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

村上 颯人[1,a)]　藤田 彬[2]　佐々木 貴之[3]　田辺 瑠偉[3]　山田 明[4]　吉岡 克成[5]　松本 勉[5]

概要：セキュリティ設定に不備のあるIoT機器やマルウェア感染した機器をネットワーク観測によって発見し，当該機器のユーザに対して対策のための通知や情報提供を行う活動の重要性が高まっている．広く実施されているISPによる注意喚起を補完するセキュリティ通知手法として，我々はユーザ端末にインストールされた専用アプリケーションを通じて注意喚起を行うモデルに着目し，その実現例としてユーザ参加型のセキュリティプロジェクトであるWarpDriveにおける通知実験とその効果測定方法を検討してきた．本報告では，1000人規模のWarpDriveアクティブユーザのうち，サイバー攻撃を受ける可能性があるポートの開放とネットワークサービスの公開を継続的に行っている60人に対して実際に通知実験を行った結果を示す．実験の結果，通知したユーザの28人 (47%) から反応が得られ，通知していない時と比べて3倍以上のポート開放状況の改善が見られた．また，通知時のアンケートでは，注意喚起対象ユーザのネットワーク環境は20人 (74%) が自宅，6人 (22%) が勤務先，1人 (4%) が外出先との回答が得られた．さらに，自宅からインターネット接続するユーザ20人のうち，半数の10人はポート開放とサービス公開は意図的でないと回答した．これらの結果は今後，エンドユーザへの効果的な注意喚起を検討する上での重要な知見といえる．

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

Measuring the effectiveness of notification to the users of insecure IoT devices via dedicated apps

Hayato Murakami[1,a)]　Akira Fujita[2]　Takayuki Sasaki[3]　Rui Tanabe[3]　Akira Yamada[4]
Katsunari Yoshioka[5]　Tsutomu Matsumoto[5]

Abstract: The activities to notify users of IoT devices with inadequate security settings and/or malware-infection have become increasingly important. As a complement to the widely conducted notifications by ISPs, we have considered a notification channel in which users are notified via dedicated application installed on their PC or mobile devices. We have prepared a notification experiment using a security client distributed by a security project, WarpDrive. This paper reports the results of the actual notification experiment, in which we sent out notifications to WarpDrive users on possibly insecure network services that might become a target of cyber attacks. Among around 1000 active users, we identified 60 users who continuously have their ports open and expose their network services to the Internet. As a result of the experiment, 28(47%) of the notified users visited our notification page, and 25% of them remediated their situation by closing the ports, which is 3 times as many as the natural remediation. In the questionnaires to the notified users, 20(74%) of them said they connected their devices at home, 6(22%) at work, and 1(4%) elsewhere. Also, of the 20 users who connected their device at home, 10 of them answered that exposing the network service was not intentional. We believe these results can serve as a basis for improving security notifications to end users.

Keywords: IoT devices, security notification, dedicated apps

1. はじめに

近年，様々な機器がインターネットに接続されるようになり，この状況はモノのインターネット (IoT) と称されている．しかし，脆弱な設定のままインターネットに接続されている IoT 機器が存在しておりマルウェアに感染するケースが後を絶たない．このため，そのような設定に不備のある IoT 機器やマルウェア感染した機器を迅速に特定し, 機器のユーザに対してセキュリティ対策のための注意喚起や情報提供を行う活動の重要性が高まっている．

実際に，産業制御システムを対象にセキュリティ通知を行なった研究 [12] や，コンシューマ向けの機器を対象に注意喚起を行なった研究 [5] が存在する．日本国内においても，サイバー攻撃の対象になりやすい脆弱な機器の調査や，その機器の利用者への注意喚起が行われている [1], [6].

我々は論文 [14] において，ユーザ端末にインストールされた専用アプリケーションを通じて注意喚起を行うモデルに着目し，その実現例としてユーザ参加型のセキュリティプロジェクトである WarpDrive [7] における通知実験の枠組みとその効果測定方法を検討した．本報告では，当該モデルを用いて実際に通知実験を行い，その効果を測定する．具体的には，1000 人規模の WarpDrive ユーザに対して，サイバー攻撃の対象となり得る 23 種類のポートにスキャンを継続的に行い，定常的にポートが開放されている 60 人に WarpDrive の専用アプリであるタチコマセキュリティエージェント (タチコマ SA) を介して注意喚起を行い，以下の知見を得た.

