作成日：2022/02/20
更新日：2022/02/21

学認における検証済み属性表現の必要性と技術仕様（案）

伊藤忠テクノソリューションズ株式会社
OpenID Foundation eKYC-IDA WG
OpenID ファウンデーションジャパン
富士榮　尚寛

次世代の学認参加機関の Identity Provider が発行する検証済み属性表現の仕様案を示す。

1. 学認トラストフレームワークにおける検証済み属性表現の必要性

学認トラストフレームワークを構成する上で機関を超えて受け渡されるアイデンティティ情報に関する検証状態を付加する必要性について、学認トラストフレームワークの現状および他のドメインにおけるトラストのあり方を踏まえ考察する。

（ア）学認に関連するエンティティと信頼の現状

ISO/IEC 24760-1:2019 の定義を基に関連するエンティティ/用語の整理を行う。

表 関連エンティティ/用語の整理(ISO/IEC 24760-1:2019)

エンティティ/用語	説明	学認の文脈におけるエンティティの例
IIA: Identity Information Authority	属性の真正性・正確性の保証を行う Entity related to a particular domain that can make provable statements on the validity and/or correctness of one or more attribute values in an identity.	大学や機関の学生課/人事部門
IIP/IdP: Identity Information Provider/ Identity Provider	アイデンティティ情報を提供する (IIA と同一のエンティティであることも多い) Entity that makes available identity information.	大学や機関の認証基盤
Credential	認証に使われるアイデンティティ Representation of identity for use in authentication.	学生 ID、パスワード等

Verifier	Verification（特定のエンティティに関連するアイデンティティ情報が正確であることを確立するためのプロセス）を実行するエンティティ Entity that performs verification.	大学や機関の認証基盤
Relying party/RP	特定のエンティティに関するアイデンティティ情報の Verification に依拠するエンティティ Entity that relies on the verification of identity information for a particular entity.	大学や機関の認証基盤/アプリケーション

関連するエンティティを学認関連機関(大学/機関等)に当てはめると下図の通りとなる。

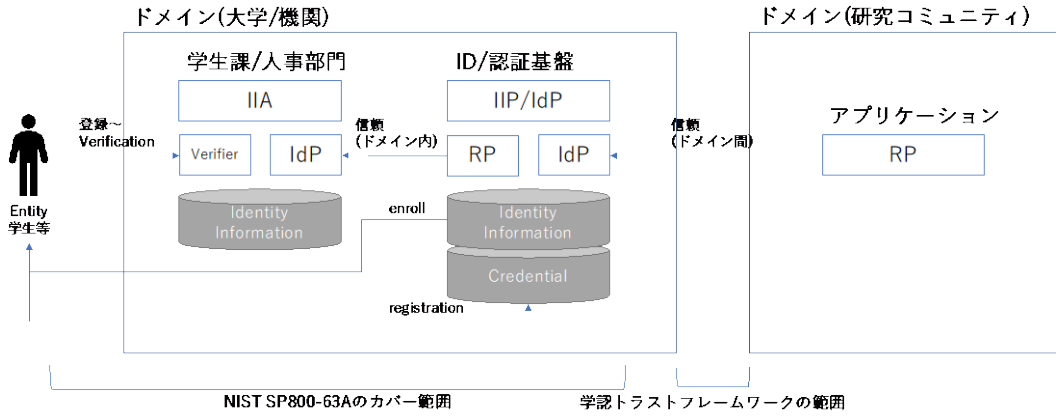

図 学認関連機関におけるエンティティの関係性

(イ)学認トラストフレームワークのスコープ

ドメインを超えた RP-IIP/IdP 間の信頼関係をスコープとする。

※ドメイン内において RP は IIA の行う Verification プロセスに対して暗黙の信頼を置くが、ドメインを超えて RP は IIP/IdP を信頼するためには、IIP/IdP が提供する Identity Information が IIA によるどのような Verification プロセスを経て登録されたのかを IIP/IdP に明示的に求める必要がある。

(ウ)信頼モデルの変化

従来のトラストフレームワークにおいてはトラストフレームワークに対する包括的な信頼を置くことにより、当該フレームワーク参画している(認定された)機関については

RP が自ら検証を行うことなく暗黙的に信頼[1]を置いてきた。

しかしながら、従来の学認においてはスケーラビリティを実現するために RP の個別の要求への対応は難しく、広く浅いレベルの要件の実現に留まってきた。その結果として各研究コミュニティは個別に IIA より情報を取得し、Verify を行う必要があった。

