

# 認証局の導入と運用

～PKIアーキテクチャの考え方とその運用～

---

**NEC** IT基盤システム開発事業部  
セキュリティ技術センター 小松文子(Ayako Komatsu)  
a-komatsu@ay.jp.nec.com

# contents -

---

- 認証局と公開鍵証明書の発行
  - PKIモデル
  - 認証局と公開鍵証明書発行のながれ
- PKI導入検討ステップ
  - PKIアーキテクチャ
  - 鍵運用ライフサイクル
  - 証明書ポリシーと運用規程
- 証明書ポリシーと運用規定
- グリッド環境への適用課題

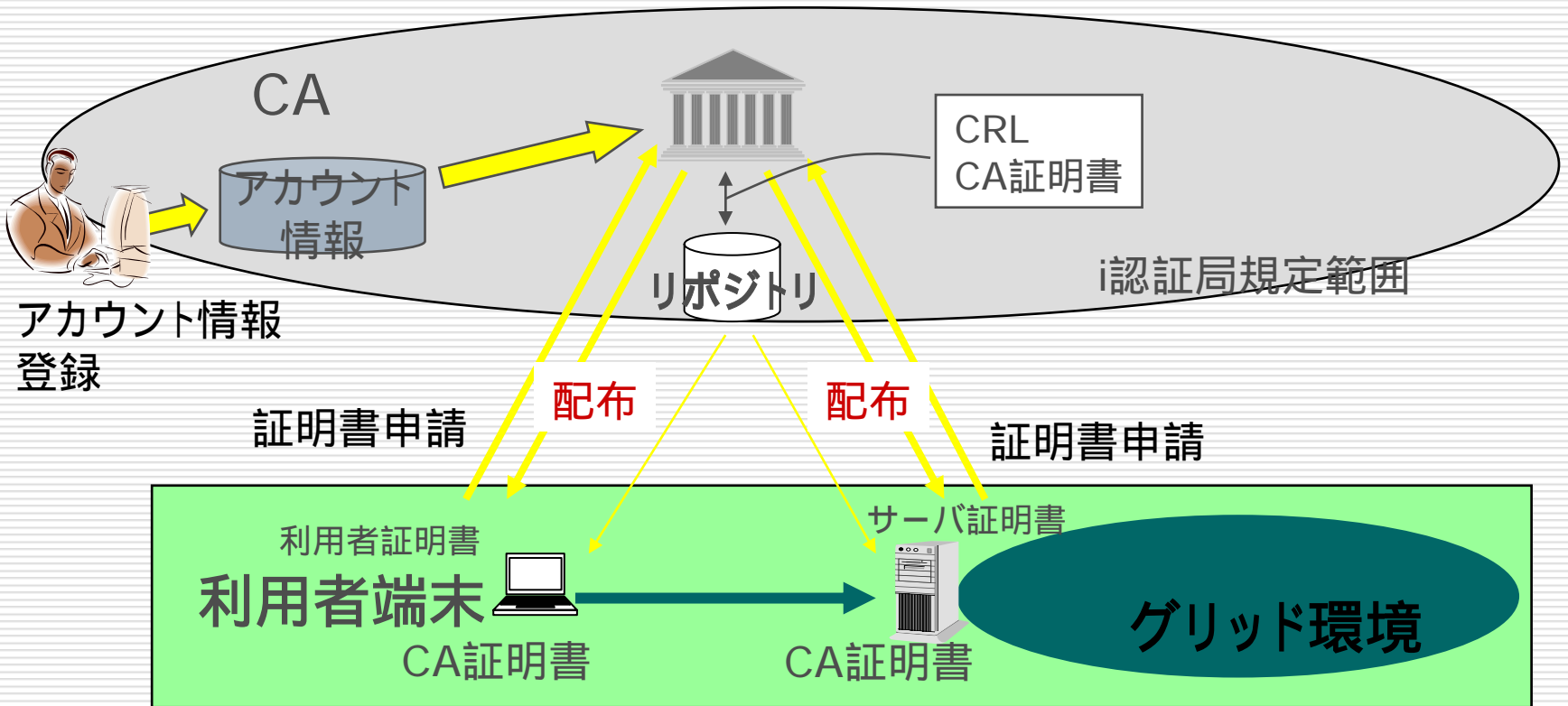
# PKIの要素

---

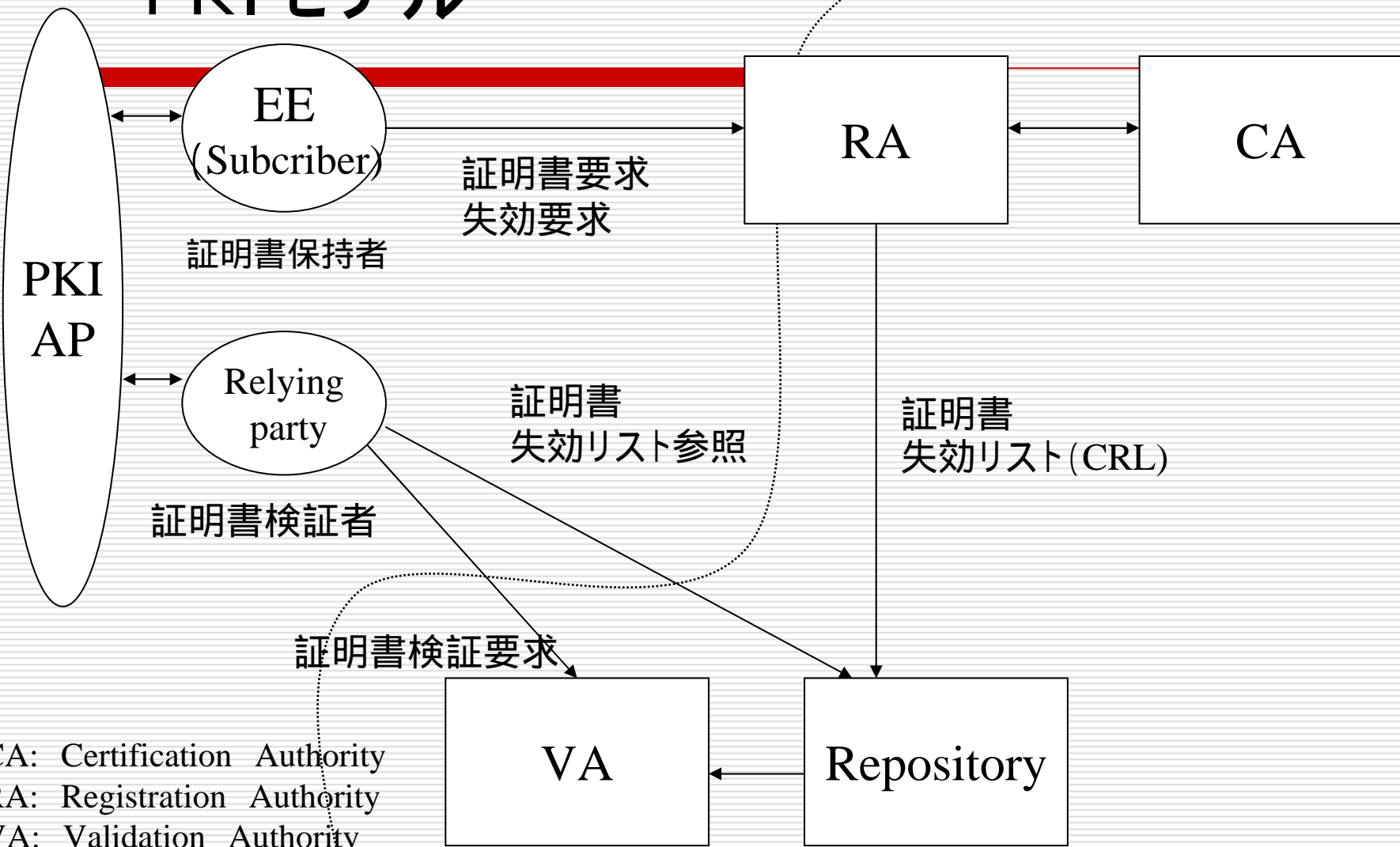
- 認証局:CA(Certification Authority)
