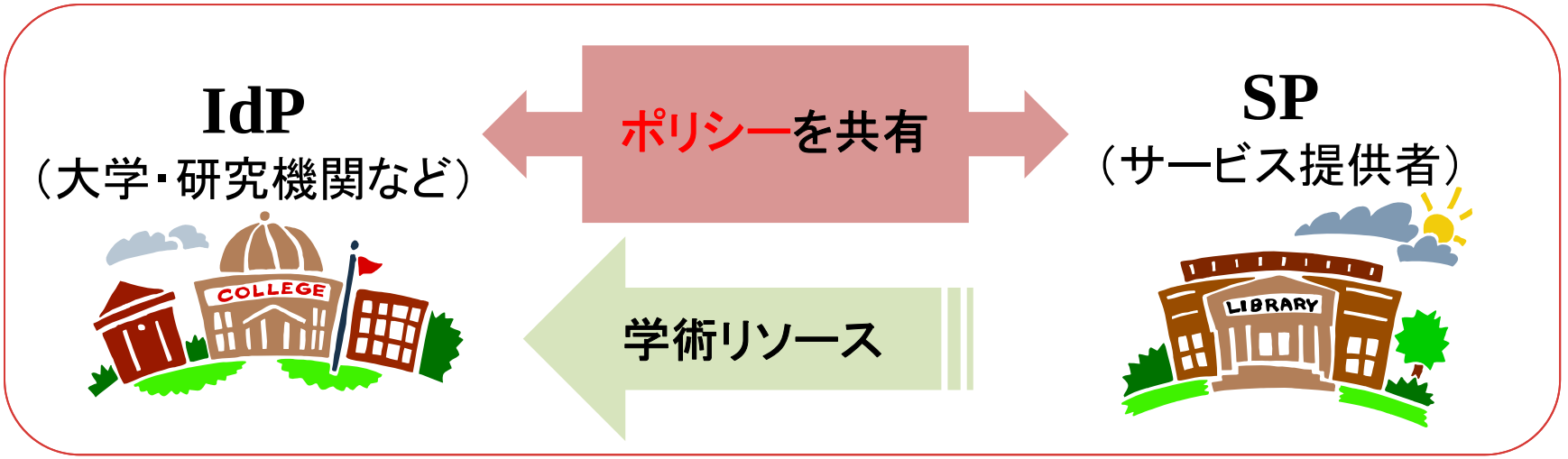
学認の現状と今後の展望

国立情報学研究所

作成日：2011年10月20日

学術認証フェデレーションとは

IdPとSPの信頼の輪

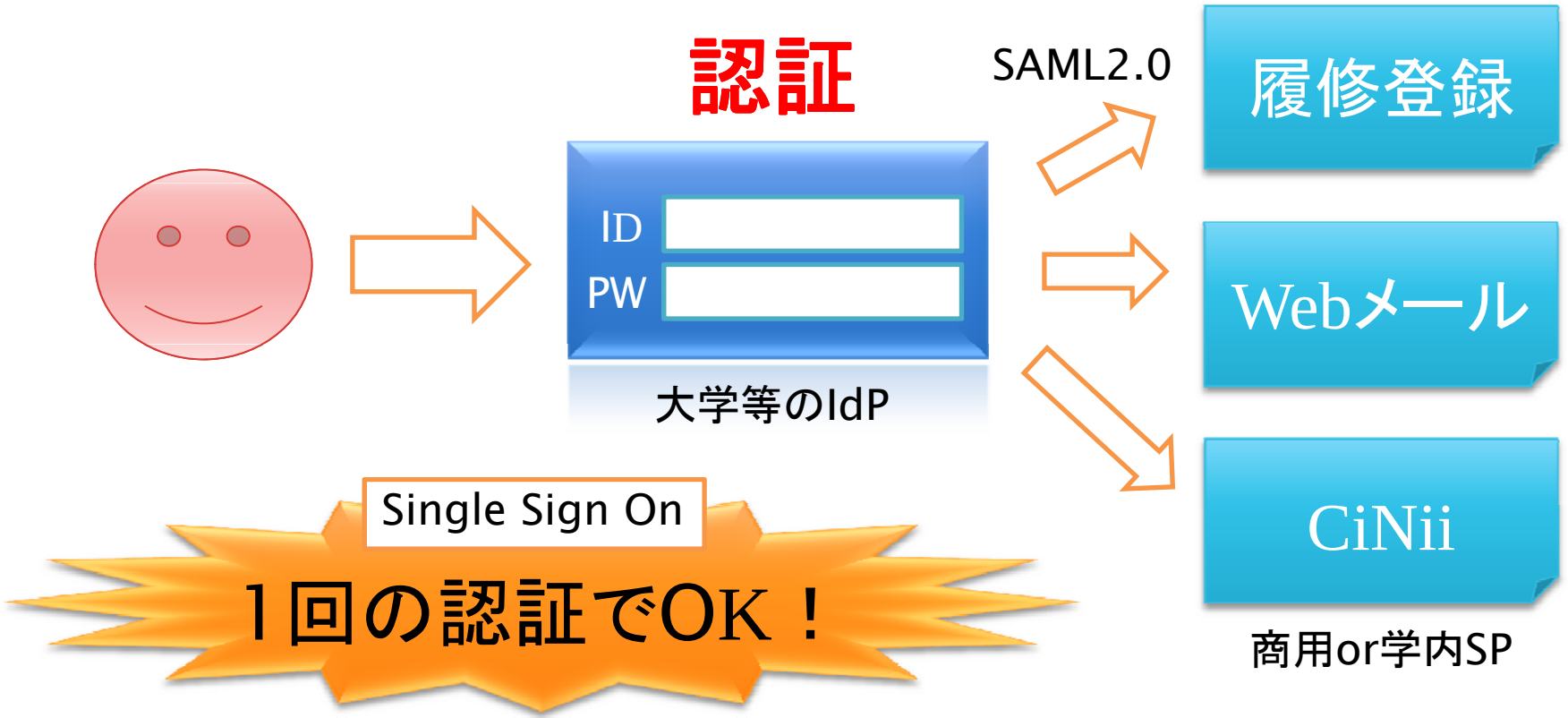


- ポリシーを信頼し合うことで認証連携を実現
- 学術リソースを利用・提携

日本の学術認証フェデレーションは「学認」

学認のメリット

1つのIDとパスワードで色々なサービスが使える！



学認における認証のフロー

ブラウザ画面の推移

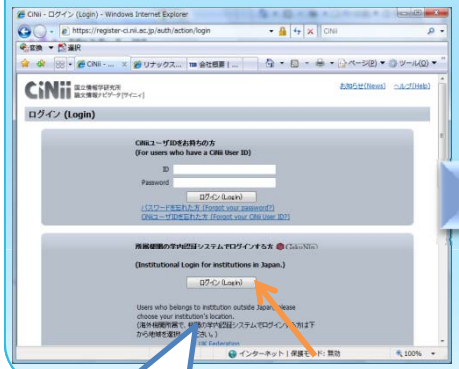
認証成功

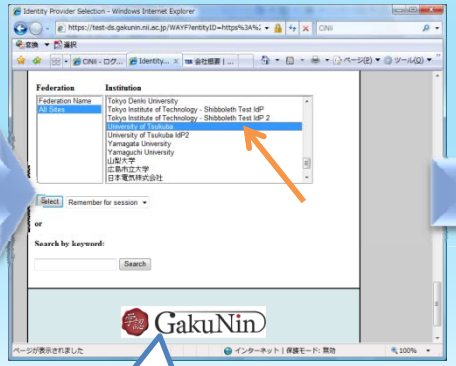
①Shibboleth認証

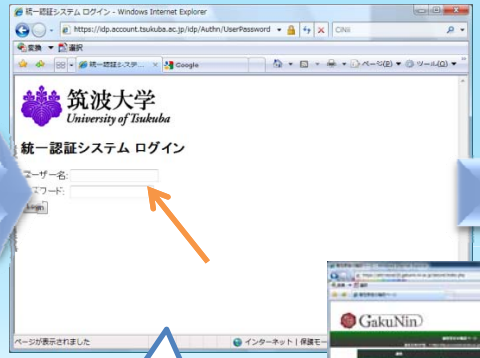
②所属機関を選択

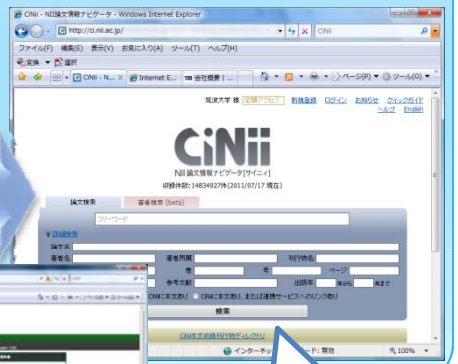
③IDとPWを入力

④画面が表示される









SP
（リソース提供者）

DS
（ディスカバリーサービス）

SP

IdP
（所属機関）

SAML
（属性抽出）

SP
（リソース提供者）

学認のメリット

具体例

- 個人情報入力の機会が軽減
- どこからでもサービスの利用が可能
- ID･PWの使い分け不要
- サービス運営側の負担を軽減

