国内フリマサイトにおけるサポートが終了した中古ルーターの流通状況の調査

新堀 寛大[1,a)]　九鬼 琉[1]　藤井 翔太[2]　佐々木 貴之[2]　小林 信博[4]　吉岡 克成[3]

概要：CtoC-EC サイト (フリマサイト) で取引される中古 IoT 機器の中には，メーカーによるサポートが終了した（EoS）機器や，既知の脆弱性を抱えた機器が存在しているが，その流通状況やリスクの実態については十分に明らかにされていない．そこで本研究では，国内最大級のフリマサイトであるメルカリにおけるルーターの出品状況を調査した．ユーザーによって作成された商品説明文および商品画像に含まれる表記揺れや記述様式の差異を正確に解析するため，大規模言語モデル（LLM）を用いてモデル名およびメーカー名を自動的に抽出した．抽出した機器情報をもとに，NVD および JVN から取得した脆弱性情報，ならびに各社が公表しているサポート終了機器のリストと照合することにより，サポート終了済および既知の脆弱性を有するルーターの出品状況を明らかにした．さらに，我々が運用するハニーポットで観測された情報と照らし合わせ，実際に攻撃を受けている脆弱性があるか調査した．調査の結果，収集した 18,466 件の出品情報から，174 メーカーの 3,150 件の機種名が抽出された．そのうち 2,829 件 (313 機種) がサポート終了済機器，1,014 件 (108 機種) がサポート終了後に脆弱性が公開されていることを確認した．また，サポート終了後に脆弱性が公開された機器の内 288 件 (79 機種) が購入されていた．288 件の機器の中には，ハニーポットで攻撃リクエストを観測した脆弱性の影響を受ける機器が 109 件 (6 機種) あり，実際に攻撃を受ける可能性が高い機器がフリマサイトで取引されていることが明らかとなった．上記の解析の制約として，ユーザーが商品説明に記載したモデル名の表記揺れを LLM が完全に正規化できず，機種数が重複して計上されている場合がある．

キーワード：フリマサイト，IoT 機器，End of Support (EoS)

Investigation of the Distribution of End-of-Support Used Routers on Japanese Flea Market Platform

Shimbori Kanta[1,a)]　Kuki Ryu[1]　Shota Fujii[2]　Sasaki Takayuki[2]　Kobayashi Nobuhiro[4]
Yoshioka Katsunari[3]

Abstract: Some secondhand IoT devices traded on CtoC e-commerce sites (flea market) include devices that have reached end-of-support (EoS) status or contain known vulnerabilities. However, the situation of these devices remains unclear. To investigate the devices traded on the flea market, we surveyed router listings on Mercari, Japan's largest flea market platform. To accurately analyze variations and formatting differences in user-created product descriptions and images, we extracted model and manufacturer names using Large Language Models (LLMs). Based on the extracted information, we identified EoS devices and routers with known vulnerabilities by cross-referencing vulnerability data from NVD and JVN, plus manufacturers' end-of-support lists. We then compared findings with our honeypot observations to identify actively exploited vulnerabilities. The model extracted 3,150 device model names and 174 manufacturer names among 18,466 listings.We confirmed 2,829 listings (313 models) were EoS devices, and 1,014 listings (108 models) had post-EoS vulnerabilities. Additionally, 288 listings (79 models) with post-EoS vulnerabilities had already been purchased. Among these, 109 listings (6 models) contained unpatched vulnerabilities observed in honeypot attacks, revealing that devices likely to be attacked are being traded on flea market sites. As a limitation of the above analysis, the LLM could not fully normalize variations in model names described by users in product descriptions, which may have resulted in duplicate counting of device models.

Keywords: Flea market site, IoT devices, End of Support (EoS)

1. はじめに

現在，CtoC-EC サイト (フリマサイト) の市場規模は継続的な拡大を見せている．令和 5 年度の経済産業省の調査 [1] では，フリマサイトの市場規模は 2020 年から拡大を続けており，2022 年には 2 兆 3630 億円，2023 年には 2 兆 4817 億円と毎年 5 %の伸びを示している．これに伴い，フリマサイトへの IoT 機器の流通量も増加している．PC 等の高機能で複雑なシステムを持つ機器であれば，古くなると OS のサポート終了やアプリの非対応により，セキュリティアップデートや最新ソフトウェアが使えなくなり，破棄されることが多い．それに対し，ルーターやネットワークカメラなどの IoT 機器は要求される機能がシンプルであり，古い機器でも基本的に使用可能であるため，中古商品として出品されやすい．

しかし，IoT 機器の中には既にメーカーによるサポートが終了しており，既知の脆弱性が修正されない機器も存在する．そのような機器がフリマサイトに出品された結果，次の購入者の手に渡り，脆弱なまま使用される可能性もある．このような脆弱な機器を使用し続けた場合，ユーザーのプライバシーが危険に晒されるだけでなく，Mirai のようなボットネットを形成するマルウェアにより DDoS 攻撃の踏み台とされる可能性もある．

