マルチメディア通信と分散処理　97－21
コンピュータセキュリティ　8－21
（2000．3．22）

IPv6対応電子メール自動暗号化処理サーバの試作（2）

伊藤昌彦† 永江由紀子† 畑中雅彦† 田島和典†† 青木貴††
† 室蘭工業大学
††ニッテツ北海道制御システム（株）

現在、多数の暗号化電子メール・パッケージが公開され、製品化されている。しかし、暗号化鍵の管理・更新作業等において、利用者に複雑で面倒な操作を強いる場合が多い。我々は、組織間のビジネスメールを対象に、電子メールの自動暗号化／復号化処理を行うプロキシ・サーバ（Crypt-Mail Secretary：CMS）の研究・開発を行っている。

本報告では、既に報告済みの CMS 基本システムの機能拡張として、次世代インターネット・プロトコルである IPv6 へも対応可能とさせるとともに、セキュリティ強化を目的に複数の暗号化方式への対応も可能としたので、その結果について報告する。

A Trial Construction of Automatic Cryptograph Server for Mail Based on IPv6 (2)

Masahiko ITO†, Yukiko NAGAE†, Masahiko HATANAKA†
Yasunori TAJIMA††, Takashi AOKI†
†Muroran Institute of Technology
Nittetsu Hokkaido Control System Co., Ltd

There are many implementations for encrypted mail, but most of them require tedious and trouble-some key management jobs of every end user. For the purpose of easier way using business mail between sites, we have been developing automatic cryptograph server for mail (Crypt-Mail Secretary: CMS). In this report, we show our new CMS implementation. This enhanced CMS is able to cryptograph mails not only based on IPv4 but IPv6, and it can handle several different cryptographic algorithms depend on the site's addresses.

1 はじめに

インターネットの普及に伴い、インターネットを利用した情報通信が頻繁に行なわれるようになった。しかし、盗聴や不正なアクセス等の不正行為も行なわれている。そこで現在、暗号化技術を用いたセキュリティ対策が注目をされている。特に電子メール・サービスに関しては個人的な情報を送受信することも多く、盗聴に弱いシステム構成を持つことから、電子メールの暗号化処理は有効なセキュリティ対策である。しかし、現在公開されている暗号化電子メール・パッケージは個人を対象にしたものが多く、暗号化処理の可否判断や不特定多数の暗号化鍵の収集・管理には利用者の介在が必要となり利用者の負担となることもある。そこで、

複数のユーザが一つの電子メール・サーバを使用して電子メールの送受信を行なう LAN (Local Area Network) 環境等のメール・システムに着目し、既存のメール・システムに暗号化処理サーバを追加することによって利用者個人の特別な操作無しに電子メールを自動的に暗号化／復号化するサーバ(Crypt-Mail Secretary : CMS)を検討し、現行のインターネット・プロトコル (Internet Protocol : IP)である IPv4 (Internet Protocol version 4)で動作する CMS の試作・動作確認を行っている[1]。

IPv4は20年近くも前に作られたものであることから、現在さまざまな技術的問題が発生し始めている。その中でも最も深刻な問題は IP アドレスの枯渇であり、2010 年頃には枯渇するだろうという予想もある[2]。そこで、IPv4 が抱いている問題の抜本的な解決を目的に標準化が進められているものが、次世代インターネット・プロトコル (Internet Protocol version 6 : IPv6) であり、現在では、基本部分の仕様はほぼ決定している。また、種々のプラットホームで動作する実装が公開され、世界規模での IPv6 テスト・ネットワーク (6bone) による評価実験が行われるなど、IPv6 への移行準備が進んでいる。

そこで、電子メールを自動的に暗号化／復号化するサーバの次世代インターネット・プロトコルである IPv6 への対応も検討し、試作を行った。しかし、以前試作を行った暗号化処理サーバでは、IPv6 のみ動作するものであり、IPv6 対応というには不十分なものであった[3]。

そこで今回は、既存の IPv4 専用と IPv6 専用の CMS を統合し、IPv6/IPv4 の両方に対応した暗号化処理サーバの実装を行なったので報告する。また、暗号化処理サーバの拡張として行なった複数の暗号方式へ対応についても報告する。

2 CMS について

2.1 CMS の概要

電子メールを自動的に暗号化／復号化するサーバである CMS の概要について説明する。まず、CMS の大きな特徴について以下に示す。

- 送信先・送信元のドメイン名 (メールアドレスの '@' 以下) によって暗号・復号化処理の有無および方式を判断する。
- 暗号鍵などの情報は CMS が管理する。
- 既存の電子メール・システムに大きな変更を加えずに暗号・復号化機能を追加できる。