学認によるメリットの事例

- **EJリソースへのリモートアクセス利用の申請業務削減**
  - 学認に参加することで学生や院生もSSO環境で学内外を問わず気軽に使えるようになり、利用者の反応も良い。しかも、図書館の担当者からは、学外利用のための申請業務が激減して業務が軽減されたという声も出ているなど、好意的に受け入れられている。（山形大学：Case Study No.02）
- **学生専用用サイト利用のためのコスト削減**
  - 例えば、Microsoft社のDreamSparkを使うには国際学生証が必要だったが、学認に参加することでこの発行コストが不要になるなど、学認が提供するサービスを利用している学生や教員から、便利になったという声を多く聞く。（成城大学：CaseStudy No.06）
- **遠隔講義のためのコスト削減**
  - 学認が提供するFaMCUsは、パソコンを使っての利用にも対応しており、教員の創意工夫を活かした遠隔授業の実現や、他にも通常の会議や学生との個人面談など、学生・教職員のコミュニケーションツールとしての活用にも期待が高まる。（日本大学：CaseStudy No.07）
- **学内ID管理工数の削減**
  - 学内向けとしてShibboleth対応のサービスが約20稼働しており、ピーク時で1日1万1千件、平均で1日5千件（学生数は約1万人）程度の利用があるが、問題なく稼働している。ID統合前の課題でもあった、複数の立場を持つ利用者への対応も自動処理できるようになり、個別対応から解放されるなど業務の簡略化にも貢献できている。（金沢大学：CaseStudy No.09）
