平成 27 年度クラウド等の最先端情報通信技術を活用した学習・教育モデルに関する実証別冊

セキュリティ要件ガイドブック

平成 28 年 3 月 31 日

NTT コミュニケーションズ株式会社

目次

1.はじめに

本書は、平成 27 年度「クラウド等の最先端情報通信技術を活用した学習・教育モデルに関する実証」において、技術仕様検討の一環として作成した、教育クラウドプラットフォームの一部もしくは、全てを構築し、提供する事業者（以下、事業者）向けの「セキュリティ要件ガイドブック」である。

2.ガイドブックの目的及び概要

2.1ガイドブックの目的

「セキュリティ要件ガイドブック」（以下、「本ガイドブック」）は、平成 27 年度「クラウド等の最先端情報通信技術を活用した学習・教育モデルに関する実証」において検討を行った教育クラウドプラットフォームについて、教育クラウドプラットフォームには児童生徒のアカウント情報や学習記録データなど、秘匿性の高い情報が保存されるため、事業者が教育クラウドプラットフォームを構築・提供する際には、適切なセキュリティ対策を講じるべきと考えられる。そのため、本書では教育クラウドプラットフォームを構築・提供する際に求められるセキュリティ要件を示すことを目的とする。

2.2教育クラウドプラットフォームの概要

教育クラウドプラットフォームの概要図 2-1 に示す。

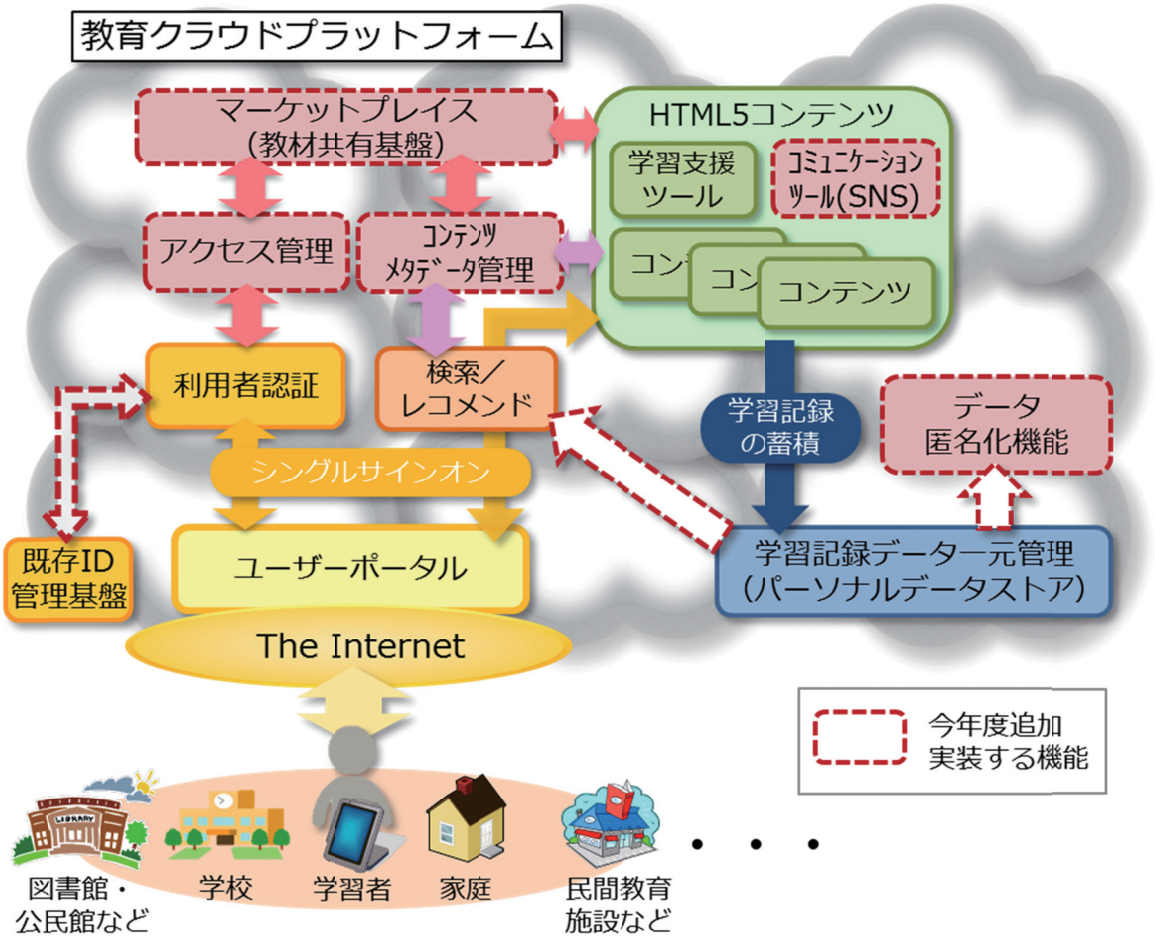


図 2-1　教育クラウドプラットフォームの概要

2.3ガイドブックの適用範囲および前提条件

事業者は、本事業と同様に IaaS のうちパブリック・クラウドサービスを選択し、公開された標準仕様をもとに教育クラウドプラットフォームを構築することを前提とする。本ガイドブッ

クではそのような事業者がセキュリティ対策を適切に実施できるよう、求められる要件を整理した。

本ガイドブックは、教育クラウドプラットフォームに求められるセキュリティ要件と、具体的なセキュリティ管理施策の実施例の 2 部から構成されている。

前半部分は、情報セキュリティマネジメントシステムの国際標準である ISO/IEC 27001:2013（JIS Q 27001:2014） 附属書 A の管理策（14 分野）の構成に沿い、教育クラウドプラットフォームに求めるべきと考えられるものを整理した。

後半部分は、特定非営利活動法人日本セキュリティ監査協会（JASA）[1]が主導するクラウドセキュリティ推進協議会[2]にて取りまとめられたクラウドサービスにおける基本リスクを元に、具体的な管理施策の例を提示している。

[1] 監査人資格制度の運営など、情報セキュリティ監査制度の普及促進を行う団体。http://www.jasa.jp/

[2] クラウド情報セキュリティ監査制度の創設など、クラウドの情報セキュリティに関する普及啓発を行う組織。http://jcispa.jasa.jp/

3.教育クラウドプラットフォームに求められるセキュリティ要件

3.1情報セキュリティのための方針群

3.1.1基本的な考え方

本項では、事業者の教育クラウドプラットフォーム運用に関する情報セキュリティポリシーについて記載する。当該ポリシーを通じ保護すべき情報は、利用者の個人情報や学習記録データである。また、当該ポリシーでは、情報の機密性（漏えい防止）、完全性（喪失の防止）、可用性（必要なタイミングで必要な情報にアクセス可能）、及びプラットフォームのサービス継続の 4 点を扱うこととする。

3.1.2求められている要件

表 3-1　プラットフォーム運用ポリシー

要件	プラットフォーム運用ポリシーとして、利用者の情報（個人情報、学習記録データ）の安全性（機密性、完全性、可用性）及びプラットフォームのサービス継続を含む方針を策定し、管理層の承認を得て、従業員及び関連する外部関係者に通知すること。
考え方	教育クラウドプラットフォームの運用ポリシーでは、利用者の情報（個人情報、学習記録データ）の漏えいや喪失の防止、必要なタイミングで必要なデータへのアクセス、契約に則ったサービス継続を実現する方針を策定することが望まれる。

3.2情報セキュリティのための組織

3.2.1基本的な考え方

本項では、情報セキュリティのための組織（内部組織）について、採り上げている。当該組織は、事業者が教育クラウドプラットフォームのセキュリティ対策を実施及び運用するためのもので、当該組織を中心に、情報セキュリティの役割と責任を定め、割り当てる必要がある。

3.2.2求められている要件

表 3-2　内部組織

要件	教育クラウドプラットフォームのセキュリティ対策を実施し、運用する情報セキュリティ担当組織を定めること。当該組織には、プラットフォームのセキュリティに関する役割と責任を割り当てること。
考え方	教育クラウドプラットフォームのセキュリティ対策を担当し責任を

	負う組織を明確にすることで、対策の実施が確実に進むものと期待される。

表 3-3　モバイル機器の利用及び校外学習

要件	教育クラウドプラットフォームの運用において、モバイル機器の利用及び校外学習に係るリスクを管理するために、必要な方針とその対策を採用すること。
考え方	教育クラウドプラットフォームの運用において、モバイル機器の利用やテレワーキングを通じて生じるリスクを洗い出し、そのリスクを管理するための方針と対策を採用することが期待される。たとえば、組織外ネットワークを利用する際の安全な通信、モバイル機器の紛失に伴う情報流出対策などが挙げられる。

3.3人的資源のセキュリティ

3.3.1基本的な考え方

一般的には、組織が人的資源として管理する従業員及び契約相手を対象とする。教育クラウドプラットフォームにおいては、これを運用するサポート要員（従業員及び運用に関する業務委託契約を締結しているパートナー企業等）を対象として検討する。

3.3.2求められている要件

表 3-4　人的資源のセキュリティ

要件	教育クラウドプラットフォームを運用するサポート要員（従業員及び運用に関する業務委託契約を締結しているパートナー企業等）に対して、雇用前、雇用期間中、雇用の終了及び変更の各段階で、必要な対策や教育及び訓練を行うこと。
考え方	教育クラウドプラットフォームを運用するサポート要員（従業員及び運用に関する業務委託契約を締結しているパートナー企業等）には、雇用前の選考や雇用条件（雇用契約書への反映）、雇用期間中の教育及び訓練、懲戒手続、雇用の終了及び変更後の遵守事項について、セキュリティ上の配慮が必要である。

3.4資産の管理

3.4.1基本的な考え方

本項では、資産の管理を採り上げる。資産の管理は、資産に対する責任、情報分類、媒体の取扱いの 3 つのカテゴリで構成される。資産には、利用者の情報（個人情報、学習記録データ）

及び教育クラウドプラットフォームに関連する機器・ソフトウェアが含まれる。利用者には、教員・ICT 支援員、児童・生徒が該当する。

3.4.2求められている要件

表 3-5　資産に対する責任

要件	情報及び教育クラウドプラットフォームに関連する資産を特定すること。特定した資産を管理すること。資産の利用の許容範囲に関する規則を文書化すること。全ての従業員及びプラットフォームの運用に関する業務委託契約を締結しているパートナー企業等は雇用、契約の終了時に、資産の全てを返却すること。
考え方	教育クラウドプラットフォームでは、利用者の情報（個人情報、学習記録データ）が格納される可能性があるため、それを前提とした資産管理が求められる。

表 3-6　情報分類

要件	教育クラウドプラットフォームで扱う情報を、重要性に応じて分類し、ラベル付けすること。情報をレベルに応じて安全に取り扱うこと。
考え方	利用者の個人情報は個人情報保護に係る法的対応が必要となる。また、学習記録データもセンシティブ情報として十分な保護が必要とされる。

3.5アクセス制御

3.5.1基本的な考え方

本項では、情報及びプラットフォームに対するアクセス制御について採り上げる。アクセス制御は、アクセス制御に対する業務上の要求事項、プラットフォームのサポート要員（運用に携わる従業員及び業務委託契約を締結しているパートナー企業）及び利用者のアクセス管理、サポート要員及び利用者の責任、システム及びアプリケーションのアクセス制御の 4 つのカテゴリで構成される。利用者には、教員・ICT 支援員、児童・生徒が該当する。

3.5.2求められている要件

表 3-7　アクセス制御に対する業務上の要求事項

要件	保護すべき情報及び教育クラウドプラットフォームへのアクセス制御方針を業務及び情報セキュリティの要求事項に基づいて文書化すること。

考え方	保護すべき情報（利用者の個人情報、学習記録データ）へのアクセス制御方針については、個人情報保護を考慮する必要がある。また、利用者が、プラットフォームへのアクセスが認められれば、権利を有する教材コンテンツを利用できるようにすることが望まれる。

表 3-8　サポート要員及び利用者のアクセス管理

要件	プラットフォームのサポート要員（運用に携わる従業員及び業務委託契約を締結しているパートナー企業）、利用者のそれぞれについて、登録及び登録削除に関する正式なプロセスを実施すること。全ての種類のサポート要員及び利用者に必要なアクセス権を割り当てる又は無効化するプロセスを実施すること。サポート要員の特権的アクセス権の割当て及び利用を制限すること。サポート要員及び利用者に対するパスワードの割当てを正式な管理プロセスで管理すること。サポート要員及び利用者のアクセス権を定期的にレビューすること。サポート要員及び利用者の異動等に応じて、アクセス権を削除又は修正すること。
考え方	サポート要員及び利用者のアクセス権を適切に設定するための仕組みを実現する。本プラットフォームの場合、教員・ICT 支援員が児童・生徒に対して、利用できる教材コンテンツへのアクセス権を設定できるようにする必要がある。また、教員が傘下の児童・生徒の個人情報及び学習記録データにアクセスできること、教員や ICT 指導員の異動、児童・生徒の転出・転入、クラス替え等に応じてアクセス権を変更できることが求められる。

表 3-9　操作者及び利用者の責任

要件	教育クラウドプラットフォームのサポート要員及び利用者がパスワードを定められた手順で利用し、保護すること。
考え方	教育クラウドプラットフォームの利用者にも、自らのパスワードを保護する責任を持たせることが望ましい。ただし、児童・生徒には複雑なパスワードを保護・管理することが難しいケースもある点を許容しなければならない。

表 3-10　システム及びアプリケーションのアクセス制御

要件	教育クラウドプラットフォームで管理する情報やアプリケーションへのアクセスを制限すること。プラットフォームへのアクセスは、セキュリティに配慮したログオン手順によって制御すること。パスワー

	ド管理システムは対話式で、良質なパスワードを確実とすること。特権的なユーティリティプログラムの使用を制限すること。プログラムソースコードへのアクセスを制限すること。
考え方	保護すべき情報（利用者の個人情報、学習記録データ）へのアクセス制御については、個人情報保護法に適用した手法を採用し、管理する必要がある。

3.6暗号

3.6.1基本的な考え方

本項では、暗号による管理策を採り上げる。教育クラウドプラットフォームにおいては、個人情報や学習記録データを暗号化し、保護する必要がある。暗号は、暗号化だけでなく、その鍵管理にも対応が求められる。

3.6.2求められている要件

表 3-11　暗号

要件	利用者の情報（個人情報、学習記録データ）を保護するために、暗号の利用方針を策定し、実施すること。暗号鍵の管理について、利用、保護及び有効期間に関する方針を策定し、実施すること。
考え方	教育クラウドプラットフォームでは、利用者の個人情報や学習記録データが格納される可能性があるため、それらを暗号化して保護することが望ましい。

3.7物理的及び環境的セキュリティ

3.7.1基本的な考え方

本項では、物理的及び環境的なセキュリティを採り上げる。一般的には、施設や区画への物理的なアクセスや、装置の環境上の脅威（災害、停電、盗難、破壊等）についての対策を検討するが、教育クラウドプラットフォームの場合、プラットフォームを構成するサーバ群はクラウド環境にあるため、後者については対象から外す。

3.7.2求められている要件

表 3-12　物理的セキュリティ

要件	教育クラウドプラットフォームの開発・運用環境について、物理的セキュリティ境界を定め、運用すること。セキュリティを保つべき領域（オフィス、部屋及び施設）を入退出管理策によって保護すること。

考え方	教育クラウドプラットフォームでは、利用者の個人情報が格納される可能性があるため、基盤として使用するクラウド環境にも個人情報保護への対応を求める必要がある。

3.8運用のセキュリティ

3.8.1基本的な考え方

本項では、セキュリティを保った運用を行うための取組みを採り上げる。セキュリティは機密性だけでなく、完全性や可用性も考慮する必要がある。具体的には、操作ミスでデータが消失したり、プラットフォームの性能不足で児童・生徒の同時アクセスによってサービスに支障を来したりするようなことがないよう、対策を立てることが求められる。また、マルウェア対策、ログ管理、運用ソフトウェアの管理、ぜい弱性管理、監査対応等についても、運用の維持という観点から述べる。

3.8.2求められている要件

表 3-13　運用の手順及び責任

要件	運用に関する操作手順を文書化すること。情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更を管理すること。要求されたシステム性能を満たすよう、資源の利用状況を監視・調整するとともに、将来必要となる容量・能力を予測すること。
考え方	教育クラウドプラットフォームのメンテナンスやバックアップの作業において、操作ミスが起きないよう、手順を明文化し、誰でも対応できるようにしておくことが望ましい。また、システム性能の制約でサービス品質が損なわれることのないよう監視するとともに、容量・能力の増強の要否についても検討する取組みが必要とされる。

表 3-14　マルウェアからの保護

要件	マルウェアから保護するために、サポート要員（運用に携わる従業員及び業務委託契約を締結しているパートナー企業）や利用者（教員・ICT 支援員、児童・生徒）への啓発とともに、検出、予防及び回復のための管理策を実施すること。
考え方	教育クラウドプラットフォームに接続するサポート要員や利用者に対し、端末のマルウェア対策を促すことが望まれる。また、プラットフォーム側のマルウェア対策を導入・運用することが求められる。

表 3-15　バックアップ

要件	教育クラウドプラットフォームの情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査すること。
考え方	想定外のトラブルにより学習記録データ等の重要情報が消失するリスクに備え、教育クラウドプラットフォームのバックアップを定期的に取得することが望まれる。なお、クラウドサービスのバックアップサービスでも代替可能と考えられる

表 3-16　ログ管理

要件	イベントログ（利用者の活動、例外処理、過失及び情報セキュリティ事象）、作業ログ（システムの実務管理及び運用管理）を取得し、保護するとともに、定期的にレビューすること。領域内のシステムクロックを同期させること。
考え方	ログは適切に取得し、改ざんされないよう保護する必要がある。また、情報セキュリティ事象等の問題が発生していないか、定期的にレビューすることが望ましい。なお、ログを正確に分析するためには、システムクロックの同期がとれていることが重要である。

表 3-17　運用ソフトウェアの管理

要件	運用に関わるソフトウェアの導入を管理する手順を行うこと。
考え方	教育クラウドプラットフォームの運用に関わるソフトウェアについて、導入する際の管理が適切に行えるよう、手順を定め実施することが求められている。

表 3-18　技術的ぜい弱性管理

要件	教育クラウドプラットフォームの技術的ぜい弱性に関する情報は、時期を失することなく取得すること。当該脆弱性によるプロットフォームのリスクを評価し、必要に応じて対策を適用すること。利用者によるソフトウェアのインストールを管理すること。
考え方	教育クラウドプラットフォームを構成するソフトウェアのぜい弱性が攻撃された場合、利用者の情報やサービスに深刻な問題が生じる可能性があるため、常にぜい弱性情報を取得し、対策の要否や実施について検討する必要がある。また、想定外のぜい弱性を持ち込まないよう、利用者によるソフトウェアのインストールを管理することが望まれる。

表 3-19　情報システムの監査に対する考慮事項

要件	教育クラウドプラットフォームの検証を伴う監査要求事項及び監査活動は、サービスの中断を最小限に抑えるために、慎重に計画し、合意すること。
考え方	システム監査のために運用を中断しなければならない可能性があるが、利用者に対する影響を最小限に抑えるように、準備する必要がある。

3.9通信のセキュリティ

3.9.1基本的な考え方

本項では、通信のセキュリティを確保するための取組みを採り上げる。具体的には、ネットワークセキュリティの管理と、転送される情報の保護が対象となる。

3.9.2求められている要件

表 3-20　ネットワークセキュリティ管理

要件	ネットワークを管理し制御すること。全てのネットワークサービスについて、セキュリティ機能、サービスレベル、及び管理上の要求事項を特定し、サービス合意書にも盛り込むこと。情報サービス、利用者及び情報システムは、ネットワーク上でグループごとに分離すること。
考え方	教育クラウドプラットフォームを利用する上で、情報をやり取りするネットワークの安全性を確保する必要がある。

表 3-21　情報の転送

要件	利用者の情報（個人情報、学習記録データ）等の転送時の安全性を維持するために、情報の転送方針、手順及び管理策を整備すること。事業者と外部関係者の間のセキュアな転送を可能にすること。電子メールに含まれた情報を適切に保護すること。秘密保持契約又は守秘義務契約のための要求事項を特定し、レビューし、文書化すること。
考え方	利用者の情報等が転送される際に流出するリスクを抑制することが求められる。

3.10システムの取得、開発及び保守

3.10.1基本的な考え方

本項では、システムの取得、開発及び保守におけるセキュリティの確保を採り上げる。具体的には、新しい情報システムもしくは既存の情報システムの改善、開発及びサポートプロセス、試験データにおけるセキュリティの確保が対象となる。

3.10.2求められている要件

表 3-22　システムの取得、開発及び保守

要件	新システム又は既存システムの改善に関する要求事項に、情報セキュリティに関連する要求事項を含めること。電子商取引等のアプリケーションがネットワークを経由する場合、その取引が保護されていること。特にアプリケーションの決済を含むトランザクション情報がネットワーク経由する場合、その情報が保護されていること。
考え方	教育クラウドプラットフォームの開発や改訂には、情報セキュリティに関する検討が必須であり、これを徹底する必要がある。

表 3-23　開発及びサポートプロセスにおけるセキュリティ

要件	教育クラウドプラットフォームの開発のための規則を整備し、適用すること。システムの変更は、変更管理手順を用いて管理すること。OS を変更する場合、組織の運用又はセキュリティに悪影響が出ないように、プラットフォームをレビューし、試験すること。パッケージソフトウェアの変更は必要な変更だけに限定し、厳重に管理すること。セキュリティに配慮したシステムを構築するための原則を確立し、実装に対して適用すること。セキュリティに配慮した開発環境を確立し、適切に保護すること。外部委託したシステム開発活動を監督し、監視すること。セキュリティ機能の試験は開発期間中に実施すること。新システム及び改訂・更新のために、受入れ試験のプログラム及び関連する基準を確立すること。
考え方	教育クラウドプラットフォームの開発や変更に関するプロセスを管理することが求められる。その際、外部委託する場合には、その監督、監視を行う必要がある。

表 3-24　試験データ

要件	試験データを注意深く選定し、保護し、管理すること。

考え方	教育クラウドプラットフォームの構築・更新時には、適切な構成の試験データを選択し、保管する必要がある。その際、利用者の情報（個人情報、学習記録データ）を含むデータは試験に用いるべきではない。仮にそれらを試験に用いる場合には、予め使用方法や使用範囲を設定し、管理する必要がある。

3.11供給者関係

3.11.1基本的な考え方

本項では、供給者、すなわち各種業務の委託契約を締結しているパートナー企業に対する情報セキュリティの確保を採り上げる。具体的には、パートナー企業がアクセスできる組織の資産の保護、供給者のサービス提供の管理が対象となる。パートナー企業には、一般に IT サービス提供者、セキュリティサービス提供者、設備運用の委託先、経営及び業務のコンサルタント、システムの開発者、クラウド事業者が挙げられる。

3.11.2求められている要件

表 3-25　供給者関係における情報セキュリティ

要件	供給者（各種業務の委託契約を締結しているパートナー企業）が組織の資産にアクセスできる場合、情報セキュリティ要求事項について、供給者と合意すること。組織の情報に対して、アクセス、処理、保存若しくは通信を行う供給者、又は組織の情報のための IT 基盤を提供する供給者と合意すること。供給者の再委託先や、供給者の情報セキュリティに関連する組織に対する情報セキュリティ要求事項について、供給者と合意すること。
考え方	パートナー企業が教育クラウドプラットフォームにアクセスできる場合、プラットフォームの事業者は、パートナー企業に対し情報セキュリティ対策を求める必要がある。特に、パートナー企業が利用者の情報（個人情報、学習記録データ）までアクセスできる場合には、パートナー企業の二次委託先、三次委託先等を含め、委託前の調査や委託中の監査等を通じて、情報セキュリティ確保を徹底するよう要求する必要がある。

表 3-26　供給者のサービス提供の管理

要件	組織は供給者のサービス提供を定常的に監視し、レビューし、監査すること。供給者によるサービス提供の変更を管理すること。
考え方	教育クラウドプラットフォームの事業者が、たとえばクラウド事業者

	のサービスレポートを入手し評価すること、情報セキュリティ監査を実施すること、さらにクラウド事業者のサービス変更により、リスク対策が損なわれたり、新たなリスクが発生したりすることがないよう確認することが挙げられる。

3.12情報セキュリティインシデント管理

3.12.1基本的な考え方

本項では、情報セキュリティインシデントの管理を採り上げる。情報セキュリティインシデントは「望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの」と定義される。また、情報セキュリティ事象は「情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象」と定義される。情報セキュリティインシデントは利用者の情報（個人情報、学習記録データ）の流出やサービスの中断など、深刻な事態を招く可能性があるため、発生時には適切に対処し、影響の拡大を抑制できるようにすることが重要である。

3.12.2求められている要件

表 3-27　情報セキュリティインシデントの管理及びその改善

要件	情報セキュリティインシデント対応に関する管理層の責任及び手順を確立すること。情報セキュリティ事象が、適切な管理者への連絡経路を通して、速やかに報告されること。従業員及び契約相手に、発見した又は疑いを持った情報セキュリティ弱点を記録し報告するよう要求すること。情報セキュリティ事象を評価し、情報セキュリティインシデントに分類するか否かを決定すること。情報セキュリティインシデントは、文書化した手順に従って対応すること。情報セキュリティインシデントの分析及び知識を、将来的なインシデントの可能性や影響を低減するために用いること。組織は、証拠となりうる情報の特定、収集、取得及び保存のための手順を定め、適用すること。
考え方	事業者は、教育クラウドプラットフォームに関連する情報セキュリティ事象についてできるだけ早く把握した上で、分析、対応・復旧、再発防止等の取組みを速やかに実施できるよう、あらかじめ準備する必要がある。

3.13事業継続マネジメントにおける情報セキュリティの側面

3.13.1基本的な考え方

本項では、事業継続マネジメントにおける情報セキュリティの継続を採り上げる。具体的には、情報セキュリティの継続と、情報処理施設の可用性が対象となる。

3.13.2求められている要件

表 3-28　情報セキュリティ継続

要件	困難な状況における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定すること。情報セキュリティ継続に対する要求レベルを得るためのプロセス、手順及び管理策を確立し、文書化し、実施すること。情報セキュリティ継続のための管理策を、定められた間隔で検証すること。
考え方	教育クラウドプラットフォームにおいては、児童・生徒の個人情報や学習記録データを扱う以上、困難な状況に陥った場合でも情報セキュリティを継続することが求められる。

表 3-29　冗長性

要件	情報処理施設は、可用性の要求を満たすのに十分な冗長性をもって導入すること。
考え方	事業者は、教育クラウドプラットフォームを運用する上で、情報処理施設の可用性を確保することが必要になる。

3.14順守

3.14.1基本的な考え方

本項では、法的及び契約上の要求事項の順守（コンプライアンス）と、情報セキュリティのレビューについて取り上げる。想定される法令としては、不正アクセス禁止法、個人情報保護法、著作権法、不正競争防止法などが挙げられる。

3.14.2求められている要件

表 3-30　法的及び契約上の要求事項の順守

要件	事業者が順守すべき法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを特定し、文書化し、最新に保つこと。知的財産権及び権利関係のあるソフトウェア製品の利用に

	関連する、法令、規制及び契約上の要求事項を順守する手順を実施すること。法令、規制、契約及び事業上の要求事項に従って、記録を、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護すること。プライバシー及び個人を特定できる情報（PII）は、関連する法令及び規制が適用される場合には、その要求に従って保護すること。暗号化機能は、関連するすべての協定、法令及び規制を順守して用いること。
考え方	教育クラウドプラットフォームを開発・運用する上で、個人情報保護法や著作権法、及びそれらを踏まえた規制、契約上の要求事項を順守する必要がある。

表 3-31　情報セキュリティのレビュー

要件	情報セキュリティ及びの実施の管理に対する事業者の取組みについて、定期的又は重大な変化が生じた場合に、レビューを実施すること。管理者は、自らの責任の範囲内にある情報処理及び手順の、情報セキュリティの方針群、標準類、他のセキュリティ要求事項に対する順守状況を定期的にレビューすること。情報システムの、情報セキュリティの方針群、標準類、他のセキュリティ要求事項に対する順守状況を定めに従ってレビューすること。
考え方	教育クラウドプラットフォームの情報セキュリティについて、事業者、管理者によるレビューと、技術的観点のレビューが求められる。

4.具体的なセキュリティ管理施策

本項では、クラウドセキュリティ推進協議会が取りまとめた基本リスクに対して、具体的な管理施策の例をセグメントごとに提示する。4.2 にて記載するネットワーク構成は典型的な構成を想定したものであり、各事業者が構築、運用する実際のネットワークに応じて適宜適用いただくことを前提としている。

なお、あくまでも本ガイドブックはセキュリティ対策部分に焦点を絞っており、セキュリティの確保に関係のない教育クラウドプラットフォームの構成要素については扱わない。

4.1基本リスク

クラウドセキュリティ推進協議会が取りまとめた基本リスクを表 4-1 に示す[3]。番号に付与されている H, M, L の接頭辞は、それぞれリスクの重大性が高、中、低であることを示している。

表 4-1　クラウドセキュリティ推進協議会による基本リスク

カテゴリ	番号	リスクの識別名	リスクの具体的な内容
保護すべき情報が漏えいするリスク(機密性)	H05	利用者・サービス間の情報隔離に失敗する	クラウドサービスを構成するメカニズムの不備・欠陥や脆弱性への攻撃により、異なるユーザやサービス間の隔離が失われることで、ユーザの機密情報の漏えいなどが生じ、事業者の評判が失墜する。
	H06	サービスエンジンの制御機能を奪われる	脆弱性等を通じてサービスエンジンの制御を奪われることで、クラウドサービスに特化した攻撃（サービスエンジン経由の情報漏えい、リソースの逼迫化によるサービスのマヒ等）が行われる可能性がある。
	M07	クラウドプロバイダでの内部不正－特権の悪用	・クラウド事業者における従業員の悪意の行動が、あらゆるクラウドサービスに影響を及ぼす。 ・従業員が犯罪組織の標的とされ、上記の行動を行う。
	M08	管理用ユーザインターフェースに、不正にアクセスされ、使用、操作される	・クラウドサービスのユーザ向けに、インターネットからリソース制御を可能とするインタフェースが悪用され、サービス全体に影響を及ぼす。 ・クラウド事業者の管理者の制御用インタフェースも同様に悪用されることで、さらなる影響を及ぼす。

[3] http://jcispa.jasa.jp/downloadf/basic_risks_2014.pdf
および http://jcispa.jasa.jp/downloadf/pdf2012/2012_cloud_doc04.pdf を元に作成

カテゴリ	番号	リスクの識別名	リスクの具体的な内容
	M09	データ転送途上における攻撃、データ漏えい（アップロード時、ダウンロード時、クラウド間転送）	ユーザ環境とクラウドサービス、もしくは分散されたクラウドサービス相互間でのデータ転送機会が生ずることで、その転送中のデータの漏えいのリスクが生じる。
	M10	利用者別の情報削除、廃棄に失敗する	ストレージやバックアップテープ等の物理媒体を他のユーザと共用する場合、媒体には常時複数ユーザのデータが記録されるため、特定ユーザのデータだけを消去する目的で、その媒体を物理的に破壊することはできない。
	L14	サプライチェーン先から提供される業務が不全となる	・クラウドサービスにおける認証等のサービスを外部委託することで、その委託先サービスに脆弱性が存在するとクラウドサービス全体に影響が及ぶ可能性がある。 ・どの部分を外部委託しているかを明示しないことで、ユーザによるクラウドサービスへの信頼度が低下する。
	L18	データの集中により当局によるデータ押収が行われた場合、他利用者含め 情報が開示され、またサービスが停止する	クラウドサービス上にデータが集中することで、司法当局によるデータの押収が行われた場合に、開示したくないデータまで開示されるリスクが増大するため、ユーザによるクラウドサービス利用を躊躇させる要因となる可能性がある。
	L19	国内外の法令等の開示、提出命令により、他利用者含め情報が開示され、 またサービスが停止する	クラウドサービスの物理的インフラが設置される地域（国、州など）によっては、異なる司法上の解釈や独裁的な警察権力、国際的取り決めが遵守されないなどの影響がユーザに及ぶ可能性がある。
情報及び処理が改ざんされる	H01	利用者・サービスの高集約、共有化により、障害が派生、拡大する	仮想化技術は、１台の物理ホストに n 台の仮想マシンを集約することで、リソースの利用効率を n 倍に高める一方、障害発生時の影響も n 倍に拡大する。また、データセンタの大規模利用は、１か所のデータセンタ

カテゴリ	番号	リスクの識別名	リスクの具体的な内容
リスク(完全性)			に多数の利用者を収容することで、インフラの利用効率を高める一方、データセンタ内の障害発生時の影響も拡大する。例えば、データセンタ内のネットワークの設定ミスが、クラウドシステムの大半の機能を停止させ、大規模障害が発生するリスクがある。
	H06	サービスエンジンの制御機能を奪われる	脆弱性等を通じてサービスエンジンの制御を奪われることで、クラウドサービスに特化した攻撃（サービスエンジン経由の情報漏えい、リソースの逼迫化によるサービスのマヒ等）が行われる可能性がある。
	M07	クラウドプロバイダでの内部不正－特権の悪用	・クラウド事業者における従業員の悪意の行動が、あらゆるクラウドサービスに影響を及ぼす。 ・従業員が犯罪組織の標的とされ、上記の行動を行う。
	M08	管理用ユーザインターフェースに、不正にアクセスされ、使用、操作される	・クラウドサービスのユーザ向けに、インターネットからリソース制御を可能とするインタフェースが悪用され、サービス全体に影響を及ぼす。 ・クラウド事業者の管理者の制御用インタフェースも同様に悪用されることで、さらなる影響を及ぼす。
	L14	サプライチェーン先から提供される業務が不全となる	・クラウドサービスにおける認証等のサービスを外部委託することで、その委託先サービスに脆弱性が存在するとクラウドサービス全体に影響が及ぶ可能性がある。 ・どの部分を外部委託しているかを明示しないことで、ユーザによるクラウドサービスへの信頼度が低下する。
サービス提供ができなくなるリスク(可用性)	H01	利用者・サービスの高集約、共有化により、障害が派生、拡大する	仮想化技術は、１台の物理ホストにｎ台の仮想マシンを集約することで、リソースの利用効率をｎ倍に高める一方、障害発生時の影響もｎ倍に拡大する。また、データセンタの大規模利用は、１か所のデータセンタに多数の利用者を収容することで、インフラの利用効率を高める一方、データセンタ内の障害発生時の影響も拡大する。例えば、データセンタ内のネットワークの設定ミスが、クラウドシステムの大半の機能を停止させ、大規模障害が発生するリスクがある。
	H02	仮想／物理の設計・運用の不整合	仮想化技術は、キャパシティのオーバーサブスクリプションを可能にするため、仮想リソースの総和と物理リソースの総和は一致するとは限らない、ソフトウェ

カテゴリ	番号	リスクの識別名	リスクの具体的な内容
			アと物理ホストが一対一対応しない、仮想スイッチと物理スイッチの VLAN 設計が異なるなど、従来のコンピュータ、ネットワークの設計・運用管理のノウハウが通用しないことが多い。仮想/物理にまたがるコンピュータとネットワークの大規模化・複雑化によって、予期せぬ不具合、大規模障害が発生するリスクがある。
	H03	他の共同利用者の行為による信頼の喪失	・他のユーザの活動により、同じクラウドサービスを利用するユーザの IP アドレスが外部サービスによりブロックされる。 ・他のユーザの活動により、利用していたストレージが押収されてサービスの継続が困難になる。
	H04	リソースの枯渇（リソース割当の過不足）	・クラウド事業者の予想を超えるユーザの需要増により、インフラやリソースがユーザの需要を満たせずサービスに支障が生ずることで、ユーザの減少や評判の低下を招く。 ・上記のリスクを回避するためにリソースを増強することで、場合によっては過剰投資として収益性を低下させる。
	M11	クラウド内 DDoS/DoS 攻撃	悪意のユーザもしくはユーザ環境の乗っ取り等を通じて同じクラウドサービス内を起点とする DDoS/DoS 攻撃が行われることで、インターネット経由の場合よりも大きな被害がユーザに発生する。
	L12	ロックインによるユーザの忌避	クラウドプロバイダが、外部リソースを利用してユーザデータを保護する必要性が生じても、相互接続性がないために、データ移行ができない。
	L14	サプライチェーン先から提供される業務が不全となる	・クラウドサービスにおける認証等のサービスを外部委託することで、その委託先サービスに脆弱性が存在するとクラウドサービス全体に影響が及ぶ可能性がある。 ・どの部分を外部委託しているかを明示しないことで、ユーザによるクラウドサービスへの信頼度が低下する。
	L18	証拠提出命令と電子的証拠開示	クラウドサービス上にデータが集中することで、司法当局によるデータの押収が行われた場合に、開示したくないデータまで開示されるリスクが増大するため、ユーザによるクラウドサービス利用を躊躇させる要因

カテゴリ	番号	リスクの識別名	リスクの具体的な内容
			となる可能性がある。
	L19	司法権の違い	クラウドサービスの物理的インフラが設置される地域（国、州など）によっては、異なる司法上の解釈や独裁的な警察権力、国際的取り決めが遵守されないなどの影響がユーザに及ぶ可能性がある。

4.2想定するネットワーク構成

本ガイドブックにて想定するネットワーク構成を図 4-1 に示す。

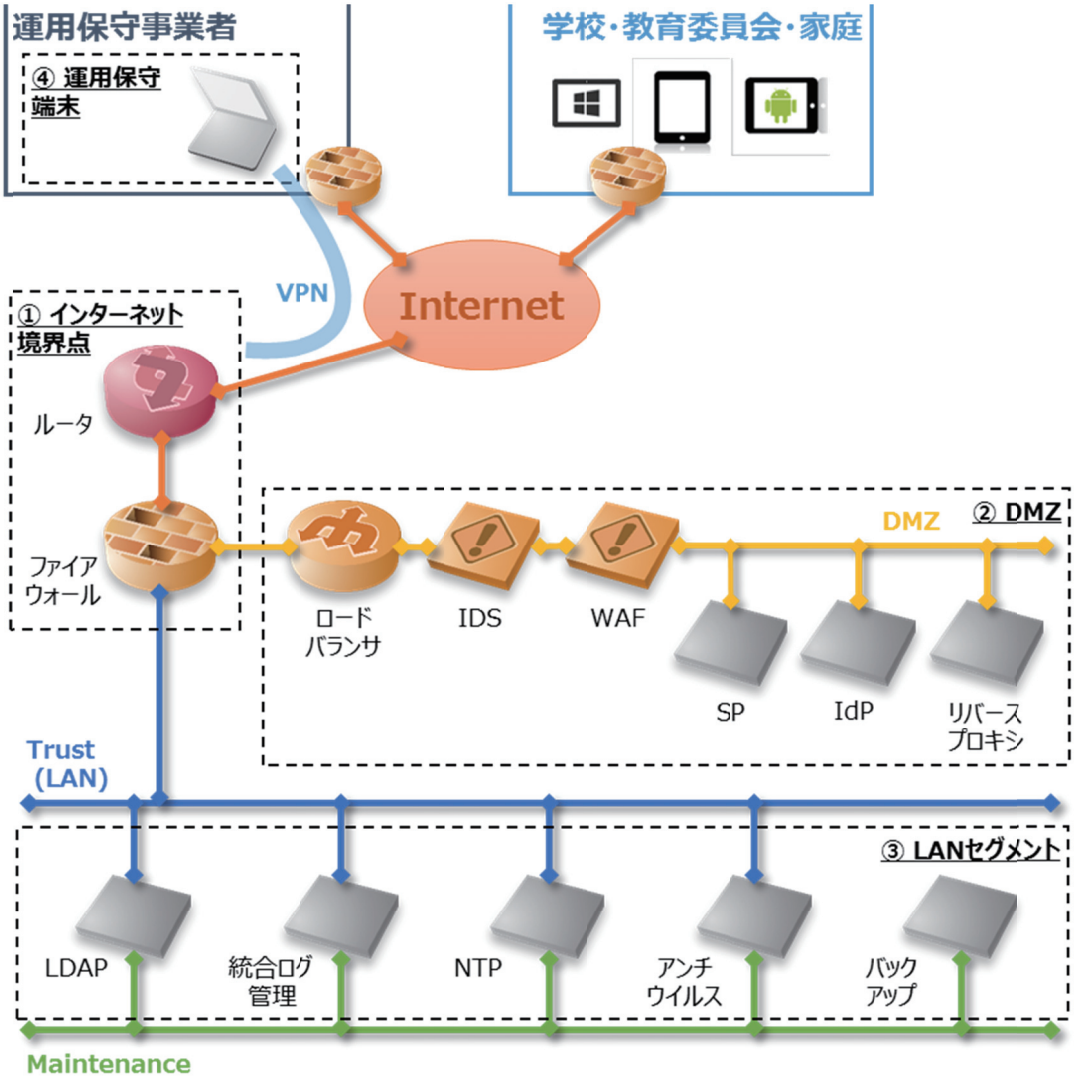


図 4-1　想定するネットワーク構成図

4.3具体的なセキュリティ管理施策

4.1 に示した基本リスク、および 4.2 に示した想定ネットワーク図を元に、具体的なセキュリティ管理施策を下記に示す。各施策の末尾に【】で囲んだ内容は、4.1 の基本リスクの番号と対応しており、その施策の実施によって軽減されることが想定されるリスクの番号を表して

いる。ただし、4.1 の基本リスクにはクラウド環境の運用事業者のみでは対応できず、利用者が受容しなければならないリスクや、クラウド事業者の選定に関する内容も含まれているため、すべてのリスクを網羅するものではなく、あくまでもクラウド環境を構築する上での技術的な観点に絞って記載する。

4.3.1インターネット境界点

インターネット境界点において導入することが想定されるサービス/機器、および実装すべき機能の概要を表 4-2 に示す。

表 4-2　インターネット境界点におけるサービスと機能

対象サービス	施策 No	実装すべき管理施策の概要
-	A-01	ISP[4]のサービスを利用し、サービス妨害を目的とした大量のデータ送信（DDoS[5]攻撃）が確認された場合、該当の通信を遮断する。【M11】
ルータ	A-02	外部からのアクセスログをすべて取得し、統合ログ管理サーバに送信する。【H06・M11】
	A-03	運用保守事業者が使用する運用保守端末からの Internet VPN 接続を受け付け、クライアント証明書による認証およびワンタイムパスワードによる二要素認証を行ったうえで、VPN トンネルを構築する。【M08】
ファイアウォール	A-04	インターネット、DMZ、LAN セグメントの 3 つのセグメント間における通信に関して、送信元/先の IP アドレスおよびポート番号にてルール（ACL[6]）を設定し、制御する。【H06・M11】
	A-05	ファイアウォールを経由するすべての通信（成功、失敗を問わない）のログを取得し、統合ログ管理サーバに送信する。【H06・M11】

