仕　様　書

1　事業名

平戸市教育ネットワークシステム構築事業

2　背景と目的

本市教育委員会で稼働中のサーバ機器は､導入から５年を迎えようとしており、機器の老朽化による障害や保守サービスの終了が間近に迫っている。このため、機器等のリプレイスが必要となっている。

また、現在、本市の各小中学校で利用している校務用PCは、インターネットへの接続は原則禁止とし、学校外への持ち出しも禁止する運用を行っている。文部科学省が提唱している校務DXの課題としても挙げられているが、校務処理のほとんどを職員室内で行うように制限されており、現代のライフスタイルに応じたテレワーク等のフレキシブルな働き方にはそぐわない状態となっている。

以上のことから、本事業では文部科学省公表の「GIGAスクール構想の下での校務DXについて」の記載内容に則り、クラウドサービスを利用して業務データの保護や業務継続性の確保を実現し、ゼロトラストセキュリティを導入することで、教職員及び事務職員の働き方の選択肢を増やし、働き方改革を実現することを目的とする。

3　業務概要等

本事業では､「７　構築要件」に調達範囲を示す。また、下記については既存機器等を継続利用または本市が別途調達することから本業務対象外とする｡ただし、クラウドサービスを導入するにあたり、下記について設定変更等が発生する場合は、本市が指名する事業者に見積もりを行い、提案価格に含めることとする。

(1) 各小中学校の校内LAN配線
(2) 各小中学校の無線アクセスポイント及び管理コンソール
(3) 各小中学校のインターネット回線
(4) 校務用PC、学習用PC及びプリンタ等の情報処理機器類
(5) 各小中学校と本庁舎間の回線及びネットワーク機器類
(6) 学習系ネットワーク
(7) 学習系ネットワークに係る各種クラウドサービス（Google Work s pace、デジタル教科書やiFilter@クラウドなど）

4　契約期間

(1) 構築期間

契約締結日から令和７年９月30日まで

(2) 保守運用期間

令和７年９月１日から令和12年８月31日まで

(3) 各種ライセンス

各種ライセンスについては、令和７年８月１日に仮稼働ができるよう５年間（長期継続契約、単年度契約の別は問わない。）の契約を行う。

5　スケジュール

本業務のスケジュールについては、契約締結日（予定）から令和７年９月30日までを構築期間とし、本稼働開始を令和７年９月１日とする。ただし、スケジュールについては現段階では予定であり、事業者の提案により本市に最適なスケジュールにて実施するものとする。

構築スケジュール

年	令和７年						
月	４月	５月	６月	７月	８月	９月	10月
予定	公告	選定 契約締結	調査・設計 構築・移行		テスト 運用	★本稼働開始	

6　現状と課題

(1) 校務用PC環境

各職員は校務用PCを利用しており、原則、校外持出を禁止としている。現在の運用では有線で接続されていることから、自席以外での利用ができない。

また、校務用PCは、閉域環境での利用を前提としており、インターネットを閲覧するためにはデスクトップ仮想化ソフトを利用している。しかしながら、インターネット経由で利用しているシステムにおいては、一部がデスクトップ仮想化ソフトでは対応できないため、その分について特定通信として接続されている。

校務用PCはActiveDirectoryで、一括で管理されており、グループポリシーを用いて設定変更等を行っているが、別途、外部記憶媒体の接続を禁じたり操作ログを取得するために資産管理ソフトを利用している。

現在、オフィスソフトとしてMicrosoft Office 2019、2021を利用しているが、Microsoft 365への移行を検討している。

なお、校務用PCの台数は、370台であり、その利用者は、平戸市立小中学校の教職員・事務職員及び教育委員会職員である。

(2) 共有フォルダ

共有フォルダは各小中学校単位でWindowsサーバを用いて構築されており、その使用容量は、7.79TBである。

また、共有フォルダ内で校長、教頭、事務職員及び教員のフォルダを作成し、それぞれ以下のとおりアクセス権を付与している。

ア　校長フォルダ　　校長
イ　教頭フォルダ　　校長、教頭
ウ　事務職員フォルダ　　校長、教頭、事務職員
エ　教員フォルダ　　校長、教頭、事務職員、教員
オ　教育委員会フォルダ　教育委員会職員

(3) 資産管理ツール

校務用PCは、ハンモック社AssetViewで管理を行っているが、校務用PCの校外持出可を実現するために、クラウドサービスを利用したIT資産管理ツールへ移行する。

