情報処理学会論文誌 Vol.61 No.3 695–706 (Mar. 2020)

特定のIoT機器のWebUIを狙ったサイバー攻撃の分析

藤田 彬[1,a)] 江澤 優太[2] 田宮 和樹[2] 中山 颯[2] 鉄 穎[2] 吉岡 克成[1,3] 松本 勉[1,3]

受付日 2019年6月17日, 採録日 2019年11月29日

概要：IoT 機器には機器の管理や操作のための WebUI を持ちインターネットに接続可能な機器が多数存在する．それらの機器のなかには，脆弱性や認証の問題を抱えたままインターネット上に公開されているものが存在する．本研究では IoT 機器の実機を用いることでハニーポットを構築し，WebUI に対する攻撃の観測を行う．観測結果には Web サイト公開用の通常の Web サーバに対する攻撃も観測されるため，観測対象機器向けの攻撃を判別する指標を示す．次に，自動化されている攻撃の特徴を示し，IoT 機器向けの攻撃を分析する手法を提案する．提案手法をもとに検証実験を行い，特定の IoT 機器向けの攻撃が自動化されている実態を示す．

An Analysis of Cyber Attacks Targeting WebUI of Specific IoT Devices

Akira Fujita[1,a)] Ezawa Yuta[2] Kazuki Tamiya[2] Sou Nakayama[2] Ying Tie[2]
Katsunari Yoshioka[1,3] Tsutomu Matsumoto[1,3]

Received: June 17, 2019, Accepted: November 29, 2019

Abstract: There are many IoT devices that have WebUI for device management and operation. Some of them are open to the Internet with vulnerability and weak credentials. In this paper, we propose a honeypot to monitor attacks against these WebUIs by using bare-metal devices. The observation results contain attacks against regular Web servers, so we show how to identify attacks targeting particular device. Next, we show some of the attacks are automatically conducted by using some tools or malware. Our observation and analysis shows that attacks on WebUI of IoT devices are widely conducted with a certain degree of automation.

1. はじめに

近年，様々なもの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．IoT を構成する様々な機器（以下，IoT 機器）のなかには，Web ブラウザを介して自機器の遠隔操作や設定を行うことを目的としたユーザインタフェース（以下，WebUI）を有するものが多数存在する．

IoT 機器はキーボード，ボタン，ディスプレイ等の入出力デバイスが貧弱であるため，機器の設定，操作，状態確認等を，WebUI を介して行う場合が多い．多くの IoT 機器で WebUI を介してのネットワーク設定，時刻設定の確認や変更が可能であり，ファームウェア更新等も可能である．また，機器特有の操作も多種存在し，プリンタのインク残量の確認，IP カメラの映像へのアクセス，ズームや首振り等の操作，放送受信機では映像の取得や録画予約等に利用されている．

これら IoT 機器の WebUI の一部で，脆弱性や設定の不備が発見された事例が報告されている．ルータの設定ファイルを遠隔から WebUI を介して取得可能である事例 [1] や，バッファオーバフローによりマルウェア感染する事

[1] 横浜国立大学先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[2] 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, Yokohama, Kanagawa 240–8501, Japan
[3] 横浜国立大学大学院環境情報研究院
Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[a)] fujita@ynu.ac.jp

例 [2] 等，WebUI に起因した脆弱性を持つ機器が多数報告されている．また，認証過程を経ずに，もしくはマニュアルに記載のデフォルトのパスワードで管理・設定画面にアクセス可能な IP カメラやルータ等，初期状態の設定に不備のある機器が多数発見されている [3], [4], [5], [6], [7]．また，それらの機器が一般家庭ではなく，インフラ設備等の国民生活上重要な施設に設置されていた事例も報告されている [8]．このような IoT 機器の WebUI が，実際に攻撃を受けるか否か，また攻撃を受けたとしてどのような攻撃であるか，詳細を観測して攻撃に対する対策を検討する必要がある．

インターネットからの攻撃を観測する際には，囮となるシステム（以下，ハニーポット）を設置して同システムの送受信パケットを分析する手法が用いられる．特に，ハニーポットを用いて IoT 機器への攻撃を観測する研究は，これまでにも多数行われている [9], [10], [11], [12], [13], [14], [15], [16]．しかしながら，IoT 機器の WebUI に対する攻撃の有無および攻撃手順の詳細に関する調査は十分に行われていない．

Web サーバを模したハニーポット [17], [18] や Web アプリケーションを模したハニーポット [19], [20]，Web アプリケーションフレームワークを模したハニーポット [21] を用いて，Web サービスの脆弱性を狙った攻撃を観測する研究についても，多くの先行研究が存在する [22], [23], [24], [25], [26], [27]．しかしながら，IoT 機器の WebUI はインタフェースの内容や機能が機器の種類に応じて様々であるうえ，インタフェースの操作が複雑であり，また操作に対する Web サーバサイドからの応答も多様である．そのため，Web サービスにおける汎用的な応答のみを返すような従来の Web サーバハニーポットでは，IoT 機器で想定されるような WebUI 内のボタンや入力フォーム等の各種オブジェクトの操作も含めた攻撃の詳細を観測することは難しい．

また，観測される攻撃には，実在する特定の機器の WebUI を狙った攻撃が含まれる可能性がある．それらの攻撃を観測するためには，対応する機器の実際の WebUI に可能な限り近い機能およびデザインを有したハニーポットが必要となる．これらのことから，IoT 機器の WebUI に対する攻撃の観測には，実際の機器（以下，実機）を用いたハニーポットを使用することが望ましいといえる．

本研究では，IP カメラ 2 機種，ルータ 3 機種，ポケットルータ 2 機種，プリンタ 1 機種，放送受信機 1 機種の計 9 機種の実機をハニーポットとして用い，攻撃の観測を行う．ハニーポットが観測するアクセスには，各機器を狙った攻撃だけでなく，一般の Web サイトを狙う攻撃も含まれるため，HTTP リクエストのパスに着目して各機器に特化した攻撃の判定を行う．また，JavaScript ファイルや CSS ファイル，PNG，JPG 等の画像ファイルを取得するか，同種のアクセスパターンが複数の観測点において観測されるか，といった観点で攻撃がマルウェアや攻撃ツールにより自動化されているかを判断する．

9 機種のそれぞれに 10IP アドレスを割り当て（計 90IP アドレス），それぞれ約 80 日～250 日に及ぶ観測を行ったところ，9 種類の機器のうち 7 種類の機器に対して，それぞれの機器に特化したものととらえられる攻撃が観測された．具体的には，IP カメラの設定ファイルを取得する攻撃，ルータの DNS 設定を変更する攻撃等が観測された．これらの攻撃はいずれも，攻撃対象となる機器の WebUI がもつ機能や構成，機能設定時に指定する必要のあるパラメータ名のような詳細を事前に認識していない限りは成立しないものと考えられる．さらにこれらの攻撃は，観測状況から判定したところ，自動化されたアクセスであった．このことから，IoT 機器の WebUI を狙った攻撃は，個人の攻撃者による試行段階ではなく，ツールやマルウェアによる自動化が行われる段階に入っていると考えられる．一方，人間の攻撃者による攻撃としては，ルータに対して DDNS 設定や VPN 設定を変更することでバックドアを確保したうえで，機器のファームウェアを更新し，脆弱性を修正することで当該機器を独占して踏み台化することを狙ったと考えられる攻撃が観測された．

