資料６－１

情報通信ネットワークにおける
サイバーセキュリティ対策分科会
とりまとめ（案）

－総合的な IoT ボットネット対策の実現に向けて－

2023 年６月

総務省　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

目次

はじめに

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。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である。

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うるサイバー攻撃には、マルウェアに感染した多数の IoT 機器等が踏み台となり、「攻撃インフラ」となって利用されていることが問題となっている。

「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」は、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、2019 年から開始された脆弱性のある IoT 機器の調査及び注意喚起を行う NOTICE（National Operation Towards IoT Clean Environment）や、2022 年から開始された「電気通信事業者におけるフロー情報分析による C&C サーバ検知及び共有に関する調査」等の取組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」の下に本年１月に設置されたものである。

分科会において、多くの関係団体、関係事業者や有識者から貴重な発表をいただき、活発な議論が行なわれた。本とりまとめは、この分科会における議論を踏まえたものであり、現状・成果及び課題等を踏まえ、端末（IoT 機器）側、ネットワーク側各々について今後取り組むべき対応策を「総合的な IoT ボットネット対策」として示したものである。情報通信ネットワークの安全性・信頼性を確保していくため、本とりまとめを踏まえ、総務省、関係団体、関係事業者、利用者等の関係者が適切に役割分担を図りながら、「総合的な IoT ボットネット対策」の実現に向けて取組を加速することを期待する。

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。2022 年７月に大手携帯キャリアにおいて通信サービス障害が発生した際には、延べ約 3,091 万人以上の利用者が影響を受け、物流や金融等の様々な分野において広範な影響を及ぼしたこと等を踏まえれば、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、国民生活や社会経済活動に多大な影響が及ぶ状況となっている。

このような状況のもと、情報通信ネットワークの安全性・信頼性を確保することは一層重要となっている。

（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や IoT ボットネットの現状

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については、世界全体においても引き続き増大しており、2022 年第３四半期のネットワーク層で発生した DDoS 攻撃の数は、前年比 97%増[1]となっている他、攻撃対象の拡大及び攻撃継続時間の増加もみられている。また、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」も拡大している。

国立研究開発法人情報通信研究機構（NICT）においては、ダークネット（未使用の IP アドレス）を活用したサイバー攻撃の観測網（NICTER）を構築し、国内外で発生している無差別型サイバー攻撃の状況を観測しているが、この観測結果によれば、IoT 機器を狙った攻撃が最も大きな割合を占めている（図１）。

さらに昨年春以降、国内において 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の感染による影響が大きい（図２）。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[2]。

こうしたネットワークカメラを含む IoT 機器については、社会全体のデジタ

---

[1] Cloudflare DDoS 脅威レポート 2022 年第 3 四半期
https://blog.cloudflare.com/ja-jp/cloudflare-ddos-threat-report-2022-q3-ja-jp/

[2] 第 41 回サイバーセキュリティタスクフォース NICT プレゼン資料
https://www.soumu.go.jp/main_content/000854031.pdf

ル化を促進する大きな役割を果たしている一方で、機器のライフサイクル（製品寿命）が長い、監視が行き届きにくい、開発者が想定していなかった接続が行われる等の特性から、サイバー攻撃の対象として狙われやすくなっている。

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。また、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 攻撃により、閲覧が困難になる等の事象が断続的に発生している他、家庭用ルーターがサイバー攻撃に悪用されていることが判明し、本年春に警察庁等から注意喚起が発出[3]されている。

さらに最近では、ID・パスワードの脆弱性を狙ったログインによる侵入だけではなく、リモートコード実行やコマンドインジェクション等、ファームウェア[4]をはじめとする様々なソフトウェアの脆弱性を狙ったマルウェアが増えており、こうした脆弱性に対する攻撃コードがプラットフォーム上で公開されると、それを悪用したサイバー攻撃のリスクが急増する傾向にある[5]。

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、こうした攻撃は感染機器を観測している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他、機器の再起動といった簡易な手法では駆除できないマルウェアも新たに観測される等、サイバー攻撃の手法も多様化している[6]。

---

[3] https://www.npa.go.jp/bureau/cyber/pdf/20230328_press.pdf

[4] 機器の内部に組み込まれた、機器を制御するためのソフトウェア

[5] 第1回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 吉岡構成員プレゼン資料
https://www.soumu.go.jp/main_content/000856810.pdf

