# Shibbolethを支える認証基盤技術

平成21年度情報処理軽井沢セミナー
2009/09/01
国立情報学研究所　西村健

# Shibbolethが正しく動作するために大事なこと

- IdPは大学構成員の個人情報を扱っている！
- SPは自分たちのサービスが（も）大事！
  - 個人情報を漏えいしたら大変……
  - なりすましで赤の他人に利用されたら大変……

もっと言うと

- 通信を盗聴されないために……
- IdPが相手のSPを正しく認識するために
- SPが相手のIdPを正しく認識するために

# この講義で出てくるキーワード

- 認証　電子署名　暗号化　認証局　PKI
- Webブラウザに表示される鍵マーク?

# 内容

- 認証って何？
- PKIという枠組
  - インターネットの安全性の基礎の基礎
  - インターネットを使う時、理解しているのといないのとでは大きく違う
  - リテラシーとして
    - なかなか理解してもらえない…

# 電子証明書（認証）

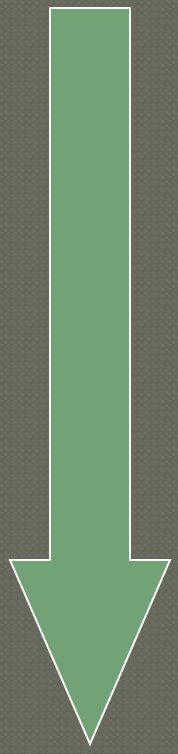
# ID（アイディー）ってなに？

- **Identification**　識別子（アイデンティティ？**identity**）
  ‖
- **identify**するためのもの
  ⇊
- システムが操作者／対象を識別するためのもの
  - ○○にだけ許される操作、××だけが閲覧できる情報…

# 現実社会では…

- 免許証、保険証、印鑑証明
  - 有印文書の「印」
- ○○病院の診察券、TSUTAYAの会員証
- 「法人」
- …

# IDにはレベルがある



確からしさ
UP

- 完全自己申告
- IPアドレス（もしくはそれに類するもの）
- 任意のメールアドレスとの紐付け
- 「生きている」メールアドレスとの紐付け
- 学内システムで使っているアカウント
- ？？？
- ？？？

# 世の中にあふれる詐欺

インターネットは現実世界の縮図である

- 他人を騙る
  - 振り込め詐欺
- 他人のIDによる不正アクセス
  - 不正アクセス禁止法
    - 他人のID利用の禁止
    - 他人のコンピュータへの侵入禁止
    - 他人のパスワード等の無断提供禁止
    - アクセス管理者による防御措置（責務）
  - オンラインバンキング、電子商取引
  - オンラインゲーム

# 認証の分類

- 本人だけが知っていること
  - パスワード等
  - 漏洩・解読（辞書攻撃）の問題
- 本人だけが持っているもの
  - クレジットカード、セキュリティトークン等
- 本人の身体的特徴
  - 指紋、指静脈、虹彩等

# いろいろな認証

- マトリクス認証
- ワンタイムパスワード
- 生体認証
- 電子証明書

# 電子証明書の対象(ID)はさまざま

- サーバ証明書
- クライアント証明書
- 無線LANの機器認証

- 住基カード（公的個人認証サービス）

# IDの評価基準

- 電子証明書は、正しく運用管理すれば現在の技術では最強の認証強度を持つと言われている
  - どういった内容を？
  - 誰に？
  - どの程度？
  - どういった手段で確認する？

# 技術の話 「公開鍵暗号」

# 暗号に必要なこと（１／２）

用語

- 元の文：平文
- 平文を別の形に変えること：暗号化
- 別の形：暗号文
- 暗号文を平文に戻すこと：復号

# 暗号に必要なこと（２／２）

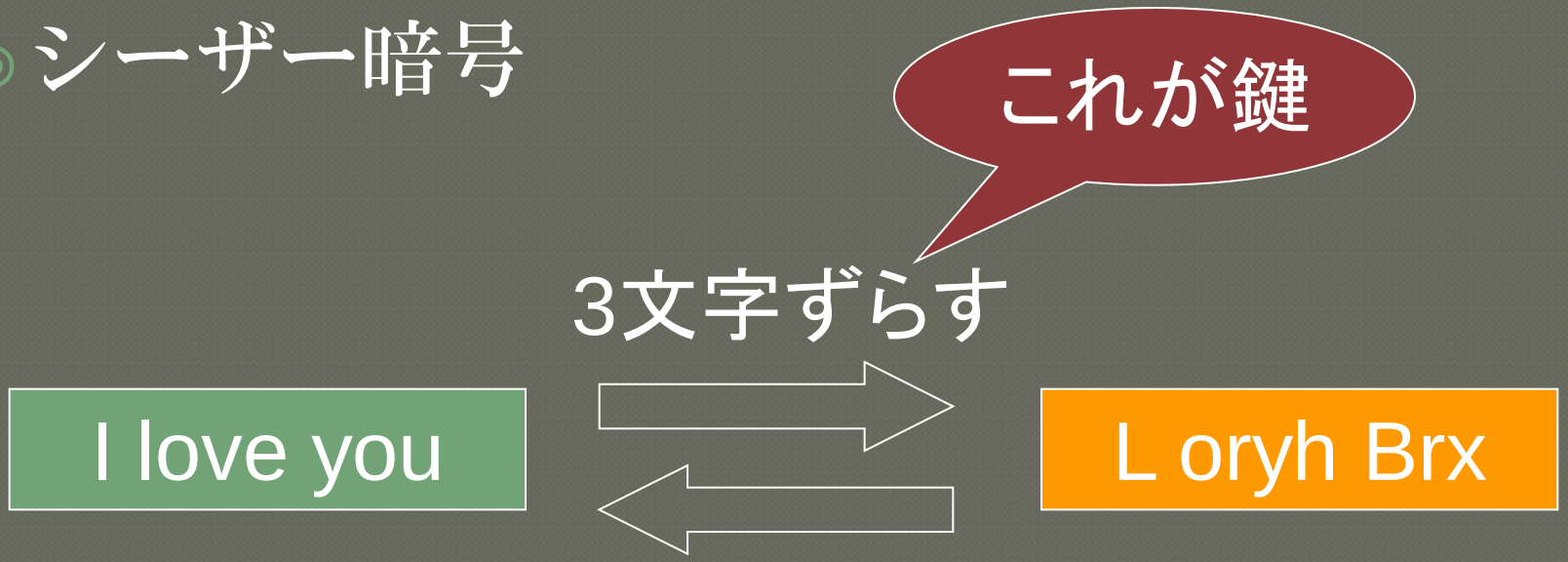
- 相手（例：Webサーバ）のみが復号できること
  - つまり、第三者が暗号文から平文を推定すること（解読）が困難であること

インターネット上のやりとりの場合は特に

- 暗号化／復号アルゴリズムが公開されていること
- アルゴリズムは公開してその他の秘密情報を二者で共有するという方法が一般的
  - 秘密情報のことを「鍵」という

