Vol.2017-DPS-170 No.27
Vol.2017-CSEC-76 No.27
2017/3/3

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

森博志[†1]　鉄穎[†1]　小山大良[†1]　藤田彬[†2]　吉岡克成[†2†3]　松本勉[†2†3]

概要：近年，十分なセキュリティ対策が施されていない IoT 機器を狙ったサイバー攻撃が問題となっている．特に Telnet に代表される脆弱なサービスを狙ったマルウェア感染が深刻化している．しかし IoT 機器に対する脅威はこれだけではない．IoT 機器には機器の設定や制御を行ったり，状態を確認するための Web ユーザインターフェイスを備えているものが多く存在するが，これらのアクセス制御についても十分な対策や適切な設定がなされていない可能性がある．本研究ではネットワークスキャンによる能動的観測と IoT 機器を模したハニーポットによる受動的観測から IoT 機器の状況を調査した結果を報告する．調査の結果，工場や発電所などで使用される計測機器がマルウェア感染しているといった非常に深刻な状況やダムなどの水処理施設の遠隔監視制御システムの状態が認証なしに誰でもアクセス可能となっているなど多数の事例が見つかった．

キーワード：IoT, ネットワークスキャン

Investigation into IoT Security by Active Observation and Passive Observation

HIROSHI MORI[†1]　YING TIE[†1]　TAIRA OYAMA[†1]
AKIRA FUJITA[†2]　KATSUNARI YOSHIOKA[†2†3]　TSUTOMU MATSUMOTO[†2†3]

1. はじめに

近年，十分なセキュリティ対策が施されていない IoT 機器を狙ったサイバー攻撃が問題となっている．特に Telnet に代表される脆弱なサービスを狙ったマルウェアの感染が深刻化している．例えば Telnet を狙って感染を行うマルウェアである Mirai[1]とその亜種は 2016 年 9 月末にソースコードが公開された[2]こともあり大量の IoT 機器が感染した．マルウェアに感染した IoT 機器による DoS 攻撃は脅威であり実際に世界的に有名な SNS サイトが一時的に閲覧出来ない状態になった[3]．このような脆弱なサービスを狙って IoT 機器に侵入を行うマルウェアによる問題は国内でも報道されている．しかし IoT 機器に対する脅威はこれだけではない．

IoT 機器には機器の設定や制御を行ったり，状態を確認するための Web ユーザインターフェイス(以下，Web UI と呼ぶ)を備えているものが多く存在するが，これらのアクセス制御についても十分な対策や適切な設定がなされていない可能性がある．アクセス制御に問題がある場合，攻撃者により機器の持つ情報の盗取や遠隔操作が行われる危険性がある．どのような問題が起こり得るかは IoT 機器が提供する機能によって異なるが，例えばルータであればネットワークの制御設定が変更され，ルータの利用者が悪意のあるサーバに通信を誘導されるシナリオなどが考えられる．更に重要施設の制御機器が遠隔操作された場合には人命に関わる問題になる可能性もある．そのためアクセス制御が適切でない Web UI を持つ IoT 機器の実態を把握することが重要である．

本研究ではこれらの機器の調査を能動的観測手法である，ネットワークスキャンにより行う．また IoT 機器の中には既にマルウェアに感染し，他の IoT 機器に対して不正ログインにより感染を広げようとする機器が存在する．そこで本研究では受動的観測手法であるハニーポットによりマルウェア感染 IoT 機器の調査も行う．

調査の結果，工場や発電所などで使用される計測機器がマルウェアに感染しているといった非常に深刻な状況や，ダムなどの水処理施設の遠隔監視制御システムの状態が認証なしに誰でもアクセス可能となっているなど多数の事例が見つかった．

2. IoT 機器の深刻度と調査技術

本研究ではインターネットに接続されている，組み込み機器などの特定の機能のみ提供する機器を IoT 機器と呼ぶ

†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
Faculty of Environment and Information Sciences, Yokohama National University

こととする．

IoT 機器は NAS やブロードバンドルータのような一般家庭で使用されているような機器から太陽光発電や水処理プラントのような工場や病院など重要施設に関するものまで多様であり，また機器によって脆弱性の内容や重大さが異なる．そこで本研究では IoT 機器の機能が停止した場合の利用者への影響の大きさを機器重要度，脆弱性を突かれた場合の機器への影響の大きさを脆弱性重大度とし，表 1 のように分類する．カテゴリの数字が小さいほど問題が深刻であり対応が急がれる．

