サイエンティフィックシステム研究会
システム技術分科会2008年度第2回会合
「組織と認証　～誰を認証すべきか～」

私は誰？
組織、そしてサービスからみた認証とUPKI

岡部 寿男

（京都大学 学術情報メディアセンター）

平成21年1月29日（木）

あらまし

- 組織における認証・認可の課題を、大学における認証システムの構築に絡めて考察する。

1. 「誰を認証すべきか」の視点から、大学が情報システムの利用者として扱う必要のある対象を分類し、それぞれに対するアカウント発行時の身元確認や失効の手順について、セキュリティポリシーとからめて概説する。
2. NIIによるSSLサーバ証明書発行プロジェクトを例に、サーバの認証について紹介する
3. 「私は誰？」、すなわち利用者がどういう立場で情報システムを扱おうとしているかの観点から、認証と権限管理の分離の必要性について述べ、京都大学における統合認証システムの運用の状況と権限委譲の試みについて紹介する。
4. 組織をまたがる認証としてUPKI認証連携基盤の取り組みについて述べ、組織間の認証連携（federation）の仕組みと、「私は誰？」かどこまで明らかにしてよいかなど組織間のプライバシー保護の課題についても考察する。

（１）誰を認証すべきか
～アカウント管理の課題～

そもそも「認証」とは（1）

『政府機関の情報セキュリティ対策のための統一基準』の定義

「**主体**」
- 情報システムにアクセスする者や、他の情報システム及び装置等をいう。主体は、主として、人である場合を想定しているが、複数の情報システムや装置が連動して動作する場合には、情報システムにアクセスする主体として、他の情報システムや装置も含めるものとする。

「**識別**」
- 情報システムにアクセスする**主体**を特定することをいう。

「**識別コード**」
- **主体**を**識別**するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザID が挙げられる。

「**主体認証**」（認証）
- 識別コードを提示した**主体**が、その識別コードを付与された**主体**、すなわち正当な**主体**であるか否かを検証することをいう。識別コードとともに正しい方法で**主体認証情報**が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した**主体**を正当な**主体**として認識する。なお、「認証」という用語は、公的又は第三者が証明するという意味を持つが、本統一基準における「**主体認証**」については、公的又は第三者による証明に限るものではない。

「**主体認証情報**」
- **主体認証**をするために、**主体**が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。

そもそも「認証」とは（2）

「ログイン」
- 何らかの**主体**が**主体認証**を要求する行為をいう。ログインの後に**主体認証**が行われるため、ログインの段階ではその**主体**が正当であるとは限らない。

「ログオン」
- **ログイン**の結果により、**主体認証**を要求した**主体**が正当であることが情報システムに確認された状態をいう。

「**複数要素**（複合）**主体認証**（multiple factors authentication/composite authentication）**方式**」
- 知識、所有、生体情報などのうち、複数の方法の組合せにより**主体認証**を行う方法である。

「**主体認証情報格納装置**」
- **主体認証情報**を格納した装置であり、正当な**主体**に所有又は保持させる装置をいう。所有による**主体認証**では、これを所有していることで、情報システムはその**主体**を正当な**主体**として認識する。代表的な主体認証情報格納装置として、磁気ストライプカードやICカード等がある。

「**アクセス制御**」
- 主体によるアクセスを許可する客体を制限することをいう。

「**権限管理**」（認可）
- 主体認証に係る情報（識別コード及び主体認証情報を含む）及びアクセス制御における許可情報を管理することをいう。

そもそも「認証」とは（3）

『識別コードを提示した主体が識別コードを付与された主体か否かを検証』

すなわち認証の問題とは

- 誰に識別コード（ユーザID）を付与するか？
  - 「誰を認証すべきか？」
- どのように識別コードと主体認証情報（パスワード，ICカード）を付与するか？
  - 「どうやって認証するか？」
- どのように提示した主体が本物かを検証するか？
  （ここはある程度機械的に処理できる）

セキュリティポリシー上の規定

高等教育機関の情報セキュリティ対策のためのサンプル規程集

国立情報学研究所 国立大学法人等における情報セキュリティポリシー策定作業部会

電子情報通信学会 ネットワーク運用ガイドライン検討WG

http://www.nii.ac.jp/csi/sp/

- 仮想国立A大学におけるセキュリティポリシー
  - 文学部と理学部の2学部で構成され、両学部とも在学生が1,000 人(1学年250 名)ずつ
  - 学内共同利用施設として情報メディアセンターと図書館
  - 学内ネットワークや学内共同利用の情報システムは情報メディアセンターの担当
- 政府機関統一基準に準拠

サンプル規程集の構成

赤字は2007年度の追加・改称文書，§は策定手引書
(*) UPKI共通仕様を参照，(**) 各大学にて策定することを想定

ポリシー	実施規程	手順等
A1000 情報システム運用基本方針 A1001 情報システム運用規程	A2101 情報システム運用・管理規程 A2102 情報システム運用リスク管理規程 A2103 情報システム非常時行動計画に関する規程 A2104 情報格付け規程	A3100 情報システム運用・管理手順の策定に関する解説書 A3101 情報システムにおける情報セキュリティ対策実施規程§ A3102 例外措置手順書； A3103 インシデント対応手順 A3104 情報格付け取扱手順； A3105 情報システム運用リスク評価手順 A3106 セキュリティホール対策計画に関する様式§ A3107 ウェブサーバ設定確認実施手順§ A3108 メールサーバのセキュリティ維持手順§ A3109 人事異動の際に行うべき情報セキュリティ対策実施規程 A3110 機器等の購入における情報セキュリティ対策実施規程§ A3111 外部委託における情報セキュリティ対策実施手順 A3112 ソフトウェア開発における情報セキュリティ対策実施手順§ A3113 外部委託における情報セキュリティ対策に関する評価手順 A3114 情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書(*) A3115 情報システムの構築等におけるST 評価・ST 確認の実施に関する解説書(*)
	A2201 情報システム利用規程	A3200 情報システム利用者向け文書の策定に関する解説書 A3201 PC取扱いガイドライン A3202 電子メール利用ガイドライン； A3203 ウェブブラウザ利用ガイドライン A3204 ウェブ公開ガイドライン； A3205 利用者パスワードガイドライン A3211 学外情報セキュリティ水準低下防止手順 A3212 自己点検の考え方と実務への準備に関する解説書
	A2301 年度講習計画	A3300 教育テキストの策定に関する解説書 A3301 教育テキスト作成ガイドライン(利用者向け) A3302 (部局管理者向け)； A3303 (CIO/役職者向け)
	A2401 情報セキュリティ監査規程	A3401 情報セキュリティ監査実施手順
	A2501 事務情報セキュリティ対策基準	A3500 各種マニュアル類の策定に関する解説書； A3501 各種マニュアル類(**) A3502 責任者等の役割から見た遵守事項
	A2601 証明書ポリシー(*) A2602 認証実施規程(*)	A3600 認証手順の策定に関する解説書 A3601 情報システムアカウント取得手順

誰を認証すべきか？(1)

A1001 情報システム運用基本規程
A1001-03（定義）

- 第三条 本基本規程において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。
- 八 利用者
  - 教職員等及び学生等で、本学情報システムを利用する許可を受けて利用するものをいう。
- 九 教職員等
  - 本学に勤務する常勤又は非常勤の教職員（派遣職員を含む）その他、部局総括責任者が認めた者をいう。
- 十 学生等
  - 本学通則に定める学部学生、大学院学生、研究生、研究員、研修員並びに研究者等、その他、部局総括責任者が認めた者をいう。
- 十一 臨時利用者
  - 教職員等及び学生等以外の者で、本学情報システムを臨時に利用する許可を受けて利用するものをいう。

誰を認証すべきか？(2)

- 大学で正規の身分を持つ人
  - 教職員（就業規則に基づき大学に雇用されている）
    - 常勤（いわゆる定員内）
      - 任期なし／任期付き
    - 特定有期雇用職員：年俸制
      - 外部資金による特任教員
    - 有期雇用職員（日給制）
    - 時間雇用職員（時給制）
      - 事務補佐員（秘書業務）など（週最大30時間）
      - 非常勤講師…年1回だけの講義担当者まで入れれば常勤職員より多い
      - RA, TAなどの学生としての身分を併せ持つケースも

    非正規雇用
  - 学生等
    - 学部学生、大学院学生、外国学生、委託生、科目等履修生、聴講生、特別聴講学生、特別研究学生など（大学通則に基づく）
    - 研究生（研究生規程に基づく）
    - 研究員、研修員など（研修規程に基づく）
      - 内地研究員（内地留学制度による他大学教員）、教育研究期機関研究員など
      - 日本学術振興会特別研究員（ポスドク）
    - 民間等共同研究員
    - 招へい外国人学者，外国人共同研究者［雇用関係なし］

誰を認証すべきか？(3)

- 大学との契約に基づき居る人
  - 派遣職員
  - 委託業務従事者
    - 生協職員も?
  - 文部科学省共済組合職員
  - 職員組合専従職員
  - 産学連携施設入居者
    - 大学内に制度的に整備された施設で研究を行う、大学外の身分の研究者等
  - 大学関係組織(同窓会，TLO，地域交流センター，財団，…)
- 以前大学に籍のあった人
  - 名誉教授(称号であって身分ではない)
  - 卒業生
  - 元教員、元学生
- 正式の契約はないが研究室レベルで認めて大学に居る人
  - 短期の訪問客
  - 企業からの派遣者、外部資金での雇用者

c.f. 客員教授
（称号であって身分は他にある）

誰を認証すべきか？(4)

