教育クラウドプラットフォーム
参考技術仕様

平成29年６月30日

総務省

目次

1. はじめに

1.1 本仕様の概要

教育クラウドプラットフォーム参考技術仕様（以下「本仕様」という。）は、総務省「先導的教育システム実証事業※」における実証成果を踏まえ、クラウド環境で実装された複数の教材コンテンツ（提供事業者が異なるものを含む。）をシングルサインオンで利用することができ、異なるプラットフォームとの間でも、相互にデータ連携を行うことができる教育クラウドプラットフォームに求められる技術要件について取りまとめている。

なお、本仕様で示す各要件は、教育クラウドプラットフォームを実装する際の技術的仕様の一例を示したものであり、ここで示す仕様以外により教育クラウドプラットフォーム等を実装することを妨げるものではない。

本仕様においては、多様な主体による参入を可能とすることにより、健全な競争環境の実現や事業継続性の確保を実現するため、教育クラウドプラットフォームを構成する要素をモジュール化した上で、プラットフォーム相互間での連携も可能とするアーキテクチャを採用している点において、その特色がある。

本仕様は、今後、新たに教育クラウドプラットフォームを提供する事業者、システム更改をする事業者にとって要求定義から要件定義に係るプロセスに関し、参考となるものとなることを想定しており、その内容については、今後の技術革新等を踏まえ改訂を行う。

※　平成 26 年度から平成 28 年度まで文部科学省「先導的な教育体制構築事業」と連携して事業を実施した。

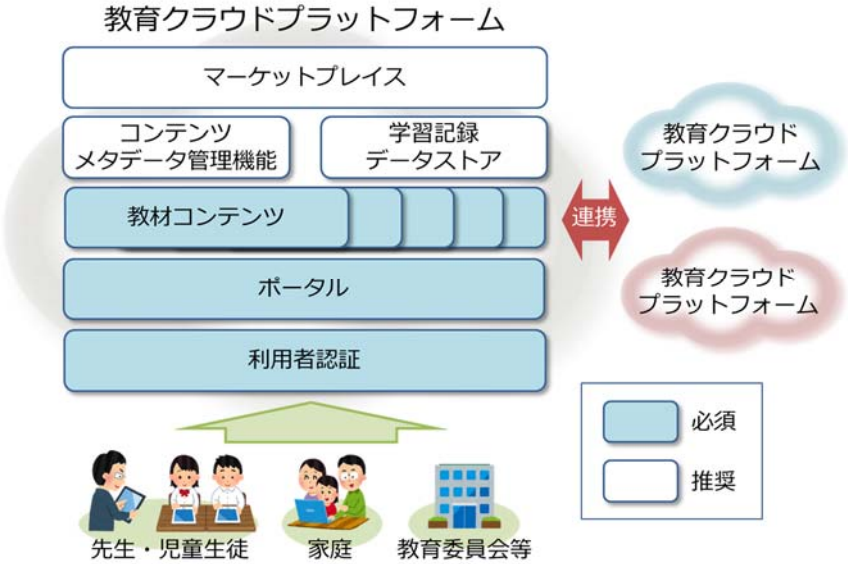

図 1. 教育クラウドプラットフォームの概要

1.2 本仕様の構成

本仕様は、以下の内容によって構成される。

- **構成要件**

  教育クラウドプラットフォームを構成する構成要素（必須・推奨の別がある。）と各構成要素間の関係について規定したもの。

- **共通要件（構成要素共通）**

  教育クラウドプラットフォーム全体に対して、又は各構成要素に共通して、適用される要件。このうち、セキュリティ要件と利用環境要件については、独立の項目として規定している。

  - **セキュリティ要件**

    教育クラウドプラットフォームが確保すべきセキュリティに関する要件。

  - **利用環境要件**

    教育クラウドプラットフォームの提供に当たり前提とすべき利用環境の要件。

- **システム要件（構成要素別）**

  - **認証基盤（必須要素）**

    教育クラウドプラットフォームへのアクセスを確認し、予め設定された権限に応じて教育クラウドプラットフォームの各機能に対する利用認可を行うシステム。アクセス制限を行うことによりセキュリティを向上させるほか、個別の学習者や利用者単位で学習記録データや利用履歴の記録・管理を行うことを可能にする。

  - **教材コンテンツ（必須要素）**

    学習者や利用者が授業・学習を行うための多種多様な教材やツール等のシステム。一斉授業、個別学習、協働学習など、多様な授業・学習時に利用される。

  - **ポータル（必須要素）**

    学習者や利用者に対して利用可能な教材コンテンツへのアクセス手段や必要な情報を一元的に提供するシステム。機能や情報を集約することで、利用者の利便を向上させる。

  - **マーケットプレイス（推奨要素）**

    利用者に対して、教材コンテンツの利用申請・購入のために必要な機能（教材コンテンツに関する情報の表示を含む。）を、教材コンテンツ提供事業者に対して、教材コンテンツを教育クラウドプラットフォームに登録するために必要な機能を提供するシステム。

  - **コンテンツメタデータ管理（推奨要素）**

    教材コンテンツが有する情報資源の属性（名称、提供者、対象学年、教科等）

を統合的に管理するシステム。複数の教材コンテンツを横断して検索したり、複数の教材コンテンツに係る学習記録データを統合して活用・分析したりすることなどを容易にする。

- **学習記録データストア（推奨要素）**
  教材コンテンツを用いた学習記録データを統合的に記録・管理するためのシステム。統合的な記録・管理が実現することで、複数の教材コンテンツを横断した学習状況の表示や分析などを行うことを容易にする。

1.3 要求水準等

本仕様では要件の要求水準を次の記述方針に従い表示する。

- 【必須】：要件が対応されなければならないことを示す。
- 【推奨】：要件の対応は必須ではないが、対応が推奨されることを示す。
- 【任意】：要件の対応は必須ではなく、必要に応じて判断するべきことを示す。

