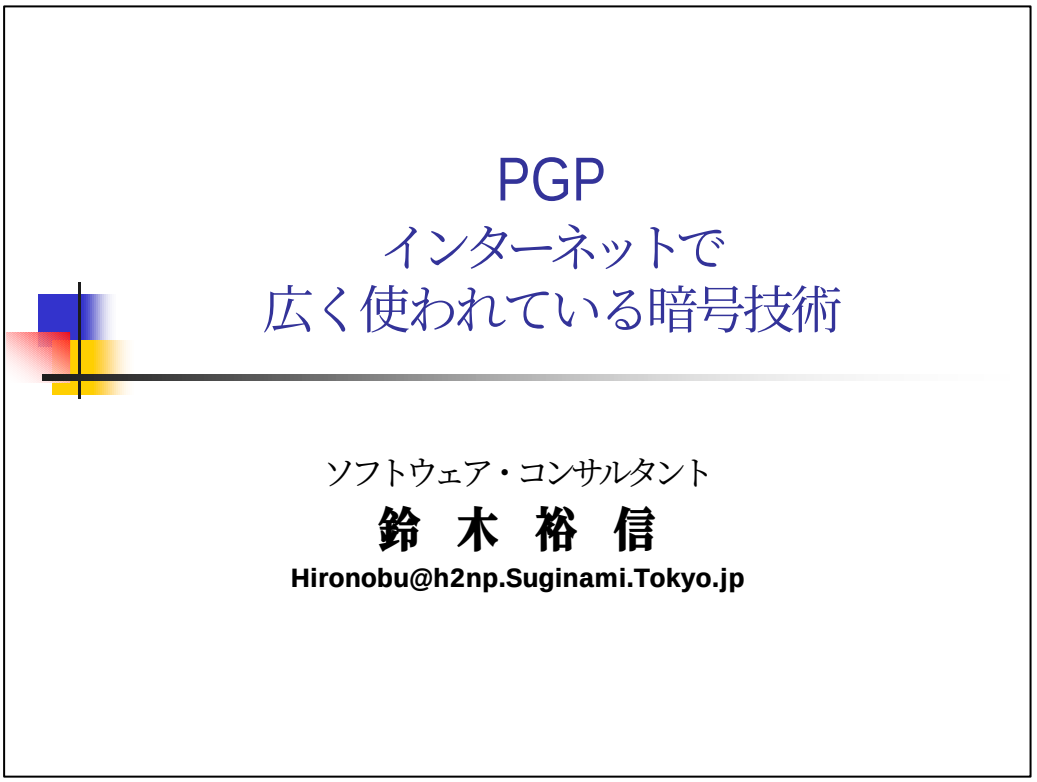


PGP
インターネットで
広く使われている暗号技術

ソフトウェア・コンサルタント
鈴　木　裕　信
Hironobu@h2np.Suginami.Tokyo.jp

インターネット上における情報

- ネットワークとネットワークが限りなく接続している空間
- 通過するすべてのネットワーク上の安全性を検証するのは不可能

PGP(プリティ・グッド・プライバシー)は汎用の暗号ソフトウエアである。今、インターネットの中でこのようなツールを必要としているデータ交換は色々あるが、一番使われているのは暗号メールである。

なぜ、このようなセキュリティが必要なのか。

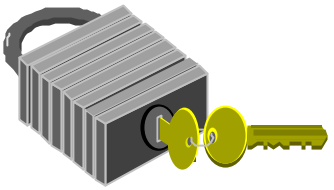
ネットワークとネットワークが限りなく接続しているコンピューターネットワーク空間がインターネットである。つまり通過するすべてのネットワーク上の安全性を検証するのは不可能だと言える。

たとえば私が、ヨーロッパにメールを出すときに、どういう経路でメールが流れているかはほとんど事前に検証することは不可能である。私が家から出したメールは、多分NTTのOCNに行き、そこからNTTのアメリカの子会社へ、さらにアメリカ国内のネットワークを通ってヨーロッパへ行くだろう。ヨーロッパのネットワークを経由して、ヨーロッパの大学の友達へメールが届くはずだ。

これのどこに落とし穴があるのかユーザーには分わからない。結局、自分自身でデータを守るしかない。もちろんネットワーク全体を守ることは不可能であるから、どう守るかということになる。一番簡単なのは、コンテンツ自体を暗号で守ること。そこにPGPによるセキュリティのニーズが出てくるのである。

