3D−9

同報暗号メールシステムの構築*

黒田康嗣　菊池 浩明†

(株)富士通研究所‡

1 はじめに

計算機の相互接続による広域ネットワークの商用化に伴い、ユーザを特定した機密性のある同報通信が強く求められている。

同報暗号通信方式には、メンバ間で暗号鍵を共有する共通鍵方式と、各メンバが全メンバの公開鍵のリストを管理する個別鍵方式の2種類がある。

しかし、共通鍵方式では、暗号鍵の横流しの恐れあり、閉鎖性に問題がある。一方、個別鍵方式では、横流しの心配はないが、メンバの追加や削除が困難である。

そこで本稿では、上記方式の問題点を指摘し、その問題を解決するために、送信者と受信者の間に鍵交換センタを設けた鍵交換方式を提案する。さらに提案方式に基づく同報暗号メールシステムの実装について報告する。

2 従来の同報暗号通信方式

従来の同報暗号通信方式として、共通鍵方式と個別鍵方式[1]を挙げ、それらの問題点を指摘する。

2.1 共通鍵方式

共通鍵方式では、メンバ共通の暗号鍵を用意し、全メンバがメンバ共通の暗号鍵を共有する。

発信者は、メンバ共通の暗号鍵で、平文を暗号化して送信する。暗号文を受けとった各メンバは、メンバ共通の暗号鍵で暗号文を復号し、平文を読む。

図1に共通鍵方式を示す。

図で、A, B, C, Dは同報暗号通信のメンバ、K_Mはメンバ共通の暗号鍵、Pは平文、C_Mは暗号文を表している。

共通鍵方式には以下の問題点がある。

- メンバ共通の暗号鍵を、メンバ全員で共有しなければならず、第3者に秘密情報が洩れる可能性が高い。また、悪意を持つメンバが、意図的に暗号鍵を横流しする不法行為も否定できない。
- メンバが同報暗号通信から脱退する時は、新しくメンバ共通の暗号鍵を作成し、各メンバに配り直さなければならない。
- 暗号方法として、公開鍵暗号法を採用すると、第3者が同報暗号通信に情報を送信出来てしまい、閉鎖性が悪い。

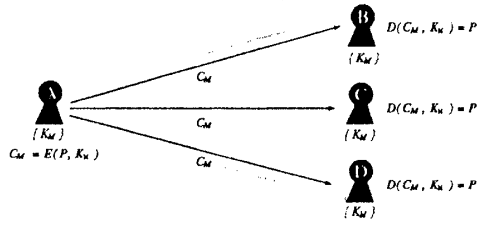

図 1: 共通鍵方式

2.2 個別鍵方式

個別鍵方式は、各メンバがメンバのリストとすべてのメンバの公開鍵のリストを共有する。発信者は、平文を各メンバの公開鍵で暗号化して送信する。暗号文を受けとった各メンバは、自分の秘密鍵で暗号文を復号し、平文を読む。

図2に個別鍵方式を示す。

図で、PK_M, SK_Mはメンバ共通の公開鍵、秘密鍵。PK_A, PK_B, PK_C, PK_DとSK_A, SK_B, SK_C, SK_Dは、同報暗号通信するメンバの公開鍵、秘密鍵。$E()$は暗号化、$D()$は復号化を表している。

個別鍵方式には以下の問題点がある。

- 各メンバが、全メンバのリストと公開鍵を管理しなければならならず、各メンバの負担が大きい。
- メンバが同報暗号通信に入会、脱会する時は、全メンバに入会、脱会するメンバの名前と公開鍵を伝え、各メンバにそれを反映してもらわなければならない。
- 上記過程で、送信した情報が、新メンバに送信されなかったり、脱会したメンバに情報が送信されてしまう可能性がある。

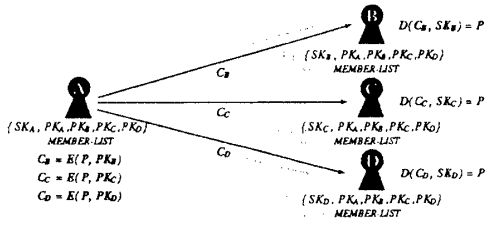

図 2: 個別鍵方式

*An implementation of secure broadcast communication in Privacy Enhanced Mail

†Kuroda Yasutsugu, Kikuchi Hiroaki

‡Fujitsu Laboratories Ltd., 1015 kamiodanaka nakahara-ku kawasaki Japan, 213

3 鍵交換方式

2節で挙げた問題点を解決するために、共通鍵方式と個別鍵方式を組み合わせた、鍵交換方式 "A secure Broadcast communication with key swiching" を提案する。鍵交換方式は、送信者と受信者の間に、鍵交換センタを設けることを特徴としている。鍵交換センタは、メンバ共通の公開鍵 PK_M と秘密鍵 SK_M、同報通信を行なうメンバのリストと全メンバの公開鍵を持つ。また、各メンバは、メンバ個人の公開鍵 PK_i と秘密鍵 SK_i、メンバ共通の公開鍵 PK_M を持つ。

