令和９（2027）年度

共同利用型基盤の更改に係る

設計･開発及び運用･保守業務一式

別紙１　要件定義書

令和８（2026）年３月

栃木県経営管理部行政改革 ICT 推進課

1. 業務要件定義

1.1. 業務概要

(1) 業務概要

【共同利用型基盤の設立目的】

栃木県（以下「本県」という。）においては、県全体のインフラコストの最適化や業務システム導入に係る時間の短縮化を目的として、"共同利用型基盤"を平成 28（2016）年より設置・運用してきている。

【共同利用型基盤の概要】

本県は、県全体のインフラコストの最適化や業務システム導入に係る時間の短縮化を目的として、"共同利用型基盤"を平成 28（2016）年から設置・運用している。

令和 8（2026）年 3 月時点で、第２期共同利用型基盤（以下「第２期基盤」という。）が稼働しており、約 65 の業務システムが第２期基盤を利用している状況である。第２期基盤の機器リース期間満了が令和 9（2027）年 10 月末のため、令和 9（2027）年 11 月以降に第 3 期共同利用型基盤（以下「本基盤」という。）への切り替えを予定している。

本基盤は、中長期的な視点で見た際の「業務効率化・県民サービス向上」を目的として、パブリッククラウド（以下単に「クラウド」という。）環境に構築する方針としたが、第２期基盤上の各業務システムが希望するタイミングに合わせた段階的なクラウドリフトが出来るように、本基盤をハイブリッド（第２期基盤同様のオンプレミス環境＋クラウド環境（AWS））構成とすることとし、令和 14（2032）年 10 月までに全ての業務システムをクラウド環境に移行すること（フルクラウド化）を目指すこととした。

【共同利用型基盤業務の概要】

本基盤の更改と同時にクラウドリフト可能な第２期基盤上の業務システムについては、本基盤構築時にクラウド上の仮想マシンを移行する業務を実施する。

また、本基盤の運用期間では、第２期基盤と同様に、当該基盤を管理する栃木県共同利用型基盤管理者（以下「基盤管理者」という。）が各業務システム主管課からの基盤利用申請を踏まえ、仮想マシン等のインフラリソース提供・変更・撤去に係る業務実施を予定している。

なお、本基盤のオンプレミス環境に業務システムの新規利用受入れを行うことは想定していない。基盤のフルクラウド化に向け、新規利用受入れについては、クラウドでのインフラリソース提供を実施する。

1.2. 業務内容

(1) 業務内容

基盤管理者は、業務として栃木県共同利用型基盤利用者（以下「基盤利用者」という。）に対して以下のインフラ機能の提供・変更・撤去を実施すること。なお、本基盤において新規で払い出すインフラ機能は原則としてクラウドサービス提供事業者が提供するマネージドサービスで実装すること。また、"基盤新規利用の業務システム"や"オンプレミス基盤からクラウド移行する業務システム"に対し、技術的なインフラ設計支援及び移行支援を業務として実施する。

一部業務の実施に当たっては、業務システム担当職員及び業務システム構築・運用事業者からシステム固有要件が示された場合には、基盤管理者と業務システム担当職員及び業務システム構築・運用事業者の双方協議の上で取り込みについて検討する。

表 1-1 基盤管理者が基盤利用者に提供する主なインフラ機能

項番	提供する機能	概要	補足
1	仮想マシン	業務システム向けに IaaS ベースの仮想マシンインスタンス及びブロックストレージを払出し、提供	基盤利用者は、OS 内の詳細セットアップ・アプリインストールを実施
2	ネットワーク及びファイアウォール	業務システム向けに、ネットワークセグメントと仮想マシン向けファイアウォール等を提供	基盤利用者は、業務通信等の要件を基盤管理者へ申請
3	ロードバランサ	業務システム（冗長構成の仮想マシン）向けに、http ベース又は tcp/ip ベースのロードバランサを提供	
4	ウイルス対策	項番 1 で払出した仮想マシン向けに、マシン内のウイルス対策処理及びパターンファイル等最新化機能を提供	ウイルス対策の除外設定が必要な場合は基盤利用者側から申し出
5	バックアップ・リストア	基盤管理者から払出された仮想マシンインスタンス及びデータベースインスタンスに対し日次バックアップ（スナップショット）及びリストア機能を提供	左記以外の個別バックアップ要件がある場合は、基盤利用者が個別でデータバックアップ機能を実装
6	共有ストレージ	業務システムのデータ保管等を目的とし、オブジェクトストレージを提供	
7	データベース	オンプレミス環境の IaaS 仮想マシン向けに Oracle ライセンスを提供、また、クラウド環境向けに PaaS のデータベースインスタンスを提供	PaaS の場合も、データベース内設計は基盤利用者側で実施
8	各種監視	業務システムに対する各種監視機能を提供 ※死活監視、性能監視、サービス監視、ログ監視等	
9	サーバ OS パッチ適用	業務システム IaaS 仮想マシン（Windows）向けに、OS パッチのオンライン適用機能（WSUS サーバ）を提供	

1.3. 業務の規模

本基盤で実現する業務で想定される規模について、以下に示す。なお、以下の内容については、過去の業務実績等に基づく値ではなく、本調達時点の想定に基づく値である点に留意すること。

(1) 基盤利用者数

本基盤の運用開始年度における想定基盤利用者数を下表に示す。

表 1-2 本基盤の運用開始年度における基盤利用者数（想定）

項番	基盤利用者	主な利用拠点	利用時間帯	人数	補足
1	業務システム担当職員	栃木県庁	8:30～ 17:15	およそ 200 人	本基盤上に構築された、業務システムの担当職員（業務システム主管課長を含む）
2	本県職員	栃木県庁	8:30～ 17:15	およそ 5000 人	本基盤上に構築された業務システムの利用による、間接的な基盤利用を想定。
3	業務システム構築・運用事	栃木県庁	8:30～	およそ	業務システムの構築・運用を実施。

項番	基盤利用者	主な利用拠点	利用時間帯	人数	補足
	業者	事業者拠点	17:15	200 人	事業者拠点からの利用は、リモート保守要件を満たした場合に限る。

(2) 本基盤の管理者数

本基盤の管理者数を下表に示す。

表 1-3 本基盤の管理者数（想定）

項番	管理者	主な利用拠点	人数	補足
1	基盤管理者	栃木県庁	およそ 10 人	基盤担当職員、基盤設計・開発業務受託者、基盤運用・保守業務受託者を指す。ただし、人数に基盤設計・開発業務受託者は含んでいない

1.4. 業務実施の時期・時間

(1) 業務実施時期・期間及び繁忙期

本基盤の運用に係る業務の通常期と繁忙期を下表に示す。

表 1-4 業務の通常期、繁忙期

項番	実施時期・期間	
1	通常期	下記以外
2	繁忙期	7 月、12 月

(2) 業務の実施・提供時間

本基盤については、基盤担当職員の責任のもとで基盤運用・保守業務受託者が運用作業を実施すること。なお、本基盤のサービス提供時間、システム障害時の対応、問い合わせ対応については以下のとおりとする。

ア サービス提供時間

本基盤は計画停止を除き、24 時間 365 日において、仮想マシン稼働及び各種基盤機能（マネージドサービス）の提供ができること。また、本基盤における各種インフラ機能（仮想リソース）の払出業務等は、開庁日（※1）の 8:30～17:15 のみ業務実施時間とする。ただし、予め日時調整を行い実施する作業については、この限りでない。

イ システム障害時の対応

システム障害の発生時は、復旧を最優先して迅速に対応すること。障害の原因究明・恒久的対策は、システム復旧後、翌開庁日の運用時間内にシステム保守として実施すること。

また、システム側の障害の原因究明・恒久的対策についても協力し、結果を基盤担当職員に報告すること。

ウ 問い合わせ対応

本基盤の業務（環境払出/変更/削除を含む）に関する問い合わせ対応の受付時間等及びクラウドサービスに関する問い合わせ対応の受付時間等を下表に示す。

表 1-5 本基盤の業務に関する問い合わせ対応の受付時間等

項番	問い合わせ方法	受付時間	対応時間	補足

1	電話	開庁日 8:30~17:15	開庁日 8:30~17:15	
2	電子メール等コミュニケーションツール	24 時間 365 日	同上	

表 1-6 クラウドサービスに関する問い合わせ対応の受付時間等

項番	問い合わせ方法	受付時間	対応時間	補足
1	電子メール等コミュニケーションツール	24 時間 365 日	開庁日 8:30~17:15	

※1 開庁日は、「栃木県の休日に関する条例」第 2 条に準じるものとする。
（1） 日曜日及び土曜日
（2） 国民の祝日に関する法律（昭和 23 年法律第 178 号）に規定する休日
（3） 12 月 29 日から翌年の 1 月 3 日までの日（前号に掲げる日を除く。）

1.5. **業務の実施等**

(1) 業務の実施等

本基盤の業務の実施場所に関する要件について、以下に示す。

なお、業務実施に当たっては、「栃木県情報セキュリティポリシー」等本県の情報セキュリティに関する規程等を満たし、かつ本県が認めた場合に限り、遠隔地での設計・開発業務及び運用・保守業務の実施を認める。遠隔地としては、基盤設計・開発業務受託者の拠点及びリモート監視サービス提供拠点を想定している。

表 1-7 基盤設計・開発業務受託者の業務の実施場所

項番	場所名	実施体制	実施業務	所在地
1	栃木県庁本庁舎	基盤設計・開発業務受託者 基盤運用・保守業務受託者	以下機能を提供する。 ・仮想マシン ・ネットワーク及びファイアウォール ・ロードバランサ ・ウイルス対策 ・バックアップ・リストア ・共有ストレージ ・データベース ・各種監視 ・サーバ OS パッチ適用	栃木県宇都宮市塙田 1-1-20

1.6. **サービスレベル目標**

(1) サービスレベル目標

本基盤のサービスレベル目標（SLO）を下表に示す。また、運用期間における本基盤のサービス仕様及び利用動向を踏まえ、必要に応じて更に SLO を追加又は変更する場合がある。

表 1-8 サービスレベル目標（SLO）

項番	指標の種類	指標名	計算式	単位	目標値	計測方法	計測周期
1	信頼性（可用性）	共通機能の稼働率	年間実稼働時間／年間予定稼働時間 x 100 なお、当該計算式において、年間実稼働時間は	%	99.5%以上	本基盤の監視機能等から取得する。	年次 （月次で途中過程を報告）

項番	指標の種類	指標名	計算式	単位	目標値	計測方法	計測周期
			「基盤利用者が本基盤を利用可能な時間の合計」、年間予定稼働時間は「年間稼働時間（24 時間 365 日）から計画停止時間及び大規模災害による停止・縮退時間を除いた時間の合計」とする。				

1.7. 情報システム化の範囲

(1) 情報システム化の範囲

本調達の範囲は、下図の赤枠部分に示す範囲である。

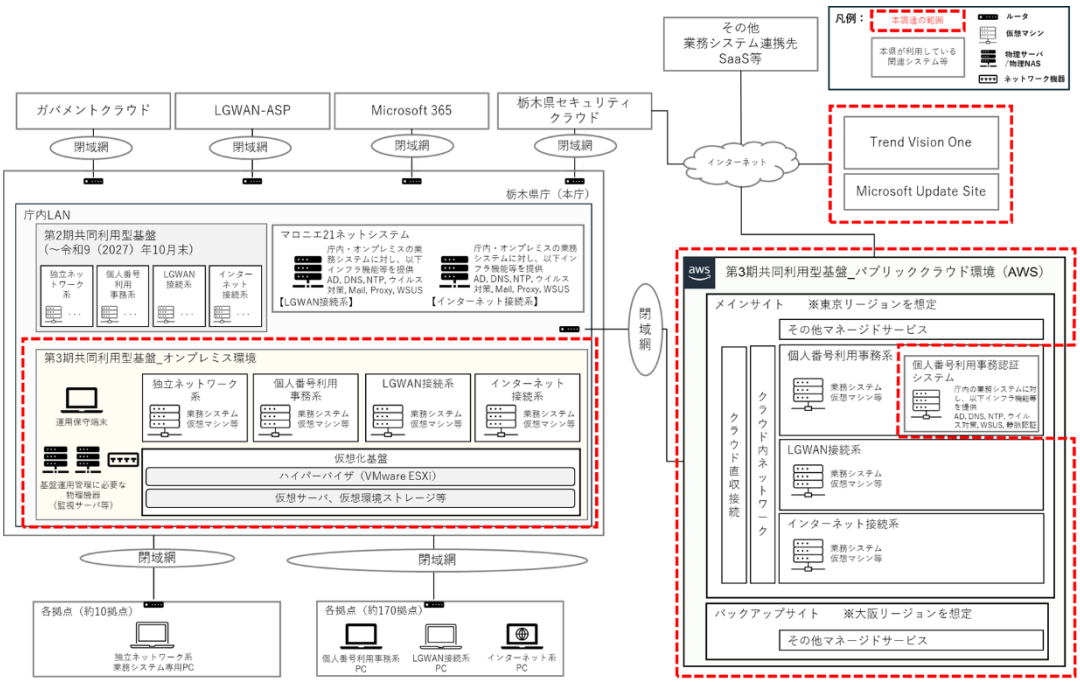

図 1-1 システム全体構成図

1.8. 業務の継続の方針等

(1) 業務の継続の方針等

本基盤の継続に関しては「3.9 継続性に関する事項」に記載する対策を講じること。

1.9. 情報セキュリティ対策の方針等

本基盤の情報セキュリティ対策に係る具体的な要件は、「3.10 情報セキュリティに関する事項」を参照すること。

(1) 情報セキュリティ対策の基本的な考え方

本県では、地方公共団体における情報セキュリティポリシーに関するガイドライン（以下「総務省ガイドライン」という。）に記載の自治体機密性分類をもとに、本県独自の機密性分類を設定している。

本基盤上では、総務省ガイドラインにおける自治体機密性 1 から 3B までに該当する情報を取り扱う業務システムが稼働することを前提とした情報セキュリティ対策（適切なクラウドサービスの選定を含む。）を講じること。

表 1-9 総務省ガイドラインにおける機密性の分類、分類基準の例示

分類	分類基準	情報資産	クラウドサービス（※1）の範囲
自治体機密性3A	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成 23 年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書	＜例＞ ・「行政文書の管理に関するガイドライン」上の極秘文書、秘文書に相当する文書（統一基準における機密性３情報に相当する情報） ・極秘文書：秘密保全の必要が高く、その漏えいが国の安全、利益に損害を与えるおそれのある情報を含む行政文書 秘文書：極秘文書に次ぐ程度の秘密であって、関係者以外には知らせてはならない情報を含む極秘文書以外の行政文書	「行政文書の管理に関するガイドライン」、統一基準の規定に則って取り扱うものとする（なお、上記ガイドラインにおいては、極秘文書について、インターネットに接続していない電子計算機又は媒体等に保存することが求められている（※2））
自治体機密性3B	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	＜例＞ ・データベースや台帳形式になった住民情報を含む個人情報ファイル及びこれに準ずる情報 （住民記録システム、税務システム、国民健康保険システム、生活保護システム、農業委員会台帳システム、貸付金償還システム等に保存される住民の個人情報）	ISMAP 登録サービスは利用可（8.3 で規定されるアクセス制御、機密性保護のための暗号化等が必要） ※統一基準改定に合わせて、8.3 でクラウドサービスの利用について規定
自治体機密性3C	行政事務で取り扱う情報資産のうち、自治体機密性３B 以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	＜例＞ ・職員としての属性に基づく個人情報 ・オンライン申請の処理等により、システム処理上一時的にインターネット上に保管されるデータ ・文書管理システムの決裁文書として保存されている個人情報 ・施設設計情報や入札予定価格など非公開情報	
自治体機密性2	行政事務で取り扱う情報資産のうち、自治体機密性３に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	＜例＞ ・政策検討に関する情報	可 （8.3 で規定されるアクセス制御、機密性保護のための暗号化等が必要）
自治体機密性1	自治体機密性２又は機密性３の情報資産以外の情報資産	＜例＞ ・将来公表する予定の文書（白書の案等） ・公表された情報	可

注）自治体機密性３C 情報については、情報資産単位でのアクセス制御、業務システムログ管理の実施等、β'モデルにおいてインターネット接続系に求められている対策を実施することで、インターネット接続系における取扱いが可能。

※１ クラウド事業者が提供するサーバやネットワークなどのインフラを、仮想化技術により複数のユーザで共用し、個々のユーザが、システムの運用体系を完全に制御することが難しいサービスを想定している。

※２ 「行政文書の管理に関するガイドライン」（平成 23 年４月１日内閣総理大臣決定、令和４年２月 7 日全部改定）第 10 秘密文書等の管理

出典：総務省．地方公共団体における情報セキュリティポリシーに関するガイドライン（令和 7 年３月版）．2025-3-28. https://www.soumu.go.jp/main_content/001000932.pdf, （参照 2026-3-16）

2. 機能要件定義

2.1. 機能に関する事項

(1) 本基盤のクラウド環境における機能要件
本基盤でクラウド環境に要求する主要な機能の要件を以下に示す。

ア　クラウド環境全体管理
- 業務システム単位ごとに領域（アカウント/ネットワークなど）を準備できること。
- 業務システム単位ごとに "作成"、"削除"、"停止" などを GUI や CLI を利用することで容易に行えるように設計すること。
- 組織管理機能を利用し、クラウド環境内において、業務システム単位でセキュリティ統制/ガバナンス統制/コスト管理が行えること。また、業務システム担当職員及び業務システム構築・運用事業者にクラウド管理コンソールにおいて操作可能な範囲を周知すること。

