セキュリティサーバ等認証設定業務委託仕様書

1　件名

セキュリティサーバ等認証設定業務委託

2　事業目的

令和７年９月を移行目標とする基幹系情報システムの国標準準拠システムは、マイナンバー情報を取り扱うことから、多要素認証が国ガイドラインに義務付けられており、セキュリティ認証サーバ及び基幹系ネットワークパソコンにセキュリティ認証を施す必要があるため、サーバ等への認証設定業務を委託するものです。

3　契約期間

契約締結日から令和７年９月30日まで

4　稼働時期

令和７年９月16日（予定）

5　前提条件

構築するサーバ機器、端末及びネットワーク回線については、本市が所有している機器等を使用し、システム構築に付随するソフトウェアの調達及び管理・運用については本仕様書に記載する。

6　作業場所

本市指定場所

7　構築概要

受注者は以下のものを構築すること。また、構築にあたり、各サーバに必要なシステム要件は発注者と協議すること。協議のうえ、サーバ構成設計書を作成すること。

ア　Active Directory（以下、ＡＤという。）サーバ
イ　Domain Name System（以下、ＤＮＳという。）サーバ
ウ　ファイルサーバ
エ　バックアップサーバ
オ　顔認証システムサーバ
カ　ウイルス対策ソフトウェア配信サーバ
キ　クライアント構築

8　構成及び設定作業概要

8－1　基本要件

(1)　受注者は、すべてのサーバ等において、それぞれの機能を正常かつ安全に使用できるよう、必要なソフトウェアの導入、各種設定を行うこと。

(2)　受注者は、本契約締結後、速やかに業務計画書を提出すること。
なお、業務計画書は、作業工程の全体、各工程の詳細内容等が確認できる構成とすること。

(3)　受注者は、サーバ等及び端末設定後、ネットワーク接続の動作確認等の必要な調整を行った上で引き渡すこと。

(4)　受注者は、構築期間中に、設定内容の見直し等を行ったとき、また管理・運用期間中に、機器が正常に動作しないことが判明したときは、設定変更を行い、本仕様書記載の機器を含めて再設定すること。

(5)　受注者は、上記(1)～(4)を達成するために、既存のネットワーク等の設定変更が伴う場合において発生する経費についても、本調達費用に含むものとする。ただし、既存ネットワーク担当業者との打ち合わせに必要な調整は、発注者が行うものとする。

(6)　委託業務が完了したときは、速やかに受注者は発注者に作業完了報告を書面で提出すること。

8－2　構成

(1)　セキュリティ認証サーバ

(2)　セキュリティ認証サーバ上に顔認証システムサーバを構築すること。また、ＡＤサーバ（正）およびウイルス対策ソフトウェア配信サーバを仮想サーバとして構築すること。

(3)　ファイルサーバ

(4)　ファイルサーバ上にＡＤサーバ（副）を仮想サーバとして構築すること。

(5)　ストレージ

(6)　サーバ用無停電電源装置

8－3　設置場所

(1)　セキュリティ認証サーバに関しては、寝屋川市上下水道局４階に設置

(2)　ファイルサーバに関しては、寝屋川市サービスゲート２階に設置

(3)　端末に関しては、寝屋川市上下水道局４階にて保管

9　委託作業概要

9－1　サーバ等設定作業

受注者は、サーバ等に対する共通設定項目の作業を行うこと。なお、発注者が所有するサーバ等は別紙１のとおり。

(1)　各サーバ機器への設定及び調整作業を行うこと。なお、サーバ仮想化については、仮想化技術による機器集約と、OS、ソフトウェア等が最高の性能を得られるように最適化を想定すること。

