GPG/PGP キーサインパーティ

~ Kansai Open Forum 2012~

佐々木洋平/Youhei SASAKI
mailto: uwabami@debian.or.jp
IRC/twitter nick: uwabami

keysignparty-ja/Debian JP Project/関西 Debian 勉強会

2012 年 11 月 10 日 - 於: 大阪南港 ATC 10F 特設ステージ

自己紹介

- 佐々木洋平 (@uwabami)

自己紹介

- 佐々木洋平 (@uwabami)
- Debian JP Project/関西 Debian 勉強会

自己紹介

- 佐々木洋平 (@uwabami)
- Debian JP Project/関西 Debian 勉強会
  - 今日 17:00 から 9F room #3 で
    「Debian 7.0 “Wheezy” の紹介」 やります.

自己紹介

- 佐々木洋平 (@uwabami)
- Debian JP Project/関西 Debian 勉強会
  - 今日 17:00 から 9F room #3 で
    「Debian 7.0 “Wheezy” の紹介」 やります.
- ksp-ja(key sign party-ja) メンバ:
  https://sites.google.com/site/kspjapanese/

なんでキーサインするの？

なんでキーサインするの?

- PGP/GPG は公開鍵暗号方式
  → 公開鍵を誰かに保証してもらう必要がある

GnuPG

なんでキーサインするの?

- PGP/GPG は公開鍵暗号方式
  → 公開鍵を誰かに保証してもらう必要がある
- しかし PGP/GPG には認証局が無い

なんでキーサインするの?

- PGP/GPG は公開鍵暗号方式
  → 公開鍵を誰かに保証してもらう必要がある
- しかし PGP/GPG には認証局が無い
  - 自分が相手を信頼して、相手が自分を信頼する

GnuPG

なんでキーサインするの?

- PGP/GPG は公開鍵暗号方式
  → 公開鍵を誰かに保証してもらう必要がある
- しかし PGP/GPG には認証局が無い
  - 自分が相手を信頼して、相手が自分を信頼する
  - これを PGP/GPG ユーザで相互に行う
    → ネットワークが構築される (Web of Trust)

GnuPG

なんでキーサインするの?

- PGP/GPG は公開鍵暗号方式
  → 公開鍵を誰かに保証してもらう必要がある
- しかし PGP/GPG には認証局が無い
  - 自分が相手を信頼して、相手が自分を信頼する
  - これを PGP/GPG ユーザで相互に行う
    → ネットワークが構築される (Web of Trust)
- 実際に会って、相手の公開鍵と公的 ID（パスポート、運転免許証）を確認、そして署名＝キーサイン

GnuPG

なんでキーサインするの?

- PGP/GPG は公開鍵暗号方式
  → 公開鍵を誰かに保証してもらう必要がある
- しかし PGP/GPG には認証局が無い
  - 自分が相手を信頼して、相手が自分を信頼する
  - これを PGP/GPG ユーザで相互に行う
    → ネットワークが構築される (Web of Trust)
- 実際に会って、相手の公開鍵と公的 ID（パスポート、運転免許証）を確認、そして署名＝キーサイン
- 誰とも鍵交換してない GPG 署名なんて意味がない
  ... だって誰にも信頼されてないじゃない...

使い所

- 開発者にとっては...
  - 存在証明
    - 公開サーバのアカウント認証など
  - ソフトウェアのリリース署名
    - Debian、Ubuntu では必須
    - パッケージへの署名、投票の署名...
    - Linux カーネル, ...
- ユーザによっては...
  - メールの署名/暗号化
  - データファイルの署名
  - ソフトウェアの改竄チェック
    - リポジトリの署名チェック (apt, yum etc..)

使い所

- 開発者にとっては...
  - 存在証明
    - 公開サーバのアカウント認証など
  - ソフトウェアのリリース署名
    - Debian、Ubuntu では必須
    - パッケージへの署名、投票の署名...
    - Linux カーネル, ...
- ユーザによっては...
  - メールの署名/暗号化
  - データファイルの署名
  - ソフトウェアの改竄チェック
    - リポジトリの署名チェック (apt, yum etc..)

