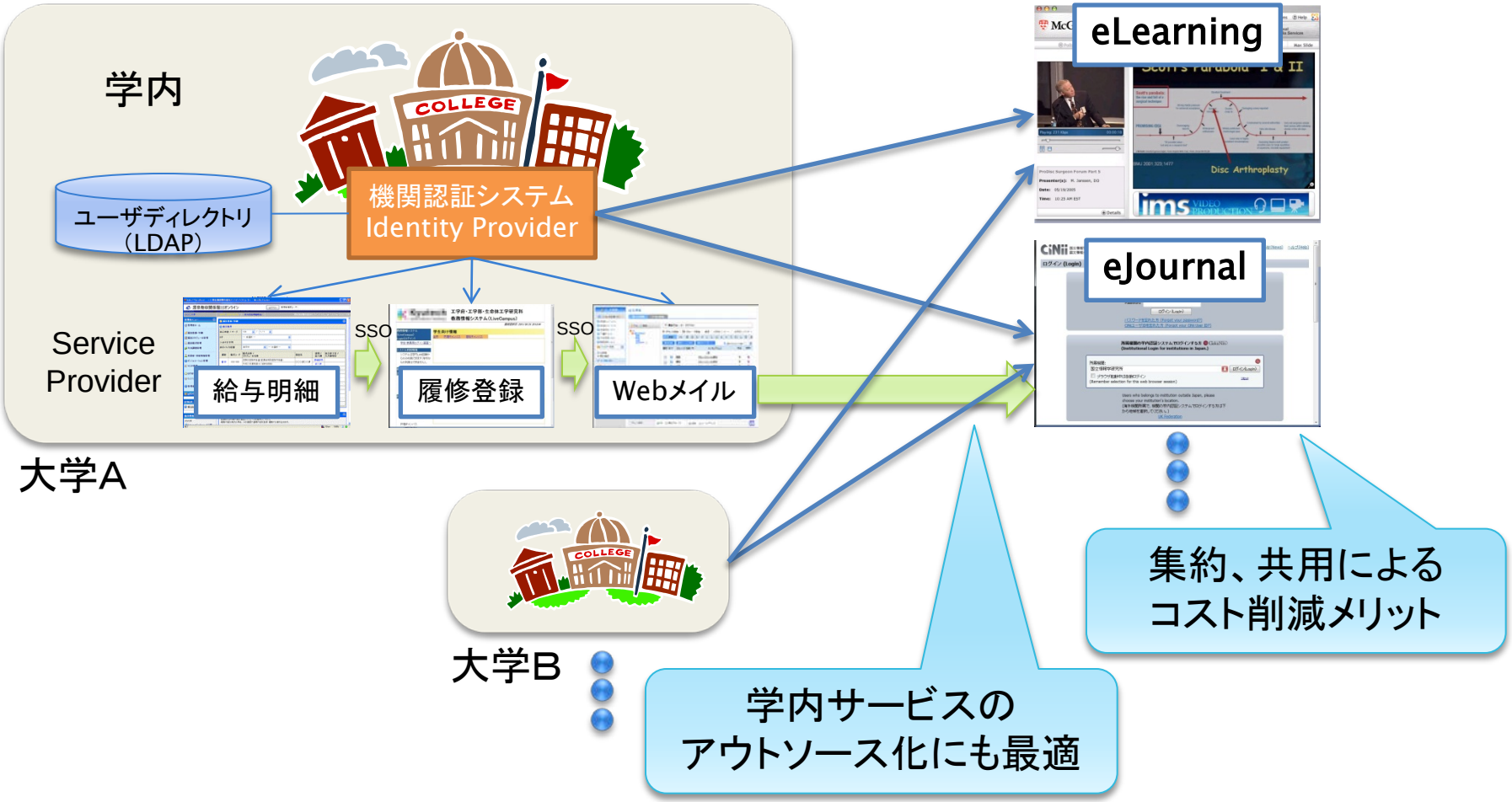
情報流通連携のための
オープンなID連携プラットフォームにおける
プライバシー保護機能の高度化の研究開発

中村素典、西村健、山地一禎/国立情報学研究所、佐藤周行/東京大学、
岡部寿男/京都大学、山崎崇生、南剛志、崎村夏彦/野村総合研究所

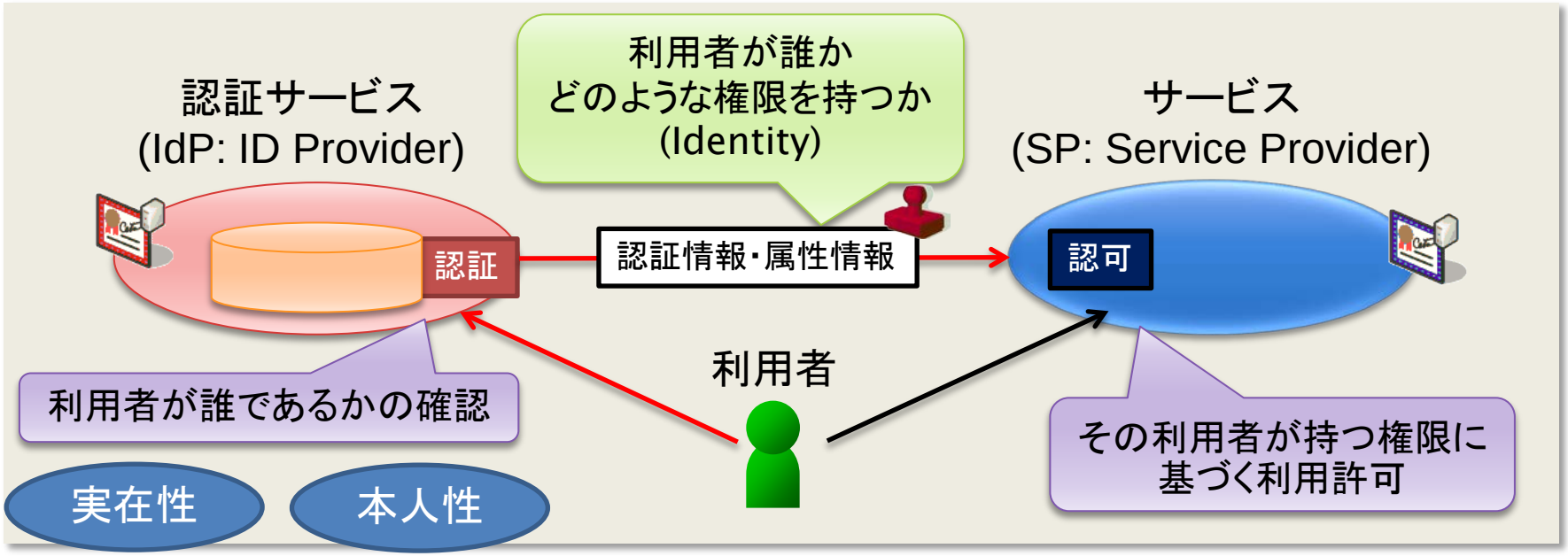
オープンなID連携基盤によるサービス共有

組織内に閉じていたシングルサインオン（SSO）の仕組みを組織外に



ID連携の基礎となる認証と認可の分離

- 認証
  - 利用者が誰であるかの確認
- 認可
  - その利用者が持つ権限に対応した利用許可



学術認証フェデレーション「学認」

- シングルサインオン(SSO)技術に基づく学術研究支援IT基盤の構築
- IdP･SP相互の信頼を持続する信頼フレームワークの提供
- 国際連携･産学連携による利便性向上、付加価値の実現、新サービスの創出
- 多様なニーズに応え、利便性･セキュリティを向上させる技術開発

クラウド活用を支援

LoA 認定による、PubMed、e-Radアクセス

学割サービス

多要素認証、個人情報保護、Virtual Organization

SP

サービス提供

図書館システム | Webメール | グループウェア | Eラーニング | 電子ジャーナル

大学間連携

GakuNin運営組織
- フェデレーション　ポリシーの策定
- IdP運用評価
- 広報･普及

ディスカバリーサービス | 学認申請システム | メタデータリポジトリ | 情報提供サイト

匿名性･仮名性実現 | 学内統合認証との連携 | 属性情報提供

ID管理

IdP

大学 A　教員

大学 B　職員

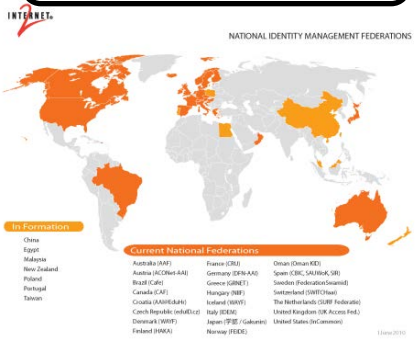
大学 C　学生

個人認証で学外からも快適アクセス

ID管理工数の低減
セキュリティレベルの底上げ
個人情報保護

シングルサインオンでスムーズなアクセス

フェデレーションの構築は世界各国で進行中!