情報セキュリティとして求められるもの

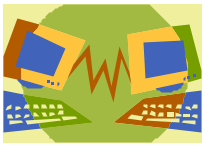
- 秘匿性
  - 通信している内容を第三者に知られない
- 完全性
  - 通信した内容を改竄から守る
- 認証性
  - なりすましを防ぐ



ここでは大きく三つに分類している。「通信している内容を第三者に知られない秘匿性」、「通信した内容を改ざんから守る完全性」、「なりすましを防ぐ認証性」である。秘匿性、完全性までは古くから必要性が認識されていたが、認証性についてはインターネット時代になって新しく注目をあびるようになった。

インターネットでは誰でもがネットワークを使えるので、途中で誰が改ざんしたかとか、誰がなりすましているかは、ネットワークの向こうなので解らない。単にメールに書かれた自称○○になってしまうわけである。これらは認証技術を使って防がなければならない。

データをどのレベルで守るのか



- データパケットのレベル
  - IPSec
- 通信を行っているセッションのレベル
  - SSL・SSH
- コンテンツレベル
  - PGP・S/MIME

http://www.imc.org/smime-pgpmime.html

コンピューターでの通信では、いろんなレベルで守ることが可能である。まずデータパケットレベル。一番下のIPのデータ(一個一個砕いていくデータ)のレベルで守る方法がある。IPVer6の中に組み込まれるIPSecと呼ばれるものである。これが良くVPNなどに使われる技術だ。

アプリケーションが通信を行っているセッションのレベルで守る方法もある。SSHとかSSLである。SSLを例にあげよう。エレクトリックコマースなどのサイトで、クレジットカードで支払う場合、Webブラウザの下の方に鍵がかかったようなマークが出る。それはセッションレベルでデータが守られている印しである。盗聴や改ざんができないようになっている。

次にコンテンツレベル。つまりメールなどの中味を守る方法である。これがPGPであり、S/MIMEである。MIMEとはメールの中にデータとかファイル、画像、音声を入れて送るフォーマットである。たとえばOutLookとかネットスケープなどでメールを出すときにはMIMEが使える。S/MIMEは業界標準でいろいろなツールがサポートしているのであるが、実はインターネット全体で見るとPGPの利用者が多い。皆が支持するのは何故かPGPである。双方の比較に関しては、http://www.imc.org/smime-pgpmime.html が参考になる。これを見ると利用者やシェアの違いが書かれている。

電子メールでの暗号化

- PGP
  - 汎用の暗号プログラムを応用し電子メールに利用している
    - プレインテキスト
    - アタッチファイル
- S/MIME
  - 電子メール専用の暗号化プロトコル
- PEM
- その他独自システム

暗号の世界ではPGPとS/MIMEが大半のシェアを占めている。

PGPは汎用の暗号プログラムである。それを電子メールに対して応用している。たとえばメールのストラクチャを変えずに、データだけを暗号化してさらにアスキーコードの羅列に変換することも可能であるし、自分で一回暗号化したファイルを、そのままアタッチの形で送ってしまう方法もある。

