Basic認証要求応答に着目したデバイスフィンガープリントの調査

大塚 瑠莉[1,2,a)]　吉岡 清和[3]　インミンパパ[4]　吉岡 克成[4,5]

概要：Basic 認証は，インターネット初期から使用されている認証方式の 1 つであり，実装が容易かつ多くの Web サービスに対応可能であることから現在でも IoT 機器から汎用的な Web サーバまで，幅広く利用されている．広域スキャンシステムである Shodan では，Basic 認証要求応答を返信するホストが全世界で 250 万件以上確認されており，その要求応答のなかには，接続機器の推定に至る情報を含むものが存在する．本研究では，HTTP/1.0，HTTP/1.1 それぞれについて，Basic 認証の要求応答から，これらの機器の推定が可能かどうかを調べた．その結果，産業用機器から一般消費者向けの機器まで 400 種類以上の機器の型番を識別することができ，そのうち, 80%は Shodan において機器識別がされていなかった．また OpenAI の LLM による自動判定結果と比較したところ，HTTP/1.0 において gpt-4-turbo-2024-04-09 により 81%が人間の推定結果と一致することが確認された．

キーワード：Basic 認証, IoT, デバイスフィンガープリント, HTTP

Investigation of Device Fingerprinting Focused on Basic Authentication Requests

Ruri Otsuka[1,2,a)]　Kiyokazu Yoshioka[3]　Yin Minn Pa Pa[4]　Katsunari Yoshioka[4,5]

Abstract: Basic authentication is one of the authentication methods for web services that has been used since the early days of the Internet. It is still widely used today in various devices, from IoT devices to general-purpose web servers, due to its ease of implementation and compatibility with many web services. The Internet-wide scanning system, Shodan, has identified over 2.5 million hosts worldwide that respond to Basic authentication requests. Among these responses, some contain information that can be used to infer the connected devices. In this study, we investigated whether fingerprinting these devices from Basic authentication responses in HTTP/1.0 and HTTP/1.1 is possible. As a result, we were able to infer more than 400 device models ranging from industry to consumer devices, 80% of which were not identified by Shodan. Furthermore, it was confirmed that 81% of the inference results of HTTP/1.0 responses by gpt-4-turbo-2024-04-09 matched those inferred by humans.

Keywords: Basic authentication, IoT, Device Fingerprinting, HTTP

[1] 三菱電機株式会社
Mitsubishi Electric Corporation,Kamakura,Kanagawa 247-8501,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] 川崎市立川崎高等学校
Kawasaki High School, Kawasaki, Kanagawa 210-0806, Japan
[4] 先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University, Yokohama, Kanagawa 240-8501, Japan
[5] 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)] Otsuka.Ruri@bp.MitsubishiElectric.co.jp

1. はじめに

Basic 認証 [1] は，実装が容易かつ多くの Web サービスに対応可能なことから，IoT 機器の開発時から運用時において幅広く使用されている．IP カメラの Web ブラウザ経由での映像閲覧，機器の管理画面へアクセスする際の認証といったマニュアルに記載されている機能だけでなく，マニュアルに記載されておらずユーザの使用を想定していないページ等でも Basic 認証が利用される場合がある [2][3]. インターネット接続機器の広域スキャンシステムである Shodan [4] では，スキャンシステムからの接続要求に対して Basic 認証要求応答を返信するホストが全世界で 250 万件以上確認されている [5].

Basic 認証における認証要求応答には，図 1 のようにメーカや型番と推定される文字列を記載しているものがあり，これらの応答から機器の種別等を推定できる場合がある．Basic 認証スキームではスキーム名「Basic」，認証パラメータ「realm」が必須であり，realm は HTTP 認証における保護領域を示す [1][6]．図 1 はメーカや型番と推定される文字列が realm 値に含まれている例である．昨今，IoT 機器を狙うサイバー攻撃が増大し，特に機器固有の脆弱性を狙う攻撃が増加していることから [2][7][8]，インターネット上に存在する機器の種別や型番を特定し，脆弱な機器に対しては適切な対策を行うことが重要となっている [9]. そこで本研究では，Basic 認証要求応答に着目し，機器を推定するためのデバイスフィンガープリントになりえるかを調査する．具体的には以下の Research Questions(RQ) を設定する．

RQ1. インターネット上でアクセス可能な機器の Basic 認証要求応答から，どの程度の機器推定が可能か.

