三重県共通機能基盤再構築及び運用保守業務委託

仕様書（案）

令和 6 年 3 月

三重県総務部デジタル推進局デジタル改革推進課

目　　次

1.背景及び目的

1.1.　はじめに

本仕様書は、令和 6 年度に実施する三重県共通機能基盤再構築及び運用保守業務（以下「本業務」という。）の仕様について記載している。

なお、用語の定義については、別紙１「用語の定義」を参照すること。

1.2.　背景

三重県では、平成 21 年度から三重県中小システム統合サーバ（以下「統合サーバ」という。）を構築し、平成 26 年度と令和 2 年度の二度に渡り再構築を行っている。令和 2 年度の再構築時には、ライセンス等の制約から、VMware 社の VMware vSphere を利用した統合サーバと Microsoft 社の Hyper-V を利用した統合サーバ（2 系統の統合サーバ）を構築している。

統合サーバは、主に中小規模のシステムを仮想化したうえで統合するために導入したもので、これにより、それぞれの情報システムでサーバを調達することによる重複投資を抑制するとともに、セキュリティ向上や業務負荷の軽減という効果を生み出すことができている。（令和 5 年 10 月現在、44 システム、165 サーバが稼働している。）

また、三重県では、平成 21 年度から三重県リモート保守環境（以下「リモート保守環境」という。）を構築し、平成 26 年度と令和 2 年度の二度にわたり再構築を行っている。

リモート保守環境は、遠隔地からインターネット経由で三重県情報ネットワーク上のシステムを安全に運用保守ができるシステムであり、このシステムを利用することで、それぞれのシステムにおける運用保守対応や緊急時対応等の投資を抑制するとともに、セキュリティの向上や業務負荷の軽減という効果を生みだしている。（令和 5 年 10 月現在、27 システムがリモート保守環境を利用している。）

統合サーバ、リモート保守環境は、これまで別契約によりそれぞれ構築していたが、令和 2 年度において、2 つの契約を一括契約とすることで両システムを統合し、「三重県共通機能基盤システム（以下、「共通機能基盤」という。）」として再構築を行った。

本業務は、令和 7 年度末で既存の共通機能基盤が保守期限を迎えるため、新たな共通機能基盤（以下、「本システム」という。）として、再構築を行うものである。

1.3. 目的

今後も共通機能基盤の利用による重複投資の抑制、セキュリティの向上、業務負荷の軽減等の効果を上げていくために、これまで以上に多くのシステムにサーバ統合化とリモート保守環境の利用を推進していく。そのため、本システムの再構築に必要な設計、機器等の納入、及び、構築、運用保守等を円滑に行うとともに、統合サーバや~~バックアップ~~ストレージ等として利用可能なクラウドサービスの導入を本業務の目的とする。

2. 契約概要

2.1. 案件名

三重県共通機能基盤再構築及び運用保守業務

2.2. 調達範囲

本業務における調達範囲は、以下のとおり。

ア　本システムの設計

イ　本システムの機器、及び、ソフトウェア等の納入・設置

ウ　本システムの構築・設定・テスト

エ　既存共通機能基盤から本システムへの移行に係る移行設計・移行作業・移行支援

オ　本システムの運用保守

カ　データセンター、及び、回線の利用に関する費用、及び、作業

キ　クラウドサービスやクラウドサービスに接続するために利用する回線に関する費用、及び、作業

2.3. 機器設置場所

システムに必要なサーバ機器等は、原則として本県が指定する「三重県情報ネットワークに接続済みの津市内データセンター」に設置すること。

なお、津市内データセンター以外に受託者が用意するデータセンターへ機器等を設置することも可とするが、そのデータセンターを三重県情報ネットワークに接続するための専用回線（4Gbps 以上の帯域保証）、及び、ネットワーク機器を用意する他、その構築、及び、運用保守についても本業務に含めること。

サーバ機器類を設置したデータセンターとは別拠点のデータセンターに、レプリケーション用のバックアップストレージを設置すること。

なお、レプリケーション用バックアップストレージを「5.4.12.クラウドサービスに関する詳細要件」にて後述するクラウドサービス上に構築することも可とする。

※ 本仕様書では、便宜的に「サーバ機器等を設置するデータセンター」をIDC1、「レプリケーション用のバックアップストレージを設置するデータセンター（IDC1とは別拠点）」をIDC2と表記している。BCPの観点から、IDC2はIDC1から物理的に十分離れた場所に用意すること。

2.4. 履行場所

本業務の履行場所は次のとおりである。

ア 三重県本庁舎（津市広明町13番地）（以下「本庁」という。）

イ サーバ機器等を設置する津市内データセンター（IDC1）、レプリケーション用バックアップストレージを設置するデータセンター（IDC2）

ウ 受託事業者内

エ その他、機器等を設置する三重県の機関等

2.5. 契約履行期間

履行期間は契約締結日から令和14年3月31日までとする。

履行期間内におけるスケジュールの概要は以下のとおり。

ア 令和7年6月30日までを、設計（基本、詳細）、機器、及び、ソフトウェア等の納入、設置、構築、設定、テスト等の期間とする。

イ 令和7年7月1日から令和8年3月31日までを移行期間とする。

ウ 令和8年4月1日から令和14年3月31日までを本システムの運用期間とする。

エ 令和7年7月1日から令和14年3月31日までをクラウドサービス利用期間とする。

※ 詳細は、「3.3. 想定スケジュール」を参照すること。

2.6. 支払条件等

2.6.1. 支払条件

本業務の利用に係る費用の支払条件は以下のとおりである。

設計構築等（①設計、②構築、③テスト稼働、④移行）にかかる費用は、各年度において、①から④のそれぞれ完了した分の完了検査を行い、相当分を支払うこととする。

運用保守等（⑤運用保守、⑥クラウド利用等）にかかる費用は、年度ごとに完了検査を行い、相当分を支払うこととする。運用保守費用については、運用費用、保守費用、データセンター費用、回線費用等が含まれるものとする。

各年度の支払額は、次の割合を目安として、契約時に協議するものとする。

表 2.6.1　支払割合の目安

年度	設計構築等費用	運用保守等費用
令和 6 年度	総契約額の●.●%	－
令和 7 年度	総契約額の	
令和 8 年度	－	
令和 9 年度	－	
令和 10 年度	－	
令和 11 年度	－	
令和 12 年度	－	総契約額の●.●%
令和 13 年度	－	総契約額の●.●%

公告時に公開します。

2.6.2.　　内訳資料の提出

上記支払条件を踏まえて契約額の内訳資料を作成し、契約締結前までに提出すること。特に、設計、機器、及び、ソフトウェア等の納入、設置、構築、テスト、移行、運用、保守、データセンター、回線、クラウドサービス利用料については明確に分割することとし、また、年度毎でも分割すること。

内訳項目の細目とその金額が明確な内訳資料を作成し提出すること。

2.7.　本県からの提供資料

既存共通機能基盤（統合サーバ、及び、既存リモート保守環境）に係る構成詳細や公開情報等については、以下の資料（ア～エ）を参照すること。なお、以下の資料で提供されていない設計構成情報、ハードウェア・ソフトウェア構成に係る情報、監視・運用・保守に係る情報については、競争入札参加資格確認申請により有資格者であることが確認され、守秘義務に関する誓約書を提出した者に対して開示することが可能である。

ア　参考資料 1「統合サーバの利用について」
　既存統合サーバの設計構成情報、ハードウェア・ソフトウェア構成に関する情報

イ　参考資料 2「統合サーバ利用ガイドライン_ver1.2」
　既存統合サーバを利用する情報システム受託事業者向けの資料

ウ　参考資料 3「リモート保守環境の利用について」
　既存リモート保守環境の設計構成情報、ハードウェア・ソフトウェア構成に関する情報

エ　参考資料 4「リモート保守環境利用ガイドライン_ver1.2」
　既存リモート保守環境を利用する情報システム受託事業者向けの資料

3. 調達全般に関する共通要件

3.1. プロジェクト管理要件

3.1.1. プロジェクトの体制

本業務のプロジェクト体制に関する要件は以下のとおりである。

ア 受託事業者は、本業務の遂行を確実とする体制（支援体制を含む）を確保していること。

イ 作業について十分な知識を有するものが責任ある立場でプロジェクトを実施すること。

ウ 作業に従事する者が、本県、及び、関係者と充分な協力が図れるような体制とすること。

エ 最適化された本システムの設計・構築を実現するため、本システムの基本設計に関して、本システムで利用する仮想化ソフトウェア等にかかる開発企業等に対して問い合わせ等が可能なこと。

3.1.2. プロジェクト管理等

本業務のプロジェクト管理に関する要件は以下のとおり。

ア 受託事業者は業務計画書を作成のうえ、本県に提出し、本県の承認を得たうえで業務を実施すること。

イ 原則として、本県と合意した業務計画書に従って作業を実施すること。

ウ プロジェクトの遂行に当たり、業務計画書の内容に変更が必要となる場合は、本県と協議し、承認を得ること。また、下表「プロジェクト管理項目」のとおり、進捗管理、品質管理、変更管理を徹底すること。

表 3.1.2 プロジェクト管理項目

管理項目	管理内容
進捗管理	・業務計画策定時に定義したスケジュールに基づく進捗管理を実施すること。 ・受託事業者は、実施スケジュールと現状との差を把握したうえで、進捗の自己評価を実施し、月例報告会において本県に報告すること。 ・進捗、及び、進捗管理に是正の必要がある場合は、その原因、及び、対応策を明らかにし、速やかに是正の計画を策定し、本県の承認を得ること。

管理項目	管理内容
品質管理	・業務計画策定時に定義した品質管理方針、及び、品質管理基準に基づく品質管理を実施すること。 ・受託事業者は、品質基準と現状との差を把握したうえで、品質の自己評価を実施し、各工程完了報告会において本県に報告すること。 ・品質、及び、品質管理に是正の必要がある場合は、その原因と対応策を明らかにし、速やかに是正の計画を策定し、本県の承認を得ること。
変更管理	・仕様確定後に仕様変更の必要が生じた場合において、受託事業者はその影響範囲、及び、対応に必要な工数等を識別した上で、変更管理会議を開催し、本県と協議のうえ対応方針を確定すること。

エ　プロジェクト全般の品質状況を監査する品質管理体制を整え、品質管理責任者を設置すること。

オ　必要に応じて適宜ミーティング等を実施し、本県に対し報告、及び、作業内容の説明・協議を行うこと。

カ　全ての作業において、本県が提供した、個人情報を含む業務上の情報は細心の注意をもって管理し、第三者に開示、又は、漏洩しないこと。また、漏洩しないために必要な措置を講ずること。

3.2.　責任分界点

本県が指定する三重県情報ネットワーク用ラック内の L2/L3 スイッチの接続インターフェースまでを受託事業者の責任分界点とする。責任分界点までの全ての機器とラックの準備、及び、配線を受託事業者の責任で行うこと。なお、下図「責任分界点」については、三重県情報ネットワークに接続された IDC1 を想定したものであるが、他の IDC や本業務で整備する回線等についても、同様に本県の既存機器との接続点までを責任分界点とする。

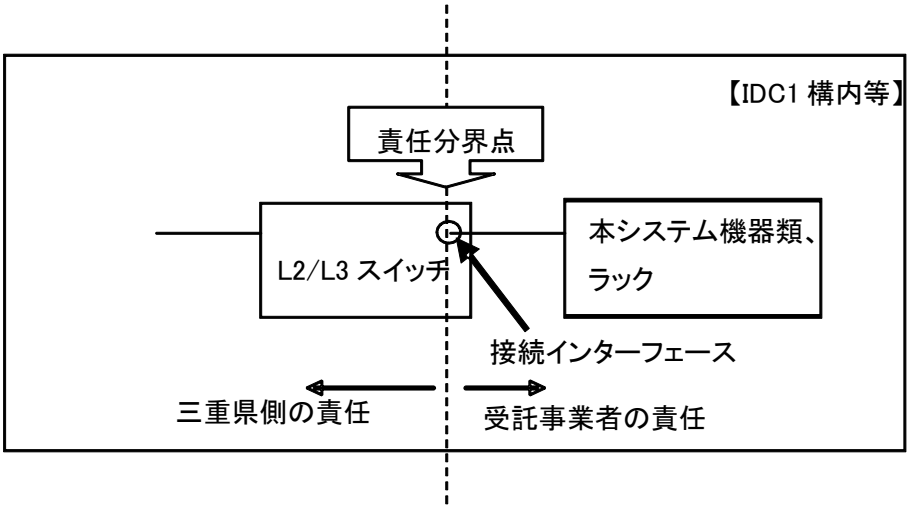

図 3.2 責任分界点

3.3. 想定スケジュール

「三重県共通機能基盤再構築及び運用保守業務委託」における想定スケジュールは以下のとおりである。

受託事業者は、運用開始までの作業スケジュールを県と協議のうえ、決定すること。

① 設計 : 契約締結日～令和 7 年 3 月 31 日
② 構築 : 令和 7 年 4 月 1 日～令和 7 年 6 月 30 日
③ テスト稼働 : 令和 7 年 7 月 1 日～令和 8 年 3 月 31 日
④ 移行 : 令和 7 年 7 月 1 日～令和 8 年 3 月 31 日
⑤ 運用保守 : 令和 8 年 4 月 1 日～令和 14 年 3 月 31 日
⑥ クラウド利用 : 令和 7 年 7 月 1 日～令和 14 年 3 月 31 日

年 月	令和 6 年	令和 7 年			～	令和 8 年		～	令和 14 年
		1～3	4～6	7		3	4		3
①設計	→	→	⇢						
②構築		⇢	→						
③テスト稼働				→	→	→			
④移行				→	→	→			
⑤運用保守							→	→	→
⑥クラウド利用				→	→	→	→	→	→

図 3.3 想定スケジュール

「①設計」の工程では、「②構築」以降の工程で必要になる全ての設計（基本設計、詳細設計）を行うこと。

「②構築」の工程では、機器、及び、ソフトウェア等の調達、納入、設置、構築、設定、テスト等の業務を行うこと。

「③テスト稼働」の工程では、段階的な移行が可能な状態にするとともに、移行した各情報システムの安定運用を行うこと。

「④移行」の工程では、移行が必要な情報システムについて移行作業を行うこと。

「⑤運用保守」の工程から本システムの本格稼働となるため、安定的な運用を行うこと。

「⑥クラウド利用」の工程では、必要なクラウドサービスの利用ができること。

3.4. 他の受託事業者との調整

ア　本業務の履行上、三重県情報ネットワーク受託事業者、及び、既存共通機能基盤~~統合サーバ~~受託事業者等と調整等が必要となる場合は、受託事業者の責により調整すること。なお、当該調整に関する費用を本県に請求することはできない。

イ　他の受託事業者が導入した機器等について、本業務を実施するうえで設定変更等が必要となる場合は、本県の承認後、それらの機器を所管する受託事業者と協議等を実施したうえで、設定変更内容に関する設計を受託事業者が主体的に実施すること。また、これら設計については、本県、及び、他の受託事業者に説明を行い、設定変更内容についての承認を得ること。

ウ　実際の設定変更作業は他の受託事業者との契約の範囲内で本県を通じて依頼が可能だが、契約の範囲を越える内容については、受託事業者の責により実施すること。なお、当該調整に関する費用を本県に請求することはできない。

エ　契約の範囲の目安として、日常的に発生しうる設定変更や協議への参加、問い合わせ等については対応可能である。ただし、作業時の立会においては、受託事業者ごとに対応が分かれるので注意すること。

オ　本業務の履行期間中において、三重県情報ネットワークの再構築が行われる可能性があり、その際、共通機能基盤の設定変更や立会い等が必要になる場合がある。その場合、三重県情報ネットワーク受託事業者との調整について、本業務の範囲内として行うものとする。なお、三重県情報ネットワークの再構築に伴い、サーバ等のハードウェアの増設が必要になる場合は、本業務の範囲外とする。

4. 納品物件

4.1. ハードウェア・ソフトウェア

本業務に必要な全てのハードウェア・ソフトウェア（ライセンス、又は、サブスクリプション契約による利用権等）を納入すること。

ア　本システムは、履行期間内は保守可能であることを前提とする。契約期間中に本システムで利用している製品のサポートが終了する場合は、受託事業者の責において後継製品や同等の性能を持った代替製品への移行を行い、継続してサポートが受けられるように対応を行うこと。その場合、当該製品がサポート終了を迎える前に、本県に代替品の説明を実施したうえで承認を得ること。

イ　本システムを確実に稼働させるために必要なソフトウェア（パッケージ、ミドルウェア含む）について、各要件に基づき選定し、ソフトウェア仕様、及び、構成案を提示すること。その際、本システムのソフトウェアライセンスが過大・過小とならないよう、適切なライセンス体系に基づく構成で提案すること。

4.2. ドキュメント

受託事業者は以下のドキュメントを指定された期日までに、本県に納品すること。納品方法は、電子媒体と紙面での納品を各 1 部とする。

なお、電子媒体のファイル形式については、本県と事前に協議を行い、決定すること。

4.2.1. 業務計画書

業務計画書の内容は以下のとおりとする。業務計画書の内容うち、設計構築等に関するものは契約締結後 10 開庁日以内に提出すること。

ア　業務スケジュール

イ　業務遂行体制・業務従事者名簿

ウ　機器及びソフトウェア等一覧

エ　進捗管理基準

オ　品質管理基準

カ　変更管理基準

キ　工程完了判定基準

ク　コミュニケーション計画

4.2.2.　　各種設計書、完成図書及び報告書

受託事業者は各工程の計画、成果を示すドキュメントを作成すること。

想定するドキュメントは以下のとおりである。

ただし、各工程に着手する前に、当該工程において作成するドキュメントに関し、本県と協議すること。また、内容に関しては、レビュー会を設けて本県に対し十分な説明を行い、内容の承認を得てから納品すること。特に、設計、構築、移行等の重要工程完了時の納品物については、工程完了判定会議を開催し、県の承認を得ること。

表 4.2.2 納入ドキュメント一覧

フェーズ	No.	成果物	提出期限
設計	1	基本設計書	令和 7 年 3 月
	2	詳細設計書	令和 7 年 3 月
	~~32~~	構築設計書	令和 7 年 3 月
	~~43~~	移行設計書	令和 7 年 3 月
	~~54~~	テスト設計書	令和 7 年 3 月
	~~65~~	運用保守設計書	令和 7 年 3 月
構築	~~6~~	~~詳細設計書~~	~~令和 7 年 6 月~~
	7	テスト結果報告書	令和 7 年 6 月
	8	ラック配置図	令和 7 年 6 月
	9	物理配線図	令和 7 年 6 月
	10	機器及びソフトウェア等一覧（構築完了後）	令和 7 年 6 月
	11	運用保守手順書（リストア手順書を含む）	令和 7 年 6 月
	12	移行計画書・手順書	令和 7 年 6 月
	13	操作説明書	令和 7 年 6 月
	14	共通機能基盤利用者向け説明資料等	令和 7 年 6 月
	15	運用保守体制表	令和 7 年 6 月
テスト稼働～	16	運用保守報告書（課題管理表を含む）	テスト稼働開始後から契約終了まで、月次で提出すること
	17	運用保守作業報告書（障害記録を含む）	テスト稼働開始後、運用保守作業対応の都度、提

			出すること
	18	品質報告書	各年度末
随時	19	移行完了報告書	各情報システムの移行完了後、速やかに提出すること
	20	会議・打合せ議事録 ※対象は、契約終了までの全ての会議体。	会議終了後、速やかに提出すること（次回会議まで、遅くとも１週間以内に提出すること）

