学認について

平成27年度　新潟県大学図書館協議会研修会@長岡高専

国立情報学研究所　学術基盤課（認証担当）　野田　英明

本日の内容

- 「認証」と図書館サービス
- 学認を使ったリモートアクセス
- 学認のしくみ
- 学認に参加するために

本日の内容

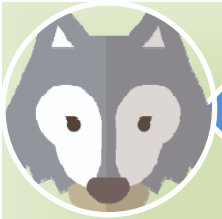
- 「認証」と図書館サービス
- 学認を使ったリモートアクセス
- 学認のしくみ
- 学認に参加するために

学術認証フェデレーション
「学認」

・・・「認証？」

図書館における典型的な「認証」の事例。

【認証】とはなにか　～グリム童話を例に～



「あけておくれ，おかあさんだよ」

「おかあさんなら白い手をしているはずだよ」
（※1）

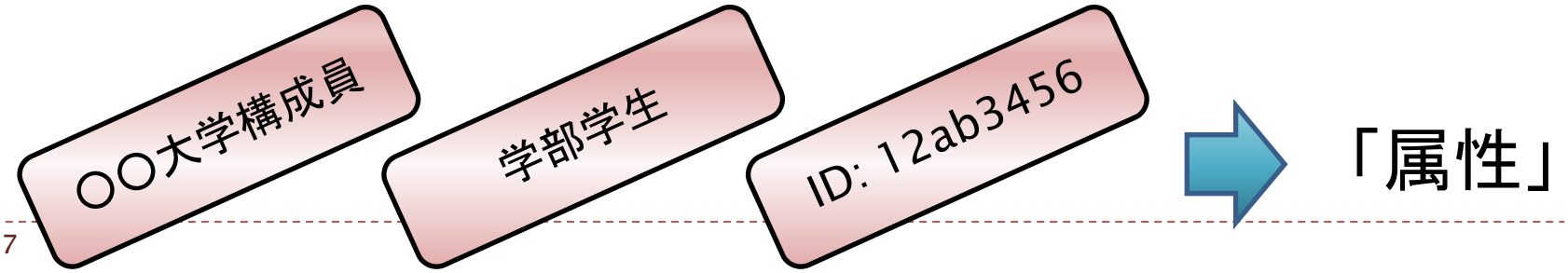
「ほら，白い手だよ～」

「おかあさんだね，入ってきていいよ」（※2）

「認証」と「認可」 そのはたらき

- 【認証】 その人は間違いなく本人か，検証すること（※1）
  - パスワード，暗証番号・・・（本人の記憶による検証）
  - ICカード，マトリクス，SMS・・・（本人の所有物による検証）
  - 指紋，指静脈，虹彩・・・（本人の生体情報による検証）

- 【認可】 その人は何ができるかを特定し，許可すること（※2）
  - 「大学の構成員だから，電子ジャーナルが読める」
  - 「学部学生だから，図書を5冊まで貸出できる」
  - 「この先生は図書を延滞してたから，きょうは貸出禁止！」



認証と認可による「アクセス管理」

- 電子ジャーナル等，利用資格を有する者の範囲は，契約に明記される。
  - 「利用資格を有する人には，適切にアクセス権限を付与」
  - 「利用資格のない人は，確実にアクセス不可とする」
- 「認証(authentication)」と「認可(authorization)」を組み合わせることにより，この制御が実現される。
  - 学内からのアクセスであれば，「IPアドレス認証」を用いるのが一般的
    （契約内容によっては，IPアドレス認証だけでは制御に不足することもあります）
  - では，学外からアクセスするにはどうすればいい？

本日の内容

- 「認証」と図書館サービス
- 学認を使ったリモートアクセス
- 学認のしくみ
- 学認に参加するために

リモートアクセスとは？

- 電子ジャーナル等の利用では「IPアドレス認証」を使うのが一般的。
- 機関のIPアドレス範囲外からのサービス利用が「リモートアクセス」。
- 多くの電子ジャーナルでは，契約上，リモートアクセスが認められる。
- 個々の雑誌・パッケージにおける利用可否は，各社の契約書，もしくは，JUSTICE標準提案書にてご確認ください（参加機関限定）。

これまでのリモートアクセス

- 大手出版社の電子ジャーナルでは，各社にID・パスワード発行を申し込むことにより，リモートアクセスが可能。

- 利用する側にとっては，手間のかかる方式でもある。
  - 出版社ごとに，それぞれ申し込まないといけない （>_<）
  - 出版社ごとに，ID・パスワードを使いわけないといけない （>_<）
  - そもそも，パスワードが発行されるまで待っていられない （-_-#
  - 図書館にとっても，利用者案内やID管理など負担が重い・・・

- ID発行を個別に申し込むうえ，個人情報の登録が必須という問題も。
  - パスワードの使いまわしによる，アカウント乗っ取りリスクの増大
  - 不必要に個人情報を外部に出させることの是非

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～

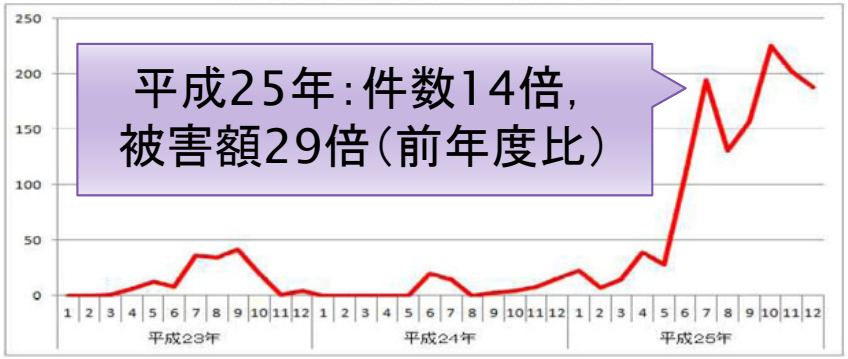
- ネットバンキングにおける不正送金の急増
- スパム送信数の急増（大学のメールサーバもターゲット）
- パスワード使いまわしによる被害の拡大

