

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

近年,IoT 機器の爆発的な増加に伴い,生成されるデータ量は急激に増加している。さらに,IoT は家庭や産業,医療,農業など多様な分野で活用されるようになり,生成されるデータの種類や粒度も一層多様化している。

また,従来の中央集権型による IoT データ管理には主に以下の 3 つの課題が存在する。第一に,スケーラビリティの問題である。IoT デバイスの急増により,そのデータを保存する中央サーバーへの負荷が指数関数的に増大し,処理能力の限界に達する可能性がある。第二に,セキュリティ上の問題である。中央サーバーは単一障害点となりやすく,攻撃対象として脆弱である。第三に,プライバシー保護の問題である。個人情報を含む IoT データが集中することで,情報漏洩時の被害が甚大化するリスクがある。

これらの課題を解決するために,本研究ではユーザ主権型 ID に基づいた分散型データ管理システムの実現を目指す。本システムは,以下の三点を重視して設計されている。

1. データの分散管理:中央集権型管理から脱却し,分散型ファイルシステムである InterPlanetary File System(以下 IPFS)を用いることで,単一障害点を排除しシステムの堅牢性を向上させる。
2. ユーザの真正性確保:分散管理環境におけるなりすまし防止のため,分散型識別子である Decentralized Identity(以下 DID)を活用し,データ所有者の身元を保証する。
3. データの信頼性と改ざん防止:ブロックチェーンを活用し,データが改ざんされていないことを検証可能とする。

以上の要素を組み合わせることで,IoT データに対する分散型かつ信頼可能な管理基盤を構築することを目指す。

## 2 関連研究

IoT データ管理におけるプライバシー確保は,従来より大きな研究課題とされている。現行の IoT システムは,多くが中央集権型のクライアントサーバーモデルに依存しており,生成される膨大なデータはサービスプロバイダを介して管理される。このような中央集権型モデルは,ユーザの行動履歴や個人情報が第三者に漏洩・不正利用されるリスクを内包している。この問題に対処するため,近年ではブロックチェーンを基盤とした分散型データ管理アーキテクチャの研究が進められている。

IoT とブロックチェーンの統合に関する典型的なユースケースとしては,(1) イベントの改ざん防止ログ,(2) アクセス制御の管理,(3) IoT センサーデータの購入などが挙げられる[1]。これらの研究では,ブロックチェーンが持つ分散性と改ざん耐性を活用し,IoT 環境におけるデータ完全性の確保を目指している。一方で,既存の研究の多くは概念設計やプロトコル提案に留まり,Proof-of-Concept レベルの実装や性能評価が十分に行われていないことが課題とされている。

Ali ら[2]は,ブロックチェーンと IPFS を組み合わせたモジュラーコンソーシアムアーキテクチャを提案している。このモデルでは,IoT デバイスをプライベートな「サイドチェーン」にグループ化し,アクセス制御の管理を「コンソーシアムブロックチェーン」によって実現する。サイドチェーンはセンサーデータ生成イベントを記録し,コンソーシアムブロックチェーンはアクセス要求の不変なログを保持することで,プライバシー保護とアカウンタビリティを両立させている。さらに,データ自体は IPFS 上に保存され,ブロックチェーンはハッシュのみを記録することで,ストレージ効率とセキュリティの両立を実現している。

評価実験として,Ethereum(PoW) および Monax(PoS/Tendermint) を用いた性能比較が行われている。その結果,Monax はサイドチェーンレベルで低い処理オーバーヘッドを示す一方で,コンソーシアムレベルでは高いネットワークトラフィックオーバーヘッドが課題となった。Ethereum はコンソーシアムレベルで通信効率に優れるものの,PoW に基づく高い計算コストが問題点として指摘されている。このように,ブロックチェーンのコンセンサスメカニズムの選択は,IoT 分散アーキテクチャの実用性に直接影響を与えることが明らかとなっている。

