セコムIS研究所
Intelligent Systems Laboratory

PKI ～基礎と応用～
基礎編

セコム株式会社 IS研究所
サイバーセキュリティ・ディビジョン
松本　泰
yas-matsumoto@secom.co.jp
2003 年 12月 4日

セコムIS研究所
Intelligent Systems Laboratory

PKI ～基礎と応用～ 基礎編

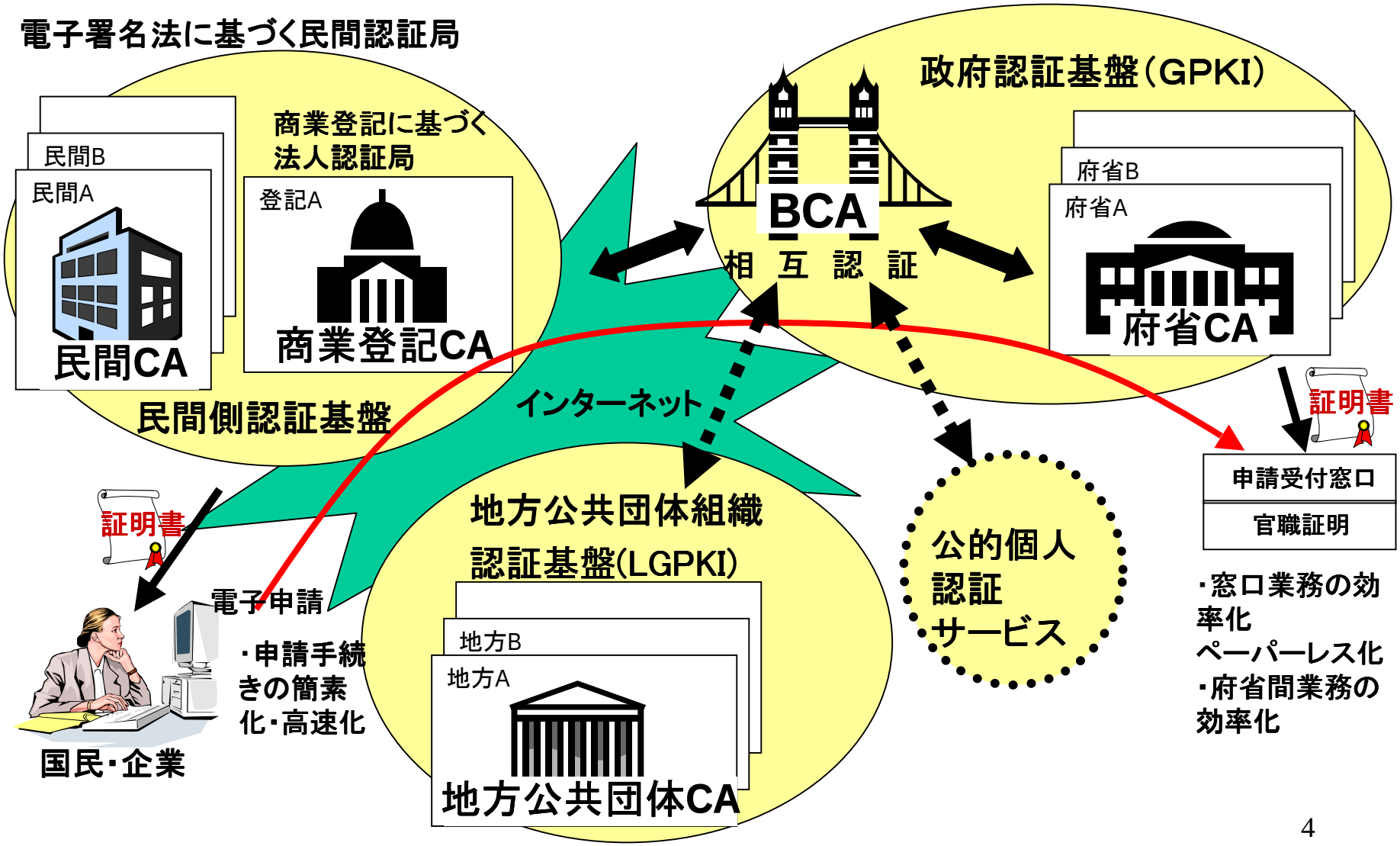
- PKIの動向とPKI技術の概要
- 署名者
- 署名検証者
- 認証局の信頼
- まとめ

セコムIS研究所
Intelligent Systems Laboratory

PKIの動向とPKI技術の概要

PKIの動向とPKI技術の概要
GPKI、LGPKIと公的個人認証サービス

セコムIS研究所
Intelligent Systems Laboratory



PKIの動向とPKI技術の概要
公的個人認証サービス

- 自治体が**市民**に配布する証明書
- 2002年12月のオンライ3法可決により正式に構築が決定
  - 「電子署名に係る地方公共団体の認証業務に関する法律（公的個人認証法）」
- 住基カードに証明証および鍵を格納可能
  - 住基カードは、2003年８月25日より配布開始
  - 耐タンパ性を備えたICカードに秘密情報を格納
    - #現時点ではちゃんと評価されていないという批判もある

セコムIS研究所
Intelligent Systems Laboratory

PKIの動向とPKI技術の概要
東海4県の電子申告

- 電子申告
- 東海4県の電子申告
  - 名古屋国税局管内（岐阜県、静岡県、愛知県、三重県の4県）で2004年2月から実施
  - 個人の所得税・消費税の電子申告を開始
  - 実質的に最初の公的人認証サービスの証明書を使ったアプリケーション??
- 全国への拡大
  - 2004年6月以降
- http://e-tax.nta.go.jp/

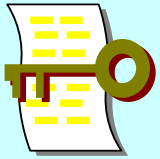
PKIの動向とPKI技術の概要
ユビキタス時代の認証技術

セコムIS研究所
Intelligent Systems Laboratory

- e-Japan戦略II – 次世代情報通信基盤の整備
  - 高速・超高速インターネットと無線インターネットの普及
  - いつでもどこでも何でもつながるユビキタスネットワーク
- ユビキタス環境での安全で便利な認証の統合
  - Anywhere, Anytime, Anyplace モバイルオフィスの実現
  - 理想的は、所持による認証（ハードウェアトークン）など組合したPKIが理想
  - 色々な認証を統合するためにはPKIの仕組みを正しく理解することが重要
    - 暗号クレデンシャルの扱い -> CryptoAPIなど
    - 証明書プロファイル
    - 証明書失効リストの扱い

