宗像市教育情報ネットワーク整備事業

仕様書

宗像市　教育総務課

事業概要

1.1 事業名

宗像市教育情報ネットワーク整備事業

1.2 背景・目的

国は、GIGAスクール構想の下、種々の教育データを総合的に可視化し、学校経営・学習指導の高度化を図ることを将来に見据え、校務系・学習系ネットワークの統合やクラウドを活用した校務処理等により効率化を図り、教職員の働きやすさと教育活動の一層の高度化を目指す次世代の校務DXを推進している。

そのためには、校務処理に対する抜本的な改善が必要である。校務の効率化に大きく寄与してきた従来の校務支援システムは、多くの自治体でシステムを自前サーバに構築し、閉鎖網で稼働させており、校務用端末も職員室に固定されている。これらの仕組みは従前の政府全体のセキュリティ対策を踏まえたものであったが、1人1台端末の整備とクラウド活用を核とするGIGAスクール時代の教育DXや働き方改革の流れに適合しなくなっており、本市も例外ではない。

本市は令和８年度に次世代の校務 DX が実現できる統合型校務支援システム（以下「校務支援システム」という。）への切り替えを予定している。それを踏まえ、本事業でクラウドサービスの利活用を前提としたネットワーク構成及びそれに伴うアクセス制御による対策を講じたシステム構成（ゼロトラスト環境）を構築することで、教職員 PC1 台化、サーバのクラウド化及び一元管理、学校間ネットワークを実現し、教員同士の情報共有を活性化させるとともに教育の質向上に繋げることを目的とする。

対象範囲

2.1 本事業の範囲

以下に、本事業範囲を記載する。

項目		説明
ゼロトラスト型システム基盤		
	ID 統制	ID 管理基盤、多要素認証、SSO、アクセスコントロール等
	デバイス統制・保護	機能制限、紛失時対応、リモートアクセス、ポリシー等一斉配布、Windows Update 等一斉管理、IDaaS との連携等
	EPP	マルウェア検知・遮断等
	EDR	SOC 等による監視機能、攻撃後の対応、IDaaS との連携等

	ネットワークセキュリティ	アプリケーション単位の接続制御、IDaaS との連携、通信経路の暗号化、悪性な WEB コンテンツへのアクセス制限（フィルタリング）、WEB 経由データのマルウェア検出、シャドーIT の制限、テナント識別等
	データ漏えい防止	機密ファイルやメールの暗号化及びアクセス制御等
	ログの収集・分析	指導者用端末のログ収集、可視化
	クラウドストレージ及びバックアップ構築	機密性の高いデータの保存場所と想定しており、業務継続性を確保するために迅速なデータ復旧が行えるよう、別途随時バックアップを取得する構成とすること。
ネットワーク統合		
	ネットワーク統合	新指導者用端末は、GIGA 系ネットワークに接続する。新指導者用端末から既存プリンタへの印刷を許可するための、ネットワーク機器（ルータ等）への配線等を実施することとする。
	無線アクセスポイント	無線アクセスポイントの調達、設定、設置
	バックアップ用 NAS	バックアップ用 NAS の調達、設置
指導者用端末キッティング及び保守		
	指導者用端末のキッティング及び搬入設置	新指導者用端末の初期設定、キッティング、設置・移行に係る対応、再利用端末の再設定
	既存校務用端末の回収・廃棄	令和 8 年 3 月下旬を目途に既存校務用端末の回収と廃棄。
	指導者用端末の保守	ハードウェア等の保守（一次切り分け、障害対応）
	新指導者用端末は別業務にて調達を行う。納期：令和 7 年 11 月末	

なお、校務支援システムについては、ふくおか電子自治体共同運営協議会が導入決定した統合型校務支援システムを令和 8 年 4 月から利用予定である。

2.2　整備後の運用

ゼロトラスト型システム基盤について、令和 12 年 3 月 31 日までの期間、ライセンス使用及び運用保守を継続する前提で整備を行うこととし、令和 8 年度からは教育情報ネットワーク運用保守業務委託として単年度の契約を想定している。

なお、令和 8 年度については、同業務委託の中で新任の教職員を対象にシステムの運用研修を 4 月に 1 回程度行うものとする。

システム構成

3.1 本事業の考え方

本事業においては下記の項目を重視する。

①校務系の ID 管理の一元化

②学校外での業務を見越したクラウドサービス基盤による利便性の向上

③情報漏えい防止のためのデータ管理・制御

④ディレクトリサービスによるユーザー保守・管理負担の軽減

・本市では、Microsoft 365 が持つサービス及び機能を活用することを想定しているが、別ソリューションの提案を行う場合は、後述する要件を満たすソリューションであると共に、有効性・コスト・運用面のメリットについて提案をすること。

・要求機能に掲げる事項のみを実現すればよいのではなく、全体が機能するために当然実現しなければならない機能・作業も含まれるものとし、高価・複雑・不安定よりも安価・シンプル・頑丈なシステムの構築を目指すこと。

・最新あるいは今後リリース予定のサーバ OS、クライアント OS、ブラウザのバージョンにも対応できるよう考慮されたものとすること。

・クライアントは DHCP での運用を基本とする。

・セットアップ等の作業場所は受注者側で確保すること。ただし、システム基盤構築作業の接続を要するものについては、作業場所を協議の上で決定することとする。その場合において、発注者側で大規模な作業場所を確保することは困難なため、留意の上で見積及び作業を行うこと。