- 臨時利用者（大学の情報システムを臨時に許可を受けて利用する人）

〔例〕

  - 全国共同利用スーパーコンピュータの利用者
  - 無線LANを利用する来訪者
  - 専用サイトにアクセスする研究グループのメンバー
- 注意
  - 物理的に大学に居るとは限らない
  - 教育研究機関関係者とは限らない
  - どこの誰か認証できているとは限らない

どうやって認証するか？(1)

A2101 情報システム運用・管理規程
A2101-47（アカウント管理手続の整備）
第四十七条 部局技術責任者は、アカウント管理を行う必要があると認めた情報システムにおいて、アカウント管理について、以下の事項を含む手続を明確にすること。
- 一 主体からの申請に基づいてアカウント管理を行う場合には、その申請者が正当な主体であることを確認するための手続
- 二 主体認証情報（パスワード）の初期配布方法及び変更管理手続
- 三 アクセス制御情報の設定方法及び変更管理手続

A2101-49（アカウントの発行）
第四十九条
2 アカウント管理を行う者は、アカウント管理を行う必要があると認めた情報システムにおいて、情報システムを利用する許可を得た主体に対してのみ、アカウントを発行すること。
3 アカウント管理を行う者は、アカウントを発行するにあたっては、期限付きの仮パスワードを発行する等の措置を講じることが望ましい。

A2101-51（アカウントの有効性検証）
第五十一条 アカウント管理を行う者は、発行済のアカウントについて、次号に掲げる項目を一か月毎に確認すること。
- 一 利用資格を失ったもの
- 二 部局総括責任者が指定する削除保留期限を過ぎたもの
- 三 パスワード手順に違反したパスワードが設定されているもの
- 四 六か月以上使用されていないもの

2 アカウント管理を行う者は、人事異動等、アカウントを追加又は削除する時に、不適切なアクセス制御設定の有無を点検すること。

どうやって認証するか？(2)

- 実在性の確認
  - 職員：人事簿
    - 常勤職員:OK
    - 非常勤職員：？？
  - 学生：学籍簿
    - ？？
  - それ以外
    - リクエストベースでのアカウント発行は可能だが、失効処理が難しい
- 認証方式の検討
  - パスワード？
  - ICカード？
  - バイオメトリック？
- 本人性の確認
  （原則）写真付き身分証で手渡し確認
    - 職員：職員証
    - 学生：学生証
  - それはどうやって配ったの？
  - 身分証に写真がない人は？
  - 遠隔地は？

  学内事務手続きや学内便がどれくらい信用できるか？

サービスによっては対面認証が義務付けられることがある

どうやって認証するか？(3)

A3600 認証手順の策定に関する解説書

- A大学では、
  - アカウントの発行に際しては原則として写真付身分証による対面での本人確認を義務付け。
  - 学生については全学アカウントの発行に際して講習会の受講を義務付け。
  - 学生・教職員以外の者の申請に当たっては、関係部局長(来学中に利用する訪問者などの臨時利用者を受け入れた部局の長など)名での受入証明書の提出を要件。
- 実際の運用にあたっては以下のような点についても検討が必要。
  - 医学部、歯学部、獣医学部、薬学部のような6 年制の学部の学生に対して、卒業まで6 年間有効のアカウントを発行してよいか、他の学部と合わせて4 年＋2 年の更新とするか。博士課程5年一貫教育の場合も同様。
  - 名誉教授に対するアカウントを発行するか、年度ごとの更新処理は必要か。
  - 卒業生に対するアカウントを発行するか、有効期限の設定、利用者との契約をどうするか
  - 本人死亡に伴うアカウント失効処理手順をどうするか。
    - 知財の継承のほか労災の認定などにおいてもデータの保全が求められることがある。

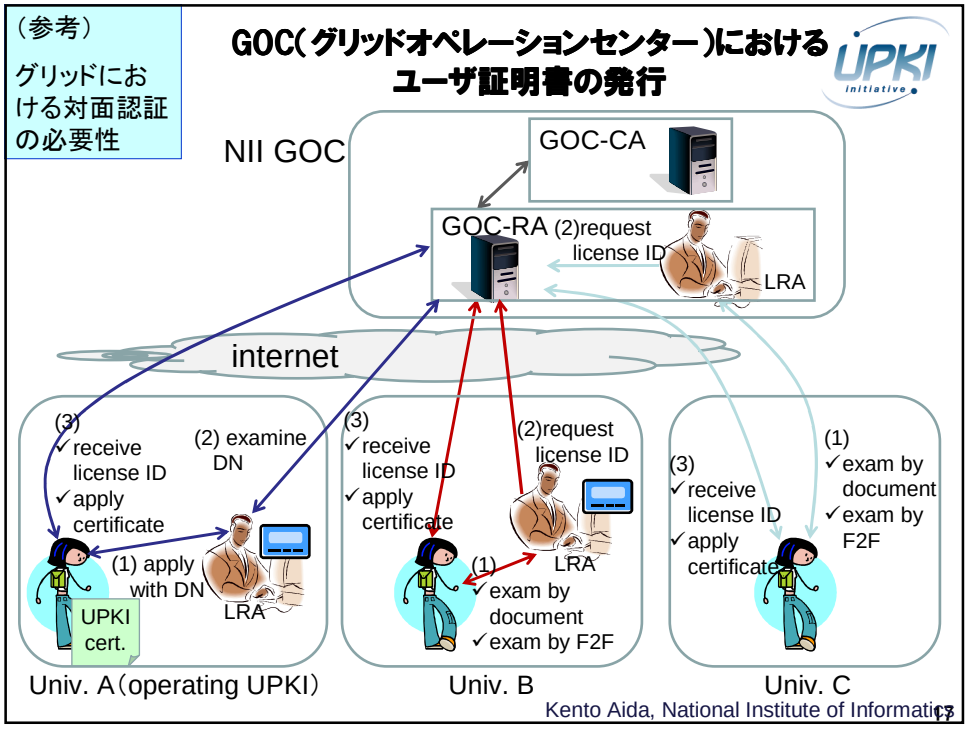
A大学情報システム全学アカウント交付申請区分　　20XX年度版

区分：A大学情報システム運用基本規程 A1001-03（定義）の定めによる。

	身分			講習会受講	更新手続き	備考
一 学生等	学部学生 大学院学生	学生証 （学生部発行・顔写真あり）	「学生証」「職員証」等の大学発行の身分証を提示、顔写真付のものについては対面にて確認	必要	必要 （身分変更が生じた年度のみ）	10月入学生については所定の年限の9月末で失効
	研究生 研究員 研修員 研究者 他	学生証 （部局発行・顔写真なし）			必要 （毎年度）	アカウントの有効期限は身分証の有効期限と年度末の早い方まで
二 教職員等	常勤教職員 特定有期雇用教職員	職員証 （人事部発行・顔写真あり）				着任早々で身分証を未取得の場合は「人事異動通知書」の提示。身分証番号を所属人事又は総務担当より入手。さらに以下のいずれかの方法で顔写真を確認する。1）公的機関発行の顔写真付身分証の提示　2）1ヶ月以内に顔写真付職員証を持参して再確認
	時間雇用職員 有期雇用職員 事務補佐員 技術補佐員 他 外国人研究員 外国人教師 客員教員 招聘外国人学者 派遣職員 他	身分証（職員証等） （部局発行・顔写真なし）			必要 （毎年度）	着任早々で身分証を未取得の場合は「労働条件通知書」または「受入証明書」の提示。身分証番号を所属人事又は総務担当より入手。
三 臨時利用者	訪問者 受託業務従事者 他	身分証 （受入証明書に記載の所属機関発行）	受入部局長名で受入証明書等の提出	必要 （学生のみ）	必要 （毎年度）	個別に情報メディアセンター全学アカウント担当へ問い合わせる。

（参考）

グリッドにおける対面認証の必要性



（２） サーバの認証とSSLサーバ証明書

NIIによるサーバ証明書発行の基本方針

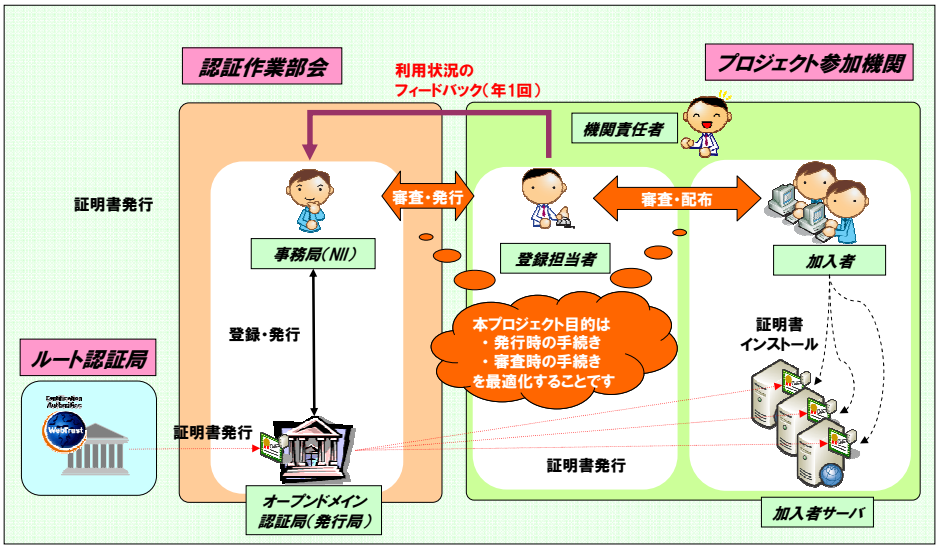
目的 サーバ証明書を安コストで提供(価格・人的コスト)