なお、現行のAssetViewで利用している機能は次のとおりである。

ア　IT資産管理
イ　アプリケーション配布
ウ　デバイス制御
エ　ファイル暗号化
オ　PC操作ログ管理
カ　不正PC遮断
キ　リモートコンソール

(4) セキュリティ

校務用PCと各イントラサーバのウイルス対策ソフトとして、ESETを利用しており、EPPのみ導入している。

また、現在はオンプレミスでサーバを構築して運用しているが、校務用PCの校外持出可を実現するにあたり、クラウドサービスを利用したウイルス対策への移行を行う。

なお、現状として、校務用PCにログオンする際には、ユーザーIDとパスワードで行っているが、二要素認証や二段階認証は導入していない。

(5) クラウドサービス

クラウドサービスは次のものを利用している。

ア　長崎県校務支援システム

イ　Google Workspace for Education

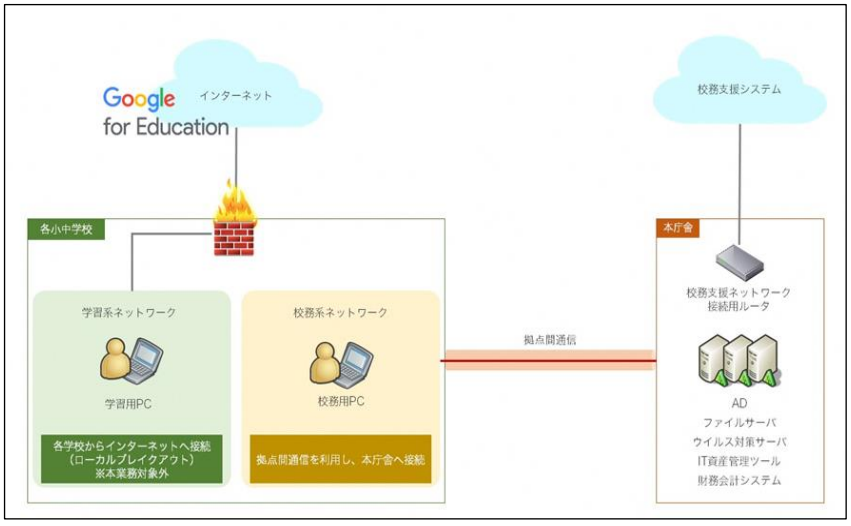
(6) ユーザー数

市立小中学校に所属している教職員等及び児童生徒数は以下のとおりである。

ユーザー区分	人数
教職員（校長教頭事務職員を除く）	229人
校長教頭事務職員	68人
児童生徒	1,960人
教育委員会事務局職員	21人

(7) その他

一部の校務用PCでは財務会計システムを利用しているが、本業務完了後も継続して利用する。なお、財務会計システムは平戸市行政ネットワークに構築されており、校務系ネットワークとは異なるセグメントに属している。



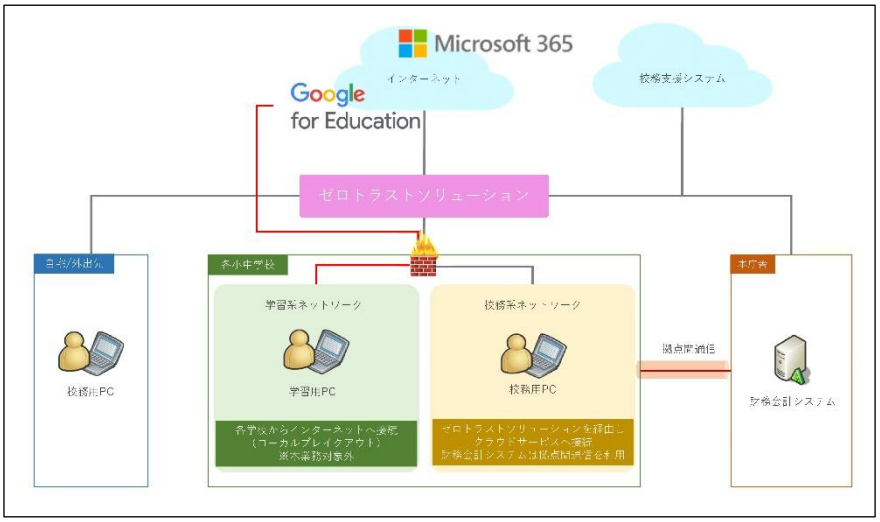
7　構築要件

本業務の実施にあたり、以下の各項目を満たす内容で、かつ、本市にとって最善と思われる提案をすること。

(1) 基本要件

ア　提案するサービス及び製品は、原則として提案時点で商品化されていること。

イ　原則としてクラウドサービスの提案を行うこと。
ウ　提案時点で商品化されていないサービス、機器及びソフトウェアを提案する場合には、技術的要件を満たすことの証明及び納入期限までに製品化され納入できることを保証する資料及び確約書等を提出すること。
エ　校務系ネットワークと学習系ネットワークは論理的に分離すること。
オ　校務用PCにおいて、ロケーションフリーで利用できるようにセキュリティ要件を満たすこと。
カ　校務用PCは既存PCを利用する。



