Vol.2020-CDS-29 No.1
2020/12/3

ブロックチェーンを用いたマルチベンダ電子文書の P2P 型セキュリティ管理手法の研究

川島　悠太[1,a)]　寺島　美昭[1,b)]

概要：現在、マルチベンダ間で利用される電子文書のセキュリティは、クラウドなど第三者機関のストレージへ文書を保存し、アクセス権を他の企業へ配布する集中型で管理される。この方法は企業間で電子文書を利用する利点である流通自由度を低下させ、開発時に企業間で電子的に取り扱う利便性を妨げる。しかし、流通自由度と文書の安全性はトレードオフの関係性であり、P2P 型の文書管理では文書の安全性に課題がある。そこで本報告では、マルチベンダ開発企業間で開発電子文書を P2P 型で管理するセキュリティ管理手法を提案する。ここでは、ブロックチェーンを応用した実現性の高い設計を報告し、開発電子文書の利便性、流通自由度と安全性の両立について考察する。

A Study on P2P-Type Security Management of Multi-Vendor Electronic Documents Using Blockchain

1. 背景

企業、自治体などにおける電子文書の利用は、情報の伝達速度を高めるとともに、いつでもどこでも見られるという電子文書の特性から、業務の柔軟性を高める効果が期待できる。年々複数の組織間で開発プロジェクトを遂行するマルチベンダ的な動きが活発になっていることから、1 対 1 ではなく、1 対多で文書を共有する手法が重要となっている。しかし、組織を跨がるような電子文書の共有手法については明確な規格がないため 1 対 1 を複数回行うことで実質的な 1 対多として扱っているケースがほとんどである。(図 1)

組織を跨がる文書共有として現在主流となっているのは、電子文書を PDF などの形式に変換して、パスワードで安全性を担保して電子メールで送信することや、クラウド等の共有ストレージにアップロードすることであ。電子メールは人的ミスによる文書の流出や誤送信のリスクが有り、クラウドは第三者機関による集中管理であるため、重大なセキュリティ課題があった場合でも文書の発行元は文書を削除するような対策を取れない。また、関係企業以外には

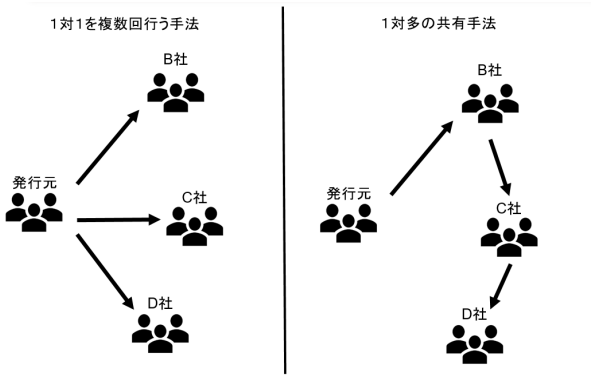

図 1　ファイル共有手法

見せられない機密要求の高い文書も電子文書として扱っていくことを考えると、第三者機関を信頼して文書を預けるのは困難である。そこで、P2P 型の文書管理が期待されている。

本稿では、複数の企業でプロジェクトを遂行するマルチベンダな状況において、発行元から共有先、共有先から別の共有先へと文書が流れるような流通状況において P2P 型で発行元企業の権利を守りつつ、ブロックチェーンを応用した実現性の高い設計を報告し、開発電子文書の利便性、流通自由度と安全性の両立について考察する。本稿における実現性とは、電子文書の管理を共通認識とされているイ

[1] 創価大学大学院情報システム工学専攻
Soka, Hachioji, Tokyo 192–8577, Japan
[a)] e19m5211@soka-u.jp
[b)] tyoshi@soka.ac.jp

ンフラ上で構成できることを指し、流通自由度は各社の文書管理を尊重した形式で、文書管理システムが API 等の役割として機能している状態を指す。安全性は文書が改ざんや不正な閲覧が困難な形式で保存されていることを指す。