- 注意喚起を行った 60 人のうち 47%にあたる 28 人が注意喚起の内容を記した専用 Web ページ (通知ページ) にアクセスしており，うち 20 人は注意喚起後 3 日以内にアクセスしていた.
- ポート開放の状態が時間の経過と共に改善するユーザの割合 (改善率) は，注意喚起を実施しない場合に 5 週間で約 7.5%であったのに対して，専用アプリによる注意喚起後は 5 週間で約 25 %と 3 倍以上となった.
- 注意喚起対象ユーザへのアンケートに回答した 27 人のうち，20 人 (74%) は自宅，6 人 (22%は勤務先，1 人 (4%) は外出先のインターネット環境を利用していると回答した. 自宅回線を利用する 20 人のうち，50%にあたる 10 人はポート開放は意図的でないと答えた.

このように専用アプリを用いた注意喚起の効果が確認できた. また，ユーザのインターネット接続環境やポート開放の意図などの情報が得られた. これらの結果は IoT 機器の安全な利用を促進するための注意喚起活動において重要な情報であると考えられる.

2. 関連研究

マルウェア感染した機器や脆弱性をもつシステムの管理者や所有者，製造者に対して注意喚起などの情報提供を行う際の効果を検証する研究が広く行われている.

これらの研究は, サーバやシステムの管理者, 機器の製造者等への注意喚起を想定している場合 ([2], [9], [10], [11], [12]) と，一般ユーザを対象にしている場合 ([1], [3], [4], [5], [6]) に大別される. 前者は一定の技術や知識を有している対象への注意喚起であるのに対して，後者は十分な技術や知識を必ずしも有していない一般ユーザが相手となるため，効果的な注意喚起を行うには特に様々な工夫が必要となる.

文献 [5] では，ISP が IoT 機器のマルウェア感染が疑われるユーザに対応を促すため，外部との通信が制限された Walled Garden と呼ばれる環境に感染ユーザを強制的に配置し，注意喚起用の Web ページに誘導することで注意喚起を行っている．また，日本国内において，マルウェア感染が疑われるユーザや容易に推測可能なパスワードが設定されているなど，マルウェア感染の恐れがある機器のユーザに対して注意喚起を行っている [1], [6]. しかし，これらの研究や活動は ISP を経由した注意喚起活動であり，一般に設備や作業のコストが高い上，我が国においては通信の秘密の観点からも実施の妥当性を十分に検討する必要がある．我々はこれまで ISP を経由する以外の方法で一般ユーザに注意喚起を行う方法として，専用クライアントを介した注意喚起モデルを検討している．さらに，その実現例としてサイバー攻撃の観測・検知・分析やユーザへの警告や助言を行う WarpDrive プロジェクト [7] において開発された，セキュリティクライアント「タチコマ・セキュリティ・エージェント [8]（以下，タチコマ SA)」を用いた注意喚起の枠組みを設計した [14]．本報告ではこの準備に基づき実際に注意喚起を実施した結果を報告する.

3. 専用エージェントを用いた注意喚起

はじめに，**図 1** に WarpDrive プロジェクトにおける注意喚起活動の全体図を示す.WarpDrive では, 専用のセキュリティエージェントであるタチコマ SA をユーザに配布しており, 実証実験実施期間中のアクティブユーザ数は PC 版で 700 人規模, モバイル版で 300 人規模となっている. これらのエージェントから得られる情報は WarpDrive 基

[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] 情報通信研究機構
National Institute of Information and Communications Technology
[3] 横浜国立大学先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University
[4] 株式会社 KDDI 総合研究所
KDDI Research, Inc.
[5] 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
Graduate School of Environment and Information Sciences, Yokohama National University / Institute of Advanced Sciences, Yokohama National University
[a)] murakami-hayato-nv@ynu.jp

