資料3

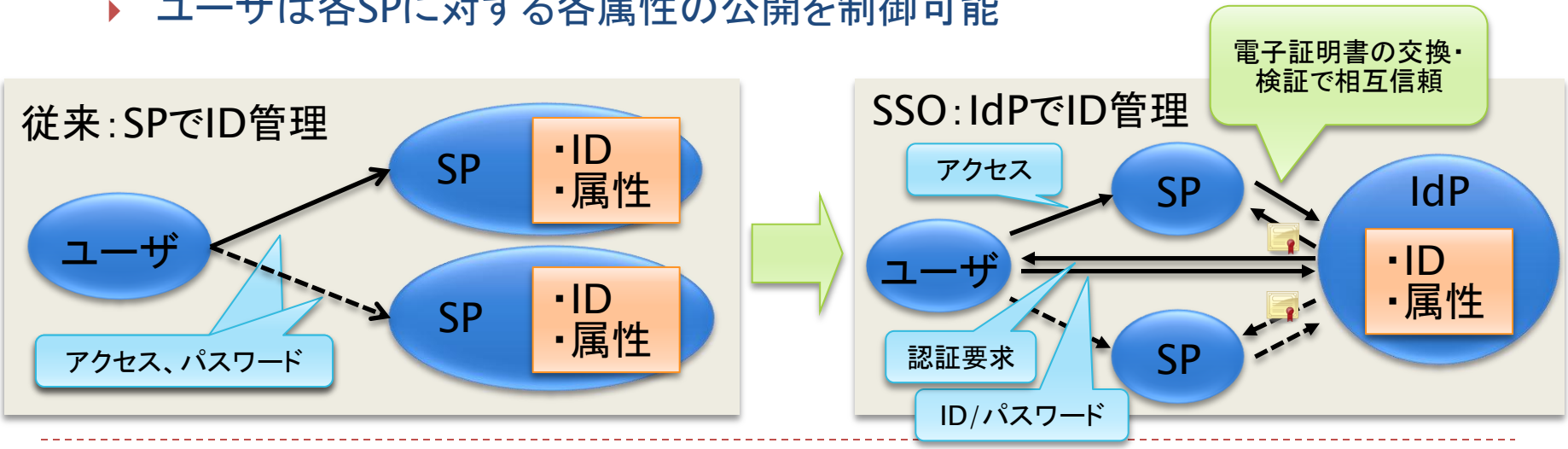
学術認証フェデレーション「学認」による セキュリティ向上

国立情報学研究所　山地一禎、中村素典

平成23年度第3回学術情報基盤オープンフォーラム

学術認証フェデレーションとは

- 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
- プライバシ保護を考慮したシングルサインオン（SSO）技術
  - ユーザのユニークネスを保証しつつ個人情報は出さない
  - SPは必要な情報のみをIdPに要求
  - ユーザは各SPに対する各属性の公開を制御可能

