親展機能付き電子メールシステム

7K－5

小林　信博，岡本　隆司，桜井　幸一
三菱電機(株)情報システム研究所

1　はじめに

現在ビジネス分野等において、電子メールシステムが、従来の紙の文書に替わる高速伝達手段として盛んに利用され始めている。しかし、安全面から考えて幾つかの問題点がある為に、これを契約書等の重要書類に対して用いることはできなかった。我々はこのような問題を解決するものとして、「検印付き電子メールによる回覧システム」[1]をＵＮＩＸ[1]システム上で開発し、その応用範囲の拡大に努めてきたが、今回は更に、送信者の指定した受信者にしか読むことができない電子的な親展機能を実現したのでこれを報告する。

2　開発方針

本システムを開発するに当たって、以下の開発方針を設定した。

1. 「検印付き電子メールによる回覧システム」との共存
   既に我々の開発した「検印付き電子メールによる回覧システム」の機能を損なうことなく親展機能を追加し、その応用範囲の拡大を目指す。
2. 標準方式への対応
   世界的なネットワークである Internet において、電子メールの暗号化方式として標準化されたＰＥＭ[4]への対応を図ることにより、システムとしての汎用性を高める。
3. 鍵管理方式の改善
   実運用を考えた際に問題となる、ユーザが鍵管理に費やす労力の低減を図り、安全性を高めるとともに、利便性を向上させる。
4. スループットの向上
   多量の計算を必要とする暗号処理の高速化を図ることによってユーザの操作に対する応答性を改善するとともに、処理能力の低い計算機上においても実用的な動作を目指す。

A Confidential Electronic Mail System
Nobuhiro KOBAYASHI, Takashi OKAMOTO, Kouichi SAKURAI
Mitsubishi Electric Corp.

3　実現方法

3.1　親展機能

電子的な親展に相当するメール文章の秘匿化は、秘密鍵暗号方式と公開鍵暗号方式を組み合わせた複合方式により実現した。一般に、暗号の処理速度は秘密鍵暗号方式の方が高速であり、鍵管理は公開鍵暗号方式の方が容易であるので、メール文章は秘密鍵暗号方式により高速に暗号化し、その秘密鍵を公開鍵暗号方式により暗号化してメールとともに送る。親展及び親展解除の手順を以下に示す。

表 1: 親展の手順

処理	順番	処理内容
準備	1	受信者は、事前に秘密鍵から公開鍵を作成し、これを発信者に公開する
発信	2	発信者は、乱数によりセッション鍵を生成し、メール本文を暗号化する
	3	セッション鍵を、受信者の公開鍵を用いて暗号化する
	4	暗号化されたメール本文、及び暗号化されたセッション鍵を送付する
受信	5	受信者は、自分の秘密鍵を用いてセッション鍵を復号化する
	6	復号したセッション鍵を用いて、暗号化されたメール本文を復号化する

以上の手順によって親展及び親展解除を行なう。なお、文章の改ざんについては、既に開発済みの検印機能を用いて検証を行なう。

3.2　従来システムとの共存

従来のシステムでは、公開鍵方式によるデジタル署名技術を応用した電子的な検印と、指定された回覧経路にそった配送及び多重検印を実現しており、検印情報及び回覧情報は、メールのヘッダ部に拡張ヘッダとして格納されている。今回開発した親展機能においては、メール本文のみを秘匿化の対象とすることにより、従来システムとの整合性をとった。また、この方式を採用することにより、検印＋回覧，親展＋回覧，検印＋親展＋回覧と用途に応じた機能