コンテンツ系サービス

ScienceDirect
ISI Web of Knowledge
SpringerLink
SCOPUS
CAMBRIDGE UNIVERSITY PRESS
PATHOLOGY IMAGES
ebrary
EBSCO HOST
4
KOD
IEEE Xplore
360
IOPscience
KARGER
BioOne
Emerald
CENGAGE Learning
Researchmap
CiNii
NII-REO
Informatics SQUARE
JAIRO Cloud
Most of Major Publishers
nature.com
HighWire
palgrave macmillan
ANNUAL REVIEWS
eduroam
RefWorks
Microsoft DreamSpark

GakuNin Ready!
ICTSFC

各種基盤系サービス

UQ WiMAX
edubase
学内事務サービス
eLearning ePortfolio
FaMCUs
WebELS Ver. 6.0
Fshare β
Foodle

金沢大学総合メディア基盤センターデータリポジトリ
IMC Data Repository
Information Media Center of Kanazawa University
金沢大学 KANAZAWA UNIVERSITY
山形大学 YAMAGATA UNIVERSITY
広島大学
佐賀大学

フェデレーションの拡大に向けて
― 学認とOpenIDとの連携 ―

- 民間デファクトであるOpenID対応のサービスが、学認IdPで認証して利用できるようになれば、**学認（大学）向けのサービス**がさらに広がる
  - 学認にて**プロトコルゲートウェイ**によるOpenID Connect対応

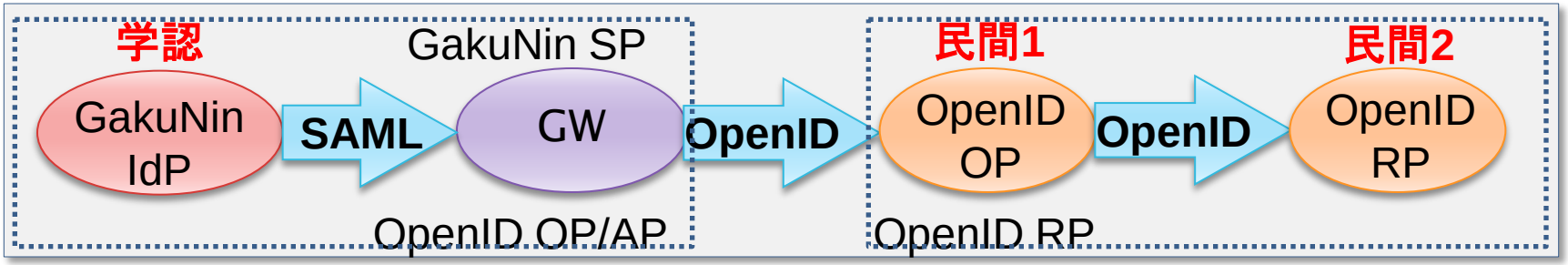
- 民間（OpenID OP）から 学認対応SP へのアクセスが可能になれば、**産学協同研究**の情報基盤としての活用や**保護者向けサービス**へも展開できる
  - Google/Yahooなどのアカデミックサービスを利用している大学の、学認参加も容易に

SAML/OpenID連携のパターン例

0. 学認に直接参加（SAMLのみ）

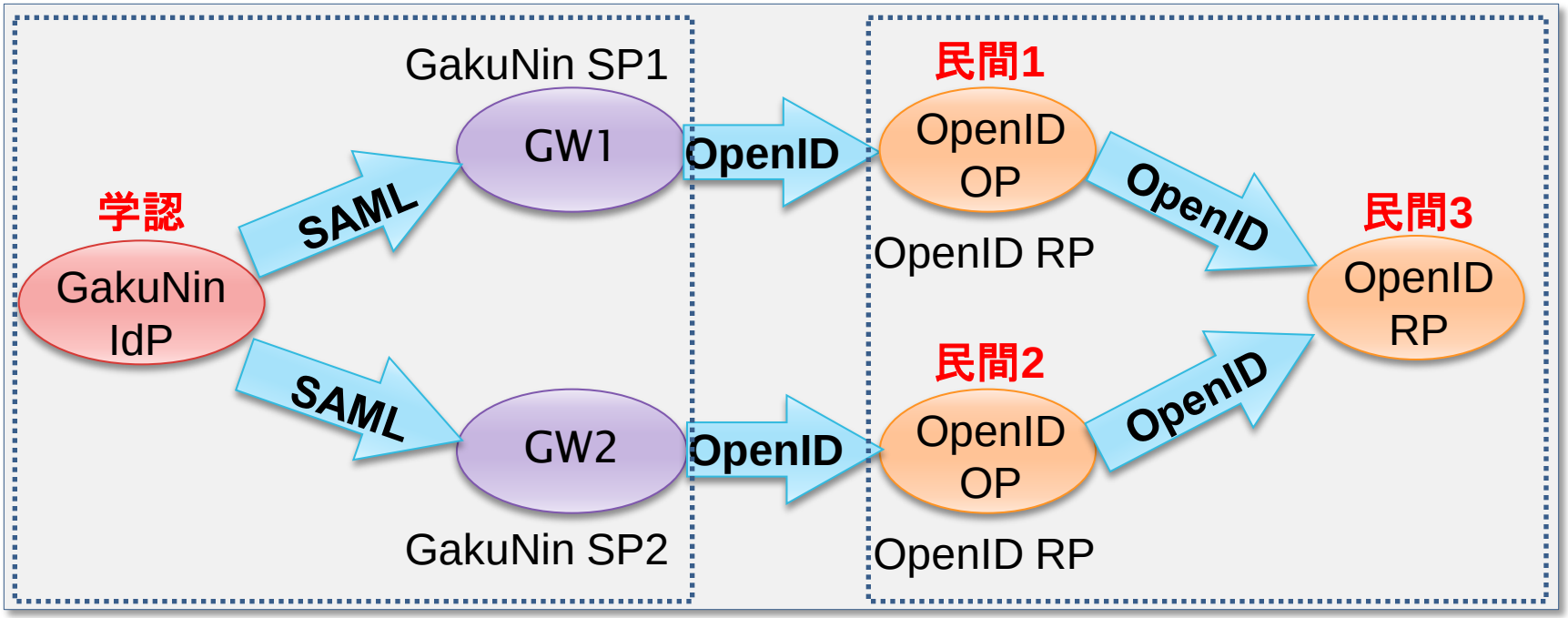
1. シンプルな連携

2. 民間OP経由の連携



SITFにおけるOpenID連携のパターン例

3. 複雑な連携



オープンなID連携基盤の拡大に向けて

属性情報の扱い（特にプライバシー）の不安の払拭が必要

- 「情報流通連携のためのオープンなID連携プラットフォームにおけるプライバシー保護機能の高度化」
  - PEOFIAMP: Privacy Enhancements for Open Federated Identity/Access Management Platforms
  - 平成24年度 総務省 戦略的国際連携型研究開発推進事業

    - ID連携プラットフォームにおけるID提供者、サービス提供者、ユーザそれぞれにおける、プライバシーにかかわる情報の扱いに関するポリシー表現とその制御を行う技術の開発
    - SAML、OpenIDそれぞれへの対応だけでなく、**両者の連携**利用も考慮し、実利用を目指した汎用的技術の開発

