2. 電子認証とPKI

1

認証

認証（身元確認）方法

1. 本人の記憶

パスワード、暗証番号など

2. 本人の所有物

身元確認用のトークン（社員カード、クレジットカード、運転免許証等）

3. 本人の特徴（Biometrics）

・**身体的特徴**：指紋、虹彩、網膜パターン、人相、掌形など
・**行為的特徴**：声紋、筆跡（署名）、キーストロークパターンなど

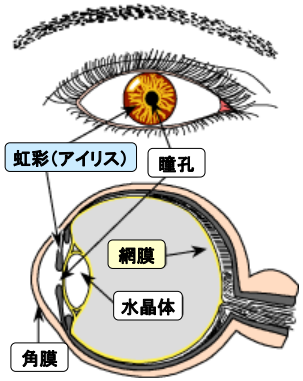
自分自身と特定のシステム（本人データの保持）との間の身元確認

2

付. バイオメトリクス認証製品(1)

NECの指紋認証装置
SecureFinger PI300PU-01

沖電気の虹彩認証装置
アイリスパス-S



3

付. バイオメトリクス認証製品(2)

カメラ部(上)
液晶ガイダンスパネル(下)

富士通の非接触型手のひら
静脈認証装置 PalmGraph

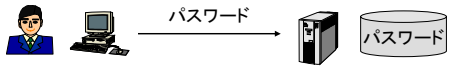
松下電工の顔認証装置
デイリフェイス

4

パスワード

パスワード

頭の中のパスワード



受信パスワードと保管パスワードの一致のチェック

パスワードの欠点

・意味のある文字列、アルファベット文字列、短い文字列にすると解読されやすい
・意味のない文字列、特殊文字を含む文字列、長い文字列にすると覚えにくい
・安全性向上のためには、パスワードの頻繁な更新が必要だが、それが面倒
・パスワードを端末に貼り付けるなどの不注意な利用者を排除することが困難

パスワードの推測

オンライン攻撃：オンラインで推測したパスワードを入力

オフライン攻撃（辞書攻撃）：パスワードファイルを盗み、辞書に基づき、パスワードを生成し、一致性をチェック

☆ 5

ワンタイムパスワード（1）

ワンタイムパスワード：一度限りの使い捨てパスワード

ワンタイムパスワードの方式

1. **同期方式**
   - ○ 時間同期
   - ○ カウンタ同期
2. **非同期方式**
   - ○ チャレンジ・レスポンス
   - ○ 一方向性関数

