電子メールにおける送信者認証のためのEthereumを用いる電子証明書管理システムの設計

奥田 康介[1]　堀 良彰[2]　大谷 誠[3]

概要：本研究では，多種多様なメール攻撃を対策するために，メール送信者のなりすまし防止に着目した．従来の対策では，電子証明書を用いた電子メールの署名や暗号化を行う S/MIME(Secure /Multipurpose Internet Mail Extensions) と呼ばれる技術が存在するが，信頼できる認証局が発行した電子証明書が必要なため，現在普及していない．そこで，認証局がなくても電子証明書の信頼性を担保するために，Ethereum が持つブロックの改ざん困難性を活用する電子証明書の管理システムの設計に取り組む．

Design of Digital Certificate Management System for Email Sender Authentication Using Ethereum

Abstract:
In this study, focused on email senders as a countermeasure for email attacks. There is a countermeasure called S/MIME which to encryption or sign to email using to digital certificate. However, S/MIME need a trusted certificate issued by certificate authority. Therefore, it is not widespread. In this study, we designed a digital certificate management system that use Ethereum of block tampering difficulty for ensure to reliability of digital certificate.

1. はじめに

1.1 研究背景

電子メールは時間や場所関係なく相手とコミュニケーションできるツールとして，多くの人がメールアドレスを持ち，日常生活やビジネスでメールを利用している．しかし気軽にメールを送受信できることで，悪意のあるメールを受け取り，メール攻撃に巻き込まれる可能性がある．

実際にメールによる攻撃は，特定の組織や個人を対象として，悪意のあるファイルへ誘導する URL を添付して，マルウェアをダウンロードさせる標的型メール攻撃 [1] や正規なサービス提供者になりすまし，個人の情報を搾取するフィッシングメール [2] など攻撃対象や目的などが多種多様になり，業種に関わらず相対している．そのため，2011 年から 2020 年にかけて IPA(情報処理機構) の 10 大脅威として恐れられている [3]．また特に最近では，新型コロナウイルスの出現により，感染防止のため企業や学校ではテレワーク環境の導入を強いられている．その結果，自宅の無防備なインターネット環境や外部の無料 Wi-Fi を利用する人々が増えているため，フィッシングメールやマスクの提供，感染症などの新型コロナウイルスを題材としたスパムメールなどが世界中に広まっている．標的型メール攻撃による件数は，警察庁の調査 [4] では，図 1 のように 2020 年上半期で 3978 件発生して，2019 年上半期と比較して約 1.5 倍増加している．

そのため，悪意のあるメール攻撃から資産を守るために，メール攻撃に対してより一層対策する必要がある．そこで本研究では, 既存のメール攻撃の対策を調査して，電子証明書による対策に着目した．この対策は，電子証明書で自身の正当性を示すことができるが，信頼できる電子証明書が普及していない問題がある．そこで，電子証明書の普及させるため，電子証明書の信頼性を担保するための手法として，Ethereum を導入する電子証明書の管理システムを考案した．

[1] 佐賀大学大学院 理工学研究科,
Graduate School of Science and Engineering, Saga University
[2] 佐賀大学 全学教育機構,
Organization for General Education, Saga University
[3] 佐賀大学 総合情報基盤センター,
Computer and Network Center, Saga University

