資料４－４

これまでの論点整理（案）

令和5年4月

これまでの情報通信ネットワークにおけるサイバーセキュリティ対策分科会の検討状況

これまでの情報通信ネットワークにおけるサイバーセキュリティ対策分科会（以下「分科会」という。）において、

- IoTにおけるサイバーセキュリティの確保に向けた取組（NOTICE等）の現状と課題
- 情報通信ネットワークにおけるサイバーセキュリティ対策の現状と課題（総合実証の検討等）
- 上記課題の解決に向けた必要な検討

等についてご議論いただいたところ。

回　次	議　事　内　容
第１回 （R5.1.18）	✓ 情報通信ネットワークにおけるサイバーセキュリティ対策分科会について ✓ IoTボットネットの現状について（吉岡構成員） ✓ NOTICEの取組状況について （NICT、ICT-ISAC、NOTICEサポートセンターヒアリング）
第２回 （R5.2.16）	✓ 通信事業者によるサイバーセキュリティ対策の取組状況と課題について （NTTコミュニケーションズ、KDDI、ソフトバンク、インターネットイニシアティブ、ICT-ISACヒアリング）
第３回 （R5.3.16）	✓ 国内のIoT機器が踏み台となった最近のサイバー攻撃事案について ✓ 地域ISP等によるサイバーセキュリティ対策の取組状況と課題について （射水ケーブルネットワーク、INC長野ケーブルテレビ、JAIPAヒアリング） ✓ メーカー等によるサイバーセキュリティ対策の取組状況と課題について （DLPA、ヤマハ、ゼロゼロワンヒアリング）
第４回 （R5.4.21）	✓ フロー情報分析によるC&Cサーバ検知に関する調査の報告（NTTコミュニケーションズ） ✓ 効果的な利用者への周知啓発について（辻構成員） ✓ 諸外国のボットネット対策について

（１）脆弱性等のあるIoT機器の状況

【現状とこれまでの成果】

- 今年度末までの5年間の時限措置として、NICTが、不正アクセス禁止法の例外として、特定アクセス行為によりID・パスワードに脆弱性のあるIoT機器を検知し、認定協会であるICT-ISACを通じてISPに通知し、利用者への注意喚起を実施。参加ISPの数も徐々に拡大し、現在は77社のISPが参加中。
- 上記に加え、NICTがNICTERにより感染通信を出しているIoT機器を検知し、NOTICEの枠組みを活用して、利用者への注意喚起を実施。

【課題】

- 情報通信ネットワークの機能に支障を及ぼし得るサイバー攻撃の発生数や規模等は増大しており、こうした攻撃に悪用される可能性のあるIoT機器の数も、デジタル化を背景に引き続き増加することが見込まれる。
- 外部から来る攻撃通信よりも、自網内のボットネットから外部に向かう攻撃通信の方が対策が困難。そのため、ボットネットを可能な限り減らしていく取組が必要。
- ID・パスワードに脆弱性があるIoT機器は現在でも一定数残存。そのうち、2020年のIoTセキュリティ基準施行前に発売された古い機器が大半を占めている。
- 感染通信を出しているIoT機器の検知数は、昨年春以降、マルウェア活動の活発化等を背景に高止まっている。
- ファームウェア等のID・パスワード以外の脆弱性があるIoT機器を狙った攻撃（リモートコード実行等）が増えているが、こうした機器については、NOTICEの調査の過程で検知できる場合があるものの、現行のNOTICEにおいて対処はできていない。

【対応の方向性（案）】

- 現在のサイバー攻撃の脅威や脆弱性等のあるIoT機器の状況等を踏まえ、NOTICEについては継続して取り組む必要があるのではないか。
- ID・パスワード以外の脆弱性のあるIoT機器についても、NOTICEの枠組みを活用して幅広く対処を可能とすべきではないか。