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）



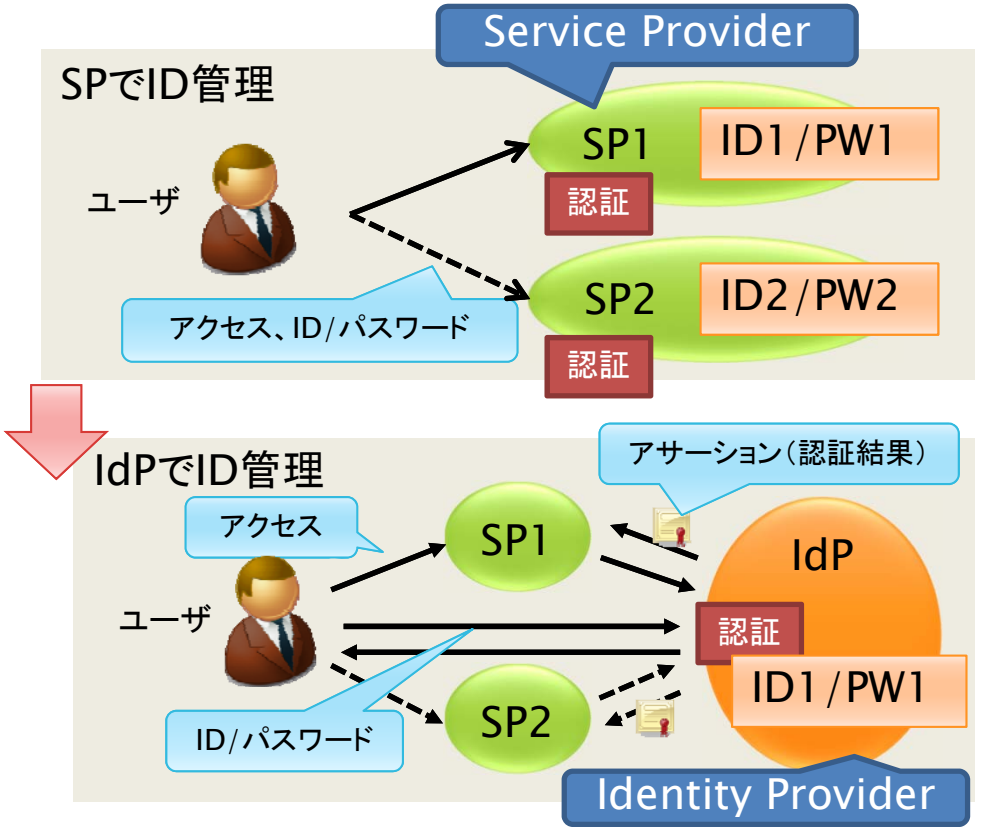
平成25年：件数14倍，
被害額29倍（前年度比）

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

情報処理推進機構「パスワード　ーもっと強くキミを守りたいー」
https://www.ipa.go.jp/security/keihatsu/munekyun-pw

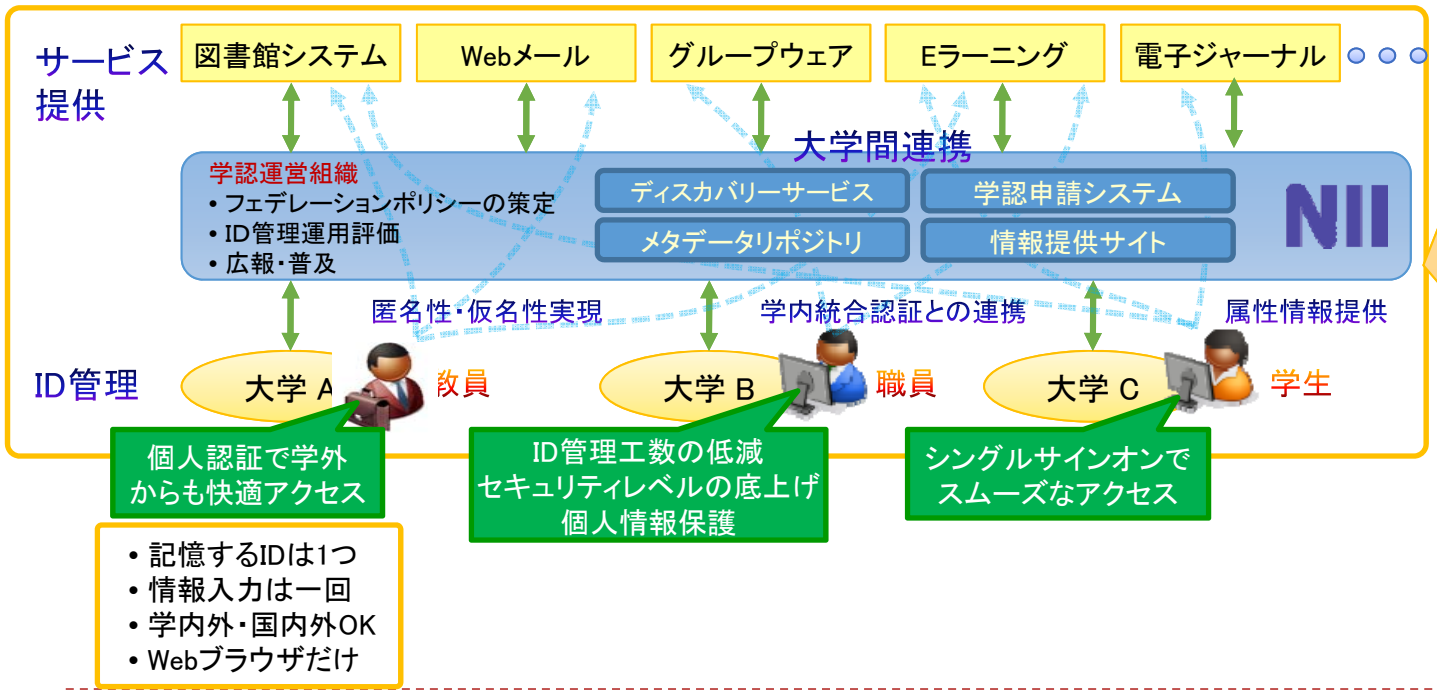
シングルサインオン(SSO)によるソリューション

- サービス個別のID/パスワードから，シングルサインオンへ
  - 1回のログインで，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
- 「認証」と「認可」を分離，認証は機関が用意する認証サーバに集約
  - 全てのサービスが，一組のID/パスワードで利用可能（便利）
- サービス側は，認証サーバから送られる認証結果を信頼して「認可」
  - パスワードはサービス側に渡らない（安全）
- IPアドレスに依拠しないため，リモートアクセスが実現できる



