6　IoT 機器のセキュリティ対策
6　Security Measures for IoT Devices

6-1　NOTICE プロジェクトの 5 年間の成果と新たな歩み
6-1　The Achievements of the NOTICE Project over the Past Five Years and New Advances

衛藤 将史　笠間 貴弘
ETO Masashi and KASAMA Takahiro

NICT ナショナルサイバーオブザベーションセンターにおける、日本国内の脆弱（ぜいじゃく）な IoT 機器の調査と注意喚起の取組である「NOTICE」プロジェクトの過去 5 年間の活動について報告する。本プロジェクトは 2019 年に開始され、総務省、NICT、ISP 及び IoT 機器ベンダーとの連携を通じて進められてきた。本稿では、脆弱な IoT 機器のリスク、具体的な調査手法、実際に行われた注意喚起の事例及びプロジェクトの成果等について詳述する。最後に IoT 機器のセキュリティ向上に向けた新たな取組と今後の展望について述べる。

This paper reports on the activities of the “NOTICE” project, an initiative by National Cyber Observation Center of NICT to investigate and raise awareness about vulnerable IoT devices within Japan over the past five years. The project, which began in 2019, has been advanced through collaboration with the Ministry of Internal Affairs and Communications, NICT, ISPs, and IoT device vendors. This paper details the risks posed by vulnerable IoT devices, specific survey methods, actual examples of awareness efforts, and the outcomes of the project. Finally, it discusses new initiatives and future prospects aimed at improving the security of IoT devices.

1　はじめに

インターネットの発展に伴い、Internet of Things（IoT）機器が私たちの生活に欠かせないものとなった一方で、IoT 機器に関わるサイバー攻撃は増加の一途をたどっており、私たちの生活に深刻な影響を及ぼしている。このような状況をふまえ 2019 年 2 月より、IoT 機器のセキュリティ対策を推進することを目的として、総務省、NICT 及び電気通信事業者（インターネットサービスプロバイダ。以下「ISP」という。）の連携の下、サイバー攻撃に悪用されるおそれのある IoT 機器の調査及び当該機器の利用者への注意喚起を行う取組「NOTICE（National Operation Towards IoT Clean Environment）」が開始された。NICT は、IoT 機器のサイバーセキュリティ対策に貢献するため、サイバーセキュリティ戦略等の政府の方針を踏まえ、NICT の有する技術的知見を活用して、日本国内に存在するパスワード設定等に不備のある IoT 機器の調査及び ISP への情報提供に関する業務を実施することとなっている。

本稿では、NOTICE プロジェクトの 5 年間の活動実績を振り返り、今後の展望について述べる。

2　IoT を取り巻くサイバーセキュリティの状況

IoT 機器が関与するサイバー攻撃は年々増加しており、その被害も大きくなっている。代表的な被害事例として、2016 年に発生した IoT マルウェア（不正プログラム）Mirai による攻撃が挙げられる。Mirai は脆弱な IoT 機器に感染し、それらを踏み台にして標的となるサーバーに大量のトラフィックを送りつけ、サービスを停止させるなどの攻撃、いわゆる分散型サービス妨害（Distributed Denial of Service: DDoS）攻撃を行い、結果として Twitter や Netflix など、多くのウェブサイトが一時的に利用できなくなるなど、深刻な被害をもたらした [1]。