[4] Internet Service Provider の略。インターネット接続事業者。

[5] Distributed Denial of Service の略。攻撃対象に対して不正パケットを大量に送信し、ネットワーク負荷を高めてサービスを妨害する攻撃の手法。

[6] Access Control List の略。

4.3.2DMZ

DMZ[7]（非武装地帯）において導入することが想定されるサービス/機器、および実装すべき機能の概要を表 4-3 に示す。

表 4-3　DMZ（非武装地帯）におけるサービスと機能

対象サービス	施策 No	実装すべき管理施策の概要
ロードバランサ	B-01	タブレット端末との間の通信における SSL/TLS 通信の暗号化および復号処理を行う。【M09】
	B-02	必要に応じ、配下ネットワークのサービスを冗長化し、可用性の向上を図る。【H01・H02・H04】
IDS[8]	B-03	外部から内部に対して侵入を試みる通信を監視し、不正な通信が確認された場合は統合ログ管理サーバに送信した上で、システム管理者に通知する。【H06・M11】
	B-04	不正な通信のパターンファイル（シグネチャ）を定期的に更新する。【H06・M11】
WAF[9]	B-05	Web アプリケーションに対して侵入を試みる通信を監視し、不正な通信が確認された場合は統合ログ管理サーバに送信した上で、通信を遮断し、システム管理者に通知する。【H06】
	B-06	不正な通信のパターンファイル（シグネチャ）を定期的に更新する。【H06】
SP	B-07	アクセスの履歴をすべて取得し、統合ログ管理サーバに送信する。【H06・M11】
	B-08	内部 NTP サーバもしくは外部 NTP サービスを参照し時刻を同期する。【H06】
IdP	B-09	アクセスの履歴をすべて取得し、統合ログ管理サーバに送信する。【H06・M11】
	B-10	内部 NTP サーバもしくは外部 NTP サービスを参照し時刻を同期する。【H06】
リバースプロキシ	B-11	LAN セグメントからインターネットセグメントに対する http/https 通信をすべて集約する。【H06】

[7] De-Militarized Zone の略。

[8] Intrusion Detection System の略。外部からの不正な侵入を試みる通信を検知するシステム。

[9] Web Application Firewall の略。Web アプリケーションに対する不正な攻撃を遮断するシステム。

対象サービス	施策 No	実装すべき管理施策の概要
	B-12	悪意のあるサーバや業務に関係のないサーバへの通信を遮断する（ブラックリスト方式）。【H06】
	B-13	内部 NTP サーバもしくは外部 NTP サービスを参照し時刻を同期する。【H06】

4.3.3LAN セグメント

LAN セグメントにおいて導入することが想定されるサービス/機器、および実装すべき機能の概要を表 4-4 に示す。

表 4-4　LAN セグメントにおけるサービスと機能

対象サービス	施策 No	実装すべき管理施策の概要
LDAP	C-01	ユーザの属性情報を暗号化して格納する。【-】
	C-02	パスワード情報はハッシュ化して保存する。【H06】
	C-03	パスワードポリシーを定め、適用する。【H06】
	C-04	一定回数のパスワード誤入力があった場合にアカウントをロックする。【H06】
統合ログ管理	C-05	各種サービスから送信されたログを集約し、一定期間保存する。【H06】
	C-06	一定期間経過後のログは外部メディア等に保存し、ロールオーバーする。【H06】
	C-07	ログのハッシュ化を行い、ログの改ざんに備える。【H06】
NTP	C-08	外部の複数の NTP サーバと通信し、時刻同期を行う。【H06】
	C-09	LAN セグメントおよび DMZ のすべてのサーバおよびネットワーク機器との時刻同期を定期的に行う。【H06】
アンチウイルス	C-10	アンチウイルスのパターンファイルを常に更新する。【H06】
	C-11	LAN セグメントおよび DMZ のすべてのサーバにおけるパターンファイルを更新し、最新状態に保つ。【H06】
	C-12	不正なプログラム（マルウェア）をリアルタイムで検知し、駆除、削除、ファイル拡張子の変更、隔離等の対応を行うとともに、システム管理者に通知する。【H06】
バックアップ	C-13	LAN セグメントのすべてのサーバのバックアップを取得し、世代管理を行う。【H01・H02】
	C-14	必要に応じて、システム領域とデータ領域を分けて取得し、柔軟なリストアが可能な状態にする。【H01・H02】
-	C-15	各サービスの CPU、メモリ、ハードディスク等のリソースを常時

対象サービス	施策 No	実装すべき管理施策の概要
		監視し、利用状況が増加した場合でもシステムの可用性を損なわないように必要な対応を行う。【H04】
	C-16	LDAP サーバの暗号化に使用した秘密鍵を記録媒体に保存し、厳密に保管する。【H06】

4.3.4運用保守端末

運用保守端末において導入することが想定される機器、および実装すべき機能の概要を表 4-5 に示す。なお、ネットワーク図に記載のとおり、運用保守端末は運用事業者のオフィスからリモートで各種サーバが稼動するクラウドサービスに対して接続することを想定している。

表 4-5　運用保守端末におけるサービスと機能

対象機器	施策 No	実装すべき管理施策の概要
保守用端末	D-01	Internet VPN を使用するためのクライアント証明書をインストールする。【M08】
	D-02	ワンタイムパスワードを利用して Internet VPN の VPN トンネルを構築する。【M08】
	D-03	クライアントの操作ログをすべて取得する。【M08】

4.4基本リスクとセキュリティ管理施策の対応

表 4-6 に 4.1 で示した基本リスクと 4.3 の各項で示したセキュリティ管理施策の対応を示す。

表 4-6　基本リスクとセキュリティ管理施策の対応

カテゴリ	番号	リスクの識別名	対応する管理施策
保護すべき情報が漏えいするリスク(機密性)	H05	利用者・サービス間の情報隔離に失敗する	-
	H06	サービスエンジンの制御機能を奪われる	A-02, A-04, A-05, B-03, B-04, B-05, B-06, B-07, B-08, B-09, B-10, B-11, B-12, B-13, C-02, C-03, C-04, C-05, C-06, C-07, C-08, C-09, C-10, C-11, C-12, C-16
	M07	クラウドプロバイダでの内部不正－特権の悪用	-
	M08	管理用ユーザインターフェースに、不正にアクセスされ、使用、操作される	A-03, D-01, D-02, D-03

カテゴリ	番号	リスクの識別名	対応する管理施策
	M09	データ転送途上における攻撃、データ漏えい（アップロード時、ダウンロード時、クラウド間転送）	B-01
	M10	利用者別の情報削除、廃棄に失敗する	-
	L14	サプライチェーン先から提供される業務が不全となる	-
	L18	データの集中により当局によるデータ押収が行われた場合、他利用者含め情報が開示され、またサービスが停止する	-
	L19	国内外の法令等の開示、提出命令により、他利用者含め情報が開示され、 またサービスが停止する	-
情報及び処理が改ざんされるリスク(完全性)	H01	利用者・サービスの高集約、共有化により、障害が派生、拡大する	B-02, C-13, C-14
	H06	サービスエンジンの制御機能を奪われる	A-02, A-04, A-05, B-03, B-04, B-05, B-06, B-07, B-08, B-09, B-10, B-11, B-12, B-13, C-02, C-03, C-04, C-05, C-06, C-07, C-08, C-09, C-10, C-11, C-12, C-16
	M07	クラウドプロバイダでの内部不正－特権の悪用	-
	M08	管理用ユーザインターフェースに、不正にアクセスされ、使用、操作される	A-03, D-01, D-02, D-03
	L14	サプライチェーン先から提供される業務が不全となる	-
ビス提供ができなくなるリスク(可用性)	H01	利用者・サービスの高集約、共有化により、障害が派生、拡大する	B-02, C-13, C-14
	H02	仮想／物理の設計・運用の不整合	B-02, C-13, C-14
	H03	他の共同利用者の行為による信頼の喪失	
	H04	リソースの枯渇（リソース割当の過不足）	B-02, C-15
	M11	クラウド内 DDoS/DoS 攻撃	A-01, A-02, A-04, A-05, B-03, B-04, B-07, B-09
	L12	ロックインによるユーザの忌避	-
	L14	サプライチェーン先から提供される業務	-

カテゴリ	番号	リスクの識別名	対応する管理施策
		が不全となる	
	L18	証拠提出命令と電子的証拠開示	-
	L19	司法権の違い	-

平成 27 年度クラウド等の最先端情報通信技術を活用した学習・教育モデルに関する実証別冊

クラウド環境構築ガイドブック

平成 28 年 3 月 31 日

NTT コミュニケーションズ株式会社

目次

1.はじめに

本書は、平成 27 年度「クラウド等の最先端情報通信技術を活用した学習・教育モデルに関する実証」において、技術仕様検討の一環として作成した、事業者向けの「クラウド環境構築ガイドブック」である。

2.ガイドブックの目的及び概要

2.1ガイドブックの目的

「クラウド環境構築ガイドブック」（以下、「ガイドブック」）は、平成 27 年度「クラウド等の最先端情報通信技術を活用した学習・教育モデルに関する実証」において検討を行った教育クラウドプラットフォームについて、事業者が構築する際に有益と考えられる、以下の 3 点の情報を提供することを目的とする。

① 教育クラウドプラットフォームを構築する上でクラウド環境に求める要件（3 章）
② クラウド環境を構築するための手順（4 章）
③ 教育クラウドプラットフォームを構成する各モジュールをセットアップするための手順（5 章～6 章）

2.2教育クラウドプラットフォームの概要

教育クラウドプラットフォームの概要を図 2-1 に示す。

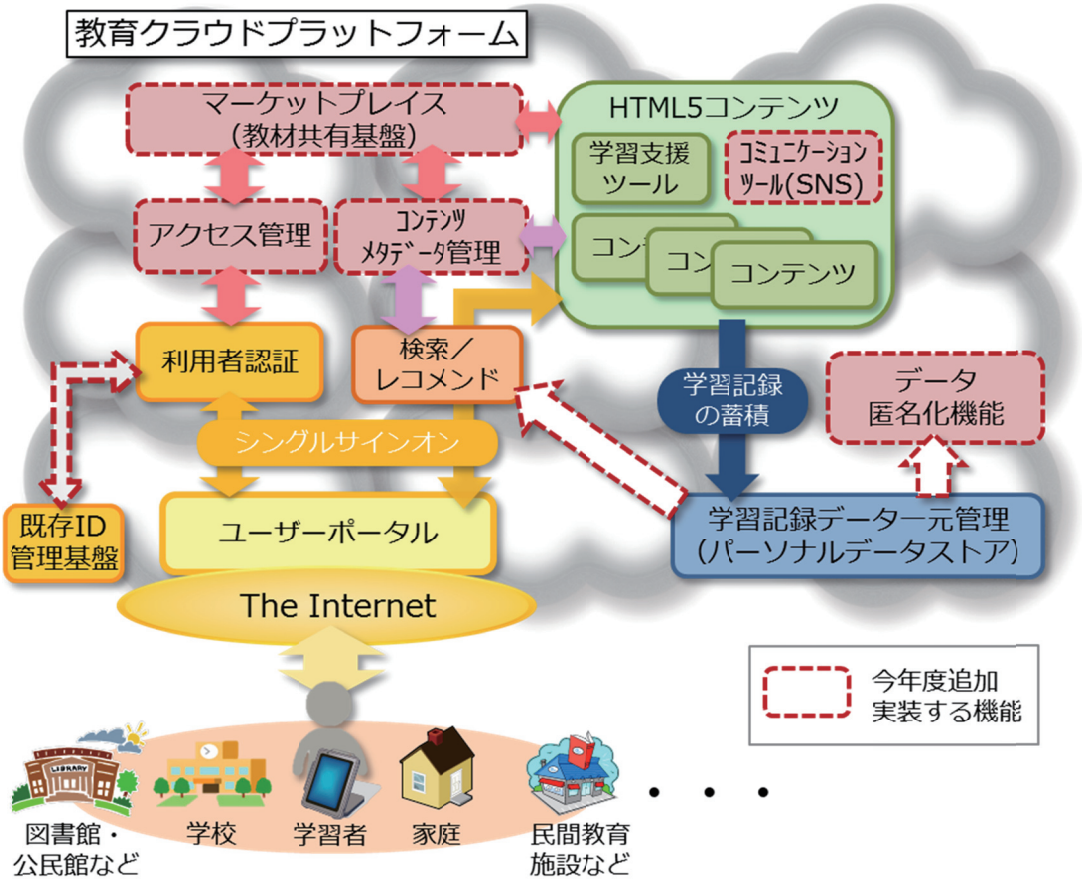


図 2-1 教育クラウドプラットフォームの概要

2.3ガイドブックの適用範囲および前提条件

教育クラウドプラットフォームは、前項で示した各機能をパブリック・クラウドサービス（IaaS）上で実現することを前提とする。

ガイドブックでは、パブリック・クラウドサービス（IaaS）に対して、特に非機能要件に対する考え方や求める要件を示すこととする。

非機能要件の項目については、独立行政法人情報処理推進機構（IPA）が公表している「非機能要求グレード」で定められた項目の中から、パブリック・クラウドサービス（IaaS）の要件と考えられる項目を選択した。

3.教育クラウドプラットフォームにもとめる要件

3.1可用性

3.1.1継続性

3.1.1.1運用スケジュール

表 3-1　運用時間

運用時間	
要件	運用時間は、24 時間 365 日稼働とすること。
考え方	教育クラウドプラットフォームでは、一般的なパブリック・クラウドサービス（IaaS）を想定するため、IaaS の基盤に対しては 24 時間 365 日の運用を想定する。

3.1.1.2稼働率

表 3-2　稼働率

稼働率	
要件	稼働率は、99.9%（1 年間に合計 9 時間弱の停止を許容）以上とすること。
考え方	SLA（サービス・レベル・アグリーメント）として、IaaS には 99.9%以上の稼働率を求めることとする。 教育クラウドプラットフォームでは、IaaS 上に OS やミドルウェア、アプリケーションなどを稼働させるため、それらの障害やメンテナンスのために、プラットフォーム全体の稼働率は IaaS の稼働率よりも低くなる。

3.1.2耐障害性

3.1.2.1ネットワーク

表 3-3　回線の冗長化

回線の冗長化	
要件	回線の冗長化は、インターネット接続回線について冗長化構成を取ること。
考え方	クラウドサービスにおける可用性確保において、インターネット接続回線の耐障害性は重要な要素である。クラウドサービス全体の可用性は稼働率で担保されると考えられるが、インターネット接続回線については冗長化構成を求めることで、インターネット側の障害に起因する不具合の可能性を軽減できる。

3.1.2.2データ

表 3-4　バックアップ方式

バックアップ方式	
要件	バックアップ方式は、オンラインバックアップを定期的に取得すること。
考え方	障害の発生に備えて、データのバックアップを定期的に取得する必要がある。クラウド環境で用意されているバックアップ機能を用いてオンラインバックアップを取得することが望ましい。

表 3-5　データ復旧範囲

データ復旧範囲	
要件	データ復旧範囲は、仮想マシンおよび業務データを含むすべてのデータを対象とすること。
考え方	教育クラウドプラットフォームでは、クラウドサービス（IaaS）上に各種ミドルウェアおよびアプリケーションを搭載して運用することが想定される。このため、障害発生時の復旧において、業務データのみならず、ミドルウェアやアプリケーションのデータもバックアップから復旧することで、早期の復旧を目指すことが可能となる。

3.2性能・拡張性

3.2.1業務処理量

3.2.1.1業務量増大度

表 3-6　データ量増大度

データ量増大	
要件	データ量増大に対しては、必要に応じて業務データ領域およびログデータ領域を拡張できること。
考え方	運用を開始した仮想マシンについて、配信するコンテンツ数や学習記録データの増加などによりディスク容量を増やす場合に、仮想マシンのタイプを変更したり、ディスクを追加したりするだけで、スケールアップによりデータ領域が拡張できるクラウド環境が望ましい。

3.2.1.2保管期間

表 3-7　ログデータの保管期間

ログデータの保管期間	
要件	ログデータの保管期間は、12 年間以上とできること。
考え方	ログデータの保管については、長期間にするとその分のログ記録領域がひつようになり、それらの分析にも多くのリソースが必要となるため、適切に設

	定する必要がある。 一方、教育クラウドプラットフォームにおいては、ビッグデータ活用の観点から、可能な限りログデータを蓄積することも考慮する必要がある。 ここでは、教育クラウドプラットフォームを利用する児童・生徒が、小学校・中学校・高等学校の合計 12 年間を過ごす間のログデータが消されずに蓄積できることを考慮した。

3.2.2リソース拡張性

3.2.2.1CPU 拡張性

表 3-8　CPU 拡張性

CPU 拡張性	
要件	CPU 拡張性は、業務開始当初に選択した仮想マシンと比較して、高速な CPU や追加のコア数を選択できること。
考え方	多様な教育 ICT サービスや教材コンテンツの開発が促されるよう、選択可能な CPU の幅が広いクラウド環境が望ましい。 また、運用を開始した仮想マシンについて、アクセスの増加などにより CPU リソースを増やす場合に、仮想マシンのタイプを変更するだけで、スケールアップにより CPU が拡張できるクラウド環境が望ましい。

3.2.2.2メモリ拡張性

表 3-9　メモリ拡張性

メモリ拡張性	
要件	メモリ拡張性は、業務開始当初に選択した仮想マシンと比較して、容量の大きなメモリサイズを選択できること。
考え方	多様な教育 ICT サービスや教材コンテンツの開発が促されるよう、選択可能なメモリ容量の幅が広いクラウド環境が望ましい。 また、運用を開始した仮想マシンについて、アクセスの増加などによりメモリ容量を増やす場合に、仮想マシンのタイプを変更するだけで、スケールアップによりメモリ容量が拡張できるクラウド環境が望ましい。

3.2.2.3ディスク拡張性

表 3-10　ディスク拡張性

運用時間	
要件	ディスク拡張性は、業務開始当初に選択した仮想マシンと比較して、容量の大きなディスクを選択できること。
考え方	多様な教育 ICT サービスや教材コンテンツの開発が促されるよう、選択可能

	なディスク容量の幅が広いクラウド環境が望ましい。 また、運用を開始した仮想マシンについて、配信するコンテンツ数や学習記録データの増加などによりディスク容量を増やす場合に、仮想マシンのタイプを変更したり、ディスクを追加したりするだけで、スケールアップによりディスク容量が拡張できるクラウド環境が望ましい。

3.2.3性能品質保証

3.2.3.1帯域保証機能の有無

表 3-11　帯域保証

帯域保証	
要件	帯域保証の設定は、サーバ毎に設定できること。
考え方	帯域保証機能については、アプリケーションの重要度に応じて設定できることが望ましい。例えば、コンテンツ視聴に帯域を占有されて、ポータルサイトへのアクセスに支障が出ないように、サーバ毎に設定できることが望ましい。

3.2.3.2スパイク負荷対応

表 3-12　トランザクション保護

トランザクション保護	
要件	一斉アクセスに係るピーク分散等を踏まえ、最適なリソースにて運用を行うこと。
考え方	教育クラウドプラットフォームの利用者の特性から、学校での授業開始時などに想定を超えたアクセスが集中する可能性がある。このようなピーク特性を考慮して、リソースの配置・運用を考慮する必要がある。

3.3運用・保守性

3.3.1通常運用

3.3.1.1バックアップ

表 3-13　バックアップ自動化の範囲

バックアップ自動化の範囲	
要件	バックアップ自動化の範囲は、仮想マシン単位で自動的にバックアップが取得できること。
考え方	一般的なクラウド環境では、仮想マシンのバックアップ（スナップショット）を定期的に取得する機能が備わっている。バックアップの自動化は、当該スナップショット機能を用いて定期的に取得することを想定する。

表 3-14　バックアップ取得間隔

バックアップ取得間隔	
要件	バックアップ取得間隔は、日次以上の頻度で取得できること。
考え方	スナップショット機能を用いたバックアップを日次で実施した場合、障害発生時には前日時点までの復旧が容易となる。 一方、スナップショット機能で取得したバックアップを、何世代前まで保持するかによって、バックアップ用に必要なデータ領域が大きくなる。このため、バックアップの頻度と保管する世代数を適切に設定する必要がある。

3.3.1.2運用監視

表 3-15　サーバの監視

サーバの監視	
要件	サーバの監視について、仮想マシンの死活監視がリアルタイム（分単位）でできること。
考え方	クラウド環境（IaaS）に対しては、仮想マシンまでが運用監視の対象となることから、仮想マシンの死活監視までを求めることとする。 一方、教育クラウドプラットフォームの全体的な運用監視については、仮想マシンの死活監視に加えて、アプリケーションレベルでの監視を行うことが望ましい。

表 3-16　ネットワークの監視

ネットワークの監視	
要件	ネットワークの監視について、障害や通信量の監視がリアルタイム（分単位）でできること。
考え方	ネットワークの監視については、障害の監視（死活監視）に加えて、通信量の監視を行うことで、ネットワーク輻輳の予兆などが確認できることが望ましい。

3.3.1.3時刻同期

表 3-17　時刻同期設定の範囲

時刻同期設定の範囲	
要件	時刻同期設定の範囲は、仮想マシンや仮想ネットワーク機器(FW やロードバランサなど）、監視機能を含めること。
考え方	障害発生時のログの確認のためには、クラウド環境（IaaS）全体で時刻同期が行われている必要がある。

3.3.2保守運用

3.3.2.1計画停止

表 3-18　計画停止

計画停止	
要件	計画停止は、1 ヶ月前に通知すること。ただし、停止時間は稼働率に含めないこととする。
考え方	クラウド環境（IaaS）の計画停止（メンテナンスなど）については、教育クラウドプラットフォーム利用者への周知期間や、他事業者のリソースへの再配置作業などを考慮して、事前に通知される必要がある。

3.3.2.2定期保守頻度

表 3-19　定期保守頻度

定期保守頻度	
要件	定期保守頻度は、月 1 回程度以下とすること。
考え方	仮想マシンの停止を伴う定期保守（計画停止）は、その頻度が高くなると、教育クラウドプラットフォーム全体の稼働率を下げる要因となるため、必要最小限に抑える必要がある。

3.3.3障害時運用

3.3.3.1システム異常検知時の対応

表 3-20　システム異常検知時の対応可能時間

システム異常検知時の対応可能時間	
要件	システム異常検知時の対応可能時間は、24 時間 365 日とすること。
考え方	クラウド環境（IaaS）の稼働時間として 24 時間 365 日を求めることから、対応（問い合わせ受付、障害回復への対処、など）も同様とする必要がある。

3.4セキュリティ

3.4.1前提条件・制約条件

3.4.1.1情報セキュリティに関するコンプライアンス

表 3-21　遵守すべき法令等

遵守すべき法令等	
要件	遵守すべき法令等については、個人情報保護法を遵守すること。
考え方	教育クラウドプラットフォームでは、利用者の個人情報が格納される可能性

	があるため、基盤として使用するクラウド環境にも個人情報保護への対応を求める必要がある。

表 3-22　クラウド環境の設置場所

クラウド環境の設置場所	
要件	クラウド環境の設置場所は、日本国内のデータセンターで運用設置されていること。取り扱うデータは、日本国内のみで管理できること。
考え方	クラウド環境が海外で運用設置された場合、設置場所の法令等で強制的にデータ開示がなされる可能性がある。そのため、児童・生徒の個人情報を保管する教育クラウドプラットフォームでは、日本国内で運用されているクラウド環境を選択する必要がある。

表 3-23　クラウド環境を提供する事業者

クラウド環境を提供する事業者	
要件	クラウド環境を提供する事業者は、特定のクラウド事業者によるロックインを抑止し、3 者（子会社、関連会社を除く）以上により提供されるクラウド環境とすること。
考え方	クラウド環境については、特定のクラウド事業者によるロックインにより、当該事業者の状況に依存する恐れがある。そこで、教育クラウドプラットフォームでは、複数社のクラウドを連携させて使うことで、一部のクラウド事業者に支障が生じた場合でも、運用を継続できる方策を講じることが望ましい。

3.4.2不正追跡・監視

3.4.2.1不正監視

表 3-24　不正監視

不正監視	
要件	不正監視については、ネットワークに対する不正アクセスなどを監視すること。
考え方	教育クラウドプラットフォームは、利用者はインターネットからのアクセスが前提となる。インターネットにおける昨今のサイバーセキュリティ上の脅威を考慮して、クラウド環境のネットワークに対する不正アクセスを適切に監視する必要がある。

3.4.3ネットワーク対策

3.4.3.1ネットワーク制御

表 3-25　ネットワーク制御

ネットワーク制御	
要件	ネットワーク制御は、不正なネットワークへのアクセスを制御（抑制）できること。
考え方	クラウド環境のネットワークに対する不正アクセスについては、検知をするとともに、抑制（不正アクセス元のホストからのアクセスの遮断など）できることが望ましい。

3.4.3.2サービス停止攻撃の回避

表 3-26　ネットワーク輻輳対策

ネットワーク輻輳対策	
要件	ネットワーク輻輳対策は、ネットワーク停止攻撃に対して制御（抑制）できること。
考え方	クラウド環境のネットワークに対するサービス不能（DoS）攻撃については、検知するとともに、抑制（不正アクセス元のホストからのアクセスの遮断など）できることが望ましい。

3.4.4マルウェア対策

3.4.4.1マルウェア対策

表 3-27　マルウェア対策実施範囲

マルウェア対策実施範囲	
要件	マルウェア対策実施範囲は、クラウド環境全体とすること。
考え方	教育クラウドプラットフォームのセキュリティ対策を行う観点から、その基盤になるクラウド環境においてもマルウェア対策を施す必要がある。

3.5システム環境・エコロジー

3.5.1システム制約/前提条件

3.5.1.1運用時の制約条件

表 3-28　運用時の制約条件

運用時の制約条件	
要件	運用時の制約条件は、個人情報保護法およびプライバシーマークに準拠すること。

考え方	教育クラウドプラットフォームでは、利用者の個人情報が格納される可能性があるため、基盤として使用するクラウド環境にも個人情報保護への対応を求める必要がある。

3.5.2システム特性

3.5.2.1特定製品指定

表 3-29　特定製品採用の有無

特定製品採用の有無	
要件	特定製品採用については、仮想マシン上で稼働させる OS は、教育クラウドプラットフォームで必要な OS を選択できること。
考え方	多様な教育 ICT サービスや教材コンテンツの開発が促されるよう、選択可能な OS の種類の幅が広いクラウド環境が望ましい。

3.5.3機材設置環境条件

3.5.3.1耐震/免震

表 3-30　耐震

耐震	
要件	耐震については、震度 7 相当（1000 ガル）を想定すること。
考え方	クラウド環境としては、日本国内への設置を求めることから、耐震対策が必要となる。

3.5.3.2電気設備適合性

表 3-31　停電対策

停電対策	
要件	停電対策は、72 時間以上を想定すること。
考え方	クラウド環境は、日本国内のデータセンターへの設置を想定し、適切な停電対策（非常用発電装置など）が施されていることが求められる。

3.5.4環境マネージメント

3.5.4.1エネルギー消費効率

表 3-32　エネルギー消費の目標値

エネルギー消費の目標値	
要件	エネルギー消費の目標値は、PUE 値が 1.8 以下であること。

考え方	環境配慮の観点から、教育クラウドプラットフォームで利用するクラウド環境についても、適切なエネルギー消費の目標値を設定する必要がある。

4.クラウド環境を構築するための手順

4.1サーバ環境の構築について

本事業で構築した教育クラウドプラットフォームには、3 社のクラウドサービス（エヌ・ティ・ティ・コミュニケーションズ株式会社：Cloudn 、日本電気株式会社：NEC Cloud IaaS、富士通株式会社：FUJITSU Cloud IaaS Trusted Public S5）を採用している。

大規模な障害を想定すると複数のクラウドサービスを組み合わせた方が高いシステムが構築できると考えられるが、構築手順の複雑化が懸念される。そこで、ここでは構築例としてエヌ・ティ・ティ・コミュニケーションズ株式会社：Cloudn を利用し、同様の環境を構築する場合の手順を示すこととする。

4.2利用したサーバのスペック一覧について

本事業で利用した仮想サーバの一覧は以下の通りである。

Cloudn はインターネットを介し接続可能なコントロールパネルから仮想サーバを作成することができる。仮想サーバの具体的な作成方法は、「Cloudn Compute FLAT タイプ 操作マニュアル 3.1. 仮想サーバを作成する」に記載がある。

なお、同様の仮想サーバはテンプレートを利用することで効率的に作成することが可能である。テンプレートの作成方法については、4.4 に記載している。

表 4-1　本事業で利用した仮想サーバ

サーバ名	CPU	メモリ	ディスク容量	OS
マイポータル(SP)	8vCPU	16GB	15GB+40GB	CentOS 6.5
リバプロ SP	2vCPU	4GB	15GB	CentOS 6.5
PDS	4vCPU	8GB	15GB+1000GB	CentOS 6.5
共通 I/F MBaaS+オーサリングツール(SP)	4vCPU	8GB	15GB	CentOS 6.5

4.3仮想サーバへの通信制御について

インターネットを介して接続可能なシステムを構築する場合、サーバへの通信を適切に制御することが必要となる。本事業で利用した仮想サーバの通信制御ルールは以下の通りである。

Cloudn は仮想サーバへセキュリティグループ（SG）を適用することで、仮想サーバへのアクセス制御を行うことが可能となる。同じセキュリティグループが適用 された仮想サーバは、同一のアクセス制御（フィルタルール）が適用されるため、グループ単位でまとめて管理することができる。

セキュリティグループの適用方法は、「Cloudn Compute FLAT タイプ 操作マニュアル 6.1.

セキュリティグループを設定する」に記載がある。

なお、初期状態においては「受信」は全て「禁止」、「送信」は全て「許可」となっているため、下表には許可した「受信」、禁止した「送信」を記載している。

表 4-2　許可した仮想サーバの受信

サーバ名	プロトコル	開始ポート	終了ポート	CIDER
マイポータル（SP）	TCP	22	22	0.0.0.0/0
マイポータル（SP）	TCP	80	80	0.0.0.0/0
マイポータル（SP）	TCP	443	443	0.0.0.0/0
マイポータル（SP）	TCP	8443	8443	0.0.0.0/0
マイポータル（SP）	TCP	5902	5902	0.0.0.0/0
リバプロ SP	TCP	22	22	0.0.0.0/0
リバプロ SP	TCP	80	80	0.0.0.0/0
リバプロ SP	TCP	443	443	0.0.0.0/0
リバプロ SP	TCP	8443	8443	0.0.0.0/0
リバプロ SP	TCP	5902	5902	0.0.0.0/0
PDS	TCP	22	22	0.0.0.0/0

表 4-3　禁止した仮想サーバからの送信

サーバ名	プロトコル	開始ポート	終了ポート	CIDER
PDS	TCP	80	80	0.0.0.0/0
PDS	TCP	443	443	0.0.0.0/0
共通 I/F MBaaS+オーサリングツール(SP)	TCP	22	22	0.0.0.0/0
共通 I/F MBaaS+オーサリングツール(SP)	TCP	80	80	0.0.0.0/0
共通 I/F MBaaS+オーサリングツール(SP)	TCP	443	443	0.0.0.0/0
共通 I/F MBaaS+オーサリングツール(SP)	TCP	8443	8443	0.0.0.0/0
共通 I/F MBaaS+オーサリングツール(SP)	TCP	5902	5902	0.0.0.0/0

4.4仮想サーバへのバックアップについて

サーバのバックアップにはバックアップ用のソフトウェアを用いることが一般的であるが、クラウドサービスの付加機能を利用することで簡易に取得することが可能である。本事業では、

クラウドサービスの付加機能を利用し、ルートディスク（OS が格納されているディスク領域）、データディスク（データ格納されているディスク領域）それぞれのバックアップを取得した。

Cloudn はルートディスク用にはスナップショット、データディスク用には Backup Advanced という付加サービスを提供しており、本事業でもこれを利用した。

それぞれ、「Cloudn Compute FLAT タイプ 操作マニュアル 5.1. スナップショットを作成する」、「Cloudn ComputeBackup Advanced 操作マニュアル」に詳細な操作手順が記載されている。

なお、取得したスナップショットからは仮想サーバのテンプレートを作成することができる。テンプレートを利用すれば、同様のサーバを簡単にクローニングすることができ、効率的に仮想サーバを作成することが可能である。テンプレート作成の方法、テンプレートから仮想する方法は、「Cloudn Compute FLAT タイプ 操作マニュアル 5.4. スナップショットからテンプレートを作成する」、「Cloudn Compute FLAT タイプ 操作マニュアル 3.1. 仮想サーバを作成する」に記載されている。

4.5DNS サーバの構築について

クラウドサービスを利用し、システムを構築する場合は、仮想サーバを作成した後に必要となるミドルウェアやソフトウェアをインストールすることが一般的である。ただし、DNS サーバのように汎用的なものに関しては、それ自体が付加機能として提供されているケースも珍しくない。その場合は GUI からの操作のみなど、簡易な手段で臨む機能が利用可能となる。

本事業の DNS サーバも Cloudn の付加機能として提供されている DNS を利用している。詳細な操作手順は、「Cloudn Compute FLAT タイプ 操作マニュアル Cloudn DNS 操作マニュアル」に記載がある。

5.SP サーバ構築手順

5.1本項の概要

本章では、サービスプロバイダー（SP）のモジュールとして Shibboleth SP を利用した SP サーバの構築手順について記述する。

Shibboleth モジュールは、米国 Internet2 が開発、提供しているオープンソースであり、認証･認可に関する世界標準である SAML2.0 に対応した SP サーバの機能を提供する。国内では、国立情報学研究所[1]が構築、運用する学術認証フェデレーション[2]（以下、“学認”）において、Shibboleth モジュールが広く利用されており、学認のサイトから技術ガイド[3]やドキュメントといった様々な関連情報が提供されている。

本章では、学認の技術ガイドにしたがって SP サーバを構築、設定する手順を中心に記述する。

5.2構築にあたっての前提条件

5.2.1動作環境

Linux が稼働するサーバ、もしくは仮想サーバ。

5.2.2サーバ構成

本手順書では、1 台のサーバ内に Shibboleth SP モジュールと教材コンテンツを入れる構成、および Shibboleth SP モジュールを用いたリバースプロキシーサーバを構築する手順を示す。

5.2.3利用 OS・利用モジュール

本手順書では、下記の OS、パッケージの利用を前提とする。OS、および各パッケージで異なるバージョンを利用する場合は、学認の技術ガイド等を参考に利用するバージョンに合わせた設定とすること。

① CentOS 6.4
② Apache 2.2.15
③ Shibboleth SP 2.5.3

---

[1]大学共同利用期間法人 情報・システム研究機構 国立情報学研究所： http://www.nii.ac.jp/

[2]学術認証フェデレーション： https://www.gakunin.jp/

[3]学認「技術ガイド」： https://www.gakunin.jp/technical/

5.2.4本手順実施にあたり必要となるファイル一覧

本手順の実施にあたり必要となるファイルを以下に示す。

SP 設定ファイル

- shibboleth2.xml
- attribute-map.xml
- attribute-policy.xml

エンティティ・認証メタデータテンプレート

- sp-metadata-template.xml

5.3SP サーバ構築手順

学認の技術ガイドを参考に、Shibboleth SP のインストールおよび設定を行う。

5.3.1SP インストール

学認の技術ガイド「貴学にて SP をインストールする場合の構築手順」[4]を参考にして、下記をインストールする。

① CentOS

Apache のデフォルト設定では http、https の両方が動作する設定となっている。コンテンツの構成や扱う情報にも依存するが、セキュリティを考慮して http を停止して https のみを利用する設定を推奨する。

② Shibboleth SP

5.3.2SP 設定①

下記のインストールされている設定ファイルを、教育クラウドプラットフォーム構築用の設定ファイル（別途配布）に置換える。

① shibboleth2.xml

（/etc/shibboleth/shibboleth2.xml を置換える）

置換えた後、ホスト名を記入する。（１か所）

shibboleth2.xml の“[HOST_NAME]”部分を、SP サーバのホスト名に変更する。

② attribute-map.xml

（/etc/shibboleth/attribute-map.xml を置換える）

---

[4] 「貴学にて SP をインストールする場合の構築手順」：
https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=12158264

③ attribute-policy.xml
（/etc/shibboleth/attribute-policy.xml を置換える）

5.3.3SP 設定②

下記の証明書設定を実施する。

① サーバ証明書
パブリック証明書を用意（購入）して、ssl.conf に設定する。

② 認証メタデータ署名証明書
認証メタデータ署名証明書”jsfed-signer-2015.pem”を、DS 管理者（トラストフレームワーク管理機関）から入手し、フィンガープリントが下記と一致することを確認する。
E9:63:2F:6B:84:1A:B1:5A:2C:34:06:DE:D2:3B:E0:95:DC:AA:CC:01
(SHA-1 フィンガープリント)
確認した証明書を下記に設置する。
/etc/shibboleth/cert/jsfed-signer-2015.pem

5.3.4エンティティ・認証メタデータの作成

教育クラウドプラットフォーム構築用設定ファイル（別途配布）の、エンティティ認証メタデータ・テンプレートファイル（”sp-metadata-template.xml”）に対して、下記の手順を実施し、エンティティ認証メタデータを作成する。

① shibboleth 用証明書の記載（１か所）
sp-metadata-template.xml の“[CERTIFICATE]”を/etc/shibboleth/sp-cert.pem ファイルの中身に書き換える。ただし、sp-cert.pem の中身の----で始まる行（最初と最後の行）は含めない。

② ホスト名の記入（５か所）
sp-metadata-template.xml の“[HOST_NAME]”部分を、SP サーバのホスト名に変更する。

③ 提出
作成したエンティティ・認証メタデータを DS 管理者（トラストフレームワーク管理機関）に提出する。

5.4SP サーバ運用手順

5.4.1Shibboleth 認証を行うロケーションの設定

デフォルト設定では、/secure へのアクセス時に Shibboleth 認証が行われる。
教材コンテンツが html5 の場合、“<ドキュメントルート>/secure”の配下にコンテンツを配置することで Shibboleth 認証による教育コンテンツへのアクセスを行う SP サーバとなる。

このロケーションを変更するには、/etc/httpd/conf.d/shib.conf 内の<Location /secure>を修正する。

ロケーションの設定変更以外、Shibboleth 認証で送受信する属性の利用やセッション連携等、コンテンツと Shibboleth の連携設定に関する詳細は学認の技術ガイドを参照すること。

5.4.2学校の認可設定

利用ライセンスを保有する学校のみが教育コンテンツにアクセス可能となるよう設定を行う。

SP の設定ファイル shib.conf に、各学校の学校名（ローマ字）=”o”を記述する。

/etc/httpd/conf.d/shib.conf の<Location /secure>中に下記の通り記述する。

設定例：

＜３つの学校 “o”=”School1”, “o”=”School2”, “o”=”School3”をアクセス許可とする場合>

```
----------------------------------------
<Location /secure>
  AuthType shibboleth
  ShibCompatWith24 On
  ShibRequestSetting requireSession 1
  require o School1 School2 School3      ← “require o”の後に学校名（ローマ字）を記述する。
  require shib-session
</Location>
----------------------------------------
```

5.5リバースプロキシ設定手順

既存のコンテンツサーバを利用するが、Shibboleth SP モジュールをインストールできない等、Shibboleth SP のリバースプロキシをコンテンツサーバのフロントに設置する構成が考えられる。以下では、１～４で構築した SP サーバをリバースプロキシとして設定する方法を記述する。

5.5.1Apache の設定変更

Apache の httpd.conf にリバースプロキシーの設定を追記する。

既存のコンテンツサーバの URL が https://edu-example.org/ とした場合、以下を /etc/httpd/conf/httpd.conf に追記する。

```
----------------------------------------------------------
ProxyPass / https://edu-example.org/
ProxyPassReverse / https://edu-example.org/
----------------------------------------------------------
```

5.5.2Shibboleth の設定変更

教材コンテンツで、Shibboleth の属性を利用する場合、下記の設定により Shibboleth SP が IdP サーバ、および AtrP サーバから受信した属性をヘッダーで教材コンテンツに渡す設定が必要となる。このため、shib.conf に”ShibUseHeaders On”の設定を追記する。

設定例：

```
----------------------------------------
<Location /secure>
  AuthType shibboleth
  ShibCompatWith24 On
  ShibRequestSetting requireSession 1
  ShibUseHeaders On                    ← “ShibUseHeaders On”を追記します。
  require shib-session
</Location>
----------------------------------------
```

6.IdP サーバ・AtrP サーバ構築手順

6.1本項の概要

本章では、ID プロバイダー（IdP）、および属性プロバイダー（AtrP）のモジュールとして Shibboleth IdP を利用した IdP サーバ､および AtrP サーバの構築手順について記述している。

Shibboleth モジュールは、米国 Internet2 が開発、提供しているオープンソースであり、認証・認可に関する世界標準である SAML2.0 に対応した IdP サーバ、および AtrP サーバの機能を提供する。

国内では、国立情報学研究所が構築、運用する学術認証フェデレーション （以下、“学認”）において、Shibboleth モジュールが広く利用されており、学認のサイトから技術ガイドやドキュメントといった様々な関連情報が提供されている。

本章では、学認の技術ガイドにしたがい、IdP サーバおよび AtrP サーバの設定手順を中心に記述する。

6.2前提条件

6.2.1動作環境

Linux が稼働するサーバ、もしくは仮想サーバ。

6.2.2サーバ構成

本手順書では、学認の技術ガイドによるサーバ構成と同様、 1 台のサーバ内に IdP と IdP 用 LDAP、もしくは AtrP と AtrP 用 LDAP を構築する手順を示す。

ただし、運用にあたっては、LDAP サーバを別に構築して、TRUST セグメントに設置し、IdP サーバ、もしくは AtrP サーバを DMZ セグメントに設置する等、セキュリティを考慮した構成とすることを推奨する。

6.2.3利用 OS、利用モジュール

本手順書では、下記の OS、パッケージの利用を前提とする。OS、および各パッケージで異なるバージョンを利用する場合は、学認の技術ガイド等を参考に利用するバージョンに合わせた設定とすること。

① CentOS 6.4
② Apache 2.2.15
③ Tomcat 8.0.15
④ JDK 1.7
⑤ OpenLDAP 2.4

⑥ Shibboleth IdP 2.4.2

6.2.4本手順実施にあたり必要となるファイル

IdP 属性設定ファイル

- attribute-filter.xml
- attribute-resolver.xml

AtrP 属性設定ファイル

- attribute-filter.xml
- attribute-resolver.xml

エンティティ・認証メタデータテンプレート

- idpatrp-metadata-xml201xxx.txt

スキーマ

- eduperson.schema
- edumember.schema
- gakunin.schema
- jsfedperson.schema

テストデータ作成ファイル

- idp-test.ldif
- atrp-test.ldif

6.3IdP サーバの構築

学認の技術ガイドを参考に、IdP と IdP 用 LDAP をインストールし、設定する。

6.3.1IdP インストール

学認の技術ガイド「旧：貴学にて IdP をインストールする場合の構築手順」[5]を参考にして、下記をインストールする。

① CentOS （OpenLDAP 含む）
② jdk、tomcat
③ Shibboleth IdP

[5]「旧：貴学にて IdP をインストールする場合の構築手順」：
https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=12158257

