SCIS 2025 2025 Symposium on
Cryptography and Information Security
Kokura, Japan, Jan. 28 – 31, 2025
The Institute of Electronics,
Information and Communication Engineers

Basic 認証要求応答に着目した機器推定への ChatGPT search の適用
Application of ChatGPT Search to Device Inferrance Focusing on Basic Authentication Requests and Responses

大塚瑠莉 *†‡ インミンパパ ‡ 吉岡克成 §‡
Ruri Otsuka Yin Minn Pa Pa Katsunari Yoshioka

あらまし IoT 機器から汎用的なウェブサーバまで，インターネット上で幅広く使用されている認証方式の 1 つに Basic 認証がある．Basic 認証は，保護領域に対してアクセスされた際にクライアントへ認証要求応答をするが，その応答内にはメーカや製品型番など接続機器の推定へ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接続機器が推定可能かどうかを調査した．人手でのウェブ検索による機器推定と OpenAI の LLM による推定，ウェブ検索機能を有する AI サービスである ChatGPT search による推定結果を比較した結果，人による推定で 414 種類の機器が推定され，そのうち入手できた 7 機器については，推定結果と合致しており，推定結果の一定の妥当性が確認された．また，人による推定結果に対し，OpenAI の LLM では HTTP/1.0 において最大 81%，ChatGPT search では HTTP/1.0 において最大 90%の一致結果となり，これらを適用した機器推定の有用性を確認できた．

キーワード Basic 認証，デバイスフィンガープリント，LLM

1 はじめに

IoT 機器から汎用的なウェブサーバまで，インターネット上で幅広く使用されている認証方式の 1 つに Basic 認証 [1] がある．Basic 認証は，実装が容易かつ多くのウェブサービスに対応可能であるという利点から，IP カメラのウェブブラウザ経由での映像閲覧等，機器のマニュアルに記載されている機能だけでなく，管理者向けのページ等でも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，Basic 認証要求応答を返すホストが全世界で 250 万件以上確認されている [5]．利便性の高い Basic 認証ではあるが，認証時にやりとりするパケットを平文で送信することから，第三者に盗聴された場合に簡単に復号できてしまうというセキュリティ上の危険性も含む．Basic 認証における認証要求応答には，メーカーや型番を示すと推測される文字列を記載しているものがあり，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]．メーカーや型番と推定される文字列が realm に含まれている時，Basic 認証が利用されているサーバーの認証要求応答を入手してしまえば，それらの情報は簡単に入手できてしまう．IoT 機器の普及に伴い，IoT 機器がサイバー攻撃の標的となること，その中でも特に機器固有の脆弱性が標的になること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である [9]. Basic 認証における認証要求応答に接続機器の情報が含まれることは，一部のセキュリティ実務者や研究者等にとって既知の知見であると考えられるが，インターネット上で観測される Basic 認証応答に対して機器の識別可能性を大規模に調査した研究は我々の知る限り行われていなかった．そこで我々は，Basic 認証要求応答に含まれるメーカや製品型番を示すと推測される文字列を用いて手動でウェブ検索を行うことで 414 種類の機器の型番を推定できることを示した [10]．さらに手動での推定結果と OpenAI の LLM [11] による推定

* 三菱電機株式会社, 神奈川県鎌倉市大船 5-1-1, Mitsubishi Electric Corporation, 5-1-1, Ofuna, Kamakura, Kanagawa
† 横浜国立大学大学院環境情報学府, 神奈川県横浜市保土ケ谷区常盤台 79-7, Graduate School of Environment and Information Sciences, YokohamaNational University, 79-7, Tokiwadai, Hodogaya, Yokohama, Kanagawa
‡ 横浜国立大学先端科学高等研究院, 神奈川県横浜市保土ケ谷区常盤台 79-5, Institute of Advanced Sciences, Yokohama NationalUniversity, 79-5, Tokiwadai, Hodogaya, Yokohama, Kanagawa
§ 横浜国立大学大学院環境情報研究院, 神奈川県横浜市保土ケ谷区常盤台 79-7, Graduate School of Environment and Information Sciences, YokohamaNational University, 79-7, Tokiwadai, Hodogaya, Yokohama, Kanagawa

結果が最大で HTTP/1.0 において 81% の一致率となることを示した．しかしながら，これらの推定結果が実際に正しいかは検証できていなかった．そこで本研究では，手動で推定した機器のうち入手可能であった 7 機種について実際の機器の応答を確認し，推定の正しさを検証する．さらに，ウェブ検索により関連機器を探索するというタスクに対して，ウェブ検索機能を有する AI サービスである ChatGPT search[12] を用いた推定を新たに行い，従来の LLM の推定結果と比較する．具体的には以下の Research Questions(RQ) を設定する．

