5ZA-05

マルチベンダ開発に向けた 電子文書の流通管理手法の提案

氏　名† 川島悠太　氏　名† 寺島美昭

所　属† 創価大学大学院工学研究科情報システム工学専攻

1. はじめに

企業や自治体などで管理されている電子文書は、組織内で電子ファイルとして保存されていたとしても、他の企業や自治体に共有される際には印刷、メールなどで共有されることが多い。しかし、マルチベンダ開発などの共有が複数回行われる図 1のような状況では、この手法は非常に手間がかかる。また、共有先に悪意のあるユーザが存在した場合、文書が流出する可能性がある。データセンタで管理する場合は管理主体が発行元から第三者機関に変わるため現在の共有手法では共有した文書の管理を発行元が行えていないという問題がある。

発行元による文書管理を実現するために、本研究では P2P 型データ管理手法であるブロックチェーンを用いる。ブロックチェーンインフラを用いることで導入の容易な設計が可能となる。

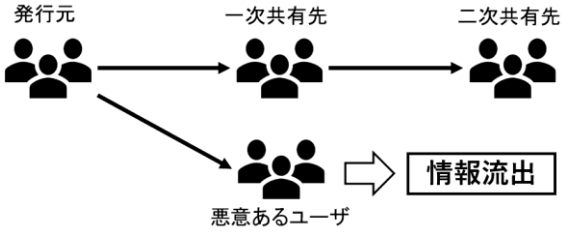

図 1　想定シーン

2. 研究課題

2.1. 文書の保存方式

今回利用するブロックチェーンは通貨管理を目的とした技術である。通貨を管理する場合は、送受金の履歴管理に用いられることが多いが、文書を管理する場合は文書データを管理することが重視される。そのため文書データの一貫性や、保存されている場所まで管理する必要がある。ブロックチェーンは、履歴保持に特化した技術であるため、容量の大きいデータを保持することは考慮されていない。文書をどのように保持し、流通させるかが課題となる。

2.2. 閲覧権の関連を確保

発行元の一元管理を実現するために、閲覧権を関連付けて閲覧権に追跡可能性を付与する必要がある。本稿では、関連閲覧権としてこの課題を解決する手法を提案する。

日本電信電話株式会社の近田ら[1]は社内インフラなどで用いられている暗号化ソリューションとブロックチェーンを組み合わせた。電子文書の共通鍵をブロックチェーン上で受け渡すことで 1 対 1 の文書共有を実現している。しかし、近田らの研究では文書が複数回共有されていくことが想定されていなかった。

3. 提案手法

本研究では、電子文書が 2 社、3 社と流通していくことを想定し、流通していても発行元の権利を守りつつ文書を管理可能な管理形態を目指す。文書の流通管理を行うためのセキュリティ要件は以下の 4 項目であると定義した。図解を図 2に示す。

- 流通性
  - ➢二次、三次の共有が行えること
- 機密性
  - ➢文書の流出を阻止、または検知できること
- 記録性
  - ➢閲覧記録や流通状況の履歴管理ができる
- 一貫性
  - ➢流通している文書は全て同一であること

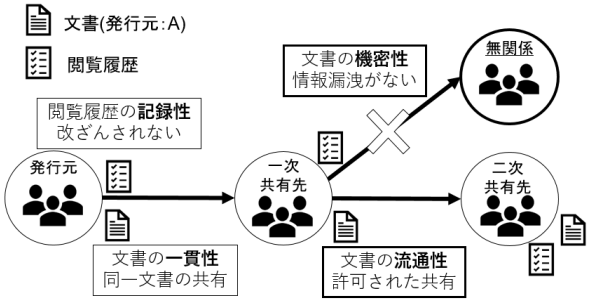

図 2　セキュリティ要件

ブロックチェーンを用いることで改ざんに対して耐性を持った履歴管理を行うことが可能と

P2P security management method for electronic documents in multi-vendor development
† Soka University

なる。またハッシュ変換を用いることで各共有先における文書の一貫性を保つことができる。

流通性と機密性を解決するために、関連閲覧権(図 3)を提案する。発行元が閲覧権を発行する際に、二次共有が行われる前提で発行し、一次共有先は付与された閲覧権を分割、関連付けて閲覧権を管理する。