そこで本研究では，日本最大級のフリマサイトであるメルカリを対象とし，サポートが終了したルーターの流通状況を調査した．ルーターを対象とした理由は，IoT 機器の中でも常時インターネットに接続されており，攻撃を受けやすいからである．具体的には，メルカリにおいて「無線 LAN ルーター」カテゴリで出品されている商品の商品名，商品説明，商品画像，出品日時，価格，販売状況をクローラーを用いて収集した．ユーザーが作成した商品名や商品説明内に記載されているメーカー名およびモデル名には記述不足や表記揺れが含まれており，正確なメーカー名とモデル名を機械的に抽出することは難しい．そこで，これらの商品名，商品説明，および商品画像を LLM に入力し，出品されているルーターのメーカー名とモデル名の推測および正規化を行うことで，柔軟に機器の情報を収集した．LLM によるメーカー名およびモデル名の推測の正確性を検証するため，クローラーで収集したデータから一部をランダムで抽出して手動で正解データセットを作成し，LLM による出力と比較する評価を行い，後述の通り，十分な精度を有することを確認した．また，機器のサポート終了状況を調査するため，フリマサイトに出品されていたルーターのうち上位 5 社のメーカーに調査対象を絞り，各メーカーの公式 Web ページからサポート終了製品のモデル名とサポートが終了した日付の一覧を収集し，フリマサイトから収集したメーカー名およびモデル名と照合することで，出品されているルータのうちサポート終了を迎えている機器の件数と割合を調査した．さらに，機器に既知の脆弱性が存在しているかを調査するため，Japan Vulnerability Notes (JVN) と National Vulnerability Database (NVD) の API を用いて，フリマサイトから収集した機器のモデル名で検索し，当該機器に紐付く CVE-ID とその公開日，Common Vulnerability Scoring System (CVSS) スコアを収集した．加えて，脆弱性の公開日を前述のサポート終了日と比較することで，サポート終了後に脆弱性が見つかったルーターの特定も行った．上記の調査に際しては，LLM が出力したモデル名のユニーク数を計数し，これを機種数とした．ただし，ユーザーが商品説明に記述するモデル名には表記ゆれが存在するため，同一機種のルーターについて重複して計数してしまうことがある．このため，本論文で示す機種数は，実際の機器数よりも過大に算出されている可能性がある．

2025 年 6 月 5 日から 7 月 19 日までの間にメルカリ上から 18,466 件の出品情報を取得し，そのうち約 90%に相当する 16,583 件の出品についてメーカー名とモデル名を推測し，最終的に 174 社のメーカーにわたる 3,150 件の機種名を抽出した．さらに，出品されていた機器のうち，上位 5 メーカーの中でサポート終了日の一覧を公表している BUFFALO，NEC，ELECOM，I-O DATA に該当する出品は 10,791 件 (1,890 機種) あり，そのうち，調査を実施した 2025 年 7 月 19 日時点でサポートが終了していると判明した機器の出品が 2,829 件 (313 機種) であり，971 件の出品が購入されていた．さらに，サポート終了後に脆弱性が公開されている機器の出品が 1,014 件 (108 機種) 確認され，そのうち，288 件の出品が購入されていた．サポート終了後に脆弱性が公開された 108 機種には，32 件の脆弱性があり，その内 CVSS スコアが High(7.0) 以上であった脆弱性は 20 件 (43 機種) であった．この中で実際に悪用が確認された脆弱性のリストである KEV カタログ（Known Exploited Vulnerabilities Catalog）[2] に掲載されている脆弱性が 1 件 (8 機種) であった．

また，我々の研究室で運用する HTTP ハニーポット群で攻撃状況を調査した結果，セキュリティパッチが提供されておらず，かつその脆弱性に攻撃が観測されているルーターが 2,034 件（10 機種) 出品されており，そのうち 1,101

[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] 横浜国立大学大学院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/先端科学高等研究院
Faculty of Environment and Information Sciences, Yokohama National University / Institute of Advanced Sciences, Yokohama National University
[4] 長崎県立大学シーボルト校情報システム学部
Faculty of Information Systems, Nagasaki Prefectural University of Siebold
[a)] shimbori-kanta-hw@ynu.jp

件が購入されていることが明らかとなった．そのうち，サポート終了後に当該脆弱性が公開された機器は，185 件（8 機種) であった．ただし，サポート中に当該脆弱性が公開された機器についても，サポート期間内ではあるがセキュリティパッチが当てられず，回避策を行って使用を続けるか買い替えを検討するようメーカーから発表があった．よって，当該脆弱性の情報を知らず，回避策を実施していない利用者は，脆弱性のある機器を使用することになる．

加えて，本手法の精度を評価するために，メルカリに出品されている脆弱性のあるルーターから 103 件をランダムに抽出し手動での調査と比較したところ，手動での調査と 86%結果が一致した．一致しない場合の原因として，複数のルーターがセットで出品されている場合に 1 つしか推測できていない場合や，正確な出力を求めた結果十分な情報が得られず「Unknown」と出力してしまった場合があった．