- **LMSの大学間連携によるコスト削減**
  - eK4や本学の取り組みは、Shibbolethを活用した地域限定の大学間連携であるが、この規模を拡大し、全国の大学がコンテンツを蓄積しているLMSを学認がサービスとして提供できるようになると、大学間連携の大きなブレークスルーになると期待している。（徳島大学：CaseStudy No.13）

学認ケーススタディシリーズ

https://www.gakunin.jp/docs/fed/info

- 学外サービスとの認証連携に備えて／北海道大学
- 認証基盤も冗長構成化して可用性を向上／山形大学
- 電子図書館サービスにShibbolethを導入／筑波大学
- 図書館主導で実現したShibboleth認証／千葉大学
- 情報リソースの共有で運用コストを低減／東京農工大学
- 学認が実現する日本の学力水準の向上／成城大学
- キャンパス間をつなぐ遠隔授業／日本大学
- 学認のサービスが応える医療系大学のニーズ／東邦大学
- 学内/学外サービスの双方に認証基盤を用意／金沢大学
- 京都大学 独立した組織間での認証連携を実現／京都大学
- 大学間共用e-ラーニングシステムへの活用／京都産業大学
- ゲスト利用者のネットワーク認証に活用／広島大学
- 大学間認証連携のキラーコンテンツLMS／徳島大学
- 統合認証基盤とSingle Sign-On連携／佐賀大学

