大和高田市
仮想化基盤導入仕様書

令和7年度10月版

第1章 調達概要

(1) 経緯

本市では、令和３年の新庁舎移転に合わせて職員が利用する端末をネットワークごとに物理端末・仮想端末で切り分けた仮想環境を導入した。「端末管理の簡素化」、「執務環境の省スペース化」、「セキュリティの強化」を目的にとして、本市業務を本仮想環境で推進しているところである。

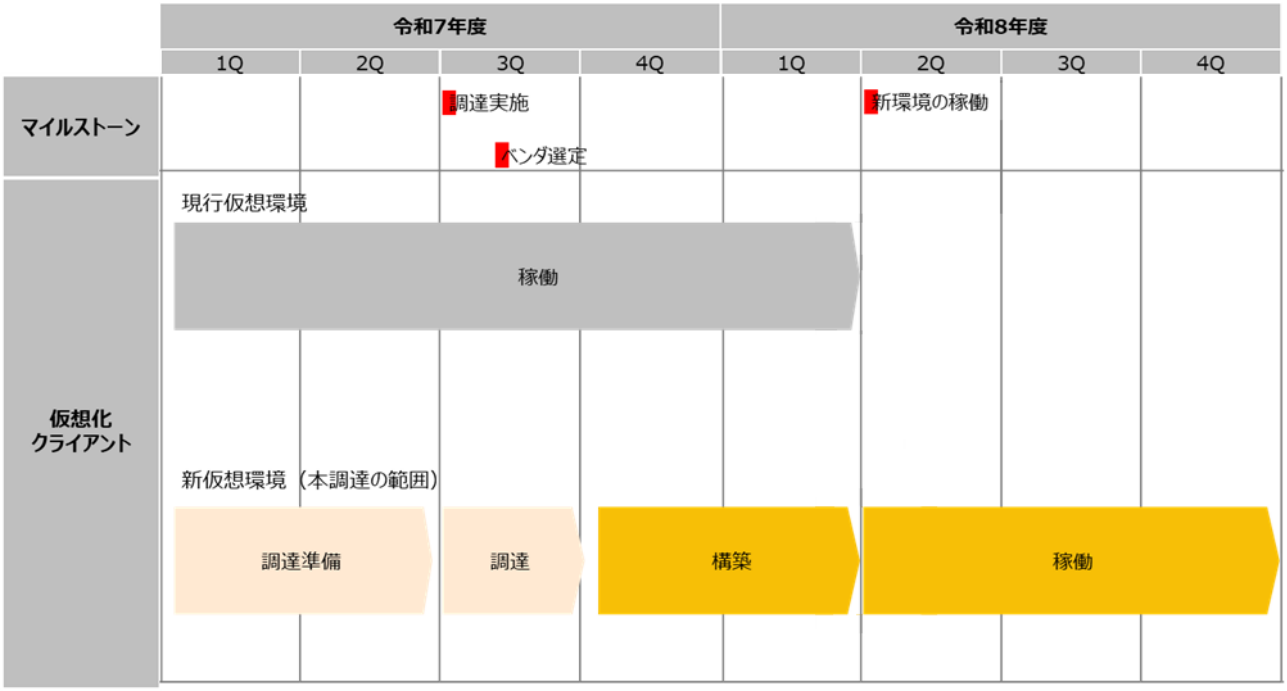
導入後５年を迎えるにあたり、総務省が推奨する三層分離モデルを踏まえたセキュリティ強化と構成見直しを行いつつ、さらなる端末利用の効率化、経費の削減などを念頭に置いた環境の見直しのため、本仮想環境の入れ替え・更新を行う必要がある。

新仮想環境においては、行政コストの適正化の観点から、費用と業務効率性のバランスをとった環境を目指していく。加えて、今後の行政・地域 DX を踏まえた柔軟な環境かつ、セキュリティにも強い環境としていく必要もある。

