高島市校務支援システム更新業務
仕　様　書

令和７年５月

高島市教育委員会事務局

教育指導部　学事施設課

目　次

1. 業務名

高島市校務支援システム更新業務

2. 業務の背景・目的

本市教育委員会事務局（以下「本市」という。）では、市内１９小中学校教職員の業務の効率化、事務負担の軽減および行政事務コストの削減を図るため、令和元年度にセンターサーバや統合型校務支援システム等（以下「現行システム」という。）を自庁設置方式（オンプレミス）により構築し運用している。

本業務は、現行システムのサーバ機器等の経年劣化や保守期間終了によるハードとソフトの問題に対処するとともに、システム管理担当者の負担軽減および情報セキュリティ対策の機能強化を図るため、クラウドサービスを主体とするシステム（以下「新システム」という。）に更新することを目的に実施するものである。

3. 基本方針

(1) ゼロトラスト環境の構築

文部科学省の「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）」（以下「ガイドライン」という。）で示されている「認証、暗号化、不正アクセスの監視等による強固なアクセス制御を前提とする対策を講じたシステム構成（以下「ゼロトラスト」という。）」を構築することにより、校務支援システムへのセキュアな接続環境を整備する。

(2) パブリッククラウドの利用

市所有設備にかかる保守管理の負担を軽減するため、市役所本庁舎 3F 電算室内に極力サーバ等の機器を置かず、インターネットを通信経路とする外部のクラウドシステム（以下「パブリッククラウド」という。）のサービスを利用することを基本とする。

(3) データ共有の円滑化

校務系ネットワーク（校務支援システム等を利用）と学習系ネットワーク（１人１台タブレット端末：iPad を利用）との物理的なネットワーク分離を当面は継承しつつも、ゼロトラスト環境の構築とパブリッククラウドの利用によって、校務系と学習系とのネットワーク間でのデータ共有の円滑化を図る。

4. 現行システム等が抱える課題

(1) https でセキュアに接続するためのゼロトラスト環境が未構築

校務支援システムにアクセスする際、通信経路での第三者による情報の盗聴や改ざんのリスクを防止し安全に通信を行う SSL（暗号化通信）環境がない。

(2) 校務系ネットワークと学習系ネットワークとの物理的分割

① 校務系・校務外部接続系ネットワーク、学習系ネットワークとのデータのやり取りの煩雑さ

② 校務系ネットワーク集約による通信速度低下の懸念

③ 校務系ネットワークへの有線 LAN 接続による校務執務場所の固定化

(3) オンプレミス型システムでの運用

① 校外からのアクセス禁止によるリモートワーク等が不可
② 災害時やパンデミック時の事業継続性（BCP）

(4) 端末スペック不足および管理面の課題

① 多要素認証対応デバイス未搭載によるゼロトラスト環境非対応
② 未知の脅威に対する対応

5. 業務期間

(1) 準備期間

契約締結の日から令和８年２月２８日までとし、新システムの構築、稼働テスト、データ移行、現行システムからの切替等の作業を行う準備期間とする。

(2) 切替期間

準備期間のうち、令和８年２月２１日から２月２８日までの８日間（予備日含む）を、現行システムから新システムへの切替期間とする。この期間中に現行システムを停止し、新システムが暫定稼働することになる。

(3) 運用期間

令和８年３月１日から令和１３年２月２８日までの５年間とする。

試験稼働：　令和８年３月１日から３月３１日までの１ヶ月間
本稼働　：　令和８年４月１日から令和１３年２月２８日までの５９ヶ月間

また、運用期間を終了しても、本市が指定する期間で引き続き契約を延長（１年間の契約延長を想定）できるとともに、その際には、契約のサイクル等が要因の違約金は発生しないこと。

6. システムおよびネットワークの構成

(1) システムの基本構成

新システムの構成は、上記 3.基本方針に掲げるゼロトラスト環境の構築とパブリッククラウドの利用を基本とする。別紙１「教育ネットワーク概要図（校務系および学習系)」、別紙２「校務系ネットワークと校務システムの活用イメージ」を参照すること。

(2) ネットワーク基盤

① 現行システム

現行システムでは、庁内イントラネットワーク（有線 LAN、市情報政策課で管理）に校務系ネットワーク環境（校内有線 LAN）を構築し、校務系および校務外部接続系の２つのセグメントに論理分割され、校務系セグメントは機微情報や個人情報を取り扱うため、インターネットへの接続はできない。また、校務外部接続系から校務系への接続は、仮想デスクトップを用いている。

なお、１人１台タブレット端末を利用する学習系ネットワーク環境（通常は、WiFi＋Cellular モデルの iPad 端末で４GLTE 回線サービスを利用。別途 iPad OS のアップデート等のため、校内職員室等に無線 LAN を構築）とは物理的に分離されており、現時点では両ネットワークの統合はされていない。

② 新システム

ア）ネットワーク構成

新システムでは、インターネットを経由しパブリッククラウドへアクセスする必要があるが、庁内イントラネットを継続利用することで通信料の低減と情報セキュリティ対策の強化を図る。

ネットワーク構成は校務外部接続系がベースとなるが、設計については、現行システムの状況を踏まえて、本市と提案者が協議した後、庁内イントラネットの運用保守に携わる事業者を入れた三者で調整を行う。また、庁内イントラネットにかかるネットワークの設定変更等については、下記イ）ネットワーク基盤の再構築において当該事業者が実施する。

- 新システムのネットワーク構成について、ゼロトラスト環境の構築とパブリッククラウドの利用を前提に、最適と考える提案を行うこと。
- 本市との契約締結後、現行システムの導入・運用保守に携わる事業者との連携を密にして、現行システムのコンフィグ環境を把握しておくこと。
- 庁内イントラネットの運用保守に携わる事業者との連携を密にして、本市のイントラネット環境の状況を把握しておくこと。

イ）ネットワーク基盤の再構築　　※別業務で対応

インターネットへの接続回線および支所～学校間の通信回線の増速について検討中であり、これらのネットワーク基盤の再構築に関しては、本業務の調達範囲には含まない。

7. 本業務の調達範囲

本業務の調達範囲は、クラウドシステムの構築業務と、システムが安定的に稼働するうえで必要な運用保守業務とする。

(1) 運用要件

① ユーザー数

ア）校務系ネットワークからのユーザー

校務 PC 端末を用いて、下記 9.システム要件(1)クラウド基盤で導入する Microsoft365 A5 Education Faculty（以下「M365 A5」という。）の認証基盤、Office アプリ（Word、Excel、PowerPoint 等)、共有ストレージおよび(2)個別システム等の本業務で構築するクラウドシステム全般にアクセスする者（学校教職員と教育委員会事務局職員等）は、最大 380 名である。

イ）学習系ネットワークからのユーザー

別紙３「タブレット端末等納入場所一覧」に記載する学習用１人１台タブレット端末を用いて、M365 A5 の認証基盤、Office アプリ、共有ストレージにアクセスする者（学校の児童生徒、教職員および教育委員会事務局職員等）は、最大 3,250 名である。ただし、個別システムにはアクセスしない。

