ISS-P-038

ブロックチェーンを用いたPGP公開鍵の配布モデル

佐藤　直己† 　広奥　暢† 　中島　潤†
†北海道情報大学大学院　経営情報学研究科

1. はじめに

電子メールで使用されている暗号化技術には，S/MIME や Pretty Good Privacy[1]（以下，PGP）がある．S/MIMEとPGPの違いは，公開鍵の取り扱いや適用範囲である．S/MIME は公開鍵の正当性を認証局が証明するため不特定多数に適している．一方，PGP では認証局を設置しないため，誰でも鍵情報を登録でき，小規模なコミュニティに適している．しかし事前にフィンガープリントを二者間で共有しなければならず，公開鍵の正当性は各利用者の責任で信頼する必要がある． そこで，インターネット上から誰でも鍵の登録，検索や取得ができるように有志が運営する鍵サーバが複数あり，公開鍵の交換を円滑にしている．しかし大規模に運営するとなった場合，以下の課題もある．1. 登録するメールアドレスは本人が所有しているか確認していないため，悪意ある利用者が他人のメールアドレスを登録し，なりすますことができる．2. セキュリティ不足や悪意ある鍵サーバ管理者などによって，鍵サーバ内の鍵情報を改竄される可能性がある．これらの課題を解決する一つの方法として，Google 社が開発した E2Email[2]があるが，Gmail の利用者のみに限られた適用範囲となる．本研究では，セキュリティや利便性を向上させ，課題の解決とPGPの適用範囲を広げることを目的とし，PGP公開鍵配布モデルを提案する．

2. ブロックチェーンを用いたPGP公開鍵の配布モデルの提案

ブロックチェーン技術を用いることによって，中央集権的な管理機構を持たず，ネットワーク上に分散している各ノードが検証した正当な情報を保持することができる．ブロックチェーン上に鍵情報を登録することで，ブロックチェーンの特徴により，鍵情報は，ネットワーク上に繋がっている鍵サーバ同士で共有することができ，鍵情報の改竄が極めて困難で，セキュリティ，利便性や耐久性の向上が期待される．また，PGP の Web of trust 理念とブロックチェーン信頼性の仕組みは近似しており，技術的観点から親和性があると考える．上節の課題を解決するため，以下の手順で公開鍵を登録する．

1. ユーザが鍵サーバ上に公開鍵を登録する際には，GPG で使用されているフォーマット形式に従い，ASCII Armor 化された公開鍵情報（Public Key，User ID，Signature を含んだデータ構造，以下 AA 鍵）を鍵サーバに送信する．
2. 受信した鍵サーバは，AA 鍵からメールアドレスを取り出し，ランダムな文字列の確認用トークンを含んだ URL リンク付きメールを返信する．
3. 有効なメールアドレスと確認されたのち，AA 鍵をブロックチェーン上に登録し反映する．

この手順により，登録する公開鍵のメールアドレスの有効性を確認でき，鍵情報の改竄を防止できる．また，クライアントでは，どの鍵サーバからでも公開鍵の検索や取得ができるようになる．

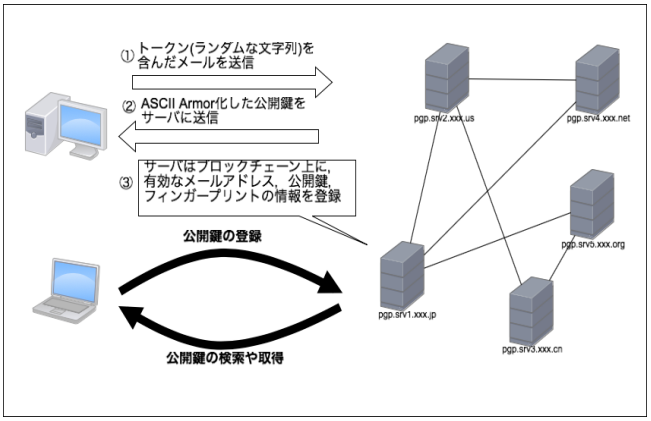

図1. 公開鍵の配布モデルフロー

3. まとめ

本研究では，メールアドレスの正当性や PGP 公開鍵サーバの課題を解決するため，ブロックチェーン技術を用いた公開鍵配布モデルを提案した．ブロックチェーン技術と組み合わせることで，鍵サーバは鍵情報を分散管理ができ改竄が困難となり，セキュリティや耐久性が向上し有意であると考えている。また，ファイルやメールの暗号化をはじめ，応用として他技術と組み合わせ失効期限を設けるなどして，二次利用の防止などの応用[3]が期待できる．本研究で提案した配布モデルによって，PGP の適用範囲が広がり，より普及する可能性があると考える．最後に試作環境を通した評価・検証について，当日ポスターで発表する．

参考文献

[1] Philip R. Zimmermann, ”PGP: Source Code and Internals”, The MIT Press, 1995

[2] Google, “E2EMail is a simple Chrome application – a Gmail client that exchanges OpenPGP mail.”, https://github.com/e2email-org/e2email, 参照 Feb. 8,2018.

[3] Hitachi Solutions, “Data Leakage Prevention Solution HIBUN”, http://www.hitachi-solutions.com/hibun/sp/, 参照 Feb. 8,2018.