このような状況において、本調達を行うものである。

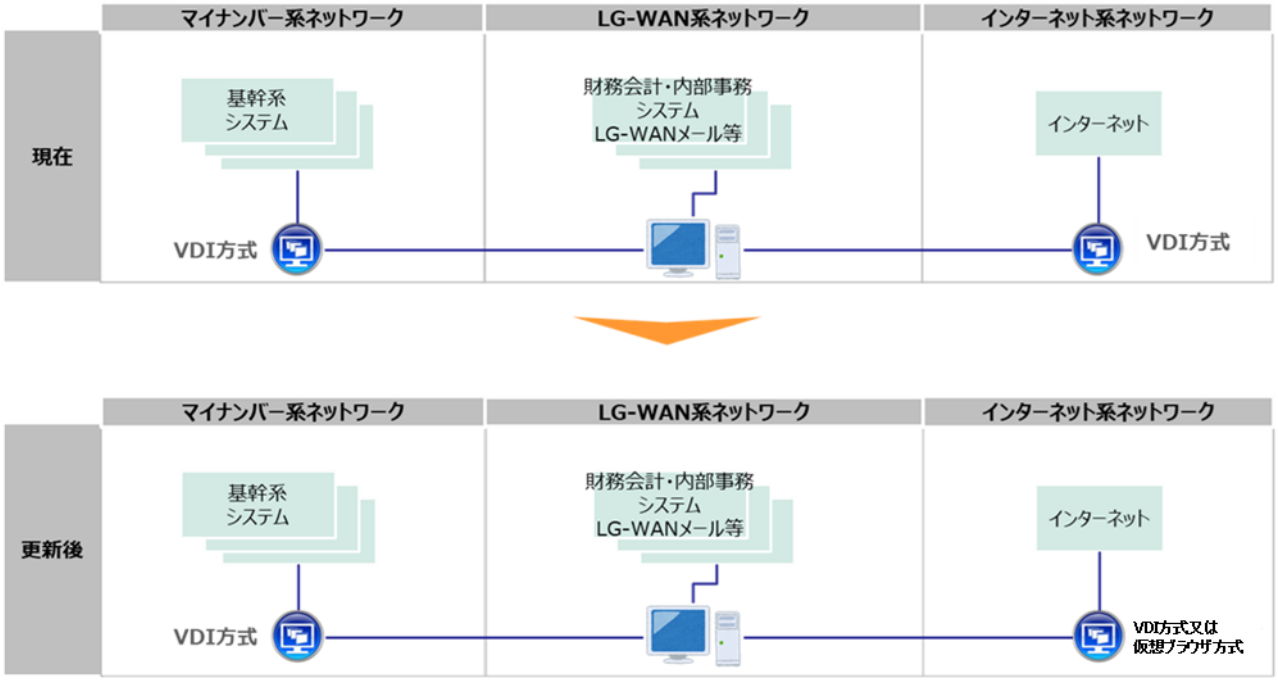
(2) 構築スケジュール

- 下図の通り、令和８年７月の本稼働に向けて調達・構築を行う。
- 令和７年度に調達を行い、構築を進める。
- 納入期限は令和８年６月30日とする。
- 稼働後は60か月間（令和８年７月～令和13年６月）利用する。※以降の契約は別途調整



（3） 導入後の仮想化基盤のイメージ案

仮想化基盤について現行及び更新後のイメージ像を以下に示す。



（4） 調達範囲

- 対象端末の仮想デスクトップ環境
- 仮想化環境を稼働するために必要となるハードウェア、ソフトウェア（必要ライセンスも含む。）の導入・保守
- 仮想デスクトップを利用するためのサーバ等の設置、設定及び動作確認
- 仮想デスクトップの切替え作業及び切替えにおける本市作業の支援（本市が利用するシステムベンダへの問合せ対応も含む。）
- 稼働後における運用サポート及び利用に関するヘルプデスク対応
- 稼働後の端末入替時の端末初期設定に必要なマスターPC 及びイメージ作成の作業協力

（5） 成果物

想定する成果物を下記に示す。下記以外にも成果物がある場合には合わせて納品すること。なお、納期については、別途本市と調整すること。

- プロジェクト計画書
- プロジェクト管理資料（進捗報告書、課題管理表、運用サポート報告）
- 要件定義書（各要件項目一覧と概要、機器構成一覧、構成概要図、サイジング結果）
- 基本設計書（ハードウェア及びソフトウェア一覧、システム構成図、ラック構成図、ネットワーク設計書、ネットワーク論理構成図、ネットワーク物理構成図、パラメータ設定資料）
- テスト計画・テスト結果報告書
- 各種マニュアル
- 研修計画
- 運用計画

第2章 構築要件

（1） 端末要件

ア. 端末構成

・ LGWAN 系を物理端末（以下「LGWAN 系端末」という。）として継続利用すること。LGWAN 系端末から仮想化されたマイナンバー系ネットワークの端末（以下「マイナンバー系端末」という。）、インターネット系ネットワークの端末（以下「インターネット系端末」という。）を利用する。

・ マイナンバー系端末で窓口業務専用として利用している端末については、物理端末とする。

・ インターネット系端末で専用ソフトを利用する端末を必要とする所属につきインターネット系物理端末を１台ずつ配置する予定である。

・ 仮想クライアントの利用想定台数は、下記のとおり。現時点で想定される各ネットワークで作成するクライアントのマスタについては、「想定マスタ数」に記載する。ただし、マスタ数については構築の中で変動する可能性がある。なお、マスタは、「エ.各端末の利用システム」に記載している「利用システム」を参考に各所属の利用環境に合わせて作成すること。

ネットワーク	台数	次期形態	想定マスタ数
マイナンバー系	400 台	仮想クライアント	7
LGWAN 系	600 台	物理クライアント	6
インターネット系	600 台	仮想クライアント	2

※同時接続数は各ネットワークの台数の８割程度とする。

・ 利用箇所は、本庁舎及び出先機関とする。

・ 仮想クライアントの実現方式については、下記とする。

マイナンバー系端末　⇒　VDI 方式

インターネット系端末　⇒　方式を問わない。ただし、三層分離αモデルに対応すること。またセキュリティ上分離性が低いローカルコンテナ方式及び RDS 方式は除く。

・ 端末やプリンタについては、本市に設置済みの機器を使用すること。

・ 仮想化基盤構築で構成するハードウェア等については、特定のベンダの技術に依存することなく、広く公開された技術や規格に基づき、一般的なオープンシステムに求められる互換性や相互運用性が保証されていること。

・ 起動（仮想クライアントへのログインから画面表示まで）の時間が、通常業務を行う上で支障のない時間以内であること（理想値は１分程度を想定している。）。

・ 物理端末については、操作をしない時間が１０分を経過するとスクリーンセーバー起動による画面ロックを行う設定とし、ロック状態となった場合も仮想クライアントへの接続が切れないこと。また、画面復帰後にスクリーンセーバーが起動する前の状態で引き続き仮想クライアントの操作ができること。

イ. ソフトウェア

・ 仮想クライアント作成に必要な Microsoft のライセンスを必要年数分含めること。5 年分で、導入時点で途中までしかライセンスを購入できない場合は別途追加で購入が必要な旨を明記した上で追加ライセンスについても含めること。
・ 仮想クライアントの OS は Windows11Pro とし CAL が必要な場合には合わせて購入すること。
・ Office については、本市所有のライセンスを使用すること。所有ライセンスは以下のとおり。本市所有のライセンス分を差し引いた不足分を購入すること。

