学認における属性交換フレームワーク

島岡 政基 †‡　　佐藤 周行¶

†セコム株式会社 IS 研究所
東京都三鷹市下連雀 8-10-16
セコム SC センター

‡総合研究大学院大学
複合科学研究科情報学専攻
東京都千代田区一ツ橋 2-1-2

¶東京大学
東京都文京区弥生 2-11-16

ID 連携にもとづくフェデレーションは，サービス提供者から認証情報を分離する．これが更に発展した形として，認可などに用いる属性情報もサービス提供者あるいは認証情報提供者から分離する，属性交換にもとづくフェデレーションが知られている．しかし属性情報は，扱う情報の多様性，また利用するアプリケーションから求められる要件などの点で認証情報と大きく異なり，保証レベルも含め新たなフレームワーク整備が喫緊の課題である．学認では，大学が属性情報提供者となって属性交換を行うフレームワーク整備を進めている．本稿では，属性交換フレームワークの概観と属性の保証レベルに関する検討状況について報告する．

The Attribute Exchange Framework in Gakunin

Masaki SHIMAOKA†‡　　Hiroyuki SATO¶

†SECOM Co., Ltd.　‡The Graduate University for Advanced Studies
¶The University of Tokyo

Abstract The ID federation separates authentication information from a service provider. The attribute exchange that separates an attributes used for the authorization from service provider or identity provider is known as the form that the ID federation developed into more. However, the attribute is very different from credentials used for the authentication at the points such as the diversity of information and the requirements from an application. Therefore, establishing of novel framework including the level of assurances is an urgent problem. Gakunin is developing the framework of attribute exchange with the universities. This paper describes the outlook of attribute exchange framework and the considerations of Levels of Attribute Assurance.

1　はじめに

SNS や e-コマースサイトなど多くのオンラインサービスの提供者 (以下，SP: Service Provider) が，ユーザに関する様々な情報を集め，サービスに利用しようとしている．収集する情報の中には，クレジットカード番号などの決済情報や，なりすましを防ぐための認証情報など，一定の確からしさを必要とするものもある．こうしたいわゆる属性情報の確からしさを各 SP が個別に検証することは非効率であり，既に検証済みの組織から当該情報を提供してもらう方が合理的な場合もある．そして，このような組織を横断する形での属性情報の交換を安全に実現するためには，その属性情報が一定の確からしさを有していることを保証する仕組みが必要となる．

具体的には，この属性情報の確からしさを示す尺度として属性情報の保証レベル (LoAA: Level of Attribute Assurance) を規定し，当該属性情報の提供組織である AP(Attribute Provider) が，その保証レベルに準拠する形で属性情報を

提供するためのフレームワーク，即ち属性交換フレームワークを整備することが必要である．国立情報学研究所の学術認証フェデレーション (学認) は，組織を横断する形での認証情報の提供を実現する，いわゆる ID 連携のためのトラストフレームワークを提供している．学認では，この学認のトラストフレームワークをベースとした属性交換フレームワークとして，OpenID ファウンデーション・ジャパンとともに「学生 ID のためのトラストフレームワーク (Student Identity Trust Framework: SITF) [1]」を実装中である．

本稿では，属性交換フレームワークの概観と属性の保証レベルの検討状況について報告する．2 節で，ID 連携とトラストフレームワークについて解説を行い，3 節で属性交換に応用する際に生じる課題について述べる．4 節では既存のトラストフレームワークを拡張する形で実現する属性交換フレームワークの提案と，その実践に必要となるドキュメントスィートについて述べる．5 節では，実際に学認のトラストフレームワークを拡張する形でドキュメントスィートの整備を進めている状況と検討内容について述べる．最後に 6 節で，同様の課題を解決しようとしている先行事例との比較考察を行う．

2　ID 連携とトラストフレームワーク

2.1　ID 連携と属性交換

ID 連携は，ユーザの ID 情報をサービス間で交換する仕組みであり，ID 情報を提供する Identity Provider (IdP)，IdP から ID 情報を受け取り活用する Service Provider(SP)，SP が提供するサービスを利用するユーザによって構成される．モデルとしては単純だが，実社会においては IdP としてユーザが所属する企業や日常的に利用するインターネットサービスプロバイダーや SNS など，SP としてネットショップや SaaS など，多様なプレイヤーで構成される，いわゆるマルチステークホルダーモデルとして捉えた方が自然である．

