



セキュリティ要件ガイドブック

平成 29 年 7 月 31 日
エヌ・ティ・ティ・コミュニケーションズ株式会社

Transform your business, transcend expectations with our technologically advanced solutions.

目次

1	ガイドブックの目的及び概要	5
1.1	ガイドブックの目的	5
1.2	ガイドブックの適用範囲および前提条件	6
1.3	ガイドブックの構成	6
2	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	8
6.	情報セキュリティのための組織	8
6.1	内部組織	8
6.1.1	情報セキュリティの役割及び責任	9
6.1.2	職務の分離	9
6.2	モバイル機器及びテレワーキング	10
6.2.1	モバイル機器の方針	10
6.3	クラウド利用者とクラウド事業者の公平な取引を確保するための措置	11
6.3.1	クラウドサービスの情報セキュリティマネジメントに係る提供条件の明確化	11
6.3.2	利用者接点とサプライチェーンにおける情報提供・共有	11
8	資産の管理	12
8.1	資産に対する責任	12
8.1.1	資産の目録	12
8.1.2	資産の管理責任	12
8.1.5	クラウド利用者から預託された情報の返却	13
8.2	情報分類	13
8.2.1	情報の分類	14
8.2.2	資産の取扱い	14
9	アクセス制御	15
9.1	アクセス制御に対する業務上の要求事項	15
9.1.1	アクセス制御方針	15
9.1.2	ネットワーク及びネットワークサービスへのアクセス	15

9.2	利用アクセスの管理	16
9.2.3	特権的アクセス権の管理	16
9.2.4	利用者の秘密認証情報の管理	17
9.4	システム及びアプリケーションのアクセス制御	17
9.4.1	情報へのアクセス制限	17
9.4.4	特権的なユーティリティプログラムの使用	18
9.5	仮想化されたクラウドサービスのアクセス制御	18
9.5.1	仮想化資源の分離の確実な実施	19
10	暗号	20
10.1	暗号による管理策	20
10.1.1	暗号による管理策の利用方針	20
10.1.2	鍵管理	20
12	運用のセキュリティ	22
12.1	運用の手順及び責任	22
12.1.1	操作手順書	22
12.1.2	変更管理	22
12.1.3	容量・能力の管理	23
12.2	マルウェアからの保護	23
12.2.1	マルウェアに対する管理策	24
12.3	バックアップ	24
12.3.1	情報のバックアップ	24
12.4	ログ取得及び監視	25
12.4.1	イベントログ取得	25
12.4.2	ログ情報の保護	26
12.4.3	実務管理者及び運用担当者の作業ログ	26
12.5	運用ソフトウェアの管理	26
12.5.1	運用システムに関わるソフトウェアの導入	27
12.6	技術的ぜい弱性管理	27

12.6.1	技術的ぜい弱性の管理	28
12.7	情報システムの監査に対する考慮事項	28
12.7.1	情報システムの監査に対する管理策	28
13	通信のセキュリティ	30
13.1	ネットワークセキュリティ管理	30
13.1.4	仮想ネットワークにおいて重視すべき脆弱性	30
13.2	情報の転送	30
13.2.2	情報転送に関する合意	31
13.2.4	秘密保持契約又は守秘義務契約	31
15	供給者関係	32
15.1	供給者関係における情報セキュリティ	32
15.1.1	供給者関係のための情報セキュリティの方針	32
15.1.3	ICT サプライチェーン	32
15.2	供給者のサービス提供の管理	33
15.2.1	供給者のサービス提供の監視及びレビュー	33
15.2.2	供給者のサービス提供の変更に対する管理	33
16	情報セキュリティインシデント管理	35
16.1	情報セキュリティインシデントの管理及びその改善	35
16.1.2	情報セキュリティ事象の報告	35
16.1.4	情報セキュリティ事象の評価及び決定	35
16.1.7	証拠の収集	36
17	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	37
17.2	冗長性	37
17.2.1	情報処理施設の可用性	37
18	順守	38
18.1	法的及び契約上の要求事項の順守	38
18.1.1	適用法令及び契約上の要求事項の特定	38
18.1.2	知的財産権	38

18.1.3 記録の保護	39
18.1.4 プライバシー及び個人を特定できる情報（PII）の保護.....	39
18.1.5 暗号化機能に対する規制	40
18.2 情報セキュリティのレビュー	40
18.2.1 情報セキュリティの独立したレビュー	40
18.2.2 情報セキュリティのための方針群及び標準の順守	41
18.2.3 技術的順守のレビュー	41

1 ガイドブックの目的及び概要

1.1 ガイドブックの目的

「教育クラウドプラットフォーム参考技術仕様」（以下「参考技術仕様」という。）は、教育クラウドプラットフォームを実装する際の一例として、クラウド環境で実装された複数の教材コンテンツをシングルサインオンで利用することができ、異なるプラットフォームとの間でも、相互にデータ連携を行うことができる教育クラウドプラットフォームに求められる技術要件について取りまとめている。

本ガイドブックは、参考技術仕様に基づき、教育クラウドプラットフォームを新たに提供する事業者、システム更改をする事業者に対し、求められるセキュリティ要件を示すことにより、その一助となることを目的としている。

総務省が平成 26 年度から平成 28 年度まで実施した「先導的教育システム実証事業」で作成した参考技術仕様及び各ガイドブックと教育クラウドプラットフォームの提供に向けた工程との関係については、下図 1-1 で示すとおりである。

本ガイドブックは、教育クラウドプラットフォームを提供するうえでのセキュリティに関し、要求定義から要件定義までに係るプロセスについて、事業者の参考となることを想定している。

	要求定義	要件定義	設計	実装
全体構成/ 相互運用性	参考技術仕様			
セキュリティ	セキュリティ要件 ガイドブック			
クラウド環境 (PaaS/IaaS)			クラウド環境構築 ガイドブック	
教材コンテンツ			コンテンツ作成 ガイドブック	
		アクセシビリティ ガイドブック		

図 1-1 参考技術仕様・各ガイドブックと教育クラウドプラットフォーム開発工程との関係

教育クラウドプラットフォームの概要を図 1-2 に示す。

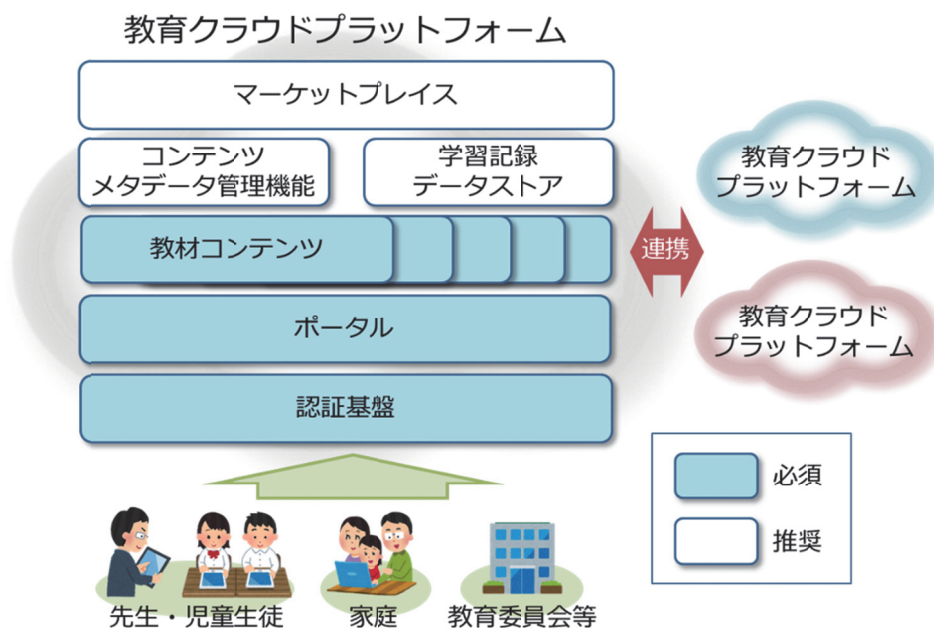


図 1-2 教育クラウドプラットフォームの概要

1.2 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におけるセキュリティ要件を検討するにあたり、クラウドサービスを含めた ICT システムに基づく組織における情報セキュリティマネジメントの基盤としては ISO/IEC などの国際標準化機関が定める ISO/IEC27001（情報セキュリティマネジメントシステム 要求事項）及び ISO/IEC 27002（情報セキュリティ管理策の実践のための規範）などの国際規格があり、それらに基づいて情報セキュリティマネジメントを実施することが可能となっている。

総務省では事業者と利用者の契約に基づく役割と責任の分担に関する諸問題を解消・緩和するため、上記の国際規格の ISO/IEC 27002 に基づき、事業者がクラウドサービスを提供する場合に特に重視すべき、利用者との接点において対応すべき実務に係る指針を加えた「クラウドサービス提供における情報セキュリティ対策ガイドライン（総務省・平成 26 年 4 月）」を作成している。

本セキュリティ要件ガイドブックでは、前述した「クラウドサービス提供における情報セキュリティ対策ガイドライン（以下「情報セキュリティ対策ガイドライン」という。）」を踏まえ、教育クラウドプラットフォームを提供する際に実施すべき実務について理解するために参考となる情報を提供している。

このため、「クラウドサービス提供における情報セキュリティ対策ガイドライン」の「第 I 部 序編 1. 目的」に記載のある通り、ISO/IEC 27002 に基づく情報セキュリティマネジメントを行うための知識を有している事業者を読み手として想定している。

1.3 ガイドブックの構成

次章「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」にて、ISO/IEC 27002:2013 の目次構成に基づき、「情報セキュリティ対策ガイドライン」で示された 10 領域 25 目的に重点化して、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を把握することが容易になるよう、解説を加えている。次章の構成を図表 1 に示す。本ガイドラインを読むに当たり、その内容を理解するためには、ISO/IEC 27002 に基づく情報セキュリティマネジメントを行うための知識を有していることが望ましい。

表 1 第Ⅱ部の構成

領域	目的
6. 情報セキュリティのための組織	6.1 内部組織
	6.2 モバイル機器及びテレワーキング
	6.3 クラウド利用者とクラウド事業者の公平な取引を確保するための措置
8. 資産の管理	8.1 資産に対する責任
	8.2 情報分類
9. アクセス制御	9.1 アクセス制御に対する業務上の要求事項
	9.2 利用アクセスの管理
	9.4 システム及びアプリケーションのアクセス制御
	9.5 仮想化されたクラウドサービスのアクセス制御
10. 暗号	10.1 暗号による管理策
12. 運用のセキュリティ	12.1 運用の手順及び責任
	12.2 マルウェアからの保護
	12.3 バックアップ
	12.4 ログ取得及び監視
	12.5 運用ソフトウェアの管理
	12.6 技術的ぜい弱性管理
	12.7 情報システムの監査に対する考慮事項
13. 通信のセキュリティ	13.1 ネットワークセキュリティ管理
	13.2 情報の転送
15. 供給者関係	15.1 供給者関係における情報セキュリティ
	15.2 供給者のサービス提供の管理
16. 情報セキュリティインシデント管理	16.1 情報セキュリティインシデントの管理及びその改善
17. 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	17.2 冗長性
18. 順守	18.1 法的及び契約上の要求事項の順守
	18.2 情報セキュリティのレビュー

2 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

以下にて、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を示す。項番は「1.4 ガイドブックの構成」で示す通り、ISO/IEC 27002:2013 を参照しながら確認することを想定し、ISO/IEC 27002:2013 の目次構成に基づき記載している。

6. 情報セキュリティのための組織

6.1 内部組織

【目的】

組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。

【補足事項】

教育クラウドプラットフォーム提供事業者にとっての利用者接点はクラウド利用者としてのエンドユーザ、クラウド事業者としての ASP・SaaS 提供事業者（サービスプロバイダ）、IaaS 提供事業者、PaaS 事業者との間に生じる。図 2 は利用者接点となるステークホルダとの関係性を示す。情報セキュリティ対策ガイドラインでは、「ガバナンスの実態が異なる組織が利用者接点を形成することから、その両側の組織の間で情報セキュリティマネジメントの統制が不十分になりやすく、これに対する管理策が必要である」としている。

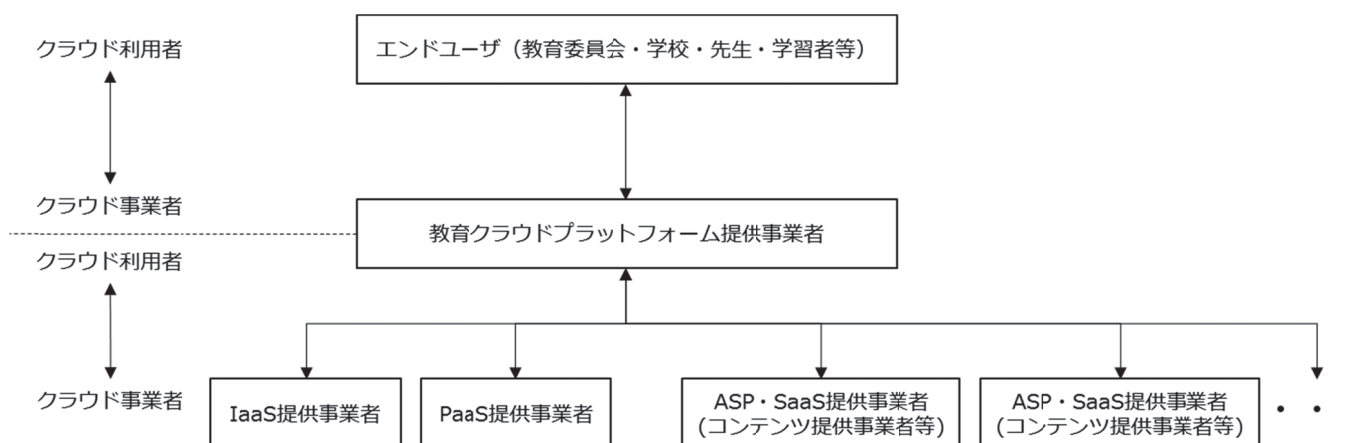


図 2 教育クラウドプラットフォーム提供事業者と利用者接点が生じるステークホルダの関係性

6.1.1 情報セキュリティの役割及び責任

【管理策】

全ての情報セキュリティの責任を定め、割当ることが望ましい。

【補足事項】

教育クラウドプラットフォーム提供事業者は、エンドユーザに対して個々の情報資産の保護と特定の情報セキュリティプロセスの実施に対する責任を利用規約・SLAなどで規定し、同意を得ることが必要である。教育クラウドプラットフォーム提供事業者はアグリゲータとして、複数のサービスプロバイダとの契約をとりまとめることとなるが、各々のサービスプロバイダが管理する情報資産や情報セキュリティプロセスの範囲に幅がある。そのため、相互の管理責任の分担や免責の範囲が不明確になりやすく、特に慎重に責任の範囲を定めることが求められる。教育クラウドプラットフォーム提供事業者は、サービスプロバイダ側の規定した責任範囲を確認し、これに基づいて自らの管理責任の範囲を定義することが必要である。

6.1.2 職務の分離

【管理策】

相反する職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離することが望ましい。

【補足事項】

教育クラウドプラットフォームでは、ASP・SaaSとして複数の教材コンテンツ等が提供されることになる。各々の教材コンテンツにおけるシステム設計・構築やサービス運用・設定における人為的ミスが、多数のエンドユーザに影響を及ぼし、教育クラウドプラットフォーム全体の信用低下に繋がる恐れがある。そのため、教育クラウドプラットフォーム提供事業者は、自身はもとより、教材コンテンツ提供事業者に対しても、開発・保守の実務を行う者と運用を行う者の役割と責任を明確に分離することを求める必要がある。

6.2 モバイル機器及びテレワーキング

【目的】

モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。

【補足事項】

本項目におけるモバイル機器は、教育クラウドプラットフォームにおいては情報端末と読み替えることができる。エンドユーザーにおける情報端末からの情報漏洩、教育クラウドプラットフォーム提供事業者及び教材コンテンツ提供事業者による情報端末から取得された情報の不正利用等である。これらに対する管理策が求められている。

6.2.1 モバイル機器の方針

【管理策】

モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用することが望ましい。

【補足事項】

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、マルチ OS・マルチブラウザに対応するため、主に HTML5 を用いて開発されることを想定している。情報セキュリティ対策ガイドラインは、「HTML5 等の先進的な Web 技術を用いるケースが増えており、これらに特有の脆弱性を持ち込む可能性が高まるため、Web サービスの開発段階から留意する必要がある」としている。