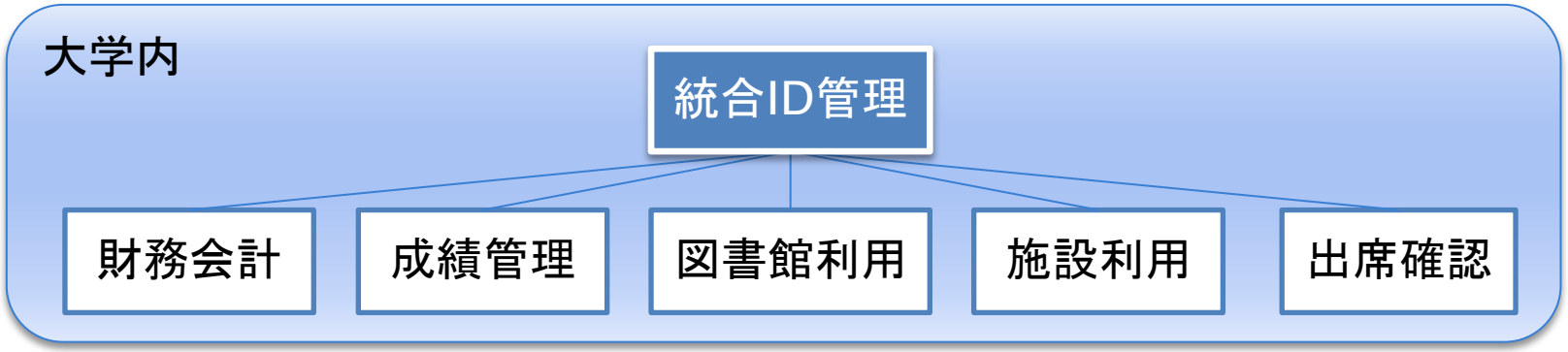


セキュリティを考慮した認証システム

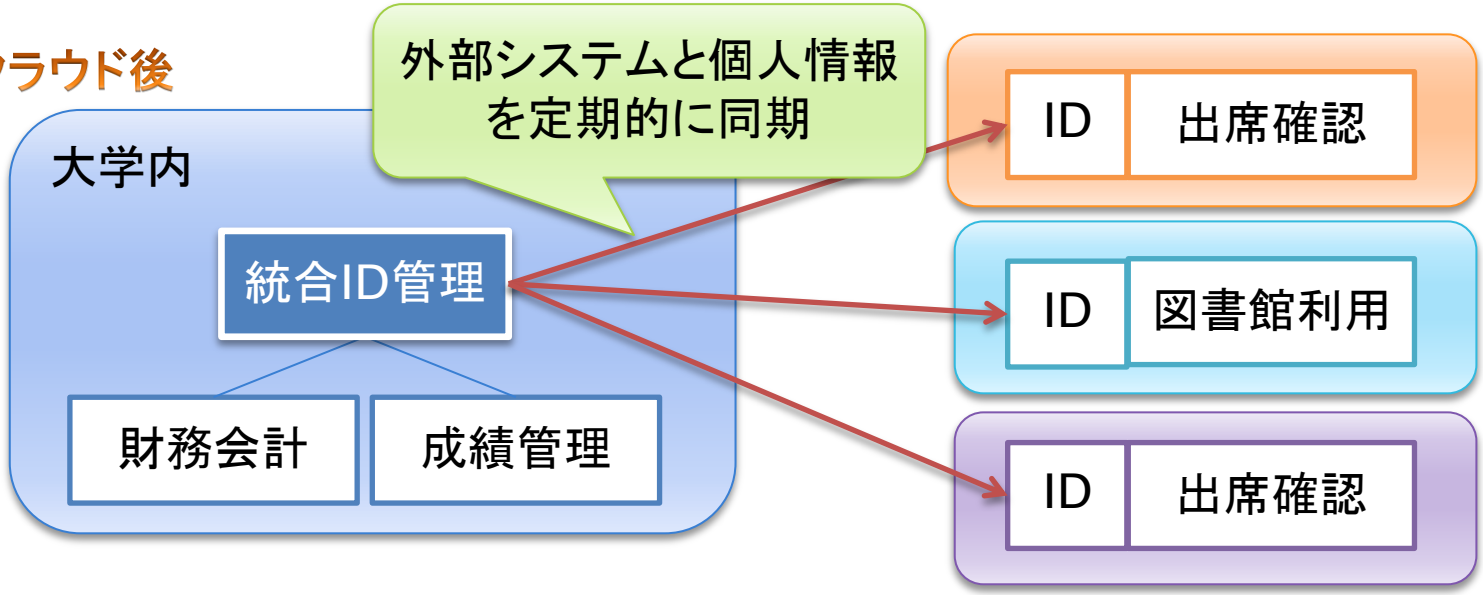
- 個人情報を扱う上での学認の利点
  - 大学も安心して外部サービスに接続できる仕組み
- 認証の保証レベルにも対応した学認のフレームワーク
  - ミッションクリティカルなサービスにも接続できる仕組み