ユビキタス時代の認証技術

セコムIS研究所

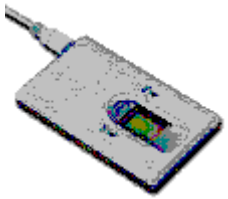


アリスの私有鍵

暗号クレデンシャル

アリスは、自分が守るべき情報は、ハードウェアトークンに格納して使用する。
ハードウェアートークンは、耐タンパー性が要求される。

基本的にアリスにとっての秘密情報は、アクセスポイント側には保持されない。



USBトークン

指紋認証

ICカード

セキュリティチップ搭載PC。

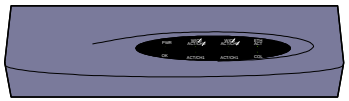
アリス

802.1X EAP-TLS

IPSec VPN
IKE X.509認証

SSLクライアント認証
SSL-VPN

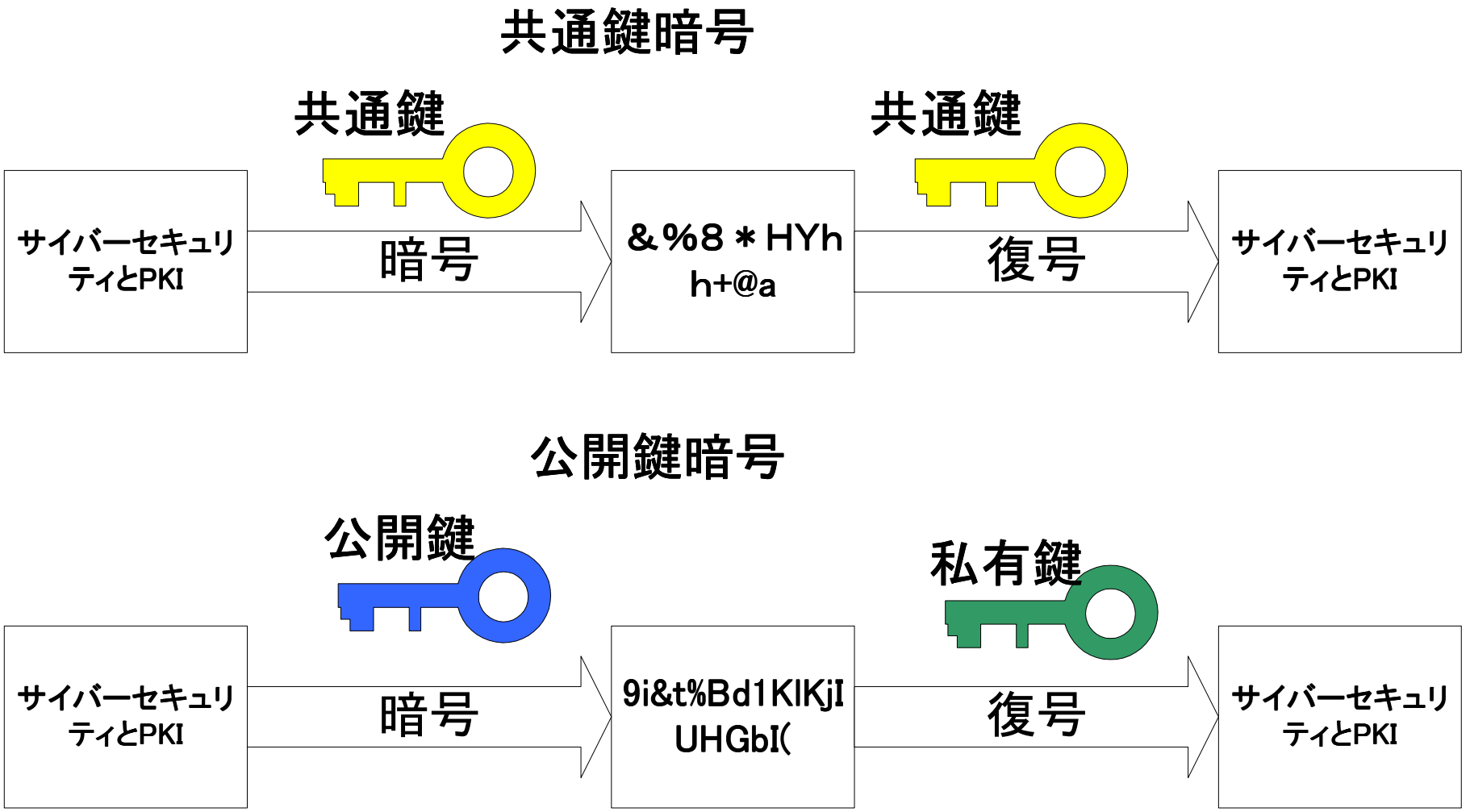