イ　仮想マシン
- 仮想マシンインスタンスの OS として、以下が払出せること。また、下記以外の OS についても、個別で業務システム担当職員及び業務システム構築・運用事業者が望む場合は、基盤担当職員と協議の上、当該 OS の払出を実施すること。
  - Windows Server 2019 / 2022 / 2025 以降
  - Red Hat Enterprise Linux 8 / 9 / 10 以降
  - Ubuntu Linux 24 / 25 以降
- 仮想マシンインスタンスの稼働場所を日本国内に指定できること。
- メーカーサポートが継続している OS バージョンについては、本機能でもサポートされること。
- 仮想マシンインスタンス向けの CPU アーキテクチャとして、x86-64 が提供されていること。
- 仮想マシンインスタンスで使用する CPU の製品名が開示されていること。
- 仮想マシンインスタンスで使用する CPU が複数の製造会社の製品から選べること。
- 業務システムの特性に合わせて、仮想マシンインスタンスに割り当てる CPU グレード、メモリ割り当て量を複数の選択肢から選べること。
- 運用時において、仮想マシンインスタンスのスケールアップ/ダウンによる拡縮が行えること。

ウ　ストレージ
- 各種ストレージは稼働場所を日本国内に指定できること。
- 仮想マシンインスタンスが利用するブロックストレージについて、HDD か SSD かを選択可能であること。また、業務システムの特性に合わせ、ストレージアクセス性能を選択可能なこと。
- ブロックストレージの払出しにおいては、業務システム担当職員及び業務システム構築・運用事業者にヒアリングの上最適なボリューム構成を取ること。また、コスト最適化のため、各ブロックストレージ容量はスモールスタートで払出すこと。
- 業務システム稼働後に、任意のタイミングでブロックストレージの容量拡張ができること。
- 保管を主目的としアクセス頻度が低いデータについては、ブロックストレージより安価なオブジェクトストレージで保管する設計を実装し、全体コスト最適化を図ること。（例：ログ、退避用業務データ等）
- オブジェクトストレージのデータアクセスは、仮想マシン経由に限定し、業務システム担当職員や業務システム構築・運用事業者等によるクラウド管理コンソールからのストレージアクセス及びデータのダウンロード行為を禁止できること。

・　オブジェクトストレージに格納されるデータに対して、データ改ざん・誤削除の対策を実装すること。
・　オブジェクトストレージに格納されるデータに対して、データ削除タイミング等のライフサイクルの設定が可能なこと。（コスト最適化のため、保管期限を超えたデータは自動削除できる等の機構を準備すること）
・　NFS 又は SMB で接続可能なファイルストレージを準備可能な機能を有していること

エ　データベース
・　以下のデータベースマネジメントシステムについては、PaaS 型データベースが提供できること。
  ➢　Oracle Database 19c / 21c 以降
  ➢　Postgres SQL 17 / 18 以降
・　提供するデータベースインスタンスのサービス稼働場所は、日本国内に閉じられること。
・　データベースインスタンスを提供する際、業務システム担当職員及び業務システム構築・運用事業者がデータベースマネジメントシステムのライセンスを持ち込んだ場合は BYOL 型の PaaS サービス提供を検討し、コスト最適化を図ること。
・　手動でのデータベースインスタンスへのパッチ適用機能を有すること。（パッチの適用タイミングは業務システム担当職員及び業務システム構築・運用事業者で判断する。）
・　提供するデータベースインスタンスにおいては、PITR（Point In Time Recovery）を有するバックアップリカバリ機能を実装できること。
・　運用時において、データベースインスタンスのスケールアップ/ダウンによる拡縮が行えること。
・　提供するデータベースインスタンスにおいて、データベース監査ログ等の取得が可能なこと。

オ　名前解決
・　本基盤のクラウド内の名前解決機能は、クラウドのマネージドサービスで実装すること。
・　名前解決実装に用いるマネージドサービスは、冗長化等を検討し、理論上の稼働率が 99.99%以上となる高可用性の構成を取ること。
・　基盤内部の名前解決について、オンプレミス側の名前解決機能（＝マロニエ 21 ネットシステムの名前解決機能）と相互に名前解決可能になるよう、条件付きフォワーダ相当の機能を有すること。
・　基盤外部からの名前解決について、県民からの本基盤上の業務システムへのアクセス等で外部からのインターネットアクセス（外部公開）を許可する必要がある場合は、「インターネット→栃木県セキュリティクラウド→本基盤クラウド環境」の通信経路とし、栃木県セキュリティクラウドと連携して本通信に必要な名前解決が実装できること。

カ　時刻同期
・　クラウド基盤において、協定世界時（UTC）を基準とした正確な日本標準時（JST）を提供する時刻同期サービスを実装すること。また、このサービスを基盤全体の統一時刻として利用し、各システムの時刻を同期できること。

キ　プロキシ
・　以下の通信についてはクラウド環境からインターネットへのアウトバウンド通信を直接許可することを想定している。
  ➢　ウイルス対策ソフトのパターンファイル更新
  ➢　クラウド環境上の仮想マシン OS 等に対する修正プログラム適用
  ➢　クラウド環境上の仮想マシンにインストールされたソフトウェアのアクティベーション
  上記通信の実装に伴い、インターネット境界点に本基盤（クラウド）内共用のプロキシ機能を設置し、当該アウトバウンド通信のアクセスログ取得と通信アクセス先の URL フィルタリング制御を実装する

こと。

ク　ネットワーク

- 「(1)キ　プロキシ」に記載のとおり、本基盤ではクラウドからインターネットへのアウトバウンド通信の要件があるため、当該通信を実装可能なネットワーク環境を設計すること。
- 本基盤上の各業務システムに対し論理的に独立した仮想ネットワーク（Virtual Private Cloud）を払出せるようにネットワーク設計を行うこと。
- 「(1)オ　名前解決」に記載のとおり、本基盤ではインターネットから本基盤上の一部業務システムへのインバウンド通信要件があるため、当該通信においては栃木県セキュリティクラウドの CDN 機能を介して通信ができるようにネットワークを実装すること。
- クラウド内の通信については、クラウドが提供するプライベート通信機能等を利用し、当該通信がインターネット経由の通信にならないように設計を行うこと。
- 本基盤上のシングル構成の業務システム群については、連携通信の発生を考慮し、基本的には同一のアベイラビリティゾーン（AZ）に設置する方針とし、通信コストの最適化を図ること。ただし、冗長構成で信頼性を確保している業務システムに関しては、この限りではない。
- 本基盤上の異なる業務システム間の連携通信については、異なる仮想ネットワーク間の連携通信となることを想定している。当該連携通信の実装には、クラウド内にネットワーク HUB 機能を用いることで実現すること。また、当該 HUB 機能においては通信障害などの原因特定のために通信ログが採取できる機能を有すること。
- 本基盤上の業務システムが属するネットワークは、いわゆる「三層の構え」による自治体情報セキュリティ対策のための以下の 3 層のネットワーク（以下「自治体 3 層ネットワーク」という。）を想定し、総務省ガイドラインや栃木県セキュリティポリシーに基づいて構成すること。
  - インターネット接続系
  - LGWAN 接続系
  - 個人番号利用事務系

  また、各ネットワークに対し管理領域を用意し、WSUS 機能やウイルス対策機能等を設置すること。なお、今後の業務システム担当職員及び業務システム構築・運用事業者の希望により、上記に該当しない独立ネットワーク系の業務システムを本基盤のクラウド環境に受け入れる可能性があることをネットワーク設計に考慮すること。
- 庁内 LAN と本基盤のクラウド環境を接続する閉域網回線（以下「クラウド接続回線」という。）は、別の調達により、回線事業者から調達予定である。ただし、当該クラウド接続回線をクラウド環境に接続するための仮想ネットワークの設計・実装は、基盤設計・開発業務受託者が実施すること。なお、クラウド接続回線は自治体 3 層ネットワーク構成によるルーティング方式で調達を予定し、各回線は信頼性確保のためデュアルロケーションによる接続方式とする。
- 特定通信等、自治体 3 層ネットワークをまたいだ業務システム間の連携通信が発生することも考慮すること。

ケ　ファイアウォール

- 単一のセキュリティ機能に依存せず、複数の防御レイヤを組み合わせてリスクを低減すること。
- ネットワーク境界及びサブネットレベルで、明示的な許可ルールのみを適用する「デフォルト拒否」ポリシーを採用すること。
- インバウンド及びアウトバウンド通信は、必要最小限のポート・プロトコル・送信元/宛先に限定すること。
- サブネット単位でアクセス制御を行い、異なるセグメント間の通信を制御すること。

・ 本基盤上の業務システムの通信要件についても、業務システム担当職員及び業務システム構築・運用事業者に対し、基盤設計・開発業務受託者又は基盤運用・保守業務受託者がヒアリングを実施し、当該事業者にてファイアウォール設定の実装を行うこと。 また、ファイアウォールの設定については必要最低限の通信許可設定とすること。
・ 仮想ネットワークの単位でもアクセス制御を行い、本基盤上の異なる業務システム間の通信についても適切に制御すること。（透過設定）

コ ロードバランサ
・ 業務システム担当職員及び業務システム構築・運用事業者の要求に応じて、クラウドが提供するマネージドサービスのロードバランサが提供できること。
・ 以下を満たすアプリケーション層ロードバランサが提供可能なこと。
  - HTTP/HTTPS レベルでの負荷分散をサポートし、TLS 終端（SSL オフロード）を実施可能である。また、HTTPS 通信を強制し、TLS 証明書の管理ができること。
  - パスベース、ホストベースのルーティングをサポートし、ヘッダーやクエリパラメータによる動的ルーティングが可能であること。
  - アプリケーションレベルのヘルスチェック（HTTP ステータスコード）をサポートできる。また、ヘルスチェックの実行間隔、タイムアウト、再試行回数を設定可能であり、ヘルスチェックに失敗したロードバランス先のターゲットを自動的に切り離し、正常なターゲットのみへトラフィックを転送できること。
  - スティッキーセッション（Cookie ベース又はアプリケーション定義）をサポートし、セッションの一貫性を確保できること。
・ 以下を満たすネットワーク層ロードバランサが提供可能なこと。
  - TCP/UDP レベルでの負荷分散をサポートできること。
  - ソース IP 保持（透過型ロードバランシング）をサポートできること。
  - TCP 又は HTTP ヘルスチェックが可能で、ヘルスチェックの実行間隔、タイムアウト、再試行回数を設定可能であり、ヘルスチェックに失敗したロードバランス先のターゲットを自動的に切り離し、正常なターゲットのみへトラフィックを転送できること。
  - アウトバウンド先の相手がソースを絞ってアクセス制限をしていた場合を考慮して IP アドレス固定をできること。

サ 認証・アカウント管理
・ ユーザアカウントの発行単位は個人単位とし、共用禁止とすること。
・ クラウド（クラウド管理コンソール）を利用するユーザアカウント等には、各ユーザ・各マネージドサービスに対し必要最低限な権限付与を行えること。
・ 業務システム単位ごとにアカウントのグループ化を行えること。
・ クラウド管理コンソールアクセスの認証については、多要素認証を必須として実装できること。

シ 暗号化管理
・ 各種データを保管する領域については、格納領域の暗号化を実施すること。
・ http 等のデータ通信について、暗号化が実施できること。
・ クラウドの機能にて、暗号鍵の管理が行えること。
・ 暗号鍵は、クラウドの機能を利用して独自発行した鍵が利用可能であること。
・ クラウド内で発行した証明書、外部機関が発行した証明書などを一元管理できる機能を有すること。
・ 証明書の有効期限が切れる前に通知される仕組みを採用すること。

・　利用する暗号技術は、最新の『CRYPTREC 暗号リスト』に基づき、クラウドサービスで選択可能な範囲から方式を選定すること。

ス　ウイルス対策

・　クラウド内で稼働する仮想マシンに対し、ウイルス対策機能を実装すること。また、業務システム担当職員及び業務システム構築・運用事業者の要望に応じて、ウイルス対策のスキャン除外設定の実装等も調整すること。
・　ウイルス対策のスキャンに用いるパターンファイルは、日次以上の頻度でオンラインアップデートができる構成を取ること。
・　クラウド内で稼働する仮想マシンに対し、振る舞い検知機能を実装すること。また、昨今のセキュリティ事案を鑑み、予防的統制だけでなく、発見的統制の強化できるよう EDR/XDR や変更監視などの機能を保有していること。

セ　クラウド内脅威分析

・　システムの操作ログ、名前解決ログなどを収集・リアルタイムで分析し、クラウド内の悪意ある挙動や不正アクセスを検知できる機能を実装すること。
・　外部の脅威情報やブラックリストを活用し、既知・未知の脅威を検知する、脅威インテリジェンス連携が実装できること。また、検知した脅威内容について、基盤管理者等へ発報ができること。

ソ　コスト管理

・　業務システムの単位で月額クラウド利用料の予算設定ができること。
・　利用料実績が予算を超過した（設定閾値を超えた）場合等に、対象の業務システム担当職員及び業務システム構築・運用事業者並びに基盤管理者に対し、アラート通知が発報できること。
・　業務システム単位にて、クラウドサービスごとの利用状況を可視化し、コスト分析が行える機能を有すること。
・　基盤管理者が分析内容を CSV 等の形式でエクスポートする機能を有すること。
・　予算利用状況を可視化できるコストレポートを週次で出力できること。

タ　バックアップ・リストア

・　本基盤が提供するバックアップ・リストア機能は、仮想マシンインスタンス及びデータベースインスタンス単位でバックアップ（スナップショット）を取得し、有事の際にリストア可能な方式とすること。
・　バックアップ機能の提供対象は以下クラウド上の仮想リソースとすること。
    ➢　仮想マシン（IaaS ベース）
    ➢　データベース（PaaS ベース）

    また、取得したバックアップデータはバックアップを取得したリージョンとは別の国内リージョンにデータ同期ができること。
・　本基盤が提供するバックアップの取得頻度は、日次とすること。
・　本基盤が提供するバックアップ機能のバックアップ世代数は、7 世代とすること。
・　バックアップ処理が失敗した場合は、基盤管理者に対し、その旨の発報が可能なこと。
・　上記以上のバックアップ要件が必要な場合は、業務システム担当職員及び業務システム構築・運用事業者で個別バックアップを実装するため、当該要件を実装するに当たって必要となるストレージ等（個別バックアップ領域）の払出しについては、基盤管理者側で対応すること。
・　本基盤が提供するバックアップデータからのリストア機能については、バックアップの世代指定が可能かつサーバディスクボリューム単位及びファイル単位でのリストアが可能なこと。また、別の国内リージョンに

保管されたバックアップデータからメインリージョンでリストアができること。

チ　性能情報収集

- システムやサービス処理の稼働状況を継続的に収集し、性能分析・障害検知・キャパシティ計画に活用できる機能を実装すること。また、収集した情報はモニタリングが可能であること。
- 収集する性能情報は、以下を想定している。
  - リソースの稼働状況に係る情報
  - リソース利用率に係る情報（CPU、メモリ、ストレージ、回線ネットワーク帯域等）
  - 可用性に係る情報（ロードバランサ分散先ターゲットの台数等）
  - 業務条件に応じた独自指標

ツ　システム監視

- 性能情報収集機能で収集した情報に閾値を設定する等で、クラウド環境内のリソースに対し以下の監視が実現できること。
  - 死活監視
  - OS のプロセス/サービス監視
  - リソース監視
  - テキストログ監視
- 監視により異常を検知した場合は、適切な通知先に異常検知内容を発報できること。
  また、発報先について発報先上限数が無いこと。

テ　マネージドサービス監視

- クラウド事業者が管理しているクラウドの各マネージドサービスについて、利用するリージョンにおける稼働正常性ステータスを一覧表示できること。
- クラウド環境に影響する以下イベントを、基盤管理者が業務システム単位で情報表示できること。
  - サービスやリソースに影響を与える障害イベント
  - メンテナンスやアップデートの予定
  - アカウント管理やセキュリティに関する重要な通知
- 基盤利用者に重大な影響を与えるイベント等を含む、マネージドサービス単位の通知については、通知先を指定して発報ができること。

ト　ログ管理

- 本基盤として、以下のログ種別を定義し、ログ管理を実施すること。
  - 基盤ログ（システムログ）：システムの稼働状況やイベントを記録するログ
  - 基盤ログ（証跡ログ）　　：利用者やシステムの操作履歴を証拠として残すログ
- ログの保管要件については、以下とすること。
  - 基盤ログ（システムログ）：1 年以上
  - 基盤ログ（証跡ログ）　　：5 年以上
- ログの保管に際しては、基盤全体のコストが最適化されるよう設計に留意すること。
- 保管しているログについては各業務サーバ等で閲覧が可能なこと。
- 業務システム担当職員及び業務システム構築・運用事業者が実施すべき業務ログ等のログ保管についても適切に実施されるよう、基盤設計・開発業務受託者及び基盤運用・保守業務受託者にて統制を取ること。

ナ　クラウド API 操作証跡取得

- クラウド内でユーザアカウント及びサービスが API 操作した実行履歴を証跡（操作履歴）として取得

できること。また、取得された証跡が改ざんされていないことを確認できる機能（整合性の検証機能）を有していること。
・ 直近 3 カ月以内の証跡については、障害調査等のために簡易に検索・閲覧ができること。