製品	ライセンス数
Office Standard 2019	301
Office Standard 2021	286

・ 各環境においては、Office ソフトの利用ができること。マイナンバー系の Office は、デスクトップアプリ版とすること。
・ OS に関しては、Microsoft Windows Server Update Service（WSUS)が利用できること。ただし、マイクロソフト社より WSUS の将来的な廃止が発表されているため、廃止後の代替となる更新手段が利用できる仕組みとすること。
・ 仮想クライアントで必要となるソフトウェアライセンス等について購入し、5 年分の更新・保守費用も含めること。ただし、VDA ライセンスについては 3 年分の購入とする（4 年目以降の更新は別途費用)。なお、ウイルス対策ソフトライセンスについては、現在トレンドマイクロ「TRSL ｳｲﾙｽﾊﾞｽﾀｰ ｺｰﾎﾟﾚｰﾄｴﾃﾞｨｼｮﾝ Plus ガバメント」を 1,600 ライセンス（令和 8 年 6 月 30 日まで）保有しており、継続利用する予定である。
・ 仮想クライアントを利用するために必要となるソフトウェア（パッケージライセンス、死活監視ソフト、バックアップソフト等）に、物理端末にインストールするものも含めて構築の範囲内として準備する。
・ 管理系サーバで WindowsServer が必要な場合は、必要な WindowsServer ライセンスを購入すること。
・ なお、各種ライセンスについては構成内容に相応しいライセンスを採用し、かつ、経済的な構成で提案すること。
・ 仮想端末へのディスク及び OS 拡張を端末を停止させることなく実施できること。
・ シンクライアントパッケージの USB ポートリダイレクト制御について、同時更改予定の資産管理システム(SKYSEA Client View)又は今回導入する製品と連携して USB ポートの ON/OFF を制御できるようにすること。

ウ．端末のスペック
・ 仮想化クライアントに求めるスペックについては、下記の最低スペック以上のスペックとし、LGWAN 系端末（物理端末）や構成するサーバのスペック等も踏まえて、システム利用上問題ない端末スペックとすること。
・ 仮想クライアント 1 台当たり 50iops(R:W=5:5)の性能を確保する。
・ 現行物理端末の最低スペックについては下記のとおり。

ネットワーク	CPU	メモリ	HDD
マイナンバー系	Core i5 4590	4GB	250GB
LGWAN 系	Core i5 4590	2GB	250GB
インターネット系	Core i5 3470	2GB	250GB

エ．各端末の利用システム

・ 各ネットワーク環境からは下記のシステムを利用しており、新仮想環境構築後も同様のシステムを利用する。

・ 現行の基幹系システムは端末情報を登録しており、その端末番号でコンピュータ名を管理しているため、その基幹系システム側で採番されたコンピュータ名で新たに構築する仮想端末においても管理できること。

ネットワーク	利用システム
マイナンバー系 **R07.06 現在**	基幹系システム（COKAS-R/AD Ⅱ） 滞納管理システム（DIALOGUE） 健康管理システム（LOGHEALTH21/AD Ⅱ） 障害者福祉システム（G-Trust Ⅱ） ※上記システムのサーバは、キステム社のデータセンターに設置 確定申告支援システム（The 確定申告） ※上記システムのサーバは庁舎内に設置 生活保護システム（ふれあい）等 ※上記システムのサーバは LGWAN－ASP
マイナンバー系 **R08.01 以降**	基幹系システム（COKAS-R/4G） 滞納管理システム（DIALOGUE） 健康管理システム（LOGHEALTH21/AD Ⅱ） 障害者福祉システム（G-Trust Ⅱ） ※上記システムのサーバは、ガバメントクラウド（AWS）上に設置 確定申告支援システム（The 確定申告） ※上記システムのサーバは庁舎内に設置 生活保護システム（ふれあい）等 ※上記システムのサーバは R08.06 以降にガバメントクラウド（AWS）上に設置
LGWAN 系	EVE MA、内部情報システム、財務会計システム（LOGFIN21 for.NET）、グループウェア、 LG メール等
インターネット系	各種インターネット等

オ．周辺機器

・ 印刷は各ネットワークに接続されている既設プリンタを使用する。

・ 窓口専用として使用するマイナンバー系端末は物理端末を想定しており、現在の基幹系システムで利用している周辺機器（スキャナー、OCR 等）を継続利用すること。

・ 現在はマイナンバー系物理端末及び仮想化基盤利用可能な LGWAN 系物理端末において、Windows ログオン時及びグループウェアの起動時に生体認証（EVE MA による指紋認証）を

導入しているが、今後リプレイスがなされる場合に、仮想クライアント側の要件、相互動作実績等を加味し、生体を利用した認証ができるよう配慮すること。

カ．データ保存

・ 仮想クライアントについては、基本的にローカルへのデータ保存はせず、仮想基盤上のファイルサーバにデータを保存することとする。このため、仮想クライアントのローカルドライブについては必要最低限の容量とすること。
・ ファイルサーバの保存データ量については、下記のボリュームを想定している。（インターネット系については構成によっては不要）

ネットワーク	ボリューム
マイナンバー系	1 人 500MB×400 人分＋200GB（予備領域）
LGWAN 系	1 人 500MB×600 人分＋200GB（予備領域）
インターネット系	1 人 500MB×600 人分＋200GB（予備領域）

キ．セキュリティ管理

・ 仮想クライアントのウイルス・セキュリティ対策を講じること。
・ クライアントのウイルス対策ソフトについては、本市が保有するウイルス対策ソフトのライセンスを使用すること。以下に本市が現在利用しているウイルス対策ソフトを記載する。