[1]ＵＮＩＸオペレーティングシステムは、ＵＮＩＸシステムラボラトリーズ社が開発し、ライセンスしています。

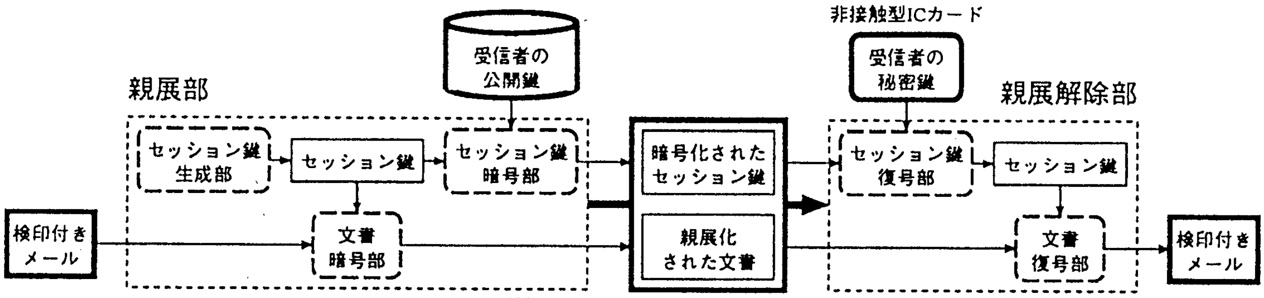

図 1: システム概略図

の組合せが可能である。

3.3 非接触型ＩＣカードを用いた鍵管理

各ユーザの管理する秘密鍵は、非接触型ＩＣカードの内部に保存した。これにより、従来のパスワード方式と比較して、よりランダムで長い秘密鍵の使用が可能となり、安全性を高めることができた。また、また物理的に管理しやすく、パスワードの入力の手間も省けるので、ユーザの利便性が増した。更に、非接触型であるので、ユーザに意識させることなく、自動的に秘密鍵を読みとることが可能である。

3.4 Internet の標準方式ＰＥＭに準拠

親展で用いる暗号化されたセッション鍵や、メールの受信者の公開鍵、そして暗号化されたメール本文は、それぞれ Internet の標準方式であるＰＥＭに準拠した形で、メールのボディ部に格納した。従って、親展処理済みのメールを従来のＵＮＩＸ電子メール同様に既存のネットワークを通じて配送することが可能である。

