特集：コンピュータセキュリティ

暗号化電子メールシステムの現状

溝口佳寛*

近年のインターネットの普及により電子メールによる情報交換を行う機会は，ますます増える一方である。本稿では電子メールにおいて内容の漏洩を防ぐための暗号化，発信者の確認（認証）と内容の改ざんを防ぐための電子署名について述べる。最初に，基礎となる暗号化手法を簡単に説明した後，電子メールでの暗号・電子署名の必要性と実現方法について述べる。最後に，実際の暗号化電子メールシステムの例としてインターネット標準仕様として提唱されているPEM（Privacy Enhanced Mail）の実現と暗号・認証ソフトウェアとしてインターネット上で普及しているPGP（Pretty Good Privacy）ソフトウェアを紹介する。

キーワード：電子メール，暗号，電子署名，PEM，PGP

1．はじめに

近年の日本におけるインターネット参加組織の増加は著しく，また，多くのインターネットプロバイダの出現や大手パソコン通信サービスからもインターネット電子メールが出来るようになったことにより多くの人が職場や家庭で電子メールを使えるようになってきている。本稿では，電子メールを利用するにあたって，個人の秘密を守るための暗号化，文書の内容が改ざんされていないことと発信者を確認するためのユーザ認証について，その仕組みを簡単な例で説明する。インターネット上では，さまざまな仮想空間が構築されつつあるが，そのときに現実空間での概念と仮想空間での概念との対応づけは，インターネット社会での種々の問題点を理解する上で非常に重要である。従って本稿では，通常の手紙において秘密を守るための工夫と暗号化電子メールとの対応づけを行い，通常の郵便と何が同じで何が異なるかを述べる。最後に，暗号化電子メールのインターネット標準であるPEM（Privacy Enhanced Mail）と暗号・認証のためのソフトウェアとして草の根的に普及しているPGP（Pretty Good Privacy）ソフトウェアについて具体例とともに安全な電子メール通信を行うために必要な事項と問題点を解説する。

* みぞぐち よしひろ　九州工業大学情報工学部制御システム工学教室
〒820 福岡県飯塚市川津680-4
Tel. 0948-29-7700
（原稿受領　1996.03.22）

2．秘密鍵暗号方式

まずはじめに暗号化に関する基本的な事項をまとめる。計算機の中ではメール文書を含む全ての文書は各文字のコードを表すコード（数字）の列として表現されファイルに格納される。例えば'a'という文字のコードは97であり，それを2進数で表現すると'$01100001_{(2)}$'となる。図1に簡単な暗号化と復号化の例を示す。AさんとBさんは，通信中の通信文の秘密が洩れないように通信で用いる暗号方式（この例で紹介する最も簡単な暗号方式を「REI」と呼ぶことにする。）を定め，

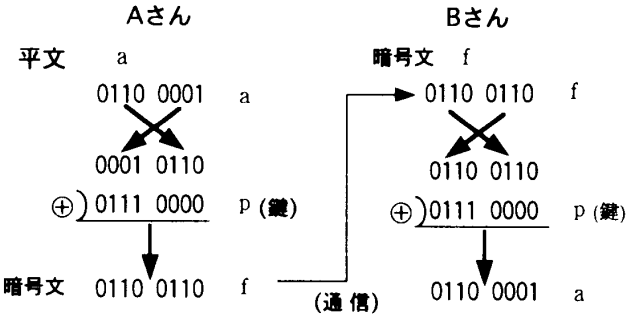

図1　簡単な秘密鍵暗号方式（REI）による暗号と復号の例

暗号に用いる鍵（この例では'p'）を決めておく。Aさんは暗号化する前の平文（plaintext）を作成し，それを暗号化する。暗号化された文書は暗号文(ciphertext)と呼ばれる。その後，電子メール等の通信手段を用いて暗号文をBさんへ送る。ここで例として紹介している暗号方式「REI」のアルゴリズムは次の通りである。