また、一般的なシステムでの電子メールの流れと CMS を実装したシステムでの電子メールの流れを図 1 に示す。

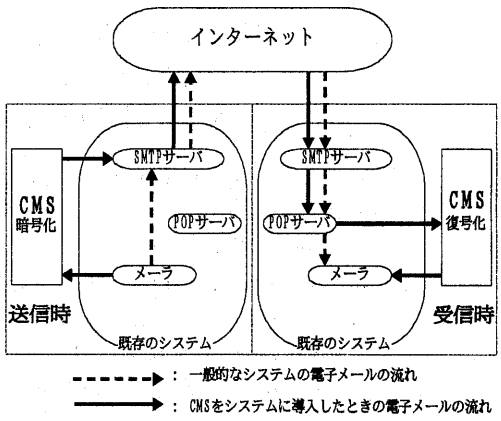

図 1　CMS を含むメール・システムの構成図

CMS では暗号化処理を施す設定をしたドメインに対しては、インターネット上のセキュリティを確保することができる。しかし、CMS サーバとメーラの間では、電子メールは平文のまま流れるため、LAN 内部を流れるデータに対してセキュリティを確保することはできな

い。これらについては、サイト外部からのセキュリティ確保はファイアウォール等で確保できる問題であると考え、本研究の目的としている暗号化処理サーバの適用範囲ではないと考えている。

2.2 CMS - SMTProxy の構成

図2に CMS - SMTProxy の構成と処理の流れを示す。CMS - SMTProxy では、メーラからの接続および SMTP コマンド[4]を受信すると、SMTP に沿った返答を独自に返し、受信したコマンド列を宛先別に格納する。その後、送信先と送信元のメール・ドメインを分析し、設定した暗号情報に従ってメール本文の暗号化処理を行なう。メーラから終了命令を受信すると、CMS - SMTProxy は、指定された SMTP サーバに接続し、格納したコマンド列順番に送信する。また、同時に、送信終了後に SMTP サーバとの接続を切る。

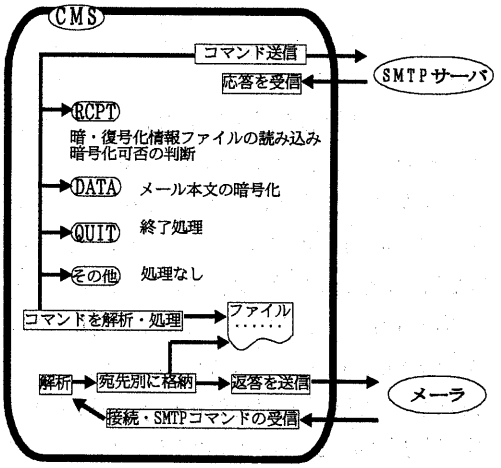

図2 CMS - SMTProxy の構成図

2.3 CMS - POProxy の構成

図3に CMS - POProxy の構成と処理の流れを示す。CMS - POProxy では、メーラからの接続を受けると、指定された POP サーバへ接続を行なう。その後、メーラから送られてきた POP コマンド[5]を POP サーバへ中継し、POP サーバから送信される返答をメーラへ中継する。POP サーバからメール本文が返答された場合には、送信元のメール・ドメインを分析し、設定した暗号化情報に従ってメール本文の復号化処理を行なう。メーラから終了命令を受信すると終了処理を行ない、POP サーバとの接続を切る。

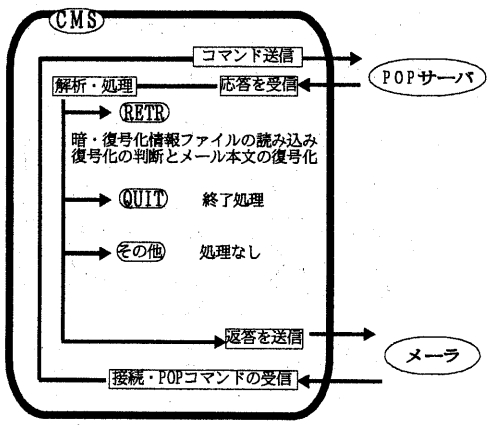

図3 CMS - POProxy の構成図

3 CMS の拡張

3.1 IPv6/IPv4 用 CMS の統合

IPv6/IPv4 で動作する CMS と IPv6/IPv4 専用でそれぞれ動作する CMS のアクセス方法を図4に示す。CMS を IPv6/IPv4 で動作させることによって、メール・システム上で動作するメーラ、SMTP サーバ、POP サーバはプロトコルを意識する必要がない。このことから、IPv6/IPv4 が混在したネットワーク環境にお