これらを行うには Web of Trust に参加している必要がある

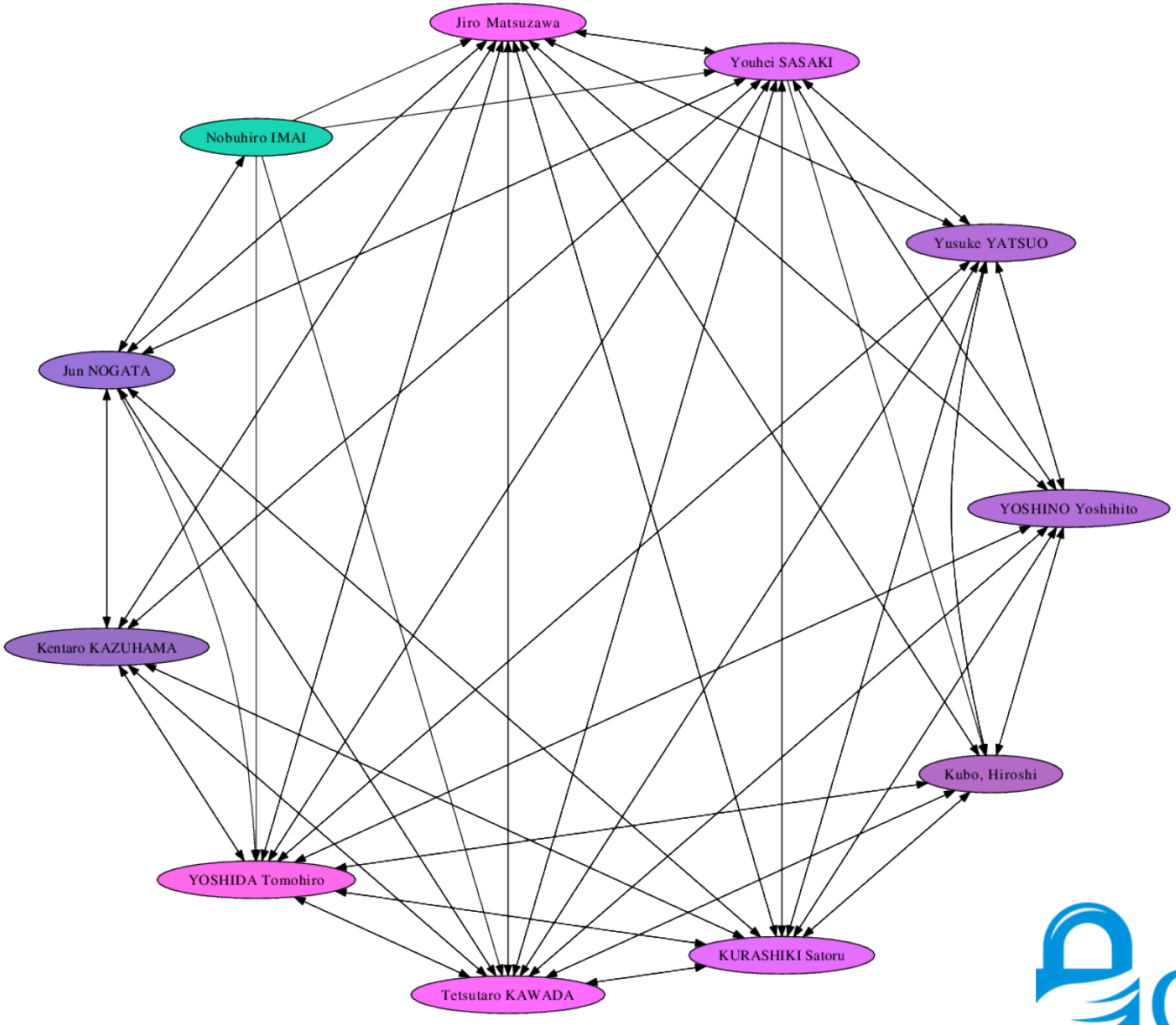
というわけで、キーサインしましょう。

キーサインの流れ

1. キーサーバに自分の公開鍵をアップロード
2. 相手の確認 (名前、公開鍵の指紋, ID、メールアドレス)
3. 相手の公開鍵に署名（メールアドレス毎に！）
4. 署名した相手に公開鍵を送信（メールアドレス毎に！）
5. 相手に署名された自分の鍵を取り込む
6. キーサーバに自分の公開鍵をアップロード

