Computer Security Symposium 2017
23 - 25 October 2017

管理 WebUI の画像的特徴に基づく IoT 機器判別手法の提案

内田 佳介[†1]　森 博志[†1]　藤田 彬[†2]　吉岡 克成[†2†3]　松本 勉[†2†3]

概要：近年，IoT 機器を狙ったサイバー攻撃が脅威となっていることから，IoT 機器の利用状況やセキュリティの実態を調査するための広域スキャン技術の重要性が高まっている．本研究では，IoT 機器の管理 WebUI の画像的特徴に基づきクラスタリングを行い，IoT 機器を判別する手法を提案する．実際に広域スキャンによって収集した Web コンテンツを用いて評価実験を行った結果，同一または類似機器の管理 WebUI 画像が同一のクラスタに集約されることがわかった．本手法は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上で有効といえる．

キーワード：IoT，ネットワークスキャン ，階層的クラスタリング

A method to find IoT devices based on image features of their WebUI

Keisuke Uchida[†1]　Hiroshi Mori[†1]　Akira Fujita[†2]　Katsunari Yoshioka[†2†3]
Tsutomu Matsumoto[†2†3]

Abstract: In recent years, cyber-attacks targeting IoT devices are becoming a major threat and Internet wide scanning for investigating the usage and security status of IoT devices are increasingly important. In this paper, we utilize hierarchical clustering for images of web contents captured by wide network scanning to find IoT devices. We show 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, network scan, hierarchical clustering

1. はじめに

近年, Mirai に代表される IoT マルウェアの大規模感染が報告され，IoT 機器を狙ったサイバー攻撃が脅威となっている．IoT 機器のセキュリティ状況を能動的観測と受動的観測により調査した先行研究[1]では，インターネットに接続されている IoT 機器の Web ユーザインタフェース（以下，管理 WebUI）が，任意のホストからアクセス可能な状態になっている事例を報告している．その事例にはルータや Web カメラなどの一般的な IoT 機器だけでなく，ダムや発電所などの重要施設で使用されている産業用制御機器が含まれることが指摘されている．また，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，これに伴いマルウェアに感染した機器も増加している[2]．このような状況を改善するには，IoT 機器の利用状況やセキュリティの実態を把握することが必要不可欠である．前述の先行研究では，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手動で IoT 機器の WebUI を判別していたため，効率が悪く，また見逃しの恐れがあった．

本研究では IoT 機器の自動判別の第一歩として，管理 WebUI の画像的特徴に着目した IoT 機器の発見手法を提案する．提案手法は同一または類似 IoT 機器の管理 WebUI が視覚的に類似した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，それらを画像向けハッシュアルゴリズムである Average Hash にかけた上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，国内のある AS の IP アドレスレンジへの広域スキャンにより収集された全 14,744 枚の Web コンテンツ画像が 1,707 個のクラスタに分割された．これらのクラスタの要素を，サンプリングを行った上で目視により確認したところ，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 機器の管理 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．

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などの特定の機能のみを提供する機器を IoT 機器と呼

†1 横浜国立大学
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
Graduate School of Environment and Information Sciences,
Yokohama National University

ぶこととする．例えば，IoT 機器には，ブロードバンドルータや NAS など一般家庭向けの機器だけでなく，工場や病院など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[1]では，手動で IoT 機器の判定を行なっていたため，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．

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[3][4]，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[5][6]，画像的特徴だけでなく HTML などから取得したテキスト情報など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 機器が備える管理 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．

本研究では，先行研究[1]と同様に IoT 機器判別手法の自動化を最終的な目標に据えるが，本稿では最終的な目標を達成するための前段階として，効率的な IoT 機器の発見手法を提案する．

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，WebUI 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，出力したハッシュ値の間で比較可能なファジーハッシュアルゴリズムに入力しハッシュ値を算出する．次に，ハッシュ値を用いて教師なし学習の一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．さらに，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上で目視による判定を行い，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，そのクラスタについて詳細に調査することで効率的に IoT 機器を発見する．以下の節で各手順の詳細を述べる．

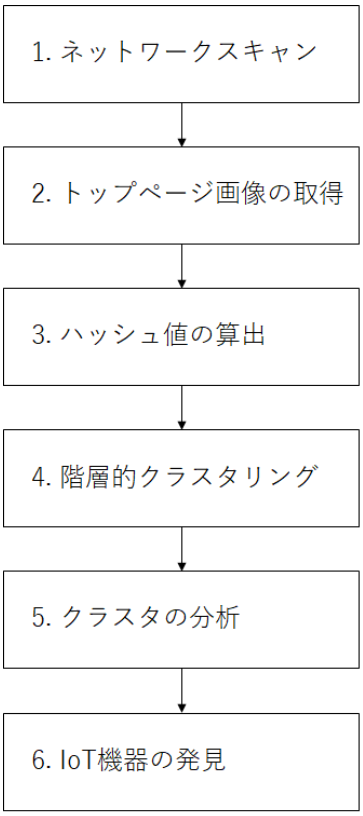

図 1　提案手法の処理手順
Figure 1　Procedure of the proposal method.

