GPG/PGP クイックスタート

佐々木 洋平

uwabami@gfd-dennou.org

京大・数学/地球流体電脳倶楽部

2013/11/15 ITPASSセミナー/EPnetFaN座学編
於)神戸大学自然科学総合研究棟3号館

自己紹介

About me

Name & Contact:

- ✓ 佐々木洋平/Youhei SASAKI
- ✓ @see: about.me/uwabami

Affiliation & Activity:

- ✓ 京大・数学教室/地球流体電脳倶楽部
- ✓ Debian Project/Debian JP Project

今日のお題

今日のお題

要旨:

GPG/PGP はファイルの暗号化，複合，電子署名等に用いられるソフトウェアである．本セミナーでは．ソフトウェア開発者のみならず，ソフトウェアの使用者にとっても必須教養である(と講演者自身は思っている) GPG/PGPについて解説する

[cited from `『[itpass 7640] ITPASS セミナーのご案内 (2013/11/15)』']

検索

murashin
@murashin

フォロー中

@uwabami 誤字: 複合→復号

返信 リツイート お気に入りに登録 その他

2013年11月12日 - 19:07

@murashinさんへ返信する

...Orz

今日のお題

要旨:

GPG/PGP はファイルの暗号化，復号，電子署名等に用いられるソフトウェアである．本セミナーでは．ソフトウェア開発者のみならず，ソフトウェアの使用者にとっても必須教養である(と講演者自身は思っている) GPG/PGPについて解説する

[cited from `『[itpass 7640] ITPASS セミナーのご案内 (2013/11/15)』']

お品書き

- PGP/GPG
- 公開鍵暗号
- Web of Trust

お品書き

- ✓ PGP/GPG
- ✓ 公開鍵暗号
- ✓ Web of Trust

PGP

Pretty Good Privacy:

- ✓ 1991, Philip Zimmermann
- ✓ 公開鍵暗号方式を扱うソフトウェア
- ✓ 特許(RSA), 米国輸出規制(暗号≒武器)

OpenPGP

OpenPGP:

- ✓ RFC. 最新版は RFC4880
- ✓ PGP互換の暗号ソフトウェアの要件

GnuPG(GPG)

GNU Privacy Guard:

- ✓ GNU による OpenPGP の自由な実装.
- ✓ GPL-3+

というわけで

規格:

- ✓ OpenPGP, RFC4880

実装:

- ✓ GnuPG(GPG). 自由ソフトウェア
- ✓ PGP: シェアウェア (現在は Symantec が販売)

