校務支援システムのクラウド化における
クラウド基盤要件書
Ver1.0

2025 年 10 月 3 日

（一財）全国地域情報化推進協会
教育・校務ワーキンググループ

作成・改訂履歴

０．９版2025 年 3 月 4 日

１・０版2025 年 10 月 3 日

目次

1. 本書の定義

1.1. 本書の目的

「GIGA スクール構想の下での校務 DX について」（文部科学省 R5.3.8）で示された「次世代の校務 DX の方向性」を実現するために必須、有用なクラウド基盤要件を可視化し、「クラウド化」という概念の形骸化を防止することを目的とする。
本書を参照した校務支援システムベンダーやパブリッククラウド事業者の宣言により、学校設置者が校務 DX の実現に向けたクラウド基盤の対応状況を容易に確認できることになる。

1.2. 本書の活用方法

本書は「次世代の校務 DX の方向性」を実現するために必須、有用なサービスを具備、実装している事を宣言するための要件書である。

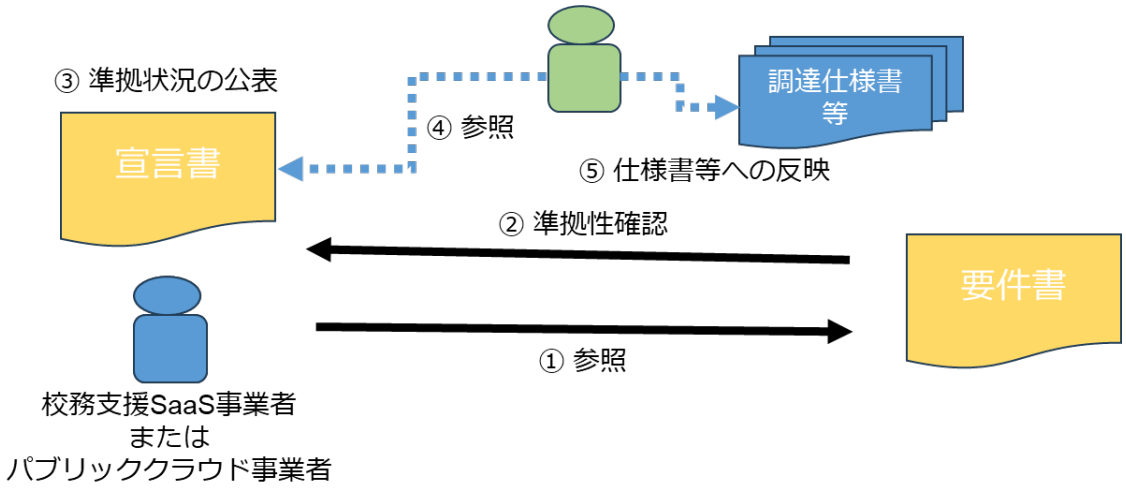


図 1.本書の活用方法

要件書を参照し、宣言書を発行する主体は校務支援 SaaS 提供事業者、またはパブリッククラウド事業者となり、宣言書は調達者が仕様書を策定するにあたって利用されるものとする。
【本書の活用方法まとめ】
① 校務支援 SaaS 事業者またはパブリッククラウド事業者が要件書を参照
② 校務支援 SaaS 事業者またはパブリッククラウド事業者が準拠性を確認後
③ 校務支援 SaaS 事業者またはパブリッククラウド事業者が要件適合宣言書（別紙 1）を用いて準拠性を公表
④ 公表された宣言書を調達者が参照し、調達目的に合致する内容か確認
⑤ 調達者が調達仕様要件への反映や、調達仕様要件の充足確認として利用

1.3. 本書の運用ポリシー

本書のアップデート方針（要検討）

国の動向変化や、本書の利用状況を踏まえた教育委員会へのヒアリング、APPLIC 内校務支援システムベンダーのレビューを経て、年に 1 回程度の改訂審査を実施する。時期は 11 月～12 月に改訂の必要性について協議し、ヒアリングや動向調査に着手する。改訂版は 2 月～3 月を予定する。

1.4. 対応レベル

本書における要件は、「次世代の校務 DX の方向性」を実現するために比較的安易に実装できると考えられる要件（要件①）と、実装がより高度で今後想定される連携等に有効である要件（要件②）の 2 つの階層に分ける。要件①は主にクラウド上にシステムをリフトした時点でクラウド化のメリットを享受できるものとして整理し、要件②は、API 連携やデータ加工処理等、今後想定される連携や開発に有効なものであったり、より高度な可用性やセキュリティを実現できるものとして整理する。