学術認証フェデレーション「学認」

- 学術認証フェデレーションとは
  - 定められた規程（ポリシー）を信頼しあうことで，相互に認証連携を実現し，学術リソースを利用・提供する機関や組織から構成された連合体のこと
  - 機関（IdP）がIDと属性を管理し，サービス提供者（SP）がそれを利用して認可



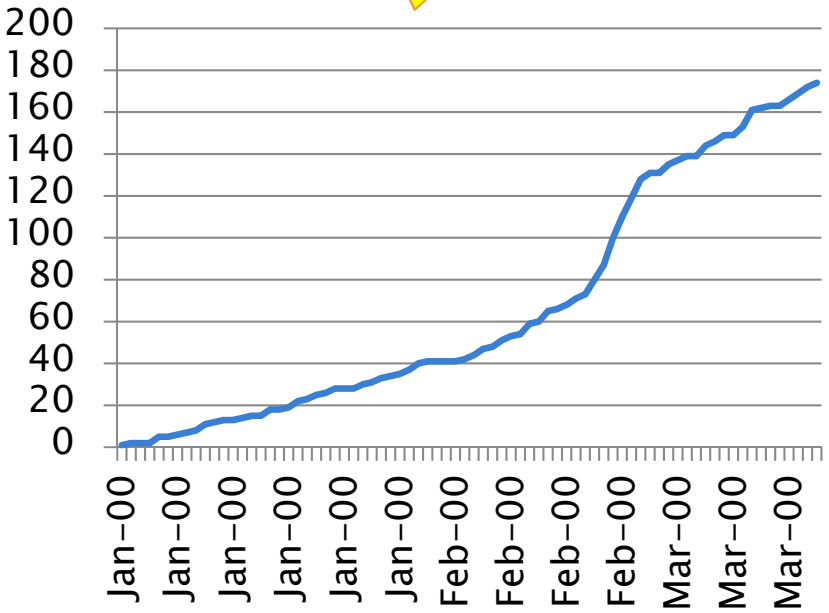
クラウドの活用を支援

- 民間フェデレーションとの連携による学割サービス等の開発
- より高度で便利な本人確認手法との連携機構の開発と提供
- 信頼レベル認定による格付け
- きめ細かなプライバシー保護のための制御機構の開発と提供
- 共同研究や共同利用を支援するグループアクセス機構の提供