- 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申請者の本人意思を確認する作業
  - 実在性確認: 当該サーバが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

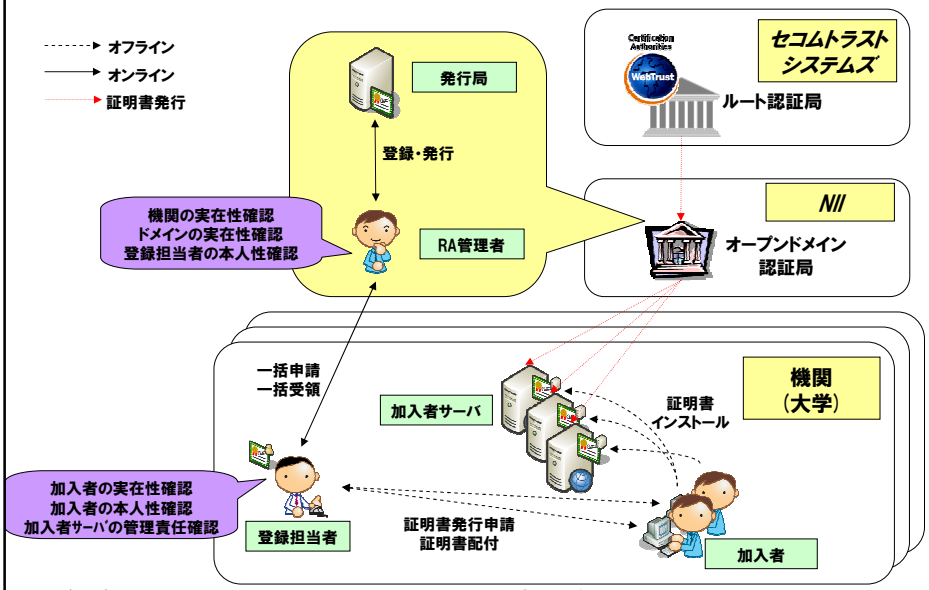
プロジェクト参加者の役割

組織	役割	説明
NII	発行局	認証局の鍵管理、サーバ証明書発行など セコムトラストシステムズへ運用委託
	事務局	プロジェクト参加申請、証明書発行申請にあたり、審査業務を行う
機関 (大学)	機関責任者 (1機関1名)	本プロジェクト参加にあたり、各機関で選出した代表者。 課長職相当または准教授以上
	登録担当者 (複数名可)	本プロジェクトの参加機関側の事務的な窓口。 大学の規模等に応じて複数名選出可。
	加入者	Webサーバを管理し、本プロジェクトのサーバ証明書を利用する。 機関に所属する教職員。
不特定多数	利用者	加入者サーバへアクセスし、その証明書を検証する。

プロジェクト概念図



証明書発行の流れ

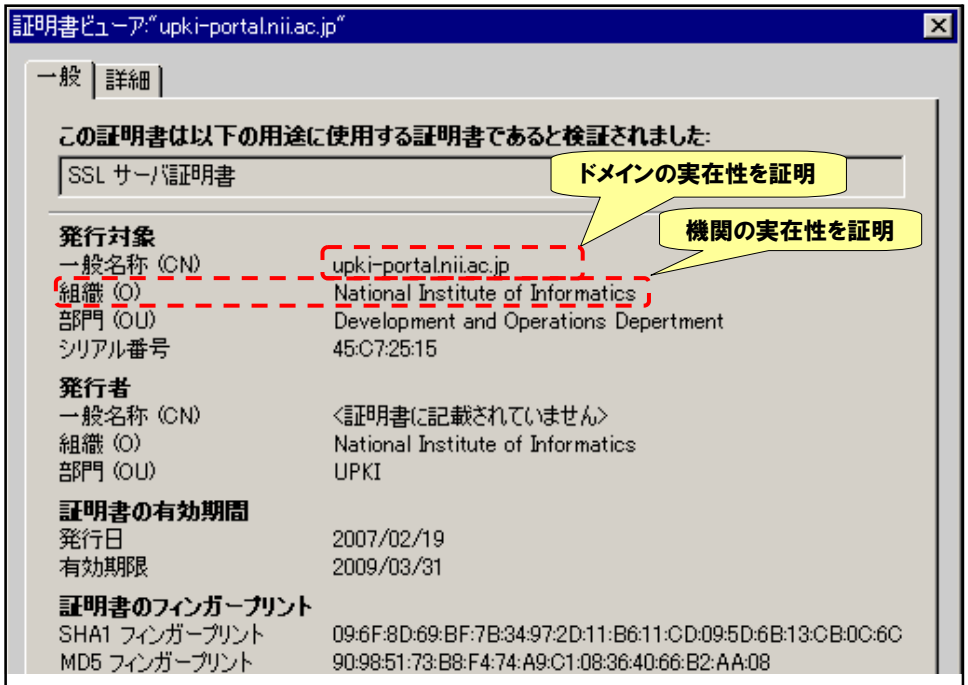


商用証明書との比較
～審査項目の違い～

機関側の審査項目は確認手順調査表でチェック

審査項目	審査者	商用サービス オンライン認証 登録局	商用サービス オンライン認証 利用者	商用サービス 機関認証 登録局	商用サービス 機関認証 利用者	本プロジェクト 登録局	本プロジェクト 機関責任者	本プロジェクト 登録担当者	本プロジェクト 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



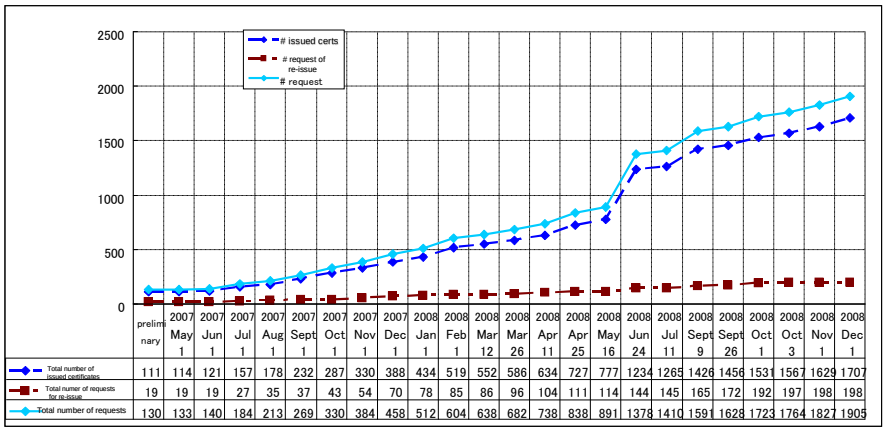
プロジェクトへの参加条件
サーバ証明書の発行条件

- 対象
  - SINET加入機関のうち、
    - 大学，短期大学，高等専門学校，大学共同利用機関
    - 独立行政法人，公益法人，大学共同利用機関法人，学校法人，地方独立行政法人
    - 本プロジェクト参加対象機関の長が設置する組織
  - 日本学術会議協力学術研究団体のうち、
    - 本プロジェクトが対象とするドメイン名を保有し部会が認めた団体
- 対象サーバ
  - 属する機関が所有または管理するサーバ
  - サーバ認証を必要とするサーバ
- ドメイン
  - 属する機関の主たるドメイン
    - 原則としてac.jpドメイン
    - プロジェクト参加申込時に指定