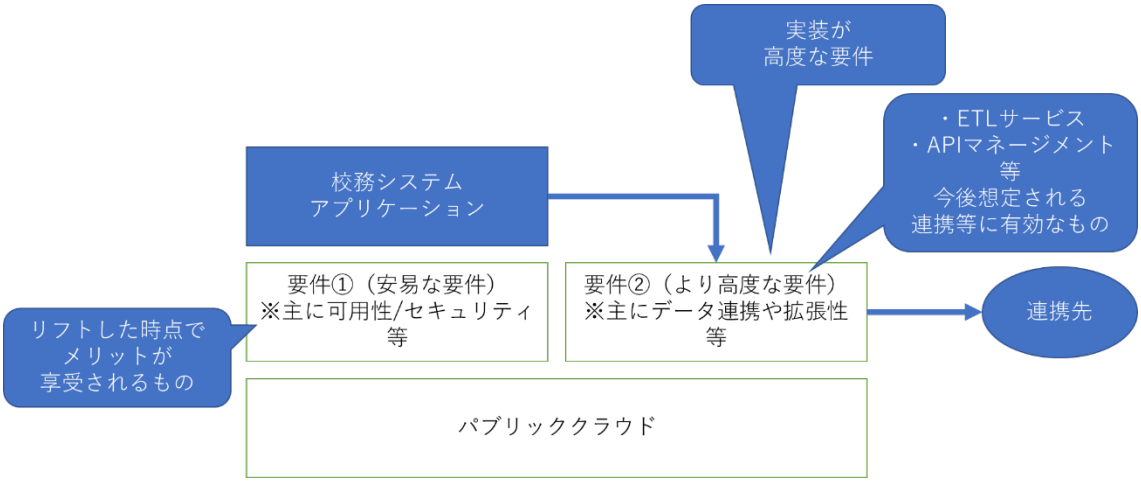


図 2.対応レベル毎の要件

要件①を全て満たす場合は、（可用性やセキュリティ、安定性がある基盤として）校務ＤＸに向けて、クラウド基盤要件を充足しているものとして宣言できるものとする

要件①と②を全て満たす場合は可用性やセキュリティに加えてデータ連携や拡張性を備えたものとして校務ＤＸに向けて、より高度なクラウド基盤要件を充足として宣言できるものとする。

2. 校務システムをクラウド化するにあたって、基盤に求めるべき要件

2.1. 要件一覧

2.1.1. 要件①と規定した目的

＜基本的な契約等＞

①-1. 日本国の法令の範囲内で運用できるサービスであること。また、日本国内の裁判所を合意管轄裁判所とすること。
目的：トラブル、法的な対応を円滑に行うため。

＜レジリエンス向上＞

①-2. 仮想マシンの稼働するハードウェアは冗長化されており、ハードウェア故障時には自動的に、正常なハードウェアから復旧すること。
目的：一般的なクラウド環境の可用性水準を示す事で、要件水準を統一する。

①-3. ネットワーク含めたデータセンターレベルのハードウェアまで完全に冗長化されていること。
目的：一般的なクラウド環境の可用性水準を示す事で、要件水準を統一する。

①-4. クラウドサービス内で冗長性を確保し、主要な機能においては１つのリージョン内で高い SLA（99.9%以上）を提供すること。
目的：一般的なクラウド環境の可用性水準を示す事で、要件水準を統一する。

①-5. 受電方法と非常用発電設備は冗長化されており、非常用電源（自家発電機）を有していること。かつ、データセンター毎に冗長化されており、法定点検や工事等の際にも止まることなく電力供給が可能なこと。
目的：一般的なクラウド環境の可用性水準を示す事で、要件水準を統一する。

①-6. データセンターの被災時には、被災地とは別の地理的に離れたロケーションでシステムをバックアップデータから復旧可能とする機能を提供すること。
目的：災害対策を簡易に実現する。

①-7. クラウド側でサービスとして提供されているインターネット回線は冗長化されていること。
目的：クラウド側でサービスとして提供されるインターネット回線が安定運用されている事を担保する。

①-8. OS を含むデータ全体のバックアップを取得できること。取得したバックアップはいつでも仮想マシンの復元に使用できること。復元時は別のサイズの仮想マシンを選択できること。
目的；バックアップデータから簡易に仮想マシンを復旧し、可用性を高める。

①-9. 全てのマネージドサービスは、可用性が確保されている状態で提供されているか、利用者側で機能を選択をすることで可用性を実現できるように設計されていること。
目的：可用性が担保されたマネージドサービスを提供しているクラウド事業者を選定することで、高可用性を実現する。

①-10. バックアップを保管するストレージは、二重化以上の保護をされた高い耐久性を持たせ、ファイルの永続的な保管ができること。
目的：データ消失のリスクを低減させる。

＜標準的なセキュリティ対策＞

①-11. 選定するクラウド基盤は、ISO27017 を取得していること。
目的：セキュリティの要求水準を底上げする。

①-12. クラウド環境に対する攻撃、または想定しない行動が取られ、セキュリティ上の脅威に晒される可能性が出た場合にこれを検出する機能が提供されること。
目的：ヒューマンエラーの防止や、乗っ取り被害による構成破壊工作を防止する。

①-13. バックアップデータをマシンイメージごと保管するストレージサービスは WORM 機能を有し、バックアップデータをランサムウェアから保護すること。
目的：ランサムウェア対策が簡易に実行できる環境を利用可能とする。

①-14. クラウド環境にアクセス可能なアカウントは、ID/パスワードの他、多要素認証（MFA）や接続元 IP アドレス制限などを利用して強固な認証を行うことができること。
目的：クラウド環境のアカウント保護を実現する。

①-15. アカウント毎に操作権限を付与できること。
目的：クラウド環境のアカウント保護を実現する。

＜標準的な拡張性や運用要件＞

①-16. 新サービスや新機能が定期的にリリースされ続けており、技術革新が頻繁におこなわれているクラウド事業者であること。
目的：技術革新が頻繁に行われているクラウド事業者を選定することで、最新技術への追随性を高め、アプリケーションの陳腐化を防ぐ。

①-17. インターネット回線の帯域制限は無く、利用実態に応じた帯域を利用できること。
目的：クラウド側でサービスとして提供されるインターネット回線が安定運用されている事を担保する。

①-18. 24 時間 365 日の日本語によるサポートを提供すること。
目的：必要なサポートや運用支援水準を定める。

①-19. メンテナンスや障害情報などについて、適切に日本語で通知を行うこと。
目的：必要なサポートや運用支援水準を定める。

①-20. オンプレミス環境からのクラウドリフトを容易に実現するためのサービスなどが提供されていること。
目的：クラウドへのリフト対応を簡易に実現させる。

①-21. 配備された各リソースについて、運用状況を踏まえて容易に増強または縮小させることができること。
目的：柔軟にコンピューティングリソースの増強、また縮小を行い、効率的な運用を行える環境を目指す。