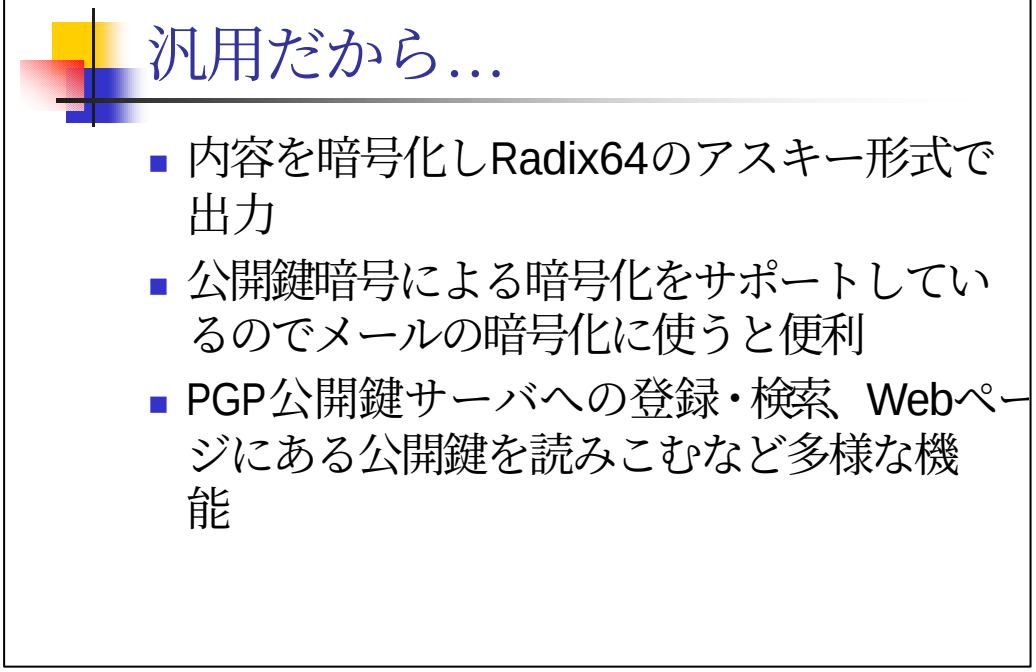
このほかにPEMというものもある。これも電子メール専用の暗号プロトコルである。ところがあまりはやらずに廃れてしまっている。RFCという形で標準化されたが、これは全然はやらなかった。

その他独自のシステムもある。大手のNTTからベンチャー企業まで日本でも数種類ある。導入している会社もあるようだが、内容もピンからキリまであるようで安全性やどれだけポピュラーなのかは不明である。

PGPとは何か

- 汎用の暗号プログラム
  - 共通鍵暗号
  - 公開鍵暗号
  - 電子署名
  - 鍵交換
  - その他の気の利いた周辺機能

繰り返すが、PGPは汎用の暗号ソフトウェアである。共通鍵暗号(一つの鍵で暗号化する)と公開鍵暗号の二つの鍵を使って守る。電子署名、鍵交換、そのほかにも気のきいた周辺機能もある。そういう点でも受けていると思う。たくさん使われているので、たとえば文字を変えたり、圧縮したり、鍵の検索が楽など、ユーザーニーズを反映して細かいところで気がきいている。



中味を暗号化してbase64のアスキー形式にして出力してくれる。それをメールに貼り込んで送れば、誰にも読めない形で内容を送ることができる。相手はこの意味不明な文字列を、元に戻して読むことができる。公開鍵暗号なので非常に便利なのである。

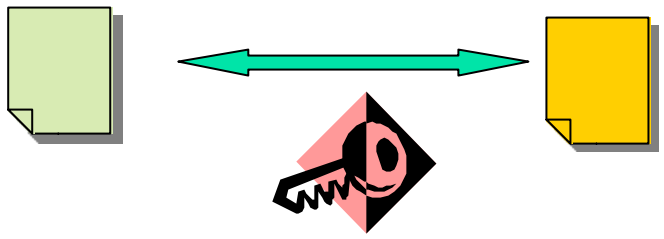
もう一つ便利なのが、PGP公開鍵サーバーへの登録、検索、あるいはWebページにある公開鍵を読み込むことができる点である。たとえば皆さんに暗号化してもらうために私の鍵ををお配りしなければならない。いちいち会って渡すのは大変だから、いったん鍵をプールするようなサーバーに入れておくとか、鍵をWebページに埋め込んで、PGP鍵を自動的に読み込んでもらうこともできほうが楽である。こうして多人数の間でメールの交換が楽にできるわけである。

PGP公開鍵サーバーを日本で唯一、行っているのは私の管理しているサーバーである。現在鍵は62万鍵ある。データベースのサイズは、データだけで６GBある。一回ダンプしてバックアップし、元に戻そうとすると二晩かかる。毎日、何千というレベルでどんどん増えている。２年前までは、この鍵が10万もなかった。最近２年間で50万ぐらい増えている。３年後には100万を超しそうな勢いである。データ数も10GB、20GBへと拡大していくだろう、と推測している。

公開鍵サーバーは、大きく分けて二通りある。商用のものと、フリーソフトとして作っているものである。私はフリーソフトに協力している。全世界の鍵を同期させているので、アメリカのサイトに登録すると自動