(2)　各サーバへのOS設定及び調整作業を行うこと。最新のセキュリティパッチを適用すること。不要なサービスは無効化すること。

(3)　各サーバへのバックアップソフトウェア設定及び調整作業を行うこと。

(4)　各サーバへのウイルス対策ソフトウェア設定及び調整作業を行うこと。

(5)　各機器のネットワーク設定及び調整作業を行うこと。各サーバに静的IPアドレスを設定すること。IPアドレスは発注者から指定する。

(6)　各ネットワーク機器への疎通確認作業を行うこと。

(7)　無停電電源装置管理ソフトウェア設定及び調整作業を行うこと。

(8)　無停電電源装置の機器動作確認を行うこと。

(9)　動作確認及び機能検証完了後、テスト結果報告書を作成すること。また、システムバックアップを行うとともに、バックアップデータを発注者に提出すること。

9－2　セキュリティ認証サーバ

(1)　受注者は別紙２の顔認証システムの要件を満たすソフトウェアを用意し、セキュリティ認証サーバにシステム構築及び認証作業を行うこと。

(2)　顔認証システムに必要なライセンス数は512台用意すること。

(3)　セキュリティ認証サーバが障害等により使用できない場合であっても、端末にログインできる環境を構築すること。

9－3　ＡＤサーバおよびＤＮＳサーバ

(1)　ＡＤサーバにドメイン構築に対する各作業を行うこと。

(2)　ドメインサーバに規定するサーバにより、仮想化サーバから独立したドメインサーバを設置し、ドメイン構築を行うこと。

なお、ドメインサーバの２台のうちプライマリは寝屋川市サービスゲート、セカンダリは寝屋川市上下水道局に設置し両機器間で冗長化を行うこと。

(3)　Microsoft社のＡＤを継続し、ＡＤサーバは現行の設定を移行して構築すること。

(4)　ドメインやサーバ、コンピュータの名前をアドレスに変換する機能を設定すること。

(5) 新たに構築するＡＤサーバには、新たに構築したサーバや端末名を新規で登録すること。新しい端末名は発注者から指定する。なお現行のＡＤサーバには、200 台のコンピュータが登録されている。
(6) ドメインに参加しているコンピュータに対して時刻同期を行うこと。
(7) ＡＤサーバ（正）とＡＤサーバ（副）については、サーバ機器が故障した際でも利用できるように同期を行うこと。

９－４　ファイルサーバ

(1) ファイルサーバを構築し、動作検証を行うこと。
(2) 現行のフォルダ構成及び各所属におけるアクセス権限や格納データの移行を行い、新しいファイルサーバ切替え（令和７年９月中旬を想定）まで、上記内容について、現行サーバとの整合性をとること。なお、データ移行については、事前にデータ移行を行い、整合性を確認したうえで、本番切替え時は差分移行を行うこと。
(3) データのバックアップの設定を行い、障害発生時及び一定期間内におけるデータの復元をファイル単位でも行えるよう設定すること。
(4) 受注者が提供する他システムのファイルについても移行すること。

９－５　ウイルス対策ソフト配信サーバ

(1) 受注者は、発注者が提供するサーバにウイルス対策ソフトをインストールすること。
(2) 発注者が指定する端末及びサーバについて、ウイルス対策ソフトのインストール及び定義更新、セキュリティ状況の監視等は、サーバにて一括管理ができる仕組みを構築すること。
(3) 適宜ライセンスの増加による適用や更新ができること。
(4) 発注者が提供するＵＳＢ等を利用し、ウェブ上からダウンロードしたウイルス定義ファイルをサーバから各端末機等（サーバ含む。）に対して、定期的（一週間程）に一斉にウイルス定義ファイルを配信できる仕組みを構築すること。
(5) ウイルス定義ファイルの配信方法については、受注者側で手順書を作成すること。

９－６　サーババックアップ

(1) 本仕様書により構築した仮想環境（必要なソフトウェアをすべてインストールした状態）全体のバックアップデータを取得し、サーバ障害時等に迅速かつ柔軟に対応できる機能を確立すること。復旧に必要な手順書等を納品すること。

(2) (1)に規定する仮想環境全体のバックアップについて、システムイメージについては、初期導入時及び仮想環境に変更を加えた時（仮想ＯＳ追加等）に行い、データベース部分については日次バックアップを行うこと。
(3) バックアップ処理等をスケジュールによる自動実行が可能であること。
(4) バックアップデータから各システム及びデータの復元が簡易に行えること。
(5) バックアップの実施に当たっては、業務遂行に支障が生じないこと。
(6) バックアップ及び復元システムの運用マニュアルを作成すること。
(7) その他データベースの領域等詳細については別途協議するものとする。

９－７　端末設定作業

(1) 発注者が所有する端末は別紙３のとおりであり、別紙３に掲げる区分毎に同一の設定を実施すること。
※　端末が故障時等の理由により、他の端末に環境構築する必要が生じた際に、費用を生じさせることなく復旧させることができること。復旧に必要な手順書等を納品すること。
(2) 端末のコンピュータ名及びIPアドレスは受注者から提供する情報を使用すること。
(3) OSはWindows11とし、ライセンス認証を行うこと。導入時点でマイクロソフト社より公表されているWindows及びOfficeの修正ファイルを適用すること。なお、更新プログラムのクラスが「重要な更新」であるものは全て適用すること。また、その他の更新プログラムのクラスのものについては、必要に応じて適宜適用すること。ただし、別紙３の（１）パソコン（60台）については、ライセンス認証は不要とする。
(4) Microsoft Officeのインストール及びライセンス認証を行うこと。
ア　使用者がライセンス認証の入力を必要としないようにすること。なお、ＭＡＫキーは発注者から提供する。
イ　起動しているWordとExcelは同一のプログラムを開いたとき、新しいウインドウで起動するように設定すること。
ウ　Wordのページ設定については、発注者の指定する書式で起動するように設定すること。
エ　別紙３の（１）パソコン（60台）については、インストール及びライセンス認証は不要とする。
(5) ソフトウェアについて、次のものをインストール及び設定すること。
ア　Adobe Acrobat Reader
イ　ウイルス対策ソフト
(ｱ) ウイルス対策ソフトはTrend Micro社製の製品とする。
(ｲ) 必要なライセンス数は452台とする。
(ｳ) ウイルス対策ソフトは５年間以上使用可能できるように用意すること。