② 端末台数

現行システムでは、教職員が校務 PC 端末（全ての端末の OS が Microsoft Windows10 Pro）を 370 台利用しているが、OS のサポート終了（令和 7 年 10

月 14 日）を考慮し、令和６年度から計画的に Windows11 Pro に端末を更新しており、令和９年度には全て置き換わる予定である。

③ 利用時間

新システムを利用する時間は、基本的に 24 時間 365 日とする。

ただし、新システムの停止が必要な保守作業時（バックアップおよびシステム稼働に必要な再起動等）は除くものとする。

(2) 関係事業者

① 事業者との連携調整

新システムの構築にあたっては、以下の関係事業者との情報共有を密にし、相互の責任分界点で不明瞭な箇所が発生しないように努め、問題が発生した場合は、提案者が主体的に問題解決を図ること。

特に、現行システムのコンフィグ環境および庁内イントラネット環境、共有ストレージ（ファイルサーバ）のフォルダ構成・アクセス権限などは、十分な事前確認が必要である。

② 事業者名

- 現行システム（校務支援システム）の導入・運用保守に携わる事業者：
  ㈱内田洋行　教育 ICT 事業部 西日本第１営業部
- 庁内イントラネットの運用保守に携わる事業者：
  NEC ネッツエスアイ㈱ 京滋支店
- 庁内イントラネット、インターネット回線のネットワーク提供事業者：
  ㈱オプテージ ｿﾘｭｰｼｮﾝ事業推進本部 公共営業部 自治体営業チーム
- 現行タブレット端末の導入・運用保守に携わる事業者：
  ソエダ㈱および SB C&S㈱ ICT 事業本部 ｴﾃﾞｭｹｰｼｮﾝ ICT 統括部 営業推進部
- 学習系ネットワーク（無線 LAN）の運用保守に携わる事業者：
  富士電機 IT ソリューション㈱　西日本事業本部 京都支店
  富士通ネットワークソリューションズ㈱　ﾋﾞｼﾞﾈｽｲﾉﾍﾞｰｼｮﾝ本部

(3) システム構築業務

① プロジェクト管理等

ア）プロジェクトおよびシステム構築体制

- 契約締結後、以下の②要件定義～⑥研修会の開催、ならびに(4)運用保守業務までの一連の作業をプロジェクトと捉え、スケジュール管理、品質管理、リスク管理等、プロジェクトの推進および管理に必要な事項の方針について、「プロジェクト計画書」に取りまとめて事前に文書で提出し、本市の承認を受けること。
- プロジェクトに携わる全ての人員（再委託先があれば含む）について、所属、氏名、役割、メールアドレス等を記載した構築体制表を、速やかに提出すること。人員の変更が発生するたびに修正版を作成し、差し替えること。

イ）構築定例会議

- 毎月１回、定例会議（オンライン会議を可）を開催し、新システム構築にかかる各プロジェクトやスケジュールの進捗状況、課題等を報告すること。

・　協議に必要な資料は提案者が作成し、前日までに本市へ提出すること。
・　課題や懸案事項は課題管理表に整理のうえ、本市との今後の協議に臨むこと。
・　定例会議後に会議録を作成し、その内容について本市の承認を受けること。

② 要件定義 ～ 構築・導入

・　本業務で構築する新システムが円滑・迅速に導入され、かつ、適正に運用されるよう、調査（現行システムのコンフィグ環境の確認等）、新システムおよびネットワークの設計について、提案者の責任と負担において実施すること。
・　現行システムのコンフィグ環境を踏まえて、提案者側から新システムでの推奨値を示し、本市の要望をヒアリングすること。また、本市と協議し決定したパラメータ値に従って、新システムにかかる各種設定作業を行うこと。
・　システム設計（基本、詳細、セキュリティ、移行、運用等）およびネットワーク設計（物理構成、論理構成）を実施すること。
・　各設計にて作成した要件定義書および設計書を本市へ提出すること。
・　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。
・　本業務で調達するハードウェア以外に、提案者が必要とするハードウェアの調達を別途行った場合は、契約期間終了後にハードウェアを本市へ無償譲渡すること。
・　本仕様書に特に記載する場合を除き、準備期間中におけるソフトウェアのライセンス費用等については、提案者側の負担とすること。

③ 稼働テスト

・　本市との協議により作成した要件等に定めるアクセス制御等のセキュリティの諸設定について、設計どおりに動作するかテストすること。
・　現行システムから新システムへの移行を円滑かつ着実に行うため、テストは本番運用の環境において実施し、各種テストを入念に実施して切り戻しのないようにすること。
・　本業務では、テスト環境の調達は想定していない。本番運用環境とは別にテスト環境を用意する場合は、その費用は提案者の負担で構築すること。
・　テストの実施にあたっては、テスト実施計画書を作成し本市の承認を得た後、その実施結果をテスト結果報告書に取りまとめて本市へ提出すること。

④ データ移行

ア）現行システムからのデータ移行

現行システムの運用終了後、その保存データの一部を新システムへと移行する必要がある。本市および現行システムの導入・運用保守に携わる事業者との連携を密にして、本市が求めるデータを新システムへと移行する作業について、効率的な実施時期およびツール等の手法を提案すること。

イ）新システム運用終了後のデータ移行

本業務で構築・導入した新システムの環境およびデータ等は今後、運用終

了後に名義変更等による管理権限の引き渡しにより、本業務の提案者以外への引き継ぎを可能にするとともに、データ抽出等の移行に必要な作業は、本業務の契約範囲内で無償にて実施すること。

⑤ マニュアルの作成

システムの設定手順や操作手順、運用に関するマニュアルを作成し、後日でも随時確認ができるようにすること。マニュアルに記載する内容に変更があった場合は、随時差し替えを行うこと。

⑥ 研修会の開催

ア）管理担当者向け

- 本業務の準備期間中（令和８年２月２８日まで）に、新システムに関する管理担当者向けの研修会を開催すること。また、その内容や手法、回数等について研修計画書を作成し、本市と協議のうえ決定すること。
- 管理担当者向けの研修資料は電子データで納品することとし、印刷は不要とする。

イ）教職員向け

- 本業務の運用期間（試験稼働：令和８年３月１日から３月３１日まで）に、新システムに関する教職員向けの研修会を開催すること。また、その内容や手法、回数等について研修計画書を作成し、本市と協議のうえ決定すること。
- 教職員向けの研修資料は電子データで納品することとし、印刷は不要とする。また、研修会で教職員から受けた質疑等については、本市と協議のうえ回答を作成すること。