端末	ウイルス対策ソフト
マイナンバー系端末	Apex One
LGWAN 系端末	Apex One
インターネット系端末	Apex One

・ 本市ではウイルス対策ソフトのサーバから一括してウイルス定義の更新やウイルス対策ソフトのアップデートの適用を管理している。今回の構築以降も現行の運用を維持できること。
・ 一斉ウイルススキャン実行時に仮想環境に影響が出ない構成にすること。

ク．アクセス制御

・ LGWAN 系端末から各仮想クライアントへは画面転送のみを許可する。なお、コピー、ファイル転送及びリダイレクト印刷については設定ができること。
・ 印刷は各ネットワークに接続されている既設プリンタを使用する。
・ 印刷用プリントサーバは印刷の安定稼働のため、専用の物理サーバを導入すること。
・ 各ネットワークを跨ぐファイル受渡しについて、媒体渡しは原則不可とする。ただし、システム管理者により許可された場合には、受渡しを可能とする。
・ 仮想サーバ・クライアントの Windows ライセンス認証がインターネットに接続せずとも認証できるように考慮すること。
・ 利用者の操作ログの取得が可能なこと。
・ 同時更改予定の資産管理システム(SKYSEA Client View、各系統で管理サーバあり)を利用し、物理及び仮想端末の管理ができること。

ケ．VDI 方式

・ ActiveDirectory と連携できること。
・ 負荷分散のためのロードバランシングを行うこと。
・ 管理を簡易に行うために管理 GUI を備えていること
・ 管理が容易に行えるようにすること。
・ ユーザー割り当て方式として、専用割り当てを採用し、フルクローン方式とすること。
・ 通信は、暗号化されていること。
・ ユーザー認証が可能であること。
・ クリップボードの制限に詳細な設定があること（テキストのみコピー可能等)。
・ 仮想端末の追加・変更・削除、設定の追加・変更・削除等の管理を簡易にするため、管理 GUI から操作できること。
・ 各端末に対して、一括でソフトウェアの導入・削除・変更できること。
・ VDI については、VDI 方式によるシステム／アプリケーションの利用を安定的かつ快適に行うため、VDI 方式に最適化されたストレージを導入すること。
・ ソリューションは指定しないが、基幹システムで動作実績のあるソリューションで構成すること。
・ ブラウザは Edge の最新バージョンが使用できること。

コ．インターネット接続系の仮想化方式

・ 管理を簡易に行うために管理 GUI を備えていること。
・ 通信は、暗号化されていること。
・ AD と連携し、AD ユーザでのログインが可能なこと。
・ クリップボードの制限に詳細な設定があること（テキストのみコピー可能等)。
・ 仮想端末又は仮想画面の追加・変更・削除、設定の追加・変更・削除等の管理を簡易にするため、管理 GUI から操作できること。
・ 各端末に対して、一括でソフトウェアの導入・削除・変更できること。
・ 選択した仮想化方式に最適化されたストレージを導入すること。
・ ソリューションは指定しないが、インターネット環境で動作実績のあるソリューションで構成すること。
・ ブラウザは Edge の最新バージョンが使用できること。

(2) サーバ要件

ア．ハードウェア要件

・ 仮想化基盤のサーバについては、本市庁舎既設ラック（河村電器産業株式会社製 ITS42-1020）に設置すること。調達機器が 1 ラックに収まらない場合については、別途協議とする。
・ 可用性とデータの堅牢性を担保することから 3 ノード以上の構成とし、導入後 1 ノード単位の増設が可能であること。また、ノードの増設を GUI 画面から行えること。
・ 仮想化基盤以外に物理端末や各種ソフトウェアの管理等で本仮想化基盤を運用するために必要となるサーバ、機器がある場合には、含めて構築こと。

・ 電源は無停電電源装置（UPS）による電源供給ができること。なお、UPS についても本調達に含めること。
・ 冗長化構成とし、障害が発生した場合でも業務が停止しない構成であること。
・ 物理的な故障によるデータ消失を防止する構成にすること。
・ ハードウエアリソースのスケールアウトが可能であること。拡張性の目安として システムを停止することなく、構成部品またはサーバの追加によって、ストレージ容量を 2 倍 に、仮想化サーバ台数を 2 倍程度にスケールアウト可能であること。
・ 物理サーバへのメモリ等の各種リソース追加が容易にできること。
・ 構築を可能な限り短期間で行うとともに、構築時のトラブルを軽減するため、本調達と同規模以上のシステムにおいて実績がある、かつ動作検証済みの機器とすること。
・ 最大接続台数の規模でサイジングを行うこと。なお、CPU、メモリ及びストレージについてサイジングの根拠を示す資料を提示すること。
・ 端末台数に従い、実際に想定される端末稼働率と、障害時における業務継続性を踏まえた適切な余剰性能の確保に配慮すること。
・ 5 年間はメーカー保守が受けられる機器を選定すること。
・ ライセンス管理サーバが必要な構成の場合は、キー管理サービス（KMS）を導入すること。
・ 仮想サーバ、マイナンバー利用事務系 VDI、インターネット接続系仮想化システムは、それぞれ分離されたサーバで構成すること。