2.1.2.　要件②と規定した目的

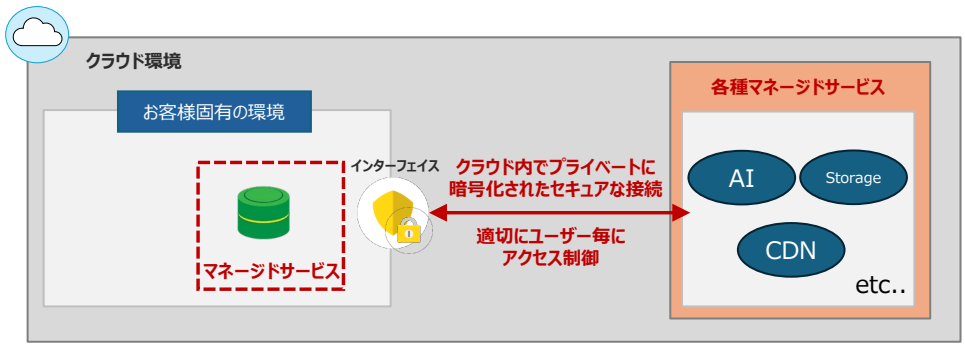
＜より高度なセキュリティ対策＞

②-1.　選定するクラウド基盤は、児童生徒や教職員、保護者などの個人情報等を保護するための認証を取得していること。
【必須】ISMAP 認証
【推奨】ISO27018
目的：セキュリティの要求水準を底上げする。

②-2.　VSS（共通脆弱性評価システム）スコアや、影響範囲の大きさなどを考慮して、世界的なセキュリティインシデント発生時には、迅速に影響を受けるサービス範囲や対応策を通知すること。
目的：セキュリティの要求水準を底上げする。

②-3.　利用できるマネージドサービスや同一クラウド基盤上の他者サービスをプライベートなネットワークからも利用できること。利用にあたってはアクセス制御をかけられること。
目的：提供されているマネージドサービスはプライベートな独立性を担保する必要がある。

要件②-3イメージ

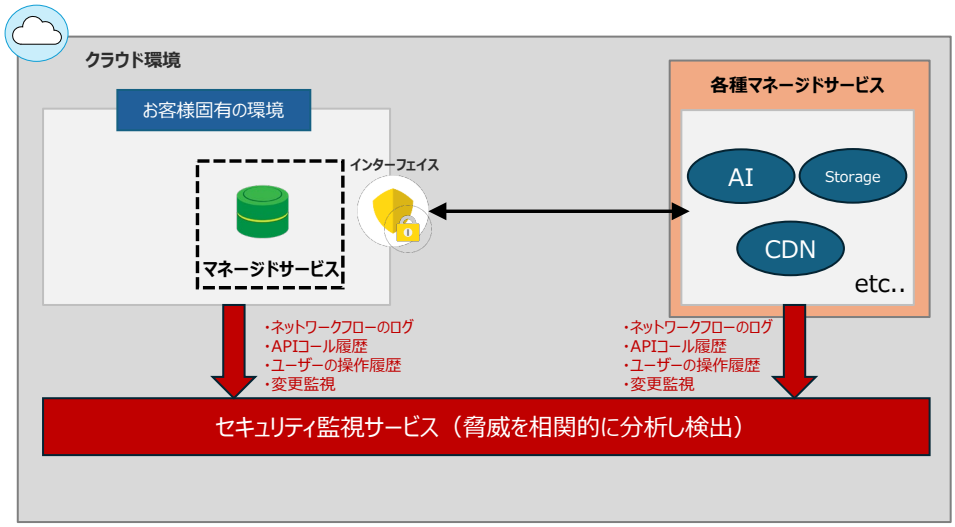


②-4.　構成変更のトラッキングができ、決められたルールに違反した構成変更を制限、またはアラートを挙げる機能を有すること。
目的：ヒューマンエラーや乗っ取りによる構成破壊工作を防止する。

②-5.　環境に配備したリソースに対する脅威検出機能、サービスを利用できること。
目的：セキュリティ強化対策が簡易に実行できる事を担保する

②-6.　脅威検出にあたっては、悪意のある通信、変更監視、不正操作等を継続的にモニタリングが可能であること。
目的：セキュリティ強化対策が簡易に実行できる事を担保する

要件②-5、6イメージ



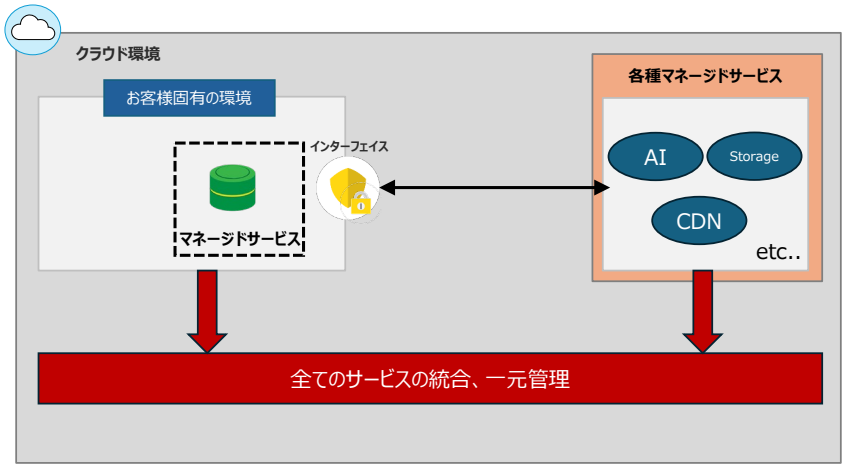
＜より高度な拡張性や将来性＞

②-7.　データベースや運用管理ツール等、従来は利用者側で購入し、導入して利用していたミドルウエアやツール等がマネージドサービスとして利用できること。
目的：マネージドサービスが提供されているクラウド事業者を選定することでシステムの開発ライフサイクルを加速する。

