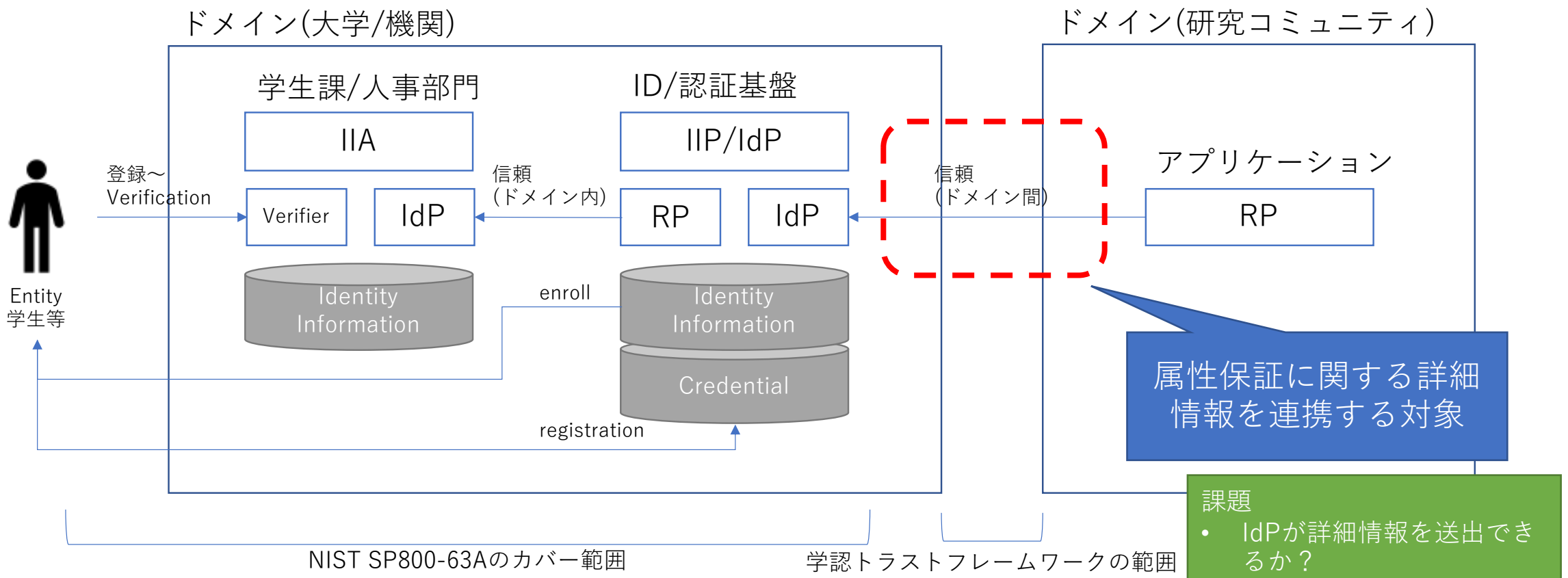
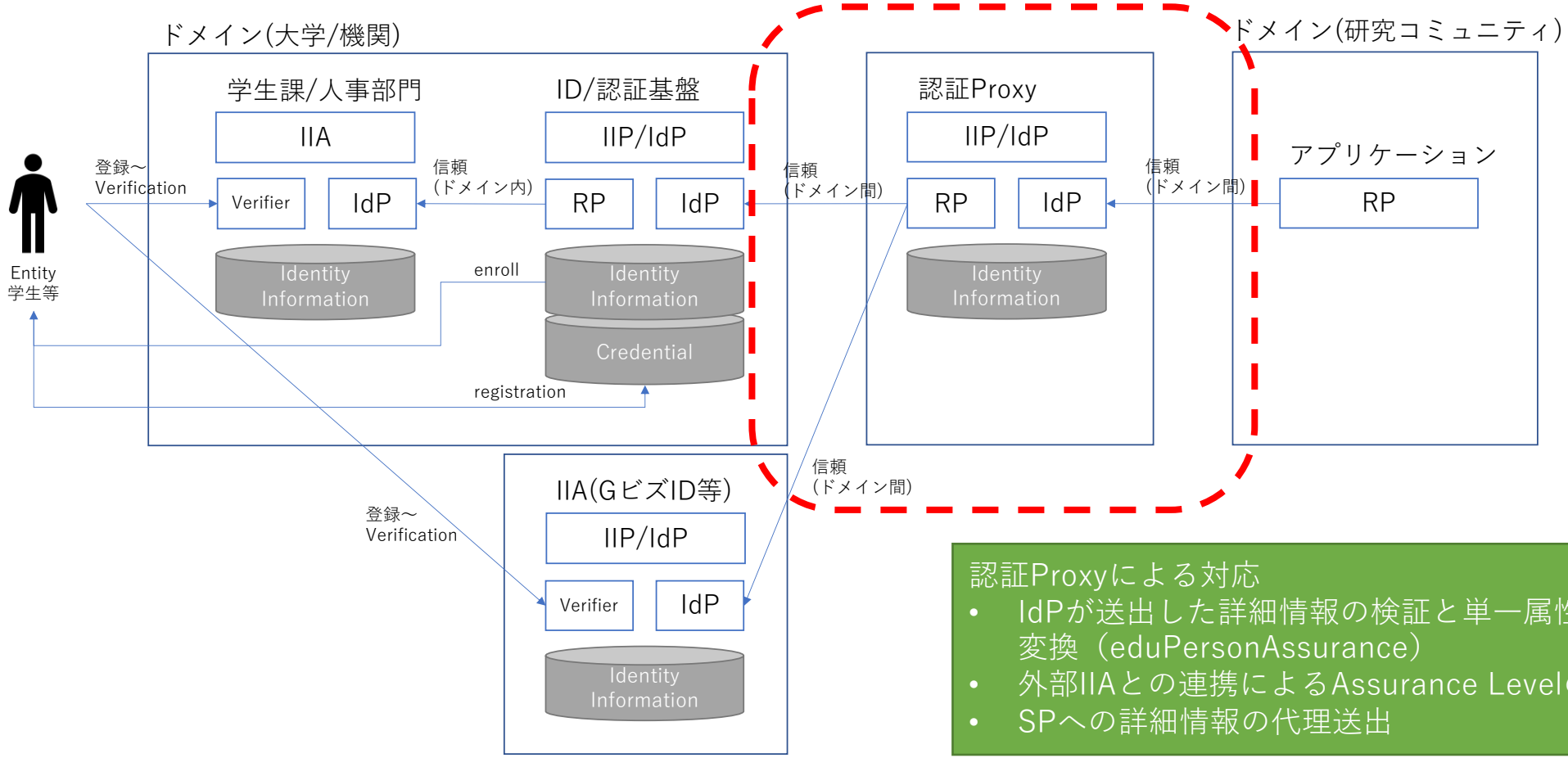
ID保証の表現方法（ミニマム実装案）