無線LANのアクセスポイント



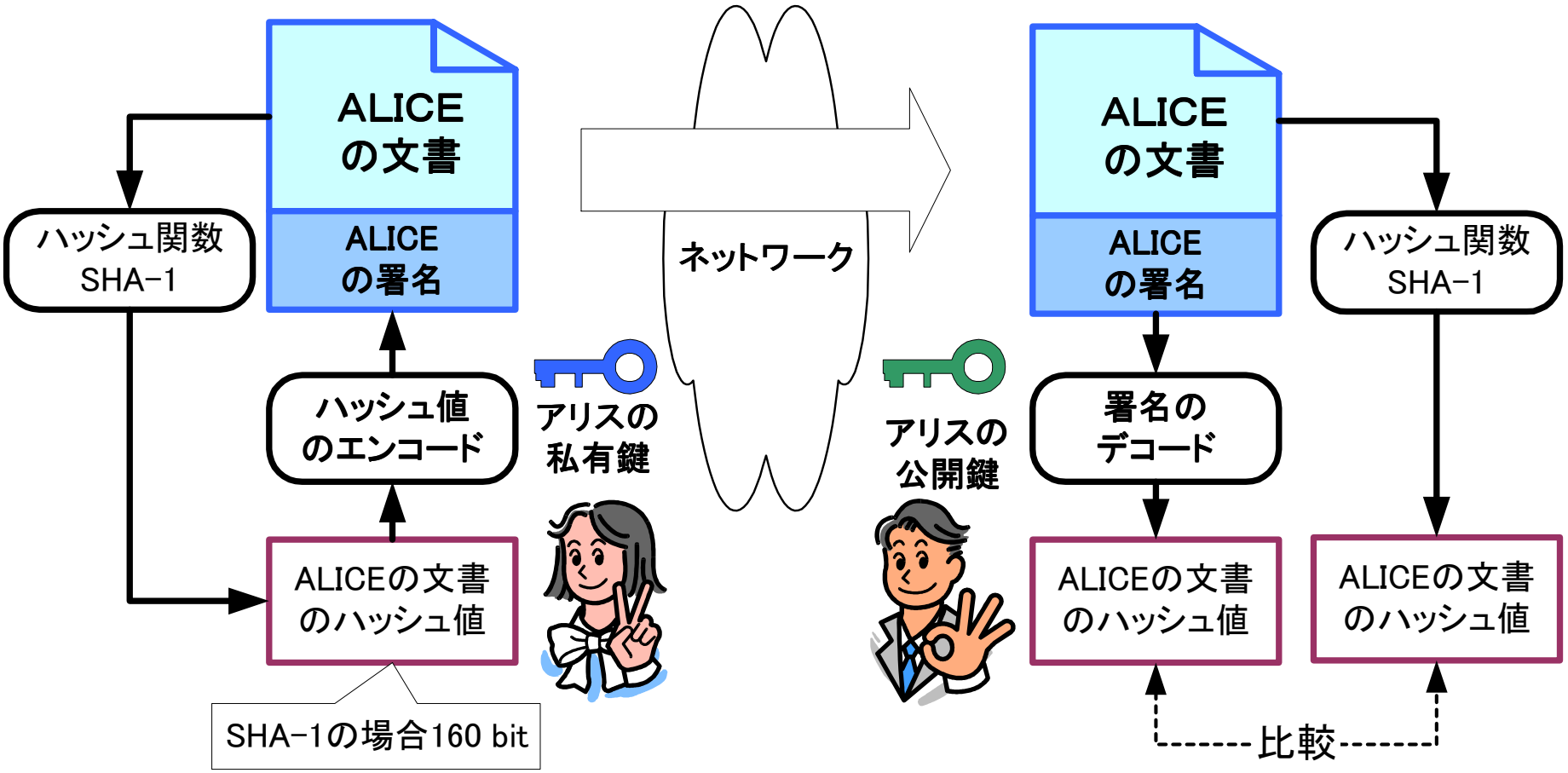
VPN装置

WWWサーバ

PKIの動向とPKI技術の概要
共通鍵暗号と公開鍵暗号

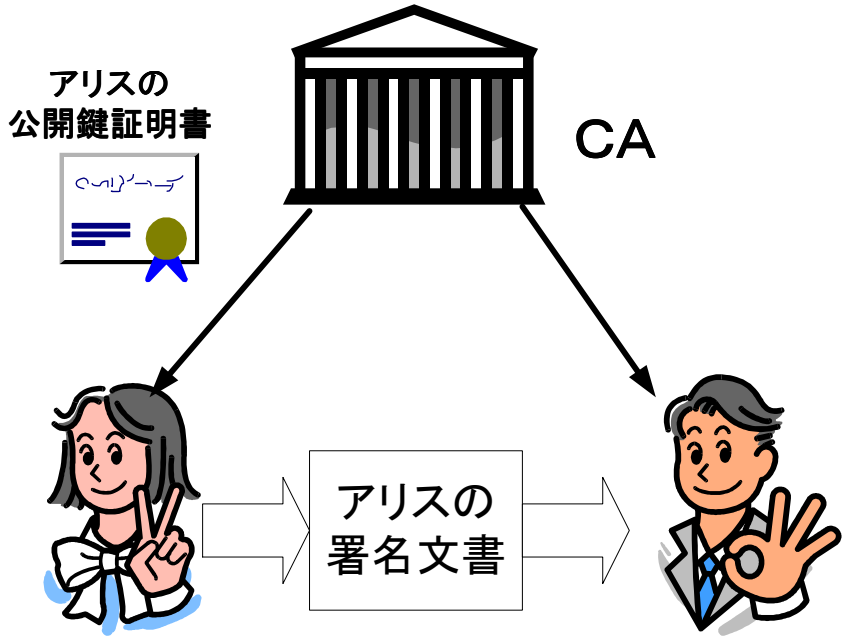


PKIの動向とPKI技術の概要
署名の仕組み

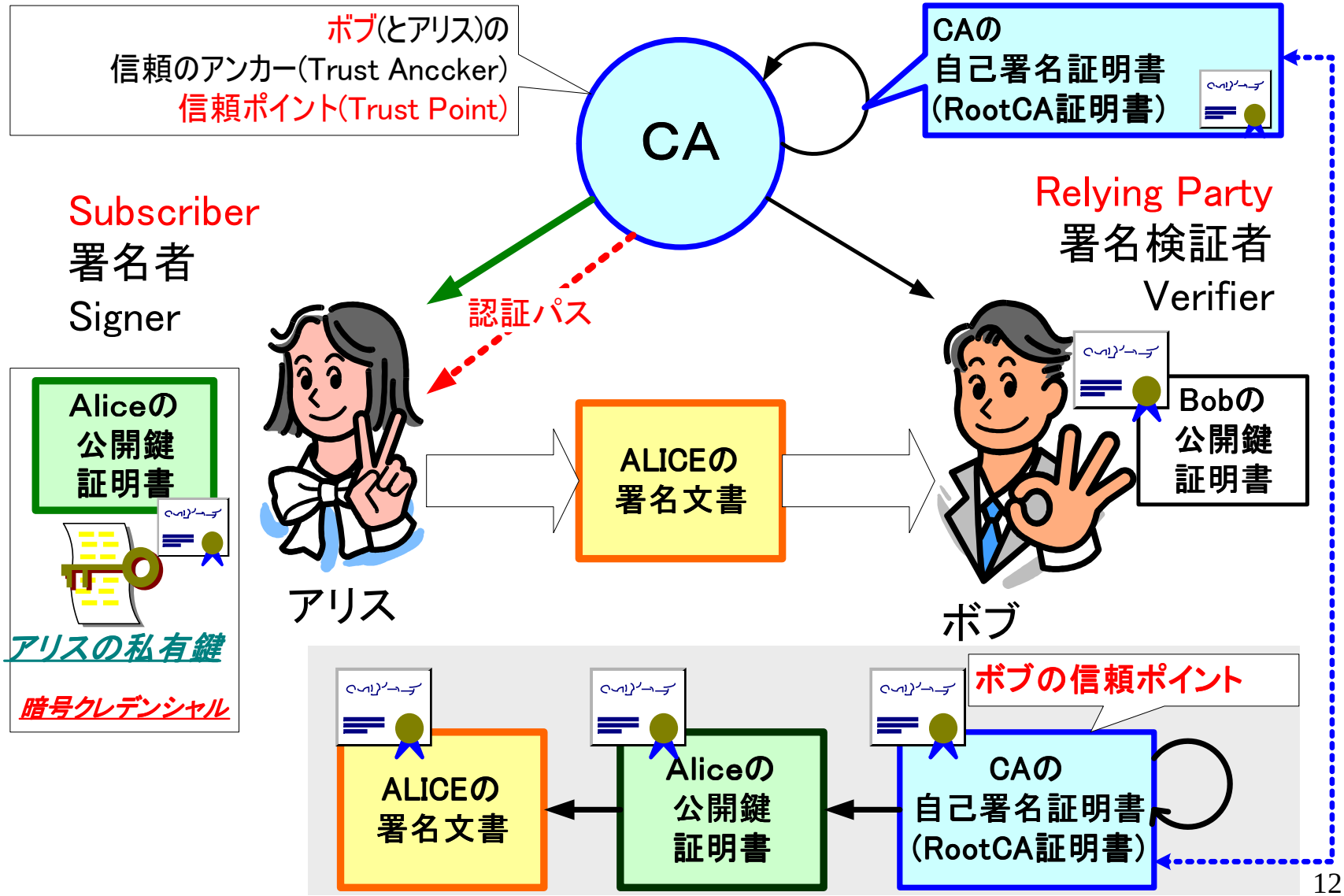


PKIの動向とPKI技術の概要
TTPよる認証（アリスの公開鍵を信じるのか）

- TTP(Trusted Third Party)とは
  - 信頼できる第三者機関
  - TTPによって署名されたデータは信用できるものとする
  - 代表的な例はCA（Certificate Authority）
  - CAは印鑑証明を発行してくれる役所のイメージ

