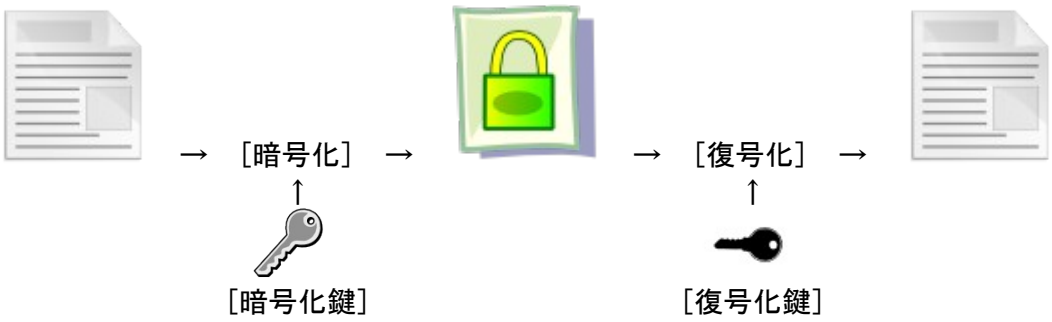
情報セキュリティ　ー 2017/12/07

3 情報セキュリティ対策

3.1 暗号技術

暗号化

データが第三者に(見られても・盗聴されても)わからないようにする



暗号化方式

・共通鍵暗号方式(秘密鍵暗号方式)

鍵が１つ(暗号化鍵と復号化鍵が同じ)

教科書例) シーザー暗号

DES, AES 方式が代表例

・公開鍵暗号方式

鍵が２つ(暗号化鍵と復号化鍵が違う)