共通鍵暗号

- 暗号化する時の鍵と復号化する時の鍵が同じ暗号方式
  - 長年にわたり暗号といえばこの方式
  - 高速に処理ができる



共通鍵暗号とは、暗号化するときの鍵と復号化するときの鍵が同じという方法である。公開鍵暗号ができるまでは、有史以来、暗号といえばこの方法であった。利点は非常に高速に処理ができることである。データを鍵一つで暗号化し、同じ鍵を使ってもとに戻す。

公開鍵暗号

- 暗号化する鍵と復号化する鍵が違う暗号方式
  - 概念：１９７６年W. Diffie,M.Hellman/同時期にRalph Merkle
  - RSA暗号：１９７８年R. Rivest, A.Shamir, L. Adleman
  - ElGamal暗号：１９８５年T.ElGamal
  - 楕円暗号：１９８５年N. Kobliz/V.S. Miller

公開鍵と秘匿鍵を持つことの利点

- 秘匿鍵を持つものしか復号化できない
  - 秘匿鍵が他者から漏れ出す心配がない
  - 鍵配送の問題がなくなる
- 公開鍵（暗号化を行う鍵）は1つで良い
  - 複数の秘匿鍵を管理する必要がなくなる

秘密の情報をやり取りするメンバーと言えば、実際には限られた範囲である場合はほとんどである。

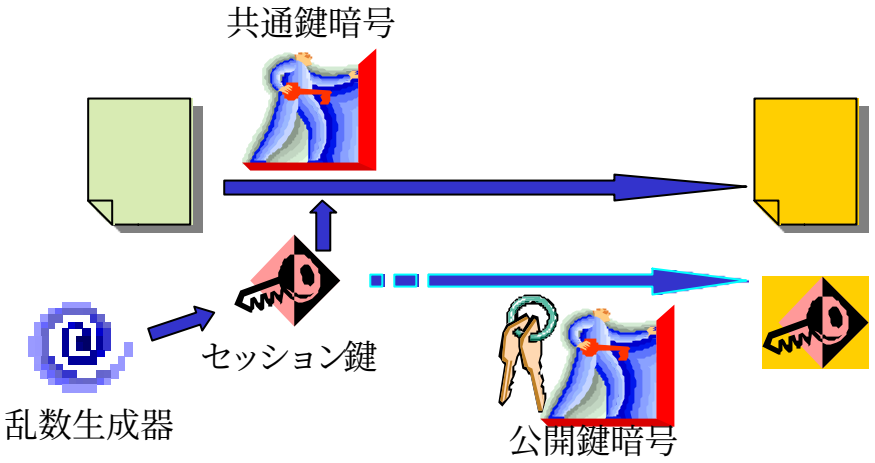
たとえば西海岸にあるコンピューターリテラシーという書店は、自分のWebページの上に、PGP公開鍵を置いている。「この鍵を使って、暗号化してメールを出してください」といったシステムを取り入れているのだ。このように小回りが効くのでSOHOビジネスでは非常に重宝している。

最新のPGPは、専用の認証サーバーとかX.509のフォーマットをサポートしている。大企業のエンタープライズコミュニケーションにも、商用のものが使えるようになっている。