クラウド上サービスを利用する際のID管理は

クラウド前

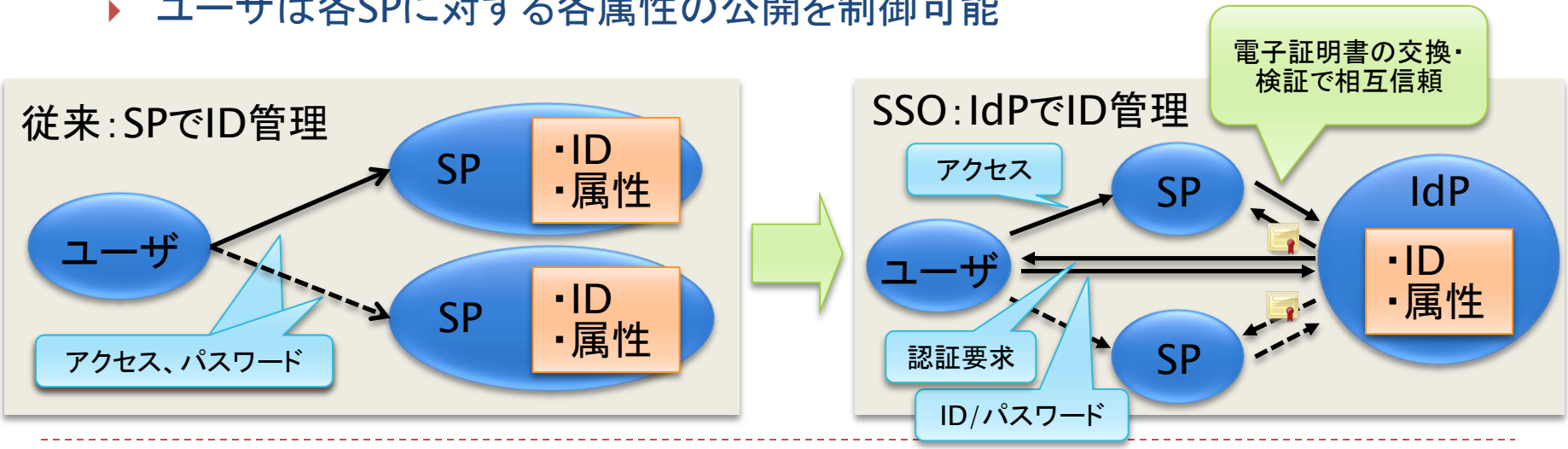


クラウド後



学術認証フェデレーションとは

- 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
- プライバシ保護を考慮したシングルサインオン（SSO）技術
  - ユーザのユニークネスを保証しつつ個人情報は出さない
  - SPは必要な情報のみをIdPに要求
  - ユーザは各SPに対する各属性の公開を制御可能



クラウドと学認

- 学認はまさにクラウドのための認証システム

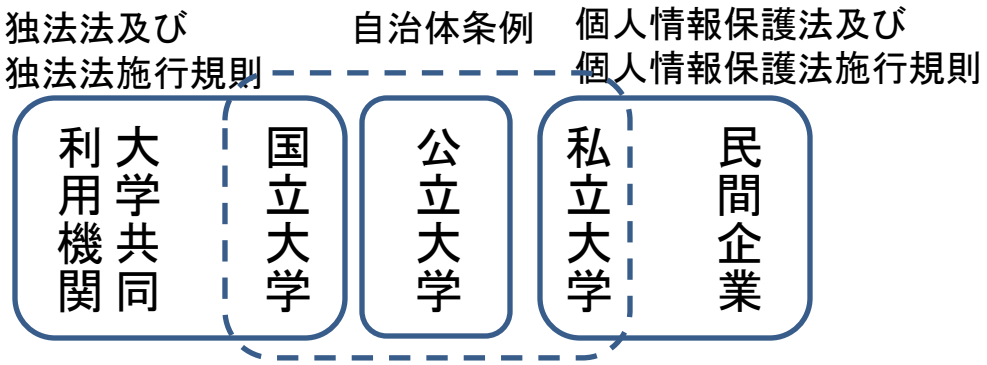
- どのような情報が大学のIdPからSPに渡るか？
  - 認証の結果
    - 個人情報にならないチケットをIdPとSPで相互確認
  - ユーザの属性
    - 17種類のユーザ属性を学認ポリシーで規定
      - 例：組織名、職種、匿名ID、メイルアドレス、氏名など

これらの情報をいかにIdPからSPに提供するか？

ユーザ属性

- 付加的な情報として属性情報を送ることができる
  - SPからの要請とユーザの承認に基づく属性送信
    （無用な情報は送らない）
  - 暗号化することで情報漏洩を防止
  - 匿名性を維持しつつ異なるユーザであることを示すための属性として匿名ID（eduPersonTargetedID）を用意
    （SP間の結託防止）
  - 個人情報を送信する際には、Opt Inができる仕組みを提供

・大学における個人情報保護



独法法：独立行政法人等の保有する個人情報の保護に関する法律
個人情報保護法：個人情報の保護に関する法律

・個人情報保護法と独法法の差異

a.個人情報の定義

個人情報保護法

生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別できるもの。（他の情報と**容易に**照合することができ、それにより特定の個人を識別することができるもととなるものを含む）

