スマートホーム向け規格Matterの競合についてのセキュリティ問題

須田 光[1,a)]　須崎 有康[1,b)]

概要：本研究は、スマートホーム向け規格「Matter」におけるセキュリティと制御の整合性に関する課題を明らかにすることを目的とする。Matter では、複数の Commissioner によるデバイス管理が可能とされ、柔軟なスマートホーム構築が期待されている。しかし、実機による動作検証の結果、仕様上の曖昧さが複数の問題を引き起こすことが確認された。検証では、他の Commissioner が登録した公開鍵を含む Fabric や NOC の情報を第三者が取得・削除可能であることが判明し、権限管理やプライバシー保護の観点で問題があることがわかった。また、コミッショニングが失敗してもデバイス上に NOC が残存し、上限に達することで新たな Commissioner の追加が不可となるケースが確認された。これはユーザから見えない内部状態が障害の原因となる点で、操作と状態の不一致を引き起こす可能性がある。これらの結果は、Matter における Commissioner 間の責任分離や制御権限の可視性が不十分であり、現行仕様ではセキュリティおよびユーザビリティに課題があることを示している。本研究は、スマートホーム環境におけるセキュアな多元制御のあり方を再考するための実証的知見を提供するものである。

キーワード：Matter

Security Issues Arising from Controller Conflicts in the Matter Smart Home Standard

Hikari Suda[1,a)]　Kuniyasu Suzaki[1,b)]

Abstract: This study aims to clarify issues related to security and control consistency in the Matter standard, a protocol designed for smart home environments. Matter allows multiple Commissioners to manage a single device, enabling flexible smart home configurations. However, through practical testing with actual devices, we identified several problems stemming from ambiguities in the specification. Using the command-line tool chip-tool, we confirmed that a third party can retrieve and delete Fabric and NOC information—including public keys—registered by other Commissioners, raising concerns about access control and privacy protection. Additionally, even when commissioning fails, the NOC remains stored on the device, and once the NOC limit is reached, new Commissioners cannot be added. This creates a situation where internal device states invisible to the user can become the root cause of failure, potentially leading to inconsistencies between user actions and device states. These findings suggest that the current Matter specification lacks sufficient mechanisms for isolating responsibilities among Commissioners and for ensuring visibility and traceability of control authority. This study provides empirical insights that contribute to rethinking secure multi-party control architectures in smart home environments.

Keywords: Matter

[1] 情報セキュリティ大学院大学
Graduate School of Information Security, Institute of Information Security
[a)] mgs241101@iisec.ac.jp
[b)] suzaki@iisec.ac.jp

1. はじめに

世界の IoT デバイスの数は 2023 年には 378 億台に及び、2026 年には 500 億台にのぼると予測されている [1]。

IoT 市場の中で特に高成長が期待されている市場のひとつとして、スマート家電や IoT 化された電子機器などを含む家庭用 IoT デバイスが挙げられており、総務省の令和 6 年版情報通信白書によると、世界の IoT デバイスのうち、2023 年に 124.2 億台だった消費者向け IoT デバイスは 2026 年には 184.1 億台にまで増加すると予測されている。

一方で、家庭でこうした多様なモノをインターネットに繋いで運用する際には、相互運用性についての課題が指摘されている [2]。

現在、各メーカーは異なる通信プロトコルを使用しているため、デバイス同士が同じネットワーク上でスムーズに連携することが困難である問題が存在する。また、デバイスの互換性が不十分であるため、異なるブランドやプラットフォームのデバイス間での相互作用が難しく、ユーザーにとって使い勝手の悪い環境が生じているという問題も存在する。

このような相互運用性に関する課題を解決するために注目されているのが、Matter [3] [4] という新しい通信規格である。Matter は、異なるメーカーやデバイスがシームレスに連携できるよう設計されており、IoT デバイスの相互運用性を向上させることが期待されている。

Matter は、2022 年に CSA（Connectivity Standards Alliance）がリリースした、スマートホームデバイス向けの通信規格である。CSA には、Apple、Google、Amazon、Samsung など、スマートホーム業界の主要企業が連携して推進しており、2025 年現在では 280 社以上が加盟している [5]。