- 登録局:RA(Registration Authority)
- ディレクトリ
- 公開鍵証明書
- 失効リスト(CRL)
- 証明書有効検証機関(VA:Validation Authority)
- 証明書利用者またはエンドエンティティ(End Entity)またはSubscriber
- 証明書利用者または証明書検証者(Relying Party)

# PKI環境

一つの認証局とリポジトリを設置し、グリッド環境を利用するための認証に使用できる公開鍵証明書を配布する例。



# PKIモデル

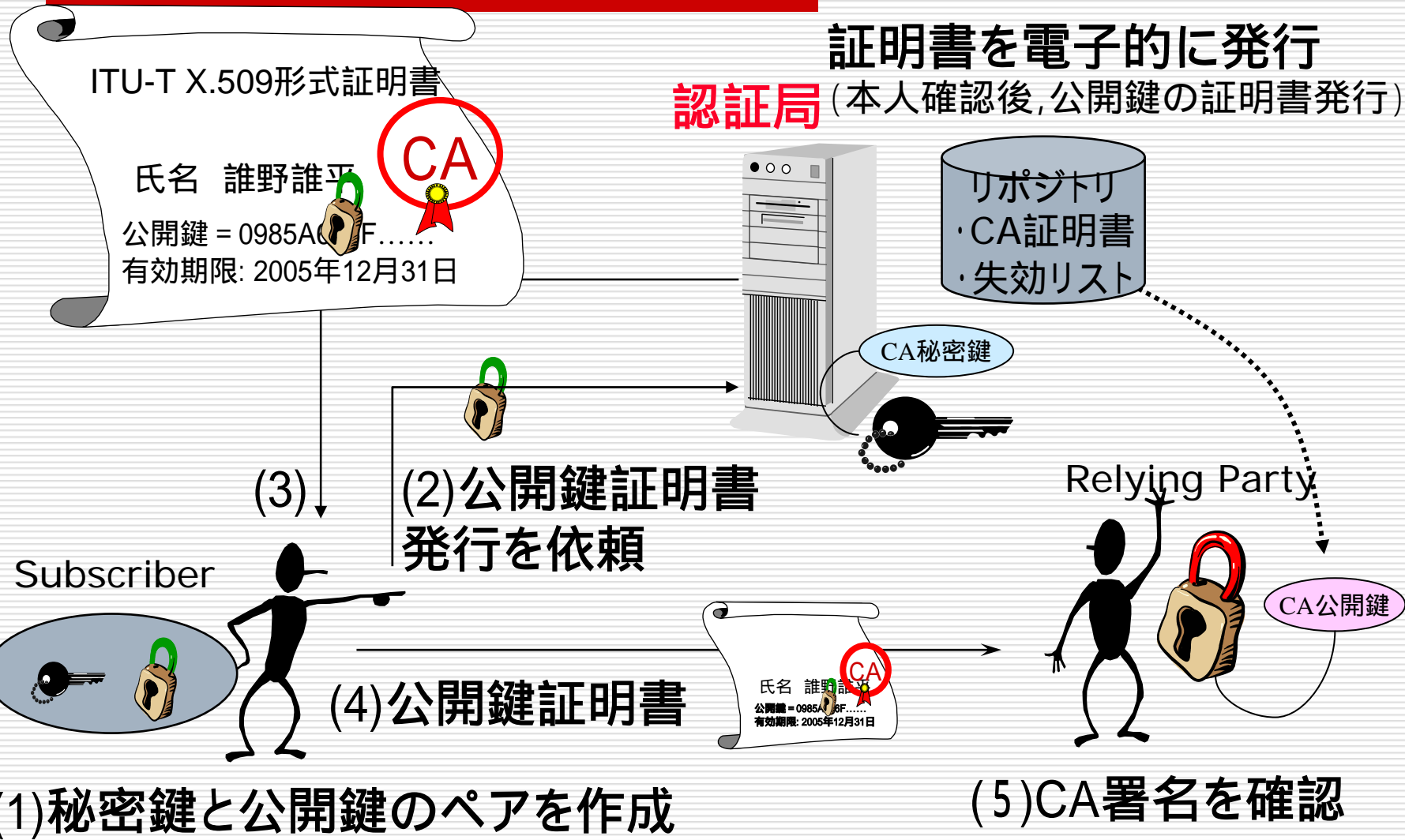


CA: Certification Authority  
RA: Registration Authority  
VA: Validation Authority  
PKI-AP: PKIアプリケーション  
CRL: Certificate Revocation List

