セキュリティ注意喚起を受けた IoT機器所有者の行動要因の調査フレームワーク

関戸 恒介[1,a)]　山口 陽平[1,b)]　櫛引 淳之介[1,c)]　田中 秀一[4]　川村 慎太郎[4]　藤田 彬[4]
佐々木 貴之[2,d)]　吉岡 克成[3]

概要：脆弱な状態でインターネットに公開された IoT 機器やマルウェア感染した IoT 機器の対策の１つとして, そのような機器の所有者に対する注意喚起が行われている．しかし，サイバー衛生向上のためには，現時点では直ちに攻撃に繋がらない潜在的なリスクに対しても，その衛生環境を管理することが望ましい．そのような潜在的なリスクを注意喚起し，機器所有者に行動を促すことはできるのだろうか．効果的な注意喚起のためには，所有者を動機付け，所有者の対処能力に応じた注意喚起が必要である．そこで，潜在的なリスクへ所有者がどのように対処するのか，その要因は何であるかを調査するためのフレームワークを提案する．提案フレームワークは, HTTP, リモートプリント, SSH などのサービスをスキャンし, ポートの開放が確認された所有者に対して注意喚起を行うものである．その際，所有者がポート開放を改善した際のプロセスや，改善しなかった際の阻害要因についても調査を行う．また，必要に応じてユーザサポートを実施する．本稿では, 本フレームワークにおける注意喚起のフローや内容, アンケートとユーザサポートの設計について論ずる．また, ユーザ参加型のセキュリティプロジェクト WarpDrive のシステムを用いた実証実験を予定しており, 計画中の実装についても述べる．

キーワード：IoT 機器，セキュリティ通知，セキュリティアプリ

Framework for Investigating Behavioral Factors of IoT Device Owners Who Received Security Notification

Kohsuke Sekido[1,a)]　Youhei Yamaguchi[1,b)]　Junnosuke Kushibiki[1,c)]　Tanaka Hidekazu[4]
Shintaro Kawamura[4]　Akira Fujita[4]　Takayuki Sasaki[2,d)]　Katsunari Yoshioka[3]

Abstract: One of the countermeasures against IoT devices exposed to the Internet in a vulnerable state or infected with malware is to alert the owners of such devices. However, to improve cyber hygiene, it is desirable to manage the hygiene environment even for potential risks that do not immediately lead to attacks at present. Is it possible to raise awareness of such potential risks and encourage device owners to take action? For effective notifications, it is necessary to motivate owners and provide notifications tailored to their ability to respond. Therefore, we propose a framework to investigate how owners address potential risks and what factors influence their behavior. The proposed framework scans services such as HTTP, remote printing, and SSH, and alerts owners when open ports are detected. During this process, we also investigate the steps owners take when they close exposed ports, as well as the factors that hinder mitigation when they don't. Additionally, user support is provided as needed. In this paper, we discuss the flow and content of notifications within this framework, as well as the design of the questionnaire and user support. We also plan to conduct empirical experiments using the system of WarpDrive, a user-participatory security project. This paper also describes the implementation plan for these experiments.

Keywords: IoT device, Security Notification, Security App

1. はじめに

IoT の普及に伴い, 所有者の意図に反してインターネット上に公開された IoT 機器を狙った攻撃が問題となっている. そのような攻撃は, 様々な対策の進められてきた 2024 年現在においても依然として多く, NICTER の観測レポート [1] によると，攻撃関連の宛先ポートの上位 10 種類のうち 6 種類が IoT 機器でよく利用されるものであった.

このような状態を解消するため, 研究者や公的機関などにより脆弱な IoT 機器やマルウェアに感染した機器の所有者に対する注意喚起が行われており, 一定の効果を示している [2][3][4][5][6][7]. また，機器所有者がリスク解消する妨げとなる要因についても，アンケートなどを通じた調査が行われている [8][3].

以上のような先行事例における注意喚起は深刻度の高いリスクを抱える機器の所有者を対象としたものが多い．そのため，現時点では直ちに攻撃に繋がらないリスク，例えば，IoT 機器の Web インターフェースの公開やリモートコントロールに用いられるサービスの公開のような潜在的なリスクを抱えた機器の所有者に対してどのような効果があるのかについての知見は少ない．しかし, サイバー衛生向上のためには, 潜在的なリスクについても管理し, 先手を打って対策することが望ましい.

そのような潜在的なリスクを注意喚起し, 機器所有者に行動を促すことはできるのだろうか. モチベーション，能力，きっかけによって行動が起こるとする B=MAP モデルによると，効果的な注意喚起のためには，所有者を動機付け，所有者の対処能力に応じた注意喚起が必要である．潜在的なリスクに対する注意喚起では，機器所有者のモチベーションと対処能力の双方について課題が生じることが予想される．しかしながら，その実態は明らかになっていない.