また、2017 年には Reaper と呼ばれる新しい IoT マルウェアが発見された。Reaper は、既知の脆弱性を利

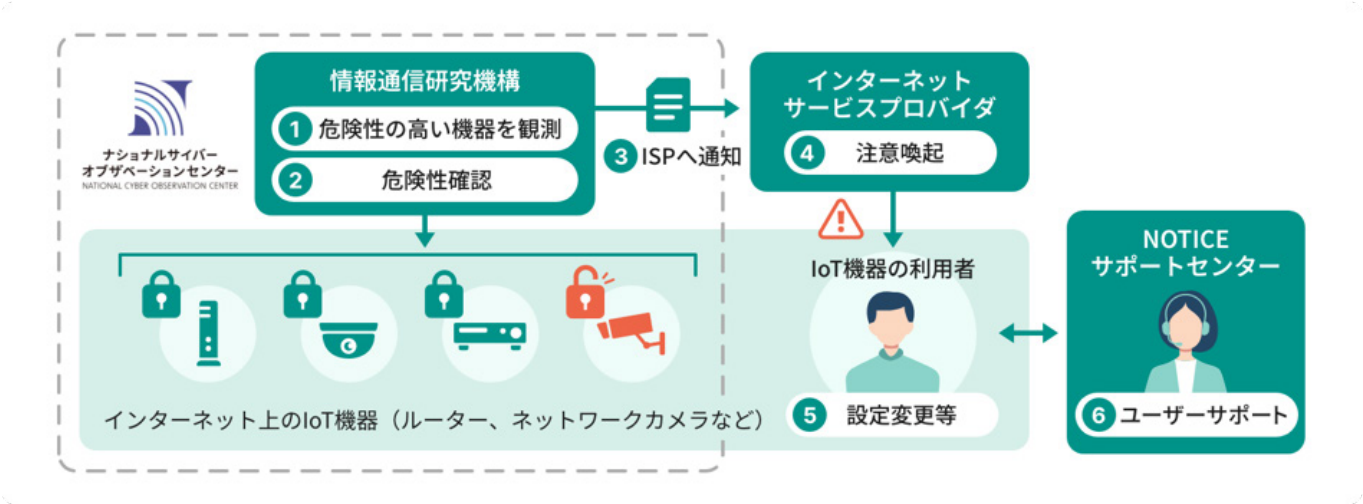

図 1　NOTICE 調査の全体像

用して IoT 機器に感染し、その規模を急速に拡大させ、2017 年の時点で数百万台の感染デバイスを制御下に置き、潜在的に大規模な DDoS 攻撃を引き起こす可能性があるとされた [2]。

さらに、2022 年 9 月 20 日から 28 日にかけて、日本国内のマンション入居者用無料 Wi-Fi サービスで使用されていた Wi-Fi ルーターが IoT マルウェア（Fodcha と推定）に感染し、大規模な DDoS 攻撃に悪用された。全国で約 30 万世帯が当該 Wi-Fi サービスを利用しており、被害は広範囲に及んだ [3]。

脆弱な IoT 機器は、サイバー攻撃の格好の標的となるだけでなく、攻撃の踏み台としても悪用される危険性がある。攻撃者は、脆弱な IoT 機器に侵入し、それを足掛かりに他の機器やネットワークへの攻撃を仕掛けることから、被害は IoT 機器自体に留まらず、より広範囲に波及する可能性がある。例えば、家庭内の IoT 機器がマルウェアに感染した場合、その機器が接続されているホームネットワーク全体が危険にさらされる。また、企業や組織のネットワークに接続された IoT 機器が攻撃された場合、機密情報が漏えいしたり、業務が停止したりするなど、深刻な被害が生じるおそれがある。

このように、セキュリティ対策が十分に行われていない IoT 機器は、マルウェアに感染し、サイバー攻撃に加担してしまう危険性がある。特に、管理機能に適切なアクセス制限を設定していない、推測しやすいパスワードを用いている、ファームウェアのアップデートを行っていないなどの場合に、サイバー攻撃に悪用される可能性が高まることから、このような脆弱な状態の機器を見つけ出し、事前に適切な対策を施しておくことが重要である。

一方で、IoT 機器にはそのセキュリティ対策の推進が難しい側面がある。例えば、IoT 機器に関する具体的なセキュリティリスクや対策手法に関する情報が十分に認知されていないことから、特に一般利用者における対策が進みにくい点が挙げられる。また、ルーターや監視カメラに代表される IoT 機器の多くは 24 時間稼働し、かつ通常は直接の操作を必要としないことから、利用者が乗っ取られたことに気づきにくい点も IoT セキュリティ対策推進の難しさの一つと言える。

3　NOTICE: IoT 機器調査及び利用者への注意喚起の取組

これまで述べたような IoT 機器等を悪用したサイバー攻撃の深刻化や危険性、対策の難しさ等をふまえ、総務省、NICT 及び ISP の連携の下、図 1 に示すとおり、サイバー攻撃に悪用されるおそれのある IoT 機器の調査及びそれらの機器の利用者への注意喚起を行う取組「NOTICE」が 2019 年 2 月より開始された。以降、現在に至るまで、IoT 機器のセキュリティ対策向上を推進することによりサイバー攻撃の発生やその被害を未然に防ぐため、IoT 機器の安全な管理方法の広報や、危険性がある IoT 機器の管理者・利用者への注意喚起等に取り組んでいる。

