認証技術の利用

ネットワークセキュリティ技術研修

2008.8.22

国立情報学研究所　中村素典

内容

- PKIによる認証基盤
- 大学間認証連携(UPKI)
  - サーバ証明書発行
  - 無線LANローミング
  - シングルサインオン

ネットワークセキュリティにおける4つの脅威

- 盗聴
- 改竄 (かいざん)
- 成りすまし
  - フィッシング、Man-in-the-middle
- 否認

→ 対策は暗号化と署名 (認証)

認証のための暗号方式

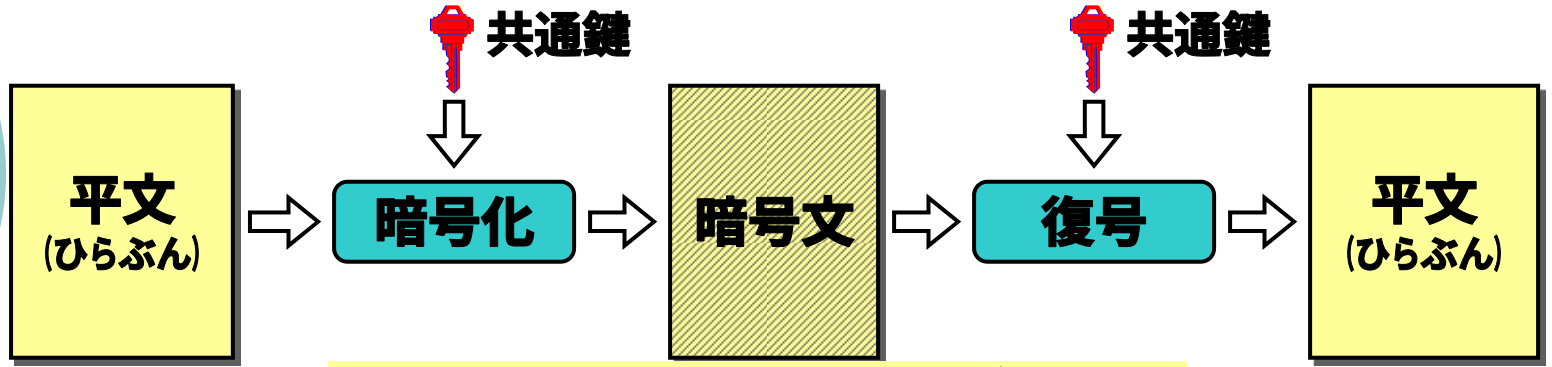
- 共有鍵方式
  - パスワード
    - サーバに生パスワード保存?
    - ネットワークに復号容易なパスワードが流れる?
    - 認証可能な回数に制約? (ワンタイムパスワード)
- 公開鍵方式
  - 公開(public)鍵と私有(private)鍵の2つを用いる
    - 私有鍵は本人のみが持つ
    - 公開鍵は相手を問わず広く公開
  - 暗号化に加えて署名を実現

暗号方式の使い分け

- 鍵の数
  - O(n×n) ⇔ O(2n)
- 処理速度
  - 公開鍵暗号の計算は共有鍵暗号より遅い
- 発行のコスト
  - 有効期限の設定
  - 再発行のコスト(失効処理など)
- その他の制限との組み合わせ
  - IPアドレスによる制限等
    - Brute forceアタックの回避

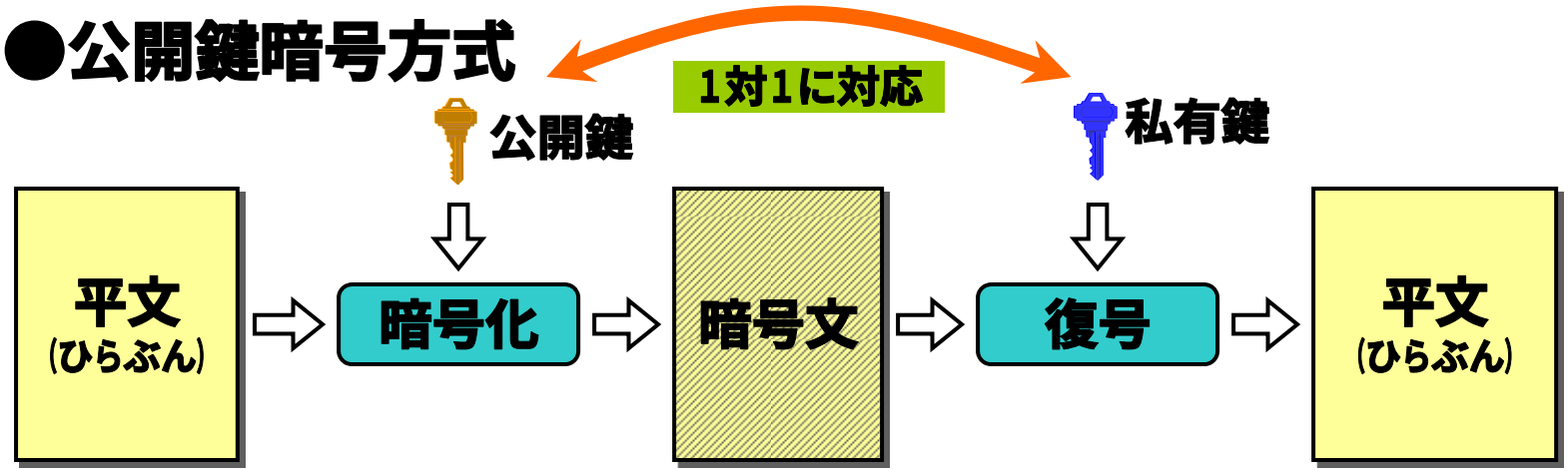
■共通鍵暗号方式と公開鍵暗号方式

●共通鍵暗号方式



→暗号化と復号の鍵が同一

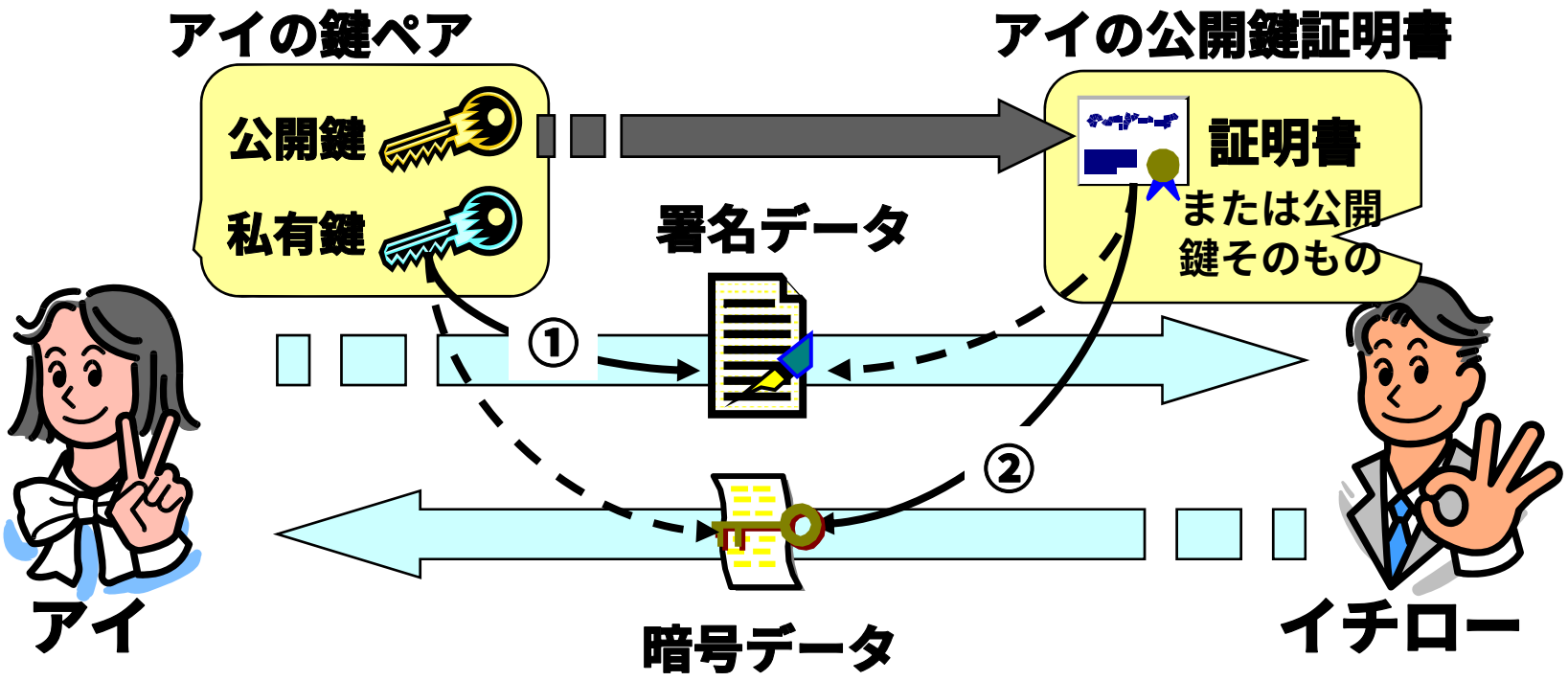
●公開鍵暗号方式



→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



公開鍵方式を利用する際の考慮点

- 私有鍵の配布
  - 本人だけに確実に渡す方法
  - 漏洩対策
- 公開鍵の配布
  - 信頼性の確保（なりすまし防止）

いかに安全に鍵を受け渡すか

- 対面による本人確認
- 別チャンネルの利用
  - 例：クレジットカード情報はFAXや電話で
- Finger Printを事前に公知
  - 別チャンネルで
- CA（認証局）による
  - 信頼関係のリンクが切れないよう配慮が必要

私有鍵の保管方法

- ハードディスク
  - 安価、セキュリティ面が不安（耐タンパ性なし）
- USBトークン
  - 高価、かさばる
- ICカード
  - USBトークンより安価、アクセス用のハードウェアが必要、盗難にあうと表面記載の個人情報とともに悪用される危険

公開鍵の利用：SSLサーバ証明書

- https://.....
- **効果**
  - **盗聴防止、改ざん防止（通信の暗号化）**
    - **公開鍵を利用した共有鍵の受け渡し**
      - **処理効率の問題**
  - **（サーバの）なりすまし防止**
    - **サーバ証明書の検証が重要**
    - **サーバ名の確認も重要**
      - **表示とリンクのURLが異なる場合**
        - <A HREF="SITE B">SITE A</A>
      - **フィッシングサイトも正しい証明書を持っているかも**