ニ 構成情報管理
・ クラウド環境におけるサーバ OS の構成情報を一元的に管理し、セキュリティ及び運用の可視性を確保できること。具体的には、以下の情報等を管理すること。
  ➢ OS バージョン・パッチレベル情報
  ➢ ネットワーク情報
  ➢ インストール済ソフトウェア情報
・ サーバ OS の構成情報は定期的に収集し最新化すること。
・ クラウド内の環境構成情報についても採取し、構成情報の変更履歴が追える機能を有すること。また、逸脱した構成情報の変更が行われた場合、検知及びアラート通知が可能なこと。

ヌ パッチ適用管理
・ クラウド環境上のサーバにおける OS パッチ適用状況が適宜確認できる機能を有すること。
・ 本基盤として、WSUS 機能を提供すること。なお、WSUS 機能の管理対象は以下とする。
  ➢ クラウド環境上の仮想マシン
・ yum リポジトリも必要に応じて準備すること。

ネ ジョブ管理
・ 必要に応じて本基盤上のインフラ管理機能及び業務システムが、クラウドより提供されるマネージドサービスを利用可能な状態にすること。

ノ リモート接続
・ クラウド管理コンソールにアクセス可能な端末は特定の構築・保守端末に限定すること。（許可外の作業端末からはアクセス不可であること。）
・ クラウド環境内のサーバ OS へは本県庁舎に設置予定の運用保守端末から接続することを前提とすること。（≒栃木県セキュリティポリシーから逸脱しない接続とすること。）

ハ 運用保守端末
・ クラウド管理コンソール等、クラウド環境の運用に必要なブラウザやソフトウェアを提供すること。

ヒ その他
本システムの構築・運用において、クラウドサービスプロバイダから提供されるエンタープライズレベルのサポートを必須とする。具体的には、以下の条件を満たすこと。
・ 24 時間 365 日、日本語対応での技術サポートを提供できること。
・ 重大障害時の優先対応及び迅速なエスカレーション体制を備えていること。
・ 専任のテクニカルアカウントマネージャー（TAM）又は同等の窓口を設置し、運用・設計に関する相談が可能であること。
・ ベストプラクティスやアーキテクチャレビューの提供を含む、プロアクティブなサポートサービスを利用できること。

(2) 本基盤のオンプレミス環境における機能要件
本基盤でオンプレミス環境に要求する主要な機能の要件を以下に示す。

ア 仮想サーバ

・ 物理サーバ上で複数の仮想マシンを動作させることができる仮想サーバを用意すること。
・ 仮想マシン及び仮想マシンを構成するファイルは、仮想サーバを停止することなく、基盤システムを構成するハードウェア間を任意に移動（ライブマイグレーション）できること。
・ 仮想化基盤を構成する機器は仮想化ホスト、共有ストレージ、ネットワーク機器ごとにそれぞれ複数台でクラスタを構成できること。また、クラスタは冗長性を考慮した構成とすること。
・ 追加クラスタソフトウェア等を利用せずハイパーバイザのみで、仮想サーバを二重化し、HA 構成を実現できること。
・ 仮想マシンが稼働する物理ホストに障害が発生し、異なる物理ホスト上で仮想マシンが再起動される際に、再起動する仮想マシンの優先順位を設定できること。
・ 仮想化ハイパーバイザは、仮想マシンのディスクごとにストレージ I/O 性能を制御する機能を有すること。また、ストレージ使用量と I/O 負荷状況を監視し、仮想マシンを構成するファイルの初期配置、再配置を動的、かつ自動的に行えること。
・ 仮想化ハイパーバイザは、仮想ネットワークの属性ごとにそれぞれネットワーク I/O 性能を制御する機能を有すること。
・ 本基盤オンプレミス環境における仮想マシンの管理/設定を行う仮想化統合管理サーバを設置すること。
・ 仮想化統合管理サーバはライセンス削減と管理性の観点から仮想アプライアンスサーバとして構築すること。
・ 仮想マシンに対するスナップショットやテンプレートを用いたクローンが作成可能なこと。
・ 仮想環境の物理サーバを横断するように仮想スイッチや仮想ファイアウォール、仮想ルータを構成し、設定を一元化できること。また、トラブルシュートを効率的に行うため仮想スイッチ上にミラーポートを構成できる機能を有すること。
・ 仮想マシンの移行性を向上させるため、仮想統合管理サーバ間において仮想マシンを無停止で移動（ライブマイグレーション）させることが可能なこと。
・ 業務システムごとにアクセス権を設定し、業務システム担当職員及び業務システム構築・運用事業者が管理外のシステムを操作できないようにすること。
・ 仮想マシンの OS として掲げるものが使用可能であること。なお、業務システムに払出す仮想マシンに必要な以下に掲げる OS ライセンスについては、基盤管理者にて用意すること。また、以下以外の OS についても、個別で業務システム担当職員及び業務システム構築・運用事業者が望む場合は、基盤担当職員と協議の上、当該 OS の基盤受入を実施すること。
  - Windows Server 2019 / 2022 / 2025 以降
  - Red Hat Enterprise Linux 8 / 9 / 10 以降

イ 共有ストレージ
・ 本基盤オンプレミス環境における仮想マシン領域として使用する仮想環境用ストレージを用意すること。
・ 本基盤オンプレミス環境における仮想マシンのバックアップ用ストレージとして使用するバックアップ用ストレージを用意すること。
・ RAID は 6 以上相当とすること。
・ 仮想環境用ストレージとバックアップ用ストレージ間でレプリケーションが行えること。
・ 定期的にスナップショットを取得可能であること。保存可能な世代数は 7 世代以上であること。
・ バックアップ用ストレージ内に業務データのバックアップ領域を用意すること。プロトコルは CIFS、NFS 及び SMB を想定すること。

ウ　データベース

・　基盤利用者に Oracle Database Standard Edition 2 のライセンスが提供可能であること。

エ　名前解決

・　本基盤のオンプレミス環境のサーバの名前解決機能を運用管理サーバに用意すること。

オ　時刻同期

・　本基盤のオンプレミス環境のサーバ等の時刻同期ができるように NTP 機能を構築すること。

カ　プロキシ

・　本基盤のオンプレミス環境において、最新のウイルスパターンファイルをダウンロードする際は、マロニエ 21 ネットシステムのプロキシ機能を利用するよう構築すること。

キ　ネットワーク

・　本基盤オンプレミス環境における仮想ネットワークは、オーバーレイ型ネットワークによって、物理ネットワークトポロジとは分離された柔軟な仮想ネットワークとすること。
・　異なるセグメントであっても同一仮想化ホストサーバ内の仮想マシン間通信はホスト内部で完結し、物理ルータへの転送が不要な構成とすること。
・　基盤システムを利用するためのネットワークを業務用ネットワーク、基盤システムを管理するためのネットワークを管理用ネットワークとして用意すること。
・　管理用ネットワーク経由で仮想マシン同士が通信可能とならないよう、セキュリティに配慮すること。
・　管理用ネットワークからインターネットに接続できないこと。
・　本基盤上の各業務システムに対し論理的に独立した仮想ネットワークを払出せるようにネットワーク設計を行うこと。
・　本調達機器については、県ネットワーク及び管理用ネットワークへの接続を行うこと。接続に必要となる要件を確認し、設計・開発及び設定作業を行うこと。詳細は「図 3-1　次期基盤システムのイメージ」を参照すること。
・　「(2)エ　名前解決」に記載のとおり、本基盤ではインターネットから本基盤上の一部業務システムへのインバウンド通信要件が必要となるため、外部からのインターネット通信があることを考慮した設計とすること。
・　本基盤上の業務システムが属するネットワークは、以下の自治体 3 層ネットワークを想定し、総務省ガイドラインや栃木県セキュリティポリシーに基づいて構成すること。
    - ➢　インターネット接続系
    - ➢　LGWAN 接続系
    - ➢　個人番号利用事務系
・　業務システム担当職員及び業務システム構築・運用事業者の希望により、上記に該当しない独立ネットワーク系の業務システムを本基盤オンプレミス環境に存在するため、それらを考慮したネットワーク設計とすること。
・　特定通信等、自治体 3 層ネットワークをまたいだ業務システム間の連携通信が発生することも考慮すること。

ク　ファイアウォール

・　脅威侵入時の内部拡散防止のため、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を構成すること。

ケ　ロードバランサ

・ ロードバランサ機能を利用し複数の仮想マシンの集合への通信をロードバランスさせることにより、通信の負荷分散及び可用性の向上を実現する機能を構成すること。
・ ロードバランサは冗長構成とすること。
・ ロードバランサはライセンス削減と管理性の観点から本基盤のオンプレミス環境上に仮想アプライアンスとして構築すること。
・ セッション維持機能として以下分散方式に対応していること。
  - ノード単位の分散
  - Cookie オプション
  - URL リライトオプション
  - HTTP 認証ヘッダーオプション
  - SSL セッション ID オプション
・ ロードバランサライセンスについては 34 台分用意すること。

コ 認証・アカウント管理
・ ユーザアカウントの発行単位は個人単位とし、共用禁止とすること。なお、業務システム単位ごとにアカウントのグループ化が行え、適切な権限付与が行えること。
・ 本基盤オンプレミス環境における仮想基盤（管理コンソール）を利用するユーザアカウント等には、各ユーザに対し必要最低限な権限付与を行えること。

サ ウイルス対策
・ 本基盤のオンプレミス環境における Windows 及び Linux の仮想マシンは、エージェント方式でアンチウイルス機能を実現すること。
・ 業務システム担当職員及び業務システム構築・運用事業者の要望に応じて、ウイルス対策のスキャン除外設定の実装等を調整すること。
・ ウイルス対策のスキャンに用いるパターンファイルは、日次以上の頻度でオンラインアップデートができる構成を取ること。
・ ウイルス対策ソフトのパターンファイルを含むアップデートは、自動で行えること。
・ 本基盤オンプレミス環境内で稼働する仮想マシンに対し、振る舞い検知機能を実装すること。また、昨今のセキュリティ事案を鑑み、予防的統制だけでなく、発見的統制の強化できるよう EDR/XDR や変更監視などの機能を保有していること。
・ 本基盤オンプレミス環境内で稼働する仮想マシンに向けたウイルス対策機能と別に、Apex One の管理サーバをクラウド内に設置し、以下に対しウイルス対策機能を提供すること。なお、Apex One のライセンスについては、別事業者調達物（マロニエ 21 ネットシステム所有）を利用すること。
  - 本基盤を構成する運用保守端末
  - 本基盤_オンプレミス環境を構成する物理サーバ

シ バックアップ・リストア
・ 「(2) イ 共有ストレージ」に記載のとおり、仮想マシン単位のバックアップを取得し、有事の際にリストア可能なこと。
・ 上記以上のバックアップ要件が必要な場合は、業務システム担当職員及び業務システム構築・運用事業者で個別バックアップを実装するため、当該要件を実装するに当たって必要となるストレージ等（個別バックアップ領域）の払出しについては、基盤管理者側で対応すること。
・ 本基盤が提供するバックアップデータからのリストア機能については、バックアップの世代指定が可能かつサーバディスクボリューム単位及びファイル単位でのリストアが可能なこと。また、バックアップ用ストレー

ジに保管されたバックアップデータから仮想環境用ストレージにリストアが行えること。
- 運用管理サーバとシステム監視サーバのバックアップ機能については、システムを含むイメージバックアップが可能なこと。
- 運用管理サーバとシステム監視サーバのリストア機能については、バックアップの世代指定が可能かつサーバディスクボリューム単位及びファイル単位でのリストアが可能なこと。

ス　性能情報収集
- 本基盤オンプレミス環境における仮想化環境全体のステータスを分析し、仮想基盤のキャパシティやリソースの使用状況などを可視化・分析する仮想化統合監視サーバを設置すること。
- 本調達機器等の機器についても、監視対象となるため、仮想化統合監視サーバで各種監視を行うための設定を行うこと。なお、必要な設定情報等については、本県と協議の上、決定すること。
- 仮想化統合監視サーバはライセンス削減と管理性の観点から仮想アプライアンスサーバとすること。
- 本基盤オンプレミス環境における仮想化基盤の使用状況最適化を図るために仮想基盤の状況を、把握・可視化する運用監視機能を有すること。
- 仮想化統合監視サーバは、仮想マシンのステータスを俯瞰的に確認できるダッシュボードを有すること。また、これをカスタマイズできる機能を実装すること。
- 統計情報を一定期間蓄積することで、監視対象オブジェクトの正常稼働状態を学習し、学習したデータから動的閾値を生成できること。
- 動的な閾値を利用し、各仮想基盤オブジェクト（仮想マシンや仮想サーバ、クラスタ、データストアなどの仮想基盤オブジェクト）の異常性を判断できること。
- 仮想化統合ログサーバにプラグインを追加することで仮想ネットワーク製品やストレージ製品のステータスを可視化できること。
- リソース使用状況から、CPU、メモリ、ディスク領域の枯渇時期（残り時間）を自動的にシミュレーションし、自動表示できること。
- 管理対象の仮想マシンにエージェント等のインストールが不要であること。
- ユーザがシナリオを入力することで、任意の時点（リソースの変更日時を将来時点にするなど）から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。また、そのシナリオを保存できること。
- 仮想基盤の最適化を行うことを目的として、現在の仮想マシンの稼働状況や、残り何台の仮想マシンが稼働できるか等の情報が定量的且つリアルタイムに把握できる機能を実装すること。また、定期的に自動でレポート出力できる機能を実装すること。
- 本基盤オンプレミス環境における仮想化環境全体のログを収集し可視化・分析する装置として仮想化統合ログサーバを設置すること。
- 本基盤オンプレミス環境サーバにおいては、本調達機器の各種ログも取得するため、仮想化統合ログサーバとの連携を行うこと。なお、必要な設定情報等については、本県と協議の上、決定すること。
- 仮想化統合ログサーバはライセンス削減と管理性の観点から仮想アプライアンスサーバとすること。
- 本基盤オンプレミス環境における仮想基盤ならびに仮想ネットワークのシステムログを一元的に収集し、分析できること。
- 仮想化ハイパーバイザのログについての説明を仮想化統合ログサーバ上に組み込み、必要時に参照できるようにすること。
- 収集されたログを分析することで、特定のログの単位時間当たりの出現数に応じてアラートを発報できること。
- 日々の運用に柔軟に対応できるよう、カスタマイズ可能なダッシュボードを作成する機能を実装すること。
- 仮想基盤や仮想ネットワークについて、VMWare が提供するダッシュボードが使用できること。

・　監視により異常を検知した場合は、適切な通知先に異常検知内容を発報できること。

セ　システム監視

・　本基盤オンプレミス環境における仮想サーバ及びネットワーク機器等の物理機器の監視を行う装置としてシステム監視サーバを設置すること。
・　監視項目は以下の監視が実現できること。
  ➢　リソース監視
  ➢　ハードウェア監視
・　監視により異常を検知した場合は、適切な通知先に異常検知内容を発報できること。
  また、発報先について発報先上限数が無いこと。
・　一部の異常検知については、積層信号灯に対しアラート設定を実装すること。アラート設定の実装対象となる異常検知の項目については県と調整すること。
・　本基盤の業務時間外において、基盤の死活監視等により翌日の基盤稼働に影響を及ぼす重大な異常を検知した場合、当該内容を基盤担当職員及び基盤運用・保守業務受託者に対して、電話により発報すること。また、当該異常検知に係る電話での発報実績等について四半期単位のレポートの出力が行えること。

ソ　ログ管理

・　本基盤オンプレミス環境のログ管理として、以下のログ種別を定義し、ログ管理を検討すること。
  ➢　基盤ログ（システムログ）：システムの稼働状況やイベントを記録するログ
  ➢　基盤ログ（証跡ログ）　　：利用者やシステムの操作履歴を証拠として残すログ
・　ログの保管要件については、以下とすること。
  ➢　基盤ログ（システムログ）：1 年以上
  ➢　基盤ログ（証跡ログ）　　：5 年以上
・　ログの保管に際しては、基盤全体のコストが最適化されるように設計に留意すること。
・　保管しているログについては各業務サーバ等で閲覧が可能なこと。
・　業務システム担当職員及び業務システム構築・運用事業者が実施すべき業務ログ等のログ保管についても適切に実施されるよう、基盤設計・開発業務受託者及び基盤運用・保守業務受託者にて統制を取ること。

タ　パッチ適用管理

・　本基盤として、WSUS 機能を提供すること。なお、WSUS 機能の管理対象は以下 2 つとする。
  ➢　本基盤の運用保守端末
  ➢　本基盤の物理サーバ（運用管理サーバ等）

チ　ジョブ管理

・　必要に応じて本基盤上のインフラ管理機能及び業務システムが利用可能な状態にすること。

ツ　リモート接続

・　オンプレミス環境内のサーバ OS へは本県庁舎に設置予定の運用保守端末から接続することを前提とすること。（≒栃木県セキュリティポリシーから逸脱しない接続とすること。）
・　既存基盤システム（第 2 期基盤）で業務システムが構築したリモート保守回線を用いて実装しているリモート接続については、本基盤のセキュリティ対策に影響の無い範囲で引き続き実装を可能とすること。