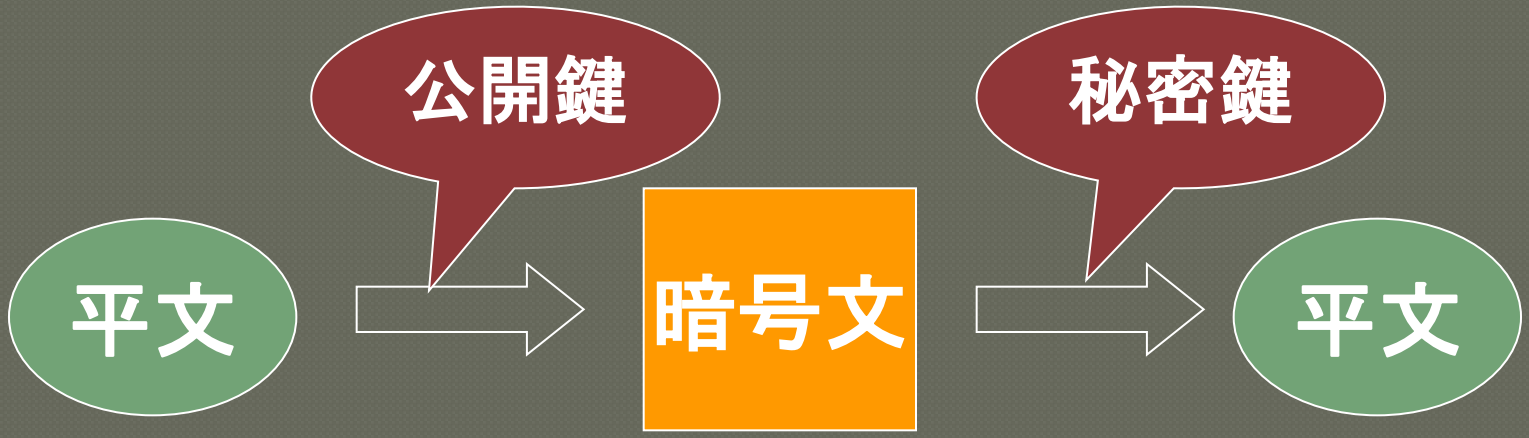
# 簡単な暗号

- シーザー暗号



# 公開鍵暗号

- 2種類の鍵（鍵ペア）を使用する



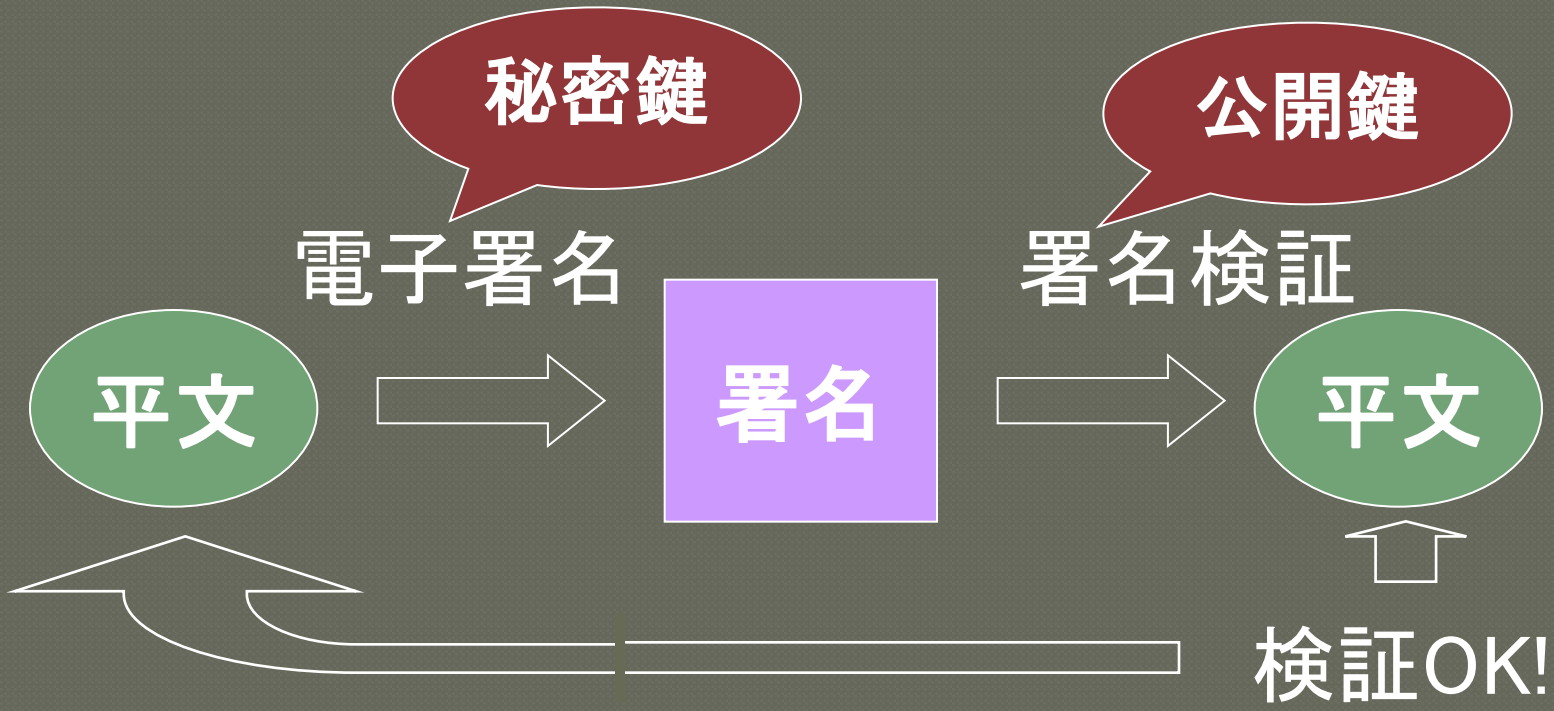

- 公開鍵で暗号化された暗号文は対応する秘密鍵でしか復号できない
- 公開鍵を公開しておいて、暗号化に利用してもらう

# RSAアルゴリズムの詳細

- 素数p, qに対して
  - 適当なe
  - 計算されたd　　$(de \equiv 1 \pmod{(p-1)(q-1)})$
  - 公開鍵：N=p×q および e
  - 秘密鍵：d および N
- 平文Mに対して
  - 暗号化：　　$C = M^e \pmod{N}$
  - 復号：　　$M = C^d \pmod{N}$