調査結果から，購入されたルーターの約 3 分の 1 はメーカーによるサポートが終了していることが判明した．一般的にこれらの機器の使用は推奨されていない [3]．一方で，サポートが終了し，その後に公開された脆弱性を有するルーターの購入件数は 288 件と出品全体のごく一部にとどまった．しかし，288 件のうち 66 件のルーターについて，セキュリティパッチが当てられていない脆弱性を標的とした大規模な攻撃がハニーポットで観測された．この結果は，脆弱性を持つルーターが中古市場で流通し，購入者が知らずにセキュリティリスクを抱える状況を示している．

今後は取得対象期間や IoT 機器のカテゴリの拡大などを通じて，より包括的な実態把握を目指す予定である．さらに，将来的にはフリマサイトプラットフォーマーやユーザーへのインタビューを通じて社会的な課題を明らかにする予定である．

本論文の貢献は以下である．

- フリマサイトにおける中古 IoT 機器の流通について，セキュリティ問題を提起し，ルーターに関する調査を初めて行った．
- メルカリにおいて，サポートが終了したルーターが 2,829 件 (ルーター出品の 15%)，その中でサポート終了後に脆弱性が公開された機器は 1,014 件 (5%) であり，そのうち購入された機器は 288 件であった．
- ハニーポットによる情報収集からセキュリティパッチが提供されておらず，かつその脆弱性に攻撃が観測されているルーターが 2,034 件出品されており，そのうち 1,101 件が購入されていた．

2. 背景

本研究の背景として，サポートが終了した IoT 機器がフリマサイトで販売されている問題がある．PC やスマートフォンなどの汎用的な機器では，定期的な OS の更新や大規模なバージョンアップ（メジャーアップデート），さらには新世代 OS への移行（アップグレード）が行われる．加えて，多様なアプリケーションが提供されており，それらの機能拡張や追加に伴って対応 OS の更新が必要となる場合も多い．このため，最新のアプリケーションや機能を利用したいユーザにとって，機器を買い替える動機が生じやすい．これに対して，IoT 機器は特定の用途に特化して使用されることが多く，同一機器における OS のアップグレードやアプリケーションの更新は限定的である．その結果，機器の買い替えにつながる動機が生じにくい．

サポートが終了している IoT 機器はセキュリティパッチやファームウェアアップデートの提供が停止するため，新たに発見された脆弱性に対して無防備な状態に置かれてしまう．特にルーターのような IoT 機器の場合，常時インターネットに接続されており，外部からセキュリティソフトを導入することができないため攻撃者の標的となりやすい [4]．その結果，ユーザーの通信情報が第三者によって抜き取られる恐れや，Mirai やその亜種のような脆弱な IoT 機器を標的としてボットネットを形成するマルウェアにより DDoS 攻撃の踏み台とされる恐れがある．

また，フリマサイトにおける取引では，売り手と買い手の間に情報の非対称性が存在する．売り手は機器のサポート状況を把握していても，商品価値の低下を恐れて意図的に型番を隠蔽する可能性がある．その場合，買い手はサポートが終了した機器であることを認識せずに購入する可能性がある．

3. 関連研究

中古市場で流通している IoT 機器への調査について，Peiyu らの論文 [5] では，IoT 機器が再利用された際にパスワードや Wi-Fi 情報などユーザーの機密データが漏洩するリスクについて，ユーザー調査と IoT 機器のファームウェア分析により調査を行った．これにより，中古 IoT 機器を使用することの危険性を示している．また，Maxwell らの論文 [6] では，廃棄やリサイクルを行った IoT 機器について，個人情報の消去を行っているかユーザー調査によって明らかにし，対策方法を提示している．これらの論文は中古 IoT 機器に含まれている機密データについて調査した研究である．それに対し，本論文は中古市場におけるルーターの取引数と EoS の数について調査を行っている．

Dingding らの論文 [7][*1]では，インターネット空間に存在する EoS の IoT 機器の数と，それらに存在する脆弱性について調査している．インターネット空間には 300 万台以上の EoL デバイスが稼働しており，80 万台以上に OS コマンドインジェクション等の高リスクな脆弱性が存在しており，このうち 62 %は EoL 後に発見されたものであるとしている．この論文ではインターネット空間のルーターにつ

[*1] [7] では End-of-Life(EoL) を用いているが、本論文の EoS と同じ定義である

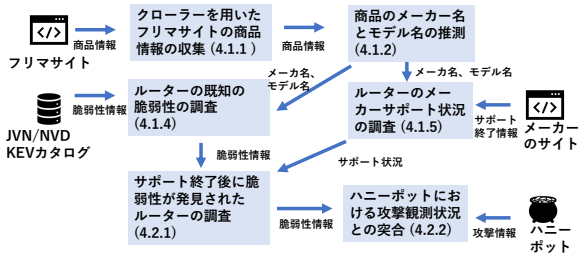

図 1　研究手法の概要

いて研究を行っているのに対し，本論文では，中古市場で EoS 製品がどれほど広がっているかについて調査を行う．

4.　調査手法

日本におけるフリマサイトとして，メルカリやヤフオク，ラクマ，ヤフーフリマ等があるが，本研究では国内におけるフリマサイトの初期調査として，6 割以上の市場シェアがある [8] メルカリを対象に調査を行った．

