千歳市小中学校教育系ネットワーク構築業務

仕様書

令和８年４月

千歳市教育委員会

目次

１．調達件名

千歳市小中学校教育系ネットワーク構築業務

２．調達要件

2.1　調達の背景・目的

千歳市（以下、当市という。）では、教員が授業に使用する指導者用コンピュータの更新を計画している。その際、従来は別に整備していた校務用コンピュータとの「強固なアクセス制御」を講じた上での統合を検討しており、これは「GIGA スクール構想の下での校務 DX について（詳細版）」及び令和７年３月改訂の文部科学省「教育情報セキュリティポリシーに関するガイドライン」（以下、ガイドラインという。）に次世代の学校 ICT 環境の推奨される姿として提言されている整備である。

本業務を行うことにより、多忙な教員の業務効率化が図られ、学校教育の質の向上を通じて、「住民の利便性向上」を実現することを目的とする。

2.2　調達方針

現状、当市において教職員は２台以上の端末を使い分けており、校務処理は職員室に限定されている。端末の一台化とクラウド活用、及び校務のロケーションフリー化は、教職員の働き方の選択肢を増やし、効率的な業務環境を実現することで学校教育の質の向上を実現するために必要不可欠なものとなる。

学校教育の質の向上を実現するために、本業務では、ガイドラインで示されている「強固なアクセス制御」を講じたセキュリティ環境を導入し、重要性分類Ⅱ以上の情報をパブリッククラウド上で適切に取り扱い情報を守りながら、学校における働き方改革、教育活動の高度化、教育現場のレジリエンスの確保に資するよう取り組むこととする。

「強固なアクセス制御による対策」とは、インターネットを通信経路とする前提で、内部・外部からの不正アクセスを防御するために、多要素認証による利用者認証、端末認証、端末・サーバ・通信の監視・制御を組み合わせたセキュリティ対策のことを指しており、この対策を講じるにあたっては、利用者毎に情報へのアクセス権限を適切に設定するとともに、アクセスの真正性、端末・サーバ・通信の安全性を確保する観点から、端末とクラウドサービスを提供するサーバ間の通信を暗号化し、認証により利用者のアクセスの適正さを常に確認できるものとする。

本業務により、教員が職員室以外や学校外からでも、機微度の高い情報（成績、指導記録等）を含むデータへ安全にアクセスし、授業準備や個別指導を深化させ、学校教育の質の向上を目指す。

なお本業務は、総務省「デジタル活用推進事業債」を活用した事業であり、制度の趣旨を踏まえた業務の遂行となるよう心掛けること。

2.3　業務範囲

本業務の範囲は以下のとおりとする。

（1）　指導者用コンピュータ/校務用コンピュータの統合端末（1 人 1 台）でクラウド環境を安全に利用可能なセキュリティ環境（SASE/エンドポイントセキュリティ等、強固なアクセス制御技術）の導入及び構築

（2）　セキュリティシステム導入

（3）　M365 導入/データ移行支援

（4）　統合端末の安全な利用に必須となる既存の校内 LAN 整備/関連システム事業者等、及び、端末調達事業者等との連携・調整対応

2.4　履行期間

（1）　構築期間　：　契約締結日～令和８年 11 月 30 日（予定）

（2）　試験運用期間　：　令和８年 12 月下旬～令和９年 2 月下旬（想定）

（3）　本運用開始日　：　令和９年 3 月 1 日（想定）

なお、本運用開始日以降は令和 13 年度末までを利用期間とする。

2.5　作業工程概要

（1）　スケジュール

構築期間における作業項目について、作業開始から本運用開始日（本運用開始日以降に実施する作業等を提案する場合はその作業期間まで）のスケジュール（案）を、作業工程等が分かるよう詳細に示すこと。なお、具体的なスケジュールについては、発注者との本業務の契約締結時までに協議の上決定する。

（2）　作業工程等

スケジュール（案）で示した作業工程について、その内容や役割分担等について示すこと。

（3）　留意事項

本業務により構築する環境は、2.4（3）の利用期間が終了するまで使用、保守することを前提とすることから、その点に十分留意の上スケジュール（案）及び作業工程等を検討し、納期を遵守すること。

その上で、本業務の履行にあたり、発注者および受託者の責めに帰さない事由により、納期の遵守が困難となる恐れが生じた場合は、受託者は速やかにその理由及び影響を書面にて発注者へ報告し、必要に応じて双方協議のうえ適切な措置を講ずるものとする。

３．システム要件

3.1　基本要件

3.1.1　目的

（1）　本業務は、千歳市内の小学校・中学校・小中併置校において、校務ならびに学習に用いる統合端末とネットワーク基盤を再構築し、教育現場における業務の効率化及び安全性の向上を図ることを目的とする。

（2）　設計及び運用に際しては、校務と学習の論理分離と適切なアクセス制御を前提とし、校内外を問わず安定した可用性・性能を確保することにより、教職員及び児童生徒が円滑に教育活動を遂行できる環境を実現するものとする。

3.1.2　適用範囲

（1）　対象とする。学校は、千歳市内25校とし、教職員約700名とする。これらの数値は概数であり、今後の増減に応じて柔軟に拡張可能な設計とする。

（2）　本業務の対象とする。端末は、校務及び学習の業務に用いる端末（以下、統合端末という。）とする。

　なお、学習系 Chromebook 端末、PC 教室端末、図書館用端末等は既存環境での利用を継続し、本業務の適用範囲の対象外とする。

（3）　学校内の無線利用が可能なエリアにおいて、同等の利用性を提供するものとする。

（4）　インターネット接続は、各学校から直接インターネットへ接続する方式（ローカルブレイクアウト）を原則とする。統合端末から庁内情報システム向け通信（例えば、財務会計システムへの通信等）については、既存の安全な拠点間接続（閉域網、VPN、SD-WAN等）を確保する。

（5）　校外（研修先や他校等）における端末利用についても、適切な認証及び端末管理に基づき、安全な業務遂行を可能とする。

（6）　統合端末の対応OSはWindows 11（及び構築時点での後継版を含む）とし、台数は約700台とする。

（7）　学校ごとに運用しているオンプレミスの Active Directory（以下、ADという。）は廃止し、当該 AD に登録されているユーザー情報を統合の上、新規 AD を構築すること。新規に登録する情報は、教育委員会の承認を得た内容に基づいて設定するものとする。

3.1.3　準拠と方針

（1）　本業務は、文部科学省が定めるガイドライン（令和７年３月改訂）ならびに「千歳市教育情報セキュリティポリシー」に準拠し、整合を確保するものとする。

（2）　設計・運用においては、ゼロトラストの原則に基づき、以下の対策を全業務運用に適用するものとし、これらは強固なアクセス制御による対策として運用するものとする。