6.3.2IdP 設定①

学認の技術ガイド「旧：IdP セッティング」[6]を参考にして、下記を設定します。

① handler.xml
② login.config

6.3.3IdP 設定②

下記のインストールされている設定ファイルを教育クラウドプラットフォーム構築用設定ファイル（別途配布）に置換える。

① attribute-resolver.xml
（/opt/shibboleth-idp/conf/attribute-resolver.xml を置換える）
② attribute-filter.xml
（/opt/shibboleth-idp/conf/attribute-filter.xml を置換える）
③ logout.jsp
（/usr/java/tomcat/webapps/idp/logout.jsp を置換える）

6.3.4IdP 設定③

下記の証明書設定を行います。

① サーバ証明書
パブリック証明書を用意（購入）して、ssl.conf に設定する。
② 認証メタデータ署名証明書
認証メタデータ署名証明書”jsfed-signer-2015.pem”を、DS 管理者（トラストフレームワーク管理機関）から入手する。
フィンガープリントが下記と一致することを確認する。
E9:63:2F:6B:84:1A:B1:5A:2C:34:06:DE:D2:3B:E0:95:DC:AA:CC:01
(SHA-1 フィンガープリント)
確認した証明書を下記に設置する。
/opt/shibboleth-idp/credentials/jsfed-signer-2015.pem

6.3.5エンティティ・認証メタデータの作成(IdP)

教育クラウド用設定ファイル（別途配布）の、エンティティ認証メタデータ・テンプレート

---

[6]「旧：IdP セッティング」：
https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=12158259

ファイル（”idpatrp-metadata-template201xxx.xml”）に対して、下記の作業を実施し、エンティティ認証メタデータを作成する。

① shibboleth 用証明書の記載（２か所）

entity-metadata-template.xml の“[CERTIFICATE]”をインストールディレクトリの credentials/idp.crt ファイルの中身に書き換える。ただし、idp.crt の中身の----で始まる行（最初と最後の行）は含めない。

② ホスト名の記入（９か所）

entity-metadata-template.xml の“[HOST_NAME]”部分を、IdP サーバのホスト名に変更する。

③ セキュリティスコープの記入（２か所）

entity-metadata-template.xml の“[SECURITY_SCOPE]”部分を、IdP サーバのドメインに変更する。

④ 提出

作成したエンティティ・認証メタデータを DS 管理者（トラストフレームワーク管理機関）に提出する。

6.4IdP 用 LDAP サーバの構築

本手順書では、IdP サーバに CentOS インストール時にインストールされる OpenLDAP を設定して利用する手順を記述します。

学認の技術ガイド「OpenLDAP の設定」[7]を参考にして、下記を設定します。

6.4.1デフォルト設定

LDAP サーバのデフォルト設定を実施する。スキーマは下記の通り追加登録を行う。

・ 教育クラウドの追加スキーマについて：

教育クラウドの IdP 用 LDAP では、３つの追加スキーマを利用する。

学認の技術ガイドでは、「eduPerson スキーマ」の追加方法が記載されているため、同様に、下記２つを追加登録する。

・Gakunin スキーマ

学認の技術ガイド「属性リスト」[8]からダウンロードする。

・教育クラウドのスキーマ

---

[7]「OpenLDAP の設定」：
https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=12158408

[8]「属性リスト」： https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=12158166

教育クラウドプラットフォーム構築用設定ファイル（別途配布）の”jsfedperson.schema”

6.4.2テストデータ作成

教育クラウド用設定ファイル(別途配布)の”idp-test.ldif”を利用してテスト用データを LDAP へ登録する。

6.5AtrP サーバの構築

AtrP サーバの構築では、まず「6.3 IdP サーバの構築」にしたがって IdP サーバを構築する。この IdP サーバに対して下記の追加設定を行うことで AtrP サーバの構築が完了となる。

6.5.1IdP サーバ構築時の利用ファイル

「6.3.3. IdP 設定②」で利用する下記のファイルは、AtrP 用を利用する。

① attribute-resolver.xml
② attribute-filter.xml

6.5.2Back-Channel（SOAP）通信の設定

学認の技術ガイド「Back-Channel の設定」[9]を参考にして、設定を実施する。

6.6AtrP 用 LDAP サーバの構築

本手順書では、AtrP サーバに CentOS インストール時にインストールされる OpenLDAP を設定して利用する手順を記述する。
学認の技術ガイド「OpenLDAP の設定」を参考にして、下記の設定を実施する。

6.6.1デフォルト設定

LDAP サーバのデフォルト設定を実施する。スキーマは下記の通り追加登録を行う。

- 教育クラウドの追加スキーマについて：
  教育クラウドの IdP 用 LDAP では、４つの追加スキーマを利用する。
  学認の技術ガイドでは、「eduPerson スキーマ」の追加方法が記載されているため、

[9]「Back-Channel の設定」：
https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=12158421#id-サーバ証明書の設定(IdP)-back-channel

同様に、下記 3 つを追加登録する。

・eduMember スキーマ、Gakunin スキーマ：

学認の技術ガイド「属性リスト」 からダウンロードする。

・教育クラウドのスキーマ

教育クラウドプラットフォーム構築用設定ファイル（別途配布）の”jsfedperson.schema”

6.6.2テストデータ作成

教育クラウド用設定ファイル（別途配布）の”atrp-test.ldif”を利用してテスト用データを LDAP へ登録する。

6.7IdP サーバの運用（ライセンス属性出力の設定）

ライセンス属性 “jsFedLicense”は、学校がライセンスを所有する教材コンテンツのコンテンツ UUID を示します。このライセンス属性は、マイポータルにおいて教材コンテンツのアイコン表示／非表示の制御等で利用される。

この設定は、IdP の設定ファイルである attribute-resolver.xml に対して実施する。

コンテンツ UUID については、コンテンツメタデータを参照すること。

/opt/shibboleth/conf/attribute-resolver.xml の、

<resolver:AttributeDefinition xsi:type="ad:Script" id="jsFedLicense" sourceAttributeID="jsFedLicense">において、下記の通り設定する。

設定例： ＜教材コンテンツのライセンスを 3 つ保有する場合＞

```
            if ("test_o".equals(o.getValues().get(0))) {
jsFedLicense.getValues().add("cab817d6-83dd-4842-bc87-7c8fc650399a");
jsFedLicense.getValues().add("ab42b863-3b89-4ca0-b883-fe96a5c985be");
jsFedLicense.getValues().add("ae00b375-4468-4760-8732-30fd5df0171e");
            }
          ]]></ad:Script>
```

平成 27 年度クラウド等の最先端情報通信技術を活用した学習・教育モデルに関する実証別冊

コンテンツ作成ガイドブック

平成 28 年 3 月 31 日

NTT コミュニケーションズ株式会社

目次

1.はじめに

平成 27 年度「クラウド等の最先端情報通信技術を活用した学習・教育モデルに関する実証」では、教育クラウドプラットフォームを構築し、児童生徒がいつでも・どこでも学べる環境に関する実証を行った。この教育クラウドプラットフォームで提供する教材コンテンツはすべて HTML5 形式とすることにより、特定の OS やブラウザに依存することなく、幅広く利用できる環境を目指している。

本書は、HTML5 による教材コンテンツを開発し提供する事業者（以下、コンテンツプロバイダ）向けの「コンテンツ作成ガイドブック」である。

2.ガイドブックの目的及び概要

2.1ガイドブックの目的

本ガイドブックは、教材コンテンツを提供するコンテンツプロバイダに対し、その意義やメリットを説明するとともに、教材コンテンツを HTML5 化するにあたって考慮すべきポイントを提示することにより、多くの教材コンテンツが HTML5 形式で提供され、学習者や教員に多くの選択肢を提供できるようにすることを目的としている。

2.2教育クラウドプラットフォームの概要

教育クラウドプラットフォームの概要を図 2-1 に示す。

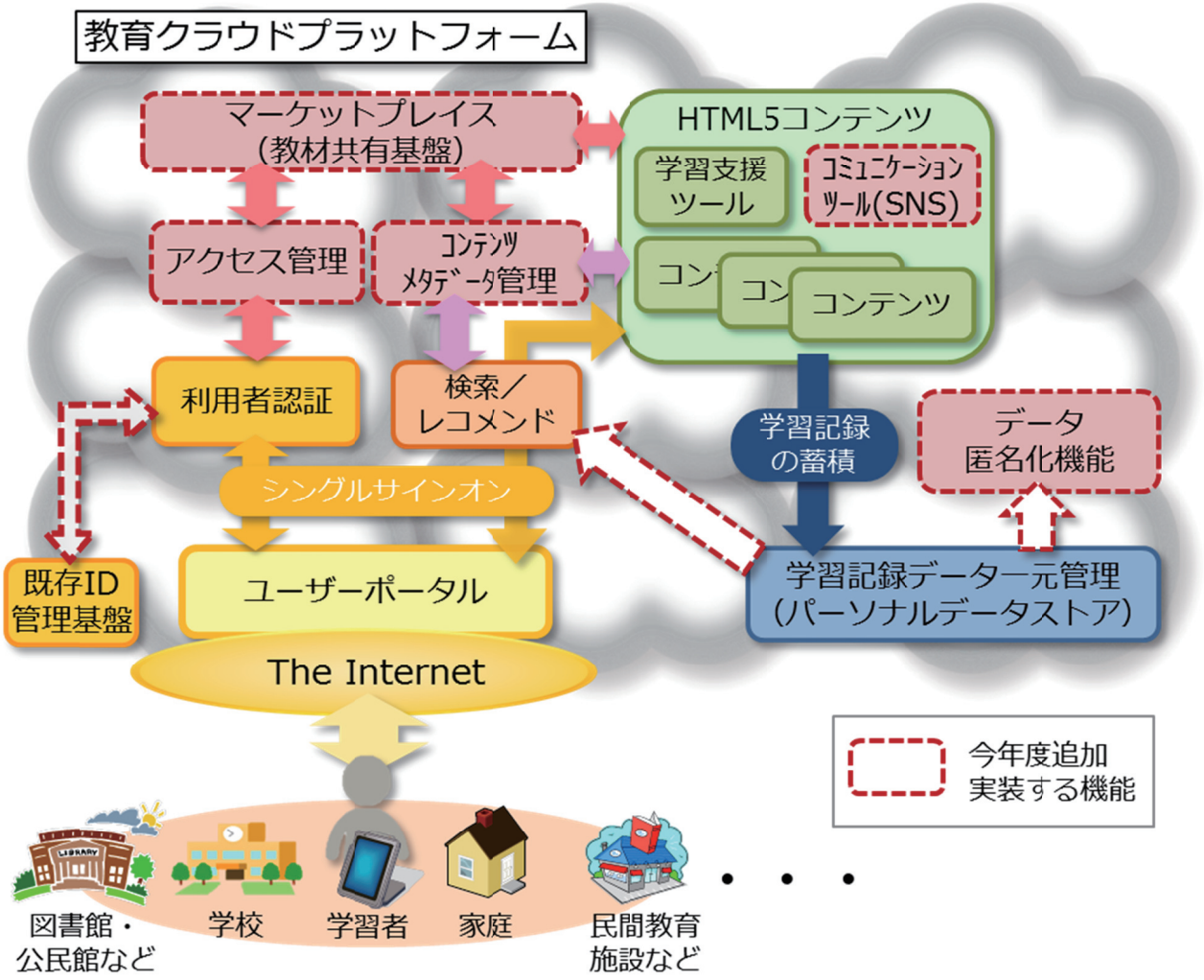


図 2-1　教育クラウドプラットフォームの概要

教育クラウドプラットフォームは、児童生徒や教員など教材コンテンツの利用者に対して、シングルサインオンの機能を提供している。一度教育クラウドプラットフォームにログインしてしまえば、その後は教材コンテンツ個別の ID・パスワードを入力することなく、様々な教材コンテンツが利用できる仕組みを整えている。そのため、コンテンツプロバイダはこの教育ク

ラウドプラットフォームと連携することにより、多くの児童生徒や教員による利用を見込むことが可能となる。

教育クラウドプラットフォームにおける教材コンテンツは主にタブレットなどの端末から利用されることを想定しているが、タブレット端末には iOS・Android・Windows など様々な OS や、それに付随するブラウザが存在する。学校における機器配備状況によって使用される OS やブラウザは異なり、そのバージョンの違いも含めて組み合わせを考えると多くのパターンが考えられる。そのため、各 OS に特化したネイティブアプリケーションの形式で教材コンテンツを作成してしまうと、その教材コンテンツを使える学校とそうでない学校とが出てきてしまい、汎用性に欠ける可能性がある。

そこで、教育クラウドプラットフォームで扱う教材コンテンツはすべて HTML5 形式としている。HTML5 形式とすることにより、以下のようなメリットを享受することが可能となる。

- 複数の OS やブラウザで利用できる
- 利用にあたり特別なプラグインを必要としない
- 音声や動画などマルチメディアコンテンツを扱うことができる
- オブジェクトの移動や描画などの表現ができ、インタラクティブな教材コンテンツを作りやすい

しかしながら、教材コンテンツを HTML5 化することによって上記のようなメリットを無条件に享受できるわけではなく、いくつかの注意点がある。そこで本ガイドブックでは、コンテンツプロバイダが新たに HTML5 による教材コンテンツを作成する上で課題となりやすいポイントについて、簡単な補足情報を提供する。

3.HTML5 による教材コンテンツ作成にあたって考慮すべきポイント

3.1OS の違いによる教材コンテンツの開発手法の違い

静的なコンテンツであれば HTML5 による開発はさほど難しくはないが、教材コンテンツはマウスやキーボードの利用によるインタラクティブなものが多く、動的なコンテンツが中心となる。それらのアクションを検知し制御するためには、単純な HTML5 だけでは十分でなく Java Script による開発を伴うのだが、この Java Script の部分が OS やブラウザに依存してしまう。使用できる関数に差があるなどの理由から、スクリプトの記述方法が異なるため、ブラウザを検出し、それぞれに対応できるプログラムを選択する必要がある。ブラウザによって CSS などのソースの解釈も多少異なるため、その挙動の差異をコンテンツ側で吸収できるように設計・開発しなければならない。つまり、単純に HTML5 で教材コンテンツを開発したとしても、マルチ OS・マルチブラウザに対応できるということではない点に留意する必要がある。

さらに、タブレット端末によってはタッチパネルによる操作と、マウス・キーボードによる操作の両方が行われる可能性がある。iPad の場合はタッチパネルのみを想定すればよいが、Windows のタブレット端末の場合は両方がありうる。マルチ OS・マルチブラウザに対応させる場合、教材コンテンツ側はタッチパネルとマウス・キーボードの両方を想定して開発を行わなければならない。

このように、HTML5 により多様なブラウザ・OS に対応できるようになる一方で、細かな部分では差がある。今後、HTML5 の更なる普及により改善される可能性はあるが、現状ではこれらの違いをコンテンツプロバイダ側にて吸収しなければならない。

OS・ブラウザ等の違いを吸収する作業で有用となる 2 つのサイト

- Can I use... (http://caniuse.com/)

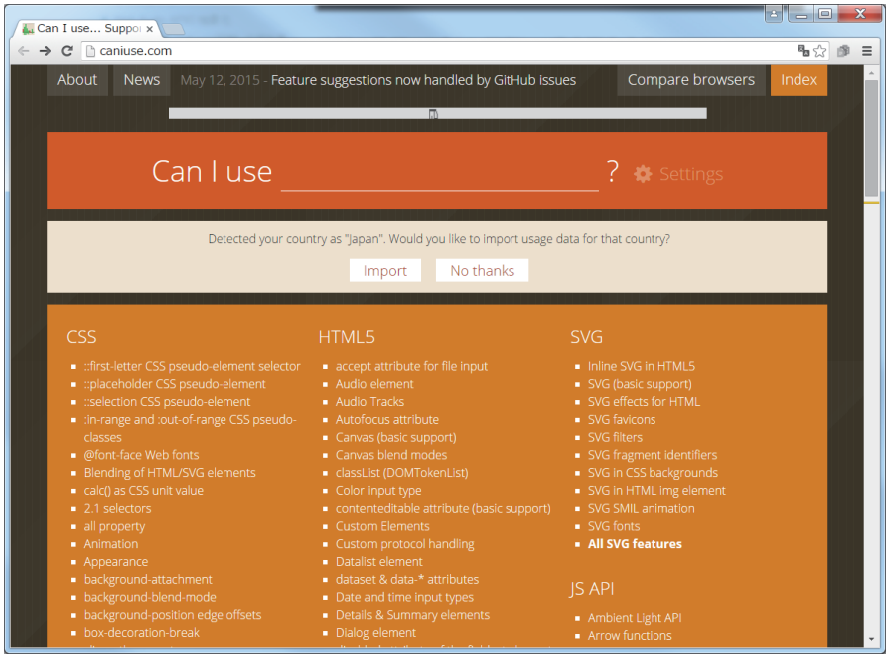


図 3-1　Web サイト「Can I use...」のトップページ

図 3-1 に示す Web サイトでは、HTML5 や Java Script の各種機能が、多様な Web ブラウザでどのようにサポートされているかを確認することができる。使用したい機能を一覧から選択することも、画面上部の検索窓に入力して探すことも可能である。

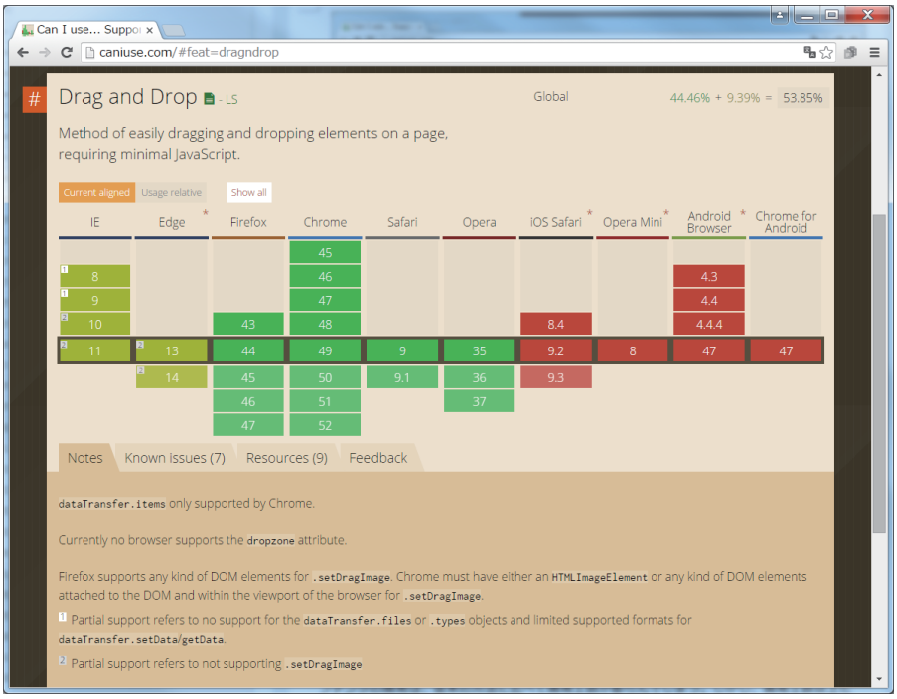


図 3-2　Drag and Drop 機能の対応状況

図 3-2 は、教材コンテンツでも利用があると思われる Drag and Drop 機能の対応状況を

示した画面である。ブラウザごとに対応状況が色分けして示されている。緑色で表示されている Firefox, Chrome, Safari, Opera では対応しているが、黄緑色で表示されている IE, Edge については一部の要素に制限があることを示している。iOS Safari, Opera Mini, Android Browser, Chrome for Android については赤色で表示されており、Drag and Drop 機能が対応していないことがわかる。

このサイトでは、各機能の利用に当たってポイントとなる機知の情報（Known Issue）や、参考になる情報のソース（Resources）なども併せて提示してくれる。HTML5 コンテンツを開発する上での参考となるだろう。

- Mobile HTML5 (http://mobilehtml5.org/)

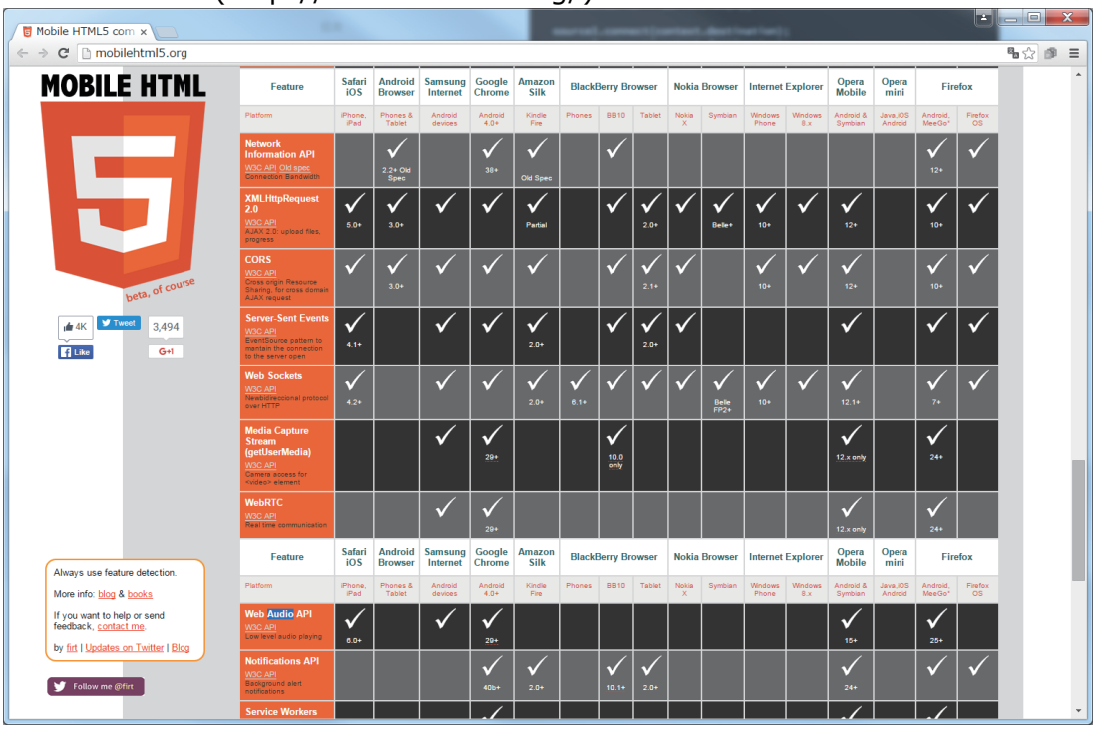


図 3-3　Web サイト「Mobile HTML5」のトップページ

図 3-3 は、モバイル端末にフォーカスして HTML5 機能のサポート状況を整理した Web サイトである。教育用教材に特化しているわけではないため、教育現場では使用されない端末なども含まれているが、高い一覧性が確保されている。この表からも、サポートされている比率の高い機能もあれば、そうでない機能もあることがわかる。

3.2対象とする OS・ブラウザの多様性による検証工数の増加

教材コンテンツを HTML5 で開発する上で、検証のための工数を考慮しておく必要がある。教材コンテンツをマルチ OS・マルチブラウザ対応とすることにより、対象としなければならない OS 及びブラウザのバージョンの種類が増大する。その組み合わせの分だけ動作環境のパターンが存在するため、教材コンテンツを提供するコンテンツプロバイダがすべてのパターンを網羅して検証することを想定すると、単一プラットフォームへの対応の場合と比べて、検証工数が膨大となってしまう。

その状況に拍車をかける要因として、セキュリティ対策や不具合修正のため、近年の OS やブラウザが頻繁にアップデートされることが挙げられる。マイナーバージョンも含めてすべての機能を厳密に検証しようとすると工数はさらに膨らむことになる。

3.3HTML5 コンテンツの開発生産性

Web ブラウザにおけるリッチなアプリケーションを提供する HTML5 以外の技術として Adobe Flash が挙げられる。Adobe Flash は開発ツールが充実しているが、HTML5 はまだ整備が十分でなく、開発生産性はまだ低いと言わざるを得ないとの指摘がある。Flash は iOS に対応していないため HTML5 での実装が必要となるが、途中まで Flash で作成し、HTML5 に変換するというプロセスを経ているコンテンツプロバイダも存在する。

このように HTML5 での開発環境が整っていない状況は HTML5 普及の過渡期としての問題ともいえるが、限られた予算や人員の中で効率的・効果的に教材コンテンツを開発しなければならないコンテンツプロバイダとしては非常に重要な要素と言えるだろう。

3.4HTML5 が利用可能な環境の制約

HTML5 は比較的新しい規格であり、古いバージョンのブラウザでは動作しない。学校現場にはまだ古い端末が数多く残っており、それらもサポート対象とする場合は HTML5 を規格として採用することがそもそも不可能である。Safari や Chrome などのブラウザは自動アップデートが行われるが、Internet Explorer の場合は古いバージョンのまま取り残されている端末も存在すると想定される。

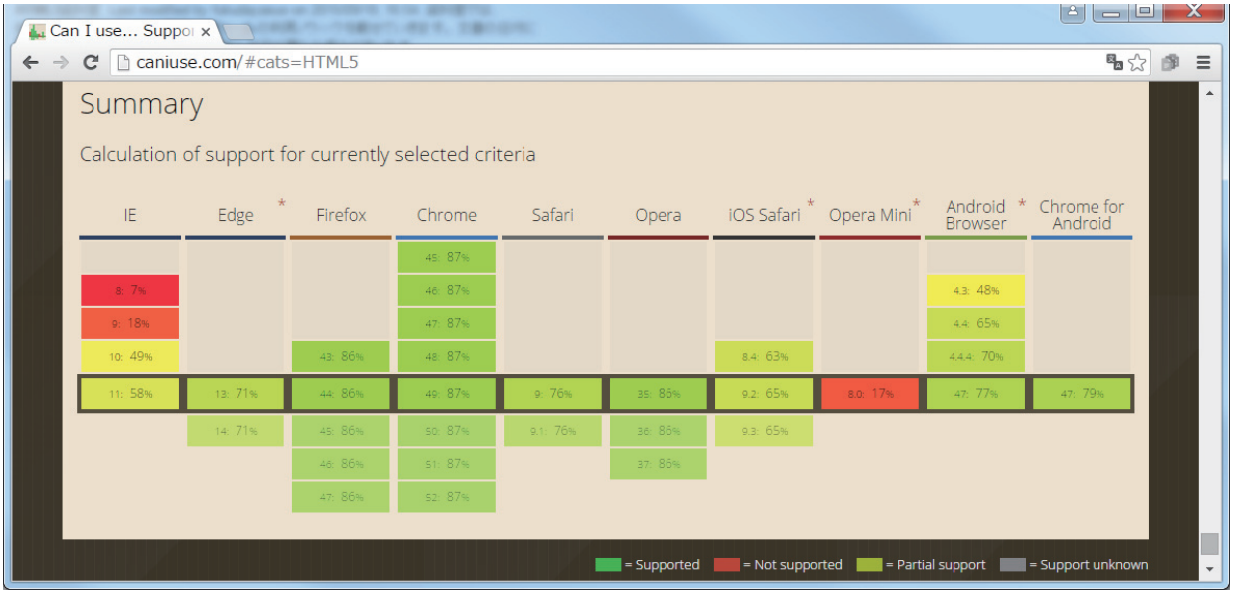


図 3-4　HTML5 全機能の対応状況

図 3-4 は 3.1 で紹介した「Can I Use...」という Web サイトにおける、HTML5 全機能のブラウザごとの対応状況を示している。HTML5 の機能といっても複数あり、それぞれによってブラウザの対応状況が異なるため、網羅率をパーセンテージで表記している。

この図には IE7 はすでに表示対象から外れており、IE8 は 7%、IE9 は 18%しか HTML5 の機能をサポートしていないことがわかる。ブラウザによって HTML5 の扱いの得意、不得意があるのは否めないが、少なくとも古いバージョンのブラウザでは、HTML5 による表現に多くの制限が課せられることは明らかである。

平成 27 年度クラウド等の最先端情報通信技術を活用した学習・教育モデルに関する実証別冊

アクセシビリティガイドブック

平成 28 年 3 月 31 日

NTT コミュニケーションズ株式会社

目次

1.アクセシビリティガイドブックの概要

1.1.ガイドブックの目的

平成 25 年 6 月に閣議決定された日本再興戦略では、2010 年代中に 1 人 1 台の情報端末による教育の本格展開に向けた方策を整理し、推進することを掲げている。同じく閣議決定された世界最先端 IT 国家創造宣言においても、2010 年代中にはすべての小学校、中学校、高等学校、特別支援学校で教育環境の IT 化を実現するとともに、学校と家庭がシームレスでつながる学習・教育環境を構築することが明記されている。

本ガイドブックは、身体的な障害や発達障害によって、教育を受けるうえで様々な困難があり、特別な支援が必要な児童・生徒に対し、ICT を効果的に利活用することで、学習効果をあげ、児童・生徒の可能性を拡げることを目指し、上記の目的を達成するために考慮すべき内容をまとめたものである。

1.2.ガイドブックの構成

本ガイドブックは、アクセシブルな教材制作において留意すべき事項として、W3C で規定されている Web Contents Accessibility Guideline 2.0 をベースに、教育用コンテンツを特別な支援が必要な児童・生徒にも利用可能にするための要件を検討したものである。

ガイドブックの構成は以下のとおりである。

2-1.見やすいコンテンツを心がける
2-2.代替テキストを提供する
2-3.音声や映像コンテンツを注意して用いる
2-4.構造化に留意する
2-5.多様な方法でのアクセスを確保する
2-6 その他の留意事項

（アクセシビリティ実装Q＆A）

なお、上記の要件への適合を簡易的にチェックするための、チェックリストを巻末に掲載した。

2.アクセシビリティとして必要な要素

教育コンテンツは、あらゆる人の利用を想定する必要がある。また HTML5 は、アクセシビリティを考慮に入れて設計されているため、適切な実装を行うことで、容易にアクセシブルなコンテンツの制作を行うことが可能である。本章では、アクセシビリティについて、コンテンツ制作において配慮すべき点をまとめた。

2.1.見やすいコンテンツを心がける

2.1.1.色の違いだけで情報を提供しない

- 色を使って情報を伝える際は、その色の違いがわからなくても、同じように情報が伝わるようにしなければならない。(例：「赤い文字部分について回答せよ」は不可)
- グラフを色分けのみで表さず、それぞれの要素をテキストで伝えたり、ドットや格子など模様も用いたりして、色の違いが分からなくても理解できるようにする。

参考ガイドライン（WCAG 2.0）

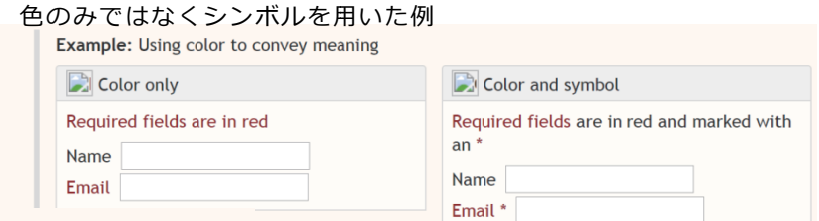
1.4.1 色の使用：情報を伝える、何が起こるかあるいは何が起きたかを示す、利用者の反応を促す、あるいは視覚的な要素を区別する唯一の視覚的な手段として、色のみを使用しない。（レベル A）

色の使用: 達成基準 1.4.1 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/visual-audio-contrast-without-color.html

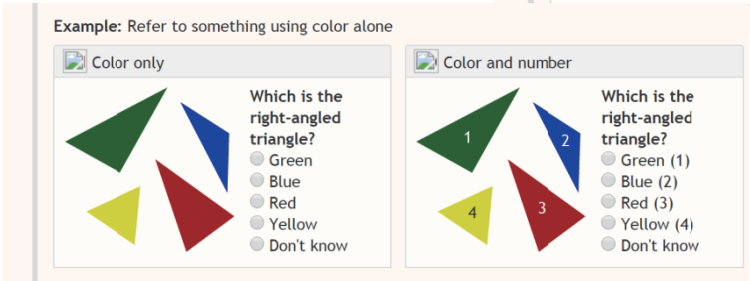
参考情報

色覚障害の方が、区別の困難な色の組み合わせ
http://www.nig.ac.jp/color/gen/index.html2

色のみではなくシンボルを用いた例



色のみではなく数字を用いた例



W3C Home "Tips on Designing for Web Accessibility"より転載
https://www.w3.org/WAI/gettingstarted/tips/designing.html#dont-use-color-alone-to-convey-information

2.1.2.テキストや画像には、少なくとも 4.5：1 のコントラスト比をもたせる

■ 日本語では、22 ポイント以上または 18 ポイント以上の太字は、3:1 以上のコントラスト比を確保すればよい。

参考ガイドライン（WCAG 2.0）

1.4.3 最低限のコントラスト：テキストおよび画像化された文字の視覚的な表現には、少なくとも 4.5：1 のコントラスト比をもたせる。ただし、次の場合は除く：(レベル AA)

- **大きな文字：サイズの大きなテキスト及びサイズの大きな画像化された文字には、少なくとも 3：1 のコントラスト比がある。**
- **付随的：テキスト又は画像化された文字において、次の場合はコントラストの要件は該当しない。アクティブではないユーザインタフェース・コンポーネントの一部である、装飾だけを目的にしている、誰も視覚的に確認できない、又は重要な他の視覚的なコンテンツを含む写真の一部分である。**
- **ロゴタイプ：ロゴ又はブランド名の一部である文字には、コントラストの要件はない。**

最低限のコントラスト: 達成基準 1.4.3 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/visual-audio-contrast-contrast.html

テキストと背景のコントラストの例

Example: Contrast ratio

Insufficient	Sufficient
Some people cannot read text if there is not sufficient contrast between the text and background. For others, bright colors (high luminance) are not readable; they need low luminance.	Some people cannot read text if there is not sufficient contrast between the text and background. For others, bright colors (high luminance) are not readable; they need low luminance.

W3C Home "Tips on Designing for Web Accessibility"より転載
https://www.w3.org/WAI/gettingstarted/tips/designing.html#dont-use-color-alone-to-convey-information

2.1.3.コンテンツの情報や機能を、形や大きさ、視覚的な位置や方向を使って説明する際は、それらの違いがわからなくても、ユーザーが理解できるようにしなければならない

■ 例：「回答を送信するには右の［送信］ボタン、キャンセルするには左の［キャンセル］ボタンを押してください。」は可。「送信するには右のボタン、キャンセルするには左のボタンを押してください」は不可。

参考ガイドライン（WCAG 2.0）

1.3.3 感覚的な特徴：コンテンツを理解し操作するための説明を、形、大きさ、視覚的な位置、方向、または音のような、構成要素が人間の感覚に示す特徴だけで提供しない。（レベル A）

感覚的な特徴: 達成基準 1.3.3 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/content-structure-separation-understanding.html

2.2.代替テキストを提供する

2.2.1.すべての画像などの非テキストコンテンツには、音声などに変換できるように、代替テキストを提供する

- 画像に文字がある場合には、その文字をそのまま代替テキストとして記述する。
- 非テキストコンテンツがイラストの場合、その内容を細かくテキストで表現する必要はなく、簡潔な・画像に文字がある場合には、その文字をそのまま代替テキストとして記述する。
- 非テキストコンテンツがイラストの場合、その内容を細かくテキストで表現する必要はなく、簡潔な説明にする。
  例：「イラスト：がんの群れが空を飛んでいる」
- ボタン等に画像を使用している場合も、ボタンのラベルや機能がわかるように、代替テキストを提供する。
- 映像、アニメーションについても、代替テキストを提供する。
- 非コンテンツテキストが、装飾や見た目の整形のためだけを目的としている場合は、代替テキストを提供する必要はないので、alt 属性を空（alt=””）にする。
- CSS を用いて背景画像として指定する際は、装飾だけを目的にした画像だけにする。

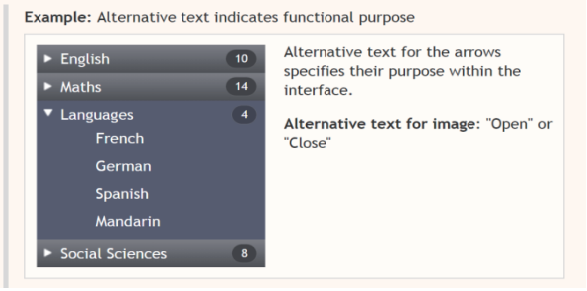
F3: 達成基準 1.1.1 の不適合事例－CSS を用いて、重要な情報を伝える画像を表示させている｜WCAG 2.0 実装方法集
http://waic.jp/docs/WCAG-TECHS/F3.html

- CSS で表示した画像は、Windows のハイコントラストモード（反転表示）では非表示となってしまうため、注意が必要である。

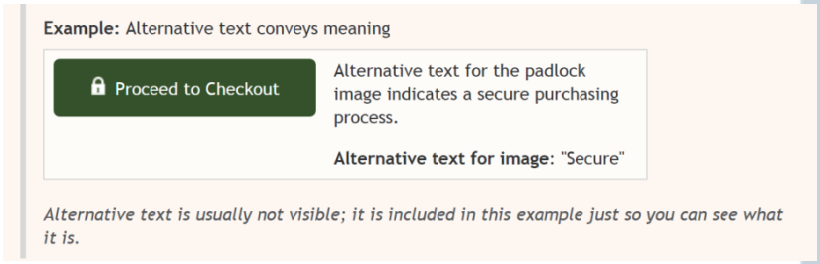
参考ガイドライン（WCAG 2.0）

1.1.1 非テキストコンテンツ：利用者に提示されるすべての非テキストコンテンツには、同等の目的を果たす代替テキストがある。（レベル A）
非テキストコンテンツ: 達成基準 1.1.1 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/text-equiv-all.html

テキスト（数字）で下の階層があることを示した例



セキュリティ保護を示す鍵の画像にテキストを加えた例



W3C Home "Tips on Designing for Web Accessibility"より転載
https://www.w3.org/WAI/gettingstarted/tips/designing.html#dont-use-color-alone-to-convey-information

2.3.音声や映像コンテンツを注意して用いる

2.3.1.映像コンテンツに音声が含まれている場合は、音声の内容をキャプションで提供する

参考ガイドライン（WCAG 2.0）

1.2.2 収録済の音声コンテンツのキャプション:同期したメディアに含まれているすべての収録済の音声コンテンツに対して、キャプションを提供する。ただし、その同期したメディアがテキストの代替メディアであって、代替メディアであることが明確にラベル付けされている場合は除く。（レベル A）

収録済の音声コンテンツのキャプション: 達成基準 1.2.2 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/visual-audio-contrast-contrast.html

2.3.2.映像コンテンツの映像だけで伝えている情報には、音声ガイドか代替コンテンツを提供する

参考ガイドライン（WCAG 2.0）

1.2.1 収録済の音声しか含まないメディア及び収録済の映像しか含まないメディア:収録済の音声しか含まないメディア及び収録済の映像しか含まないメディアは、次の事項を満たしている。ただし、その音声又は映像がテキストの代替メディアであって、代替メディアであることが明確にラベル付けされている場合は除く（レベル A）：

- **収録済の映像しか含まない場合:時間の経過に伴って変化するメディアに対する代替コンテンツ又は音声トラックによって、収録済の映像しか含まないコンテンツと等価な情報を提供している。**

収録済の音声しか含まないメディア及び収録済の映像しか含まないメディア: 達成基準 1.2.1 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/media-equiv-av-only-alt.html

参考ガイドライン（WCAG 2.0）

1.2.3 収録済の映像コンテンツの代替コンテンツ又は音声ガイド: 同期したメディアに含まれている収録済の映像コンテンツに対して、時間の経過に伴って変化するメディアに対する代替コンテンツ又は音声ガイドを提供する。ただし、その同期したメディアがテキストの代替メディアであって、代替メディアであることが明確にラベル付けされている場合は除く。（レベル A）

収録済の映像コンテンツの代替コンテンツ又は音声ガイド: 達成基準 1.2.3 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/media-equiv-audio-desc.html

2.3.3.音声ファイルで伝えている情報には、テキストに書き起こした代替コンテンツを提供する

参考ガイドライン（WCAG 2.0）

1.2.1 収録済の音声しか含まないメディア及び収録済の映像しか含まないメディア:収録済の音声しか含まないメディア及び収録済の映像しか含まないメディアは、次の事項を満たしている。ただし、その音声又は映像がテキストの代替メディアであって、代替メディアであることが明確にラベル付けされている場合は除く（レベル A）：

- **収録済の音声しか含まない場合:時間の経過に伴って変化するメディアに対する代替コンテンツによって、収録済の音声しか含まないコンテンツと等価な情報を提供している。**

収録済の音声しか含まないメディア及び収録済の映像しか含まないメディア: 達成基準 1.2.1 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/media-equiv-av-only-alt.html

2.3.4.効果音の使用にも留意する

■ 例えば、正解・不正解を示す効果音を用いる場合、効果音だけでなく、「正解」「不正解」と画面上にも表示する。

参考ガイドライン（WCAG 2.0）

1.3.3 感覚的な特徴：コンテンツを理解し操作するための説明を、形、大きさ、視覚的な位置、方向、または音のような、構成要素が人間の感覚に示す特徴だけで提供しない。

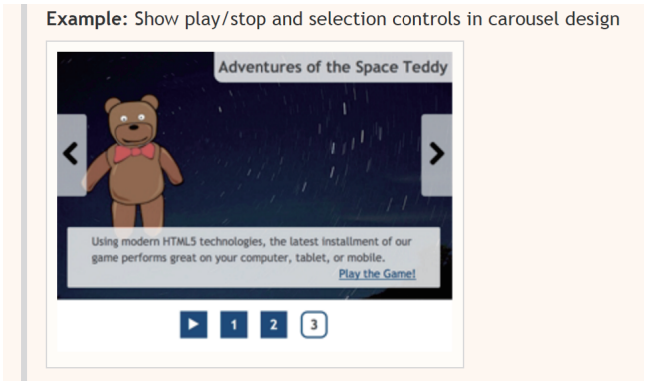
（レベル A）
感覚的な特徴：達成基準 1.3.3 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/content-structure-separation-understanding.html

2.3.5.ページが読み込まれると同時に音声を再生することは避けるか、ユーザーがすぐに一時停止できるようにする。あわせて、音声が再生されていることを画面上で視覚的にわかりやすく示す

参考ガイドライン（WCAG 2.0）

1.4.2 音声制御： ウェブページ上にある音声が自動的に再生され、その音声が 3 秒より長く続く場合、その音声を一時停止又は停止するメカニズム、もしくはシステム全体の音量レベルに影響を与えずに音量レベルを調整できるメカニズムを提供する。（レベル A）
音声制御：達成基準 1.4.2 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/visual-audio-contrast-dis-audio.html