また、各要件に対して具体的な要件規定の例を示す場合には【規定例】と表示し、ある規定例に特定の前提条件がある場合には【規定例：（前提条件の内容）】と表示する。

その他の補足的な説明がある場合には【注記】と表示した上で記述する。

1.4 用語

用語	説明
アイデンティティプロバイダ（IdP）	教育クラウドプラットフォームへのアクセス者への認証を行い、アイデンティティ情報の提供を行うもの。
アクセシビリティ	情報、サービス、ソフトウェア等が、どの程度広範な人に利用可能であるかを表す概念。特に障がい等のハンディを持つ人にとっての使いやすさの度合いを表す。（平成 28 年版情報通信白書）
アクセス制御	教育クラウドプラットフォームへのアクセスに対し利用者を識別し、規定された権限に応じ許可されたシステムにアクセスできるようにする仕組み。認証と利用認可を組み合わせたもの。
学習記録データ	児童生徒の学習の過程や成果等が示されているものとして、「学習履歴」「学習記録」「学習成果物」をまとめて総称したもの。 （文部科学省「学びのイノベーション事業」実証研究報告書）
学習履歴	プログラムへの操作やプログラムの動作を記録したもの。 （文部科学省「学びのイノベーション事業」実証研究報告書）

用語	説明
学習記録	学習活動によって生まれる記録であり、例えば演習問題の解答や得点、アノテーション等。 （文部科学省「学びのイノベーション事業」実証研究報告書）
学習成果物	学習記録の一つであり、観察・実験の記録、調べ学習のまとめ等、特に、独立しても意味を持つようなもの。 （文部科学省「学びのイノベーション事業」実証研究報告書）
学習者	児童生徒等の教育クラウドプラットフォームを利用して学習を行う者。
学校等	学校教育法（昭和２２年法律第２６号）に規定する小学校、中学校、義務教育学校、高等学校、中等教育学校及び特別支援学校のほか、在外教育施設、フリースクール、公営塾等の教育施設を含む。
コンテンツメタデータ	コンテンツに関連する情報のこと。コンテンツの検索や管理などで用いられる。
シングルサインオン（SSO）	認証を必要とする複数のシステムを使用する際、一度のログイン操作によって、許可されているすべてのシステムにログインできるようにするもの。
シングルログアウト（SLO）	認証を必要とする複数のシステムからログアウトをする際、一度のログアウト操作によって、許可されているすべてのシステムからログアウトできるようにするもの。
先導的教育システム実証事業	平成 26 年度から平成 28 年度にかけて総務省が行った実証事業。時間や場所、端末や OS を選ばず、最先端のデジタル教材等を利用でき、かつ低コストで導入・運用可能な「教育クラウドプラットフォーム」についての実証を行った。文部科学省「先導的な教育体制構築事業」と連携して実施した。
先導的な教育体制構築事業	平成 26 年度から平成 28 年度にかけて文部科学省が行った事業。最先端の情報通信技術を活用し、異なる学校間及び学校と家庭との連携を深め、新しい学びを推進するための指導方法の開発、教材・指導実践事例等の共有等の研究を行った。総務省「先導的教育システム実証事業」と連携し実施した。
認証	教育クラウドプラットフォームへのアクセスを確認し、利用者を識別するもの。
トラストフレームワーク	一定のポリシーに準拠していることについて認定・監査を行うことにより、プライバシー・セキュリティに関する信頼性を担保し、ＩＤ連携や自由なデータ移転を促進・協力しようという、ＩＤ発行・認証者やサービス提供者によって作られた枠組みのこと。

用語	説明
	（総務省「パーソナルデータの利用・流通に関する研究会」報告書）
パーソナルデータ	個人情報に限定されない、個人の行動・状態に関するデータ。
パブリッククラウド	民間事業者が保有・運営するサーバにより提供されるクラウドサービスであって、インターネット経由で提供・利用されるもの。
利用者	教育クラウドプラットフォームを利用し、授業・学習を実施するもの及びその環境を管理するもの。授業・学習で利用する学習者や教員に加え、教育委員会や学校管理者、保護者などが想定される。
利用認可	認証によって確認された利用者に対し、規定された権限に応じ、許可されたシステムにアクセスできるようにすること。
Caliper Analytics v1 (Caliper)	学習記録データのプロトコルとデータ形式に関する国際標準仕様群。教育 ICT に関する国際標準化団体 IMS Global により 2015 年 10 月に公開された。
CSV	データ形式に関する国際標準仕様（RFC 4180）
Experience API 1.0.3 (xAPI)	学習記録データのプロトコルとデータ形式に関する国際標準仕様群。米国国防総省内組織 ADL により 1.0 版が 2013 年 3 月に公開された。
HTML5	2014 年 10 月に W3C 勧告となったウェブコンテンツのデータ形式に関する国際標準仕様 （W3C HTML5 A vocabulary and associated APIs for HTML and XHTML ）
HTTPS	暗号通信のプロトコルに関する国際標準仕様（RFC 2818）
LOM	教育に関するコンテンツのためのメタデータ仕様 （IEEE 1484.12.1 – 2002 Standard for Learning Object Metadata ）
OpenID Connect 1.0 (OIDC)	SSO 認証のためのプロトコルとデータ形式に関する国際標準仕様群。米国 OpenID 財団により 2014 年 2 月から公開された。
RDF	情報共有・再利用のための識別子に URI を用いたグラフ構造によるデータ形式に関する国際標準仕様群。インターネット技術に関する国際標準化団体 W3C により 1999 年 2 月から公開された。
SAML 2.0 (SAML)	SSO 認証や第三者へのリソース利用認可のためのプロトコルとデータ形式に関する国際標準仕様群。インターネット技術に関する国際標準化団体 OASIS により 2015 年 3 月から公開された。
SCIM 2.0	認証用 ID 管理のプロトコルとデータ形式に関する国際標準仕様（RFC7642, RFC7643, RFC7644）

