宇和島市統合型情報システム更改事業
仕様書

令和８年２月

宇和島市

第１章　概要

(1) 目的

本市では、令和３年度に構築した情報系システムとセキュリティ強靭化システムを統合した「統合型情報システム」が運用開始から５年を迎え、更新が必要となっている。

加えて、近い将来発生が危惧される南海トラフ巨大地震に対応するため、システム部門の業務継続性を強化する必要性が高まっている。

これらを踏まえ、日々進化するサイバー攻撃への備えを行うとともに、業務負担の軽減と災害時の業務継続性の向上を目的として、統合型情報システムの更改を実施するものである。

(2) 履行期限

構築期間　契約締結日の翌日から令和８年11月30日まで

運用期間　令和８年12月１日から令和13年11月30日まで

(3) 事業概要

①実施場所

・宇和島市役所　　愛媛県宇和島市曙町１番地

・データセンター　四国内（本市において別途用意）

②調達範囲

本調達の範囲は、統合型情報システムの構築及び本稼働以降5年間の運用保守とし、仕様書記載の有無に関わらず本システムが稼働するために必要なハードウェア及びソフトウェアの調達、搬入、設置、設定、運用保守、回線使用料（サポートに係るもの）、運用保守終了後の機器の撤去・運搬を含む。なお、処分は市にて行う。

③更改対象システム

更改対象のシステムは、別紙１「更改対象システム」に示すとおりとする。

(4) 基本情報

①クライアント端末

形状	ノートパソコン	デスクトップパソコン
台数	510 台	590 台
OS	Windows11 Pro 64bit	同左
CPU	Intel Core i3（6 コア）	Intel Core i3（4 コア）
メモリ	8GB	同左
ストレージ	SSD 256GB	SSD 128GB
モニタ	13.3 インチ（解像度 1,920×1,080）、 外部モニタ 24 インチ（同解像度）	24 インチ（解像度 1,920×1,080）
内蔵カメラ	あり	なし
ブラウザ	Microsoft Edge、Google Chrome、Firefox	同左

※ＣＰＵ・メモリは平均的なスペックのものを記載

②複合機

Canon　C5860F（17台）・C5850F（67台）・C3930F（124台）

③静脈センサー

富士通　PalmSecure-SL FAT13SLD01（410台）

④OCR・スキャナ

東芝　S2700EH

RICHO/富士通 Fi-7800・FI-8930・Fi-8170

富士通　FI-60F・FI-65F・FI-70F

EPSON　ES-2200・DS-510・DS-530・DS-531・DS-571W・GT-S640

ジェイエスキューブ　TOM9500ex

⑤ネットワーク構成

基幹系システム（総合行政システム）やデータセンターへの接続は図１のとおりである。現行では本市サーバ室内に統合型情報システムを構築しているが、次期システムはデータセンター内に構築すること。なお、本市からデータセンターへの接続回線は本市において用意する。

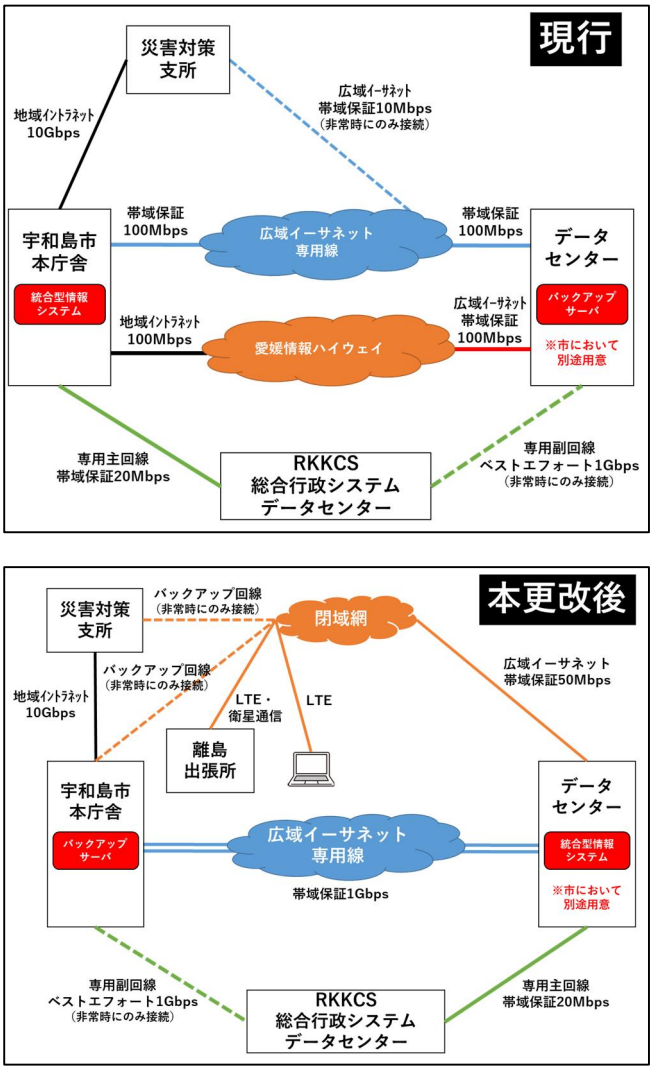

図１．ネットワーク構成概要

第２章．基本方針

(1) セキュリティ対策

本システムは、本市の情報セキュリティポリシー及び国のセキュリティポリシーガイドラインに則り実装するものであり、本市の行政事務を支える情報の機密性・完全性・可用性を確保する必要がある。

そのため、不正アクセスを防止するためのアクセス制御やバックアップの取得、ログの管理等、高度な情報セキュリティを有するシステムを構築すること。

(2) 災害対策

本システムは、災害時に基幹行政システムや防災関連システム等の重要システムを使用する上で必要となる機能であるため、自然災害等からシステム停止を未然に防止するとともに、停止した場合に早期に復旧できるよう、本市のＩＣＴ－ＢＣＰの強化につながるシステムを構築すること。

(3) 業務効率化

人口減少社会が進む中、多様化する住民ニーズに限られた人員で対応していく必要がある。

高度なセキュリティを確保しつつも、リモートワーク等により効率的に業務ができるシステムを構築すること。

また、ＡＤサーバと連携するなど、機構改革や人事異動等による組織改編にもスムーズに対応できるシステムを構築すること。

(4) 現行システムへの影響

本システム調達において、本市の基幹系システム及びネットワークに影響が出ないよう、受託者は本市及び現行保守事業者と協議し、必要に応じて現行保守業者に委託すること。

なお、その際の委託費用は受託者負担とする。

・総合行政システム保守業者　株式会社RKKCS

・ネットワーク保守業者　　エフサステクノロジーズ株式会社

(5) 履行期限厳守

実施要領に記載の履行期限までに確実に更改を完遂できるよう、業務遂行環境を確保すること。

(6) 法令等遵守

本業務に関係する法令ほか、本市の個人情報保護条例・情報セキュリティーポリシーを遵守すること。

また、総務省策定「地方公共団体における情報セキュリティポリシーに関するガイドライン（令和７年３月版）」に準拠すること。

第３章．基本要件

(1) 共通要件

①過去 10 年以内に、当市と同規模（人口 5 万人以上）の自治体において、本事業と類似する事業（情報系システムおよび自治体情報セキュリティ対策「三層の対策」の構築）の受託実績を有すること。

②プライバシーマーク（P マーク）又は ISO/IEC 27001 情報セキュリティマネジメントシステム（ISMS）の認証を取得していること。

③安定したレスポンスで動作することを条件とし、既存ネットワーク帯域の占有率、輻輳に十分に配慮し構築すること。

④本システムは５年以上使用するため、将来的な拡張性に配慮し構築すること。

⑤既存機器への設定変更、ソフトウェアのインストール等が必要な場合は、本市と協議の上、受託者において効率的に行うこと。

⑥本システム調達で提案するハードウェアは提案時点で最新機種にて構成し、旧機種や中古機種の提案は認めない。

(2) ネットワーク分離

現行のシステム構成と同じく業務端末をＬGWAN接続系に配置するモデル（αモデル）とし、仮想化技術によるネットワーク分離（論理分離含む）やファイアウォールによる厳密なアクセス制御を行い、高度なセキュリティを確保すること。

①マイナンバー利用事務系（住基、税、社会保障システムなど）

ア）原則として、他の領域と通信できないようにし、仮想デスクトップ環境下でブラウザを用いてマイナンバー利用事務系へのアクセスが可能であること。

イ）国等の公的機関が構築したシステム（eLTAX、ぴったりサービス）等、十分に安全性が確保された外部接続先について、インターネット等からLGWAN-ASPを経由してマイナンバー利用事務系にデータの取り込みを可能とすること。

ウ）端末からの情報持ち出し不可設定を実現すること。

エ）端末への多要素認証を導入すること。なお、第１章(4) 基本情報に記載するノートパソコンについては顔認証を、デスクトップパソコンについては静脈認証を可能とすること。

オ）ＬGWAN接続系とのネットワーク間でファイル授受を可能とすること。なお、ファイル授受において上司の承認を求めるよう設定すること。

②ＬGWAN接続系（グループウェア、文書管理システム、財務会計システムなど）

ア）インターネット接続系と通信を分離した上で、必要な通信だけを許可できること。

イ）端末のブラウザを用いてＬGWANサイトへアクセスが可能であること。

ウ）インターネット接続系からのデータ及びメールの無害化を実施すること。

エ）端末からの情報持ち出し不可設定を実現すること。

③インターネット接続系（インターネットメール、ホームページ管理システムなど）

ア）ＬGWAN接続系と通信を分離した上で、仮想ブラウザを用いてインターネットへのアクセスが可能であること。

イ）愛媛県情報セキュリティクラウドに接続すること。

(3) セキュリティ対策

①昨今及び将来のサイバー攻撃に対応すべく、最新の技術を採用した無害化処理・サンドボックス検知・ウィルス検知・ログ分析・監視等を導入し、侵入防止はもとより、侵入後における適切な対策によるセキュアな環境を構築すること。

②サーバ単位にウィルス対策を講じることとし、５年分のライセンス更新費用も含むこと。

③ウィルス対策ソフトのパターンファイルは、常に最新状態に保つよう構築すること。

④ＯＳやアプリケーションの修正プログラムの適用又はマルウェア対策ソフトのパターンファイル更新も含めて、最良の対策を講じること。

(4) 災害対策

①本庁舎サーバ室内にバックアップサーバを設置し、データセンターに保存されているファイルサーバのバックアップを取得すること。

②バックアップは、ネットワークトラフィックへの負荷を勘案し業務時間外に日次で実施し、30日分以上を保管できること。

③災害等により本庁舎のネットワークが停止（コアスイッチ停止）した場合にデータセンター内のＬ３スイッチがルーティング処理を引き継ぎ、閉域網へのバックアップ回線を接続することで、本庁舎及び災害対策支所からデータセンター内の統合型情報システムを利用できるよう設定すること。なお、バックアップ回線については別途市が用意する。

(5) リモートワーク環境

①本市が別途用意する端末及び閉域網を利用して、データセンターに接続し、統合型情報システムを利用できること。

②閉域網への接続にあたっては、厳格にアクセス制御を行い、本市職員・端末以外からの接続を制限すること。

第４章．機能要件

(1) システム要件

別紙２「システム要件」に基づき、要件全てを網羅する提案を行うこと。

第５章．構築要件

(1) 基本方針

①本市が別途用意するデータセンター内にシステムを構築すること。
なお、サーバラック仕様は以下のとおりとし、２ラックに収まる構成で提案すること。
＜１ラックあたりのサーバラック仕様＞
・19インチラック
・外形寸法：幅600㎜×奥行900㎜×高2000㎜
・ユニット数　41U
・積載荷重：1,000kg
・電力量 8kVA（定格）
・棚板1枚標準装備

②第３章(4)に記載するバックアップサーバを本市サーバ室に構築すること。なお、サーバラックは、既存19インチラックの空き領域に収容することとし、設置場所については、本市と協議の上、決定すること。

③サーバ機器等については可能な限り受託者社内にてセットアップし、データセンター及び本市サーバ室での作業期間を可能な限り短縮すること。

④バックアップは必須とし、各サーバ単位に必要となるデータのバックアップは今回構築する機器に格納すること。

⑤本市にて稼動している既存サーバ等監視システムにて一元管理できるよう設定すること。

(2) プラットフォーム要件

①インフラ／ハードウェア要件

ア）共通要件

・各システムが高品質、高信頼かつ安定稼働するために必要なハードウェアを導入すること。
・障害における他への影響の極小化、効率的なメンテナンス性を考慮した構成とすること。
・サーバデータは適切にバックアップでき、データが破損した場合にも復旧できる構成とすること。
・各システムの安定稼動を考慮し、機器の冗長化など故障・障害対策を講じること。
・サーバ、ストレージ及びネットワーク等のハードウェア機器は、仮想化が適さないものを除き、仮想化技術を用いることで集約を図ること。
・障害や災害時等のオフライン時においてもセキュアな環境で最低限の業務を遂行することを可能とすること。

イ）サーバ

・省エネ、長時間運用に対応したものであること。
・設置スペースを考慮し、可能な限り仮想化を行うこと。
・機器障害が発生した場合でも運用停止のないシステム構成であり、市民サービスに影響がないこと。
・ＬＡＮ、ファン、電源に関しては冗長化を行うこと。
・ＯＳは、ＷｉｎｄｏｗｓとＬｉｎｕｘに限定する。（日本語をサポートしていること）

ウ）ストレージ

・サーバ処理性能の向上、ネットワーク負荷軽減、データアクセスセキュリティの観点からＮＡＳ構成とし、冗長化できるＲＡＩＤ構成とするなど高信頼、高性能な構成とすること。

エ）障害時における即時復旧

・ＣＰＵ、メモリ、電源等の本体装置異常時のサーバ自動切替構成等の機能を備えた構成とすること。

・障害時における業務継続性を向上させるため、物理障害のポイントを削減し、各サービスの特性を踏まえた冗長化構成、バックアップ体制を講じること。

②周辺機器

別紙２「システム要件」に記載のハードウェアのほか、本提案システムに必要な機器を提案に含めること。

③テスト環境

運用における調査・検証・事前確認等が行えるよう、テスト環境を構築すること。

(3) ネットワーク要件

図２「システム構成図」を元に、セキュアなネットワークを設計・構築すること。

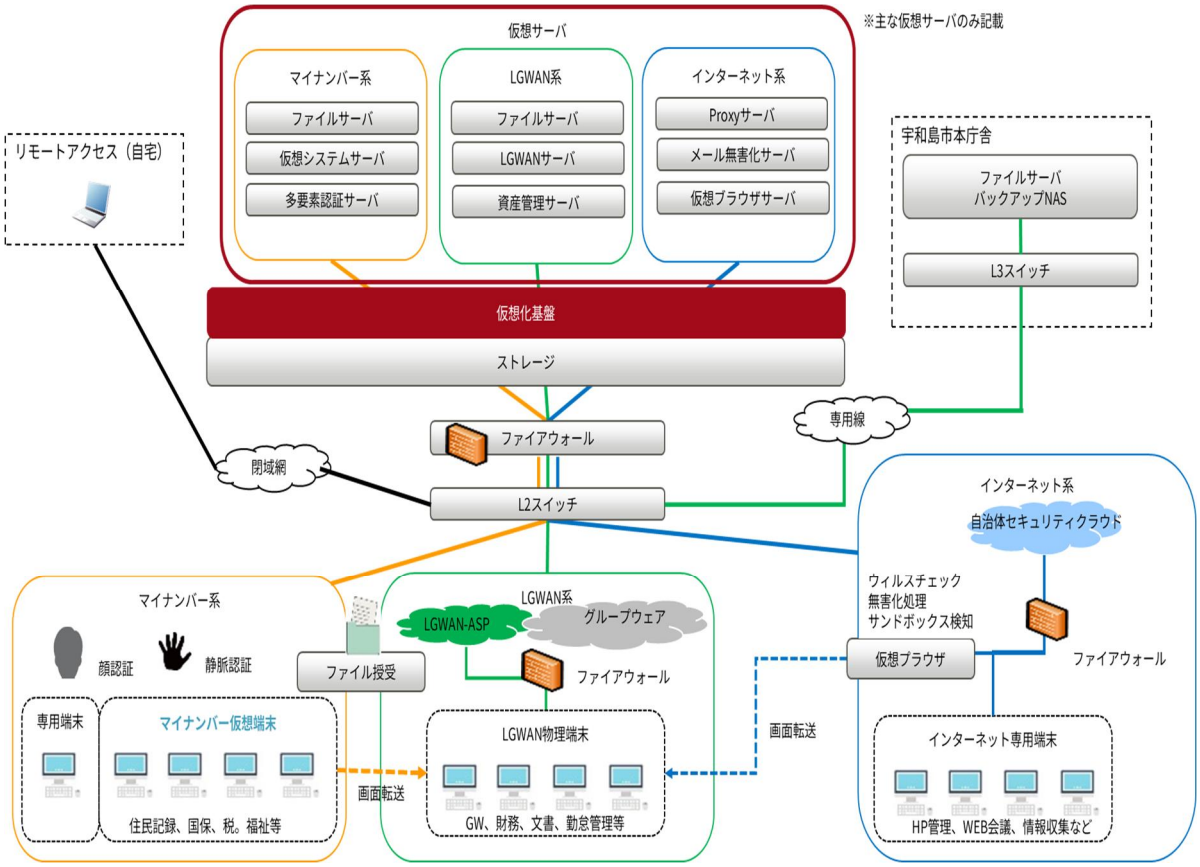

図２．システム構成図

(4) 事業遂行体制

①プロジェクト体制

ア）本事業を確実に遂行する体制（支援体制含む）を確保すること。

イ）本事業において十分な知識を有する者をプロジェクト管理者として置き、構築又は運用の経験を有する者をプロジェクト要員として参画させること。

ウ）以下のいずれかの資格を有するものをプロジェクト要員として参画させること。

・情報処理技術者（プロジェクトマネージャー試験）

・ＰＭＰ（プロジェクトマネジメントプロフェッショナル試験合格者）

②プロジェクト管理

ア）作業着手以降稼動まで月次で進捗報告会を開催することとし、プロジェクト管理者の出席を必須とする。また、適宜打ち合わせ等を実施し、本市に対し報告及び作業内容の説明・協議を行うこと。

