OpenPKSD

白黒バージョン

# 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**

**hironobu@h2np.net**



**(2002年1月版)**

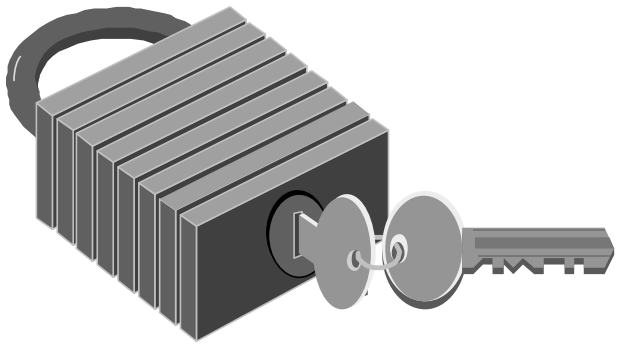
# インターネット上における情報

- 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

OpenPKSD

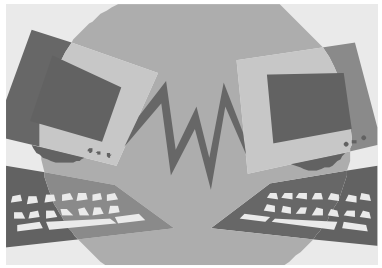
# 情報セキュリティとして求められるもの

- 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



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