# 電子署名

- データが途中で改竄されていないことを確認するための方法。公開鍵暗号技術が使われる。



# 電子証明書

- 公開鍵証明書、デジタル証明書とも
- 認証対象が所有する秘密鍵に対応する公開鍵に対して、その「名前」を対応付けるもの

# 証明書の詳細説明は後述

- 誰が署名するの？
  → PKIが関連してくる

# Shibbolethでの利用例

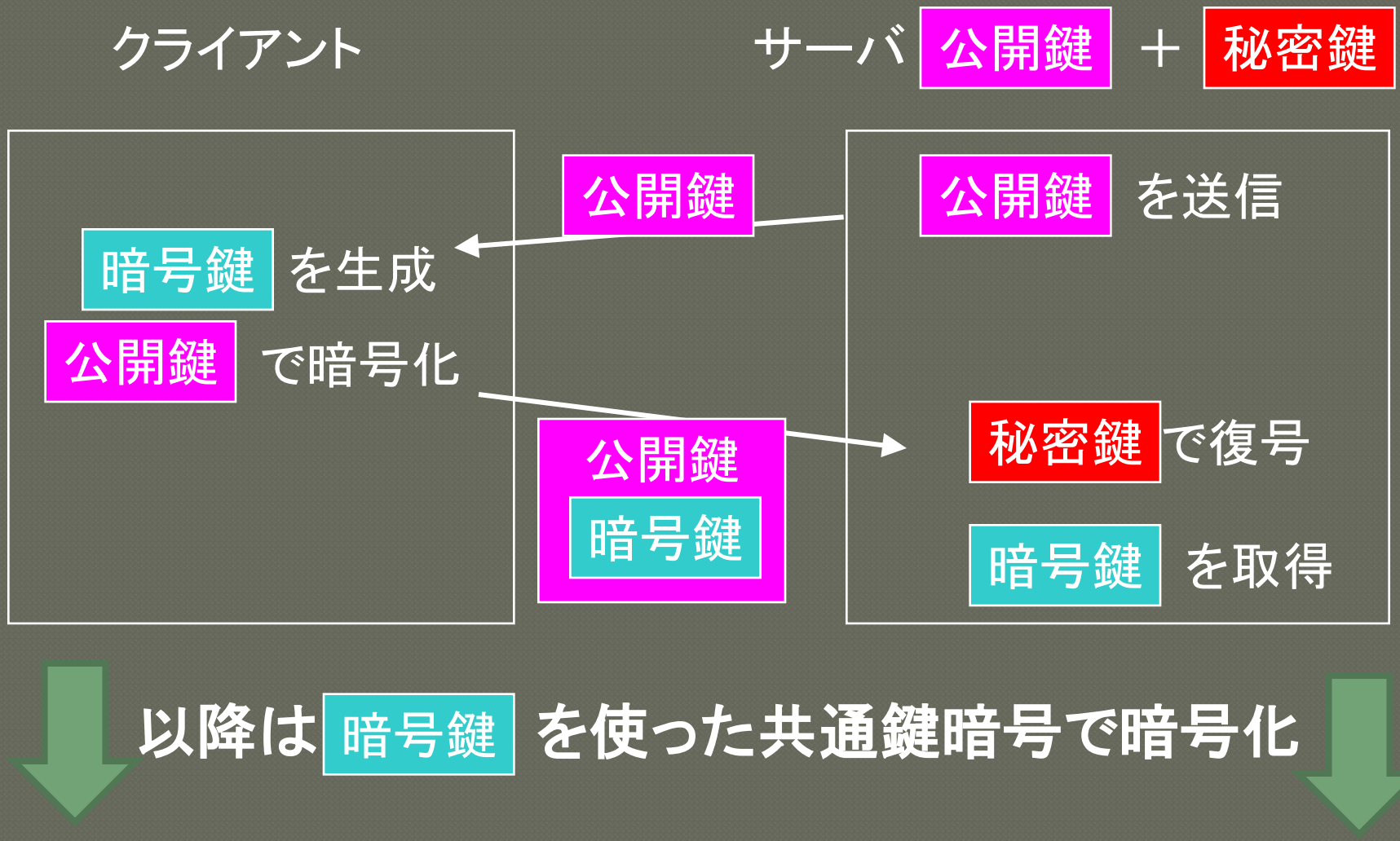
- IdP/SPにインストールされるHTTPSサーバ証明書
  - IdPとユーザ、SPとユーザ間の通信の安全
- IdPとSPとの間で通信する際に使用する証明書
  - 上記サーバ証明書と同じ場合もある
- メタデータへの電子署名
  - フェデレーションに参加しているIdP/SP情報を間違いなく受け渡すための仕掛け

# 例　https://...

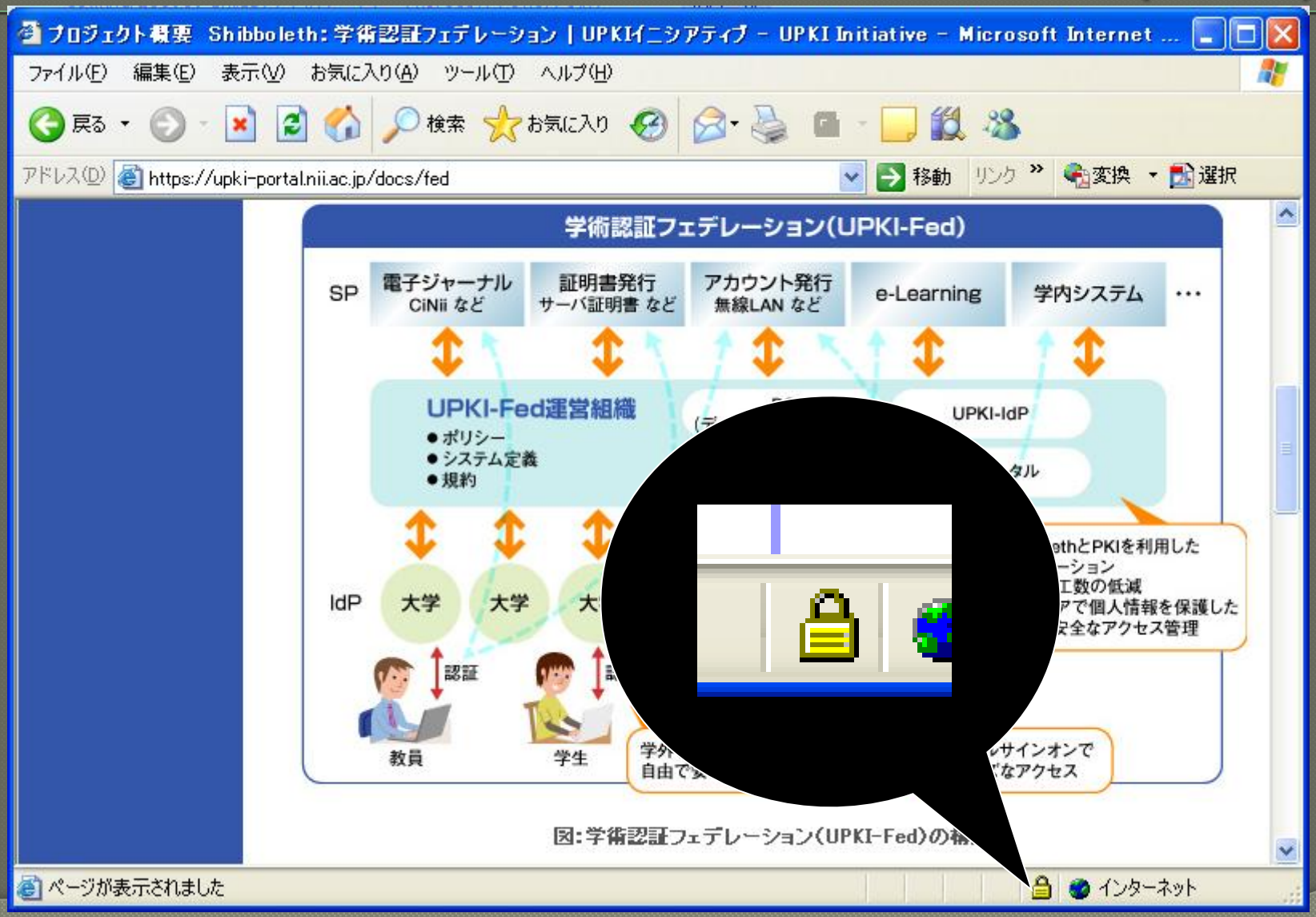
- SSL (Secure Sockets Layer) / TLS (Transport Layer Security)
- 通信先の認証
  - つまりクライアント（ブラウザ）がWebサーバを認証する
- 暗号化

