6D-03

ブロックチェーン技術を利用した企業間認証基盤の提案

本庄　将也†　　松本　光弘†　　松山　賢‡　　酒巻　一紀‡　　菅野　幹人‡　　白木　宏明†
三菱電機株式会社　情報技術総合研究所†　三菱電機インフォメーションシステムズ株式会社‡

1. はじめに

経済産業省は「Connected Industries」を国産業が目指す姿として掲げており、協業の流れが今後加速すると考えられる。そのため、様々な業種で企業間連携が注目されている。

企業間連携が活発になり、様々な企業の社員が密に連携を取りながら業務を行うようになった場合、各企業の業務システムを様々な企業の社員が利用するようになると考えられる。このとき、相互の認証システムに他社の社員を追加しなければならず、ユーザ ID や認証情報の管理が煩雑になることが課題となる。

この課題の解決策の一つとして、企業間認証が挙げられる。企業間認証は、複数の企業の社員のユーザ ID を一元管理し、一つの認証システムでユーザ認証を実施することで、複数の企業の社員の認証が可能とするシステムである。

複数企業が企業間認証を利用する場合、ID as a Service(IDaaS)や OpenID 等の第三者機関による認証サービスを利用するか、参加企業の内の 1 社が代表して認証システムを構築し稼働させる必要がある。しかし、前者は第三者に社員情報を提供するセキュリティリスクがあり、後者は企業間認証システムの開発や運用費用の分担が難しいという問題があった。

本論文では、上記の問題を解決する新しい企業間認証として、ブロックチェーン技術を利用した企業間認証基盤を提案する。提案手法は、ユーザ認証に必要な情報を各社がブロックチェーン上で共有し、各企業にそれぞれ配置した認証サーバがブロックチェーンから認証情報を取得し、ユーザが入力した情報との整合性を検証することで認証を実現する。また、提案手法がスループットや処理時間の観点で実用に足ることを示すために、ブロックチェーンの性能を実験環境で評価する。

Decentralized authentication system using blockchain technology
†Mitsubishi Electric Corporation Information Technology R&D Center
‡Mitsubishi Electric Information Systems Corporation

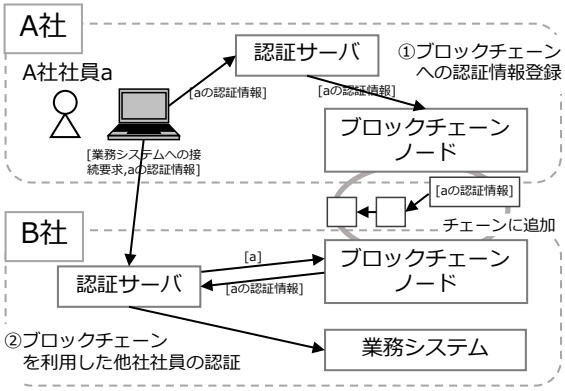

図 1 提案企業間認証基盤の概念図

2. 提案手法

本論文で提案する企業間認証基盤について説明する。システムの全体構成の概念図を図 1 に示す。1 つの企業は必ずブロックチェーンノードと認証サーバを保有する。ブロックチェーンノードはブロックチェーンに参加するノードで、少なくともブロックチェーンへの登録機能とブロックチェーンの参照機能を持つ。認証サーバはユーザ認証を行うサーバである。認証サーバはブロックチェーンノードを利用してブロックチェーンに登録された認証情報を取得し、これと入力された認証情報からユーザ認証を行う。認証方式は、パスワード認証や生体認証等、既存の手法を利用する。図 1 には、企業間認証基盤を利用する 2 社が示されている。まず、A 社社員 a が自社の認証サーバを経由してブロックチェーンに認証情報を登録する。a の認証情報はブロックチェーンを経由して B 社も閲覧可能な状態となる。次に a は B 社の業務システムにアクセスする。この時、B 社の認証サーバによるユーザ認証が行われ、B 社の認証サーバは a から送信された認証情報とブロックチェーンに登録されている a の認証情報から認証を行う。認証が成功すれば、a は B 社の業務システムを利用可能となる。

