2025 年度　卒業論文

DID に基づいた IoT データ管理システムの構築と評価

2026 年 2 月 10 日

システム工学部システム工学科
(学生番号: 60276128)

竹内 結哉

和歌山大学システム工学部

1 はじめに

2 背景技術

2.1 分散型識別子 (Decentralized Identifier:DID)

従来のインターネットにおける識別子 (例：メールアドレスや SNS アカウント) は, 特定の企業や組織が発行・管理する中央集権的な仕組みに依存している. このため, アカウント停止やセキュリティ侵害のリスク, さらにはユーザーが自らのアイデンティティを完全に管理できないという課題が存在する.

分散型識別子 (以下 DID) は, この問題を解決するために W3C により標準化が進められている新しい識別子である. DID は「did:example:xxxx」のような形式を持ち, ブロックチェーンなどの分散型台帳に基づいて管理される. 各 DID には対応する DID Document が存在し, 公開鍵や認証手段, サービスエンドポイントなどを含むことで, 所有者の真正性を保証する.

本研究においては,DID を用いることで IoT データ所有者の識別と認証を分散的に行い, ユーザー自身が自己主権的にデータを管理できる仕組みを実現する. これにより, なりすましの防止やデータ所有権の正当性証明が可能となる.

2.2 分散型ファイルシステム (InterPlanetary File System:IPFS)

IoT 機器から生成されるデータは膨大かつ多様であり, 従来の中央集権型サーバに保存する方式では, スケーラビリティの限界, 単一障害点, セキュリティリスクなどの問題が生じる. 特に, 中央サーバーにデータが集中すると攻撃対象となりやすく, 情報漏洩時の被害も大きくなる.

惑星間ファイルシステム (以下 IPFS) はこれらの課題を解決するために提案された分散型のファイルシステムである. IPFS はコンテンツアドレス方式を採用しており, ファイルはその内容に基づくハッシュ値で一意に識別される. このため, データが改ざんされれば異なるハッシュ値となり, 完全性の検証が容易である. また, ピアツーピアネットワークを介して効率的にデータを配信できるため, 冗長性・可用性に優れ, 単一障害点を排除できる.

本研究では,IPFS を利用して IoT データを分散的に保存し, そのハッシュ値のみをブロックチェーンに記録する方式を採用する. これにより, ブロックチェーンにデータ本体を保存する必要がなくなり, 処理負荷を軽減しつつデータの信頼性を保証できる.

2.3 DID と IPFS の統合による効果

DID と IPFS を組み合わせることで, データ管理における 2 つの要件, すなわち「所有者の正当性」と「データの改ざん防止」を同時に満たすことが可能となる. 具体的には,IoT データを IFPS に保存し, そのハッシュ値を DID とともにブロックチェーンに記録することで,

- DID によるデータ所有者の真正性の保証
- IPFS ハッシュによるデータ完全性の保証

を実現できる. これにより, 中央集権型管理の問題を解消し, 信頼可能でユーザー主権的な IoT データ流通基盤の構築を可能とする.