表 1　脆弱性重大度・機器重要度に応じた IoT 機器の問題の深刻度

	脆弱性カテゴリ 1（マルウェア感染）	脆弱性カテゴリ 2（設定変更・情報アクセス）	脆弱性カテゴリ 3（機器存在露見）
重要度カテゴリ 1（重要機器）	非常に深刻	深刻	場合によっては深刻
重要度カテゴリ 2（重要機器以外）	深刻	場合によっては深刻	深刻ではない

脆弱性重大度

カテゴリ 1：マルウェアや攻撃者に制御を乗っ取られる．（例：認証が脆弱な Telnet サービス，CWMP 脆弱性[4]，特定のモデムの脆弱性[5]）

カテゴリ 2：機器の設定変更，機器が有する内部情報にアクセス可能．（例：管理用 Web UI の認証がない，または認証が脆弱な機器）

カテゴリ 3：機器の存在，種別が遠隔から把握できるものの，設定変更や機器が有する内部情報へのアクセスができない．（例：管理用 Web UI に外部からアクセスすることで機器の存在が確認できるものの機器の設定変更や内部情報にはアクセスできない場合）

カテゴリ 3 の機器は不正な操作や情報の盗取の対象とならないため深刻度は低いが，DoS 攻撃の対象となる場合や，将来脆弱性が発見され脆弱性カテゴリが 1, 2 に変化する可能性がある．

機器重要度

カテゴリ 1：利用者の生活や生命に直接影響を及ぼす可能性がある重要な機器（医療機器，HEMS，産業制御システム，重要インフラ）

カテゴリ 2：カテゴリ 1 以外の機器

脆弱性重大度のカテゴリ 2, 3 についてはネットワークスキャンと Web UI の調査により判断が可能であるが，脆弱性 1 については判断が難しい．そこで本研究ではマルウェア感染機器の情報についてはハニーポットを利用する．

3. IoTPOT

IoTPOT[6]は Telnet サービス等が動作している IoT 機器を模したハニーポットであり，攻撃者からの不正なログインンチャレンジやログイン後の実行コマンドの観測が可能である．また IoTPOT ではアクセスをしてきたホストの特定のポート（22/ssh, 23/telnet, 80/http など）に対してスキャンを行い，アクセス元の機器情報を収集する．本研究では IoTPOT により観測した攻撃ホストをマルウェア感染機器とする．

4. 関連研究

ネットワークスキャンツールとして nmap[7]が広く知られている．また近年ではより高速にスキャンを行うことが出来る zmap, zgrab[8,9]や masscacn[10]が公開されている．

zmap を開発したミシガン大学の研究チームは当該ネットワークスキャナを用いた研究を複数件発表している．文献[11]では Heartbleed と呼ばれる OpenSSL[12]の脆弱性を持つサーバの公開状況や，サーバ管理者による当該脆弱性への対応について調査しており，脆弱性の持つ機器の調査に zmap を利用している．また文献[13]では Modbus や BACnet など 5 つの産業制御用プロトコルに対して zmap によりスキャンを行い，インターネットからアクセス可能な機器を探すと同時に，誰が産業用プロトコルへのスキャンを行っているかについて調査するために，ハニーポットによる調査を行っている．本研究は IoT 機器を調査する目的にネットワークスキャンやハニーポットを利用しているという点について当該研究と類似しているが，スキャン対象のプロトコルが違う点や，ハニーポットを脆弱機器の特定に利用しているという点で本研究とは異なる．

