学認の活動状況と今後の展開

2014年度「SINET及び学認・UPKI証明書説明会」

次世代学術情報基盤

大学などの学術研究・教育活動の連携・推進

学術情報の公開と共有の拡充 Resource & Service

- 学術情報流通の促進と**オープンアクセス**の推進
- 大学の**機関リポジトリ拡充**の推進

CiNii JAIRO Cloud
学術コンテンツ基盤

クラウド基盤 Cloud

- クラウドサービス利活用促進による**大幅なIT経費削減・研究教育環境の高度化**

日本版「NET+」

Cloud Gateway

認証・セキュリティ強化 Security

- 大学全体の**セキュリティレベルの底上げ**
- 利用者認証の連携促進による**認証システムの高度化**

学術認証フェデレーション
HPCI認証
サーバ証明書
VPN

学術情報ネットワークの運用 Network

- 国内回線は**全国100Gbps化**
- 海外**（米国・欧州・アジア）**との高速接続
- 多様化するニーズに応えるSDNなどの**最新ネットワーク技術の導入**

急増するセキュリティ・インシデント
～パスワードの漏洩とアカウントの乗っ取り～

- ネットバンキングにおける不正送金の急増
- スパム送信数の急増（大学のメールサーバもターゲット）
- OpenSSL（暗号通信ソフトウェア）の脆弱性(HeartBreed)

ネットバンキングでの被害額・被害件数

1　被害件数、被害額

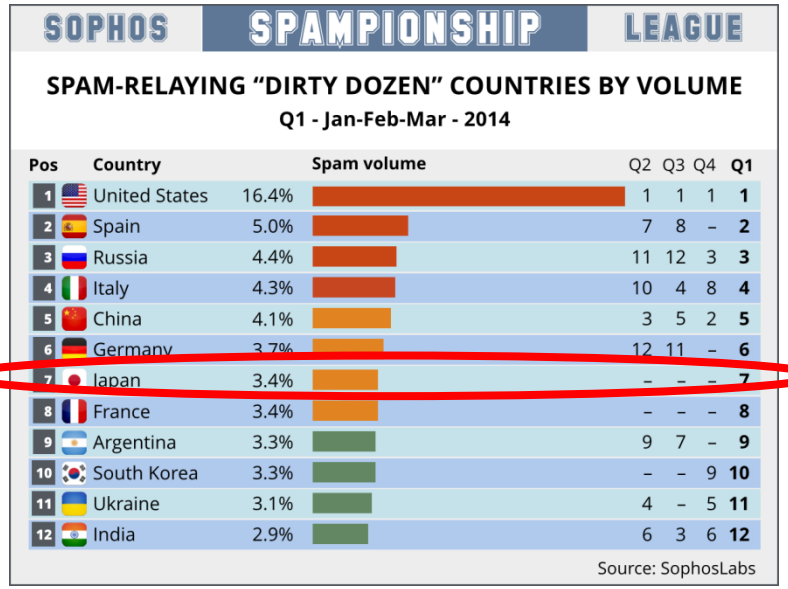
平成２５年	１，３１５件，約１４億０，６００万円
平成２４年	６４件，約　４，８００万円
平成２３年	１６５件，約　３億０，８００万円

月別発生件数（平成２３年～平成２５年）

平成25年：件数14倍、
被害額29倍（前年度比）

2014年1月30日、警視庁発表
Source: http://www.i-infini.com/security/?p=281

スパム送信国ランキング



SOPHOS SPAMPIONSHIP LEAGUE

SPAM-RELAYING "DIRTY DOZEN" COUNTRIES BY VOLUME
Q1 - Jan-Feb-Mar - 2014

Pos	Country	Spam volume	Q2	Q3	Q4	Q1
1	United States	16.4%	1	1	1	1
2	Spain	5.0%	7	8	–	2
3	Russia	4.4%	11	12	3	3
4	Italy	4.3%	10	4	8	4
5	China	4.1%	3	5	2	5
6	Germany	3.7%	12	11	–	6
7	Japan	3.4%	–	–	–	7
8	France	3.4%	–	–	–	8
9	Argentina	3.3%	9	7	–	9
10	South Korea	3.3%	–	–	9	10
11	Ukraine	3.1%	4	–	5	11
12	India	2.9%	6	3	6	12

Source: SophosLabs

Source: https://www.sophos.com/ja-jp/press-office/press-releases/2014/04/ns-dirty-dozen-q1-2014.aspx

大学間連携のための全国共同電子認証基盤（UPKI）

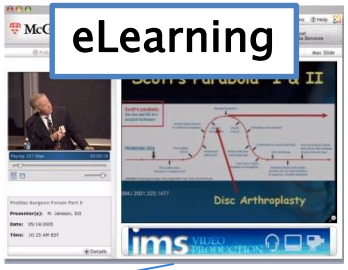
- CSI実現に向けての、大学等の学内および大学間連携のための電子認証基盤
  - 学術ネットワーク運営・連携本部　認証作業部会（2005年設置）
    - 7大学情報基盤センター、東工大、KEK、NIIで構成
    - 「大学間連携のための全国共同電子認証基盤構築事業」として活動開始
      - 文部科学省（2006年度～2008年度）
- PKI技術の普及・活用のための6つの課題を設定

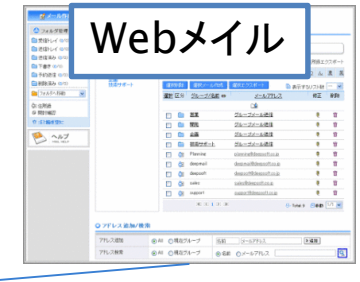
1	UPKI共通仕様の作成・配布	学内認証局構築のためのCP/CPSおよび調達仕様書の雛形を提供（済）
2	オープンドメイン サーバ証明書発行	「UPKIオープンドメイン証明書自動発行検証プロジェクト」で300以上の機関に対して無償で提供中（のべ15000枚以上を発行）
3	大学間無線LANローミング	国際学術無線LANローミング基盤eduroamとして展開（国内約60機関）
4	シングルサインオン検討	学術認証フェデレーション「学認」として運用中
5	認証局ソフトウェアパッケージ開発	無線LAN認証等に適用可能なNAREGI-CAをベースとしたスタートパックを提供（済）
6	S/MIME証明書の試験利用	実用化に向けてオープンドメインクライアント証明書の配布コストが懸案

大学等におけるIT環境整備の動き(1):学内認証統合

- 管理者
  - ID管理工数の軽減
- 利用者
  - ID/Passwordを使い分ける必要なし

サービス毎の
アカウント管理は
面倒





ユーザディレクトリ(LDAP)

人事課　学務課　総務課

このユーザ情報の一元化の整備に加えて

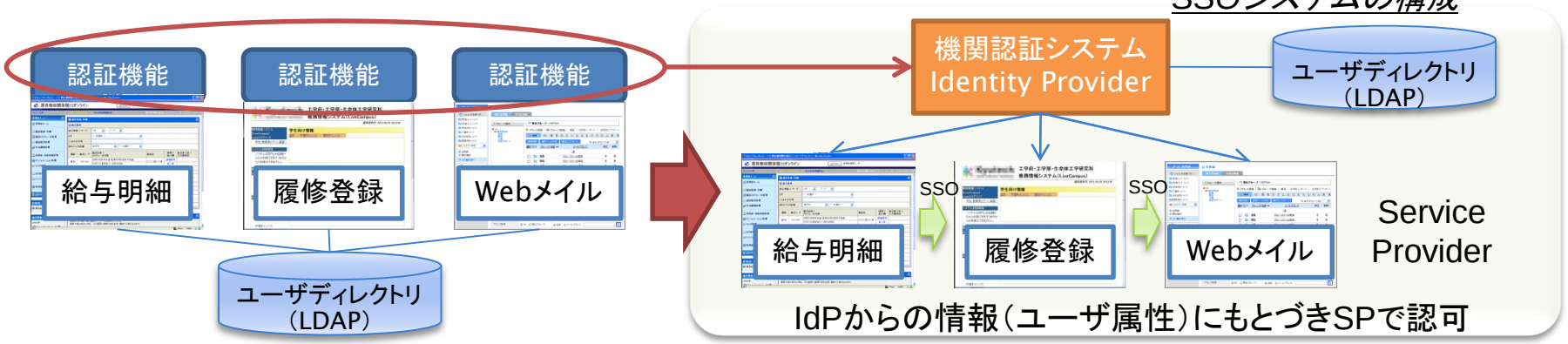
大学等におけるIT環境整備の動き(2):シングルサインオン(SSO)への対応

- 統合認証されても、アプリケーションアクセスするたびに、同じIDとパスワードの入力を要求される

Single Sign On

- 一度の認証手続きだけで、複数のサービスを受けることができる技術
  - 利用者の利便性の向上
- 利用者の認証とサービス利用の可否判断(認可)を分離
  - セキュリティ対策レベルの底上げ

