Computer Security Symposium 2017
23 - 25 October 2017

# 実機を用いたハニーポットによる組込み機器のWebUIに対するサイバー攻撃の分析

江澤 優太[†1]　田宮 和樹[†1]　中山 颯[†1]　鉄 穎[†1]　吉岡 克成[†2]　松本 勉[†2]

**概要**：組込み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 IoT 機器が多数存在し，それらの中には，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 機器向けの攻撃の自動化が行われていることを示す．

**キーワード**：IoT，Web，ハニーポット，実機

# An Analysis of Attacks Targeting WebUI of Embedded Devices by Bare-metal Honeypot

Yuta Ezawa[†1]　Kazuki Tamiya[†1]　Sou Nakayama[†1]　Ying Tie[†1]
Katsunari Yoshioka[†2]　Tsutomu Matsumoto[†2]

***Abstract***: There are many embedded devices that have WebUI for device management and operation, and 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 show that attacks on WebUI of IoT devices are widely conducted with certain degree of automation.

***Keywords***: IoT, Web, Honeypot, Bare-metal

## 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(以降では IoT 機器と呼ぶ)の中には，Web ブラウザを用いて機器の遠隔操作や設定を行う Web ユーザーインターフェイス(以降では WebUI と呼ぶ)を有するものが多数存在する．この WebUI を介してルータの設定ファイルを遠隔から取得可能であったり[1]，バッファオーバーフローによりマルウェア感染する[2]など，WebUI に起因する脆弱性を持つ機器は多い．また，デフォルトのパスワードでログインできたり，そもそも認証なしで管理・設定画面にアクセス可能な IP カメラやルータ等の機器が多数発見されている[3, 4, 5].

ハニーポットを用いて IoT 機器への攻撃を観測する研究[6, 7]がこれまで行われているが，上述のような WebUI に対する攻撃の調査は十分に行われていなかった．IoT 機器の WebUI は，その内容や機能が機器の種類に応じて様々である上，動作も複雑であるため， Web サービスの汎用的な応答だけを行うような従来の Web サーバハニーポット[8, 9]では攻撃の詳細な観測が難しい．

そこで，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，攻撃の観測実験を行う．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, CSS, PNG, JPG など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．

上記の 9 機種それぞれに 10IP アドレスを割り当て，それぞれ約 80 日~250 日におよぶ観測を行った結果，7 種類の機器に対して，それぞれの機器に特化していると判断される攻撃が観測された．IP カメラの設定ファイルを取得する

†1 横浜国立大学
Yokohama National University
240-8501 神奈川県横浜市 保土ヶ谷区常盤台 79-1
{ezawa-yuta-xd, tamiya-kazuki-gj, nakayama-sou-ch, tie-ying-fc}@ynu.jp
†2 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
{yoshioka, tsutomu}@ynu.ac.jp

攻撃，ルータの DNS 設定を変更する攻撃など，攻撃対象機器に応じて自動化されたアクセスが観測された．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上で，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．

本稿の構成は次のとおりである．まず，第 2 章で IoT 機器の WebUI について説明し，第 3 章で提案手法について述べる．第 4 章では検証実験について述べ，第 5 章で観測結果に関する考察を行う．第 6 章で関連研究について述べ，最後に第 7 章でまとめと今後の課題を述べる．

## 2. IoT 機器の WebUI

### 2.1 IoT 機器の WebUI で用いられる認証方式

IoT 機器の WebUI では，ユーザの認証のためにベーシック認証，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．

ベーシック認証とダイジェスト認証は HTTP で定義された認証方式である．ベーシック認証では，HTTP リクエストのヘッダの Authorization フィールドに，ID と Password の組みをコロンでつなぎ，Base64 でエンコードして送信し，認証を行う．ダイジェスト認証は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あり，ID と Password の MD5 ハッシュ値をサーバに送信することで認証を行う．

フォーム認証と呼ばれる認証方式は，JavaScript 等で認証用のフォームを用意する方法であり，HTTP で定義されていないため，認証フォームや送信するリクエストは WebUI の実装により異なる．

### 2.2 WebUI の機能

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，状態確認などを，WebUI を介して行う場合が多い．多くの IoT 機器でネットワーク設定，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なども可能である．また，機器に特化した操作として，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，ズームや首振りなどの操作，放送受信機では映像の取得や録画予約などに利用されている．

## 3. 提案手法

### 3.1 ハニーポットの構成

本節では，実機を用いることで様々な IoT 機器の WebUI への攻撃を観測するハニーポットを提案する．本手法では，IoTPOT[6, 7]の構成を元に拡張を行う．提案手法の構成は図 1 の通りである．なお，図 1 では，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，受け取った通信を通信制御マシンへ転送する．通信制御マシンでは，各観測点に対応する IoT 機器の実機へ通信を転送し，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かのように見える．