商用PGPはネットワークアソシエイツが出している。エンタープライズコミュニケーションなどいろんなビジネスをサポートできるように、いろんなツールが出ている。

共通鍵暗号と公開鍵暗号

- 暗号ツールではこの両者の組み合わせ

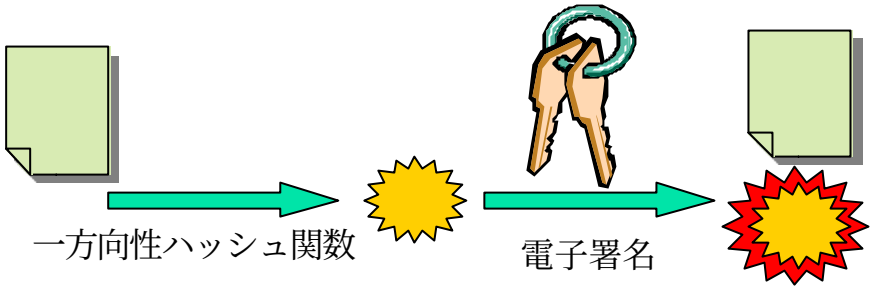


電子署名

- 改竄の検出
- 誰が署名したのかがわかる

電子署名は２つの技術が使われる

- 一方向性ハッシュ関数
  - データの“指紋”を作る
- 電子署名アルゴリズム
  - “指紋”の改竄を防ぐ

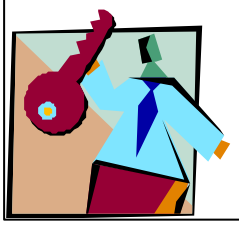


鍵交換

- 相手から公開鍵をもらう
  - 相手に暗号メールを送るため
  - 相手の電子署名をチェックするため
- 入手した公開鍵は本当に相手のものか

どう鍵を保証するか

- 直接本人に確かめる
  - 相手が多くなれば多くなるほど手間が増える
- 第三者が保証する
  - 自分は保証先を信じる
    - 局方式
      - 中心となる組織を作りそこが保証に関する手続きを一手に引き受ける
    - 信頼チェーン
      - 自分の信頼できるものが保証するのでその保証を信じる



PGP

- 1991年Philip Zimmermanによって最初のバージョンが作られる

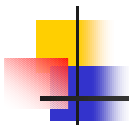
PGPはフィリップ・ジママンによって91年に作られた。彼はニュージャージーで1954年に生まれ、フロリダの大学を卒業してソフトウエアのフリーのプログラマーとなった。社員として企業に勤めたことがない。彼が活動の拠点にしていたのは、コロラドのボルダーという小さくてきれいな街である。コロラド州立大学のコンピューターサイエンス学科があり、ハイテクな街で出版、ソフトウエア関連企業が多くある。IBM、HPなどの研究所もある。

モチベーション

- FBIが反核団体のパソコンを違法押収し中にある情報を勝手に盗み出した。

彼がどうしてPGPを作ったのか。

最初、フィリップ・ジンマーマンは暗号の専門家ではなかった。あるとき、FBIが反核団体のパソコンを違法押収し、その中にあるメンバーリストを持っていってしまった。それを守るためのプログラムを作ったのがきっかけであった。彼自身、反核の活動家で、過去に三度ほど核実験反対のデモで逮捕されている。



バージョンの変遷

- 1991年 バージョン1．0
  - RSA＋Bass-O-Magic
- バージョン2．0(2.6.3i)
  - RSA+IDEA
- バージョン2．6
- バージョン5．0
  - DH/DSS+CAST/(RSA,IDEA)

91年に最初のバージョン1.0を出している。公開鍵暗号方式はRSAである。これはスタンダードなものだが、共通鍵暗号は彼が考えたBass-O-Magicというものを使ったそうだ。共通鍵方式にはDESというものがあるが、それを使わなかったのは、それは米国政府が作ったもので、秘密の扉が隠されているかもしれない、と考えたからしい。

しかし残念なことにBass-O-Magicは、暗号としての役目を果たす内容のものではなかったようである。

そこで改良を加えて出来上がったのが、バージョン2.0である。ヨーロッパで作られ、スイスのアスコムという企業がパテントを持つIDEAという共通鍵を採用している。これは非常に良くできたものであった。

ここまで彼はパテントに関して無神経だったようである。RSAに関してはパテントを持っていたRSA社との間で争いが起こる。パテントの一部を持っているMITが中に入って、RSA-REFというライブラリーを使えばRSA社は認める、という形で両者の調整をつけた。

ただしRSA-REFに自分で手を加えられなくなってしまった。さらにRSA-REFは米国外へ持ち出せない、という条件も付けられてしまったのである。性能はRSA社の商用バージョンよりも、鍵の決め方とか暗号の処理の仕方とか50%は性能が落ちる、と言われている。

IDEAは非商用に限ってフリーであるが、商用にはライセンス料が必要な決まりになっていた。そこで登場したのが2.6.3iというものである。RSA-REFをヨーロッ

現在のバージョン

- PGP 6.5
  - Network Associates, Inc
- GNUPG 1.0
  - GNU version of PGP
  - Werner Koch