※ １回あたりの研修時間は最大で２時間 30 分程度、想定参加人数は最大 60～70 人程度、５回開催を上限と想定

(4) 運用保守業務

① システム保守

ア）基本事項

- 本業務で調達・構築した新システムおよびネットワーク機器等にかかる業務全般を、運用保守業務の範囲とする。
- 別業務で調達した 9.システム要件(3)ネットワーク機器等③その他機器ア）校務 PC 端末およびイ）校務プリンタについて、ハードウェアの故障・障害が発生した場合の現地訪問対応（市内１９小中学校および教育委員会事務局での現地作業。以下同じ）は不要だが、本市管理担当者からの問い合わせに対して、技術的助言や支援等を行うこと。
- 新システムはパブリッククラウドの利用が基本となり、本庁 3F 電算室に設置する 9.システム要件(3)ネットワーク機器等②納入機器ア）ファイアウォール、市内１９小中学校および教育委員会事務局に設置するイ）校内 LAN 用スイッチを除いて、システム障害等発生時において、提案者の保守作業者が本市へ来庁する機会はほとんどない。

したがって、リモート保守の必要性、来庁しての現地訪問対応も含めて、新システムおよびネットワーク機器（ファイアウォール、校内 LAN 用スイッ

チ）の最適な保守方法について提案すること。

イ）運用保守体制

・　運用保守に携わる全ての人員（再委託先があれば含む）について、所属、氏名、役割、メールアドレス、緊急連絡先等を記載した運用保守体制表を、契約締結後に速やかに提出すること。

・　新システムの運用保守を統括する全体統括者を置くこと。

　全体統括者は、新システムの運用状況を保守定例会議において本市へ報告するとともに、新システムの維持・向上を図るため、継続的な運用改善の提案を行い、本市の承認を得て、その改善策を推進させること。

・　システム利用にかかる致命的な障害等が発生した場合を想定し、契約締結後、本市からの緊急連絡受付窓口の電話番号を速やかに提示すること。

・　人員の変更が発生するたびに修正版を作成し、差し替えること。

ウ）システム障害およびセキュリティインシデント等の発生時の対応

・　新システムの運用開始以降、システム障害およびセキュリティインシデント等の発生状況を 24 時間 365 日監視し、異常を検知した場合には、本市へ速やかに電話、電子メール等で通知すること。

・　教職員の業務に重大な影響を及ぼすシステム障害、セキュリティインシデント等が発生した場合には、本市と協議のうえ、業務時間外や休日等も含めて、障害切り分け作業、障害復旧作業（学校への現地訪問対応を含む）等の迅速な対応を実施すること。

・　システム障害およびセキュリティインシデント等が発生した場合における本市と提案者の役割分担等を示して、システム障害等対応マニュアルを作成し提出すること。

・　本市の求めに応じて、障害等の原因究明や技術的助言および支援等を行うこと。

・　障害復旧後に原因の分析、実施した対処・措置、再発防止策（サービス低下防止策）等を記載した障害対応報告書を作成し、概ね 7 営業日以内に提出すること。

エ）セキュリティメンテナンス

・　新システムおよびネットワーク機器（ファイアウォール）への更新プログラム適用やアップデート等にかかる情報を随時提供するとともに、本市の求めに応じて技術的助言および支援等を行うこと。

　※　別業務で調達した校務 PC 端末、校務プリンタの情報提供を含むものとするが、更新プログラムの適用やアップデート等の作業については、本市管理担当者が資産管理システムを用いて行う。

・　脆弱性にかかる情報は、本市および提案者双方が迅速に共有のうえ、可能な限り早期に更新プログラム等を適用できるようにすること。

・　ソフトウェアのライセンス更新等に伴う各種手続きを支援すること。

・　計画的なシステムの停止が発生する場合は、１週間前までに本市へ事前に通知すること。

オ）ヘルプデスク

・　新システムの運用期間中において、ユーザーからの操作方法、システム障害発生等の問い合わせに対応するためのヘルプデスク（コールセンター）を設置すること。
・　本市からの問合せに対し、随時回答または連絡を受けた翌営業日までに、一次回答を行うこと。ただし、障害発生等緊急の対応が必要な場合は、迅速な対応を行うこと。
・　平日の９時～１７時に、電話・メールによる障害の受付、切り分け、エスカレーションに対応可能であること。ただし、時間外に受付けた問い合わせの対応については、翌営業日以降とする。
・　ヘルプデスク専用の電話番号を用意し、必要に応じて複数回線を用意すること。（時期による増減は可）
・　迅速な問い合わせ対応ができるよう十分な人員を確保すること。
・　ヘルプデスクでの対応スタッフには、事前に研修等の教育を十分に行い、問い合わせの際にシステム利用者が混乱しないよう迅速かつ正確な対応を行うこと。
・　ヘルプデスクへの問い合わせおよび回答の内容について、一案件ごとに必要な項目を記録し、全件蓄積・保管すること。下記④保守定例会議で本市へ報告・提出すること。

カ）リモート保守

・　本市への提案により、リモート保守を行う場合には、専用線、閉域網、あるいは暗号化された通信による接続方式の提案を行い、本市の承認を得ること。
・　リモート保守を行う場合、その対象を明確にして、事前に本市へ説明し、本市の承認を得ること。
　※ ネットワーク機器（ファイアウォール）、クラウド基盤、個別システム（①統合型校務支援システム、②教育系グループウェア、③資産管理システム）、その他
・　リモート保守環境に必要となる通信回線、機器およびライセンス等の費用はすべて提案者の負担とし、契約締結時にリモート保守対応にかかる覚書を締結すること。
・ 本市の新システム（ファイアウォール、クラウド基盤および個別システム）へリモート保守のため接続する際は、グローバル IP アドレスや保守用アカウントによる制御、本市と同等のセキュリティ対策を講じること。
・　リモート保守作業を行う場合、事前にリモート保守作業計画書を提出し、本市の許可を得たときのみとすること。ただし、緊急時の場合は、本市へ電話連絡することにより許可するものとする。

② 年次更新

教職員の異動等に伴う以下の作業について実施、または、本市の求めに応じて技術的助言および支援等を行うこと。

・　校務支援システムにおける年次更新処理（教職員の異動および児童・生徒の

進級処理）作業の支援。実作業は、小中学校の担当者が行う。
- 教育系グループウェアのユーザー登録、年次更新処理（教育委員会事務局職員を含む）
- 各種基本設定の管理、設定書の作成・更新（随時）

③ 運用支援

本業務で構築した新システムの機能や活用方法等について、教職員および教育委員会の業務効率化に資する場合には、随時情報提供し支援すること。

④ 保守定例会議

ア）定例会議（令和８年度）

新システムの本格運用の初年度となる令和８年度は、引き続き毎月１回の会議（オンライン会議を可）を開催し、運用・保守状況や課題等について報告および協議すること。

また、月次の運用状況レポート（インシデント報告含む）を、Excel 形式データで本市へ翌月１０日までに提出すること。

イ）定例会議（令和９年度以降）

令和９年度以降は、四半期に１回を目途に会議（オンライン会議を可）を開催し、課題の進捗状況等を中心に報告および協議すること。

なお、月次の運用状況レポート（インシデント報告含む）については、引き続き Excel 形式データで本市へ翌月１０日までに提出すること。

ウ）臨時会議（緊急的な課題解決）

運用期間中において、新たに緊急的に対応を要する課題や検討事項が発生した場合には、提案者による運用環境のアセスメントや改善策の提案等を受けて、本市と提案者において課題等解決のための会議（オンライン会議を可）を随時開催すること。