3.1　NOTICE プロジェクトの組織体制

NOTICE プロジェクトは総務省、NICT、ICT-ISAC を中核として、インターネットサービスプロバイダ（ISP）や IoT 機器ベンダーなどの民間事業者とも連携し、官民一体となって推進されている。このうち総務省は、本プロジェクトの方針決定や全体調整を担い、NICT は技術的な調査・分析やシステム運用などを担当する。ICT-ISAC は、その会員企業である ISP やベンダー等との情報連携・共有を担う。ISP は、自社の

ネットワークにおける観測結果を NOTICE に提供するほか、NOTICE からの注意喚起情報をユーザに周知する役割を担う。IoT 機器ベンダーは、自社製品の脆弱性情報の把握や対策の実施、NOTICE との連携による情報共有などを担っている。また、NOTICE では総務省を中心として、IoT 機器のセキュリティ確保の重要性や具体的な対策等について、広く国民に情報発信を行うとともに、IoT 機器のベンダー等関係事業者に対して、NOTICE の取組や IoT 機器のセキュリティ確保の重要性等について周知を図っている。このように、NOTICE は、多岐にわたる関係者がそれぞれの役割を担い、協力することで、IoT 機器のセキュリティ対策を推進している。

3.2　NOTICE の沿革

NICT の業務に、パスワード設定等に不備のある IoT 機器の調査等を追加（5 年間の時限措置）する国立研究開発法人情報通信研究機構法（NICT 法）等の改正が行われ、2018 年 11 月 1 日に施行された。NICT では、同改正及び実施計画の認可に伴い、ナショナルサイバーオブザベーションセンターを 2019 年 1 月 25 日付で設置し、NOTICE における調査業務を同年 2 月 20 日より開始した。NOTICE の立ち上げに至る背景を含む沿革を表 1 に示し、そのうち主要なものを以下で述べる。

①Mirai による大規模な DDoS 攻撃（2016 年 10 月）

多数の IoT 機器で構成されるボットネット（マルウェア「Mirai」の感染により乗っ取られた IoT 機器群）から DDoS 攻撃が実行され、米国の大手 Web サービスが数時間にわたりアクセスできない事態が発生 [1]。この事件が NOTICE 事業の開始に向けた法改正等の契機の一つとなった。

②NICT 法の改正（2017 年 11 月）

IoT 機器などを悪用したサイバー攻撃の深刻化をふまえ、NICT の業務に、パスワード設定等に不備のある IoT 機器の観測（特定アクセス行為）などを追加する「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」が 2018 年 5 月に成立、11 月に施行された。

③NOTICE の開始（2019 年 2 月）

前述の NICT 法等の改正に基づき、NICT がサイバー攻撃に悪用されるおそれのある IoT 機器を観測し、ISP を通じて管理者・利用者への注意喚起を行う取組「NOTICE」を開始した。

④マルウェア感染機器への注意喚起の開始（2019 年 6 月）

NICT サイバーセキュリティ研究室が運用しているサイバー攻撃観測システム「NICTER」[6] を活用し、マルウェアに感染していることが検知された IoT 機器に対し、ISP から管理者・利用者へ注意喚起を行う取組を開始した。

⑤ NICT 法の再改正（2023 年 12 月）

「国立研究開発法人情報通信研究機構法の一部を改正する等の法律」が成立。2023 年度末までとされていた特定アクセス行為等の運用期限が撤廃されるとともに、IoT セキュリティに関する観測・助言業務（サイバーセキュリティ対策助言等業務）を充実させることとなった。

⑥新しい NOTICE の開始（2024 年 4 月）

NICT 法の改正を受け、NOTICE の活動を拡大し、脅威観測の強化等の取組を開始した。

表 1　NOTICE の沿革

年月	NOTICE に関連する主な出来事
2016年10月	マルウェア「Mirai」による大規模な DDoS 攻撃によるネットワーク障害の発生（①）
2017年 9 月	米国クラウド事業者に対する大規模な DDoS 攻撃が発生 [4]
2017年11月	NICT 法の一部を改正する法律の施行（②）
2019年 1 月	NICT における調査業務の実施計画の認可
2019年 1 月	広報の開始・ISP の参加
2019年 2 月	NOTICE の開始（③）
2019年 6 月	マルウェア感染機器への注意喚起の開始（④）
2022年 9 月	日本国内で感染した IoT マルウェアによる海外への攻撃 [3]
2023年 2 月	アジア最大規模の DDoS 攻撃にボットネットが使用される [5]
2023年12月	NICT 法の一部を改正する法律（再改正）の成立（⑤）
2024年 4 月	新しい NOTICE の開始（⑥）

