情報処理学会論文誌 Vol.60 No.3 849–858 (Mar. 2019)

WebUIの画像的特徴に基づくIoT機器判別手法

藤田 彬[1,a)] 内田 佳介[2] 森 博志[2] 吉岡 克成[1,3] 松本 勉[1,3]

受付日 2018年6月8日, 採録日 2018年12月4日

概要：近年 IoT 機器を狙ったサイバー攻撃が高度化・広範化の一途をたどっており，IoT 機器の利用状況および設定状況，セキュリティ対策の実態をインターネットから観測するための広域ネットワークスキャン技術および機器種別・機器名の特定技術の重要性が高まっている．本研究では，Web サービスが稼働するネットワーク機器を対象に，WebUI の画像的な特徴に基づいて効率的に IoT 機器のホストを検出する手法の構築を試みる．広域ネットワークスキャンにより取得した WebUI のスクリーンショット画像に対してクラスタリングを行い，多くの IoT 機器の WebUI 画像を含むクラスタを検出する．実験の結果，本手法により，同一または類似する機器の WebUI 画像が同一のクラスタに凝集する傾向にあることが分かった．本手法はサイバー攻撃の対象となりうる IoT 機器の早期発見と対策の実施を行ううえで有効といえる．

キーワード：IoT，能動的観測，WebUI，perceptual hash，階層的クラスタリング

A Method to Find IoT Devices Based on Image Features of Their WebUI

Akira Fujita[1,a)] Keisuke Uchida[2] Hiroshi Mori[2]
Katsunari Yoshioka[1,3] Tsutomu Matsumoto[1,3]

Received: June 8, 2018, Accepted: December 4, 2018

Abstract: In recent years, cyber-attacks targeting IoT devices are becoming a major threat. A technique of wide network scanning for investigating the usage and security status of IoT devices and identifying product names or types of IoT devices are increasingly important. In this research, we aim to construct a method to efficiently detect IoT devices hosts based on image features of its WebUI, from network devices on which Web services run. We utilize hierarchical clustering for screenshot images of WebUIs captured by wide network scanning to find out IoT devices. Our experiment shows that WebUIs of similar IoT devices can be clustered in to the same group by our method and variety of devices can be identified by manually investigating these clusters. The proposed method is effective for identification of IoT devices in large network.

Keywords: IoT, active monitoring, WebUI, perceptual hash, hierarchical clustering

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 [1], [2]．Telnet をはじめとした様々なネットワークサービスの脆弱性を狙った攻撃が増加し，これにともないマルウェアに感染した機器が増加している [3]．IoT 機器におけるセキュリティ対策の状況を調査した先行研究 [4] では，インターネットに接続された IoT 機器ホストの Web ユーザインタフェース（以下，WebUI）が，任意のホストからアクセス可能な状態になっていた事例が報告されている．それらの事例には，ルータや Web カメラ等の一般的な IoT 機器に限らず，ダムや発電所等重要なインフラ設備で運用されているものと考えられる産業用制御機器も含まれる．このような機器の WebUI においては，機器の名称や種別，場合

[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

によっては設置場所を特定しうる情報が公開されていることがある．これらの情報は攻撃者の興味を引く可能性があり，ひいては攻撃手段の選定，最適化を行う糸口となる恐れがあるため，公開することには一定の危険がともなうといえる．もし攻撃者が機器の特定に成功すると，少なくとも当該機器における既知の脆弱性を調べることができる．いうまでもなく，機器についての情報が与えられる前と比較すると，機器が何らかの侵入もしくは改ざん等の攻撃を受ける危険性は高まる．機器運用上特段の必要がない限り，IoT 機器のような使途の機器の WebUI は，関係者外に公開しないか何らかのアクセス制限を設ける方が安全といえる．しかしながら，機器の WebUI がインターネットに公開されていたとして，エンドユーザがその状況を能動的に察知する可能性は低いと考えられる．この場合においては，エンドユーザはまず自機器に割り当てられたグローバル IP アドレスを知り，その上で Web ブラウジングやポートスキャン等の手段を用いて自機器の公開状況を検証する必要がある．十分なリテラシーを有するエンドユーザであれば当該検証作業を行ったうえで察知可能であるが，エンドユーザのリテラシーによっては看過されやすいものと考えられる．機器製造者が初期設定として WebUI をインターネットに公開する設定を行っていた場合，当該設定のまま運用されるケースが多いものと見込まれる．このことから，WAN 側からの機器の観測状況と観測状況に対応してとるべき対策がエンドユーザからみて受動的かつ解釈が容易な形式で通知される枠組みを実現することが望ましいといえる．

本研究では，WAN 側からの機器の観測状況と観測状況に対応してとるべき対策をエンドユーザが認識するまでの間に，1) 他者による機器の発見，2) 発見した機器の状況分析，3) エンドユーザへの対策の通知という手順のシナリオを想定したうえで，「1) 機器の発見」の方法を検討する．このシナリオのうち，2) 発見した機器の状況分析および 3) エンドユーザへの対策の通知は，自動化が難しく，大半において人間のインテリジェンスに頼る必要があるものと考える．多くの場合機器上で動くサービスは機器により異なり，同種の機器において同一のサービスが動作している場合でもサービス中の一部の機能を特別に使用しているもしくは使用していない場合がある等，個々の事例における例外的状況に対する判断を行う必要がある事例が存在することから，機器の状況分析の自動化は難しいといえる．発見した機器の情報からエンドユーザとのコンタクトポイントを得るまでのアプローチは，当該機器のメーカが顧客情報を所有しているか否かによって，2 通り考えられる．発見した機器が産業用制御機器等ベンダを介して業者に販売されるような IoT 機器である場合は，おおむね機器メーカ側が顧客情報を所有している．この場合，当該機器について広域的に観測された設定不備や脆弱性に関する情報をメーカに通知し，メーカが顧客情報をたどりエンドユーザもしくは機器を購入・設置したベンダに対処方法を伝えるというフローが考えられる．一方で，小売店でエンドユーザに直接販売されるような民生用の IoT 機器は，メーカ側が顧客情報を詳細に把握していないことが多く，メーカ経由でのエンドユーザへの通知は不可能と考えられる．このような場合，公的に WAN 側からの調査を実施する機関がエンドユーザの契約回線を管理する ISP 事業者に問い合わせ，ISP 事業者経由でエンドユーザに対策の通知を行うという経路が考えられる．これら 2 通りのフローにおいてエンドユーザに通知する対処方法としては，「メーカが作成した機器ファームウェアのアップデートファイルの入手方法およびアップデート手順」「セキュリティ上望ましい機器設定への変更方法」等が共通してあげられるが，いずれのフローにおいても，調査主体は事前に機器メーカと対策を検討し，あらゆるリテラシーレベルのエンドユーザが対処方法を正確に解釈できるような通知内容を作成したうえで，対応がとられやすい通知手段を講じる必要がある．