再生／停止と選択の制御を可能にしている例



W3C Home "Tips on Designing for Web Accessibility"より転載
https://www.w3.org/WAI/gettingstarted/tips/designing.html#dont-use-color-alone-to-convey-information

2.3.6.コンテンツが自動的に動作する場合は、5 秒以内に停止させるか、ユーザーが一時停止や停止を行えるようにする

参考ガイドライン（WCAG 2.0）

2.2.1 調整可能な制限時間:コンテンツに制限時間を設定する場合は、次に挙げる事項のうち、少なくとも一つを満たしている：(レベル A)

- 解除：制限時間があるコンテンツを利用する前に、利用者がその制限時間を解除することができる。又は、
- 調整：制限時間があるコンテンツを利用する前に、利用者が少なくともデフォルト設定の 10 倍を超える、大幅な制限時間の調整をすることができる。又は、
- 延長：時間切れになる前に利用者に警告し、かつ少なくとも 20 秒間の猶予をもって、例えば「スペースキーを押す」などの簡単な操作により、利用者が制限時間を少なくとも 10 倍以上延長することができる。又は、
- リアルタイムの例外：リアルタイムのイベント（例えば、オークション）において制限時間が必須の要素で、その制限時間に代わる手段が存在しない。又は、
- 必要不可欠な例外：制限時間が必要不可欠なもので、制限時間を延長することがコンテンツの動作を無効にすることになる。又は、
- 20 時間の例外：制限時間が 20 時間よりも長い。

調整可能な制限時間: 達成基準 2.2.1 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/time-limits-required-behaviors.html

参考ガイドライン（WCAG 2.0）

2.2.2 一時停止、停止、非表示:動きのある、点滅している、スクロールする、又は自動更新する情報に対しては、次のすべての事項を満たしている（レベル A）：

- 動き、点滅、スクロール：動きのある、点滅している、又はスクロールしている情報が、(1) 自動的に開始し、(2) 5 秒よりも長く継続し、そして(3) その他のコンテンツと並行して提示される場合、利用者がそれらを一時停止、停止、又は非表示にすることのできるメカニズムがある。ただし、その動き、点滅、又はスクロールが必要不可欠な動作の一部である場合は除く。
- 自動更新：自動更新する情報が、(1) 自動的に開始し、(2) その他のコンテンツと並行して提示される場合、利用者がそれを一時停止、停止、もしくは非表示にする、又はその更新頻度を調整することのできるメカニズムがある。ただし、その自動更新が必要不可欠な動作の一部である場合は除く。

一時停止、停止、非表示: 達成基準 2.2.2 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/time-limits-pause.html

2.3.7.動画やアニメーションに閃光がある場合は、どの 1 秒間においても 3 回以下とする

参考ガイドライン（WCAG 2.0）
2.3.1 3 回の閃光又は閾値以下:ウェブページにある閃光は、どの 1 秒間においても 3 回以下である、又は一般閃光閾値及び赤色閃光閾値を下回っている。（レベル A） 3 回の閃光又は閾値以下: 達成基準 2.3.1 を理解する｜WCAG 2.0 解説書 http://waic.jp/docs/UNDERSTANDING-WCAG20/seizure-does-not-violate.html

2.4.構造化に留意する

2.4.1.HTML ソースをユーザーエージェントが解釈できるようにコーディングする

■ 仕様で認められている場合を除いて、以下の四点に留意する

- 開始タグと終了タグがある
- 仕様に準じた入れ子になっている
- 同一要素内で属性が重複していない
- ID（id 属性値）がユニークである

参考ガイドライン（WCAG 2.0）

4.1.1 構文解析: マークアップ言語を用いて実装されているコンテンツにおいては、仕様で認められているものを除いて、要素には完全な開始タグ及び終了タグがあり、要素は仕様に準じて入れ子になっていて、要素には重複した属性がなく、どの ID も一意的である。(レベル A)

構文解析: 達成基準 4.1.1 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/ensure-compat-parses.html

2.4.2.そのコンテンツの主たる自然言語を HTML ソースコードで明示する

■ html 要素の lang 属性を用いて、日本語であることを明示する（例：<html lang=”ja”>）

参考ガイドライン（WCAG 2.0）

3.1.1 ページの言語: それぞれのウェブページの主たる自然言語がどの言語であるかを、プログラムが解釈可能である。(レベル A)

ページの言語: 達成基準 3.1.1 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/meaning-doc-lang-id.html

2.4.3.ページの主題が分かるようにページタイトルを記述する

■ できるかぎり同一の教材コンテンツ内ではユニークなページタイトルとし、教材コンテンツ名と併記する。（例：<title>｛ページタイトル｝｜｛教材名｝</title>）

参考ガイドライン（WCAG 2.0）

2.4.2 ページタイトル: ウェブページには、主題又は目的を説明したタイトルがある。(レベル A)

ページタイトル: 達成基準 2.4.2 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/navigation-mechanisms-title.html

2.4.4.画面の領域をセクショニング要素やランドマーク属性を用いてマークアップする

■ 画面の領域を HTML5 の適切なセクショニング要素を用いてマークアップする。（例：<header>, <nav>, <main>, <article>, <footer>）
■ メインコンテンツ領域をマークアップする main 要素には、WAI-ARIA のランドマーク属性 role=”main”を併用する（例：<main role=”main”>｛ここがページのメインコンテンツ部分｝</main>
■ その他、以下のセクショニング要素でも WAI-ARIA のランドマーク属性を併用する。

- ARIA11: Using ARIA landmarks to identify regions of a page｜Techniques for WCAG 2.0
  http://www.w3.org/WAI/GL/WCAG20-TECHS/ARIA11.html（英語）
  ✓ ヘッダー領域：<header role="banner">
  ✓ 検索フォーム：<form role="search">
  ✓ ナビゲーションバー：<nav role="navigation">
  ✓ 補足情報等：<aside role="complementary">
  ✓ フッター領域：<footer role="contentinfo">

- Using WAI-ARIA Landmarks –2013| The Paciello Group Blog
  http://blog.paciellogroup.com/2013/02/using-wai-aria-landmarks-2013/

参考ガイドライン（WCAG 2.0）
2.4.1 ブロック・スキップ: 複数のウェブページ上で繰り返されているコンテンツのブロックをスキップできるメカニズムが利用可能である。(レベル A) ブロック・スキップ: 達成基準 2.4.1 を理解する｜WCAG 2.0 解説書 http://waic.jp/docs/UNDERSTANDING-WCAG20/navigation-mechanisms-skip.html

2.4.5.見出しやリスト、データテーブルは、見た目だけでなく、ソースコードで見出しやリスト、データテーブルの要素を用いてマークアップする

参考ガイドライン（WCAG 2.0）
1.3.1 情報及び関係性: 表現を通じて伝達されている情報、構造、及び関係性は、プログラムが解釈可能である。プログラムが解釈可能にすることができないウェブコンテンツ技術を用いる場合は、それらがテキストで提供されている。(レベル A) 情報及び関係性: 達成基準 1.3.1 を理解する｜WCAG 2.0 解説書 http://waic.jp/docs/UNDERSTANDING-WCAG20/content-structure-separation-programmatic.html

2.4.6.可能なかぎり、リンクテキストだけでリンク先が分かるようにする

- 「こちら」、「ここをクリック」、「一覧」、「詳細」のように、ユーザーがリンク先を特定できないリンクテキストの使用は避ける。

- リンク画像の場合は、alt 属性の代替テキストがリンクテキストとなる（当ガイドライン 2-1.も参照のこと）。

参考ガイドライン（WCAG 2.0）
2.4.4 文脈におけるリンクの目的: それぞれのリンクの目的が、リンクのテキストだけから、又はプログラムが解釈可能なリンクの文脈をリンクのテキストとあわせたものから解釈できる。ただし、リンクの目的が一般的にみて利用者にとって曖昧な場合は除く。(レベル A) 文脈におけるリンクの目的: 達成基準 2.4.4 を理解する｜WCAG 2.0 解説書 http://waic.jp/docs/UNDERSTANDING-WCAG20/navigation-mechanisms-refs.html

2.4.7.テーブルをレイアウトのために使用する際は、スクリーンリーダーで読み上げた際に意図したとおりの意味が通じる順序になるように注意する

参考ガイドライン（WCAG 2.0）
1.3.2 意味のある順序:コンテンツが提供されている順序がその意味に影響を及ぼす場合には、正確な読み上げ順序はプログラムが解釈可能である。(レベル A) 意味のある順序: 達成基準 1.3.2 を理解する｜WCAG 2.0 解説書 http://waic.jp/docs/UNDERSTANDING-WCAG20/content-structure-separation-sequence.html

2.4.8.文字間にスペースや改行が入ることでスクリーンリーダーが一つの単語として認識できなくなるため、見た目の表示のために文字間にスペースや改行を入れたい場合は、CSS を用いて指定する

参考ガイドライン（WCAG 2.0）
1.3.2 意味のある順序:コンテンツが提供されている順序がその意味に影響を及ぼす場合には、正確な読み上げ順序はプログラムが解釈可能である。(レベル A) 意味のある順序: 達成基準 1.3.2 を理解する｜WCAG 2.0 解説書 http://waic.jp/docs/UNDERSTANDING-WCAG20/content-structure-separation-sequence.html

2.5.多様な方法でのアクセスを確保する

2.5.1.ユーザーがコンテンツを利用する際、タッチやマウス以外の、キーボードや外付けスイッチなど複数の方法でのアクセスが可能なようにする

■ リンクやフォームのコントロールは、キーボードの Tab キーでもフォーカスがあたるようにする

- H91：HTML のフォーム・コントロール及びリンクを用いる｜WCAG 2.0 実装方法集
  http://waic.jp/docs/WCAG-TECHS/H91.html

■ マウス対応のイベントハンドラだけでなく、キーボードのイベントハンドラも併用する。

- SCR20: キーボードとその他のデバイス特有の機能を両方とも用いる｜WCAG 2.0 実装方法集
  http://waic.jp/docs/WCAG-TECHS/SCR20.html
- SCR35: アンカー及びボタンの onclick イベントを用いて、アクションをキーボードで操作可能にする｜WCAG 2.0 実装方法集
  http://waic.jp/docs/WCAG-TECHS/SCR35.html

■ ドラッグ＆ドロップ機能についても、キーボード操作を可能にすることができる。

- 9. Drag-and-Drop Support ｜WAI-ARIA 1.0 Authoring Practices
  http://www.w3.org/TR/wai-aria-practices/#dragdrop（英語）
- Drag and Drop Example | Dev.Opera
  http://devfiles.myopera.com/articles/735/example.html

参考ガイドライン（WCAG 2.0）

2.1.1 キーボード操作:コンテンツのすべての機能は、個々のキーストロークに特定のタイミングを要することなく、キーボード・インタフェースを通じて操作可能である。ただし、その根本的な機能が利用者の動作による始点からの終点まで続く一連の軌跡に依存して実現されている場合は除く。(レベル A)

キーボード操作: 達成基準 2.1.1 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/keyboard-operation-keyboard-operable.html

参考ガイドライン（WCAG 2.0）
2.1.2 フォーカス移動:キーボード・インタフェースを用いてキーボード・フォーカスをそのウェブページのあるコンポーネントに移動できる場合、キーボード・インタフェースだけを用いてそのコンポーネントからフォーカスを外すことが可能である。さらに、その操作が修飾キーを伴わない矢印キー、修飾キーを伴わない Tab キー、又はフォーカスを外すその他の標準的な方法で可能な場合を除き、キーボード・フォーカスをそのコンポーネントから外す方法を利用者に知らせる。(レベル A) フォーカス移動: 達成基準 2.1.2 を理解する｜WCAG 2.0 解説書 http://waic.jp/docs/UNDERSTANDING-WCAG20/keyboard-operation-trapping.html

2.5.2.キーボードの Tab キーによるフォーカス移動順序は、ユーザーが予期できるように、画面での表示順序または操作上の論理的な順序と一致するようにする

参考ガイドライン（WCAG 2.0）
2.4.3 フォーカス順序:ウェブページが順番にナビゲートできて、そのナビゲーション順序が意味又は操作に影響を及ぼす場合、フォーカス可能なコンポーネントは意味及び操作性を保持した順序でフォーカスを受け取る。(レベル A) フォーカス順序: 達成基準 2.4.3 を理解する｜WCAG 2.0 解説書 http://waic.jp/docs/UNDERSTANDING-WCAG20/navigation-mechanisms-focus-order.html

2.5.3.フォーカスを受け取ったり、フォーム・コントロールの設定を変更したりしただけで、ユーザーが予期しない動作を起こさない

■ onfocus を用いて、ボタンを実行するなどのイベントを起動させない。

- H84: select 要素とボタンを併用して、アクションを実行するようにする｜WCAG 2.0 実装方法集
  http://waic.jp/docs/WCAG-TECHS/H84.html

■ 「ユーザーが予期しない動作」は、WCAG 2.0 では「状況の変化」として用語定義されており、新しいウィンドウやポップアップウィンドウを開く、フォーカスを別の要素に移動させる、別のページに移動させるなどの動作が該当する。

参考ガイドライン（WCAG 2.0）

3.2.1 オン・フォーカス:いずれのコンポーネントも、フォーカスを受け取ったときに状況の変化を引き起こさない。(レベル A)

オン・フォーカス: 達成基準 3.2.1 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/consistent-behavior-receive-focus.html

参考ガイドライン（WCAG 2.0）

3.2.2 ユーザインタフェース・コンポーネントによる状況の変化:利用者が使用する前にその挙動を知らせてある場合を除いて、ユーザインタフェース・コンポーネントの設定を変更することで状況の変化を引き起こさない。(レベル A)

ユーザインタフェース・コンポーネントによる状況の変化: 達成基準 3.2.2 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/consistent-behavior-unpredictable-change.html

2.5.4.入力フォームでは、各コントロールとそれぞれに対応するラベル(項目名)とを、ソースコードで関連付ける

■ これにより、マウスやタッチ操作をしづらいユーザーが、ラベルの部分でもコントロールを選択できるようになり、スクリーンリーダーでもコントロールと関連づけたラベルが一緒に読み上げられるようになる。

- H44: label 要素を用いて、テキストのラベルとフォーム・コントロールを関連付ける｜WCAG 2.0 実装方法集
  http://waic.jp/docs/WCAG-TECHS/H44.html
- H65: label 要素を用いることができないとき、title 属性を用いてフォーム・コントロールを特定する｜WCAG 2.0 実装方法集
  http://waic.jp/docs/WCAG-TECHS/H65.html

参考ガイドライン（WCAG 2.0）

1.3.1 情報及び関係性:表現を通じて伝達されている情報、構造、及び関係性は、プログラムが解釈可能である。プログラムが解釈可能にすることができないウェブコンテンツ技術を用いる場合は、それらがテキストで提供されている。(レベル A)

情報及び関係性: 達成基準 1.3.1 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/content-structure-separation-programmatic.html

参考ガイドライン（WCAG 2.0）

3.3.2 ラベル又は説明文:コンテンツが利用者の入力を要求する場合は、入力箇所のラベル又は入力方法についての説明文を提供する。(レベル A)

ラベル又は説明文: 達成基準 3.3.2 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/minimize-error-cues.html

2.5.5.入力エラーが発生しうるコンテンツでは、エラーメッセージでエラー箇所を特定する

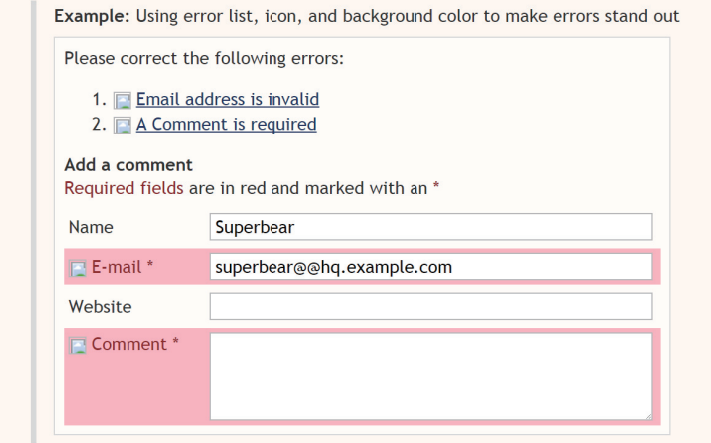
■ どの入力箇所や選択箇所がエラーになっているのかが分かるように明示して、可能であればエラーの内容をテキストで説明する。エラーメッセージのテキストで説明することによって、スクリーンリーダーを使用していても、エラー内容を把握することができるようになる。

参考ガイドライン（WCAG 2.0）

3.3.1 入力エラー箇所の特定:入力エラーを自動的に発見された場合は、エラーとなっている箇所を特定し、そのエラーを利用者にテキストで説明する。(レベル A)

入力エラー箇所の特定: 達成基準 3.3.1 を理解する｜WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/minimize-error-identified.html

入力エラーがあったことをリスト表示、アイコン、背景色で示した例



W3C Home "Tips on Designing for Web Accessibility"より転載
https://www.w3.org/WAI/gettingstarted/tips/designing.html#dont-use-color-alone-to-convey-information

2.5.6.独自の UI コンポーネントを作成する際は、その役割や状態をユーザーエージェントが解釈できるようにする

■ WAI-ARIA を用いることで、ブラウザや支援技術にその UI コンポーネントの情報を伝達することができるほか、キーボード操作を可能にできる。

- Accessible Rich Internet Applications (WAI-ARIA) 1.0｜W3C
  http://www.w3.org/TR/wai-aria/（英語）
- WAI-ARIA 1.0 Authoring Practices-An author's guide to understanding and implementing Accessible Rich Internet Applications
  http://www.w3.org/TR/wai-aria-practices/（英語）
- Using WAI-ARIA in HTML
  http://www.w3.org/TR/aria-in-html/（英語）

- ARIA4: Using a WAI-ARIA role to expose the role of a user interface component | Techniques for WCAG 2.0
  http://www.w3.org/WAI/GL/2014/WD-WCAG20-TECHS-20140107/ARIA4（英語）
- OpenAjax Examples by ARIA Roles| OpenAjax Alliance　Accessibility Task Force
  http://oaa-accessibility.org/examples/roles/（英語）
- ARIA5: Using WAI-ARIA state and property attributes to expose the state of a user interface component
  http://www.w3.org/WAI/GL/2014/WD-WCAG20-TECHS-20140107/ARIA5（英語）
- OpenAjax Examples by ARIA States| OpenAjax Alliance Accessibility Task Force
  http://oaa-accessibility.org/examples/states/（英語）
- OpenAjax Examples by ARIA Properties| OpenAjaxAlliance Accessibility Task Force
  http://oaa-accessibility.org/examples/props/（英語）

参考ガイドライン（WCAG 2.0）

2.1.1 キーボード操作:コンテンツのすべての機能は、個々のキーストロークに特定のタイミングを要することなく、キーボード・インタフェースを通じて操作可能である。ただし、その根本的な機能が利用者の動作による始点からの終点まで続く一連の軌跡に依存して実現されている場合は除く。(レベル A)

キーボード操作: 達成基準 2.1.1 を理解する | WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/keyboard-operation-keyboard-operable.html

参考ガイドライン（WCAG 2.0）

4.1.2 プログラムが解釈可能な識別名・役割及び設定可能な値:すべてのユーザインタフェース・コンポーネント（フォーム、リンク、そしてスクリプトが生成するコンポーネントなどを含む）では、識別名及び役割は、プログラムが解釈可能である。また、利用者が設定可能なステータス、プロパティ、そして値はプログラムが設定可能である。そして、支援技術を含むユーザーエージェントがこれらの項目が変更された通知を受け取ることができる。(レベル A)

プログラムが解釈可能な識別名・役割及び設定可能な値: 達成基準 4.1.2 を理解する | WCAG 2.0 解説書
http://waic.jp/docs/UNDERSTANDING-WCAG20/ensure-compat-rsv.html16

2.6.その他の留意事項

2.6.1.ユーザーの集中力、注意力に配慮し、ページの内容や映像コンテンツの情報量が過大にならないように配慮する

■ 画面に表示する情報量は最小限として、シンプルな構成とする。多くの色を用いないように配慮する（または、そのように制御可能とする）

参考： WCAG 2.0
1.3 適応可能： 情報あるいは構造を損なうことなく、さまざまな方法（例えば、よりシンプルなレイアウト）で提供できるように、コンテンツを制作する。

■ 音声に対して字幕が表示される場合には、字幕の表示／非表示を選択可能とする。

■ 集中力が持続する時間に配慮し、映像コンテンツは２・３分で要点をまとめたものが望ましい（要点をまとめたものを用意する、分割可能とするなど）。

2.6.2.操作方法に一貫性を持たせる

■ 共通領域および各コンテンツを通じて、インタフェースの構成や基本的な操作（起動、終了、進む、戻る、繰り返す、採点など）については、極力、ボタン等のデザインや操作方法を統一することが望ましい。

■ 日常的に使用しているブラウザ（IE や Chrome）の機能や操作方法と整合させることが望ましい。

3.アクセシビリティ実装 Q&A

3.1.Q. 全角，半角について,数字は，全角でなく半角のほうが良いのか？

A.

OS やリーダーによって読み方が違うのですが、半角の場合は「ひゃくにじゅうさん」全角の場合は「いちにいさん」と読むものがあるので、今回は下記のように決めさせてください。
「まとまった数として読ませたいときは半角。そうでないときは全角」
今回は教材ですので、通常は半角になると思います。（「いちにいさん」から「ひゃくにじゅうさん」を推測させることが必要、という考えもあるかもしれませんが、今回は「ひゃくにじゅうさん」と読ませることで統一してください）

3.2.Q. 単位について「200g」「30l」は，「200 グラム」「30 リットル」と日本語にしたほうが良いのか？

A.

はい。「200g」「30l」などは，「200 グラム」「30 リットル」と記載してください。

3.3.Q. その他,筆算の問題の場合，問題画面は，筆算式を表示し「～を計算しましょう」としますが，代替テキストは「～を筆算でしましょう」と，より詳しくしたほうが表示した方が良いか？

A.

「～を計算しましょう」と問題文と同じ文を代替テキストで用意し、筆算式が画像で表示されていることも代替テキストで伝えるのが、理想的な形になると思います。
そのように説明すると冗長と感じられたり、読ませ方が複雑になってしまう場合は、目で得られる情報と同じ情報を提供できるように要約して「～を筆算でしましょう」とします。

3.4.Q. 「18×13」の「×，÷」などの演算記号は，「かける」などの日本語にする必要はあるか？

A.

はい。OS やリーダーによって違うので「かける」「わる」とひらがなで記載ください。

3.5.Q. 「（）や□にあてはまる数を答えなさい」の（）や□は，日本語にする必要はあるか？

A.

はい。「かっこ」「しかく」としていただくと確実に読み上げますが、設問部分と回答部分を同じにしていただく必要があります。

例：6 かっこ 3 いこーる 2。かっこにあてはまるのは何か答えなさい。
「（）」の間に言葉が入っていたりして「かっこ」と書くのが難しい場合は、設問も回答も「（）」としていただき、同じように読み上げさせます。（思っているように読まないことより、設問と回答が違ってしまうことのほうが問題になると思います）

3.6.Q.読み上げの確認方法を知りたい。

A.

以下の方法があります。

- Windows 8.1 の場合:
  Win キーと Enter キーを同時に押すか、検索で探して「ナレーター」を起動して、メモ帳などの文字を読ませる。

- iOS の場合:
  設定－一般－アクセシビリティの「選択項目の読み上げ」をオンにして、メモなどの文字を読ませる。

3.7.Q.要件を満たしている例、満たしていない例など、具体例を見て参考にしたい.

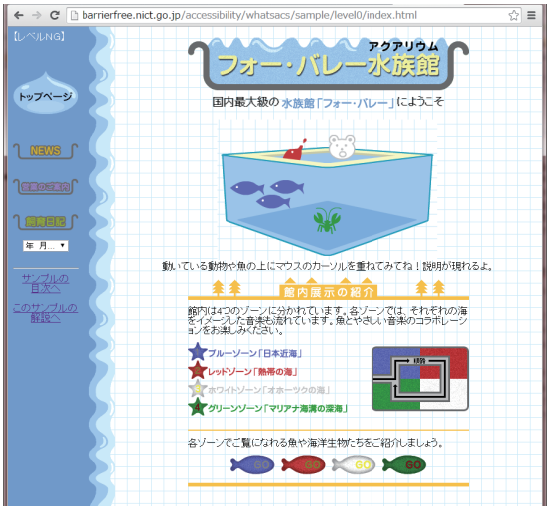
A.

以下のサイトで具体例を紹介しています。

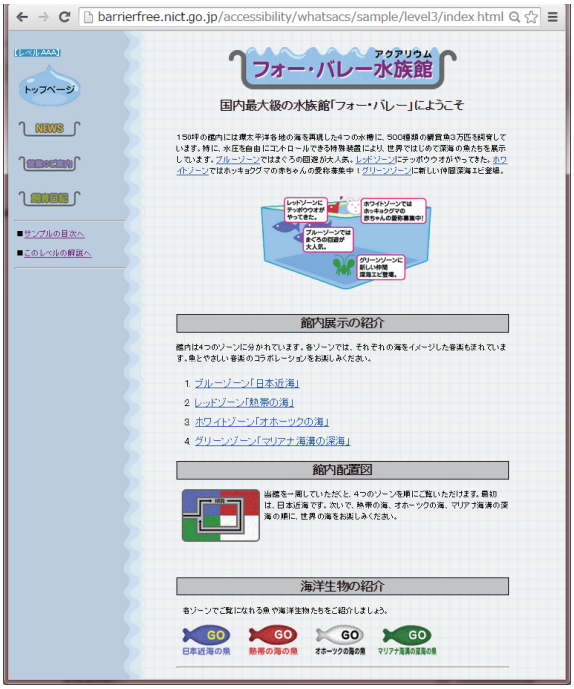
- ウェブアクセシビリティ・サンプルサイト
  （みんなのウェブ　情報バリアフリーのための情報提供サイト）
  http://barrierfree.nict.go.jp/accessibility/whatsacs/sample/index.html

  WAI の WCAG1.0 に示されたウェブアクセシビリティの 3 つのレベル（A，AA，AAA）に適合したウェブページのサンプルを紹介。同じテーマ、同じ内容のウェブページについて、「アクセシビリティが確保されていない」から「トリプル A レベルのアクセシビリティが確保されている」までの 4 種類のサンプルと解説が示されている。

＜適合していないページのサンプル＞



＜レベル AAA のサンプル＞



3.8.Q.作成したコンテンツのアクセシビリティをチェックしたい.

A.

以下のツールが利用可能です。

- みんなのアクセシビリティ評価ツール： miChecker (エムアイチェッカー) Ver. 1.2
  （総務省ＨＰ　「情報アクセシビリティの確保」よりダウンロード可能）
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/b_free/miChecker_download.html

ウェブアクセシビリティ対応の取組みを支援するために、総務省が開発し無償公開しているアクセシビリティのチェックツール。平成 22 年 8 月の JIS X 8341-3:2010 の改正に合わせて開発されたもの。検証作業の支援を目的とするが、同時に知識の習得にも役立つよう配慮されている。

【特徴】

- 明らかな問題がある箇所を特定する
- 問題がある可能性が高い箇所、問題かどうかを人が判断すべき箇所を特定する
- 音声読み上げソフトによる読み上げ順などを視覚的にシミュレーションする
- 問題箇所に該当する JIS X 8341-3:2010 の関連情報へのリンクを提供し、理解を深められるよう支援する
- JIS X 8341-3:2010 に基づく検証、試験の実施を支援する付属資料を提供する

【画面のイメージ】

評価対象とするページのＵＲＬを入力すると、対象ページを読み込み、問題のある個所などを表示する、

付録．チェックリスト【例】

チェック対象	チェック日時	担当者
	年　　月　　日	

番号	チェック項目	頁	評価	対応要否	対応状況等
2-1.	**見やすいコンテンツへの心がけ**				
2-1.1.	色の違いだけで情報を提供していない	2			
2-1.2.	テキストや画像には、少なくとも 4.5:1 のコントラスト比をもたせている	3			
2-1.3.	コンテンツの情報や機能を、形や大き、視覚的な位置や方向を使って説明する際は、それらの違いがわからなくても、ユーザーが理解できるようにしている	4			
2-2.	**代替テキストの提供**				
2-2.1.	すべての画像などの非テキストコンテンツには、音声などに変換できるように、代替テキストを提供している	5			
2-3.	**音声や映像コンテンツを注意して用いる**				
2-3.1.	映像コンテンツに音声が含まれている場合は、音声の内容をキャプションで提供している	6			
2-3.2.	映像コンテンツの映像だけで伝えている情報には、音声ガイドか代替コンテンツを提供している	7			
2-3.3.	音声ファイルで伝えている情報には、テキストに書き起こした代替コンテンツを提供している	8			
2-3.4.	効果音の使用にも留意している	9			
2-3.5.	ページが読み込まれると同時に音声を再生することは避けるようにしているか、ユーザーがすぐに一時停止できるようにしている。あわせて、音声が再生されていることを画面上で視覚的にわかりやすく示している	9			

番号	チェック項目	頁	評価	対応要否	対応状況等
2-3.6.	コンテンツが自動的に動作する場合は、5 秒以内に停止させるか、ユーザーが一時停止や停止を行えるようにしている	10			
2-3.7.	動画やアニメーションに閃光がある場合は、どの 1 秒間においても 3 回以下としている	11			
2-4.	**構造化への留意**				
2-4.1.	HTML ソースをユーザーエージェントが解釈できるようにコーディングしている	12			
2-4.2.	そのコンテンツの主たる自然言語を HTML ソースコードで明示している	12			
2-4.3.	ページの主題が分かるようにページタイトルを記述している	13			
2-4.4.	画面の領域をセクショニング要素やランドマーク属性を用いてマークアップしている	14			
2-4.5.	見出しやリスト、データテーブルは、見た目だけでなく、ソースコードで見出しやリスト、データテーブルの要素を用いてマークアップしている	15			
2-4.6.	可能なかぎり、リンクテキストだけでリンク先が分かるようにしている	15			
2-4.7.	テーブルをレイアウトのために使用する際は、スクリーンリーダーで読み上げた際に意図したとおりの意味が通じる順序になるように注意している	16			
2-4.8.	文字間にスペースや改行が入ることでスクリーンリーダーが一つの単語として認識できなくなるため、見た目の表示のために文字間にスペースや改行を入れたい場合は、CSS を用いて指定している	16			
2-5.	**多様な方法でのアクセスの確保**				
2-5.1.	ユーザーがコンテンツを利用する際、タッチやマウス以外の、キーボードや外付けスイッチなど複数の方法でのアクセスが可能なようにしている	17			
2-5.2.	キーボードの Tab キーによるフォーカス移動順序は、ユーザーが予期できるように、画面での表示順序または操作上の論理的な	19			

番号	チェック項目	頁	評価	対応要否	対応状況等
	順序と一致するようにしている				
2-5.3.	フォーカスを受け取ったり、フォーム・コントロールの設定を変更したりしただけで、ユーザーが予期しない動作を起こしていない	19			
2-5.4.	入力フォームでは、各コントロールとそれぞれに対応するラベル(項目名)とを、ソースコードで関連付けている	20			
2-5.5.	入力エラーが発生しうるコンテンツでは、エラーメッセージでエラー箇所を特定している	21			
2-5.6.	独自の UI コンポーネントを作成する際は、その役割や状態をユーザーエージェントが解釈できるようにしている	22			
2-6.	**その他の留意事項**				
2-6.1.	ユーザーの集中力、注意力に配慮し、ページの内容や映像コンテンツの情報量が過大にならないように配慮している	24			
2-6.2.	操作方法に一貫性を持たせている	24			

平成 27 年度クラウド等の最先端情報通信技術を活用した学習・教育モデルに関する実証別冊

学校情報管理ポリシーガイドブック

平成 28 年 3 月 31 日

NTT コミュニケーションズ株式会社

SEAMLESS CLOUD FOR THE WORLD

目次

1.本ガイドブックの位置づけ

学校情報管理ポリシーガイドブック（以下、本ガイドブックと記載）は、教育委員会や学校が、平成 27 年度「クラウド等の最先端情報通信技術を活用した学習・教育モデルに関する実証」において提供する教育クラウドプラットフォームを活用する際に、情報セキュリティについて何を配慮すべきかを簡潔にまとめたものです。

教育クラウドプラットフォームの導入当初から出てきている大きな課題として、教育クラウドプラットフォーム利用時の情報セキュリティポリシーの変更の必要性と、各学校で実施される児童生徒の端末の持ち帰りと持込みにおけるセキュリティの配慮事項と情報セキュリティポリシーの変更の必要性が出てきており、これらは、今後、教育クラウドプラットフォームを活用する予定がある教育員会や学校が必ず直面する課題であることから、これらの課題に絞って、どのように対応すべきかのノウハウを整理することは非常に有意義であると考えました。

そこで、本ガイドブックでは、これらの 2 点に的を絞り、今後、教育クラウドプラットフォームを導入する教育委員会や学校が課題に直面したときにどのように解決を図るかを検討する際の参考になるようにノウハウを整理してまとめました。

なお、本ガイドブックの作成にあたっては、実証地域の教育委員会にヒアリングを実施した内容を元にしてガイドブックの作成を行ったため、必ずしも全ての教育委員会や学校で参考となる内容にはなっていない箇所もあります。本事業で別途作成した情報セキュリティポリシーガイドラインでは、より幅広い教育委員会や学校の参考になるようにガイドラインを作成していますので、そちらも合わせてご参照いただければ、より一層、教育クラウドプラットフォーム導入時の情報セキュリティにおける配慮事項への理解が深まることが期待されます。

2.情報セキュリティポリシーの概要と用語の定義

2.1情報セキュリティポリシーの概要

一般的に、情報セキュリティポリシーは、「基本方針」「対策基準」「実施手順」の 3 つから構成されます。「基本方針」「対策基準」「実施手順」の概要は以下の通りです。

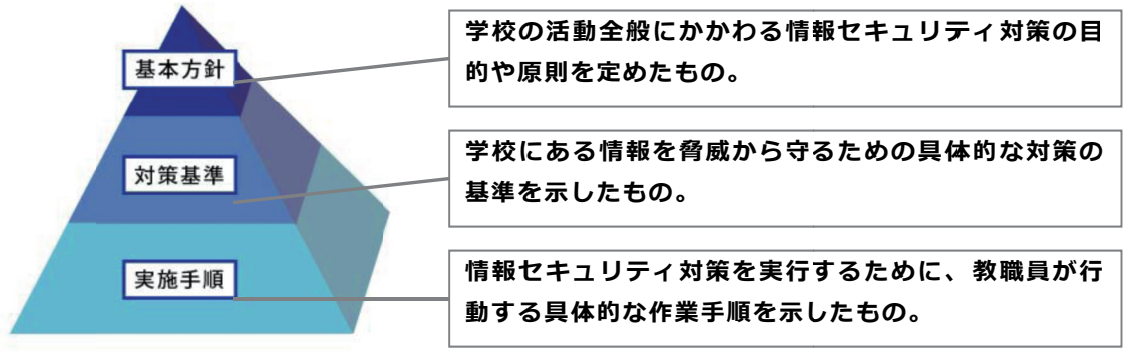


図 2-1 情報セキュリティポリシーの概要
（出典：「教育の情報化に関する手引」（文部科学省））

「基本方針」「対策基準」の記載項目については、決まったものはありませんが、「地方公共団体における情報セキュリティポリシーに関するガイドライン」（総務省）の項目例に従うことが一般的です。なお、教育クラウドプラットフォームの導入及び児童生徒の端末の持ち帰り・持ち込みの実施に伴い、「基本方針」「対策基準」で変更の可能性がある項目は以下の下線の箇所です。

＜情報セキュリティポリシー基本方針の項目例＞

1. 目的
2. 定義
3. **対象とする脅威**
4. **適用範囲**
5. 教職員等の遵守義務
6. 情報セキュリティ対策
7. 情報セキュリティ監査及び自己点検の実施
8. 情報セキュリティポリシーの見直し
9. 情報セキュリティ対策基準の策定
10. 情報セキュリティ実施手順の策定

＜情報セキュリティポリシー対策基準の項目例＞

1. 対象範囲
2. 組織体制
3. 情報資産の分類と管理方法
4. 物理的セキュリティ
5. 人的セキュリティ
6. 技術的セキュリティ
7. 運用
8. 評価・見直し

また、実施手順につきましては、各自治体や教育委員会が独自に作成しており、特に一般的な記載の様式はありませんが、記載項目の一例として「学校における情報セキュリティについて」（文部科学省）の記載されている実施手順における主な記載事項と、実施手順の項目の中で変更の可能性がある項目を下線で示します。

＜情報セキュリティポリシー実施手順の項目例＞

1．目的
2．適用者
3．用語の定義
4．管理体制
5．情報区分
6．日常の留意事項
7．ネットワークの利用・管理
8．緊急時及び障害発生時の対応
9．**情報セキュリティ研修等**

（出典：「学校における情報セキュリティについて」（文部科学省））

なお、「基本方針」「対策基準」「実施手順」の各項目の詳細な記載方法については、「地方公共団体における情報セキュリティポリシーに関するガイドライン」（総務省）及び「学校における情報セキュリティについて」（文部科学省）をご覧ください。

2.2用語の定義

本ガイドブックで出てくる用語のうち、定義が曖昧なもの、分かりにくいものについて以下で説明します。

1. 個人情報

一般的には、学校における個人情報は、生存する教職員、児童・生徒、保護者に関する情報で、その情報に含まれる氏名、生年月日その他の記述等により、特定の個人を識別できるものを指しますが、本ガイドブックでは、その中の児童・生徒の学習履歴に関連する個人情報を個人情報と記載します。

2. 教育クラウドプラットフォーム

平成 27 年度クラウド等の最先端情報通信技術を活用した学習・教育モデルに関する実証（総務省）にて各学校に提供されているクラウド環境を指します。

3. プライベートクラウド

自治体又は教育委員会、学校法人などが自らクラウドの環境を構築して、配下の学校等に対してサービスを提供する形態のクラウドを指します。

3.教育クラウドプラットフォーム利用に際するセキュリティ上の留意事項

3.1教育クラウドプラットフォームを利用する際の情報セキュリティポリシーの変更

教育クラウドプラットフォームを利用する場合に、教育委員会及び学校向けの既存の情報セキュリティポリシーを変更するか否かについては、教育クラウドプラットフォームをどのように使うのか、教育委員会の所有しているクラウド環境がどのようになっているのかによって異なってきます。

表 3-1　情報セキュリティポリシーの変更必要性の有無

教育クラウドプラットフォームの活用方法	教育委員会の既存のクラウド環境	情報セキュリティポリシーの変更必要性の有無
教材だけでなく個人情報を含む情報も保管	個人情報を含む校務情報を既存のプライベートクラウド環境で保管している	既存のプライベートクラウド上に個人情報を保管するように情報セキュリティポリシーが作成されているが、それとは異なる新たなクラウド環境に個人情報を保管するため、**情報セキュリティポリシーの変更が必要となる場合がある。**
	既存のクラウド環境は存在しない	クラウド環境に個人情報を保管することが想定されていない情報セキュリティポリシーとなっているため、**個人情報をクラウドでどのように扱うかの規約も含めて情報セキュリティポリシーの大幅な変更が必要となる。**
教材などの個人情報を含まない情報のみ保管	個人情報を含む校務情報を既存のプライベートクラウド環境で保管している	既存のプライベートクラウド上に個人情報を保管するように情報セキュリティポリシーが作成されているため、**情報セキュリティポリシーの変更が必要とならない場合が多い。**
	既存のクラウド環境は存在しない	教育クラウドプラットフォームでは個人情報を活用せずに利用するため、情報セキュリティポリシーの変更は必要ない場合が多いが、**クラウドを活用することに関連してポリシーへの追記が必要になる場合がある。**

教育クラウドプラットフォームに教材などの個人情報を含まない情報のみを保管して利用する場合は、情報セキュリティポリシーを変更せずに利用できる場合が多いですが、児童生徒の学習履歴などの情報を管理できないため、教育クラウドプラットフォームを有効に活用できません。

教育クラウドプラットフォームを有効に活用するには、個人情報を含めて教育クラウドプラットフォーム上で管理することが必要になり、そのためには、情報セキュリティポリシーの変更が必要になる場合が多いです。既に、自治体又は教育委員会が所有する既存のプライベートクラウド環境上で個人情報を含む校務情報を扱っている場合は、既存プライベートクラウドとの紐付けのための情報のみを教育クラウドプラットフォーム上に保管する方法も考えられますが、この場合でも情報セキュリティポリシーの変更が必要になる可能性があります。各地方公共団体の個人情報保護条例で定められている内容に従って、適切な対応を行うようにして下さい。以下に、教育クラウドプラットフォームを利用する場合に、情報セキュリティポリシー基本方針、情報セキュリティポリシー対策基準、情報セキュリティポリシー実施手順で変更が必要になる項目と、その修正のポイントについて記載します。

（１）情報セキュリティポリシー基本方針

①　対象とする脅威

教育クラウドプラットフォームを利用する場合は、新たなクラウド環境上に情報を保管することになるため、新たな脅威が発生するかを検討する必要が生じます。

例えば、新たな脅威としては、以下のようなものが考えられます。

- 教育クラウドプラットフォームの運用事業者によるデータの流出・漏えい
- 教育クラウドプラットフォーム環境の災害・事故、サービス妨害攻撃によるサービス停止等による授業実施や学校業務の停止
- 教育クラウドプラットフォーム環境と学校を結ぶネットワーク環境の災害・事故等による授業や学校業務の停止
- 教育クラウドプラットフォーム環境への不正アクセス・不正操作によるデータの破壊・改ざん・消去　など

上記のような項目を追加すべきかを検討する必要があります。

②　適用範囲

教育クラウドプラットフォームを利用することにより、セキュリティポリシーに準拠しなければいけない者や情報資産の範囲に変更が生じる可能性があります。セキュリティポリシーの適用範囲として変更になる可能性があるものとしては、以下のようなものが考えられます。

- 外部委託業者を適用範囲に含めるか
- ネットワーク事業者
- （情報資産）教育クラウドプラットフォーム環境のシステム、設備、記録媒体　など

上記のような項目を追加すべきかを検討する必要があります。

（２）情報セキュリティポリシー対策基準

① 対象範囲

基本的には、基本方針の適用範囲に準じるため、基本方針の変更に従って修正を行う必要があります。

② 情報資産の分類と管理方法

通常、学校で扱う情報資産については、基本方針の適用範囲に従い、機密性、完全性、可用性のそれぞれの視点から重要度に応じて分類（３～５段階程度で分類）され、その取扱制約が定められています。

分類	分類基準	取扱制限
機密性３	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	・私物パソコンでの作業禁止（機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の外部記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・外部記録媒体の施錠可能な場所への保管
機密性２	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
機密性１	機密性２又は機密性３の情報資産以外の情報資産	

