ＰＣ稼働遮断システム構築業務 仕様書

第１ 基本事項
　１ 業務名
　２ 目的
　３ 契約期間
　４ 構築の背景と方針
第２ 業務の概要
　１ システム構成概要
　２ システム構成の考え方
　３ 業務の範囲
　４ スケジュール及び体制
　５ 成果品
第３ 機能要件
　１ システムの機能
第４ 非機能要件
　１ システムの規模
　２ システム方式に関する要件
　３ セキュリティ要件
　４ バックアップ
　５ サーバ要件
　６ クライアント要件
　７ テスト要件
　８ 手引書の作成
　９ クライアントセットアップ及びクライアント再セットアップ
　１０ 履行場所
　１１ 関係法令等の遵守
　１２ 留意事項

第１　基本事項

１　業務名

ＰＣ稼働遮断システム構築業務

２　目的

本業務は、客観的で適正な勤務時間管理の把握と長時間労働の抑制を図り、職員のワーク・ライフ・バランスの向上、健康の確保の推進を目的として、本県服務給与システム（以下「総務事務システム」という。）と連携して、職員が業務において使用する業務用端末（以下「ＰＣ」という。）のログオン・ログオフ時間の把握、勤務時間等に応じてＰＣの稼働を遮断するシステムの構築を委託するものである。

３　契約期間

契約締結日から令和５年３月 31 日まで

４　構築の背景と方針

(1)　背景

近年、労働力人口が急激に減少し、人材の量的な確保が困難となる中、職員（働く人）ひとり一人が健康でいきいきと働ける環境を整備することがますます重要となっており、本システムを導入し、適切な勤務時間管理を徹底することにより、職員の労働環境の改善を図る。

(2)　方針

本システムは、本県の勤務時間制度、勤務実態等に対応した機能が求められる。

ア　職員それぞれの勤務時間に合わせた対応

本県では、公務能率の向上及び仕事と家庭生活等の両立を推進することなどを目的として、フレックス制を導入している。また、職務の特殊性等により、通常とは異なる勤務時間で勤務する職員もおり、週休日や休暇を含め、職員一人ひとりの勤務実態に応じた勤務管理が可能となる機能が求められる。

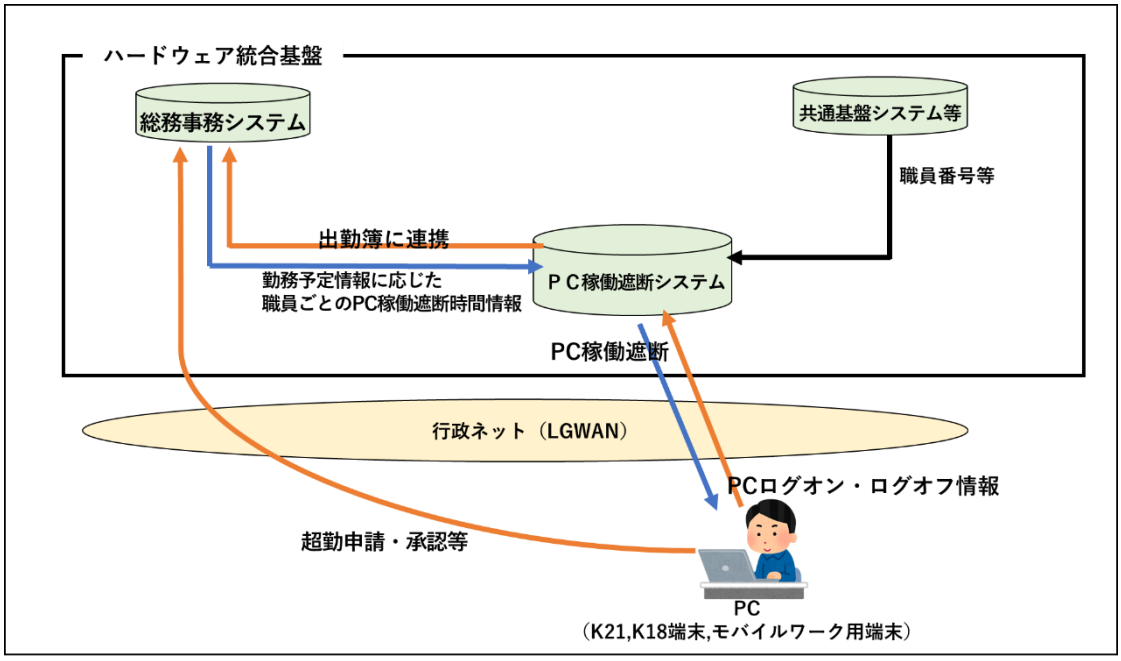
イ　業務遂行体制の確保

本システムは、職員の業務遂行に大きな影響をあたえることから、公務上、真にやむを得ない事情により、緊急に処理することを要する重要な業務が生じた場合においてはＰＣの遮断機能を解除するなど業務遂行体制の確保の観点から必要な機能を備える必要がある。

また、業務内容等により一部の所属や職員を本システムの対象外とするなど、業務執行体制に応じ柔軟に対応する必要がある。

第２　業務の概要

１　システム構成概要



※本県では、庁内のネットワークをインターネット接続系、行政ネット（LGWAN）接続系及び個人番号利用事務系の３層に分離しており、相互の通信は特定のもののみ許可している。本システムは、行政ネットワーク（プライベートネットワーク）を利用する。

※共通基盤システムは、庁内ネットワーク等に関する利用者情報や権限等を管理するもの。

(1)　全体概要

総務事務システムと本システムを連携させ、以下を実現することにより、客観的で適正な勤務時間の把握と長時間労働の抑制を図る。

・本システムにおいて、ＰＣログオン・ログオフ時間を把握し、総務事務システムと連携の上、同システム上の出勤簿に当該時間を表示する。

・総務事務システムにおいて、職員ごとの勤務日・勤務時間・休暇情報・超過勤務命令時間等をもとに、ＰＣ稼働遮断時間を算出し、当該情報を本システムに連携させ、勤務時間等以外の時間帯に関しては、各職員のＰＣの稼働を遮断する。