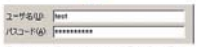
時間同期方式

6

付．時間同期方式の例（RSA SecurID）

①入力ウィンドウが表示される

②事前登録のユーザ名を入力



③事前登録のPIN番号とカードに表示された番号を連続して入力但し、画面上には表示されない

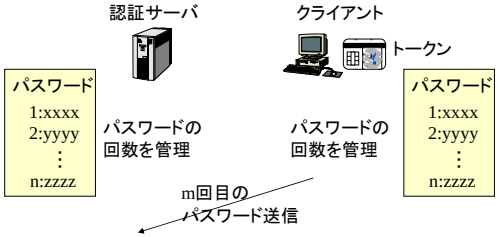
認証中画面

③認証OKなら、画面右下に鍵のマークが表示される

7

ワンタイムパスワード（2）

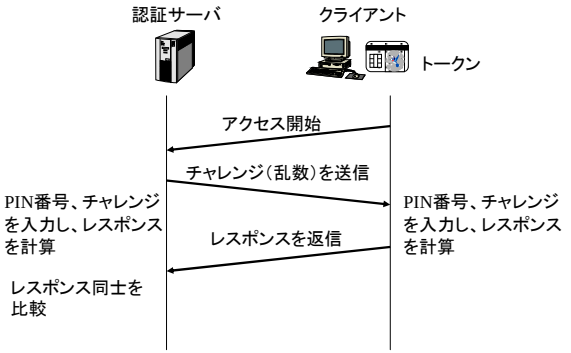
カウンタ同期方式



8

ワンタイムパスワード（3）

チャレンジ・レスポンス方式



（注）PIN: Personal Identification Number

S/Key

一方向性関数方式

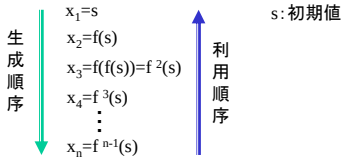
S/Key：Bellcore社によって開発された一方向性関数利用のワンタイムパスワード

