参考資料 3-3

平成 26 年度クラウド等の最先端情報通信技術を活用した学習・教育システムに関する実証別冊

セキュリティ要件ガイドブック（案）

2015 年 3 月

目 次

はじめに

本書は、平成 26 年度「クラウド等の最先端情報通信技術を活用した学習・教育システムに関する実証」において、技術仕様検討の一環として作成した、事業者（プラットフォーム事業者）向けの「セキュリティ要件ガイドブック」である。

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

「セキュリティ要件ガイドブック」（以下、「ガイドブック」）は、平成 26 年度「クラウド等の最先端情報通信技術を活用した学習・教育システムに関する実証」において検討を行った学習・教育クラウド・プラットフォームについて、事業者が満たすべきセキュリティ要件を示すことを目的とする。

1.2 学習・教育クラウド・プラットフォームの概要

学習・教育クラウド・プラットフォームの概要を図 1-1 に示す。

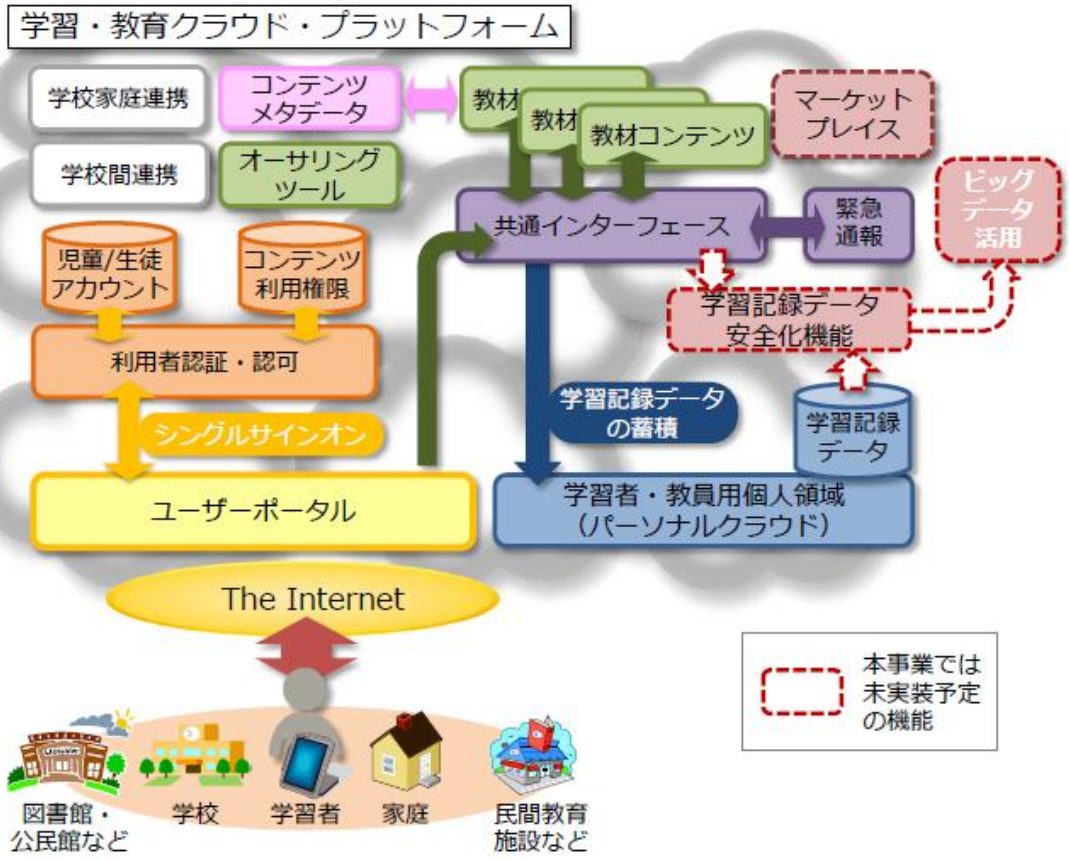

図 1-1 学習・教育クラウド・プラットフォームの概要

1.3 ガイドブックの適用範囲および前提条件

学習・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。

本ガイドブックでは、そうしたプラットフォームを提供する事業者に求められる情報セキ

ュリティの考え方や求められる要件を示す。

情報セキュリティの項目については、ISO/IEC 27001:2013 附属書 A の管理策（14 分野）の構成に沿って整理した。

2. 学習・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

2.1 情報セキュリティのための方針群

(1) 基本的な考え方

本項では、情報セキュリティのための方針群を採り上げる。ここでは、主に事業者が学習・教育クラウド・プラットフォームを運用するポリシーが対象となる。保護すべきデータとしては、利用者の個人情報や学習記録データが挙げられる。また、当該ポリシーで扱う要件として、データの機密性（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データにアクセス可能）が挙げられる。

(2) 求められている要件

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、利用者の安全性（機密性、完全性、可用性）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	学習・教育クラウド・プラットフォームの運用ポリシーでは、利用者の個人情報及び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を実現する方針を策定することが望まれる。

2.2 情報セキュリティのための組織

(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、事業者が学習・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。

また、一般的には、組織における就業に関わる事項として、モバイル機器の利用及びテレワーキングを対象とする。これを学習・教育クラウド・プラットフォームにおける教員・学習者等のモバイル機器の利用及び校外学習に置き換えて検討する。