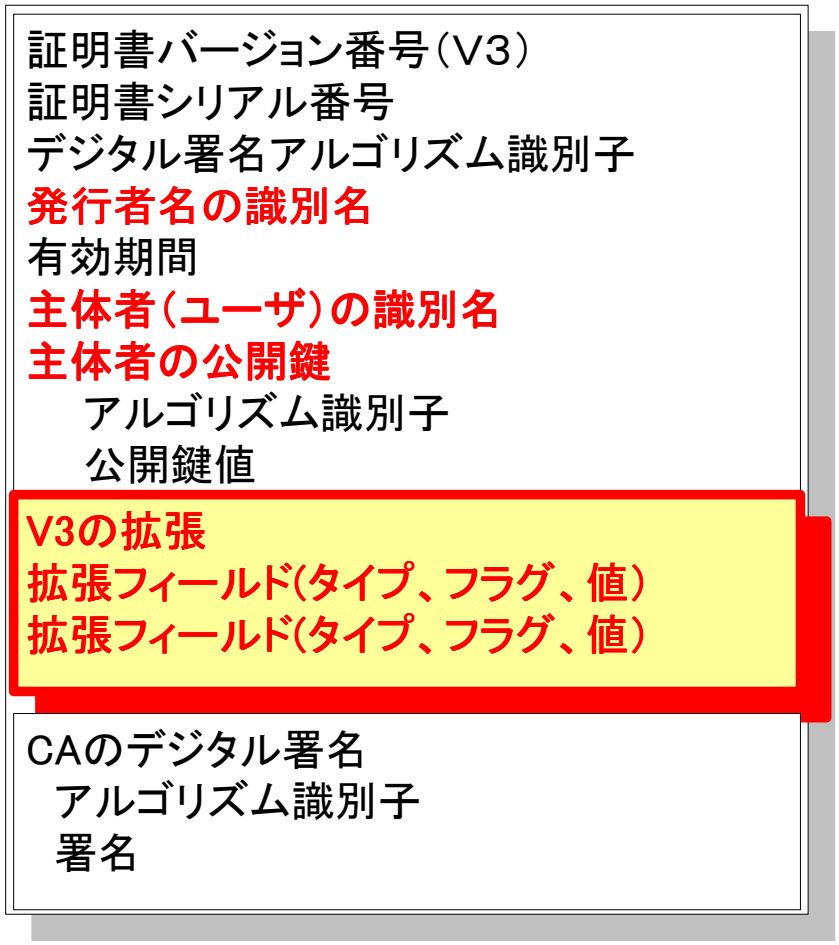


PKIの動向とPKI技術の概要
PKIの基本的な信頼モデル



PKIの動向とPKI技術の概要
X.509証明書

セコムIS研究所
Intelligent Systems Laboratory



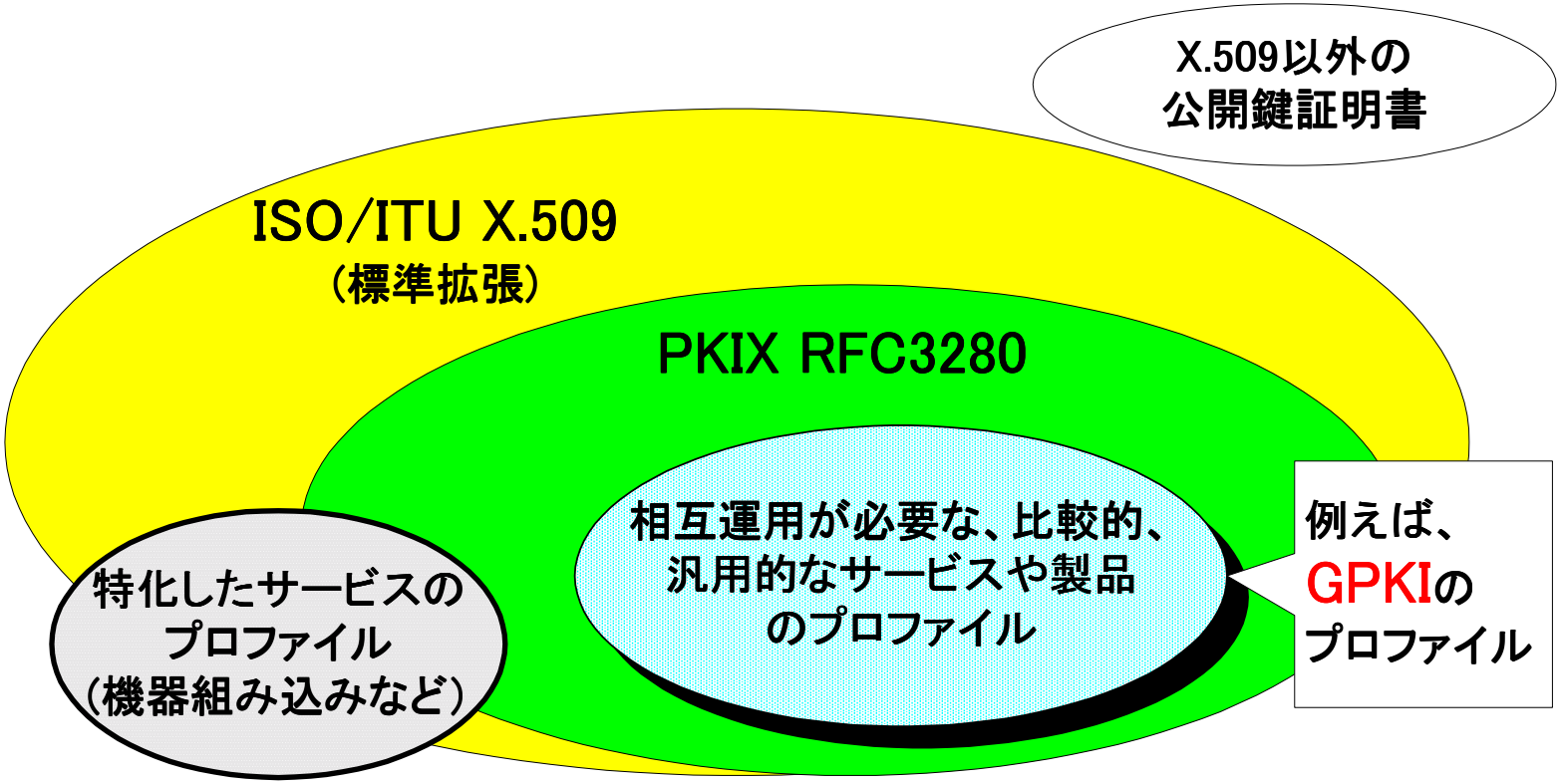
- 代表的な公開鍵証明書
  - 主体者(アリス)と、主体者(アリス)の公開鍵や、その他の属性をCA鍵(アリスの証明書を発行したCAの署名鍵)の署名でバインドする。
  - この時、主体者(アリス)の公開鍵に対応した私有鍵は、主体者(アリス)しか使用できないことが理想。
- **1997年版 X.509 3rd Edition**
  - X.509v3証明書フォーマット
    - X.509V3拡張
  - 14の標準拡張フィールド