用語	説明
SP/RP	認証基盤により提供される認証情報を信頼し、利用者にサービスを提供するもの。OIDC においては、「Relying Party（RP）」と、SAML においては「Service Provider（SP）」と定義されている。教育クラウドプラットフォームにおいては、教材コンテンツ、ポータル、マーケットプレイス及び学習記録データストアが該当する。
TLS 1.2	HTTPS に用いる暗号通信のプロトコルに関する国際標準仕様（RFC 5246）
W3C	World Wide Web Consortium（ワールド・ワイド・ウェブ・コンソーシアム）の略称。World Wide Web で使用される各種技術の標準化を推進する為に設立された非営利の標準化団体。

2. 構成要件

教育クラウドプラットフォームの構成に係る要件を以下に示す。

2.1 教育クラウドプラットフォームの構成要素

本仕様においては、教育クラウドプラットフォームの構成要素について「必須構成要素」と「推奨構成要素」に分類して規定している。

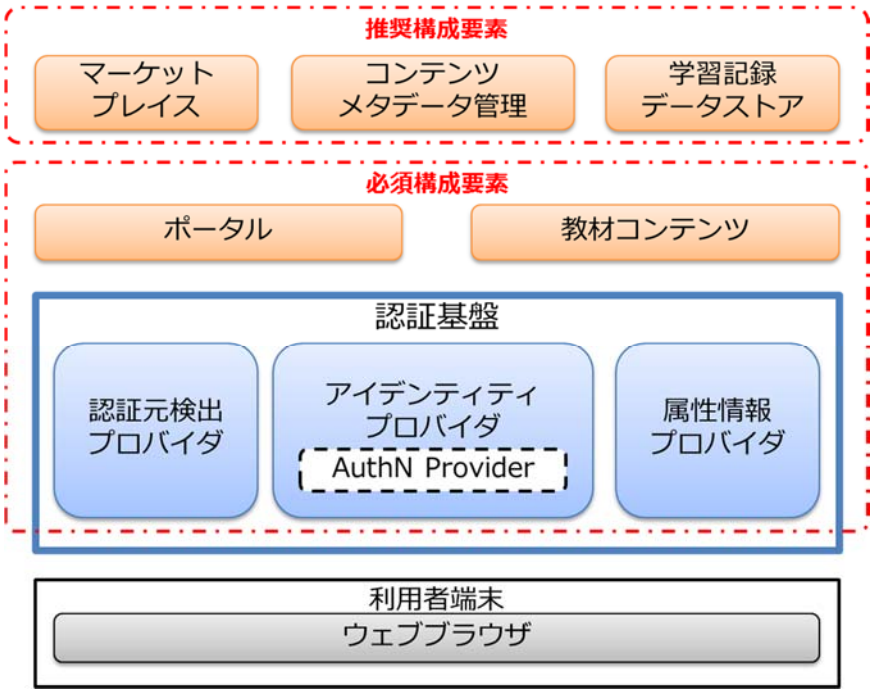

図 2　構成要素の分類

2.2 必須構成要素

必須構成要素は、本仕様で規定する教育クラウドプラットフォームに必ず実装されるべき構成要素である。教育クラウドプラットフォームの必須構成要素について以下に示す。

- **認証基盤**
  - 教育クラウドプラットフォーム外の認証基盤（AuthN Provider）との認証連携が可能なアイデンティティプロバイダ（IdP）を 1 つ以上有すること。
  - 属性情報プロバイダ（AtrP）を 1 つ以上有すること。
  - シングルサインオンの対象範囲内に 2 つ以上の IdP が存在する場合、シングルサインオンの対象範囲内の複数の認証基盤が共用する構成要素として、認証元検出プロバイダを 1 つ以上有すること。

- **教材コンテンツ**
  - 教材コンテンツを 2 つ以上有すること。

- **ポータル**
  - ポータルを 1 つ以上有すること。

  【注記】
  1 つの教育クラウドプラットフォームにおいて、学校や利用者などのニーズ（コミュニケーション機能、学習記録データ表示等）に応じて、ポータルが 2 つ以上実装・提供されることがあり得ると想定している。

2.3 推奨構成要素

推奨構成要素は、本仕様で規定する教育クラウドプラットフォームに必ず実装されるべき構成要素ではないものの、提供されることが望ましい機能を有する構成要素である。教育クラウドプラットフォームの任意構成要素について以下に示す。

- **マーケットプレイス**
  - マーケットプレイスを有することが望ましい。

- **コンテンツメタデータ管理**
  - コンテンツメタデータ管理を有することが望ましい。

- **学習記録データストア**
  - 学習記録データストアを有することが望ましい。

2.4　利用者と構成要素の関連

学習者や教員等の主な利用者と構成要素の関連をユースケース図で以下に示す。構成要素は、認証基盤と利用者から直接利用される直接利用構成要素と基本的に他構成要素から間接利用される間接利用構成要素に分類される。コンテンツメタデータ管理を除く構成要素は、認証基盤と連携してシングルサインオン（SSO）を実現する。