そこで, 本研究では, IoT 機器所有者への注意喚起と同時にアンケートを行うことでユーザの対処能力やモチベーションについて調査する手法を提案する．提案手法では, B=MAP モデルに基づいたアンケートを設計し，アンケート結果とスキャン結果を照らし合わせて，所有者がリスクを解消できた要因やできなかった要因を調べる．具体的には, IoT 機器の Web インターフェースの公開やリモートコントロールに用いられるサービスをスキャンし, ポートの開放が確認された所有者に対して注意喚起を行う. その際, 所有者がサービスを意図して公開しているか, リスクを認識しているか, 対処能力やモチベーションがあるかについても調査する. さらに, 所有者がポート開放を改善した際のプロセスや, 改善しなかった際の阻害要因についても調査を行い, 必要に応じてユーザサポートを行う.

今後, 提案手法を注意喚起システムである WarpDrive に実装し, 実際に調査を実施する予定である．本稿では, 実装の構想や実験デザインについても述べる. WarpDrive における 2024 年 8 月 21 日現在の直近 1 週間の全 PC ユーザ数は 1,377 であり，そのうち，IoT 機器で頻繁に使われているポートや実際に攻撃が行われているポートの開放によるリスクが確認され，注意喚起対象となるものは 71 ユーザであった．対象のリスクとして，とりわけ 443/TCP（HTTPS）や 80，8080/TCP（HTTP），22/TCP（SSH），1723/TCP（PPTP）といった IoT 機器の Web インターフェースやリモート接続で用いられるプロトコルが多く存在していた．今後，これらのポートが開放されている IoT 機器の所有者に注意喚起とアンケートを実施する予定である.

2. 関連研究

IoT 機器のセキュリティに関する研究において，マルウェア感染や脆弱性が確認された機器所有者への注意喚起とその効果検証，および所有者の行動要因を調査する研究が進められている．Sombatruang らは，エンドユーザにセキュリティリスクの解消を促す際の課題として，対策の必要性を理解しつつも，IoT 機器の安全確保が機器の正常使用よりも優先度が低いことを指摘している [9]．また，IoT セキュリティ診断 Web サービス [10] を通じた調査では，ユーザの IT リテラシーが対策実施の障害となったことが報告されている [3].

マルウェア感染機器所有者への注意喚起後の行動を詳細に調査した研究 [8] では，対策実施に必要な手順が十分に提供されていなかったり，逆に複数の情報源から手順が提供されたりして，必要な対策が十分に実施されなかったことが明らかになった．さらに，対策が正しく実施できたかどうかを機器所有者自身で確認する方法がないケースがあったことも報告された.

DNS アンプ攻撃に悪用可能なサービスが動作したホスト管理者への注意喚起を行った研究 [5] では，サポートへのメッセージ分析を通じて行動要因を調査した．その結果，16.1%のユーザが設定変更によりサービスが使用できなくなるとして対策実施を拒否し，40%以上のユーザが追加情報や追加サポートを求めたことが報告されている．大学内

[1] 横浜国立大学大学院環境情報学府
Graduate School of Environment and Information Sciences, Yokohama National University
[2] 横浜国立大学先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University
[3] 横浜国立大学大学院環境情報研究院/先端科学高等研究院
Faculty of Environment and Information Sciences, Yokohama National University / Institute of Advanced Sciences, Yokohama National University
[4] 情報通信研究機構 NICT
[a)] sekido-kohsuke-zs@ynu.jp
[b)] yamaguchi-youhei-zd@ynu.jp
[c)] kushibiki-junnosuke-tf@ynu.jp
[d)] sasaki-takayuki-yv@ynu.ac.jp

ネットワークにおける FTP，Telnet の公開状況や脆弱性を調査し，機器所有者に注意喚起を実施した研究 [6] では，多くの所有者が単純にデバイスの使用を中止することで対策を実施したことが示されている．また，Telnet や FTP の無効化による影響を懸念する所有者に対し，現地でのサポートにて実際には影響がないことを説明することで対策実施を促進できたことが報告されている．

これらの研究は，主に機器のマルウェア感染や脆弱性といった高リスクの事例に限定されていた．一方，村上らの研究 [4] では，ユーザ参加型セキュリティ対策プロジェクト WarpDrive[11] の 1,000 人規模のユーザを対象に，潜在的なリスクを持つポートに対する注意喚起を実施している．その結果，4 回の通知で 60 人に実施され，最終的にリスクの解消に至ったユーザは 25%で，自然解消率の 3 倍以上であったことが報告されている．しかし，この研究では注意喚起の効果について分析した一方で，ユーザが実際にとった対策や行動要因に関するユーザスタディの観点からの調査や分析が不十分であった．