(ｴ) ウイルス定義ファイルの配信日時及び手法等については別途協議とする。

ウ　顔認証システムクライアント

(6) ブラウザの設定

Microsoft Edge（デスクトップ版）に設定すること。

(7) コントロールパネルについては次のとおり設定すること。

ア　コントロールパネルにシステム、デバイス、個人用設定のみ表示すること。

イ　ユーザがログオフすることができるようにすること。

ウ　アクセサリ内の「ゲーム」をアンインストールすること。

エ　「全ての組織のネットワーク接続」の自動検索を行わないように設定すること。

(8) 動作確認

ア　Windows11へログオンができ、Microsoft Officeが問題なく動作することを確認すること。

イ　デスククトップへの書き込みを禁止し、ローカルディスクを見せない設定にすること。

ウ　原則、端末からＵＳＢ等へのデータ書き出しを禁止すること。ただし、必要に応じてＵＳＢ等へのデータ書き出しを可能に変更できること。

エ　ＵＳＢ等からデータ読み込みは可能とする。

オ　ＡＤのユーザ設定に対して、任意のネットワークドライブを割り当てすること。

カ　顔認証システムで顔認証したのちにＩＤ及びパスワードでパソコンにログインできること。

キ　上記の他、発注者の指定する動作確認を実施すること。

(9) 端末の個別設定と動作の確認作業

ア　発注者の指定するコンピュータ名を設定すること。

イ　発注者の指定するドメインへの設定と動作確認を行うこと。

ウ　作業内容に基づいた設定等状況について、動作確認を行うこと。

(10) その他

ア　端末は個人番号利用系事務を行うことから、必要なセキュリティ対策を遺漏なく実施すること。

イ　各ユーザがログイン後に使用する各システムについて、各システムの動作を妨げることが無いよう調査、調整を行うこと。本業務で調達したシステムが起因する場合、速やかに原因を解明し、対応すること。

ウ　発注者の指定するドメインに参加させ、ＡＤへの登録を行うこと。

エ　Adobe ReaderがWebブラウザ上で使用できるように設定すること。

オ　Bluetoothをオフに設定すること。

カ　発注者が指定する端末管理名をラベルテープで作成し、端末本体とACアダプタに貼付すること。

キ　その他のセキュリティ対策に必要な事項については、協議の上、対応すること。

10　委託業務体制

本業務遂行にあたって受注者は業務への影響を生じさせることなく円滑に業務を行うことができる業務体制を構築すること。

なお、業務体制について発注者に対し下記内容を通知すること。

(1)　受注者の管理体制

受注者は、情報セキュリティマネジメントに関する認証であるISO/IEC27001（JIS Q 27001）を取得していること。

(2)　作業責任者の配置

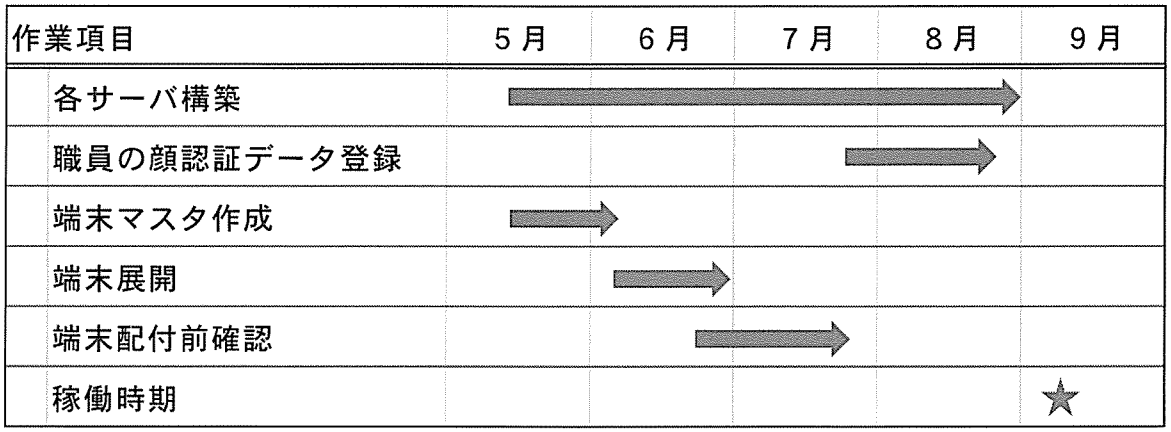
受注者は本仕様書に示す全行程における作業責任者を置くこと。作業責任者は、本契約締結時に、各業務について作業責任者・作業従事者等の人員配置等の業務体制を書面で作成し、発注者に提出・説明すること。

