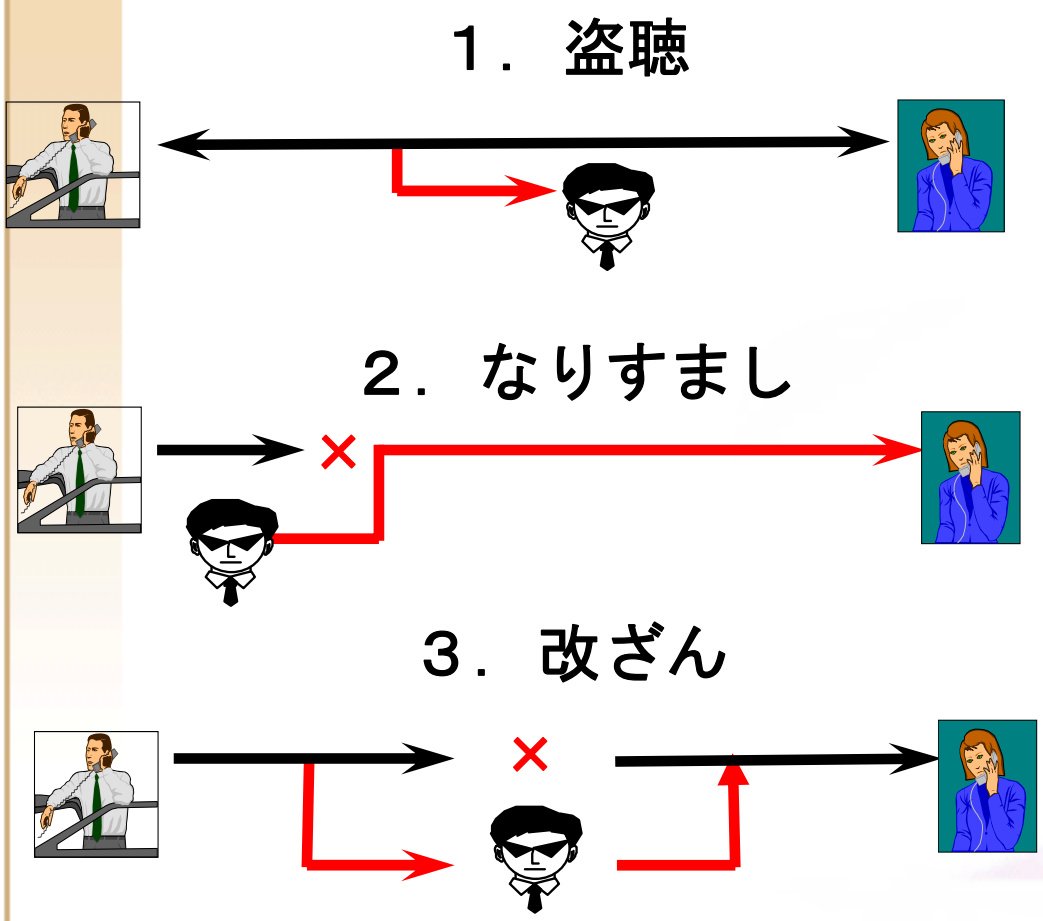
# 易しいPKI：
# なぜ安全なのか

国立情報学研究所
学術ネットワーク研究開発センター
谷本 茂明 tanimoto@nii.ac.jp
https://upki-portal.nii.ac.jp/

# Agenda

1. （Principle of PKI）なぜ安全なの？
   a. 公開鍵暗号
   b. 暗号化と署名
2. （Knowledge of PKI）どう実現しているの？
   a. 主な構成要素：証明書、認証局、リポジトリ
   b. 運用ポリシー：CP/CPS
3. （Interoperability of PKI）どう使うの？
   a. メール（S/MIME）、Web（SSL）
   b. UPKI