[6] 脚注5参照。

図１　増加・多様化する無差別型サイバー攻撃～NICTER による観測～

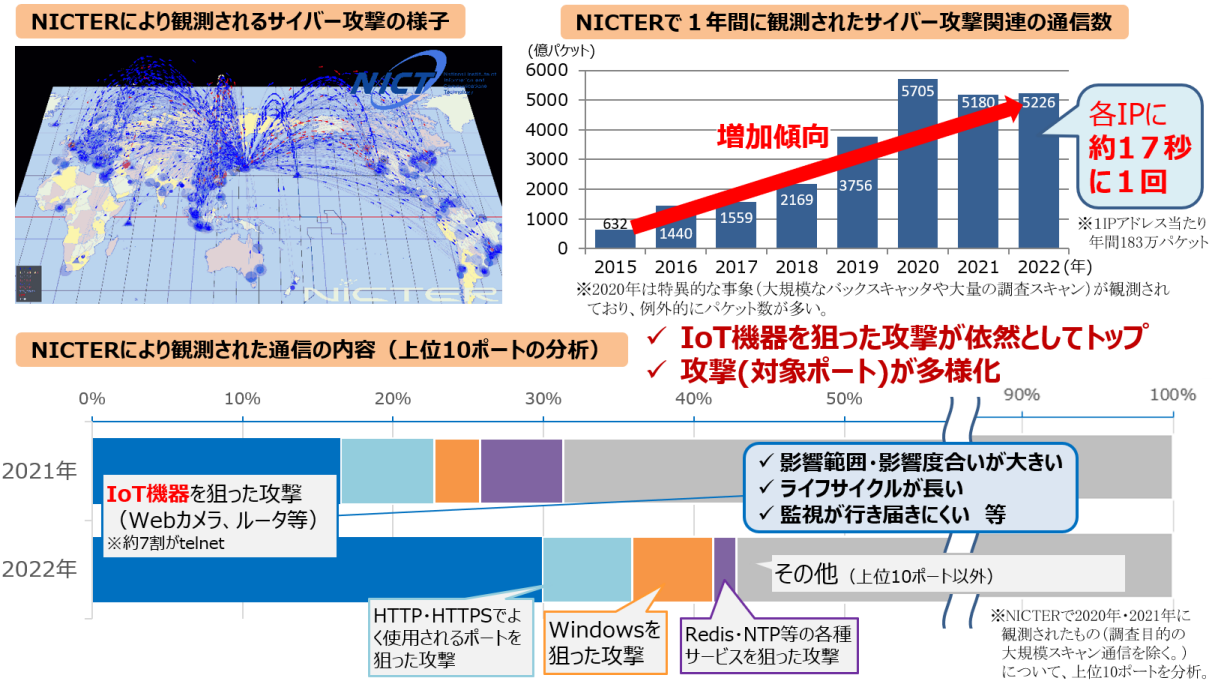
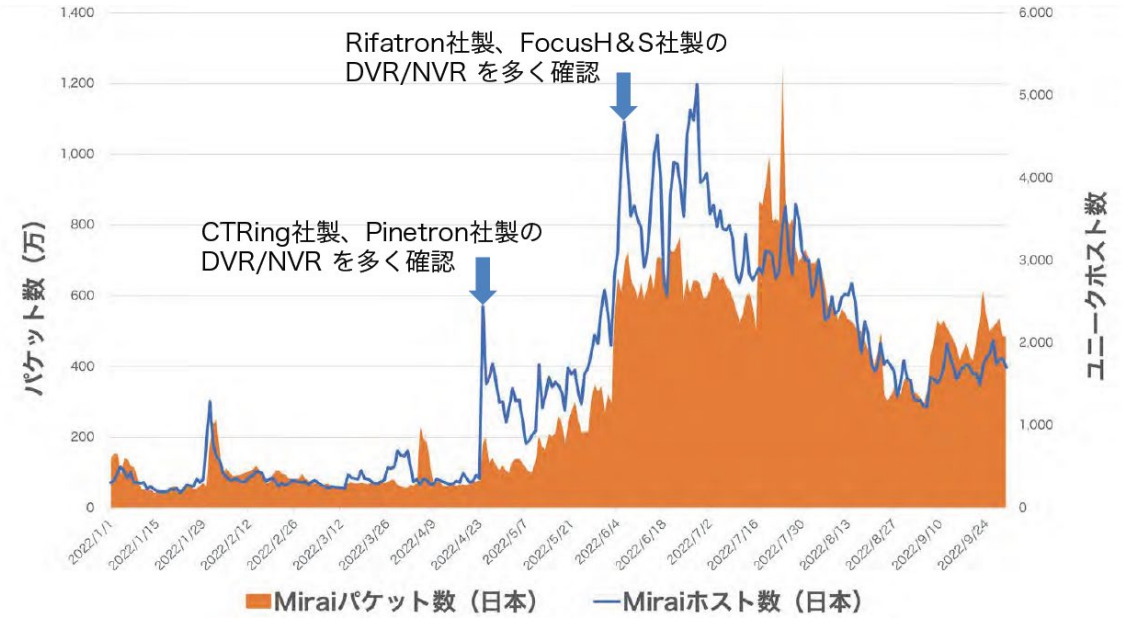


図２　日本を送信元とする Mirai の特長を持つパケット数とユニークホスト数（日毎）



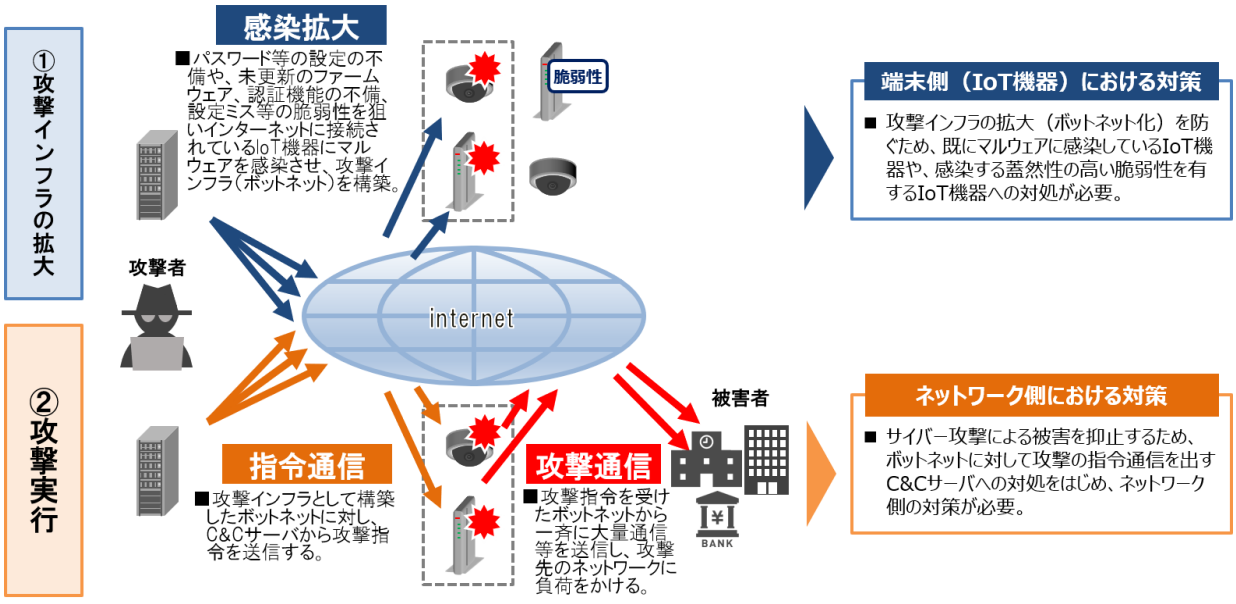
（３）情報通信ネットワークにおけるサイバーセキュリティ対策の強化に向けて

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、攻撃の踏み台として悪用できるようにした攻撃インフラ（IoT ボットネット）の拡大と、②C&C サーバ[7]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、攻撃先への大量通信の送信により攻撃を実行、という２つの段階がある（図３）。

このような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ための端末（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 サーバへの対処のための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である。

その際、端末（IoT 機器）側の対策については、開発・製造といった段階でも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、PC やスマートフォンにおける OS のアップデート等や、クラウドサービス（SaaS）等の事例を参考にしつつ、ISP、メーカー、SIer[8]、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求められる。

図３　DDoS 攻撃の段階と対応策



[7] Command and Control サーバの略であり、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に対して攻撃者から指令を送り、制御を行うサーバコンピュータのこと。

[8] システムの開発から保守・運用までを請け負う事業者

２．端末側における対策（NOTICE）

（１）これまでの取組

2015 年～2016 年頃、「Mirai」と呼ばれるマルウェアの感染が急速に拡大し、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した。