イ）必要な作業を明確化し、作業項目を体系的に整理して文書化すること。作業項目等に変更があった場合についても変更理由を明確にして報告し承認を得ること。

ウ）議事録については、受託者が会の終了後、速やかに作成し、本市の承認を得ること。

(5) スケジュール

以下の本市指定イベントを明記した上で、構築スケジュールを提出すること（様式任意）

①更改業務期間： 契約締結日の翌日から本稼働（令和８年12月１日予定）の前日まで

②最低運用期間： 本稼働から60ヶ月間

③搬入開始可能時期： 令和８年７月以降

④操作研修時期： 令和８年10月頃

⑤稼動判定検査： 令和８年11月頃

⑥最終検査・引渡・本稼動： 令和８年12月

(6) システム移行要件

新システムへの移行においては、業務に支障がないよう十分配慮し、移行作業が極力簡易となるように努めること。また、各システムの特性について、十分考慮した上で本市と適時調整を行い、円滑に行うこと。

①基本方針

ア）次期システムへの移行は受託者が責任を持って管理すること。

イ）移行計画においては、本市及び現行基盤システム側で行うべき作業も含めて検討した上で計画書を作成し、現行保守事業者と協力して対応すること。

ウ）計画書に沿って実施する現行システムのデータ抽出及び設定変更作業、導入機器の現行ネットワーク接続作業については、本市及び現行保守事業者と協議し、必要に応じて現行保守業者に委託すること。なお、その際の委託費用は受託者負担とし、移行に必要な機器の準備や接続も受託者が実施すること。

エ）移行作業は現行システムの運用中の作業となるため、受託者は現行システムの停止や性能劣化等を発生させないための対策を講ずること。

オ）移行にあたっては職員負担の軽減に留意すること。

②システム移行条件

ア）移行計画書の作成

受託者は、本番環境へのシステム移行及びデータ移行に備えて、移行の方法、環境、ツール、工程等を記載した移行計画書の作成を行うこと。

イ）リハーサルの実施

移行データ及び移行手順の検証、移行時間の測定等、本番移行を想定した内容でリハーサルを実施すること。可能な限り本番と同等のツール、データ、手順を実施し、本番環境との差分を少なくすること。

ウ）データ移行

移行データは、受託者にて分析、変換、移行及び検証を実施し新システムへ移行を行うこと。データ移行の実施結果及び検証結果については本市に報告すること。

エ）その他

停止による業務影響が大きなシステムは、現行及び次期システムの並行稼働期間を設けることを必須とし、切り戻しを可能とすること。

移行が失敗した場合に備え、綿密な切り戻し手順及びスケジュールを準備し、本市の承認を得ること。

関係するシステムについては可能な限り移行タイミングを分割し、移行失敗に伴う切り戻しや業務影響を最小限に抑えるようスケジュールを作成すること。

③データ移行作業場所

データの移行作業場所は、市役所本庁舎内及び本市が用意するデータセンターに限定する。

④データの取り扱いについて

可搬媒体を用いて作業を行う場合は、パスワード等による暗号化を施すなど情報漏えい対策に留意し、事前に本市の承認を得ること。

(7) 研修

研修の実施にあたっては、以下の要件を満たすこと。

①研修計画の策定

本市職員が円滑に本システムを利用できるよう、受託者は本市と協議の上、研修計画を策定すること。

また、研修で使用する資料については、事前に本市の承認を得て準備すること。

②研修内容

システム利用者（一般職員）向け研修とシステム管理者（情報システム部門職員）向け研修とする。

③研修環境

本稼働までに職員が自由に操作できる研修用のデモ環境を用意すること。研修に必要な端末等のクライアント機器は本市にて用意するが、セットアップは受託者にて行うこと。

第６章．保守要件

(1) ハードウェア保守

①障害対応

導入する機器全てに対し、以下条件にてオンサイトサポートを実施すること。

ア）ハードウェアトラブルに関し、一元的な窓口を開設すること。

イ）基本的な対応時間帯は平日の８時30分から17時15分までとするが、発生する障害の影響度により24時間365日対応すること。

ウ）対応依頼の連絡を受けてから３時間以内に本市が別途用意するデータセンターに到着可能な拠点を四国内に保持すること。

エ）上記拠点には、常時、技術者を配置しておくこと。

オ）上記拠点には、本システムの主要部品を常時配備しておくこと。

カ）機器の障害対応終了後は、原因及び修理内容を速やかに報告すると共に、定期的にまとめて本市に報告すること。

キ）ハードディスクには個人情報等重要データが含まれるため、故障等により交換する場合は事前に本市の許可を得た上で、本市職員が立ち会いのもと行うこと。また、交換したハードディスクは物理的破壊により復元不可能な状態とし、実施後は完了証明書を発行すること。

②定期点検

ア）導入機器の定期点検を年に１回実施すること。

イ）実施時期は業務への影響を避けるため土日祝日とし、本市の指定時期に実施すること。

ウ）定期交換部品は提案に含めるものとし、別途費用が発生しないこと。

③安定稼動対策

ア）導入する機器に対し、ＬGWAN回線又はインターネット回線経由でハードウェアＣＰＵ、電源などの故障・異常、メモリエラー、ＦＡＮ寿命など障害予兆、異常情報を本市の指定するメールアドレスに提供すること。

イ）障害未然防止、障害管理を目的に24時間365日閲覧可能な、本市専用のＷｅｂサイトを提供し、トラブルやＱ＆Ａの対応履歴、事例、ＯＳ等ソフトウェア修正情報情報を掲載すること。

ウ）障害未然防止として、本市稼働中の監視サーバにより得た障害予兆や、他団体で発生した重要障害については、本市担当者と相談の上、速やかに対策を講じること。

エ）システムを長期間にわたり安定して利用するために、内蔵バッテリ・駆動系部品等を定期的に交換すること。

オ）稼動後は本市の求めに応じて定期的に報告会を開催し、トラブル発生状況などを取りまとめ報告すること。

カ）本庁舎及びデータセンターの計画停電時など、本市からの申し出があった場合は、現地での稼働立会いを行うこと。

キ）その他必要と思われる対策について、提案すること。

(2) ソフトウェア保守

①システムサポート

導入するシステム全てに対し、以下条件にてオンサイトサポートを実施すること。

ア）トラブルやＱ＆Ａに関し、窓口を開設すること。(窓口受付時間：８時30分から17時15分)

イ）基本的な対応時間帯は平日の８時30分から17時15分までとする。ただし、発生する障害の影響度によっては本市と調整し、計画保守として対応すること。

ウ）ＯＳのセキュリティパッチ適用、ミドルウェアの修正パッチ適用、エラーログ調査等の定期点検を少なくとも年に１回実施することとし、適用については本市と十分な協議の上実施すること。

エ）対応依頼の連絡を受けてから速やかにリモート接続による障害対応を行うこと。ネットワーク障害等でリモート接続ができない場合は、３時間以内に本市が別途用意するデータセンターに到着可能な拠点を保持すること。

オ）稼動後は本市の求めに応じて定期的に報告会を開催し、トラブル発生状況などを取りまとめ報告すること。

ク）バグフィックスの早期提供を実施すること。

ケ）納入機器及びソフトウェアにファームウェア修正、パッチ等が出た際には、適用の要否を検討し、必要と認められる際には本市と相談のうえ、適用作業を行うこと。

コ）本市からの運用相談に対応すること、また必要に応じて現地サポートすること。

サ）その他必要と思われるサポートについて、提案すること。

シ）LGWAN利用機関のメールドメイン配送情報が更新された場合、必要に応じて、メールサーバの設定変更を行うこと。

ス）年１回、導入システムに関する人事異動の対応支援を行うこと。

(3) その他

本システム調達に係る運用保守契約が満了後、本市が延長保守を希望した場合は、本仕様と同等の内容によるハードウェア及びソフトウェア保守を継続できること。（１年程度を想定）

なお、延長保守料金については、本契約における毎月の保守料金額を超えないこと。

第７章．その他

(1) 納品物

引渡時期までに以下納品物を作成し、本市の承認を得ること。また、内容確認が容易にできるようインデックスを付すなどして納品すること。

①納品物

・業務完了報告書
・導入スケジュール
・会議・打合せ議事録
・導入機器一覧
・各システム毎の設計書
・移行計画書
・機器構成図
・ラック構成図
・ネットワーク図
・テスト仕様書兼成績書
・運用マニュアル/操作マニュアル
・端末セットアップ手順書
・本市と協議し作成した図書等

②納品形式

・業務完了報告書は紙媒体で１部、それ以外は電子媒体（ＤＶＤ等）　１部

③納品時期

令和８年11月30日

④納品場所

宇和島市企画政策部デジタル推進課情報統計係

(2) 検査

引渡前に実施する稼動判定検査に対応すること。

・指定納期遵守及び品質保持のため、稼動判定検査を実施する。
　時期についてはスケジュールに記載し提案すること。
・稼動判定検査にて指摘事項が発生した場合は、手直しを実施し再度稼動判定検査を受けること。手直しに要する費用は、受託者負担とする。

(3) 瑕疵担保責任

納品後、１年以内に発生した瑕疵については受託者の責任にて修正・対応すること。

(4) 再委託の禁止

本業務遂行に関し本市に対する事前の申請、並びにこれに対する本市の承認がなければ、業務の全部、又は一部を第三者に委託してはならない。

(5) 営業行為の禁止

提案書提出に際し、第三者を介しての営業行為及び庁舎外での折衝等を行わないこと。

また、本市からの依頼以外の営業行為は行わないこと。

(6) 仕様書と提案書の内容一致

提案内容については、虚偽がなく仕様書の要件をすべて満たすこと。また、仕様に基づき、追加費用を生じることなく提出した見積書の範囲内において対応を行うこと。

(7) 守秘義務

本市から開示した情報は、一切他へ漏らさないこと。運用保守業務終了後も同様とする。

【別紙１】更改対象システム

●ハードウェア

項	システム	数量
1	仮想化基盤ストレージ	1式
2	仮想化基盤サーバ	1式
3	LGWAN系Active Diretoryサーバ	1台
4	管理兼バックアップサーバ	1式
5	運用管理用コンソール	1式
6	周辺機器（ディスプレイ、ＫＶＭ）	1式
7	LGWANファイアウォール	2台
8	インターネットファイアウォール	1台
9	強靭化ファイアウォール	2台
10	ネットワーク機器①（サーバ集約スイッチ(10G)）	2台
11	ネットワーク機器②（サーバ集約スイッチ（業務））	2台
12	ネットワーク機器③（サーバ集約スイッチ（管理））	2台
13	ネットワーク機器④（系間用スイッチ）	1台
14	ネットワーク機器⑤（データセンタースイッチ）	2台
15	本庁バックアップNAS	1台

●仮想サーバ

項	システム	数量
16	多要素認証サーバ	2台
17	LGWANサーバ	1台
18	負荷分散装置	2台
19	ファイル授受	1台
20	個人番号利用事務系Active Diretoryサーバ	2台
21	インターネット系Active Diretoryサーバ	2台
22	LGWAN系ファイルサーバ	2台
23	仮想デスクトップ接続サーバ	2台
24	DHCPサーバ	2台
25	外部DNS/MAILサーバ	1台
26	インターネット系proxyサーバ	1台
27	内部DNS/MAILサーバ	1台
28	メール無害化サーバ	2台
29	仮想ブラウザ	4台
30	資産管理サーバ	2台
31	LGWAN系WSUSサーバ	1台
32	ネットワーク監視サーバ	1台
33	Syslogサーバ	1台
34	プリントサーバ	2台
35	ウィルス対策サーバ	2台
36	個人番号利用事務系ファイルサーバ	1台

【別紙２】

宇和島市統合型情報システム更改事業仕様書

システム要件

令和８年２月

宇和島市

ー　目次　ー

●ハードウェア

●仮想サーバ

仮想化基盤ストレージ

仕様内容		
1．基本構成		
	（1）	ストレージ専用装置であること。
	（2）	HA-Ｐａｉｒ構成であること（2台のストレージコントローラー構成）
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件
	①	メインサイト（1台）
	a)	メモリ：１２８ＧＢ以上
	b)	ネットワーク：１０ＧＢＡＳＥ－Ｔ×８以上
	c)	電源：冗長構成
	d)	ＲＡＩＤ：ＲＡＩＤ４、ＲＡＩＤ-DP、ＲＡＩＤ－ＴＥＣ
	e)	サポートプロトコル：ＮＦＳ、ＣＩＦＳ、ＩＳＣＳＩ、ＦＣ
	f)	サポートドライブ：ニアラインＳＡＳ　ＨＤＤ　４ＴＢ（７．２Ｋｒｐｍ）、ＳＡＳ　ＳＳＤ　７．６ＴＢ
	g)	ドライブ総容量：２７６ＴＢ以上
	h)	ラックマウントタイプとすること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	仮想化基盤サーバとの接続は１０ＧＢＡＳＥ－Ｔで接続可能なこと。
	b)	1台のファイルサーバによって複数のディスク領域を提供すること。 また各種サーバが必要とするディスク領域において適切なアクセス権の管理方式を設定できる機能を有すること。
	c)	ＮＡＳ（ＮＥＴＷＯＲＫ Ａｔｔａｃｈｅｄ Ｓｔｏｒａｇｅ）システムであること。
	d)	制御部は、汎用ＯＳではなく最適化された専用ＯＳであること。
	e)	構成として、HA-Ｐａｉｒ構成として動作すること。
	f)	構成として、ストレージ提供サービス（ＣＩＦＳやＮＦＳなど）に応じた仮想ストレージを構成できること。
	g)	データを効率的に格納する機能（圧縮、重複排除）を有すること。
	h)	同一ＲＡＩＤグループ内でのディスクの二重障害時でもデータ消失がないこと。
	i)	サーバ領域を８０ＴＢ以上とすること。
	j)	運用中でも動的に増減できるファイルシステムをサポートすること。
	k)	運用中でも動的に拡大できるＲＡＩＤ制御機構を有すること。
	l)	ハードウェアの異常、障害予兆が発生した場合に、メール通知が可能なこと。
	m)	各仮想サーバ、庁内クライアントからアクセス可能であること。
	n)	ストレージの管理は、ＧＵＩおよびＣＬＩで管理が可能なこと。
	o)	複製ボリュームを作成可能であること。
	p)	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	（2）	設定要件
	①	共通
	a)	納入時点での最新ファームウェアの適用を行うこと。
	b)	最適なパフォーマンスになるよう、ＲＡＩＤ構成の設定を行うこと。
	c)	仮想化基盤サーバをストレージ装置に全て接続し、実装すること。
	d)	データが破損した場合、高速リカバリー可能なこと。
	e)	ファイルデータに対し瞬時にバックアップが取得できること。また、バックアップの世代管理が1000世代以上可能なこと。
	f)	ハードウェアを監視し、故障を検出した際にシステム管理者に通知されるように設定を行うこと。
	g)	耐障害性の観点から必要な本数分スペアディスクの設定を行うこと。

仮想化基盤ストレージ

仕様内容		
	h)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	i)	新装置導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	②	以下のボリューム構成を行うこと。
	a)	仮想サーバ格納領域
	b)	個人番号利用事務系仮想PCユーザプロファイル格納領域
	（3）	データ移行
	①	共通
	a)	現行のストレージからデータロストなしに、オンラインでデータ移行が可能なこと。なお、完全なデータ移行を実現するために、システム切替時に限り、静止点が必要な場合は、この限りではない。
	b)	データ移行は、既存業務に影響がない状態で行うこと。
	c)	仮想サーバ格納領域
	d)	ファイルサーバ用データ格納領域（ファイルデータ領域は本庁・支所分を含める構成とすること。）