2 章では P2P 型の文書管理の先行研究を説明し、3 章では関連研究をふまえた本稿のアプローチについて述べる。4 章では実現に向けた課題を、5 章で課題を解決する提案システムの詳細について述べ、6 章に実験結果。7 章で考察を述べて、8 章でまとめと今後の課題について触れる。

2. 関連研究

P2P 型文書管理では、ブロックチェーンを用いた研究が主流である。ブロックチェーンは 2008 年に暗号通貨ビットコインのコア技術として登場した。特定の管理者なしに、通貨の送金等の取引が行え、多数のノードでデータを管理することで改ざんに強い耐性を持つ分散型取引台帳である。近年では、Ethereum というブロックチェーン基盤の登場で、ブロックチェーン上で動作するスマートコントラクトというプログラムが用いられている。スマートコントラクトにより、取引の自動化や複雑な処理機能をもたせることや電子コンテンツを通貨の形式で管理する、トークン化管理が行えるようになったため、利便性が格段に上昇した。そのため、貿易や電子カルテ、国籍など様々な場面において、トラストレスなシステム構築を推進する足がかりとして利用されている。その中には電子文書の管理も含まれている。関連研究として、本稿と同様に電子文書の流通管理を目的として具体的な解決手法まで検討されている論文と、本稿の文書管理手法の参考とした論文をそれぞれ紹介する。

2.1 流通性を考慮したドキュメント管理手法

日本電信電話の近田らによって、暗号化ソリューションとブロックチェーンの組み合わせによって 1 対 1 の文書の流通管理を行う手法が検討されている。文書は暗号化され、企業の文書管理でも用いられる暗号化サーバによって管理されているが、この状態は各企業が独自で管理をしている。しかし、独自管理では共有先で文書が悪用される危険性があるため、暗号化サーバとブロックチェーンネットワークを繋ぐ API サーバを各社に導入することで、共有先企業のファイル操作等を逐次ブロックチェーンに格納し、共有先における文書の取り扱いを把握するという手法が取られている。文書はブロックチェーン上ではなく、暗号化サーバで管理されているが、ブロックチェーンと無関係というわけではなく、電子コンテンツをブロックチェーン上のトークンと紐付けることが出来る ERC721 を用いることで文書ブロックチェーン上で管理する手法を提案している。

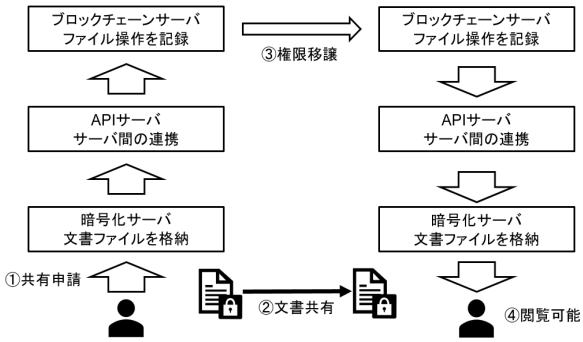

図 2 3 つのサーバによる文書管理

2.2 ブロックチェーンにおけるコンテンツ制御手法

日本電信電話株式会社の大橋らはトークン連動型のファイルシステムを提案している。本稿と同じく、クラウドは単一障害点となりうるという点を危険視し、P2P 型のデータ共有の中でも、IPFS によるデータの流動性に特化したデータ管理と、分散クラウドストレージという安全性は高いが流動性は低いデータ管理手法の中間の管理手法を提案してる。ルートオブジェクトをトークン化し、コントラクトの ABI 情報などをもたせた共有情報や、分割した文書 ID を紐付けることで管理を行う。