PGPは
使った事が
ありません

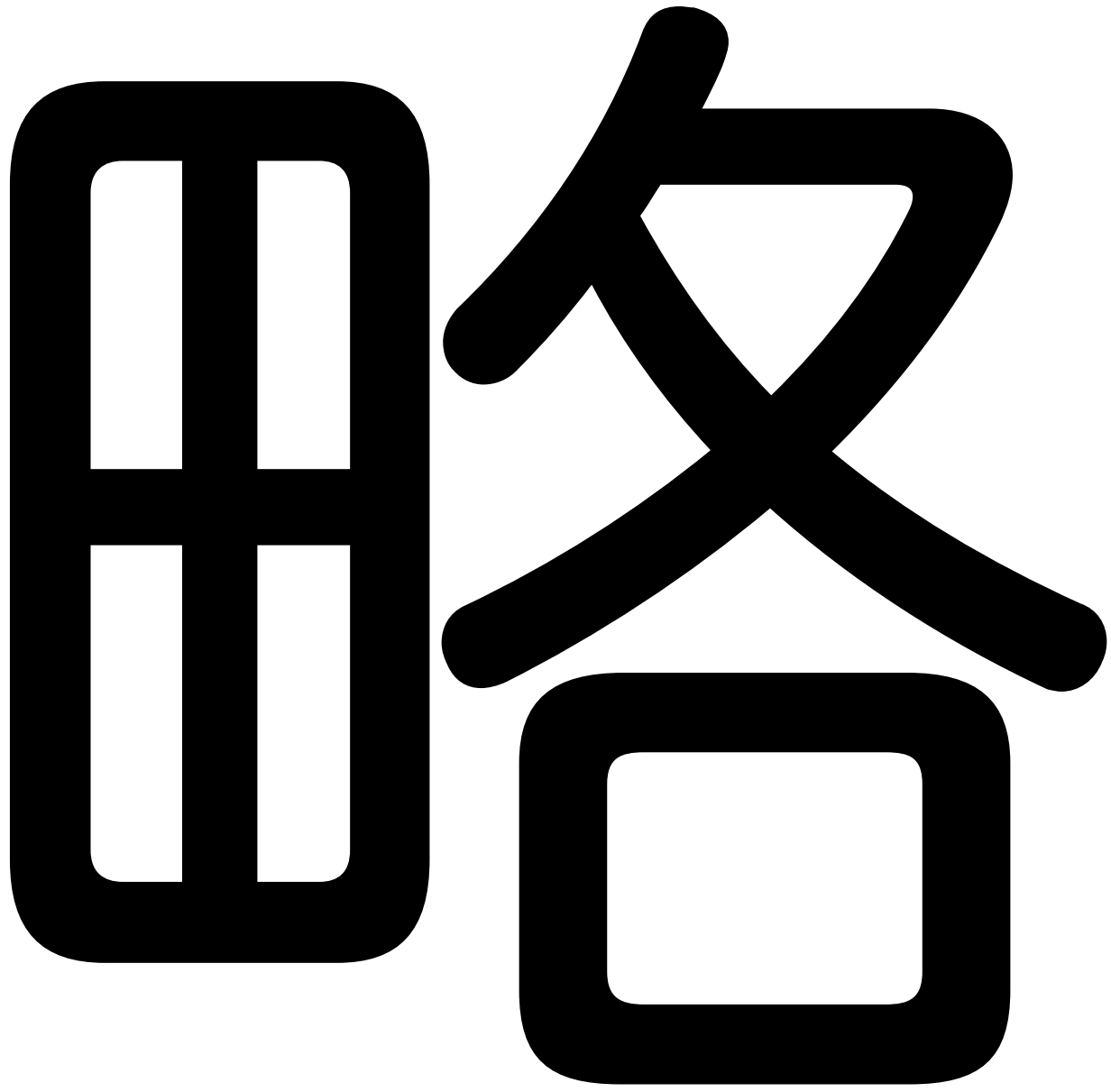
GPG/PGP でできること

- ファイルやメールの暗号化
- 電子署名

ファイルやメールの暗号化

実演

暗号方式の詳細