テ　電源管理

- 電源障害や停電が発生した場合に備え、高機能無停電電源装置（以下「UPS」という。）による電源供給を行うこと。
- UPS 障害に備え、UPS の冗長化を行うこと。
- オンプレミス環境の機器設置場所において、電源障害や停電を検知したら、自動的に OS のシャットダウンが行えること。

ト　運用保守端末

- 業務システム担当職員及び業務システム構築・運用事業者が、担当システムや担当システムの仮想マシンを操作・管理するための端末を、運用保守端末として提供すること。
- 仮想マシンの管理に必要となる適切な設定を実施すること。

2.2. 画面に関する事項

(1) 画面に関する事項

前述の「2.1 機能に関する事項」を実現するために必要な画面については、独自の画面作成を想定していないが、基盤設計・開発業務受託者の提案を踏まえ必要に応じて決定する。

2.3. 帳票に関する事項

(1) 帳票に関する事項

前述の「2.1 機能に関する事項」を実現するために必要な帳票については、独自の帳票作成を想定していないが、基盤設計・開発業務受託者の提案を踏まえ必要に応じて決定する。

2.4. データに関する事項

(1) データに関する事項

本基盤においてデータの概念設計等は実施しない。

2.5. 外部インタフェースに関する事項

本基盤の外部インタフェース（外部システム連携）に関する要件を以下に示す。なお、一部のインタフェースは機能要件の変更に合わせて修正が必要になることが想定される。新たに追加となった機能への対応を含め、外部インタフェースの修正が必要になる場合については、設計工程で基盤担当職員と協議の上対応すること。なお、インタフェースについては API 連携を原則とし、旧来型のインタフェースについては API 化を積極的に提案すること。

(1) 外部システム連携先

本基盤は、下表に示す他の情報システム等と連携する。なお、下表の外部システム連携先は現在の想定である。設計工程において、連携先システム担当と調整の上、決定すること。

表 2-1 外部システム連携先一覧（想定）

項番	連携システム名	連携システム概要	連携目的	補足
1	マロニエ 21 ネットシステム	いわゆるイントラネットシステム。LGWAN 接続系及びインターネット接続系において端末や NTP/DNS/ウイルス対策といったインフラ管理機能を本県全体に提供。	本基盤上の業務システム（LGWAN 接続系及びインターネット接続系）に対するインフラ管理機能の提供	
2	個人番号利用事務認証システム	個人番号利用事務系において端末や NTP/DNS/ウイルス対策といったインフラ管理機能を本県全体に提供。	本基盤上の業務システム（個人番号利用事務系）に対するインフラ管理機能の提供	
3	庁内 LAN	栃木県庁舎内に提供されているネットワーク。 本県庁コアスイッチでネットワーク全体を管理。 庁内から本基盤のクラウド環境に閉域接続するための閉域網を管理。	本基盤内機器の一部 IP 管理	
4	栃木県セキュリティクラウド	サイバー攻撃や情報漏洩からデータを守るための高度なセキュリティ対策を提供するサービス	インターネット接続点におけるセキュリティ確保（CDN/WAF）	
5	本基盤上の業務システムの、業務連携先システム	左記のとおり	業務連携	業務連携通信の実装経路について、基盤管理者も実装調整に入ること

3. 非機能要件定義

3.1. ユーザビリティ及びアクセシビリティに関する事項

(1) 基盤利用者の種類、特性

基盤利用者の種類、特性について、下表に示す。

表 3-1 基盤利用者の種類、特性

項番	利用者区分	基盤利用者の種類	利用イメージ	特性
1	業務システム担当職員	本基盤上の業務システムの設計・開発又は運用保守担当職員	本基盤上の業務システムの設計・開発又は運用保守に当たり、必要に応じて本基盤の操作を行う。	パソコンの操作について、事務作業等に係る一定の知識・スキルはあるが、情報システムに関する専門的、技術的な知識・スキルは多くはないため、ユーザビリティ上留意する必要がある。
2	本県職員	本基盤上の業務システムを利用する、全本県職員。 直接利用するのは業務システムで、本基盤の直接の操作は実施しない想定。	職務を遂行するため、本基盤上の業務システムの操作を行う。	パソコンの操作について、事務作業等に係る一定の知識・スキルはあるが、情報システムに関する専門的、技術的な知識・スキルは多くはないため、ユーザビリティ上留意する必要がある。
3	業務システム構築・運用事業者	本基盤上の業務システムの設計・開発又は運用・保守業務受託者	本基盤上の業務システムの設計・開発又は運用保守に当たり、本基盤の操作を行う。	情報システムに係る一定の専門的、技術的な知識・スキルはあるが、クラウドサービスについては知見レベルの差異があることをユーザビリティ上留意する必要がある。

(2) ユーザビリティ要件

本基盤ではユーザビリティに関する要件は設けないが、「表 3-1 基盤利用者の種類、特性」に示す役割・業務内容に基づき、各利用者の特性を十分に留意すること。

(3) アクセシビリティ要件

本基盤ではアクセシビリティに関する要件は設けないが、「表 3-1 基盤利用者の種類、特性」に示す役割・業務内容に基づき、各利用者の特性を十分に留意すること。

3.2. **システム方式に関する事項**

(1) システム方式についての全体方針

システム方式についての全体方針を下表に示す。本基盤は IaaS とマネージドサービスを組み合わせた構成として、「とちぎ県庁クラウド利活用方針」及び「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針（以下「クラウド方針」という。）」に準拠し、クラウドサービスの提供機能を最大限活用するようデザインされた構成とすること。特に、信頼性、拡張性（スケーラビリティ）、継続性等の向上に寄与するクラウドサービスと構成を選定すること。なお、システム構成の検討に当たっては、「ガバメントクラウド利用における推奨構成」（デジタル庁）を参照すること。

表 3-2 システム方式についての全体方針

項番	観点	全体方針
1	インフラ全体構成	・本基盤においては、オンプレミスとクラウドによるハイブリッド構成とすること。なお、オンプレミスについては、本基盤と同時にクラウドリフトできない業務システムの受け皿としてのみ構築する。 ・オンプレミスとクラウドの各環境は、それぞれでインフラ機能を完結させ、オンプレミス基盤を撤去しても運用ができる構成とすること。（例：オンプレミス環境の監視はオンプレ用監視ソフトウェアを導入したサーバ、クラウド環境の監視は当該クラウドの SaaS で実装）
2	システム構成	・本基盤のシステム構成はクラウドサービス上に用意される管理領域と基盤利用者が使用する領域で構成すること。 ・本基盤の特性を十分に検討し、クラウドサービスプロバイダやデジタル庁のガバメントクラウドが提供するリファレンスアーキテクチャに準拠した形で PaaS、SaaS、IaaS 等の最適なサービスを採用し、構築すること。 ・クラウドサービスプロバイダが提供するマネージドサービスを最大限活用することを基本とし、アプリケーションの作り込みを削減できる設計とすること。特にデータベース、認証、セキュリティ機能や運用管理機能はクラウドサービスが提供する機能を最大限活用すること。 ・クラウドサービスが責任共有モデルとして提供されている前提を踏まえ、クラウドサービスを利用するに当たって必要となる考慮事項について検討を行い、安全かつ効率的に本基盤を構築すること。 ・予防的統制と発見的統制を実施すること。また、クラウドサービスを利用するために作成する各種アカウントについては、ガバナンスやセキュリティに係るポリシーを設定の上で、権限管理を確実に行うこと。クラウドサービスを利用するために作成する各種アカウントについては、多要素認証を必須とすること。 ・リソース使用量の変動等に柔軟に対応するとともに、コスト削減を図るため、民間クラウドサービスを利用すること。

		・全体構成及び利用するクラウドサービスについては、移行、引継ぎ、確実なサービス提供等について問題が生じないことを確認し、本調達の要件を踏まえ、確認結果と合わせて適切なものを採用すること。
3	ソフトウェア製品の活用方針	・SaaS については、開発量削減の観点から幅広く優先的に、その利用を検討すること。ただし、ニーズにマッチしているか、開発量削減に貢献するか、セキュリティ対策は十分か、費用対効果は十分に得られるか等を慎重に考慮すること。 ・広く市場に流通し、利用実績を十分に有するソフトウェア製品を活用すること。 ・アプリケーションの動作、性能等に支障を来たさない範囲において、可能な限りオープンソースソフトウェア（OSS）製品（ソースコードが無償で公開され、改良や再配布を行うことが誰に対しても許可されているソフトウェア製品）の活用を図ること。ただし、それらの OSS 製品のサポートが確実に継続されていることを確認すること。 ・ノンプログラミングによる画面生成等プロトタイピング用のツール等を利用することにより、システムライフサイクルコストの削減等が見込める場合には、積極的に採用を検討すること。

(2) クラウドサービスの選定、利用に関する要件

ア　セキュリティ確保のため、本基盤で用いるクラウドサービスは、原則として ISMAP クラウドサービスリストに登録されているクラウドサービスを選定すること。なお、例外的に ISMAP クラウドサービスリストに登録されていないクラウドサービスを選定する場合は、基盤設計・開発業務受託者の責任において、当該クラウドサービスが「ISMAP 管理基準」の管理策基準における統制目標（3 桁の番号で表現される項目）及び末尾に B が付された詳細管理策（4 桁の番号で表現される項目）と同等以上のセキュリティ水準を確保しているものを選定すること。

イ　情報資産を管理するデータセンタの設置場所に関しては、国内（東京/東日本リージョン）であること。

ウ　契約の解釈が日本法に基づくものであること。

エ　クラウドサービスの利用契約に関連して生じる一切の紛争は、日本の地方裁判所を専属的合意管轄裁判所とするものであること。

オ　基盤担当職員の指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。なお、本基盤上の業務システムにおいて、インターネットに公開している部分を除き、国外から情報資産へアクセスする場合も日本国外への持ち出しに該当する。

カ　障害発生時に縮退運転を行う際にも、情報資産が日本国外のデータセンタに移管されないこと。

キ　情報資産の所有権がクラウドサービス事業者に移管されるものではないこと。従って、基盤担当職員が要求する任意の時点で情報資産を他の環境に移管させることができること。

ク　クラウドサービスの可用性を保証するための十分な冗長性、障害時の円滑な切替え等の対策が講じられていること。

ケ　クラウドサービス上で取り扱う情報について、機密性及び完全性を確保するためのアクセス制御、暗号化及び暗号鍵の保護並びに管理を確実に行うこと。

コ　クラウドサービスに係るアクセスログ等の証跡を保存し、基盤担当職員からの要求があった場合は提供すること。

サ　インターネット回線を通じたセキュリティ侵害を防ぐため、インターネット回線と本基盤との接続点の通信を監視すること。

シ　クラウドサービスの提供に関する以下の認証を取得していること。
・　ISO/IEC 27017:2015

(3) 開発方式

ア　基盤導入時の業務システムクラウドリフトに当たっては、クラウドリフトする業務システム担当職員及び業務システム構築・運用事業者向けに事前検証を目的とした開発環境等をクラウド上で 3 か月分用意すること（基盤テストによるインフラ品質担保中でも業務システムが先行でクラウド実機検証を実施できることを目的とする）。各環境の詳細については「3.11.情報システム稼働環境に関する事項」を参照すること。

イ　API 設計には必要に応じて Open API 設計用のツールを利用すること。

(4) 機器等の設置方針

本基盤はクラウドサービスを前提としているため、設置場所についてはクラウドサービスプロバイダの提供する場所となるが、その際は日本国内のリージョンを選択すること（メインサイトは東京等の東日本設置リージョン、バックアップサイトは大阪等の西日本設置リージョンとすること）。また、本基盤の運用保守端末は、本県庁舎内に設置すること。

(5) その他

システム方式に係るその他の要件を以下に示す。

ア　本基盤は短期間での機能追加・改善を行うことが想定されており、できるだけ簡潔なアーキテクトかつ簡易な構成とすること。なお、IaaS/PaaS については単一クラウドサービスでの構築を想定している。

3.3. **システム規模に関する事項**

本基盤の規模要件を以下に示す。また、本基盤の規模に関する業務要件は、「1.3 業務の規模」を参照のこと。

(1) 規模に関する前提条件

本基盤はクラウドサービスを利用して運用されるため、以下の取り組みを行うこと。

ア　運用期間中において利用予定範囲を超過することがないよう、情報システムの縮退を検討するために必要となる情報収集等の仕組み（クラウドサービスの課金状況やリソースの利用量の監視、一定の閾値を超えた場合のアラート処理等）を設けること。定量的に計測したデータについては、ダッシュボード等による状況の可視化を行うこと。また、リソース利用状況に基づいたリソース見直しを行う点に留意し、情報収集の仕組みについても修正可能とすること。

イ　クラウドサービスのマネージドサービスを効果的に活用し、コスト削減を継続的に図ること。原則としてサーバレスの構成を取ることとするが、仮想マシンインスタンスを利用してサーバを立てる場合は、サーバのスペック等を適切な範囲に調整してコスト削減を継続的に図ること。

ウ　リソース確保の方式（リザーブドインスタンス、スポットインスタンス等）についても検討すること。

(2) データ量

本基盤で想定されるデータ量は、以下に示す。なお、年間データ増加量は仮定をおいた上での試算結果を記載しているため、設計時には改めて運用設計等を考慮の上、必要なデータ量のサイジングを行うこと。

下表の各フェーズの値について、フェーズ内のいずれの時期においてもセル記載内のデータ容量のストレージが設置されているものとする。

表 3-3 データ量の想定（累積）

項番	フェーズ名	ブロックストレージ容量	オブジェクトストレージ（基盤ログ等）容量	オブジェクトストレージ（重要業務データ）容量	データベース用ストレージ容量
1	基盤構築時	39.3TB	104.5TB	5.5TB	4.4TB
2	運用 1 年目	66.6TB	108.9TB	6.1TB	6.8TB
3	運用 2 年目	88.6TB	118.2TB	6.8TB	9.6TB
4	運用 3 年目	162.5TB	160.8TB	9.2TB	30.1TB
5	運用 4 年目	185.5TB	174.5TB	10.5TB	42.6TB
6	運用 5 年目	217.8TB	188TB	12TB	45.0TB

なお、上記フェーズはいずれも 12 カ月とする。ただし、開発環境の設置時期（※3 カ月）は、「基盤構築時」に内包される。

(3) 基盤利用者数

想定される基盤利用者数は、「1.3 業務の規模」を参照のこと。想定基盤利用者数を考慮の上、必要スペックの柔軟なサイジングを行うこと。

(4) 保管データ量・保管期間

本基盤に保管するデータ量については、基盤担当職員と協議の上、決定すること。
なお、各データの保管期間の要件について以下に示す。

ナ　基盤ログ（システムログ）

仮想マシン及びクラウドのマネージドサービスから出力されるログファイルを想定。
オブジェクトストレージにおいて 1 年以上のデータ保管を必須とする。

ニ　基盤ログ（証跡ログ）

仮想マシン及びクラウドのマネージドサービスから出力されるログファイルの内、証跡を想定。
オブジェクトストレージにおいて 5 年以上のデータ保管を必須とする。

ヌ　バックアップデータ

7 世代の世代管理を必須とする。なお、ブロックストレージ容量及びデータベース用ストレージ容量において、全

体の 6 割は国内のバックアップリージョン（想定：大阪等の西日本設置リージョン）にもデータ退避されることを想定すること。

ネ　その他、業務システム担当職員及び業務システム構築・運用事業者が保管を必要とする業務データ

業務システム担当職員及び業務システム構築・運用事業者の求める保管要件に合わせ、提供すること。なお、無制限に大量のデータが格納されることを防止するため、データ保存量に上限を設定し、適切な管理を行うこと。また、オブジェクトストレージ容量（業務データ）については、「表 3-3 データ量の想定（累積）」に「オブジェクトストレージ内重要業務データ容量」として示すデータ量について、国内のバックアップリージョン（想定：大阪等の西日本設置リージョン）へのデータ同期を想定すること。

3.4. 性能に関する事項

本基盤はクラウドサービスを利用するため、クラウドサービスを適切な構成で利用することで、拡張性を確保すること。また、本基盤上の業務システムによる業務処理の特徴を考慮し、業務処理のピーク時においてもレスポンスの低下等を招かないように、十分な処理性能が確保可能なクラウドサービスを用いること。

(1) 性能指標を考慮する対象

本基盤では、本基盤上の業務システムの業務処理に対して設定する性能指標（応答時間やスループット）を考慮する対象は無い。

3.5. 信頼性に関する事項

本基盤に備える機能の停止等による業務への影響を最低限にとどめるため、クラウドサービスの利用を前提として、以下に示す要件を踏まえ本基盤の信頼性を確保すること。

(1) 可用性要件

単一障害点（SPOF）を極力排除するとともに、障害発生時に影響範囲を最小化する手法を検討し、一律ではなく機能又はセグメントの特性に応じた合理的な設計とすること。また、SPOF の発生が避けられない場合においてそれらの稼働状況を管理する仕組みを準備すること。

ア　可用性に係る目標値

可用性に係る目標値を下表に示す。

表 3-4 可用性に係る目標値

項番	指標名	目標値	補足
1	運用時間	開庁日の 8:15~ 17:30	以下に該当する時間を除く。 ・　接続回線の計画停止時間 ・　大規模災害等の天災地変に起因する停止時間 ・　連携する情報システムやクラウドサービス又は通信ネットワークの障害・計画停止・緊急メンテナンス等に起因する停止時間 ・　法定停電対応に係る停止時間 ・　本基盤のメンテナンスによる計画停止時間
2	稼働率	99.5%以上	本基盤における稼働率を以下の計算式により定義する。 稼働率＝年間実稼働時間／年間予定稼働時間 x 100