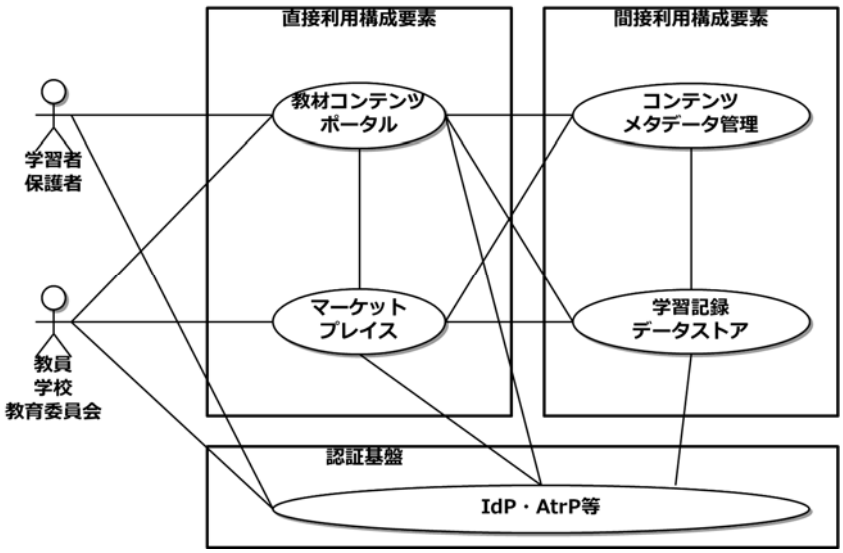

図 2　利用者と構成要素の関連

2.5　構成要素間の関連

構成要素間の関連を以下の図 3 に示す。認証基盤については、認証基盤内の構成要素の関連を併せて示す。

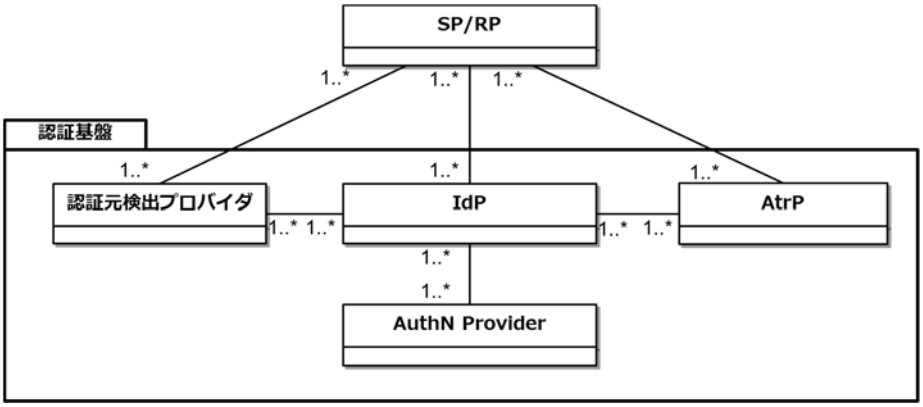

図 3. 認証基盤の構成要素の関連

3. 共通要件

教育クラウドプラットフォームの各システムに共通する要件を以下に示す。

3.1 共通要件

1. 【必須】提供される構成要素がパブリッククラウド上で提供されるものであること。
2. 【必須】アクセシビリティに配慮したものであること。

3.2 セキュリティ要件

教育クラウドプラットフォームのセキュリティ要件については、ISO/IEC 27002 に基づき、総務省が平成 26 年４月に作成・公表した「クラウドサービス提供における情報セキュリティ対策ガイドライン」から、必要な情報を記載している。各要件の末尾にて「クラウドサービス提供における情報セキュリティ対策ガイドライン」における第Ⅱ部の項目番号を括弧書きで記載している。

3.2.1 情報端末の方針

1. 【必須】情報端末において、利用者に一定強度以上のパスワード設定を義務付けること。また、教育クラウドプラットフォームへの接続時に一定強度以上のパスワードが設定されているかの有無をチェックすること。（6.2.1 (d)）
2. 【必須】情報端末と教育クラウドプラットフォームとの間の通信は十分な強度の暗号を用いて暗号化すること。（6.2.1 (e)）

3.2.2 情報へのアクセス制限

1. 【必須】教育クラウドプラットフォーム上で記録・管理される情報の機密性確保、完全性・真正性の検証、アクセス制御における認証、否認防止等について、暗号化を適用する範囲を明確にし、教材コンテンツ提供事業者等に情報開示すること。（10.1.1 (b)）

3.2.3 容量・能力の管理

1. 【任意】教育クラウドプラットフォーム提供事業者が取得するバックアップのうち、教育クラウドプラットフォームの提供に不可欠な設定などに関するデータのバックアップと、構成要素の預託データのバックアップを分離すること。（12.3.1 (a)）
2. 【任意】構成要素の預託データのバックアップにおいて、個々の構成要素の預託データを特定できる、ないしは検索可能な措置を講じること。（12.3.1(b)）

3.2.4　セキュリティログの管理

1. 【必須】脅威として監視すべきイベント等を定め、これに基づいて、教育クラウドプラットフォームとして取得するイベントログの範囲、内容、粒度等を定めること。（12.4.1 (a)）
2. 【必須】ログ情報の保護に関し、適切なアクセス制御、資源の分離等の保護対策を適用し、ログ情報の記録の削除や、改ざん、ログ取得設定の変更などを防止すること。（12.4.2 (a)）
3. 【必須】記録媒体の提出命令等によるサービス停止を防ぐため、ログ情報のバックアップを作成するとともに、ログ情報を利用者/特権ユーザ単位に管理できる措置を講じること。（12.4.2 (b)）
4. 【推奨】システムの脆弱性、サービス管理のためのアプリケーションなどの脆弱性を利用した管理用インターフェースの悪用を防ぐため、管理アプリケーションに対する利用状況やそのためのプログラム等の構成管理状況のログを取得し、監視等の措置を講じること。（12.4.3(b)）