参加機関数	84機関
証明書発行枚数	1,700枚

〔H20.12月中旬時点での実績値〕

サーバ証明書発行数

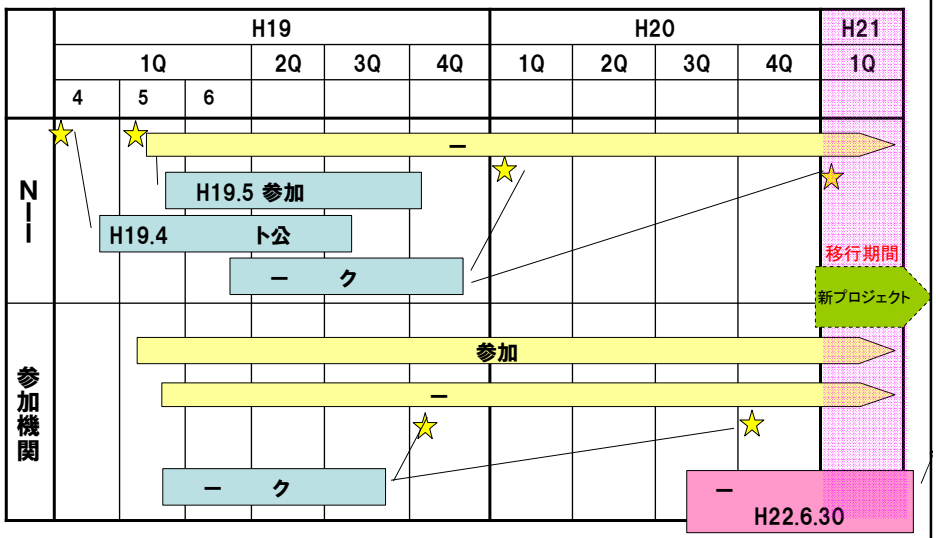


	preliminary	2007 May 1	2007 Jun 1	2007 Jul 1	2007 Aug 1	2007 Sept 1	2007 Oct 1	2007 Nov 1	2007 Dec 1	2008 Jan 1	2008 Feb 1	2008 Mar 12	2008 Mar 26	2008 Apr 11	2008 Apr 25	2008 May 16	2008 Jun 24	2008 Jul 11	2008 Sept 9	2008 Sept 26	2008 Oct 1	2008 Oct 3	2008 Nov 1	2008 Dec 1
Total number of issued certificates	111	114	121	157	178	232	287	330	388	434	519	552	586	634	727	777	1234	1265	1426	1456	1531	1567	1629	1707
Total numer of requests for re-issue	19	19	19	27	35	37	43	54	70	78	85	86	96	104	111	114	144	145	165	172	192	197	198	198
Total number of requests	130	133	140	184	213	269	330	384	458	512	604	638	682	738	838	891	1378	1410	1591	1628	1723	1764	1827	1905

プロジェクト参加機関内訳

	Total	国立大学	公立大学	私立大学	短大など	国立研究機関など	非機関プロジェクト
参加機関数	84	45	7	21	4	4	3
全機関数	N/A	87	76	582	460	N/A	N/A
Ratio (%)	N/A	51.7	9.2	3.6	0.9	N/A	N/A

プロジェクトスケジュール



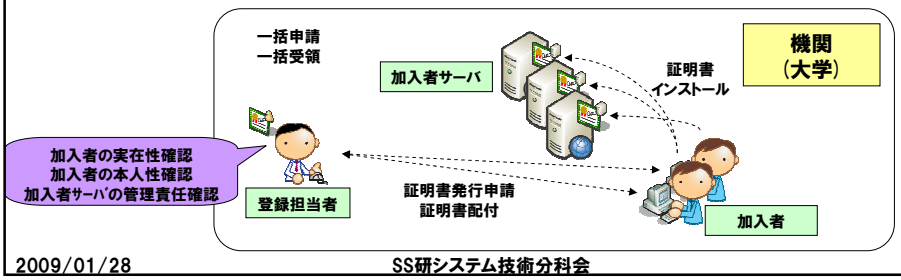
京都大学での実装例

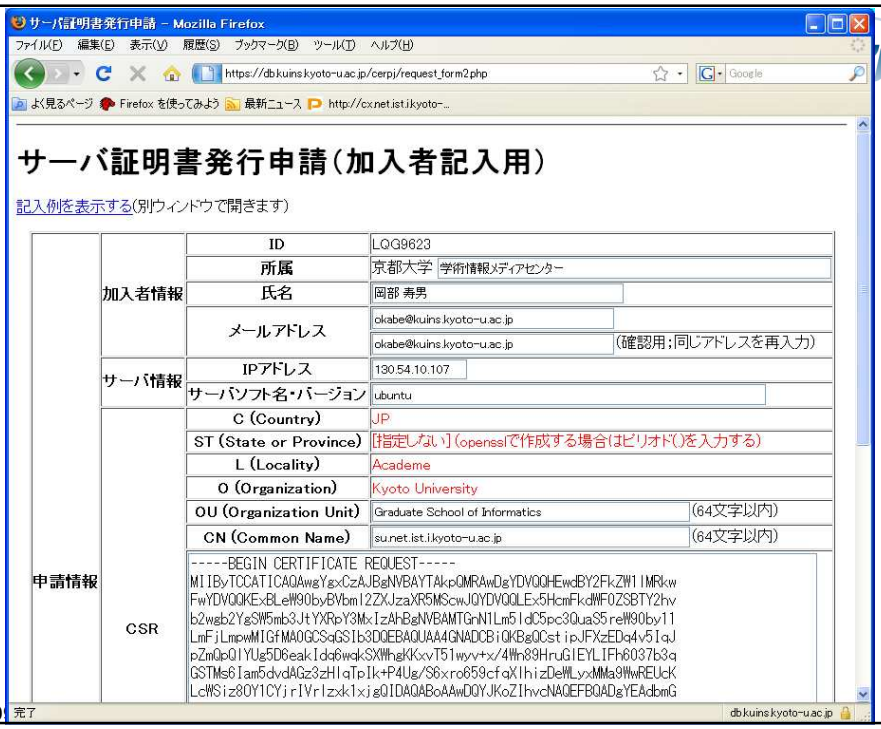
- 登録担当者の責務
  - 加入者の実在性確認
  - 加入者の本人性確認
  - 加入者が当該FQDNのサーバの管理責任を有するかの確認

サーバというモノをどのように認証するか？

- 京大ではKUINS（学内LAN）で負担金制
  - IPアドレスごとに管理責任者が一意に紐付け

⇒当該サーバの管理責任者によるオンライン申請で実在性・本人性・管理責任を確認





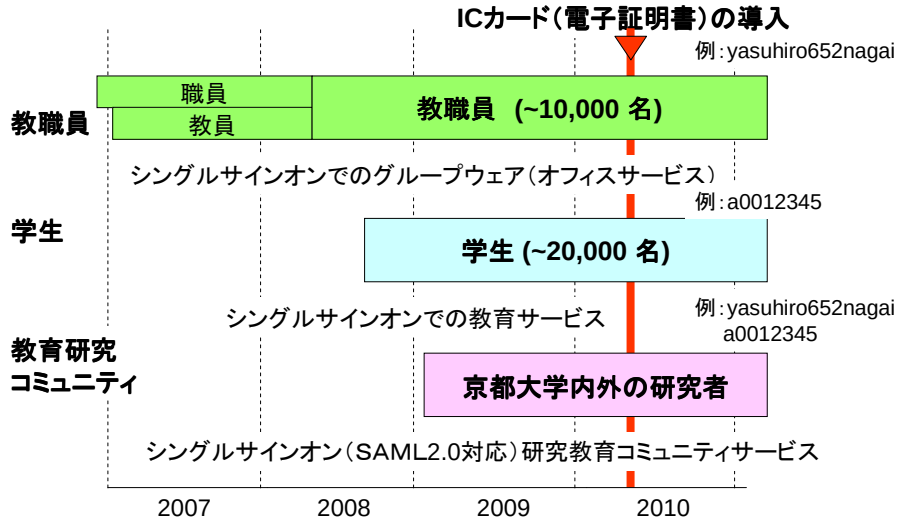
〔関連研究〕

- 平野・内藤: “UPKIイニシアティブ『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』と名古屋大学における事例”,
  - 名古屋大学情報連携基盤センターニュース Vol.6 No.4
    - http://www2.itc.nagoya-u.ac.jp/pub/pdf/contents/contents06_04.htm
- 西村・佐藤:“東京大学におけるサーバ証明書発行体制の構築と課題”,
  - 情報処理学会第48回DSM研究会・第26回QAI研究会(平成20年3月、北陸先端大)
- J. Meijer (UNINETT, Norway), “Community SSL/TLS Server Certificate”
  - APAN 25th Workshop (Hawaii)
    - http://www.apan.net/meetings/hawaii2008/proposals/middleware.html

