OpenPKSD

PGP/ GPG
インターネットで
広く使われている暗号技術

OpenPKSDプロジェクト

鈴 木 裕 信

(2002年1月版)

本プレゼンテーションは、1999年に大阪で行われたソフトウェア技術者協会のフォーラムで利用したプレゼンテーションを改定し、2002年 1月に公開したものである。

OpenPKSD

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)やGPG (グニュ・プライバシー・ガード)はOpenPGP (RFC2440) を実装した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。

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。

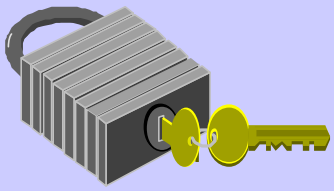
たとえば私が、ヨーロッパにメールを出すときに、どういう経路でメールが流れているかはほとんど事前に検証することは不可能である。私が家から出したメールはOCNに行き、そこからNTTのアメリカの子会社へ、さらにアメリカ国内のネットワークを通ってヨーロッパへ行くだろう。さらにヨーロッパ内のいくつかのネットワークを経由して、友達へメールが届くはずだ。

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。ではどうやって守るのか？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やGPGによるセキュリティのニーズが出てくるのである。

OpenPKSD

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



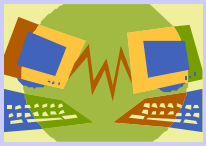
ここでは大きく三つに分類している。「通信している内容を第三者に知られない秘匿性」、「通信した内容を改ざんから守る完全性」、「なりすましを防ぐ認証性」である。秘匿性、完全性までは古くから必要性が認識されていたが、認証性についてはインターネット時代になって新しく注目をあびるようになった。

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。

OpenPKSD

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



コンピューターでの通信では、色々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のように一番下の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の中にも組み込まれるIPSecがこれに当たる。これが良くVPNなどに使われる技術である。

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やSSL (TLS) である。エレクトリックコマースなどのサイトではSSLが普及している。途中でデータの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OpenPGP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。パソコン上で使われる多くのメールプログラムは標準的にMIMEが使える。S/MIMEはセキュリティ拡張である。S/MIMEは業界手動で標準されたので、いろいろなツールがサポートしている。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。またSSL(TLS)やIPSecでも　OpenPGPの鍵を使おうという規格が提案されている。

OpenPKSD

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

暗号メールの世界ではOpenPGPとS/MIMEがシェアの殆どを占めている。

PGPやGPG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ので、自分で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。現在では、PGP/GPGをサポートするメールプログラムがたくさんある。

このほかにPEMというものもある。これは古くからある電子メール専用の暗号プロトコルである。しかし、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、これは受け入れられなかった。

その他独自のシステムもある。大手企業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。

OpenPKSD

PGP/GPG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やGPG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暗号方式を使って守る。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。

OpenPKSD

汎用だから...

- 内容を暗号化しRadix64のアスキー形式で出力
- 公開鍵暗号による暗号化をサポートしているのでメールの暗号化に使うと便利
- PGP公開鍵サーバへの登録・検索、Webページにある公開鍵を読みこむなど多様な機能

内容を暗号化して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良い。相手は内容を復号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。

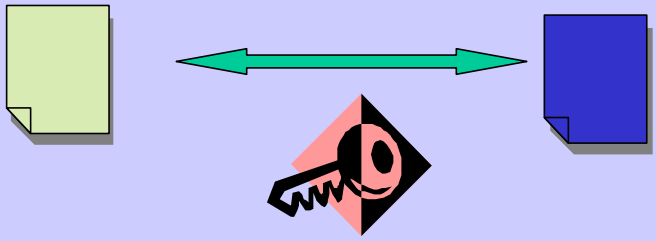
PGP公開鍵サーバーへの登録、検索、あるいはWebページにある公開鍵を読み込むことができる点も便利である。いったん鍵をプールするようなサーバーに入れておくとか、鍵をWebページに埋め込んで相手に取り出してもらう。公開鍵サーバーの実装にはいくつかあり、商用もフリーソフトウェアもある。

日本におけるPGP公開鍵サーバーはpgp.nic.ad.jpである。フリーソフトウェアであるHorowitz版pksdを利用している。現在公開鍵は１５０万～２００万鍵程度が登録されているはずである。現在はあまりにも鍵が多くてpgp.nic.ad.jp上ではデータベースの内容を計測できていない。２００１年は３１万鍵ほど増えた。１９９９年に「３年後には１００万を超しそうな勢いである」と説明したことがあるが、実際には２００１年の初頭には１００万鍵をオーバーしていた。