公開鍵の信頼性の確保

- 認証局(CA: Certificate Authority)による署名パスの確認 (信頼のおける第3者)
- 事前に公開鍵を安全に配布し、クライアントにインストール

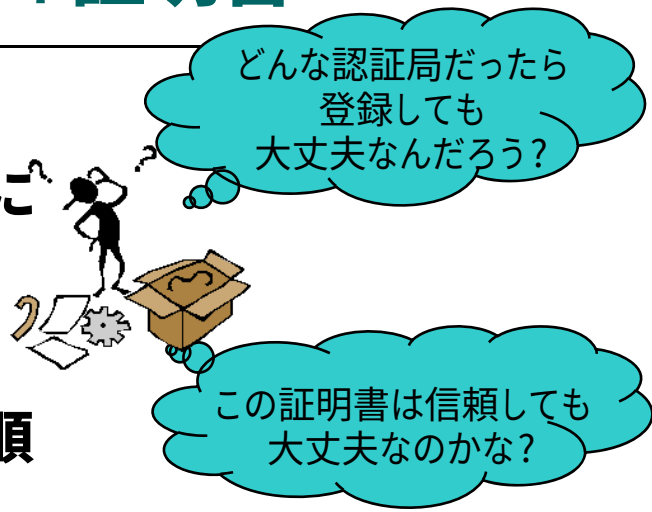
- 信頼性を提供する範囲
  - オープンドメイン
    - 国際規準WebTrust for CA準拠 (参考：EV証明書)
    - 多くのクライアントに証明書がインストール済み
      - クライアント (配布) の信頼性問題
  - クローズドドメイン (プライベート認証局)
    - 組織ごとの独自のルート認証局
      - ユーザにどのようにしてインストールさせるか (サーバ証明書の場合)
  - オレオレ証明書 (自己署名のみ)
    - サーバ単位でユーザが信頼の可否を判断
    - フィンガープリントを確認するくらいしか検証の方法がない?

公開鍵の信頼性の確保（続き）

- 鍵の紛失、盗難、廃止等への対応
  - 廃棄証明書リストの管理
    - CRL: Certificate Revocation List

プライベート認証局とプライベート証明書

- **プライベート認証局**
  - **ユーザがクライアントアプリケーションに後から登録する必要がある**
- **プライベート証明書**
  - **認証局からの信頼を何らかの追加手順なしには確認することができない**



これらは信頼してもらうには、利用者に何らかの設定や操作をしてもらう必要がある。

ここの確認手順を省略してしまうのがいわゆる「オレオレ証明書」

プライベート証明書は関係者限定の用途以外の利用は困難

オレオレ証明書と大学教育

- 誤った理解
  - 警告が出ても無視していい
    - 何かしらの理由がなければ警告は出ません
  - 警告を回避するには証明書を登録すればいい
    - どんな証明書でも登録していいわけではありません
- 必要な教育
  - 警告の理由と無視してもよい状況の説明
  - 登録してよい証明書といけない証明書の識別方法

十分な教育なしにプライベート証明書を使うことは最高学府として学生にさせるべきではない

オープンドメイン認証局とは?

- **国際規準**WebTrust for CA**に準拠**
  - **認証局の運用の厳格さを審査する規準**
    - **定期的に外部監査を受けているか?**
    - **認証局の鍵ペアは安全に管理されているか?** など
- Web**サーバに関する実在性を確認**
  - Web**サーバのドメイン**
  - Web**サーバを所管する機関**
- **主要なPKIアプリケーションの証明書リストに予め登録済。**

客観的で公平な規準

証明書用途に適した確認内容

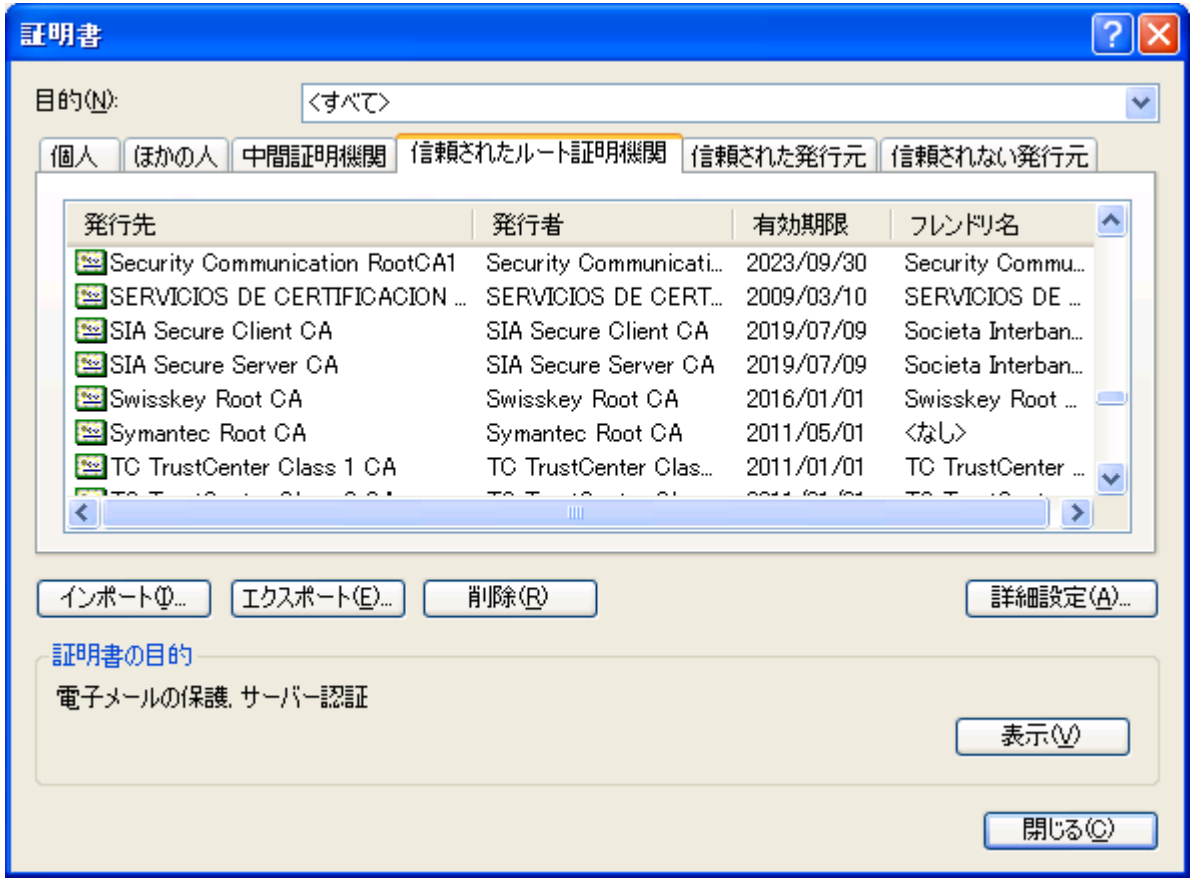
認定された認証局だから安心だね！
何も操作しなくても信頼できるから簡単だね！

オレオレ証明書の区分（高木浩光氏による）

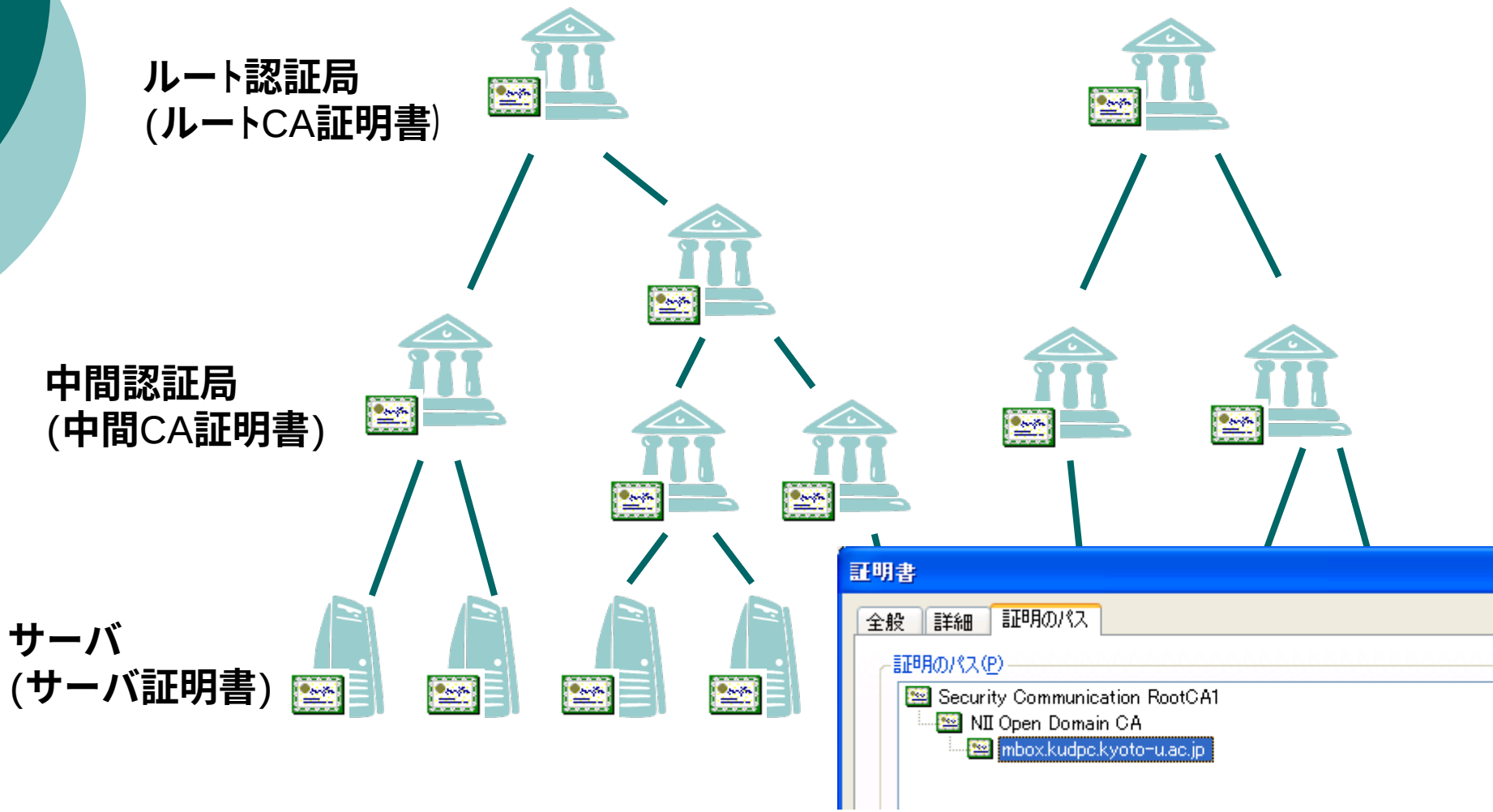
http://takagi-hiromitsu.jp/diary/20051118.html#p01　より