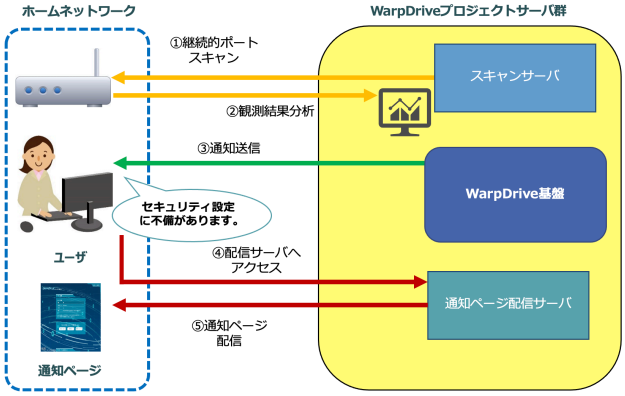


図 1: WarpDrive における注意喚起活動の全体図

盤に送信され蓄積される．WarpDrive 基盤はエージェントを介して各ユーザに個別のメッセージを送付する機能も有しており，この機能を利用して注意喚起を行う．

タチコマ SA を介した注意喚起の概要は以下の通りである.(1) タチコマ SA をインストールしているユーザに対しポートスキャンを継続的に行う (2) 各ユーザのポート開放状況の推移を分析し，セキュリティ不備の可能性があるユーザを通知対象ユーザとして選定する (3)WarpDrive 基盤からセキュリティ不備の可能性がある旨を記した通知ページを各ユーザに送付する. 通知ページは当該ユーザのネットワーク環境やポート開放の意図を確認するためにアンケート形式になっており，ユーザの回答に従い，タチコマ SA は必要な対策等をユーザに提示する．

3.1 ポートスキャンによるセキュリティ調査

WarpDrive 基盤は各ユーザが自身の端末にインストールしたタチコマ SA とやり取りを行うことで，定期的にユーザの端末のグローバル IP アドレスを取得している．さらにこれらのグローバル IP アドレスに対してポートスキャンを行い，IoT 機器のセキュリティ上の不備を調査する．具体的には，Telnet や Web 系のプロトコルをはじめとして，IoT 機器においてサイバー攻撃の対象となり得る 23 種類のポートを対象とする．対象ポートを**表 1** に示す．各ユーザについて最低 1 日に 1 回のスキャンを実行する．ただし，タチコマ SA がインストールされた機器のグローバル IP アドレスが変わる度にスキャンを再実行するため，1 日に複数回スキャンを実行する場合もある．一方，ユーザの端末が稼働していない場合には，グローバル IP アドレスを取得できないためスキャンは行わない．ユーザの端末へのスキャンは専用のスキャンサーバを用いて行っており，スキャン結果は全て当該サーバに保持される．

WarpDrive ユーザに対するポートスキャンは 2018 年 10 月より開始し，本報告執筆時も継続して実施している. **表 2** に 2021 年 4 月〜6 月の 3 ヶ月間におけるスキャン結果のうち，特に開放状態が散見された 8 つのポートに関して期

表 1: スキャン対象ポートと想定サービス名

調査対象ポート	想定サービス	調査対象ポート	想定サービス
21/tcp	FTP	5431/tcp	UPnP
22/tcp	SSH	49152/tcp	UPnP
23/tcp	telnet	52869/tcp	UPnP
2323/tcp	telnet	19/udp	chargen
23231/tcp	telnet	53/udp	DNS
53/tcp	DNS	123/udp	NTP
80/tcp	HTTP	1900/udp	SSDP
81/tcp	HTTP	5350/udp	NAT-PMP
8080/tcp	HTTP	5351/udp	NAT-PMP
443/tcp	HTTPS	5353/udp	DNS
445/tcp	SMB	11211/udp	memchached
5000/tcp	UPnP		

表 2: 2021 年 4 月〜6 月におけるスキャン結果

調査対象ポート	人数
21/tcp	28
22/tcp	74
23/tcp	25
80/tcp	160
8080/tcp	43
443/tcp	166
445/tcp	17
53/udp	7

間内に一度でもポート開放が確認されたユーザ数を記している.80, 443/tcp など Web 関係のポートや 22/tcp (SSH) が多く観測されている. 一方で Mirai などの IoT マルウェアに狙われることが多い 23/tcp (telnet) なども検出されている.4 章ではこれらのポートに関して注意喚起を行う．

3.2 通知対象ユーザの選定

タチコマ SA は持ち運びが容易なノート PC やスマートフォンにインストールされていることが多く，ユーザの外出時等には異なるネットワーク環境からインターネットに接続される場合がある. また，ルータなどのインターネット接続機器の買い替えやインターネットサービスプロバイダの変更等により，ポート開放状況が変化し得る. そのため，ポートスキャンの結果から継続的なポート開放状態が確認された場合にのみ，注意喚起を行う. 具体的には注意喚起実施前に 1 ヶ月間の通知対象選定期間を設け, 以下の条件に基づき選定を行う．