ここで ID 情報とは，狭義にはユーザを識別する認証結果を指すが，広義にはユーザの所属組織やメールアドレスなどの様々な属性情報を含み，SP におけるアクセス制御などに様々な応用が可能である．一般に ID 連携と言う場合は前者を指していることが多く，後者は区別のために属性交換と呼ばれる場合がある．本稿では前者を ID 連携，後者を属性交換と表記し，ID 連携・属性交換と表記した場合には広義の ID 連携を意味するものとする．

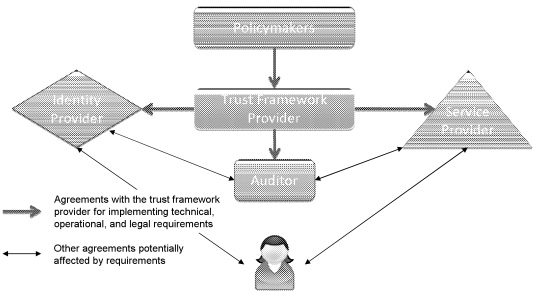

図 1: Open Identity Trust Framework Model

2.2　保証レベル

SP は，IdP から提供される認証結果が信頼できるものであることを前提にユーザにサービスを提供する．つまり認証結果には一定の信頼性が要求されることになる．これを表現するものとして 4 段階の保証レベル (Level of Assurance) が規定されており，表 1 の 2 列目に示す [2].

保証レベルの評価軸はトラストフレームワークによっても異なるが，例えば [2] では本人確認手続き，クレデンシャル管理，認証プロセスの 3 つの評価軸において，それぞれどの程度の安全性・信頼性を確保できているかによって評価される．

2.3　トラストフレームワーク

マルチステークホルダーモデルの ID 連携を適切に運用する仕組みとして，図 1 に示す Open Identity Trust Framework Model[3] と呼ばれるトラストフレームワークモデルが普及しており，国内では学認，海外では Open Identity Exchange (OIX) などが採用している．

ID 情報を交換するにあたっては，通信プロトコル，認証プロセス，クレデンシャルのデータフォーマットといった技術的要件だけでなく，クレデンシャルに一定の信頼性を確保するため

表 1: 4 段階の保証レベル

Level	Level of Assurance [2]	Credential Assurance Level [6]	Identity Assurance Level [6]
None	Not Assigned	**No confidence required** that the client maintained control over the entrusted credential and the credential has not been compromised	**No confidence required** that the client is or is not who they claim to be.
1 – Low	**Little or no confidence** in the claimed or asserted identity	**Little confidence required** that the client maintained control over the entrusted credential and the credential has not been compromised	**Little confidence required** that the client is or is not who they claim to be.
2 – Medium	**Some confidence** in the claimed or asserted identity	**Some confidence required** that the client maintained control over the entrusted credential and the credential has not been compromised	**Some confidence required** that the client is or is not who they claim to be.
3 – High	**High confidence** in the claimed or asserted identity	**High confidence required** that the client maintained control over the entrusted credential and the credential has not been compromised	**High confidence required** that the client is or is not who they claim to be.
4 – Very High	**Very high confidence** in the claimed or asserted identity	**Very high confidence required** that the client maintained control over the entrusted credential and the credential has not been compromised	**Very high confidence required** that the client is or is not who they claim to be.

に IdP が遵守すべき本人確認要件や，SP に提供された ID 情報の目的外利用を禁じるプライバシー保護要件などの運用要件も必要になってくる．そこで，IdP および SP が遵守すべき技術・運用要件などを規定する Trust Framework Provider (TFP) と呼ばれる第三者機関を設置する．TFP が規定する基準は，現実的には既存の制度や規格など外部の制約に従う形で決められることが多い．TFP が従う上位の制度や規格をポリシーメーカーと呼ぶ．また，TFP が規定する各種規準に IdP および SP が継続的に遵守していることを確認するために，査定人 (Assessor) による査定が行われる．査定規準や査定人の認定なども TFP が行う．