3.1 ネットワークスキャン

インターネットからアクセス可能な状態である IoT 機器の管理 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 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である ZMap[7]を使用してポートスキャンを行う．

3.2 トップページ画像の取得

ネットワークスキャンにより発見した，80/tcpポートでセッション確立が可能なホストに対して，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[8]を用いて以下のURLにアクセスすることでトップページ画像を保存する．

http://<調査対象ホストのIPアドレス>/

3.3 ハッシュ値の算出

3 章 2 節にて取得したトップページ画像を，画像向けファジーハッシュアルゴリズムである Average Hash アルゴリズム[9]に入力し，画像のフィンガープリントとなる 64bit 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 距離を非類似度として扱うことが可能である．

3.4 階層的クラスタリング

前節にて算出した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．

3.5 クラスタの分析

デンドログラムは，クラスタリングの過程をグラフとして表しているに過ぎず，有意性のあるクラスタを得るためには分析者がクラスタを結合する際の距離に上限を設ける必要がある．本手法では，分析者が対象画像中から，異なるクラスタに分類されると予想される k 種類の IoT 機器の管理 WebUI 画像を選択し，以下の条件で上限を定めた．

- 選択した画像がそれぞれ異なるクラスタに所属する．
- 上記を満たした上で，選択された画像が所属するクラスタのサイズが最大となる．

クラスタ間距離の上限を定め，対象画像がクラスタに分割された後，要素数が 2 以上となるクラスタの要素をサンプリングした上で，IoT 機器の管理 WebUI が高い確率で含まれるクラスタを判定し，その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．

なお，IoT 機器の管理 WebUI の判定は以下の基準に基づいて目視によって行う．

- IoT 機器と判断される機種名，型番などが記載されている．
- ”ルータ”，“NAS”など，IoT 機器と推測できる情報が記載されている．

4. 評価実験

提案手法の有効性を検証するため，我々は提案手法を実装し，国内のある AS の IP アドレスレンジをスキャンすることによって収集したトップページ画像 14,744 枚を対象に評価実験を行なった．

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なった．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予想される IoT 機器の管理 WebUI 画像を k=10 種類選択し，3 章 5 節で述べた方法によりクラスタを得た．

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なった．

(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 機器が 50%以上を占めるようなクラスタ数
(5) (4)を調査する過程にて発見された IoT 機器の種類数
(6) 要素数が 1 であるクラスタについて，IoT 機器の割合
(7) 対象全体のうち，IoT 機器の占める割合

なお，目視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，(6), (7)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なった．

4.2 実験結果

本実験の結果を表 1 に示す．本実験により，14,744 枚の対象画像が 1,707 個のクラスタに分割され，そのうち要素数が 1 であるものは 1,331 個，要素数が 2 以上であるものは 376 個であった．特に，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わかった．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．これらが IoT 機器の管理 WebUI である割合は 12%であり，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 機器の管理 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わかる．また，本実験を通してルータ，NAS，産業用制御機器などを含む少なくとも 8 種類のカテゴリにまたがる 136 種類の IoT 機器を発見することができた．その内訳を表 2 に示す．

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

(1)	(2)	(3)	(4)	(5)	(6)	(7)
1,707[個]	1,331[個]	376[個]	138[個]	136[種類]	12[%]	34[%]

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
NAS	15
ルータ	20
NVR	15
遠隔監視機器（電力モニタなど）	11
セキュリティアプライアンス	2
産業用制御機器	6
コピー機	2
その他	7
合計	136