# 認証局(CA)と公開鍵証明書の発行の流れ

## 証明書を電子的に発行

**認証局** (本人確認後, 公開鍵の証明書発行)



# PKI導入検討ステップ

---

- 証明書発行目的および対象を決定
  - 誰に何の目的で証明書を発行するか
- PKIアーキテクチャの策定
  - 相互認証モデル
- 鍵と証明書のライフサイクル
  - 鍵運用ライフサイクルに従った運用手順の策定
- CP/CPSの作成
  - 役割と組織
  - 物理セキュリティ
  - 運用および技術仕様を明文化

# 証明書発行目的および対象を決定

---

## □ 証明書発行目的

### ■ 利用者認証

- SSL/TLS (VPN, 無線LAN, Web認証など)
- Two-phase Strong Authentication

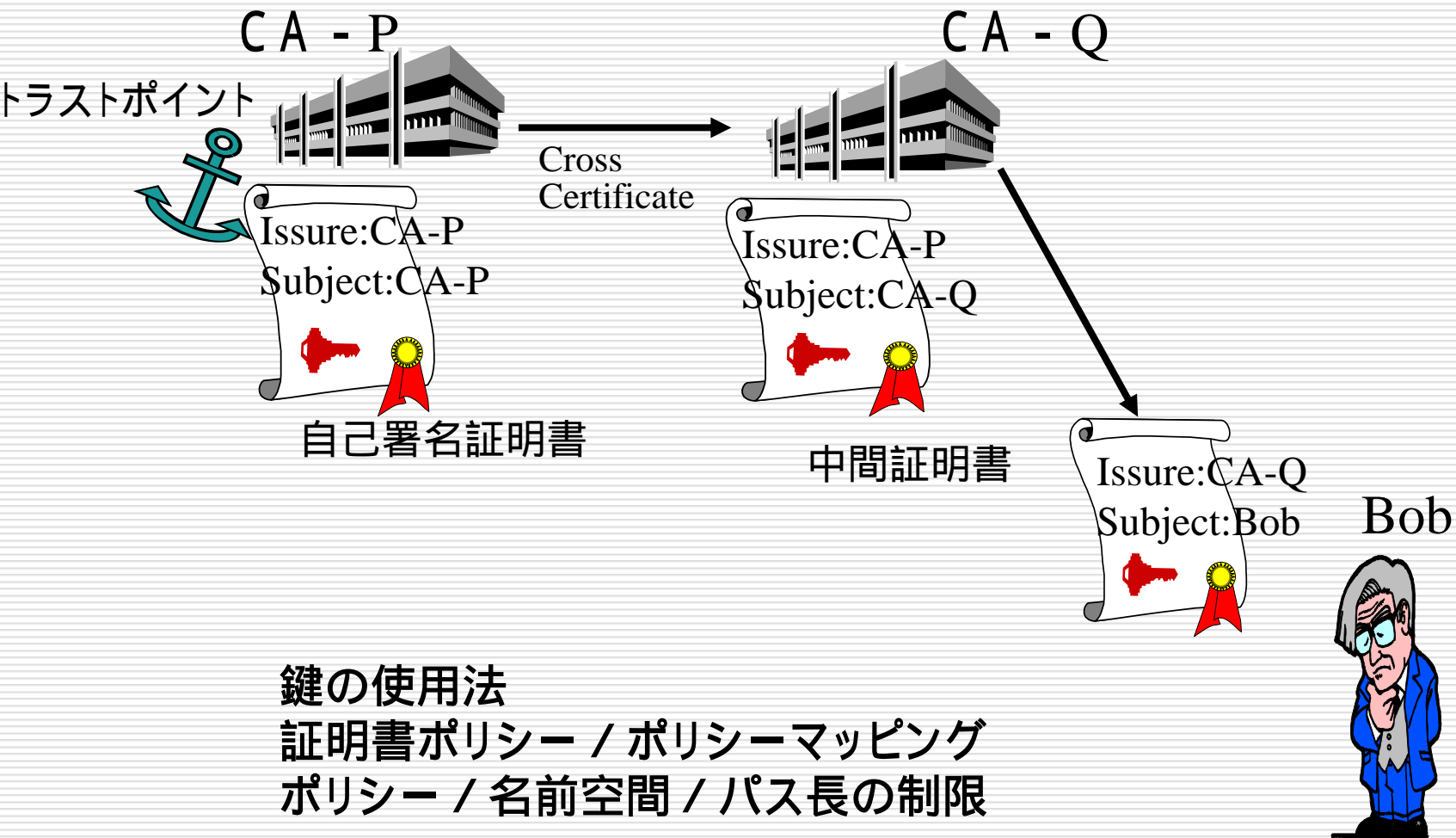
### ■ 電子署名

- 電子メール(S/MIME)、電子申請、電子契約書

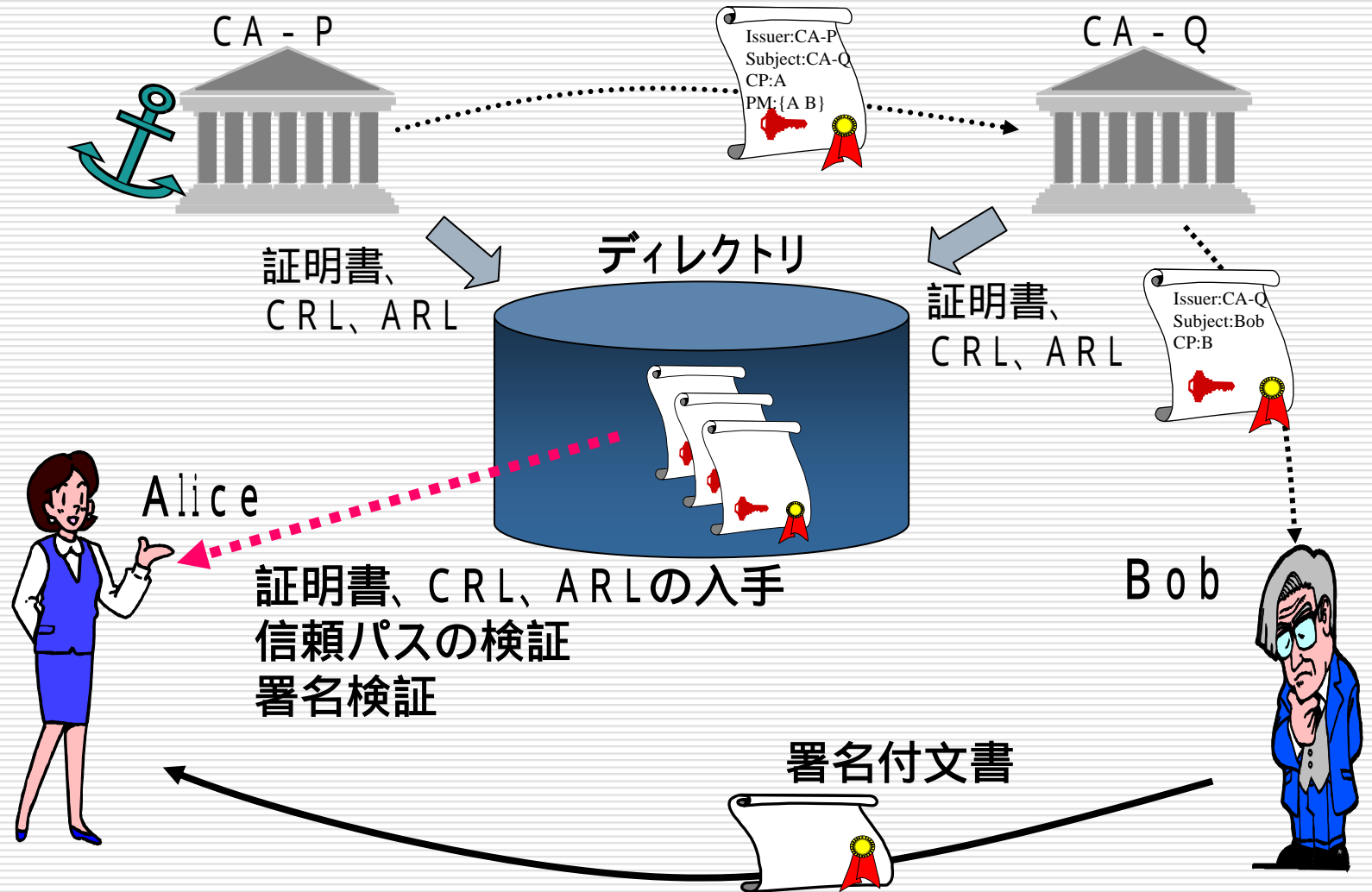
## □ 対象

- 組織を構成する特定の要員
- サーバやクライアント/システムや機器

# PKIアーキテクチャと信頼パス

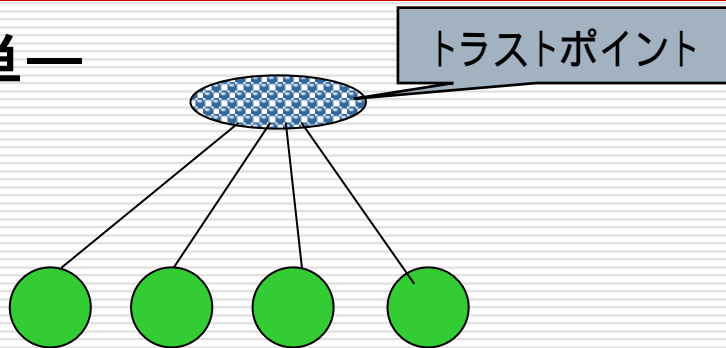