5. システム設計に関する要件

5.1. 既存共通機能基盤の構成

5.1.1. 全体構成

既存共通機能基盤は、統合サーバ、及び、リモート保守環境により構成されている。既存共通機能基盤にかかる全体構成は、以下のとおり。

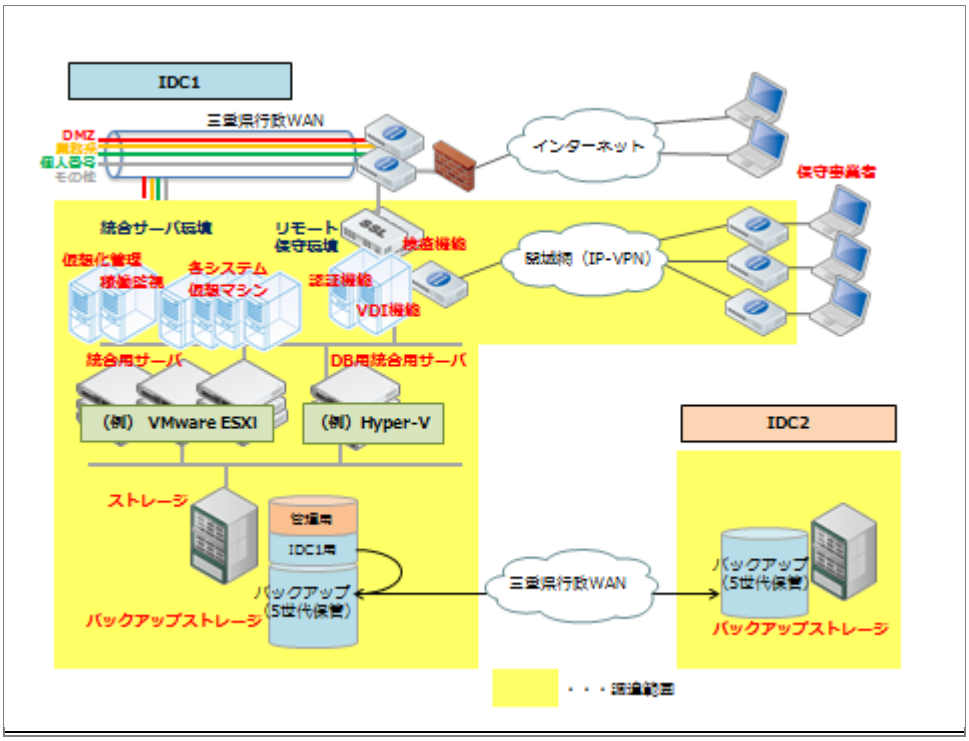

図 5.1 既存共通機能基盤の全体構成

5.1.2. 既存統合サーバの概要

既存統合サーバの概要は、以下のとおり。

なお、既存統合サーバの詳細は、参考資料 1「統合サーバの利用について」、参考資料 2「統合サーバ利用ガイドライン_ver1.2」を参照すること。

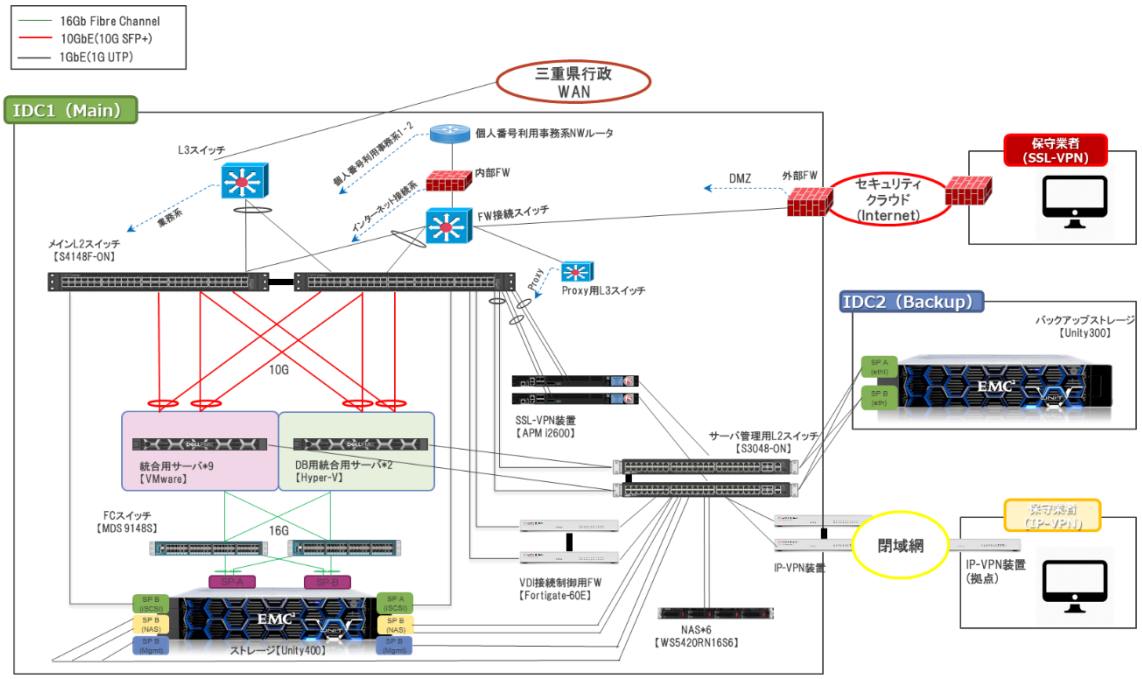

図 5.2 既存統合サーバの全体概要

表 5.1 既存統合サーバにおける機器構成とその概要

分類	概要
仮想化ソフトウェア	・ 通常利用向け統合用サーバの仮想化ソフトウェアとして VMware 社の vSphere ESXi 6.7 Update2、DB 用統合用サーバの仮想化ソフトウェアとして Microsoft 社の Hyper-V7.0 を採用している。 ・ DB 用統合用サーバにおいて、Oracle 社製データベースソフトウェアである、OracleDB を利用可能な構成としている。（通常利用向け統合用サーバでは OracleDB の利用は禁止されている。）
仮想化管理サーバ/統合サーバ管理ソフトウェア	・ vSphere で構築を行っている通常利用向け統合用サーバを管理するための仮想化管理サーバは、vCenter を導入した仮想マシンで、構築している。（以下、「仮想化管

	理サーバ（vCenter)」と言う。） ・ Hyper-V で構築を行っている DB 用統合用サーバを管理するための仮想化管理サーバは、SCVMM を導入した仮想マシンで、構築をしている。(以下、「仮想化管理サーバ（SCVMM)」と言う。） ・ それぞれの仮想化管理サーバにおいて、統合用サーバの障害時に別の統合用サーバ上で自動起動させるための HA 機能が利用できるようにしている。(HA 機能：統合用サーバで障害等が発生した場合に、影響を受けた仮想マシンを異なる統合用サーバ上で再起動させることで、ダウンタイムを最小化できる高可用性機能のこと）
統合用サーバ（通常利用向け統合用サーバ、DB 用統合用サーバ)	・ 通常利用向け統合用サーバは 9 台（8 台＋HA 機能用 1 台)、DB 用統合用サーバは 2 台（1 台＋HA 機能用 1 台）で構成している。 ・ 接続先となるセグメントとして、インターネット接続系ネットワーク、LGWAN 接続系ネットワーク、個人番号利用事務系ネットワークにおけるそれぞれの業務端末接続用セグメント、サーバセグメント、DMZ セグメント等、各情報システムからの要望に応じてさまざまなネットワークセグメントで利用可能な仮想マシンを提供している。 ・ CPU、ディスクのオーバーコミットは許可しているが、メモリについてのオーバーコミットは許可していない。
メインストレージ/バックアップストレージ	・ メインストレージは、津市内データセンターに設置している。(実容量 メイン領域 140TB、バックアップ領域 150TB) ・ メインストレージは、メイン領域とバックアップ領域で構成されており、メイン領域に通常利用向け統合用サーバ、DB 用統合用サーバそれぞれの仮想マシン本体のデータを格納するとともに、メイン領域と物理的に独立したバックアップ領域にバックアップデータについて格納している。 ・ メイン領域には、各仮想マシンで利用する業務データ保存用領域についても用意され、格納している。

	・ バックアップストレージは、メインストレージとは別の筐体とし、構築当初は志摩市内のデータセンターに設置していたが、現在は、津市内データセンター（メインストレージと同一建物内）に設置している。（実容量150TB） ・ バックアップストレージは、メインストレージからのレプリケーションデータを格納している。 ・ バックアップソフトウェアとして、Veeam 社の Veeam Backup & Replication を利用しており、バックアップサーバにて、各仮想マシンのバックアップを一元管理している。各仮想マシンには、仮想マシン提供時にバックアップ用エージェントソフトウェアをインストールしている。 ・ バックアップについては、重複排除技術を用いて容量削減を行っている。
稼働監視サーバ/稼働監視ソフトウェア	・ 共通機能基盤における各種稼働監視を行うため、仮想化管理サーバ（vCenter）、仮想化管理サーバ（SCVMM）による稼働監視機能を利用するとともに、別途、稼働監視サーバを仮想マシンとして構築し、稼働監視ソフトウェアとして、NTT データ社製 Hinemos を利用して稼働監視を行っている。
ログ収集サーバ	・ 各種ログを収集するため、ログ収集サーバ（syslog サーバ）を導入し、3 か月分については閲覧可能状態で保存し、3 か月経過したものから、メインストレージへアーカイブ形式で保存している。
VDI 接続制御用ファイアウォール	・ リモート保守環境で利用する VDI 環境を制御するため、VDI 接続制御用ファイアウォールを導入している。また、同ファイアウォールにて、統合用サーバ、ストレージ等についてもアクセス制御を行っている。（三重県情報ネットワーク上の他のセグメントからのアクセスを制限している。）
Active Directory	・ 統合サーバ、及び、リモート保守環境におけるユーザ管理、及び、権限管理を実施するため、Active Directory を導入している。（ドメイン名：miekiban.local）

	・ 三重県情報ネットワーク上に行政利用用として構築済みの別ドメイン（ドメイン名：mieken.jp）と信頼関係を設定し、mieken.jp ドメインユーザ等を参照できるようにしている。
NAS	・ 大容量データの内、バックアップを取得する必要がないデータの保存場所として、6 台の NAS を用意し、各情報システムに提供している。(実容量 1 台当たり 6TB　1 システムが利用中)
L2 スイッチ	・ 既存統合サーバ、および、リモート保守環境を構築するための機器を接続するスイッチとして、L2 スイッチを導入している。 ・ L2 スイッチは二重化されており、各機器等への接続は経路が冗長化されている。 ・ 既存共通機能基盤内のネットワークについては、10Gbps での通信を行っている。

5.1.3.　既存リモート保守環境の概要

既存リモート保守環境における「インターネット VPN 接続」「IP-VPN 接続」におけるそれぞれの概要は、以下のとおり。

なお、既存リモート保守環境の詳細は、参考資料 3「リモート保守環境の利用について」、参考資料 4「リモート保守環境利用ガイドライン_ver1.2」を参照すること。

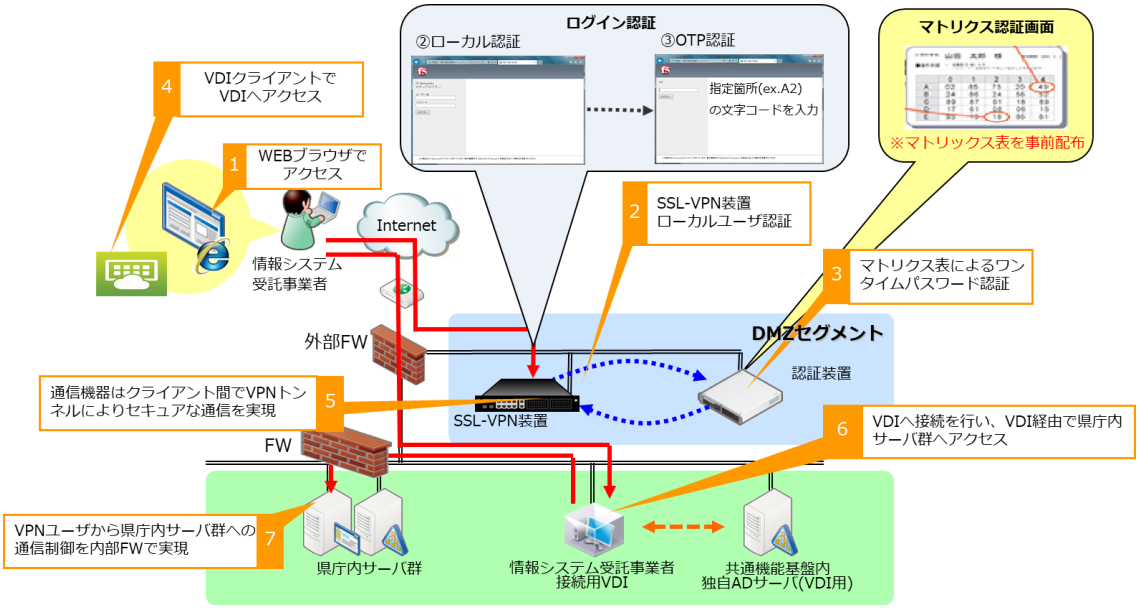

図 5.3 既存リモート保守環境（インターネット VPN 接続）の全体概要

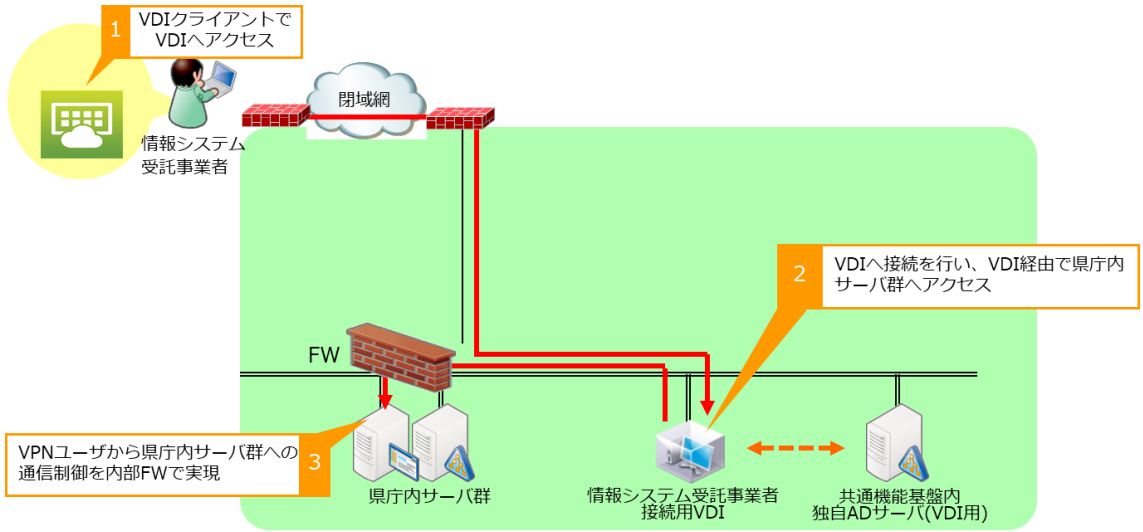

図 5.4 既存リモート保守環境（IP-VPN 接続）の全体概要

表 5.2 既存リモート保守環境における機器構成とその概要

分類	概要
全体構成	・ 各情報システム受託事業者が保守拠点からリモート保守先のサーバ等へアクセスを行うためのリモート保守環境として、「インターネット VPN 接続」「IP-VPN 接続」による 2 系統のリモート保守環境を構築している。 ・ 通常はインターネット VPN 接続方式を利用することとしているが、個人番号利用事務系ネットワークへ接続する場合のみ、IP-VPN 接続方式を利用することとしている。（個人番号利用事務系ネットワークへのアクセスは、インターネット VPN 接続方式によるリモート接続を認めていない。） ・ インターネット VPN 接続、IP-VPN 接続の双方において、一旦、情報システム受託事業者接続用の VDI 環境にログインしたうえで、リモート保守先のサーバ等へ画面転送方式によるアクセスを行っている。
SSL-VPN 装置	・ インターネット VPN 接続を行うため、SSL-VPN 装置を導入している。 ・ SSL-VPN 装置にて、情報システム受託事業者が利用する接続端末の、端末固有情報、OS のセキュリティパッチ適用状況、マルウェア対策ソフトウェアの更新状況等について確認（検疫処理）を行っている。

IP-VPN 接続用ネットワーク機器	・ IP-VPN 接続で利用する閉域網の両端として、IDC1 と IP-VPN 接続によるリモート保守を利用する各情報システム受託事業者における保守拠点の双方に IP-VPN 接続用ネットワーク機器を設置し、セキュリティを確保した通信を行っている。
IP-VPN 接続用貸し出し端末/閉域網	・ IP-VPN 接続による接続を行うため、情報システム受託事業者向けに閉域網を提供している。 ・ IP-VPN 接続で利用する端末として、本県から「IP-VPN 接続用貸し出し端末」の貸し出しを行っている。(本端末以外の端末からの接続を認めていない。)
VDI 環境	・ インターネット VPN 接続、IP-VPN 接続に関わらず、リモート保守環境を利用してリモート保守先のサーバ等へアクセスする場合、サーバ等へ直接アクセスするのではなく、VDI 環境を経由してアクセスしている。 ・ VDI 環境からリモート保守先のサーバ等へのアクセスは、原則として、統合サーバにおける仮想化管理ソフトウェアのコンソール機能から画面転送方式によるアクセスを行うことで、安全性を確保している。(一部、直接アクセスも許可している。) ・ VDI 環境は、統合サーバ上に VMware 社 VMware Horizon により構築している。
認証装置	・ インターネット VPN 接続による接続時においては、SSL-VPN 装置での端末チェック後、又、IP-VPN 接続に接続時においては、利用開始時に、認証装置による利用者認証を行っている。 ・ 認証は ID/パスワードによる認証に加えて､マトリクスコードによるマトリクス認証を行っている。

5.1.4.　三重県情報ネットワークの概要

三重県情報ネットワークは、令和元年度において、既存の三重県行政 WAN を拡張する形で再構築を行っている。また、令和 4 年度、令和 5 年度においては構成等の変更を行った。(アからエは令和元年度に実施、オからキは令和 4,5 年度に実施)

ア　既存の三重県行政 WAN（インターネット接続系ネットワーク、LGWAN 接続系ネットワーク、個人番号利用事務系~~接続系~~ネットワーク）の構成を踏襲した。(三層モデル：αモデル)

イ　各市町とデータセンター等を接続するため、三重県内の広域ネットワークとしてネットワークの拡張を行った。さらに、県内各拠点を接続するための主回線についても見直しを行った。

ウ　災害対策として、防災ネットワークと相互接続し、有線回線/バックアップ回線の切断時でも通信ができるようにした。さらに、各総合庁舎で無線 LAN が利用できるようにした。

エ　ライフワークバランス対策として、モバイルワーク環境の構築の他、ファイルサーバやファイル交換システムを構築した。

オ　α モデルからβ’モデルへの移行（業務端末を LGWAN 接続系ネットワークからインターネット接続系ネットワークへ移動）を行った。

カ　無線 LAN の拡張（本庁＋総合庁舎の 1 部分　→　本庁＋4 周辺庁舎＋総合庁舎（全フロア））を行った。

キ　DX 推進基盤（Microsoft 社 Office365 の利用開始、Salesforce 社 Slack の利用開始等）の導入を行った。

ク　三重県情報ネットワークの概要については、別紙２「三重県情報ネットワーク論理ネットワーク概要図」を参照すること。

ケ　既存共通機能基盤の構築時において、サーバ機器類を設置するデータセンター（津市内 IDC1）と、レプリケーション用のバックアップストレージを設置するデータセンター（志摩市内 IDC2）を別の場所とすることで、大規模災害時においても同時に被災しないような構成としていたが、運用期間中において、IDC2 が廃止されることになったことに伴い、IDC2 に設置していた機器は IDC1 に移設を行った。

5.1.5.　運用保守業務

既存共通機能基盤における運用保守業務は、既存の共通機能基盤にかかる受託事業者、共通機能基盤担当職員で対応を行っている。

運用保守業務の内、「情報システム担当職員、情報システム受託事業者からの問い合わせ、作業依頼対応にかかる一次受付」については共通機能基盤担当職員で実施している。

5.1.6.　共通機能基盤の利用状況

既存共通機能基盤の構築時において、今後の利用状況等の調査を踏まえ、十分なキャパシティプランニングを行い、必要となるスペック等の計算を行った。しかし、運用 2 年目（令和 3 年度時点）で統合用サーバのメモリの他、ライセンス数等の不足が顕在化したため、令和 4 年度において、増強等を行った。

現在の利用状況は、別紙３「既存共通機能基盤における利用リソース一覧」を参照すること。

5.2.　システム設計に関する基本方針

本業務における設計業務において、以下の基本方針を踏まえて設計を行うこと。

ア　本業務において、共通機能基盤の再構築を行うこととしているが、原則として、既存システムにおけるシステム構成を踏襲すること。なお、本仕様書に記載された各種要件を満たすことを条件として、他の構成による再構築も可とするが、各種テストや移行にかかる作業の他、利用者向け説明資料（手順書、利用マニュアル、ガイドライン等）の作成等にも時間がかかることが想定されるため、十分考慮して対応を行うこと。また、それらの構成を実現するための費用等についても本業務の範囲内となるので注意すること。

