資料43－３

# 「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」の検討状況について

令和５年４月

サイバーセキュリティタスクフォース事務局

# 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<br>（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<br>✓ IoTボットネットの現状について（吉岡構成員）<br>✓ NOTICEの取組状況について<br>（NICT、ICT-ISAC、NOTICEサポートセンターヒアリング） |
| 第２回<br>（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<br>（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<br>（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<br>✓ 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<br>（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）<br>✓ 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<br>（DLPA、ヤマハ、ゼロゼロワンヒアリング） |
| 第４回<br>（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）<br>✓ 効果的な利用者への周知啓発について（辻構成員）<br>✓ 諸外国におけるサイバーセキュリティ対策の取組事例<br>✓ 論点整理 |

**今後のスケジュール（予定）**

第５回（５月中旬）　とりまとめ骨子（案）

第６回（６月中旬）　とりまとめ（案）

# 1. 端末側の対策（NOTICE）の現状と課題

## （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。
- 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。

## （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。

## （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。

## （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。

## （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）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。

# （参考）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

## 目的

- サイバー空間があらゆる主体が利用する公共空間となり、デジタル化を支える情報通信ネットワークは、今や国民生活や経済活動の重要かつ不可欠な基盤となっている中、サイバー攻撃により情報通信ネットワークの機能に支障が生じた場合には、社会・経済に多大な影響を及ぼすおそれがあり、その安全性・信頼性の確保は喫緊の課題。
- 本年８月にとりまとめられた「ICTサイバーセキュリティ総合対策2022」を踏まえ、依然としてIoT機器を狙ったサイバー攻撃が多く発生している状況等に対応するため、NOTICEや「電気通信事業者による積極的なサイバーセキュリティ対策に関する総合実証」等の取組みを含めた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について検討を行うことを目的として、「サイバーセキュリティタスクフォース」の下に分科会を設置。

## 主な検討事項

- 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方策

## 構成員

| | | | |
|---|---|---|---|
| 後藤　厚宏 | 情報セキュリティ大学院大学　学長 | 井上　大介 | NICTサイバーセキュリティ研究所 サイバーセキュリティネクサス長 |
| 河村　真紀子 | 主婦連合会　会長 | 小塚　荘一郎 | 学習院大学法学部　教授 |
| 小山　覚 | (一社)ICT-ISAC　ステアリング・コミッティ運営委員長<br>NTTコミュニケーションズ（株）　情報セキュリティ部長 | 齋藤　衛 | (株)インターネットイニシアティブ　セキュリティ本部長 |
| 田中　暁 | KDDI(株)　情報セキュリティ本部　セキュリティ管理部長 | 辻　伸弘 | ＳＢテクノロジー(株)　プリンシパルセキュリティリサーチャー |
| 藤本　正代 | 情報セキュリティ大学院大学　教授 | 吉岡　克成 | 横浜国立大学大学院環境情報研究院　教授 |

（オブザーバ）ＮＩＳＣ、経産省

## スケジュール

| | |
|---|---|
| 令和４年１２月 | 第41回サイバーセキュリティタスクフォース（分科会設置を決定） |
| ５年　１月 | 第１回分科会（以降月１回程度のペースで開催） |
| 令和５年夏 | とりまとめ |