図3に鍵交換方式を示す。図では、メンバ A がメンバ B, C, D に、鍵交換方式を使って同報暗号通信を行なっているところを示している。

以下、鍵交換方式の情報の流れを図3を使って説明する。

(1) A は平文 P をメンバ共通の公開鍵 PK_M で暗号化し、暗号文 C_M を作る。

(2) A は、暗号文 C_M を鍵交換センタに送信する。

(3) 鍵交換センタは、暗号文 C_M をメンバ共通の秘密鍵 SK_M で復号化して平文 P を取り出す。

(4) 鍵交換センタは、取り出した平文 P を同報暗号通信のメンバ B, C, D の公開鍵で暗号化して暗号文 C_B, C_C, C_D を作る。

(5) 鍵交換センタは、暗号文 C_B, C_C, C_D を B, C, D に送信する。

(6) B, C, D は、暗号文 C_B, C_C, C_D を B, C, D 個人の秘密鍵で復号化して平文 P を取り出す。

鍵交換方式により、秘密情報の保持を最小限におさえ、メンバが脱退する毎に、メンバ共通の秘密鍵、公開鍵を新たに作成する必要がなく、同報暗号通信の管理者だけがメンバの入会、脱会の管理をする同報暗号通信が可能となり、共通鍵方式と個別鍵方式の問題点を解決することができる。

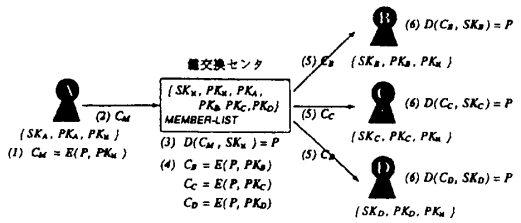

図 3: 鍵交換方式

4 同報暗号メールシステムの構築

4.1 実装

鍵交換方式の応用として、ネットワーク上に同報暗号メールシステムを試みた。この構築にあたり、暗号メールプロトコル PEM[1] を実装した FJPEM[2] を利用した。

メールシステムにおける同報通信は、一般にメーリングリストと呼ばれる。メーリングリストとは、同報通信のための Email アドレス (以下、ML アドレスと略す) を設け、その ML アドレスにメールを送信すると、全メンバに同報通信するものである。我々は、ML アドレスに鍵交換センタの機能を付加することで、同報暗号メールシステムを構築した。

図3に示したように、発信者が暗号文を送信し、メンバが暗号文を受信し復号する間に、ネットワークを流れる暗号文は二種類ある。発信者と ML アドレスの間の暗号文 C_M と ML アドレスと各メンバの間の暗号文 C_A, C_C, C_D である。鍵交換センタは、ML アドレスが暗号文 C_M を受信すると、C_M を復号し、平文 P から暗号文 C_B, C_C, C_D を作る。ただし、PEM のアプリケーションを応用したため、C_B, C_C, C_D は平文を暗号化した DES の鍵を、各々の公開鍵について暗号化したものであり、実際には C_B, C_C, C_D を含む同一の暗号メールが各々に送信される。従って、送信する暗号メールの大きさは、ユーザの数に比例することになる。

また、平文を元に作る電子署名により、ML アドレスでは、情報の改竄の検出と送信者の認証が可能である。本実装では、電子署名の検証結果が無効である場合と、非メンバからのメールである場合には、発信者にメールを送り返している。

なお、本実装は、perl と C 言語で構成されている。

4.2 評価

メンバが n 人とすると、鍵交換センタでの処理は、DES の暗号 1 回、復号 1 回、RSA の復号化 1 回、RSA 暗号化 n 回が必要である。鍵交換センタでの処理時間を表 1に示す。処理時間は、SS2(SunOS4.1.2, 28MIPS) を用いて、2kbyte の平文を 100 回処理した時間の平均を計算したものである。

ユーザ数 (人)	1	5	10	50	n
処理時間 (sec)	3.35	3.90	4.65	10.78	0.15n+3.25

表 1: 鍵交換センタの処理時間

表1を見てわかるように、n 人のメンバに対して 0.15n+3.25 秒のオーバヘッドがかかる。メンバ 1000 人では 2.5 分余りのオーバヘッドになるが、メールシステムは即応性を要求されないため、致命的な問題ではない。

しかし、PEM のヘッダは、メンバが一人増える毎に、暗号鍵の情報が約 200byte 増える。メールシステムの最大送信量が 50Kbyte 程度なので、平均的なの平文の長さを 2Kbyte とした場合、同報暗号通信できるメンバ数の最大値は 225 名たらずである。これを解決するには，受信者毎に暗号処理をして送信する機能を、PEM に拡張する必要がある.

5 おわりに

本稿では、共通鍵方式と個別鍵方式の問題点を指摘し、これらの問題点を解決する鍵交換方式を提案した。

さらに、鍵交換方式の応用として、同報暗号メールシステムを構築し、評価を行なった。その結果、暗号処理のオーバーヘッドは致命的な問題ではないが、メンバが約 200 名を越える場合に、問題が生じることがわかった。このシステムは、現在富士通研究所内で試験運用中である。

WIDE プロジェクトのセキュリティWG のメンバと、富士通研の pem-dev メーリングリストのメンバに感謝する。

参考文献

[1] J. Linn, S. Kent, D. Balenson, B. Kaliski, "Privacy Enhancement for Internet Electronic Mail: Part I,II,III,IV," *RFC-1421,1422,1423,1424*, 1993

[2] 菊池浩明, 森下哲次, "暗号電子メール PEM(Privacy Enhanced Mail) の実装と課題," 情処第 46 回全国大会,1,pp.99-100, 1993