キ　Microsoft 365 EducationのA3またはA5のライセンスを導入すること。
ク　校外での利用を想定し、職員室、事務室及び校長室は有線ネットワーク（固定IP）とし、教室は、無線ネットワーク（DHCP）とすること。
ケ　本市ネットワークは行政側で管理を行っているため、設定変更等が必要な場合は行政側ネットワーク保守業者と連携をすること。

(2) アカウント要件
ア　Microsoft 365で提供されている「Microsoft Entra ID」を利用すること。
イ　「ア」の初期設定を行うこと。
ウ　アカウントはIDの統合管理を行い、可能な限り、下記に記載しているサービスにもシングルサインオン（以下、「SSO」）でアクセスできる仕組みを提案すること。
・Microsoft 365 Education
・Google Workspace for Education
・長崎県校務支援システム
エ　組織や役割に応じた権限が付与できること。また、その権限設定を業務

システムやファイルサーバに適用できること。

オ　校務用PCのEntra IDへの参加（ドメイン参加）は平戸市が行うことを想定しているため、その作業の補助を行うこと。

(3) ビジネスチャット要件

ア　ビジネスチャットとして、Microsoft 365に含まれている「Microsoft Teams 」が利用できること。

イ　「ア」の初期設定を行うこと。

ウ　Teamsのチームやグループチャット機能を用いて､校内のみならず学校間をまたいだ情報共有が行えること。

エ　Teamsの利用を各職員の個人用スマホから利用できること｡その際に利用する個人用スマホには､｢Temas上のデータが個人用スマホに残らない。｣､｢個人用スマホを紛失した際にTemas上のデータ等を閲覧できなくする。｣等の対策を施すこと。

(4) 共有フォルダ

ア　Microsoft 365で提供されている「Microsoft 365 SharePoint Online」を導入すること。

イ　ドキュメントのバージョン履歴を自動的に保存し、必要に応じて以前のバージョンに戻せるよう設定を行うこと。

ウ　ユーザやグループごとに異なるアクセス権限の設定を行うこと。

エ　校務用PCにユーザーの所属校等の共有フォルダへ簡単にアクセスできる設定を提案すること。

オ　本市のインターネット接続環境（利用サービス名：フレッツ　光ネクスト　ファミリー・スーパーハイスピードタイプ　隼）を考慮し、効率的な共有フォルダ環境があれば提案すること。