Shodan[14]や Censys[15]では全 IP アドレス空間をスキャンした結果を公開しておりこれらのサービスでは Telnet, SSH, FTP や Windows のファイル共有システムのデフォルトポート番号，産業制御システムに利用されるサービスのデフォルトポート番号の解放状況や，それぞれのサービスにアクセスした際のペイロードなどについて定期的に調査を行いその結果を公開しており，誰でも利用することが可能である．Shodan や Censys では本研究が調査の対象としている HTTP のデフォルトポート(80/tcp)に関する情報も調査・公開しており，ポートの解放状況だけでなく，ルートページのコンテンツについても知ることができ，本研究でも活用している．しかしルートページのコンテンツだけでは WebUI が IoT 機器のものなのかどうか判断することが難しいものや，モバイルネットワークなどの IP アドレスの割り当てが頻繁に変更されるネットワーク下の機器についてはこれらのサービスで公開されている IP アドレスが古いことがあり，当該サービスだけで本研究の目的を達成することは難しく，本研究では独自の調査手法と上記のサービスを組み合わせて調査を行っている．

5. 提案手法

本研究の調査手順を図 1 に示す．提案手法ではまず調査対象の IP アドレスに対してポートスキャンを行い Web UI のデフォルトポートとして使用される 80/tcp でセッション確立が可能であるホストの IP アドレスを絞り込む．次に，絞り込んだ IP アドレスに対して HTTP によりルートページにアクセスを行いその応答を収集する．インターネット上には一般的な Web サイトが多数存在するため, 収集した応答から IoT 機器による応答を選別する必要がある．そこで提案手法では IoT 機器の Web UI を HTTP 応答の特徴から選別する．そして，それらの Web UI や同時に動作している Telnet などのサービスについてセキュリティ上の問題がないかどうか詳細に調査を行う．さらに脆弱性が存在する機器についてはインターネットからアクセス可能な同一機種や同様の脆弱性が存在する可能性がある類似機器を探索する．また脆弱性カテゴリ 1 の機器については受動的に脆弱な機器を特定可能であるが，脆弱性カテゴリ 2, 3 の機器については能動的に脆弱な機器を見つける必要があるため調査の流れが異なる．

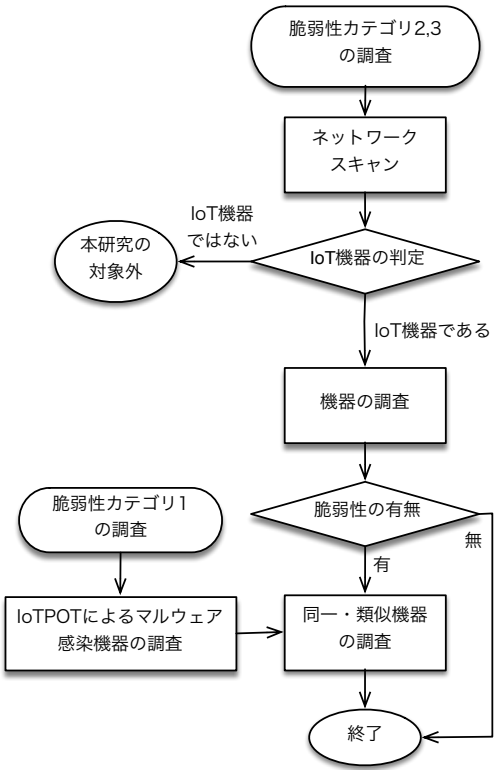

図 1　提案手法による IoT 機器の調査の手順

以下ではそれぞれの処理について詳細を述べる．

5.1 ネットワークスキャン

インターネット上に公開されている IoT 機器の Web UI を見つけるために，80/tcp ポートに対してポートスキャンツールである zmap によりポートスキャンを行う．次にポートスキャンにより発見した 80/tcp でセッション確立が可能なホストに対して以下の URL で HTTP によりアクセスを行いルートページのコンテンツを収集する．

http://<調査対象のホストの IP アドレス>/

本研究による調査ではアプリケーションレイヤスキャンツールである zgrab により HTTP ボディや HTTP ヘッダの情報を収集すると同時に Web ページをレンダリングして画像として保存するツールである cutycapt[16]により当該 URL にアクセスした際にブラウザに表示される画面のスクリーンショットを保存する．またルートページが HTML や Javascript によりリダイレクト処理される場合についてはリダイレクト先のページも調査する．なお，ネットワークスキャン中にスキャン対象の IP アドレス割り当てが変わり，スキャンされない場合や反対に複数回同一機器がスキャンされる可能性があることに留意する必要がある．