Matter の最大の特徴は、オープンソースかつロイヤリティフリーな標準規格である点にある [6]。これにより、異なるメーカーが開発したデバイスでも、共通の仕様に基づいて相互に接続・制御可能となる。ユーザは、複数のアプリを切り替える必要がなく、単一のプラットフォームから一括管理できる環境が実現される。

本稿では Matter のセキュリティ問題について述べるとともに、複数の制御主体が同一デバイスに対して操作を試みた際に生じうる制御競合やアクセス可視性の欠如といった問題に注目し、今後の設計改善に向けた検討の方向性について報告する。

本稿の貢献は以下のとおりである．

- 既存研究で指摘された Matter の課題を整理するとともに，実機検証を通じて，仕様に準拠していても実運用においてセキュリティリスクとなり得る挙動を明らかにした．
- 制御主体による操作がユーザの認識外でデバイス内部状態に影響し，NOC の保存や上限到達といった不整合を引き起こすことを観測し，その具体的事例を示した．
- 得られた知見に基づき，アクセス制御強化，内部状態管理の厳格化，および UI レベルでの状態可視化の必要性を指摘し，仕様と実装の両面からの改善に資する設計指針を提供した．

2. Matter について

Matter は、スマートホーム分野における相互運用性とセキュリティの確保を目的として開発されたアプリケーション層の通信プロトコルである。その通信基盤は IPv6 を前提に設計されており、ネットワーク層および物理層としては、Thread、Wi-Fi、Ethernet がサポートされている。特に Thread は、IEEE 802.15.4 を基盤としたメッシュ型の低消費電力ネットワークであり、スマートホーム機器における常時接続性と電力効率の両立に適している [7]。

Matter ではこのように複数の物理層に対応しつつも、すべての通信はアプリケーション層で抽象化されるため、デバイスの通信方式の違いを意識せずに連携が可能となっている。

Matter の通信・制御における論理的な枠組みとして重要なのが、Fabric と呼ばれる概念である。Fabric は、共通の信頼ルートを持つ Commissioner（制御主体）とその配下のデバイス群からなる論理的なネットワークドメインである。同一の Fabric 内では、各ノードが Fabric ID と Node ID により一意に識別され、Operational Certificate によって相互の認証が可能となっている。1 つのデバイスは複数の Fabric に同時に所属でき、たとえば家庭用と来客用の制御系を分離するといった柔軟な運用が可能となる（図 1）。Fabric はアクセス制御の範囲指定といったセキュリティ機構にも密接に関係しており、Matter におけるセキュリティとプライバシーの中核を成している。

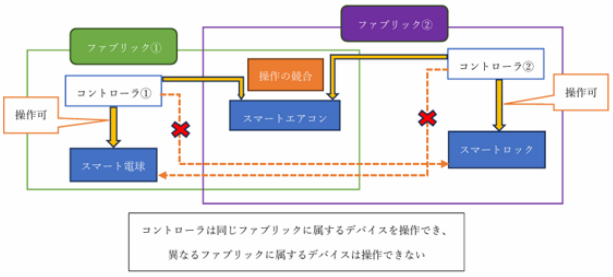

図 1 Matter のファブリックごとのデバイスの制御関係

Commissioning は、Matter デバイスを新たな Fabric に参加させるための一連のプロセスである。デバイスは Bluetooth などを通じて自身の情報をアナウンスし、Commissioner はこれを受けて Commissioning を開始する。まず最初に、デバイスと Commissioner 間でセキュアなチャネルが確立されると、デバイスは自己の正当性を証明するために Device Attestation Certificate（DAC）を提示する。Commissioner はこの DAC をもとに、信頼チェーンの上位に位置する Product Attestation Intermediate（PAI）および Product Attestation Authority（PAA）を参照し、デバイスが CSA の認定製造者によって発行されたものであるかどうかを検証する（図 2）。