以下では，2 章で提案手法について述べる．3 章で検証実験について，4 章で観測結果に関する考察を行う．5 章で関連研究について述べ，6 章でまとめと今後の課題を述べる．

2. 提案手法

2.1 ハニーポットの構成

様々な IoT 機器の実機を用い，IoT 機器の WebUI をターゲットとした攻撃を観測するハニーポットを提案する．**図 1** に本研究において提案するハニーポットの構成を示す．図 1 における実線は通信の流れを表す．

各観測点では，プロキシスクリプトが動作しており，80/tcp ポートおよび 8080/tcp ポートのみを開放している．各プロキシスクリプトは，受け取った通信を実機制御マシンへ転送する．実機制御マシンでは，各観測点に対応する IoT 機器の実機へ通信を転送する．IoT 機器の実機は，自機に対する通信への応答を，実機制御マシンを介してプロキシスクリプトに転送する．実機の応答を各観測点のプロキシスクリプトへ転送することで，攻撃者からは各観測点で IoT 機器が動作しているように見える．また，このような構成とすることで，1 台の実機につき複数の IP アドレスで通信を観測できるため，攻撃の観測範囲を拡張できる．

観測される通信には，IoT 機器の脆弱性を狙い，マルウェア感染や機器を乗っとるためのもの等，機器や外部に対して深刻な被害を与えるものも存在する．外部に被害が及ぶことを未然に防ぐため，実機から外部に向けて新たにセッション確立を試みる通信を通信制御部において制限す

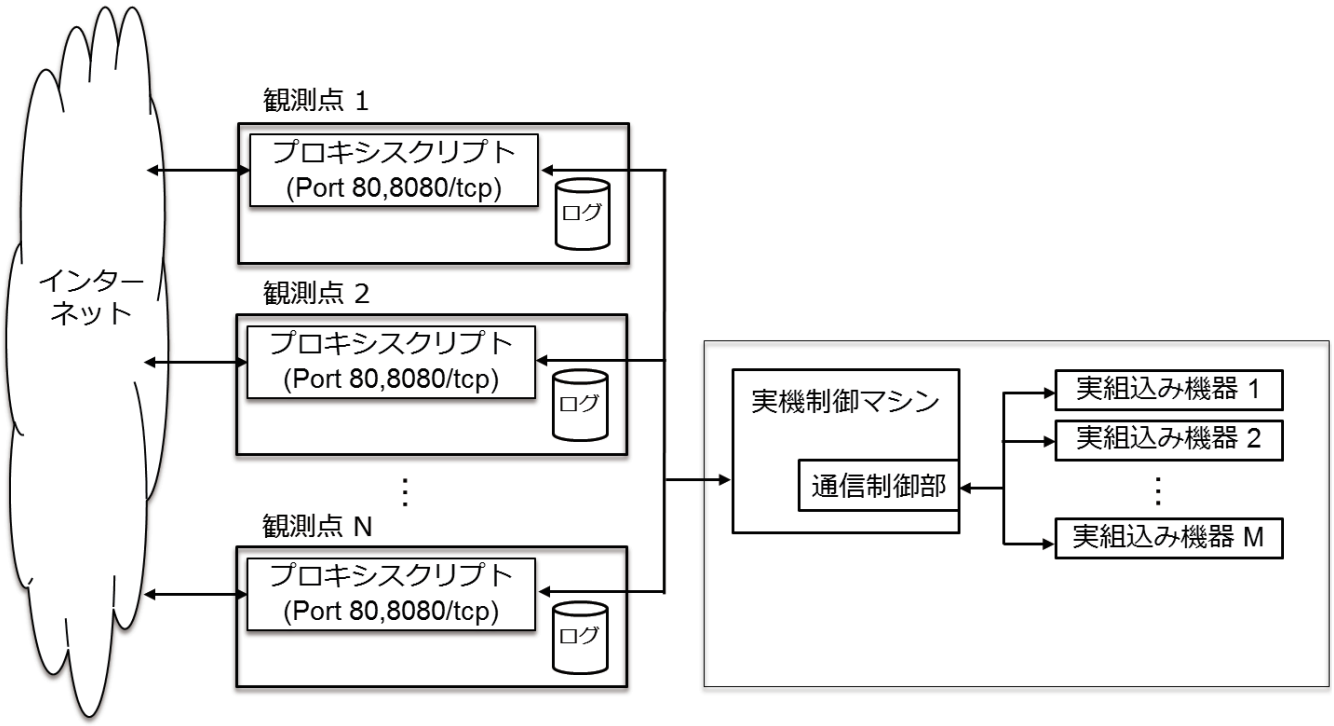


図 1 ハニーポットの構成
Fig. 1 Structure of honeypot.

る．通信制御部には iptables モジュールを実装する．当該モジュールにおいては，観測点の 80/tcp および 8080/tcp に届くインバウンド通信を，対応する実機の Web サービスのデフォルトポートに転送する．アウトバウンド通信については，実機側からセッションを張る試行をすべて遮断する制御を行う．通信制御部にはスイッチングハブを介して 9 機種の IoT 機器の実機がつながっている．実機間でのマルウェア感染の拡大を防ぐため，スイッチングハブに接続された機器間で発生する通信を遮断する設定をスイッチングハブに施す．

また，観測に用いる IoT 機器は侵入によりマルウェアに感染する可能性があるため，機器を初期状態に戻すことを目的として，定期的にシャットダウンおよび再起動を実施する．文献 [28] において，IoT 機器を再起動することでマルウェアが駆除されることが示されていることから，定期的な機器のシャットダウンおよび再起動の実行は有効といえる．なお，ファームウェアアップデート等，機器設定を工場出荷時の状態に戻す操作によっても状態を復元できないようなリクエストについては，実機に転送しないように設定する．これらの処置はハニーポットを安定的に運用するための処置であるが，定期的な自動処理として実施することで保守上のコストを低減する狙いがある．

これらの構成により，当該ハニーポットでは，80/tcp および 8080/tcp を対象とした HTTP リクエストおよびポートスキャン試行を検出できる．観測可能な HTTP リクエストには，各実機への正規リクエスト以外の一般的な Web サーバの脆弱性を狙った HTTP リクエストを含む．受信したリクエストが各実機の Web サービスにおいて正規のリクエストと見なされる場合，当該リクエストに対応するレスポンスデータを返信する．このため，攻撃者が正規のリクエストを送信し続ける限り，攻撃者の挙動を観測することができる．本研究のハニーポットは，観測対象を Web サービスへの通信に限ったうえで，低い保守コストでありながらも高対話型で，多種の機器への攻撃を同時観測するという点に特徴を持つハニーポットといえる．

2.2 特定機器向けの攻撃の判定方法

機器において観測される通信には，各機器に特化した攻撃だけでなく通常の Web サーバに対する攻撃も非常に多く観測される．一方，特定の機器向けの攻撃では各機器に特徴のあるパスをリクエストするといった特徴がある．これらに着目し，観測対象機器向けの攻撃を抽出する．

IoT 機器の WebUI では，ユーザ認証の方式として，主にベーシック認証，ダイジェスト認証とフォーム認証の 3 種類の認証方式が用いられる．

ベーシック認証 HTTP リクエストヘッダの Authorization フィールドに，ID とパスワードの組みをコロン (:) でつなぎ，Base64 方式でエンコードして送信し，認証を行う．HTTP で定義された認証方式である．