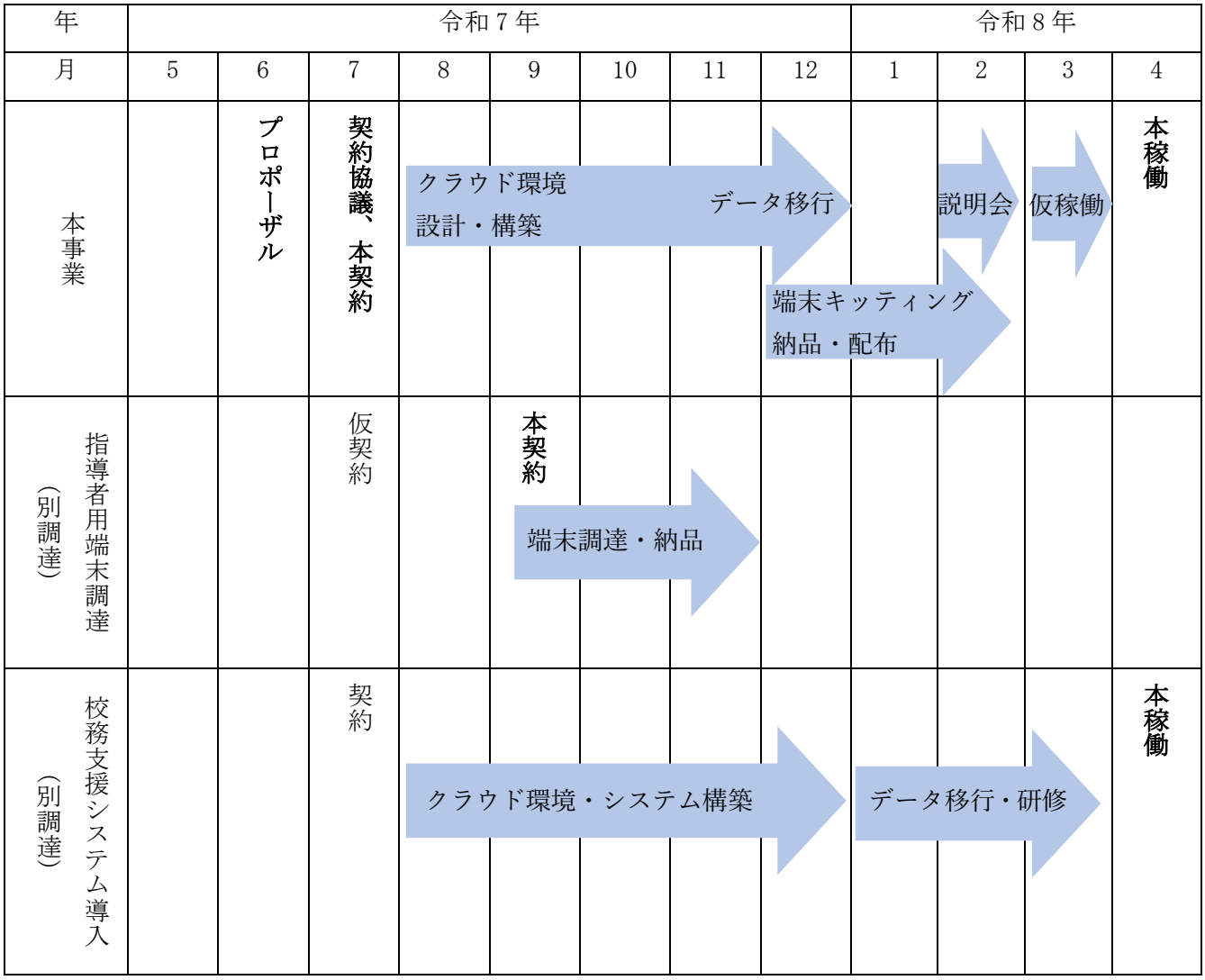
・今回構築する環境に切り替える際、既存環境を長期間停止することは業務への支障が大きいため、停止期間等の影響が最小限となるよう考慮すること。

・令和 8 年 3 月から校務支援システムの仮稼働、及び令和 8 年 4 月から校務支援システムの本稼働を開始できるよう各種の構築を行うこととする。

3.2 履行期間

履行期間は契約締結日の翌日から令和 8 年 3 月 31 日まで。

予定スケジュールは以下の通りとする。



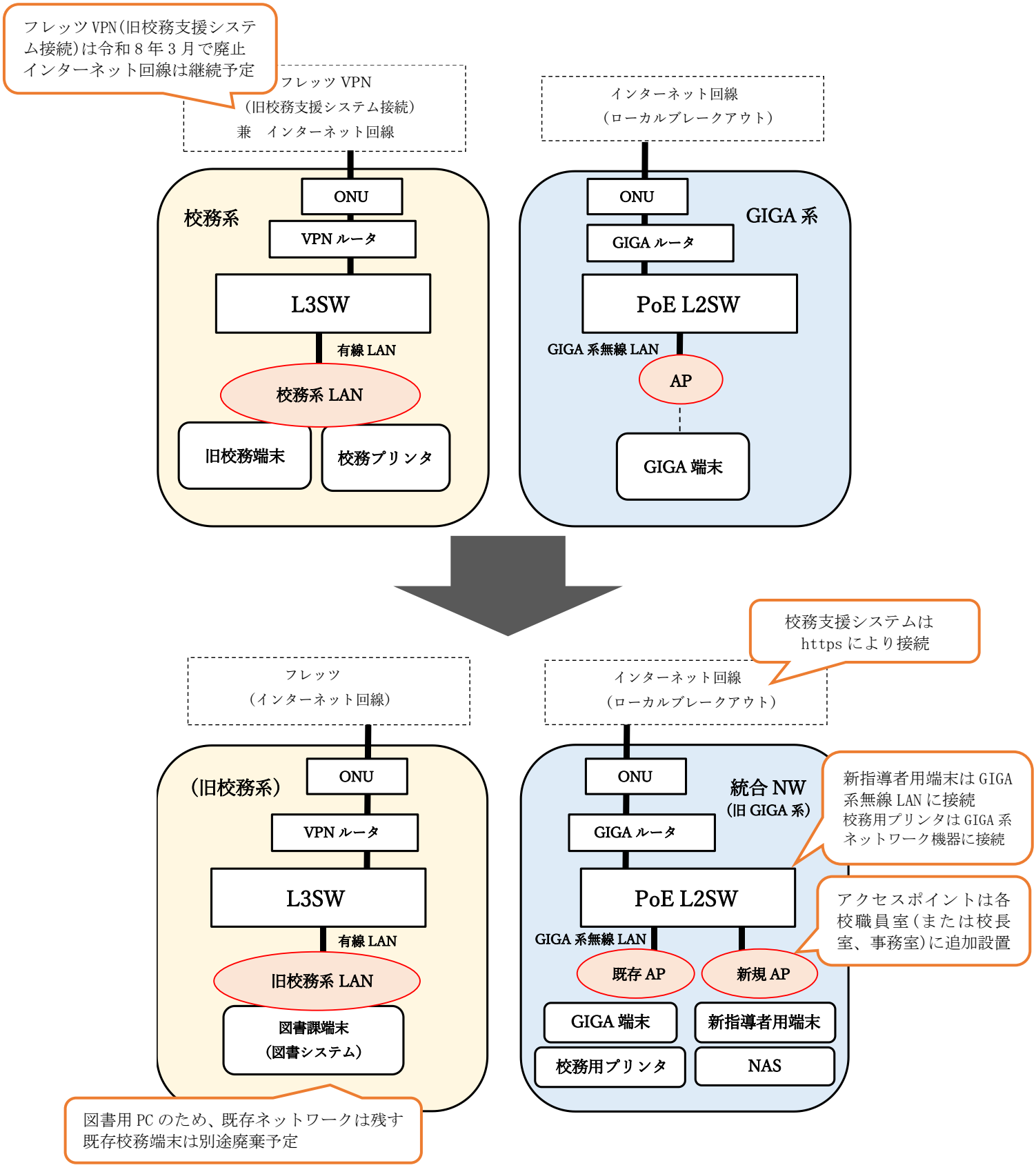
3.3 履行場所

宗像市内の小・中・義務教育学校全 21 校及び宗像市役所を対象とする。

履行場所の所在地については、「別紙 1　履行場所一覧」を参照のこと。

3.3 ネットワーク構成

ネットワーク構成は校務系・GIGA 系（学習系）に物理的分離しており、本事業を経て、GIGA 系（学習系）に統合を予定している。



システム基盤の機能要件

本システムは新規契約予定の Microsoft365 テナント上に構築することを想定している。

Microsoft365 A3 又は A5 の 780 ライセンス調達を必須とし、これに含まれる諸機能を主として構築すること。構築に係る設定内容については、発注者との協議により適宜決定することとし、必要な情報は発注者の求めに応じて、随時提供すること。