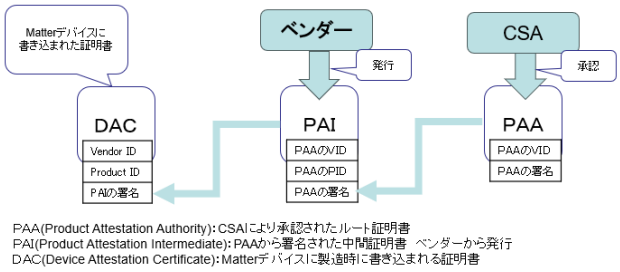

図 2　デバイスの真正性を確認するための証明書の検証

この Attestation フェーズを通過した後、Commissioner は新たな Fabric における Node Operational Certificate（NOC）を生成し、デバイスに発行する。NOC には Node ID や Fabric ID などの識別情報が含まれ、以降の通信における認証および暗号化の基盤となる（図 3）。さらに、Commissioner は Thread や Wi-Fi のネットワーク資格情報をデバイスに渡し、これによりデバイスは Fabric に参加し、同一ドメイン内の他ノードと安全に通信できる状態となる。すべての通信は AES-CCM により暗号化され、OperationalCredentials Cluster を通じて証明書や鍵の発行・管理が行われる。

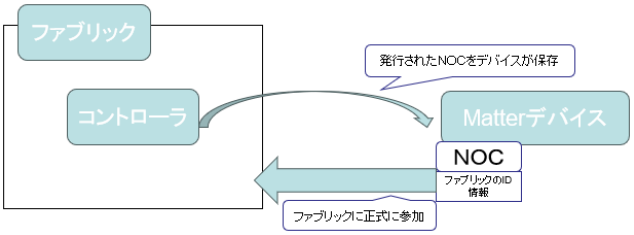

図 3　NOC の発行とデバイスによる NOC 保存

Matter では、これらの通信および操作をアプリケーション層で標準化するために、Cluster と呼ばれるデータモデルを導入している。Cluster は、デバイスの機能を構造化された単位として定義するものであり、属性（Attributes）、コマンド（Commands）、イベント（Events）から構成される。たとえば、On/Off Cluster では、スイッチの状態を保持する属性と、オン・オフを切り替えるためのコマンドが規定されている。

各デバイスは複数の Endpoint を持ち、それぞれに複数の Cluster が割り当てられることで、複数機能の一体的な構成が可能となる。これらの Cluster 定義は CSA において規定されている。このような標準化されたモデルにより、異なるベンダが開発した Matter 準拠デバイスであっても、相互に理解可能なデータ構造と操作体系を共有することができる。

以上のように、Matter は物理層の違いを吸収した IP ベースの通信構造を土台とし、Fabric による信頼ドメインの確立、Commissioning によるセキュアな導入プロセス、証明書による認証構造、そして Cluster による機能のモデル化という多層的な設計を通じて、高い相互運用性とセキュリティを実現している。

3. Matter のセキュリティ問題についての先行研究

Matter はスマートホームにおける相互運用性の向上を実現する一方で、ユーザーが安全かつ適切に制御を行うためのインタフェース設計やアクセス管理などに関するセキュリティ課題が指摘されている。本節では、Matter におけるセキュリティ上の問題について、2 つの先行研究を通じて紹介する。

3.1 Matter のユーザー向け制御機能における設計上の脆弱性

Wang らによる論文 Hidden and Lost Control on Security Design Risks in IoT User-Facing Matter Controller [8] は、Matter プロトコルにおけるユーザー操作インタフェース（UMCCI：User-facing Matter Control Capabilities and Interfaces）に潜在する設計上の脆弱性を体系的に分析し、“UMCCI Flaws”と呼ばれる欠陥の類型を定義・整理している。