# 認証局を信頼した署名検証



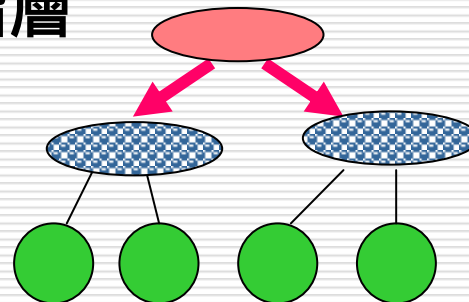
# PKIアーキテクチャ

A. 単一



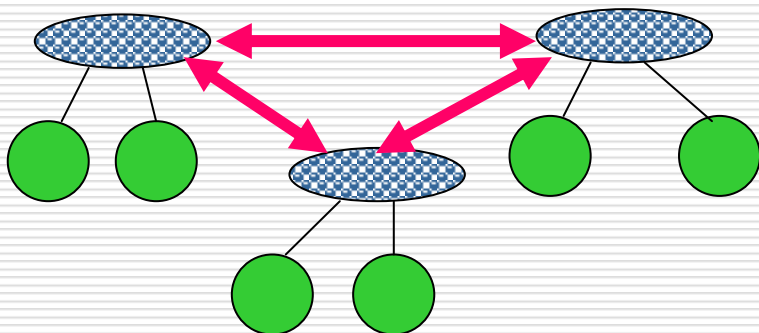
単一を複数もつマルチトラスト形態あり

B. 階層



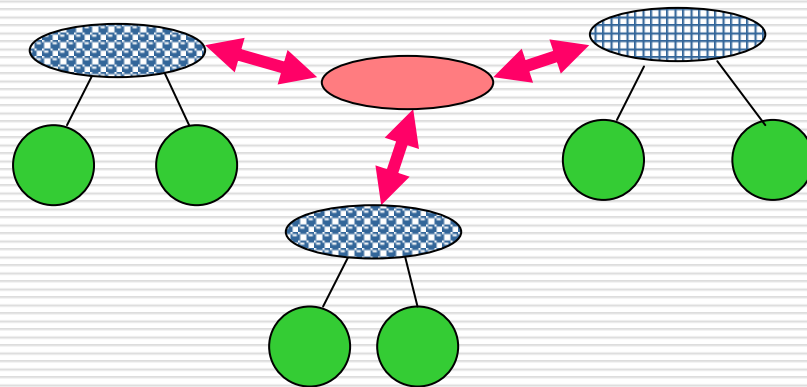
ルートが信頼性担保

C. メッシュ



各々が信頼性担保  
相互認証複雑

D. ブリッジ



各々が信頼性担保、第三者が仲介

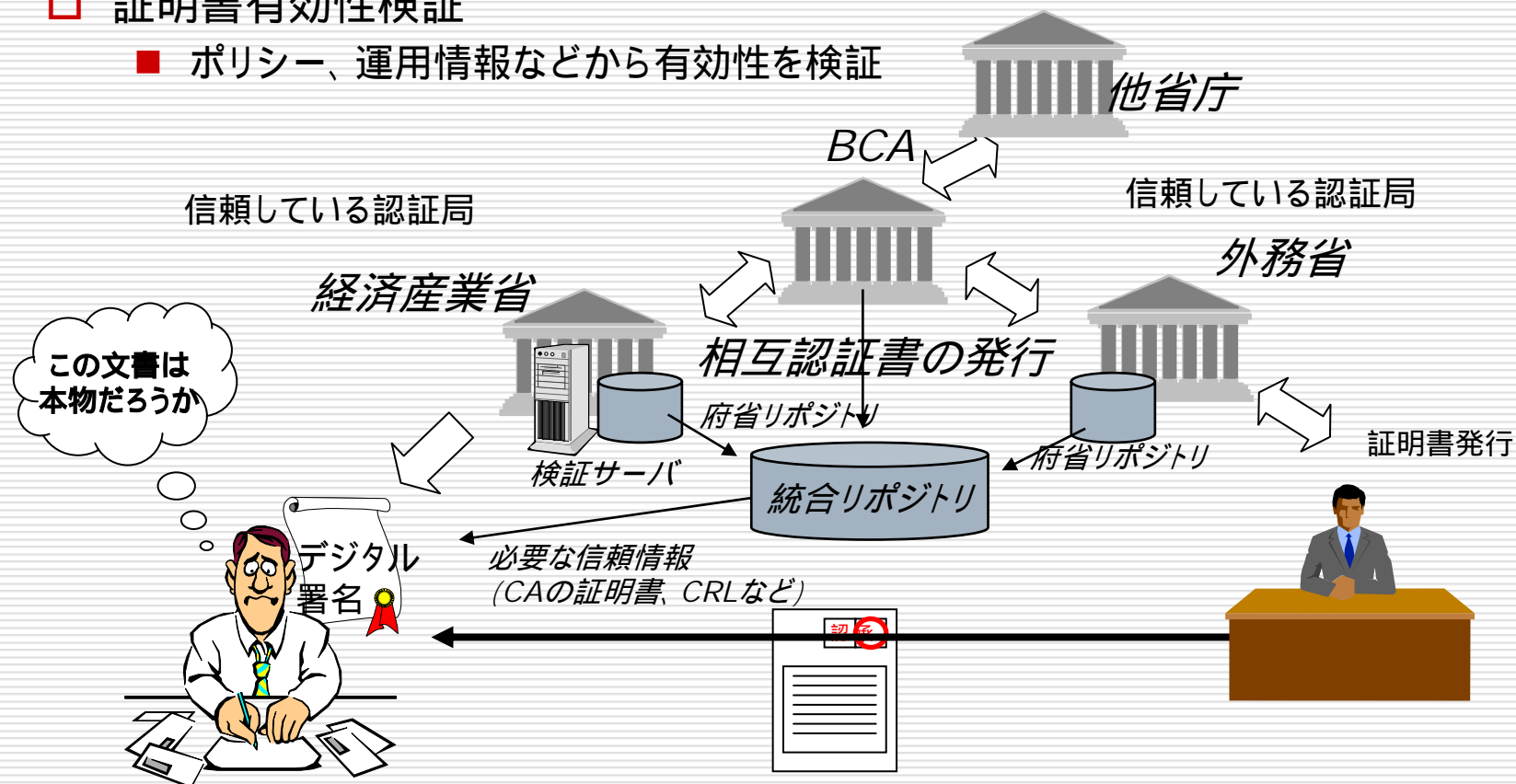
# 例:GPKI ブリッジCA

## □ 認証パス構築

- 利用者が信頼する認証局から相手の認証局までの信頼関係を探索すること

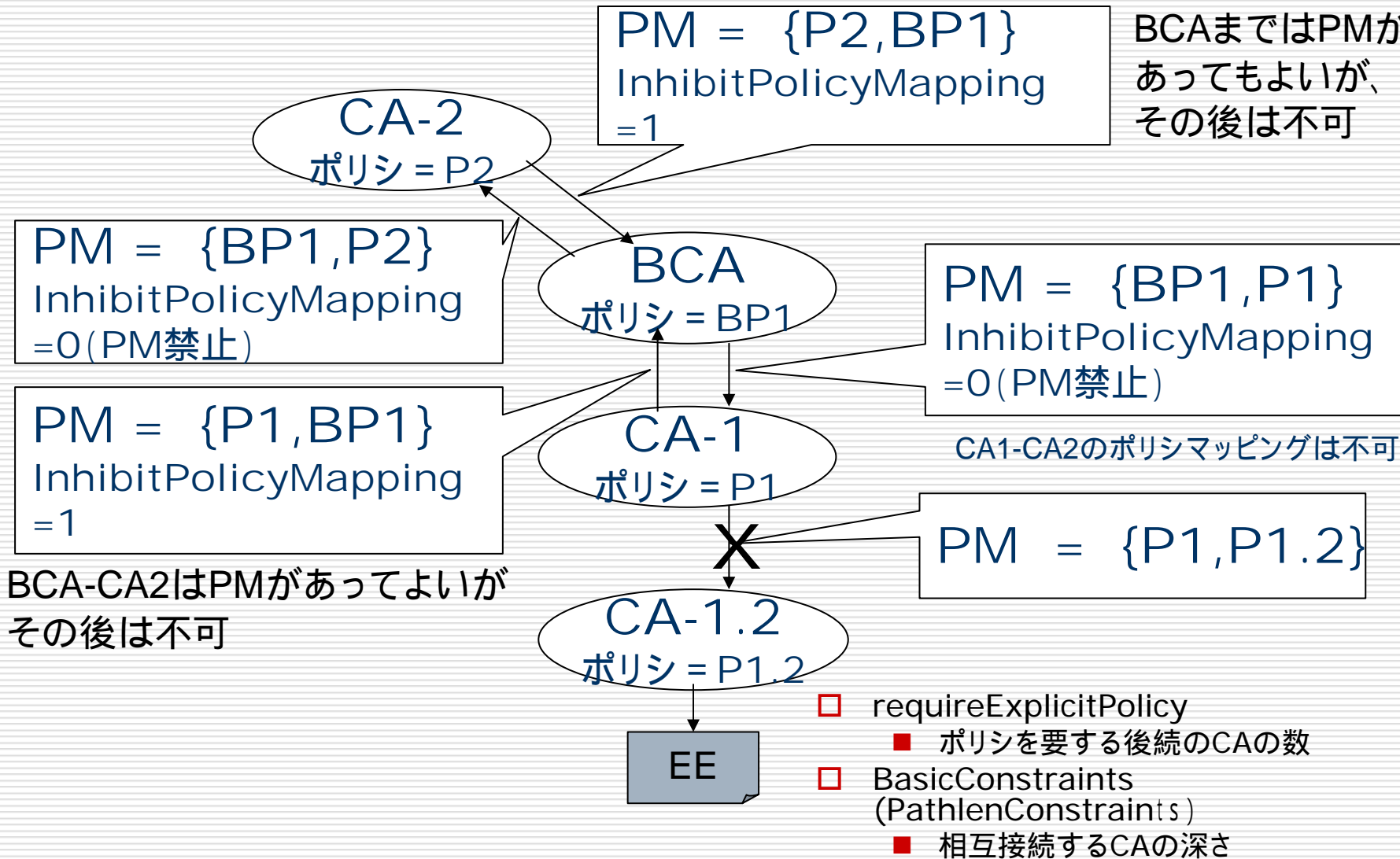
## □ 証明書有効性検証

- ポリシー、運用情報などから有効性を検証

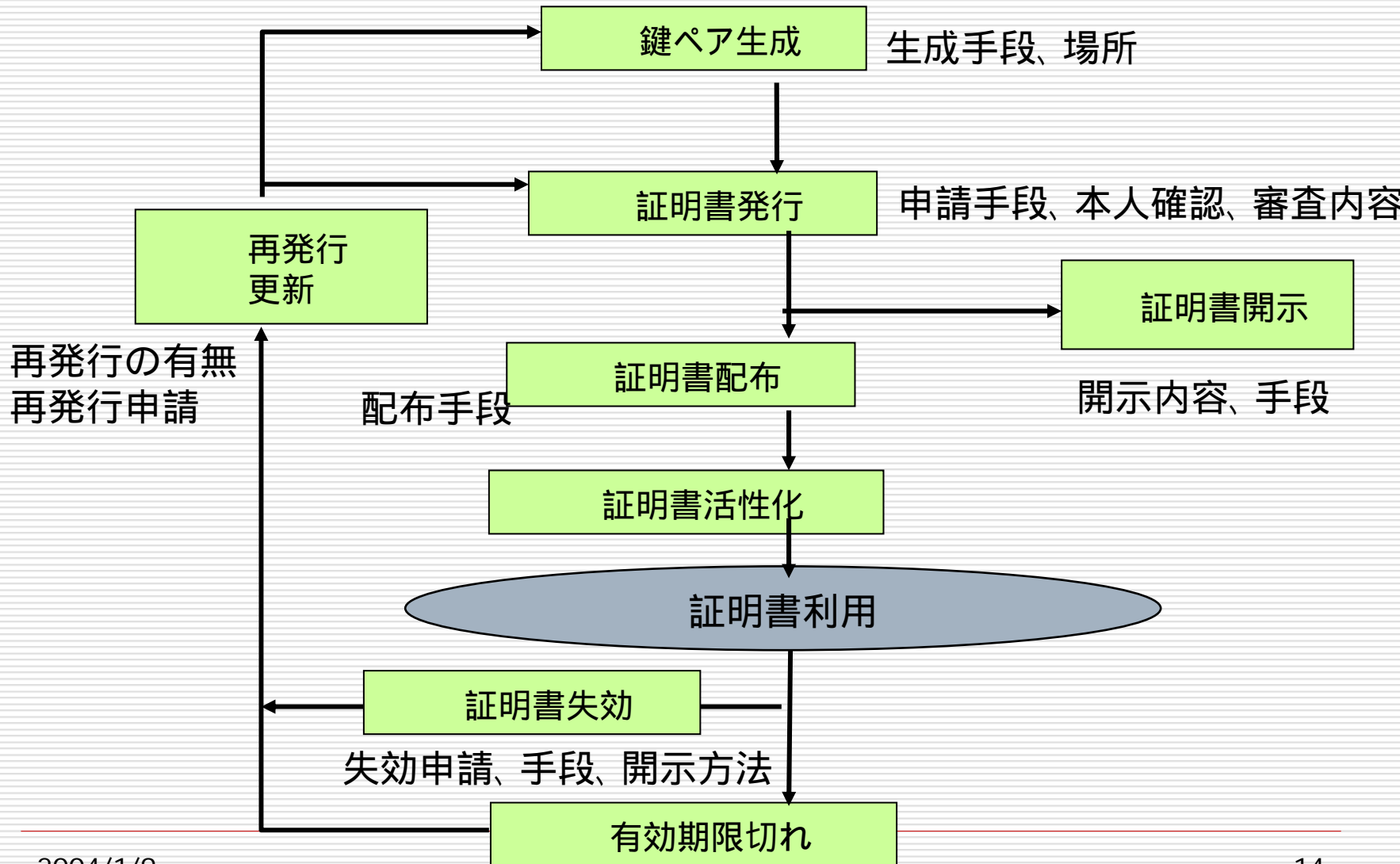


# CA信頼パス構築におけるポリシー制御の例

- Policy Mapping
  - 異なるポリシーを許容することを明示
- InhibitPolicyMapping
