Copyright© 2022 The Institute of Electronics,
Information and Communication Engineers

SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

分散台帳技術におけるユーザの同意に基づくアクセス制御フレームワーク

An Access Control Framework Based on User Consent in Distributed Ledger Technology

掛井将平* Shohei Kakei
今村光良† Mitsuyoshi Imamura
白石善明‡ Yoshiaki Shiraishi
廣友雅徳†† Masanori Hirotomo
齋藤彰一* Shoichi Saito

キーワード 分散台帳技術，スマートコントラクト，アクセス制御，OpenID Connect, Hyperledger Fabric

あらまし

分散台帳技術（Distributed Ledger Technology, DLT）は，ネットワーク上の複数のノードで共有される分散台帳とその分散台帳のインタフェースとして機能するスマートコントラクト（Smart Contract, SC）から構成される．SC は複数の当事者間で事前に合意された条件に基づいた処理を実行する仕組みであり，その処理結果のみが分散台帳に記録される．この特定の主体に依存しない処理の仕組みが，中央集権的な信頼が排除されたシステムを構築する仕組みとして注目されている．

ノードの参加形態に応じて，DLT は「自由参加型」と「許可型」のシステムに分類される．不特定多数のノードでネットワークを構成する自由参加型の DLT は，単一信頼点となる管理者がおらず耐障害性に優れる．一方で，SC に不具合があってもシステムを停止できず，被害が拡大しやすい傾向にある[1]．許可型の DLT は，特定の組織のみで構成されるコンソーシアムでネットワークを運用することで，コンソーシアムの判断に応じてシステムの停止や保守が可能であるが，コンソーシアムへの信頼が生じる．DLT を用いたシステムの構築においては，両者の特性を踏まえた検討が求められる．

許可型の DLT は多様な組織でコンソーシアムを組むことでその耐障害性を高めることができるが，参加組織の増加に伴い SC を悪用した分散台帳への不正アクセスのリスクが高まる．そこで本研究では許可型の DLT において，

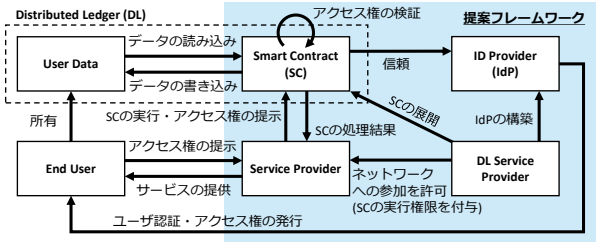

図 1 提案フレームワークの概要

SC の実行権限と分散台帳へのアクセス権限を分離したアクセス制御フレームワーク（図 1）を提案する．提案フレームワークでは，OpenID Connect（OIDC）の IdP により発行されるトークンを分散台帳内のユーザデータへの「アクセス権」とし，この権限の有効性を SC の処理の中で検証する．その結果，ユーザの意思に基づいた SC の実行であることがネットワークの参加者間で合意形成される．本稿では，まず，サービス提供者によるトークンの不正利用のリスクを整理したうえで提案フレームワークを設計する．そして，OIDC 準拠の ID プロバイダである Keycloak と許可型の DLT である Hyperledger Fabric を用いた提案フレームワークの実装を示し，その評価を行う．

参考文献

[1] 北條真史，鳩貝淳一郎，“暗号資産における分散型金融 －自律的な金融サービスの登場とガバナンスの模索－，” 日銀レビュー，2021-J-3，2021 年 4 月．

* 名古屋工業大学，〒466-8555 愛知県名古屋市昭和区御器所町，Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya, Aichi, 466-8555, Japan.
† 野村アセットマネジメント㈱，〒135-0061 東京都江東区豊洲 2-2-1，Nomura Asset Management Co., Ltd., 2-2-1 Toyosu, Koto-ku, Tokyo, 135-0061, Japan.
‡ 神戸大学，〒657-8501 兵庫県神戸市灘区六甲台町 1-1，Kobe University, 1-1 Rokkodai-cho, Nada-ku, Kobe, Hyogo, 657-8501, Japan.
†† 佐賀大学，〒840-8502 佐賀県佐賀市本庄町 1，Saga University, 1 Honjo-machi, Saga, Saga, 840-8502, Japan.