伊予市テレワーク環境構築事業

要件一覧

令和 7 年 12 月
愛媛県伊予市

目次

1. Microsoft 365 利用環境構築に係る個別要件

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協議の上決定すること。

1.1. ファイルサーバー（既存から移行及び新規構築）

(1) 既存のファイルサーバーで保存しているデータをクラウドに移行する。

(2) 市や組織として管理・利用するデータは、SharePoint Online、個人で管理・利用するものは OneDrive に保存する想定である。

(3) データ移行は原則職員が実施するが、サイト、フォルダ作成及び適切なアクセス権の設定を市と協議したうえで設定すること。フォルダ作成と共有手順、アクセス権設定の手順書を用意すること。実データの移行方法やツール選定、作業上の支援については(9)に定める。

(4) クラウドストレージの容量は 5TB 以上とすること。

(5) 利用者が従来の共有ドライブと同様の操作感で利用できるよう、Windows エクスプローラからのファイル操作（閲覧・編集・ドラッグ&ドロップ・コピー/移動）が可能となる構成とすること。

(6) Windows 10/11 で利用しているデバイスのマイドキュメント、マイピクチャ及びデスクトップに保存されているデータは、原則としてユーザー毎の OneDrive に保存されるよう Intune で設定すること（Known Folder Move（KFM）等の機能を用いることを想定する）。

(7) クラウドと端末の両方で保存されているデータについては、一定期間利用しない場合に端末からデータを自動的に廃棄し、クラウド側を原本とする運用とすること（Files On-Demand 等を用いた構成を想定する）。具体的な期間や挙動は、市と協議のうえ決定すること。

(8) クラウドストレージサービス上に保存しているデータは、原則組織外への共有はできないようにするが、特定サイトのみ組織外への共有を許可するよう設定を行うこと。対象サイトについては市と協議し決定すること。

(9) クラウドストレージサービス上のデータ肥大化が発生しないよう保持できるデータサイズの上限値を設定する。複数の世代を保持できる Office アプリについては、市と協議して保持する世代数を決定すること。

(10) OneDrive に保存しているデータについても、組織外への共有はできない設計とするが、今後外部共有を行うことも想定されることから、外部共有する際の手順書を用意すること。

(11) データ移行作業そのものは発注者側で実施する。ただし、事業者は以下の点について支援を行うこと。

① 適切な移行ツール・方法の提示

② ツールの使用方法の説明（必要に応じた操作マニュアルの提供を含む）
③ 作業計画や手順に関する助言
④ 発注者による作業中に発生した不具合に対する技術的な問い合わせ対応

1.2. メール（既存から移行及び新規構築）

(1) インターネット系メールシステムをクラウドサービス型メールへ移行することとし、運用中のメールドメインについてもクラウド側へ移行対象とすること。

(2) LGWAN 系メールについてもクラウドサービス型メールへ統合し、職員が単一のメールアドレスでインターネット系・LGWAN 系双方に対して送受信できる環境を構築すること。

(3) 本システムでは、職員個人のメールアドレスに加え、部署・係・業務用の共有メールアドレスを複数運用することを想定している。これらの共有アドレスの追加に伴い、ユーザーライセンスを別途購入する必要が生じないメールサービスとすること。

(4) LGWAN とクラウドサービス型メールの間でメール中継を行うメールリレーサーバー（仮想マシン）を経由して配送する方式とする。ただし、メールリレーサーバーの構築及び運用保守は本事業の対象外とし、既存の仮想基盤保守事業者側で対応することとする。

(5) 上記構成に伴い、クラウドメールサービスとメールリレーサーバー間の接続試験、疎通確認、メール配送に関するトラブル発生時の原因切り分けなどについては、関連事業者と連携し原因切り分けに必要な技術的協力を行うこと。

(6) メールドメインのクラウドサービス側への移行については、市が主体となって手続きを実施するものとする。ただし、移行作業に必要な DNS 設定変更の内容、手続きの流れ、影響範囲について、市が適切に判断できるよう専門的な助言を行うこと。