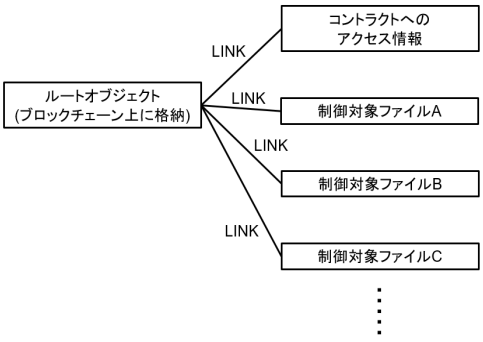

図 3 分散ファイルシステム上のデータ構造

3. 研究課題

発行元、一次共有先、二次共有先の 3 社による文書共有をベースに説明する。文書の発行元企業から共有先企業への共有の際、発行元企業には文書の閲覧を常に履歴として監視、文書の共有や停止を発行元の判断で自由に行う、文書が不正に閲覧や改ざん等が行われることなく管理できるという 3 つのニーズが存在する。しかし、一次共有先には文書の管理は自由に行い、柔軟な状況にも対応出来るようにすることや、開発の下請け企業などの提携先企業へ文書を共有したいというニーズが存在する (図 4)。

これらのニーズを満たし、実現性と流通自由度を持った P2P 型の文書管理を実現するためには図 5 の 7 点を満たす

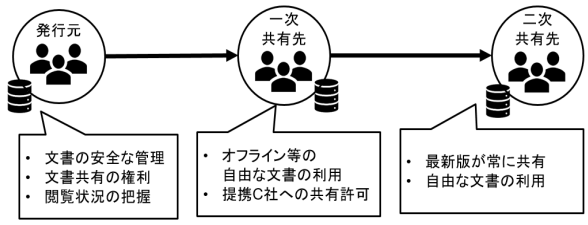

図 4　各社の文書管理要件

必要がある。

(1) 共有や閲覧の履歴情報を改ざん困難な形式で保持する
(2) 共通認識となるインフラ上で構築できる
(3) 管理を中立として、分散的な管理が可能
(4) 発行元が文書の所在を明確に把握できる
(5) 文書は流出や改ざん困難な保存がされる
(6) 文書が不正な方法で閲覧されない
(7) トラブルの際、発行元が共有停止の判断を行える

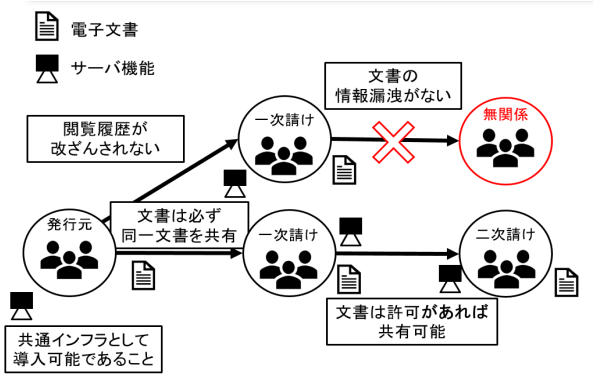

図 5　P2P 型共有管理要件

(1)(2)(3) に関してはブロックチェーンを用いることで解決が見込めるため、特に検討と工夫が必要な (4)(5)(6)(7) についてここで詳細を述べる。

3.1　文書の所在管理 (4)(5)

通貨の管理においては、通貨の送金履歴を記録することがブロックチェーンの主な役割であった。しかし、文書管理の際は文書データの実体を管理する必要がある。文書などのデータ容量の大きいデータをブロックチェーンで管理する場合は、データを分割し、IPFS や分散クラウドなどの手法で保存する。その分割したデータの所在をアドレスとしてリスト化したルートオブジェクトだけをブロックチェーンに格納する場合が多いが、企業の機密文書を扱う場合は、他者へのデータ委託には流出や改ざん、意図しない削除、紛失等のリスクが伴うため文書の所在を明確にし、データの安全性を守るような所在管理手法を検討する必要がある。