観測される通信には，IoT 機器の脆弱性を狙い，マルウェア感染やマシンを乗っ取るためのものなど，深刻な被害を与えるものも存在する．そこで，外部に被害を与えないため実機から新たにセッションを繋ごうとする通信は通信制御部で通信に制限をかける．

また，観測用の IoT 機器は侵入によりマルウェア感染する可能性があるため，機器を初期状態に戻すために定期的に電源を落とし再起動する．論文[10]では，機器の再起動によりマルウェアが駆除されることが示されており，定期的な機器のシャットダウンと再起動は有効といえる．

また，ファームウェアアップデートなど機器のリセット(工場出荷状態に戻す操作)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．

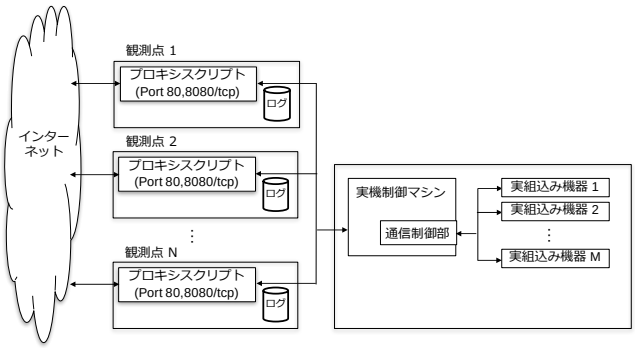


図 1 ハニーポットの構成

### 3.2 特定機器向けアクセスの分析方法

観測した通信には，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ため，これに着目し，観測対象機器向けの攻撃を抽出する手法を以下で説明する．

**フォーム認証**

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は観測対象機器を狙う攻撃として判定する．

**ベーシック認証・ダイジェスト認証**

ハニーポットの WebUI へのログインに用いる ID/Password は初期状態のデフォルト値から変更していないため，これらの機器を狙う攻撃は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して判断する．

**認証のない機器**

認証の無い機器においては，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して判断する．

### 3.3 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，ツールやマルウェア等により自動化されていると予想されるアクセスを以下の流れで判定する．

**判定方法 1(非ブラウザアクセスの判定)**

フルブラウザによるアクセスと異なり，ツールやマルウェアによる特定機器を狙った攻撃は，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．そこで, 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 などの画像ファイルが自動的に取得されるかを調べておく．そして，ブラウザと異なり，特定のファイルのみを要求するアクセスを自動化されていると判定する．

**判定方法 2(同時並列アクセスの判定)**

ツールやマルウェアにより効率的にサイバー攻撃が行われると，ハニーポットでは同種の攻撃を頻繁に観測するようになる．そこである一定期間に一定数以上のハニーポットに対して同様のパスを要求するアクセスを観測した場合に，攻撃が自動化されていると判断する．次章の検証実験では 1 分以内に各機器のハニーポットが動作する 10IP アドレスのうち 9IP アドレス以上に対して同種のリクエストが届いており, これを自動化された攻撃であると判定した．

## 4. 検証実験

### 4.1 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 機種の実機を用い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．なお，各実機に対応する観測点はそれぞれ連続する 10IP を用いた．また, ルータ C は非公式のカスタムファームウェアを使用し，それ以外の機器では公式のファームウェアを使用した．

各観測点の 80/tcp 及び 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．なお，前章で述べた機器の定期的な再起動や，ファームウェア更新処理のブロック

表 1 実験概要

| 機器名 | メーカ国/地域 | 認証方法 | ID/Password | 観測IP | 観測期間 | 観測日数 |
|---|---|---|---|---|---|---|
| IPカメラA | 日本 | ベーシック認証<br>ダイジェスト認証 | admin/12345 | 10IP | 2016/12/16~2017/8/16 | 244日 |
| IPカメラB | 台湾 | ベーシック認証 | admin/(null) | 10IP | 2016/11/30~2017/8/16 | 260日 |
| ルータC | 台湾 | ベーシック認証 | admin/admin | 10IP | 2016/11/30~2017/3/8<br>2017/4/12~2017/8/16 | 226日 |
| ルータD | 台湾 | ベーシック認証 | admin/admin | 10IP | 2016/12/16~2017/2/5<br>2017/2/23~2017/3/3<br>2017/4/12~2017/5/3 | 83日 |
| ルータE | 台湾 | フォーム認証 | admin/admin | 10IP | 2016/12/16~2017/1/27<br>2017/2/22~2017/3/7<br>2017/4/12~2017/7/17 | 154日 |
| ポケットルータF | 日本 | フォーム認証 | admin/admin | 10IP | 2016/11/30~2016/11/30<br>2016/12/5~2017/3/1 | 88日 |
| ポケットルータG | アメリカ | フォーム認証 | admin/(null) | 10IP | 2016/12/16~2017/8/16 | 244日 |
| プリンタH | アメリカ | なし | なし | 10IP | 2016/11/30~2017/3/1<br>2017/6/24~2017/8/16 | 146日 |
| 放送受信機I | ドイツ | なし | なし | 10IP | 2016/12/9~2017/2/11<br>2017/2/22~2017/3/1<br>2017/6/24~2017/7/26 | 106日 |

