5Q-07

暗号化メール自動診断機構の設計と実装

村瀬晋二*　若山公威**　鈴木春洋*　岩田彰**

*（株）シーティーアイ　SI 事業部

**名古屋工業大学　電気情報工学科

1. はじめに

近年，インターネットやエクストラネット上での電子メールのやり取りを安全に行うため，公開鍵暗号方式によるメッセージの暗号化や電子署名が利用されている。

平成 11 年 4 月より，S/MIME を用いた暗号化メールサービスをエクストラネット上で開始したが，平文メールの運用とは異なり，さまざまな運用上の問題が発生している。このため，暗号化メールの利用者が増加しないのが現状である。

暗号化メールが広く一般ユーザに普及するためには，解決すべきいくつかの問題がある。問題の一つに，メールクライアントの設定が一般ユーザにはまだまだ複雑であり，かつ設定確認が容易ではない点が挙げられる。

そこで，本研究では暗号化メールの利用促進を目的とし，S/MIME を用いた暗号化メール自動診断機能の設計を行い実装した。

2. 暗号化メールの運用上の問題点と解決方法

暗号化メールの運用における問題点はさまざまあるが，実際の利用者からの問い合わせは例えば以下のような内容である。

Case 1:「電子署名が無効であると表示されるがどういうことか」

Case 2:「添付ファイルを暗号化メールで送ると送信先がファイルを開けない場合がある」

Case 3:「暗号化＋電子署名メールは使えるが電子署名メールが使えない」

Case 1 の場合，実際に電子署名が無効である場合もあるが，暗号化メールクライアントの設定不備が原因である場合がある。設定不備が原因である場合は設定マニュアルを参照して設定が正しいかどうかチェックしてもらうが，設定不備箇所が発見できない場合もあった。最終的に解決できない問題を切り分けるために，電子署名付きのメールを運用担当者へ送付してもらう方法を採った。運用管理者はメールの生データを技術担当者に渡し，技術担当者がメールの内容を AiCrypto[1]または OpenSSL[2](SSLeay[3])を用いて ASN.1 パースして解析することで原因を突き止めた。

Case 2 の場合は，ある特定の暗号化クライアントから送信するメールに限り，添付ファイル名が 30 文字以上になると添付メールが正常に送付できないのが原因であった。

原因がメールサーバ側にある場合が Case 3 である。エクストラネット上で暗号化メールを送受信する時，各社のメールサーバ(MTA)が異なる可能性がある。ある MTA の古いバージョンが電子署名を削除してしまうのが原因であった。

Case 2 はクライアントの仕様であり問題の切り分けは容易である。また，Case 3 は正常に動作する環境を構築すれば，構築後はトラブルが発生しにくい。ただし，Case 1 のようにクライアント側で設定変更できてしまう場合は，ユーザが誤って設定を変えてしまうことが考えられ，実際に何度も発生した。

Case 1 の対応にはすべて人手を介しているため問題解決に要するコストおよび時間がかかるのが問題である。本研究ではこの問題を解決するため，自動で暗号化メールクライアントの設定内容を診断するためのサーバを開発した。

3. S/MIME

S/MIME は現在多く利用されている S/MIME version2[4]を対象とした。

S/MIME v2 は PKCS #7[5]を S/MIME として扱う方式であるが，仕様上はかなり柔軟性を持たせてあり，互換性に関しては暗号化メールクライアント開発元の実装によってかなり左右される可能性がある。

RFC2311 には受信時には多くのフォーマットに対応するべきであり，送信時には一般的なフォーマットで出力すべきであると明記してある。

しかし，暗号化メールクライアントの実装次第で，一般的なフォーマットで送信されるかどうかは変わってしまうため，現状では暗号化メールク

Implementation of Auto Check Server for S/MIME
Shinji MURASE*, Kimitake WAKAYAMA**, Shunyo SUZUKI*, Akira IWATA**
*CTI Co., Ltd.
**Nagoya Institute of Technology

ライアントに依存している。例えば Internet Explorer5 付属の Outlook Express5 は暗号化メールクライアントの送信設定を変更可能なため，送信相手に適したメールを送信することが可能である。その反面，一般ユーザが誤って設定変更してしまった場合，S/MIME メールが正常に送受信できなくなり，原因の発見が困難になることが考えられる。実際，ユーザ向け設定マニュアルも一通り揃えたが，基本設定以外の項目に関しては注意深く設定を見比べないと，設定誤りを検出するのが困難であった。そこで，設定誤りを検出する補助的役割を担う暗号化メール診断サーバが必要となった。

4 システム概要

暗号化メール診断サーバを用いた場合のメールの流れを図 1 に示す。

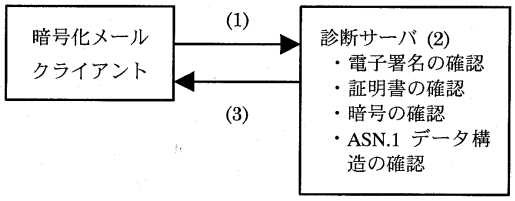

図 1 メールの流れ

また，システムの流れは以下の通りである。

(1)ユーザは暗号化メール診断サーバのメールアドレスへ S/MIME メールを送信する。
(2)暗号化メール診断サーバは電子署名または暗号化部分を切り出し，診断を行う。
Case 1: 電子署名のみ
(application/x-pkcs7-signature)
(a)電子署名の抽出
(b)電子署名の復号化
(c)電子署名の確認
Case 2: 電子署名＋暗号化
(application/x-pkcs7-mime)
(a)共通鍵，本文の抽出
(b)共通鍵の復号化
(c)本文の復号化
(d)電子署名の抽出～確認(Case 1 と同じ)
Case 3: 平文，その他
(a)診断なし
(3)暗号化メール診断サーバは診断結果をまとめ，ユーザへ返送する。

5 実装

AiCrypto1.1+gcc2.8.1 を用いて Solaris2.5.1 上で開発を行った。

RSA 暗号処理, DES などのブロック暗号処理, SHA-1 などのハッシュ関数，証明書，CRL，PKCS#12 のハンドリング等は AiCrypto に実装済みであるためそのまま利用した。

PKCS#7 のハンドリングに関しては，AiCrypto には基本的な機能しかないため，必要な機能を実装した。また，S/MIME 処理を行うために必要な MIME の正規化機能を実装した。

暗号化メールメールクライアントには Internet Explorer5 付属の Outlook Express5 と Netscape Communicator4.5 付属の Netscape Messenger を使用し，本システムで暗号化メールの自動診断が行えることを確認した。

6 おわりに

サーバ側で暗号化メールクライアントの設定内容を診断する方式を提案し，S/MIME メールにおける暗号化メール診断サーバを設計，実装した。本方式は S/MIME メールのみでなく，PGP などの他の暗号化メールにも適用可能である。また，証明書の有効性確認プロトコル(OCSP[6])のメール版として利用することも可能である。

今後は S/MIME version3[7]への対応を検討する予定である。

参考文献

[1] 若山 公威, 奥野 琢人, 岩田 彰, 村瀬 晋二, 鈴木 春洋: "暗号ライブラリと認証局パッケージの開発", 第 59 回情報処理学会全国大会, 1999.
[2] http://www.openssl.org/
[3] http://www.ssleay.org/ssleay/
[4] S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade, L. Repka: "S/MIME Version 2 Message Specification", RFC2311, 1998.
[5] B. Kaliski: "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC2315, 1998.
[6] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC2560, 1999.
[7] B. Ramsdell: "S/MIME Version 3 Message Specification", RFC2633, 1999.