3.2　文書の閲覧方法 (6)

文書は保存するだけではなく、閲覧する必要がある。開

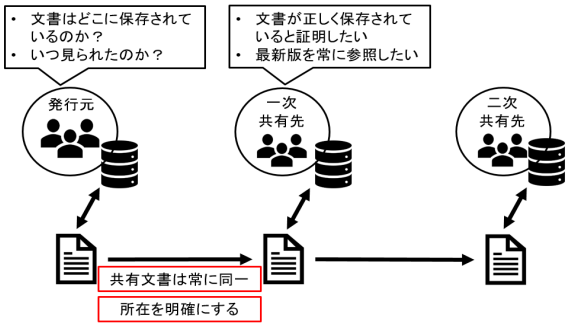

図 6　文書の所在管理

発シーンでは同一のプロジェクトに参加していても、一部のユーザのみにしか共有しない文書も存在するため、共有された許可のあるユーザのみが閲覧できるような工夫が必要となる。

3.3　発行元の権利 (7)

1 章にも記載したが、現在の共有手法の大きな問題点は、発行元が文書に対してなにもアクションが取れない手法が多いことにある。発行元は、共有先企業が不正な方法で文書にアクセスした際や、正規の手段でも発行元が意図しない場合は文書の共有を停止するなどの対策が必要となる。

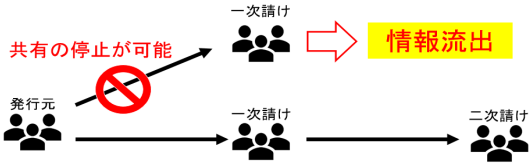

図 7　トラブルの際の共有停止

4.　提案

課題 (1)(2)(3) の解決方法について述べ、システムモデルを示してから各課題を解決する手法について述べる。

課題 (1)(2)(3) を満たすための手法として、 2 章の関連研究から、ブロックチェーン基盤の Ethereum を利用する。ブロックチェーンにはどんなユーザでも参加できるパブリックネットワークと、一部の参加者のみで構成されるプライベートネットワークがあり、プライベートネットワークには企業連携のためのネットワークであるコンソーシアムネットワークが存在する (図 8)。本研究では、文書の安全な管理とマルチベンダでの利用を目指していることから、ベンダ間ネットワークに複数のユーザが存在するようなコンソーシアム型におけるシステム利用として検討する。

4.1　システムモデル

検討するシステムの大まかなモデルについて述べる。文

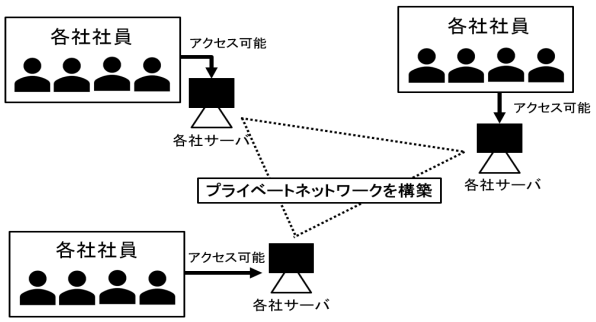

図 8　コンソーシアム型ネットワーク

書の流通性と安全性を兼ね備えつつ、各社が自由な管理を行うためには図 9 のように文書や取引記録、権限情報などを管理するブロックチェーンレイヤーと各社が通常の文書を管理する際にも用いている企業レイヤーに分割して考える必要がある。企業レイヤーについては、ブロックチェーンサーバと各社ユーザを繋ぐことができれば良い。例として、各社がリモート対応という形式にしているのであれば、API サーバでカフェ等社外にいるユーザを管理し、API サーバがブロックチェーンサーバに行いたい動作を伝え、共通インフラとなっているブロックチェーンレイヤーから文書を取り出して来れば良い。これにより各社が文書の利用をある程度任意に決めることができるようになり、文書の利便性の高い設計が可能となる。