・秘密鍵暗号方式で，鍵は8ビット（すなわち1文

字）とする。

- 平文を8ビット（すなわち1文字）ごとのブロックに分割し暗号化する。
- ブロックの上位4ビットと下位4ビットを交換する。
- 平文ブロックと鍵との排他的論理和（⊕）を暗号文ブロックとする。
- 平文から暗号文を得る方法と暗号文から平文を得る方法は同じである。

排他的論理和とは，各ビットごとの演算で，$0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$ となる演算である。この例では平文'a'を鍵'p'で暗号化し暗号文'f'を用いて通信が行われている。例では平文が1文字であるが複数文字列の場合，各1文字（8ビット）ごとに暗号化を行いその結果の文字列を暗号文として用いる。

さて，ここでAさんが暗号化した文書を復号化（解読）するときに必要なものは「暗号方式」と「鍵」である。Bさん以外の通信文の盗聴者が，この2つを知っていた場合，または，推測出来た場合に通信の秘密が漏洩してしまう。従って，この2つを秘密にしておくことは非常に重要なことであるが，現実には「暗号方式」を通信する人ごとに変えるということは通信する人ごとに暗号化のプログラムを準備するということであり現実的ではない。そこで「暗号方式」は共通にし，通信ごとに異なる「鍵」を用い，それを秘密にするという方式を使う。我々が日常生活で使っているロッカーや玄関の錠を考えてみて欲しい。錠のデザインは同じであるが，鍵の溝の種類が非常に沢山あるために，同じ種類の錠を使っていても自分の鍵で人のロッカーを開けることは出来ない。ここでいう錠が「暗号方式」に対応し，鍵が「暗号鍵」に対応する。従って，鍵の種類が豊富にあり，鍵の種類が用意に推測出来ない暗号方式が頑強な暗号方式と言える。

ここで用いた暗号方式「REI」は説明を簡単にするために鍵を8ビットとしたので，鍵は256通りしかなく簡単に暗号破りが行われてしまう。実際に使われている暗号方式では，もっと長いビット数を持った鍵を用い，また暗号化・復号化の方式も「REI」のように転置1回，排他的論理和1回というような簡単なものではなく，もっと複雑な構成が用いられ容易に解読されないような工夫がされている。しかし，基本的には平文をブロックに分け，転置や排他的論理和を複数回繰り返すという「REI」と同様な考え方であるので秘密鍵暗号方式の雰囲気は「REI」の例で理解出来る。

秘密鍵暗号方式として最も知られている方式として，DES（Data Encryption Standard）方式がある。米国規格基準局（NBS：National Bureau of Standard）は1973年にコンピュータの暗号化に使う方式を公募し，IBM社から提案された方式をデータ暗号化標準（DES）として1977年に公布した。DESは秘密鍵暗号方式として完成度の高い方式とみなされ，米国規格規格協会（ANSI：American National Standards Institute）でも1981年から（DEA：Data Encryption Algorithm）という名前で標準化され，多くのデジタル通信や計算機アプリケーションで利用されている。DESは，平文を64ビットのブロックに分け，56ビットの鍵を用いて暗号化する。暗号化は転置と換字と排他的論理和を組み合わせた処理を16段繰り返すことにより，平文のビットパターンをかき混ぜ暗号文に変換する。後に紹介するPEMでは，このDES方式が用いられる。DES方式の詳細は，参考文献[1),4)]など多くの暗号に関する教科書に紹介されている。

3．公開鍵暗号方式と電子署名

秘密鍵暗号方式の大きな問題点は鍵の配布にある。送信者と受信者で共通な鍵を持つ必要があるため，何らかの方法で鍵を伝えねばならない。しかし，その際に鍵を盗聴されると，それ以降の暗号通信が全て漏洩することになる。その欠点を克服するために考案された暗号方式が公開鍵暗号方式である。ここでは1978年にRivet, Shamir, そして，Adlemanによって考案されたRSA公開鍵暗号方式について紹介する[7)]。このRSA暗号方式は電子署名にも用いることが出来，後述するPEMやPGPでも使われている暗号方式である。図2はAさんが平文（この例では文字コード30で表される1文字）をRSA暗号方式を用いてBさんに送る例を示している。その手順は以下の通りである。