3. 背景

3.1 B=MAP モデル

本研究では，BJ Fogg が提唱した B=MAP モデル [12] に基づいて分析を行う．B=MAP モデルは, 人間の行動がどのように形成され変化するのかを説明するモデルであり, 人間の行動を Motivation, Ability, Prompt の 3 要素で説明する．このモデルでは, 人間は M, A, P の全てが揃うときに行動を起こし, いずれか 1 つでも欠けていると行動しないと考える．

3.2 WarpDrive

WarpDrive[11] は，ユーザ参加型の Web 媒介型攻撃の実態把握や対策を展開するプロジェクトである．ユーザは専用のアプリケーションであるタチコマ・セキュリティ・エージェント（以下「タチコマ SA」と呼ぶ）をインストールすることでプロジェクトに参加できる．タチコマ SA は PC ユーザ向けに Chrome 拡張機能，モバイルユーザ向けに Android アプリが提供されている．タチコマ SA をインストールすることで誰でも本プロジェクトに参加することができる．

4. リサーチクエスチョン

IoT 機器への攻撃対策として, 脆弱な機器やマルウェア感染した機器所有者に対する注意喚起が行われており，一定の成果を示している．また，注意喚起を受けた機器所有者の行動やその要因についても調査されている [8]．しかし，サイバー衛生向上のためには，現時点では直ちに攻撃に繋がらない潜在的なリスクに対しても，その衛生環境を管理することが望ましい．そのような潜在的なリスクを注意喚起し，機器所有者に行動を促すことはできるのだろうかという疑問が浮かぶ．例えば，所有者が IoT 機器のサービスを意図的に公開していることが，所有者のリスク対処のモチベーションを低下させるかもしれない．しかしながら，このことについては，先行研究では十分に明らかにされてはいない．

そこで，本研究では，**RQ1．潜在的なリスクに関するセキュリティ通知を受けた IoT 機器所有者は，自身の機器のセキュリティリスクに対してどのような行動を取るのか．**に回答するためのフレームワークを提案する。さらに，フレームワークを通じた調査においてリスクが解消した/しなかった機器所有者へのアンケートにより，**RQ2．潜在的なリスクに関するセキュリティ通知を受けた機器所有者の行動要因は何か**に答えることができることも示す．

5. 注意喚起モデルと IoT 機器所有者の行動要因の調査フレームワーク

本論文では，潜在的なセキュリティリスクを持つ家庭向け IoT 機器所有者に対する注意喚起を通じて，彼らがそのようなリスクを解消する行動要因を調査するためのフレームワークを提案する．本章ではその詳細を説明する．

5.1 フレームワークの適用条件

本フレームワークは，IoT 機器のセキュリティリスクと対処方法を機器の所有者に個別に通知し，対策を勧める注意喚起活動に適用可能である．また，行動要因を調べるために，通知送付後に機器所有者に対するフォローアップが実施可能である必要がある．具体的には，リスクが見つかった IoT 機器を再度スキャンし，注意喚起者がリスクを解消したかどうかを確認できる必要がある．そのために，IP アドレスが変更された場合にも機器を追跡できるような仕組みが存在することが望ましい．また，対策の実施を確認できない所有者に対してスキャン結果を再度伝えるフォローアップやユーザサポートを実施するために，注意喚起者と機器所有者の間で双方向かつ任意のタイミングでコミュニケーションをとることができる必要もある．

機器所有者と注意喚起者の間にあらかじめコミュニケーションチャネルが存在する場合は本フレームワークが適用可能である．具体的には，専用アプリやセキュリティ診断 Web サービスを通じた注意喚起では，サービス利用開始と同時に，ユーザと注意喚起者とのコミュニケーションチャネルが確保される．また，ISP やネットワーク管理者が主体となって，自身が管理する IP アドレスを調査する場合では，彼らとリスクが見つかった機器所有者との間に何らかの連絡手段が存在する．前者は WarpDrive[11] や “am I infected”[10]，後者は大学ネットワークを対象にセキュリティ調査を実施した研究 [6] などが該当する．