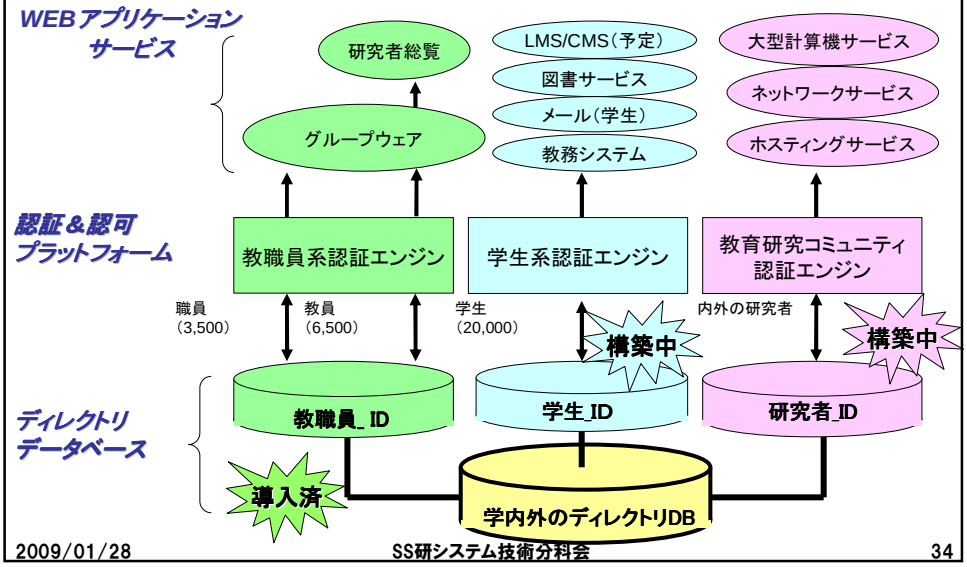
(3) 京都大学における認証基盤の構築 ～SSOと権限委譲～

認証基盤の構築スキーム

※H20年度4月時点で全学オーソライズされた実施スキーム

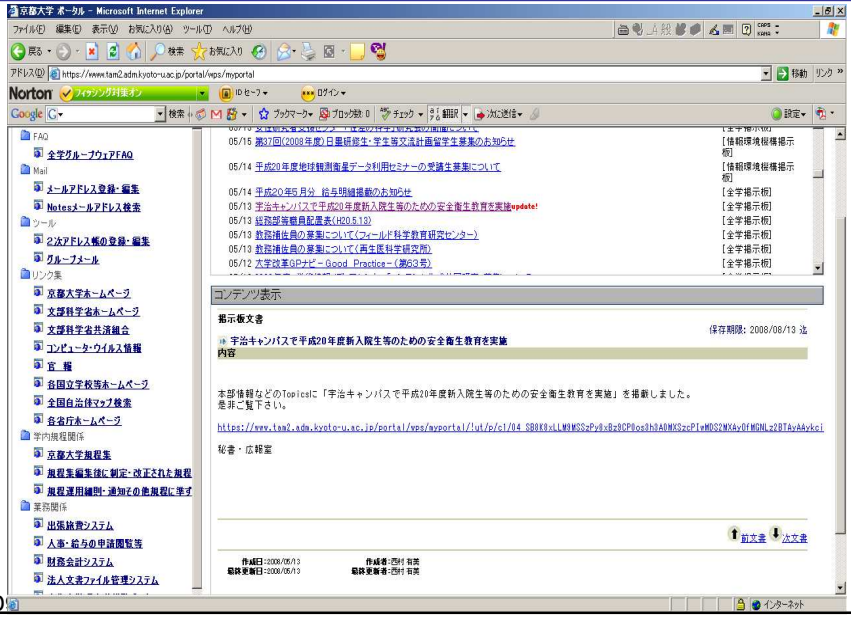


認証基盤全体イメージ



教職員用ｸﾞﾙｰﾌﾟｳｪｱ認証（例）

※H20年度4月時点で既に稼動中



ICカードの券種イメージ

IC職員証

京都大学職員証

写真

氏名：京大　次郎
職員番号：8桁＋1桁

有効期限：平成23年 3月31日
上記の者は本学の職員であることを証明する。

発行年月日
京都大学総長　印

IC　注意事項

ﾊﾞｰｺｰﾄﾞ

本証に関する連絡先：
人事部職員課
TEL075-753-2057

IC学生証

京都大学学生証

写真

平成20年4月入学
○○学部　○○学科
学生番号　1111-11-1111
氏名：　京大　太郎
生年月日：平成XX年XX月　X日
有効期限：平成23年 3月31日
上記の者は本学部学生であることを証明する
発行年月日
京都市左京区吉田本町
京都大学○○学部長　○○　○○　印

通学定期券発行控シール
貼付欄

ﾊﾞｰｺｰﾄﾞ

この学生証を拾得された方は
教務企画課TEL075-753-2493
にご連絡ください7

認証ICカード（仮称）

京都大学認証ICカード

写真

氏名：　京大　京子

有効期限：平成23年 3月31日

発行年月日
京都大学情報環境機構
印

IC　注意事項

本証に関する連絡先：
情報環境部
TEL075-753-2057

再利用のため裏面には
バーコードなし

■磁気ストライプ
- 個人番号＋再発行回数（現行とおり）

■バーコード（病院等で利用し実績有り）
- 個人番号（10桁、NW7）

■電子データ
- 認証用識別名（DN）、利用者ID（CN）（接触ICチップに搭載）
- 基本ID情報（FCFフォーマットに準拠（※1）

（※1）利用者区分（2Byte）＋ID番号（個人番号12Byte）＋再発行フラグ（1Byte）
＋氏名（半角カタカナ／英字）＋学校識別コード＋発行年月日＋有効期限

利用サービスのイメージ

主な対象者	教職員（常勤）	教職員（非常勤）	学生	その他
証の名称	職員証	認証ICカード	学生証	施設利用証
導入後の利用サービス（共通）	**物理的セキュリティ** （例：建物への入退館、図書館、サーバ室、研究室、事務室など）			
	・グループウェアの**個人認証** ・**電子メール暗号化** （外部へはパブリック証明書利用を推奨） ・**セキュアな印刷とコピー**		**証明書自動交付**	
4年後を目処に収容するサービス	生協など**少額決済** 電子ロッカー 施設利用システム連携			
	グループウェア以外の**セキュアな業務への認証／暗号化**（PKI利用）		**教育利用** （出欠、レポート）	
5年以降に収容を検討するサービス	**部局の業務、サービスへの適用**（例：システムログインなど）			
	他大学との研究・教育リソースの共有（認証など）		他大学と単位互換 OBカード利用など	

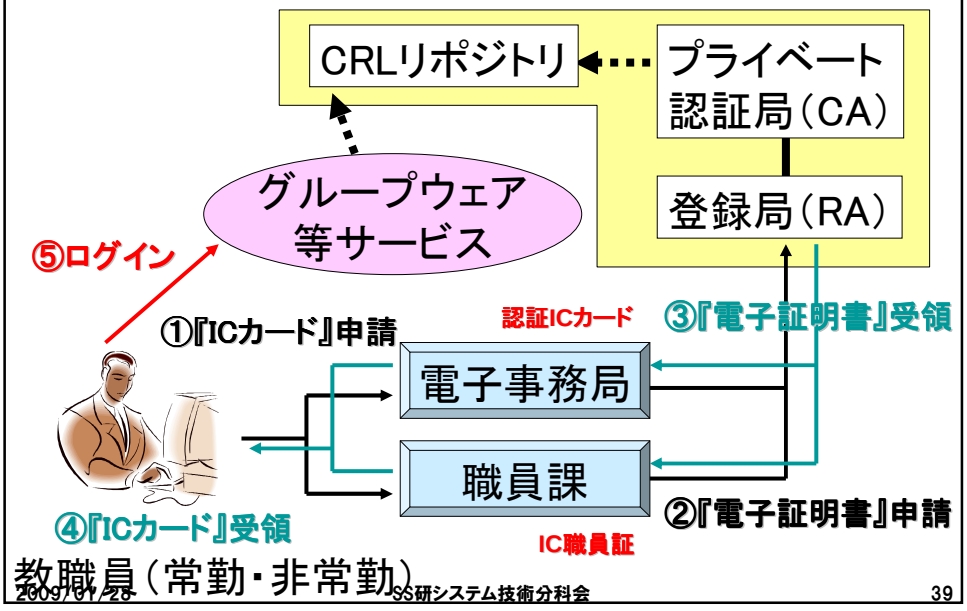
（参考）現行の職員証・学生証について

- **国立K大学の職員証**
  - **平成１３年に磁気カード化**
    （それまでは紙パウチ）
  - **図書館の入館証として利用可**
  - **職員番号・生年月日を表面に表示**
  - **職員は首にぶら下げることになっているらしい**
- **学生証もおおむね同様**
- **他大学との互換性はまったくなし**
  - **謎の職員番号体系**

平成２３年３月末日失効

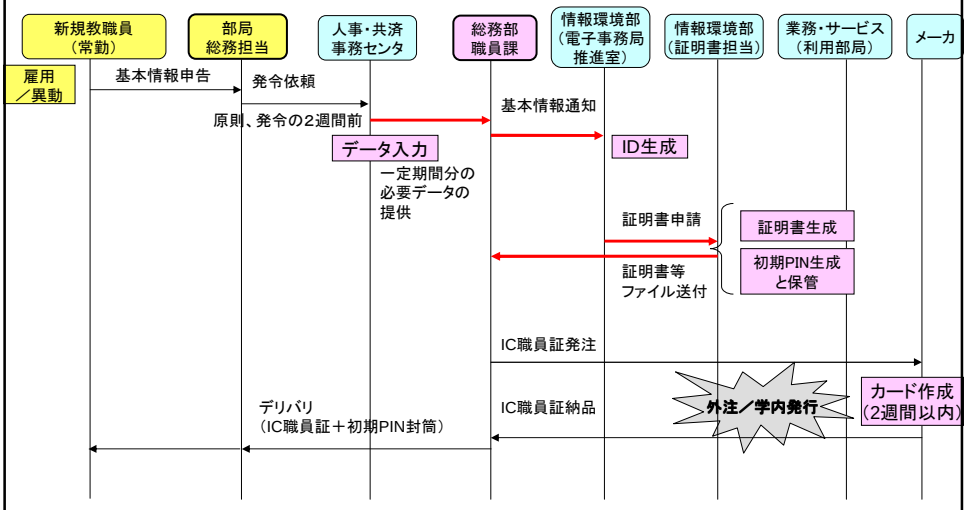
認証局等運用イメージ

※H20年度6月より調達中



IC職員証発行イメージ（例）

※H20年度6月より調達中



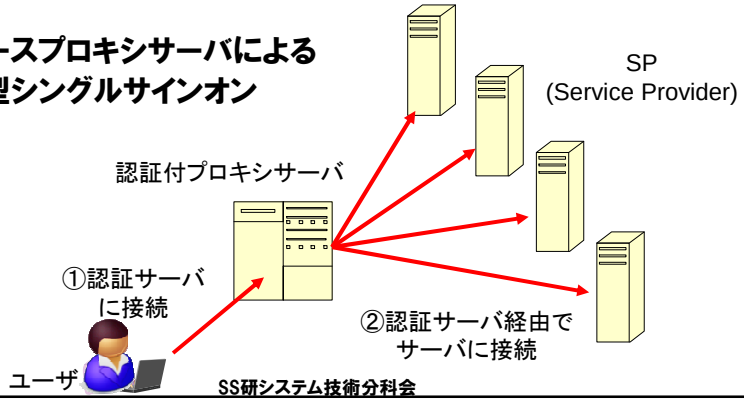
シングルサインオンとは

シングルサインオン(single sign on)