図 3-1 機密性による情報資産分類の例

教育クラウドプラットフォームを利用することにより、基本方針の適用範囲に変更が生じた場合は、その変更内容に応じて情報資産の分類と管理方法を変更する必要があります。変更になる可能性があるものとしては、以下のようなものが考えられます。

- 教育クラウドプラットフォームに既存の情報資産を預ける場合に、その情報資産の制約条件が満たされない場合の分類・制約条件の見直し
- 教育クラウドプラットフォームを利用することで新たな情報資産を扱うことになった場合のその情報資産の分類と取扱制約の追加

上記のような項目を追加すべきかを検討する必要があります。

③ 物理的セキュリティ

通常、基本方針で定めた「対象となる脅威」に対して物理的に対応できる対策を、対策基準の物理的セキュリティに記載しています。

教育クラウドプラットフォームを利用することにより、基本方針で定めた「対象となる脅威」が新たに出てきている場合は、外部に設置する装置、外部ネットワークの扱い等についての記載内容の変更・追加が必要になる可能性があります。記載内容が変更になる可能性があるものとしては、以下のようなものが考えられます。

- サーバ等の管理方法に関する変更・追記
- 管理区域（情報システム室等）の管理に関する変更・追記
- 通信回線及び通信回線装置の管理に関する変更・追記

上記のような項目を追加すべきかを検討する必要があります。

④　人的セキュリティ

通常、基本方針で定めた「対象となる脅威」に対して人的に対応できる対策を、対策基準の人的セキュリティに記載しています。

教育クラウドプラットフォームを利用することにより、基本方針で定めた「対象となる脅威」が新たに出てきている場合は、教育・訓練、外部委託の管理等についての記載内容の変更・追加が必要になる可能性があります。記載内容が変更になる可能性があるものとしては、以下のようなものが考えられます。

- 職員等の遵守事項
- 研修・訓練
- 事故、欠陥等の報告
- ID 及びパスワード等の管理

上記のような項目を追加すべきかを検討する必要があります。

⑤　技術的セキュリティ

通常、基本方針で定めた「対象となる脅威」に対して技術的に対応できる対策を、対策基準の技術的セキュリティに記載しています。

教育クラウドプラットフォームを利用することにより、基本方針で定めた「対象となる脅威」が新たに出てきている場合は、アクセス記録、障害記録、バックアップ、アクセス制御、外部ネットワークに接続することで内部ネットワークが脅威にさらされない対策等についての記載内容の変更・追加が必要になる可能性があります。記載内容が変更になる可能性があるものとしては、以下のようなものが考えられます。

- コンピュータ及びネットワークの管理
- アクセス制御
- システム開発、導入、保守等
- 不正プログラム対策
- 不正アクセス対策
- セキュリティ情報の収集

上記のような項目を追加すべきかを検討する必要があります。

（３）情報セキュリティポリシー実施手順

①　情報区分

実施手順の「情報区分」では、その中で定める情報資産の範囲を明確にした上で、「対策

基準」で決定した重要度ごとに情報資産を整理し、重要度ごとに対策基準で定めた制約条件に従って情報資産の取扱方法を明確に示します。

基本方針

学校の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

対策基準

基本方針に従って対策基準で情報資産の分類の定義を明確化

重要度	定義
A	指導要録や評定一覧表、定期考査素点表、教職員等の給与関係書類や手当関係書類等、プライバシー性が非常に高く、情報が漏えいした場合、生徒や保護者、教職員等にとって経済的な損失や精神的な苦痛が非常に大きい校務情報。
B	生徒の通知表や定期考査答案用紙、住所録や緊急連絡先等のプライバシー性が高く、情報が漏えいした場合、生徒や保護者、教職員等に経済的な損失や精神的な苦痛が大きい校務情報。また、情報が漏えいした場合、学校運営に支障をきたす校務情報。
C	学校紹介パンフレット、PTA 資料等の配布もしくは公開されてもよい校務情報のうち、個人情報を含むもの。
D	実施後の未使用考査問題、職員会議資料等の配布もしくは公開されてもよい校務情報のうち、個人情報を含まないもの。

実施手順

対策基準で定めた重要度毎に対象となる情報資産とその取扱方法を明確化

	情報資産	取扱方法
重要度A	生徒等の障がいの状況、事件・事故、指導記録、保護者の収入等の情報等、プライバシー性が高い情報並びに指導要録や成績一覧表等、児童・生徒の情報が高度に集積している帳票や電子データ等 ＜学籍関係＞ 〇指導要録（学籍に関する記録）その写し及び抄本　〇出席簿　〇卒業証書授与台帳　〇転退学受付（整理）簿 〇転入学受付（整理）簿　〇就学児童・生徒異動報告　〇休学・退学願等受付（整理）簿 〇教科用図書給付児童・生徒名簿　〇要・準要保護児童・生徒認定台帳　〇その他校内就学援助関係書類 ＜成績関係＞ 〇指導要録（指導に関する記録）その写し及び抄本　〇評定一覧　〇進級・卒業判定会議録・会議資料 〇定期考査素点表　〇成績に関する個票等 ＜生徒指導関係＞ 〇事故報告書・記録簿　〇生徒指導・特別指導等記録簿　〇児童・生徒等の個人写真 ＜進路関係＞ 〇卒業生進路先一覧等　〇進路希望調査 〇進路指導記録　〇入学者選抜に関する表簿（願書等） ＜教務関係＞ 〇高校入試関連資料（合否判定資料等含む。） ＜健康関係＞ 〇健康診断に関する表簿・歯の検査表　〇心臓管理等医療情報 〇保健日誌 ＜事務関係＞ 〇住民票・戸籍謄本・抄本など　〇監査調書　〇叙位・叙勲書類　〇卒業生台帳 〇授業料関連書類 〇給与関係書類 〇手当関係書類	・持ち出し禁止 ・電子データは、教育委員会が設置するアクセス権限の設定ができる装置に保存 ・リモートアクセスシステムを利用して、自宅のパソコンからアクセス可能 ・簿冊等の紙文書は施錠可能な場所に保管

図 3-2　情報資産の重要度に従った取扱い方法の例

情報教育クラウドプラットフォームを利用することにより、対策基準で基本方針の適用範囲の変更に伴い情報資産の分類と管理方法を変更した場合は、その内容に従って、具体的な情報資産ごとにその重要度と管理方法を明確にしてポリシーの変更・追記が必要になります。

なお、対策基準で情報資産の分類と管理方法を変更していない場合でも、情報教育クラウドプラットフォームを利用することにより新たに管理する情報資産が出てきた場合は、情報資産ごとに既存のどの区分に当てはまるかとその管理方法についてポリシーの変更・追記が必要になります。

② 日常の留意事項

実施手順の「日常の留意事項」では、「情報区分」で示した取扱方法について、教職員が遵守すべき具体的な手順を、学校での日常的な業務に関連付けて、分かりやすく記載しています。

場面	留意事項	禁止事項
ログイン ID 及びパスワードの管理	・パスワードの入力時に覗き込まれることがないよう留意すること。 ・パスワードを失念した場合は指示に従いパスワードの発行を受けること。	・パスワードを他人に教えたり、メモを取ったりすること。 ・利用者個人で設定するパスワードは、長期間同じものを使用すること。
ソフトウェアの利用	・ウイルス対策ソフトの定義ファイルが、最新の状態に更新されていること。 ・ソフトウェアをインストールする場合には、所定の様式に記入すること。	・ライセンス、著作権法違反（違法な複製）のソフトウェアを使用すること。 ・校長の許可なく、校務用パソコンにソフトウェアをインストールすること。 ・教育委員会が配備又は学校で購入した公用のソフトウェア以外の市販ソフトウェアを使用すること。 ・職務に関係ないフリーのソフトウェアやファイル共有ソフトウェア等を導入すること。 ・ファイル交換ソフトをインストールすること。

図 3-3　日常の留意事項の記載例

実施手順の「情報区分」で変更・追記があった場合は、その変更内容に応じて「日常の留意事項」を変更する必要があります。変更になる可能性があるものとしては、以下のようなものが考えられます。

- コンピュータ及びネットワークの管理
- アクセス制御
- システム開発、導入、保守等
- 不正プログラム対策
- 不正アクセス対策
- セキュリティ情報の収集

上記のような項目を追加すべきかを検討する必要があります。

③　ネットワークの利用・管理

実施手順の「ネットワークの利用・管理」では、「対策基準」の「物理的セキュリティ」、「技術的セキュリティ」の内容に従って、情報資産の取扱いをネットワーク上で行う場合に、

サービスごとの利用に関する遵守事項について具体的に記載しています。

教育クラウドプラットフォームを利用することにより「物理的セキュリティ」、「技術的セキュリティ」の関連する記載内容に変更が生じた場合は、その具体的な利用と管理の方法についてポリシーの変更・追記が必要になります。

④　緊急時及び障害発生時の対応

実施手順の「緊急時及び障害発生時の対応」では、「対策基準」の「人的セキュリティ」の内容に従って、障害や事故等が発生した際、被害の拡大防止や復旧に向けた手順等、教職員等が対応しなければならない事項を具体的に記載しています。

教育クラウドプラットフォームを利用することにより「人的セキュリティ」の関連する記載内容に変更が生じた場合は、その具体的な緊急時及び障害発生時の対応についてポリシーの変更・追記が必要になります。

⑤　情報セキュリティ研修等

実施手順の「情報セキュリティ研修等」では、「対策基準」の「人的セキュリティ」の内容に従って、情報セキュリティに関する教職員等を対象とした研修を実施する場合は、具体的な研修内容、参加対象者等について具体的に記載しています。

教育クラウドプラットフォームを利用することにより「人的セキュリティ」の関連する記載内容に変更が生じた場合は、その具体的な情報セキュリティ研修等の開催内容等についてポリシーの変更・追記が必要になります。

なお、以上でポイントを述べた情報セキュリティポリシーの変更に当たっては、教育委員会では、自治体の情報セキュリティポリシーを流用している場合が多いこと、自治体の情報セキュリティポリシーによる様々な縛りが発生する場合があること（例：自治体の外にはサーバを設置できない、無線 LAN の利用は禁止など）、情報セキュリティポリシーの作成や変更を教育委員会のみで実施することは困難であること、などから、教育クラウドプラットフォームを導入する際は、自治体の情報政策関連の部署と密に連携をしながら進めることが望ましいです。

ポイント

＜教育クラウドプラットフォームを利用する際の情報セキュリティポリシーの変更＞

- 自治体又は教育委員会が所有する既存のプライベートクラウド環境上で個人情報を含む校務情報を扱い、連携して教育クラウドプラットフォーム上の学習履歴情報を活用する場合でも、情報セキュリティポリシーの変更を伴う可能性があるため、各地方公共団体の個人情報保護条例で定められている内容に従っ

ポイント

て、適切な対応を行うようにして下さい。

- 既存のプライベートクラウドがない場合は、クラウド環境でどのような情報をどのように扱うかを明確にした上で、情報セキュリティポリシーの変更を行う必要があります。
- 教育クラウドプラットフォームの導入の際は、自治体の情報政策関連の部署と密に連携をしながら進めることが望ましいです。

コラム

- セキュリティポリシーでは、教育委員会や学校で扱っている情報を重要度に応じて 3～5 の分類（情報区分）に分けていることが一般的です。この情報区分ごとに、どのように情報を取り扱うか（例：校外への持ち出しは禁止）を定めています。
- セキュリティポリシー上では、情報を保管する媒体の扱いについて必ずしも記載されているとは限りません。情報区分ごとにどの媒体で情報を扱えるかを記載することは理想的ではありますが、ポリシーの見直しが頻繁に必要となる可能性が高くなります。例えば、学習・教育クラウド・プラットフォームは校内と同様と定義することによって、「校外への持ち出しは禁止」に当たらないと解釈する方法もあります。

3.2クラウド間連携

3.1 で既に説明した通り、自治体又は教育委員会が所有するクラウドが既にある場合は、既存環境を最大限に活用するために、個人情報を既存のクラウド環境で扱い、教育クラウドプラットフォーム上では既存のクラウド環境との紐付けの情報のみを扱って、学習履歴などの情報を活用する方法も考えられます。

具体的な方法の一つとして、それだけでは個人を特定できない関連付けのための番号を、既存クラウドと教育クラウドプラットフォームの両者で保有する方法があります。こうすることによって、教育クラウドプラットフォームの情報のみを見ただけでは、どれが誰の情報かが特定できませんが、既存クラウド側で関連付け情報を介して個人を特定することによって、学習履歴などの情報を利活用することが可能となります。

このように、教育クラウドプラットフォームだけを見ただけでは個人を特定できず、既存クラウドと連携することによって個人を特定できるような何らかの方法を用いることでクラウド間連携を行う場合でも、他の情報と照合することで、特定の個人が識別できるものとして個人情報と同様の扱いが求められる場合があり、情報セキュリティポリシーの変更が必要になる場合があります。各地方公共団体の個人情報保護条例で定められている内容に従って、クラウド間連携を行った際に教育クラウドプラットフォーム上に保存される関連付けの情報について、どのように扱うのが適切かを把握した上で、適切な対応を行うようにして下さい。

ポイント

<クラウド間連携を行う場合のポイント>

- クラウド間連携を実現するには、個人を特定できない関連付けのための情報を、既存クラウドと教育クラウドプラットフォームの両者で保有して、既存クラウド側で個人情報との紐付けを行うことで情報の利活用を行う必要があります。
- クラウド間連携を行う際は、各地方公共団体の個人情報保護条例で定められている内容に従って、教育クラウドプラットフォーム上に保存される既存クラウド環境との関連付けの情報について、どのように扱うのが適切かを把握した上で、適切な対応を行うようにして下さい。

4.児童生徒の端末の持ち帰り、持込みでのセキュリティ上の留意事項

4.1児童生徒の端末の持ち帰りの際のセキュリティ上の留意事項

児童生徒の端末の持ち帰りについては、テスト前や長期休み期間中など、児童生徒が自習をする機会が多い時期に限定的に実施されている場合が多くなっています。しかしながら、端末の持ち帰りを実施する際の課題は多く、気軽に持ち帰りを実施できていないのが実情です。児童生徒の端末の持ち帰りを実施する際のセキュリティ上の課題は以下の通りです。

- 様々なネットワーク環境が存在する児童生徒の家庭にて、専門知識なしに持ち帰り端末を簡単かつ安全に接続できる環境をどのように提供するか
- 自宅で児童生徒が安全にインターネットに繋げられる環境をどのように提供するか
- 端末の盗難、紛失時に重要度の高い情報の流出をどのように防ぐのか

各課題に対する対応は各実証地域の学校にて試行錯誤しながら実施しているところで、今後の技術の進歩によって新たな対応方法が出てくる可能性もありますが、現時点で、一定の効果が得られている対応策は以下の通りです。

1. 様々なネットワーク環境が存在する児童生徒の家庭にて、専門知識なしに持ち帰り端末を簡単かつ安全に接続できる環境をどのように提供するか

   児童生徒の家庭でのネットワーク接続環境については、千差万別の環境が存在していることが想定されることから、端末側の設定のみで簡単かつ安全な接続に対応することは容易ではないと考えられます。そこで、モバイルルータも合わせて持ち帰らせることで、ネットワークへの接続も学校側で制御できるようにすることが効果的な対応策です。
   なお、ネットワーク環境が存在しない児童生徒の家庭も一定割合で存在することから、家庭環境の違いを児童生徒に感じさせずに済む効果もあります。

2. 自宅で児童生徒が安全にインターネットに繋げられる環境をどのように提供するか

   端末に、児童生徒が閲覧することが好ましくないサイトへのアクセスをブロックするフィルタリングソフトウェアを導入し、自宅で児童生徒がインターネットを閲覧する際に、全てのサイトに自由にアクセスすることを防ぐことができます。なお、１でモバイルルータを導入した場合は、フィルタリングの機能を持ったモバイルルータを導入すれば、新たにソフトウェアを導入する必要がなくなります。

3. 端末の盗難、紛失時に重要度の高い情報の流出をどのように防ぐのか

児童生徒が端末を持ち帰る際に、端末上の個人情報等を削除し、教材やドリルなどを保存した持ち帰り専用の環境に入れ替えた上で児童生徒に渡し、端末を持ち帰り後に学校に持ってきた際には、校内で利用する環境を復元する運用を行うことで、万が一、児童生徒が端末を紛失したり盗難にあったりした場合でも、個人情報等の重要度の高い情報の流出を防ぐことができます。

ポイント

<児童生徒の端末の持ち帰りの際のセキュリティ上の留意事項>

- 児童生徒が端末を持ち帰る際は、家庭でのネットワーク接続とインターネットの閲覧について、学校側で制御が行える環境を提供する必要があります。
- 端末上に個人情報が存在する場合は、持ち帰り時の端末設定と学校内での端末設定の内容を入れ替えることで、情報漏えいを防ぐことができます。
- 新たな技術の出現によって対応策が変わってくるため、定期的にベンダーなどから情報収集を行い、新たな対応策の導入について検討を行うことが必要です。

コラム

- 端末環境の入れ替えは、毎回、手動で運用を行っていると大変であることから、専用のツールなどで自動化を図ることも合わせて検討する必要があります。

4.2児童生徒用端末持込み時におけるセキュリティ上の留意事項

教育クラウドプラットフォームの利用にあたり、児童生徒用が自費で端末を購入する場合、学校では児童生徒が独自に選定した端末を持ち込み、授業で活用されるケースと、児童生徒が家庭にある様々な端末を自由に持ち込むものではなく、指定された機種を購入し持ち込むケースが考えられます。また、双方のケースにおいて家庭では家庭のネットワーク環境からインターネット経由で教育委員会が用意している教材コンテンツを利用するというシーンが想定されます。そのような環境を想定した場合に、児童生徒の端末の持込みを実施する際のセキュリティ上の課題は以下の通りです。

- 児童生徒の端末を校内ネットワークに安全に接続する環境をどのように提供するのか
- 自宅で児童生徒が安全にインターネットに繋げられる環境をどのように提供するか
- 端末の盗難、紛失時に重要度の高い情報の流出をどのように防ぐのか

各課題に対する対応は各学校にて試行錯誤しながら実施しているところで、今後の技術の進歩によって新たな対応方法が出てくる可能性もありますが、現時点で、一定の効果が得られている対応策は以下の通りです。

1. 児童生徒の端末を校内ネットワークに安全に接続する環境をどのように提供するのか

児童生徒が購入した端末を受け取る前に、学校側で環境設定などを行い、端末の機能に制御をかけることで、児童生徒が備品として購入した端末のみしか校内ネットワークに接続できず、更に、接続後も学習系ネットワークのみに接続が可能で、校務系のネットワークには接続ができないように制御が可能となります。また、アプリケーションのインストールを禁止し、事前の環境設定でウイルス対策ソフトの設定を行うことで、児童生徒の端末が家庭のネットワーク環境でウイルスに感染するのを防ぐことが可能となります。

2. 自宅で児童生徒が安全にインターネットに繋げられる環境をどのように提供するか

学校側の事前の環境設定の際に、端末に、児童生徒が閲覧することが好ましくないサイトへのアクセスをブロックするフィルタリングソフトウェアを導入し、自宅で児童生徒がインターネットを閲覧する際に、全てのサイトに自由にアクセスすることを防ぐことができます。

3. 端末の盗難、紛失時に重要度の高い情報の流出をどのように防ぐのか

学校側の事前の環境設定の際に、端末管理ツールを導入して、管理サーバよりリモートにて端末を管理し、第三者による端末操作を防止することで、端末の盗難・紛失時の情報漏えいを防止できます。更に、端末内の情報を暗号化することで、情報漏えいの防止を強化でき

ます。

なお、教育クラウドプラットフォーム上で学習履歴を含めた個人情報を扱う場合は、原則、端末内にはデータは保存されないため、端末管理ツールの導入等の情報漏えい防止対策に伴う作業負荷は発生しなくなります。

ポイント

<児童生徒の端末の持ち込の際のセキュリティ上の留意事項>

- 児童生徒に端末を渡す前に、端末に対してセキュリティ上の各種設定を施すこと、アプリケーションのインストールを禁止することなど、学校側で端末の制御がある程度行えるようにする必要があります。
- 端末上の情報の漏えいの防止は、端末のリモート管理と端末上の情報の暗号化の 2 つの技術的対策を施すことで、情報漏えいを防ぐことができます。なお、教育クラウドプラットフォーム上で学習履歴を含めた個人情報を扱う場合は、原則、端末内にはデータは保存されないため、情報漏えいのリスクは低減されます。
- 新たな技術の出現によって対応策が変わってくるため、定期的にベンダーなどから情報収集を行い、新たな対応策の導入について検討を行うことが必要です。

コラム

- 児童生徒が所有する端末であるにも関わらず、学校側で様々な制限を設けていることについては、保護者の理解が必須となります。保護者へのパンフレットの配布、説明会の開催など、理解を得られるように様々な周知活動を行うことが重要です。
- 端末を児童生徒が購入することに関しては、義務教育ではない高校では、教科書を生徒が購入しているなど、備品の購入に関して理解が得られやすい環境であることから、小中学校よりは導入が容易であるかもしれません。

4.3児童生徒の端末の持ち帰り・持込みの実施による情報セキュリティポリシーの変更

児童生徒の端末の持ち帰り、持込みについては、これまでに学校で行われていた情報端末の活用とは大きく異なり、学校の情報機器を校外に持ち出す、学校の情報機器でないものを校内に持ち込むという情報機器の校内校外の移動が頻繁に発生することから、校内に固定された情報端末の扱いを前提とした既存の情報セキュリティポリシーでは対応が難しくなってきています。以下に、児童生徒の端末の持ち帰りを行う場合の情報セキュリティポリシー基本方針、情報セキュリティポリシー対策基準、情報セキュリティポリシー実施手順で変更が必要になる項目と、その修正のポイントについて記載します。

（１）情報セキュリティポリシー基本方針＞

①　対象とする脅威

児童生徒の端末の持ち帰りを行う場合は、学校の情報資産を校外に持ち出すことになるため、新たな脅威としてどのようなものが発生するかを検討する必要が生じます。

例えば、新たな脅威としては、以下のようなものが考えられます。

- 持ち帰り時の端末からのデータの流出・漏えい
- 端末の破壊・盗難
- 不正アクセス・不正操作による端末上の情報の破壊・改ざん・消去　など

上記のような項目を追加すべきかを検討する必要があります。

②　適用範囲

児童生徒の端末の持ち帰りを行う場合、セキュリティポリシーに準拠しなければいけない者や情報資産の範囲に変更が生じる可能性があります。セキュリティポリシーの適用範囲として変更になる可能性があるものとしては、以下のようなものが考えられます。

- 適応範囲に児童生徒を含める
- 児童生徒の持ち帰り端末　など

上記のような項目を追加すべきかを検討する必要があります。

（２）情報セキュリティポリシー対策基準＞

①　対象範囲

基本的には、基本方針の適用範囲に準じるため、基本方針の変更に従って修正を行う必要があります。

②　情報資産の分類と管理方法

通常、学校で扱う情報資産については、基本方針の適用範囲に従い、機密性、完全性、可用性のそれぞれの視点から重要度に応じて分類（３～５段階程度で分類）され、その取扱制約が定められています。

児童生徒の端末を持ち帰る場合に、基本方針の適用範囲に変更が生じた場合は、その変更内容に応じて情報資産の分類と管理方法を変更する必要があります。また、適応範囲に変更がない場合でも、児童生徒が端末を持ち帰ることで、その端末が区分されている情報資産の分類とその制約条件を変更しないといけない場合があります。

セキュリティポリシーの「情報資産の分類と管理方法」として変更になる可能性があるものとしては、以下のようなものが考えられます。

- 児童生徒が持ち帰る端末の情報資産への追加と制約条件の明確化
- 既に情報資産に登録されている端末を児童生徒が持ち帰る端末として使う場合は、その分類と制約条件が適切かの確認及び必要に応じた分類・制約条件の見直し　など

上記のような項目を追加すべきかを検討する必要があります。

③　物理的セキュリティ

通常、基本方針で定めた「対象となる脅威」に対して物理的に対応できる対策を、対策基準の物理的セキュリティに記載しています。

児童生徒の端末を持ち帰る場合に、基本方針で定めた「対象となる脅威」が新たに出てきている場合は、自宅からのネットワークアクセスや持ち帰り時の端末の扱い等についての記載内容の変更・追加が必要になる可能性があります。

記載内容が変更になる可能性があるものとしては、以下のようなものが考えられます。

- 通信回線及び通信回線装置の管理に関する変更・追記
- 持ち帰り端末等の管理に関する項目の追加

上記のような項目を追加すべきかを検討する必要があります。

④　人的セキュリティ

通常、基本方針で定めた「対象となる脅威」に対して人的に対応できる対策を、対策基準の人的セキュリティに記載しています。

児童生徒の端末の持ち帰りにより、基本方針で定めた「対象となる脅威」が新たに出てきている場合は、端末及び児童生徒の自宅でのネットワーク環境等に関しての教職員及び児童生徒・保護者に対しての教育・訓練等についての記載内容の変更・追加が必要になる可能性があります。

記載内容が変更になる可能性があるものとしては、以下のようなものが考えられます。

- 児童生徒、保護者等の遵守事項に関する項目の追加
- 研修・訓練に関する変更・追記
- 事故、欠陥等の報告に関する変更・追記
- ID 及びパスワード等の管理に関する変更・追記

上記のような項目を追加すべきかを検討する必要があります。

⑤　技術的セキュリティ

通常、基本方針で定めた「対象となる脅威」に対して技術的に対応できる対策を、対策基準の技術的セキュリティに記載しています。

児童生徒の端末の持ち帰りにより、基本方針で定めた「対象となる脅威」が新たに出てきている場合は、持ち帰り時の端末からのデータの流出・漏えい、端末の破壊・盗難、不正アクセス・不正操作による端末上の情報の破壊・改ざん・消去等についての記載内容の変更・追加が必要になる可能性があります。

記載内容が変更になる可能性があるものとしては、以下のようなものが考えられます。

- コンピュータ及びネットワークの管理に関する変更・追記
- アクセス制御に関する変更・追記
- 不正プログラム対策に関する変更・追記
- 不正アクセス対策に関する変更・追記
- セキュリティ情報の収集に関する変更・追記

上記のような項目を追加すべきかを検討する必要があります。

（３）情報セキュリティポリシー実施手順＞

① 情報区分

実施手順の「情報区分」では、その中で定める情報資産の範囲を明確にした上で、「対策基準」で決定した重要度ごとに情報資産を整理し、重要度ごとに対策基準で定めた制約条件に従って情報資産の取扱方法を明確に示します。

児童生徒の端末の持ち帰りにより、対策基準で基本方針の適用範囲の変更に伴い情報資産の分類と管理方法を変更した場合は、その内容に従って、具体的な情報資産ごとにその重要度と管理方法を明確にしてポリシーの変更・追記が必要になります。

なお、対策基準で情報資産の分類と管理方法を変更していない場合でも、児童生徒の端末の持ち帰りにより新たに管理する情報資産が出てきた場合は、情報資産ごとに既存のどの区分に当てはまるかとその管理方法についてポリシーの変更・追記が必要になります。

② 日常の留意事項

実施手順の「日常の留意事項」では、「情報区分」で示した取扱方法について、教職員が遵守すべき具体的な手順を、学校での日常的な業務に関連付けて、分かりやすく記載しています。

児童生徒の端末の持ち帰りにより、実施手順の「情報区分」で変更・追記があった場合は、その変更内容に応じて「日常の留意事項」を変更する必要があります。変更になる可能性があるものとしては、以下のようなものが考えられます。

- コンピュータ及びネットワークの管理に関する変更・追記
- アクセス制御に関する変更・追記
- システム開発、導入、保守等に関する変更・追記
- 不正プログラム対策に関する変更・追記

- 不正アクセス対策に関する変更・追記
- セキュリティ情報の収集に関する変更・追記

上記のような項目を追加すべきかを検討する必要があります。

③ ネットワークの利用・管理

実施手順の「ネットワークの利用・管理」では、「対策基準」の「物理的セキュリティ」、「技術的セキュリティ」の内容に従って、情報資産の取扱いをネットワーク上で行う場合に、サービスごとの利用に関する遵守事項について具体的に記載しています。

児童生徒の端末の持ち帰りにより、児童生徒の自宅から外部ネットワークを利用する場合等、「物理的セキュリティ」、「技術的セキュリティ」の関連する記載内容に変更が生じた場合は、その具体的な利用と管理の方法についてポリシーの変更・追記が必要になります。

④ 緊急時及び障害発生時の対応

実施手順の「緊急時及び障害発生時の対応」では、「対策基準」の「人的セキュリティ」の内容に従って、障害や事故等が発生した際、被害の拡大防止や復旧に向けた手順等、教職員等が対応しなければならない事項を具体的に記載しています。

児童生徒の端末の持ち帰りにより、「人的セキュリティ」の関連する記載内容に変更が生じた場合は、児童生徒の端末の持ち帰り時での緊急時・障害発生時の具体的な対応についてポリシーの変更・追記が必要になります。

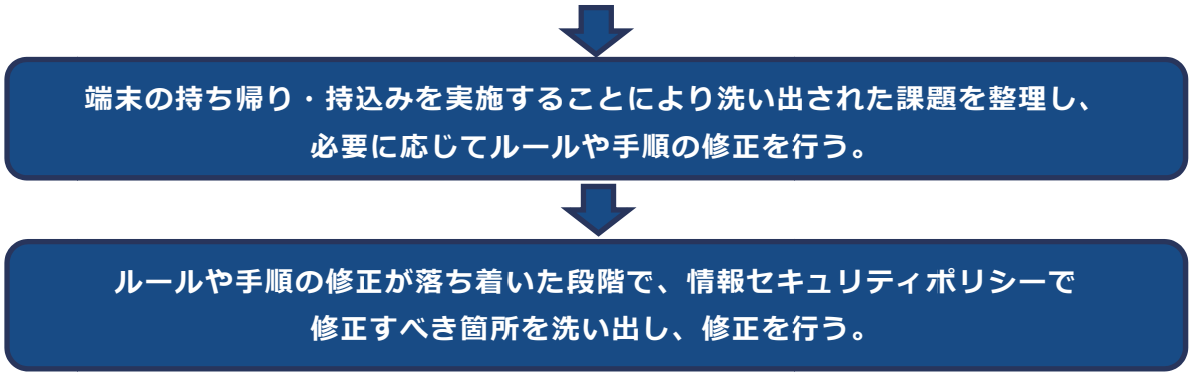
⑤ 情報セキュリティ研修等

実施手順の「情報セキュリティ研修等」では、「対策基準」の「人的セキュリティ」の内容に従って、情報セキュリティに関する児童生徒、保護者、教職員等を対象とした研修を実施する場合は、具体的な研修内容、参加対象者等について具体的に記載しています。

児童生徒の端末の持ち帰りにより、「人的セキュリティ」の関連する記載内容に変更が生じた場合は、児童生徒の端末の持ち帰りにともなう研修等の具体的な開催内容等についてポリシーの変更・追記が必要になります。

以上でポイントを述べた情報セキュリティポリシーの変更には時間がかかることから、当面の対応として以下のような手順で進めながら、将来的には、情報セキュリティポリシーを改定することが望ましいです。

情報セキュリティポリシーに抵触しない範囲で端末の持ち帰り・持込みを実施し、詳細なルールや手順は教育委員会又は学校にて別途作成する。



端末の持ち帰り実施時の詳細なルールとしては、以下の規定（ルール）を作成し運用を実施することが望ましいです。

- 児童生徒用タブレット PC の利用規則（教職員向け／児童生徒向け）
- 児童生徒用タブレット PC の持ち帰り規則（教職員向け／児童生徒向け）
- インターネット利用規定（教職員向け）
  - ✧ インターネットの利用形態
  - ✧ 個人情報の発信とその範囲
  - ✧ セキュリティ対策、セキュリティの維持・管理
  - ✧ 著作権
  - ✧ 教師による指導
  - ✧ 管理運用
  - ✧ 管理規定の見直し
- 個人情報管理規定（教職員向け）

ポイント

＜児童生徒の端末の持ち帰り・持込みの実施による情報セキュリティポリシーの変更＞

- 児童生徒の端末の持ち帰り、持込みは、これまでの情報セキュリティポリシーでは対応できない可能性が高く、変更に向けた検討が必要です。
- 児童生徒の端末の持ち帰り、持込みについては、当面は情報セキュリティポリシーに抵触しない範囲内で実施し、詳細なルール等については別途作成して周知します。
- 児童生徒の端末の持ち帰り、持込みで明らかになった課題を整理し、その結果を反映するかたちで情報セキュリティポリシーの変更を行います。

教育クラウドプラットフォームの要求機能仕様に関する標準仕様

平成 28 年 3 月 31 日

NTT コミュニケーションズ株式会社

目次

1. はじめに

この項目は参考資料である※

1.1 本ドキュメントの概要

教育クラウドプラットフォームの要求機能仕様に関する標準仕様（以下、本ドキュメント）は、総務省「先導的教育システム実証事業」の結果に基づき、教育クラウドプラットフォーム（以下、本プラットフォーム）および連携する各種機能を含めた全体システム（以下、本システム）の全体アーキテクチャ、データ要件、機能要件および非機能要件を定義する。

1.2 本ドキュメントの構成

本ドキュメントは、以下の内容から構成される

- システム要求：本ドキュメントで定義される各要件の前提となる要求について示す。
- 全体アーキテクチャ：本プラットフォーム全体の設計方針について示す。
- データ要件：本プラットフォームで取り扱うデータの要件について示す。
- 共通バックエンド：本プラットフォームのモジュール構成と、各モジュールの機能要件および非機能要件について示す
- サービスプロバイダ：本プラットフォームと連携するサービスに期待する機能要件について示す。

1.3 要求水準

本ドキュメントの要求水準とその表現とは、「しなければならない」(MUST)、「してはならない」(MUST NOT)、「必須である」(REQUIRED)、「するものとする」(SHALL)、「しないものとする」(SHALL NOT)、「すべきである」(SHOULD)、「すべきではない」(SHOULD NOT)、「推奨される」(RECOMMENDED)、「してもよい」(MAY)、および「任意である」(OPTIONAL) は、RFC 2119 に記述に従って解釈される。

ただし、要求水準が指定される際は、表現に関わらず要求水準の指定に従う。例えば、以下の要件はMUSTとして取り扱う。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-1-2-3	MUST	校務情報は、課金機能に用いるため所属学校の情報が含まれる。

※本ドキュメントの記述について、項目全体が規定に関する補足的な説明である場合は、「この項目は参考資料である」と項目先頭に記載される。項目途中より規定に関する補足的な説明が記載される際は、「注記」と項目途中に記載される。また、この仕様のすべての「記述例」も補足的な説明である。

2. 主な前提仕様

この項目は参考資料である

2.1 APPLIC プラットフォーム通信標準仕様 V2.1

本仕様は以下を参照すること。

http://www.applic.or.jp/URN/APPLIC-0009-2010/APPLIC-0009-2010-01/APPLIC-0009-2010-01-02plat.pdf

2.2 APPLIC アーキテクチャ標準仕様 V2.0

本仕様は以下を参照すること。

http://www.applic.or.jp/APPLIC/2008/APPLIC-0006-2008/APPLIC-0006-2008-01/APPLIC-0006-2008-01-01.pdf

2.3 IEEE 1484.12.1 – 2002 Standard for Learning Object Metadata

本仕様は以下を参照すること。

http://dx.doi.org/10.1109/IEEESTD.2002.94128

2.4 Schema.org – Review

本仕様は以下を参照すること。

https://schema.org/Review

2.5 ATOM 配信フォーマット

本仕様は以下を参照すること。

https://www.ietf.org/rfc/rfc4287.txt

2.6 ATOM 出版プロトコル

本仕様は以下を参照すること。

https://www.ietf.org/rfc/rfc5023.txt

3. 用語

この項目は参考資料である

用語	説明
パーソナルデータ	実質的個人識別性を有する個人に関する情報
実質的個人識別性	プライバシーの保護というパーソナルデータの利活用の基本理念を踏まえて実質的に判断される個人識別性
ID プロバイダ（IdP）	利用者のアイデンティティ登録、クレデンシャルを発行する期間のこと。ID プロバイダは、自身が運営する登録局（Registration Authorities）及び検証者を含んで良い。
リライング・パーティ（RP）	アイデンティティのアサーションやクレームに依存する主体
アトリビュート・プロバイダ（AtrP）	利用者の依頼により、利用者に関する属性情報を提供する。または、集約し、一元管理する主体。属性情報の提供には、IdP を中継して RP へ提供する方法と IdP を中継せず直接 RP へ提供する方法がある。
シングルサインオン（SSO）	認証を必要とする複数のアプリケーションを使用する際、一度だけ認証を行うことで、許可されているすべてのシステムを利用できるようにするもの。
トラストフレームワーク	アイデンティティ情報を交換する当事者に対する要求とその要求を強制する枠組み。
機密性	認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性。
完全性	資産の正確さ及び完全さを保護する特性。
可用性	認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。
権威ある源泉	学校や会社などの信頼性の高い情報源。
同意情報	個人識別可能情報を利用する組織が取得する利用者本人または適切な代理人の同意。
アクセス制御	アクセス制御とは，情報資源の不正利用を防止するために，決められた規則に従って資源へのアクセスを制限することである。
アクセス要求	主体がオブジェクトに対して実行したい操作
オブジェクト	アクセスを受ける受動的な実体
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
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
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
学習成果物	学習記録の一つであり、例えば、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を指すときに用いる
アクセス制御執行機能（AEF）	あるアクセス要求に対する ADF による判定結果を執行する機能
アクセス制御決	利用許諾条件と同意情報に従って、アクセス要求元の個人属性や環境情報を元にアクセスの可

定機能（ADF）	否を決定する機能
サービスプロバイダ（SP）	RP のうち教材コンテンツ・マーケットプレイス・データストアなどの ASP・SaaS のこと
Software as a Service（SaaS）	アプリケーションやデータベースをサービスとして提供するクラウドサービス。
Backend as a Service（BaaS）	SaaS に対して認証機能や配信機能などの汎用機能を提供するクラウドサービス
コンテンツ	著作権によって保護される教材コンテンツ、学習指導案、活用方法の総称
教材コンテンツ	発表・表示、道具・実習、実験観察・体験などの学習サービスを提供するコンテンツ
学習指導案	授業単位の授業シナリオ
活用方法	教育ＩＣＴ活用事例集などの教材コンテンツの活用に関する情報コンテンツ
（Universally Unique Identifier）UUID	オブジェクトを一意に識別するための識別子
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校務分野の ASP･SaaS を提供する形態であり、いわゆる一般的な民間 ASP･SaaS 事業者により、サービス提供が行われるものである。
Learning Object Metadata（LOM）	教育に関するコンテンツのためのメタデータ仕様
有害情報	インターネットを利用して公衆の閲覧（視聴を含む。以下同じ。）に供されている情報であって青少年の健全な成長を著しく阻害するもの
コンテンツ評価	任意のコンテンツに対して作成された定量的または定性的な評価情報のこと
Experience API（xAPI）	学習活動の履歴を記録・検索・抽出するため記録データフォーマットおよびデータ通信プロトコル仕様

4. システム要求

この項目は参考資料である

4.1 システム要求の概要

本プラットフォームの要件定義の対象となる要求は、「公教育向けプラットフォームの在り方」および「本事業のプラットフォーム開発方針」に基づき「要求一覧」に定義する。

4.2 公教育向けプラットフォームの在り方

1. 多種多様なコンテンツを自由に選択し、多様な学びを行うことができる

- いつでも、どこでも、だれでも学ぶことが可能
- 一人一人の個性・能力・意欲に応える学びを実現
- 課題の発見・解決に向けた主体的・協働的な学びを実現

2. 全国へ普及可能な技術・費用により、教育の情報化を推進する

- クラウドサービスを用いて導入・運用の容易・簡便化と費用低減を実現
- モジュール化とオープンアーキテクチャの活用による健全な競争環境の実現
- 公教育・私教育・他分野等の連携による社会インフラの最適化とコスト削減

3. 標準化によるデータ連携がもたらす新たな価値創出と教育エコシステムの実現

- コンテンツの増加と流通促進による学習・教育環境の向上と市場の活性化
- 学習記録データの利活用による学びの高度化とデータ利用機会の創出
- 教育分野以外（防災・医療等）とのデータ連携による新たな価値の創出

4.3 本事業のプラットフォーム開発方針

- プラットフォームの運営に必要とされる国の予算を最小限とし、民間のビジネスベースとして自走が可能なモデルとすること
- 新規事業者（EdTech事業者など）が参入しやすいオープンなプラットフォームであること
- 全国への普及を前提に、教育委員会や学校がプラットフォームを導入する際、従来よりトータルコストが低いモデルであること
- 今後の技術の発展を柔軟に取り込めるよう、国際規格やオープンな技術に依拠した技術標準（共通仕様）とすること
- 教育クラウドプラットフォームに関する技術標準（共通仕様）を用いて、ベンダーロックインを排除し、健全な競争環境とすること

4.4 要求一覧

4.4.1 要求の概要

この項目は参考資料である

要件定義の対象とするべき要求は、次に示す1つのビジネス要求と4つのユーザ要求により定義される。

- ビジネス要求
  - 共通バックエンドの運営に関するビジネス要求
- ユーザ要求
  - 学習活動の利活用に関するユーザ要求
  - 利便性や周辺機能に関するユーザ要求
  - 本システムの調達と運用に関するユーザ要求
  - コンテンツ販売に関するユーザ要求

各要求の主語となるユーザの定義は、以下に定義する。

- 共通バックエンド提供事業者：共用データレポジトリ、AtrP、Authz Providerを提供する事業者
- 学習者：児童生徒を含む学習サービスの利用者
- 教員：学校の教授、助教授、教頭、教諭、助教諭、養護教諭、養護助教諭、栄養教諭、常勤講師
- 保護者：親権者または未成年後見人
- 学校：幼稚園、小学校、中学校、高等学校、大学、専修学校、インターナショナルスクールなどの教育機関
- 教育委員会：地方教育行政のための数人の教育委員からなる合議制機関および事務局
- サービス事業者：サービスプロバイダの運営事業者
- 私教育提供事業者：学校教育と連携する学習塾や予備校などの私的な教育機会の提供事業者
- 研究者・他分野の団体等：教育分野の研究者および保健医療や行政などの隣接分野の団体

4.4.2 BIZ：共通バックエンドの運営に関するビジネス要求

要件種別	要件番号	要求水準	内容
要求	MIC-REQ-BIZ-1	MUST	共通バックエンド提供事業者は、コンテンツ提供者の事業規模（資本金・社員数・売上・利益など）で連携するサービス提供事業者を拒絶することがないバックエンド型プラットフォームサービスを提供したい
要求	MIC-REQ-BIZ-2	MUST	共通バックエンド提供事業者は、フロントエンドがウェブブラウザかつバックエンドがパブリッククラウドのみで構成可能なシステムを実現したい
要求	MIC-REQ-BIZ-3	MUST	共通バックエンド提供事業者は、国際規格やオープンな技術に依拠した技術標準を作成したい