(5) セキュリティ要件

文部科学省が公表している「GIGAスクール構想の下での校務DXについて」の資料に記載している内容に基づき、最適な組み合わせを提案すること。

ただし、③-6について本市では外部公開しているサーバが存在しないため、不要とする。

また、Windows OSに限らず、Chrome OSでも利用できるものを提案すること。

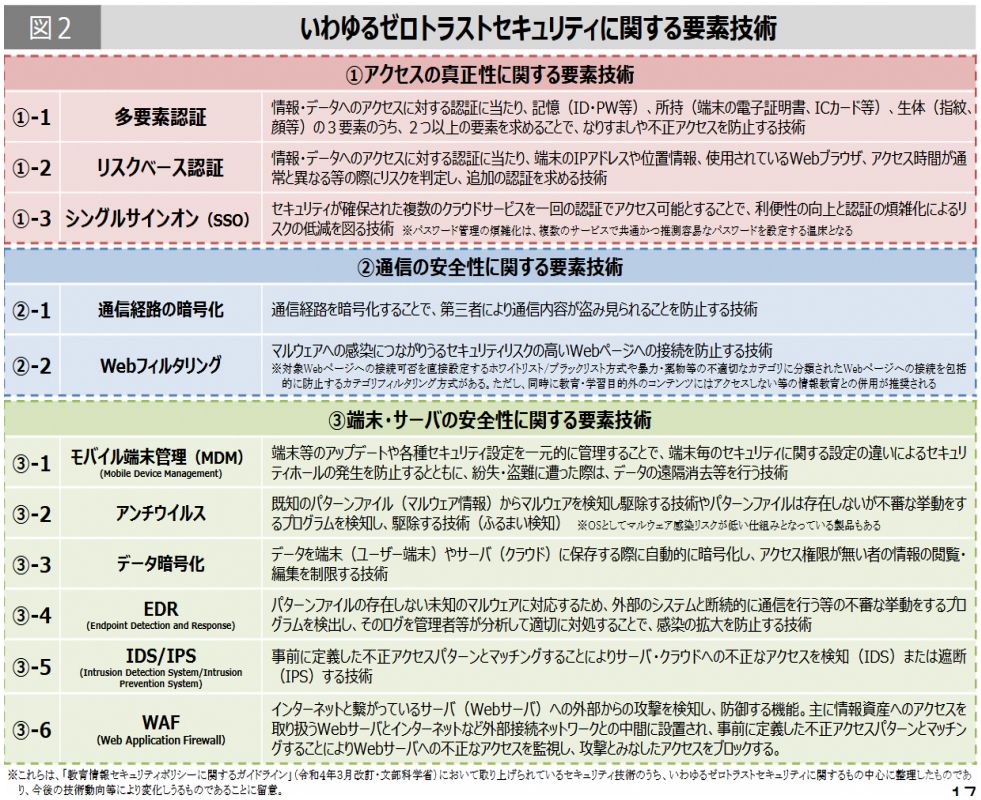


図2 いわゆるゼロトラストセキュリティに関する要素技術

①アクセスの真正性に関する要素技術		
①-1	多要素認証	情報・データへのアクセスに対する認証に当たり、記憶（ID・PW等）、所持（端末の電子証明書、ICカード等）、生体（指紋、顔等）の３要素のうち、２つ以上の要素を求めることで、なりすましや不正アクセスを防止する技術
①-2	リスクベース認証	情報・データへのアクセスに対する認証に当たり、端末のIPアドレスや位置情報、使用されているWebブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、追加の認証を求める技術
①-3	シングルサインオン（SSO）	セキュリティが確保された複数のクラウドサービスを一回の認証でアクセス可能とすることで、利便性の向上と認証の煩雑化によるリスクの低減を図る技術 ※パスワード管理の煩雑化は、複数のサービスで共通かつ推測容易なパスワードを設定する温床となる
②通信の安全性に関する要素技術		
②-1	通信経路の暗号化	通信経路を暗号化することで、第三者により通信内容が盗み見られることを防止する技術
②-2	Webフィルタリング	マルウェアへの感染につながりうるセキュリティリスクの高いWebページへの接続を防止する技術 ※対象Webページへの接続可否を直接設定するホワイトリスト/ブラックリスト方式や暴力・薬物等の不適切なカテゴリに分類されたWebページへの接続を包括的に防止するカテゴリフィルタリング方式がある。ただし、同時に教育・学習目的外のコンテンツにはアクセスしない等の情報教育との併用が推奨される
③端末・サーバの安全性に関する要素技術		
③-1	モバイル端末管理（MDM） (Mobile Device Management)	端末等のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールの発生を防止するとともに、紛失・盗難に遭った際は、データの遠隔消去等を行う技術
③-2	アンチウイルス	既知のパターンファイル（マルウェア情報）からマルウェアを検知し駆除する技術やパターンファイルは存在しないが不審な挙動をするプログラムを検知し、駆除する技術（ふるまい検知） ※OSとしてマルウェア感染リスクが低い仕組みとなっている製品もある
③-3	データ暗号化	データを端末（ユーザー端末）やサーバ（クラウド）に保存する際に自動的に暗号化し、アクセス権限が無い者の情報の閲覧・編集を制限する技術
③-4	EDR (Endpoint Detection and Response)	パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、そのログを管理者等が分析して適切に対処することで、感染の拡大を防止する技術
③-5	IDS/IPS (Intrusion Detection System/Intrusion Prevention System)	事前に定義した不正アクセスパターンとマッチングすることによりサーバ・クラウドへの不正なアクセスを検知（IDS）または遮断（IPS）する技術
③-6	WAF (Web Application Firewall)	インターネットと繋がっているサーバ（Webサーバ）への外部からの攻撃を検知し、防御する機能。主に情報資産へのアクセスを取り扱うWebサーバとインターネットなど外部接続ネットワークとの中間に設置され、事前に定義した不正アクセスパターンとマッチングすることによりWebサーバへの不正なアクセスを監視し、攻撃とみなしたアクセスをブロックする。

※これらは、「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4年3月改訂・文部科学省）において取り上げられているセキュリティ技術のうち、いわゆるゼロトラストセキュリティに関するもの中心に整理したものであり、今後の技術動向等により変化しうるものであることに留意。