- Bさんは2つの素数 p, q を選び，$n = p \cdot q$, $m = (p-1) \cdot (q-1)$ を計算し，任意に $d\,(<n)$ を選び，$e \cdot d \bmod n = 1$ となる e を計算する。
- BさんはAさんへ n, e を伝える。
- Aさんは平文 M（ここでは30）に対して，暗号文 $C = M^e \bmod n$ を計算する。
- AさんはBさんへ暗号文 C を送信する。
- Bさんは受信した暗号文 C に対して，$M' = C^d \bmod n$ を計算する。

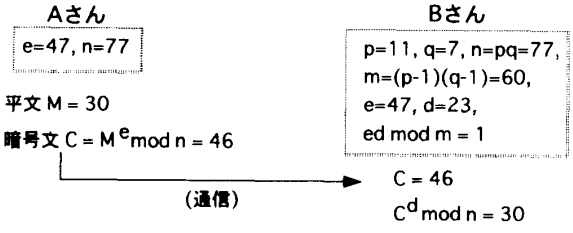

図2　RSA公開鍵暗号方式による暗号と復号の例

・数学の整数論の基本的な性質から実は $M=M'$，すなわち得られた M' がAさんが送信した平文であることが保証されている。

ここで演算 mod n は整数 n で割った余りを表す。Aさんが暗号化のために用いた2つの数 n と e を暗号鍵（公開鍵）といいBさんが復号化のために用いた2つの数 n と d を復号鍵（秘密鍵）という。公開鍵方式は，このように暗号化の鍵と復号化の鍵が異なり暗号鍵を公開しても復号鍵を知らない限り復号出来ないような方式である。このRSA暗号方式の場合，公開されている n と e から復号鍵 d を得るためには n の素因数分解，すなわち $n=p\cdot q$ となる p, q を知る必要がある。図2の例では $n=77$ と小さな数であるために簡単に素因数分解 7・11を求めることが出来，簡単に秘密鍵 d が計算出来てしまうが，実際には512ビットから1024ビットで表される大きな n を用いる。n が非常に大きな数の場合，その素因数を求めることは非常に困難である（時間がかかる）ことが知られている（厳密には，高速な素因数分解アルゴリズムが知られていない）。現在知られている最も高速な素因数分解アルゴリズムを用いて100Mipsの計算機を使って512ビットの n の素因数分解を行った場合，単純計算でも3000年以上かかることがわかる。既存の素因数分解アルゴリズムでは n の大きさに対して処理時間が指数関数的に増大するため，もっと大きな n（例えば1024ビット）に対しては絶対に素因数分解計算不可能といっても良い。

さて，このRSA暗号方式であるが電子署名（印鑑）にも使うことが出来る。BさんからAさんに数'07', '14', '11'で表される文書を送りたかったとする。その際，この3つの数字から作られる何らかの数 M（ハッシュ値と呼ぶ）を計算し，Bさんの秘密鍵 n と d をあたかも暗号化鍵のように用いて $C=M^d \bmod n$ を計算する。そして，この数 C を文書の最後に付けて送る（図3を参照）。文書を受け取ったAさんは $M'=C^e \bmod n$ を計算し，その数が受け取った文書から得られるハッシュ値であることを確認する。数学的には $M=M'$ であることが知られており，Aさんの M' の計算式で M となる C を計算出来るのは d を知っているBさんだけであることもわかる。このことにより，Aさんが計算した M' と文書のハッシュ値が等しくない場合は，文書に何らかの改ざんが行われた場合か，Bさん以外の署名が付与された場合であることがわかる。この例では説明を簡単にするために，文書から得られる何らかの数 M（ハッシュ値）を簡単な和で求める例を用いた。この例では，簡単な置換を行った文書でも同じハッシュ値を取るため改ざんが起こったかどうかを確認する方法としては弱い方法となっている。実際の例，例えばPEMやPGPなどでは，Rivestにより考案されたMD5と呼ばれるハッシュ関数を用いる。MD5は任意の長さの文書から128ビットの数（ハッシュ値）を得るアルゴリズムでしかも逆方向の処理が出来ないように工夫されている。