※なお、ＰＣ利用職員の識別については、共通基盤システム等からＰＣ稼働遮断システムに職員番号等を連携させることにより行うことを想定している。

(2)　業務概要

本システムは、上記(1)を実現するために、ＰＣログオン・ログオフ時間の把握と勤務時間等終了時にＰＣの稼働を遮断するシステムである。具体的には以下のとおり動作するも

のとするが、詳細については「第３ 機能要件」及び「第４ 非機能要件」を参照のこと。

ア　ＰＣのログオン・ログオフ時間を把握

・各職員のＰＣのログオン・ログオフ時間を把握し、総務事務システムに連携

イ　勤務時間等以外のＰＣの利用について、次の動作で利用を制限

・総務事務システムよりＰＣ稼働遮断時間に関するデータを連携

・ＰＣのデスクトップに警告画面を表示し、利用を抑止

・職員の勤務時間等に応じ、所定の時間にＰＣの稼働を遮断

・稼働遮断後にＰＣを利用しようとする際には、警告画面を表示するとともに、一定時間内に稼働の遮断を解除する手続きがなければ再び稼働を遮断する

２　システム構成の考え方

サーバにインストールする側のシステムを、以下「ＰＣ稼働遮断システム管理ソフト」とし、ＰＣにインストールする側のシステムを、以下「ＰＣ稼働遮断システムエージェントソフト」とする。

(1)　ＰＣ稼働遮断システム管理ソフト

ア　各職員のＰＣのログオン・ログオフ時間を把握してデータを作成し、総務事務システムに自動でデータ連携すること。なお、データはＣＳＶ形式で所定のフォルダに格納すること。

イ　総務事務システム等から提供される各職員のＰＣ稼働遮断時間に関するデータを自動で連携させること（１日に３回程度を想定)。なお、データはＣＳＶ形式で所定のフォルダに格納するので、本システムにおいてその情報を取得し稼働すること。

ウ　本番環境をハードウェア統合基盤上に構築すること。

（別紙１「ハードウェア統合基盤における業務アプリケーションの適合要件」を参照）

(2)　ＰＣ稼働遮断システムエージェントソフト

ア　ＰＣ稼働遮断システム管理ソフトの情報を取得し、ＰＣの稼働を遮断させること。

イ　ＰＣ上に導入すること。

ウ　ＰＣ単位ではなく利用する職員単位で管理を行うこと。

３　業務の範囲

本業務は、本システムの設計・開発、導入等のシステム構築を行うものであり、その範囲は以下のとおり。なお、本システムが稼働するサーバ機器、0S 等については、仮想サーバ環境として県がハードウェア統合基盤にて提供するので、本業務には含まない。また、本システムの保守・運用や、本システムとの連携等により、別途必要となる総務事務システムの改修についても、本業務に含まない。

(1)　本システムの基本設計、詳細設計、開発、テスト及び導入

ア　設計には、運用設計を含む。

イ　ハードウェア統合基盤は、0S 等のソフトウェアのインストールを行った状態で提供するので、受託者はこれに構築するシステムを導入する。

(2)　ソフトウェアライセンスの取得

本システムの構築に際し必要となるソフトウェアのライセンスの取得。

(3)　ソフトウェアの調達範囲

本調達に含むソフトウェアの範囲は、下表の発注区分で「本調達範囲」と示すものとする。

ＰＣ稼働遮断システム管理ソフト

項番	ソフトウェア	発注区分	説明
1	0S	別紙１「ハードウェア統合基盤における業務アプリケーションの適合要件」参照	オペレーティングシステム
2	データベース	本調達範囲	データベースソフトウェア
3	ウイルス対策ソフトウェア	サーバ台数５台未満かつトレンドマイクロ社のウイルスバスターの場合のみ統合基盤で調達	コンピュータウイルスの検知、駆除
4	本システムのアプリケーション	本調達範囲	システム本体（プログラム実行環境を含む）
5	運用管理ソフトウェア	本調達範囲	運用管理に必要なもの
6	その他	本調達範囲	上記のほかに本システムの稼働に必要となるソフトウェアがある場合は、本調達の範囲とする

ＰＣ稼働遮断システムエージェントソフト

項番	ソフトウェア	発注区分	説明
1	ＯＳ	本調達 範囲外	オペレーティングシステム
2	本システムのアプリケーション	本調達範囲	システム本体 （プログラム実行環境を含む）

※なお、本システムの稼働（令和５年４月１日以降）に伴い、ライセンスなど、ソフトを使用するに当たり必要となる費用については、本調達範囲とする。ただし、当該ソフトの利用期間は、令和５年４月１日～令和９年９月３０日までとし、保守・運用経費については含まないものとする。

(4)　付帯作業

ア　稼働前の職員に対する操作研修に利用できる説明資料の提供

なお、内容は動画等による理解しやすいものとし、内容については県の承認を得ること。

イ　各種取扱説明書の作成

ウ　本業務において構築した本システムから次期システムへ移行する際のデータ抽出及び抽出したデータの説明資料の作成

４　スケジュール及び体制

(1)　スケジュール

本業務におけるスケジュールは、概ね以下のとおりである。本業務と並行して総務事務システムにおいても、改修を行う予定であるため、連携テスト等を行う際には、同システムの改修スケジュールにも留意すること。なお、同システム改修スケジュールについては、別途県より提供する。

また、本システムの稼動開始は令和５年４月１日以降とする。

	令和４年	令和５年		
	12 月	１月	２月	３月
プログラム開発	→	→		
単体テスト			→	
連携テスト			→	
運用テスト				→
運用準備				→

(2)　業務実施スケジュール計画書

受託者は、契約締結後、各工程の期間を明らかにした業務実施スケジュールを含む業務実施計画書を提出し、県の承認を得ること。

(3)　開発体制

ア　システムの高い品質を確保し、かつ全行程が遅滞なく進められるよう十分な体制をとること。

イ　システム構築における各工程の完了時には、県のレビューを受けて承認を得ること。

ウ　定量的な品質管理に努め、定期的（最低月１回以上）に進捗を報告すること。なお、報告の際に必要となる資料や議事録等については、全て受託者が作成し、県の承認を得ること。

