伊予市個人番号利用事務系ネットワークサーバーサービス提供業務

別添資料

令和６年４月
愛媛県伊予市

目次

1. システム個別要件

システムの個別要件については、下記のとおりとする。

なお、本システム要件は設定に係る最低限の方針を定めるものであり、詳細の設定情報については受注後本市と行うこと。

1.1. 資産管理システム（新規構築）

個人番号利用事務系端末 200 台（上限）を対象に、SKY 株式会社の SKYSEA Client View 又は同等品を導入すること。個人番号利用事務系端末へのエージェントインストール作業は手順書を用意するとともに必要に応じて技術支援を行うこと。標準化の要件とされているログ取得への対応を行うとともに、配備する端末では Microsoft365 を導入することから、効率的な環境整備が可能である提案を行うこと。

(1) 必要なログの要件

(ア) 操作ログ

操作者 ID 日時等の管理

(イ) 表示画面のハードコピー機能

(ウ) 表示画面のハードコピー印刷機能

(エ) クライアント操作(OS ショートカットキー、他社アプリケーション製品等)

(オ) 印刷ログ

オプション連携が必要であればそれも含めて提案を行うこと。

① 印刷者 ID・印刷日時等の管理

② 住民情報システムからクライアントへ出力されたログの管理

(カ) プレビュー、印刷、ファイル出力等

① クライアントからプリンタへ出力されたログの管理

② 出力した印刷イメージの記録

印刷イメージの取得のため、PRINT EYE for SKYSEA Client View 又は同等品を導入すること。

(ケ) バックアップしたログデータに関して、管理機から変換することなく検索できること。

(2) USB デバイス管理

(ア) USB デバイスの種別やデバイス種別に対応するメディアごとに、一括で使用不可/読み取り専用/使用不可能の設定ができること。

(イ) USB デバイスをコンピュータに挿入した際、利用した USB デバイスのシリアルナンバー、ベンダーID を自動で収集し、管理台帳を作成できること。

(ウ) 台帳上で指定した USB デバイスを使用許可/不許可を設定できること。

(エ) 管理台帳に登録されたメディアに対して個体識別情報を自動発行し、メディアごとに使用不可/読み取り専用/使用不可能を設定できること。

(オ) USB メモリ等の端末への着脱日時と記録されたファイル情報を確認できる

こと。

(カ) 管理台帳に登録されている USB メモリについて、USB メモリをクライアントコンピューターに挿入することでその有無を一括管理でき、管理台帳に反映できること。

(3) Microsoft３６５の管理に関する要件

(ア) クライアントコンピューターにインストールされている Microsoft Office 製品の更新（アップデート）や、展開（インストール）を設定する機能を有すること。

(イ) Microsoft Office 製品や更新プログラムを配布する配布端末の管理や、配布端末に設定する配布ポイントの管理ができること。

(ウ) 部署ごとに Microsoft Office の更新（アップデート）設定の適用を制御できること。

(4) その他の要件

(ア) ソフトウェアについては、契約期間中に有効な保守契約をメーカーとの間で結んでおき、電話、E-Mail、Fax による問い合わせサポート、メーカーで提供するユーザー向け情報提供 Web サイトの利用、最新版へのソフトウェアバージョンアップが行えるようにしておくこと。

1.2. 生体認証システム（新規構築）

個人番号利用事務系での環境構築を目指し、顔認証システムを採用、個人番号利用事務系端末 200 台（上限）を対象に、株式会社ディー・ディー・エスの多要素認証基盤 EVEMA 又は同等品を導入すること。

(1) 基本要件

(ア) Windows ログオン時又は各種アプリケーションへのログイン時（仮想環境へのログインを含む）、もしくはその両者において、「生体認証（顔認証）」が可能な認証システムであること。

(イ) 怪我等で登録あるいは認証が容易に出来ない場合には、管理者が発行する一時的なパスワードにより認証させることが出来るなどの代替措置をとることが可能であること。

(ウ) ドメイン環境のクライアント端末、ワークグループ環境のクライアント端末及び仮想環境上で動作する仮想サーバーに認証機能が使用できること。その際、仮想環境上で認証ハードウェアを利用できること。

(エ) ネットワーク途絶等により認証サーバーを利用できない場合には、クライアント端末単独でログオン認証を代替できるオフライン認証機能を有すること。

(オ) 既定の認証装置が利用できない場合の代替ログオン手段として、一時的に利用可能な緊急時パスワードで認証を行える機能を有すること。また、緊急時

パスワードは、利用可能な日付および回数を制限できる機能を有すること。

(カ) 認証時のログは Windows 標準のイベントビューアーに出力する機能を有すこと。また、ログを一覧化するためのビューアー機能が標準機能として含まれていること。ログについては必要に応じて解析を行うこと。

(キ) 将来的に指紋、手のひら、指静脈認証などの多様な認証装置を選択適用できる拡張性を有し、将来的な認証要素見直しに容易に対応できる認証システムであること。

(ク) 管理者メンテナンス性の向上のため、リモート接続による生体認証を用いた認証が可能であること。

(ケ) 将来的にシンクライアント端末や仮想デスクトップ環境に移行した場合でも、追加オプションではなく既存環境で生体認証が対応できること。

(コ) 本システムの機能により、ドメインユーザーの認証要素を使い個人番号利用事務系端末のローカルユーザーによるログインが可能であること。

(サ) ログオン後の業務アプリケーションに対して、アプリケーション側を改修することなく、多要素認証機能によりセキュリティを強化できる機能を有すること。

(2) 顔認証エンジンについて

(ア) 顔認証サーバーのリソースについては、全職員分の認証情報（顔情報、パスワード情報等）及び認証時のログを格納できる容量を確保すること。

(イ) 顔写真や動画によるなりすましを防止するため、パッシブ方式（対象物の画像情報から距離情報を取り出す方式）による偽造対策が顔認証エンジンにより取られていること。あわせて認証時に顔の左右向きを指定し、その動作を確認する機能が搭載されていること。