本提案手法では、トランザクションに認証情報を含めることができればどのようなブロックチェーンでも利用可能である。

例えば、Bitcoin [1]や Ethereum [2]は、仮想通貨の取引の他にユーザが任意のデータを登録

する手段があるため、本提案手法のブロックチェーンとして利用可能である。パブリックブロックチェーンと呼ばれるこれらのブロックチェーンは、世界各地のノードによって運用される分散システムであるため可用性は高いが、世界中に認証情報を公開してしまうという特徴がある。これは第三者機関に認証を委託するより認証情報の公開範囲が広いと言える。

一方、Hyperledger に代表されるプライベートブロックチェーンは、許可された参加者だけで構築するブロックチェーンであり、情報公開範囲は参加者だけで閉じられる。

以上から、第三者に社員情報を提供することなく、認証を実施したい場合、プライベートブロックチェーンが適していると言える。

また、ブロックチェーンは各ノードがシステム維持責任を平等に負うため、コストの分担も平等化しやすいと考えられる。

3. ブロックチェーンの性能評価実験

提案手法の認証機能が実運用に足るか調査を行う。検証環境にプライベートブロックチェーンの 1 つである Hyperledger Fabric [3]を構築し、ブロックチェーンへのデータの書き込み速度と読み込み速度を計測する。これにより、ブロックチェーンが認証機能の性能要件のボトルネックとなり得るか判定できる。

3.1 実験設定

検証環境の構成を表 1 に示す。1 台のサーバに 4 台の VM を作成し、この 4 台の VM でブロックチェーンを動作させる。ブロックチェーンに登録するデータは、パスワード認証を想定し、ユーザ ID とパスワード、属性情報を含む文字列とする。ブロックチェーンへのアクセスは、それぞれの VM に Hyperledger Fabric が提供する REST API を利用してアクセスするクライアントを複数起動し、それを用いる。データ登録時間及び参照時間は、そのクライアントが REST API を使用してから応答があるまでの実時間とする。

3.2 実験結果及び考察

データ登録とデータ参照における最大スループットと平均処理時間を表 2 に示す。スループットはブロックチェーン全体で 1 秒当たりに処理できるデータ件数であり、処理時間はクライアントの処理要求から結果が返ってくるまでの時間を表す。また、表 2 の平均処理時間は、最大スループットとなる条件においての平均処理時間である。

表 1 検証環境構成

項目	設定内容
サーバ CPU	Intel Xeon CPU X5670 @ 2.93GHz (物理コア 6, 論理コア 12) ×2
ハイパーバイザ	VMware ESXi 5.5.0
VM 数	4
VM 構成	2 CPU, メモリ 4GB
ブロックチェーン OSS	Hyperledger Fabric v0.6.1-preview

表 2 検証環境での処理性能

	最大スループット	平均処理時間
データ登録	175.88［件/秒］	0.416［秒］
データ参照	351.76［件/秒］	0.233［秒］

データ登録は認証システムで頻発する操作ではないため、検証結果の性能で十分であると考えられる。データ参照は認証処理の度に発生するため、始業開始時にピークになると考えられる。最大スループットで 10 分間稼働したとき、約 21 万人のユーザ認証を行うことができる計算となるため、多くのケースで実運用に足る性能であると考えられる。

4. おわりに

本論文では、企業間連携が密になり各企業の業務システムを相互利用する際に有効である企業間認証について、従来の中央集権的な方法ではなく、協力する各企業が分散的に管理する方法を提案した。また、提案手法の認証情報の管理方法にはプライベートブロックチェーンを用い、参加企業間だけでの情報共有や運用コストの平等化が可能であることを示した。さらに、プライベートブロックチェーンの一種である Hyperledger Fabric の性能検証を行い、スループットや処理時間の観点では実運用に足ることを示した。

参考文献

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. https://bitcoin.org/bitcoin.pdf.

[2] G. Wood, "ETHEREUM: A secure decentralised generalised transaction ledger," 2014. http://gavwood.com/paper.pdf.

[3] C. Cachin, "Architecture of the Hyperledger Blockchain Fabric," *Proc. Workshop on Distributed Cryptocurrencies and Consensus Ledgers,* 2016.