- 利用者が、1回のログイン手続きで、認証を必要とする複数のサービスを利用できるようにする仕組み
- 代わりにその1回のログイン手続きは十分セキュアにする

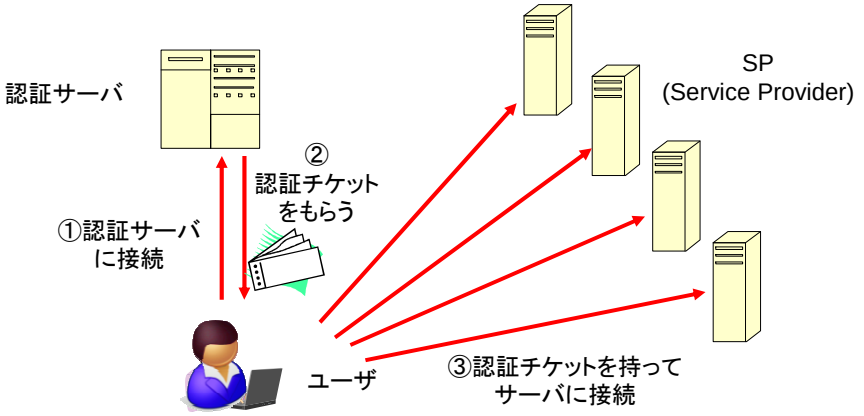
（注）単にすべてのサービスで同じID/パスワードを使うのとは違う！

（例）リバースプロキシサーバによる集中型シングルサインオン



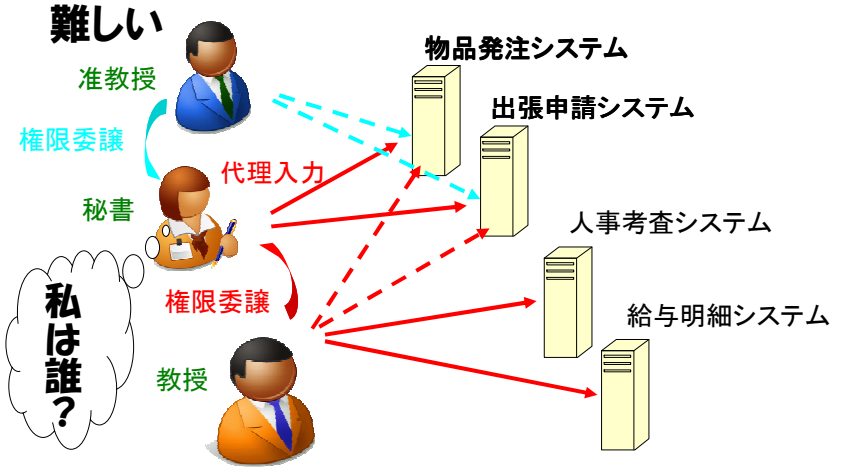
分散型シングルサインオン

SAML (Security Assertion Markup Language) などの考え方



シングルサインオンの課題

- サービスごとの権限委譲による代理入力が難しい



代理入力方式の提案と評価

（京都大学・学術情報メディアセンター　永井靖浩 教授）

- SSO＋ID名寄せで運用の問題が懸念される

  -現実運用中の代理入力、役職IDの『認可』対処

- SSO環境で、電子証明書を利用して権限委譲による『認可』処理（代理入力）を考案

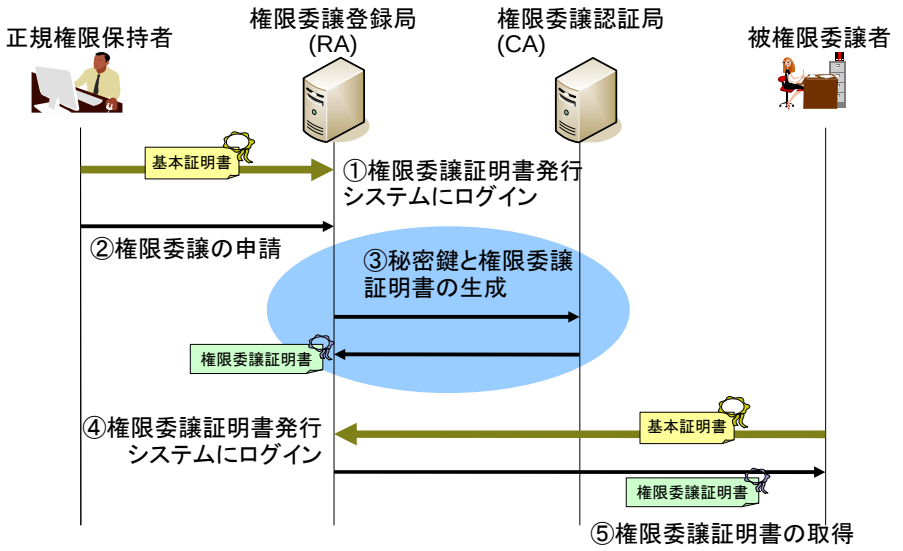
  -『認証』で基本証明書（ICカード）を利用するのであれば
  権限委譲の『認可』も同じ作法で利用

- 『認可』対応は原則バックエンド側（代理入力）だが必要な『認可』情報をICカードで分散管理

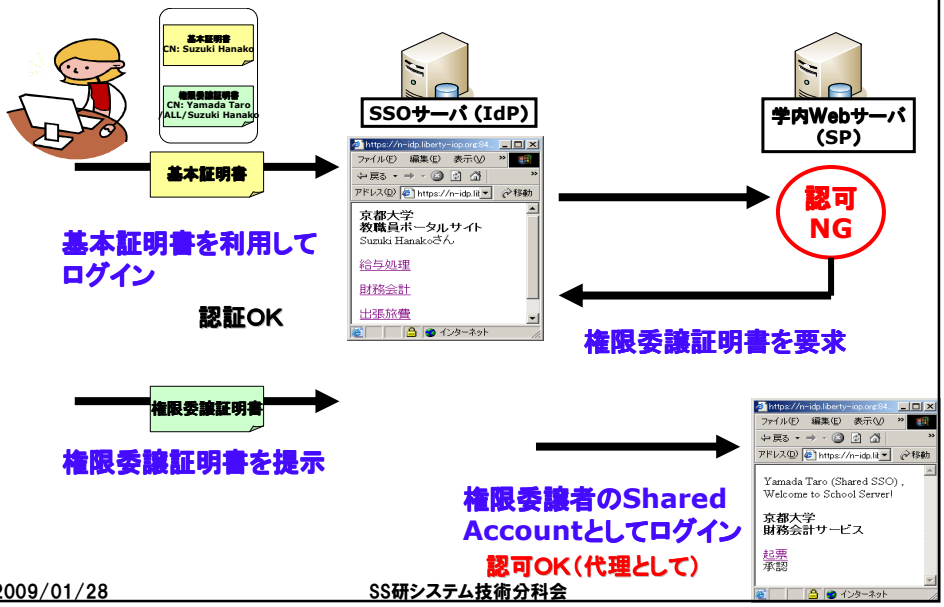
  -委譲情報（属性情報）をサーバに格納するのではなく、利用者が
  権限委譲証明書として保管

  -『認証』の基本証明書と共にICカードに格納して利用

権限委譲証明書の発行の流れ



権限委譲時の認証・認可処理

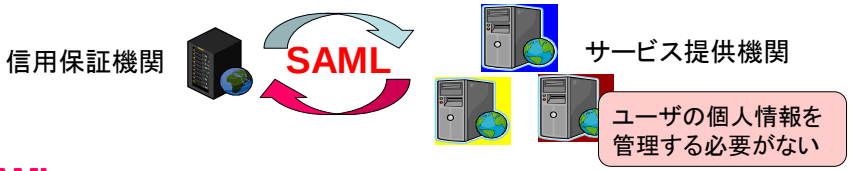


（4）UPKI認証連携基盤 SSO実証実験

FIMとSAML

FIM（連携アイデンティティ管理）とは

- 認証とサービス提供を分離する
- 情報システムで利用する認証情報などをドメインや サービスの敷居を越えてやりとりする仕組み



SAML（Security Assertion Markup Language）

- 認証情報を安全に交換するためのXML仕様
- 国際標準化団体**OASIS**（Organization for the Advancement of Structured Information Standards）によって策定
- Shibboleth、Liberty Alliance、.NET Passportなどが適用