RQ1. Basic 認証要求応答に基づく機器推定はどの程度の精度が得られるのか．

RQ2. ウェブ検索機能を有する LLM である ChatGPT search により Basic 認証要求応答に基づく機器推定は改善するか．

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 414 種類の機器の型番と思われる文字列を識別し，そのうち入手できた 7 機種については推定に利用した Basic 認証要求応答と同じ WWW-Authenticate ヘッダーフィールドを持つことから，機器推定には一定の妥当性があることが確認された．RQ2 に対しては人間による推定結果と比較した時，OpenAI の LLM では HTTP/1.0 において最大 81%であるのに対して，ChatGPT search では HTTP/1.0 において最大 90%の一致結果となった．このように Basic 認証要求応答に着目した機器の推定は有効であり，ウェブ検索機能を有する LLM を用いることで機器推定の作業の精度を改善可能であることがわかった．

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[1]．一般的に，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，HTTP 認証を使用するサーバは 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，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．このことから，Shodan のウェブインタフェース上で,「Basic」「realm」,「HTTP/1.0 401 Unauthorized」または「HTTP/1.1 401 Unauthorized」を全て含む応答を行うホスト群を，含むべき文字列を検索クエリで指定することにより調査した．検索クエリで指定した結果得られた，ホスト数が多い応答内容の上位 1,000 種類[2]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 のウェブ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た．それらの応答には，Basic 認証の設計 [1] で共通して定められた文字列以外に，認証パラメータ「realm」の後に続く文字列や server フィールドに含まれる文字列など，応答を特徴づける文字列を含む．これらの文字列を，メーカーや型番などの機器識別に繋がる文字列と考え，手動で抽出した．抽出した文字列についてウェブ検索を行い，一致する文字列を含むウェブサイトを調査した．それらが IoT 機器やウェブアプリケーションのようなネットワークへ接続する可能性がある機器やサービスに関するものであるかを調べ，機器識別に繋がる情報であるかを判断した．ここで機器識別に繋がる情報を所有すると判断したものには，メーカーのウェブサイトや公開されている電子マニュアル，通信販売サイトが挙げられる．応答内の文字列を含むかどうか，ネットワークへつながる機能があるか，という特徴が合致する機器が存在するか確認し，確認された機器については，公開情報（メーカーのウェブサイトや電子マニュアル，脆弱性情報等）から，ネットワーク接続機能を有する可能性が高いことを条件に，その応答をする機器であると推定した．

2.2 実機での確認

推定した機器のなかで，実際に入手できた 7 種類の実機 (表 1) を用い，それらにアクセスして Basic 認証要求通信を取得した．なお，表 1 中のメーカー名，型番は，アルファベットで匿名化しており，同じアルファベットに関しては同じメーカー名を示す．これらの機器に対して、ローカルネットワーク環境から「GET / HTTP/1.1」リクエストを送信し，リクエストに対する応答として，機器から送られる通信を観測し，Basic 認証要求に含まれるメーカ名，型番を示すと推測される文字列がどの程度実機の情報を反映しているのか確認する．さらに，2.1 章で機器推定の手がかりとなった Basic 認証要求と当該機器の実機から得た応答とを比較する．具体的には，応答において WWW-Authenticate ヘッダーフィールドを

[1] 得られる情報の一例として，IP アドレスごとの解放ポート，ポートに対する応答が挙げられる．

[2] 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．

含む行が完全に一致するかを調査する．

表 1: 入手した実機一覧

型番	メーカー	デバイス種別詳細	HTTP version
a	A 社	スマート Wi-Fi ルーター	1.0
b	A 社	トライバンド ギガビットルーター	1.0
c	A 社	ワイヤレスルーター	1.0
d	A 社	ワイヤレスルーター	1.0
e	B 社	ADSL モデムルーター	1.1
f	B 社	ADSL モデムルーター	1.1
g	C 社	ネットワークカメラ	1.1

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 [11] による機器推定を行った．調査は，Basic 認証要求応答のリストを入力として OpenAI の API を利用して機器推定を行う python プログラムを自作して行った．LLM へ入力するプロンプト [10] は，与えられた Basic 認証要求応答の内容から，機器名，メーカー名，型番，タイプ，信頼度を回答させる．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．