通知対象選定条件

- 1 ヶ月のうち最低 4 日以上ポート開放している (ただし，ポート開放が確認された期間が特定期間に連続している場合は, 6 日以上連続している場合のみ注意喚起対象とする)
- 選定期間の後半 2 週間で 1 日でも開放されている

上記条件を全て満たしているユーザを通知対象とする．

なお，上記の条件に加えて，サービスの特徴に応じて付加的な条件も適用した. 具体的には, Web サービス (80, 8080, 443/tcp) については明らかに公開を意図したコンテンツが確認できる場合 (例. 個人の Web サイトなど) は，通知対象から排除した.SSH 等のサービスについてもユーザが意図的に公開している可能性があるが，これらについては注意喚起を行った上で，公開の意図をユーザにアンケートで確認することとした.

3.3　ユーザへのセキュリティ通知の提示

WarpDrive 基盤 (以下, 基盤) から通知メッセージを受信するとタチコマ SA はアイコンの色を変更する等の方法でユーザに知らせる．PC 版のタチコマ SA の通知画面を**図 2**，モバイル版の通知画面を**図 3** に示す.

PC 版タチコマ SA における通知時の画面遷移：PC 版では Windows の通知領域やブラウザの拡張機能として画面右上に専用のアイコンが表示される（**図 2a** の右上の青色の丸が 3 つ三角に並んだもの）. 通知が機器に届くと, このアイコンが図 2a に示すように赤色に変化する．次にそのアイコンをクリックすると, **図 2b** に示すポップアップ画面が表示される．そして**図 2c** に示すように, ポップアップ画面の左下に通知メッセージが表示され, そのメッセージをクリックすると通知ページに遷移する.

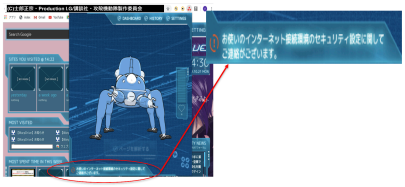
モバイル版タチコマ SA における通知時の画面遷移：モバイル版では画面中央に専用のキャラクターが表される（**図 3a**）. 通知が機器に届くと, そのキャラクターから吹き出し型のメッセージが表示される．次にそのキャラクターをタップすると, **図 3b** に示す画面が表示される．そしてその画面の「アンケートを開く」という部分をタップすると, **図 3c** の画面が表示され, その画面のお知らせの中の「お使いのインターネット...」という通知メッセージをタップすると, 通知ページに遷移する.

通知ページでは, ユーザの機器のポート開放状況についての詳細な情報と対策法に加え, ユーザのネットワーク環境やサービスの公開意図を確認するためのボタン選択形式のアンケートが表示される．通知ページの画面を**図 4** に示す. 画面の上部には機器の IP アドレス, プロバイダ情報と開放ポートが表示され, 下部でアンケートが表示される. 通知ページは通知ページ配信サーバ上でホスティングされており，その URL は通知対象ユーザ毎にユニークであるため，ユーザが通知ページにアクセスしたか否かをサーバ側から判定可能である．また, 通知ページにあるアンケートのボタンが押された際，ユーザ ID やページの URL，押したボタンの ID ，日時などを基盤側に送信する．これにより，各ユーザがどのようにアンケート回答を行なったのかをサーバ側で分析することが可能である.

ここで，**図 5** にユーザへのアンケートの内容とアンケートへの回答に応じた対策提示のフローを示す．アンケート

(a) アイコン

(b) ポップアップ画面



(c) 通知メッセージ

図 2: PC 版タチコマ SA のアイコンと画面遷移

(a) アイコン

(b) 途中画面

(c) 通知メッセージ

図 3: モバイル版タチコマ SA のアイコンと画面遷移

図 4: 通知ページ

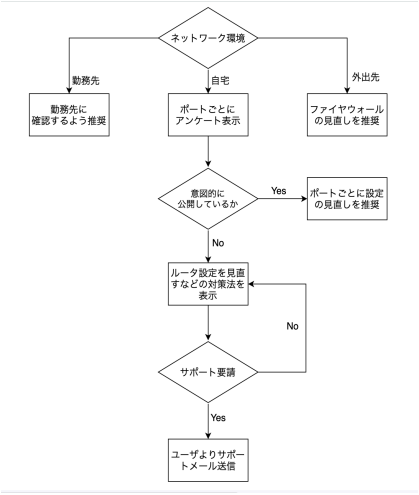


図 5: アンケートと対策提示フロー

の具体的な内容は以下の通りである.