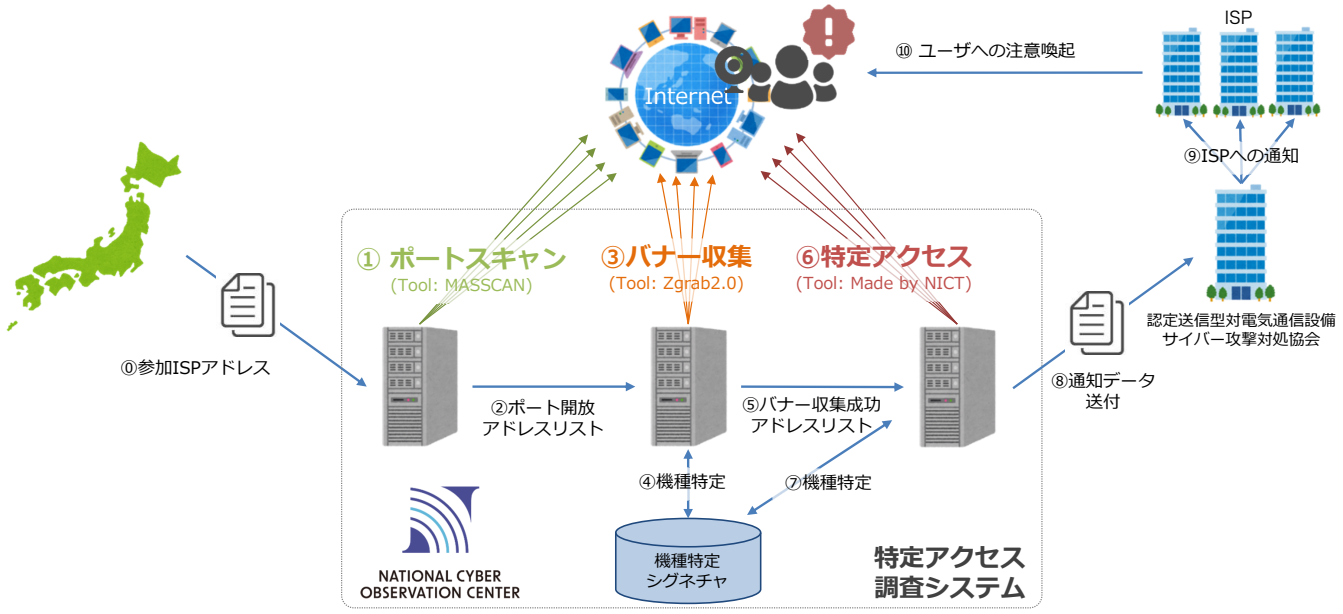

図 2　NICT による特定アクセス調査の概要

3.3　NOTICE における NICT の従来の調査業務

NOTICE における NICT の役割は、日本国内に存在するサイバー攻撃に悪用されるおそれのある IoT 機器を発見し、当該機器の情報を ISP 等へと通知することである。これまでの NOTICE においては ID・パスワードに脆弱性がある IoT 機器の調査を図 2 に示す流れで実施してきた。以下で主要な調査手順について説明する。

(1) ポートスキャン

日本国内のグローバル IP アドレス（IPv4 かつ NOTICE に参加している ISP が保有するアドレスに限定）を対象として、複数の宛先ポート番号に対して通信を行い反応が返ってくるかを確認する。ポートスキャンでは、大量の IP アドレスに対して通信を行う必要があるため、オープンソースソフトウェアの高速スキャンツールである MASSCAN [7] を用いている。

(2) バナー収集

ポートスキャン調査によって応答が得られた IP アドレス・ポート番号に対して実際にリクエスト等を送信し、機器からの応答（バナー）を収集する。収集されたバナーを分析することで、当該 IP アドレス･ポート番号で稼働する機器が何の機器なのかを判定したり、特定アクセスの対象となる ID･パスワードによる認証要求を返す機器かを確認したりすることができる。バナー収集対象数はポートスキャン対象数に対して 2 桁のオーダーで少なくなるため、バナー収集では高速性よりも安定性と拡張性を考慮してオープンソースソフトウェアの Zgrab 2.0 [8] を用いている。

