奈良県ハードウェア統合基盤再構築・運用業務仕様書

２０１９年8月

奈良県総務部情報システム課

1. はじめに

1.1. 背景と目的

本県では、奈良県第二次情報システム最適化計画に基づき、庁内で利用している業務システムを集約して一元管理するための仮想化基盤であるハードウェア統合基盤を構築し運用を行っていますが、現行の契約期間満了に伴い再構築を行います。

1.2. 履行期間

契　　約	日	～	令和２年	３月	環境構築
令和２年	４月	～	令和３年	２月	移行・調整及び試行運用
令和３年	３月	～	令和８年	２月	運用保守及び機器等使用

1.3. 奈良県ハードウェア統合基盤等の範囲

現行の奈良県システム全体構成図及び更改範囲は別添資料の図１のとおりです。また、新ハードウェア統合基盤の概要図は別添資料の図２のとおりです。

1.3.1. 対象範囲

ハードウェア統合基盤の更改範囲は以下のとおりです。

(1) ハードウェア統合基盤（仮想化基盤、ファイアーウォール、ロードバランサー、統合ストレージ、統合バックアップ、Oracle 利用領域　等）の設計、再構築
(2) Windows 関連サーバー群（Active Directory、DNS、WSUS、VAMT 等）の再構築、Windows Server ライセンス
(3) Windows VDA (Virtual Desktop Access)のライセンス　80 本（令和３年３月～令和８年２月まで利用可能であること）
(4) LGWAN 系ファイルサーバーの再構築及びデータ移行
(5) LGWAN 系グループウェアシステム、統合ＩＤ管理システム、資産管理・ログ管理システムの再構築及びデータ移行
(6) 認証基盤（顔認証等）の構築
(7) 現行仮想化基盤に搭載している各業務システムの移行
(8) 統合運用監視業務
(9) 設置場所選定・ハードウェア仕様設計
(10) データセンター及びデータセンターまでの回線
(11) 上記に係る付帯作業、契約期間中の運用保守、機器等使用及び必要なソフトウェアライセンス

1.4. 納品物

本調達における納品物は次のとおりとする。

No.	カテゴリ	納品物	内容	納入期限
1	プロジェクト管理	プロジェクト計画書 (業務実施計画書)	業務の目的実施体制、実施内容、スケジュール、管理方法等を実施計画としてまとめたもの。	契約締結後、速やかに。
		ＷＢＳ	作業項目の明確化とともに、スケジュール管理、工数の割り出しを行うため、作業項目にスケジュール及び工数を細分化し、記載したもの。 ※プロジェクト計画書提出時及び進捗会議毎に提出すること。	
2	基本設計	基本設計書	各システムの要件を実現するために実装すべき機能や基礎的な事項についてまとめたもの。	契約締結後、速やかに。
		ネットワーク構成図	ネットワーク構成を分かりやすくまとめたもの。物理構成図と論理構成図の２種類。	
		ラック搭載図	機器をラック搭載した場合の図面。	
3	詳細設計	詳細設計書	基本設計書で定められた内容を実現するために、それをどう表現するかを具体的に定めたもので、各機器へ設定するパラメータ等の設定根拠及び設定ルール等技術的な事項をまとめたもの。	令和２年３月31 日（※移行・調整及び試行運用期間中に変更があった場合は、変更したものを令和３年２月 28 日までに提出すること）
		設定書	各機器への設定情報をまとめたもの。	
		機器詳細書	機器ごとの品名、型番、導入時期、ポートの接続状況についてまとめたもの。機器にソフトウェアが導入されている場合は、ソフトウェア名及びバージョンについても記載を行うこと。	
		移行計画書	既存ハードウェア統合基盤の全データを新環境へ移行する計画を定義したもの。	
4	運用設計	操作手順書及び運用手順書	奈良県担当者及び運用管理者用の操作手順書及び運用マニュアルをまとめたもの。	令和３年２月28 日
		障害対応マニュアル	障害時における復旧手順等についてまとめたもの 。	
5	品質管理（運用試験）	テスト計画書	構築したサーバー等の品質を検査するために実施する試験の内容について定義したもの。	令和２年３月31 日（※移行・調整及び試行運用期間中に変更があった場合は、変更したものを令和３年２月 28 日までに提出すること）
		テスト結果報告書	テスト計画書に基づき実施したテストの結果をまとめたもの。	
6	その他	ハードウェアー式	必要な機器（ラックマウントキット及びケーブル等の構築に必要な機器を含む）。	令和２年３月31 日（※移行・調整及び試行運用期間中に変更があった場合は、変更したものを令和３年２月 28 日までに提出すること）
		ソフトウェアー式	必要なソフトウェア及びオペレーティングシステム。	
		ライセンスー式	保証書、ライセンス証書（またはそれに代わる資料）。	
		マニュアルー式	各機器に日本語の操作マニュアル等を添付すること。 (メーカーマニュアルに日本語版が無い場合は独自に作成することも可)	

1.5. 作業要件等

1.5.1. 対象実施体制

⑴プロジェクト体制・メンバー

本調達内容を適切・効率的に履行するためのプロジェクト体制及び本業務を遂行するうえで、必要な人員を提案すること。

なお、本業務を遂行する体制として、以下に示す要件を満たすこと。

⑺プロジェクト責任者

本業務の全責任を負う受託者における作業責任者。プロジェクト計画書を策定し、本業務を円滑に遂行するための各作業工程管理及び関連する業務や利害関係者との調整ができるなど、作業全体を充分に管理可能な知識・経験を有している者。

⑴プロジェクトマネージャ

プロジェクト責任者から指示される作業を確実に履行できる知識・経験を有している者。

⑼プロジェクト品質管理者・セキュリティ管理者

プロジェクト責任者及びプロジェクトマネージャとは別に、プロジェクト品質管理者・セキュリティ管理者を配置すること。

⑵作業体制に関する留意事項

⑺品質保証及び監査の体制を確立すること。

⑴受託者の作業内容及びスケジュール、業務の進捗管理を行いながら円滑に作業を実施できる体制を整備し、体制図とともに各要員の責任や役割分担について提示すること。

⑼作業スケジュールに応じて、要員の増減なども検討すること。作業体制を変更しようとする場合は、事前にその旨を書面により報告するとともに、奈良県の承認を得ること。

⑽受託者が、プロジェクト計画書等で示した業務作業が適正に履行されていない、または、本調達仕様書において定義する各要件を満たしていないと奈良県が判断した場合には、奈良県は、受託者に対して体制の変更を指示することができるものとし、受託者はその指示に従い、適切に対応すること。

1.5.2. 対象実施要件

⑴作業場所

設計、設定準備は受託者所内で実施すること。機器の設置・設定及び各作業に関する打ち合わせや、報告、レビュー及び進捗会議等については、主に奈良県の会議室等で実施すること。

⑵設備及び備品

本業務に使用する設備及び消耗品等については受託者が負担すること。県庁舎内で使用する電気料金等の光熱水費については奈良県の負担とする。

⑶奈良県からの貸与物件

各業務内容の検討に必要な物件・資料の内、返却の必要なもの及び持出禁止条件に該当するものについては、契約書の秘密保持及び個人情報保護事項に従い所定の手続きにより貸与する。

⑷奈良県からの提供物件

本業務に必要な前記の貸与物件・資料以外については、契約書の秘密保持及び個人情報事項に従い所定の手続きにより提供する。

⑸会議体

本業務の実施にあたっては、次の会議体を開催し、議事内容について責任のある回答ができる要員を参加させること。会議の開催にあたっては、受託者側で必要な討議資料を用意すること。

また、各会議体について受託者側で議事録を作成すること。

会議名称	開催頻度	内容
1. 進捗会議	最低月１回以上	本業務の進捗状況確認やスケジュール管理、課題検討及び解決、品質管理及び推進に必要となるワーキンググループ会議間の総合的な調整を行う。
2. 工程完了判定会議	各工程完了時	各工程業務結果報告及び稼動判定を行う会議。

⑹プロジェクト管理要件

受託者は、本業務にかかる作業を主体的に管理・維持すること。受託者は、契約後１０日以内に以下の項目について定めたプロジェクト計画書を提出し、奈良県の承認を受けること。

⑺プロジェクトの背景、方針、目的
⑴対象範囲（スコープ）
⑼成果物
⑽制約条件
⑾体制と役割分担
⑿コミュニケーション（会議体、合意形成プロセス）
⒀進捗管理

タスクの状況把握及びスケジュール管理を行うことを目的とするため、受託者は、進捗管理表を作成し、定期的に作業名、奈良県／受託者の作業区分、責任者、作業の開始日・完了予定日、完了基準、実績値を記入すること。

スケジュール差異、工数差異、スケジュール効果指標、工数効果指標、予測総工数、残工数の指標等を用いて、進捗状況を定量的に分析すること。

各タスクの進捗状況に関して、会議体において報告を行うこと。対象とする作業期間に予定していた全タスクに関する進捗状況の分析結果を報告し、計画から遅れが生じた場合は、要因を調査し、体制の見直しを含む改善策を提示し、奈良県の承認を得た上でこれを実施すること。

⒁課題管理、リスク管理

プロジェクトの中で発生する各種課題について、課題の認識、対応案の検討、解決及び報告のプロセスを明確にすることを目的とするため、課題管理を実施すること。

課題管理にあたり、課題内容、影響、優先度、発生日、担当者、対応状況、対応策、対応結果、解決日を課題一覧にまとめ、一元管理すること。また、その他必要と考えられる項目についても管理すること。

⒂情報セキュリティ管理

各作業工程において、情報セキュリティに関する事故及び障害等の発生を未然に防

ぐこと、並びに、発生した場合に被害を最小限に抑えることを目的とするため、奈良県情報セキュリティポリシーの内容を理解し、遵守すること。

奈良県情報セキュリティポリシーは、契約締結後、受託者が奈良県に守秘義務の誓約書を提出した後に開示するものとする。情報セキュリティ対策の実施状況については、定期的に内部監査を実施し、県側に報告すること。

情報セキュリティ対策の内容については、各作業工程の状況に応じて適宜改善策を検討し、県側の承認を得ること。

情報セキュリティに関する事故及び障害等が発生した場合には、速やかに県側に報告し、対応策について協議すること。

㈡文書管理

会議･打ち合わせにおける議事録等の作成、保管、管理を行なうこと。

2. 前提条件

2.1. 現行ハードウェア統合基盤

現行ハードウェア統合基盤の構成図は、別添資料の図３のとおりです。
奈良県が保有し、利用可能なライセンスは表１のとおりです。

表１　奈良県保有ライセンス一覧

項　目	品　名	ライセンス数	形　態	期　限
1.グループウェア関係	m-FILTER MailFilter	7,000	使用許諾	～2022.2.28
	m - FILTER FILE SCAN	1	使用許諾	～2022.2.28
2.資産管理ソフト	SKYSEA Government License Light Edition シンクライアントライセンス	4,500	使用許諾	～2022.2.28
3.認証ツール	EVE MA サーバライセンス	1		
	EVE MA クライアントライセンス	5,000		
4.Windows Server デバイス CAL	Windows Server 2019 デバイス CAL	5,500		

2.2. 現状の認証の流れ

現状の認証の流れは、別添資料の図４のとおりです。

2.3. 電子計算機室

情報管理棟２階（但し、出入口は地下１階。エレベータあり。フリーアクセス。）
①ラック設備：　１９インチラック（免震機構付き）３ラックまでの設置が可能。
既存ラックを利用する場合は、４２U まで利用可能（ただし、電源工事は必要）
②床面耐荷重：　床積載荷重　W=0.5t/㎡　水平入力 0.5G
③空調設備　：　24 時間 365 日　温度設定 22℃　夜間・休日　28℃以上で空調動作保証運転
④電　源　　：　単相 100V、200V
※電源工事、LAN 配線工事等が発生する場合は、本調達の範囲に含めること