学認参加IdPの推移（2015/10末現在）

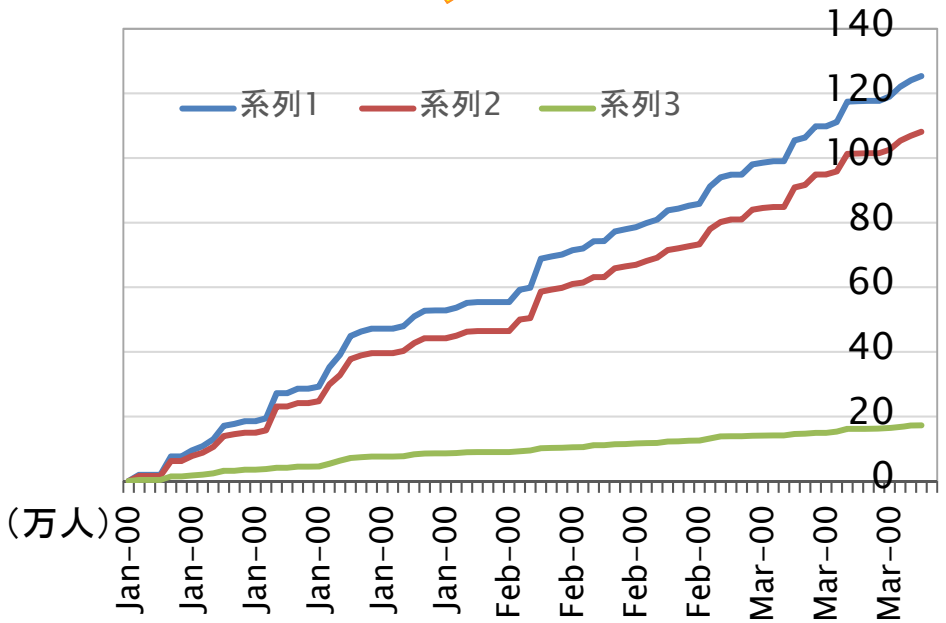
機関数

174機関



ユーザ数

総ID数約125万

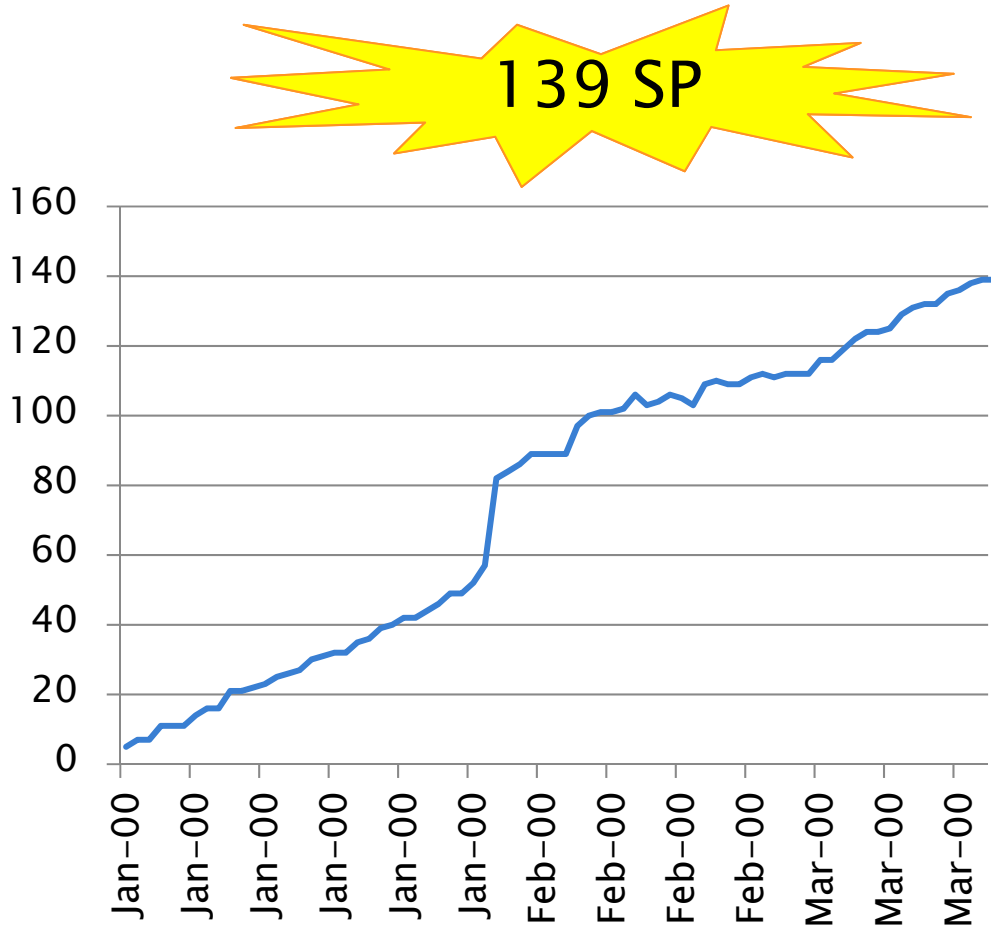


	国立大学	公立大学	私立大学	短期大学	高等専門学校	共同利用機関	その他	合計
学認参加数	59	12	44	0	51	1	7	174
カバー率	69%	12%	7%	0%	89%			
総機関数	86	92	603	334	57			

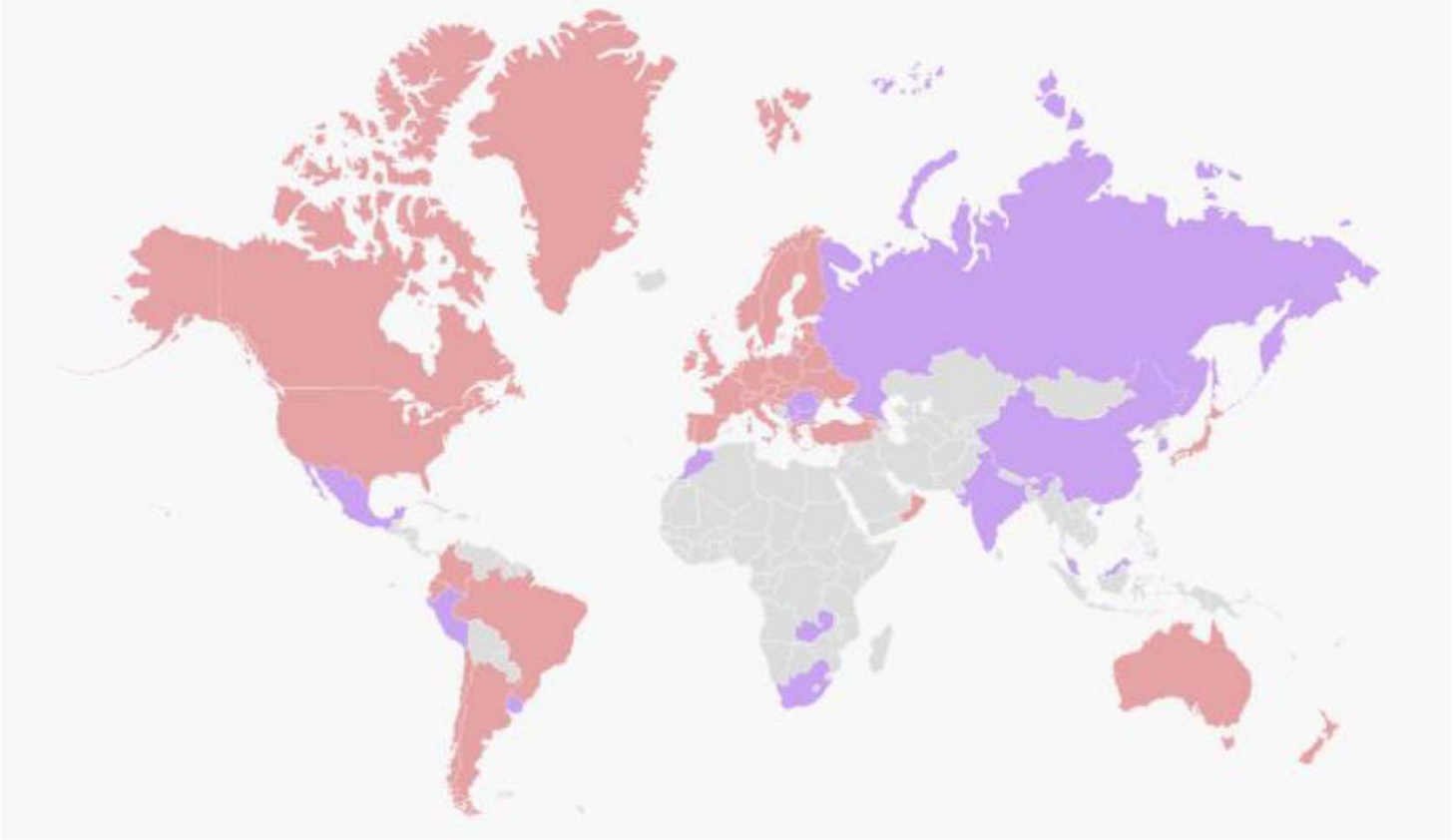
学認参加SPの推移（2015/10末現在）

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



世界各国で構築されるフェデレーション



赤： 運用中のフェデレーション
紫： 試行運用のフェデレーション

本日の内容

- 「認証」と図書館サービス
- 学認を使ったリモートアクセス
- **学認のしくみ**
- 学認に参加するために

Shibbolethとは

- 標準プロトコル(SAML)によって，サービス利用認可のための属性情報をやり取りするためのミドルウェア。
- オープンソース(無償)である。
- 米国EDUCAUSE／Internet2にて2000年に発足したプロジェクト。現在の開発主体はShibboleth Project / Shibboleth Consortiumに移行。
  - http://shibboleth.net/
- 最新はIdP 3.1.2, SP 2.5.5。IdPは11月に3.2.0がリリース予定。
- 欧米でﾌｪﾃﾞﾚｰｼｮﾝを通じて実運用拡大。

  とりわけ学術系の利用が軸となっている。

フェデレーション構築に必要なサーバ

- IdP（Identity Provider）　大学（サービス利用者側）が用意
  - フェデレーション内に構成員の情報を提供するサーバ
  - フェデレーションに参加する大学等が構築

