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

このドキュメントについて

- このドキュメントは、PGP に関して理解をしている方が、他の方に説明するための資料の素材として役立てていただくことを目的としたものである。

- したがって、そのまま説明資料として活用するには、不十分な点があることを、ご了承いただきたい。

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

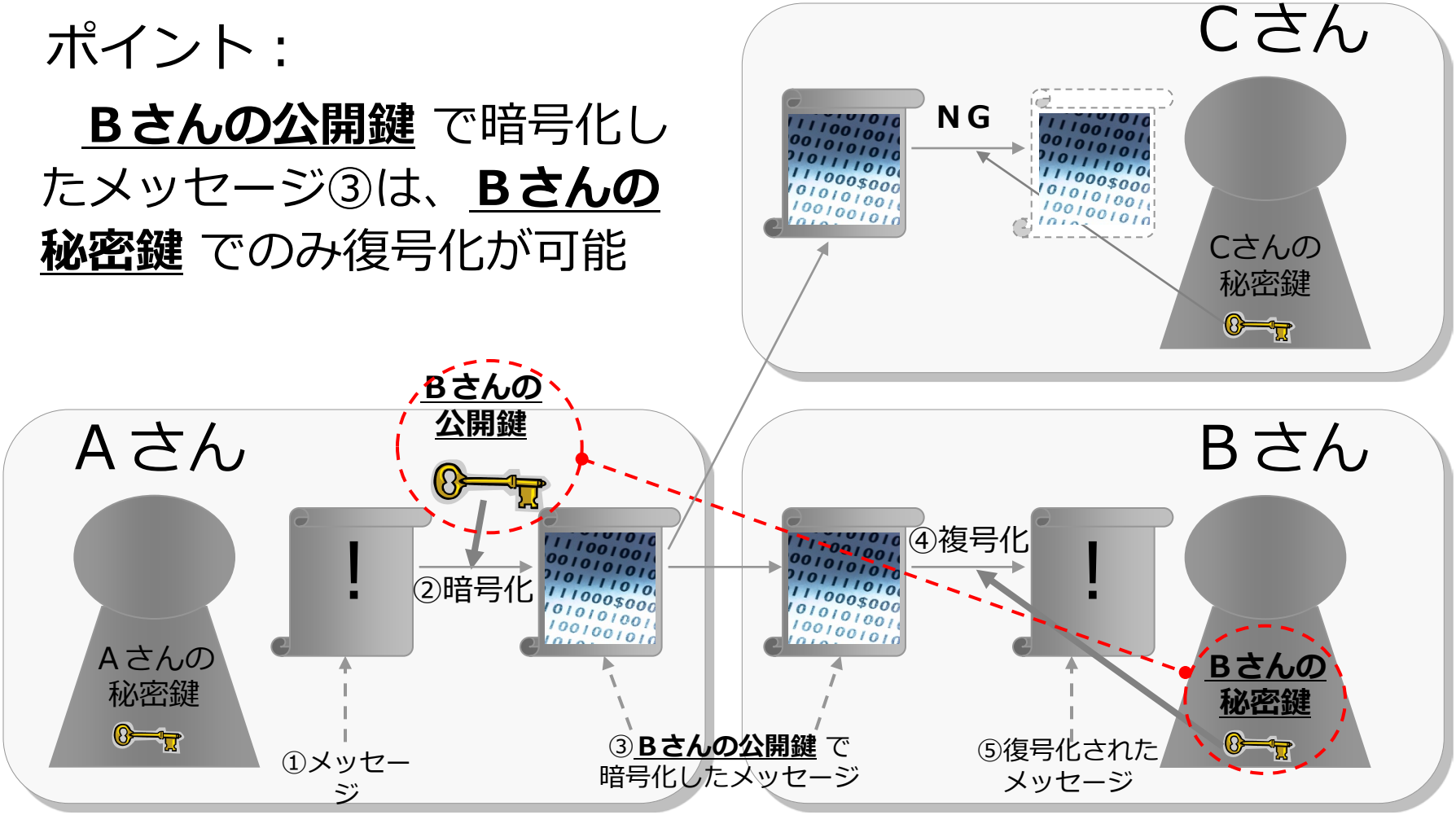
PGP とは

- PGP（Pretty Good Privacy）は、フリーツールや商用ツールなどさまざまな方法で提供されている、世界標準の暗号化ソフトウェアである
  - 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：