2.4 トラストフレームワークのドキュメントスイート

一般的なトラストフレームワークは，ポリシーメーカーが規程類を整備し，TFP や IdP，SP，ユーザはそれらの規程に準拠することでトラストフレームワークに参加し，その利便性を享受することができる．トラストフレームワークが整備する規程類は，概ね以下に分類することができる．

2.4.1 契約関連規程

本規程は IdP および SP の要件や責務，免責などについて規定している．後述の各種規程類の上位文書に位置づけられ，下位文書への準拠などが要件として求められる．

2.4.2 (認証の) 保証レベル規準

各トラストフレームワークは，2.2 節で述べたようにいくつかの評価軸にもとづいていくつかの保証レベルを規定している．各トラストフレームワークはそれぞれ独自の評価軸を持つ場合もあるが，将来的にトラストフレームワーク間での相互運用を想定して，表 1 のいずれかの保証レベルにマッピング可能な形で規定されていることが多いようである．IdP は，提供する認証結果についてどのレベルの信頼性を保証できるか本規準をもとに決定し，当該レベルにおける技術・運用規準 (後述) を満たす形でシステムを実装・運用することが求められる．

表 2: 技術・運用規準で規定する項目の例 [4]

一般的組織要件	運用要件
組織・サービスの成熟度	クレデンシャル運用環境
査定への通知・合意	クレデンシャル発行・更新・失効
情報セキュリティ管理	クレデンシャルのステータス管理
査定記録	クレデンシャルの検証・認証
運用基盤	
セキュアな通信	

2.4.3 技術・運用規準

本規準は，2.4.2 節で決定した保証レベルを保証するために遵守すべき各種技術・運用要件を規定する．IdP は，該当する保証レベルの要件に従ってシステムを実装・運用する必要がある．本規準は査定人から査定基準としても参照される．規定される内容はトラストフレームワークによって様々であるが，例えば [4] では，一般的な組織要件と運用要件に大別して以下の項目について規定している．

2.4.4 (認証) プロファイルセット

本仕様は，同じトラストフレームワークの IdP・SP 間における相互運用性確保のため，ID

連携において利用される認証方式(例えばSAML, OpenID など) における通信プロトコルやデータフォーマットなどについて規定する.

2.4.5 査定規準

本規準では，IdP・SP を査定するための査定要件や監視人の資格などについて規定する．具体的なシステム査定要件については 2.4.3 節で述べた技術・運用規準を参照する場合が多い.

3 属性交換への適用課題

[3] をはじめ既存のトラストフレームワークは ID 連携を前提として設計されたものが多く，より広義な属性交換を実現しようとした場合には，いくつかの課題を解決する必要がある．本節では，トラストフレームワークを属性交換に適用する場合の課題について示す.

3.1 Level of Attribute Assurance

ID 連携は，IdP から SP に認証結果を提供するための仕組みであり，その認証結果の信頼性を保証する概念として保証レベルが確立されている．一方属性交換では，SP に提供されるのは認証結果に限らない多様な属性情報である．

属性情報の信頼性を保証するには，属性情報にもやはり何らかの保証レベルが必要になると考えられるが，既存の保証レベルの評価軸は認証結果に特化している．例えば，2.2 節で示したクレデンシャル管理では，パスワードや私有鍵など認証に用いるクレデンシャルの強度が保証レベルの尺度になっており，こうした評価軸を属性情報に適用することは難しいと考えられる．属性情報の場合は，例えば所属部門や肩書きなどの属性情報はユーザの所属組織が付与するものであり，こうした属性情報を付与するいわゆる**信頼できる源泉** (Authoritative source) への照会などは，評価軸の一例として考えることができよう．こうした属性情報特有の評価軸を持つ保証レベルの必要性は，6 節で述べるように先行事例でも議論されており，本稿では Level of Attribute Assurance(LoAA) と呼ぶ.