# ■インターネット上の主な脅威と対処例




## PKI

暗号化
（公開鍵暗号、共通鍵暗号）

認証
（公開鍵暗号、共通鍵暗号）

ディジタル署名
（公開鍵暗号、ハッシュ関数）

# Agenda

1. （Principle of PKI）なぜ安全なの？
   a. 公開鍵暗号
   b. 暗号化と署名

（Knowledge of PKI）どう実現しているの？

認証局、証明書

CP/CPS

（Interoperability of PKI）どう使うの？

メール（S/MIME）、Web（SSL）

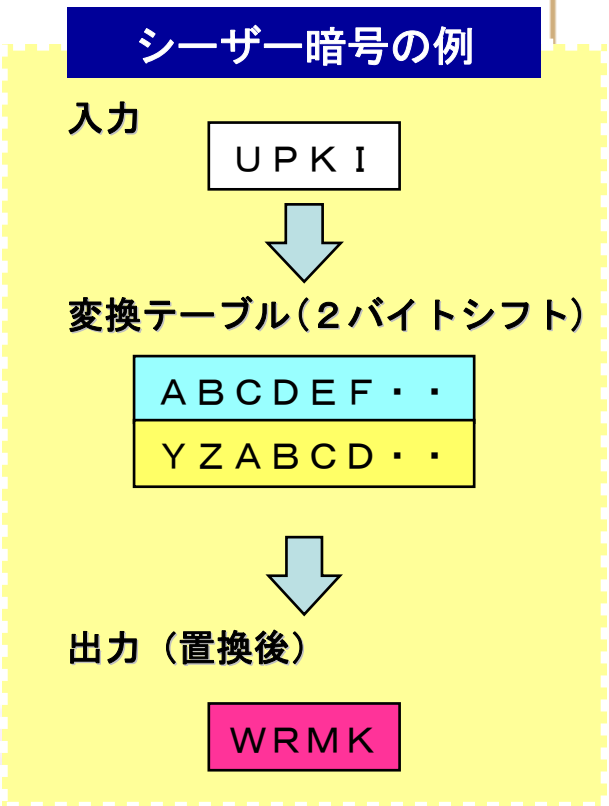
UPKI

# ■ 暗号とは？

●互いに秘密の知識を共有して、他人には分からない方法で情報交換を行うこと

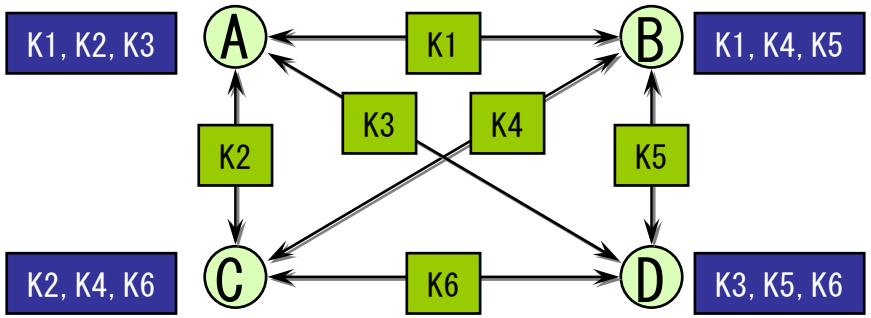
●古典暗号（代表例：ｼｰｻﾞｰ暗号）
- ➢鍵とアルゴリズムの概念未分化
- ➢アルゴリズム：秘密
  - ➢ 暗号利用が広まるとアルゴリズム数が爆発
- ➢置換え空間：小（例：ｱﾙﾌｧﾍﾞｯﾄ26文字）

●現代暗号
- ➢鍵とアルゴリズムを分化
- ➢アルゴリズム：公開
- ➢鍵：秘密（共通鍵暗号）
- ➢置換え空間：大



# ■現代暗号の進化
## ～クローズド環境からオープン環境へ～

- クローズド環境
  - 共通鍵ｋの数
    - ◆通信相手数だけ管理必要

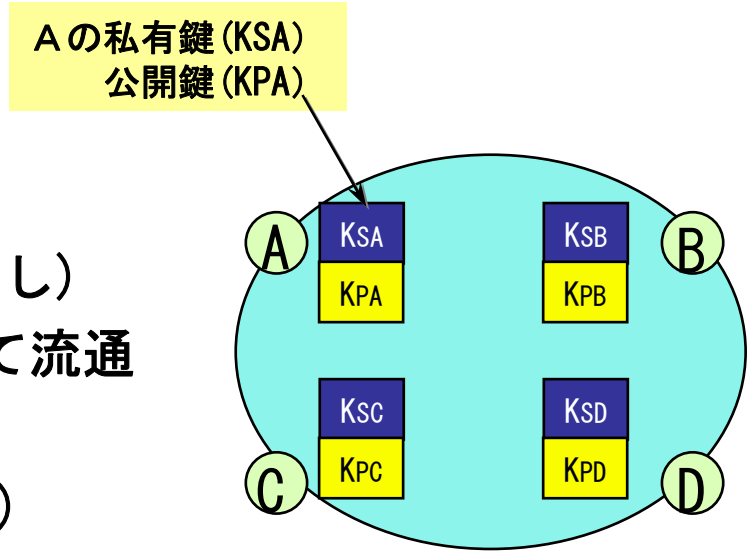



- オープン環境（インターネット）

➡ 鍵の数が爆発

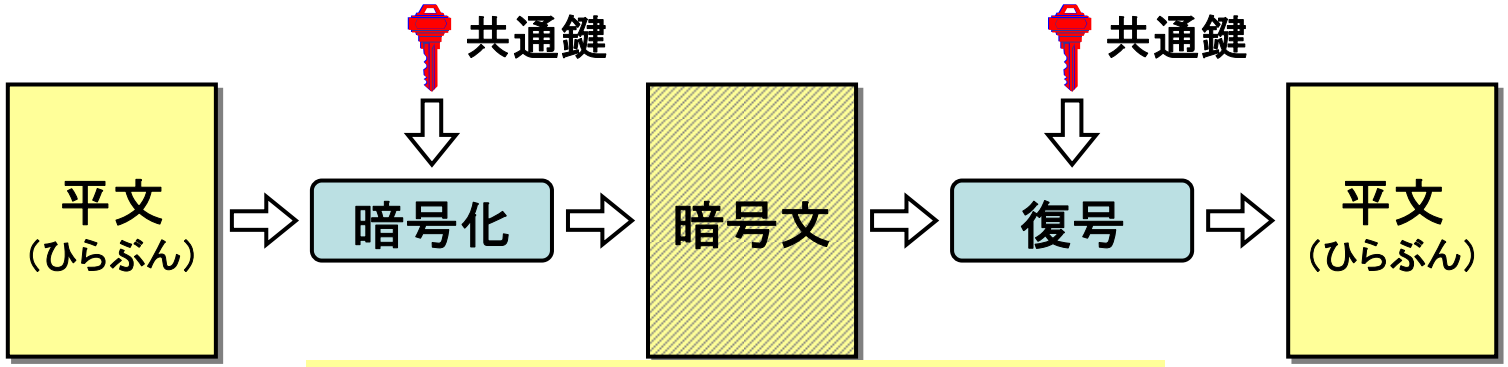
⇩ 鍵を公開

◆ 公開鍵暗号
  - 私有鍵のみ秘密（鍵の数の爆発なし）
  - 公開鍵はネットワーク等によって流通
  - 鍵の空間を拡大
    （公開鍵から私有鍵の推定を防止）



