初めてのキーサインパーティ

齋藤 雄介 ysaito@golangcoder.club

2017 年 9 月 16 日

参考にした資料

キーサインパーティで参考にさせていただいた資料

GPG キーサインパーティ
資料

岩松 信洋 iwamatsu@debian.org
IRC nick: iwamatsu

2010 年 09 月 11 日

caffを使おうとして

Homebrew から消えてた

```
$ brew search signing-party
 ==> Searching local taps...
 ==> Searching taps on GitHub...
 ==> Searching blacklisted, migrated and deleted formula
 signing-party was deleted from homebrew/core in commi
```

gpg のみでやってみよう

gpg の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
```

つまづいた

相手の公開鍵で暗号化するところを自分の公開鍵で暗号化してしまった

```
$ gpg --encrypt --recipient 相手の公開鍵 ID 相手の公開鍵
```

gpg の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
```

caffをつかわないなら

参考: https://github.com/thinkAmi/caffish-ps

```
# キーサーバより相手の公開鍵を取得し、
# 自分の公開鍵の鍵束に入れる
$ gpg --keyserver pgp.mit.edu --recv-key 相手の公開鍵 ID

# 表示されるフィンガープリントと、
# 手元の書類のフィンガープリントが一致していることを確認
$ gpg --fingerprint 相手の公開鍵 ID

# 相手の公開鍵に署名
$ gpg --sign-key 相手の公開鍵 ID

# 署名した公開鍵をエクスポート
$ gpg --export -a 相手の公開鍵 ID > ./foo.gpgkey

# 自分の秘密鍵で署名した相手の公開鍵を、相手の公開鍵を使って暗号化
$ gpg --no-auto-check-trustdb  --trust-model=always \
  --armor --recipient 相手の公開鍵 ID --encrypt ./foo.gpgkey
# foo.gpgkey.asc が生成される
# 暗号化した公開鍵をメールに添付し、
# メール本文を暗号化して相手へ送信
```

そうだ caff つかおう

もう一つ詰まったところ

Debian strech に caff をいれてメールサーバを立てて...

```
$ caff -u 自分の公開鍵 ID 一人目の公開鍵 ID 二人目の公開鍵 ID...
[NOTICE] Fetching keys from pool.sks-keyservers.net, this may t
[WARN] Local-user 自分の公開鍵 ID is not defined as one of your
[ERROR] None of the local-user keys seem to be known as a keyic
# ~/.caffrc はちゃんと設定しているはずだけど...
# 自分の公開鍵のフィンガープリントの後半１６桁

$ caff 一人目の公開鍵 ID 二人目の公開鍵 ID...
# 通った
```