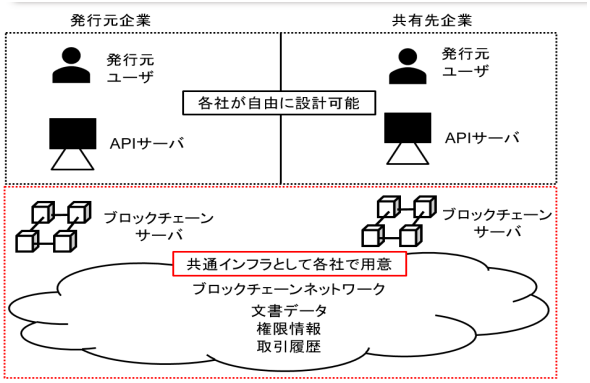

図 9　システムモデル

システムモデルから本稿において重要となるのはブロックチェーンレイヤーの設計となる。そこで本稿では残った課題 (4)(5)(6)(7) を実現する機能として、文書管理における重要点をシステムの動作を 3 つに分けた。

- 共有：所在明確かつ改ざん、流出困難な文書保存
- 閲覧：許可されたユーザのみ閲覧可能な手法
- 削除：発行元の判断で文書の共有停止が行える

これらの動作におけるシステムモデルの動作とそれを実現するための機能処理について述べる。

4.2　共有

共有は各社のユーザからブロックチェーンサーバへ共有取引の発行を行う。本稿では 2.2 節のトークン型コンテンツ管理手法を参考に文書の管理を行う。3.1 項で述べたように、文書を開発プロジェクトに関係のないユーザに委託することは困難であることから、文書はブロックチェーン上で管理する。共有取引の発行に必要な情報は、相手先のブロックチェーンネットワークにおけるアドレスと、文書データである。現在の Etheruem のコントラクト機能はバイナリデータの変換に対応できていないため、ブロックチェーン上で Base64 形式等の文字列形式に変換してからコントラクトへ渡す。コントラクト上で文書文字列を一定サイズに分割してデータグラムとし、それらにランダムな ID を割り振る。ID はランダムに割り振ることでデータグラムを集めて ID を順番に並べて復元するような方法での文書の不正な復号を防止する。ランダムに ID が振られたデータを復元するためにルートオブジェクトを作成し、ID の順序を記録することで、ルートオブジェクトからのみ文書データを復元できる。この手法ではルートオブジェクトを所持していることが文書のアクセス権を有していることを示す。そのため、ルートオブジェクトはブロックチェーン上に配置するのではなく、トークン化して共有先企業へ共有する。

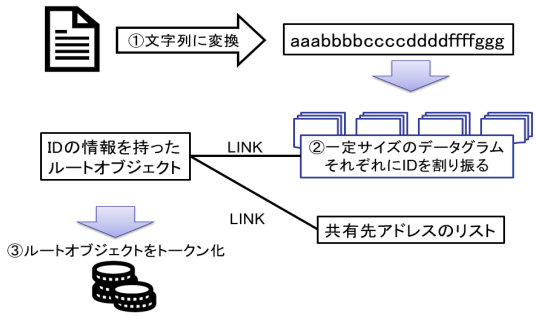

図 10　文書共有処理 (ルートオブジェクトの共有化)

4.3　閲覧

閲覧も共有時と同様に各社のブロックチェーンサーバから閲覧取引の発行を行う。閲覧の際に重視されるのは、共有されていないユーザが不正にアクセスすることができないように処理されることである。そこで、本稿では、文書の共有情報というアドレスリストを作成し、文書文字列の復号前に共有情報に閲覧申請を行ったアドレスが有効であるかを確認することで文書の安全なアクセスを実現する。