PKIの動向とPKI技術の概要
X.509証明書拡張(v3拡張)

セコムIS研究所
Intelligent Systems Laboratory

No	標準拡張(X.509v3)	説明
1	発行者鍵識別子	発行者の鍵の識別に使用されCA鍵の更新に必要
2	主体者鍵識別子	主体者の鍵の識別に使用されCA鍵の更新に必要
3	鍵使用方法	私有鍵の使用方法。例えば署名用鍵で、暗号化を禁止する
4	私有鍵有効期間	証明書の有効期間に対して、私有鍵の有効期間。
5	証明書ポリシ	証明書ポリシIDなどが格納される。ポリシによる制御などに使用
6	ポリシマッピング	PKIドメイン間のポリシのマッピングを行う
7	主体者別名	主体者の別名が格納される。例えばVPN装置の場合のIPaddress
8	発行者別名	発行者の別名が格納される。
9	主体者ディレクトリ属性	証明書の主体者のためのディレクトリ属性
10	基本制約	証明書の種類(CAorEE)。CAだった場合パス数の制限
11	名前制約	CA証明書で、相手のCAが発行する名前による制約
12	ポリシ制約	CA証明書で、相手のCAが発行するポリシ関係制約
13	拡張鍵使用方法	"鍵使用方法"以外の鍵使用方法のOIDが格納される。
14	CRL配布点	失効情報リストの配布点のDNやURLが格納される。

PKIの動向とPKI技術の概要
証明書のプロファイルの関係



- RFC3280（RFC2459）準拠の意味するもの
  - 証明書発行そのものよりも、そのプロファイルを解釈するアプリケーションの実装が格段に難しい。アプリケーションにおいて、**100％ RFC3280**サポートは、まずない。

PKIの動向とPKI技術の概要
X.509証明書拡張の実装とGPKIの要求
（クライアントの証明書検証の実装）

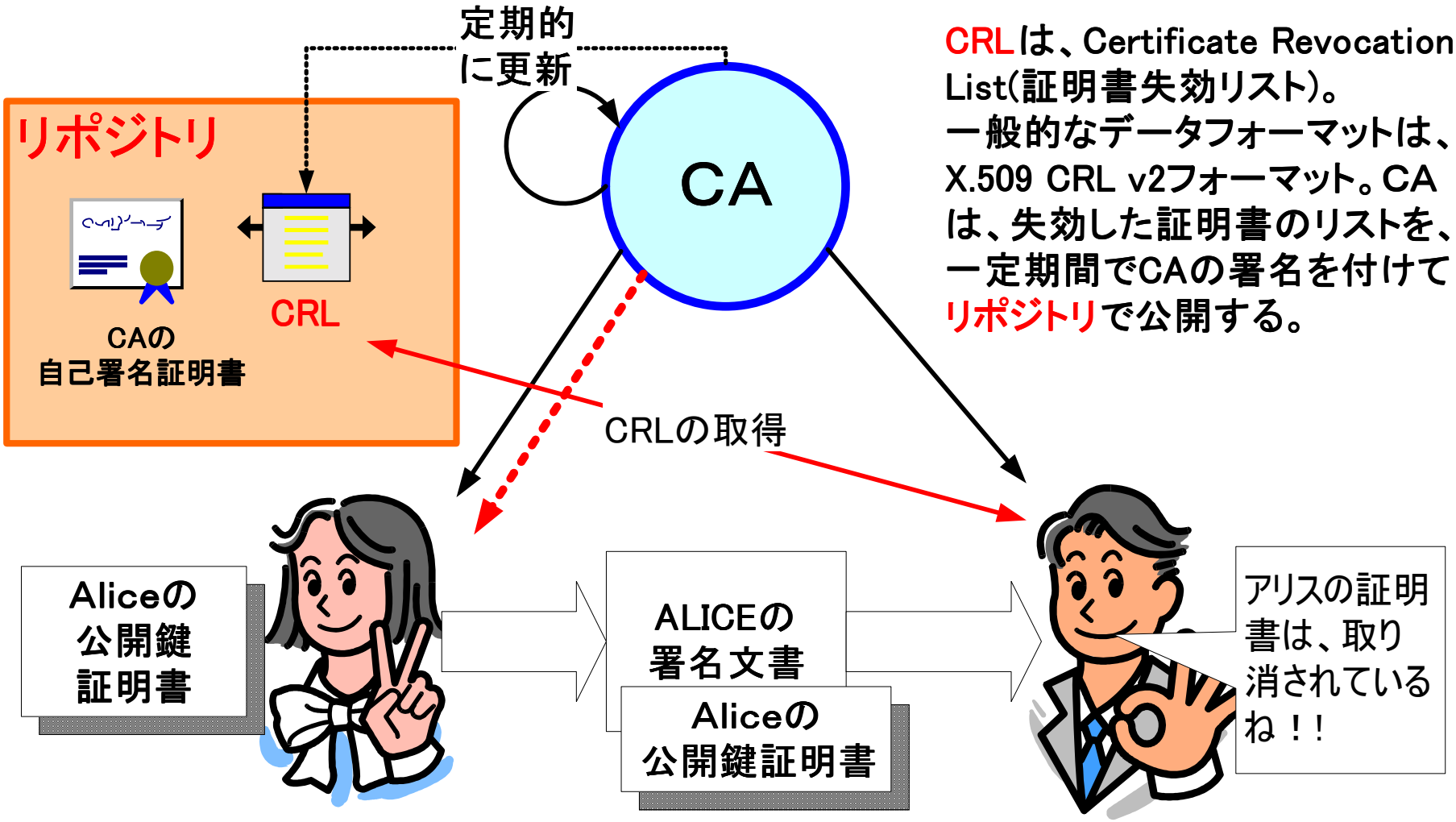
セコム IS 研究所
Intelligent Systems Laboratory

	Microsoft CryptoAPI Win-2000	Micosoft CryptoAPI Win-XP	JDK1.4 Cert. Path lib.	サンプル実装(*1)	GPKIの要求（パス構築、パス検証）
基本制約拡張	○	○	○	○	必須
ポリシ制約拡張	×	○	○	○	必須
ポリシマッピング拡張	×	○	○	○	必須
名前拡張	×	○	○	○	必須
AIA拡張 / OCSP	×	×	×	○	必須(官側のみ)
動的パス構築	×	△	○	○	必須
CRL IDP *2	×	○	×	○	必須