(3) 特定アクセス行為

ID・パスワードによる認証要求のあった機器に対し、実際に容易に推測可能な ID･パスワードを用いてログインを試みる行為を「特定アクセス行為」と呼ぶ。バナー収集の結果、NOTICE の調査対象プロトコルが動作しており ID･パスワードによる認証要求のあった機器に対して特定アクセス行為を行い、特定アクセスに成功する機器（＝サイバー攻撃に悪用されるおそれのある機器）であるか確認する。特定アクセス行為に用いるプログラムは NICT で開発したものである。

(4) ISP への通知

特定アクセス行為に成功した機器について、当該機器への通信の送信元 IP アドレス、送信先 IP アドレス、通信日時（タイムスタンプ）等の情報を内容とする通信履歴等の電磁的記録を作成し、ISP へと通知を行う。

3.4　これまでの実施状況

2023 年 12 月の時点で、国内 82 社の ISP が NOTICE への参加手続きを完了している。当該 ISP に係る約 1.12 億 IP アドレスに対して約 600 種の ID・パスワードを用いて調査を実施し、2023 年度では延べ 61,845 件が注意喚起対象として ISP へと通知された。図 3 は、NOTICE における Telnet と SSH プロトコルによる ID・パスワード脆弱性の調査によって脆弱と判断された、注意喚起対象数を示したグラフである。通知を受けた各 ISP から機器の所有者に対して注意喚起が実施されたことで、2023 年 12 月時点で Telnet/SSH プロトコルにおける注意喚起対象数はピーク時（2020 年 12 月時点）と比較し約 32 % の削減につながっている。なお、新たに接続された IoT 機器が NOTICE 調査で発見され、通知数の増加につながるケースがあるため、NOTICE の注意喚起によって対処された IoT 機器は

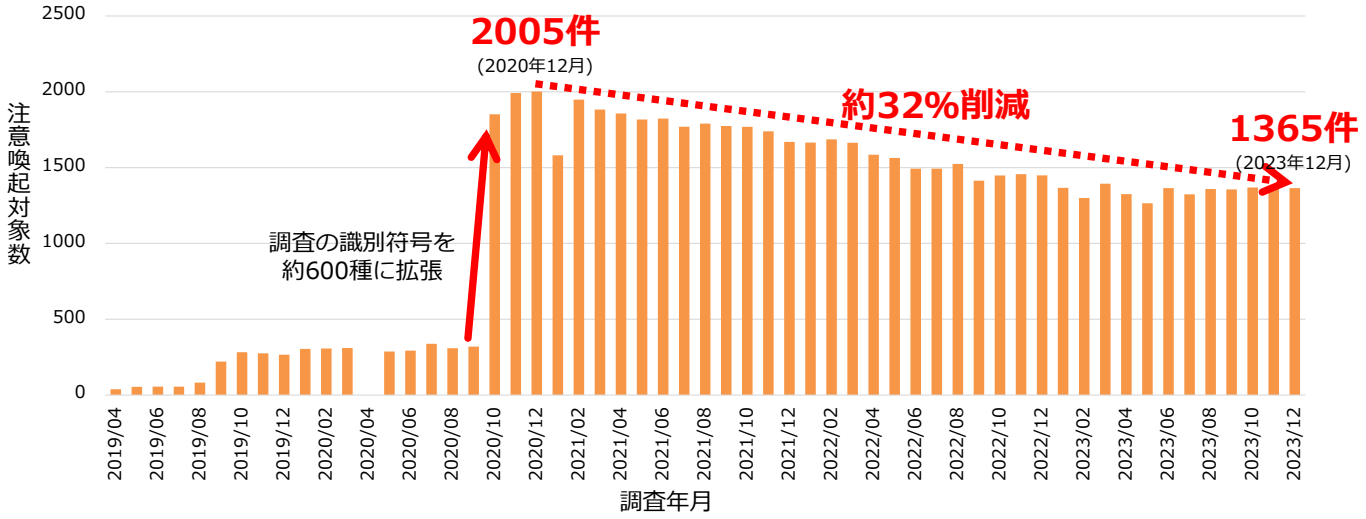

図 3　Telnet/SSH の月ごとの注意喚起対象数の推移（2023 年 12 月時点）

単純な通知件数の削減数よりも多いことが想定される。

また、2021 年度には、特定アクセスの調査対象プロトコルとして従来の Telnet 及び SSH に加え、HTTP/HTTPS の ID･パスワード認証（Basic 認証及び Digest 認証）、2022 年度には HTTP/HTTPS のフォーム認証に対する特定アクセス機能を実現し、以降それらの調査においても機器所有者への注意喚起を行い、日本国内の IoT 機器のセキュリティ対策向上へ貢献している。なお、最新の調査の実施状況は、NOTICE の Web サイト [9] にて公表されている。