3.3　利用環境要件

3.3.1　情報端末に係る要件

1. 【必須】オペレーティングシステム（OS）が Windows7 以降、MacOSX 以降、iOS9 以降、Android5.0 以降又は Chrome OS のいずれかであること。
2. 【必須】画面解像度が 1366x768 相当以上であること。
3. 【必須】中央演算装置（CPU）が 2 コア 1.7GHz 相当以上であること。
4. 【必須】メモリが 2GB 以上であること。
5. 【必須】HTML5 対応のウェブブラウザを有すること。

3.3.2　接続ネットワークに係る要件

1. 【推奨】動画コンテンツの利用を想定する場合、1 同時接続あたり 1.4Mbps の帯域が確保されること。
2. 【必須】HTTPS 通信は、TLS1.2 以上に対応すること。

【注記】

動画コンテンツより低帯域の教材コンテンツを利用する場合、1.4Mbps 以下でも教育クラウドプラットフォームの利用は可能。また、本要件については、「3.2.1　情報端末の方針」も参照。

4. 認証基盤に係るシステム要件

認証基盤に係るシステム要件を以下に示す。

4.1 アイデンティティプロバイダ（IdP）

アイデンティティプロバイダ（IdP）は、「アカウント管理機能」及び「認証機能」により構成される。

4.1.1 アカウント管理機能

アカウント管理機能は、アカウント情報を管理運用するための機能として、「属性ベースアクセス制御機能」、「アカウント一括操作機能」、「アカウント操作機能」及び「監査ログ記録機能」により構成される。

4.1.1.1 アカウント情報のデータ要件

1. 【必須】IdP 内で一意の IdP アカウント ID を有すること。
2. 【必須】IdP アカウント ID に対応した、認証用のパスワードを有すること。
3. 【必須】教育クラウドプラットフォーム内で一意の、各システムで共通的に利用する利用者識別用 ID を有すること。

【注記】

IdP で管理される IdP アカウント情報は、IdP アカウント ID をキーとして IdP アカウントのパスワードを管理する。当該パスワードの設定については、システムセキュリティ要件の「3.2.1 情報端末の方針」も参照。

4.1.1.2 属性ベースアクセス制御機能

1. 【必須】管理権限を有する利用者の職位、所属組織等の属性に応じて、対象範囲のアカウントのアクセス制御管理を行うことができること。

4.1.1.3 アカウント一括操作機能

1. 【推奨】アカウント情報の登録、変更及び削除を一元的に行うことができること。

   【規定例】

   - アカウントのプロビジョニング機能は、SCIM2.0 プロトコルによるデータの操作が可能であること。
   - アカウントのプロビジョニング機能は、CSV ファイルによるデータの操作が可能であること。

4.1.1.4　アカウント操作機能

1. 【必須】IdP アカウント ID とパスワードに対して個別に操作を行うことができること。
   (ア) 【必須】アカウント操作は、IdP アカウント ID に対して利用停止（非アクティブ化）と利用再開（アクティブ化）の設定ができること。
   (イ) 【必須】アカウント操作は、パスワードに対してリセットを含む「パスワード変更」が可能なこと。

4.1.1.5　監査ログ記録機能

1. 【必須】アカウント情報の追加、変更、削除等の重要な操作についての監査ログを記録することができること。

   【注記】

   本機能については、「3.2.4　セキュリティログの管理」も参照。

4.1.2　認証機能

認証機能は、教育クラウドプラットフォームが利用者を認証する機能として、「シングルサインオン機能」、「AuthN Provider 連携機能」、「SP/RP アクセス制御機能」、「属性情報取得問合せ機能」、「監視ログ記録機能」及び「シングルログアウト機能」により構成される。

4.1.2.1　シングルサインオン機能

1. 【必須】一度の認証によってトラストフレームワーク内の対応 SP/RP に対しての認証を実現すること。
2. 【必須】認証プロトコルは、SAML2.0 又は OpenID Connect のいずれかとすること。
3. 【必須】トラストフレームワークのためのシステム間の相互認証機能を有すること。

   【規定例：SSO のプロトコルとデータ形式を SAML とする場合】

   - トラストフレームワーク構成のために SAML メタデータを管理・配付する機能を有すること。

   【規定例：SSO のプロトコルとデータ形式を OIDC とする場合】

   - トラストフレームワーク構成のために OpenID プロバイダメタデータを管理・配付する機能を有すること。

4. 【必須】SP/RP へ通知する個人識別子として利用者識別用 ID を利用すること。

【注記】

シングルサインオンに必要な各種要件は、採用する認証プロトコルの仕様に従う。

【注記】

トラストフレームへの参加に際しては、掲載するコンテンツ教材コンテンツの安全性・安定性が担保されるよう、提供者審査、コンテンツ審査等のプロセスを有することが望ましい。

4.1.2.2 AuthN Provider 連携機能

1. 【必須】AuthN Provider と連携し、個人認証機能を提供することができること。
   (ア) 【必須】AuthN Provider アカウント ID を有すること。
   (イ) 【必須】教育クラウドプラットフォーム提供事業者によって示される複数の AuthN Provider から利用対象を選択できること。
   (ウ) 【必須】利用者識別用 ID と AuthN Provider アカウント ID の関連状態を管理できること。
2. 【任意】トークン認証（ワンタイム・パスワード）、IC カード認証、生体認証等の強力な認証方式と組み合わせることが可能であること。
3. 【推奨】利用者の状況や利用環境に応じて、あらかじめ決められた回数、ログインに失敗したアカウントを、自動的にロックして使用不能にできること。