イ．ソフトウェア要件
・ ハイパーバイザについては、安定した動作実績の多い製品を利用するものとし、可能な限り最新バージョンを採用すること。
・ 基盤上で動作する 1 台のハイパーバイザの負荷が高い場合、サービスの停止を伴わずに、仮想マシンがサーバの負荷が低い別のハイパーバイザ上に自動的に移行される機能を有すること。
・ ハードウェア障害が発生した場合に別のサーバで仮想マシンが自動的に起動することにより、高い業務継続性を提供すること。
・ ログオンストーム対策、ブートストーム対策ができること。
・ 画面転送プロトコルには信頼性が高く狭帯域に最適な画面転送プロトコルを採用すること。
・ ネットワーク帯域に応じてモニターの解像度や色の解像度を制限する事で通信量を軽減できる機能を有すること。
・ ユーザー数の変動に応じて、仮想デスクトップ環境の迅速な提供が可能であること。
・ 各種サーバで WindowsServer のライセンスが必要な場合には、その購入も含めること。
・ 仮想化基盤を運用する上で必要となる上記以外のソフトウェアがある場合には、その購入も含めること。
・ 各種ライセンスについては、経済的な構成で提案すること。
・ 1 つ又は複数の仮想マシンを仮想化基盤上で他のネットワークから起動し、トラブルシュート、テスト及びトレーニングを実行可能なこと。
・ 5 年間はメーカー保守が受けられること。

(3) ストレージ要件

- 電源、ネットワークインタフェース及びコントローラ部は、二重化構成とすること。
- ネットワークインタフェースは、10Gbps 以上で構成すること。ストレージ本体のほか、仮想化基盤のサーバに接続するスイッチ類も含めること。
- ストレージは二重書き込み相当又は RAID 6 相当以上の冗長構成とし、データの保全を図ること。
- SSD 等、ストレージの構成単位の単一障害発生時、および自動で冗長性能が復旧した後に 2 回目の障害が発生した状態においてもデータ喪失しない構成であること。
- ノード停止又はディスク障害によりデータの冗長性が失われた際に、即時ミラーデータ又はパリティから正常な領域に再生成することで自動的に冗長性を回復する機能を有すること。
- 物理ボリュームの容量を仮想的に割り当てができ、無停止で物理ディスクの追加が可能であること。
- 既存データについて影響を与えず、動的に論理ディスクの拡張・追加が容易に実現できること。
- IOPS 値を高め高速化した構成とすること。
- 自動エラーチェック等を要し、異常を検出した場合に通知機能があること。
- 構成モジュールの障害の検出と予防検出を行うための情報が収集され、適切に管理できる障害管理機能を実現できること。
- 共用ストレージへのアクセス制御機能として、不要なサーバからのアクセス防御が可能であること。
- シンプロビジョン機能によりディスク容量を効率的に利用可能なこと。
- 搭載する SSD はキャッシュ利用のみではなく、全てデータ領域として利用可能であること。
- ストレージ内に複数の領域を定義し、仮想マシンを分けて配置できること。
- 圧縮・重複排除機能が利用可能であること。
- 仮想マシンが別ノードへ移動した際も、その仮想マシンが動作するノードに仮想マシンのデータを再配置可能であること。

(4) ネットワーク

- ネットワークは、本市が敷設したネットワークを利用すること。(各フロアへの配線などは本業務には含めない。ただし、導入するサーバ等機器間における配線については、本業務に含めること。)
- 各系統間の通信制御は、既設のネットワーク分離用 FW(Fortigate101F)を利用すること。
- 既存の 3 系統のネットワークは現在有線 LAN であるが、今後無線 LAN とすることも検討しているため、無線環境に対応できること。
- 仮想基盤上に仮想ネットワークを設計・構築し、セキュリティを考慮した設定を行うこと。
- プロキシサーバは、既存のものを利用すること。
- 障害に備えて冗長化構成にすること。
- 1Gbps 以上の通信速度があること。
- ループ検出機能を有すること。

・ IEEE802.1Q VLAN Tagging に準拠していること。
・ ネットワーク機器等のステータス監視ができること。
・ VLAN 等のネットワーク設計を行い、セキュリティを考慮した設定を行うこと。

(5) ファイルサーバ
・ 仮想クライアントからデータを保存するためのファイルサーバを構築すること。
・ 容量については、（1）カの内容を参照すること。
・ 個人・組織ごとに領域を設定できること。
・ 更新差分管理等の世代管理ができること。
・ 将来的に容量の拡張が容易にできること。
・ 各課、役割に応じたフォルダを作成し、適切なアクセス権が設定できること。
・ 1 人当たり、7iops(R:W=5:5)の性能を確保すること。

(6) ActiveDirectory
・ マイナンバー系 ActiveDirectory 、LGWAN 系 ActiveDirectory については、既設サーバを利用することとする。
・ インターネット系 ActiveDirectory については、現行の仮想環境導入事業者で構築しており、本調達に正・副のサーバを含むこと。
・ ActiveDirectory については、既存ドメインを継承させること。
・ 利用するアプリケーションの制限ができること。
・ 新たに構築するインターネット系の ActiveDirectory については、OU、グループ、ユーザー等の管理を効率的に実施することができるソフトウェア等について提供すること。
・ 人事異動時に必要となる OU、グループ、ユーザー情報を事前に登録でき、指定した日時に各システムに反映できること。
・ CSV ファイルによるグループ・ユーザー情報の追加・変更・削除ができること。
・ ActiveDirectory 管理ツールは専用サーバを建てることなく管理用端末で運用可能なこと。
・ 3 系統の各クライアントは移動プロファイル等を利用し、個人のユーザーID のプロファイル情報をどの端末でも実現できること。また、3 系統のネットワーク全てにおいて Windows のフォルダリダイレクト機能を利用し、デスクトップ、その他のドキュメント等、各ユーザープロファイル中の指定されたフォルダ及びデータについては、ファイルサーバに保存すること。
・ ログイン時にプロファイル容量増大によりログオン時間が遅延しないように構築すること。