5つの研究開発課題とユースケース

① (1–1) バックチャネル在学確認におけるプライバシ保護

- 学割継続契約（毎月払、毎年払）における在学確認に対する同意

② (1–2/2–1) AP選択機能の実現と、AP連携の仮名化

- 成績証明（編入学、技能認定試験など）
- グローバル識別子を用いずにAPから当該ユーザの属性情報を取得

③ (1–3/2–2) 対IdP秘匿、認可条件秘匿

- 利用サービスのIdPに対する秘匿（学生証提示モデル）
- 就職活動時の成績条件に基づく採用一時フィルタリング

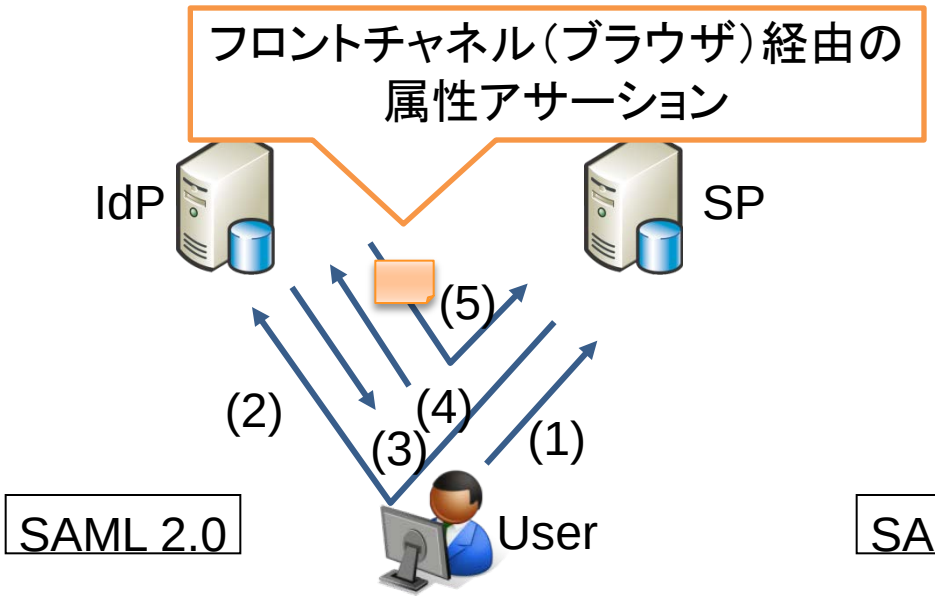
④ (1–4/2–3) 対プロキシ秘匿、プライバシに配慮した重複検出

- 属性情報のプロキシに対する秘匿
- 学割契約等の重複適用防止

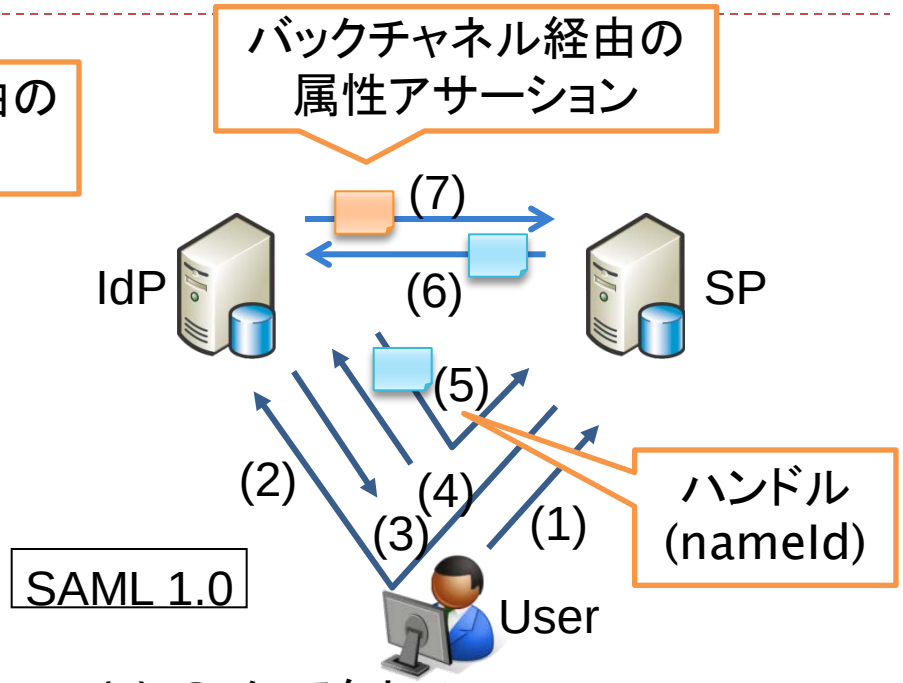
⑤ (2–4) 非WebサービスでのSSO活用による安全性向上

- SSH, IMAP, SMTP, …

SAMLによるSSO：2通りの属性情報受け渡し

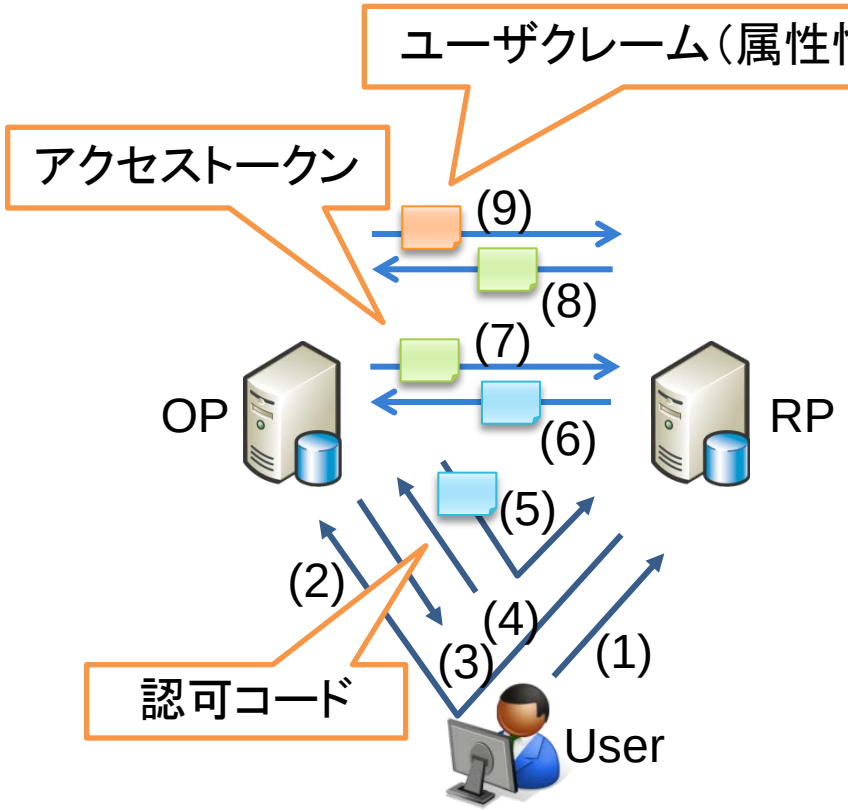


(1): SPへのアクセス
(2): DS経由でIdPにリダイレクト
(3): 認証要求
(4): *ID とパスワード*の入力
(5): 属性アサーションの送信



(1): SPにアクセス
(2): DS経由でIdPにリダイレクト
(3): 認証要求
(4): *ID とパスワード*の入力
(5): 属性情報取得のための*ハンドル*
(6): *ハンドル*による属性情報要求
(7): 属性アサーションの送信

OpenID ConnectにおけるSSOと属性情報受け渡し



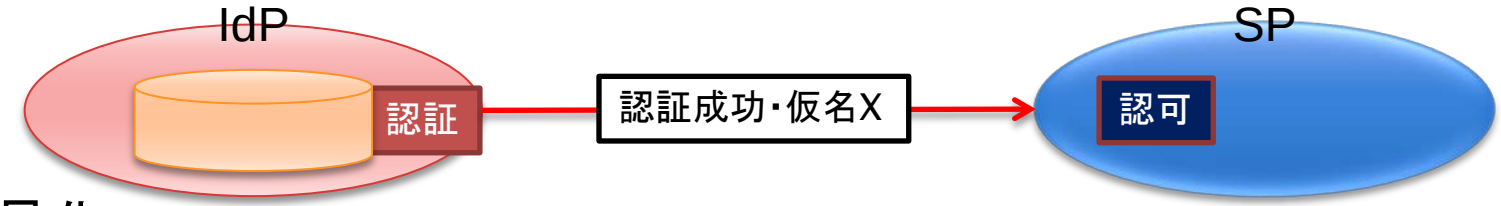
(1): RPにアクセス
(2): OPにリダイレクト
(3): 認証要求
(4): *ID* と*パスワード*の入力
(5): 属性情報取得のための認可コード
(6):認可コードでアクセストークン要求
(7): アクセストークン（＋IDトークン）
(8): アクセストークンでユーザクレーム要求
(9): ユーザクレーム（属性情報）