- 第一種オレオレ証明書
  - 不特定多数に利用させることを想定していて、ルート証明書もサーバ証明書もインストールさせるつもりのないもの。
- 第二種オレオレ証明書
  - 不特定多数に利用させることを想定していて、ルート証明書かサーバ証明書をインストールするよう促しているが、インストール方法として安全な手段が用意されていないもの。
- 第三種オレオレ証明書
  - 不特定多数に利用させることを想定していて、ルート証明書かサーバ証明書をインストールするよう促しており、安全なインストール方法が用意されているもの。
- 第四種オレオレ証明書
  - 特定の者だけに利用させることを想定しているもの。
- 第五種オレオレ証明書
  - 正規の認証局から取得したサーバ証明書であるが、一部のクライアントでその認証局がルートとして登録されていないもの。
- 第六種オレオレ証明書
  - 正規の認証局（中間認証局）から取得したサーバ証明書であるが、中間認証局の証明書をサーバに設置していないため、クライアントが認証パスを検証できないもの。

登録されているルート認証局の確認
(クライアントの種類やバージョンで内容が異なる)



認証局による署名のパス



運用コストの問題

- オープンドメインークローズドドメイン
- インソースーアウトソース
  - 初期費用と維持費用
- RAをどこまで展開するか(分散ー集中)
- 有効期限
  - 鍵の更新、再配布

CAの選択

- 利用者の範囲に依存する
  - 組織専用サーバ、GRID等特定利用者向けサービス
    - クローズドドメインCAでも良い
  - 公開Webサーバ
    - オープンドメインCAが望ましい
  - メールの署名、暗号化(S/MIME)
    - オープンドメインCAにすべき

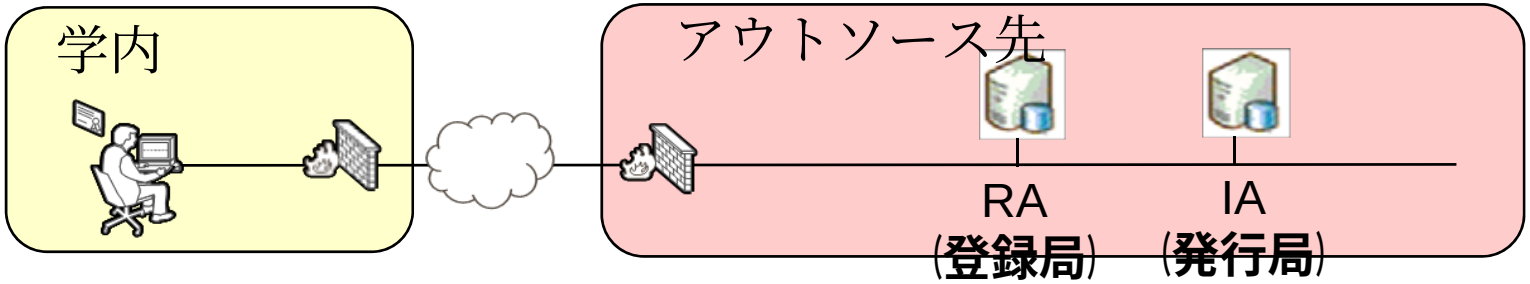
:

PKIシステムの運用

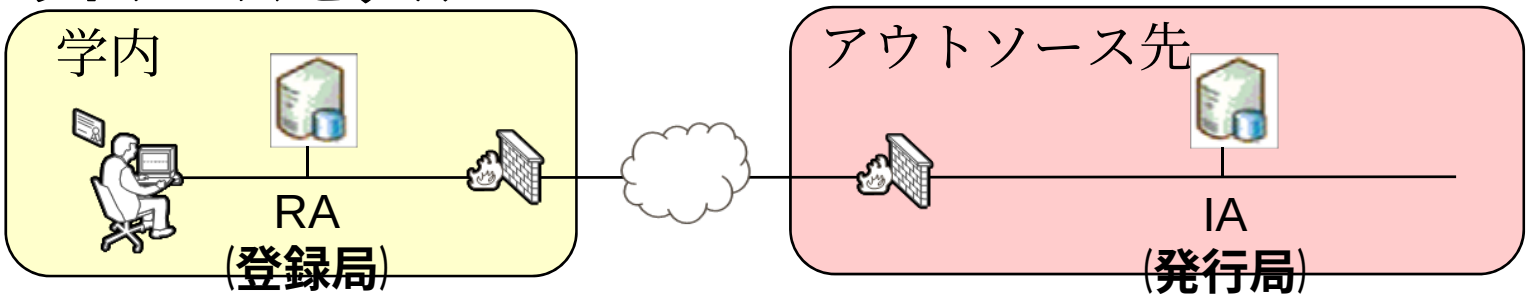
- 認証局の運用
  - インソース
    - 自前でサーバを設置･運用
      - 認証局の安全性の確保
  - アウトソース
    - 外部委託
      - フル / IA:Issuing Authorityのみ
- 登録局(RA: Registration Authority)
  証明書発行依頼業務 (審査)
  - ユーザの実在性確認
  - ユーザの本人性確認
- 信頼性の担保
  - 運用ポリシーの策定、公開と、それに基づく運用、監査

認証局(CA)の運用モデル

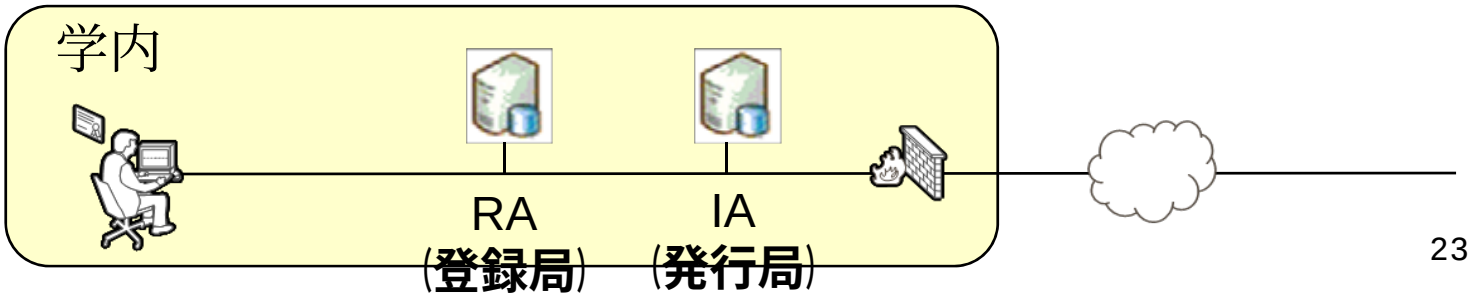
フルアウトソースモデル



IAアウトソースモデル



インソースモデル



運用ポリシー：CP/CPS

- **証明書ポリシー**
  - CP: Certificate Policy

  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。
- **認証局運用規定**
  - CPS: Certification Practice Statement

  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

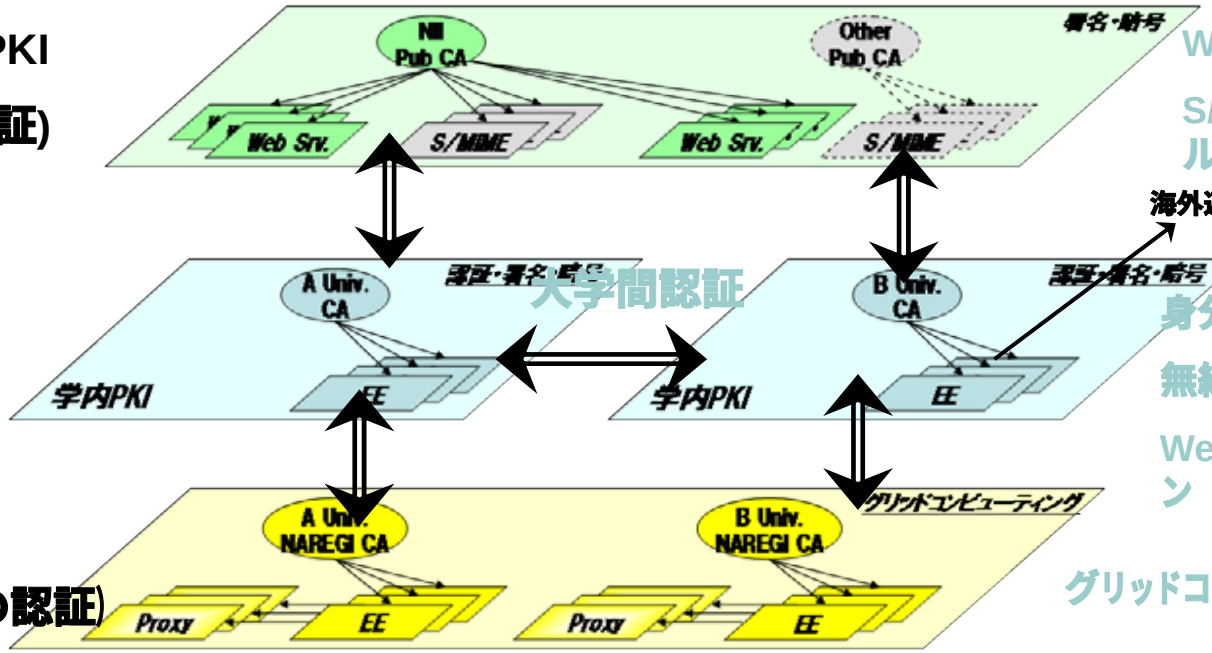
PKIの応用

- ネットワークアクセスローミング
- 別サービス用アカウント等の自動発行
- GRIDのアクセス認証
- 共有データベースの認証
- 大学間単位互換
- シングルサインオン
- フェデレーション
- タイムスタンプ、長期署名
  - 実験ノート、知財

大学間認証連携 (UPKI)