伊藤忠テクノソリューションズ株式会社
OpenID Foundation
富士榮　尚寛


ドメイン(大学/機関)
ドメイン(研究コミュニティ)
学生課/人事部門
ID/認証基盤
IIA
IIP/IdP
アプリケーション
登録～
Verification
Verifier
IdP
信頼
(ドメイン内)
RP
IdP
信頼
(ドメイン間)
RP
Entity
学生等
Identity
Information
enroll
Identity
Information
Credential
registration
属性保証に関する詳細情報を連携する対象
課題
IdPが詳細情報を送出できるか？
SPが詳細情報を受け取り検証できるか
NIST SP800-63Aのカバー範囲
学認トラストフレームワークの範囲

認証Proxyによる吸収



認証Proxyによる対応

- IdPが送出した詳細情報の検証と単一属性への変換（eduPersonAssurance）
- 外部IIAとの連携によるAssurance Levelの向上
- SPへの詳細情報の代理送出

現状のIdP/SPの状況を踏まえたパターン

		SP		
		詳細属性に対応可能	**単一属性なら対応可能**	**対応不可**
IdP	**詳細属性に対応可能**	**<u>③詳細属性の送出～検証</u>**	**<u>③認証Proxy等で対応</u>** - 詳細属性の受け取り - eduPersonAssuranceへ変換しSPへ送出	**<u>③認証Proxy等で対応</u>** - 詳細属性の受け取り - SPは認証Proxyを暗黙t形に信頼
	単一属性なら対応可能	**<u>③認証Proxy等で対応</u>** - eduPersonAssuranceの受け取り、IdPより情報を収集 - 詳細属性を送出	**<u>②eduPersonAssuranceを送出～検証</u>**	**<u>②認証Proxy等で対応</u>** - eduPersonAssuranceの受け取り - SPは認証Proxyを暗黙的に信頼
	対応不可	**<u>③認証Proxy等で対応</u>** - IdPから情報を収集 - 詳細属性を送出	**<u>②認証Proxy等で対応</u>** - IdPを暗黙的に信頼 - eduPersonAssurance生成しSPへ送出	**<u>①現状</u>** 相互に暗黙的に信頼