5.2 IoT 機器の判定

インターネット上には IoT 機器以外のホストによる Web サイトが多数存在しているため，5.1 節で発見した Web ページを持つホストの中から IoT 機器を選別する必要がある．本研究では 5.1 節で収集した情報を元に，以下の観点から選別を行う．

IoT 機器の画像有無：

収集した Web ページに IoT 機器の画像がある．

機器設定ページの有無：

収集した Web ページに IoT 機器のものと思われる設定項目や型番などの機器情報がある．

特定文字列の有無：

「システム」や「ルータ」など, 収集した Web ページに IoT 機器であることが推測できる単語がある

HTTP 応答ヘッダの Server フィールド：

HTTP 応答ヘッダの Server フィールドの値を見ると, Web サーバプログラムの名前やバージョンを確認することが出来る．一般的な Web サイトは Apache や IIS，nginx など広く利用されているサーバプログラムによりホスティングされていることが多いが，IoT 機器では組み込み用の Web サーバプログラムや IoT 機器メーカ独自の Web サーバプログラムが利用されていることが多いため，本フィールドから IoT 機器を判定できる場合がある．

上述の条件では未知の Web サイトの判定を自動で行うことは難しい. そこで提案手法では未知の Web サイトについては目視により判定を行う．ただし調査により既知となった Web サイトについては画像を登録し, 画像比較により類似度が低いもののみ未知の Web サイトとして扱うこと

で，目視による判定の負担を減らす．また，IoT 機器の WebUI の情報が十分に蓄積された後には，機械学習等により，目視による判定の代替を行うことを検討している．

5.3 Web UI の詳細な調査

前節で述べた手法により IoT 機器として判定したホストの Web UI に対して詳細に調査を行い，セキュリティ上の問題がないかどうか調べる. Web UI や他ポートで動作しているサービス（例：Telnet バナー）などから機器名が特定出来る場合は Web 検索エンジンにより当該機器のマニュアルの入手を試み，当該機器の Web UI がどのような機能を提供しているのか調査する．また Web UI にパスワード認証機能があった場合，初期パスワードが記載されていないかについても調査する．マニュアルが入手できない場合は Web UI の画面からどのような機能が提供されているのか推測する．また認証せずに機器の設定の変更や重要な情報が閲覧可能になっていないか調査する．

さらに機器によっては Telnet や Modbus など HTTP 以外のサービスが動作している場合がある．そのため 80/tcp 以外に対してもポートスキャンを行い調査を行う．なお，これらの機器の中にはルータを経由してインターネット接続を行っており，ルータのポートフォーワーディング機能により，外部から内部のこれらの機器のサービスへアクセスできるようになっている場合がある(図 2 参照). この場合，応答パケットの TTL 値から各サービスが動作する機器へのホップ数を推定し，機器の接続状況の推定を行う．

5.4 同一または類似機種の調査

前節で危険性が高いと判断した機器について，同一機種や類似機種がインターネット上に存在するかどうかを調査する．

5.4.1 ルートページが同じ Web UI の検索

アプリケーションスキャナである zgrab では 80/tcp ポートに対してルートページの HTTP Body の sha256 ハッシュ値を記録することができる．そのため検索したい機器と同一 Web UI を持つ機器をネットワークスキャン結果から容易に探すことが可能である. しかし本手法による検索では，HTTP Body が完全に一致している必要があるため同一機種による Web UI でも HTTP Body の一部が異なる場合（例えば，IoT 機器の設置場所の名前が HTTP Body に含まれている場合）は見つけることができない．

5.4.2 HTML のタイトルタグによる検索

IoT 機器によっては Web UI のタイトルが機種名になっていたり，特徴のあるものになっていることがあり，同じタイトルを持つものを Censys で検索することで同一機種や類似機種を見つけられる場合がある．

5.4.3 HTTP 応答ヘッダによる検索

5.2 節で述べたように HTTP 応答ヘッダの Server フィールドには，Web サーバプログラムやそのバージョン名が記述されているため，当該情報や他の HTTP 応答ヘッダを組み合わせて検索することで同一機種や類似機種を見つけられる場合がある．