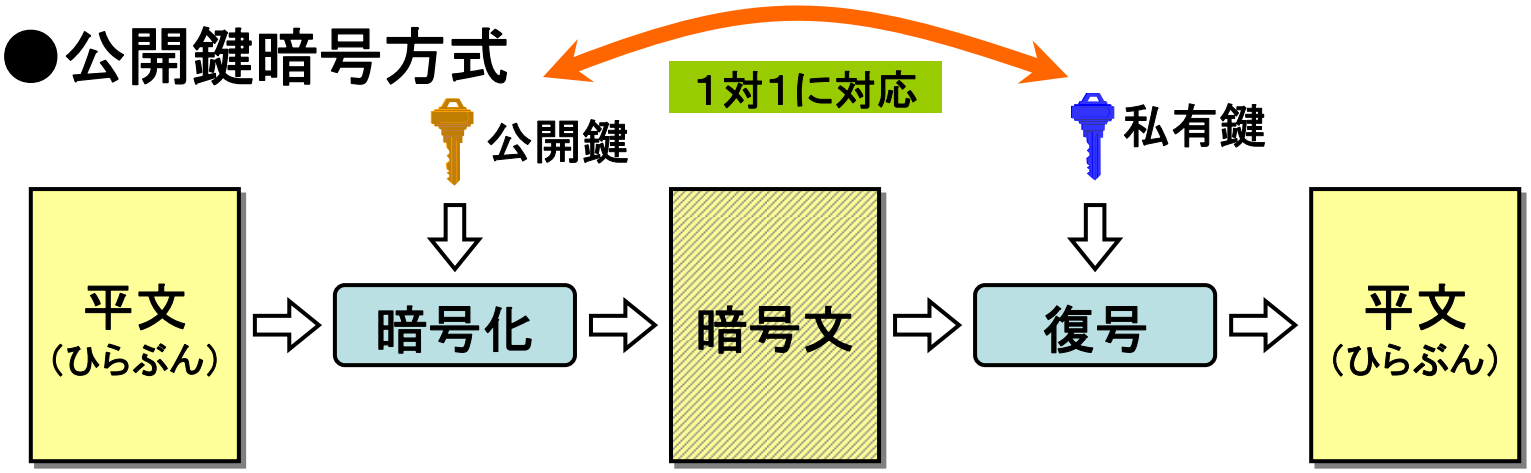
# ■共通鍵暗号方式と公開鍵暗号方式

## ●共通鍵暗号方式




→暗号化と復号の鍵が同一

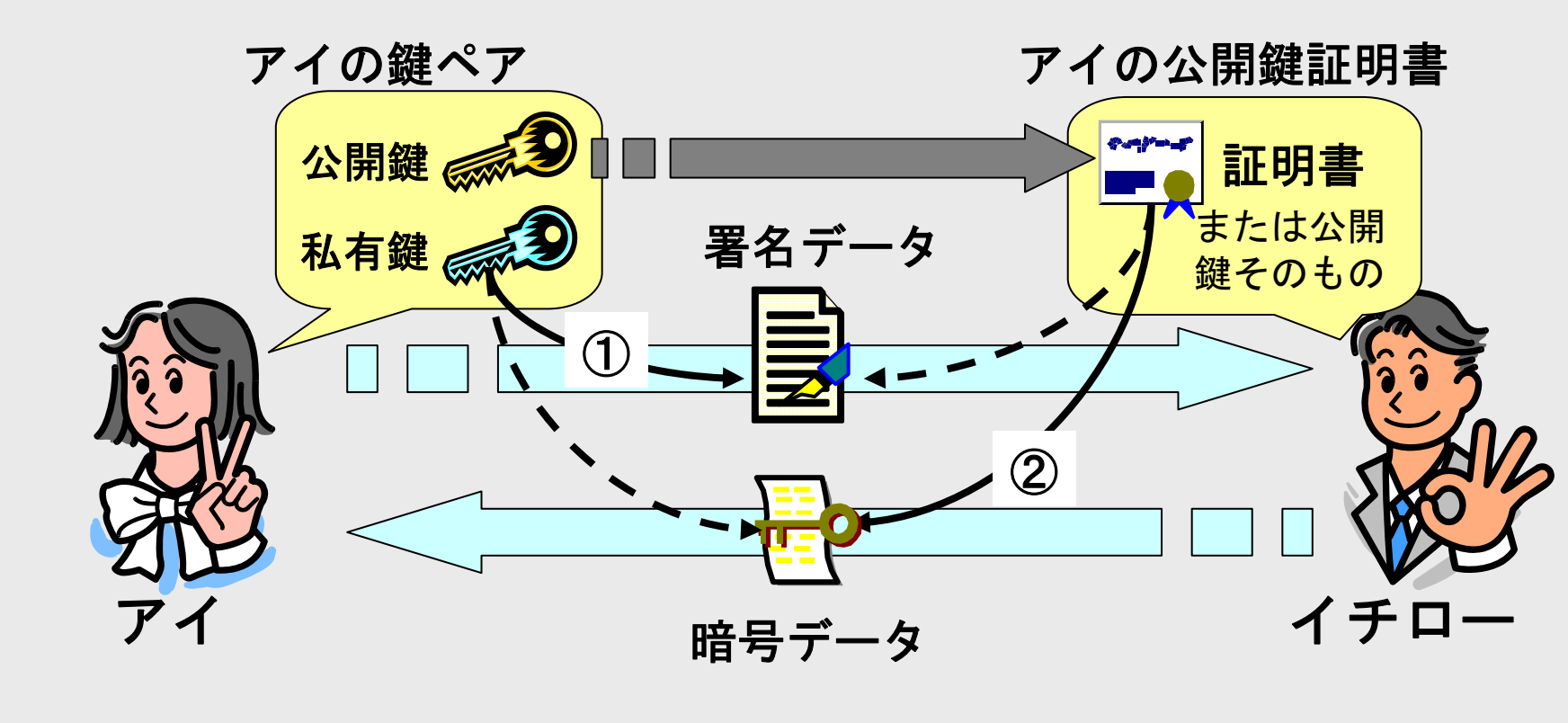
## ●公開鍵暗号方式




→暗号化と復号の鍵が異なる

# ■　暗号化と署名

- 以下の仕組みを利用して署名/暗号を実現
  ① 署　名：私有鍵でエンコード→公開鍵でデコード
  ② 暗号化：公開鍵でエンコード→私有鍵でのみデコード



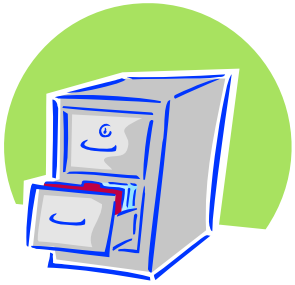
# Agenda

1. （Principle of PKI）なぜ安全なの？
   a. 公開鍵暗号
   b. 暗号、署名
2. （Knowledge of PKI）どう実現しているの？
   a. 主な構成要素：証明書、認証局、リポジトリ
   b. 運用ポリシー：CP/CPS
3. （Interoperability of PKI）どう使うの？
   a. メール（S/MIME）、Web（SSL）
   b. UPKI