2.4. 利用予定ネットワーク

2.4.1. 全庁統合ネットワーク

ネットワークの概要及び接続箇所・帯域については、以下のとおりです。
①本庁舎
帯域：大和路情報ハイウェイ（大安寺ＡＰ）と県庁舎（情報管理棟）間は１Gbps（帯域確保）
庁舎内は 100Mbps（ベストエフォート）

②出先機関
接続箇所数：１３９拠点
帯域：大和路情報ハイウェイのアクセスポイントと出先機関建物間は
10/30/100Mbps（帯域確保）

2.4.2. 大和路情報ハイウェイ

全庁統合ネットワークにおいて、本庁舎と各出先機関の各ＬＡＮを接続するＷＡＮ

2.5. 職員が利用するパソコン

現行、庁内の職員に配備しているパソコン（共通端末）の仕様は、表２のとおりです。

表２　職員配備パソコンの仕様

項目	仕様
CPU	Celeron3850U 1.80GHz Core i 3-6100U 2.30GHz
内蔵ディスク	SSD　128GB
メモリ	4GB
解像度	WXGA 1280×768
ＯＳ	Windows10
Internet Explorer	Ver.11
一太郎	Pro4
Word	Ver.2013、2016
Excel	Ver.2013、2016
Access	Ver.2013、2016
Power Point	Ver.2013、2016
Adobe Reader	Adobe Acrobat DC
Lhaplus	Ver.1.73
Media Player	Ver.12.0

(1) ActiveX コントロールや Java アプレット等に関しては、特に制限を設けていないが、県が指定する配信ソフトウェア(SKYSEA)により自動配信が可能なこととし、使用に当たっては事前に本県の承認を得ること
(2) 利用する職員には、ドメイン（Active Directory）上のユーザー権限（制限ユーザ）しか保有していない。その場合にも、問題なくシステムが利用可能であること
(3) OS や Web ブラウザのバージョンアップにも対応可能であること
(4) 各職員に１台配備しているパソコンは、ＬＧＷＡＮ系ネットワークに接続されている
(5) ファイルサーバー、メールシステムなどを利用する職員は約 6,000 人とする
(6) 管理対象パソコンは、共通端末及び各所属が共通端末と同一仕様で調達した端末とし、約 6,000 台とする

3. システム要件（製品機能で達成できない場合は、運用で代替すること）

3.1. 全体要件

項番	要　件	必須項目
1	仮想化によるシステム全体の集約化を図り、ハードウェア統合基盤を構築すること	○
2	仮想化基盤、統合ストレージ、統合バックアップ、運用監視機能等、本調達仕様による構築、運用管理、移行に必要となるすべてのソフトウェアを導入すること	○
3	ハードウェア統合基盤は、奈良県庁及び奈良県各出先機関から大和路情報ハイウェイ（又は、大和路情報ハイウェイ、統合ネットワークと直接接続された専用回線）を経由して利用すること	○
4	ハードウェア統合基盤は、県民への情報提供、地方自治体及び中央省庁との情報連携の為、ファイアーウォール等を介して、インターネット回線及びLGWANと接続すること	○
5	異なるアドレス体系を有する複数の組織、部署による共有利用を想定しているため、論理的にネットワークを分割及び統合する機能を有する機器及びシステムを採用すること	○
6	機器構成は、物理的にシンプルな構成とすること	○
7	県庁内で利用されている各種システムが稼働する為、設定等により柔軟な利用が可能なシステムを採用すること	○
8	同じデータセンター内に設置する機器のネットワークは、各機器間を10Gbps以上の帯域で接続すること	○
9	庁内システムの構成を考慮し、柔軟なネットワーク構成を設定可能とすること	○
10	ハードウェア統合基盤は、「ハウジング型」、「クラウドサービス型」のいずれの提供形態かを明確にすること	○
11	導入するソフトウェア間の組み合わせ及びハードウェアとの組み合わせを事前検証し、障害・不具合が発生しないようにすること	○
12	導入時のソフトウェアのバージョンは基本的に最新版とし、最新のアップデートプログラム及びパッチが適用済であること。これ以外のバージョンを導入する場合は、事前に奈良県と協議を行い、承認を得ること	○
13	ソフトウェアのパッチ及び最新アップデートプログラムが契約期間中入手可能であること。契約期間中にサポートが終了する場合は、受託者負担で必要な措置を講じること	○
14	ライセンスは奈良県名義で調達し、調達したライセンス(ソフトウェアアシュアランス、サブスクリプション、保守サポートを含む)の更新に関する情報を契約終了後、協議の上奈良県に引き継ぐこと（クラウドサービス型を提案する場合でライセンスが県に帰属しないものは除く）	○
15	ストレージ装置は、ディスクドライブ、コントローラ、電源、冷却ファンなどの主要コンポーネントが冗長化されており、且つ、障害時にサービスに影響なく保守が可能であること（バックアップストレージを除く）	○
16	ディスクドライブが故障した場合でもRAID技術等によりデータ・アクセスを継続して行うことができ、データ冗長性の自動復旧が可能であること	○
17	ハードディスクの自動エラーチェック機能により、ハードウェア障害を事前に検知する機能を有し、ハードディスク破損前に正常なハードディスク（スペアディスク）へデータ移行が可能であること	○
18	ボリューム内のデータ使用率が増大した際に、業務を中断すること無く必要に応じてボリュームの拡大が行えること（バックアップストレージを除く）	○
19	サービス継続性の観点から、ハードウェアの自己診断機能を持ち、異常が検知された場合には自動的に障害を通知する機能を有すること	○
20	本調達で導入するグループウェア、ファイルサーバー及び今後統合基盤へ移行される大規模システム等については、ロードバランサー等により、利用する際にストレスのないレスポンスを実現すること	○
21	庁内システム導入業者等が、ハードウェア統合基盤上にシステムを導入できるよう、必要な環境等を提供すること	○
22	計画保守の実施については、事前に県への報告を行い、システム運用上の提供を考慮し、適切な計画の下に保守作業を実施すること	○
23	本調達により発生する電源工事、LAN配線工事は本調達の範囲に含めること	○
24	奈良県庁舎の電子計算機室に機器を設置する場合は「2.3. 電子計算機室」の要件に従うこと	○

3.2. 仮想化基盤要件

3.2.1. 仮想化基盤要件

仮想化基盤のネットワークは、マイナンバー系ネットワークの仮想化基盤、LGWAN 系ネットワークの仮想化基盤及びインターネットに接続されている仮想化基盤の３つに分かれる。インターネットに接続されている仮想化基盤は、直接、インターネットに接続するもので、インターネット回線も調達に含むものとする。

項番	要　件	必須項目
1	仮想化基盤システムは、物理サーバー上に仮想化ソフトウェアを配置し、その上で仮想マシンを稼働させること（仮想マシンは、庁内システム用のアプリケーション、ミドルウェアをインストールしてシステムを利用）	○
2	仮想化基盤は、ハイパーバイザー型のソフトウェア構成であること	○
3	仮想マシンは、マイナンバー系、LGWAN 系、インターネット系に論理分割を行うこと	○
4	仮想化基盤用ストレージのディスクは、SSD 又は SAS と同等以上の性能を有すること。なお、仮想化基盤用ストレージの構成は、外部ストレージ構成、もしくは仮想化ソフトウェアのストレージ仮想化機能により物理サーバーの内蔵ディスクでストレージを提供する構成とすること	○
5	仮想化基盤を構成する機器は、ノード（コントローラ等）を追加することで、必要容量と処理能力の拡張が可能であること	○
6	仮想化基盤の帯域制御の仕組みについて提案すること	○
7	予備のリソースを確保し、サーバーの障害に対応できる構成とすること	○
8	物理サーバーに障害が発生した場合でも、少ないダウンタイムで仮想マシンの再起動を行い、システムの運用を継続する機能を有すること	○
9	サービスを停止させることなく物理サーバー間の移動が可能であること	○
10	仮想マシンは、無停止かつ自動的に他の物理サーバーへ移動可能な構成とすること（無停止とは、業務に支障が生じない程度の停止をいう）	○
11	ストレージ使用量と I/O 負荷状況を監視し、仮想サーバーを構成するファイルの初期配置・再配置を、仮想サーバーを稼働させたまま自動的に行えること	○
12	仮想ネットワーク属性毎のネットワーク I/O を制御する機能を有すること	
13	物理サーバーは複数台で構成し、冗長化を行うこと	○
14	複数物理サーバー上に構成される仮想環境用論理スイッチを一元的に管理できる機能を有すること	○
15	仮想化ソフトウェアを実行している複数の物理サーバー間において共通の仮想スイッチを利用可能であること	○
16	ハードウェア統合基盤を構築する上で、現在奈良県が保有するサーバライセンス、クライアントライセンス以外のライセンスが必要となる場合は、必要数を用意すること	○
17	V2V、P2V での移行受入が可能であること	○
18	仮想マシンは、Microsoft Windows 系 OS、LINUX 系 OS に対応していること	○
19	仮想マシンの展開には、マスターイメージからの展開が可能であること	○
20	プリンタリダイレクト、USB デバイスリダイレクト、カードリーダーリダイレクトに対応していること	○
21	画面転送プロトコルは、ネットワーク帯域に応じて画質の調整、補完機能を有し、狭帯域、広帯域に応じたチューニングが可能であること	○
22	画面転送プロトコルは一般的に解読不可能とされる暗号化強度(AES 128bit 以上等)での通信が可能であること	○
23	仮想ソフトウェアのファイアーウォール機能により、同一セグメント内の仮想マシン間の通信制御が可能な構成とすること	
24	仮想マシンに対し、バックアップ・リストアが可能であること	○
25	１週間に１回以上、仮想マシンのイメージバックアップの保存を行うこと	○
26	仮想化基盤移行対象システム及び仮想化基盤へ搭載しているシステムの更改時は、ハードウェア統合基盤の最新仕様を提示し、庁内システムベンダーへ説明を行うこと	○

27	開発・検証用の仮想マシンを構築、利用、廃止できること	○
28	開発・検証用仮想マシンは、本運用仮想マシンとは独立して構築、利用、廃止できるものとし、仮想マシンや OS 上の設定、OS 上での本運用仮想マシンに影響を与えにくい構成であること	○
29	開発・検証用仮想マシンを利用する各システム管理者に対し、ハードウェア統合基盤の提供者としての支援を行うこと	○
30	仮想化基盤への移行及び庁内システム更改作業（支援）については、庁内システムの更改時に合わせて、受託者が契約の範囲内で計画的に行うこと	○
31	庁内システム導入業者に対し、仮想マシンの Administrator 権限（ローカル、ドメイン）と仮想マシンの状態監視が行えるよう権限を付与できること	○
32	庁内システム導入業者が、他の事業者のシステムの状態を確認・アクセスができないようにすること	○
33	受託者及び県の管理担当者は、全ての仮想マシンへのアクセス権を有すること	○
34	庁内システムの移行・更改のために必要となるネットワーク環境整備等を行う場合、受託者は必要な情報の提供のほか、他事業者と協力し、作業にあたること	○