SSOシステムの構成

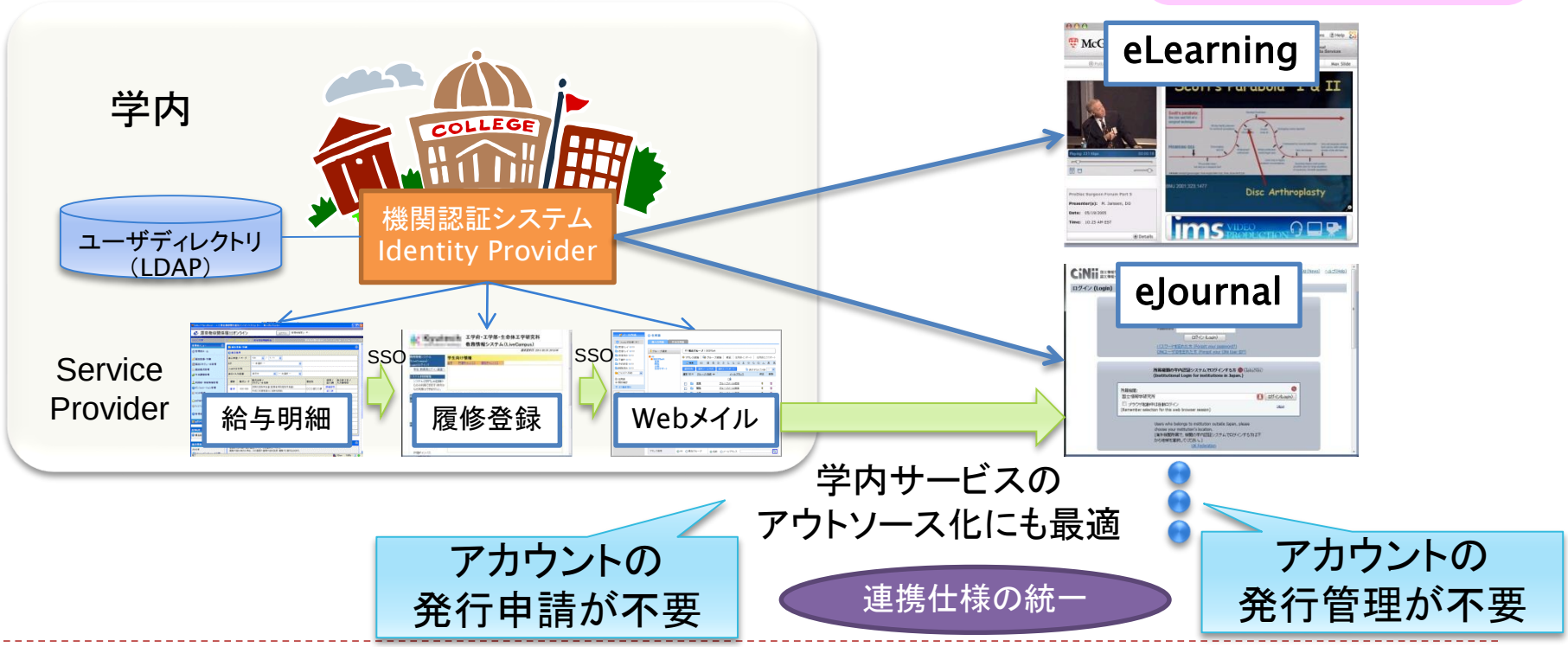


SSO技術の学外への展開：ID連携
学術認証フェデレーション「学認」

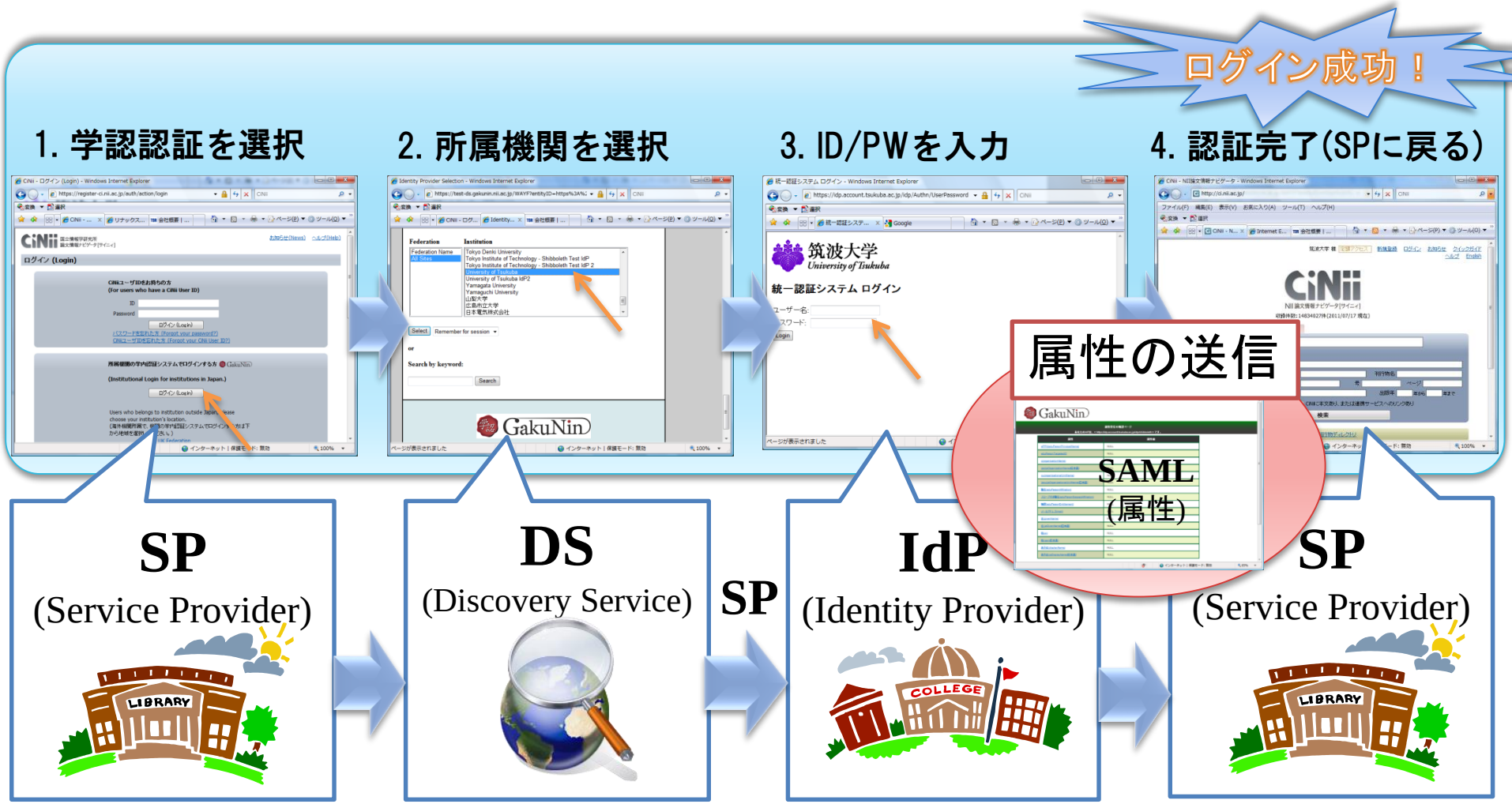
学内SSOの仕組みをグローバルに

GakuNin

・学外コンテンツ
・クラウドサービス
などへのアクセスにも



学認における認証手順



学認で扱う属性情報（IdPからSPへ送出）

属性	内容
OrganizationName (o)	組織名
jaOrganizationName (jao)	組織名（日本語）
OrganizationalUnit (ou)	組織内所属名称
jaOrganizationalUnit (jaou)	組織内所属名称（日本語）
eduPersonPrincipalName (eppn)	フェデレーション内の共通識別子
eduPersonTargetedID	フェデレーション内の仮名識別子
eduPersonAffiliation	職種 (Staff, Faculty, Student 等)
eduPersonScopedAffiliation	職種（@scopeつき）
eduPersonEntitlement	資格
SurName (sn)	氏名（姓）
jaSurName (jasn)	氏名（姓）（日本語）
GivenName	氏名（名）
jaGivenName	氏名（名）（日本語）
displayName	氏名（表示名）
jaDisplayName	氏名（表示名）（日本語）
mail	メールアドレス
gakuninScopedPersonalUniqueCode	学生・職員番号（@scopeつき）

実際に使われる属性情報の例

サービスA (1項目必須)

eduPersonPrincipalName(必須)

サービスB (1項目必須)

eduPersonAffiliation (必須)
eduPersonTargetedID

サービスC (必須項目なし)

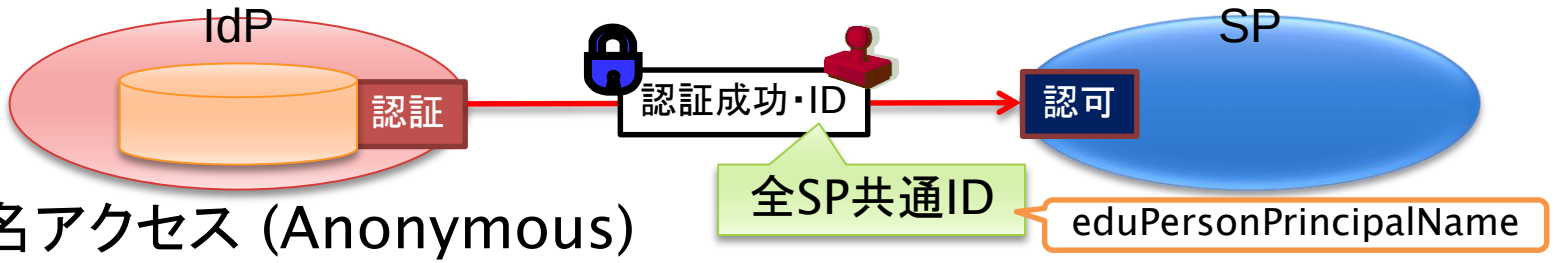
eduPersonEntitlement
eduPersonAffiliation

必要最低限のみを送出

(参考) 学認技術運用基準
http://id.nii.ac.jp/1149/00000212/

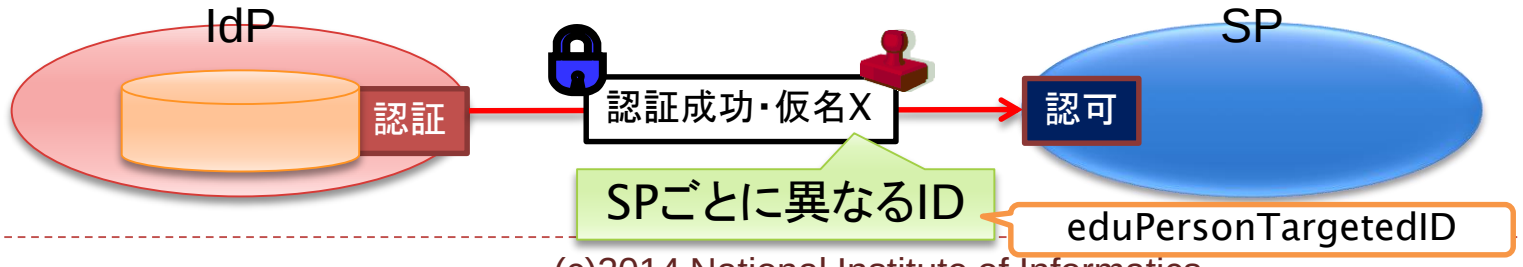
プライバシー保護：匿名アクセス、仮名アクセス

- 通常アクセス



- 匿名アクセス (Anonymous)
  - ID情報を送らないので、実際に誰かはわからない

- 仮名アクセス (PPID: Pairwise Pseudonymous Identifier)
  - SP毎に異なるIDを送ることで、SP間での行動履歴の名寄せを防止
    - プライバシーを保護



プライバシー情報の送信制御（承諾）
uApprove.jp (IdPプラグイン)