(7) クラウドサービス型メールにおいて利用するメーリングリスト、共有メールボックス、グループ設定については、市と協議のうえ設計・登録を実施すること。

(8) クラウドサービス型メールとして Microsoft Exchange Online を利用する場合、必要となる既設 Active Directory（AD）サーバーのスキーマ拡張に関する手順書を作成し、市を通じて既存保守業者に提示すること。

(9) メール送受信におけるファイル無害化機能を適用し、安全なメール運用を実現すること。

(10) メールの利用環境として、Web ブラウザ、Outlook クライアント、BYOD 端末のスマートフォンアプリからのアクセスを可能とすること。

(11) Outlook クライアントのプロファイル設定、初回セットアップ、Exchange Online との接続設定が利用者操作なしで完了するよう、必要な構成を事前に実施すること。

(12) メール保存期間、キャッシュモード、添付ファイルの扱い、アーカイブ、署名、迷惑メール設定など、自治体業務に適した Outlook の推奨設定を市と協議し、事前に反映すること。

(13) 職員が円滑に利用開始できるよう、メール操作方法及び Outlook の利用手順を含む利用者向けマニュアルを作成し、市へ提示すること。

1.3. チャット・WEB 会議ツール（新規構築）

(1) Microsoft Teams 会議等の外部接続を伴うサービスについては、総務省ガイドライン β' モデルを参考に基本設計を行うこと。

(2) 他自治体での導入実績を踏まえた推奨構成を提示し、市の要望に応じて最適な設計を行うこと。

(3) 利用開始時は庁内での利用を基本とし、外部ユーザー招待は Teams 会議への参加のみ許可し、外部とのチャット・ファイル共有は無効化した構成とすること。

(4) 将来的に外部共有を有効化する可能性を踏まえ、外部共有設定の変更手順及び運用フローを管理者向けマニュアルとして作成・提示すること。

(5) Teams のチャット、通話、Web 会議、画面共有等の基本操作について、利用者向けマニュアルを提示すること。

(6) 会議録画データの保存場所・保持期間・公開範囲については、市と協議の上決定すること。

(7) チャット履歴、会議ログ等の監査ログの取り扱いは、市の情報セキュリティ方針に基づき、市と協議の上決定すること。

(8) Microsoft Teams のチーム／チャネルで共有されるファイルは、原則として対応する SharePoint Online サイト（ドキュメントライブラリ）上のデータとして保存されることを前提とし、権限設定・保持ポリシー・バックアップ方針が本項のファイルサーバー要件と一貫するよう設計すること。

(9) 利用者が Teams の「ファイル」タブからアクセスする場合であっても、当該ファイルの実体は SharePoint Online 上の原本とし、エクスプローラ（OneDrive 同期）を通じたアクセスとの間で整合性が保たれるようにすること。

2. 利便性の高さと経済性を備えたグループウェアの選定に関する個別要件

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協議の上決定すること。

2.1. グループウェア（既存から移行及び新規構築）

(1) 現在利用している Desknet's NEO から置き換えとなる。Microsoft 365 製品又は別のクラウドサービスにて対応するものとする。

(2) 現在 Desknet's NEO で利用しているポータルサイトの機能としては、スケジュール、設備予約、掲示板、リンク集、文書管理（マニュアル・様式集)、ワークフロー、アンケートがあるため、これらが現行と同等の機能で利用できること。

(3) ユーザーインターフェース（UI）は、職員が PC やスマートフォンなど、いかなるデバイスからアクセスしても見やすく、使いやすい画面となるようデザインし、各機能へのアクセスが直感的かつ効率的に行えるように配慮すること。

(4) スケジュール機能は、職員の個人及び組織の予定を効率的に管理・共有するための機能として、以下の要件を満たすこと。

・個人及び組織予定の管理：ユーザーは、自分の個人予定と組織の共有予定を 1 つの画面で統合的に管理・表示でき、簡単に切り替えて確認できること。また、過去の予定や会議をキーワードや日付で検索が可能であること。