　(a)　利用者 ID の一元管理

　(b)　多要素認証の適用

　(c)　端末のセキュリティ状態確認

(d)　校務／学習ネットワークの論理分離
(e)　端末・ユーザー・組織・アプリケーション単位の条件付きアクセス
(f)　データの暗号化及び持出し時の承認・記録
(g)　横断的なログの取得・分析（認証・アクセス・操作の可視化）
(h)　最小特権の適用（ロール／権限の適正化）
(i)　端末紛失時にモバイルデバイス管理によるリモートワイプ（遠隔削除）及び必要に応じた再登録

なお、上記（i）について、リモートワイプを実施した場合に、必要に応じて端末の再登録及び利用再開に係る設定作業が可能となるよう手順の整理を行うこと。

（3）　校務支援システムへの接続は、現行では閉域網を原則とし、将来はインターネット接続オプションまたは同等のセキュリティを担保したサービスにて接続することとする。

（4）　ネットワーク基盤は、庁舎・データセンター等のオンプレミス環境、またはクラウド基盤（IaaS 等）や、オンプレミス環境およびクラウド基盤を組み合わせた構成を含め、適切な環境に構築すること。その場合における要件は、別紙「クラウド基盤構築基本要件」を参照すること。

（5）　標準化技術を基本とし、同等以上の機能を有する代替提案については、安全性・可用性・運用性の観点から受け入れるものとする。クラウドサービス（SaaS 等）を利用する場合は、サービス提供事業者のサービス要件・監査報告書等に基づき、認証・アクセス制御・データ暗号化・テナント分離・運用管理・インシデント対応・監査／ログの提供体制等の妥当性を確認するものとする。

（6）　本業務で端末へ設定及び導入するソフトウェア類のインストールは端末調達事業者が実施するものとする。本業務の受託者は発注者を通じて端末調達業者と連携・調整対応すること。なお、インストールに必要な情報等（リスト、手順、マスタデータ等）の作成および提供は本業務の受託者が行うものとする。

3.2　要求仕様

前述の「3.1　基本要件」に基づき、本業務の目的・方針を達成するために必要な機能を以下に記載する。要求仕様の各項目において機能が重複する場合には、要求仕様の実現にあたり最適な組み合わせで機能を選定し構成すること。本項において、文末が「～こと」とあるものは必須要件とし、満たさない場合は評価の対象外とする場合がある。また、「～が望ましい」とあるものは加点評価の対象とする。あるいは代替案により同等以上の効果が得られる場合には加点評価の対象とする。

3.2.1　エンドポイントセキュリティ

3.2.1.1 基本機能

【必須要件】

（1） 校務系/学習系環境は、基本的に相互間領域へのアクセスができないよう設計すること。
（2） 校務系/学習系環境は、利用できるアプリケーションをそれぞれの領域ごとに制限できること。
（3） 学校外での利用を想定し、リモート環境から校務系/学習系環境を利用できること。
（4） 校務系・学習系の環境におけるファイルの授受は、データ暗号化等の仕組みを介して安全に実施し、ファイルの持出しは管理者等による承認が行えること。
（5） 教職員の利便性を考慮し、1台の端末で複数の領域（モード）を利用できること。

【希望要件】

以下２つの要件のうち、いずれかを満たすこと。

なお、いずれの要件を選択する場合であっても、高度なセキュリティ環境を維持しつつ、教職員および管理者の運用負荷が増加しない（あるいは自動化・簡略化等により低減される）提案であることを重視する。

＜要件１　（1）～（12）のすべての要件を満たすこと。＞

（1） １台の端末で、複数のモード（例えば、校務・学習・校外モード等）を利用できること。
（2） モード毎に通信接続先、ファイル・データ保存場所、使用アプリケーション、クリップボードを完全分離できること。
（3） 統合端末1 台を操作するとき、同時に両方の画面が表示できないよう完全分離できること。
（4） 各モードの定義は管理者により設定可能なこと。
（5） 各モードで利用できるアプリケーション等は、モード毎に指定できること。
（6） 使用できる有線LAN、Wi-Fi のアクセスポイント、プロキシ、VPN をモード毎に設定可能なこと。
（7） 指定したパスのファイルに対するアクセスの制御をモード毎に設定可能なこと。
（8） モードの切り替え時にスクリプトやプログラムなどのプロセスを実行可能なこと。
（9） ISO/IEC15408 EAL3 認証または同等の基準のセキュリティ基準を満たしていること。
（10） AD の属性情報を同期し、管理者による持ち出し承認等を行う持出専用のフォルダ等を使用できること。

(11) 端末の操作ログを自動で取得し、「PC 名、ファイル名、アプリケーション名、ユーザー名、アクセス日時」などの履歴を網羅的に記録できること。
(12) ユーザーの操作履歴について、「実行ユーザー、操作日時、アクセス元、対象データ、実施操作の内容」などを詳細に記録できること。

＜要件２　（1）～（7）のすべての要件を満たすこと。＞
（1） 隔離領域内での作業と隔離領域外での作業がユーザーの操作によって切り替え可能であること。
（2） 画面上のアイコンをクリックすると、隔離領域内のアプリケーションを一時的に非表示とする機能を有すること。
（3） PC ロック時に自動的に隔離領域内のアプリケーションを非表示にできること。
（4） セキュアコンテナ型セキュリティソフトウェアは脆弱性対応を含むアップデートプログラムが適宜ベンダーより提供されること。
（5） アプリケーションが隔離領域内で動作している状態であることを、視覚的に容易に確認できること。
（6） セキュアコンテナ型セキュリティソフトウェアには、隔離領域内で Web 参照を可能とする専用のセキュアブラウザが同梱されていること。
（7） セキュアブラウザを利用して Web サイトへアクセスする際は、アクセス先 Web サーバーとコンピュータとで直接通信させることなく、専用のセキュアゲートウェイを経由した通信経路に限定することが可能なこと。

3.2.1.2 データの暗号化・複合化

【必須要件】
（1） 校務系/学習系の環境におけるファイルの授受は、データ暗号化等の仕組みを介して安全に実施し、ファイルの持ち出しは管理者等による承認が行えること。
（2） 校務系の環境から、校務支援システムおよびMicrosoft 365（SharePoint、OneDrive、Exchange、Office)、Google Workspace（ドライブのみ、管理者承認が必要)、デジらく採点２（クラウド版）へのアクセスを可能とすること。
（3） 学習系の環境から、Microsoft 365（Office のみ)、Google Workspace へのアクセスを可能とし、校務支援システムおよびMicrosoft 365（SharePoint、OneDrive、Exchange）へのアクセスは拒否すること。

