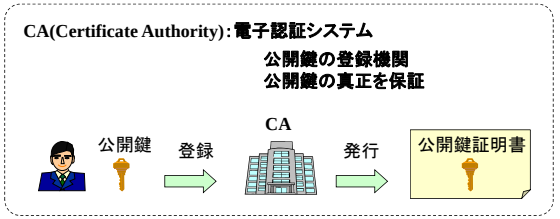
4．公開鍵インフラストラクチャ（PKI）

電子認証システム

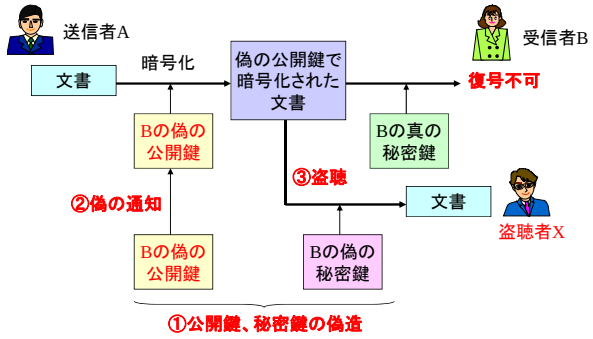
印鑑（実印）の登録

公開鍵の登録



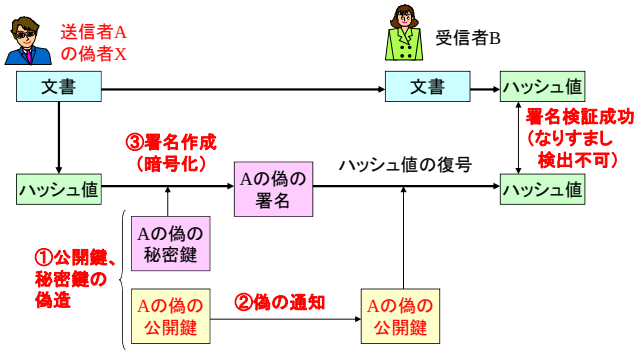
公開鍵証明書の必要性（1）

偽の公開鍵を用いた場合の情報の流出（暗号化への影響）



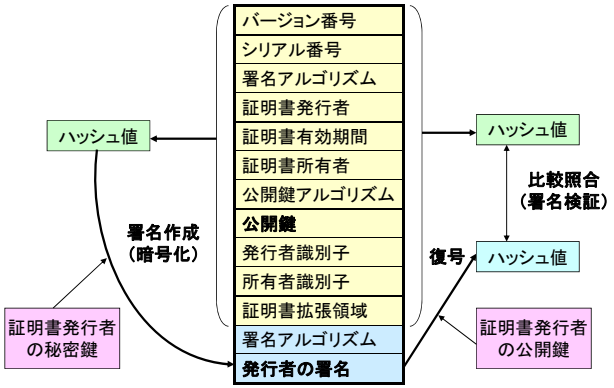
公開鍵証明書の必要性（2）

偽の公開鍵を用いた場合のなりすまし（ディジタル署名への影響）



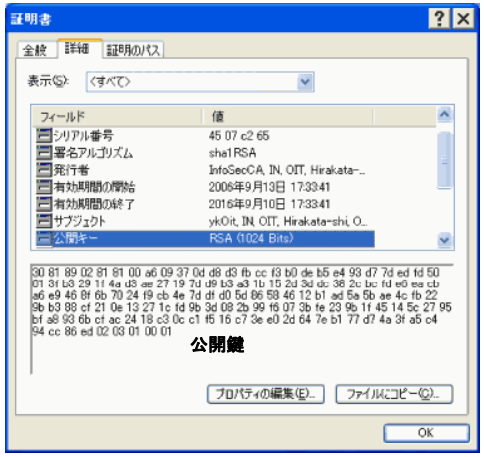
公開鍵証明書

X.509証明書（Certificate） X.500シリーズ勧告：ITU-T/ISO共同の国際標準

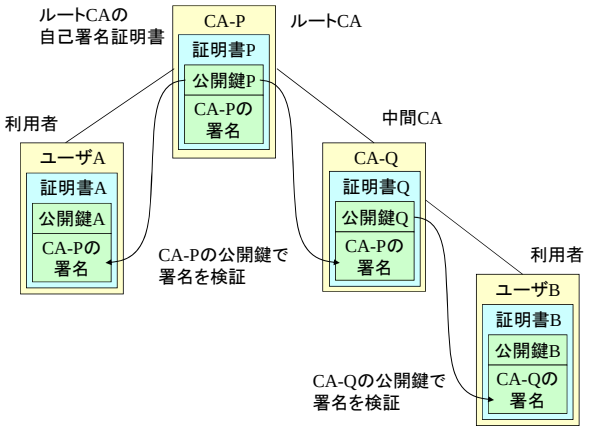


（注）公開鍵証明書はディジタル証明書と呼ばれる場合もある

付．公開鍵証明書の例