(3)　作業体制の変更

受注者は作業責任者もしくは作業従事者に変更等が必要になった場合は速やかに発注者へ通知し、変更内容を書面で届け出ること。

11　想定スケジュール

発注者は下記のスケジュールを想定している。詳細については別途協議すること。ただし、稼働時期については延期を認めない。



12　保守概要

12－1　保守対象

受注者は、本仕様書により調達するシステム等に関わる全てを5年保守すること。

12－2　保守受付時間等

(1)　受注者は、本仕様書により調達するシステム等の保守に関する窓口を設置すること。

(2)　受注者は、窓口の連絡受付手段として、電話および電子メールを提供すること。

(3)　電話による受付は、原則として、月曜日から金曜日まで（国民の祝日に関する法律に定める休日及び年末年始の休日（12月29日から翌年の1月3日までの日）除く）の午前9時00分から午後5時30分までとする。

(4)　電子メールによる受付は、24時間365日受信可能とする。

12－3　保守要件

(1)　受注者は、対象機器の保守は「13　管理・運用」に規定する業務従事者と連携して、原則、訪問修理で行うものとする。

(2)　受注者は、保守を行う際には、業務に影響を及ぼさないように作業を行うこと。システムを停止する必要がある場合等は夜間休日に作業を実施すること。

(3)　受注者は、保守の責任体制を明確にしておくこと。

(4)　受注者は、システム等に対し、5年サポートすること。

12－4　保守・障害対応・点検作業詳細

(1)　受注者は、システム等を常時、正常な状態で使用できるように保守すること。

(2)　受注者は、予防保守として、システム等の点検を実施すること。点検内容については、「13　管理・運用」のとおりとする。

(3)　受注者は、下記の障害対応を行うこと。

ア　障害発生時には、受注者は障害の切り分け、システム等の復旧、調整等の正常な状態への復旧に必要な措置を行うこと。

イ　一般的な障害における障害対応作業

1つの原因に対して影響が1つの端末に限定される、一般的な障害に対しては、発注者と初期対応内容や対応スケジュール等について協議し決定すること。ただし、発注者の業務に深刻な支障が生じる場合は、土・日・祝日についても対応作業を要求することがある。

ウ　深刻な障害における障害対応作業

1つの原因に対して複数の端末に影響を及ぼす可能性がある、以下の深刻な障害については、休日、年末年始を含め、当日中に対応を開始すること。

(ｱ)　ファイル改ざん、データ漏えい等の被害

(ｲ)　ウイルス感染

(ｳ)　利用者サービスの停止又はその可能性のある障害

エ　受注者は、障害復旧後、発生した障害履歴を一元管理し、原則として障害復旧後の翌営業日の午前9時00分から午後5時30分に、作業報告書を提出

すること。ただし、障害復旧に時間を要する場合、速やかに判明している原因及び復旧見込み等を発注者に報告し、対応等の承認を得ること。

オ　障害原因が保守対象外の機器等の場合は、速やかに発注者に障害の原因及び調査結果を報告すること。

⑷　保守対象機器毎の点検、修理等の履歴を常に把握し、発注者より要求があった場合は、発注者に情報提供すること。

⑸　本仕様書により調達する機器の設定変更、機能追加、OS、ソフトウェアのバージョンアップ等を行う場合に機器、OS、ソフトウェアの操作方法、設定変更方法（チューニング等）について、技術支援を行うこと。