  - ポリシマッピングが許されなくなるまでの証明書数



# 鍵運用ライフサイクル



# 認証局運用のポイント

---

- 認証局
  - CA秘密鍵の管理
    - 秘密鍵漏洩を防ぐ(ハードウェアセキュリティモジュールの使用)
  - CA公開鍵の管理
    - CAなりすましをふせぐ
  - 申請時の本人確認
    - EEなりすまし
- エンドエンティティ
  - 秘密鍵の管理
    - EE秘密鍵漏洩をふせぐ
  - 認証局公開鍵(トラストポイント)の管理
- 共通
  - CA証明書の期限管理
  - EE証明書の期限管理

# 認証局運用のポイント

---

- 失効リスト(CRL)発行頻度、開示手段の決定
  - 例: 1週間に1度発行。OCSPレスポンスの設定、ディレクトリ(リポジトリ)上CRLの調査など
- 運用時間帯
  - 24H7D、必要に応じて保守時間を設けるなど。
- 物理的セキュリティ
  - CA秘密鍵を保護する観点での検討
- 要員教育
  - 服務規程およびセキュリティ教育が必要
- 証明書、CRLプロファイルを規定
  - 証明書に記載する項目についての詳細
    - 鍵用途、利用者の識別名、失効理由など

# 証明書ポリシーと認証局運用規程

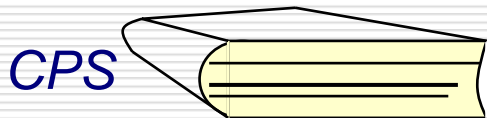