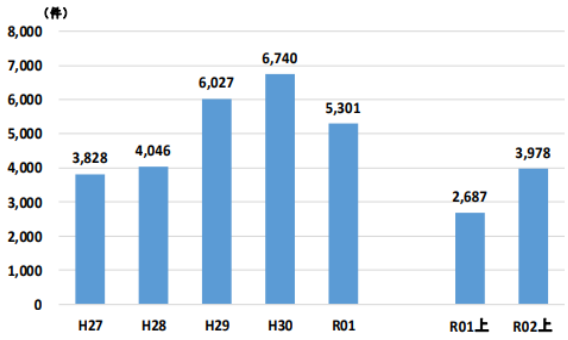

図 1　標的型メール攻撃の件数

1.2　研究目的

本研究では，標的型メール攻撃などのメール攻撃を迅速に発見して被害を抑えるため，メールに署名や暗号化を行い，なりすましなどの悪意のあるメールを発見することに焦点を当てた．しかし，従来の電子証明書を用いてメールへ署名や暗号化を行う場合，電子証明書の信頼性を確保するため，信頼できる認証局や電子証明書の発行費用，管理などが必要である．そこで，認証局を必要としない自己署名証明書を活用する．しかし，自己署名証明書では，電子証明書の信頼性を担保できない．

そのため本研究では，電子証明書の信頼性を担保する仕組みとして，Ethereum のブロック改ざん困難に着目した．ブロック改ざん困難とは，ブロックチェーンは複数のブロックが連結したものであり，ブロックの生成には直前のブロックの情報が関わっている．そのため，ブロックの改ざんには連結したブロックも改ざんする必要がある．そこで，改ざんが困難なブロックチェーンに電子証明書を登録することで，信頼性を担保する方法を提案した．

1.3　論文構成

第 1 章では，本研究の背景と目的について述べる．第 2 章では，研究背景で述べたメール攻撃に対しての従来の対策を紹介する．第 3 章では，本研究で提案するシステムの構成や特徴について説明する．また第 4 章で，設計した本システムの動作について解説を行う．最後に第 5 章で本研究のまとめや課題について説明する．

2.　従来のメール攻撃対策

2.1　既存の技術

2.1.1　S/MIME

S/MIME とは，信頼できる第 3 者の認証局から発行される電子証明書を用いて，メールの署名や暗号化を行うメール攻撃の技術的対策の 1 種である [5]．S/MIME を活用することで，メールの改ざんや盗聴，なりすましを防ぐことができる．しかし，個人での導入が可能であるが，電子証明書の信頼性を確保するためには，認証局から発行する必要があり，電子証明書の発行費用や更新などの手間がかかる．そのため，現在普及していない．

2.1.2　PGP

PGP（Pretty Good Privacy）は，S/MIME とは違い，認証局から発行された電子証明書を使用しない．事前に電子証明書を当事者間で交換することで，お互いの電子証明書を用いて，メールの署名や暗号化を行うメール攻撃の技術的対策の 1 種である [6]．しかし，認証局から発行されていないため，電子証明書には信頼性がなく，なりすましが発生する可能性がある．

2.1.3　訓練メール

訓練メールとは，前述した S/MIME や PGP とは違い，メール攻撃に対して事前に教育して，メール受信者のメール攻撃への対応力を向上させる人的対策の 1 つである [7]．実際に組織などを対象に疑似標的型メール攻撃を行い，組織の社員が不審な添付ファイルを開いていないかを調査する．また訓練メールを実施することで，不審メールに対する組織全体の対応力を高めることができると考えられる．しかし，訓練メールを実施しても組織の 1 割が標的型メール攻撃の被害を受け，機密情報などが漏えいする恐れが考えられる．

2.2　先行研究

2.2.1　安全・安心電子メール利用基盤（SSMAX）

SSMAX（Secure and Safe E-mail Exchange Framework）とは，図 2 の構成でお互いのメール送受信者がそれぞれの組織に属することで，組織メールサーバが組織の電子証明書を使用して，メールへ署名や暗号化を行う．そのため，メールの送受信者はお互いの電子証明書を保持しなくてもよい先行研究である [8]．しかし，個人でのセキュリティ対策には不向きであり，組織メールサーバが電子証明書を管理しているため，障害が発生した場合，メールへの署名や暗号化を行うことができないと考えられる．