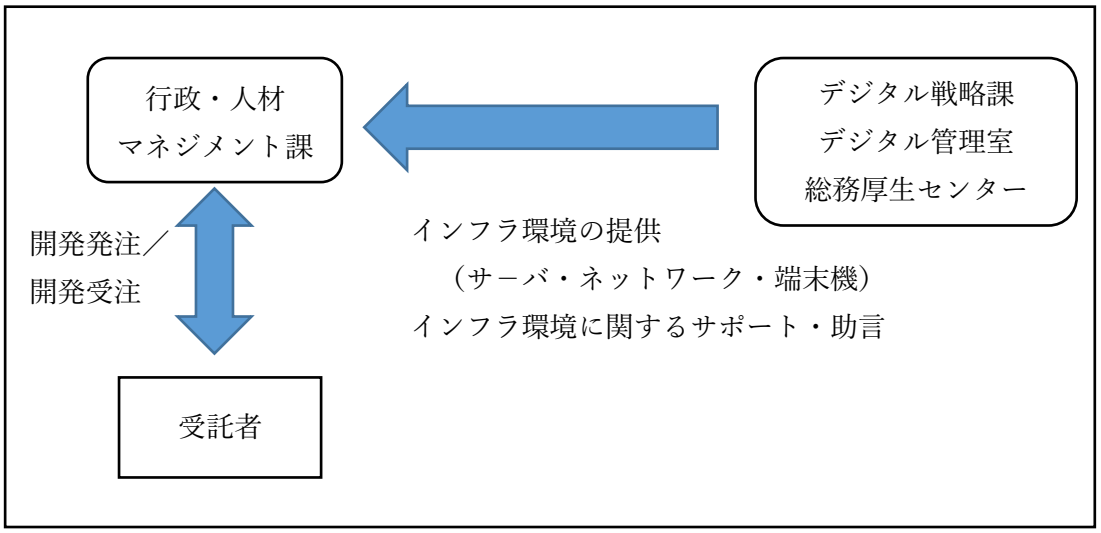
エ　単体テストまでの間、開発に必要な場所、機器及びソフトウェア等、本業務にかかる一切の経費は、受託者の負担とする。なお、単体テスト後の連携テスト等については、県が提供する機器等を使用して行うことができる。

オ　他のシステムやネットワークの停止を伴う作業は、閉庁日又は夜間での実施を前提とすること。

(4)　役割分担

受託者と県担当部署との関係及び各自の役割分担は以下のとおりとする。なお、別紙１「ハードウェア統合基盤における業務アプリケーションの適合要件」も確認すること。

【受託者と県担当部署との関係】



【役割分担】

凡例 ☆：承認、◎：作業主体、○：作業支援／参加、△：必要により支援

工程	大区分	小区分	受託者	行政・人材ﾏﾈｼﾞﾒﾝﾄ課	デジタル管理室	総務厚生センター
設計、開発						
	1 全体管理	庁内関係所属との調整		◎		
	2 要件定義・設計	要件定義、基本設計	◎	☆		○
		詳細設計	◎	☆		○
	3 システム構築	ハードウェア統合基盤関係		別紙１「ハードウェア統合基盤における業務アプリケーションの適合要件」参照		
		アプリケーション構築	◎			
		基本動作確認	◎	☆		△
	4 テスト	単体テスト	◎	☆		△
		連携テスト、運用テスト	◎	☆		○
	5 サーバセットアップ	サーバセットアップ（各種設定、データ投入等）	◎	△		
	6 クライアントセットアップ		◎	△	△	

5　成果品

成果品は、電子媒体２部、紙媒体２部を納品すること。ただし、プログラム一式の紙での納品は不要である。なお、各成果品の納品時期については、別途、県より指定するため、これに従うこと。

年度	成果品
令和４年度	業務実施計画書
	基本設計書
	インターフェース設計書
	詳細設計書
	運用設計書
	プログラム一式（ソフトウェア含む。）
	テスト計画書

	テスト結果報告書
	運用手順書
	受入テストのシナリオ及び報告書
	操作手引書（利用者用）
	操作手引書（システム管理者用）
	職員向け説明資料
	管理情報一覧（作成したユーザ・パスワード一覧、ホスト名、機器の設定値等）
	ライセンス関係資料（ライセンス証書、シリアルナンバー一覧表等）
	エージェントソフト導入手順書

第３　機能要件

１　システムの機能

本業務で構築する本システムの機能要件は以下のとおり。

No.	項　目		内容
1	全体要件		本システムが停止している場合でも、PC を通常どおり使用して業務を行うことができること。
2			共通基盤システム等から職員番号等を自動連携させることにより、PC 利用者の識別を行うこと。 ※なお、連携様式については、CSV 形式を想定している。
3			職員がPCにログオンした後、自動的に本システムエージェントソフトを起動し、下記基本要件の動作対象となる職員かどうか判断ができること。
4			PC 稼働遮断システムに係るソフトをインストールした PC において、対象職員であれば、どの職員がログオンしても、下記基本要件に記載の機能が動作すること。
5			管理者権限のある職員による PC 稼働遮断システムに係る機能制御の仕組みを有すること。
6	基本要件	勤務時間の記録	対象職員の PC ログオン・ログオフ時間を記録し、当該データを総務事務システムに自動で連携すること。 ※なお、全記録データのうち、連携を行うデータの設定については、県と協議のうえ、決定すること。
7			上記自動連携に関しては、1日につき任意の時間帯に3回程度行うこと。 ※なお、連携様式については、CSV 形式を想定している。
8		PC稼働の遮断	総務事務システムより、本システム対象職員に係る勤務予定情報等を自動連携し、当該情報に基づき、PCの稼働を以下のとおり制御すること。 ・勤務日 勤務終了時刻又は超過勤務命令時間等から一定時間経過後、PC の稼働を遮断する 勤務開始時刻より一定時間前までの時間帯はPCの稼働を遮断する ・週休日・休日 勤務命令のない又は勤務日に設定されていない週休日・休日は PC の稼働をログオン後一定時間経過後に遮断する ※なお、総務事務システムより受取を予定している各職員に係る勤務予定情報等（CSV 形式）は所定の場所に保存されるため、本システムの責任により、当該データを取り込み、稼働すること。当該情報は、職員の勤務日・勤務時間・休暇情報・超過勤務命令の有無等に基づき、総務事務システム側で算出された、PC の稼働遮断時間に係る情報である。
9			上記自動連携に関しては、1日につき任意の時間帯に3回程度行うこと。
10			PC 稼働遮断時間帯にログオンを行った場合には、一定時間経過後に再度 PC の稼働を遮断する機能を有すること。
11			PC の稼働遮断は、以下の段階を有すること。また、遮断方法については、管理者側で選択できる仕組みを有していること。 ・通知（職員ごとに設定された PC 利用可能時間が終了する旨等を PC の画面上に表示する） ・警告（PC の稼働を遮断する情報を PC の画面上に表示する） ・遮断（強制的に PC の電源を落とす、または、ログオフ状態にする）
12			緊急時など、職員の判断で PC 稼働遮断システムの稼働を解除できる仕組みを有していること。

