資料44－４

「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とりまとめ」（案）の概要

令和５年６月

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

（１）国民の日常生活や社会経済活動に必要不可欠な情報通信ネットワーク

- 社会全体のデジタル化の進展に伴い、必要不可欠な基盤としての情報通信ネットワークへの依存度は更に高まっている。

（２）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やIoTボットネットの現状

- **サイバー攻撃の発生件数や規模の増大**
  DDoS攻撃等のサイバー攻撃の発生数・規模とも引き続き増大しており、こうしたサイバー攻撃が踏み台として利用するIoT機器、サーバ、コンピュータ等のいわゆる「攻撃インフラ」も拡大。
- **IoT機器を狙った攻撃**
  無差別型サイバー攻撃の観測網であるNICTERの調査によれば、IoT機器を狙った攻撃が最も多くの割合を占めており、特に、昨年春以降、Mirai系マルウェアの活動が活発化。特に脆弱性のあるネットワークカメラの感染による影響が大きい。
- **サイバー攻撃手法の多様化**
  最近では、ファームウェアをはじめとする様々な脆弱性を狙ったマルウェアが増える等、サイバー攻撃の手法も多様化。

（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の強化に向けて

- 大規模サイバー攻撃への対策として、攻撃インフラの拡大を防ぐ端末（IoT機器）側の対策、IoTボットネットに対して指令を出すC&Cサーバへの対処を行うネットワーク側の対策の双方から、総合的なIoTボットネット対策を講じていくことが必要。
- 端末（IoT機器）側の対策については、裾野が非常に広く様々な種類があり、メーカーも多数存在していることや、ライフサイクルが長い等のIoT機器の特性も十分踏まえ、ISP、メーカー、SIer、流通業者、利用者等のステークホルダー各々が適切に役割分担をしながら、必要な対策を講じていくことが必要。

2. 端末側における対策（NOTICE）①

（１）これまでの取組

- 2018年にNICT法を改正し、５年間の時限措置（不正アクセス禁止法の例外）として、NICTが、ID・パスワードに脆弱性のあるIoT機器を調査してISPに通知を行い、ISPが個別の利用者への注意喚起を行う取組を2019年２月に開始。
- 上記の取組に加え、NICTが、NICTERによりマルウェアの感染通信を出しているIoT機器を調査し、NOTICEの枠組みを活用して個別の利用者への注意喚起を行う取組を2019年6月から開始。
- 2023年６月時点で78社のISPがNOTICEに参加。

（２）現状・成果と課題

	①脆弱性があるIoT機器の調査	②利用者への注意喚起	③メーカーの対応	④NOTICEの運営
現状・成果	➢ ID・パスワードに脆弱性があるIoT機器について、現在までの累計で8万件以上のISPへの通知を実施。 ➢ 感染通信を出しているIoT機器について、現在までの累計で62万件以上のISPへの通知を実施。	➢ 利用者への注意喚起等により、ID・パスワードに脆弱性のあるIoT機器は一定数減少。 ➢ 一部のISPでは、レンタルサービスの提供によりセキュリティ対策をISP側で実施。 ➢ IoTセキュリティ基準を満たさない場合等にISPが端末の接続を拒否できる制度を措置。	➢ 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を実施。 ➢ 一部のメーカーではファームウェアの自動更新機能等を搭載したルーターを販売。 ➢ NOTICEとメーカーとの連携により、脆弱性のあるIoT機器に対処した事例もある。	➢ 脆弱性等のあるIoT機器を「プッシュ型」で対処する枠組みの実現。 ➢ ISPやメーカーとの連携により、利用者への注意喚起を要せずに対処した事例もある。 ➢ Emotetや不正アクセス検知等の当初想定していなかったリスクにも活用。
課題	➢ 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し、そのうち10年以上前に発売された古い機器が４割以上。 ➢ 感染通信を出しているIoT機器の数は、昨年春以降、マルウェア活動の活発化等を背景に高止まり。 ➢ 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機器を狙ったサイバー攻撃の増加。	➢ 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不十分。 ➢ 法人利用者については、管理責任の所在が曖昧で適切に注意喚起が届かないケース等も存在。 ➢ 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。	➢ サポートが終了している古い機器や、ファームウェアが古いままの機器が一定数残存。 ➢ 中小企業の場合、壊れるまで機器を利用する傾向がある。 ➢ NOTICEにおけるメーカーとの連携はアドホック的な対応に留まる。	➢ NOTICE参加ISPにとっては一連の業務に係る負担が大きい。 ➢ 調査を実施するNICTにおいて体制や人員の充実が必要。 ➢ 未参加ISPが管理するIPアドレス等は調査の対象外。 ➢ NOTICE調査で得られた様々なデータについて、更なるサイバー攻撃への対策に向けて、有効活用していくことが必要。