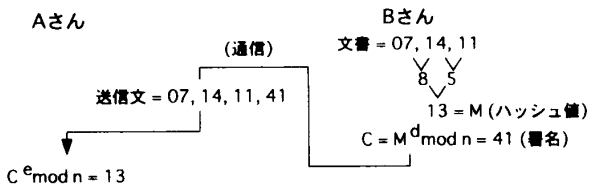

図3　RSA公開鍵暗号方式を用いた電子署名の例

4．電子メール配送の仕組み

現在，インターネットに接続されている計算機はIPアドレスと呼ばれる各計算機ごとに異なるアドレスが付与されている。同じIPアドレスを付与された計算機は全世界に2台以上存在することはない。電子メールの配送元計算機は送信先アドレスのドメインに対して，DNS（Domain Name Server）へそのドメインの配送先計算機のIPアドレスを問い合わせ，その計算機と通信を行う。通信は，SMTP（Send Mail Transfrer Protocol）と呼ばれるプロトコルに基づきメール転送が行われる。一般には，配送先計算機とメール受信計算機が等しいことが多いが，組織によっては組織内のサブドメイン全ての配送先計算機を1つの計算機にし，組織外からのメールは一旦全てその計算機で受取り組織内へ再配布するという方式を取っている所も少なくない。また，電子メールの送受信が出来る計算機は，自組織宛だけでなく，どの宛先のメールであろうともSMTPでメール配送が行われて来ると一旦は受取り，送信先メールアドレスを解釈して再配布（中継）するという仕組みになっている。インターネット上での電子メールの信頼性を考えた時に問題となる事柄は，

・IPアドレスを偽った計算機にメールを送っていないか（経路制御のごまかし）。
・DNSで正しい配送先（IPアドレス）が答えられているか（DNSサーバの嘘付き問題）。
・SMTPプロトコルでの通信中のパケットが盗聴されていないか。
・メールが中継されて届いた場合，中継計算機での改ざん等がないか。
・計算機管理者によるユーザのメールのプライバシーが侵害されていないか。

である。これらの問題を解決する方法として，以下では，暗号化メールと電子署名を用いた秘密の漏洩や改ざんが行われない，または，行われたことを確認出来るような仕組みについて紹介する。もちろん，上記の問題のいくつかは，別の形（例えばネットワーク・通信の仕組み自体を改良するなど）の解決方法があるものもあるが，ここでは，そのことについては省略する。

5．郵便葉書と電子メール

一般の電子メールは，郵便に例えると郵便葉書のようなものと考えることが出来る。もちろん，法律によって定められている郵便局員による郵便の配送と各組織ごとの計算機がインターネット接続されて定められたプロトコル(技術的な約束事)だけによって配送を行っている電子メール配送とは異なる部分もある。その法律や管理組織の違いによる問題については後の節で述べることにする。発信者から送られた電子メールは，そのままの形で送信される。すなわち中継する各計算機では，読もうと思えば内容を見ることが出来る。しかし，各配送プログラムは，出来るだけ読まないように注意しながら配送する。配送途中にファイルとして保存されているメールは計算機管理者であれば内容を確認することが可能であるが，例え送信エラーなどで溜ったファイルであっても出来るだけ内容を読まないように心がけるべきである。また自動配送プログラムもエラーメールについては，管理者へその本文とともにエラーを伝えるのではなく，メールヘッダー（宛先等の情報）部分だけを報告するように作られている。郵便葉書の場合，郵便配達員が故意ではなくても内容を読む（目にする）かもしれない。また，組織宛の手紙を組織内で事務担当者が再配布する時に，事務担当者がその内容を読むかもしれない。だからといって，葉書が使われないことはない。手軽な葉書で十分な通信もあるのである。

6．封書の手紙と暗号化電子メール

ここでは，他人に簡単に読まれたくない文書を送ることを考える。「他人に読まれたくない。」という要求を実現するために通常の郵便では，封書に入れ簡単には見えなくする。さらに，悪質な盗み読みを防ぐために封印をし開封されていないかを確認出来るようにする。万一，他人が開封したことがわかれば，開封した人が犯罪者として法律で罰せられるので他人の封書を不用意に開封する人はいない。電子メールの場合，他人宛のメールを読んだという証拠を残す仕組みを作ることも難しいが，法的処罰が可能かどうかも微妙なところがある。そこで，電子メールでの「他人に読まれたくない。」という要求は，メール文書を暗号化するという形で実現する。