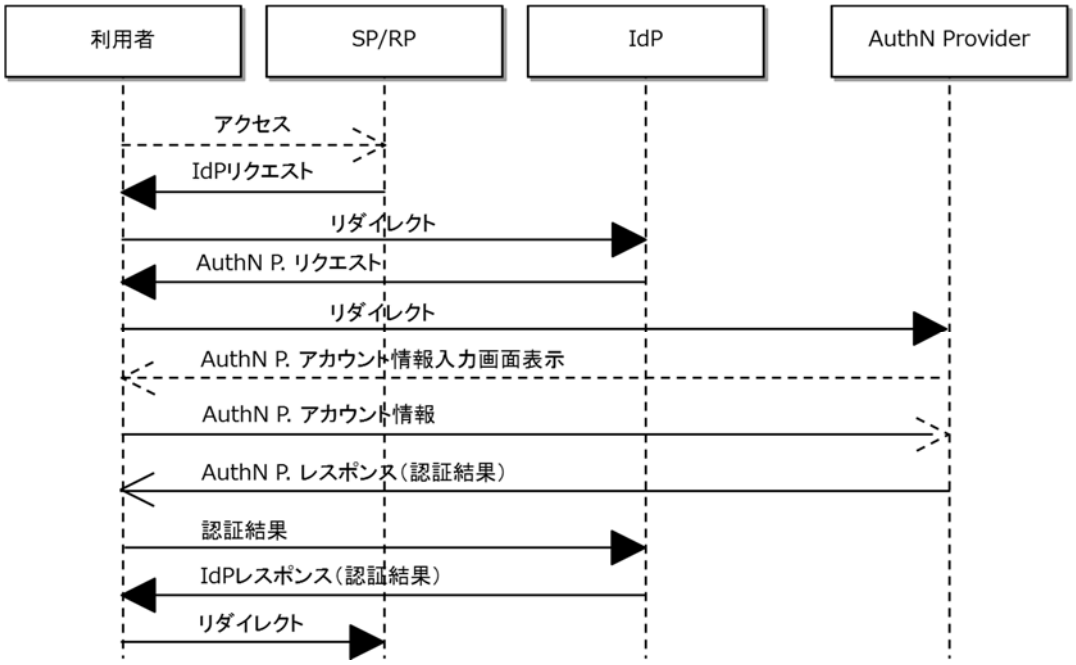

図 4.IdP と AuthN Provider の連携

4.1.2.3　SP/RP アクセス制御機能

1. 【必須】SP/RP へのアクセスに対して、URL をベースとしたアクセス制御の機能を提供することができること。

【注記】

本機能については、「3.2.2　情報へのアクセス制限」も参照。

4.1.2.4　属性情報取得問合せ機能

1. 【必須】利用者の属性情報を SP/RP に対して渡すことができること。
2. 【必須】IdP アカウント ID ごとに、AtrP の所在を示す URL による「AtrP エンドポイント情報」を有すること。
3. 【必須】SP/RP が IdP を介して AtrP の属性情報を問合せることができること。

【規定例：SSO のプロトコルとデータ形式を SAML とする場合】

- 属性情報連携のプロトコルとデータ形式は、SAML の「AttributeQuery」に準拠すること。

【規定例：SSO のプロトコルとデータ形式を OIDC とする場合】

- 属性情報連携のプロトコルとデータ形式は、OIDC の「Aggregate Claims」に準拠すること。

4. 【必須】SP/RP が直接 AtrP の属性情報を問合せることができること。

【規定例：SSO のプロトコルとデータ形式を SAML とする場合】

・ 属性情報連携のプロトコルとデータ形式は、SAML の「AttributeQuery」に準拠すること。

【規定例：SSO のプロトコルとデータ形式を OIDC とする場合】

・ 属性情報連携のプロトコルとデータ形式は、OIDC の「Distributed Claims」に準拠すること。

【注記】

属性情報取得問合せ機能は、SP/RP が AtrP から利用者の属性情報を取得する際に IdP が担当する機能である。SP/RP の属性情報取得問合せは、一旦 IdP によって受け付けられた後に AtrP に通知され、AtrP により属性情報の提供可否が判断される。属性情報を提供可能な際、AtrP は、IdP に対して、属性情報自身を提供するか、属性情報の取得方法を通知する。