※ルータCでは非公式のカスタムファームウェアを使用

については，本検証実験では実装していない．

そして，ファイヤーウォールが存在するルータではファイヤー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初期パスワードから変更せず実験を行った．

### 4.2 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と各機器を狙うリクエストを送信したホスト数は表 2 の通りであった．なお，ルータ E とポケットルータ G の観測結果において，ログイン試行ホスト数より，特定機器へのアクセスホスト数が多くなっているが，これは認証成功時の HTTP クッキー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， 図 2 から図 6 ではリクエスト中の文字列の一部をマスキングしている．

表 2 検証実験結果概要

| 機器名 | リクエストホスト数 | ログイン試行ホスト数 | ログイン成功ホスト数 | 特定機器へのアクセスホスト数 |
|---|---|---|---|---|
| IPカメラA | 8695 | 222 | 26 | 25 |
| IPカメラB | 10426 | 239 | 19 | 12 |
| ルータC | 6661 | 298 | 103 | 79 |
| ルータD | 3359 | 105 | 51 | 38 |
| ルータE | 5469 | 8 | 8 | 11 |
| ポケットルータF | 2769 | 0 | 0 | 0 |
| ポケットルータG | 8724 | 36 | 6 | 12 |
| プリンタH | 3876 | | | 1 |
| 放送受信機I | 3299 | | | 17 |

**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していた．具体的には，これら 25 ホストの全てが，当該機器が撮影中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上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．一方設定変更画面へアクセスしたホストはいなかった．機器の表示言語は他設定と異なりトップ画面から変更可能であり，攻撃者の中には言語設定をデフォルトで表示される日本語から英語や中国語に変更する攻撃者が存在した．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．

**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順番に送信し，カメラの Wi-Fi 接続情報，カメラ周辺の Wi-Fi の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り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 ホストしか観測されなかった．

```
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

**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，図 3 に示すリクエスト群を順番に送信し，Wi-Fi の設定情報やネットワークの設定情報を取得していた．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っていないため, 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 サーバに接続するための 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/Password が合計 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，いずれも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．

なお，上述の図 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確認された．同一ホストからのアクセスであるにも関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る可能性がある．

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など，攻撃者の試行錯誤の様子が観測された．

加えて，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 アドレスが変更した際にも，攻撃者は登録したドメインにより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 サーバ設定を行おうとしたホストであった．

当該ルータのファイヤーウォール機能をオンにする操作が合計 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ヤーウォールを有効にする際，WebUI の WAN 側待ち受けポートを 8780/tcp ポートに変更しており，他の侵入者を排除する意図が読み取れる．なお，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のアクセスが可能であることから，このような変更を行ったとしても，機器の所有者は気づかない可能性が高い．

```
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

**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．そのうち，9 ホストがログイン後，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ていた．このうち，4 ホストはルータ C において，図 3 に示す順にリクエストを行っ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 のプロトコルは設定可能な openVPN，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 サーバの設定もおこなっており，1 ホストは更に機器のファームウェアの更新を行った．当該機器のファームウェアアップデートにより WebUI に外部からアクセス可能な設定が修正されるため，これをあえて行うことで当該機器を独占して踏み台化しようとし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 も最近のものであり，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であると考えられる．

```
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

**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おこなったが，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「x.3.244.130～x.3.244.141」と「y.152.208.2～y.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おり，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ーワーダとして働いていることが分かった．フォーワード時に 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行おうとしていた．このように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している実態が確認できた．

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，ファイヤーウォールを 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．

```
POST /xxxxx_xxxxx.htm HTTP/1.1

productid=xx-
xxxxxx&current_page=xxxxxxxx_xxxx_xxxxxxx.asp&next_page=xxxxxxxx_xx
xxxxxxxxxxx_xxxxxxx.asp&modified=0&action_mode=apply_new&action_wa
it=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_sta
ticip_x_0=cc
```

図 5 ルータ E で観測された DNS 変更リクエストの一部