文書を閲覧する流れについて説明する。閲覧に必要な情報は、トークン化したルートオブジェクトのみである。共有先企業は、認証用コントラクトへアクセスし、トークンからルートオブジェクトへアクセスして、ID リストからデータグラムを結合して、分割前の文書データの文字列を取り出す。その文書文字列をコントラクトからブロック

チェーンサーバへ送信してブロックチェーンサーバに文書を復元させる。コントラクトは共有先企業が所持しているトークンと、共有情報から認証を行い、共有情報に合致していれば文書の復元を行い、文書を共有先企業へ閲覧させる。コントラクトのアクセス情報はブロックチェーンに履歴として格納されるため、いつ、どの企業が、どの文書を閲覧したのかを発行元企業は知ることが出来る。

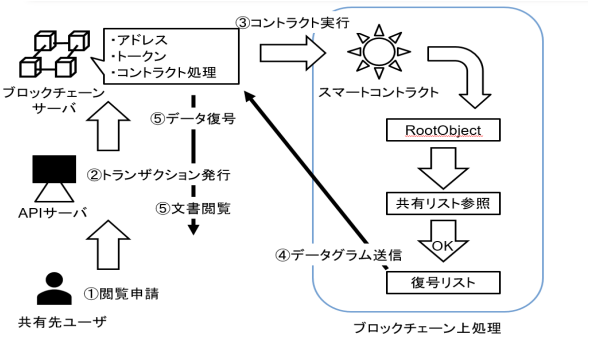

図 11　閲覧時の実行処理

4.4　削除

削除は、共有先でトラブル等があった際に、文書の発行元のみが行える動作である。共有している発行文書の共有情報にアクセスし、共有先アドレスを指定して文書の共有を停止する。先述したように、文書の閲覧の際は毎回、文書の共有情報にアクセスするため、トークンを持っていても、共有情報で文書の共有が停止されていることが分かれば文書の閲覧はできない。これによって共有されている文書も閲覧を制限することが可能となる。

4.5　ブロックサイズの拡張

これらの手法を実現には、ブロックサイズ問題が課題となる。ブロックサイズは、ブロックチェーンネットワークの円滑な実行のために、予め決められているブロック 1 つあたりの処理やデータ量の上限である。ブロックサイズの拡張を行うメリットとして、コントラクトの処理上限が拡張されるため、複雑な処理が行いやすくなること、文書データなどの大きいサイズのデータを管理しやすくなることが挙げられる。デメリットとしてはブロックの肥大化問題と実行コストが挙げられる。ブロックの肥大化はブロックチェーンネットワークへのデータ共有時間を増加し、長期間の運用の際はネットワーク全体の動作を遅らせる可能性が指摘されている。実行コストについては、ブロックチェーン開発で一般的に利用される Ethereum などの開発基盤では、コントラクトの実行の際に gas と言われるコストを支払わなければ実行が行えない。gas は複雑な処理になるほど高額となっていく。ブロックサイズの拡張によって、コントラクトの担う役割が多くなる今回の手法では、無視できないほど高額になる可能性がある。だが、これらはパブリックブロックチェーンにおけるネットワークを常に動作させるモチベーションを保つためのものである。プライベートネットワークにおいては各社が分散して処理機能を担い、ネットワークを運営していくモチベーションも存在する。また、参加するユーザ数も限られているため、共有に致命的な遅れが出るほどの共有時間は発生しないと予測し、今回はブロックサイズの拡張を行う。しかし、本稿の目的は実現性のある文書管理システムの設計のため、具体的な処理時間や消費した gas 値などを、実際に試作システムを用いて実験を行い、利便性と実現性を確認する。

5.　設計

実現性を確認するために Ethereum 上で試作システムの構築を行った。ソフトウェア構成の詳細について述べる。本試作システムでは、トークン化の実現、スマートコントラクトの利用という機能の側面と、プライベートネットワークの設定、ブロックサイズの拡張、豊富な開発情報というサポートの側面から Ethereum を用いて試作システムの開発を行った。具体的に使用したソフトウェアと役割について述べる。試作システムの構成は OSS を主軸に組み立てた (図 12)。各 OSS によるシステムの処理手順は図 13 とし、詳細も各項で説明する。