4.1 ゼロトラスト型システム基盤要件

4.1.1 認証基盤

当システムについては、「Microsoft Entra ID」を利用することを想定している。なお、以下の要件を満たす同等の代替サービスによる提案も可とする。

・サービスを利用するためにサーバの設置や Agent インストールを必要とせず、Windows、Mac、iOS、Android 等様々な OS に対応し、特定のデバイスに依存しない認証サービスを利用できること。
なお、Authenticator など認証アプリケーションのインストールは可能とする。

・主要な機能をブラウザで管理できること。また、特殊な機能の設定や一括処理をする際には PowerShell や API を使ったプログラム等からの管理ができること。

・今回調達する指導者用端末及び再利用端末について、校務支援システムにアクセスできるよう構築を行うこと。

・ユーザー、ユーザーの所属するグループ、接続元ネットワークの IP アドレスや、接続するデバイスの状態に応じてサービス利用ができるように構築を行うこと。

・パスワードのリセットや再発行等のアカウント管理手法について具体的な提案を行うこと。

・管理者は利用者の認証アクセス状況をレポートとして確認することができるとともに、外部からの不正アクセスの疑いのある事象についての対処方法、アカウントのセキュリティ対策についても具体的な提案を行うこと。

・校務支援システムへの認証・ 連携を考慮に入れた設計構築を行うこと。接続方式 https 接続を想定している。また、校務支援システムの Web アプリケーションに対して、外部からの安全なリモートアクセスを可能とするための機能を有していること。

・人事異動・組織改変に対して、柔軟かつ簡単に対応できるよう考慮すること。

・業務にて利用するサービスとのユーザー情報連携が可能であること。

4.1.2 メールシステム

当システムについては、「Exchange Online」を利用することを想定している。なお、以下の要件を満たす同等の代替サービスによる提案も可とする。

（1）メールシステム

・構築するネットワークの内外に対してメールの送受信が行えること。

・現行利用しているメールアドレス、ドメインを新環境でも利用できること。

・個人のメールアドレスとは別に学校代表アカウント、共有メールアドレスの設定を行えるようにすること。

（2）メールセキュリティ対策機能

・メールによる標的型攻撃等の高度な脅威からの保護を目的として、危険な添付ファイルに対する対策と、悪意のあるリンクに対する保護を実施できること。

・ゼロデイ攻撃等未知の攻撃手法に対しても可能な限り添付ファイルの安全性を検証するため、サンドボックス環境等により動的解析を実施したうえで受信できる機能を有すること。

・既知の攻撃に対してはメールボックスに届く前に安全性を精査すること。また、ゼロデイ攻撃等未知の攻撃に対しては端末の EDR 等により添付ファイルの安全性を分析する機能を有すること。

・メール本文中の URL やハイパーリンクについて、リンク先の安全性についてチェックできること。また、当該リンク先がファイルであった場合は、添付ファイルと同様にサンドボックスでスキャンできること。

・メール本文中の URL やハイパーリンクについて、不審なものである場合、利用者がクリックした際に適切な処置ができること。

・脅威を検知したメールの状況・統計情報・アクション(配送、隔離、削除等)等が確認できること。

4.1.3 ファイル共有システム

当システムについては、「Share Point Online」を利用することを想定している。なお、以下の要件を満たす同等の代替サービスによる提案も可とする。

・共同作業や情報を共有する利用者を指定したチームを作成でき、チーム内限定のビジネスチャットやファイル共有等が行えること。

・チーム内に目的に応じたチャネルを作成でき、ビジネスチャットやファイル共有を整理して行えること。

・「ファイル共有・管理」サービスと連携し、ファイルの共有や Office ファイルの共同編集機能を提供すること。

・ファイルのアップロードやダウンロード、閲覧、編集において可能な限り統合コミュニケーションサービスのアプリケーション内で操作が完結すること。

・認証基盤に登録されたユーザー及びグループ毎にセキュリティ、アクセス権等が設定できること。

・後述するセキュリティ要件を満たすよう、アカウント属性に対応したラベル設定に応じて、各ファイルの暗号化が可能であること。
・ファイル共有システム内で、削除、紛失、破損等のよる要因で使用できなくなったファイルを復元する機能を有すること。
・現行のファイルサーバ資産をファイル共有システムへ移行すること。
・(現行ファイルサーバ資産容量：各校約 2TB 程度) ファイルサーバ資産移行に際し、移行タイミングにおける利用者の負担を極力軽減するように努めること。 (ダウンタイムが発生しないようにファイル共有システムへの移行を行えるよう提案すること)
・ファイル共有システム内のフォルダ構成は発注者が指示する各校統一した構成とすること。
・データ移行の方法については契約後、別途協議のうえ決定すること。

4.1.4 グループウェア

・PC より、電子メール、チャット、音声、動画、資料共有等を用いたコミュニケーション機能を提供すること。なお、音声通話機能、ビジネスチャット機能及び Web 会議機能を、原則として単一のツールにより提供すること。
・外部関係者とのコミュニケーションにも使用できること。
・外部関係者とのやりとりについてはセキュリティに配慮した設計を行うこと。
・任意の複数の利用者とテキストメッセージ（チャット等)、音声、ビデオ、ファイル及び画面共有を用いたリアルタイムの会議（以下 Web 会議）ができること。
・専用クライアントアプリケーション以外に、ブラウザーベースのクライアントで主要機能が利用できること。
・共有されたファイルに対し、複数メンバーでのリアルタイム同時編集が可能であること。
・管理者によって保持ポリシーを設定でき、一定期間保持する、一定期間経過後削除するといった制御が可能なこと。

4.1.5 EPP 及び EDR

・Windows 11 に対する侵入検知などのログ情報を収集し、世界中のセキュリティインシデントデータと照らし合わせることにより異常な挙動や攻撃者の手法を検出し管理ポータルから一元的に管理、確認可能であること。
・端末のふるまいを検知して脅威の検出を行うこと。
・各端末の脆弱性情報を確認することができること。
・検出した脅威を可能な限りリモートで除去することができること。

・脅威が検出された端末を管理ポータルの操作により遠隔でネットワークから隔離できること。
・脅威の侵入経路などのトラッキングが行えること。
・定期的に最新のセキュリティ状態に更新がされること。

