別紙1 機能要件・非機能要件一覧

□機能要件（設計要件）

基本設計・詳細設計に関する要件	項目	機能	要件
全般	全般	全般	本機能要件・非機能要件一覧に記載のない項目であっても、本市のネットワーク構築・運用に当たって必要となる機器・機能を備える設計を行うこと。
		設計方針	文部科学省策定の「GIGAスクール構想の下での校務DXについて」におけるゼロトラストセキュリティ対策に準じた設計であること。
		セキュリティ基準	文部科学省策定の「教育情報セキュリティポリシーに関するガイドライン（令和 6 年 1 月）」に基づく情報セキュリティ対策に対応できる設計であること。
教職員が利用する統合端末に対する要件	再設定	ー	移行中および本稼働後のネットワーク環境を利用するために必要な、端末の再設定内容について設計を行うこと。また、段階的に導入されている既存端末のリース期間にも留意した設計を実施すること。
	端末ポリシー	ー	移行中および本稼働後のネットワーク環境を利用するために必要な、端末に適用するポリシーについて設計を行うこと。
	端末管理	MDM機能	端末の紛失・盗難に遭った際は、ロックや初期化（ワイプ）、データの遠隔消去が可能な設計とすること。
			新規端末に対して、最初にログオンしたユーザーに応じたアプリケーションのインストールや設定の適用を、リモートで行う機能を有すること。（キッティング要件の設計に利用）
	資産管理（インベントリ/配布/ログ）	資産管理機能	仕様書に示す教職員ユーザー数に対応できる設計とすること。
			クライアント端末のハードウェア/ソフトウェア情報、レジストリ情報を取得できる設計とすること。
		ライセンス管理	アプリケーションのインストール状況及びライセンス管理が可能であり、ライセンスの過不足を容易に確認できる設計とすること。
		アプリケーション配布	ファイル配布、プログラム実行、レジストリ編集のタスク設定が可能であり、ネットワークへの負荷を考慮した分散配布ができる設計とすること。
		ログ収集機能	クライアント端末で起動しているプロセスの情報や、ファイル操作履歴の追跡ログを取得できる設計とすること。
		ログ保存期間	各種ログを最低1年以上保管できる設計とすること。（ストレージ容量のサイジングを行うこと）
		デバイス制御	特定の可搬記録媒体（USB、カメラ等）を除き、任意の媒体を接続できないように制御できる設計とすること。
			USBデバイス、FD/SDカード、CD/DVD/Blu-ray、共有フォルダ、ポータブルデバイス等の制御（書込み許可、読み込み専用、使用禁止）ができる設計とすること。
現教育ネットワークの機器に対する要件	拠点ルータ性能	外部インタフェース	今後更改を予定する拠点ルーターやその配下のスイッチに関しては、10GbE SFP+ポート数など柔軟性を考慮した設計とすること。
	認証機能	設計条件	現行のLDAPサーバーの構成情報や児童生徒も利用している既設GWS基盤にも留意した設計とすること。
		アクセス制御	職員は自身に紐づく組織や役割に応じた権限が付与され、権限に応じた業務システムやファイルサーバなどにアクセスできる設計を行うこと。
		構成管理	複数のグループポリシーを管理し、出来るだけシンプルな設計を行うこと。
		拡張性	将来、教職員人数の増加に対応できる拡張性がある設計であること。

	共有ストレージ	容量	共有ストレージの共有領域は将来的な拡張領域、一部教職員の使いすぎにも留意しながら500TB程度を前提とした設計を実施すること。
		性能	仕様書に示す教職員アカウント数に対応できること。
		セキュリティ	組織単位、個人単位でファイルの閲覧共有・閲覧制限を行える設計であること。
		信頼性	職員が誤削除したファイルを復旧できること。
		運用・保守・管理	システム管理者は、フォルダー単位で使用できる容量の制限を設けることができる設計であること。
学校内のネットワーク機器に対する要件	フロアスイッチ	外部インタフェース	既存機器に対して、10GbE SFPポート数など、５年以上の利用を想定した柔軟性、拡張性を考慮した設計とすること。
		性能	児童生徒が授業等やMEXCBT等で一斉利用することも想定した設計を実施すること。
			タグVLAN、ACL（アクセス制御リスト）による通信制御に対応した機器を前提とした設計を行うこと。
		運用・保守・管理	機器の設定/状態管理をリモートで管理可能な設計を行うこと。
	無線LAN	性能	児童生徒が授業等やMEXCBTで利用することも想定した設計を実施すること。設計するネットワーク環境に対応させるために必要となる設定内容について設計を行うこと。
		災害用統一SSID「00000JAPAN」	専門の知識を有しない市職員であっても、災害用統一SSID「00000JAPAN」の発動・停波を行うことができる手順の設計をすること。
		運用・保守・管理	今回の構成にあたり既設APへの設定変更が必要になる為、運用・保守・管理においてもそれを想定し設計すること。
クラウドサービスに関する要件	全般	全般	サービス提供POPとログ保存先が日本国内に選択できる設計とすること。
		通信経路暗号化	端末とクラウドサービス間での通信経路の暗号化により、第三者による通信内容の盗み見を防止できる設計とすること。
	統合ID管理	統合ID管理	既存システムの運用を十分に理解した上で教職員の負担が軽減できる設計を実施すること。各種システム・サービスやクラウドサービスに対して共通のIDでアクセスできる構成が可能な設計であること。なお、既存システムには、Google workspace、学習eポータル、校務支援システム等が含まれる。
		IDワークフロー	既存システムの運用を踏まえ、本市が利用しているサービスやシステムのID連携に向けたワークフロー等の運用を設計すること。
	認証	リスクベース認証	匿名IPからのアクセスや、複数回のログイン失敗等不正アクセスの疑いがある事象を検知し、多要素認証を要求する等の自動対処機能を有する設計とすること。
			定期的なパスワード変更をしなくてもよい運用を実現できる設計とすること。
			端末のIPアドレスや位置情報、アクセス時間が通常と異なる等のリスクを判定し、追加の認証を求めることができる設計とすること。
		端末アクセス制御	管理者が認めた端末のみネットワークに接続できる設計とすること。
	EDR機能	EDR	未知のウイルスの検知を行うことや、端末のふるまい検知、脅威の侵入経路のトラッキングが行える設計とすること。