(3) 特記事項

(ア) 修正パッチの適用及びソフトのアップデート等が必要な場合は保守範囲で対応すること。

(イ) LAN インターフェース冗長化及び障害対策の設定

(ウ) クライアント PC へのクライアントソフトのインストール支援

(エ) 顔情報等の登録手順の提示

1.3. AD サーバー（2 台、既存から移行及び新規構築）

現行 AD 環境よりリソースやポリシーを移行しつつ、最新 OS にて再構築を行うこと。

(1) 基本要件

(ア) ユーザー及びデバイスを管理するためのグループポリシーの提案を行い設定すること。なお、内容については受注後本市と協議すること。

1.4. ファイルサーバー（既存から移行及び新規構築）

現行ファイルサーバーよりデータを移行しつつ、最新 OS にて再構築を行うこと。

(1) 基本要件

(ア) ファイルの容量を効果的に使うよう適切な設計を行うこと。またデータのバックアップを行うとともに、ユーザーが誤ってファイルサーバー上のデータを削除してしまった場合も、データ復旧を簡易に行うことが出来るよう設計を行うこと。バックアップの保存期間については、市担当者と協議の上決定する。

1.5. ウイルス対策サーバー（新規構築）

個人番号利用事務系端末 200 台及び個人番号利用事務系サーバーを対象に、Trend Micro 社の Apex One を導入する。（ライセンスは本市が保有するものを使用する。）なお、個人番号利用事務系端末へのエージェントインストール作業は手順書を用意するとともに必要に応じて技術支援を行うこと。本サーバーはインターネット接続が出来ないため、自治体情報セキュリティ向上プラットフォームからパターンファイルを取得出来るよう設定を行うこと。

(1) 基本要件

(ア) 最新のパターンファイルが適用出来る設定を行うこと。

(イ) 本製品に関する脆弱性に関する情報収集については適宜実施し、対応パッチが公開された場合は速やかに市担当者と協議し、適用時期や適用までの暫定対応について決定すること。

(ウ) ウイルス対策ソフトがウイルスを検知した場合に本市担当者及び受託者が通知を受け取ることが可能な設定を行うこと。また、対策や原因の究明について対応を行うこと。

1.6. 監視サーバー（新規構築）

監視対象は本業務で導入するサーバー機器、仮想マシン及びネットワーク機器とする。監視内容は契約締結後、本市と協議のうえ決定すること。本市指定のメールアドレスに対してメール通知設定を行うこととリソースの監視及び分析を行い定期的に本市担当者に報告を行うこと。

(1) 基本要件

(ア) OS、バージョンについては構築時点での最新版もしくは伊予市と協議の上決定することとする。

(イ) 不具合時には本市担当者及び受託者に速やかに通知がいくものとする。

(ウ) 更改時にはサイジングの問題がないよう、常時状態（リソース状況）が分かるような構成を実装すること。

1.7. WSUS サーバー(新規構築)

個人番号利用事務系端末 200 台及び個人番号利用事務系サーバーの Windows Update を集約するために WSUS サーバーを構築する。なお、更新プログラムの取得先は自治体情報セキュリティ向上プラットフォームとする。なお、必要なアップデートのタイ

ミングや作業について本市担当者と協議のうえサポートを実施すること。

1.8. プリントサーバー（新規構築）

個人番号利用事務系端末が利用するプリンタの制御を行うため、プリントサーバーを構築する。

(1) 基本要件

(ア) プリントサーバーへ登録するプリンタは同年度に別事業で調達を予定している。

(イ) プリンタドライバはメーカー提供のものを本市が準備する。

1.9. 地籍サーバー（物理サーバーから令和 7 年度移行予定）

アプリケーションの構築は本市指定の別事業者が行うため、仮想マシンの作成及び OS インストールまで行うこと。

1.10. 税務 LAN サーバー（物理サーバーから令和 7 年度移行予定）

アプリケーションの構築は本市指定の別事業者が行うため、仮想マシンの作成及び OS インストールまで行うこと。

1.11. その他

1.11.1. 他機関とのオンライン連携

公的な機関等からオンラインでのデータ連携について対応ができる構成にしておくこと。

例：軽自動車検査協会に納税情報をオンラインで連携

1.11.2. 暗号化に関する要件（推奨）

ファイルの暗号化について、効果的で省力化が可能なものを提案すること。

2. 報告書及び成果物一覧

(1) 次のドキュメントを、印刷物及び電子記録媒体にて各 1 部提出すること。

(ア) 要件定義書（業務要件、機能要件、非機能要件等）

(イ) 設計書（システム・機器等）

(ウ) 納入機器等一覧

(エ) ネットワーク接続図、サーバーラック搭載図

(オ) フォルダ構成図、アクセス権限一覧

(カ) 運用・操作マニュアル（管理者）

(キ) 操作マニュアル（利用者）

(ク) 保守体制図

(ケ) 移行関連資料

(コ) 結果報告書（テスト・移行等）

(サ) 作業報告書

(シ) その他本市が必要と認めた書類