ステップ

① 現状：暗黙的な信頼

② eduPersonAssuranceの活用

- データの標準化：例）Gakunin_IAL1, Gakunin_AAL2
  - トラストフレームワーク
  - レベル
- 認証Proxyによる属性送出の代行

③ 詳細属性への対応

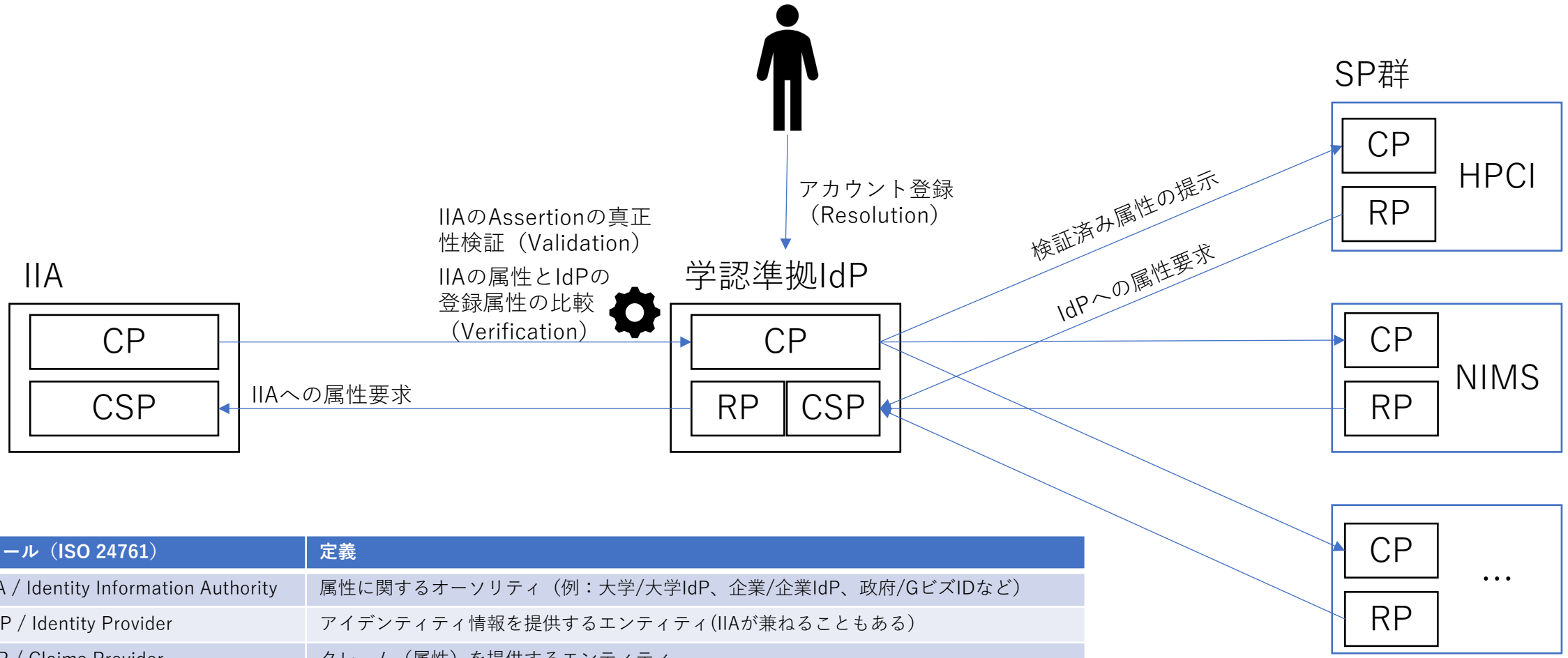
- Identity Assurance表現への対応

以降、バックアップ

背景

- 研究コミュニティにおいては本人確認＜所属確認
  - 戸籍上の本人確認を主眼に置いた現状のeKYCサービスはあまり役に立たない
  - 所属機関によるお墨付きが重要
- OpenID Connectの世界ではIALを表現するためにレベル＋具体的な確認方法やエビデンスも含めてRP（SP）へ送出するプロファイル（OpenID Connect for Identity Assurance）の開発が行われている。また同時に所属していることを表明するための方法（Authority Claims）もあわせて検討されている
- eKYC等の本人確認手段の評価・検討を行う前に各研究コミュニティが求める本人確認・所属確認の結果に関する情報の精査と送出方法を検討する必要があるのではないか？
  - 具体的には学認IdPが送出する属性にValidation/Verification結果やEvidence情報を含めるとどうなるか？
- その上で、運用の効率化を行うためにeKYCサービスを採用することを検討する方がよいのではないか？