13　管理・運用

13－１　運用管理の範囲

運用管理の範囲は、本仕様書により「７　構築概要」の範囲とする。

13－２　人員体制

業務従事者は、ネットワーク、セキュリティ、システム管理等について専門的な知識及び技術を有し、本業務を円滑に遂行するために十分な能力を有する者であること。

13－３　業務内容

⑴　アカウント管理

ユーザのアカウント情報を一元的に管理するため、ＡＤの設定変更（グループポリシーの作成等）等を行うこと。

※　作業内容については、別途協議するものとする。

⑵　端末、プリンタ管理

機器に対し、以下の管理を行うこと。

ア　ハードウェア、ソフトウェアの資産管理及び管理台帳の作成・更新

イ　ＵＳＢ等のデバイス制御管理及び管理簿の作成・更新

ウ　パソコン、プリンタの操作説明や障害対応等

エ　業務ソフトウェアのインストール・アンインストール

⑶　サーバ、ネットワーク管理

ア　ディスク領域及びイベントログ等の確認

イ　各種サーバ、ネットワーク機器の構成、所在、設定情報に関するドキュメントの作成と更新

ウ　ＩＰアドレスの管理

⑷　ウイルス対策

ウイルス対策ソフト管理ツールを用いて、以下の管理を行うこと。

ア　ウイルス定義ファイルの一元管理

イ　ウイルス感染監視

⑸　バックアップ

ア　定時バックアップの実施（自動バックアップが正常に行われているかの確認も含む。）及び各種定期点検支援

イ　業務システムサーバ及びファイルサーバのデータバックアップ

⑹　手順書

ア　ユーザーアカウントの作成・有効化・無効化

イ　パスワード忘失者に対するリセット

ウ　アカウント管理簿の作成・更新

エ　ウイルス定義ファイルの適用方法

⑺　その他

システム運用、障害切り分け、障害除去及び保守点検業務等の作業にあたっては、保守担当業者との連携を密にとり対応を行うこと。

14　納品物

14－1　構築業務完了時

下記の納品物を納めること。

⑴　構築の終了時に作業完了報告書

⑵　プロジェクト管理文書（課題管理台帳、議事録）

⑶　設計書（基本及び詳細設計書、機器及びソフトウェア一覧、システム構成図）

⑷　計画書及び結果報告書（移行、試験、検収）

⑸　各種マニュアル（管理者および一般職員向け操作マニュアル、運用・保守手順書、バックアップ・復旧手順書等）

⑹　運用保守手順書及び体制図

14－2　管理・運用時

下記の納品物を納めること。

作業完了報告書（随時）

15　その他

15－1　機密保持

⑴　業務委託実施前のセキュリティ対策

ア　寝屋川市情報セキュリティポリシーを遵守すること。

イ　個人情報漏えい防止のための技術的安全管理措置に関する取り決めを発注者に提出すること。

ウ　受注者は、この契約による事務を処理するための個人情報の取扱いについては、別記「個人情報取扱特記事項」を守らなければいけない。

エ　受注者は、アクセスを許可する情報の種類と範囲、アクセス方法の明確化すること。また、生成から廃棄までの情報のライフサイクル全般での管理の実施すること。

オ　セキュリティインシデント発生時が発生した際は、発注者による検査および公表する場合がある。

(2)　業務委託実施中のセキュリティ対策

ア　情報資産の適正な取扱いのための情報セキュリティ対策を実施すること。

イ　契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告を求める場合がある。

ウ　情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合、委託事業の一時中断など必要な措置を講じる場合がある。

(3)　業務委託終了時の対策

ア　受注者は契約期間を通じて別記「個人情報取扱特記事項」が遵守されたことを報告すること。

イ　受注者は発注者から提供を受けた情報を含め、委託業務により知り得た全ての情報について守秘義務を負うものとし、取り扱った情報の返却、廃棄又は抹消すること。

(4)　その他

ア　受注者は正当な理由があってやむを得ず第三者に開示する場合、書面によって事前に承諾を得ること。また、情報の厳重な管理を実施すること。

イ　発注者が提供した資料は、原則として全て複製禁止とすること。ただし，業務上やむを得ず複製する場合であって、事前に書面にて発注者の許可を得た場合はこの限りではない。なお、この場合にあっても使用終了後はその複製を発注者に返納又は焼却・消去する等適切な措置をとり、機密を保持すること。

ウ　再委託等の禁止

受注者は、委託業務の処理を第三者に委託し、又は請負わせてはならない。ただし、「業務委託契約に関する再委託ガイドライン」を遵守し、書面により発注者の承諾を得た場合はこの限りではない。

エ　個人情報の取扱いに関し、発注者が報告書等の提出を求めた場合については、速やかに提出する。

15－2　調整事項

機器更改に伴い庁内ネットワーク環境に停止等が発生する場合、関係各所との調整は発注者にて行う。受注者は調整が必要となる事項については、事前に発注者と協議し承諾を得ること。