RQ2. 既存の広域スキャンシステムでは Basic 認証が動作する Web サービスから機器の推定をどの程度行っているか.

RQ3. LLM は Basic 認証要求応答から機器の推定を行う作業をどの程度の精度で行うことができるか.

まず，RQ1 に答えるため，Basic 認証が使用されており，かつ，インターネット上でアクセス可能な機器の認証要求応答からどの程度の機器推定が可能か，Basic 認証が稼働している HTTP のバージョン（HTTP/1.0，HTTP/1.1）ごとに調査する．この調査には広域スキャンシステムである Shodan [4] を活用し，得られた認証要求応答から人間が機器推定を行う．次に，RQ2 に答えるために機器推定が可能な認証要求応答に対して，広域スキャンシステム Shodan における機器推定結果との比較を行う．RQ3 に対しては，OpenAI の LLM [10] による機器推定と人間による推定を比較する．調査の結果，RQ1 に対しては産業用機器から一般消費者向け機器まで 400 種類以上の機器の型番を識別し，機器の推定を行えることがわかった．RQ2 に対しては，人間による推定結果を正解データとした時，Shodan が推定できた型番は全体の 20%にあたる 84 種類のみであり，メーカーに関しては全体の 8.1%である 8 種類のみ推定できた．RQ3 に対しては人間による推定結果を正解データとした時，LLM の 2 種類のモデルでは，gpt-3.5-turbo-0125 は HTTP/1.0 で全体の 70%，HTTP/1.1 で全体の 51%，gpt-4-turbo-2024-04-09 は HTTP/1.0 で全体の 81%，HTTP/1.1 で全体の 53%を推定できた．このように Basic 認証要求応答に着目したフィンガープリントは広域スキャンにおける機器推定に有効であり，LLM を用いることで一定の精度で期推定ができることがわかった．

```
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm=“ルータメーカー名 型番”
x-frame-options: SAMEORIGIN
Set-Cookie: XSRF_TOKEN=1222440606; Path=/
Content-type: text/html
```

図 1 Basic 認証要求応答の例

Fig. 1 Example of basic authentication request response.

2. 調査方法

2.1 Basic 認証要求応答による機器推定

Basic 認証が動作し，かつ，インターネット上でアクセス可能な機器の種類や応答内容について，インターネット接続デバイス検索エンジンである Shodan [4] を用いて調査した．Shodan はインターネットを継続的に探索（広域スキャン）することで，接続されているデバイスのホストや探索時の応答などの情報を集めており，ユーザは検索条件を入力することで該当する情報を得ることができる．Basic 認証で保護されている領域に対してクライアントがアクセスをすると，サーバは 401 Unauthorized 応答をする [1]. この際，Basic 認証が動作しているホストは，スキーム名「Basic」，認証パラメータ「realm」を含む WWW-Authenticate ヘッダーフィールドと，「HTTP/1.0 401 Unauthorized」もしくは「HTTP/1.1 401 Unauthorized」の文字列を含む応答をする．Shodan の Web インタフェース上で，「Basic」「realm」「HTTP/1.0 401 Unauthorized」を全て含む応答を行うホスト群と，「Basic」「realm」「HTTP/1.1 401 Unauthorized」を全て含む応答を行うホスト群の上位 1,000 種類[*1]を調査した．各応答は Shodan によって一意のハッシュ値で管理されており，Shodan の Web インタフェースで該当のハッシュ値を「hash: ハッシュ値」で検索すると，そのハッシュ

[*1] Shodan の仕様上，1,000 種類まで確認ができたため，これを調査範囲とする．実際にインターネット上に晒されている応答の種類はこれを超えると考えられる．