*1　Challenge PKI 2002プロジェクトで開発したサンプル実装

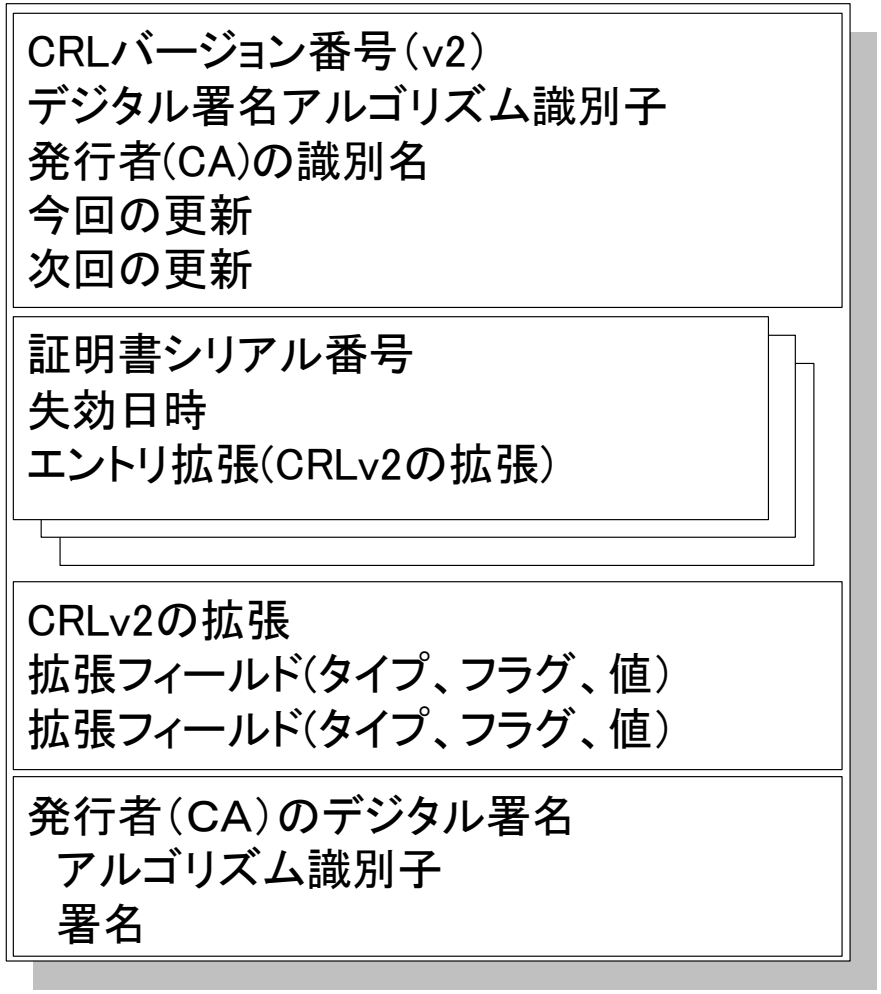
*2　これはX.509証明書ではなくCRL。 CRL IDP (issuing distribution point)

PKIの動向とPKI技術の概要
証明書の失効



CRLは、Certificate Revocation List(証明書失効リスト)。
一般的なデータフォーマットは、X.509 CRL v2フォーマット。CAは、失効した証明書のリストを、一定期間でCAの署名を付けてリポジトリで公開する。

PKIの動向とPKI技術の概要
CRL（証明書失効リスト）



- **CRL**
  - **あるCAが発行した証明書の有効期限内に証明書を失効したい場合、このCRLに、失効したい証明書のシリアル番号を入れて*リポジトリ(LDAPサーバなど)*で公開する。**
  - **CRLは一定期間毎にCAの署名を付けて発行される。**
- **1997年版 X.509 3rd Edition**
  - CRLv2フォーマット
  - X.509v3証明書と同じく拡張がある

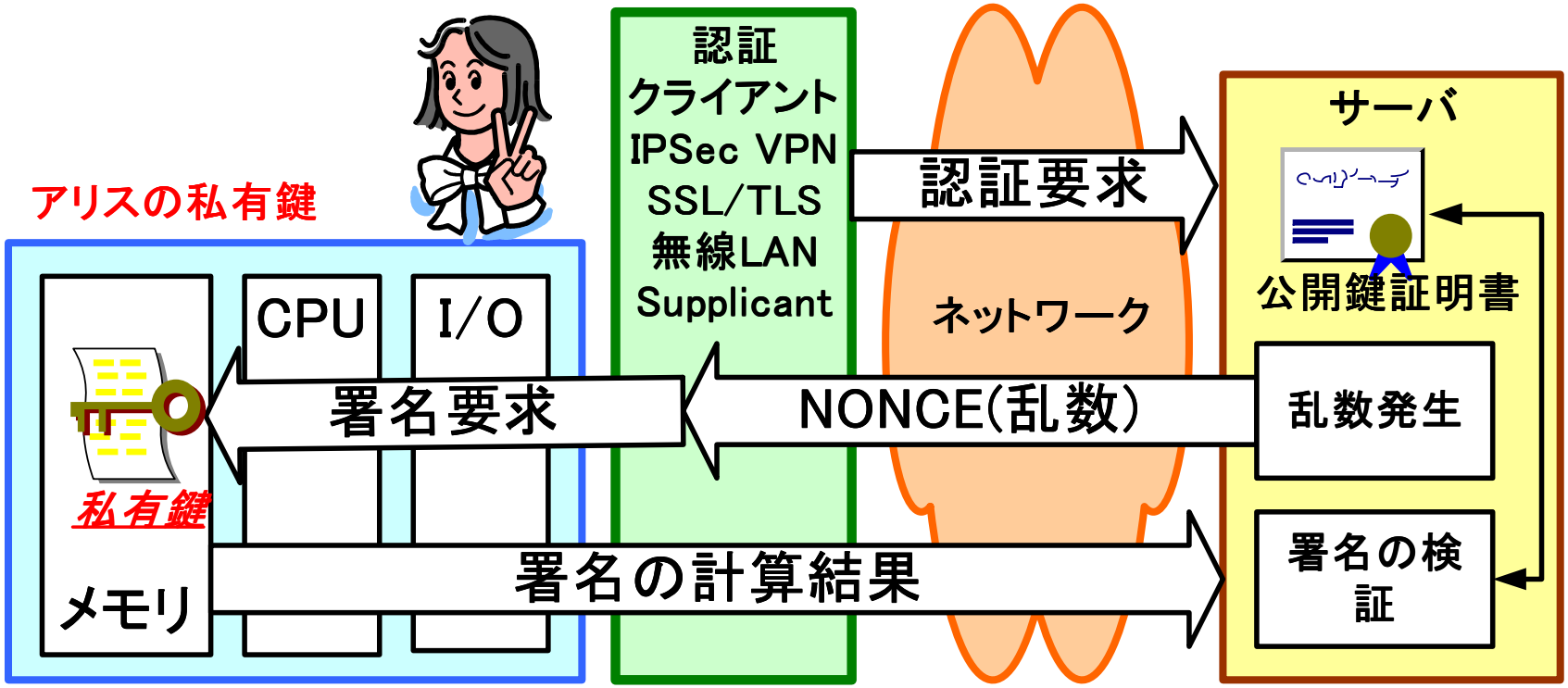
PKIの動向とPKI技術の概要
X.509 の証明書フォーマット

X.509 Edition	証明書 フォーマット	CRL フォーマット	備考
1st Edtion 1988	V 1	V 1	古いrootCAの証明書にV1 フォーマットのものがある
2nd Edtion 1994	V 2	V 1	ほとんど使用されていない??
3rd Edtion 1997	V 3	V 2	14個の(v3)標準拡張フィールド
4th Edtion 2000	V 3	V 2	標準拡張フィールドがひとつ追加された