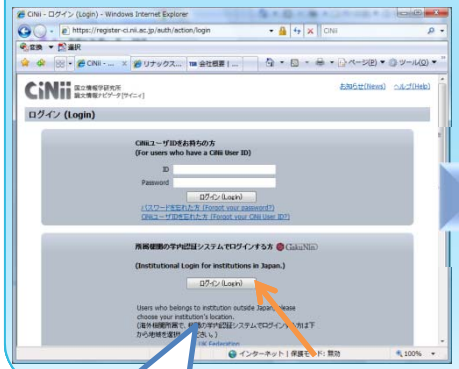
- SP（Service Provider）　大学他（サービス提供側）が用意
  - 認証を受けた人に対してサービスを行うサーバ
  - 電子ジャーナル，データベース，E-ラーニング等
    Webベースのシステムであれば何でも可

- DS（Discovery Service）　フェデレーションが用意
  - SPへのアクセスの際にIdPを検索するシステム
  - フェデレーションが運用
  - WAYF (Where Are You From) サービスとも呼ばれる(Shib 1.x)

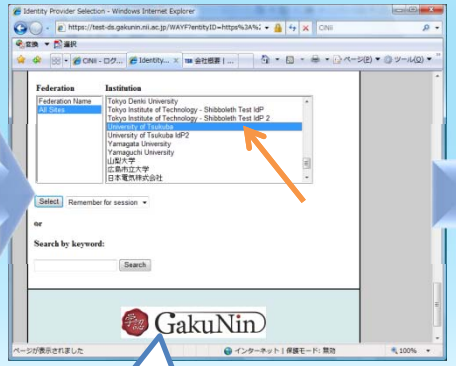
学認における認証手順

ログイン成功！

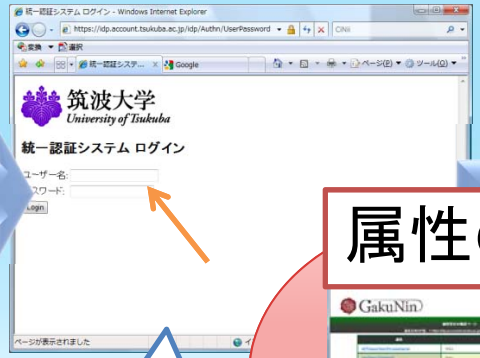
1. 学認認証を選択



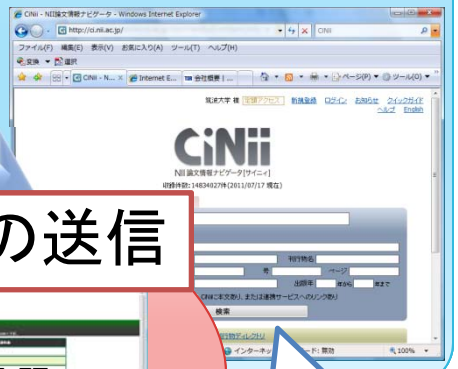
2. 所属機関を選択



3. ID/PWを入力



4. 認証完了(SPに戻る)



属性の送信

SP
(Service Provider)

DS
(Discovery Service)

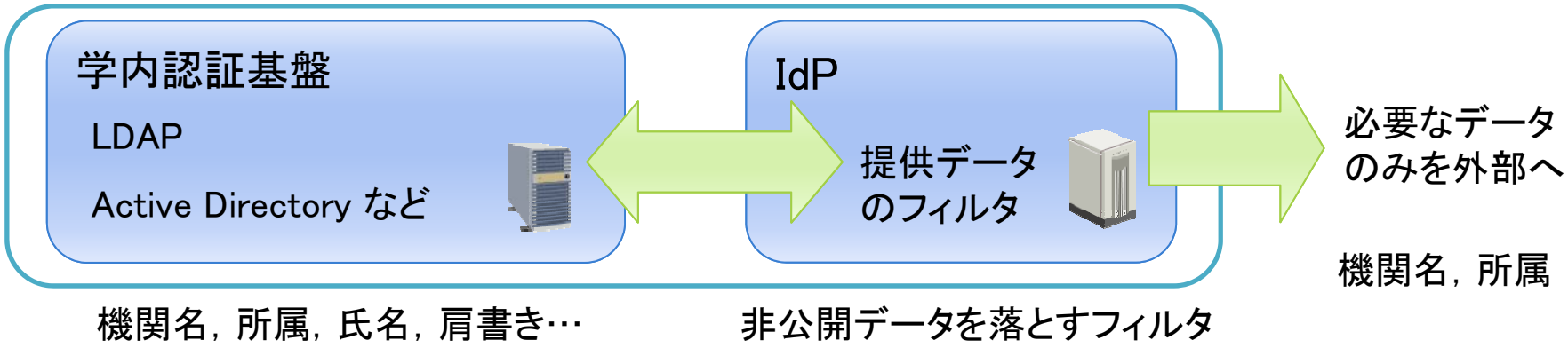
SP

IdP
(Identity Provider)

SP
(Service Provider)

