JPCERT CC®

組織内CSIRT構築の参考資料
PGPの説明に役立つデータ

一般社団法人
JPCERT コーディネーションセンター

本資料について

- 本資料は、FIRSTなどのCSIRTコミュニティーにおいてCSIRT間で交換するメッセージの暗号化に一般的に使用されるPGPについて概説することを目的としている。PGPを理解している人が、他の人にPGPの概要を説明するための資料として使用することを想定しており、PGPの技術や使用法の詳細について説明するものではない。

目次

- PGP とは
- 暗号化について
- 電子署名について
- 信頼の輪について
- （参考）JPCERT/CC の署名付きドキュメント

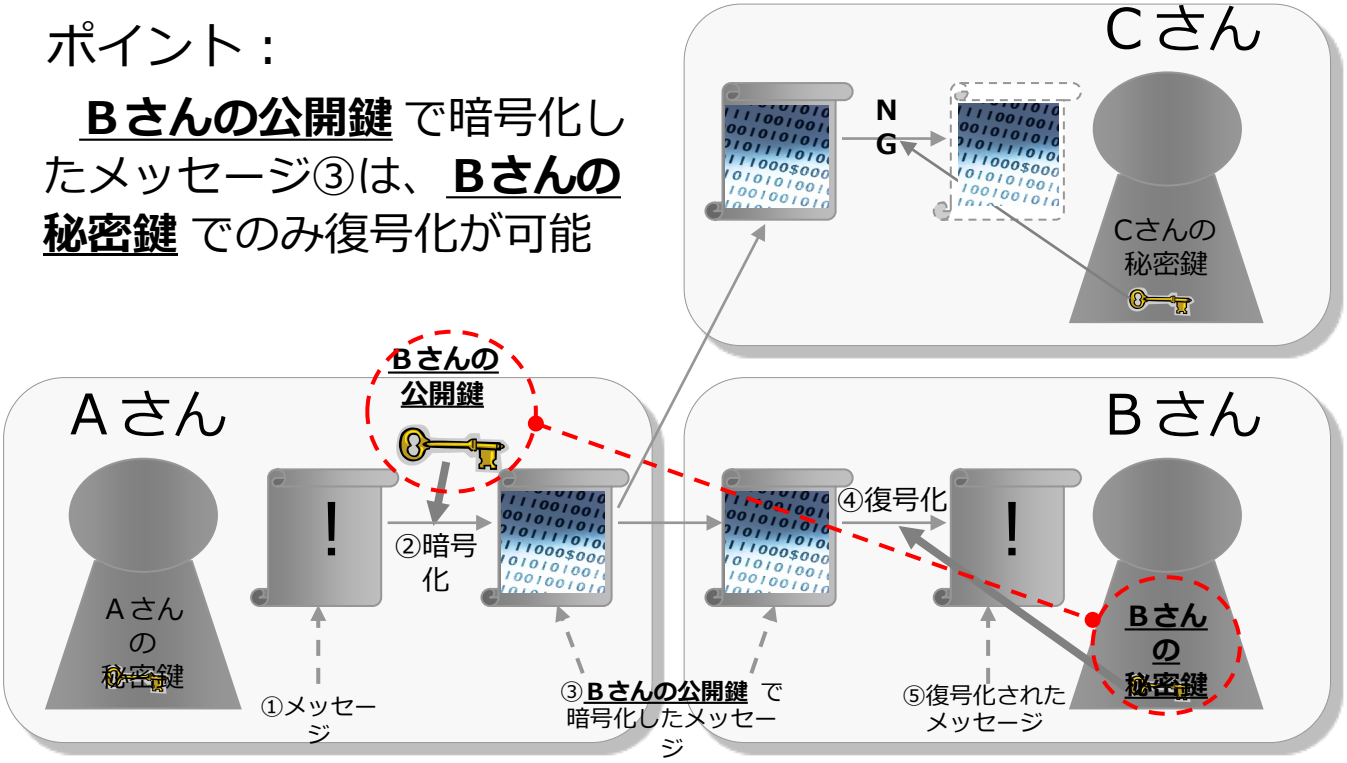
PGPとは

- PGP（Pretty Good Privacy）は、フリーツールや商用ツールなどさまざまな形で提供され、広く利用される標準的な公開鍵暗号ソフトウェア
- FIRST（https://www.first.org/）などのCSIRTコミュニティーにおいては、異なる組織のCSIRTが互いに信頼し機微な内容を含むメッセージを交換する際に使用する暗号化ツールとして一般的に利用されている
  - 秘密鍵と公開鍵のペア
    - 公開鍵を相手に渡す
    - 秘密鍵は自分で保持する。
  - 電子メールの暗号化
    - 第三者からの盗聴を防ぐ
  - 電子署名
    - 送信元の成りすましの防止
    - 電子メールの改ざんの検知