仮想化基盤サーバ

仕様内容		
1．基本構成		
	（1）	サーバ９台以上で構成すること。
	（2）	本機器上で稼働する仮想マシンは以下の通りとすること。
	①	－仮想PC　３００台以上
	②	－仮想サーバー　４０台以上
2．ハードウェア／ソフトウェア要件		
	（1）	サーバ（９台以上）
	①	ハードウェア要件
		以下に仮想基盤サーバ１台あたりのハード要件を示す
	a)	ＣＰＵ：Ｉｎｔｅｌ　Ｘｅｏｎ　６５３０Ｐ　プロセッサー　（２．３０ＧＨｚ、３２コア、１４４ＭＢ）×２以上
	b)	メモリ：２５６ＧＢ以上
	c)	ディスク：物理容量　１００ＧＢ（システム領域）
	d)	ディスク：物理容量　１５０ＧＢ（その他領域）以上
	e)	ＬＡＮ：２０ポート以上
	f)	通信速度：１０Ｇｂｐｓ、１Ｇｂｐｓ
	g)	電源：１００Ｖもしくは２００Ｖ対応、冗長構成
	h)	保守作業の時間短縮のため、通電されていない状態でも、システムボード上にモジュールやコンポーネントの異常・故障をLED通知できること。
	i)	OSハング時や緊急時にコンソールを接続しなくてもシステムのリブートが可能なように、本体にリセットボタンがあること
	j)	システム異常時のカーネルダンプ採取などを行う、本体にNMIボタンがあること
	（2）	ソフトウェア要件
	a)	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｈｙｐｅｒ－Ｖ以降であること。
	b)	サーバ管理ソフトウェアを導入すること。
	c)	仮想マシンが動作する環境を提供すること。
	d)	仮想化機能等を利用する上で必要となるＷｉｎｄｏｗｓライセンス等も本調達の範囲に含めること。
	e)	仮想化機能等を利用する上で必要となるＬｉｎｕｘライセンス等も本調達の範囲に含めること。
	f)	ウイルス対策ソフトウェアを導入すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	サーバ単体のハードウェアを監視し、故障の検出・システム管理者に通知可能なこと。
	b)	仮想マシンのシステム領域のイメージバックアップ／リカバリが可能なこと。
	c)	実行中のゲストOSを停止することなく運用状態のまま別の物理ストレージ上に移行できる機能を持つこと。
	d)	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	②	仮想化機能
	a)	Ｈｙｐｅｒ－Ｖのホストクラスタ（ＷＳＦＣ）機能を有すること。
	b)	Ｈｙｐｅｒ－Ｖ　Ｌｉｖｅ　Ｍｉｇｒａｔｉｏｎ機能を有すること。
	c)	Ｈｙｐｅｒ－Ｖの災害対策機能を有すること。
	（2）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	納入時点で最新のセキュリティパッチを適用すること。
	c)	ウイルス対策ソフトにより毎日スケジュールスキャンおよびパターンファイルが自動更新されるように設定を行うこと。

仮想化基盤サーバ

仕様内容		
	d)	ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	e)	ハードウェアを監視し、故障を検出した際にシステム管理者に通知されるように設定を行うこと。
	f)	仮想化基盤サーバ１台がダウンしても残った仮想化基盤サーバ上で仮想サーバを稼働させることができること。
	g)	設定後、システムイメージのフルバックアップを行うこと。
	h)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	②	仮想化機能
	a)	本サーバ上で稼働する仮想サーバの配置場所はストレージ装置上となるように設定を行うこと。
	b)	本サーバ上で稼動する仮想サーバが最適なパフォーマンスになるように適切に設定を行うこと。
	c)	現在稼働している仮想化基盤サーバから当市が指定する仮想マシンを本調達で導入する仮想化基盤サーバ上に移行し、正常に動作するよう設定を行うこと。
	d)	移行する仮想マシンに必要なリソース（ＣＰＵ、メモリ、ディスク容量）については既存環境を確認し算出すること。
	e)	仮想マシンの移行については本市及び現行保守事業者と協議し、必要に応じて現行保守業者に委託すること。 その際の委託費用は受託者負担とすること。
	f)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。

LGWAN系Active Diretoryサーバ

仕様内容		
1．基本構成		
	（1）	サーバ構成は３台以上の構成として動作させること。
	①	１台はラックマウント物理単体サーバとして動作させること。
	②	デバイスＣＡＬを１５００台分用意すること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件（物理サーバ）
	①	サーバ（１台）
	a)	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｓｔａｎｄａｒｄ　Ｅｄｉｔｉｏｎ以降であること。
	b)	ＣＰＵ：Ｉｎｔｅｌ　Ｘｅｏｎ　６３２５Ｐ（３．５ＧＨｚ/4ｺｱ/１２ＭＢ）以上
	c)	メモリ：１６ＧＢ以上
	d)	内蔵ディスク:３００ＧＢ（１０Ｋｒｐｍ）×２（ＲＡＩＤ１＋ＨＳ）以上
	e)	ホットスペア用のディスクを搭載できること。
	f)	ＬＡＮ：２ポート以上
	g)	１９インチラックマウントサイズ１Ｕ以内で搭載できること。
	h)	保守作業の時間短縮のため、通電されていない状態でも、システムボード上にモジュールやコンポーネントの異常・故障をLED通知できること。
	i)	OSハング時や緊急時にコンソールを接続しなくてもシステムのリブートが可能なように、本体にリセットボタンがあること
	j)	システム異常時のカーネルダンプ採取などを行う、本体にNMIボタンがあること
	（2）	ハードウェア要件（仮想サーバ 2台）
	a)	ＣＰＵ：２コア以上
	b)	メモリ：４ＧＢ以上
	c)	ディスク：２００ＧＢ（システム領域、データ領域）以上
	d)	ＬＡＮ：１ポート以上
	（3）	ソフトウェア要件（物理）
	a)	ウイルス対策ソフトウェアを導入すること。
	b)	バックアップソフトウェアを導入すること。
	c)	サーバ機能としてＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインコントローラ機能を提供すること。
	d)	Ｗｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５ デバイスＣＡＬを１５００用意すること。
	（4）	ソフトウェア要件（仮想サーバ）
	a)	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｓｔａｎｄａｒｄ　Ｅｄｉｔｉｏｎ以降であること。
	b)	ウイルス対策ソフトウェアを導入すること。
	c)	サーバ機能としてＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインコントローラ機能を提供すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	管理兼バックアップサーバと連動してデータのバックアップ／リカバリが可能なこと。
	b)	ウイルスリアルタイムスキャン、スケジュールスキャン、ウイルスパターンファイルの自動更新機能を有すること。
	②	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインコントローラ機能
	a)	ドメインコントローラ機能、ＤＮＳ機能を提供すること。
	（2）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	納入時点で最新のセキュリティパッチを適用すること。

LGWAN系Active Diretoryサーバ

仕様内容		
	c)	ウイルス対策ソフトにより毎日スケジュールスキャンおよびパターンファイルが自動更新されるように設定を行うこと。
	d)	ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	e)	バックアップのスケジュール設定を行うこと。
	f)	設定後、フルバックアップを行うこと。
	g)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	h)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	i)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。
	②	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインコントローラ機能
	a)	既存サーバ上のドメインに含まれるドメイン名、アカウント、設定情報などはすべて引き継ぐように設定を行うこと。
	b)	ポリシー設計は原則変更しないものとする。ただし、Ｗｉｎｄｏｗｓ　Ｓｅｒｖｅｒ２０２５での新機能についてセキュリティ設計上有効な機能については市担当者と協議のうえ設定を行うこと。
	c)	マルチマスタ構成とし１台の障害時においても継続して業務が提供できるように設定を行うこと。

管理兼バックアップサーバ

仕様内容		
1．基本構成		
	（1）	ラックマウント単体サーバとして動作させること。
	（2）	サーバ構成は１台構成とする。
	（3）	バックアップ用のストレージを用意すること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件
	①	サーバ（１台）
	a)	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｓｔａｎｄａｒｄ　Ｅｄｉｔｉｏｎ以降であること。
	b)	ＣＰＵ：Ｉｎｔｅｌ　Ｘｅｏｎ　６３２５Ｐ（３．５ＧＨｚ/４ｺｱ/１２ＭＢ）以上
	c)	メモリ：１６ＧＢ以上
	d)	内蔵ディスク:ＨＤＤ３００ＧＢ（１０Ｋｒｐｍ）×３（ＲＡＩＤ１＋ＨＳ）以上
	e)	ホットスペア用のディスクを搭載できること。
	f)	ＬＡＮ：２ポート以上
	g)	１９インチラックマウントサイズ１Ｕ以内で搭載できること。
	h)	保守作業の時間短縮のため、通電されていない状態でも、システムボード上にモジュールやコンポーネントの異常・故障をLED通知できること。
	i)	OSハング時や緊急時にコンソールを接続しなくてもシステムのリブートが可能なように、本体にリセットボタンがあること
	j)	システム異常時のカーネルダンプ採取などを行う、本体にNMIボタンがあること
	②	バックアップストレージ（１台）
	a)	ストレージ専用装置であること。
	b)	メモリ：６４ＧＢ以上
	c)	ネットワーク：１０ＧＢＡＳＥ－Ｔ×８以上
	d)	電源：冗長構成
	e)	ＲＡＩＤ：ＲＡＩＤ０、ＲＡＩＤ１、ＲＡＩＤ１０、ＲＡＩＤ５、ＲＡＩＤ６、ＲＡＩＤ－ＤＤＰ
	f)	サポートプロトコル：ｉＳＣＳＩ、ＦＣ
	g)	ハードディスク：２４ＴＢ（７．２Ｋｒｐｍ）
	h)	ハードディスク総容量：１２７ＴＢ以上
	i)	ラックマウントタイプとすること。
	（2）	ソフトウェア要件（サーバ）
	a)	サーバ管理ソフトウェアを導入すること。
	b)	ウイルス対策ソフトウェアを導入すること。
	c)	バックアップソフトウェアを導入すること。
	d)	本調達で導入するサーバ（仮想、物理）のバックアップに必要なソフトウェア及びライセンスを調達すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	サーバ単体のハードウェアを監視し、故障の検出・システム管理者に通知可能なこと。
	b)	サーバ内蔵のハードディスクの監視、管理や設定などＲＡＩＤ管理が可能なこと。
	c)	トラブル時の障害調査を迅速にするため、サーバ環境等の調査用資料を一括で取得可能なこと。
	d)	システム領域のイメージバックアップ／リカバリが可能なこと。

管理兼バックアップサーバ

仕様内容		
	e)	ウイルスリアルタイムスキャン、スケジュールスキャン、ウイルスパターンファイルの自動更新機能を有すること。
	f)	サーバのハード寿命情報、ハードディスク異常等を本装置にて収集し、発生する障害予兆、異常情報を当市の指定するＥ－Ｍａｉｌアドレスに通知する機能を有すること。
	g)	バックアップデータの取得作業は自動化することを前提とし、原則としてシステム運用担当者による作業を必要としないこと。ただし、バックアップメディアの交換等はこの限りではないが、日次バックアップなど頻繁に行う作業については極力自動化できること。
	h)	増分バックアップによりバックアップ時間を短縮できること。
	i)	定期バックアップをスケジュールし、次回のバックアップ予定時刻までに古い世代の増分バックアップは自動的にフルバックアップへ統合できること。
	j)	仮想サーバのバックアップはエージェントレスのバックアップとし、Windowsサーバはサーバ全体の復元及びファイル単位の復元が可能であり、Linuxサーバはサーバ全体の復元が可能であること。
	k)	仮想サーバが起動中に取得できること。（アプリケーション整合性は考慮しない）
	l)	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	（2）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	納入時点で最新バージョンを導入すること。
	c)	納入時点で最新のセキュリティパッチを適用すること。
	d)	ウイルス対策ソフトにより毎日スケジュールスキャンおよびパターンファイルが自動更新されるように設定を行うこと。
	e)	既存ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	f)	ハードウェアを監視し、故障を検出した際にシステム管理者に通知されるように設定を行うこと。

運用管理用コンソール

仕様内容		
1．基本構成		
	（1）	ノートパソコンであること。
	（2）	本調達で導入するサーバを管理するため、管理コンソール1台を構成すること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件
	①	クライアント（1台）
	a)	ＣＰＵ：インテル® Core™ 3プロセッサー １００U以上
	b)	メモリ：８ＧＢ以上
	c)	内蔵ディスク:暗号化機能付フラッシュメモリ(ＤＲＡＭ－ｌｅｓｓ　ＳＳＤ／ＰＣＩｅ　ＮＶＭｅ)２５６ＧＢ
	d)	通信：８０２．１１ａｘ無線ＬＡＮ&Ｂｌｕｅｔｏｏｔｈ、有線ＬＡＮ×１
	（2）	ソフトウェア
	a)	ＯＳはＷｉｎｄｏｗｓ１１ Ｐｒｏであること。
	b)	ウイルス対策ソフトウェアを導入すること。
3．システム仕様		
	（1）	機能要件
	①	管理機能
	a)	Ｈｙｐｅｒ－Ｖの管理機能を利用可能なこと。
	b)	各サーバ用ウイルス対策ソフトウェアの管理機能を利用可能なこと。
	c)	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙの管理機能を利用可能なこと。
	d)	Ｗｉｎｄｏｗｓパッチ配信サーバ（ＷＳＵＳ）の管理機能を利用可能なこと。
	e)	ファイアウォールの管理機能を利用可能なこと。
	f)	負荷分散装置の管理機能を利用可能なこと。
	g)	その他本調達におけるシステムにて必要となるツールおよび管理機能を利用可能なこと。
	h)	本調達で導入するサーバをリモート操作可能な管理機能を利用可能なこと。
	i)	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	（2）	設定要件
	①	共通
	a)	管理機能を全てコンソールから行えるように設定すること。

周辺機器（ディスプレイ、ＫＶＭ）

仕様内容		
1．基本構成		
	（1）	ラックマウントタイプであること。
	（2）	以下のハードウェア要件、組合せ、数量については本提案に合わせて最適な構成にすること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件
	①	ディスプレイ
	a)	ＬＣＤ：１８．５インチＴＦＴ－ＬＣＤ@６０Ｈｚ
	b)	表示色：１，６６７万色以上
	c)	解像度：１３６６×７６８以上
	d)	マウス：タッチパッドなこと。
	e)	１９インチラックマウントサイズ１Ｕ以内で搭載できること。
	②	ＫＶＭ
	a)	ＫＶＭポート：ＲＪ-４５(黒）×8
	b)	サーバ接続台数：ラックマウント単体サーバと接続可能なこと。
	c)	サーバ切り替え：ホットキーによる切り替え、オンスクリーンディスプレイでの切り替えが可能であること。
	d)	１９インチラックマウントサイズ１Ｕ以内で搭載できること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	今回調達するサーバの画面を切り替えて操作可能なこと。
	（2）	設定要件
	①	共通
	a)	サーバとＫＶＭを接続する専用ケーブルを必要本数用意すること。

LGWANファイアウォール

仕様内容		
1．基本構成		
	（1）	ラックマウント機器として動作させること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件
	①	ＬGWAN用ファイアウォール（２台）
	a)	１０/１００/１０００ＢＡＳＥ-Tを８ポート以上搭載可能なこと。
	b)	ＲＳ２３２-Cシリアルインターフェースが１ポート以上あること。
	c)	ＵＰＳ－ＬＡＮが1ポート以上あること。
	d)	１９インチラックに搭載可能であること。高さは１U以内であること。
	e)	運用管理ＬＡＮが１ポート以上あること。
	f)	消費電力が８２W以下であること。
	g)	質量が９ｋｇ以下とすること。
	h)	日本国内製造であること。
	i)	ＭＡＲＫスイッチがあり、保守作業が容易なこと。
	j)	装置の冗長化（ホットスタンバイ）が可能なこと。
3．システム仕様		
	（1）	機能要件
	①	ファイアウォール機能
	a)	ＦＷはＩＰｖ４とＩＰｖ６のステートフルインスペクションをサポートしていること。
	b)	Ｌ２/Ｌ３/Ｌ４フィルタリング(FW)をＩＰｖ４とＩＰｖ６でサポートしていること。
	c)	ＦＷの性能は５Ｇｂｐｓ以上、２００，０００同時セッション以上をサポートしていること。
	d)	Ｐ２Ｐソフトの検知・遮断をサポートしていること。
	e)	アプリケーション単位で検知・遮断をサポートしていること。
	②	ネットワーク機能
	a)	ＶＬＡＮ（ＰｏｒｔＶＬＡＮ、ＴａｇＶＬＡＮ、ＭＡＣＶＬＡＮ）をサポートしていること。
	b)	ＮＡＴ（アドレス変換）／ＮＡＰＴ（ＩＰマスカレード)をサポートしていること。
	c)	ＩＰｖ４ルータ機能としてＳｔａｔｉｃ、ＲＩＰｖ１/ｖ２、ＯＳＰＦｖ２、ＢＧＰｖ４をサポートしていること。
	d)	ルータモード、ブリッジモードをサポートしていること。
	③	管理機能
	a)	日本語ＷｅｂＵＩとＣＬＩの両方での設定が可能で、ＣＬＩはｔｅｌｎｅｔとＳＳＨをサポートしていること。
	b)	ＳＮＭＰｖ１、ＳＮＭＰｖ２ｃ、ＳＮＭＰｖ３プロトコルにて、ＭＩＢ２および拡張ＭＩＢの監視に対応していること。
	c)	Ｓｙｓｌｏｇ転送機能をサポートしていること。
	d)	全てのログをマニュアル（日本語）に記載があること。
	e)	無停電電源装置と電源連動可能であること。
	（2）	設定要件
	①	共通
	a)	納入時点での最新ファームウェアの適用を行うこと。
	b)	ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	c)	市指定の管理コンソールからのみＷｅｂＵＩにアクセス可能となるように設定を行うこと。
	d)	平行稼働を考慮した設定を行うこと。
	e)	既存環境で使用している機器のファイアウォール設定をすべて引き継ぐように設定を行うこと。
	f)	現行ネットワークの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。

