資料5－３

分科会取りまとめ骨子（案）

－総合的なIoTボットネット対策の実現に向けて－

令和５年５月

分科会取りまとめの構成（案）

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
（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
（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

２．端末側における対策（NOTICE）

（１）これまでの取組
（２）現状・成果と課題
①脆弱性等がある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
（３）今後の対応に向けた基本的な方向性
（４）今後の対応策

３．ネットワーク側その他における対策

（１）これまでの取組
（２）現状・成果と課題
①C2サーバの検知能力の向上・検知情報の効果的な利活用
②IoTボットネットの可視化
（３）今後の対応策

参考資料

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が進む中、その基盤となる情報通信ネットワークは必要不可欠なものとなっている。昨今の通信障害が発生した際にも、物流や金融をはじめとする様々な分野において広範な影響を及ぼしたことを踏まえれば、サイバー攻撃によって情報通信サービスの安定的な提供に支障が生じれば、国民の日常生活や社会経済活動に大きな影響を及ぼす可能性があり、安全・安心な情報通信ネットワークを確保していくことは極めて重要な課題となっている。

（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の現状

- DDoS攻撃をはじめとす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の発生数や規模等は増大している他、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、コンピューター等のいわゆる「攻撃インフラ」も拡大している。
- 国内においても、NICTER観測によれば、昨年春以降、Mirai系マルウェアの活動が活発化しており、特に脆弱性のあるネットワークカメラが感染した影響が大きい。こうしたネットワークカメラは、１台当たり数十Mbpsのトラフィックを発生させることも可能であり、強力なDDoS攻撃の踏み台となるおそれがある。
- 実際に、国内のIoT機器を踏み台として海外に向けた大規模なDDoS攻撃が発生し、情報通信サービスの安定的な提供に大きな支障を及ぼしかねない事案も起きており、こうした大規模サイバー攻撃が国内に向けられた場合のリスクも想定した対策を実施する必要がある。なお、大規模サイバー攻撃に至らないものの、政府機関や重要インフラ事業者等のウェブサイトを狙ったDDoS攻撃が断続的に発生している。
- 最近はログインによる侵入ではなく、リモートコード実行やコマンドインジェクション等の様々な脆弱性を狙ったマルウェアが増えており、脆弱性攻撃コードが公開されるとサイバー攻撃のリスクが急増する傾向がある。
- この他、少数のサーバから直接サイバー攻撃を行うケースも発生しているが、こうした攻撃はダークネットやハニーポットといった従来の手法では観測できない可能性がある。

（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

- DDoS攻撃のように情報通信ネットワークの機能に支障を生じさせるような大規模サイバー攻撃は、主に①IoT機器にマルウェアを感染させて攻撃の踏み台として悪用できるようにしたインフラ（IoTボットネット）の拡大と、②C2サーバからネットワークを通じてIoTボットネットに指令を出して攻撃を実行、という２つの段階がある。
- このような大規模サイバー攻撃への対策として、現在の取組状況や課題を踏まえた上で、端末側（IoT機器）、ネットワーク側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である。
- その際、端末側（IoT機器）については、開発・製造といった段階で適切なセキュリティ対策が講じられることが望ましいものの、IoT機器には様々な種類があり、メーカーも多数存在していることや、ライフサイクルの長さ等も踏まえれば、現段階においては、ISP、メーカー、SIer、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求められる。