16　疑義等の決定

本仕様書に記載のない事項及び疑義が生じた場合は、発注者受注者協議の上、業務を行うこと。

別紙１　サーバ等一覧

(1)　セキュリティ認証サーバ機器（１台）

仕様項目	内容
CPU	・Intel Xeon Gold 6526Y プロセッサー
メモリ	・64GB
アレイコントローラ	・RAID0、1、1+0、5、5+0 構成およびホットスペア構成機能をサポートするストレージコントローラを搭載
内蔵ディスク	・480GBのSDDをRAID5 (3+1) +HSで搭載し、ホットプラグに対応
光学式ドライブ	・DVD-RAM ドライブを本体処理装置に内蔵
ネットワーク	・1000Base-T の LAN ポートをオンボードで１ポート
管理 LAN ポート	・サーバ管理専用 LAN ポートを１ポート
インターフェース	・外部接続可能なUSB3.0インターフェースは２ポート ・ディスプレイはKVMスイッチ接続
電源	・900W
サーバ OS 及びゲスト OS	・Microsoft Windows Server 2022 Standard をサーバ OS 及びゲスト OS を含み３台分あり
イメージバックアップソフトウェア	・OS や仮想マシン等のイメージバックアップ及びリストアを行うためのソフトウェアあり
セキュリティ対策ソフト	・PKG Trend Micro Server Protection for Windows

(2)　ファイルサーバ機器（１台）

仕様項目	内容
CPU	・Intel Xeon Gold 6526Y プロセッサー
メモリ	・64GB
アレイコントローラ	・RAID0、1、1+0、5、5+0構成およびホットスペア構成機能をサポートするストレージコントローラを搭載
内蔵ディスク	・RAID6+HSを構成し、10TB以上の容量を利用可能
光学式ドライブ	・光学ドライブとして DVD-RAM ドライブを本体処理装置に内蔵
ネットワーク	・1000Base-T の LAN ポートをオンボードで１ポート
管理 LAN ポート	・サーバ管理専用 LAN ポートを１ポート
インターフェース	・外部接続可能なUSB3.0インターフェースは２ポート ・ディスプレイはKVMスイッチ接続
電源	・900W

サーバOS及びゲストOS	・Microsoft Windows Server 2022 Standardをサーバ OS及びゲストOSを含み3台分あり
イメージバックアップソフトウェア	・OSや仮想マシン等のイメージバックアップ及びリストアを行うためのソフトウェアあり
セキュリティ対策ソフト	・PKG Trend Micro Server Protection for Windows

(3) ストレージ装置(1台)

仕様項目	内容
データ容量	・利用可能領域は10TB
ホストインターフェース	・サーバとの接続はPCIカード、経路とも冗長構成である ・ファイバチャネルが使用できる
システムメモリ	・システムメモリ容量は筐体全体で16GB搭載

(4) サーバ用無停電電源装置(3台)

仕様項目	内容
動作方式	・ラインインタラクティブ方式
定格容量	・1500VA/1200W
入力電圧	・AC100V
出力コンセント	・NEMA 5-15Rを6個
USBポート	・サーバと接続するUSBポートを有している
ソフトウェア	・停電時に自動でサーバをシャットダウンさせることのできる電源管理ソフトウェアを用意している

別紙２　顔認証システム要件

顔認証システム仕様

１　認証デバイス

⑴　多要素認証ができること。

⑵　認証デバイスとして以下を選択できること。

・　外付けカメラ（顔認証用）

・　内蔵 Web カメラ（顔認証用）

２　動作環境（端末、接続先）

⑴　利用者端末のログオン先が WORKGROUP 環境であってもドメイン環境であっても利用できること。

⑵　ファットクライアントを利用する場合、以下の OS に対応していること。

・　Windows 11 Pro/

⑶　ライセンスについては端末台数とし、必要台数は 512 台とする。

３　本人認証機能

⑴　生体情報による本人認証

⑵　顔による本人認証が可能であること。

⑶　顔認証を提案する場合、以下の機能を有すること。

・　端末利用ユーザが離席した際、一定時間経過後、画面ロックが可能なこと。

・　認証成功/失敗時の顔写真データをログとして保存できること。

・　一定間隔で端末利用ユーザが本人であるということ確認し、認識できない場合、画面をロックする機能を有すること。

・　顔の特徴点データは認証時の最新のデータで更新できること

※　顔写真データで登録しても認証時に更新されること。

・　まばたきを検知し写真によるなりすまし対策ができること。

・　顔の特徴点データを１ユーザが複数登録できること。

・　マスクを着用した状態でも顔認証が行えること。その際、サーバに登録する顔情報はマスクを着用していない状態の顔情報のみでよいこと。

・　マスクを着用した状態でもなりすまし対策のまばたき検知が行えること。

・　顔認証エンジンが国産であること。

・　生体認証時に、任意のパスワード（Windows、認証システム独自パスワード）を入力することでログオンできること。

・　生体認証機器を利用している場合でも複数の Windows アカウントの利用ができること。

・　顔情報の登録は、既に存在する顔写真から一括して取り込む方法、利用者個別に顔撮影と同時に登録する方法の両方が利用可能であること。また、利用者端末上で利用者本人の操作で本人認証後に自身で顔情報が登録可能であること。
・ 顔情報の登録は、顔写真データから一括登録することができること。顔写真データは、既存の顔画像ファイルもしくは、生体認証システム付属の撮影ツールを用いて顔画像を撮影し、顔写真のデータにできること。
・ 顔情報の登録は、利用者端末上で利用者本人の操作で、本人認証後に顔情報の登録ができること。
・　顔認証時にカメラで映している顔認証の照合画面を表示する事が可能であること。また照合画面を非表示にすることも可能であること。
・　認証サーバ上で顔画像を保存せずに顔の特徴点データのみでも利用が可能なこと。

