笠間氏】
- 本分科会で整理した取組全体を通じて、目指すべき共通の到達点・目標を設定すべき。【後藤主査、田中構成員、斎藤構成員】

前回分科会における主なご意見②（ネットワーク側その他における対策）

【C2サーバの検知・検知情報の共有・利活用】

- MiraiやEmotetのC2サーバの検知も出来ており、今後の成果が期待される。【小山構成員】
- 検知したC2サーバ情報の共有が遅れると、C2サーバのIPアドレスが既に移動していて有効活用ができない可能性もあるため、検知結果の素早い共有方法や対策の検討が必要。【後藤主査、辻構成員】
- 各社が自社網におけるC2サーバの状況を確認出来ることが、日本全体のネットワークの状況を見る上で必要。【齋藤構成員】
- 検知結果のISP間の相関を見ると、ISPごとに検知しているC2サーバの系統が異なるため、検知ポイントを増やすことが出来れば全体像が見えてくるだろう。【辻構成員】
- 各社の分析手法等を共有する上では、精度向上やノウハウ蓄積のため、各社ある程度同じ対象を調査した上で、対策を行うべきIoT機器やボットネットを確定する必要がある。【小山構成員】
- 検知されたC2サーバへの対応については、利用者への注意喚起等をせずになるべく大元でどのような効果的な対策を取れるかという観点から検討できると良い。【河村構成員】

【IoTボットネットの可視化】

- C2サーバの居場所は頻繁に変わる一方で、感染端末の場所は変わらないため、感染端末は次々異なるC2サーバから攻撃指令を受けている状況。そのためIoTボットネットの全体像の可視化を進めることは大変重要であり、統合分析対策センター（仮称）の取組に期待したい。IoTボットネットの変遷を可視化し、対策の効果を確認できると良い。【小山構成員】
- 各社が自社網におけるC2サーバの状況を確認出来ることが、日本全体のネットワークの状況を見る上で必要。【齋藤構成員】（再掲）
- 検知結果のISP間の相関を見ると、ISPごとに検知しているC2サーバの系統が異なるため、検知ポイントを増やすことが出来れば全体像が見えてくるだろう。【辻構成員】（再掲）
- IoTボットネットの対策による効果を上げていくには、ボットネットの追跡性を高める意識をしながらC2サーバの検知精度の向上に取り組むことが必要。【小山構成員】

前回サイバーセキュリティタスクフォース（４／２８）でいただいた主なご意見

- 既に運用されているIoT機器への対策も重要であるが、これから出てくる新たな製品についてもラベリングや適合性評価等の観点から対策を考えていく必要があるのではないか。【後藤座長、徳田構成員、中尾構成員】

- NOTICE運営に必要な人員の確保についてはISPにとっても負担となっているため、フロー全体を見直す良い機会と考えている。【徳田構成員】

- 「サイバー攻撃に効果的に対処していくためには、脆弱性のあるIoT機器、ボットネット、C2サーバ等全体を俯瞰した対応が必要」という指摘は大変重要であるが、その対応策として統合分析対策センター（仮称）の立ち上げのみならず、幅広い対策が必要ではないか。【林構成員、若江構成員】