4.1.6 資産管理システム

当システムについては、Microsoft 365 に含まれる MDM「Microsoft Intune」を資産管理システムとして利用することを想定している。なお、これに付随した以下の要件を満たすサービスの提案も可とする。

・OS として、Windows、iOS、Android を使用するデバイスについて各デバイスの設定を強制する機能を有すること。
・OS として、Windows、iOS、Android を使用するデバイスについてデバイスを初期化することができること。
・MDM にデバイス登録することで、登録済みデバイスのみアクセスを許可する設定ができること。
・Windows 機能更新プログラムのバージョン固定等の更新プログラム管理ができること。
・管理画面から、ログの閲覧、資産情報の閲覧、USB メモリの管理、ポリシーの適用、ソフトウェア配布等が可能なこと。
・各クライアントコンピューターに関する各種ハードウェア情報を、資産情報として自動的に収集できること。
・収集したハードウェア及びソフトウェア情報を、一覧で表示できること。
・指定したクライアントコンピューターに対して、任意のプログラムを配布し、自動的にプログラムのインストール及びアンインストールを行う機能を有すること。
・配布したソフトウェアの配布状況及びインストール状況を確認することができること。配布したソフトウェアのインストール / アンインストールが失敗した場合は、失敗したクライアントコンピューターを指定して再実行が行えること。
・クライアントコンピューターがソフトウェアの配布を受ける際、すでに同一のセグメント内のクライアントコンピューターに配布されたソフトウェアがキャッシュとして残っている場合、そのクライアントコンピューター（以下キャッシュ端末と呼ぶ）からソフトウェアを配布できること。
・4GB 以上のサイズのソフトウェアをキャッシュ配布で配布できること。
・指定したクライアントコンピューターに対して、Windows 更新プログラムを配布し、自動的に更新プログラムの実行を行う等のセキュリティパッチを適用する機能を有すること。
・配布した Windows 更新プログラムが適用されていないクライアントコンピューターを検出し、一覧化できること。

・クライアントコンピューター上で印刷が実行された際に、その印刷されたドキュメント名、1 回の印刷枚数、ファイルパスなどをログとして記録できること。
・クライアントコンピューターから One Drive へのアップロード及びダウンロード操作に対して、ログを収集できること。
・また、アップロード元及びダウンロード先ファイルのフルパスを記録できること。
・ルールに反した操作をしたクライアントコンピューターの利用者に注意を促すため、メッセージの内容はルール違反の操作ごとに設定できること。
・指定したアプリケーションの実行を検知及び禁止できること。
・クライアントコンピューター上での、Web サイトの閲覧や Web サイトからのファイルダウンロード／アップロード操作を検知及び禁止できること。ただし、フィルタリング等の他製品で仕様を満たすことも可とする。
・Web サイトの閲覧や Web サイトからのファイルアップロードを禁止する際は、キーワードや URL で禁止サイトを設定できること。
・特定の URL からのダウンロードを禁止から除外するよう、設定できること。ただし、フィルタリング等の他製品で仕様を満たすことも可とする。
・USB デバイス台帳に登録されたデバイス情報を基に、その USB デバイスの使用許可/不許可などを設定できること。
・許可した USB デバイスのみを使用可能としそれ以外の使用を禁止できるような運用が可能であること。
・個々の USB デバイスに使用可能/読み取り専用/使用不可能を設定できること。
・デバイス種別ごとに、一括で使用可能/読み取り専用/使用不可能の設定ができること。
・設定ができるデバイスの種類は以下の通りとする。
・デバイス種類（USB メモリ、USB ハードディスク、CD/DVD ドライブ、Blu-ray ドライブ、デジタルカメラ、モバイル端末、USB デバイスや CD/DVD/Blu-ray ドライブなどの記憶媒体）を、クライアントコンピューターに接続及び書き込みを行った場合に検知及び禁止ができること。

4.1.7 フィルタリング

・安全な Web サイトにのみアクセスできるホワイト運用又はブラックリスト運用が可能な DB を搭載していること。
・ファイルの拡張子をリスク別にダウンロード制限が可能であり、Web サイトにアクセスしただけでマルウェアに感染してしまう攻撃の対策ができること。
・なお、OS やアプリケーションのアップデートなどに利用されるサイトのダウンロードは許可でき、利便性を損なわずにセキュリティを担保できること。

・フィルタリング設定のテンプレートが用意されていること。また、日本の組織に応じたグループ・ユーザー管理ができそれを基にフィルタリングルールの設定ができること。
・国内で販売されている製品で、日本語によるサポート対応が可能であること
・レポート機能が無償で付属されており、外部 DB を用意せず利用可能なこと。
・グループごとに有効期間が指定でき、特定日以降フィルタリング開始とするグループ事前設定や、複数のユーザー及びグループを対象にする柔軟なポリシー作成が可能なこと。また、ユーザーの Web 利用のフィルタリング機能の時間制限ができること。
・脅威情報への通信が発生した際に、管理者にメール通知が可能なこと。
・脅威情報サイトへのアクセス情報（アクセスの発生日時、該当ユーザー、該当端末、適切な対処方法）に関するレポートを管理者にて確認することが可能なこと。

4.1.8 多要素認証

当システムについては、「Windows Hello」を利用することを想定している。 なお、以下の要件を満たす同等の代替サービスによる提案も可とする。

・ログイン方法は Windows ログオンによるものとし、顔認証、PIN コードによる二要素認証に対応していること。
・前述の認証基盤と連携することとし、認証基盤の登録情報を元に認証するものとする。
・ネットワーク障害によりクライアントがネットワークから切り離された場合、キャッシュ等により一定期間内はクライアントにログインできること。
・生体情報の読み込みが正常にできない場合に、他の方法を用いてログインが可能なこと。

システム基盤の非機能要件

5.1 規模・性能要件

利用者数・データ量に応じた、経済的かつ高パフォーマンスなシステム導入のため、規模・性能要件は、次のとおりとする。

本システムを利用する端末は、次のとおりである。サーバ機器及びサービスの選定では、これを踏まえて、快適な使用環境が実現されるよう最適な機器・サービスのサイジングを行うこと。

＜規模について＞

指導者用端末	・指導者用端末 … 780 台(うち、750 台を新規調達し、30 台は既存端末を再利用する) ※端末の仕様に関しては指導者用端末の仕様（参考）を参照すること。

5.2 セキュリティ要件

5.2.1 教育情報セキュリティポリシーに関するガイドラインへの準拠

・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。）（令和７年３月文部科学省）に準拠すること。

5.2.2 認証とアクセス制御

・指導者用端末と Microsoft 365 サービスのシングルサインオンを行うこと。

・端末へのサインインについては、2 要素以上の多要素認証を行うこと。

・テレワーク等で外部から校務支援システムへアクセスする場合は、指導者用端末からの接続のみ許可するようにアクセス制御を行うこと。

・テレワークの際にはモバイルデバイス等を使った多要素認証が可能であること。本要件については必須とはしないが、導入時の設計・テストにおいて利便性を考慮した上で採用を検討すること。