17

(6) IT資産管理要件

「６－(3) IT資産管理ツール」に記載している製品と同等のものを提案すること。

(7) 仮想サーバ構築要件

教育委員会では図書システム用のサーバを管理しているため仮想サーバを導入し移行を行うこと。

また、仮想サーバでは各種機器の監視を行うためのシステム等も稼働させるため、それらが十分に稼働できるスペックの仮想サーバを提案すること。

ア　必要なスペックは下記のとおりである。

用途	vCPU	vMem	vDisk	OS
図書用AD	2	4	120GB	Windows
図書用DB	2	4	550GB	Windows
図書用資産管理システム	2	8	200GB	Windows
図書用ウイルス対策システム	4	4	100GB	Windows
監視システム	2	8	320GB	Windows
ログ管理システム	2	3	600GB	CentOS
DHCP	2	4	40GB	CentOS

イ　機器の冗長化は不要

ウ　毎日バックアップを取得すること。なお、NASを提案する場合はバックアップ先と同一筐体でも可とする。
エ　無停電電源装置を導入すること。
オ　各サーバの移行作業を実施すること。
カ　各サーバはAHV上で稼働している。

(8) データ移行要件
ア　データ移行について、各職員による作業や確認が必要となることを想定しているが、業務負荷軽減や安全にデータ移行を進める観点から移行時のマニュアル作成や問い合わせ対応などの各種作業の補助を行うこと。
イ　現行Active Directory等の構成情報を基にしてMicrosoft Entra IDに移行すること。なお、移行については、現行の環境への影響を最小限に抑えること。
ウ　現行のファイルサーバに格納されているデータについては、本業務で導入するSharePointに移行するため、移行のための最適な提案を行うこと。
エ　各職員が利用している校務用PC内に保存されているデータについては、本業務で導入するMicrosoft OneDriveに移行するため、その補助を行うこと。

(9) その他の要件
ア　校務用PCから本市行政環境に構築されている財務会計システムが利用できること。
イ　本業務でのネットワーク等の設定変更に要する費用については、現行保守事業者と調整を行い本業務受託業者が負担すること。

8　運用要件
(1) 基本要件
ア　通常保守・運用対応時間は、原則として本市開庁日の午前９時から午後５時までとする。ただし、対象サービス等のトラブルの重要度、緊急度が大きいと判断した場合や本市から要請した場合はこの限りでない。
イ　提案する機器については、原則、オンサイト保守とすること。
ウ　本業務で導入したクラウドサービスに関する問い合わせ（質問、障害等）や運用作業依頼を受け付ける窓口（以下、「保守・運用窓口」という。）を設置すること。
エ　保守・運用窓口は、一本化の上、受注者が責任を持って運用し、電話及びメール等により受け付けを可能とすること。
オ　本市からの問い合わせや依頼については、速やかに対応することとし、

回答に時間を要する場合は、必ず回答期日や状況などを適宜報告すること。

カ　保守・運用窓口にて受け付けた内容を記録し、回答状況の管理を行うこと。

キ　受注者は、保守・運用における体制及び保守・運用窓口の連絡先が明記された資料を提示すること。

ク　上記「キ」における資料は常に最新の状態に更新し、変更がある場合は本市へ報告すること。

ケ　本業務で導入したクラウドサービスに関する各種資料（構築業務時の成果物及び保守・運用業務にて作成した資料）は、常に最新かつ完全な状態に保つこと。なお、修正箇所については必要な説明を行うこと。

コ　受注者がリモートアクセスを行う場合は、必ず事前申請を行い、本市の許可を得ること。

サ　今後の運用中に調達機器と他の機器との接続及び別途調達したソフトウェアを本市がインストールするような場合、本市と密接に連絡が取れる体制を整備し、連絡があった場合は支援すること。

シ　保守対応は日本語で実施すること。

ス　年に１回、休日における停電作業を予定しているため、受注者保守対象の機器の安全な停止、起動及び動作確認を行うこと。なお、停電作業に伴い障害が発生した際には、必要に応じて保守対応を行うこと。

(2) 定期報告

本格稼働から四半期に１回、定例報告会を開催し、「保守作業報告書」「運用作業状況報告書」、必要に応じて「提案書」を提出すること。

(3) システムパフォーマンスの管理

ア　システム資源（CPU、メモリ容量、ディスク容量、ライセンス等）の利用状況監視を行い、必要な対策案（チューニング、リソースの追加等）の検討及び対策を実施すること。

イ　上記「ア」を実施する場合は、事前に本市と協議した上で実施すること。

(4) ソフトウェアのバージョンアップ

OS、ミドルウェア、アプリケーション、ソフトウェアのバージョンアップ、セキュリティプログラム等の適用に関しては、その適用の判断に必要な調査・評価を行い、本市に助言すること。

9　保守要件

(1) 基本要件

ア　本市の重大な過失によるトラブルを除き、全ての障害及び故障等を保守の対象とすること。

イ　必要に応じて、各メーカーと協力し、ハードウェア及びソフトウェアの保守対応を行うこと。

ウ　ハードウェアの修理又は交換を行う際に、ラックからの取り外しや、据え付け・調整作業が必要な場合は、実施すること。また、必要に応じて、本市と協議の上、設定内容の再投入など設定作業を行うこと。