6.3 クラウド利用者とクラウド事業者の公平な取引を確保するための措置

【目的】

クラウド利用者の情報セキュリティマネジメント方針に適合したクラウドサービスの選択を確実にするため。

【補足事項】

教育クラウドプラットフォームは、複数のサービスプロバイダをアグリゲーションしエンドユーザに提供することから、各々の教材コンテンツの提供にあたり、エンドユーザの責任範囲を明確化し、エンドユーザの理解を深めることにより、ニーズに適合した教育クラウドプラットフォームを選択できる環境を構築していくことが求められる。

6.3.1 クラウドサービスの情報セキュリティマネジメントに係る提供条件の明確化

【管理策】

クラウドサービスの情報セキュリティマネジメントに係る責任範囲、サービスレベル、クラウド利用者個別に対応可能な範囲等の提供条件を明確に定め、文書化することが望ましい。

【補足事項】

教育クラウドプラットフォームを提供する場合、エンドユーザはアグリゲータである教育クラウドプラットフォーム提供事業者の利用規約に同意することになる。教育クラウドプラットフォーム事業者は、複数のサービスプロバイダとの契約をとりまとめることとなることから、情報セキュリティマネジメントに係る責任範囲の構造が複雑化し、その分担が不明確になりやすいため、特別な注意を払う必要がある。

6.3.2 利用者接点とサプライチェーンにおける情報提供・共有

【管理策】

目的や場面に応じて、クラウド利用者が必要とする情報を提供できる仕組みを構築することが望ましい。インシデント発生時には、ICT サプライチェーンで情報を共有し、クラウド利用者が必要とする情報を早く提供することが望ましい。

【補足事項】

アグリゲータである教育クラウドプラットフォーム提供事業者は、各々のサービスプロバイダとの緊急時の情報提供と情報受付に係る規定を確認し、これに基づいて情報セキュリティインシデントの情報を教育クラウドプラットフォーム全体で共有するための連絡体制を構築することが求められる。また、構築した連絡体制に基づき、教育クラウドプラットフォーム提供事

業者は、情報セキュリティインシデントの際のコンタクト窓口を設置することが必要となる。

8 資産の管理

8.1 資産に対する責任

【目的】

組織の資産を特定し、適切な保護の責任を定めるため。

【補足事項】

教育クラウドプラットフォームでは、個人情報などを取り扱うことが想定されている。それらの情報に対する教育委員会や学校などに格別の保護要求と、教育クラウドプラットフォーム提供事業者、及び教育クラウドプラットフォームに係る情報セキュリティマネジメント並びにそのガバナンスの実態と整合せず、情報の保護に支障をきたすことを防ぐ必要がある。

8.1.1 資産の目録

【管理策】

情報及び情報処理施設に関連する資産を特定することが望ましい。また、これらの資産の目録を、作成し、維持することが望ましい。

【補足事項】

教育クラウドプラットフォーム提供事業者は、エンドユーザから預託された情報と、教育クラウドプラットフォームを運用するための内部情報を、別の資産として分類することが求められる。そのうえで、エンドユーザが資産目録として情報の記録・維持するために必要となる、教育クラウドプラットフォームにおける情報の管理水準について、情報セキュリティ対策ガイドラインの 6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(i)の手法に基づき、SLA 記載の範囲内でエンドユーザに提供することが求められる。特に教育クラウドプラットフォームでは、複数のサービスプロバイダが提供する教材コンテンツ等のサービスが含まれることが想定されるため、各々のサービスプロバイダの管理水準について確認し、情報を提供していく必要がある。

8.1.2 資産の管理責任

【管理策】

目録の中で維持される資産は、管理されることが望ましい。

【補足事項】

教育クラウドプラットフォーム提供事業者は、情報資産及び情報処理施設に関連する資産（仮想化資源を含む）において、機密性や完全性などの特性に応じて、適切な管理を行うことが求められる。エンドユーザから預託された情報と、教育クラウドプラットフォームを運用するための内部情報のそれぞれについて、エンドユーザの合理的な理解を得られる水準での管理が行われることが望ましい。

また、預託情報を収集する際にはその利用目的を明確にし、エンドユーザの合意を得た上で収集するものとし、その目的の範囲を超えた利用、及び第三者への開示は行わないことを管理ポリシーに明示することが望ましい。ただし、エンドユーザには児童・生徒が含まれることから、合意の方法については契約主体と予め協議することが求められる。

8.1.5 クラウド利用者から預託された情報の返却

【管理策】

クラウド利用者がクラウドサービスの利用を終了するにあたり、預託された情報を、クラウド利用者が取扱うことができる形でクラウド利用者に返却し、クラウドサービスの提供に供する情報処理施設等から二度と取り出せないようにすることが望ましい。

【補足事項】

教育クラウドプラットフォームでは、児童・生徒の成績情報などが蓄積される可能性がある。児童・生徒の転校に伴う教育委員会の変更や、教育クラウドプラットフォーム提供事業者によるクラウドサービス提供終了などの理由により、クラウドサービスの終了や別のクラウドサービスへの移行が発生することを想定する必要がある。そのため、教育クラウドプラットフォーム提供事業者はエンドユーザの要求に基づき、情報漏洩のリスクに配慮した上で、当該エンドユーザのデータを汎用的な形式で出力することが望ましい。また、当該エンドユーザのデータが教育クラウドプラットフォーム提供事業者に残っていないことを保証するための証明書を発行できることが望ましい。

その観点において、データ返却要求の受付から返却、消去に至るまでのプロセスや手段が明確に定義され、かつエンドユーザに開示されていることが望ましい。

8.2 情報分類

【目的】

組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。

【補足事項】

アグリゲータである教育クラウドプラットフォーム提供事業者は、多くのエンドユーザとの契約、及び様々なサービスプロバイダとの契約を取りまとめる立場にあるとともに、エンドユーザから個人情報を含む多くの機微情報の委託を受けることとなる。そのため、教育クラウドプラットフォーム提供事業者には、それらの情報を分離し、適切な情報セキュリティポリシーや管理水準を適用することが求められる。情報セキュリティ対策ガイドラインでは、「クラウド利用者から寄託を受ける情報、及び提供するそれぞれのクラウドサービスにおいて供する情報資産等について、クラウド利用者ごと、及びクラウドサービスごとに適切に管理ができるように、必要となる情報の分類を行うことが求められる」としている。

8.2.1 情報の分類

【管理策】

情報は、法的要求事項、価値、重要性、及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から、分類することが望ましい。

【補足事項】

教育クラウドプラットフォームにおいては、児童・生徒の個人情報を含む、機微な情報が扱われることが想定される。その一方において、教育クラウドプラットフォーム提供事業者がサービスを提供する上で必要となる内部情報も管理されることとなる。これらの情報の重要度は異なることから、教育クラウドプラットフォーム提供事業者は、それぞれの情報を管理する場所を物理的に分けるなど、情報の重要度に応じた適切な管理を行うことが求められる。

8.2.2 資産の取扱い

【管理策】

資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施することが望ましい。

【補足事項】

教育クラウドプラットフォーム提供事業者は、多くのエンドユーザから情報の預託を受けることとなるが、それらの情報は後に返却が必要となることを想定しておく必要がある。エンドユーザへの返却に際して、その他のエンドユーザの情報と混同してしまう危険性があることから、技術面、運用面の両面から、エンドユーザの情報を論理的に分離し、適切に返却できる仕組みを整えることが望ましい。

9 アクセス制御

9.1 アクセス制御に対する業務上の要求事項

【目的】

情報及び情報処理施設へのアクセスを制限するため。

【補足事項】

教育クラウドプラットフォームは、インターネットを經由してサービス提供されることから、教育クラウドプラットフォーム提供事業者、エンドユーザ、サービスプロバイダ以外の第三者による不正なアクセスや攻撃の脅威にさらされる。

加えて、クラウドサービスでは、教育クラウドプラットフォーム提供事業者とサービスプロバイダによるサービス連携がなされること、サービスプロバイダが提供するサービスを複数のクラウド利用者が利用することなどから、アクセス制御に係る脆弱性や不完全なアクセス制御などにより、エンドユーザや第三者による不正アクセス等も生じうる。

このようなアクセス制御の脆弱性や不完全性により、個人情報を含む、エンドユーザから預託された情報の完全性や機密性、可用性が侵害される恐れがある。このリスクに対処するため、アクセス制御サービスの提供機構の冗長化、ソフトウェアの高信頼化と試験の徹底、操作ミスの防止、運用手順書の質の向上など、幅広い対策を考慮することが求められる。

9.1.1 アクセス制御方針

【管理策】

アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューすることが望ましい。

【補足事項】

教育クラウドプラットフォームでは、教育クラウドプラットフォーム提供事業者がアグリゲータとなり、多くのエンドユーザの契約を一元的に管理し、様々なサービスプロバイダが提供するサービスを一元的にエンドユーザに提供する。その範囲において、教育クラウドプラットフォーム提供事業者がエンドユーザから預託を受けた情報の一部をサービスプロバイダと共有し、アクセス制御が行われる。その際に、教育クラウドプラットフォーム提供事業者とサービスプロバイダとの間で、アクセス制御に関する方針が共有されていない場合、アクセス制御が不適切に行われるリスクがあることから、教育クラウドプラットフォーム提供事業者はアクセス制御に関する方針や要求事項を明確にサービスプロバイダに要求することが求められる。

9.1.2 ネットワーク及びネットワークサービスへのアクセス

【管理策】

利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを、利用者に提供することが望ましい。

【補足事項】

教育クラウドプラットフォームには、児童・生徒の個人情報を含む機微度の高い情報が格納されていることが想定され、かつインターネットを経由してアクセスすることが可能である。そのため、厳重なアクセス制御を行う必要がある。一方で、教育クラウドプラットフォームは学校外での授業や家庭学習にて利用される可能性があること、海外の日本人学校からも利用される可能性があることを考慮すると、情報セキュリティ対策ガイドラインの実務のポイント(b)に記載されている、「国内からクラウドサービスを利用するクラウド利用者に限定」や「アクセス元サーバに対する認証を行う」といった対策をとることが困難な場合が想定される。

そのため、教育クラウドプラットフォーム提供事業者は、自らが提供する教育クラウドプラットフォームの利用方法に考慮し、適切なアクセス制御を行い、その方式についてエンドユーザに対して情報提供することが望ましい。

9.2 利用アクセスの管理

【目的】

システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。

【補足事項】

教育クラウドプラットフォームの利用者は、教育委員会、学校（教員）、児童・生徒、児童・生徒の保護者など多岐にわたり、それぞれがアクセス可能なデータ、及び利用可能な教育クラウドプラットフォームの機能は異なるため、ユーザの適切な認証、及び認可を行うことが求められる。加えて、秘密認証情報の割当てを正式なプロセスによって管理運用することも求められる。

9.2.3 特権的アクセス権の管理

【管理策】

特権的アクセス権の割当て及び利用は、制限し、管理することが望ましい。

【補足事項】

教育クラウドプラットフォームの場合、複数の教育委員会や学校を 1 つのサービスとして同居させるマルチテナント方式でサービス提供されることが想定される。その場合、教育クラウドプラットフォーム事業者の特権的アクセス権が第三者に詐称

されると、被害が大きく拡大する可能性がある。そのため、特権的アクセス権の保護には、一般のエンドユーザ（個人）とは異なる格別の対策が求められる。

9.2.4 利用者の秘密認証情報の管理

【管理策】

秘密認証情報の割当ては、正式な管理プロセスによって管理することが望ましい。

【補足事項】

教育クラウドプラットフォームの利用者は、教育委員会、学校（教員）、児童・生徒、児童・生徒の保護者など多岐に渡る。教育クラウドプラットフォーム提供事業者は、それぞれの利用者に対し、それぞれの契約内容に基づき、秘密認証情報を適切に付与することが求められる。

9.4 システム及びアプリケーションのアクセス制御

【目的】

システム及びアプリケーションへの、認可されていないアクセスを防止するため。

【補足事項】

教育クラウドプラットフォームの場合、パブリッククラウドで提供されることが前提となっていることや、オープンなネットワークから第三者による不正なアクセスや攻撃が生じやすい。従って、システム及びアプリケーションに対するアクセス制御のための措置を十分講じていないと、教育クラウドプラットフォームや提供する教材コンテンツ、データ等の情報資産に対する改ざん、破壊、情報漏えい等が生じる恐れがある。

加えて、参考技術仕様における教育クラウドプラットフォームでは、異なるプラットフォームとの間でも、相互にデータ連携を行うことができるアーキテクチャを採用しており、サービス間連携が行われる場合が想定され、アクセス制御に係る脆弱性などにより、接続先サービスの提供事業者、利用者等による不正アクセス等の事態も生じうる。

これらの課題に対応するため、システム及びアプリケーションへのアクセスを、認可されている者に限定するための措置を講じるほか、逆に認可しているアクセスについては、完全に機能できるような対応を図ることが求められる。

9.4.1 情報へのアクセス制限

【管理策】

情報及びアプリケーションシステム機能へのアクセスは、アクセス制御方針に従って、制限することが望ましい。

【補足事項】

教育クラウドプラットフォームは学校内、学校外、家庭など、様々な場所から利用され、またアクセスする端末の環境も多岐に渡ることが想定される。情報セキュリティ対策ガイドラインには「クラウド利用者側の環境（利用する Web ブラウザ、OS、その他のアプリケーション、デバイス等）における脆弱性により、クラウドサービスへの重大な影響が生じる恐れがあるため、これに対応する措置を講じる必要がある」と記述されており、教育クラウドプラットフォーム提供事業者は、エンドユーザの環境に依存して発生する脆弱性情報について情報を収集した上で、適切な形でエンドユーザに対して危険性や対応手順などに関する情報を提供することが望ましい。

9.4.4 特権的なユーティリティプログラムの使用

【管理策】

システム及びアプリケーションによる制御を無効にすることができるユーティリティプログラムの使用は、制限し、厳しく管理することが望ましい。

【補足事項】

教育クラウドプラットフォームにおいて、児童・生徒のアカウントを一括で登録・変更・削除するツール等のユーティリティツールが提供されることが考えられる。このようなユーティリティツールはシステムに対して広範的に制御を行うことができることが想定され、悪用された場合の被害も甚大なものとなる恐れがあることから、利用可能なユーザを限定する、認証を強化する、利用の記録（ログ）を残すなど、厳重な管理が要求される。

9.5 仮想化されたクラウドサービスのアクセス制御

【目的】

仮想化されたクラウドサービスにおいて認可されていないアクセスを防止するため。

【補足事項】

教育クラウドプラットフォームは、パブリッククラウドで提供されることが前提となっており、仮想化されたクラウド基盤による提供が想定される。仮想化環境においては、ソフトウェアによる分離機能のせい弱性によって、利用者からの預託情報や教育クラウドプラットフォームを提供するために用いられるクラウド事業者の情報処理施設等に対する不正アクセスが生じることがある。これに対する管理策が求められる。

9.5.1 仮想化資源の分離の確実な実施

【管理策】

クラウドサービス上のクラウド利用者の仮想化資源を、他のクラウド利用者の仮想化資源やクラウドサービスの内部管理用の仮想化資源と確実に分離し、アクセス制御を確実にすることが望ましい。

【補足事項】

教育クラウドプラットフォームでは、仮想化されたクラウド基盤によるマルチテナント方式での提供が想定される。そのため、各テナントの仮想化マシンの分離は物理的な分離ではなく、ソフトウェアにより実現されているため、ソフトウェアの分離機能に脆弱性が生じると、マルチテナント環境において、利用者が、他のクラウド利用者やクラウドサービス提供に係る情報やシステムに対して不正アクセスし、情報、システム等の改ざん、破壊、盗聴、漏えい等を行う恐れがある。このため、仮想化マシンの分離を適切に実施し、アクセス制御を確実にするための措置を講じる必要がある。

そのため、教育クラウドプラットフォーム事業者は、ソフトウェアの分離機能の技術的ぜい弱性を管理するとともに、クラウド利用者がクラウドサービス上にインストールするソフトウェアに起因する脅威も考慮して、仮想化マシンによるクラウド利用者の利用環境の分離（テナント分離）が適切に実施されるための措置を講じる必要がある。