参加機関 https://www.gakunin.jp/docs/fed/participants

学認で利用できるサービス

- 図書館系EJ, DB
  - Science Direct, SCOPUS, SpringerLink, Web of Knowledge, OvidSP, RefWorks, ebrary, Cambridge Journals Online, EBSCO host, 研究社KOD, IEEE Xplore, Serials Solutions, CiNii, NII REO
  - 学認ライブラリチームにて接続対応中サービス
    - PubMed, JSTOR, Karger, IOP, Emerald, Cengage, Wiley, Royal Society of Chemistry, Thieme, ProQuest, Nature…
- 情報系コラボレーションツール
  - TV会議（NII），ファイル共有（NII, 金沢大），eScienceプラットフォーム（山形大，金沢大），ネットワーク接続（eduroamshib, 広島大，佐賀大），eLearning（NII），予定調整（UNINETT，アットウエア）
  - GakuNin mAPを軸にコラボレーションを強化
- 学内システムのSP対応状況
  - メールサービス（商用），履修登録システム（商用），給与システム（商用），図書館業務システム（商用），ポータルサイトシステム（商用），学内LAN（OSS），設備予約・グループウエア（商用，OSS），掲示板システム（商用），LMS（商用、OSS），SNS（OSS），CMS（OSS），リバースプロキシー（商用）

学認への参加方法

- 学認申請システム
  - 学認への参加申請，メタデータ登録・更新等がWebを通してオンラインで可能

- テストフェデレーション（技術検証環境）
  1. 申請情報登録（およびアカウント作成）
  2. 事務局での参加承認
  3. フェデレーションメタデータの自動更新

通常一日で
参加完了
利用開始可能

学認が提供するテストSPやIDPを利用して接続確認

- 運用フェデレーション（実アカウントを用いた本格利用）
  - オフラインによる確認が1ステップ増えるだけ

実施要領，システム運用基準が守られていることが前提

Shibboleth環境の構築研修会

- 日程：年3回程度実施，来年度も同様に予定
- 場所：国立情報学研究所　20階実習室
- カリキュラム
  - 1日目午前　：学認とは何か？
  - 1日目午後　：Shibboleth IdP導入実習
  - 1日目夜　　：情報交換会
  - 2日目午前　：Shibboleth SP導入実習
  - 2日目午後　：応用演習

大学向け研修会詳細
http://www.nii.ac.jp/hrd/ja/joho-karuizawa/index.html　に掲載

IdPホスティング実験

- 趣旨
  - 学認に参加したいが、費用、体制、システム等の面で、準備に時間がかかっている機関の存在
  - IdPホスティングによるスタートアップ支援
    - 需要調査
    - 技術的要件調査
    - 継続的なIdPホスティングサービスのありかた検討
- 方法
  - NIIにてIdPホスティング用の環境を用意
    - ユーザ情報は、エクセル等での登録 / 大学のLDAPとの接続
- 問い合わせ先
  - idp-hosting@nii.ac.jp

学認アンケート調査

- 趣旨
  - 学認では、定められた規定（ポリシー）を信頼し合うことで、IdPとSPの間で相互接続が可能
    - 学術認証フェデレーション実施要領
    - 学術認証フェデレーション システム運用基準
  - 信頼関係（トラストサークル）を保つことは、参加機関に対し学認が果たすべき重要な役割
- 方法
  - 各機関にIdP運用の自己評価アンケートを実施
  - アンケートの内容は，ポリシーに基づいた運用を確認する簡単なもの
  - 平成23年10月より順次実施
- 効果
  - 定期的な運用の確認を必要とするPubMedなど，米国NIHが提供する95のサービスに接続可能

この意味とは？

Level of Assurance

- NIHのサービスを学認SPとして利用
  - 米国連邦政府内のサービス(SP)を、外部の認証システム(IdP)に接続する場合には、SP側がIdPの保証レベル(Level of Assurance, LoA)を要求。
  - 4つのレベルを規定
    - レベル1: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
    - レベル2:社会保障Webサイトを通じて自身の住所記録を変更
    - レベル3: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
    - レベル4: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
  - PubMedの要求はLevel 1(最低)であり、利用するためには学認のIdPが米国の基準に則ったLevel 1を取得する必要あり。