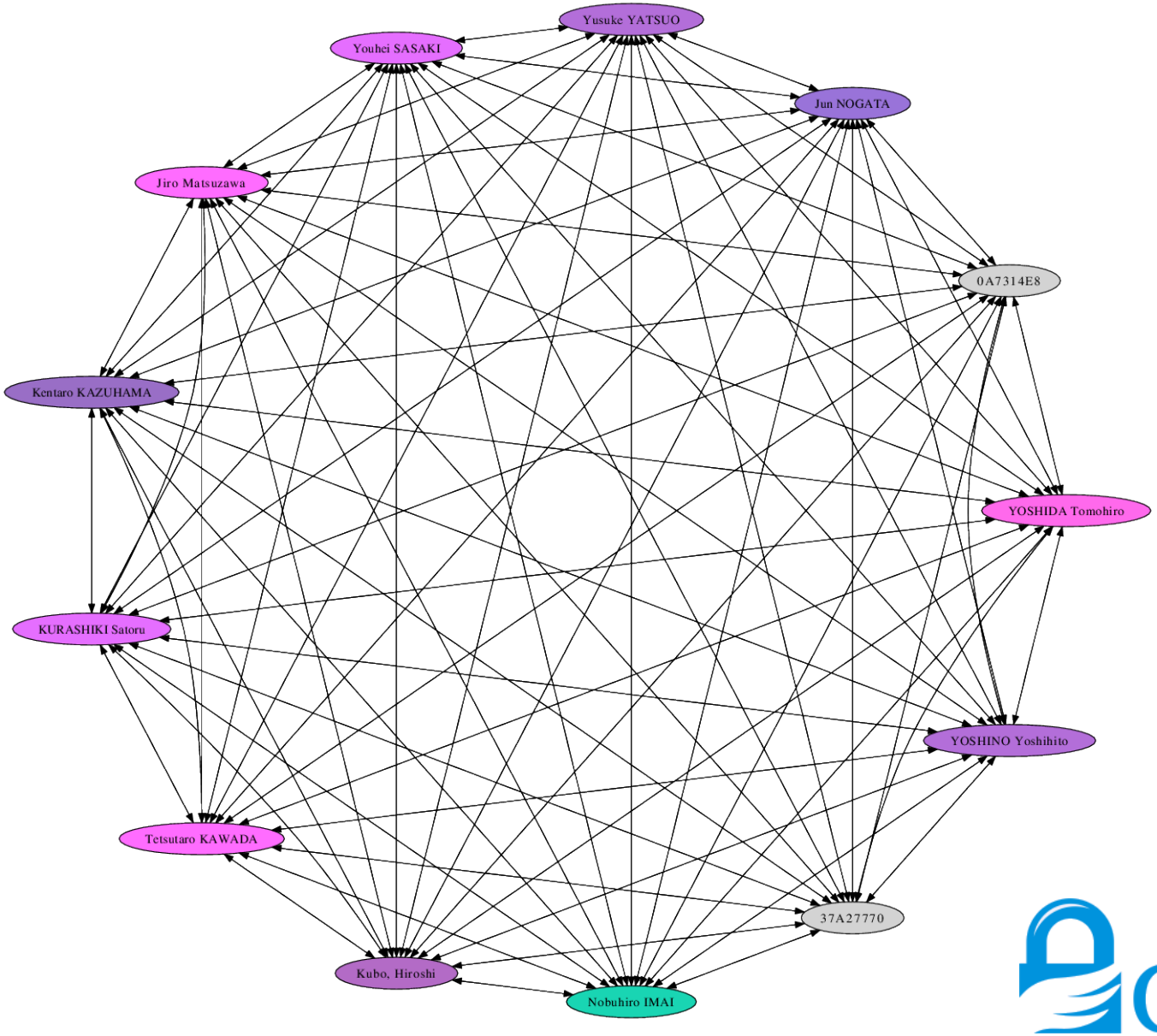
GnuPG

キーサインパーティ前の WoT



GnuPG

キーサインパーティ後の WoT (予想)



GnuPG

GPG サインパーティ後

- 相手にサインして送るまでが GPG サイン。
- caff を使うと楽ちんです。

Have any questions?

本日の SHA256 ハッシュ

```
05ad 8a0d 63ad f630
4fb8 61be f4b4 b201
2776 701c e429 6c2d
d27e 3375 67b3 8e8c
```