セキュリティホールか意図的なバックドアか？ IoT機器におけるマニュアルに記載されていない Telnet・SSHサービスの調査

宮本 岩麒[1,a)]　九鬼 琉[1,b)]　藤井 翔太[1,c)]　佐々木 貴之[1,d)]　吉岡 克成[1,e)]

概要：IoT 機器の普及が進む一方で，ユーザーマニュアルに記載のないアクセス機構が実装されている機器が存在し，深刻なセキュリティリスクに繋がる恐れがある．しかし，これらの隠されたアクセス機構がどの程度の機器に存在しているのか，さらにそれらは意図的に埋め込まれたバックドアなのか，開発過程の見落としによるセキュリティホールなのかは明らかになっていない．そこで本研究では，大規模なファームウェア解析，マニュアル調査，およびメーカーへのアンケート調査を通じて，この問題の実態解明を試みる．202 社から収集した 173,768 個のファームウェアを解析した結果，エミュレーション環境において 9 社 63 機種でマニュアルに記載のない Telnet/SSH サービスを発見した．このうち 6 社 16 機種でハードコードされたアカウントによる遠隔ログインが可能であった．これらの発見についてメーカーへアンケート調査を行った結果，9 社中 7 社から何らかの回答を得た．このうち 3 社は保守・管理目的での実装を認めたが，アクセス機構がマニュアルに記載されていない理由についての十分な説明はなかった．以上により本研究では，大規模なファームウェア解析とメーカーへのアンケート調査を通じて，IoT 機器におけるマニュアルに記載されないアクセス機構の実態について議論する．

Security Hole or Intended Backdoor? Investigating Undocumented Telnet and SSH Services on IoT Devices

Iwaki Miyamoto[1,a)]　Ryu Kuki[1,b)]　Shota Fujii[1,c)]　Takayuki Sasaki[1,d)]　Katsunari Yoshioka[1,e)]

Abstract: The proliferation of Internet of Things (IoT) devices enhances daily life, yet some devices contain undocumented access mechanisms not mentioned in user manuals, potentially leading to serious security risks. However, the extent to which these hidden access mechanisms exist and whether they represent intentionally embedded backdoors or overlooked security vulnerabilities remains unclear. This research clarifies this issue through large-scale firmware analysis, user manual investigation, and manufacturer surveys. Analysis of 173,768 firmware images from 202 companies revealed undocumented access mechanisms in 63 device models from 9 manufacturers within emulation environments. Among these, 16 device models from 6 manufacturers permitted remote login through hardcoded accounts. Manufacturer surveys yielded responses from 7 of the 9 companies. While 3 manufacturers acknowledged implementing these features for maintenance and management purposes, they provided insufficient explanations for why these mechanisms were undocumented. This research discusses the actual state of hidden access mechanisms in IoT devices.

[1] 横浜国立大学
Yokohama National University
[a)] miyamoto-iwaki-yk@ynu.jp
[b)] kuki-ryu-dr@ynu.jp
[c)] fujii-shota-pv@ynu.ac.jp
[d)] sasaki-takayuki-yv@ynu.ac.jp
[e)] yoshioka@ynu.ac.jp

1. はじめに

IoT(Internet of Things) 機器の普及は日常生活に大きな利便性をもたらす一方で，新たなセキュリティリスクを生み出している．特に，一部の IoT 機器では，ユーザーマ

ニュアルに記載のない Telnet や SSH サービスが有効化されていたり，ハードコードされたアカウントが埋め込まれていたりする事例が多数報告されている [1], [2], [3]．これらのマニュアルに記載されていないアクセス機構は，ユーザーの認知や同意なしに機器メーカーあるいは第三者によるリモートアクセスを可能にするものであり，長期的かつ持続的なセキュリティリスクに繋がる恐れがある．

この問題に対し，先行研究では主に二つのアプローチを通じて取り組まれてきた．一つは，IoT 機器のファームウェアの解析を通じて，隠されたアクセス機構を検出する技術的アプローチである．具体的には，ハードコードされた認証情報の抽出や疑わしいコードパターンの特定を行う静的解析 [4] や，エミュレーション環境下でファームウェアの動作を観察し，不審なネットワークサービスや脆弱な実装を発見する動的解析 [5] などが挙げられる．もう一つは，IoT 機器メーカー向けのベストプラクティスの策定および推奨事項の提示 [6] や，IoT 市場における規制強化の提言 [7] などの予防的アプローチである．

これらの先行研究の多くは特定の機器や少数の事例を対象とした分析にとどまっており，このような IoT 機器のアクセス機構がどの程度存在しているかという点について，大規模かつ体系的に実態を把握する研究は限られている．また，発見されたアクセス機構がユーザーマニュアルなどで適切に明示されているかどうかを検証する視点も十分に検討されてこなかった．