今後、研究コミュニティ等が学認参画機関のみならず民間企業との連携を行うためには従来のトラストフレームワークに対する暗黙的な信頼に加え、RP が IIP/IdP が提供する Identity Information の登録時に IIA にて実行した Verification プロセスに関する情報を取得し、自ら検証をすることを可能にする必要がある。

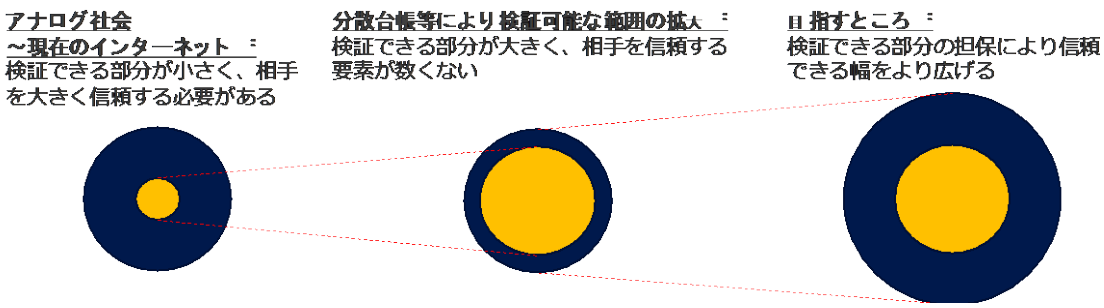

図 検証可能な範囲を広げることによる信頼の拡張(内閣官房 Trusted Web 推進協議会資料に対し加筆)

2. 従来の SAML における信頼性を表現するための属性表現

SAML Assertion において認証コンテキストを表現するための仕様として AuthnContextClassRef[2]が挙げられる。AuthnContextClassRef を利用すると SAML SP が SAML IdP へ指定する認証強度への対応を要求することができる。

例) SAML SP から最低限 Password を利用した認証を要求

```
<AuthnRequest …>
  <RequestedAuthnContext Comparison="minimum" …>
    <AuthnContextClassRef [中略]>
      urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </AuthnContextClassRef>
  </RequestedAuthnContext>
```

[1] 事実の確認をしない状態で、相手が期待した通りに振る舞うと信じる度合い（内閣官房/Trusted Web 推進協議会における定義より）

[2] http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

```
</AuthnRequest>
```

しかしながら、AuthnContextClassRef の利用においては以下の問題点がある。

- あくまで認証手段に関する情報を定義することしかできず、NIST SP800-63 で定義される Identity Proofing の強度レベル(SP800-63A)、認証の強度レベル(SP800-63B)を立体的に表現することができない
- 現状存在する SAML SP の実装系においては PasswordTransport を固定的に受け入れるものが多く、他の値を設定することで結果的に既存のシステムへの破壊的変更を与える可能性がある

そこで、本書では SAML Assertion のスキーマを拡張することにより ID 保証レベルおよび認証強度を表現するための属性表現を提案する。
ID 保証レベルに関しては本書 3 節の(ア)～(ウ)のうち 1 つもしくは複数を Assertion に含めて送出することを可能とする。これは先行事例である OpenID Connect for Identity Assurance[3]における Verified Claims/Authority Claims の表現方法と互換性を持たせることにより今後各機関の IdP が OpenID Connect への対応を行う場合にスムーズに置き換えができるようにする。また、検証済み属性と未検証属性が混在するユースケースが存在することも考慮し、検証済み属性には Prefix として”Verified_”を付加する。
また、認証強度に関しては本書 4 節に後述する(ア)～(イ)のうち 1 つもしくは複数を Assertion に含めて送出することを可能とする。
(SAML Assertion として表現するために Attribute Value は JSON をシリアライズしたものを利用する)

3. ID 保証に関する信頼性を表現するための属性表現の提案
   (ア) トラストフレームワークによる ID 保証レベルの表現
   特定のトラストフレームワークにより定義された信頼性レベルを表現する。
   なお、学認においては保証レベルを表現する属性として eduPersonAssurance[4]が利用されているため、本表現との関係性については議論する必要がある。
   例) 学認トラストフレームワークの IAL: 2 を表現する例(Value は表記上わかりやすくするため JSON 表現としているが実際は Stringify する)

```
<Attribute Name=”AssuranceDefinitions”>
  <AttributeValue>
  {
```