(7) ファイル授受サーバ
ネットワーク間を超えるファイル授受を行うためのサーバを構築すること。
ア. 製品
・ ファイル無害化のアップロード操作ログが資産管理システム SKYSEA と連携できるため、「Smooth File ネットワーク分離モデル」とする。ただし、下記要件を満たせる場合には、それ以外のソフトウェアでも可とする。
イ. ファイル交換機能
・ Web ブラウザを介して、セグメント間でファイル送受信が行える仕組みであること。

・ ウイルス対策ソフトによりアップロードされたファイルのウイルスチェックが可能であること。
・ アップロードした Office ファイルは、自動的に PDF 化又はファイル無害化されること。また異なるセグメント間でのファイルの受渡しにおいて、セグメント A からセグメント B へ又は、セグメント B からセグメント A へ等の方向性によって PDF 化又はファイル無害化の ON/OFF 設定が可能なこと。
・ ファイルダウンロードする際にパスワード付 ZIP ファイルに変換することができること。

ウ. ファイル無害化機能
・ 以下の Microsoft Office ファイル及び JUST Office ファイル（ver3 及び 4）よりマクロ、OLE、ActiveX、DDE を除去することができること。また、挿入されている画像ファイル（jpg、jpeg、tif、tiff、png、gif、bmp）のメタ情報を除去して再挿入できること。
“xls、xlsx、xlsm、ppt、pptx、pptm、doc、docx、docm"
・ 以下のファイルよりマクロを除去することができること。
・ “jtd、jtdc、 dxf、dwg"
・ 以下の花子ファイルよりマクロ、OLE、画像を除去することができること。
“jhd”
・ PDF ファイルよりスクリプトを除去することができること。
・ 以下の画像ファイルよりメタ情報を除去し、再構成することができること。
“jpg、jpeg、tif、tiff、png、gif、bmp、wdp、ico"
・ csv ファイルより外部関数を実行できない状態にすることができること。
・ 以下の圧縮ファイルを展開し内部のファイルを再帰的に無害化できること。
“zip、cab、lzh、7z、rar、tar、bz2、gz、xz”
・ 内部のファイルが無害化非対応のファイルの場合、同ファイルは削除され無害化可能なファイルのみ再構成すること。また、削除されたファイルをユーザーが確認することができること。

エ. 上長承認機能
・ 上長承認機能を有していること。
・ 上長承認の依頼通知は Email で自動的に送信されること。Email には URL が記載されており、クリックすることで承認画面に直接遷移することができること。

オ. 認証機能
・ 認証機能を有しており、 Active Directory/Open Ldap と連携が可能であること。Active Directory/Open Ldap と連携しないローカルユーザーを別途設定できること。

カ. 特権ユーザー
・ 一般ユーザーと異なったルールでファイル送受信が可能な特権ユーザーの登録が可能であること。

キ. ユーザー管理機能
・ ファイル送受信システムに登録できる利用者は職員数に関係なく登録可能であること。職員数の増減によってライセンス費用が変化しないこと。

ク. セグメント管理機能
・ セグメント毎に無害化、PDF 化、非無害化の有効/無効、上長承認の要/不要を設定することが

できること。

・ セグメントごとに背景色等を設定できること。（VDI 環境下においてユーザーが識別しやすくする為）

ケ．その他管理機能

・ 操作ログを確認することができること。日時、ファイル名、ユーザー名等を取得できること。

コ．構成

・ ファイル無害化を制御するサーバの構築に当たっては、仮想化基盤上に仮想マシンとして設計・構築すること。また、前述した仮想化基盤のＨＡ機能を活用し、可用性を高めること。

（8） バックアップ・リストア

・ バックアップ対象データは、マイナンバー系、LGWAN 系、インターネット系全てのデータを対象とすること。
・ バックアップ取得により、データの喪失がないこと。
・ 業務に影響が出ないようにバックアップすること。
・ バックアップデータは、仮想化基盤のサーバとは別筐体に保存されること。
・ バックアップジョブによる運用管理が行えること。
・ 仮想環境に構成変更があった場合は、全体又はクライアント単位で、ディスク又はテープに対するバックアップを行うこと。
・ フルバックアップは初回のみとし、2 回目以降は増分バックアップ等によりバックアップ時間が永続的に長期化しない方法をとること。
・ バックアップデータは、バックアップストレージ等に 7 世代以上保存すること。
・ バックアップしたデータについては、仮想クライアント単位及び仮想サーバ単位でリストア可能なこと。
・ 最上位の共有フォルダ単位で日次バックアップしたデータを、アクセス権等の情報を保持したままフォルダ又はファイル単位でリストアできること。
・ 仮想クライアント環境、ファイルサーバ、仮想サーバ及び各環境を構成する物理サーバごとに最適なバックアップを構成し、環境や障害パターンに応じた適切なリストア方法を確立すること。
・ バックアップストレージ内のデータを別のバックアップストレージへ自動的にコピーでき、データの検証と修復機能を有すること。
・ ウイルススキャンしながらリストアをし、ウイルスへの感染が確認された場合、リストアをキャンセルする、又はネットワークを遮断した上でリストアする等の処置がとれること。
・ リストアは、バックアップと同様に業務ネットワークとは独立した専用のネットワークを使用することで、本番環境に影響しない安全かつ高速なリストアを可能とすること。
・ 各仮想マシンのバックアップは、仮想ディスク全体のバックアップを実施し、リストア時に OS の再インストールが不要であること。リストア先は元とは別のホストでも可能であること。
・ 人為的ミス等による論理障害に対するリストアは、ストレージ筐体内のバックアップデータ（もしくはスナップショットデータ）から高速にリストア可能な構成にすること。
・ SQL Server のバックアップオプションを含むこと。