3.2.2. 仮想サーバー要件

項番	要　件	必須項目
1	別添表１に示す仮想サーバーのうち、個別システム欄に「○」のあるものはすべて移行対象とし、リソースを確保すること（Oracle 搭載サーバーについては、別途要件を示す）	○
2	別添表１に示す仮想サーバーのうち、「新世紀統合財務システム」「奈良県土木事務管理システム」については、契約期間中に更新するため、移行方法については、奈良県の指示に従うこと	○
3	項番１とは別に、運用期間中（５年合計）、vCPU：100 コア、メモリ：500GB、ディスク：5TB の増加を見込むこと	○
4	項番１、項番３及び増加する仮想マシンとは別に、開発・検証用仮想マシンに必要なリソース（vCPU：30 コア、メモリ：100GB、ディスク：1TB）を見込むこと	○
5	別添表１に示す仮想サーバー及び今後５年間に搭載するサーバーの Windows Server OS（Windows Server 2019 以前のバージョンに対応）のライセンスを本調達に含めること	○
6	仮想環境上のゲスト OS の Windows Server OS ライセンスは、政府機関向け Windows Server 2019 Datacenter エディション（政府機関向け）又は SPLA（Microsoft Services Provider License Agreement）とすること	○
7	個別システム用アプリケーション、ミドルウェアをインストールし、利用することが可能であること	○

3.2.3. VDI 要件

項番	要　件	必須項目
1	VDI へは、職員一人１台パソコンを介して利用できるものとすること	○
2	別添表１の VDI 欄に「○」のあるものはすべて移行対象とすること	○
3	契約期間中の MicrosoftVDA　ライセンス　80 セットを本調達に含めること（インターネット環境で利用しているライセンスを含む）	○
4	契約期間中に追加する VDI（23 セット）については、１台あたり、vCPU：２コア、メモリ：4GB、ディスク：100GB を見込むこと	○
5	帳票印刷に対し、アプリケーションを利用する端末に設定されているプリンタドライバの設定ができること	○
6	VDI を構成する管理サーバーや仮想デスクトップは仮想化基盤上に構築すること	○
7	Active Directory との認証連携により接続制御が可能であること	○
8	仮想デスクトップを利用者の所属部門や業務に応じてグループ単位で管理、展開が可能であること	○
9	一人のユーザーに対して複数のデスクトップ環境を割り当てることが可能であること	○
10	マルチモニタ環境での利用が可能であること	○

3.2.4. ファイアーウォール要件

項番	要　件	必須項目
1	データセンター、県庁等、各拠点間にはファイアーウォールを設置し、制御を行うこと	○
2	ファイアーウォールは論理分割が可能であること	○
3	奈良県の電子計算機室に設置するファイアーウォールはラックに設置すること（ラックマウント型とすること）	○
4	冗長構成とすること	○
5	LAN 配線工事を実施すること（必要な部材については本調達に含めること）	○

3.2.5. ロードバランサー要件

項番	要　件	必須項目
1	仮想ロードバランサー、物理ロードバランサーのどちらでも可とする	○
2	冗長構成とすること	○
3	ロードバランスは以下の機能を有すること 項　目 / 内　容 対応プロトコル / TCP/UDP HTTP、HTTPS ロードバランス方法 / ラウンドロビン Source IP Address Hushing Least Connections 健全性チェック / TCP/UDP/ICMP HTTP（GET,OPTION,POST） HTTPS（GET,OPTION,POST） パーシステンス / Source IP cookie SSL session ID	○
4	ロードバランサーで CSR の生成が可能であること	○
5	ロードバランサーに SSL 証明書のインストールが可能であること	○
6	契約期間中にロードバランサーの設定変更、追加は本調達の範囲に含めること	○

3.2.6. Oracle DB を利用するサーバーに関する要件

項番	要　件	必須項目
1	Oracle DB の対象サーバーは、別添表１「各 IDC に設置している仮想サーバー」において Oracle 欄に「○」が記載されているものとすること	○
2	現行の仮想サーバーから Oracle DB サーバーに移行する方法について提案すること	○
3	Oracle DB 利用サーバーは、仮想サーバー又は物理サーバーで提供を行うこと（冗長化を含めたサーバー構成について提案すること）	○
4	仮想化基盤上で Oracle DB を利用する場合は、オラクル社が認めた方式での提供を行うこと	○
5	仮想化基盤で Oracle DB を提供する場合は、対象サーバー全体の 20％の余剰リソースを見込むこと	○
6	物理サーバーで Oracle DB を提供する場合は、対象サーバーそれぞれ冗長構成とすること。また、各サーバーで 20％の余剰リソースを見込むこと。なお、新世紀統合財務システムについては別添表２に示す仕様を満たすこと	○
7	対象サーバーの契約期間中の Oracle DB ライセンス及び期間中の保守費用を本調達に含めること（現行のエディションは「Oracle Database Standard Edition One」を使用している）	○
8	物理サーバーで Oracle DB を提供する場合は、予備機として CPU４コア、メモリ８GB、ディスク 500GB のサーバーを２台用意すること。	○

3.3. ファイルサーバー要件

項番	要　件	必須項目
1	ファイルサーバー用ストレージのディスクは、SATA と同等以上の性能を有すること	○
2	ディスク容量は RAID5 相当以上の保護レベル構成で、75TB 以上の実効容量を提供すること（重複排除機能、圧縮機能等を有効化した状態での容量）。なお、重複排除機能、圧縮機能等を無効化にした状態で 50TB 以上の実効容量を備えること	○
3	全庁受渡フォルダ、部局共有フォルダ、所属共有フォルダ、個人フォルダを作成し、利用できること	○
4	重複排除機能、圧縮機能を有すること	○
5	ストレージ装置は、無停止で重複排除、圧縮等の設定変更が可能であること	○
6	ログデータを保存すること	○
7	保存したログデータを外部記録媒体に定期的にアーカイブし保存すること	○
8	Active Directory や ID 管理システムと連携し、フォルダ等へのアクセス権の設定を行うこと（Active Directory を変更後、即時反映を行うこと）	○
9	第一階層のフォルダ単位で容量制限ができるクォーター機能を有し、容易にクォーター管理できること	○
10	クォーター管理については第一階層のフォルダごとの使用量、使用量の推移等の利用状況を管理できること	○
11	スナップショット（シャドウコピー）機能等によるバックアップを１日２回、１４世代以上保存し、容易に復旧できること	○
12	SMB、NFS プロトコルでアクセス可能なこと	○
13	コントローラは冗長化されており、故障時にも業務が継続可能であり、性能低下は通常稼働時の 30%程度とし業務に支障がでないこと	○
14	ディスク、電源や単一のコントローラの障害によるデータへのアクセスが損なわれないこと	○
15	システムを停止することなく交換対応（電源、ディスク交換、単一コントローラ）が可能なこと	○
16	OS をアップデートする際、サービス無停止であること	○
17	OS アップグレード後に一定期間内の不測の事態に備え、データを保持したままロールバックが可能なこと	○
18	管理対象のユーザー、グループ数は、それぞれ 10,000 程度とする	○
19	OS は汎用的な OS を使わずにファイルサービスに特化した専用 OS であること	

3.4. 統合バックアップ要件

項番	要　件	必須項目
1	大規模災害等を考慮し、県内外データセンター等のバックアップ拠点へデータの保存が可能なバックアップ機能を考慮すること	○
2	バックアップの対象は、仮想化基盤（物理サーバーで Oracle DB を提供する場合の Oracle DB を含む。）、ファイルサーバーとする	○
3	メインサイトとバックアップサイトは別のデータセンターとすること。なお、「2.3.電子計算機室」で示す奈良県庁舎の電気計算機室をバックアップサイトとすることも可とする。その際、ラックの増設等が必要な場合は本調達の範囲に含めること	○
4	バックアップデータを収容するディスクは SATA と同等以上の機能を有すること	○
5	仮想化基盤用ストレージ及びファイルサーバー用ストレージのフルバックアップが 1 世代以上保存可能な容量を用意すること	○
6	ファイルサーバーのフルバックアップ（過去のフルバックアップと差分バックアップを合成し、最新のフルバックアップを生成でも可）を１日に１回以上行うこととし、業務に支障をきたさな	○

	いこと	
7	各仮想サーバーのイメージバックアップは、メインサイト及びバックアップサイトに保存すること	○
8	仮想サーバーに搭載している各庁内システムのバックアップデータが保存でき、CIFS、NFS でアクセスできる領域（庁内システムごとにアクセス権を設定すること）を 10TB 以上用意すること	○
9	バックアップ用ストレージは冗長化を行うこと	○
10	バックアップシステムによる方式においては、仮想マシン及びデータの保護を目的とし、「仮想マシンのシステム障害の復旧」及び「データ損失時の復旧」等の対応が可能であること	○
11	ハードウェア統合基盤搭載システム以外の庁内システムのバックアップデータの保存が可能であること（アクセス権の設定も可能であること）	○
12	メインサイトに障害が発生した場合、バックアップサイトからサービスを継続できること。その際、Active Directory による認証等、必要な機能を継続利用できること	○
13	バックアップサイトへ保存されたバックアップデータからメインサイトでのリストア及びバックアップサイトでのリストアが可能な環境を整備すること	○
14	リストアについては、一括バックアップからのリストア、個別バックアップから、仮想サーバー単位・フォルダ単位・ファイル単位でのリストア又はデータ抽出、スナップショットからのリストアいずれにも対応すること	○
15	庁内利用システムからハードウェア統合基盤（プライマリ拠点）のバックアップ領域へのバックアップ用データ格納、バックアップ領域内でのバックアップデータ生成及び遠隔バックアップ拠点へのバックアップデータ格納完了までの一連の作業を１日１回以上行えること	○
16	RPO(目標復旧地点)は、24 時間以内とすること	○
17	仮想マシンの RTO(目標復旧時間)は、24 時間以内とすること	○
18	メインのファイルサーバーに障害が発生した場合は、２時間以内に復旧またはバックアップサーバー（メインサイトに設置のバックアップサーバーも可）へ切り替えて業務継続できる環境とすること。その際、バップアップサーバー内のデータは、障害発生前のメインのファイルサーバー内のデータと同一であること。また、メインのファイルサーバー復旧後にバックアップサーバーで更新したファイルを同期すること	○
19	仮想サーバーをリストアするのに必要なリソース（vCPU：50 コア、メモリ：110GB、ディスク：5TB）を見込むこと	○
20	バックアップの方法、リストアの方法、災害等大規模障害発生時の運用方法について提案すること	○
21	スケジュール設定による定期バックアップができること	○
22	ファイルサーバーのバックアップについては、ファイル単位で復元することができること	○
23	バックアップ領域は、マイナンバー系、LGWAN 系、インターネット系に論理分割を行うこと	○

3.5. 認証基盤要件

項番	要　件	必須項目
1	顔認証＋ＰＩＮコードの二要素の認証により、ドメインユーザー（行政ネット）にて Windows へのログオンが自動でできること	○
2	顔認証＋ＰＩＮコードでログオンできない場合は、手動でのＩＤ、緊急パスワード＋ＰＩＮコードでログオン可能なこと	○
3	パソコン操作中に画面ロックがかからないこと	○
4	オフライン状態でも一定期間クライアントの認証が行える機能を有すること（一定期間キャッシュを保持できること）	○
5	Windows ログオンなしで、他のユーザーによる強制サインアウト、シャットダウンができること	○
6	顔情報をユーザーで撮影し、個別に登録ができること	○
7	CSV ファイル等により、ユーザー情報の一括登録ができること	○
8	6,000 ユーザーが利用できる環境を構築すること（必要なライセンスはすべて本調達に含めること）	○