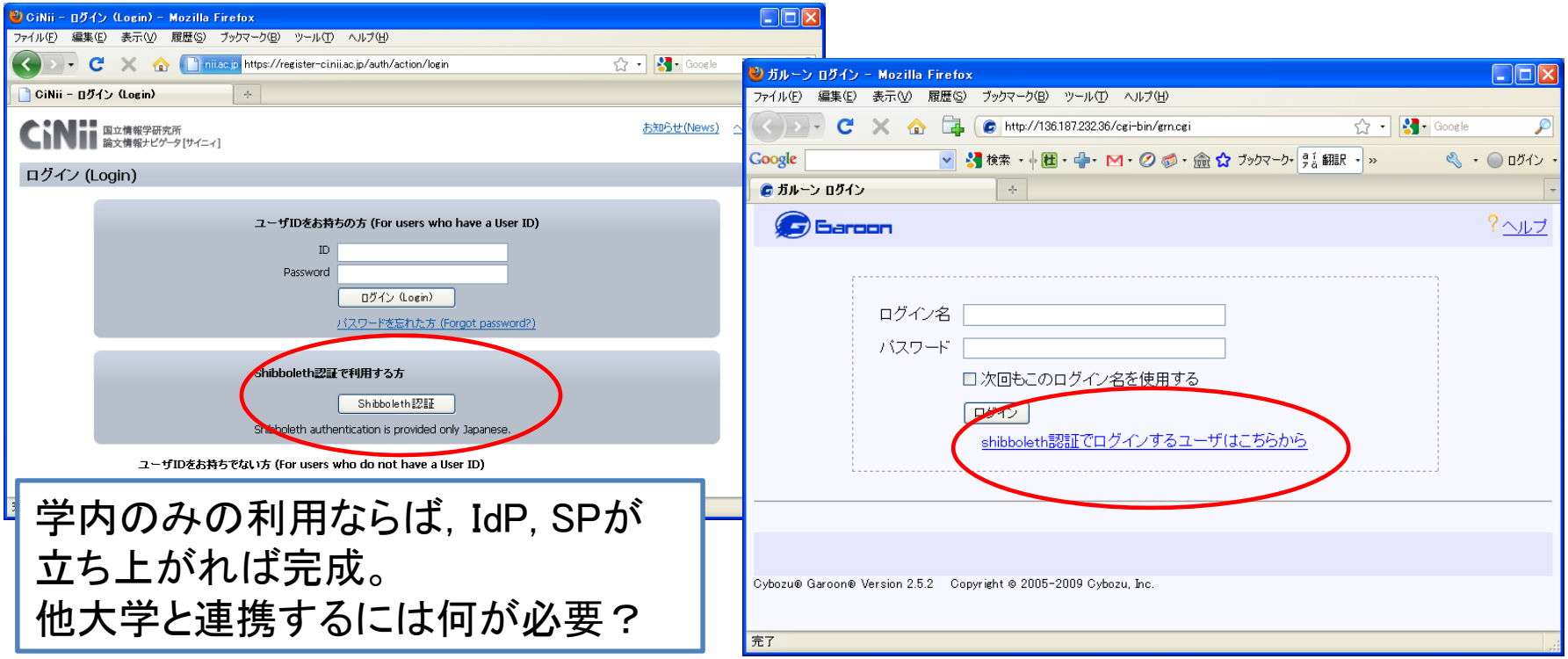
IdP (Identity Provider)とは

- フェデレーション内に情報を提供するサーバであり，大学等が構築
- IdP自身は情報を持たない
- 情報はLDAPやActive Directory等，既存の認証基盤を参照
- IdPは単なるフィルタであり，学内認証基盤から特定のデータのみを抽出して提供する
- 公開できるデータの制御が可能である
  - このため，Shibbolethはしばしば個人情報保護に優れていると言われるが，サーバ自体がハッキングに強固という意味ではない。
  - 慎重な操作が必要なのは，LDAPやActive Directoryと同じ



SP (Service Provider)とは

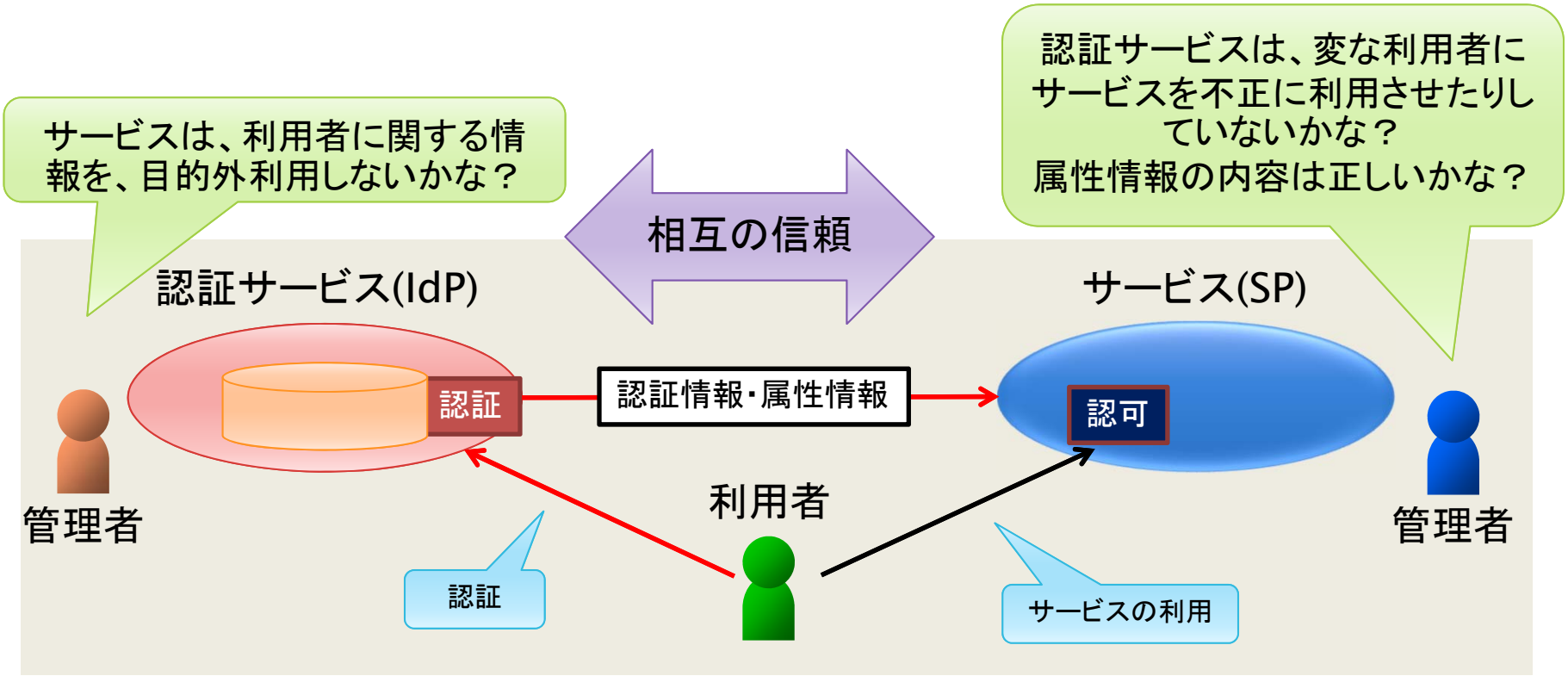
- サービスを提供するWebサーバのこと
- “シボレスログイン”等のボタンがあればShibbolethで利用可能なSPである
- 電子ジャーナルに限らず，いろいろなサービスをShibboleth化することが可能（例：無線LAN認証，サイボウズ）