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、2018 年 11 月に国立研究開発法人情報通信研究機構法（平成 11 年法律第 162 号）を改正し、2024 年３月末までの５年間の時限措置（不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）の例外）として、NICT が、同様の手法（特定アクセス行為[9]）により、ID・パスワードに脆弱性のある IoT 機器を調査して電気通信事業者（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月に開始した。

なお、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／ssh のみ、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。

また、上記の取組に加えて、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月から開始している。

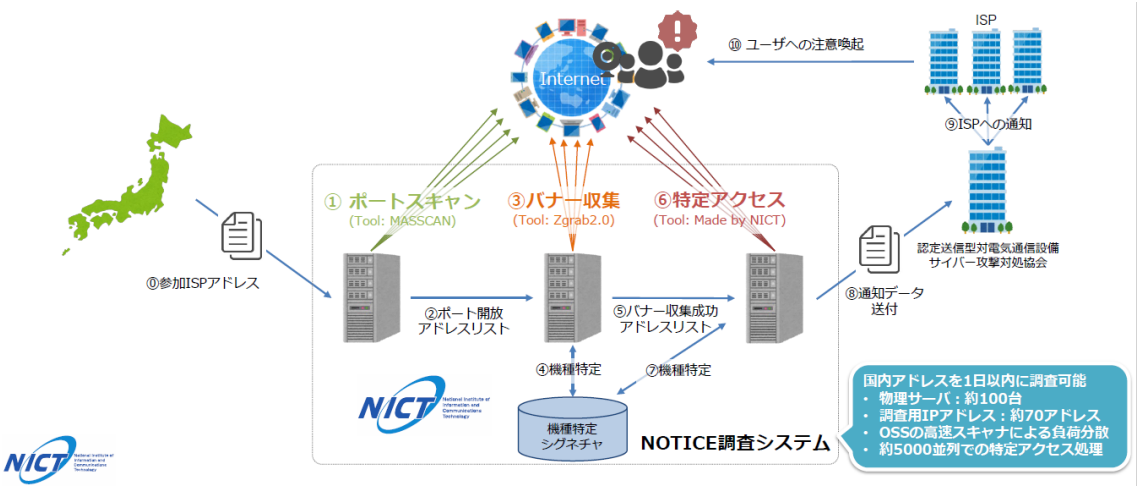
こうした NOTICE の取組は、ISP の自主的な協力を基本としており、2019 年の開始当初の参加 ISP は 24 社であったが、その後参加数は徐々に拡大し、2023 年６月時点で 78 社の ISP が NOTICE に参加しており、NOTICE の調査対象となる IP アドレスの総数も 1.12 億アドレス[10]となっている。

---

[9] 国立研究開発法人情報通信研究機構法附則第8条第4項第1号。

[10] JPNIC が管理する日本国内の IP アドレスは約 1.9 億あるが、このうち NOTICE に参加している ISP が管理している IP アドレスを調査対象としている。

図４　ID・パスワードに脆弱性がある IoT 機器の調査の概要



（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】

NOTICE の取組により、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。その結果、ID・パスワードに脆弱性があるとして ISP に通知した IoT 機器の数は、直近では月平均 4,000 件程度で推移しており、現在までの累計で８万件以上の通知を実施している（図５）。

また、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 400～700 件程度で推移しており、現在までの累計で 62 万件以上の通知を実施している（図６）。