9	利用したユーザーのログを取得できること	○
10	庁内のシステムへのシングルサインオン機能（代行入力可）を有すること	○
11	シングルサインオンは Web システム、Windows ベーシック認証、VMware Horizon View（パスワード変更画面を含む）に対応していること	○
12	シングルサインオン機能は、別途調達している財務会計システム、総務事務システム、土木事務管理システム、ファイル転送システムなどの Web システムに対応すること	○
13	シングルサインオン対象システムのパスワード変更は、本調達の認証基盤からのパスワード変更のみで各業務システムと連携し変更を行うこと	○
14	職員に配備しているパソコンを令和３年度に閉域接続専用 SIM での庁内ネットワーク接続に対応させる予定である。以下の項目に対応すること ①管理者が許可したパソコンのみ庁内ネットワークへ接続できるよう制限する機能を有すること（現行のモバイルパソコンでは顔認証サーバーが動的にファイアーウォールと連携し、認証に成功したユーザーの PC の経路を開放し、認証に伴う認可によるアクセス制御を実現している） ②①について、現行の仕組みに影響を与えないこと	
15	顔認証による Windows ログオンは令和２年７月から試行運用を行い、令和３年３月から全台の運用を行うこと	○
16	視覚障害者等、顔認証ができない職員が別の二要素認証で対応できる環境を 100 ユーザー分本調達に含めること	○
17	顔認証において、写真で認証できないような仕組みを有すること	
18	現在運用中のソフトウェア EVE MA（DDS 社製）と異なるソフトウェアを導入する場合には、共通端末に導入されているクライアントソフトのアンインストール及び新認証ソフトのインストール（必要な場合）等の作業を行うこと	○

3.6. 資産管理・ログ管理機能要件

項番	要　件	必須項目
1	各クライアントコンピューターから資産情報をスケジュール設定に応じて定期的に自動的に収集し一覧で表示できること	○
2	メモリ増設等資産情報が変化した際には管理者にメール通知ができること	
3	変更された資産内容を指定して検索・表示できること	
4	クライアントコンピューターに関する各種インベントリ情報を自動で資産情報として収集する機能を有すること	○
5	検索条件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で検索が可能であること	○
6	クライアントコンピューター上のソフトウェアに関するインストール状況を収集する機能を有すること	○
7	クライアントコンピューターごとにアプリケーション状況を把握できること	○
8	クライアントコンピューターにインストールされている実行ファイルをクライアントコンピューターごとに一覧化する機能を有すること	○
9	特定のファイル名に含まれるキーワードを指定すると、自動で検索が行われ、発見されたファイルに関する情報が一覧形式で確認できること	○
10	発見されたクライアントコンピューター上にポップアップ形式で通知及び管理者にメールで通知できる機能を有すること	○
11	クライアントコンピューターにインストールするソフトウェアのライセンス番号管理機能を有すること	○
12	指定したクライアントコンピューターに対して、任意のプログラムを配布し、自動的にプログラムの実行を行う機能を有すること	○
13	端末側では全く操作をする必要がないインストール（いわゆるサイレントインストール）機能を有すること	○
14	ソフトウェアの配布期間と対象端末を設定し、配布したソフトウェアのインストール状況を確認することができること	○
15	ソフトウェア配布時にネットワーク、サーバー、端末に負荷のかからない設計がされていること	○
16	プログラム配信時、また修正プログラムを配布するにあたって、メーカーから配布されたファイルに管理者が手を加えることなく配布、適用することが可能であること	○

17	ユーザーが利用中であっても、管理者権限でアプリケーションのインストールができること	○
18	ファイル転送において、何らかの理由により、クライアントとの通信が切断しても再接続時にファイルの再転送ができること	○
19	更新プログラムの配布に必要となるターゲット、スケジュール、通知などの設定をひな形として保存し、定期的に発生する更新プログラムの適用作業の負担を軽減することや、人為的な操作により発生する誤設定のリスクなどを回避することに活用可能なこと	○
20	Administrator 権限でログインしていない端末であってもプログラム配布が出来るよう、管理機からプッシュ、およびクライアントコンピューターからのプルによる配布方法を選択可能なこと	○
21	端末及びユーザーのグループ管理機能を有すること（グループは３階層以上設定可能であること）	
22	運用管理に利用するグループとは別に、任意指定端末や、検索した資産情報リストをグループとして登録でき、そのグループに対してソフトウェア配布やファイル配布等の各種操作が可能なこと	
23	クライアントコンピューターに対して、Windows 更新プログラムやセキュリティパッチを適用する際、WSUS（Microsoft Windows Server Update Services）等のサービスと連携し、更新日や更新時間を設定して自動的に適用できること。クライアントコンピューターが電源 OFF を制御できる環境下にある場合、適用時に電源 OFF が自動で行える設定ができること	○
24	USB メモリ及び USB 外部ストレージをクライアントコンピューターもしくは管理者のクライアントコンピューターに挿入した際、利用した USB メモリ等のメーカー名、シリアルナンバー、ベンダーID を自動で収集し、管理台帳を作成できること（利用者や所属部署、管理番号などを任意で入力できること）	○
25	収集した USB デバイスの情報をもとに指定した USB メモリの使用許可/不許可を設定できること	○
26	USB デバイス及びその他の外部記録媒体（SD カード、DVD 等）について、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/読み取り専用の設定ができること	○
27	クライアントコンピューターに対して行われた操作、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、USB メモリなどの記憶媒体を利用した内容等を記録し、表示する機能を有すること	○
28	ログをユーザー名、操作種別、日付等によりソートして表示でき、CSV 形式等のファイルに出力可能なこと	○
29	収集されたファイル操作ログから、一つのファイルに対して、行われた操作（コピー・ファイル名変更、新規作成、削除など）を抽出して表示する機能を有すること	○
30	バックアップとしてアーカイブし保存されたログについては、閲覧する際にリストアすることなく、通常のログ検索と同様に管理コンソールから直接検索し、閲覧することが可能であること	○
31	クライアントコンピューター上でアプリケーションソフトウェアから印刷が実行された際に、その印刷されたドキュメント名を記録する機能を有すること	○
32	特定のクライアントコンピューターに対して、ネットワーク経由で、リモート操作が行える機能を有すること	○
33	遠隔からの操作を受けるクライアントコンピューターの画面を、管理者画面で拡大・縮小、全画面表示を行うことができ、管理機画面をクライアントコンピューター側に表示させる機能を有すること	
34	リモート操作時に、操作機側とクライアントコンピューター間でファイルの転送ができる機能を有すること	○
35	リモート操作時に、操作機側とクライアントコンピューター間でテキストデータや画像データをコピー＆ペーストできる機能を有すること	○
36	リモート操作時に、画面表示の減色等を行うことで、データ転送量を軽減する設定ができること	○
37	各クライアントコンピューターに対して、特定のアプリケーション起動などを禁止できること	○
38	クライアントコンピューター上で Microsoft Internet Explorer を使って Web の閲覧やダウンロード、ファイルアップロード等について、ログとして記録する機能を有すること	○
39	収集したログに基づいて、事前定義されたルールに反した操作が行われた際に、管理者に通知する機能を有すること	○
40	事前定義されたルールに反した操作が行われた際に、その操作を行った利用者のクライアントコンピューターのデスクトップ上にリアルタイムで、ポップアップ形式による通知ができること	○
41	端末操作（USB の利用可否、ログ収集機能、ファイル操作制御など）に関する設定については、グループ、端末単位の設定のほかにログオンユーザごとのポリシー設定が可能であること	
42	管理用ソフトウェアを複数のパソコンにインストール可能であること	○
43	現在運用中のソフトウェア SKYSEA Client View（SKY 社製）と異なるソフトウェアを導入する場合には、共通端末に導入されているクライアントソフトのアンインストール及び新運用管理ソフトのインストール（必要な場合）等の作業を行うこと	○

44	ポップアップ形式でユーザーに情報配信ができること	○
45	保守契約期間中については、ソフトウェアの最新版のプログラム提供を無償で行うこと	○
46	管理用ソフトウェアをインストールした端末の管理台帳をグループごとに作成できること	○
47	ウィルス対策ソフトと連動または管理者が手動で操作することでウィルス感染した端末を資産管理サーバー等特定のサーバーとのみ通信できる状態へ通信制御できること	
48	クライアントソフトは契約期間中、仮想化基盤でも利用できるライセンス 5,500 本を本調達に含めること	○
49	契約期間中、業務システムのソフトウェア情報、システム情報を取得できるツール 500 ライセンスを本調達に含めること（ツールはサーバーにインストールしているアプリケーションに影響を与えないこと）	○

3.7. グループウェア要件

項番	要　件		必須項目
1	認証機能	ユーザーＩＤ、パスワードによる認証が可能であること	○
2		ユーザーＩＤ毎のアクセス制御が可能であること	○
3		7,000 ライセンス利用可能なこと	○
4		パスワードの有効期限を設定できること（有効期限を設定した場合は、有効期限が切れる前、もしくは切れた時にパスワードの再設定が可能であること） 本機能は Active Directory 側で連携できるのであればそちらで満たすことも可とする	○
5		ユーザー管理情報及びグループ管理情報をエクセル又はＣＳＶ等によって一括登録や一部変更（差分登録）できること	○
6		ユーザー管理情報を一括登録や一部変更するための仕組み（マクロ・ツール等）の構築、操作マニュアルを作成し、県担当者に対し導入後も操作支援を行うこと	○
7		小規模な人事異動時にはユーザー、グループ、所属管理がＧＵＩ上から容易にメンテナンスできること	○
8		管理者はグループウェアの各機能を個別に休止設定できること（スケジュール、施設予約等）	○
9		長期不在等のユーザーを下記のとおり休止設定できること	
		①ユーザー本人がログインできないこと	○
		②他ユーザーにより検索ができないこと	○
		③不在通知が自動送信できること	
10	アドレス帳機能	全庁／個人のアドレス帳を以下の通り管理できること ①全庁アドレス帳は、階層構造で所属／役職順に表示できること ②アドレス帳に役職名を表示できること ③アドレス帳内の職員を検索できること	
11		全ユーザーはユーザーの個人アドレス帳を管理（作成／修正／削除）でき、他のユーザーからは閲覧できないこと	○
12		アドレス帳はグループウェア利用者以外のユーザー情報についても登録が行えること	○
13		ユーザーが、アドレス帳のデータをＣＳＶ形式等でインポート／エクスポートできること	○
14	キャビネット機能	フォルダ単位に、個人、グループ、所属単位で「フォルダ登録／更新権、文書登録／更新権、フォルダ内容参照権」が設定できること	○
15		文書を登録する際、登録日の情報も併せて登録できること	○
16		文書更新時に排他制御ができること	○
17		フォルダは階層（ツリー）及びカテゴリ別に表示されること	
18		掲示期間を設定できること	○
19		登録されている文書を、表題や内容についてフォルダを横断して全文検索できること	
20		新着情報を表示できること	○