イ　既存統合サーバの再構築を実施すること。統合用サーバとして、既存統合サーバと同様に 2 系統（通常利用向け統合用サーバ、DB 用統合用サーバ）の構成とし、原則として、既存統合サーバで利用している仮想化ソフトウェアの後継ソフトウェアを採用すること。

ウ　既存リモート保守環境の再構築を実施すること。接続方式として、インターネット VPN 接続、及び、IP-VPN 接続が引き続き利用できること。

エ　IDC1 に本システムに必要となる全ての機器等を設置すること。IDC2 にはレプリケーション用バックアップストレージを設置することとし、接続するための専用回線、ネットワーク機器の構築、及び、運用保守についても本業務に含めること。なお、IDC1、又は、IDC2 に設置する機器等について、「5.4.12.クラウドサービスに関する詳細要件」にて後述するクラウドサービス上に構築することで、機器の設置自体を不要とする構成も可とするが、クラウドサービスを利用するために必要となる全ての費用についても、本業務の範囲内に含めること。

オ　移行作業として、既存統合サーバ上の仮想マシン全てや、既存リモート保守環境を利用中の各情報システム受託事業者に設置済みの端末からのアクセス等、全てのサービスについて移行を行うこと。なお、移行作業は、既存システムの運用保守期限である令和 8 年 2 月末日まで（令和 8 年 3 月は既存機器の撤去期間として予定している）に終了させること。既存統合サーバからの移行手法については仮想化ソフトウェアメーカーがサポートする移行ツール等を使用するなど、円滑な移行ができるようにすること。また、移行作業は平日夜間（17:15～翌 6:00）と土休日のみでの作業実施を原則とすること。なお、既存システムに影響のない作業の場合は、平日、日中時間帯での作業も可とする。

カ　システム障害時等のデータ保護を目的とし、バックアップを行うこと。バックアップには圧縮機能や重複排除機能を採用することで、ネットワーク負荷の軽減、バックアップ時間の短縮、バックアップデータ容量の削減等を行うこと。

キ　データ等のバックアップにかかる新機能として、ランサムウェア等によるバックアップデータの消失を防ぐため、書き換え禁止措置を行うこと。

ク　新機能として、「5.4.12. クラウドサービスに関する詳細要件」にて後述するクラウドサービスの利用による統合サーバを構築し、利用できるようにすること。なお、クラウドサービスを統合サーバとして利用するために必要となる費用についても、本業務の範囲内に含めること。

ケ　部品の 2 重化、機器の 2 重化など、各機器の障害時を想定した冗長性を確保すること。

コ　本システムの全体概要として、既存の共通機能基盤の構成を踏襲することを基本方針とするが、本仕様を満たしたうえでより効率的な構成がある場合は本県の承認を得たうえで、変更してもよいものとする。

サ　使用するソフトウェアはシステムへの影響が無い限り、納入時点での最新のセキュリティパッチ等の適用を行い、セキュリティホール対策が完了したものを~~うえで~~納入すること。

シ　本県がシステムに不要と判断するソフトウェア・サービスについては停止させる、又は、インストールしないこと。

ス　本業務について、契約書、及び、本仕様書に明示されていない事項でも、その履行上当然必要な事項については、受託事業者が責任を持って対応すること。

セ　本仕様書に記載されている全ての業務に対し、いかなるケースにおいても本県に対し、別途費用を請求することはできない。ただし、本県の要求仕様変更による追加費用については別途協議を行うこととする。

ソ　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、本県と協議のうえ、定めるものとする。

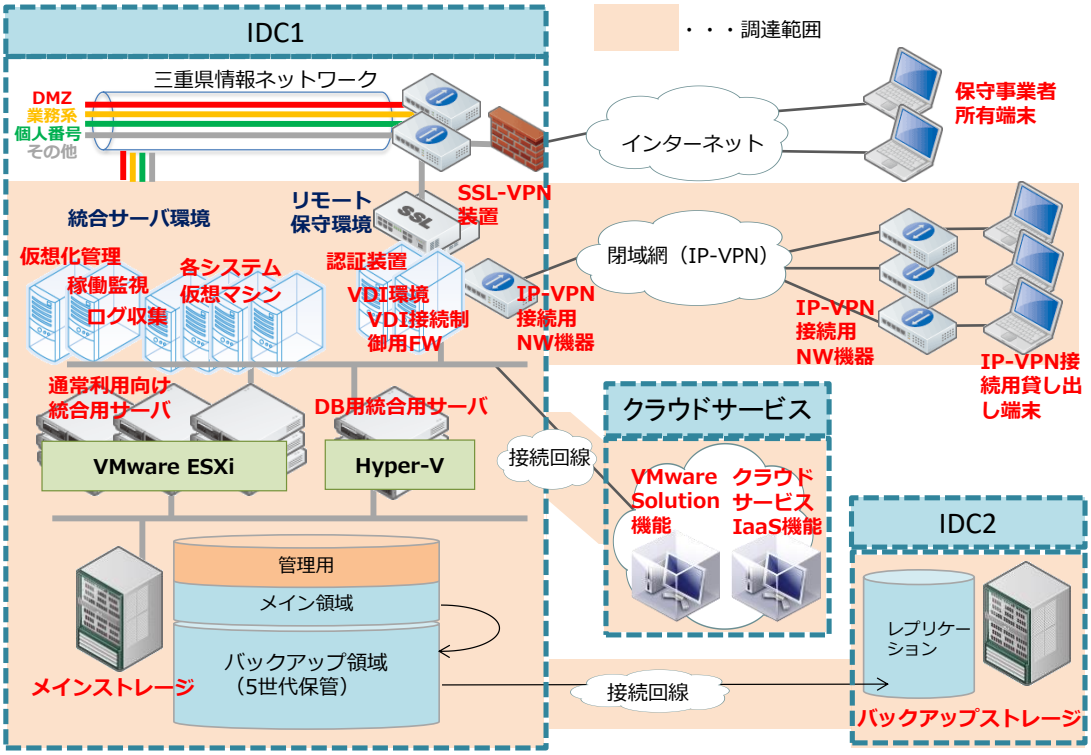

図 5.5 本システムの全体概要

5.3. 設計業務に関する要件

設計業務に関する要件は以下のとおり。

5.3.1. 設計業務に関する共通要件

設計業務について、以下の要件を満たすこと。

ア 設計業務を実施する際は、既存共通機能基盤の設定、及び、構成を理解したうえで各種設計を行うこと。

イ 設計業務は、契約開始後より令和 7 年 3 月末日までに実施し、実施した設計毎にそれぞれの設計書を成果物として作成すること。また、作成した設計書は、本県に対しレビューを実施し、本県の承認後、提出すること。

ウ 設計として、基本設計、詳細設計、構築設計、移行設計、テスト設計、運用保守設計等、必要な設計を行うこと。

エ 設計時において、最適な設計を実施できるよう、仮想化ソフトウェア製造元のエンジニアへ技術問合せが行える体制、又は、それに準じる体制を確保すること。

5.3.2.　基本設計、詳細設計にかかる詳細要件

基本設計・詳細設計として、以下の要件を満たすこと。

ア　本システムの全体構成や納品する機器、及び、ソフトウェア一覧、構築期間、移行期間、運用保守期間における業務内容等、本業務を実施するうえで必要となる基本的な内容等について基本設計を行うこと。

イ　本業務で利用可能となるクラウドサービスについてどのような形で構築し、利用できるようにするかについても、基本設計に含めること。

ウ　本業務で導入する機器やソフトウェア等について、利用方法等にかかる詳細な検討を行ったうえで、各種設定を行うために必要となる詳細設計を行うこと。

5.3.3.　構築設計にかかる詳細要件

構築設計として、以下の要件を満たすこと。

ア　本業務で導入する機器等について、構築作業を行うために必要となる構築設計を行うこと。

イ　各機器の搬入、設置、本システムに必要なOSのインストール、ソフトウェアのインストール・設定作業は原則として全て受託事業者が実施すること。

ウ　設置場所への納入、設置作業、配線作業並びにネットワークへの接続作業の実施においては、本県、又は、関係者と事前に協議を行い設計に反映させること。

エ　既存共通機能基盤、又は、三重県情報ネットワークの停止を伴う作業は、原則、認められないので注意すること。ただし、避けられない場合は、閉庁日もしくは夜間での限られた時間での実施となるため、注意すること。

オ　三重県情報ネットワークのファイアウォールの通過許可ルールの追加・変更等、他の事業者に作業を依頼する必要がある場合は、作業指示書等を作成したうえで、本県に提出し承認を得ること。

カ　各機器のシステムログを取得・保存できるようにすること。また、各機器において、時刻同期を行うことで、ログの出力時刻が適切に記録されるようにすること。

キ　本システムで提供する各種サービスは、既存共通機能基盤と並行して提供することが可能と想定しているが、既存共通機能基盤で提供している各種サービスの停止を伴う構築作業が発生する場合は、平日夜間（17:15～翌 6:00）、又は、閉庁日での実施を基本とすること。なお、各種サービスの停止を伴わない場合は、平日、日中時間帯での作業を可とする。

ク　本システムの構築後、既存共通機能基盤から本システムへの移行作業を行うために、既存共通機能基盤において、バージョンアップ等の設定変更等が必要になった場合、既存共通機能基盤にかかる受託事業者の了解を得て、実施することは可能だが、バージョンアップ後から既存共通機能基盤の利用を完全に停止するするまので間においても既存の共通機能基盤にて適切なサポートが受けられるようにすること。

5.3.4.　移行設計にかかる詳細要件

移行設計として、以下の要件を満たすこと。

ア　本システムの構築後、既存共通機能基盤から本システムへの移行作業を行うために必要となる移行設計を行うこと。

イ　移行対象として、既存共通機能基盤が各情報システムに対して提供している全ての機能を対象とすること。

ウ　移行作業開始前までに、情報システム担当職員、及び、情報システム受託事業者を対象とした移行作業説明会を実施すること。また、説明会に必要となる各情報システム担当職員、及び、情報システム受託事業者向け資料についても作成を行うこと。

エ　移行作業は、令和 7 年 7 月から令和 8 年 2 月末までの間に確実に実施できること。

オ　移行期間中において、既存環境からの移行だけでなく、共通機能基盤の新規利用についても想定されるため、必要に応じて対応が可能なこと。

カ　統合サーバにおける仮想マシンの移行については、V2V(Virtual to Virtual)を基本とし、計画的、かつ、スムーズな移行ができるようにすること。なお、既存共通機能基盤と本システムとのソフトウェアバージョン違い等からスムーズな移行ができないことが想定される場合は、必要に応じて、仮想化ソフトウェアメーカーのサポートする仮想マシン移行ツールの利用についても検討すること。

キ　統合サーバにおける仮想マシンの移行については、極力、アプリケーションの整合性を満たした移行方法を採用すること。なお、移行後に各業務システム側にて動作確認を依頼する予定だが、動作に異常がある場合は、再移行を行うなど、可能な範囲で支援を行うこと。

ク　統合サーバにおける仮想マシンの移行については、バックアップや監視用エージェントソフトウェア、仮想化ソフトウェア用エージェントソフトウェア等にかかる変更(再設定)など、仮想マシン側で設定変更等が発生する場合は、可能な限り、受託事業者側で対応を行なうこと。

ケ　仮想マシン上で動作している情報システムに対して、情報システム担当職員や情報システム受託事業者に作業等を依頼する場合は、手順書作成の他、必要

な支援を行うこと。また、過度の負担とならないよう留意すること。

コ　統合サーバ上の仮想マシンの移行において、異なる仮想化ソフトウェア間（vSphere から Hyper-V、又は、その逆、又は、vSphere/Hyper-V からそれら以外の仮想化ソフトウェア）の移行については移行後における仮想マシンの動作保証がされないため、原則として不可とするが、多数の実績があり、かつ、移行用ツールが提供されている等の場合は、情報システム担当職員、及び、情報システム受託事業者の許可を得た場合のみ可とする。

サ　既存共通機能基盤を利用する情報システムについて、情報システム担当職員、及び、情報システム受託事業者と協議を行い役割分担や費用負担等について、承認を得た場合に限り、仮想マシンの再構築等による移行も可とする。

シ　長時間の停止が許されない仮想マシンの移行作業は、平日夜間（17:15～翌6:00）、又は、閉庁日での実施を基本とすること。その他の仮想マシンについては、平日、日中時間帯での作業も可とするが、できる限り業務に影響のないよう配慮すること。

ス　サンプルとしていくつかの仮想マシンに対して移行テストを実施し、移行想定時間を確認すること。また、各情報システムの運用状況を踏まえ、仮想マシンの移行順序について決定すること。

セ　移行対象となるそれぞれの仮想マシンにおいて、移行作業に必要となる作業の詳細（具体的な移行日時や作業の役割分担等）を明らかにした移行計画を策定すること。

ソ　策定した移行計画については、各情報システム担当職員、及び、情報システム受託事業者に説明を行ったうえで承認を得ること。なお、各情報システム担当職員、及び、情報システム受託事業者から質問や相談があった場合は、詳細ヒアリングを実施する等により、各情報システムの移行条件を確認したうえで、移行計画へ反映させること。

タ　移行作業完了時において、仮想マシン単位で移行作業の内容や懸案事項等をまとめた移行完了報告書を速やかに提出できるようあらかじめ様式等について準備を行うこと。

5.3.5.　テスト設計にかかる詳細要件

テスト設計として、以下の要件を満たすこと。

ア　本システムにかかる各種テストを行うために必要となるテスト設計を行うこと。

イ　テスト設計後、各種テストを実施するためのテスト計画書、及び、テスト仕様書を作成すること。

ウ　テスト計画書として、単体テスト、結合テスト、総合テスト、運用テスト、性能テスト、負荷テスト、耐障害機能テスト、障害検知機能テスト、故障予兆検

知機能テスト、冗長化テスト、リストアテスト等、テストの分類、テストの目的、方法、結果の判定基準等について、それぞれ策定することとし、また、策定したテスト計画に沿って実施する必要がある詳細なテスト項目について、テスト仕様書として策定すること。

エ　障害検知機能テスト等、本システムのサービス停止を伴うテスト等については、移行作業開始以降、実施できなくなると想定されるため、移行期間開始前までに終了できるように計画すること。

オ　バックアップやリストアについて、情報システム単位のデータリストアから、ファイル単位のデータリストアまで、漏れなくテストを実施すること。また、その際、事前に作成したマニュアルや手順等についても確認を行い、運用管理期間開始後において、確実な操作が実施できるようにすること。

カ　全てのテストが問題なく終了したことを記録したテスト結果報告書を作成し、本県に対して報告を行ったうえで、承認を得ること。テスト結果報告書には、単体テスト、結合テスト、総合テスト、運用テスト、性能テスト等の実施結果を含めるものとする。

キ　テスト結果が設計内容の想定と異なる場合は、再度、設計から見直しを実施すること。

5.3.6.　運用保守設計

運用保守設計として、以下の要件を満たすこと。

ア　本システムにかかる運用保守業務を行うために必要となる運用保守設計を行うこと。

イ　共通機能基盤担当職員、情報システム担当職員、又は、情報システム受託事業者の負荷軽減や、セキュリティ・可用性の向上を見据えた、運用保守業務について設計を行うこと。

5.4.　詳細な機能要件

機能要件の詳細は以下のとおり。設計業務において、以下の機能要件を実現できるよう設計を行うこと。

5.4.1.　機器の全体構成

本システムにおける機器の全体構成について、以下の要件を満たすこと。

ア　機器構成は、原則として、既存共通機能基盤における機器構成を踏襲すること。なお、具体的には、「5.1 既存共通機能基盤の構成」における統合サーバを構成する「仮想化ソフトウェア」「仮想化管理サーバ/統合サーバ管理ソフトウェア」「統合用サーバ（通常利用向け統合用サーバ、DB 用統合用サーバ）」「メインストレージ/バックアップストレージ」「稼働監視サーバ/稼働監視ソフトウェア」「ログ収集サーバ」「VDI 接続制御用ファイアウォール」「ActiveDirectory」

「NAS」「L2 スイッチ」、リモート保守環境を構成する「SSL-VPN 装置」「IP-VPN 接続用ネットワーク機器」「IP-VPN 接続用貸し出し端末/閉域網」「VDI 環境」「認証装置」、本業務で利用を開始するクラウドサービス、等を構成要素として設計を行うこと。また、これらの機器以外に、本仕様書の要件を満たすために必要となる機器や仮想アプライアンス、追加コンポーネント等がある場合は、それらにかかる費用についても、本業務に含めること。

イ　IDC1 内における本システムのネットワーク帯域は原則として 10Gbps 以上となるようにすること。三重県情報ネットワークのスイッチからの割り当ては 1Gbps 単位であるため、必要数を見積もり、配線等を行うこと。既存共通機能基盤については、三重県情報ネットワークから 1Gbps×4 ポートの割り当てがあるが、本システムにおける必要帯域について、検討したうえで決定すること。三重県情報ネットワークが接続されているデータセンター内ラックからのラック間配線（三重県情報ネットワーク用ラックから本システム用ラックまで）についても、本業務の範囲内とする。これらのネットワークに関する構成は、下記の既存共通機能基盤ネットワーク図を参考にすること。

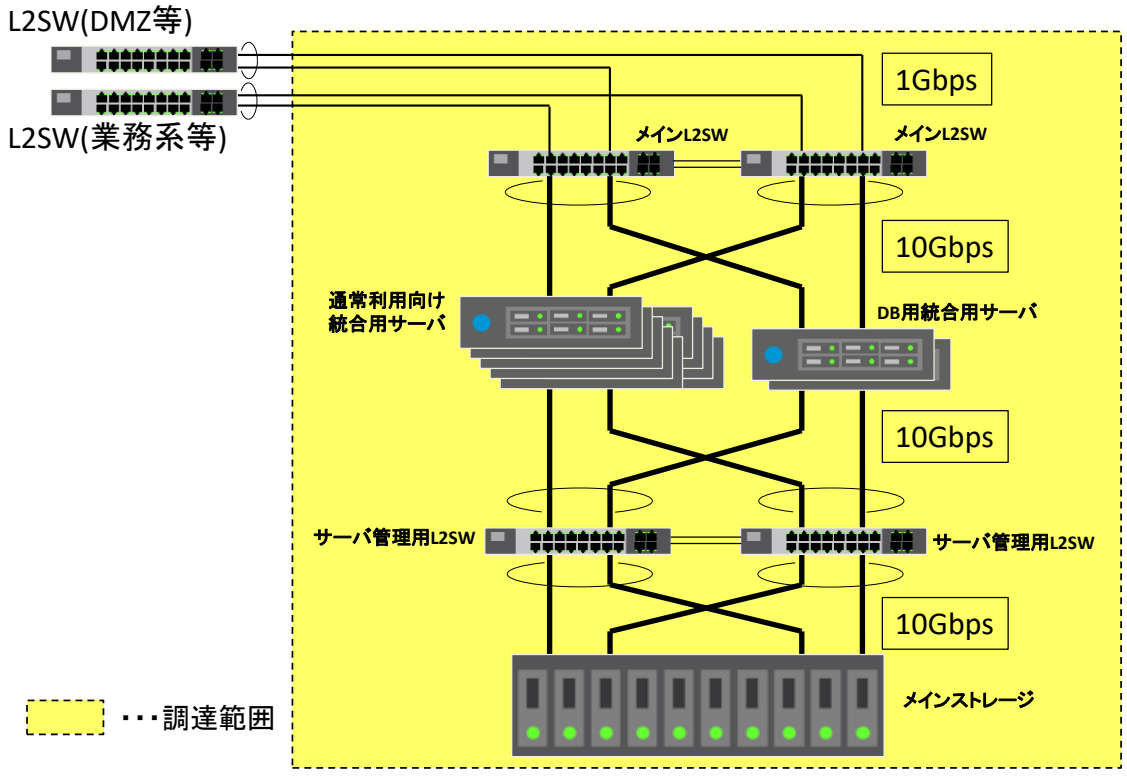

図 5.6 共通機能基盤ネットワーク図（案）

ウ　本システムにおいて、既存共通機能基盤におけるネットワークセグメント（インターネット接続系ネットワーク、LGWAN 接続系ネットワーク、個人番号利用

事務系ネットワークにおけるそれぞれの業務端末接続用のセグメント、サーバセグメント、DMZ 等）が引き続き利用できるようにすること。また、今後、利用するセグメントが増える可能性もあるため、柔軟に対応できるようにすること。

エ　既存共通機能基盤では、各仮想マシンに対して、管理用セグメントから各種管理用アクセス（通常利用向け統合用サーバにおいては、仮想化ソフトウェア管理ソフトウェア（vCenter）における vMotion や監視用通信など）が可能となるような構成にしており、また、これらのセグメントは、セキュリティ対策のため、業務で利用するセグメントからは直接通信ができない別セグメントとしている。そのため、引き続き、管理用セグメントから各種管理ができるようにするとともに、可能な限り既存の管理用セグメントにかかる構成を踏襲すること。