1．端末側の対策（NOTICE）の現状と課題

【第3回までの構成員等のご意見】

＜対策の必要性＞

- 端末に関して認識している脅威としては、DoS/DDoS攻撃の踏み台となること、不正アクセスの踏み台となること、端末内のプロバイダ情報を盗んで悪用されることがある。【ヤマハ】
- 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】
- 国内数千台のボットであっても数百GbpsものDDoS攻撃が生じた事例のインパクトは大きく、機器ベンダとの連携、攻撃観測と対処、ユーザーサポート等を組み合わせた有効な対策を実施していくべき。【*小山構成員*、吉岡構成員】
- 中から外に向かう攻撃通信が脅威。原因者の特定や、脆弱性のある機器情報の共有により、プッシュ型で顧客のサポートができるようになることがNOTICEに期待する部分。【INC長野ケーブルテレビ、射水ケーブル】
- outboundの大量性を伴う通信についても、頻度や規模が増している。自社網を安定的に運用するために、このような攻撃に積極的に対応することが必要だが、inboundの通信よりも対策の難しさがある。【齋藤構成員】
- C&Cサーバの通信に対処できたとしても、放置することで他の攻撃者に脆弱性や認証情報が悪用される可能性が高いことから、今個別に行っている活動を連携させ、IoTが勝手に悪用されない対策を行うべき。【齋藤構成員】

＜NOTICEの調査対象＞

- 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。【井上構成員、吉岡構成員】
- 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】
- 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】
- 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】
- ルータ自体だけでなくその先に接続されている機器も攻撃対象となっているのであれば今後そのような機器にも対策を広げていく必要がある。【吉岡構成員】

（２）利用者への注意喚起

【現状とこれまでの成果】

- 利用者への注意喚起によって脆弱性のあるIoT機器は一定数減少。あるISPにおいて注意喚起の進捗状況を適切に管理することで、ID・パスワードに脆弱性等のあるIoT機器がゼロになった事例もある。
- 利用者からの問合せ対応等のため、「NOTICEサポートセンター」を設置。
- 一部のISPでは、IoT機器が適切に管理されるよう機器のレンタルサービスを提供している事例もある。
- インターネット等に接続される端末が、端末設備等規則で定めるIoTセキュリティ基準を満たさない場合等において、ISPが端末の接続を拒否できる制度を措置。

【課題】

- IoT機器の適切なセキュリティ対策に対する利用者の意識が十分ではなく、対策方法も一般の利用者にとって難しいものとなっている。
- 法人利用者については、管理責任の所在が曖昧など適切なIoT機器の管理体制がないケースや、コストがかかるため、実害がない限りはファームウェアの更新や設定変更が行われないケースがある。
- 利用者において実際に対処を完了したかどうか確認が出来ていない等、注意喚起による効果測定が十分に行われていない。
- サイバー攻撃に悪用されるおそれのある端末を接続拒否する約款については、利用者の理解が得られにくいことが課題。

【対応の方向性（案）】

- NOTICEの情報発信とあわせて、メーカーやSIer等の関係者と連携しつつ、IoT機器の適切な管理に関する利用者への周知啓発を更に強化する必要があるのではないか。
- ファームウェアの自動更新等、利用者が意識せずにIoT機器を適切に管理可能な製品・サービスの普及に努めるべきではないか。
- 利用者への実態調査や「am I infected?」との連携等により、注意喚起による効果のより詳細な把握に努めるべきではないか。
- サイバー攻撃に悪用されるおそれのある端末の接続拒否については、注意喚起の実効性向上に向けて、利用者の理解を十分に得つつ、ISPが対応可能な方策を検討していく必要があるのではないか。