	ファイル暗号化・アクセス制御機能	アクセス制御	情報の閲覧・編集制限（アクセス権限制御）ができる設計とすること。
		ファイル暗号化	ファイルを端末やクラウドストレージに保存する際、Officeファイル及びOfficeファイル以外の文書ファイル（PDF等）の暗号化が可能な設計であること。暗号化されたファイルは、万が一漏洩したとしても外部の人間がアクセスできない設計とすること。
	メール/スケジュール	メール	インターネットメールに対応し、仕様書に示す教職員ユーザー数に対応できる設計とすること。
		メールセキュリティ強化	既知のスパム/マルウェアを検知し添付ファイルを削除できることや、未知のマルウェアを含む添付ファイルやハイパーリンク等、未知の攻撃を検知・ブロックできる設計とすること。
			メール本文に機密情報を含んでいないかチェックし、含んでいる場合にブロックもしくは警告後に理由入力させてから送信するなど、機密情報漏洩の対策ができる設計とすること。
			メール送信時に宛先、本文、添付ファイル、特定キーワード等を送信者自身がチェック後、メールを送信することが可能な設計とすること。（送信保留機能を有する設計とすること。）
		アドレス帳	学校/組織ごとのアドレスをまとめたカスタムアドレス帳を作成でき、更新を含めた運用設計を実施すること
		スケジュール管理	組織及び個人単位でスケジュールの登録が行え、メールと連携する機能を有する設計とすること。
	大容量ファイル転送	ファイル転送	メールサービスの送信制限を超えた場合に備え、大容量のファイル（2GBまで）を送付できる仕組みを提供する設計とすること。
	チャット/Web会議	チャット	個人単位のチャット機能、添付ファイルの投稿、通知機能を有し、管理者が容量の上限設定やチーム作成権限の制限ができる設計とすること。
		Web会議	映像かつ音声による1,000人以上の同時利用が可能な設計とすること。 （ネットワーク帯域に配慮した設計を行うこと）
	ゼロトラストソリューション	全般	アンチウイルス機能、DNSフィルタリング、SSLインスペクション、WEBフィルタリングなど、各種セキュリティ機能がエンドポイントに提供できる設計とすること。
		アクセス制御	校務支援システムやファイルサーバ等の校内アプリケーションに対していわゆるゼロトラストアクセスを有する設計とすること。なお、校務支援システムはR11年度からクラウド運用を行い、それまでは現環境への安全なアクセスを可能にする設計を行うこと。また、将来的な行政系サービスへの接続も留意した設計を実施すること。
		接続要件	ゼロトラストソリューションに常時接続になる機能があるよう設計すること（ロケーションフリー）。
			自宅の回線でも学校教育ネットワーク環境にアクセスできる設計とすること。
			学校外からアクセスするとき、職位・組織単位でアクセス可能な範囲を制御できる設計とすること。
		アンチウイルス	シグネチャベースのマルウェア対策が可能な設計とすること。
		運用管理	端末からネットワーク経路の通信状況と各種サービスまでのネットワークおよびアプリケーションのパフォーマンスを可視化できる設計とすること。
		SSLデコード	SSL(HTTPS）通信を解析・制御可能であり、復号化に上限がない設計とすること。
	その他	ログ管理	ユーザーのアクセスログ及び管理者の操作ログについて、契約期間中の保持が可能なこと。また、管理者画面から確認できる設計とすること。

□**非機能要件（設計要件）**

非機能要件	項目	機能	要件
非機能要件	可用性要件	冗長構成	冗長構成を考慮した設計とすること
	セキュリティ	ー	学校内/学校外問わず一貫したレベルのセキュリティが提供できる設計とすること。
	認証取得	認証取得	校正する機器・ソフトウェア等が、ISO27001、ISO27017、ISO/IEC27018などの世界標準のセキュリティ認証を取得していることを前提にした設計とすること。