値に対応付けられた応答内容と，その応答をするホストの一覧が閲覧可能である HTTP/1.0，HTTP/1.1 それぞれについて 1,000 種類の応答内容を確認し，含まれる情報からメーカや型番などの機器識別に繋がる情報を抽出した．得られた情報から推定される機器について，製造メーカの WEB サイトや公開されている電子マニュアルを調査し，実際に合致する機器が存在するか確認した．また，Basic 認証要求応答からでは機器推定ができないものについては，同一な realm 値を持つ応答群に対してクラスタリングを行い，どの程度の種類の機器が含まれているのかを調査した．具体的には，2 つの応答間の編集距離をそれらの応答の長さの大きい方で割った正規化距離を用いて最短距離法による階層的クラスタリングを行い，様々な閾値でクラスタ数がどのように変化するかを調べた．

2.2 既存の広域スキャンシステムによる機器推定

既存の広域スキャンシステム Shodan による機器推定の状況を次のように調査した．2.1 節で得た各応答のハッシュ値を Web インタフェース上で検索することで，Shodan がそのハッシュ値に対応付けている応答を行うホストの情報を得ることができる．人間による機器推定ができた認証要求応答について各応答を行うホストをハッシュ値により検索し，1 つのハッシュ値につき任意の 3 つのホストを選んだ．ホストは検索結果画面よりランダムに選んだが，待ち受けポート数が異常に多いなど，通常の機器ではないと推測されるホストは選択から除外した．各ホストについての詳細情報を確認し，検索したハッシュ値の応答をするポート番号で動作しているサービスに対し，Shodan がどのような識別をしているか調査した．また，Shodan がそのホスト全体に対してどのようなタグ付けをしているか，ハッシュ値の応答をするポート番号以外ではどのような識別をしているのかを合わせて調査した．これらの結果と人間による機器推定の結果を比較することで，Shodan が Basic 認証要求応答からどの程度，機器推定を行っているかを確認する．

2.3 LLM による機器推定

HTTP/1.0，HTTP/1.1 それぞれ 1,000 種類の Basic 認証要求応答に対して，OpenAI の LLM [10] がどのような機器と推定するかを調査した．Basic 認証要求応答をもとに LLM が機器やサービスを高い精度で特定できるならば，広域スキャンシステムで検知した多数のホストに対して機器推定を自動で行えることとなり，非常に有益である．LLM へ入力するプロンプトは付録の図 A·1 の通りであり，プロンプト内の「No.」は Shodan で得られた順位，「Hash」は応答につけられたハッシュ値，「response」は Basic 認証要求応答の内容である．LLM は与えられた Basic 認証要求応答の内容から，機器名，メーカ名，型番，タイプ，信頼度を回答する．各回答がどのような理由で導出されたかを「reason」で回答させることにより，LLM が応答内容のどこに反応して判断をしているのかも確認できるようにした．LLM のモデルによる精度の違いを検証するために，gpt-3.5-turbo-0125 と gpt-4-turbo-2024-04-09 でそれぞれ評価し，いずれも temperature=0 で設定した．