・校務支援システムに接続する際には、Microsoft365 で認証された特定の端末及び特定のユーザーからのみの接続を許可すること。

5.2.3 情報漏えい対策

・教職員が新規作成・編集したファイルは教職員しか閲覧することができない機密ラベルを付与すること。

・教職員が新規作成・編集時に付与する機密ラベルのレベルの変更（役職に応じた閲覧・編集範囲の制限など）が可能で、レベルの詳細については設計にて定義すること。

・メールの誤送信があった場合でもアクセス権のない者が閲覧できないように対策できること。

5.2.4 ログの保管

・以下に記載するログ管理を行えるように構築すること。

Microsoft 365 サービスのアクティビティログ

- Entra ID のサインインログ
- Entra ID の監査ログ

・ログはクラウド上で統合管理し、脅威の分析・可視化を可能とすること。

・認証基盤と連携して管理ポータルへのアクセス制御を行うこと。

・クライアントコンピューターに対して行われた操作、ログオン・ログオフの日時、ファイル操作、Web へのアクセス及びアップロード・ダウンロード、USB メモリなどの記憶媒体を利用した内容、記憶媒体のシリアル情報等をログとして記録する機能を有すること。

・Web サイトの閲覧が行われた内容について、ウインドウタイトル、URL をログとして記録できること。また、Web ダウンロード及び Web サイトへの書き込みが行われた内容について、URL、書き込み内容などをログとして記録できること。尚、以下のブラウザに対応していること。

Google Chrome、Microsoft Edge（Chromium 版）、Firefox

・クライアントコンピューター内の蓄積されたログ（一時的なログを含む）については、暗号化等により保護され、クライアントコンピューター利用者はログの内容を確認できない機能を有すること。

5.2.5 セキュリティソフト・セキュリティパッチの要件

・Windows の指導者用端末に対しては、品質更新プログラムを随時配信すること。なお、意図していないタイミングで配信されないよう、予めスケジュールの設定が可能であること。

・Windows の機能更新プログラムについては、バージョン固定等が可能であること。

・機能更新を行う場合は事前にテスト端末等で更新後の挙動を確認した上で配信を行うこと。

・指導者用端末に関してはユーザー操作により更新処理を実行できるようにすること。なお、テレワーク時でも更新が可能となるよう可能な限りインターネット経由で配信すること。

・指導者用端末の更新プログラムの適用状況を確認できる仕組みを構築すること。

ハードウェアの設置台数及び機能要件

6.1.1 設置台数一覧

設置校及び設置台数については以下を想定しているが、詳細は発注者と協議の上、決定する。

No	名 称	無線アクセスポイント	NAS	指導者用端末
1	吉武小学校	2	1	20
2	赤間小学校	2	1	60
3	赤間西小学校	2	1	35
4	日の里東小学校	2	1	31
5	日の里西小学校	2	1	36
6	河東小学校	2	1	51
7	河東西小学校	2	1	51
8	南郷小学校	2	1	29
9	東郷小学校	2	1	49
10	自由ヶ丘小学校	2	1	45
11	自由ヶ丘南小学校	2	1	25
12	玄海小学校	2	1	19
13	玄海東小学校	2	1	20
14	地島小学校	0	1	10
15	城山中学校	2	1	56
16	日の里中学校	2	1	32
17	河東中学校	2	1	50
18	中央中学校	2	1	42
19	自由ヶ丘中学校	2	1	37
20	玄海中学校	2	1	21
21	大島学園（義務教育学校）	1	1	26
22	宗像市教育委員会	0	0	35
合計		39	21	780

6.1.2 ハードウェア仕様

無線アクセスポイントの仕様

メーカー	仕様	特記事項
Cisco Systems	Cisco Meraki MR36 無線アクセスポイント クラウド管理型　型番：MR36-HW	
Cisco Systems	Cisco Meraki MR アクセスポイント用 共通ライセンス 5 年　型番： LIC-ENT-5YR	

NAS の仕様

メーカー	仕様	特記事項
BUFFALO	LinkStation 2.5GbE 搭載　高速モデル　1 ベイ 4TB　型番：LS710D0401	

指導者用端末の仕様（参考）

項目	仕様	特記事項
形状	ノートブック型	
OS	Windows11 Pro	
CPU	インテル®　CoreTMi5-1340P プロセッサー以上	
メインメモリ	16GB 以上	
SSD	256GB（PCIe、NVMe 対応）以上	
ディスプレイ	13.3 型～14.0 型　タッチパネル式（静電容量式／マルチタッチ対応）	
マウス	光学式マウス（有線）	
解像度	1,920×1,200 ドット以上	
Web カメラ	有効画素数約 92 万画素(デュアルマイク付／Windows Hello 対応）以上	
LAN	1000BASE-T/100BASE-TX/10BASE-T 準拠　WakeupOnLAN 対応	
インターフェース	HDMI 出力端子×1 、LAN（RJ45）×1、USB3.2（Gen1）Type-A コネクタ×2 、Thunderbolt 4（USB4 Type-C）コネクタ×2 以上（Power Delivery 対応、外部ディスプレイ出力対応であること）、マイク入力/ヘッドホン出力端子×1	

本体質量	1.4kg 以下	
バッテリー	駆動時間が、JEITA バッテリ測定法 Ver3.0 で 動画再生時：8.0 時間以上、アイドル時：18 時間以上であること。 使用者にてバッテリーパックの交換が簡単且つ安全にできること。 バッテリ交換時にマザーボードには触れられない構造になっていること。	
無線 LAN	Wi-Fi　6E（IEEE802.11ａｘ）（2.4Ｇbps）対応＋IEEE802.11ac/a/b/g/n 準拠	
Bluetooth	Bluetooth ワイヤレステクノロジーVer.5.3 準拠	
付属品	AC アダプタ、覗き見防止フィルター	

6.1.3 既存環境との接続

・プリンタ

各学校設置のプリンタ及び複合機・スキャナ等の再設定・ドライバーインストールについては、発注者と協議の上、実施すること。

プリンタの IP アドレス等ネットワーク情報の変更が別途必要な場合は実施すること。

※「別紙２　プリンタ等一覧」を参照

・無線 LAN

既存の学習系ネットワークに接続すること（SSID 等情報は受注者へ提供することとする）
5GHz デジタル証明書なし、ID/パスワード認証　MAC アドレスフィルタリングあり

MAC アドレス登録のため、新規指導者用端末の MAC アドレスを発注者に提出すること。

構築作業要件

本事業では、「GIGA スクール構想」を実現するための「宗像市校内通信ネットワーク整備業務」で構築した、校内ネットワーク、無線アクセスポイントを校務環境でも利用することで、安全安心に配慮した、校務用サービス環境の実現を目指す。