8. 業務の実施場所と学校関係者数

市内１９小中学校、本市の本庁舎（2F 教育委員会事務局、3F 電算室）とする。

また、市内１９小中学校の名称と住所、教職員数および児童生徒数については、別紙３「タブレット端末等納入場所一覧」を参照すること。

9. システム要件

市内１９小中学校および教育委員会事務局（本庁舎新館 2F）のユーザーを対象とするクラウド基盤および個別システムを構築すること。なお、各システムに関しては「別紙４：システム機能要件表」に基づき、「標準対応」と「オプション対応」のいずれかに「○」を付したうえで、公募型プロポーザルへの参加申込時に本市に提出すること。

(1) クラウド基盤

① 基本事項

- クラウド基盤は M365 A5 の導入を必須とし、これに含まれる諸機能を用いて、ゼロトラスト環境の構築に必要な機能を実現するものとするが、当該ライセンスだけでは機能が不足する、または、操作性に難があるなどの場合には、別途必要なライセンスやツール等を提案すること。
- 9.システム要件(3)ネットワーク機器等に記載する UTM（統合脅威管理）機能を有するネットワーク機器（ファイアウォール）を本業務で調達する。端末認証やアクセス制御の機能強化、ネットワーク通信負荷の低減を図るため、クラウド基盤と UTM との連携によるゼロトラスト環境の構築について提案すること。
- クラウド基盤システムのバックアップ対策について提案すること。

② 調達ライセンス

M365 A5： 380 ライセンス

- 当ライセンスは、校務 PC 端末（Windows10 Pro または Windows11 Pro）のユーザー（学校教職員と教育委員会事務局職員等）380 名が利用するが、その他として、学生無償ライセンス特典“Student Use Benefit”の付与により、当ライセンスに紐付けする形で、学習用１人１台タブレット端末のユーザー（児童生徒、教職員および教育委員会事務局職員等）最大 3,250 名も利用できるようにすること。

  なお、準備期間中にクラウド基盤を構築し各種設定を行う必要があることから、ライセンスの調達期間は、令和７年１１月１日から令和１３年２月２８日までの６４ヶ月とする。

※ 令和７年度に別業務において、現行の学習用１人１台タブレット端末（iPad6 と iPad8 の合計 3,540 台）を更新し、令和８年１月５日から２月２８日までの間に新端末（iPad11 を想定）への入れ替えを行う予定である。

※ 当タブレット端末の更新について、別業務の受注者との連携を密にするとともに、新旧端末の入れ替えスケジュールに支障が出ないよう、本市および別業務の受注者と調整しながら、クラウド基盤の構築を進めること。

③ 必要な機能

- 以下のア）～ク）の各機能の項目について、機能の実現性、無償または有償の区分、有償の場合はその費用(導入費用＋5 年間運用費用)を示すとともに、提案者の考える最適なゼロトラスト環境を提案すること。
- ゼロトラスト環境の構築にあたり、ア）～ク）の機能以外に、提案者が必要

と考える機能があれば、その機能の必要性、機能の詳細内容、無償または有償の区分、有償の場合はその費用（導入費用＋5 年間運用費用）を示して提案すること。

ア）認証基盤（IDaaS 等）

- 複数のサービス（Web サービスやアプリケーション）に登録されている ID とパスワードの一元管理、ならびに各システムへの認証をクラウドサービスにて行う（IDaaS：Identity as a Service）としての機能を備えること。
- 人事異動等の発生時に、本市によるアカウントの随時追加、削除、編集等が可能であること。
- 現行の Microsoft アカウント情報（児童生徒含む〇〇アカウント程度）を引き継ぐとともに、本市が業務利用する各システムおよびサービスとのシングルサインオン連携またはユーザー情報連携が可能であること。
  ※ 現行では、校務 PC 端末は Microsoft Office LTSC Standard を、タブレット端末（iPad）は Microsoft Office 365 A1 を利用しており、これらの状況を踏まえて、M365 A5 の環境で Office アプリ（Word、Excel、PowerPoint 等）が利用できるようにすること。
- 生体情報（顔）および知識情報（PIN またはパスワード）の２つを組み合わせた多要素認証が可能であること。また、非常の際には、多要素認証を利用せずに、業務端末へログインできる設定が可能であること。

イ）アクセス制御

- 事前に定義した不正アクセスパターンとのマッチングにより、クラウド等への不正なアクセスを検知（IDS：Intrusion Detection System）または遮断（IPS：Intrusion Prevention System）できること。
- 個人契約のテナントやシャドーIT 等、セキュリティ上懸念があるサービス等へのアクセスを制御できること。

ウ）フィルタリング

- 認証基盤（IDaaS）と連携するとともに、悪質な Web コンテンツやアプリケーション等へのフィルタリングが可能であること。
- フィルタリング設定のテンプレートが用意されているとともに、グループごとのルール設定やホワイトリスト運用が可能であること。

エ）アンチウィルス

- パターンマッチングの他、機械学習やふるまい解析等の技術により、既知または未知にかかわらず、不審な挙動をするマルウェア等の検知や遮断が可能であること。（ふるまい検知）
- 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などの不審な挙動をするプログラムの検知や感染拡大の防止（EDR：Endpoint Detection and Response）が可能であること。
- 認証基盤（IDaaS）と連携するとともに、脅威が検出された時は、即座にメール等で管理担当者へ当該校務 PC 端末やユーザー情報等を通報できるこ

と。
・　随時、最新のセキュリティ状態に更新できること。
・　脅威の侵入経路等について、トラッキングが可能であること。

オ）デバイス管理（MDM 等）

・　校務 PC 端末のデバイス管理を行う。なお、以下の機能について、9.システム要件(2)個別システム③資産管理システムの機能と重複する場合は、システム管理担当者の運用負担とならないよう、手順書（マニュアル）に記載するなど配慮すること。

※　令和７年度に別業務において、現行の１人１台タブレット端末を更新し、その中でタブレット端末専用の MDM を別途調達する予定である。

・　校務 PC 端末に対して、アプリケーションの一斉配付や Windows Update 等の一斉管理ができること。その際、配付の時間帯等を本市が任意に指定できるとともに、ネットワーク等の負荷分散を図る機能を備えること。
・　校務 PC 端末を紛失した際、遠隔操作にて当該端末内の特定フォルダのデータ消去等ができること。
・　ユーザーからの操作方法等の問合せ時に、管理担当者が当該ユーザーの校務 PC 端末にリモートでアクセスし、両者が当該端末画面を確認しながら管理担当者による操作ができること。

カ）共有ストレージとデータファイルの暗号化

a）　現行システム等（ファイルサーバ）の構成

➢ 校務系セグメントの配下に校務系ファイルサーバを構築

仮想基盤上にファイルサーバを構築し、全体共有領域は 2TB、各校内の共有領域は 500GB×19 校＝9.5TB、合計 11.5TB でクォーターを設定。

原則、全体共有領域は全校からアクセス可能とし、各校の領域は、その該当校に所属の教職員のみからアクセス可能。また、複数校を掛け持つ拠点校指導員が数名おり、複数校へのアクセス許可設定。