3. 結果

3.1 Basic 認証要求応答を用いた人間による機器推定

2024 年 5 月時点で「Basic」「realm」「HTTP/1.0 401Unauthorized」を全て含む応答ホストは 326,802 件，「Basic」「realm」「HTTP/1.1 401Unauthorized」を全て含む応答ホストは 2,130,983 件 Shodan で見つかった．なお，「HTTP/1.0 401Unauthorized」を含む応答ホストは 1,836,639 件，「HTTP/1.1 401Unauthorized」を含む応答ホストは 23,089,042 件ヒットしたことから，存在するホスト数は HTTP/1.1 の方が 10 倍以上多いことがわかる．HTTP/1.0 と HTTP/1.1 について，ハッシュ値ベースで各 1,000 種類の応答内容が存在することを確認したが，実際に Basic 認証要求応答の内容を調査した 2024 年 5 月時点で，当該応答をもつホストの存在が確認できたのは HTTP/1.0 が 760 種類，HTTP/1.1 が 999 種類であった．それ以外のホストは停止したか，アドレスの変更によりスキャン結果から外れたものと思われる．そこで，今後の結果では調査の母数を HTTP/1.0 は 760 種類，HTTP/1.1 は 999 種類とする．Basic 認証要求応答に含まれる情報から，「機器名」「メーカ名」「型番」を調査した．型番まで一意に推定できたもの，型番までは推定できなくても機器名やメーカ名など一部は推定できたもの，何も推定できなかったものの件数と，母数に占める割合を有効数字第 2 位まで求めたものを，表 1 に示す．なお，バージョン情報や型番の情報が含まれていなくても，応答内容から Web サービスやアプリケーションが一意に特定できるものについては，型番も特定できたとみなす．型番まで一意に特定できたものは，HTTP/1.0 の応答が 348 種類で全体の 46%，HTTP/1.1 の応答が 293 種類で全体の 29%，一部特定できたものは，HTTP/1.0 が 188 種類で全体の 25%，HTTP/1.1 が 297 種類で全体の 30%，何も特定できなかったものは，HTTP/1.0 が 224 種類で全体の 30%，HTTP/1.1 が 409 種類で全体の 41%であった．Basic 認証要求応答のなかには，同じ機器からの応答と判断ができるものでも，応答の中に含まれる Date フィールドなど，応答する度に異なる値を含むため，毎回ハッシュ値が異なるものも存在した．特定できた型番の種類を求めたところ，HTTP/1.0，HTTP/1.1 を合わせて，136 種のメーカーと 414 種類の型番を推定することができた．全体の傾向として，HTTP/1.0 の方が HTTP/1.1 よりも推定可能なものが多く，これは HTTP/1.0 と比較して HTTP/1.1 の方が製造時期が新しく，Basic 認証実

表 1　機器推定件数（母数に対する割合（%））
Table 1　Number of inferred devices (percentage of population(%)).

	HTTP/1.0	HTTP/1.1
母数	760	999
推定可能	348 (46%)	293 (29%)
一部推定可能	188 (25%)	297 (30%)
推定不可	224 (30%)	409 (41%)

表 2　機器分類と該当する型番数（割合（%））
Table 2　Device classification and percentage of applicable model numbers(%)).

Category	Type	HTTP/1.0	HTTP/1.1
H/W	server	1 (0.29%)	18 (6.1%)
H/W	network	280 (80%)	129 (44%)
H/W	media	23 (6.6%)	47 (16%)
H/W	consumer	14 (4.0%)	12 (4.1%)
H/W	industrial	23 (6.6%)	25 (8.5%)
S/W	application & OS	7 (2.0%)	62 (21%)

装時にセキュリティ面が強化されているためと推測される．推定できた型番を分類した結果が表 2 である．型番について，まずはハードウェアとソフトウェアに大分類し，ハードウェアは「server」「network」「media」「consumer」「industrial」に小分類した．「server」はプロキシサーバやウェブサーバなどが該当し，「network」はルータやスイッチ，モデムやゲートウェイ等，「media」は IP カメラや DVR 機器等，「consumer」は HEMS[*2] やプリンター等，「industrial」はレーザーやパワーマネジャー等が該当する．ソフトウェアには，アプリケーションサービスや OS 等が該当する．HTTP/1.0，HTTP/1.1 ともに，ルータやスイッチ等のネットワーク関連製品である「network」が最も多くの割合を占め，HTTP/1.0 では 80%，HTTP/1.1 では 44%であった．HTTP/1.0 と比較して HTTP/1.1 ではプロキシサーバや Web サーバ等のサーバ類である「server」やアプリケーションソフトウェア等と判断される「S/W」の割合が大きく増加した．これは，サーバやソフトウェアは運用中にアップデートされることが多く，HTTP/1.0 から HTTP/1.1 へ移行したものが多いことや，そもそもそれらの製品ライフサイクルが組込み機器よりも早いことが原因として考えられる．このように産業用機器から一般消費者向けの機器まで多様な IoT 機器の型番が推定された．