・会議作成と設備予約連携：会議作成時に複数人を招待し、会議室や備品などの設備予約と連携して、予約状況を自動的に反映できること。

・繰り返し予定と通知機能：定期的な予定を繰り返し設定でき、予定や変更について自動通知を参加者に送信できること。

(5) 設備予約機能は、会議室や備品などの施設予約を効率的に行うことが出来るものであり、以下の要件を満たすこと。

・既存グループウェアに登録されている施設や備品を事前に登録し、予約可能な状態にすること。登録内容については別途市から提示するものとする。

・予約時には、重複予約防止機能が働き、同じ設備に対する重複予約が行われないようにすること

・設備の空き時間を検索し、利用者が予約可能な時間帯を簡単に確認出来ること。

・予約内容の変更やキャンセルが可能で、その際に自動で関係者に通知が送られること。

(6) 掲示板機能は、職員間で情報共有を効率的に行うための機能として、以下の要件を満たすこと。

・投稿機能：職員が簡単に投稿できること。投稿内容には、タイトル、本文、添付ファイルが含まれることができ、画像やリンクの埋め込みも可能であること。

・閲覧機能：掲示板への投稿は誰でも閲覧可能であり、投稿日時や投稿者名が明記されること。

・カテゴリ分け機能：掲示板の投稿をカテゴリやタグで分類できること。カテゴリ別にフィルターをかけて、必要な情報をすぐに探し出せる機能を搭載すること。

・検索機能：掲示板内の投稿をキーワードやタグ、カテゴリで簡単に検索でき

ること。

・通知機能：新しい投稿などがあった際、通知機能があり、利用者が適切に情報をキャッチできるようにすること。

・権限管理機能：掲示板の管理者が投稿内容や閲覧者の権限を管理できること。特に、一部の掲示板に対して制限を設け、特定のグループや部署だけがアクセスできるようにする機能を提供すること。

・投稿の編集/削除機能：投稿者が自身の投稿内容を編集・削除できること。また、管理者が不適切な投稿に対して編集・削除を行うことができること。

(7) リンク集機能は、職員間で必要なウェブサイトや社内リソースを効率的に共有するための機能として、以下の要件を満たすこと。

・リンク管理機能：ユーザーは、リンクの追加、編集、削除が可能で、リンクごとにリンク名、URL、説明、カテゴリを設定できること。

・アクセス権限管理：リンク集への編集権限は管理者に制限され、一般ユーザーは閲覧のみができるように設定されること。

(8) 文書管理（マニュアル・様式集）機能は、職員間で文書を効率的に管理・共有するための機能として、以下の要件を満たすこと。

・ユーザーは、文書をシステムにアップロードし、フォルダ階層を用いて文書を整理・管理できること。

・各文書に対して、閲覧、編集、削除の権限をユーザー単位又はグループ単位で設定できること。

・文書の検索機能として、タイトル、タグ、作成者、更新日などで文書を簡単に

検索できること。

・バージョン管理機能を提供し、文書の変更履歴を管理し、過去のバージョンを復元できること。

(9) ワークフロー機能は、申請・承認・回覧等の業務プロセスをオンライン化し、その可視化及び効率化を図る機能として、以下の要件を満たすこと。なお、具体的に対象とする申請業務については、本市と協議のうえ決定すること。

・最大 6 段階まで承認の階層を設定でき、複数人に申請内容を回覧できること。

・依頼者は承認がどこまで進んでいるか確認できること。

・発信した承認依頼、依頼されている承認タスクを一覧で表示できること。

(10) アンケート（フォーム）機能は、職員向けの意向把握・回答収集・集計・共有を安全に行う機能として、以下の要件を満たすこと。

・単一/複数選択、記述、分岐ロジック、必須/任意を設定でき、組織内限定配布（全庁/部門/グループ）、期間限定公開に対応できること。

・1 人 1 回等の重複回答防止、匿名/記名の切替を選択可能であること。

・回答の自動集計・可視化（グラフ等）に対応し、CSV/Excel 等へのエクスポート及び権限を制御した結果共有が可能であること。

(11) ベースとなるポータルサイトや掲示板、リンク集等へのアクセスは、庁内の Windows11 及び BYOD のスマートフォンからのアクセスを想定している。SharePoint Online をベースとして構築する場合は、モダン UI のサイトで構築することとし、レイアウトや構成の検討には一定の時間を要することから、十分な検討期間を確保し市と協議の上決定すること。