➢ 校務外部接続系セグメントの配下に校務外部接続系ファイルサーバを構築

Synology社のNASを導入し、ファイルサーバを構築。

全体共有領域は5TB（教材ファイル共有1TB、デジタル教材共有4TB)、各校共有領域は1.5TB×19校＝28.5TB、合計容量33.5TBを割り当て。

各校のフォルダ内には、デジタルカメラ等の記録用画像データを保存する「画像フォルダ」、授業準備等で用いる「指導・事務フォルダ」の２つを作成し、適切にアクセス制御。

全体共有領域は、全校からアクセス可能。各校の領域は、その該当校に所属の教職員のみからアクセス可能。また、複数校を掛け持つ拠点校指導員が数名おり、複数校へのアクセス許可設定。

➢ 学習系タブレット端末（iPad）

Office 365 A1ではOneDrive、SharePointOnline、Exchange　テナント全体で100TBが利用可能（OneDriveの上限は最大100GB）だが、全体の使用容量は3,540台で3TB程度である。

b) 新システム（クラウドストレージ）

- 校務系ネットワーク（校務 PC 端末）および学習系ネットワーク（学習用１人１台タブレット端末)のユーザーがインターネット経由でアクセスするクラウドストレージは、全体領域として 138TB 程度（基本 100TB＋380 ユーザー×100GB）のディスク容量を備えること。
- クラウドストレージのフォルダ構成およびアクセス権限等は、認証基盤（IDaaS 等）と連携して、ユーザーの職位やグループごとに柔軟に設定できるとともに、本市との協議により決定すること。
- 現行システムおよび現行タブレット端末の導入・運用保守に携わる事業者との連携を密にして、現行の共有フォルダ(ファイルサーバ等)の構成、権限等の状況をヒアリングし把握すること。
- 現行システムの導入・運用保守に携わる事業者との連携を密にして、現行の共有ストレージ（オンプレファイルサーバ）の保存データについて、本業務で構築する新システムのクラウドストレージへデータ移行作業を行うこと。
  - ※ すべてのデータを移行するのではなく、事前に各小中学校やユーザー向けにアナウンスを行い、それぞれがデータの整理（校務系フォルダ、指導教材フォルダ、画像フォルダに 3 分類に整理するなど）を行って容量を圧縮したうえで、データ移行を実施する流れを想定。
  - ※ フォルダ構成や権限に関する図表等の資料をもとに、必要なデータのみを移行することを関係者に説明したうえで実施することを想定。
- バージョンの履歴機能および削除ファイルの復元機能を有すること。復元可能な期間は、削除操作から 30 日を保障すること。
- ユーザーがアクセス可能なフォルダについては、Windows 標準のエクスプローラからショートカット等により直接接続できるよう、個人で設定するためのマニュアルを作成するとともに、MDM 等でのクラウドストレージへのショートカットの一斉配付が設定できること。
- 高島市教育情報セキュリティポリシー（令和５年４月）および高島市教育情報セキュリティ運用規程（令和２年３月）に定める情報資産等の分類に基づいて、アクセス権限がないユーザー（第三者含む）がデータファイルを扱えないよう制御できること。
- 機微情報を含む重要なデータファイルについては、その操作ログもしくは全てのファイルの操作ログを取得し、外部記憶媒体への持ち出しが制限可能であるとともに、クラウドストレージからのダウンロードを検知できること。
- 基本的に、クラウドストレージに保存するデータファイルは、ユーザーが特に意識することなく自動暗号化されること。
- クラウドストレージにおいて、自動暗号化に対応していない拡張子のファイルがある場合、補完する別途ツールやソフトウェアの導入、費用対効果および運用方法を含めた最適な提案を行うこと。また、手動による暗号化での運用方法も選択肢の一つとして、自動暗号化との費用対効果やリスクを比較検討したうえで併せて提案すること。

キ）エンドポイントセキュリティ

- 校務 PC 端末をマルウェアの脅威、情報漏えいなどから守るセキュリティ対策、監視体制について提案すること。
- イベントログの取得を前提に、セキュリティインシデント発生時の調査や対処などの恒久的な対応を示すとともに、四半期毎にレポートを提出すること。
- サイバー攻撃に対する検出や監視、対応策等の助言を行うこと。

ク）DNS（名前解決）

- IP アドレスとドメイン名の紐づけを行う DNS サーバについて、管理負担の軽減のため、クラウドサービスの利用による名前解決を行うこと。

(2) 個別システム

クラウド基盤以外に構築する個別システムは次のとおりであり、必要なライセンス数を調達すること。なお、システムの製品名を指定しているものについては、本市での実績を優先し、同等機能を有していても他のシステムは認めない。

また、現行システムの導入・運用保守に携わる事業者との連携を密にして、新システムへのデータ移行を行うこと。

① 統合型校務支援システム

現行システムでは、㈱スズキ教育ソフトの「スズキ校務」をオンプレミスにて運用しており、すでに実績があることから、新システムでも継続利用することとし、クラウド利用のため SaaS 版を指定とする。

- ユーザー（小中学校１９校の学校教職員と教育委員会事務局職員等）は最大 380 名、同時接続数は 120 名程度とし、運用期間の５年間システムを利用できるライセンスを調達すること。
- 現行システムの「スズキ校務」から「evanix（SaaS 版）」へデータ移行を行うこと。
- 個人情報や機微情報を取り扱うことから、通信経路の暗号化処理（SSL による暗号化通信）を講じること。
- 統合型校務支援システムは、パッケージシステムを帳票以外はノンカスタマイズで利用する。カスタマイズ箇所については、本市と協議すること。
- 外字の使用はない。
- 統合型校務支援システムの仕様に関しては「別紙５：統合型校務支援システムの要件」を参照のこと。
- 国および滋賀県における法令等の改正により、カスタマイズ帳票およびシステム標準帳票様式の見直しが発生する場合は、軽易な修正プログラムは無償で提供し、適用作業まで実施すること。ただし、大規模な制度改正により別途有償対応となる場合は、本市と協議すること。

【指定品】　㈱スズキ教育ソフト：　evanix（SaaS 版）

② 教育系グループウェア

現行システムでは、㈱ネオジャパンの「Desknet's NEO」をオンプレミスにて運用しており、すでに実績があることから、新システムでも継続利用することとし、クラウド版を指定とする。

- ユーザーは、①校務支援システムのユーザー380 名＋120 名の計 500 名とし、運用期間の５年間システムを利用できるライセンスを調達すること。
- 現行システムの「Desknet's NEO」から「Desknet's NEO（クラウド版）」へデータ移行を行うこと。
- グループウェアに求める機能は、「お知らせ（インフォメーション）、スケジュール、電子メール（ウェブメール）、設備予約、回覧・レポート、タイムカード、文書管理、キャビネット、電子会議室、ToDo、アンケート、アラーム、メモパッド、アドレス帳、ユーザー名簿、来訪者管理」の標準機能である。
- カスタマイズについては、特になし。