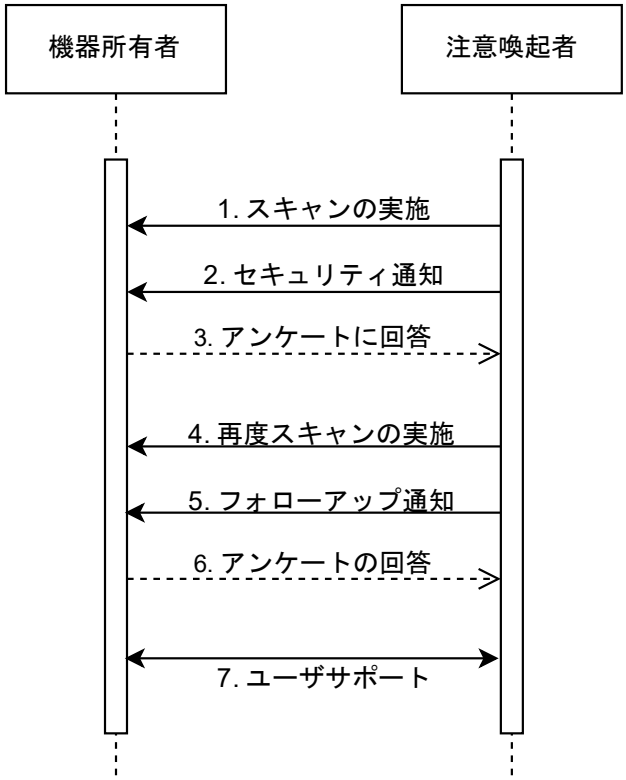

図 1 調査フレームワークのフロー
*2 以降，いつでも機器所有者から依頼可能．必要に応じて注意喚起者からユーザサポートを受けるように促すことも可能．

5.2 注意喚起と調査の手順

注意喚起と調査手順の概略を図 1 に示す．まず，IoT 機器に対してポートスキャンを実施し，セキュリティリスクが発見された場合，その旨を機器所有者に通知をする．また，一定期間後に再度ポートスキャンを実行し，セキュリティリスクが解消したかどうかを伝えるフォローアップ通知を実施する．また，セキュリティリスクの通知と同時にアンケートを実施する．さらに，セキュリティ通知を受けたユーザは任意のタイミングでサポートを依頼することができる．必要に応じて注意喚起者からユーザサポートを受けるように促すことも可能であると尚良い．

以下では，IoT 機器のセキュリティリスクの調査，注意喚起の内容，行動要因の調査のためのアンケート，ユーザサポートについて述べる．

5.2.1 IoT 機器のセキュリティリスクの調査

ポートスキャンによって IoT 機器の潜在的なリスクとなりうる TCP ポートの公開を調査する．ここでは，IoT 機器の潜在的なリスクとして，Web インターフェイスの公開（HTTP, HTTPS で用いられるポートの開放）やリモートアクセスに用いられるサービスの公開（SSH や RDP, PPTP など VPN で用いられるポートの開放）などを想定し，各々のポートの開放を 1 つのリスクとみなす．特に HTTP, HTTPS ポートの開放が確認された対象については自動化した Web ブラウザでスクリーンショットも取得する．スクリーンショットは，機器の所有者が注意喚起対象の機器を特定する手がかりとして，機器の所有者に提示される．

5.2.2 セキュリティ通知の送付

5.2.1 項にて特定した IoT 機器の所有者に対してリスクの解消を促すため，セキュリティ通知を送付する（以下，初回通知と呼ぶ）．初回通知を送付してから一定の期間が経過したら，フォローアップのため，機器所有者にリスクが解消したかを伝える（以下，フォローアップ通知と呼ぶ）．特にリスクが解消していない機器の所有者に対して対策方法などを改めて提示する．また，必要に応じて注意喚起者から積極的にサポートを受けるよう促す．

初回通知とフォローアップ通知では，5.2.1 項にて検出したそれぞれのリスクについて，リスクの説明と対策方法を提示する．特に Web 系ポートについては機器所有者が該当機器の型番やサービスについて理解を促すためスクリーンショットも同時に送付する．以下に HTTP，HTTPS ポートの開放が確認された機器所有者に対する通知コンテンツの例を示す．

- リスク名：誰でも以下の Web 画面にアクセス可能 [スクリーンショットを添付する．]
- Web 画面がインターネットに公開されています。不正アクセスを受けたりマルウェア感染する恐れがあります。対策が必要です。
- ルーターの設定画面の場合，機器のマニュアルに従って管理画面のインターネットへの公開を停止してください。自宅内の機器の画面の場合、ルーターのマニュアルに従って「ポート変換」＊の設定を確認し、[該当のポート番号] の設定をオフにしてください。
  ＊メーカにより呼び方が異なり、「ポートフォワーディング」「ポートマッピング」「静的 NAT」などと呼ばれることもあります。

5.2.3 行動要因の調査のためのアンケート

5.2.2 項における初回通知，フォローアップ通知の送付と同時にアンケートを実施する．以下では，それぞれのアンケート内容について述べる．

5.2.3.1 初回通知でのアンケート

初回通知と同時に実施するアンケートの項目を表 1 に示す．なお，複数のリスクが検知された機器所有者に対しては，それぞれのリスクごとにアンケートを実施する．

まず，リスクの原因となっている機能を機器所有者が意図してインターネットに公開しているのかを尋ねる．次にその機能の使用用途や機器のタイプ（ルータ，カメラなど），メーカ，型番を尋ねる．さらに，その機能をどのように設定したのかを尋ねる．