21		使用頻度が高いフォルダのショートカット（お気に入り）を、ユーザー毎に登録できること	○
22		文書、及びフォルダをドラッグ&ドロップ操作で移動できること	○
23		関連する文書を「関連文書」として設定でき、関連文書同士は自動的に相互リンクされ、文書の閲覧画面から互いの文書を参照できること	○
24		保存容量は、全体で 12GB 以上であること	○
25		保存容量は、以下のとおり設定を行うこと 各課別情報共有エリア：１スレッド 5MB まで、全スレッド 10GB 訃報情報エリア：１スレッド 5MB まで、全スレッド 200MB 要綱共有エリア：１スレッド 5MB まで、全スレッド 1GB	
26	掲示板機能	登録・参照権限のない利用者には掲示板が表示されないこと	○
27		利用者は登録した投稿を削除できること	○
28		投稿件名一覧画面に表示する件名が多数ある場合には、ページ分割されること	○
29		件名一覧及びその内容を印刷できること（添付ファイルを除く）	○
30		投稿文にあるメールアドレスやＵＲＬはハイパーリンク表示すること	○
31		投稿件名一覧表示時に、投稿者、投稿日、件名等表示されている項目で、昇順、降順に表示を変えられること	○
32		掲示板ごとに開始日、終了日を入力することで掲示期間の設定が可能であること	○
33		掲示期限の過ぎた掲示板は自動的に削除されること	○
34		未読の掲示板記事については識別できること	○
35		掲示板に登録する際、登録者名に加えて所属名を表示できること	○
36		掲示板に投稿があった場合は、対象ユーザーへ通知する機能を有すること	○
37		管理者は投稿文の削除ができること	○
38		管理者は、掲示板ごとに、掲示情報を登録・更新、閲覧できる個人及びグループをそれぞれ設定できること	○
39		管理者は、カテゴリ、サブカテゴリに対してアクセス権（参照のみ、登録可能、削除可能など）設定できること	○
40		管理者は、掲示板毎に管理者権限を委譲できること	○
41		掲示作成時に定期的に内容を自動保存でき、作成中に編集画面を閉じてしまった場合でも、次に掲示作成画面を開いた際に、編集中だった内容を回復できること	○
42		掲示作成時に、画像ファイルをグループウェアにアップロードして、本文に画像を掲載できること	○
43		保存容量は、全スレッドで 10GB 以上とすること	○
44	Web メールシステム	LGWAN 用メールアドレスを 7,000 ユーザー付与可能であること	○
45		本調達の Active Directory のユーザーアカウントと整合が取れること	○
46		メールボックスの容量は 350MB/ユーザーとすること	○
47		メールボックスのユーザー毎の容量制限を行うこと	
48		メールクライアントの機能を有すること	○
49		POP 又はＩＭＡＰ、SMTP プロトコルを持つメールサーバーに対応が可能なこと	○
50		通常、メールの送受信データはグループウェアサーバー上に保存され、クライアント PC 上には保存されないこと	○
51		POP before SMTP 及び SMTP 認証によるメール送信時の認証に対応していること	○
52		SSL/TLS 及び、STARTTLS による暗号化に対応していること	○
53		１ユーザーにつき、複数のメールアカウントを登録でき、かつ、それぞれ別の受信トレイが表示され、混在しないこと	
54		ログアウトなしで複数メールアカウントの切り替えが可能であること	
55		メールアカウント毎に送信・受信メールサーバーの設定ができること	
56		グループウェア上でメールを受信した場合に、アカウント毎にメールサーバー上に受信したメールを残すか残さないかの設定ができること。メールサーバー上に	○

		メールを残す場合、受信してから一定期間の経ったメールを、受信サーバーから自動的に削除できること	
57		「フォルダ」、「メール一覧」、「プレビュー画面」の３画面構成で、画面を切り替えることなくメールを効率的に処理できること	○
58		３画面構成の他に、メールのプレビューを行わず、「フォルダ」、「メール一覧」のみ表示する、２画面構成を選択できること	○
59		メール一覧にて、メールの未読・既読の判別が可能なこと	○
60		メールボックスの使用及び全容量が画面に表示されること	○
61		新着メールの通知機能があること	○
62		ドメイン別にメール振り分け機能があること	○
63		メールアドレスの文字数の制限について提案すること	○
64		一定間隔（分単位）でメールの有無を自動でチェックし、ユーザーへ知らせる機能を有すること	○
65		削除したメールは一旦ゴミ箱に格納されること	○
66		ゴミ箱に格納されたメールは日数による削除期間が指定できること	○
67		メールを参照しながら、別のウインドウでメール返信作業を行うなど、複数のメール処理が可能なこと	○
68		重要なメールにフラグをつけて、他のメールと差別化できること	○
69		メールデータに付箋を付与でき、ポータル画面から、検索することなく該当するメールを表示できること	○
70		メール作成時に Office 文書等のファイルを添付できること	○
71		メール作成時に重要度、開封確認要求が可能なこと	○
72		メール作成時に定期的に内容を自動保存でき、メールを送信または下書き保存せずに編集画面を閉じてしまった場合でも、次にメール作成画面を開いた際に、編集中だった内容を回復できること	
73		メールを送信する直前に、内容の確認画面を表示し、宛先や本文、添付ファイル等を１件ずつチェックさせる運用が可能なこと。また、どの項目を表示/チェックさせるかを管理者が設定できること	
74		メールを送信する直前に、内容の確認画面を表示し、庁外のメールアドレス（ホワイトリストに設定されていないドメイン）の宛先を強調表示できること	
75		メールを送信する直前に、内容の確認画面を表示し、宛先/CC に一定数のアドレスが指定されている場合に、BCC での送信を促す警告メッセージを表示できること	
76		メールを送信後、設定した時間内であれば、メール送信の取り消しが可能なこと	○
77		アドレス帳より送信先を指定できること	○
78		署名を複数登録できること	○
79		よく使う挨拶文や、よく送る相手など、宛先やメール本文を指定したメールの雛形をテンプレートとして保存できること	○
80		階層化可能なフォルダでメールを管理できること（横断して検索ができること）	○
81		メール及びフォルダをドラッグ&ドロップ操作で移動できること	○
82		マウスの右クリック操作によるメニュー表示が可能なこと	○
83		キーワードによる検索が可能なこと	○
84		受信メールの条件振分が可能なこと	○
85		迷惑メールの強制削除が可能なこと	○
86		管理者は各ユーザーのメールボックス容量を１MB 単位で指定できること	○
87		管理者は、各ユーザーのメール使用容量を確認できること	○
88		.eml 形式で複数件のメールの一括ダウンロードが可能であること	○
89		.eml 形式で複数件のメールの一括インポートが可能であること	○
90		複数人で共有可能なアカウントを登録できること	
91		共有可能なアカウントからメールを送信した場合に、後からそのメールを誰が送	

		信したか確認できること	
92		管理者権限の範囲を限定して指定ユーザーへ委譲できること	○
93		人事異動時等職員情報に変更がある場合は、逐一更新すること	○
94	メールアーカイブ（送受信メール保存）対策	庁内メールも含め、全てのメールの送信、受信メールを保存すること（保存期間は１年間を想定）	○
95		サーバー単体構成でも、保存メールのメール本文、テキストの添付ファイル内容が確認可能な機能を提供すること	○
96		メールの送信、受信データをアーカイブすること（メールサーバーとは別のサーバーにアーカイブサーバーを構築すること）	○
97		アーカイブサーバーに２ケ月間以上保存し、外部媒体に１年間以上保存すること	○
98		直前まで流通していたメールが検索可能であること	○
99	メール誤送信対策（添付データ自動暗号化対策など）	送信時に添付データの自動暗号化を実施すること	○
100		メール配送機能を有すること	○
101		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	○
102		設定済みルールの判定結果による添付ファイルの自動パスワード暗号化を、標準機能のみを用いZIP形式やAES（Advanced Encryption Standard）256bit形式で行えること	○
103		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	○
104		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	○
105		送信メールの保留時間設定箇所は、宛先が庁内か庁外かで分かれており、庁内外時間差配送が可能なこと	○
106		強制BCCが設定できること	○
107	スケジュール管理機能	個人、グループ、所属単位に、日、週間、月間でリスト表示できること	○
108		スケジュールの詳細を他のユーザーに公開可能であること	○
109		ユーザー毎に、公開された複数のほかのユーザーのスケジュールをグルーピングできること	○
110		１つのスケジュール毎に公開／非公開が設定可能であること	○
111		スケジュールを代理人に管理させることが可能であること	○
112		期限を設定し、自動でデータ削除が行えること	○
113		予定の登録、変更がドラッグ＆ドロップ操作できること	○
114		予定の登録、変更について、一度に複数スケジュールを操作できること	○
115		複数のユーザーを指定して予約できること	○
116		複数のユーザーの空き時間を検索して一括予約できること	○
117		登録者及び対象ユーザーに対し予約したことを案内（メール等）できること	○
118		他人から予約されたスケジュールに対して、出席／欠席等の意思表示ができること	○
119		重複予約チェックできること	○
120		毎日、毎週の定例予約ができること	○
121		登録者が公開／非公開の別を指定して予約できること	○
122		既に予約されている内容を引用（コピー）して新たな予約を作成できること	○
123		予約されている内容を編集することができること	○
124		登録者は予約を取消すことができること	○
125		スケジュール開始時にユーザーに知らせる機能（ポップアップ等）を有すること	○
126		スケジュールはＣＳＶ形式のファイルで入出力ができること	○
127		個人スケジュール及びグルーピングされたスケジュールを整形して印刷できること	○
128		管理者はスケジュールの公開する範囲を個人または部局、所属、グループ単位に	○

		設定できること	
129		管理者は随時、ユーザー以外のスケジュール（例：部局別所管課スケジュール）が作成できること	○
130		本調達の Active Directory のユーザーアカウントと整合が取れること	○
131	職員ポータル機能	他システム等へのリンク設定（ブックマーク）が可能であること	○
132		ポータル画面にメール、キャビネット、スケジュール、掲示板等を表示できること	○
133	チャット機能	特定のユーザーを指定し、1 対 1 のメッセージ交換が可能であること	○
134		会話形式のインターフェースであること	○
135		グループチャット機能を有すること	
136		ログの保管（ユーザー及び管理者）について提案すること	○
137		本調達の Active Directory のユーザーアカウントと整合が取れること	○
138	ウェブ会議機能	複数拠点・複数人で、映像・音声によるオンライン会議が可能であること	○
139		５会議室以上、各会議室５アカウント以上が利用できること	○
140		プレゼン資料等のファイルや自分の PC の画面を会議画面に映して、参加者と共有可能であること	○
141		ウェブ会議中に、参加者同士でテキストメッセージを送信することが可能であること	○
142		会議室の予約及び参加者の指定をグループウェアで行うことが可能であること	○
143		本調達の Active Directory のユーザーアカウントと整合が取れること	○
144	その他	特定の送信元からのメールを指定したメール送信サーバーへ転送可能であること	○
145		統合 Windows 認証によるシングルサインオンに対応していること	○
146		本調達範囲である ID 管理システム及び認証基盤と連携してシングルサインオンによるログオンを行うこと	○
147		視覚障碍者向けの読み上げソフト（JAWS 等）に対応していること（対応していない場合は、対象者のみ別のメールソフト等を提供すること）	○

3.8. ＩＤ管理システム要件

項番	要　件	必須項目
1	ファイルサーバーのフォルダ割当用 Active Directory 連携データの作成を行うこと	○
2	Active Directory 連携データは、行政ネット、番号ネット、インターネットの各ネットワークに設置する Active Directory サーバー用に出力可能であること	○
3	Active Directory 連携データの対象者を抽出できるよう対象者フラグの設定が可能であること	○
4	ユーザー、組織、セキュリティグループ等を管理する画面を GUI で提供すること	○
5	認証基盤と連携を行うこと	○
6	認証基盤要件に記載するシングルサインオンシステムと連携する機能を有すること	○
7	ユーザーの役割によって、適切なメニューを切り替えて表示し、役割毎の画面を提供する機能を有すること	○
8	画面毎に権限のないユーザーが表示できないようにするアクセス制御機能を有すること	
9	LDAP サーバー、Active Directory にプロビジョニングする機能を有すること	○
10	ID 管理システムに登録したデータを Active Directory へ自動反映できること	○
11	管理項目の追加が可能であること	○
12	共通基盤システムから提供される所属・職員データ等の CSV ファイルによる一括登録、変更等が行えること	○
13	現行で個別に管理している ID/パスワードに関しては、複数の認証システムで同時に更新可能な	○