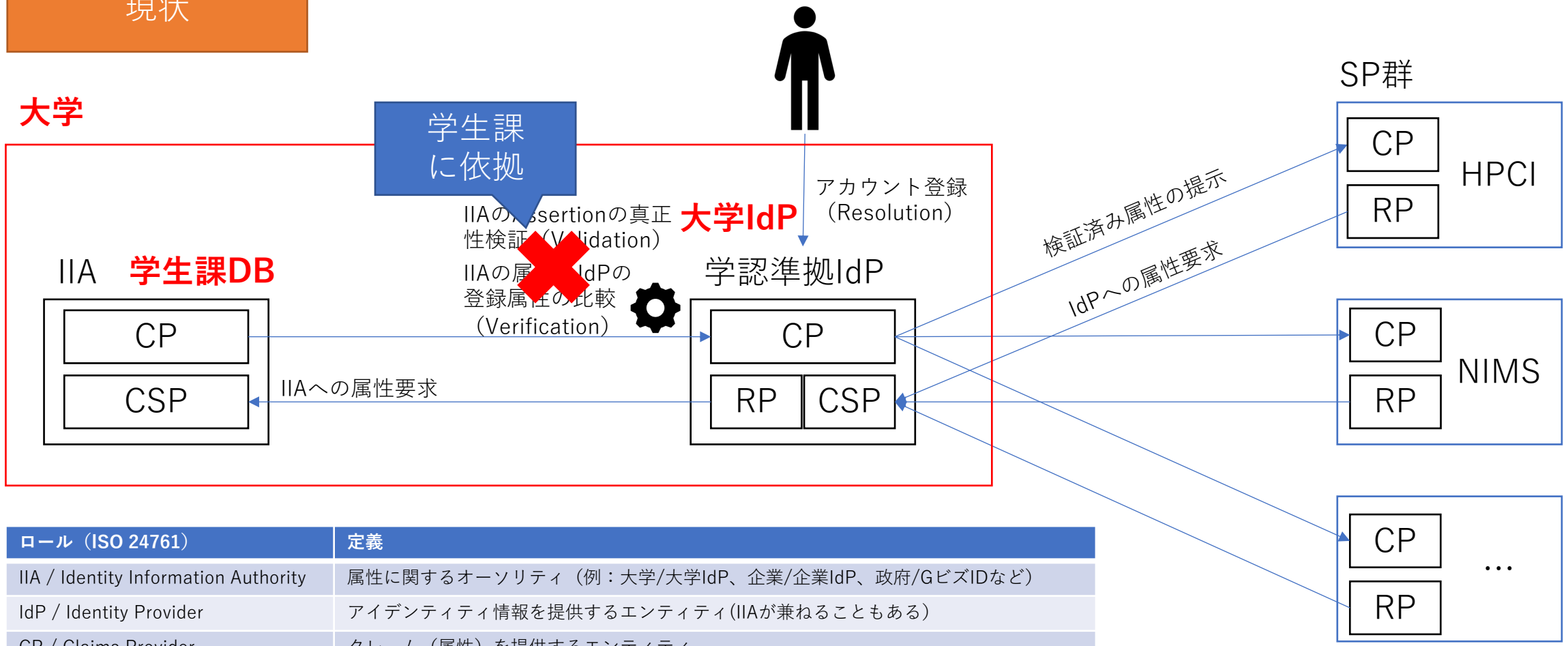
学認トラストフレームワークの適用イメージ



ロール（ISO 24761）	定義
IIA / Identity Information Authority	属性に関するオーソリティ（例：大学/大学IdP、企業/企業IdP、政府/GビズIDなど）
IdP / Identity Provider	アイデンティティ情報を提供するエンティティ(IIAが兼ねることもある)
CP / Claims Provider	クレーム（属性）を提供するエンティティ
CSP / Credential Service Provider	クレデンシャル（認証時に利用する属性）の管理を行うエンティティ
RP / Relying Party	とくていのエンティティのアイデンティティ情報に依拠するエンティティ