・ バックアップデータの重複排除及び圧縮機能を有すること。
・ スナップショット機能が利用可能であり、任意のタイミングの他、毎時間、日次、週次、月次で自動での取得が可能であること。
・ スナップショット機能の利用においては追加ライセンスが不要であること。
・ スナップショットの取得および統合時に本システムへの影響が発生しないこと。
・ スナップショットは仮想マシン単位で取得でき、また任意の世代からのリストアが実行可能であること。
・ ゲスト OS の静止点を確保できるスナップショットに対応していること。
・ スナップショットは、ランサムウェア等による改ざんを一切受けず、常時保全される構造であること。

(9) 運用管理
・ 統合的に仮想環境の管理ができること（本件において、構築・導入したサーバ、クライアント、ネットワーク、その他の仮想環境）。
・ 障害発生時、通知機能があること。
・ 仮想環境のログが管理できること。
・ リソース状況を GUI で確認できる機能を有すること。
・ 仮想マシンのリソース割り当てを一覧又はリスト出力で確認できること。
・ 稼働状態についてレポートを生成する機能を有していること。
・ 将来のクラスタ拡張に備え、複数のクラスタを一元管理できる機能を有すること。
・ ハードウェアおよびソフトウェアの障害、設定した閾値の超過について、アラート通知を行えること。
・ 複数の端末から管理画面が参照及び更新ができること。
・ 各運用やバックアップ等をスケジューリングできること。
・ サーバやネットワーク機器等のステータス監視ができること。
・ ホスト及びホスト上で稼働する仮想ゲストのリソース容量を監視可能であること。
・ 仮想基盤で導入するハードウェア及びソフトウェアで発生する事象を一元管理できること。
・ 仮想基盤で導入するハードウェア及びソフトウェアが出力する各種イベントログの情報を監視できること。
・ 仮想基盤で導入するネットワーク機器が備えている SNMP エージェントに対するマネージャ機能として、ネットワーク使用状況や障害を監視できること。
・ 仮想マシンの追加・削除や割り当てリソースの変更、仮想マシンの再起動、その他ライブマイグレーションによる負荷の平準化等を行えること。
・ サーバ及び端末の追加が容易にできるように、各種マスターモデルを作成すること。

(10) 非機能要件
ア. 性能
・ 過不足ない十分な性能及びレスポンスを確保すること。
・ 最大負荷時においても余裕のある設計とすること。

・ 運用期間中の職員増や端末増を考慮するため、ライセンス等は除き可能な限り余裕のある設計とすること。

イ.　可用性

・ 原則として、２４時間３６５日利用可能であること。
・ 窓口開庁している時間（平日 8:30～17:15）においては、稼働率を 99.9%とし、業務継続性を確保するとともに、負荷分散等を実現するための機能を実装すること。
・ ゲスト OS でのシステム障害の際は、影響範囲は該当仮想クライアントを利用しているユーザーのみとなること。
・ 仮想基盤はビデオ会議システム（WebEx 等）等を利用し、メーカーサポート等とインターネット経由で接続し、管理画面やログ内容の確認作業、QA 対応などリモートでのサポートが実施できること。尚、使用されるシステムはユーザーからの明示的なログイン操作等の許可をもって接続できるものであり、VPN 等の追加設備を必要とするものでないこと。

ウ.　拡張性

・ 仮想端末の増設時の作業や、各ネットワークで利用するシステムが追加となった場合の端末設定における作業は、容易に行えること。
・ 仮想基盤（各ハードウェア・ソフトウェア）については、拡張が容易にできること。

エ.　その他

・ ハードウェア及びソフトウェアについて、予防交換やパッチ適用等の業務システムを可能な限り停止せずに実施できる構成であること。
・ 仮想基盤を構成するハードウェア及びソフトウェアは、保守が受けられ一体として動作するよう動作検証も取られていること。
・ 電源及び LAN 配線については既設のものを利用することとし、追加工事が必要な場合については構築費用に含むこと。なお、本システムで利用可能な電源容量は２０００ＶＡとする。
・ USB ドングル等を利用するシステムについては動作確認を行うこと。また、設定変更等が必要な場合は各ベンダと調整を行い、仮想環境での対応を要する部分については本業務内で行うこと。なお、USB ドングルを利用するシステムは、以下を想定しているが、今後増減する可能性もある。

（USB ドングル利用システム）
土地家屋履歴管理システム

(11) 切替え

ア.　新仮想環境への移行

・ 現行ベンダーと連携し、本番稼働に向けた移行を行うこと。新仮想環境への移行時期については、本市と調整の上で確定すること。

イ.　データ移行

・ 現行環境からの次期環境への必要なデータ移行は原則ベンダー側が実施する。対象は（１）カに記載のデータ、管理者が指定する端末構築用データ一式及び次期環境に必要な設定データとする。

・ 開発スケジュールを踏まえた、新旧環境間のデータ移行可能時期を提示すること。
・ 各クライアントで動作するシステムについて、アプリケーションのインストール、ネットワーク設定、動作確認等の接続調整を行うこととし、移行費用は含めること。

（主な設定）

・ネットワーク設定（IP アドレスは市から指定）
・ユーザ設定
・ソフトウェア・ドライバインストール
・ドメイン参加・ポリシー適用
・ブラウザ設定
・動作確認

（アプリケーション）

・Microsoft Office
・EVE MA
・SKYSEA Client view
・Trend micro Apex One
・プリンタ・スキャナドライバー（機種は部門毎に異なる）
・各利用システム

（12） 研修

・ 仮想クライアントの利用方法について、各課代表者への利用者研修を行うこと。
・ 仮想基盤を効果的に運用ができるように、管理者向けの研修を行うこと。
・ 研修の対象者は、利用者研修が約１００名、管理者研修が 6 名程度を想定している。
・ 研修にあたっては、研修計画を作成し、マニュアルに関しても本市の要望に沿ったものを用意すること。