(2) 求められている要件

内部組織	
要件	学習・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	学習・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。

モバイル機器の利用及び校外学習	
要件	学習・教育クラウド・プラットフォームにおいて、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	学習・教育クラウド・プラットフォームにおいてモバイル機器を利用すること及び校外学習で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、校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。

2.3　人的資源のセキュリティ

(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。学習・教育クラウド・プラットフォームにおいては、これを運用する従業員及び契約相手を対象として検討する。

(2) 求められている要件

人的資源のセキュリティ	
要件	学習・教育クラウド・プラットフォームを運用する従業員及び契約相手に対して、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	従業員及び契約相手には、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。

2.4　資産の管理

(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、情報（教材コンテンツ、利用者の個人情報及び学習記録データ）及び学習・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。また、利用者には、教員・ICT 支援員、児童・生徒が該当する。また、学習・教育クラウド・プラットフォームでは必ずしも媒体の利用を想定していないが、教材や利用者側の事情で媒体が利用される可能性を考慮し、要件に含める。

(2) 求められている要件

資産に対する責任	
要件	情報及び学習・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。全ての従業員及び利用者（教員・ICT 支援員、児童・生徒）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	学習・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、それを前提とした資産管理が求められる。また、教材コンテンツの利用の許容範囲にも留意する必要がある。

情報分類	
要件	学習・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	学習・教育クラウド・プラットフォームで扱う情報のうち、教材コンテンツは著作権の保護、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。

媒体の取扱い	
要件	学習・教育クラウド・プラットフォームで扱う情報が媒体に保存された場合、認可されていない開示、変更、除去又は破壊を防止すること。
考え方	媒体を利用する場合、媒体の管理や処分、輸送について、セキュリティに配慮した手順を定める必要がある。特に、教材の複製に係る著作権違反の防止、媒体の処分に際しては物理的な破壊やデータ消去ツールの適用が求められる。

2.5 アクセス制御

(1) 基本的な考え方

本項では、情報の機密性、完全性及び可用性を維持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、利用者アクセスの管理、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。

(2) 求められている要件

アクセス制御に対する業務上の要求事項	
要件	情報及び学習・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	情報（教材コンテンツ、利用者の個人情報及び学習記録データ）へのアクセス

	制御方針については、教材コンテンツの利用権や個人情報保護を考慮する必要がある。

利用者アクセスの管理	
要件	利用者の登録及び登録削除についての正式なプロセスを実施すること。全ての種類の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。特権的アクセス権の割当て及び利用を制限すること。利用者に対する秘密認証情報の割当てを正式な管理プロセスで管理すること。利用者のアクセス権を定期的にレビューすること。従業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	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。特に、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。

利用者の責任	
要件	学習・教育クラウド・プラットフォームの利用者（教員・ICT 支援員、児童・生徒）がパスワードを定められた手順で利用すること。
考え方	学習・教育クラウド・プラットフォームの利用者に、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。

システム及びアプリケーションのアクセス制御	
要件	学習・教育クラウド・プラットフォームを介した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	学習・教育クラウド・プラットフォームを介した情報やアプリケーションへのアクセスを制御する必要がある。

2.6　暗号

(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。学習・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。

(2) 求められている要件

暗号	
要件	情報（個人情報、学習記録データ）を保護するために、暗号を利用すること。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	学習・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。

2.7 物理的及び環境的セキュリティ

(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、学習・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。

(2) 求められている要件

物理的セキュリティ	
要件	学習・教育クラウド・プラットフォームの開発・運用環境(オペレーション)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	学習・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。

2.8 運用のセキュリティ

(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す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。

(2) 求められている要件

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	学習・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。

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、オペレータや利用者（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	学習・教育クラウド・プラットフォームに接続するオペレータや利用者に対し、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。

バックアップ	
要件	学習・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、学習・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。

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。

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	学習・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。

技術的ぜい弱性管理	
要件	学習・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	学習・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、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。

情報システムの監査に対する考慮事項	
要件	学習・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、利用者にかかる迷惑を最小限に抑えるように、準備する必要がある。

2.9　通信のセキュリティ

(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。

(2) 求められている要件

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	学習・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。

情報の転送	
要件	転送する情報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	情報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。

2.10　システムの取得、開発及び保守

(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。

(2) 求められている要件

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	学習・教育クラウド・プラットフォームの開発や改訂に、情報セキュリティを欠くことがないようにする必要がある。

開発及びサポートプロセスにおけるセキュリティ	
要件	学習・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	学習・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。

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	学習・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、児童・生徒の個人情報や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。

2.11　供給者関係

(1) 基本的な考え方

本項では、業務やシステム等の委託先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、供給者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。供給者は、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、システムの開発者が挙げられており、クラウド事業者も含まれる。

(2) 求められている要件

供給者関係における情報セキュリティ	
要件	供給者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	学習・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に対し情報セキュリティ対策を求める必要がある。

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	学習・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することがないよう確認することが挙げられる。

2.12　情報セキュリティインシデント管理

(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。

(2) 求められている要件

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、学習・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や情報セキュリティインシデントについて把握し、対応する必要がある。

2.13　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

(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。

(2) 求められている要件

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	学習・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。

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	学習・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。

2.14　順守

(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。

(2) 求められている要件

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	学習・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。

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	学習・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。