さらに，OpenAI の LLM に基づいた生成 AI である ChatGPT [13] も調査に用いた．ChatGPT の機能の 1 つである ChatGPT search [12] では，プロンプトへ記述された質問に対してウェブ検索を行い，ウェブソースへのリンクとともに回答する．ChatGPT search ではプロンプト入力時にウェブ検索を行うため，最新の情報を反映した機器推定が行える可能性がある．ChatGPT のモデルは GPT-4o を使用し，temperture=0 で設定した．入力するプロンプトは付録の図 1 の通りであり，[10] をもとに作成した．なお，ChatGPT search では API 機能が実装されておらず，デスクトップとモバイルアプリでのみ使用可能であるため，API 使用時のように Basic 認証要求応答のリストを順番に読み込ませることができず，「response」に該当する Basic 認証要求応答の内容を直接デスクトップの ChatGPT に与えた．また，ChatGPT のデスクトップではチャット形式で回答を得るため，実験の途中で使用モデルや temperature の値が変更されていないかを確認するため，ChatGPT search のプロンプトに「gpt model」「gpt temperature」「source url」の項目を追加した．加えて，ChatGPT search は回答の根拠となるウェブソースのリンクを回答とともに出力するが，これらはブラウザ上にしか出力されないため，「source url」の項目を追加することにより，明示的に参照リンクを回答内に出力させるようにした．

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 件が Shodan 上で見つかった．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」「メーカー名」「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ー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 2 に示す．アプリケーションによっては IoT 機器のような型番がなく，アプリケーション名のみで提供されているため，型番の情報が含まれていなくても，応答内容からアプリケーションが一意に特定できるものについては，型番も推定できたとみなした．型番まで一意に推定できたものは，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%，一部推定できたものは，HTTP/1.0 が 188 種類で全体の 25%，HTTP/1.1 が 297 種類で全体の 30%，何も推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．

推定できた型番をもとに，その型番が付いているデバイスもしくはサービスのメーカーが該当の型番をどのような名称で販売しているかを，メーカーのウェブサイト

表 2: 機器推定件数（母数に対する割合（%））

	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%)

や公開されているマニュアルより調査し，分類した．分類した結果 [10],「サーバー」「ネットワーク」「メディア」「コンシューマ」「産業」「アプリケーション&OS」にタイプ分けすることができ，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．

3.2 実機での確認

表 1 記載の，7 種類の機器に対して，ローカルネットワーク上で「GET / HTTP/1.1」リクエストを送り，リクエストに対する応答として，機器から送られたパケットを取得した．7 種全ての機器は，リクエストに対する応答として「HTTP/1.0 401 Unauthorized」もしくは「HTTP/1.1 401 Unauthorized」を返し，通信の中には，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が含まれていた．なお，realm には，表 3 の realm 列記載の通り，メーカー名や型番と推測される文字列が含まれており，それらは実機の情報と一致した．具体的には，WWW-Authenticate ヘッダーフィールド内に，No.1 の機器は「realm = “メーカー名 型番”」，No.6 の機器は「realm = “型番”」と記載があった．さらに，その機器であると推定した Shodan により観測された応答内容と，今回実機から得た応答内容を比較した結果，調査対象である 7 種全ての機器に対して，WWW-Authenticate ヘッダーフィールドの記述が完全に一致した．また，得られた WWW-Authenticate ヘッダーフィールドと同一の WWW-Authenticate ヘッダーフィールドをもつホストが Shodan 上でどの程度存在するのかを調査した．調査には Shodan の Web インタフェースを用い,「HTTP/1.0 401 Unauthorized」もしくは「HTTP/1.1 401 Unauthorized」,「WWW-Authenticate:Basic realm=“realm”」を検索クエリで指定し，同一の WWW-Authenticate ヘッダーフィールドをもつホストを検索する．それらの結果（2024 年 12 月時点）をまとめたものが表 3 であり，検索クエリ指定時の，HTTP バージョン，“realm” の値については，表 3 中に記載の通りである．同一の WWW-Authenticate ヘッダーフィールドをもち，かつ，インターネットに接続されている機器が複数存在することを改めて確認した．