オ　既存共通機能基盤における機器構成として、統合用サーバを 2 系統用意するなど、OracleDB にかかるライセンスが最小限となる構成としているため、原則として、この構成を踏襲すること。なお、本仕様書にかかる要件を満たす場合に限り、既存共通機能基盤と異なる構成についても可とするが、変更に伴い発生する費用の全てについて、本業務に含めること。

カ　設計した内容は、「基本設計書」に反映させること。また、「機器及びソフトウェア等一覧」についても作成すること。

5.4.2.　仮想化ソフトウェアに関する詳細要件

本業務で利用する仮想化ソフトウェアについて、ソフトウェアライセンス、及び、機能に関する以下の詳細要件を満たすこと。なお、特に指定のない限り、通常利用向け統合用サーバ、及び、DB 用統合用サーバの双方で利用する仮想化ソフトウェアのいずれにおいても当該要件を満たすこと。

(1) ソフトウェアライセンス

ア　本環境を構築するため、仮想化ソフトウェア（契約時において最新のもの）に関するライセンス、又は、サブスクリプション契約による利用権等を必要数用意すること。使用する仮想化ソフトウェアは、原則として、既存統合サーバで利用している仮想化ソフトウェア（通常利用向け統合用サーバ VMware 社 vSphere、DB 用統合用サーバ Microsoft 社 Hyper-V）の後継ソフトウェアを採用すること。

イ　本システムにおける仮想化ソフトウェアについて十分な検討を行ったうえで、製品仕様や利用ライセンス、サブスクリプション契約における利用プラン等を決定すること。なお、検討時において、仮想化ソフトウェア開発企業等と十分連携したうえで決定することが望ましい。

ウ　仮想化ソフトウェアに関する各種要件を満たすために別途必要となるソフト

ウェアがある場合、これらに関するライセンス等についても必要数用意すること。

エ　仮想化ソフトウェアかかるライセンス等を調達するの際は、以下の仮想化ソフトウェア開発企業担当者に問い合わせを行い、必要となるライセンスの確認を行うこと。

VMware 株式会社
公共営業統括本部　西日本公共営業部
和田　務　氏
tsutomu.wada@broadcom.com
080−3526−8187

日本マイクロソフト株式会社
パブリックセクター事業本部
髙橋　知里　氏
chisato.takahashi@microsoft.com
03-4535-3677

日本オラクル株式会社
クラウド事業統括　公共・社会基盤営業統括
公共営業本部　デジタル・ガバメント推進部
菊地　司　氏
tsukasa.kikuchi@oracle.com
080-1285-4705

(2) 機能

ア　仮想マシンの OS として、Windows（Server OS、 Client OS)、Linux(Red Hat)（いずれについても契約時点においてサポート期間内のバージョンのもの）が利用可能であること。なお、Linux については、本県が指定したディストリビューション以外に複数のディストリビューションが利用可能であり、導入後のサポートについても可能なこと。

イ　仮想マシンの雛形（クローン、テンプレート）を作成することで、容易に展開（デプロイ）ができること。

ウ　統合用サーバのリソースを有効に活用するため、CPU、メモリ、ディスクの実容量よりも多くのリソースを割当（オーバーコミット設定）ができること。

エ　導入する仮想化ソフトウェアについては、大規模な再構築を必要とせず、概ね5 年以上利用できる~~単一バージョンのソフトウェアライフサイクルが 5 年以上の~~ものを選定すること。

オ　統合用サーバで障害等が発生した場合に、影響を受けた仮想マシンを異なる統合用サーバ上で再起動させることで、ダウンタイムを最小化できる高可用性機能（HA 機能）を利用できること。

カ　既存統合サーバから仮想マシンの計画的移行が行えること。移行については、仮想化ソフトウェア間のバージョン違いなどを考慮したうえで、実績のある手法を選択できること。アプリケーションの整合性を満たした移行を実現するため、必要に応じて、移行用ツールが利用できること。

キ　通常利用向け統合用サーバ用の仮想化ソフトウェアにおいて、脅威侵入時の内部拡散防止等のセキュリティ対策のため、仮想化ソフトウェアに組み込まれた分散ファイアウォールを利用し同一セグメント内の仮想マシン間の通信制御（マイクロセグメンテーション）が可能であること。また、運用性の高いセキュリティポリシーの管理を実現するために、分散ファイアウォールを適用する対象として、タグや仮想マシン名、OS 名等のオブジェクトに紐付けてルールの作成ができる機能を有すること。なお、分散ファイアウォール以外の手法により上記の要件を実現することも可とする。

ク　公衆網を介してクラウドサービスにおけるプライベートクラウド環境（クラウドサービス上に構築した統合サーバ環境）へのセキュアなアクセスを実現するため、IPSec VPN、及び、L2VPN を構成する機能を有すること。

ケ　仮想マシンに最適なネットワークリソースを提供するために、仮想化ソフトウェアは、定義された論理的なネットワークリソース毎にそれぞれネットワーク I/O 性能（I/O 流入量）を制御する機能を有すること。

コ　仮想マシンに最適なストレージリソースを提供するために、仮想化ソフトウェアは、仮想マシンのディスク毎にストレージ I/O 性能を制御する機能を有すること。

サ　特段の理由により、後継ソフトウェア以外の仮想化ソフトウェアに変更する場合は、統合サーバ上の仮想マシン、及び、仮想アプライアンスについて、既存の共通機能基盤からの移行だけでなく、動作についても保証できること。

5.4.3.　仮想化管理サーバ、統合サーバ管理ソフトウェアに関する詳細要件

本業務で利用する統合サーバ管理ソフトウェア、及び、統合サーバ管理ソフトウェアを利用するために必要となる仮想化管理サーバについて、仮想化管理サーバ、ソフトウェアライセンス、及び、機能に関する以下の詳細要件を満たすこと。

また、本業務で利用する統合サーバ管理ソフトウェアについて、ソフトウェアライセンス、及び、機能に関する以下の詳細要件を満たすこと。なお、特に指定のない限り、通常利用向

け統合用サーバ、及び、DB 用統合用サーバの双方を管理するために必要となるそれぞれの統合サーバ管理ソフトウェアのいずれにおいても要件を満たすこと。

(1) 仮想化管理サーバ

ア　通常利用向け統合用サーバ、及び、DB 用統合用サーバの双方で仮想化管理サーバをそれぞれ IDC1 に 1 台ずつ以上用意すること。ただし、仮想マシンでの構成でも可とする。なお、仮想化管理サーバに必要なサーバについては、統合サーバ上に仮想マシンとして作成してもよいこととするが、仮想化管理サーバ用のリソース（CPU、メモリ、ディスク）は、統合サーバにおける必要リソースとは別で用意すること。

イ　仮想化管理サーバ自体の障害対応として、バックアップ、及び、リストアが可能な構成とすること。

ウ　統合サーバを利用した場合、統合サーバ上の HA 機能を利用した冗長化構成を利用することが可能となるため、フェイルオーバーが発生した時も仮想化管理サーバにかかる各機能が正常に動作するように設計すること。

(2) ソフトウェアライセンス

ア　本システムにおける運用管理を行うため、導入する仮想化ソフトウェアに対応した統合サーバ管理ソフトウェア（契約時において最新のもの）に関するライセンス、又は、サブスクリプション契約による利用権等を必要数用意すること。

イ　統合サーバ管理ソフトウェアを利用するうえで仮想化管理サーバにデータベース用ソフトウェアなど、別途必要になるソフトウェアがある場合、これらに関するライセンス等についても必要数を用意すること。

(3) 機能

ア　本業務にて構築する統合用サーバの状態と構成、及び、仮想マシンの状態と構成を統合管理し、CPU、メモリ、ストレージ、ネットワーク等の状態を確認できること。

イ　仮想化管理サーバにおける統合サーバ管理ソフトウェアの操作は GUI 画面により実施できること。また、GUI 画面はブラウザからのアクセスを基本とし、全機能が標準的なブラウザ（Edge 等）で利用可能なこと。

ウ　仮想マシンごとに、「5.4.16. ActiveDirectory に関する詳細要件」で後述する Active Directory で管理されたユーザを割り当て、仮想マシンの操作・閲覧権限等の付与ができること。

エ　本業務の共通機能基盤担当職員、及び、受託事業者には、仮想化ソフトウェア全体の管理者権限等の付与ができること。

オ　各仮想マシンの情報システム担当職員、又は、情報システム受託事業者には、該当する仮想マシンの電源 ON/OFF 操作等の限定された権限等の付与ができる

こと。

カ　統合サーバ全体のシステムログ、アラートログ、ステータスログや統合サーバ上で発生したイベント情報等を収集・保管できること。

キ　統合用サーバ、仮想化管理サーバの各種ログ（操作ログを含む）を収集し、管理（表示・検索）できること。操作ログは閲覧可能な形式で 3 カ月分、アーカイブ形式で 3 年間保存し、県の求めに応じ開示できること。

ク　ネットワークトラフィックの確認、及び、収集が可能であること。

ケ　本業務で納入する各機器、及び、各情報システムが利用する仮想マシン等について、ノードダウン、及び、リンクダウン、サービスダウン等の稼働監視を行い、リアルタイムにメール等により通知する稼働監視機能があること。

コ　稼働監視機能については、統合サーバ管理ソフトウェアにより実現する以外に、別途稼働監視ソフトウェアを導入したり、納入するハードウェア等と SNMP 連携ができるような形で実現することも可とするが、運用管理が煩雑にならないよう、できるだけシンプルな構成とすること。

サ　別途稼働監視ソフトウェア等を導入するために必要となる経費についても本業務の範囲内となるので注意すること。

以下に記述する機能については、通常利用向け統合用サーバ用の統合サーバ管理ソフトウェアにおける必須要件とする。（なお、DB 用統合用サーバ用の統合サーバ管理ソフトウェアにおいても、同様の機能があることが望ましいが、統合サーバの安定稼働が実現できれば、運用保守業務による対応を行う等、代替機能も可とする。）

シ　統合サーバのキャパシティ管理ができること。

ス　リソース使用状況トレンドから、CPU、メモリ、ディスク領域の枯渇時期（残り時間）を見積り、その結果を毎月三重県に提示できること。

セ　環境の健全性やリスク等について、仮想マシン単位やクラスタ単位等で数値化により把握できること。

5.4.4.　統合用サーバ（通常利用向け統合用サーバ、DB 用統合用サーバ）に関する詳細要件

本業務で利用する統合用サーバについて、機器、機能、及び、ソフトウェアライセンスに関する以下の詳細要件を満たすこと。なお、特に指定のない限り、通常利用向け統合用サーバ、及び、DB 用統合用サーバの双方で要件を満たすこと。

(1) 機器

ア　統合用サーバ（通常利用向け統合用サーバ、DB 用統合用サーバ）~~、~~において、別紙３「既存共通機能基盤における利用リソース一覧」、別紙４「本システムに必要となるリソースの想定」に基づき、最適な機器構成について設計を行うこと。なお、別紙 4 におけるリソースの想定については、リモート保守環境用

の VDI 環境や仮想化管理サーバ用の仮想マシン等にかかるリソースを考慮していないため、必要なリソースを追加したうえで設計を行うこと。

イ　統合用サーバのハードウェアは高可用性機能（HA 機能）を考慮した構成とすること。なお、県が要求するリソース（CPU、メモリ、ディスク容量）を満たしていれば、台数にかかる制限はないが、高可用性機能（HA 機能）を考慮した構成として、N+1 以上の構成とすること。さらに、それぞれの統合用サーバについて、ハードウェアを構成する部品を可能な限り冗長化するなどにより、可用性を考慮した構成とすること。

ウ　統合用サーバのハードウェアにおいて、拡張性を考慮した構成とすること。特に、メモリについては、運用保守期間において、メモリ単体での増設ができるようにすること。

エ　統合用サーバは、利用セグメントに応じてサーバを物理的に分割するのではなく、論理的かつセキュアにネットワークを分割することで、サーバリソースを有効に活用できる構成とすること。

オ　統合用サーバ、及び、「5.4.5.メインストレージ/バックアップストレージに関する詳細要件」で後述するメインストレージ/バックアップストレージについて、HCI(Hyper-Converged Infrastructure)による構成も可とするが、統合用サーバ、メインストレージ/バックアップストレージにおけるそれぞれの要件以上の構成とすること。ただし、HCI による構成を採用することで、実現することに特段の合理性がない要件については、本県の承認の元、当該要件を別の形で実現することも可とする。

カ　通常利用向け統合用サーバ、及び、DB 用統合用サーバで必要となるリソースについて、「5.4.12. クラウドサービスに関する詳細要件」にて後述するクラウドサービス上の統合サーバに確保することで、通常利用向け統合用サーバ、及び、DB 用統合用サーバのリソースを削減して構築することも可とする。なお、通常利用向け統合用サーバ、及び、DB 用統合用サーバのリソースを削減した場合、削減したリソースにより通常利用向け統合用サーバ、及び、DB 用統合用サーバを利用できなくなる仮想マシンについて、クラウドサービス上の統合サーバにおいて、利用可能となるよう、クラウドサービス上の統合サーバにおいて、リソースの確保を行うこと。また、クラウドサービス上の統合サーバで確保したリソースやクラウドサービス上の統合サーバにて当該仮想マシンを稼働させるために必要となる費用についても、本業務の範囲内に含めること。

キ　統合用サーバの内、通常利用向け統合用サーバの全てを「5.4.12. クラウドサービスに関する詳細要件」にて後述するクラウドサービス上の統合サーバに構築する構成（オンプレミスの統合用サーバをなくす構成）は、不可とする。

（通常利用向け統合用サーバをオンプレミス環境で利用できること。）

ク　統合用サーバ１台あたりの仕様として、以下の要件を満たすこと。なお、以下の要件を踏まえて、本県の承認の元、HDD を SSD に変更したり、RAID ではなく独自の可用性向上策を実現する構成等にて構築を行うことも可とする。

表 5.3 統合用サーバ機器要件

No	項目	機能
1	筐体形状	・ラックマウント型
2	CPU	・別紙３「既存共通機能基盤における利用リソース一覧」、別紙４「本システムに必要となるリソースの想定」から、納入台数に応じて１台当たりの必要リソースを見積もること。
3	メモリ	
4	HDD	・RAID1、又は、RAID5で構成し、実容量100GB以上 ・回転速度10,000rpm以上 ・SAS対応のディスクドライブ ・ホットスワップ（活性交換、ホットプラグ等）対応
5	RAID	・RAID1、又は、RAID5 に対応していること。
6	光学ドライブ	・DVD-ROM ドライブ８倍速以上 ・OS がブート可能であること。
7	USB	・USB 2．0 × １以上
8	LAN I/F	・本システム内のネットワークは 10Gbps 以上×2（冗長化構成）となるように必要ポート数を用意すること。 ・ネットワークの冗長化構成がとれること。
9	ストレージ I/F	・NFS、又は、FC（ファイバーチャネル）で、10Gbps 以上×2本の冗長化構成とすること。必要に応じ、サーバ・ストレージ接続スイッチを用意すること。
10	ファン	・ファンの冗長化をすること。
11	電源装置	・電源の冗長化をすること。
12	その他	・システムボード（CPU、メモリを含む）、光学ドライブ、USB、外部記憶装置以外の部品は、単一障害点がない構成とすること。

(2) 機能

ア　既存共通機能基盤におけるネットワークセグメント（インターネット接続系ネットワーク、LGWAN 接続系ネットワーク、個人番号利用事務系ネットワークにおけるそれぞれの業務端末接続用セグメント、サーバセグメント、DMZ 等）が引き続き利用できるようにすること。なお、上記以外に本システムを運用

管理するうえで必要になる管理セグメント等は別途用意すること。今後、各システムで利用するセグメントが増える可能性があるため、柔軟に対応できるようにすること。

イ　既存共通機能基盤では、各仮想マシンに対して、管理用セグメントから各種管理用アクセス（通常利用向け統合用サーバにおいては、仮想化ソフトウェア管理ソフトウェア（vCenter）における vMotion や監視用通信など）が可能となるような構成にしており、また、これらのセグメントは、セキュリティ対策のため、業務で利用するセグメントからは直接通信ができない別セグメントとしている。そのため、引き続き、管理用セグメントから各種管理ができるようにするとともに、可能な限り既存の管理用セグメントにかかる構成を踏襲すること。

(3) ソフトウェアライセンス

ア　統合用サーバに導入するソフトウェアライセンスとして、以下のソフトウェアライセンスを用意すること。

イ　通常利用向け統合用サーバ、及び、DB 用統合用サーバをどのような構成で構築する場合であっても、DB 用統合用サーバにおいて必要となる OracleDB 用ライセンスの他、全てのソフトウェアライセンスについて、ライセンス違反が発生しないよう、十分に注意すること。

表 5.4 統合用サーバ用ソフトウェアライセンス

No	項目	数量	備考
1	Windows Server Datacenter Edition	必要数	・導入する全台の統合用サーバで利用できるライセンス数を用意すること。 ・導入時における最新版のライセンスを提供し、必要に応じてダウングレードして利用すること。 ・ServicePack 等は最新版を適用すること。
2	Oracle Database Standard Edition 2	必要数	・DB用統合用サーバで利用できるライセンス数を用意すること。 ・導入時における最新版のライセンスを提供し、旧バージョンの使用も可能とすること。 ・データベースソフトウェア等を仮想環境で使用する際のライセンス体系を考慮すること。

5.4.5.　メインストレージ/バックアップストレージに関する詳細要件

本業務で利用するメインストレージ/バックアップストレージについて、機器、及び、機

能に関する以下の詳細要件を満たすこと。なお、特に指定のない限り、通常利用向け統合用サーバ、及び、DB 用統合用サーバの双方で利用するそれぞれのストレージのいずれにおいても要件を満たすこと。

(1) 機器（メインストレージ）

ア　NFS、又は、FC（ファイバーチャネル）のインターフェースを持ったストレージを通常利用用統合用サーバ、及び、DB 用統合用サーバのそれぞれに対して、IDC1 に 1 台以上ずつ用意すること。なお、インターフェースは 10Gbps 以上×2 本の冗長化構成とし、必要に応じ、サーバ・ストレージ接続スイッチを用意すること。

イ　ストレージは可用性、及び、拡張性を考慮した構成とすること。なお、コントローラや部品等は冗長化を実施し、単一障害ポイントを無くすこと。

ウ　不意の停電時にキャッシュ上のデータを保護する仕組みを有すること。

エ　メインストレージを、仮想マシンにおける本体データ等の保存先として利用するためのメイン領域と、メイン領域のバックアップを保存するためのバックアップ領域に分割できること。

オ　メイン領域とバックアップ領域において、利用するディスクを重複させないなど、メインストレージ内で物理的に分割することで可用性を向上させることができること。

カ　~~「5.4.4.統合用サーバ（通常利用向け統合用サーバ、DB 用統合用サーバ）に関する詳細要件」で記載された統合用サーバ、及び、メインストレージについて、HCI(Hyper-Converged Infrastructure)による構成も可とするが、統合用サーバ、メインストレージにおけるそれぞれの要件以上の構成とすること。~~

キ　~~メインストレージで必要となるリソースについて、「5.4.12. クラウドサービスに関する詳細要件」にて後述するクラウドサービス上の統合サーバに確保することで、メインストレージのリソースを削減して構築することも可とする。なお、メインストレージのリソースを削減した場合、削減したリソースによりメインストレージを利用できなくなる仮想マシンについて、クラウドサービス上の統合サーバにおいて、利用可能となるよう、クラウドサービス上の統合サーバにおいて、リソースの確保を行うこと。また、クラウドサービス上の統合サーバで確保したリソースやクラウドサービス上の統合サーバにて当該仮想マシンを稼働させるために必要となる費用についても、本業務の範囲内に含めること。~~

ク　~~メインストレージをどのような構成で構築する場合であっても、DB 用統合用サーバにおいて必要となる OracleDB 用ライセンスの他、全てのソフトウェアライセンスについて、ライセンス違反が発生しないよう、十分に注意すること。~~

ケ　メインストレージの仕様として、以下の要件を満たすこと。なお、以下の要件を踏まえて、本県の承認の元、HDD を SSD に変更したり、RAID ではなく独自の可用性向上策を実現する構成等にて構築を行うことも可とする。