2. 端末側における対策（NOTICE）

（１）これまでの取組

- 2015年頃より、「Mirai」というマルウェアに感染した多数のIoT機器を踏み台とした大規模なDDoS攻撃が国内外において発生。
- こうした多数のIoT機器がDDoS攻撃の踏み台となる事態を未然に防止するため、当時主流であったID・パスワードの脆弱性を狙った感染手法に着目し、今年度末までの５年間の時限措置（不正アクセス禁止法の例外）としてNICT法を改正し、NICTが、同様の手法（特定アクセス行為）により、予め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（NOTICE）を2019年2月に開始。
- NICTからISPへの通知については、認定送信型対電気通信設備サイバー攻撃対処協会（認定協会）である（一社）ICT-ISACを通じて実施している。
- 調査を開始した当初は、ID・パスワードは100通り、通信プロトコルはtelnet、ポートも1つのみが調査対象であったが、サイバー攻撃の手法の変化等も踏まえ、 ID・パスワードについては2020年10月に600通りに拡大した他、通信プロトコルについては2022年6月にhttp／httpsを追加するとともにポートも順次追加し、現在は39のポートを対象に調査を実施している。
- 上記の取組に加えて、NICTが無差別型サイバー攻撃の観測網である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月に開始。
- NOTICEは、ISPの自主的な協力を基本としており、2019年の開始当初の参加ISPは24社のみであったが、参加数は徐々に拡大して現在は78社となり、NOTICEの調査対象となるIPアドレスの総数も1.12億アドレスとなっている。

（２）現状・成果と課題

①脆弱性等があるIoT機器の調査

（現状・成果）

- ID・パスワードに脆弱性があるIoT機器については、国内の1.12億IPアドレスを対象に、NICTが法律に基づいて調査を実施し、全体的な動向を把握できるようになった。
- ID・パスワードに脆弱性があり、注意喚起対象としてISPに通知したIoT機器の数は毎月4,000件程度あり、現在までの累計で8万件以上の通知を実施している。
- NICTERにより検知され、注意喚起対象としてISPに通知した感染通信を出しているIoT機器の数は、直近では1日平均500～700件程度で推移しており、現在までの累計で61万件以上の通知を実施している。
- 検知された機種については、ID・パスワードに脆弱性があるIoT機器及び感染通信を出しているIoT機器双方ともルーターが最も多くを占めており、次いでネットワークカメラとなっている。

（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、こうした攻撃の踏み台となる可能性のある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。
- ISPにとっては外部から来る攻撃通信よりも、自網内のIoTボットネットから外部に向かう攻撃通信の方が、正常な通信を遮断するおそれがあるため対策が困難。そのため、IoTボットネットと、ボットネット化する可能性があるIoT機器を可能な限り減らしていく取組が必要である。
- 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。注意喚起対象となったIoT機器のうち、10年以上前に発売された古い機器が4割以上を占めている。
- NICTERにより検知された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機器を狙った攻撃が増えているが、こうした機器については、NOTICE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。

（２）現状・成果と課題

②利用者への注意喚起

（現状・成果）

- 利用者への注意喚起によってID・パスワードに脆弱性のあるIoT機器は一定数減少。あるISPにおいては、注意喚起の進捗状況を適切に管理することにより、ID・パスワードに脆弱性のあるIoT機器がゼロになった事例もある。
- 「NOTICEサポートセンター」においては、問合せ対応や機器別の脆弱性解消マニュアルの作成等、注意喚起を受けた利用者のサポート等を行っている。
- 一部のISPでは、ファームウェアの自動更新等、利用者が意識することなくIoT機器が適切に管理されるよう、ルーター等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について、初期設定のパスワードの変更を促す等の機能やソフトウェア更新機能等の要件を定めたIoTセキュリティ基準を端末等設備規則において新たに定めるとともに、当該要件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、ルーターのパスワード変更といった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、所有者・設置者・利用者各々が異なり、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。
- 注意喚起を受けた利用者について、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。

（２）現状・成果と課題

③メーカーの対応

（現状・成果）

- メーカーにおいては、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。
- （一社）デジタルライフ推進協会（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とメーカーとの連携により、脆弱性のある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）