表 1 初回通知でのアンケート

No.	対応する RQ	アンケート項目	種類
1-1	2	この機能を意図してインターネットに公開していますか.	はい/いいえ/わからない
1-2	1, 2	用途に心当たりがあれば教えてください.	自由記述
1-3	1, 2	機器に心当たりがあれば, 機器のタイプ (ルーター, カメラなど), メーカー, 型番を分かる範囲で教えてください.	自由記述
1-4	1, 2	どのように設定したか心当たりがあれば教えてください.	自分で設定した/初期設定/わからない/その他
1-5	2	あなたは提示されたリスクをどれだけ深刻なものと受け止めていますか.	自由記述
1-6	2	あなたはリスクを解消したいと考えていますか	1 - 5
1-7	2	あなたは提示された対策を実施したいと考えていますか.	1 - 5
1-8	2	提示された対策をご自身で実施できますか.	1 - 5
1-9	2	実施できない場合，その理由を教えてください.	自由記述

次に，提示したリスクをどれだけ深刻なものと受け止めているかを機器所有者に質問する．次に，機器所有者がどの程度リスクを解消したいと考えているか，どの程度提示された対策を実施したいと考えているかを尋ねる．最後に，機器所有者にとっての対策の難易度を調査するために，提示された対策を自身で実施できるか，実施できない場合，その理由は何かを尋ねる．

5.2.3.2 フォローアップ通知でのアンケート

フォローアップ通知でのアンケートでは，セキュリティ通知を受けて機器所有者がどのような行動を取ったのか/何もしなかったのかと，その要因を調べる．実施するアンケートの内容を表 2 に示す．なお，複数のリスクが検知された機器所有者にはそれぞれのリスクに対しては，それぞれのリスクごとにアンケートを実施する．

まず，機器所有者にどのような対策の実施を検討したかを確認する．検討していなかった場合には「なし」と回答するよう指示する．次に，対策実施と機器のマニュアルの関係を調査する．具体的には，対策を検討する際に参考にしたものを尋ね，機器のマニュアルを見つけることができたかどうかを確認し，マニュアル中に対策実施のための手掛かりがあったかどうかを質問する．続いて，機器所有者が検討した対策が最後まで実施できたのかを確認する．最後に，対策を実施する上で困った点や難しかった点があったかどうかを質問する．

5.2.4 ユーザサポート

機器所有者は，注意喚起の実施者から一方的にセキュリティ通知を受けるだけでなく，機器所有者が個別のサポートを受けられることが望ましい．IoT 機器の潜在的なリスクに対する注意喚起は，マルウェア感染や脆弱性に対する注意喚起に比べ，リスクを理解するために必要な知識や想定されるユースケースが多い．また，機器所有者が該当の機能を利用している場合は代替手段が必要だが，その設定はただ機能を停止するよりも難しいと想定される．例えば，リモートデスクトップのための RDP がインターネットに直接公開されていた場合，外出先からリモートデスクトップを安全に使い続けるために，新たに VPN の設定をするなど，機器所有者にとって今まで経験のない作業が必要になると考えられるためである．これらすべてに対応した通知コンテンツを作成することは困難であり，潜在的なセキュリティリスクに対する機器所有者の行動を調べるためにもユーザサポートの提供が望ましい．

5.3 調査結果の分析

以上の調査フレームワークに基づいてスキャンやアンケート，ユーザサポートを実施し，その結果を分析することで，リサーチクエスチョンに回答できる．

5.3.1 IoT 機器所有者の行動 (RQ1) の分析

セキュリティ通知を受けた機器所有者がどのような行動を取るのかを，スキャン結果とアンケートの結果をもとに分析する．

- セキュリティリスクの解消が確認されたか．ポートスキャン結果を基に，ポート開放が解消されたを分析することにより確認できる．
- 機器所有者がどのような対策を検討したか．アンケート No.2-1,2-2 を分析することにより，対策の検討の有無と検討内容，その際に何を参考にしたのかを確認できる．
- その対策がどこまで実施できたか．アンケート No.2-3,2-4,2-5 を分析することにより，検討した対策内容と，マニュアルが対策の助けとなったか，最後まで対策を実施出来たかを確認できる．

5.3.2 IoT 機器所有者の行動要因 (RQ2) の分析

BJ Fogg が提唱した B=MAP モデル [12] に基づいて，セキュリティ通知をきっかけ（Prompt）とした機器所有者の

表 2　フォローアップ通知でのアンケート

No.	対応する RQ	アンケート項目	答え方
2-1	1	どのような対策の実施を検討しましたか？（検討していなかった場合は「なし」と記載ください.）	自由記述
2-2	1,2	対策を検討する際に参考にしたものを教えてください.	自由記述
2-3	1,2	機器のマニュアルは見つけられましたか.	はい/いいえ
2-4	2	マニュアルから対策の実施のための手掛かりは見つけられましたか.	はい/いいえ
2-5	1	対策は最後まで実施できましたか	はい/いいえ
2-6	2	対策を実施する上で困った点や難しかった点はありましたか.	自由記述

行動要因を「機器所有者がリスクを解消するモチベーション」,「対策を実施するモチベーション」,「対策を自身で実行する能力」に分けて分析する.