(12) ポータルサイトは職員で変更する運用も想定されるため、想定される変更に対応できるよう管理者向けマニュアルを作成すること。

(13) グループウェアの新しいインターフェースに関して、利用者がスムーズに移行できるよう、利用者マニュアルを用意すること。

3. セキュリティ対策と管理者の省力化に関する個別要件

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協議の上決定すること。

3.1. 端末及びサーバーのセキュリティ対策（新規構築）

(1) 端末、サーバーを同じソリューションにて EPP（ウィルス対策)、EDR を構成し Windows Autopilot による自動展開時にオンボーディングすること。

(2) 対処不要なアラートに関しては、管理者に通知しないよう適正な設定を行うこと。

(3) 検出に関するオプション設定、拡張機能の設定を行うこと。なおポリシー設定、有効化/無効化設定に関しては、過去実績に基づく推奨設定を明示し、市と協議して構成すること。

(4) 疑似マルウェア等を用いて検出・通知の動作確認を行うこと。

(5) 端末情報の確認手段について、管理者向けマニュアルに記載すること。

(6) 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及び対象カテゴリ分類された 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によって、不要なカテゴリへのアクセスをブロックする設定を実施すること。方式及びカテゴリについては市と協議して構成すること。また、リストの追加と削除、カテゴリの変更手順を運用マニュアルに記載すること。

(7) Web フィルタリングについては、庁内だけではなく庁外からのインターネット利用時にも有効となるよう構成すること。

(8) β´モデルにおける継続的な脅威検知・モニタリング体制を確立するため、マネージドセキュリティサービス（MSS）を提供すること。

(9) MSS は 24 時間 365 日の常時監視を提供し、EDR 製品に関してアラートの一次

対応が可能な運用体制を提供すること。通知は対応が必要と判断されるアラートに限定し、不要通知を最小化すること。

(10) MSS で監視する対象は本件で調達・適用する EDR 製品とし、当該 EDR が管理する全ての対象端末（クライアント及びサーバ）を含むこと。

(11) 本市で対応が必要なことについては、不正アラート検知後速やかに連絡を行うこと。

(12) MSS にて検知した不正又はアラートについて調査・分析を実施し、一次対応（切り分け、封じ込め、隔離の実施又は実施指示等）を行った上で、速やかに推奨対応を報告すること。重大インシデントと判断される場合は、被害最小化のためネットワーク隔離を速やかに実施すること。

(13) 調査・分析・報告はセキュリティアナリストによる有人対応で行い、報告、連絡及び成果物は日本語で提供すること。

(14) インシデントの再発防止の為、マネージドセキュリティサービスの月次レポートにて再発防止策、改善策の提案を行うこと。

(15) サービス開始前に運用設計（通知基準、SLA、エスカレーション経路、連絡体制、定期会議体）を合意のうえ文書化し、サービス終了時又は延長時には、運用手順、検知・対応履歴等の引継ぎ資料を提出すること。なお、引継ぎ資料についてもサービス開始前に協議して決定するものとする。

3.2. クラウドサービスのセキュリティ対策（新規構築）

(1) メールにおけるファイル無害化に対応するため、フィッシング対策、安全な添付ファイル機能、安全なリンク機能、迷惑メールフィルター機能、マルウェア対策機能の有効化とポリシー設定を行うこと。ポリシー設定については、過去実績に基づく推奨設定を明示し、市と協議して構成すること。

(2) アラートが検出された際の通知設定を行うこと。通知先については別途指示とする。

(3) 疑似マルウェアファイル付きメール、疑似フィッシングメール（不正な URL のブロック確認）を用いて動作確認を行うこと。

(4) メールに加え、クラウド上のデータストレージ（個人用及び組織用）についても、メール同様に安全な添付ファイル機能を有効化し、マルウェア等を含むデータに対して隔離、廃棄などの対応が可能な構成とすること。