学認トラストフレームワークの適用イメージ

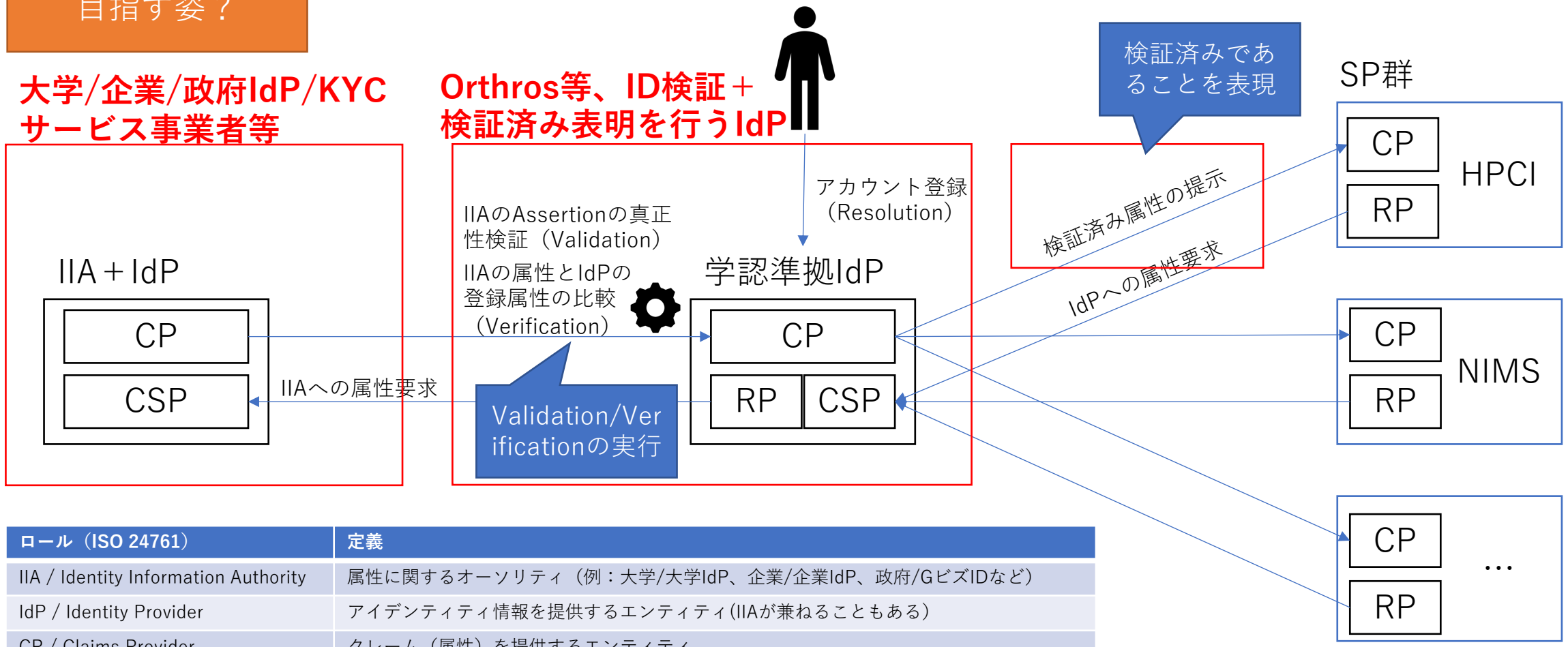
現状



ロール（ISO 24761）	定義
IIA / Identity Information Authority	属性に関するオーソリティ（例：大学/大学IdP、企業/企業IdP、政府/GビズIDなど）
IdP / Identity Provider	アイデンティティ情報を提供するエンティティ(IIAが兼ねることもある)
CP / Claims Provider	クレーム（属性）を提供するエンティティ
CSP / Credential Service Provider	クレデンシャル（認証時に利用する属性）の管理を行うエンティティ
RP / Relying Party	とくていのエンティティのアイデンティティ情報に依拠するエンティティ

学認トラストフレームワークの適用イメージ

目指す姿？



ロール（ISO 24761）	定義
IIA / Identity Information Authority	属性に関するオーソリティ（例：大学/大学IdP、企業/企業IdP、政府/GビズIDなど）
IdP / Identity Provider	アイデンティティ情報を提供するエンティティ(IIAが兼ねることもある)
CP / Claims Provider	クレーム（属性）を提供するエンティティ
CSP / Credential Service Provider	クレデンシャル（認証時に利用する属性）の管理を行うエンティティ
RP / Relying Party	とくていのエンティティのアイデンティティ情報に依拠するエンティティ