「照合容易性」の規程があるため、内部にない情報と照合しなければならない情報は個人情報ではない。

独法法

生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別できるもの。（他の情報と照合することができ、それにより特定の個人を識別することができるもととなるものを含む）

「照合容易性」の規程がないため、内部にない情報と照合しなければならない情報も個人情報になる。

・その他の主な差異

項目	個人情報保護法	独法法
利用目的の特定	個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。	独立行政法人等は、個人情報を保有するに当たっては法令の定める業務を遂行するため必要な場合に限り、かつ、その利用の目的をできる限り特定しなければならない。
利用目的の通知	個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している 場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。	独立行政法人等は、本人から直接書面に記録された当該本人の個人情報を取得するときは、次に掲げる場合を除き、あらかじめ、本人に対し、その利用目的を明示しなければならない。
第三者提供の制限	個人情報取扱事業者は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識 別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項につい て、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にか かわらず、当該個人データを第三者に提供することができる。	オプトアウトについての規程は無し
開示	個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの利用目的の通知を求められたときは、本人に対し、遅滞なく、これを通知しなければならない。	利用目的の開示請求条項は無し

良く使われる属性

- OrganizationName
  - Ex. National Institute of Informatics
- eduPersonEntitlement
  - サービスを利用する資格情報。SPサイトが受信する文字列を決定し，IdPサイトはSPサイト毎にその値を利用。IdPサイトでは，SPサイトが決めるサービス利用資格に従い，各ユーザの属性として送信する値を設定。
  - 設定例：urn:mace:dir:entitlement:common-lib-terms
- eduPersonAffiliation
  - 利用者の職位として，5つの値が利用可能。IdPサイトでは，組織内の実際の詳細職位とのマッピングが必要。また，利用できる値は，「卒業生」等，必要に応じて追加を検討。
  - 設定例："faculty"，"staff"，"student"，"member"，無し（空白）

良く使われる属性

- eduPersonTargetedID
  - フェデレーション内で一意な，かつ，SPサイト毎に異なる永続的な利用者識別子を送信。これは，SP間での利用者の特定を防ぐことを目的とし，識別子の値はハッシュ等により，本属性単体ではSP側でユーザの特定が不可能。
  - フォーマット
    - <IdPのentityID>，<SPのentityID>，およびハッシュ化した識別子を”！”で結合
    - ハッシュ値は、uidのSPのentityIDをもとに計算
  - 設定例：
    https://idp.sample.ac.jp/idp/shibboleth!https://sp.sample.ac.jp/shibboleth-sp!+Lxxl7QLnCkaKguy5xjNLRBkdD=
  - V.S eduPersonPrincipalName （個人情報）
    - 設定例：t-ninsyo2009@b-univ.ac.jp