4.4.3 LEA：学習活動の利活用に関するユーザ要求

要件種別	要件番号	要求水準	内容
要求	MIC-REQ-LEA-1	SHOULD	教員と学校と私教育提供事業者は、学習者の学習状況を任意のタイミングで把握したい
	理由	学習記録データを任意のタイミングで集計・分析・閲覧することにより、授業の理解度を把握することができる。これにより学習者の理解度を把握し授業進行の品質を向上させるため	
要求	MIC-REQ-LEA-2	SHOULD	教員と学校と教育委員会と私教育提供事業者は、蓄積された学習者の情報より学習者の学習状況を分析的に把握したい
	理由	エビデンスドベースドの学習環境を整備し、授業・学校経営を改善するため。また、学習記録を集計・分析・閲覧することにより、子どもの理解度や達成度を的確に把握し、また弱点やその克服方法を明らかにすることができるため。	
要求	MIC-REQ-LEA-3	SHOULD	サービス提供事業者と私教育提供事業者と研究者・他分野の団体等は、利用認可された学習記録データを教材制作や教育研究に活用したい
	理由	全国規模でデータを俯瞰する事による科学的根拠に基づく改善活動や様々なデータ利活用を行うため。また、学習記録データを分析し、コンテンツ内容の利用状況や理解度、例題の正答率等に基づいて問題点を把握することにより、コンテンツ内容の改善や例題の差替え、その他コンテンツをより活用できるように改善することができるため。	
要求	MIC-REQ-LEA-4	SHOULD	学習者と教員と保護者と学校と教育委員会は、教材コンテンツや学習状況に対する学習者自身や他者からの評価を共有したい
	理由	学習の理解度を共有することで、評価尺度（広義の学力）に対しての充足・不足の項目を把握し、学習環境改善やコンテンツ改善などを行うため	
要求	MIC-REQ-LEA-5	MUST	学習者と教員と保護者は、学習者の個性・能力・意欲に応じた教材コンテンツを利用したい
	理由	ICT を用いた効果的な個別学習を実現するため	
要求	MIC-REQ-LEA-6	MUST	教員と保護者と学校と教育委員会は、教育方針や ICT 環境に応じた教材コンテンツを利用したい
	理由	コンテンツの選択と組み合わせを行うことで、それぞれの学習環境に応じた適切な学習を提供するため	
要求	MIC-REQ-LEA-7	SHOULD	教員は、提供されるコンテンツの全部、または一部を利用し、担当する学習者に即したコンテンツを作成・提供したい
	理由	コンテンツをカスタマイズすることで、より効果的な教材を利用した授業を実施するため	

4.4.4 UTL：利便性や周辺機能に関するユーザ要求

要件種別	要件番号	要求水準	内容
要求	MIC-REQ-UTL-1	MUST	教員と学校と教員委員会は、他の教員や学校と情報交換を行いたい
	理由	指導方法や自作コンテンツを共有することで教員の負荷削減に貢献できるため	
要求	MIC-REQ-UTL-2	MUST	教育委員会は、教員が学校内外の校務環境に依存せず学習準備を行えるようにしたい
	理由	自宅環境などからでも学習準備を可能にすることで、教員の負荷削減に貢献できるため	
要求	MIC-REQ-UTL-3	MUST	教育委員会は、教材の利用と授業展開について事前にレコメンドを行えるシステムを教員に提供したい
	理由	品質の高い授業を可能にする教室環境を整備したいため	
要求	MIC-REQ-UTL-4	MUST	教育委員会は、教材の利用と授業展開について任意のタイミングでレコメンドを行えるシステムを教員に提供したい
	理由	教員の負荷削減のため	
要求	MIC-REQ-UTL-5	MUST	学習者と教員は、時間と場所に依存せずコンテンツを利用したい
	理由	教室内の学習を家庭や塾やその他任意の学習空間と連携することで新たな学びを実現するため。また、自宅環境などからでも学習準備を可能にすることで、教員の負荷削減に貢献できるため。	
要求	MIC-REQ-UTL-6	MUST	学習者と教員は、十分に簡易な利用手続きでコンテンツを利用したい
	理由	本システムのユーザは、学習者および教員であり、十分に簡易な UX を実現できなければ実用が困難であるため	
要求	MIC-REQ-UTL-7	MUST	学習者と教員は、学習過程に必要なデータ（学習記録データ等）を異なる学習環境で相互運用したい
	理由	教室内の学習を家庭や塾やその他任意の学習空間と連携することで新たな学びを実現するため。また、学校内外の学習過程を異なる環境に引き継ぎたいため。	
	説明	学習過程は、学習記録データとして記録されることとする。	

4.4.5 LGS：本システムの調達と運用に関するユーザ要求

要件種別	要件番号	要求水準	内容
要求	MIC-REQ-LGS-1	MUST	学校と教育委員会は、自治体が定める制度（入札等）に即したコンテンツ調達がしたい
	理由	本システムを学校に導入する際は、自治体が定める調達を行う必要があるため	
	説明	本システム要求ではないためスコープ外	
要求	MIC-REQ-LGS-2	MUST	教育委員会は、所属学校が利用するコンテンツを教育委員会で一括購入したい
	理由	学校の予算と教育委員会の予算が異なる管理であるため	
要求	MIC-REQ-LGS-3	MUST	学校は、学校配当予算の範囲で必要なコンテンツを選択したい
	理由	各学校の実情に合わせたコンテンツ利用を行えるようにするため	

要求	MIC-REQ-LGS-4	MUST	学校と教育委員会は、学期単位など任意の期間で利用できる契約形態でのコンテンツを購入したい
	理由	教材として利用期間が限定的である場合があるため	
要求	MIC-REQ-LGS-5	SHOULD	学校と教育委員会は、コンテンツの内容を購入前に試用などで確認したい
	理由	品質の確認および授業準備などに利用したいため	
要求	MIC-REQ-LGS-6	MUST	学校と教育委員会は、不適切なコンテンツを除外する仕組みを有するシステムを導入したい
	理由	利用者の安全のため	
要求	MIC-REQ-LGS-7	MUST	学校と教育委員会は、認証基盤などを既に保有する場合、本システムを既存システムと連携したい
	理由	学校や教育委員会が既に独自で導入した本システムを有効活用するため	
要求	MIC-REQ-LGS-8	MUST	学校と教育委員会は、異なるサービス事業者のソリューションを自由に組み合わせたい
	理由	特定の事業者のソリューションに限定されないため	
要求	MIC-REQ-LGS-9	MUST	学校と教育委員会は、不具合発生時に学習現場の担当者が復旧対応を可能なシステムを導入したい
	理由	学校と教育委員会は、管理・運用に専門知識が必要となる ICT 機器（サーバ等）を学校で管理・運用したくないため	
要求	MIC-REQ-LGS-10	SHOULD	学校と教育委員会は、稼働率などが明示されており、可用性の高い本システムが欲しい
	理由	授業に用いる本システムは、信頼性が十分に高くなければ利用できないため	
要求	MIC-REQ-LGS-11	MUST	学校と教育委員会は、国・自治体等で定められた規定に基づき、適切なデータ管理・運用を簡便に行いたい
	理由	パーソナルデータに関する規定は、各自治体で定められる条例に従うため	

4.4.6 MKT：コンテンツ販売に関するユーザ要求

要件種別	要件番号	要求水準	内容
要求	MIC-REQ-MKT-1	MUST	サービス提供事業者は、全国の教育委員会・学校のコンテンツ購入者に対し、コンテンツを確認してもらえる機会を作りたい
	理由	販売機会拡大のため	
要求	MIC-REQ-MKT-2	MUST	サービス提供事業者は、提供するコンテンツの活用事例などを、全国の教育委員会・学校に共有したい
	理由	サービス提供事業者は、全国の教育委員会・学校のコンテンツ購入者に対し、コンテンツを確認してもらえる機会を作りたい	
要求	MIC-REQ-MKT-3	MUST	サービス提供事業者は、販売・流通網の優劣ではなく、コンテンツの価値と価格で選択されたい
	理由	サービス提供事業者の、資本関係や企業規模による囲い込みを行わないようにするため	
要求	MIC-REQ-MKT-4	MUST	サービス提供事業者は、提供する教材コンテンツのメタデータ管理や提供を外部に委託したい

5. 全体アーキテクチャ

5.1 全体アーキテクチャの構成要件

全体アーキテクチャの構成要件を以下に示す。

要件種別	要件番号	要求水準	内容
構成要件	MIC-PACK-BIZ-1-1-1	MUST	共通バックエンドは、「個人認証機能」や「トラストフレームワーク機能」を有する Id プロバイダ（IdP）を有する
構成要件	MIC-PACK-BIZ-1-1-2	MUST	共通バックエンドは、校務情報や IdP アカウント ID などの属性情報の管理機能を有する校務 AtrP を有する
構成要件	MIC-PACK-BIZ-1-1-3	MUST	共通バックエンドは、パーソナルデータとコンテンツで構成されるアクセス制御対象オブジェクトへのアクセス制御を行うアクセス認可プロバイダー（Authz Provider）を有する。
構成要件	MIC-PACK-BIZ-1-1-4	MUST	本システムは、学習記録データ等のパーソナルデータや自作コンテンツ等のアクセス制御対象オブジェクトを管理する「アクセス制御対象オブジェクト管理機能」を有するサービスプロバイダを 1 つ以上連携する
構成要件	MIC-PACK-BIZ-1-2-1	MUST	共通バックエンドは、課金機能を提供する「マーケットプレイスサービスプロバイダ」を 1 つ以上連携する
構成要件	MIC-PACK-BIZ-1-2-7	MUST	共通バックエンドは、コンテンツ提供機能を有する「コンテンツサービスプロバイダ」または「マーケットプレイスサービスプロバイダ」を1つ以上連携する
構成仕様	MIC-PACK-BIZ-1-3-1	MUST	共通バックエンドは、複数のコンテンツサービスプロバイダに対してコンテンツメタデータやコンテンツ評価の提供を行う「共有データレポジトリ」を有する。
構成仕様	MIC-PACK-BIZ-1-5-1	MUST	共通バックエンドは、共通バックエンド全体のパフォーマンスログと監査イベント情報を統合的に管理する「Auditレポジトリ」を有する。
構成要件	MIC-PACK-BIZ-2-1	MUST	本システムは、フロントエンドにウェブブラウザのみで実現できること
構成要件	MIC-PACK-BIZ-2-2	MUST	本システムは、バックエンドがパブリッククラウドのみで実現できること
構成要件	MIC-PACK-LGS-8-1	MUST	本システムは、異なる事業者によって運営されるドメインの異なるサービスを連携させることができる

注記

本プラットフォームは、各SPにバックエンドサービスを提供するBaaSとしてアーキテクチャを定義する。IdPおよびAuthz Providerは、汎用化された外部サービスによって本プラットフォームの構成要素とすることを想定する。校務システム、NTPおよび利用者端末は、本プラットフォームの範囲には入らないこととする。

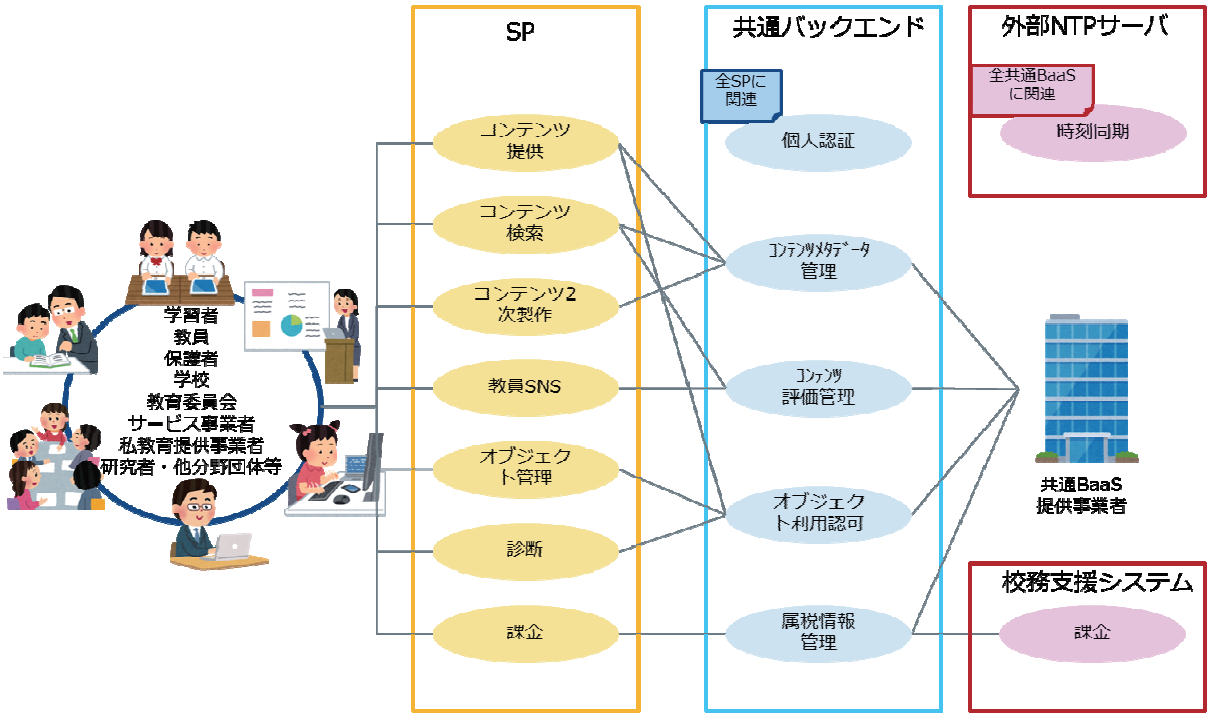


図 5-1 UC図

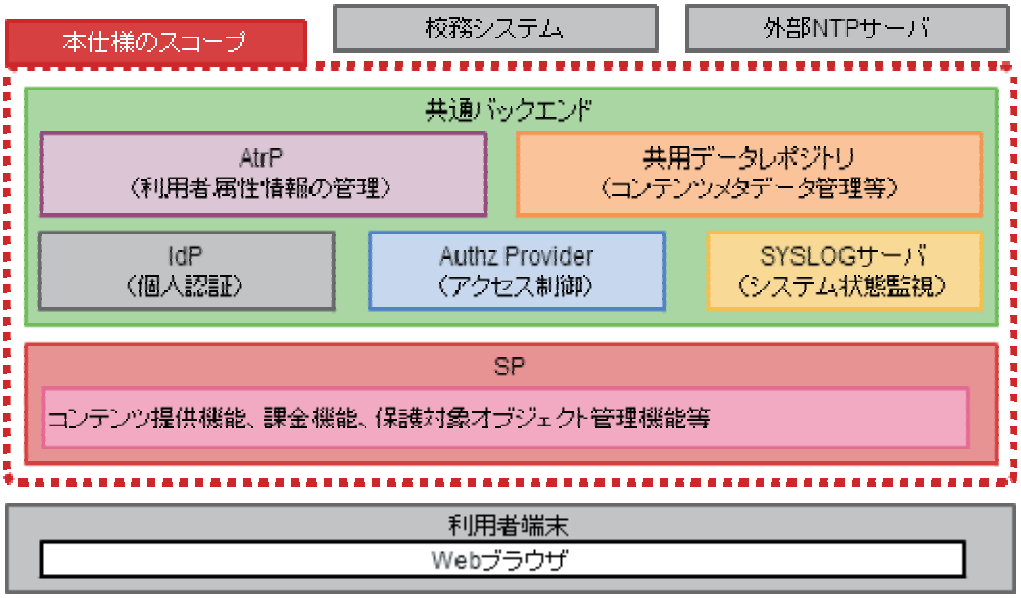


図 5-2 概念図

5.2 アーキテクチャおよび技術標準の採用方針

アーキテクチャおよび技術標準の採用方針を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-3-1	MUST	本システムに用いるデータのデータバインドは、国際標準化団体により策定・議論されている規格を用いること。また、本事業でデータバインドの独自拡張等を行う際は、これを公開しなければならない。
非機能要件	MIC-NONF-BIZ-3-2	MUST	本システムに用いるデータ通信プロトコルは、国際標準化団体により策定・議論されている規格を用いること。また、本事業でデータ通信プロトコルの独自拡張等を行う際は、これを公開しなければならない。

5.3 利用者端末要件

利用者端末要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-2-1-1	SHOULD	フロントエンドに iOS 端末を用いる際は、OS バージョンを 7 以降とし、ウェブブラウザは Safari の 7 以降とする
非機能要件	MIC-NONF-BIZ-2-1-2	SHOULD	フロントエンドに Android 端末を用いる際は、OS バージョンを 4.2 以降とし、ウェブブラウザは Chrome の 3.2 以降とする
非機能要件	MIC-NONF-BIZ-2-1-3	SHOULD	フロントエンドに Windows 端末を用いる際は、OS バージョンを 7 以降とし、ウェブブラウザは IE の 11 以降とする
非機能要件	MIC-NONF-BIZ-2-1-4	SHOULD	フロントエンド端末の画面サイズは、7 インチ以上とする
非機能要件	MIC-NONF-BIZ-2-1-5	SHOULD	フロントエンド端末の RAM は、32bit 機で 2GB 以上とし、64bit 機で 4GB とする

5.4 通信要件

通信要件を以下に示す。

要件種別	要件番号	要求水準	内容
通信要件	MIC-COMM-BIZ-3-2-1	MUST	SP は、利用者端末との通信に IPv4 を使用する。
通信要件	MIC-COMM-BIZ-3-2-2	MUST	SP は、利用者端末との通信に HTTP 1.1 を使用する。

通信要件	MIC-COMM-BIZ-3-2-4	MUST	共通バックエンドは、連携する SP との通信に IPv4 を使用する。
通信要件	MIC-COMM-BIZ-3-2-5	MUST	共通バックエンドは、連携する SP との通信に HTTP 1.1 を使用する。
通信要件	MIC-COMM-BIZ-3-2-3	MUST	SPは、利用者端末との通信に暗号強度128bit以上のTSL1.2通信による「セキュア通信機能」に対応する
通信要件	MIC-COMM-BIZ-3-2-6	MUST	共通バックエンドは、連携するSPとの通信に暗号強度128bit以上のTSL1.2通信による「セキュア通信機能」に対応する
通信要件	MIC-COMM-BIZ-3-2-7	MUST	共通バックエンドは、Auditレポジトリとの通信に、Syslogプロトコル（RFC5424）をSyslog Message over TLS（RFC5425）で仕様する。TLSのバージョンは1.2を推奨する。

注記

校務システムと校務AtrP間の通信要件については、「7.2.2.2 通信要件」に示すとおり、SSL3.0/TSL1.0通信の利用等を別途定義する。

6. データ要件

6.1 データ要件の概要

この項目は参考資料である

データ要件は、本プラットフォームで取り扱うデータの要件を定義する。

6.2 エンコーディング

本プラットフォームで取り扱うデータのエンコード要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-3-1-7	SHOULD	共通バックエンドで取り扱うデータのエンコーディングは、UTF-8 を用いる。
データ要件	MIC-DATA-BIZ-3-1-8	SHOULD	共通バックエンドで取り扱うデータは、BOM（Byte Order Mark）を使用しない。
データ要件	MIC-DATA-BIZ-3-1-9	SHOULD	共通バックエンドで取り扱うデータは、改行コードに”LF”を使用しない。

注記

校務システムおよびSPで取り扱うデータのエンコーディングについては、本ドキュメントで定義しない。

6.3 属性情報

6.3.1 IdP アカウント ID

平成28年度に検討予定

6.3.2 パスワード

平成28年度に検討予定

6.3.3 本人確認済み ID

本人確認済みIDの要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-1-2-4	MUST	属性情報は、IdPアカウントID、所属学校を有することとする。また、学校で本人確認がされて校務情報と紐付けられたIdPアカウントIDを本人確認済みIDとする。

6.3.4 校務情報

校務情報の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-1-2-3-5	MUST	校務情報は、課金機能に用いるため所属学校の情報が含まれる。

注記

校務情報および所属学校の具体的なデータ型およびメタデータは、校務情報システムの採用仕様に準拠するものとして、本ドキュメントでは定義しない。

6.3.5 教員の担当教科

教員の担当教科の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-UTL-1-1-3-1	MUST	属性情報は、教員の「担当教科」の項目を有する

注記

教員の担当教科の具体的なデータ型およびメタデータは、校務情報システムの採用仕様に準拠するものとして、本ドキュメントでは定義しない。

6.3.6 教員の勤続年数

教員の勤続年数の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-UTL-1-1-3-2	MUST	属性情報は、教員の「勤続年数」の項目を有する

注記

教員の勤続年数の具体的なデータ型およびメタデータは、校務情報システムの採用仕様に準拠するものとして、本ドキュメントでは定義しない。

6.4 アクセス制御対象オブジェクト

アクセス制御対象オブジェクトの要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-1-4-6	MUST	アクセス制御対象オブジェクトとは、Authz Providerのアクセス制御対象となる実体データとする

6.4.1 学習記録データ

学習記録データの要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-1-4-7	MUST	学習記録データとは、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とする
データ要件	MIC-DATA-UTL-7-2-1	OPTIONAL	学習記録データのデータフォーマットは、xAPI に準拠する

注記

学習記録データの定義は、「学びのイノベーション事業実証研究報告書 2-2, 3 学習記録データ」に準ずる。

6.4.2 コンテンツ

コンテンツの要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-3-2	MUST	コンテンツとは、教材コンテンツ、自作コンテンツ、学習指導案、活用方法の総称とする
データ要件	MIC-DATA-LEA-7-2-2	SHOULD	コンテンツは、コンテンツ自身に「コンテンツ利用許諾条件」を有する

注記

コンテンツ自身に「コンテンツ利用許諾条件」を持つ具体的な例としては、例えば、SPが利用許諾条件およびプライバシーポリシーを個別に運用する場合や、オフラインコンテンツ等に著作物利用許諾条件を添付する場合を想定する。

6.4.2.1 学習指導案

学習指導案の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-3-4	MUST	学習指導案とは、授業単位の授業シナリオである

6.4.2.2 活用方法

活用方法の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-3-5	MUST	活用方法は、教育ＩＣＴ活用事例集などの教材コンテンツの活用に関する情報コンテンツとする。

6.4.2.3 教材コンテンツ

教材コンテンツの要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-3-3	MUST	教材コンテンツとは、発表・表示用教材、道具・実習用具教材、実験観察・体験用教材として利用するコンテンツとする

6.4.2.4 自作コンテンツ

自作コンテンツの要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-LEA-7-2-6	MUST	2 次制作された教材コンテンツを含む自作コンテンツは、学習サービスとしてコンテンツメタデータ管理機能に登録することができることとする。

6.5 コンテンツメタデータ

コンテンツメタデータの要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-3-1-1-6	MUST	コンテンツメタデータとは、コンテンツの種別や動作環境、および著作権情報などを定義したデータとする。
データ要件	MIC-DATA-BIZ-1-3-1-1-6-1	MUST	LOM の教材コンテンツは、"5.2 Learning Resource Type"に対して「教材」の語彙で定義する
データ要件	MIC-DATA-BIZ-1-3-1-1-6-2	MUST	LOM の学習指導案は、"5.2 Learning Resource Type"に対して「学習指導案」の語彙で定義する
データ要件	MIC-DATA-BIZ-1-3-1-1-6-3	MUST	LOM の活用方法は、LOM の"5.2 Learning Resource Type"に対して「活用方法」の語彙で定義する
データ要件	MIC-DATA-BIZ-3-1-1	OPTIONAL	コンテンツメタデータの配信フォーマットは、ATOM配信フォーマットに準拠すること
データ要件	MIC-DATA-BIZ-3-1-2	MUST	コンテンツメタデータの項目は、LOMに準拠すること

6.5.1 学習指導要領番号

学習指導要領番号の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-LEA-5-5-1	MUST	コンテンツメタデータは、メタデータ項目に診断機能の結果への対応項目として、教材が対象とする「学習指導要領番号」または、「誤概念」の項目を有する
データ要件	MIC-DATA-LEA-5-5-1-1	OPTIONAL	LOM の学習指導要領番号は、"9.2.2 Taxon"に「gprcf」を設定し、"9.2.2.2 Entry"に学習指導要領メタデータを設定する

6.5.2 学習指導要領メタデータの概要

この項目は参考資料である

学習指導要領メタデータは、デジタル教科書コンテンツの単元、章、設問等の構成要素が学習指導要領に記された「各学年の目標及び内容」のいずれに対応しているかを特定するための付加情報として用いる。学習指導要領メタデータは、以下に示す要素によって構成される。

要素	例1	例2
学習指導要領 公示年度	小学校学習指導要領 （平成20年3月）	中学校学習指導要領 （平成20年3月、平成22年11月一部改正）
教科	算数	国語
学年	4年生	1年生
内容	A　数と計算 (1)　整数が十進位取り記数法によって表されていることについての理解を深める。 ア　億、兆の単位について知り、十進位取り記数法についてまとめること。	B　書くこと 書くことに能力を育成するため、次の事項について指導する。 エ　書いた文章を読み返し、表記や語句の用法、叙述の仕方などを確かめて、読みやすく分かりやすい文章にすること
メタデータ表記	H20-E02-J4-A-1-a	H22-H01-JH1-B-1-d

表 6-1　学習指導要領メタデータの要素

本メタデータは、コンテンツドキュメントのファイル全体および部分の block 要素に付与することができる。

6.5.3 学習指導要領メタデータの要素

6.5.3.1 学習指導要領公示年度

学習指導要領の版を特定するため、指導要領が公示された年度に関する情報を持つ。年号を示すアルファベット及び年度を示す数字。平成25年は、H25 となる。

6.5.3.2 教科または科目

教科名（科目名）を示す英数文字列により、教科コード（高校の場合は科目コード）を指定する。

6.5.3.3 学年

学校種別を示すアルファベット及び学年を示す数字により学年を指定する。小学校、中学校、高等学校は、それぞれE（Elementary School）、JH（Junior High School）、H（High School）とする。

6.5.3.4 内容

学習指導要領の各教科で記述された内容のどの箇所に対応した教材内容かを特定する。各教科の学年別の「目標及び内容」の、段落構成に対応する。段落構成は最大3階層とする。

第1階層は、大文字アルファベット（A、B、C、･･･）に対応する。大文字アルファベット以外に[ ]で

括られた記述がある場合は、A、B、等に引き続くアルファベットを適用する。A、B等の大文字アルファベットの項番が付与されていない場合は、第2階層から付与する。

第2階層：(1)、(2)等の項目についてカッコを除外した数字で表現する。

第3階層：(1)、(2)等の下の階層の項番（ア、イ、ウ、･･･）を、小文字アルファベットに置き換えて表現する（ア：a、イ：b、ウ：c、エ：d、オ：e）。

6.5.4 算数的な活動

算数的な活動の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-LEA-5-5-1	MUST	コンテンツメタデータは、メタデータ項目に診断機能の結果への対応項目として、教材が対象とする「学習指導要領番号」、「誤概念」、「算数的な活動」の項目を有する
データ要件	MIC-DATA-LEA-5-5-1-3	OPTIONAL	LOM の算数的な活動は、"9.2.2 Taxon"に「gprcf」を設定し、"9.2.2.2 Entry"に算数的な活動コードを設定する

注記

算数的な活動コードは、APPENDIXを参照すること。

6.5.5 誤概念

誤概念の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-LEA-5-5-1	MUST	コンテンツメタデータは、メタデータ項目に診断機能の結果への対応項目として、教材が対象とする「学習指導要領番号」または、「誤概念」の項目を有する
データ要件	MIC-DATA-LEA-5-5-1-2	MUST	LOM の誤概念は、"9.3 Taxon"に対応する誤概念の内容を自由記述により設定する

6.5.6 学年

学年の要件を以下に示す。

要件種別	要件番号	**要求水準**	内容
データ要件	MIC-DATA-LEA-6-1-1	MUST	教材コンテンツメタデータは、メタデータ項目に「学年」への対応項目を有する

データ要件	MIC-DATA-LEA-6-1-1-1	MUST	LOM の学年は、"5.7 Typical Age Range"に学年を設定する

6.5.7 教科

教科の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-LEA-6-1-2	MUST	教材コンテンツメタデータは、メタデータ項目に「教科」への対応項目を有する
データ要件	MIC-DATA-LEA-6-1-2-1	MUST	LOM の教科は、"9.2.2 Taxon"に「教科」を設定し、"9.2.2.2 Entry"に教科の種別を設定する

6.5.8 対応教科書

対応教科書の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-LEA-6-1-3	MUST	教材コンテンツメタデータは、メタデータ項目に「対応教科書」への対応項目を有する
データ要件	MIC-DATA-LEA-6-1-3-1	MUST	LOM の対応教科書は、"9.2.2 Taxon"に「教科書」を設定し、"9.2.2.2 Entry"に教科書の該当項目を設定する

6.5.9 動作条件

動作条件の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-LEA-6-2-2	MUST	教材コンテンツメタデータは、メタデータ項目に「動作条件」への対応項目を有する
データ要件	MIC-DATA-LEA-6-2-2-1	MUST	LOM の動作条件は、"4.4 Requirement"に動作条件内容を設定する

6.5.10 コンテンツ利用許諾条件

コンテンツ利用許諾条件の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-LEA-7-2-1	MUST	コンテンツメタデータは、メタデータ項目に「コンテンツ利用許諾条件」への対応項目を有する
データ要件	MIC-DATA-LEA-7-2-1-1	MUST	LOM のコンテンツ利用許諾条件は、"6.2 Copyright and Other Restiction"に利用許諾条件または利用許諾条件の参照先を設定する

6.5.11 コンテンツ識別子

コンテンツ識別子の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-UTL-3-7-1	MUST	コンテンツメタデータとコンテンツ評価は、対象コンテンツ実体情報への参照が可能な「コンテンツ識別子」を有する
データ要件	MIC-DATA-UTL-3-7-1-2	OPTIONAL	LOM のコンテンツ識別子は、"7.2.1.1 Catalog"に「コンテンツ識別子」を設定し、"7.2.1.2 Entry"にコンテンツ識別子の UUID を設定する

6.5.12 コンテンツメタデータ識別子

コンテンツメタデータ識別子の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-4-1-2	MUST	コンテンツメタデータは、対照のコンテンツに対応するメタデータの一式に対応した IRI である「コンテンツメタデータ識別子」を有する
データ要件	MIC-DATA-BIZ-1-4-1-2-1	MUST	LOM のコンテンツメタデータ識別子は、"3.1 Identifier"に対して UUID で定義する

6.6 コンテンツ評価

コンテンツ評価の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-3-1-4	OPTIONAL	コンテンツ評価の配信フォーマットは、ATOM配信フォーマットに準拠すること

データ要件	MIC-DATA-BIZ-3-1-5	MUST	コンテンツ評価の項目は、schema.orgに準拠すること

注記

ATOM配信フォーマットを利用した際の記述サンプルを以下に示す。

```
<?xml version="1.0" encoding="utf-8"?>
<feed xmlns="http://www.w3.org/2005/Atom">

  <title>Example Feed</title>
  <link href="http://example.org/"/>
  <updated>20XX-12-13T18:30:02Z</updated>
  <author>
    <name>John Doe</name>
  </author>
  <id>urn:uuid:60a76c80-d399-11d9-b93C-0003939e0af6</id>

  <entry>
    <title>Atom-Powered Robots Run Amok</title>
    <link href="http://example.org/2003/12/13/atom03"/>
    <id>urn:uuid:1225c695-cfb8-4ebb-aaaa-80da344efa6a</id>
    <updated>20XX-12-13T18:30:02Z</updated>
    <summary>Some text.</summary>
    <content type="application/xml" xmlns=” http://schema.org” >
        <reviewBody>レビュー文章</reviewBody>
        <reviewRating>
            <reviewValue>3</reviewValue>
        </reviewRating>
    </content>
  </entry>

</feed>
```

図 6-1 ATOM配信フォーマットを用いたコンテンツ評価の記述例

6.6.1 コンテンツ識別子

コンテンツ識別子の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-4-2-1	MUST	コンテンツ評価の評価対象は、schema.orgの"itemReviewed"で定義する
データ要件	MIC-DATA-UTL-3-7-1	MUST	コンテンツメタデータとコンテンツ評価は、対象コンテンツ実体情報への参照が可能な「コンテンツ識別子」を有する
データ要件	MIC-DATA-UTL-3-7-1-1	OPTIONAL	コンテンツ識別子は、UUID を用いる

6.6.2 評価文章

評価文章の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-4-2-2	MUST	コンテンツ評価の評価文章は、schema.orgの"reviewBody"で定義される

6.6.3 評価等級

評価等級の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-4-2-3	MUST	コンテンツ評価の評価等級は、schema.orgの"reviewRating"で定義される

6.7 アクセス制御情報

6.7.1 アクセス制御ポリシー

アクセス制御ポリシーの要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-1-3-7	MUST	アクセス制御ポリシーとは、利用許諾条件と同意情報から合成されるアクセス制御のルールとする
データ要件	MIC-DATA-BIZ-3-1-3	OPTIONAL	アクセス制御ポリシーのフォーマットは、XACML3.0 に準拠すること

6.7.2 利用許諾条件

利用許諾条件の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-1-3-8	MUST	利用許諾条件とは、コンテンツまたはパーソナルデータの権利者によって作成されるデータの利用条件とする

6.7.2.1 パーソナルデータ利用許諾条件

パーソナルデータ利用許諾条件の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-1-4-4-5	SHOULD	パーソナルデータ利用許諾条件は、アクセス制御対象オブジェクトの扱いをコンテンツに変更する際、または異なる国や地域の利用者に対して有償利用者の同意情報がそのまま利用できる「複数根拠法対応構造」を有する

注記

パーソナルデータ利用許諾条件は、経産省「消費者向けオンラインサービスにおける通知と同意・選択のためのガイドライン」に準拠して作成されることが望ましい。

6.7.2.2 コンテンツ利用許諾条件

コンテンツ利用許諾条件の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-1-3-3-5	MUST	利用許諾条件は、コンテンツに著作権者によりコンテンツ利用許諾条件が明示されない際、本システム内において適用される「コンテンツ利用許諾基本条件」を有する
データ要件	MIC-DATA-LGS-5-1	SHOULD	コンテンツ利用許諾条件は、「試用条件」を設定できることとする。
データ要件	MIC-DATA-BIZ-1-2-4	MUST	SP 個別運用利用許諾条件は、 1 ヵ月単位以下の期間の利用権利を管理できることとする
データ要件	MIC-DATA-BIZ-1-2-5	MUST	SP 個別運用利用許諾条件は、学校単位および教育委員会単位の属性情報に対応できることとする
データ要件	MIC-DATA-BIZ-1-2-6	MUST	SP 個別運用利用許諾条件は、教育委員会が保有するコンテンツ利用権利を所属学校で利用可能とする、ロールベースアクセス制御のためのロール情報を設定できることとする

注記

コンテンツ利用許諾基本条件は、本プラットフォームを用いたサービス定義の際に別途定義されることを想定する。

コンテンツ利用許諾条件は、クリエイティブ・コモンズにより定義される「クリエイティブ・コモンズ・ライセンス」に対応可能であることが望ましい。

参考：http://creativecommons.org/

6.7.3 同意情報

同意情報の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-1-3-9	MUST	同意情報とは、同意を必要とする利用許諾条件に対して利用者が同意した内容とする

注記

同意情報は、パーソナルデータとする。

同意情報は、利用許諾条件に対する明示的同意・非同意（オプトイン）と暗黙的非同意（オプトアウト）の情報を取り扱えることとする。また、利用許諾条件に依存せずに、「誰が・何を・誰に・どのような条件で」利用許諾するかを表現することができる。

6.8 監査イベント情報

監査イベント情報の要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-1-1-3-14	MUST	監査イベント情報は、「いつ」「誰が」「誰の」情報にアクセスしたかの情報を有する

注記

監査イベント情報は、「JAHIS IHE-ITIを用いた医療情報連携基盤実装ガイド 本編 ver.1.0」 および「 ヘルスケア分野における監査証跡のメッセージ標準規約 Ver1.1」を参考とする。

6.9 パフォーマンスログ

パフォーマンスログの要件を以下に示す。

要件種別	要件番号	要求水準	内容
データ要件	MIC-DATA-BIZ-3-1-6	MUST	パフォーマンスログのフォーマットは、RFC5424に準拠すること

7. 共通バックエンド

7.1 共通バックエンドの概要

この項目は参考資料である

共通バックエンドは、BaaS（Backend As a Service）として各SPに対して共通サービスを提供する本プラットフォームの実体である。共通バックエンドを構成するモジュールのうち、IdPおよびAuthz Providerは、本プラットフォームの独自仕様に依存せず、外部サービスとして調達可能な要件であることとする。

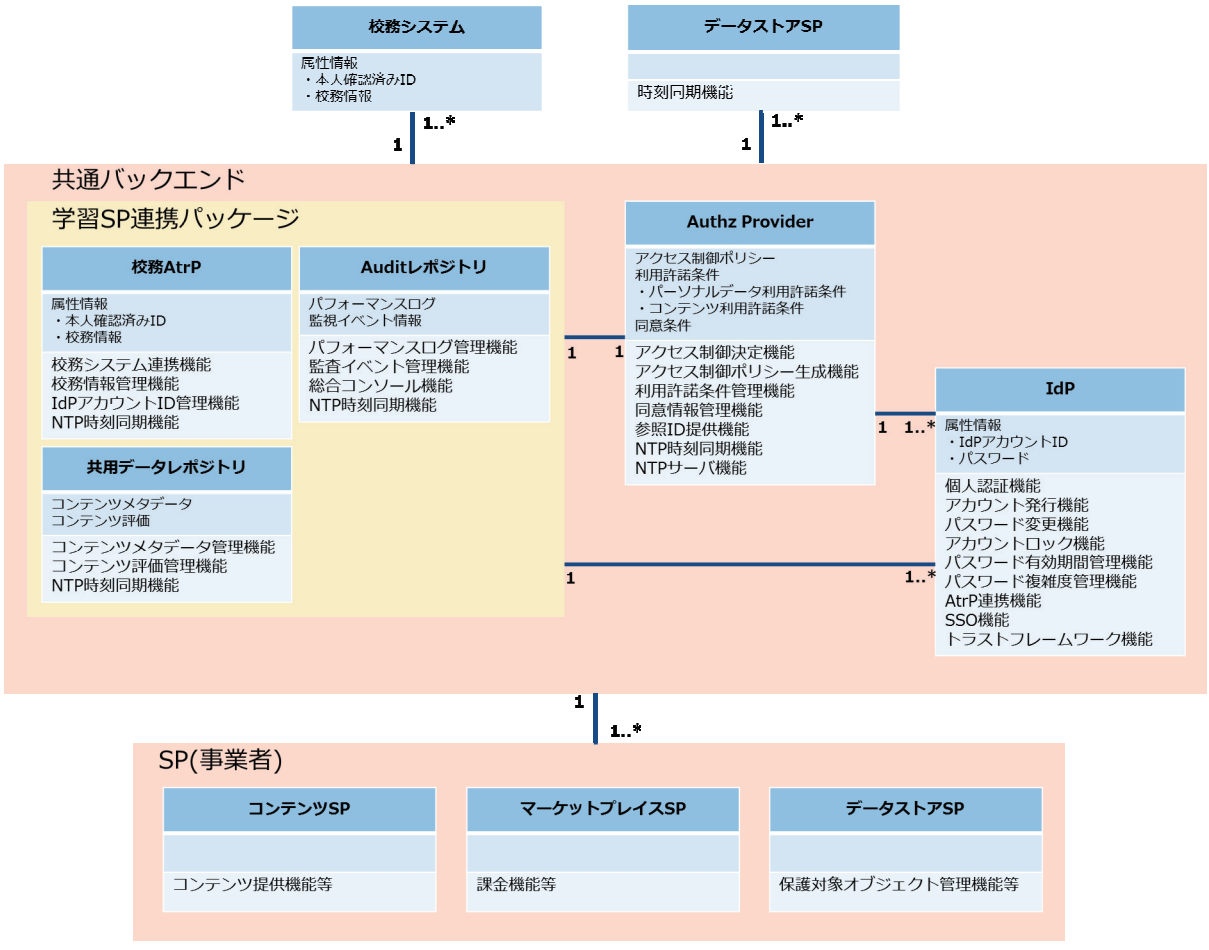


図 7-1　パッケージ図

7.2 校務 AtrP

7.2.1 校務 AtrP の概要

この項目は参考資料である

校務AtrPは、校務システムと連携し、校務情報から取得した属性情報を、SPが利用するためのモジュールである。本ドキュメントでは、校務システムの仕様については、校務システムの標準仕様であるAPPLIC プラットフォーム通信標準仕様およびアーキテクチャ標準仕様に準拠するものとし、同仕様の「統合DB機能」の「公開用DB方式」に基づくインタフェースを参考に要件を定義する。

このため、校務AtrPは、校務システムに対しては統合DBインタフェースを定義し、SPに対してはAtrP機能を定義する。

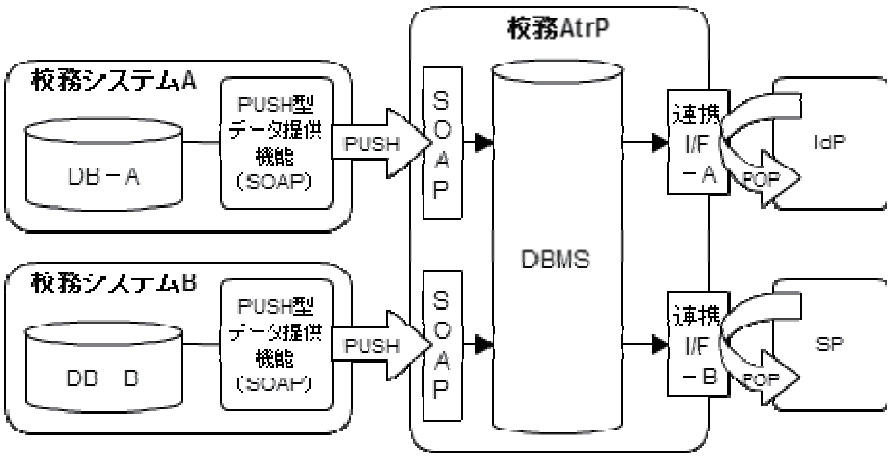


図 7-2　校務AtrPと他システム連携

7.2.2 統合 DB インタフェース要件

7.2.2.1 データ要件

データ要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-1-2-1-3	MUST	統合 DB インタフェースで交換されるメッセージである XML インスタンスは、プラットフォーム通信標準のメッセージ定義仕様における XML 定義仕様を満たすこと。
非機能要件	MIC-NONF-BIZ-1-1-2-1-4	MUST	統合 DB インタフェースは向けのサービスインタフェース定義の WSDL 定義は、プラットフォーム通信標 準のメッセージ定義仕様における WSDL の XML 定義要件を満たすこと。