(5) メール及びクラウドデータのセキュリティ運用管理の責任範囲、検出ログの保持期間、アラート発生時の対応手順等を明示し、管理者向けマニュアルを作成すること。

3.3. 情報漏えい対策（新規構築）

(1) 業務端末の利用環境を統合的に管理し、情報漏えい対策及び不正アクセス防止を実現すること。本システムは、Intune 等の既存クライアント管理基盤と役割

が重複しないよう整理し、相互補完的に構成すること。

(2) 庁内領域及び庁外領域（USB メモリ等の外部記憶媒体、メール添付、Web アップロード、管理外サーバー、許可クラウド等）を論理的に区別できること。庁内領域の定義方法（ホスト名、IP アドレス、共有フォルダパス、URL 等）や具体的な範囲は、市と協議のうえ決定すること。

(3) 庁内領域から庁外領域へファイルを持ち出す際、ファイル拡張子に依存せず自動的に暗号化又は持ち出し禁止の制御ができること。暗号化されたファイルは、市が許可した端末又は環境でのみ復号可能とし、暗号化・復号は通常のファイル操作の延長で自動的に行われること。自動暗号化の対象範囲や例外の取扱いは、市と協議して構成すること。

(4) 庁外領域への正当なファイル持ち出しに対し、持出専用フォルダ等を用いた申請・承認の仕組みを有すること。承認済ファイルについては、パスワード付き暗号化 ZIP 等、平文での持ち出しを禁止する設定が可能であり、持ち出し先の種別（外部記憶媒体、メール、Web 等）に応じて許可する形式を制御できること。

(5) 利用者の操作ログ及び庁外領域への持ち出し履歴を取得し、ユーザー名、端末名、日時、対象ファイル名、操作内容、持ち出し経路等を特定できること。インシデント発生時に、いつ、だれが、何を、どのような手段で外部に持ち出したかを追跡できること。ログの保存期間や参照方法は、市と協議して構成すること。

(6) 庁内 PC のローカルドライブに保存可能な領域を特定の領域に制限できること。当該領域に保存されたデータを、管理者が指定したタイミング（起動・終了、ログオン・ログオフ、時間・曜日等）で自動削除できるとともに、必要に応じて遠隔から削除命令を実行可能であること。

(7) ファイル暗号化に用いる暗号方式として、AES 256bit 以上の暗号強度を利用できること。

(8) 未管理端末からのアクセスを禁止し、市が管理・登録した端末のみが業務ネットワーク及び業務システムに接続できること。公衆 Wi-Fi 等の不特定ネットワーク利用時にも、暗号化通信や接続先制御等により安全な通信環境を確保できること。

(9) 1 台の端末上で LGWAN 環境とインターネット環境（必要に応じて基幹系環境を含む）を論理的に分離し、利用者が簡易な操作で安全に環境を切り替えられること。有線 LAN、Wi-Fi アクセスポイント（SSID）、プロキシ、VPN 接続等の条件に応じて、接続可能な通信経路を制御できること。

(10) Intune 等の既存クライアント管理基盤では対応が困難な利用者支援（遠隔操作によるサポートや個別アプリケーションのインストール等）を行えること。

(11) 端末のOS及び主要アプリケーションの更新管理、脆弱性パッチ適用、セキュリティ状態の監視・可視化を定期的に自動実施し、管理者が容易に監査・確認できること。また、端末の利用状況について定期的なレポート出力が可能であること。

(12) 導入にあたり、構築事業者は初期設定支援及び管理者向けトレーニングを提供し、運用マニュアルに具体的な利用手順を記載すること。また、Active Directory や Entra ID 等のディレクトリサービスと連携し、ユーザー又はグループ単位での権限設定やポリシー適用が可能であること。必要に応じて、Intune やログオンスクリプト等を用いたサイレントインストールやアップデートを行えること。

(13) 運用管理負荷低減のため、上記要件を単一のソフトウェアで実現すること。

3.4. LGWAN 接続環境構築（新規構築）

(1) Windows11 端末及び市が指定する端末から LGWAN を利用するにあたり、端末本体にデータを残さない画面転送型ブラウザもしくは仮想デスクトップ環境を導入すること。これにより、業務端末に対する情報漏洩リスクを低減すること。LGWAN 環境内に存在する特定システムへのアクセスについて、円滑に切替可能な利用環境を提供すること。