匿名、仮名によるプライバシー保護

- 通常アクセス

- 匿名アクセス
  - ID情報を送らないので、実際に誰かはわからない

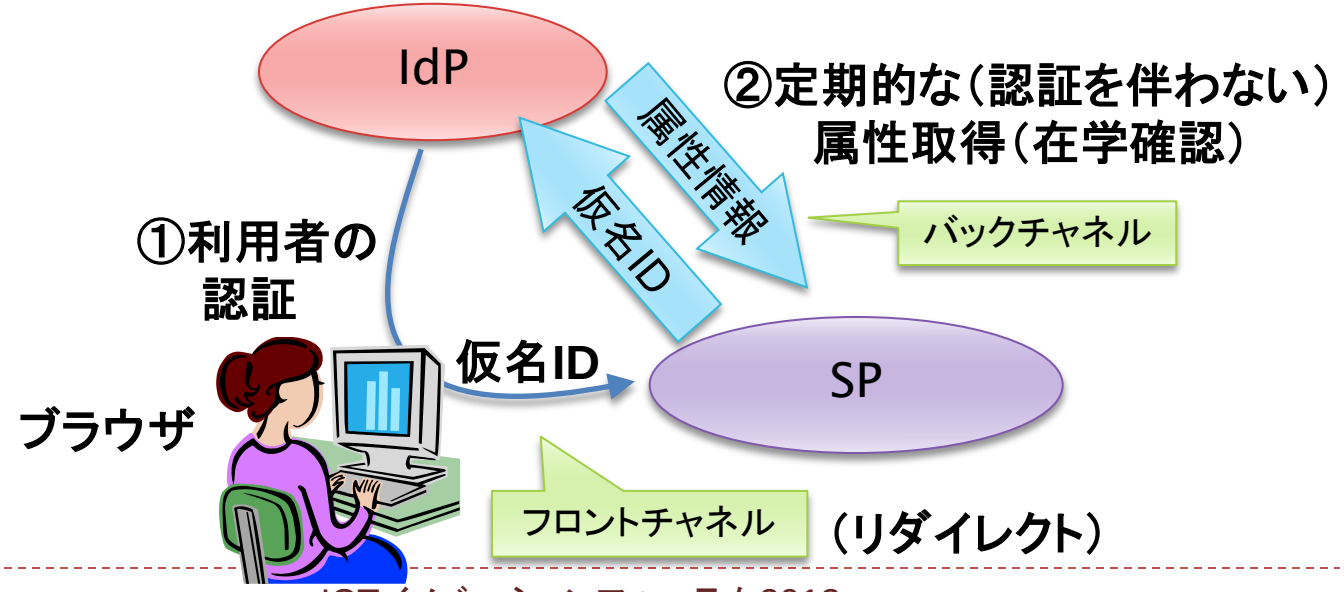
- 仮名アクセス (PPID: Pairwise Pseudonymous Identifier)
  - SP毎に異なるIDを送ることで、SP間での行動履歴の収集を防止



- 暗号化

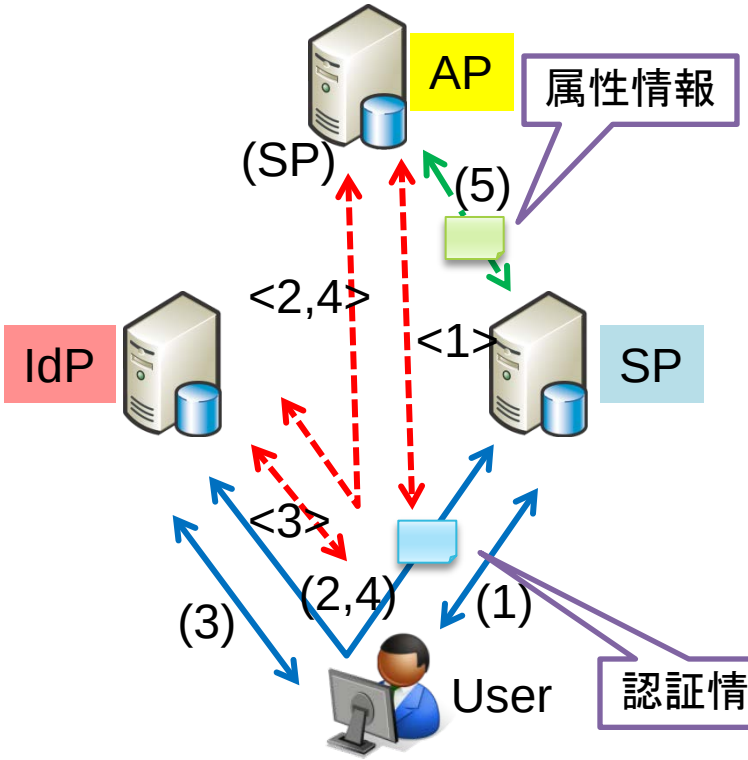
①バックチャネルにおける在学確認とプライバシ保護

- **定期的な在学確認**には利用者の介在が不要なバックチャネルが有効
- バックチャネルに利用者の識別のため仮名ID（persistentID、SP毎に異なる識別子）を用いた**定期的（認証非同期）な属性情報の取得**
  - 通常のtransientId(テンポラリなID)は月単位，年単位では持続しない
- バックチャネルによる認証非同期な属性情報取得のための**事前同意**
  - 属性情報の変化による、属性情報送信の停止
  - 属性情報の取得状況の確認と、同意のキャンセルの仕組みも用意



②属性プロバイダ(AP)の利用

- ユーザの属性情報は、様々な組織から提供される
  - IdP：ユーザ認証＋属性情報を提供
  - AP：属性情報の提供のみ



<1>: access to AP as a SP
<2>: redirect to IdP
<3>: authentication
<4>: assertion with attributes (ePPN)

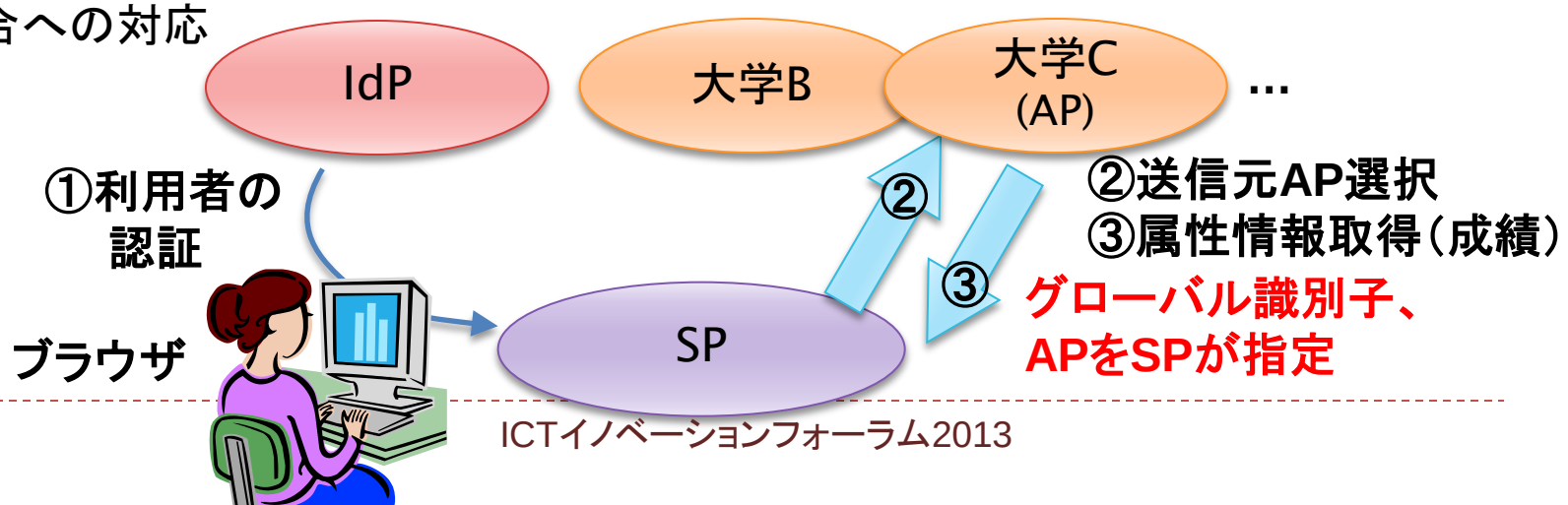
(1): access to SP
(2): redirect to IdP
(3): authentication
(4): assertion with attributes (ePPN)
(5): back-channel query with ePPN