非機能要件	MIC-NONF-BIZ-1-1-2-1-11	SHOULD	統合 DB インタフェースは、校務 AtrP と校務システムの間で交換されるデータの文字コードは UTF-8 または 16 を推奨する。

注記

本要件は、以下を参照すること

- APPLIC プラットフォーム通信標準仕様V2.1，3.2, 3.3
- APPLIC アーキテクチャ標準仕様V2.0，4.5.4

7.2.2.2 通信要件

通信要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-1-2-1-1	MUST	統合 DB インタフェースは、SOAP 1.1 を使用する。
非機能要件	MIC-NONF-BIZ-1-1-2-1-2	MUST	統合 DB インタフェースは、SOAP 通信は Basic Profile 1.0 に準拠すること。
非機能要件	MIC-NONF-BIZ-1-1-2-1-10	MUST	統合 DB インタフェースは、校務システムに対し、校務 AtrP の DB 更新機能（PUSH 型データ提供機能）として SOAP のインタフェース を提供する必要がある。
非機能要件	MIC-NONF-BIZ-1-1-2-1-5	MUST	統合 DB インタフェースを使用する際は、SSL3.0/TSL サーバ 1.0 認証およびクライアント認証を使用する。
非機能要件	MIC-NONF-BIZ-1-1-2-1-6	MUST	統合 DB インタフェースを使用する際は、暗号強度 128bit 以上の SSL3.0/TSL1.0 通信による「セキュア通信機能」を使用する。

注記

本要件は、以下を参照すること

- APPLIC プラットフォーム通信標準仕様V2.1，2.3.1, 5.3.1, 5.3.2
- APPLIC アーキテクチャ標準仕様V2.0，4.5.4

7.2.2.3 メッセージ交換パターン

メッセージ交換パターンの要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-1-2-1-7	MUST	統合 DB インタフェースは、「リクエスト・レスポンス型同期型レスポンス」を使用する。

注記

本要件は、以下を参照すること

- APPLIC プラットフォーム通信標準仕様V2.1，6.2.1

7.2.2.4 障害通知

障害通知の要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-1-2-1-8	MUST	統合 DB インタフェースは、メッセージ送信側の MEP 処理系は、下位レベルで検知した障害が通知される。
非機能要件	MIC-NONF-BIZ-1-1-2-1-9	MUST	統合 DB インタフェースは、すべての即時対応処理により、開始側の業務ユニットに障害報告がされなければなら ない。

注記

本要件は、以下を参照すること

- APPLIC プラットフォーム通信標準仕様V2.1，6.3.3, 6.4

7.2.3 AtrP 機能要件

7.2.3.1 本人確認済み ID 管理機能

本人確認済みID管理機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能仕様	MIC-FUNC-BIZ-1-1-2-2	MUST	校務 AtrP は、校務システムにより本人確認された本人確認済み ID を管理する「ID 管理機能」を有する

機能要件	MIC-FUNC-BIZ-1-1-2-2-1	MUST	ID 管理機能は、校務情報および本人確認済み ID を登録する「本人確認済み ID 登録機能」を有する
機能要件	MIC-FUNC-BIZ-1-1-2-2-2	MUST	ID 管理機能は、本人確認済み ID から所属学校などの校務情報を参照する「校務情報参照機能」を有する
機能要件	MIC-FUNC-BIZ-1-1-2-2-3	MUST	ID 管理機能は、本人確認済み ID と校務情報を削除する「本人確認済み ID 削除機能」を有する

注記

ID管理機能で管理されるIDは、校務システム経由で本人確認がされるものとする。ただし、校務情報管理機能は、本人確認情報を保持しないため、ID更新機能は有さない。

IDの本人確認は、

- 校務システムがIdPアカウントを予め取得し、学習者に配布する
- 学習者が保持するIdPアカウントに対し校務システムがIdPに対して個人認証をする

上記、いずれかの方法で関連付けされるものとする。

7.2.4 非機能要件

7.2.4.1 可用性

7.2.4.1.1 稼働率

稼働率の要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-1-2-6	MUST	校務 AtrP の稼働率は、授業時間中に関しては数分以上の停止を許容しない。ただし、授業時間外に関してはこの限りではない。
非機能要件	MIC-NONF-BIZ-1-1-2-6-1	MUST	授業時間を 7 時から 18 時とし、授業時間中の稼働率は、99.99%とする
非機能要件	MIC-NONF-BIZ-1-1-2-6-2	MUST	授業時間外の稼働率は、99.9%とする

7.2.4.2 性能・拡張性

拡張性の要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能	MIC-NON	MUST	校務 AtrP の拡張性は、自治体の方針変更によるユーザの大量増減に対応するため、

要件	F-BIZ-1-1-2-8		柔軟な拡張性を有さなくてはならない。

7.2.4.2.1 オンラインレスポンス

オンラインレスポンスの要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-1-2-7	MUST	校務 AtrP のオンラインレスポンスは、授業時間中に関しては大規模同時アクセスに対する十分な性能を確保しなくてはならない。ただし、授業時間外に関してはこの限りではない。
非機能要件	MIC-NONF-BIZ-1-1-2-7-1	MUST	授業時間を 7 時から 18 時とし、授業時間中の稼働率は、99.99%とする
非機能要件	MIC-NONF-BIZ-1-1-2-7-2	MUST	授業時間外の稼働率は、99.9%とする

7.2.4.3 運用・保守性

7.2.4.3.1 運用監視

運用監視の要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-1-2-9	MUST	校務 AtrP の運用監視は、Audit レポジトリによるパフォーマンス監視に対応する

7.2.4.4 セキュリティ

7.2.4.4.1 利用制限

利用制限の要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-1-2-10	MUST	校務 AtrP の利用制限は、学習者、教員、保護者などのロールに、上位下位の権限設定ができる「ロールベースアクセス管理機能」を有する

7.2.4.4.2 不正監視

不正監視の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-2-11	MUST	校務 AtrP は、任意の NTP サーバと時刻同期を行う「NTP 時刻同期機能」を有する
非機能要件	MIC-NONF-BIZ-1-1-2-2-1-1	MUST	本人確認済みID登録機能の不正監視は、本人確認済みID登録機能の実行時に監査イベントデータを生成し、Auditレポジトリに送信する
非機能要件	MIC-NONF-BIZ-1-1-2-2-2-1	MUST	校務情報参照機能の不正監視は、校務情報参照機能の実行時に監査イベントデータを生成し、Auditレポジトリに送信する
非機能要件	MIC-NONF-BIZ-1-1-2-2-3-1	MUST	本人確認済みID削除機能の不正監視は、本人確認済みID削除機能の実行時に監査イベントデータを生成し、Auditレポジトリに送信する

7.3 共用データレポジトリ

7.3.1 共用データレポジトリの概要

この項目は参考資料である

共用データレポジトリは、コンテンツメタデータとコンテンツ評価の集積と配布を行う。このモジュールで取り扱う情報は、トラストフレームワーク内において共有情報として取り扱えるものとする。

7.3.2 機能要件

7.3.2.1 コンテンツメタデータ管理機能

コンテンツメタデータ管理機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能仕様	MIC-FUNC-BIZ-1-3-1-1	MUST	共用データレポジトリは、複数のコンテンツサービスプロバイダに対してコンテンツメタデータの収集と提供を行う「コンテンツメタデータ管理機能」を有する
機能仕様	MIC-FUNC-BIZ-1-3-1-3	OPTIONAL	コンテンツメタデータ管理機能は、ATOM出版プロトコルを用いる

7.3.2.1.1 コンテンツメタデータ登録機能

コンテンツメタデータ登録機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-3-1-1-1	MUST	コンテンツメタデータ管理機能は、コンテンツメタデータの登録を行う「コンテンツメタデータ登録機能」を有する
機能要件	MIC-FUNC-BIZ-1-3-1-1-1-1	MUST	コンテンツメタデータ登録機能は、登録するメタデータにコンテンツ利用許諾条件が含まれていた際は、利用許諾条件を Authz Provider へ登録処理を行い、登録結果を登録者に通知する。

7.3.2.1.2 コンテンツメタデータ取得機能

コンテンツメタデータ取得機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-3-1-1-2	MUST	コンテンツメタデータ管理機能は、コンテンツメタデータの取得を行う「コンテンツメタデータ取得機能」を有する

7.3.2.1.3 コンテンツメタデータ更新機能

コンテンツメタデータ更新機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-3-1-1-3	MUST	コンテンツメタデータ管理機能は、コンテンツメタデータの更新を行う「コンテンツメタデータ更新機能」を有する
機能要件	MIC-FUNC-BIZ-1-3-1-1-3-1	MUST	コンテンツメタデータ更新機能は、更新するメタデータにコンテンツ利用許諾条件が含まれていた際は、利用許諾条件を Authz Provider へ更新処理を行い、更新結果を登録者に通知する。

7.3.2.1.4 コンテンツメタデータ削除機能

コンテンツメタデータ削除機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-3-1-1-4	MUST	コンテンツメタデータ管理機能は、コンテンツメタデータの削除を行う「コンテンツメタデータ削除機能」を有する

7.3.2.2 コンテンツ評価管理機能

コンテンツ評価管理機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能仕様	MIC-FUNC-BIZ-1-3-1-2	MUST	共用データレポジトリは、複数のサービスプロバイダに対してコンテンツ評価の収集と提供を行う「コンテンツ評価管理機能」を有する
機能仕様	MIC-FUNC-BIZ-1-3-1-4	OPTIONAL	コンテンツ評価管理機能は、ATOM出版プロトコルを用いる

7.3.2.2.1 コンテンツ評価登録機能

コンテンツ評価登録機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-3-1-2-1	MUST	コンテンツ評価管理機能は、コンテンツ評価の登録を行う「コンテンツ評価登録機能」を有する

7.3.2.2.2 コンテンツ評価取得機能

コンテンツ評価取得機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-3-1-2-2	MUST	コンテンツ評価管理機能は、コンテンツ評価の取得を行う「コンテンツ評価取得機能」を有する

7.3.2.2.3 コンテンツ評価更新機能

コンテンツ評価更新機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-3-1-2-3	MUST	コンテンツ評価管理機能は、コンテンツ評価の更新を行う「コンテンツ評価更新機能」を有する

7.3.2.2.4 コンテンツ評価削除機能

コンテンツ評価削除機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-3-1-2-4	MUST	コンテンツ評価管理機能は、コンテンツ評価の削除を行う「コンテンツ評価削除機能」を有する

7.3.3 非機能要件

7.3.3.1 可用性

7.3.3.1.1 稼働率

稼働率の要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-3-6	MUST	共有データレポジトリの稼働率は、授業時間中に関しては数分以上の停止を許容しない。ただし、授業時間外に関してはこの限りではない。
非機能要件	MIC-NONF-BIZ-1-3-6-1	MUST	授業時間を 7 時から 18 時とし、授業時間中の稼働率は、99.99%とする
非機能要件	MIC-NONF-BIZ-1-3-6-2	MUST	授業時間外の稼働率は、99.9%とする

7.3.3.2 性能・拡張性

7.3.3.2.1 オンラインレスポンス

オンラインレスポンスの要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-3-7	MUST	共有データレポジトリのオンラインレスポンスは、授業時間中に関しては数分以上の停止を許容しない。ただし、授業時間外に関してはこの限りではない。
非機能要件	MIC-NONF-BIZ-1-3-7-1	MUST	授業時間を 7 時から 18 時とし、授業時間中の稼働率は、99.99%とする
非機能要件	MIC-NONF-BIZ-1-3-7-2	MUST	授業時間外の稼働率は、99.9%とする

7.3.3.3 運用・保守性

7.3.3.3.1 運用監視

運用監視の要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-3-8	MUST	共有データレポジトリの運用監視は、Audit レポジトリによるパフォーマンス監視に対応する

7.3.3.4 セキュリティ

7.3.3.4.1 利用制限

利用制限の要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-3-9	MUST	共有データレポジトリの利用制限は、学習者、教員、保護者などのロールに、上位下位の権限設定ができる「ロールベースアクセス管理機能」を有する

7.3.3.4.2 不正監視

不正取得の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-3-10	MUST	共有データレポジトリは、任意の NTP サーバと時刻同期を行う「NTP 時刻同期機能」を有する
非機能要件	MIC-NONF-BIZ-1-3-1-1-1-2	SHOULD	コンテンツメタデータ登録機能の不正監視は、コンテンツメタデータ登録機能の実行時に監査イベントデータを生成し、Auditレポジトリに送信する
非機能要件	MIC-NONF-BIZ-1-3-1-1-3-2	SHOULD	コンテンツメタデータ更新機能の不正監視は、コンテンツメタデータ更新機能の実行時に監査イベントデータを生成し、Auditレポジトリに送信する
非機能要件	MIC-NONF-BIZ-1-3-1-1-4-1	SHOULD	コンテンツメタデータ削除機能の不正監視は、コンテンツメタデータ削除機能の実行時に監査イベントデータを生成し、Auditレポジトリに送信する
非機能要件	MIC-NONF-BIZ-1-3-1-2-1-	SHOULD	コンテンツ評価登録機能の不正監視は、コンテンツ評価登録機能の実行時に監査イベントデータを生成し、Auditレポジトリに送信する

	1		
非機能要件	MIC-NONF-BIZ-1-3-1-2-3-1	SHOULD	コンテンツ評価更新機能の不正監視は、コンテンツ評価更新機能の実行時に監査イベントデータを生成し、Auditレポジトリに送信する
非機能要件	MIC-NONF-BIZ-1-3-1-2-4-1	SHOULD	コンテンツ評価削除機能の不正監視は、コンテンツ評価削除機能の実行時に監査イベントデータを生成し、Auditレポジトリに送信する

7.4 IdP

7.4.1 IdP の概要

この項目は参考資料である

IdPは、利用者に対しIDとパスワードの発行・管理を行い、教育クラウドプラットフォームにアクセスする者を認証するためのモジュールである

7.4.2 機能要件

7.4.2.1 個人認証機能

個人認証機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-1-1	MUST	IdP は、アクセスする主体を ID およびパスワード等により識別および認証する「個人認証機能」を有する
機能要件	MIC-FUNC-BIZ-1-1-1-1-1	SHOULD	個人認証機能の不正監視は、監査イベントデータを生成し、Auditレポジトリに送信する

7.4.2.2 アカウント発行機能

アカウント発行機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-1-14	MUST	IdPは、IDおよび初期パスワードを発行する「アカウント発行機能」を有する

7.4.2.3 校務 AtrP 連携機能

校務AtrP連携機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-1-6	OPTIONAL	IdP は、校務アトリビュート・プロバイダ（校務 AtrP）と連携して SP に属性情報の参照を提供する「校務 AtrP 連携機能」を有する

注記

SPが利用者の校務AtrPで管理される所属学校等を要求する際、IdPがその中継を行ってもよいこととする。ただし、本要件は、IdPに関する仕様に準拠するため今後変更の可能性がある。

7.4.2.4 パスワード変更機能

パスワード変更機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-1-2	SHOULD	IdP は、利用者自身がパスワードを変更できる「パスワード変更機能」を有する
機能要件	MIC-FUNC-BIZ-1-1-1-2-1	SHOULD	パスワード変更機能の不正監視は、監査イベントデータを生成し、Auditレポジトリに送信する

7.4.2.5 アカウントロック機能

アカウントロック機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-1-3	SHOULD	IdP は、一定回数以上のパスワード誤入力を検知した場合、自動的にアカウントをロックする「アカウントロック機能」を有する
機能要件	MIC-FUNC-BIZ-1-1-1-3-1	SHOULD	アカウントロック機能の不正監視は、監査イベントデータを生成し、Auditレポジトリに送信する

7.4.2.6 パスワード有効期間管理機能

パスワード有効期間管理機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FU	SHOULD	IdP は、パスワードに有効期間を授け、過去に使用したパスワードの利用を一定世

	NC-BIZ-1-1-1-4		代の間は使用不可とする「パスワード有効期間管理機能」を有する

7.4.2.7 パスワード複雑度管理機能

パスワード複雑度管理機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-1-5	SHOULD	IdP は、パスワードの長さや複雑さ（英数字等の組み合わせ）に一定の条件を設ける「パスワード複雑度管理機能」を有する

7.4.2.8 SSO 機能

SSO機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-1-7	MUST	IdP は、連携するサービスプロバイダ間で認証状態を共有する「SSO 機能」を有する

7.4.2.9 トラストフレームワーク機能

トラストフレームワーク機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-1-8	MUST	IdP は、連携するサービスプロバイダを事前に審査して登録する「トラストフレームワーク機能」を有する

7.4.3 非機能要件

7.4.3.1 可用性

7.4.3.1.1 稼働率

稼働率の要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-1-1-9	MUST	IdP の稼働率は、授業時間中に関しては数分以上の停止を許容しない。ただし、授業時間外に関してはこの限りではない。

非機能要件	MIC-NONF-BIZ-1-1-1-9-1	MUST	授業時間を 7 時から 18 時とし、授業時間中の稼働率は、99.99%とする
非機能要件	MIC-NONF-BIZ-1-1-1-9-2	MUST	授業時間外の稼働率は、99.9%とする

7.4.3.2 性能・拡張性

拡張性の要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-1-1-11	MUST	IdP の拡張性は、自治体の方針変更によるユーザの大量増減に対応するため、柔軟な拡張性を有さなくてはならない。

7.4.3.2.1 オンラインレスポンス

オンラインレスポンスの要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-1-1-10	MUST	IdP のオンラインレスポンスは、授業時間中に関しては大規模同時アクセスに対する十分な性能を確保しなくてはならない。ただし、授業時間外に関してはこの限りではない。
非機能要件	MIC-NONF-BIZ-1-1-1-10-1	MUST	授業時間を 7 時から 18 時とし、授業時間中の稼働率は、99.99%とする
非機能要件	MIC-NONF-BIZ-1-1-1-10-2	MUST	授業時間外の稼働率は、99.9%とする

7.4.3.3 セキュリティ

7.4.3.3.1 不正監視

不正監視の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-1-13	MUST	IdPは、任意のNTPサーバと時刻同期を行う「NTP時刻同期機能」を有する
非機能要件	MIC-NONF-BIZ-1-1-1-1-1	SHOULD	個人認証機能の不正監視は、監査イベントデータを生成し、Auditレポジトリに送信する

非機能要件	MIC-NONF-BIZ-1-1-1-2-1	SHOULD	パスワード変更機能の不正監視は、監査イベントデータを生成し、Auditレポジトリに送信する
非機能要件	MIC-NONF-BIZ-1-1-1-3-1	SHOULD	アカウントロック機能の不正監視は、監査イベントデータを生成し、Auditレポジトリに送信する

7.5 Authz Provider

7.5.1 Authz Provider の概要

この項目は参考資料である

Authz Providerは、個別のSPでアクセス制御の対象とならないコンテンツやパーソナルデータへのアクセス制御機能を認可機能として提供する。Authz Providerは、異なるSP間に認可機能を提供するため、認可の根拠となる利用許諾条件と同意情報を集中管理する。

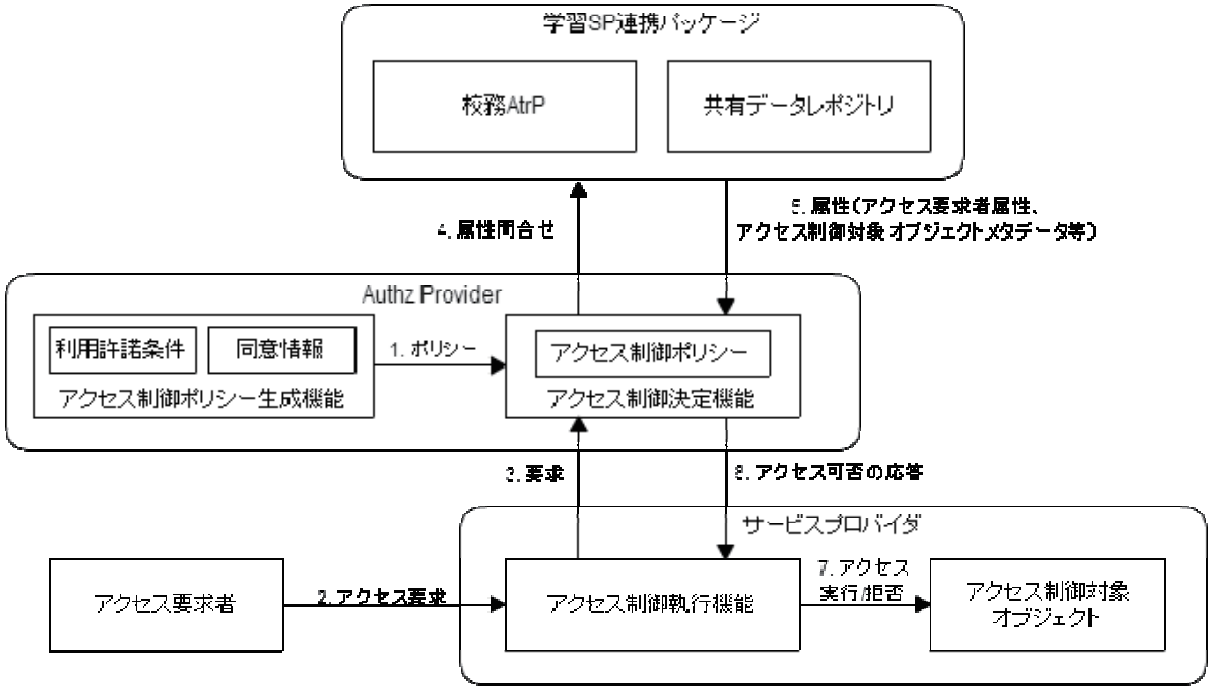


図 7-3 アクセス制御

7.5.2 機能要件

7.5.2.1 アクセス制御決定機能

アクセス制御決定機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-3-1	MUST	Authz Provider は、アクセス制御対象オブジェクト管理機能からアクセスされるパーソナルデータのアクセス要求に対して、アクセス制御ポリシーに従い許可または拒否の判定を行う「アクセス制御決定機能」を有する

7.5.2.2 アクセス制御ポリシー生成機能

アクセス制御ポリシー生成機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-3-2	MUST	Authz Provider は、利用許諾条件と同意情報よりアクセス制御ポリシーを生成する「アクセス制御ポリシー生成機能」を有する

7.5.2.3 利用許諾条件管理機能

利用許諾条件管理機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能仕様	MIC-FUNC-BIZ-1-1-3-3	MUST	Authz Provider 能は、「利用許諾条件」を管理する「利用許諾条件管理機能」を有する

7.5.2.3.1 利用許諾条件登録機能

利用許諾条件登録機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-3-3-1	MUST	利用許諾条件管理機能は、「利用許諾条件」の生成・継承関係の妥当性確認・保存を行う「利用許諾条件登録機能」を有する

注記

継承関係の妥当性確認とは、既存コンテンツの2次利用によって制作されたコンテンツの著作権が、既存コンテンツ側の利用許諾条件と整合することを確認することである。

7.5.2.3.2 利用許諾条件参照機能

利用許諾条件参照機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-3-3-2	MUST	利用許諾条件管理機能は、利用許諾条件管理機能が管理する「利用許諾条件」を参照する「利用許諾条件参照機能」を有する

7.5.2.3.3 利用許諾条件更新機能

利用許諾条件更新機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-3-3-3	MUST	利用許諾条件管理機能は、「利用許諾条件」を更新する「利用許諾条件更新機能」を有する

7.5.2.3.4 利用許諾条件削除機能

利用許諾条件削除機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-3-3-4	MUST	利用許諾条件管理機能は、「利用許諾条件」を削除する「利用許諾条件削除機能」を有する

7.5.2.4 同意情報管理機能

同意情報管理機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能仕様	MIC-FUNC-BIZ-1-1-3-4	MUST	Authz Provider は、利用許諾条件への同意情報を管理する「同意情報管理機能」を有する

7.5.2.4.1 同意情報登録機能

同意情報登録機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-3-4-1	MUST	同意情報管理機能は、学習者または保護者より利用許諾条件への同意情報を取得し、新規登録を行う「同意情報登録機能」を有する

7.5.2.4.2 同意情報参照機能

同意情報参照機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-3-4-2	MUST	同意情報管理機能は、学習者または保護者より同意情報の参照を行う「同意情報参照機能」を有する

7.5.2.4.3 同意情報更新機能

同意情報更新機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-3-4-3	MUST	同意情報管理機能は、学習者または保護者より同意情報の変更を行う「同意情報更新機能」を有する

7.5.2.4.4 同意情報削除機能

同意情報削除機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-3-4-4	MUST	同意情報管理機能は、学習者または保護者より同意情報の削除を行う「同意情報削除機能」を有する

7.5.2.5 参照 ID 提供機能

参照ID提供機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-3-6	MUST	Authz Provider は、名寄せのための「参照 ID 提供機能」を有する

7.5.2.6 統合管理 UI 機能

統合管理UI機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-3-15	SHOULD	Authz Providerは、利用者に対して利用許諾条件管理機能および同意情報管理機能を実行する「統合管理UI機能」を有する
機能要件	MIC-FUNC-BIZ-1-	SHOULD	Authz Providerは、登録済みの利用許諾条件に対して、利用許諾条件管理機能を実行する「利用許諾条件管理UI」を有する

	1-3-15-1		
機能要件	MIC-FUNC-BIZ-1-1-3-15-2	SHOULD	Authz Providerは、登録済みの同意情報に対して、同意情報管理機能を実行する「同意情報管理UI」を有する

注記

統合管理UI機能は、Webインタフェースに限定せず、email他各種コミュニケーションツールと連携できることを想定する。

7.5.3 非機能要件

7.5.3.1 可用性

7.5.3.1.1 稼働率

稼働率の要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-1-3-10	MUST	Authz Provider の稼働率は、授業時間中に関しては数分以上の停止を許容しない。ただし、授業時間外に関してはこの限りではない。
非機能要件	MIC-NONF-BIZ-1-1-3-10-1	MUST	授業時間を 7 時から 18 時とし、授業時間中の稼働率は、99.99%とする
非機能要件	MIC-NONF-BIZ-1-1-3-10-2	MUST	授業時間外の稼働率は、99.9%とする

7.5.3.2 性能・拡張性

7.5.3.2.1 オンラインレスポンス

オンラインレスポンスの要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-1-3-11	MUST	Authz Provider のオンラインレスポンスは、授業時間中に関しては大規模同時アクセスに対する十分な性能を確保しなくてはならない。ただし、授業時間外に関してはこの限りではない。
非機能要	MIC-NON	MUST	授業時間を 7 時から 18 時とし、授業時間中の稼働率は、99.99%とする

件	F-BIZ-1-1-3-11-1		
非機能要件	MIC-NONF-BIZ-1-1-3-11-2	MUST	授業時間外の稼働率は、99.9%とする

7.5.3.3 運用・保守性

7.5.3.3.1 運用監視

運用監視の要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-1-3-12	MUST	Authz Provider の運用監視は、Audit レポジトリによるパフォーマンス監視に対応する

7.5.3.4 セキュリティ

7.5.3.4.1 利用制限

利用制限の要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-1-3-13	MUST	Authz Provider の利用制限は、学習者、教員、保護者などのロールに、上位下位の権限設定ができる「ロールベースアクセス管理機能」を有する

7.5.3.4.2 不正監視

不正監視の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-3-5	MUST	Authz Provider は、外部 NTP と時刻同期を行う「NTP 時刻同期機能」を有する
非機能要件	MIC-NONF-BIZ-1-1-3-20-1	MUST	アクセス制御ポリシー生成機能の不正監視は、監査イベントデータを生成し、Auditレポジトリに送信する
非機能要件	MIC-NONF-BIZ-1-1-3-3-1-1	SHOULD	利用許諾条件登録機能の不正監視は、監査イベントデータを生成し、Auditレポジトリに送信する
非機能要	MIC-NON	SHOULD	利用許諾条件参照機能の不正監視は、監査イベントデータを生成し、Auditレポジ

件	F-BIZ-1-1-3-3-2-1		トリに送信する
非機能要件	MIC-NONF-BIZ-1-1-3-3-3-1	SHOULD	利用許諾条件更新機能の不正監視は、監査イベントデータを生成し、Auditレポジトリに送信する
非機能要件	MIC-NONF-BIZ-1-1-3-3-4-1	SHOULD	利用許諾条件削除機能の不正監視は、監査イベントデータを生成し、Auditレポジトリに送信する
非機能要件	MIC-NONF-BIZ-1-1-3-4-1-1	SHOULD	同意情報登録機能の不正監視は、監査イベントデータを生成し、Auditレポジトリに送信する
非機能要件	MIC-NONF-BIZ-1-1-3-4-2-1	SHOULD	同意情報参照機能の不正監視は、監査イベントデータを生成し、Auditレポジトリに送信する
非機能要件	MIC-NONF-BIZ-1-1-3-4-3-1	SHOULD	同意情報更新機能の不正監視は、監査イベントデータを生成し、Auditレポジトリに送信する
非機能要件	MIC-NONF-BIZ-1-1-3-4-4-1	SHOULD	同意情報削除機能の不正監視は、監査イベントデータを生成し、Auditレポジトリに送信する
非機能要件	MIC-NONF-BIZ-1-1-3-6-1	SHOULD	参照ID提供機能の不正監視は、監査イベントデータを生成し、Auditレポジトリに送信する

7.6 Audit レポジトリ

7.6.1 Audit レポジトリの概要

この項目は参考資料である

Auditレポジトリは、本プラットフォーム内のログ情報の管理を行う。

7.6.2 機能要件

7.6.2.1 パフォーマンスログ管理機能

パフォーマンスログ管理機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-5-1-1	MUST	Auditレポジトリは、パフォーマンスログの収集と分析を行う「パフォーマンスログ管理機能」を有する。

7.6.2.1.1 パフォーマンスログ収集機能

パフォーマンスログ収集機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-5-1-1-1	MUST	パフォーマンスログ管理機能は、共通バックエンドで生成したパフォーマンスログを収集する「パフォーマンスログ収集機能」を有する。

7.6.2.1.2 パフォーマンスログ参照機能

パフォーマンスログ参照機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-5-1-1-2	MUST	パフォーマンスログ管理機能は、収集したパフォーマンスログを参照する「パフォーマンスログ参照機能」を有する

7.6.2.1.3 パフォーマンスログ破棄機能

パフォーマンスログ破棄機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-5-1-1-3	MUST	パフォーマンスログ管理機能は、収集したパフォーマンスログを破棄する「パフォーマンスログ破棄機能」を有する

7.6.2.2 監査イベント情報管理機能

監査イベント情報管理機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-5-1-2	MUST	Auditレポジトリは、監査イベント情報の収集と分析を行う「監査イベント情報管理機能」を有する。

7.6.2.2.1 監査イベント情報収集機能

監査イベント情報収集機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-5-1-2-1	MUST	監査イベント情報管理機能は、共通バックエンドで生成した監査イベント情報を収集する「監査イベント情報収集機能」を有する

7.6.2.2.2 監査イベント情報参照機能

監査イベント情報参照機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-5-1-2-2	MUST	監査イベント情報管理機能は、収集した監査イベント情報を参照する「監査イベント情報参照機能」を有する

7.6.2.2.3 監査イベント情報破棄機能

監査イベント情報破棄機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-5-1-2-3	MUST	監査イベント情報管理機能は、収集した監査イベント情報を破棄する「監査イベント情報破棄機能」を有する

7.6.2.3 統合コンソール機能

統合コンソール機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-5-1-3	SHOULD	Auditレポジトリは、システム全体を一元的に監視する「統合コンソール機能」を有する

7.6.2.3.1 パフォーマンス分析機能

パフォーマンス分析機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUN	SHOULD	統合コンソール機能は、収集したパフォーマンスログを分析してパフォーマンス監

	C-BIZ-1-5-1-3-1		視を行う「パフォーマンス分析機能」を有する

7.6.2.3.2 パフォーマンス状態可視化機能

パフォーマンス状態可視化機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-5-1-3-2	MUST	統合コンソール機能は、収集したパフォーマンスログの分析結果を可視化する「パフォーマンス状態可視化機能」を有する

7.6.2.3.3 不正利用分析機能

不正利用分析機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-5-1-3-3	SHOULD	統合コンソール機能能は、収集した監査イベント情報から不正利用を検出する「不正利用分析機能」を有する

7.6.2.4 NTP サーバ機能

NTPサーバ機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-5-1-4	MUST	Auditレポジトリは、外部NTPサーバと時刻同期を行う「NTP時刻同期機能」を有する
機能要件	MIC-FUNC-BIZ-1-5-1-5	MUST	Auditレポジトリは、標準時刻情報を配信する「NTPサーバ機能」を有する

注記

本プラットフォーム内の時刻同期は、特に理由がない限りAuditレポジトリ経由で行われることとする。

7.6.3 非機能要件

7.6.3.1 可用性

7.6.3.1.1 稼働率

稼働率の要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-5-1-7	MUST	Auditレポジトリの稼働率は、監視対象システムより高い稼働率であることとする

7.6.3.2 セキュリティ

7.6.3.2.1 不正監視

不正監視の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-5-1-4	MUST	Auditレポジトリは、外部NTPと時刻同期を行う「NTP時刻同期機能」を有する
非機能要件	MIC-NONF-BIZ-1-5-1-6	MUST	パフォーマンスログと監査イベント情報の保管期間は、少なくとも１年は保管、最低３ヶ月間はオンラインで閲覧利用できるようにする。
非機能要件	MIC-NONF-BIZ-1-5-1-1-2-1	MUST	パフォーマンスログ参照機能は、監査イベントデータを生成して保存する
非機能要件	MIC-NONF-BIZ-1-5-1-1-3-1	MUST	パフォーマンスログ破棄機能は、監査イベントデータを生成して保存する
非機能要件	MIC-NONF-BIZ-1-5-1-2-2-1	MUST	監査イベント情報参照機能は、監査イベントデータを生成して保存する
非機能要件	MIC-NONF-BIZ-1-5-1-2-3-1	MUST	監査イベント情報破棄機能は、監査イベントデータを生成して保存する

注記

PCI DSS v3.1 "10.7 Retain Audit trail history for at least one year; at least three months of history must be immediately available for analysis." を参考とする。

外部NTPの接続先と接続頻度は、利用するパブリッククラウドの基盤の推奨から別途検討すること。

8. サービスプロバイダ

8.1 サービスプロバイダの概要

この項目は参考資料である

SPは、本プラットフォームの提供する機能を利用して各種サービスを利用者に提供する。SPの提供するサービス仕様については、各SPが独自に定義することとする。以下の図では、SPの類型例として、コンテンツSP、マーケットプレイスSP、データストアSPを示す。

- コンテンツSP：教材コンテンツや学習ツールを提供するSPの類型である。必須機能として、コンテンツ提供機能のみを有する。
- マーケットプレイスSP：課金機能を提供するSPの類型である。本SPは、課金機能を連携するSPに提供する。
- データストアSP：コンテンツ提供を行わず、データ保存機能のみを提供するSPの類型である。本SPは、学習用途の利用に限定されない。

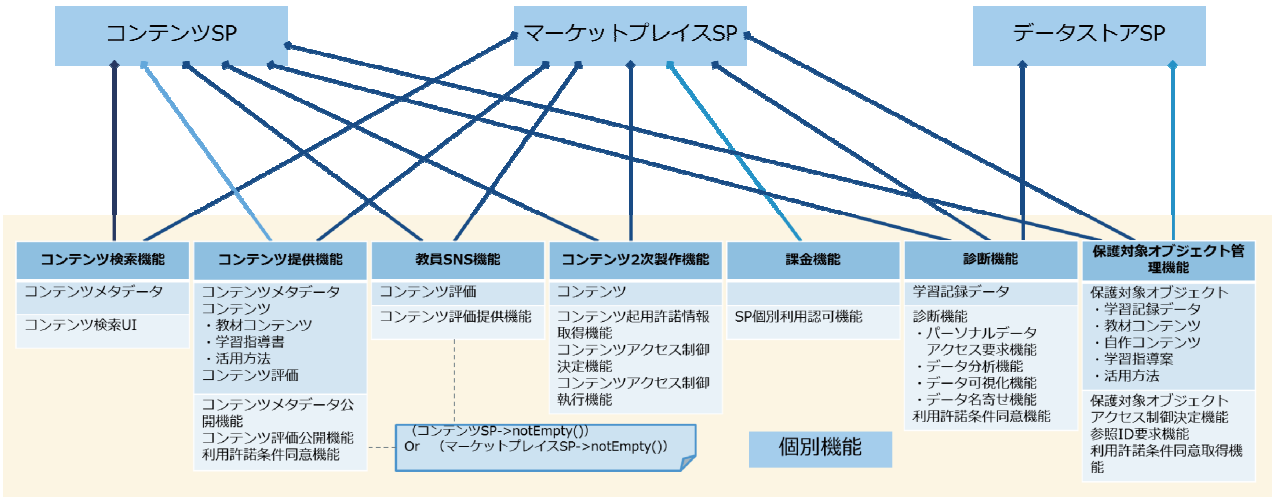


図 8-1 クラス図

8.2 機能要件

8.2.1 コンテンツ提供機能

コンテンツ提供機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
構成要件	MIC-PACK-BIZ-1-2-7	MUST	共通バックエンドは、コンテンツ提供機能を有する「コンテンツサービスプロバイダ」または「マーケットプレイスサービスプロバイダ」を1つ以上連携する
機能要件	MIC-FUNC-BIZ-1-4-1	MUST	コンテンツサービスプロバイダは、コンテンツメタデータ管理機能にコンテンツメタデータを公開する「コンテンツメタデータ公開機能」を有する

8.2.2 コンテンツ検索機能

コンテンツ検索機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-LEA-5-5	MUST	本システムは、診断結果に応じたコンテンツを検索・提示する「コンテンツ検索機能」を有する
機能要件	MIC-FUNK-LEA-5-5-2	MUST	コンテンツ検索機能は、校務 AtrP のコンテンツメタデータ提供機能を利用するための「コンテンツ検索 UI 機能」を有する
機能要件	MIC-FUNK-LEA-5-5-2-1	MUST	コンテンツ検索 UI は、コンテンツのメタデータを提供する「コンテンツメタデータ管理機能」と連携する
機能要件	MIC-FUNC-LEA-6-1	MUST	本システムは、学習者の所属学校・学年・教科・学習内容に応じたコンテンツを検索・提示する「コンテンツ検索機能」を有する
機能要件	MIC-FUNC-LEA-6-2	MUST	本システムは、整備されている（する予定の）ICT 環境に応じたコンテンツを簡便に検索・提示する「コンテンツ検索機能」を有する

8.2.3 教員 SNS 機能

教員SNS機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-UTL-1-1	MUST	本システムは、教員の属性を元に他の教員や学校によるコンテンツ評価、学習指導案、活用方法を共有やコミュニケーションを行う「教員 SNS 機能」を有する。
機能要件	MIC-FUN	MUST	本システムは、他の教員や学校による教材評価、学習指導案、活用方法を共有す

	C-UTL-1-1-1		る「コンテンツメタデータ管理機能」を有する。
機能要件	MIC-FUNC-UTL-1-1-2	SHOULD	本システムは、自作コンテンツや学習指導案を公開する「アクセス制御対象オブジェクト管理機能」を有する。
機能要件	MIC-FUNC-UTL-1-1-3	SHOULD	本システムは、教員の属性を元にコミュニケーションするために、教員の担当教科、勤続年数を管理する「校務 AtrP」を有する。
機能要件	MIC-DATA-UTL-1-1-3-3	MUST	サービスプロバイダは、コンテンツ評価の配信を行う「コンテンツ評価公開機能」を有する

8.2.4 コンテンツ 2 次制作機能

コンテンツ2次制作機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-LEA-7-2	MUST	本システムは、コンテンツを素材として作成した自作教材を利用する「コンテンツ 2 次制作機能」を有する
機能要件	MIC-FUNC-LEA-7-2-3	MUST	コンテンツ 2 次制作機能は、コンテンツの 2 次利用操作のコンテンツの利用許諾条件をコンテンツ自身または、共通バックエンドから取得する「コンテンツ利用許諾情報取得機能」を有する
機能要件	MIC-FUNC-LEA-7-2-3-1	MUST	コンテンツ利用許諾情報取得機能は、コンテンツのメタデータを提供する「コンテンツメタデータ管理機能」と連携する
機能要件	MIC-FUNC-LEA-7-2-4	MUST	コンテンツ 2 次制作機能は、コンテンツの 2 次利用操作の可否をコンテンツの利用許諾条件に基づいて決定する「コンテンツアクセス制御決定機能」を有する
機能要件	MIC-FUNC-LEA-7-2-5	MUST	コンテンツ 2 次制作機能は、コンテンツアクセス制御決定機能の判断に基づいて、2 次利用操作の実行を行う「コンテンツアクセス制御執行機能」を有する

注記

2次制作された教材コンテンツは、学習サービスとしてコンテンツメタデータ管理機能に登録することができることとする。

コンテンツアクセス制御執行機能は、一般的にDRMの機能等が該当する。

8.2.5 課金機能

課金機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
非機能要件	MIC-NONF-BIZ-1-2-2	MUST	課金機能は、各自治体の調達方法に準拠すること
機能要件	MIC-PACK-UTL-6-1	MUST	本システムは、コンテンツごとの利用登録を一元化できること

注記

利用登録の一元化とは、マーケットプレイスを通じて学習サービス利用権を取得する際、学習者の所属学校または教育委員会をマーケットプレイスに通知することで利用を行えることとする。

8.2.5.1 SP 個別運用利用認可機能

SP個別運用利用認可機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-2-3	MUST	課金機能は、商用コンテンツへのアクセス制御を行う「SP個別運用利用認可機能」を有する
機能要件	MIC-FUNC-BIZ-1-2-3-1	MUST	SP個別運用利用認可機能は、コンテンツの利用可否をコンテンツのコンテンツ利用許諾条件に基づいて決定する「SP個別アクセス制御決定機能」を有する
機能要件	MIC-FUNC-BIZ-1-2-3-2	MUST	SP個別運用利用認可機能は、SP個別アクセス制御決定機能の判断に基づいて、コンテンツサービスの提供を行う「SP個別アクセス制御執行機能」を有する
機能要件	MIC-FUNC-BIZ-1-2-3-3	MUST	SP個別運用利用認可機能は、教育委員会と学校のそれぞれの権限設定より、教育委員会が保有するコンテンツ利用権利を学校で利用可能な「ロールベースアクセス制御機能」を有する
機能要件	MIC-FUNC-BIZ-1-2-3-4	SHOULD	SP個別運用利用認可機能は、「試用条件」を設定できることとする。
機能要件	MIC-FUNC-BIZ-1-2-3-5	MUST	SP個別運用利用認可機能は、1ヵ月単位以下の期間の利用権利を管理できることとする
機能要件	MIC-FUNC-BIZ-1-2-3-6	MUST	SP個別運用利用認可機能は、学校単位および教育委員会単位の属性情報に対応できることとする
機能要件	MIC-FUNC-BIZ-1-2-3-7	MUST	SP個別運用利用認可機能件は、教育委員会が保有するコンテンツ利用権利を所属学校で利用可能とする、ロールベースアクセス制御のためのロール情報を設定できることとする