調査手法の概要を図 1 で示す．メルカリ内で「無線 LAN ルーター」カテゴリに登録されている商品について，クローラーを用いて商品名，商品詳細，商品画像，商品が購入済みか，商品詳細の最終更新からどれほど時間が経っているかを収集する．この調査により 2025 年 6 月 5 日から 7 月 19 日までの間に 18,466 件の出品情報を取得し，174 社のメーカーにわたる 3,150 件の機種名を抽出した．

4.1　データ収集

4.1.1　クローラーを用いたフリマサイトの商品情報の収集

メルカリの「無線 LAN ルーター」カテゴリから商品情報を収集するため，Python を用いて Web クローラーを開発した．Web ページの動的コンテンツ取得にはブラウザ自動操作ライブラリの Selenium を使用した．データは毎週土曜日に，更新日時が新しい順にソートされた商品から取得した．

メルカリの Web サイトは次のような構造になっている．検索結果ページには複数の商品が一覧表示され，各商品をクリックすると詳細ページに移動する．また，画面をスクロールすると追加の商品が動的に読み込まれ，一定数に達すると次ページへのボタンが表示される．この構造に対応するため，以下のステップでクローラーを実装した．

(1) メルカリの「無線 LAN ルーター」カテゴリで検索を行った後に Web ページを一番下までスクロールし，そのページ内全ての商品の個別ページへの URL を収集する
(2) 次のページへ遷移し（1）と同様の操作を行う
(3) この操作をメルカリの検索結果取得の上限である 100 ページ分行う
(4) 収集した個別ページへアクセスし，商品名，商品説明，商品画像，最終更新から経過した期間を記録する

上記の収集処理を，2025 年 6 月 5 日から 7 月 19 日までの間に，8 回実施した．同じ出品の情報が複数回収集される場合があるため，出品個別ページの URL をもとに同一出品の識別を行い，同じ出品があった場合，最新の情報を採用した．

4.1.2　出品されている商品のメーカー名とモデル名の推測

データ分析のために収集した商品名，商品詳細，商品画像からメーカー名とモデル名を抽出する．メーカー名は機器のサポートが終了しているか，モデル名は脆弱性があるかの調査に用いる．商品名と商品詳細からメーカー名やモデル名を機械的に抽出することは難しい，なぜなら，これらの情報はユーザーが入力したものであり，ユーザーごとに表記方法が違うためである．また，ユーザーによってはメーカーや型番に関する情報を商品名と商品詳細に記載しておらず，商品の写真から情報が得られる場合もある．

そこで本研究では，メーカー名とモデル名の抽出に大規模言語モデル（LLM）を用いる．LLM の特徴である自然言語の理解能力を活かし，商品名，商品詳細，商品画像からモデル名とメーカー名を推測させる商品情報推測システム (以下，推測システムと呼ぶ) を構築した．LLM のモデルは gpt-4o を用い，temperature は 0.7 とした．この際，LLM が推測したメーカー名について表記ゆれが起こらないようにするために，メルカリにおける出品件数上位のメーカー 5 社 (BUFFALO，NEC，ELECOM，TP-Link，I-O DATA) については，プロンプト内で表記を指定した．使用したプロンプトを以下に示す．

プロンプト

以下の情報はメルカリにおいて「無線 LAN ルーター」と検索して出てきた商品における商品名、商品説明、商品画像の情報です。これらの情報を分析して、ルーターのメーカー名とモデル名を推測してください。メーカー名について「Buffalo」「バッファロー」は「BUFFALO」、「Aterm」「nec」「エヌイーシー」は「NEC」、「IOdata」「アイオーデータ」は「I-O data」、「エレコム」「elecom」は「ELECOM」、「tplink」「TPLink」は「TP-Link」などのように、正式なメーカー名を使用してください。
レスポンスは上記の形式のみで回答し、余計な説明は不要です。

4.1.3　メーカー名とモデル名の推測精度の検証

LLM が推測したメーカー名とモデル名が人間が調査したものとどれほど離れているか，テストデータを作成して検証を行った．具体的には，クローラーで収集した出品データからランダムに 103 件の出品データを選び，それらについてメーカー名とモデル名を手動で確認し正解データセットを作成した．並行して，同様の出品データを推測シ

ステムに入力し，メーカー名とモデル名を推測させた．最後に，推測システムの出力結果と人手で推測した結果の一致度を評価した．

その結果，103 件のデータのうち 89 件のデータで LLM の出力と手動の結果が一致した．一致しなかった 14 件について，モデル名を正しく推測できなかったものが 5 件，メーカー名を正しく推測できなかったものが 4 件，それ以外の理由が 3 件であった．モデル名およびメーカ名の誤推測が生じる要因として，ユーザが商品説明に記載したモデル名/メーカ名の表記ゆれが挙げられる．例えば，半角スペースと全角スペース，英字の大文字と小文字などの違いにより，LLM がこれらを正規化できず，正式なモデル名/メーカー名を出力できない場合がある．それ以外の理由としては，複数のルーターがセット売りされていた際，１つのルーターについては正しく推測できているがその他について推測できていない場合であった．