UPKIの基本アーキテクチャ

- 3階層のPKI（Public Key Infrastructure)による役割分担と連携



各PKI層のコンセプト

- オープンドメインPKI
  - いわゆるパブリックPKI
  - ルート証明書が予め配布されたPKI
  - 皆が信頼しているPKI、誰でも検証できるPKI
- キャンパスPKI
  - 各大学が個別のポリシに合わせて構築するプライベートPKI
  - その大学のユーザ(教職員and/or学生)であることを証明する
  - ユーザ(教職員and/or学生)への厳格な(対面等の配付が可能
- グリッドPKI
  - AP Grid PMAなどグリッド独自のセキュリティレベル
  - プロキシ証明書など一般的なPKIとは明らかに異なる概念

用途に応じたPKI層の使い分け

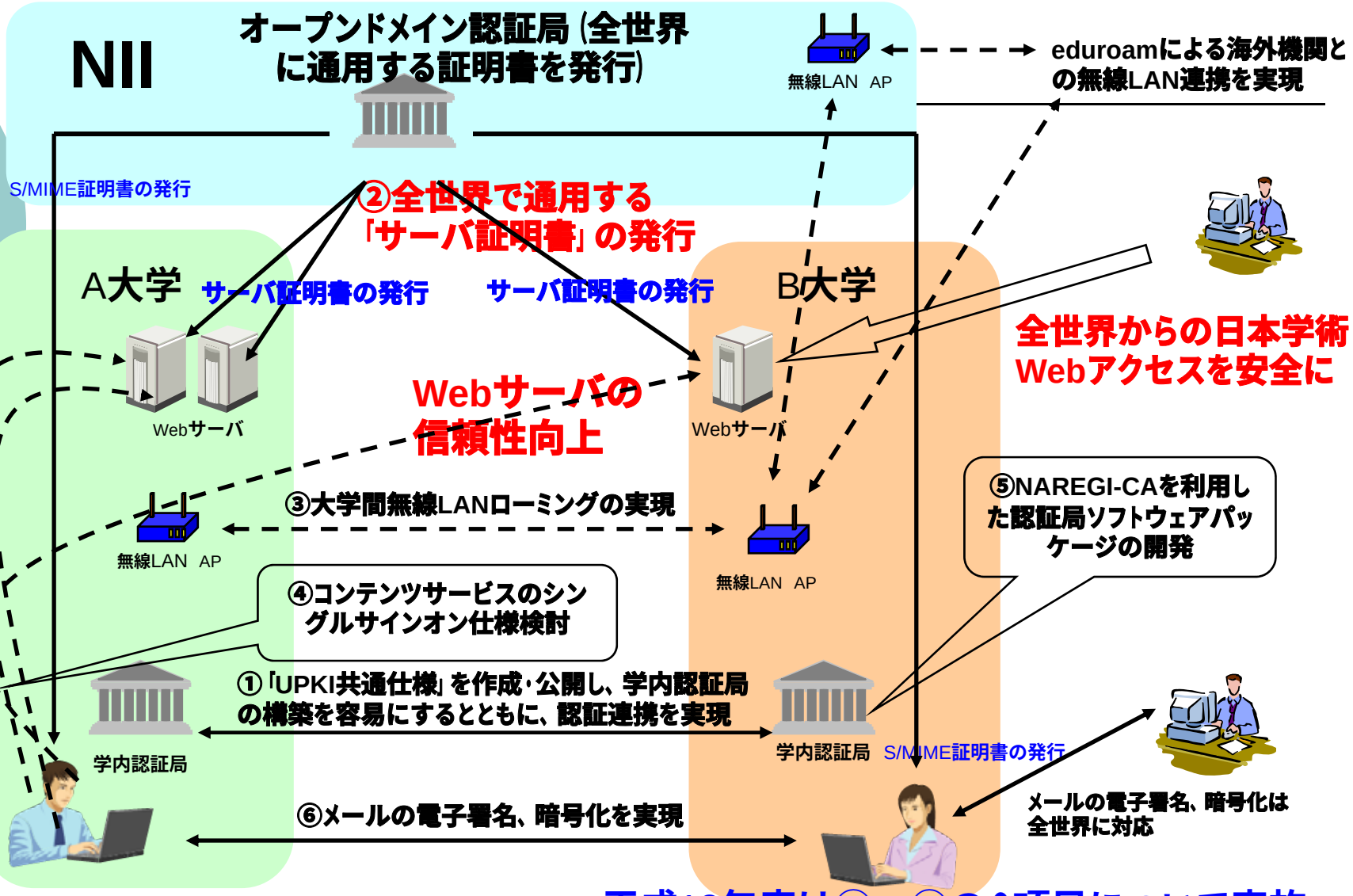
領域	用途	利用する証明書	ポイント
学外(公衆)	サーバ認証	オープンドメインPKIによるパブリックなサーバ証明書	誰でも検証できること
	クライアント認証	キャンパスPKIによるユーザ証明書をベースとしたID連携	保証レベルの担保
	S/MIME(署名・暗号)	オープンドメインPKIによるパブリックなS/MIME証明書	誰でも検証できること
学内	サーバ認証	オープンドメインPKIによるパブリックなサーバ証明書	ルート証明書の配布
	クライアント認証	キャンパスPKIによるプライベートなユーザ(教職員and/or学生)証明書	特定の認証局からのみ検証できること
	暗号	学外同様S/MIMEを利用、または共通鍵による暗号化＋クライアント認証等によるアクセス制御	鍵預託・鍵更新
	署名	キャンパスPKIによるプライベートなユーザ(教職員and/or学生)証明書	本人による鍵生成 または認証局による厳密な鍵ペア配付
グリッド	MyProxy認証	グリッドPKIによるグリッドユーザ(グリッド利用者)証明書	
	Delegation	グリッドPKIのグリッドユーザ鍵ペアによるプロキシ証明書	ユーザによる権限委譲

各PKI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	全国共同利用センター
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	計算機資源の安全な共有
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（成績証明書、事務ペーパレス化等）	プロキシ証明書の発行など
証明書発行対象	サーバ、自然人など	教職員、学生など	各地域の計算機資源、計算機利用者など
信頼者（Relying Party）	不特定多数	主に学内関係者	計算機利用者
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 、インソースなど	全国共同利用センター

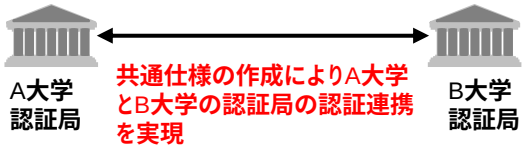
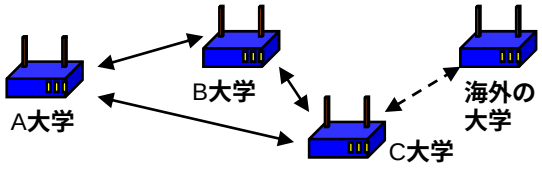
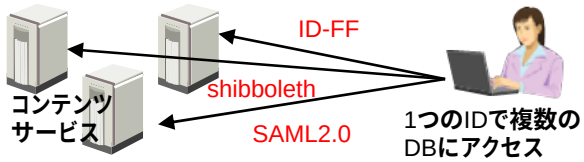
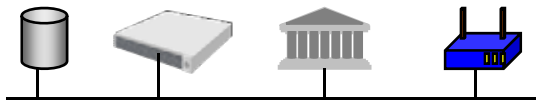
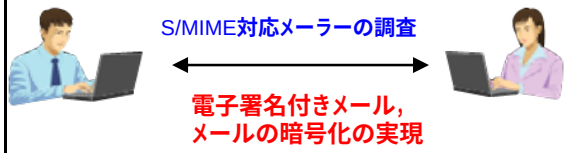
UPKI構築の全体スケジュール

UPKIで開発中のアプリケーション等



平成18年度は①～⑥の6項目について実施

これまで実現したUPKIの成果

項番	事項	内容
1	「UPKI共通仕様」の作成と配布	 「UPKI共通仕様」の利用により大学での ・学内認証局の構築 ・CP/CPS等の規程の整備 が容易に実現可能に
2	オープンドメイン認証局の構築とサーバ証明書の発行	 オープンドメイン認証局の構築により，全世界に通用するサーバ証明書を発行し，大学のWebサーバの実在性証明と通信の暗号化を実現
3	大学間無線LANローミングの実現 (東北大学が中心)	 eduroamによる大学間無線LANローミングを実現。海外のeduroam参加機関との連携も実現
4	コンテンツサービスのシングルサインオン仕様検討	 各種データベースサーバへのシングルサインオンを実現するため，shibboleth，SAML2.0等の仕様を調査し，UPKIにふさわしい方式を検討
5	NAREGI-CAを利用した認証局ソフトウェアパッケージの開発	 オープンソースの認証局ソフトウェアあるNAREGI-CAを用いて，認証局を簡単に構築し，無線LAN認証を容易に実現できるソフトウェアを開発 これにより，大学の認証局構築を促進する
6	S/MIME証明書の試験利用	 S/MIME証明書を，認証関係者間で試験利用するとともに，対応メーラーの調査，WebメールでのS/MIME利用の調査研究を実施

キャンパスPKI共通仕様（ガイドライン）の作成

先行大学の調査結果を踏まえて、**キャンパスPKI共通仕様**として以下に示すガイドラインを作成した。

(1)作成にあたって：キャンパスPKIガイドラインの作成にあたって、以下の点に留意した

- 各大学の調達・設計における参考資料、たたき台、雛形として活用できること
- 必ずしも準拠性を求めるものではないが、将来的に相互接続を想定している場合には本仕様に準拠することが望ましい