			また、解除の際には、解除パスワードの使用や解除理由の記録を必要とするなど、安易な解除を防止する機能を備えていること。なお、解除パスワードは変更可能であること。
13	蓄積データ収集・分析機能		以下の情報を記録する機能を有すること。 ・職員特定情報（職員番号等）、ログオン・ログオフ時間 （要件6に該当） ・職員特定情報（職員番号等）、緊急時対応機能の使用日時等 （要件 12 に該当）
14			蓄積したデータは CSV 形式で出力できること。
15			蓄積したデータは、2年間程度閲覧できる状態にすること。ただし、データ保存の方法については、CSV 形式の情報を出力して所定のフォルダに保存する方法をとるなど、必ずしもサーバー内に留めておく必要はない。
16	管理機能		通知・警告画面の内容は、管理者により、任意に変更することができること。
17			通知・警告画面は、管理者により、表示のタイミングを設定できること。
18			管理者の権限により、本システムの対象職員を変更できる機能を有していること。
19			管理者の権限により、災害発生時など、任意の期間、本システムが機能しないように設定できること。
20			本システムが正常に稼働しない事象が生じた場合に、管理者がそれを認識できる機能を有していること。 （ただし、ハードウェア統合基盤上で障害が生じた場合を除く）

第４　非機能要件

１　システムの規模

(1)　対象職数・端末数

・職 員 数：一般職員約 5,000 人（教職員、県警を除く）

うち、特別職、管理職、短時間勤務職員等については、ＰＣのログオン・ログオフ時間による勤務時間の記録のみを行い、ＰＣ稼働遮断の対象外とすることを想定している。

・端末台数：共通端末 約 5,000 台

モバイルワーク用端末 約 100 台(ノートＰＣ型 70 台･タブレット型 30 台)

※本システムエージェントソフトのインストールは、上記の計 5,100 台程度に対して行う想定をしており、その方法に関しては県と協議のうえ、決定することとする。

※なお、本システムは、公示日時点の最新のバージョンにも対応させること。また、今後のＰＣの更新やソフトウェアのバージョンアップ等への対応が最小限となるよう設計すること。

※「共通端末」は、職員（教職員、県警除く）に配備されている事務用端末である。本県では現在、職員用端末として、平成 30 年度導入端末（以下、「K18 端末」という。）と令和３年度導入端末（以下、「K21 端末」という。）の２世代を利用している。

※「モバイルワーク用端末」は、「共通端末」とは別に、職員がモバイルワークを実施するために用意された事務用端末であり、ノートＰＣ型とタブレット型の２種類ある。

２　システム方式に関する要件

(1)　基本的な考え方

ア　構築する本システム管理ソフトは、Windows Server 2019 上で稼働すること。

イ　機能追加又は改修を加えることができるシステムとすること。

ウ　ＰＣの更新やＯＳ・ブラウザのバージョンアップへの対応が可能であること。

(2)　処理方式

ＰＣに特別な設定やプログラムのインストールを行う際は、インストールが自動実行できるなど、職員に過度の負担なく導入できるものとすること。この構築に係る費用は全て受託者が負い、実施にあたっては県の承認を得ること。

３　セキュリティ要件

(1)　本システムの利用に関し、不正侵入対策を講じること。

(2)　サービス、ポートは、必要なものに限定すること。

(3)　ソフトウェアは、契約期間中を通じて脆弱性に対するセキュリティ更新プログラムが提供されるものであること。

(4)　権限のない者による情報へのアクセスができないよう、アクセス権限を設定すること。
(5)　サーバへのアクセスログを取得すること。

４　バックアップ

県が提供するハードウェア統合基盤のバックアップ運用を踏まえ、適切にバックアップを行うこと。詳細については、別紙１「ハードウェア統合基盤における業務アプリケーションの適合要件」にて示す。

５　サーバ要件

本システム管理ソフトは県が設置したハードウェア統合基盤上に構築する仮想マシンにて稼動するものとする。受託者は、これに構築する本システムの導入を行うこと。なお、仮想マシンは、行政ネット接続系（LGWAN）に設置し、本番環境を構築することを想定しており、ネットワーク利用に関しては庁内ネットワーク機器に必要な設定を行うための調整が必要となる。

ハードウェア統合基盤の詳細は別紙１「ハードウェア統合基盤における業務アプリケーションの適合要件」にて示す。なお、具体的な論理サーバスペック等に関しては、システム構築時に県と協議を行うこと。

(1)　引渡し時のサーバ環境

仮想サーバは、県にて以下の作業を実施後、引き渡される。

ア　仮想サーバの作成
イ　Windows のインストール
ウ　最低限のネットワーク設定
　（IP アドレス・ゲートウェイ設定、コンピュータ名設定）
エ　ウイルス対策ソフトのインストール
　（ただし、トレンドマイクロ社製ウイルスバスター以外のソフトを希望する場合には、受託者にて調達のうえ、インストールすること）
オ　仮想ディスク全体のバックアップ設定

(2)　サーバ運用

ア　稼働時間

仮想サーバは原則、定期的な停止を行わない。ただし、機器のメンテナンス等のために、メンテナンス日を設けサーバを停止することがある。

イ　バックアップ

別紙１「ハードウェア統合基盤における業務アプリケーションの適合要件」に基づき、データの日次バックアップを行うこと。障害発生時には、統合基盤で取得する週次バックアップを併用してシステムを復旧する。