- 公開鍵暗号体系を利用
  - 秘密鍵・公開鍵
  - 公開鍵→証明書
  - 電子署名

# SSL/TLSプロトコル簡略版



# ブラウザで見てみよう(1/2)

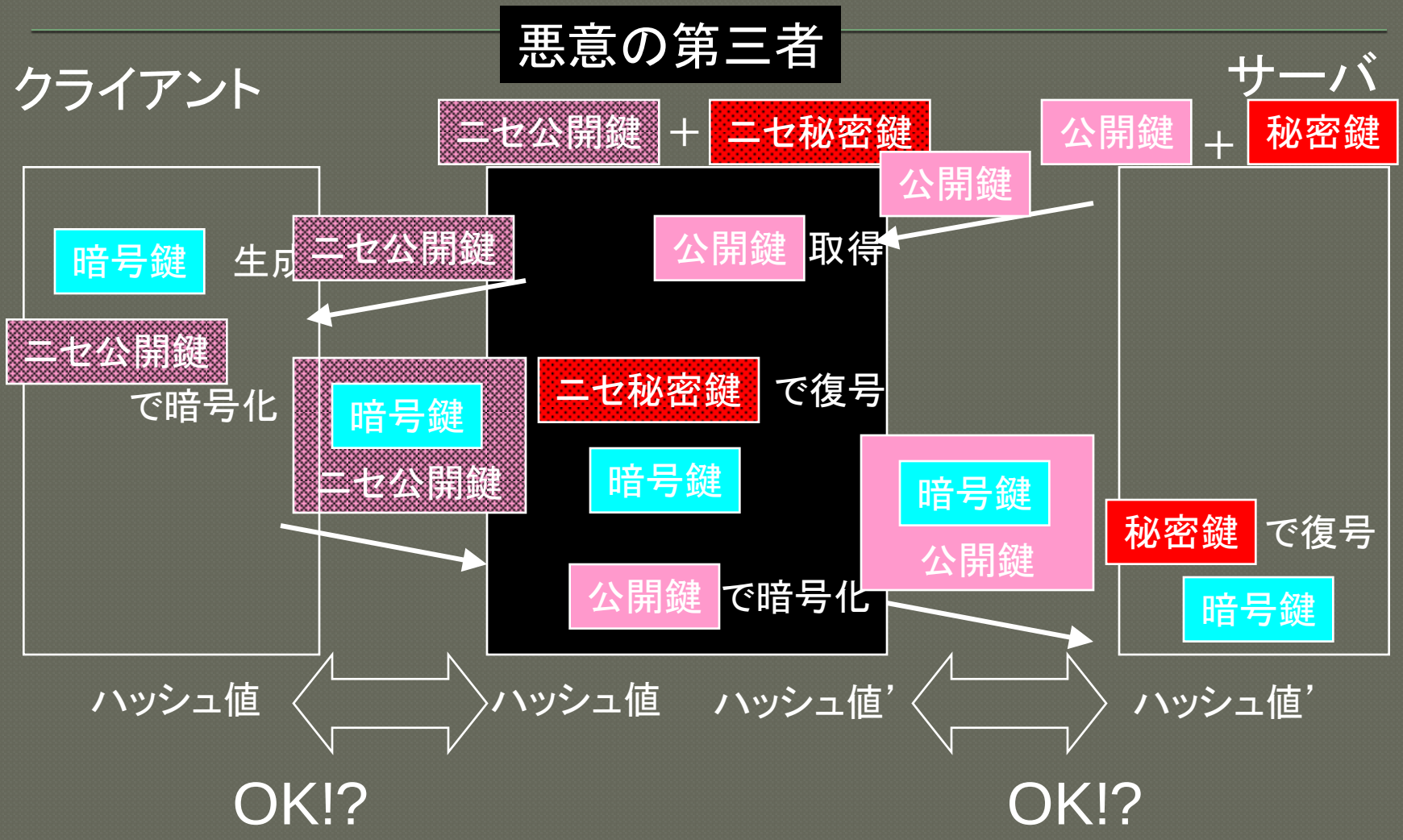


# ブラウザで見てみよう(2/2)

# サーバ証明書の注意点

- 証明の対象がFQDN (Fully Qualified Domain Name)であること（EVでない証明書の場合）
- サイト／サーバの信頼性は何ら保証していない！
- 運営している会社についても…
  - やみくもに「信用できるんだー」と思うのは危険
- フィッシング詐欺防止になる？

# 公開鍵暗号の弱点
## Man in the Middle Attack



# PKI（Public Key Infrastructure, 公開鍵基盤）

# 証明書署名問題の解決方法その１（限定的）

- ShibbolethのIdP-SP間の通信の安全性を保証する証明書は、誰が保証している？
  - →フェデレーションのメタデータに入っているものと比較すればよい
- では、メタデータの正しさは誰が保証する？
  - →メタデータには電子署名がされている
- では、その電子署名に使用される証明書の出自は誰が保証している？
  - →フェデレーション参加時にこの証明書が配付されるのでこれをもとに検証できる

→万事OK!

ただし、このように証明書の確認ができる例は少ない
（大学構成員全員に証明書を配付することが難しい、など）

# PKI（Public Key Infrastructure）

- 公開鍵基盤（公開鍵暗号基盤、公開鍵認証基盤とも）
- 自分の名前と公開鍵に対する「お墨付き」を与えるもの
  - 自己申告では証明の意味がない
- 世の多くの人が信用する認証局(Certification Authority, CA)を構築し、認証局が各認証対象に証明書を発行する
  - つまり、認証局が独自の鍵ペア（秘密鍵・公開鍵）を持ち、サーバ証明書の署名は認証局の秘密鍵により生成される
- 商用認証局の有名どころは VeriSign, Thawte, GeoTrust, Comodoなど