AP連携の仮名化とAP選択機能の実現

- 従来のShibboleth実装によるAPからの属性取得（Simple Aggregation）
  - 利用者を示すグローバル識別子が必要
  - SPが参照するAPを指定する

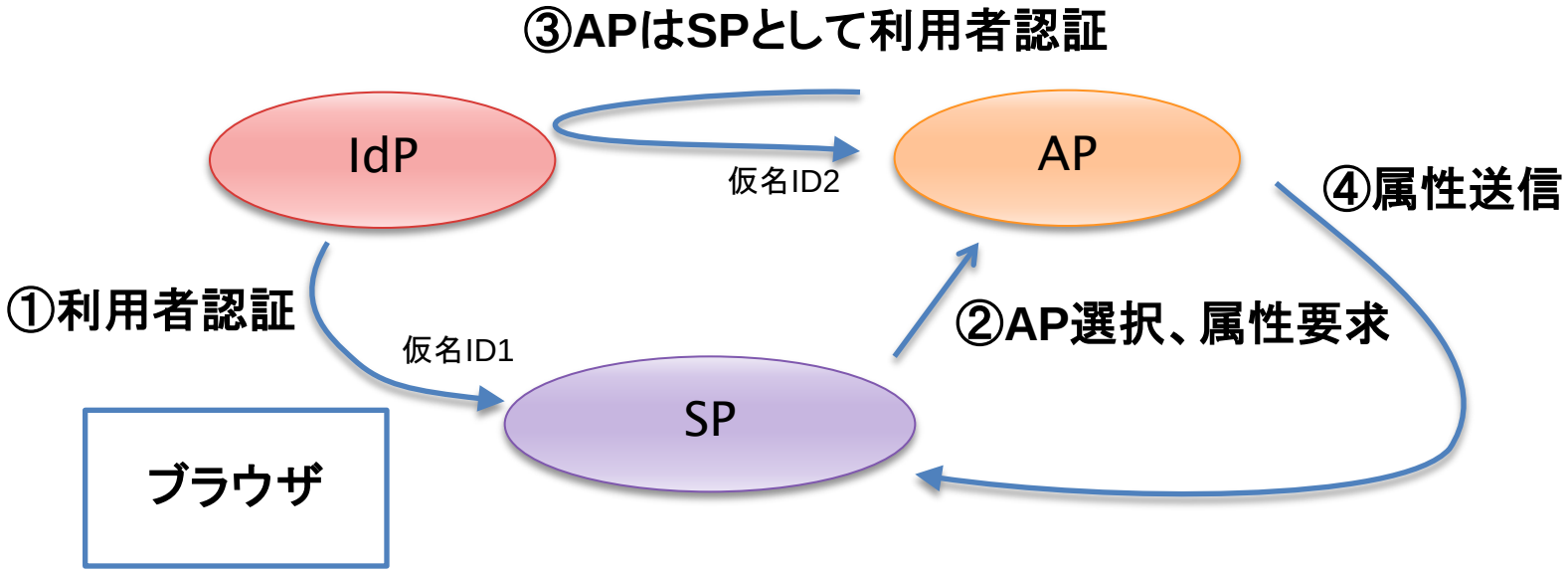
- 問題1：プライバシー（利用者追跡）の問題
  AP連携を行うSPはグローバル識別子を取得することになり、SPをまたがった利用者追跡が可能

- 問題2：多数のAPの中からの選択
  複数大学間での単位互換など、利用者が送信元の大学を選択する必要がある場合への対応



実現方法

- フロントチャネル経由の属性情報取得
  - APが同一IdPで再認証(SSO)することでグローバル識別子が不要
  - （副産物として）利用者認証と分離し，任意のタイミングでAPから属性取得が可能に（ブラウザ経由）