ネットワーク環境に関するアンケート：通知対象ユーザがタチコマ SA をインストールした端末を接続しているネットワーク環境について以下の選択肢で確認を行う.

- 勤務先など：ネットワーク管理者とやり取りを行える可能性が高いことから，ポート開放が意図して行われているか管理者に問い合わせを行うよう推奨する文言を提示し，注意喚起を終了する.
- 外出先 (ホテル・カフェなど)：ネットワーク管理者とのやり取りは難しいため，ファイアウォール機能の有効化など自身で行える対策を推奨する文言を提示し，注意喚起を終了する.
- 自宅 (モバイル含む)：各ポートについて開放状況を確認する以下の追加アンケートを表示し，その回答に従い，対策を推奨する文言を提示する.

ポートの開閉状況に関するアンケート：ネットワーク環境に関するアンケートでユーザが「自宅（モバイルを含む)」を選択した場合にのみ追加で表示され，各開放ポートについて以下の選択式質問を提示する.

- 意図して公開：ユーザが該当ポートを意図的に開放していると判断し，適切な ID・パスワードの設定などサービスを公開するための対策の確認を促す文言を提示して当該ポートに関する注意喚起を終了する.
- 公開の意図はない：公開の意図がないにも関わらずポートが開放されている状態であるため，セキュリティ対策が必要と判断する．次に，自身で対策可能であるかを確認し，ユーザが自身で対策可能と回答した場合にはルータの設定変更や更新，該当ポートへのアクセス制限など，各ポートに関する一般的なセキュリティ対策をユーザに提示する．一方で，自身で対策ができないと回答した場合には，サポート窓口のメールアドレスを表示し，メールによるサポートを行う.
- わからない：公開の意図はない場合と同様.

表 3: 各実証実験の通知送付日, 対象機器, 対象ポート

	通知送付日	対象機器	調査対象ポート
実験 1	2019/10/30	PC	23/tcp
実験 2	2020/5/12	PC	21,22,23,445,80,8080,443/tcp
実験 3	2020/11/20	PC	21,22,23,445,80,8080,443/tcp,53/udp
実験 4	2021/2/19	モバイル	21,22,23,445,80,8080,443/tcp,53/udp

表 4: 各実証実験での通知人数とポートの内訳

開放ポート	実験 1	実験 2	実験 3	実験 4	計
21/tcp	0	6	0	2	8
22/tcp	0	9	2	3	14
23/tcp	8	5	1	2	16
445/tcp	0	1	1	0	2
80, 8080, 443/tcp	0	8	11	4	23
53/udp	0	0	3	0	3
21,22/tcp	0	1	0	0	1
22,445/tcp	0	2	0	0	2
計	8	32	18	11	-

4. 実証実験

前節で説明した仕組みを用いて，実際に WarpDrive ユーザへの注意喚起を計 4 回行った. 各実証実験の通知送付日と対象機器, 通知対象ポートを**表 3** に示す. 4 回の実証実験において, アクティブユーザ約 1000 人 (PC 版約 700 人, モバイル版約 300 人) のうち, 計 60 人の通知対象が存在した. なお，9 人のユーザは複数の実験で通知対象となっている. 各回ごとの通知人数の内訳と開放が確認されたポートを**表 4** に示す.

実証実験 1 における通知ページの差異について　実証実験 1 ではタチコマ SA の配布開始から注意喚起実験開始日まで 1 年以上経過していた. 実証実験 1 の開始時点でセキュリティ通知はユーザにとって事前告知もない急な出来事であり, ユーザの不安を煽ることになる可能性があったため，セキュリティ通知に関する説明を含むランディングページを最初に表示し，次に通知ページ (メインページ) を提示するようにした. これらの画像をそれぞれ**図 6**, **図 7** に示す. 通知ページ (メインページ) のデザインはその後の実証実験 2 以降とは若干異なっているが，アンケートの質問事項や提示する対策の文言は同様である.