なお、【利用者接点とサプライチェーンにおける実務のポイント】の(b)「IaaS・PaaS の場合は、クラウド利用者がクラウドサービス上にインストールしたソフトウェアに潜在するマルウェア等のリスクについても考慮すること。」については、教育クラウドプラットフォーム事業者から見たクラウド利用者である教育委員会や学校による教育クラウドプラットフォームへのソフトウェアのインストールは想定されないため、除外される。一方、教育クラウドプラットフォームにおいて、利用者が自作教材等のファイル共有などは想定されるため、アップロードされるファイルに対するセキュリティ対策等を行うとともに、ファイルの登録者と利用者のログを取得し、監査ができる環境を整えることが望ましい。

10 暗号

10.1 暗号による管理策

【目的】

情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。

【補足事項】

情報セキュリティ対策ガイドラインには、「クラウドサービスにおける暗号の適用範囲、暗号化の強度、暗号鍵管理の確実性はサービスレベルに依存することから、クラウド利用者が、自らが求める要求レベルを確保したクラウドサービスを確実に選択できる環境整備が求められる」との記載があるが、教育クラウドプラットフォームの場合、利用者が教育委員会、学校（教員）、児童・生徒、児童・生徒の保護者と多岐にわたり、かつ利用者自らが暗号化の強度や暗号鍵の管理についての要求レベルを明確にすることができない場合が想定される。そのため、教育クラウドプラットフォーム提供事業者は、取り扱う情報の重要性に応じて適切な管理策を検討し、それを適用することが求められる。

10.1.1 暗号による管理策の利用方針

【管理策】

情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施することが望ましい。

【補足事項】

教育クラウドプラットフォーム提供事業者は、サービスプロバイダとの間における伝達する情報について、暗号化の方式、暗号鍵管理の主体、責任分解点について予め協議し、合意しておくことが望ましい。

10.1.2 鍵管理

【管理策】

暗号鍵の利用、保護及び有効期間（lifetime）に関する方針を策定し、そのライフサイクル全体にわたって実施することが望ましい。

【補足事項】

教育クラウドプラットフォームでは、複数の事業者が教材コンテンツを提供することが想定されるため、教育クラウドプラットフォーム事業者が管理する暗号鍵の不正利用は、教材コンテンツを含めたサービス全体の機密性・完全性を損なう。また、

クラウド事業者が管理する暗号鍵の喪失は、教材コンテンツを含めたサービス全体の暗号化されたデータの完全性を損なう。このため、暗号鍵の保護と管理（暗号鍵を実際に用いる段階での管理を含む）を確実にすることが求められる。

12 運用のセキュリティ

12.1 運用の手順及び責任

【目的】

情報処理施設の正確かつセキュリティを保った運用を確実にするため。

【補足事項】

教育クラウドプラットフォームは、学校の授業もしくは家庭学習における教材として使用されることが想定され、エンドユーザが教育クラウドプラットフォームを利用したいときに利用できない場合、授業や学習の進行を妨げてしまう恐れがある。そのため、教育クラウドプラットフォーム提供事業者はサービスを適切に維持するための情報を整備し、エンドユーザに適切に提供することが望ましい。

12.1.1 操作手順書

【管理策】

操作手順は、文書化し、必要とする全ての利用者に対して利用可能とすることが望ましい。

【補足事項】

教育クラウドプラットフォーム提供事業者は、教育クラウドプラットフォームにおけるセキュリティを担保する上で重要となる、ログイン認証機能やパスワード変更機能について、エンドユーザが理解しやすい操作手順書を作成することが求められる。エンドユーザには児童・生徒も含まれるため、表記の難易度によって複数種類を用意するなどの配慮がなされることが望ましい。また、サポート窓口（ヘルプデスク）によるサポート体制を整備し、エンドユーザの円滑かつ安全な利用を支援することが望ましい。

12.1.2 変更管理

【管理策】

情報セキュリティに影響を与える、組織、業務プロセス、情報処理施設及びシステムの変更は、管理することが望ましい。

【補足事項】

教育クラウドプラットフォームは、パブリッククラウドで提供されることを前提としており、オープンなネットワークを通じてサービス提供を行うため、第三者等からサービスに供するシステムに対する攻撃がなされる脅威があり、これによって悪意のあるブ

プログラムの改ざん、変更、破壊等がなされる恐れがある。そのため、教育クラウドプラットフォーム提供事業者は定期的に変更管理の状況を確認するとともに、変更管理に関する手順等を文書化し、適切な変更管理を行うとともに、意図しない変更が行われた場合に、速やかに元の構成に戻せる措置を講じることが求められる。

また、教育クラウドプラットフォームでは複数の事業者が教材コンテンツを提供することが想定されるため、【利用者接点とサプライチェーンにおける実務のポイント】(e)で示されている通り、教材コンテンツについての変更についても教育クラウドプラットフォーム提供事業者が、適切な手段で利用者に情報提供されることが望ましい。

12.1.3 容量・能力の管理

【管理策】

要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測することが望ましい。

【補足事項】

教育クラウドプラットフォームでは様々なエンドユーザに対し、サービスプロバイダが提供する教材コンテンツや、教育クラウドプラットフォームそのものが持つ授業支援機能を、共有のプラットフォームにて提供されることが想定される。そのため、一部のユーザによって高負荷を発生させるような処理や、記憶領域を枯渇させるような操作が行われると、他のユーザに悪影響を及ぼす恐れがある。そのため、教育クラウドプラットフォーム提供事業者は、以下のような対策を検討し、導入することが望ましい。

- (a) サービスを安定的に維持するために必要なリソースを定期的に監視する
- (b) ユーザの操作に一定の制限をかける（保存可能な容量に上限を設ける等）
- (c) 大量の高負荷アクセスが集中した場合でも処理を分散する（コンテンツデリバリーネットワークの活用等）
- (d) 統計的にシステム負荷の高い状況を予測し、オートスケーリング等の技術にてシステムのキャパシティを動的に制御する

12.2 マルウェアからの保護

【目的】

情報及び情報処理施設がマルウェアから保護されることを確実にするため。

【補足事項】

教育クラウドプラットフォームのシステムにマルウェアが感染した場合には、サービスに供するシステムの改ざん、破壊等による、システムの停止、管理しているクラウド利用者の預託データ等の漏えい等の発生、クラウド利用者が利用するシステム等への感染といった深刻な事態を招く恐れがある。

このため、マルウェア対策を行うとともに、クラウド事業者のどの情報処理施設が感染したのかを、適切な手段を選択して、利用者に情報提供することが求められる。

12.2.1 マルウェアに対する管理策

【管理策】

マルウェアから保護するために、利用者に適切に認識させることと併せて、検出、予防及び回復のための管理策を実施することが望ましい。

【補足事項】

教育クラウドプラットフォームでは、教員が作成した教材をアップロードして共有する機能や、児童・生徒からのファイル提出機能が提供されることが想定される。これらのファイルにマルウェアが混入し、それをダウンロードしたエンドユーザが感染することを防止するため、アップロードされたファイルを格納する前にマルウェアの有無を検査することが望ましい。

12.3 バックアップ

【目的】

データの消失から保護するため。

【補足事項】

教育クラウドプラットフォームでは、児童・生徒の学習記録データなどの機微度の高い情報が格納されていることが想定される。データ消失により、学習活動に支障が生じるなどの影響が想定されるため、バックアップ等によるデータの保全が必要となる。

また、一部の利用者の預託データについて、証拠提出の要請や、司法官憲等による提出命令などが生じた場合に、当該利用者に関するデータだけでなく、他の利用者の預託データまでもが一緒に提出されてしまう恐れがある。ハードディスクが提出された場合だけでなく、教育クラウドプラットフォーム事業者が取得したバックアップが提出された場合も同等のことが生じうる。これによって、多くの利用者の預託データが提出先の管理下に置かれる等の事態を生じ、結果として教育クラウドプラットフォーム全体の信用低下などに繋がりがかねない。従って、これを防止する措置を講じることが求められる。

12.3.1 情報のバックアップ

【管理策】

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、検査することが望ましい。

【補足事項】

教育クラウドプラットフォームは、マルチテナント方式を用いることが想定されることから、複数の利用者の預託データを一括してバックアップを取得することが多い。一方で、特定のクラウド利用者の預託データの提出命令等が生じた場合でも、サービスレベルを保証したまま継続できるようにするため、【利用者接点とサプライチェーンにおける実務のポイント】(a)(b)(c)で示された処置を実施することが望ましい。

12.4 ログ取得及び監視

【目的】

イベントを記録し、証拠を作成するため

【補足事項】

教育クラウドプラットフォーム提供事業者は、アグリゲーションサービスとして様々な教材コンテンツを一元的に提供することが想定される。教育クラウドプラットフォーム提供事業者では、自身が提供しない教材コンテンツに対する利用者のイベントの記録が難しい場合がある。そのため、教材コンテンツ提供事業者との協議、調整を行い、教育クラウドプラットフォーム全体として取得、管理するイベントログを整理し、利用者に情報提供することが望ましい。

12.4.1 イベントログ取得

【管理策】

利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューすることが望ましい。

【補足事項】

情報セキュリティ対策ガイドラインには「アグリゲーションサービス事業者においては、アグリゲーションサービス全体について、統一したポリシーでログ取得等を行うことが求められる」との記載がある。教育クラウドプラットフォーム提供事業者は、様々なサービスプロバイダが提供する教材コンテンツを一元的に管理し、エンドユーザに提供するが、サービスプロバイダには小規模な事業者が含まれることも想定されるため、統一したポリシーに当てはめてログを取得できない場合も考えられる。そのため教育クラウドプラットフォーム提供事業者は、最低限必要と考えられる要求事項を整理し、サービスプロバイダとの協議、調整を行うことが望ましい。

12.4.2 ログ情報の保護

【管理策】

ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護することが望ましい。

【補足事項】

情報セキュリティ対策ガイドラインには「アグリゲーションサービスを提供する場合は、供給者との間で、ログ情報の保護に関する方針や対応策について、統一したポリシーが適用されていない場合には、アグリゲーションサービス全体として講ずべき情報セキュリティマネジメントに必要なログの保護がなされない恐れが生じる」との記載がある。教育クラウドプラットフォーム提供事業者は、様々なサービスプロバイダが提供する教材コンテンツを一元的に管理し、エンドユーザに提供するが、サービスプロバイダには小規模な事業者が含まれることも想定されるため、統一したポリシーに当てはめてログ情報を保護できない場合も考えられる。そのため教育クラウドプラットフォーム提供事業者は、最低限必要と考えられる要求事項を整理し、サービスプロバイダとの協議、調整を行うことが望ましい。

12.4.3 実務管理者及び運用担当者の作業ログ

【管理策】

システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューすることが望ましい。

【補足事項】

情報セキュリティ対策ガイドラインには「クラウド事業者及び全ての供給者において取得するログを突合する必要等が生じるが、クラウド事業者が、供給者が取得するログで対象とするイベントの範囲や、イベントにおける詳細事項について確認し、同意していない場合には、ログの分析に必要な情報が記録されない恐れがある」との記載がある。教育クラウドプラットフォーム提供事業者は、様々な教材コンテンツ提供事業者が提供する教材コンテンツを一元的に管理し、エンドユーザに提供するが、教材コンテンツ提供事業者には小規模な事業者が含まれることも想定されるため、教育クラウドプラットフォーム全体としてログを統合し、分析を行うことができない場合も考えられる。そのため教育クラウドプラットフォーム提供事業者は、最低限必要と考えられる要求事項を整理し、教材コンテンツ提供事業者との協議、調整を行うことが望ましい。

12.5 運用ソフトウェアの管理

【目的】

運用システムの完全性を確実にするため。

【補足事項】

教育クラウドプラットフォーム提供事業者は、利用するクラウドサービスに合わせて運用システムを利用、または導入し、システムの変更管理を行うことが望ましい。

また、情報セキュリティ対策ガイドラインの【クラウドサービスの提供において特に留意すべき課題との関係】では「クラウド利用者がクラウド上にインストールしたソフトウェアが悪意を持った動作をすることで、クラウドサービスの継続や信用に影響を及ぼす恐れがある。このため、これに対する管理策が求められる。」と記載されている。一方で、教育クラウドプラットフォームの場合、利用者による教育クラウドプラットフォーム上でのソフトウェアのインストールは想定されていないため、本件に関する対応策は除外される。

12.5.1 運用システムに関わるソフトウェアの導入

【管理策】

運用システムに関わるソフトウェアの導入を管理するための手順を実施することが望ましい。

【補足事項】

12.5 で補足した通り、教育クラウドプラットフォームでは、利用者による教育クラウドプラットフォーム上でのソフトウェアのインストールは想定されていない。一方、教育クラウドプラットフォームにおいて、利用者が自作教材等のファイル共有などは想定される。そのため、アップロードされるファイルに対し、ウイルス等に感染していないことを確認し、必要に応じ対処できるようにすること、アップロードや変更の証跡を記録しその記録を保存・保護すること、不正な挙動を示した場合はその原因となったファイルを特定、必要な措置を講じること等が求められる。

12.6 技術的ぜい弱性管理

【目的】

技術的ぜい弱性の悪用を防止するため。

【補足事項】

教育クラウドプラットフォーム提供事業者は、アグリゲーションサービスとして様々な教材コンテンツを一元的に提供することが想定される。そのため、技術的ぜい弱性の悪用により、教育クラウドプラットフォームの継続に影響を被ることに留まらず、教材コンテンツ事業者の事業・権利保護・コンプライアンス確保に支障をきたすことがありうる。このため、技術的ぜい弱性の悪用防止には、重点を置いて取り組むことが求められる。

12.6.1 技術的ぜい弱性の管理

【管理策】

利用中の情報システムの技術的ぜい弱性に関する情報は、時期を失わずに獲得することが望ましい。さらに、それらと関連するリスクに対処するために、適切な手段をとることが望ましい。

【補足事項】

教育クラウドプラットフォームでは、複数の教材コンテンツを提供するアグリゲーションサービスであることを踏まえ、【利用者接点とサプライチェーンにおける実務のポイント】で示されている(a)(b)(c)において、利用者への情報提供にとどまらず、教材コンテンツ提供事業者に対しても情報提供することが必要となる。

12.7 情報システムの監査に対する考慮事項

【目的】

運用システムに対する監査活動の影響を最小限にするため。

【補足事項】

運用システムの点検を伴う監査要求事項及び活動は、教育クラウドプラットフォームの運用業務プロセスの中断を招く恐れがある。その場合、アグリゲーションしている教材コンテンツへの利用の停止が伴う可能性がある。このため、監査要求事項及び活動が教材コンテンツを含めた教育クラウドプラットフォーム全体のサービスレベル低下に繋がらないための措置を講じることが求められる。

12.7.1 情報システムの監査に対する管理策

【管理策】

運用システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、合意することが望ましい。

【補足事項】

【利用者接点とサプライチェーンにおける実務のポイント】の「(a) クラウドサービスの監査について方針を定め、監査を定期的に実施する、監査対象となる資源とサービス提供に係る情報資産等の分類を適切に行い、監査対象を明確にし、最小限の監査により、管理策の十分性を確認できるようにする等、効果的な監査を実施できるようにする措置を講じること。」について、教育クラウドプラットフォーム事業者は定期監査を実施するとともに、その監査基準を教材コンテンツ事業者に示し、定期監査の実施を求めることにより、教材コンテンツを含めた教育クラウドプラットフォーム全体での情報システムの運

平成 28 年度クラウド等の最先端情報通信技術を活用した教育クラウドプラットフォームに関する実証別冊
セキュリティ要件ガイドブック

用水準を高めていくことが望ましい。

13 通信のセキュリティ

13.1 ネットワークセキュリティ管理

【目的】

ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。

【補足事項】

ネットワークの設計ミスや設定ミスは、サービスの全面停止や可用性喪失を生じやすい。教育クラウドプラットフォーム事業者は、認証基盤など複数の教材コンテンツが利用するシステムを提供するため、その影響は教材コンテンツを含めた教育クラウドプラットフォーム全体に及ぶ可能性がある。そのため、ネットワークの設計・設定ミスの防止について、特に慎重な管理を行うことが求められる。

13.1.4 仮想ネットワークにおいて重視すべき脆弱性

【管理策】

仮想ネットワークの複雑な構成や設定に伴う管理ミスを防止する措置を講じることが望ましい。

【補足事項】

教育クラウドプラットフォームでは、パブリッククラウドで提供することが前提となっており、仮想環境で提供されることが想定され、仮想ネットワークの構築・運用が求められる。教育クラウドプラットフォーム提供事業者は、仮想ネットワークと物理ネットワークの対応関係を明確し、統合的な管理が必要となる。