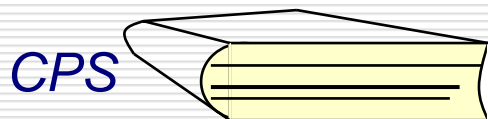
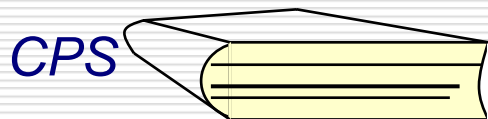
---

- RFC2527 Certificate Policy and Certification Practices Framework
  
- 証明書ポリシー (Certificate Policy)
  - セキュリティポリシー (ルール)
  - 証明書によって何を (What) するか
  
- 認証局運用規程 (Certification Practices Statement)
  - ポリシーを実行するための手続き
  - いか (How) ポリシーを実行するか？

# CPと CPS

## 認証局運用規定(CPS)

認証局が証明書発行において取るべき実施規定(HOW)



CPで規定された方針を、認証局運用に適用するための実施手順を記述する。認証局が、どのように特定のCPを実行するかについて記述した詳細な文書。

## 証明書ポリシー

特定のコミュニティ・グループやアプリケーションに対して共通のセキュリティ要件と証明書適用について記述したルール群(WHAT)

証明書ポリシー  
CP

- ・発行した証明書と、その証明書の状態情報を維持するためのセキュリティポリシーを記述する文書
- ・セキュリティポリシーは、証明書生成から、その満了または失効まで適用される。そのポリシーを適用する方法は指定しない

# CP/CPSで記述する内容

---

- 一般規定
  - CA、RAの義務、責務、連絡先、証明書の適用範囲
  - 料金、公開リポジトリ、準拠性監査、機密情報への方針、知的財産権
- 識別と認証
  - 証明書発行に先立つCA、RAにおける識別・認証手段
  - 鍵更新や失効要求の認証方法など
- 運用要件
  - 証明書発行、受け入れ、一時停止、失効、監査手順、記録の保管、危殆化など
- 技術的な要件
  - CA秘密鍵の生成、保護などの鍵管理
  - コンピュータセキュリティ管理、ライフサイクルセキュリティ管理、ネットワークセキュリティ、暗号モジュールの管理など

- 
- 物理的、手続き、個人のセキュリティ制御
    - CA局設置場所、物理アクセス、電力と空調、水害、防火、廃棄、バックアップ場所
    - 運用に関連する個人に関する規定。役割、背景、訓練、契約など
  - 証明書とCRLプロフィール
    - 発行証明書とCRLの内容に関する情報
  - CPSの管理
    - 仕様の変更手順
    - 開示と通知手順
    - CPS承認手順