3.2 Level of Protection

ID 連携において SP に提供される認証結果が認証目的以外への応用が難しいのに対して，属性交換において SP に提供される属性情報は，アクセス制御をはじめ提供サービスのパーソナライゼーションなど様々な応用が想定される．こうした応用は，属性情報の二次利用・再配布などをもたらす可能性もあり，また参照する属性情報によってはユーザのプライバシーに配慮する必要がある．IdP は，提供先の SP が属性情報を安全に管理することを前提に属性情報の提供を行うべきである．つまり SP の属性情報に関する安全管理には一定の信頼性が要求されるべきであり，そのためには例えば，収集した情報の保存期間や，ISMS など適切なセキュリティ管理基準への準拠性，プライバシーといった評価軸が必要になると考えられる．これを表現するものとして，Level of Protection(以下，LoP) という概念が広まりつつある [3][5] [1] .

3.3 属性プロファイルセット

属性交換では，AP・SP 間で多様な属性情報が流通することになる．この時，流通する属性情報がどのようなスキーマなのか，またそれぞれの LoAA はどうなのか，ということは AP と属性情報の組み合わせ問題になってしまい，非常に使い勝手の悪いものになってしまう．そこで，属性情報の種類や構造を定義したスキーマと各属性情報の LoAA などを何らかの粒度でまとめた属性プロファイルセットを定義しておくことで，属性交換を使いやすいものにすることができると考えられる.

4 属性交換フレームワークの設計

本節では，3 節で示した課題を解決可能な形で既存のトラストフレームワークを拡張する属性交換フレームワークを提案する．図 2 にその概要を示す.

属性交換フレームワークは，プレイヤーとしては新たに AP が増えただけだが，ドキュメン

[1] 明確に Level of Protection という言葉は用いていないが，SP に対して属性情報の収集に対する規制やプライバシーへの配慮を求める動向は下記にも確認することができる. https://refeds.terena.org/index.php/Introduction_to_Code_of_Conduct

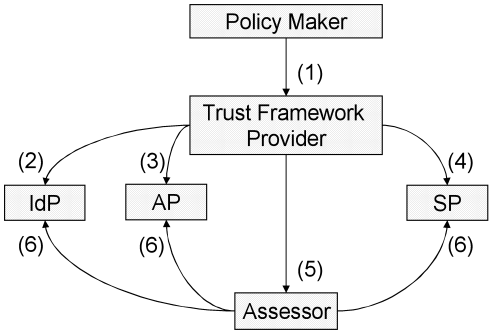

図 2: 属性交換フレームワークの概要

	IdP	AP	SP
(a) 契約関連規準			
(b) 信頼性規準	LoA	LoAA	LoP
(c) 技術・運用規準			
(d) プロファイルセット	認証プロファイルセット	属性プロファイルセット	
(e) 監査規準			

図 3: 属性交換フレームワークのドキュメントスィート

トスィートは図 3 のように追加および改訂されることになる．網掛け部分は一例としての既存トラストフレームワークである学認のドキュメントスィートとの差分，つまり新たに記述する必要がある部分となる．これについては 5 節で後述する．各ドキュメントは属性交換フレームワークにおいての利用については図 2 のように適用される．

4.1 ドキュメントスィートの利用イメージ

図 2 の番号に沿って各プレイヤー間の関係を以下に示す．各項目末尾の記号は，準拠すべき図 3 の文書を意味する．

(1) **ドキュメントスィートの策定**
TFP は，国際標準など [1] ポリシーメーカーから与えられた条件の下で図 2 に示した一連のドキュメントスィートを策定する．

(2) **LoA および認証プロファイルの選択 (a, b-LoA, c, d)**
IdP は，規定された LoA において適切なレベルを選択する．また，認証プロファイルセットが複数提供されている場合は，利用する任意のプロファイルセットを選択することが可能である．IdP は，選択した LoA のレベルに応じた技術・運用規準の要件と，選択したプロファイルセットの要件をそれぞれ満たす形でシステムを実装・運用することが求められる．

(3) **LoAA および属性プロファイルの選択 (a, b-LoAA, c, d)**
AP は，規定された LoAA において適切なレベルを選択する．また，属性プロファイルセットが複数提供されている場合は，利用可能なプロファイルセットを選択することが可能である．AP は，選択した LoAA のレベルに応じた技術・運用規準の要件と，選択したプロファイルセットの要件をそれぞれ満たす形でシステムを実装・運用することが求められる．