注意喚起対象となった機種については、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（図７）。

図５　パスワード設定等に不備がある IoT 機器に対する注意喚起対象件数の推移（2023 年４月）

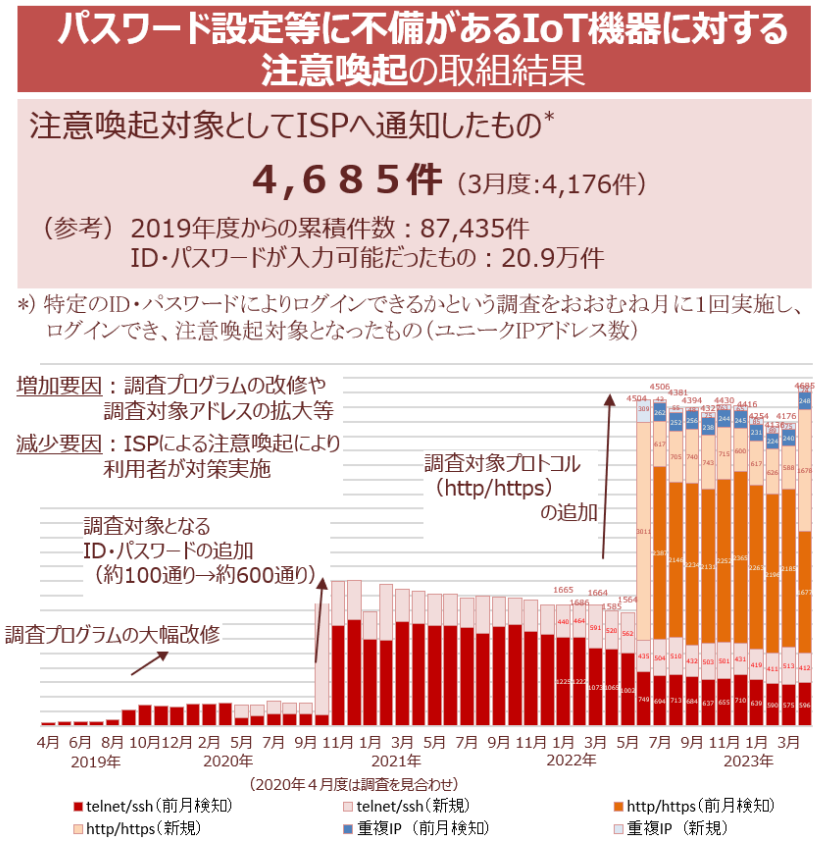


図６　感染通信を出しているIoT機器に対する注意喚起対象件数の推移（2023年４月）

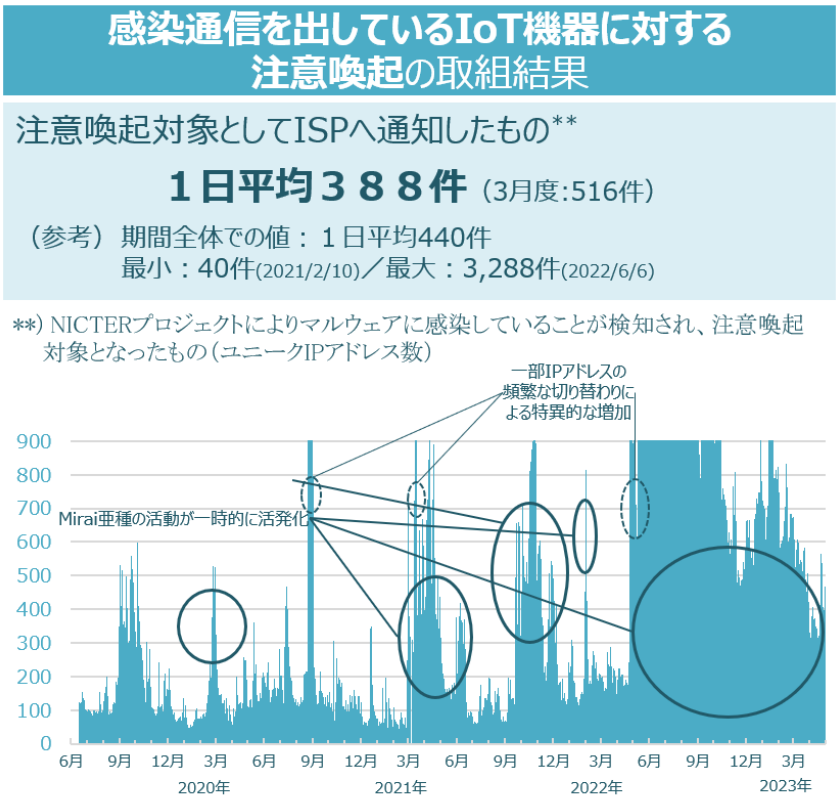
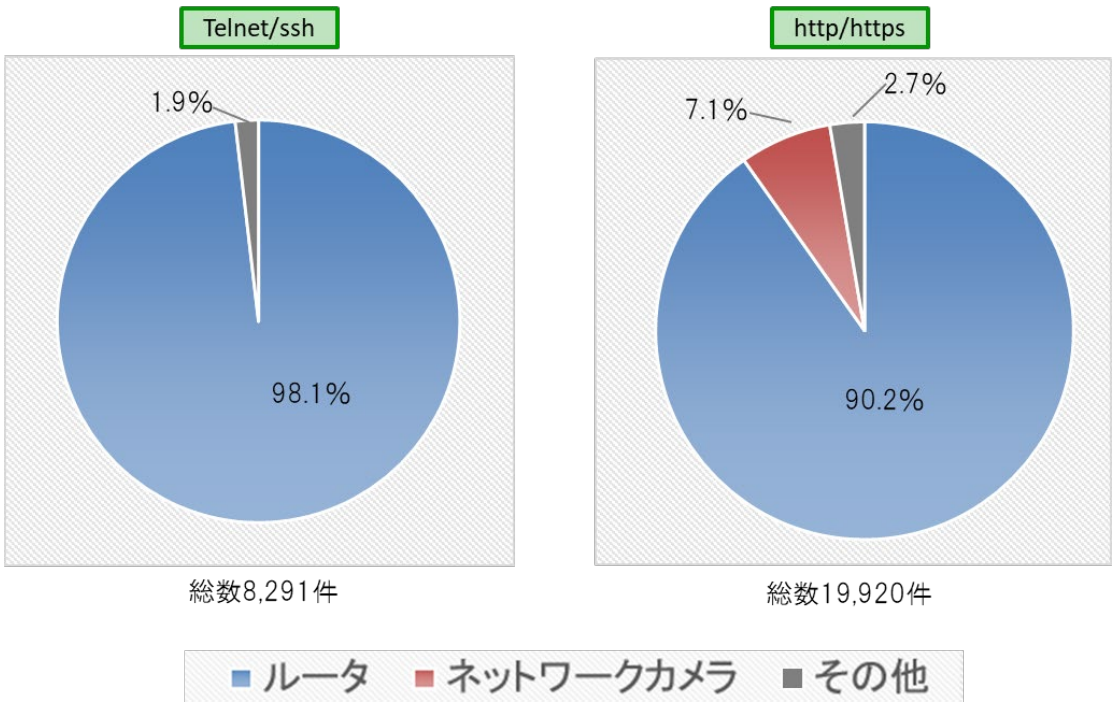


図７　注意喚起対象となったIoT機器の機種の内訳（2022年11月～2023年４月）



【課題】

１（２）で述べたように、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していくことが見込まれる。

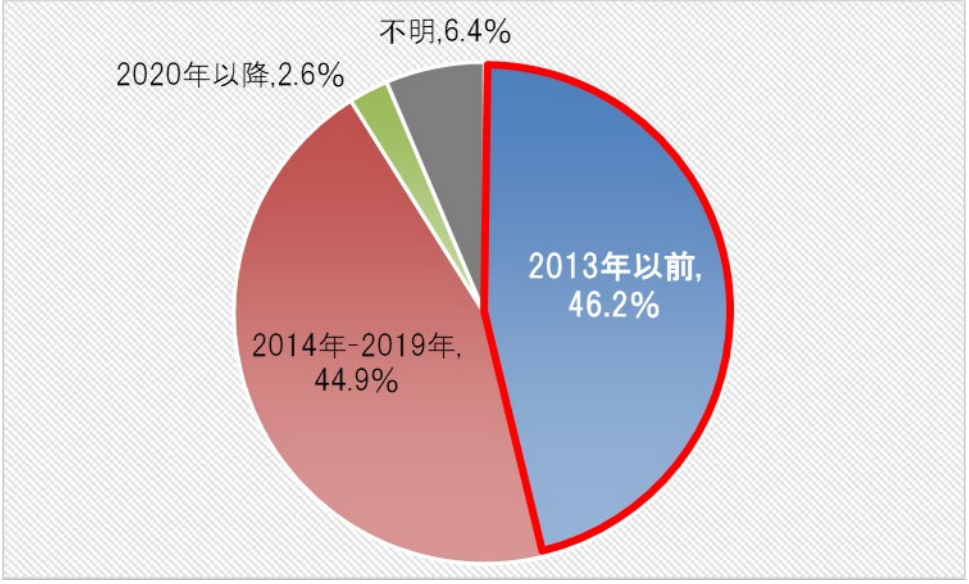
また、ISP にとっては、外から自網へ向けて送信される攻撃通信よりも、自網内の IoT ボットネットから外へ送信される攻撃通信の方が、正常な通信も遮断するおそれがある等の理由により、一般的に対策が困難とされている。そのため、こうした IoT 機器を踏み台としたサイバー攻撃を未然に防ぐためには、IoT ボットネットと、ボットネット化する可能性がある IoT 機器を可能な限り減らしていく取組が必要である。

この点、NOTICE の取組によって、IoT ボットネット対策は一定の成果を上げているものの、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ている。特に、注意喚起対象となった機器のうち、10 年以上前に発売された古い機器が４割以上を占めており、IoT 機器のライフサイクルの長さが明らかとなっている（図８）[11]。また、１（２）で述べたように、NICTER により検知され、注意喚起対象となっ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。