7.1.1 搬入設置等

・既存の指導者用端末との入替スケジュール及び計画書を作成し、発注者の承認を得ること。

・今回導入するハードウェア及びソフトウェア等の全てを一括して学校に搬入すること（宅配便等の利用は不可とする）。

・不要な梱包材、廃材等はすみやかにすべて引き取ること。

・機器の搬入、調整及びこれらに付帯する工事に関わる費用はすべて含めること。

・搬入・設置に際して、校舎等施設を破損することがないこと。万一、搬入・設置時、または作業を行う際に、納入業者の責により校舎等施設を破損した場合は直ちに教育総務課へ破損の状況、原因等を報告し、納入業者が全額負担において修繕すること。

・無線アクセスポイントは各学校職員室（または事務室、校長室）に設置すること。近くの PoE スイッチングハブから配線し、取付場所は各学校と協議の上、決定すること。

- 敷設ケーブルの両端に、接続先等をラベリングすること。
- 10GBASE-T に対応した CAT6A 以上の配線を敷設すること。
- 発注者にて指示する色のケーブルで配線を行うこと。
- 配線を行う際、区画や壁を通す必要がある場合は事前に発注者と協議の上、施工すること。
- 各ケーブルのフルーク試験を行うこと。
- ケーブルが露出する場合は、モール・マジックテープ・インシュロック等で保護すること。
- 本業務実施にあたり必要な材料等に係る費用はすべて盛り込むこと。

・GIGA 系ネットワーク機器（ルータ）と校務用プリンタ間の物理配線を行うこと。その際、ケーブル等が露出しないよう施工すること。スイッチングハブにて集約して接続も可とするが、費用に含めること。ネットワーク機器の設定変更が必要な場合は発注者にて実施するため、費用には含めない。

・別調達である指導者用端末は指導者用端末調達の落札者での納入を予定しているため、キッティング作業場所を準備し、必要台数・住所・担当者・連絡先等を提供すること。保証書の抜き取り、シリアル番号リスト（Excel）の提供は指導者用端末調達の落札者にて行う。

・指導者用端末の初期不良が発生した場合は、発注者に連絡の上、指導者用端末調達の落札者にて交換対応となる。指導者用端末調達の落札者による交換対応が著しく遅れた場合、スケジュールや配布計画の変更を発注者に連絡し、都度対応を協議するものとする。

7.1.2　端末廃棄

・既存の校務用端末について、3 月下旬を目途に回収及び廃棄を行う。

なお、回収及び廃棄の時期については発注者と協議の上、決定する。

7.1.3　構築業務要件

基本要件

(1)　5 年間運用できるシステム及びハードウェアを選定すること。

(2)　調達する全てのソフトウェアは、原則、導入時の最新バージョンを導入すること。

(3)　システムの運用に関して、本市で必要となる運用設計支援を行うこと。

(4)　指導者用端末はマルウェア対策、情報漏えいなどのセキュリティ対策をすること。ログの取得を前提とし、インシデント発生時など市の要望に応じてレポートを提出すること。

プロジェクト体制

(1) プロジェクト体制表の作成にあたっては、作業責任者、役割、連絡先を明確にすること。

(2) プロジェクトマネージャーまたは作業責任者について、以下の各条件を満たすこと。

(ア) システム

(イ) 設計・構築・運用等の業務経験を 5 年以上有していること。

(ウ) 福岡県内や近郊のサポート経験を有すること。

(エ) Microsoft365 に関する構築・運用保守業務の実績を保有すること。

(オ)「プロジェクトマネージャー」等の IPA が認定する高度認定資格、又は同等の資格を保有していること。

プロジェクト管理

(1) 本システムの導入過程の経過、進捗状況を、定例会議（月 1 回）を通じて報告すること。また進捗報告書及び打合せ会議に際しては、議事内容を事前に提示するとともに、毎回、受注者が議事録を作成し、会議終了後、速やかに提出すること。

(2) 本サービスの提供を進めていくうえで必要となる関係部署、関係機関との調整用資料等の作成についても支援すること。なお、課題や資料を随時共有できること。

(3) 設計、構築期間においては、必要に応じて検討会を実施し、スムーズな業務進行を図ること。また、仕様や要件の確認及び確定に関しては、必ず書面により行うこと。

(4) 課題管理表については、毎回の会議の中で確認を行うこと。

7.1.4 指導者用端末の設定・キッティング

・新規の指導者用端末のマスターデータを作成し、展開すること。また、円滑な保守・運用のため、リカバリー媒体を作成すること。

・マスターレビュー後、パイロット校を定め、試験導入・ネットワーク等の動作検証を実施すること。

・各学校に設置するバックアップ用 NAS を指導者用端末から利用できるよう接続すること。(バックアップ用 NAS の初期設定は発注者にて行う)

・全ての新規の指導者用端末でゼロトラスト型システム基盤を経由し、インターネット利用ができるように、設定作業と動作確認を行うこと。

・全ての新指導者用端末及び既存指導者用端末で、「すぐーる」(株式会社 Visor) 及び「採点ナビ」(株式会社教育ソフトウェア) を利用できるよう設定すること。

・OS については、Windows 11 Pro 以上であること。

・管理に必要な番号等を機器に管理シール等で貼付しておくこと。(貼付方法や場所当は事前に発注者と協議すること。) また、梱包材 (外箱) にも同一のシールを貼付すること。

・指導者用端末から Windows Defender の自動アップデートができるように設定すること。

・指導者用端末入替に関わる利用者向け手順書を作成し、各教職員へ配布すること。

・引き渡し時には指導者用端末の初期ログイン・パスワード変更の案内表を作成し、学校の業務に支障がないよう交換作業を行うこと。

・各指導者用端末は認証基盤によるドメイン管理下に置くこと。

・校務ソフトウェア仕様以外のフリーソフトウェア、個別アプリケーションについては発注者及び各学校と協議の上、各指導者用端末にインストールすること。

・指導者用端末に関する Windows アップデートに関しては、今回導入するシステムにより定期的にアップデートを行うよう設定を行うこと。

・その他指導者用端末の環境設定に関する項目は別途発注者と協議の上､決定すること。

7.1.5 無線アクセスポイントの設定・キッティング

・既存の無線アクセスポイントから送出する SSID に接続可能とすること。また、デバイス登録、ネットワーク設定、チャネル設定、セキュリティ設定等を既存環境に合わせて実施すること。(IP アドレス等既存ネットワーク情報は受注者のみに提示する)

・無線アクセスポイントのバージョンを最新とし、ファームウェアを最新までアップデートを行うこと。

8.1 運用・保守性

8.1.1 システムメンテナンス

・利用者に影響のあるシステムへのメンテナンスは、可能な限り業務影響がない時間帯で実施すること。
・利用者に影響のあるメンテナンスを行う際には、事前に発注者と調整の上、利用者への周知を行った上で実施すること。