一般の手紙文書の場合，差出人を確認するには，差出人しか持っていない印鑑や筆跡によって確認する。内容が改ざんされていないことを保証するためには，封印にも当人しか持っていないはずである印鑑などを用いる。電子メールの場合，3節で述べたようにMD5と呼ばれるハッシュ関数を用いて文書から128ビットの数（MIC：Message Integrity Code）を得て，それを発信者の秘密鍵で暗号化し文書に添付する。このことを電子署名を行うと言う。受信者は計算によって発信者を確認すると同時に内容に改ざんがないことも確認出来る。

7．電子メールにおけるプライバシーについて

先にも述べたように，電子メール配送は法的に秘密が守られたシステムではない。また，社内においても会社所有の計算機を用いて行われる電子メールコミュニケーションについて，どれだけ個人のプライバシーが守られるかは保証されていない。電子メールを使うときは，ユーザはパスワードを入力して使うのでプライバシーが守られていると信じがちであるが，郵便や電話などの法律で定められた事業と異なる電子メール通信の場合，システムの管理責任はそれを所有する企業にあるために利用者のプライバシー保護についての方針はその企業が定めることになる。企業は，企業が所有するシステム内の全ての文書を（たとえ個人のメールであっても）見る権利がある。米国では，企業秘密を電子メールにより社外に送信したことにより処分された例，また，公序良俗に反するメールを多数受信していて処分された例などが報告されている。いずれも会社側が社員の電子メールを監視しており，そのメールが法廷で証拠として採用されている。電子メールを導入している組織は増えているが，組織による電子メールの監視について明言している組織は多くない。もちろん，組織によっては，監視を明言したり，監視しないことを明言している例もあるが，電子メールの運用については無方針という組織が大部分であろう。ある組織が，電子メールの監視をしないこと，個人の秘密を守ることを明言したとしても，その組織発の電子メールにより他組織に損害が出た場合(例えば，システム障害，法に違反する取り引きなど）には，システムを所有する組織としての責任がなくなるわけではない。

このように個人対個人の電子メールシステムに対して，個人の秘密を守る手段としての暗号化電子メールシステムがあるが，電子メールシステムについては，

それを実現しているシステムを所有し管理している組織が考えなければならない，個人の秘密に関する非常に複雑で難しい問題が残っている[8)9)]。

8．暗号化電子メールシステムの実際

8.1 PEMの概要

PEMは，暗号化電子メールのインターネット標準であり，1989年にインターネット標準化のための文書RFC1113-1115として紹介され現在改訂され10)，11)，12)，13)に規定されている。PEMは現在使われているインターネット電子メール環境で，データの秘密性とデータ元の認証を行うための枠組を定めたものである。PEMの実装として米国内にはいくつか製品があるが，米国の輸出規制のために日本国内で利用することは出来ない。日本国内でのPEMの実装として，WIDEプロジェクトによるFJPEMという実装があり1994年3月より公開実験が行われている[3)]。また，松崎ら[5)]，小方ら[2)]による実装もある。

PEMによる暗号化メールでは，RSA公開鍵暗号方式とDES暗号方式が用いられる。メッセージ本文の暗号化にはDESが用いられ，その鍵をRSA公開鍵暗号方式により暗号化する。発信元の認証にはRSA-MD5と呼ばれる方式が使われる。

公開鍵と個人の対応は，認証局により発行される証明書によって保証される。また，認証局に階層構造を持たせることにより，大規模組織での分散鍵保証が出来るようになっている。