4.1.4 ルーターの既知の脆弱性の調査

JVN および NVD が提供する WebAPI を利用し，推測システムが出力したモデル名をキーワードとして脆弱性情報を検索する．脆弱性情報が取得できた場合は CVE-ID と公開日を記録し，モデル名と紐付ける．両データベースで同一の脆弱性情報が確認された場合には，公開日は両者のうち早い方を採用する．また，それらの脆弱性が悪用されているかを調査するために，KEV カタログ [2] を取得し，CVE-ID との照合を行った．

4.1.5 ルーターのメーカーサポート状況の調査

ルーターのサポート状況について，以下の手順で調査を行った．まずメーカー公式サイトから各モデルのサポート情報（モデル名，サポートの有無，サポート終了年月）を収集し，メーカーごとのサポート状況データベースを作成する．そして，クローラーで収集したデータのモデル名とサポート状況データベースのモデル名を照合し，各モデルのサポート状況を特定する．

サポート状況データベースの作成では，対象となる企業が膨大な数であるため，メルカリにおける出品件数上位 5 社のルーターメーカー (BUFFALO，NEC，ELECOM，TP-Link，I-O DATA) の中からサポート状況を公開していない TP-Link を除いた 4 社のみでデータベースを作成した．なお，この 4 社のみでメルカリ内の商品情報が 10,791 件あり，全体の 65 %以上を占める．

4.2 データ分析

4.2.1 サポート終了後に脆弱性が公開されたルーター

サポート終了後に脆弱性が公開されたルーターの数を調査する．このようなルーターはセキュリティアップデートが行われる可能性が低く，既知の脆弱性が修正されないため，攻撃を受ける可能性が他のルーターと比べても高い．このようなルーターがメルカリ内でどの程度出品されているのか，また実際にどの程度購入されているのかを調査する．

さらに，サポートが終了したルーターが持つ脆弱性の重大度を調査するため，脆弱性の CVSSv3.0 のスコアを参照し，v3.0 のスコアが算出されていない古い脆弱性については v2.0 のスコアを参照した．具体的には，サポート終了後に JVN または NVD で公開された脆弱性の CVE-ID を抽出し，その CVE-ID に紐付く CVSS スコアを収集する．また同時に KEV カタログを用いて，現時点で悪用が確認されている脆弱性が存在するかの調査を行う．

4.2.2 ハニーポットにおける攻撃観測状況との突合

メルカリに出品されていた機器に紐づく CVE-ID について，実際のインターネット空間上でどの程度攻撃が観測されているかを把握するため，我々が運用する HTTP ハニーポット群である X-POT[9] における観測ログとの突合を行った．X-POT は，インターネット上に公開されている機器やサービスの応答を収集することにより，模倣する機器の種類を拡張することができる適応型 HTTP ハニーポットである．観測された攻撃リクエストについては，既知の公開脆弱性情報などに基づき，攻撃の対象機器や脆弱性（CVE-ID）を特定し，当該ログにタグ付けする機能を備えている [10]．

本研究では，2019 年 7 月 21 日から 2025 年 8 月 8 日までの約 6 年間に，日本国内を含む計 22 件のインスタンスから収集した観測ログを用いて，各 CVE-ID ごとに全期間における攻撃観測件数（HTTP セッション数）を調査した．なお，X-POT の観測対象は HTTP プロトコル経由のリクエストに限定され，さらに分析対象は OS コマンドインジェクションなどのリモートコード実行を目的とした深刻な脆弱性を狙った攻撃のみに限られることから，本分析はすべての既知の脆弱性に対する攻撃傾向を網羅するものではない点に留意が必要である．

5. 調査結果

5.1 中古機器全体の流通状況

メルカリ内のルーター全体の分析結果を以下に示す．今回の調査では 2025 年 6 月 5 日から 2025 年 7 月 19 日の期間で，重複を除いて 18,466 件のルーターが出品されていた．このうち 1,667 件については，商品ページへの URL は収集できたが，商品が削除されていたため商品ページへアクセスできず，商品情報の詳細を収集することができなかった．これは，出品者によって出品が取り下げられた，規約違反によりフリマサイト運営者によって削除された，取引完了後に出品者によって商品情報が削除された等の可能性がある．

全体の出品状況について，2025 年 7 月 19 日の段階で出品ステータスが「出品中」となっているのが 9,156 件，購入済みとなっているのが 7,643 件であった．最終更新時間

表 1　メルカリにおけるメーカー別出品数・機種数

メーカー名	出品件数	機種数	メーカー名	出品件数	機種数
BUFFALO	5,337	914	NEC	3,369	475
TP-Link	2,820	325	ELECOM	1,274	331
I-O data	811	170	ASUS	378	84
ZTE	368	38	その他	2,226	835
不明	1,883	-			
	合計	18,466 件	3,150 機種		

は「5 分前」から「半年以上前」まで存在していた．メルカリは半年より前の更新時間については表示しておらず，また出品された日付等も表示していないため，6 か月以前に出品された商品については正確な出品時期の特定は困難である．