ウ　パッチ適用

県では、パッチの自動配布や自動適用の設定を行わない。また、パッチの適用も行わない。システムへの影響を確認の上、受託者にて必要なパッチを適用する運用とすること。また、構築時にも受託者にて、必要なパッチを適用すること。

エ　障害・問合せ対応

受託者にて仮想サーバ環境の問題かシステムアプリケーションの問題であるか切り分けること。切り分けの結果、仮想サーバ環境の問題である場合は、県と調整すること。

6　クライアント要件

職員は、県が職員に配備しているＰＣにて本システムエージェントソフトを使用する。

現在のＰＣの標準的な仕様は以下のとおり であるが、本システムは、公示日時点の最新バージョンにも対応させること。また、今後のＰＣの更新やＯＳ・ソフトウェアのバージョンアップ等への対応が最小限となるよう設計すること。

ア　共通端末（約 5,000 台）

項目	仕様	
端末番号	Ｋ１８	Ｋ２１
OS	Windows 10 Professional 64bit	Windows 10 Professional 64bit
CPU	Intel Core i3-6100U 2.30GHz	Intel Core i5-10210U 1.60GHz
メインメモリ	4GB	8GB
内蔵ディスク	SSD 128GB	SSD 128GB
ブラウザ	Microsoft Edge	
Office ソフト	Microsoft Office 2013(32bit) 一太郎 Pro4	Microsoft Office 2021(32bit) 一太郎 Pro4
ビューア	Adobe Acrobat Reader DC	
その他	ログイン時に顔認証ソフトウェアによる認証を実施している。	

イ　モバイルワーク用端末（約 100 台：ノートＰＣ型 70 台・タブレット型 30 台）

項目	仕様	
形態	ノートＰＣ型	タブレット型
OS	Windows 10 Pro	Windows 10 Pro
CPU	Intel Core i5-7200U	Intel Core M3-7Y30
メインメモリ	8GB	4GB
内蔵ディスク	SSD 128GB	SSD 128GB
ブラウザ	Microsoft Edge	
Office ソフト	Microsoft Office Pro 2016 一太郎 Pro4	
ビューア	Adobe Acrobat Reader DC	

７　テスト要件

(1)　テスト内容

テストは、総務事務システム等との連携を含め、本システムの各機能が正常稼働することを検証すること。

(2)　テスト計画、実施及び報告

テスト実施に当たっては、事前に計画書を提出し、県の承認を得たうえで、関係者との調整も含め実施し、その結果をテスト報告書として取りまとめること。

特に、本業務には既存システムとの連携が含まれており、本システムの導入と並行して総務事務システムの改修作業が実施される予定であることから、当該改修作業の進捗状況や連携テスト後のシステム修正等を考慮し、計画を作成すること。

８　手引書の作成

以下の手引書を作成すること。

(1)　導入手順書

(2)　操作手引書（利用者用）

(3)　操作手引書（システム管理者用）

(4)　運用手順書

システム管理者が、運用に関する操作が可能となるよう運用手順を記載したもの。

(5)　職員向け説明資料

９　クライアントセットアップ及びクライアント再セットアップ

ＰＣへのエージェントソフトのインストールについては、SKYSEA Client View を用いた配信によるインストールを想定しているが、詳細については県と協議のうえ行うこととする。また、インストール失敗の際の対応なども記載した、詳細なエージェントソフト導入手順書を作成すること。

１０　履行場所

本業務において、本番環境と同環境で実施する必要のある業務を履行するにあたっては、県本庁舎で行うこと。これら以外の業務を履行するにあたっては、奈良県と協議のうえ、受託者が開発業務履行場所を確保すること。

１１　関係法令等の遵守

(1)　受託者は、奈良県個人情報保護条例、奈良県暴力団排除条例、奈良県公契約条例、奈良県情報セキュリティポリシー並びにその他関係法令等を遵守し、適法かつ適切に業務を遂行すること。

(2)　特に別紙２～５については、遵守すること。

１２　留意事項

(1)　受託者は、運用開始までの作業スケジュールを県と協議し、決定すること。

(2)　受託者は、業務の一部を第三者に委託し、又は請け負わせようとする場合は、あらかじめ書面により委託者の承諾を得なければならない。また、承認を受けた内容を変更しようとする場合についても同様に委託者の承諾を得なければならない。

(3)　この場合において、受託者は第三者の行為について委託者に対して全ての責任を負うものとする。

(4)　また、委託業務において受託者が作成する情報については、担当者からの指示に応じて適切に取り扱うこと。

(5)　契約に不適合があった場合、受託者は正当な理由がある場合を除き、速やかに本県の指示に従い、成果物の修補、代替物の引渡し又は不足分の引渡しによる履行の追完を行うこと。ただし、受託者が契約不適合に該当しないと判断する場合は、早急に協議を行い、対応を決定する。本仕様書に明記されていない細部の事項については、発注者と協議すること。