4　ユーザ管理

⑴　認証サーバで、ユーザデータの一元管理ができること。
⑵　オフライン状態でもクライアントでの認証が行える機能を有すること。
⑶　ＡＤが有る環境、無い環境のどちらでもユーザ管理ができること。
⑷　ユーザ認証基盤としてＡＤを利用する場合やＡＤと連携する機能を利用する場合、ＡＤに対してスキーマ拡張、新規モジュール、新規テンプレートなどを適用しなくても導入可能なこと。
⑸　ＡＤと連携して、ＡＤにユーザ追加／削除することで自動的に認証サーバにユーザ追加／削除できること。
⑹　ＡＤのセキュリティグループ単位でユーザ管理ができること。
⑺　ユーザ情報の追加/変更/削除など一括でのユーザ管理が可能なこと。

5　ログ機能

⑴　利用者の認証時のログを収集するログサーバ機能を有していること。
⑵　認証サーバでの管理者による操作ログが収集できること。
⑶　各端末でのユーザ認証に関して、ログを収集可能なこと。また、ログ送信時は暗号化されていること。
⑷　ログ出力の項目として「日時」「コンピュータ名」「IP アドレス」「ログオンユーザ名」を取得可能で、二次利用可能な形式で保存可能なこと。
⑸　共有アカウントを利用したログオン操作に関して、ユーザを特定できる内容がログ出力されること。
⑹　利用者ログを複数人の管理者が同時に閲覧できる機能を有すること。
⑺　各端末がオフライン状態でのログに関して、オンラインに切り替わった際にログサーバにログ送信できること。

(8) 顔認証利用時に認証成功/失敗時の顔写真データをログとして保存できること。

6 運用管理

(1) 共有端末等での運用に際して、一つのWindowsアカウントを複数の利用者で利用する場合、ログオフを行うことなく、利用者の入れ替わりが可能なこと。

(2) 認証サーバでの管理者操作画面には、認証サーバ独自のIDとパスワードでログインが可能であり、ＡＤ上の特別な権限は不要であること。

(3) クライアント端末メンテナンス操作について、運用管理者による実機操作で、認証システム独自のパスワードでWindowsログオン可能なこと。

(4) 認証クライアントソフトの展開に関して、サイレントインストールが可能なこと。

(5) 別途管理用の端末を用意しなくともシステムの管理ができること。

(6) クライアント端末の設定を、サーバから変更して、クライアント側に反映させることができること。

別紙３　端末一覧

(1)　パソコン（60 台）

仕様項目	内容
型式	ノートパソコン
ＣＰＵ	インテル　Core™ i5-1335U
メモリ	8GB
ディスプレイ	15.6 型（1920×1080 ドット同等又はそれ以上）
ストレージ	SSD 256GB
キーボード	テンキー付きキーボード
有線 LAN	1000BASE-T
インターフェース	USB Type-A を２個 有線ＬＡＮポート HDMI
Web カメラ	HD 解像度（720P）対応カメラ/有効画素数 92 万画素
ＯＳ	Windows 11 Pro 日本語版（64bit）
アプリケーション	Microsoft Office LTSC profesional 2021

(2)　パソコン（370 台）

仕様項目	内容
型式	ノートパソコン
ＣＰＵ	AMD Ryzen™ 5 7535U
メモリ	8GB
ディスプレイ	15.6 型
ストレージ	SSD 256GB
キーボード	テンキー付きキーボード
有線 LAN	1000BASE-T
インターフェース	USB Type-A を２個 有線ＬＡＮポート HDMI
Web カメラ	HD 解像度（720P）対応カメラ/有効画素数 92 万画素
ＯＳ	Windows 11 Pro 日本語版（64bit）
アプリケーション	Microsoft Office LTSC Standard 2021

(3) パソコン（22台）

仕様項目	内容
型式	ノートパソコン
ＣＰＵ	インテル　Core™ i5-1335U
メモリ	8GB
ディスプレイ	15.6型
ストレージ	SSD 256GB
キーボード	テンキー付きキーボード
有線LAN	1000BASE-T
インターフェース	USB Type-Aを２個 有線ＬＡＮポート HDMI
Webカメラ	HD解像度（720P）対応カメラ/有効画素数92万画素
ＯＳ	Windows 11 Pro 日本語版（64bit）
アプリケーション	Microsoft Office LTSC Standard 2024