LGWANファイアウォール

仕様内容		
	g)	新装置導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。

インターネットファイアウォール

仕様内容		
1．基本構成		
	（1）	ラックマウント機器として動作させること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件
	①	ファイアウォール（1台）
	a)	１０/１００/１０００ＢＡＳＥ-Tを１２ポート以上搭載可能なこと。
	b)	ＲＳ２３２-Cシリアルインターフェースが１ポート以上あること。
	c)	ＵＰＳ－ＬＡＮが1ポート以上あること。
	d)	１９インチラックに搭載可能であること。高さは１U以内であること。
	e)	運用管理ＬＡＮが１ポート以上あること。
	f)	消費電力が１６７W以下であること。
	g)	質量が１５ｋｇ以下とすること。
	h)	日本国内製造であること。
	i)	ＭＡＲＫスイッチがあり、保守作業が容易なこと。
3．システム仕様		
	（1）	機能要件
	①	ファイアウォール機能
	a)	ＦＷはＩＰｖ４とＩＰｖ６のステートフルインスペクションをサポートしていること。
	b)	Ｌ２/Ｌ３/Ｌ４フィルタリング(FW)をＩＰｖ４とＩＰｖ６でサポートしていること。
	c)	ＦＷの性能は１５Ｇｂｐｓ以上、２，０００，０００同時セッション以上をサポートしていること。
	d)	Ｐ２Ｐソフトの検知・遮断をサポートしていること。
	e)	アプリケーション単位で検知・遮断をサポートしていること。
	②	ネットワーク機能
	a)	ＶＬＡＮ（ＰｏｒｔＶＬＡＮ、ＴａｇＶＬＡＮ、ＭＡＣＶＬＡＮ）をサポートしていること。
	b)	ＮＡＴ（アドレス変換）／ＮＡＰＴ（ＩＰマスカレード)をサポートしていること。
	c)	ＩＰｖ４ルータ機能としてＳｔａｔｉｃ、ＲＩＰｖ1/ｖ２、ＯＳＰＦｖ２、ＢＧＰｖ４をサポートしていること。
	d)	ルータモード、ブリッジモードをサポートしていること。
	e)	ＰＰＰｏＥクライアントをサポートしていること。
	③	管理機能
	a)	日本語ＷｅｂＵＩとＣＬＩの両方での設定が可能で、ＣＬＩはｔｅｌｎｅｔとＳＳＨをサポートしていること。
	b)	ＳＮＭＰｖ１、ＳＮＭＰｖ２ｃ、ＳＮＭＰｖ３プロトコルにて、ＭＩＢ２および拡張ＭＩＢの監視に対応していること。
	c)	Ｓｙｓｌｏｇ転送機能をサポートしていること。
	d)	全てのログをマニュアル（日本語）に記載があること。
	e)	無停電電源装置と電源連動可能であること。
	（2）	設定要件
	①	共通
	a)	納入時点での最新ファームウェアの適用を行うこと。
	b)	インターネットへの接続にあたり、自治体セキュリティクラウドのポリシーに則った設定を行うこと。
	c)	セキュリティチェックツール等によりセキュリティ監査し、監査結果の提示を行うこと。
	d)	ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	e)	運用管理コンソールからのみＷｅｂＵＩにアクセス可能となるように設定を行うこと。
	f)	平行稼働を考慮した設定を行うこと。

インターネットファイアウォール

仕様内容		
	g)	既存環境で使用している機器のファイアウォール設定をすべて引き継ぐように設定を行うこと。
	h)	外部セグメント、DMZセグメント、内部セグメントの設定を行うこと。
	i)	現行ネットワークの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	j)	新装置導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。

強靭化ファイアウォール

仕様内容		
1．基本構成		
	（1）	ラックマウント機器として動作させること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件
	①	ファイアウォール（2台）
	a)	１０/１００/１０００ＢＡＳＥ-Tを８ポート以上搭載可能なこと。
	b)	ＲＳ２３２-Cシリアルインターフェースが１ポート以上あること。
	c)	ＵＰＳ－ＬＡＮが1ポート以上あること。
	d)	１９インチラックに搭載可能であること。高さは１U以内であること。
	e)	運用管理ＬＡＮが１ポート以上あること。
	f)	消費電力が８２W以下であること。
	g)	質量が９ｋｇ以下とすること。
	h)	日本国内製造であること。
	i)	ＭＡＲＫスイッチがあり、保守作業が容易なこと。
	j)	装置の冗長化（ホットスタンバイ）が可能なこと。
3．システム仕様		
	（1）	機能要件
	①	ファイアウォール機能
	a)	ＦＷはＩＰｖ４とＩＰｖ６のステートフルインスペクションをサポートしていること。
	b)	Ｌ２/Ｌ３/Ｌ４フィルタリング(FW)をＩＰｖ４とＩＰｖ６でサポートしていること。
	c)	ＦＷの性能は5Ｇｂｐｓ以上、２００，０００同時セッション以上をサポートしていること。
	d)	Ｐ２Ｐソフトの検知・遮断をサポートしていること。
	e)	アプリケーション単位で検知・遮断をサポートしていること。
	②	ネットワーク機能
	a)	ＶＬＡＮ（ＰｏｒｔＶＬＡＮ、ＴａｇＶＬＡＮ、ＭＡＣＶＬＡＮ）をサポートしていること。
	b)	ＮＡＴ（アドレス変換）／ＮＡＰＴ（ＩＰマスカレード)をサポートしていること。
	c)	ＩＰｖ４ルータ機能としてＳｔａｔｉｃ、ＲＩＰｖ1/ｖ２、ＯＳＰＦｖ２、ＢＧＰｖ４をサポートしていること。
	d)	ルータモード、ブリッジモードをサポートしていること。
	e)	ＰＰＰｏＥクライアントをサポートしていること。
	③	管理機能
	a)	日本語ＷｅｂＵＩとＣＬＩの両方での設定が可能で、ＣＬＩはｔｅｌｎｅｔとＳＳＨをサポートしていること。
	b)	ＳＮＭＰｖ１、ＳＮＭＰｖ２ｃ、ＳＮＭＰｖ３プロトコルにて、ＭＩＢ２および拡張ＭＩＢの監視に対応していること。
	c)	Ｓｙｓｌｏｇ転送機能をサポートしていること。
	d)	全てのログをマニュアル（日本語）に記載があること。
	e)	無停電電源装置と電源連動可能であること。
	（2）	設定要件
	①	共通
	a)	納入時点での最新ファームウェアの適用を行うこと。
	b)	庁内ネットワークに対し、インターネット接続系、個人番号利用事務系、ＬＧＷＡＮ接続系の３系統にネットワーク分離を行うこと。
	c)	市指定の管理コンソールからのみＷｅｂＵＩにアクセス可能となるように設定を行うこと。
	d)	平行稼働を考慮した設定を行うこと。
	e)	既存環境で使用している機器のファイアウォール設定をすべて引き継ぐように設定を行うこと。

強靭化ファイアウォール

仕様内容		
	f)	現行ネットワークの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	g)	新装置導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。

ネットワーク機器①（サーバ集約スイッチ（10G））

仕様内容		
1．基本構成		
	（1）	本調達に必要となるネットワーク機器の導入を行うこと。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件
	①	共通
	a)	１０ＧＢＡＳＥ－Ｔ×４８以上
	b)	ラックマウントタイプ：１Ｕ以内（１台あたり）
	c)	質量が８．２５ｋｇ以下（１台あたり）とすること。
3．システム仕様		
	（1）	機能要件
	①	以下のスイッチ機能を有すること。
	a)	スイッチファブリックとして、６４０Ｇｂｐｓのバックプレーン容量を有すること。
	b)	４７６．１９Ｍｂｐｓ以上のパケット処理能力を有すること。
	c)	Ｓｔａｃｋ構成が可能であること。
	d)	スパニングツリー構成が可能なこと。
	e)	ポートベースＶＬＡＮ、８０２．１Ｑが可能なこと。
	f)	４０００以上のＶＬＡＮが設定可能なこと。
	（2）	設定要件
	①	共通
	a)	仮想化基盤サーバとストレージ間の通信で利用する接続インターフェースは１０ＧＢＡＳＥ－Ｔインターフェースで接続すること。
	b)	１台のスイッチに障害が発生しても通信経路が確保できるよう冗長構成とすること。
	c)	納入時点で最新のファームウェアを導入すること。
	d)	既存ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	e)	利用しないポートについては、設定により接続できないようにすること。
	f)	現行ネットワークの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	g)	新装置導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。

ネットワーク機器②（サーバ集約スイッチ（業務））

仕様内容		
1．基本構成		
	（1）	本調達に必要となるネットワーク機器の導入を行うこと。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件
	①	共通
	a)	インターフェース（１０／１００／１０００ＢＡＳＥ－Ｔ）×９６以上
	b)	ラックマウントタイプ：１Ｕ以内（１台あたり）
	c)	質量が７．４５ｋｇ以下（１台あたり）とすること。
3．システム仕様		
	（1）	機能要件
	①	以下のスイッチ機能を有すること。
	a)	スイッチファブリックとして、２５６Ｇｂｐｓのバックプレーン容量を有すること。
	b)	１９０．４７Ｍｂｐｓ以上のパケット処理能力を有すること。
	c)	Ｓｔａｃｋ構成が可能であること。
	d)	スパニングツリー構成が可能なこと。
	e)	ポートベースＶＬＡＮ、８０２．１Ｑが可能なこと。
	f)	４０００以上のＶＬＡＮが設定可能なこと。
	（2）	設定要件
	①	共通
	a)	１台のスイッチに障害が発生しても通信経路が確保できるよう冗長構成とすること。
	b)	納入時点で最新のファームウェアを導入すること。
	c)	既存ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	d)	利用しないポートについては、設定により接続できないようにすること。
	e)	現行ネットワークの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	f)	新装置導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。

ネットワーク機器③（サーバ集約スイッチ（管理））

仕様内容		
1．基本構成		
	（1）	本調達に必要となるネットワーク機器の導入を行うこと。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件
	①	共通
	a)	インターフェース（１０／１００／１０００ＢＡＳＥ－Ｔ）×９６以上
	b)	ラックマウントタイプ：１Ｕ以内（１台あたり）
	c)	質量が７．４５ｋｇ以下（１台あたり）とすること。
3．システム仕様		
	（1）	機能要件
	①	以下のスイッチ機能を有すること。
	a)	スイッチファブリックとして、２５６Ｇｂｐｓのバックプレーン容量を有すること。
	b)	１９０．４７Ｍｂｐｓ以上のパケット処理能力を有すること。
	c)	Ｓｔａｃｋ構成が可能であること。
	d)	スパニングツリー構成が可能なこと。
	e)	ポートベースＶＬＡＮ、８０２．１Ｑが可能なこと。
	f)	４０００以上のＶＬＡＮが設定可能なこと。
	（2）	設定要件
	①	共通
	a)	１台のスイッチに障害が発生しても通信経路が確保できるよう冗長構成とすること。
	b)	納入時点で最新のファームウェアを導入すること。
	c)	既存ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	d)	利用しないポートについては、設定により接続できないようにすること。
	e)	現行ネットワークの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	f)	新装置導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。

ネットワーク機器④（系間用スイッチ）

仕様内容		
1．基本構成		
	（1）	本調達に必要となるネットワーク機器の導入を行うこと。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件
	①	共通
	a)	インターフェース（１０／１００／１０００ＢＡＳＥ－Ｔ）×４８以上
	b)	1G　ＳＦＰスロット×４以上
	c)	ラックマウントタイプ：１Ｕ以内
	d)	質量が４．５３ｋｇ以下とすること。
3．システム仕様		
	（1）	機能要件
	①	以下のスイッチ機能を有すること。
	a)	スイッチファブリックとして、１０４Ｇｂｐｓのバックプレーン容量を有すること。
	b)	７７．３８Ｍｂｐｓ以上のパケット処理能力を有すること。
	c)	スパニングツリー構成が可能なこと。
	d)	ポートベースＶＬＡＮ、８０２．１Ｑが可能なこと。
	e)	１０００以上のＶＬＡＮが設定可能なこと。
	f)	自動ネゴシエーション機能を有すること
	（2）	設定要件
	①	共通
	a)	仮想化基盤サーバ間の通信で利用する接続インターフェースは１０００ＢＡＳＥ－Ｔインターフェースで接続すること。
	b)	納入時点で最新のファームウェアを導入すること。
	c)	既存ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	d)	利用しないポートについては、設定により接続できないようにすること。
	e)	現行ネットワークの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	f)	新装置導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。

ネットワーク機器⑤（データセンタースイッチ）

仕様内容		
１．基本構成		
	（１）	本調達に必要となるネットワーク機器の導入を行うこと。
２．ハードウェア／ソフトウェア要件		
	（１）	ハードウェア要件
	①	共通
	a)	インターフェース（１０／１００／１０００ＢＡＳＥ－Ｔ）×４８以上
	b)	ラックマウントタイプ：１Ｕ以内（１台あたり）
	c)	質量が７．２７ｋｇ以下とすること。（１台あたり）
３．システム仕様		
	（１）	機能要件
	①	以下のスイッチ機能を有すること。
	a)	スイッチファブリックとして、２０８Ｇｂｐｓのバックプレーン容量を有すること。
	b)	１５４．７６Ｍｂｐｓ以上のパケット処理能力を有すること。
	c)	Ｓｔａｃｋ構成が可能であること。
	d)	スパニングツリー構成が可能なこと。
	e)	ポートベースＶＬＡＮ、８０２．１Ｑが可能なこと。
	f)	４０００以上のＶＬＡＮが設定可能なこと。
	g)	自動ネゴシエーション機能を有すること
	（２）	設定要件
	①	共通
	a)	１台のスイッチに障害が発生しても通信経路が確保できるよう冗長構成とすること。
	b)	納入時点で最新のファームウェアを導入すること。
	c)	既存ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	d)	利用しないポートについては、設定により接続できないようにすること。
	e)	BCP対策として、本庁のネットワーク停止時（本庁コアスイッチ停止持）に本スイッチがルーティング処理を引継ぎ、業務継続に必要なネットワークに対してルーティング処理が行えるようにすること。
	f)	市が別途用意する閉域網と接続する設定を行うこと。
	g)	現行ネットワークの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	h)	新装置導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。

本庁バックアップNAS

仕様内容		
1．基本構成		
	（1）	１９インチラックに搭載可能であること。高さは１U以内であること。
	（2）	１台のアプライアンス構成とすること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件
	a)	ＣＰＵ：２コア以上
	b)	メモリ：２ＧＢ以上
	c)	ディスク：２４ＴＢ以上（システム領域、データ領域）
	d)	ＬＡＮ：２ポート以上
	（2）	ソフトウェア要件
	a)	ＬＡＮのチーミングに対応していること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	ハードウェアを監視し、故障の検出・システム管理者にメール通知が可能なこと。
	b)	内蔵ハードディスクを複数台搭載可能であること。
	c)	内蔵ハードディスクを ＲＡＩＤ 構成で運用できること。また、ＲＡＩＤ 障害発生時にリビルド（再構築）機能を有すること。
	d)	ウィルス検索をリアルタイムに行い、ウィルス感染から防ぐことが可能であること。
	（2）	設定要件
	①	共通
	a)	本庁バックアップＮＡＳにデータセンタ内ファイルサーバのファイルを定期的（例：1日1回）にバックアップ取得すること。
	b)	データセンタ内ファイルサーバへのアクセスが不可となった場合、庁内端末から本庁バックアップＮＡＳへ直接アクセスを行い、格納されているファイルの閲覧が可能なこと。