【希望要件】
以下２つの要件のうち、いずれかを満たすこと。
なお、いずれの要件を選択する場合であっても、高度なセキュリティ環境を維持しつつ、教職員および管理者の運用負荷（ファイルの暗号化・復号、承認作業の手間等）が適切に抑制されていること、あるいは利便性を向上させる工夫があることを重視する。
＜要件１　（1）～（10）のすべての要件を満たすこと。＞
（1） データの暗号化において、AES 暗号 256Bit の暗号強度が利用できること。
（2） ファイル個別ではなく、信頼領域/非信頼領域といったホワイトリストにて情報漏洩対策を

行えること。

（3） 統合端末における信頼領域/非信頼領域の定義は管理者により設定可能なこと。

（4） 統合端末の、信頼領域にはファイルが平文で保存されること。

（5） 統合端末から非信頼領域へのファイルの持ち出しは、管理者により許可されたもののみ可能なこと。

（6） ファイルの持ち出しに関する申請があった場合は、管理者に自動で通知する機能を有していること。また、承認・否認した場合は、申請者に自動で通知が飛ばせること。

（7） 統合端末の信頼領域に存在する全てのファイルを、非信頼領域に持ち出す際はファイル拡張子に依存せず自動的に暗号化されること。

（8） 暗号化されたファイルを信頼領域に戻した際に、自動的に復号化されること。

（9） 暗号化及び復号化にパスワード入力が不要なこと。

(10) 信頼領域から非信頼領域へファイルを持ち出す場合の持出専用フォルダを設定可能なこと。また、持ち出すファイルは平文を禁止し、パスワード暗号化をかけたZIP 形式に強制変換することも可能なこと。

＜要件２　（1）～（9）のすべての要件を満たすこと。＞

（1） 隔離領域内で実行されたアプリケーションが行うファイルの書き換え（保存）やレジストリ値の変更が、隔離領域外の環境には影響を与えないように制御し、コンピュータの環境を保護できること。

（2） セキュアコンテナ型セキュリティソフトウェアのプロセスはローカルのプロセスと分離されており、ローカル環境と隔離環境間の意図しない通信を防ぐことができること。

（3） 隔離領域内で実行されたアプリケーションと、OSや隔離領域外で実行された他のアプリケーション間とのデータ通信（COM 経由によるデータ通信）を禁止できること。

（4） 隔離領域内外で実行されるアプリケーション間のクリップボードデータコピーにおいて、双方向のコピー制御、およびテキストデータ（Web リンク等の書式を含む）のみに限定した双方向のコピー制御が可能であること。

（5） 隔離領域内で実行されたアプリケーションからの印刷処理を制御可能なこと。

（6） ２つの異なるネットワーク間で、WEBブラウザを利用したファイルの送受信機能を提供すること。

（7） ファイルの選択はドラッグ&ドロップで行えること。なおドロップ可能な領域はブラウザの全領域で可能なこと。

（8） ファイルの送信時に第三者による承認が行えること。承認者は管理者もしくはユーザー自身によって複数指定でき、また承認者に対して任意のコメントを入力できること。

（9） Active Directory認証を利用する場合、統合Windows認証により、Windows ドメインにログオン済みのユーザー端末（Web ブラウザ）が持つWindowsの資格情報を利用し、ID/パスワードの入力を省略したログインができること。

3.2.1.3 ドライブの暗号化

【希望要件】

以下の要件のいずれかを満たすことが望ましい。満たさない場合には、代替案を提示すること。

なお、代替案により同等以上の効果が得られる場合には加点評価の対象とする。
（1） 統合端末の記憶装置（HDD・SSD）に対し、ドライブ全体の暗号化が可能なこと。
（2） 統合端末の廃棄の際に、情報を復元困難な状態にする措置として暗号化消去が可能なこと。また、暗号化消去の実施完了情報を出力可能なこと。
（3） 暗号化後に外部記録媒体を追加した場合でも、自動的に暗号化が可能であること。

3.2.1.4 ファイルの保存制限及び削除

【希望要件】

以下の要件のいずれかを満たすことが望ましい。満たさない場合には、代替案を提示すること。なお、代替案により同等以上の効果が得られる場合には加点評価の対象とする。
（1） 統合端末のローカルドライブにファイルを保存できる領域を特定の領域のみに制限可能なこと。
（2） 特定の領域に保存されたデータを、管理者が指定したタイミングにて自動で削除可能なこと。
（3） データ削除のタイミングはOS起動・終了、ログオン・オフなどから選択して設定可能なこと。
（4） 管理者が特定の統合端末に対して、遠隔で特定領域に保存されたファイルの削除命令を発行可能なこと。

3.2.1.5 アプリケーションの制限

【希望要件】

以下の要件のいずれかを満たすことが望ましい。満たさない場合には、代替案を提示すること。なお、代替案により同等以上の効果が得られる場合には加点評価の対象とする。
（1） 特定のアプリケーションのみ起動を制限可能なこと。
（2） 起動制限をモード毎に設定可能なこと。
（3） 禁止あるいは許可するアプリケーションは、アプリケーション名だけではなく、ファイル・ハッシュ値による指定ができること。

3.2.1.6 IP送信

【希望要件】

以下の要件のいずれかを満たすことが望ましい。満たさない場合には、代替案を提示すること。なお、代替案により同等以上の効果が得られる場合には加点評価の対象とする。
（1） IPプロトコルを使用したデータ送信（書き込み）を制限可能なこと。
（2） 送信（書き込み）の許可・制限は、アプリケーション名、IPアドレス、ポート番号の組み合わせにより設定可能なこと。
（3） IP送信の制限をモード毎に設定可能なこと。

3.2.1.7 情報漏洩対策

【希望要件】

以下の要件のいずれかを満たすことが望ましい。満たさない場合には、代替案を提示すること。なお、代替案により同等以上の効果が得られる場合には加点評価の対象とする。

（1） USB 接続によるファイルの持ち出し時に、「マシン名」、「ユーザー名」、「端末識別子」の組み合わせで許可設定が行えること。

（2） データ転送機能を持つ Bluetooth デバイス、近距離共有機能を利用したデータ転送を制限できること。

3.2.2 ネットワークセキュリティ

3.2.2.1 基本機能

【必須要件】

（1） セキュリティ機能とネットワークアクセス機能を統合したクラウドサービスであること。

（2） 管理者が許可したクラウドアプリケーション利用時に、脅威防御を行い、安全なアクセスを提供すること。

（3） 自社 PoP をグローバルに展開し、プライベートバックボーンによるメッシュ接続を構成するとともに、日本国内においては東京および大阪を含む複数個所に自社 PoP を設置していること。