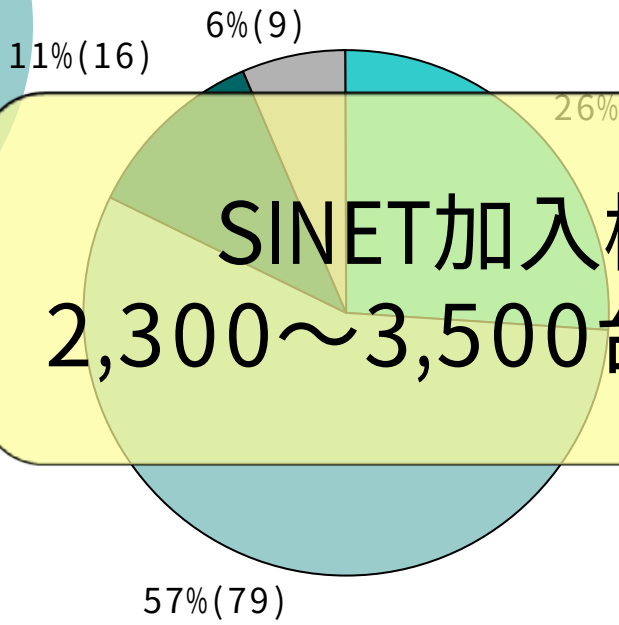
(2)ガイドラインの構成：

キャンパス PKI共通仕様

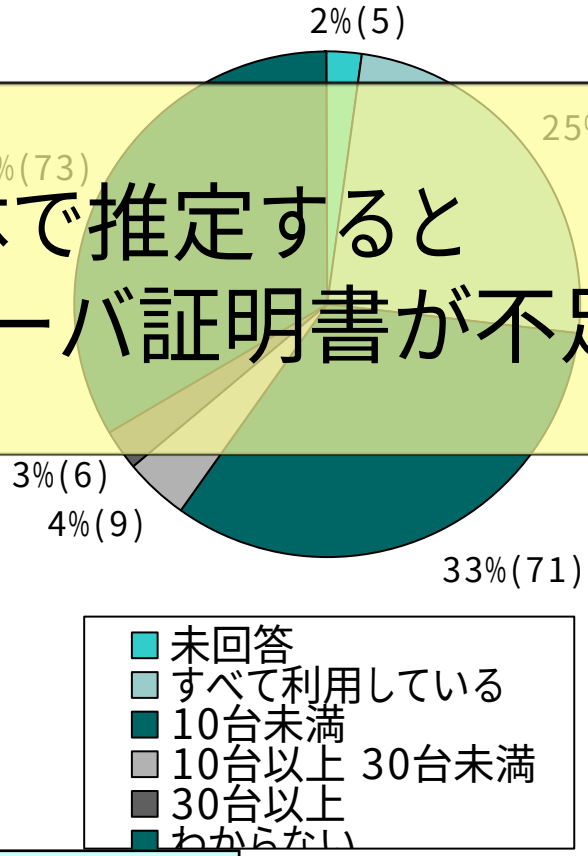
- **(1)ガイドライン利用の手引き**
- **(2)キャンパス PKI 調達仕様ガイドライン**
  - ①キャンパス PKI調達仕様ガイドライン編
  - ②キャンパス PKI調達仕様テンプレート編
- **(3)キャンパス PKI CP/CPSガイドライン**
  - ①キャンパス PKI CP/CPSガイドライン編
  - ②キャンパス PKI CP/CPSテンプレート編

大学等におけるサーバ証明書の実態

証明書の利用状況
(未回答･わからないを除く)



証明書を利用できていない台数

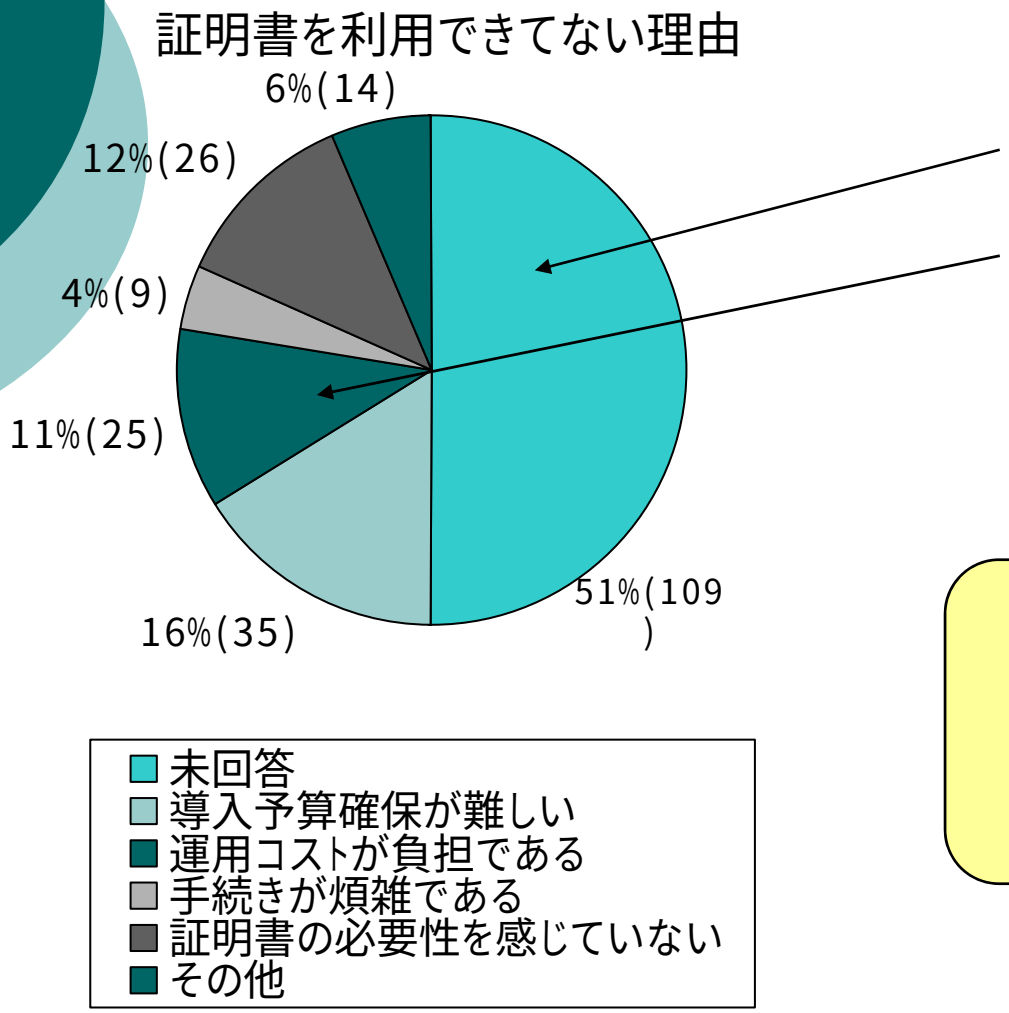


SINET加入機関全体で推定すると
2,300～3,500台分のサーバ証明書が不足

H18年度「大学等における電子証明書の利用状況に関する実態調査」より

対象: SINET加入機関818件、うち有効回答218件

普及が進まない理由



- **理由がわからない!!**
- **運用コストの負担**
  - **実際に生じる負担は?**

実際に使ってもらって
確認してはどうか?

サーバ証明書発行･導入における啓発･評価研究プロジェクト

認証局を用いた評価研究

体験を通じて啓発

- **目的**
  - **大学等のサーバ証明書の普及を推進**
  - **認証局を用いた研究開発 ⇒ 登録発行業務の改善**
  - **学術機関のWebサーバ信頼性向上**
  - **サーバ証明書の導入･運用ノウハウの共有**
  - **参加者のサーバに対してのサーバ証明書無償配布**
- **期間**
  - 2007/04/01～2009/03/31

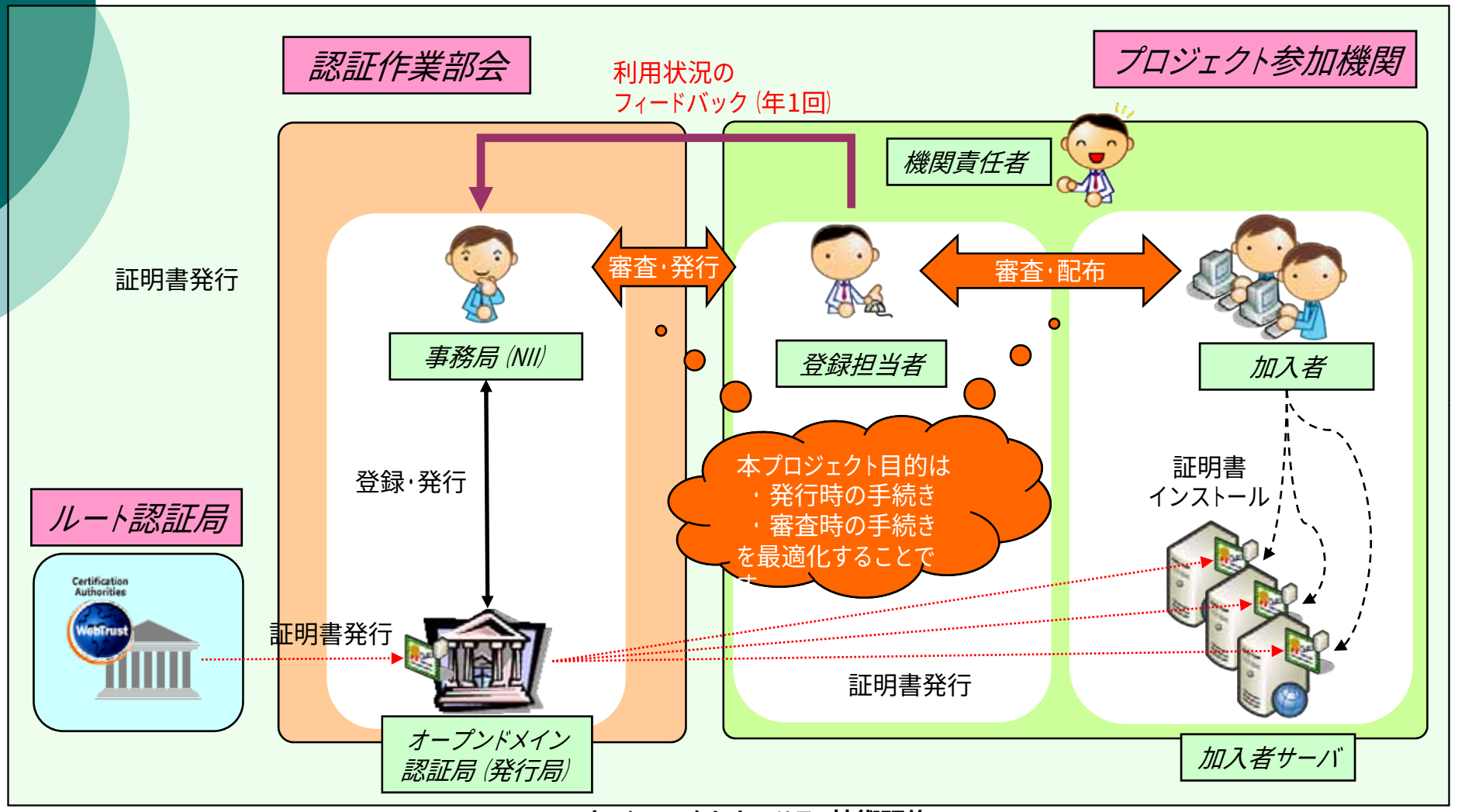
2010/06/30**まで有効**

- **ゴール**
  - H19年度: **サーバ証明書の普及が進まない理由･課題の整理**
  - H20年度: **サーバ証明書の普及促進の仮説･立証**
  - **将来的に: キャンパスPKI層を活用した証明書発行業務の自動化**
- **主な作業**
  - **プロジェクト参加機関の募集**
  - **各登録担当者へのS/MIME証明書発行**
  - **参加機関が管理するサーバに対するサーバ証明書の発行**
  - **参加機関加入者によるサーバ証明書の導入･運用**
  - **発行手続、導入手順などに対する改善案･Tipsのフィードバック、整理･公開**