- 送信が必須でない属性情報に関して、ユーザが送信の可否を個別に指定可能
- 将来の挙動について指定可能

IdP 2.4に対応しました

必須の属性情報

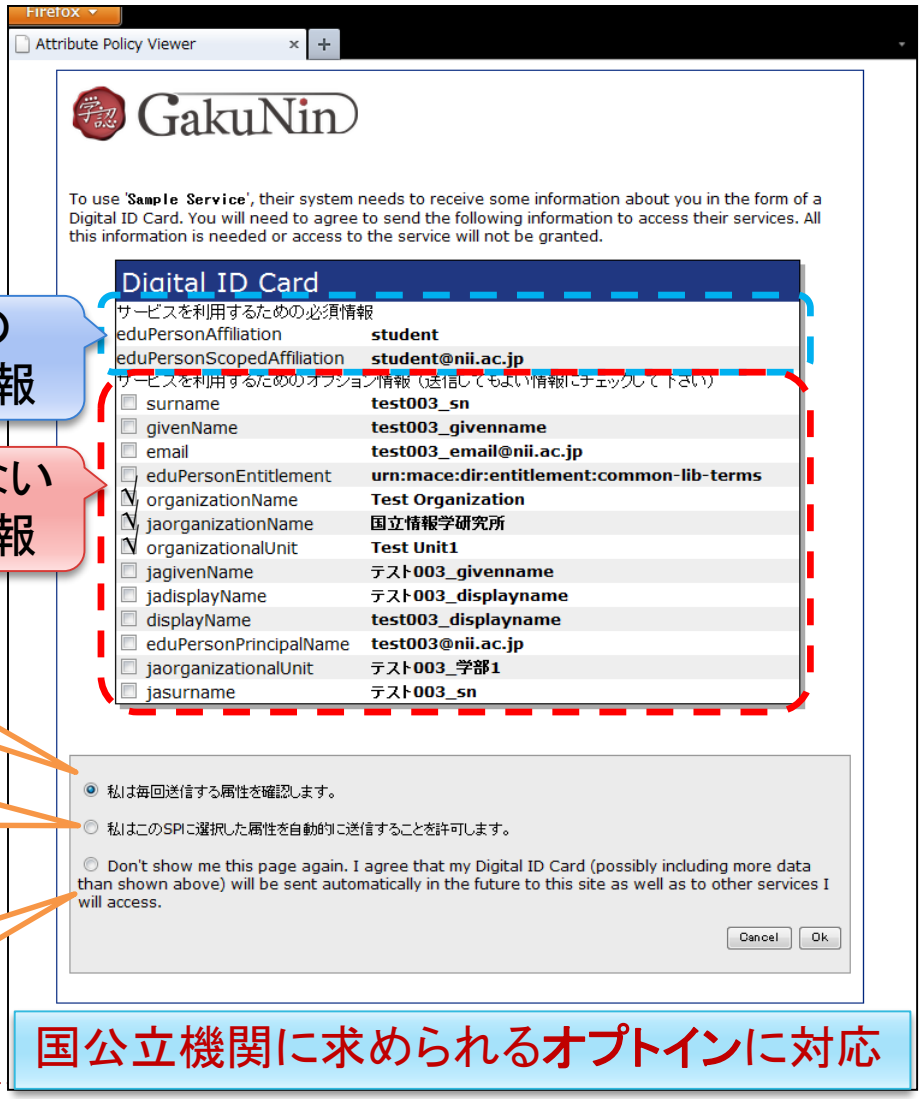
必須でない属性情報

次回の同一SPアクセス時も再び同意が必要

同一SPについては将来の同一内容の送信について同意

全てのSPに対して全ての属性情報を送ることを同意

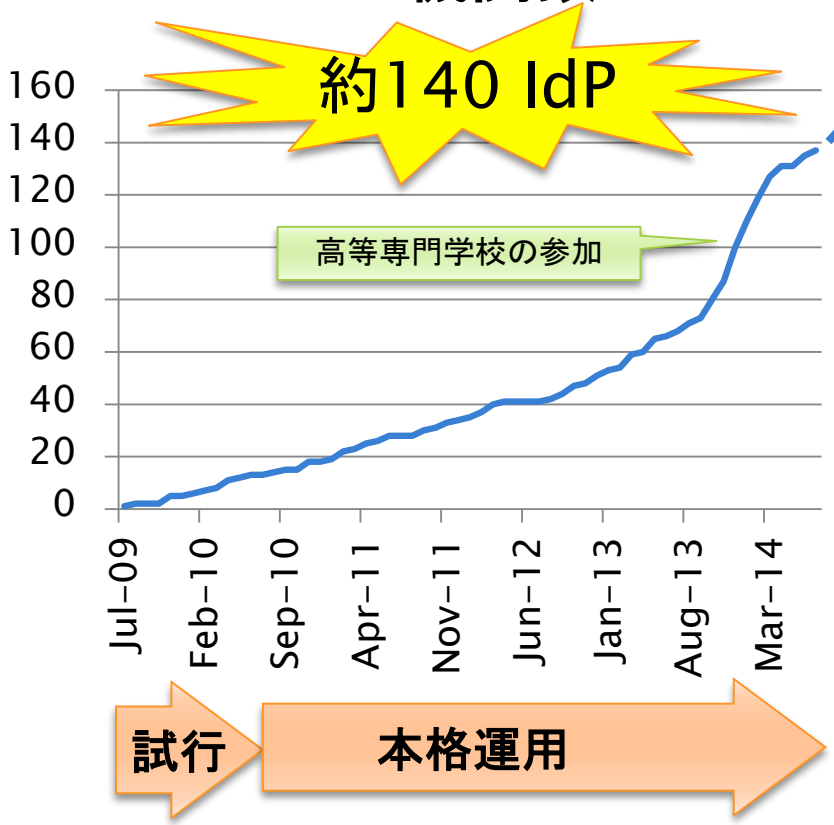
※遵守すべき個人情報保護法が異なることによる→



国公立機関に求められるオプトインに対応

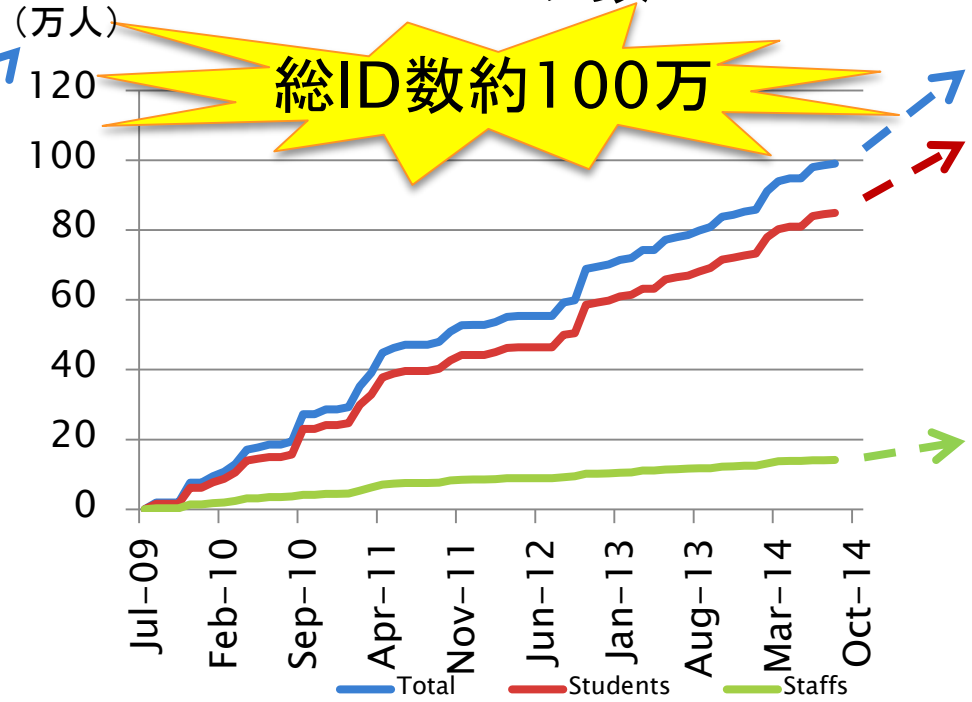
学認参加IdPの推移（2014/9/1現在）

機関数



試行 → 本格運用

ユーザ数



参考：高等教育人口は350万人（文部科学省）

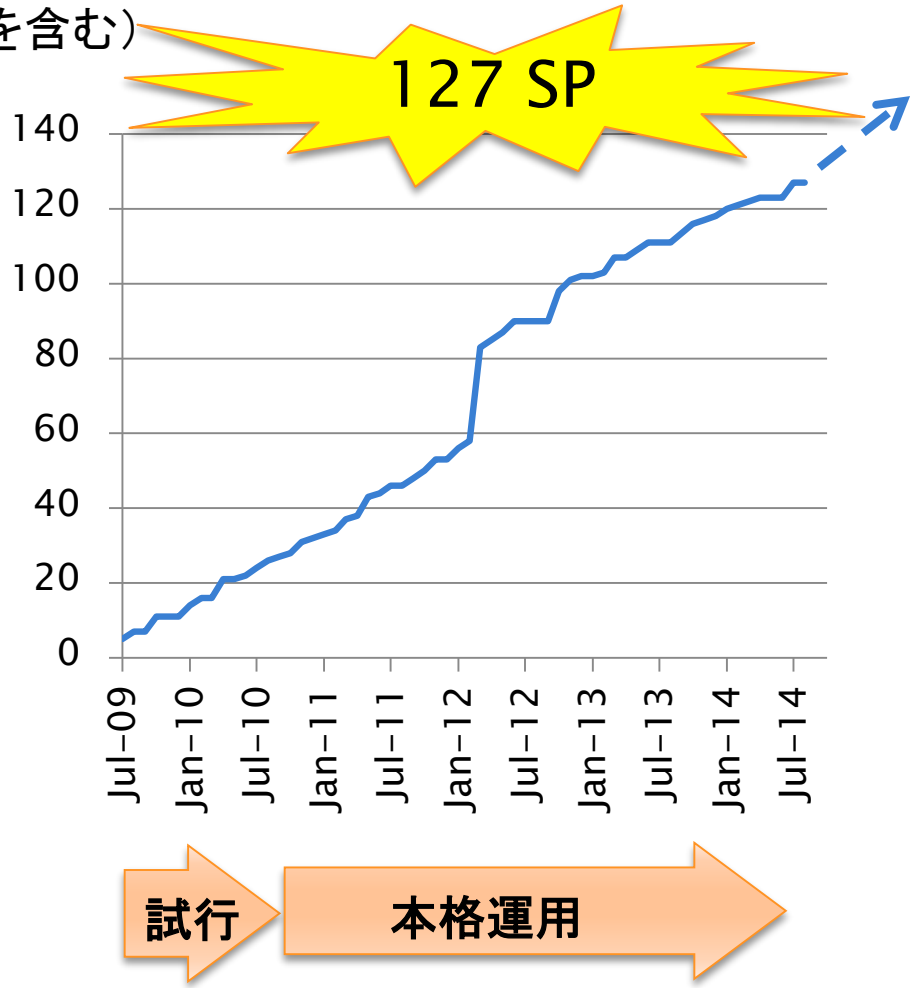
学生の割合は、80%強

	国立大学	公立大学	私立大学	短期大学	高等専門学校	共同利用機関	その他	合計
学認参加数	46	5	29	0	51	1	7	139
カバー率	53%	5%	5%	0%	89%			
総機関数	86	92	603	352	57			

学認参加SPの推移（2014/9/1現在）

メタデータ登録数（公開準備中を含む）

- コンテンツ系サービス
  - 電子ジャーナル
  - 機関リポジトリ
  - 文献検索
  - 論文・業績情報管理
  - 開発環境（ソフトウェア）
- 基盤系サービス
  - 無線ネットワークアクセス
  - Eラーニング
  - テレビ会議
  - ファイル共有
  - メーリングリスト
  - クラウド環境