(2) ブラウザ画面転送等により、ローカル端末にキャッシュや一時ファイル等を残さないこと。

(3) LGWAN システムへのアクセスについても、業務に支障がないよう適切に切替・利用できる仕組みを提供すること。

(4) 各種 Web アプリケーション（庁内業務で利用される LGWAN-ASP サービスや LGWAN 系システム等）が安定して動作すること。

(5) 利用者が業務上必要とする機能（印刷、ファイルのダウンロード、アップロード等）について、セキュリティ要件を満たす範囲で適切に制御可能であること。

(6) プロキシ経由での接続が必要となる LGWAN 上の特定サイトにも対応できること。また、クライアント側で PAC ファイル等によるプロキシ自動設定を利用できる構成とし、必要な設定作業については、本事業の構築事業者が主体となって提案すること。なお、PAC ファイルの配布方法や配信基盤の構成等の詳細については、本市及び関係事業者との協議により決定するものとする。

(7) ブラウザ更新時や OS 更新時も互換性を維持できること。また、障害発生時に他のアクセス手段へ切替可能であること。

(8) LGWAN 接続ブラウザ経由のログイン履歴を取得でき、管理者が必要に応じて監査可能であること。

(9) LGWAN 接続環境で利用する端末及びブラウザについて、更新手順や管理者運用マニュアルを作成し、利用者・管理者に提示すること。

3.5. バックアップ（新規構築）

(1) ファイルサーバーのデータ、Microsoft Teams、メールを対象としたデータバックアップができること。また、利用者の誤操作によりデータ紛失等が発生した場合は、本バックアップから復旧対応可能であること。

(2) バックアップ先は同一のデータセンターではない、別のデータセンターに保管できること。

(3) メール単体の復元から、メールボックスの復元まで可能であること。同様にファイル単位でも復元可能であること。

(4) ランサムウェアで暗号化されてしまった場合、暗号化される前に取得したバックアップデータより対象のデータを復旧できること。

(5) 本市が指定した領域のバックアップを行うよう初期設定を行うこと。

(6) 日次運用のバックアップ結果を確認し、エラー有無の確認を行うこと。エラーが発生している場合には報告を行い、原因と対処方法を調査すること。

(7) 日次の正常性確認及びリストア状況を、1 か月ごとに報告書として提示すること。

(8) リストア手順などが記載された管理者運用マニュアルを提示すること。リストアの際に不具合が発生した場合調査を行うこと。

(9) バックアップの保持期間は 5 年以上とする。

3.6. デバイス管理（新規構築）

(1) 新規に導入する Windows 11 デバイスは、Microsoft Entra Hybrid Join 構成となるため、Entra ID に登録されたデバイスを Microsoft Intune にオンボードすること。

(2) AD サーバーと Entra ID 間でデバイスオブジェクトの同期等が必要となる。既設 Microsoft Entra Connect で同期対象 OU の設定が必要となる認識である。手順書を作成して市経由で保守業者に提示すること。

(3) 登録デバイスに対して構成プロファイル及びコンプライアンスポリシーを適用する。構成プロファイルは、過去実績に基づく利用頻度の高い設定項目などを紹介し、コンプライアンスポリシーは、過去実績に基づく推奨設定を明示し、市と協議して構成すること。

(4) 庁内利用及び庁外利用それぞれに合う条件に応じたアクセス制御を Intune で構成する。庁外利用時には決められたポリシーに合致するデバイス（市が認めたデバイス）のみが Microsoft 365 環境に接続できるように制御する想定だが、詳細条件については市と協議して構成することとする。

(5) 端末の紛失や盗難があった場合に備えて、BitLocker による端末ディスクの暗号化をすること。

(6) 端末の紛失や盗難があった場合に備えて、データを遠隔で消去できるようにリ

モートワイプ機能を構成すること。本手順については、管理者運用マニュアルに記載すること。

(7) Windows Update の更新を管理ができること。Windows Update の管理については情報漏えい対策ソフトウェアとの役割が重複することなく、両者が相互補完的に機能すること。

(8) Windows Update for Business の設定及び配信を行うことで、回線帯域を軽減できるよう配信の最適化機能を利用すること。その他に関しては、過去実績に基づく推奨設定を明示し、市と協議して構成すること。