証明書発行の基本方針

- 用語の定義
  - 本人性確認：なりすましや否認を防止するために本人意思を確認する作業
  - 実在性確認：証明書に記載する組織に実在することを確認する作業
- 審査項目の分担による発行業務の最適化
  - その審査を一番手早く実現できるのは誰か?
  - 認証局が最低限責任を負うべき項目は?
- 商用サービスと同等の保証レベル
  - 機関の実在性認証まで含めた審査項目→分担して実現

プロジェクト概念図


認証作業部会
利用状況の
フィードバック（年1回）
プロジェクト参加機関
機関責任者
証明書発行
審査・発行
審査・配布
事務局（NII）
登録担当者
加入者
登録・発行
本プロジェクト目的は
・発行時の手続き
・審査時の手続き
を最適化することで
証明書
インストール
ルート認証局
Certification Authorities
WebTrust
証明書発行
証明書発行
オープンドメイン
認証局（発行局）
加入者サーバ

商用証明書との比較
～審査項目の違い～

機関側の審査項目は確認手順調査表でチェック

審査者 / 審査項目		商用サービス				本プロジェクト			
		オンライン認証		機関認証					
		登録局	利用者	登録局	利用者	登録局	機関責任者	登録担当者	利用者
機関	本人性確認	×		○					
	実在性確認	×		○		○			
ドメイン	本人性確認	○		○		× →	○		
	実在性確認	○		○		○			
機関責任者	本人性確認					○			
	実在性確認					○			
登録担当者	本人性確認					○			
	実在性確認					× →	○		
加入者	本人性確認	×		○		× →		○	
	実在性確認	×		○		× →		○	
加入者サーバ	本人性確認		○		○				○
	管理責任確認		○		○			○ ←	×

「認証方法の違いによる役割と活用場面（企業の実在性認証とオンライン認証）」より
http://www.verisign.co.jp/server/first/difference.html

無線LANにおける個人認証方式

- 802.1x
  - **パスワード認証**
    - EAP-TTLS, EAP-PEAP
  - PKI**認証**
    - EAP-TLS
- RADIUS**サーバ間で認証連携させる**
  - EduRoam
    - **世界規模の大学間認証連携**
    - http://www.eduroam.jp/

(参考) IEEE802.1Xの認証プロトコル

- EAP (Extensible Authentication Protocol)の種類

方式	クライアント認証方式	サーバ認証方式	セキュリティレベル	運用工数
EAP-TLS	証明書	証明書	高	高
EAP-TTLS	ID/パスワード	証明書	中	中
EAP-PEAP	ID/パスワード	証明書	中	中
LEAP	ID/パスワード	ID/パスワード	低	低
EAP-MD5	ID/パスワード	無し	低	低

EduRoamとは

- ヨーロッパを中心とした学術組織による無線LANローミング方式
  - ヨーロッパのデファクトスタンダード
  - オーストラリア、香港、台湾なども参加
- 参加組織に所属する利用者は、他の参加組織で無線LANローミングを利用可能
- 国立情報学研究所(NII)を中心に国立七大学等で導入作業中

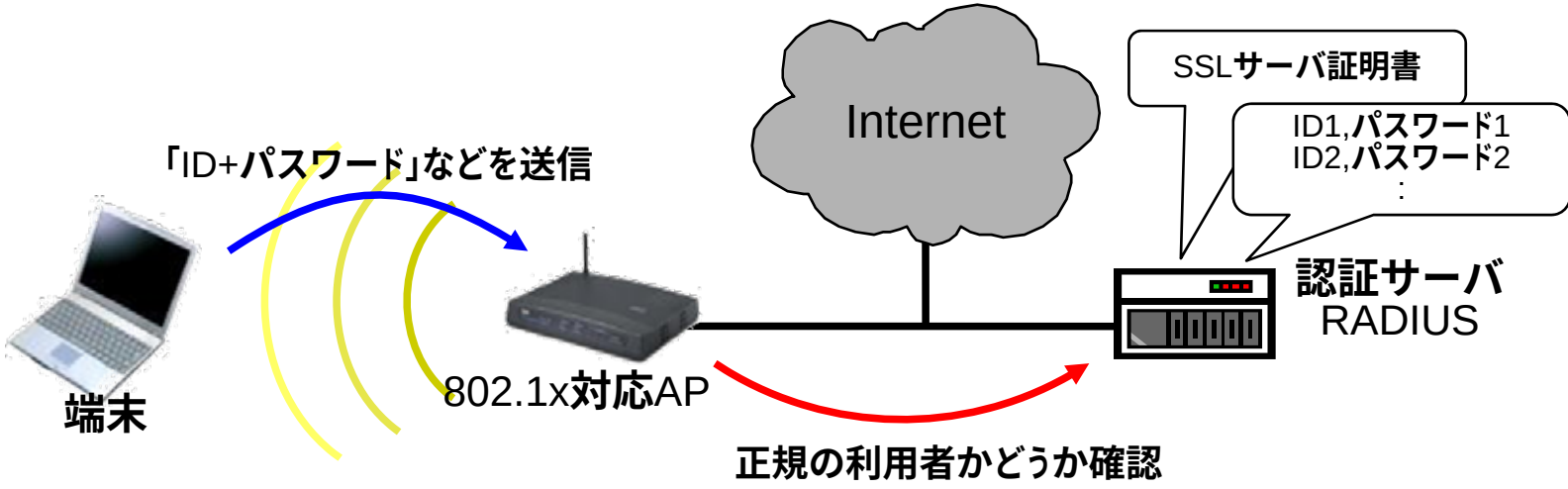
EduRoamに参加している国

http://www.eduroam.org/ より引用

EduRoamの仕組み(1/2)

IEEE 802.1x を利用

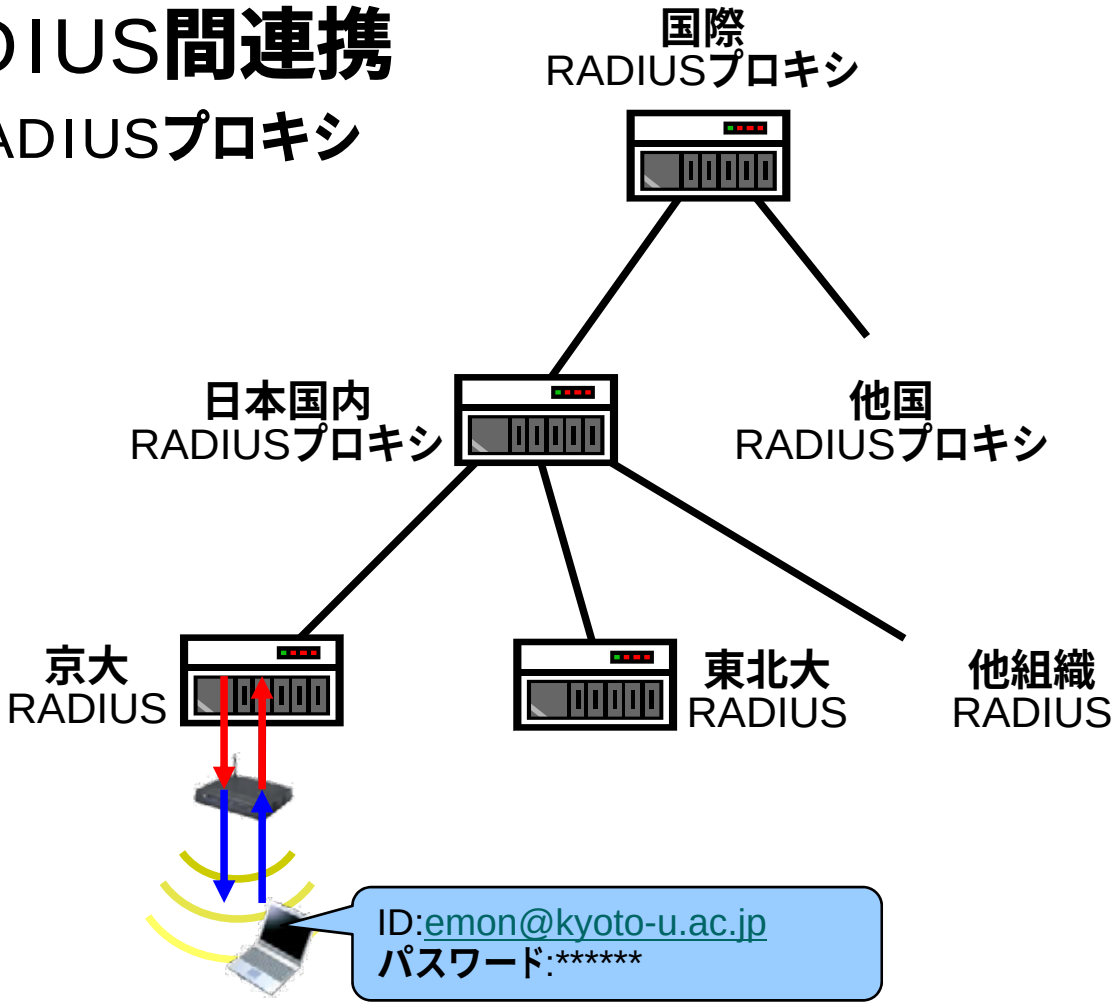
- **無線アクセスポイント(AP)やLANスイッチで ユーザを認証するための仕組み**
- **「ID＋パスワード」や「SSLクライアント証明書」で 端末を認証**
- **認証サーバとしてRADIUSを利用**



EduRoamの仕組み(2/2)