図 3のように文書を閲覧するための権利同士を関連付けることにより、発行元は「発行元が直接文書を共有した企業の閲覧権」から「共有先が二次共有した企業の閲覧権」まで追跡可能な閲覧権である。発行元から文書を共有された一次共有先は、新たに文書を他の共有先に文書を共有する際に、閲覧権を分割して共有することで、閲覧権同士の関連を保って文書を共有する事ができる。

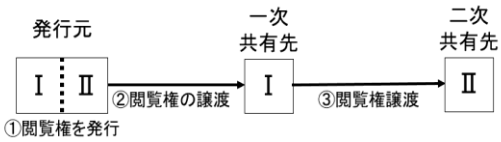

図 3　関連閲覧権

閲覧権を文書ごとに発行するために、閲覧権に文書の情報を付与しておく。一次共有先で利用される閲覧権を一次閲覧権とし、二次共有先で利用される閲覧権を二次閲覧権と定義する。付与する情報は表 1の通り。

表 1　閲覧権付与情報

一次閲覧権	二次閲覧権
発行元情報	発行元情報
一次共有先情報	二次共有先情報
文書情報	一次共有先情報
	文書情報

4. 試作システム構成

提案を評価するために試作システムを構成する。閲覧権はブロックチェーンとの互換性の高い通貨規格による実装を行う。通貨に対し、表1の発行元、一次共有先、二次共有先情報にはブロックチェーン上で定義されるアドレスを用いる。アドレスを用いることによって、個人の判別が可能となる。今回の試作システムにおける文書情報には PDF ファイルを文字列に変換したものを用いる。PDF ファイルを Base64 に変換し、その文字列をハフマン符号化によって可逆暗号方式による暗号化を行う。閲覧の際は逆順に復号して閲覧する。そのため、本試作システムでは閲覧権が文書ファイルを保持しているというモデルとなる。

閲覧権に使用する通貨規格は ERC721 と ERC998 規格を用いる。ERC721 は代替不可能トークンを作成するための規格である。代替不可能トークンとは、通常通貨とは異なり、通貨に PDF などのデジタルデータの情報を付与させることで通貨が独自性を持つ。それにより他の通貨と差別化され、代替することができない特性を持つトークンである。ERC998 は、通貨に所持されることができるという特性を持つ通貨規格である。これにより通貨と通貨を関連付けることができる。

試作するシステムの構成図を図 4に示す。3 台の PC にそれぞれ発行元、一次共有先、二次共有先の役割を持たせ、文書の共有、閲覧が可能であるかを確認する。

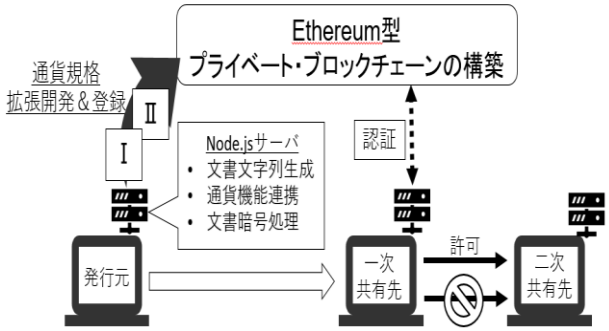

図 4 試作システム構成図

5. まとめ

本稿では、文書の流通を管理するために管理要件の分析を行い、流通性、機密性、記録性、一貫性の 4 つのセキュリティ要件を定義した。ブロックチェーンを用いることで改ざんされにくい履歴機能を実現し、ハッシュ変換により文書の同一性を確保することができるため、記録性と一貫性は解決できる。流通性と機密性の解決には通貨規格をベースとした関連閲覧権を提案した。また、それらの機能を確認するための試作システムの構成についても述べた。

今後の課題として、本稿の提案では電子文書を閲覧権で保持しているが、データサイズが肥大化することが懸念されるため電子文書の保存方式に関して検討を進めていく必要がある。

参考資料

[1]. 近田昌義 渡邊大喜 大橋盛徳 石田達郎 藤村滋 中平篤 冨永隆「ブロックチェーンを利用した組織感のドキュメント流通」信学技法 2019

[2]. 渡邊大喜, 大橋盛徳, 藤村滋, 中平篤“ブロックチェーン上の構造化データに対する権限分散を考慮した開示制御手法, 情報処理学会第 80 回全国大会講演論文集