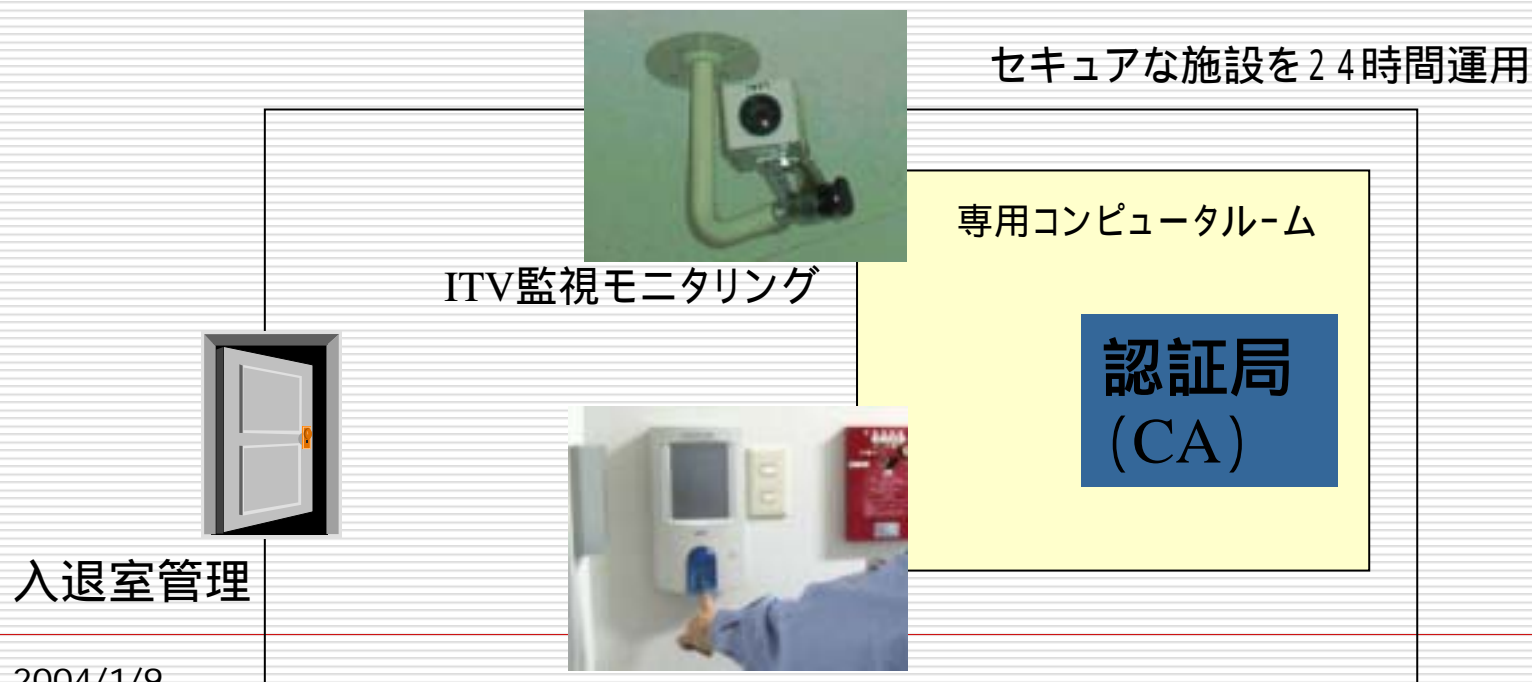
# 物理的セキュリティ (場所、建物の設備) の例

## 建物の構造や関連設備の適切な防災および安全対策 CA設置室の隔離と入退室、不正侵入監視の実施

建物: 耐火、耐震構造、電源 (2重化、無停電)、空調、入退室管理、侵入検知  
専用コンピュータールーム (他業務と分離)

: 入退室管理、不正侵入監視

生体認証、複数人操作、監視カメラ24H監視、モーションセンサ、耐火金庫など

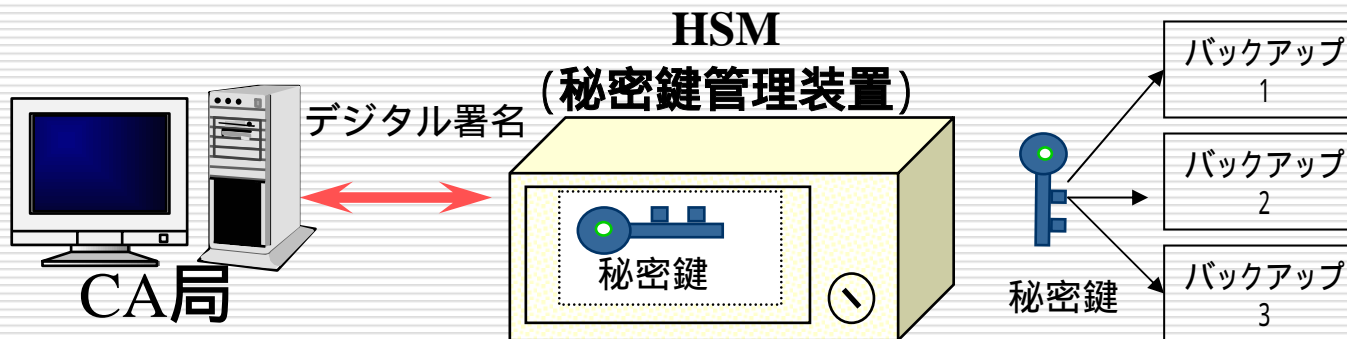


# 物理的セキュリティ (発行・登録業務の設備) の例

## ・CA秘密鍵管理

CA秘密鍵のセキュリティ確保手段  
HSM\*によるCA秘密鍵管理  
CA秘密鍵分割保管  
複数人制御  
鍵の定期更新 など

CAの秘密鍵が盗まれたら  
たいへん！  
証明書が偽造されて  
信頼基盤がくずれてしまう。



CK-Guard : 秘密鍵の漏洩を防ぐためのタンパフリー専用装置  
(内部の構造や情報を不正に読み出したり変更したり  
できないように保護された装置)  
2004/1/9

\*HSM: ハードウェアセキュリティモジュール

# グリッド環境へのPKI適用

---

- 識別と認証 (Identification & Authentication)
  - 本人識別と認証
  - 従来のアカウントとの関係
  - 課金との関係
  
- PKIドメインの定義とVOの対応づけ
  - 従来の固定的なPKIドメインのポリシーと柔軟なVOをいかに対応づけるか。