RADIUS間連携

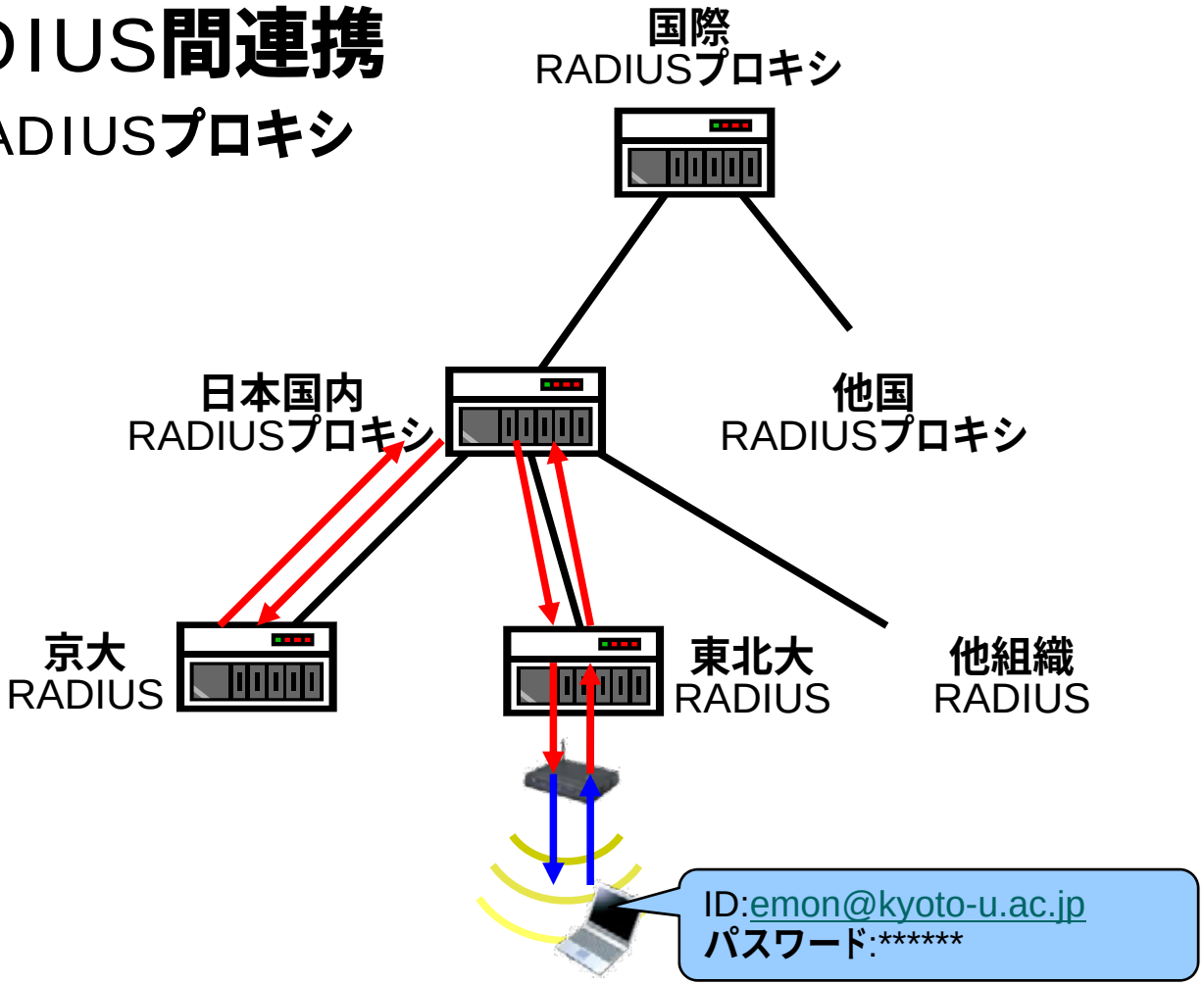
- RADIUSプロキシ



EduRoamの仕組み(2/2)

RADIUS間連携

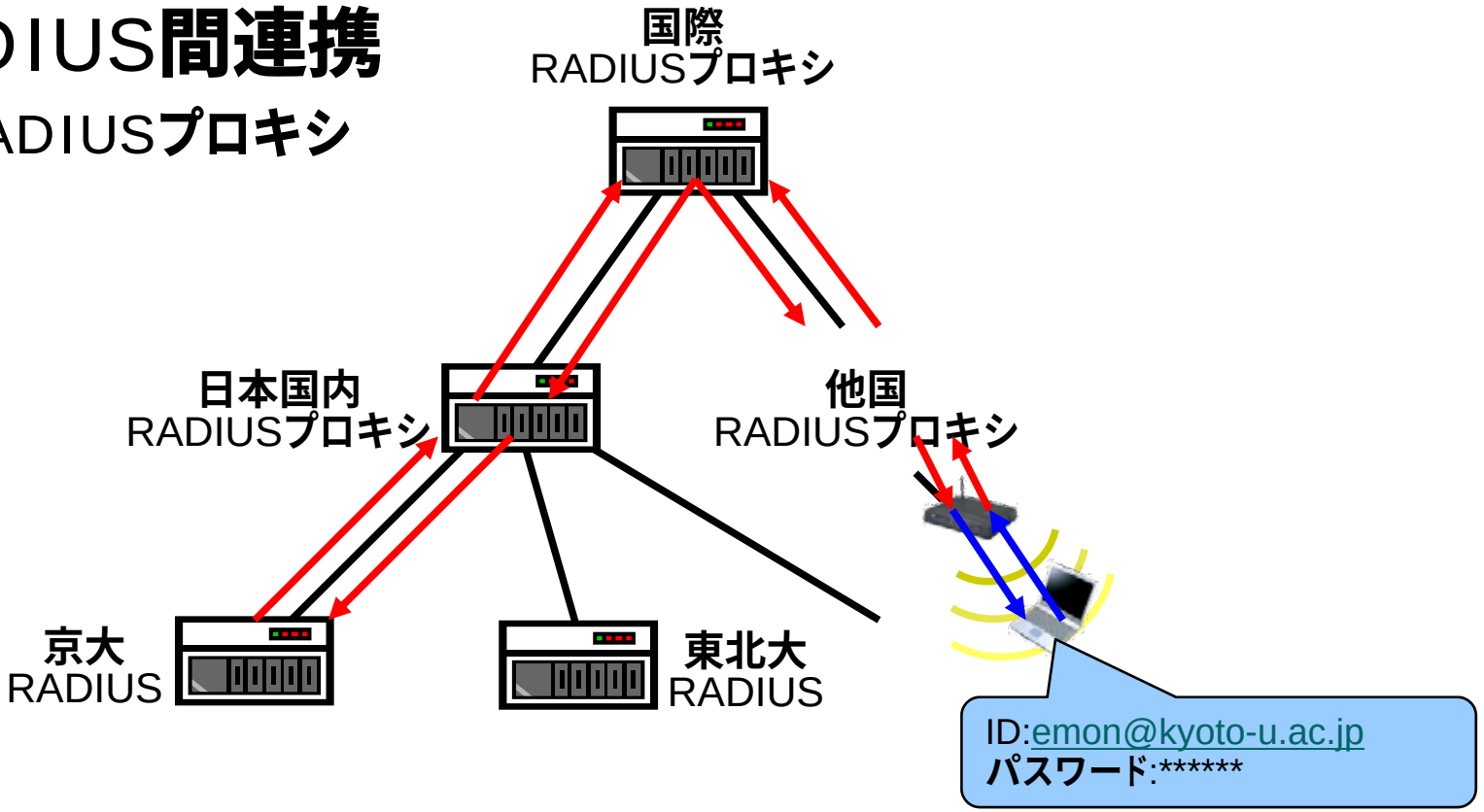
- RADIUSプロキシ



EduRoamの仕組み(2/2)

RADIUS間連携

- RADIUSプロキシ



統合認証基盤導入の背景

- 大学における様々な処理の電子化
  - 教育用計算機システム（学生用）
  - 大型計算機（スパコン）システム（研究者用）
  - 図書館データベース（ＯＰＡＣ等）
  - 人事システム（給与）
  - 会計システム（予算・発注・支払）
  - 事務（教職員）用グループウェア（文書共有）
  - 事務用メールシステム
  - 教務システム（学籍、成績）
  - 講義情報（シラバス、休講情報、履修登録）
  - E-ラーニングシステム
  - 研究者総覧データベース
  - Webポータルサービス
  - キャンパスネットワーク管理システム
  - 入退室管理システム
  - ：

本当に効率化されているのか？？

問題の要因

- 導入に際して連携が行われない
  - 組織が大きい
  - 部局自治の尊重
  - 担当部署の違い
  - 入札による調達
    - 独立した仕様
    - 特定業者に依存しない
- 歴史的経緯
  - 旧システムからの連続性
- 属性に依存したID
  - 進学、転学部、就職でIDがかわる
  - 例外がたくさん

非効率なだけで済むのか？

- どんなシステムもIDとパスワードが必要
- IDやパスワードがシステムごとに異なる
  - パスワードの変更が面倒
  - 覚えきれないので書き留める
  - 様々な形態でパスワードがネットワークを流れる
  - 同じパスワードの長期間利用
    - パスワードの流出
      - 個人情報の流出
    - システムごとに窓口が異なる
      - 手続きのためにあちこちに行かなければならない
- IDカードの種類が多くなる

統合IDにすると

- 利便性の向上
  - 一組だけ覚えればOK
    - 複雑なパスワードの利用が期待できる
    - 定期的なパスワード変更が期待できる
  - システムごとにログイン処理が不要(SSO)
- コスト削減
  - システムごとのID管理のコスト
    - 発行、削除、パスワード変更、紛失対応
    - 初期パスワード配布問題
      - 大きな大学では数万人規模
  - 業務、窓口が一元化できる
    - ワンストップサービス
  - 新たなシステムの導入が容易

どこがこの業務を引き受けるのか？

統合認証基盤整備の際の検討事項

- ID**設計**
- **シングルサインオン化**
- PKI:**公開鍵認証基盤**
  - Public Key Infrastructure

認証と承認

- **認証**: Authentication
  - **その人が誰かを確認すること、本人確認**
- **承認**: Authorization
  - **その人に利用する権限を与えること、認可**