# ■　PKIの主な構成要素：証明書、認証局、リポジトリ

**証明書**：鍵ペアの所持者であることを保証した情報。X.509 標準に準拠する公開鍵証明書

**認証局**：証明書を発行する認証機関を指す。認証局（CA ）はユーザの身元と鍵ペアの所有を確認し、その公開鍵証明書を発行



**リポジトリ**：証明書や、証明書の状態に関する情報（失効情報等）等を利用者（リライングパーティ）への情報提供

# ■PKIの主な構成要素：加入者、利用者

加入者（サブスクライバ）：

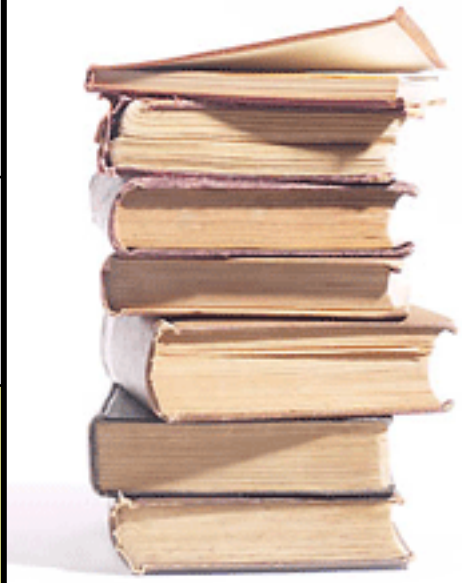
- 認証局から証明書を発行されたエンティティ
- 証明書に記載された公開鍵に紐づけられた秘密鍵を持つ。

利用者（リライングパーティ）：

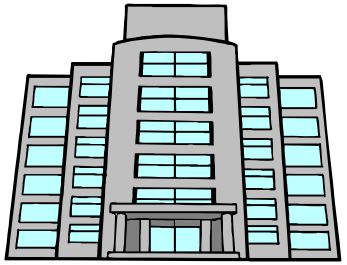
- サブスクライバの証明書を検証するエンティティ

# ■公開鍵証明書
## X.509証明書フォーマット

| | |
|---|---|
| **基本領域** | バージョン番号(v3)<br>シリアル番号<br>署名アルゴリズム<br>**発行者識別名**<br>有効期間<br>**主体者識別名**<br>主体者公開鍵情報 |
| **拡張領域** | 拡張名(OID)<br>タイプ、値 |
| **CAの署名** | |



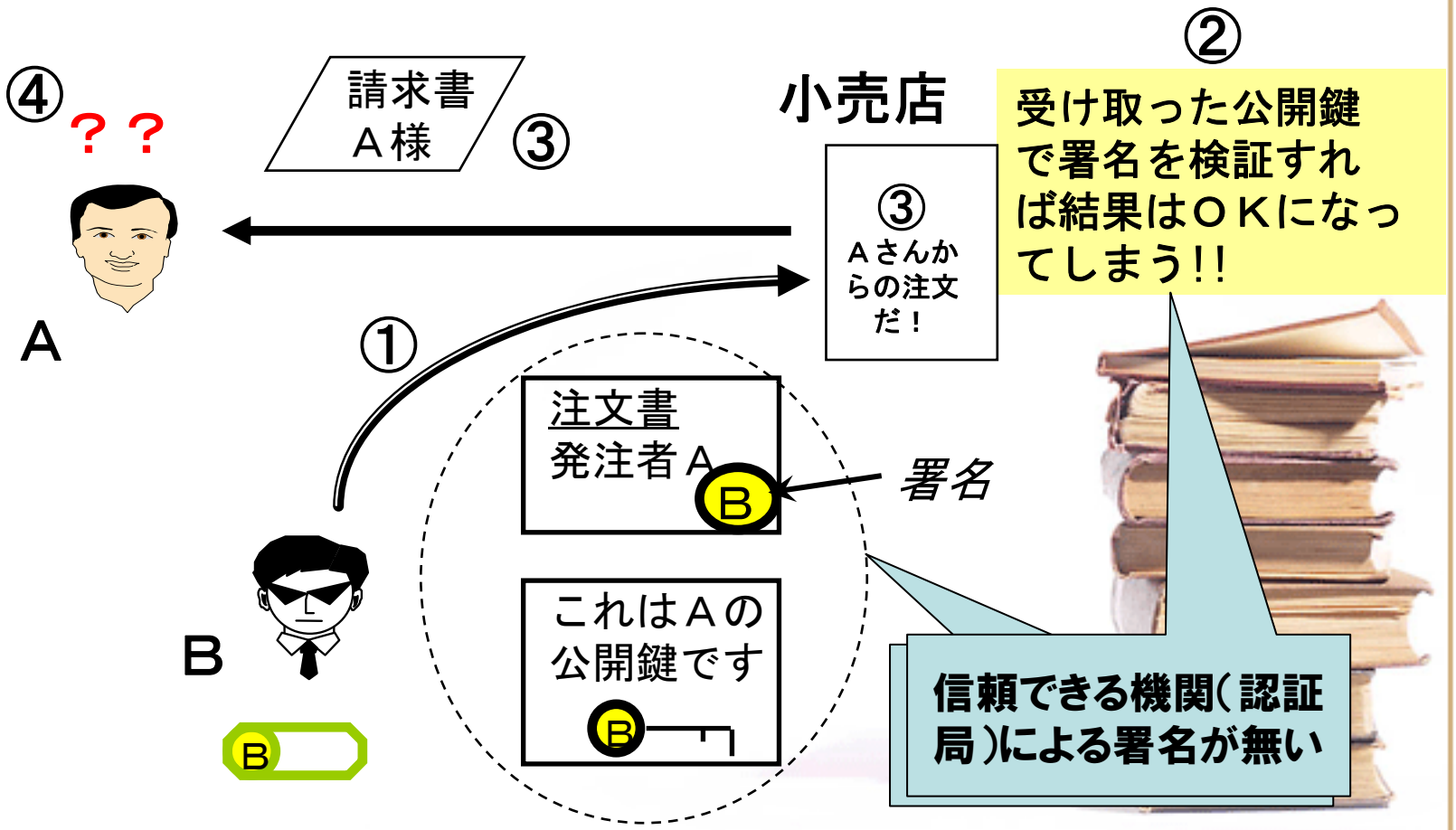
# ■認証局(CA: Certification Authority)