- IoT機器はメーカーが多数存在しており、安くてセキュリティ品質の悪いIoT機器も販売できる環境であるため、一定の寡占状況にあるPCやスマートフォンと比較して、安全な機器の提供に向けた対策はより難しい状況にある。
- 国内のインターネットに接続されているIoT機器のうち、メーカーのサポート期間が終了しているEOL（End Of Lifeの略）を迎えた古い機器や、ファームウェアが更新されずに古いままになっている機器が一定数残存している。
- IoT機器は製品寿命が一般的に長く、特に中小企業の場合、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。
- NOTICEにおいては事案に応じて個別にメーカーとコミュニケーションを取っているが、恒常的に連携を図っていくような取組が必要である。

（２）現状・成果と課題

④NOTICEの運営

（現状・成果）

- NOTICEの取組により、脆弱性等の問題のあるIoT機器を特定し、利用者からサイバー攻撃の被害の申告を受けてから対処するのではなく、未然に「プッシュ型」で対処につなげる枠組みができた。
- NOTICE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や、IoT機器の検知数の急変により不正アクセスを検知し、ISPに情報提供した事案等、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から注意喚起対象となる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となっている。
- 脆弱性等のあるIoT機器の調査を担うNICTにおいても、サイバー攻撃の手法の変化等に対応した十分な調査を実施するため、体制や人員の充実が必要となっている。
- 未参加のISPが管理するIPアドレスは調査対象外となっている他、参加ISPの卸先ISPがNOTICEに参加していない場合、脆弱性等のあるIoT機器が検知されたとしても個別の利用者への注意喚起を行うことができない。
- NOTICEの調査を通じて国内のIoT機器等に関するデータが蓄積されてきていることから、国内のネットワークの状況の可視化や関係団体との協調など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。

（３）今後の対応に向けた基本的な方向性

これまでの現状・成果及び課題を踏まえ、今後のNOTICEをはじめとする端末側における対策については、**国民の日常生活・社会経済活動に必要不可欠な情報通信サービスの安定的な提供を確保するため、IoT機器を踏み台としたサイバー攻撃の脅威に対する観測能力を強化し、攻撃の脅威に応じた効果的な対処の促進に向けて**、以下のような方向性で取り組むべきである。

- **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**

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ついては、発生数・規模ともに増大しており、攻撃の踏み台となる可能性のある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中、こうした攻撃に効果的に対応していくためには、脅威を観測した上でリスク評価を行っていくことが必要不可欠であることから、これをNOTICEの役割として明確に位置づけ、脆弱性等のあるIoT機器に対する観測能力の維持・強化を図る。

- **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**

脆弱性等のあるIoT機器への対処をより効果的に促していくため、利用者への注意喚起の実効性向上を図るとともに、 幅広い関係者との連携により状況に応じた多様な手段を講じる。

（４）今後の対応策

①脆弱性等のある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）や感染通信を出しているIoT機器の調査については、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、機器の脆弱性及び攻撃コードの公開状況や国内における普及状況等、脅威度に応じて個別に判断しつつ、NOTICEの枠組みを活用して必要な調査及び対処を可能とする。
- 上記を実施するため、必要な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の情報発信とあわせて、メーカーやSIer等の関係者と連携しつつ、一般利用者・法人利用者それぞれに向け、IoT機器の適切な管理（ID・パスワードの変更、ファームウェアの更新、新しい機器への買い替え等）を推進するための周知啓発・サポートを更に強化する。その際、安全な機器やサービスを選ぶといった利用者に求められる役割もあわせて周知啓発を行う。
- IoT機器の管理状況等に関する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、累次にわたって注意喚起に応じない場合等、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。

（４）今後の対応策

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に加え、ISPやメーカーとの連携により成果を上げている事例を踏まえ、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。

（※）脆弱性のあるIoT機器に対する利用者への注意喚起以外の対処例
ISPとの連携・・機器がレンタルサービス等を通じてISPによって管理されている場合、ISP側で一括して対処。
メーカーとの連携・・・注意喚起対象となった製品についてメーカーに情報提供した上で、ファームウェアの改修や新製品の機能改善につなげる。
SIerとの連携・・・法人利用者等、機器の設置・管理にSIerが関与している場合、SIerを通じて対処を依頼。

