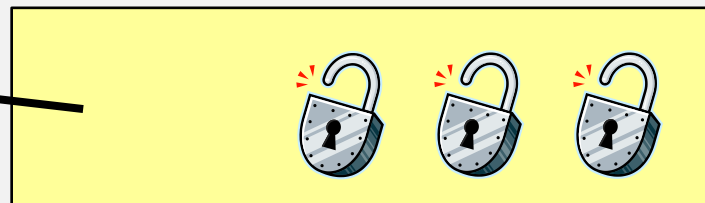


電子署名

公開鍵取得



復号



錠前を開ける

公開鍵

暗号化



鍵で施錠



秘密鍵

証明書

施錠できる者は秘密鍵を持つもののみ



この公開鍵の
持ち主は誰か

1. 公開鍵を信頼できる手段で取得 証明書
2. 認証局による電子署名
3. 自己申告を信頼 (初回) → **Phishingの可能性**

公開鍵基盤

(PKI)



認証局の
公開鍵で
復号 →



証明書：
持ち主は〇〇

暗号化

認証局



認証局の秘密鍵

認証局の公開鍵は既知