初回通知時のアンケートを通じて,「機器所有者がリスクを解消するモチベーション」,「対策を実施するモチベーション」を，以下のように分析できる.

- 機器所有者が通知されたセキュリティリスクを深刻なものだと考えているかどうか．アンケート項目 No.1-5 にて，機器利用者に直接聞いている.
- 機器所有者がセキュリティリスクの要因となったサービスを意図して公開しているかどうか．アンケート項目 No.1-1 にて，機器利用者に直接聞いている.
- 機器所有者が対策の実施による副作用を懸念しているかどうか．アンケート項目 No.1-2,1-3,1-4,1-8,1-9,2-1,2-6 を分析することにより，何を目的にポートを公開していたか，どのような対策を検討して，その結果，対策を実施したのか否かを分析することにより，副作用の懸念を確認する.
- 機器所有者が対策の実施を面倒だと感じているかどうか．アンケート項目 No.1-8,2-1,2-6 を分析することにより，確認出来る.

同様に,「機器所有者が対策を自身で実行する能力の結果」の要因を，以下のように分析可能である.

- 機器所有者がセキュリティリスクの内容や対策方法を理解する十分な IT リテラシーを持っているか．アンケート項目 No.1-9,2-1,2-6 にて，対策の実施の可否や困難な点を聞くことにより，利用者の IT リテラシーの有無を確認する.

また，ユーザサポートにおける機器所有者とのやり取りの結果を，以上の項目に当てはめて分析を行うことも可能である.

6. WarpDrive を用いた注意喚起と調査のデザイン

本章では，WarpDrive を用いて実施予定の注意喚起及び調査のデザインについて述べる.

まず，タチコマ SA から定期的に機器のグローバル IP アドレスを取得する．そのグローバル IP アドレスに対してスキャンを実施し，その結果をもとにリスクのある機器を特定する．対象ユーザに対してタチコマ SA を介してセキュリティ通知を送り，同時にアンケートを実施する．通知を確認したユーザに対しては，初回通知から 1 週間後にリスク解消の有無を伝えるフォローアップ通知を実施し，また，必要に応じてタチコマ SA 経由の個別のユーザサポートを実施する.

6.1 WarpDrive 特有の課題

WarpDrive プロジェクトでは，タチコマ SA はスマートフォンやノートパソコンなどにインストールされることがあり，ユーザの自宅や外出先，勤務先など複数のインターネット環境を利用することがある．そのため，5.1 節の「機器所有者と注意喚起者が双方向かつ任意のタイミングでコミュニケーションをとることが可能」という要件を満足するためには，WarpDrive ユーザと機器所有者，すなわちタチコマ SA から取得したグローバル IP アドレスのスキャンにより発見された機器の所有者が一致している必要がある.

そのような場合に絞って調査を行うため，スキャン結果による注意喚起対象の絞り込みと，通知送付時にネットワーク環境に対する確認を実施する．具体的には，ユーザの自宅や外出先，勤務先などは IP アドレスの AS 番号が異なると仮定して，ユーザが日常的に利用しているネットワークであることを確認するために「あるユーザに対して特定されたリスクのある機器のうち，直近 1 ヶ月で 2 回以上同一の AS 番号で発見されている」という条件を設ける．加えて，直近の問題のみを注意喚起するために「そのうち 1 回は 1 週間以内に発見されている」という条件を加える.

しかし，以上のプロセスでは，外出先などで，ユーザ自身が機器の所有者ではない場合を完全に排除することができない．そのため，注意喚起対象の機器がユーザの所有物であるかどうかを確認するために，検出したリスクが自宅の機器のものであるかを，注意喚起実施時にアンケートで確認する.

表 3　通知対象ポート一覧

プロトコル	ポート番号	リスク名
LPR IPP	515 631	無断で印刷される恐れ
SSH	22	ルータ・コンピュータ・IoT 機器を無断で操作される恐れ
RDP	3389	PC を無断で操作される恐れ
FTP	21	データの漏洩の恐れ
-	50000	カメラの映像が無断で見られる恐れ
PPTP	1723	自宅ネットワークに侵入される恐れ
POP3 POP3S	995 110	メール受信サーバーが攻撃される恐れ
SMTP	25,465	メール送信サーバーが攻撃される恐れ
HTTP, HTTPS	80 など* 443	誰でも以下の Web 画面にアクセス可能
MS-SQL-S MySQL	1433 3306	データベースの情報の漏洩・改ざんの恐れ
TELNET	23	古い通信プログラムの動作

*...NICTER 観測レポート [1] を参考に 81, 3128, 8000, 8080, 8082, 8443, 8081, 10000, 10001 も含めた