【指定品】　㈱ネオジャパン：　Desknet's NEO（クラウド版）

③ 資産管理システム

現行システムでは、㈱内田洋行の「AssetBase」をオンプレミスにて運用している。新システムでは指定品とはしないが、校務 PC 端末 380 台、運用期間を５年間として、以下の機能を実現できるシステムのライセンスを調達すること。

ア）セキュリティパッチの管理

- 新システムの運用開始以降、セキュリティパッチを保守業務としてダウンロードおよび配信する。その際に、ネットワークへの影響を抑えることができること。
- セキュリティパッチおよび更新プログラムを配布する際、同一サブネット内の管理対象の校務 PC 端末に既にそれらのファイルがキャッシュとして残っていた場合は、そのキャッシュを使ってファイルを取得（ダウンロード）できること。
- セキュリティパッチ適用済み／未適用の結果を、Web レポート画面にて確認できること。

イ）USB デバイス制御

- USB メモリや外付けハードディスクなどの外部記憶媒体について、使用許可／不許可等の設定ができること。

ウ）情報資産管理

- 校務 PC 端末上のハードウェア情報およびソフトウェアに関するインストール状況を収集する機能を有すること。
- 校務 PC 端末ごとにアプリケーション状況を把握できること。
- 情報の収集は、決められた時刻に全台一斉に実行されるのではなく、自動で分散実行して、ネットワークや校務 PC 端末の負荷を低減できること。
- 手動による任意タイミングでも実行できること。

・　ハードウェア台帳で、重複した校務 PC 端末(端末シリアル番号または MAC アドレスが重複した端末）を抽出して表示できること。

エ）操作ログ

・　ログオン、ログオフ、外部記憶媒体の利用などの校務 PC 端末の操作ログを収集できること。

(3) ネットワーク機器等

以下のとおり、校務系ネットワーク機器の調達と設置を行う。

① 基本事項

・　下記の②納入機器に関する納入・設置計画書を令和７年１０月３１日までに提出し、本市の承認を受けること。
・　納入機器に初期不良や瑕疵があった場合は、速やかに交換すること。
・　１９小中学校、教育委員会事務局および本庁 3F 電算室への納入・設置作業において、納入機器の破損等が生じた場合は、すべて提案者側がその責任を負うこと。
・　主に教育施設内での作業となるので、特に安全管理に注意を払うとともに、児童生徒や教職員、その他市民等に対する迷惑・影響を最小限にとどめるよう、納入・設置スケジュールは本市および各小中学校と調整を行うこと。また、学校の授業や行事等の妨げとならないよう注意するとともに、作業時間帯は９時から１７時までとすること。
・　本市が指定する名称や管理番号等を記載したラベルシールを用意し、納入機器の指定位置に貼り付けるとともに、管理番号一覧表を Excel データで本市へ提出すること。
・　納入機器の動作テスト（疎通確認）を各納入場所において行うこと。
・　機器納入・設置後に不用となった外箱、梱包材等の廃棄物については、提案者の責任において撤去処分すること。

② 納入機器

ア）ファイアウォール

現行の庁内イントラネットでは、ルータと L3 スイッチ（センタースイッチ）の間に、ファイアウォール（FortiGate 101F）が２台設置（スタック構成）され、情報政策課で管理している。別紙１「教育ネットワーク概要図（校務系および学習系)」参照

これらは、校務 PC 端末（校務系ネットワーク）を含む他のインターネット接続系 PC 端末からインターネットへ接続する際、外部から侵入してくる不正アクセス等を防御する盾の役割を担っている。

本業務では、UTM（統合脅威管理）機能を有し、校務 PC 端末専用の認証やアクセス制御、ネットワーク通信負荷の低減を行うファイアウォール機器を新たに調達・設置する。

・　機器は、上記 FortiGate 101F とは別の型番で、下記製品を指定品とし、運用期間の５年間利用できるライセンスや保守パックを調達すること。

・　ファイアウォールの稼働において、10 分の商用電源供給が可能な UPS（無停電電源装置）を調達し、3 分での自動シャットダウン設定をすること。
・　機器および UPS は、本庁 3F 電算室の 19 インチラック内に設置することになるが、現行システムのサーバ等機器が設置されている教育系ラック内は現在、空きがない。現行システムのサーバ機器や UPS の撤去を令和８年度上半期に予定しており、それまでの間は、ラック外での一時的な仮設運用も含めて提案すること。なお、電源確保については、追加工事不要である。
・　クラウド基盤とファイアウォールとの連携によるゼロトラスト環境の構築について提案すること。
・　ラックへの機器の設置および設定作業にあたっては、市情報政策課、庁内イントラネットの運用保守に携わる事業者とも調整が必要になるので、打合せに必要な資料を準備しておくこと。

【指定品】　フォーティネット：　FortiGate 100F　２台（スタック構成）

イ）校内 LAN 用スイッチ

・　１９小中学校および教育委員会事務局には、市情報政策課整備の L3 スイッチの校務外部接続系セグメントポートに接続する校務系ネットワーク機器（スイッチ、HUB）が設置されているが、経年劣化により今回更新を行う。
・　現行機器を新機器に入れ替え（更新）するとともに、ネットワーク通信に必要な設定を行うこと。また、現行のネットワーク機器は、提案者が引き取り廃棄処分すること。
・　現行機器の設置状況および配線図については、別紙６「ネットワーク機器設置一覧表」および別紙７「校内 LAN 配線図」を参照すること。
・　既設の LAN ケーブル（青色の Cat6 ケーブル）を継続使用するが、テスターにより導通不可の場合、代わりの Cat6 ケーブルを用意し配線すること。
・　基準品の製品については、本市の事前確認を受けて承諾を得た場合、同等品以上の他の製品の納入を認める。その際は、基準品との機能比較表やカタログ等の資料を添付のうえ、別紙８「同等品確認書」を提出すること。
・　新機器への更新にあたり、庁内イントラネットの運用保守に携わる事業者とも調整が必要になるので、打合せに必要な資料を準備しておくこと。

a）基幹スイッチ

・　校内 LAN 用の基幹スイッチおよび職員室スイッチを計 55 台調達し、現行機器と入れ替え（更新）すること。
・　電源内蔵メタル筐体で、16 ポート 1000BASE-T 対応のレイヤー２スイッチであること。
・　ループ防止機能を有し、静音ファンレス設計で、動作時環境温度 50℃に対応すること。

【現行機器】　　エレコム　EHB-UG2A16-S
【新機器：基準品】　エレコム　EHB-UG2B16-S

b) スイッチ（島 HUB）

- 職員室用の島 HUB、校長室・保健室・事務室用および教育委員会事務局（学事施設課）の島 HUB を計 73 台調達し、現行機器と入れ替え（更新）すること。
- 電源内蔵メタル筐体で、8 ポート 1000BASE-T 対応のレイヤー２スイッチであること。
- ループ防止機能を有し、静音ファンレス設計で、動作時環境温度 50℃に対応すること。