OpenPKSD

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。

OpenPKSD

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

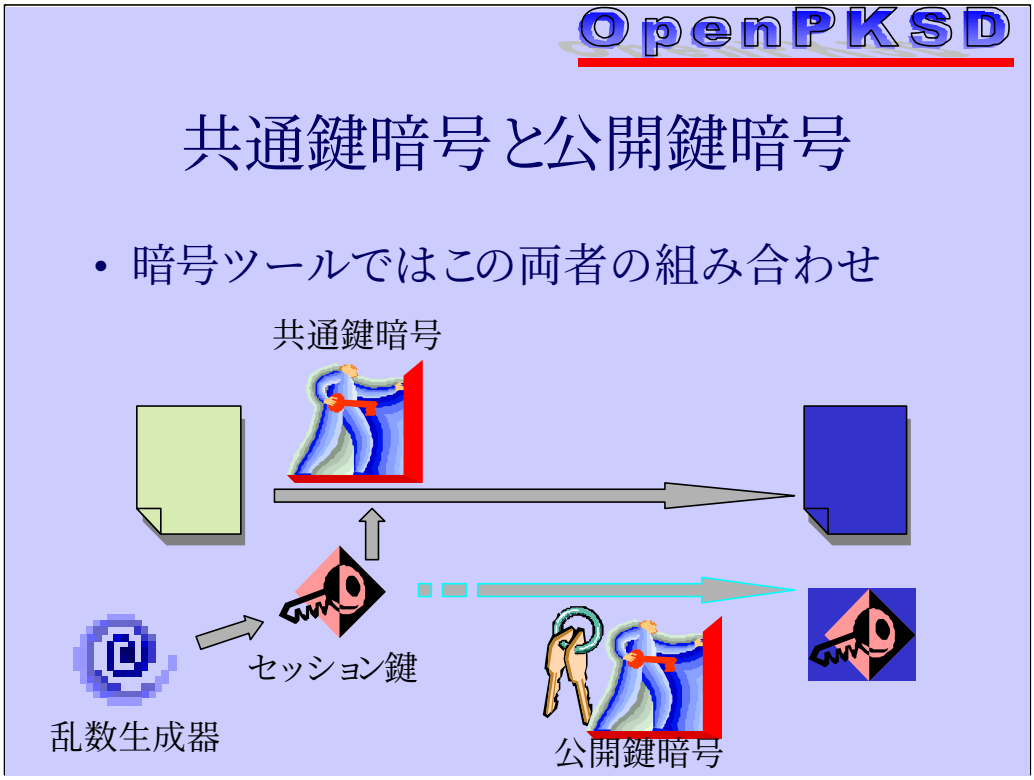
（スライド参照のこと）

OpenPKSD

公開鍵と秘匿鍵を持つ利点

- 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

（スライド参照のこと）



まず乱数生成器からセッション鍵を生成し、そのセッション鍵を使い共通鍵暗号で内容を暗号化する。次にセッション鍵を公開鍵暗号を使い暗号化する。両者を相手に送付する。

OpenPKSD

電子署名

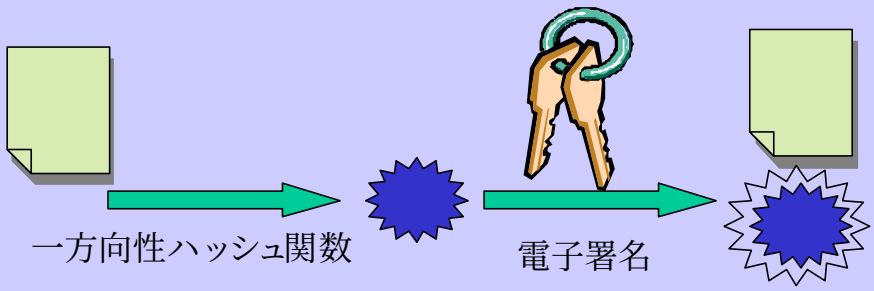
- 改竄の検出
- 誰が署名したのかがわかる

(スライド参照のこと)

OpenPKSD

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



（スライド参照のこと）

OpenPKSD

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

(スライド参照のこと)

OpenPKSD

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

局方式はX.509認証局方式である。信頼のチェーンはOpenPGPが採用している認証方法である。局方式は立ち上げのコスト、運用のコストがかかる。

OpenPKSD

PGP

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

ちなみにPEMは既に１９８０年代に規格化が終わっていた。必ずしもPGPが最初の暗号ソフトウェアというわけではない。

OpenPKSD

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。

（スライド参考のこと）

OpenPKSD

バージョンの変遷

- 1991年　バージョン1．0
  - RSA＋Bass-O-Ma gic
- 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)

（スライド参考のこと）

OpenPKSD

現在のバージョン(2002年2月)

- PGP 7.7.1
  - Network Associates, Inc
- GNUPG 1.0.6
  - GNU version of PGP
  - Werner Koch

（スライド参照のこと）

OpenPKSD

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

日本ではInvestigation（疑惑）という単語が「訴えられた」という具合に誤って翻訳されたものが多かった。中には「裁判中である」なとど言い切っているマスコミ報道もあった。Zimmermann本人によれば司法や行政からコンタクトはなかったそうだ。ただ最後に「あなたへの調査は打ち切りました」という手紙が来たそうである。その手紙が唯一無二の接点だそうだ。

OpenPKSD

標準化

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

（スライド参照のこと）

OpenPKSD

OpenPGP

- ハッシュ
  - MD5, SHA-1, RIPE-MD/168,MD2
- 共通鍵暗号
  - IDEA, 3DES, CAST, Blowfish, Safer-128, AES 128/192/256
- 公開鍵暗号
  - RSA, ElGamal(DH)
- 電子署名
  - RSA, ElGamal(DH), DSA

現在では、これだけの種類の暗号アルゴリズム・ハッシュアルゴリズムが利用できる。DHはDiffie-Hellman**方式の略である。**RFC2440**ではElgamal (Diffie-Hellman)と表現しているので、それに習っている。**