いても既存のシステムに大きな変更・制限をすることなくCMSを追加することができると考えている。

CMSはSMTPサーバとPOPサーバの二つのアプリケーションとコネクションを確立する。今回の改良では、getaddrinfo(3) 関数 [6] を用い通信先がIPv6の場合にはIPv6用ソケットを、IPv4の場合にはIPv4用のソケットをそれぞれ作成し通信を行うようにする。また、CMSはメーラからのコネクション要求を待ち受けする。その際には、計算機上でIPv4とIPv6の両方で待機する。ただし、一つの計算機に対してIPv6/IPv4の両方のアドレスを割り当てた場合においては、コネクション要求をする際に、どちらのアドレスが使用されるかは明確に定義はされない[6]。

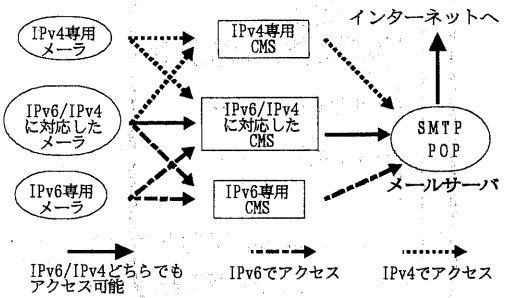

図4　CMSのアクセス方法

3.2 複数暗号方式の拡張

複数の暗号方式に対応するために以下の変更を行った。

- 暗号情報として、サイト名のほかに暗号方式の種類と暗号鍵を追加する。
- サイト名に対して、暗号方式と暗号鍵は一意に設定する。すなわち、同時に複数の方式を設定しない。
- 暗号方式と暗号鍵の変更を可能にする。

暗号化／復号化の際に使用する情報は、暗号化対象の組織名、暗号化アルゴリズム、暗号鍵として使用する文字列であり、これらを暗号情報として管理する。

3.3 暗号情報の保存と保護

暗号化情報を保護するために、暗号情報管理プログラムを新たに作成した。その仕様を以下に示す。

- 暗号情報はサイト名を鍵とするハッシュテーブルとしてファイルに保存する。
- 暗号鍵はファイル作成時に管理者の鍵で暗号化処理することで保護する。復号化はCMS起動時に鍵を入力することで行なう。
- 暗号情報管理プログラムは起動時に管理者の鍵を必要とする。

4 実装

4.1 開発言語と開発環境

実装を行なったOS (Operating System)はFreeBSD3.1、IPv6プロトコル・スタックにkame [1] を使用した。開発言語はC言語を使用し、暗号化プログラム本体は既存のCMS用のJAVA言語で作成されたものを流用した。しかし、既存のIPv4で動作するCMSはすべてJAVA言語で作成されているのに対し、IPv6対応CMSでは、JAVAがIPv6に対応していないため通信部分のみC言語で記述を行った。ただし、JAVA言語で記述されたCMSとC言語で作成されたCMSの通信部分のインターフェースとしてJava Native Interface (JNI)を用いた。既存のIPv4のみで動作するCMSとIPv6対応CMSを比較した構成図を図5に示す。

1) http://www.kame.net/

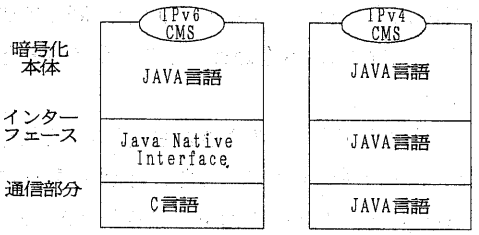

図5 CMSの構成図

4.2 暗号化アルゴリズムとライブラリ

今回実装したCMSの暗号化アルゴリズムライブラリには、対象鍵暗号方式の暗号化アルゴリズムである IDEA (International Data Encryption Algorithm) および DES (Data Encryption Standard)、また一般に使用されている PGP (Pretty Good Privacy) 暗号を採用した。これらは、いずれも暗号化ライブラリである Cryptix3.1.1 [2]を使用した。

5 動作確認実験

今回実装した暗号化処理サーバの動作確認を行なうために、電子メールの送受信実験を行なった。

5.1 実験環境

実験を行なうために、研究室内ネットワーク上に二つ、学外にインターネットを挟んで一つの電子メール・システムを用意し、それぞれを組織A、組織B、組織Cと仮定した(図6参照)。組織 A、組織 B の電子メール・システムは、SMTP サーバ、POP サーバ、暗号化サーバ CMS によって構成し、組織 C の電子メール・システムは、SMTP サーバと POP サーバのみで構成した。