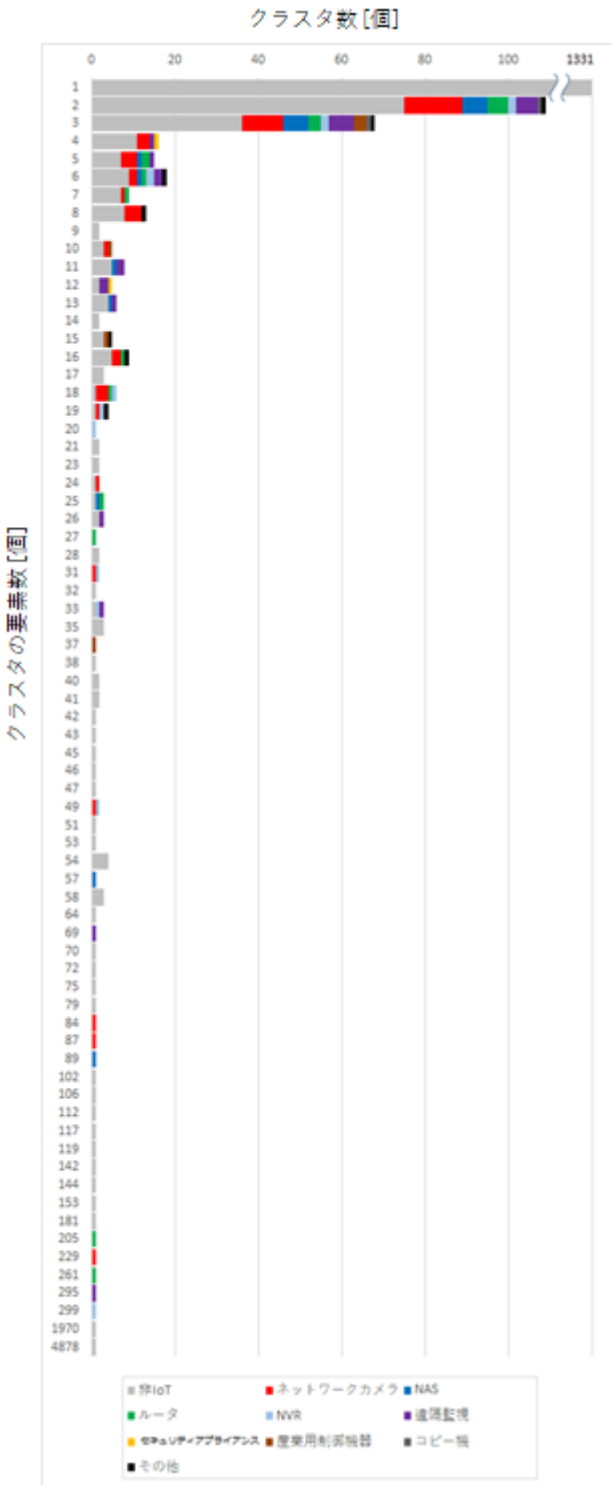

図 2　クラスタの分布

Figure 2　Distribution of clusters.

さらに，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 の縦軸はクラスタの要素数を，横軸は対応するクラスタの数を表している．

図 2 において，灰色で表され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ある．それ以外の色で表され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り，表 2 の機器カテゴリごとに色分けされている．

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 機器の管理 WebUI 画像が凝集していることがわかる．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 機器が凝集されているが，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

前章の結果から，同一または類似 IoT 機器の管理 WebUI 画像が同一クラスタに凝集している傾向が強く，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わかった．同一クラスタに分類された類似機器の例を図 3 に示す．（製品名やメーカ名，ロゴマークなどは黒塗り処理を行っている．）

図 3　同一クラスタに分類された類似機器の例

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

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 機器がトップページに備える管理 WebUI の多くがログイン画面であることが今回の結果につながったと思われる．

しかし，同一または類似 IoT 機器のすべてが同一クラスタに凝集する訳ではなく，複数のクラスタに分散している機器が存在することを確認した．図 4 にその例を，図 5 にはそれぞれの画像のハッシュ値を表すマトリクスを，図 6 には R,G,B 値のヒストグラムを示す．図 4 のような管理 WebUI が複数のクラスタに分散して存在する原因として，個体ごとの管理 WebUI の構図や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にリサイズするため，単純な拡大縮小に強い反面，縦横比の変化に弱い特徴がある．そのため，図 5 をみると，実際に構図や縦横比の違いがハッシュ値にも表れることがわかる．その一方で，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おり，IoT 機器の管理 WebUI の類似性を構図だけではなく，色情報の観点からも見いだせることが判明した．

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てしまった機器のなかで，画像に使用されている色が類似しているケースは他にも複数確認されており，画像の類似度を測る際には，文献[5]でも示されているように，画像のテクスチャだけでなく，色情報を併用することで，より多くの IoT 機器の管理 WebUI を同一クラスタに凝集させることが可能であると思われる．

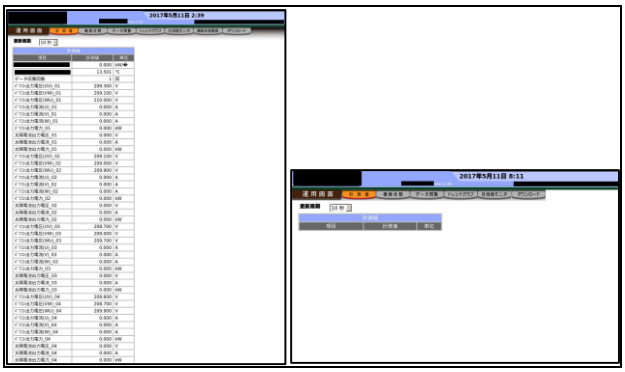

図 4　同一クラスタに分類されなかった同種機器の例
Figure 4　Examples of same IoT devices in different cluster.