また、教育委員会や学校等の利用者がオンプレミス環境から移行する場合、移行中の悪意ある攻撃に留意する必要があり、【利用者接点とサプライチェーンにおける実務のポイント】(c)で示されている通り、「仮想/物理ネットワークの再構成、移行、試験運用のプロセスで悪意の攻撃を受けないように、クラウド利用者にセキュリティ管理の徹底を助言すること。」が求められる。

13.2 情報の転送

【目的】

組織の内部及び外部に転送した情報のセキュリティを維持するため。

【補足事項】

教育クラウドプラットフォーム提供事業者は、認証基盤など複数の教材コンテンツと情報の転送が行われるシステムを提供するため、情報転送に必要な資源の割当がなされないと、教材コンテンツを含めた教育クラウドプラットフォーム全体のサービス低下を招く可能性があるほか、の完全性を損なうことにつながる。さらに内外の情報転送において、必要な安全措置が講じられていないと、盗聴等の情報漏えいが生じる等の可能性を生じる。

13.2.2 情報転送に関する合意

【管理策】

合意では、組織と外部関係者との間の業務情報のセキュリティを保った転送について、取り扱うことが望ましい。

【補足事項】

教育クラウドプラットフォームでは、教育クラウドプラットフォームとエンドユーザの間、及び教育クラウドプラットフォーム提供事業者とサービスプロバイダとの間での通信が発生することが想定される。いずれの通信についても、機微な情報が伝達される可能性があることから、適切な暗号化処理を行い、データの改ざんや盗聴への対策を行うことが求められる。

13.2.4 秘密保持契約又は守秘義務契約

【管理策】

情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ってレビューし、文書化することが望ましい。

【補足事項】

教育クラウドプラットフォームは海外の日本人学校が利用することが想定される。その利用者の個人情報や教育クラウドプラットフォーム提供事業者の機器に保存されることとなるが、日本人学校が存在する国及び地域と別の場所に保存する場合、その国及び地域から個人情報を移転する形となるため、その国及び地域の法令や規則に準拠する必要がある。関連する法令や規則をあらかじめ調査し、必要と考えられる対策を検討しておくことが望ましい。

15 供給者関係

15.1 供給者関係における情報セキュリティ

【目的】

供給者がアクセスできる組織の資産の保護を確実にするため。

【補足事項】

本節における「供給者」は、主に教材コンテンツ提供事業者と読み替えることができる。教育クラウドプラットフォームでは、複数の教材コンテンツ提供事業者の教材コンテンツがアグリゲーションサービスとして提供される。教育クラウドプラットフォーム提供事業者と教材コンテンツ事業者の間の情報セキュリティマネジメントに対するポリシーの違いに起因した脆弱性の発生や、障害時における対応等に係る管理責任等の範囲についての認識の齟齬などに伴う対応の遅延等から、結果として利用者へのサービス提供に支障をきたす恐れがある。そのため、教育クラウドプラットフォーム提供事業者と教材コンテンツ事業者の間でのポリシーの違い等から生じる実装面、運用面のリスクへの管理策が必要となる。

15.1.1 供給者関係のための情報セキュリティの方針

【管理策】

組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化することが望ましい。

【補足事項】

【利用者接点とサプライチェーンにおける実務のポイント】示され要件を満たすため、教育クラウドプラットフォーム事業者は、マーケットプレイス等による教育クラウドプラットフォーム上での教材コンテンツ提供に関する基準を設けることが求められる。教材コンテンツ提供に関する基準には、情報セキュリティに関し遵守すべき要件を含めることとし、教材コンテンツ事業者と合意し、契約として文書化することが望ましい。教材コンテンツの提供にあたり、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提供に関する基準を設け、確認を行うこと。

15.1.3 ICT サプライチェーン

【管理策】

供給者との合意には、情報通信技術（以下、ICT という。）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めることが望ましい。

【補足事項】

教育クラウドプラットフォームは、複数の教材コンテンツを統合的に提供するアグリゲーションサービスのため、一部の教材コンテンツのセキュリティリスクが、他の教材コンテンツや教育クラウドプラットフォーム全体に影響を及ぼす可能性がある。そのため、教育クラウドプラットフォーム提供事業者は、15.1.1 の補足事項に記載した教材コンテンツ提供に関する基準に、情報セキュリティリスクに対処するための要求事項を含めるとともに、教材コンテンツ提供事業者の利用規約、SLA 等の規定により、情報セキュリティマネジメントに関する要求事項への対応状況を確認し、教育クラウドプラットフォームの利用者の要求を満足できる教材コンテンツ提供事業者を選定することが求められる。

15.2 供給者のサービス提供の管理

【目的】

供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。

【補足事項】

15.1.3 により合意した情報セキュリティマネジメントの要求事項が、一部の教材コンテンツ提供事業者により管理されないことで、教育クラウドプラットフォーム全体の提供品質や情報セキュリティに影響を及ぼす恐れがあり、合意に留まらず合意レベルの維持していくことが求められる。

15.2.1 供給者のサービス提供の監視及びレビュー

【管理策】

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、監査することが望ましい。

【補足事項】

【利用者接点とサプライチェーンにおける実務のポイント】の(c)にある通り、教育クラウドプラットフォーム提供事業者は「提供するクラウドサービス全体についての監視、レビュー、監査実施に対する責任を果たすこと。」が求められる。15.1.1 の補足事項で記した「教材コンテンツ提供に関する基準」において、外部監査人による「クラウド事業者のセキュリティ管理に係る内部統制保証報告書」の提供を求めることで代替が可能であり、これによって教育クラウドプラットフォーム提供の管理統制業務の負担を軽減することができる。

15.2.2 供給者のサービス提供の変更に対する管理

【管理策】

関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、供給者によるサービス提供の変更（現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む。）を管理することが望ましい。

【補足事項】

教育クラウドプラットフォームは、複数の教材コンテンツを統合的に提供するアグリゲーションサービスのため、一部の教材コンテンツによるサービスの変更が、他の教材コンテンツや教育クラウドプラットフォーム全体に影響を及ぼす可能性がある。例として、一部の教材コンテンツでの属性情報の変更や学習の記録について誤りが発生した場合、全ての教材コンテンツにおいてそのデータをもとにサービスが提供される、などが想定される。

そのため、【利用者接点とサプライチェーンにおける実務のポイント】の(b)にある通り、「一部の供給者が行う変更に関する管理を行い、クラウドサービス全体として変更に伴う影響を最小限にするための対応策を講じること。」が求められ、また、(a)にある通り、「ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、供給者が提供するサービスの変更に伴う影響範囲等について事前に把握し、他の供給者が提供するサービスに不測の障害等を生じないように、必要な情報を提供すること。」の処置が求められる。

16 情報セキュリティインシデント管理

16.1 情報セキュリティインシデントの管理及びその改善

【目的】

セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。

【補足事項】

教育クラウドプラットフォームの場合、情報セキュリティインシデントはアグリゲーションしている教材コンテンツでも起こる可能性がある。情報セキュリティインシデント対応において、教材コンテンツ事業者を含め、一貫性のある効果的な取組みを行うことが求められる。

16.1.2 情報セキュリティ事象の報告

【管理策】

情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけ速やかに報告することが望ましい。

【補足事項】

教育クラウドプラットフォームでは、コンテンツ提供事業者との管理責任等の範囲に関する理解の齟齬等に起因して、情報セキュリティ事象の発見や対応切り分けに支障が出やすい。この課題を克服するために、教育クラウドプラットフォーム提供事業者と教材コンテンツ提供事業者間の管理責任等の分担範囲の明確化が求められる。

管理責任等の分担範囲の明確化においては、15.1.1 の補足事項で記した「教材コンテンツ提供に関する基準」などにおいて、【利用者接点とサプライチェーンにおける実務のポイント】(a)で記されている「クラウドサービス提供におけるそれぞれの管理責任等の範囲を明確に設定すること。」を文章化しておくことが望ましい。

16.1.4 情報セキュリティ事象の評価及び決定

【管理策】

情報セキュリティ事象は、これを評価し、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が望ましい。

【補足事項】

教育クラウドプラットフォーム事業者は、教育クラウドプラットフォームにおける情報セキュリティインシデントの分類基準を確立するとともに、教材コンテンツ提供事業者にもその基準を開示し、分類基準に応じた同様の対処を実施していくことが求められる。

16.1.7 証拠の収集

【管理策】

組織は、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用することが望ましい。

【補足事項】

教育クラウドプラットフォーム事業者は、情報セキュリティインシデントの事後対応における証拠収集・保全に関し、アグリゲーションしている教材コンテンツにおける証拠収集・保全が必要になる可能性がある。そのため、証拠となり得る情報の特定、収集、取得及び保存のための手順を教材コンテンツ事業者にも予め定め、適用することを求める必要がある。

その場合、クラウド利用者の権利を保護するため、【利用者接点とサプライチェーンにおける実務のポイント】に記されている「(c)クラウド利用者が行う証拠収集の制限事項について定義し、クラウド利用者と合意すること。」や「(d)クラウド利用者が、証拠として利用できる情報へのアクセスを要請し、その許諾を得るための手順をクラウド利用者と合意すること。このアクセスに費用や料金が発生する場合は、それを文書化してクラウド利用者に示すこと。」に関し、教育クラウドプラットフォーム事業者がアグリゲータとして代替して実施することが求められる場合がある。

17 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

17.2 冗長性

【目的】

情報処理施設の可用性を確実にするため。

【補足事項】

教育クラウドプラットフォーム提供事業者は、認証基盤など複数の教材コンテンツと情報の転送が行われるシステムを提供するため、サービスの停止は教材コンテンツを含めた教育クラウドプラットフォーム全体の停止を招く可能性がある。このため、教育クラウドプラットフォーム事業者が提供するシステムに関する情報処理施設の可用性確保は、最優先事項として取り組むことが求められる。

17.2.1 情報処理施設の可用性

【管理策】

情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入することが望ましい。

【補足事項】

【利用者接点とサプライチェーンにおける実務のポイント】の(a)にて「ID 管理サービス、課金サービスなどの基幹機能において、単一障害点となっているものを特定し、十分な冗長性と障害時の円滑な切替を確保すること。」と記されている通り、複数の教材コンテンツが利用するシステムにおいては、特に十分な冗長性と障害時の切替方法の確保が求められる。教育クラウドプラットフォームにおいては、共通利用するシステムとして認証基盤、ポータルが必須要件となっており、推奨要件としてもマーケットプレイス、学習記録データストア、コンテンツメタデータ管理があり、これらのシステムについては特に十分な対処が求められる。

18 順守

18.1 法的及び契約上の要求事項の順守

【目的】

情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。

【補足事項】

教育クラウドプラットフォームにおいては、在外教育施設での利用など、サービス対象となる国が複数にわたるケースが想定される。また、パブリッククラウドサービスでの提供を前提としていることから、複数の国等に存在する資源を利用するクラウドサービスを利用しサービス提供することも想定される。利用者、及び利用するクラウド事業者の適用法を踏まえたサービス提供が求められる。

18.1.1 適用法令及び契約上の要求事項の特定

【管理策】

各情報システム及び組織について、全ての関連する法令、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り組みを、明確に特定し、文書化し、また、最新に保つことが望ましい。

【補足事項】

在外教育施設や日本国外の利用者に対して教育クラウドプラットフォームを提供する場合、【利用者接点とサプライチェーンにおける実務のポイント】で示された「(a) 複数国のクラウド利用者に対してサービス提供を行う、又は複数国の資源やサービスを利用してサービス提供を行うクラウド事業者は、サービス対象や利用資源が越境することによってクラウドサービスに生じうる、適用法の違いによるリスクを事前に把握すること。」を踏まえ、利用者の国での法令に則った対応が必須となる。また、複数の国等に存在する資源を用いてクラウドサービスを提供する場合、適用法令の違いから、当該資源が存在する国の法令違反を疑われ、当該国の司法官憲等による記録媒体の差押え等によって、サービス提供ができない状態に陥る恐れがある。そのため、【利用者接点とサプライチェーンにおける実務のポイント】で示された「(b) 複数国の資源やサービスを利用してサービス提供を行うクラウド事業者は、当該資源やサービスが存在する国において適用される法令等に係るリスクに対して、サービス提供上必要な措置を講じること。」を踏まえてサービス提供することが求められる。

18.1.2 知的財産権

【管理策】

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の順守を確実にするための適切な手順を実施することが望ましい。

【補足事項】

18.1.1 の補足事項で記した要件と同様に、利用者、利用するクラウドサービスに適用される法令、規制等を踏まえたサービス提供が求められる。教育クラウドプラットフォームは複数の教材コンテンツのアグリゲーションサービスであるため、教材コンテンツについても同様に適法される法令、規制等に応じた知的財産権への対応が求められる。

18.1.3 記録の保護

【管理策】

記録は、法令、規制、契約及び業務上の要求事項に従って、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が望ましい。

【補足事項】

複数の国等に存在する資源を用いてクラウドサービスを提供する場合、適用法令の違いから、当該資源が存在する国の法令違反を疑われ、当該国の司法官憲等による記録媒体の差押え等によって、サービス提供ができない状態に陥る恐れがある。それらの対応として、12.3 で記したバックアップについての考え方を踏まえ、【利用者接点とサプライチェーンにおける実務のポイント】の(a)「当該国の司法官憲等の不測の差押えを受けた場合であっても、クラウドサービスが停止しないように、国境を越えたバックアップを行う等の必要な措置を講じること。」や(b)「無関係なクラウド利用者の預託情報が一緒に流出しないように、預託情報を容易に分離できる等の必要な措置を講じること。」の対応が求められる。

18.1.4 プライバシー及び個人を特定できる情報（PII）の保護

【管理策】

プライバシー及び PII の保護は、関連する法令及び規制が適用される場合には、その要求に従って確実にすることが望ましい。

【補足事項】

18.1.1 の補足事項で記した要件と同様に、利用するクラウドサービスに適用される法令、規制等を踏まえたプライバシー及び PII の保護が求められる。教育クラウドプラットフォームは複数の教材コンテンツのアグリゲーションサービスであるため、教材コンテンツについても同様に適法される法令、規制等に応じたプライバシー及び PII の保護が求められる。

18.1.5 暗号化機能に対する規制

【管理策】

暗号化機能は、関連する全ての協定、法令及び規制を順守して用いることが望ましい。

【補足事項】

18.1.1 の補足事項で記した要件と同様に、利用者、利用するクラウドサービスに適用される法令、規制等を踏まえた暗号化機能が求められる。教育クラウドプラットフォームは複数の教材コンテンツのアグリゲーションサービスであるため、教材コンテンツについても同様に適法される法令、規制等に応じた暗号化機能が求められる。また、国によっては公的秩序等の観点から、暗号化通信等を禁止しているケースがあり、暗号化機能の適用範囲について留意が必要となる。

18.2 情報セキュリティのレビュー

【目的】

組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。

【補足事項】

教育クラウドプラットフォームの場合、教育クラウドプラットフォーム提供事業者による情報セキュリティマネジメントのレビューを実施するだけでは、目標とするサービスレベルを確保する方策としては不十分であり、アグリゲーションする教材コンテンツ提供事業者との関係でもレビューを実施することが求められる。

18.2.1 情報セキュリティの独立したレビュー

【管理策】

情報セキュリティ及びその実施の管理（例えば、情報セキュリティの管理目的、管理策、方針、プロセス、手順）に対する組織の取組みについて、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施することが望ましい。

【補足事項】

教育クラウドプラットフォーム提供事業者は、教材コンテンツを含めた教育クラウドプラットフォーム全体に対する管理責任を果たすのに必要なレビュー・監査等を実施できる対応策を講じることが求められる。そのため【利用者接点とサプライチェーンにおける実務のポイント】の(b)で記されている「供給者が行う独立したレビュー・監査の実施方針について把握し、必要な調整を行うことで、ICT サプライチェーン全体においてレビュー・監査等に係る一貫した方針の適用が必要な範囲を明

確にし、これを適用するための措置を講じること。」の実施が必要となる。具体的には、の実施方針を開示し、教材コンテンツ事業者による情報セキュリティ及びその実施の管理に対するレビュー・監査内容を把握し、必要に応じて一貫した方針となるよう調整を行うことが必要となる。

18.2.2 情報セキュリティのための方針群及び標準の順守

【管理策】

権利者は、自分の責任の範囲内における情報処理及び手順が、適切な情報セキュリティのための方針群、標準類、及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューすることが望ましい。

【補足事項】

教育クラウドプラットフォーム提供事業者は、教材コンテンツを含めた教育クラウドプラットフォーム全体に対する管理責任を果たすために、適切な情報セキュリティマネジメントのための方針群、標準類等が順守されているかを定期的にレビューすることが求められる。そのため【利用者接点とサプライチェーンにおける実務のポイント】の(a)で記されている「供給者が行う情報セキュリティマネジメントのための方針群、標準類等の順守に係る定期的なレビュー結果を入手し、必要な調整を行うことで、ICT サプライチェーン全体において一貫した定期的レビューを行う範囲を明確にし、各供給者にこれを実施させるための措置を講じること。」の実施が必要となる。具体的には、教材コンテンツ事業者による方針群、標準類等の順守に係る定期的なレビュー結果を把握し、必要に応じて一貫した方針となるよう調整を行うことが必要となる。

18.2.3 技術的順守のレビュー

【管理策】

情報システムを、組織の情報セキュリティのための方針群及び標準の順守に関して、定めに従ってレビューすることが望ましい。

【補足事項】

教育クラウドプラットフォームにおいて、特定の教材コンテンツに依存し、あるいは影響を受ける部分を有する場合には、その教材コンテンツに係る技術的な順守状況を監視することが求められるが、教材コンテンツ事業者の機密であることを理由としてレビュー結果が教育クラウドプラットフォーム事業者に提供されず、十分なレビュー等ができない恐れがある。そういった懸念への対応として、教育クラウドプラットフォーム事業者は、教材コンテンツ提供事業者と機密保持契約の締結等、必要な措置を講じ、当該教材コンテンツの技術的な順守状況のレビュー結果等を入手できるようにする必要がある。



クラウド環境構築ガイドブック

平成 29 年 7 月 31 日
エヌ・ティ・ティ・コミュニケーションズ株式会社

Transform your business, transcend expectations with our technologically advanced solutions.