ダイジェスト認証 ベーシック認証では防げなかった盗聴や改竄を防ぐために考案された認証方法で，ID とパスワードの MD5 ハッシュ値をサーバに送信することで

認証を行う．HTTP で定義された認証方式である．

フォーム認証 Javascript 等で認証用のフォームを用意する方式．認証フォームや送信するリクエストは個々の WebUI の実装により異なる．HTTP で定義された認証方式ではない．

本研究では，これら 3 種の認証方式を備えた WebUI，および認証過程のない WebUI を備えた IoT 機器のハニーポットにより攻撃の観測を行う．以下では，認証方式の種別に，ハニーポットで観測されるアクセスを当該機器向けの攻撃と判定する方法について説明する．

ベーシック認証およびダイジェスト認証の攻撃判定方法 ハニーポットの WebUI へのログインに用いる ID およびパスワードを初期値から変更しないため，アクセスが当該機器を狙う攻撃であった場合，認証を突破することが想定される．認証を突破した後，各機器に固有のパスにリクエストを送った場合，このアクセスを当該機器を狙った攻撃と判定する．

フォーム認証の攻撃判定方法 フォーム認証は機器によって独自に実装されているため，これらの機器にログインするには各機器に対応した通信を行う必要がある．そのため，ログインに成功した通信には観測対象機器を狙う攻撃と判定する．

認証のない機器の攻撃判定方法 認証のない機器においては，観測したリクエストのパスが当該機器に固有のパスである場合に，このアクセスを当該機器を狙った攻撃と判定する．

2.3 自動化されたアクセスの判定方法

観測されたアクセスのうち，以下の条件 1 もしくは条件 2 に合致するアクセスを，ツールやマルウェア等により自動化されたアクセスと判定する．

条件 1：非ブラウザアクセス 事前に，ブラウザにより各機器の WebUI の各ファイルパスにアクセスし，要求したファイルに付随して JavaScript ファイル，CSS ファイル，PNG や JPG 等の画像ファイルが自動的に取得されるか否かを調べる．そのうえで，ブラウザによるアクセスとは異なり，特定のファイルのみを要求するアクセスを検出し，これを自動化されたアクセスと判定する．ツールやマルウェアによる特定機器を狙った攻撃は，フルブラウザによるアクセスと異なり，効率化のため WebUI の特定のファイルに対して行われるという特徴がある．このことから，当該条件を設ける．

条件 2：同時並列アクセス 当該 IP アドレスからの通信に関して，ある一定期間に一定数以上のハニーポットに対して同一のリクエストラインの HTTP リクエストが観測された場合，これを自動化されたアクセスと判定する．ツールやマルウェアは，効率的に攻撃を展開するために，同時に複数の IP アドレスに対して同じもしくは類似した特徴を持ったアクセスを試みる特徴がある．このことから，当該条件を設ける．

3. 検証実験

3.1 実験方法

提案手法により，IoT 機器の WebUI に対する攻撃の観測を行う．検証実験では 9 機種各 1 機の実機を用いたハニーポットを構築し，**表 1** に示す観測期間で実験を行った．9 機の実機それぞれにつき，各 10IP アドレス分の観測点を設定した．各観測点の IP アドレスは，すべて日本国内の単一の組織が管理する連続した IP アドレスである．

各観測点の 80/tcp および 8080/tcp に届いた通信を実機の 80/tcp に転送するよう設定した．80/tcp および 8080/tcp のほか，81/tcp 等の TCP ポートについても HTTP サービスが稼働している事例もみられるが，他のポートと比べてサービス稼働ポートとして選択されることが多い 80/tcp および 8080/tcp ポートを選び，観測対象とした．

ファイアウォールが存在するルータではファイアウォールをオフに設定し，外部から WebUI にアクセスできるように設定した．また，認証がある機器については機器の認証パスワードを初期状態で設定されているものから変更せずに実験を行った．

自動化されたアクセスを判定する方法のうち 2.3 節で述べた同時並列アクセスの判定については，ハニーポットが動作する 10IP アドレスのうち，1 分以内に 9IP アドレス以上に対して特定の IP アドレスから同種のリクエストが届いた場合，自動化されたアクセスと判定した．

なお，2.1 節で述べた機器の定期的なシャットダウンおよび再起動や，ファームウェア更新処理のブロックについては，本検証実験では実装していない．

3.2 実験結果

ハニーポットで観測された HTTP リクエストの送信ホスト数，ログイン試行を行ったホスト数，認証に成功したホスト数をそれぞれ**表 2** に示す．ルータ E とモバイルルータ G の観測結果において，ログイン試行ホスト数より特定機器を狙うリクエストを送信したホスト数が多いが，これは認証成功時の HTTPcookie を用いて別のホストからのアクセスが行われたためである．なお，以降において実際のリクエストや IP アドレスを示す際には，文字列の一部を文字「x」によりマスキングして示す．リクエストをマスキングする箇所については，当該箇所が機器固有のリクエストパスの一部であることを示す．

3.2.1 IP カメラ A

8,695 ホストからのリクエストを受信し，そのうち 26 ホストがログインに成功した．そのうち，25 ホストは当該機器特有のファイルを要求するリクエストを送信した．具体的には，これら 25 ホストのすべてが，当該機器が撮影中

表 1 実験概要およびハニーポットの設定
Table 1 Summary of experiment and honeypot setting.

機器名	メーカ国/地域	認証方法	ID/Password	観測期間	観測日数
IP カメラ A	日本	ベーシック認証 ダイジェスト認証	admin/12345	2016/12/16 – 2017/8/16	244 日
IP カメラ B	台湾	ベーシック認証	admin/(null)	2016/11/30 – 2017/8/16	260 日
ルータ C	台湾	ベーシック認証	admin/admin	2016/12/16 – 2017/3/8 2017/4/12 – 8/16	226 日
ルータ D	台湾	ベーシック認証	admin/admin	2016/12/16 – 2017/2/5 2017/2/23 – 3/3, 2017/4/12 – 5/3	83 日
ルータ E	台湾	フォーム認証	admin/admin	2016/12/16 – 2017/1/27 2017/2/22 – 3/7 2017/4/12 – 7/17	154 日
モバイルルータ F	日本	フォーム認証	admin/admin	2016/11/30 2016/12/5 – 2017/3/1	88 日
モバイルルータ G	アメリカ	フォーム認証	admin/(null)	2016/12/16 – 2017/8/16	244 日
プリンタ H	アメリカ	認証なし	(null)	2016/11/30 – 2017/3/1 2017/6/24 – 8/16	146 日
TV 放送受信機 I	ドイツ	認証なし	(null)	2016/12/9 – 2017/2/11 2017/2/22 – 3/1, 2017/6/24 – 7/26	106 日

表 2 実験結果の概要
Table 2 Result of experiment.