多要素認証サーバ

仕様内容	
1．基本構成	
（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
①	個人番号利用事務系ネットワーク上に仮想サーバとして2台動作させること。
（2）	顔認証及び静脈認証に対応していること。
（3）	衛生面を考慮し、認証装置に対して完全非接触で認証できること。
（4）	顔認証は、ノートPC内蔵カメラを使用することができ、省スペース化が図れること。
（5）	静脈認証は、現有の静脈センサーを利用できること。
2．ハードウェア／ソフトウェア要件	
（1）	ハードウェア要件（仮想サーバ2台）
①	多要素認証サーバ（２台）
a）	ＣＰＵ：４コア以上
b）	メモリ：１６ＧＢ以上
c）	ディスク：３００ＧＢ（システム領域、データ領域）以上
d）	ＬＡＮ：１ポート以上
②	認証機器
a）	現行機による対応とする。
（2）	ソフトウェア要件（仮想サーバ）
a）	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｓｔａｎｄａｒｄ　Ｅｄｉｔｉｏｎ以降であること。
b）	ウイルス対策ソフトウェアを導入すること。
c）	多要素認証用のライセンスを１１００準備すること。
3．システム仕様	
（1）	機能要件
①	共通
a)	顔認証及び静脈認証ログオンによる確実な本人認証が可能なこと。
b)	１：１認証方式に対応していること。
c)	Windowsログオン及びＰＣロック、スクリーンセーバーロックの解除時の認証に利用可能なこと。
d)	Windowsログオンに関しては、既存のActiveDirectoryドメインと連携して稼働可能なこと。
e)	Windowsログオン時の認証後に、Windowsパスワードを手入力してログオンする設定が可能であること。
f)	特定のアプリケーション起動時へのログオン認証が適用できること。
g)	一つのWindowsアカウントを、複数の認証ユーザーに設定できること。
h)	共用のWindowsアカウントを設定しているメンバー間では、Windowsロック状態を他のメンバーにてロック解除できること。また、個人の認証履歴を残すことが可能であること。
i)	利用者が認証できない場合は、管理者が該当利用者に対して非常用パスワードを発行することにより、利用者はユーザーＩＤと非常用パスワードの手入力にてログオン可能となること。
j)	顔認証においては、マスクを着用した顔画像を登録することなく、マスクを着用していても認証できること。
k)	顔認証においては、認証対象の顔データを最新に保ち、認証時の精度を高めるため、顔認証時に顔データを定期的に更新できること。
l)	管理者が非常用パスワードを発行する際には、非常用パスワードの利用可能期間、失敗可能回数を設定することが可能であること。
m)	全ての認証端末において、顔及び静脈情報登録処理などの管理者機能が使えること。
n)	ログオン履歴および認証システムの管理操作履歴を取得する機能を有すること。 認証ログにより、いつ、誰が、どのクライアントで認証成功／認証失敗したか特定できること。
o)	複数人で同一のWindowsアカウントを使用する場合も、個人の認証履歴を残すことが可能であること。
p)	蓄積されたログの中から、WindowsID／生体認証ID／コンピュータ名／期間／対象イベント（ログオン成功／ログオン失敗 等）などをキーとしてログを抽出できるツールを提供すること。
q)	氏名、ユーザーＩＤ、パスワード等のユーザー情報を、ＣＳＶ形式にて一括登録／更新／削除が可能なこと。また、登録済みユーザー情報はＣＳＶ形式にて抽出可能なこと。

多要素認証サーバ

仕様内容		
	r)	顔及び静脈登録画面および顔及び静脈認証画面において、センサーが撮影している生体情報を利用者がリアルタイムに確認できるようになっていること。
	s)	顔認証においては、写真データからの一括登録が可能であること。
	t)	他の利用者によってWindowsロックされたまま放置されている場合に、強制的にログオフ（又はシャットダウン）を実行できる機能を有すること。
	u)	ネットワーク障害等で認証サーバと通信できない場合は、ログオン情報をキャッシュしておき、キャッシュ情報を使った認証によりセキュアにログオンできること。更に、キャッシュには有効期限（日数）を設定できること。
	v)	Windows管理者権限がなくても、認証システムの管理者権限さえあれば、認証システムの管理ツールを起動できること。 ※認証システムの管理者権限と、Windowsの管理者権限は分離できること。
	w)	生体認証情報は、多要素認証サーバにて保持すること。
	x)	管理兼バックアップサーバと連携してデータのバックアップ／リカバリが可能なこと。
	y)	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	（２）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	原則として最新バージョンとし、納入時点でセキュリティの脆弱性が無いバージョンであること。
	c)	必要に応じて、現行サーバ上に登録されている職員のアカウントおよび静脈データの移行を行うこと。
	d)	バックアップのスケジュール設定を行うこと。
	e)	設定後、フルバックアップを行うこと。
	f)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	g)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	h)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。

LGWANサーバ

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件（仮想マシン）
	a)	ＣＰＵ：２コア以上
	b)	メモリ：４ＧＢ以上
	c)	ディスク：２００ＧＢ（システム領域、データ領域）以上
	d)	ＬＡＮ：１ポート以上
	（2）	ソフトウェア要件（仮想マシン）
	a)	ＯＳはＲｅｄＨａｔ　Ｅｎｔｅｒｐｒｉｓｅ　Ｌｉｎｕｘ　ｖ９．０　以降であること。
	b)	ウイルス対策ソフトウェアを導入すること。
	c)	サーバ機能として名前解決サーバ機能、メールサーバ機能、ＮＴＰサーバ機能を提供すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	管理兼バックアップサーバシステムと連携してデータのバックアップ／リカバリが可能なこと。
	b)	ウイルスリアルタイムスキャン、スケジュールスキャン、ウイルスパターンファイルの自動更新機能を有すること。
	②	名前解決サーバ機能
	a)	ＯＳ標準ＤＮＳサーバソフトウェアであるｂｉｎｄと同等の機能を有すること。
	b)	原則として最新バージョンとし、納入時点でセキュリティの脆弱性が無いバージョンであること。
	③	メールリレーサーバ機能
	a)	ＯＳ標準ＳＭＴＰサーバソフトウェアであるｐｏｓｔｆｉｘと同等の機能を有すること。
	b)	原則として最新バージョンとし、納入時点でセキュリティの脆弱性が無いバージョンであること。
	④	ＮＴＰサーバ機能
	a)	ＯＳ標準ＮＴＰサーバソフトウェアであるｎｔｐと同等の機能を有すること。
	b)	原則として最新バージョンとし、納入時点でセキュリティの脆弱性が無いバージョンであること。
	（2）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	納入時点で最新のセキュリティパッチを適用すること。
	c)	ウイルス対策ソフトにより毎日スケジュールスキャンおよびパターンファイルが自動更新されるように設定を行うこと。
	d)	バックアップのスケジュール設定を行うこと。
	e)	設定後、フルバックアップを行うこと。
	f)	内部ＤＮＳ／ＭＡＩＬサーバと連携し、ｌｇドメイン宛てのメールの振り分けを行うこと。
	g)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	h)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	i)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。

負荷分散装置

仕様内容		
1．基本構成		
	（1）	ラックマウント機器又は仮想アプライアンスとして動作させること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件（物理アプライアンス）
	①	負荷分散装置（２台）
	a)	１０/１００/１０００ＢＡＳＥ-Tを８ポート以上搭載可能なこと。
	b)	ＲＳ２３２-Cシリアルインターフェースが１ポート以上あること。
	c)	１９インチラックに搭載可能であること。高さは１U以内であること。
	d)	運用管理ＬＡＮが１ポート以上あること。
	e)	消費電力が８２W以下であること。
	f)	質量が９ｋｇ以下とすること。
	g)	日本国内製造であること。
	（2）	ハードウェア要件（仮想アプライアンス）
	①	負荷分散装置（２台）
	a)	ＣＰＵ：１コア以上
	b)	メモリ：４ＧＢ以上
	c)	ディスク：１００ＧＢ以上
	d)	ＬＡＮ：８ポート以上
3．システム仕様		
	（1）	機能要件
	①	負荷分散機能
	a)	サーバ負荷分散方式として、以下の方式をサポートしていること。 ラウンドロビン、静的な重み付け、最小コネクション数、最小クライアント数、最小サーバ負荷、最小データ通信量、最小応答時間
	b)	一意性保証（セッション維持）として、以下の方式をサポートしていること。 ノード単位(IPアドレス単位)、ノード単位(ネットマスク単位)、 コネクション単位、cookie単位、cookie･URLリトライ単位、HTTPヘッダー情報単位、 HTTP認証ヘッダー単位、SSLセッションID単位、SIPゲートウェイcall-ID単位
	c)	サーバ負荷分散機能は３．８Ｇｂｐｓ以上、２００，０００同時セッション以上をサポートしていること。
	d)	ＩＰｖ４とＩＰｖ６をサポートしていること。
	e)	故障したサーバが復旧したとき、負荷分散対象サーバに自動・手動で組み込む機能を有していること。
	f)	セッションリカバリー機能があり、サーバ故障時でも別サーバとの通信が継続できること。
	②	ネットワーク機能
	a)	ＶＬＡＮ（ＰｏｒｔＶＬＡＮ、ＴａｇＶＬＡＮ、ＭＡＣＶＬＡＮ）をサポートしていること。
	b)	ＮＡＴ（アドレス変換）／ＮＡＰＴ（ＩＰマスカレード)をサポートしていること。
	c)	ＩＰｖ４ルータ機能としてＳｔａｔｉｃ、ＲＩＰｖ１/ｖ２、ＯＳＰＦｖ２、ＢＧＰｖ４をサポートしていること。
	d)	ルータモード、ブリッジモードをサポートしていること。
	③	管理機能
	a)	日本語ＷｅｂＵＩとＣＬＩの両方での設定が可能で、ＣＬＩはｔｅｌｎｅｔとＳＳＨをサポートしていること。
	b)	ＳＮＭＰｖ１、ＳＮＭＰｖ２ｃ、ＳＮＭＰｖ３プロトコルにて、ＭＩＢ２および拡張ＭＩＢの監視に対応していること。
	c)	Ｓｙｓｌｏｇ転送機能をサポートしていること。
	d)	全てのログをマニュアル（日本語）に記載があること。
	e)	物理アプライアンスの場合、無停電電源装置と電源連動可能であること。
	（2）	設定要件
	①	共通
	a)	納入時点での最新ファームウェアの適用を行うこと。

負荷分散装置

仕様内容		
	b)	仮想デスクトップ接続サーバの負荷分散設定を行うこと。
	c)	既存ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	d)	管理コンソールからのみＷｅｂＵＩにアクセス可能となるように設定を行うこと。
	e)	現行ネットワークの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	f)	新装置導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。

ファイル授受

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件（仮想サーバ）
	①	ファイル共有アプライアンス（1台）
	a)	ＣＰＵ：１ＣＰＵ以上、4コア以上
	b)	メモリ：8ＧＢ以上
	c)	ディスク：1,100ＧＢ（システム領域、データ領域）以上
	d)	ＬＡＮ：2ポート以上
	②	ソフトウェア要件
	a)	ウィルスチェック機能を有すること。
	b)	以下のブラウザに対応していること。 ・Mozilla Firefox ・Google Chrome ・Microsoft Edge
	c)	SSLに対応していること。
	d)	ファイル授受のライセンスを４００準備すること。（ファイル授受の利用ユーザー数は４００）
	e)	ウイルス対策ソフトウェアを導入すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	個人番号利用事務系とLGWAN接続系の異なるネットワーク間でデータファイルを受け渡しができること。
	b)	ファイル送受信の証跡を自動的に記録できること。
	c)	第三者によるデータファイルのアップロード承認機能を有すること。
	d)	ウイルスチェック機能を標準搭載していること。
	e)	接続元IPアドレスによるアクセス制限が行えること
	f)	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	（2）	設定要件
	①	共通
	a)	納入時点での最新ファームウェアの適用を行うこと。
	b)	既存ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	c)	現行装置の設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	d)	新装置導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	e)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。

個人番号利用事務系Active Diretoryサーバ

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
	①	個人番号利用事務系ネットワーク上に仮想サーバとして2台動作させること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件（仮想サーバ2台）
	a)	ＣＰＵ：４コア以上
	b)	メモリ：８ＧＢ以上
	c)	ディスク：１００ＧＢ（システム領域、データ領域）以上
	d)	ＬＡＮ：１ポート以上
	（2）	ソフトウェア要件（仮想サーバ）
	a)	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｓｔａｎｄａｒｄ　Ｅｄｉｔｉｏｎ以降であること。
	b)	ウイルス対策ソフトウェアを導入すること。
	c)	サーバ機能としてＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインコントローラ機能を提供すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	管理兼バックアップサーバシステムと連動してデータのバックアップ／リカバリが可能なこと。
	b)	ウイルスリアルタイムスキャン、スケジュールスキャン、ウイルスパターンファイルの自動更新機能を有すること。
	②	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインコントローラ機能
	a)	ドメインコントローラ機能、ＤＮＳ機能を提供すること。
	（2）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	納入時点で最新のセキュリティパッチを適用すること。
	c)	ウイルス対策ソフトにより毎日スケジュールスキャンおよびパターンファイルが自動更新されるように設定を行うこと。
	d)	ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	e)	バックアップのスケジュール設定を行うこと。
	f)	設定後、フルバックアップを行うこと。
	g)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	h)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	i)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。
	②	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインコントローラ機能
	a)	既存サーバ上のドメインに含まれるドメイン名、アカウント、設定情報などはすべて引き継ぐように設定を行うこと。
	b)	ポリシー設計は原則変更しないものとする。ただし、Ｗｉｎｄｏｗｓ　Ｓｅｒｖｅｒ２０２５での新機能についてセキュリティ設計上有効な機能については市担当者と協議のうえ設定を行うこと。
	c)	マルチマスタ構成とし１台の障害時においても継続して業務が提供できるように設定を行うこと。

インターネット系Active Diretoryサーバ

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
	①	インターネット接続系ネットワーク上に仮想サーバとして2台動作させること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件（仮想サーバ2台）
	a)	ＣＰＵ：４コア以上
	b)	メモリ：８ＧＢ以上
	c)	ディスク：１００ＧＢ（システム領域、データ領域）以上
	d)	ＬＡＮ：１ポート以上
	（2）	ソフトウェア要件（仮想サーバ）
	a)	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｓｔａｎｄａｒｄ　Ｅｄｉｔｉｏｎ以降であること。
	b)	ウイルス対策ソフトウェアを導入すること。
	c)	サーバ機能としてＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインコントローラ機能を提供すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	管理兼バックアップサーバシステムと連動してデータのバックアップ／リカバリが可能なこと。
	b)	ウイルスリアルタイムスキャン、スケジュールスキャン、ウイルスパターンファイルの自動更新機能を有すること。
	②	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインコントローラ機能
	a)	ドメインコントローラ機能、ＤＮＳ機能を提供すること。
	（2）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	納入時点で最新のセキュリティパッチを適用すること。
	c)	ウイルス対策ソフトにより毎日スケジュールスキャンおよびパターンファイルが自動更新されるように設定を行うこと。
	d)	ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	e)	バックアップのスケジュール設定を行うこと。
	f)	設定後、フルバックアップを行うこと。
	g)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	h)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	i)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。
	②	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインコントローラ機能
	a)	既存サーバ上のドメインに含まれるドメイン名、アカウント、設定情報などはすべて引き継ぐように設定を行うこと。
	b)	ポリシー設計は原則変更しないものとする。ただし、Ｗｉｎｄｏｗｓ　Ｓｅｒｖｅｒ２０２５での新機能についてセキュリティ設計上有効な機能については市担当者と協議のうえ設定を行うこと。
	c)	マルチマスタ構成とし１台の障害時においても継続して業務が提供できるように設定を行うこと。

LGWAN系ファイルサーバ

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
	①	本庁用サーバ、支所用サーバとして別々に動作させること。
	②	本庁用サーバ、支所用サーバ合計で２０ＴＢ以上のディスク容量を確保し、設計時に協議の上、容量の割り当てを行うこと。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件
	①	以下に本庁用で動作するファイルサーバシステムのハード要件を記載する
	a)	ＣＰＵ：４コア以上
	b)	メモリ：８ＧＢ以上
	c)	ディスク：物理容量　１４ＴＢ以上（システム領域、データ領域）以上（本庁用ファイルサーバ）
	d)	ＬＡＮ：１ポート以上
	②	以下に支所用で動作するファイルサーバシステムのハード要件を記載する
	a)	ＣＰＵ：４コア以上
	b)	メモリ：８ＧＢ以上
	c)	ディスク：物理容量　３ＴＢ以上（システム領域、データ領域）以上（支所用ファイルサーバ）
	d)	ＬＡＮ：１ポート以上
	（2）	ソフトウェア要件
	①	以下に本庁用で動作するファイルサーバシステムのソフトウェア要件を記載する
	a)	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｓｔａｎｄａｒｄ　Ｅｄｉｔｉｏｎ以降であること。
	b)	ウイルス対策ソフトウェアを導入すること。
	c)	本庁・支所の庁内行政端末(職員端末)へファイルデータ格納機能を提供すること。
	（3）	ソフトウェア要件
	①	以下に支所用で動作するファイルサーバシステムのソフトウェア要件を記載する
	a)	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｓｔａｎｄａｒｄ　Ｅｄｉｔｉｏｎ以降であること。
	b)	ウイルス対策ソフトウェアを導入すること。
	c)	本庁・支所の庁内行政端末(職員端末)へファイルデータ格納機能を提供すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	管理兼バックアップサーバシステムと連携してデータのバックアップ／リカバリが可能なこと。
	b)	ウイルスリアルタイムスキャン、スケジュールスキャン、ウイルスパターンファイルの自動更新機能を有すること。
	②	ファイルサーバ機能
	a)	ファイルサーバ機能を有すること。
	b)	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	（2）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	納入時点で最新のセキュリティパッチを適用すること。
	c)	ウイルス対策ソフトにより毎日スケジュールスキャンおよびパターンファイルが自動更新されるように設定を行うこと。
	d)	ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	e)	遠隔地保管（データセンター外）にデータバックアップを行うようスケジュール設定を行うこと。
	f)	ＬＧＷＡＮ接続系のＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインに参加を行うこと。