エ　本市において使用する既存の端末及びプリンタ等の保守は、本業務の対象外とする。ただし、本業務で導入したクラウドサービス等に起因する事案については適宜対応すること。

オ　受注者が障害を検知した場合、または本市からのメールによる通報を受けた場合、長崎県内の事業所から90分以内に、システム復旧に必要な専門技術者が現地に到着し、保守作業を開始すること。なお、保守作業者は、本市の構成を理解し、障害原因の切り分けを行える技能を持つ者が行うこと。

カ　本業務で提案する機器に関して､ファームウェアの更新情報を定期的(最低月１回）に収集し、本市に情報提供を行うこと。

キ　稼働する各種サーバのOS及びミドルウェアに関して、パッチ等の更新情報を定期的（最低月１回）に収集し、情報提供を行うこと。

ク　パッチ、ファームウェアの更新情報については、適用要否と対応時期を提案し、本市と協議すること。

ケ　パッチやファームウェアの適用に際しては、テスト環境等による十分な影響調査を行った上で、本市と協議の上で適用すること。

コ　本業務で導入していないシステムのOS及びミドルウェアや各種ソフトウェアは各システムの保守業者が行うため本業務の保守要件の対象外とする。

サ　端末に対するWindowsアップデートや各種導入ソフトウェアのパッチ適用、バージョンアップを行うこと。

(2) インシデント対応

ア　システムの稼働監視及び障害監視を行い、障害が発生または検知された時は、速やかに状況を把握・分析し、障害箇所の特定を行うこと。

イ　障害発生時にシステム監視の結果検出された事象を記録、回避策を実施し、通常状態への早期復旧を図ること。

ウ　障害発生時、速やかに復旧を図ることができるよう緊急連絡体制等の連絡網を確立し、本市の承認を得ること。

エ　障害の発生に備え、データ等のバックアップ及びデータベースログの採

取等を行うこと。

オ　職員等から障害連絡を受けた時は、状況の把握等を行い、障害箇所の特定を行うこと。

カ　上記「オ」において、関係部署等への連絡を行うとともに、必要に応じて現地対応を実施すること。

キ　障害箇所が受注者の保守範囲外である場合は、当該箇所の保守業者と協力し、原因特定に努めること。

ク　受注者がサービスを提供するシステムの障害については、影響範囲の調査、初期対応、根本対応を行うこと。

ケ　受注者が本市に設置したサーバ等のハードウェア及びOS等の障害並びにネットワーク障害については、復旧対応作業について、各メーカーへの指示及び全体の進捗管理を行うこと。

コ　障害復旧後にアプリケーションをはじめとする各種ソフトウェアやデータの復旧作業を行うこと。なお、障害原因の切り分けを行える技能を持つ者が行うこと。

サ　障害及び災害等によりシステム異常等が発生した際の対策として、システムバックアップ及び業務データのバックアップを実施すること。

シ　各ハードウェア障害時には、当該機器またはそれを構成する部品等の調達・交換・修理等を迅速に行う等、受注者の負担により常時正常な稼動を保証すること。

ス　本業務ハードウェアに搭載された記録媒体に障害が発生した際に、当該機記録媒体を取り外し交換した場合、取り外した記録媒体については、受注者データを消去したうえで廃棄を行うこと。

セ　修理対応後、障害個所の修理又は交換後、機器が適正に機能するか動作確認すること。

ソ　発生した障害に対して解析を行い、根本原因を究明し、必要な場合は、再発防止策を検討すること。また、原因、影響範囲、対処方法、再発防止策を取りまとめ、報告書として本市に報告すること。

(3) 保守回線

ア　各システム等の保守について、庁外からのリモート保守が利用できる環境を構築すること。その際、利用する回線は本市が指定する回線を利用すること。また、行政機関用ネットワークを介して接続する場合は、本市と行政機関用ネットワーク保守業者と協議を行いながら構築すること。

イ　接続端末のエンドポイントセキュリティ（OSパッチ、ウイルス対策ソフト等）の適用状態を確認する機能を有すること。

ウ　本業務の保守業務にて保守回線を利用する場合は、下記の条件を満たすこと。

(ｱ) リモート保守端末は、本業務専用とし、他の業務との共用は一切しないこと。
(ｲ) リモート保守端末から保守業務以外のインターネット利用は行わないこと。
(ｳ) リモート保守端末には、十分なセキュリティ対策を施し、これを維持すること。
(ｴ) 利用実績について定期的に報告を行うこと。
(ｵ) リモート保守端末の設置時および本市が必要と判断した際に設置状況の査察を受け入れること。