目次

1. ガイドブックの目的及び概要	3
1.1 ガイドブックの目的	3
1.2 教育クラウドプラットフォームの概要	3
2. プロトタイプにおけるシステム構成.....	5
3. アイデンティティプロバイダ (IdP)	6
3.1 動作環境.....	6
3.1.1 サーバ構成	6
3.1.2 OS・モジュール.....	6
3.2 IdP サーバ構築手順	6
3.2.1 IdP の設定	6
3.2.2 エンティティ・認証メタデータの作成.....	7
3.3 LDAP サーバ構築手順	8
3.3.1 スキーマの追加設定.....	8
3.3.2 テストデータ作成	8
4. 属性情報プロバイダ (AtrP)	9
4.1 動作環境.....	9
4.1.1 サーバ構成	9
4.1.2 OS・モジュール.....	9
4.2 AtrP サーバの構築.....	9
4.2.1 AtrP の設定.....	9
4.2.2 Back-Channel (SOAP) 通信の設定	9
4.3 LDAP サーバの構築	11
4.3.1 スキーマの追加設定.....	11
4.3.2 テストデータ作成	11
5. サービスプロバイダ (SP)	12
5.1 動作環境.....	12

5.1.1 サーバ構成	12
5.1.2 OS・モジュール.....	12
5.2 SP サーバ構築手順	12
5.2.1 SP の設定	12
5.2.2 エンティティ・認証メタデータの作成.....	13
5.2.3 ロケーションの設定.....	13
5.2.4 利用学校の認可設定.....	13
5.2.5 属性情報の利用設定.....	13
5.3 リバースプロキシ構築手順.....	14
5.3.1 Apache の設定変更.....	14

1.ガイドブックの目的及び概要

1.1ガイドブックの目的

「教育クラウドプラットフォーム参考技術仕様」（以下「参考技術仕様」という。）は、教育クラウドプラットフォームを実装する際の一例として、クラウド環境で実装された複数の教材コンテンツをシングルサインオンで利用することができ、異なるプラットフォームの間でも、相互にデータ連携を行うことができる教育クラウドプラットフォームに求められる技術要件について取りまとめている。

本ガイドブックは、参考技術仕様に基づき、教育クラウドプラットフォームを新たに提供する事業者、システム更改をする事業者に対し、教育クラウドプラットフォームのクラウド環境（PaaS）の必須要件である認証基盤について、総務省が平成 26 年度から平成 28 年度まで実施した「先導的教育システム実証事業」（以下「本事業」という。）において実証に用いたプロトタイプ of の構築手順を示すことにより、その実行環境の構築の一助となることを目的としている。

本事業で作成した参考技術仕様及び各ガイドブックと教育クラウドプラットフォームの開発工程との関係については、下図 1-1 で示すとおりであり、本ガイドブックは、クラウド環境の構築に係る設計から実装までに係るプロセスに関し、事業者の参考となることを想定している。

	要求定義	要件定義	設計	実装
全体構成/ 相互運用性	参考技術仕様			
セキュリティ	セキュリティ要件 ガイドブック			
クラウド環境 (PaaS/IaaS)			クラウド環境構築 ガイドブック	
教材コンテンツ			コンテンツ作成 ガイドブック	
		アクセシビリティ ガイドブック		

図 1-1 参考技術仕様・各ガイドブックと教育クラウドプラットフォーム開発工程との関係

1.2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 1-2 に示す。

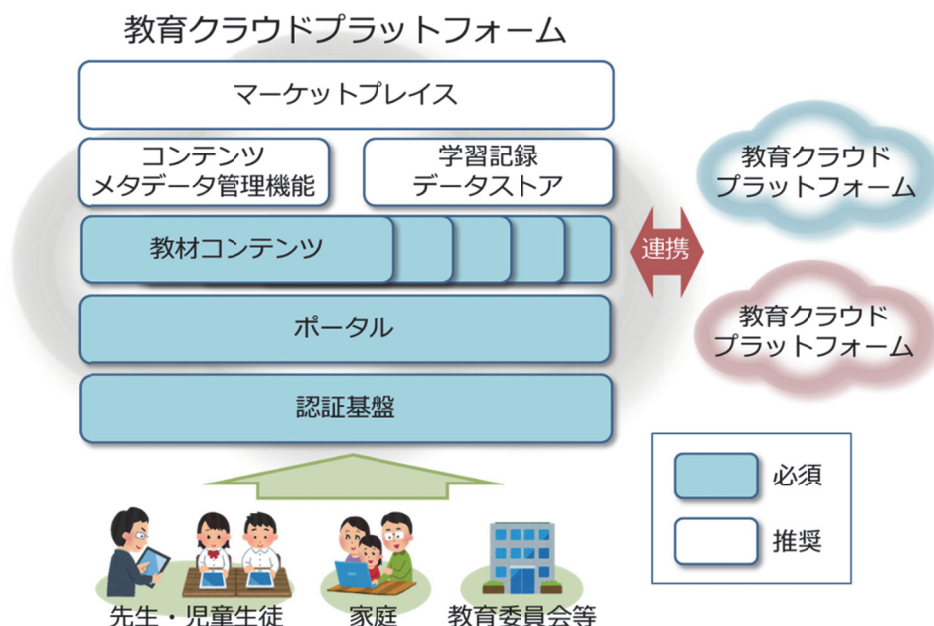


図 1-2 教育クラウドプラットフォームの概要

参考技術仕様で示された教育クラウドプラットフォームは、多様な主体による参入を可能とすることにより、健全な競争環境の実現や事業継続性の確保を実現するため、教育クラウドプラットフォームを構成する要素をモジュール化した上で、プラットフォーム相互間での連携も可能とするアーキテクチャを採用している。

教育クラウドプラットフォームの構成要素のうち、利用者が授業・学習時に利用するポータルや教材コンテンツの相互連携を実現するクラウド環境（PaaS）については、認証基盤、マーケットプレイス、学習記録データストア、コンテンツメタデータ管理があり、このうち、認証基盤は参考技術仕様において必須要件となっている。本ガイドブックは、本事業のプロトタイプで実装した手順に基づき作成されており、教育クラウドプラットフォームを新たに提供する事業者が、認証基盤を構築する際の具体的な手順の例を提供する。

2. プロトタイプにおけるシステム構成

本事業の教育クラウドプラットフォームのプロトタイプにおいて、認証プロトコルは、国際規格で広く一般で普及しており、日本では国立情報学研究所¹と大学・研究機関が構成する学術認証フェデレーション²（以下、学認）でも採用実績がある SAML2.0³を採用した。

プロトタイプでは、認証連携や属性情報の連携を実現するにあたり、以下の構成要素を実装している。

① アイデンティティプロバイダ (IdP)

教育クラウドプラットフォームへのアクセス者への認証を行い、アイデンティティ情報 (ID・パスワード等) の提供を行うもの。

② 属性情報プロバイダ (AtrP)

教育クラウドプラットフォームの利用者の属性情報 (所属学校・学年等) の提供を行うもの。

③ サービスプロバイダ (SP)

認証基盤により提供される認証情報を信頼し、利用者にサービスを提供するもの。プロトタイプにおいては、教育クラウドプラットフォームにおいては、教材コンテンツ、ポータル、マーケットプレイス及び学習記録データストアが該当する。

上記の実装にあたっては、SAML2.0 に対応した Shibboleth を採用している。Shibboleth は Internet2⁴が開発、提供しているオープンソースであり、日本でも学認において広く採用されており、学認による技術ガイドや米国 Shibboleth Consortium による参考情報など、様々な関連情報が提供されている。

次章以降にて、プロトタイプにおける各構成要素の構築手順を示す。

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 SSO 認証や第三者へのリソース利用認可のためのプロトコルとデータ形式に関する国際標準仕様群。インターネット技術に関する国際標準化団体 OASIS により 2015 年 3 月から公開された。

⁴ 米国の最先端ネットワーキングコンソーシアム。高等教育機関、企業、政府機関などが参画している

3. アイデンティティプロバイダ (IdP)

3.1 動作環境

3.1.1 サーバ構成

IdP を構築するにあたり、IdP サーバと LDAP サーバは同一サーバで提供することも可能だが、セキュリティを考慮し、プロトタイプでは IdP サーバと LDAP サーバを分離して構築した。LDAP サーバを TRUST セグメントに設置し、IdP サーバを DMZ セグメントに設置した構成としている。

3.1.2 OS・モジュール

IdP サーバ、LDAP サーバの構築にあたり、以下の OS、モジュールを利用した。

- ・ IdP サーバ・LDAP サーバ共通
 - ・ CentOS 6.4
- ・ IdP サーバ
 - ・ Apache 2.2.15
 - ・ Tomcat 8.0.15
 - ・ JDK 1.7
 - ・ Shibboleth IdP 2.4.2
- ・ LDAP サーバ
 - ・ OpenLDAP 2.4

3.2 IdP サーバ構築手順

3.2.1 IdP の設定

①パラメータの設定

- ・ handler.xml

IdP が行う認証の方式として、下記の通り ID/パスワード認証を選択。

<!-- Login Handlers -->のブロックをコメントアウト。

<!--Username/password login handler -->のブロックにあるコメントを外して有効化。

- ・ login.config

IdP が行う認証では、「3.3 LDAP サーバ構築手順」で設定する LDAP を用いるため、下記の通り LDAP との接続設定を行う。

ShibUserPassAuth {...}内のコメントを外して有効化。

上記で有効化した ldapUrl, baseDn, ssl の各設定を下記の通り記載。

```
ldapUrl = "ldap://localhost"
```

```
baseDn="<ldap に設定するベース DN>"  
ssl="false"
```

下記の行を追記。

```
subtreeSearch="true"
```

②一部設定ファイルをプロトタイプ用設定ファイル（Appendix 参照）へ置換え

• attribute-resolver.xml

インストールされている"/opt/shibboleth-idp/conf/attribute-resolver.xml"と置換える。

IdP が送信する属性は、「3.3 LDAP サーバ (IdP 用) 構築」で設定する LDAP から取得するため、下記の通り LDAP との接続設定を実施。

```
<!--Example LDAP Connector -->
```

 ブロックのコメントを外して有効化。

上記で有効化した ldapURL, baseDN, principal, principalCredential の各行にて、LDAP の URL、ベース DN、principal、principal のパスワードをそれぞれ設定。

• attribute-filter.xml

インストールされている"/opt/shibboleth-idp/conf/attribute-filter.xml"と置換える。

• logout.jsp

インストールされている"/usr/java/tomcat/webapps/idp/logout.jsp"と置換える。

③認証メタデータ証明書の設定

認証メタデータ署名証明書"jsfed-signer-2015.pem"を下記に設置。

```
/opt/shibboleth-idp/credentials/jsfed-signer-2015.pem
```

設置したファイル名を relying-party.xml に設定する。

```
<!-- Trust engine used to evaluate the signature on loaded metadata. -->
```

 の内容にあるコメントを外し有効化。

有効化した中の<Certificate>に証明書のファイル名を設定。

3.2.2 エンティティ・認証メタデータの作成

エンティティ認証メタデータ・テンプレートファイル ("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。

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 ファイルの中身を書き換。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。

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。

3.3 LDAP サーバ構築手順

3.1.2 で示した OpenLDAP の初期設定を行ったうえで、プロトタイプとして行った手順を記述している。

3.3.1 スキーマの追加設定

以下の追加スキーマ（Appendix 参照）を LDAP サーバに登録。

- eduPerson スキーマ
- Gakunin スキーマ
- jsfedperson.schema

3.3.2 テストデータ作成

idp-test.ldif（Appendix 参照）を利用してテスト用データを LDAP へ登録。

4.属性情報プロバイダ (AtrP)

4.1 動作環境

4.1.1サーバ構成

AtrP を構築するにあたり、AtrP サーバと LDAP サーバは同一サーバで提供することも可能だが、セキュリティを考慮し、プロトタイプでは AtrP サーバと LDAP サーバを分離して構築した。LDAP サーバを TRUST セグメントに設置し、AtrP サーバを DMZ セグメントに設置した構成としている。

4.1.2 OS・モジュール

AtrP サーバ、LDAP サーバの構築にあたり、以下の OS、モジュールを利用した。

- ・ AtrP サーバ・LDAP サーバ共通
 - ・ CentOS 6.4
- ・ AtrP サーバ
 - ・ Apache 2.2.15
 - ・ Tomcat 8.0.15
 - ・ JDK 1.7
 - ・ Shibboleth IdP 2.4.2
- ・ LDAP サーバ
 - ・ OpenLDAP 2.4

4.2AtrP サーバの構築

4.2.1 AtrP の設定

AtrP サーバの設定は、「3.2 IdP サーバの構築手順」にしたがって IdP サーバを構築し、下記の追加設定を行うことで完了となる。

「3.2 IdP サーバの構築手順 ②」で利用する下記のファイルは、AtrP 用の設定ファイル(Appendix 参照)を利用した。

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

4.2.2 Back-Channel (SOAP) 通信の設定

IdP との通信時に Transport Layer Security (TLS) 接続を行うため、Back-Channel の設定を行った。設定手順は学認の技術ガイドを参考にして実施している。以下、学認の技術ガイドより手順を抜粋して記載

する。

①キーストアの設定

以下の通り、サーバ証明書を格納したキーストアを作成。

```
# cd /opt/shibboleth-idp/credentials
# openssl pkcs12 -export -out pkcs12.p12 -in サーバ証明書.crt -inkey サーバ秘密鍵.key -name
サーバ名
(ここで聞かれるエクスポートパスワードにはキーストアパスワードと同じものを指定)
# keytool -importkeystore -srckeystore pkcs12.p12 -destkeystore keystore.jks ¥
-srcstoretype pkcs12 -deststoretype jks -srcalias サーバ名 -destalias サーバ名 ¥
-storepass キーストアパスワード
# rm pkcs12.p12
# chmod 600 /opt/shibboleth-idp/credentials/keystore.jks
```

Tomcat を"tomcat"ユーザで実行する場合は、さらに以下のコマンドを実行し Tomcat が読み取れるように設定。

```
# chgrp tomcat /opt/shibboleth-idp/credentials/keystore.jks
# chmod g+r /opt/shibboleth-idp/credentials/keystore.jks
```

②ライブラリのコピー

tomcat6-dta-ssl-2.0.0.jar (Appendix 参照) を\$CATALINA_HOME/lib 配下にコピーする。

```
# wget https://build.shibboleth.net/nexus/content/repositories/releases/edu/internet2/middle
deware/security/tomcat6/tomcat6-dta-ssl/2.0.0/tomcat6-dta-ssl-2.0.0.jar
# cp tomcat6-dta-ssl-2.0.0.jar $CATALINA_HOME/lib
```