LGWAN系ファイルサーバ

仕様内容		
	g)	設定後、システムイメージのフルバックアップを行うこと。
	h)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	i)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	j)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。
	②	ファイルサーバ機能
	a)	既存ファイルサーバ(本庁・支所)上にあるデータについてはフォルダ構成およびアクセス権を維持した状態で移行を行うこと。
	b)	ストレージ上のデータ格納領域をファイルサーバの共有領域として動作するように設定を行うこと。
	c)	部署単位に容量制限を行うこと。容量制限については、市担当者と協議の上、決定すること。

仮想デスクトップ接続サーバ

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
	（2）	本機器上で稼働する仮想マシンは以下の通りである。
	①	－仮想デスクトップ接続サーバ　２台以上
	②	－個人番号利用事務系仮想PC　２９８台以上
	③	－ＬＧＷＡＮ接続系仮想PC　１台以上
	④	－インターネット系仮想PC　１台以上
2．ハードウェア／ソフトウェア要件		
	（1）	仮想デスクトップ接続サーバ要件（仮想マシン２台）
	a)	ＣＰＵ：８コア以上
	b)	メモリ：１６ＧＢ以上
	c)	ディスク：１００ＧＢ（システム領域、データ領域）以上
	d)	ＬＡＮ：１ポート以上
	e)	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｓｔａｎｄａｒｄ　Ｅｄｉｔｉｏｎ以降であること。
	f)	ウイルス対策ソフトウェアを導入すること。
	（2）	仮想ＰＣ要件（仮想マシン３００台）
	a)	ＣＰＵ：２コア以上
	b)	メモリ：８ＧＢ以上
	c)	ディスク：１００ＧＢ（システム領域、データ領域）以上
	d)	ＬＡＮ：１ポート以上
	e)	ＯＳはＷｉｎｄｏｗｓ１１以降であること。
	f)	ウイルス対策ソフトウェアを導入すること。
	g)	以下ソフトウェアライセンスを本調達に含めること ・Ｍｉｃｒｏｓｏｆｔ　Ｏｆｆｉｃｅ　ＰｒｏｆｅｓｓｉｏｎａｌＰｌｕｓ　２０２４　・・・７０台分
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	仮想基盤サーバ上に構築すること。
	b)	管理用画面は日本語のUIが提供されること。
	c)	マウスカーソルが指すボタンの簡易説明が表示される設定ができる機能を有すること。
	d)	各サーバーは、環境構築状況や問題の発生状況を正しく確認できるよう、UI上に構成図として視覚的に表示されること。
	e)	アイコン上やサーバー登録一覧にアラートや異常状態の情報を表示できること。発生している一番優先順位の高いアラート項目の色で、各サーバーの状態を色付けして表示でき、アラートの詳細機能も確認できること。
	f)	各サーバーのメモリ使用率やネットワークの送信・受信量などのパフォーマンスに関する情報を、グラフで視覚的に確認できること。
	g)	各サーバーのシステム稼働ログやイベントログを収集し、収集したログを対象サーバー、対象期間、ログ種別、警告レベル、キーワード等の検索条件を複数指定して検索できること。 また、ログの検索条件は保存できること。
	h)	仮想端末起動の集中によるサーバーの負荷を軽減させるため、あらかじめ仮想端末を起動するスケジュールを設定できること。（曜日 / 時刻）
	i)	ランチャーで接続失敗や認証不可などのエラーが発生すると、問い合わせ番号が記載されたエラー画面を物理端末に表示すること。 また、その問い合わせ番号から詳細や対処方法を管理画面上で確認し、メモも追記できること。
	j)	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	②	カタログ管理機能
	a)	ユーザーが使用する、同一構成の仮想端末の作成を行いやすいよう、UI上で仮想化の方式や設定について、イラストとヒントを用いて解説されていること。

仮想デスクトップ接続サーバ

仕様内容		
	b)	VDIのマスターイメージのチェックポイントに対して、Windows11の機能更新プログラムを適用する機能を有すること。機能更新プログラムの内容によっては、チェックポイントへ適用後、必要な対応を行う場合を考慮し、製品の保守契約ユーザー用Webサイトにて適切な情報を提供していること。
	c)	VDIで利用するOSについての大型アップデート（機能更新プログラム）について、その適用や管理を行うための専用の更新支援機能を搭載していること。
	d)	VDIの仮想端末カタログの作成や再作成を行う際に、操作ログ収集用のモジュールが自動でインストールできること。
	③	運用管理機能
	a)	1台の物理端末で、異なる仮想イメージを利用できるランチャーを備えていること。また、ランチャーのアイコン色を利用者ごとに任意で設定できること。
	b)	アカウント管理については、Microsoft Active Directory上のユーザー情報を利用して実現可能なシステムであること。
	c)	各シンクライアントの利用状況を把握するため、シンクライアントの操作画面を管理用画面で一覧表示する機能を有すること。
	d)	物理端末と仮想端末間のクリップボード共有は、指定したクリップボードのデータカテゴリ別（テキスト、ファイルなど）ごとに、制限できること。また、物理端末から仮想端末へのクリップボード共有のみ / 仮想端末から物理端末へのクリップボード共有のみ許可する設定もできること。またプリセット設定を利用してクリップボード制限が行えること。
	④	サポート・ライセンス
	a)	シンクライアントソフトウェアの保守サービスについて、契約利用期間内はメーカーから提供が受けられる契約をメーカーと締結しておくこと。
	b)	シンクライアントシステムのソフトウェアを開発サポートする組織は、日本国内に存在し、日本国内でトラブル解決が完結するメーカーの製品であること。
	c)	サポート情報や技術情報等のメーカーから提供される情報については、すべて日本語であること。
	d)	契約利用期間内は必要に応じてシンクライアントシステムのアップデート・最新版へのバージョンアップが可能であること。
	e)	今後の利用するアプリケーションソフトウェアの変化に対応するため、シンクライアントソフトウェアについては、VDI方式、SBC(RDS)方式のどちらでも利用可能なライセンスを契約利用期間中使えるようにすること。
	f)	シンクライアントソフトウェアについては、仮想端末上でのファイル操作やWebアクセスの操作ログを収集する権利を含むこと。
	（2）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	納入時点で最新のセキュリティパッチを適用すること。
	c)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	d)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	e)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。

DHCPサーバ

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
	（2）	仮想サーバとして2台動作させること。
	（3）	下記用途向けにＩＰアドレスの自動割り当てを行うこと。
	a)	個人番号利用事務系仮想PC
	b)	無線ＬＡＮ（フリーＷｉ-Ｆｉ）
	c)	無線ＬＡＮ（ＬＧＷＡＮ接続系）
	d)	無線ＬＡＮ（セキュリティクラウド接続）
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件（仮想マシン）
	a)	ＣＰＵ：１コア以上
	b)	メモリ：４ＧＢ以上
	c)	ディスク：１００ＧＢ（システム領域、データ領域）以上
	d)	ＬＡＮ：１ポート以上
	（2）	ソフトウェア要件（仮想マシン）
	a)	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｓｔａｎｄａｒｄ　Ｅｄｉｔｉｏｎ以降であること。
	b)	ウイルス対策ソフトウェアを導入すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	管理兼バックアップサーバと連携してデータのバックアップ／リカバリが可能なこと。
	b)	ウイルスリアルタイムスキャン、スケジュールスキャン、ウイルスパターンファイルの自動更新機能を有すること。
	c)	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	②	ＤＨＣＰサーバ機能
	a)	指定した範囲のＩＰアドレスを自動的に割り当てる機能を有すること。
	③	ＫＭＳサーバ機能
	a)	個人番号利用事務系仮想PCに対し、Windows OSやOfficeソフトに関するライセンス認証機能を有すること。
	（2）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	納入時点で最新のセキュリティパッチを適用すること。
	c)	ウイルス対策ソフトにより毎日スケジュールスキャンおよびパターンファイルが自動更新されるように設定を行うこと。
	d)	ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	e)	バックアップのスケジュール設定を行うこと。
	f)	ＬＧＷＡＮ接続系のＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインに参加を行うこと。
	g)	設定後、フルバックアップを行うこと。
	h)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	i)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	j)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。
	②	ＤＨＣＰサーバ機能
		下記用途向けに指定した範囲のＩＰアドレスを自動的に割り当てるよう設定を行うこと。
	a)	個人番号利用事務系仮想PC

DHCPサーバ

仕様内容		
	b)	無線ＬＡＮ（フリーＷｉ-Ｆｉ）
	c)	無線ＬＡＮ（ＬＧＷＡＮ接続系）
	d)	無線ＬＡＮ（セキュリティクラウド接続）
	③	ＫＭＳサーバ機能
	a)	個人番号利用事務系仮想PCに対し、Windows OSやOfficeソフトに関するライセンス認証を行うように設定を行うこと。

外部DNS/MAILサーバ

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件（仮想マシン）
	a)	ＣＰＵ：２コア以上
	b)	メモリ：４ＧＢ以上
	c)	ディスク：１２０ＧＢ（システム領域、データ領域）以上
	d)	ＬＡＮ：１ポート以上
	（2）	ソフトウェア要件（仮想マシン）
	a)	ＯＳはＲｅｄＨａｔ　Ｅｎｔｅｒｐｒｉｓｅ　Ｌｉｎｕｘ　ｖ９．０　以降であること。
	b)	ウイルス対策ソフトウェアを導入すること。
	c)	サーバ機能として名前解決サーバ機能、メールリレーサーバ機能、ＮＴＰサーバ機能を提供すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	管理兼バックアップサーバと連携してデータのバックアップ／リカバリが可能なこと。
	b)	ウイルスリアルタイムスキャン、スケジュールスキャン、ウイルスパターンファイルの自動更新機能を有すること。
	②	名前解決サーバ機能
	a)	ＯＳ標準ＤＮＳサーバソフトウェアであるｂｉｎｄと同等の機能を有すること。
	b)	原則として最新バージョンとし、納入時点でセキュリティの脆弱性が無いバージョンであること。
	③	メールリレーサーバ機能
	a)	ＯＳ標準ＳＭＴＰサーバソフトウェアであるｐｏｓｔｆｉｘと同等の機能を有すること。
	b)	原則として最新バージョンとし、納入時点でセキュリティの脆弱性が無いバージョンであること。
	④	ＮＴＰサーバ機能
	a)	ＯＳ標準ＮＴＰサーバソフトウェアであるｎｔｐと同等の機能を有すること。
	b)	原則として最新バージョンとし、納入時点でセキュリティの脆弱性が無いバージョンであること。
	（2）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	納入時点で最新のセキュリティパッチを適用すること。
	c)	ウイルス対策ソフトにより毎日スケジュールスキャンおよびパターンファイルが自動更新されるように設定を行うこと。
	d)	ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	e)	バックアップのスケジュール設定を行うこと。
	f)	各サーバ機能を提供するにあたり必要最低限のポート以外はインターネットからアクセスできないように設定を行うこと。
	g)	セキュリティチェックツール等によりサーバの状態を監査し、監査結果の提示を行うこと。
	h)	設定後、フルバックアップを行うこと。
	i)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	j)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	k)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。
	②	名前解決サーバ機能
	a)	本市で運用している公開ドメインおよびホスト情報を適切にインターネットへアナウンスするように設定を行うこと。
	b)	庁内からの名前解決要求を受けてインターネット上のホスト情報を提供できるように設定を行うこと。

外部DNS/MAILサーバ

仕様内容		
	c)	インターネットへ公開するにあたり必要な脆弱性対策を行うこと。
	③	メールリレーサーバ機能
	a)	本市で運用しているメールドメインのみを外部から受信しメール無害化サーバにリレーできるように設定を行うこと。
	b)	庁内からインターネットへのメールを正常に送信できるように設定を行うこと。
	c)	インターネットへ公開するに当たり必要な脆弱性対策を行うこと。
	④	ＮＴＰサーバ機能
	a)	インターネット上のＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	b)	庁内からのみ時刻同期要求を受けて時刻情報を提供できるように設定を行うこと。
	c)	インターネットへ公開するに当たり必要な脆弱性対策を行うこと。

インターネット系proxyサーバ

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
	（2）	愛媛県セキュリティクラウドを経由しインターネットが参照できること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件（仮想マシン）
	a)	ＣＰＵ：２コア以上
	b)	メモリ：４ＧＢ以上
	c)	ディスク：１００ＧＢ（システム領域、データ領域）以上
	d)	ＬＡＮ：１ポート以上
	（2）	ソフトウェア要件（仮想マシン）
	a)	ＯＳはＲｅｄＨａｔ　Ｅｎｔｅｒｐｒｉｓｅ　Ｌｉｎｕｘ　ｖ９．０　以降であること。
	b)	ウイルス対策ソフトウェアを導入すること。
	c)	サーバ機能としてＰｒｏｘｙサーバ機能を提供すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	管理兼バックアップサーバと連携してデータのバックアップ／リカバリが可能なこと。
	b)	ウイルスリアルタイムスキャン、スケジュールスキャン、ウイルスパターンファイルの自動更新機能を有すること。
	②	Ｐｒｏｘｙサーバ機能
	a)	ＯＳ標準Ｐｒｏｘｙサーバソフトウェアであるｓｑｕｉｄと同等の機能を有すること。
	b)	原則として最新バージョンとし、納入時点でセキュリティの脆弱性が無いバージョンであること。
	（2）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	納入時点で最新のセキュリティパッチを適用すること。
	c)	ウイルス対策ソフトにより毎日スケジュールスキャンおよびパターンファイルが自動更新されるように設定を行うこと。
	d)	ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	e)	バックアップのスケジュール設定を行うこと。
	f)	設定後、フルバックアップを行うこと。
	g)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	h)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	i)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。
	②	Ｐｒｏｘｙサーバ機能
	a)	インターネット系端末から愛媛県セキュリティクラウドを経由し、インターネットが参照できるように適切に設定を行うこと。

内部DNS/MAILサーバ

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件（仮想マシン）
	a)	ＣＰＵ：２コア以上
	b)	メモリ：４ＧＢ以上
	c)	ディスク：２００ＧＢ（システム領域、データ領域）以上
	d)	ＬＡＮ：１ポート以上
	（2）	ソフトウェア要件（仮想マシン）
	a)	ＯＳはＲｅｄＨａｔ　Ｅｎｔｅｒｐｒｉｓｅ　Ｌｉｎｕｘ　ｖ９．０　以降であること。
	b)	ウイルス対策ソフトウェアを導入すること。
	c)	サーバ機能として名前解決サーバ機能、メールサーバ機能、ＮＴＰサーバ機能を提供すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	管理兼バックアップサーバシステムと連携してデータのバックアップ／リカバリが可能なこと。
	b)	ウイルスリアルタイムスキャン、スケジュールスキャン、ウイルスパターンファイルの自動更新機能を有すること。
	②	名前解決サーバ機能
	a)	ＯＳ標準ＤＮＳサーバソフトウェアであるｂｉｎｄと同等の機能を有すること。
	b)	原則として最新バージョンとし、納入時点でセキュリティの脆弱性が無いバージョンであること。
	③	メールリレーサーバ機能
	a)	ＯＳ標準ＳＭＴＰサーバソフトウェアであるｐｏｓｔｆｉｘと同等の機能を有すること。
	b)	原則として最新バージョンとし、納入時点でセキュリティの脆弱性が無いバージョンであること。
	④	ＮＴＰサーバ機能
	a)	ＯＳ標準ＮＴＰサーバソフトウェアであるｎｔｐと同等の機能を有すること。
	b)	原則として最新バージョンとし、納入時点でセキュリティの脆弱性が無いバージョンであること。
	（2）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	納入時点で最新のセキュリティパッチを適用すること。
	c)	ウイルス対策ソフトにより毎日スケジュールスキャンおよびパターンファイルが自動更新されるように設定を行うこと。
	d)	ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	e)	バックアップのスケジュール設定を行うこと。
	f)	設定後、フルバックアップを行うこと。
	g)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	h)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	i)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。
	j)	メールアカウントの登録・修正・削除手順を用意すること。
	②	名前解決サーバ機能
	a)	本市で運用している庁内ドメインおよびホスト情報を適切に庁内へアナウンスするように設定を行うこと。
	b)	庁内からの名前解決要求を受けて庁内サーバのホスト情報を提供できるように設定を行うこと。
	c)	行政端末からＬＧＷＡＮドメインが参照できるように設定を行うこと。