Basic 認証要求応答から型番まで推定ができないものについては，同一な realm 値を持つ応答群に対してそれぞれ階層的クラスタリングを行い，閾値を変更することでどの程度の機種が存在するかを調査した．具体的には応答間の編集距離を大きい方の応答の長さで割った正規化距離を用いて最短距離法による階層的クラスタリングを行った．

図 2 は，realm 値から機器が推定できない HTTP/1.0 の

[*2] HEMS: Home Energy Management System

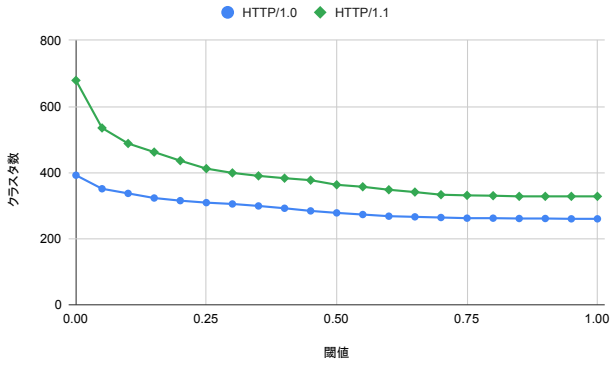

図 2　realm 値から機器を推定できない応答のクラスタ数
Fig. 2　Number of response clusters whose device model cannot be inferred from realm value.

応答 392 種類と HTTP/1.1 の応答 679 種類を，realm 値ごとにクラスタリングした結果の合計数で，横軸はクラスタリング時の閾値，縦軸は合計クラスタ数である．閾値 1.0 は同一の realm 値を持つ全ての応答を一つのクラスタとしたものであり，機器が推定できない realm 値の種類数と同値である．同じ機器が異なる realm 値を持つことはないと仮定すると，少なくとも realm 値の種類数である 260 種類 (HTTP/1.0)，328 種類 (HTTP/1.1) 程度の種類の機器は存在すると考えられる．また，閾値が低下してもクラスタ数が急激に上昇しないことからクラスタを構成する応答群は一定の類似度を有していることが分かる．閾値が 0.05 以下では急激にクラスタ数が上昇するがこれは Date など，アクセスする度に異なる値が付与されるフィールドの影響である．上記から機器が推定できない応答を返す機器の種類数は，realm 値の種類数に近いと推測される．

3.2　広域スキャンシステムによる機器推定

表 1 で機器推定可能であった 641 種類の Basic 認証要求応答に対して，Shodan [4] でハッシュ値を検索し，ハッシュ値に対応する応答をするホストを任意に 3 つ選び，当該ホストの Basic 認証が動作する Web サービスに対して Shodan がどのような識別をしているか調査した．なお，ホストは検索結果画面よりランダムに選んだが，待ち受けポートが異常に多いなど通常の機器ではないと推測されるホストは選択から除外した．Basic 認証要求応答に対して人間が推定した 414 個の型番とメーカ数 136 社を正解データとし，Shodan にホストの情報が残っていた型番 393 個 125 社を母数とした際の Shodan の機器判別の成功件数と成功率を表 3 に示す．なお，Shodan がハッシュ値に対応する応答に対して一意に型番を推定可能なタグ付けをしている時，機器推定成功とみなし，バージョン情報の有無は条件としなかった．一方，タグ付けがされていないものや型番を一意に推定できないものについては，機器推定失敗とみなした．Shodan が特定できた型番は 393 個中 84 個

表 3　Shodan による機器推定件数とその割合）
Table 3　Number of devices identified by Shodan (percentage of population(%)).

	型番数	メーカ数
母数	393	125
推定可能	84 (20%)	8 (5.9%)

(20%) のみであり，125 社中 8 種 (5.9%) であった．これらの結果より，Shodan が識別できるメーカーや型番には偏りがあると共に限定的であるといえる．識別結果が記載される欄に型番以外の文字列が記載されている応答も確認でき，Shodan は該当文字列がメーカ名や型番かどうかは明確に区別せずに，応答から機械的に文字列を取り出している可能性がある．さらに，検索した Basic 認証要求応答を行うポート以外で，同じ型番の応答と識別されているポートや，全く別の機器として識別されているポートが確認できた．これは，ルータやスイッチ等のネットワーク機器のポートフォーワーディング設定等により，同一 IP アドレスにおいて複数の機器にアクセス可能な状態になっているか，IP アドレスの変更により異なる機器の応答が混合していることが原因と考えられる．