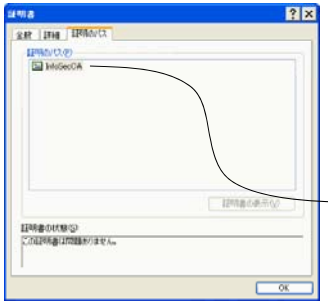


公開鍵証明書チェーン

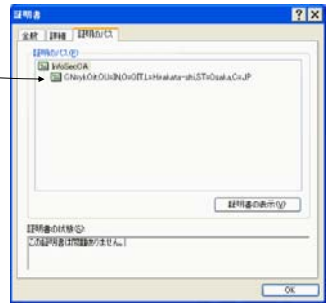


付．公開鍵証明書チェーンの例

CAの公開鍵証明書



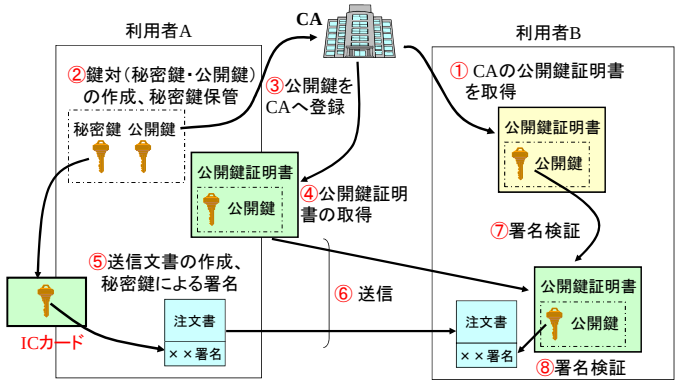
利用者の公開鍵証明書



公開鍵証明書使用の流れ

CA(Certificate Authority):公開鍵の登録機関 ⇨ 公開鍵の真正を保証

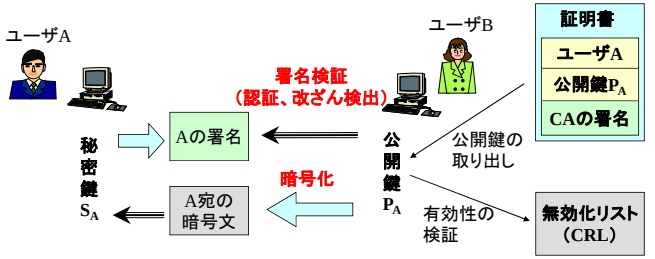
信頼できる第三者機関(TTP: Trusted Third Party)



PKI

公開鍵インフラストラクチャ(PKI: Public Key Infrastructure)

- 公開鍵暗号方式に基づくセキュリティ基盤(但し、共通鍵も使用)
- 特定のシステムに依存しない広域性
- 認証(Authentication)、完全性(Integrity)、秘匿性(Confidentiality)の提供