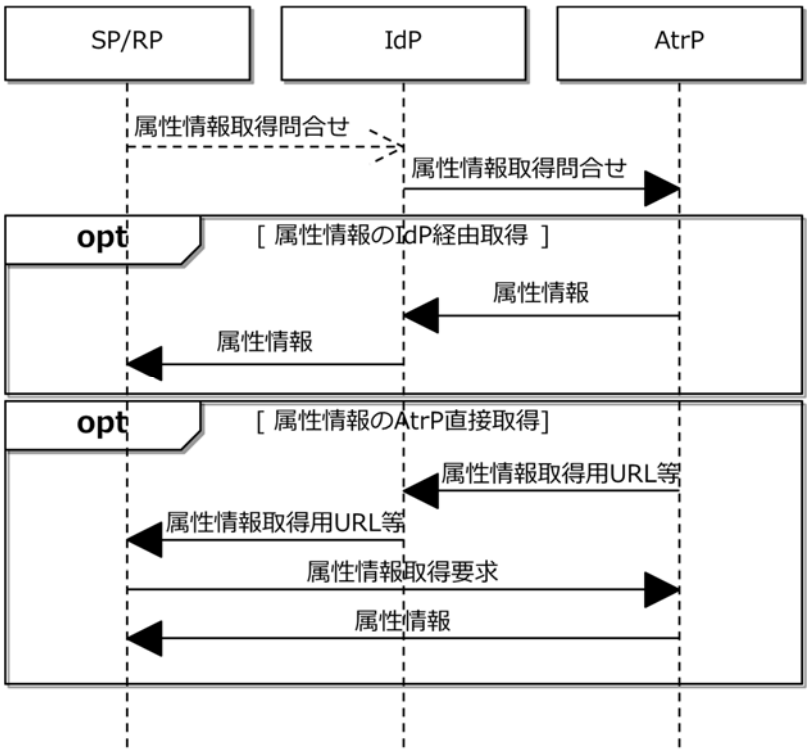

図 5. SP/RP による属性情報取得の例

4.1.2.5 監査ログ記録機能

1. 【必須】アカウント認証やアクセス制御に関する、重要な操作を監査ログに記録することができること。

【注記】

本機能については、「3.2.4 セキュリティログの管理」も参照。

4.1.3 シングルログアウト機能

1. 【必須】SLO（シングルログアウト）機能を有すること。

   【規定例：SSO のプロトコルとデータ形式を SAML とする場合】

   - SLO のプロトコルとデータ形式は、SAML の「SAML Single Logout」に準拠すること。

   【規定例：SSO のプロトコルとデータ形式を OIDC とする場合】

   - SLO のプロトコルとデータ形式は、OIDC の「Session Management」に準拠すること。

4.2 属性情報プロバイダ（AtrP）

属性情報プロバイダ（AtrP）は「属性情報取得問合せ応答機能」及び「パーソナルデータ利用認可機能」により構成される。

4.2.1 属性情報のデータ要件

1. 【必須】教育クラウドプラットフォーム内で一意の、各システムで共通的に利用する利用者識別用 ID を有すること。
2. 【必須】現在の所属、以前所属した学校・組織、役割等の所属情報を有すること。

   【規定例】

   所属情報として、所属自治体履歴情報、所属学校履歴情報、所属学年履歴情報、所属学級履歴情報を有すること。

【注記】

属性情報の真正性の確認は、教育委員会や学校などにより行われることを想定している。

【注記】

属性情報は必要に応じ追加することができる。

4.2.2 属性情報取得問合せ応答機能

1. 【必須】SSO のプロトコルとデータ形式に準拠した、属性情報取得問合わせに対する応答機能を有すること。

   【規定例：SSO のプロトコルとデータ形式に SAML を採用する場合】

   - 「AttributeQuery」に準拠すること。

   【規定例：SSO のプロトコルとデータ形式に OIDC を採用する場合】

   - 属性情報を IdP 経由で提供する際は、「Aggregate Claims」に準拠すること。
   - 属性情報の AtrP から直接提供をする際は、「Distributed Claims」に準拠

すること。

2. 【必須】個人識別子として利用者識別用 ID を利用すること。

4.2.3 パーソナルデータ利用認可機能

1. 【任意】パーソナルデータ許諾情報の登録、更新及び削除を行うことができること。
   (ア)【任意】パーソナルデータ許諾情報は、データ管理責任者となる教育委員会や事業者が定めるポリシーに基づき定義できること。
   (イ)【任意】パーソナルデータ許諾情報は、同意情報に基づき定義できること。
2. 【任意】パーソナルデータ許諾情報に基づいてアクセス制御を判断することができること。
3. 【任意】パーソナルデータ許諾情報に基づいてアクセス制御を執行することができること。
4. 【任意】個人識別子として利用者識別用 ID を利用すること。

4.3 認証元検出プロバイダ

4.3.1 認証元検出機能

1. 【必須】提供された IdP 識別子に対し、対応する IdP エンドポイント情報を提供することができること。

   【規定例：SAML 仕様の IdP と SP/RP がそれぞれ 2 つ以上ある際】

   - SAML Discovery Profile に対応し、Discovery Service からユーザの SAML IdP のエンドポイント情報を提供可能とすること。

   【規定例：SAML 仕様と OIDC 仕様の IdP と SP/RP がそれぞれ 1 つ以上あり、SP/RP への SSO のプロトコルとデータ形式を SAML とする場合】

   - OpenID Connect Discovery に対応し、ユーザに OpenID OP のエンドポイント情報を提供すること。
   - SAML 仕様と OIDC 仕様間のプロトコルとデータ形式の変換を行うこと。

   【規定例：SAML 仕様と OIDC 仕様の IdP と SP/RP がそれぞれ 1 つ以上あり、SP/RP への SSO のプロトコルとデータ形式を OIDC とする場合】

   - SAML Discovery Profile に対応し、ユーザに SAML IdP のエンドポイント情報を提供すること。
   - SAML 仕様と OIDC 仕様間のプロトコルとデータ形式の変換を行うこと。

【注記】

認証元検出プロバイダの「認証元検出機能」は、機能の一部又は全部を特定の IdP の機能として実装してもよい。

5. 教材コンテンツ

教材コンテンツに係る要件を以下に示す。

5.1 シングルサインオン対応機能

本機能の要件は、「4.1.2.1 シングルサインオン機能」と「4.3.1 認証元検出機能」を参照すること。

5.2 属性情報に基づく利用認可機能

1. 【必須】利用者の属性情報に基づき利用認可を行うことができること。

【注記】
属性情報の取得方法は、「4.1.2.4 属性情報取得問合せ機能」を参照。

5.3 教材コンテンツ表示用 UI 機能

1. 【必須】HTML5 に準拠した教材コンテンツを HTTPS により提供することができること。
2. 【推奨】Web Contents Accessibility Guideline 2.0 に準拠すること

6. ポータル

ポータルに係る要件を以下に示す。

6.1 シングルサインオン対応機能

本機能の要件は、「4.1.2.1 シングルサインオン機能」と「4.3.1 認証元検出機能」を参照すること。

6.2 属性情報に基づく利用認可機能

1. 【必須】利用者の属性情報に基づき利用認可を行うことができること。

【注記】
属性情報の取得方法は、「4.1.2.4 属性情報取得問合せ機能」を参照。

6.3 ポータル表示用 UI 機能

1. 【必須】HTML5 に準拠したポータルを HTTPS により提供することができること。
2. 【必須】教材コンテンツを識別するための教材コンテンツ情報を表示することができること。
3. 【必須】教材コンテンツに到達するための教材コンテンツへのリンク機能を有すること。
4. 【必須】UI コンテンツのプロトコルとデータ形式は、HTTPS 及び HTML5 に準拠すること。
5. 【推奨】Web Contents Accessibility Guideline 2.0 に準拠すること。