また、ナショナルサイバーオブザベーションセンターではこれらの調査業務に加えて NOTICE 事業の附随業務として、IoT セキュリティの向上を目的とした様々な研究開発にも取り組んできた。具体的には、NOTICE と NICTER のダークネット観測の結果から、ID･パスワード設定に不備のある IoT 機器がマルウェアに感染していない状況やその要因、サイバー攻撃に悪用されるリスクに関する分析 [10][11] や、調査結果から、パスワード設定に不備のある IoT 機器の実態と、注意喚起後のユーザのパスワード変更行動を分析した研究 [12]、調査で発見された IoT 機器の実機を用いて、不正ログイン後の悪用可能性を調査し、設定情報の窃取や任意プログラム実行、DDoS 攻撃などのリスクが高い機器が存在することを示した研究 [13][14]、さらに管理用 WebUI を有する IoT 機器が多いことを踏まえ、管理用 WebUI のコンテンツ情報と画像特徴量を組み合わせた機種特定手法を提案した研究 [15] 等、IoT 機器の利用実態や NOTICE 事業が抱える課題に焦点を当て、その解決に向けた研究開発に取り組み、結果として IoT セキュリティの向上に貢献した。

4 新しい「NOTICE」2024 年度からの新たな取組

これまでの 5 年間の取組により、前述のとおり一定の成果は得られたものの、IoT 機器を悪用した DDoS 攻撃などのサイバー攻撃が引き続き発生している。

IoT 調査を業務として規定した 2021 年施行の改正 NICT 法では、NOTICE 業務実施の期限を 2023 年度末と定めていたところ、引き続き発生する IoT 機器に関するサイバー攻撃に対応するため、再度の NICT 法の改正（図 4）を受けて、2024 年度より「サイバーセキュリティ対策助言等業務」の一部として業務が継続されることなった。

これを機に本事業は新しい「NOTICE」として業務内容を刷新し、IoT 機器の悪用によるサイバー攻撃の発生・被害の抑制のため、プロジェクト全体として以下の取組を推進することとなった。

- IoT 機器の悪用を予防する安全管理対策の広報活動の強化
- NICT が 2023 年度末までに限り行うこととされていた ID･パスワードに不備がある IoT 機器の調査（特定アクセス行為）と注意喚起の 2024 年度以降の継続
- 新たに「ファームウェアに脆弱性がある IoT 機器」の調査の NICT の業務としての位置付けと NOTICE の枠組みを通じた注意喚起の実施
- 「既にマルウェアに感染している IoT 機器」の情報提供の NICT の業務としての位置付けと NOTICE の枠組みを通じた注意喚起の継続
- 従来から協力関係にある ISP に加え、IoT 機器のメーカーやその他セキュリティ関係機関等との連携の強化