機器名	HTTP リクエストの送信ホスト数 [1]	ログイン試行ホスト数	ログイン成功ホスト数	特定機器を狙うリクエストを送信したホスト数
IP カメラ A	8,695 (1,353)	222	26	25
IP カメラ B	10,426 (1,540)	239	19	12
ルータ C	6,661 (1,773)	298	103	79
ルータ D	3,359 (1,489)	105	51	38
ルータ E	5,469 (1,488)	8	8	11
モバイルルータ F	2,769 (291)	0	0	0
モバイルルータ G	8,724 (1,391)	36	6	12
プリンタ H	3,876 (748)	(null)	(null)	0
TV 放送受信機 I	3,299 (881)	(null)	(null)	17

[1] 括弧内の数値は，HTTP リクエストの送信ホストのうち 2.3 節に示す方法により自動化されたアクセスを行ったと判定されたホストの数

の映像へアクセスしていた．このことから，認証を突破したうえでカメラの映像を閲覧する攻撃が存在することが明らかとなった．一方，当該機器の WebUI には機器設定を変更するページが存在するが，この画面にアクセスするホストは存在しなかった．しかしながら，機器の WebUI の表示言語については，他の設定と異なり WebUI のトップページから変更可能であり，一部の攻撃者については言語設定を機器のデフォルト設定である日本語から英語や中国語に変更する挙動が観測された．このことは，攻撃者がブラウザを用いて手動で機器にアクセスし内容を確認している可能性があることを示唆している．

3.2.2 IP カメラ B

10,426 ホストからのリクエストを受信し，そのうち 19 ホストがログインに成功した．そのうち 11 ホストはログイン後に映像にアクセスせずに，**図 2** に示すリクエスト群を図示した順番のとおりに送信し，カメラの Wi-Fi 接続情報，カメラ周辺の Wi-Fi アクセスポイントのスキャン，カメラの DDNS や PPPoE の設定情報の取得を行っていた．この攻撃は，フルブラウザによるアクセスと異なる画像ファイルの取得を行わないため，自動化されていると思われる．一方，映像を取得したホストは，IP カメラ A と異なりわずかに 1 ホストが観測されるのみであった．

```
GET /
GET /setup_xxxx_2.htm
GET /cgi-bin/xxxx_xxxx.cgi?rescan=0
GET /cgi-bin/xxxx_xxxx.cgi?rescan=1
GET /status_info.htm
GET /logout.htm
```

図 2 IP カメラ B への特徴的なアクセスの流れ
Fig. 2 Example of targetted HTTP request for IP camera B.

```
GET /
GET /xxxxxx-xxx/xxxxxxxx.asp
GET /xxxxxxxx_xxx_xxxxxxx.asp
GET /xxxxxx-xxx/xxxxxxxx.asp
GET /Logout.asp
```

図 3 ルータ C への特徴的なアクセスの流れ
Fig. 3 Example of targetted HTTP request for router C.

```
GET /
POST /apply.cgi
GET /xxxxxx-xxx/xxxxxx.asp
GET /xxxxxxxx_xxx_xxxxxxx.asp
GET /
GET /Logout.asp
```

図 4 ルータ D への特徴的なアクセスの流れ
Fig. 4 Example of targetted HTTP request for router D.

3.2.3 ルータ C

6,661 ホストからのアクセスを観測し，そのうち 103 ホストがログインに成功した．そのうち 25 ホストが，ログイン後に**図 3** に示すリクエスト群を図示した順番に送信し，Wi-Fi の設定情報やネットワークの設定情報を取得した．この攻撃は，フルブラウザによるアクセス時に発生する JavaScript や CSS，画像ファイルへのリクエストを行わないため，ツール等による自動化された攻撃と考えられる．

また，ログイン後，当該ルータを VPN サーバとして動作させる設定を行う攻撃が 17 ホストから観測された．ルータ上で動作させた VPN サーバが接続するための VPN クライアントの登録が 12 ホストから行われ，VPN クライアントが用いる ID およびパスワードが計 14 組登録されていた．当該ルータは VPN のプロトコルとして openVPN，L2TP，PPTP の 3 種をサポートするが，サポートされているすべてのプロトコルが攻撃者により選択されていた．また，登録済みの VPN クライアントを削除する操作も観測された．

図 3 に示すリクエスト群を送信した後に VPN の設定変更を試みるホストも観測された．同一ホストからのアクセスであるにもかかわらず前者のリクエストと後者のリクエストにおける User-Agent は異なっていた．前者のアクセスはツールにより広範囲にスキャンをする目的で利用しており，それによって攻撃対象であるハニーポットを発見した後，ブラウザ等の別の方法であらためてログインし VPN の設定変更を行っていた可能性がある．

また，当該ルータを VPN クライアントとして設定することを試みる攻撃を 5 ホストから観測した．接続先の VPN サーバの IP アドレスとして当該ルータ自体の IP アドレスを誤って設定した後，別の IP アドレスに変更する等，攻撃者が試行錯誤する様子が観測された．

DDNS の設定変更を行う攻撃が，4 ホストから観測された．DDNS 設定を行うことで，当該ルータに割り当てられたグローバル IP アドレスが変わった際にも攻撃者は登録したドメインにより当該ルータにアクセスすることが可能となる．上記の 4 ホストのうち 2 ホストが，ドメイン「asu-us.(xxx).com」，「KamioMisuzu.(xxx).com」の登録を行っていた．この 2 ホストのうち 1 ホストは，上述の VPN サーバ設定を試みたホストであった．

当該ルータのファイアウォール機能をオンにする操作が計 2 ホストから観測された．前述の DDNS 設定を行ったホストはファイアウォールを有効にする際，WebUI の WAN 側の待ち受けポートを 8780/tcp ポートに変更している．この挙動からは，他の侵入者を排除する意図が読み取れる．WAN 側の待ち受けポートを変更したとしても LAN 側ではデフォルトポートでアクセスできることから，変更があった際に機器の所有者が気付く可能性は低い．

3.2.4 ルータ D

3,359 ホストからのアクセスを観測し，そのうち 105 ホストがログインに成功した．うち 9 ホストが，ログイン後に**図 4** に示すリクエストを順番に送信し，Wi-Fi の設定情報やネットワークの設定情報を取得した．このうち 4 ホストは，ルータ C に対して図 3 に示すリクエストを送信したホストと同一であった．

VPN サーバの設定を試みる攻撃が 7 ホストから観測された．VPN のプロトコルは，同機器において設定可能な openVPN および PPTP の 2 種のいずれも，攻撃に使用されていた．一方，ルータを VPN クライアントとして設定する攻撃は観測されなかった．

DDNS 用ドメインの登録を行う攻撃を 2 ホストから観測し，「AD.(xxx).com」，「ADdfsads.(xxx).com」というドメインが登録されていた．2 ホストとも VPN サーバの設定も行っており，1 ホストはさらに機器のファームウェアの更新を行った．当該機器では，ファームウェアアップデートを行うことで，WebUI に外部からアクセス可能な設定が修正され，外部から WebUI にアクセスできなくなる．このファームウェアアップデートの内容を事前に知ったうえでアップデート処理を行ったとすると，当該機器を独占して踏み台化する意図を持っていた可能性が考えられる．このホストからのアクセスは，ブラウザによるアクセスにより発生する JavaScript，CSS，画像ファイル等のリクエストも含んでいた．User-Agent も新しいものであり，アクセス時間も約 35 分と長いことから，人間によるブラウザを用いたアクセスと考えられる．

3.2.5 ルータ E

5,469 ホストからのリクエストを観測し，そのうちわずかに 8 ホストがログイン試行を行ったが，全 8 ホストがログインに成功していた．このうち 2 ホストより自動化されたキャッシュ DNS 設定変更リクエストを観測した．このリクエストの一部を**図 5** に示す．リクエストにより新たに設定されるキャッシュ DNS サーバの IP アドレスは

```
POST /Forms/xxxx_xxx_x HTTP/1.1

uiViewIPAddr=192.168.1.1&dhcpFlag=0&uiViewNetMask=255.255.255.0&lan_RIPVersion=RIP2-
B&lan_RIPDirection=Yok&lan_IGMP=IGMP+v2&igmp_snoop_act=1&dhcpTypeRadio=1&dhcp_StartIP=192.168.1.100&sysPoolCount=101&dhcp_LeaseTime=259200&uiViewDNSRelay=Kullan%FDc%FD+tan%FDml%FD+DNS+Sunucu&uiViewDns1Mark=x.3.244.134&uiViewDns2Mark=x.3.244.138
```