また,[1] では,IoT センサーから得られるデータを二重チャネル (Dual Channel) で配信するミドルウェアが提案されている。一方は Ethereum と IPFS を用いたインテグリティチャネルで,データ完全性を保証する。もう一方は MQTT を利用したリアルタイムチャネルで,低遅延かつ高速な配信を実現する。この方式は,後からインテグリティチャネルを参照することで,リアルタイムチャネル経由で受け取ったデータの改ざん検出が可能になる点に特徴がある。ただし,Raspberry Pi を用いた評価では,インテグリティチャネルにおいて数百秒規模の遅延やデータ欠損が発生

するなど、ブロックチェーンのオーバーヘッドとリソース制約の影響が確認されており、実運用に向けた課題も示されている。

本研究は、これらの先行研究の知見を基盤としつつ、IoT データ管理における **DID** と **VC** の統合に焦点を当てる。既存研究が主に公開鍵基盤に依存したアクセス制御を行っていたのに対し、本研究では DID/VC を導入することで、より柔軟かつ標準化された認証・検証モデルを提供する点に新規性がある。また、Ethereum および IPFS を用いたローカル環境での実装と性能測定を通じて、スケーラビリティと実用性の両面から評価を行うことを目的としている。

### 3 準備

本研究では、分散型データ管理の基盤技術として IPFS, DID、およびブロックチェーンを用いる。本章では、これらの技術の概要を説明し、さらに本研究で使用した実験環境について述べる。

#### 3.1 IPFS

IPFS は、ファイルを单一サーバに保存する従来の方式とは異なり、世界中のノードに分散的に保存するピアツーピア型のファイルシステムである。特徴は「コンテンツアドレス方式」である点で、保存されたファイルはその内容を基に計算される Content Identifier(以下 CID) によって参照される。CID はファイル内容のハッシュ値であるため、以下の性質を持つ。

- 同一内容のファイルは必ず同じ CID となる。
- 1 ビットでも内容が変更されれば別の CID となる。
- CID から元のデータを推測することはできない。

この仕組みにより、ファイルが改ざんされていないかを CID の比較によって確認できる。

本研究では、ユーザが保有する IoT データを IPFS に保存し、得られた CID をブロックチェーンに記録することで、データの真正性と参照可能性を確保している。

#### 3.2 DID

DID は、特定の中央管理者に依存せずに個人が自分自身で生成・管理できる識別子であり、分散型デジタルアイデンティティの基盤となる技術である。DID は単なる文字列であるが、この DID に関する公開鍵や認証方法等をまとめた文書を DID Document と呼び、識別子の正当性確認に用いる。DID Document はブロックチェーンなどの改ざん耐性を持つ基盤に保存されることで、第三者がその内容を検証可能となる。

本研究では、ユーザ A が発行した DID と DID Document をブロックチェーンに登録し、IoT データの所有者であることを証明するための基礎情報として利用する。

さらに本研究のシステムでは、企業がユーザに対して Verifiable Credential(以下 VC) を発行し、IoT データが正当なデバイスによって生成されたものであることを保証する仕組みを構築する。VC の検証時には、DID Document に記録された公開鍵により署名を確認し、データの真正性を確認することができる。

#### 3.3 ブロックチェーン

ブロックチェーンは、ネットワーク上の複数のノードが同一のデータを共有し、合意形成に基づいて取引履歴を記録する分散型台帳である。記録されるデータは複数の取引をまとめた「ブロック」に格納され、各ブロックは直前のブロックのハッシュ値を保持することで鎖状に連結される。この構造により、一部のブロックが改ざんされると以降すべてのブロックの整合性が崩れるため、改ざんは即座に検知される。

特に重要なのは、ハッシュ値の性質である。ハッシュ値はデータから一方向的に算出される識別子であり、内容にわずかな変更があっても全く別の値となる。また、ハッシュ値から元のデータを復元することはできない。ブロックチェーンではこの性質を利用し、データの完全性を保証している。