個人情報の扱いについては？

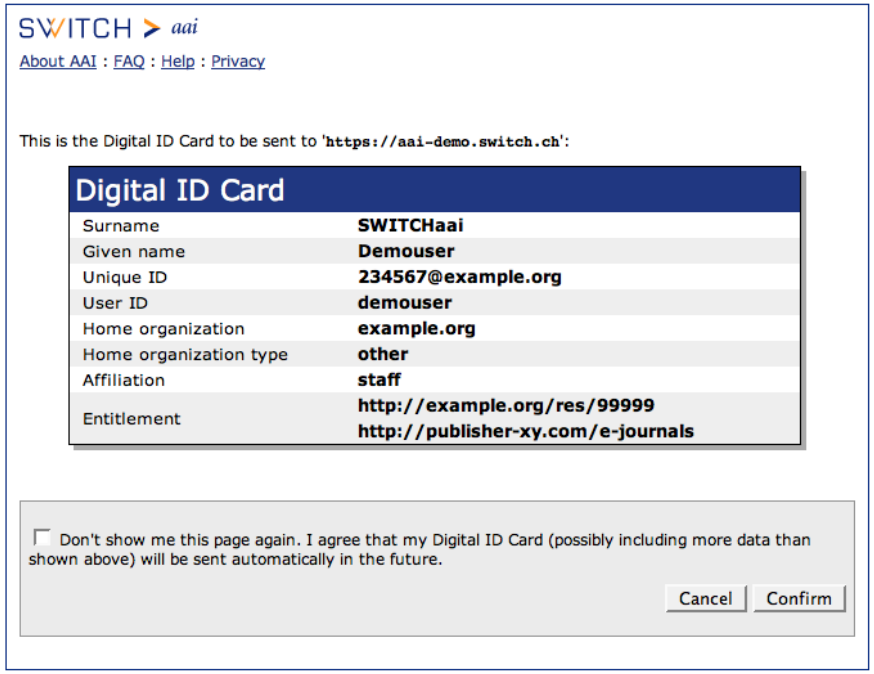
個人情報

Name (abbreviation)	Description
OrganizationName (o)	組織名
jaOrganizationName (jao)	組織名（日本語）
OrganizationalUnit (ou)	部門名
jaOrganizationalUnit (jaou)	部門名（日本語）
eduPersonPrincipalName (eppn)	フェデレーション内で固有の個人識別子
eduPersonTargetedID	SP毎に固有の個人識別子（匿名識別子）
eduPersonAffiliation	Staff, Faculty, Student, Member
eduPersonScopedAffiliation	Staff, Faculty, Student, Member（@scopeつき）
eduPersonEntitlement	SP毎に固有の付加情報
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	表示用氏名
jaDisplayName	表示用氏名（日本語）
mail	E-mail アドレス
gakuninScopedPersonalUniqueCode	学生番号、職員番号（@scopeつき）

学認参加以前に収集した個人情報は目的外利用となるため本人同意が必要

IdPにおけるユーザ同意機構の実装 (uApprove)

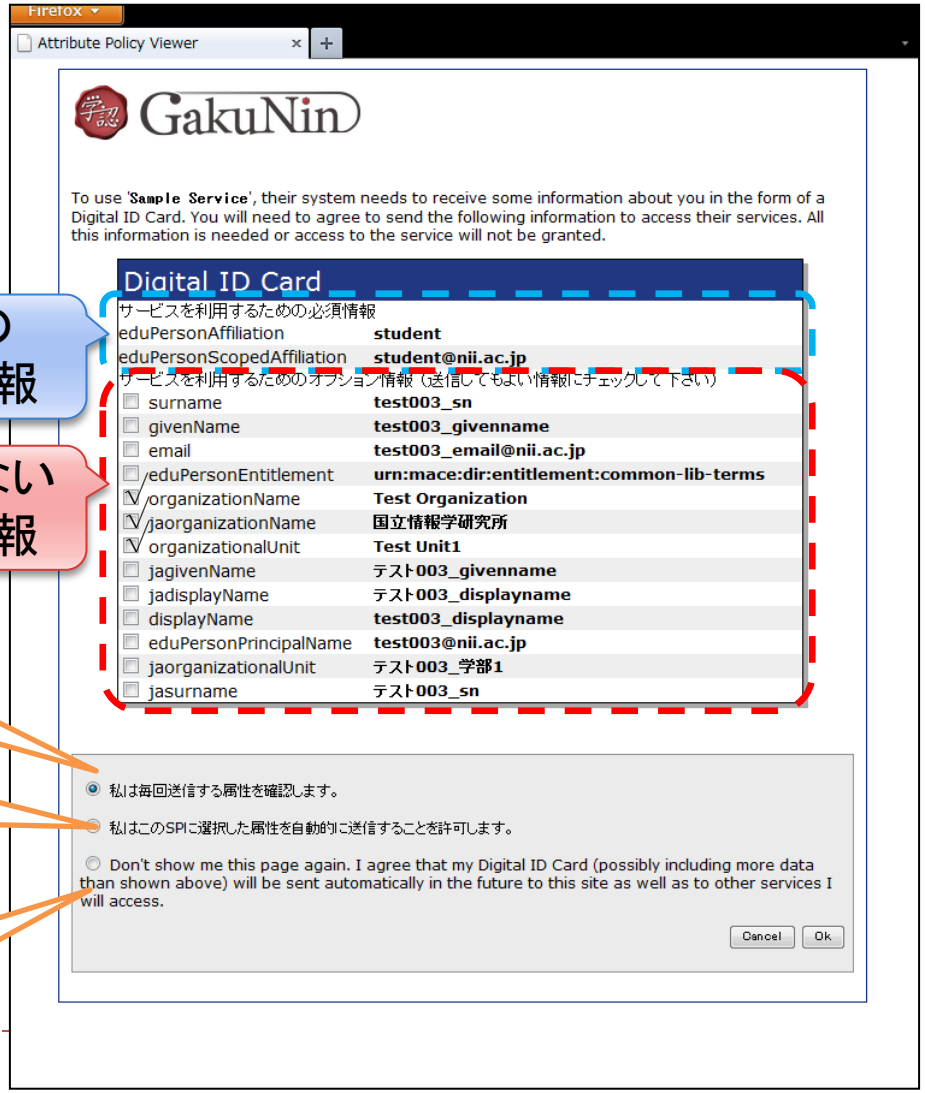
- SWITCH（スイス）から提供
  - Shibboleth IdPのプラグイン
- 送信される属性情報全てに対する、まとめての同意
  - どの属性情報が送信されるかは、IdPの管理者が指定する