図 5 ルータ E で観測された DNS 変更リクエストの一部
Fig. 5 Part of HTTP request to change DNS setting for Router E.

```
POST /xxxxx_xxxxx.htm HTTP/1.1

productid=xx-
xxxxxx&current_page=xxxxxxxx_xxxx_xxxxxxx.asp&next_page=xxxxxxxx_xxxxxxxxxxxx_xxxxxxx.asp&modified=0&action_mode=apply_new&action_wait=30&action_script=restart_net_and_phy&first_time=&preferred_lang=JP&firmver=x.x.x.x&lan_ipaddr=192.168.1.1&lan_netmask=255.255.255.0&dhcp_staticlist=&dhcp_enable_x=1&lan_domain=&dhcp_start=192.168.1.2&dhcp_end=192.168.1.254&dhcp_lease=86400&dhcp_gateway_x=&dhcp_dns1_x=x.3.244.136&dhcp_wins_x=&dhcp_static_x=0&dhcp_staticmac_x_0=&dhcp_staticip_x_0=cc
```

図 6 ルータ C，ルータ D で観測された DNS 変更リクエストの一部
Fig. 6 Part of HTTP request to change DNS setting for Router C and Router D.

「x.3.244.130〜x.3.244.141」と「x.152.208.2〜x.152.208.6」の範囲であった．なお，これらの IP アドレスに名前解決を行うと，これらのアドレスとは異なる IP アドレスから権威サーバにリカーシブクエリが届くことを確認している．このことから，上記のアドレスは別のキャッシュサーバに DNS クエリを転送するフォワーダとして働いていることが分かった．フォワード時に DNS クエリを盗聴している可能性がある．

キャッシュ DNS サーバ設定を変更する上記の 2 ホストは別のハニーポットであるルータ C とルータ D に対しては，**図 6** に示すリクエストを送信し，設定変更を試みた．同じ目的の攻撃であっても，機器に合わせてリクエストの内容を変更したものとみられる．このように，ターゲットに合わせて設定を調整する攻撃も存在することが確認できた．

ログインに成功した 8 ホストのうちの 1 つは，言語表示設定を中国語に変更し，ファイアウォールを on にする設定を行っていたが，この理由については不明である．

3.2.6 モバイルルータ F

ログイン試行は観測されなかった．

3.2.7 モバイルルータ G

8,724 ホストからのアクセスのうち，6 ホストのみがログインに成功した．うち 5 ホストは，フルブラウザアクセス時に取得する JavaScript ファイルや画像ファイルを取得し，機器のログイン後のトップページにアクセスした．なお，当該機器はファイルストレージ機能も有しており，上記の 5 ホストのうち 4 ホストは，当該機器に保存されているファイル一覧を取得した．また，5 ホストのうち 3 ホストは機器のネットワーク設定情報の取得も試みた．

3.2.8 プリンタ H

3,876 ホストからのアクセスを観測したが，本研究で設定した観測点および観測期間においては，当該機器を狙った攻撃は観測されなかった．しかしながら，観測点の変更，あるいは観測期間の長期化等を行うことで，当該機器を狙った攻撃が観測される可能性もある．

3.2.9 TV 放送受信機 I

3,299 ホストからのアクセスを観測したが，トップページ以外の情報にアクセスしたのは 3 ホストであり，保存されている映像の一覧やチャンネル一覧の取得を行った．そのうち 1 ホストより電源を消そうとする通信を観測し，実際に実機の電源がオフとなった．ネットワークの設定の取得や変更を行う攻撃は観測されなかった．

3.2.10 観測結果のまとめ

複数機器において，機器にアクセスした際に表示されるデフォルトの言語から言語設定を変更するアクセスを観測した．IP カメラやルータにおいて，ネットワーク設定を取得する自動化された攻撃を観測した．ルータのキャッシュ DNS 設定を変更する攻撃では，同じ目的の攻撃でも機器に合わせてリクエストの内容を変更する自動化された攻撃を観測した．複数種類のルータにおいて，VPN サーバの設定を行う攻撃を観測したが，この攻撃を行ったすべてのホストは JavaScript ファイルを取得している．人間によるブラウザを用いたアクセス，あるいは前述の自動化された DNS の設定変更と比較してもより高度な自動化が行われた手法によるアクセスと考えられる．ファイアウォールを有効にする攻撃やファームウェア更新により脆弱な設定を解消する攻撃では，攻撃者があらかじめ別のポートで WebUI にアクセス可能なように設定したり，VPN の設定を行う挙動が観測されたことから，攻撃者はバックドアを作成したうえで，脆弱な設定を修正して独占的に機器の踏み台化を行おうとしていた可能性が考えられる．

4. 考察

IP カメラ，ルータで観測されたような，ネットワーク情報を取得する自動化された攻撃では，Wi-Fi の SSID とパスワードが取得可能である．インターネット上には，Wi-Fi の SSID でおおよその位置を特定するサービス [29] が存在することから，攻撃者に Wi-Fi を無料で不正に利用される危険性がある．

また，IP カメラのネットワーク設定情報を取得する攻撃では，周辺の Wi-Fi のアクセスポイントの情報を取得する挙動が観測された．前述のようにアクセスポイントの位置を特定するサービスが存在することから，IP カメラの物理的位置の特定に用いられる可能性がある．

ルータの設定情報を取得する自動化された攻撃の後，同じアドレスからブラウザ等により VPN の設定を変更する

攻撃を観測した．このように同一の攻撃者が複数のツールやクライアントソフトを用いて効率的に攻撃先の探索や不正活動を行う様子が観測できた．

ルータの DDNS を設定する攻撃では，動的に変更された後も当該ルータに接続が可能であり，またルータの設定確認は頻繁に行われないことから長期間にわたり乗っ取られる危険性がある．

モバイルルータに保存されているファイルを確認した攻撃者がいたことから，重要な文書をモバイルルータ内部に保存していた場合，情報流出につながる危険性がある．

IoT 機器向けのアンチウィルスソフトは普及しておらず，また，攻撃により VPN や DDNS の設定変更が行われた場合でも，設定自体はルータの正規の機能であるため，不正使用に気付くことが難しいと考えられる．検証実験における設定では，デフォルトの認証設定やアクセス制御なしにインターネットから WebUI にアクセス可能な状態に機器を設定したことが攻撃をうける根本的な理由であるため，必要なサービス以外は WAN 側からアクセスできないよう設定することやパスワードを十分強固なものに設定するといった基本的な対策を行うことで多くの攻撃を防ぐことができると考えられる．しかしながら，そのような基本的な対策が行われていない機器が多く存在することも調査 [7] により明らかになっている．本研究における検証実験は，それらの基本的な対策が行われていない機器を狙ったサイバー攻撃を観測したものといえる．