現在はバージョン6.5である。これの開発はネットワーク・アソシエイツで行われている。フリーであることには変わりない。アメリカではつい最近まで、暗号の輸出規制があった。そのためアメリカの人たちは、ソースコードをプリントアウトして、何万ページという本にしてヨーロッパへ持っていき、元のソフトウエアに戻したわけである。最初は単純にプリントアウトしたものだったが、後にエラー補正の入ったプリントフォーマットを考え、それでソフトウエアの入ったコードを印刷した。それをスキャナで読み込むわけである。

余談だがこのやり方はデータ保存という観点からは合理性がある。私たちはすぐ、光ディスクやフロッピーにデータを入れようと思うが、しかしよく考えると、紙のほうが情報の寿命が長いように思えるのである。光ディスクとかフロッピーディスクは５～７年でフォーマットが変わる。アルゴリズムさえ解っていると、どんな時代でも紙は読み込むことができる。

ネットワーク・アソシエイツによって、どんどんと商用化が進んだ。処理は複雑化し、機能も付け足され、売り物としての価値を高めるための周辺システムなどもたくさんでき始めている。

一方、ネットワーク・アソシエイツの意向に左右されずに、シンプルで自分たちで手を加えられるものとしてドイツで作られたのがGNUPG1.0である。これを作っているワーナ・コッホが11月の始めに東京へやって来て、GUNPGについて講演した。

PGPとZimmerman

- 不正輸出疑惑をかけられる
- RSAREFのライセンス問題
- PGP Incの設立とNAIへの吸収合併
- 数々の人権団体からの表彰

映画や本が作れるほどジママンとPGPは数奇な道を歩んでいる。91年に不正輸出疑惑が起こるが、それは自分が作ったプログラムを友達に渡したからである。その友達の中の誰かがBBSに乗せた。そこからダウンロードした誰かがインターネットのニュースに掲載して全世界に広まった、というわけである。それによって暗号の不正輸出とされたのだ。

PGPがはやってきたので、会社にしようという動きが出てきた。アメリカのベンチャーとしてPGPInc.が立ち上がったのであるが、金目当ての人間が上層部に集まり、ジママンの意見は通ることはなかったという。しかし間もなく、その会社も立ち行かなくなって、ネットワーク・アソシエイツに吸収されてしまった。

彼にとって悪いことが続くのだが、世界中の人権団体から多数の賞をもらっている。彼はダライラマやアウンサン・スーチーなど数多くの人権活動家や民主主義活動家たちは、専制的な政府からプライバシーを守るためのツールとしてPGPを使っている。彼の当初の目的通りPGPが人権運動などで活躍していることに満足なようである。

標準化

- RFC1991(1996)
  - PGP Message Exchange Format
- RFC2015(1996)
  - MIME Security with Pretty Good Privacy (Oct 1996)
- RFC2440(1998)
  - OpenPGP Message Format

PGPが広がりを見せるに従って、ジママンの手を離れるようになっていく。

ネットワーク・アソシエイツが、PGPを本格的な事業の対象とすると、マーケティングによってPGPの方針が決められるように変化した。それを修正するかのように、OPEN-PGPというフォーマットも決まった。これによってGUNPGPのように第三者がPGPを作っても、このフォーマットに従っていれば変換ができるようにしたのである。

そうした中から、96年にRFC1991が登場してきた。RFCはリクエスト・フォー・コメントの略で、「コメントを求めます」という名のインターネットの標準化文章である。これはゆるやかな合意ではあるが、インターネット上の事実上の標準として認めてしまうことである

OpenPGP

- ハッシュ
  - MD5, SHA-1, RIPE-MD/168,MD2
- 共通鍵暗号
  - IDEA, 3DES, CAST, Blowfish, Safer-128
- 公開鍵暗号
  - RSA, ElGamal(DH)
- 電子署名
  - RSA, ElGamal(DH), DSA

その新たなフォーマットの仕様であるがハッシュ関数でMD5、SHA-1、RIPE-MD/168、MD2となった。これは実装しているか、しつつあるものである。このほかワイズマン研究所のエリ・ビハムが考えたタイガーなど、新しいハッシュ関数がリザーブされている。今後のPGPが進んでいくロードマップはできている。

共通鍵暗号ではIDEA、3DES、CAST、Blowfish、Safar-128などがリザーブされている。公開鍵暗号ではRSAとElGamal。電子署名はRSAとDSAである。

これらの仕様でパブリックドメインが作られる、つまり誰でも自分の手で作ることができるのである。