さらに，このようなマニュアルに記載されていないアクセス機構が発見された場合に，それが開発上の不備や見落としにより意図せず製品に残留した「セキュリティホール」なのか，あるいはメーカーによって意図的に実装された「バックドア」なのかによって，求められる対応や社会的影響は大きく異なる．前者であれば，セキュリティパッチの適用や開発プロセスの改善といった対応が有効であるのに対し，後者の場合，メーカーに対する透明性や情報開示責任の追及，さらには業界団体や公的機関を通じた規制措置や情報共有などの対応が求められるためである．しかしながら，こうした実装の背後にある根本的な原因やメーカーの意図性については，先行研究では明らかにされていない．そこで本研究では，**RQ1：ユーザーマニュアルに記載されていないハードコードされたアカウントによる Telnet/SSH アクセスが可能な IoT 機器は，どの程度存在しているか？**および **RQ2：機器メーカーはユーザーマニュアルに記載されていないアクセス機構を意図的に実装しているか？そうであればその目的は？**に取り組む．

まず, RQ1 に答えるため, 202 社の IoT 機器メーカーから収集した 173,768 件のファームウェアに対して静的・動的解析を実施し，ハードコードされたアカウントと Telnet/SSH サービスの存在を調査した．また，対応するユーザーマニュアルを収集してアクセス機構の記載状況を確認し，未記載の機器についてはエミュレーション環境でログインできるかどうかを実験した．以上により，9 メーカーの 63 機種において，ユーザーマニュアルに記載されていない Telnet または SSH サービスが有効になっていることを確認した．さらに，このうち 6 メーカーの 16 機種では，ハードコードされたアカウントを用いたリモートログインが可能であることを仮想環境上で実証した．

続いて，RQ2 に答えるため，マニュアルに記載されていないアクセス機構が確認されたメーカーに対してアンケート調査を実施した．我々が準備した 11 項目の質問と追加の問い合わせを通じて，実装意図，技術的設計，改善予定等について調査した．その結果，連絡した 9 社中 7 社から回答を得たが，製品サポート終了や脆弱性管理ポリシー範囲外等を理由に，我々が用意したアンケートに完全に回答したメーカーはなかった．実装目的について具体的に回答した 3 社は遠隔保守目的と述べたが，ユーザーへの非開示理由については明確な説明が得られず，メーカー側の情報開示や説明責任に関して課題があることが明らかとなった．

本研究の貢献を以下に示す:

- IoT 機器のファームウェアの大規模解析およびユーザーマニュアルの調査を通じて，9 メーカーの 63 機種において，マニュアルに記載されていないアクセス機構の存在を明らかにした．
- メーカーへのアンケート調査を通じて，これらのアクセス機構が実装される背景にあるメーカーの意図と，メーカー側の説明責任の課題を明らかにした．

2. 背景および関連研究

2.1 メーカーが IoT 機器に埋め込むバックドア

メーカーによって IoT 機器に埋め込まれたバックドアは，重大なセキュリティリスクをもたらす．本研究では，「バックドア」を「メーカーによって意図的に実装されたアクセス機構」と定義する．Hashemi ら [8] は，IoT 機器のバックドアを体系的に 3 つの主要カテゴリーに分類した：ハードコードされた認証情報，文書化されていないインターフェース，意図しないネットワーク動作である．

ここで，機器がサポート終了 (EoS) に達した後の脆弱性対応が問題となる．IoT 機器の多くは EoS 後も長期間使用され続けるため，発見されたバックドアは修正されずに攻撃の侵入口として残存する [9]．Bakhshi ら [10] は，ファームウェアの脆弱性に関する包括的な調査から，メーカーが埋め込むバックドアを繰り返し発生する問題として指摘している．これらは個々の機器の侵害にとどまらず，ネットワーク全体への侵入経路となる可能性がある．

2.2 ユーザーマニュアルに記載のないアクセス機構に関するインシデントとメーカーの開示

我々の知る限り，IoT 機器におけるユーザーマニュアル

に記載のないアクセス機構の存在の背後にある意図を調査しようとした学術研究はない．そこで，セキュリティアドバイザリ，脆弱性レポート，関連する出版物などから，ユーザーマニュアルに記載のないアクセス機構の意図や目的が記述されている事例を収集し，分析した．

分析の結果，ユーザーマニュアルに記載のないアクセス機構の導入理由は主に 3 つであった．リモート管理の効率化 [11]，パスワード紛失時の緊急回復手段 [12]，開発段階のデバッグ機能の残存 [13] である．また，ユーザーマニュアルに記載されていないアクセス機構に対するメーカーの対応は，不適切なことがある．多くのメーカーは，独立したセキュリティ研究者の報告後にのみこれらの機能を認め，技術的な必要性の主張を行う傾向がある．さらに事例として，あるネットワーク機器では，Telnet 経由でログイン可能なアカウントが発見され，メーカーは診断機能として説明したが，パッチ適用後に再有効化と隠蔽の試みが判明したものも存在する [14]．このような事後的かつ防御的な対応は，脆弱性が公表されるまでの期間，ユーザーを不必要なリスクに晒し続ける．さらに，同様の問題の再発防止策や他製品での情報開示も不十分であり，これらは IoT 機器業界全体の課題である．