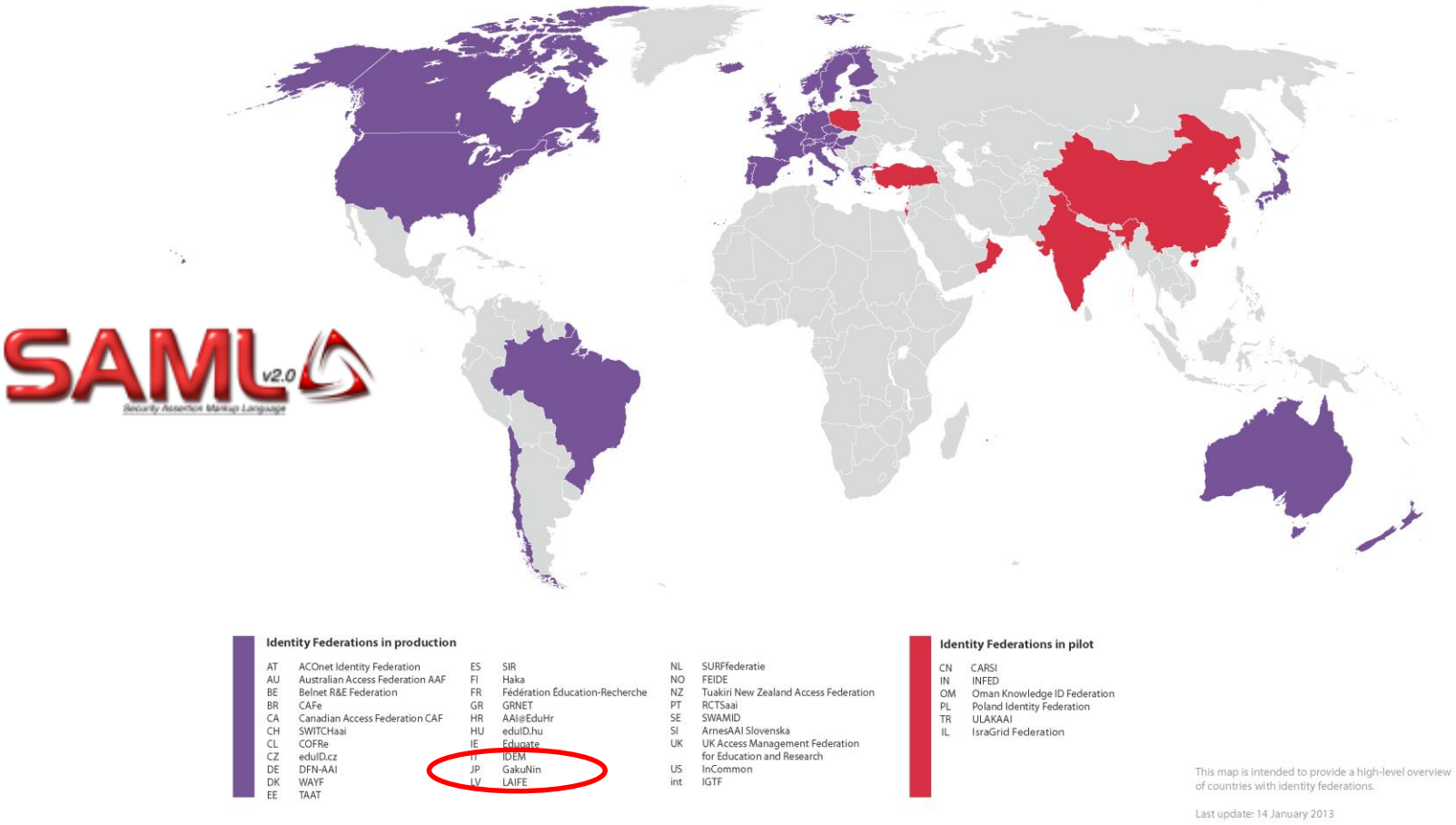


世界の学術フェデレーション

国を単位とする学術フェデレーションの広がり

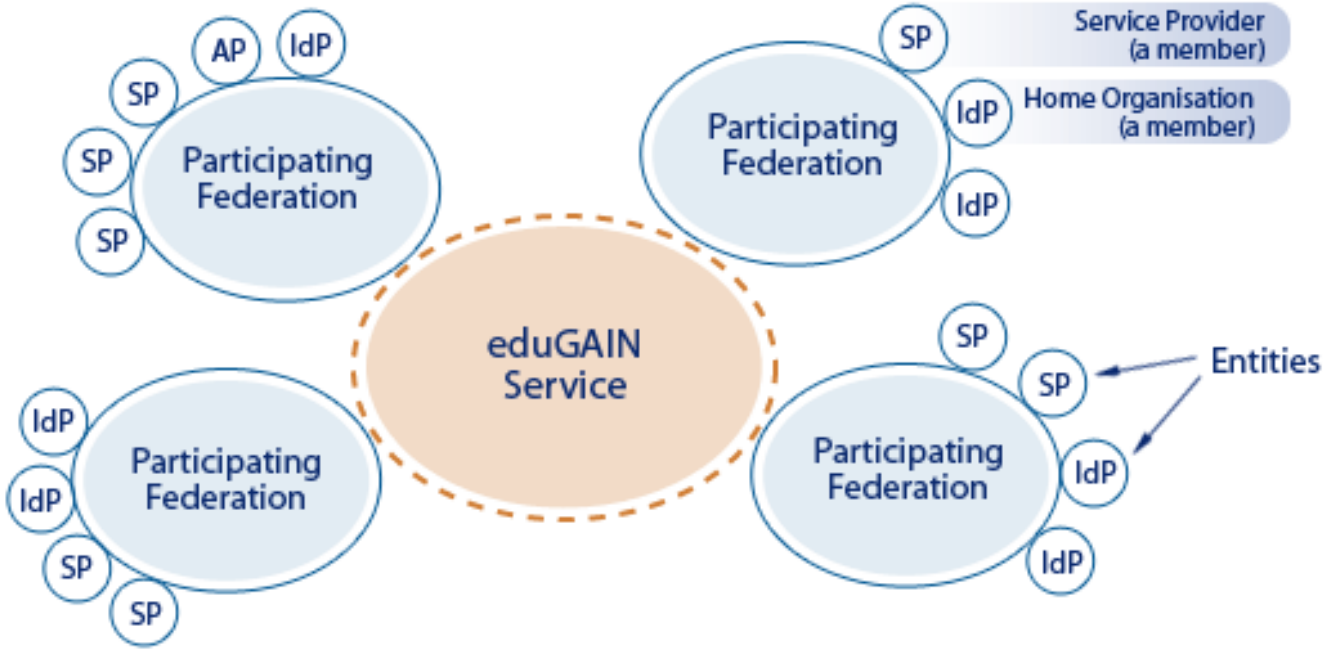
REFEDS

SAML v2.0



Source: https://refeds.org/docs/REFEDSmap.pdf

eduGAIN によるフェデレーション連携（インターフェデレーション）



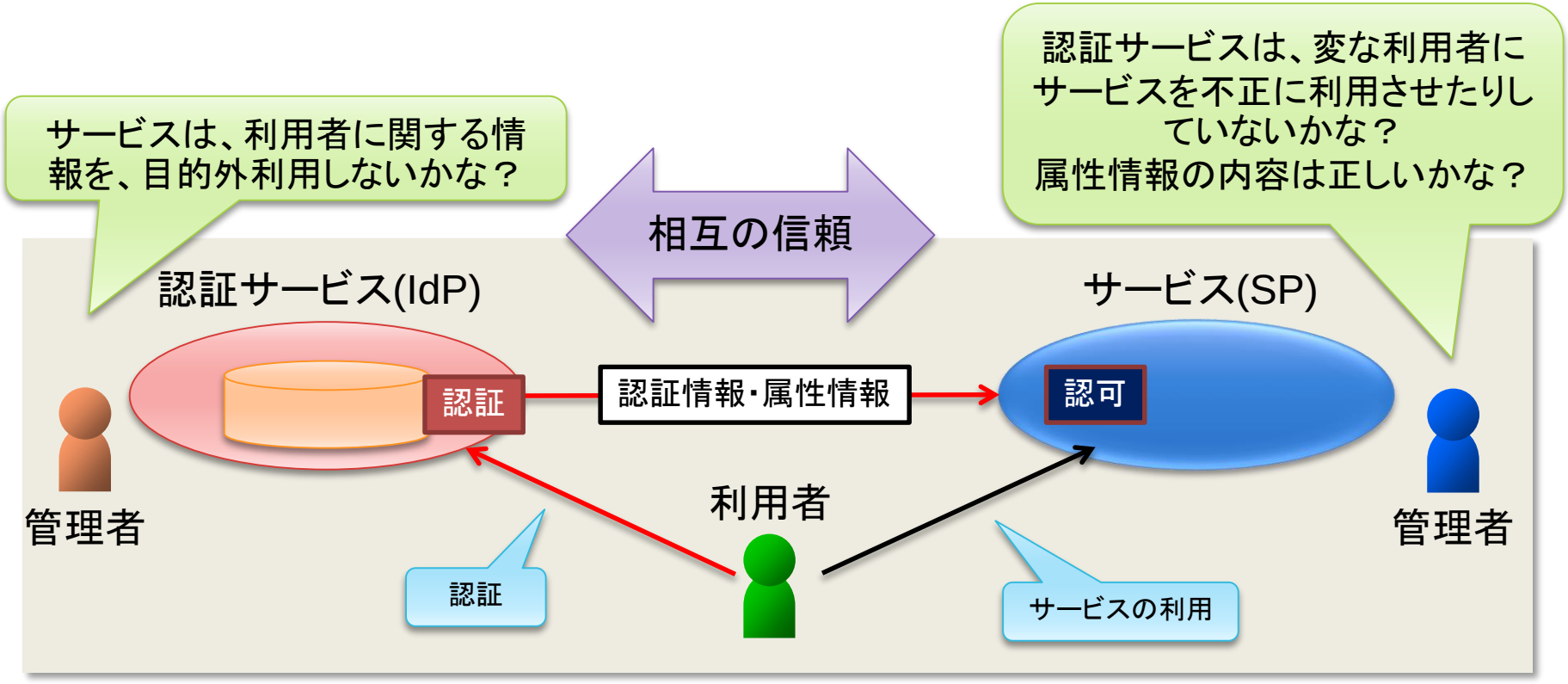
- eduGAIN経由で利用可能なサービス（500以上）
  - SURFconext, FileSender, Foodle, perfSONAR, GRID系サービスなど
  - http://goo.gl/G6pYDV

eduGAINのSPにアクセスするには

- IdPがeduGAINに参加する必要があります
  - 当該SPが学認に参加している場合を除く
- 学認申請システムには、IdPをeduGAINに登録する機能があります
  - IdP管理者が、「eduGAINへ参加する」にチェックを入れることで、メタデータがeduGAINに送られます

SSO技術の組織間利用での信頼

- 「認証」と「認可」の分離
  - **認証**：本人確認 (Authentication)
  - **認可**：その人に利用させるかどうかの判断 (Authorization)
- 異なる組織が個別に管理するため、相互の信頼が重要



学認で定めるIdPの要件（技術運用基準）

- 組織の構成員であることの保証
  - 卒業、退職などによる異動の適切な反映
  - 名誉教授、OB、図書館の地域内利用者、その他ゲスト等の扱い
- 識別子再利用についての考慮
  - 同一識別子を利用する場合は、一定期間あける
- ユーザの同一性の保証
  - パスワード配布時の本人確認
  - 適切に管理された役職アカウント
- 個人情報保護への対応
  - 国公立大学ではオプトインが原則
- ログの保存
  - インシデント対応のための記録

機関として責任を持った
IDおよび属性の保証

⇒定期アンケート（毎年）によるチェックとフィードバックで信頼性を維持

- IdP of the Year 2012 ― 大阪大学
- IdP of the Year 2013 ― 山形大学

LoA1認定
第1号

「本人」であることの確からしさ
LoA: Level of Assurance（4つのレベル）

- （米）OMB M-04-04 E-Authentication Guidance for Federal Agencies (2003)
- （米）NIST SP800-63 Electronic Authentication Guideline (2006発行, 2011改訂)
- ITU-T X.1254 Entity Authentication Assurance Framework (2012-09承認)
- ISO/IEC 29115:2013 Entity authentication assurance framework (2013-04)

世界標準へ

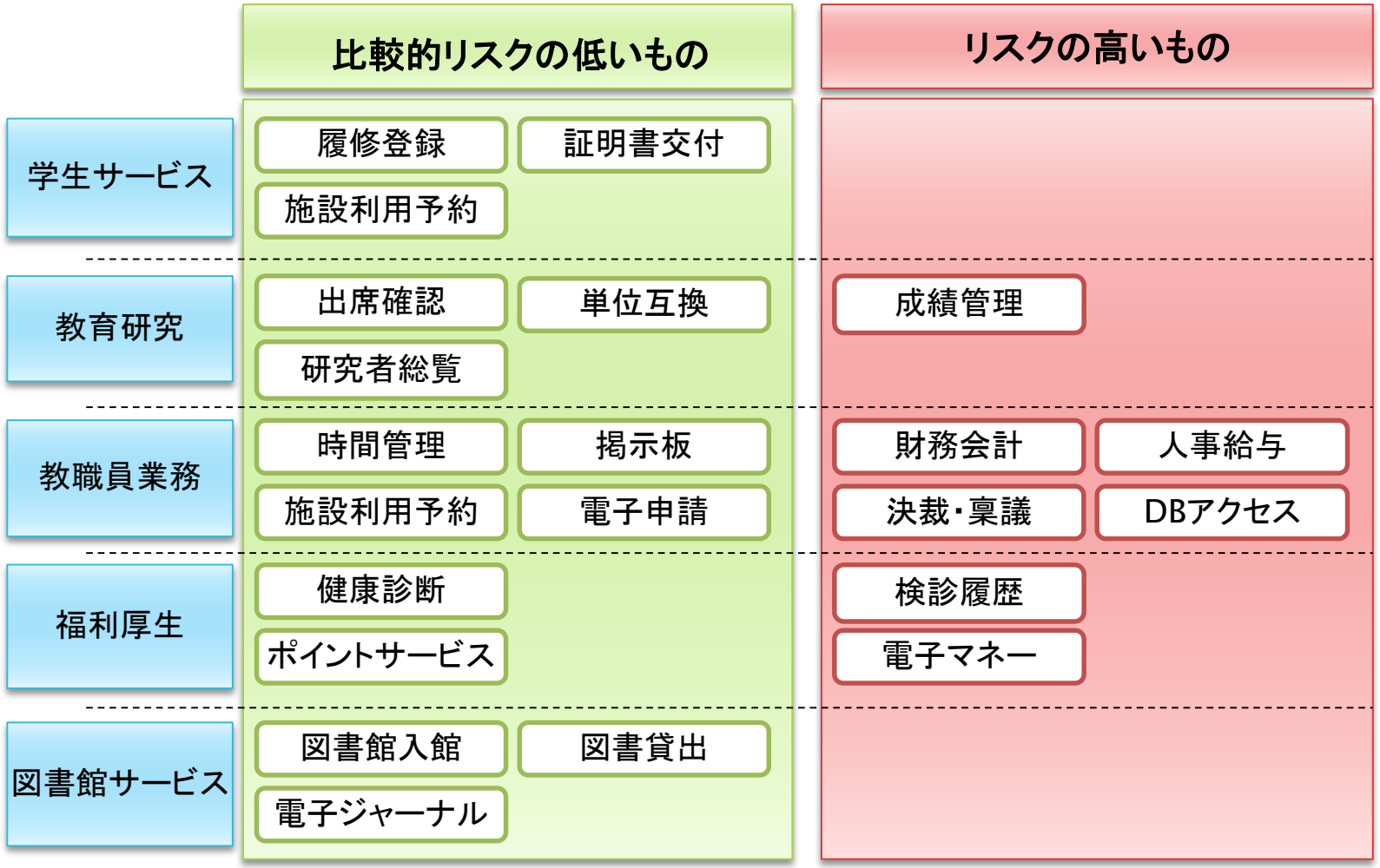
Level	Description
1 – Low	Little or no confidence in the asserted identity 身元確認不要、仮名 例：whitehouse.govのWebサイトでのオンラインディスカッションに参加
2 – Medium	Some confidence in the asserted identity 身元識別（身分証明書）、単一要素認証可、失効処理 例：社会保障Webサイトを通じて自身の住所記録を変更
3 – High	High confidence in the asserted identity 多要素認証 例：特許弁理士が特許商標局に対し、機密の特許情報を電子的に提出
4 – Very high	Very high confidence in the asserted identity 対面による発行、ハードウェアトークン 例：法執行官が、犯罪歴が格納されている法執行データベースにアクセス