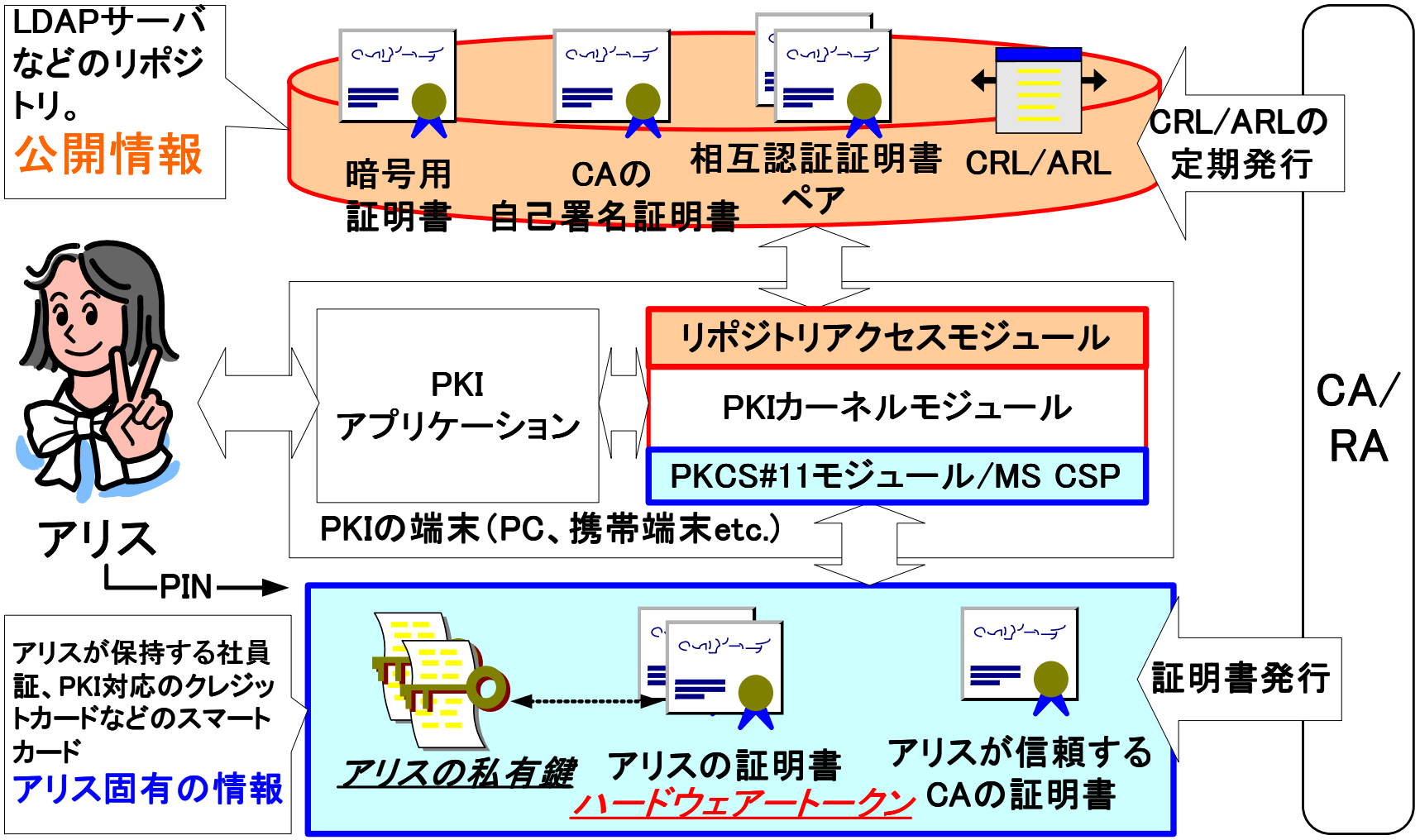
PKIの動向とPKI技術の概要
ハードウェアトークンを使用した認証の例

セコムIS研究所
Intelligent Systems Laboratory

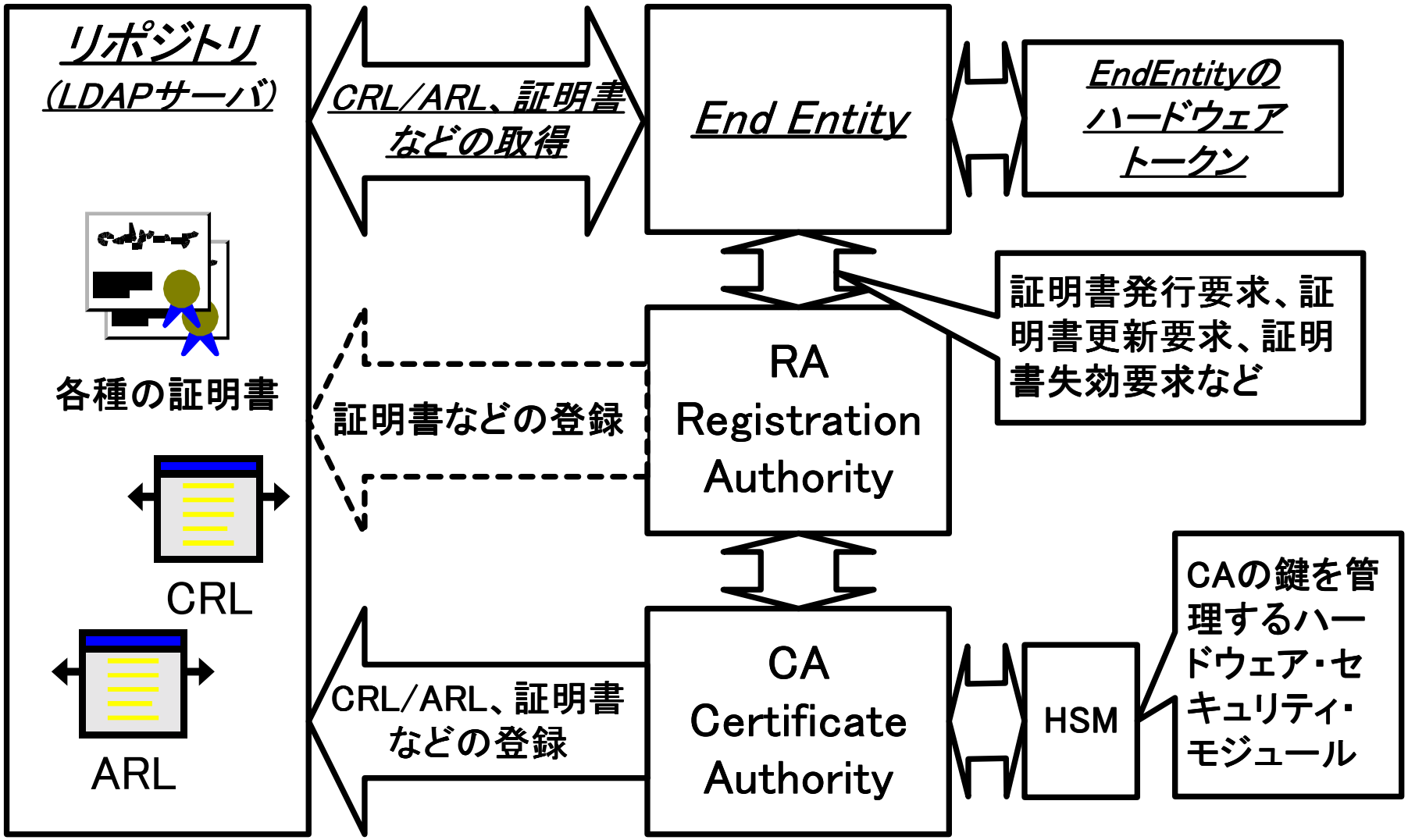
- アリスの秘密情報（私有鍵）はハードウェアトークンから出ない
  - もちろんネットワークにも流れない
- アリスの秘密情報は、サーバには、格納されない
  - サーバは、アリスの秘密情報（例えばパスワード）を預かる必要がない
  - これは、アリスとっても、サーバの運用者にとってもメリット