# 例として：サーバ証明書を欲しい人が行なうこと（されること）

- 発行会社（認証局）を選ぶ
- サーバと管理者（責任者）の関係を審査される
- ドメイン所有者との関係を審査される
- 発行料金を支払う

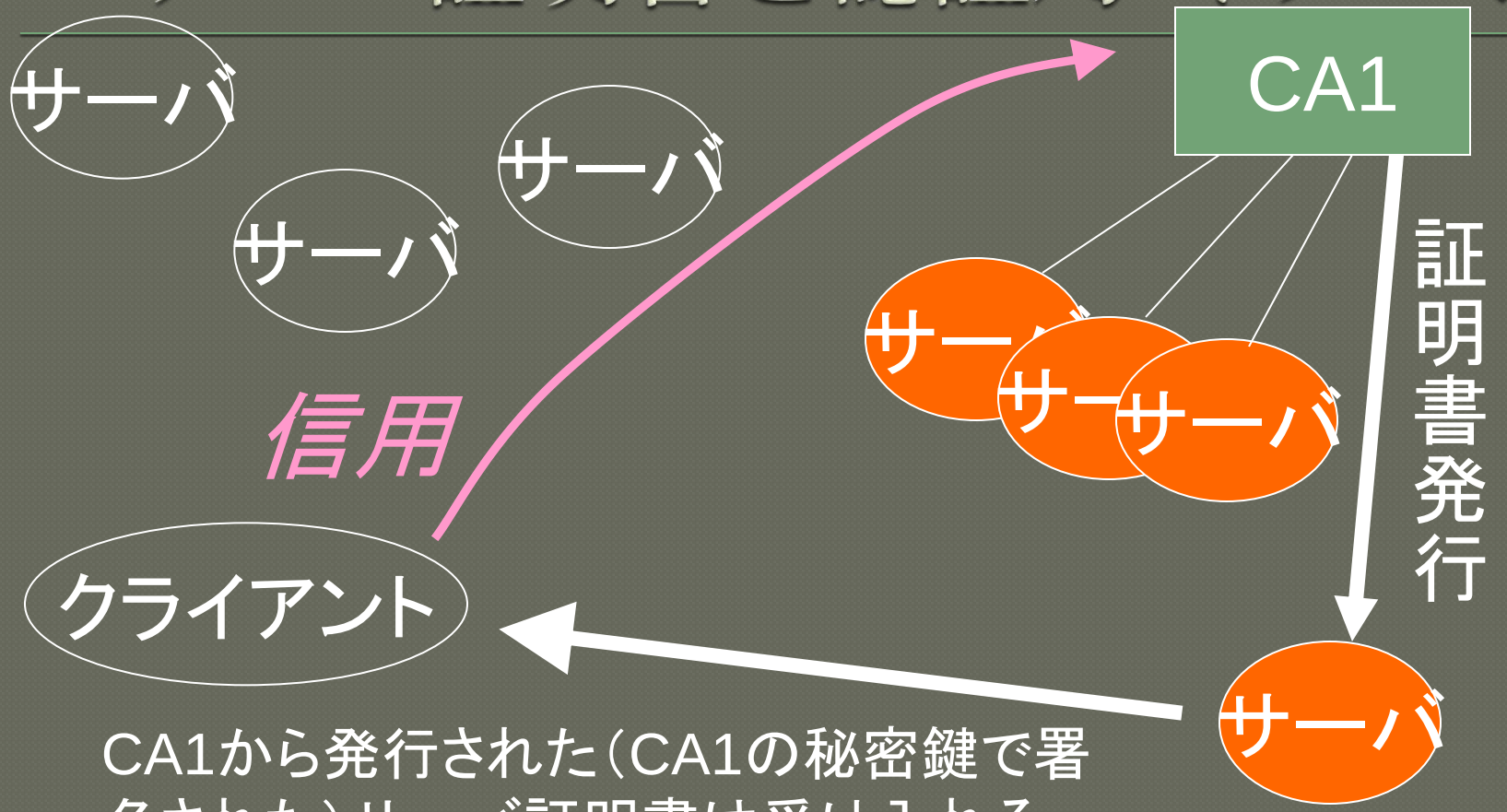
# 発行会社が行なうこと

- 申請者の身元確認
- ドメイン所有者の身元確認
  - 電話
  - WHOIS
  - 登記の提出

# 信用される証明書

- 多くの人から信用されるためには、発行のための基準が公開されそれを守っていることを証明できることが必要（WebTrust for CA）
  - 外部監査によって証明
- ブラウザが信用できる／できないの基準を持つ
- 緑のバー － EV SSL証明書

# サーバ証明書と認証局-イメージ




CA1から発行された（CA1の秘密鍵で署名された）サーバ証明書は受け入れる

# 信用されない証明書

- 多くの人から信用されているわけではない認証局の証明書
  - プライベート証明書
  - 自己署名証明書
- 別途自力で認証局の信用度を確かめること推奨
  - その認証局の公開鍵も何らかの安全な方法で取得する必要がある
- 「警告を無視してください」は多くの場合に不適切

# PKIの能力(ちから)

- 認証一般
  - サーバだけでなく個人に対する身元確認も
- 通信路の暗号化（SSL/TLS)
- 文書に対する暗号化
  - メールの暗号化・電子署名（S/MIME)
- 文書に対する電子署名
  - 電子決裁
  - 電子カルテ

# 組織に閉じた運用も有用

- 人の認証の場合は特に、組織内の個人への証明書発行をその組織内の認証局によって行なうことが多い
  - サーバ証明書のところで出てきた分類でいうとプライベート証明書
- 組織内のサービスはその個人証明書を元に行なうことができる
  - 他組織がその証明書を信用するかは別問題

# PKIによる認証の「信用」

- どうやってサーバ/サーバ管理者を識別するか
  - 赤の他人が証明書を取得しては水の泡
  - この識別(審査)を行なう機関を登録局(Registration Authority)と呼ぶ（通常認証局内にある）
  - 対面で手渡しが最も確実だが……
- 個人証明書の場合は秘密鍵格納メディアの問題
  - 秘密鍵を外部に取り出せない構造のものもある（例：ICカード）
- etc.