このように機器の状況分析や機器設定の不備や脆弱性に関する通知は，特に人間のインテリジェンスを介したうえで行われるべき対処過程であるといえる．調査主体が通知のフェーズにインテリジェンスを集中できるよう，そのほかのフェーズが極力自動的に行われる環境が望ましい．特に，機器がどのような経路で販売される類のものであるかを含め，機器の種類に関する情報が自動的に提供されるような仕組みは有用といえる．そこで，WAN 側からのスキャン結果に基づいて，エンドユーザが所有する IoT 機器の存在および機器の種類に関する情報を正確かつ効率的に得るための手法を提案する．

インターネット上の WebUI の大半は，IoT 機器のように特定の機能のみを提供する機器ではない汎用サーバ機器で稼働する一般的な目的のものであり，IoT 機器上で稼働するものはごくわずかである．これらをすべて人手で判別することは現実的といえず，何らかの自動的な判定機構もしくは推定機構が必要となる．しかしながら，ある WebUI が IoT 機器のものであるか否かを識別するルールの構築は困難である．用いられる Web サーバソフトウェア等に両群間で明確な違いが存在せず，少なくとも，HTTP レスポンスにおけるメタ的な情報のみから両群を識別することは不可能といえる．他方で人の目でブラウジングする状況において IoT 機器の WebUI は，他の一般的な目的で公開された WebUI と比較して視覚的に弁別可能なページレイアウト上の共通した特徴を有すると考えられる．このページレイアウトの違いは，ソース記述上では小さな違いであることが多いが，Web ブラウザ上にレンダリングされたイメージにおいては明確な違いとして認識可能なものである．

本研究では，広域スキャンにより得られる莫大な Web コンテンツ群の中から，IoT 機器の WebUI をその画像的特

徴に着目して判別する手法を提案する．提案手法は同一または類似 IoT 機器の WebUI が視覚的に類似したレイアウトデザインであると仮定し，WebUI のレンダリング画像のクラスタリングを行うことで IoT 機器を判別する．具体的には，広域スキャンによって収集した Web コンテンツから，トップページ画像を抽出し，それらを perceptual hash の 1 種である Average Hash に変換したうえで階層的クラスタリングによって分類する．評価実験では，日本国内のある単一 AS の IP アドレスレンジにおける広域スキャンにより収集された全 14,744 枚のトップページ画像が 1,707 個のクラスタに分割された．全 1,707 クラスタについてそれぞれサンプリングの上，各クラスタに含まれる一部の要素（トップページ画像）について人手での検証を行ったところ，1,707 個のうち 138 個のクラスタについては 50%以上の要素が同一または類似の IoT 機器の WebUI であると判定された．具体的には，カメラ，NAS，ルータ，産業用制御機器等，少なくとも 8 種類のカテゴリにまたがる 136 種類の機器が発見された．提案手法は膨大な Web コンテンツ群の中から IoT 機器を発見する方法として利用できると考えられる．

以下では，2 章で関連研究について，3 章で提案手法の詳細について，4 章で提案手法による IoT 機器の WebUI の検出効率の評価実験およびその結果について，5 章で 4 章における実験結果についての考察をそれぞれ述べる．

2. 関連研究

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等の特定の機能のみを提供する機器を IoT 機器と呼ぶこととする．たとえば，IoT 機器には，ブロードバンドルータや NAS 等一般家庭向けの機器だけでなく，工場や病院等で使用される産業用制御機器も含まれ，その種類は多岐にわたる．そのような IoT 機器のセキュリティ状況を，広域スキャン技術を用いた能動的観測とハニーポットによる受動的観測により調査した先行研究 [4] では，手動で IoT 機器の判定を行っていたため，人的コストが高く，実用的な調査手法ではなかった．そのため，IoT 機器のセキュリティ状況の調査手法の自動化・効率化が求められる．

広域的にポートスキャンを実施し，スキャン結果を蓄積する試みとして，Censys [5] および SHODAN [6] があげられる．Censys は，本研究と同様に，ZMap [7] および Zgrab [7] を用いてポートスキャンと Web サービスのコンテンツ取得を行う．SHODAN は独自の手法を用いており詳細は不明である．両手法ともスキャン結果をデータベース化し，同データベース内をフリーワードで検索する機能をユーザに提供している．ユーザが何らかの IoT 機器の存在を知りそれらの機器種別もしくは機種名を知るためには，あらかじめ当該機器の何らかの特徴をユーザが認識している必要がある．一方，本研究による手法では，ユーザが機器の特徴を事前に知る必要がなく，またどのような機器を発見しようとしているかを知らなくても，スキャン結果から WebUI の構成が互いに類似した機器の群を自動的に抽出することで，未知の機器を発見できる．