この他、同じく１（２）で述べたように、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が増えている。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り、メーカー等に情報提供した事例はあるものの、アドホック的な対応にとどまっており、現行の NOTICE の枠組みにおいては十分対処ができていない状況にある。

[11] 脚注 15 参照。2020 年4月の IoT セキュリティ基準施行後の新しい機器については、ID・パスワードの脆弱性等、一定の対策が進んでいる。

図８　注意喚起対象となった IoT 機器の発売年の割合（2022 年 11 月～2023 年４月）



②利用者への注意喚起

【現状・成果】

NOTICE の枠組みを通じて個別の利用者への注意喚起を実施するとともに、「NOTICE サポートセンター」を設置し、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を行う等の取組により、ID・パスワードに脆弱性のある IoT 機器は一定数減少している他、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で、注意喚起対象件数がゼロになった事例もある[12]。

また、一部の ISP においては、一般家庭向けにルーター等の IoT 機器のレンタルサービスを提供しており、最新のファームウェアの提供や機器の監視といったセキュリティ対策を ISP 側で一括して行っている事例がある。

さらに 2020 年４月に、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

[12] 検知された IoT 機器の利用者が全て法人利用者であり、ISP による通知データを顧客単位で紐付け、歴月管理を行い対処状況を把握しながら、メールでの注意喚起を実施したもの。

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[13]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している。

【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ないことに加え、ルーターのパスワード変更等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[14]。

特に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である等適切な IoT 機器の管理体制がないため、適切に注意喚起が届かないケースや、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等の対処が行われないケースもある。

また、こうした利用者側の課題に加え、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ことが課題となっている。

一方、IoT セキュリティ基準を満たさない端末やマルウェアに感染している端末等、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も課題となっている。

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

---

[13] 電気通信事業法（昭和 59 年法律第 86 号）において、電気通信事業者が、技術基準を満たさない端末設備からの自社の電気通信回線設備への接続の請求を拒否することができることとされており、当該技術基準を具体的に定めた端末設備等規則（昭和 60 年郵政省令第 31 号）において、ネットワークに係る攻撃は電気通信回線設備の機能に障害を与え又は他の利用者に迷惑を及ぼしうるものであることを踏まえ、電気通信回線設備に直接接続される端末機器を対象に、IoT 機器の特性を踏まえた最低限の技術基準として、①アクセス制御機能、②アクセス制御の際に使用する ID／パスワードの初期設定の変更を促す等の機能、③ファームウェアの更新機能、④変更した ID／パスワードを維持する機能を具備することを追加で定めている。

[14] （一社）デジタルライフ推進協会（DLPA）が 2023 年3月に実施した Wi-Fi ルーター利用者向けアンケートの結果は以下のとおり。

- 57.8%の利用者が Wi-Fi ルーターのセキュリティを意識したことがない
- 81.7%の利用者が自宅の Wi-Fi ルーターがサイバー攻撃されると考えたことがない
- 購入時のパスワードをそのまま利用している利用者が 42.7%

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。

特に、（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。

さらに、NOTICE の調査で検知した機器について、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】

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[15]。

IoT 機器はライフサイクルが一般的に長く、特に中小企業の場合、定期的に設備更改が行われる大企業と比較すると、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。

また、前述のとおり、現行の 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、アドホック的な対応にとどまっているため、今後恒常的に連携を図っていくような取組も必要となっている。

④NOTICE の運営

【現状・成果】

NOTICE の取組により、利用者からサイバー攻撃の被害の申告を受けて対処するのではなく、あらかじめ脆弱性等の問題のある IoT 機器を特定して利用者へ注意喚起を実施することにより、未然に「プッシュ型」で対処につなげる枠組みができたことは成果の１つと言える。

---

[15] 第3回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 (株)ゼロゼロワンプレゼン資料
https://www.soumu.go.jp/main_content/000868984.pdf

また、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ケースや、ISP やメーカーと連携してファームウェアの更新・適用を行ったケース等、利用者への注意喚起を実施せずに対処に成功した事例もある。

さらに、海外の捜査当局から警察庁に国内の「Emotet[16]」感染端末の情報提供があり、警察庁と連携して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例もある。

【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していくため、関係団体や関係事業者とも連携して体制や人員を充実することが課題となっている。

また、NOTICE の調査対象として未参加の ISP が管理する IP アドレスは対象外となっているとともに、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等の課題がある。

更に、NICT においては、2019 年以降の NOTICE の調査を通じて国内の IoT 機器の脆弱性等に関する様々な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等に取り組むとともに、研究・レポートの公表等を通じて積極的に情報公開を図ることにより、更なるサイバー攻撃への対策に向けて、これを有効活用していくことが必要である。

[16] 情報の窃取や他のマルウェアへの感染のために悪用されるマルウェアであり、現在においても攻撃活動が断続的に発生している。

（３）今後の対応に向けた基本的な考え方

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、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

サイバー攻撃の踏み台となり得る脆弱性のあるIoT機器に対する観測能力を維持・強化する観点から、今年度末までの時限措置となっている特定アクセス行為によるID・パスワードに脆弱性があるIoT機器の調査について、NICTERによる感染通信を出しているIoT機器の調査も含め、NICTが来年度以降も継続して取り組む必要がある。

また、サイバー攻撃手法の多様化に対応するため、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、攻撃コードの公開状況及び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実施することが求められる。

これらの取組を継続的に実施することを可能とするため、早急に制度的措置を講じることが必要である。

②利用者への注意喚起等の実効性向上

利用者への注意喚起等の実効性を向上させるため、ホームページの充実等を含めNOTICEの情報発信を強化するとともに、メーカーやSIer等の関係者との連携により、一般利用者・法人利用者それぞれに向けて、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含めて利用者によるIoT機器の適切な管理を推進するための周知啓発を更に強化する。その際、脆弱性等のあるIoT機器が、利用者本人やネットワーク全体に対して、どのような不利益・リスクを生じさせるのか、また、その対応策について分かりやすく伝わるよう工夫する。

また、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?[17]」との連携等を進めることにより、注意喚起による効果のより詳細な把握に取り組む。

更に、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利用者が応じない場合等について、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

[17] 横浜国立大学が実施している、利用者の申請に基づいてIoT機器のマルウェア感染と脆弱性を確かめる検査サービス。https://amii.ynu.codes/

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

脆弱性等のある IoT 機器への対応を進める際に ISP やメーカーとの連携により効果的に成果を上げている事例があることを踏まえ、②の利用者への注意喚起のみに依存するのではなく、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（※）を行うことができるように、関係団体、ISP、メーカー、SIer 等の関係事業者等と連携を進めることが必要である。