```
POST /Forms/xxxx_xxx_x HTTP/1.1

uiViewIPAddr=192.168.1.1&dhcpFlag=0&uiViewNetMask=255.255.255.0&l
an_RIPVersion=RIP2-
B&lan_RIPDirection=Yok&lan_IGMP=IGMP+v2&igmp_snoop_act=1&dhcpT
ypeRadio=1&dhcp_StartIP=192.168.1.100&sysPoolCount=101&dhcp_Leas
eTime=259200&uiViewDNSRelay=Kullan%FDc%FD+tan%FDml%FD+DNS+S
unucu&uiViewDns1Mark=x.3.244.134&uiViewDns2Mark=x.3.244.138
```

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

**ポケットルータ F**

ログイン試行を観測できなかった.

**ポケットルータ 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へアクセスを行っていた．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ていた．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も取得しようとした.

**プリンタ H**

3,876 ホストからのアクセスを観測したが，当該機器を狙った攻撃は観測されなかった.

**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。その内の 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．一方，ネットワークの設定の取得や変更を行う攻撃者は観測されなかった.

**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 カメラやルータで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，この攻撃を行った全てのホストは JavaScript ファイルを取得しており, 人間によるブラウザを用いたアクセスか, 上述の自動化された DNS の設定変更より高度な自動化が行われていると考えられる．ファイヤー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，攻撃者が予め別のポートで 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上で，脆弱な設定を修正して独占的に踏み台化を行おうとしていた可能性が考えられる.

## 5. 考察

IP カメラ，ルータで観測された自動化されたネットワーク情報を取得する攻撃では，Wi-Fi の SSID と Password が取得可能なことから、攻撃者に Wi-Fi を無料で、不正に利用される危険性がある.

IP カメラのネットワークの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. 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が存在するため，IP カメラの物理的位置を割り出すの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.

ポケット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，重要な文書をポケット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イ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である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．一方，そのような基本的な対策が行われていない機器が大量に存在することも調査[11]により明らかになっており，それを狙ったサイバー攻撃が今回の実験により観測されたといえる.

## 6. 関連研究

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検体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[8, 9]．本研究で拡張した IoTPOT[6, 7]では，従来 WebUI の観測はスクリプトを用いたベーシック認証と DVR の特定脆弱性の模擬と実機を用いた IP カメラの模擬のみであった.

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[12]が提案されている．しかし，実機が侵入を受け，攻撃に悪用された際のアクセスの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ーのみであり，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述べられていない．

IoT 機器の Telnet に対する自動アクセスの検知手法の提案[13]が提案されている．また，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 サイトに対する自動アクセスを検知する手法[14]がある．これに対して，本研究ではハニーポットの WebUI に対し観測されたアクセスが自動化されているという観点で分析を行った．

## 7. まとめと今後の課題

本稿では，実機を用いることで IoT 機器の WebUI に対する攻撃を観測するための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などの IoT 機器の WebUI に対する攻撃を観測し，提案手法の有効性を示した．

また，VPN の設定変更攻撃など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のハニーポット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のか調査を行いたい．また，ファームウェアアップデートやファイヤーウォールを有効とすることによる脆弱性の解消や電源オフによる機器の停止によりハニーポットが停止してしまうという問題を解決する方法を検討したい．

**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] “Vulnerability Note VU#447516 - Linksys SMART WiFi firmware contains multiple vulnerabilities”, https://www.kb.cert.org/vuls/id/447516, (参照 2017/08/27).
[2] “Vulnerability Note VU#332115 - D-Link routers contain buffer overflow vulnerability”, https://www.kb.cert.org/vuls/id/332115, (参照 2017/08/27).
[3] “Insecam World biggest online cameras directory”. http://www.insecam.org/, (参照 2017/08/24).
[4] “Shodan”. https://www.shodan.io/, (参照 2017/08/24).
[5] “Censys”. https://censys.io/, (参照 2017/08/24).
[6] Pa, Y, M, P,. Suzuki, S. Yoshioka, K. Matsumoto, T. Kasama, T. and Rossow, C.. IoTPOT: Analysing the Rise of IoT Compromises. USENIX/WOOT, 15, 2015
[7] 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. 2016, vol. 115, no. 488, ICSS2015-47, p. 1-6.
[8] “GitHub - mushorg/glastopf: Web Application Honeypot”. https://github.com/mushorg/glastopf, (参照 2017/08/24).
[9] “GitHub - rep/dionaea: dionaea low interaction honeypot”. https://github.com/rep/dionaea, (参照 2017/08/24).
[10] 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 マルウェア駆除と感染防止に関する実機を用いた実証実験: 2017, 暗号と情報セキュリティシンポジウム(SCIS), 3E1-5 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. In Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security, 2017, p. 57–68.
[11] 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. コンピュータセキュリティ (CSEC), 2017, 2017-CSEC-76(27), p. 1-6.
[12] 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. In Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security, 2017, p. 57–68.
[13] 髙橋 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. 2017, 暗号と情報セキュリティシンポジウム(SCIS), 3E1-2
[14] Xie, Y. and Yu S.-Z.. A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors. IEEE/ACM TRANSACTIONS ON NETWORKING. 2009, VOL 17, NO. 1, p. 54-65.