そのほかにも，広域スキャン技術を用いて IoT 機器のセキュリティ状況を調査・把握する試みが行われており [8], [9]，主に機器別のポート待ち受け状態の特徴に着目した分析を行っているが，本研究では特徴的なポート待ち受け状態に頼らず機器の WebUI の画像的特徴のみから IoT 機器判定を試みる．

また，類似画像検索サービスや UI の利便性向上を目的に，Web ページ上に存在する画像を階層的クラスタリングによって分類する研究が報告されており [10], [11]，画像的特徴だけでなく HTML 等から取得したテキスト情報等様々な観点で画像分類を行っている．本研究では，同一または類似 IoT 機器が備える WebUI のレイアウトが類似しているケースが多い点に着目し，IoT 機器にターゲットを絞り画像的特徴のみを用いて分類を試みる．

3. 提案手法

提案手法の処理手順を**図 1** に示す．本手法では，まず対象となる IP アドレスに対してポートスキャンを行い，Web サービスのデフォルトポートである 80/tcp についてセッションが確立できるホストの IP アドレスを絞り込む．絞り込んだ IP アドレスに対して，トップページのスクリーンショット（以下，トップページ画像）を収集する．収集した画像を，Perceptual Hash [12] に入力して画像のハッ

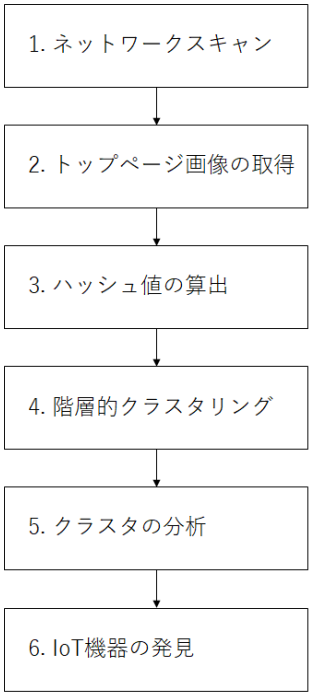

図 1 提案手法の処理手順
Fig. 1 Procedure of proposal method.

シュ値を得る．Perceptual Hash はファジーハッシュアルゴリズムの 1 種で，出力したハッシュ値の間でハッシュ値間の距離を算出可能なハッシングアルゴリズムである．次に，ハッシュ値を用いて教師なし学習の 1 種である階層的クラスタリングによって，トップページ画像を分類する．最後に，得られたクラスタ中の要素に対して，サンプリングを行ったうえで人手による判定を行い，同一または類似 IoT 機器が高い割合で存在するクラスタを推定し，当該クラスタについて詳細に調査することで効率的に IoT 機器の WebUI を発見する．以下では，各手順の詳細を述べる．

3.1 ネットワークスキャンおよびトップページ画像の取得

インターネットからアクセス可能な状態に設定された IoT 機器の WebUI を発見するために，調査対象の IP アドレスレンジについて，HTTP サービスのデフォルトポートである 80/tcp ポートに対して，ミシガン大学の研究チームが開発した高速ポートスキャンツール「ZMap [7]」を使用してポートスキャンを行う．なお，8080/tcp，81/tcp 等，他の TCP ポートについても Web サービスが稼働している事例があり，これらが IoT 機器ホストであることも多い．しかしながら，IoT 機器以外の一般的な Web サーバの WebUI が大半を占める画像セットから IoT 機器の WebUI 画像を抽出し，IoT 機器の発見作業の効率化を議論することが本研究の目的であることから，他の Web サービスポートと比べて一般的な Web サーバが稼働していることが多い 80/tcp を選び，探索対象とする．

次に，ポートスキャン結果のうち，HTTP サービスとの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トップページのコンテンツを収集する．本研究では，下記の URL で Web サーバにリクエストを送信した際に返されるディレクトリインデックスのファイルを，トップページと呼ぶこととする．

http://調査対象ホストの IP アドレス/

トップページのコンテンツ収集にはアプリケーションレイヤスキャンツール「Zgrab [7]」を用いる．Zgrab により HTTP ボディや HTTP ヘッダの情報を収集する．また同時に，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 [13]」を用い，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．画像取得時には，広告画像やロゴ等の IoT 機器の WebUI ではない可能性を示す素性となる情報を失わないように，横幅ピクセル数の最小値を 800 px，縦幅ピクセルの最小値を 600 px に設定してキャプチャを実行する．トップページが 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対象とする．なお，スキャン対象が動的 IP アドレスを用いている等の要因により，ネットワークスキャン中にスキャン対象の IP アドレスの割当てが変わりスキャンが実施できない場合や，複数回同一機器がスキャンされる可能性がある．

3.2 ハッシュ値の算出

3.1 節における処理過程で取得したトップページ画像を，Perceptual Hash の 1 種である Average Hash アルゴリズム [14] に入力し，画像のフィンガープリントとなる 64 bit のハッシュ値を算出する．このハッシュ値は，ハッシュ値間の Hamming 距離を計算可能で，当該距離を画像間の視覚的な非類似度としてとらえることができる．

提案手法における入力には，一般的な Web ページでみられる縦方向にスクロールして閲覧する類の縦長レイアウトの縦横比を持つ画像が想定される．一方で，IoT 機器の WebUI はスクロールが不要な 1 : 1 に近い縦横比を持つことが多いと考えられることから，8×8（$= 64$ bit）のハッシュ値を出力することとする．なお，試行的に 8×8 px の分割数をより高い分割数としたところ，ハッシュ値算定にかかる計算時間が大幅に増加することが分かった．このことから実行コストとのトレードオフに鑑みて，分割数を 8×8 px にとどめることとした．