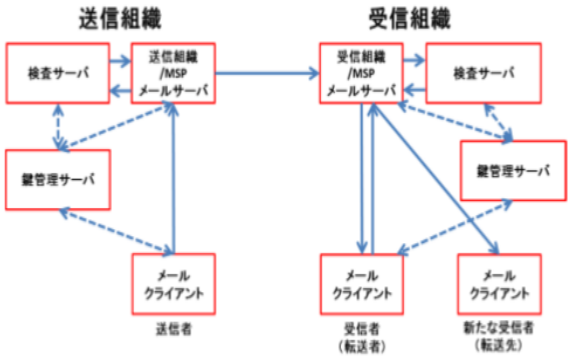

図 2　SSMAX の構成

2.2.2 Blockchain and Smart Contract for Digital Certificate

Ethereum を用いたオンラインで卒業証明書を取得するシステムで，大学の卒業証明書などの証明書を Ethereum 上に登録することで，大学に問い合わせることなく，オンライン上から証明書を入手できる仕組みである [9]．しかし，この先行研究では Ethereum に登録する証明書は卒業証明書など永続的なもので，登録し続けても問題ない．それに対して，更新が必要な電子証明書を用いる本研究では，電子証明書の更新動作が必要になる．

3. システムの概要

電子証明書の信頼性を認証局が行い，先行研究の SSMAX と Ethereum を用いたオンラインでの証明書取得システムを参考にして，電子証明書の信頼性を Ethereum で担保する図 3 のようなシステムを設計した．

次に，本システムを構成する 5 つの要素を解説する．

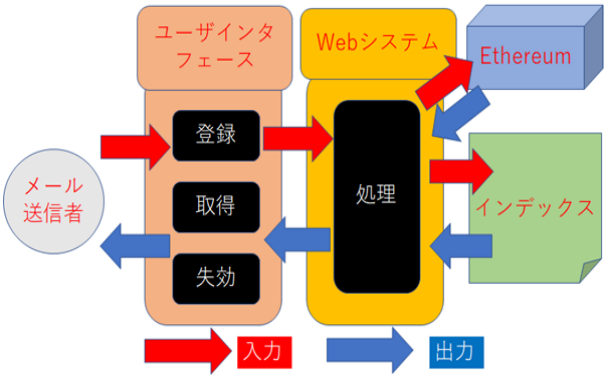

図 3　システムの設計

3.1 メール送信者

メール送信者は，自身で電子証明書を発行した自己署名証明書を用いて，本研究の電子証明書管理システムを動かして，電子証明書の登録や取得を行う人．

3.2 ユーザインタフェース

ユーザインタフェースでは，メール送信者が自身の電子証明書を登録する，相手の電子証明書を取得する，自身の電子証明書の失効するなどの動作を行い，Web システムにその入力情報を送信するものである．

3.3 Web システム

Web システムでは，ユーザインタフェースから電子証明書やメールアドレスの情報を受け取る．その後，Web システムが Ethereum に電子証明書を登録や取得，失効などの動作を行い，またインデックスに追記を行う．

3.4 Ethereum

Ethereum とは，分散されたアプリケーション開発やスマートコントラクトのアプリケーション構築を可能にする，グローバルに非中央集権化されたオープンソースの演算の基盤である．本研究では，Web システムから受け取ったメールアドレスや電子証明書を Ethereum に登録するスマートコントラクトを動作させている．

3.5 インデックス

インデックスとは，実行したトランザクションとメールアドレスを対応付けて記録するテキストファイルである．本システムでは，電子証明書に登録しているがどのブロックに登録されているか特定できない．そのため，Ethereum に登録した際に発生したトランザクションを用いることで，登録されたブロックを特定できる．

4. システムの設計

4.1 電子証明書の登録

Ethereum に自身の電子証明書を登録する動作である．また Web システムからでしか登録できないようにして，悪意のある利用者に誤った電子証明書を登録されないように，パスワードを使用した認証を行う．動作の流れは以下の手順である（図 4）．