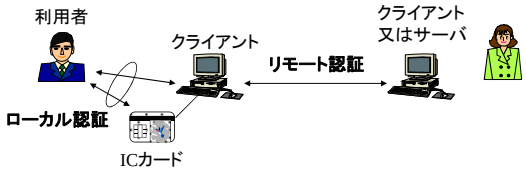


CRL: Certificate Revocation List

ローカル認証とリモート認証

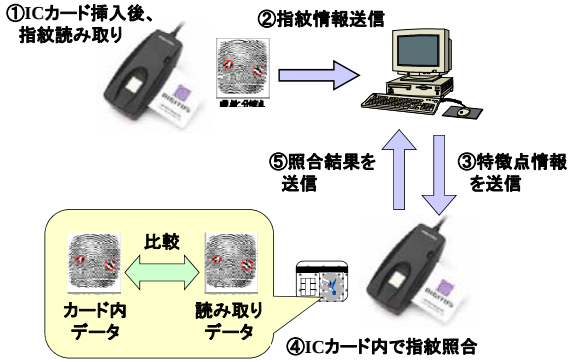
ローカル認証
- 利用者に物理的に近接した装置との間の認証
- 利用者が直接かかわる
- バイオメトリクス認証などを使用

リモート認証
- ネットワークを介したリモート装置との間の認証
- 利用者が直接かかわる場合とかかわらない場合がある
- PKI などを使用

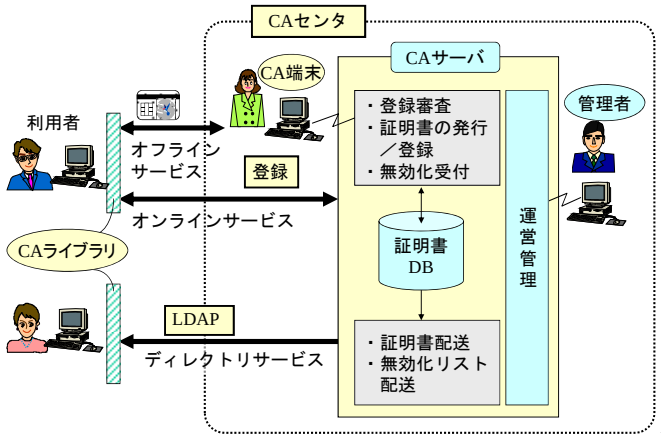


付. ローカル認証の例

ICカード内での指紋照合



CAセンタの構成



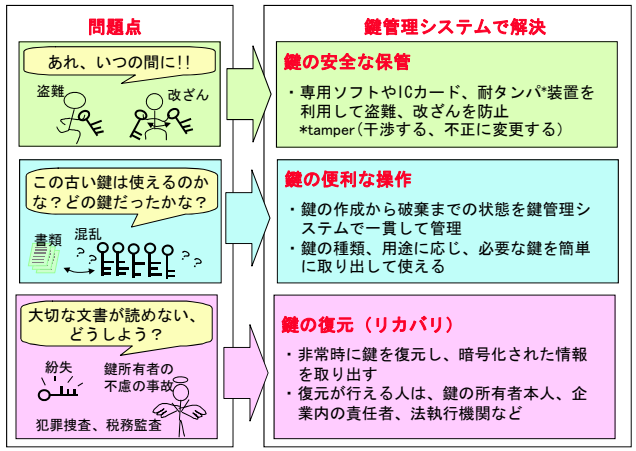
13

付. CAサービスの例

項番	機　能	ユーザから見た機能概要
1	**証明書発行**	公開鍵を登録し、その証明書を取得
2	**証明書無効化**	自分の証明書を無効化。無効化した証明書は証明書無効化リストCRLに掲載。
3	**証明書保留**	緊急時に自分の証明書の効力を停止（後で無効化）
4	**証明書無効化禁止／禁止解除**	指定したユーザの証明書の無効化を禁止／禁止を解除（特権機能）
5	**証明書参照**	指定したユーザの公開鍵証明書を取得
6	**証明書無効化リスト参照**	無効化された公開鍵証明書の一覧を取得
7	**利用者情報更新／参照**	登録した個人情報を更新または参照
8	**有効期限切れ予告通知**	公開鍵証明書の有効期限切れが来る前にCAから予告通知を行う
9	**証明書検証**	証明書の有効性を検証

14

付. 鍵管理と鍵リカバリ



15