	プロビジョニングシステムを導入することで、ID/パスワードの一括管理、セキュリティグループへの個人情報の紐づけ、年度切り替え時の CSV ファイル等からの一括登録・更新作業ができること	
14	GUI でユーザー情報、組織情報の CSV ファイルでダウンロードする機能を有すること	○
15	CSV ファイルを出力し、その CSV ファイルを処理するコマンドスクリプトを起動することにより、プロビジョニングする機能を有すること	○
16	GUI からプロビジョニング先を追加し、GUI で連携先ホスト名、連携用 ID・パスワード等のパラメータを指定できること	○
17	GUI でユーザー情報、組織情報などを一覧表示する際に、その列の表示・非表示を切り替え、列の幅や順序をカスタマイズする機能を有すること（次のログイン時にもカスタマイズ内容が残っている機能を有すること）	

3.9. Windows 関連サーバー要件

3.9.1. Active Directory／DNS（Domain Name System） サーバー要件

項番	要 件	必須項目
1	Active Directory 及び DNS の設定内容は原則として、既存のものを移行し、セキュリティグループ、グループポリシー等の整理行った上、WindowsServer2016 以降のものにバージョンアップを行うこと	○
2	拠点間の冗長性を考慮し、複数台のドメインコントローラ構成とすること（Active Directory 上で管理するユーザー、グループ数はそれぞれ 10,000 程度とする）	○
3	災害等による障害を考慮したシステム構成とすること	○
4	ハードウェア統合基盤の有効利用の為、ドメインコントローラの仮想化基盤上での動作を考慮すること	○

3.9.2. WSUS（Microsoft Windows Server Update Services）要件

項番	要 件	必須項目
1	WSUSサーバーを構築・設定すること（端末に対し安定して配信できる構成とすること）	○
2	Update データは LGWAN-ASP より取得すること	○

3.9.3. ボリュームライセンス認証管理ツール（VAMT）要件

項番	要 件	必須項目
1	VAMT サーバーの構築・設定を行うこと	○

3.10. セキュリティ要件

項番	要 件	必須項目
1	ウィルス対策ソフトの管理対象は、庁内ネットワーク（行政ネット）に接続するすべてのサーバー及びクライアントとすること（対象台数：約 5,500 台）	○
2	ウィルス対策ソフトは日本国内での導入実績があること	○
3	ウィルス対策（ハイパーバイザー、ストレージ、管理対象機器）について提案すること	○

4	ウィルス対策ソフトのパターンファイルを最低１日１回最新のものに更新すること	○
5	仮想マシンに対するセキュリティ対策として、以下の事項が適正に実施されているか、定期的に確認できること ①仮想マシンへのウィルス対策ソフトの導入状況 ②仮想マシンに導入されているウィルス対策ソフトの設定（常時監視、完全スキャンとなっているか） ③仮想マシンに導入されているウィルス対策ソフトのエンジン、パターンファイルのバージョン ④サポート期間中の Windows のセキュリティパッチ適用状況	○
6	ハードウェア統合基盤に関するセキュリティ対策として、セキュリティパッチ適用及びコンピュータウィルス対策を実施すること	○
7	定時ウィルスチェックの実行、更新ファイルの配布等、高負荷の処理を実行することによる、システム・端末の応答時間の著しい低下（いわゆるアンチウィルスストーム）を発生させないような対策が実装されていること	○
8	ハードウェア統合基盤上の仮想マシン数、ストレージ容量等の多寡によりライセンス料金に変動を来さないこと	○
9	既存環境の Microsoft Windows Server 2008　について、令和３年度末までサポートできる仕組みを構築すること（対象は 50 クライアント）	○
10	受託者は適正なセキュリティ運用管理体制を有すること	○
11	受託者は ISMS 適合性評価制度(ISO/IEC 27001:2005、JIS Q27001:2006)の認証、又はこれらと同等の情報セキュリティに関するマネジメントシステムの認証を取得していること	○

3.11. 統合運用監視要件

項番	要　件	必須項目
1	ハードウェア統合基盤を構成する機器及び仮想マシンは、運用監視機能を提供する各種サーバー群から接続可能な構成とすること	○
2	適切なアクセス管理を実施すること	○
3	利用するソフトウェアは、安定稼働・サポートの観点から、導入ベンダーの責任において安定稼働・サポートが行えるものを使用すること	○
4	保守期間中の運用管理ソフトウェアのバージョンアップ対応を行うこと	○
5	運用管理端末において、原則 GUI ベースの操作画面から操作を行えること	○
6	Ping および SNMP(MIB)による物理サーバー、ネットワーク機器、ストレージ、周辺機器及び仮想マシンの死活監視を行うこと	○
7	物理サーバー、ストレージおよび仮想マシンの CPU、メモリ、ディスク使用率を監視すること	○
8	物理サーバー、仮想マシンおよびネットワーク機器のトラフィック情報（回線使用率等）を監視すること	○
9	物理サーバー及び仮想サーバーにおいて、アプリケーションログやシステムログのエラー、警告メッセージを監視すること	○
10	物理サーバー、ネットワーク機器、ストレージ、周辺機器及び仮想サーバーから送信される SNMP-TRAP を監視すること	○
11	運用管理・利用支援業務の処理に係るログを管理し、CSV ファイル形式のデータ出力ができること（統計情報として契約期間中蓄積すること）	○
12	監視対象オブジェクトの正常稼働状態を分析し、システムの正常性を監視できること	○
13	新たに仮想マシンが増えた場合は、監視対象に含めることができること	○
14	仮想基盤におけるリソース使用状況を収集し、リソース使用状況トレンドから、将来的に必要なリソース量や必要時期を算出する機能を有すること	○
15	残存リソース（キャパシティ）を構築可能な仮想マシン数として換算できること	○
16	追加予定の仮想マシンおよびリソース（ストレージ等）を入力することで、キャパシティシミュレーションが実現可能な機能を有すること	○
17	各仮想マシンのリソース使用状況から割当過剰な仮想マシンや割当不足の仮想マシンをリストアップし、推奨割当値を示すことができること	○
18	統合基盤を構成するハードウェアの稼働状況を把握し、週次、月次、年次の単位で、CSV ファ	○

	イル形式およびグラフ等でデータ出力できる統計情報の内容について提案すること。具体的には以下の内容を想定している。 ①物理サーバー及び仮想マシンのCPU、メモリ、ディスク使用率、ディスクI/O回数等の性能情報 ②ストレージのI/O、スループット、レスポンス、キャッシュ等の性能情報 ③ネットワーク機器、物理サーバーおよび仮想マシンのトラフィック量、パケット量等のネットワーク性能情報	
19	リソース状況及び将来のリソース予測を行う機能を有すること ＜分析対象＞ 仮想化基盤：CPU、メモリ、ネットワークなどのリソース ストレージ：ディスクリソース、I/O、ネットワークなどのリソース ネットワーク：ネットワークポート、負荷状況等のリソース	○
20	ハードウェア統合基盤の稼働監視だけでなく、ハードウェア統合基盤全体のリソース課題や危険性を発見できること	○
21	監視対象の特性に合わせてエージェント監視、エージェントレス監視、SNMP監視が行えること	○
22	仮想化基盤の監視については、基盤の監視(データストアの容量監視、CPU／メモリリソース監視、ネットワーク監視)と、基盤上で提供される仮想マシン(CPU／メモリ／ディスクのリソース監視、電源状態)の監視が実施できること	○
23	新たに庁内システムが基盤上に追加された場合、追加された仮想マシンに対して動的に監視を適用する機能も有すること	○
24	仮想マシンを利用する庁内システム運用職員及び、庁内システム納入業者等が、管理対象システムのみの稼動状況を閲覧できる機能を有すること	○
25	本調達のサーバー群全体を監視すること ①リソース状況の監視 ②仮想化基盤の監視(トラフィック、パフォーマンス、システム異常検知、各種アラートなど) ③プロセス死活監視	○
26	職員一人1台パソコンについて、以下の内容を監視すること ①端末操作の監視（ログ取得） ②セキュリティ・インシデント監視 ③ソフトウェアの配布、インストール(OS等のバージョンアップ、パッチ適用含む) ④USBデバイスの管理(資産管理システムによる制御など) ⑤リモート操作(各種トラブル対応含む) ⑥特定のアプリケーションの起動禁止　他	○

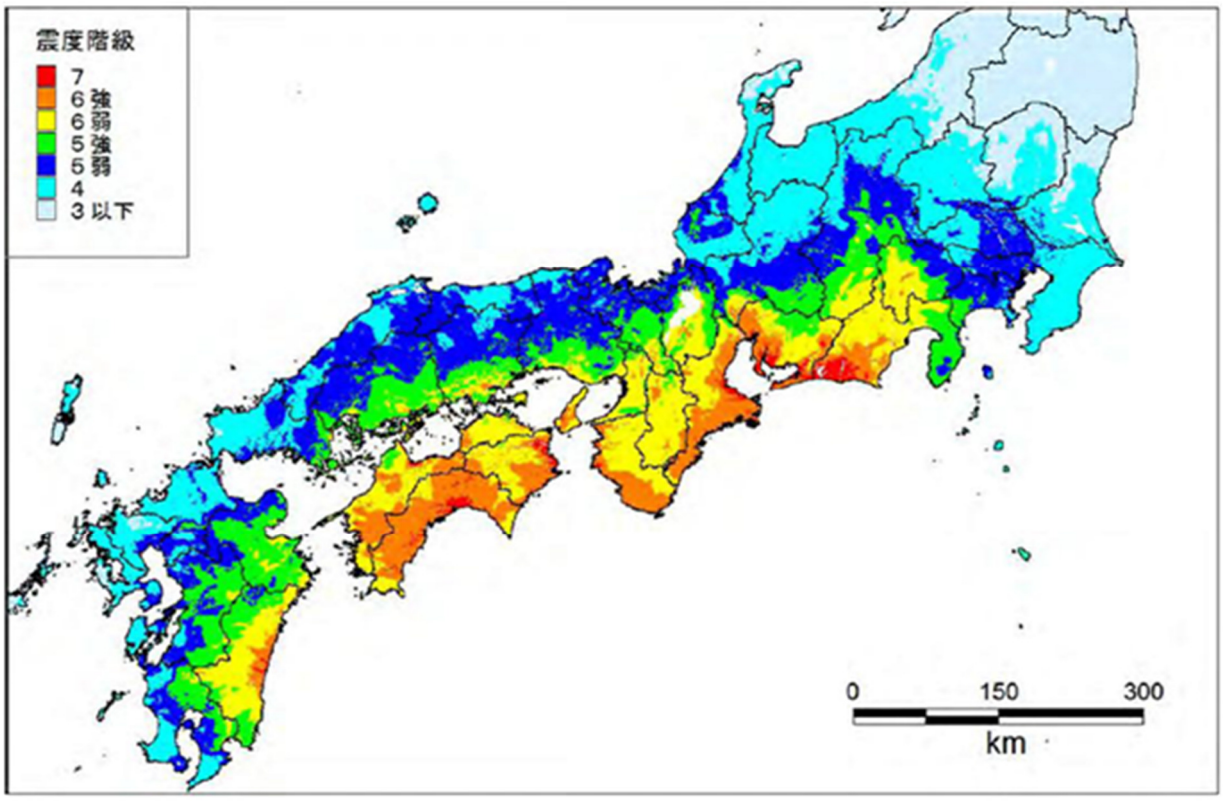
3.12. ＩＤＣ及び接続回線要件

3.12.1. データセンター要件

項番	要　件	必須項目
1	データセンターは日本国内であること。また、奈良県による監査の受け入れが可能であること	○
2	ハードウェア統合基盤が安定して稼働できる環境を提供すること	○
3	ルータ等の回線接続機器を提供すること	○
4	インターネット回線の設置が可能であること	○
5	設置場所における保守・運用にかかる費用は受託者の負担とすること	○
6	IDCは、いわゆる「南海トラフ地震」に伴う激甚災害を想定し、プライマリ拠点及びバックアップ拠点は、図５の南海トラフ巨大地震の震度分布の６弱以下の地域と５強以下の地域を設定すること（施設について、震度６強の地震に対しても障害無く稼働できる環境を提供できる場合にはこの限りではない）	○
7	建物は、建築基準法（昭和25年5月24日法律第201号）で定められた耐火建築物であること。また、消防法に基づいた消火設備及び火災感知設備を有すること	○
8	建物は、新耐震基準（昭和５６年）を満たしていること	○
9	データセンターは、日本データセンター協会が定めるティア３相当以上であること	○

