

# Why GPG Key sign?

東京エリア Debian 勉強会 in OSC 2009 Tokyo/Fall

岩松 信洋 iwamatsu@debian.or.jp  
IRC nick: iwamatsu

2009年10月31日

# なぜキーサインするのか？

- PGP/GnuPG は認証局がないので、自分が相手を信頼するしかない。
- キーサインパーティを行って、PGP/GnuPG の公開鍵をソーシャルな情報とともに交換し、信頼の輪 (web of trust) を広げる。

# 使いどころ：フリーソフトウェア開発者の場合

- アカウント作成時のチェックに使ったり。(インターネット上での存在を示す。)
- ソフトウェアのリリース時に使ったり。
- Debian ではパッケージへの署名、投票などに使う。

## 使いどころ：ユーザの場合は？

- メールへの署名 / 暗号化に利用。
- Debian 開発者になるための通過儀礼。

# 使いどころ：ユーザの場合は？

身近なところでは、改竄のチェックにつかう。Debian の場合は `secure-apt` で使われている。

```
# apt-get update
.....
W: GPG error: http://cdn.debian.or.jp testing Release: The following
  signatures couldn't be verified because the public key is not
  available: NO_PUBKEY 9AA38DCD55BE302B
# gpg --keyserver wwwkeys.eu.pgp.net --recv-keys 9AA38DCD55BE302B
# gpg --armor --export 9AA38DCD55BE302B | apt-key add -
# apt-get update
.....
Fetched 2B in 1s (1B/s)
Reading package lists... Done
```

×:エラーがでなくなった！これで大丈夫です！（って書いてある Web サイト多いよね。）

：ちゃんと鍵と信頼度をチェックしましょう。

鍵のチェックには、Web Of Trust に入らないとできない。

# チェックする簡単な方法

9AA38DCD55BE302B の鍵に署名している人は...

```
pub 4096R/55BE302B 2009-01-27
uid Debian Archive Automatic Signing Key (5.0/lenny) <ftpmaster@debian.org>
sig sig3 55BE302B 2009-01-27 ----- 2012-12-31 [selfsig]
sig sig 7E7B8AC9 2009-01-27 ----- Joerg Jaspert <joerg@debian.o
sig sig DOEC0723 2009-01-27 ----- Mark Hymers <mhy@debian.org>
sig sig BE9BF8DA 2009-01-27 ----- Mike O'Connor (stew) <stew@vi
sig sig 30B94B5C 2009-05-24 ----- ***** (imacat) <imacat@mai
```

## 鍵のチェック

```
$ gpg --keyserver pgp.mit.edu --recv-keys 55BE302B
$ gpg --list-sig 55BE302B
pub 4096R/55BE302B 2009-01-27 [満了: 2012-12-31]
uid Debian Archive Automatic Signing Key (5.0/lenny)
<ftpmaster@debian.org>
sig 7E7B8AC9 2009-01-27 [ユーザー ID が見つかりません]
sig DOEC0723 2009-01-27 [ユーザー ID が見つかりません]
sig BE9BF8DA 2009-01-27 [ユーザー ID が見つかりません]
sig 30B94B5C 2009-05-24 [ユーザー ID が見つかりません]
sig 3 sig 55BE302B 2009-01-27 Debian Archive Automatic Signing Key (5.0/1
```

...。だれともサインしていないようです。

# trust path finder

しかし Web of Trust なので、信頼のパスが使える。  
trust path finder<sup>1</sup>を使うと、信頼のパスが分かる。

PGP key statistics : Nobuhiro Iwamatsu <iwamatsu.at.debian.org>

[40AD1FA6](#) - Nobuhiro Iwamatsu <iwamatsu.at.debian.org>

trust paths :

from  to

from  to

see also :

- [key statistics](#) in the [wotsap analysis](#) by [Jörgen Cederlöf](#)
- look up [Nobuhiro Iwamatsu](#) on [Google](#)
- [analysis of the strong set in the PGP web of trust](#)
- [FAQs about the PGP pathfinder and key statistics](#)

statistics :

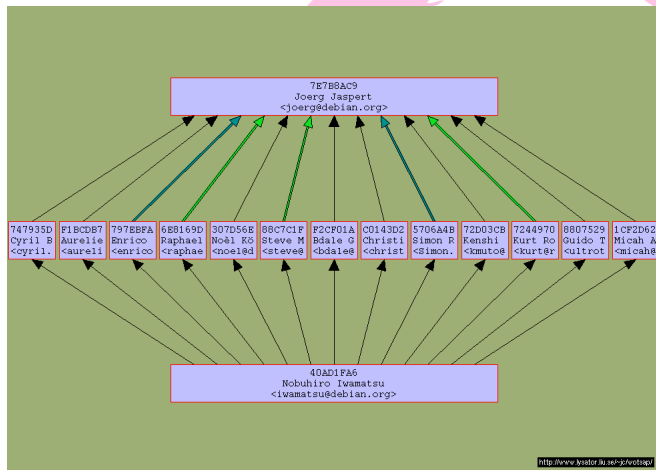
signatures	54
keys signed	61
mean shortest distance (msd)	4.3812
msd ranking	2079

cross signatures : 36

---

<sup>1</sup>[http://pgp.cs.uu.nl/mk\\_path.cgi](http://pgp.cs.uu.nl/mk_path.cgi)