別記

個人情報取扱特記事項

（基本的事項）

第１条　受注者は、個人情報（特定個人情報を含む。以下同じ。）の保護の重要性を認識し、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、個人情報を適正に取り扱わなければならない。

（適正管理）

第２条　受注者は、この契約による事務に関して知り得た個人情報の漏えい、滅失、き損の防止その他の個人情報の適正な管理のために必要な措置を講じなければならない。

２　受注者は、前項に定める必要な措置として、個人情報の取扱いに係る管理規程等を整備するとともに、管理責任者を選定して管理体制を整備しなければならない。

３　受注者は、この契約における個人情報を取り扱う場所（以下「作業場所」という。）及び保管場所を定め、入退室の規制、防犯防災対策その他の安全対策の措置を講じなければならない。

４　受注者は、この契約の業務に着手する前に、前２項に規定する措置のうち、必要な事項について書面により発注者に報告しなければならない。

（秘密の保持）

第３条　受注者は、この契約による事務に関して知り得た情報をみだりに他人に知らせてはならない。この契約が終了し、又は解除された後においても同様とする。

（事務従事者への周知）

第４条　受注者は、この契約による事務に従事している者（以下「事務従事者」という。）に対し、次の各号に掲げる個人情報の保護に関して必要な事項を周知しなければならない。

(1)　在職中及び退職後においても、この契約による事務に関して知り得た個人情報をみだりに他人に知らせ、又は不当な目的に使用してはならないこと。

(2)　作業場所から個人情報を無断で持ち出してはならないこと。

(3)　前２号に掲げるもののほか、個人情報を保護するために必要と認めること。

（教育の実施）

第５条　受注者は、事務従事者に対し、この契約により遵守しなければならない事項、個人情報に関する法令等（寝屋川市個人情報の保護に関する法律施行条例及び寝屋川市個人情報の保護に関する法律施行細則を含む。）に関し、必要な研修を実施しなければならない。

（収集の制限）

第６条　受注者は、この契約による事務を行うために個人情報を収集するときは、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。

（目的外利用・提供の禁止）

第７条　受注者は、この契約による事務に関して知り得た個人情報を契約の目的以外の目的のために利用し、又は第三者へ提供してはならない。

（複写又は複製の禁止）

第８条　受注者は、発注者の承諾がある場合を除き、この契約による事務を行うために発注者から引き渡された個人情報が記録された資料等を複写し、又は複製してはならない。

（再委託の禁止）

第９条　受注者は、発注者の承諾がある場合を除き、この契約による事務を処理するための個人情報を自ら取り扱うものとし、第三者に当該事務を委託してはならない。

２　受注者は、委託業務の一部を再委託するときは、再委託先において個人情報を適切に取り扱うことができることを確認した上で、その内容を発注者に報告し、再委託することについて発注者の承諾を受けなければならない。

３　前２項の規定は、再委託先が再々委託を行う場合以降も準用する。

（実地による調査等）

第 10 条　発注者は、委託業務に関する個人情報の取扱について、この特記事項に基づき必要な措置が講じられているかどうか受注者に報告を求め、必要があると認めるときは、実地の調査を行うことができる。

２　受注者が、委託業務の一部を再委託するときは、再委託される業務に係る個人情報の秘匿性等その内容やその量等に応じて、受注者を通じて又は発注者自らが前項の措置を実施する。個人情報の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。

（資料等の返還等）

第 11 条　受注者は、この契約による事務を処理するために、発注者から提供を受け、又は自らが収集し、若しくは作成した個人情報が記録された資料等（以下「資料等」という。）を厳重に保管し、この契約が完了、その他の理由により終了し、又は解除された場合は、直ちに発注者に返還し、又は引渡し、そのことを書面で報告するものとする。ただし、受注者が資料等を直ちに発注者に返還し、又は引渡すことができない特別の事情があると発注者が認める場合は、受注者が資料等を廃棄又は消去し、そのことを書面で報告するものとする。

（事故発生時の報告）

第 12 条　受注者は、この契約に違反する事態が生じ、又は生ずるおそれがあることを知ったときは、速やかに発注者に報告し、発注者の指示に従うものとする。この契約が終了し、又は解除された後についても同様とする。

（契約の解除及び損害賠償）

第 13 条　発注者は、次の各号のいずれかに該当するときは、この契約の解除及び損害賠償の請求をすることができる。

(1)　この契約により取り扱う個人情報について、受注者又は第９条における再委託先等の責めに帰すべき理由による漏えい、滅失又はき損等があったとき。

(2)　前号に掲げる場合のほか、受注者がこの特記事項に違反し、委託業務の目的を達成することができないと認めるとき。