1F-5　　証明書によるメール送信者確認方法に関する研究

本郷 鉄兵，上原 稔
東洋大学工学部情報工学科

1　はじめに

近年，電子メールにおいて，セキュリティの問題が数多く発生している [1]．問題の原因の１つとして，不正なメールが送信された場合に，現在広く使われているメール送信方法では，ユーザの認証を行なわないために，その送信者を特定することが難しいということがあげられる．

わたしたちは，安全な電子メール環境の構築のためには，このような問題を解決する必要があると考え，ユーザ認証を行なう Web メールシステムの開発を行なってきた [2]．これは WWW 環境から利用する MUA で，メール受信サーバを使って，ユーザ名とパスワードによる認証を行なう機能を持っている．このシステムを使ってメールを出すには必ず認証が必要となるため，メールサーバのあるネットワーク内においては成り済ましができなくなる．

しかし，この認証だけでは，大学の研究室や企業のイントラネットのような隔絶されたネットワークにおいては有効でも，インターネットに接続されたネットワークにおいては，外部からの成り済ましを防ぐには不十分である．そこで，わたしたちは，送信者情報を含んだ証明書をメールに添付し，受信者がこれを送信元 Web メールシステムに問い合わせることで，送信者の確認をすることができるシステムを構築することを考えた．証明書は暗号化されてメールに添付され，送信元 Web メールシステムでしか復号化できない．この仕組みによって，Web メールシステムがメール送信者を特定でき，またメールの受信者が送信者を確認できるようになると考える．

2　関連研究

本研究に関連して，送信者認証方法である SMTP AUTH と，暗号化メッセージや電子署名などに関する規格である S/MIME について述べる．

"Mail sender confirmation by the certificate",
Teppei HONGOU, Department of Information and Computer Sciences,Toyo University

2.1　SMTP AUTH

SMTP に認証機能を付け加えるものとして，"SMTP Service Extension for Authentication"[3] が提唱されている．これは，SMTP で認証をするために AUTH コマンドを拡張，定義するものである．SMTP AUTH は将来的には有望であるが，現時点ではまだ一部のクライアントでしか対応がなされていないため，導入コストの点で問題があると考える．

2.2　S/MIME

S/MIME[4] は，電子メールに暗号化や電子署名などを付加するための規格である．S/MIME を利用して電子署名を付加する場合には，認証機関から証明書を入手する必要がある．現時点では，対応しているクライアントが限られていることもあり，導入コストの点で問題があると考える．

3　システム概要

本システムは，送信前のメールに自動的に証明書が添付するものである．また，メッセージの受信者は証明書をシステム側に問い合わせることで送信者を知ることができる (Fig.1)．

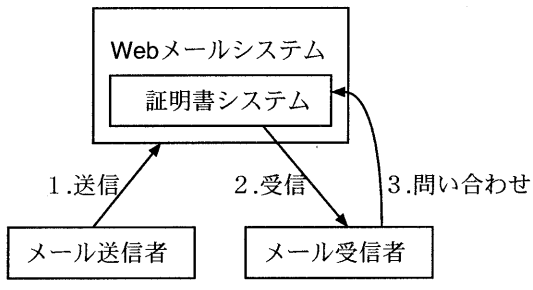

Fig. 1. 送信者証明

この証明書には，以下のような内容が含まれている．

MAIL-ID　システムがメールに付ける ID で，一意な番号である．

USER-ID メールの送信者に一意につけられた番号である.

CLIENT-ID メールが出されたサーバに一意につけられた番号である.

MD5SUM 送信メッセージから生成した, MD 5 メッセージダイジェスト [5] である.

これらの内容が, システム内にある固有に持つ鍵で暗号化され, メッセージに添付される. 受信者はこの証明書と送信者の情報を Web メール CGI に送信し, 問い合わせる.

Web メールシステムはこの証明書による問い合わせがあった場合, 同様の鍵で証明書を復号化し, 同様の内容が記録されているログと照合する. 照合に成功したら, その証明書が Web メール CGI によるものであることを応答する. そして, 受信者が受け取ったメッセージのチェックサムとを照合することで, 内容の改竄のチェックを行うことができる.

4 実装

本システムは, Web メールシステム (Fig.2) に統合された形で実装されている. 証明書は Web メールシステムの CGI が自動作成して, メールに添付する.

この Web メールシステムでは, メール送信時に認証を行われ, その際に入力されたユーザ名からあらかじめ用意されたデータファイルから USER-ID を取得する. また同様に CLIENT-ID を取得する. MAIL-ID と MD5SUM は, 送信される本文が入力され, メール送信操作を行う前段階で自動的に作成する. これらの内容をファイルに書き込み, 暗号化を施したものを送信する際に添付する. 暗号化には PGP を利用する.

受信者がメールの送信者を確認するためには, 証明書を Web メールシステムにアップロードする必要がある. Web メールシステムで受信した場合には, 確認のための動作が自動的に行われ, メールの送信者を確認することができる. 通常のメールクライアントで受信した場合には, 添付された証明書を一度ローカル環境に保存し, Web メールシステムに用意された Web ページを利用してアップロードすることで確認することができる.

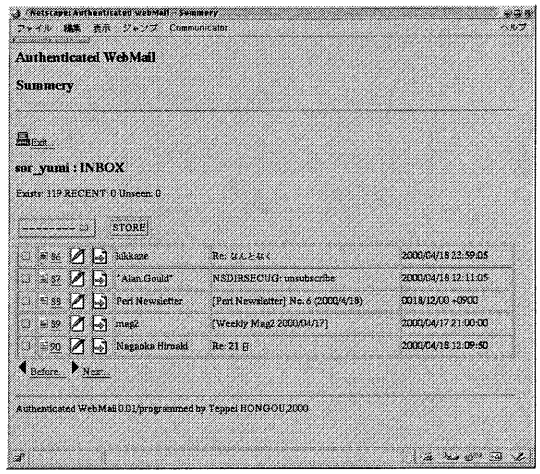

Fig. 2. Web メールシステム

5 まとめ

本論文では, メール送信者を確認する手段としての証明書システムと, Web メールシステムにおける実装について述べた. 本システムを利用することで, 安全性の高い電子メール環境を構築することができることを提案した.

6 今後の課題

今後の課題として, 以下の点が挙げられる.

- SMTP AUTH や S/MIME などの標準化技術への対応.
- 証明書の暗号化方式の検討.
- メッセージ本文の暗号化と, それに伴う公開鍵保存用サーバの開発.

参考文献

[1] 上原 稔, 松元 明弘, 森 秀樹,"キャンパスネットワークにおける高信頼アカウント", 情報科学論集, No. 30, pp.87-96, 東洋大学情報センター, 1999.

[2] 本郷 鉄兵, 上原 稔, "認証 Web メールの開発", 情報処理学会第 59 回全国大会, 1999

[3] J. Myers,"SMTP Service Extension for Authentication",RFC 2554,March 1999

[4] S. Dusse 他, "S/MIME Version 2 Message Specification",RFC 2311,March 1998

[5] R. Rivest,"The MD5 Message-Digest Algorithm",RFC 1321,April 1992