【第3回までの構成員等のご意見①】

＜周知啓発強化＞

- 「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。【河村構成員、吉岡構成員、ICT-ISAC】
- ルータのような機器にはセキュリティ寿命があり、あまりにも古いものを使っていること自体にはある程度ユーザー側にも責任があるとも言える。ファームウェア更新やサポート終了といった情報の効果的な利用者側への提供の仕方も課題。【吉岡構成員、DLPA】
- 利用者にセキュリティの話をする場合、機器購入のタイミングでわかりやすく説明することが必要。【小山構成員、藤本構成員】
- NOTICEの枠組で注意喚起への対処がなされないのは法人が大半。担当者の存否や、SIerが入る場合に契約者と管理者が異なり問題の所在が曖昧になる等、対処のハードルが高い点を考える必要がある。【小塚構成員、小山構成員、田中構成員、ヤマハ】
- 法人ユーザーが用いる機器には、インターネット接続を想定せず、Slerによる設定のために全てのポートが開いた状態で販売しているものがあった。意図的な設計であれば良いかもしれないが、メーカーが想定しない利用時のリスク対策ついて何も考えていない場合は問題。リモートからアクセスする必要性がある場合に必要な対策については周知が必要。【小山構成員】

＜利用者の対策が不要なサービス・製品の普及＞

- 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る消費者が思い悩まなくても済むような仕組みづくりやネットワーク側での対策が重要。【河村構成員、後藤主査】
- セキュリティ性能の高さが機能や価格同様に製品の付加価値として認識される市場形成ができるとよい。【井上構成員】

【第3回までの構成員等のご意見②】

＜効果の把握＞

■ NOTICEプロジェクトを発展させていくためには、利用者が対処を行ったのか、問い合わせ後の問題の有無など効果測定を行っていくことが課題。【NOTICEサポートセンター】

＜端末の接続拒否等の対応＞

■ 技術的条件に基づき契約約款上で禁止行為及び違反時の利用停止措置を規定しているが、脆弱性を理由とした停止措置は利用者からの理解を得ることが困難。【田中構成員】

（３）メーカーの対応

【現状とこれまでの成果】

- IoT機器の適切な管理に関する利用者への周知啓発、機器のサポート期間終了やファームウェアの更新等に関する情報提供に取り組んでいる。
- DLPAに加盟しているメーカーにおいては、個体毎に異なるID・パスワードが設定されており、ファームウェアの自動更新機能を有しているルーターを「DLPA推奨Wi-Fiルーター」として販売しており、当該ルーターについてはNOTICEの調査においてこれまで1台も検知されていない。
- NOTICEとの連携により、ファームウェアの改修や新製品のセキュリティ機能の改善につながった事例もある。

【課題】

- メーカーのサポート期間が終了しているEOL（End Of Lifeの略）を迎えた古いIoT機器や、ファームウェアが古いままになっているIoT機器が一定数残存。
- 中小企業の場合、大企業と比較してコストを抑えるため壊れるまで機器を利用する傾向が強く、10～15年利用される事例もある。

【対応の方向性（案）】

- 引き続き、関係者と連携しつつ、サポート期間終了やファームウェアの更新等に関する情報の確実な提供、利用者にとって分かりやすい設定・操作が可能な機器やマニュアルの提供、IoT機器の適切な管理に関する周知啓発に努めるべきではないか。
- サイバー攻撃の脅威情報の共有や脆弱性のある機器への対処等、NOTICEとメーカーとの連携を更に促進する必要があるのではないか。