（4） エンドポイントセキュリティと連携し、ゼロトラストネットワークを適用できること。

（5） 校内の無線アクセスポイント（AP）を介した利用、及びローカルブレイクアウト回線からの通信に対応すること。

（6） 情報セキュリティ、クラウドサービス、個人情報保護及びプライバシー管理に関する国際規格（ISO/IEC 27001、27017、27018）に準拠していること。

3.2.2.2 SD-WAN 機能

（1） インターネットに接続するすべてのデバイスのアクセス制御と、接続状況を確認するための機能を備えたサービスであること。

（2） アプリケーションへのアクセスを制御する機能として、社内アプリケーションセッションの前にユーザーとデバイスを検証し、組織が定めたそのアプリケーションにアクセスするためのポリシーを制御できるサービスであること。

（3） クラウド接続や拠点間接続において仮想的な WAN を構築し、通信の監視や制御によるトラフィックコントロールを行うことで輻輳や遅延を防止すること。

（4） メーカーが運用管理するクラウドサービスであること。

（5） 優先度の高い接続やトラフィックタイプに基づくルーティングが可能であること。

3.2.2.3 セキュリティ機能

【必須要件】

（1） URL フィルタリングの機能を有すること。

（2） アンチマルウェア機能を有すること。

（3） レポート機能や分析機能を有すること。

【希望要件】

以下の要件のいずれかを満たすことが望ましい。満たさない場合には、代替案を提示すること。なお、代替案により同等以上の効果が得られる場合には加点評価の対象とする。

（1） TLS インスペクションにより HTTPS 暗号化通信の検査が可能であること。

（2） URL フィルタリングにより不適切なウェブページへのアクセスを防止できること。

（3） アンチマルウェア及び次世代アンチマルウェア（AI・機械学習対応）に対応していること。

（4） IPS（侵入防止システム）機能を有していること。
（5） 脅威防御ポリシーの設定を管理者がカスタマイズ可能であること。
（6） マルウェアに感染したエンドポイントを検出する機能を有していること。
（7） クラウドアクセスセキュリティブローカー（CASB）機能を有し、以下（a）～（d）を実施できること、かつ以下（e）を実施できることが望ましい。
(a) クラウドアプリケーションの使用状況とリスクの可視化
(b) ポリシー設定運用とアクセス制御
(c) 既知及び未知のクラウド脅威からの保護
(d) データ保護
(e) データ損失防止（DLP）
（8） クラウドアプリケーションの使用状況をリアルタイムでモニタリング可能であること。
（9） WAN ファイアウォール機能を有し、サイト、ユーザー、サブネット間のトラフィックを制御できること。
(10) 管理者がクライアント PC に対し、ユーザー認証、アクセス制限、ネットワークルールの適用を設定可能であること。
(11) クラウドアクセスに対して多要素認証の設定が可能であること。
(12) 違法または潜在的に悪意のあるトラフィックをブロックする機能を有していること。

3.2.2.4 レポート機能

【必須要件】
（1） セキュリティ管理用のレポート生成が可能であり、以下の内容を網羅すること。
(a) セキュリティイベントの概要
(b) ブロックされたセキュリティイベント
(c) インターネットファイアウォールイベント
(d) WAN ファイアウォールイベント
(e) IPS イベント
(f) アンチマルウェアイベント
(g) 不審なアクティビティイベント
(h) DNS 保護イベント
（2） レポート生成のスケジュール設定が可能であり、自動的に任意のメールアドレスに送信できること。

3.2.3 Microsoft 365

3.2.3.1 業務範囲

発注者が導入するクラウド基盤のうち、本業務で使用するライセンス「Microsoft 365 for Education A3」（当該ライセンスについては発注者が別途調達するものとし、ライセンス調達に係る作業は本業務の範囲に含まない）を利用したテナント構築及び設計に関わる作業を対象とする。

（1） テナント構築に係る利用要件の整理を行うこと。また、整理した結果は発注者に提示し、承認を得ること。

（2） 承認された利用要件に基づき、必要に応じて以下の設定を行うこと。

(a) 新規ユーザー（Microsoft アカウント）の作成

(b) 作成したユーザーへの「Microsoft 365 for Education A3」ライセンスの割り当て

(c) 作業に必要な Microsoft 365 管理権限の付与

3.2.3.2 調達機器・機能等の技術的要件

クラウド基盤構築に関わる性能、機能及び技術等の要件は、以下に示すとおりである。設計内容に関する項目は、設計案を作成し、要件整理結果を発注者に提示して、承認を得ること。

（1） 認証基盤

新設する AD の情報を、クラウドサービス「Microsoft Entra ID」に同期するため、Microsoft Entra Connect を利用し、以下の内容を設定可能とすること。なお、システム構成上、新規 AD の設置環境がオンプレミス環境又はクラウド基盤のいずれの場合においても、本要件の適用対象とする。

(a) パスワードの有効期間に関する設定

(b) ユーザー、ユーザーの所属するグループ、接続するデバイスの状態に応じてサービスの利用を制御する設定

(c) 管理権限のロール設定や管理者権限の必要な操作に関する設定

(d) その他認証基盤構築に必要な内容

（2） ドメイン統合

Microsoft 365 にオリジナルドメインである「chitose-edu.jp」を紐付け、教職員については「chitose-edu.jp」で端末・Microsoft 365 とも利用できるようにすること。

（3） デバイス管理

デバイス管理は「Microsoft Intune (MDM)」を利用し、下記の内容を設定可能とすること。

(a) デバイスの設定を強制、初期化する機能に関する設定

(b) OS のバージョン、パスワードの設定、ロックの設定、端末のテナント管理下からの脱落などの状態を監視し、違反した場合にアクセスブロックする機能に関する設定

(c) MDM にデバイス登録済みの場合に限りアクセスを許可する設定

(d) MDM に登録できるデバイスを事前に制限する機能に関する設定

(e) 外部登録端末の制限に関する設定

（4） 教職員用メール

教職員用のメールは「Exchange Online」を利用し、下記の内容を設定可能とすること。利

用するドメインは「chitose-edu.jp」とする。

なお、「Exchange Online」へのデータ移行は原則ユーザー等にて実施する想定とし、必要に応じて発注者と受託者で別途協議すること。

(a) データ損失防止（DLP）機能に関する設定

(b) スパムメール、フィッシング対策に関する設定

(c) リンク、添付ファイルの安全性を解析し、ブロック等の対応に関する設定

(d) メールの操作ログ取得及びアクセス履歴に関する設定

(e) 使用しているドメイン「chitose-edu.jp」が利用可能かを確認すること

（5） ストレージ（校務系データ）及びファイル共有

校務系データ用のストレージについては、現在オンプレミスのNetwork Attached Storage（以下、NASという。）を利用している。このNASに格納されているデータを移行する先として「SharePoint Online」及び「OneDrive」を構築すること。