出品されていたルーターのメーカー内訳について表 1 に示す．全体のメーカー数は 174 社，機種数は 3,150 機種であった．BUFFALO，NEC の上位 2 社で全出品の約半分 (8,706 件) を占めており，そこに TP-Link，ELECOM，I-O DATA を加えた 5 社で約 75 % (13,611 件) を占めている．

表 1 の機種数については，LLM による推測の段階でテキストベースの商品情報に加えて商品画像も入力するなど，表記ゆれの抑制に努めた．しかし，それらを行った上でなおモデル名の表記ゆれが残存し，重複を完全には排除できていない可能性がある．

5.2　サポートが終了した中古ルーターの流通状況

BUFFALO，NEC，ELECOM，I-O DATA の 4 社についてサポートが終了したルーターの数を表 2 に示す．今回の調査ではサポートが終了していると判明した機器の出品が 2,829 件 (313 機種) あり，971 件の出品が購入されていることが判明した．サポートが継続している製品は 3,924 件中 2,594 件購入されているため，購入済みの割合はサポート中の機器よりサポートが終了した機器の方が少なくなっている．

各社におけるサポート不明機器の理由を調査したところ，次の 2 つの理由が判明した．1 つ目はルーターの販売会社と製造会社が異なり，製造会社がサポート状況を公開していない場合である．例えば，メルカリ内で出品されているルーターの中には UQ コミュニケーションズ株式会社が NEC に委託して ODM 生産を行っている製品が一定数存在した．この場合，出品者がこれらのルーターを NEC の製品として商品説明を記載し，LLM がその記載に基づいて誤った推測を行ってしまうため，「不明」として分類せざるを得なかった．また，NEC と UQ コミュニケーションズ双方の公式 Web ページでは，これらの製品のサポート状況について発表していなかった．

2 つ目は，同一のモデルに対してユーザーごとに異なる形式で記述される場合である．NEC 製のルーター「PA-W300P-B」を例に挙げると，フリマサイトのユーザーは「PA-W300P」「W300P」「Aterm PA-W300P」「Aterm W300P」など，ユーザーによって多様な記述方法を取る．今回利用した LLM のモデルではこれらのモデルの正規化までは行うことができず，そのままモデル名として出力されてしまう．このような表記揺れは，機種数の計測の際の重複計上の原因になっている．

5.3　サポート終了後に脆弱性が公開されたルーターの流通状況

サポートが終了した後に脆弱性が公開された製品の数を表 2 に示す．全体としてこのような製品は 1,014 件 (108 機種) 出品されており，さらにその中で 288 件 (79 機種) は実際に取引されていることが判明した．これら 288 件の 79 機種のうち，それらの機種に見つかっている脆弱性は 32 件であり，CVSS スコアが High (7.0) 以上であった脆弱性は 20 件 (43 機種) であった．ある製品には CVSSv3 が Critical (9.0) である脆弱性が発見されており，少なくとも過去 1 か月以内に取引されていた．

また，出品されていた 1,014 件のうち，KEV カタログに掲載された脆弱性に該当するものは 185 件あり，そのうち 20 件は実際に購入されていた．当該脆弱性に対する攻撃は，次節で示すハニーポットでも観測されていた．

5.4　ハニーポットにおける攻撃観測状況

メルカリに出品されていた機器に紐づく既知の CVE-ID について，ハニーポットにおける攻撃観測状況を調査したところ，14 件の CVE-ID について，当該脆弱性を狙う攻撃が観測されていたことを確認した．中でも CVE-2014-8361 を狙う攻撃リクエストは 14 件の CVE-ID のうち最多となる 118,988 件観測されており，観測期間末の直近 7 日間（2025/8/2〜8）でも攻撃が継続していた．CVE-2014-8361 は Realtek SDK の Miniigd サービスに起因するリモートコード実行の脆弱性であり，BUFFALO，NEC，ELECOM など複数ベンダーにわたる多数の製品が影響を受ける．メルカリにおける当該脆弱性の影響を受ける機器の出品は 1,221 件 (108 機種) あり，うち 650 件（54.2%）が購入済であった．さらに，本脆弱性の影響を受ける機器のうち一部（10 機種）はセキュリティパッチが提供されておらず，製品の使用停止や緩和策の適用が推奨されていた [11], [12]．

サポートが終了した後に当該脆弱性が公開された機器に限定すると，前節で示した KEV カタログに記載されている機器数と同じであり，当該脆弱性の影響を受ける機器の出品は 185 件 (8 機種)，うち 20 件（11%）が購入済である．

6.　考察と課題

6.1　フリマサイトにおける中古ルーターの脅威

今回の調査から，フリマサイト内でサポートが終了したルーターや脆弱性を持つルーターは取引されているが，出

表 2　メルカリにおける EoS 製品の出品数 (機種数)

メーカー名	総出品数	サポート中	サポート状況不明	サポート終了	サポート終了後に脆弱性公開	サポート終了後に公開された脆弱性が KEV に掲載
BUFFALO	5,337 (914)	2,589 (188)	1,316 (589)	1,432 (137)	468 (46)	0
NEC	3,369 (475)	694 (88)	2,466 (334)	588 (53)	379 (39)	163 (6)
ELECOM	1,274 (331)	493 (37)	502 (248)	279 (46)	123 (19)	22 (2)
I-O data	811 (170)	148 (15)	133 (78)	530 (77)	44 (4)	0
合計	10,791 (1,890)	3,924 (328)	4,417 (1,249)	2,829 (313)	1,014 (108)	185 (8)