# 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

# 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

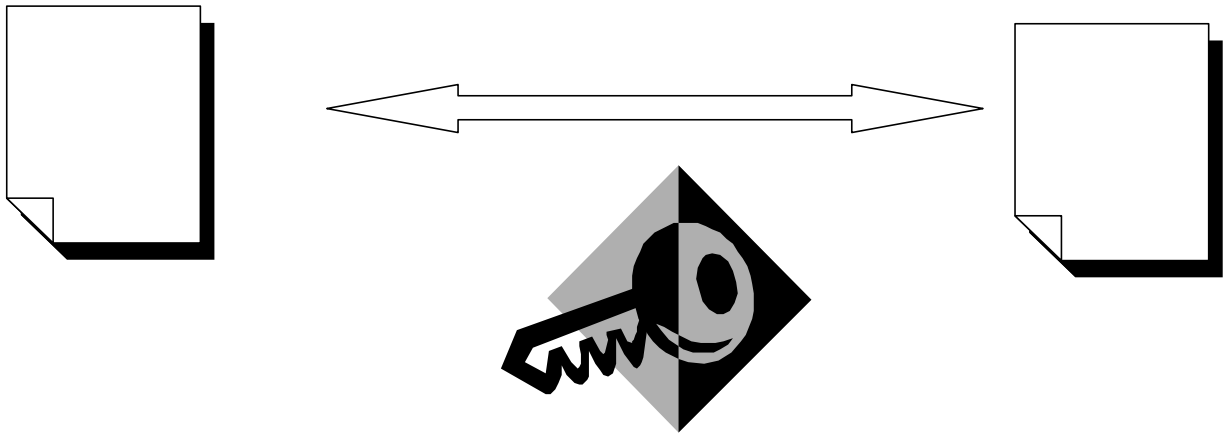
OpenPKSD

# 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

# 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



# 公開鍵暗号

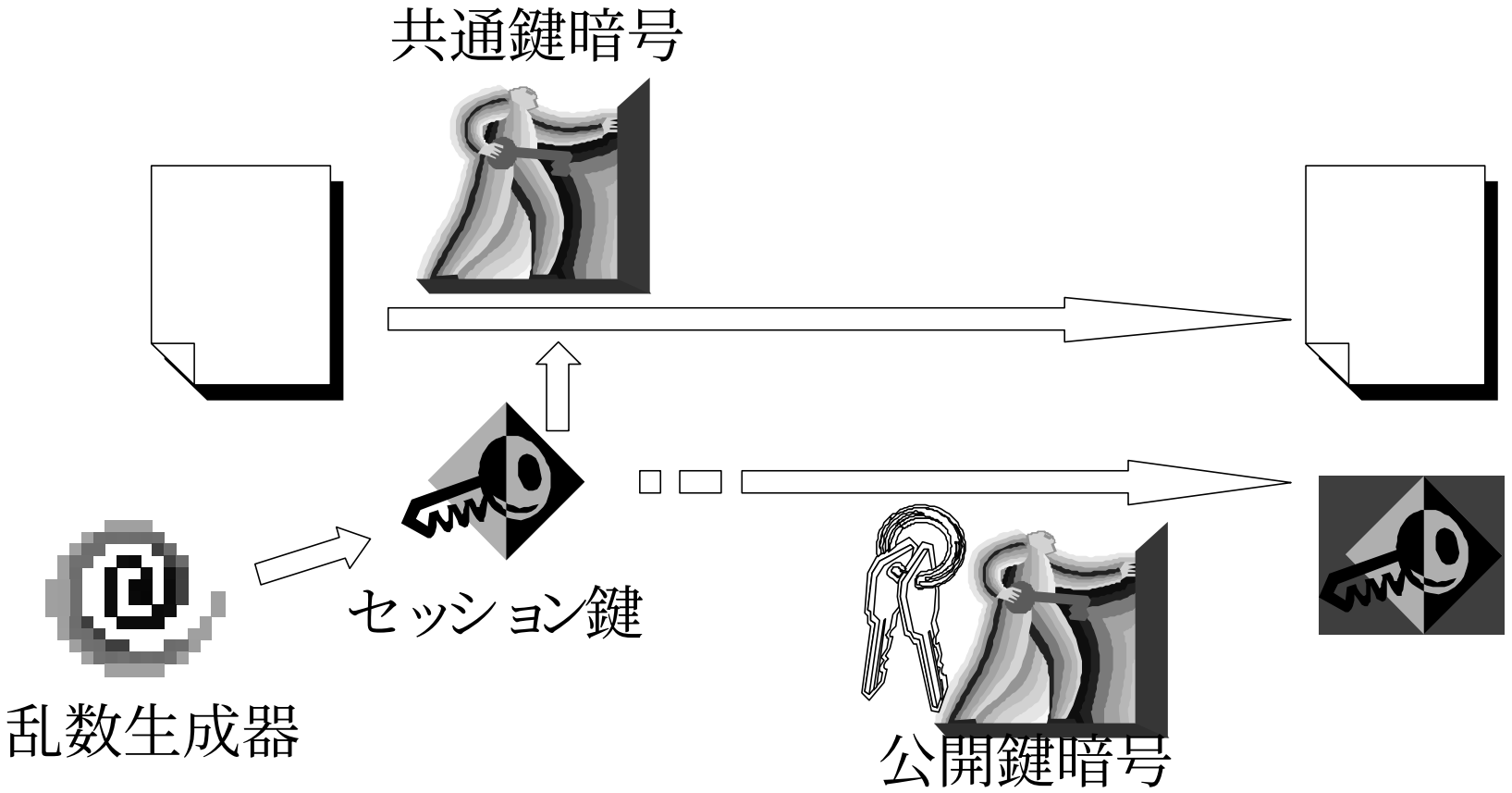
- 暗号化する鍵と復号化する鍵が違う暗号方式
  - 概念：1976年 W. Diffie,M.Hellman/同時期にRalph Merkle
  - RSA暗号：1978年 R. Rivest, A.Shamir, L. Adleman
  - ElGamal暗号：1985年 T.ElGamal
  - 楕円暗号：1985年 N. Kobliz/V.S. Miller