(9) アプリケーション制限、パスワードポリシー、ロック画面ポリシー等について過去実績に基づく推奨設定を明示し、市と協議して構成すること。

(10) 業務用端末に対して Microsoft 365 Apps のアプリケーションを配布すること。また、更新設定も行うこと。その他のアプリケーションについても、基本的には Intune にて配布を行う。配布するアプリケーションは、10 個程見込んでおくこと。証明書も配布すること。また、利用するプリンタも対象とすること。

(11) アプリケーション配布とプリンタ/複合機設定については、導入後に変更や追加となる可能性もあることより、手順について管理者運用マニュアルに記載すること。

(12) スマートフォン等の BYOD 端末の利用を想定しているが、こちらはデバイス管理（MDM）は行わず、アプリケーション管理（MAM）を実装すること。なお、MAM の利用にあたりデバイス登録が出来るよう手順書を用意すること。

(13) 業務用端末及び BYOD 端末の紛失や盗難があった場合に備えて、データを遠隔で消去できるようにリモートワイプ機能を構成すること。本手順については、管理者向けマニュアルに記載すること。なお、BYOD 端末については、個人領域には影響を与えないようにすること。

(14) アプリケーション管理について過去実績に基づく推奨設定を明示し、市と協議して構成すること。基本方針として、市の管理領域にあるデータを個人領域にコピーや保存をできないようにすること。

(15) BYOD 端末に対して Microsoft 365 Apps のアプリケーションを配布すること。また、配布するアプリケーションは、M365Apps を想定すること。

(16) アプリケーション配布は導入後に変更や追加となる可能性を考慮し、手順について管理者向けマニュアルに記載すること。

(17) 次期導入の端末では、Windows Hello を使用した生体認証によるログオンを想定しているため、Windows Hello for Business（WHfB）を構成すること。

(18) WHfB を導入する際、生体認証（指紋／顔）又は PIN を主要なサインイン方法とすること。

(19) WHfB の導入にあたり、Intune を介したキーのプロビジョニング、PIN 強度

ポリシー、生体認証設定などを構成し、管理者運用マニュアル及び利用者向け手順書に具体的手順を記載すること。

(20) 端末情報の確認手段について、管理者運用マニュアルに記載すること。

(21) その他、Intune にて実施する端末管理については、市と協議のうえ対応すること。

3.7. 端末展開（新規構築）

(1) 新規に導入する Windows 11 デバイスは Windows Autopilot を利用し、自動的に Microsoft Entra Hybrid Join で構成しながら展開できるようにすること。

(2) Autopilot で必要となるデバイス登録用のシリアルナンバー/Windows Product ID/Hardware Hash が記載された一覧ファイルを市で用意する。一覧ファイルを用いて Intune に登録すること。

(3) 一覧ファイルを用いた Intune へのデバイス登録、プロファイル割り当て、来年度導入予定端末の先行納入分（数台程度）を用いた AutoPilot 実機動作確認を構築事業者が実施し、結果を報告すること。

(4) 初回セットアップにおける利用者操作を最小化するため、AutoPilot プロファイルを自治体向けに最適化して構成すること（言語設定、キーボード設定、不要画面の非表示化等）。過去実績に基づく推奨設定を明示し、市と協議して構成すること。

(5) Microsoft Entra Hybrid Join の安定稼働に必要となる前提条件（ネットワーク要件、ドメイン参加に必要な接続要件、証明書、OU 同期設定等）を構築事業者が確認し、市に提示すること。必要に応じて既設 Entra Connect サーバーの OU 設定等を調整し、手順書として市に提示すること。

(6) 初回セットアップで必要な情報（通信先、プロキシ設定、証明書要件等）など一覧したものは市から提供するものとする。

(7) 担当者が端末を預かってセットアップする場合を想定し、操作手順・注意点を記載したマニュアル（利用者向け）を提供すること。

(8) 展開に失敗した場合の初期化、再登録、トラブル解決手順を管理者運用マニュアルに記載すること。

(9) 庁内での実際の作業時間や流れを踏まえて、1 台あたりの目安作業時間や作業工程を提示し、無理のない運用フローを市と協議して決定すること。

(10) その他、Autopilot を利用した端末展開に関する構築・運用事項については、市と協議のうえ対応すること。