# 公開鍵暗号GnuPGを使ってみる

松本　眞

平成19年1月11日

## 基本的参考文献

- GNU Privacy Guard講座 http://hp.vector.co.jp/authors/VA019487/
- GnuPGの使い方 http://hp.vector.co.jp/authors/VA019487/howtouse.html

## 1　インストール・スタート

GNU Privacy Guard 講座 http://hp.vector.co.jp/authors/VA019487/ から、Windows, Mac, Linux などに install できる。

広島大学情報メディアセンターのICE端末で linux を利用する場合には、すでにインストールされているので、以下それを仮定する。

1. linux を選んで、ICE端末にログインする。
2. WWW ブラウザ fire fox を起動し、GnuPGの使い方 http://hp.vector.co.jp/authors/VA019487/howtouse.html を見る

## 2　自分の鍵の作成・他人の公開鍵の取り込み

1. GNOME端末を開く（左上の「アプリケーション」から「システムツール」から「GNOME端末」を選んでクリック。）
2. GNOME端末で、gpg --gen-key と入力する。以下、「GnuPGの使い方」のホムペの通りに端末で入力をえらぶと、いずれ公開鍵・秘密鍵が作成され、適切な場所に保存される。

   パスフレーズは、あらかじめ考えておくと良い。他のマシンのパスワードなどは使わないほうが良い。

3. 破棄証明書は、とりあえず作らなくていい。

4. 鍵の登録も、とりあえずしなくてよい。

5. `http://keyserver.veridis.com/` で、Search のところに Makoto Matsumoto と入れると、松本眞の公開鍵が出てくる。

6. KeyID の、番号のところをクリックして、ディスクに保存すると、公開鍵が保存できる。ファイル名がそのままではながくなるので、適宜短いファイル名 (mm-public.asc など）として保存する。

7. GNOME 端末で、`gpg --import mm-public.asc` を実行する。これにより、松本眞の公開鍵があなたの gpg のデータベースに登録される。

8. 鍵の指紋はとりあえず使わない。

# 3 暗号化したファイルを送る

1. 暗号化したいファイルを作る。内容は、あなたの授業に対する簡単な感想などでよい。

   ファイルを作成するには、画面左の「GNOME テキスト・エディタ」をクリックして開き、中に文章を打ち込んで、「保存」をクリックし、適当な名前を入れて、「OK」をクリックすればよい。

   例えば、kansou というファイルにする。

2. GNOME 端末で、例えばあなたの学籍番号が ub030000 ならば、`gpg -o ub030000.asc -ea kansou` と入力することで、kansou というファイルを暗号化したファイルを ub030000.asc という名前で作成せよ、という指令ができる。この入力後、受取人を指定することになる。例えば、m-mat とすると、松本眞が受取人に指定され、松本眞の公開鍵による暗号化が行われる。

3. 松本眞宛メールにて、ub030000.asc を添付ファイルとしたメールを送信する。タイトル (件名) は、自分の学籍番号にする。本文は、自分の名前にする。

   松本眞のメールアドレスは`m-mat at math.sci.hiroshima-u.ac.jp` (at は@にする) である。

4. Linux から出るときは、左上の「アクション」から「ログアウト」を選択する。

5. 松本眞が、`gpg -d ub030000.asc` を実行すると、復号化された内容がコンソールにあらわれる。

# 4 二人ずつペアになって

1. 二人ずつペアになる (A と B とする)。
2. 自分の公開鍵を相手にメールやフラッシュメモリにて送付する。
3. A は暗号化したいファイルを作り、B からもらった公開鍵で暗号化し、B に送る。
4. B は、受け取った暗号文を、上記の要領で（B の秘密鍵で) 復号化して読む。
5. A と B の役目を入れ替えて実行してみる