3.3 階層的クラスタリング

算出した各トップページ画像のハッシュ値を入力とし，階層的クラスタリングによってトップページ画像の分類を行う．具体的には，入力データ間の距離（非類似度）を Hamming 距離，クラスタ間の類似度を Single-linkage 法 [15] により定義することで，クラスタ間の階層的関係を表すデンドログラム（樹状図）を得る．

これまで提案されてきたクラスタリング手法には，大別して階層的クラスタリングと非階層的クラスタリングの 2 種がある．このうち非階層的クラスタリングについては，代表的なものに k 平均法があげられる．事前調査として本研究における入力画像群に k 平均法を適用すると，出力するクラスタ数を小さく設定した際に，出力クラスタの要素数が人手で確認することが現実的でないほどの大きさとなることが分かった．また，出力するクラスタ数を大きく設定しても，出力クラスタ内に IoT 機器の WebUI の画像が含まれる割合が全体的に低い傾向にあることが分かった．この事前調査の結果より，非階層的クラスタリングは用いず，階層的クラスタリングアルゴリズムを適用することとする．

3.4 クラスタの分析

階層的クラスタリングは，入力した要素がすべて個別のクラスタに属する状態から，クラスタ間の距離に基づいてクラスタどうしを結合していき，最終的には 1 つのクラスタにまとめるアルゴリズムであるが，この過程のいずれかのうちクラスタの分類状況が最も有意な状態を選択する必

要がある．提案手法では，ヒューリスティックに基づき，「初めに定める k 種類の画像（以下，シード画像）を含むクラスタ（以下，シードクラスタ）がいずれも互いに別のクラスタとして分類される状態において，各シードクラスタの要素数が最も大きい状態」を最も有意な分類状態とする．この分類状態においては，各クラスタに集まった要素（画像）どうしの類似性が全体的に高く，かつ類似性の低い画像の混入程度も小さいと見込まれる．

全クラスタリング過程の中から最も有意な分類状態を選択し，要素数が 2 以上となるクラスタすべてについて各クラスタにつき 10 個の要素をランダムに抽出し，IoT 機器の WebUI が 50%以上の確率で含まれるクラスタを判定する．クラスタ内の要素が 10 個未満の場合は，全要素を抽出して判定を行う．

このようにして得られた「IoT 機器の WebUI が 50%以上の確率で含まれるクラスタ」に含まれる画像を 1 データずつ確認することで，詳細に調査を行い，効率的に IoT 機器を発見する．IoT 機器の WebUI の判定は以下の基準に基づいて人手で行う．

- IoT 機器と判断される機種名，型番等が記載されている（基準 a）．
- “ルータ”，“NAS” 等，IoT 機器と推測できる情報が記載されている（基準 b）．

具体的には，Web ページのタイトル，ヘッダ部，フッタ部を参照したうえで，文ではない単独の文字列（以下，候補文字列）が存在するか否かを確認する．基準 a については，候補文字列が英数字および記号の羅列である場合は型番を示すもの，候補文字列が造語と思われる語を含む場合は機器シリーズの名称であると推測する．その後型番もしくは機器シリーズの名称と推測される文字列をクエリとして Web 検索を実行し，検索結果に該当する機種が存在するかを確認し，その機種が IoT 機器であるか否かを判断する．また基準 b については，候補文字列中に機器の種類を示す一般名詞が含まれるかを調べ，含まれる場合はその一般名詞が指す意味から IoT 機器であるか否かを判断する．

予備調査として，提案手法によりスキャン・保存した画像の中から，1 名の分析者が上記の基準に沿って IoT 機器の WebUI 画像と思われる画像および IoT 機器の WebUI 画像ではないと思われる画像をそれぞれ同数ずつとなるよう，計 100 枚（50 枚 × 2 カテゴリ）無作為に抽出した．その後，他の 1 名の分析者が同じ判定基準に沿って上記 2 カテゴリの判定を行ったところ，100 枚を抽出した 1 名と後で判定を行った 1 名の間で，すべての判定結果が一致した．このとき，100 枚の画像を抽出した 1 名による判定結果，および IoT 機器と判定された画像とそうでない画像が半分ずつ含まれることは，後で判定を行った 1 名に提示しなかった．このことから，当該判定基準について，個人間で判断に違いが生じることは稀であると考えられる．

当該判定基準は，基準に合致した画像に対応するホストが IoT 機器であることを示す基準であるが，実インターネット空間におけるすべてのタイプの IoT 機器の WebUI 上の特徴を網羅的にまとめたフィンガープリンティングルールではない．実際には，機器や型番等の特徴が WebUI 上に表記されない IoT 機器ホストや，IoT 機器であることを示す特徴の情報を WebUI 上に記載しないホスト，Web サービスを提供しない IoT 機器ホストが多く存在するが，本研究ではこれらを抽出対象の範囲外とする．

4. 評価実験

提案手法の有効性を検証するため，APNIC により日本国内に割り当てられたアドレス帯のうち，ある単一 AS の IP アドレスレンジをスキャンして得られたトップページ画像 14,744 枚を対象に評価実験を行った．なお当該 AS の IP アドレスレンジには，他の AS と比べて多くの IoT 機器ホストが存在する傾向にあることが人手での事前調査により判明している．

4.1 実験概要

提案手法により，対象画像 14,744 枚に対してクラスタリングを行った．出力されたデンドログラムに対しては，分析者が対象画像中からそれぞれ異なるクラスタに分類されると想定する IoT 機器の WebUI 画像を $k = 10$ 種類選択し，3.4 節で述べた方法によりクラスタを得た．先行研究 [4] における日本国内へのポートスキャンでは，「ネットワークカメラ」「ルータ」「NAS」等 10 種の機器種別に分類できる機器の WebUI が発見された．この結果より，日本国内のネットワークレンジでは少なくとも 10 種類の機器種別のホストからの応答が見込まれると想定し，この 10 種の機器の WebUI 画像をシード画像とした．