②-8.　提供されている全てのマネージドサービスに関する技術情報及び用例等がインターネット上に複数年間公開されているクラウド事業者を選定すること。
目的：提供されているマネージドサービスの情報が一般的に公開されているクラウド事業者を選定し、導入の敷居を下げ、ロックインを防ぐ。

②-9.　マネージドサービスとして提供される機能の監視、ログ管理はクラウドの管理画面、または管理 API と統合され、一元管理できること。
目的：提供されているマネージドサービスが、セキュアに管理運用できることを担保する。

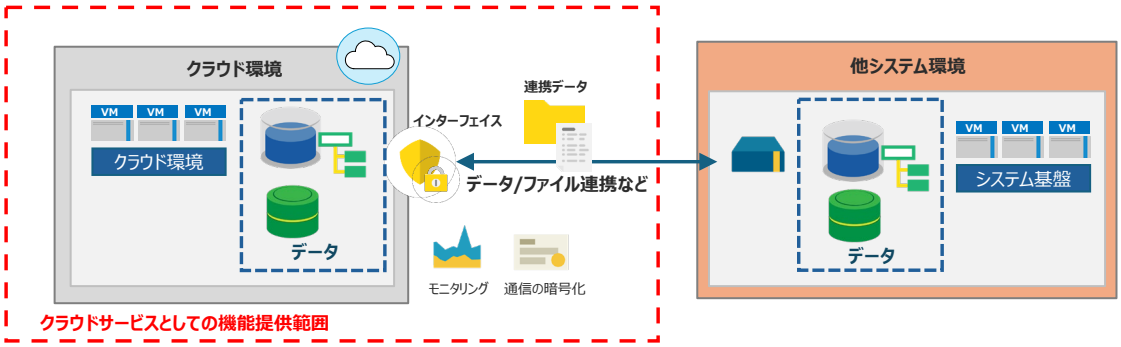
要件②-9イメージ



②-10.　API サービスとして、ルーティング、アクセス制御、ログ管理などの基本機能を提供すること。また、ファイル共有サービスでは、保管時および転送時の暗号化、IP 制限による接続制御、データ単位でのアクセス管理を実装すること。さらに、RESTful API による標準的なインターフェースを提供し、API コールを含むアクセスログの取得・保存およびデータ更新時のイベント通知機能を具備すること。

目的：将来的なデータ連携、システム間連携を想定し、API 連携やファイル連携を簡易に実現し、セキュアに管理運用できることを担保する。

要件②-10イメージ



クラウドの機能として提供されるインターフェイス（マネージドAPI、ファイル共有などの他システムとの連携機能）を活用することで以下の効果を得ることが可能です。
・校務データ、学習系データ、教育行政・福祉系データなどの、各種システム間のデータ連携
・データやシステムの連携時に、通信の安全性確保などのセキュリティ対策
・クラウドの標準機能として提供されるため、構築期間の短縮と運用負荷の低減
※本機能を利用する場合、連携するシステムとの調整、開発が必要となります。

3. 要件の解説

3.1. 要件①の解説、期待されるメリット

要件				解説	期待されるメリット	
番号	カテゴリ	目的	要件	必要な理由	主として教育委員会・学校（SaaS利用者）	主として校務システムメーカー（SaaS提供者）
1-1	基本的な契約等	トラブル、法的な対応を円滑に行うため。	日本国の法令の範囲内で運用できるサービスであること。また、日本国内の裁判所を合意管轄裁判所とすること。	クラウド事業者は国外や遠隔地の企業である可能性があるため、紛争解決の迅速化と効率化、および当事者の便宜を図る目的で、仕様書に合意管轄裁判所を明記します。	個人情報の漏洩やクラウドサービスが長期に利用できない等、法的措置が必要な事案が生じた際、対応を円滑にできます。	
1-2	レジリエンス向上	一般的なクラウド環境の可用性水準を示す事で、要件水準を統一する。	仮想マシンの稼働するハードウェアは冗長化されており、ハードウェア故障時には自動的に、正常なハードウェアから復旧すること。	ハードウェアの故障に備え、冗長化によってシステム停止を防ぎ、サービス継続性を高めます。自動復旧機能により、迅速な復旧が可能となり、システム停止時間を最小限に抑えます。	クラウドサービスの安定的・継続的な利用が可能となります。	
1-3	レジリエンス向上	一般的なクラウド環境の可用性水準を示す事で、要件水準を統一する。	ネットワーク含めたデータセンターレベルのハードウェアまで完全に冗長化されていること。	仮想マシン（サーバー）だけでなく、ネットワークやデータセンター全体のハードウェアを冗長化することで、より強固な可用性を実現します。		
1-4	レジリエンス向上	一般的なクラウド環境の可用性水準を示す事で、要件水準を統一する。	クラウドサービス内で冗長性を確保し、主要な機能においては1つのリージョン内で高いSLA（99.9%以上）を提供すること。	SLAによって、クラウド事業者が提供するサービスの可用性を保証します。校務や授業への影響を最小限に抑えます。 SLA：Service Level Agreementの略で、クラウド事業者とその利用者の間で結ばれる、サービスのレベル（定義、範囲、内容、達成目標等）に関する合意サービス水準、サービス品質保証などと訳されます。一般的には契約書などに含まれています。	サービスが利用できる時間帯や障害率の上限などを明確にでき、安定的に利用することが可能となります。	
			国内に複数のリージョンが存在し、リージョン同士が数百km以上離れていること。	地理的に離れた複数のリージョンを持つことで、大規模災害が発生した場合でも、別のリージョンにシステムを切り替えることで、事業継続性を確保します。数百km以上の距離があれば、広範囲な災害の影響を分散できます。 リージョン：１つのデータセンター、または同じ地域にある複数のデータセンター環境のこと	地震等の大規模災害で校務支援システムを稼働しているデータセンターが損傷した場合でも、切り替えることで継続して校務支援システムを利用することができます。	
1-5	レジリエンス向上	一般的なクラウド環境の可用性水準を示す事で、要件水準を統一する。	受電方法と非常用発電設備は冗長化されており、非常用電源（自家発電機）を有していること。かつ、データーセンター毎に冗長化されており、法定点検や工事等の際にも止まることなく電力供給が可能なこと。	データセンターは大量の電力を消費するため、電力供給の停止はシステム全体に影響を及ぼします。データセンターでは、受電方法と非常用発電設備を冗長化することで、電力供給の途絶を防ぎ、安定したサービス提供を可能にします。 法定点検や工事などによる計画停止時にも、冗長化された電力供給システムによって、システムを停止することなく運用を継続できます。	急な障害等で電力供給が途絶した場合でも、サービスを安定的に利用できる。計画的な電力供給停止の場合でも、システムを継続的に利用できます。	
1-6	レジリエンス向上	災害対策を簡易に実現する。	データセンターの被災時には、被災地とは別の地理的に離れたロケーションでシステムをバックアップデータから復旧可能とする機能を提供すること。	大規模災害が発生した場合、データセンターが被災する可能性があります。地理的に離れたロケーション（地域）にバックアップデータを保管し、迅速にシステムを復旧できます。	大規模災害でデータセンターが損傷した場合でも、システムを迅速に復旧できます。	
1-7	レジリエンス向上	クラウド側でサービスとして提供されるインターネット回線が安定運用されている事を担保するため。	クラウド側でサービスとして提供されているインターネット回線は冗長化されていること。	インターネット回線の障害は、クラウドサービスへのアクセスを遮断し、業務に大きな影響を与える可能性があります。回線を冗長化することで、インターネット接続を維持します。	ネットワークの障害が発生しても、サービスを途切れることなく利用することができます。	