本研究で攻撃観測および分析の対象とした機器のほかにも多くの種類の IoT 機器が存在する．たとえば，情報処理推進機構（IPA）は，IoT 機器のうち情報家電に類する機器を「生活支援機器」および「エンタテイメント機器」，「ヘルスケア機器」，「ネットワーク機器」の 4 種のカテゴリに分類した [30]．本研究で取り上げた機器については，TV 放送受信機 I がエンタテイメント機器に，残りすべての機器がネットワーク機器に分類され，その他のカテゴリ（生活支援機器およびヘルスケア機器）に分類される機器については攻撃観測および分析の対象としていない．しかしながら，本研究で得られた機器に対する攻撃のリスクに関する知見はこれらのカテゴリを横断したもので，機器の設定管理を行う WebUI が WAN からアクセス可能な形で公開されている限り，本研究で発見した攻撃の対象となる可能性を否定できない．また同様に，前述の「必要なサービス以外は WAN 側からアクセスできないよう設定する」もしくは「パスワードを十分強固なものに設定する」といった基本的な対策についても，機器のカテゴリを横断して一定の効果をもつものと考えられる．

本研究を実施する以前から既知であった IoT 機器に対する脅威として，Mirai およびその亜種 [31] による攻撃があげられる．Mirai およびその亜種は，基本的に「Telnet サービスがアクティブなホストを走査してログイン試行を行い，ログインに成功した場合に機器を乗っ取り，C&C サーバと通信しながら標的となるホストに攻撃を仕掛ける」という挙動をみせる．本研究で観測した攻撃は，この「機器を乗っ取る意図が見られる点」が Mirai およびその亜種と共通しているが，Mirai およびその亜種がシステムの管理者権限を奪取して対象機器を任意のマルウェアに感染させる等，機器の深いレベルに侵入するのに対し，本研究で観測した攻撃は Web アプリケーションに割り当てられた通常の操作権限が許す範囲内で機器を操作するレベルにとどまる．このように考えると本研究で観測した攻撃のインパクトは小さいようにとらえられるが，操作による変更が不揮発な記録としてシステムに残るという特徴を持っている．たとえば，攻撃者が WebUI を不正に操作して機器の設定に変更を加えたとすると，機器の正規ユーザが機器を再起動したとしてもその設定は正規ユーザが明示的に修正しない限りは復元されない．他方で Mirai およびその亜種は，感染した機器を再起動することで削除できる．このように本研究で観測した攻撃は，機器状態を変更する作用に高い持続性を持つという特徴を有しているといえる．

本研究では，「特定機器向けの攻撃判定」および「自動化されたアクセス判定」の 2 つの判定手法を用いて，観測された HTTP リクエストを分析した．以下では，当該手法の正確性についての考察を述べる．特定機器向けの攻撃判定については，図 2 や図 3，図 4 等に示したように，特定機器向けの攻撃と判定されたアクセスにおいて該当する機器固有のリクエストパスが連続して含まれていることから，当該判定を受けた攻撃ホストが特定の機器に合わせた HTTP リクエストを送信していたことが分かる．本研究の観測結果の分析において「特定機器向けの攻撃判定」により特定機器向けの攻撃を行ったと判定された攻撃ホストからのアクセスには，いずれもこの機器固有のリクエストパスが連続する形で含まれている．このことから，当該判定手法は高い正確性を持つものと考えられる．自動化されたアクセス判定の正確性については，自動化されたアクセスが持つと推測される特性について検討することで正確性を考察する．自動化されたアクセスの場合，アクセスのタイミングに周期性がみられる傾向にあるものと考えられる．あるアクセスと次のアクセスの間のインターバルについては，自動化されたアクセスの場合インターバルのばらつき（標準偏差）が小さく，自動化されていないアクセスの場合ばらつきが大きくなるものと考えられる．この差が有意な差であることを検証するため，アクセスログ中のアクセス間のインターバルを計算したうえで，「自動化アクセスと判定された群」および「自動化アクセスと判定されなかった群」のそれぞれについて無作為に 500 件ずつアクセスログを抽出した．各群についてインターバルの標準偏差を計算して，Mann-Whitney の U 検定により検討したところ，有意水準 5%（両側検定）で有意な差が認められた

($p = .020$)．このとき各群におけるインターバルの標準偏差の平均値は，自動化アクセスと判定された群で 8.75，自動化アクセスと判定されなかった群で 11.1 であった．自動化されたアクセスとそうでないアクセスの間の差異として想定した，「アクセスタイミングのインターバルの標準偏差に関する群間での大小関係」に一致する結果となっていることから，本研究で用いた自動アクセスホストの判定手法は一定の正確性を持つものと考えられる．

5. 関連研究

5.1 Web サービスのハニーポットに関する研究

Web サービスの汎用的な応答を行うことにより，リモートエクスプロイトにより感染拡大を行うマルウェア観測やマルウェア検体の収集を行うサーバ型ハニーポットの研究が活発に行われている [18], [19]．これらの研究のなかでも特に IoT 機器への攻撃を観測する目的で構築されたサーバ型ハニーポットに「IoTPOT」[9], [11] がある．しかしながら IoTPOT における WebUI への攻撃の観測機構では，スクリプトを用いたベーシック認証と DVR（Digital Video Recorder）の特定の脆弱性を模擬するか，実機を用いた IP カメラの模擬をして WebUI に対するリクエストを観測するのみであった．IoT 機器の実機を用い，観測のために大規模にプロキシを分散配置するハニーポットとして SIPHON [32] が提案されている．しかしながら，実機が侵入を受け，攻撃に悪用された際のアクセス制御については述べられていない．また，用いられている実機が IP カメラやネットワークビデオレコーダのみであり，各観測機器に対してどのような不正アクセスが発生するのかは十分に示されていない．文献 [33] では，重要インフラ施設で運用される IoT 機器の実機を用いて作成したハニーポットで攻撃を観測している．当該研究では，人手によりブラウザを用いてハニーポットの WebUI にアクセスした攻撃者の挙動を抽出・分析し，認証設定等の基本的なセキュリティ対策に問題のある実機がさらされる脅威を明らかにしている．文献 [34] では，観測点と IoT 機器の実機とを VPN フォワーダを介して接続して実機に対する攻撃通信を収集している．観測できる攻撃活動や検知できる攻撃範囲といった面では，多様な国に観測点を設けることで地理的な差異によるアクセスの傾向の違いも検討することが可能な設定となっている．本研究のハニーポットも，設計上は多様な観測点で観測可能な拡張性を有するが，本稿で示した観測試行においては単一の国の IP アドレスで観測する設定としている．他方でハニーポットの運用コストや攻撃観測の効率性といった面については，実機がマルウェアに感染した際の手立てにおいて本研究との違いがあると考えられる．文献 [34] では，実機からのアウトバウンド通信を分析したうえで，実機がマルウェアをダウンロードする通信を遮断する制御を行うが，想定外の通信によりマルウェアに感染した場合に自動的に機器の復旧を行う手立てが用意されていないものと考えられる．これに対し，本研究のハニーポットでは，定期的に機器のシャットダウンおよび再起動を実施してマルウェアを削除することで自動的に機器の保守を行い，ハニーポット運用の低コスト化を図っている．また文献 [34] では，観測された HTTP リクエストがツールやマルウェア等により自動化されたアクセスであるか否かという分析を行っていないが，本研究では当該分析を行い，特定の機器の WebUI に特化した自動的な攻撃の存在を発見することに成功している．

5.2 Web サービスへの自動アクセスの検出に関する研究

文献 [35] では，IoT 機器の Telnet に対する自動アクセスを検知する手法が提案されている．また，文献 [36] では，DDoS 攻撃の検知のため HTTP リクエストに対して隠れセミマルコフモデルを適用することで Web サーバへの自動アクセスを検知する手法が提案されている．これらに対して本研究では，自動アクセス検出の偽陰性事例を最低限に抑えるため，2.3 節に示すような非ブラウザアクセスもしくは同時並列アクセスと見なされるものをすべて自動アクセスと判定することにして，ハニーポットの WebUI に対するアクセスの分析を行った．