1）利用者は，電子証明書をユーザインタフェースに入力して，Web システムに送信する．

2）Web システムは電子証明書からメールアドレスを取得して，そのメールアドレスにランダムに生成したパスワードを添付して送信する．

3）そのパスワードを利用者が入力することでパスワードによる認証を行い，認証が成功した場合のみ Ethereum に電子証明書とメールアドレスを登録する．

4）登録したメールアドレスと電子証明書を登録した際に，Ethereum で発生したトランザクションをインデックスに追記する．

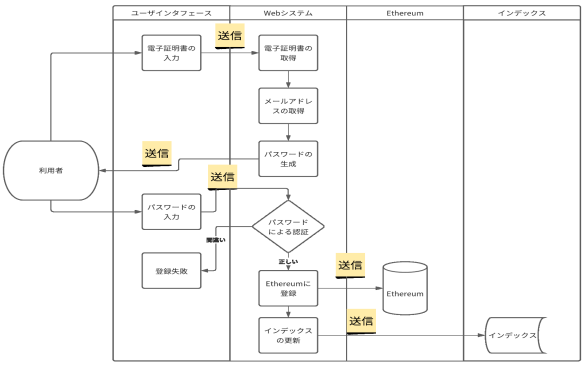

図 4　電子証明書の登録の流れ

4.2 電子証明書の取得

Ethereum にある電子証明書を取得する動作である．取得にはユーザインタフェースに相手のメールアドレスを入力する．動作の流れは以下の手順である（図 5）．

1）利用者は，ユーザインタフェースに取得したい電子証明書のメールアドレスを入力して，Web システムに送信する．

2）Web システムは，メールアドレスに対応したトランザクションをインデックスから取得する．

3）取得したトランザクションから取得したい電子証明書を特定して取得する．

4）取得した電子証明書は符号化されているため，Ethereum-input-data-decoder[10] で復号を行い，その結果をユーザインタフェースに表示させる．

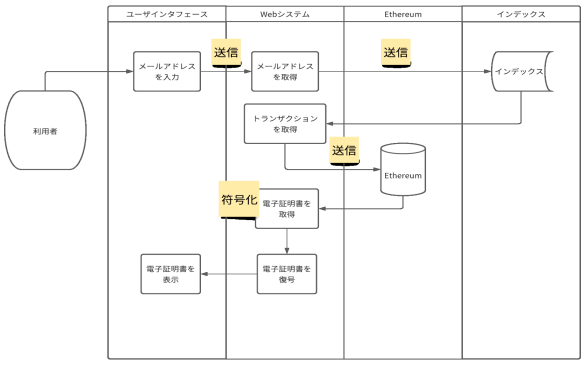

図 5 電子証明書の取得の流れ

4.3 電子証明書の失効

使用していない電子証明書を失効する動作である．電子証明書は永続的なものではなく，使用していない，また有効期限が切れることが考えられる．しかし，Ethereum に登録することで，現在使用できない電子証明書も参照される．そこで，新規に電子証明書が空白のブロックを生成して，Ethereum に登録する．取得する際に新しいブロックを参照することで，失効された電子証明書を参照できなくする．失効の手順については，以下の手順である（図 6）．

