



Why GPG Key sign?

- GPG キーサインパーティ at OSC 2010 Kansai@Kyoto -

佐々木洋平


`uwabami@debian.or.jp`

2010年7月10日



なぜ GPG
キーサインを
するのか？



A large, hand-drawn pink circle with a textured, brushstroke-like appearance, centered on the page. The circle is slightly irregular and has some darker pink spots, giving it a dynamic, artistic feel.

リア充



Why GPG key sign?

- PGP/GnuPG には認証局がない
 - 自分が相手を信頼するしかない
- キーサインパーティで PGP/GnuPG 公開鍵とともにソーシャルな情報を交換
 - 信頼の輪 (Web of Trust) を広げる



使い所: 開発者の場合

- ネット上での存在証明
 - 公開サーバでのアカウントの作成などに使用
- ソフトウェアリリースの署名
 - Debian ではパッケージの署名/投票に使用



使い所: ユーザの場合

- メールの署名/暗号化
- 入手したソフトウェアの改竄チェック
 - Debian では開発者になるための通過儀礼



GPG キーサインの流れ

- 1 相手の確認: 公開鍵の指紋とソーシャルな ID の確認
- 2 相手の公開鍵に自分の GPG 鍵で署名
- 3 署名した相手の公開鍵を送る
 - きちんと送るまでがキーサインパーティです.

1. 相手の確認



1. 相手の確認





今回はグループキーサイン方式

- 事前登録した人の分の GPG 指紋はテキストに記入
- SHA256 ハッシュで一括チェック
- あとは ID のみチェックしましょう.
 - この場で終わらない場合でも随時エソカイとかで...

A large, thick, pink brushstroke graphic that forms a circle with a smaller circle inside it, creating a spiral-like effect. The brushstroke is centered behind the text.

sha256sum

```
8c3cfe558b98c05  
c0a43558f0d7c717  
8a8e4ae2f17bc213  
db5a25aa6bc45a4e
```



キーサインパーティ後

- 1 相手の公開鍵に自分の GPG 鍵で署名
- 2 署名した相手の公開鍵を送る



最後に

きちんと送るまでがキーサインパーティです。
ちゃんと鍵に署名して相手に送りましょう。



参考資料

- 第 56 回東京エリア Debian 勉強会 2009 年 9 月発表資料
- GnuPG Keysigning Party HOWTO



sha256sum

```
8c3cfe558b98c05  
c0a43558f0d7c717  
8a8e4ae2f17bc213  
db5a25aa6bc45a4e
```