お品書き

- PGP/GPG
- 公開鍵暗号
- Web of Trust

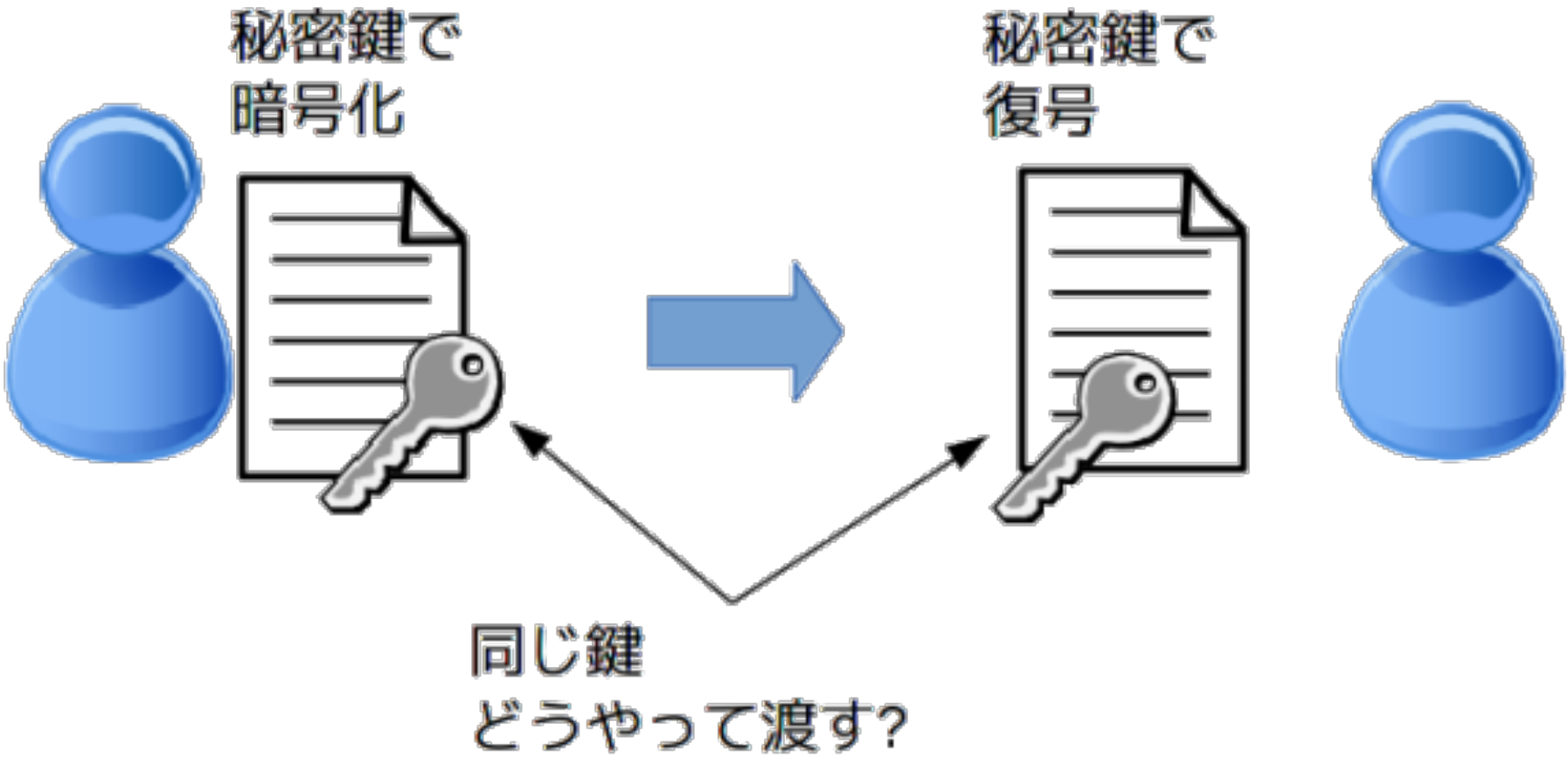
公開鍵暗号とは?

- ✓ 暗号化と復号に別々の鍵を使う
- ✓ 片方の鍵を公開できる(公開鍵)