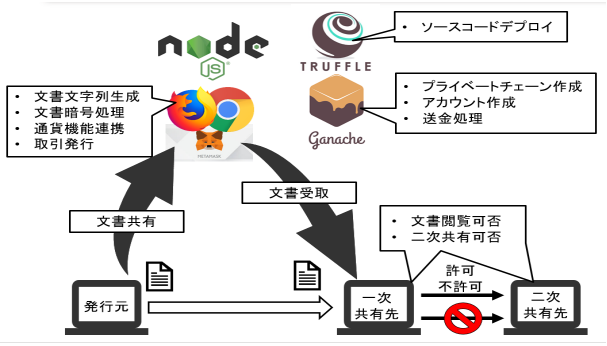

図 12　試作システム全体図

5.1　プライベートネットワークの構築と設定

Ethereum 基盤の ganache-cli を用いてプライベートネットワークを構成した。ganache-cli はブロックサイズやブロックの格納周期なども個別に設定可能となっている。ganache-cli と同一の企業が配布している OSS に Truffle があり、ganache-cli へ自作したコントラクトを格納して動作させたり、スマートコントラクト用言語である Solidity をコンパイルし、テストする機能を持つ。

本試作ではブロックサイズを 1 億として設定した。Ethereum のパブリックネットワークは 1000 万として設定されているが、予備実験において 1000 万の設定では 18.3KB の文書サイズでも格納できなかったため、暫定的

に 10 倍として設定した。

5.2 アカウント管理機能

ganache-cli で構築したプライベートネットワークのアカウントを動作させるために、実際にサーバを介した動作を確認する必要があるため、GoogleChrome の拡張機能である Metamask を用いて Web 上でアカウントの秘密鍵の管理を行った。

5.3 サーバ機能

これらのブロックチェーンシステムにアクセスするためのブロックチェーンサーバとして Node.js を用いてサーバ機能を構築する。javascript には Web3 というブロックチェーンアプリケーションにトランザクションを発行する機能を保有しているため、javascript のみでサーバ機能を担える。主な役割としては、文書を Base64 形式へ変換し、トランザクションとして発行する。その他に、複合した文書の表示などは Web 上で行う。

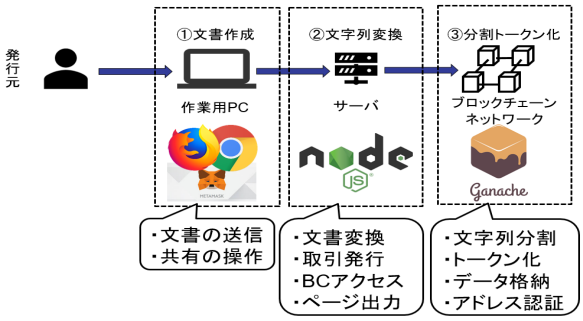

図 13 試作システム処理手順

6. 実験

システムの利便性とシステム設計の課題を調査するために実験を行った。文書を変換し、分割して格納するまでを実験した。文書サイズは 18.3KB と 159KB で行った。各サイズにおける消費した gas と実行時間を示す (表 6)。

文書サイズ	消費 gas 値 (gas)	実行時間 (ms)
18.3KB	22263804	28793.2
159KB	29675655	42969.9

3000 万未満の消費 gas で 40 秒前後の実行時間という結果が得られた。パブリックブロックチェーンにおける処理時間が約 15 秒であることを考えると、時間については改善の余地があると考えられる。また、gas については 18.3KB と 159KB とでは 10 倍程度のサイズ差があるが、消費 gas は 10 倍とはなっていないことから、比例関係ではなかった。そこで 1MB の PDF で実験を行ったところ、Web ページが落ちてしまったため実験結果が得られなかった。ガスリミットを増やしても同様の結果になったことから Web 上での処理をなくすか、トランザクションを複数回にするなどの対策が必要になると考えられる。そこで 18.3KB 時の各処理ごとの gas 消費量をテストした結果を示す (表 6)。