次に，得られたクラスタに対し，以下の 7 項目について調査を行った．

(1) 全クラスタ数
(2) (1) のうち，要素数が 1 であるクラスタ数
(3) (1) のうち，要素数が 2 以上であるクラスタ数
(4) (3) のうち，同種または類似 IoT 機器の WebUI の画像が 50%以上を占めるようなクラスタ数
(5) 要素数が 1 であるクラスタについて，IoT 機器の WebUI である割合
(6) 対象画像全体において IoT 機器の WebUI の画像が占める割合
(7) (4) を調査する過程において発見された IoT 機器の種類数

人手による判定の負担を軽減するため，(4) を調査する際に，要素数が 10 以上のクラスタについては 10 個の要素をランダムにサンプリングし，(5)，(6) においてはそれぞれ対象から 100 個をランダムにサンプリングして調査を

行った．後述のとおり，要素数が 1 であるクラスタは 1,331 個あり，対象画像は全体で 14,744 枚である．これらをそれぞれ母集団として要求精度 10%，信頼率 95%の設定でランダムサンプリングすることを考えると，必要サンプル数は要素数が 1 であるクラスタについては 90 個，対象画像全体については 96 枚である．そこで，それぞれ必要数を上回る 100 個をランダム抽出することとする．

さらに以下の 5 項目について調査を行った．以下では，要素数が 2 以上のクラスタを陽性画像クラスタ，要素数が 1 のクラスタを陰性画像クラスタとして表記する．

- 真陽性率：陽性画像クラスタに IoT 機器の WebUI 画像が含まれる割合
- 偽陽性率：陽性画像クラスタに IoT 機器の WebUI 画像以外の画像が含まれる割合
- 偽陰性率：陰性画像クラスタに IoT 機器の WebUI 画像が含まれる割合
- 探索効率 A：陽性画像クラスタを調査したときに IoT 機器の WebUI 画像を発見する期待値の相加平均
- 探索効率 B：陽性画像クラスタのうち IoT 機器が 50%以上を占めるクラスタを調査したときに IoT 機器の WebUI 画像を発見する期待値の相加平均

後述のとおり，陽性画像クラスタが 376 個，陰性画像クラスタが 1,331 個あるため，要求精度 10%，信頼率 95%の設定下で，それぞれ陰性画像クラスタについては 90 個，陽性画像クラスタについては 77 個のクラスタを各母集団からランダムにサンプリングする必要がある．そこでそれぞれの必要数を上回る 100 個ずつのクラスタをそれぞれの母集団から抽出して，各数値を算出することとする．また，探索効率 B を算出する際には，3.4 節に示した方法に基づいて，IoT 機器が 50%以上を占めるクラスタを推定する．なお，偽陰性率と (5) の算出方法は同一である．

4.2 実験結果

本実験の結果を**表 1** に示す．(1) 14,744 枚の対象画像が 1,707 個のクラスタに分割され，(2) そのうち要素数が 1 であるものは 1,331 個，(3) 要素数が 2 以上であるものは 376 個であった．特に，(4) 同一または類似 IoT 機器が 50%以上と判定されたクラスタは 138 個であり，全クラスタ数 1,707 と比較して，少数のクラスタに同一または類似 IoT 機器が凝集していることが分かった．これら 138 個のクラスタに含まれる画像はすべてで 2,773 枚である．当該クラスタ群に含まれる画像は最終的に人手で確認する必要のあるセットであることから，提案手法を用いることで，人手ですべてを調査すべき対象画像がおよそ 19%に（全画像 14,744 枚から 2,773 枚まで）縮小されたととらえることができる．要素数が 1 である 1,331 個のクラスタは，他の画像と類似しないものと判断できる．(5) これらが IoT 機器の WebUI の画像である割合は 12%であり，(6) 対象画像全体に含まれる IoT 機器の割合である 34%の半分以下の数値になっていることからも，相対的に IoT 機器の WebUI が同一クラスタに凝集していることが確認でき，階層的クラスタリングによる分類が有効であることが分かる．

要素数が 2 以上のクラスタ（陽性画像クラスタ）と要素数が 1 のクラスタ（陰性画像クラスタ）を 4.1 節に示した方法でサンプリングした結果，陽性画像クラスタのサンプル 100 個には 1,158 枚，陰性画像クラスタのサンプル 100 個には 100 枚の画像が含まれた．これらの画像群に関して，真陽性率および偽陽性率，偽陰性率，探索効率 A，探索効率 B を算出すると，真陽性率が 85%，偽陽性率が 15%，偽陰性率が 12%，探索効率 A が 8.83，探索効率 B が 19.97 となった．

また，(7) 本実験を通してルータ，NAS，産業用制御機器等を含む少なくとも 8 種類のカテゴリにまたがる 136 種類の IoT 機器が発見された．その内訳を**表 2** に示す．なお，これら 136 種類の IoT 機器の WebUI 画像の一部については，異なる種類の機器の画像が同じクラスタに分類されるケースがみられた．

本実験によって得られたクラスタの分布を**図 2** に示す．図 2 において，円は各クラスタを表し，円の大きさは当該

表 1 評価実験の結果
Table 1 Result of the evaluation experiment.

(1)	1,707 個
(2)	1,331 個
(3)	376 個
(4)	138 個
(5)	12%
(6)	34%
(7)	136 種類
真陽性率	85%
偽陽性率	15%
偽陰性率	12%
探索効率 A	8.83
探索効率 B	19.97

表 2 発見された IoT 機器の内訳
Table 2 Detail of found IoT devices.