# 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

# 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



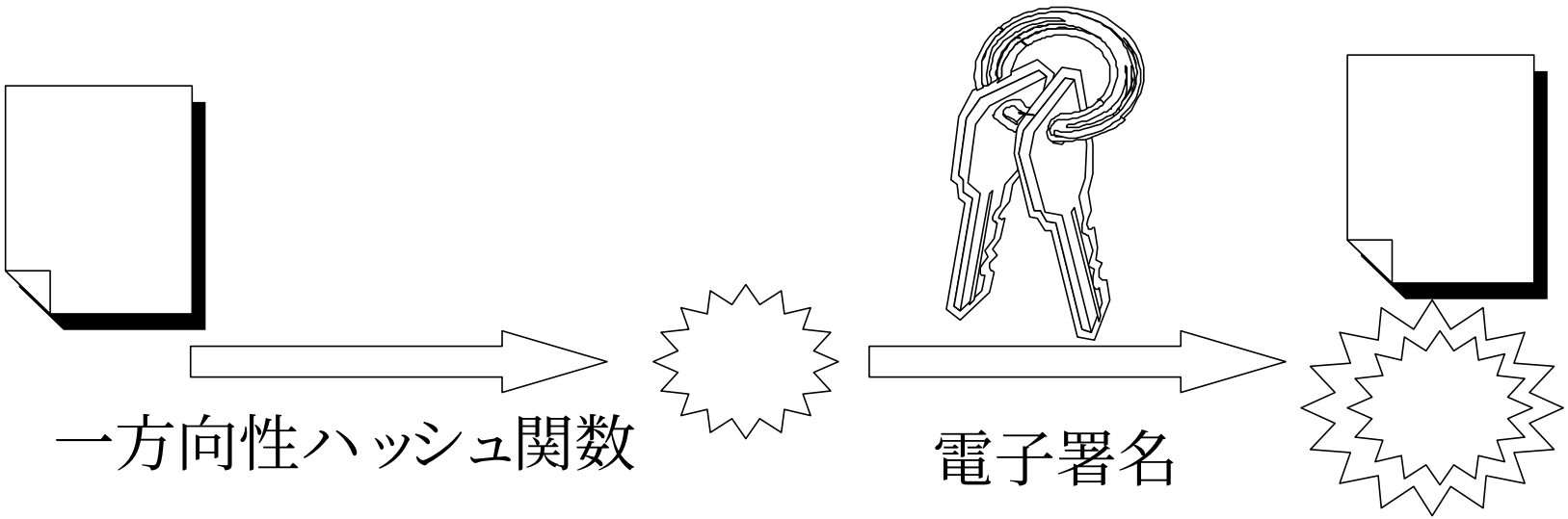
# 電子署名

- 改竄の検出
- 誰が署名したのかがわかる

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

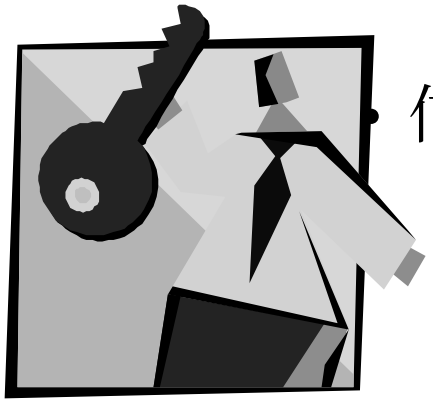


# 鍵交換

- 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

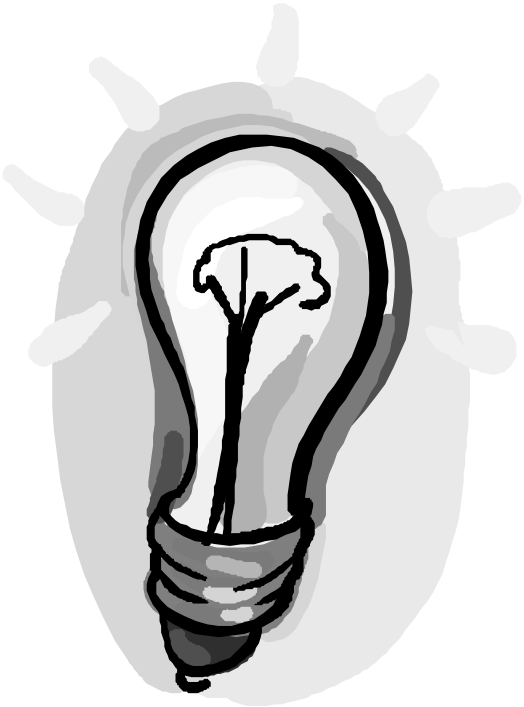


# PGP

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

# 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。



# 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)

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

# 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

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

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