一方向性関数　　f(x)としてMD4を使用

$y=f(x)$　容易に計算可能

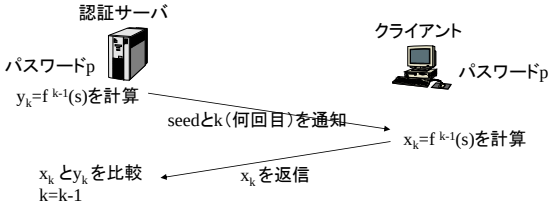
$x=f^{-1}(y)$　逆関数の計算は困難

ワンタイムパスワードの生成と利用

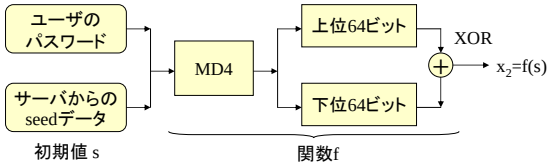


S/Keyによる認証

S/Keyによる認証手順

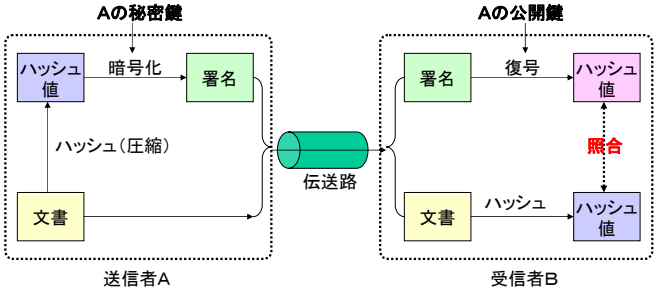


関数f の計算



ディジタル署名

公開鍵暗号によるディジタル署名

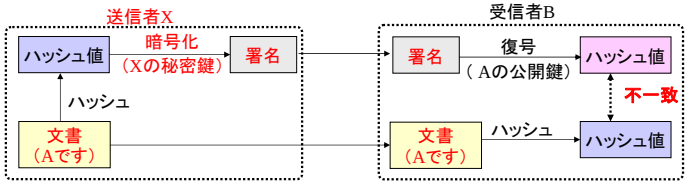


ハッシュアルゴリズムは共通

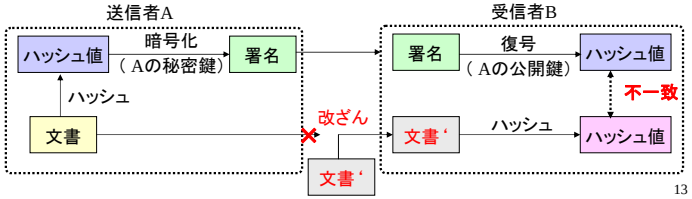
ハッシュ値：メッセージダイジェスト

ディジタル署名の効果

1. なりすましの検出

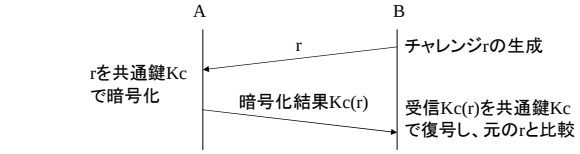


2. 改ざんの検出

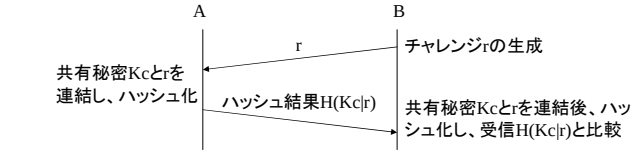


共通鍵暗号やハッシュによる認証

共通鍵暗号による認証



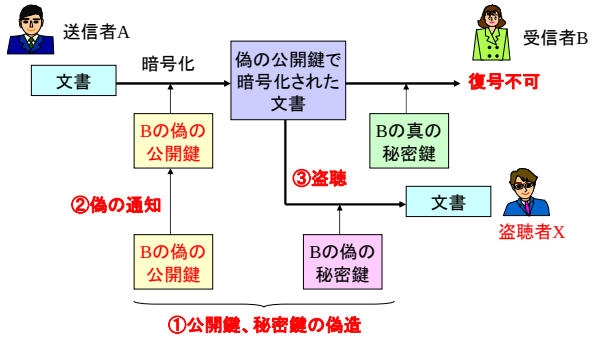
ハッシュによる認証



両方式とも、秘密情報を通信路に流すことなく、認証を行える

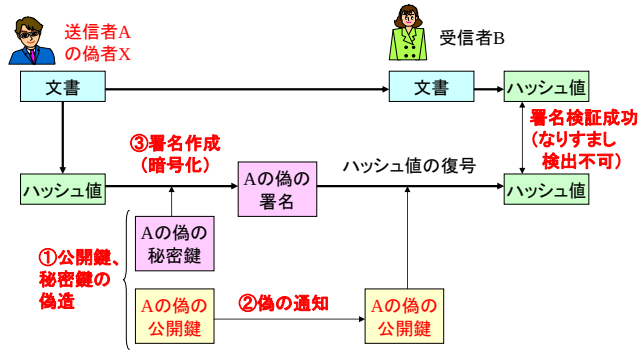
公開鍵証明書の必要性（1）

偽の公開鍵を用いた場合の情報の流出（暗号化への影響）



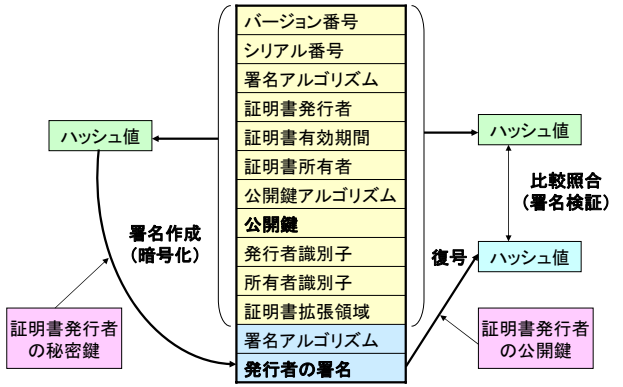
公開鍵証明書の必要性（2）