3. 手法

本研究では，以下に示す手順によって，ユーザーマニュアルに記載されていないアクセス機構が実装されているファームウェアを特定した．**3.1** ファームウェア収集，**3.2** ハードコードされたシステムユーザーの調査，**3.3** デフォルトで有効な Telnet/SSH サービスの調査，**3.4** ユーザーマニュアル調査，**3.5** Telnet/SSH 経由でのログインの調査，**3.6** 機器メーカーへのアンケート調査．

3.1 ファームウェア収集

先行研究が公開している IoT ファームウェアデータセット [15] から 120,669 件のファームウェアを収集した．また，追加でメーカーのウェブページから 53,099 件のファームウェアを収集した．合計で，202 社のメーカーから 173,768 件のファームウェアを収集した．複数のバージョンが利用可能な機種については，入手可能な全てのファームウェアバージョンを収集した．

3.2 ハードコードされたシステムユーザーの調査

本研究では，IoT 機器ファームウェアの約 86%で使用されている Linux を含む Unix 系 OS を対象とした [4]．ハードコードされたアカウントを調査するため，ファームウェアを unblob [16] を用いて展開し，ファイルを抽出した．さらに，展開したファームウェアの`/etc/passwd` および`/etc/shadow` を調査し，以下の条件を満たすアカウントが存在するファームウェアを特定した．

- `/etc/passwd` で，ログイン可能なシェルが割り当てられているアカウントを対象とした．
- `/etc/shadow` で，パスワードが設定されたログイン可能なアカウントを確認した．

3.3 デフォルトで有効な Telnet/SSH サービスの調査

本研究では，FirmAE [5] を使用して，ファームウェアを仮想環境上でエミュレートして実行した．エミュレーションが成功した場合，すべての TCP ポート (`-p-`) に対して Nmap サービスおよびバージョン検出スキャン (`-sV`) を実施し，Telnet または SSH がデフォルトで有効になっているファームウェアを特定した．一部の IoT 機器は ping 要求に応答しないため，Nmap によるスキャンがスキップされる．これを回避するため，`-Pn` オプションを使用してこのステップを無効にした．また，応答が極端に遅いホストを無視するため，`--host-timeout` オプションを用いてホストごとのタイムアウトを 300 分に設定した．

3.4 ユーザーマニュアル調査

機器に実装されている Telnet/SSH サービスやアカウントがユーザーマニュアルに記載されていない場合，ユーザーはリスクを認識できない．そこで，前節までの調査により特定された各機器について，メーカーの公式ウェブサイトから最新のユーザーマニュアルを取得した．次に，2 名の研究者が以下の基準に基づいて各ユーザーマニュアルを独立して調査した．判断が異なる場合は，内容を協議して合意した結果を用いた．

(1) Telnet または SSH の存在や使用方法の記載があるか．
(2) Telnet または SSH 経由で機器にアクセスできるアカウントの認証情報の記載があるか．

3.5 Telnet/SSH 経由でのログインの調査

特定されたアカウントによって機器にアクセスできるかどうかを検証するため，FirmAE によりファームウェアをエミュレートし，その仮想環境に対して接続を試みた．

その際，ファームウェア内にハードコードされているデフォルトパスワードが脆弱であるかどうかを評価した．具体的には，Linux システムのパスワードがハッシュ化された形で格納される`/etc/shadow` ファイルに対し，パスワード解析ツールである Hashcat [17] を使用して平文パスワードの復元を試みた．この際，侵入テストで利用される一般的なパスワード群である `RockYou.txt` を辞書として使用した．さらに，推測しやすいパスワードとして，ユーザー名と同一のパスワードについても検証を行った．Hashcat によりパスワードを特定できなかったファームウェアについては，正しいパスワードが判明していた場合にログインが可能かどうかを試行した．具体的には，展開されたファームウェアの`/etc/shadow` ファイルを編集し，対象アカウン

表 1　アンケート項目 (アンケート本文は英語)

#	質問内容
1	Telnet/SSH サービスに関する我々の調査結果を検証しましたか？
2	正しいまたは誤りであると検証された場合，検証プロセスを説明してください.
3	検証していない場合，検証を実施しなかった理由を説明してください.
4	これらの調査結果のセキュリティへの影響をどのように評価しますか？
5	セキュリティリスクではないと考える場合，その根拠を提供してください.
6	これらの調査結果に対処するためにどのような措置を取る予定ですか，またいつまでに実施しますか？
7	我々の通知前に Telnet/SSH サービスの存在を認識していましたか？もしそうであれば，いつからですか？
8	Telnet/SSH サービスの目的，対象ユーザー，およびユーザーマニュアルに記述されていない理由を説明してください.
9	Telnet/SSH サービスの実装元を明確にしてください.
10	誰によってこの機能は実装されましたか？
11	この問題が品質保証 (QA) プロセスで検出されなかった最も近い理由は何だと考えますか？また，将来的にこれらのプロセスを改善する予定はありますか？

トのパスワードハッシュを変更することで，ログインできるか試行した.