機器カテゴリ	種類数
ネットワークカメラ	58
ルータ	20
NAS	15
NVR	15
遠隔監視機器（電力モニタ等）	11
産業用制御機器	6
セキュリティアプライアンス	2
コピー機	2
その他	7
合計	136

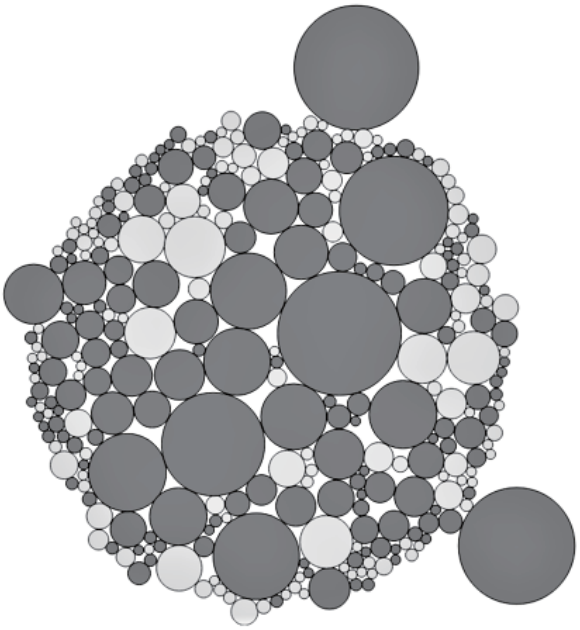

図 2 クラスタの大きさの分布（濃色：同一または類似 IoT 機器が 50%以上含まれるクラスタ，淡色：同一または類似 IoT 機器が 50%未満のクラスタ）

Fig. 2 Distribution of cluster size.

クラスタに含まれる要素数を表す．また，濃色で表したクラスタは同一または類似 IoT 機器が 50%未満の割合で含まれるクラスタで，淡色で表したクラスタはいずれも同一または類似 IoT 機器が 50%以上の割合で存在するクラスタである．なお，クラスタリングの対象となった 14,744 枚の画像においては，HTTP のエラー応答ページおよび空白のページ（HTML の body タグ内が空白），Web サーバのテストページの画像が多く含まれ，それぞれ大きなクラスタを形成したが，図 2 ではそれらのクラスタを除外して示す．

実験の結果得られたクラスタの多くは，要素数が 2 や 3 となる小さなクラスタであり，このようなクラスタに多くの IoT 機器の WebUI 画像が凝集していることが分かる．要素数が 200 を超えるような巨大なクラスタには，個体数が多いカメラ，ルータ，NVR といった IoT 機器の WebUI 画像が凝集しているが，これらと同程度の数の遠隔監視機器が発見されていることは特筆すべき点である．

5. 考察

4 章の結果から，同一または類似 IoT 機器の WebUI 画像が同一クラスタに凝集する傾向が強く，そのようなクラスタを優先的に調査することで，効率的に IoT 機器を発見可能であることが分かった．

提案手法によるクラスタリングを経ない場合，14,744 枚の画像がすべて異なるクラスタに属すると見なされ，かつ対象画像全体において IoT 機器の WebUI 画像が占める割合が 34%であることから，あるクラスタを調査したときの発見数の期待値は平均して 0.34 である．ところが，提案手法によるクラスタリングを経ると，陽性画像クラスタを調査する際の発見画像数の期待値は平均して 8.83（探索効率 A）となる．さらに陽性画像クラスタのうち 50%以上が IoT 機器であると推測できたクラスタについてのみ探索作業を進めた場合，発見数の期待値は平均して 19.97（探索効率 B）となり，かつ実際に人手で調査する必要がある画像の枚数を全対象画像に対しておよそ 19%まで縮小できる．このように，提案手法により大きく IoT 機器探索の効率が向上することが分かる．

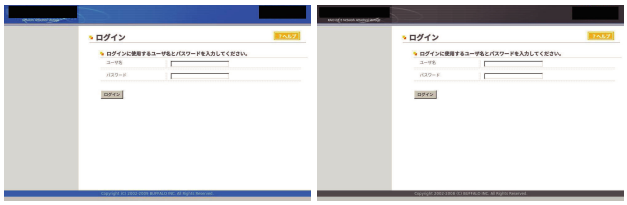

図 3 同一クラスタに分類された類似機器の例

Fig. 3 Examples of similar IoT devices in the same cluster.

また，探索効率が向上するだけでなく，探索対象となる陽性画像クラスタにおいて実際に IoT 機器の WebUI 画像が含まれる割合（真陽性率）が 85%と，十分な正確性を持った分類が行われたといえる．人手による最終的な調査対象となるクラスタに分類されるべき画像がそうでないクラスタに分類されるいわゆる見逃しについても，陰性画像クラスタに分類された画像のうち，本来は陽性画像クラスタに分類されて調査対象となるべきものであった画像が存在する割合（偽陰性率）は 12%である．さらに，陽性画像クラスタのうち IoT 機器の WebUI 画像が 50%以上と推定されるクラスタのみに調査対象を限定する際に見逃すことになるクラスタは，除外されるクラスタ（IoT 機器の WebUI 画像が 50%未満と推定されるクラスタ）238 個中 12 個（約 5%）である．以上より，提案手法による分類が IoT 機器探索について一定の網羅性も有することが分かる．

同一クラスタに分類された類似機器の例を**図 3** に示す（機器名や機器製造者名，ロゴマーク等は黒塗り処理を施した）．

図 3 のような，クラスタリングがうまく働いた好例は，画像の構図やレイアウトが固定されたログイン画面や設定画面を備える IoT 機器に多く見られた．IoT 機器のトップページの UI の多くがログインや機器設定のためのインタフェースであり，かつ当該インタフェース中の入力フォームおよびそれらの配置レイアウトが類似することから，提案手法のように視覚的に類似した画像を収集する処理が有効に働くものと考えられる．

一方で，同一または類似 IoT 機器が同一クラスタに凝集せず，複数のクラスタに分散した機器の画像（以下，誤分類画像）が，前述の陽性画像クラスタのサンプルセット 100 クラスタにおいて，2 組存在した．以下ではそれぞれについて考察する．

図 4 同一クラスタに分類されなかった同種機器の例
Fig. 4 Examples of same IoT devices in different cluster.