- 基本機能：
  - 公開鍵暗号利用時に、その公開鍵が確かに加入者（サブスクライバ）本人のものであることを証明するための「公開鍵証明書」を発行／管理する
  - 要求に応じて証明書を配布する
  - 証明書の失効リスト（CRL）を管理する

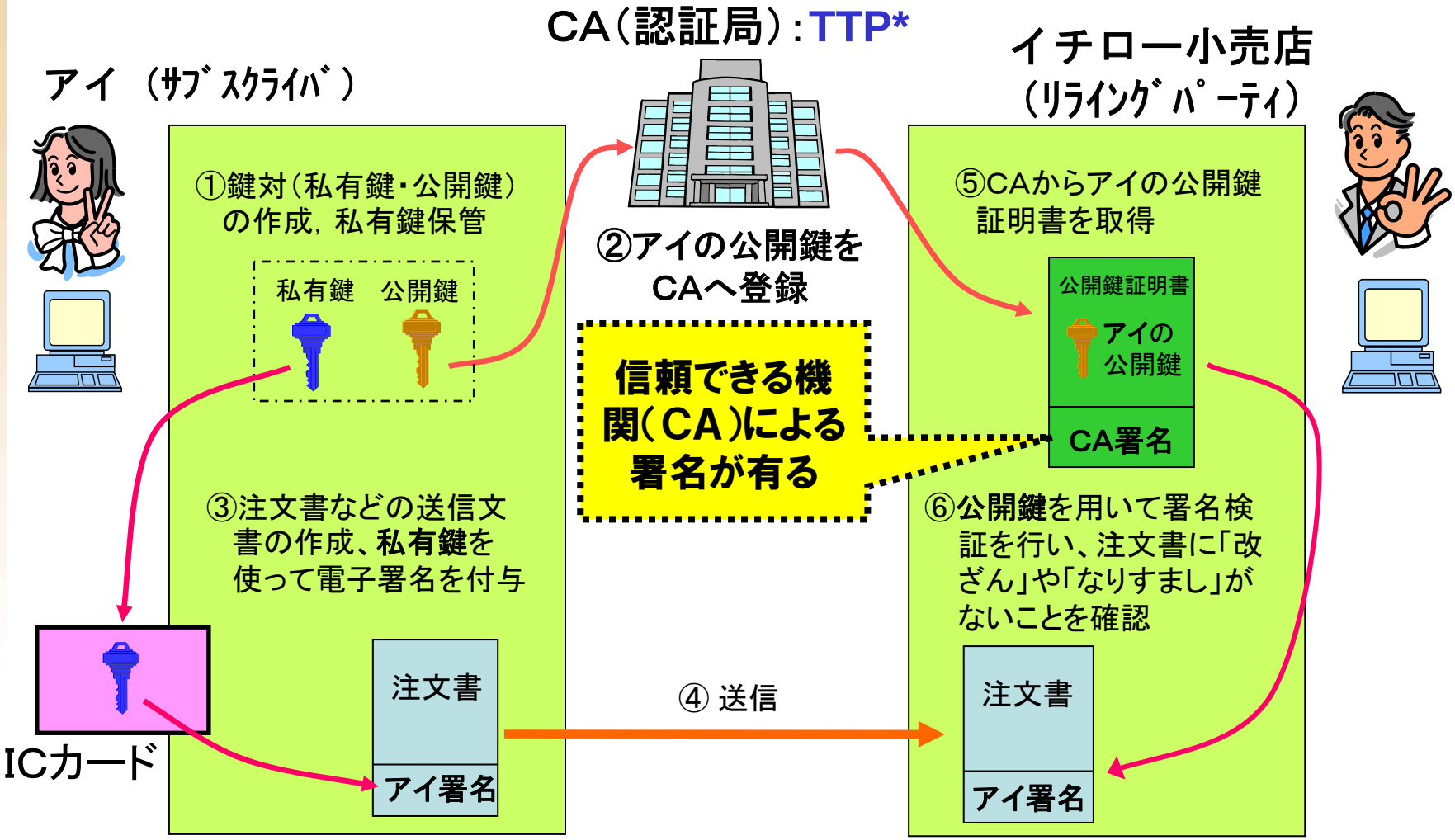
# ■認証局の必要性

## ●なりすましの脅威（認証局が無い場合）

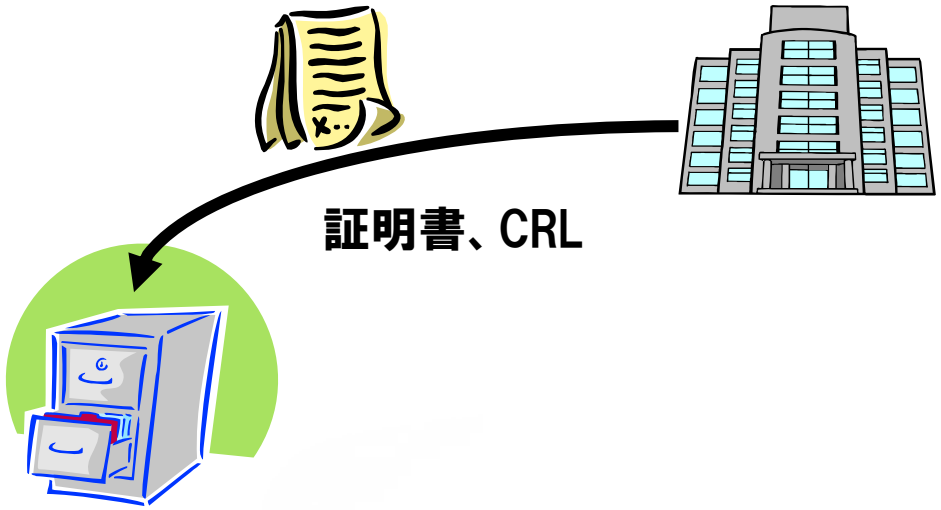


＊：信頼できる第三者機関（TTP： Trusted Third Party）

# ●認証局が有る場合



# ■リポジトリ




## ●リポジトリ

◆証明書および CRL を格納し公開

- CA が発行した証明書や CRL を格納、利用者（リライングパーティ）が検索して取得出来るようにする。

※CRL（失効リスト）：私有鍵の紛失・盗難や証明書記載内容の変更に伴う再発行などの際に発行される

# ■ 運用ポリシー：CP/CPS

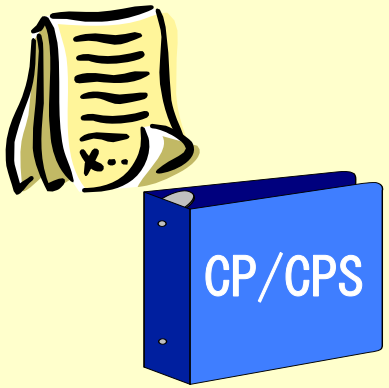
- CP：証明書ポリシー
  - 証明書を発行する際の基準。**身元確認方法や鍵ペアの生成方法、想定するアプリケーションなどを記述**したもの。一般的には、証明書を発行する認証局毎に定義して用いる。
- CPS：認証局運用規定
  - CPの要件を満たすために、**認証局がどのような運用を行うかを規程**したものがCPS