http://www.switch.ch/aai/support/tools/uApprove.html

ユーザに選択権を与える拡張：uApprove.jp

- 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選択できる
- 将来の挙動について指定できる



セキュリティを考慮した認証システム

- 個人情報を扱う上での学認の利点
  - 大学も安心して外部サービスに接続できる仕組み
- 認証の保証レベルにも対応した学認のフレームワーク
  - ミッションクリティカルなサービスにも接続できる仕組み

学認のアカウント管理に関するポリシー

- 8.1) 利用者ID の管理　　学認システム運用基準より
  - 全ての利用者情報は，実在するアカウント情報でなければならない。また，各エンティティにおいて，利用者ID の有効期間が終了した場合，あるいは，利用者から利用意思の撤回があった場合には，遅滞なくその利用者ID の利用を停止しなければならない。
- 8.2) 利用者ID の再利用
  - eduPersonPrincipalName，およびeduPersonTargetedID に関して，かつて利用されていたが，現在利用されていない利用者ID を他者が使用する場合は，最終の利用時から最低24 ヶ月間は再利用すべきではない。
- 8.3) ID 利用者の同一性の保証
  - 前項における再利用の場合を除いて、IdP では、同一ID でのアクセスが同一人物からによることを保証するための方策を講じなければならない。
- 8.8) 参加機関の責任
  - GakuNin に参加する各参加機関は，相互に協力して認証連携を実現することとする。そのため，各参加機関では自らが送信する情報の信頼性や正確性について努力義務を負うものとする。ただし，その限りにおいて，故意または重大な過失によるものを除き，送信した情報の信頼性や正確性に不備があったことにより生じた損害について責任を負わないものとする。なおこの規定は，参加機関の間で送受する情報の信頼性や正確性についての責任に関し別途の取りきめをすることを妨げるものではない。

比較的高いレベルの運用基準をもち定期的な評価を実施 → LoA

学認における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(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。