3.3　LLM による機器推定結果

HTTP/1.0，HTTP/1.1 の Basic 認証要求応答の内容が確認できた 760 種類，999 種類のそれぞれに対して，OpenAI の LLM [10] の 2 種類のモデルを活用して機器推定実験を行った．Basic 認証要求応答に対して人間が推定した 414 件の型番を正解データとして，LLM の各モデルが機器推定結果を評価したものが表 4 である．人間が推定した 414 件の型番では，機器の種類だけでなくバージョンまでを推定対象としており，バージョンが異なる場合はそれぞれを別の型番としているが，LLM のモデルに対する評価では，本実験の主な目的である機器種類の推定が正しければ推定成功と判断し，バージョンは推定対象としなかった．また，プロンプトで要求した「device」「maker」「model_number」「type」のいずれかの項目に人間が回答した型番が含まれており，機器が一意に推定できるものについては，推定成功と判断した．なお，同じメーカーの型番の中には類似しているものもありシリーズ違いと思われるが，これらに関しては別の機器として扱うため，シリーズが異なるものを推定した場合には機器特定成功とはみなさない．414 件の型番のうち，gpt-3.5-turbo-0125 では 61%，gpt-4-turbo-2024-04-09 では 67%の機器を推定することができた．どちらのモデルでも全体の 60%以上は推定できたが，より高性能なモデルである gpt-4-turbo-2024-04-09 の方が推定できるものは多くなった．gpt-3.5-turbo-0125 では推定できても gpt-4-turbo-2024-04-09 では推定できなかった型番は 21 件確認できた．gpt-3.5-turbo-0125 では応答内に含まれる WWW-Authenticate フィールドに含まれる文字列をそのまま機器推定結果として出力しているが，gpt-4-turbo-2024-04-09 ではその情報だけでは機器推定に不十分であると判断したり，別のフィールドの情報も含めて出力したりしている．21 件の型番については，明確に型番と判明する文字列が WWW-Authenticate フィールド内に含まれていなかったため，gpt-4-turbo-2024-04-09 は他のフィールドからも判断を試み，結果的に判定が誤った可能性が高い．

表 4　LLM による機器推定件数（母数に対する割合（%））
Table 4　Number of devices identified by LLM (percentage of population(%)).

	gpt-3.5-turbo-0125	gpt-4-turbo-2024-04-09
母数	414	414
推定可能	251 (61%)	278 (67%)

表 5　LLM による認証要求応答の識別（母数に対する割合（%））
Table 5　Identification of authentication request response by LLM (percentage of population(%)).

LLM model	HTTP version	推定数	割合 (%)
gpt-3.5-turbo-0125	HTTP/1.0	146	70%
gpt-3.5-turbo-0125	HTTP/1.1	107	51%
gpt-4-turbo-2024-04-09	HTTP/1.0	170	81%
gpt-4-turbo-2024-04-09	HTTP/1.1	111	53%

推定された型番が HTTP/1.0 と HTTP/1.1 のどちらで動いている機器なのかを，型番推定に使用した応答から求めた．414 種類の型番のうち，HTTP/1.0 で動いている型番は 209 種類，HTTP/1.1 で動いている型番は 209 種類であり，どちらのバージョンでも動いている型番は 4 種類確認された．LLM の 2 種類のモデルが推定した型番について，HTTP のバージョンごとに分類した結果が表 5 である．HTTP/1.0 と HTTP/1.1 の機器推定合計数が表 4 と異なるが，これはどちらのバージョンでも動いている機器を含むためである．gpt-3.5-turbo-0125 では，HTTP/1.0 で動く機器については全体の 70%を正しく推定し，HTTP/1.1 で動く機器については全体の 51%を正しく推定した．gpt-4-turbo-2024-04-09 では，HTTP/1.0 で動く機器については全体の 81%を正しく推定し，HTTP/1.1 で動く機器については全体の 53%を正しく推定した．LLM のどちらのモデルでも HTTP/1.0 で動く機器に対する特定精度は HTTP/1.1 に比べて高かった．これは HTTP/1.0 は Basic 認証要求応答内に機器推定につながる文字列が含まれることが多いためである．LLM のモデルによる推定精度の差は，HTTP/1.0 の方が顕著に確認できた．