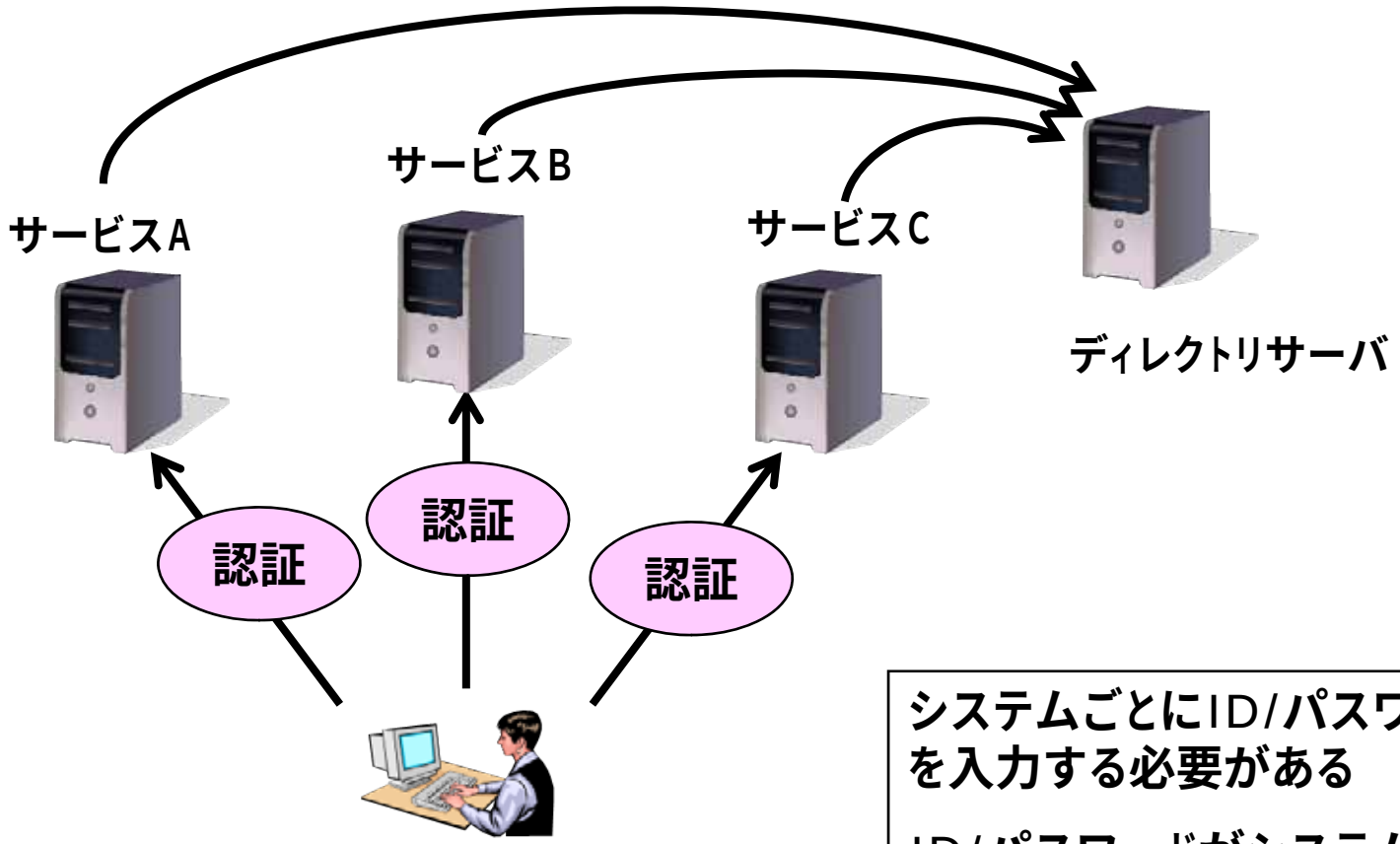
統合認証基盤では、区別して考える

- **他に以下を含めて**AAA, 4A**等と呼ばれる**
  - Accounting (**課金**)
  - Administration (**アクセス、ユーザ、PW管理**)
  - Auditing (**監査ログ収集**)

シングルサインオン (SSO: Single Sign-On)

- 一度だけ認証を受けることで複数のアプリケーションが利用可能になる仕組み
  - 統合IDにするだけでは効果が薄い
- 実現方式
  - ライブラリ型
  - エージェント型
  - リバースプロキシ型

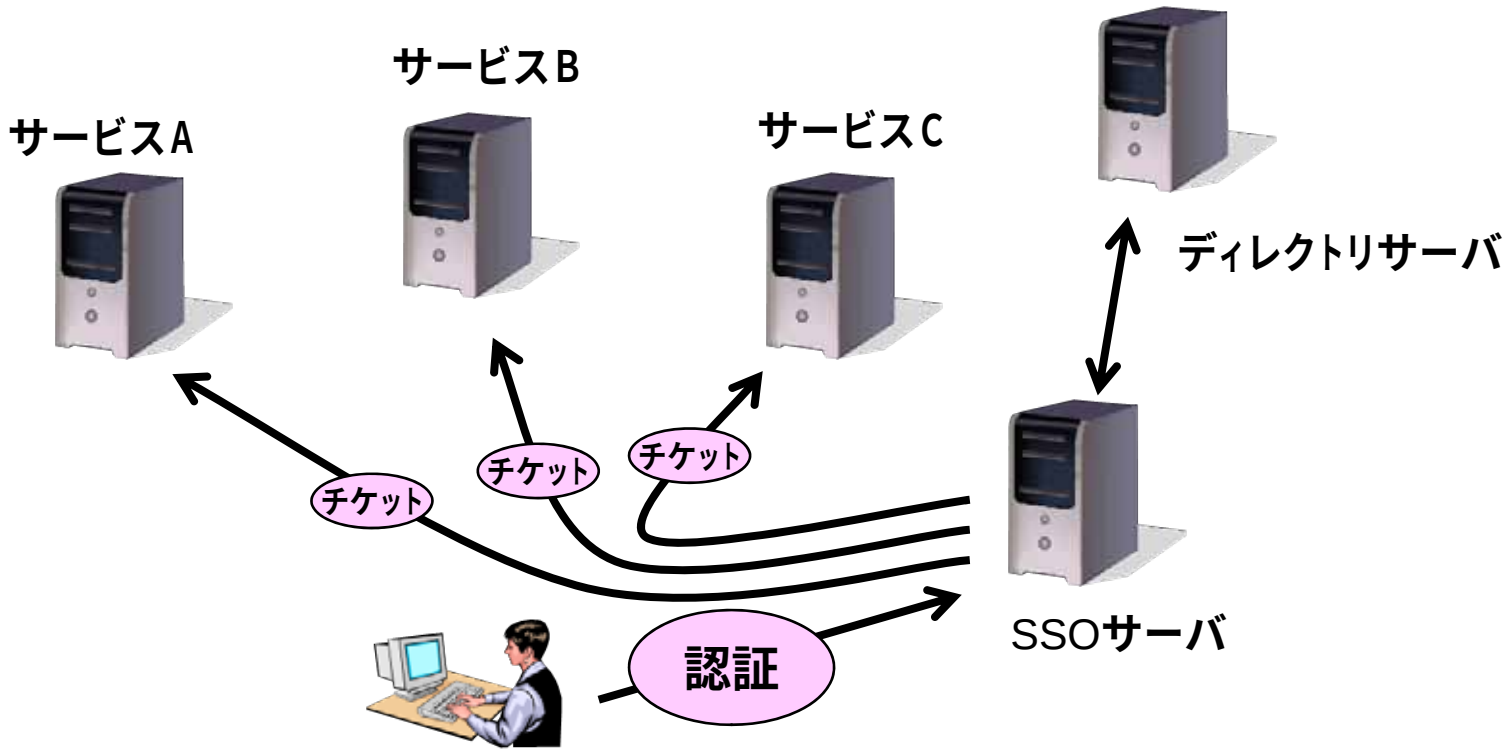
従来のアクセス方法



システムごとにID/パスワードを入力する必要がある

ID/パスワードがシステム毎に何度も流れる

SSOを導入すると



SSO移行時の検討

- セキュリティの脆弱化はないか？
  - フィッシング
  - チケットの横取りと再利用
- 利便性は低下しないか？
  - セキュアになるほど面倒になる
- 複数の認証方式に対応させることも可能
  - 認証を受けた方式に応じて
    利用可能範囲を変える、とか

Shibboleth

- **米国**EDUCAUSE／Internet2**にて**2000**年に発足したプロジェクト**
- SAML、eduPerson**等の標準仕様を利用し、認可のための属性交換を行う**
- **個人情報保護への考慮**
- **フェデレーション構築への活用**

シングルサインオン(SSO)実証実験

- 各大学の利用者にとって安全･安心かつ有効に学術サービスが利用できる基盤の実証と検討

- Shibbolethを用いたIdP，SPの構築
- シングルサインオン環境の実現
- フェデレーションの構築

https://upki-portal.nii.ac.jp/SSO

フェデレーション

- あるルール（ポリシー）のもとで属性交換の相互運用に合意した組織（IdP、SP）の集合
- 世界のIdP
  - 米国：InCommon, 英国：The UK Access Management Federation, フランス：CRU, ノルウェイ：FEIDE, フィンランド：HAKA, スイス： SWITCHaai, オーストラリア： MAMS、AAF など
- 世界のSP
  - ScienceDirect, Ovid Technologies, JSTOR, ExLibris, Digitalbrain, Thomson Gale など

UPKIイニシアティブ

- UPKIの相互運用性，利用促進に関しての意見交換や技術的な検証を行う場として設立（2006年8月16日）
- UPKIイニシアティブの活動は，主にホームページ上のUPKIポータルを使用

  https://upki-portal.nii.ac.jp/

まとめ

- PKIによる認証基盤
- 大学間認証連携 (UPKI)
  - サーバ証明書発行
  - 無線LANローミング
  - シングルサインオン
  - GRID

各大学での取り組み(1)

- **東北大学**
  - http://www2.he.tohoku.ac.jp/center/risyuu/pamphlet.pdf
- **東京大学**
  - http://www.pki.itc.u-tokyo.ac.jp/
- **東京工業大学**
  - http://portal.titech.ac.jp/
- **名古屋大学**
  - http://www.icts.nagoya-u.ac.jp/nuid/index.htm
- **京都大学**
  - https://upki-portal.nii.ac.jp/item/idata/odatao/csi20060517/CSIsession4.pdf/download
- **大阪大学**
  - http://repository.cmc.osaka-u.ac.jp/ja/index.html
- **九州大学**
  - http://www.slrc.kyushu-u.ac.jp/japanese/project/iccard/

各大学での取り組み(2)

- **筑波大学**
  - https://account.tsukuba.ac.jp/index.html
- **群馬大学**
  - http://account.media.gunma-u.ac.jp/
- **名古屋工業大学**
  - http://www.cc.nitech.ac.jp/news/20070324_01_i.html#pagetop
- **広島大学**
  - http://auth.hiroshima-u.ac.jp/
- **高知大学**
  - http://www.iic.kochi-u.ac.jp/ipc/system/ldap.htm
- **福岡大学**
  - http://www.ipc.fukuoka-u.ac.jp/service/index.html#ninsho

- **文部科学省**
  - https://shinsei-cert.mext.go.jp/guide/ninsyo/index.html
- **政府認証基盤**(GPKI)
  - http://www.gpki.go.jp/documents/gpki.html