6.2　WarpDrive を用いた注意喚起とアンケートの実施

スキャン対象ポート：スキャン対象の TCP ポートを表 3 に示す．NICTER の観測結果 [1] や文献 [4] を参考に，攻撃が実際に行われていることが明らかになっているポートや，IoT 機器で頻繁に使われているサービスに関連するポートを選定した．また，HTTP，HTTPS については，IoT 機器の WebUI を取得するためスクリーンショットも収集する．

通知の送付とアンケートの実施方法：セキュリティ通知とアンケートは，タチコマ SA の機能と Google フォームを併用して実施する．具体的には，タチコマ SA の機能を用いてユーザに対して，セキュリティリスクの概要と Google フォームのリンクを含むメッセージを送信する．Google フォームの 1 ページ目でセキュリティリスクについての詳しい説明や対策方法示し，2 ページ目以降に 5 章で論じたアンケートを実装する．なお，サービス品質向上のために，「本注意喚起が役に立ったか」と「良かった点」「悪かった点」を追加でユーザに質問する．

ユーザサポート：タチコマ SA がユーザと注意喚起者の間で一対一のコミュニケーションをチャット形式でとることができる特徴を利用し，注意喚起対象の WarpDrive ユーザに対してユーザサポートを提供し，セキュリティリスクや対策方法などについての質問を受け付ける．チャットでは，通常のテキストのほか，画像の添付をすることも可能である．ユーザは，初回通知受け取り後いつでもサポートを依頼することができる．

7.　考察

7.1　制限事項

本フレームワークを実現するためには，注意喚起やフォローアップのためのコミュニケーションチャネルの確保が必要である．そのため，不特定多数のアドレスに対してスキャンを行い，見つかったリスクに対して注意喚起する場合，IP アドレスから機器所有者を特定する必要がある．法人や大学が IP アドレスの管理者である場合は，一般に連絡先が公開されているため注意喚起者から直接連絡することが可能であるため，本フレームワークを適用した調査を実施できる．しかし，IP アドレスの管理者が ISP である場合は，注意喚起者は ISP を介して機器所有者に注意喚起を実施する．そのため，その都度注意喚起のために ISP と交渉を実施しフォローアップを実施することは現実的に困難であろう．

7.2　注意喚起の対象となるユーザ数の見積もり

2024/8/21 現在の 1 週間で見つかった全 PC ユーザは 1,377 名であった．そのうち，6.1 節より，ユーザが日常的に利用するネットワークに対する 1 週間以内に発見された表 3 に示したリスクを通知する場合，71 ユーザが通知対象であった．図 2 に通知対象ユーザの見積もりを示す．通知対象のリスクとして，とりわけ 443/TCP（HTTPS）や 80,8080/TCP（HTTP）のような IoT 機器の Web インターフェースでよく用いられるポートや，22/TCP（SSH），1723/TCP（PPTP）といった遠隔でコンピュータや IoT 機器を操作するために用いられるプロトコルが多く存在していた．

7.3　今後の課題

今後，意図的に IoT 機器のサービスを公開している機器所有者への対応をさらに検討する必要がある．特に，その機器所有者がその機能を使い続けたいと考えている場合，どのような対策を推奨すべきかを慎重に検討する必要がある．例えば SSH の機能を使う場合には，パスワード認証を無効にして公開鍵認証でのみログインできるようにする，デフォルトのポート番号を変更するなどが考えられる．セキュリティリスクと利便性のバランスを考慮した適切な対策を提案することが重要である．

8.　まとめ

本論文では，IoT 機器の潜在的なセキュリティリスクに対する注意喚起を受けた機器所有者の対策行動とその要因を調査する手法を提案した．それは，注意喚起と同時に実施するアンケートや，その後のフォローアップでのアンケート，ユーザサポートを通じて，機器所有者が取った実