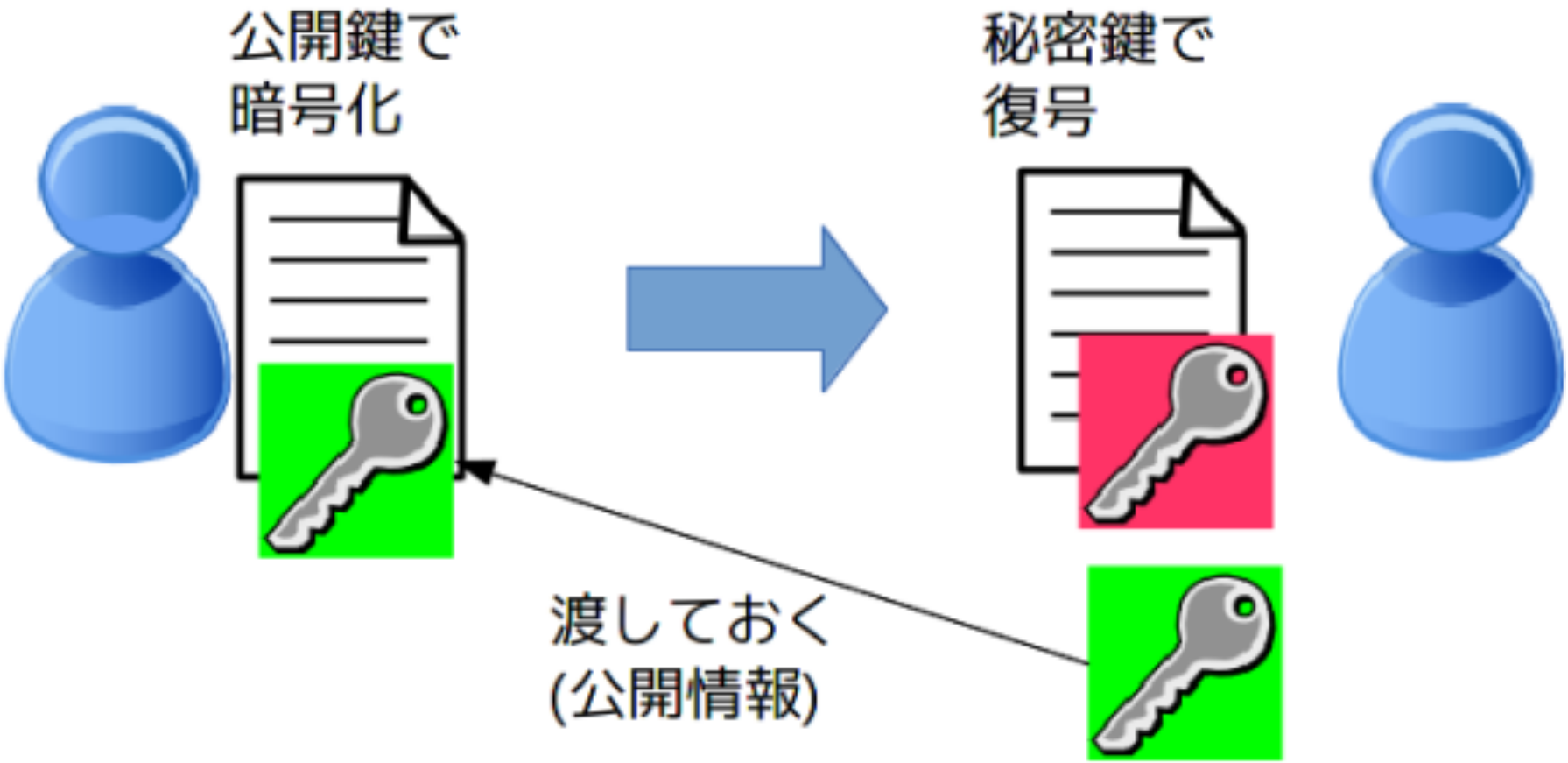
共通鍵暗号

- ✓ 古典的暗号方式
- ✓ 鍵の交換問題

鍵の交換問題



公開鍵暗号方式



公開鍵の取得

公開鍵サーバの例

有名所:

- ✓ pgp.mit.edu
- ✓ pools.sks-keyservers.net
- ✓ keys.gnupg.net

Debian:

- ✓ keyring.debian.org

というわけで

ファイル/メールの暗号化:

- ✓ 受け取る人の公開鍵で暗号化
- ✓ 受け取り手が自分の秘密鍵で復号

電子署名:

- ✓ 作成者の秘密鍵で署名
- ✓ 受け取った人は作成者の公開鍵で検証

お品書き

- PGP/GPG
- 公開鍵暗号
- Web of Trust

公開鍵の信用問題

- その公開鍵は，誰のモノか?
- 公開鍵への署名
  - 信用情報
  - 公開鍵に対して，秘密鍵で署名を追加

誰に署名してもらうか?

- ✓ 認証局
- ✓ 他の PGP/GPG ユーザ

Web of Trust(WoT)

- 信頼できる人の公開鍵を互いに秘密鍵で署名
- その蓄積で互いを信用
  - 「信用できる人が信用する鍵ならば信用できる」

WoT に参加するには?

- ✓ 公開鍵を公開
  - ✓ 鍵サーバにアップロード
- ✓ 直接会って身分証明

ここから
ぐだぐだ

おしまい