以上の試行によりログインできた場合，アカウントの動作と権限についても調査した.

3.6　機器メーカーへのアンケート調査

ファームウェア解析により特定された Telnet/SSH サービスとハードコードされたアカウントを持つ機器のメーカーに対し，アンケート調査を実施した．各メーカーの公式ウェブサイトから適切な連絡先を特定し，利用可能な場合はセキュリティ報告用の窓口を優先した．これらが利用できないか応答がない場合は，技術サポートまたはカスタマーサービスに連絡した．すべてのコミュニケーションは英語で実施し，信頼性確立のために所属機関を明示した.

アンケート調査では，研究目的を説明し，機器ごとの調査結果を要約した上で，**表 1** に示す 11 項目のアンケートへの回答をメーカーに依頼した．アンケートへの回答は任意であり，すべての回答は論文において匿名化されることをメーカーに保証した．また，メーカーが不完全な回答をした場合，不明な点について追加で問い合わせを行った.

アンケートの目的は，メーカーがこれらのサービスを意図的に実装したかを明らかにすることである．まず，我々の調査がファームウェアエミュレーションに基づくものであり，実機での検証ではないことから，事実確認の質問から開始した (質問 1〜3)．次に，我々の調査結果のセキュリティへの影響をメーカーがどう評価するか，またその後の対応措置についての質問を設けた (質問 4〜6)．さらに，Telnet/SSH サービスや文書化されていないアカウント実装の背景と経緯に関する質問を設けた (質問 7〜10)．最後に，なぜこの問題が開発・品質保証プロセスで発見されなかったのか，今後の改善計画について質問した (質問 11).

表 2　ファームウェア解析結果

指標	件数
ファームウェア総数	173,768
抽出されたファイル	約 1 億 7,100 万
`/etc/passwd` を含む	73,683
`/etc/shadow` を含む	65,061
ハードコードされたアカウントを含む	8,406
FirmAE によるエミュレーション成功	2,260
開放 TCP サービスあり	1,580
Telnet 有効	294
SSH 有効	232
Telnet または SSH 有効	481
重複除去後の固有機種数	165
マニュアルに Telnet/SSH サービスが記載	102
マニュアルに Telnet/SSH サービスが未記載	63
C1: Telnet/SSH サービスが未記載かつ ログイン可能なアカウントを確認	16
C2: Telnet/SSH サービスのみ未記載	47

4.　結果

4.1　ファームウェア解析

本節では，ファームウェアの解析結果を示す (**表 2**)．調査は，埋め込まれたアカウントを検出するための静的解析，Telnet および SSH サービスの特定とログイン可能性を評価するための動的解析，そしてこれらのアクセス機構がユーザーに開示されているかを調査するためのユーザーマニュアル調査から構成される．これらの結果は，マニュアルに記載されていないアクセス機構がどの程度実装されているかを示す．ただし，これらの結果はエミュレーション環境から得られたものである．エミュレーションと実機間の違い，および正常にエミュレートできなかった多数のファームウェアを考慮すると，実際の問題の範囲は本結果と異なる可能性がある．これらの差異については，5.5 節，5.4 節で議論する.

4.1.1　ハードコードされたアカウント

202 社の IoT メーカーから合計 173,768 件のファームウェアを展開した結果，合計で約 1 億 7100 万のファイルが抽出された．`/etc/passwd` および`/etc/shadow` ファイルは，それぞれ 73,683 件および 65,061 件のイメージから発見された．そのうち，少なくとも 1 つのログイン可能なアカウントを含むファームウェアは 8,406 件存在した．ここでログイン可能なアカウントとは，有効なシェル (`/bin/false` および`/sbin/nologin` を除く) を持ち，パスワードが無効でないハードコードされたアカウントを指す.

4.1.2　デフォルトで有効な Telnet/SSH サービス

FirmAE を使用して，ログイン可能なアカウントを持つ 8,406 件のファームウェアの動的解析を試みた．その結果，2,260 件 (約 26.9%) のファームウェアが TCP サービスを検査できる状態まで正常に起動した．これらのうち，1,580 件で少なくとも 1 つの TCP ポートが開放されている

ことが確認された．具体的には，294 件のファームウェアで Telnet が有効化され，232 件で SSH が有効化されていた．また，Telnet または SSH が有効化されていたファームウェアは 481 件であった．

4.1.3 ユーザーマニュアル調査とログイン可否

発見したアクセス機構およびアカウントがどの程度マニュアルに記載されているかを評価するため，まずファームウェアのバージョン違いによる重複を除外し，Telnet または SSH が起動する 165 件の最新のファームウェアを特定した．次に，これら 165 機種のユーザーマニュアルを手動で確認した．その結果，102 機種で Telnet/SSH サービスまたはアカウントに関する記述がユーザーマニュアルに存在した．これらの機種のアクセス機構はエンドユーザーに対して透明性があると判断し，以降の分析から除外した．