- ISP及びメーカーと連携し、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。
- メーカーと連携し、IoT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

- 関係者間でサイバー攻撃の脅威を評価し、目指すべきゴールや必要な対策について認識の共有を図りつつ、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ため、司令塔としての役割を担う体制を整備する。
- NOTICEの取組にメーカーも参画し、ファームウェアの更新や新製品への対応も含め、脆弱性等のあるIoT機器への効果的な対処に向けて恒常的に情報共有・連携を図る。
- NICTにおいて脆弱性等のあるIoT機器の調査を十分に行うための体制・人員の柔軟な確保に取り組む。
- NOTICEの調査で得られたデータについて、情報公開や関係機関との共有を適切に進めることで、国内のインターネットに接続されている機器の状況の可視化等、サイバー攻撃対策の強化に資するよう更なる有効活用を図る。
- NOTICEの情報発信を更に強化し、参加ISPの拡大を図る。

3. ネットワーク側その他における対策

（１）これまでの取組

- 大規模化・複雑化・巧妙化するサイバー攻撃に対して、予め電気通信事業者が積極的に対処できるようにするため、平時から電気通信事業者が自網内の通信トラフィックに係るデータを収集・蓄積・分析し、サイバー攻撃の指令元となっているC2サーバである可能性の高い機器の検知等を行うことが求められている。

- これを踏まえ、まず、2021年11月に「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会　第四次とりまとめ」において、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（※）の統計的・相関的な分析によるC2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（通信の秘密の侵害に該当しない）として法的整理を実施した。

（※）通信トラフィックに係るデータのうち、IPアドレス及びポート番号等のヘッダ情報並びにルータでヘッダ情報を抽出する際に付与されるタイムスタンプ等の情報（通信の内容は含まない）

- その上で、この法的整理に基づき、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C2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運用面の課題整理のための実証事業を実施している。

- 本実証事業については、ISP3社がグラフマイニングと機械学習の2つの手法によりフロー情報を分析して被疑C2サーバを検知し、ICT-ISACにおいて検知された被疑C2サーバの多面的な分析・評価を実施するとともに、事業者間の情報共有等に関する検討を行っている。

（２）現状・成果と課題

①C2サーバの検知・検知情報の共有・利活用

（現状・成果）

- ISP３社ともフロー情報の分析により、多くの被疑C2サーバが検知され、当該手法の有効性が確認されるとともに、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から、より迅速な対応につなげられる可能性も期待される。
- 特定のISPのみが検知した被疑C2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C2サーバを検知できる可能性や、より影響度の高いC2サーバを特定できる可能性も期待される。
- ICT-ISACにおいては、会員社のうち13社がWGに参画し、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、課題の整理を行っている。

（課題）

- C2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を図るとともに、関係機関との連携によるソース情報の拡充を図っていくことが必要である。
- C2サーバの生存期間は限られているため、データのリアルタイム性の確保が重要である。
- 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や共有すべきデータの検討とあわせて、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である。
- C2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おり、より多くのISPがC2サーバを検知するためには、検知手法の共有が必要不可欠である。

（２）現状・成果と課題

②IoTボットネットの可視化

（現状・成果）

- 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、端末側（IoT機器）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している。

（課題）

- C2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、ボットネット端末は次々異なる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ていくことが必要。
- 多数のIoT機器を踏み台とした大規模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、IoT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となっている。
- 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。

3. ネットワーク側その他における対策

（３）今後の対応策

①C2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るC2サーバの更なる検知精度の向上や、検知・評価に係る作業の短縮化に取り組むとともに、C2サーバの死活監視を通じてその活動状況を逐次観測することにより、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C2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、C2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、C2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

- NOTICEで検知された脆弱性等のある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）」を立ち上げる等、ISP等の幅広い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。