本研究では、IoT データの要約情報 (IPFS の CID) および DID Document をスマートコントラクト経由でブロック

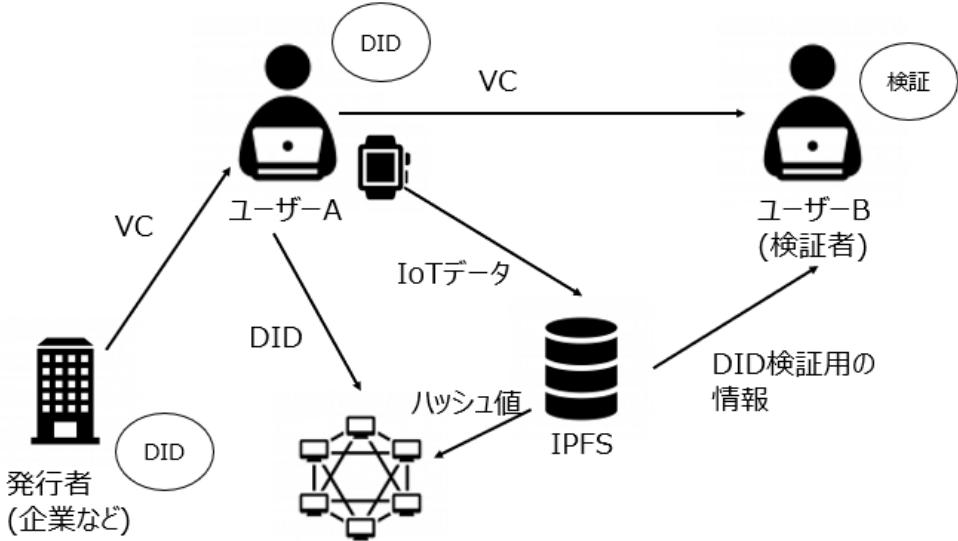


図 1 提案システムの概要図

チェーンへ記録することで、データ登録の証跡を改ざん不能に保持できるようにしている。

さらに、既存研究においても議論されているように,Proof-of-Work(以下 PoW)はエネルギー消費が大きく、リソース制約のある IoT 環境には適さないことが指摘されている [1]. そのため、本研究においても PoW ベースのブロックチェーンは採用せず、より実装や評価に適した Ethereum 環境を主に使用することとした。

## 4 システム構成

本研究で提案するシステムは、IoT データを分散的に管理するために,DID,IPFS, およびブロックチェーンを連携させたものである。本章では、まずシステム全体の流れを示した後、各要素の役割について説明する。

### 4.1 システムの概要

本研究で提案するシステムの全体像を図 1 に示す。1 に示すように、ユーザ A は自身の IoT データを IPFS に格納し、その結果として得られるハッシュ値(以下 CID)を、自身の識別子である DID とともにブロックチェーンに記録する。その後、発行者が IoT データの真正性を保証する Verifiable Credential(以下 VC)を発行し、検証者であるユーザ B がブロックチェーン上の DID 情報と VC を突き合わせることで、ユーザ A の正当性を検証する。

#### 4.1.1 データ所有者(ユーザ A)

ユーザ A は、自身の識別子として DID を保持し、その検証用情報(公開鍵など)をブロックチェーンに格納する。さらに、保持している IoT データを IPFS に格納し、IPFS から返される CID を取得する。この CID はデータの一意なハッシュ値であり、データ改ざん検知に利用できる。ユーザ A は、CID と自身の DID を組み合わせてブロックチェーンに登録することで、データの所有者であることを保証する。

#### 4.1.2 発行者(企業など)

発行者とは、ユーザ A に対して VC を発行する主体である。本研究ではユーザ A が所持している IoT 機器の製造元企業などを想定している。発行者はユーザ A が保持している IoT データが自社製品によって生成されたデータであることを確認し、その真正性を保証する VC をユーザ A に発行する。

#### 4.1.3 検証者(ユーザC)

検証者は、ユーザAとIoTデータを取引する相手、すなわちデータの受領者を想定している。検証者は、ユーザAから提示されたVCを受け取り、ブロックチェーン上のDID情報と照合することで、ユーザAが真正なデータ所有者であることや、IoTデータについて企業が保証していることについて確認する。

## 5 システム全体のフロー

本研究で構築したシステムは、IoTデータを提供するユーザA、データの真正性を確認する企業(発行者)、および最終的にVCを検証する第三者(検証者)により構成される。システムの処理は、登録フェーズと検証フェーズの2つに大別される。

登録フェーズではDID・DID Document・IoTデータがブロックチェーンおよびIPFSに記録され、企業によるVC発行までが行われる。一方、検証フェーズでは、提示されたVCの署名検証を通じてユーザAが真正なデータ提供者であることを確認し、安全なデータ取引を可能にする。