要件				解説	期待されるメリット	
番号	カテゴリ	目的	要件	必要な理由	主として教育委員会・学校（SaaS利用者）	主として校務システムメーカー（SaaS提供者）
1-8	レジリエンス向上	バックアップデータから簡易に仮想マシンを復旧し、可用性を高める。	OSを含むデータ全体のバックアップを取得できること。取得したバックアップはいつでも仮想マシンの復元に使用できること。復元時は別のサイズの仮想マシンを選択できること。	OSを含むデータ全体のバックアップがあれば、システム全体を迅速に復旧できます。	システムに障害が起こった場合でも、システム全体を迅速に復旧できます。	
1-9	レジリエンス向上	可用性が担保されたマネージドサービスを提供しているクラウド事業者を選定することで、高可用性を実現する。	全てのマネージドサービスは、可用性が確保されている状態で提供されているか、利用者側で機能を選択をすることで可用性を実現できるように設計されていること。	マネージドサービスは、クラウド事業者が運用を代行するため、利用者は運用負荷を軽減できます。可用性が確保されたマネージドサービスを利用することで、利用者自身で複雑な設定や運用を行うことなく、高可用性を実現できます。 マネージドサービス：マネージドサービスとは、データベースやインフラ運用（バックアップ、監視）など、クラウド事業者が管理してくれるサービスのことです。	複雑な設定や運用操作を行うことなく、使いたいサービスを使うことができます。	
1-10	レジリエンス向上	データ消失のリスクを低減させる。	バックアップを保管するストレージは、二重化以上の保護をされた高い耐久性を持たせ、ファイルの永続的な保管ができること。	ストレージ（データ保管領域）の故障や災害などによるデータ消失を防ぐため、ストレージの二重化以上の冗長化が必要です。	データの消失を防ぐことができます。	
1-11	標準的なセキュリティ対策	セキュリティの要求水準を底上げする。	選定するクラウド基盤は、ISO27017を取得していること。	ISO27017は、クラウドサービスにおける情報セキュリティ管理に関する国際規格であり、取得していることは、クラウド事業者が一定水準以上のセキュリティ対策を実施していることを示します。	情報セキュリティ管理を確実に行っているクラウドサービスを見分けることができます。	
1-12	標準的なセキュリティ対策	ヒューマンエラーの防止や、乗っ取り被害による構成破壊工作を防止する。	クラウド環境に対する攻撃、または想定しない行動が取られ、セキュリティ上の脅威に晒される可能性が出た場合にこれを検出する機能が提供されること。	セキュリティ上の脅威を早期に検知することで、被害を最小限に抑え、迅速な対応を可能にします。	クラウド基盤への攻撃など、セキュリティに対する脅威へ迅速に対応できます。	
1-13	標準的なセキュリティ対策	ランサムウェア対策が簡易に実行できる環境が必要。	バックアップデータをマシンイメージごと保管するストレージサービスはWORM機能を有し、バックアップデータをランサムウェアから保護すること。	WORM（Write Once Read Many）機能は、一度書き込んだデータを変更・削除できないようにする機能であり、ランサムウェアによるデータの暗号化や改ざんを防ぎます。 ランサムウェア：コンピュータシステム内のデータやファイルへのアクセスを制限し、その制限を解除するために身代金（ランサム）を要求する不正なソフトウェアの一種です。感染すると、システムが使用不能になったり、重要な情報が漏洩する危険性があります。 （参考） ランサムウェア等によるサイバー攻撃について(注意喚起) https://www.mext.go.jp/content/20230202-mxt_jogai02-000003278_001.pdf	想定しないデータの暗号化や改ざん、喪失を防止することができます。	
1-14	標準的なセキュリティ対策	クラウド環境のアカウント保護を実現する。	クラウド環境にアクセス可能なアカウントは、ID/パスワードの他、多要素認証（MFA）や接続元IPアドレス制限などを利用して強固な認証を行うことができること。	ID/パスワードのみの認証は、パスワード漏洩や推測による不正アクセスのリスクがあります。そのため、多要素認証（例：MFA、接続元IPアドレス制限）などの多層的な認証方式を導入することで、不正アクセスを防止し、アカウントを保護します。 多要素認証：複数の異なる認証要素を組み合わせることで、単一の認証要素が破られた場合でも不正アクセスを防ぐことを目的とします。	システムに対する不正なアクセスを防ぎ、セキュリティを確保できます。	