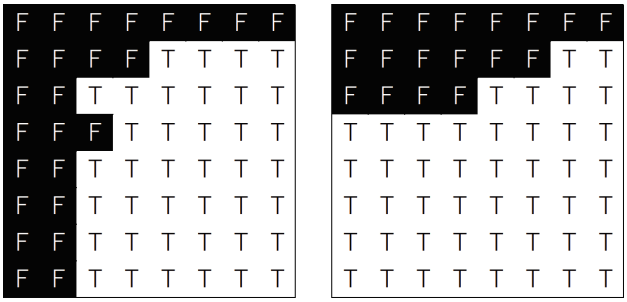

図 5 図 4 に示す画像のハッシュ値を表すマトリクス
Fig. 5 Hash values matrix of Fig. 4.

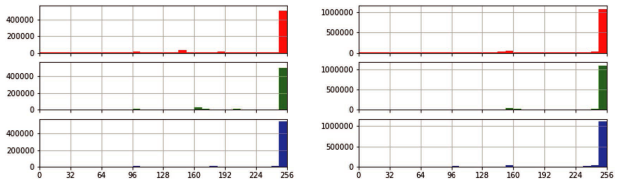

図 6 図 4 に示す画像の R，G，B ヒストグラム
Fig. 6 R, G, B histogram of Fig. 4.

図 4 に 1 組目の誤分類画像の事例を，図 5 にそれぞれの画像のハッシュ値を表すマトリクスを，図 6 に R，G，B 値のヒストグラムを示す．図 4 には，画像の縦横比の明瞭性のため，画像のフチに黒線を付した．図 5 中の F および T は，Average Hash の出力値における 0 と 1 を，それぞれ 0 を F，1 を T として表記したものである．図 4 のような WebUI が複数のクラスタに分散して存在する原因として，機器個体ごとの WebUI の縦横比の差異が大きいことが考えられる．本研究で用いたファジーハッシュアルゴリズムは，あらゆるサイズの画像を一定のサイズ（8 × 8 px）および縦横比（1 : 1）にリサイズするため，相似する画像の類似判定は高い精度で行える反面，レイアウトが類似していてもオリジナル画像の縦横比が異なる画像間の類似判定は精度が低くなる特徴がある．図 5 をみると，実際に縦横比の違いがハッシュ値にも表れることが分かる．一方で，それぞれの画像に含まれる R，G，B 値のヒストグラム（図 6）は非常に近い分布を示していることが分かる．図 4 の例のように，同一または類似 IoT 機器でありながら複数のクラスタに分類された機器のなかで，画像に使用される色が類似しているケースは他にも複数確認している．文献 [10] でも示されているように，画像の構図上の特徴のみでなく色情報（ピクセルの RGB 値の分布）も分析対象とすること

図 7 WebUI を構成するパーツは類似しているがレイアウトが異なる例
Fig. 7 Examples of WebUIs which have similar component with different layout.

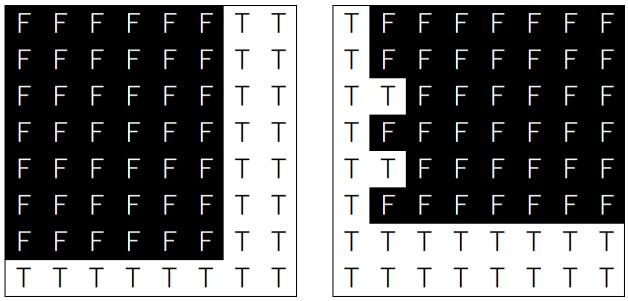

図 8 図 7 に示す画像のハッシュ値を表すマトリクス
Fig. 8 Hash values matrix of Fig. 7.

で，WebUI の類似判定の精度は向上するものと思われる．また図 4 の例では，両 UI のページソース（HTML 記述）を比較しても，一定程度のオーバラップがみられる．両画像間のハッシュ値の距離，色情報の比較に加えて，ページソースの比較をあわせて行うことでより高い精度で判定を行えるものと思われる．

また，WebUI を構成するパーツは類似するものの，レイアウトが異なるために異なるクラスタに分類された類似機器も存在した（2 組目の誤分類画像の事例）．事例を図 7 に示し，図 8 にハッシュ値を表すマトリクスを示す．図 8 中の F および T は，図 5 における表記と同じ意味で用いる．この例では，レイアウトが左右反転しているために，その違いがハッシュ値の Hamming 距離に大きく表れ，類似度が低く算出された．このようなケースに備え，画像を上下左右に反転させた場合の類似度についても考慮する必要があると考えられる．

このように，提案手法により収集した多くの WebUI 画像から，IoT 機器の WebUI に共通して現れる特有のパターンやそれらに対する知見を蓄積することが，より高い精度で IoT 機器を判別する方法の確立につながると考えられる．

6. おわりに

本稿では，IoT 機器が備える WebUI の画像的特徴に基づいた階層的クラスタリングにより，インターネットに WebUI を公開している IoT 機器を効率的に探索する手法を提案した．評価実験の結果，提案手法を用いると同一または類似する IoT 機器が同一のクラスタに凝集する傾向が