[3] https://openid.net/specs/openid-connect-4-identity-assurance-1_0-ID3.html

[4] https://meatwiki.nii.ac.jp/confluence/display/GakuNinShibInstall/eduPersonAssurance

```
    “trust_framework”: “nii_gakunin_ial_2022”,
    “assurance_level”: “2”
  }
  </AttributeValue>
</Attribute>
<Attribute Name=”Verified_displayName”>
  <AttributeValue>
    学認太郎
  </AttributeValue>
</Attribute>
```

(イ)Verification プロセスに関する属性情報の表現

Verifier が実行する Verification(Identity Proofing)の詳細を表現する。

- 適用した法令やルール
- 利用したエビデンス
- エビデンス検証(Validation)の手段
- エビデンスと提示エンティティ(Applicant)の同一性検証(Verification)の手段
- 各プロセスを実行した日付時刻
- 各プロセスを実行したエンティティ

例) 学認の基準に則り運転免許証を利用し対面で本人確認を実施したことを表現する例(Value は表記上わかりやすくするため JSON 表現としているが実際は Stringify する)

```
<Attribute Name=”AssuranceDefinitions”>
  <AttributeValue>
  {
    “trust_framework”: “nii_gakunin_ial_2022”,
    “assurance_level”: “2”,
    “evidence”: [
      {
        “type”: “document”,
        “validation_method”: {
          {
            “type”: “pipp”,
            “time”: “2022-02-22T00:00:00Z”,
            “entity”: “school office”
          }
```

```
        },
        “verification_method”: {
          {
            “type”: “pipp”,
            “time”: “2022-02-22T00:00:00Z”,
            “entity”: “school office”
          }
        },
        “document_details”: {
          “type”: “driving_permit”,
          “document_number”: “000000000000”,
          “date_of_issuance”: “2021-01-01”,
          “date_of_expiry”: “2025-12-31”,
          “issuer”: {
            “name”: “Minato Police Office”,
            “country”: “Japan”
          }
        }
      }
    ]
  }
  </AttributeValue>
</Attribute>
<Attribute Name=”Verified_displayName”>
  <AttributeValue>
    学認太郎
  </AttributeValue>
</Attribute>
```

（ウ）当該機関への所属に関する属性情報の表現

（イ）が本人確認について表現するのに対し、機関への所属していることを以下の属性として表現する。

- 所属機関名
- 所属機関の法人番号
- 当該エンティティの所属機関における役割
- 役割の期間

- 役割を付与したエンティティと付与方法

例）学認の基準に則り当該の個人が大学に所属していることを表現する例(Value は表記上わかりやすくするため JSON 表現としているが実際は Stringify する）

```
<Attribute Name=”AssuranceDefinitions”>
  <AttributeValue>
  {
    “trust_framework”: “nii_gakunin_ial_2022”,
    “assurance_level”: “2”,
    “authority”: [{
      “applies_to”: {
        “organization_name”: “Kyoto-University”,
        “organization_number”: “999999”
      },
      “permission”: [{
        “role”: “Student”,
        “validity”: [{
          “start”: “2021-04-01T00:00:00Z”
        }]
      }],
      “granted_by”: {
        “method”: “examination”,
        “granting_body”: “admission_office”,
        “reason”: “pass the exam”
      }
    }]
  }
  </AttributeValue>
</Attribute>
<Attribute Name=”Verified_displayName”>
  <AttributeValue>
    学認太郎
  </AttributeValue>
</Attribute>
```

信頼性を表現するための属性表現に関する詳細仕様(案)は以下の通りである。

表）属性表現一覧

カテゴリ	Claim 名	意味
フレームワーク	Trust_framework	適用する法令やルール(トラストフレームワーク)
信頼レベル	Assurance_level	Trust_framework における信頼レベル
本人確認時のエビデンス	Evidence	利用したエビデンスに関する情報
	Type	エビデンスのタイプ
	Validation_method	エビデンスの真正性検証に関する情報
	Type	真正性検証に利用した手法(例) pipp: 対面確認/physical in person proofing
	Time	検証を行った日付時刻
	Entity	検証を行ったエンティティ
	Verification_method	エビデンスと持参人の同一性検証に関する情報
	Type	同一性検証に利用した手法(例) pipp: 対面確認/physical in person proofing
	Time	検証を行った日付時刻
	Entity	検証を行ったエンティティ
	Document_details	エビデンス文書の詳細に関する情報
	Type	エビデンスのタイプ
	Document_number	エビデンスの文書番号
	Date_of_issuance	エビデンスの発行日
	Date_of_expiry	エビデンスの失効日
	Issuer	エビデンスの発行者にかんする情報
	Name	エビデンス発行者名
	Country	エビデンス発行国
機関への所属	Authority	権威に関する情報