学内のみの利用ならば，IdP，SPが立ち上がれば完成。
他大学と連携するには何が必要？

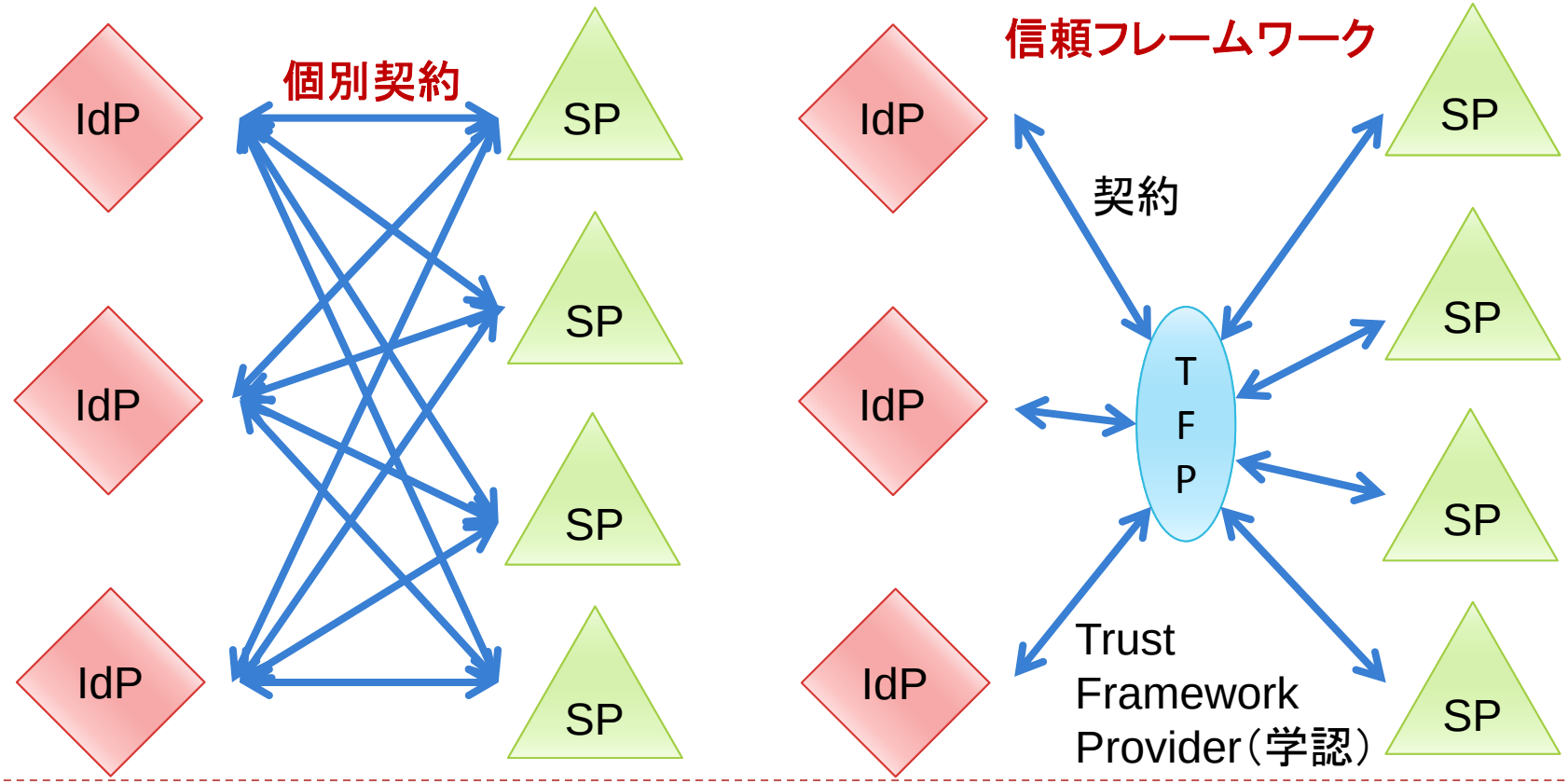
SSO技術の組織間利用での信頼

- 「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



信頼フレームワークの効果

- 一律のポリシーに基づく信頼フレームワークの導入により、個別契約での
  N×Mの関係が、N＋Mの関係に削減



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
- IdP of the Year 2014 ― 金沢大学

LoA1認定 第1号

学認で扱う「属性」

学認で使用される属性情報の種類は18種類。
これらを用いて認可処理などが可能。

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匿名識別子
eduPersonAffiliation	職種
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）
isMemberOf	所属するグループ名

実際に使われる属性情報の例

サービスA (1項目必須)

eppn (必須)
eduPersonAffiliation

サービスB (1項目必須)

eduPersonAffiliation (必須)

サービスC (2項目必須)

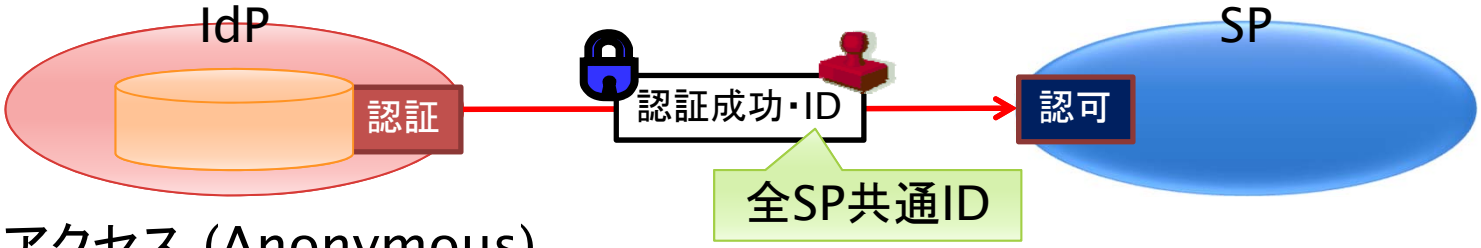
eduPersonTargetedID (必須)