②SOAP 設定

\$CATALINA_BASE/conf/server.xml ファイルに以下を追加する。

```
<Connector port="8443"
    protocol="org.apache.coyote.http11.Http11Protocol"
    SSLImplementation="edu.internet2.middleware.security.tomcat6.DelegateToApplicati
onJSSEImplementation"
    scheme="https"
    maxPostSize="100000"
    SSLEnabled="true"
    clientAuth="want"
    sslProtocols="TLSv1,TLSv1.1,TLSv1.2"
    sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
    keystoreFile="/opt/shibboleth-idp/credentials/keystore.jks"
    keystoreFile="キーストアパスワード" />
```

4.3 LDAP サーバの構築

3.1.2 で示した OpenLDAP の初期設定を行ったうえで、プロトタイプとして行った手順を記述している。

4.3.1 スキーマの追加設定

以下の追加スキーマ（Appendix 参照）を LDAP サーバに登録。

- eduPerson スキーマ
- Gakunin スキーマ
- jsfedperson.schema

4.3.2 テストデータ作成

atrp-test.ldif（Appendix 参照）を利用してテスト用データを LDAP へ登録。

5. サービスプロバイダ (SP)

5.1 動作環境

5.1.1 サーバ構成

SP を構築するにあたり、プロトタイプでは教材コンテンツのサーバで SP を構築する構成と、既存の教材コンテンツサーバに SP を構築できない場合に対応するため、リバースプロキシを介することで教材コンテンツサーバを SP として設定する構成の 2 つの方式を提供した。

「5.2 SP サーバ構築手順」では 2 つの方式で共通の手順を示し、「5.3 リバースプロキシ構築手順」にて、リバースプロキシを用いた方式で追加すべき手順を示している。

5.1.2 OS・モジュール

SP サーバの構築にあたり、以下の OS、モジュールを利用した。

- ・ CentOS 6.4
- ・ Apache 2.2.15
- ・ Shibboleth IdP 2.4.2

5.2 SP サーバ構築手順

5.2.1 SP の設定

①一部設定ファイルをプロトタイプ用設定ファイル (Appendix 参照) へ置換え

- ・ shibboleth2.xml

インストールされている/etc/shibboleth/shibboleth2.xml と置換える。

置換えた後、ホスト名を記入する。

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

- ・ attribute-map.xml

インストールされている/etc/shibboleth/attribute-map.xml と置換える。

- ・ attribute-policy.xml

インストールされている/etc/shibboleth/attribute-policy.xml と置換える。

②認証メタデータ署名証明書を設置

認証メタデータ署名証明書 “jsfed-signer-2015.pem” を下記に設置。

/etc/shibboleth/cert/jsfed-signer-2015.pem

証明書のファイル名が異なる場合は、①で置換えた shibboleth2.xml 内の証明書のファイル名を修正する。設置したファイル名を relying-party.xml に設定する。

5.2.2 エンティティ・認証メタデータの作成

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、下記の作業を実施し、エンティティ認証メタデータを作成。

① shibboleth 用証明書に記載 (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。
entity-metadata-template.xml の “[HOST_NAME]” 部分を、IdP サーバのホスト名に変更。

5.2.3 ロケーションの設定

Shibboleth のデフォルト設定では、/secure へのアクセス時に認証が行われる。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 SP サーバとなるため、/etc/httpd/conf.d/shib.conf 内の <Location/secure> を修正する。

5.2.4 利用学校の認可設定

教材コンテンツの利用を認可している学校のみがアクセス可能となる設定を行う。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>
```

教材コンテンツの利用を認可している学校のみがアクセス可能となる設定を行う。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 >

5.2.5 属性情報の利用設定

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ために、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”を追記する。  
  require shib-session  
</Location>
```

5.3 リバースプロキシ構築手順

教材コンテンツのサーバに SP を構築できない等の場合、教材コンテンツのサーバと IdP サーバ/AtrP サーバの間に Shibboleth SP のリバースプロキシを設置し、リバースプロキシを経由することで教材コンテンツサーバを SP として設定することができる。プロトタイプのリバースプロキシの構築は、「5.2 SP サーバの構築手順」に以下の追加手順を行うことで完了となる。

5.3.1 Apache の設定変更

Apache の httpd.conf に対し、接続する教材コンテンツのサーバに関する設定を行う。

【設定例】

既存のコンテンツサーバの URL が https://edu-example.org/の場合

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




コンテンツ作成ガイドブック

平成 29 年 7 月 31 日
エヌ・ティ・ティ・コミュニケーションズ株式会社

Transform your business, transcend expectations with our technologically advanced solutions.

目次

1. ガイドブックの目的及び概要	2
1.1 ガイドブックの目的	2
1.2 教育クラウドプラットフォームの概要	3
2. 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	5
2.1 OS の違いによる教材コンテンツの開発手法の違い.....	5
2.2 対象とする OS ・ブラウザの多様性による検証工数の増加	7
2.3 HTML5 コンテンツの開発生産性	8
2.4 HTML5 が利用可能な環境の制約	8
3. コンテンツメタデータ	9
3.1 国際標準規格.....	9
3.2 学習要素リスト.....	10

1. ガイドブックの目的及び概要

1.1 ガイドブックの目的

「教育クラウドプラットフォーム参考技術仕様」（以下「参考技術仕様」という。）は、教育クラウドプラットフォームを実装する際の一例として、クラウド環境で実装された複数の教材コンテンツをシングルサインオンで利用することができ、異なるプラットフォームの間でも、相互にデータ連携を行うことができる教育クラウドプラットフォームに求められる技術要件について取りまとめている。

本ガイドブックは、参考技術仕様で求められる要件を踏まえ、実際にコンテンツ提供事業者が教育クラウドプラットフォーム上の教材コンテンツを開発・実装する際の設計指針や、開発・実装のプロセスにおける要件を整理することを目的としている。

総務省が平成 26 年度から平成 28 年度まで実施した「先導的教育システム実証事業」で作成した参考技術仕様及び各ガイドブックと教育クラウドプラットフォームの開発工程との関係については、下図 1-1 で示すとおりであり、本ガイドブックが、教育クラウドプラットフォーム上の教材コンテンツ制作の範囲で、設計から開発・実装に係るプロセスに関し、事業者の参考となることを想定している。

	要求定義	要件定義	設計	実装
全体構成/ 相互運用性	参考技術仕様			
セキュリティ	セキュリティ要件 ガイドブック			
クラウド環境 (PaaS/IaaS)			クラウド環境構築 ガイドブック	
教材コンテンツ			コンテンツ作成 ガイドブック	
		アクセシビリティ ガイドブック		

図 1-1 参考技術仕様・各ガイドブックと教育クラウドプラットフォーム開発工程との関係

1.2 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 1-2 に示す。

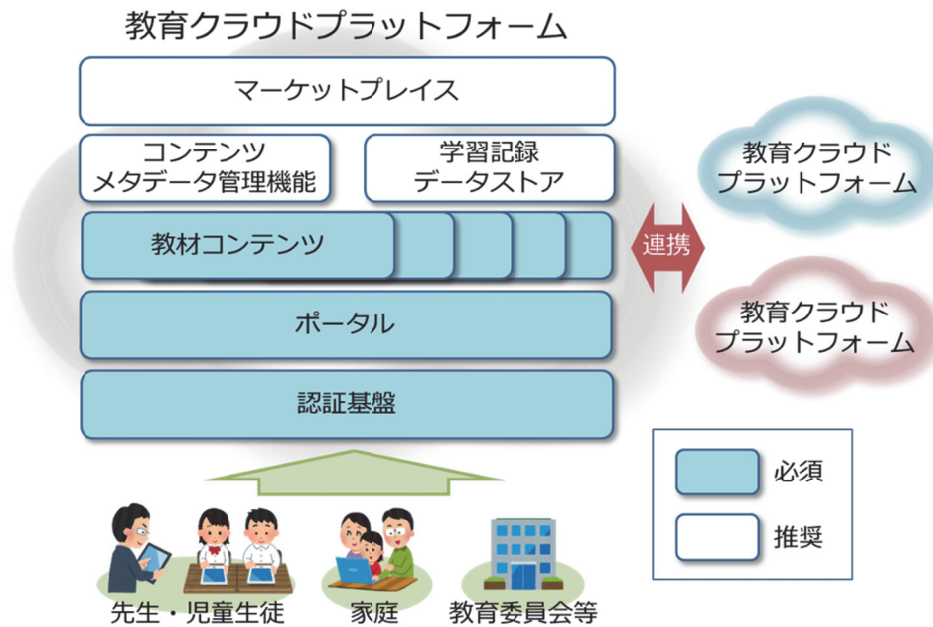


図 1-2 教育クラウドプラットフォームの概要

参考技術仕様に準拠した教育クラウドプラットフォーム相互間では、クラウド環境で実装された複数の教材コンテンツのシングルサインオンによる利用や学習履歴等に係るデータ連携を行うことが可能になる。コンテンツ提供事業者にとっては、教育クラウドプラットフォーム上に教材コンテンツを提供することにより、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、コンテンツ提供事業者が新たに 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。

また、教材コンテンツを広く流通させる上で重要な要素のひとつであるコンテンツメタデータについて記載する。各教材コンテンツについてコンテンツメタデータを整備することにより、教材コンテンツの検索性や、教材コンテンツ間の連携が可能となる。

2. 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

2.1 OS 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教材コンテンツ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/)

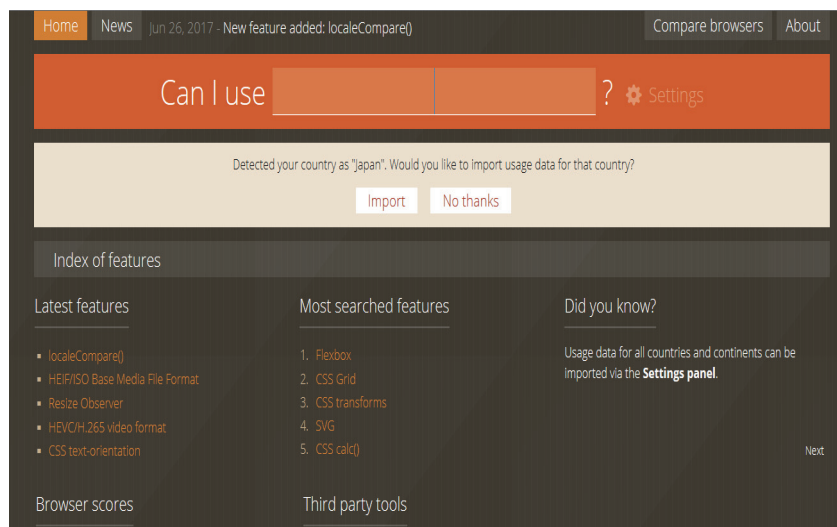


図 2-1 Web サイト「Can I use...」のトップページ

図 2-1 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。

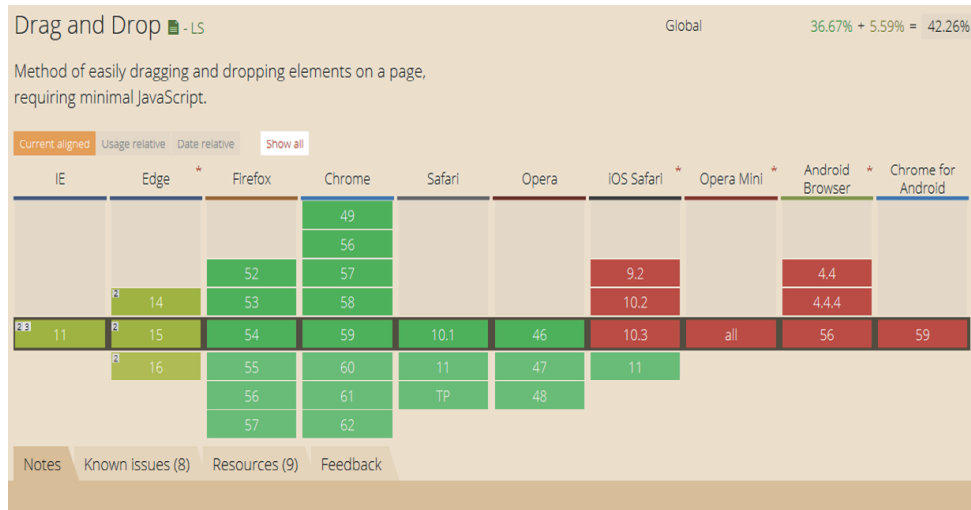


図 2-2 Drag and Drop 機能の対応状況

図 2-2 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 機能に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 issues) 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/>)

The screenshot shows the 'MOBILE HTML5' website with a large '5' logo and a table titled 'HTML5 compatibility on mobile and tablet browsers with testing on real devices'. The table lists various HTML5 features and their support status across different browsers and devices.

Feature	Safari iOS	Android Browser	Samsung Internet	Google Chrome	Amazon Silk	BlackBerry Browser	Nokia Browser	Internet Explorer	Opera Mobile	Opera mini	Firefox
Application Cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web storage	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web SQL storage	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IndexedDB	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Geolocation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Multimedia	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web Workers	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Viewport definition	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

図 2-3 Web サイト「Mobile HTML5」のトップページ

図 2-3 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。教育用のコンテンツ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。

2.2 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。また、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提供事業者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ふ。

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 やブラウザが頻り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。

2.3 HTML5 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提供事業者も存在する。

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提供事業者としては非常に重要な要素と言えるだろう。

2.4 HTML5 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(以下「IE」という。)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。

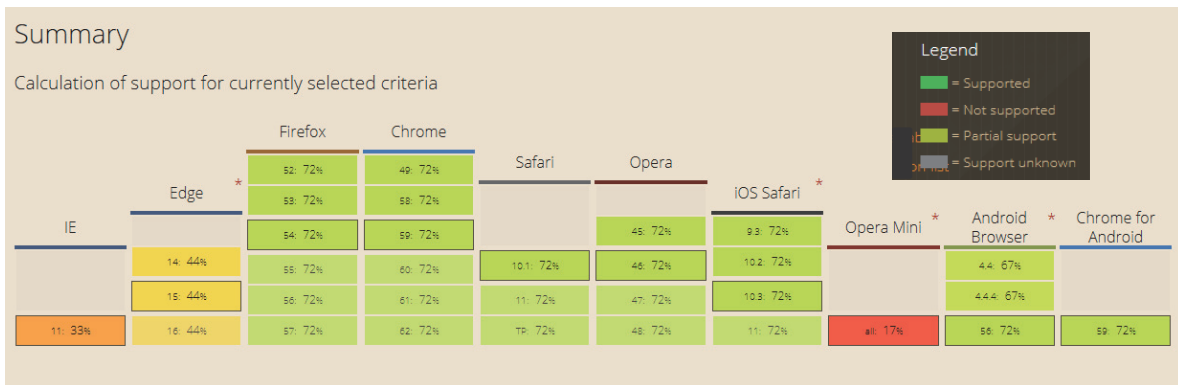


図 2-4 HTML5 全機能の対応状況

図 2-4 は 2.1 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 IE では IE11 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、不得意があり、また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。

実証内容 平成 28 年度「最先端情報通信技術を活用した教育クラウドプラットフォームに関する実証」
実施報告書
➤ 4.3 教材コンテンツ

3. コンテンツメタデータ

3.1 国際標準規格

複数の教材コンテンツプラットフォームの間にてメタデータを相互にやり取りすることを目的とし作成されたメタデータ体系として、LOM (Learning Object Metadata) が存在する。IEEE¹により標準化が行われ、現在は IEEE1484.12.3-2005 という標準として規定されている。LOM は教材コンテンツに特化したメタデータであり、下記の特徴をもつ。

- デジタル教材、非デジタル教材の両方が対象
- 9つの属性と、その要素を細分化したサブ属性の複数階層構造（表 3-1）。
- LOM に定義された属性のうち使用する属性を選択する、もしくはオリジナルの属性を定義して使用する、などのカスタマイズが可能