			当該計算式において、年間実稼働時間は「基盤利用者が本基盤を利用可能な時間の合計」、年間予定稼働時間は「年間稼働時間（開庁日の8:15~17:30）から計画停止時間及び大規模災害による停止・縮退時間を除いた時間の合計」とする。

イ　可用性に係る対策

本基盤の可用性を確保し、前述に示した稼働率を遵守するため、以下に示す要件に基づく対策を行うこと。

- 本基盤を構成するサーバ、ネットワーク機器及びネットワーク経路について、システムの要件に応じて冗長化を行うこと。特にクラウド接続回線において、複数の論理インタフェースを構成し、異なる物理回線・経路でネットワーク冗長化すること。なお、クラウド接続回線は別事業者（庁内 LAN 管理者）での調達を予定しており、回線とクラウドの接続ポイントはデュアルロケーション構成を想定している。
- 本基盤に係る運用・保守上の人的ミスに起因する障害が本基盤の可用性に影響を与える事態を未然に防止するため、「3.17 運用に関する事項」及び「3.18 保守に関する事項」を踏まえ、適切な手順書を整備すること。また、定型的なオペレーションは自動化すること。

(2) 完全性要件

以下に示す要件を踏まえ、本基盤の完全性を確保するための対策を行うこと。

ア　本基盤運用中に障害・トラブル等が発生した際に原因追求が可能となるよう、操作ログやアクセスログ等のシステムログ、例外事象の発生に関するログ等を取得・保管し、必要な時に出力可能とすること。ログの出力に当たっては、ログの出力レベル（ERROR、WARNING、INFO、DEBUG 等）の設定を可能とすること。なお、証跡に係るログの保管期間は 5 年間以上とすること。

3.6. 拡張性に関する事項

(1) 性能及び機能の拡張性

ア　基本方針

本基盤の利用率の増加、データ量の増加等により、利用資源の規模・性能を拡張する必要が生じた場合に備え、可能な限り性能の拡張を柔軟に行えるよう、設計・開発を行うこと。また、将来の制度改正等により機能を拡張する必要が生じた場合に備え、容易に機能追加・変更を行えるよう、設計・開発を行うこと。

イ　マネージドサービスなどの活用

本基盤はクラウドサービスを利用する想定としている。本基盤の構築に当たっては、当該クラウドサービスのマネージドサービスなどを可能な限り活用することにより、処理能力等の動的調整を実現することとし、業務量及び処理能力の拡張性については特段の拡張性要件を定義しない。

ウ　モニタリングと定期的な報告

本基盤の運用に当たっては、定期的な運用報告においてサーバコア数やディスク、メモリ、ネットワークの帯域などの使用状況等を確認すること。またリソースの増加の必要性が見込まれる場合は、リソースの増強の必要性の有無を判断できるような形で基盤担当職員に報告を行うこと。

エ　割り当て変更

業務量の増減に伴い、これらリソースの割り当てを動的に行えるようにし、基盤担当職員の指示に基

づきリソースの割り当てを変更すること。

3.7. **上位互換性に関する事項**

(1) 上位互換性

クラウドサービスの活用を踏まえ、OS、サーバソフトウェアのバージョンアップ又は変更に備え、本基盤を構成すること。

ア　クラウドサービスのバージョンアップ

本基盤の構成にクラウドサービスのマネージドサービスを採用する場合、軽微なバージョンアップについては自動適用を前提とできるか検討すること。大規模なバージョンアップについては、ソフトウェアの影響を事前に精査し、適用を検討すること。

イ　OS 等への依存

原則として、特定バージョンへの依存は避けること。なお、やむを得ず OS、ミドルウェア等の特定バージョンに依存する場合は、その利用を最低限とすること。

ウ　クライアント端末の更新

クライアント端末が更新され、OS や Web ブラウザとして新しいバージョンのものを利用する場合も、業務運営に極力支障が生じないよう計画されたシステム構成とすること。

(2) 業務分担

本基盤を構成する機器・ソフトウェアの更新、バージョンアップの必要性が生じた場合は、各事業者がそれぞれの担当範囲において影響調査、対応策の検討を実施すること。

ア　業務システム構築・運用事業者は、本基盤上の（自担当の）業務システムへの影響調査、対応策の検討を実施する。基盤運用・保守業務受託者は、本基盤の影響調査、対応策の検討を実施すること。

イ　機器・ソフトウェアの更新、バージョンアップの対象が持ち込みソフトウェアの場合は、基盤運用・保守業務受託者が実施する影響調査、対応策の検討を機器賃貸借受託事業者が支援すること。また、問合せについて、機器賃貸借受託事業者に限らず基盤管理者全員が直接実施できること。

3.8. **中立性に関する事項**

(1) オープンな標準的技術又は製品の採用

本基盤を構成するサーバ、ソフトウェア、アプリケーションとして、市場で広く利用されている製品群及びクラウドサービスが提供する標準的なサービスを除き、特定事業者の技術に依存しないオープンな技術仕様に基づくものを選択すること。

ア　データの可搬性の担保

データの可搬性の担保に当たっては、以下の要件を満たすこと。

・　本基盤内のデータ（クラウド環境設定情報等）については、XML や CSV、JSON 等の標準的な形式で取り出すことができるものとすること。

イ　オープンソースソフトウェア（OSS）活用

ソフトウェア又はアプリケーションについてフレームワークを活用する場合は、可能な限りオープンソースソフトウェアとして提供されているフレームワークを選定すること。

ウ　オープンなインタフェースの活用

本基盤を構成するサーバ、ソフトウェア等は、原則として仕様が公開された API 等のインタフェースを選定すること。

3.9. 継続性に関する事項

本基盤の停止等に際しても必要最低限の業務を継続（又は回復）するため、以下に示す要件を踏まえ、本基盤の継続性を確保すること。

(1) 継続性に係る目標値

以下に、機能停止等の原因となる事象の規模に応じて継続性に係る目標値を示す。

ア　予測可能な障害発生時

予測できる障害（一時的な過負荷等）については、あらかじめ業務停止を回避するための対策を講ずること。特に、クラウド接続回線における単一障害発生時は業務停止せずに処理継続可能な構成を取ること。

イ　業務停止を伴う障害発生時

予測困難な事象により業務停止を伴う障害が発生した場合の目標駆けつけ時間、目標復旧レベル（RLO）及び目標復旧時点（RPO）を下表に示す。

表 3-5 継続性に係る目標値（業務停止を伴う障害発生時）

項番	目標駆けつけ時間 ※障害対処開始までの目標時間	目標復旧レベル （RLO）	目標復旧時点 （RPO）
1	2 時間以内	通常どおりのサービスレベルに復旧	1 営業日以内の時点（最新の日次バックアップからの復旧）

(2) 継続性に係る対策

本基盤の継続性要件を実現するために、以下の対策を講じること。

ア　冗長化

クラウド接続回線及び経路について、故障等を検知した際、自動的に予備の通信経路へ切替える等、適切に冗長化を行い、特定の部分の障害による本基盤クラウド部分への接続停止を極力回避するよう、設計時に配慮すること。

イ　災害対策

災害対策の方針として、 本基盤上の、ミッションクリティカルな業務システムをはじめとした重要業務システムは、日本国内の異なるリージョン（想定：大阪リージョン）に仮想マシン及びデータベースインスタンス、業務データのバックアップを実施しておき、災害発災時にはそのバックアップから本番同等の環境を構築できるようにすること。

ウ　アベイラビリティゾーン

仮想リソースが複数台構成の場合、アベイラビリティゾーン（以下「AZ」という）については、マルチ AZ によって複数の AZ をまたいだシステム冗長化を実現し、可用性を高める方針とすること。別途、基盤担当職員から要求があった場合は、その他の AZ 構成も検討すること。

エ　データバックアップ

・　バックアップ対象

データバックアップに当たっては、本基盤の稼働に必要な全データを復旧可能とすることを前提として、外部組織から再入手可能なデータの有無を含め、保全対象を精査し、復旧時に必要となるデータを過不足なく保全対象に含めることができるようにすること。なお、クラウドサービスのマネージドサービスを利用することで自動的にバックアップを取得できる部分はあるが、オペレーションミスやアプリケーションのバグ等に起因するデータ破壊に対しても破壊前の時点まで遡れるように、バックアップの実施方法について配慮すること。

・　バックアップ頻度

仮想マシンやデータベースインスタンスのバックアップ取得間隔は、原則日次とする。

・　保存期間

万一の障害発生に備え本基盤の稼働に必要な全データを復旧可能とするとともに、過去のシステム処理に問題が発生した場合に原因分析を可能とすることを目的として、日次のバックアップについては、7 日分のデータをバックアップとして保持すること。

・　アクセス権限

バックアップしたデータの保管場所にはアクセス権限を付与し、基盤管理者以外がアクセスできないようにすること。また、設計にはランサムウェア対策についても考慮を行うこと。

・　バックアップツール

バックアップ対象、頻度、バックアップデータへのアクセス権限及び保存期間といったバックアップポリシーを一元的に管理できる機能を持った、クラウドサービスプロバイダが提供するバックアップサービスをできるだけ利用すること。

オ　システムバックアップ

クラウドサービスのマネージドサービスにおけるバックアップ機能を有効に活用すること。

なお、仮想マシンインスタンスを利用してサーバを立てる場合のバックアップ方式は、バックアップ＆リストア、コールドスタンバイ、ウォームスタンバイ、マルチサイトの 4 つのディザスタリカバリ方式のうち、バックアップ＆リストアの構成を想定している。また、データ量については、「3.3 システム規模に関する事項　(4) 保管データ量・保管期間」を参照すること。

「表 3-5 継続性に係る目標値（業務停止を伴う障害発生時）」に示す目標駆けつけ時間、RLO、RPO を満たすようにすること。

3.10. 情報セキュリティに関する事項

(1) セキュリティ対応方針

セキュリティ要件を決定するためのシステム特性や特に対処すべきセキュリティリスク、セキュリティ対応方針を下表に示す。

表 3-6 本基盤におけるセキュリティ対応方針

項番	分類	概要
1	原則	・ 「栃木県情報セキュリティポリシー」等本県の情報セキュリティに関する規程等に準拠した情報セキュリティ対策を講ずること。「政府機関等のサイバーセキュリティ対策のための統一基準」及び「総務省ガイドライン」と同様の考え方を取っているので、具体的な対策を講じるに当たっては必要に応じ参照すること。なお、本県の情報セキュリティに関する規程等により難い合理的な理由がある場合には、協議すること。
2	システム特性（概要）	【基盤利用者】 ・ 基盤利用者は業務システム担当職員及び業務システム構築・運用事業者、本県職員を想定している。 【基盤で取り扱う情報】 ・ 本基盤ではログデータ及びシステムバックアップデータを管理する。 ・ 本基盤では直接特定個人情報は取扱われない。ただし、本基盤上の業務システムにおいては、取り扱いが生じる場合がある。 ・ 本基盤では総務省ガイドラインにおける自治体機密性 3A に該当する情報は扱わない。また、機密性 3A に該当する情報を扱う業務システムの基盤利用も想定しない。 【利用環境・ネットワーク構成】 ・ 業務システム担当職員及び業務システム構築・運用事業者は、庁内に設置された運用保守端末、もしくは個別にリモート接続申請をした業務システム構築・運用事業者管理端末を利用し、ブラウザからインターネットを介して本基盤のクラウド管理コンソールにアクセスし、ログインして各種機能を使用する。 ・ 基盤管理者は庁内に設置された運用保守端末、もしくは個別にリモート接続申請をした基盤設計・開発業務受託者管理端末もしくは基盤運用・保守業務受託者管理端末を利用し、ブラウザからインターネットを介して本基盤のクラウド管理コンソールにアクセスし、システム管理を実施する。 ・ 外部システムとの接続については、「2.5. 外部インタフェースに関する事項」に記載。 【その他】 ・ 業務システムには県政や県民に係る機密性の高い情報資産を扱う業務が含まれており、本基盤インフラにはミッションクリティカル（県民の生活の存続に欠かせない重大）な業務システムを安定稼働させるためのインフラとして機能することが求められていることから、可用性に関しても機密性、完全性と同等に高いレベルで担保する必要がある。
3	優先的に対処すべきセキュリティリスク	【優先的に対処すべきセキュリティリスク】 ・ 本基盤に保存されている個人情報が、外部からの不正アクセスで漏洩するリスク。 ・ 管理者アクセスに必要な IP アドレス、ID、パスワードなどの認証情報が漏洩し、想定外のリモート環境から不正アクセスされるリスク。
4	セキュリティ対応方針	【セキュリティ要件のベースライン】 ・ 本基盤においては、セキュリティ要件を過不足なく導出するため、「栃木県情報セキュリティポリシー」をセキュリティベースラインとする。また、NCO（国家サイバー統括室）の提供する情報システムに係る政府調達におけるセキュリティ要件策定マニュアルもセキュリティ技術観点の整理で参考にする。 【優先的に対処すべきセキュリティリスクへの対応方針】 ・ 上記の優先的に対処すべきセキュリティリスクについては、多層防御の観点で発生確率を抑えるとともに、発生時の範囲を極小化するような対策を実施する。 ・ 不正アクセス対策として不正ログイン対策、脆弱性対策を徹底するともに、攻撃やインシデントの兆候を早期検知できるような仕組みを導入する。 【その他セキュリティリスクへの対応方針】 ・ 上記以外のセキュリティリスク（内部不正や人為的ミス等に起因するもの、サプライチェーンに起因するもの等）についても発生時影響は看過できないことから、予防的な対策だけでなく早期検知するための対策を実施し、リスクを低減する。

(2) セキュリティ要件

上記のセキュリティ対応方針に基づき、設計・開発を行うこと。

開発の各工程において、本セキュリティ要件に則ってセキュリティ対策がもれなく実装されていることを検証する方法を定め、要件のトレーサビリティを確保することが求められる。

開発工程以降、セキュリティ対策を具体化する過程でセキュリティ上の懸念が発生した場合は、基盤担当職員と協議の上、必要に応じて追加のセキュリティ対策を検討すること。また、デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」の記載内容（要求事項、実施内容、重要なセキュリティ対策の考え方）に従い、各工程でのセキュリティ対応状況について抜け漏れを確認して是正すること。加えて、デジタル庁「政府情報システムにおける脆弱性診断導入ガイドライン」の 4 付録 A を参考に情報システムの脆弱性が作りこまれないように留意すること。

(3) 情報セキュリティの確保

ア　本調達機器等について、セキュリティを確保するために以下の作業を実施すること。
また、実施した作業内容については履歴（作業日、作業をおこなった機器、作業内容、作業者を含む。）を残すこと。

- 本調達に係る業務を行う業者は、事業者組織全体のセキュリティを確保するとともに、本県から求められた当該業務の実施において情報セキュリティを確保するための体制を整備すること。
- 本調達に係る業務の実施のために本県から提供する本県の安全に関する重要な情報その他当該業務の実施において知り得た本県の安全に関する重要な情報については、情報のライフサイクルの観点から管理方法を定め、その秘密を保持し、また当該業務の目的以外に利用しないこと。
- 本調達機器等における以下の脆弱性対策を実施すること。
  - 本調達に含まれる機器及びソフトウェアの中で脆弱性対策を実施するものを適切に決定すること。
  - 脆弱性対策を行うとした機器及びソフトウェアについて、公表されている脆弱性情報及び公表される脆弱性情報を把握すること。
  - 把握した脆弱性情報について、対処の要否、可否を判断すること。対処したものに関して対処方法、対処しなかったものに関してその理由、代替措置及び影響を納品時に本県に報告すること。
- 本調達に係る業務の遂行において、定期的に情報セキュリティ対策の履行状況を報告するとともに情報セキュリティが侵害され又はその恐れがある場合には、直ちに本県に報告すること。

3.11. 情報システム稼働環境に関する事項

クラウドサービスの構成、ハードウェアの構成、ソフトウェア製品の構成、ネットワークの構成、施設・設備要件等について記載する。

(1) システム構成

設計・開発及び運用・保守に用いる環境としてクラウドサービス上に構築する「本番環境」、「開発環境」の 2 種類を準備すること。

環境の構成や利用方法の詳細は、基盤担当職員と協議の上決定すること。

ア　本番環境

「図 1-1　システム全体構成図」に記載のとおり、本番環境はクラウド環境とオンプレ環境を準備すること。なお、運用終年度（≒次々期システム稼働時）には、本基盤上の各業務システムをクラウド移行することが完了し、フルクラウドとなることを想定している。

イ　開発環境

基盤導入フェーズにおいて本基盤上の各業務システムがクラウド移行する際に、本番環境の利用よりも先行して事前検証を行える開発環境をクラウド環境内に整備すること。なお、開発環境については本基盤の構築期間中のうち 3 か月間維持を想定し、本基盤上の業務システムの利用完了後に撤去すること。また、開発環境のサーバについては、検証で利用しない場合はサーバを停止する運用を実施し、コスト適正化を図ること。

(2) クラウドサービス構成

ア　クラウドサービスの要件

クラウドサービスの要件については、「3.2.システム方式に関する事項」の「（1）システム方式についての全体方針」、「（2）クラウドサービスの選定、利用に関する要件」を参照すること。また、クラウドサービスの仕様変更及びサポート終了に関する通知を基盤管理者及び基盤利用者が事前に受領できる仕組みを用意すること。