10	地震に対する被害防止対策を講じていること	○
11	建物は、津波、高潮、集中豪雨、漏水等に対する水害対策を講じていること	○
12	利用できる回線業者の制限が無いこと。複数の回線事業者の回線を利用した冗長構成を構成可能なこと	○
13	避雷設備及び雷サージ対策などによる直撃雷対策を講じていること	○
14	地方公共団体の発行する洪水・津波・土砂災害・火山ハザードマップ上において、被害の予想される区域に指定されていないこと。指定されている場合は、必要な対策を講じていること。また液状化のリスクがないこと	○
15	AC100V と AC200V の電源が提供可能であること	○
16	商用電源の停電の際、24 時間以上電力供給が可能な発電機設備を有すること（発電機設備が稼働するまでの間、瞬断することなく十分な電力供給が可能な蓄電池設備を有すること）	○
17	24 時間 365 日稼働可能な空調設備を有すると共に、当該設備の一部が故障又は点検等で停止した場合でも、各ラックに対して十分な冷却効果が望める空調能力に支障をきたさないこと	○
18	入室資格を有する者のみが入室できる管理設備を有すること。24 時間 365 日入退室管理が行われていること	○
19	設備機器を運用するスペースは、外部から見えない構造となっていること	○
20	作業に必要な照明及び非常時の非常灯については、建築基準・消防法を順守し、整備すること	○
21	設置場所調達要件により提供されるデータセンター環境において、障害が発生した場合は、24 時間 365 日対応可能であること	○
22	障害対応の実施後は、障害報告を行い、その履歴管理を行うこと	○
23	セキュリティ事故発生等の緊急時に奈良県の指示に従い、ログ等の情報提供を行うこと	○
24	設備環境において、定期点検、日常点検により十分な点検項目が適切な点検サイクルで実施されていること	○

図５　中央防災会議の南海トラフ巨大地震の震度分布
（強震動生成域を陸側寄りに設定した場合）



※　平成２４年８月２９日
中央防災会議防災対策推進検討会議
南海トラフ巨大地震対策検討ワーキンググループの資料より引用

3.12.2. **回線要件**

項番	要　件	必須項目
1	大和路情報ハイウェイ又は統合ネットワークと、ハードウェア統合基盤、統合バックアップ拠点を相互に接続する回線サービスはインターネット回線から物理的もしくは論理的に分離された専用回線（インターネット VPN は除く）とし、初期経費、ランニングコスト、保守経費を本調達に含めること	○
2	漏洩・盗聴・利用権限管理等について、十分なセキュリティ対策が施されていること	○
3	ハードウェア統合基盤設置拠点としてデータセンターを活用する場合には、LGWAN 接続によるサービス提供も可とするが、前提として、地方共同法人地方公共団体情報システム機構に LGWAN の ASP サービス（ファシリティサービス）として登録されていること	○
4	IDC～大和路ハイウェイ・センタースイッチまでの回線（専用回線）は、正回線を 1 Gbps 以上の帯域を有するギャランティ型回線、副回線を 1Gbps の帯域を有するベストエフォート型回線以上の冗長構成で提供すること	○

4. 運用・保守業務要件

4.1. 運用業務要件

4.1.1. 運用体制

項番	要　件	必須項目
1	県からの申告及び運用監視ツール等で検知したインシデントに基づき運用業務を実施すること。また、窓口は一元化すること	○
2	受託者は、県庁内もしくは主たるシステム設置場所へ運用者を常駐させ、運用業務を行うこと（現行は３名程度が常駐）	○
3	連絡体制として、運用窓口への連絡が口頭、電話、FAX、電子メールいずれかの方法で常時できること	○
4	ハードウェア統合基盤に関する障害情報について、県に遅延なく公表すること	○
5	関連する他の業務システムの運用ＳＥと円滑なコミュニケーションのもと、業務連携を行うこと	○

4.1.2. 対応時間

項番	要　件	必須項目
1	運用監視ツールを用いた自動監視については、24 時間 365 日の対応を行うこと	○
2	受付及び対応時間は、原則、年末年始を除く平日８時 30 分～１７時 15 分とすること（ただし、「サマータイム」等の実施により、開庁時間が変更となった場合は、対応時間も合わせて変更することがある）	○
3	ハードウェア統合基盤設置拠点及びバックアップ拠点をデータセンターとする場合は、24 時間 365 日とすること	○
4	人事異動、共通端末更新、障害発生時には開庁時間外であっても対応すること	○

4.1.3. 運用業務範囲及び内容

<table>
<tr><th>項番</th><th colspan="2">要　件</th><th>必須項目</th></tr>
<tr><td>1</td><td rowspan="8">全体</td><td>ハードウェア統合基盤（ファイルサーバー群、グループウェア、その他周辺機器・機能を含む）全体を運用業務対象範囲とすること</td><td>○</td></tr>
<tr><td>2</td><td>共通端末等の障害対応、ソフトウェアインストール対応、人事異動対応並びにエンドユーザの支援及び相談対応を行うこと。なお、必要に応じてエンドユーザへの電話連絡等を行うこと</td><td>○</td></tr>
<tr><td>3</td><td>本調達範囲の物品の運用、監視及び障害対応等を行うこと</td><td>○</td></tr>
<tr><td>4</td><td>ハードウェア統合基盤及び統合バックアップ（遠隔地バックアップ含む）の運用管理を行うこと</td><td>○</td></tr>
<tr><td>5</td><td>仮想化基盤に業務システムを構築する際に支援を行うこと</td><td>○</td></tr>
<tr><td>6</td><td>バージョンアップ等の作業の際は、計画及び手順書を作成し、県に提案すること</td><td>○</td></tr>
<tr><td>7</td><td>運用監視ツール等を利用し、以下の運用監視を行うこと
<table>
<tr><th>項　目</th><th>対　象</th></tr>
<tr><td>構成管理</td><td>ハードウェア
仮想マシン
ネットワーク(基盤内のみ)
ゲスト OS （クラウドサービスの場合）
ミドルウェア（クラウドサービスの場合）</td></tr>
<tr><td>変更管理</td><td>ハードウェア統合基盤の状態が変更、更新された際に構成情報等を変更</td></tr>
<tr><td>稼働管理</td><td>ハードウェア
仮想マシン
ネットワーク(基盤内のみ)
ゲスト OS （クラウドサービスの場合）
ミドルウェア（クラウドサービスの場合）</td></tr>
</table></td><td>○</td></tr>
</table>

		<table><tr><td>性能管理</td><td>ハードウェア 仮想マシン ネットワーク(基盤内のみ) 基盤側で割当てたリソースについて、アプリケーション等が正常動作する為の性能管理</td></tr><tr><td>セキュリティ管理</td><td>ネットワーク(基盤内のみ) ウィルス管理ソフトウェアによるウィルス対策</td></tr><tr><td>バックアップ管理</td><td>基盤上で取得したバックアップの履歴、ジョブ管理</td></tr></table>	
8	グループウェアに関する運用業務	組織改正、職員採用・異動等に伴うアカウント、スケジュール、ウェブ会議、チャット、各種キャビネット、ポータル画面等の作成・変更及び、利用権限の変更等の作業を行うこと	○
9		アカウントやグループ毎のメールフォルダ、キャビネット等の容量設定作業を行うこと	○
10	ファイルサーバー及びWindows 関連サーバーに関する運用業務	ファイルサーバーの運用管理(ユーザー管理、死活監視、アクセスログ管理・監査等)を行うこと	○
11		Active Directory の運用管理(ユーザー管理、グループ管理、パスワード変更、グループポリシーの設定・配布等)を行うこと	○
12		組織改正、職員採用・異動等に伴うドライブ・フォルダ構成及びユーザー構成の変更、利用権限の変更等の作業を行うこと	○
13		WSUS のアップデートファイル更新、配信設定、Windows アップデート内容の検証等の運用業務を行うこと	○
14		WSUS のアップデートファイルは、LGWAN-ASP サービスからアップデートプログラムを取得すること	○
15		共通端末の Windows のメジャーアップデートを年１回以上行うこと（アップデート前に共通端末に標準でインストールされているソフトウェアの検証を行うこと）	○
16		共通端末に対し、適宜 Windows のセキュリティパッチの適用を行うこと（アップデート前に共通端末に標準でインストールされているソフトウェアの検証を行うこと）	○
17		VAMT を使用し、対象端末の Microsoft 製品のライセンス認証を行うこと	○
18		ＤＮＳサーバーの維持管理（正常稼働の監視）	○
19		設定ファイル（Named Conf　ゾーンファイル）の変更を行うこと	○
20		ログ監査に必要な情報を抽出すること	
21		一定期間アクセスのないフォルダを出力すること	
22		アクセスの多いユーザーの特定、アクセスの多いディレクトリの特定をすること	
23		ログデータはローカルディスクに１年間分以上を保存すること	
24		保存したログデータを外部記録媒体に定期的にアーカイブし保存すること	
25		検索結果を条件指定によりレポートを作成し、Excel 形式、CSV 形式等のファイルに出力を行うこと	
26		将来、Office365 を使った場合の運用対応を見込むこと	
27	統合ＩＤ管理システムに関する運用管理業務	組織改正、職員採用・異動等に伴うドライブ・フォルダ構成及びユーザ構成の変更、利用権限の変更等の作業等を行うこと	○
28	資産管理に関する運用業務	ユーザー管理、デバイス管理、セキュリティパッチ検証、配布、適用、資産管理等を行うこと	○
29		資産管理ソフトで以下のソフトウェアライセンスの管理を行うこと ①資産管理ソフトへソフトウェアライセンス番号の入力 ②資産管理ソフトで管理している端末とソフトウェアライセンス番号の紐付け ③ソフトウェアライセンス番号の有効期間の管理 ④ソフトウェアライセンス重複防止の管理	○
30		ソフトウェアインストール申請時のソフトウェアの情報収集及び有害なものでないことを確認し、県へ報告すること	○
31	認証基盤に関する運用	顔情報（写真、顔識別情報等）の撮影、登録、管理、削除等の対応を行うこと	○
32		シングルサインオンの項目に変更があった場合は対応すること	○