以下では、両フェーズの詳細な処理について説明する。

### 5.1 登録フェーズ

登録フェーズの全体像を図2に示す。本フェーズは、DIDの生成・登録、IoTデータの保存、CIDの登録、および企業によるVC発行、ユーザAによるVCへの署名までの流れで構成される。

#### 5.1.1 DIDの生成とDID Documentの登録

まず、ユーザAおよび企業はそれぞれDIDを生成し、公開鍵などの識別情報を含むDID Documentを作成する。作成したaDID Documentはスマートコントラクト(registerDIDDocument)を通じてブロックチェーンへ登録される。これにより、各主体の公開鍵が台帳上に保持され、後続処理における署名検証の基盤が整備される。

#### 5.1.2 IoTデータの保存とCIDの取得

次に、ユーザAは自身が保有するIoTデータをIPFSに保存する。保存されたデータに対し、IPFSは一意のCID(Content Identifier)を返却する。

#### 5.1.3 CIDとDIDのブロックチェーンへの記録

ユーザAは取得したCIDと自身のDIDをスマートコントラクト(registerDIDDocument)を用いてブロックチェーンへ登録する。これにより、「どのDIDがどのIoTデータの所有者であるか」が改ざん耐性を持って記録され、第三者は所有者を検証可能となる。

#### 5.1.4 企業によるデータ真正性の確認とVC発行

企業は、ブロックチェーン上のDIDとCIDの整合性を確認し、ユーザAが登録したデータが真正であるかを検証する。正当性が確認された場合、企業はユーザA向けにVCを発行する。VCには企業のDIDによる署名が付与され、内容の真正性が保証される。

#### 5.1.5 ユーザAによるVCへの追加署名

最後に、ユーザAは自身のDIDに紐づく秘密鍵を用いてVCに追加署名を行う。これにより、企業とユーザAの双方が署名したVCが完成し、検証フェーズにおいて提示・検証可能な証明情報となる。