【現行機器】　　エレコム　EHB-UG2A08-S
【新機器：基準品】　エレコム　EHB-UG2C08-S

③ その他機器

ア）校務 PC 端末

１９小中学校および教育委員会事務局に設置された現行の校務 PC 端末を新機器に入れ替え（更新）し、ネットワーク通信に必要な設定を行う。

現在、校務系ネットワークと学習系ネットワークは物理的に分離され、両者のネットワーク統合は行っていないので、校務 PC 端末の無線機能は利用せず、職員室等において有線でのネットワーク接続を行う。

a) 調達　　※別業務で調達

令和７年度に別業務において、ノートパソコン（OS：Windows11 Pro 64bit、メインメモリ：8GB、SSD：256GB、内蔵カメラ：フロントあり、Windows Hello for Business 対応）を本市が調達する。

b) 手順書

- 新システムのクラウド基盤および個別システムを利用するため、校務 PC 端末の初期設定に必要なネットワークやソフトウェアの手順書（マニュアル）および設定チェックシートを作成し、令和７年１１月２８日までに提出すること。
- IP アドレスの管理や払い出しは本市で行うが、ゲートウェイやドメインの設定、新システムの接続先 URL、ショートカット、ネットワークドライブの割り当てなど、項目ごとの手順書を作成すること。
- 令和７～９年度の間は、Windows10 Pro 64bit と Windows11 Pro 64bit の２つの OS の校務 PC 端末が混在することになる。また、Windows Hello 未対応の端末があり、生体情報（顔）と知識情報（PIN またはパスワード）を組み合わせた多要素認証ができないので、PIN またはパスワードでの端末認証ができるよう手順書を作成すること。

c) 機器の設定　　※本市で設定

b）の手順書と設定チェックシートをもとに、本市の管理担当者が校務 PC 端末の設定作業と現地配布を行う。提案者の作業は不要である。

イ）校務プリンタ　　※別業務で調達

ア）校務 PC 端末と同様に、令和７年度に別業務において本市が調達し、本市の管理担当者がネットワークの接続や印刷等の初期設定を行う。

10. 提出図書

本市が新システムを円滑に運用できるよう、準備期間が完了した段階で図書を紙媒体で２部、電子データを１部提出すること。なお、電子データはPDF形式に加え、編集可能なデータ形式（拡張子：.docx .xlsx .pptx等）も併せて提出すること。

【図書の提出先】

〒520-1592　滋賀県高島市新旭町北畑565番地
高島市教育委員会事務局　学事施設課

以下に、提出図書に含まれるものを示す。

① 納品物一覧
② プロジェクト計画書（スケジュール表を含む）
③ 構築体制表（体制図・緊急連絡先）
④ 課題管理表
⑤ 会議録
⑥ 要件定義書および設計書
・新システムの要件定義、設計内容、設定情報の一覧等
（クラウド基盤の基本・詳細設計、運用設計）
（個別システムの基本・詳細設計、運用設計）
・新システム構成図等
（新システム、ネットワークおよび共有ストレージ等の構成図）
⑦ テスト実施計画書およびテスト結果報告書
⑧ システム設定手順（マニュアル）
・新システム（クラウド基盤、個別システム）について、構築時までに実施した設定作業に関する手順書
⑨ 操作手順マニュアル（運用マニュアル含む）
新システムの運用上、必要な操作をまとめた手順書を作成すること。なお、必要な操作とは、初期設定時の手順を示すものではなく、導入後に発生しうる事象に関する操作手順も含み、少なくとも下記については記載してあること。
・管理ツールやアカウントのアップデート
・設定情報の追加、変更、削除
⑩ 研修計画書
⑪ 研修資料（管理担当者向け・教職員向け）
⑫ 研修会の質疑・回答
⑬ 運用保守体制表
⑭ システム障害等対応マニュアル
⑮ 障害対応報告書
⑯ ヘルプデスクの記録（問い合わせおよび回答の内容）
⑰ リモート保守対応にかかる覚書　　※必要があれば
⑱ リモート保守作業計画　　※必要があれば
⑲ 月次の運用状況レポート（インシデント報告含む）
⑳ 機器納入・設置計画書
㉑ ラベルシールおよび管理番号一覧表

㉒ PC 端末の初期設定に必要なネットワークやソフトウェアの手順書（マニュアル）および設定チェックシート
㉓ 業務完了報告書　　１部
㉔ ライセンス証書　　１式
㉕ 納入機器の保証書　１式
㉖ その他本市が求めるもの　　必要数

11. 契約方法

「高島市校務支援システム更新業務　公募型プロポーザル実施要領」に基づき、提案者からの提案内容を評価し、最優秀事業者を１者選定する。

事業者選定後、本市契約審査会を経て、１者随意契約により業務契約を締結する。

12. 支払い

1)　買い取りで調達する 9.システム要件(3)ネットワーク機器等②納入機器ア）ファイアウォールおよびイ)校内 LAN 用スイッチ、業務管理、クラウド基盤の構築、研修会のイニシャルコストについては、令和７年度予算により一括で支払う。

2)　1）以外のクラウドシステムおよびその他ソフトウェアのライセンス料、運用保守等のランニングコストについては、本市と提案者で協議を行い、別表に令和７年度～令和 12 年度の年度別支払額を明記のうえ支払うこととする。

13. 著作権

本業務で作成されたドキュメント、データに関する著作権については、本市に帰属する。ただし、成果物に提案者または第三者の著作物が含まれる場合、提案者が本業務を行うにあたり、新たに作成した著作物を除き、当該著作物の著作権は、従前からの著作権者に帰属する。

14. 機密保持等

1)　受注者は、個人情報の取扱いについて、個人情報の保護に関する法律および高島市教育情報セキュリティポリシーを遵守するとともに、別記「情報セキュリティの確保にかかる特記事項」を守らなければならない。

2)　受注者は、以下の資格をいずれか１つ以上有するものとし、公募型プロポーザルへの参加申込時に資格証の写しを本市に提出すること。

ア　ISO15001（プライバシーマーク：個人情報セキュリティ）

イ　ISO27001（ISMS：情報セキュリティマネジメントシステム）

15. 損害賠償および不適合責任

提案者が業務の履行に関し、自己の責に帰すべき事由により本市に損害を与えたときは、提案者の負担において本市の指定する期限までに原状回復するか、または、その損害を全額賠償するものとする。

また、作業にあたっては、細心の注意を払うこと。その際、施設・設備および第三者等に損害を与えた場合、賠償に要する費用は提案者の負担とすること。

さらに、本業務終了後の過失等に起因する不良箇所が発見された場合は、提案者

の負担において修正およびその他必要な作業を行うものとする。

16. 再委託

本業務を第三者に再委託することは禁止する。ただし、やむを得ず本業務の一部を第三者に委託する必要があるときは、あらかじめ再委託先の事業者名、作業内容および作業場所等を本市へ届け出て、本市の承認を得なければならない。

また、再委託を受けた者に対しても、機密保持等について同様の義務を負うものとする。

17. その他

1) 数量等に変更が生じた場合は、設計額に対する落札率により変更するものとする。

2) 作業にあたっては、労働基準法および労働安全規則等関係諸法規に従い、事故防止、盗難および児童生徒等の安全に万全を期すること。また、事前に本市および各小中学校と調整するとともに、すべての作業が完了した時点で、完了報告書および写真を提出すること。