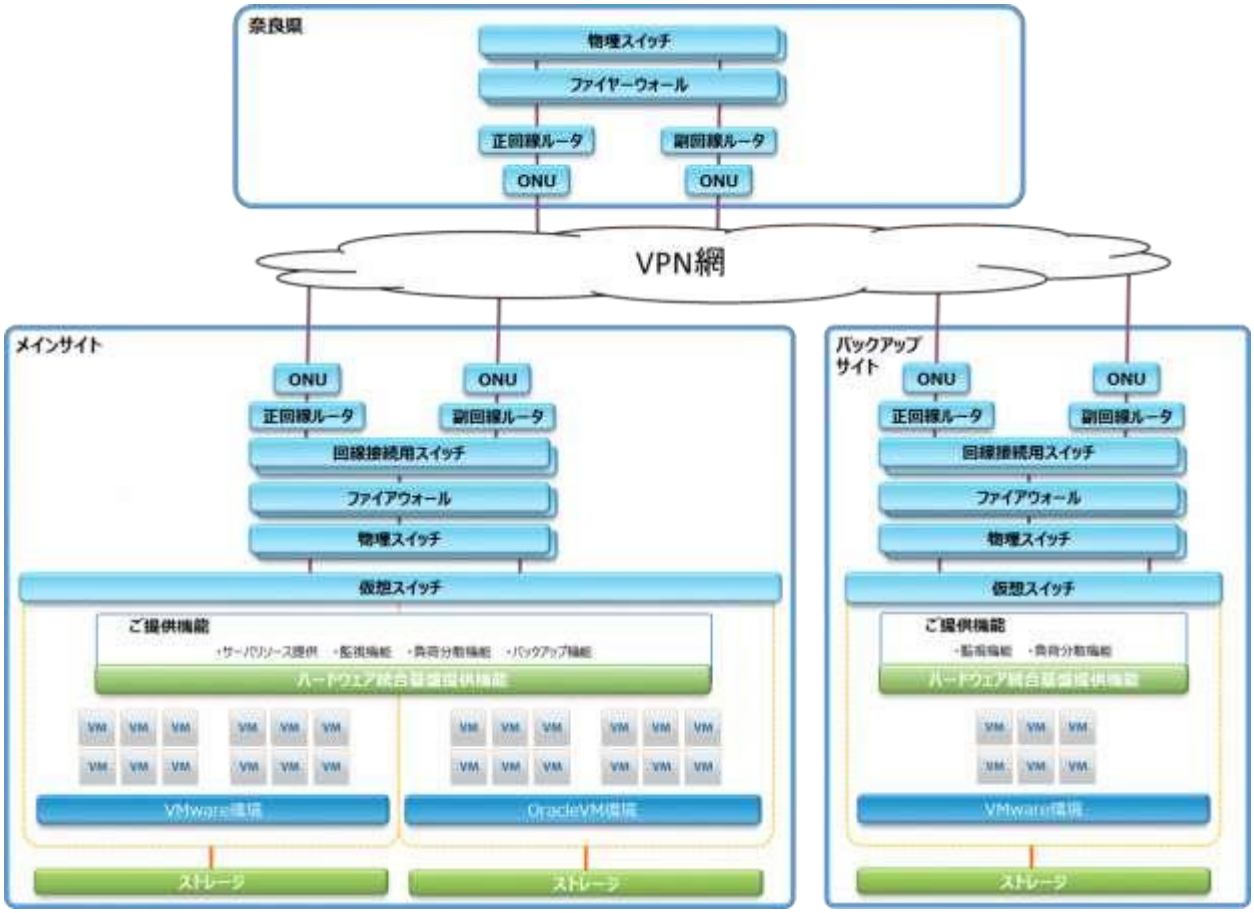
(6)　本仕様書に定めのない事項が発生した場合及び疑義が生じた場合は、県と協議のうえ定めるものとする。

ハードウェア統合基盤における業務アプリケーションの適合要件

1. ハードウェア統合基盤

ハードウェア統合基盤に業務システムサーバを仮想構築するにあたり、ハードウェア統合基盤における前提条件は以下のとおりとする。

(1) 構成



(2) ハイパーバイザの種類

VMware vSphere ESXi6.5 以上

ただし Oracle VM が利用できないため、Oracle 社製品は利用不可

(3) 仮想サーバの冗長性

HA（High Availability）機能により冗長化を実施

(4) 仮想サーバ用 OS について

OS 種別により、ハードウェア統合基盤にて提供するものと、業務システムベンダにて用意するものがある。

表１．ライセンスについて

	内容
Windows Server	ハードウェア統合基盤にて提供※1
Red Hat Enterprise Linux	ハードウェア統合基盤にて提供
その他 OS	業務システムベンダにて用意

※1 クラウド環境の WindowsServer に対するクライアントアクセスライセンス(CAL)も提供する。

(5) ロードバランサー (VMware NSX Edge)

ハードウェア統合基盤が備える機能を使用可能とする。

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

2.システム構築及び運用について

(1) システム構築方法

①Windows Server、Red Hat Enterprise Linux についてはハードウェア統合基盤構築ベンダが仮想サーバのリソースの払い出しを実施する。

②業務システムベンダは、上記以外の構築作業を実施すること。

(2)リモートメンテナンス

①奈良県庁からの接続

サーバルームに設置のハードウェア統合基盤接続用端末を使用して、仮想サーバの保守運用を実施する。

(3) 仮想サーバの保守運用

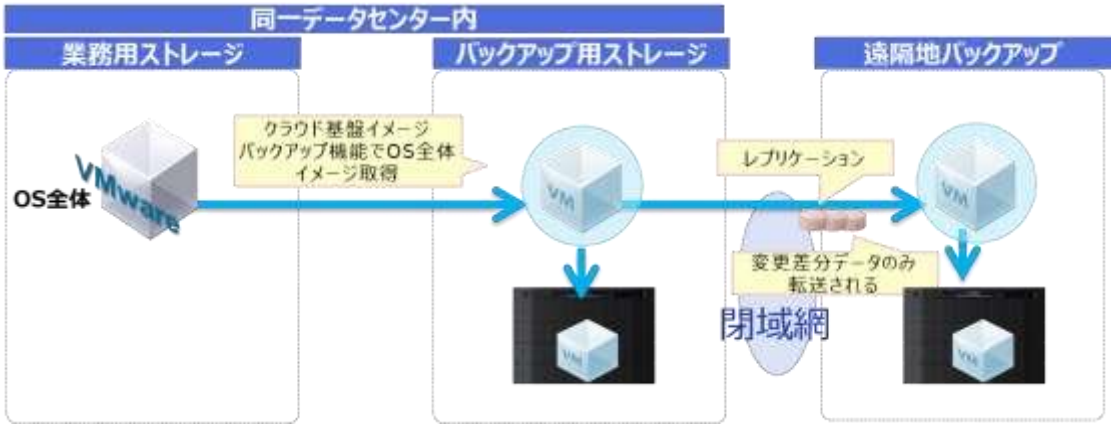
仮想サーバ OS とアプリケーションのパッチの適用は、業務システムベンダが行うこと。