公開鍵暗号システムの信頼性を確立するためには，公開されている鍵とその鍵を所有する本人との対応付けが重要である。誰かが他人になりすまして自分の公開鍵を他人の公開鍵であると公開した場合，その人はなりすました他人宛のメールを読むことが出来てしまう。その危険を防ぐために，PEMでは認証局を階層構造に作ることにより上位階層の認証局の公開鍵さえ正しく所有していれば下位認証局やその認証局で認証されたユーザの公開鍵とユーザの対応を正しく確認出来る仕組みを実現している。

ただし，認証局の設置が複数組織にまたがる場合に，その階層をどのように定め，構成するかが難しく，PEMの利用は1組織，または，1プロジェクト内でしか行われていないのが実状である。

8.2 PGPの概要

PEMでの鍵管理の繁雑さ（認証局階層という組織が先に必要）とは対照的にPGPは個人ベースで簡単に使えるという点でPEMよりも遥かに利用者が多く広く使われている。PGPも本文を秘密鍵暗号方式で暗号化し秘密鍵をRSA公開鍵暗号方式で暗号化しメッセージに付与する。ただし，PGPで利用される秘密鍵暗号方式は，DESではなくIDEA（the International Data Encryption Algorithm）と呼ばれる1991年にスイスのLaiによって考案されたアルゴリズムである。IDEAはDESの倍以上の128ビットの鍵を使い，暗号プロセスもDESの約2倍の繰り返しプロセスを用いる。しかも，DESを3回繰り返し用いるトリプルDESと呼ばれる暗号方式よりも高速であることが知られている。IDEAはDESよりもはるかに多くの数学的理論に基づいている。このことは，人々により安心感を与えるが，どのような暗号方式でも暗号が破られないことは保証出来ない。

以下に，PGPを用いて実際に電子メール通信を行う場合の例を具体的に紹介する。図4では指紋（finger print）を用いた鍵の正当性の確認例，図5では第3者認証による鍵の交換例について述べる。第3者認証による鍵の交換を用いることにより，例えば組織の長が各メンバーの公開鍵に署名を行えば，組織の長の公開

- AさんもBさんもPGPコマンドが使える計算機環境でなければならない．
- Aさんは自分のPGPの鍵を生成する．
- AさんはBさんへAさんの公開鍵を電子メール等で伝える．
- BさんはAさんから来た公開鍵が本当にAさんの物であることを確認するために公開鍵の指紋(finger print)と呼ばれる16バイトの数を電話等の信頼出来る方法で確認する．
- Bさんも同様に公開鍵をAさんに伝える．

図4　AさんとBさんの公開鍵の交換

- AさんとBさん，BさんとCさんは安全に公開鍵の交換が出来ているとする．
- AさんもCさんもそれぞれ自分の公開鍵にBさんの署名を入れてもらう．
- AさんとCさんは，お互いにBさんの署名入りの自分の公開鍵を交換する．
- Bさんを信頼出来るのであれば，Aさんと Aさんの公開鍵，Cさんと Cさんの公開鍵の対応は，Bさんの署名により保証される．

図5　Bさんの公開鍵を知っているAさんとCさんが公開鍵の交換

鍵を安全に取得している各メンバー間での公開鍵の交換は，通常の電子メール等で安全に行うことが出来ることになる。最後に，配布する公開鍵(図6)，署名だけを行った文書(図7)，暗号化と署名を行った文書(図8)の例を載せる。

```
---BEGIN PGP PUBLIC KEY BLOCK---
Version: 2.6.2i

mQBNAsCiuBkAAAECAMgxLQJhqxjWfDrA+xXkwJa8NmBBEE2m+rdS4vc/JdHs
fgruQyX4aoQ73CARIOLEwAWTWV4AXCYu2+H150EABRG0KHlvc2hpaGlybyBNa
Z3VjaGkgPHhQGNlcy5reXV0ZWNoLmFjLmpwPg==
=bP0c
---END PGP PUBLIC KEY BLOCK---
-----------------------------------
Type bits/keyID    Date       User ID
pub  512/E1F5E741 1995/11/10 Yoshihiro Mizoguchi <ym@ces.kyutech.ac.jp>
     Key fingerprint = AE 66 FD 46 63 E3 76 DC  31 06 64 E6 72 1C C7 36
-----------------------------------
```

