中澤ゼミ

プライベート･コミュニケーションの安全性確立 ～PGP の普及に向けて～

A1200327 馬場奏恵

1 はじめに

近年，ネットワークインフラの整備が進むにつれて，情報漏洩事件も頻発するようになった．2003 年 11 月には，個人情報[1]保護法が成立して以来最大規模となる，メールマガジン購読者 18 万人分の個人情報が大手コンビニチェーンから流出した．また，複数の大手システムインテグレータ[2]から受託先企業のシステムに入っていた個人情報が漏洩する事件も発生している[1].

このような事件が多発していることから，個人が自分の個人情報を企業などに提供する場合，慎重に取り扱わなくてはならない．何の対策も施さない状態で電子メールを送信したり，データを保存したりすることが情報漏洩につながるからである．これらを防止するためには，データを第三者に把握されないようにすることが必要である．

最近では，ネットショッピングやインターネットオークションなどで個人情報が入った電子メールを送信する機会が増加している．このため電子メール上でのセキュリティを保護するための暗号ソフトウェアが必要になる．しかし，インターネットユーザーのセキュリティ意識は未だ不十分な点や，暗号の仕組みが理解しにくいという点から暗号ソフトウェアは十分に普及していない．

本研究では，個人情報の保護という観点に着目し，電子メール暗号化ソフトウェア PGP（Pretty Good Privacy)を普及させるための方策について議論する．具体的には，PGP の暗号システムや普及が進まない原因を調査し，広報活動でセキュリティ意識を高めさせ，インターフェイスの改善で操作しやすい PGP を提案していく．

2 PGP の暗号システム

2.1 PGP の暗号方式[1][2]

PGP とは Pretty Good Privacy の略で，1991年に Philip R. Zimmermann が作成した．これは，共通鍵暗号方式と公開鍵暗号方式を組み合わせた電子メールに用いられる暗号システムである．

共通鍵暗号方式は，暗号化と復号化で同じ鍵を使う暗号方式である．扱いが簡単であり，処理速度が速い半面，相手先ごとに固有の鍵を作成しなければならないこと，あらかじめ安全な方法で相手に鍵を渡さなければならないという問題がある．

もう一つの公開鍵暗号方式は，暗号化と復号化を公開鍵と秘密鍵という異なる２つの鍵によって行う方式である．公開鍵は，暗号文を作り出す鍵であり，通信相手に提供する鍵としてインターネット上でも通信できる．だれもがこの公開鍵で暗号文を作成して送信することができる．暗号文の受け手は，秘密鍵で復号化する．ここで秘密鍵とは，公開鍵とペアになっており，本人だけが利用できるように厳重に管理されるものである．共通鍵暗号方式に比べて処理速度は極めて遅い．しかし，共通鍵暗号方式で問題になっていた鍵の配送問題が公開鍵暗号方式で解決できる．

PGP の暗号化にはこれら両方の暗号方式を利用しており，公開鍵暗号アルゴリズムである RSA と共通鍵暗号アルゴリズムである AES を併用している[3]. PGP の鍵タイプには，Diffie-Hellman/DSS 鍵方式，RSA 鍵方式，RSA Legacy がある．Diffie-Hellman/DSS 鍵方式は 5.0 以降で採用されたタイプなので，通常はこれを選択する．RSA は 7.0 で採用された新しい鍵方式だがそれ以前のバージョンとは互換性がない．RSA Legacy は古いタイプの鍵で 2.6.3i とやりとりする場合に使用する．新しいタイプほど安全性が高いが，バージョンとの互換性が低下してくる．鍵サイズは 1024～4096 バイトであるが，通常サイズは 2048 バイトが適当である．鍵サイズが大きいほど暗号の解読が難解になるが，暗号処理は遅くなる．

2.2 PGP の機能

PGP は現代の暗号ソフトウェアに必要な機能をほぼ備えている．それは，デジタル署名，証明書作成，圧縮，大きなファイルの分割と結合，鍵リングの管理である．鍵リングの管理とは，生成した自分の鍵ペアや，入手した公開鍵を管理することである．鍵を管理しているファイルを鍵リングと呼ぶ．

2.3 信頼の網[4]

---

[1]氏名，生年月日または個人別に付けられた番号，記号その他の符号，画像や音声によって個人を識別できる情報である．他の情報によって個人を識別できる情報も含む[2].