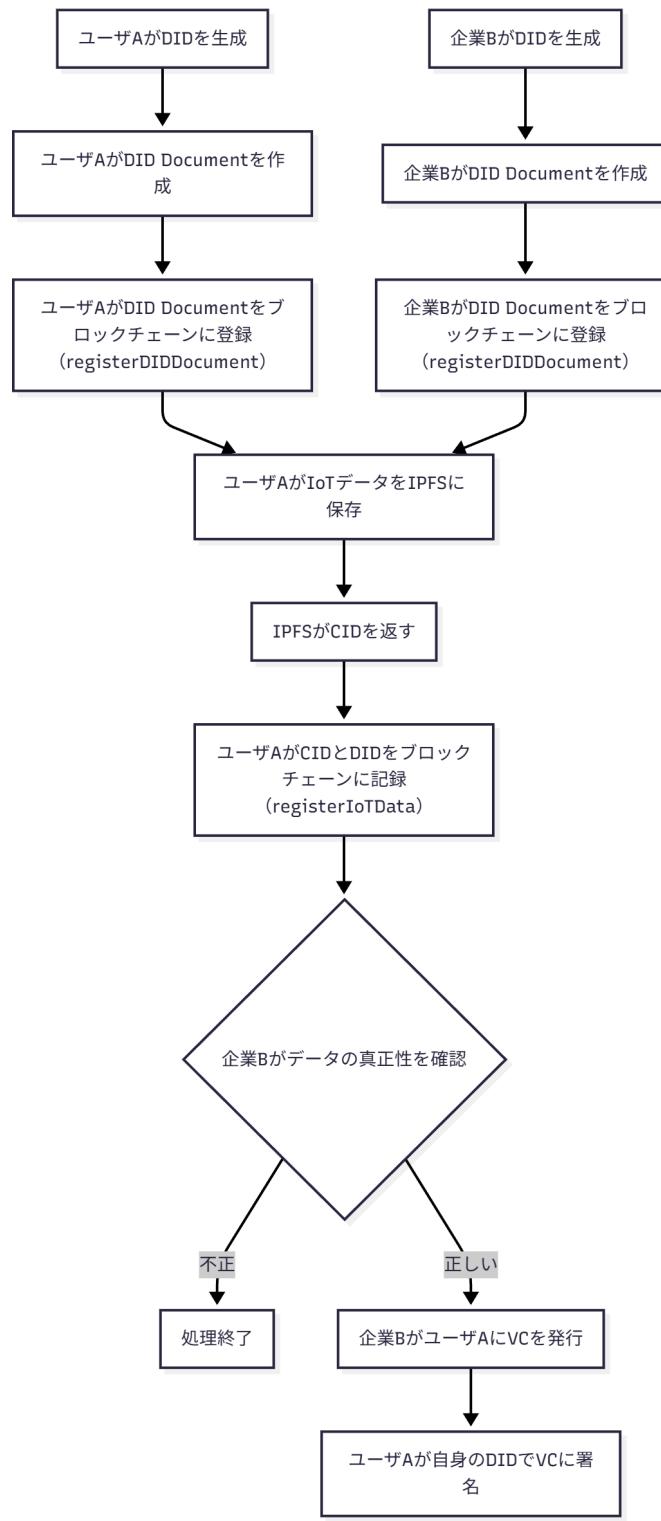


図2 登録フェーズのフローチャート

## 5.2 検証フェーズ

検証フェーズの処理全体を図 3 に示す。本フェーズでは、ユーザ A が提示した VC に含まれる署名を順に検証し、データ提供者の正当性を確認する。

### 5.2.1 VC の提示と受領

ユーザ A は完成した VC を検証者へ提示する。検証者は VC を受け取り、内容に含まれる署名情報と DID 情報を確認する。

### 5.2.2 企業の署名検証

検証者はまず VC に含まれる企業の署名を検証する。署名の公開鍵は、ブロックチェーンへ登録された企業の DID Document から取得される。署名が不一致であった場合、VC は不正と判断され処理を終了する。

### 5.2.3 ユーザ A の署名検証

企業の署名が正当であった場合、次にユーザ A の署名が検証される。ユーザ A の公開鍵は同様に DID Document から取得でき、署名が一致する場合、ユーザ A が IoT データの正当な保有者であることが確認される。不一致の場合、処理は終了する。

### 5.2.4 データの取引の実行

企業およびユーザ A の署名がいずれも正当であれば、検証者はユーザ A が真正なデータ提供者であると判断できる。この確認を基に、検証者はユーザ A と安全にデータ取引を実行する。