文書化が確認されなかった残りの 63 機種は，明示されないリモートアクセス機構を実装していると判断し，ログイン可否の調査やメーカーへの問い合わせを含む最終的な分析対象として選定した．

エミュレーション環境で Telnet/SSH 経由のログインを調査し，以下の 2 つのリスクタイプに分類した：

- **カテゴリ 1(C1)**：マニュアルに記載されていないアカウントを持ち，かつ Telnet または SSH 経由でログイン可能な機器．6 メーカーの 16 機種が該当した．
- **カテゴリ 2(C2)**：マニュアルに記載されていない Telnet/SSH サービスを持つ機器 (C1 を除く)．6 メーカーの 47 機種が該当した．

表 3 に，C1 に分類される 16 機種の詳細を示す．表に，機器ごとのメーカー (匿名化)，機器リリース年，アカウントパスワードの複雑性 (Hashcat などで特定可能かどうか)，サポート終了 (EoS) 状態，ログイン可能なアカウントの権限の情報を示す．C1 に分類される機器のうち 8 機種では，Hashcat やユーザー名と同一のパスワードで容易に復元された．また，9 機種でサポート終了していない状態であった．さらに，ログイン可能であることを確認したハードコードされたアカウント 16 個のうち，14 個がルート権限を付与されていた．

RQ1 への回答． ファームウェア解析により，収集した 173,768 件のファームウェアのうち 8,406 件に，ログイン可能なシェルを持つハードコードされたアカウントが存在することが示された．このうち 481 件でエミュレーション環境で Telnet または SSH サービスがデフォルトで起動し，ファームウェアのバージョン違いによる重複を除外すると，165 機種を特定した．さらにマニュアルを調査することにより，9 メーカーの 63 機種でマニュアルに記載されていないアクセス機構を実装している可能性が示された．具体的には，47 機種でマニュアルに記載されていない Telnet/SSH サービスが起動し，16 機種でハードコードされたアカウントでリモートアクセスできる可能性がある．

表 3 マニュアルに記載されていないアカウントで Telnet/SSH ログイン可能な C1 に分類される機器の詳細

メーカー (匿名化)	リリース年	脆弱なパスワード	EoS	ルート権限
A	2019	–	~	✓
B	2020	–	–	✓
B	2018	–	–	✓
B	2018	–	–	✓
B	2018	–	–	✓
B	2019	–	–	✓
B	2013	✓	✓	✓
B	2013	✓	✓	✓
E	2010	✓	✓	–
F	2017	–	✓	–
G	2012	✓	✓	✓
G	2011	✓	✓	✓
G	2012	✓	✓	✓
H	2014	–	~	✓
H	2013	✓[*1]	~	✓
H	2013	✓[*1]	~	✓

4.2 機器メーカーからの回答

ファームウェア解析で特定したユーザーマニュアルに記載されていないアカウントや Telnet および SSH サービスを実装した可能性のある 9 メーカーに対し，実装の意図と認識を理解するためのアンケート調査を実施した (**表 4**)．アンケート調査の結果，9 メーカーのうち 7 メーカーが何らかの回答を提供した (「調査中」などの暫定的な返信を含む) が，我々が用意したアンケートに完全に回答した企業はなかった．メーカーがアンケートへの回答を拒否した理由として，製品のサポート終了 (EoS) 状態や，公式の脆弱性管理ポリシーの範囲外であることが挙げられた．

その後，我々からの追加の問い合わせに回答したメーカーの大部分は，最終的に自社の機器に Telnet または SSH サービスが実装されていることを認めた．実装目的について回答した 3 社は，メーカーによる運用・保守サービスまたはリモート管理機能を目的とすると説明した．しかし，これらの機能をユーザーマニュアルに明記しなかったことについて十分な説明をしたメーカーはなかった．以下に，各メーカーの回答の概要を示す．

メーカー A は，報告した機種で SSH サービスがデフォルトで有効であり，アカウントがユーザーマニュアルに記載されていないことを認めた．これらの実装目的を機器故障時の運用・保守サポート用と説明し，アカウントは強力なパスワードポリシーで保護されているため理論的にブルートフォース攻撃は困難と主張した．加えて，報告した機種はメーカーによるサポートを終了しており，代替品として

表 4 アンケートに対するメーカーの回答概要

メーカー	R1	R2	R3	R4	R5	R6
A	✓	✗	✓	✓	✓	メーカーによる保守運用サービス用
B	✓	✗	✓	✗	–	リモート管理用
C	✓	✗	✓	✗	–	–
D	✓	✗	~[*1]	~[*1]	~[*1]	一般的な管理インタフェース
E	✓	✗	–	–	–	–
F	~[*2]	–	–	–	–	–
G	✓	–	–	–	–	–
H	✗	–	–	–	–	–
I	✗	–	–	–	–	–

列名 (R1〜R6) は，メーカーからの回答における主要なポイントを示す．アンケート項目番号との混同を避けるため「R」を使用．

R1: 回答受領 (何らかの形式で)
R2: 提供したアンケート票に回答
R3: Telnet/SSH 機能を実装
R4: Telnet/SSH がデフォルトで有効
R5: マニュアルに Telnet/SSH の記述なし
R6: Telnet/SSH の目的と想定ユーザー