品数全体の 10,791 件に対して，サポートが終了したルーターの件数は 2,829 件（26.2%）と限定的であることが明らかとなった．その一方で，サポート終了後に脆弱性が公開されている機器の出品が 1,014 件確認され，288 件の出品が購入されていたことが判明した．また，ハニーポットによる観測で実際に攻撃を受けている脆弱性の影響を受けるルーターが 2,034 件出品されており，そのうち 1,101 件が購入されていることを確認した．

これらの脆弱性については，メーカーから軽減策や回避策が公開されている．しかし，今回の調査では出品者がこうしたセキュリティリスクを商品説明に記載している例は見つからなかった．購入者は脆弱性の存在を知らないまま機器を使用し，サイバー攻撃の被害に遭う危険性がある．

サポートが終了した機器については数多くの出品と取引を確認した．これらの機器について，一般的に使用を停止することが推奨されているが，実際にそのまま利用し続けることにどれほどリスクがあるのかは判明していない．そこで，今後は脆弱性が修正されない機器を使い続けることのリスクについて，詳細な分析を進める．

また，メルカリにおける脆弱性を持つルーターの流通の実態が明らかになったが，ユーザーのセキュリティリスクに対する認識の程度については不明な点が多い．ユーザーは中古機器を購入する際にセキュリティにどれほど気をつけているのか，ユーザーは脆弱な機器であることを知った上で購入していたのか，知らなかった場合，もし脆弱な機器であると知ったならばユーザーの購入意欲にどれほど違いがあるのか，ユーザーの視点に立った調査を行うことが必要である．

6.2　課題

6.2.1　モデル名の表記揺れ

フリマサイトの商品名や商品説明がユーザーによって任意に記載されることに加え，LLM による推測においてもメーカー名やモデル名に表記揺れが生じるため，データの表記に一貫性を欠くという問題が生じる．出力するメーカー名やモデル名をプロンプト内で指定することで表記揺れを回避できるが，メーカー名やモデル名を網羅的に指定することは難しい．「JVN が公表している「JPCERT/CC 製品開発者リスト 登録ベンダ一覧」を参考にメーカー名を出力してください」というプロンプトで推測を行った場合でも表記揺れは発生した．

また，OEM/ODM の供給形態に起因して，単一の製品が複数の事業者によって異なるブランド名やモデル番号で流通するケースにおいて脆弱性の有無やサポートの状況について正確に把握することが難しい場合がある．ユーザーがフリマサイトで出品する場合は一方のモデル名で出品していることが多いため，それら 2 つを同一製品として計数するにはそれぞれの対応表を作成する必要があり，OEM/ODM の機種数を考えると困難である．

6.2.2　Web クローリングにより収集できる情報の限界

メルカリの Web サイトの仕様上，カテゴリ検索では 100 ページ分までしか取得できない制限がある．「無線 LAN ルーター」カテゴリには大量の出品があるため，この 100 ページ制限により全ての出品情報を収集できていない可能性がある．ただし，本研究のデータには最終更新が「半年以上前」となっている古い出品も含まれていることから，過去 1 年間の出品の大部分はカバーできていると推測される．今後も継続的にデータ収集を行うことで，より網羅的な情報収集が可能になると見込まれる．

6.3　今後の展望

フリマサイト事業者とユーザーのセキュリティ意識調査：フリマサイトの運営会社と実際に利用しているユーザーに対してアンケート調査を実施する予定である．具体的には，フリマサイトの運営会社では EoS 機器の出品に対してどのような見解を持っているか，ユーザー側では購入時にサポートや脆弱性の有無をどの程度意識しているかを明らかにする予定である．

フリマサイト事業者や機器メーカーと連携した中古機器購入者への注意喚起：本研究の調査結果をもとに，フリマサイト事業者や IoT 機器メーカーと連携して中古ルーター購入者に対する効果的な注意喚起の方法を検討する．具体的には，商品ページでのセキュリティ警告の表示や，メーカーのコンパニオンアプリを用いて機器のサポート終了情報の発信などが考えられる．実際に注意喚起を実施した後の購入者行動の変化を追跡調査することで，どのような方法が最も効果的かを評価することも可能である．

EoS ルーターのセキュリティリスク調査：メーカーや公

的機関が行う注意喚起では，サポートが終了したルーターは買い替えが推奨されている．しかし，実際にサポートが終了したルーターがどの程度危険かは明らかになっていない．そこで，サポート終了しているか否かで攻撃を受ける件数に差はあるのか，実際に悪用される割合は変わるのか等を調査し，今回の調査で判明した EoS のルーターにどれほど脅威があるのかを明らかにする．