**CP : Certificate Policy**
**CPS: Certification Practice Statement**

# ■CP/CPSの主な内容

●RFC3647（CP/CPSのフレームワークを規定）での主な内容は、下記のとおり。

(1)　概要
(2)　公開とリポジトリの責任
(3)　本人性確認と認証
(4)　証明書のライフサイクル
(5)　設備、管理、運用上の統制
(6)　技術的セキュリティ管理
(7)　証明書、失効リスト、OCSPのプロファイル
(8)　準拠性監査とその他の評価
(9)　他の業務上の問題及び法的問題
(10)　証明書、ARL/CRLプロファイル例



（参考）

# UPKI共通仕様*でのCP/CPSガイドライン記述例

*:https://upki-portal.nii.ac.jp/upkispecific/specific

4.1.1　概要

【解説】

本節では認証局の名前、サービス名、大枠のサービス内容、相互認証を行う等の宣言を行い、認証局の概要について記す。また、相互認証の方式についても簡単に定義しておくことが望ましい。

【記述例】

1　はじめに

〇〇電子認証局は、〇〇大学により運営され、〇〇大学内及び大学間のサービスにおける電子認証のために必要となる電子証明書（以下、「証明書」という）を発行する。

本文書において、「〇〇 電子認証局（以下、「本認証局」という）」の権利または義務は国立大学法人たる〇〇大学 に帰属することを意味する。

本認証局は、大学間のサービスを共有するために相互認証接続を行う 。

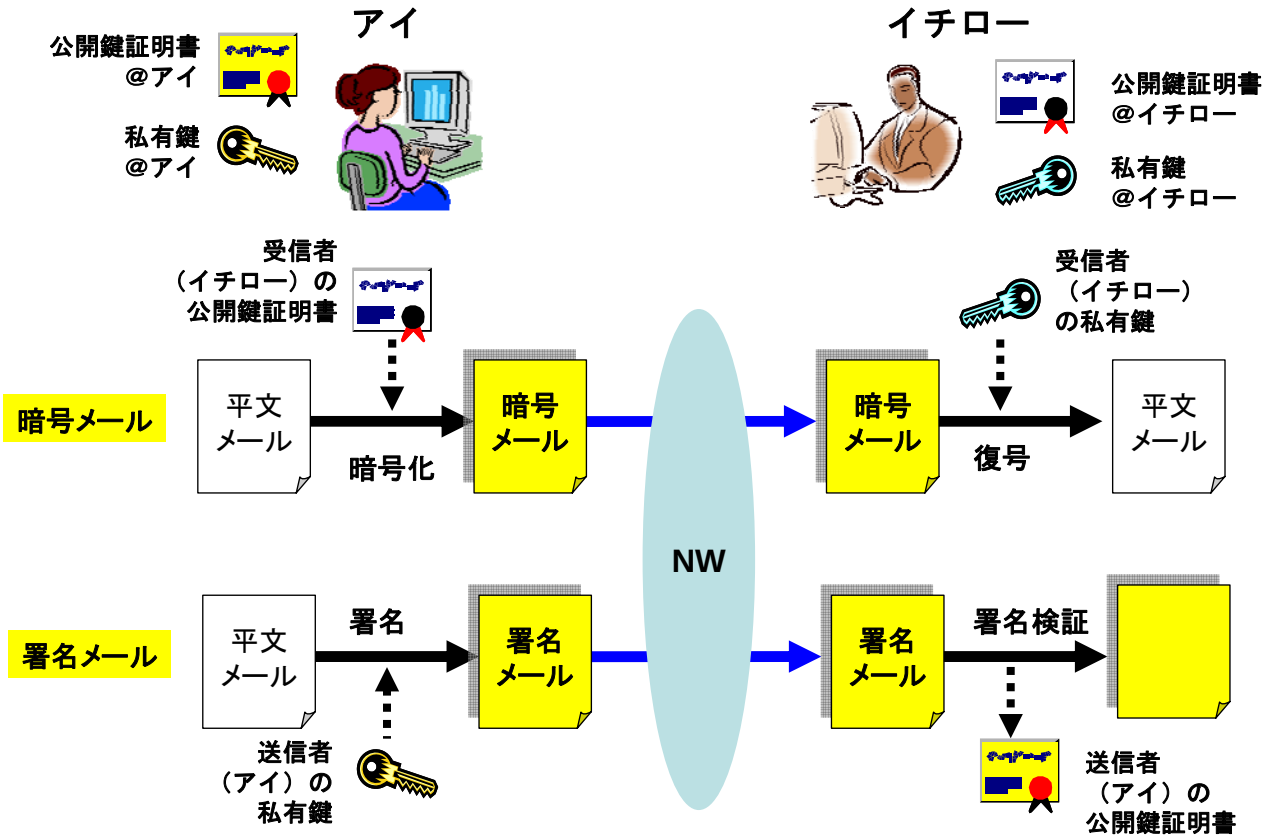
上記のように、ガイドラインの各章において、それぞれ解説と記述例を示し、 理解し易いようにしている。