eduPersonEntitlement
eduPersonScopedAffiliation
（どちらか必須）

(参考)
https://meatwiki.nii.ac.jp/confluence/x/1oS5

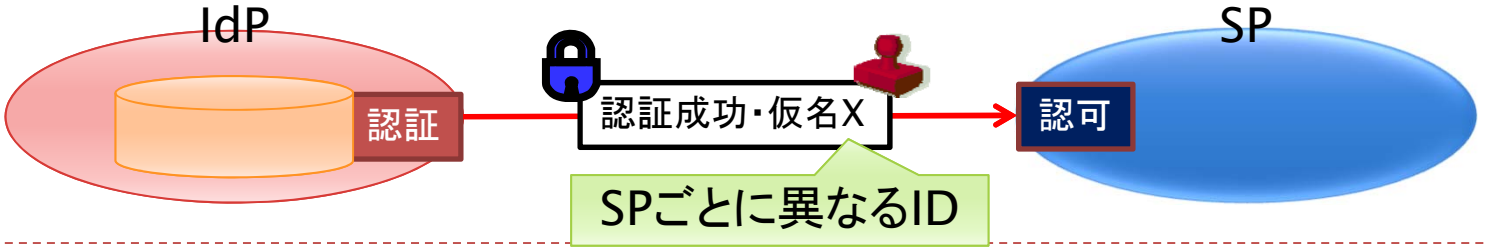
プライバシー保護：匿名アクセス、仮名アクセス

- 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
    - プライバシー保護



本日の内容

- 「認証」と図書館サービス
- 学認を使ったリモートアクセス
- 学認のしくみ
- 学認に参加するために

学認参加のための第一歩

- とにかく，IdPを構築しましょう。
- IdPを作るためには，「利用者を一元的に管理しているサーバ」が必要です。
  - LDAPサーバやActive Directory等が相当。
  - 多くの場合，情報センター（もしくは，これに相当する組織）が持っています。
  - 利用者データの管理がどのくらいの頻度で行われているか，要確認。
  - データのメンテナンスを誰が行うか，調整が必要なことも。
- 学内の既存データを活用できるか，調整が重要です。
  - 属性情報を学外に出すことには，学内合意が必須。
  - 特に個人情報を学外に出すことへの抵抗は強い。
  - 大学名など，比較的抵抗の少ない属性から，スモールスタートでも良いのでは？

利用したいサービスを確認

- どのサービスを利用したいのか，計画を立てます。
  - サービスごとに，利用権限を持つ者の範囲も異なります。
  - 利用権限を持つ者の範囲と認証サービスの利用者の範囲が異なる場合，
    契約に違反することがないよう，手立てを考える必要があります。

- 利用したいサービスに必要な属性は送信可能か，確認します。
  - 学認で利用が認められる属性は18種類。
  - 元になる利用者サーバに，全ての属性が揃っていることは，ほとんどありません。
  - 利用したいサービスで必要な属性のみ，送信できればOK！
  - 電子ジャーナルだけなら，必要な属性は大幅に絞られます。

属性の管理は，IdP構築時だけではなく，運用開始後も関わってきます。

学認は「大学・サービス提供者・NIIの連携」で実現されていますが，各大学における「図書館と情報センターの連携」も，きわめて重要です。

IdPを構築したら –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になります

- テストフェデレーション
  1. 参加申請用のアカウント作成
  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の場合は？
  - オフラインによる確認が1ステップ増えるだけ （学長印を付した書面の提出）

実施要領，技術運用基準が守られていることが前提

SPを利用するために

- 電子ジャーナルなど，商用SPの多くは，「学認に参加」しただけでは利用できません。
  - 学認は「認証」を行っているだけなので，契約のないタイトルは読めません。
- IdPに，利用したいSP向けの設定を追加することが必要です。
- あわせて,SP側にも「学認経由で利用」の申込を必要とすることも。
  - 詳しくは，学認ウェブサイト「IdP・SP一覧」をご参照ください。

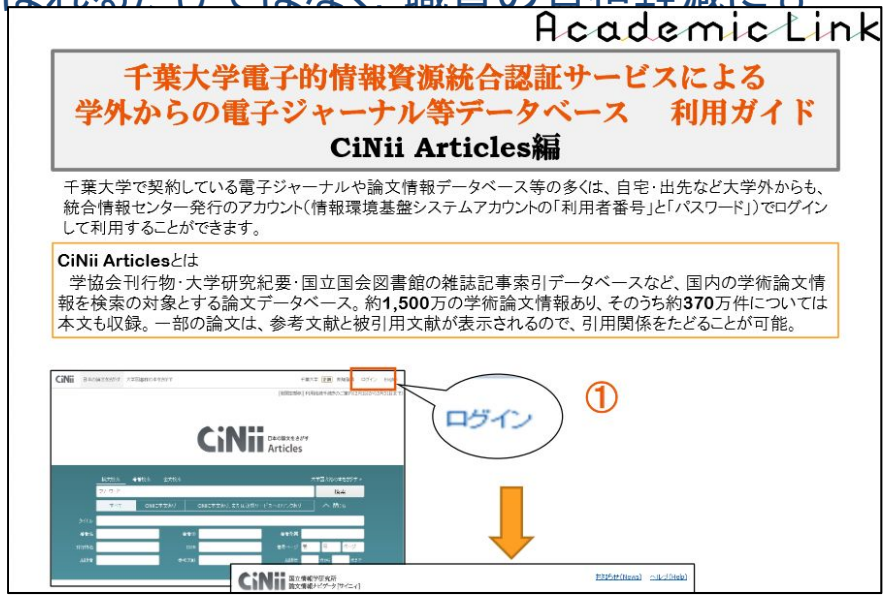
https://www.gakunin.jp/participants/

さあ，利用を始めましょう。

- 図書館と情報センターで，利用者サポートの分担を決めておくと良いでしょう。
  - 利用者アカウントのことは，情報センターでないと判らないことが多いです。

- 学認経由での利用方法は，サービスによって様々です。
  - 利用ガイドを用意しておくと，利用者に喜ばれるだけではなく，職員の負担軽減にも

（千葉大学の例　http://www.ll.chiba-u.ac.jp/remote.html）



安全に利用するために

- 学認では，一組のID / パスワードで多くのサービスが利用可能。
  - 覚えるべきパスワードはひとつだけ
  - パスワードが漏洩すると，多くのサービスに不正アクセスされる危険も

- 各機関のセキュリティポリシーに従い，できるだけ強固なパスワードを設定するよう，ご案内をお願いします。

情報処理推進機構「パスワード　ーもっと強くキミを守りたいー」
https://www.ipa.go.jp/security/keihatsu/munekyun-pw

学認に関するお問合せは・・・

国立情報学研究所　学術基盤推進部

学術基盤課　総括・連携基盤チーム（認証担当）

mail: gakunin-office@nii.ac.jp

まで，お気軽にどうぞ。