Matter は、1 つのデバイスに対して複数の Commissioner（デバイスを制御・管理する Matter コントローラ）を同時に接続可能とするマルチアドミン構成を標準仕様として採用しており、スマートホーム環境における柔軟な制御を可能にしている。また、Commissioner とデバイスとの間には Fabric（信頼されたデバイスと Commissioner で構成される論理的なセキュリティドメイン）が構築される。Fabric は、共通のルート証明書によって認証されることで、構成メンバー同士のセキュアな通信と相互制御を実現する。これにより、異なるアプリやデバイス間でも、安全に制御情報を共有できるよう設計されている。

一方で、その設計上、ユーザーがどの Commissioner や Fabric が現在自身のデバイスに接続されているかを正確

に把握し、制御権を適切に管理するためのユーザーインタフェース（UI）設計が、各ベンダの裁量に委ねられているという実態がある。著者らは、この状況がユーザーの制御認知・アクセス管理能力を損なうリスクを孕んでいることを実証的に明らかにしている。

研究では、Apple、Google、Samsung、Tuya など 8 社が提供する計 11 種類の Matter 対応デバイスおよびそれに対応するスマートフォンアプリを対象に、UMCCI が提供する制御の可視性、アクセス制御情報（ACL）の表示・管理機能について評価を実施。その結果、以下のような重大な欠陥が確認された。

- 複数のアプリにおいて、Matter Controller（Commissioner）の一覧表示が不完全である
- Fabric 内の ACL 情報が UI 上で表示されない、または不正確であるユーザーが既に削除したと信じていた Commissioner が、実際には制御権を保持し続けている

特に Apple Home や Tuya Smart においては、接続済みの他の Commissioner や Fabric が UI 上で明示的に表示されない、あるいは偽装された Vendor ID や Label によってユーザーが誤認するといった挙動が観察された。

これらの問題の発見と実証には、LLM（大規模言語モデル）を活用した UI 探索技術を備えた自動検証ツール「UMCCI Checker」が用いられた。同ツールは、ベンダアプリの GUI を自動的に探索・解析し、UMCCI Flaws を検出する機能を備える。検証の結果、以下のような攻撃が可能であることが確認された。

- Label や Vendor ID を偽装し、正規の Commissioner であるかのように見せかける
- UI 上に表示されない隠れた Fabric への継続的アクセスを維持する
- ACL を書き換え、所有者の操作権限を意図的に低下させる

これにより、ユーザーが自身のデバイスに対する制御状態を正確に把握できず、セキュリティ上の深刻な盲点が生じうることが明らかになった。さらに本研究では、UMCCI Flaws の根本原因を以下の 2 つのカテゴリに整理している。

- ベンダ実装側の設計不備：例として、接続済み Commissioner の表示ロジックの欠陥、ACL の状態表示の欠如など
- Matter 標準仕様側の設計不足：たとえば、Vendor ID や Label が任意に設定可能であり、それらの表示値の真正性を検証する仕組みが Matter 仕様に含まれていない

これらの観点から、著者らは CSA および各ベンダに対し、UMCCI 設計に関するガイドラインの整備と、Matter 仕様における UI レベルのセキュリティ要件の明確化と強化を提案している。以上より、本論文は、Matter の通信路や暗号機構そのものには直接的な脆弱性が存在しないことを前提としつつも、ユーザーインタフェース層における情報の可視性と真正性の欠如が、実運用上の重大なセキュリティ問題につながることを体系的に示したものであり、ユーザー中心の IoT セキュリティ設計における新たな課題を提起している。

3.2 制御主体のセキュリティリスク

Shashwat らによる論文 Security Analysis of Trust on the Controller in the Matter Protocol Specification [9] は、Matter プロトコルにおける制御主体の信頼モデルに着目し、Commissioning においてデバイスの制御を行う側の認証が Matter 仕様上要求されていないことが重大なセキュリティリスクとなることを体系的に分析した研究である。Matter では、Commissioning の過程においてデバイス側が Device Attestation Certificate（DAC）を提示し、Connectivity Standards Alliance（CSA）が管理する分散コンプライアンス台帳（Distributed Compliance Ledger: DCL）に登録された証明書チェーン（PAA → PAI → DAC）を通じて、その正当性が検証される。