||

「秘密鍵」と「公開鍵」

公開鍵で暗号化したデータは秘密鍵で復号化できる

秘密鍵で暗号化したデータは公開鍵で復号化できる

RSA 方式が代表例

特徴

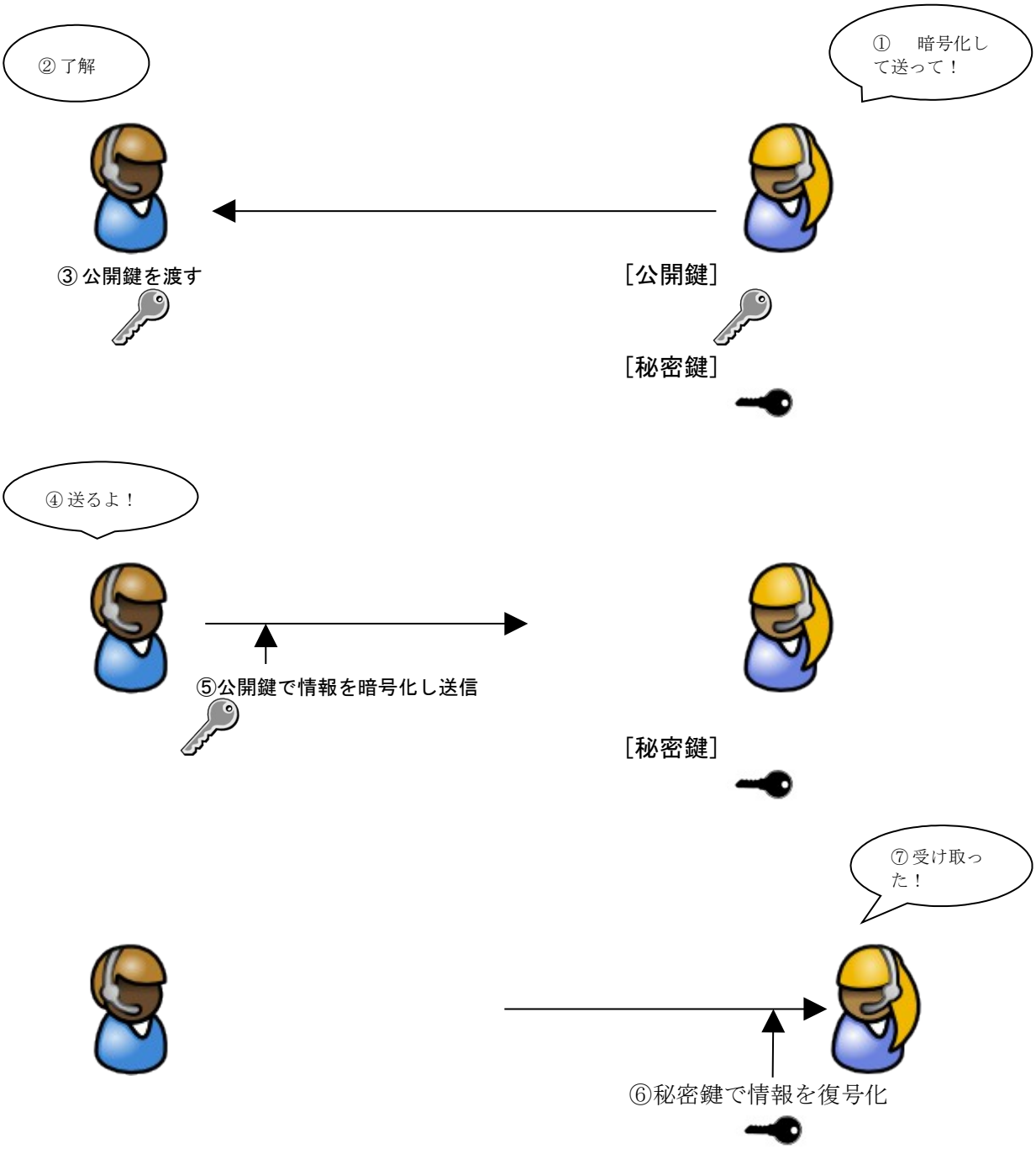
	共通鍵暗号	公開鍵暗号
暗号化/復号化の鍵	１つ(同じもの)	異なる(秘密鍵と公開鍵)
鍵の扱い	秘密	暗号化の鍵を公開(公開鍵) 復号化の鍵は秘密(秘密鍵)
不特定多数との通信	適さない	適する
処理の効率	良い	悪い
代表的なもの	DES	RSA

話題) 実際のインターネット上の通信では「公開鍵暗号」と「秘密鍵暗号」を組み合わせて使用する → SSL

・最初に「公開鍵暗号」によって「秘密鍵」を交換

・その後「秘密鍵暗号」によって情報通信

公開鍵暗号の手順



☆ポイント

公開鍵（公開されている）を手に入れる人は、誰でも暗号化することができる
だが、復号化できるのは秘密鍵（本人だけが管理）を持っている本人だけ！
||
鍵を１つ持っていても内容を見ることができない！

ハッシュ関数

内容がわずかでも改ざんされるとハッシュ値が大きく変わる性質がある
ハッシュ値から元のデータを推測することは困難
→ ハッシュ値をあらかじめ計算して比較
→ 改ざん検知

デジタル署名(電子署名)

改ざんの有無の検証 & 発信者が本人かどうか(=「なりすまし」を防ぐ)の証明

ハッシュ関数を利用

・改ざんの確認(情報の完全性)

公開鍵暗号方式を利用

・暗号化の逆
・「秘密鍵」で暗号化したメッセージをつける。「公開鍵」で戻せれば本人！

→ 改ざん，なりすまし，否認　の防止

PKI(Public Key Infrastructure)

公開鍵暗号を利用した電子証明社会基盤(セキュリティ・インフラ)
→ SSL，S/MIME などで利用

認証局(CA)

発信者が現実に存在する人・組織なのかを第三者によって保障してもらう
→　実印登録・印鑑証明
認証局を信頼できるか？が PKI 成功の基盤

GPKI → 政府が運営する PKI → 電子政府