表 ~~56~~.5 メインストレージ機器要件

No	項目	機能
1	コントローラ	・コントローラの冗長化をすること。
2	ストレージ I/F	・NFS、又は、FC（ファイバーチャネル）で、10Gbps 以上×2 本の冗長化構成とすること。 ・必要に応じ、サーバ・ストレージ接続スイッチを用意すること。
3	ホットスペアディスク	・ホットスペアディスクに対応していること。
4	HDD/SSD	・メイン領域用のHDD/SSDはオールフラッシュ構成、又は、同構成と同等以上とすること。 ・バックアップ領域用のHDD/SSDはSATA、又は、NL-SASと同等以上とすること。 ・キャッシュ用のSSDが搭載されていること。 ・HDDの回転速度は10,000rpm以上とすること。 ・メイン領域の容量として、別紙３「既存共通機能基盤における利用リソース一覧」、別紙４「本システムに必要となるリソースの想定」にかかる仮想マシン等の保存に必要な容量を保存できること。 ・バックアップ領域の容量として、重複排除・圧縮機能等を使用し、日次でバックアップを行い、メイン領域 の5世代以上のデータ保存が可能であること。 ・メイン領域からバックアップ領域へ高速バックアップが可能であること。 ・RAID6相当以上で構成すること。 ・ホットスワップ（活性交換、ホットプラグ等）に対応しており、無停止でのディスク交換が可能なこと。 ・ホットスペアディスクは2本以上とし、ストレージメーカーが推奨する本数を用意すること。 ・領域を2つ以上に分割できること。
5	接続形式	・コントローラが二重化されており、統合用サーバとマルチパス構成がとれること。

6	LAN I/F	・本システム内のネットワークは 10Gbps 以上×2（冗長化構成）となるように必要ポート数を用意すること。 ・バックアップストレージとの通信に LAN I/F を利用する場合は、管理用の LAN I/F 等と分離して利用できること。
7	ファン	・ファンの冗長化をすること。
8	電源装置	・電源の冗長化をすること。
9	その他	・本業務で納入する統合用サーバの電源 ON,OFF 時においても、ストレージ機器内のデータの整合性が保証できること。 ・予兆診断、自動通報の機能を有すること。 ・筐体形状はラックマウント型であること。 ・メイン領域からバックアップ領域へのフルバックアップ時や差分バックアップ時、及び、IDC１から IDC2 へのレプリケーション時において、稼働中の仮想マシン等に影響を及ぼさずに処理が可能な構成とすること。

(2) 機器（バックアップストレージ）

ア　バックアップストレージを IDC2 に１台用意すること。

イ　バックアップストレージは可用性を考慮し、部品の冗長化をすること。

~~ウ　バックアップストレージで必要となるリソースについて、「5.4.12. クラウドサービスに関する詳細要件」にて後述するクラウドサービス上の統合サーバに確保することで、バックアップストレージのリソースを削減して構築することも可とする。なお、バックアップストレージのリソースを削減した場合、削減したリソースによりバックアップストレージを利用できなくなる仮想マシンについて、クラウドサービス上の統合サーバにおいて、利用可能となるよう、クラウドサービス上の統合サーバにおいて、リソースの確保を行うこと。また、クラウドサービス上の統合サーバで確保したリソースやクラウドサービス上の統合サーバにて当該仮想マシンを稼働させるために必要となる費用についても、本業務の範囲内に含めること。~~

~~エ　バックアップストレージをどのような構成で構築する場合であっても、DB 用統合用サーバにおいて必要となる OracleDB 用ライセンスの他、全てのソフトウェアライセンスについて、ライセンス違反が発生しないよう、十分に注意すること。~~

オ　バックアップストレージの仕様として、以下の要件を満たすこと。なお、以下の要件を踏まえて、本県の承認の元、HDD を SSD に変更したり、RAID ではなく独自の可用性向上策を実現する構成等にて構築を行うことも可とする。

表 5.6 バックアップストレージ機器要件

No	項目	機能
1	HDD/SSD	・容量として、メインストレージからのレプリケーションで必要となる容量を確保できること。 ・ディスクはRAIDで保護されていること。 ・ホットスワップ（活性交換、ホットプラグ等）に対応しており、無停止でのディスク交換が可能なこと。 ・重複排除・圧縮機能等を使用し、バックアップ容量の削減が可能なこと。 ・ディスクはSATA、又は、NL-SASと同等以上とすること。 ・キャッシュ用のSSDが搭載されていること。 ・HDDの回転速度は7,200rpm以上とすること。
2	LAN I/F	・100BASE-TX/1000BASE-T 対応ポートを必要数用意すること。 ・ネットワークの冗長接続が可能なこと。
3	電源装置	・電源の冗長化をすること。
4	レプリケーション	・IDC1 から IDC2 へのレプリケーション（遠隔バックアップ）が可能なこと。
5	変更禁止	・ランサムウェア対策として、バックアップデータの変更禁止処理が可能なこと。
6	その他	・予兆診断、自動通報の機能を有すること。 ・筐体形状はラックマウント型であること。 ・レプリケーションを実施する際に、稼働中の仮想マシン等に影響を及ぼさずに処理が可能な構成とすること。

(3) 機器（メインストレージ/バックアップストレージ共通）

ア 「5.4.4.統合用サーバ（通常利用向け統合用サーバ、DB 用統合用サーバ）に関する詳細要件」で記載された統合用サーバ、及び、メインストレージ/バックアップストレージについて、HCI(Hyper-Converged Infrastructure)による構成も可とするが、統合用サーバ、メインストレージ/バックアップストレージにおけるそれぞれの要件以上の構成とすること。ただし、HCI による構成を採用することで、実現することに特段の合理性がない要件については、本県の承認のうえ、当該要件を別の形で実現することも可とする。

イ メインストレージ/バックアップストレージで必要となるリソースについて、「5.4.12. クラウドサービスに関する詳細要件」にて後述するクラウドサービス上の統合サーバに確保することで、メインストレージ/バックアップストレージのリソースを削減して構築することも可とする。なお、メインストレー

ジ/バックアップストレージのリソースを削減した場合、削減したリソースによりメインストレージ/バックアップストレージを利用できなくなる仮想マシンについて、クラウドサービス上の統合サーバにおいて、利用可能となるよう、クラウドサービス上の統合サーバにおいて、リソースの確保を行うこと。また、クラウドサービス上の統合サーバで確保したリソースやクラウドサービス上の統合サーバにて当該仮想マシンを稼働させるために必要となる費用についても、本業務の範囲内に含めること。

ウ　メインストレージ/バックアップストレージをどのような構成で構築する場合であっても、DB 用統合用サーバにおいて必要となる OracleDB 用ライセンスの他、全てのソフトウェアライセンスについて、ライセンス違反が発生しないよう、十分に注意すること。

(4) 機能（メインストレージ）

ア　統合用サーバ上の仮想マシンにおける本体データの保管先として利用でき、かつ、複数の仮想マシンから同時アクセスが可能であること。

イ　統合サーバ管理ソフトウェア、又は、ブラウザから IP 通信等で直接ストレージに接続することにより、容量変更、状態確認等のストレージの管理ができること。

ウ　スナップショットの作成や削除、データバックアップやリストアの際に稼働中の仮想マシンに影響を及ぼさないこと。

エ　OS 領域を含む領域が全て RAID6 相当以上で構成されることとし、同一 RAID グループ内でディスク 2 重障害が発生してもサービス停止しないこと。

オ　冗長コントローラやストレージ間のデータ移行等を用いることで、停止させずにストレージ OS、ファームウェア等のパッチ適用やアップグレード等が実施でき、任意に切り戻し運用ができること。

カ　重複排除機能によりデータ容量を削減できること。

キ　メイン領域とバックアップ領域を物理的に分割（ディスクを分ける等）できること。

ク　バックアップ領域にメイン領域のデータをバックアップできること。

ケ　バックアップは自動で取得するよう設定できること。なお、バックアップは業務に影響の無い夜間等で毎日行い、RPO（リカバリポイント目標）は 1 日以内とすること。

コ　仮想マシン本体のデータをバックアップ領域に取得する際に、仮想マシン自体や統合用サーバ、ネットワーク、ストレージ等に過度な負荷がかからないようにすること（過度な負荷とは、バックアップ取得中に動作が不安定になったり、ping による応答がなくなるレベルとする。）。

サ　各仮想マシンにエージェントをインストールする必要がある場合は、インス

トールに関する各種マニュアルの整備や障害発生時の切り分け支援、リストア時の支援等についても本業務の範囲内とする。

シ　バックアップ用エージェントソフトウェアについては、必要数分のライセンスを用意すること。また、1 ライセンス単位で追加購入が可能なこと。

ス　バックアップは、可能な限りフルバックアップを取得することとし、リストア時間が短縮できるよう考慮すること。また、5 世代以上の世代管理を行い、本県の求めに応じて指定する世代のデータリストアが可能なこと。

セ　仮想マシン内だけでなく仮想マシン間で重複するデータの除外を行う機能を有すること。

ソ　取得したバックアップデータから仮想マシンのフルリストアや特定のファイルのみのリストアができること。

タ　IDC1 に設置したメインストレージにおけるバックアップ領域のデータを IDC2 に設置したバックアップストレージへ世代の差分データをレプリケーションできること。また、レプリケーション用ネットワーク負荷を低減させる機能を提供可能なこと。

チ　バックアップ、及び、リストア機能の効率化を実現するために、バックアップサーバを導入し、ソフトウェアによるバックアップ方式も可とする。

ツ　ディスク障害時のデータ復旧の際にはディスク容量全体の複製をすることなく、実際のデータ分だけ複製できること。

テ　メインストレージに必要なリソースを「5.4.12.　クラウドサービスに関する詳細要件」にて後述するクラウドサービス上の統合サーバに確保する形で構築する場合、クラウドサービス上の統合サーバ内のメインストレージ用として確保したリソースにおいても、メインストレージに対して必要とされる各種要件（バックアップ機能や重複除外機能等）に準じた機能が利用できること。

(5) 機能（バックアップストレージ）

ア　IDC1 のメインストレージにおけるバックアップ領域のデータをレプリケーションにより取得可能であること。また、レプリケーション用ネットワーク負荷を低減させる機能を提供可能なこと。

イ　レプリケーション済みのデータによりリストアが可能なこと。

ウ　レプリケーションにおいては、ネットワークトラフィックを軽減させるため、重複排除や圧縮技術を利用したり、細かい単位で差分ブロック転送したりする等、効率的な転送方法を利用できること。

エ　バックアップデータの改ざんや意図せぬ暗号化に備えるため、変更禁止処理が可能なバックアップシステムを利用すること。

オ　バックアップ、及び、リストア機能の効率化を実現するために、バックアップサーバを導入し、ソフトウェアによるバックアップ方式も可とする。

カ　IDC1 からレプリケーション等によりバックアップデータを日次で 5 世代ずつ保存できること。メインストレージのバックアップデータが消失しても、バックアップストレージのバックアップデータからリストアができること。

キ　バックアップからのリストアとして、通常はメインストレージのバックアップ領域からメイン領域へのリストアを予定しているため、運用保守期間においてバックアップストレージからのリストアは発生しないと想定しているが、テスト期間におけるリストアテストの実施や毎年度実施予定のリストア訓練等でリストアを実施する必要があるため、対応が可能なこと。

ク　バックアップストレージに必要なリソースを「5.4.12.　クラウドサービスに関する詳細要件」にて後述するクラウドサービス上の統合サーバに確保する形で構築する場合、クラウドサービス上の統合サーバ内のバックアップストレージ用として確保したリソースにおいても、バックアップストレージに対して必要とされる各種要件（レプリケーション等）に準じた機能が利用できること。

5.4.6.　SSL-VPN 装置に関する詳細要件

本業務で利用するリモート保守環境用 SSL-VPN 装置について、機器、及び、機能に関する以下の詳細要件を満たすこと。

(1) 機器

ア　インターネット VPN 接続によるリモート保守環境を構築するため、SSL-VPN 装置を導入すること。

イ　SSL-VPN 装置は、冗長化構成とし、無停止でファームウェアのバージョンアップ等が可能なこと。

ウ　SSL-VPN 装置は、三重県情報ネットワークの DMZ に設置し、インターネットからの接続ができるようにすること。

エ　SSL-VPN 装置として、ソフトウェア製品等による構成も可とするが、アプライアンスの SSL-VPN 装置を冗長化構成としたときと同程度の可用性を実現すること。

オ　インターネット VPN 接続によるリモート保守環境を利用するシステムとして最大 50 システム、150 ユーザ（端末）を想定しているため、150 ユーザ（端末）が登録可能、かつ、~~ソフトウェアライセンス等の追加により、同時に 100 ユーザからの~~アクセスが可能な製品を選定すること。

カ　ソフトウェアライセンス等の追加により、インターネット経由で接続する各情報システムにおける受託事業者端末について、セキュリティチェック等の検疫機能が利用可能な機器を選定すること。

(2) 機能

ア　検疫機能として、事前登録済み、かつ、セキュリティが確保された端末に限定

して接続させることができるよう端末固有情報、エージェントソフトウェアのインストール有無、OS のセキュリティパッチ適用状況、マルウェア対策ソフトウェアの更新状況等の適用状況の確認と十分な対応がなされているかの判定が可能なこと。また、判定結果を基に接続の可否について制御が可能なこと。

イ　SSL-VPN 装置を利用するに当たり、有償の SSL サーバ証明書を必要数用意し、適用すること。

ウ　SSL-VPN 接続の利用者として、150~~70~~ユーザ（端末）以上の登録が可能であること。また、同時に 70 ユーザ（端末）からの接続が可能であること。

エ　「5.4.11.認証装置にかかる詳細要件」にて後述する認証装置と連携し、認証機能を提供できること。

オ　本県が用意するパソコン以外のパソコンから接続することを想定しているため、機器に依存しない仕組みにすること。また、今後の検討として、タブレット端末で利用する場合の環境や条件を提示できる~~する~~こと。

カ　インターネット VPN 接続によるリモート保守環境を利用中の端末に対して、リモート保守環境利用中は、印刷や、接続先サーバから外部へのデータ保存、接続先サーバへのデータのアップロードができないよう、セキュリティ上の制限が可能なこと。

5.4.7.　IP-VPN 接続用ネットワーク機器に関する詳細要件

本業務で利用するリモート保守環境用 IP-VPN 接続用ネットワーク機器について、機器、及び、機能に関する以下の詳細要件を満たすこと。

(1) 機器

ア　IDC1 とリモート保守環境利用事業者間を結ぶ閉域網を介して、IP-VPN 接続によるセキュアな通信を実現できる IP-VPN 接続用ネットワーク機器を導入すること。

イ　機器構成として、各リモート保守環境利用事業者側に IP-VPN 接続用ネットワーク機器を設置し、IDC1 側に各リモート保守環境利用事業者からの通信を集約するためのセンター機器を設置する構成が可能なこと。最大 20~~50~~か所のリモート保守環境利用事業者から IP-VPN 接続が可能なこと。

(2) 機能

ア　IP-VPN 接続用ネットワーク機器の Private 側は、本システムの管理用セグメントに接続できるようにすること。

イ　IP-VPN 接続用ネットワーク機器の Public 側は閉域網と接続できること。

ウ　通信速度として、100Mbps 以上の性能を有すること。

エ　拠点については、別紙５「リモート保守環境利用システム（保守事業者所在地）」を参照すること。

オ　保守拠点数は 8 とし、8 拠点分のリモート保守環境利用事業者側に設置する IP-VPN 接続用ネットワーク機器を用意すること。また、最大 2050 か所まで拡張できること。なお、8 拠点を越えて利用する場合、保守拠点側に新たに IP-VPN 接続用ネットワーク機器が必要になるが、当該機器の調達については、本業務の範囲外とする。

カ　~~また、~~管理用拠点が必要な場合は、別途必要数を見込むこと。

5.4.8.　IP-VPN 接続用貸し出し端末に関する詳細要件

本業務で利用するリモート保守環境用 IP-VPN 接続用貸し出し端末について、機器、及び、機能に関する以下の詳細要件を満たすこと。

(1) 機器

ア　IP-VPN接続を利用する各情報システム保守事業者に貸し出しを行う IP-VPN接続用貸し出し端末として、本県が用意する次の端末でも利用が可能なこと。ただし、OS については運用期間内に OS を Windows11 に変更する予定のため、変更後も利用可能なこと。また、ブラウザ、マルウェア対策ソフトウェア等についても同様にバージョンアップすることが想定されているため、これらに対しても対応可能であること。

表 5.7 本県が用意する IP-VPN 接続用貸し出し端末

種類	スペックの詳細
メーカー	Lenovo
型番	ThinkPad X395
CPU	Ryzen 5 PRO 3500U
クロック	2.10Ghz
SSD 容量	256GB
メモリ	8GB
画面サイズ	13.3 型ワイド
画面解像度	1920×1080
OS	Windows 10 Professional 64bit
ブラウザ	Microsoft Edge
マルウェア対策	Microsoft 社　Microsoft Defender
USB ポート	USB 3.1 Type-C×2、USB 3.1×1

イ　IP-VPN 接続用貸し出し端末として、受託事業者内、及び、県庁内で利用できる端末を合計 2 台以上用意し、本業務における運用保守業務を行うための専用端末として納品する~~利用可能な形に設定を行う~~こと。なお、その他の拠点用 IP-VPN 接続用貸し出し端末の調達は本業務の対象外とする。

ウ　IP-VPN 接続用貸し出し端末として、本県が別途用意する端末について、本業務の運用~~保守~~期間中に機器更新を実施する予定だが、新たに導入する端末の参考とするため、IP-VPN 接続を行うために必要となるスペック等について本県に提示すること。また、提示したスペックに準拠した端末を購入後、IP-VPN 接続用貸し出し端末として利用できるよう設定を行うこと。

(2) 機能

ア　IP-VPN 接続用貸し出し端末は、リモート保守環境利用事業者に設置された、IP-VPN 用ネットワーク機器の Private 側に接続することで、IP-VPN 接続によるリモート保守環境の利用が可能なこと。

5.4.9.　閉域網に関する詳細要件

本業務で利用するリモート保守環境用閉域網について、機能に関する以下の詳細要件を満たすこと。

(1) 機能

ア　IDC1 と IP-VPN 接続によるリモート保守環境利用事業者間を結ぶ閉域網を必要な拠点数分用意すること。

イ　閉域網は、IDC1 とリモート保守環境利用事業者に設置された IP-VPN 接続用ネットワーク機器の Public 側で接続し、両拠点間における IP-VPN 接続用の通信回線として利用できること。

ウ　通信速度は、100Mbps 以上（ベストエフォート）とすること。

エ　保守拠点の所在に応じ、エリア間接続を考慮すること。

オ　拠点については、別紙５「リモート保守環境利用システム（保守事業者所在地)」を参照すること。各拠点に設置する回線費用についても本業務に含めること。

カ　保守拠点数は 8 とし、最大 20~~50~~か所まで拡張できること。なお、8 拠点を越えて利用する場合、保守拠点側に新たに閉域網が必要になるが、当該回線の調達については、本業務の範囲外とする。

キ　~~また、~~管理用拠点が必要な場合は、別途必要数を見込むこと。

~~ク　リモート保守環境全体で 80 システム、150 端末（ユーザ）以上の登録が可能であること。~~

5.4.10.　VDI 環境に関する詳細要件

本業務で利用するリモート保守環境用 VDI 環境にかかる機器、ソフトウェアライセンス、及び、機能に関する以下の詳細要件を満たすこと。

(1) 機器

ア　リモート保守環境で利用するため、原則として、既存リモート保守環境における VDI 環境構築用ソフトウェア（VMware 社製 VMware horizon）の後継ソフトウェアにより~~る~~ VDI 環境を構築~~導入~~すること。

イ　VDI 環境に必要なサーバについては、統合サーバ上に仮想マシンとして作成してもよいこととするが、リモート保守環境用のリソース（CPU、メモリ、ディスク）は、統合サーバにおける必要リソースとは別で用意すること。

ウ　統合サーバを利用した場合、統合サーバ上の HA 機能を利用した冗長化構成を利用することが可能となるため、フェイルオーバーが発生した時も VDI 環境にかかる各機能が正常に動作するように設計すること。

エ　VDI 環境の代わりにリモート保守環境用ハードウェアを利用した構成も可とする。ただし、VDI 環境構築用ソフトウェアにより構築した VDI 環境と比較して、同等以上の性能を有するとともに、セキュリティ対策等ができること。さらに、ハードウェアを導入することに伴い、必要となる、機器故障対応、セキュリティパッチ対応等、運用上、必要になる全ての業務についても、本業務に含めること。その他、以下に記載された「（２）ソフトウェアライセンス」「（３）機能」についても、必要な要件を満たすこと。~~（~~