- PAA（Product Attestation Authority）：CSA が認定するルート認証局。信頼の起点。
- PAI（Product Attestation Intermediate）：メーカーに割り当てられる中間認証局。
- DAC（Device Attestation Certificate）：個々のデバイスに格納される証明書で、PAI によって署名される。

一方、制御主体についてはこれに対応する認証の仕組みがプロトコル上まったく存在しない。そのため、任意のアプリケーションが Controller 機能を実装し、自由に Commissioning を実行できる構造となっている。

著者らはこの構造的な非対称性に注目し、Matter 公式の chip-tool を用いて独自に制御主体を実装した。そして市販の Matter 対応スマートプラグに対して、正規の制御主体アプリ（Google Home）と自作制御主体の双方から Commissioning を実施し、その制御挙動を比較した。その結果、正規・非正規を問わずデバイスは同様に応答・制御可能であり、制御主体の正当性を保証する手段が存在しないことが実証された。

さらに本論文では、同一デバイスが複数の Matter Fabric に所属し、異なる制御主体から同時に制御される状況において、Fabric 間で設定された Automation ルールが交差的に干渉するリスクについても指摘している。たとえば、Fabric A において「照明 ON 時に空気清浄機を起動する」という Automation が設定されている場合に、Fabric B の制御主体が照明を ON にすることで、Fabric A 側の Automation が意図せず作動する可能性がある。このように、Matter のマルチアドミン機能が予期せぬかたちで相互に影響し合い、ユーザーの意図しない動作が発生する恐れ

が示されている。

これらの設計的リスクに対し、著者らは以下のような具体的な対策を提案している。

- デバイス側が制御主体の DAC を要求・検証する仕組みをプロトコルに導入する（双方向認証の導入）。
- アプリマーケット等で制御主体アプリの開発者に対して CSA が信頼性認証を付与し、ユーザーに可視化する仕組みを設ける。

特に、信頼できない制御主体がユーザーの認知外で Commissioning を実行できる状況を放置すれば、制御の乗っ取りや Automation ルールの悪用による二次被害に発展しかねないと強く警鐘を鳴らしている。

本研究は、Matter 仕様がデバイス側には厳格な証明書ベースの認証を要求する一方で、Controller 側を無条件に信頼するという根本的な非対称性を明確にし、プロトコル設計者や実装者に対して、設計見直しの必要性を迫る極めて重要な知見を提供している。Matter の普及に伴い、制御主体側の認証不在はセキュリティ上の重大な盲点となりうることを示している。

4. 検証した Matter のセキュリティ問題

本研究では、スマートホーム向け規格「Matter」における複数 Commissioner 間の競合が、セキュリティおよび制御の一貫性に与える影響を明らかにすることを目的とし、実機を用いた動作検証を行った。

なお、本研究は特定メーカー・製品の評価を目的としないため、メーカー名および製品名は伏せ、仕様・挙動に基づいて記述する。

実験には、Matter 対応スマート電球 A（Fabric 上限 7）および Matter 対応スマート電球 B（Fabric 上限 5）を使用した。

4.1 他 Commissioner による Fabric 削除

本検証では、A、B どちらの電球についても、第三者の Commissioner が登録した Fabric に対して、その Fabric および関連する NOC（Node Operational Certificate）情報を削除可能であることを確認した。この操作は、Matter 1.4 仕様書における定義（Core Specification 11.18.6.12）[10] に適合しており、削除対象 Fabric に関連する全ての Fabric-Scoped データが不可逆的に削除された。

しかし、仕様では「管理者の管理下にない既存 Fabric を削除する場合は、明示的なユーザー同意を得なければならない」と規定されているにもかかわらず、本検証環境では当該同意取得プロセスが実装上省略されていた。この結果、ACL（Access Control List）が適切に構成されていない場合、異なる管理主体間での Fabric 削除が可能となり、サービス拒否攻撃（DoS）や意図しない制御権限剥奪のリスクが存在する。

この挙動は仕様に準拠しているものの、実装上のアクセス制御ポリシーに依存して安全性が大きく変動するため、運用環境における管理者権限の厳格化および削除操作時のユーザー通知が不可欠である。