処理名	消費 gas 値 (gas)
Base64 格納	768119
Base64 ＋ハッシュ格納	1081176
アドレス＋ Base64 格納	15784873
文字列の分割格納	20075199
アドレス＋分割格納	22263804

以上の結果から、文書の分割処理により多くの Gas 値が消費されていることが分かった。分割処理をコントラクト上ではない手法で実現できればより gas や時間を抑えた設計が可能となると考えられる。

7. 考察

実験結果から、分割処理について考察を行う。まず、1MB 以上の PDF を扱ったことによる Web ページが落ちてしまった問題について。今回の試作システムでは、GoogleChrome 等のブラウザ機能として文書の変換を行ったため、Web ページが落ちるという問題が起こった。これを解決する手法として、文書の変換をブラウザ上ではなくサーバ上で行う方法が考えられる。18.3KB の PDF でも Base64 形式に変換すると 24368 文字となる。1MB の際はより多くの文字列へと変換されたという予想から、Web 上で保持し続けられるデータを超過したことから Web ページが落ちてしまったと考えられる。そこでブラウザ上から文書データをサーバへ送信し、サーバで文書を変換することで 1MB の文書でも実験を行うことが可能であると考えられる。

次に分割処理については、コントラクト上ではなく、これもサーバで行う方法が考えられる。コントラクト上で行うメリットは発行するトランザクションを 1 つにすることで分割した文書データの ID の関連が明確になることであった。トランザクションの関連を管理する手法を検討することで、サーバでの文書分割が可能となると考えられる。しかし、複数のトランザクションを発行するため、実行に時間がかかることが予想されるが、ブロックチェーンネットワーク全体として処理が少なくなるため、長期運用まで視野にいれるのであれば検討する必要がある。

8. まとめと今後

本稿では、ブロックチェーンを応用した実現性の高い設計を報告し、開発電子文書の利便性、流通自由度と安全性の両立について考察を行った。文書に対する各社のニーズ

の違いから、文書管理システムの要件を分析し、それらを満たす機能を提案した。その提案の実現性を確認するために Ethereum という共通認識のあるインフラ上に試作システムの構築を行い、機能を API として利用できる設計とすることで利便性を、文書をブロックチェーン上で保存し閲覧する手法を工夫することで安全性を確認した。実験結果から試作システムには時間とコストの課題があることを確認し、考察から今後はサーバの役割を増やすことや、トランザクションの関連を追いかける手法が必要であることを示した。

参考文献

[1] 近田 昌義、他 6 名「ブロックチェーンを活用した組織間のドキュメント流通 」 日本電信電話株式会社 NTT サービスエボリューション研究所 電子情報通信学会 信学技報　LOIS2019-03

[2] 大橋 盛徳、他 5 名「トークン連動型分散ファイルシステムの提案」 日本電信電話株式会社 NTT サービスエボリューション研究所 情報処理学会第 81 回全国大会

[3] 石田 達郎、他 4 名「ブロックチェーン上で柔軟なトークン設計によって実現するコンテンツ管理手法」 日本電信電話株式会社 NTT サービスエボリューション研究所 情報処理学会第 81 回全国大会

[4] 加嵜長門、篠原航「ブロックチェーンアプリケーション開発の教科書」マイナビ出版 2018 年

[5] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System, ” http://bitcoin.org/bitcoin.pdf ,2020/5/18 アクセス

[6] W. Entriken, D. Shirley, J. Evans, and N. Sachs, “ERC-721 Non -Fungible Token Standard, ” 2018 ,https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md . 2020/4/30 アクセス