(4) **LoP の選択および認証・属性プロファイルの選択 (a, b-LoP, c, d)**
SP は，規定された LoP において適切なレベルを選択する．またサービスに必要な属性情報を含むプロファイルセットと，対応可能な認証プロファイルセットを選択する．SP は，選択した LoP のレベルに応じた技術・運用規準の要件と，選択した各プロファイルセットの要件をそれぞれ満たす形でシステムを実装・運用することが求められる．

(5) **査定人の認定 (a, e)**
TFP は，査定規準で規定した査定資格を持つ査定人を任命する．査定人は，査定規準にもとづいて定期的に IdP，AP，SP を査定する．

(6) **IdP/AP/SP の準拠性査定 (c, e)**
査定人は，IdP については所定の LoA，AP については所定の LoAA，SP については所定の LoP をそれぞれ継続的に遵守していることを確認するために，定期的な査定を行う．査定は，技術・運用規準を中心に，契約関連規程や各 IdP/AP/SP が対応するプロファイルセットについても要件を満たしていることを査定する．

4.2 保証レベルの拡張

3節で述べた通り，属性交換においては従来のLoAに加えてLoAAおよびLoPが必要となる．APが提供する属性情報の信頼性について，SPによる測定可能な指標としてのLoAAが，またSPが収集した認証結果・属性情報の安全性について，IdP/AP/ユーザによる測定可能な指標としてのLoPがそれぞれ整備される必要がある．特にLoAAに関しては，属性情報がユーザに紐づいた情報である以上は認証結果との紐付けて考えることが不可欠である．そのため，LoAとLoAAの尺度は対比できる形で規定しておくことが好ましいと考えられる．6.1節で述べるカナダ政府の事例[6]においても表1の右2列に示したように，Identity Assurance Level(LoAAに相当)はCredential Assurance Level(LoAに相当)と同じ4段階で規定されており，またその尺度は抽象的には同一である．

4.3 属性プロファイルセットの定義

属性交換においてはAPは多様な属性情報を提供できるべきであるが，提供する種類がAP毎に異なっていたり，また属性毎にLoAAが異なるケースなどに柔軟に対応しようとすれば，これを受け取るSP側の対応コストは肥大化してしまう．そこで例えば，少なくともどのAPからも等しく提供可能な属性のセットや各属性値の定義を規定するなどして，冗長な柔軟性を排除していくつかのプロファイルを定義して利便性を確保することが，属性交換においては有効と考える．こうした属性プロファイルセットは，トラストフレームワークの範囲を超えて，即ち汎用的な仕様を策定しようとすると発散しがちだが，トラストフレームワーク毎に策定する限りは有効な仕様が策定できると考えている．何故ならば，トラストフレームワークに参加するステークホルダーは概ね共通の目的や動機を持ってトラストフレームワークに参加しているはずであり，従ってその目的や動機に沿った属性プロファイルを策定可能だからである．

4.4 技術・運用規準

APおよびSPのためにLoAAやLoP，属性プロファイルセットを規定する以上は，技術・運用規準もこれに対応する必要がある．特にLoPは，収集した情報の保存期間やセキュリティ管理基準への適合など技術基準への影響も大きくなる可能性がある．

5 学認への実装状況

前節の属性交換フレームワークを実現するため，著者らはSITF[1]においてその一部を実装中である．本節では，実装の一部を紹介する．

5.1 前提

SITFは，例えばアカデミックライセンスに対応したコンテンツプロバイダや就職活動支援サイトのような学生資格を必要とするSPを対象に，学生資格など大学が保有する属性情報を提供するトラストフレームワークである．IdPとして，学生が日常的に利用している民間の認証サービス事業者を，APとして学認に対応した学内認証基盤を想定している．既存の学認の規程類は，大学の認証基盤はIdPとして振舞うことを前提とした記述となっていること，またそのままではAPへの適用が困難であったことから，属性交換フレームワークとそれにもとづく形での規程類へ再整備を検討することになった．属性交換フレームワークで整備すべき規程類は図3に示した通りだが，今回はこのうち1) APに関する契約規準，2) LoAA，3)，属性プロファイルセットの3種類について策定を行った．