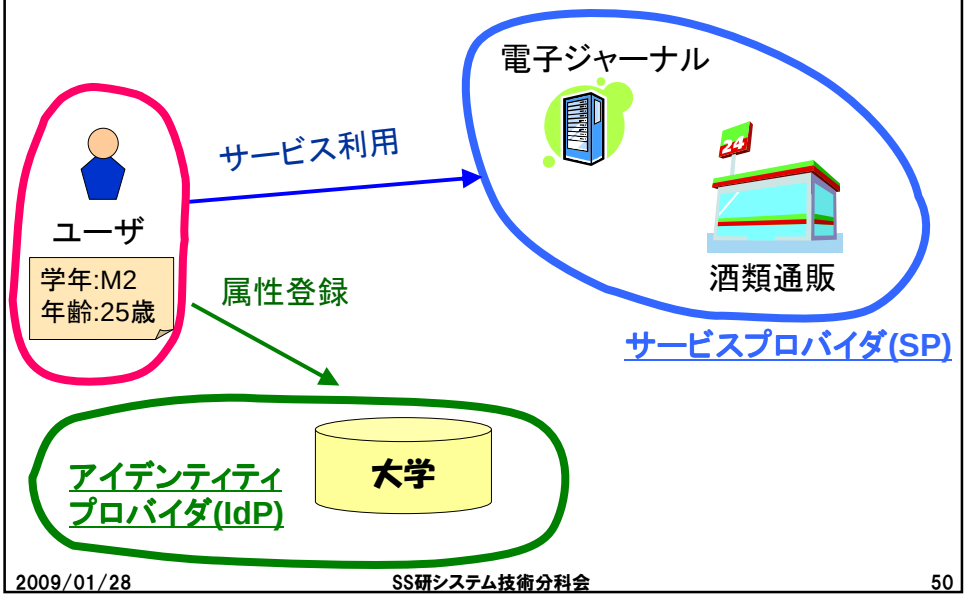
Shibbolethとは

Shibboleth

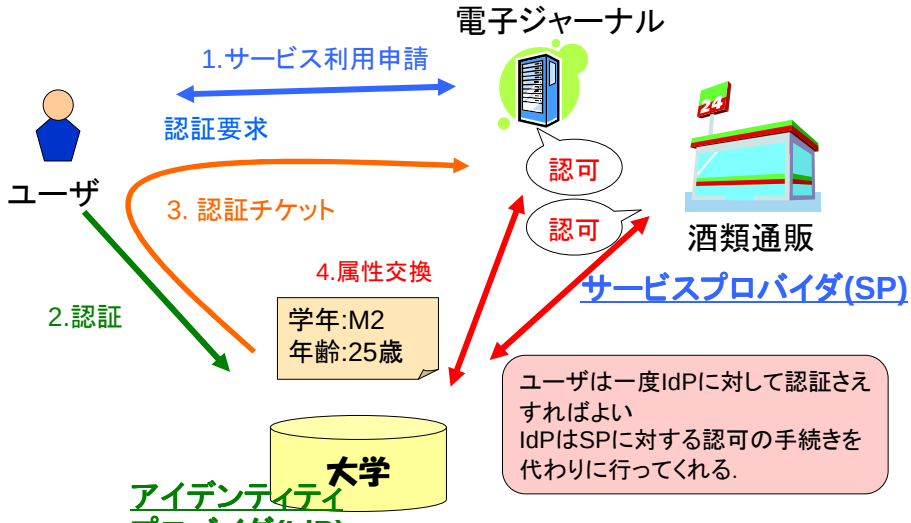
- Internet2/MACEプロジェクト
- SAMLをベースとした認証連携を実現するオープンソースの開発
  - •SAML2.0準拠の実装であるShibboleth2.0が最新版(H20.3)
- 欧米の大学・図書館等で普及

[URL] http://shibboleth.internet2.edu/

Shibbolethのアーキテクチャ



Shibbolethにおける認証・認可の流れ



属性とサービス

属性

- 大学が管理する属性
  - 学部・学科・学年
  - 取得単位・成績
- 他の機関により証明されるべき属性
  - 生年月日・本籍
  - 住所
  - 免許・資格
- 学生本人が登録する属性
  - 進路希望
  - 連絡先

サービス

- 大学が契約するサービス
  - 図書館・電子ジャーナル
  - 他大学科目の聴講
  - 鉄道の学割
- 提供者が身分・資格確認をする必要があるサービス
  - 携帯電話購入
  - 酒類販売
  - 就職活動・他大学進学
- いずれでもないもの
  - 就職情報メルマガ

Trust

- FIM(連携ID管理)は、IdPとSPの間のtrust(信頼関係)に依っている
  - SPは、IdPがユーザに関して正しい情報を送ってくることを信頼
  - IdPは、SPに送った属性が適切に利用することを信頼
  - もっと複雑な信頼関係もありうる…

認証連携とプライバシ

- Shibboleth/SAML型の認証連携では
  - IdP側はユーザがSPからどのようなサービスを受けているか知らない
    - 属性交換が不要なサービスであればどこのSPにアクセスしているかもIdPにはわからない

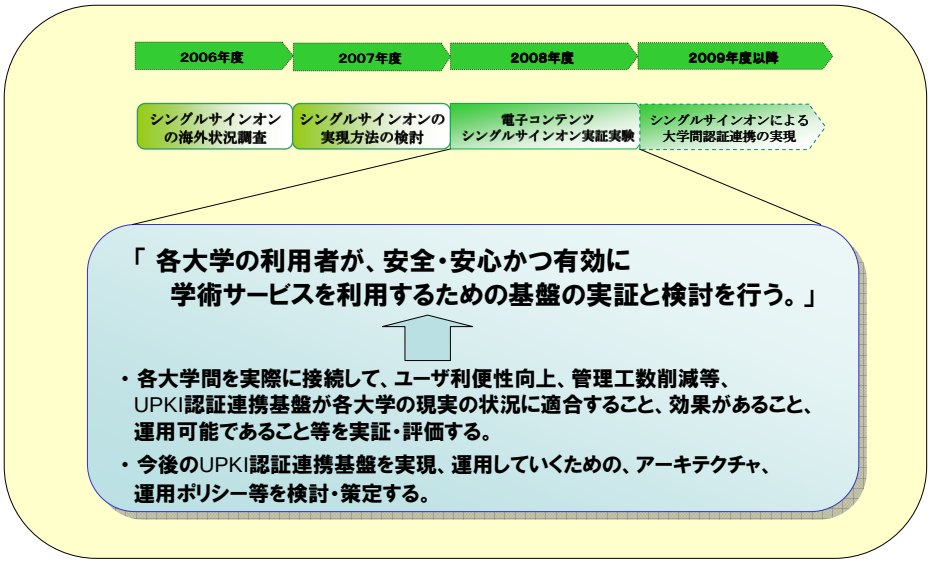
    「私はどこにいるか」を隠す
  - 認証チケットに仮名を用いることで、SPはユーザが誰なのかを知りえない
    - 複数のSPが結託し名寄せすることで意図しない形でプライバシーが漏出することを防ぐ

    「私は誰か」を不用意に明らかにしない

Federationについて

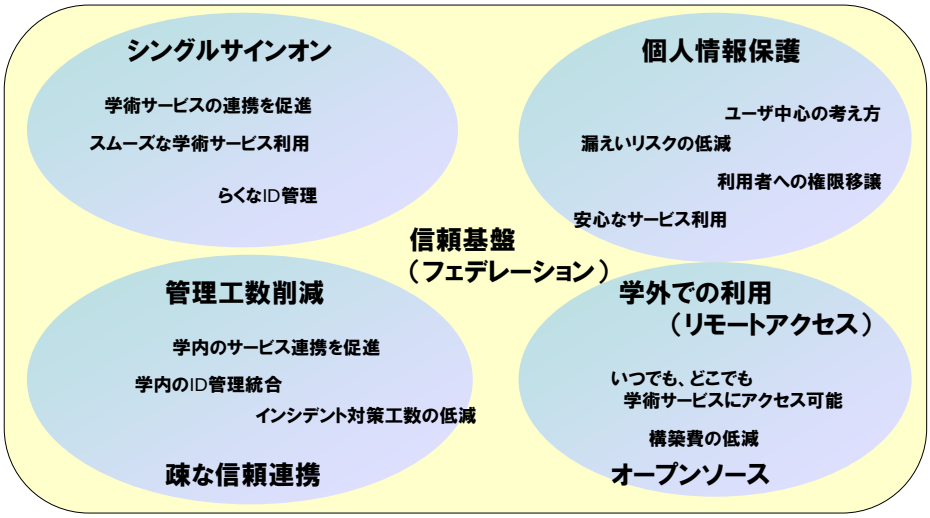
- あるルール(ポリシー)のもとで属性交換の相互運用に合意した組織(IdP、SP)の集合
- Federation運営組織が、ポリシー策定や認証局の認定、DS、メタデータDLサイトの提供を行う
- 世界のIdP;
  - 米国: InCommon
  - 英国: The UK Access Management Federation
  - スイス: SWITCHaai
  - オーストラリア: MAMS、AAF
  - フィンランド: HAKA
  - フランス: CRU
  - ノルウェイ: FEIDE
  - デンマーク: WAYF
  - ドイツ: DFN-AAI
- 世界のSP;
  - ScienceDirect、 Ovid Technologies、JSTOR、ExLibris、Digitalbrain、Thomson Gale等
  - Blackboard、WebCT、Moodle、OLAT、WebAssign等
  - DSpace, uPOrtal, Napster, Sharepoint, Symplicity, TWiki, Zope+Plone, eAcademy等

