電子メールにおける暗号化支援ツールの作成

東京工科大学　工学部　情報通信工学科
坪川研究室 00D096 古久保 慎剛

1　背景・目的

電子メールは、個人の日常生活やビジネスシーンでの連絡手段として広く利用されている。その一方で、送信過程において盗聴、改竄などを容易にされてしまうといった危険性も持ち合わせている。その対策として暗号化技術が使われているが、現在のメール暗号化ソフトでは、自分の好きなメールをつかえず、使い勝手が良くないことや、暗号化のための操作手順が複雑でわからないなどの問題もありなかなか普及しないのが現状である。

そこで本研究では、それらの問題の解決策として、メーラとサーバーを仲介し、鍵の管理、暗号化・復号化の作業を自動で行う仲介ソフトを作成する。これにより、ユーザがメーラなどの環境をかえることなく、手軽に暗号化メールを利用ですることができる。

2　暗号化支援ツール

2.1　ツールの概要

本研究で作成したツールは、クライアントマシンに常駐し、メーラとサーバの仲介を行う。メーラは、仲介ツールと接続し、メールの送受信を行う。仲介ツールは、メーラから接続を受けるとサーバと接続し、メーラの代理として送受信を行う。送受信の際に、暗号化、復号化、鍵の作成・付加などの処理を行った上でメールを中継する。全体のイメージを図１に示す。

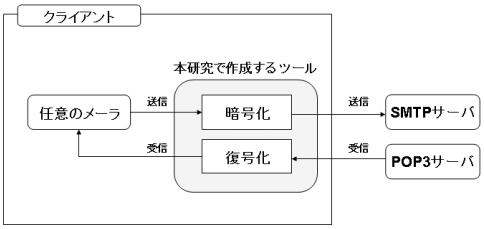

図 1: 全体の流れ

2.2　送受信の流れ

仲介ツールの送受信の流れを図２に示す。送信時、仲介ツールはメーラから受け取ったコマンドから、送信者と受信者のメールアドレスを取得する。送信者アドレスから自分の公開鍵を検索し、鍵をメールヘッダに付加する。もし鍵がない場合は作成後に付加する。受信者のアドレスからは、対応する公開鍵を検索し鍵が見つかれば、暗号化し暗号化処理済みという情報を付加した後にサーバに送信する。もし鍵が見つからない場合はそのままサーバに送信する。

受信時、サーバから受け取ったでータから、メールヘッダを解析し送信者と受信者のメールアドレスと送信者の鍵情報、暗号化処理情報を取得する。もし鍵情報が見つかれば、送信者メールアドレスをファイル名としてローカルに保存する。次に暗号化処理情報から暗号化の有無を判断し、暗号化されていれば、受信者の秘密鍵を使用して復号化を行った後にメーラに送信する。もし暗号化されていないならそのままメーラに送信する。

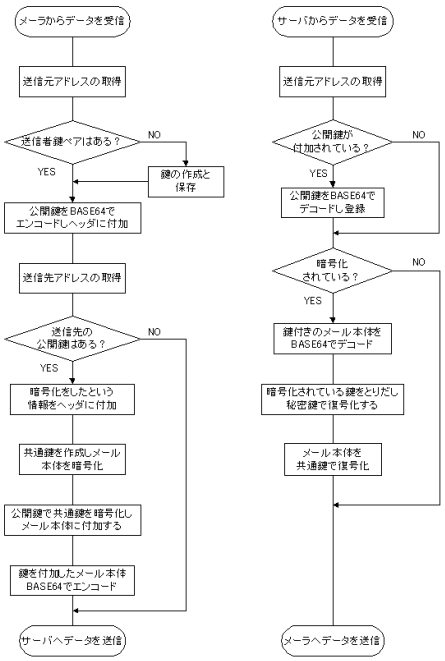

図 2: 送受信の流れ

2.3　暗号化手法

本研究では、公開鍵暗号方式と共通鍵暗号方式の２つの方式を併用する形で暗号化を実装する。データを受け取った仲介ツールは、RC4 共通鍵を作成し本文を暗号化する。次に本文を暗号化した共通鍵を、送信先の RSA 公開鍵で暗号化する。暗号化された共通鍵を本文の先頭につけてサーバへ送信する。受信側は、共通鍵を本文の先頭から取り出し自分の秘密鍵で復号化した後に取り出した鍵で本文を復号化し、メーラに渡す。

公開鍵の配送は、仲介ツールがメール送信時に、毎回鍵情報をヘッダに付加して送信することによって実装される。鍵は受信側の仲介ツールによって保存され、次回送信時からは、暗号化処理が実行されることになる。

3　まとめ

本ツールを利用して、OutlookEcpress、Outlook2000、EUDORA、AL-MAIL32、Becky!などのメーラで送受信実験を行った結果、実験を行ったすべてのメーラにおいて正常に送受信を行うことができた。また、仲介ツールとサーバ間で送受信された情報を監視したところ、正常に暗号・復号化処理が行われていた。

また、メールのウィルスチェックツールなどとの衝突の確認を行ったところ、暗号化送受信はできるものの、ウィルスチェック機能は有効に働かなくなる結果になった。今後このような問題点を解決することによりより機能的なツールになると考える。