イ　クラウド環境に構築するサーバ（IaaS）の要件

本基盤上の業務システムのサーバの内、クラウド環境に構築が必要なサーバの要件については、「別添 2　クラウド環境に構築するサーバ（IaaS・PaaS）の要件【秘密】」を参照すること。

(3) オンプレミス環境のハードウェア要件

オンプレミス環境のハードウェア要件を以下に示す。なお、特定の装置への依存により、将来的な情報システムの拡張及び更新や事業者間での引継ぎが妨げられることがないよう十分に配慮すること。
オンプレミス環境と県庁コアスイッチ、既存システムスイッチと接続すること。
次期基盤システムのイメージを「図 3-1　次期基盤システムのイメージ」に示す。

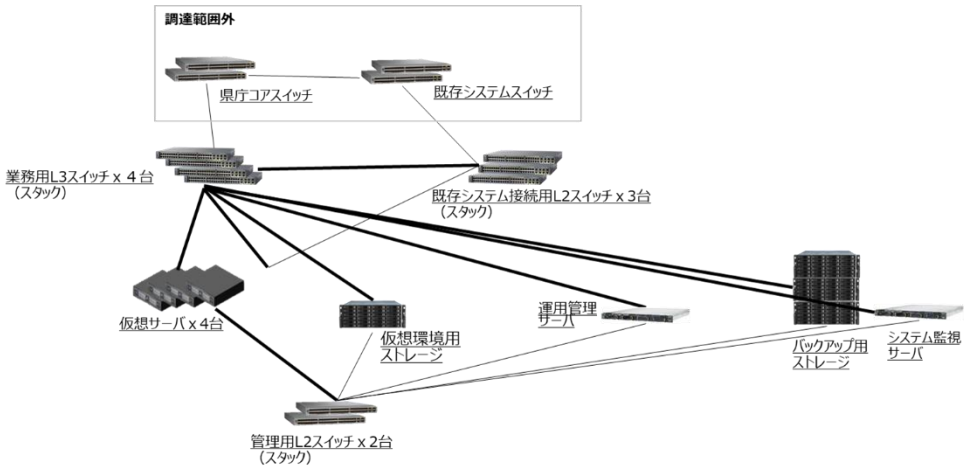

図 3-1　次期基盤システムのイメージ

ア　ハードウェア共通要件

- 本調達機器等は、新品であること。
- 賃貸借の期間中は保守部品の供給が行われること。

・ 本調達機器等は、運用環境を考慮して、可能な限り最新の技術を採用すること。
・ 本調達機器等は、可能な限り省スペース設計、省電力設計であること。
・ 本調達機器等は、製品の動作が保証又は確認されたものであること。
・ 本調達機器等において納入期限までに発見された本調達機器等の不具合については、基盤設計・開発業務受託者の責任と負担で迅速に対応すること。
・ 各ハードウェアに搭載される OS 及び基本的なソフトウェアについて、納入期限までに指摘されている脆弱性や修正ファームアップ等の有無を確認し、これを本県に報告し、本県と協議の上、納入期限までに適切な対策処理を行うこと。
・ 各種災害（地震等）対策等を十分考慮し、安全かつ信頼性のある機器等を納品すること。
・ 将来におけるハードウェア、ソフトウェアの増強・ネットワークの拡大・接続機器の増設及び拡張を想定し、互換性・移植性・接続性を確保でき柔軟に対応できるよう考慮されていること。
・ 本調達機器等は、機械的及び電気的に人体に危険がないものであること。
・ 本調達機器等は、特に定めのないものは、日本産業規格（JIS）又はそれと同等の規格に適合する品質優良なものを使用すること。
・ 本調達機器等は、5 年間、24 時間 365 日の運用に耐えうる機器であること。

イ 仮想サーバ

仮想サーバは PRIMERGY RX2530 M8 同等品以上であること。

仮想サーバ機器メーカー及び VMware メーカー（Broadcom 社）にて VMware Cloud Foundation 9 系の動作確認が行われている製品であること。

・ 形状
  - ラックマウント型（1U 以下）であること。
・ CPU
  - Intel Xeon 6747P プロセッサー（2.70GHz、48 コア、288MB）×2 以上を有すること。
・ メモリ
  - 1536GB 以上（64GB 6400 RDIMM×24 枚以上）を有すること。
  - メモリモジュールを最大 32 枚搭載可能であること。
  - 1bit のメモリエラーを同時に 4 か所まで訂正可能であること。
  - メモリスロットにメモリモジュールの搭載順序がわかるしくみを有すること。
  - 8TB 以上のメモリを搭載可能であること。
  - メモリミラーリング機能に対応していること。
・ OS ブート専用モジュール
  - システムボード上に OS の起動を高速化するモジュール（M.2 Flash モジュール）を搭載可能であること。
  - VMware ハイパーバイザ用の M.2 Flash モジュールを搭載すること。
  - M.2 Flash モジュールは冗長化構成とすること。
・ USB インタフェース
  - USB3.2 Gen1x1 準拠 4 ポート以上を有すること。
・ LAN インタフェース
  - 10GBASE-T×10 以上を有すること。
  - 1 枚の LAN カードではなく、複数の LAN カードで実装すること。
  - 1000BASE-T×1 以上を有すること。
  - リモート管理用専用 LAN ポート× 1 以上を有すること。
  - サーバ本体に、オンボード LAN ポートの転送速度を表示する機能を有すること。

- LAN ポートを最大 20 ポート以上搭載可能であること。
- 10Gbps の LAN ポートを 20 ポート以上搭載可能であること。
- 100Gbps の LAN ポートを搭載可能であること。
- オンボード LAN ポートのポート数を増設する機能を有すること。

・ PCI スロット
- 拡張バススロット数×5 以上を有すること。
- 上記のうち、PCI Express 5.0（×16 レーン）×3 スロット以上を有すること。

・ 電源ユニット
- 2200W 電源×2（冗長構成）を有すること。
- 80PLUS Platinum 認証以上を取得した電源ユニットを搭載できること。
- 200V 電源ケーブル×2 を用意すること。
- 活性交換（ホットプラグ）に対応していること。

・ ファン
- 活性交換（ホットプラグ）に対応していること。

・ サーバ管理
- OS の稼働状態に関わらずサーバ本体のリモート管理が行えるリモートプロセッサを内蔵すること。
- リモート管理モジュールの設定変更の際は認証をおこなうこと。

・ 保守
- 借入期間中、24 時間 365 日当日訪問修理が受けられること。
- 仮想サーバ及び仮想サーバ上で稼働する仮想マシンのオペレーティングシステムについて、借入期間中 24 時間 365 日サポートが受けられること。

・ 消費電力
- 最大消費電力（カタログ記載）：2894W（200V 時）以下であること。
- 電力監視、消費電力上限値設定が可能なこと。

・ 安全対策
- 電源ケーブル抜け防止の仕組みが提供されていること。
- 本体に NMI ボタン、リセットボタンを有していること。

・ 故障通知等
- システムボード上にモジュールやコンポーネントの異常・故障を通知する LED があること。（通電されていない状態でも通知が可能であること）
- 故障した DIMM を、システムボード上の DIMM スロットの LED 点灯で特定できること。
- システムボード上で、故障したファン・PCI カード・SAS アレイコントローラカード等の LED 通知が可能であること。
- 外面で CPU、メモリ、ファンの故障予兆を通知可能であること。

・ その他
- 動作時の騒音（カタログ記載）：77db 以下であること。
- 本体重量が ラックレールを含んだ状態で 23.8kg を超えないこと。

・ 必要台数
- 4 台用意すること。

ウ　運用管理サーバ

運用管理サーバは PRIMERGY RX2530 M8 同等品以上であること。

・ 形状
- ラックマウント型（1U 以下）であること。

- OS
  - Windows Server 2022 Standard 以上を搭載すること。
- CPU
  - Intel Xeon 6507P プロセッサー（3.50GHz、 8 コア、48MB）×1 以上を有すること。
- メモリ
  - 64GB 以上（16GB 6400 RDIMM×4 枚以上）を有すること。
  - メモリモジュールを最大 32 枚搭載可能であること。
  - 1bit のメモリエラーを同時に 4 か所まで訂正可能であること。
  - メモリスロットにメモリモジュールの搭載順序がわかるしくみを有すること。
  - 4TB 以上のメモリを搭載可能であること。
  - メモリミラーリング機能に対応していること。
- 内蔵 HDD
  - 960GB（2.5 インチ,SATA SSD）×4 以上を搭載すること。
  - RAID 構成：RAID5+hotspare で構成すること。
  - 2.5 インチ SSD を最大 8 本搭載可能であること。
- OS ブート専用モジュール
  - システムボード上に OS の起動を高速化するモジュール（M.2 Flash モジュール）が搭載可能であること。
- 光学ドライブ
  - 内蔵 DVD-ROM ユニット×1 を搭載すること。
- USB インタフェース
  - USB3.2 Gen1x1 準拠 4 ポート以上を有すること。
- LAN インタフェース
  - 10GBASE-T×2 以上を有すること。
  - 1000BASE-T×4 以上を有すること。
  - リモート管理用専用 LAN ポート× 1 以上を有すること。
  - サーバ本体に、オンボード LAN ポートの転送速度を表示する機能を有すること。
  - LAN ポートを最大 20 ポート以上搭載可能であること。
  - 10Gbps の LAN ポートを 20 ポート以上搭載可能であること。
  - 100Gbps の LAN ポートを搭載可能であること。
  - オンボード LAN ポートのポート数を増設する機能を有すること。
- PCI スロット
  - 拡張バススロット数×5 以上を有すること。
  - 上記のうち、PCI Express 5.0（×16 レーン）×3 スロット以上を有すること。
- 電源ユニット
  - 900W 電源×2（冗長構成）を有すること。
  - 80PLUS Platinum 認証以上を取得した電源ユニットを搭載できること。
  - 100V 電源ケーブル×2 を用意すること。
  - 活性交換（ホットプラグ）に対応していること。
- ファン
  - 活性交換（ホットプラグ）に対応していること。
- サーバ管理
  - OS の稼働状態に関わらずサーバ本体のリモート管理が行えるリモートプロセッサを内蔵すること。
  - リモート管理モジュールの設定変更の際は認証をおこなうこと。

・ 保守
  - 借入期間中、24 時間 365 日当日訪問修理が受けられること。
  - オペレーティングシステムについて、借入期間中 24 時間 365 日サポートが受けられること。
・ 消費電力
  - 最大消費電力（カタログ記載）：2894W（200V 時）以下であること。
  - 電力監視、消費電力上限値設定が可能なこと。
・ 安全対策
  - 電源ケーブル抜け防止の仕組みが提供されていること。
  - 本体に NMI ボタン、リセットボタンを有していること。
・ 故障通知等
  - システムボード上にモジュールやコンポーネントの異常・故障を通知する LED があること。（通電されていない状態でも通知が可能であること）
  - 故障した DIMM を、システムボード上の DIMM スロットの LED 点灯で特定できること。
  - システムボード上で、故障したファン・PCI カード・SAS アレイコントローラカード等の LED 通知が可能であること。
  - 外面で CPU、メモリ、ファンの故障予兆を通知可能であること。
・ その他
  - 動作時の騒音（カタログ記載）：77db 以下であること。
  - 本体重量が ラックレールを含んだ状態で 23.8kg を超えないこと。
・ 必要台数
  - 1 台用意すること。

エ　システム監視サーバ

システム監視サーバは PRIMERGY RX2530 M8 同等品以上であること。

・ 形状
  - ラックマウント型（1U 以下）であること。
・ OS
  - Red Hat Enterprise Linux 9 以上を搭載すること。
・ CPU
  - Intel Xeon 6507P プロセッサー（3.50GHz、 8 コア、48MB）×1 以上を有すること。
・ メモリ
  - 32GB 以上（32GB 6400 RDIMM×1 枚以上）を有すること。
  - メモリモジュールを最大 32 枚搭載可能であること。
  - 1bit のメモリエラーを同時に 4 か所まで訂正可能であること。
  - メモリスロットにメモリモジュールの搭載順序がわかるしくみを有すること。
  - 4TB 以上のメモリを搭載可能であること。
  - メモリミラーリング機能に対応していること。
・ 内蔵 HDD
  - 960GB（2.5 インチ,SATA SSD）×4 以上を搭載すること。
  - RAID 構成：RAID5+hotspare で構成すること。
  - 2.5 インチ SSD を最大 8 本搭載可能であること。
・ OS ブート専用モジュール
  - システムボード上に OS の起動を高速化するモジュール（M.2 Flash モジュール）が搭載可能であること。

- 光学ドライブ
  - 内蔵 DVD-ROM ユニット×1 を搭載すること。
- USB インタフェース
  - USB3.2 Gen1x1 準拠 4 ポート以上を有すること。
- LAN インタフェース
  - 10GBASE-T×2 以上を有すること。
  - 1000BASE-T×4 以上を有すること。
  - リモート管理用専用 LAN ポート× 1 以上を有すること。
  - サーバ本体に、オンボード LAN ポートの転送速度を表示する機能を有すること。
  - LAN ポートを最大 20 ポート以上搭載可能であること。
  - 10Gbps の LAN ポートを 20 ポート以上搭載可能であること。
  - 100Gbps の LAN ポートを搭載可能であること。
  - オンボード LAN ポートのポート数を増設する機能を有すること。
- PCI スロット
  - 拡張バススロット数×5 以上を有すること。
  - 上記のうち、PCI Express 5.0（×16 レーン）×3 スロット以上を有すること。
- 電源ユニット
  - 900W 電源×2（冗長構成）を有すること。
  - 80PLUS Platinum 認証以上を取得した電源ユニットを搭載できること。
  - 100V 電源ケーブル×2 を用意すること。
  - 活性交換（ホットプラグ）に対応していること。
- ファン
  - 活性交換（ホットプラグ）に対応していること。
- サーバ管理
  - OS の稼働状態に関わらずサーバ本体のリモート管理が行えるリモートプロセッサを内蔵すること。
  - リモート管理モジュールの設定変更の際は認証をおこなうこと。
- 保守
  - 借入期間中、24 時間 365 日当日訪問修理が受けられること。
  - オペレーティングシステムについて、借入期間中 24 時間 365 日サポートが受けられること。
- 消費電力
  - 最大消費電力（カタログ記載）：2894W（200V 時）以下であること。
  - 電力監視、消費電力上限値設定が可能なこと。
- 安全対策
  - 電源ケーブル抜け防止の仕組みが提供されていること。
  - 本体に NMI ボタン、リセットボタンを有していること。
- 故障通知等
  - システムボード上にモジュールやコンポーネントの異常・故障を通知する LED があること。（通電されていない状態でも通知が可能であること）
  - 故障した DIMM を、システムボード上の DIMM スロットの LED 点灯で特定できること。
  - システムボード上で、故障したファン・PCI カード・SAS アレイコントローラカード等の LED 通知が可能であること。
  - 外面で CPU、メモリ、ファンの故障予兆を通知可能であること。
- その他
  - 動作時の騒音（カタログ記載）：77db 以下であること。

- 本体重量が ラックレールを含んだ状態で 23.8kg を超えないこと。

・ 必要台数
- 1 台用意すること。

オ 仮想環境用ストレージ

仮想環境用ストレージは ETERNUS AX2300 同等品以上であること。

・ 形状
- 本県の指定する 19 インチラックに搭載できること。
- 2U 以内であること。

・ 機能
- 仮想サーバのデータストア領域として使用できること。
- VMWare vSphere と連携できること。
- SnapShot、SnapMirror 機能を有すること。
- Snapshot 機能においては 1023 世代まで維持管理を可能とし、更新データは差分情報のみでの管理が可能であること。
- SnapShot 領域がオンラインで拡張、縮小可能であること。
- 筐体内での世代管理（SnapShot）イメージに対して、書き込み処理が行えること。
- 別の専用装置などを必要とせず、重複排除（De-duplication） 圧縮（Compression）集約（Compaction）の機能を有すること。
- 重複排除機能は効率性を重視して、ブロック単位での重複を排除する機能を有すること。
- 必要に応じてボリューム容量を動的に増減可能なこと。
- シン・プロビジョニングを実現可能であること。
- NFS、CIFS、iSCSI、FC、NVMe/FC をサポートすること。
- システムを稼働させたまま、障害が発生したディスクドライブの交換を行えること。

・ コントローラ
- 2 基搭載（冗長化構成）すること。
- 冗長化された 2 つのコントローラは、それぞれが並列にストレージ処理を提供可能であること。

・ ディスク構成
- 15.3TB（2.5 インチ NVMeSSD）×18 本以上搭載すること。
- 以下の RAID レベルをサポートすること。
  RAID-TEC、RAID6（RAID-DP）、RAID4
- SnapShot 領域を除く実効容量が 188TB 以上となるように構成すること。

・ インタフェース
- デュアルコントローラ構成にて以下のインタフェースを有すること。
  Ethernet（25Gbit/s、10Gbit/s）：16 ポート以上
  Ethernet 10G Base-T（10Gbit/s）：8 ポート以上

・ メモリ容量
- 128GB 以上のメモリ容量を有すること。

・ ドライブ数
- 最大 72 本のディスクドライブを搭載可能であること。

・ 管理
- 日本語の GUI を有すること。
- GUI と同等の操作ができる CLI を有すること。
- 運用中のファームアップデートが可能なこと。

- 装置へのアクセス情報を Syslog で転送できること。
- ドライブの故障兆候を検出し、自動的にリビルドする機能を有すること。
- 装置耐用年数（5 年）内の定期交換部品交換が不要なこと。