4.1 実験結果と考察

4.1.1 注意喚起効果

図 8 に注意喚起後に通知ページにアクセスを行ったユーザ数の時間推移を示す. 注意喚起を行った 60 人のユーザのうち，47%にあたる 28 人が通知ページにアクセスを行っている. また，そのうち 20 人は注意喚起後 3 日間のうちにアクセスを行っている. このことからタチコマ SA によるセ

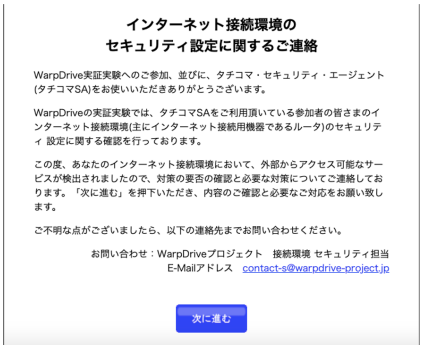


図 6: ランディングページ

図 7: 通知ページ (メインページ)

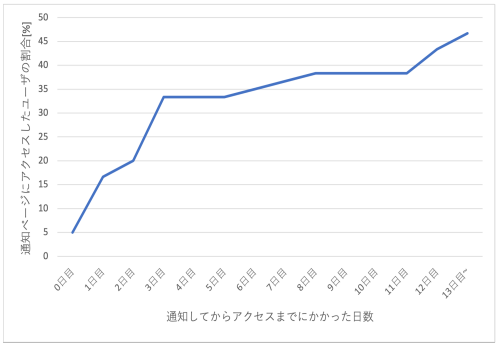


図 8: 注意喚起後の通知ページへのアクセス人数の推移

キュリティ通知には一定の注意喚起効果があると考えられる. 一方, 残りの 8 人については, アクセスまでに 1〜2 週間かかっており, GUI デザインの改善により注意喚起効果を改善できる余地があると思われる. なお，PC 版とモバイル版では通知ページへアクセスしたユーザの割合はそれぞれ 47%と 45%であり，大きな差異は見られなかった. モバイル版の GUI デザインは PC 版の注意喚起実験結果をふまえて，メッセージ受信時の視認性を重視したにも関わらず，その効果は明確に確認できなかった.

4.1.2 セキュリティ改善効果

タチコマ SA による注意喚起により，ポート開放状況が改善し，セキュリティ向上につながったかを検証する. そのため，注意喚起を行なった場合のポート開放状態と, 注意喚起を行わなかった場合の状態とを比較する.

ある基準期間 T において定常的にポート開放状態にあるユーザ集合を U とする. 次に期間 T の最後から i 週が経過した時点で，U 内のユーザのうち，ポート開放状態が改善したユーザの集合を F_i とする. このとき，F_i/U を i 週経過時の改善率と呼ぶこととする. なお，注意喚起を実施していない期間の改善率を特に自然改善率と呼ぶ. **図 9** の青の破線は，注意喚起を実施していない期間である 2021 年 4 月の 1 か月間を T とした場合の自然改善率の推移を示したものである. 図より，$i = 5$ 週で自然改善率は約 7.5%となっている. 自然改善の理由としては，ルータなどの機器の買い替えや設定変更，ファームウェア更新が考えられる. 一方，図 9 のオレンジの実線は，4 回の注意喚起実験における改善率の平均値であり，$i = 5$ 週で約 25%となっている. 自然改善率と比べ 3 倍以上の改善率となっており，明らかに注意喚起の効果が読み取れる. また，注意喚起時の改善率は注意喚起後一週間で急増し，その後の増加傾向は自然改善率のそれと大きく変わらないことから，注意喚起の効果のほとんどは注意喚起後の 1 週間に現れているといえる.

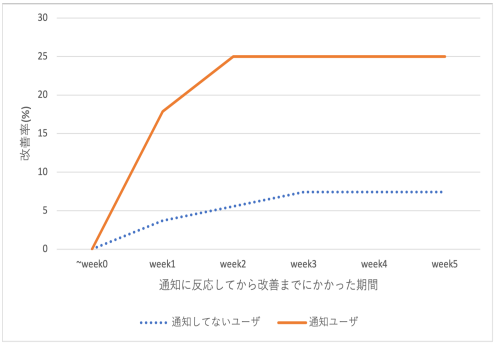


図 9: ポート改善率の推移

4.1.3 ユーザのインターネット接続環境とポート開放の意図

次に，ポート開放状態にあるユーザのインターネット接続環境の実態とポート開放の意図に関するアンケートの結果を分析する. アンケートに対するユーザの回答を**表 5** に示す. 注意喚起を行った 60 人のユーザのうち，27 人から回答が得られた.27 人の回答者のうち，20 人 (74%) は自宅にてインターネット接続していると回答し，6 人 (22%) は勤務先，1 人 (4%) は外出先と回答している. 勤務先や外出先で定常的にタチコマ SA がインストールされた PC やスマートフォン端末を利用するユーザは限られると思われるため，この結果と整合しているといえる.