OpenID 2.0はLoA-2まで対応、SAML/OpenID ConnectはLoA-4まで対応

LoA で定める認証強度要件

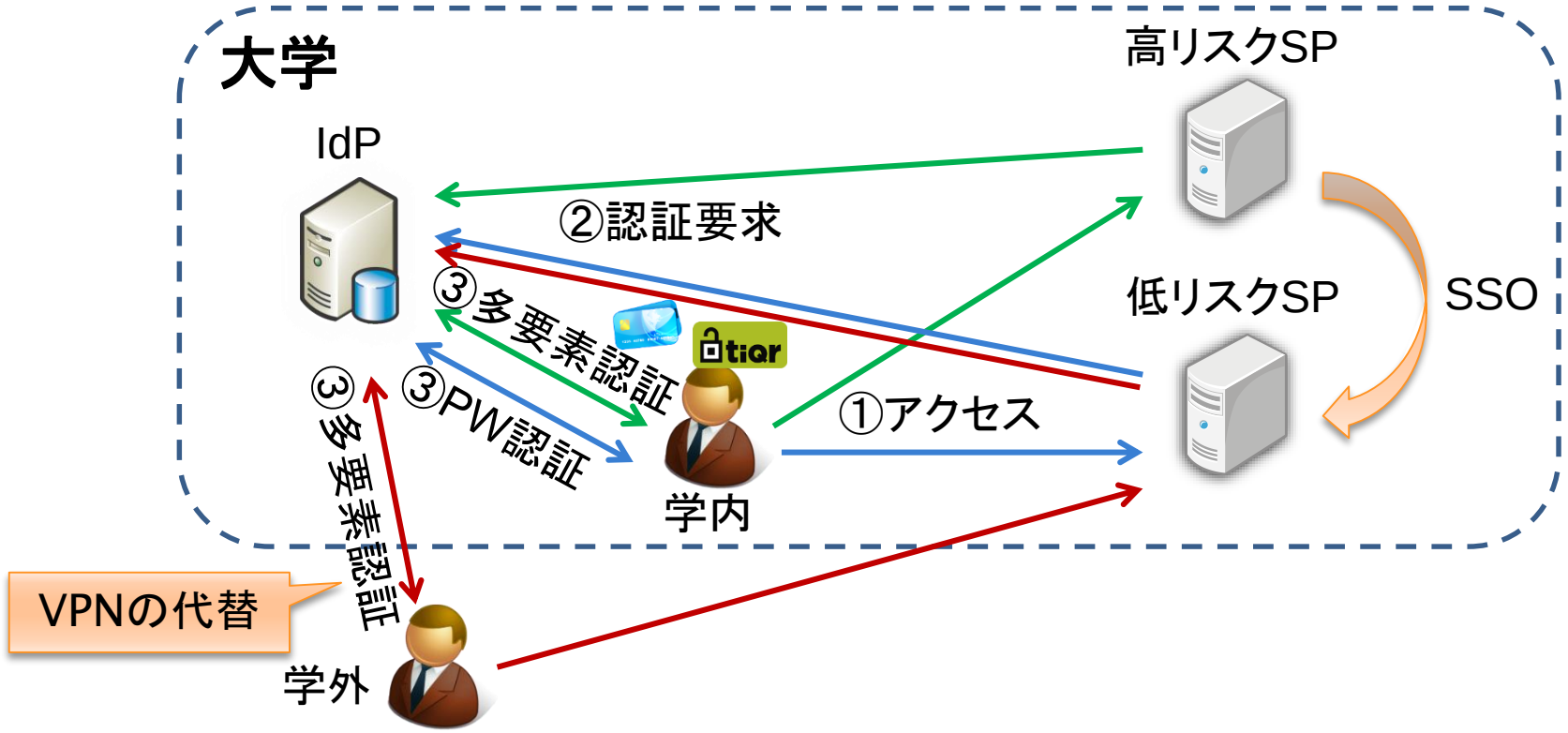
- レベル1
  翻訳版：http://www.ipa.go.jp/files/000025342.pdf
  - ユーザの同一性を保証（身元識別は不要）、認証の有効期限なし
  - チャレンジ-レスポンス可（辞書攻撃に弱い）
- レベル2
  - 単一要素認証、身元識別あり、失効処理の保証（ライフサイクル管理）
  - オンライン推測攻撃を防止すること（パスワード/TLS可）
  - 認証サーバでの平文パスワード保持の禁止
- レベル3
  - 複数要素認証、ソフト暗号化トークン使用可
  - なりすまし攻撃、中間者攻撃を防止すること
- レベル4
  - 実用上最大限の保証、ハード暗号化トークンを使用
  - 認証後の暗号化処理も認証プロセスに結びつく鍵を使用

サービス毎に要求される認証強度：リスクに基づくサービスの分類（例）



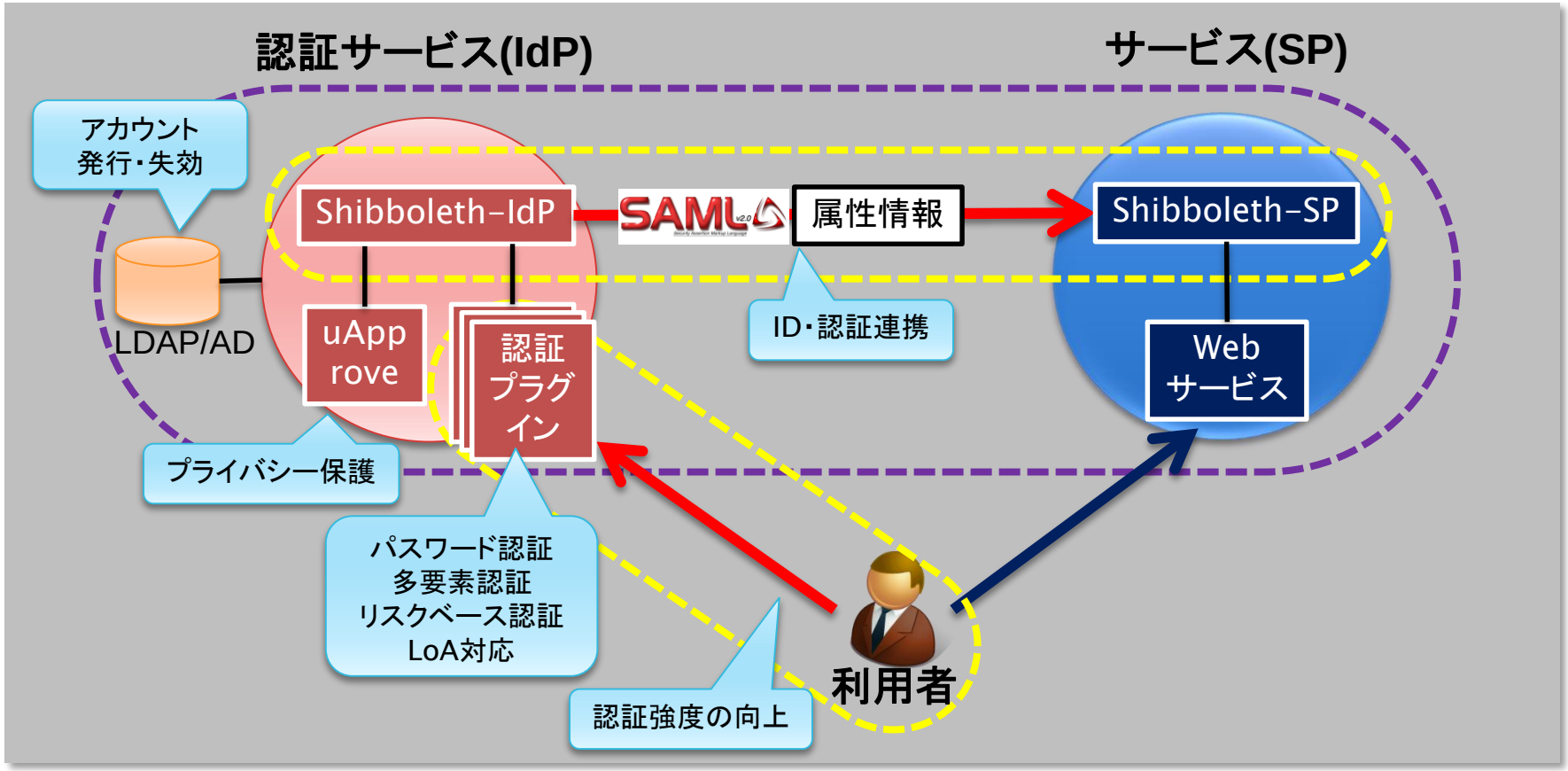
認証強度の使い分け

- SPのリスクレベルに応じた認証強度（方式）の切り替え
  - Shibboleth IdPへのプラグインとして開発中



IdPにおける運用管理のイメージ

- Shibboleth IdPでは、多様や認証方式やプライバシー保護をプラグインにより柔軟にサポート



高度な認証方式の導入

- 高度な認証方式
  - マトリックス
  - キャプチャ
  - ワンタイムパスワード
  - 電話によるコールバック
  - 電子証明書（クライアント証明書）
  - 生体情報
  - 組み合わせ
    - 二段階（二要素）認証
    - リスクベース認証
      - 利用環境の変化をチェック