✓: 確認済み ✗: 否定 ~: 部分的に確認または不明確 –: 言及なし
[*1] 一部の機器は ISP 管理下にあり，確認が制限される
[*2] セキュリティチームが調査中

これらの問題が対処された後継機種への移行を推奨すると説明した．当該後継機種では，SSH はデフォルトで無効になっており，LAN 側からのみアクセス可能で，これらの存在はユーザーマニュアルに明記されている．

メーカー B は，Telnet および SSH サービスはデフォルトで無効であると主張した．アカウントの実装については，「報告された製品は専門的なネットワーク機器であり，ユーザーが独自のパスワードを設定する」と主張した．これらの主張を検証するため，1 つの実機を購入して検証を行った．その結果，Telnet および SSH サービスがデフォルトで無効であり，WebUI の管理画面での操作により有効化できることを確認した．これは，エミュレーション環境と実機の間のギャップを示している．この問題については， 5.4 節でさらに議論する．その後，root アカウントがマニュアルに記載されていない理由と root アカウントのパスワードの開示を求めたところ，メーカー B は説明を変更し，「root アカウントはメーカーのトラブルシューティング専用であり，ユーザー向けではないためマニュアルに記載していない」と述べた．さらに，パスワードの開示を拒否した．

メーカー C は，公式ウェブサイトからダウンロード可能な最新ファームウェアバージョンにおいて Telnet がデフォルトで有効であることを否定し，報告した機器の大部分が現在サポート終了であることを強調した．その後の問い合わせに対し，メーカー C は報告した機器のうち 2 機種において Telnet/SSH が起動していないことを実験により確認し，その結果を提示した．これについても，エミュレーション環境と実機の間にギャップが存在することを示しており，5.4 節で議論する．

メーカー D は，SSH と Telnet を標準管理インタフェースとして実装していることを認めた．また，機器マニュアルにはプロトコルの一般的な説明のみで実装の説明が不十分であったことを認めた．報告した製品には特定 ISP 向けカスタマイズ製品が存在し，アクセス機構の実装・デフォルト構成・マニュアル内容はメーカーではなく ISP が決定・管理しており，同社は詳細を把握していないと述べた．

メーカー E は，報告した製品がサポート終了状態であることを指摘し，報告したセキュリティリスクへの対処や文書化されていないリモートアクセスサービスに関する情報提供を行わなかった．代わりに，ファイアウォールの使用・IDS/IPS システム展開・疑わしいログイン活動の監視などの緩和策の実施を我々に推奨した．

RQ2 への回答．アンケート調査を行った結果，9 メーカーのうち 7 メーカーから何らかの回答を得た．その結果，メーカーはリモート管理や保守・運用サポートなどの目的で，ユーザーマニュアルに記載せずに Telnet/SSH サービスとアカウントを IoT 機器に意図的に実装していることが明らかとなった．3 メーカーはアクセス機構の実装がメーカーによる運用・保守を目的としていることを認めたが，4 メーカーは製品のサポート終了などを理由にその存在を明確に説明せず，一貫性のない回答をした．また，全メーカーがアクセス機能がユーザーマニュアルに記載されていない理由を明確にしなかった．

5. 考察

5.1 推奨事項

本研究では，主に一般消費者向け IoT 機器 (エンドユーザーが使用者兼管理者となる機器) を対象としており，以下の推奨事項もこの範囲に限定される．

機器メーカーは，製品に含まれるすべてのネットワークサービスと認証情報をユーザーマニュアルに明記すべきである．また，アクセス機構の実装は最小限に抑え，必要時には安全な実装と明示的ユーザー同意を得る必要がある．規制機関および標準化団体は，一般消費者向けの IoT 機器製品に対してネットワークサービスと認証情報の開示を義務化するべきである．これにより，ユーザーが製品ライフサイクル全体でセキュリティ確保に必要な情報を確実に入手できるようになる．エンドユーザーは，透明性とセキュリティへの明確な取り組みを示すメーカーを選択し，可能な限り認証製品を採用すべきである．

5.2 サポート終了後のメーカーの責任

アンケート調査に対して回答が得られた 7 メーカーのうち，4 メーカーがサポート終了している機器について脆弱

性対応を拒否したが，Telnet/SSH サービスはユーザに開示されておらず，ユーザーは適切な対策を実施できない．深刻なセキュリティリスクについては，サポート終了後も情報開示と緩和策の提供がメーカーの社会的責任として残る．

5.3 文書化されないアクセス機能の潜在的リスク

本研究で明らかになったアクセス機構の問題は，調査対象の Telnet/SSH 以外にも広がる可能性がある．Web インターフェースや独自 API などにおいても，ユーザーマニュアルに記載されていない管理者アカウントやハードコードされた認証情報を含む可能性がある．