1）利用者は，ユーザインタフェースにメールアドレスを入力して，Web システムに送信する．

2）Web システムはランダムなパスワードを生成して，そのメールアドレスに添付して送信する．

3）電子証明書を登録する動作と同様にパスワードによる認証を行い，認証が成功した場合，電子証明書が空白のものを Ethereum に登録する．

4）電子証明書を取得する際に，電子証明書が空白であれば，失効していると Web システムが判断する．

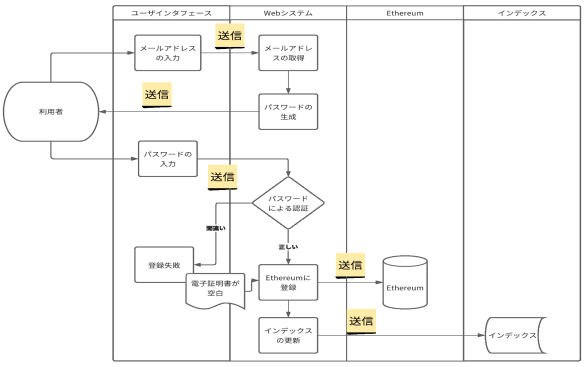

図 6 電子証明書の失効の流れ

5. おわりに

5.1 まとめ

本研究では，電子証明書の信頼性の担保するため，Ethereum を活用する電子証明書の管理システムを設計した．そこで，実際にユーザインタフェース，Web システム，Ethereum，インデックスを構築して，システムの動作を確認した．その結果，ユーザインタフェースに入力した電子証明書やメールアドレスを Web システムに送信して，Web システムを通じて Ethereum に接続を行い，電子証明書の登録，インデックスを利用して電子証明書の取得や失効などの動作検証ができた．

5.2 今後の課題

本研究のシステムでは，Web システムを通じて Ethereum に電子証明書を登録や取得などの動作を行う．そのため，Web システムに障害が発生した場合に，先行研究の SSMAX 同様に電子証明書の取得，暗号化ができなくなることが考えられる．そこで，システムの対故障性を向上させるため，Web システムを複数導入して，動作検証を行う必要がある．

また本研究では，動作検証に使用したブロック数は 10 数個の状態で実装を行った．しかし，利用者が増加することで Ethereum に登録するブロック数も増加するため，本システムを実装する際，利用者数が数百数千になる場合が考えられる．その場合での電子証明書を Ethereum に登録，取得の動作について影響がでるのか本システムの拡張性を検証するため，確認する必要がある．

参考文献

[1] サイバーセキュリティ.com: 標的型メール攻撃とは？その特徴と対策を徹底解説 (online)，入手先 ⟨https://cybersecurity-jp.com/security-measures/18646⟩ (2021.02.11).

[2] サイバーセキュリティ.com: フィッシング詐欺メールとは？方法や種類、効果的な対策について徹底解説 (online)，入手先 ⟨https://cybersecurity-jp.com/column/29673⟩ (2021.02.11).

[3] IPA: ”情報セキュリティ 10 大脅威” 14 年のランキン

グ分析 ～サイバーセキュリティ脅威の変遷～ (online), 入手先 ⟨https://www.ipa.go.jp/files/000074098.pdf⟩ (2021.02.11).
[4] 警察庁: 令和 2 年上半期におけるサイバー空間をめぐる脅威の情勢等について, 警察庁広報資料 , 入手先 ⟨http://www.npa.go.jp/publications/statistics/cybersecurity/data/R02_kami_cyber_jousei.pdf⟩, (2020)
[5] B. Ramsdell, Ed.: S/MIME Version 3 Certificate Handling, RFC2632 (1999)
[6] D. Atkins, W. Stallings, P. Zimmermann: PGP Message Exchange Formats, RFC1991 (1996)
[7] アクモス株式会社: 第 2 回標的型攻撃メールはどう防ぐ？-標的型攻撃メール訓練ソリューションのご紹介 - (online), 入手先 ⟨https://www.acmos.co.jp/blog/detail8.html⟩ (2021.02.11).
[8] 才所敏明, 五太子政史, 辻井重男: 「安全・安心電子メール利用基盤（SSMAX）」悪意のあるメールの根絶とメール内容の確実な保護を目指して, 情報処理学会論文誌, Vol. 59, No.9, pp. 1545-1556 (2018).
[9] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen: Blockchain and Smart Contract for Digital Certificate, Proceedings of the 2018 IEEE International Conference on Applied System Innovation (ICASI), pp.1046-1051 (2018).
[10] Miguel Mota: ETHEREUM INPUT DATA DECODER (online), 入手先 ⟨https://github.com/miguelmota/ethereum-input-data-decoder⟩ (2021.02.11).