2. 端末側における対策（NOTICE）②

（３）今後の対応に向けた基本的な考え方

- **サイバー攻撃の踏み台となり得るIoT機器に対する観測能力の維持・強化**
- **幅広い関係者との連携や対処手段の多様化等による「プッシュ型支援」の強化**

（４）今後の対応策

①脆弱性があるIoT機器の調査の延長・拡充

- 今年度末までの時限措置となっているID・パスワードに脆弱性があるIoT機器の調査（特定アクセス行為）について、感染通信を出しているIoT機器の調査も含め、来年度以降も継続して取り組む。
- ファームウェア等のID・パスワード以外の脆弱性のあるIoT機器についても、脅威度に応じて個別に判断しつつ、NOTICEの枠組みにより必要な調査及び対処を実施する。
- これらの取組を継続的に可能とするため、早急に制度的措置を講じる。

②利用者への注意喚起の実効性向上

- NOTICEの情報発信強化とあわせて、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。
- IoT機器の管理状況等に関する利用者への実態調査等により、注意喚起による効果のより詳細な把握に取り組む。
- 感染通信を出している端末やサイバー攻撃の踏み台となり得る脆弱性のある端末について、ISPが接続拒否できる具体的な要件や手続等の妥当性についてあらかじめ示すため、「端末設備の接続に関するガイドライン（仮称）」を策定する。

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

- 利用者への注意喚起のみに依存するのではなく、幅広い関係者との連携により、ケースバイケースで様々な手段を活用しつつ総合的に対処を行う。
- 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・サービスの普及に取り組む。
- ISP及びメーカー等の関係者が連携し、利用者が安全な製品・サービスを選択する際に必要な情報の確実な提供等に取り組む。

④①～③を効果的に実施するためのNOTICEの運営体制の強化

- NOTICEの柔軟かつ効率的な運営に取り組むため、司令塔としての役割を担う体制を整備・確立する。
- NOTICEにメーカー等も参画し、幅広い関係者が恒常的に情報共有・連携を図るような枠組みをつくる。
- NOTICEの調査で得られたデータについて、研究・レポートの発表等を通じた情報公開等により更なる有効活用を進める。
- IoT機器の調査を担うNICTの体制・人員の柔軟な確保に取り組む。
- NOTICEの情報発信強化により、参加ISPの拡大を図る。

（参考）今後のNOTICEの全体像

NOTICEステアリングコミッティ

・NOTICEプロジェクトの司令塔として、サイバー攻撃の事象・脅威の認識共有やリスク評価を行い、対応方針を策定

観測・調査　～脅威観測～

NICT

○特定アクセス
・ID・パスワードに脆弱性がある機器
○ポートスキャン
・リフレクション攻撃の踏み台となっている機器
・ファームウェア等の脆弱性がある機器
○NICTER
・感染通信を出している機器

