分散台帳技術による信頼できる電子メールとそれを利用した電子出版の実現に向けて

渡部 太揮[1]　新城 靖[1]　周 毅[1]　宝田 一希[1]

1. はじめに

現在，Kindle や Book Walker, Doly といった様々な電子出版プラットフォームが普及している．これらのプラットフォームの多くは特定の企業に依存した中央集権的な構造を持っている．中央サーバの管理者は出版物に対していかなる操作も可能である．これを悪用すれば，検閲や出版物の販売停止などを行うこともできる．例えば 2020 年 7 月に Amazon Kindle ストアはライトノベルと漫画を出版者に告知をせず，一方的に販売を停止した [1].

本研究の目的は，中央サーバに依存しないアプリケーション開発を支援することでこのような中央集権的な構造に起因する問題を解消することである．そのために本研究では，本研究室で開発している分散台帳技術を用いたコミュニケーションチャネル [2] を利用する．本研究ではこの仕組みに信頼できるメールの送受信機能を追加し，その上位層で動作するアプリケーションとして電子出版を実現する．**信頼できるメール**とは，1 台のコンピュータ内で送受信されるメールと同じように，送信者のアドレスや内容が改ざんされないことが保証されるメールである．この仕組みを利用するアプリケーションの開発者は，分散台帳技術の複雑なプログラミングを一切行うことなく，分散台帳技術が提供する利点を享受できる．たとえば，分散台帳技術が提供するメッセージの内容やメッセージの送信者を認証する機能を，トランザクションやディジタル署名に関するプログラミングを行うことなく利用することが可能となる．

2. 分散台帳を用いたコミュニケーションチャネルを利用した信頼できるメール

本研究室で開発している分散台帳技術を用いたコミュニケーションチャネルは層構造を持ち，一番下層に分散台帳技術である Ethereum のスマートコントラクトがイベントのブロードキャストを行う [2]．その上に 1 対 1 の通信を行うユニキャスト層と 1 対多の通信を行うマルチキャスト層が構築されている．ユニキャスト層の上位には，Web ブラウザ間通信技術である WebRTC（Web Real-Time Communication）が利用可能になっている．それを用いて Web ブラウザでビデオ通話機能が実装されている．マルチキャスト層の上位では IP アドレス管理層があり，これは VPN（Virtual Private Network）と SIP（Session Intention Protocol）で利用されている．VPN では NFS や Web，SIP では移動端末における音声・ビデオ通話のアプリケーションが動作する．本研究では，そのうちユニキャスト層を利用して信頼できるメールを実装する．

図 1　分散台帳技術による信頼できるメールの実装

信頼できるメールを実装するための層構造を**図 1** に示す．信頼できるメールは，アプリケーション開発者から見ると，1 台のコンピュータ内で閉じたローカルのメールに見える．分散台帳技術を用いて，コンピュータの間でメールを送受信する機能を分散台帳トランスポートと呼ぶ．これは本研究室で開発している分散台帳技術を用いたコミュニケーションチャネルのユニキャスト層，および IPFS（InterPlanetary File System）[3] の上に構築される．そして従来の MTA（Mail Transport Agent）に対して，コンピュータ間でのメールの転送機能を提供する．

従来のメールでは，送信側のユーザは MUA（Mail User Agent）を通じてメールを作成する．MUA は MTA にメール送信を依頼する．MTA は DNS を通じて送信相手を探索し，SMTP（Simple Mail TransferProtocol）などのプロトコルを用いてメールを送信する．受信側は MTA が受信したメールをメールボックスに保存し，ユーザは MUA を通じてメールを読む．

本研究で実装する信頼できるメールは分散台帳上のウォレットで通信相手を指定する．この時，メールを送受信する相手はローカルのコンピュータに登録し，ウォレットのアドレスと対応させる．これにより，アプリケーションの開発者はローカルのユーザを指定してメールの送受信を行