【第3回までの構成員等のご意見】

＜メーカー等との連携の必要性＞

- 初期のMiraiのようにTelnetから多様な機器に感染する、というケースだけでなく、特定機種の脆弱性やセキュリティ不備を狙った攻撃も増えるため、機器のベンダとの連携の重要度がさらに高くなる。【吉岡構成員】
- NOTICEの取組は、現在は実際に調査をしているNICTとISPと総務省の枠組みでの活動となっているが、今後次期NOTICEで機器を実際に製造しているメーカーも含めた一体的活動となるための体制を検討したい。【井上構成員、DLPA、ヤマハ】
- 監視カメラ等の機器が踏み台になる状況は日本以外でも同じような状況である可能性がある。今後はネットワークのフローを見ることができる通信事業者とメーカとが連携し、バナー情報やC&Cサーバとの通信の有無等から踏み台となっているIoT機器等の対象を絞って対策を打つべき。【小山構成員】
- 「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】（再掲）
- 法人ユーザーが用いる機器には、インターネット接続を想定せず、SIerによる設定のために全てのポートが開いた状態で販売してあるものあった。意図的な設計であれば良いかもしれないが、メーカーが何も考えていない場合は問題。リモートからアクセスする必要性がある場合に必要な対策については周知が必要。【小山構成員】（再掲）
- ルータのような機器にはセキュリティ寿命があり、あまりにも古いものを使っていること自体にはある程度ユーザー側にも責任があるとも言える。ファームウェア更新やサポート終了といった情報の効果的な利用者側への提供の仕方も課題。【吉岡構成員、DLPA】（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る消費者が思い悩まなくても済むような仕組みづくりやネットワーク側での対策が重要。【河村構成員、後藤主査】（再掲）
- IoT機器メーカー数は多く、上流工程でのセキュリティ対策だけでは必要性の訴求方法が課題。【齋藤構成員】
- ISP、機器メーカ及び関係者がそれぞれ独立したセキュリティ対策活動を行うのではなく連携することが必要。特に機器メーカは業界の連携が進んでいるようであり、モデルケースとして活動を広げるべき。【吉岡構成員】

（４）NOTICEの運営

【現状とこれまでの成果】

- NOTICEの取組により、脆弱性等のあるIoT機器の全体的な動向を把握し、注意喚起等の対処につなげる枠組みができたことは大きな成果。
- NOTICEの調査の過程でISPが管理しているIoT機器に脆弱性があることが判明し、 ISPと連携してパスワードを変更した事案、ISPやメーカーと連携してファームウェアの更新・適用を行った事案等、利用者への注意喚起を実施せずに対処に成功した事案もある。
- Emotetに感染している端末の利用者への注意喚起を実施した事案等、NOTICEの枠組みを活用して当初想定していなかったサイバー攻撃のリスクに対処した事案もある。

【課題】

- NOTICEに参加しているISPにとっては、NICTが検知したIoT機器の通知を受けた後、利用者の特定から注意喚起、問合せ対応までの一連の業務に係る負担が大きく、効率性も踏まえて取り組むことが必要。
- 未参加ISPが管理するIPアドレスは調査対象外。

【対応の方向性（案）】

- ISPによる利用者への注意喚起のみに依存せず、多様な関係者と連携しつつ事案の性質に応じた柔軟な対処を進めることが必要ではないか。
- PDCAサイクルを回しながら、NOTICEの柔軟かつ効率的な運営に取り組む必要があるのではないか。
- NOTICEの情報発信に引き続き取り組み、参加ISPの拡大を図るべきではないか。

【第3回までの構成員等のご意見】

＜注意喚起に限定しない柔軟な対処＞

- 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】（再掲）
- 注意喚起を行うためには、ユーザー特定から文面作成・送付の一連の流れに相当な金額・負荷がかかることから、今後は効果とのバランスをとっていくことが課題。【小山構成員、田中構成員、ソフトバンク】

＜柔軟かつ効果的な運営体制＞

- 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】
- NOTICEの取組は、現在は実際に調査をしているNICTとISPと総務省の枠組みでの活動となっているが、今後は機器を実際に製造しているメーカーも含めた一体的活動となるための体制を検討したい。【井上構成員、DLPA、ヤマハ】（再掲）
- ISP、機器メーカ及び関係者がそれぞれ独立したセキュリティ対策活動を行うのではなく連携することが必要。特に機器メーカは業界の連携が進んでいるようであり、モデルケースとして活動を広げるべき。【吉岡構成員】（再掲）

＜参加ISPの拡大＞

- 中から外に向かう攻撃通信が脅威。原因者の特定や、脆弱性のある機器情報の共有により、プッシュ型で顧客のサポートができるようになることがNOTICEに期待する部分。【INC長野ケーブルテレビ、射水ケーブル】（再掲）