内部DNS/MAILサーバ

仕様内容		
	③	メールリレーサーバ機能
	a)	メール無害化サーバ経由で受信したインターネットメールをＬＧWAN接続系メールサーバにリレーできるように設定を行うこと。
	b)	庁内から外部ＤＮＳ／ＭＡＩＬサーバ経由でインターネットへのメールを正常に送信できるように設定を行うこと。
	c)	ＬＧWANドメイン宛のメールをＬＧWANサーバへ配送できるように設定を行うこと。
	d)	本市で運用しているドメイン（導入業者に別途指示する）のメールを正常に受信できるように設定を行うこと。
	e)	本市で運用しているドメイン（導入業者に別途指示する）の既存メールスプールデータの移行を行うこと。
	④	ＮＴＰサーバ機能
	a)	外部ＤＮＳ／ＭＡＩＬサーバと正常に時刻同期できるように設定を行うこと。
	b)	庁内からのみ時刻同期要求を受けて時刻情報を提供できるように設定を行うこと。

メール無害化サーバ

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件（仮想マシン）※メールサーバ
	a）	ＣＰＵ：８コア以上
	b）	メモリ：８ＧＢ以上
	c）	ディスク：１３００ＧＢ（システム領域、データ領域）以上
	d）	ＬＡＮ：１ポート以上
	（2）	ハードウェア要件（仮想マシン）※無害化サーバ
	a）	ＣＰＵ：８コア以上
	b）	メモリ：８ＧＢ以上
	c）	ディスク：２００ＧＢ（システム領域、データ領域）以上
	d）	ＬＡＮ：１ポート以上
	（3）	ソフトウェア要件（仮想マシン）
	a）	物理環境、仮想環境上のWindows/Linuxの64bit OSに対応しているソフトウェアであり、64bitネイティブに動作すること。
	b）	ウイルス対策ソフトウェアを導入すること。
	c）	メール無害化に必要なライセンスを１２００準備すること。（利用メールアカウント数は１２００）
3．システム仕様		
	（1）	機能要件
	①	共通機能
	a）	メール通信プロトコルはSMTP、SMTPS、POP3、POP3Sの全てに対応しており、メール暗号化通信方式としてSTARTTLSにも対応していること。
	b）	1通のメールを宛先ドメイン単位で分割することができることで、多段構成としなくとも社外/社内/グループ会社等の宛先ドメインごとに送信メールの添付ファイル自動暗号化ルール適用を実現できること。
	c）	安全な差出人の「IPアドレス」と「ドメイン」をデータベース化して配信機能を有し、そのデータベースを利用して安全なメールのみを受信できる機能を有すること。 また、データベースに存在しない「IPアドレス」と「ドメイン」を収集し精査した上でデータベースとして配信できること。
	d）	受信したメールの添付ファイルを本文から削除し、内部ネットワークへメール無害化した形でメール本文のみ配送を可能とすること。且つ、HTMLメールやリッチテキストメールの本文テキスト化によるURL表示偽装などの攻撃防御と、URLリンク文字一部置換による人為的ミス削減が可能なこと。
	e）	送信ルールについて、複数ルールを組み合わせルールセットとして管理し、ルールの有効/無効の切り替えが運用に合わせて可能なこと。
	f）	特定のキーワードが含まれた場合など特定の条件下において、送信時に添付ファイルの自動パスワード暗号化を実現し、ZIP形式やAES(Advanced Encryption Standard) 256bit形式で送信できること。 あわせて、添付ファイル暗号化時の拡張子やファイル名を指定可能なこと。
	g）	送信メールを即時送信せず、事前に設定した任意の時間、一時保留可能なこと。保留時間設定箇所は、宛先が庁内か外部かで分かれており、時間差配送が可能なこと。
	h）	受信者本人が送信元メールアドレスのブラックリスト・ホワイトリストへの追加作業を、手動登録及びCSVファイルインポート等の手段で実施可能なこと。
	i）	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	②	ファイル無害化機能
	a）	添付ファイルを自動で無害化し、無害化後のファイルをメールに自動で再添付し配送可能なこと。
	b）	無害化処理は、OfficeファイルやPDFファイルほか200以上のファイル拡張子に対応していること。
	c）	無害化処理において、OLEオブジェクトは無害化後に再構成されること。
	d）	受信したファイルがパスワード付きZIPであってもメールセキュリティ製品上で解凍し、無害化処理を実行可能なこと。
	③	添付ファイル転送機能
	a）	ファイルをストレージ上にアップロードし、特定の宛先へ転送することができること。
	b）	ファイルの閲覧者をメールアドレス単位で指定できること。
	c）	100MBまでのファイルを転送できること。

メール無害化サーバ

仕様内容		
	d)	アップロードできるファイルの数に上限がないこと。
	e)	ファイルが少なくとも30日間保持されること。
	f)	ストレージ上に保管されるファイルが暗号化されていること。
	g)	ファイルをストレージ上にアップロードすると、アンチウイルス機能でウイルスチェックが実施されること。
	h)	アップロードしたファイルの一覧をポータル画面にて管理・閲覧できること。
	i)	受信者は共有URLへアクセスし、メールアドレスを入力後、ワンタイムパスワードを入力し、設定されたメールアドレスの場合はファイルのダウンロードができること。
	j)	宛先メールアドレスに送信されるメールの本文内に記載されるURL案内文言を任意に変更できること。
	k)	アップロードしたファイルに付与されている閲覧権限/ファイルサイズ/申請日時/セキュリティ判定結果/ファイル閲覧ログの全てがアップロードしたユーザー本人が確認できること。
	（2）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	原則として最新バージョンとし、納入時点でセキュリティの脆弱性が無いバージョンであること。
	c)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	d)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	e)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。

仮想ブラウザ

仕様内容		
1．基本構成		
	（1）	仮想ブラウザサーバは仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
	①	ユーザ端末の論理的に分離された仮想環境で、仮想ブラウザを実行できること。また仮想環境で実行するブラウザによってアクセスする Web サイトの情報は、仮想環境内に留めてユーザ端末のローカル環境と共有しないこと。
	②	ユーザ端末に生成される仮想環境は、ローカルコンテナ方式によりローカル環境と分離されていること。
2．ハードウェア／ソフトウェア要件		
	（1）	仮想マシン構成要件（サーバ）
	①	仮想ブラウザサーバ（4台以上）
	a)	ＣＰＵ：４コア以上
	b)	メモリ：８ＧＢ以上
	c)	ディスク：１００ＧＢ（システム領域、データ領域）以上
	d)	ＬＡＮ：１ポート以上
	（2）	ソフトウェア要件
	a)	仮想ブラウザの同時接続ライセンスを５００準備すること。
	b)	ウイルス対策ソフトウェアを導入すること。
3．システム仕様		
	（1）	機能要件
	①	共通機能
	a)	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	②	仮想ブラウザ機能
	a)	ユーザは仮想ブラウザのアプリケーションウインドウが直観的にわかること （枠線を表示し、仮想ブラウザであることがわかること）
	b)	仮想ブラウザからユーザ端末に設定されたプリンタに印刷できること。
	c)	ユーザ端末と仮想ブラウザ間のコピー・アンド・ペーストを許可または不許可に設定できること。 また、方向の制御もできること。
	d)	仮想ブラウザでダウンロードしたファイルの拡張子に関連付けられた Officeファイル（Word,Excel,PowerPoint）が利用できる機能を有すること。 ただし、セキュリティの観点からマクロ実行やアプリケーション連携機能は利用できないものとし、閲覧レベルでよいものとする。
	e)	ダウンロードファイルについてアンチウィルス機能を標準で有すること。
	f)	仮想ブラウザとして Firefox または Google Chrome、Microsoft Edge（Chromium 版）を使用でき、管理サーバの設定もしくはクライアントによる接続時に起動する仮想ブラウザを選択できること。
	g)	仮想ブラウザはユーザ端末のローカル環境のブラウザと同時に実行できること。
	h)	１ユーザアカウントで仮想ブラウザは同時にひとつだけ実行でき、起動後にブラウザタブの追加、別ウインドウでの表示が可能であること。
	i)	仮想ブラウザで Web 会議システム（Zoom、WebEX、Teams）が利用できること。ただし、Web 会議システムがサポートしているブラウザの前提でよい。
	j)	ユーザ個別に履歴/ブックマーク/パスワード/Cookie/証明書/例外サイト等の情報が保存可能なこと。
	k)	ユーザ端末で指定した URL を含むハイパーリンクをクリック、もしくはユーザ端末のブラウザで指定した URL を含む接続を行った際に、自動的に仮想ブラウザで当該 Web ページを開く機能を有すること。
	l)	ユーザ端末で指定した URL を含んだ Web アクセスで、自動的に仮想ブラウザを起動するリストは、前方一致および正規表現によるリスト設定が可能であり、設定によりリストにマッチした場合とアンマッチの場合を切り替えられる機能を有すること。
	m)	指定した時間、操作が行われていない場合に仮想ブラウザを自動で閉じるアイドルタイムアウト機能を有すること。また、設定は１分単位で可能なこと。
	n)	操作の有無に関わらず、指定した時間で仮想ブラウザを自動で閉じる強制タイムアウト機能を有すること。また、設定は１分単位で可能なこと。
	o)	仮想ブラウザから共有フォルダのマウントが可能なこと。マウントに必要なアカウントは個別指定または仮想ブラウザ起動で使用するアカウントをそのまま利用可能なこと。
	p)	ユーザ端末に生成される仮想環境は、ローカルコンテナ方式によりローカル環境と分離されていること。
	q)	ファイルシステムおよびネットワークの分離境界を超えたアクセスは拒否されること。
	r)	管理サーバは、ユーザ端末に対しては制御情報を含めた受動的通信のみを行うこと。

仮想ブラウザ

仕様内容		
	s)	緊急を要する事態等に、接続ライセンスの上限を超えるユーザ端末の接続を一定期間許容する運用モードがあること。
	③	セキュリティ機能
	a)	仮想環境のキャッシュやダウンロード領域は仮想ブラウザ終了時に削除され、再起動時は初期化された状態になること。ただし、ブックマークや履歴などはユーザ毎に管理サーバに保存し、再起動時も利用できる設定が可能であること。
	b)	ユーザ端末と仮想環境間のファイル転送は原則禁止であること。 ただし、ファイル持ち込み機能およびファイル持ち出し機能を設定することで、別の装置を必要とすることなく、クライアントソフトウェアによってファイル転送が可能になること。
	c)	仮想環境内では、インターネットから取得したプログラムが実行できないこと。
	d)	専用のVPNによるネットワーク分離機能を有すること。またはプロキシを強制することでネットワーク分離できること。
	e)	ネットワーク分離機能により、仮想環境からのアクセス先を制限できること。
	④	耐障害性機能
	a)	仮想ブラウザは管理サーバダウン時にオフラインキャッシュによる前回の接続情報を使ってオフライン起動できること。
	b)	オフライン起動は、管理サーバダウン時だけでなく管理サーバ過負荷状態でも使用できること。また、この機能により、管理サーバへの想定外の認証集中時でも安定して仮想ブラウザが起動できること。
	⑤	管理機能
	a)	ユーザアカウントは、CSV による一括登録、変更、削除ができること。
	b)	ユーザ認証に関する機能を有し、下記のいずれかを選択できること。 ① 管理サーバにユーザ情報を設定し、クライアントからの接続時にユーザ認証する機能を有すること。 ② Active Directory と連携しケルベロス認証する機能を有すること。 ③ ユーザ端末のドメインユーザでのシングルサインオンが可能なこと。
	c)	ユーザの利用状況をログとして記録できること。また、Web GUI の管理画面で閲覧でき、CSV ファイルでエクスポートできること。
	d)	ユーザのファイル転送操作をログとして記録できること。また、 Web GUI の管理画面で閲覧でき、CSV ファイルでエクスポートできること。
	e)	ユーザ端末から仮想環境へファイルの持ち出し（アップロード）をする際に上長承認によるワークフロー機能の利用を選択できること。
	f)	ファイルの持ち出し（アップロード）によりファイルを持ち出したことをログとして記録できること。
	（2）	設定要件
	①	共通
	a)	原則として最新バージョンとし、納入時点でセキュリティの脆弱性が無いバージョンであること。
	b)	設定により、ローカル環境から仮想環境にアップロードが可能であること。
	c)	設定により、仮想環境からローカル環境にファイル持ち込みが可能であること。ただし、ファイル持ち込みの際は無害化処理を施すこと。無害化に対応していない拡張子については、サンドボックスによる検知が可能であること。
	d)	クライアントソフトウェアをバージョンアップする機能を有し、アップデートに対する期間等の設定が行えること。

資産管理サーバ

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
	①	証跡管理ができること。
	②	外部媒体制御・持ち出し管理ができること。
2．ハードウェア／ソフトウェア要件		
	（1）	仮想マシン構成要件（サーバ）
	①	マスターサーバ（1台）
	a)	ＣＰＵ：８コア以上
	b)	メモリ：８ＧＢ以上
	c)	ディスク：４００ＧＢ（システム領域、データ領域）以上
	d)	ＯＳ：以下のオペレーティングシステムに対応していること。 ・Windows Server 2025 Standard Edition
	②	データーサーバ（1台）
	a)	ＣＰＵ：８コア以上
	b)	メモリ：８ＧＢ以上
	c)	ディスク：１３００ＧＢ（システム領域、データ領域）以上
	d)	ＯＳ：以下のオペレーティングシステムに対応していること。 ・Windows Server 2025 Standard Edition
	（2）	ソフトウェア要件
	a)	資産管理のライセンスを１５００準備すること。（管理対象の端末台数は１５００台）
	b)	ウイルス対策ソフトウェアを導入すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	管理対象端末から操作ログをネットワーク経由で自動的に収集し、管理できる機能を有すること。また、１つのコンソール画面から統合的に管理できること。
	b)	収集可能なログは、ログオン、ログオフの日時、実行されたソフトウェアについての起動・終了時間、ファイル操作、共有フォルダへのアクセス・ファイル操作、Webへのアクセス、USBメモリなどの記憶媒体を利用した内容、記憶媒体のシリアル情報、接続した通信デバイス、及び外部との通信状況等とする。
	c)	クライアントコンピューターからサーバー上の共有ファイルや、クライアントコンピューターもしくは組織外のコンピューターから、クライアントコンピューター上に作成された共有フォルダ（ファイルサーバー）へのアクセスおよびファイル操作(作成、コピー、ファイル名変更、移動、上書き、削除)をログとして記録する機能を有すること。 また、操作したファイルのフルパスを、フォルダオプション設定を変更することなく、ログとして表示すること。
	d)	Webへのアクセスログについて、httpsでの通信を含め、Microsoft Internet Explorer及びGoogle ChromeによるWebの閲覧やダウンロード、アップロード及び書き込みついて記録できること。また、Microsoft 365 / Office Online上でファイルをローカルに作成した時の、ファイル名やファイルパスをログとして記録する機能を有すること。
	e)	Bluetooth接続、無線LANアクセスポイントへの接続、TCP/IP通信等による接続が行われた際に、通信デバイスの情報を記録できること。
	f)	端末機を管理する管理機コンピューターの操作に対しても同様にログ収集が行えること。また、ログ検索・閲覧やリモート操作などの情報セキュリティ対策機能に対する操作に対するログも取得でき、管理者間で相互に検索及び閲覧が行えること。
	g)	操作ログをリアルタイムに収集し、当日の操作ログに対しても速やかに検索・閲覧が行えること。
	h)	収集したログデータは一定期間ごとに圧縮した状態で自動的にバックアップでき、バックアップデータも展開やリストアの作業をすることなく管理コンソールから閲覧できること。 また、圧縮してバックアップした複数のログデータに対して、まとめて検索できること。
	i)	特定の行為及び内容から、事前定義されたルールに従い、自動で通知する機能を有すること。
	j)	通知は、システム管理者に対して以外にも、端末機の利用者に対してポップアップで表示ができること。