[1] 筑波大学

表 1 表の例

機能	要求メッセージ	応答メッセージ
一覧の取得	（パラメータ無し）	出版物の一覧（ID, タイトル等）
詳細の取得	出版物の ID	出版物の詳細（表紙，目次等）
購入	出版物名, 送金情報	購入の成否，出版物

えるようになる．

送信側の分散台帳トランスポートは MTA からメールを受け取ると，受信側のユーザ名からウォレットのアドレス，およびその公開鍵を得る．次に，IPFS 上にメール本文をその公開鍵で暗号化して保存する．この時，IPFS からはコンテンツに基づくアドレスが得られる．この IPFS のアドレスを，受信側のウォレットのアドレスと公開鍵を指定してユニキャスト層の機能を使って送信する．

受信側の分散台帳トランスポートはユニキャスト層の機能を使って IPFS のアドレスを受信し，IPFS からメール本文を取得し，自身の秘密鍵で復号する．分散台帳トランスポートは，送信者のウォレットのアドレスをローカルのユーザ名にマップし，MTA に渡す．MTA が受信者のメールボックスにメールを保存することでメールの受信が完了する．

3. 信頼できるメールを用いた電子出版

本研究では 2 章で述べた信頼できるメールを用いて電子出版のアプリケーションを実装する．電子出版に必要な機能は次の 3 つである．

- 出版物の登録
- カタログの配布
- 出版物の購入

本研究では電子出版をクライアントサーバモデルに基づいて実装する．購入者側でクライアント，出版者側でサーバを動作させる．クライアントとサーバ間のメッセージの送受信を信頼できるメールを用いて行う．

表 1 にクライアントとサーバの間で交わされるメッセージを示す．このメッセージは，ユーザが直接電子メールとして送受信するものではなく，電子出版アプリケーションのクライアント，およびサーバが内部的に送受信するものである．サーバ側（出版者側）では，あらかじめ出版物をコマンド等で登録しておく．表 1 の一覧の取得，および詳細の取得は，カタログの配布を実装するものである．

4. 関連研究

S.Wang らは，分散台帳技術，IPFS，および属性ベース暗号を組み合わせたデータ共有フレームワークを提案している [4]．IPFS は大きなデータを保存するために用いている．属性ベース暗号は複数のユーザにアクセスを許可するために利用している．本研究ではメールの送受信は 1 対 1 で行われるため，通常の公開鍵暗号を用いる．本研究の特徴は，アプリケーションをローカルのメールを送受信するプログラムとして開発できる点にある．

5. おわりに

本研究の目的は中央サーバに依存しないアプリケーションの開発を支援することである．そのために本研究では分散台帳技術上に信頼できるメールを実装し，そのようなアプリケーションをメールを送受信するプログラムとしてアプリケーションを実装する．

現在までに電子出版をクライアントサーバモデルに基づいたローカルのメールを送受信するアプリケーションとして実装した．今後は，分散台帳トランスポートの実装を行う．

参考文献

[1] Rafael Antonio Pienda.: “Publishers Comment on Amazon Kindle’s Delisting of at Least 15 Light Novels, Manga（Updated)”, animenewsnetwork.com, （2020-07-15）.
入手先 ⟨https://www.animenewsnetwork.com/news/2020-07-15/publishers-comment-on-amazonkindle-delisting-of-at-least-15-light-novels-manga/161872⟩. （2021-10-27）.

[2] 宝田一希, 周毅, 新城靖, 林致遠: ”ブロックチェーン技術を用いたソーシャルコミュニケーションチャネル”, 情報処理学会第 33 回コンピュータシステム・シンポジウム（2021）.

[3] J. Benet.:“IPFS – content addressed, versioned, P2P file system, CoRR 入手先 ⟨http://arxiv.org/abs/1407.3561, 2014. http://arxiv.org/abs/1407.3561⟩.

[4] S. Wang, Y. Zhang, and Y. Zhang.:“A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems,” IEEE Access, vol.6, pp. 38437-38450, 2018.