# Agenda

1. （Principle of PKI）なぜ安全なの？
   a. 公開鍵暗号
   b. 暗号化と署名
2. （Knowledge of PKI）どう実現しているの？
   a. 主な構成要素：認証局、登録局、リポジトリ
   b. 運用ポリシー：CP/CPS
3. （Interoperability of PKI）どう使うの？
   a. メール（S/MIME）、Web（SSL）
   b. UPKI

# ■ メール（S/MIME）

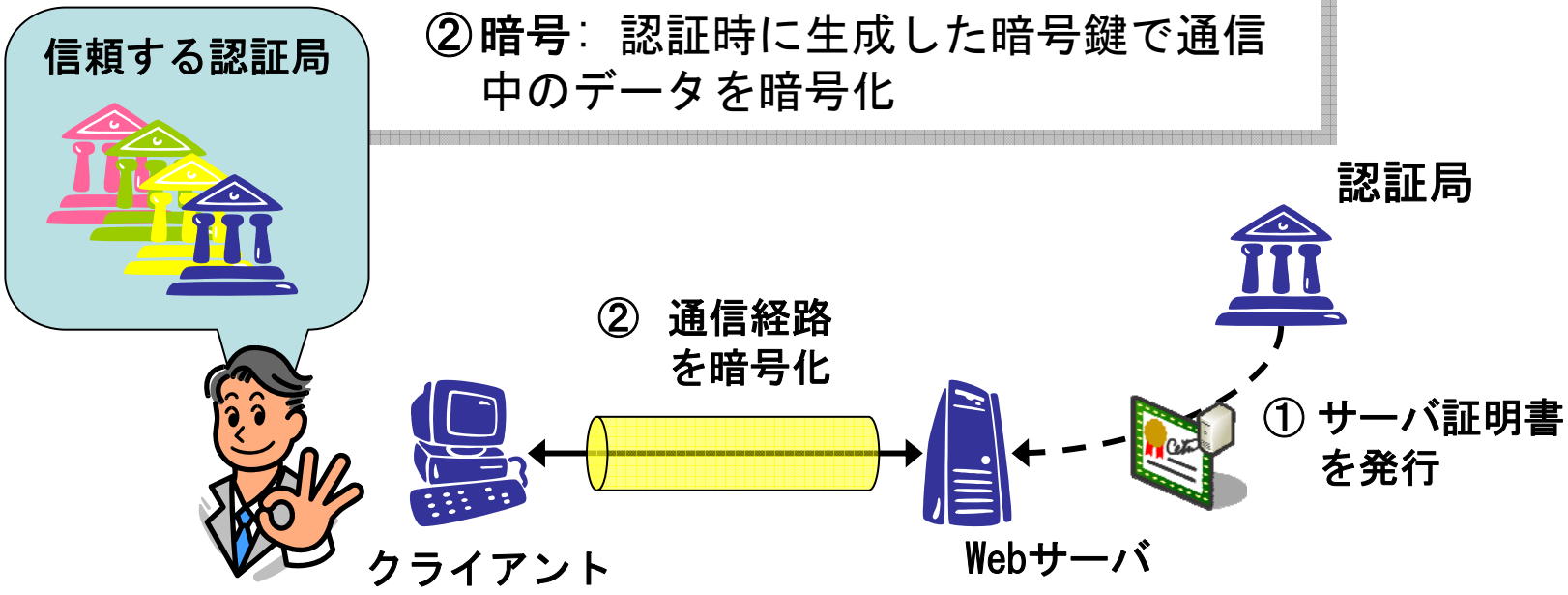
- S/MIME（Secure/MIME）は、証明書を利用して電子メールに暗号化とデジタル署名のセキュリティを提供（基本は、スライド８：暗号化と署名）