4 システム

4.1 システム構成

図１にシステムの概略図を、図２に実行例を示す。

4.2 暗号仕様

今回使用した暗号の仕様を以下に示す。

表 2: 暗号仕様

暗号方式	アルゴリズム	鍵サイズ byte
公開鍵暗号	ElGamal 法	秘密鍵 8, 公開鍵 48
秘密鍵暗号	独自方式 CBC	192

4.3 処理速度

UNIX-EWS（CPU: 68030, 20 MHz）にて２KB のファイルを親展，親展解除した際の時間を計測したところ、それぞれ 1.5 sec， 0.3 sec であり、実用的な速度を得ることができた。

```
To: toka
Bcc: n-koba@ecs.isl.melco.co.jp
X-Sinf: n-koba@ecs.isl.melco.co.jp
X-Circ: sakurai
Subject: test of pem
X-Sign: M3]-'R-E5#$$4IR3'A\/L#.(\5@DAX7^HVO^3^[-!];W]>&)-\5:(-U@'I[Y^MB
 ]@>,3*CO;.KR?2AH:&AH:&CT[.KH[&AH:&AH:&^KL[3H:&AH;^NO^2AH:&AM5"^@,7-N+6M
 OBF\'96-S+FES;^YM96OC;RYC;RYJ<^'@(^!A@@JCOD^YTXAFM+06J3_6\+>\2)A([+-'OW
 MSRSEUI(B4V^H;F/O.4B)4NFKC^H''8^2YX<O]U10?>D$60>:|[.3!`?7@$&'''R`

-----BEGIN PRIVACY-ENHANCED MESSAGE-----
Proc-Type: 4, ENCRYPTED
Content-Domain: RFC822
DEK-Info: XXXA_1.1
Originator-Certificate:
 T9NHyNlVDEEUpyTHh8PzDOI8Vgkh4X+o2v+T+7dBRb3peGJN8VaIdlgHp7S+19geM
 TKjzbOryfShoaGhoaGj07Oro7GhoaGhoaG+rs7ToaGhob+ux+6hoaGhVCAgMXNuLW
 tvYmFA2WNzLmlzbC5tZWxjbySjbySqcCAgICBhYgqjvk+SO4hmLOWqT/W8Le8SJhI
 7LdHv3tzyzllpIYU2Cg--
Key-Info: XXXB_1.0,
 MkVFRkQ5MUM4RkIwNTYxMkE1OzEONEY0OENEOTlFOTA5MTA0RTM0MkY4OEY5N0EyN
 Tk4N0ZCMTIzQTA5NjcJRDJDRjcwREM2NTRGMOM5MjEyOzk1MTNCOzc0OjglNDkxMA
 --
MIC-Info: XXXC_1.0, XXXD_1.0,
 MCB+slIrdlX5KOAHfU/5B2YklzI4Vp/2rqweZmquChF6T9YWuB0e4fVhZfirNkKBo4
 m+wBQucJJiwb2M9YOBl19XMEt9mp6tnH6Axd9BLAS6JnR3WgHjkFBTIzB5JRwp7Hb
 RjwBlON/entIcs/K/LKql5uKfucUwqQemlltBTervoPe3XRMPyRYTB79G7nMjfbHq
 djICFbgGYai9tRYybTS+2ItajAc3HPe4Fvh+lNfYIeVLYGLc8UX8o+ACPpBCNBec-
Recipient-ID-Asymmetric:
 dG9rYR--
Key-Info: XXXB_1.0,
 NjBENDhFMzAzRDAzOEY2RUVFRjOzOzRDNURBRjlCMzBDODE0NDYlNzglMzE2OTY2N
 OO4OjOOODNCMDczRjhBN0YyRDg0NzcyMkYOOjcwMjM4OTA4MEI5RkRBOTA3MDA2MA
 --
Recipient-ID-Asymmetric:
 bllrb2JhOGVjcy5pc2wubWVsY28uY28uanA-
Key-Info: XXXB_1.0,
 NUYzRjVFNOY2RDhCNkMzOUFFNzg5MjVBNjc4NjUwMkIzNkQyOTQ1NTNBMDIyNDk5M
 DBDOTkwOjYzNDI4NEE3NkO1OEVCOzA0MkRGRDdGNzVDOzlBMDlDRjVFOjc3RkNGMA
 --

 NTkg3g9CvILSlDoKpyCu+vtyEcWJbgbl3EcXmHbputRABBOgKwYGMozOo3WfYMZ96
 ekF/sA44mLwXBZ566eqMlTZEb4GP73eKlcOAU6ZIelsrenOh9qBYUcBlXWlJztZVz
 EjljSORrcFUJ7YzTpNRoAEl6WtbI2vPEAFBQcdpmGFuy0-
-----END PRIVACY-ENHANCED MESSAGE-----
```

図 2: 実行例

5 おわりに

本稿では、「親展機能付き電子メールシステム」の実現と、そのシステム構成について述べた。本システムでは、従来システムとの整合性をとりながら親展機能を実現するとともに、ＰＥＭへの対応を図っている。また、非接触型ＩＣカードにより鍵管理を行い、安全性とユーザの利便性を高めた。今後は、X.509 形式の証明書への対応を行なっていきたい。

参考文献

[1] 小林，岡本，桜井，" 検印付き電子メールによる回覧システム"，情報処理学会第 45 回全国大会

[2] 辻井，笠原，" 暗号と情報セキュリティ"，昭晃堂，1990

[3] David H.Crocker，" RFC822「STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES」"，1982

[4] J.Linn，S.Kent，D.Balenson，" RFC1421 〜 RFC1423「Privacy Enhancement for Internet Electronic Mail:Part I 〜 III」"，Feb.,1993

[5] 舘林，松崎，原田，宮地，多田，" 暗号化電子メールシステム"，情報処理学会第 46 回全国大会

[6] 菊池，森下，" 暗号化電子メールＰ.ＥＭ（Privacy Enhanced Mail）の実装と課題"，情報処理学会第 46 回全国大会