構築にあたり事前にデータ移行検証を実施する。データ形式等に起因してデータ移行不可となるファイル等については、利用者にて移行可能な状態に修正するものとする。また、SharePoint上で正常に動作しないデータについても利用者が修正等を行うこととする。

データ移行検証の対象校として本業務内の小学校1校・中学校1校（以下、パイロット校という。）を選定し、検証結果を発注者に報告すること。なお、パイロット校を含め、データの移行は原則ユーザーまたは端末調達事業者にて実施する想定で、発注者と受託者で協議の上端末調達事業者と連携・調整対応すること。また、下記の内容を設定可能とすること。

(a) データの自動暗号化に関する設定

(b) データへのアクセス権に関する設定

(c) ドキュメントライブラリ管理に関する設定

(d) 機密レベルに対応したラベル設定

(e) ファイル操作に関するログを保持する設定

(f) データ移行手順の提示

(g) プリンタ（複合機）でスキャンしたデータを SharePoint Online に格納可能とする設定

（6） フィルタリング

インターネットフィルタリング・メールフィルタリングは、下記の内容を設定可能とすること。

(a) クラウドサービスとして提供されていること

(b) 脅威ドメイン情報を元に、端末が通信しようとしている先が悪性かどうか判別し、危険と判定された場合は通信を自動的にブロックができること

(c) ブラックリスト運用を想定し、特定のURLの許可・ブロック設定ができること

（7） エンドポイント対策

エンドポイント対策は、下記の内容を設定可能とすること。

(a) 次世代マルウェア対策

(b) 攻撃面の削減ルール

(c) デバイス制御

(d) エンドポイント ファイアウォール

(e)　ネットワーク保護

(f)　アプリケーション制御

（8）　利用ログ管理

利用ログ管理は、下記の内容を設定可能とすること。

(a)　下記のログが取得できること

① 監査ログ

② サインイン・認証ログ

③ セキュリティ関連ログ

(b)　上記ログに関して、下記の条件を満たしていること

・ ファイル操作やメール送受信、サインイン履歴、管理者操作のログを取得できること

3.2.4 校内ネットワーク

ネットワーク設計において以下の要件を満たすこと。

（1） 現行の学習系ネットワークの保守業者への情報提供依頼、構成変更等に伴う作業に要する経費は、受託者にて事前に見積を取得し、積算に含めること。なお、受託者が原稿ネットワークの構成変更等に伴う作業を行う場合には、事前に現行の保守業者との合意形成を図った上で、発注者の承認を得るものとする。また、変更箇所を明記した設定資料を作成し提出すること。万が一、当該作業に起因して既存環境に支障が生じた場合は、受託者の責任と費用において速やかに復旧対応を行うこと。

（2） 本更改に係るシステムが、円滑かつ迅速に導入され、かつ運用されるよう設計を行うこと。

（3） 必要に応じて、ハードウェアの適切な設置場所及び必要スペックを調査するためにネットワークアセスメントを実施すること。

（4） ネットワーク設計（物理構成設計、論理構成設計）、システム設計（基本設計、詳細設計、セキュリティ設計、移行設計、運用設計等）、ネットワーク配線設計を実施すること。

（5） 通信経路について、学習系は各校ローカルブレイクアウトする既存回線を継続利用する。校務系は、学習系と同一の物理回線で、論理的に分離された通信経路を利用する。ただし、校務系のうち庁内情報システム向け通信（例えば、財務会計システムへの通信等）については、既存回線を継続利用することとし、既存の校内LAN整備/庁内情報システム事業者と連携・調整対応のうえ、必要な経費は受託者にて事前に見積を取得し積算に含めること。

（6） 各種設計する際に配線や電波利用の調査が必要な場合、その作業にかかる費用は本業務の対象外とする。

（7） 調査した内容を踏まえて設計した結果、示しているシステムに変更が生じる場合は、発注者の承認を得て調整すること。各設計にて作成したドキュメントは、発注者へ納品すること。

（8） 本業務の実施に伴い必要となる軽微なLAN配線等の作業については、本業務の範囲内で受託者が実施すること。ただし、壁面の貫通や大規模な管路敷設など、当該作業が建設業法に基づく建設工事に該当する場合、その工事に係る費用負担及び発注手続き等は発注者が行うものとし、本業務の見積積算には含めないこと。受託者は、事前調査や設計の段階で当該工事の必要性が判明した場合は、速やかに発注者へ報告し対応を協議すること。

3.2.4.1 SSIDの新規定義

現行の学習系ネットワークで利用中の無線アクセスポイントに対し、校務系ネットワーク用のSSIDを新規に定義・追加する。学習系／校務系の各SSIDは、互いに独立したセグメントとして運用する。

3.2.4.2 モード間のアクセス制御

3.2.1.1（5）のとおり設定するモード（領域）毎の通信について、学習系・校務系の異なるモード（領域）間の通信を制御すること。

3.2.4.3　アドレスレンジの定義

【希望要件】

以下の要件を満たすことが望ましい。満たさない場合には、代替案により同等以上の効果が得られる場合には加点評価の対象とする。

学習系・校務系それぞれに対し、識別可能なアドレスレンジを定義する。アドレスの付与はモードや隔離領域毎に独立して行う。

なお、校外系に関しては当該アドレスレンジの対象外とする。

3.2.4.4　インターネットへの接続について

学習系・校務系として定義されたアドレスレンジからの通信はSASE製品を経由し、各学校から直接インターネットに接続すること。

3.2.4.5　有線接続機器について

学習系・校務系の接続は基本的に無線アクセスポイントを介して実施する。有線接続については、校内の校務系物理スイッチに接続された所定の場所からの接続のみを許容する構成とし、その前提に基づいて校内ネットワークを設計すること。

3.3　一般事項

（1）　調達機器等は中古品でないものとする。

（2）　ネットワークのプロトコルはTCP/IPを基本とする。

（3）　本調達機器等のソフトウェアのバージョン確定にあたっては発注者と協議すること。また、バージョン確定後から、納入完成期限までにバージョンアップのあることが確認された場合には発注者の承諾を得た後、最新バージョンを導入するものとする。