4.　関連研究

IoT 機器のデバイスフィンガープリントやラベル付けに着目した研究は，本研究以外にも進められている．ネット

ワークトラフィックの情報をもとにIoT機器をラベル付けするだけでなく [11]，ネットワークトラフィックの情報を機械学習の学習データに用いてIoT機器のラベル付け [12] や分類 [13] を行う研究も存在する．これらはIoT機器の情報収集方法としてネットワークトラフィックというパッシブな方法を採用している点で，アクティブなスキャン結果を用いている本研究とは情報収集方法の点で異なる．文献 [14] はアクティブなスキャン結果を用いている点で類似したおり，スキャンにより得られたOSフィンガープリントを学習させて機器識別のフレームワークを作成したいる．また，ハニーポットによるパッシブなデータも用いて調査をしている研究がある [12]．本研究はこれらの既存研究と比較して，Basic認証という古くから広い分野で利用されている機能の特徴を用いるため，一般消費者向け機器から産業用機器まで多様な分野のIoT機器を推定できる点やShodanという一般にも利用可能な検索エンジンから得られる情報からでも機器推定が可能である点が異なる．

5. 研究倫理への対応について

本研究は十分なセキュリティ対策がとられていない可能性のあるBasic認証動作機器やサービスを調査し推定するものであり，その内容がそれらに対する攻撃を助長する可能性を完全に否定できない．そのため，攻撃対象になりえる機器の情報や推定に必要な情報については一部を詳細に記述しないことで秘匿している．一方，研究者に対しては情報提供依頼に応じて個別に調査結果を提供することで研究の恩恵の最大化を目指す．これまで明らかでなかった，Basic認証の認証要求応答が，Basic認証動作機器やサービスのデバイスフィンガープリントになりえることを本論文により示すことは，IoT機器等のセキュリティ向上に貢献するものであり，その恩恵は十分に大きいと考える．

6. まとめ

本研究では，インターネットへ晒されているBasic認証サービスのBasic認証要求応答から機器推定が可能かどうかを調査するとともに，Shodanや LLMを活用して人間以外も推定できるかを確認することで，Basic認証要求応答の内容がデバイスフィンガープリントになりえるかを調査した．その結果，Basic認証という同じ認証方式であっても，HTTP/1.0，HTTP/1.1によってBasic認証要求応答の内容や，動作する機器の傾向に違いがあることや，HTTP/1.0では46%，HTTP/1.1では29%の認証要求応答から合計414種類の機器の推定が可能と判明した．それらの機器に対して，広域スキャンシステムShodanでは20%の機器しか推定できず，機器推定においてShodanの識別だけでは不十分であると確認できた．LLMによる評価では，gpt-3.5-turbo-0125と gpt-4-turbo-2024-04-09ともに60%以上の機器を推定することができ，大まかな機器推定であれば大規模に自動化処理ができる点で有用である．HTTP/1.0に限れば推定精度はさらに向上する．Basic認証要求応答は，評価者が人間でもLLMでも，Basic認証動作機器のフィンガープリントになりえるといえる．そのため，機器の設定を間違えてインターネット上に晒してしまうと，Basic認証要求応答から接続している機器が推定されてしまうため注意が必要である．一方これらの情報は，使い方を工夫すれば，企業のシステム管理者がネットワーク内に存在する機器を推定するなど，セキュリティを高めることに役立つ可能性も考えられる．