6. IoT 機器の実態調査

提案手法により実際に IoT 機器の実態調査を行った．調査対象は攻撃への悪用を防ぐため明かさないこととする．調査対象のアドレス帯に対して zmap, zgrab により 2017 年 1 月にネットワークスキャンを行い，その結果 1,820,621IP アドレスから 80/tcp に対するスキャンの応答を確認し，そのうち 1,422,766IP アドレスから HTTP による何らかの応答を収集した．また調査対象アドレス帯のうち 2017 年 1 月 4 日から同月の 31 日までの期間に IoTPOT に対して不正ログインを試みた 331IP アドレスのホストをマルウェア感染 IoT 機器として扱う．調査の結果，表 2 に示すように脆弱性があると考えられる様々な IoT 機器を確認した．

以下では，調査により確認した事例を一部報告する．なお，調査により問題を確認した機器で深刻なものについては機器オーナや製造者に順次情報提供している．

表 2　調査により確認した機器

	脆弱性カテゴリ１ （マルウェア感染）	脆弱性カテゴリ２ （設定変更・ 情報アクセス）	脆弱性カテゴリ３ （機器存在露見）
重要度カテゴリ１ （重要機器）	流量計測装置*	水処理遠隔制御装置	ビル空調システム モノレール広告システム
重要度カテゴリ２ （重要機器以外）	ルータ カメラ NAS	ルータ カメラ NASなど多数	ルータ カメラ NASなど多数

*厳密には計測装置と同一 IP アドレスで動作している機器の感染を確認

6.1 ルータ

家庭用のブロードバンドルータや企業などの組織用の高性能ルータ，SIM カードなどを利用するモバイルルータなど多種多様なルータの Web UI がインターネットからアクセス可能になっている．多くのルータの Web UI は操作をするためにパスワード認証を行う必要があり，これらの機器のオーナが意図してインターネットからアクセス出来る状態にしている可能性も考えられる．しかし以下に述べる事例では攻撃者によりパスワード認証を突破される可能性がある．ルータの設定が攻撃者により変更された場合，当該機器に接続している LAN 内の機器がインターネット上に晒されたり，LAN 内の機器の通信先を悪意のあるサーバに誘導されることが考えられる．

A 社製のルータ(機器 1)は，工場出荷状態では認証なしに Web UI にアクセスすることが可能であり，ユーザの PPPoE 接続情報などを自由に閲覧することができ，設定も自由に変更できると推測される. ネットワークスキャンの結果，259IP アドレスに同一機種が割り当てられており，一部の機器については実際に認証機能が動作していないことを確認した．

B 社のモバイルルータ(機器 2)は，Basic 認証により Web

UI へのアクセスを制限している．しかし当該機器のマニュアルはインターネットから入手可能であり，工場出荷状態の認証情報が記載されている．また当該機器はデフォルトの設定では WAN 側からのアクセスが有効になっているため，パスワードを変更せずにインターネットに接続した場合，攻撃者により設定が変更される恐れがある．また当該機器はシャトルバスの車内インターネット接続サービスに利用されていることが判明している．ネットワークスキャンの結果 550IP アドレスに同一機種が割り当てられていることを確認した．

C 社のモバイルルータ 3 機種(機器 3, 4, 5)は上記の機器と同様にインターネットから入手可能なマニュアルに工場出荷状態における Web UI のユーザ名とパスワードが記載されている．さらにこれらの機器のユーザ名は固定されており変更することができず，また機器 3, 機器 4 についてはパスワードを 4 桁の数字にしか設定できない．ユーザ名が固定されておりパスワードの組み合わせ数が少ないことから，仮にユーザがパスワードを変更しても攻撃者に認証を突破される恐れがある．ネットワークスキャンにより 2379IP アドレスに同一機種が割り当てられていることを確認した．また当該機器はファームウェアのバージョンを更新することでデフォルトの設定ではインターネットからアクセス出来なくなることを確認している．

6.2 Web カメラ

様々な Web カメラの映像が任意のアドレスから閲覧できる状態になっていることが知られており，Insecam[17]ではそのような Web カメラの情報が公開されている．本研究においても同様な状態にある Web カメラを多数発見している．さらに IoTPOT による観測結果から，マルウェアに感染している思われる機器も確認した．Web UI や Telnet バナーからこれらのカメラの型名を特定できなかったが，HTML のタイトルに特徴があり，当該特徴を持つ 50IP アドレスから IoTPOT への不正ログインを確認した．ネットワークスキャンの結果 1,115IP アドレスに同一または類似機種が割り当てられており同様にマルウェアに感染している可能性がある．