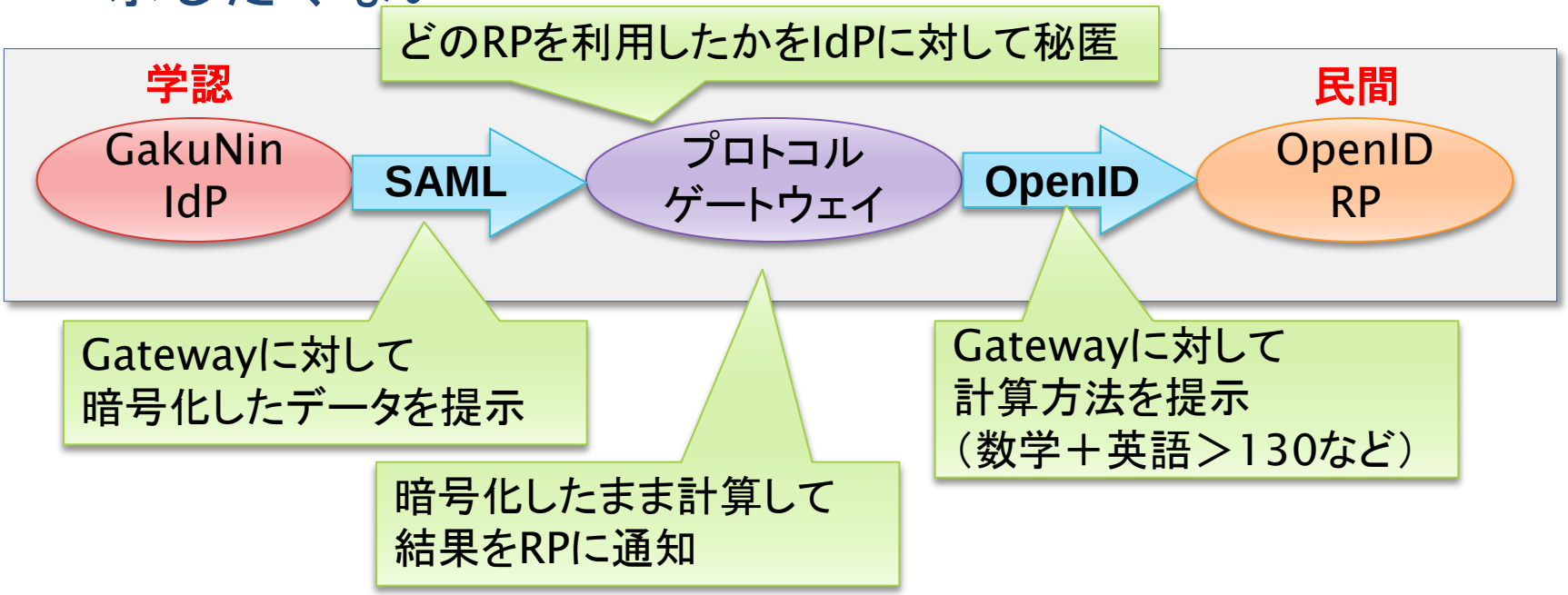


③対IdP秘匿、認可条件秘匿

A) IdPに対して、ユーザがどのRPを利用したかを秘匿

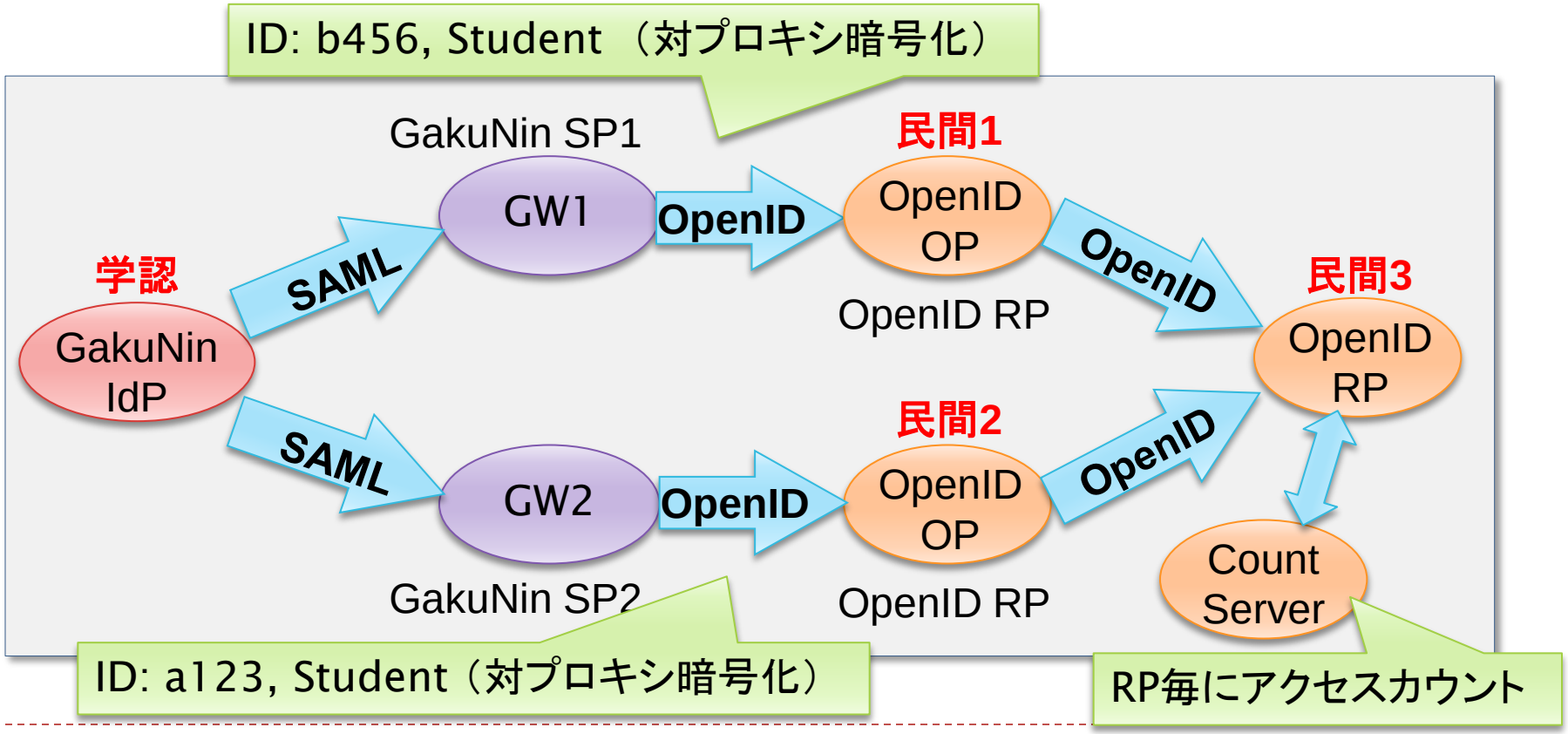
B) 属性情報の参照におけるプライバシ保護

- ✓ IdPはRPに対して、成績の生データを開示したくない
- ✓ RPはIdPに対して、成績をどのように利用したかを開示したくない



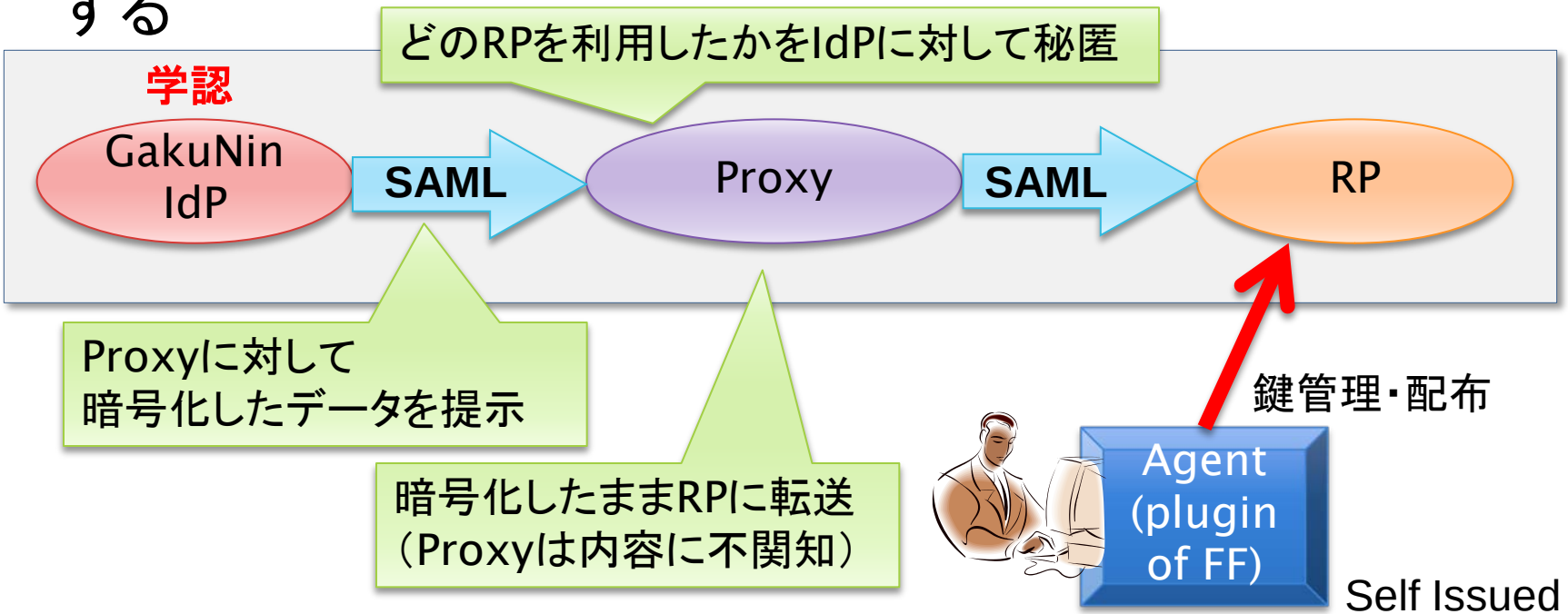
④対プロキシ秘匿、プライバシに配慮した重複検出

A) プロキシを経由する属性情報を、プロキシに見せない
B) 異なる民間IDへの属性情報の紐付けの考慮
   - ✓ 仮名性を維持したまま、重複検出



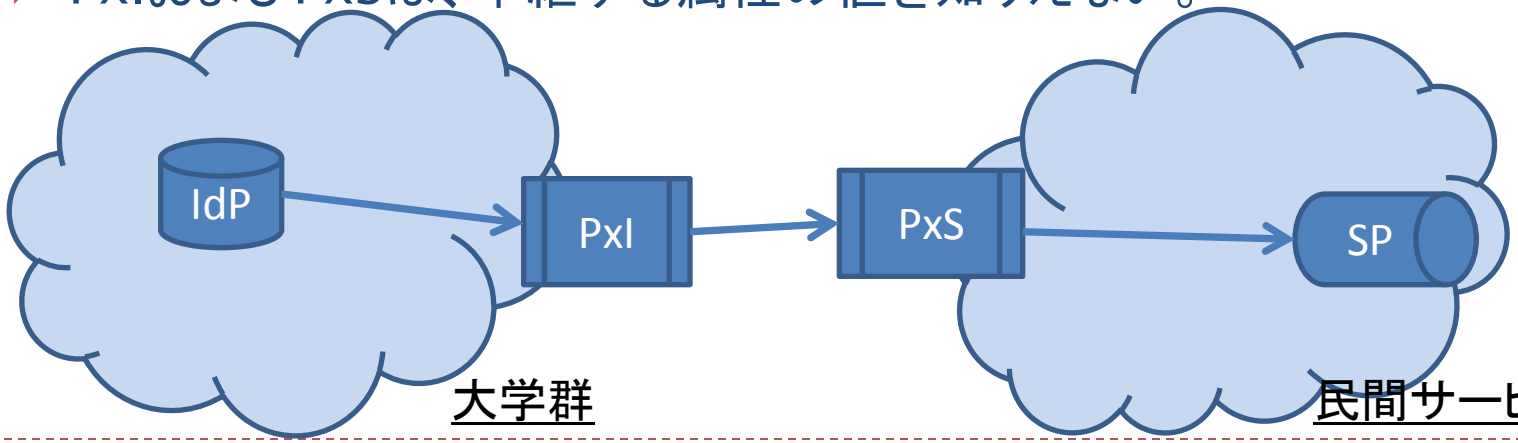
対IdP秘匿の方法1：エージェント利用

- IdPに対して、ユーザがどのRPを利用したかを秘匿できるProxyを開発（SimpleSAML.php）
