株式会社SasaeL

要件適合宣言書

要件番号	要件	対応有無	根拠	関連URL・参考資料
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。	○	日本法を準拠法とし、東京地方裁判所を合意管轄裁判所とする特約条項が用意されています。	https://services.google.com/fh/files/misc/ja-google-cloud-terms-of-service.pdf
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。	○	Compute Engineは「ライブ マイグレーション」機能を備え、ハードウェア保守や故障の予兆時に、稼働中のVMを別のホストへ自動移動させ継続稼働させます。	https://cloud.google.com/compute/docs/instances/live-migration?hl=ja
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。	○	リージョン、ゾーン（独立したデータセンター群）という階層構造により、電力、冷却、ネットワークを含め完全に冗長化されています。	https://cloud.google.com/compute/docs/regions-zones?hl=ja
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。 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。	○	東京と大阪の2リージョンがあり、400km以上離れています。主要な構成で99.9%以上のSLAを提供可能です。	https://cloud.google.com/compute/sla?hl=ja
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。	○	Googleのデータセンターは、複数の電力系統、非常用発電機、UPSを備え、無停止での点検・保守が可能な設計となっています。	https://cloud.google.com/terms/data-processing-addendum
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。	○	スナップショットの遠隔地保管や、Cloud Storageのマルチリージョン設定により、地理的に離れた場所での復旧が可能です。	https://cloud.google.com/architecture/disaster-recovery?hl=ja
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。	○	Google独自のグローバルネットワークは、独自の海底ケーブルや数多の拠点により、インターネット経路が高度に冗長化されています。	https://cloud.google.com/networking?hl=ja
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。	○	マシンイメージやスナップショットによりOSを含む丸ごとのバックアップが可能。復元時に異なるマシンタイプを選択できます。	https://cloud.google.com/compute/docs/machine-images?hl=ja
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。	○	Cloud SQLの高可用性構成やCloud Storageの自動複製など、主要マネージドサービスは標準で高可用性を提供しています。	https://cloud.google.com/sql/docs/mysql/high-availability?hl=ja
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。	○	Cloud Storageは、イレブンナイン（99.999999999%）の年間耐久性を設計目標としており、データは自動的に多重化保管されます。	https://cloud.google.com/storage/docs/availability-durability?hl=ja
①-11	選定するクラウド基盤は、ISO27017を取得していること。	○	ISO/IEC 27017（クラウドセキュリティ認証）を取得済みです。	https://cloud.google.com/security/compliance/iso-27017?hl=ja
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。	○	Security Command Center (SCC) により、不審なアクティビティや構成の不備をリアルタイムで検出・通知します。	https://cloud.google.com/security-command-center?hl=ja
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。	○	Cloud Storageの「バケットロック」機能により、WORMを有し、ランサムウェア等の改ざんから保護します。	https://cloud.google.com/storage/docs/bucket-lock?hl=ja
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。	○	Cloud Identity/IAMにて、多要素認証（MFA）およびIP制限の設定が可能です。	https://docs.cloud.google.com/docs/authentication/mfa-requirement?hl=ja https://docs.cloud.google.com/access-context-manager/docs/overview?hl=ja
①-15	アカウント毎に操作権限を付与できること。	○	IAMにより、ユーザーやグループ単位で細かな権限を付与できます。	https://cloud.google.com/iam/docs/overview?hl=ja
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。	○	毎年数千を超える新機能・サービスをリリースしており、生成AIなどの最新技術も迅速に提供されています。	https://cloud.google.com/release-notes?hl=ja
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。	○	インターネット接続サービスに帯域制限はありません。	https://docs.cloud.google.com/compute/docs/network-bandwidth?hl=ja
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。	○	日本語による24時間365日のサポートを提供しています。	https://docs.cloud.google.com/support/docs/language-working-hours?hl=ja
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。	○	サービスヘルスのダッシュボード等を通じ、障害やメンテナンス情報を日本語で適切に通知する仕組みがあります。	https://status.cloud.google.com/regional/asia?hl=ja
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。	○	Migrate to Virtual Machinesサービスにより、オンプレミス環境からの容易なリフト＆シフトが可能です。	https://cloud.google.com/migrate/virtual-machines?hl=ja
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。	○	Compute Engineのマシンタイプを即座に変更できるほか、オートスケール機能により負荷状況に応じたリソースの自動的な増減が可能です。	https://docs.cloud.google.com/compute/docs/autoscaler?hl=ja

要件番号	要件	対応有無	根拠	関連URL・参考資料
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	○	ISMAPやISO 27018認証を取得しています。	https://cloud.google.com/security/compliance/ismap?hl=ja https://cloud.google.com/security/compliance/iso-27018?hl=ja
②-2	CVSS（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。	○	脆弱性発生時はCVSSスコアを含むアドバイザリを迅速に公開し、影響範囲と対応策を利用者に通知します。	https://docs.cloud.google.com/advisory-notifications/docs/overview?hl=ja
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。	○	Private Service Connectにより、マネージドサービスをインターネットを経由せずプライベートなネットワークから利用可能です。	https://docs.cloud.google.com/vpc/docs/private-service-connect?hl=ja
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。	○	Cloud Asset Inventoryによる変更履歴の追跡や、組織ポリシーによる違反の自動検出が可能です。	https://cloud.google.com/asset-inventory/docs/overview?hl=ja
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。	○	Security Command Centerにより、環境全体のリソースに対する脅威や脆弱性を継続的に自動検出します。	https://cloud.google.com/security/products/security-command-center?hl=ja
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。	○	VPC Flow LogsやCloud Loggingにより、通信、操作、変更監視をリアルタイムで継続的にモニタリング可能です。	https://cloud.google.com/logging/docs/overview?hl=ja
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ェ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。	○	データベース、監視、運用管理ツール等の機能を、インストール不要なマネージドサービスを提供しています。	https://cloud.google.com/products?hl=ja
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。	○	全サービスの技術仕様や事例はインターネット上に公開されており、常時参照が可能です。	https://cloud.google.com/docs?hl=ja
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。	○	全てのサービスのログ・監視データはCloud Logging / Monitoringに集約され、管理画面や管理APIで一元管理できます。	https://cloud.google.com/stackdriver/docs?hl=ja
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。	○	API Gatewayによる制御やCloud Storageの暗号化・IP制限・REST API、およびデータ更新時のイベント通知機能を具備しています。	https://cloud.google.com/api-gateway?hl=ja https://docs.cloud.google.com/docs/security?hl=ja

上記の通り、当社のクラウド型校務支援システム「SasaeL 校務」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 Ver1.0」の要件①②に対応していることを宣言します。

2026年2月13日