実証実験の目的

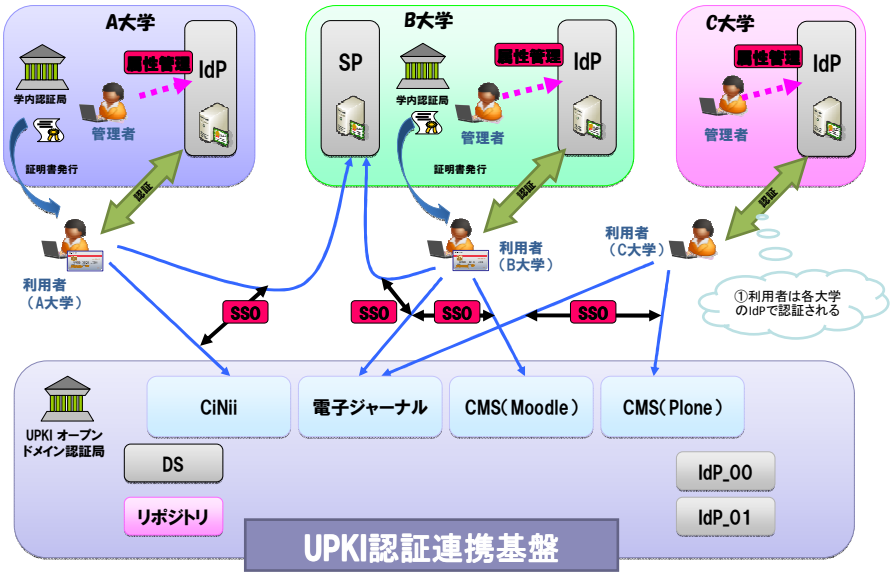


UPKI認証連携基盤の利便性

実証実験で、様々な利便性を検証して、枠組みの検討・定義を行う。

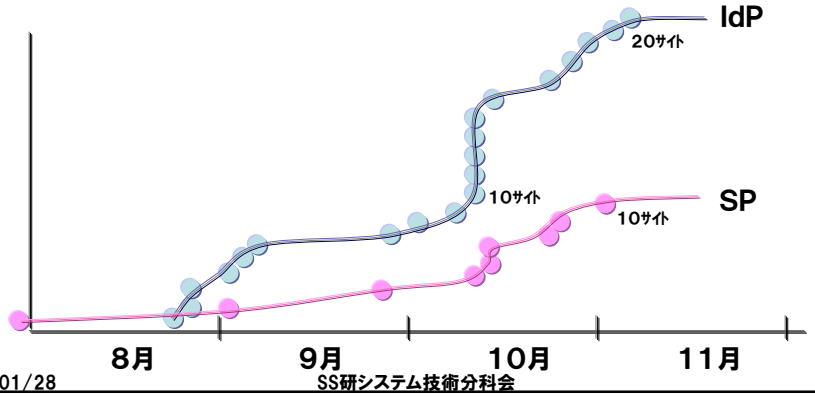


実証実験の概要



実証実験参加機関

- 参加機関（26機関）　　2008年11月現在
- IdP（18機関、20サイト）
- SP（9機関、10サイト、公開3サイト）



構築状況一覧

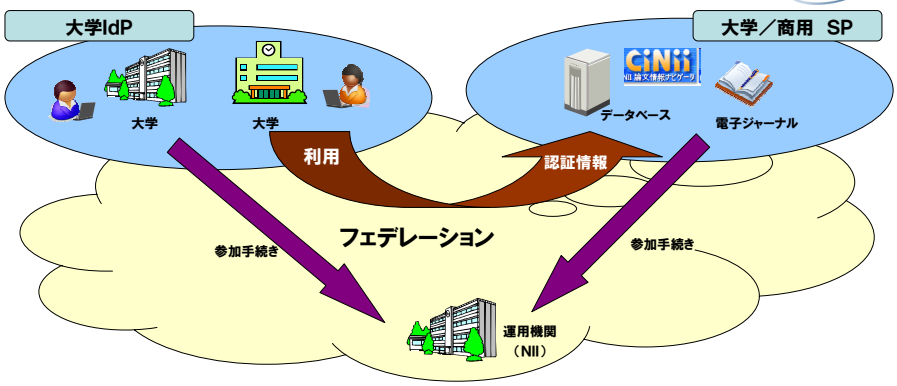
参加機関名称	IdP	SP
北海道大学	○	－
東北大学	○＊	－
山形大学	－	－
高エネルギー加速器研究機構	－	－
筑波大学	○	（未公開）
筑波技術大学	－	－
千葉大学	△	－
東京大学	○＊	－
東京工業大学	○	（未公開）
お茶の水女子大学	－	－
産業技術大学院大学	○2	マルチマウスAP、（構築中）
慶応義塾大学	－	－
国立情報学研究所	○2＊	CiNiiテスト＊

参加機関名称	IdP	SP
金沢大学	○	ファイル送信サービス、（DSpace）
名古屋大学	○	－
愛知県立看護大学	○	－
京都大学	○	（無線LANアカウント発行）
京都産業大学	－	－
大阪大学	○	（グリッド証明書発行）
愛媛大学	－	－
徳島大学	－	（OpenPNE）
広島大学	○	－
山口大学	○＊	（未公開）＊
九州大学	○	－
熊本大学	○	－
佐賀大学	○＊	（未公開）

○　：構築済み
2　：2サイト構築
△　：接続実験中
＊　：メタデータ自動更新設定済み

2008年11月現在

2－1. フェデレーションの構築（平成21年度～）



- 大学等とNIIが連携してフェデレーションを構築・運用する。
- フェデレーションへの電子ジャーナル等出版社の参加を交渉し，対象コンテンツの拡充を図る。（Elsevier社は，平成20年度中に実現予定）
- NIIが提供するコンテンツのシングルサインオン化を実現。

2－2. フェデレーション構築スケジュール

事　項	内　容
実証実験の成果の利用	（平成21年1月～3月） • 実証実験で使用したIdP，SPを継続して運用 • 大学で構築されたIdP，SPの，フェデレーションへの移行
規程（ポリシー）の作成	• フェデレーションの規程（ポリシー）を年度内に作成 • パブリックコメントを実施予定
対象コンテンツの拡充	• 国立大学図書館協議会等の協力により，商用電子ジャーナル各社と交渉を実施（Elsevier社のScience Directについては，平成20年11月中に実現予定） • NIIコンテンツサービスのシングルサインオン化実施
フェデレーション試行運用の実施	• 平成21年度は，試行運用としてフェデレーションを運用 • 試行運用を行いながら，問題点の改善，規程の改訂を実施 • 引き続き，大学への参加を広く呼びかける

（まとめのまえに）
近頃おさわがせの「個人情報」

平成17年4月、個人情報保護法施行

- 「個人情報」とは
  - 生存する個人に関する情報で、特定の個人を識別可能なもの（個人情報保護法第2条第1項）
- 個人情報漏洩事故・事件
  - 新聞紙上に載らない日がないくらい…

（企業にとって）
  - 顧客データベースが「宝の山」から「危険物」に

（個人にとって）
  - 自分に関する情報がどこでどう流通しているか、相変わらず全くわからない

プライバシとセキュリティ

- ITが簡単・低コストにするもの
  - コンピュータによる検索、複製
  - ネットワークを介しての送信、公開
- ITが困難にするもの
  - 通信している相手がどこの誰か？
  - 自分の情報が相手にどこまで伝わっているのか？

そもそもコンピュータとか
インターネットってどういうしくみ？

〔サイバー犯罪：ITを悪用〕
- 架空請求詐欺
- オークション詐欺
- フィッシング詐欺
- オレオレ詐欺
- 振り込め詐欺

これからますます
暮らしにくい世の中
になるのか？

“Trust” ― 信頼関係

- いまさらITのない社会に戻れない
- IT社会において失われつつあるもの
  - 人と人との信頼関係
    - 相手と対面
    - しかるべき第三者から紹介
- 実は、個人情報のやりとりの多くは、信頼関係がないがゆえの代用
  （典型例）いろんな登録での生年月日
- 「攻め」のセキュリティとプライバシー
  - 積極的に**信頼関係**を築く
  - 不必要な個人情報をやりとりしない

一見さんお断り

○○さんのご紹介やったら…

まとめ

- 大学における認証
  - 大学における構成員管理の難しさ
  - セキュリティ上の要請に伴う認証基盤の導入と強化
    - 個人認証
    - サーバ認証
  - 認証と権限管理の分離
    - シングルサインオンと権限委譲の両立
- 組織をまたがる認証：認証から認証連携へ
  - 認証とサービスの分離
    - 組織の壁を越えたサービスの提供とプライバシ保護