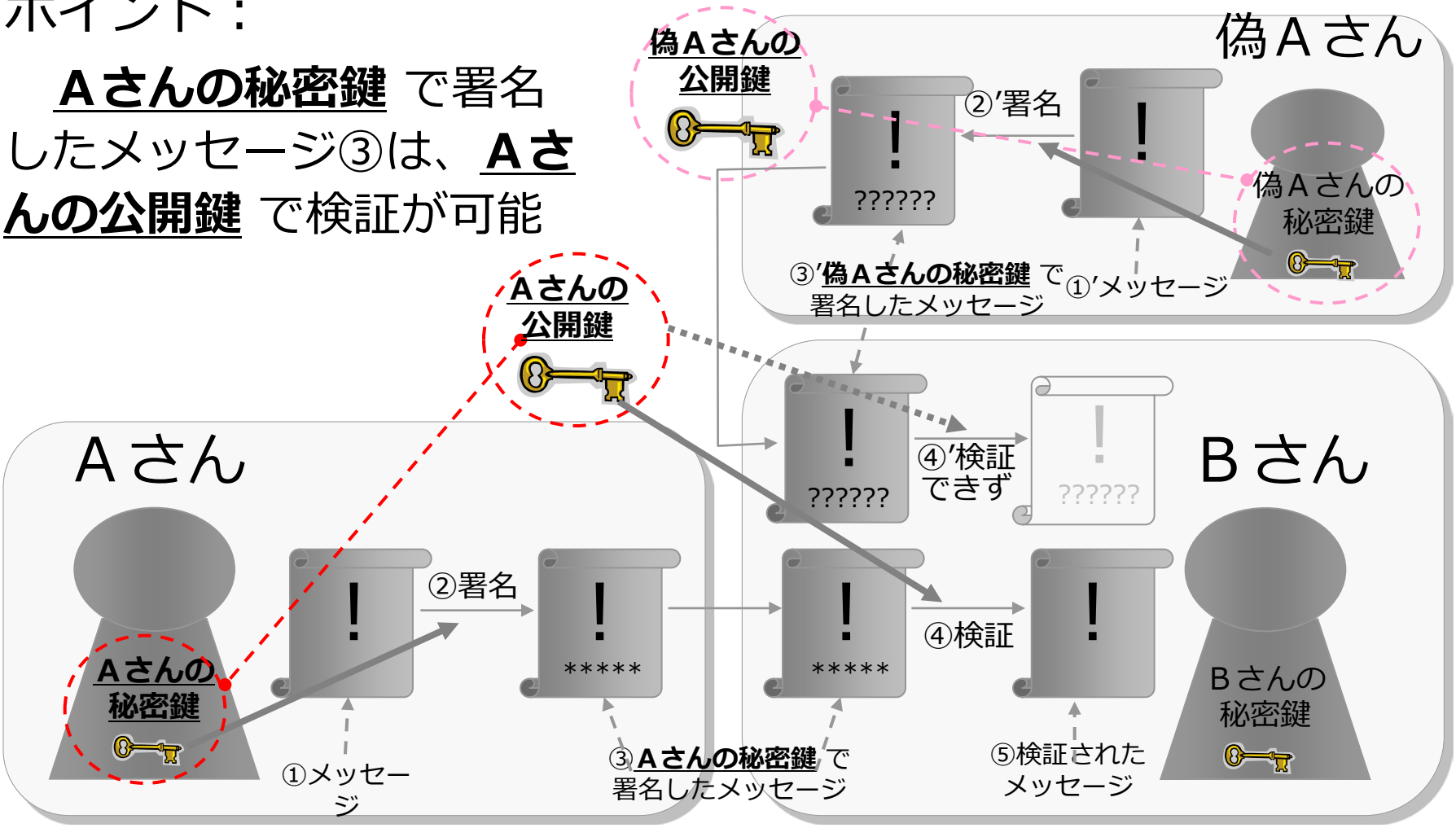
Bさんの公開鍵 で暗号化したメッセージ③は、**Bさんの秘密鍵** でのみ復号化が可能