BtoC EC サイトにおける EoS ルーターの調査：本研究ではフリマサイトを調査したが，大手 BtoC EC サイトでも EoS ルーターの流通状況を調査する．大規模な BtoC サイトでは様々な販売者がサイト内で出品を行うマーケットプレイス型の出品が行われることがある．このような場合，すでにサポートが終了した製品が在庫として残り，新品の商品として売られている場合がある．このような場合についても調査を行い，EoS ルーターの流通状況の全体像をより正確に把握する予定である．

6.4 研究倫理

本研究を実施するにあたり，Menlo Report [13] に基づいて，研究で得られる利益の最大化と，起こりうる害の最小化を考慮して実施した．

Web クローリングによりフリマサイトのサーバーへ過度な負荷が掛かることを防ぐため，各リクエスト間の待機時間を 2 秒に設定した．データ収集の範囲については，フリマサイトの robots.txt で許可されている範囲を遵守し，ユーザー登録やログインを必要としない一般公開ページ（出品一覧ページおよび商品個別ページ）のみをアクセス対象とした．加えて，個人情報に該当する可能性のある出品者情報については一切収集せず，商品情報のみに限定して収集した．さらに，研究の透明性を確保するため，Web クローラーを実行するサーバー上に Web ページを公開し，研究実施機関，研究目的，連絡先情報，およびオプトアウトの申請方法について明記した．これにより，サイト運営者が必要に応じて研究者に連絡し，データ収集の停止を要請できる体制を整えた．

収集したデータの取り扱いに関して，脆弱性が確認されているルーターについては，メーカー名や機器のモデル名を適切に匿名化し，特定の製品が識別されないよう配慮した．一方で，フリマサイト名および（脆弱性の特定に直結しない範囲での）メーカー名については，公表による業績やブランドイメージへの負の影響が軽微であると判断したため，学術的な再現性と透明性の観点から実名を記載した．

7. 結論

本研究では，中古市場におけるサポートが終了しているルーターや，その中で脆弱性を持つルーターの流通状況について初めて調査を行った．フリマサイトで販売されているルーターを Web クローリングによって調査し，ユーザーが記載した商品情報から LLM を用いてメーカー名，モデル名を抽出した．また，脆弱性データベースの API やメーカー公式サイトの機器サポート情報を用いて，サポートが終了した製品やサポート終了後に脆弱性が公開された商品の数を分析した．本研究ではフリマサイト上で 18,466 件の出品情報を収集し，その情報から 3,150 件の機種名を抽出した．そのうち 2,829 件（313 機種）がサポート終了済機器，1,014 件 (108 機種) がサポート終了後に脆弱性が公開されていることを確認し，さらにその中で 288 件 (79 機種) は実際に取引されていることが判明した．

謝辞　本研究の一部はＮＥＤＯ（国立研究開発法人新エネルギー・産業技術総合開発機構）の委託事業「経済安全保障重要技術育成プログラム／先進的サイバー防御機能・分析能力強化」（JPNP24003）によるものである．

参考文献

[1] 経済産業省 商務情報政策局情報経済課. 令和５年度 電子商取引に関する市場調査 報告書. https://www.meti.go.jp/press/2024/09/20240925001/20240925001-1.pdf, 2023.
[2] CISA. Known exploited vulnerabilities catalog. https://www.cisa.gov/known-exploited-vulnerabilities-catalog.
[3] IoT 推進コンソーシアム 総務省経済産業省. Iot セキュリティガイドライン ver 1.0. https://www.soumu.go.jp/main_content/000428393.pdf, 2016.
[4] 警視庁. Wi-fi（無線 lan）ルーターをお使いの方へ - 警視庁ホームページ. https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/security/cyber401.html, 2024.
[5] Peiyu Liu, et al. How IoT Re-using Threatens Your Sensitive Data: Exploring the User-Data Disposal in Used IoT Devices. In *IEEE Security and Privacy*, 2023.
[6] Maxwell Keleher, et al. Balancing Security and Longevity: Benefits of Modular IoT Infrastructure. In *New Security Paradigms Workshop*, 2025.
[7] Dingding Wang, et al. An Empirical Study on the Insecurity of End-of-Life (EoL) IoT Devices. In *IEEE Transactions on Dependable and Secure Computing*, 2023.
[8] 株式会社大和総研. 令和３年度 電子商取引に関する市場調査. https://www.meti.go.jp/press/2022/08/20220812005/20220812005-i.pdf, 2021.
[9] 佐々木貴之 他. ハニーポットによる攻撃観測と多角的分析のための統合アーキテクチャの提案. 情報処理学会コンピュータセキュリティ研究会, 2022.
[10] 九鬼琉 他. ハニーポットで観測される新規エクスプロイトの分類手法の提案. コンピュータセキュリティシンポジウム 2024 論文集, 2024.
[11] JVN iPedia. Jvndb-2021-000028 複数の aterm 製品における複数の脆弱性. https://jvndb.jvn.jp/ja/contents/2021/JVNDB-2021-000028.html, 2021.
[12] JVN iPedia. Jvndb-2021-000008 複数のエレコム製品における複数の脆弱性. https://jvndb.jvn.jp/ja/contents/2021/JVNDB-2021-000008.html, 2021.
[13] The menlo report: Ethical principles guiding information and communication technology research, 2012.