（※）脆弱性等のある IoT 機器に対する利用者への注意喚起以外の対処例

連携例	対処例
ISP との連携	レンタルサービス等を通じて機器が ISP によって管理されている場合、利用者に直接対処を求めることなく ISP 側で一括して対処する。
メーカーとの連携	注意喚起対象となった製品について、利用者への情報提供、ファームウェアの改修・更新や新製品の機能改善等必要な対処を促す。
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 を通じて機器の ID・パスワードの設定等やファームウェアの更新等必要な対処を促す。

さらに、ISP 及びメーカー等の関係者が連携し、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。

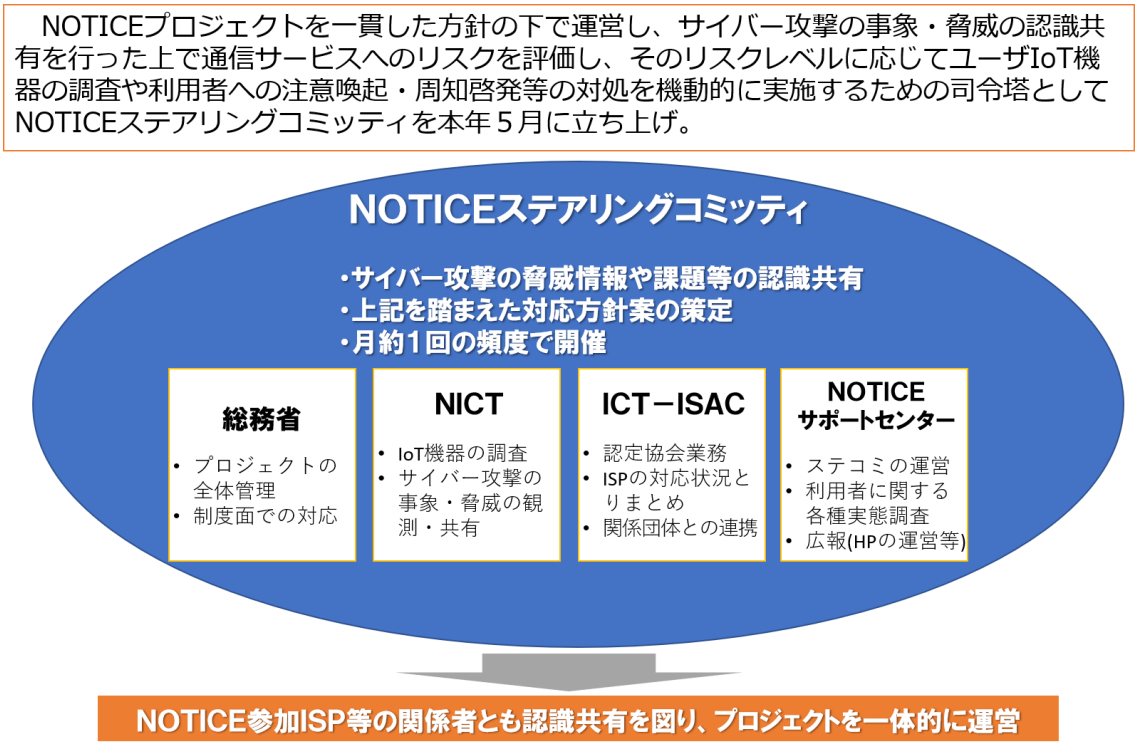
また、メーカーや流通業者と連携し、IoT 機器のサポート期間終了やファームウェアの更新等、利用者が安全な製品・サービスを選択する際に必要な情報の確実な提供、利用者にとって分かりやすい設定・操作が可能な機器やマニュアルの提供を進める。

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（NOTICE ステアリングコミッティ）を整備・確立する（図９）。

図９　NOTICE ステアリングコミッティの概要



その際、③にあるように総合的な対処を進める観点から、NOTICE の取組にメーカーや SIer 等も参画し、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 機器への総合的・効果的な対処の推進に向けて、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（図 10）をつくる。

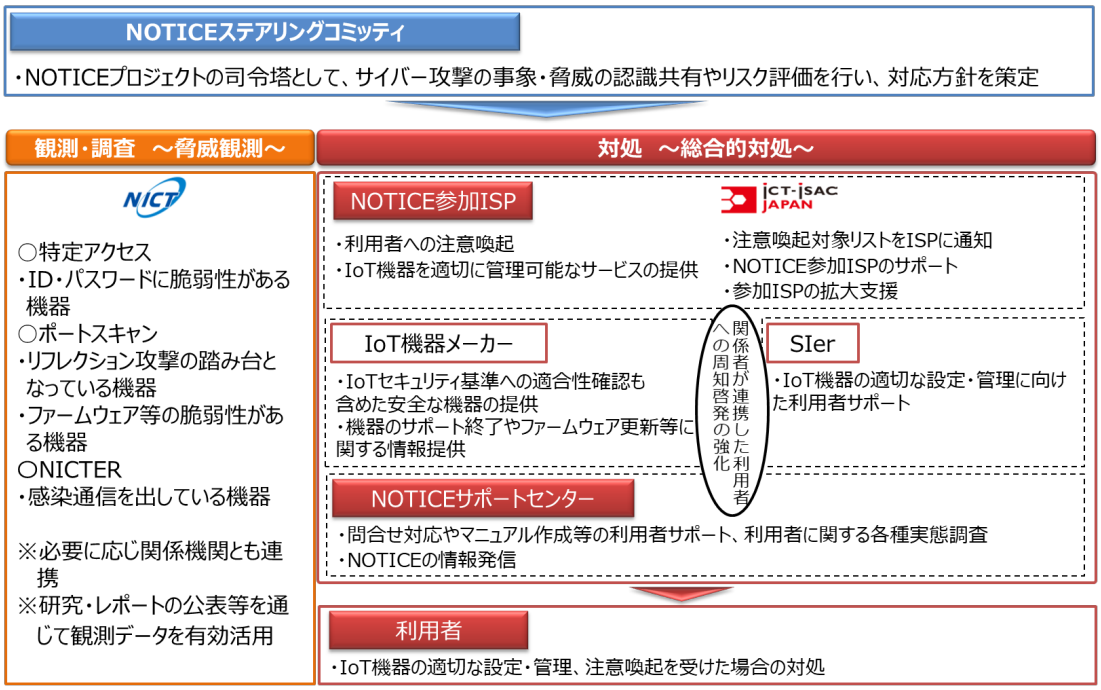
また、②にあるように NOTICE の情報発信を更に強化することにより、一般利用者の理解を得るとともに、参加 ISP の拡大を図る。