4.2 他 Commissioner による Fabric 情報の取得

検証により、A、B どちらの電球についても、Fabrics 属性を読み出すことで、第三者の Commissioner が登録した Fabric の RootPublicKey、VendorID、FabricID、NodeID および Label が取得可能であることが確認された。この属性は Matter 仕様書において FabricDescriptorStruct 型（Core Specification 11.18.4.5）[10] として定義されている。

仕様上、この情報公開は「Fabric 間の管理主体に対する透明性」を目的としており、VendorID 等は AddNOC コマンドで指定された値に基づく。しかし、RootPublicKey は運用証明書チェーンのルート公開鍵と一致するため、異なる管理主体が混在する環境では鍵情報の広範な露出につながる。

本検証の結果は仕様に準拠しているが、実運用においては Fabric 間の鍵情報共有が意図せず生じる可能性があり、アクセス制御リスト（ACL）またはアクセス制限リスト（ARL）による参照主体の制限、並びに UI 上での可視化・注意喚起が望まれる。

4.3 Commissioning 失敗時における NOC 残存と上限到達

実験では、正規の制御主体となるアプリを用いて Commissioner を追加する際、1 回の操作で NOC が 2 件保存するケースが複数回発生した。その結果、ユーザの認識として一つの Commissioner を追加した場合でも、電球 A および電球 B で上限に到達し、新規 Commissioner の追加が不可能となるケースがあった。

また、メーカー独自の制御主体となるアプリで Commissioning が失敗した場合に、アプリ上ではデバイスの追加に失敗しているものの、デバイス中では NOC が保存されているという挙動が観測された。

本検証結果は、ユーザーインタフェース上で原因が明示されないため、利用者が原因不明のまま追加失敗を繰り返す状況を引き起こす可能性がある。したがって、NOC テーブル管理と Fail-Safe 動作の実装検証、並びに UI における上限到達警告の表示が不可欠である。

4.4 総括

これらの結果は、Matter の多元制御環境における責任分離の不十分さと制御権限の可視性不足を示している。特に、(1) 権限を持たない主体による Fabric 削除、(2) 他主体の鍵情報取得、(3) 失敗時の状態ロールバック不備は、

セキュリティと運用性の双方に重大な影響を及ぼす可能性がある。本研究は、仕様上許容されている動作であっても実運用環境でのリスクが高まる事例を示しており、今後のMatter 仕様改訂やベンダー実装において、アクセス制御強化、状態管理の厳格化、UI 上での状態可視化が不可欠であることを提言する。

5. 考察

本研究では、Matter の多元制御環境において複数 Commissioner が同一デバイスを操作する際に発生するセキュリティおよび整合性上の問題を実機検証により明らかにした。以下では、各検証結果に基づいて考察を行う。

5.1 Fabric 削除のリスク

他 Commissioner による Fabric 削除は仕様上許容されている動作であるものの、実装においてユーザー同意の取得が省略されていた。

本来「管理下にない Fabric を削除する場合にはユーザー承認が必要」と規定されているが、実際にはこれが機能せず、他主体による権限剥奪が可能となった。

これは 仕様と実装の乖離によって利用者が意図しない制御不能状態に陥る危険を示しており、アクセス制御の厳格化や UI 上での明示的な承認要求が不可欠である。

5.2 Fabric 情報の取得と公開鍵の露出

Fabrics 属性の取得を通じて、第三者の Commissioner が登録した RootPublicKey や FabricID を閲覧できることが確認された。

仕様上は「管理主体間の透明性」を目的としているが、実運用では鍵情報の過剰な露出につながる。

透明性と秘匿性のバランスを欠いた設計であり、今後は ACL や UI 警告を通じて利用者にリスクを可視化すべきである。

5.3 NOC 残存と上限到達

一部の正規アプリで Commissioning を行った際、一度のコミッショニング操作で NOC が複数保存される場合があった。また Commissioning 失敗時に NOC が残存し、上限到達によって新規追加が不可能となる挙動が観測された。