・ その他
- 日本語のマニュアルを納品すること。

・ 保守
- 借入期間中、24 時間 365 日当日訪問修理が受けられること。

・ 消費電力
- コントローラシェルフの最大消費電力が、1,303W [1,320VA]以下であること。
- ストレージシェルフの最大消費電力が、934W [946VA]以下であること。

・ 必要台数
- 1 台用意すること。

カ　バックアップ用ストレージ

仮想環境用ストレージは ETERNUS HX2300 同等品以上であること。

・ 形状
- 本県の指定する 19 インチラックに搭載できること。
- 4U 以内であること。

・ 機能
- 仮想サーバのデータストア領域として使用できること。
- VMWare vSphere と連携できること。
- SnapShot、SnapMirror 機能を有すること。
- Snapshot 機能においては 1023 世代まで維持管理を可能とし、更新データは差分情報のみでの管理が可能であること。
- SnapShot 領域がオンラインで拡張、縮小可能であること。
- 筐体内での世代管理（SnapShot）イメージに対して、書き込み処理が行えること。
- 別の専用装置などを必要とせず、重複排除（De-duplication） 圧縮（Compression）集約（Compaction）の機能を有すること。
- 重複排除機能は効率性を重視して、ブロック単位での重複を排除する機能を有すること。
- 必要に応じてボリューム容量を動的に増減可能なこと。
- シン・プロビジョニングを実現可能であること。
- NFS、CIFS、iSCSI、FC、NVMe/FC をサポートすること。
- システムを稼働させたまま、障害が発生したディスクドライブの交換を行えること。

・ コントローラーシェルフ、ドライブシェルフ
- 各 1 台以内で構成すること

・ コントローラ
- 2 基搭載（冗長化構成）すること。
- 冗長化された 2 つのコントローラは、それぞれが並列にストレージ処理を提供可能であること。

・ ディスク構成
- 22TB（3.5 インチ NL-SAS HDD）×24 本以上搭載すること。
- 増設時は、SSD/SAS/NL-SAS からディスクを選択できる、かつ同一シェルフ内に混在させられること。
- 以下の RAID レベルをサポートすること。
  RAID-TEC、RAID6（RAID-DP）、RAID4

- 実効容量が 282TB 以上となるように構成すること。

・ インタフェース
- デュアルコントローラ構成にて以下のインタフェースを有すること。
- Ethernet（25Gbit/s、10Gbit/s）：4 ポート以上

・ メモリ容量
- 128GB 以上のメモリ容量を有すること。

・ ドライブ数
- 最大 144 本のディスクドライブを搭載可能であること。

・ 管理
- 日本語の GUI を有すること。
- GUI と同等の操作ができる CLI を有すること。
- 運用中のファームアップデートが可能なこと。
- 装置へのアクセス情報を Syslog で転送できること。
- ドライブの故障兆候を検出し、自動的にリビルドする機能を有すること。
- 装置耐用年数（5 年）内の定期交換部品交換が不要なこと。

・ その他
- 日本語のマニュアルを納品すること。

・ 保守
- 借入期間中、24 時間 365 日当日訪問修理が受けられること。

・ 消費電力
- コントローラシェルフの最大消費電力が、729W [740VA]以下であること。
- ドライブシェルフの最大消費電力が、346W [354VA]以下であること。

・ 必要台数
- 1 台用意すること。

キ　業務用 L3 スイッチ

業務用 L3 スイッチは Catalyst 9300X-24HX 同等品以上であること。

・ 形状
- ラックマウント型（1U 以下）であること。

・ スタック
- 業務用 L3 スイッチ同士をスタック接続すること。

・ インタフェース
- 10G マルチギガビット×24 ポート以上を有すること。
- 25G イーサネット×8 ポート以上を有すること。
- 業務用 L3 スイッチ全体で下記の SFP+/SFP28 モジュールを用意すること。
  SFP+モジュール　10GBase-SR：14 以上
  SFP28 モジュール　10/25GBase-CSR：12 以上

・ スイッチング容量
- スタック接続時 800Gbps 以上の性能を有すること。

・ 転送レート
- 654.72Mpps 以上の性能を有すること。

・ 電源
- 2 基搭載可能であること。

・ ファン

- 冗長化されていること。

・ エアフロー
- ラック全体のエアフローを考慮し、サーバ同様に前面吸気、背面排気であること。

・ 外形寸法
- W×D×H（mm）:445×446×44（mm）以下であること。

・ 重量
- 標準搭載時の重量が 6.25kg 以下であること。

・ その他基本機能
- レイヤ 2、ルーテッドアクセス（RIP、EIGRP スタブ、OSPF - 1,000 ルート）、PBR、PIM スタブマルチキャスト（1,000 ルート）、PVLAN、VRRP、CDP、QoS、FHS、802.1x、MACsec-128、CoPP、SXP、IP SLA レスポンダ、SSO を有すること。
- NETCONF、RESTCONF、gRPC、YANG、PnP Agent、ZTP/Open PnP、GuestShell（On-Box Python）を有すること。
- モデル駆動型テレメトリ、サンプル NetFlow、SPAN、RSPAN を有すること。

・ 最大消費電力
- 180W 以下であること。

・ 保守
- 借入期間中、24 時間 365 日オンサイト保守が受けられること。

・ 必要台数
- 4 台用意すること。

ク 管理用 L2 スイッチ

管理用 L2 スイッチは Catalyst 9200L-24PXG-2Y 同等品以上であること。

・ 形状
- ラックマウント型（1U 以下）であること。

・ スタック
- 管理用 L2 スイッチ同士をスタック接続すること。

・ インタフェース
- 10G マルチギガビット×8 ポート以上を有すること。
- 1GB イーサネット×16 ポート以上を有すること。
- 25GB 固定アップリンク×2 ポート以上を有すること。

・ スイッチング容量
- 292Gbps 以上の性能を有すること。

・ 転送レート
- 229.16Mpps 以上の性能を有すること。

・ 電源
- 2 基搭載可能であること。

・ ファン
- 冗長化されていること。

・ エアフロー
- ラック全体のエアフローを考慮し、サーバ同様に前面吸気、背面排気であること。

・ 外形寸法
- W×D×H（mm）:445×350×44（mm）以下であること。

・ 重量

- 標準搭載時の重量が 5.44kg 以下であること。

・ その他基本機能
- レイヤ 2、スタティックルーティング、ルーテッドアクセス（RIP、EIGRP スタブ、OSPF - 1,000 ルート）、PBR、PIM スタブマルチキャスト（1,000 ルート）、PVLAN、VRRP、CDP、QoS、FHS、802.1x、MACsec-128、CoPP、SXP、IP SLA レスポンダ、SSO を有すること。
- NETCONF、RESTCONF、YANG、PnP エージェント、PnP を有すること。
- モデル駆動型テレメトリ、サンプル NetFlow、SPAN、RSPAN を有すること。

・ 最大消費電力
- 90W 以下であること。

・ 保守
- 借入期間中、24 時間 365 日オンサイト保守が受けられること。

・ 必要台数
- 2 台用意すること。

ケ 既存システム接続用 L2 スイッチ

既存システム接続用 L2 スイッチは Catalyst 9300L-48T-4X 同等品以上であること。

・ 形状
- ラックマウント型（1U 以下）であること。

・ スタック
- 既存システム接続用 L2 スイッチ同士をスタック接続すること。

・ インタフェース
- 10/100/1000Base-T×48 ポート及び SFP/SFP+×4 ポート以上を有すること。
- 既存システム接続用 L2 スイッチ全体で下記の SFP+モジュールを用意すること。
  SFP+モジュール 10GBase-SR：4 以上

・ スイッチング容量
- 176Gbps 以上の性能を有すること。

・ 転送レート
- 130.95Mpps 以上の性能を有すること。

・ 電源
- 2 基搭載可能であること。

・ ファン
- 冗長化されていること。

・ エアフロー
- ラック全体のエアフローを考慮し、サーバ同様に前面吸気、背面排気であること。

・ 外形寸法
- W×D×H（mm）:445×449×44（mm）以下であること。

・ 重量
- 標準搭載時の重量が 7kg 以下であること。

・ その他基本機能
- レイヤ 2、ルーテッドアクセス（RIP、EIGRP スタブ、OSPF - 1,000 ルート）、PBR、PIM スタブマルチキャスト（1,000 ルート）、PVLAN、VRRP、CDP、QoS、FHS、802.1x、MACsec-128、CoPP、SXP、IP SLA レスポンダ、SSO を有すること。
- NETCONF、RESTCONF、gRPC、YANG、PnP Agent、ZTP/Open PnP、GuestShell

（On-Box Python）を有すること。
- モデル駆動型テレメトリ、サンプル NetFlow、SPAN、RSPAN を有すること。

・ 最大消費電力
- 110W 以下であること。

・ 保守
- 借入期間中、24 時間 365 日オンサイト保守が受けられること。

・ 必要台数
- 3 台用意すること。

コ 管理用ハブ

管理用ハブは SH1516ATE スイッチングハブ同等品以上であること。

・ 形状
- ラックマウント型（1U 以下）であること。

・ インタフェース
- 10/100/1000Base-T×16 ポート上を有すること。
- Auto MDI/MDI-X に対応していること。

・ スイッチング容量
- 32Gbps 以上の性能を有すること。

・ 電源
- AC100V であること。

・ 外形寸法
- W×D×H（mm）：266×162×43.5（mm）（突起物を除く）以下であること。

・ 重量
- 1.7kg 以下であること。

・ その他機能
- 電源ケーブル抜け防止の仕組みを有すること。

・ 最大消費電力
- 12W 以下であること。

・ 保守
- 借入期間中、24 時間 365 日オンサイト保守が受けられること。

・ 必要台数
- 6 台用意すること。

サ 運用保守端末

運用保守端末は LIFEBOOK A5513/R 同等品以上であること。

・ 形状
- ノートブック型であること。

・ 液晶
- 液晶画面は 15.6 型フル HD であること。

・ OS
- Windows 11 Pro 64bit を搭載すること。

・ CPU
- インテル Corei5-1345U プロセッサー相当以上であること。

・ メモリ

- 16GB 以上であること。

・ ディスク
- 暗号化機能付フラッシュメモリ（DRAM-less SSD/PCIe NVMe）256GB 以上であること。

・ 光学ドライブ
- 内蔵 DVD-ROM ユニットを搭載すること。

・ マウス
- 光学式マウスを添付すること。

・ 媒体
- OS・ドライバのリカバリ媒体を提供すること。

・ ビジネスソフトウェア
- Microsoft Office LTSC Standard 2024 を 7 台分提供すること。

・ 保守
- 借入期間中、24 時間 365 日オンサイト保守が受けられること。

・ 環境
- 国際エネルギースタープログラム対応製品であること。
- エコマークを取得していること。

・ 必要台数
- 13 台用意すること。

シ　管理用プリンタ

管理用プリンタは XL-9460 同等品以上であること。

・ 基本仕様
- A3 両面対応モノクロレーザープリンタであること。

・ 印刷速度
- 46ppm 以上であること（A4 片面印刷時）。

・ ウォームアップタイム
- 16 秒以下であること。

・ 対応用紙サイズ
- A3、A4 に対応していること。

・ 用紙種類
- 普通紙、再生紙が利用可能であること。

・ 給紙カセット容量・個数
- 550 枚×2 個以上であること。

・ ネットワーク
- 100BASE-TX あるいは 1000BASE-T を 1 ポート以上有すること。

・ 電源
- AC100V で利用可能なこと。

・ 消費電力
- 最大消費電力：1320W 以下であること。
- スリープモード時：0.35W 以下であること。

・ プリンタドライバ
- Windows11 で利用可能なこと。

・ 外形寸法
- 寸法（幅×奥行×高さ）：499×388[518]×320 以下であること。

［］：突起物及びカセット延長時。

・ 保守
  - 借入期間中、24 時間 365 日オンサイト保守が受けられること。
・ 環境
  - 国際エネルギースタープログラム対応製品であること。
・ 必要台数
  - 1 台用意すること。

ス 無停電電源装置（運用管理サーバ、システム監視サーバ、ネットワーク機器用 UPS）

無停電電源装置（運用管理サーバ、システム監視サーバ、ネットワーク機器用 UPS）は高機能無停電電源装置（Smart-UPS SMX 3000RMJ）同等品以上であること。

・ 停電時の保持時間
  - 10 分以上保持すること。
・ 定格容量
  - 2400VA/2400W の容量以上を有すること。
・ 出力コンセント
  - NEMA 5-15R×7 の形状のコンセントを有すること。
  - 必要に応じてコンセントボックス等でコンセント数を増やすこと。
・ LAN ポート
  - LAN ポート×1 以上を有し、電源管理用ソフトウェアと連携してネットワーク経由での電源管理が可能であること。
・ 保守
  - 借入期間中、24 時間 365 日オンサイト保守が受けられること。
・ 必要台数
  - 4 台以内で用意すること。

セ 無停電電源装置（仮想サーバ、ストレージ用 UPS）

無停電電源装置（ストレージ用 UPS）は高機能無停電電源装置（Smart-UPS RT 5000）同等品以上であること。

・ 停電時の保持時間
  - 10 分以上保持すること。
・ 定格容量
  - 5200VA/4600W の容量以上を有すること。
・ 出力コンセント
  - NEMA L6-20R×2、L6-30R×2 の形状のコンセントを有すること。
  - 必要に応じてコンセントボックス等でコンセント数を増やすこと。
・ LAN ポート
  - LAN ポート×1 以上を有し、電源管理用ソフトウェアと連携してネットワーク経由での電源管理が可能であること。
・ 保守
  - 借入期間中、24 時間 365 日オンサイト保守が受けられること。
・ 必要台数
  - 6 台以内で用意すること。

ソ ラック周辺機器

・ ディスプレイ
  - 19 インチラックに搭載可能で 17 インチ以上の画面を有すること。
  - 収納時は 1U の占有とすること。
  - 電源ケーブルを付属すること。
  - 1 台用意すること。
・ KVM スイッチ
  - KVM スイッチのポートは 16 ポート以上有すること
  - 電源ケーブルを付属すること。
  - ディスプレイと同じラック位置に取り付けすること。
  - 1 台用意すること。
・ KVM ケーブル
  - KVM ケーブルは USB とすること。
  - 6 本用意すること。

タ　ポータブル HDD

ポータブル HDD は HD-PGAC1U3-BA 同等品以上であること。

・ ディスク容量
  - 1TB 以上とすること。
・ 必要台数
  - 1 台用意すること。

チ　積層信号灯

積層信号灯は NHB4-3-RYG 同等品以上であること。

・ LED ユニット色
  - 赤、黄、緑の 3 色とすること。
・ インタフェース
  - Ethernet（RJ-45）を 1 ポート有すること。
・ ネットワークプロトコル
  - HTTP、HTTPS、SSH、RSH に対応すること。
・ 音圧
  - ブザーの音圧は 80dB とすること。
・ 電源
  - AC アダプタを付属すること。
・ 保守
  - 借入期間中、先出しセンドバックが受けられること。
・ 必要台数
  - 1 台用意すること。

(4) ソフトウェア構成

本基盤の構築に当たっては、可能な限りクラウドサービス提供のサービスを活用すること。また、いずれのソフトウェアについても原則として最新バージョンを適用とし、製品ライセンス及び製品問合せのサポートは構築期間から準備すること。なお、ソフトウェアサポートの維持（いわゆるモダンライサイクルポリシー）のために必要となる、ソフトウェアのバージョンアップについては構築期間・運用期間中問わずバージョンアップを実施する計画を基盤設計・開発業務受託者にて立案し、基盤運用・保守業務受託者への引継ぎまで実施すること。
本基盤で調達必須とするソフトウェアを下表に示す。

ただし、下表の項番 29、30 の IPCOM については同等品以上の製品の代替調達も可とする。

なお、下表記載物以外にソフトウェアの個別調達が必要な場合においては、特定のソフトウェアへの依存により将来的な情報システムの拡張及び更新や事業者間での引継ぎが妨げられることがないよう十分に配慮すること。