　　本調達に係るサーバ、ネットワーク機器等の構成における脆弱性対策を実施すること。

（4）　本調達機器等及びその構成・配置については運用環境を考慮して、可能な限り最新の技術を採用すること。

（5）　本調達機器等は可能な限り省スペース設計、省電力設計であること。

（6）　ハードウェア及びソフトウェアは、製品の動作が保証又は確認されたものであること。

（7）　納入期限までに発見された本調達機器等の不具合については、受託者の責任と負担で迅速に対応すること。

（8）　各ハードウェアに搭載されるOS及び基本的なソフトウェアについて、納入期限までに指摘されている脆弱性の有無を確認し、これを当市に報告し、発注者と協議の上で納入期限までに修正モジュールの導入等適切な対策処理を施すこと。

（9）　各種災害（地震等）対策等を十分に考慮し、安全かつ信頼性のあるネットワークを構築すること。

(10)　将来におけるハードウェア・ソフトウェアの増強・ネットワークの拡大・接続機器の増設及び拡張のため、互換性・移植性・接続性を確保でき柔軟に対応できるよう標準化が考慮されていること。

(11)　本調達機器等は、機械的及び電気的に人体に危険がないものであること。

(12)　本調達機器等は、特に定めないものは、日本工業規格（JIS）又はそれと同等の規格に適合する品質優良なものを使用すること。
(13)　EIA 規格準拠 19 インチラックに搭載可能なこと。
(14)　メーカーにおいて、法人向け製品として製造・販売されていること。

４．保守要件

4.1　基本要件

（1） 保守体制を整備し、故障受付は電話（平日 9:00-17:00）及びメール（24 時間 365 日）等で受け付ける。
（2） 故障は切り分け後にオンサイトまたはリモートで修理・復旧を実施可能とする。
（3） 網側の死活監視を行うこと。
（4） 保守対象は本構築で設定した端末・機器とし既存設備の故障は範囲外とする。
（5） 運用期間の基本は5年とし、入札・契約・構築・移行・運用開始の工程を計画する。
（6） 故障受付件数について月次報告を行うこと。
（7） 庁舎内等の管理者の統合端末より、学校の統合端末を遠隔リモートサポートできることが望ましい。

4.2　ハードウェア保守

（1） 本契約で調達するハードウェアについて、契約期間内はメーカーによるハードウェア保守を受けることができること。
（2） 問い合わせ窓口を用意し、必要に応じてオンサイト保守要員を派遣し、対応すること。
（3） クラウドサービスで提供する各システムについて、保守サービスを提供する拠点からリモート操作ができる環境を用意すること。

５.プロジェクト管理

本業務に係るプロジェクト管理を適切に実施すること。

5.1　プロジェクト計画及び品質基準

受託者は、本書に基づき、システム構築等作業における具体的な体制、プロジェクト管理方針、プロジェクト管理方法等を含んだプロジェクト計画書を作成し、本業務に係るプロジェクト管理を適切に実施すること。
なお、プロジェクト管理における品質基準・要員スキル要件は以下のとおりとする。

図表１　品質基準

管理項目	管理内容
進捗管理	プロジェクト計画書策定時に定義したスケジュールに基づく進捗管理を実施する。進捗及び進捗管理に是正の必要がある場合は、その原因及び対応策を明らかにし、速やかに是正の計画を策定すること。

品質管理	プロジェクト計画書策定時に定義したシステム構築等作業の品質管理方針に基づく品質管理を実施すること。品質及び品質管理に是正の必要がある場合は、その原因と対応策を明らかにし、速やかに是正の計画を策定すること。
課題・リスク管理	リスクや障害が顕在化した場合は課題管理表にて管理すること。受託者は、リスクの発生を監視し、リスクが発生した場合には、当市に報告すること。
変更管理	仕様確定後に仕様変更の必要が生じた場合には、受託者は、その影響範囲及び対応に必要な工数等を識別した上で、変更管理ミーティングを開催し発注者と協議の上、対応方針を確定すること。

図表２　要員スキル要件

要求するスキル	スキルの詳細
プロジェクト管理能力を有する者	プロジェクト実施計画を策定し、システムの設計・開発、テスト、システムの評価、プロジェクト間の調整を行い、生産性及び品質の向上に資する管理能力を有すること。
品質管理能力を有する者	受託者の品質管理規準に従い、プロジェクトを離れて第三者的かつ客観的に、プロジェクト全般の品質状況を監査し、評価・改善する能力を有すること。
導入サービスに関する専門知識を有する者	導入するシステム等に関する専門知識と、本件の要求事項を理解した上で、最適なシステム構成の設計・構築・運用に係る技術及び技術コンサルティング能力を有すること。
システム導入業務に関する知識を有する者	本件のスコープに適合した各自治体業務に精通し、他自治体事例等を提供し、業務改善及びカスタマイズ抑制、品質向上に資する能力を有すること。

5.2 会議体運営

受託者は、定期報告の会議体として定例報告会を開催することする。会議の実施方法については、プロジェクト計画書に記載の上発注者の承認を得ること。

各会議の開催にあたっては、進捗報告書、課題管理表、変更管理票、スケジュール、会議録、その他必要と思われる報告資料等を準備すること。

5.3 ユーザー教育

システム利用者である教職員及びシステム管理者向けのユーザー教育を実施すること。ユーザー教育の実施方法については発注者と協議して決定すること。

5.4 試験設計・手順書

構築したシステムの試験を実施すること。試験計画、試験手順等は実施前までに作成し、発注者の承認を受けること。

６．成果物

成果物は他に指定のない限り、履行期間終了日までに発注者に提出し確認を受けることとし、PDF 形式及びMicrosoft Office 形式（Word、Excel、PowerPoint）の電子ファイルで提出する。

6.1　プロジェクト計画書

プロジェクト計画書及び作業計画書、作業工程表等を提出すること。

6.2　設計書

提案書や各種計画に基づき、本業務に係る設計資料を提出すること。

6.3　構成図

ハードウェア構成図、納入機器一覧、その他資料を提出すること。

6.4　試験設計・手順書

試験設計を行い、試験計画、試験手順、試験結果など各種ドキュメントを提出すること。

6.5　運用手順書等

運用者及び利用者に向けた各種手順書等を作成すること。

6.6　その他の成果物

その他、発注者との協議の上、必要と判断された成果物があれば、別途提出すること。

７．その他

7.1　貸与

機器の設定等に必要な資料等は、その都度貸与する。貸与品の管理保管は、不測の事態が生じないよう適正に管理しなければならない。

7.2　機密保護・個人情報保護

（1）　本業務の遂行上知り得た秘密を他に漏らしてはならない。この項については、契約期間の終了または解除後も同様とする。また、成果物（本業務の過程で得られた記録等を含む。）を発注者の許可なく第三者に閲覧、複写、貸与または譲渡してはならない。