(2) ソフトウェアライセンス

ア　VDI 環境を構築するために必要となる VDI 環境構築用ソフトウェアについては、原則として、既存 VDI 環境における VDI 環境構築用ソフトウェアとして採用している VMware 社製 VMware Horizon を利用すること。なお、本県の承認を得たうえで、VMware Horizon 以外のソフトウェアにより、VDI 環境を構築することも可とするが、リモート保守環境を構築するために必要となる全ての要件を満たすこと。

イ　VDI 環境を構築するために必要となるライセンスを必要数用意すること。また用意するライセンスは、契約時において最新のものとすること。

ウ　VDI 環境の構築について十分な検討を行ったうえで、製品仕様や設定方法を決定すること。なお、検討時において、ソフトウェア開発企業等と十分連携したうえで決定することが望ましい。

エ　VDI 環境の各要件を満たすために別途必要となるソフトウェアがある場合、これらに関するライセンスについても必要数用意すること。

オ　VDI 環境構築用ソフトウェアにかかるライセンス等を調達する~~の~~際は、以下の担当者~~メーカー営業~~に問い合わせを行い、必要となるライセンスの確認を行うこと。

VMware 株式会社
公共営業統括本部　西日本公共営業部
和田　務　氏
tsutomu.wada@broadcom.com
080−3526−8187

日本マイクロソフト株式会社
パブリックセクター事業本部
髙橋　知里　氏
chisato.takahashi@microsoft.com
03-4535-3677

日本オラクル株式会社
クラウド事業統括　公共・社会基盤営業統括
公共営業本部　デジタル・ガバメント推進部
菊地　司　氏
tsukasa.kikuchi@oracle.com
080-1285-4705

(3) 機能

ア　リモート保守環境利用事業者からインターネット VPN 接続経由、又は、IP-VPN 接続経由で VDI 環境へログインでき、その後、仮想化ソフトウェアの管理コンソールによる各仮想マシンへの画面転送方式によるアクセスが可能となる環境を構築すること。

イ　VDI 環境からは、リモートデスクトップ（RDP）や VNC も利用できること。

ウ　VDI 環境から、仮想化ソフトウェアの管理コンソールによる、各仮想マシンの操作について、リモート保守端末等への情報流出がない等のセキュリティに留意した設定が可能であること。

エ　プロトコルの脆弱性の観点から画面転送プロトコルとして RDP の利用を制限できること。

オ　VDI 用の OS は最新版の Windows OS とすること。なお、本業務の範囲で統合用サーバに導入する Windows Server Datacenter Edition で利用できる Windows OS を利用してもよいものとする。

カ　VDI 環境への認証の際には、「5.4.11.認証装置に関する詳細要件」で後述す

る認証機能等を利用することにより、2 要素認証、又は、ワンタイムパスワード等による 2 段階認証等、安全な認証方法が利用できるようにすること。

キ　仮想化ソフトウェアにおける権限設定機能と連携し、各仮想マシンの情報システム担当職員、又は、情報システム受託事業者に対して、該当する仮想マシンにかかる電源 ON/OFF 操作等の限定された権限等の付与ができること。

ク　リモート保守端末側からファイルの送受信を制限できるなど、セキュリティの確保ができること。

ケ　同時接続で最大 70~~50~~のユーザ（端末）から接続が可能なこと。また、ライセンス等を追加購入することで、最大同時 100~~80~~接続までが可能なこと。

コ　各 VDI 環境はフルクローン形式を採用すること。ただし、必要に応じて管理者が環境を初期化できること。

サ　リモート保守環境全体で 50~~80~~システム、100VDI、150 ユーザ（端末~~（ユーザ~~）以上の登録が可能であること。

シ　1 システム当たり、2VDI を割り当て、平均 3 台のユーザ（端末）からアクセスが可能となるリソースを確保できること。又、同時に 70 ユーザ（端末）からの利用が可能なこと。

5.4.11.　認証装置に関する詳細要件

本業務で利用するリモート保守環境用認証装置にかかる機器、及び、機能に関する以下の詳細要件を満たすこと。

(1) 機器

ア　インターネット VPN 接続によるリモート保守環境を利用する際に利用者の認証を行うため、認証装置を導入すること。

イ　認証装置に必要なサーバについては、統合サーバ上に仮想マシンとして作成してもよいこととするが、認証装置用のリソース（CPU、メモリ、ディスク）は、統合サーバにおける必要リソースとは別で用意すること。

ウ　統合サーバを利用した場合、統合サーバ上の HA 機能を利用した冗長化構成を利用することが可能となるため、フェイルオーバーが発生した時も認証装置にかかる各機能が正常に動作するように設計すること。

(2) 機能

ア　インターネット VPN 接続によるリモート保守環境を利用するため、VDI 環境へアクセスを行う場合には、2 要素認証、又は、2 段階認証による認証ができる~~ようにする~~こと。

イ　認証方式として、マトリクス認証等、運用上の手間がかからないものを採用することとし、USB トークン等、端末側で物理的なものを利用しない方式とすること。なお、物理的なものを利用する場合であっても、本県側での運用上の手間が増えない場合は利用を可とする。

ウ　パスワードは最低文字数による制限が可能なこと。

エ　複数回連続で認証に失敗するとロックする機能を有すること。

5.4.12.　クラウドサービスに関する詳細要件

本業務で利用するクラウドサービスについて、全体構成、及び、機能に関する以下の詳細要件を満たすこと。

(1) 全体構成

ア　クラウドサービス上に本県のみが利用可能なプライベートクラウド環境を構築し、統合サーバとして利用できるようにすること。

イ　クラウドサービス上に構築した統合サーバについて、本業務で構築するオンプレミス環境の統合サーバと連携させることで、ハイブリッドクラウド環境として利用できるようにすること。

ウ　クラウドサービス上の統合サーバで提供可能な機能として、(1) 通常利用向け統合用サーバで利用予定の~~している~~仮想化ソフトウェア（VMware vSphere を想定）により提供される仮想化環境~~機能~~と同程度の機能~~もの~~が利用~~提供~~できる~~機能（クラウドサービス提供事業者から提供される VMware Solution~~ 環境（以下、「VMware Solution 機能」という。）と、(2) クラウドサービス毎の独自環境として~~提供事業者から~~提供されるクラウドネイティブな ~~IaaS~~ 環境（以下、「クラウドサービス IaaS 機能」という。）~~）~~が利用できること。

エ　VMware Solution 機能として、VMware Cloud on AWS、Azure VMware Solution、Google Cloud VMware Engine、Oracle Cloud VMware Solution、等を想定している。

オ　クラウドサービス IaaS 機能として、AWS、Microsoft Azure、Google Cloud、Oracle Cloud 等を想定している。

カ　本業務において、VMware Solution 機能、及び、クラウドサービス IaaS 機能として特定のクラウドサービス提供事業者から提供される機能を利用することを想定しているが、利用しなかったクラウドサービス提供事業者から提供される VMware Solution 機能、及び、クラウドサービス IaaS 機能が利用可能な構成（マルチクラウド構成）を実現するために必要となる設計についても、本業務の範囲内とする。なお、利用しなかったクラウドサービス提供事業者から提供される VMware Solution 機能、及び、クラウドサービス IaaS 機能を利用することが可能な構成を実際に構築するための業務については、本業務の範囲外とする。

キ　VMware Solution 機能、及び、クラウドサービス IaaS 機能について、当初想定した容量を超えた利用を本県が行った場合は、容量を超えた部分の費用負担は本業務の対象外とする。なお、利用状況を、本県に対して毎月報告でき、かつ、想定した容量を超える恐れがある場合は、速やかに本県に対して報告で

きるようにすること。

ク　「5.4.4. 統合用サーバ（通常利用向け統合用サーバ、DB 用統合用サーバ）に関する詳細要件」「5.4.5. メインストレージ/バックアップストレージに関する詳細要件」において、統合用サーバやメインストレージ/バックアップストレージにおける必要リソース等をクラウドサービス上の統合サーバにて確保することで統合用サーバやメインストレージ/バックアップストレージの必要リソースを削減した場合、削減したことにより統合用サーバやメインストレージ/バックアップストレージを利用できなくなる仮想マシンやストレージ容量等について、クラウドサービス上の統合サーバにおいて、利用可能となるよう、クラウドサービス上の統合サーバにおいて、リソースの確保を行うこと。また、クラウドサービス上の統合サーバで確保したリソースやクラウドサービス上の統合サーバにて当該仮想マシンやストレージ容量等を稼働させるために必要となる費用についても、本業務の範囲内に含めること。

ケ　当該クラウドサービスを利用するために必要となる回線費用についても、本業務の範囲内とする。なお、本業務で調達する回線等については、本システムのクラウドサービスを利用する仮想マシン数や規模等に応じて十分な回線容量を用意するとともに、複数回線による冗長化構成をとること。

コ

(2) 機能（VMware Solution 機能）

ア　VMware Solution 機能により利用可能となるクラウドサービス上の統合サーバに対し、オンプレミスの統合サーバ（既存共通機能基盤における通常利用向け統合用サーバ、及び、本業務で構築する~~した~~通常利用向け統合用サーバ）上の仮想マシンをシームレスに（仮想マシンについてイメージの変換等を実施せず簡単に、又は、移行用ツールを利用することでダウンタイム等が 30 分程度で容易に）~~に~~移行できること。

イ　VMware Solution 機能により利用可能となるクラウドサービス上の統合サーバ内で利用できるリソースとして、標準的な仮想マシン 10 台程度分が利用できるリソースを用意すること。（1 仮想マシン当たり 4 コア、16GByte メモリ、500GByte 程度とする。）

ウ　オンプレミスの統合サーバ上で稼働していた仮想マシンをクラウドサービス上の統合サーバへ移動したうえで、稼働させる場合、クラウドサービス上の統合サーバにおける CPU やメモリ等のリソースについて、十分注意したうえで、サイジングを行うこと。（既存共通機能基盤における各仮想マシンの利用リソース一覧は、別紙３「既存共通機能基盤における利用リソース一覧」を参照すること。特に、総合文書システムにおけるデータベースサーバをクラウドサービス上の統合サーバで稼働させる~~移動する~~場合に必要となるリソースについ

て、十分注意すること。）

エ　VMware Solution 機能により利用可能となるクラウドサービス上の統合サーバ、及び、統合サーバ上の仮想マシンについて、通常利用向け統合用サーバ用の統合サーバ~~仮想化管理サーバ（vCenter）上の仮想化ソフトウェア~~管理ソフトウェアから統合管理が可能なこと。

オ　本業務で構築する通常利用向け統合用サーバ上で稼働中の仮想マシンについて、VMware Solution 機能により利用可能となるクラウドサービス上の統合サーバへ IP アドレスを維持したまま移行が可能であるよう、通常利用向け統合用サーバと VMware Solution 機能により利用可能となるクラウドサービス上の統合サーバで同一のネットワークセグメントを利用できる機能を有すること。また、VMware Solution 機能により利用可能となるクラウドサービス上の統合サーバから通常利用向け統合用サーバ向けの移行も実施可能なこと。

カ　通常利用向け統合用サーバと VMware Solution 機能により利用可能となるクラウドサービス上の統合サーバにおいて、同一の L2 ネットワークを利用できる機能（L2 延伸機能）を有すること。

キ　VMware Solution 機能により利用可能となるクラウドサービス上の統合サーバにおいて、リソースが逼迫した際は、クラウドサービスにかかる追加手続き等を実施することで、リソースの拡張ができること。

ク　通常利用向け統合用サーバで利用する仮想化ソフトウェアで利用可能となるネットワーク仮想化機能、及び、分散ファイアウォール機能について、VMware Solution 機能により利用可能となるクラウドサービス上の統合サーバにおいても利用可能なこと。また、一元管理ができること。

ケ　VMware Solution 機能により利用可能となるクラウドサービス上の統合サーバにおいて、構築や利用するために必要となるソフトウェアライセンス、ネットワーク機器、回線等がある場合は、それらの調達についても、本業務の範囲内とし、漏れなく準備を行うこと。

(3) 機能（クラウドサービス IaaS 機能）

ア　クラウドサービス IaaS 機能により利用可能となるクラウドサービス上の統合サーバ内で利用できるリソースとして、標準的な仮想マシン 10 台程度分が利用できるリソースを用意すること。（1 仮想マシン当たり 4 コア、16GByte メモリ、500GByte 程度とする。）

イ　クラウドサービス IaaS 機能により利用可能となるクラウドサービス上の統合サーバ、及び、統合サーバ上の仮想マシンについて、運用管理を行うために必要になる管理機能がクラウドサービス提供事業者から別途提供されており、本県の情報システム単位で利用が可能なこと。

ウ　通常利用向け統合用サーバとクラウドサービス IaaS 機能により利用可能とな

るプライベートクラウド上の統合サーバにおいて、同一のL2ネットワークを利用できる機能（L2延伸機能）を有すること。

エ　クラウドサービスIaaS機能により利用可能となるクラウドサービス上の統合サーバにおいて、リソースが逼迫した際は、クラウドサービスにかかる追加手続き等を実施することで、リソースの拡張ができること。

オ　通常利用向け統合用サーバで利用する仮想化ソフトウェアで利用可能となるネットワーク仮想化機能、及び、分散ファイアウォール機能について、クラウドサービス上の統合サーバにおいても利用可能なこと。

カ　クラウドサービスIaaS機能により利用可能となるクラウドサービス上の統合サーバにおいて、構築や利用するために必要となるソフトウェアライセンス、ネットワーク機器、回線等がある場合は、それらの調達についても、本業務の範囲内とし、漏れなく準備を行うこと。

5.4.13.　稼働監視サーバ/稼働監視ソフトウェアに関する詳細要件

本業務で利用する稼働監視サーバ/稼働監視ソフトウェアについて、機器、及び、機能に関する以下の詳細要件を満たすこと。

(1) 機器

ア　本システム全体の稼働監視を実施するため、稼働監視サーバを導入するとともに、稼働監視を実施するために必要となる稼働監視ソフトウェアについても合わせて導入すること。

イ　稼働監視サーバについては、統合サーバ上に仮想マシンとして作成してもよいこととするが、稼働監視サーバ用のリソース（CPU、メモリ、ディスク）は、統合サーバにおける必要リソースとは別で用意すること。

ウ　統合サーバを利用した場合、統合サーバ上の HA 機能を利用した冗長化構成を利用することが可能となるため、フェイルオーバーが発生した時も稼働監視にかかる各機能が正常に動作するように設計すること。

(2) 機能

ア　稼働監視を行うために、各仮想マシンにエージェントソフトウェアをインストールする必要がある場合は、インストールに関する各種マニュアルの整備や障害発生時の切り分け支援等についても本業務の範囲内とする。

イ　稼働監視用エージェントソフトウェアについては、必要数分のライセンスを用意すること。また、1ライセンス単位で追加購入が可能なこと。

5.4.14.　ログ収集サーバに関する詳細要件

本業務で利用するログ収集サーバについて、機器、及び、機能に関する以下の詳細要件を満たすこと。

(1) 機器

ア　本システム全体のログを収集するため、ログ収集サーバを導入すること。

イ　ログ収集サーバについては、統合サーバ上に仮想マシンとして作成してもよいこととするが、ログ収集サーバ用のリソース（CPU、メモリ、ディスク）は、統合サーバにおける必要リソースとは別で用意すること。

ウ　統合サーバを利用した場合、統合サーバ上の HA 機能を利用した冗長化構成を利用することが可能となるため、フェイルオーバーが発生した時もログ収集にかかる各機能が正常に動作するように設計すること。

(2) 機能

ア　本システム全体のシステムログ、アラートログ、ステータスログや発生したイベント情報等を収集・保管できること。

イ　統合的なログ管理機能を有すること。なお、収集したログの中から時間、及び、文字列で検索可能であること。

ウ　収集した各種ログは閲覧可能な形式で 3 カ月分、アーカイブ形式で 3 年間保存し、県の求めに応じ開示できること。

エ　リモート保守環境における認証ログ、利用ログを保存し、リモート保守環境利用事業者側から確認できるようにすること。

5.4.15.　VDI 接続制御用ファイアウォールに関する詳細要件

本業務で利用する VDI 接続制御用ファイアウォールについて、機器、及び、機能に関する以下の詳細要件を満たすこと。

(1) 機器

ア　本システムにおける VDI 環境にかかる接続制限を行うため、VDI 接続制御用ファイアウォールを導入すること。

(2) 機能

ア　セキュリティ対策として、各 VDI 上の仮想デスクトップから接続できるネットワークが~~を~~最小限~~単位~~になるよう設計を行うこと。

5.4.16.　Active Directory に関する詳細要件

本業務で利用する Active Directory について、機器、及び、機能に関する以下の詳細要件を満たすこと。

(1) 機器

ア　本システムにおける、ユーザ管理、権限管理等を行うため、Active Directory を導入すること。

イ　Active Directory については、統合サーバ上に仮想マシンとして作成してもよいこととするが、Active Directory 用のリソース（CPU、メモリ、ディスク）は、統合サーバにおける必要リソースとは別で用意すること。

ウ　統合サーバを利用した場合、統合サーバ上の HA 機能を利用した冗長化構成を利用することが可能となるため、フェイルオーバーが発生した時も Active Directory にかかる各機能が正常に動作するように設計すること。

(2) 機能

ア　Active Directoryにより、本システム全体のユーザ管理、権限管理等が実施できること。

イ　ドメイン名は、既存共通機能基盤における「miekiban.local」を引き継ぐこと。

ウ　各情報システム担当職員のユーザ情報として、既存のActive Directoryとして、別途構築している「mieken.jp」ドメインのユーザ情報等を参照できるようにするため、「mieken.jp」ドメインとの信頼関係を設定すること。

5.4.17.　L2スイッチに関する詳細要件

本業務で利用するL2スイッチについて、機器、及び、機能に関する以下の詳細要件を満たすこと。

(1) 機器

ア　本業務を実施するうえで必要となるL2スイッチについて、必要な場所に必要数を導入すること。

イ　L2スイッチの仕様として、以下の要件を満たすこと。なお、下表は1台当たりの仕様であるため、注意すること。

表 5.8 L2スイッチ

No	項目	機能
1	機能・仕様	・本システム内のネットワーク帯域は10Gbps以上×2（冗長化構成）とすること。 ・100BASE-TX/1000BASE-T対応ポートを必要数用意すること。なお、三重県情報ネットワークのスイッチからの割り当ては1Gbps単位であるため、必要ポート数を見積もること。 ・今後の拡張性を考慮し、1Gbps×8ポート以上の予備ポートを確保できること。さらに、iSCSI用ポート等の予備として4ポート以上を確保できること。 ・冗長化構成として、2台単位で利用することとし、設定情報等は2台で共有できること。 ・L2レベルで論理的に分割可能な設計が行える機器を選定すること。 ・IEEE802.1Q機能を有すること。 ・STP、RSTP、及び、MSTP機能を有すること。 ・リンクアグリゲーション機能（IEEE802.3ad準拠）を有し、8ポート以上のグルーピングが可能であること。 ・マルチキャスト、及び、ブロードキャストのストーム発生

		を抑制できること。 ・SNMPエージェント機能を有すること。 ・Webインターフェース、又は、コマンドラインインターフェースによる設定が可能であること。コマンドラインインターフェースはtelnet、又は、SSHをサポートすること。
2	電源装置	・電源の冗長化をすること。
3	その他	・筐体形状はラックマウント型であること。

5.4.18.　NAS に関する詳細要件

本業務で利用する NAS について、機器、及び、機能に関する以下の詳細要件を満たすこと。

(1) 機器

ア　バックアップを行う必要のないデータを保存するために、iSCSI 対応の NAS（実効容量 12TB 以上、RAID5 構成）を 6 台用意すること。

イ　NAS の利用場所は IDC1 を原則とするが、本県の指示により、別拠点への設置が可能なこと。

(2) 機能

ア　本システムを利用する仮想マシンから iSCSI によるマウントが可能なこと。

イ　ディスク障害が発生した際に、交換用ディスクが購入可能であり、かつ、障害が発生したディスクを交換することにより自動復旧が可能な ~~RAID 構成が取れる~~こと。

5.4.19.　その他付帯設備装置に関する詳細要件

本業務で利用するその他付帯設備装置について、機器に関する以下の詳細要件を満たすこと。

(1) 機器

ア　その他付帯設備装置（KVM 装置、ディスプレイ、キーボード等）ついては、最適な機器を選定し、必要数を導入すること。

イ　その他付帯設備装置の仕様として、以下の要件を満たすこと。なお、下表は 1 台当たりの仕様であるため、注意すること。

ウ　下表に記載のない項目に関しては、本仕様書の各要件を満たす構成とすること。

エ　その他付帯設備装置に関して、本要件とは異なる構成による構築も可とするが、構築時や定常業務時だでなく、障害や異常が発生した異常時業務時においても、制限なく利用ができるものとすること。