	1	2	3	4	5
1	5	X	G	T	V
2	A	3	E	2	R
3	8	D	K	P	U
4	Z	4	J	M	9
5	Q	F	6	L	7

http://rsa.com/company/news/releases/images/SID800&SID7002.jpg

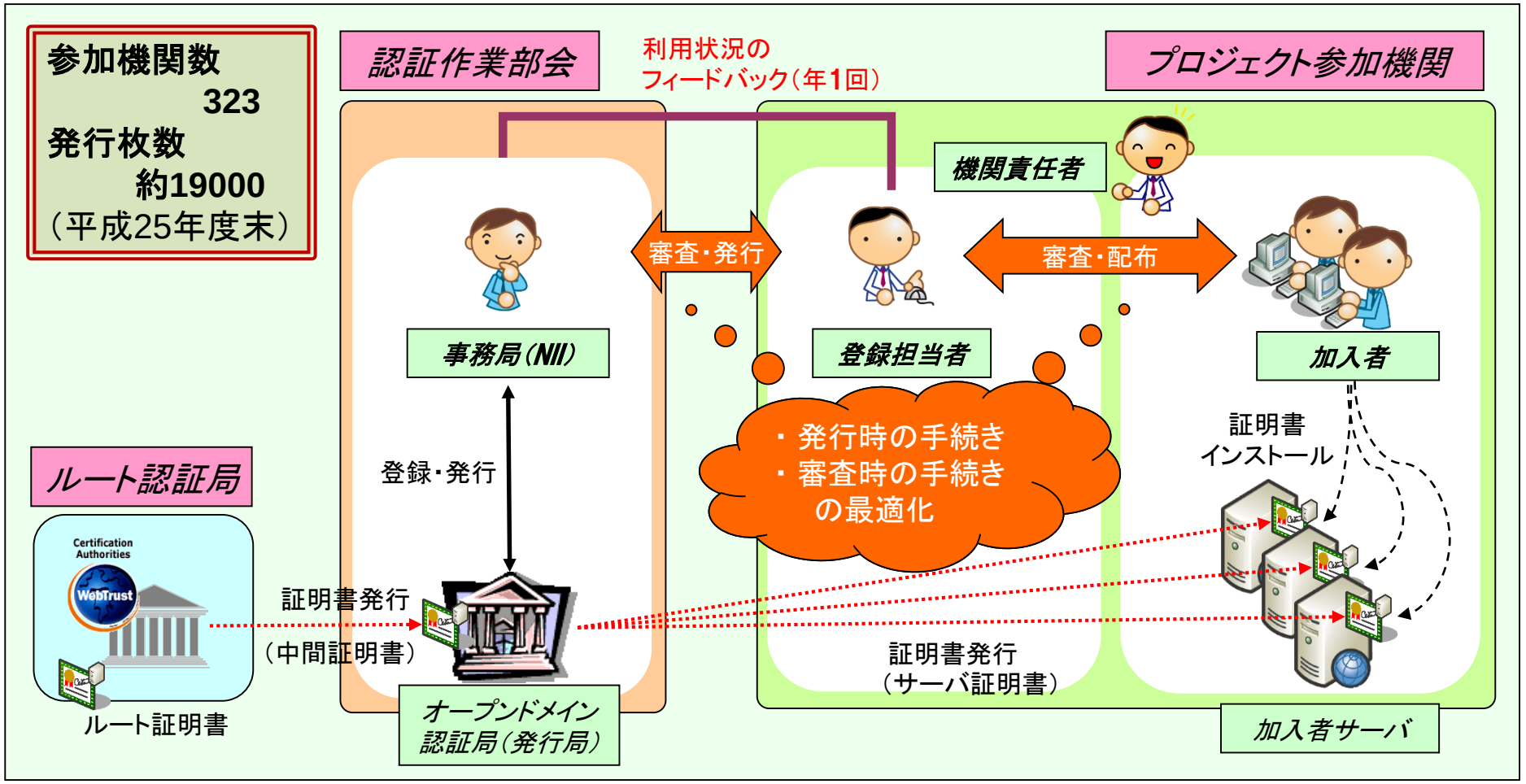
- 課題
  - 導入コストをいかに抑えるか
  - 時代と共に高度化が求められる

IdPの認証プラグインで対応

サーバ証明書の大学向け無償発行（2007年度～）

Webサーバ等の正当性の確認用証明書

- UPKIオープンドメイン証明書発行の「学術スキーム」



新UPKI証明書発行サービス(2015～)

～普及啓蒙、学術スキームの構築から，さらに次のステップへ～

- サーバ証明書

  - 従来のOV(Organization Validation)証明書だけでなく，より信頼性のレベルの高いEV(Extended Validation)証明書の発行
- クライアント証明書
  - 認証・署名・暗号化に利用可能な個人向け証明書の発行
    - 低コストで発行できるようにすることで普及啓蒙を図る

学認の普及も後押し

- 学内統合認証基盤の普及
  - 機微な情報を含む学内の多くのサービスに接続
- ID/Password認証の限界
  - クライアント証明書等を使ったセキュアな認証方法の必要性

クライアント証明書発行に関する経済効果

- 2012年度末アンケート調査
  - クライアント証明書使用中：41機関
    - 商用認証局から購入：10機関
    - 独自CA構築・運用：31機関
- クライアント証明書運用にかかる費用
  - JIPDEC JCAN証明書：初期8万円＋1,000円/人・年
    - 商用認証局から購入するともっと高価
  - 独自CAを構築すると導入に約6千万＋運用に約9百万/年（大規模大学での運用コスト例）
- 1万人規模の大学で導入すると1,000万円/年
  - 単純に40倍すると、**4億円/年** の経費が必要
    - この費用を大幅に圧縮
    - 大学での本格活用をきっかけに民間での活用が進むことを期待（特にS/MIME）

クライアント証明書の活用方法

- 発行方法
  - ユーザごと（サーバ証明書と同じ）
    - 大学担当者を経由して申請し、利用者が受領
  - バルク
    - 大学担当者がまとめて申請し、まとめて受領

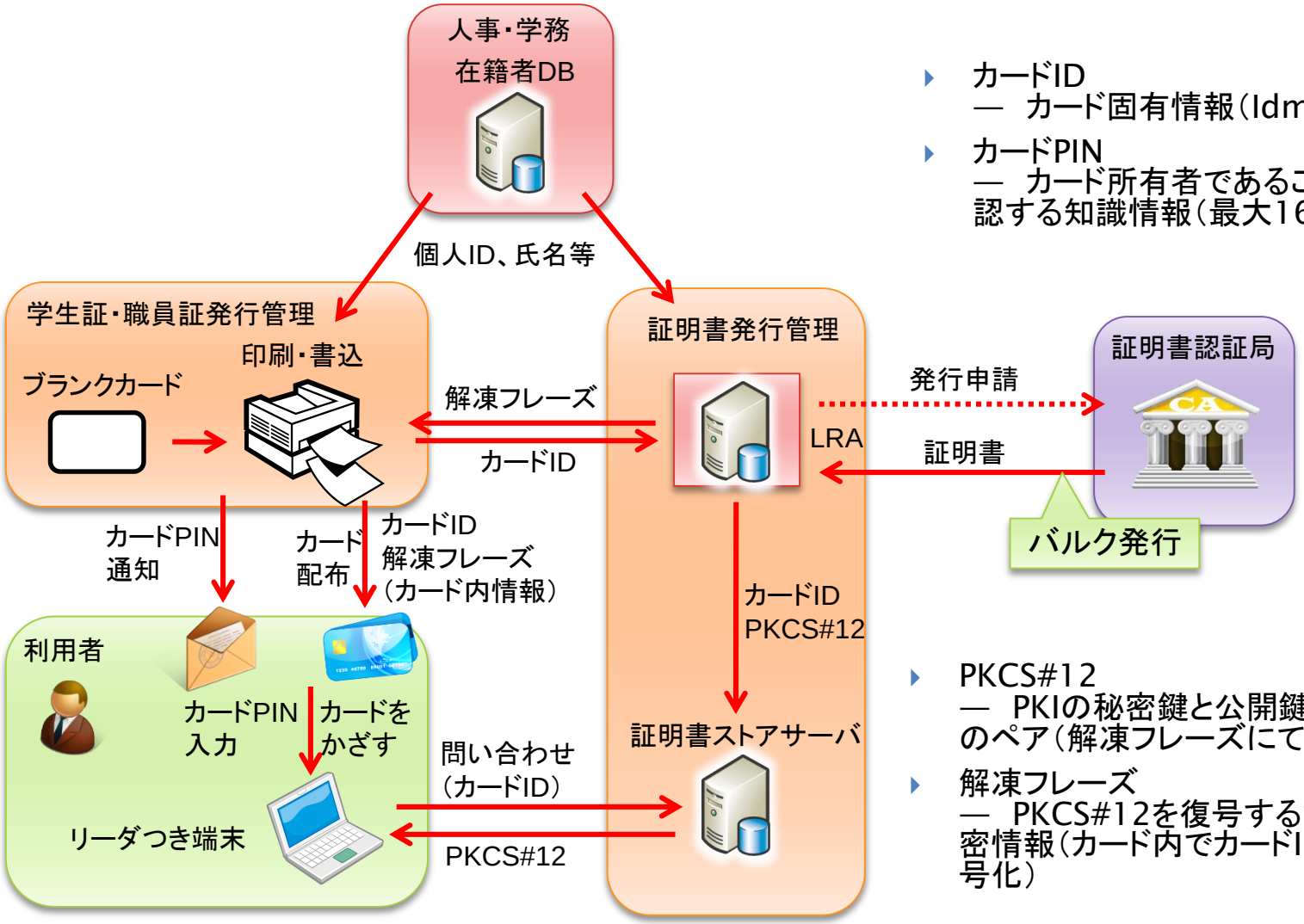
- 発行・配布の単位（複数の端末を利用するユーザがいる場合）
  - ユーザごと
    - 端末紛失等で、当該ユーザの全端末において証明書再インストールが必要。
  - 端末ごと
    - 認証/署名用途では問題なし。電子メール（S/MIME）の暗号化利用に難あり。

- 活用形態
  1. ユーザに証明書を配布し、ユーザ自身がインストール
  2. ICカード型学生証・職員証と組み合わせて利用
     - 証明書をICカードに書き込む方式（TypeB/Javaカード）
       - 証明書の更新作業が少し面倒
     - 証明書サーバと連携する方式（フェリカ FCF）
       - 証明書の更新作業が比較的容易

証明書サーバと連携するICカードの利用形態

- Felicaカードを用いるが、証明書を書き込まず、証明書サーバから秘密鍵と公開鍵証明書を取得して利用する方式
- メリット
  - FelicaカードはTypeB/Javaカードより安価
    - リーダやアプリケーションも安価
  - 証明書をカードに保存しないため、証明書の更新処理にカード側の処理を不要にできる
    - 証明書の有効期限がカードの有効期限より短くても良い
  - 他の用途（アプリケーション）との共存に有利
    - カード上に大きな領域の確保が不要
- JIPDECの「JCANパス方式」をベースに詳細検討中
  - 新名称：UPKIパス？

JCANパス方式の運用イメージ



- カードID
  - カード固有情報（Idmなど）
- カードPIN
  - カード所有者であることを確認する知識情報（最大16文字）

- PKCS#12
  - PKIの秘密鍵と公開鍵（証明書）のペア（解凍フレーズにて暗号化）
- 解凍フレーズ
  - PKCS#12を復号するための秘密情報（カード内でカードIDにて暗号化）

大学における商用クラウドサービス

- 研究教育基盤としてクラウドの利活用を促進することは今後不可欠。
- 大学等が提供するサービスに加えて，商用クラウドサービスも利用すべきである。
- 商用クラウドサービスの利用では，安全性とコストに関する問題があり，大学等がクラウドを利用する上での障壁となっている。

（日本学術会議「我が国の学術情報基盤のあり方について（提言）」、平成26/5/9、p.14-15）
http://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-22-t192-2.pdf

- 大学等の限られた（削減される）予算の中で、さらなる情報基盤環境の拡充を支援する枠組みの実現が望まれている

NET+（ネットプラス）サービス (米国Internet2)

- クラウドサービスの恩恵を効果的に享受する戦略
  - 最先端ネットワーク、ID連携、学術研究コミュニティの営業力を総合して民間サービスと効果的に連携

オランダ(SURFconext)やイギリス(Janet Brokerage)等にも同様の枠組みが存在

- ポイント
  - 学術機関がスポンサーとなり、教育研究における要求を実現
    - Tailored Services
  - 教育研究ネットワークの活用
  - 大幅なコスト削減
  - アカデミックディスカウント
  - 契約のとりまとめ
  - 学術機関とプロバイダーの両者にメリット