[2] 顧客の業務内容を分析し,問題に合わせた情報システムの企画,構築,運用などの業務を一括して請け負う業者のこと．システムの企画,立案からプログラムの開発,必要なハードウェア,ソフトウェアの選定,導入,完成したシステムの保守,管理までを総合的に行う．

2.3.1 信頼度と有効性の決定

PGPは認証局[3]を利用せず，個人同士で公開鍵の信頼性を高める「信頼の網」という仕組みを持っている．これは，公開鍵が本当にその人のものかどうか，改ざんされたものでないかを信頼させるために，公開鍵に本人や信頼し合っている人が署名を入れることができる機能である．こうしてユーザーは，相互に認証し合う信頼性の高い公開鍵を鍵リングとして所持することができる．

鍵リングに登録される公開鍵には有効性(validity)と信頼度(trust)という値がある．有効性とは，ある公開鍵が本当にその公開鍵のユーザーで示される人に属しており，改ざんもされていないと信頼できる度合いである．有効性の値は高い順から，

- complete（完全に有効）
- marginal(最低限有効)
- untrusted(無効)
- undefined(未定義)

となっている．有効性が complete でない場合，その公開鍵が偽者である可能性を示唆するために，その公開鍵が利用される度に PGP は警告を発する．信頼度とは，ある人 A が他の人 B を紹介する際に，紹介者としてどれだけ A を信頼するかという度合いである．信頼度の値は高い順から，

- ultimate(絶対的に信頼する「自分自身」)
- complete（完全に信頼する）
- marginal(ある程度信頼する)
- untrusted（信頼しない）
- unknown（未知）
- undefined（未定義）

となっている．信頼度は自分で設定し，有効性は計算により算出される．公開鍵には複数の人が署名可能であり，それぞれの信頼度の合計から有効性を決定する．

2.3.2 認証局を利用する場合との比較

PGP の場合，前述した信頼の網を使用するため，認証局という第三者的存在を必要としない．認証局を使用すれば，相互に認識していない人とも通信が可能であるが，認証局に公開鍵の署名をする申請料がかかる．一方，信頼の網の長所は，認証局のシステムの維持，管理ということが必要ない．そのため，コストもかからず，認証局への申請なども必要ないため導入も容易である．短所としては，信頼の網から秘密にしておきたい他企業との関係が証明書を提供した相手に明らかになってしまう恐れがあるため，企業においては利用しづらい点が挙げられる．

[3]電子商取引などで使われる電子的な身分証明書を発行する機関．

また，秘密鍵をなくしてしまった場合は不正に利用されるのを防止するために，公開鍵を無効とするのだが，それを伝達するのが困難であることも短所として挙げられる．これらの特徴から，PGP は友達同士などのプライベート･コミュニケーションのセキュリティを確保するのに優れた威力を発揮することが分かる．

3 PGP の現状

3.1 普及率

PGPは無料で利用することが可能であり，使いやすさも開発初期と比較して格段に改善されてきている．また，普及率が一番高いメーラーである Outlook[4]でのサポート状況は，ほとんどのバージョンがPGPをプラグイン[5]できるようになっている[5]．しかし，普及率は一向に伸びていない．日本インフォメーションセンターJPNICが設立しているPGP Public Key Serverに登録されている鍵の総数が，2001 年の時点では 1,595,374 個であった[6]．また，2001 年の日本のインターネット利用者が約 4,383 万人[7]であることから，インターネット利用者の約 3.6%しかPGPを利用していないのが現状である．

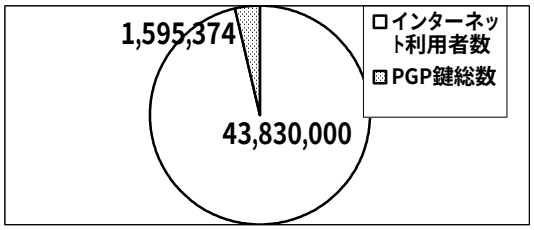

図 1. PGP Public Key Serverに登録されている鍵の総数

それに対し，ウィルス対策ソフトは 2003 年の日本のインターネット利用者が約 6,124 万人のうち，約 76.3%の人が導入･利用していることが明らかにされている[7]．

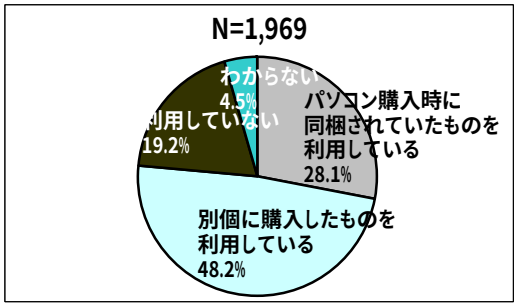

図 3.ウィルス対策ソフト利用の有無

このように，同じ被害対策ソフトでも普及率には格

[4]Microsoft Corporationの製品．

[5] アプリケーションソフトに追加機能を提供するための小さなプログラム。

中澤ゼミ

差がある．ウィルスは被害との因果関係が明確であるため，セキュリティ意識を感じてウィルスソフトを購入するのであろう．一方，PGP の普及率が低いのは，ユーザーのセキュリティ意識が低いこと，導入･操作を面倒にしてしまい，利用しないことが原因と考えられる．