暗号化について

ポイント：

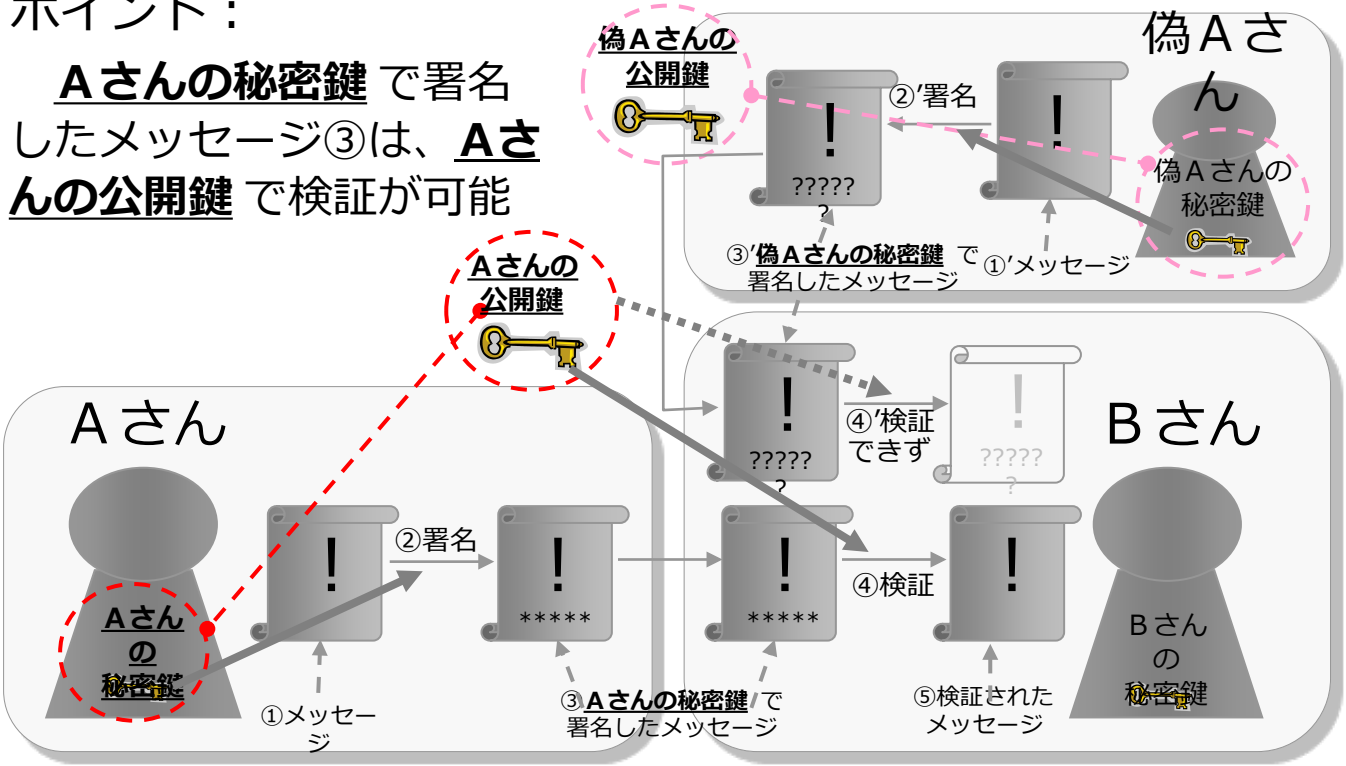
Bさんの公開鍵 で暗号化したメッセージ③は、**Bさんの秘密鍵** でのみ復号化が可能