- ここで用いる鍵管理を行うユーザエージェントを開発（FFのプラグインとして実装）-- SAML版SIIとして一部機能する



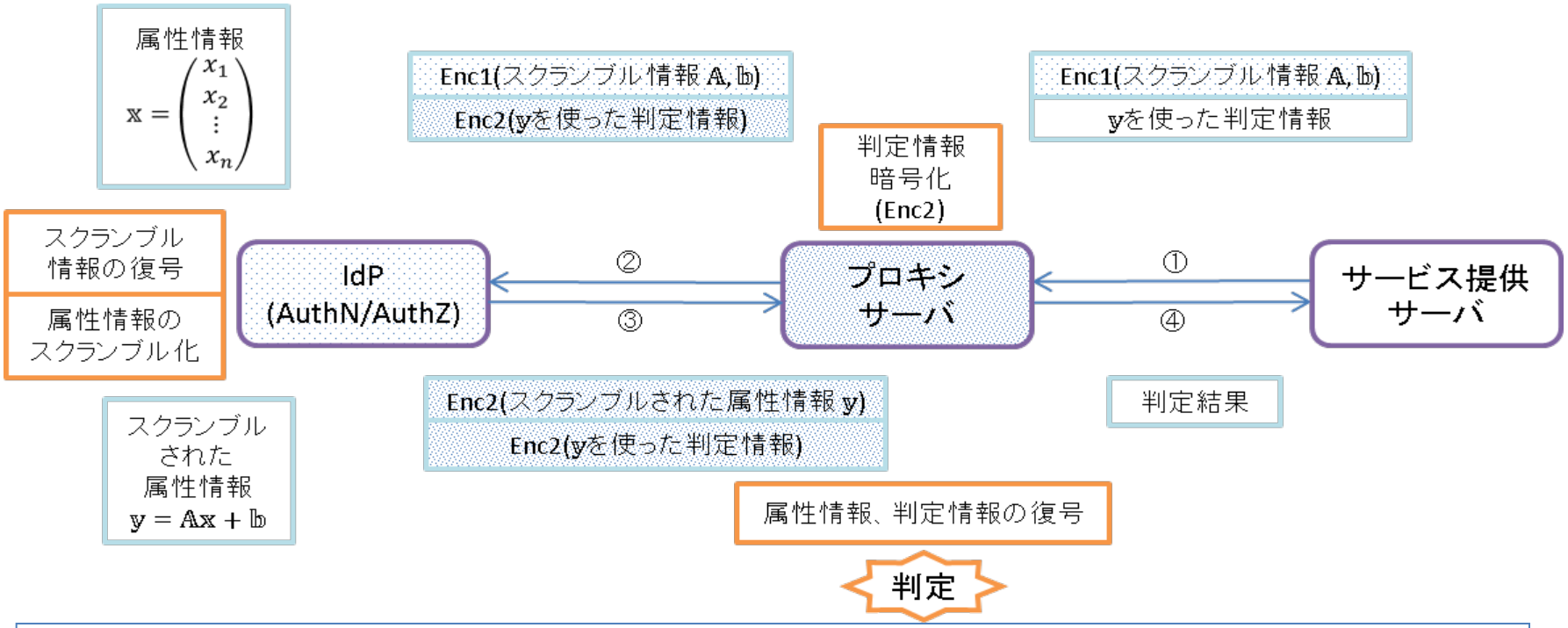
対IdP秘匿の方法2:カスケード型プロキシ

- 以下の要件を満たすカスケード型proxyをShibbolethで開発
- 前提(例)
  - IdP群と、それを代表するproxy IdP　PxI
  - SP群と、それを代表するproxy SP　PxS
- 要件
  - IdPは、自分が送出する属性がどのSPに届くかを知りえない。
  - SPは、自分が受け取った属性がどのIdPから送られて来たかを知りえない。
  - PxIおよびPxSは、中継する属性の値を知りえない。



属性と判定条件を相互に秘匿する方法

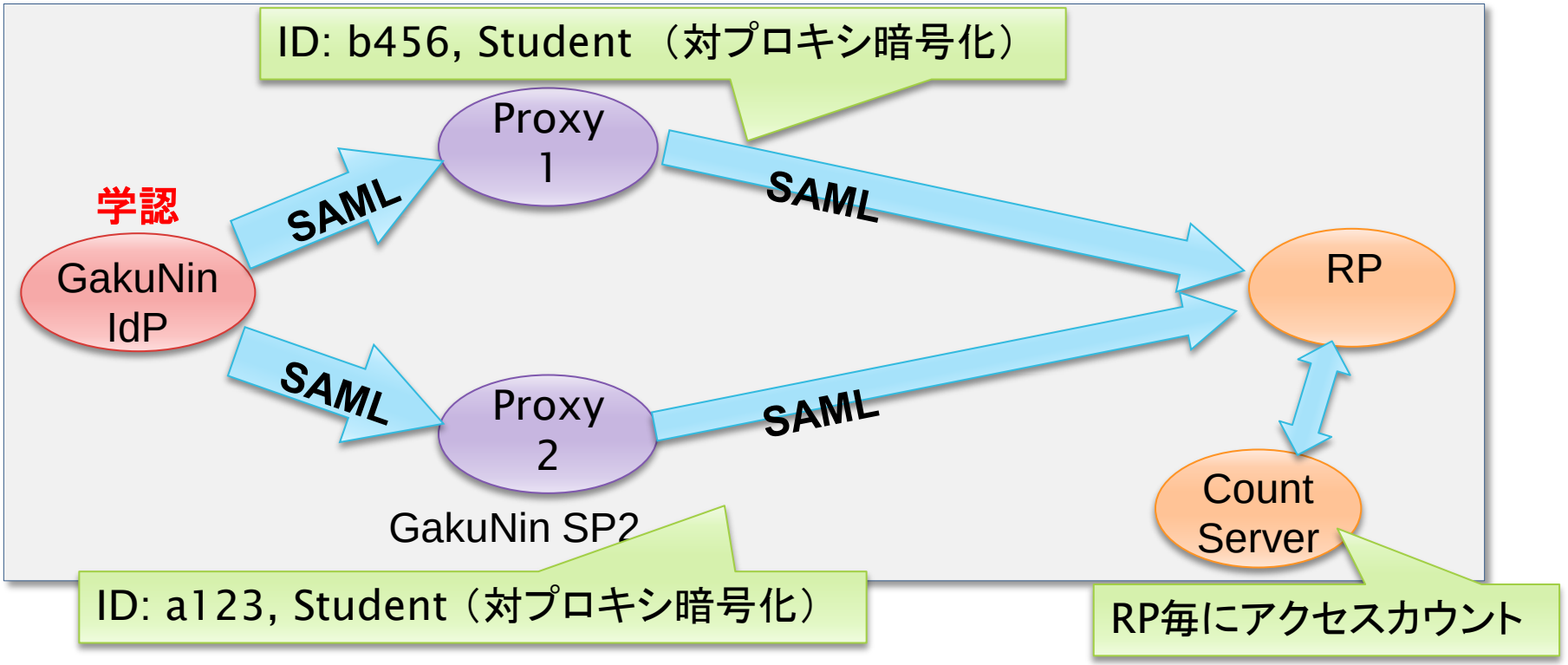
- IdPには、SPが認可にどのような判定条件を用いるかが秘匿される
- SPには、IdPが提示する属性が秘匿される
- Proxyには、判定条件も属性もスクランブルされていてわからない