6.3 重要機器

E 社の制御機器(機器 7)はアナログ・デジタル信号や PLC を Web ブラウザで遠隔から管理する機能を提供する機器である．当該機器のマニュアルは本機器の Web UI 上で閲覧可能であり，マニュアルには Web UI にアクセスする際に必要な工場出荷状態の Basic 認証情報が記載されている．またマニュアルから本機器には Linux OS が搭載されており，Basic 認証後は Web UI から任意のコマンドを実行したり，接続されている PLC に対してデータを送信出来ることが分かる．ネットワークスキャンにより 171IP アドレスに同一機種が割り当てられていることを確認した．

F 社の制御機器(機器 8)は上記機器と同様に信号の入出力や PLC 機器の管理をする機能を提供する機器であり，当該機器のマニュアルには工場出荷状態の認証情報が記載されている．ネットワークスキャンの結果 101IP アドレスに同一または類似機種が割り当てられており，発見した全 IP アドレスについてルートページに認証なしでアクセス可能であり，そのうち 46IP アドレスについてはルートページに機器の設置先と思われる，実在する浄水場や発電所，ダムなどの情報が表示される状態であることを確認した．これらの機器の Web UI から機器を遠隔操作する機能は確認できなかったが，一部の機器については HTTP の他に別ポートで産業制御用のサービスも動作しており，当該サービスは仕様上認証機能をもたないことから外部から機器を不正に操作される恐れがある．これらの機器はルータを経由して接続を行っており，ルータのポートフォーワーディングにより外部から内部機器へのアクセスを可能としているが，このルータの Web UI にもアクセスが可能な上，デフォルトの認証情報がマニュアルに記載されていることから，パスワードを変更していない場合，LAN 内の機器も攻撃の対象となる可能性がある．

G 社の計測機器(機器 9)は工場や発電所などで使用される機器であり，文献[13]により産業制御用サービスが動作していることが指摘されており，著者らの調査においても 112IP アドレスに同一機種が割り当てられ，当該サービスが動作していることを確認している．さらに IoTPOT による観測により，当該機器が割り当てられている 15IP アドレスからの不正ログインを確認した．当該機器が割り当てられている IP アドレスについて調査したところ，マルウェア感染経路として悪用されることが多い Telnet が動作していることを確認した．しかしポート番号ごとの IP ヘッダの TTL 値の比較をしたところ，HOP 数が異なっており，図 2 に示すように機器 9 とは別の，ルータなどの接続用機器がマルウェアに感染しているものと推測できる．

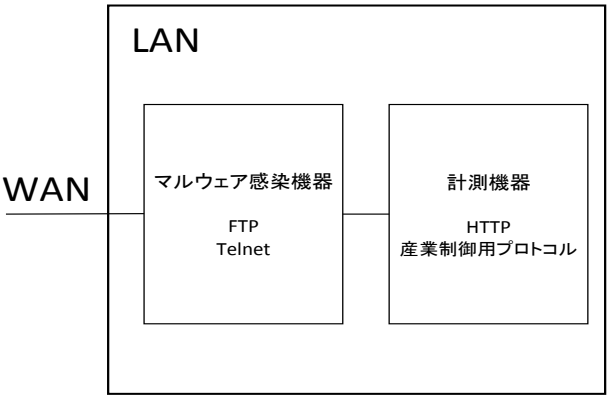

図 2　推測されるネットワーク構造

7. 考察

前章で挙げた事例から，様々な IoT 機器の Web UI がイ

ンターネットからアクセス可能な状態になっていることが分かる．しかしその全てに問題がある訳ではなく，IoT 機器のオーナが意図してインターネット上に公開している場合も考えられる．本研究により発見した Web UI がオーナが意図して公開してるものかどうか判断することは難しいが，機器の情報を閲覧できるだけでなく，機器の設定変更などの操作が可能な Web UI を提供しているにも関わらず，ユーザ認証が脆弱であったり，そもそも認証機能が存在しない Web UI がインターネット上に公開されていることは問題である．また前章で挙げたモバイルルータは同一機種であってもファームウェアのバージョンによってはインターネットからアクセスできず，製造者側がファームウェア更新時にアクセス制御の修正を行っていることがわかる．