（2）　本業務の遂行のために当市が提供した資料、データ等は業務以外の目的で使用しないこと。また、これらの資料、データ等は業務終了までに当市に返却すること。

（3）　本業務の実施における個人情報等の取扱いについては、個人情報の保護の重要性を十分認識し、個人の権利利益を侵害することのないよう必要な措置を講じること。

（4）　本業務に従事する者に対して個人情報保護の教育を行うこと。

7.3　不適合責任

（1）　本システムの本運用開始後１年の間に、正当な理由無く、本仕様書で要求した性能水準に達していないことが判明した場合及び設計ミスによる不良及び不具合が判明した場合において、発注者が改良を請求したときは、発注者と協議の上、無償で改良すること。なお、この場合、不具合の改良のために操作内容を変更しないこと。

（2）　本システムを運用する上で必要な情報の提供に努め、発注者からの障害発生時の情報開示請求などの問い合わせや助言要求に対して、誠意をもって対応すること。

（3）　受託者の責めに帰すべき理由により、第三者に損害を与えた場合、受託者がその損害を賠償すること。

7.4　契約期間終了時のデータの引継ぎ

（1）　契約期間終了時には、蓄積された全てのデータを発注者に無償で引き継ぐこと。データ形式はCSV形式を基本とし、詳細については別途協議する。

（2）　受託者は、引継ぎの完了を発注者が確認した後、すみやかに当該データの確実な消去を行い、発注者に報告すること。その際に発生する費用については、受託者にて負担すること。

7.5　その他特記事項・協議事項

発注者からのサービス改善要求に対して、協議の上、受注者が適正な要求と認められる場合は対応するものとし、本書に定めのない事項で疑義が生じた場合には、発注者と受注者が協議の上、受注者は発注者の指示に従い業務を遂行するものとする。

別紙　クラウド基盤構築基本要件

1. クラウドサービス基本要件	
1.1 サービス形態	1.IaaS（Infrastructure as a Service）及びPaaS（Platform as a Service）を提供可能なクラウドサービスであること 2.仮想マシン（VM）ベースのワークロードとコンテナベースのワークロードの両方に対応可能であること 3.従量課金制または予約インスタンスによる柔軟な課金体系を有すること
1.2 管理コンソール要件	1. Webベースの統合管理コンソールを提供すること 2. 管理コンソールへのアクセスは、当市のMicrosoft Entra IDによるシングルサインオン（SSO）認証に対応すること 3. 管理コンソールは日本語表示に対応すること 4. 管理操作の監査ログを取得・保存できること 5. APIによるリソース管理が可能であること。
1.3 テナント分離	1.他の利用者とは論理的に分離されたテナント環境を提供すること 2.テナント間でのデータ漏洩を防止する技術的措置が講じられていること
2. コンピューティング要件（IaaS）	
2.1 仮想マシン要件	1.以下のスペックの仮想マシンを提供可能であること ・vCPU：2～96コアの範囲で選択可能であること。 ・メモリ：8GB～384GBの範囲で選択可能であること。 ・ローカルストレージ：SSDに対応し、最大3,600GBまで利用可能であること。 ・ネットワーク帯域：最大35Gbps 2.Windows Server及びLinux（Red Hat Enterprise Linux、Ubuntu等）のオペレーティングシステムに対応すること 3.仮想マシンの起動・停止・再起動をオンデマンドで実行可能であること 4.仮想マシンのスケールアップ・スケールダウンが可能であること 5.仮想マシンイメージの作成・複製が可能であること 最大35Gbpsのネットワーク帯域を提供可能であること。
3. PaaS要件	
3.1 PaaSサービス	1.マネージドWebアプリケーションホスティングサービスを提供可能であること 2.サーバーレスコンピューティング機能を提供可能であること
4. ストレージ要件	
4.1 ブロックストレージ	1.仮想マシンに接続可能なマネージドディスクを提供すること 2.SSD及びHDDの選択が可能であること 3.ディスクの暗号化（保存時暗号化）に対応すること 4.スナップショットの取得が可能であること 5.以下の性能を提供可能であること ・Premium SSD：最大80,000 IOPS／スループット最大2,600 MB/秒 ・Standard SSD：最大 6,000 IOPS／スループット最大750 MB/秒 ・Standard HDD：最大 1,000 IOPS／スループット最大500 MB/秒
4.2 オブジェクトストレージ	1.大容量データの保存に適したオブジェクトストレージを提供すること 2.データの冗長化オプション（ローカル冗長、ゾーン冗長、地理冗長）を選択可能であること 3.アクセス層（ホット、クール、アーカイブ等）の設定が可能であること

	4.オブジェクトの暗号化（保存時暗号化）に対応すること 5.アクセスログの取得が可能であること 6.イミュータブル（不変）ストレージポリシーの設定が可能であること
4.3 ファイルストレージ	1.SMBプロトコルまたはNFSプロトコルによるファイル共有サービスを提供可能であること 2.Microsoft Entra IDによる認証・認可に対応すること
5. ネットワーク要件	
5.1 仮想ネットワーク	1.論理的に分離された仮想ネットワークを構築可能であること 2.サブネット分割が可能であること 3.ネットワークセキュリティグループによるトラフィック制御が可能であること 4.仮想ネットワーク間の接続（ピアリング）が可能であること
5.2 DNS	1.マネージドDNSサービスを提供すること 2.プライベートDNSゾーンの作成が可能であること
5.3 専用線接続	1.当市のオンプレミス環境との専用線接続（閉域網接続）に対応可能であること 2.VPN接続（サイト間VPN）に対応可能であること
5.4 ファイアウォール	1.マネージドファイアウォールサービスを提供可能であること 2.脅威インテリジェンスベースのフィルタリングに対応すること 3.侵入検知・防止機能（IDS/IPS）を有すること
6. Microsoft Entra ID認証要件	
6.1 基本認証要件	1. クラウド基盤の管理コンソールおよびAPIへのアクセスにおいて、当市のMicrosoft Entra IDテナントによる認証にネイティブ対応すること(外部IDプロバイダーとしての連携ではなく、クラウド基盤の認証基盤としてMicrosoft Entra IDを直接使用できること) 2. 当市のMicrosoft Entra IDで管理されるユーザーアカウント、グループ、サービスプリンシパルを、クラウド基盤のリソースに対する認証主体（セキュリティプリンシパル）として直接利用可能であること（IDの変換や同期を必要としないこと） 3. マネージドIDによるサービス間認証に対応すること（共有アクセスキーを使用しない認証方式） 4. クラウド基盤のリソースに対するアクセス許可を、Microsoft Entra IDのセキュリティプリンシパルに対して直接割り当て可能であること
6.2 認証の信頼性	1. Microsoft Entra IDとの認証連携において、トークンベースの認証を採用すること 2. セキュリティトークンの有効期限管理が可能であること 3. 認証失敗時のロックアウトポリシーを設定可能であること
7. クラウド管理コンソールへのシングルサインオン	
7.1 SSO要件	1. 当市のMicrosoft Entra IDによるシングルサインオンにより、クラウド基盤の管理コンソールにアクセス可能であること 2. 管理者が個別のクラウド基盤用アカウントを作成･管理する必要がないこと 3. Microsoft Entra IDのユーザーライフサイクル（作成、変更、削除）と自動的に同期されること
7.2 認証フロー	1. クラウド基盤の管理コンソールへのアクセス時に、Microsoft Entra IDの認証画面にリダイレクトされること 2. Microsoft Entra IDでの認証成功後、クラウド基盤の管理コンソールに自動的にログインされること 3. 既にMicrosoft 365等でMicrosoft Entra ID認証済みの場合は、再認証なしでアクセス可能