OIXからLevel1 TFPの認定を受けるべく準備中

学認としての新たな展開の可能性

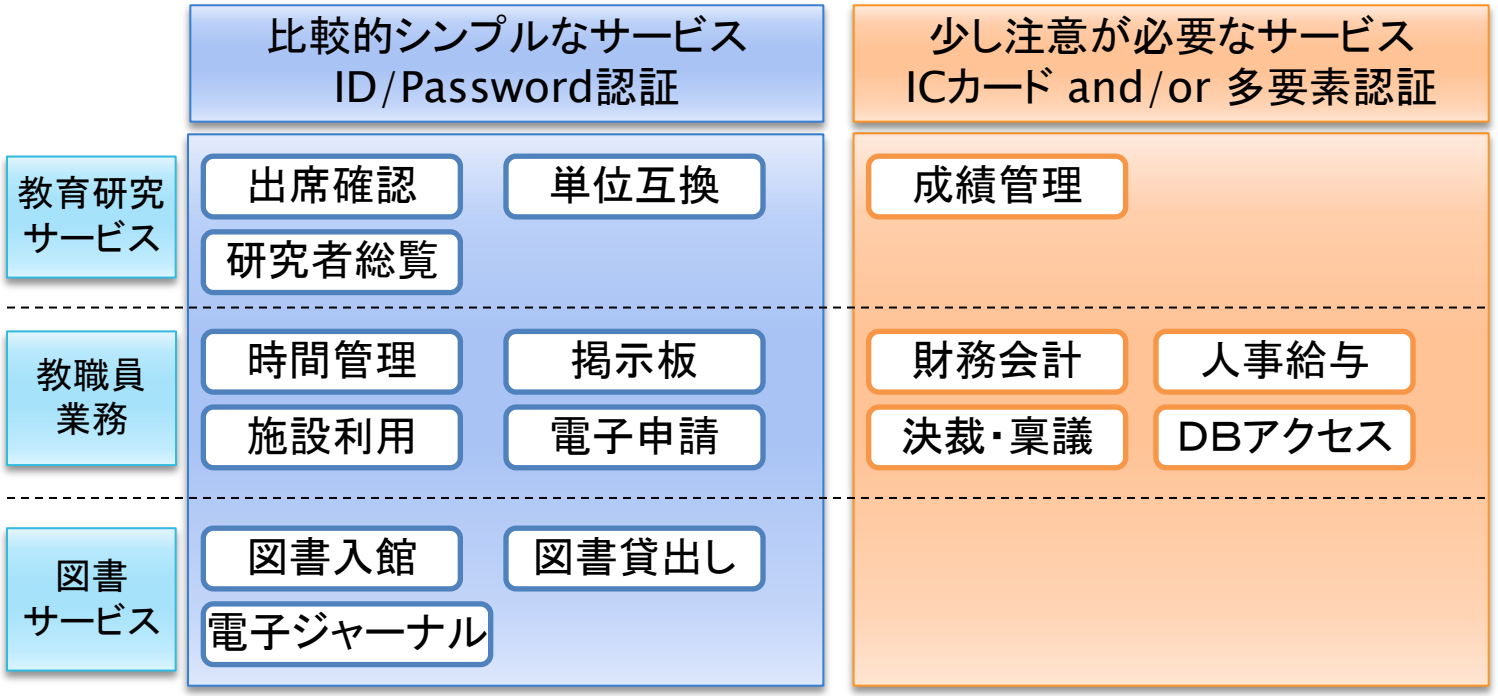
- e-Radの次期システムの開発が年末から開始
  - 独自IdPとSPを構築し、SAMLにより認証
- e-RadとReaD&ResarchMapの連携
  - 業績データの連携操作を、SAMLによるSSOで実現

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

大学内におけるLoAに関わる事例（京大）



- 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

機微な情報を扱う学内システムのクラウド化にもLoAの概念が有用

まとめ

以下の3つの観点から
セキュリティを考慮したIDフェデレーションを実現

- IdPとSPの接続に関するプロトコルとしての信頼性
  - 本日は、詳細な説明を割愛
- 法令に準拠した個人情報の扱い
- クリティカルなSPへの接続にも対応できるLoAの導入