表 3-1 に、LOM の項目およびその内容を示す。

表 3-1 LOM の項目（『情報処理』2005 年 6 月 46 巻 6 号より引用²）

No	項目名	項目名 (日本語)	説明
1	General	一般	このカテゴリには、学習オブジェクト全体としての一般的な情報が記述される。 このカテゴリに属する項目は、学習オブジェクトの識別子、タイトル、学習オブジェクトで使用されている主な言語、学習オブジェクトの説明、キーワード、対象とする範囲、構造、機能的な粒度である。
2	Lifecycle	ライフ サイクル	このカテゴリには、この学習オブジェクトの履歴、現在の状況やその影響を与えた人や、機関などの情報が記述される。 このカテゴリに属する項目は、バージョン、ステータス、この学習オブジェクトに寄与した人または機関に関する記述である。
3	Meta-Metadata	メタメタ データ	このカテゴリには、このメタデータそのものについて記述される。 このカテゴリに属する項目は、このメタデータの識別子、このメタデータに寄与した人または機関に関する記述、メタデータのスキーマ、このメタデータで使用されている言語である。
4	Technical	技術的な 情報	このカテゴリには、この学習オブジェクトに必要な技術的要件や、技術的な特徴が記述される。 このカテゴリに属する情報は、この学習オブジェクトのフォーマット（データタイプ）、データサイズ、学習オブジェクトにアクセス

¹ Institute of Electrical and Electronics Engineers の略。人間社会における有益な技術的なイノベーションの促進を目的とした米国の公益法人。 <http://www.ieee.org/index.html>

² 「学習対象メタデータ (LOM) 付与による教育用コンテンツの共有と流通」 (清水 康敬, 2005)

No	項目名	項目名 (日本語)	説明
			できる場所 (URL など)、技術的要件、インストール方法、その他の要件、再生時間である。
5	Educational	教育的な特徴	このカテゴリには、この学習オブジェクトの教育的な特徴が記述される。 このカテゴリに属する項目は、対話のタイプ、学習オブジェクトの種類、対話性のレベル、意味的な密度 (簡潔さ)、対象とするユーザの種類、この学習オブジェクトが利用される場面、対象年齢、難易度、学習時間である。利用に関するコメント、対象とするユーザの主な使用言語である。
6	Rights	権利に関する情報	このカテゴリには、この学習オブジェクトの知的所有権と使用に関する条件が記述される。 このカテゴリに属する項目は、この学習オブジェクトの値段、著作権その他の制限、利用条件に関するコメントである。
7	Relation	学習オブジェクト間の関係	このカテゴリには、この学習オブジェクトと他の学習オブジェクトとの関係性が記述される。 このカテゴリに属する項目は、関係の種類、関係する学習オブジェクトである。
8	Annotation	注釈	このカテゴリには、この学習オブジェクトの教育的な利用に関するコメントが記述される。 このカテゴリに属する項目は、この注釈を記述した人または機関、注釈を記述した日付、注釈である。
9	Classification	分類	このカテゴリには、この学習オブジェクトが、どの分類体系のどこに位置するのかが記述される。 このカテゴリに属する項目は、この学習オブジェクトを分類する目的、分類体系の名前とそのどこに位置するかを表すパス、分類の目的に対する説明・キーワードである。

この LOM は XML 形式で作成され、教材コンテンツとともにデータのやり取りが行われる。教材コンテンツの内容を示すメタデータを標準的な規格にて整備することにより、教材コンテンツの検索性や相互の連携が可能となる。

3.2 学習要素リスト

LOM はあくまでもコンテンツメタデータを記述するためのデータ構造を規定するものであり、実態のデータとして格納する情報についても標準的な規定が必要となる。LOM の場合は、アプリケーションプロファイルと呼ばれるディクショナリを整備することとされており、それぞれの属性で使用される値や語彙などを定義することが可能となっている。

日本国内で教員が教材コンテンツを検索する場合、教科や学年、キーワード等での検索のほかに、学習指導要領に基づいた検索が行われることが想定される。しかし、学習指導要領にそのまま ID を付与するだけ

では粒度が粗すぎることから、適切な教材コンテンツを検索することが難しいという課題がある。

そこで、一般社団法人日本教育情報化振興会（JAPET&CEC）では、「学習要素リスト」と名付けられた、教材コンテンツに付与するためのメタデータについての検討を行っている。表 3-2 に、中学校の理科において検討されている学習要素リストを示す。

表 3-2 学習要素リストの一例

学習指導要領				学習要素リスト				
分野	階層0	階層1	階層2	階層0	階層1	階層2	階層3	学習要素ID
1	2身の回りの物質	イ水溶液	(ア) 物質の溶解 物質が水に溶ける様子の観察を行い、水溶液の中では溶質が均質に分散していることを見いだすこと。	身の回りの物質	水溶液	物質の溶解	物質の溶け方	s12070001
			水溶液				s12070002	
			溶液の濃度				s12070003	
			(イ) 溶解度と再結晶 水溶液から溶質を取り出す実験を行い。その結果を溶解度と関連付けてとらえること。			溶解度と再結晶	溶解度と溶解度曲線	s12070004
			(内容の取扱い) 溶解度曲線についても触れること。				再結晶	s12070005

この学習要素リストは、中学校理科の学習指導要領を要素ごとに分解し、大手教材コンテンツ事業者の教材を参考に各事業者で協議して学習要素 ID を付与したものである。これにより、教科書および教材を提供する企業が共通のコードを持つことができることを想定し、検討が進められている。

なお、文部科学省においても、学習指導要領の構造や内容を一定のコードによってわかりやすく整理し、関係者の判断で幅広く活用できるようにしていくに当たっての基本的な方針や留意点の整理、方針に基づくコード試案の作成と公表を行うことを目的とし、平成 29 年 2 月より「学習指導要領における各項目の分類・整理や関連付け等に資する取組の推進に関する有識者会議」が設置されている。有識者会議では、国内外の事例を踏まえた現状と課題の整理、コード試案の作成方針と留意点の整理、今後の活用と試案の改善に向けた体制とスケジュールの動向などが議論されており、今後、有識者会議の検討結果を踏まえて標準となるデータ項目の整理が行われていくことが想定される。

実証内容 平成 28 年度「最先端情報通信技術を活用した教育クラウドプラットフォームに関する実証」
実施報告書
➤ 4.6 コンテンツメタデータ



アクセシビリティガイドブック

平成 29 年 7 月 31 日
エヌ・ティ・ティ・コミュニケーションズ株式会社

Transform your business, transcend expectations with our technologically advanced solutions.

目次

1. アクセシビリティガイドブックの概要	4
1.1 ガイドブックの目的	4
1.2 ガイドブックの構成	4
2. アクセシビリティとして必要な要素	6
2.1 見やすいコンテンツを心がける	6
2.1.1 色の違いだけで情報を提供しない。	6
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。	7
2.1.3 テキストは 200%までサイズ変更できるようにする。	8
2.1.4 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。	8
2.1.5 情報を伝達するためには文字画像ではなく、テキストを用いる。	8
2.1.6 見出しやラベルは、主題または目的を説明している。	9
2.1.7 教材の中でのナビゲーションの方法を一貫させる。	9
2.1.8 ユーザーが目的とするコンテンツを見つけるための複数の手段を用意する。	9
2.1.9 教材の中で同じ機能の表現方法に一貫性を持たせ、識別できるようにする。	9
2.1.10 教材に用いられている言語が、スクリーンリーダーやビジュアルブラウザ等のプログラムにより正しく識別できるようにする。	10
2.1.11 複数の言語が用いられている教材において、それぞれの言語が、スクリーンリーダーやビジュアルブラウザ等のプログラムにより正しく識別できるようにする。	10
2.2 代替テキストを提供する	11
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。	11
2.3 音声や映像コンテンツを注意して用いる	12
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。また、リアルタイムの音声コンテンツについてもキャプションを提供する。	12
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。	13
2.3.3 教材において提示される同期しているすべての映像コンテンツに対して、音声解説 を提供する。	14
2.3.4 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。	14
2.3.5 効果音の使用にも留意する。	14
2.3.6 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。	15
2.3.7 コンテンツが自動的に動作又は終了する場合は、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。	15
2.3.8 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。	16
2.4 構造化に留意する	17
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。	17
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。	17
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。	18
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。	18
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。	19
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。	19
2.4.7 コンテンツの順序により意味が変わる場合（たとえばテーブルを使用してレイアウ トを調整する場合等）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。	20
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。	20
2.5 多様な方法でのアクセスを確保する	21

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にする。	21
2.5.2 キーボード操作を行っている場合、画面上の複数の要素のうち、どの要素がキーボ ードフォーカスを持っているかをユーザーが容易に認識できるようにする。	22
2.5.3 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。	22
2.5.4 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だけで 、ユーザーが予期しない動作を起こさない。	23
2.5.5 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。	23
2.5.6 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。	24
2.5.7 入力エラーを自動的に検出し、修正方法が提案できる場合、ユーザーに修正方法を 提示する。	25
2.5.8 操作のミスが大きな影響を及ぼす場合には、取り消しや確認等の手段を提供する。	25
2.5.9 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	26
2.6 その他の留意事項	28
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。	28
2.6.2 操作方法に一貫性を持たせる。	28
付録. チェックリスト【例】	29

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

「教育クラウドプラットフォーム参考技術仕様」（以下「参考技術仕様」という。）は、教育クラウドプラットフォームを実装する際の一例として、クラウド環境で実装された複数の教材コンテンツをシングルサインオンで利用することができ、異なるプラットフォームとの間でも、相互にデータ連携を行うことができる教育クラウドプラットフォームに求められる技術要件について取りまとめている。

本ガイドブックは、参考技術仕様に基づき、教育クラウドプラットフォームを新たに提供する事業者、システム更改をする事業者、教材コンテンツを提供する事業者に対し、教育クラウドプラットフォームのポータルや教材コンテンツのアクセシビリティを確保することで、障害等により様々な困難があり特別な支援が必要な児童・生徒の利活用を支援することを目的としている。

また、平成 28 年 4 月 1 日に施行された「障害を理由とする差別の解消の推進に関する法律」で求められる合理的な配慮を踏まえるものとしている。

総務省が平成 26 年度から平成 28 年度まで実施した「先導的教育システム実証事業」で作成した参考技術仕様及び各ガイドブックと教育クラウドプラットフォームの提供に向けた工程との関係については、下図 1-1 で示すとおりであり、本ガイドブックは、教育クラウドプラットフォーム上でのポータルや教材コンテンツ制作の範囲で、要件定義から実装に係るプロセスで事業者が参照するべきものとして取りまとめられている。

なお、実証を通じてアクセシビリティを考慮した教材作成に関する検討を実施した。検討内容については実証実施報告書の 4.3 教材コンテンツに記載している。

	要求定義	要件定義	設計	実装
全体構成/ 相互運用性	参考技術仕様			
セキュリティ	セキュリティ要件 ガイドブック			
クラウド環境 (PaaS/IaaS)			クラウド環境構築 ガイドブック	
教材コンテンツ			コンテンツ作成 ガイドブック	
		アクセシビリティ ガイドブック		

図 1-1 参考技術仕様・各ガイドブックと教育クラウドプラットフォーム開発工程との関係

1.2 ガイドブックの構成

本アクセシビリティガイドブックは、先行して実施された総務省「教育分野における最先端 ICT 利活用に関する調査研究（平成 25 年度）」において作成された「アクセシビリティに関するガイドライン」を踏まえ、Web サービスにおけるアクセシビリティに関する国際規格である「Web Contents Accessibility Guideline 2.0」の一致規格である「JISX 8341-3 : 2016」を参照し、3 ヶ年の調査・実証を踏まえ追記を

行っている。

なお「JISX 8341-3 : 2016」については、国及び地方公共団体等の公的機関のホームページ等のアクセシビリティの指針を示している「みんなの公共サイト運用ガイドライン（総務省）」での参照規格となっており、適合レベル AA への準拠が求められており、本ガイドブックもこれに準拠したものとなっている。

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

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、色の違いがわからなくても理解できるようにする。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

1.4.1 色の使用の達成基準：色が、情報を伝える、動作を示す、反応を促す、又は視覚的な要素を判別するための唯一の視覚的手段になっていない（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

Example: Using color to convey meaning

Color only

Required fields are in red

Name

Email

Color and symbol

Required fields are in red and marked with an *

Name

Email *

色のみではなく数字を用いた例

Example: Refer to something using color alone

Color only

Which is the right-angled triangle?
 Green
 Blue
 Red
 Yellow
 Don't know

Color and number

Which is the right-angled triangle?
 Green (1)
 Blue (2)
 Red (3)
 Yellow (4)
 Don't know

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。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

1.4.3 コントラスト (最低限レベル) の達成基準 : テキスト及び文字画像の視覚的提示には、少なくとも 4.5:1 のコントラスト比がある。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文字画像には、少なくとも 3:1 のコントラスト比がある。
- 附随的: テキスト又は文字画像において、次の場合はコントラストの要件はない。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、純粋な装飾である、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、最低限の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

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.



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.

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 テキストは 200% までサイズ変更できるようにする。

- キャプション及び文字画像以外のテキストは、支援技術を用いなくても 200% までサイズ変更できるようにする。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

1.4.4 テキストのサイズ変更の達成基準： キャプション及び文字画像を除き、テキストは、コンテンツ又は機能を損なうことなく、支援技術なしで 200% までサイズ変更できる。(レベル AA)

テキストのサイズ変更：達成基準 1.4.4 を理解する | WCAG 2.0 解説書

<http://waic.jp/docs/UNDERSTANDING-WCAG20/visual-audio-contrast-scale.html>

2.1.4 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。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

1.3.3 感覚的な特徴の達成基準： コンテンツを理解し操作するための説明は、形、大きさ、視覚的な位置、方向、又は音のような、構成要素がもつ感覚的な特徴だけに依存していない(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>

2.1.5 情報を伝達するためには文字画像ではなく、テキストを用いる。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

1.4.5 文字画像の達成基準： 使用している技術で意図した視覚的提示が可能である場合、文字画像ではなくテキストが情報伝達に用いられている。ただし、次に挙げる場合を除く：(レベル AA)

- a) カスタマイズ可能：文字画像は、利用者の要求に応じた視覚的なカスタマイズができる。
- b) 必要不可欠：テキストの特定の表現が、伝えようとする情報にとって必要不可欠である。

文字画像：達成基準 1.4.5 を理解する | WCAG 2.0 解説書

<http://waic.jp/docs/UNDERSTANDING-WCAG20/visual-audio-contrast-text-presentation.html>

2.1.6見出しやラベルは、主題または目的を説明している。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

2.4.6 見出し及びラベルの達成基準： 見出し及びラベルは、主題又は目的を説明している。(レベル AA)

見出し及びラベル: 達成基準 2.4.6 を理解する | WCAG 2.0 解説書

<http://waic.jp/docs/UNDERSTANDING-WCAG20/navigation-mechanisms-descriptive.html>

2.1.7教材の中でのナビゲーションの方法を一貫させる。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

3.2.3 一貫したナビゲーションの達成基準： ウェブページ一式の中にある複数のウェブページ上で繰り返されているナビゲーションのメカニズムは、繰り返されるたびに 相対的に同じ順序で出現する。ただし、利用者が変更した場合は除く。(レベル AA)

一貫したナビゲーション: 達成基準 3.2.3 を理解する | WCAG 2.0 解説書

<http://waic.jp/docs/UNDERSTANDING-WCAG20/consistent-behavior-consistent-locations.html>

2.1.8ユーザーが目的とするコンテンツを見つけるための複数の手段を用意する。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

2.4.5 複数の手段の達成基準： ウェブページ一式の中で、あるウェブページを見つける複数の手段が利用できる。ただし、ウェブページが一連のプロセスの中の 1 ステップ又は結果である場合は除く。(レベル AA)

複数の手段: 達成基準 2.4.5 を理解する | WCAG 2.0 解説書

<http://waic.jp/docs/UNDERSTANDING-WCAG20/navigation-mechanisms-mult-loc.html>

2.1.9教材の中で同じ機能の表現方法に一貫性を持たせ、識別できるようにする。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

3.2.4 一貫した識別性の達成基準： ウェブページ一式の中で同じ機能を有するコンポーネントは、一貫して識別できる。(レベル AA)

一貫した識別性: 達成基準 3.2.4 を理解する | WCAG 2.0 解説書

<http://waic.jp/docs/UNDERSTANDING-WCAG20/consistent-behavior-consistent-functionality.html>

2.1.10 教材に用いられている言語が、スクリーンリーダーやビジュアルブラウザ等のプログラムにより正しく識別できるようにする。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

3.1.1 ページの言語の達成基準: それぞれのウェブページのデフォルトの自然言語がどの言語であるか、プログラムによる解釈が可能である。(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>

2.1.11 複数の言語が用いられている教材において、それぞれの言語が、スクリーンリーダーやビジュアルブラウザ等のプログラムにより正しく識別できるようにする。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