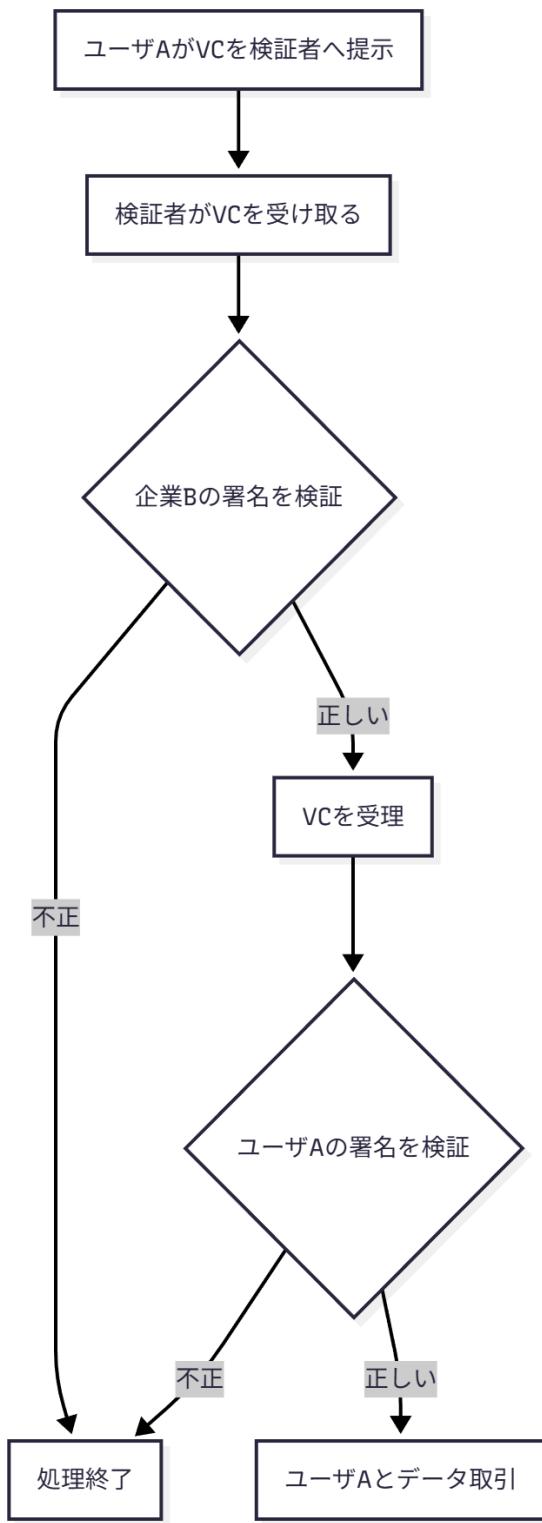


図3 検証フェーズのフローチャート

### 5.3 スマートコントラクトによる登録処理

本研究で使用したスマートコントラクトでは、ユーザの DID Document および IoT データ (CID) をブロックチェーンに記録するために `registerDIDDocument` および `registerIoTData` の 2 つの関数を提供している。それぞれの処理内容を擬似コードとして以下に示す。

---

**Algorithm 1** DID Document の登録処理 (`registerDIDDocument`)

---

**Require:** DID, DID Document(JSON 形式)

- 1: 呼び出し元アドレスを取得する (これをユーザ識別子として扱う)
  - 2: DID Document を以下の形式で保存する:
  - 3:    `records[呼び出し元アドレス].append( (DID, DID_Document) )`
  - 4: DID 登録イベントを発行する
- 

---

**Algorithm 2** IoT データ (CID) の登録処理 (`registerIoTData`)

---

**Require:** DID, CID(IPFS で取得したハッシュ値)

- 1: 呼び出し元アドレスを取得する
  - 2: IoT データを以下の形式で保存する:
  - 3:    `iotData[呼び出し元アドレス].append( (DID, CID) )`
  - 4: IoT データ登録イベントを発行する
- 

## 6 実験と考察

### 6.1 実験目的

本研究の実験目的は、提案システムが実社会の運用に耐えうる性能と有効性を備えているかを検証することである。まず、IoT データの記録から VC による検証までの一連の処理を再現し、DID・VC・IPFS・ブロックチェーンを統合したシステムとして正しく動作することを確認する。また、分散ストレージとして利用する IPFS に対して、ファイルアップロード処理の処理時間・スループット・エラー率を測定し、膨大なデータ量を扱う IoT 環境において実用的に運用可能かを評価する。さらに、DID および VC を用いたユーザ検証処理、およびブロックチェーンへのトランザクション記録に要する処理時間を測定し、提案システム全体の性能を定量的に評価する。

### 6.2 実験環境

実験は以下の環境で行った。

- OS:Windows 11 Home
- CPU:AMD Ryzen 5 PRO 7530U with Radeon Graphics(2.00Hz)
- メモリ:16GB
- IPFS:go-ipfs v0.35.0
- ブロックチェーン環境:Ganache v7.9.2
- Solidity: v0.5.16
- Node.js: v18.20.7
- Truffle: v5.11.5
- Web3.js: v1.10.0

6.3 実験方法

6.4 実験結果

6.5 考察

7 まとめ

## 参 考 文 献

- [1] Simon Krejci, Marten Sigwart, and Stefan Schulte. Blockchain- and IPFS-based data distribution for the internet of things. In Antonio Brogi, Wolf Zimmermann, and Kyriakos Kritikos, editors, *Service-Oriented and Cloud Computing*, pp. 177–191, Cham, 2020. Springer International Publishing.
- [2] Muhammad Salek Ali, Koustabh Dolui, and Fabio Antonelli. IoT data privacy via blockchains and IPFS. In *Proceedings of the Seventh International Conference on the Internet of Things*, IoT ’17, New York, NY, USA, 2017. Association for Computing Machinery.