3.2 ユーザーの意識[7]

1998 年から 2003 年までの日本国内のインターネット利用者推移を見てみると，5 年間で飛躍的に増加しており，2003 年 12 月には 6 千万人以上となっている．その中でセキュリティに対する不安を持っている利用者は 75%である．また，実際に被害に逢っている人も 60%と，かなりの割合を占めている．しかし，その被害内容には電子メールの盗聴や改ざんは見当たらない．これは，個人情報が漏洩していたとしても，電子メールからの漏洩だという確証を得ることが困難であることが原因であろう．

4 普及策

これらのことを踏まえて，普及率を上げるには次の対策が必要である．

4.1 インターネットユーザーのセキュリティ意識を高める

電子メール盗聴は，盗聴対象者のメールボックスから電子メールを取り出す方法や，盗聴対象者のメールボックスが置かれたサーバーから，盗聴者のサーバーへ電子メールのコピーを転送するなど，盗聴者がとても楽で手間がかからない方法で盗聴ができる．これらの盗聴には簡単な方法でできてしまうものもある．

また，個人情報など第三者が盗聴して利得となる情報を電子メールで送る機会が将来増加してくる．例えば，ネットショッピングをする際，ほとんどのサイトが SSL に対応しているため，このとき情報が漏洩することはない．しかし，顧客宛の受取確認メールには,何の暗号システムも使われていない．それにも関わらず，受取確認メールには，配送先の確認として顧客情報が書かれているので，非常に危険である．別の例として，インターネットオークションでは，品物が落札したときに出品者と落札者の間で,個人情報を送り合うメールのやりとりが生じる．また，最近の就職活動では，求人者が企業にアクセスする方法として,電子メールが主流になってきている．このメールにも個人情報が記載されており，危険性が高い．これらの方法で個人情報が他の人に知られてしまえば，情報が世間体に出回り，悪用される恐れがある．

これらのことから，電子メール盗聴の仕組みや，個人情報を電子メールで送信する機会が増えることを宣伝･広報し，インターネットユーザーのセキュリティ意識を高めることが必要となる．

4.2 PGP の利便性を高める

4.2.1 導入の手間を省く

インストールやダウンロードが面倒で PGP を使用しないということも普及を妨げる原因の一つである．そこで，その導入の手間を省くために，メーラーに始めから標準で PGP を組み込んでおくという方法が考えられる．ダウンロードにはファイルサイズが大きくて導入できない場合もあるし，インストールには設定などに時間がかかる．それを考慮すると，時間も手間も大幅に削減できる．

4.2.2 初心者でも使いやすいソフトウェア

現在の PGP のインターフェイスは，初心者には敷居の高いものとなっている．鍵や暗号について十分な知識を持たない人は，それらの語句が画面に表示されただけで利用を諦めてしまうであろう．そこで，表示する語句には「鍵」「暗号」などの語句は登場させないで，別の語句に言い換える．例えば暗号化は「メッセージを保護」，公開鍵は「メッセージを保護するためのもの」など，馴染みやすい語句にする．

さらに導入時の設定手順を簡略化するために，暗号化と復号化に必要な公開鍵と共通鍵の鍵ペアをインストール時に自動的に作成するようにする．この際ユーザーは，名前･メールアドレス･秘密鍵で復号化する時に必要なパスフレーズを入力するのみの作業だけとなる．また，ユーザーの負担削減のため鍵サイズや鍵タイプは標準値のままで設定しておくことにする．

最も重要な鍵の管理については，図 3 のようにユーザー各々に公開鍵を添付してメールで送信するという手間を全て自動化する．具体的には，A がメーラーのアドレス帳に PGP ユーザーを登録する度に，公開鍵をその人のアドレスに自動送信するようにする．B は公開鍵が送信されてきたら A の公開鍵ということを確認して登録する．A の公開鍵を B が受け取るときに，その鍵の署名者が B の知らない人物である C であったとする．C の信頼度は未定義なので，A の信頼度を決定するときに，「この鍵は安全かどうか分かりません」というメッセージダイアログを表示させる． B は A の公開鍵を「信頼しない」に設定すると，A の公開鍵の有効性は無効になり，逆に「信頼する」を選択した場合には，A の公開鍵は有効となる．A の公開鍵が有効となっている場合に，D の公開鍵を B が受け取るとき，信頼している A が署名していれば，A の信頼度は「信頼する」に設定さ

れているのでメッセージダイアログには「この鍵は安全です」と表示される．このように信頼の網の設定も簡略化される．そうすると，公開鍵登録完了メールが公開鍵送信元 A へ自動送信されるシステムである．