次に自宅から接続していると答えたユーザ 20 人のうち，ポート開放の意図はなかったと回答したユーザは 10 人 (50%) だった. しかし，意図的に開放していると回答したユーザの中にはインターネットに公開することが一般的ではなく攻撃を受けるリスクの高い 23/tcp (Telnet) や 445/tcp (ファイル共有など) を開放しているユーザも含まれており，意図的であってもセキュリティ上のリスクを伝

表 5: アンケートへのユーザの回答

	21	22	23	445	Web	53(udp)	計
自宅意図なし	0	5(2) ＊	1(1)	1(1)	3(1)	0	10(5)
自宅意図的	4	5(1)	1	2(1)	1	1	14(2)
勤務先	0	4	1	0	2	0	7
外出先	0	0	1	0	0	0	1
無回答	0	0	0	0	1	0	1
計	4	14(3)	4(1)	3(2)	7(1)	1	-

＊ () 内の数字は改善したユーザ数

えることには一定の意義があると思われる. 逆に，意図的に公開することも想定される 22/tcp (SSH) や Web 関連ポート (80, 8080, 443/tcp) についてはそれぞれ 5 人 (25%), 3 人 (15%) が意図的ではなかったと回答しており，これらのポートについても注意喚起を行い，公開の意図や妥当性を確認することが重要と考えられる.

4.1.4 ユーザサポート事例

実証実験 1,2,3 においてそれぞれ 1 人ずつの異なるユーザからサポート要請を受けた. サポート要請の件数はこの 3 件のみであり，多くのユーザはサポートなしに注意喚起への対応を行っていたことが分かる.

実証実験 1 でサポート要請を行ったユーザは最初にプロジェクトチームが送信したサポートメールを不審に思い，WarpDrive 公式サイトの問い合わせフォームから確認を行っていた. サポートメールの送信元アドレスが WarpDrive のドメインではなく，研究を実施した大学のアドレスであったことなどが理由として考えられる. なお，当該ユーザに対しては継続的なサポート対応を行い，注意喚起後，約 1 年を費やした後にポート開放状態の改善を確認した. 当該ユーザが使用するルータが一般家庭用ルータに比べて高機能であり，ルータメーカを含めて技術的に高度なサポートが必要であったことが長期化した理由である. なお，このような事例は他に例がなく，特異なものと考えられる.

実証実験 2 では，あるユーザからサポート要請を受けたものの，サポートを実施する前にポート開放状況が改善していることを確認した. メールにて当該ユーザに確認したところ，ルータを買い替えたという旨の回答が得られた.

実証実験 3 においてあるユーザからサポート要請を受けたものの，サポートメールに対してその後回答が得られなかった. しかし, 連絡は途絶えたものの, 約 2 ヶ月後にポート開放状態の改善が確認された.

このように事例は少ないものの，3 件のサポート事例はいずれも最終的にセキュリティ改善につながっている. サポート要請を行うユーザはセキュリティ改善に前向きであり，丁寧に対応することで改善が期待できるといえる.

5. 議論

ユーザ集合の特性　今回の実証実験により，タチコマ SA を介した注意喚起に一定のセキュリティ改善効果が確認できた. 一方でこの効果については以下の観点で慎重な検証が必要である. タチコマ SA をインストールしている WarpDrive ユーザはそもそもセキュリティに対して関心が高いと予想される. 実際，文献 [13] において実施したアンケートでは，タチコマ SA をインストールした理由として “プロジェクトへ貢献したいから”, “ブラウジングが安全になるから” と回答したユーザがそれぞれ 44.9 %と 32.1 %存在した. 一方で，セキュリティへの関心が低いユーザ群に対しては同等の効果が得られない恐れがある. また，そもそもタチコマ SA のようなセキュリティエージェントをインストールしないユーザも多いことから，今回のようなセキュリティ通知は，ISP による注意喚起などと補完的に実施すべきものと考えられる.

専用アプリ等の開発・運用・保守コスト　WarpDrive では，プロジェクトの立ち上げと共に専用のエージェントとしてタチコマ SA や WarpDrive 基盤を開発し，タチコマ SA を広く一般へ配布したが，その開発，運用，保守，配布促進には大きなコストが掛かっている. そのため，これらのコストを含めて総合的な観点で注意喚起活動の費用対効果を議論すべきである. 通知用アプリの開発や運用のコストを抑えるために，今後，既存のアプリやサービスとの連携についても検討したい.