10　付帯作業

(1) プロジェクト管理

ア　管理に要する成果物の作成

契約後、以下の資料を作成し、本市の承認を得ること。

(ｱ) プロジェクト計画書

以下を定義したプロジェクト計画書を作成すること

a　プロジェクト内容の定義

(a) 本業務の目的と達成すべき事項
(b) 進捗管理の目的と内容
(c) 各作業工程の目的と内容
(d) 品質管理の目的と内容
(e) 本市と関連事業者との間で調整が必要な事項
(f) 本業務実施に当たっての想定リスクと回避方法
(g) 本業務の関係者とその役割

b　プロジェクト管理要領

(a) 成果物作成に関する規則
(b) 機器取り扱いに関する規則
(c) 成果物作成から本市承認に至る業務フロー

(ｲ) 進捗管理

a　全体スケジュール

本業務に関する作業工程を、開始から終了まで網羅的に確認できるスケジュール表を作成すること。

b　進捗管理簿

上記スケジュールを作業内容もしくは成果物単位で分割し、各工程が視覚的に確認できる線表を作成すること。

なお、線表については、作業工程進捗状況に合わせて段階的に詳細化することを前提とする

(ｳ) 体制表

本業務にかかる定期的な進捗報告課題管理を行える体制を整え、要員の役割（責任者、担当窓口など）を明示すること

(ｴ) 課題管理表

本業務実施に当たって、検討や確認が必要となる事項及び本市に提示済みの成果物の変更について網羅的に記載された資料を作成すること。

(ｵ) 議事録

「(1)－イ」のほか、本市及び関連事業者との間で連絡及び調整した内容について記載された資料を作成し、提出すること。

イ　会議体

以下の会議体を開催し、必要となる資料は本業務の範囲内で都度作成すること。

(ｱ) 定例会

a　開催頻度

構築期間中は月１回以上とし、保守運用期間中は四半期に１回とすること。

b　議題

(a) 進捗状況報告

(b) 各種成果物のレビュー及び承認

(c) 課題及び調整事項の検討

c　出席者

(a) 本市が体制表を基に指定するもの

(b) 受託者が出席を希望する社員等及び関連事業者

d　場所

本市が都度指定する場所（Webでの実施も可能）

(ｲ) 個別検討会

受託者が必要に応じて開催するものとする。ただし、電子メール及び電話等により代替することも可能とする。

ウ　工程管理

米国PMI（Project Management Institute：プロジェクトマネジメント協会)が策定したPMBOK 第５版(Project Management Body of Knowledge:プロジェクトマネジメント知識体系ガイド）に準拠した工程管理を行うこと。

(2) 教育

提供されるクラウドサービスに関する以下の内容で教育を行うこと。

ア　クラウドサービス等の運用管理業務について運用管理者に教育を行うこと。

イ　本業務で提案するサービスについて、各職員向けの研修会を実施すること。

ウ　教育内容および方法等については、受託後、本市と協議すること。

(3) 留意事項

ア　付帯作業において本仕様書の内容とは別に必要となるサービスがある場合は、その調達については本業務に含めること。

イ　サービス提供において他のシステムやネットワークに対する影響がないように、あらかじめ調整をすること。

ウ　クラウドサービスの稼動に必要なソフトウェア等の設定等の技術支援についても、本市からの依頼に基づき確実に実施すること。

11　成果物

(1) 本業務履行に向けた各工程の計画､成果を示す以下のドキュメントを作成し、期日までに納品すること。

No.	成果物名称	内　容	期　日
1	プロジェクト計画書	・作業計画 ・業務体制 ・役割分担	契約後 14 日以内
2	基本設計書	・仕様書及び調査に基づいて定義及び設計した基本方式設計 ・機器管理資料 ・システム構成（物理図及び論理図）	令和７年 ６月末
3	詳細設計書	・各環境定義 ・機器設置図（ラック搭載図）	令和７年 ７月末
4	完成図書	・設置写真（前後） ・機器デザインシート ・ハードウェア構成図及び一覧 ・保証書等一式 （登録ユーザ ID やパスワード等の管理表も含む）	令和７年 ８月末
5	データバックアップ手順書	・各種サービス等のバックアップ手順	令和７年 ８月末
6	復旧手順書	・各種サービス等のリストア手順	令和７年 ８月末
7	障害対応手順書	・障害対応手順（障害切分対応含む）	令和７年 ８月末