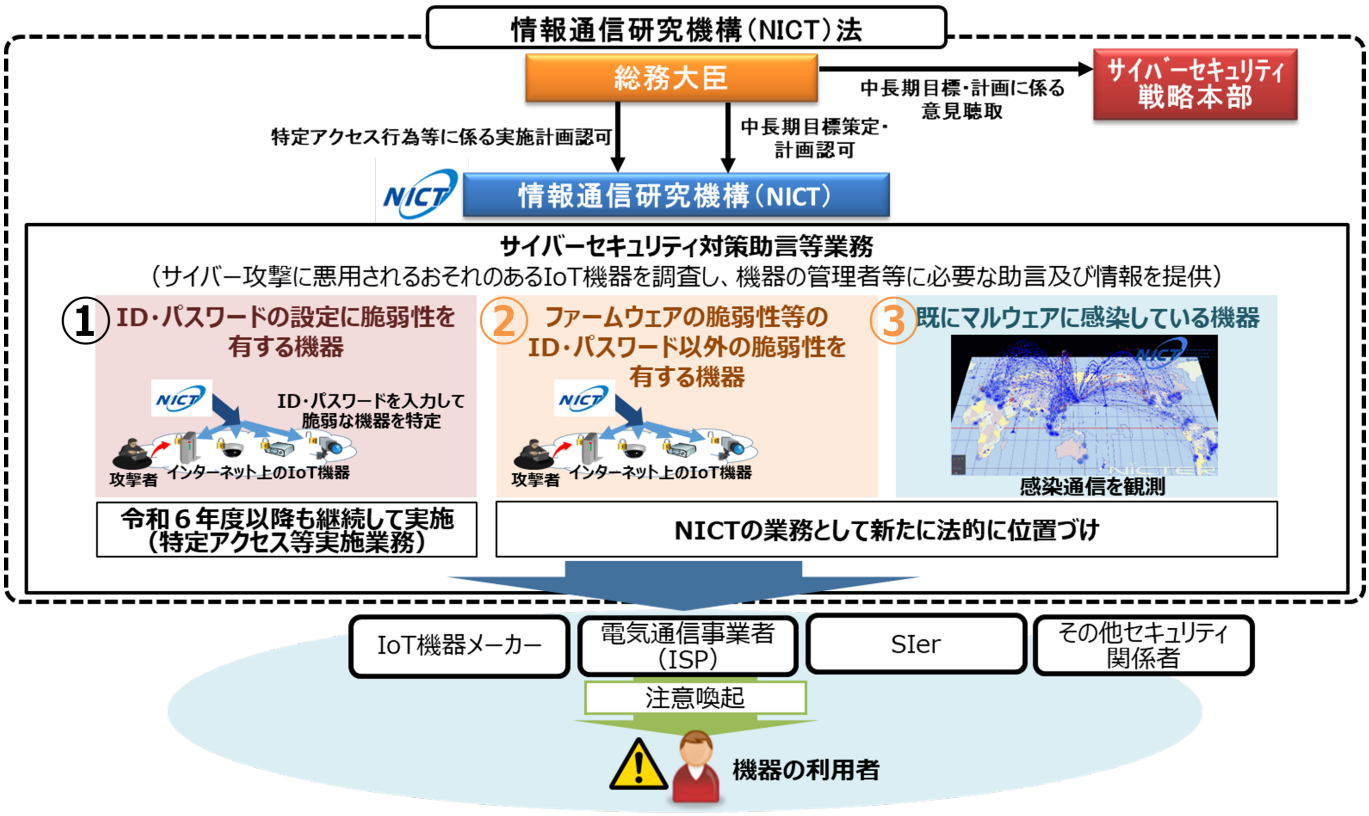

図 4　2024 年度の新たな NOTICE 調査

具体的に新たに NICT の業務として位置づけられた調査は以下のとおり。

ファームウェアの脆弱性を有する機器の調査

IoT 機器のファームウェアに存在する脆弱性は、機器の機能を悪用されたり、不正な遠隔操作を許したりするなど、深刻なセキュリティリスクを引き起こす可能性がある。NOTICE では、2024 年度から、外部から攻撃可能なセキュリティホールなどの、ファームウェアの脆弱性を有する機器を注意喚起の対象として調査する。具体的には、ネットワークからのスキャンにより対象機器の機種名等を特定し、既知の脆弱性データベースとの照合により脆弱性の有無を判断する。調査の結果、脆弱性有りと判断された場合は、機器の利用者やメーカーに注意喚起を行うとともに、ファームウェアのアップデートなどの対策を促す。

マルウェア感染機器の調査

2019 年度より実施してきた、NICTER の観測網による Mirai に感染した IoT 機器の調査について、これを 2024 年度より NICT の業務として位置づけて継続的に実施することとなった。本調査では、NICTER が収集した通信データから、Mirai に感染したと疑われる IoT 機器を特定し、その感染状況や活動状況を分析する。調査の結果、感染が確認された場合は、機器の利用者やインターネットサービスプロバイダに注意喚起を行うとともに、マルウェアの駆除を促す。