2014 – Over 300 campuses have participated and subscribed over 620 times to an Internet2 NET+ Service

collectively receiving $200M+ benefit

200億円以上の経費削減効果

NET+ Cloud Service Providers

Current Services Portfolio – **50** Services

IaaS – Infrastructure, Platform, System Security as a Service

VVC – Video, Voice and Collaboration as a Service

Content - Digital Content for Research and Education

SaaS – Software as a Service

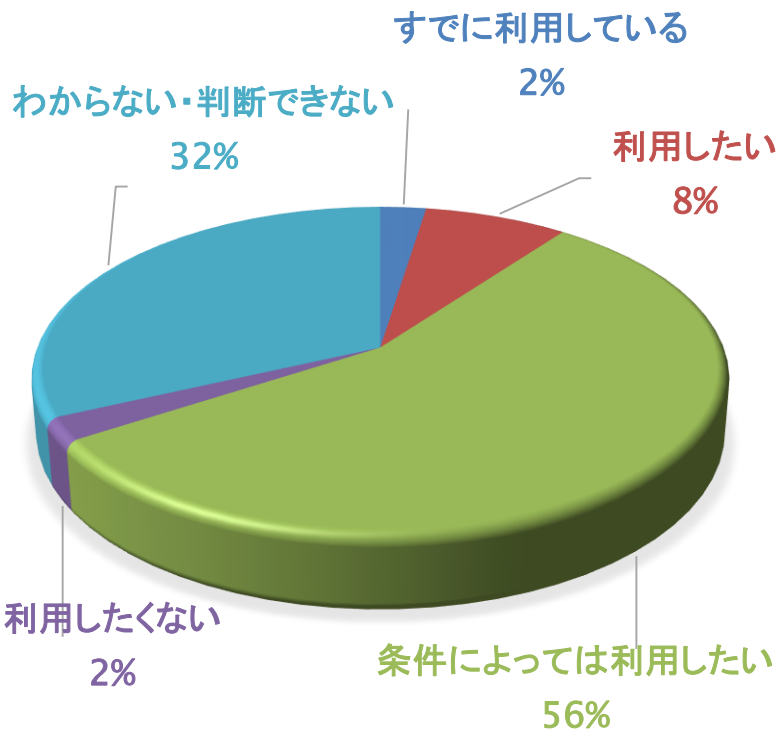
IaaM – Trust and Identity

http://www.internet2.edu/cloud-services/

クラウドへの期待と不安

- クラウドを「利用したくない」大学は少数派
  - 「条件によっては」もしくは「わからない・判断できない」という回答が9割近くも！
- 普及へのキーワードは
  - 「セキュリティ」
  - 「カスタマイズ」
  - 「コスト」
  - 「通信速度」
    - 学術機関は企業に比べて，セキュリティを理由にクラウドを敬遠する率が高い

Q: アカデミッククラウドを利用したいか？



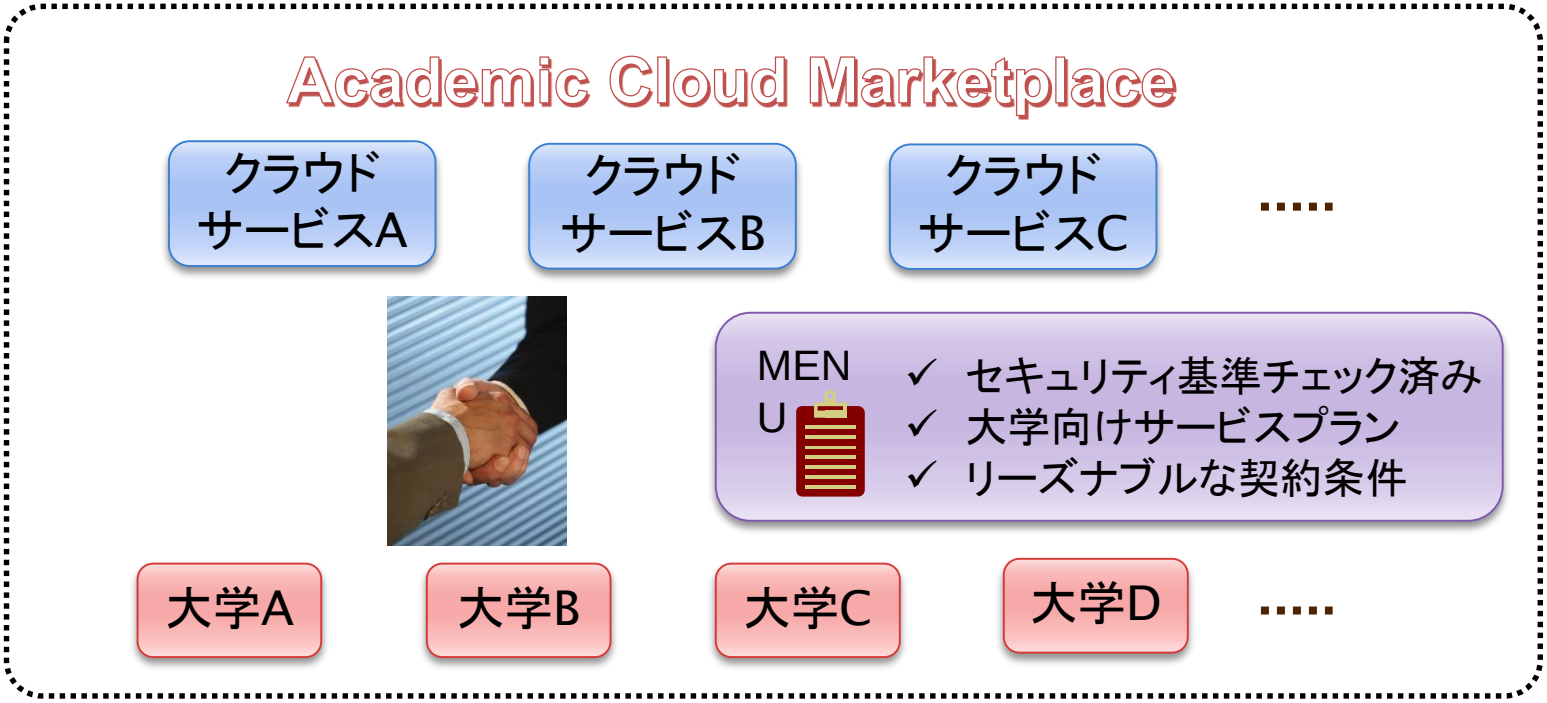
（『コミュニティで紡ぐ次世代大学ICT環境としてのアカデミッククラウド』最終報告会資料「セキュリティに係るアカデミッククラウドシステムの調査検討」をもとに作成）

http://www.icer.kyushu-u.ac.jp/sites/default/files/AC_last_report_document_2.pdf

クラウドの活用を促進するには？

- 「一定のセキュリティ基準を満たした商品」
- 「大学向けに最適化されたサービスモデル」
- 「面倒な交渉は不要，お手ごろな契約条件」

- 洗練された商品が並ぶマーケットプレイスが役立ちそう？



日本版「NET+」の目指すもの

セキュリティ	・学認によるセキュアな認証 ・セキュリティをチェックリストで確認
カスタマイズ	・大学のニーズに基づいたラインナップ ・自分の大学にぴったりの商品を選べる
コスト	・ワンストップで商品情報を収集・比較 ・アカデミック価格で購入可能

サービス選択基準・チェックリスト

- 「広島大学　クラウドサービス利用ガイドライン チェックリスト」をベースに作成

広島大学 クラウドサービス 利用ガイドライン

http://www.media.hiroshima-u.ac.jp/news/cloudguide

- 大学図書館コンソーシアム連合「JUSTICE標準提案書」を参考に，契約関係の事項を補足

JUSTICE 大学図書館コンソーシアム連合

http://www.nii.ac.jp/content/justice/

- 基本となるチェックリストを1本作成
  - サービス分野ごとに特有の評価項目を補い，バリエーションを作成していくことを視野に・・・

サービス選択基準のイメージ (クラウドストレージ)

研究データのバックアップ長期保存(データの耐久性、価格重視)
- データの高耐久性に関するSLA
- アクセス頻度小
- 低価格

サービス	SLA	データ多重化	暗号化	データアクセス	国内DC利用	準拠法	料金(100GB・月額)
A社	サービス稼働率=99.9%	有	有	即時	無	米国法	600円(30GBまで無料)
B社サービス1	サービス稼働率=99.95% データ耐久性=99.999999999%	有	有	即時	有	米国法	330円
B社サービス2	サービス稼働率=99.95% データ耐久性=99.999999999%	有	有	3-5時間待ち	有	米国法	114円
C社	サービス稼働率=99.95%	有	有	即時	有	米国法	900円
D社	サービス稼働率=99.99%	有	有	即時	有	日本法	1,100円
E社	サービス稼働率=99.9%	有	無	即時	無	日本法	799円(7GBまで無料)

学務データ(個人情報含む)の保存(データの安全性重視)
- データ暗号化
- 国内DCかつ日本法準拠事業者

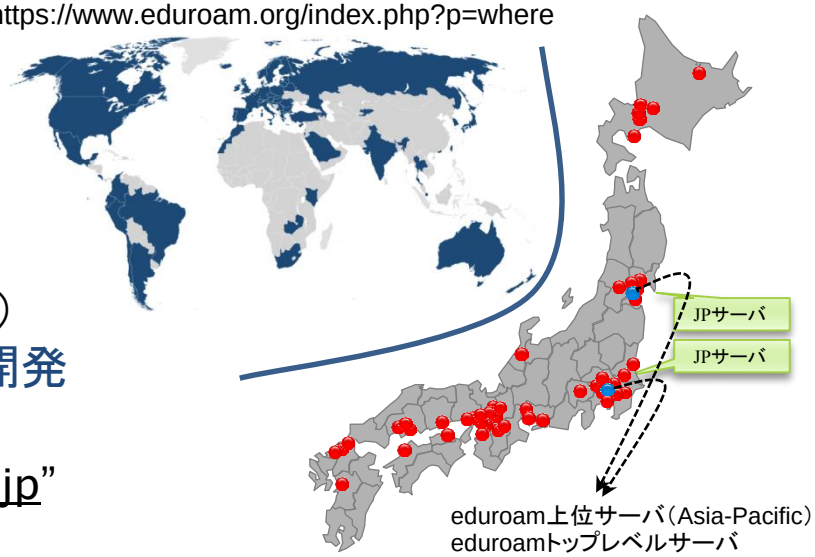
日本版「NET+」の進め方（案）

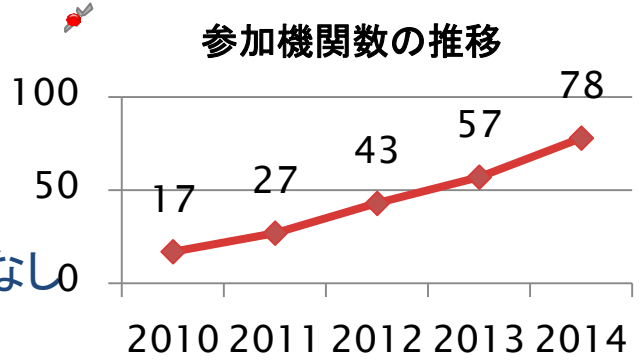
- 大学 / ベンダー / 事務局の協働で，サービス分野ごとに，クラウドサービス選択基準・チェックリストを作成します。
- 日本版「NET+」に提案したいサービスをお持ちのベンダーは，チェックリストでの確認結果とあわせて，事務局にサービスをご提案いただきます。
- 事務局ではサービス分野ごとに提案をとりまとめ，チェック結果一覧のリストを作成，参加大学に公開します。
- 各大学は自学のニーズに合わせてサービスを選択。
  契約は各大学とベンダーが個別に行います。
- 日本版「NET+」で取り扱われるクラウドサービスを利用する際は，学認による認証を必須とします。