(4) OS イメージのバックアップ／リストア方法

①OS イメージのバックアップについては、ハードウェア統合基盤構築ベンダが、週次でバックアップを実施する。

②OS イメージのリストアについては、ハードウェア統合基盤構築ベンダが、奈良県からの依頼を受け実施する。

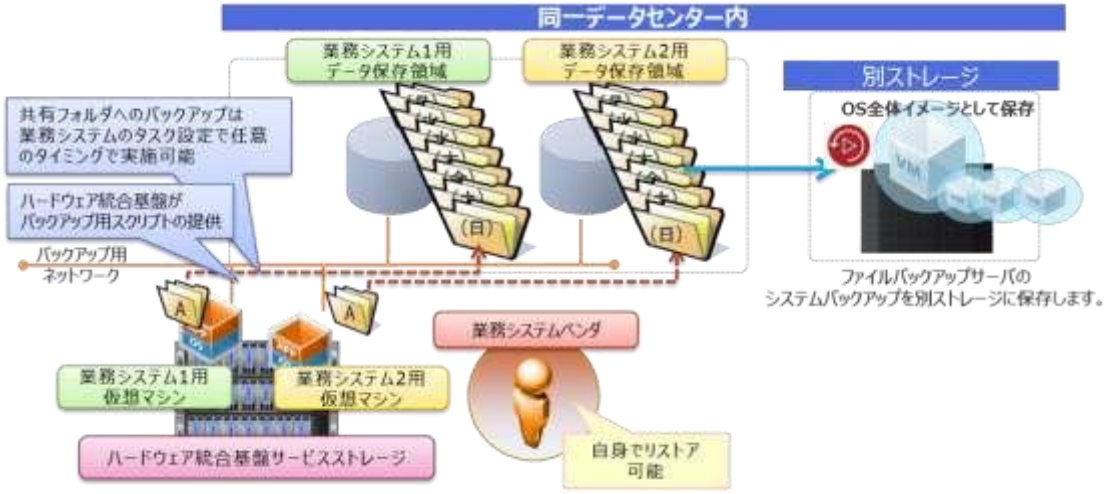
概要図(VMware 環境)



(5) データファイル及びフォルダのバックアップ／リストア方法

①データファイル及びフォルダのバックアップが必要な場合は、業務システムベンダが OS 標準コマンドを使用して、ハードウェア統合基盤が用意したバックアップサーバへバックアップを実施すること。

②データファイル及びフォルダのリストアについても、業務システムベンダにて実施すること（依頼があればハードウェア統合基盤構築ベンダでもリストア対応可能)。



(6) ジョブ管理

ジョブ管理用ソフトウェアが必要な場合は、業務システムベンダが用意すること。

(7) システム監視の方法ハードウェア統合基盤構築ベンダが、仮想サーバの死活監視、リソース（CPU、メモリ、ディスク等）監視、サービス（データベースソフトウェア等）監視を SNMP により実施する。

一部、イベントログなどの監視を行う場合は、エージェントをインストールすることで対応可能

なお、障害が発生した際は、ハードウェア統合基盤構築ベンダが業務システムベンダに対し、障害内容の通報を行う。

3.障害発生時の運用について

(1) 障害発生時の運用（リストア）について

①ファイルバックアップからのリストア

データのリカバリが必要になった場合は、ファイルバックアップ領域から業務システムベンダが任意のタイミングでデータのリストアを実施する。

②イメージバックアップからのリストア

イメージバックアップからのリカバリが必要になった場合は、ハードウェア統合基盤にてリストアを実施する。

以上

別紙２（奈良県個人情報保護条例関係）

１　業務を受託した場合には、下記「個人情報取扱特記事項」を遵守すること。

２　委託を受けた個人情報の取扱いを伴う事務に従事している者又は従事していた者は、奈良県個人情報保護条例第 64 条又は第 65 条の罰則の対象となることに留意すること。

●個人情報取扱特記事項

（基本的事項）

第１　乙は、個人情報の保護の重要性を認識し、この契約による事務の実施に当たっては、個人の権利利益を侵害することのないように、個人情報を適正に取り扱わなければならない。

（秘密の保持）

第２　乙は、この契約による事務に関して知り得た個人情報を他に漏らしてはならない。この契約が終了し、又は解除された後においても、また同様とする。

（収集の制限）

第３　乙は、この契約による事務を行うために個人情報を収集するときは、当該事務の目的を達成するために必要な範囲内で、適法かつ公正な手段により行わなければならない。

（目的外利用・提供の禁止）

第４　乙は、甲の指示がある場合を除き、この契約による事務に関して知り得た個人情報を契約の目的以外の目的に利用し、又は甲の承諾なしに第三者に提供してはならない。

（漏えい、滅失及びき損の防止）

第５　乙は、この契約による事務に関して知り得た個人情報の漏えい、滅失及びき損の防止その他の個人情報の適切な管理のために必要な措置を講じなければならない。

（従事者の監督）

第６ 乙は、この契約による事務を処理するために取り扱う個人情報の適切な管理が図られるように、従事者に対して必要かつ適切な監督を行わなければならない。

２　乙は、この契約による事務に従事している者に対し、在職中及び退職後においても当該契　約による事務に関して知り得た個人情報を他人に知らせ、又は不当な目的に使用してはならないこと、個人情報の違法な利用及び提供に対して罰則が適用される可能性があることその他個人情報の保護に関して必要な事項を周知しなければならない。

（複写又は複製の禁止）

第７　乙は、この契約による事務を処理するために甲から引き渡された個人情報が記録された資料等を甲の承諾なしに複写し、又は複製してはならない。

（再委託の禁止）

第８　乙は、甲が承諾した場合を除き、この契約による事務について第三者にその取扱いを委託してはならない。なお、再委託を受ける者は、情報セキュリティマネジメントシステム ISO/IEC27001、ISMS 認証もしくはＰマーク（プライバシーマーク）を取得していることを条件とし、認証を受けていることを証する書類として、再委託日時点で有効な登録証の写しを甲に提出すること。

（資料等の返還等）

第９　乙は、この契約による事務を処理するために、甲から提供を受け、又は乙自らが収集し、若しくは作成した個人情報が記録された資料等を、この契約の完了後、直ちに、甲に返還し、又は引き渡すものとする。ただし、甲が別に指示したときは、当該指示に従うものとする。

（取扱状況についての指示等）

第 10　甲は、必要があると認めるときは、随時、個人情報の取扱状況について、乙に対して、必要な指示を行い、若しくは報告若しくは資料の提出を求め、又は調査をすることができる。この場合において、乙は、拒んではならない。