ポート開放状況の詳細分析　今回の注意喚起活動およびその効果の分析では，個々の事例におけるポート開放の理由や原因の分析を行っていない. 簡易的な調査では，ポートスキャン時に得られた応答からユーザが使用する機器やサービスを推定可能と思われるケースが数十件程度含まれていた. このような機器の種別やサービスの内容に沿った注意喚起や対応方法の提示を行うことで，注意喚起の効果改善が期待される.

6. まとめと今後の課題

WarpDrive プロジェクトが開発、配布するタチコマ SA を介して機器の所有者にセキュリティ対策のための注意喚起や情報提供を行う通知実験を行い，その効果を測定した. 合計 4 回の実験で計 60 人に通知を行い, そのうち 28 人から反応を得られた. また注意喚起を行わない場合に比べて 5 週間で 3 倍以上のポート開放状況の改善が確認された. 今後は他のアプリや広域スキャンサービスとの連携による実証実験規模の拡大により，注意喚起効果のより詳細な評価を行いたい.

謝辞　本研究成果の一部は, 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．本研究は総務省の「電波資源拡大のための研究開発 (JPJ000254)」における委託研究「電波の有効利用のための IoT マルウェア無害化／無機能化技術等に関する研究開発」によって実施した成果を含む.

参考文献

[1] 総務省，“IoT 機器に関する脆弱性調査等の実施結果の公表，”https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000154.html，last visited 2021/08/17.

[2] F. Li, Z. Durumeric, J. Czyz, M. Karami, M. Bailey, D. McCoy, S. Savage, and V. Paxson.“You’ve got vulnerability: Exploring effective vulnerability notifications.”, 25th USENIX Security Symposium.

[3] 総務省，経済産業省，“サイバークリーンセンター（CCC）｜サイバークリーンセンターについて，”https://www.telecom-isac.jp/ccc/，last visited 2019/02/01.

[4] ICT-ISAC，“ACTIVE(マルウェア対策支援)，”https://www.ict-isac.jp/active/, last visited 2019/02/01.

[5] O. Cetin, C. Gañán, L. Altena, D. Inoue, T. Kasama, K. Tamiya, Y. Tie, K. Yoshioka, M. van Eeten, ”Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai,” The Network and Distributed System Security Symposium (NDSS 2019), 2019.

[6] 総務省，“NOTICE(National Operation Towards IoT Clean Environment)，”https://notice.go.jp/, last visited 2021/08/17.

[7] KDDI 総合研究所，セキュアブレイン，横浜国立大学，神戸大学，構造計画研究所，岡山大学，金沢大学，NICT，“WarpDrive，”https://warpdrive-project.jp/，last visited 2019/02/01.

[8] KDDI 総合研究所，セキュアブレイン，横浜国立大学，神戸大学，構造計画研究所，岡山大学，金沢大学，NICT，“WarpDrive について，”https://warpdrive-project.jp/about.html, last visited 2019/02/01.

[9] Cetin, Orcun; Hernandez Ganan, Carlos; Korczynski, Maciej; van Eeten, Michel，“Make notifications great again: learning how to notify in the age of large-scale vulnerability scanning”, WEIS 2017.

[10] Ben Stock, Giancarlo Pellegrino, Christian Rossow, Martin Johns, and Michael Backes.“Hey, you have a problem: On the feasibility of large-scale web vulnerability notification.”, 25th USENIX Security Symposium.

[11] Jia Zhang, Haixin Duan, Wu Liu, Xingkun Ya,“How to Notify a Vulnerability to the Right Person? Case Study: In an ISP Scope”, IEEE 2017.

[12] Stock, B., Pellegrino, G., Li, F., Backes, M., & Rossow, C.“Didn’t you hear me? — towards more successful web vulnerability notifications.”, The Network and Distributed System Security Symposium (NDSS 2018), 2018.

[13] Akira YAMADA, Yukiko SAWAYA, Takashi MATSUNAKA, Shoma TANAKA, and Ayumu KUBOTA,“A User Participation Type Web Security Platform and Its Real World Evaluation”, ICSS 2018.

[14] 西田慎, 保泉拓哉, 内田佳介, 藤田彬, 吉岡克成, 松本勉, ”IoT 機器のユーザへの専用クライアントを介したセキュリティ通知実験の検討”, ICSS 2019.