今回発見した問題を防ぐためには，機器の製造者が初期設定では WAN 側からのアクセスを遮断するようにするなどして，機器のユーザの意図に反してインターネットに Web UI が晒されないようにすることが重要である．またインターネットから機器の Web UI にアクセスする使用方法を想定している場合には，機器ごとに工場出荷状態のパスワードを異なるものにしたり，機器の初期利用時にユーザにパスワードの変更を促すなどして，ユーザ認証が容易に突破されないように注意して設計する必要がある．

機器流通後に脆弱性が発覚した場合でもファームウェアの更新により脆弱性を取り除ける場合もあるが，ファームウェアの更新には機器管理者による操作が必要なことが多いため，機器管理者への連絡手段の確保も重要である．

またマルウェア感染機器については Telnet が主な感染経路だと考えられるが，Telnet が動作しているにも関わらずマニュアルや仕様書にその旨が記載されていない機器も存在しており，ユーザが問題に気づくことは難しいと考えられ，Web UI と同様に製造者側の対応が重要である．

8. まとめと今後の課題

本稿ではネットワークスキャンによる能動的観測とハニーポットによる受動的観測による，インターネット上に公開されている IoT 機器のセキュリティ状況を把握する手法を提案した．また調査の結果 IoT 機器による様々な Web UI がインターネットからアクセス可能であることや，その中でもセキュリティの観点から重要と思われる事例を報告した．

本研究による調査では Web サーバとして動作しているホストの探索やそのコンテンツの収集の過程までは自動で行えているものの，それ以降の処理については人手によるものが多いため，提案手法の自動化を今後の課題としたい．

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．

参考文献

[1] “Mirai: New wave of IoT botnet attacks hits Germany”. http://www.symantec.com/connect/blogs/mirai-new-wave-iot-botnet-attacks-hits-germany, (参照 2017-02-04).
[2] “Source Code for IoT Botnet ‘Mirai’ Released” . https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/, (参照 2017-02-04).
[3] “DDoS on Dyn Impacts Twitter, Spotify, Reddit” . https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/, (参照 2017-02-04).
[4] “新しい「Mirai」、ルータを狙うポート 7547 への攻撃が示す今後の脅威” . http://blog.trendmicro.co.jp/archives/14108/, (参照 2017-02-09).
[5] “LuaBot: Malware targeting cable modems” . https://w00tsec.blogspot.jp/2016/09/luabot-malware-targeting-cable-modems.html, (参照 2017-02-09).
[6] Yin Minn PaPa and Suzuki, S., et al.. IoTPOT: A Novel Honeypot for Revealing Current IoT Threats. Journal of Information Processing, 2016, 522-533.
[7] “nmap” . https://nmap.org/, (参照 2017-02-07).
[8] Durumeric, Z., Eric W., and J. Alex, H.. ZMap: Fast Internet-wide Scanning and Its Security Applications. Usenix Security. Vol. 2013. 2013.
[9] “zmap” . https://zmap.io/, (参照 2017-02-07).
[10] “MASSCAN: Mass IP port scanner” . https://github.com/robertdavidgraham/masscan, (参照 2017-02-07).
[11] Durumeric, Z., Kasten, J., et al.. The matter of heartbleed. Proceedings of the 2014 Conference on Internet Measurement Conference. 2014, ACM, p. 475-48.
[12] “OpenSSL の脆弱性に関する注意喚起” . https://www.jpcert.or.jp/at/2014/at140013.html
[13] Ariana, M., Zane, M., et al.. An Internet-Wide View of ICS Devices. 4th Annual Privacy, Security and Trust Conference (PST), Auckland, 2016.
[14] “Shodan” . https://www.shodan.io/, (参照 2017-02-07).
[15] “Censys” . https://censys.io/, (参照 2017-02-07).
[16] “CutyCapt - A Qt WebKit Web Page Rendering Capture Utility” . http://cutycapt.sourceforge.net/, (参照 2017-02-07)
[17] “Insecam”. https://www.insecam.org, (参照 2017-02-07).