これらはユーザー UI 上でも原因が提示されない場合があり、結果として、利用者は「なぜ Commissioner が追加できないのか」を理解できず、操作と内部状態の不一致に直面する。

ここから、UI 設計と内部状態管理の連携不足がユーザビリティ上の大きな課題であることがわかる。

5.4 本研究の限界と今後の課題

本研究はスマート電球 2 種類を対象とした実験に基づくため、他カテゴリのデバイス（ロック、センサー、家電等）で同様の挙動が再現されるかは未検証である。

また、NOC テーブルの内部管理や Fail-Safe 実装の詳細はブラックボックス性が高く、完全な挙動把握には限界がある。

今後はより多様なデバイスを対象に、ACL 設定や UI 挙動を含めた横断的検証を行う必要がある。

6. まとめ

本研究では、スマートホーム規格 Matter における複数 Commissioner の競合が引き起こすセキュリティおよび整合性の問題について、実機検証を通じて以下の知見を得た。

- 他 Commissioner による Fabric 削除：ユーザー同意を経ずに異なる管理主体の Fabric を削除可能であり、権限剥奪リスクが存在することを確認した。
- Fabric 情報の過剰公開：RootPublicKey を含む情報が仕様に従って公開される結果、鍵情報の露出がセキュリティ上の懸念を生むことを示した。
- NOC 残存と上限到達問題：Commissioning 失敗時にも NOC が残存し、上限により新規追加不能となる n など、ユーザの認識の外で NOC が保存されている事象を観測した。これはユーザビリティ上で混乱をまねくことを示した。

これらの結果は、Matter 仕様が Commissioner 間の責任分離や制御権限の可視性において不十分であることを実証的に示している。

今後の展望としては、(i) アクセス制御の厳格化、(ii) NOC 管理および Fail-Safe 実装の強化、(iii) UI レベルでの状態可視化や警告機能の標準化が必要である。

これらの改善は、スマートホーム環境におけるセキュアでユーザーフレンドリーな多元制御の実現に寄与すると期待される。

参考文献

[1] 総務省. 令和６年版情報通信白書データ集.

[2] Sami S. Albouq, Adnan Ahmed Abi Sen, Nabil Almashf, Mohammad Yamin, Abdullah Alshanqiti, and Nour Mahmoud Bahbouh. A survey of interoperability challenges and solutions for dealing with them in iot environment. *IEEE Access*, Vol. 10, pp. 36416–36428, 2022.

[3] Connectivity Standards Alliance. *Matter Specification*. Version 1.0 edition, 2022.

[4] Dimitri Belli, Paolo Barsocchi, and Filippo Palumbo. Connectivity standards alliance matter: State of the art and opportunities. *Internet of Things*, Vol. 25, p. 101005, 2024.

[5] Connectivity Standards Alliance. The power of membership.

[6] Wondimu Zegeye, Ahamed Jemal, and Kevin Kornegay.

Connected smart home over matter protocol. In *2023 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–7, 2023.

[7] Van Cu Pham, Toan Nguyen-Mau, Marios Sioutis, and Yasuo Tan. Matter and echonet lite: Similarities, differences, and a bridge solution for interoperability. *Internet of Things*, Vol. 27, p. 101265, 2024.

[8] Haoqiang Wang, Yiwei Fang, Yichen Liu, Ze Jin, Emma Delph, Xiaojiang Du, Qixu Liu, and Luyi Xing. Hidden and lost control: on security design risks in iot user-facing matter controller. In *Network and Distributed System Security (NDSS) 2025*, 2025.

[9] Kumar Shashwat, Francis Hahn, Xinming Ou, and Anoop Singhal. Security analysis of trust on the controller in the matter protocol specification. In *2023 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–6, 2023.

[10] Connectivity Standards Alliance (CSA). Matter core specificataion 1.4. `https://csa-iot.org/wp-content/uploads/2024/11/24-27349-006_Matter-1.4-Core-Specification.pdf`, 2024. [Accessed 25-07-2025].