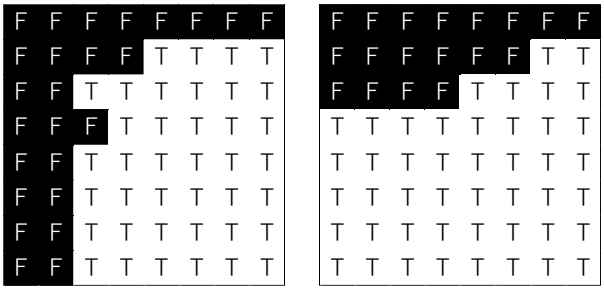

図 5　図 4 に示す画像のハッシュ値を表すマトリクス
Figure 5　Hash values matrix of Figure 4.

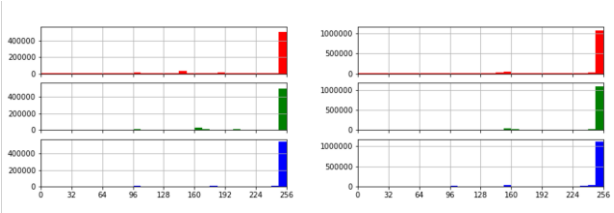

図 6　図 4 で示す画像の R,G,B ヒストグラム
Figure 6　R,G,B histogram of Figure 4.

また，管理 WebUI を構成するパーツは類似しているものの，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．その例を図 7 に示し，図 8 にハッシュ値を表すマトリクスを示す．

図 7　管理 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
Figure 7　Examples of WebUIs which have similar component with different layout.

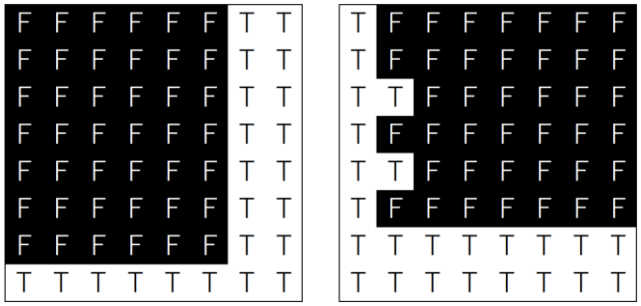

図 8　図 7 に示す画像のハッシュ値を表すマトリクス
Figure 8　Hash values matrix of Figure 7.

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 IoT 機器の管理 WebUI 画像から，IoT 機器の管理 WebUI に共通して多く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 機器を判別できる評価方法の確立に繋がると考えられる．

6.　まとめと今後の課題

本稿では，IoT 機器が備える管理 WebUI の画像的特徴にもとづいた階層的クラスタリングによる効率的な IoT 機器の発見手法を提案した．また，評価実験の結果，同一または類似 IoT 機器が同一のクラスタに凝集する傾向が強く，実際に効率よく IoT 機器を発見可能であることがわかった．また，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．

今後は，他のファジーハッシュアルゴリズムや評価方法，クラスタ連結法を用いた実験を施行していくことでより高い精度を目指す．

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，提案手法を用い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[10]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ことや，IoT機器の自動判定方法の確立を課題としたい．

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．
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] 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
[2] 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”, 情報処理学会コンピュータセキュリティシンポジウム, 2016
[3] Mirian, Ariana, et al. "An internet-wide view of ICS devices." Privacy, Security and Trust (PST), 2016 14th Annual Conference on. IEEE, 2016.
[4] Soyer, Onur, et al. "An Approach to Fast Protocol Information Retrieval from IoT Systems." Advanced Multimedia and Ubiquitous Engineering. Springer, Singapore, 2017. 226-232.
[5] Cai, Deng, et al. "Hierarchical clustering of WWW image search results using visual, textual and link information." Proceedings of the 12th annual ACM international conference on Multimedia. ACM, 2004.
[6] Xiaofei, et al. "Clustering and searching WWW images using link and page layout analysis." ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 3.2 (2007): 10.
[7] “ZMap”, https://zmap.io/, (参照 2017-08-22)
[8] “CutyCapt - A Qt WebKit Web Page Rendering Capture Utility”, http://cutycapt.sourceforge.net/, (参照 2017-08-22)
[9] "The Hacker Factor Blog", http://www.hackerfactor.com/blog/, (参照 2017-08-22)
[10] 石橋徹夫, et al. "Locality-Sensitive Hashing を用いた階層的クラスタ解析手法の高速化." 情報処理学会研究報告コンピュータビジョンとイメージメディア (CVIM) 2003.109 (2003-CVIM-141) (2003): 57-62.