参考：http://www.ipa.go.jp/security/pki/072.html#_Toc3020828

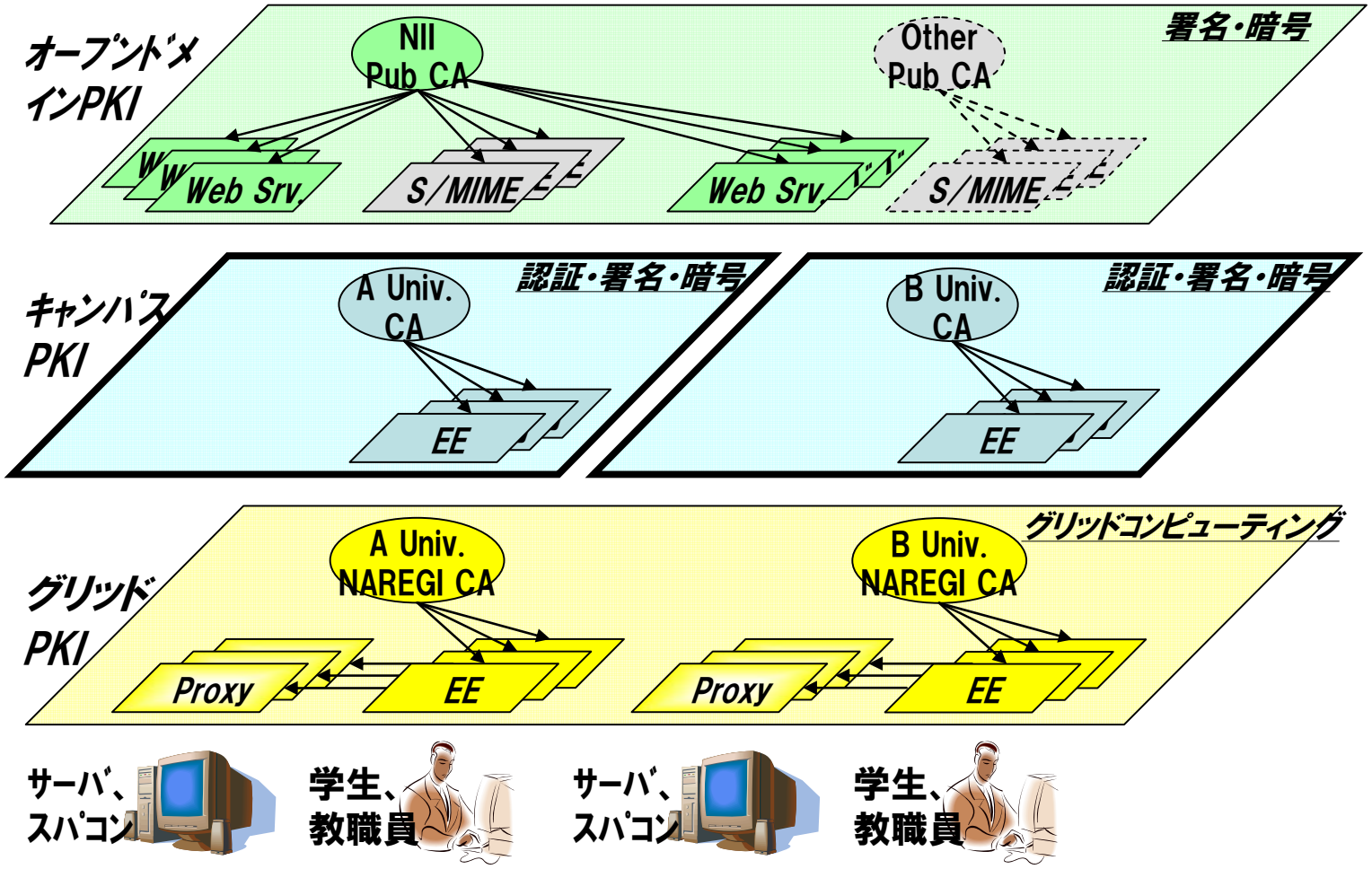
# ■ Web（SSL）

- **サーバ認証（クライアント認証）**：
  サーバ（クライアント）の真正性を確認し、通信経路を暗号化する技術
  - ①**認証**：**信頼する認証局**から発行された証明書を使って確認
  - ②**暗号**：認証時に生成した暗号鍵で通信中のデータを暗号化




サーバ認証の場合

# ■ UPKI（３層構成）


オープンドメインPKI
NII Pub CA
Other Pub CA
署名・暗号
Web Srv.
S/MIME
Web Srv.
S/MIME
キャンパスPKI
A Univ. CA
認証・署名・暗号
EE
B Univ. CA
認証・署名・暗号
EE
グリッドPKI
A Univ. NAREGI CA
B Univ. NAREGI CA
グリッドコンピューティング
Proxy
EE
Proxy
EE
サーバ、スパコン
学生、教職員
サーバ、スパコン
学生、教職員

# ■ 各層の位置づけ

| | オープンドメインPKI | キャンパスPKI | グリッドPKI |
|---|---|---|---|
| 適用領域 | インターネット | 各大学内 | グリッドコンピューティングの運用機関 |
| 目的 | インターネット上での認証、署名・暗号など | 学内NW・システムへの安全なアクセス | GSI (Grid Security Infrastructure)の構築 |
| 用途 | 主にSSL/TLS認証、その他S/MIME署名・暗号など | Web SSO、VPN、無線LAN（802.1X）、申請・署名アプリ（身分証明書、事務ペーパレス化等） | 利用者証明書、サーバ証明書の発行など |
| 証明書発行対象 | サーバ、自然人など | 教職員、学生、学内サーバなど | 利用者、サーバなど |
| 利用者（リライングパーティ） | 不特定多数？ | 主に学内関係者 | グリッド環境利用者 |
| 認証局の運用 | オープンドメイン認証事業者など | アウトソース 、インソース | GOC (Grid Operation Center) |

# ■ まとめ

1. (Principle of PKI)なぜ安全なの？
   - 基本:公開鍵暗号
   - 暗号化と署名
2. (Knowledge of PKI)どう実現しているの？
   - 主な構成要素:証明書、認証局、リポジトリ
   - 運用ポリシー:CP/CPS
3. (Interoperability of PKI)どう使うの？
   - 応用例:メール(S/MIME)、Web(SSL)
   - UPKIの概要

# 「易しいPKI：なぜ安全なのか」ご静聴、ありがとうございました

*To be continued・・・*

- 身近なPKI：サーバ証明書の重要性
- これからのPKI：さまざまな大学内サービスの認証・認可の統合

・CSIシンポジウム(一橋記念講堂)：全国大学共同電子認証基盤（UPKI）の構築