こうした取組の前提となる脆弱性等のある IoT 機器の調査について、①にもあるようにサイバー攻撃の変化に応じて十分に実施するため、主にこれを担う NICT の体制・人員の柔軟な確保が可能となるように必要な措置に取り組むとともに、必要に応じて IoT ボットネットの調査に係る関係者との連携を一層推進[18]する。

[18] IoT ボットネットの観測･調査等に関係する国内の主な観測･調査システムは参考 33 ページを参照。

さらに、このように調査体制や連携を強化することにより、例えば、外部から認証なしに管理画面にアクセスできる機器、脆弱性のある古いファームウェアのままの機器、外部に公開すべきではないポートの空き状況等、NOTICE の調査で得られた様々なデータについて、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脆弱性等に関する状況の可視化等を図り、サイバー攻撃の脅威に関する認識共有や対策の強化に資するよう更なる有効活用を進める。

図 10　今後の NOTICE の全体像



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、あらかじめ電気通信事業者が積極的に対処できるようにする観点から、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 C&C サーバである可能性の高い機器の検知等を行うことできるようにすることが重要である。

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[19]の統計的・相関的な分析による 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（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。

この整理に基づき、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 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、電気通信事業者 3 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 C&C サーバを検知し、(一社)ICT-ISAC において検知された被疑 C&C 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。

[19] 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ー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）

（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

【現状・成果】

本実証事業に参加した電気通信事業者３社それぞれにおいて、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、当該手法の有効性が確認されるとともに、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（図 11）、より迅速な対応につなげられる可能性も期待される。

また、特定の電気通信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（図 12）、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や、より影響度の高い C&C サーバを特定できる可能性も期待される。

（一社）ICT-ISAC においては、新たに WG を立ち上げ、会員社のうち 15 社が WG に参画し、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、課題の整理を行っている。

図 11　C&C サーバの先行検知

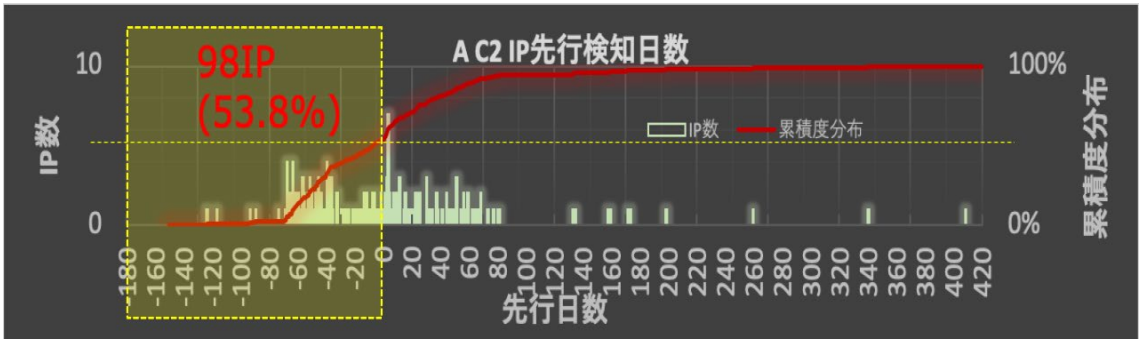


図 12　C&C サーバの検知結果と事業者間の相関性

事業者	C&Cサーバ	
	総IP数	主要な関連マルウェア
事業者A	183 (1.2/日)	Mirai系 116(61%)
事業者B	586 (12.3/日)	Mirai系 388(66%)
事業者C	160 (11.4/日)	Emotet系 86(53%)

【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。

また、８割の C&C サーバは 10 日以内で接続できなくなるとの観測結果もある[20]等、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である。

検知データをセキュリティ対策に効果的に活用するため、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や共有すべきデータの検討とあわせて、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である。

さらに、前述のように、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が期待されているが、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、より多くの事業者が C&C 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。

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（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している。

【課題】

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、ボットネット端末は次々異なる C&C サーバから攻撃指令を受けている状況であることを踏まえれば、「攻撃インフラ」としての 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である。

---

[20] 脚注5参照。

また、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、C&C 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である。

さらに、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、C&C 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ものの、個々の ISP にとってこれらの情報を総合的に収集・分析することが困難であるため、こうした取組を促進するような方策を検討していく必要がある。

（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る C&C 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、C&C 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 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。

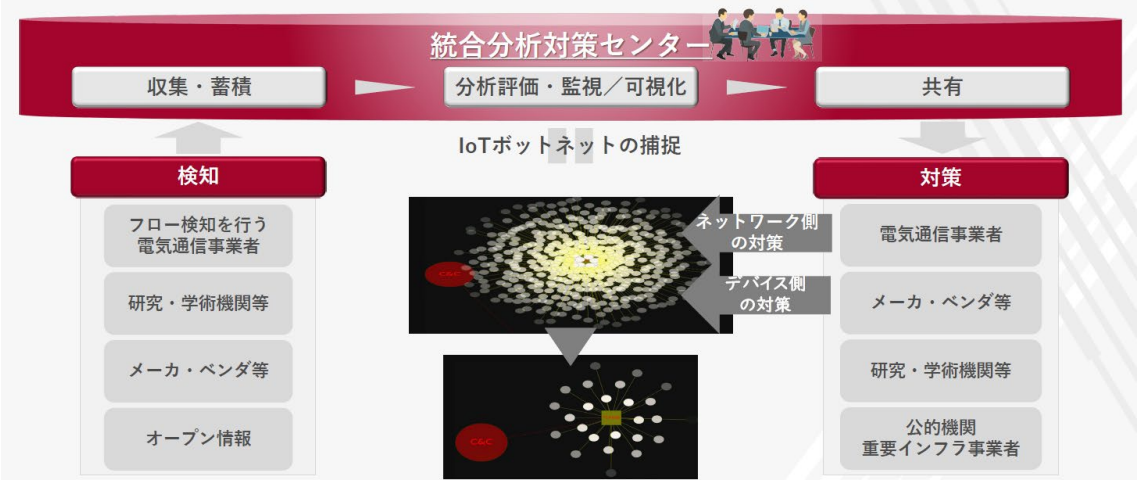
さらに、可能な限り多くの ISP が参加し、C&C サーバの幅広い検知ができるような環境を整備するため、C&C サーバの検知手法に関する ISP 間の情報共有の促進に取り組む。

②IoT ボットネットの全体像の可視化

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 C&C サーバリスト等、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。

IoT ボットネットの全体像を可視化した上で、個々の IoT ボットネットの状況に応じて効果的な対策を講じられるよう、幅広い関係者が柔軟に役割分担をしつつ、NOTICE をはじめとする総合的な対策に取り組み、その対策の効果を確認しながら、最終的に IoT ボットネットを縮小することを目指す。（図 13）