学認トラストフレームワーク
よりセキュアで信頼性の高いフェデレーションを確立

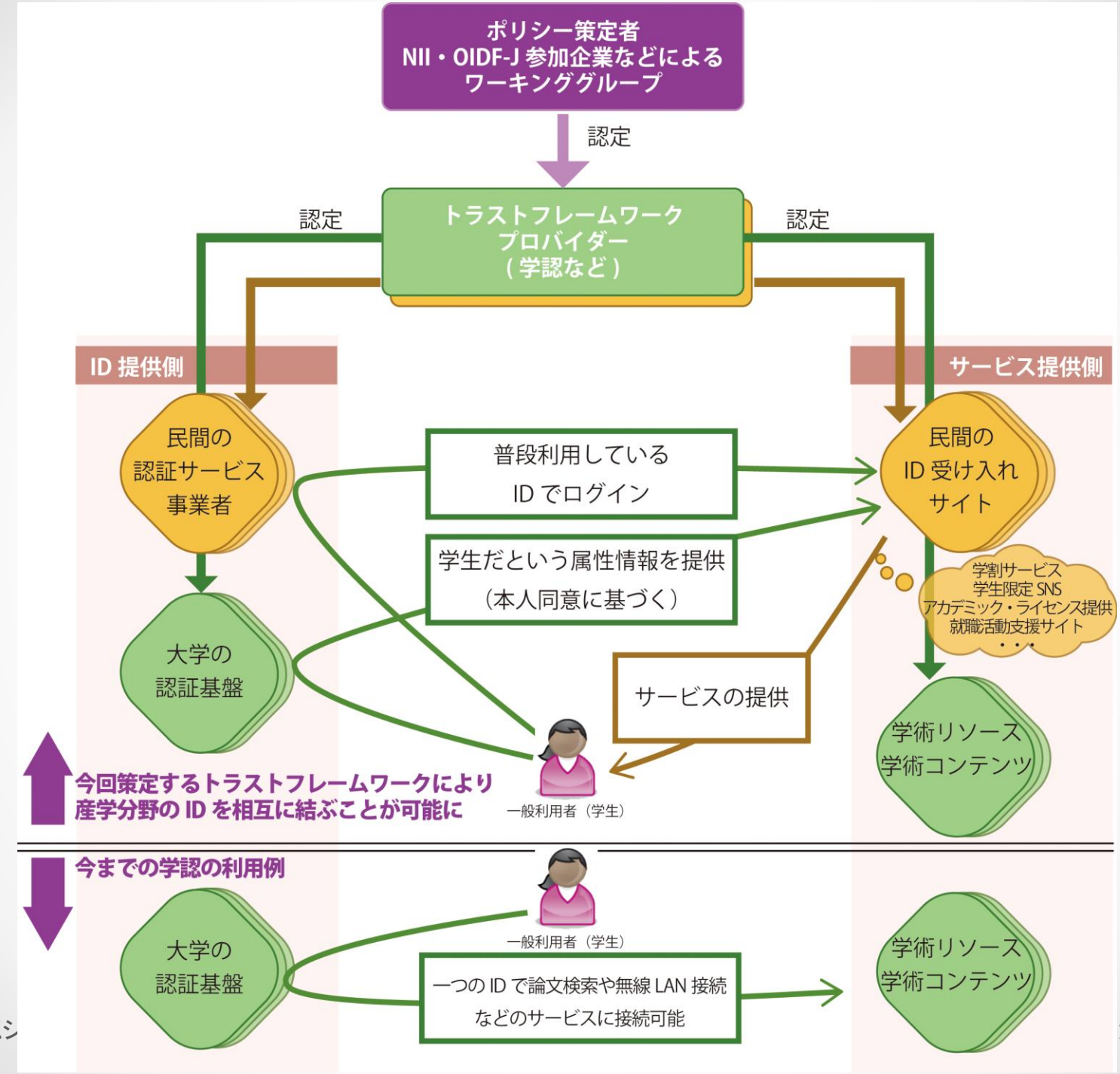
産学の ID をつなぐ世界初のトラストフレームワークの研究に着手
～利用者情報の安全な流通を目指し、学生向けサービスの提供を支援～

大学共同利用機関法人 情報・システム研究機構 国立情報学研究所
一般社団法人 OpenID ファウンデーション・ジャパン

国立情報学研究所（所長：坂内正夫、以下 NII）は、一般社団法人 OpenID ファウンデーション・ジャパン（代表理事：八木晃二、以下 OIDF-J）と共同して、「学術認証フェデレーション※1」（以下「学認」）と民間企業が提供するサービスをつなぐ「トラストフレームワーク※2」に関する研究を開始します。

本研究は、オンライン ID に信頼を付与し、さまざまなサービスで活用可能なエコシステムの実現を目指しています。産学分野の ID を相互に結ぶオープンなトラストフレームワークの策定は、世界初の試みとなります。

このトラストフレームワークの実現によって、これまでそれぞれ異なるルールや技術を用いて構築してきたサービスがシームレスにつながり、組織や業界、国境を超えた柔軟な認証が可能になるとともにさまざまな利用者情報を安全にやり取りすることが可能になります。ID 提供側とサービス提供側との信頼関係の構築が容易になることで、従来は不可能だった、より利便性の高いオンライン・サービスの創出が期待されます。


ポリシー策定者
NII・OIDF-J 参加企業などによる
ワーキンググループ
認定
認定
トラストフレームワーク
プロバイダー
（学認など）
認定
ID 提供側
サービス提供側
民間の
認証サービス
事業者
普段利用している
ID でログイン
民間の
ID 受け入れ
サイト
学生だという属性情報を提供
（本人同意に基づく）
学割サービス
学生限定 SNS
アカデミック・ライセンス提供
就職活動支援サイト
・・・
大学の
認証基盤
サービスの提供
学術リソース
学術コンテンツ
今回策定するトラストフレームワークにより
産学分野の ID を相互に結ぶことが可能に
一般利用者（学生）
今までの学認の利用例
一般利用者（学生）
大学の
認証基盤
一つの ID で論文検索や無線 LAN 接続
などのサービスに接続可能
学術リソース
学術コンテンツ