（事故発生時における報告）

第 11　乙は、この契約に違反する事態が生じ、又は生ずるおそれのあることを知ったときは、速やかに、甲に報告し、甲の指示に従うものとする。

（損害賠償等）

第 12　乙は、その責めに帰すべき事由により、この契約による事務の処理に関し、甲又は第三者に損害を与えたときは、その損害を賠償しなければならない。再委託先の責めに帰すべき事由により、甲又は第三者に損害を与えたときも、また同様とする。

２　甲は、乙がこの個人情報取扱特記事項の内容に反していると認めるときは、契約の解除又は損害賠償の請求をすることができるものとする。

注　「甲」は「実施機関」を、「乙」は「受託者」をいう。

別紙３（奈良県暴力団排除条例関係）

1　受注予定者が契約の締結までに下記要件のいずれかに該当すると認められるときは、落札者と契約を締結しないものとする。
2　契約締結後、契約の相手方が下記要件のいずれかに該当すると認められるときは、契約を解除することがあり、その場合は損害賠償義務が生じることに留意すること。

●要件

(1)　役員等が暴力団員であるとき。
(2)　暴力団又は暴力団員が経営に実質的に関与しているとき。
(3)　役員等がその属する法人等、自己若しくは第三者の不正な利益を図る目的で又は第三者に損害を与える目的で、暴力団又は暴力団員を利用しているとき。
(4) 役員等が、暴力団又は暴力団員に対して資金等を提供し、又は便宜を供与する等直接的若しくは積極的に暴力団の維持及び運営に協力し、又は関与しているとき。
(5)　上記(3)及び(4)に掲げる場合のほか、役員等が暴力団又は暴力団員と社会的に非難されるべき関係を有しているとき。
(6)　県が発注する物品購入等の契約に係る下請契約又は資材、原材料の購入契約等の契約（以下「下請契約等」という。）に当たり、その相手方が上記(1)から(5)までのいずれかに該当することを知りながら、当該者と契約を締結したとき。
(7)　下請契約等に当たり、上記(1)から(5)までのいずれかに該当する者をその相手方としていた場合（上記(6)に該当する場合を除く。）において、契約担当者が契約の相手方に対して当該下請契約等の解除を求め、契約の相手方がこれに従わなかったとき。
(8)　県が発注する物品購入等の契約を履行するに当たり、暴力団又は暴力団員から不当介入を受けたにもかかわらず、遅滞なくその旨を契約担当者に報告せず、又は警察に届け出なかったとき。

別紙４（奈良県公契約条例関係）

公契約条例に関する遵守事項（特定公契約以外用）

本業務を受注しようとする者は、この遵守事項を理解した上で受注すること。

1　奈良県公契約条例の趣旨にのっとり、公契約の当事者としての社会的責任を自覚し、本業務を適正に履行すること。

2　本業務の履行に当たり、次に掲げる事項その他の法令を遵守すること。

ア　最低賃金法第４条第１項に規定する最低賃金の適用を受ける労働者に対し、同法第３条に規定する最低賃金額（同法第７条の規定の適用を受ける労働者については、同条の規定により減額して適用される額をいう。）以上の賃金（労働基準法第 11 条に規定する賃金をいう。）の支払を行うこと。

イ　健康保険法第 48 条の規定による被保険者（同法第３条第４項に規定する任意継続被保険者を除く。）の資格の取得に係る届出を行うこと。

ウ　厚生年金保険法第 27 条の規定による被保険者（同条に規定する 70 歳以上の使用される者を含む。）の資格の取得に係る届出を行うこと。

エ　雇用保険法第４条第１項に規定する被保険者について、同法第７条の規定による届出を行うこと。

オ　労働保険の保険料の徴収等に関する法律第４条の２第１項の規定による届出を行うこと。

3　本業務の一部を、他の者に請け負わせ、若しくは委託し、又は本業務の履行に他の者が雇用する労働者の派遣を受けようとするときは、当該他の者に対し、この遵守事項を周知し、遵守するよう指導すること。

別紙５（情報セキュリティ関係）

情報セキュリティに係る特記事項

本業務委託の履行にあたり、奈良県情報セキュリティポリシーを遵守すること。特に下記の事項については留意すること

記

（認定・認証制度の適用）
第１　個人情報等を取り扱う場合、ISO/IEC27001、ISMS 認証またはプライバシーマーク等の第三者認証を取得していることを明示すること

（情報へのアクセス範囲等）
第２　取り扱う情報の種類、範囲及びアクセス方法を明確にすること（どの情報をどこに保存しているか、誰がどのようにアクセスできるのか明示すること）

（再委託先の情報セキュリティ）
第３　再委託する場合は、元請けと同等以上の情報セキュリティ対策が確保されていること（再委託先が ISO/IEC27001、ISMS 認証またはプライバシーマーク等の第三者認証を取得していること）を書面にて明示すること

（情報セキュリティ事故発生時の対応）
第４　情報セキュリティ事故またはそのおそれを覚知した場合は、直ちに発注者側担当者に連絡するとともに、発注者と連携して迅速な対応を行うこと

（電子メール利用時の遵守事項）
第５　インターネットメール送信時には、送信先メールアドレスに間違いがないか十分に確認すること。また、外部の複数の宛先にメールを送信する場合は、ＢＣＣで送信すること

（郵便等利用時の遵守事項）
第６　郵便やファックスを送信する場合は、送り先や内容に間違いがないよう複数人で確認すること

（コンピュータウイルス等の不正プログラム対策）
第７　奈良県の情報を取り扱うサーバーや端末等にはウイルス対策ソフトを導入するとともに、不正アクセスがないか監視すること

２　奈良県の情報を取り扱うサーバーや端末等で使用する OS やソフトウエアは、常に最新の状態に保つこと

（情報の持ち出し管理）
第８　仕様書等で定める場合を除き、奈良県の情報を外部記録媒体等で持ち出しすることを禁止すること

（契約満了時のデータ消去）
第９　契約満了後、特記ある場合を除き、委託先端末等に保存されている個人情報等は完全に消去の上、消去証明書を提出すること

（準拠法・裁判管轄）
第 10　データセンターを利用する場合、データセンターが国内の法令及び裁判管轄が適用される場所にあること

（契約満了時のアカウント削除）
第 11　クラウドサービス等でその利用を終了する場合、アカウントが正式に削除・返却されたことを明示すること