8.1.2 障害監視

・障害監視により異常を検知した場合は、メール等へ通知すること。
・Microsoft 管理センター等のポータルでサービスの正常性を目視確認できること。

テスト要件

9.1　対象とするテストの範囲

9.1.1 システムテスト

・各サービス、サーバの正常系・異常系のテストを実施すること。
・バックアップ及びリストアテストについては、発注者と必要性を協議の上で実施すること。

9.1.2 セキュリティテスト

・セキュリティ要件に記載の、アクセス制御・データ分類・情報漏洩対策については設計通りに動作することをシステムテストにて確認すること。
・ウイルス対策のテストについては、メーカーまたは一般に公開されているテストファイル等で実施すること。
・クラウドサービスやサーバへの侵入検知のテストまでは必須要件としないが、必要な場合はテスト計画に盛り込み協議の上適切な手続きを行った上で実施すること。

9.2 テストの実施方法

9.2.1 テスト実施計画

・テストは、本番運用を行う環境を用いて行うこと。

9.2.2 テスト環境

・本調達ではテスト環境の調達は想定していない。運用環境とは別にテスト環境を用意する場合は事業者負担で構築すること。

運用・保守要件

10.1 運用・保守対象

・運用・保守対象とするシステムは以下とする。

- 本調達で構築するゼロトラスト型システム基盤全般
- 別調達で整備する指導者用端末
- 本調達で整備する無線アクセスポイント

10.2 運用・保守内容

10.2.1 運用内容

・ 対象システムへの運用内容は以下とする。

No.	運用項目	運用内容
1	障害監視	システムの障害発生状況を監視し通知を行うこと。
2	一般的な問合せ対応	教職員等のエンドユーザーからの問合せに基づき操作方法の案内を行うこと。また不具合があった場合の一次問合せを受け付けること。また、システム管理者からの技術的な問合せについても対応を行うこと。
3	システムメンテナンス	発注者と対応を協議の上、システムメンテナンスを行うこと。またクライアントの更新プログラム配信設定のメンテナンスも含む（例：Windows のバージョン固定の解除、次期バージョンの配信許可設定）
4	定例会	障害情報、セキュリティの情報、問合せの対応履歴について情報整理し発注者へ報告すること。（月 1 回程度想定）

5	ハードウェア保守	指導者用端末の保守管理を行い、不具合が生じた場合は問合せ受付後一次切り分けまたは修繕作業を行うよう速やかに対応可能な体制を準備すること。 ※指導者用端末はメーカー5 年間引取保証を付与・登録している ※再利用端末やマウス等周辺機器は除く ※離島の学校は発注者にて対応する 新規指導者用端末が不良・故障になった場合、指導者用端末調達の落札者にて故障機の引取・交換回収、メーカー保証への修理手配を行う。 メーカー修理後、導入時の設定状態までの再設定を行うこと。 但し、以下のケースは保守対象外とする。 データの破損、紛失、機器の物理破損、本調達品以外を起因とした障害
6	インシデント監視・通報・解析（SOC）	24 時間 365 日の有人監視・電話受付（日本語）を行い、アラートの発生の確認・一次対処（隔離や停止などのオペレーション）・ログの分析等を行うこと。 監視や分析によりセキュリティインシデントを検知した場合には、1 時間以内に通報すること。 セキュリティインシデントの検出状況及びセキュリティインシデントへの対応状況等について、月 1 回レポートを作成し、提出すること。 ※詳細は 10.2.4 運用保守体制（SOC）を参照

10.2.2 保守内容

・　対象システムへの保守内容は以下とする。

No.	保守項目	保守内容
1	障害対応・復旧作業	利用者からの問い合わせ、ならびに障害監視結果を基に、障害対応・復旧作業を遠隔・現地で行うこと。
2	保守履歴管理	障害対応・復旧作業で実施した保守内容の管理を行うこと。

10.2.3 運用保守体制（システム・ハードウェア保守）

・運用保守の問合せ窓口を開設すること。

・問合せ窓口は以下の要件を満たすこと。

- 平日（土・日・祝祭日・年末年始以外）9:00-17:00 メール及び電話での問合せ対応
- 時間外のメールによる問合せに対しては、翌営業日に対応すること

・ただし、授業影響が発生するような緊急を要する障害が発生した際には、発注者と協議の上、速やかに対応すること。

10.2.4 運用保守体制（SOC）

・24 時間 365 日の有人監視を行い、アラートの発生の確認・ログの分析等を行うこと。
・監視や分析によりセキュリティインシデントを検知した場合には、1 時間以内に通報すること(SLO)
・発生したセキュリティインシデントの原因について、ログ分析等を実施し、重要度、緊急度を報告すること。報告内容には、一次対処方法を含め提示すること。
・有人による 24 時間 365 日の電話受付(日本語対応)や一次対処（隔離や停止などのオペレーション）が可能なこと。
・発生したセキュリティインシデントの解析を行い、調査結果、影響範囲、対処方法を連絡すること。
・セキュリティインシデントの検出状況及びセキュリティインシデントへの対応状況等について、月 1 回レポートを作成し、提出すること。
・運用に係る各作業については、手順書を作成し、作業を行うこと。また、運用期間中に、手順書や設計書において、内容の変更が生じた場合には、随時改訂を行い、更新履歴を付して提出すること。
・二次解析において、原因究明、影響範囲調査、及び恒久的対処支援がサービスとして提供できること。また必要に応じて SOC 対象以外の機器のログも参照できること。
・二次解析において、UEBA（職員の行動管理）を基にしたセキュリティレポートを必要に応じて提供できること。
・AD サーバのログ追跡やパソコン操作ログ等の相関分析が必要に応じてサービス提供可能なこと。
・製品の脆弱性情報を能動的に調査し、注意喚起、また必要に応じてパッチ適用も提供可能なこと。
・Internet の出入り口、IPS/IDS/WAF などのネットワーク機器、メール、サーバ/PC、モバイル環境、及びクラウドの 6 セグメントについて、すべて SOC サービスの提供実績を有すること。
・SOC サービスの検知や一次通報、二次通報など、各サービス要素を要素単位に分離し、別運用ベンダの運用サービスとマージして全体の運用サービスとして見せることができるサービスインタフェースを SOC に実装すること。
・解析が必要なインシデントは、発注者から依頼を受けなくても自ら判断し能動的に解析を行うこと。
・ホワイトハッカーチームがクラウド環境に疑似的な攻撃を仕掛けることにより、ASP 事業者が実施したインフラ設定や環境について脆弱性の穴を検出し、対処方法の支援を実施する体制を有すること。
・SOC 設備は、日本国内に設置されていること。また、データセンター等の堅牢な設備環境上で運用されており、災害時、別拠点でも運用が継続対応できる体制を有すること。
・自社で独自に国内インターネット上におとりサーバを立てて日々攻撃分析を行い、あらたな攻撃に対して対応できる体制を有すること。