検証済み属性の表現
OIDC4IDAをベースにSAML Assertionをデザイン

【送出すべき事項/IAL判別情報】
- Evidenceとして何を使ったのか
- どうやって（＋いつ、だれが）Evidence確認をしたのか
- Verificationをどうやって（＋いつ、だれが）行ったのか

【要検討】
- レベルで分けて送出するか（Strong/Weak・・・）
- 生ログを含めて送出するか（実際の確認手段・結果・Evidenceそのもの）

OIDC4IDAの例（個人の証明/Trustframework）


```
{
 "verified_claims": {
  "verification": {
   "trust_framework": "eidas",
   "assurance_level": "substantial"
  },
  "claims": {
   "given_name": "Max",
   "family_name": "Meier",
   "birthdate": "1956-01-28",
   "place_of_birth": {
    "country": "DE",
    "locality": "Musterstadt"
   },
   "nationalities": [
    "DE"
   ]
  }
 }
}
```


EU/EIDASのトラストフレームワークでSubstantialレベルで確認済み

確認済みの属性情報

OIDC4IDAの例（個人の証明/Evidence）


```
{
 "verified_claims": {
  "verification": {
   "trust_framework": "uk_tfida",
   "assurance_level": "medium",
   "assurance_process": {
      "policy": "gpg45",
      "procedure": "m1b"
   },
   "time": "2021-05-11T14:29Z",
   "verification_process": "7675D80F-57E0-AB14-9543-26B41FC22",
   "evidence": [
    {
      "type": "document",
      "validation_method": {
        "type": "vpiruv",
        "policy": "gpg45",
        "procedure": "score_3"
      },
      "verification_method": {
          "type": "pvp",
          "policy": "gpg45",
          "procedure": "score_3"
        },
      "time": "2021-04-09T14:12Z",
        "document_details": {
          "type": "driving_permit",
          "personal_number": "MORGA753116SM9IJ",
          "document_number": "MORGA753116SM9IJ35",
          "serial_number": "ZG21000001",
          "date_of_issuance": "2021-01-01",
          "date_of_expiry": "2030-12-31",
          "issuer": {
            "name": "DVLA",
            "country": "UK",
            "country_code": "GBR",
            "jurisdiction": "GB-GBN"
          }
        }
      }
    ]
  },
  "claims": {
    "given_name": "Sarah",
    "family_name": "Meredyth",
    "birthdate": "1976-03-11",
    "place_of_birth": {
      "country": "UK"
    },
    "address": {
      "locality": "Edinburgh",
      "postal_code": "EH1 9GP",
      "country": "UK",
      "street_address": "122 Burns Crescent"
    }
```


UK/TFIDAでMediumと判定。確認プロセスはGPG45準拠

確認に使ったエビデンスと確認方法

エビデンス詳細

確認済みの属性情報

OIDC4IDAの例（所属の証明）


```
{
   "sub": "BSmith",
   "email": "bobsmith@example.com",
   "verified_claims": {
    "verification": {
      "trust_framework": "entity_claims_example_framework",
      "time":"2020-04-23T18:25Z",
      "verification_process":"f24c6f-6d3f-4ec5-973e-b0d8506f3bc7"
    },
    "claims": {
      "given_name": "Bob",
      "family_name": "Smith",
      "birthdate": "1981-01-26",
      "authority": [ {
         "applies_to": {
            "company_name": "Example Company Limited",
            "company_number": "12351235",
            "jurisdiction": "england-wales"
         },
```

```
"permission": [ {
            "role": "Director",
            "validity":[ {
               "start": "2018-03-02T10:00Z"
               }]
         }],
         "granted_by": {
            "method": "appointment",
            "granting_body": "Companies House",
            "reason": "Official company officer"
         }
      }]
   }
}
```


どの機関に所属しているか？

どのような役割/立場か？

どうやってEnrollされたか？

継続検討となる課題

- 継続確認も必要ではないか
- IDaaS自体の運用
  - 誰が運用するか
  - 誰がアサーションに署名するか

- 大学が全員に対してIAL2を保証できるとは思わない
- する必要もない
- あるべき姿はSPが必要なIAL/AALを要求
- IdPはなんらかの手段で要求されたものを返す
- 手段の一つがOrthros