8	操作・運用 マニュアル	・機器操作等に関するマニュアル	令和７年 ８月末

(2) ドキュメントの内容に関しては本市に対しレビューを行い、内容の承認を得てから納品すること。
(3) 各種ドキュメントについては電子ファイルを前提とし、磁気媒体（CDも可）と紙面でそれぞれ２式を納品すること。なお、磁気媒体での納品については、本市と事前に協議を行うこと。

12　契約不適合責任

(1) 検収完了後、本業務成果物について仕様書との不一致（バグも含む。以下本条において「契約不適合」という。）が発見された場合、本市は受注者に対して当該契約不適合の修正等の履行の追完(以下本条において「追完」という。)を請求することができ、受注者は、当該追完を行うものとする。ただし、本市に不相当な負担を課するものでないときは、受注者は本市が請求した方法と異なる方法による追完を行うことができる。
(2) 上記(1)にかかわらず、当該契約不適合によっても個別契約の目的を達することができる場合であって、追完に過分の費用を要する場合、受注者は前項所定の追完義務を負わないものとする。
(3) 本市は、当該契約不適合（受注者の責めに帰すべき事由により生じたものに限る。）により損害を被った場合、受注者に対して損害賠償を請求することができる。
(4) 当該契約不適合について、追完の請求にもかかわらず相当期間内に追完がなされない場合又は追完の見込みがない場合で、当該契約不適合により個別契約の目的を達することができないときは、本市は本契約及び個別契約の全部又は一部を解除することができる。
(5) 受注者が「12 契約不適合責任」に定める責任その他の契約不適合責任を負うのは、前条の検収完了後１年以内に本市から当該契約不適合を通知された場合に限るものとする。ただし、前条の検収完了時において受注者が当該契約不適合を知り若しくは重過失により知らなかった場合、又は当該契約不適合が受注者の故意若しくは重過失に起因する場合にはこの限りでない。
(6) 上記(5)にかかわらず、検査によって本市が当該契約不適合を発見することがその性質上合理的に期待できない場合、受注者が「12 契約不適合責任」に定める責任その他の契約不適合責任を負うのは、本市が当該契約不適合を知った時から１年以内に本市から当該不適合を通知された場合に限るものとする。
(7) 上記(1)から(6)の規定は、契約不適合が本市の提供した資料等又は本市の与

えた指示によって生じたときは適用しない。ただし、受注者がその資料等又は指示が不適当であることを知りながら告げなかったときはこの限りでない。

13　その他

(1) 本業務に携わる要員は、設定障害対応が十分可能なSEを従事者とし、従事者を変更する場合は、十分な引継ぎを行い業務に支障をきたさないようにすること。

(2) 本契約について、契約書及び仕様書に明示されていない事項でも、その履行上当然必要な事項については、受託者が責任をもって対応すること。

(3) 本仕様書に記載されているすべての作業に対し、いかなるケースにおいても本市に対し、別途費用を請求することはできない。ただし、本市の要求仕様変更が生じた場合については別途協議を行うこととする。

(4) 機器納入を行ううえで必要となる関係部局、関係機関との調整用資料等を作成し、必要に応じて打合せ等に出席すること。

(5) 必要に応じ、本市にかかわるSI業者、ネットワーク業者、ハードウェア業者及び関連する委託業者若しくは保守業者等と調整、確認を行うこと。

(6) 機器納入等に伴う付帯作業等に対する契約不適合責任の期間は、本市の検査終了後１年間とし、その期間内は速やかに対応すること。

(7) 機器納入等に伴うシステムの設定運用に際しては、本市が定めた情報セキュリティポリシー、平戸市個人情報の保護に関する条例（令和４年平戸市条例第49号）等、各種規定を遵守すること。

(8) 納入業者は、何人に対しても、契約期間中、又は、契約期間終了後を問わず、業務上知りえた本市の業務の一切を漏らしてはならない。

(9) 本仕様書の記載内容に疑義が生じた場合は、本市と協議をすること。

(10) 本仕様書に記載されていない事項は、本市の指示に従うこと。

(11) 受託者は、業務の履行にあたって、暴力団、暴力団関係者又は暴力団関係法人等（以下「暴力団等」という。）による不当介入を受けたときは、次の義務を負うものとする。

ア　断固として不当介入を拒否すること。

イ　警察に通報するとともに捜査上必要な協力をすること。

ウ　本市に報告すること。

エ　業務の履行において、暴力団等による不当介入を受けたことにより工程、納期等に遅れが生じる等の被害が生じるおそれがある場合は、本市と協議を行うこと。

(12) 受託者が上記(11)のイ又はウの義務を怠ったときは、平戸市各種契約等における暴力団等の排除措置に関する要綱（平成24年平戸市告示第69号）第３条の規定により入札参加排除の措置を講じる。