3.1.2 一部の言語の達成基準: コンテンツの一節、又は語句それぞれの自然言語がどの言語であるか、プログラムによる解釈が可能である。ただし、固有名詞、技術用語、言語が不明な語句、及びすぐ前後にあるテキストの言語の一部になっている単語又は語句は除く。(レベル AA)

一部の言語: 達成基準 3.1.2 を理解する | WCAG 2.0 解説書

<http://waic.jp/docs/UNDERSTANDING-WCAG20/meaning-other-lang-id.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。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

1.1.1 非テキストコンテンツの達成基準：利用者に提示される全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提供されている。ただし、次の場合は除く（レベル A）。

- a) コントロール及び入力：非テキストコンテンツが、コントロール又は利用者の入力を受け付けるものであるとき、その目的を説明する名前（name）を提供している（コントロール及び利用者の入力を受け付けるコンテンツに関するその他の要件は、4.1 参照。）。
- b) 時間依存メディア：非テキストコンテンツが、時間に依存したメディアであるとき、代替テキストは、少なくとも、その非テキストコンテンツを識別できる説明を提供している（メディアに関するその他の要件は、1.2 参照。）。
- c) テスト：非テキストコンテンツが、テキストで提示されると無効になるテスト又は演習のとき、代替テキストは、少なくともその非テキストコンテンツを識別できる説明を提供している。
- d) 感覚的：非テキストコンテンツが、特定の感覚的体験を創り出すことを主に意図しているとき、代替テキストは、少なくともその非テキストコンテンツを識別できる説明を提供している。
- e) CAPTCHA：非テキストコンテンツが、コンピュータではなく人間がコンテンツにアクセスしていることを確認する目的で用いられているとき、代替テキストは、その非テキストコンテンツの

目的を特定し、説明して、かつ、他の感覚による知覚に対応して出力する CAPTCHA の代替形式を提供することで、様々な障害に対応している。

- f) 装飾、整形及び非表示: 非テキストコンテンツが、純粋な装飾である場合、見た目の整形のためだけに用いられている場合、又は利用者に提供されるものではない場合、その非テキストコンテンツは、支援技術によって無視されるように実装されている。

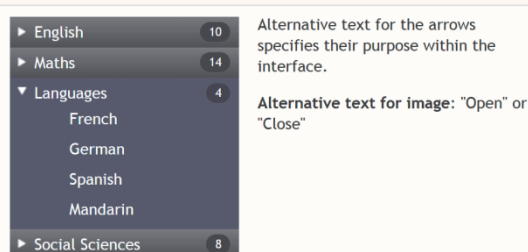
非テキストコンテンツ: 達成基準 1.1.1 を理解する | WCAG 2.0 解説書

<http://waic.jp/docs/UNDERSTANDING-WCAG20/text-equiv-all.html>

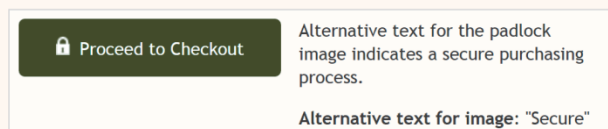
テキスト（数字）で下の階層があることを示した例

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

Example: Alternative text indicates functional purpose



Example: Alternative text conveys meaning



Alternative text is usually not visible; it is included in this example just so you can see what it is.

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。また、リアルタイムの音声コンテンツについてもキャプションを提供する。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

1.2.2 キャプション（収録済み）の達成基準: 同期したメディアに含まれている全ての収録済みの音声コンテンツに対して、キャプションが提供されている。ただし、その同期したメディアがメディアによるテキストの代替であって、メディアによる代替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/media-equiv-captions.html>

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

1.2.4 キャプション (ライブ)の達成基準：同期したメディアに含まれているすべてのライブの音声コンテンツに対してキャプションが提供されている。(レベル AA)

ライブのキャプション：達成基準 1.2.4 を理解する | WCAG 2.0 解説書

<http://waic.jp/docs/UNDERSTANDING-WCAG20/media-equiv-real-time-captions.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。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

1.2.1 音声だけ及び映像だけ (収録済み) の達成基準：収録済みの音声しか含まないメディア及び収録済み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メディアによるテキストの代替であって、メディアによる代替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)。

収録済みの映像しか含まない場合：時間依存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、収録済みの映像しか含まないコンテンツと同等の情報を提供している。

収録済みの音声しか含まないメディア及び収録済み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>

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

1.2.3 音声解説又はメディアに対する代替コンテンツ (収録済み) の達成基準：同期したメディアに含まれている収録済みの映像コンテンツに対して、時間依存メディアに対する代替又は音声解説が提供されている。ただし、その同期したメディアがメディアによるテキストの代替コンテンツであって、メディアによる代替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)。

収録済み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教材において提示される同期しているすべての映像コンテンツに対して、音声解説を提供する。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

1.2.5 音声解説 (収録済) の達成基準: 同期したメディアに含まれているすべての収録済の映像コンテンツに対して、音声解説が提供されている。(レベル AA)

収録済の音声コンテンツのキャプション: 達成基準 1.2.5 を理解する | WCAG 2.0 解説書
<http://waic.jp/docs/UNDERSTANDING-WCAG20/media-equiv-audio-desc-only.html>

2.3.4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。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

1.2.1 音声だけ及び映像だけ (収録済み) の達成基準: 収録済みの音声しか含まないメディア及び収録済み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メディアによるテキストの代替であって、メディアによる代替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)。

収録済みの音声しか含まない場合: 時間依存メディアに対する代替コンテンツによって、収録済みの音声しか含まないコンテンツと同等の情報を提供している。

収録済みの音声しか含まないメディア及び収録済み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>

2.3.5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。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

1.3.3 感覚的な特徴の達成基準: コンテンツを理解し操作するための説明は、形、大きさ、視覚的な位置、方向、又は音のような、構成要素がもつ感覚的な特徴だけに依存していない (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>

2.3.6 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。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

1.4.2 音声の制御の達成基準: ウェブページ上にある音声は自動的に再生され、3 秒より長く続く場合、その音声を一時停止若しくは停止するメカニズム、又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が利用できる (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>

2.3.7 コンテンツが自動的に動作又は終了する場合は、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。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

2.2.1 タイミング調整可能の達成基準: コンテンツに制限時間を設定する場合は、次に示す事項のうち、少なくとも一つを満たしている (レベル A)。

- 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。
- b) 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。
- c) 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って、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。
- d) 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。

e) 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。

f) 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>

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

2.2.2 一時停止、停止及び非表示の達成基準：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は、次の全ての事項を満たしている（レベル A）

a) 動き、点滅又はスクロール：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、かつ、(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が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。

b) 自動更新：自動更新する情報が、(1) 自動的に開始し、かつ、(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、若しくは非表示にする、又はその更新頻度を調整することが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>

2.3.8 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。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

2.3.1 3 回のせん（閃）光、又はしきい（閾）値以下の達成基準：ウェブページには、どの 1 秒間においても 3 回を超えるせん（閃）光を放つものがない、又はせん（閃）光が一般せん（閃）光しきい（閾）値及び赤色せん（閃）光しきい（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

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

4.1.1 構文解析の達成基準: 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、要素には完全な開始タグ及び終了タグがあり、要素は仕様に従っ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。ただし、仕様で認められているものを除く(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">`)

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

3.1.1 ページの言語の達成基準: それぞれのウェブページのデフォルトの自然言語がどの言語であるか、プログラムによる解釈が可能である(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>）

参考規格 JIS X 8341-3:2016 （WCAG 2.0 の一致規格）

2.4.2 ページタイトルの達成基準： 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>

- ✓ 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/>

参考規格 JIS X 8341-3:2016 （WCAG 2.0 の一致規格）

2.4.1 ブロックスキップの達成基準： 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するメカニズムが利用できる（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。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

1.3.1 情報及び関係性の達成基準: 何らかの形で提示されている情報、構造、及び関係性は、プログラムによる解釈が可能である、又は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)。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

2.4.4 リンクの目的 (コンテキスト内) の達成基準: それぞれのリンクの目的が、リンクのテキスト単独で判断できるか、又はリンクのテキストとプログラムによる解釈が可能なリンクのコンテキストとから判断できる。ただし、リンクの目的がほとんどの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コンテンツの順序により意味が変わる場合（たとえばテーブルを使用してレイアウトを調整する場合等）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。

参考規格 JIS X 8341-3:2016 （WCAG 2.0 の一致規格）

1.3.2 意味のある順序の達成基準: コンテンツが提示されている順序が意味に影響を及ぼす場合には、正しく読む順序はプログラムによる解釈が可能である（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。

参考規格 JIS X 8341-3:2016 （WCAG 2.0 の一致規格）

1.3.2 意味のある順序の達成基準: コンテンツが提示されている順序が意味に影響を及ぼす場合には、正しく読む順序はプログラムによる解釈が可能である（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当たるようにする

- 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>

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

2.1.1 キーボードの達成基準: コンテンツの全ての機能は、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>

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

2.1.2 キーボードトラップなしの達成基準: 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、修飾キーを伴わない矢印キー、Tab キー、又はフォーカスを外すその他の標準的な方法でフォーカスを外せない場合は、フォーカスを外す方法が利用者に通知される（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 キーボード操作を行っている場合、画面上の複数の要素のうち、どの要素がキーボードフォーカスを持っているかをユーザーが容易に認識できるようにする。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

2.4.7 フォーカスの可視化の達成基準: キーボード操作が可能なあらゆるユーザインタフェースには、フォーカスインジケータが見える操作モードがある。（レベル AA）

フォーカスの可視化: 達成基準 2.4.7 を理解する | WCAG 2.0 解説書

<http://waic.jp/docs/UNDERSTANDING-WCAG20/navigation-mechanisms-focus-visible.html>

2.5.3 キーボードの Tab キーによるフォーカス移動順序は、ユーザーが予想できるように、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。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

2.4.3 フォーカス順序の達成基準: ウェブページが順を追ってナビゲートできて、そのナビゲーション順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、意味及び操作性を損なわない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>

2.5.4 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。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

3.2.1 フォーカス時の達成基準: 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コンテキスト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>

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

3.2.2 入力時の達成基準: 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が、コンテキストの変化を自動的に引き起こさない。ただし、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く (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>

2.5.5 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と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>

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

1.3.1 情報及び関係性の達成基準: 何らかの形で提示されている情報, 構造, 及び関係性は, プログラムによる解釈が可能である, 又は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>

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

3.3.2 ラベル又は説明の達成基準: コンテンツが利用者の入力を要求する場合は, ラベル又は説明文が提供されている (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>

2.5.6 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。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

3.3.1 エラーの特定の達成基準: 入力エラーが自動的に検出された場合は, エラーとなっている箇所が特定され, そのエラーが利用者にテキストで説明される (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


Example: Using error list, icon, and background color to make errors stand out

Please correct the following errors:


1.  [Email address is invalid](#)
2.  [A Comment is required](#)

Add a comment
Required fields are in red and marked with an *

Name

 E-mail *

Website

 Comment *

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>

2.5.7 入力エラーを自動的に検出し、修正方法が提案できる場合、ユーザーに修正方法を提示する。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

3.3.3 エラー修正の提案の達成基準: 入力エラーが自動的に検出され、修正方法を提案できる場合、その提案が利用者に提示される。ただし、セキュリティ又はコンテンツの目的を損なう場合は除く。
(レベル AA)

エラー修正の提案: 達成基準 3.3.3 を理解する | WCAG 2.0 解説書

<http://waic.jp/docs/UNDERSTANDING-WCAG20/minimize-error-suggestions.html>

2.5.8 操作のミスが大きな影響を及ぼす場合には、取り消しや確認等の手段を提供する。

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

3.3.4 エラー回避の達成基準: 利用者にとって法律行為もしくは金融取引が生じる、利用者が制御可能なデータストレージシステム上のデータを変更もしくは削除する、又は利用者が試験の解答を送信するウェブページでは、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 AA)。

- a) 取消: 送信を取り消すことができる。
- b) チェック: 利用者が入力したデータの入力エラーがチェックされ、利用者には修正する機会が提供される。
- c) 確認: 送信を完了する前に、利用者が情報の見直し、確認及び修正をするメカニズムが利用できる。

エラー回避: 達成基準 3.3.4 を理解する | WCAG 2.0 解説書

<http://waic.jp/docs/UNDERSTANDING-WCAG20/minimize-error-reversible.html>

2.5.9 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/>
- 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/>
- Using WAI-ARIA in HTML
<http://www.w3.org/TR/aria-in-html/>
- 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>
- OpenAjax Examples by ARIA Roles| OpenAjax Alliance Accessibility Task Force
<http://oaa-accessibility.org/examples/roles/>
- 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>
- OpenAjax Examples by ARIA States| OpenAjax Alliance Accessibility Task Force
<http://oaa-accessibility.org/examples/states/>
- OpenAjax Examples by ARIA Properties| OpenAjaxAlliance Accessibility Task Force
<http://oaa-accessibility.org/examples/props/>

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

2.1.1 キーボードの達成基準: コンテンツの全ての機能は、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>

参考規格 JIS X 8341-3:2016 (WCAG 2.0 の一致規格)

4.1.2 名前 (name) , 役割 (role) 及び値 (value) の達成基準: 全てのユーザインタフェース コンポーネント (フォームを構成する要素, リンク, スクリプトが生成するコンポーネントなど) では, 名前 (name) 及び役割 (role) は, プログラムによる解釈が可能である。

また, 状態, プロパティ及び利用者が設定可能な値はプログラムによる設定が可能である。そして, 支援技術を含むユーザエージェントが, これらの項目に対する変更通知を利用できる (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.html#16>

2.6 その他の留意事項

2.6.1 ユーザーの集中力、注意かに配慮し、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）

参考規格 JIS X 8341-3:2016（WCAG 2.0 の一致規格）

1.3 適応可能なガイドライン：情報、及び構造を損なうことなく、様々な方法（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。

参照 「JIS X 8341-3:2016 高齢者・障害者等配慮設計指針—情報通信における機器、ソフトウェア及びサービス—第 3 部：ウェブコンテンツ」（平成 28 年 4 月）

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	6			
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	7			
2-1.3	テキストは 200%までサイズ変更できるようにしている。	8			
2-1.4.	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	8			
2-1.5	情報を伝達するためには文字画像ではなく、テキストを用いている	8			
2-1.6	見出しやラベルは、主題または目的を説明している	9			
2-1.7	教材の中でのナビゲーションの方法を一貫させている	9			
2-1.8	ユーザーが目的とするコンテンツを見つけるための複数の手段を用意している	9			
2-1.9	教材の中で同じ機能の表現方法に一貫性を持たせ、識別できるようにしている	9			
2-1.10	教材に用いられている言語がスクリーンリーダーやビジュアルブラウザ等のプログラムにより正しく識別できるようにしている	10			
2-1.11	複数の言語が用いられている教材において、それぞれの言語が、スクリーンリーダーやビジュアルブラウザ等のプログラムにより正しく識別できるようにしている	10			
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	11			
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	12			

番号	チェック項目	頁	評価	対応要否	対応状況等
	している				
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	13			
2-3.3.	教材において提示される同期しているすべての映像コンテンツに対して、音声解説を提供している	14			
2-3.4.	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	14			
2-3.5.	効果音の使用にも留意している	14			
2-3.6.	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	15			
2-3.7.	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	15			
2-3.8	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	16			
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	17			
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	17			
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	18			
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	18			
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	19			
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	19			
2-4.7.	コンテンツの順序により意味が変わる場合（たとえばテーブルを使用してレイアウトを調整する場合等）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	19			

番号	チェック項目	頁	評価	対応要否	対応状況等
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	20			
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にしている	21			
2-5.2.	キーボード操作を行っている場合、画面内の複数の要素のうち、どの要素がキーボードフォーカスを持っているかをユーザーが容易に認識できるようにしている	22			
2-5.3.	キーボードの Tab キーによるフォーカス移動順序は、ユーザーが予想できるように、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している	22			
2-5.4.	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、ユーザーが予想しない動作を起こしていない	23			
2-5.5.	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	23			
2-5.6.	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	24			
2-5.7.	入力エラーを自動的に検出し、修正方法が提案できる場合、ユーザーに修正方法を提示している	25			
2-5.8.	操作のミスが大きな影響を及ぼす場合には、取り消しや確認等の手段を提供している	25			
2-5.9.	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	26			
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	28			
2-6.2.	操作方法に一貫性を持たせている	28			