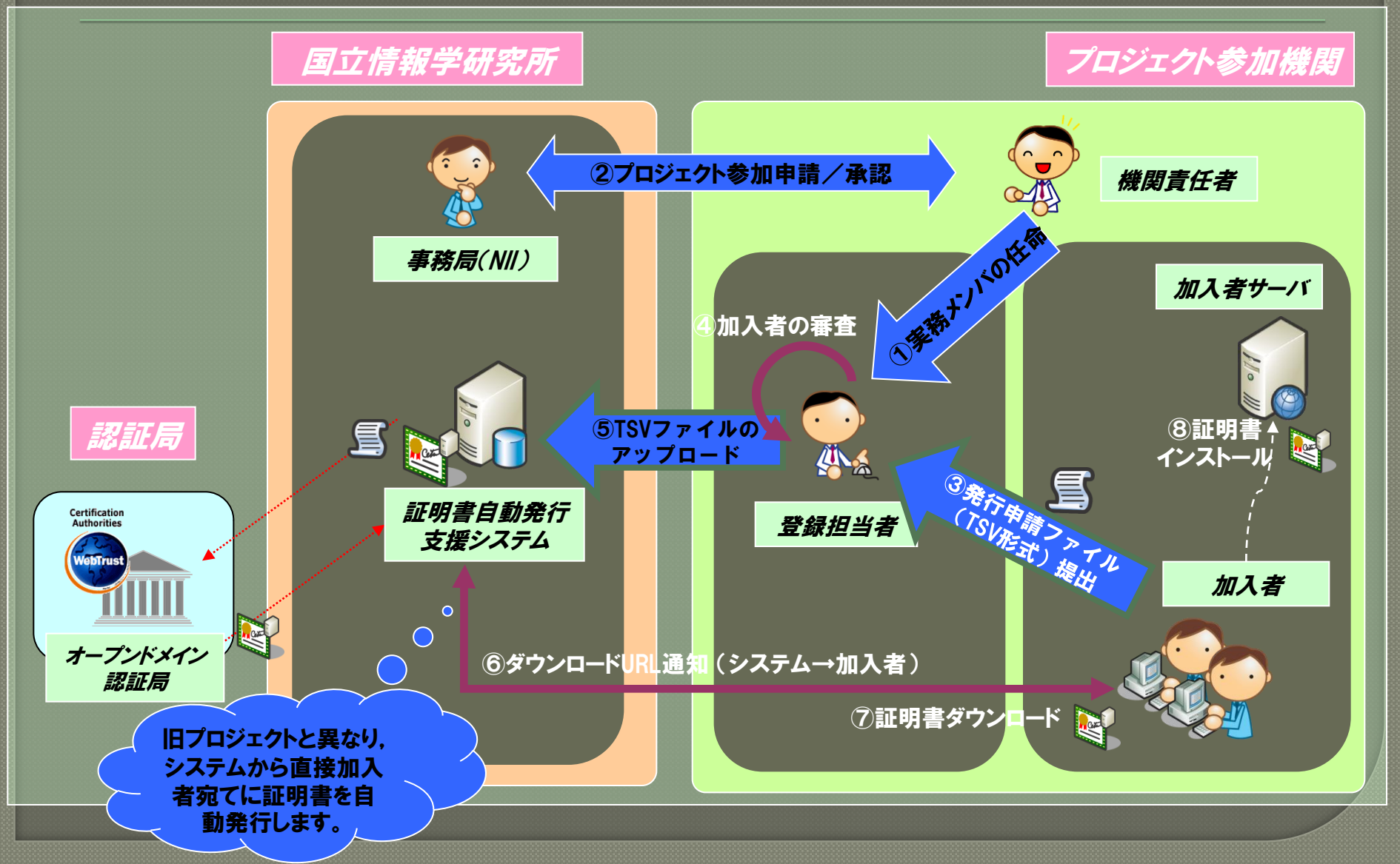
これらをどのように行なうか、何を選択したかを文書とし、これを元に信用する／しないが決定される