	Applies_to	適用先に関する情報
	Organization_name	組織名
	Organization_number	組織番号(法人番号等)
	Permission	組織内の役割に関する情報
	Role	組織内における役割
	Validity	役割の期限に関する情報
	Start/End	開始日/終了日
	Granted_by	役割を付与した主体に感する情報
	Method	付与方法
	Granting_body	付与した主体
	reason	付与した理由

4. 認証強度に関する信頼性を表現するための属性表現の提案

(ア)トラストフレームワークによる認証強度の表現

特定のトラストフレームワークにより定義された信頼性レベルを表現する。

例) 学認トラストフレームワークの AAL: 2 を表現する例(Value は表記上わかりやすくするため JSON 表現としているが実際は Stringify する)

```
<Attribute Name=”AssuranceDefinitions”>
  <AttributeValue>
  {
    “trust_framework”: “nii_gakunin_aal_2022”,
    “assurance_level”: “2”
  }
  </AttributeValue>
</Attribute>
```

(イ)実際に利用した認証方式に関する情報の表現

IIP/IdP におけるエンティティ認証の方式の詳細を表現する。

- 利用した認証器(配列にすることで多要素認証についても表現)

例) パスワードに加えてハードウェアトークンによる認証を行った例(Value は表記上わかりやすくするため JSON 表現としているが実際は Stringify する)

```
<Attribute Name=”AssuranceDefinitions”>
  <AttributeValue>
  {
    “trust_framework”: “nii_gakunin_aal_2022”,
```

```
    “assurance_level”: “2”,
    “authenticators”: [
      {
        “type”: “password”,
        “level”: “2”,
        “enroll_date”: “2020-04-01T00:00:00Z”
      },
      {
        “type”: “hardware_token”,
        “level”: “2”,
        “enroll_date”: “2021-10-01T00:00:00Z”
      }
    ]
  }
  </AttributeValue>
</Attribute>
```

信頼性を表現するための属性表現に関する詳細仕様(案)は以下の通りである。

表）属性表現一覧

カテゴリ	Claim 名	意味
フレームワーク	Trust_framework	適用する法令やルール(トラストフレームワーク)
信頼レベル	Assurance_level	Trust_framework における信頼レベル
認証器	Authentication	認証器に関する情報
	Type	認証器のタイプ
	Level	認証器の強度
	Enroll_date	エンロールした日付時刻

5. 学認トラストフレームワークにおける各保証レベルと詳細属性表現の対応

学認トラストフレームワークにおける各保証レベルと 3〜4 節に示した属性表現の対応は下記の通りとする。

表）各保証レベルと属性表現の対応

カテゴリ	レベル	属性表現	値	
ID 保証レベル	1	Evidence	Type	学生証

				社員証 運転免許証 マイナンバーカード
			date	有効期限内
			Issuer	所属機関 発行機関
		Validation method	Type	リモート
			Time	３ヶ月以内
			Entity	認定された管理者
		Verification method	Type	リモート
			Time	３ヶ月以内
			Entity	認定された管理者
		Authority	Applies_to	認定された機関
			Permission	有効期限内
			Granted_by	N/A
	2	Evidence	Type	学生証 **社員証** 運転免許証 マイナンバーカード G ビズ ID
			date	有効期限内
			Issuer	所属機関 発行機関
		Validation method	Type	リモート
			Time	３ヶ月以内
			Entity	認定された管理者
		Verification method	Type	リモート
			Time	３ヶ月以内
			Entity	認定された管理者
		Authority	Applies_to	認定された機関
			Permission	有効期限内
			Granted_by	N/A
	3	Evidence	Type	学生証 **社員証** 運転免許証

				マイナンバーカード G ビズ ID
			date	有効期限内
			Issuer	所属機関 発行機関
		Validation method	Type	リモート
			Time	３ヶ月以内
			Entity	認定された管理者
		Verification method	Type	リモート
			Time	３ヶ月以内
			Entity	認定された管理者
		Authority	Applies_to	認定された機関
			Permission	有効期限内
			Granted_by	N/A
認証強度	1	Authenticator	Type	Password
			Level	1(複雑性要件なし)
			Enroll_date	N/A
			配列要素数	1
	2	Authenticator	Type	Password SW トークン
			Level	2(複雑性要件あり)
			Enroll_date	N/A
			配列要素数	2 以上
	3	Authenticator	Type	Password HW トークン
			Level	2(複雑性要件あり)
			Enroll_date	6 ヶ月以内
			配列要素数	2 以上