謝辞　本研究は，国立研究開発法人情報通信研究機構 (NICT) の委託研究（JPJ012368C08101）により得られた成果を含む．

参考文献

[1] Reschke, J.: The ‘Basic’ HTTP Authentication Sch., Internet Engineering Task Force (IETF) (2015).
[2] 大塚瑠莉，吉岡克成：IoT家電ハニーポットを用いたIoT家電のBasic認証に対する攻撃分析，暗号と情報セキュリティシンポジウム（SCIS）(2023).
[3] 藤田彬，江澤優太，田宮和樹，中山颯，鉄穎，吉岡克成，松本勉：特定のIoT機器のWebUIを狙ったサイバー攻撃の分析，情報処理学会論文誌，Vol. 61, No. 3, pp. 695–706 (2020).
[4] Shodan: Shodan Search Engine, Shodan (online), available from ⟨https://www.shodan.io/⟩ (accessed 2023-10-23).
[5] Censys: Censys Search, Censys (online), available from ⟨https://search.censys.io/⟩ (accessed 2023-10-26).
[6] R. Fielding, M. Nottingham, J. R.: HTTP Semantics, Internet Engineering Task Force (IETF) (2022).
[7] Arwa Abdulkarim Al Alsadi, Kaichi Sameshima, J. B. K. Y. M. L. M. v. E. C. H. G. n.: No Spring Chicken: Quantifying the Lifespan of Exploits in IoT Malware Using Static and Dynamic Analysis, Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, p. 309–321 (2022).
[8] 大塚瑠莉，九鬼琉, 吉岡克成：Basic認証が動作する機器へのサイバー攻撃の観測，情報処理学会論文誌，Vol. 65, No. 9 (2024).
[9] NOTICE: NOTICE, NOTICE (online), available from ⟨https://notice.go.jp/⟩ (accessed 2024-8-19).
[10] OpenAI: OpenAI, OpenAI (online), available from ⟨https://openai.com/⟩ (accessed 2024-8-6).
[11] Bar Meyuhas, Anat Bremler-Barr, T. S.: IoT Device Labeling Using Large Language Models, arXiv:2403.01586 (2024).
[12] Arunan Sivanathan, Hassan Habibi Gharakheili, V. S.: Detecting Behavioral Change of IoT Devices Using Clustering-Based Network Traffic Modeling, IEEE Internet of Things Journal (Volume: 7, Issue: 8, August 2020), pp. 7295–7309 (2020).
[13] Ivan Cvitić, Dragan Peraković, M. P. B. G.: DEnsemble machine learning approach for classification of IoT devices in smart home, International Journal of Machine Learning and Cybernetics, pp. 3179–3202 (2021).
[14] Mirian, A., Ma, Z., Adrian, D., Tischer, M., Chuenchujit, T., Yardley, T., Berthier, R., Mason, J., Durumeric, Z., Halderman, J. A. and Bailey, M.: An Internet-wide

view of ICS devices, 2016 14th Annual Conference on Privacy, Security and Trust (PST), pp. 96–103 (2016).

付　　録

```
You are a security expert.
Your task is to determin the device information
from the Basic Authentication response content.
The response is the content of the packet that
the device responds with when a third party
accesses the device via the internet.
The device is connected to the internet and
Basic Authentication in operation.
You need to provide as accurate device information
as possible from the response.

### Requirements ###
Output should be in capital letters.
Output should be in RC8259 JSON format
with following keys:
No.: str (the '{number}' from the input)
Hash: str (the '{hash_value}' from the input)
response: str (the '{response}' from the input)
device: str (what that device's name is)
device_reason: str
(why did you determine that to be the device name?)
maker: str
(what is the name of company that manufactured.
the device)
maker_reason: str
(why did you determine that to be the manufacture?)
model_number: str (what is the model number of
the device.)
model_reason: str
(why did you determine that to be the model number?)
type: str (what type of device is it? A router, modem,
server, camera, switch, PLC, etc.)
type_reason: str (why did you determine that to be
the type?)
reliability: int(how confident are you in your answer
ron a scale of 0-10;if not confident, use 0)
reliability_reason: str(why did you assign that level
of confidence?)

###Limitation###
 If the device or service cannnot be determined from
the response content, use "UNKNOWN" for the
undetermined fields.
```

図 A·1　プロンプト内容
Fig. A·1　Prompt content.