第3章 運用サポート

（1） 運用管理

・ 運用管理として想定する事項等は以下のとおりであるが、本市職員の負担を軽減するとともに、継続かつ安定したシステム運用を実現するため、必要な運用管理を行うこと。
・ セキュリティ対策（定期的なセキュリティパッチの適用等を含む。ただし、仮想クライアントへのパッチ適用は業務に含めない。）
・ 障害対応（仮想端末に接続できない場合の障害切り分け等も含む。）を行うこと。また必要に応じて他の事業者と協力すること。
・ 本市の運用支援のため、仮想クライアントの作成、削除、ディスク追加等が可能なツールを準備・提供すること。
・ 運用マニュアルを作成し、システムの変更等があった場合は、最新の状態に更新すること。

（2） サポート

・ 本件システムの構築に精通したものが、対応を行うこと。

- 問合せ受付は、電話及びメールの両方に対応すること。
- 対応時間は原則として平日９時から１７時までとするが、重要度に応じて受付・対応ができるよう連絡体制を整備し、対応方法等について本市担当者と調整し、取り決めること。
- 障害発生時には、速やかに必要な対処を行うこと。障害発生後、概ね１時間以内に１次切り分け作業を開始すること。また、結果を報告し、調査、原因分析、修復等に必要なハードウェア又はソフトウェア保守業者の手配を行い、協力のうえ障害の修復に努めること。
- 故障したハードウェアは交換すること。ハードウェアの故障や障害時には、概ね 6 時間以内にオンサイトにて修理すること。なお、同一の機器に障害が多発する場合、是正措置をどのようにするかメーカー等と調整し、仮想基盤が安定的に利用できるように早期対応をすること。
- 修正プログラムの適用をはじめ、安定運用に必要な対応を行うこと。また、更新作業等は業務への支障が出ないよう、適切なタイミングで実施すること。
- 端末増設時や障害時（利用する基幹系システムに起因する障害も含む。）等に関して、本市から問合せがあった場合には必要な技術支援を行うこと。また、状況に応じて、システム担当事業者と連携や協力を行い、障害対応や安定稼働に努めること。
- 本市からの各種問合せについて、上限回数を設けないこと。
- 必要に応じて、仮想基盤で使用しているすべてのソフトウェア製品、ファームウェア、ドライバ等に関する各種ソフトウェア導入後に発見される脆弱性・不具合への対策を行うこと。
- 仮想基盤のシステム修正パッチ及びバージョンアップは、本市担当者と協議の上適用作業を行うこと。ただし、緊急を要するセキュリティ案件である場合は早急に対応すること。
- 重大障害の際には、経過等を取りまとめて報告すると共に改善策を本市担当者へ提示すること。
- 障害発生時、保守作業により交換した故障 HDD 又は SSD については、物理破壊を実施してデータ消去し、本市で消去されたことが確認できるようにすること。

（3） 定期報告

- 定期的な報告会を開催すること。
- 運用及び保守の実施状況（稼動・停止、性能(レスポンス)、障害発生、保守実施等）の他、以下の事項等について適切に管理し、定例会にて報告すること。（課題管理、品質管理、文書管理、変更管理、情報セキュリティ管理等）

第4章 プロジェクト管理

（1） プロジェクト計画書

- 契約後１週間以内に、プロジェクト計画書を提示すること。プロジェクト計画書には、作業範囲、WBS・作業スケジュール、体制・要員配置、役割分担一覧、進捗管理方法、コミュニケーション計画、課題・リスク管理、品質管理、工程完了判定会議、納入成果物一覧等を示すこと。
- 本業務を通じ、本市の過度な負担とならないプロジェクト計画書とすること。
- 業務遂行上必要と認められるものであって、本仕様書の解釈に疑義が生じた事項及び本仕様書に明記していない事項については、本市と協議のうえ指示に従うこと。

(2) プロジェクト体制

- プロジェクト体制については、次の要件を満たすこと。
- 作業全体を統括するプロジェクトマネージャを設置すること。
- 要員については、自治体における仮想基盤の構築・運用を経験したことがあるものを配置すること。
- 関係する他の事業者と協力し、プロジェクトを円滑に進めることができる体制であること。
- プロジェクトメンバーの変更に際しては、本市の承認を得ること。
- 品質管理責任者を配置し、成果物の品質確保ができる体制であること。

(3) 会議運営

- 構築中の定例報告会は、少なくとも月 1 回程度実施すること。
- 定例報告会では、進捗状況、リスク・課題、変更管理、WBS 等の報告資料を準備し、議事録の作成を行うこと。
- 必要に応じて、工程完了報告会を開催し、各工程の設計書、テスト結果報告書等の成果物及び実施報告書等を準備し、議事録の作成を行うこと。
- 端末から利用するシステムベンダ等と打ち合わせが必要な場合には、会議に参加すること。進捗報告書、課題管理表、変更管理表、WBS、その他必要と思われる資料を準備し、議事録の作成を行うこと。
- 各種議事録については、会議終了後 3 営業日以内に提出すること。

(4) 作業場所

- 庁舎内で作業を行う場合には、作業期間について事前に本市と協議すること。また、作業場所については本市が指示するものとする。
- 受託者にて準備する作業場所、開発環境等については、十分な情報セキュリティを確保していることをあらかじめ本市に報告し、承認を得た上で作業を開始すること。
- 本市が承認した作業場所以外で作業を行わないこと。また、本市が指定する場所及び当該作業場所以外に個人情報を持ち出さないこと。