電子署名について

ポイント：

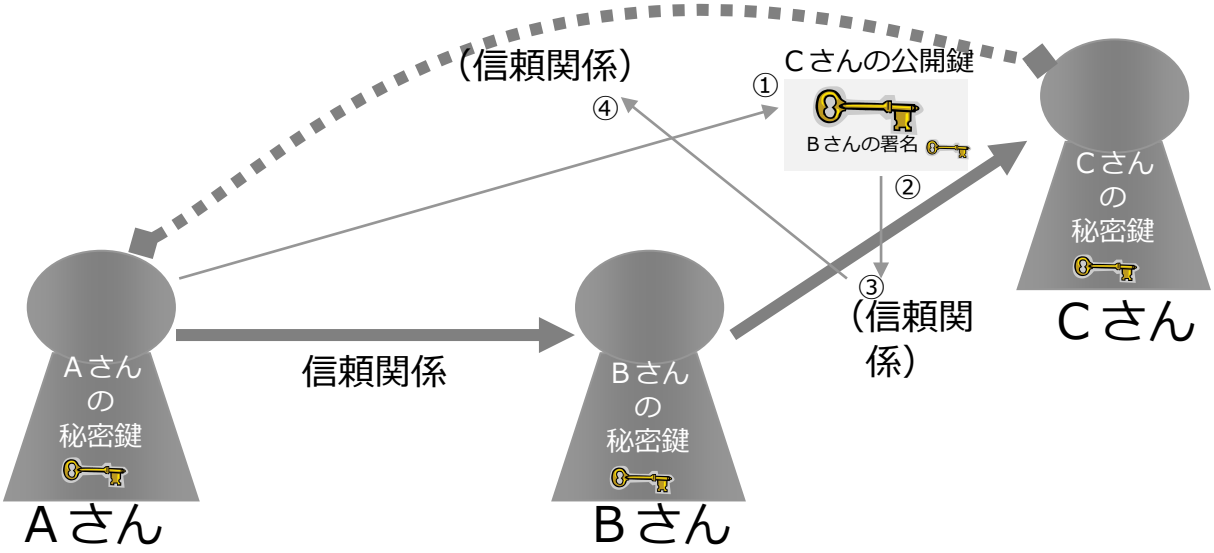
Aさんの秘密鍵 で署名したメッセージ③は、**Aさんの公開鍵** で検証が可能



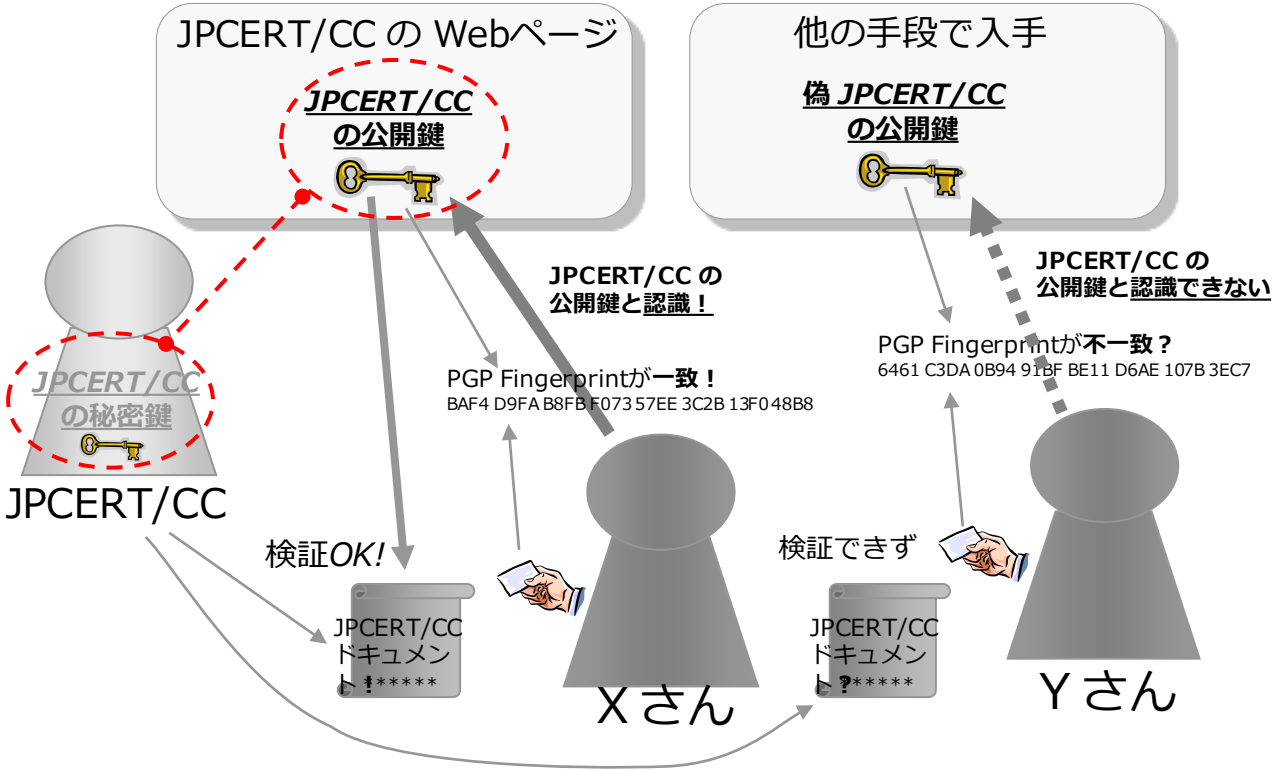
信頼の輪（Web of Trust）

（前提： Ａさんは、初めてＣさんの公開鍵を入手した。）

Ａさんは、**Ｃさんの公開鍵** 内に、すでに信頼しているＢさんの署名があること（ＢさんがＣさんを信頼していること）を確認した。したがって、ＡさんはＣさん（の公開鍵）を信頼できる。



（参考）JPCERT/CC の署名付きドキュメント



（参考）PGPを使用したメール送受信

- はじめての暗号化メール (Thunderbird編)
  https://www.jpcert.or.jp/magazine/security/pgpquick.html

初めてPGPを使用する人のための、PGPのインストールからPGPを使ったメッセージ交換までをカバーするガイドブック