また，異なるメーカー 17 機種で同一のアカウントデータ (ユーザー名，パスワードハッシュ，ソルト，最終変更日) を確認した．これは，アクセス機能が SDK などのメーカー間で共有される上流コンポーネントに由来することを示唆しており，ソフトウェアサプライチェーン管理の重要性を示す．

5.4 制限事項

ファームウェア収集． 我々の手法では，ファームウェアがメーカーの Web サイトから取得されており，OTA 更新を通じて配信されるファームウェアは対象となっていない．しかし，202 メーカーから 173,768 個のファームウェアを含むデータセットを用いたことにより，解析結果は IoT 機器の全体的な傾向を捉えていると考えられる．

ファームウェアの静的解析． メーカー独自の形式で圧縮・暗号化されたファームウェアは展開とファイルシステムの再構築を阻害する可能性がある．この課題に対し，30 種類以上のアーカイブ・圧縮・ファイルシステム形式を再帰的に解析可能な unblob を利用することで，大部分のファームウェアの展開・解析が実現された．

ファームウェアの動的解析． 動的解析では，仮想環境内でファームウェアセキュリティリスクを評価するため FirmAE を採用した．FirmAE は，カーネル修正と仮想ネットワークインターフェース生成により，従来の CPU エミュレータ (Firmadyne [18] など) に比べてエミュレーション精度を大幅に改善している．しかし，エミュレートを試行したファームウェアの 73.1%は正常に実行できなかった．この失敗の原因は，未対応の CPU アーキテクチャや独自のハードウェア依存関係による互換性の問題であると考えられる．

5.5 エミュレーション環境と実機のギャップ

ファームウェアエミュレーション技術は，セキュリティリスク識別において広く採用され，一定の信頼性を確立している．しかし，エミュレーション環境と実際のハードウェア環境の違いにより，セキュリティ評価に影響を与える可能性がある [19], [20].

表 5 エミュレーションと実機検証結果の比較

メーカー	サービス種別	エミュレーション		実機	
		サービス	ログイン	サービス	ログイン
B	Telnet/SSH	✓	✓	✗	✗
F	Telnet	✓	✗	✓[*1]	✓[*1]
F	Telnet	✓	✗	✓[*1]	✓[*1]
F	Telnet	✓	✗	✗	✗
G	SSH	✓	✗	✓	✗
G	SSH	✓	✗	✓	✗

✓: サービス起動/ログイン成功　✗: サービス無効/ログイン失敗
[*1] ハッシュ化された認証情報を含むマジックパケットにより Telnet が有効化．認証データは`/usr/etc/default` にハードコード．

そこで，エミュレーション環境と実機環境の差異を評価するため，アンケート調査で回答が得られなかった Telnet または SSH サービスが稼働している機器などについて，実機検証を実施した．具体的には，アクセス機構がデフォルト設定で起動しているかを調査した． **表 5** は，3 製造者の 6 モデルについて，エミュレーション環境と実機環境での検証結果を比較したものである．検証の結果，エミュレーション環境と実機環境では動作に相違があることが確認された．Telnet および SSH サービスのデフォルト起動状況について，6 機器中 4 機器はエミュレーション環境と実機環境で同一の結果を示したが，2 機器では異なる結果が観察された．特に製造者 F の機器では，エミュレーション環境で認証に失敗した 2 機種が，実機では認証に成功した．

以上の結果から，エミュレーション環境で安全と判定された機器が実環境では脆弱性を持つ可能性があり，逆にエミュレーション環境で検出された問題が実機では再現されない場合もある．しかしながら，市場に存在する全ての機器を物理的に検証することは，コスト面および時間的制約から現実的ではない．したがって，エミュレーションベースの大規模スクリーニングは，セキュリティリスクの初期評価において依然として重要な役割を果たす．本研究で示された限界を認識した上で，エミュレーション解析を第一段階のフィルタリングとして活用し，高リスクと判定された機器に対して選択的に実機検証を行うことが，効率性と正確性のバランスを取った戦略であると考える．

5.6 バックドア判定における意図性の評価

ファームウェア解析とメーカー調査の結果，隠されたアクセス機構が意図的なバックドアか，開発過程の見落としによるセキュリティホールかを技術的証拠のみから判定することは極めて困難であった．ハードコードされたルート権限アカウントなど特定の実装パターンは意図的設計を強く示唆するものの，その実装目的については技術的証拠だけでは判別できない．実際，本調査で確認されたアカウント名の多くは汎用的な名称 (root，admin，guest など) であり，その使用目的の推測は困難であった．

一つの事実からバックドアと判定することは困難であるが，難読化による機能の隠蔽，隠された機能有効化の仕組み，メーカーのみが知るアクセス方法，情報開示の欠如という複数要因の組み合わせは，バックドアとしての解釈を合理的に支持すると考えられる．こうした疑いを避けるため，メーカーは安全な実装，ユーザーマニュアルでの明示的な文書化を徹底すべきである．