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 [11] の 2 種類のモデルと，OpenAI の LLM に基づいた生成 AI である ChatGPT の ChatGPT search [12] 機能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 件の型番に対して，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 のモデルおよび ChatGPT search 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%，ChatGPT search では 81%の機器を推定することができた．どちらの LLM 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．ChatGPT search では，2 つの LLM モデルよりも推定できる数が増加した．ChatGPT search のみが推定できる型番は 64 件であり，そのうち 27 件は HTTP/1.0 が対応し，37 件は HTTP/1.1 が対応している．ChatGPT search は WEB 検索し回答するため，gpt-3.5-turbo-0125，gpt-4-turbo-2024-04-09 よりも，推定に使用するデータが新しい．そのため，比較的新しい HTTP/1.1 に対応している型番に対し，他の 2 つのモデルよりも推定できる数が多くなったのだと考えられる．

推定された型番が HTTP/1.0 と HTTP/1.1 のどちら

表 3: 実機調査結果と同一応答を行う Shodan 内のホスト数

型番	メーカー	HTTP バージョン	realm	検知数	手動推定結果との比較
a	A 社	HTTP/1.0	“A a”	409	一致
b	A 社	HTTP/1.0	“A b”	468	一致
c	A 社	HTTP/1.0	“A c”	135	一致
d	A 社	HTTP/1.0	“A d”	1,164	一致
e	B 社	HTTP/1.0	“e”	890	一致
f	B 社	HTTP/1.1	“f”	172	一致
g	C 社	HTTP/1.1	“g”	31	一致

表 4: LLM による機器推定件数（母数に対する割合（%））

	gpt-3.5 -turbo-0125	gpt-4-turbo -2024-04-09	ChatGPT search
母数	414	414	414
推定可能	251 (61%)	278 (67%)	336 (81%)

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．ChatGPT search では，HTTP/1.0 で動く機器については全体の 90%を正しく推定し，HTTP/1.1 で動く機器については全体の 72%を正しく推定した．全ての LLM で 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．

さらに，LLM のモデルごとに，プロンプトで入力した項目に対する回答への正答数を求めた．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 種類のそれぞれの「device」「maker」「model number」に対し，人間が推定した結果を用意した．これらの項目はプロンプトで LLM へ回答させている．人間が推定した結果に対し，LLM の回答がどの程度一致したか

表 5: LLM による認証要求応答の識別（母数に対する割合（%））

LLM model	HTTP	推定数	割合
gpt-3.5-turbo-0125	1.0	146	70%
gpt-3.5-turbo-0125	1.1	107	51%
gpt-4-turbo-2024-04-09	1.0	170	81%
gpt-4-turbo-2024-04-09	1.1	111	53%
ChatGPT search	1.0	189	90%
ChatGPT search	1.1	150	72%

を示したものが表 6，7，8 である．「完全」は「完全一致」を意味し，LLM が回答したそれぞれの項目内の文字列が，人間が推定した結果と一致した場合にカウントした．ただし，大文字と小文字の違いは無視し，「maker」や「model number」内の，Inc.，Ltd.，ハイフンの有無等は，回答としては同じ意味のため正答と扱った．「部分」は「部分一致」を意味し，LLM が回答したそれぞれの項目内の文字列が，人間が推定した結果と部分的に一致した場合にカウントした．例として，人間が推定した結果が「XXX-2120」の際に LLM が「2120」と回答した場合が挙げられる．なお，表のスペースの関係で，「model number」は表中で「model」と記述する．「device」についてはどの LLM についても人間が推定した結果と一致した数が少ない．一方，「maker」についてはどの LLM でも一致した数が多い．HTTP/1.0，HTTP1.1 ともに，gpt-3.5-turbo-0125，gpt-4-turbo-2024-04-09，ChatGPT search の順に一致した数が多くなった．「model number」については，完全一致の数は HTTP/1.0，HTTP/1.1 ともに，gpt-3.5-turbo-0125，gpt-4-turbo-2024-04-09，ChatGPT search の順に増加したが，部分一致の数は gpt-4-turbo-2024-04-09 が最も多い結果となった．「device」の一致した数については，プロンプト内容が大きく影響を与えている可能性が高い．人間が推定した結果は「ROUTER」「CAMERA」のような一般名称を用意していたが，LLM は「device」項目で型番を回答した数が多く，不一致の扱いとなったものが多く存在した．今回使用したプロンプトの説明で