CP/CPS
(Certificate Policy / Certification Practice Statement)
証明書ポリシー/認証運用規程

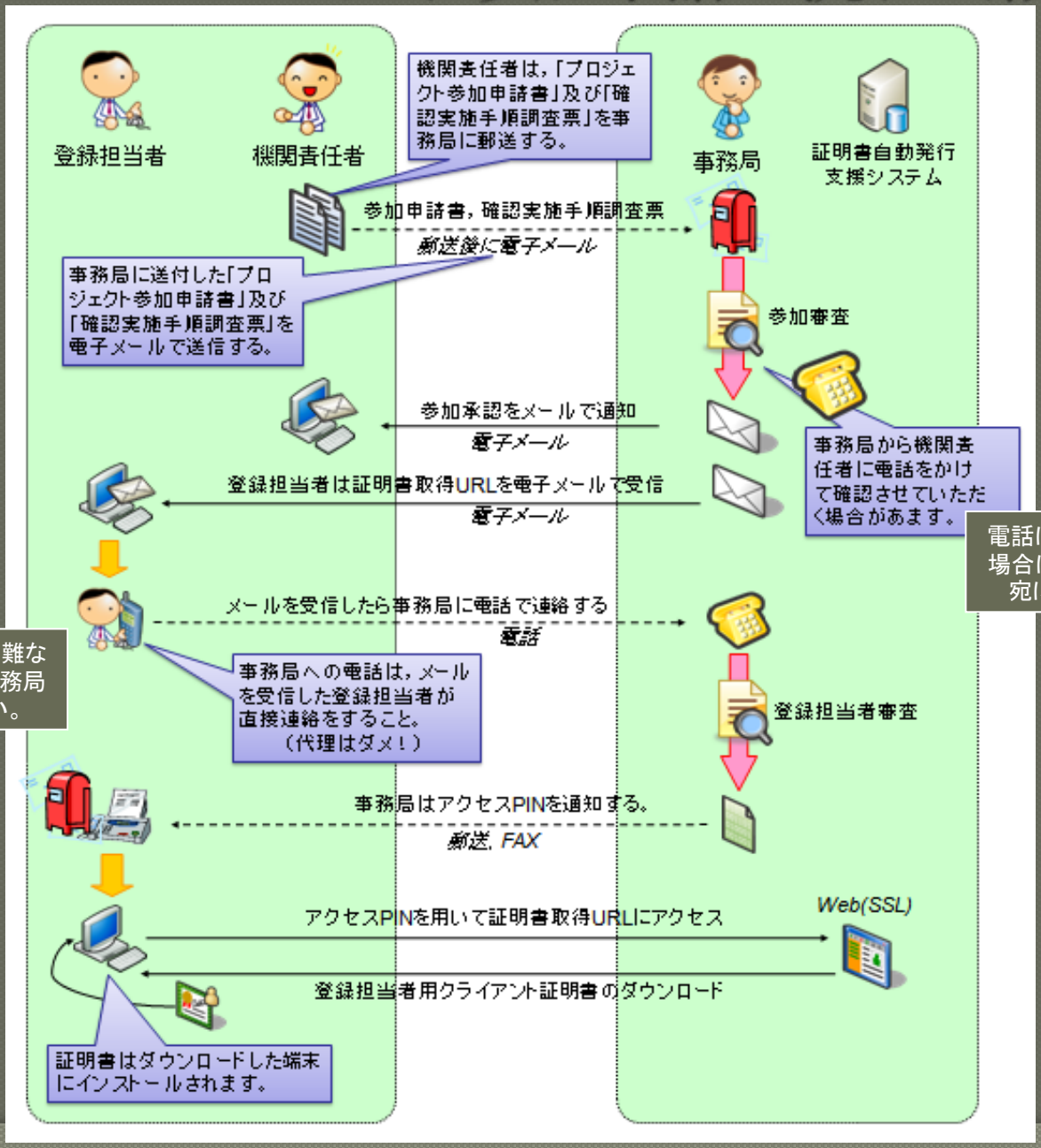
# UPKIオープンドメイン証明書自動発行検証プロジェクト

プロジェクトページ：
https://upki-portal.nii.ac.jp/docs/odcert

# UPKIオープンドメイン証明書自動発行検証プロジェクト



# プロジェクト参加申請の流れ（概要図）



# プロジェクト参加申請書（表面）の記入例　（1/2)

（表）

平成21年5月11日

UPKIオープンドメイン証明書自動発行検証プロジェクト　参加申請書

記入例

国立情報学研究所
学術情報ネットワーク運営・連携本部長　殿

所属機関名　記入例大学
機関責任者（自署）　機関責任者の自署を願います。　印

本プロジェクトの参加要領を理解し，次のとおりプロジェクトの参加を申し込みます。

| | | | | | |
|---|---|---|---|---|---|
| 参加申請種別 | (2)旧プロジェクトから継続参加 | | | | |
| 所属機関 | 機関名（日本語表記） | 記入例大学 | | | |
| | 機関名（英語表記） | The University of Example | | | |
| | 所在地 | 〒123-4567　東京都千代田区一ツ橋2-1-2 | | | |
| 機関責任者 | 氏　名 | 情報　太郎 | | 所　属 | 情報基盤センター |
| | 職　名 | センター長 | | 電話番号 | 03-1111-3333 |
| | E-Mail | taro@example.ac.jp | | | |
| | 所属住所 | 所属機関に同じ | | | |
| 対象ドメイン | example.ac.jp | | | | |
| 登録担当者1 | 氏　名 | 研究 | 花子 | 所　属 | 情報基盤センター |
| | ローマ字 | Kenkyu | Hanako | | |
| | 職　名 | 准教授 | | 電話番号 | 03-1111-7777 |
| | E-Mail | hanako@example.ac.jp | | FAX | 03-1111-8888 |
| | 所属住所 | 〒（所属機関所在地と同じ場合は省略可） | | | |
| 登録担当者2 | 氏　名 | 事務 | 一朗 | 所　属 | 基盤企画課 |
| | ローマ字 | Jimu | Ichiro | | |
| | 職　名 | 基盤企画課長 | | 電話番号 | 03-8888-9999 |
| | E-Mail | ichiro@example.ac.jp | | FAX | 03-8888-5555 |
| | 所属住所 | 〒（所属機関所在地と同じ場合は省略可） | | | |
| 登録担当者3 | 氏　名 | | | 所　属 | |
| | ローマ字 | | | | |
| | 職　名 | | | 電話番号 | |
| | E-Mail | | | FAX | |

手書き自署のうえ，押印をお願いします。

**書類確認者**

機関責任者

機関責任者は，本人性・実在性を確認・審査したうえで，登録担当者を任命してください。

4名以上の登録担当者を任命する必要がある場合は，事前に事務局までご相談ください。

# プロジェクト参加申請書（裏面）の記入例　（2/2）

必ず確認のうえ選択肢を選んでください。なお，選択肢はリストから選択可能です。（全機関必須）

旧プロジェクトの参加機関のみいずれかを選択してください。

（裏）

## 機関責任者確認事項

記入例

記　入　日　平成21年5月11日
機 関 名 称　記入例大学
機関責任者　情報　太郎

（1）以下の項目について確認の上，確認欄から該当する選択肢を選んでください。

| | |
|---|---|
| 【OK】 | SINET加入機関の確認<br>自機関が，学術情報ネットワーク(SINET)加入機関[1]であることを確認した。 |
| 【OK】 | ドメイン登録担当者への確認(ドメインの本人性確認)<br>対象ドメインでのサーバ証明書発行を，機関責任者及び登録担当者が担当することについて，ドメイン登録担当者[2]の承諾を得た。 |
| 【OK】 | 登録担当者からの承諾(登録担当者の本人性確認)<br>確認実施手順調査票で定めた手順をもとに，登録担当者がプロジェクト参加要領を理解し，参加要領第6条に定める事項について承諾していることを確認した。 |
| 【OK】 | 登録担当者の記載内容の確認(登録担当者の実在性確認)<br>参加申請書に記載した全ての登録担当者情報について，事実と相違ないことを確認した。 |
| 【OK】 | 確認実施手順調査票の確認<br>(新規参加機関の場合)確認実施手順調査票に記載した全ての情報について，事実と相違ないことを確認した。<br>(旧プロジェクト参加機関の場合)旧プロジェクトの確認実施手順から変更が無いこと[3]を確認した。 |

【旧プロジェクト参加機関のみ】

| | |
|---|---|
| (B)機関責任者変更 | 旧プロジェクトの機関責任者の本人性について，どちらか該当する項目を選択してください。後者の場合は，旧プロジェクト機関責任者氏名についてもご記入ください。 |
| | (A)旧プロジェクトの機関責任者が，引き続き本プロジェクトの機関責任者を務める。 |
| | (B)本申請書に記載されている機関責任者が，本プロジェクトの機関責任者を務めることについて，旧プロジェクト機関責任者の承諾を得ている。 |
| | 機関責任者氏名：情報　太郎 |
| | 旧プロジェクト機関責任者氏名：基盤　三郎 |

（2）その他(事務局への連絡事項などありましたらご記入ください)

公印を押印できる文書が本学所定の様式に限られるため，別途学長が押印した文書「UPKIオープンドメイン証明書自動発行検証プロジェクト参加申請について(依頼)」(○○○第XX-NN号)を文書の写として添付します。どうぞよろしくお願い致します。

書類確認者

機関責任者

機関責任者の承継や事務局への連絡事項等についてご記入ください。

# 確認実施手順調査票の記入　(1/2)

**確認実施手順調査票は，記入例を参考にしながら，貴学の実状に合わせて記入するようにしてください。**

1-2　登録担当者の本人性確認

登録担当者の本人性確認を行うにあたって、「どのような情報」をもとに、「どのような方法で」確認を行い了承を得たのかを教えてください。

| | |
|---|---|
| ○ | 「登録担当者は既に面識があるので」「直接対面で問い合わせて」了承を得ました。 |
| ○ | 「登録担当者の教職員証を提示してもらい」「直接対面で」確認しました。<br>*面識がない登録担当者の場合、顔写真付きの教職員証を使用してください。* |
| ○ | 「学内のLAN管理委員会において委員長が担当者を指名」し、「本人から直接」了承を得ました。 |
| ○ | 「最新の学内名簿で登録担当者の内線やメールアドレス」を確認し、「本人へ電話またはメールで問い合わせて」了承を得ました。 |
| × | 「登録担当者にメールまたは文書で任命通知を行い」「一定期間以内の異議申し立てがないことを以て」了承されたものとみなしました。<br>*登録担当者が必ずしもメールまたは文書を理解して合意したことが確認できません。* |