PKIの動向とPKI技術の概要
PKIアプリケーション環境の例

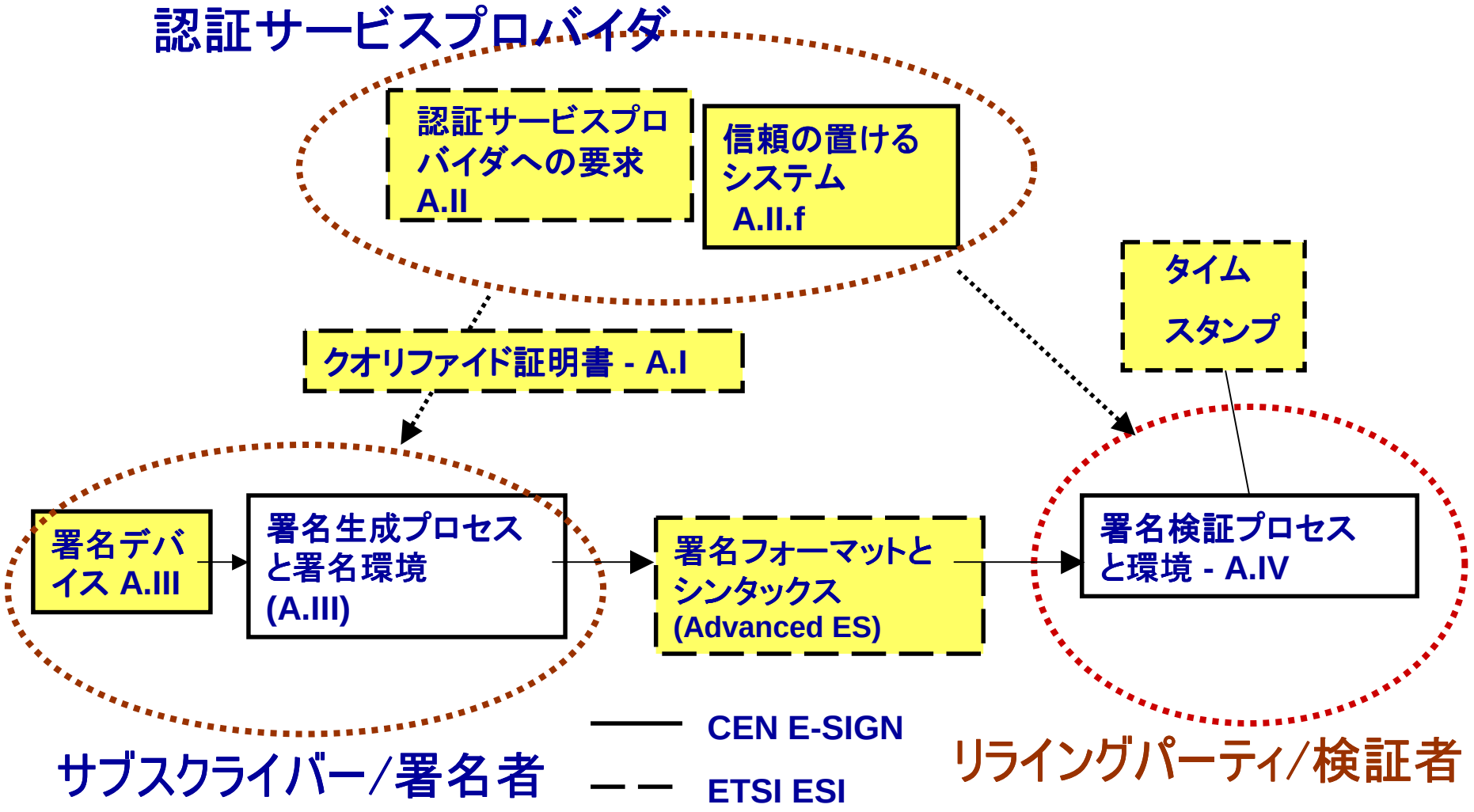


PKIの動向とPKI技術の概要
PKIの基本コンポーネント



PKIの動向とPKI技術の概要

EESSIの認証フレームワーク



PKIの動向とPKI技術の概要
EESSIの認証フレームワーク

セコム IS 研究所
Intelligent Systems Laboratory

- A.I
  - クオリファイド証明書　　自然人に発行する証明書プロファイル
- A.II
  - 認証サービスプロバイダへの要求
  - 信頼の置けるシステム
- A.III
  - 署名デバイス　　Secure signature creation device
  - 署名生成プロセスと署名環境
- A.IV
  - 署名検証プロセスと環境
- その他
  - タイムスタンプサービス
  - 署名フォーマット

PKIの動向とPKI技術の概要
PKIが安全であるための基本的な要件

セコム IS 研究所
Intelligent Systems Laboratory

- Subscriber側（アリス）の要件
  - セキュアな署名
    - なりすましをいかに防ぐか
    - 署名に使用する*私有鍵をいかに保護*するか??
    - セキュアなハードウェアトークンが有効
- Relying Party側（ボブ）の要件
  - 署名検証、証明書検証をいかに行うか
    - リポジトリ(LDAPサーバ)から必要な情報を取得
      - CRL、ARL、相互認証証明書ペアなど
    - ハードウェアトークン等に格納された*信頼ポイントの公開鍵*からのリポジトリなどから読み出した情報を元に証明書チェーンを構築、そしてパス検証を行う
- 認証局の要件
  - 認証局の運用
  - 証明書やCRLを署名する鍵の管理
  - 本人の確認方法
  - Etc…