33	業務	職員に配備しているパソコンを閉域接続専用 SIM での庁内ネットワーク接続に対応させるための設定変更等を行うこと	○
34	ウィルスチェックソフト（現行はトレンドマイクロ社・ウィルスバスター）の運用管理、障害対応	日常監視業務を行うこと	○
35		最新パターンファイルの更新を行うこと	○
36		ウィルス発生時の対応を行うこと（資産管理ソフトによる該当端末調査を含む）	○
37		ウィルチェックソフト（サーバーを含む）のインストール及びバージョンアップを行うこと	○
38		ウィルスチェックソフト（サーバーを含む）の検索エンジンのバージョンアップを行うこと	○
39	支援・相談業務	エンドユーザの支援及び相談対応として、共通端末及び各所属が共通端末と同一仕様で調達した端末の操作・障害（ハードウェア及びソフトウェア切り分け）に関する質問・相談に電話又はリモート操作等により対応すること。なお、エンドユーザー対応として端末の操作支援、ソフトウェア障害一次切り分け、ハードウェア障害一次対応及び一次切り分けは別の契約で実施しているので本調達には含まない。	○
40		共通端末及び各所属が共通端末と同一仕様で調達した端末に対して、県が承認したソフトウェアを管理者権限でインストールし、ユーザー権限で動作することを支援すること（インストールできない場合でも原因追及し、ユーザーに説明できること）	○
41		共通端末及び各所属が共通端末と同一仕様で調達した端末の障害対応を実施し、必要に応じて再セットアップ作業（ファイル復旧及びソフトウェアインストール作業含）を実施すること	○
42		windows のバージョンアップデート等により、共通端末の仕様が変更になった場合及び共通端末の更新の場合は、マスターの再作成を行うこと	○
43		共通端末及び各所属が共通端末と同一仕様で調達した端末のセットアップを行うこと	○
44		人事異動等による共通端末の再セットアップ対応を行うこと	○
45	番号系ネットワークに関する運用業務	令和４年１月より、別添「マイナンバー利用事務運用業務仕様書」の運用を行うこと	○
46	業務実績報告	業務の日報・月報を作成すること	○
47		定例会により、月１回の実績報告および翌月の予定について、奈良県と調整を行うこと	○
48	その他	障害発生時、受託者が責任をもって庁内システムと統合基盤環境の原因の切り分けを実施すること	○
49		切り分け実施後、障害の原因が統合基盤側によるものであった場合は、迅速に受託者が対応を行うものとし、障害の原因が庁内システム側によるものであった場合には、事前に取り決めた手段により庁内システム管理者及び庁内システム導入業者に対し迅速に連絡すること	○
50		運用業務内容に変更が生じた場合は、奈良県と協議の上、対応すること	○
51		庁内の他システムの運用ＳＥ等、関係者と調整・協力を行うこと	○
52		情報システム課職員等に対する技術的支援を行うこと	○
53		リモートでの運用保守について、提案すること	○
54		大地震等の大規模災害等、不測の事態が発生した場合は、協力すること	○

4.2. 保守業務要件

4.2.1. 保守体制

項番	要　件	必須項目
1	受託者は、県からの保守受付を実施すること（窓口は一元化すること）	○
2	障害と思われるインシデントが発生した場合は、障害の一次切り分けを受託者が責任をもって実	○

	施すること	
3	障害等の発生時には速やかに復旧に努め、円滑なシステム管理・運用を継続的に行えるよう体制を整えること	○
4	障害時連絡体制として、保守窓口または担当保守員への連絡が電話・FAX・電子メールいずれかの方法で常時できること	○
5	本システムの障害情報について、県に遅延なく公表すること（必要に応じてシステム開発運用受託者及びハウジング業者等にも障害情報の通知を行うこと）	○

4.2.2. 対応時間

項番	要　件	必須項目
1	障害時の受付時間は 24 時間 365 日とすること（詳細な条件については、別途締結する SLA にて定めること）	○
2	業務継続に支障がない障害の場合、保守対応時間は、年末年始を除く平日８時 30 分～１７時 15 分とすること（ただし、「サマータイム」等の実施により、開庁時間が変更となった場合は、対応時間も合わせて変更することがある）	○
3	緊急時もしくは業務継続に支障が発生した場合、保守対応は即時行うこと（詳細な条件については、別途締結する SLA にて定めること）	○
4	障害コールから２時間以内に復旧作業に取りかかれること（詳細な条件については、別途締結する SLA にて定めること）	○

4.2.3. 保守業務内容

項番	要　件	必須項目
1	アプライアンス機器を導入した場合は、ハードウェアの保守だけでなく、ソフトウェア機能の保守及びログ解析、運用監視、運用サポート等一体的な保守を行うこと	○
2	機器故障の場合は故障部品の交換対応を速やかに行うこと	○
3	障害復旧作業の実施に際しては、県及び受託者との協議の上、作業内容・作業時間等を決定すること	○
4	障害の切り分け実施後、障害の原因が統合基盤側によるものであった場合は、迅速に受託者が保守対応を行うものとし、障害の原因が庁内システム側によるものであった場合には、事前に取り決めた手段により、県と庁内システム導入業者に対し迅速に連絡を行い、庁内システム導入業者と連携して保守対応を行うこと	○
5	障害対応の実施は障害復旧及び障害報告を行いその履歴管理を行うこと	○
6	計画保守対応の実施は事前に県への報告を行い、システム運用上の影響を考慮し、適切な計画の元に作業を実施すること	○
7	グループウェアシステムにおける保守業務内容は以下の内容も含めること ①保守は２４時間（３６５日）受付、オンサイト保守とすること（県の承認を得たものについてはリモートによる対応もできるものとする） ②保守の内容は、ソフトウェアの再インストール、システムの復旧、バックアップからのリカバリ、修正ソフトウェアの適用等を行うこと	○
8	保守期間中の各種ソフトウェア（ハイパーバイザー、運用管理ソフトウェア、グループウェア等）のバージョンアップ対応を行うこと	○

4.3. サービスレベル項目（ＳＬＡ）

以下の内容を基本に、別途、SLA を締結して実施すること。評価・測定項目及びその運用について、提案すること。

【評価項目及びサービスレベル（参考）】

評価項目		サービスレベル
可用性	サービス提供時間	24 時間 365 日（計画停止・定期保守を除く ）
	月間サービス稼働率（計画停止を除く、サービス提供期間における稼働率）	試用期間（稼働後６か月）と試用期間終了後における実現可能な稼働率を提案すること。
	障害時の連絡（検知から指定メールアドレスへメールするまでの時間）	開庁日の 8:30 ～17:15 は 30 分以内 それ以外の時間帯は 1 時間以内
	障害着手（県庁舎内での作業が必要な場合、故障検知から県庁舎 内で着手するまでの時間）	開庁日の 8:30 ～17:15 は 1 時間以内 それ以外の時間帯は 2 時間以内
	障害回復時間	迅速に対応すること。 障害回復時間は県と協議のうえ決定するが、 最大でも８時間 とする。
性能	性能調整	仮想環境の利用状況に応じ、性能が劣化しないようにチューニングを実施すること。
運用支援	障害申告受付	24 時間 365 日
	電話による問い合わせ対応	年末年始を除く平日の 8:30～16:45（ただし、サマータイム等実施の際は、その開庁時間）
	メールによる問い合わせ受付	24 時間 365 日
	問い合わせへの一次回答	翌開庁日の 12:00 まで
	作業を伴う運用支援	開庁日の 8:30 ～17:15
	平均回答時間	受付から問題解決の回答までに要する時間
	問題解決率	取り決めをした問題解決（クローズ）までの時間で解決した比率
	バックログ率	1 日の終了時点で未解決の問題の比率
その他	要員教育時間	運用要員などに対する各種教育に費やす時間。 業務開始時、定期的な研修など。

※範囲はハードウェア統合基盤とし、ゲストＯＳ上の庁内システムは対象外とする。

（１）測定

各評価項目について遵守状況を毎月測定及び報告を行うこと

（２）達成できない場合

目標値を含むサービスレベルが達成できない見込となった場合は、ただちに県に報告の上、改善策を協議すること（改善策を実施してもサービスレベルの達成ができない場合等のペナルティの考え方について提案すること）

5. その他

5.1. 既存ハードウェア統合基盤からの移行

項番	要　件	必須項目
1	原則として既存ハードウェア統合基盤の全データを移行対象とすること（本調達において変更があるソフトウェアは除く）	○
2	移行期間は、令和２年４月から令和３年２月末までとすること（期間中は既存ハードウェア統合基盤と並行稼働）	○
3	移行による庁内システム（ファイルサーバーを含む）の停止は原則、業務時間外とすること	○
4	移行方法について提案すること	○
5	グループウェア（現行は「desknet's NEO V2.1 R2.1 .Gov」）の更新は、ユーザーへの負担なしで全てのデータを移行すること（メール、キャビネット、アドレス帳等）	○
6	ハードウェア統合基盤の各種ソフトウェア（ハイパーバイザー、運用管理ソフトウェア、グループウェア等）の利用方法について、以下の操作マニュアルを日本語で作成すること ①利用者マニュアル 利用者が本システムを利用するときに参照するマニュアル 本システムに共通する操作方法、メニュー項目、メッセージ等に対する説明、並びに各機能の流れに沿った処理手順、画面説明についても記載すること。また、同様の内容で Web ブラウザから参照できるオンラインヘルプ機能を用意すること ②管理者マニュアル 本システムの管理者がメンテナンスを実施するときに参照するマニュアル システムに対するアカウント管理や権限管理、その他管理業務について、操作方法を記述すること ③運用マニュアル オペレータが本システムの運用を実施するときに参照するマニュアル 運用要件にあげた監視機能、バックアップ、ジョブ管理等の運用オペレーションに対する操作方法を記述すること ④障害時対応マニュアル システムの障害発生時に管理者が参照するマニュアル 緊急時の対策として必要な措置、確認・復旧方法について専門的な知識が無くても理解できるように記述すること	○
7	グループウェアに変更がある場合は、以下の対応を行うこと ①操作研修会の実施（e ラーニングによる研修も可とする） 仮稼働までに県庁職員（約 300 名程度）を対象に実践的な操作研修を行うこと 会場、プロジェクタ、研修端末等の必要な機器は県側が用意するので、研修に必要な教材を準備し、講師を派遣すること。詳細は県と調整の上実施すること。本調達に、研修にかかる費用を含んでおくこと ②サポートデスクの設置 仮稼働開始日から本稼働後６ヶ月の間、ユーザーからの操作補助や各機能の説明等のための電話相談窓口を日本国内に設けること（電話対応時間は、平日(土日祝日を除く)の８：30 から 17：15 までとする、窓口の設置場所は問わない）	○
8	バックアップデータからの各種リストアの方法を実際に試行し、想定どおりに動作することを確認すること	○
9	既存ハードウェア統合基盤の仮想マシン移行にあたっては、管理者権限の追加付与を除き、既存環境側のバージョンアップ等の構成変更が必要ない方式で実施すること	○
10	移行で使用するソフトウェアおよびツール類を本調達に含めること。なお仮想マシン移行で使用するソフトウェアおよびツール類はメーカーのサポートが提供されることとし、既存ハードウェア統合基盤のハイパーバイザーのバージョンを問わず動作が保証されていること	○
11	仮想マシンの移行方式は、計画的な移行を実現するために、サービス停止時間を極小化した方式とすること。また、新環境での稼動確認の際に不具合が生じた場合は速やかに旧環境への切り戻しが可能な方式とすること	○

5.2. 契約期間終了時の対応

項番	要　件	必須項目
1	契約期間（再リース期間を含む）終了後は、機器等を撤去回収するものとし（クラウドサービス型の場合を除く）、その費用も負担すること（ハードディスクのデータ内容を完全消去し、その作業が完了した旨の証明書を発行すること）	○
2	次期システムへの移行の際に発生する作業支援を行うこと	○
3	資産管理ソフトのログ及びメール送受信のログを提供すること	○

5.3. その他

⑴マニュアルは電子及び紙媒体それぞれ作成すること。
⑵構成機器その他要素の使用に必須となるライセンス、付属品、消耗品、管理端末等は契約期間中に必要な数量を用意すること。
⑶本仕様書に定めのない事項が発生した場合及び疑義が発生した場合は、奈良県と協議のうえ定めるものとする。