図6　公開鍵（pgp -kxa）とその指紋（pgp -kvc）

```
---BEGIN PGP SIGNED MESSAGE---

暗号化電子メールシステムの現状

---BEGIN PGP SIGNATURE---
Version: 2.6.2i

iQBVAwUBMVAujVwmLtvh9edBAQEN1QH9F9QQuq2yfEJawYA+c3+ptfTc6Sttux
C3rWf4LYn4xZVWJaLbXhWK/ditp23HN4VyEaDkXG1qjEypJibyFyCQ==
=kQb6
---END PGP SIGNATURE---
```

図7　署名だけを行った文書（pgp -sa）

```
---BEGIN PGP MESSAGE---
Version: 2.6.2i

hEwDjbjRspWSDV0BAf9J4+58HirES/c/p3LGpeXseX+G1E7r3IbdP0nGT1baWCeY
/D4aZXZeSIaGRjj/MUQDHa9tfpd3gcaBk+dun9jcpgAAAJIlfngG1tNN3cspUmNA
JmMxcqvuEPL7rG1297/8wh3v2lPfwOA7Qq3NgfklqpeuGuCn2vHQaWkOyt3zfpi9
Q2cQ4LRL2cGGI1kG2gjmxEwZQndGf8Ml+ZJiJ36Zax7W8xQlqZkLON//w8b7PPw
jLvvS7LcT0hqVoQQ71QRw9aQcQUo3AOB6dhD/p0XZA8ClGcpHwZqdpowhb8=
=A4T3
---END PGP MESSAGE---
```

図8　暗号化と署名を行った文書（pgp -sea）

9. おわりに

暗号方式の概要とそれらを利用した暗号化電子メールシステムの実例について紹介した。暗号化電子メールを使うにあたって最も重要なことは，「人と公開鍵との対応づけを安全に知ること」と「計算機中に保存されている秘密鍵の漏洩を防ぐこと」である。また，7節で簡単に触れたが，電子メールだけでなく管理体制の全く異なる複数組織が通信プロトコルという技術的な約束だけで接続し通信しているインターネットの世界において倫理的，道徳的，法律的に整備していかねばならない問題も多く残っている。

参考文献

1) 池野信一，小山謙二．現代暗号理論．コロナ社，1983.
2) 小方学，溝口佳寛．暗号化電子メールシステムの実装と課題，電気関係学会九州支部連合会大会論文集，p.840(1993).
3) 菊地浩明，森下哲次．暗号化電子メールPEM(Privacy Enhanced Mail)の実装と課題，情報処理学会第46回全国大会，1，p.99-100(1993).
4) 松井甲子雄．コンピュータのための暗号組立法入門．森北出版，1986，166p.
5) 松崎なつめ，原田俊治，宮地充子，館林誠，多田信彦．暗号化電子メールシステム．暗号と情報セキュリティシンポジウム論文集，2C，1993.
6) B. Schneier.（力武健次監訳，道下宣博訳）E-Mailセキュリティ，オーム社，1995，411p.
7) Rivest, R.L.; Shamir, A.; Adleman, L.A method for obtaining digital signatures and public-key cryptosystems. Communications of ACM. Vol. 21, No. 2, p. 120-126 (1978).
8) Sipior, J.C.; Ward, B.T. The ethical and legal quandary of email privacy. Communications of ACM. Vol. 38, No. 12, p. 48-54 (1995).
9) Weisband, S.P.; Reinig, B.A. Managint user perceptions of Email privacy. Communications of ACM. Vol. 38, No. 12, p. 40-47 (1995).
10) Linn, J. Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures?, RFC 1421. 1993.
11) Kent, S. Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management, RFC 1422. 1993.
12) Balenson, D. Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers, RFC 1423. 1993.
13) Kaliski, B. Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services, RFC 1424. 1993.
14) Zimmermann, P.R. PGP User's Guide. 1991.

Special feature: Computer Security. Privacy Enhanced Mail System, Yoshihiro MIZOGUCHI (Dept. Control Engineerings and Science, Kyushu Institute of Technology. (680-4, Kawazu, Iizuka-shi, Fukuoka 820))