強く，実際に効率良くIoT機器を発見可能であることが分かった．階層的クラスタリングにより，すべてで1,707個あったクラスタ（画像）を凝集してIoT機器が含まれる可能性高いと判断されるクラスタ376個を抽出することができた．この抽出されたクラスタ群のうちの1つのクラスタを調査したときに発見されるIoT機器の個体数の期待値は8.83であり，クラスタリング前の同期待値が0.34であることと比較して大幅にIoT機器の発見作業を効率化できることが分かった．また抽出されたクラスタ群中に実際にIoT機器が含まれる割合（クラスタリングの真陽性率）は85%であり，十分な精確性を持つフィルタリング手法であることが分かった．本手法はサイバー攻撃の対象となりうるIoT機器の早期発見と対策の実施に有効であると考えられる．

本研究で用いた手法である階層的クラスタリングは大規模データに対して計算量が膨大になるため，提案手法を適用する対象を拡大する際，問題が発生すると予想される．今後は，文献[16]に述べられているような，階層的クラスタリングの計算量を削減する方法を適用する必要がある．

また，他のファジーハッシュアルゴリズムや評価方法，クラスタ連結法を試行することで精度の向上を図る．本研究において用いたAverage Hashは対象画像の分割数を8×8 pxと設定して実行したが，IoT/非IoTの判定に有意な素性となる情報（広告画像やロゴ等）が失われない程度の解像度で分割してハッシュ化した場合の類似判定性能および必要計算時間を検討する．また，分割時の縦横比についても，「取得した画像集合の中での平均的な縦横比を割り出してハッシュ値算出時の分割数の縦横比として採用する」「スクロールして閲覧する範囲を無視して，ブラウザが最初に表示する範囲のみをトリミングする」等，多種のレイアウトを持つ画像に対しても頑健なハッシュ化が可能な縦横比を検討する．分析対象についても，画像の構図情報のみでなく，色情報およびページソース，HTTPヘッダ等についての類似性情報を参照することで，判定精度にどのような影響がみられるかを検討する．

本研究ではポートスキャンによる探索対象を80/tcpに限定して，IoT機器ホストの発見作業の効率化手法を議論したが，81/tcpや8080/tcp等80番ポート以外のTCPポートでIoT機器ホストのWebサービスが稼働しているケースは多くみられる．今後は，他のTCPポートにも探索範囲を拡大して，当該手法の有効性を確認する．

提案手法を用いて収集するIoT機器の事例は，半教師あり学習を適用して当該手法の偽陽性率を低減したのち，それらを教師データとすることで，スキャン対象がIoT機器であるかを自動的に判定する手法の構築に用いる．

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] Symantec Security Response: Mirai: New wave of IoT botnet attacks hits Germany, available from ⟨http://www.symantec.com/connect/blogs/mirai-new-wave-iot-botnet-attacks-hits-germany⟩ (accessed 2018-05-29).
[2] Krebs, B.: DDoS on Dyn Impacts Twitter, Spotify, Reddit, available from ⟨https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/⟩ (accessed 2018-05-29).
[3] 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，コンピュータセキュリティシンポジウム2016論文集，Vol.2016, No.2, pp.870–877 (2016).
[4] 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).
[5] Durumeric, Z., Adrian, D., Mirian, A., Bailey, M. and Halderman, J.A.: Censys Security driven by data, available from ⟨https://censys.io/⟩.
[6] Matherly, J.: SHODAN, available from ⟨https://www.shodan.io/⟩.
[7] The ZMap Team: The ZMap Project, available from ⟨https://zmap.io/⟩ (accessed 2018-05-29).
[8] Mirian, A., Ma, Z., Adrian, D., Tischer, M., Chuenchujit, T., Yardley, T., Berthier, R., Mason, J., Durumerica, Z., Halderman, J.A. and Bailey, M.: An internet-wide view of ICS devices, *2016 14th Annual Conference on Privacy, Security and Trust*, Vol.2016, No.8, pp.96–103, IEEE (2016).
[9] Soyer, O., Park, K.-Y., Kim, N.H. and Kim, T.-S.: *An Approach to Fast Protocol Information Retrieval from IoT Systems*, Advanced Multimedia and Ubiquitous Engineering, pp.226–332, Springer (2017).
[10] Cai, D., He, X., Li, Z., Ma, W.-Y. and Wen, J.-R.: Hierarchical Clustering of WWW Image Search Results Using Visual, Textual and Link Information, *Proc. 12th Annual ACM International Conference on Multimedia, MULTIMEDIA '04*, pp.952–959, ACM (2004).
[11] He, X., Cai, D., Wen, J.-R., Ma, W.-Y. and Zhang, H.-J.: Clustering and Searching WWW Images Using Link and Page Layout Analysis, *ACM Trans. Multimedia Comput. Commun. Appl.*, Vol.3, No.2 (2007).
[12] Zauner, C.: Implementation and benchmarking of perceptual image hash functions (2010).
[13] Höhrmann, B.: CutyCapt, available from ⟨http://cutycapt.sourceforge.net⟩ (accessed 2018-05-29).
[14] Krawetz, N.: The Hacker Factor Blog, Hacker Factor (online), available from ⟨http://www.hackerfactor.com/blog/⟩ (accessed 2018-05-29).
[15] Everitt, B.S., Landau, S., Leese, M. and Stahl, D.: *Cluster Analysis*, Wiley (2011).
[16] 石橋徹夫，古賀久志，渡辺俊典：Locality-Sensitive Hashingを用いた階層的クラスタ分析手法（データマイニング），電子情報通信学会論文誌D-I，情報・システム，I-情報処理，Vol.88, No.4, pp.852–863 (2005).

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月同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．

内田 佳介

2018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月同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前期に進学．能動的観測によるIoT機器への攻撃リスクの検知等，ネットワークセキュリティに関する研究に従事．

森 博志 （正会員）

2013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前期修了，修士（工学）．同年4月同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に進学．ネットワーク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，耐タンパー技術，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．2005～2010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．