6. 実装モデルに関する提案

実際に各機関の IIP/IdP が本書で提案した属性表現を実装するのは困難なケースも存在すると思われるため、実装モデルとして以下の２方式を提案する。

1. IIP/IdP が直接属性表現を行う方式

各機関の IIP/IdP が本書で提案する保証レベルに関する属性表現を SAML Assertion として RP へ直接送出する。

2. Orthros 等の認証 Proxy が IIA と連携することで属性表現を代行する方式
   各機関の IIP/IdP と RP の間に認証 Proxy システムを配置することで保証レベルに関する属性表現の送出を認証 Proxy が代行する。この際、認証 Proxy と各機関の IIP/IdP の間には暗黙的な信頼関係が構築されていることが前提となる。

表) RP が詳細な属性表現を受け取り可能なケースにおける各方式の比較

	方式 1	方式 2
詳細属性の送出元	各機関の IIP/IdP	認証 Proxy
RP-IIP/IdP 間の信頼関係	直接的に信頼する (検証可能な信頼関係)	認証 Proxy と各機関の IIP/IdP 間の暗黙的な信頼関係を構築する

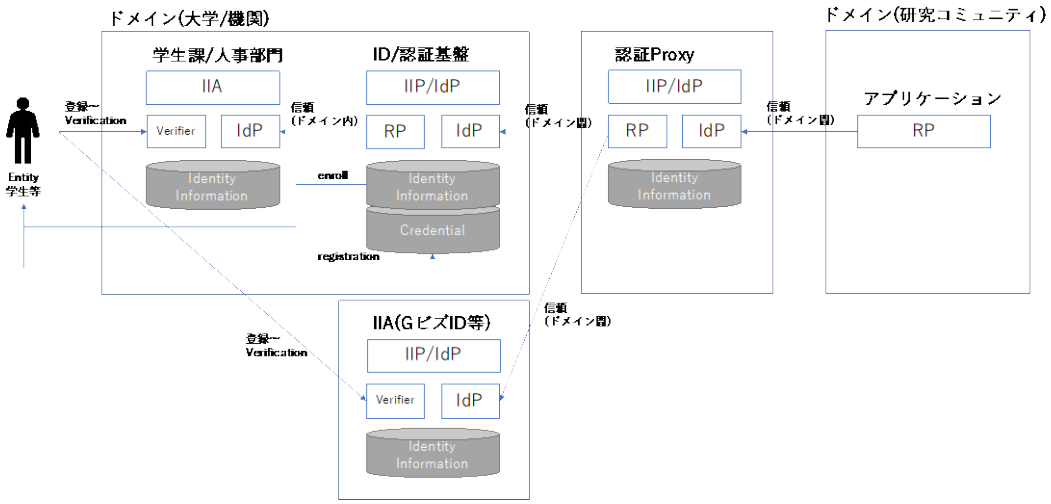

図) 実装モデルのイメージ

また、各機関の IIP/IdP 側の実装が困難なケースに加えて RP 側が詳細な属性表現を解釈し検証するための実装を行うのが困難なケースも存在すると思われる。その場合も上記の 2 つの実装方式により解決することが可能である。

1. IIP/IdP が直接属性表現を行う方式
   各 RP が各機関から送出される詳細な属性表現を解釈し、要求する保証レベルと合致することを検証する。
2. Orthros 等の認証 Proxy が IIA と連携することで属性表現を代行する方式
   認証 Proxy システムが各 IIP/IdP から取得もしくは別途 IIA から取得した情報を基に ID 保証レベル・認証強度の検証を代行し、RP へは通常の SAML Assertion のみを送出する。この際、各 RP と認証 Proxy の間には暗黙的な信頼関係が構築されていることが前提となる。

表) RP が詳細な属性表現を受け取り不可能なケースにおける各方式の比較

	方式 1	方式 2
詳細属性の解釈と検証	各 RP	認証 Proxy
RP-IIP/IdP 間の信頼関係	直接的に信頼する (検証可能な信頼関係)	RP と認証 Proxy の間に暗黙的な信頼関係を構築する