表 5.9 KVM スイッチ

No	項目	機能

1	筐体形状・サイズ	・ラックマウント型　1U 以内
2	ポート数	・必要数
3	KVM スイッチ接続用ケーブル	・各機器と KVM スイッチとの接続に必要となるケーブルについて、必要数を納入すること。
4	その他	・各サーバと接続する上で必要となるアダプタ類、ケーブル類、電源コード（OA タップを含む）等を全て納入すること。

表 5.10 ディスプレイ、キーボード等

No	項目	機能
1	形状	・ラックマウント型で省スペース型とすること。
2	KVM スイッチ	・ディスプレイ、マウス、キーボードについて、別途納入する KVM スイッチで接続先サーバの切り替えができること。
3	ディスプレイ	・画面サイズは 17 インチ以上とすること。 ・液晶ディスプレイであること。 ・1024x768 ドット以上の表示が可能なこと。
4	キーボード	・Windows 配列準拠であること。
5	マウス	・標準的なマウスとすること。
6	その他	・各サーバと接続する上で必要となるアダプタ類、ケーブル類、電源コード（OA タップを含む）等を全て含むこと。

5.5. 運用保守業務における要件

運用保守業務における要件の詳細は、以下のとおり。運用保守設計時に、以下の詳細要件を実現できるよう設計を行うこと。

5.5.1. 運用保守業務における基本事項

運用保守業務における基本事項として、以下の要件を満たすこと。

(1) 役割分担について

ア　受託事業者、共通機能基盤担当職員、情報システム担当職員、又は、情報システム受託事業者の役割分担については、現行システムにおける役割分担を踏襲すること。

イ　既存共通機能基盤における運用保守業務の役割分担については、参考資料 1「統合サーバの利用について」、参考資料 2「統合サーバ利用ガイドライン_ver1.2」、参考資料 3「リモート保守環境の利用について」、参考資料 4「リモート保守環境利用ガイドライン_ver1.2」を参照すること。

(2) リモート保守環境の利用

ア　運用保守業務について、オンサイトでの作業の他、本業務で構築するリモート保守環境を利用しての作業も可とする。

イ　リモート保守環境を利用する場合は、技術的、セキュリティ的な制限事項等により対応できない業務も想定されるので、その場合は、オンサイトでの対応を行うこと。

ウ　リモート保守環境による運用保守業務~~作業~~を行う場合、IP-VPN 接続によるリモート保守環境を利用すること。IP-VPN 接続を行うために必要となる回線費用についても、本業務の範囲内とする。なお、IP-VPN 接続用貸し出し端末としては、本業務において別途運用保守業務を行うための専用端末として納品予定の~~された~~端末の内、受託事業者側に設置した端末を利用することを想定しているが、2 ~~複数~~台以上の利用が必要な場合は、IP-VPN 接続用貸し出し端末を追加で必要数納品したうえで利用すること。

エ　リモート保守環境を利用して運用保守業務を実施する際に利用する端末は、本業務専用の端末として利用することとし、セキュリティ対策、盗難防止対策等を実施したうえで、操作ログ等についても取得すること。

(3) 業務種別

ア　運用保守業務のうち、本システムを定常的に運用するに当たり、随時、又は、定期的に必要となる業務を「定常業務」とする。

イ　運用保守業務のうち、障害や異常の発生時など、緊急、かつ、突発的な対応が必要となる業務を「異常時業務」とする。

(4) 対応時間

ア　定常業務の対応時間は、開庁日の概ね 8 時 30 分から 17 時 15 分までとする。なお、定常業務のうち、本システムの運用に著しい影響を及ぼす作業については、開庁日夜間、又は、閉庁日に行うこと。

イ　異常時業務の対応時間は、24 時間 365 日とし、異常有無を常時監視するための監視センターを組織すること。ただし、個別の事象により本県が承認した場合にはこの限りではない。なお、異常時業務に伴い発生する定常業務については、異常時業務と同等の対応時間とする。

ウ　定常時、異常時に関わらず、メール、又は、電話による受付窓口は 24 時間 365 日とすること。

(5) 定常業務時の体制

ア　本システムを利用している各情報システムの安定的な稼働を行うため、受託事業者によって提供される運用保守業務は、高いサービス品質の確保が求められる。そのため、「地方公共団体の情報システム調達仕様書における非機能要件の標準化に関する調査研究報告書」（※）に記述されている「RTO（目標復

旧時間）（業務停止時）：６時間以内」、「システム再開目標（大規模災害時）：３日以内」、「稼働率：９９．５％（年間稼働率）」等を参考に、本システムにおけるサービス基準・目標を設定し、本県の承認を得ること。

イ　受託事業者は、運用保守業務における各要件を満たすために必要となる~~な~~体制を整備し、責任をもって対応すること。

ウ　本システムで利用する仮想化ソフトウェア等にかかる開発元等に対して問い合わせ等が可能な体制、又は、それに準じる体制を整備すること。

エ　上記のサービス基準・目標、及び、運用保守業務における各要件が達成できなかった場合には、新機器の導入や体制の強化等の対応を行うこと。

(6) 異常時業務時の体制

ア　本県からの対応依頼、又は、対応が必要な事象が発生してから、初期対応を開始するまでの時間を、概ね 30 分以内とすること。大規模災害発生時においても可能な限り当該時間を目標に対応すること。なお、初期対応とは、対象箇所・原因の確認作業への着手、本県並びに本県が指定する所定の連絡先への連絡等を指す。

イ　本県からの対応依頼、又は、対応が必要な事象が発生してから、事象が発生した原因を究明し作業方法を決定するまでの時間を、概ね 90 分以内とすること。大規模災害発生時においても可能な限り当該時間を目標に対応すること。

ウ　作業員が作業場所に到着するまでの時間を開庁日の 8 時 30 分から 17 時 15 分までは 2 時間以内、上記以外の時間帯は 4 時間以内とすること。ただし、個別の事象により本県が承認した場合にはこの限りではない。大規模災害発生時においても可能な限り当該時間を目標に対応すること。

エ　作業方法が明らかになり、かつ作業が必要な場所へ到着してから、作業が完了するまでを概ね 6 時間以内とすること。また、6 時間以内の作業完了が困難と判明した場合は、1 時間以内に進捗状況と以降の対応スケジュールを本県に報告すること。

オ　作業の完了を確認してから、本県並びに本県が指定する所定の連絡先に通報するまでの時間を概ね 30 分以内とすること。

カ　障害箇所が冗長化されており本システムにおける各種機能が停止していない場合で、かつ、障害対応の際も本システムにおける各種機能が停止しない場合は、本県の承認を得たうえで、翌開庁日の 8 時 30 分から 17 時 15 分での対応も可とする。~~左記以外の場合は、本県が指定する開庁日もしくは夜間での対応を行うこと。~~

キ　障害発生時に仮想化ソフトウェア開発元と連携が可能な体制、又は、それに準じる体制を整備すること。

ク　障害対応の実施に当たっては、受託事業者は各情報システム情報担当職員、

及び、情報システム受託事業者との連携を図り、復旧に向けて、必要となる対応を行うこと。

(7) 各業務システムからの総合窓口~~受付~~機能（ポータル機能）

ア　各情報システム担当職員、及び、情報システム受託事業者からの依頼事項や問い合わせを受託事業者へ直接連絡できる機能（ポータル機能）を持つ、専用のポータルサイトを構築すること。

イ　ポータルサイトの利用者は、共通機能基盤担当職員、受託事業者、各情報システム担当職員、及び、情報システム受託事業者とし、それぞれのユーザ管理が実施できること。また、~~本業務の~~共通機能基盤担当職員、及び、受託事業者には、ポータル機能における管理者権限等の付与ができること。

ウ　各情報システム側から、受託事業者に対して、直接各種操作依頼等ができること。

エ　共通機能基盤担当職員、及び、受託事業者は、全ての作業依頼等の内容を閲覧できること。

オ　共通機能基盤担当職員、及び、受託事業者から各情報システム担当職員、及び、情報システム受託事業者に対して、掲示板機能等により周知が可能なこと。

カ　必要な情報が掲載された場合、ユーザ単位でメール等による通知が可能なこと。

キ　本システムを利用するうえで必要となる統合計画書や各種設定を安全にやり取りするための機能として、ファイル交換等の機能が利用できること。

ク　ポータルサイトは、本システム内におけるクラウドサービス上に構築することも、本システム以外のクラウドサービス上に構築することも可とするが、いずれの場合においても、当該、ポータルサイトを稼働させるために必要となる費用について、本業務の範囲内に含めること。

(8) 保守部品

ア　冗長化できない部位等については、製造会社等の 24 時間 365 日オンサイト保守対応を契約するなど、迅速な復旧が実施~~実現~~できるようにすること。

イ　冗長化できない部位等の内、製造会社等の 24 時間 365 日オンサイト保守対応が不可能な場合は、予備品の保有等により迅速な復旧を実施~~実現~~できるようにすること。

ウ　必要に応じて、保守部品（付属品、ソフトウェアを含む。）を常時保有するとともに、契約期間における安定的な供給が可能なこと。

5.5.2.　定常業務に関する要件

運用保守業務の内、定常業務として以下の業務を実施すること。

(1) 問い合わせ、及び、作業依頼対応

ア　共通機能基盤担当職員、又は、情報システム担当職員、情報システム受託事業

者からの総合窓口、電話、メール等による問い合わせや作業依頼等について、対応を行うこと。

イ　各種対応を実施する場合は、共通機能基盤担当職員の承認を受けたうえで、実施することとするが、本県との事前協議により、承認不要とした内容については、適宜、対応を行うこと。

ウ　総合窓口以外による連絡があった場合は、総合窓口への事後入力を行うこと。

(2) 手順書等の作成

ア　運用保守業務を実施するうえで、必要となる運用保守手順書を漏れなく作成すること。なお、障害時の緊急対応方法については、必ず明記すること。この時、作業を実施する担当者(受託事業者、共通機能基盤担当職員、情報システム担当職員、情報システム受託事業者など)が明確化されていること。

イ　運用保守業務を実施するうえで、共通機能基盤担当職員、情報システム担当職員、又は、情報システム受託事業者による操作が必要となる場合には、容易に作業できるよう操作説明書（インストール手順書を含む本システムの利用者向け説明資料等）を作成すること。なお、共通機能基盤担当職員、情報システム担当職員、又は、情報システム受託事業者による本システムに対する機器操作については必要最小限にとどめること。

ウ　手順書等の内容に関しては、レビュー会を設けて本県に対し十分な説明を行い、本県の承認を得ること。

エ　運用保守業務における作業内容の変更等により、手順書等の修正が発生した場合には履歴管理を行ったうえで速やかに各種手順書を修正すること。

オ　手順書の修正に当たっては本県へ説明を行い、承認を受けたうえで本県に提出すること。

(3) 説明会・教育の実施

ア　本システム稼働前に本県に対して、本システムについての説明、及び、各機器の操作教育を実施すること。実施場所や方法については、本県と協議のうえで決定すること。

イ　本県の共通機能基盤担当職員が変更となる場合などには、本県の要望に応じて再度教育を実施すること。

ウ　年 1 回程度、リストア手順書に基づくリストア訓練を実施すること。また、本県が実施する ICT-BCP 訓練や脆弱性診断等に参加すること。これらの訓練、及び、診断の結果、必要に応じて運用の見直しや運用保守手順書等の修正を行うこと。

エ　仮想化技術の最新動向、将来的な本システムの検討に有益な情報を定期的に（年 1 回程度）提供し、本県の共通機能基盤担当職員に説明を行うこと。

(4) 情報システムの仮想化時における支援

ア　情報システム担当職員、又は、情報システム受託事業者が、統合サーバを利用する際、仮想マシンのサイジングや、統合方法の決定において必要となる各種支援を行うこと。

イ　仮想マシンの作成（プロビジョニング）を行うこと。

ウ　仮想マシンの雛形（クローン、テンプレート）を作成し、容易に展開（デプロイ）ができるようにすること。

エ　~~原則として、~~契約期間中において、情報システムを新たに仮想化する際は、原則としてP2Vによる仮想化ではなく、新規OSインストール、システムインストールによる仮想化を想定しているため、必要な支援を行うこと。

オ　契約期間中、例外的に、P2V や V2V を行う必要が生じた場合には、環境の整備や操作の実施等において、問い合わせ対応や障害対応等の支援を行うこと。

(5) リモート保守環境の導入時における支援

ア　情報システム受託事業者が、新たにリモート保守環境を利用する際に必要となる各種支援を行うこと。

イ　リモート保守環境を新たに利用するために必要となるユーザ作成、SSL-VPN設定、IP-VPN設定、VDI設定、IP-VPN貸し出し端末設定等の対応を行うこと。

ウ　新たにIP-VPN接続によるリモート保守を実施する場合は、本県の指示により、閉域網を開設し、利用可能な状態にすること。

エ　新たにインターネット VPN 接続によるリモート保守を実施する~~行う~~場合は、情報システム担当職員、及び、情報システム受託事業者が利用する保守端末について、接続可能かどうかの接続テストを実施すること。

(6) 仮想マシンの運用管理

ア　仮想マシンの構成（メモリ、ディスク、プロセッサ数、ネットワークなど）変更、削除、移動等の仮想マシンについての運用を行うこと。

(7) 日常設定変更

ア　本環境を構成する、統合用サーバ、各種ストレージ、仮想化管理サーバ、及び、それらに付帯する装置の日常的な設定変更を行うこと。

(8) 構成管理

ア　本システムにて導入される、ハードウェア、及び、ソフトウェアの構成管理を行うこと。

イ　仮想マシンのCPU、メモリ、ディスク、OS等の構成管理を行うこと。

(9) ユーザ管理・権限管理

ア　仮想マシンごとに、ActiveDirectory で管理されたユーザを割り当て、仮想マシンの操作権限を付与し、ユーザを管理すること。

イ　ユーザ毎に適切な操作権限を付与し、権限を管理すること。

ウ　リモート保守環境のユーザ追加、変更等の設定変更作業を行うこと。また、利用者情報を一元管理し、利用者情報と利用状況について県に対し定期的に報告を行うこと。

(10)稼働・性能監視

ア　各機器（仮想マシンを含む）の稼働状態やサービスプロセス等について異常が発生していないかについての稼働監視を行うこと。

イ　各機器のリソース（CPU 使用率、メモリ使用率、ディスク使用率）について、性能不足や容量不足等が発生していないか性能監視を行うこと。

ウ　稼働監視、及び、性能監視における監視内容の詳細として、方法（死活監視、サービス監視、プロセス監視、http 監視等）や閾値、時間間隔等について、本県と協議のうえ、定めること。

エ　異常（閾値を超えた状況など）が検知された場合、本県並びに本県が指定する所定の連絡先に通報すること。

オ　適正な範囲外の状態が継続する場合は、対策案を報告し、本県の承認のうえ、対策を講じること。

カ　必要に応じて、監視のチューニングを行うこと。

キ　必要に応じて、監視対象の追加等を行うこと。

(11)ログ管理

ア　本システムに関する各種ログ（エラーログ、メール送信ログ等）を収集、保管すること。

イ　ログ内容について異常がないかチェックし、定期的に報告を行うこと。提出方法の詳細については、本県と協議のうえ、定めること。

ウ　仮想マシン上の情報システムのログについては、情報システム受託事業者が取得、及び、対応を行うこととするが、ログのうち、仮想マシンに関するログについては情報システム受託事業者からは確認ができないため、受託事業者が必要に応じて提供を行うこと。

(12)セキュリティ管理

ア　本システムに関する不正アクセスの有無や、ウイルス検出件数等をチェックし、定期的に報告を行うこと。

イ　仮想マシン上の情報システムのセキュリティ対策については、情報システム受託事業者が対応を行うこととするが、本件で調達する物理機器上のセキュリティ対策については、受託事業者が管理を行い、不正アクセスが検知された場合は、速やかにセキュリティ侵害の有無や影響の範囲等を調査し、報告を行うこと。なお、セキュリティ侵害があった場合は、速やかに対策を施したうえで復旧させること。セキュリティ侵害が無くても、脆弱性が発見された場合についても対策を実施すること。

(13)パッチの情報提供

ア　本システムで使用するソフトウェア製品に関するバグフィックス、セキュリティ対応等のパッチがリリースされた場合、その内容の調査を行い、適用の可否を本県に報告すること。また、安全性等の観点から即時適用することが好ましくないと判断される場合は、適用の可否について本県と協議のうえ、決定すること。

イ　緊急度の高いものは、パッチリリース情報を開庁日 3 日以内に報告すること。

(14)パッチのインストール

ア　安定した動作等のために本システムへの適用が必要、かつ、本システムへの悪影響がないと受託事業者が判断したパッチのインストールを行うこと。

イ　パッチ適用作業は、原則としてオンサイトでの作業とする。ただし、重大な影響がない場合は、リモートでの対応も可とする。

ウ　パッチ適用作業の際には、作業計画（作業後の動作確認の内容、作業時間、切り戻し作業等）について、本県と協議すること。

エ　パッチ適用による障害が発生した場合は、受託事業者にて障害対応を行うこと。

オ　緊急度が低く、かつ、本システムの停止を伴うパッチ適用作業については、まとめて適用することを可とする。

カ　パッチ適用作業について、停止時間が短くなるよう、かつ、適用漏れが発生しないよう、年間計画等を策定し、計画的に実施すること。

(15)バージョンアップの情報提供

ア　本システムで使用する全てのソフトウェア製品（ファームウェアを含む）のバージョンアップ製品がリリースされた場合、その内容の調査を行い、適用の可否を本県に報告すること。また、安全性等の観点から即時適用することが好ましくないと判断される場合は、適用の可否について本県と協議のうえ、決定すること。

イ　緊急度の高いものは、バージョンアップリリース情報を開庁日 3 日以内に報告すること。

(16)バージョンアップの実施

ア　安定した動作等のために本システムへの適用が必要、かつ本システムへの悪影響がないと、受託事業者が判断したバージョンアップ作業を実施すること。

イ　バージョンアップ作業は、原則としてオンサイトでの作業とする。ただし、重大な影響がない場合は、リモートでの対応も可とする。

ウ　バージョンアップ作業の際には、作業計画（作業後の動作確認の内容、作業時間、切り戻し作業等）について、本県と協議すること。

エ　バージョンアップ作業による障害が発生した場合は、受託事業者にて障害対

応を行うこと。

オ　緊急度が低く、かつ、本システムの停止を伴うバージョンアップ作業については、まとめて対応することを可とする。

カ　バージョンアップ作業について、停止時間が短くなるよう、かつ、適用漏れが発生しないよう、年間計画等を策定し、計画的に実施すること。

(17)データバックアップ

ア　システム障害等に備え、迅速に復旧が可能となるよう、適切に設定情報や各種バックアップデータを取得すること。

イ　システム障害等に備え、仮想マシンのバックアップデータを取得すること。詳細は、「5.4.5 メインストレージ/バックアップストレージに関する詳細要件」を参照すること。

ウ　仮想マシン上の情報システムにかかる設定変更や、セキュリティパッチのインストール等にかかる情報システムのバックアップは、情報システム担当職員~~所属~~、又は、情報システム受託事業者が対応を行うこととする。

(18)リブート

ア　本システムを安定的に稼働させるために、必要となる定期的なリブートを実施すること。

イ　仮想マシン上の情報システムについても依頼があれば、リブート等の対応を行うこと。

(19)各種報告書の作成・提出・報告

ア　運用保守報告書として、定期レポート（月次）を作成し、各情報システム(各仮想マシン)の CPU、メモリ、ディスクの消費リソース状況を報告すること。

イ　運用保守業務を実施する都度、運用保守作業報告書（障害記録を含む）を、作成し、報告すること。

ウ　障害対応を実施した際は、運用保守作業報告書として、障害の事象、影響、原因、及び、対策方法等をまとめ、速やかに提出すること。

エ　運用保守における課題や、作業依頼に対する対応状況について課題管理表等を作成し毎月提出すること。

オ　提出方法についての詳細は、本県と協議のうえ、定めること。

(20)月例報告会

ア　月例報告会として、運用保守業務にかかる報告会を毎月開催すること。

イ　月例報告会では、運用保守報告書等にかかる報告の他、必要に応じて、各種課題や要望事項等にかかる本県に対しての相談、協議等を行うこと。

ウ　月例報告会で報告する内容は、本システムを安定的に運用するために必要な内容とし、具体的には、以下の内容を想定している。

- 作業依頼に対する作業進捗状況

- 各種課題とそれに対する検討状況
- 各種要望に対する検討状況
- 各種導入機器、及び、ソフトウェア開発元ベンターからのアップグレード情報やサポート情報
- 各種ソフトウェアにおける脆弱性情報とその対応策
- 各種障害情報とその対応状況
- 共通機能基盤における各種サービスの利用状況
- 保有ライセンスとライセンスの利用状況
- バックアップ等の共通機能基盤側が提供しているサービスの提供状況
- その他必要な情報