2) http://www.cryptix.org/

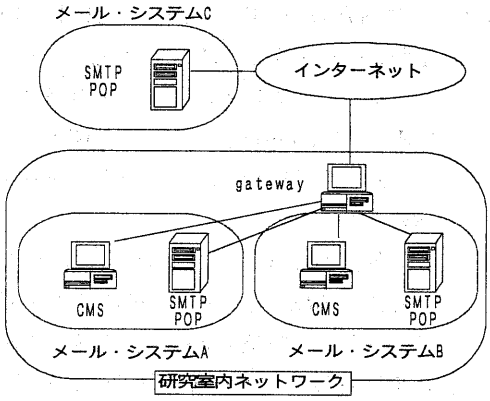

図6 実験環境

5.2 使用ソフトウェアと計算機

本実験環境の各メール・システムで使用したソフトウェアと計算機の OS を表 1 に示す。CMS を実装する計算機上では IPv6 プロトコル・スタックとして FreeBSD 用の kame を使用した。また、組織 A、組織 B の SMTP 及び POP サーバには IPv6 に対応したソフトウェアを使用した。IPv4 用メーラは Mule19.34.1 + im100 + mew1.93 を使用し、IPv6 用メーラは telnet コマンドを使用し簡易メーラとした。

表1 使用ソフトウェアと使用 OS

メール・システムA	OS	ソフトウェア
SMTPサーバ	FreeBSD3.4	sendmail6-8.9.3
POPサーバ		qpopper-2.53
CMS	FreeBSD3.1	JDK1.1.8

メール・システムB	OS	ソフトウェア
SMTPサーバ	FreeBSD3.4	sendmail6-8.9.3
POPサーバ		qpopper-2.53
CMS	FreeBSD3.1	JDK1.1.8

メール・システムC	OS	ソフトウェア
SMTPサーバ	FreeBSD2.2.6	sendmail6-8.9.3
POPサーバ		qpopper-2.53

5.3 実験方法

今回実装を行ったCMSが正常に動作しているかを確認するために、以下の 2 種類の方法で動作確認実験を行なった。

(1) CMSがIPv6/IPv4の両方に対応しているかを確認するために、IPv4 と IPv6 の両方でメールを送受信した。その際に、CMS 上で tcpdump コマンドを使用し、メール送受信時の IP パケットの流れを解析した。

(2) 暗号情報に基づいて処理が行なわれているかを確認するために、組織 A の利用者から暗号化対象の組織 A、組織 B の利用者に対して、"IDEA", "DES", "PGP" の各暗号方式を順に設定し電子メールの送信を行なった。また、組織 A の利用者から暗号化非対象の組織 C に対してメールの送受信を行なった。

5.4 実験結果

前節 (1) 項目の動作確認実験においてメーラから CMS、CMS から SMTP/POP サーバの両方においてそれぞれ IPv6/IPv4 でパケットを送受信しており CMS が IPv6/IPv4 の両方で動作することを確認することができた。

(2) 項目の動作確認実験においては、暗号化対象に設定した組織 B に対してそれぞれの暗号方式で正常にメール本文が暗号化／復号化がなされていることを確認することができた。また暗号化非対象に設定した組織 C に対しては、メール本文が暗号化されることなく平文で送信されたことを確認できた。

6 まとめ

今回報告を行なった暗号化処理サーバでは、動作確認の結果から IPv6/IPv4 でメールを送受信しており、CMS が IPv6/IPv4 の両方に対応していることを確認できた。このことから、IPv6/IPv4 が混在したネットワーク環境においても既存のシステムに大きな変更・制限を加えることなく CMS を追加することができると考える。

暗号化処理サーバの機能拡張として、複数暗号方式への対応を可能としたことから、特徴のある暗号方式を有効に活用できると考えられ、他の暗号化アルゴリズムへの移行も円滑に行うことができると考えられる。また、暗号化に必要な暗号情報を暗号情報管理プログラムで設定し、暗号化してファイルに保存することによって、暗号情報の安全性を考慮した。

今後の課題としては、今回実装した CMS の試験運用を行うとともに、暗号化アルゴリズムの追加や、モバイル端末に対応するための具体的な仕様の検討などを考えている。

参考文献

[1] 永江由紀子 他："電子メールの自動暗号化処理サーバの構築(2)," 情処研報 99-CSEC-4, pp.61-66 (1999)

[2] C.Huitema (松島栄樹 訳)：IPv6 次世代インターネット・プロトコル, プレンティスホール, 1997, pp.3

[3] 伊藤昌彦 他："IPv6 対応電子メール自動暗号化処理サーバの試作," 平成 11 年度電気関係学会北海道支部連合大会講演論文集, p.424 (1999)

[4] Simple Mail Transfer Protocol, Request For Comment (RFC) 821

[5] Post Office Protocol, Request For Comment (RFC) 1939

[6] W.Richard Stevens (篠田陽一 訳)：UNIX ネットワークプログラミング 第 2 版 Vol.1, トッパン, 1999, pp265-276