資産管理サーバ

仕様内容		
	k)	あらかじめ登録されていない端末が接続された場合、該当のクライアントコンピューター情報を取得し、一覧表示できること。
	l)	トラブル発生時の対応として、対象端末機にリモート接続できる機能を有すること。
	m)	端末にインストールするアプリケーションは、すべての機能が一つのインストーラーで提供されること。
	n)	管理兼バックアップサーバと連携してデータのバックアップ／リカバリが可能なこと。
	o)	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	②	資産管理
	a)	全ての資産を一元管理できること。
	b)	収集したハードウェアおよびソフトウェア情報を、一覧で表示できること。
	c)	収集した資産情報を検索できること。検索条件には、インベントリ情報やOSのバージョン、空き容量、死活監視状態など複数項目を指定した検索が可能で、表示項目の順序・表示非表示を定義・保存でき、呼び出せること。
	d)	資産情報の検索の際は、インベントリ情報やWindows OSのバージョン、サービスパックなどから、同時に複数項目、キーワードおよび数値の範囲を指定して検索が可能であること。 また、検索条件ごとに表示項目の順序・表示非表示を定義・保存でき、呼び出せること。
	e)	ソフトウェア導入後に機器入替などにより削除された端末についても、検索対象として指定できること。
	③	デバイス制御
	a)	USBデバイスをシリアルナンバーごとに管理する機能を有すること。また、保有USBデバイスはシステムで台帳管理し、一覧で表示できること。
	b)	登録した外部記憶媒体に対して、シリアルナンバーごとに使用制限（使用許可/読み取り専用/使用不可）の設定ができ、設定対象をActive Directoryのユーザー単位、クライアントコンピューター単位、及びユーザーとクライアントコンピューターの組み合わせ単位で指定ができること。
	c)	設定ができるデバイス種別、メディアは、デバイス種別（USBメモリ、USBハードディスクドライブ、フロッピーディスクドライブ、CD/DVDドライブ、Blu-rayドライブ、イメージスキャナー、デジタルカメラ、モバイル端末、Windows ポータブル デバイス）、メディア（DVD-RAM、SDカード、MOディスク、コンパクトフラッシュなど）とする。
	d)	デバイス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。
	e)	USBデバイス内ファイルの日時情報を比較し、システム外で作成・編集された外部ファイルの持ち込みを自動判定し、そのUSBデバイスを使用禁止にする機能を有すること。
	f)	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利用して、紛失の可能性やUSB所持者・外部ファイルの特定を自動判定する機能を有すること。
	g)	USBデバイスの管理台帳に登録されているUSBメモリについて、各USBメモリの利用者もしくは管理責任者が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。
	h)	使用制限設定は、端末機を管理するグループ単位、端末単位及び、Active Directoryのユーザー単位にも設定ができること。
	④	ソフトウェア配布
	a)	指定した端末および検索グループに対して、複数の任意のプログラムを配布し、自動的にプログラムの実行および解除を行う機能を有し、ソフトウェアの配布日時と対象端末を設定し、配布したソフトウェアの配布状況および実行状況を確認することができること。また、配布時に利用する帯域を制限できること。
	b)	指定したクライアントコンピューターおよび検索グループに対して、複数の任意のプログラムを配布し、自動的にプログラムの実行および解除を行う機能を有すること。
	c)	ソフトウェアの配布日時と対象端末を設定し、配布したソフトウェアの配布状況および実行状況を確認することができること。また、配布時に利用する帯域を制限できること。
	d)	指定した端末に対して、Windows更新プログラムを配布し、自動的にセキュリティパッチを適用する機能を有し、端末毎の更新プログラムの適用状況が管理コンソールで確認できること。
	（２）	設定要件
	①	共通
	a)	バックアップのスケジュール設定を行うこと。
	b)	設定後、フルバックアップを行うこと。
	c)	LGWAN接続系Active Diretoryサーバ上のデータと連携し、既存庶務事務システムに就業データの連携を行うこと。
	d)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	e)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	f)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。

LGWAN系WSUSサーバ

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
	（2）	本庁用、支所用ＬＧＷＡＮ接続系端末の一元管理を行うこと。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件（仮想マシン）
	a)	ＣＰＵ：４コア以上
	b)	メモリ：１６ＧＢ以上
	c)	ディスク：１５００ＧＢ（システム領域、データ領域）以上
	d)	ＬＡＮ：1ポート以上
	（2）	ソフトウェア要件（仮想マシン）
	a)	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｓｔａｎｄａｒｄ　Ｅｄｉｔｉｏｎ以降であること。
	b)	ウイルス対策ソフトウェアを導入すること。
	c)	サーバ機能としてＷｉｎｄｏｗｓパッチ配信サーバ（ＷＳＵＳ）機能を提供すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	管理兼バックアップサーバと連携してデータのバックアップ／リカバリが可能なこと。
	b)	ウイルスリアルタイムスキャン、スケジュールスキャン、ウイルスパターンファイルの自動更新機能を有すること。
	c)	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	②	Ｗｉｎｄｏｗｓパッチ配信サーバ機能
	a)	最新バージョンを導入すること。
	（2）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	納入時点で最新のセキュリティパッチを適用すること。
	c)	ウイルス対策ソフトにより毎日スケジュールスキャンおよびパターンファイルが自動更新されるように設定を行うこと。
	d)	ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	e)	バックアップのスケジュール設定を行うこと。
	f)	ＬＧＷＡＮ接続系のＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインに参加を行うこと。
	g)	設定後、フルバックアップを行うこと。
	h)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	i)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	j)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。
	②	Ｗｉｎｄｏｗｓパッチ配信サーバ機能
	a)	クライアントに配信するＷｉｎｄｏｗｓパッチを効率的に管理できるように設定を行うこと。
	b)	管理対象クライアントの設定変更が必要な場合はシステム導入と合わせて変更作業を行うこと。
	c)	ＬＧＷＡＮ上のＵｐｄａｔｅサイトから必要な更新プログラムを取得できるように設定を行うこと。
	d)	ＬＧＷＡＮ接続系ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙサーバと連携し、グループポリシーに従ってＷｉｎｄｏｗｓパッチを適用できるように設定を行うこと。

ネットワーク監視サーバ

仕様内容		
１．基本構成		
	（１）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
	（２）	稼働しているサーバ・ネットワーク機器の監視を行うこと。
２．ハードウェア／ソフトウェア要件		
	（１）	ハードウェア要件（仮想マシン）
	a)	ＣＰＵ：４コア以上
	b)	メモリ：１６ＧＢ以上
	c)	ディスク：３００ＧＢ（システム領域、データ領域）以上
	d)	ＬＡＮ：１ポート以上
	（２）	ソフトウェア要件（仮想マシン）
	a)	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｓｔａｎｄａｒｄ　Ｅｄｉｔｉｏｎ以降であること。
	b)	ウイルス対策ソフトウェアを導入すること。
	c)	監視機能を提供すること。
３．システム仕様		
	（１）	機能要件
	①	共通
	a)	管理兼バックアップサーバと連携してデータのバックアップ／リカバリが可能なこと。
	b)	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	②	監視機能
	a)	ＴＣＰ／ＩＰベースのネットワークに接続された装置の稼働状況を定期的に収集し、ＩＰ巡回ログとして本装置に蓄積する機能を有すること。
	b)	IP アドレスの範囲指定、サブネットの指定、Active Directory からのインポート、CSV ファイルからのインポートにより、装置を一括して自動検出する機能を有すること。
	c)	生成されたすべてのアラートを一覧で表示でき、一覧からアラートのフィルター、ソート、検索などの機能を有すること。
	d)	システムを構成するサーバのＣＰＵ、メモリ、ディスクの情報を定期的に収集する機能を有すること。
	e)	システムを構成するサーバのプロセスを定期的に監視し、異常発生時は指定のメールアドレスに通報を行うこと。
	（２）	設定要件
	①	共通
	a)	システムを構成するサーバ及び既存ネットワーク機器に対し、定期的に疎通確認を行う設定を行うこと。
	b)	疎通確認に対し応答しない、もしくは異常なアラームを送信した機器に対しては、Ｅ－Ｍａｉｌで通報を行うこと。
	c)	必要に応じて、可用性、応答時間、使用率、トラフィック情報、アラート/イベント、インベントリ情報などのレポートを作成すること。
	d)	バックアップのスケジュール設定を行うこと。
	e)	設定後、フルバックアップを行うこと。
	f)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	g)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	h)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。

Syslogサーバ

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件（仮想マシン）
	a）	ＣＰＵ：２コア以上
	b）	メモリ：８ＧＢ以上
	c）	ディスク：８００ＧＢ（システム領域、データ領域）以上
	d）	ＬＡＮ：１ポート以上
	（2）	ソフトウェア要件（仮想マシン）
	a）	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｓｔａｎｄａｒｄ　Ｅｄｉｔｉｏｎ以降であること。
	b）	ウイルス対策ソフトウェアを導入すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a）	管理兼バックアップサーバと連携してデータのバックアップ／リカバリが可能なこと。
	b）	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	②	監視機能
	a）	管理対象の機器に対しエージェントレスでイベントログの一元管理が可能なこと。
	b）	イベントの種類やメッセージのキーワード、イベント ID など、任意の条件に当てはまるログを収集した際に、アラートを生成することが可能であること。その際、メールによる通知だけでなく、スクリプトを実行することも可能であること。
	c）	収集したログを定期的にアーカイブ化し、さらに一定時間が経過後、ZIP 形式のファイルに圧縮が可能であること。ZIP ファイルの保持期間は、継続、1 年、6 ヶ月、3 ヶ月、1ヶ月、1 週間から選択することができ、更にアーカイブ ZIP ファイルをインポートすることで、再度レポートとして表示することも可能であること。
	d）	ホストグループを作成することで、グループごとにデバイスを確認可能なこと。
	e）	収集したログの中から、任意のホスト、ログタイプ、ログに含まれるメッセージ、時間など、さまざまな条件を指定した上で、合致するログを検索することが可能であること。
	（2）	設定要件
	①	共通
	a）	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b）	原則として最新バージョンとし、納入時点でセキュリティの脆弱性が無いバージョンであること。
	c）	バックアップのスケジュール設定を行うこと。
	d）	設定後、フルバックアップを行うこと。
	e）	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	f）	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	g）	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。

プリントサーバ

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
	（2）	LGWAN系のプリントサーバを1台、個人番号利用事務系のプリントサーバを1台 動作させること
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件（仮想マシン）
	①	LGWAN系のプリントサーバ
	a）	ＣＰＵ：４コア以上
	b）	メモリ：８ＧＢ以上
	c）	ディスク：１００ＧＢ（システム領域、データ領域）以上
	d）	ＬＡＮ：１ポート以上
	②	個人番号利用事務系のプリントサーバ
	a）	ＣＰＵ：４コア以上
	b）	メモリ：８ＧＢ以上
	c）	ディスク：１００ＧＢ（システム領域、データ領域）以上
	d）	ＬＡＮ：１ポート以上
	（2）	ソフトウェア要件（仮想マシン）
	a）	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｓｔａｎｄａｒｄ　Ｅｄｉｔｉｏｎ以降であること。
	b）	ウイルス対策ソフトウェアを導入すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a）	管理兼バックアップサーバと連携してデータのバックアップ／リカバリが可能なこと。
	②	プリントサーバ機能
	a）	市で使用しているプリンター、複合機を一元管理し、クライアントＰＣから利用できる機能を有すること。
	b）	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	（2）	設定要件
	①	共通
	a）	市が提供するプリンタや複合機のドライバーインストール作業を行うこと。
	b）	LGWAN系のプリントサーバはＬＧＷＡＮ接続系のＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインに参加を行うこと。
	c）	個人番号利用事務系のプリントサーバは個人番号利用事務系のＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインに参加を行うこと。
	d）	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	e）	納入時点で最新のセキュリティパッチを適用すること。
	f）	プリンタ増減および接続クライアントに増減が発生した際、プリンタマッピングCSVリストをメンテナンスし、更新できること。
	g）	バックアップのスケジュール設定を行うこと。
	h）	設定後、フルバックアップを行うこと。
	i）	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	j）	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	k）	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。

ウィルス対策サーバ

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
	（2）	ウイルス対策サーバ（本庁用、支所用）を１台で動作させること。
	（3）	ウイルス対策サーバ（Linuxウィルスソフト管理用）を１台で動作させること。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件（仮想マシン）
	①	ウイルス対策サーバ（本庁用、支所用）
	a)	ＣＰＵ：４コア以上
	b)	メモリ：１６ＧＢ以上
	c)	ディスク：３００ＧＢ（システム領域、データ領域）以上
	d)	ＬＡＮ：１ポート以上
	②	ウイルス対策サーバ（Linux ウィルスソフト管理用）
	a)	ＣＰＵ：４コア以上
	b)	メモリ：６ＧＢ以上
	c)	ディスク：１００ＧＢ（システム領域、データ領域）以上
	d)	ＬＡＮ：１ポート以上
	（2）	ソフトウェア要件（仮想マシン）
	a)	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｓｔａｎｄａｒｄ　Ｅｄｉｔｉｏｎ以降であること。
	b)	ウイルス対策ソフトウェアを導入すること。
	c)	サーバ機能としてクライアント用ウイルス対策ソフトの一括管理機能を提供すること。
	d)	クライアント用ウイルス対策ソフトを導入すること。本ソフトを導入するにあたり 必要に応じて既存ウィルス対策ソフトをアンインストールする費用も本調達に含めること。 リース期間中の更新ライセンスも一括納入すること。
	e)	ウイルス対策（本庁用、支所用）ライセンスを２０００準備すること。
	f)	ウイルス対策（Linux用）ライセンスを導入Linuxサーバ台数分準備すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	管理兼バックアップサーバと連携してデータのバックアップ／リカバリが可能なこと。
	b)	ウイルスリアルタイムスキャン、スケジュールスキャン、ウイルスパターンファイルの自動更新機能を有すること。
	c)	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	②	クライアント用ウイルス対策ソフトの一括管理機能を有すること。
	（2）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	納入時点で最新のセキュリティパッチを適用すること。
	c)	ウイルス対策ソフトにより毎日スケジュールスキャンおよびパターンファイルが自動更新されるように設定を行うこと。
	d)	ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	e)	バックアップのスケジュール設定を行うこと。
	f)	ＬＧＷＡＮ接続系のＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインに参加を行うこと。
	g)	設定後、フルバックアップを行うこと。
	h)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	i)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。

ウィルス対策サーバ

仕様内容		
	j)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。
	②	クライアント用ウイルス対策ソフトの一括管理機能
	a)	既存サーバと同等の設定を行うこと。
	b)	庁内で稼働中のクライアントについては本システムに移行を行うこと。
	c)	管理対象クライアントの設定変更が必要な場合はシステム導入と合わせてクライアントの変更作業を行うこと。

個人番号利用事務系ファイルサーバ

仕様内容		
1．基本構成		
	（1）	仮想基盤サーバ上で稼働する仮想マシンとして動作させること。
	①	２ＴＢ以上のディスク容量を確保し、設計時に協議の上、容量の割り当てを行うこと。
2．ハードウェア／ソフトウェア要件		
	（1）	ハードウェア要件
	①	以下にファイルサーバシステムのハード要件を記載する
	a)	ＣＰＵ：４コア以上
	b)	メモリ：８ＧＢ以上
	c)	ディスク：物理容量　２ＴＢ以上（システム領域、データ領域）以上
	d)	ＬＡＮ：１ポート以上
	（2）	ソフトウェア要件
	①	以下にファイルサーバシステムのソフトウェア要件を記載する
	a)	ＯＳはＷｉｎｄｏｗｓ　Ｓｅｒｖｅｒ　２０２５　Ｓｔａｎｄａｒｄ　Ｅｄｉｔｉｏｎ以降であること。
	b)	ウイルス対策ソフトウェアを導入すること。
	c)	個人番号利用事務系端末へファイルデータ格納機能を提供すること。
3．システム仕様		
	（1）	機能要件
	①	共通
	a)	管理兼バックアップサーバシステムと連携してデータのバックアップ／リカバリが可能なこと。
	b)	ウイルスリアルタイムスキャン、スケジュールスキャン、ウイルスパターンファイルの自動更新機能を有すること。
	②	ファイルサーバ機能
	a)	ファイルサーバ機能を有すること。
	b)	ＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙと連携可能なこと。
	（2）	設定要件
	①	共通
	a)	機能要件を満たすために必要なすべてのソフトウェアの設定を行うこと。
	b)	納入時点で最新のセキュリティパッチを適用すること。
	c)	ウイルス対策ソフトにより毎日スケジュールスキャンおよびパターンファイルが自動更新されるように設定を行うこと。
	d)	ＮＴＰサーバと正常に時刻同期できるように設定を行うこと。
	e)	個人番号利用事務系のＡｃｔｉｖｅＤｉｒｅｃｔｏｒｙドメインに参加を行うこと。
	f)	設定後、システムイメージのフルバックアップを行うこと。
	g)	現行サーバの設定および環境を調査・整理し、現状を正確に把握した上で、設定パラメータについては当市と協議を行い、決定すること。
	h)	新サーバ導入に伴い、関連する既存システムに対し、新環境との連携に必要な設定変更や調整が発生する場合、当市と協議の上、その変更作業を実施すること。
	i)	現行サーバから移行作業が発生する場合は本市及び現行保守事業者と協議し、必要に応じて作業を現行保守業者に委託すること。その際の委託費用は受託者負担とすること。
	②	ファイルサーバ機能
	a)	既存ファイルサーバ上にあるデータについてはフォルダ構成およびアクセス権を維持した状態で移行を行うこと。
	b)	ストレージ上のデータ格納領域をファイルサーバの共有領域として動作するように設定を行うこと。
	c)	容量制限を行うこと。容量制限については、市担当者と協議の上、決定すること。