はLLMにとって不十分であった可能性が高い.「maker」の一致した数については，LLMのモデルによる一貫した傾向がみられた．これは，LLMがプロンプト内容から人間が意図した回答を正しく認識し，回答できたことによるものと考える．LLMのモデルが後発モデルになるにつれ完全一致の数が増加した．一方，ChatGPT searchで部分一致の数が他のLLMよりも少なくなったのは，ウェブ検索を行い得られた文字列をそのまま出力しているため，メーカー名などが正しく回答できたためと考える.「model number」の一致した数について，完全一致の数はLLMのモデルが後発モデルになるにつれて増加した．これはLLMの性能が向上したことに加え，「maker」と同様にChatGPT searchはウェブ検索で得られた文字列をそのまま出力していることから正しく回答できたのだと考えられる．一方，部分一致の数についてはgpt-4-turbo-2024-04-09が最も多い結果となった．

表 6: LLMによる認証要求応答の各項目の正答数 (gpt-3.5-turbo-0125)

	device		maker		model	
HTTP	完全	部分	完全	部分	完全	部分
1.0	38	20	305	2	136	61
1.1	13	61	182	10	73	31

表 7: LLMによる認証要求応答の各項目の正答数 (gpt-4-turbo-2024-04-09)

	device		maker		model	
HTTP	完全	部分	完全	部分	完全	部分
1.0	31	47	323	8	164	152
1.1	22	123	217	22	114	55

表 8: LLMによる認証要求応答の各項目の正答数 (ChatGPT search)

	device		maker		model	
HTTP	完全	部分	完全	部分	完全	部分
1.0	18	50	371	11	199	74
1.1	11	166	339	2	150	36

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 [14]，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 [15] や分類 [16] 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 [17] 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 [15]．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認証動作機器の推定へつなが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，LLMを活用して人間の機器推定を支援できるかを調査した．その結果，広域スキャンシステムShodanが蓄積するBasic認証要求応答から推定した機器のうち，実機を入手できた7機器については推定に使用した認証要求応答と同様のWWW-Authenticateヘッダーフィールドを持つことが確認でき，Basic認証要求応答から機器推定することへの一定の妥当性を確認できた．さらにLLMによる機器推定では，OpenAIのLLMではHTTP/1.0において最大81%，ChatGPT searchではHTTP/1.0において最大90%のの推定が人間による推定と一致しており，人間による機器推定の支援が可能であることがわかった．

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), https://www.shodan.io/ 2023-10-23.

[5] Censys: Censys Search, Censys (online), https://search.censys.io/ 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), https://notice.go.jp/ 2024-8-19.

[10] 大塚瑠莉，吉岡清和，Pa, Y. M. P.，吉岡克成 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，情報処理学会コンピュータセキュリティシンポジウム 2024 (2024).

[11] OpenAI: OpenAI, OpenAI (online), https://openai.com/ 2024-11-22.

[12] OpenAI: ChatGPT search, OpenAI (online), https://openai.com/index/introducing-chatgpt-search/ 2024-11-22.

[13] OpenAI: ChatGPT, OpenAI (online), https://openai.com/ja-JP/chatgpt/overview/ 2024-11-22.

[14] Bar Meyuhas, Anat Bremler-Barr, T. S.: IoT Device Labeling Using Large Language Models, arXiv:2403.01586 (2024).

[15] 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).

[16] 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).

[17] 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 determine 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 is 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 the following keys:
- gpt model: str (the GPT model used to generate the answer)
- gpt temperature: str (the GPT temperature used when generating the answer)
- response: str (the ‘{response}’ from the input)
- device: str (the name of the device, if identifiable)
- device reason: str (the rationale for determining the device name)
- maker: str (the name of the device's manufacturer)
- maker reason: str (the rationale for identifying the manufacturer)
- model number: str (the model number of the device, if identifiable)
- model reason: str (the rationale for identifying the model number)
- type: str (the type of device, e.g., router, modem, server, camera, switch, PLC, etc.)
- type reason: str (the rationale for identifying the type of device)
- reliability: int (a confidence level in your answer on a scale from 0 to 10; use 0 if not confident)
- reliability reason: str (the reason for assigning this confidence level)
- source url 1: str (the first information source URL used in your analysis; if unavailable, use "EMPTY")
- source url 2: str (the second information source URL used in your analysis; if unavailable, use "EMPTY")
- source url 3: str (the third information source URL used in your analysis; if unavailable, use "EMPTY")
- source url 4: str (the fourth information source URL used in your analysis; if unavailable, use "EMPTY")
- source url 5: str (the fifth information source URL used in your analysis; if unavailable, use "EMPTY")

Limitation
- If the device, manufacturer, model number, or type cannot be determined from the response content, use “UNKNOWN” for the undetermined fields.
- If fewer than 5 source URLs are identified, fill the remaining SOURCE URL fields with “EMPT”.

図 1: プロンプト内容 2