	であること
8. 多要素認証要件	
8.1 MFA連携	1. Microsoft Entra IDの多要素認証（MFA）と連携し、クラウド基盤へのアクセス時にMFAを要求可能であること
8.2 対応する認証方式	1. 以下の多要素認証方式に対応するMicrosoft Entra IDとの連携が可能であること Microsoft Authenticatorアプリ FIDO2セキュリティキー Windows Hello for Business SMS / 音声通話
9. セキュリティ認証・第三者認証	
9.1 必須認証	以下のセキュリティ認証を取得していること。 ・ISMAP：政府情報システムのためのセキュリティ評価制度（ISMAP）のクラウドサービスリストに登録されていること。 ・ISO/IEC 27001：情報セキュリティマネジメントシステム（ISMS）の国際規格認証を取得していること。 ・ISO/IEC 27017：クラウドサービスの情報セキュリティ管理策に関する国際規格認証を取得していること。 ・ISO/IEC 27018：パブリッククラウドにおける個人情報保護に関する国際規格認証を取得していること。 ・SOC 1／SOC 2：米国公認会計士協会（AICPA）のサービス組織統制報告書（SOC 1 または SOC 2）を取得していること。
9.2 推奨認証	以下の認証を取得していることが望ましい。 - CSA STAR認証 - ISO/IEC 27701（プライバシー情報マネジメント） - ISO 22301（事業継続マネジメント） - PCI DSS（ペイメントカード業界データセキュリティ基準）
10. データセンター要件	
10.1 所在地要件	1. 本基盤のプライマリデータセンターは、日本国内に所在すること 2. 災害復旧用のセカンダリデータセンターも日本国内に所在すること 3. データセンター間は地理的に離れた場所（異なるリージョン）に配置されていること
10.2 物理セキュリティ	1. データセンターへの入退室は、生体認証等による厳格なアクセス制御が実施されていること 2. 24時間365日の監視体制が敷かれていること 3. 耐震・免震構造を有すること 4. 冗長化された電源設備及び空調設備を有すること
10.3 データレジデンシー	1. 本基盤に保存されるすべてのデータ（顧客データ、メタデータ、ログデータ）は日本国内に保存されること 2. バックアップデータも日本国内に保存されること 3. データレジデンシーに関する設定を管理コンソールから確認可能であること
11. データ保護・暗号化要件	
11.1 保存時暗号化	1. すべての保存データは暗号化されること 2. AES-256ビット以上の暗号化アルゴリズムを使用すること

	3. 以下の暗号化オプションに対応すること - プラットフォーム管理キー（サービスマネージドキー） - カスタマー管理キー（顧客が管理するキー）
11. 2 通信時暗号化	1.クラウド基盤との通信はすべてTLS 1.2以上で暗号化されること 2.管理コンソール及びAPIへのアクセスはHTTPS必須であること 3.サービス間通信も暗号化されていること
12. 監査ログ要件	
12.1 監査ログ	1. 以下の操作に関する監査ログを取得可能であること - リソースの作成、更新、削除操作 - ロール割り当ての変更 - セキュリティ設定の変更 - 認証・認可イベント 2. 監査ログには以下の情報が含まれること - 操作日時（タイムスタンプ） - 操作内容 - 対象リソース - 操作結果（成功/失敗）
13. 性能要件	
13.1 コンピューティング性能	1. ワークロードに応じて適切なvCPU、メモリを選択可能であること 2. CPU使用率、メモリ使用率のリアルタイム監視が可能であること 3. 性能のボトルネック分析が可能であること
13. 2 ストレージ性能	1. 要件に応じたIOPS及びスループットを提供可能であること 2. ディスクIOの監視が可能であること 3. バースト性能に対応すること
13.3 ネットワーク性能	1. 仮想マシンタイプに応じた十分なネットワーク帯域を提供すること 2. ネットワーク遅延の監視が可能であること 3. 高速ネットワーク機能（アクセラレーテッドネットワーキング）に対応すること
14. 拡張性要件	
14.1 スケーラビリティ	1. 仮想マシンの垂直スケーリング（スケールアップ/スケールダウン）が可能であること 2. 仮想マシンの水平スケーリング（スケールアウト/スケールイン）が可能であること 3. ストレージ容量のオンライン拡張が可能であること
14.2 リソース制限	1. サブスクリプションあたりのリソース制限を明示すること 2. 制限の引き上げ申請が可能であること 3. リソース使用量の監視・アラート機能を有すること
15. バックアップ要件	
15.1 バックアップ要件	1. 仮想マシン全体のバックアップ（スナップショット）が可能であること 2. 以下のバックアップポリシーを設定可能であること ・バックアップ頻度 ： 日次以上 ／ 世代管理 ： 複数世代の管理が可能 3. バックアップの暗号化に対応すること 4. バックアップの整合性検証機能を有すること 5. バックアップデータは本番データとは別の場所（ゾーンまたはリージョン）に保存可能であること
15.2 リストア要件	1. 仮想マシン全体のリストアが可能であること

	2. プライマリリージョンのペアリージョンへのリストアが可能であること
16. 運用・保守要件	
16.1 クラウドサービス提供者のサポート	1. クラウドサービス提供者の上位サポートプラン（プロフェッショナルサポート相当以上）を契約すること 2. クラウドサービス提供者への問い合わせ代行を行うこと
16.2 インシデント対応	クラウドサービス提供時に、クラウドサービス提供者の起因で起こったインシデント事象に対して以下のとおり対応すること。 1. インシデント発生時は速やかに当市に報告すること 2. インシデントの影響範囲、原因、復旧見込みを報告すること 3. インシデント対応後は報告書を作成し、再発防止策を提示すること
16.3 重大インシデント	1. 以下を重大インシデントとして定義し、優先的に対応すること － サービス全体の停止 － セキュリティ侵害の疑い － データの喪失または漏洩