5.2 属性プロファイルセットの定義

学認が扱う属性情報は[9]に規定されているものの，実際の提供の可否はAPである各大学の判断に任されている．つまり，SPにとっては必要な属性情報を収集可能なAPかどうか個別に確認する必要がある．そこでSITFでは，SPの参入障壁を下げるために，SPに最低限提供すべき属性情報の種類と，各属性に格納される属性値の定義について以下の通り規定した．SITFにおけるSPは学生向けサービス提供者であることから，学生であることを判別するためのいわゆる学生フラグとしてのeduPersonAffiliationと，ユーザのプライバシーを侵害しない程度の最低限の情報としてorganizationNameを提供することとした．なお，SPが属性情報を取得す

るにあたっては，最終的にユーザの同意が必要であるため，ユーザが提供を拒否した場合に本プロファイルセットで規定した属性情報と言えども取得できない可能性はある．また，下記以外の属性を提供することも可能だが，その保証レベルについては本規程の対象外としている．

- **organizationName(機関名)**
  機関が学認参加時に機関名として届け出た文字列とする．
- **eduPersonAffiliation(職種)** [2]
  student の値を持つユーザは「当該機関に在籍し，その機関の学務の管理対象になっているもの」を基本とする[3]．

5.3 LoAA の定義

LoAA は，[2] や [7] との相互運用性を確保するために，その尺度については表 1 との整合を保ちつつ図 4 のように定義した．レベルに関しては，レベル 3 および 4 は一般的なサービスでの利用頻度が低いと判断し，今回は検討外とした．LoAA の評価軸は 1) 属性情報の正確性，2) 属性情報の鮮度, 3) 認証クレデンシャルとの紐付けの 3 種類である．

5.3.1 属性情報の正確性

属性情報の正確性を測る時に，もっとも確実なのはその属性情報の付与元，いわゆる信頼できる源泉から属性情報の提供を受けることであろう．例えば役職や部署名であればユーザの所属組織，生年月日や住所は (実態はともかくとして) 行政機関が信頼できる源泉と言える[4]．SITF で扱う前節の 2 種類の属性は，いずれも信頼できる源泉から提供されるものであり，本規程ではこれをレベル 2 とした．

一方，信頼できる源泉でなくとも，例えば入学時に住民票によって本人確認を済ませている大学や，自己申告の住所に本人確認郵便を送付した実績を持つ事業者など，何らかの方法で属性情報を確認した第三者から提供される場合にも一定の正確性が与えられるべきだろう．このような，第三者によるいわゆる確認済属性 (verified attribute) については，確認方法によって正確性は異なること，またその確認方法は属性によっても異なることなどについて，引き続き議論していく必要があると認識している．

5.3.2 属性情報の鮮度

信頼できる源泉から提供された属性情報であっても，必ずしも最新の実態を反映しているとは限らない．例えば，大学が学生の身分確認を年度毎に行っていれば，年度内の身分変更は AP には適切に伝わらない可能性がある．年度内の身分変更があった場合は速やかにシステムに反映するのが理想ではあるが，属性情報に最終確認日を追記すれば，AP 側の属性情報のライフサイクル管理に依存しない形で属性情報の鮮度を測ることができる．

5.3.3 認証情報との紐づけ

LoA と LoAA では評価軸が異なるものの，両者を対比しやすいよう尺度を揃えているのは表 1 に示した通りである．評価軸が異質である以上は，尺度を揃えたからといって単純に LoA 1 と LoAA 1 とをマッピングできるわけではない．実際に，次節で示す先行研究においても，認証情報とのマッピングを明確に示したものは見当たらない．そこで著者らは，本項目に関しては原理的なアプローチではなく実績的なアプローチを取ることにした．即ち，LoA と LoAA を等価に扱うようにしてしまうことで LoAA を単純化し，使いやすいものになることを狙いとした．属性情報は多様であるが，その分複雑性も増し，分かりやすさ，使い勝手もまた難しくなる．保証レベルが多様なセキュリティポリシを単純化したように，また属性プロファイルセットも柔軟性を排除して利便性を確保する方針としたように，認証情報との紐付けもまたできるかぎり単純化してマッピングさせることで，LoAA を複雑化させずに利便性を確保し，広く使われるようになるとが期待できると考えた．

[2] student 以外の値を持つ場合は提供しなくてもよいものとする．

[3] ただし，その対象は厳密には各機関によって異なるため，各機関は student の値を付与する規準について SP に明示しなければならない．SP は，厳密な定義が機関によって異なることに理解を示し，必要に応じて各機関の規程を確認し，了承の上で利用すること．