5　おわりに

NOTICE は過去 5 年間にわたり、日本国内の IoT 機器のセキュリティ向上に貢献してきた。本プロジェクトにおいて、多くの脆弱な IoT 機器の特定と利用者への注意喚起を継続した結果、脆弱な IoT 機器の数が減少傾向にあることを確認した。また、NOTICE としての啓発活動を通じて利用者や関係機関のセキュリティ意識の向上にも貢献し、これが持続的なセキュリティ向上の基盤となっている。しかし、IoT 機器の多様性や急速な技術進化に伴い、新たな脅威が絶え間なく出現することも事実である。ナショナルサイバーオブザベーションセンターは、今後も NOTICE における官民連携の取組を継続・強化しつつ、最新の技術動向をふまえた効果的な調査に取り組み、IoT セキュリティのさらなる強化と、安全で安心な社会の実現を目指す。

【参考文献】

1　“米 DNS サービスに大規模 DDoS 攻撃で米国で twitter や spotify が長時間ダウン,”
https://www.itmedia.co.jp/news/articles/1610/22/news024.html
2　“IoT 機器を狙うボット「reaper」、数百万台のネットワーク機器に感染,”
https://blog.trendmicro.co.jp/archives/16282
3　“DDoS 攻撃の最新動向,”
https://www.fisc.or.jp/sysaud/pub/event/20221125_FISAC_01.pdf
4　“グーグル、3 年前に中国から 2.54 tbps の DDoS 攻撃を受けていた,”
https://japan.zdnet.com/article/35161125/
5　“アジア太平洋地域の記録的な DDoS 攻撃（900 Gbps）を akamai が緩和,”

https://www.akamai.com/ja/blog/security/record-breaking-ddos-in-apac
6 D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka, and K. Nakao, “nicter: An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis,” WOMBAT Workshop on Information Security Threats Data Collection and Sharing, pp.58–66, 2008.
7 R.D. Graham, “Masscan: Mass ip port scanner,” 2013. https://github.com/robertdavidgraham/masscan
8 Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J.A. Halderman, “A search engine backed by internet-wide scanning,” Proceedings of the 22nd ACM SIGSAC conference on computer and communications security, pp.542–553, 2015.
9 “Notice,” https://notice.go.jp/
10 村上 洸介，笠間 貴弘，井上 大介，“ID/Password 設定に不備のある IoT 機器におけるマルウェア感染可能性の大規模調査，”信学技報，vol.121，no.122，pp.147–152，2021.
11 K. Murakami, T. Kasama, and D. Inoue, “A Large-Scale Investigation into the Possibility of Malware Infection of IoT Devices with Weak Credentials,” IEICE Transactions on Information and Systems, vol.E106.D, no.9, pp.1316–1325, 2023.
12 村上 洸介，笠間 貴弘，井上 大介，“脆弱な IoT 機器管理用パスワードの設定状況と注意喚起効果の分析，”信学技報，vol.122，no.244，pp.20–35，2022.
13 村上 洸介，笠間 貴弘，井上 大介，“実機を使用した不正ログイン後の IoT 機器悪用可能性の調査，”信学技報，vol.122，no.86，pp.31–36，2022.
14 村上 洸介，笠間 貴弘，井上 大介，“Web 管理画面への不正ログイン成功時の悪用リスク調査，”信学技報，vol.122，no.422，pp.91–96，2023.
15 村上 洸介，笠間 貴弘，藤田 彬，浦川 順平，井上 大介，“WebUI のコンテンツ情報と画像特徴量を組み合わせた IoT 機器の機種特定手法，”信学技報，vol.121，no.410，pp.7–12，2022.

衛藤 将史（えとう まさし）

サイバーセキュリティ研究所
ナショナルサイバーオブザベーションセンター
研究センター長
博士 (工学)
ネットワーク技術、セキュリティ人材育成、
イノベーション創出、IoT セキュリティ

【受賞歴】
2021 年　科学技術分野の文部科学大臣表彰 科学技術賞 理解増進部門
2009 年　科学技術分野の文部科学大臣表彰 科学技術賞 研究部門
2007 年　暗号と情報セキュリティシンポジウム (SCIS) 論文賞

笠間 貴弘（かさま たかひろ）

サイバーセキュリティ研究所
サイバーセキュリティ研究室
室長
博士 (工学)
サイバーセキュリティ

【受賞歴】
2022 年　電子情報通信学会 ICSS 2022 年度 研究賞
2019 年　NDSS2019 Distinguished Paper Award
2011 年　情報処理学会 2011 年度山下記念 研究賞