  - 学認は、学認のIdPにLevel 1を発行できるTrust Framework Providerになる必要あり。

- 日本政府もLoAに関するガイドラインを策定

日本政府における電子認証ガイドラインとLoA

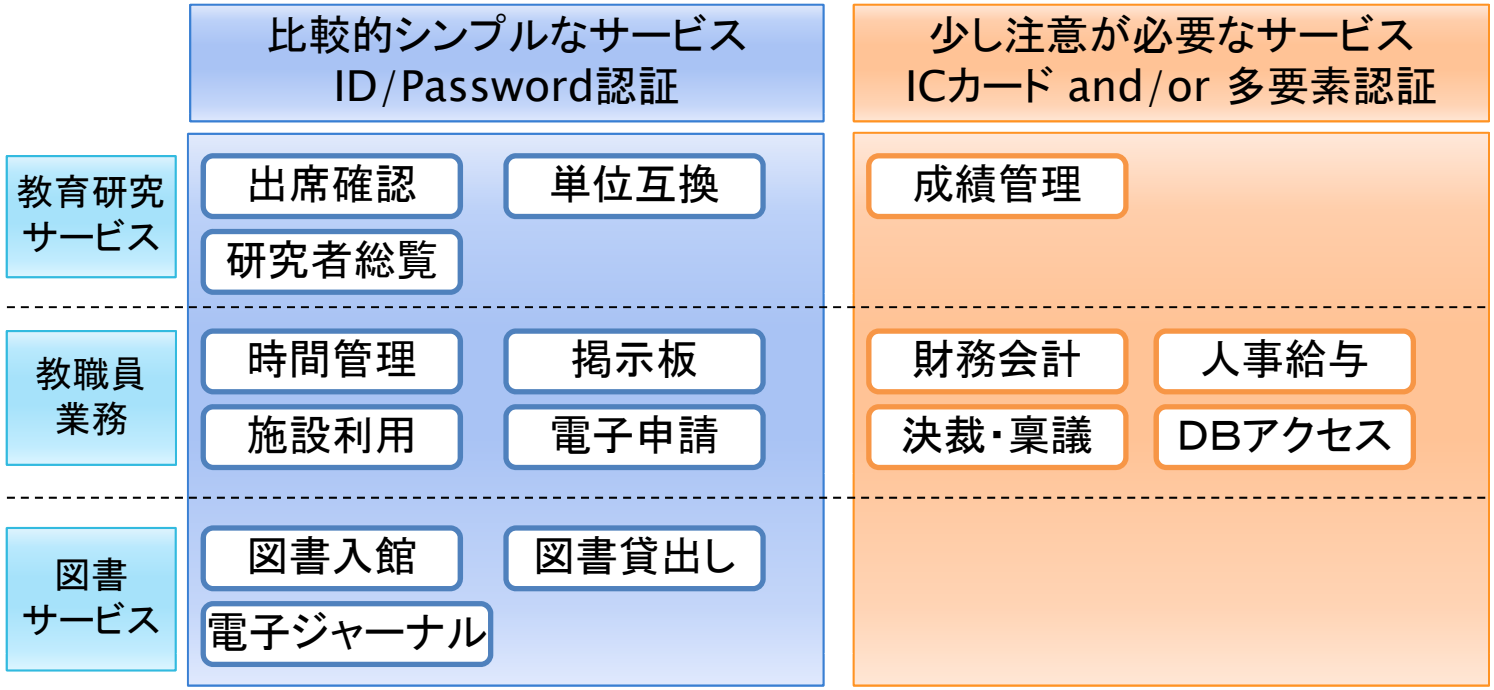
- オンライン手続きにおけるリスク評価及び電子署名・認証ガイドライン
  - 我が国の電子政府における認証方式の設計にあたり活用可能な「ものさし」を確立することを目的として策定。
  - ガイドラインは、対象となる電子手続に関するリスク評価手法とこの手法により導出される「リスクの影響度」、影響度に応じた認証方式の「保証レベル」の導出、各保証レベルに求められる対策基準を規定。
  - OMB M-04-04やNIST 800-30など米国政府を参考