要件				解説	期待されるメリット	
番号	カテゴリ	目的	要件	必要な理由	主として教育委員会・学校（SaaS利用者）	主として校務システムメーカー（SaaS提供者）
1-15	標準的なセキュリティ対策	クラウド環境のアカウント保護を実現する。	アカウント毎に操作権限を付与できること。	アカウント毎に操作権限を付与することで、不要な権限を持つアカウントを減らし、不正アクセスや誤操作による情報漏洩のリスクを低減します。	不正アクセスや誤操作によるデータの喪失、漏洩のリスクを減らします。	
1-16	標準的な拡張性や運用要件	技術革新が頻繁に行われているクラウド事業者を選定することで、最新技術への追随性を高め、アプリケーションの陳腐化を防ぐ。	新サービスや新機能が定期的にリリースされ続けており、技術革新が頻繁におこなわれているクラウド事業者であること。	IT技術は常に進化しており、最新技術を取り入れたクラウドサービス機能を活用することで、将来の需要変化への柔軟な対応、コスト最適化、及びシステム安定性が期待できます。	新たな機能の利用やサービス利用料の低下などが期待できます。	新たな機能の開発・提供、安定的な運用などサービスの高度化が実現しやすくなります。
1-17	標準的な拡張性や運用要件	クラウド側でサービスとして提供されるインターネット回線が安定運用されている事を担保するため。	インターネット回線の帯域制限は無く、利用実態に応じた帯域を利用できること。	帯域制限があると、データ転送速度が制限され、システムのパフォーマンスが低下する可能性があります。利用実態に応じた帯域を利用できることで、安定したパフォーマンスを確保します。	システム利用時の待ち時間、遅いレスポンス等を減らし、安定して利用できるようになります。	安定したサービス提供が可能になります。
1-18	標準的な拡張性や運用要件	必要なサポートや運用支援水準を定める。	24時間365日の日本語によるサポートを提供すること。	クラウド事業者は国外の事業者である場合があります。日本語によるサポートを活用することで、認識の齟齬なく課題を解決し、システム稼働への影響を最小限に抑えることができます。	システム利用に関する問題の対処方法を円滑かつ正確に理解できます。	
1-19	標準的な拡張性や運用要件	必要なサポートや運用支援水準を定める。	メンテナンスや障害情報などについて、適切に日本語で通知を行うこと。	メンテナンス情報や障害情報などを適切に日本語で通知を受けることで、システム運用状況を正確に把握し、迅速かつ適切な対応を講じることができます。	システムの運用に関する情報を円滑かつ正確に把握できます。	
1-20	標準的な拡張性や運用要件	リフト対応を簡易に実現させるため。	オンプレミス環境からのクラウドリフトを容易に実現するためのサービスなどが提供されていること。	オンプレミス環境からクラウドへの移行（クラウドリフト）は、複雑で時間とコストがかかる場合があります。移行を容易にするためのサービスが提供されていれば、移行コストを削減し、スムーズなクラウド移行を実現できます。	従前使用していたシステムからクラウド環境に円滑に移行ができるようになります。	オンプレミスのシステムをクラウド環境に移行させたいというユーザの要求に容易に対応できるようになります。
1-21	標準的な拡張性や運用要件	柔軟にリソースの増強、また縮小を行い、効率的な運用を行える環境を目指す。	配備された各リソースについて、運用状況を踏まえて容易に増強または縮小させることができること。	システムの負荷状況に応じて、柔軟にリソース（CPU/メモリなど）を増減させることで、無駄なリソースを削減し、パフォーマンス、及びコストを最適化します。	大量の操作等を行う場合でもリソースを気にする必要がなくなります。処理量に応じコストを最適化できます。	システムのリソース調整をクラウド基盤に委ねることができ、パフォーマンス低下等を招きにくくなります。