※必要に応じ関係機関とも連携
※研究・レポートの公表等を通じて観測データを有効活用

対処　～総合的対処～

NOTICE参加ISP

・利用者への注意喚起
・IoT機器を適切に管理可能なサービスの提供

ICT-ISAC JAPAN

・注意喚起対象リストをISPに通知
・NOTICE参加ISPのサポート
・参加ISPの拡大支援

IoT機器メーカー

・IoTセキュリティ基準への適合性確認も含めた安全な機器の提供
・機器のサポート終了やファームウェア更新等に関する情報提供

関係者が連携した利用者への周知啓発の強化

SIer

・IoT機器の適切な設定・管理に向けた利用者サポート

NOTICEサポートセンター

・問合せ対応やマニュアル作成等の利用者サポート、利用者に関する各種実態調査
・NOTICEの情報発信

利用者

・IoT機器の適切な設定・管理、注意喚起を受けた場合の対処

3. ネットワーク側その他における対策①

（1）これまでの取組

- 電気通信事業者におけるインターネット利用者のトラフィックのうち、必要最小限の範囲で収集するフロー情報の分析によるC&Cサーバである可能性が高い機器の検知について、正当業務行為として法的整理を実施。
- 2022～2023年度の2年間のプロジェクトとして、電気通信事業者におけるフロー情報の分析によるC&Cサーバ検知技術の有効性の検証や、事業者間の情報共有に当たっての課題整理のための実証事業を実施。

（2）現状・成果と課題

	①C&Cサーバの検知・検知情報の共有・利活用	②IoTボットネットの可視化
現状・成果	➢ フロー情報の分析により多くの被疑C&Cサーバが検知され、当該手法の有効性を確認。検知されたC&C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から、より迅速な対応につなげられる可能性も期待。 ➢ 特定の事業者のみが検知した被疑C&Cサーバが多く確認されたことから、事業者間連携を更に進めることによって、より多くのC&Cサーバを検知できる可能性等も期待。 ➢ （一社）ICT-ISACにおいては、C&Cサーバリストの情報共有・利活用の在り方や、C&Cサーバの検知手法の共有について検討している。	➢ 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に未然に対応するため、端末（IoT機器）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C&Cサーバの検知等に関する実証を各々で実施。
課題	➢ C&Cサーバの検知精度の向上に向けて、検知手法や評価手法の更なる改善等が必要。 ➢ C&Cサーバの生存期間が限られていることも踏まえ、検知データのリアルタイム性を出来るだけ確保していくことが重要。 ➢ 円滑かつ迅速にC&Cサーバリストが共有されるような仕組み等の検討とあわせて、C&C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。 ➢ C&Cサーバの検知のためにフロー情報を分析できる技術・リソースを有する事業者は一部に限られていることから、検知手法の共有が必要不可欠。	➢ C&Cサーバの居場所は頻繁に変わる一方、ボットネット端末は変わらないため、IoTボットネットの全体像の可視化を進めていくことが必要。 ➢ 大規模サイバー攻撃に効果的に対処していくためには、全体を俯瞰した対応が必要。 ➢ 恒久的な対策に向けて様々な情報を総合的に収集・分析する必要があるが、個々のISPがそれを実施することは困難。

3. ネットワーク側その他における対策②

（3）今後の対応策

①C&Cサーバの検知精度の向上・検知情報の共有・利活用等の推進

- NICTその他関係機関との連携等により、C&Cサーバの更なる検知精度の向上等に取り組むとともに、C&Cサーバの死活監視等により、収集するデータのリアルタイム性の確保を目指す。
- 検知されたC&CサーバリストについてISP間で試行的な共有・検証を行いながら、迅速かつ効果的な共有・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る。
- 可能な限り多くのISPが参加し、C&Cサーバの幅広い検知ができるような環境を整備するため、C&Cサーバの検知手法に関するISP間の情報共有の促進に取り組む。

②IoTボットネットの全体像の可視化

- 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に、「統合分析対策センター（仮称）」を立ち上げる。
- 幅広い関係者が柔軟に役割分担をしながら、NOTICEをはじめとする総合的な対策に取り組み、最終的にIoTボットネットを縮小することを目指す。