8.2.6 動的診断機能

動的診断機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-LEA-1-3	MUST	本システムは、教員が授業中に、授業中の学習者の理解度を把握する「動的診断機能」を有する。
機能要件	MIC-FUNC-LEA-1-3-1	MUST	動的診断機能は、対象学習者の学習記録データを、分析・可視化して提示する。
機能要件	MIC-FUNC-LEA-1-3-2	MUST	診断機能は、共用データレポジトリで管理された利用許諾条件への同意を共通バックエンドと連携して取得するための「利用許諾条件同意機能」を有する

注記

動的診断機能で利用されるパーソナルデータは、教室内など、応答速度が保障できる特定サービス内に限定してもよい。

8.2.7 静的診断機能

静的診断機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-LEA-2-3	MUST	本システムは、教員が授業外に、学習者の理解度を分析する「静的診断機能」を有する。
機能要件	MIC-FUNC-LEA-2-3-1	MUST	静的診断機能は、学習者の学習記録データを、複数のアクセス制御対象オブジェクト管理機能から参照する「パーソナルデータアクセス要求機能」を有する
機能要件	MIC-FUNC-LEA-2-3-2	MUST	静的診断機能は、収集した学習者の学習記録データより、各学習者および学習者集団の理解度分析を行う「データ分析機能」を有する
機能要件	MIC-FUNC-LEA-2-3-3	SHOULD	静的診断機能は、理解度分析の結果を可視化する「データ可視化機能」を有する
機能要件	MIC-FUNC-LEA-2-3-4	SHOULD	静的診断機能は、学習者が複数の学習者識別子を利用していた場合、複数の識別子を名寄せする「データ名寄せ機能」を有する。
機能要件	MIC-FUNC-LEA-2-3-5	MUST	診断機能は、共用データレポジトリで管理された利用許諾条件への同意を共通バックエンドと連携して取得するための「利用許諾条件同意機能」を有する

注記

異なる学習サービスの学習記録データ間や学習者の転校などにより、学習記録データに記録されるID情報が異なる場合、学習者本人や学校、各事業者から提供されたIDに関する情報の名寄せ処理を行う。

8.2.8 アクセス制御対象オブジェクト管理機能

アクセス制御対象オブジェクト管理機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-DATA-BIZ-1-1-4-8	OPTIONAL	アクセス制御対象オブジェクト管理機能は、xAPIに準拠する

8.2.8.1 アクセス制御対象オブジェクト保存機能

アクセス制御対象オブジェクト保存機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-4-1	MUST	アクセス制御対象オブジェクト管理機能は、新しいアクセス制御対象オブジェクトの保存を行う「アクセス制御対象オブジェクト保存機能」を有する

8.2.8.2 アクセス制御対象オブジェクト更新機能

アクセス制御対象オブジェクト更新機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-4-2	MUST	アクセス制御対象オブジェクト管理機能は、アクセス制御対象オブジェクトの更新を行う「アクセス制御対象オブジェクト更新機能」を有する

8.2.8.3 アクセス制御対象オブジェクト参照機能

アクセス制御対象オブジェクト参照機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能仕様	MIC-FUNC-BIZ-1-1-4-3	MUST	アクセス制御対象オブジェクト管理機能は、本人や許可された第三者にアクセス制御対象オブジェクトの共有を行う「アクセス制御対象オブジェクト参照機能」を有する

8.2.8.3.1 アクセス制御執行機能

アクセス制御執行機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-4-4-1	MUST	アクセス制御対象オブジェクト共有機能は、アクセス制御対象オブジェクト利用認可機能と連携してアクセスの制御を実行する「アクセス制御執行機能」を有する

8.2.8.3.2 参照ID要求機能

参照ID要求機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-4-4-2	MUST	アクセス制御対象オブジェクト共有機能は、アクセス制御対象オブジェクトの名寄せするための参照 ID を Authz Provider に要求する「参照 ID 要求機能」を有する

8.2.8.3.3 セキュア通信機能

セキュア通信機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-4-4-3	MUST	アクセス制御対象オブジェクト共有機能は、アクセス制御対象オブジェクトを送受信するために暗号強度 128bit 以上の SSL3.0/TSL1.0 通信による「セキュア通信機能」を有する

8.2.8.3.4 Authz Provider連携機能

Authz Provider連携機の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-4-4-4	MUST	アクセス制御対象オブジェクト共有機能は、学習記憶データや自作コンテンツをパーソナルデータとして利用許諾条件を Authz Provider 上で管理する「Authz Provider 連携機能」を有する

注記

パーソナルデータとしてAuthz Providerに登録されたアクセス制御対象オブジェクトは、同時に著作権コンテンツとして扱うことができないこととする。

8.2.8.3.5 共有データレポジトリ連携機能

共有データレポジトリ連携機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-4-4-6	MUST	アクセス制御対象オブジェクト共有機能は、学習記録データや自作コンテンツのメタデータを公開用コンテンツとして共有データレポジトリ上で管理する「共有データレポジトリ連携機能」を有する

注記

公開用の著作権コンテンツとして共有データレポジトリに登録されたアクセス制御対象オブジェクトは、公開以降はパーソナルデータとして扱わないための公開条件への同意を行うこととする。

8.2.8.4 アクセス制御対象オブジェクト削除機能

アクセス制御対象オブジェクト破棄機能の要件を以下に示す。

要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-4-6	MUST	アクセス制御対象オブジェクト管理機能は、アクセス制御対象オブジェクトを削除する「アクセス制御対象オブジェクト削除機能」を有する

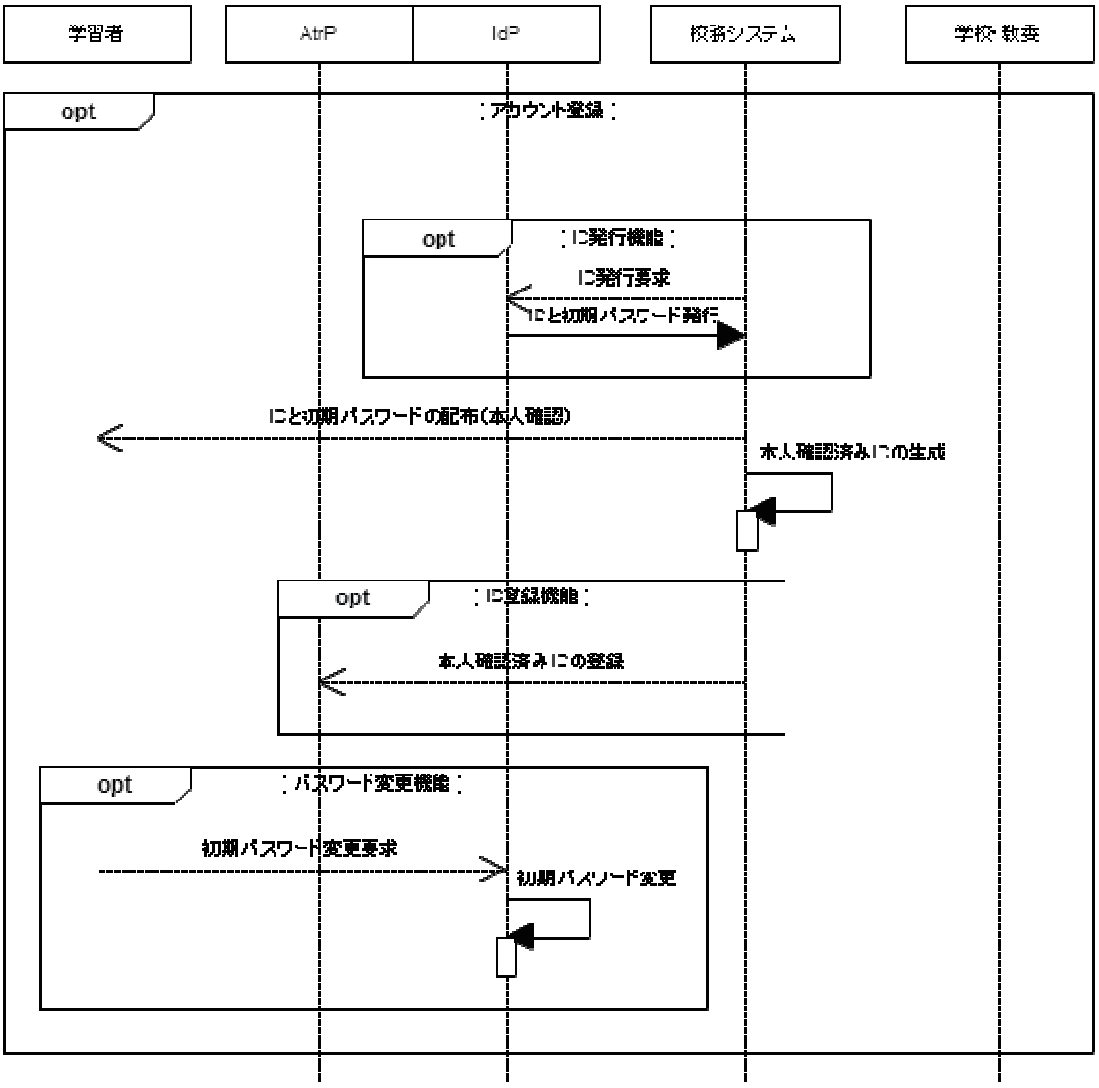
8.2.8.5 利用許諾条件同意取得機能

利用許諾条件同意取得機能の要件を以下に示す。

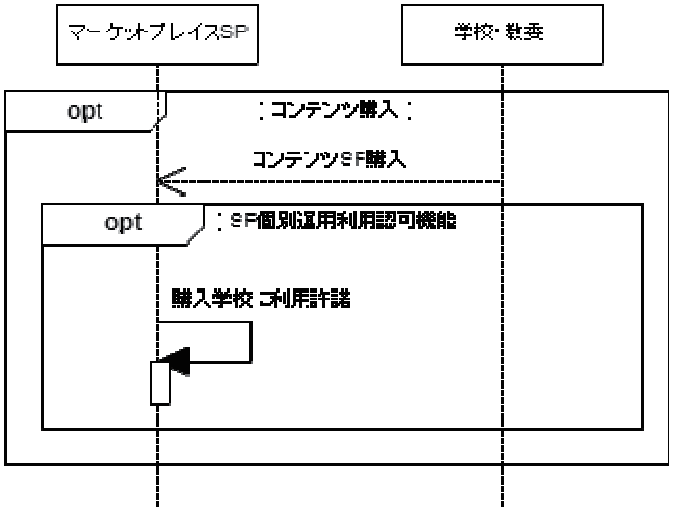
要件種別	要件番号	要求水準	内容
機能要件	MIC-FUNC-BIZ-1-1-4-7	MUST	サービスプロバイダは、共用データレポジトリで管理された利用許諾条件への同意を共通バックエンドと連携して取得するための「利用許諾条件同意取得機能」を有する

9. APPENDIX：ユースケース

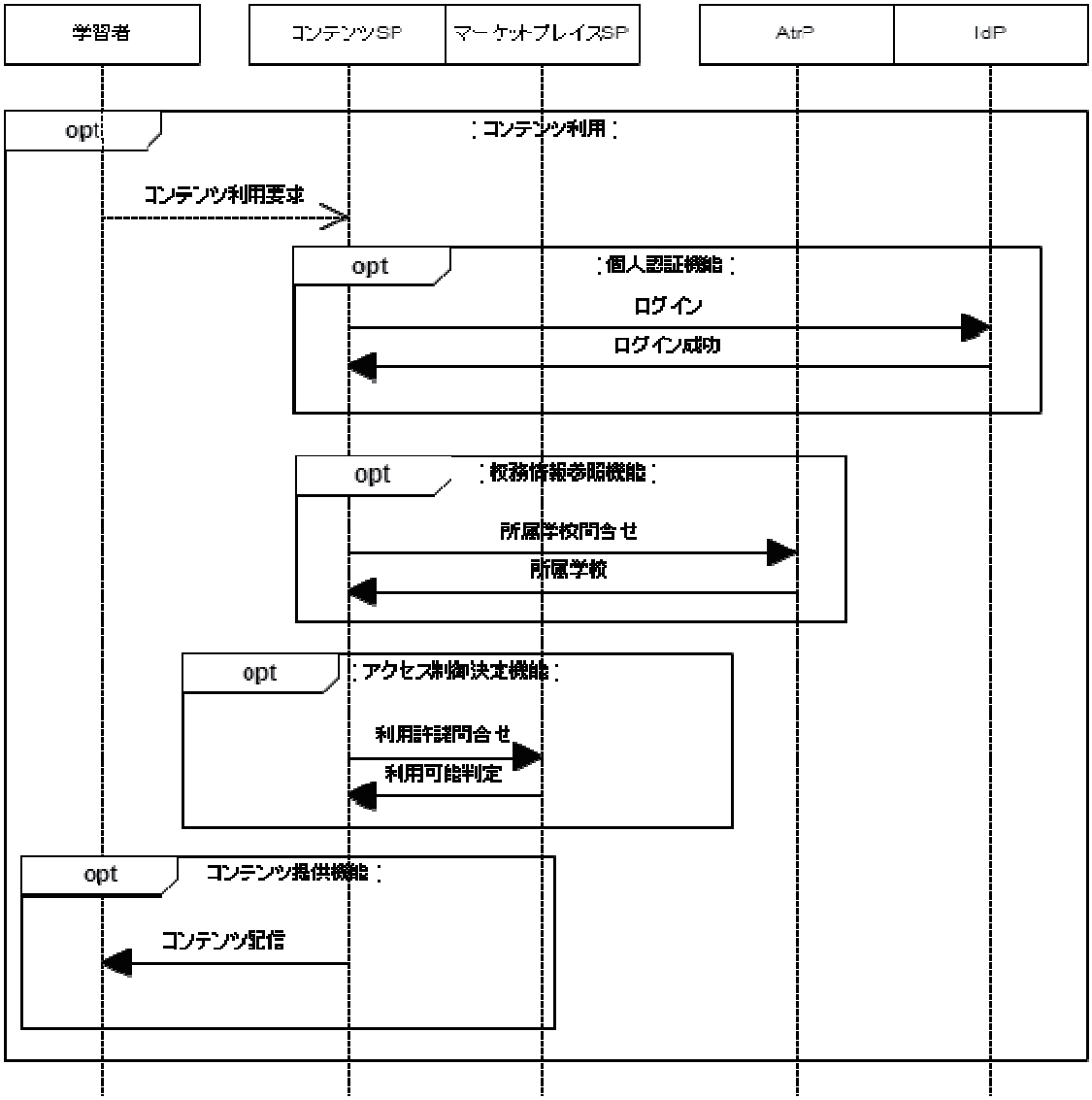
9.1 アカウント登録



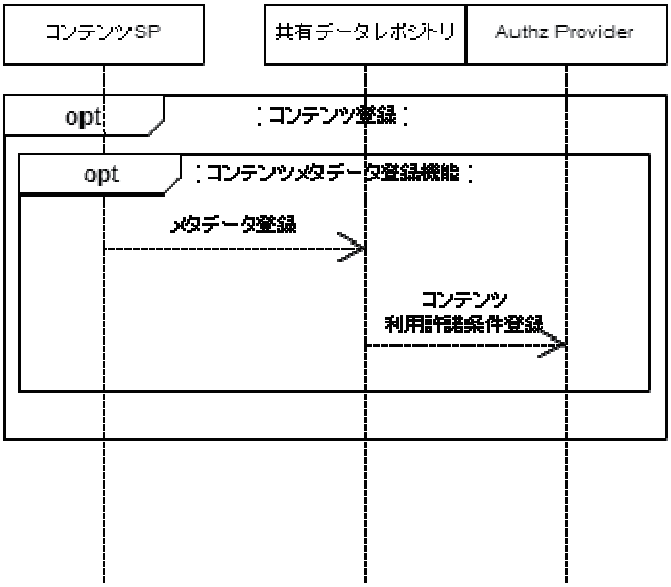
9.2 コンテンツ購入



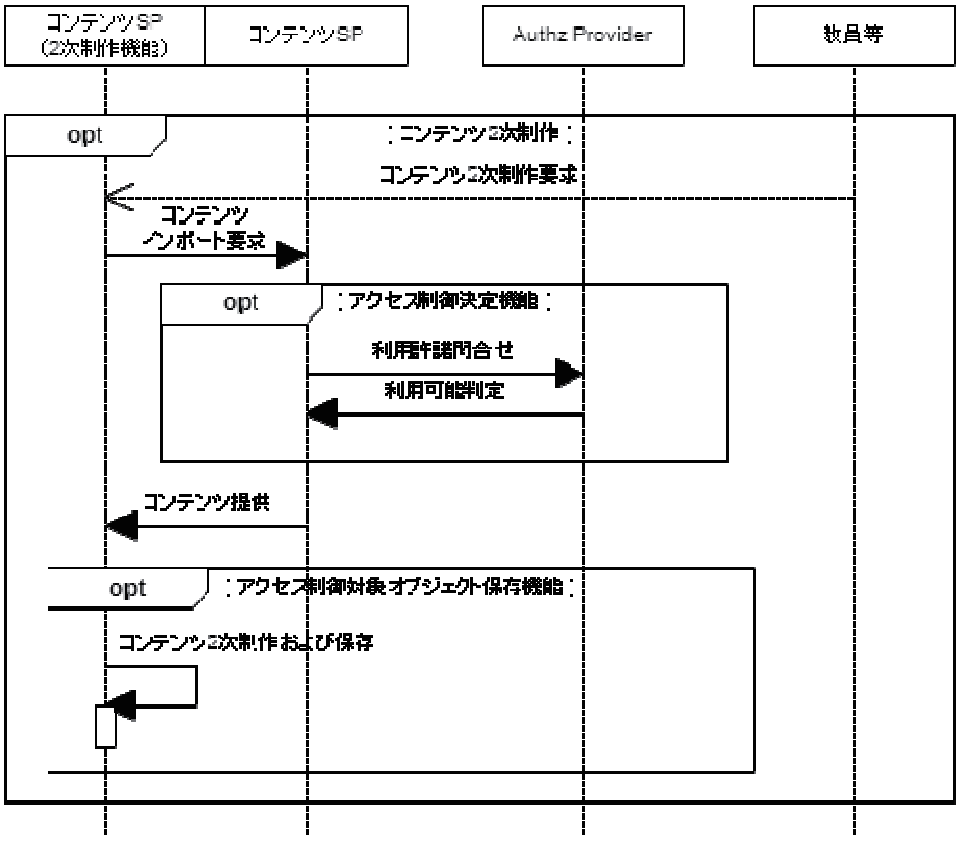
9.3 コンテンツ利用


学習者
コンテンツSP
マーケットプレイスSP
AtrP
IdP
opt
：コンテンツ利用：
コンテンツ利用要求
opt
：個人認証機能：
ログイン
ログイン成功
opt
：校務情報参照機能：
所属学校問合せ
所属学校
opt
：アクセス制御決定機能：
利用許諾問合せ
利用可能判定
opt
：コンテンツ提供機能：
コンテンツ配信

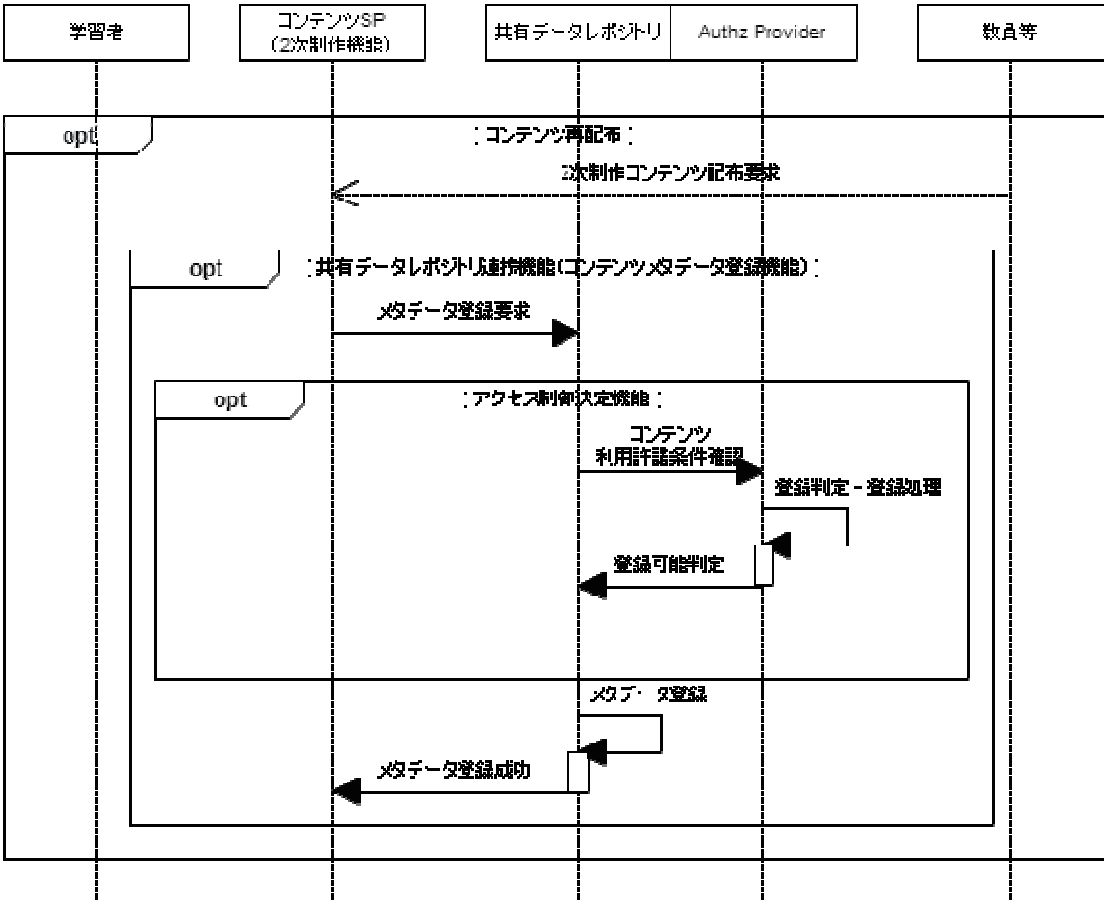
9.4 コンテンツ登録



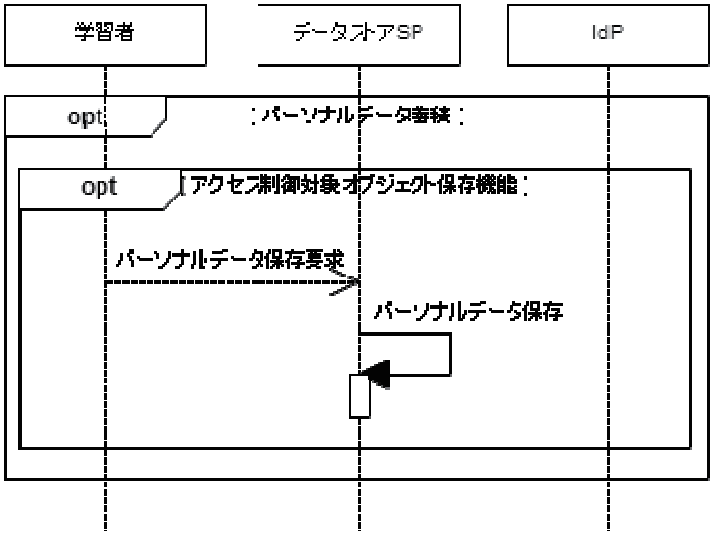
9.5 コンテンツ 2 次利用



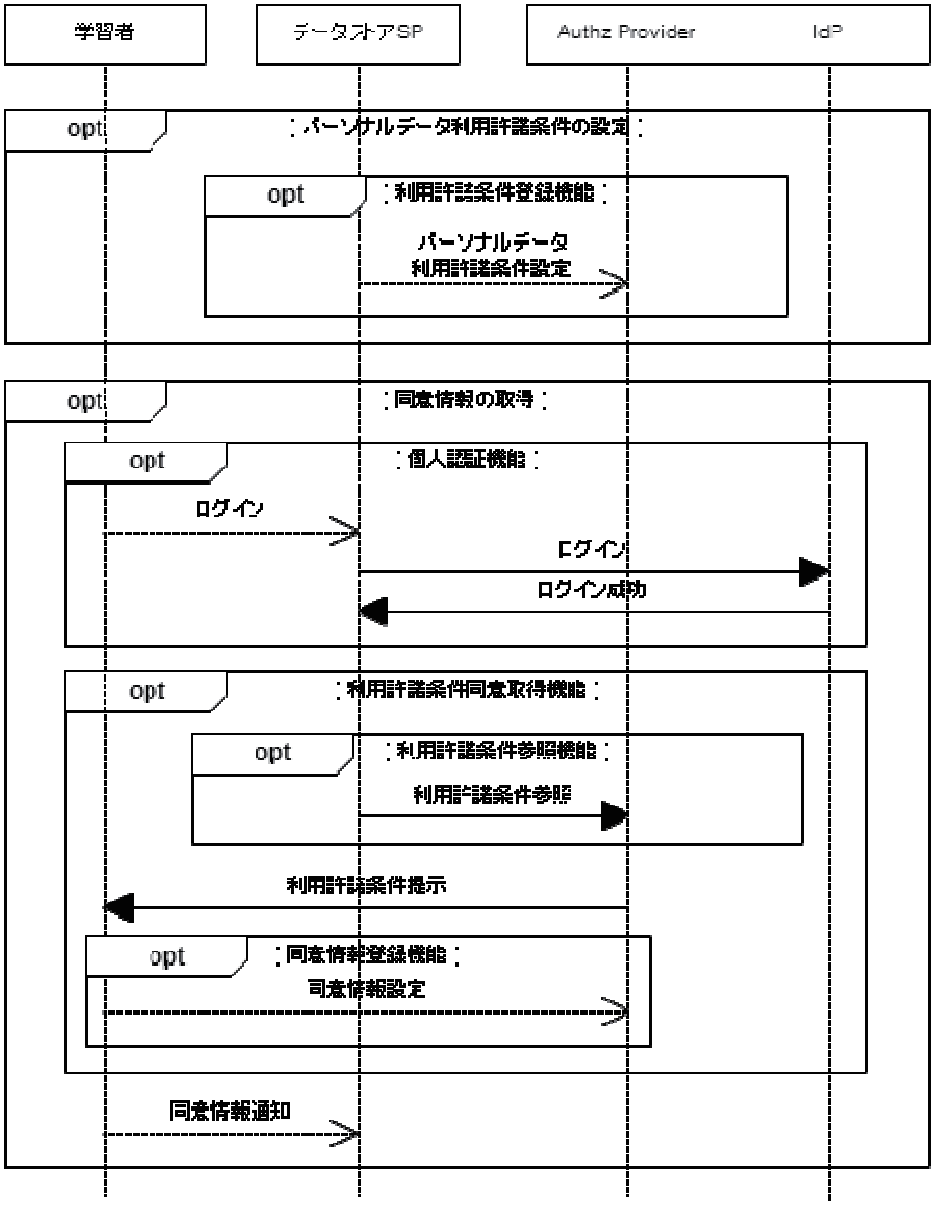
9.6 コンテンツ再配布



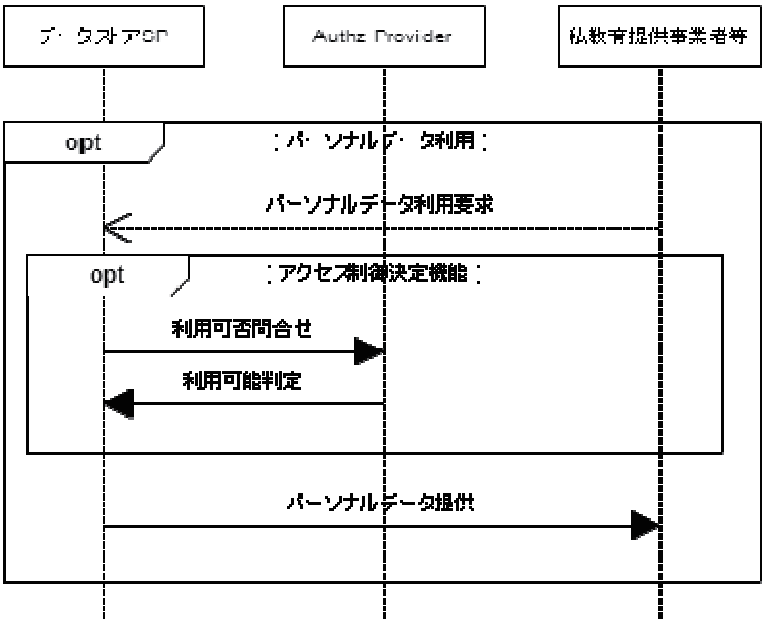
9.7 パーソナルデータ蓄積



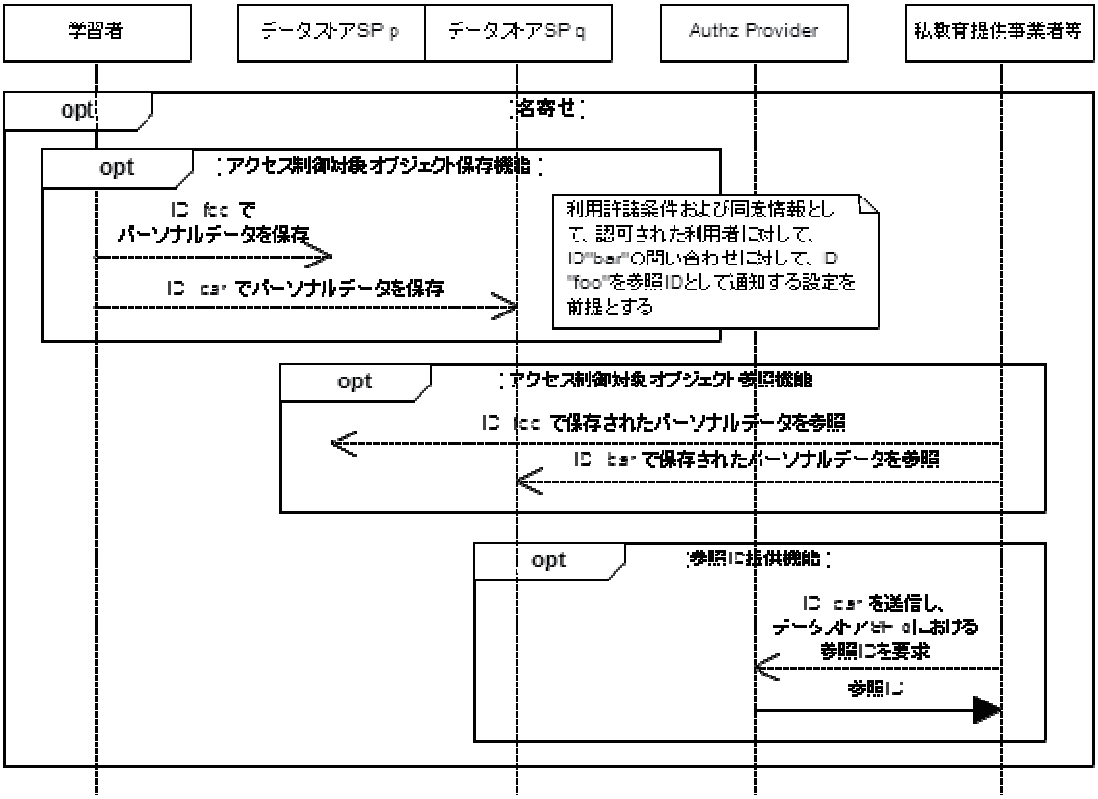
9.8 同意取得


学習者
データストアSP
Authz Provider
IdP
opt
：パーソナルデータ利用許諾条件の設定：
opt
：利用許諾条件登録機能：
パーソナルデータ
利用許諾条件設定
opt
：同意情報の取得：
opt
：個人認証機能：
ログイン
ログイン
ログイン成功
opt
：利用許諾条件同意取得機能：
opt
：利用許諾条件参照機能：
利用許諾条件参照
利用許諾条件提示
opt
：同意情報登録機能：
同意情報設定
同意情報通知

9.9 パーソナルデータ利用



9.10 名寄せ



10. APPENDIX：教科コード

10.1 小学校・中学校

教科（小学校）	教科コード	教科（中学校）	教科コード
国語	E01	国語	JH01
書写	E02	書写	JH02
社会	E03	社会（地理的分野）	JH03
地図	E04	社会（歴史的分野）	JH04
算数	E05	社会（公民的分野）	JH05
理科	E06	地図	JH06
生活	E07	数学	JH07
音楽	E08	理科	JH08
図画工作	E09	音楽（一般）	JH09
保健	E10	音楽（器楽合奏）	JH10
家庭	E11	美術	JH11
体育	E12	保健体育	JH12
道徳	E13	技術・家庭（技術分野）	JH13
外国語活動	E14	技術・家庭（家庭分野）	JH14
特別活動	E15	英語	JH15
総合的な学習の時間	E16	道徳	JH16
		特別活動	JH17
		総合的な学習の時間	JH18

10.2 高等学校

教科 (教科コード)	科目	科目コード	教科 (教科コード)	科目	科目コード
国語	国語総合	H0101	保健体育	体育	H0601
(H01)	国語表現	H0102	(H06)	保健	H0602
	現代文A	H0103	芸術	音楽Ⅰ	H0701
	現代文B	H0104	(H07)	音楽Ⅱ	H0702
	古典A	H0105		音楽Ⅲ	H0703
	古典B	H0106		美術Ⅰ	H0704
地理歴史	世界史A	H0201		美術Ⅱ	H0705
(H02)	世界史B	H0202		美術Ⅲ	H0706
	日本史A	H0203		工芸Ⅰ	H0707
	日本史B	H0204		工芸Ⅱ	H0708
	地理A	H0205		工芸Ⅲ	H0709

	地理Ｂ	H0206
公民	現代社会	H0301
(H03)	倫理	H0302
	政治・経済	H0303
数学	数学Ⅰ	H0401
(H04)	数学Ⅱ	H0402
	数学Ⅲ	H0403
	数学Ａ	H0404
	数学Ｂ	H0405
	数学活用	H0406
理科	科学と人間生活	H0501
(H05)	物理基礎	H0502
	物理	H0503
	化学基礎	H0504
	化学	H0505
	生物基礎	H0506
	生物	H0507
	地学基礎	H0508
	地学	H0509
	理科課題研究	H0510

	書道Ⅰ	H0710
	書道Ⅱ	H0711
	書道Ⅲ	H0712
外国語	ｺﾐｭﾆｹｰｼｮﾝ英語基礎	H0801
(H08)	ｺﾐｭﾆｹｰｼｮﾝ英語Ⅰ	H0802
	ｺﾐｭﾆｹｰｼｮﾝ英語Ⅱ	H0803
	ｺﾐｭﾆｹｰｼｮﾝ英語Ⅲ	H0804
	英語表現Ⅰ	H0805
	英語表現Ⅱ	H0806
	英語会話	H0807

10.3 高等学校専門学科

教科 (教科ｺｰﾄﾞ)	科目	科目 ｺｰﾄﾞ	教科 (教科ｺｰﾄﾞ)	科目	科目 ｺｰﾄﾞ
家庭	家庭基礎	H0901	家庭	生活産業基礎	H1501
(H09)	家庭総合	H0902	(H15)	課題研究	H1502
	生活デザイン	H0903		生活産業情報	H1503
情報	社会と情報	H1001		消費生活	H1504
(H10)	情報の科学	H1002		子どもの発達と保育	H1505
農業	農業と環境	H1101		子ども文化	H1506
(H11)	課題研究	H1102		生活と福祉	H1507
	総合実習	H1103		リビングデザイン	H1508
	農業情報処理	H1104		服飾文化	H1509
	作物	H1105		ファッション造形基礎	H1510
	野菜	H1106		ファッション造形	H1511
	果樹	H1107		ファッションデザイン	H1512
	草花	H1108		服飾手芸	H1513
	畜産	H1109		フードデザイン	H1514
	農業経営	H1110		食文化	H1515
	農業機械	H1111		調理	H1516

	食品製造	H1112		栄養	H1517
	食品化学	H1113		食品	H1518
	微生物利用	H1114		食品衛生	H1519
	植物バイオテクノロジー	H1115		公衆衛生	H1520
	動物バイオテクノロジー	H1116	看護	基礎看護	H1601
	農業経済	H1117	(H16)	人体と看護	H1602
	食品流通	H1118		疾病と看護	H1603
	森林科学	H1119		生活と看護	H1604
	森林経営	H1120		成人看護	H1605
	林産物利用	H1121		老年看護	H1606
	農業土木設計	H1122		精神看護	H1607
	農業土木施工	H1123		在宅看護	H1608
	水循環	H1124		母性看護	H1609
	造園計画	H1125		小児看護	H1610
	造園技術	H1126		看護の統合と実践	H1611
	環境緑化材料	H1127		看護臨地実習	H1612
	測量	H1128		看護情報活用	H1613
	生物活用	H1129	情報	情報産業と社会	H1701
	グリーンライフ	H1130	(H17)	課題研究	H1702
工業	工業技術基礎	H1201		情報の表現と管理	H1703
(H12)	課題研究	H1202		情報と問題解決	H1704
	実習	H1203		情報テクノロジー	H1705
	製図	H1204		アルゴリズムとプログラム	H1706
	工業数理基礎	H1205		ネットワークシステム	H1707
	情報技術基礎	H1206		データベース	H1708
	材料技術基礎	H1207		情報システム実習	H1709
	生産システム技術	H1208		情報メディア	H1710
	工業技術英語	H1209		情報デザイン	H1711
	工業管理技術	H1210		表現メディアの編集と表現,	H1712
	環境工学基礎	H1211		情報コンテンツ実習	H1713
	機械工作	H1212	福祉	社会福祉基礎	H1801
	機械設計	H1213	(H18)	介護福祉基礎	H1802
	原動機	H1214		コミュニケーション技術	H1803
	電子機械	H1215		生活支援技術	H1804
	電子機械応用	H1216		介護過程	H1805
工業(続き)	自動車工学	H1217	福祉(続き)	介護総合演習	H1806
(H12)	自動車整備	H1218	(H18)	介護実習	H1807
	電気基礎	H1219		こころとからだの理解	H1808
	電気機器	H1220		福祉情報活用	H1809
	電力技術	H1221	理数	理数数学Ⅰ	H1901
	電子技術	H1222	(H19)	理数数学Ⅱ	H1902
	電子回路	H1223		理数数学特論	H1903
	電子計測制御	H1224		理数物理	H1904

	通信技術	H1225		理数化学	H1905
	電子情報技術	H1226		理数生物	H1906
	プログラミング技術	H1227		理数地学	H1907
	ハードウェア技術	H1228		課題研究	H1908
	ソフトウェア技術	H1229	体育	スポーツ概論	H2001
	繊維製品	H1253	(H20)	スポーツⅠ	H2002
	繊維・染色技術	H1254		スポーツⅡ	H2003
	染織デザイン	H1255		スポーツⅢ	H2004
	インテリア計画	H1256		スポーツⅣ	H2005
	インテリア装備	H1257		スポーツⅤ	H2006
	インテリアエレメント生産	H1258		スポーツⅥ	H2007
	デザイン技術	H1259		スポーツ総合演習	H2008
	デザイン材料	H1260	音楽	音楽理論	H2101
	デザイン史	H1261	(H21)	音楽史	H2102
商業	ビジネス基礎	H1301		演奏研究	H2103
(H13)	課題研究	H1302		ソルフェージュ	H2104
	総合実践	H1303		声楽	H2105
	ビジネス実務	H1304		器楽	H2106
	マーケティング	H1305		作曲	H2107
	商品開発	H1306		鑑賞研究	H2108
	広告と販売促進	H1307	美術	美術概論	H2201
	ビジネス経済	H1308	(H22)	美術史	H2202
	ビジネス経済応用	H1309		素描	H2203
	経済活動と法	H1310		構成	H2204
	簿記	H1311		絵画	H2205
	財務会計Ⅰ	H1312		版画	H2206
	財務会計Ⅱ	H1313		彫刻	H2207
	原価計算	H1314		ビジュアルデザイン	H2208
	管理会計	H1315		クラフトデザイン	H2209
	情報処理	H1316		情報メディアデザイン	H2210
	ビジネス情報	H1317		映像表現	H2211
	電子商取引	H1318		環境造形	H2212
	プログラミング	H1319		鑑賞研究	H2213
	ビジネス情報管理	H1320	英語	総合英語	H2301
水産	水産海洋基礎	H1401	(H23)	英語理解	H2302
(H14)	課題研究	H1402		英語表現	H2303
	総合実習	H1403		異文化理解	H2304
	海洋情報技術	H1404		時事英語	H2305
	水産海洋科学	H1405			
	漁業	H1406			
	航海・計器	H1407			

	船舶運用	H1408
	船用機関	H1409
	機械設計工作	H1410
	電気理論	H1411
水産(続き) (H14)	移動体通信工学	H1412
	海洋通信技術	H1413
	資源増殖	H1414
	海洋生物	H1415
	海洋環境	H1416
	小型船舶	H1417
	食品製造	H1418
	食品管理	H1419
	水産流通	H1420
	ダイビング	H1421
	マリンスポーツ	H1422

11. APPENDIX：算数的活動コード

算数的な活動（第１学年）	コード
具体物を数える活動	1-a
計算の意味や仕方を表す活動	1-b
量の大きさを比べる活動	1-c
形を見付けたり，作ったりする活動	1-d
場面を式に表す活動	1-e
算数的な活動（第２学年）	**コード**
整数が使われている場面を見付ける活動	2-a
乗法九九表からきまりを見付ける活動	2-b
量の大きさの見当を付ける活動	2-c
図形をかいたり，作ったり，敷き詰めたりする活動	2-d
図や式に表し説明する活動	2-e
算数的な活動（第３学年）	**コード**
計算の仕方を考え説明する活動	3-a
小数や分数の大きさを比べる活動	3-b
単位の関係を調べる活動	3-c
正三角形などを作図する活動	3-d
資料を分類整理し表を用いて表す活動	3-e
算数的な活動（第４学年）	**コード**
計算の結果の見積りをし判断する活動	4-a
面積の求め方を考え説明する活動	4-b
面積を実測する活動	4-c
平行四辺形などを敷き詰め，図形の性質を調べる活動	4-d
身の回りの数量の関係を調べる活動	4-e
算数的な活動（第５学年）	**コード**
計算の仕方を考え説明する活動	5-a
面積の求め方を考え説明する活動	5-b
合同な図形をかいたり，作ったりする活動	5-c
図形の性質を帰納的に考え説明したり，演繹的に考え説明したりする活動	5-d
目的に応じて表やグラフを選び活用する活動	5-e

算数的な活動（第６学年）	コード
計算の仕方を考え説明する活動	6-a
単位の関係を調べる活動	6-b
縮図や拡大図，対称な図形を見付ける活動	6-c
比例の関係を用いて問題を解決する活動	6-d