＜主な対策基準＞

保証レベル	登録	発行・管理	トークン	認証プロセス	署名等プロセス
レベル4	**（窓口）** ・写真付き身分証明1種の提示 ・申請情報の台帳照合 ・重複登録ではないことの確認	・手渡し、本人限定受取郵便、によるトークン発行	・レベル3の基準に加え、耐タンパ性が確保されたハードウェアトークンを利用すること	・レベル3と同等の基準	・電子政府推奨暗号リストに記載の署名方式 ・電子署名用の証明書の用途は電子署名限定
レベル3	**（窓口）** ・写真付き身分証明1種（or他2種）の提示 ・申請情報の台帳（又は公的証明書）照合 **（郵送 or オンライン）** ・申請書に対する電子署名 ・申請情報の台帳（又は公的証明書）照合	・レベル4の方法に加え、書留郵便、書留郵便＋ダウンロード、電子署名＋ダウンロード、によるトークン発行	・レベル2の基準に加え、複数の認証要素を利用すること	・レベル2と同等の基準に加え、フィッシングの脅威に対する耐性	・電子政府推奨暗号リストに記載の署名方式
レベル2	**（窓口）** ・写真付き身分証明1種（or他2種）の提示 **（郵送 or オンライン）** ・申請情報に他機関の登録情報（クレジットカード番号等）を含めて申告	・レベル3の方法に加え、分割配付（一方を郵送）、メール通知後のダウンロード、によるトークン発行	・認証情報の推測確率が16384分の1未満であること	・レベル1と同等の基準に加え、盗聴、セッション・ハイジャック、中間者攻撃の脅威に対する耐性	
レベル1	**（窓口 or 郵送 or オンライン）** ・身元確認は不要 ・メールアドレスの到達確認	・レベル2の発行方法に加え、電子メールによる送付、ダウンロード、によるトークン発行	・認証情報の推測確率が1024分の1未満であること	・オンライン上の推測、リプレイ攻撃の脅威に対する耐性	

http://www.kantei.go.jp/jp/singi/it2/guide/
オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（概要版）[PDF]より抜粋

大学内におけるLoAに関わる事例



- 学内のサービスをセキュリティレベルでカテゴライズし、認証方法を区別する方法を検討
- 京都大学等の先行大学では、給与明細サービスなどに導入済

先行大学ではローカルにLoAの概念を実活用

学認としての新たな展開の可能性

- e-Radの次期システムの開発が年内に開始
  - 独自IdPとSPを構築し、SAMLにより認証
- e-RadとReaD&ResarchMapの連携
  - 業績データの連携操作を、SAMLによるSSOで実現

学認との親和性が向上

- 米国ではNSFグラント申請システムと学術認証フェデレーションInCommonを、Level2を条件に接続

学認としてLevel 2のTFP獲得を目指す
https://www.gakunin.jp/docs/fed/loa

2011年度末までの主なイベント

- 12月1日：OpenID Summit Tokyo（秋葉原）
  - 新しく公開されるプロトコルOpenID Connectでは、保証レベル（LoA）や属性交換への対応が進められる。そうした概念をSAMLにて先行して実現する学術認証フェデレーションとOpenIDファウンデーションとのコラボレーションにより、プロトコルを超えた新しい認証連携の将来像を探る。
  - http://www.event-info.com/openid/
- 12月7～9日：大学ICT推進協議会年次大会（福岡）
  - EJへのリモートアクセスを実現する学認だけでなく、大学間認証連携へと活用を展開する上で、eLearningでの利用は重要な鍵となる。地域のeLearningや全国展開を視野に入れたセキュリティラーニングにおける学認の役割を主眼に、学認の新しい活用事例を探る。
  - http://axies.jp/ja/conf2011/
- 2月13～17日：APAN（タイ，チェンマイ）
  - アジア諸国においても、学術認証フェデレーションを立ち上げる機運が高まっている。フェデレーションの世界連合REFEDSを招き、各国代表者と情報交換を進めると共に、日本が先導するアジアのインターフェデレーションを考える。
  - http://www.apan.net/meetings/future.php
- 3月5日：学認シンポジウム（都内某所を予定）
  - 学認の次世代ビジョンを一挙公開。

サーバ証明書発行プロジェクト

重要なお知らせ

「UPKIオープンドメイン証明書自動発行検証プロジェクト」は，現在の体制を継続し，**平成27年3月**まで，サーバ証明書発行のサービスを**無償で継続**致します．

- 現在の活動状況
  - 参加機関数：255
  - 発行枚数：約5000

更なるご参加をお待ちしております！

- 問い合わせ先
  - NII　学術基盤課　連携基盤チーム
  - Tel: 03-4212-2218
  - Email: cerpj2@nii.ac.jp