図 13　統合分析対策センター（仮称）のイメージ



４．今後の進め方

本とりまとめは、総合的なIoTボットネット対策の実現に向けて、端末（IoT機器）側、ネットワーク側各々について今後取り組むべき対応策を示したものであるが、いずれの対策についても着手可能なものからスピード感を持って速やかに取り組むことが求められる。

また、IoTボットネット対策は決して国内のみで完結するものではないことから、諸外国の動きや国際的な連携を常に視野に入れながら取組を進めることが必要不可欠である。

本とりまとめで示した対応策の進捗状況等については、必要に応じ、本分科会においてフォローアップを実施することとする。

「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」開催要綱

１ 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である。

本分科会は、「サイバーセキュリティタスクフォース」の下に開催される会合として、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する

２ 名称

本分科会は、「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」と称する。

３ 検討事項

（１）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

（２）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）

（３）上記課題の解決に向けた必要な方策

４ 構成及び運営

（１）本分科会の主査は、サイバーセキュリティタスクフォースの座長が指名する。

（２）本分科会の構成員は、別添のとおりとする。

（３）主査は、本分科会を招集し、主宰する。

（４）主査は、必要があると認めるときは、主査代理を指名することができる。

（５）主査代理は、主査を補佐し、主査不在のときは主査に代わって本分科会を招集し、主宰する。

（６）本分科会の構成員は、やむを得ない事情により出席できない場合において、代理の者を指名し、出席させることができる。

（７）主査は、必要に応じ、オブザーバを招聘することができる。
（８）主査は、必要に応じ、外部の関係者の出席を求め、意見を聞くことができる。
（９）その他、分科会の運営に必要な事項は、主査が定める。

５ 議事・資料等の扱い
（１）本分科会は、原則として公開とする。ただし、主査が必要と認める場合については、非公開とする。
（２）本分科会で使用した資料については、原則として、総務省のウェブサイトに掲載し、公開する。ただし、公開することにより、当事者若しくは第三者の利益を害するおそれがある場合又は主査が必要と認める場合については、非公開とする。
（３）本分科会の議事要旨は、原則として公開とする。ただし、主査が必要と認める場合については、非公開とする

６ スケジュール
本分科会は、令和５年１月から開催する。

７ その他
本分科会の事務局は、サイバーセキュリティ統括官室が行う

（別添）

「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」
構成員名簿

（敬称略、五十音順）

井 上 大 介	国立研究開発法人情報通信研究機構(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
後 藤 厚 宏	情報セキュリティ大学院大学 学長
小 山 覚	NTT コミュニケーションズ株式会社 情報セキュリティ部長 ICT-ISAC ステアリング・コミッティ運営委員長
齋 藤 衛	株式会社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 株式会社情報セキュリティ本部 セキュリティ管理部長
辻 伸 弘	SB テクノロジー株式会社 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

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

における検討状況

回次	議事内容
第１回 （2023 年 1 月 18 日）	✓ 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 ✓ NOTICE の取組状況について
第２回 （2023 年 2 月 16 日）	✓ 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
第３回 （2023 年 3 月 16 日）	✓ 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 ✓ 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
第４回 （2023 年 4 月 21 日）	✓ 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 ✓ 効果的な利用者への周知啓発について ✓ 諸外国におけるサイバーセキュリティ対策の取組事例 ✓ 論点整理
第５回 （2023 年 5 月 18 日）	✓ NOTICE ステアリングコミッティの設置について ✓ 取りまとめ骨子（案）ついて
第６回 （2023 年 6 月 19 日）	✓ 「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～総合的な IoT ボットネット対策の実現に向けて～」（案）について

（参考）

主な観測・調査システム

主体	観測・調査システム	観測・調査内容
NICT	○特定アクセス ○ポートスキャン	・日本国内で弱いID・パスワードを使用している機器を調査 ・リフレクション攻撃の踏み台になりうる機器、管理機能への認証なし管理機能アクセス可能な機器、脆弱性を有するVPN機器等を調査
	●NICTER □DAEDALUSアラート	【ダークネット観測システム】 ・マルウェアに感染した機器からのスキャンを大規模観測し、アラート発報 ・バックスキャッタによるDDoS攻撃検知
	●AmpMon （AmpPot）	【リフレクション型DDoS観測システム】 ・DRDoS（Distributed Reflection Denial-Service）、DDoS攻撃を観測し、アラート発報
	●STARDUST	【サイバー攻撃誘引基盤】人間の攻撃者による攻撃の誘引・観測
	●□WarpDrive	【Web媒介型サイバー攻撃対策プロジェクト】プロジェクト参加ユーザのWebアクセスを観測（悪性サイトを検知し、アラート発報）
	●ライブネット	【機構内システム】機構内の実トラフィックおよびセキュリティ機器から発報されるアラートを観測（観測データはNIRVANA改で統合、CUREへ蓄積）
ICT-ISAC JAPAN	●無人くん ●無人ガーZ □PRACTICE Alert	・重要インフラ観測システム（重要インフラ1000団体、3000URLのレスポンス監視） ・レスポンス観測システム（複数センサーによる特定サイトレスポンス監視） ・DRDoS攻撃アラートシステム（DNSアンプ攻撃、DRDoS攻撃、 DNSランダムサブドメイン攻撃を観測、アラートとして配信）
	○Zakion	・広域スキャンシステム（毎週スキャン、2019年以降時系列データ検索可能）
	○Vuldate	・AIによる脆弱性の攻撃利用の危険度評価・予測システム
横浜国大	●DRDoSハニーポット ●IoTPOT ●IoTボットネットC2判定・監視システム □Am I Infected？	・DRDoS攻撃、DNSランダムサブドメイン攻撃の検知 ・IoT機器等への攻撃観測、悪用された脆弱性を判別すると共にIoTマルウェアの自動収集 ・IoTPOTで収集したマルウェア検体の自動解析、機械学習によりC&Cサーバを自動判定、判定したC&Cサーバに疑似マルウェアスクリプトで接続し、攻撃命令を収集 ・NICTER情報等と突合利用してアラート表示
JPCERT/CC	●TSUBAME	・インターネット上の攻撃動向観測システム（観測用センサーを分散配置） （ICMP、FTP、SSH、TELNET、SMTP、DNS、HTTP、POP3、NTP、IMAP4、HTTPS、MSSQL、RDP等を観測）

※　下線：東京オリンピック・パラリンピック競技大会や、G7広島サミットなどの際にも主に活用、○脆弱性調査、□アラート伝達、●感染・攻撃情報