5.5.3.　異常時業務に関する要件

運用保守業務の内、異常時業務として以下の業務を実施すること。

(1) 情報システムのリストア

ア　仮想マシン上の情報システムにおいて障害や異常等の発生時、及び、本県からの依頼があった場合において、バックアップデータからのリストアを実施すること。

イ　リストア作業は依頼内容に応じて、~~から~~ファイルレベルでのリストア、又は、イメージレベルでのリストアをリストア手順書に基づき実施すること。

(2) 障害一次切り分け

ア　本県からの連絡や監視システムにおける通知メール等により、本システム、及び、本システムを利用している情報システムにおいて、障害や異常が発生したことを確認した場合、共通機能基盤担当職員、情報システム担当職員、又は、情報システム受託事業者と協力のうえ、障害の原因切り分けを行うこと。

イ　原因切り分けを行っても、障害原因が不明の場合は~~であっても~~、迅速な障害対応のため、引き続き、受託事業者が原因究明作業を実施すること。

ウ　切り分けを行った結果、本業務以外で調達したハードウェア、及び、ソフトウェアが原因の場合、又は、仮想マシン上の情報システム自体が原因の場合は、共通機能基盤担当職員に速やかに引継を行うこと。

(3) 障害対応

ア　本システム、及び、本システムを利用している情報システムにおいて、障害や異常が発生した場合には、本県並びに本県が指定する所定の連絡先に通報したうえで、必要な障害対応を行うこと。

イ　障害対応として、リモート保守による対応を可とするが、オンサイトでの対応が必要な場合は、障害発生拠点への駆けつけや、不良部品の交換等を行うこと。

ウ　部品交換等を実施した場合は、交換した機器等にかかる設定等についても実

施し、本システムを正常稼働状態に復帰させること。

エ　障害等により本システムで利用しているソフトウェアや各種データ~~や~~、本システムを利用している情報システムにおけるデータ等が破損した場合、バックアップデータ等により速やかに復旧を行うこと。また、必要に応じて、本システムの再セットアップを行うこと。

(4) 障害後是正措置・予防措置

ア　障害が発生した場合、障害に関する情報を収集したうえで、その障害情報をもとに原因を分析し、同様の障害が発生しないように是正措置・予防措置を講じること。また、直ちに障害原因が判明しない場合は、本県の承認を得たうえで、継続して調査を行い、障害原因の特定に努めること。

イ　障害情報、是正措置・予防措置の内容は障害記録として体系的に記録し、常に活用できるように保存すること。

6. 機器及びソフトウェア等に関する要件

本業務で納入する機器（ハードウェア）、及び、ソフトウェア等について、以下の要件を満たすこと。

(1) 共通要件

ア　ハードウェア、及び、ソフトウェア（アプリケーション、ミドルウェア、ファームウェア等を含む）について、全て買い取りで提供すること。

イ　ハードウェア、及び、ソフトウェアは中古品であってはならない。なお、ソフトウェアについては、ライセンス、又は、サブスクリプション契約による利用権等として納品すること。

ウ　ハードウェア、及び、ソフトウェアは、契約期間中に製造会社の製品サポート（セキュリティパッチ、脆弱性対策技術情報）の終了が予定されていない製品を選定すること。なお、契約期間中に本システムで利用している製品のサポートが終了する場合は、受託事業者の責において後継製品や同等の性能を持った代替製品への移行を行い、継続してサポートが受けられるように対応を行うこと。その場合、当該製品がサポート終了を迎える前に、本県に代替品の承認を受けること。ただし、Microsoft 製品における Server 用 OS の内、Windows Server2022 に限っては、予定されているサポート終了日が 2031 年 10 月 14 日であり、運用期間中にサポート終了を迎えることになると想定されるため、Windows Server OS にかかるライセンス調達時において、当該バージョン以降の新たなバージョンがリリースされない場合に限って、当該ソフトウェアにかかる後継製品や同等の性能を持った代替製品への移行、及び、継続

してサポートが受けられるよう対応すること、の双方について、本業務の範囲外とする。

エ　本仕様書に記述されている要件を満たすハードウェア、及び、ソフトウェアを納入することとするが、本仕様書に記述されている以外にも新たなハードウェア、又は、ソフトウェア等を用意してもよい。ただし、その場合、ハードウェア、又は、ソフトウェア等の機能、性能等を記述した資料を提出し、本県の承認を受けること。

オ　本業務の遂行に必要となる消耗品等の全てについて、契約期間内において必要な量を見積り、提供すること。

(2) ハードウェア要件

ア　本業務で納入する全てのハードウェアについて、機能・性能、及び、保守運用面等を検討のうえで最適なものを選定すること。

イ　本業務で納入する全てのハードウェアは、ラックマウントを前提とした機器選定を行うこと。なお、ラックマウントができない機器を納入する場合は、耐震や盗難対策等として、セキュリティワイヤーや固定ベルト等を用意すること。

ウ　本業務で納入する全てのハードウェアは、概ね同機種、又は、同系統の機種において多数の導入実績があること、及び、各種規格団体の規格を満たしていること。

エ　「みえ・グリーン購入基本方針」、及び、「環境物品等の調達方針」に適合していること。

オ　導入する機器については、性能や機能の低下を招かない範囲で、消費電力節減、発熱対策、騒音対策等の環境配意を行うことが望ましい。

(3) ソフトウェア要件

ア　本業務において調達するソフトウェアライセンスについては、本業務の契約終了後も本県において継続して利用できるよう、県を使用者名義とすること。ただし、県を使用者名義とすることが認められていないソフトウェアについては、適切な使用者名義を設定し、本業務にて利用できるようにすること。

イ　ソフトウェアライセンスについては、契約時の最新バージョンの使用権を確保すること。なお、最新バージョンを使用しない場合は、最新バージョンの使用権を確保したままダウングレードを行うこと。また、契約期間中にソフトウェアのサポート切れを迎えることが判明した場合は、本県と協議のうえ、本業務の範囲において後継製品等にかかるライセンスの準備、及び、バージョンアップ作業を実施すること。

ウ　ウイルス対策ソフトについて、必要に応じて本県が保有している以下のライセンスを利用することができる。

・Trend Micro ApexOne

・Trend Micro Server Protect for Linux

エ　Microsoft 社製の製品を新規で購入する場合は、調達数量や購入条件に応じて ESA、SCE、Select Plus for Government、SPLA、CSP 等を利用することができる。

オ　~~また、~~Windows server 2022 のユーザ CAL、及び、デバイス CAL は、別途本県で調達する予定のため、本業務の範囲外とする。

カ　原則としてサポートが受けられないソフトウェアの利用は許可しない。

キ　ソフトウェアについて、サブスクリプション契約による利用権等として納品することも可とするが、運用期間が終了するまでの間に利用出来なくなるとの予定が発表されているものは選定しないこと。

7. データセンターに関する要件

本業務で利用するデータセンターについて、以下の要件を満たすこと。

(1) データセンターの選定にかかる要件

ア　本システムにおける主要な機器を設置するデータセンターとして三重県情報ネットワークに接続された津市内データセンター（IDC1）にハウジングラックを必要数準備すること。

イ　バックアップ用ストレージを設置するデータセンターとして、IDC1 とは異なるデータセンター（IDC2）にハウジングラックを必要数~~を~~準備すること。なお、IDC2 の選定に当たっては、ファシリティ要件、及び、自治体等の利用実績を事前に提示し、本県の承認を得ること。なお、ファシリティ要件については、日本データセンター協会が定めるティア３相当を想定している。

ウ　IDC2 については、三重県情報ネットワークから IDC2 へ接続するためのネットワーク機器、回線等についても、本業務にて用意すること。

エ　IDC2 は IDC1 から物理的に十分離れているなど、南海トラフ巨大地震等の大規模災害発生時において、同時被災がないと想定されるデータセンターを選定すること。

オ　IDC2 については、「5.4.12.クラウドサービスに関する詳細要件」にて設計を行ったクラウドサービスを利用する形も可とする。

カ　IDC1 として、本県が指定する津市内データセンター以外のデータセンター（以下、「受託者が用意するデータセンター」という。）を利用することも可とするが、そのデータセンターを三重県情報ネットワークに接続するための専用回線（~~42~~Gbps 以上の帯域保証）、及び、ネットワーク機器の用意の他、その構築、及び、運用保守についても本業務に含めること。

キ　受託者が用意するデータセンターの選定に当たっては、IDC2 と同等以上のファシリティ要件を満たすこと。

ク　本県職員が、IDC1、IDC2 内に設置したラックや各機器の設置状態について、確認が可能なこと。また、確認を行う際は、入館申請等必要な対応を行なうこと。

(2) ハウジング等の詳細に関する要件

ア　準備するハウジングラックとして、機器を設置するために必要となるラックの他、電源、通信回線、ラック間配線等、本システムで利用するために必要となるものがあれば漏れなく用意すること。

イ　委託期間終了までにラックの追加・変更が必要な場合は、本県の承認後、本業務の範囲内で実施すること。

ウ　データセンターに IP-VPN 利用回線を準備する際、回線引込み箇所から共通機能基盤用ラックまでの配線は、全て本業務の範囲内とする。

エ　IDC1、及び、IDC2 に準備するハウジングラックで必要とされる~~の~~電源容量について確認を行い、必要に応じて追加電源の契約を行うこと。

オ　停電等の対策として必要な場合は非常用電源の準備を行うこと。ただし、データセンター内の停電対策が十分な場合で、かつ、その対策を利用する場合は、停電対策は不要とする。

カ　契約するハウジングラック数として、構築作業時の同時作業人数、耐荷重、必要電源、ラック間配線等を考慮し、必要十分なハウジングラック数を準備する~~が利用できる~~こと。

8. クラウドサービスに関する要件

本業務で利用するクラウドサービスについて、以下の要件を満たすこと。なお、「政府情報システムのためのセキュリティ評価制度（ISMAP）」に登録されたクラウドサービスを利用する場合は、以下の詳細要件は満たされているものとする。

(1) クラウドサービスの選定にかかる要件

ア　クラウドサービスにかかるサービス提供事業者が情報セキュリティポリシーを利用者に明示していること。

イ　明示しているポリシーの内容が県の情報セキュリティポリシーの規程に反した内容になっていないこと。

ウ　サービス提供事業者の情報セキュリティ管理状況に関する第三者による評価（ISMS 認証取得証明書、外部監査報告書等）が行われていること。

(2) 機能に関する詳細要件

ア　クラウドサービスで取り扱う情報資産がサービス提供事業者により、目的外利用されないこと。

イ　クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムが設置されている建物（以下、「クラウドサービスが利用するデータセンター」という。）は、地震・水害・火災への対策が行われていること。

ウ　クラウドサービスが利用するデータセンターは、日本の法令が適応されること。また、管轄裁判所に関しては、日本国内の裁判所を合意管轄裁判所とできること。

エ　サービス提供事業者若しくはサービスは、情報セキュリティや個人情報保護に係る第三者認証等のレポートにより、その管理水準が適正と認められていること。

オ　クラウドサービスの提供に用いるアプリケーション、サーバ、ストレージ、情報セキュリティ対策機器、通信機器の死活監視・障害監視について監視を行っていること。

カ　クラウドサービスの提供に用いるアプリケーション、サーバ、ストレージ、情報セキュリティ対策機器、通信機器についての技術的脆弱性に関する情報を収集し、適宜対策を行っていること。

キ　情報の盗聴・改ざん等から保護するため暗号化を行っていること。

ク　不要なサービスを停止していること。また、利用する通信プロトコル、ポートは必要最小限とし、利用していない通信プロトコル、ポートはファイアウォール等にて遮断していること。

ケ　アクセス記録が保存されていること。なお、アクセス記録にはログイン成功だけでなくログイン失敗の記録も行われていること。

コ　クラウドサービス上に保存されるデータは暗号化されていること。

サ　データの消失対策として、定期的にバックアップがとられていること。

シ　クラウドサービス上に保存されるデータについてサービス利用終了時に適切に消去されること。なお、暗号化したデータの暗号鍵を無効化することでもデータ消去措置とみなせることとする。

ス　利用しているクラウドサービスにおいて、サービス仕様の変更やサービス終了等が発表された場合、その対応策等を検討する期間を確保するため、サービス提供事業者から事前に通知がされること。

セ　サービスの稼働率や、サポート・問い合わせ窓口等に関する事項が示されていること。

ソ　利用者へ公開された情報セキュリティに関する統一的な窓口が設置されており、情報セキュリティインシデントが発生した際、利用者への報告、 収束に向けた対応等にかかる実施体制が確立されていること。

タ　クラウドサービス提供事業者の免責事項に関する記載があり、その記載内容は利用上問題ないこと。

チ　情報セキュリティインシデントが発生した場合は、情報セキュリティ管理者、及び、情報システム管理者等、並びに CSIRT（デジタル戦略企画課戦略企画班）への報告が可能なこと。

ツ　クラウドサービスの適切な利用のための規定、マニュアル等が整備されていること。

テ　クラウドサービスで利用するアカウントや各アカウントの権限を整理するとともに、認証情報の漏えいやライセンス違反が発生しないよう適切なユーザ管理が実施できること。

ト　クラウドサービス選定時に確認したセキュリティ対策が正しく設定されているかの確認が実施できること。

ナ　クラウドサービス上で利用する IT 資産（端末やサーバの OS・ソフトウェア）について、セキュリティパッチの適応等、適切に脆弱性対応が行われていること。

ニ　クラウドサービスの利用を終了する際、クラウドサービス~~サービス~~で取扱った情報資産について適切に消去されること。

ヌ　クラウドサービスを利用する際、本県のクラウド用認証基盤である、Microsoft 社 Microsoft Entra ID（Azure AD）、又は、Soliton 社 OneGate と連携し、アカウントに関するセキュリティ対策として、多要素認証、シングルサインオン、又は、それらに準じる構成が実現できること。

9. システム構築・設定作業に関する要件

本業務におけるシステム構築・設定等の作業について、以下の要件を満たすこと。

ア　システム構築・設定作業については、「5. システム設計に関する要件」で実施した基本設計、詳細設計、構築設計を元に作業を行うこと。

イ　本システムの構築時に、仮想化ソフトウェア製造元のエンジニアへ技術問合せが行える体制、又は、それに準じる体制を整備すること。

ウ　搬入時に当たって発生した不要物（梱包材等）は速やかに回収し、受託事業者の責任、負担において、安全に廃棄すること。

エ　ラックに各機器を設置する際には、空調・ファンの稼働など、ラック内の温

度に考慮した設置を行うこと。

オ　部品交換の際、機器自体をラックから引き出さなくてもよいように機器間は必要な空間を空けて設置を行うこと。

カ　機器間の空いた空間にはブランクパネル等を使用し、適切なエアフローを確保すること。

キ　機器・電源ケーブル・通信ケーブルの両端にラベル表記すること。

ク　通信ケーブルに負荷のかからないケーブリングを施すこと。

ケ　見栄え良く、整理されたケーブリングを施すこと。

10. 移行作業に関する要件

本業務における移行作業について、以下の要件を満たすこと。

ア　移行作業については、「5. システム設計に関する要件」で実施した移行設計を元に作業を行うこと。

イ　統合サーバにおける仮想マシンの移行について~~移行作業~~は、各仮想マシン~~情報システム~~単位で策定した移行計画に沿って実施すること。

ウ　統合サーバにおける仮想マシン上の情報システム内のデータや設定等において、移行に関する作業が発生する場合は、情報システム担当職員、及び、情報システム受託事業者に対して支援を行うこと。

エ　何らかの理由により、移行計画に沿った移行作業が実施できなかった場合は、速やかに原因となる事象の確認や解決策を検討したうえで、移行計画を再策定し、再度、移行作業を行うこと。

オ　各仮想マシン~~情報システム~~の移行完了後、移行作業内容や懸案事項等をまとめた移行完了報告書を速やかに提出すること。

11. テスト作業に関する要件

本業務におけるテスト作業について、以下の要件を満たすこと。

ア　テスト作業については、「5. システム設計に関する要件」で実施したテスト設計の他、テスト計画書、及び、テスト仕様書を元に作業を行うこと。

イ　本システムが設計どおりに構築されていることの確認を行うこと。想定する機能が利用できないなどの問題が発見された場合は、その原因を解明し、設計、及び、構築内容の見直しを行い、問題を解消したうえで、再度テスト作業を実施すること。

ウ　テスト作業については、原則として移行期間開始前まで完了すること。特に、移行期間開始後は、サービス停止等を行うことができなくなるため、本番稼働

環境における機能、性能、セキュリティ面について、十分な確認作業を行うこと。

エ　全てのテストが問題なく終了したことを記録したテスト結果報告書を作成、報告し、本県の承認を得ること。

オ　テスト結果報告書には、単体テスト、結合テスト、総合テスト、運用テスト、性能テスト等の実施結果を記載すること。

12.運用保守業務に関する要件

本業務における運用保守作業について、以下の要件を満たすこと。

ア　運用保守作業については、「5.システム設計に関する要件」で実施した運用保守設計を元に作業を行うこと。

イ　運用期間に発生する各種依頼や課題等について、毎月月例報告会を開催し、本県に対して毎月報告を行うこと。

ウ　月例報告会の内容については、会議開催後 1 週間を目安に議事録を作成し、本県に対して報告を行うこと。

エ　月例報告会は Web 会議による開催を基本とするが、必要に応じて対面での開催も可とする。

13.その他

13.1. 次々期調達にかかる提案

運用開始から２～３年後に、将来の再構築や機器更新に備え、本システムからの移行方法やバージョンアップ方法について提案を行うこと。また、次々期の再構築や機器更新における移行支援を行うこと。

13.2. 業務終了時に係る作業要件

13.2.1.　基本的な考え方

ア　本業務終了に当たり、次々期共通機能基盤への更新のために必要となる情報の抽出、機器の撤去等の作業を行うこと。

13.2.2.　情報抽出

ア　各機能の設定情報について提供を行うこと。なお、抽出する形式や内容等については、運用期間中に協議のうえ決定する。

イ　各機能のログ情報について、汎用的な形式（XML、CSV 等のテキストファイルを想定）で抽出すること。なお、抽出する形式や内容等については、運用期間中に協議のうえ決定する。

ウ　その他、必要に応じて、次々期共通機能基盤への移行に当たり必要となる情報の提供を行うこと。

13.2.3.　機器撤去

ア　本業務で導入した機器等のうち、本県が指定する機器について、次々期共通機能基盤へ移行後（本業務期間内）に撤去を行うこと。

イ　機器等の撤去に当たっては、機器等に保存された情報が復元できないように消去すること。

13.3. 機密保持

ア　本業務は、三重県電子情報安全対策基準（三重県情報セキュリティポリシー）を遵守して行うこと。当該ポリシーに抵触する行為、又は、事象が発生した場合や、そのようなおそれがある場合は、本県に報告を行い、本県の指示のもと速やかに対応すること。なお、三重県電子情報安全対策基準については、契約後に開示する。

イ　業務遂行上知り得た個人情報、及び、三重県の機密事項について、本業務のみに利用するものとし、契約期間中、又は、契約終了後を問わず第三者に漏えいしないこと。

ウ　それぞれの契約による事務を処理するための個人情報の取り扱いについては、契約書別記「個人情報の取扱いに関する特記事項」を守らなければならない。

13.4. 暴力団等による不当介入に対する対応

(1) 受託事業者は、業務の履行に当たって暴力団、暴力団関係者又は暴力団関係法人等（以下暴力団等という。）による不当介入を受けたときは、次の義務を負うものとします。

ア　断固として不当介入を拒否すること。

イ　警察に通報するとともに捜査上必要な協力をすること。

ウ　委託者に報告すること。

エ　業務の履行において、暴力団等による不当介入を受けたことにより工程、納期等に遅れが生じる等の被害が生じるおそれがある場合は、委託者と協議を行うこと。

(2) 受託事業者が(1)のイ又はウの義務を怠ったときは、三重県の締結する物件関係契約からの暴力団等排除要綱第７条の規定により三重県物件関係落札資格停止要綱に基づく落札資格停止等の措置を講じます。