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）



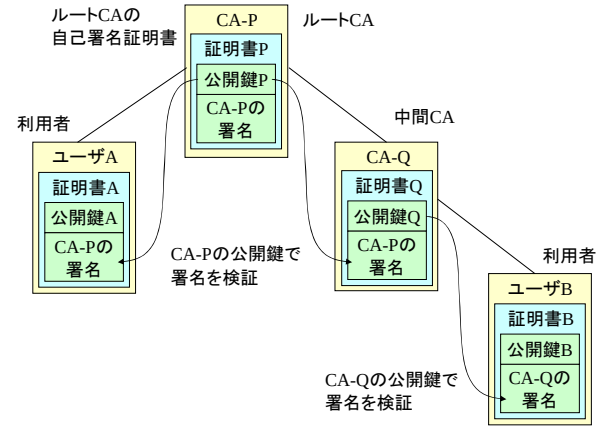
公開鍵証明書

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

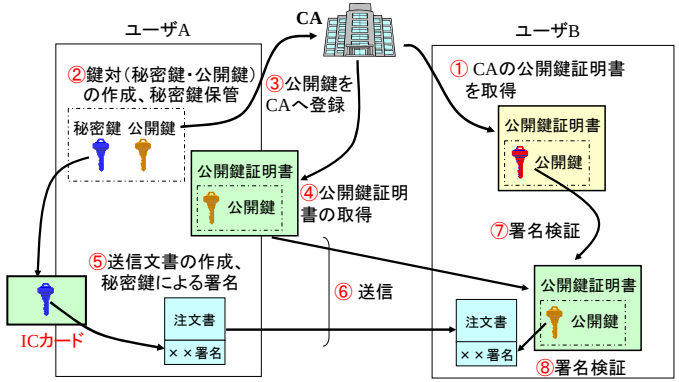
公開鍵証明書チェーン



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

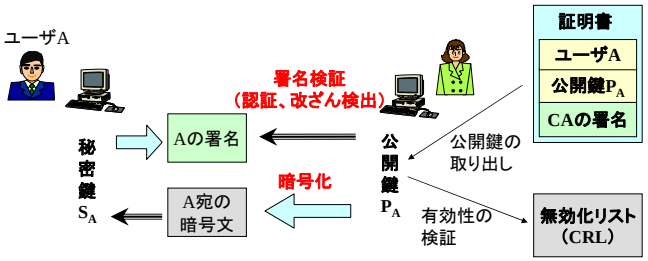
信頼できる第三者機関（TTP: Trusted Third Party）



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

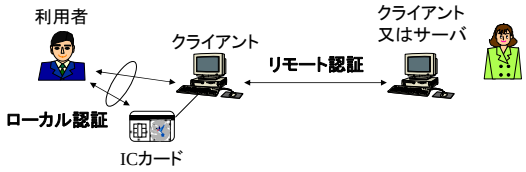


CRL: Certificate Revocation List

ローカル認証とリモート認証

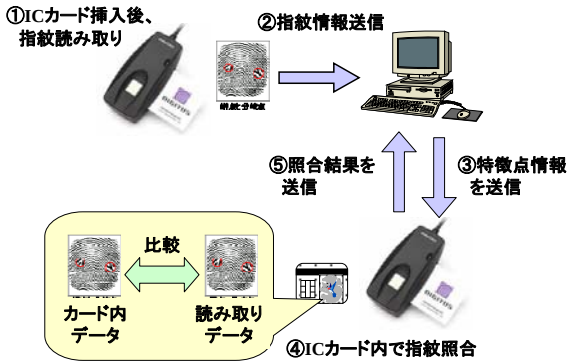
ローカル認証　・利用者に物理的に近接した装置との間の認証
・利用者が直接かかわる
・バイオメトリクス認証などを使用

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

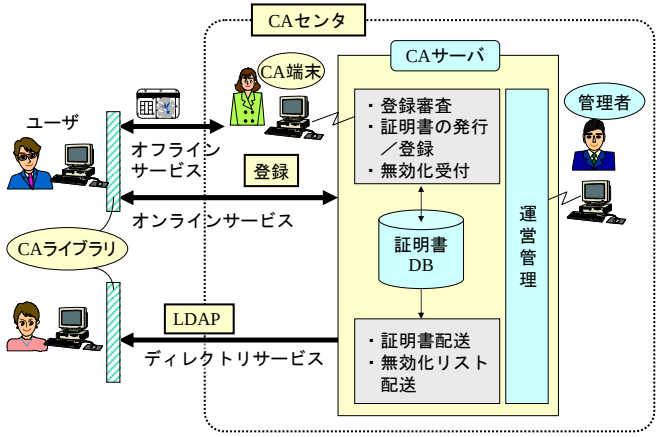


付．ローカル認証の例

ICカード内での指紋照合



CAセンタの構成



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