応用例：企業(SP)が就職面接の第一次選抜に大学(IdP)が提示する成績を用いる

研究開発の成果（東大2）
プライバシに配慮した重複検出

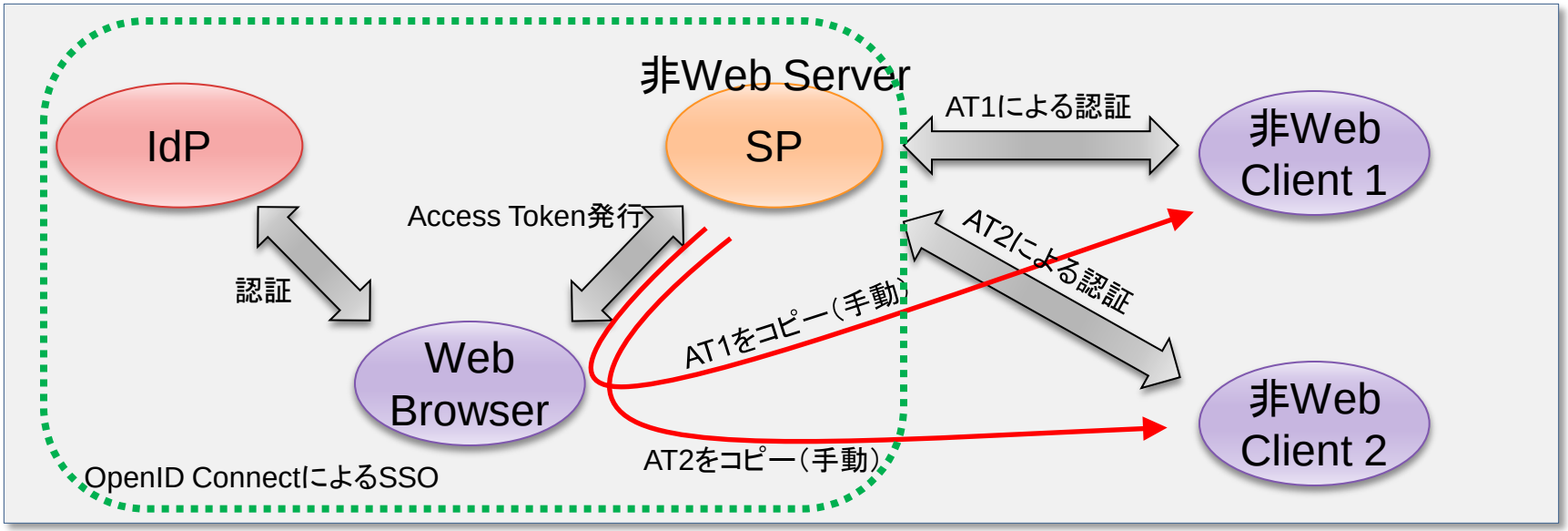
- 異なるIDへの属性情報の紐付け
  - SPに対して仮名性を維持したまま、サービス受信の重複検出を可能にするcount serverを実装（SimpleSAML.phpのSP）
  - SP側でのサービス提供の可能性を広げる



⑤非Webサービスでの SSO活用による安全性向上

- 様々なデバイスに同じパスワードを設定したくない
  - 非Webなので、Web向けSSOの仕組みが使えない
  - 従来の非Webクライアントを改変するのは面倒

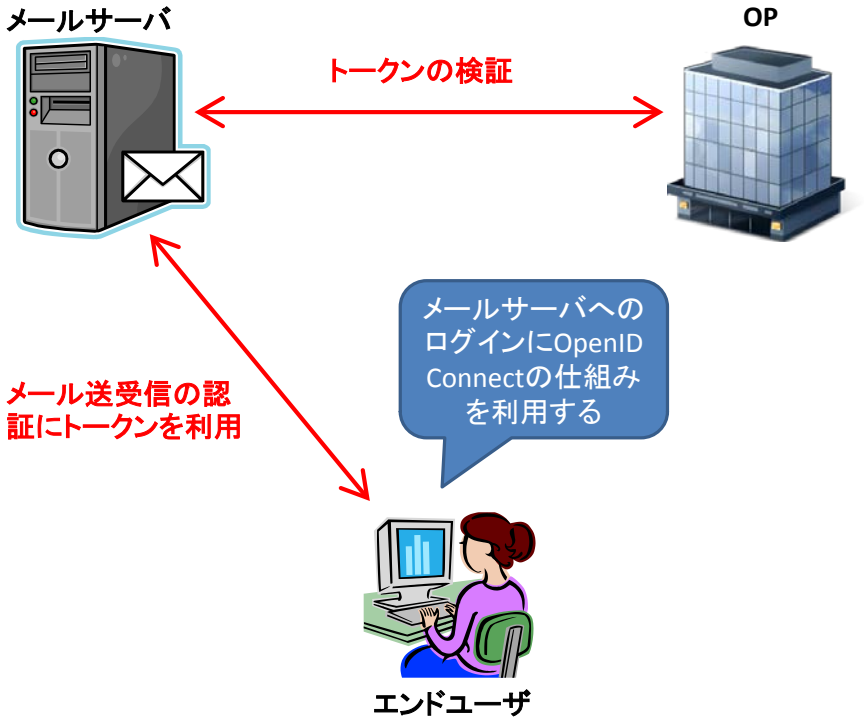
認証した相手毎に別途発行されるアクセストークンを利用



クライアントごとに、パスワードの更新が可能（デバイスを無くしても安心）

電子メール環境における動作検証

- ThunderbirdのIMAP用のトークン
- ThunderbirdのSMTP用のトークン
- iPhoneのIMAP/SMTP用のトークンの発行
- PuttyのSSH用のトークン
  - 以上に関して動作を確認



EUとの共同研究体制

- GEANT Project (FP7 GN3)
  Multi-gigabit european research and education network and associated services) [2009/4 – 2013/3]
  - Brook Schofield
    - Project Development Officer, TERENA (Amsterdam, Netherlands)
    - eduGAIN (FP7 GN3/SA3/T3) Product Manager and Task Leader
      - 国を単位として構築されている各国の学術認証フェデレーションの相互接続を行うアーキテクチャやポリシーについての研究開発とその実現
        - フェデレーション間の相互接続における技術的課題や法制度的課題についての共同研究を行い、成果物に反映する。
  - Roland Hedberg
    - (FP7 GN3/JRA3) Project
    - IT-arkitekt, Umea University (Umea, Sweden)
      - OpenID Connect等のシステム開発および相互接続性に関する研究を実施
        - OpenID 関連の研究開発についての協力
  - （参考）GEANTとNIIとは、欧州地域学術研究ネットワークであるGEANT Networkを介した研究の支援や、GEANTが推進するアジア地域学術研究ネットワークであるTEINの運用に関して協力関係にありMoUを結んでいる。

まとめと今後の課題

- ５つの課題について、
  プライバシー、セキュリティに配慮した
  ID連携プラットフォームの改良を実施、動作を確認

- 研究開発成果の公開と活用
  - オープンソース
    - 公開、フィードバック
  - 標準化提案
    - draft-sakimura-oidc-structured-token-01
    - draft-sakimura-oidc-extension-nonweb-01
  - SITF等における実サービスへの展開
    （学割、学増しサービスなど）

今後に向けて

- トラストフレームワークの展開
  - 学術から政府・民間も含む形へ一般化、さらに国際化
  - IDの保証のレベルの分類と格付け
    - 商用ID (Google, MS, Yahoo!, Apple, 楽天, …)
    - 公的ID
      - 共通番号制度
    - 準公的ID
      - 学生ID:学認
      - 社員ID
- LoA (Level of Assurance)を保証できる制度設計と、必要となる要素技術の開発
  - 多要素認証を含む認証手順の強化と、LoAの格付け
  - LoAに応じた属性交換によるプライバシー保護の強化