（1）C2サーバの検知・検知情報の共有・利活用

【現状とこれまでの成果】

- 通信ネットワークのフロー情報分析により検知された被疑C2サーバをリスト化。検知されたC2サーバの一部については、既存の手法よりも早期に検知されたことを確認。
- C2サーバリストの情報共有・利活用の在り方やC2サーバの検知手法の共有について検討し、課題を整理。

【課題】

- C2サーバの検知精度の向上に向けて、検知や評価の手法の更なる改善、検知されたC2サーバの活動状況の継続的な観測が必要。
- 円滑かつ迅速にC2サーバリストが共有されるような仕組みの検討とあわせて、C2サーバリストの具体的な利活用シーンについて更に整理が必要。
- フロー情報分析によりC2サーバを検知できる技術・リソースを有するISPは一部に限られている。

【対応の方向性（案）】

- 必要に応じて関係機関と連携しつつ、C2サーバの更なる検知精度の向上を図るとともに、C2サーバの活動状況をリアルタイムで把握するための死活監視に取り組むことが必要ではないか。
- C2サーバリストの効果的な共有・利活用に関する具体的な枠組み・ルールの策定に向けて検討を加速すべきではないか。
- C2サーバの検知手法に関するISP間の情報共有の促進等、可能な限り多くのISPがC2サーバの検知に参加できるような環境の整備に取り組むことが求められるのではないか。

2. ネットワーク側その他の対策の現状と課題

【第3回までの構成員等のご意見】

- 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】
- 消費者にセキュリティ対策を要請するのは難しい。機器設計段階でのより上流の対策やネットワーク側での対策が重要。【河村構成員、後藤主査】
- 経験則として、外部インテリジェンス情報は、自社網で検知したマルウェアの活動とは合致しない。自社網でのマルウェアの活動は各ISPがそれぞれ観測し、フロー情報分析等の手法で自社網での攻撃発生状況については常時監視することが必要。【齋藤構成員】

（２）IoTボットネットの可視化

【現状とこれまでの成果】

- 端末側の対策としてNOTICEプロジェクト、ネットワーク側の対策としてC2サーバの検知等に関する実証を各々で実施。

【課題】

- 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であり、様々な情報を重ね合わせていくことで精度を上げながら全体像を把握していくことが重要。
- 恒久的な対策に向けて、対処が必要なIoT機器の情報、マルウェアの情報、C2サーバの情報、サイバー攻撃の発生に関する情報等、全ての情報がそろっていることが必要であるが、個々のISPにとってはこれらの情報を総合的に収集・分析することは困難。

【対応の方向性（案）】

- NOTICEで検知された対処が必要なIoT機器や今般の実証で検知したC2サーバのリスト等、端末側・ネットワーク側両面から情報の収集・分析を行い、IoTボットネットの全体像の可視化につなげていくための観測網である「統合分析対策センター（仮称）」を立ち上げ、ISP等の関係者が連携しつつ総合的なIoTボットネット対策に取り組むことが必要ではないか。

【第3回までの構成員等のご意見】

- ■ 施策の効果を測定するという観点からも、ボットネットの状況等の全体像を可視化していく取組が重要。特に、一元的に情報を集め、複数の組織で参照できることが望ましい。【齋藤構成員、田中構成員、ソフトバンク】
- ■ 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）
- ■ フロー情報分析について、認定協会業務との連携の余地はないか。フロー情報だけで何か分かるわけではないため、他のセキュリティ情報との突合や分析ノウハウの共有が重要。【小山構成員】
- ■ セキュリティ人材は、高度なスキルを持った関係者が1ヶ所にいるというより、各段階での薄く広い育成がまずは重要。深いインテリジェンスは専門的な領域であるため、フロー情報など現場のデータに研究者が触れられる環境を作る取組も重要。【小山構成員、吉岡構成員】