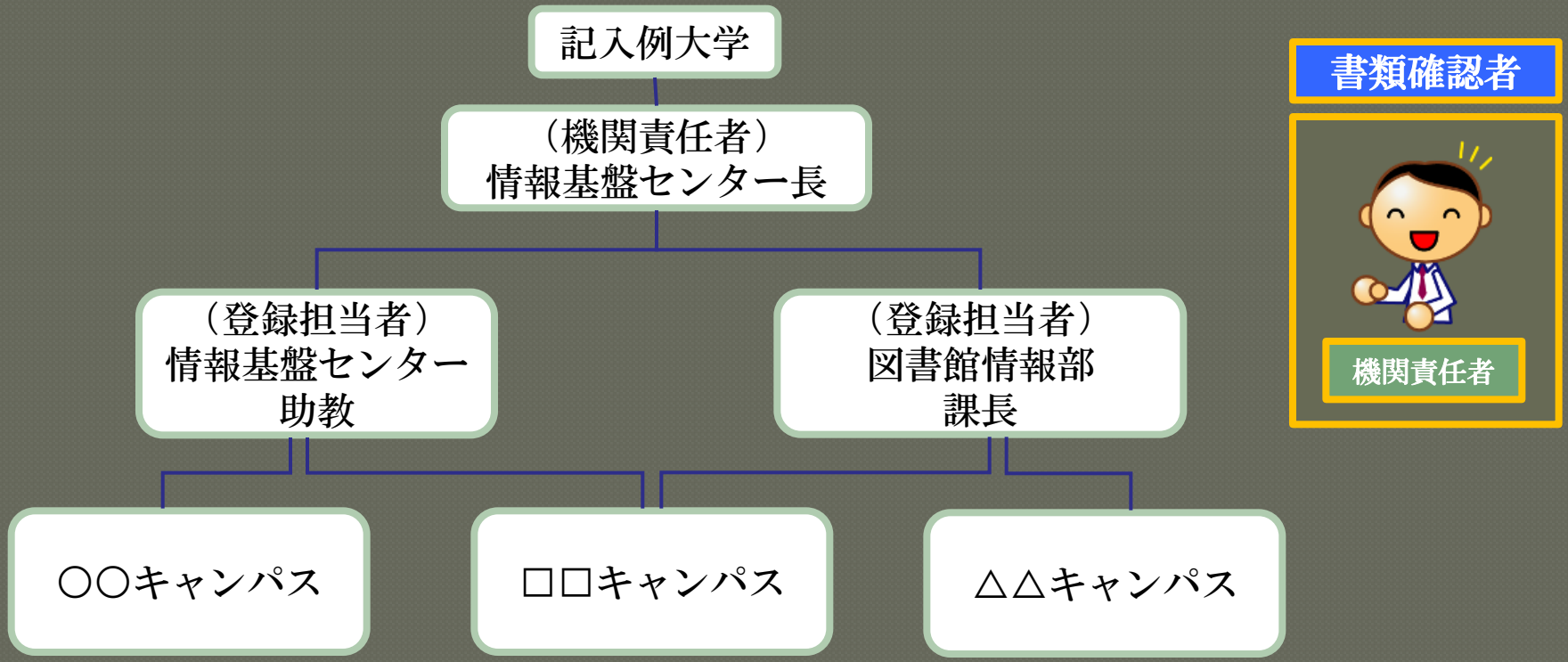
書類確認者

機関責任者

| | |
|---|---|
| 1-2 | 登録担当者の本人性確認 |
| | 登録担当者の本人性確認を行うにあたって，「どのような情報」をもとに，「どのような方法で」確認を行ったかを教えてください。 |
| | 「登録担当者は既に面識がある」ので「直接対面で問合わを行いながら」確認を実施した。また，身分証明書を提示していただいた。 |

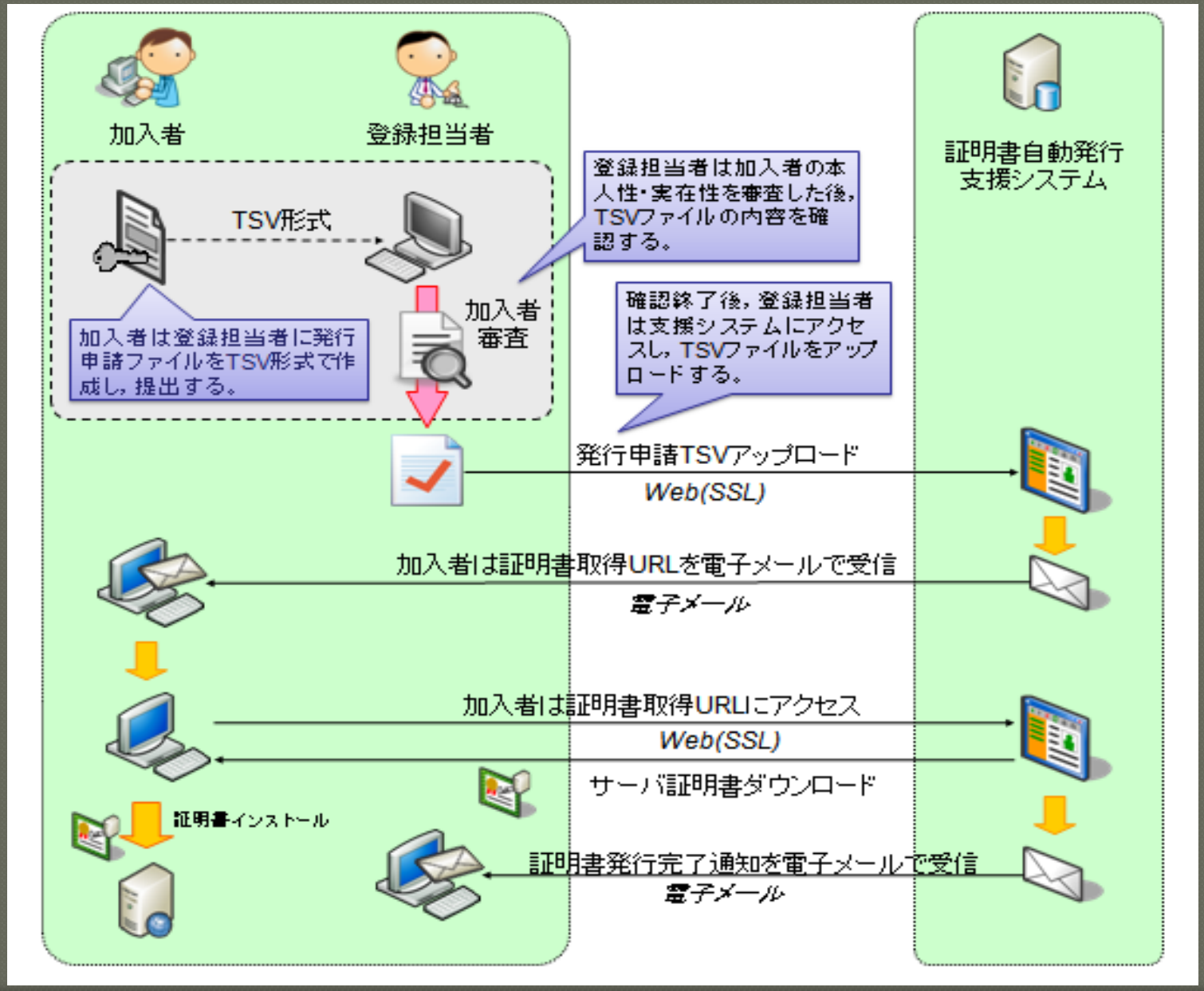
# 確認実施手順調査票の記入　(2/2)

機関責任者と登録担当者の担当や体制を図示してください。




各登録担当者が所管の部局等をお持ちでしたら，併せまして体制図中にご記入ください。

# サーバ証明書発行申請から証明書取得までの流れ



# まとめ

- 認証
  「相手」を識別するための手続き
  - 「相手」は人だけではない
  - 認証方法はID/パスワードだけではない
- 電子証明書
  公開鍵暗号という技術により電子的な「署名」を施されたデータ
- PKI
  電子証明書およびその発行機関としての認証局からなる社会基盤
  （周辺技術も含めて呼ぶ場合もある）

PKIを用いた認証によってインターネット上のやりとりの多くが安全に実現されている。公開鍵暗号という技術の上に、認証局という運用が加わって安全性が担保される。