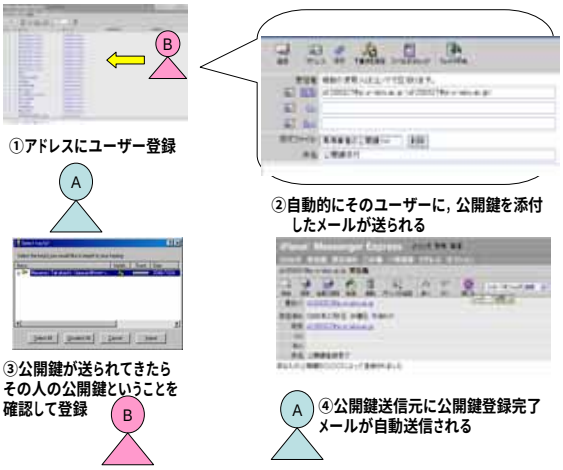

図 3.公開鍵の公開　新システムの流れ

また，暗号化では宛先の所にユーザーを入れれば，すぐに本文が暗号化される仕組みにする．復号化でも，暗号化されたメッセージを開いた途端に，パスフレーズ入力を促すダイアログが出てきて，入力すればすぐに復号化する仕組みにする．署名も同様に，ユーザーの入力や設定手順を少なくし，初心者でも利用しやすい操作手順とする．ただし安全性の面では，初心者が操作していることの詳細を理解できていないことや，信頼の網の設定基準を減らしたことにより生じる公開鍵の悪用が生じやすくなることにより，低下する可能性もあるだろう．

5 結び

1999 年 6 月 1 日に通信傍受法が可決･成立し，なおいっそうプライバシーについて重要視されるようになった[10]．しかしプライバシーを守りたいと思っていても，今までの暗号インターフェイスは敷居が高く，一般ユーザーには暗号ソフトウェアは使いにくいものであった．

本研究では，PGP の長所･短所をまとめ，その長所をどう生かすか，短所をどう改善するか議論し，普及策を考えた．提案した PGP のインターフェイスの敷居を低くし，複雑な操作を少なくしたことで，使いやすいものとした．また，盗聴の仕組みや，危険性などを宣伝･広報してセキュリティ意識を高めて PGP の必要性を感じさせることも重要である．提案した PGP を通じて暗号がどういうものであるのか認識されることは重要である．

誰にでも使いやすい本システムであるが，検討すべき課題もある．これまで暗号ソフトウェアのユーザーと言えば，PCのヘビーユーザーであり，PGPの仕組みを十分に理解していたからこそ，高いセキュリティを保つことができていた．しかし，初心者がソフトウェアの詳細を知らないまま使用していれば安全性が低下する恐れがある．また，コスト面ではPGPを非商用で利用する場合は無償だが，商用で利用する場合はライセンス料が発生する[6]．それをメーラーに組み込むことでライセンス料が発生し，メーラーやOSの価格に影響を与えることも考えなくてはならない．

今後，情報化社会がより進めば，人々のコミュニケーションの仕方も電話や手紙よりも手頃で安価な電子メールが増加していくことが予想できる．近い将来，全ての電子メールに記されるメッセージを暗号化し，セキュリティ意識を高める必要性が出てくることになるであろう．

6 参考文献

[1]http://itpro.nikkeibp.co.jp/as/ilp2/feature/，情報漏洩対策ソリューション特集,日経 BP 社
[2]http://www.jisc.go.jp/app/pager?id=6327,JIS データベース JISQ15001,JIS 日本工業標準調査会
[3]結城浩,暗号技術入門 秘密の国のアリス,日経 BP 社,2003 年 9 月
[4] http://pgp.iijlab.net/pgp/trust.html,信用モデル「信用の輪(web of trust)」のひみつ,IIJ 技術研究所
[5]http://www.cla-ri.net/pgp/pgp04.html,PGP,PGP/MIME への Windows 版 MUA のサポート状況,PGP User's manual for Windows
[6]http://pgp.nic.ad.jp/docs/2001.txt,2001 年は PGP.NIC.AD.JP がどのように使われていたか ,PGP Public Key Server
[7]http://internet.impress.co.jp/hakusyo/,インターネット白書 2003,Impress 社
[8]http://www.incidents.gr.jp/9908/mizoguchi990807/mizoguchi990807.htm,問題だらけの電子メール盗聴を許すな！,The incidents, 日経BP社
[9]http://www.nsd.co.jp/pgp/price.html,PGPPrice,PGPProducts,株式会社日本システムディブロップメント
[10]http://www.moj.go.jp/HOUAN/SOSHIKIHO/MONITOR/refer01.html,犯罪捜査のための通信傍受に関する法律，法政省

[6] IDEAアルゴリズムはMicrocript社，AESアルゴリズムはNIST（米国標準技術局），RSAアルゴリズムはRSA社にライセンスがある．