3.2. 要件②の解説、期待されるメリット

要件				解説	期待されるメリット	
番号	カテゴリ	目的	要件	必要な理由	主として教育委員会・学校（SaaS利用者）	主として校務システムメーカー（SaaS提供者）
2-1	より高度なセキュリティ対策	セキュリティの要求水準を底上げする。	選定するクラウド基盤は、児童生徒や教職員、保護者などの個人情報等を保護するための認証を取得していること。 【必須】ISMAP認証 【推奨】ISO27018	【解説】 クラウドサービスを選ぶ際の重要な安全基準についての要件です。特に、学校関係者（児童生徒、先生方、保護者）の大切な個人情報を確実に守るための認証が必要というものです。 ・ISMAP認証（必須）：政府が定めた、安全なクラウドサービスの基準を満たしているという認証 ・ISO27018（推奨）：個人情報の保護に特化した国際的な基準を満たしているという認証 ※注意点：本要件で保護できる対象はあくまでクラウド事業者がサービス提供する範囲までです。 校務システム自体のセキュリティは個別に対策する必要があります。	・国や国際機関が定めた安全基準・仕組みに基づいて運用され、定期的な監査も行われるため、個人情報漏洩リスクを低減できます。 ・利用者（教職員や保護者）に対して個人情報の安全性を説明しやすい。 ・クラウド部分に関する個別の監査を省略・簡略化できます。	・クラウド基盤部分の個人情報保護について、クラウド事業者に委ねるイ音が可能になります。 ・ユーザ（教育委員会や学校）にクラウド基盤部分の安全性を説明しやすくなります。
2-2	より高度なセキュリティ対策	セキュリティの要求水準を底上げする。	VSS（共通脆弱性評価システム）スコアや、影響範囲の大きさなどを考慮して、世界的なセキュリティインシデント発生時には、迅速に影響を受けるサービス範囲や対応策を通知すること。	【解説】 この要件は、重大なセキュリティ問題が世界的に発生した際に、クラウドサービス事業者がどのように利用者に知らせるべきかを定めたものです。	重大なセキュリティ問題の情報を迅速に入手でき、早期に適切な対応を取りやすくなります。	
2-3	より高度なセキュリティ対策	提供されているマネージドサービスはプライベートな独立性を担保する必要がある。	利用できるマネージドサービスや同一クラウド基盤上の他者サービスをプライベートなネットワークからも利用できること。利用にあたってはアクセス制御をかけられること。	【解説】 この要件は主に2つの重要な点を定めています： 1. クラウド事業者が提供する便利な標準サービス（AIによる画像認識や自然言語処理、データ分析など）を、インターネットを経由せず、プライベートな通信経路で安全に利用できることを求めています。 2. これらのサービスには、専用のリソースとして提供されるものと、複数のお客様で共有される形で提供されるものがありますが、いずれの場合もアクセス制御により、適切なセキュリティを確保する必要があります。	・セキュリティを確保しながら、クラウドならではの便利な機能を活用できます。 ・クラウド機能を利用する際、インターネットを経由しないため、通信の安全性が高く、速度も向上します。 ・必要な権限を持つユーザーやシステムのみがアクセスできますよう、細かな	・校務支援システム以外のクラウドならではの機能を、セキュリティを確保しながら利用者に提供することができます。
2-4	より高度なセキュリティ対策	ヒューマンエラーの防止や、乗っ取り被害による構成破壊工作を防止する。	構成変更のトラッキングができ、決められたルールに違反した構成変更を制限、またはアラートを挙げる機能を有すること。	【解説】 これは、クラウドシステムの「設定変更の監視と制御」に関する要件です。主に以下の2つの機能を求めています ・構成変更のトラッキング（追跡）機能 　－システムの設定や構成が変更された際の記録を取るものです。誰が、いつ、何を、どのように変更したかを追跡できます。 ・不適切な変更の予防機能 　－ファイアウォールを全開放しないなど、あらかじめやってはいけないことをルールとして組み込むことで、自動的にそれらの変更を防止、または警告することができます。	・意図しない変更を防止したり、ヒューマンエラーによる事故を未然に防ぐことが可能になります。	・利用者（教職員等）によるヒューマンエラーが低減し、運用負担を減らせます。 ・システムのガバナンス強化にもつなげられます。

要件				解説	期待されるメリット	
番号	カテゴリ	目的	要件	必要な理由	主として教育委員会・学校（SaaS利用者）	主として校務システムメーカー（SaaS提供者）
2-5	より高度なセキュリティ対策	セキュリティ強化対策が簡易に実行できる事を担保する。	環境に配備したリソースに対する脅威検出機能、サービスを利用できること。	クラウド基盤上でシステムを構築する事業者は、システムの内部で行われる通信や操作（例：データの閲覧、設定変更など）を常に監視し、不審な動きがないかをチェックする必要があります。この要件では、そのような監視を自動的に行えるサービスの利用を求めています。 またクラウド環境では、システムの操作のほとんどがAPI（システムを操作するための専用インターフェース）を通じて行われます。例えば、データの保存、サーバーの起動、ネットワークの設定変更など、すべての操作がAPIを介して実行されます。そのため、これらのAPI呼び出しを常時監視し、不正な操作や異常を検知することが重要です。 【主な監視対象】 ・クラウドサービスへのAPI呼び出しの異常 －通常使用しない操作の実行、大量のリソース作成など、異常な操作パターン、普段と異なる場所や時間帯からの操作 ・クラウド内部のネットワーク通信 －サービス間の不審な通信、想定外の通信先への接続試行 ・クラウドリソースの設定変更 －セキュリティ設定の改ざん、アクセス権限の不適切な変更	・クラウド事業者による最新の脅威情報と、校務サービス提供者の対応に関する情報が迅速に入手できます。	・大きな工数を必要とするログ収集・分析基盤を自前で構築する必要がありません。 ・クラウド特有の攻撃手法に迅速に対応できます。 ・専門的な知識が必要なAPI呼び出しの監視のための人材を確保しなくてすみます。 ・個々のシステムでは把握が難しいクラウド事業者レベルのみ把握可能な脅威情報を活用できます。 ・複数のクラウドサービスにまたがる相関分析も可能となります。
2-6	より高度なセキュリティ対策	セキュリティ強化対策が簡易に実行できる事を担保する。	脅威検出にあたっては、悪意のある通信、変更監視、不正操作等を継続的にモニタリングが可能であること。			
2-7	より高度な拡張性や将来性に関わる要件	マネージドサービスが提供されているクラウド事業者を選定することでシステムの開発ライフサイクルを加速する。	データベースや運用管理ツール等、従来は利用者側で購入し、導入して利用していたミドルウエアやツール等がマネージドサービスとして利用できること。	【解説】 この要件は、システムを運用する上で必要なさまざまなソフトウェアを、クラウド事業者が提供するサービスとして簡単に利用できることを求めています。 【従来の方式との違い】 ＜従来の方式＞ • 必要なソフトウェアを自分で購入/インストールや初期設定を自分で実施 • バージョンアップや保守作業を気にする必要がある • 障害対応を実施する必要あり/サーバーの容量管理も自分で実施 ＜マネージドサービスの場合＞ •導入、増強措置に対してライセンス購入や調達が不要で、すぐに利用開始可能 •バージョンアップや保守作業が不要な為、リスク低減 • 24時間の監視・障害対応を気にしなくて良い/ 必要に応じて自動で拡張もされるものもある 【具体的なサービス例】 • データベース/監視ツール/ バックアップツール/ ジョブ管理ツール	ー	• 運用管理の手間を大幅に削減/専門的な知識がなくても高度なツールを利用できます。 • 最新バージョンのソフトウェアを常に利用でき、システム規模の拡大・縮小が柔軟になります。 ＜例＞ データベースを利用する場合、従来は専用サーバーの準備、ソフトウェアの購入、インストール作業、定期的なバックアップ設定など、多くの準備作業が必要だった。マネージドサービスでは、必要な設定を選ぶだけで、すぐにデータベースを利用開始でき、運用管理の大部分をクラウド事業者に任せることができます。
2-8	より高度な拡張性や将来性に関わる要件	提供されているマネージドサービスの情報が一般的に公開されているクラウド事業者を選定し、導入の敷居を下げ、ロックインを防ぐ。	提供されている全てのマネージドサービスに関する技術情報及び用例等がインターネット上に複数年間公開されているクラウド事業者を選定すること。	【解説】 この要件は、実績が十分にあり、広く利用されているクラウド事業者（クラウド事業者）を選定することを求めています。 【具体例】 実績や情報公開が十分でないクラウド事業者のデータベースサービスを採用した場合、運用開始後にパフォーマンスの問題が発生しても、解決方法の情報が見つからず、事業に重大な影響を及ぼす可能性があります。 複数年に渡る豊富な技術情報や事例の公開は、そのクラウド事業者とサービスが十分な実績と信頼性を持っている証となります	ー	以下のようなリスクを未然に防止しやすくなります。 ・サービスの信頼性・安定性、実運用での問題点、性能や耐久性の実績が確認できず、トラブルが生じる。 ・想定外の制限や仕様が後から判明し、対処を求められる。 ・トラブル発生時に解決方法の情報が見つからない ・対応できます技術者が確保できず、対応が長時間化。 ・サービスが突然終了する、予告なき仕様変更が行われる。 ・技術サポート体制が不十分なことに起因する新機能の開発・展開の遅れ