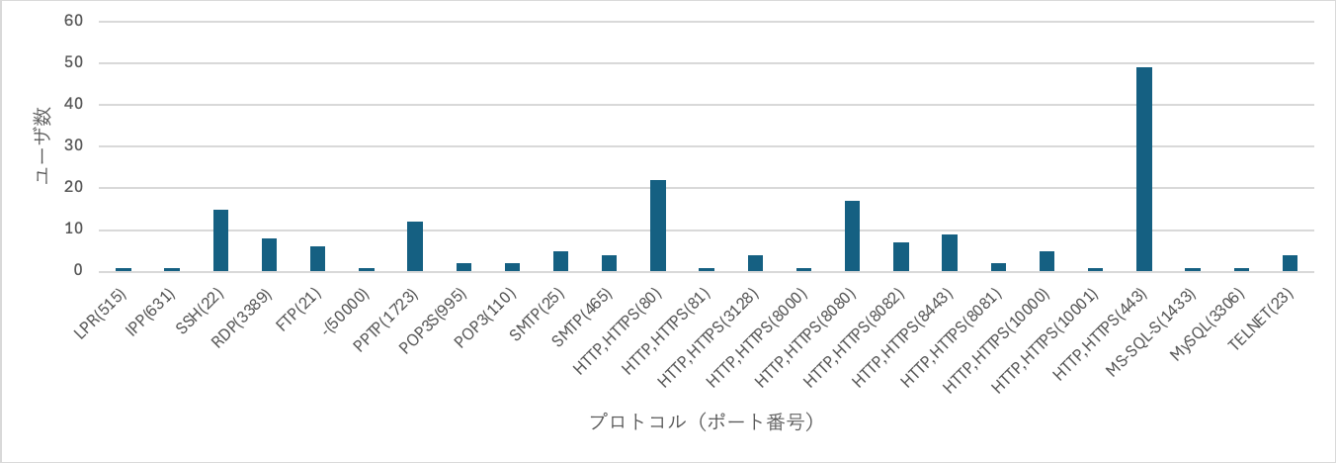

図 2 2024/8/21 時点の通知対象ユーザ数

際の行動やモチベーション，対処能力を明らかにするものである．今後，この手法を WarpDrive に実装し，調査を実施する予定である．

謝辞 本研究は，国立研究開発法人情報通信研究機構 (NICT) の委託研究（JPJ012368C05201，JPJ012368C08101）により得られた成果を含む．本研究の一部は JSPS 科研費 23K11099 の助成を受けて行われた．本研究の一部は，国立研究開発法人情報通信研究機構 (NICT) の委託研究「Web 媒介型攻撃対策技術の実用化に向けた研究開発」の支援により得られた．

参考文献

[1] 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：NICTER 観測レポート 2023，国立研究開発法人 情報通信研究機構（オンライン），入手先 ⟨"https://csl.nict.go.jp/report/NICTER_report_2023.pdf"⟩（参照 2024-8-12）．

[2] 総務省, 国立研究開発法人情報通信研究機構（NICT），一般社団法人 ICT-ISAC：NOTICE, https://notice.go.jp/.

[3] 稲澤朋也, 佐々木貴之, 吉岡克成, 松本勉：am I infected? IoT セキュリティ診断 Web サービスを用いたエンドユーザへの注意喚起の実証実験，コンピュータセキュリティシンポジウム 2022 論文集，pp. 176–183（オンライン），入手先 ⟨https://cir.nii.ac.jp/crid/1050857512396979840⟩ (2022).

[4] 村上颯人, 藤田彬, 佐々木貴之, 田辺瑠偉, 山田明, 吉岡克成, 松本勉：セキュリティ設定に不備のある IoT 機器の所有者に対する専用アプリを介した注意喚起の効果検証，コンピュータセキュリティシンポジウム 2021 論文集，pp. 183–190 (2021).

[5] Çetin, O., Gañán, C., Altena, L., Tajalizadehkhoob, S. and van Eeten, M.: Tell Me You Fixed It: Evaluating Vulnerability Notifications via Quarantine Networks, *2019 IEEE European Symposium on Security and Privacy (EuroS&P)* (2019).

[6] Takayuki Sasaki et al,: Who Left the Door Open? Investigating the Causes of Exposed IoT Devices in an Academic Network, *2024 IEEE Symposium on Security and Privacy (SP)* (2024).

[7] Sasaki, T., Fujita, A., Gañán, C. H., van Eeten, M., Yoshioka, K. and Matsumoto, T.: Exposed Infrastructures: Discovery, Attacks and Remediation of Insecure ICS Remote Management Devices, *2022 IEEE Symposium on Security and Privacy (SP)* (2022).

[8] Bouwmeester, B., Rodríguez, E., Gañán, C., van Eeten, M. and Parkin, S.: "The Thing Doesn't Have a Name": Learning from Emergent Real-World Interventions in Smart Home Security, *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)* (2021).

[9] Sombatruang, N., Caulfield, T., Becker, I., Fujita, A., Kasama, T., Nakao, K. and Inoue, D.: Internet Service Providers' and Individuals' Attitudes, Barriers, and Incentives to Secure IoT, *32nd USENIX Security Symposium (USENIX Security 23)* (2023).

[10] 横浜国立大学・情報・物理セキュリティ研究拠点：am I infected? - マルウェア感染・脆弱性診断サービス，https://amii.ynu.codes/.

[11] 国立研究開発法人情報通信研究機構（NICT），セキュアブレイン（日立システムズ），横浜国立大学, 神戸大学, 岡山大学, 金沢大学：WarpDrive, https://warpdrive-project.jp/.

[12] Fogg, B.: A behavior model for persuasive design, *Proceedings of the 4th International Conference on Persuasive Technology*, ACM (2009).