5.3 特定の IoT 機器を狙った攻撃の脅威に関する研究

文献 [37] では，およそ 1,600 万世帯を対象にした大規模なネットワークスキャンにより得られたデータから，半数以上の家庭が少なくとも 1 つ以上の IoT 機器を持つことが示されている．そのうえで複数の先行研究において，特定の種別の IoT 機器が攻撃のターゲットとなる可能性および攻撃が成立した際の脅威が明らかにされている．文献 [38] では，家庭内のエアコンやヒータ等の高出力機器を狙った IoT ボットネットが，電力グリッド内の電力需要を操作し，電力網に対する大規模な協調攻撃を仕掛ける可能性が示唆されている．またホームネットワーク内の機器以外についても，文献 [39] では，産業向け IoT 機器で構成されるネットワークに展開された機器を標的としてユーザの個人情報等を窃取するタイプのマルウェアの脅威に言及している．

6. おわりに

本研究では，実機を用いることで特定の IoT 機器の WebUI を狙った攻撃を観測するハニーポットを提案し，9 機種の実機を用いて検証実験を行った．その結果，IP カメラやルータのネットワーク情報を取得する自動化された攻撃やルータの VPN や DNS の設定変更を行う攻撃等，それぞれの機器の WebUI に特化したものととらえられる攻撃を観測し，提案手法の有効性を示した．IoT 機器の WebUI を狙った攻撃は，個人の攻撃者による試行段階ではなく，ツールやマルウェアによる自動化が行われる段階に入って

いると考えられる．また，VPN の設定変更攻撃等，一部の攻撃は手動によるアクセスであると判定された．このような挙動は低対話型のハニーポットでは観測が難しく，実機を用いた提案手法のハニーポットの有効性が示されたといえる．

今後の課題としては，攻撃者がどのような目的で DNS や VPN の設定変更攻撃を行っているか等，攻撃者の意図を探る調査を行いたい．また，当該実験で設置した実機には，攻撃が観測された実機と，実験期間中に攻撃がまったく観測されないものが存在するが，このような差異が生じる要因を検討したい．あわせて，攻撃者がどのようにして機器の存在を知ったかについても調査を行いたい．さらに，ファームウェアアップデートやファイアウォールを有効にすることで脆弱性が解消されて，攻撃の観測が持続不可能となる問題や，電源オフの操作を受けた際にハニーポットが停止してしまうという問題の解決方法を検討したい．

謝辞 本研究の一部は文部科学省国立大学改革強化推進事業の支援を受けて行われた．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．

参考文献

[1] Carnegie-Mellon-University: Vulnerability Note VU#447516 - Linksys SMART WiFi firmware contains multiple vulnerability, available from ⟨https://www.kb.cert.org/vuls/id/447516/⟩ (accessed 2019-06-17).
[2] Carnegie-Mellon-University: Vulnerability Note VU#332115 - D-Link routers contain buffer overflow vulnerability, available from ⟨https://www.kb.cert.org/vuls/id/332115/⟩ (accessed 2019-06-17).
[3] Durumeric, Z., Adrian, D., Mirian, A., Bailey, M. and Halderman, J.A.: Censys Security driven by data, available from ⟨https://censys.io/⟩ (accessed 2019-06-17).
[4] Matherly, J.: SHODAN, available from ⟨https://www.shodan.io/⟩ (accessed 2019-06-17).
[5] knownsec: Zoomeye, available from ⟨https://www.zoomeye.org/⟩ (accessed 2019-06-17).
[6] Insecam-project: Insecam World biggest online cameras directory, available from ⟨https://www.insecam.org/⟩ (accessed 2019-06-17).
[7] 森 博志，鉄 穎，小山大良，藤田 彬，吉岡克成，松本 勉：能動的観測と受動的観測による IoT 機器のセキュリティ状況の把握，情報処理学会研究報告，Vol.2017-CSEC-76, No.27, pp.1–6 (2016).
[8] 総務省：IoT 機器に関する脆弱性調査等の実施結果の公表，入手先 ⟨http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000154.html⟩（参照 2019-06-17）.
[9] Pa, Y.M.P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T. and Rossow, C.: IoTPOT: Analysing the Rise of IoT Compromises, *USENIX/WOOT*, Vol.15 (2015).
[10] Pa, Y.M.P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T. and Rossow, C.: IoTPOT: A Novel Honeypot for Revealing Current IoT Threats, *Journal of Information Processing*, Vol.24, No.3, pp.522–533 (online), DOI: 10.2197/ipsjjip.24.522 (2016).
[11] 鈴木将吾，インミンパパ，江澤優太，鉄 穎，中山 颯，吉岡克成，松本 勉：組込み機器への攻撃を観測するハニーポット IoTPOT の機能拡張，電子情報通信学会信学技報，Vol.115, No.488, pp.1–6 (2016).
[12] 伊藤克恭，長谷川皓一，山口由紀子，嶋田 創：IoT 向けプロトコル用ハニーポットの初期検討，情報処理学会研究報告セキュリティ心理学とトラスト（SPT），No.18, pp.1–6 (2017).
[13] Fraunholz, D., Zimmermann, M., Anton, S.D., Schneider, J. and Schotten, H.D.: Distributed and highly-scalable WAN network attack sensing and sophisticated analysing framework based on Honeypot technology, *2017 7th International Conference on Cloud Computing, Data Science Engineering - Confluence*, pp.416–421 (2017).
[14] 中山 颯，鉄 穎，楊 笛，田宮和樹，吉岡克成，松本勉：IoT 機器への Telnet を用いたサイバー攻撃の分析，情報処理学会論文誌，Vol.58, No.9, pp.1399–1409 (2017).
[15] Luo, T., Xu, Z., Jin, X., Jia, Y. and Ouyang, X.: Iotcandyjar: Towards an intelligent-interaction honeypot for iot devices, *Black Hat* (2017).
[16] Gandhi, U.D., Kumar, P.M., Varatharajan, R., Manogaran, G., Sundarasekar, R. and Kadu, S.: HIoTPOT: Surveillance on IoT devices against recent threats, *Wireless Personal Communications*, pp.1–16 (2018).
[17] Baecher, P., Koetter, M., Holz, T., Dornseif, M. and Freiling, F.: The nepenthes platform: An efficient approach to collect malware, *International Workshop on Recent Advances in Intrusion Detection*, pp.165–184, Springer (2006).
[18] rep: GitHub - rep/dionea: Dionea low interaction honeypot, available from ⟨https://github.com/DinoTools/dionaea⟩ (accessed 2019-06-17).
[19] mushorg: GitHub - mushorg/glastopf: Web Application Honeypot, available from ⟨https://github.com/mushorg/glastopf⟩ (accessed 2019-06-17).
[20] gbrindisi: GitHub - gbrindisi/Wordpot: A Wordpress Honeypot available from ⟨http://xxxxx.xxx/xxx/xxx/⟩ (accessed 2019-06-17).
[21] Cymmetria: GitHub - Cymmetria/StrutsHoneypot: Struts Apache 2 based honeypot available from ⟨http://xxxx.xxx/xxx/xxx/⟩ (accessed 2019-06-17).
[22] Yagi, T., Tanimoto, N., Hariu, T. and Itoh, M.: Enhanced attack collection scheme on high-interaction web honeypots, *The IEEE Symposium on Computers and Communications*, pp.81–86 (2010).
[23] 八木 毅，谷本直人，針生剛男，伊藤光恭：高対話型 Web ハニーポットにおける攻撃情報収集方式の改善，コンピュータセキュリティシンポジウム 2009（CSS2009）論文集，Vol.2009, pp.1–6 (2011).
[24] Ma, J., Chai, K., Xiao, Y., Lan, T. and Huang, W.: High-Interaction Honeypot System for SQL Injection Analysis, *2011 International Conference of Information Technology, Computer Engineering and Management Sciences*, Vol.3, pp.274–277 (2011).
[25] Canali, D. and Balzarotti, D.: Behind the Scenes of Online Attacks: An Analysis of Exploitation Behaviors on the Web, *20th Annual Network & Distributed System Security Symposium* (*NDSS 2013*), San Diego, United States (2013).
[26] 八木 毅，針生剛男：ハイブリッド型 Web ハニーポット Web Phantom の実装と評価（情報通信システムセキュリティ），電子情報通信学会技術研究報告= IEICE Technical