要件				解説	期待されるメリット	
番号	カテゴリ	目的	要件	必要な理由	主として教育委員会・学校（SaaS利用者）	主として校務システムメーカー（SaaS提供者）
2-9	より高度な拡張性や将来性に関わる要件	提供されているマネージドサービスが、セキュアに管理運用できることを担保する。	マネージドサービスとして提供される機能の監視、ログ管理はクラウドの管理画面、または管理APIと統合され、一元管理できること。	【解説】 この要件は、クラウド上で利用するさまざまなサービスの状態監視やログ確認を、バラバラのツールではなく、クラウド基盤の統一された管理機能で一括して行えることを求めています。 【従来の課題】 各サービスごとに異なる管理方法だと： ・複数の画面を行き来する必要があり、運用効率が悪く、問題発生時の原因調査に時間がかかる可能性がある ・複数のサービスにまたがる問題の把握が困難になる、サービスによっては監視できていない等のリスクが出る ・運用担当者の習熟に時間がかかる ・アクセス権限の管理が複雑化する このような一元管理機能は、大規模なシステムの安定運用には不可欠な要素となります。	ー	・一つの画面で全てのサービスの状態を把握可能になり、障害発生時の調査が効率化できます。 ・サービス間の関連性のある問題を発見しやすく、全てのサービスを網羅して監視できます。 ・運用担当者の教育コストを削減 ・アクセス権限の一元管理が可能
2-10	より高度な拡張性や将来性に関わる要件	将来的なデータ連携、システム間連携を想定し、API連携やファイル連携を簡易に実現し、セキュアに管理運用できることを担保する。	APIサービスとして、ルーティング、アクセス制御、ログ管理などの基本機能を提供すること。また、ファイル共有サービスでは、保管時および転送時の暗号化、IP制限による接続制御、データ単位でのアクセス管理を実装すること。さらに、RESTful APIによる標準的なインターフェースを提供し、APIコールを含むアクセスログの取得・保存およびデータ更新時のイベント通知機能を具備すること。	【解説】 この要件は主に2つの重要な点を定めています： ・クラウドの機能として、異なるシステムとのデータ連携やシステム間連携を実現するためのサービスを提供すること。 ・データ連携やシステム連携を安全に実現するため、クラウド機能として適切なセキュリティ対策を提供すること。 これらの機能は、現代のシステム間連携において、安全性、効率性、安定性を確保するための重要な要件と言えます。	・標準化されたデータ連携環境を利用することで、校務データ、学習系データ、教育行政・福祉系データなど各種システム間のデータ連携を素早く検討できます。 ・セキュリティ確保されたクラウドサービスを利用することで、品質の高い環境整備が可能となります。	・校務支援システムとツールサービス（保護者連絡等）を連携する際、セキュリティの確保、円滑な連携の実現、設計・構築期間の短期化、運用負荷の低減などが図れます。

4. 別紙１　要件適合宣言書

各社記入後 APPLIC 事務局に送付→各社ホームページ掲載、APPLIC ホームページ掲載

「校務支援システムのクラウド化におけるクラウド基盤要件書V1.0」普及適合宣言書

要件番号	対応有無	対応状況の詳細	（対応無の場合）部分対応、未対応の理由
①- 1			
①- 2			
①- 3			
①- 4			
①- 5			
①- 6			
①- 7			
①- 8			
①- 9			
①- 10			
①- 11			
①- 12			
①- 13			
①- 14			
①- 15			
①- 16			
①- 17			
①- 18			
①- 19			
①- 20			
①- 21			
②- 1			
②- 2			
②- 3			
②- 4			
②- 5			
②- 6			
②- 7			
②- 8			
②- 9			
②- 10			

上記の通り、当社は（一財）全国地域情報化推進協会の規定する「校務支援システムのクラウド化におけるクラウド基盤要件書V1.0」に
適合していることを宣言します。

2026年　月　日

会社・団体名
サービス名