10.3 運用・保守提供時間

・開庁日（日曜日、土曜日、国民の祝日に関する法律「昭和 23 年法律第 178 号」に規定する休日及び 12 月 29 日から翌年 1 月 3 日までの日は除く。）の 9 時 00 分から 17 時 30 分までの間とする。ただし、システム利用に致命的な障害が発生した際は、協議の上、速やかに対応を行うこと。
・開庁日内で対応が不可能な日程が存在する場合は、事前に発注者に報告し承認を得ること。

10.4 その他保守事項

システムが末永く安定稼動するよう体制を整え、メンテナンスを行うこと。

① 障害復旧時には、障害の事象、影響、原因及び対策方法等をまとめた報告書を作成し、提出すること。
② ハードウェア・ソフトウェア・サービスともに、製品及び技術に関する情報提供を行うこと。
③ 各システムの日々の運用における次の軽微な作業については、発注者にて実施する。
・年度末以外のタイミングでの配属・異動・退職等におけるユーザーアカウントの管理
・ファイル管理機能内でのファイル復元作業
・各種サーバの状態確認
・定期的なイベントログ確認等
④ 同ネットワーク内の他システムとの調整が必要なものに関しても最大限協力するものとする。
⑤ サービスパック・パッチ等については速やかに情報を入手し適用すること。
⑥ セキュリティパッチについては、スケジュールを組んで定期的に適用する仕組みとすること。
⑦ 無償あるいは保守の範囲でバージョンアップの権利を有するものについては時期を見極め積極的に適用すること。
⑧ 基本的に営業時間内でのコールを原則に経費を見積ること。
⑨ リモート保守を行う際は、 本市への接続が許可された特定端末により、セキュリティが確保されたエリアからのみ行うこととする。また、接続の際は発注者の許可を得るようにする。

説明会・研修の計画

11.1 説明会・研修

・研修対象者に即したマニュアルの作成も業務範囲とする。
・研修についてはオンライン及び対面のいずれの形式も可とする。
・オンラインで開催する際には、当日やむを得ず欠席となった利用者を配慮し、録画したデータをストリーミング形式で受講可能とする。また、録画データは一般的な端末で視聴可能なデータ形式で提供すること。

・研修会実施後に発生する研修対象者からの問い合わせを受け付ける窓口を設けること。

・研修の内容

- 管理者向け（教育総務課）
- 在籍教職員
- 新任教職員

・研修の形式

- 集合研修
- オンライン

想定している研修対象者、研修内容、研修方法、開催時期/回数は以下とするが、詳細な内容や開催日程については、発注者と別途協議の上で決定すること。

受講者分類	研修対象者	研修内容	方法	開催時期/回数
システム管理者	教育総務課システム担当	年次更新業務の説明 管理ポータルの使用方法	集合研修	仮稼働時に1回以上
在籍教職員	学校管理職・教職員	システムの利用方法 問合せ方法の説明	集合研修またはオンライン	
新任教職員	新任の教職員（受講済みの対象者を除く）	システムの利用方法 問合せ方法の説明	集合研修またはオンライン	令和8年4月に1回を想定

成果品等

12.1 完了時提出書類

受注者は、本業務完了後速やかに完成届を作成の上、発注者へ提出すること。

12.2 成果品検査等

業務の完了後、成果品を提出し発注者の検査を受けるものとし、本業務に適しないものとして修正の指示があった場合には、速やかに修正を行うものとする。

また、本業務の完了後であっても、成果品に瑕疵が発見された場合には、発注者の指示に従い速やかに成果品の修正を行なわなければならない。この場合において、当該修正に要する費用は、全て受注者の負担とする。

12.3 成果品

・以下に掲げる成果品を製本及び電子媒体で納品すること

ア．システム基本設計書（製本・PDF 各 1 部）

イ．システム詳細設計書（製本・PDF 各 1 部）

ウ．システム移行スケジュール（製本・PDF 各 1 部）

エ．指導者用端末 設定・パラメータ資料（製本・PDF 各 1 部）

オ．指導者用端末 キッティングチェックシート（製本・PDF 各 1 部）

カ．指導者用端末 学校毎のシリアル・管理番号一覧表（製本・PDF 各 1 部）

キ．指導者用端末 納入写真（製本・PDF 各 1 部）

ク．無線アクセスポイント 設定報告書（製本・PDF 各 1 部）

ケ．システム ID・パスワード一覧（製本・PDF 各 1 部）

コ．システム試験成績表（製本・PDF 各 1 部）

サ．管理者向け運用マニュアル・障害対応連絡先（製本・PDF 各 1 部）

シ．教職員向け基本操作マニュアル（製本・PDF 各 1 部）
わかりやすい内容で双方の担当者に異動が生じても速やかに引き継ぎができるようにすること

ス．指導者用端末 マスターリカバリデータ（外部記憶媒体に格納し、納品すること）

セ．その他必要と思われるドキュメントがあれば同様に納品すること

※ 電子ファイルは 1 枚のメデイアに集約すること

※「試験成績表」以外については後の改修・運用変更に備え、できるだけ編集可能なファイル形式でも納品し、加除整理を行うこと。

・電子媒体による報告書は、CD-R または DVD-R に業務名を印刷して 1 部提出すること。

・指導者用端末の不要な取扱説明書や付属品は発注者及び各学校に各一部保管とする。

・契約満了後においても、報告書等の内容について、本市からの問い合わせや根拠資料の提出要求があった際には、適宜対応すること。

12.4 成果品の納入場所

〒811-3492　福岡県宗像市東郷一丁目 1 番 1 号　宗像市教育委員会教育総務課

12.5 成果品の管理及び帰属

本業務の成果品は全て発注者の管理及び帰属とし、受注者は成果品を第三者に公表又は貸与してはならない。

12.6 その他

・本業務は、本仕様書に基づき実施すること。

・受注者は業務の進歩状況等を定期的に報告するほか、発注者の求めに応じて速やかに報告を行うものとする。

・発注者は、完成検査が完了し受注者から適法な請求書を受理した日から起算して３０日以内に受注者に支払う。

・本業務の実施にあたり、本事業で構築する環境等については、ガイドライン及び「 GIGA スクール構想の下での校務 DX について～教職員の働きやすさと教育活動の一層の高度化を目指して～（令和 5 年 3 月文部科学省)」を逸脱しないものとするとともに、関係法令、条例及び規則を遵守すること。

・本業務の遂行上知り得た秘密を他人に漏らしてはならない。

・受注者は、業務で使用する各種資料やデータに含まれる機密情報や個人情報等の紛失、漏えい等が発生しないように、データセキュリティ対策及び個人情報保護対策を講じなければならない。

・受注者は以下の資格を有すること。

ア ISO9001 QMS ：品質マネジメントシステム

イ ISO15001 プライバシーマーク：個人情報セキュリティ

ウ ISO27001 ISMS ：情報セキュリティマネジメントシステム

・本仕様書に定めのない事項や業務の実施にあたり疑義が生じた場合は、速やかに発注者と協議のうえ定めるものとする。