国際学術無線LANローミング基盤「eduroam」

- 欧州TERENAで開発された教育・研究用の学術無線LAN (wifi)ローミング基盤
- 国際的デファクト・スタンダード
  - 世界70か国・地域で展開
- 日本は「eduroam JP」の名称で参加
  - 78機関が参加（2014/9現在）
    - 原則として学術研究機関が対象（参加無料）
  - NIIと東北大学が共同で運用支援、技術開発
  - 訪問先の無線LANが無料で利用可能
    - ESSIDは“eduroam”、IDは”user@大学名.jp”
    - 互恵の精神に基づくサービス
    - 関東地域の貸会議室やカフェ等の一部でも利用可能（約130か所）
- メリット
  - 802.1X方式による安全なユーザ認証
    - クライアント証明書も利用可能
  - Windows/Mac/スマートフォン等に対応
  - 来訪者のためのネットワークを毎回構築する必要なし
  - 「学認」とも連携可能

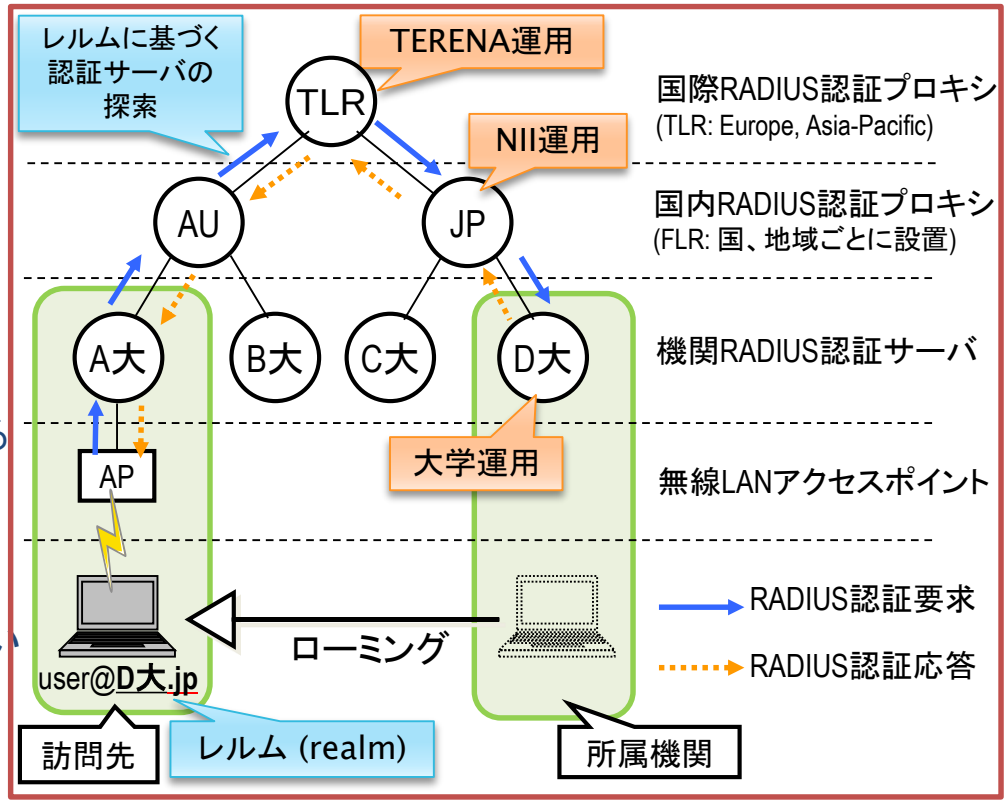
https://www.eduroam.org/index.php?p=where





eduroamの仕組みとメリット

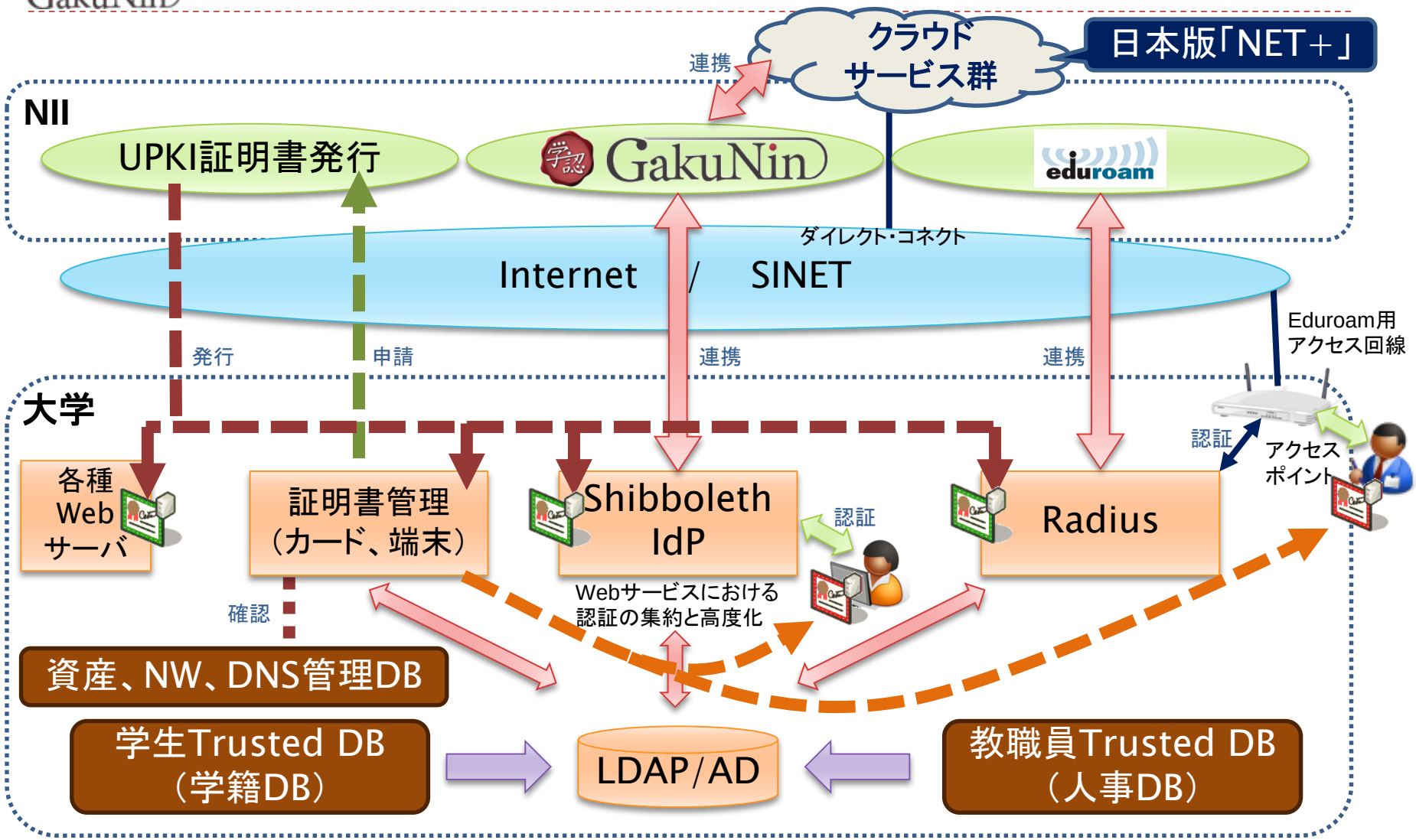
- 学術機関同士で訪問先の無線LANを無料で利用できるようにする仕組み
  - 学術機関同士でお互いの構成員が、お互いに訪問先の無線LAN利用を認める互恵の精神に基づくサービス
  - 受け入れ側は、無線LANに一時的なパスワードを設定するなど来訪者向けネットワークを毎回設定しなくてもよくなる
  - 利用者は、いつも自機関で使っているID、パスワードをそのまま利用して訪問先の無線LANが利用できる
- 所属する機関のアカウントがそのまま利用できる
  - "user@大学名.jp"
    - 例：xxx@nii.ac.jp、aaa@u-tokyo.ac.jp
- 無線LANの国際標準認証方式(IEEE 802.1x)による安全なユーザ認証
  - 利用する機種を選ばすいつも自分が使っているWindows/Mac/スマートフォン等で利用ができる
  - Web画面でIDとパスワードを入力する認証よりも安全性が高い
    （成りすまし基地局によるフィッシング防止）
  - クライアント証明書を利用すれば、推測されやすいパスワードより安全性の高い接続が可能となる



eduroam参加のための準備

- 認証(Radius)サーバの選択肢
  1. Radiusサーバを構築・運用
     - 学内アカウントをそのまま利用することが可能
  2. 代理認証サービスを利用
     - eduroam専用アカウント発行サービス
  3. 仮名アカウント発行サービス(学認連携)を利用
     - 学認用のIDを用いてeduroam用一時アカウントを発行
  - クライアント証明書による利用者認証も可能
- 無線ネットワーク
  - ゲスト用に用いるIPアドレスの選択肢
    1. 自機関が保有する別IPアドレスブロックを利用
    2. 商用回線を導入し、その回線に付随するIPアドレスを利用
    3. SINETからeduroam用アドレス(IPv4/v6)の割当を受ける
  - 認証時のレルムを見て、自機関のユーザを自機関ユーザ向けネットワークに振り分けておくと、利便性が高い
  - Eduroamに対応した民間サービスプロバイダによるキャンパス無線ネットワーク構築・運用サービスもある

大学における情報基盤の認証を中心としたイメージ



まとめ

- **大学における安全・安心な情報基盤の構築支援**
  - 学術認証フェデレーション「学認」
    - 認証基盤の共通化による管理コスト削減、利便性向上、セキュリティ強化、プライバシー保護
    - サービスのレベル分けによる複数の認証強度の併用
  - UPKI証明書サービス
    - クライアント証明書の活用による認証強度の向上
  - eduroam

GakuNin（2014年1月14日より「事業」として運用）

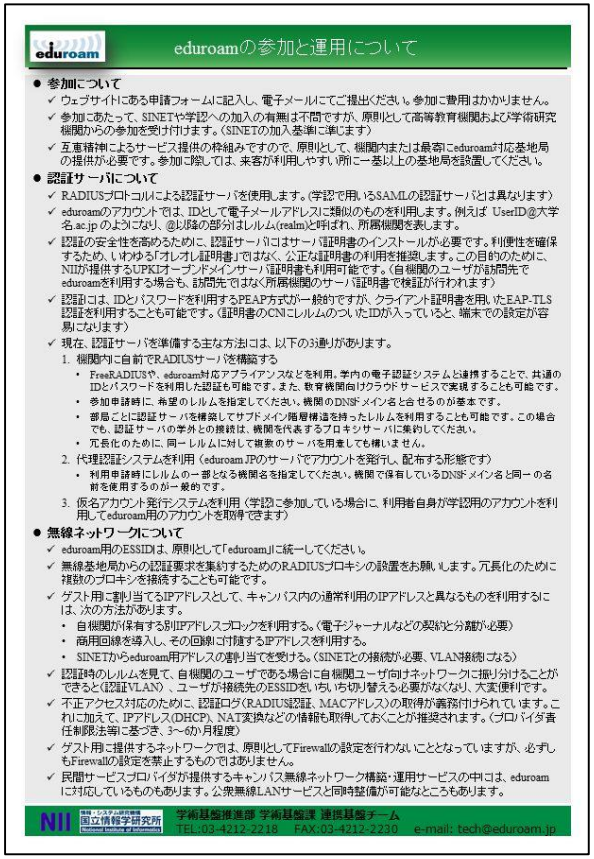
UPKI 証明書発行サービス（2015年1月より「事業」として提供開始予定）

eduroam

- **さらに、大学における情報環境の向上に向けて**
  - 日本版「NET+」の検討（名称募集中）

様々な疑問に答える
道しるべ文書「参加と運用について」公開中

http://id.nii.ac.jp/1149/00000228/



http://www.eduroam.jp/docs/eduroam-JP-flyer.pdf