電子署名について

ポイント：

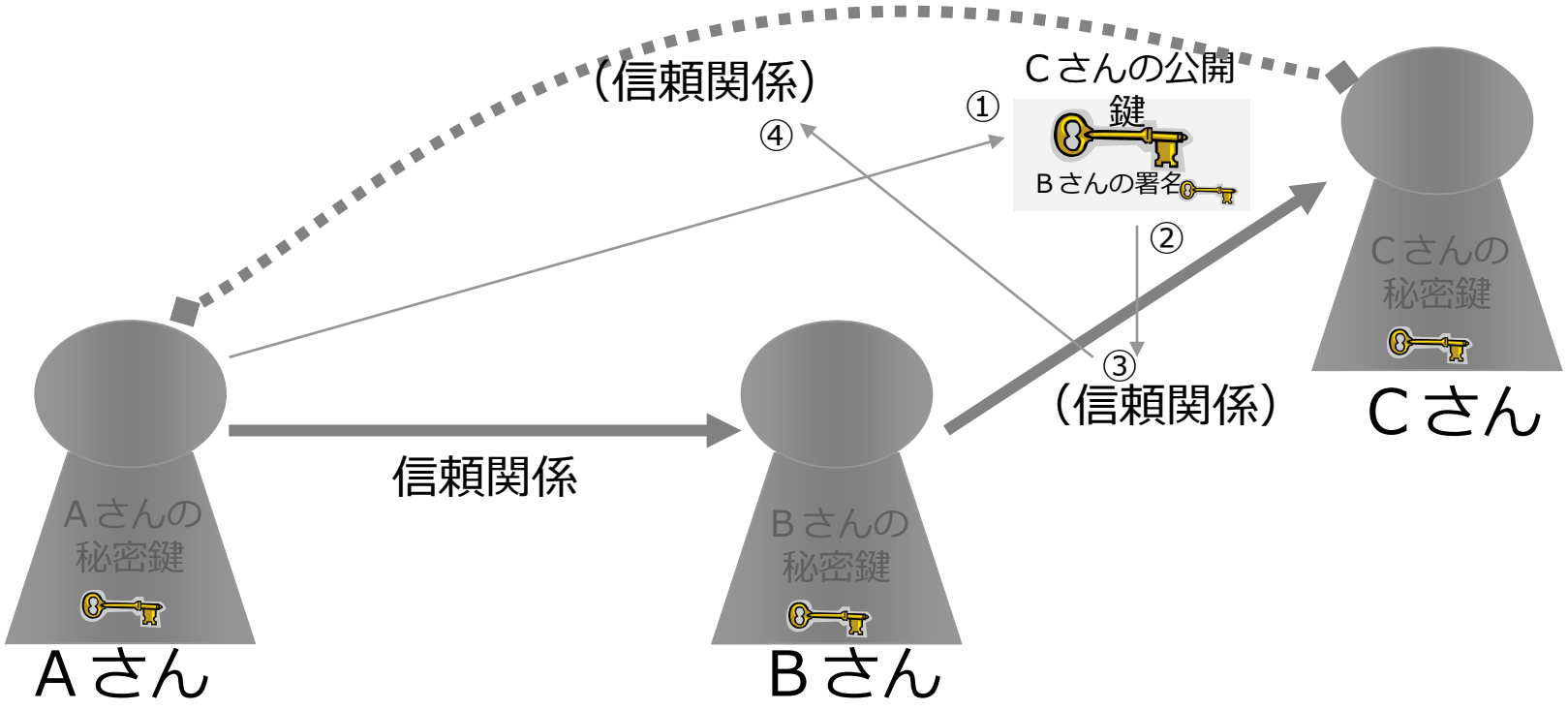
Aさんの秘密鍵 で署名したメッセージ③は、**Aさんの公開鍵** で検証が可能



信頼の輪について

（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、**<u>Ｃさんの公開鍵</u>** 内に 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