3) 高島市の発注する建設工事等における暴力団員等による不当介入の排除について、

① 提案者は、業務の履行にあたり暴力団員等（暴力団の構成員および暴力団関係者その他市発注工事等に対し不当介入をしようとするすべての者をいう）から不当介入（不当な要求または業務の妨害）を受けたときは、断固としてこれを拒否するとともに、不当介入があった時点で速やかに警察に通報するとともに、警察が行う必要な捜査に協力するものとする。

② 提案者は、前項の規定により通報を行った場合は、速やかに通報書（別記様式第１号）により高島警察署に届け出るとともに、担当職員に報告するものとする。また、提案者は以上のことについて、下請負人（すべての協力者を含む。）に対して十分に指導を行うものとする。

③ 提案者は、暴力団員等による不当介入を受けたことが明らかになり、工程等に被害が生じた場合は、監督職員と協議するものとする。

4) 本仕様書に定めなき事項または疑義が生じた場合は、本市と提案者にて協議のうえ決定することとする。

【別記】

情報セキュリティの確保にかかる特記事項

１．定義

個人情報とは、個人情報の保護に関する法律第２条第１項に規定するものをいう。

個人番号とは、住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。

特定個人情報とは、個人番号をその内容に含む個人情報をいう。

機密情報とは、この契約事務の業務遂行に必要な個人情報および特定個人情報を含む情報をいう。

２．基本的事項および利用目的

受注者は、個人情報保護の重要性を認識し、機密情報をこの契約事務の遂行のためにのみ利用するものとする。

なお、この契約による事務の実施に当たっては、個人の権利利益を侵害することのないよう、機密情報を適法かつ適切に管理し、取り扱わなければならない。

３．業務責任者等の特定

受注者は、この契約事務に係る業務責任者、業務内容、個人情報取扱者および作業場所を定め、個人情報取扱者以外のものに、この契約による機密情報を取り扱わせてはならない。

４．サービスレベルの保証

受注者は、この契約による事務を処理するため、個人情報を取り扱う外部サービスを利用する場合、業務の重要度に応じたＳＬＡ（Service Level Agreement）が締結可能であること。

なお、ＳＬＡ契約締結を行う場合は、本業務の契約締結後、別途協議を行うものとする。

５．従事者に対する教育の実施

受注者は、従業者が個人情報を取り扱うにあたり、必要かつ適切な監督を行い、従業者に対し、個人情報の適正な取扱いを周知徹底するとともに適切な教育を行わなければならない。

受注者は、この契約による事務に従事している者に対して、在職中および退職後において、その事務に関して知り得た情報を他に漏らしてはならないこと、および契約の目的以外の目的に使用してはならないことなど、情報の保護に関し必要な事項を周知するものとする。

６．目的外利用および受注者以外の者への提供の禁止

受注者は、個人情報を委託業務の遂行のためにのみ利用するものとし、事務の目的を

明確にするとともに、事務の目的を達成するために必要な範囲内で、適法かつ公正な手段により行わなければならない。

受注者は、この契約による事務に関して知り得た情報を契約の目的以外の目的のために利用し、または第三者に提供してはならない。

７．業務上知り得た情報の守秘義務

受注者は、この契約による事務に関して知り得た情報の漏えい、滅失およびき損の防止その他の個人情報の適切な管理のために必要な措置を講じなければならない。

受注者は、この契約による事務に関して知ることができた情報を他人に知らせてはならない。この契約が終了し、または解除された後においても同様とする。

８．再委託

受注者は、業務の全部または一部を第三者に再委託してはならない。ただし、事前に書面により市の承諾を得た場合は、この限りではない。

９．資料複製、持ち出しの禁止および返還等

受注者は、本市から引き渡された個人情報が記録された資料等を複写、複製または持ち出してはならない。ただし、事前に書面により市の承諾を得た場合は、この限りではない。

受注者は、この契約による事務を処理するために本市から引き渡され、または受注者自らが収集し、もしくは作成した個人情報が記録された資料、記録媒体等は、業務完了後、直ちに本市に返還し、または引き渡すものとする。ただし、本市が別に指示したときは、その指示に従うものとする。

１０．定期報告および緊急時報告義務

受注者は、個人情報の紛失、破壊、改ざん、漏洩等の危険に対して、合理的な安全管理措置を講じるものとし、この契約による事務に関するセキュリティ対策状況について、適宜市に報告しなければならない。

また、本業務の遂行において、情報セキュリティが侵害され、またはその恐れがある場合には、速やかに市に報告し、原因究明およびその対処方法等について、市と協議し実施すること。

１１．監査および検査

本市は、必要があると認めるときは、受注者がこの契約による事務の執行に当たり取り扱っている個人情報の状況について、実地調査をし、または報告を求めることができる。

１２．事故（セキュリティインシデント）発生時の措置

受注者は、万が一個人情報の紛失、破壊、改ざん、漏洩等の事故が発生した場合には、直ちに市に通知するとともに、当該事故による損害を最小限にとどめるために必要

な措置を、自らの責任と負担で講じるものとし、必要に応じ、その状況等を公表する。

また、発生した事故の再発を防ぐため、その防止策を検討し、市と協議の上、決定した防止策を、自らの責任と負担で講じるものとする。

万が一、受注者において個人情報の紛失、破壊、改ざん、漏洩等の事故が発生し、市が第三者より請求を受け、また第三者との間で紛争が生じた場合には、受注者は市の指示に基づき、自らの責任と負担でこれに対処するものとする。この場合、市が損害を被った場合には、市は受注者に対して当該損害の賠償を請求できるものとする。

１３．個人情報を取り扱う外部サービスの利用

受注者は、本業務の遂行において、個人情報を取り扱う外部サービスを利用する場合は、次に掲げる事項を定め、市に提示すること。

⑴　外部サービスの利用目的

⑵　外部サービスの利用を通じて本市が取り扱う情報の外部サービス提供者における目的外利用の禁止

⑶　外部サービス提供者における情報セキュリティ対策の実施内容および管理体制

⑷　外部サービスの提供に当たり、外部サービス提供者もしくはその従業員、再委託先またはその他の者によって、市の意図しない変更が加えられないための管理体制

⑸　外部サービス提供者の資本関係・役員等の情報、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績および国籍に関する情報提供ならびに調達仕様書による施設の場所等の指定

⑹　情報セキュリティインシデントへの対処方法

⑺　情報セキュリティ対策その他の契約の履行状況の確認方法

⑻　情報セキュリティ対策の履行が不十分な場合の対処方法

また、受注者は、本業務の遂行において、個人情報を取り扱わない外部サービスを利用する場合は、前記⑴、⑶および⑹に掲げる事項を定め、市に提示すること。

外部サービス・・・事業者等が情報システムの一部または全部の機能を提供するもので、クラウドサービス、Ｗｅｂ会議サービス、ＳＮＳ（ソーシャルネットワークサービス）、ホスティングサービス等をいう。