Report: 信学技報，Vol.113, No.502, pp.65–70 (2014).
[27] 藤本万里子，松田　亘，満永拓邦：OGNL の実行に起因する Struts 2 の脆弱性に対する防御手法の提案，コンピュータセキュリティシンポジウム 2017 論文集，Vol.2017, No.2 (2017).
[28] 田宮和樹，中山　颯，江澤優太，鉄　穎，呉　俊融，楊笛，吉岡克成，松本　勉：IoT マルウエア駆除と感染防止に関する実機を用いた実証実験 (2017).
[29] bobzilla, arkasha and uhtu: WIGLE.NET, available from ⟨https://wigle.net/⟩ (accessed 2019-06-17).
[30] 独立行政法人情報処理推進機構：情報セキュリティ 10 大脅威 2018，入手先 ⟨https://www.ipa.go.jp/files/000066221.pdf⟩（参照 2019-09-10）.
[31] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K. and Zhou, Y.: Understanding the Mirai Botnet, *26th USENIX Security Symposium* (*USENIX Security 17*), Vancouver, BC, pp.1093–1110, USENIX Association (2017).
[32] Guarnizo, J.D., Tambe, A., Bhunia, S.S., Ochoa, M., Tippenhauer, N.O., Shabtai, A. and Elovici, Y.: Siphon: Towards scalable high-interaction physical honeypots, *Proc. 3rd ACM Workshop on Cyber-Physical System Security*, pp.57–68, ACM (2017).
[33] 加藤里奈，佐々木貴之，藤田　彬，吉岡克成，松本　勉：インフラ施設の遠隔監視制御システムを模したハニーポットの提案，暗号と情報セキュリティシンポジウム（SCIS）(2019).
[34] Tambe, A., Aung, Y.L., Sridharan, R., Ochoa, M., Tippenhauer, N.O., Shabtai, A. and Elovici, Y.: Detection of Threats to IoT Devices Using Scalable VPN-forwarded Honeypots, *Proc. 9th ACM Conference on Data and Application Security and Privacy*, *CODASPY '19*, pp.85–96, ACM (2019).
[35] 高橋佑典，渡部正文，島　成佳，吉岡克成：ハニーポットへの自動化されたアクセスの判別指標の考察，暗号と情報セキュリティシンポジウム（SCIS）(2017).
[36] Xie, Y. and Yu, S.-Z.: A large-scale hidden semi-Markov model for anomaly detection on user browsing behaviors, *IEEE/ACM Trans. Networking* (*TON*), Vol.17, No.1, pp.54–65 (2009).
[37] Deepak, K., Kelly, S., Benton, C., Deepali, G., Alperovich, G., Dmitry, K., Rajarshi, G. and Zakir, D.: All Things Considered: An Analysis of IoT Devices on Home Networks, *28th USENIX Security Symposium*, USENIX Association (2019).
[38] Soltan, S., Mittal, P. and Poor, H.V.: BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid, *Proc. 27th USENIX Security Symposium*, USENIX Association (2018).
[39] Sharmeen, S., Huda, S., Abawajy, J.H., Ismail, W.N. and Hassan, M.M.: Malware Threats and Detection for Industrial Mobile-IoT Networks, *IEEE Access*, Vol.6, pp.15941–15957 (2018).

藤田 彬　（正会員）

2012 年 12 月横浜国立大学大学院環境情報学府博士課程後期修了，博士（情報学）．2013 年 1 月横浜国立大学成長戦略研究センター産学官連携研究員．同年 8 月大学共同利用機関法人情報・システム研究機構国立情報学研究所特任研究員．2015 年 6 月同特任助教．2017 年 1 月より横浜国立大学先端科学高等研究院特任教員（助教）．能動的観測および受動的観測による IoT 機器への攻撃リスクの検知，攻撃の観測等ネットワークセキュリティに関する研究に従事．

江澤 優太

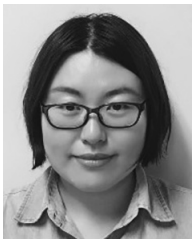
2016 年 3 月横浜国立大学理工学部数物・電子情報系学科卒業，学士（工学）．同年 4 月横浜国立大学大学院環境情報学府博士課程前期に進学．ネットワークセキュリティに関する研究に従事．

田宮 和樹

2017 年 3 月横浜国立大学理工学部数物・電子情報系学科卒業，学士（工学）．同年 4 月横浜国立大学大学院環境情報学府博士課程前期に進学．ネットワークセキュリティに関する研究に従事．

中山 颯

2016 年 3 月横浜国立大学理工学部数物・電子情報系学科卒業，学士（工学）．同年 4 月横浜国立大学大学院環境情報学府博士課程前期に進学．ネットワークセキュリティに関する研究に従事．



鉄 顕

2018 年 6 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程後期修了．博士（情報学）．情報セキュリティ，特にネットワーク攻撃観測・分析等のネットワークセキュリティ研究に従事．2018 年 8 月よりトヨタ自動車（株）で自動車の安全とセキュリティに関する研究に従事．

吉岡 克成 （正会員）

2005 年 3 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程後期修了，博士（工学）．同年 4 月独立行政法人情報通信研究機構研究員．2007 年 12 月横浜国立大学学際プロジェクト研究センター特任教員（助教）．2011 年 4 月より横浜国立大学大学院環境情報研究院准教授．マルウェア解析やネットワーク攻撃観測・検知等のネットワークセキュリティの研究に従事．2009 年文部科学大臣表彰・科学技術賞（研究部門）受賞．

松本 勉

1986 年 3 月東京大学大学院工学系研究科電子工学専攻博士課程修了，工学博士．同年 4 月横浜国立大学講師．2001 年 4 月同大学院環境情報研究院教授．2014 年 12 月より同大学先端科学高等研究院主任研究者を兼務．ネットワーク・ソフトウェア・ハードウェアセキュリティ，暗号，耐タンパ技術，生体認証，人工物メトリクス等の「情報・物理セキュリティ」の研究教育に 1981 年より従事．1982 年にオープンな学術的暗号研究を目指した「明るい暗号研究会」を 4 名で創設．2005 年～2010 年国際暗号学会 IACR 理事．1994 年第 32 回電子情報通信学会業績賞，2006 年第 5 回ドコモ・モバイル・サイエンス賞，2008 年第 4 回情報セキュリティ文化賞，2010 年文部科学大臣表彰・科学技術賞（研究部門）受賞．