6. 研究倫理

Menlo Report [21] に従い，研究における潜在的利益を最大化し，起こりうる害を最小化するよう設計した．

ファームウェア収集． 収集したファームウェアはすべてメーカーが公式サイトで公開配布しているものである．本研究は，著作権法の範囲内で実施した．

責任ある開示． 脆弱性を特定した際は，詳細な脆弱性情報と再現手順を該当機器メーカーに迅速に直接開示した．また，IPA の脆弱性届出窓口にも調査結果を報告した．第三者による悪用や搾取を防ぐため，アンケートの送付・回答状況にかかわらず，本論文では影響を受けるメーカーと特定機種の識別情報を匿名化している．これにより，重要なセキュリティ問題の適切な伝達と，意図しないリスクからのメーカーの保護を両立している．

機器メーカーへのアンケート調査． ステークホルダー保護と透明性確保のため，以下の対策を実施した．第一に，風評被害や過度な社会的注目を防ぐため，すべてのメーカー名と製品識別子を匿名化した．本研究の知見は公開ファームウェアに基づき技術的に検証可能だが，匿名化により個々の企業を不当に標的にすることなく，より広範な改善に貢献できる．第二に，メーカーの参加は完全に任意とした．回答は任意であることを明確に伝え，企業の自主性を尊重した．回答とその後のやり取りの内容は匿名化した上で論文において公開する可能性があることを，メーカー側に事前に伝えた．第三に，懸念を示した際は，投稿前に原稿の関連部分を共有できることを通知した．この事前確認により，メーカーは技術的な点を明確にし，文脈を提供し，我々の解釈を確認できた．ただし，事前確認を要求したメーカーはなかった．

7. 結論

本研究では，173,768 件の IoT 機器のファームウェアを解析し，9 社のメーカーにわたる 63 機種でユーザーマニュアルに記載されていない Telnet/SSH サービスまたはログイン可能なアカウントを特定した．メーカーへのアンケート調査により，ユーザーマニュアルに記載されていない機能の存在とリスクを明らかにし，機器の開発および文書化において説明責任の強化が必要であることを示した．

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] JVNVU#94757027 複数の PTZ カメラにおける複数の脆弱性. https://jvn.jp/vu/JVNVU94757027/.
[2] Cve-2024-57040 detail - nvd. https://nvd.nist.gov/vuln/detail/CVE-2024-57040.
[3] Cve-2024-45697 detail - nvd. https://nvd.nist.gov/vuln/detail/cve-2024-45697.
[4] Andrei Costin et al. A large-scale analysis of the security of embedded firmwares. In *USENIX Security Symposium*, 2014.
[5] Mingeun Kim et al. Firmae: Towards large-scale emulation of iot firmware for dynamic analysis. ACSAC, 2020.
[6] Jacob Wurm et al. Security analysis on consumer and industrial iot devices. In *2016 21st Asia and South Pacific Design Automation Conference*, 2016.
[7] Rolf H. Weber et al. Cybersecurity in the internet of things: Legal aspects. *Computer Law & Security Review*, 32(5):715–728, 2016.
[8] Soheil Hashemi et al. Internet of things backdoors: Resource management issues, security challenges, and detection methods. *Transactions on Emerging Telecommunications Technologies*, 32(2):e4142, 2021.
[9] Dingding Wang et al. An empirical study on the insecurity of end-of-life (eol) iot devices. *IEEE Transactions on Dependable and Secure Computing*, 21(4):3501–3514, 2024.
[10] Taimur Bakhshi et al. A review of iot firmware vulnerabilities and auditing techniques. *Sensors*, 24(2):708, 2024.
[11] Zyxel security advisory for hardcoded credential vulnerability (cve-2020-29583). https://securityaffairs.com/112877/iot/secret-backdoor-zyxel-devices.html, 2020.
[12] Clarke tags new ruggedcom vuln: Hard-coded rsa key provides new backdoor. https://www.theregister.com/2012/08/22/rugged_com_new_backdoor, 2012.
[13] Cisco removes backdoor account from ios xe software. https://www.bleepingcomputer.com/news/security/cisco-removes-backdoor-account-from-ios-xe-software/, 2018.
[14] Vodafone, huawei dispute report of telnet ‘backdoor’. https://www.bankinfosecurity.com/vodafone-huawei-dispute-report-telnet-backdoor-a-12435, 2019.
[15] Yuhao Wu and other. Your firmware has arrived: A study of firmware update vulnerabilities. In *USENIX Security Symposium*, 2024.
[16] unblob. https://github.com/onekey-sec/unblob.
[17] hashcat. https://hashcat.net/hashcat/.
[18] Firmadyne: Platform for emulation and dynamic analysis of linux-based firmware. https://github.com/firmadyne/firmadyne.
[19] W. Zhou et al. Automatic firmware emulation through invalidity-guided knowledge inference. In *USENIX Security Symposium*, 2021.
[20] Christopher Wright et al. Challenges in firmware rehosting, emulation, and analysis. *ACM Comput. Surv.*, 54(1), 2021.
[21] The menlo report: Ethical principles guiding information and communication technology research, 2012.