[4] 趣味など一部の属性情報はユーザ本人が信頼できる源泉となり得る．

Level	正確度	鮮度	認証情報との紐づけ
1	ユーザ自身による自己申告	値の最終確認日を明記すること	LoA 1以上のクレデンシャルを用いること
2	AP自身が信頼できる源泉であること または 信頼できる源泉から発行されたものであることをAP自身が確認すること	上記に加えて，必要に応じて有効期間を設定できる	LoA 2以上のクレデンシャルを用いること

図 4: 学認における LoAA の定義

6 先行事例との比較

属性交換のためのフレームワーク整備を進めている先行事例としてカナダ政府および米国政府がある．本節では、これらの事例について簡単に紹介した上で，本研究との差違について考察する．

6.1 カナダ政府

カナダ政府では，2010 年に Credential Assurance および Identity Assurance という二種類の保証カテゴリと 4 段階のレベルを定義した [6]．前者はいわゆる ID 連携に用いる認証クレデンシャルに対する信頼性即ち LoA であり，後者は属性交換で扱う属性情報に対する信頼性即ち LoAA を扱うものである．カナダ政府では，2013 年 2 月にこの [6] に準拠する形で両 Assurance に関する標準 [7] を策定したところであり，実運用はこれからと思われる．カナダ政府のこの取り組みの特徴として，LoA と LoAA を明確に分けつつ同じ 4 段階で対比しやすい形で定義している点は非常に先進的である．しかしながら，現状では 3.3 節で述べた属性プロファイルセットに関する規程が存在しないこと，また 3.2 節で示した LoP に関して議論された形跡がないことなど未解決の課題は多い．

6.2 米国政府

米国政府では 2009 年からトラストフレームワークにもとづいて，行政サービスに対して民間 IdP を活用した ID 連携を推進しているが，2011 年から Backend Attribute Exchange (BAE)[8] という属性交換の導入を進めている．AP と SP が直接属性交換すると，交換する属性情報の種類によってはプライバシーの漏洩が生じる場合がある．そこで BAE では，Attribute Service といういわゆるブローカーを介した交換方式について策定している．これは LoP とは異なるアプローチではあるものの，SP 側に属性情報のコントロールを完全には委ねない，という点で属性情報の不当な利用を防止する役割が期待される．

しかしながら，属性交換を推進する一方で LoAA の定義ができていないこと，属性プロファイルセットについてもほとんど議論された形跡がないことなど未解決の課題は多い．

7 おわりに

ID 連携をベースとしたトラストフレームワークを拡張して属性交換に対応させるための属性交換フレームワークと，そこで整備すべきドキュメントスィートについて提案した．さらに，学認の SITF に適用させるために，ドキュメントスィートの一部を規定した．今後は，規程の有用性や妥当性評価，残るドキュメントスィートの規定を進めていく予定である．本研究は，学認および OpenID ファウンデーション・ジャパンの共同研究によるものである．

参考文献

[1] “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”
http://www.nii.ac.jp/news/2011/0305/

[2] “ITU-T Recommendation X.1254 (2012)—ISO/IEC 29115:2013, Entity authentication assurance framework”, September, 2012.

[3] May Rundle, et al.,“The Open Identity Trust Framework (OITF) Model”, March 2010.

[4] Richard G. Wilsher, “Identity Assurance Framework: Service Assessment Criteria”, Version 3.0, Kantara Initiative, October 2010.

[5] “Telecom Data Trust Verification Framework”, Telecom Data Trust Framework Working Group, Open Identity Exchange, March 2013.

[6] “Pan-Canadian Assurance Model”, Treasury Board of Canada Secretariat, March 2010.

[7] “Standard on Identity and Credential Assurance”, Treasury Board of Canada Secretariat, February 2013.

[8] “Backend Attribute Exchange (BAE) v2.0 Overview”, Identity, Credential and Access Management (ICAM) Subcommittee, Federal CIO Council, January 2012.

[9] “学術認証フェデレーション システム運用基準 (Ver.1.2)”, 学術認証フェデレーション, 国立情報学研究所, 2011 年 8 月.