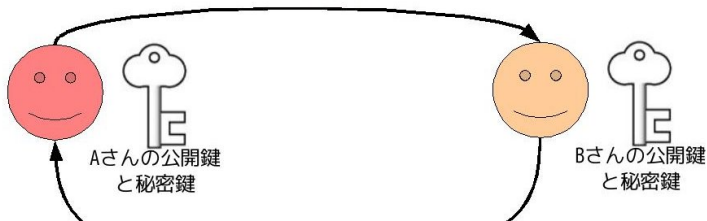
# Joerg と岩松の trust path



他の人を介して、Web of Trust がつながっていることが分かる。知り合いの知り合いがサインしているようだ。ちょっとは信用できるかな？とか。

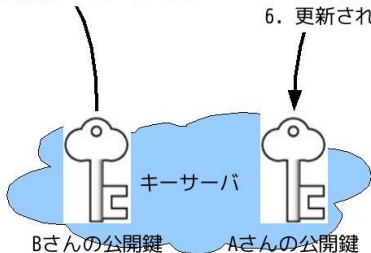
# キーサインの流れ

3. サインしたBさんの公開鍵を  
Bさんにメールで暗号化して送信する



1. 公開鍵の取得する
2. 公開鍵へのサインする

4. BさんはAさんの鍵を取得して、復号化する
5. 復号化した自分の公開鍵を自分の鍵束に入れる
6. 更新された公開鍵を再度キーサーバに送信する



# gpg コマンドでやった場合

```
$ gpg --keyserver pgp.mit.edu --recv-key 40AD1FA6
$ gpg --fingerprint 40AD1FA6
$ gpg --edit-key 40AD1FA6
$ gpg --sign-key 40AD1FA6
$ gpg --check-sig 40AD1FA6
$ gpg --export -a 40AD1FA6 > iwamatsu.gpgkey
$ iwamatsu.gpgkey を相手にメールに 署名+暗号化して送信
```

数人ならいいけど、100人と  
かやってられん！

## そこでcaffの登場。

caff は signing-party パッケージで提供されている。

```
$ sudo apt-get install signing-party
```

caff を使うための初期化を行う。caff を一回実行すると、初期ファイルを作成してくれる。

```
$ caff
.....
#
#Regards,
#{owner}
#EOM

Please edit /home/hoge/.caffrc and run caff again.
```

# caff の設定

~/caffrc にある 設定ファイルを修正する。

```
$ cat ~/.caffrc

$CONFIG{'owner'} = 'Nobuhiro Iwamatsu';
$CONFIG{'email'} = 'iwamatsu@debian.org';

$CONFIG{'keyid'} = [ qw{4121C7433170EBE9 32247FBB40AD1FA6} ]

# Additionally encrypt messages for these keyids
$CONFIG{'also-encrypt-to'} = [ qw{4121C7433170EBE9 32247FBB40AD1FA6} ]

# Mail template to use for the encrypted part
$CONFIG{'mail-template'} = << 'EOM'\maketitle#Hi,

please find attached the user id{(scalar @uids >= 2 ? 's' : '')}
{foreach $uid (@uids) {
    $OUT .= "\t".$uid."\n";
};}of your key {$key} signed by me.
.....
```

# caff の設定

caff のデフォルトの設定では、cert-digest-algo が SHA1 になっているので、<sup>2</sup> SHA512 に設定する。

```
$ mkdir -p ~/.caff/gnupghome
$ chmod 700 ~/.caff/gnupghome
$ cat >> ~/.caff/gnupghome/gpg.conf
cert-digest-algo SHA512
personal-digest-preferences SHA512
EOF
```

また、メールを使うので、ローカル（作業するマシン）の SMTP も設定しておく必要がある。

---

<sup>2</sup><http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=527944>

# caff を使った署名

署名する ID をキーサーバから取得し、指定した自分の ID で署名してくれる。そして、署名した鍵を暗号化して送信してくれる。

```
$ caff -u 自分の ID 署名する ID .....
```

# 署名完了後

署名後のデータは `~/.gnupg/pubring.gpg` ではなく、  
`~/.caff/gnupghome/pubring.gpg` に格納される。この鍵束  
を `~/.gnupg/pubring.gpg` に取り込む。

```
$ gpg --import ~/.caff/gnupghome/pubring.gpg
```

取り込んだら、自分の鍵をキーサーバに送信。

```
$ gpg --keyserver pgp.nic.ad.jp --send-keys 自分の ID  
$ gpg --keyserver pgp.mit.edu --send-keys 自分の ID
```

# 最後に

相手に鍵を送るまでがキーサインパーティです。ちゃんと相手に署名した鍵を送りましょう。