6.4 コミュニケーション機能

1. 【推奨】教員と学習者とのメッセージの交換が可能なコミュニケーション機能を有すること。

7. コンテンツメタデータ管理（推奨構成要素）

コンテンツメタデータ管理に係る要件を以下に示す。

なお、コンテンツメタデータ管理は、「2. 構成要件」で示しているとおり、その提供自体は【推奨】要件となっており、この節において【必須】要件としているものは、コンテンツメタデータ管理を提供する場合に限り【必須】要件となる。

7.1 コンテンツメタデータの管理

1. 【必須】コンテンツメタデータを有すること。
2. 【必須】コンテンツメタデータの管理機能を有すること。

【注記】

コンテンツメタデータについては、IEEE で国際標準となっている Learning Object Metadata（LOM）や、国内では一般社団法人日本教育情報化振興会（JAPET&CEC）が教科用図書ごとの差異を吸収した共通的なメタデータ「学習要素リスト」などについての検討が行われている。

7.2 コンテンツメタデータ登録機能

1. 【必須】複数のメタデータを一度に登録できること。
2. 【推奨】条件に一致するメタデータを一括して更新・削除できること。

7.3 コンテンツメタデータ問合せ応答機能

1. 【必須】コンテンツメタデータ間の検索条件の組み合わせに基づいた問合せ応答機能を有すること。

   【規定例】

   ・ コンテンツメタデータ問合せ応答機能は、メタデータの互換性定義（教科における算数⇔数学など）を用いた検索ができること。

   【規定例】

   ・ コンテンツメタデータ問合せ応答機能は、メタデータ対象が文字列の際、同形異音や振り仮名に関する対応辞書を有し、検索対象の表記揺れに対応した検索ができること。

   【規定例】

   ・ コンテンツメタデータ問合せ応答機能は、部分一致の検索の際、句読点除去

を行えること。

【規定例】

- コンテンツメタデータ問合せ機能は、検索条件に値域の範囲指定を行えること。

2. 【必須】コンテンツメタデータ問合せ応答機能の外部連携プロトコルは、HTTP 又は HTTPS に準拠することとし、データ形式は、RDF 又は JSON-LD に準拠すること。

8. マーケットプレイス（推奨構成要素）

マーケットプレイスに係る要件を以下に記す。

なお、マーケットプレイスは、「2. 構成要件」で示しているとおり、その提供自体は【推奨】要件となっており、この節において【必須】要件としているものは、マーケットプレイスを提供する場合に限り【必須】要件となる。

8.1 シングルサインオン対応機能

本機能の要件は、「4.1.2.1 シングルサインオン機能」と「4.3.1 認証元検出機能」を参照すること。

8.2 属性情報に基づく利用認可機能

1. 【推奨】利用者の属性情報に基づき利用認可が行うことができること。

【注記】

属性情報の取得方法は、「4.1.2.4 属性情報取得問合せ機能」を参照。

8.3 コンテンツ登録機能

1. 【推奨】教材コンテンツ提供事業者が、SP/RP の識別子、コンテンツの識別子、教材エンドポイント、価格情報、レビュー情報等を登録することができること。

8.4 コンテンツ検索機能

1. 【必須】HTML5 に準拠した教材コンテンツ検索と結果表示について、HTTPS により提供することができること。
2. 【必須】選択した教材コンテンツ情報を表示すること。
3. 【推奨】Web Contents Accessibility Guideline 2.0 に準拠すること。

8.5 コンテンツ利用申請・購入機能

1. 【推奨】教材コンテンツの利用権を取得するための機能を提供すること。

【注記】

教材コンテンツの利用権の取得については、教育委員会や学校等の事情に応じて、個別入札等のマーケットプレイスを介さない方法も想定される。

9. 学習記録データストア（推奨構成要素）

学習記録データストアに係る要件を以下に示す。

なお、学習記録データストアは、「2. 構成要件」で示しているとおり、その提供自体は【推奨】要件となっており、この節において【必須】要件としているものは、学習記録データストアを提供する場合に限り【必須】要件となる。

9.1 シングルサインオン対応機能

本機能の要件は、「4.1.2.1 シングルサインオン機能」と「4.3.1 認証元検出機能」を参照すること。

9.2 学習記録データ入出力問合せ機能

1. 【必須】学習記録データの入出力問合せに応答することができること。

   【規定例】

   - 学習記録データストアの外部連携プロトコルとデータ形式は、xAPI に準拠すること。

   【規定例】

   - 学習記録データストアの外部連携プロトコルとデータ形式は、Caliper に準拠すること。

9.3 パーソナルデータ利用認可機能

1. 【任意】パーソナルデータ許諾情報を登録、更新及び削除することができること。

   【規定例】

   - パーソナルデータ許諾情報は、データ管理責任者となる教育委員会や事業者が定めるポリシーに基づき定義できること。
   - パーソナルデータ許諾情報は、同意情報に基づき定義できること。

2. 【任意】パーソナルデータ許諾情報に基づいてアクセス制御を判断することができること。
3. 【任意】パーソナルデータ許諾情報に基づいてアクセス制御を執行することができること。

9.4 属性情報プロバイダへの追加要件

1. 【必須】属性情報は、URI による学習記録データストアエンドポイント情報を有すること。

【注記】

学習記録データは、教材コンテンツやポータルで生成され学習記録データストアに送信される。このため、教材コンテンツやポータルは学習記録データストアのエンドポイントを知る必要がある。