表 3-7 ソフトウェア一覧

項番	ソフトウェア名	必要数量	補足
1	VMware Cloud Foundation（384 ライセンス×5 年）	1 式 （1920 ライセンス）	サポート保守を含めること
2	VMware Cloud Foundation（384 ライセンス×1 年）	1 式 （384 ライセンス）	サポート保守を含めること
3	VMware vDefend（384 ライセンス×5 年）	1 式 （1920 ライセンス）	サポート保守を含めること
4	VMware vDefend（384 ライセンス×1 年）	1 式 （384 ライセンス）	サポート保守を含めること
5	PSO クレジット	1 式	
6	Windows Server 2025 Datacenter（16 コア） バンドル	4 ライセンス	仮想マシン用 サポート保守を含めること
7	Windows Server 2025 Datacenter Additional License（16 コア）	20 ライセンス	仮想マシン用 サポート保守を含めること
8	Single Language ガバメント OV 一括 初年度 Win Server Datacenter Core 16Licenses SA ※3 年	24 ライセンス	仮想マシン用
9	Single Language ガバメント OV 一括 初年度 Win Server Datacenter Core 16Licenses SA ※更新 3 年分	24 ライセンス	仮想マシン用 サポート保守を含めること
10	Windows Server 2025 Standard（16 コア） ダウングレードサービス付き Windows Server 2022 Standard インストール	1 ライセンス	運用管理サーバ用 サポート保守を含めること
11	RHEL VDC [PG 2CPU/ゲスト無制限（ゲスト専用）] 2CPU	4 ライセンス	仮想マシン用 サポート保守を含めること 構築期間のライセンスも含めること
12	RHEL VDC [PG 2CPU/1 ゲスト]	1 ライセンス	システム監視サーバ用 サポート保守を含めること
13	Oracle Database Standard Edition 2 1 Processor License	8 ライセンス	仮想マシン用 サポート保守を含めること 構築期間のライセンスも含めること
14	Trend Vision One Endpoint Security Pro	400 ライセンス	クラウド及びオンプレミス環境に設置されたサーバ（仮想マシン）用 構築期間のライセンスも含めること 製品サポートについてもライセンスと同期間分用意すること
15	ApexOne	一式	別事業者にて調達予定のため、調達不要
16	PowerChute Network Shutdown for Windows & Linux v5.0	2 ライセンス	運用管理サーバ、システム監視サーバ用 サポート保守を含めること
17	PowerChute Network Shutdown for Virtualization v5.0	1 ライセンス	仮想サーバ用 サポート保守を含めること

18	PowerChute Network Shutdown 1 Node License Pack for Virtualization	4 ライセンス	仮想サーバ用 サポート保守を含めること
19	Arcserve UDP 10 Advanced Edition - Server	2 ライセンス	運用管理サーバ（Linux）、システム監視サーバ（Win）用 サポート保守を含めること
20	VMware Workstation pro	1 ライセンス	
21	System Answer G3 ライセンス 5,000 項目（6 年）	1 ライセンス	サポート保守を含めること
22	System Answer G3 API オプション 5,000 項目（6 年）	1 ライセンス	サポート保守を含めること
23	System Answer G3 将来予測オプション 5,000 項目（6 年）	1 ライセンス	サポート保守を含めること
24	System Answer G3 インストールサービス	1 式	
25	System Answer G3 セットアップサービス 200 ノード	1 式	
26	System Answer G3 プロフェッショナルトレーニング（基本編）	1 式	
27	System Answer G3 プロフェッショナルトレーニング（応用編）	1 式	
28	System Answer G3 性能評価レポート（66 か月）	1 式	
29	IPCOM VE2-100 LS ソフトウェア V01（5 年 24 時間サポート付き）	34 ライセンス	仮想アプライアンス サポート保守を含めること
30	IPCOM VE2-100 LS V01 更新用サブスクリプションライセンス（1 年 24 時間サポート付き）	34 ライセンス	仮想アプライアンス サポート保守を含めること
31	Microsoft Office LTSC Standard 2024	7 ライセンス	運用保守端末用

(5) ネットワーク構成

ネットワーク構成は「図 1-1 システム全体構成図」を参照すること。本基盤のネットワーク構成については本基盤の設計・開発時に決定する。以下の点に留意すること。

ア 本基盤と、基盤外の連携先システムとをつなぐネットワークについては、別途調達・敷設される閉域網回線（専用線等）で接続し、外部からの侵入を物理的に防ぐこと。

イ 敷設される閉域網回線で本基盤に固有のグローバル IP を要する場合、適切なグローバル IP アドレス数を同時に用意すること。

ウ クラウド上に論理的に隔離された仮想閉域ネットワークを構築すること。また、本基盤上の業務システムが以下ネットワークに属することを留意すること。

- インターネット接続系
- LGWAN 接続系
- 個人番号利用事務系

また、各ネットワークに対し管理領域を用意し、WSUS 機能やウイルス対策機能等を設置すること。なお、今後の業務システム担当職員及び業務システム構築・運用事業者の希望により、上記に該当しない独立ネットワーク系の業務システムを本基盤のクラウド環境に受け入れる可能性があることをネットワーク

設計に考慮すること。

エ　業務システム担当職員及び業務システム構築・運用事業者がサーバを構築する際は、基盤管理者から払い出された CIDR を利用しなければならない。

(6) 施設・設備要件

本基盤の施設・設備要件を下表に示す。

ア　本基盤のオンプレミス機器を搭載するためのラックについては、本県で調達し、本県庁舎内に設置する前提とする。「3.11.（３）オンプレミス環境のハードウェア要件」に記載の形状要件を参照し、ラックに搭載すべき全ての調達予定物理機器が、本県の準備するラックに収まるように機器を調達すること。なお、19 インチ規格、高さ 42U のラックを 3 架準備する予定である。

イ　オンプレミス環境の設置フロアには分電盤が設置され、30A/200V 程度の電源容量を 6 口確保しているため、調達予定物理機器の総電力量が当該容量に収まるように機器を選定すること。

ウ　オンプレミス環境の設置フロアの床耐荷重は、600kg/㎡であるため、調達予定物理機器の重量が当該重量に収まるように機器を選定すること。

エ　運用保守端末についても、すべて本県庁舎内に設置を予定している。なお、設置フロアについては以下のセキュリティ対策を施している。

- 特定個人の入退室記録が記録可能

(7) 運用保守端末の要件

本基盤の運用開始時点で動作保証の対象とする PC・OS・ブラウザの考え方について、以下に示す。

ア　本基盤の運用開始時点で動作保証の対象とする端末を下表に示す。

表 3-8 動作保証対象とする運用保守端末

項番	端末	OS	バージョン
1	PC	Windows	11

イ　本基盤の運用開始時点で動作保証の対象とするブラウザは以下とする。

・　PC（Windows） の場合：Microsoft Edge/Mozilla Firefox/Google Chrome の最新バージョン

3.12. データマネジメントに関する事項

本基盤のライフサイクル全般を通じて、保有するデータ品質の維持・向上やデータの適正な利活用等を実現するため、以下に示す要件を踏まえ本基盤のデータマネジメントを実施すること。

(1) データ管理体制の明確化

本基盤で扱うデータの種別ごとに管理主体（管理する組織、担当者等）や役割の設定を基盤担当職員と共に行い、データ毎の管理責任を明確化すること。

3.13. **テストに関する事項**

本基盤のテストに関する要件を下表に示す。なお、品質管理の観点から必要に応じて基盤担当職員が指定する専門チームがテストに参加することもあるため、受け入れること。また、テストデータやテストに関連する情報の提供にも協力すること。

表 3-9 テスト要件

項番	分類	要件
1	テスト工程の定義	・ 本基盤では、以下のテストを実施する。 (1) 単体テスト (2) 結合テスト (3) 総合テスト (4) 受入テスト
2	テスト計画書	・ 各テスト工程の開始時に、以下の内容を定義したテスト計画書を作成し、基盤担当職員の承認を得ること。 ➢ テスト計画書の目的と位置付け ➢ テストの目的、概要 ➢ 対象範囲 ➢ テストスケジュール ➢ テストの観点 ➢ テスト実施体制、役割分担 ➢ テスト実施手順 ➢ テスト環境 ➢ テストシナリオの概要 ➢ 工程開始条件、工程終了条件 ➢ 成果物一覧 ➢ テスト結果に係る定性・定量評価の方法（テスト密度、バグ検出密度等） ➢ 進捗管理 ➢ 品質管理 ➢ 不具合管理 ・ 本業務を実施する各過程においてテスト計画書の内容に変更が生じる場合、変更箇所及び内容について基盤担当職員の承認を得ることを条件として、テスト計画書を適切に更新すること。 ・ 情報セキュリティの観点から必要なテストがある場合には、テスト項目及びテスト方法を定め、これに基づいてテストを実施し、その実施記録を保存すること。 ・ テストに係る管理要領を共通化し、各テスト工程において、原則として同一の管理要領を適用すること。各テスト工程に応じて部分的に異なる管理要領の適用を必要とする場合は、その適用差分のみ「テスト計画書」に記載すること。
3	テスト仕様書	・ 本基盤の各テスト工程の開始前に、テストシナリオ、テスト項目等を記載したテスト仕様書を作成すること。 ・ 各テスト工程のテスト項目は、設計書等の記述内容を網羅的に確認できるよう作成すること。 ・ 各テスト工程に応じたテスト技法を適用すること。 ・ テスト項目は、品質を確保するために十分なテスト項目を定義すること。また、テスト計画の策定時に定めた定性・定量評価方法を満たすよう作成すること。 ・ 基盤設計・開発業務受託者においてレビューを徹底し、上記要件を満たしたテスト仕様書となっているかを確認すること。
4	テストの実施	・ 作成したテスト項目に基づきテストを実施すること。 ・ テストを実施する際は証跡を取得すること。証跡の納品対象については別途基盤担当職員と協議の上決定すること。 ・ 証跡等に代表されるテストの成果物のレビューを徹底し、テスト項目に基づきテストを実施しているか確認する。想定外のテスト結果となった場合は、本基盤の欠陥であるか、想定結果が誤りである

		か等、原因を明らかにした上で必要な対応を行うこと。 ・ 欠陥を検知した場合は、その原因を明らかにした上で、原因を解消すること。 ・ テストにて、本県ネットワークへ接続する場合には、基盤担当職員と協力しテストを行い、本県内の業務等に影響がないように十分注意し実施すること。
5	テストデータ	・ 総合テスト及び受入テストにおいて実データを使用する必要がある場合は、実データの取得申請を条件として、実データの使用を許可する。なお、疑似データの作成に当たり、実データの匿名化、符号化等を行う場合は基盤設計・開発業務受託者の作業とする。 ・ 取得した実データは、適切に保管・管理すること。 ・ 受入テストにおいて作成したテストデータは、システム切替え実施前までに、検証環境等のデータも含め削除すること。 ・ 機密性の高いデータ項目や個人情報に係るデータ項目は、マスキングした上で使用すること。
6	対応状況の報告	・ テストの進捗としては、テスト実施済項目数や信頼度成長曲線等の定量的なメトリクスの推移を示すことにより、テスト進捗状況、不具合検出状況及び不具合対応状況を報告すること。 ・ 基盤担当職員からのテストの進捗状況や品質等に対する指摘に対し確実に修正すること。 ・ 各テスト工程に応じたテスト計画内容について基盤担当職員に説明し、各テスト工程における最初のテスト開始予定日の遅くとも 1 週間前までに基盤担当職員の承認を得ること。
7	テスト完了報告書	・ 各テスト工程の完了に当たっては、テスト完了報告書を作成し、基盤担当職員の承認を得ること。また、完了に当たっては以下をすべて満たすこと。 ➢ すべてのテスト項目が完了していること。 ➢ テスト結果について、定性評価及び定量評価（テスト密度、エラー検出密度等）により評価を行うこと。 ➢ テストで発生したすべての障害が、当該テスト工程内で解消されていること。 ➢ 外的要因等により次工程への申し送り事項が発生した場合は、対応方針、対応時期等を明確にした上で、基盤担当職員の承認を得ること。
8	構築時の脆弱性対策	・ 設計・開発段階の早期からセキュリティを検証すること。

- 各動作確認試験は、テスト計画書を作成し、その中でテスト項目を設定し正常性を確認し、テスト結果報告書を作成し県の承認を得ること。また、テストで使用するデータ等に関しては、基盤設計・開発業務受託者にて準備すること。
- テストデータは、テスト完了後に全て削除すること。
- テストにて、県ネットワークへ接続する場合には、本県の担当と協力しテストを行い、本県内の業務等に影響がないように十分注意し実施すること。確認テストにて、不具合が発生した場合には、県へ報告するとともに、原因の究明を行い、不具合がなくなるまでテストを実施すること。
- 報告には確認点、問題点、改善点の記載を行うこと。
- ただし、想定テスト概要やテスト実施方法等については、県及び第２期基盤運用・保守事業者と協議し詳細を決定することとする。

(1) 単体テスト

現時点で想定する単体テストの要件を以下に示す。

ア 単体テストの結果は、必要に応じて数値的指標等（試験項目数、試験消化率等）をもって報告すること。以下に示す事項については、あらかじめ基盤担当職員に提示すること。

- 単体テストのスケジュール
- テストを実施するハードウェア、ソフトウェアの構成、テストツール等の概要
- 合否判定基準 等

イ 単体テスト実施時は、テスト結果を検証するための証跡を採取すること。

(2) 結合テスト

結合テストは、本基盤の構成要素（基盤インフラ機能、ソフトウェア、ハードウェア等）に着目し、各要素の連動又は協調動作に関する設計の欠陥を検出することを目的として行う。現時点で想定する結合テストの要件を以下に示す。

ア　結合テストの観点として以下を想定する。

表 3-10 結合テストの主なテスト観点

項番	テスト種別	概要
1	システム基盤テスト	現時点で想定するシステム基盤テストの要件を以下に示す。 ・　本基盤のインフラ機能における機器あるいは機能ごとに他機器との連携が必要な部分について、他機能との連携部分が正常に動作するかを確認する。 例）他サーバとのネットワーク疎通、特定サーバに対する監視確認など。 ・　なお、冗長構成サーバにおいて片系を止まった際のシナリオテスト等、異常系確認についても、アプリなしでも実施可能な確認は本テストで実施する。
2	アプリ搭載後の確認テスト	現時点で想定するアプリ搭載後の確認テストの要件を以下に示す。 ・　業務システム固有の基盤が提供するプロセス監視、サービス監視など。 ・　業務システムのサーバ等に対する基盤提供バックアップ・リストア機能の確認など。

イ　結合テストに用いるテストデータには、テストケース、テスト項目を踏まえた疑似データを作成して使用すること。

ウ　結合テスト実施時は、テスト結果を検証するための証跡を採取すること。

エ　結合テストは、原則として本番環境において実施すること。

(3) 総合テスト

総合テストは、機能仕様及び構成に由来する欠陥を検出することを目的として行う。現時点で想定する総合テストの要件を以下に示す。

ア　総合テストの観点として下表を想定する。

表 3-11 総合テストの主なテスト観点

項番	テスト観点	概要
1	性能・拡張性	・　各仮想リソースにおいて、基盤が提供するバックアップ・リストアの実行時間を測定し、運用設計を満たすバックアップ・リストア運用が可能か検証すること。検証に当たっては、現在の想定だけではなく、今後の予想される増加量も含めて確認すること。 ・　サーバディスクのスケールアップ等、基盤利用者に提供予定の仮想リソースの拡張性について、一通り動作確認を行うこと。
2	可用性（障害）・継続性	・　疑似的に障害を発生させる等の方法により、本基盤のコンポーネントに障害が発生した場合に、どの程度許容して安定動作するか検証すること。また、システム障害及びエラー発生時の回復機能等が適切に動作することを確認すること。（冗長化された回線やロードバランサ構成における確認を想定）
3	完全性	・　疑似的に障害を発生させる等の方法により、サーバ等の稼働リソースが突然停止した場合に、稼働リソース内のディスクに格納されたデータに破損が発生していないか等について確認する。
4	セキュリティ	・　不正侵入や Web 特有の攻撃への対策、データベースへの不正アクセスなどに対する対策、データの持ち出しに対する対策、マルウェア（ウイルス）対策等のセキュリティ要件を満たしているか脆弱性検査等を実施し確認すること。
5	運用・保守性	・　運用・保守作業全般を通して、基盤運用・保守業務受託者が円滑に日々の業務を実施できることを確認すること。 ・　運用・保守における正常時、異常時の運用に関する動作を確認し、特に異常時の対応として、エラーメッセージやログ等を基に、基盤運用・保守業務受託者が業務を行えることを確認すること。

		・ 業務システム担当職員及び業務システム構築・運用事業者のアクセス権並びに基盤管理者のアクセス権を適切に設定した各アカウントで、必要な運用保守手順等を実施できるか妥当性を確認すること。

イ　総合テストに用いるテストデータには、本番運用を想定した疑似データを作成して使用すること。

ウ　システム停止に伴うシステムバックアップやシステム停止、リストア、システム起動等については、基盤設計・開発業務受託者が主体的に実施すること。

エ　総合テスト実施時は、テスト結果を検証するための証跡を採取すること。

オ　総合テストは、原則として本番環境において実施すること。

カ　既存基盤システムとの接続連携確認等のテストとして、総合テストを実施すること。

キ　テスト項目及び手順について本県と協議し、総合テスト仕様書としてとりまとめること。

ク　総合テストの実施結果として、総合テスト結果報告書を提出すること。

ケ　不具合等が発生した場合には、本県と協力して解決を行い、総合テストは不具合が無くなるまで実施すること。

コ　システム移行に関するテストを、上記要件と同様に実施すること。

(4) 受入テスト

受入テストは、要件に対する基盤リソース払出サービスの充足性確認を目的として行う。

当該テストの対象は、基盤運用・保守業務受託者が業務システム担当職員及び業務システム構築・運用事業者に対して行う一連の運用作業とし、基盤担当職員による受入テスト実施を支援すること。

構築された本基盤が要件定義書に記載した事項を適切に実現しているか、本基盤を用いて実際のサービス・業務を正しく実施できるかといった観点について机上を中心にテストを実施することとする。ただし、受入テストの目的を担保可能であることを条件に、疑似データを使用することも可能とする。

基盤設計・開発業務受託者は以下の支援を行うこと。

ア　基盤担当職員が実施する受入テスト計画書作成作業を支援するために、受入テスト計画書（案）を作成すること。基盤担当職員は受入テスト計画書（案）を基にして受入テスト計画書を作成する。なお、受入テストの実施期間は十分に確保したスケジュールとすること。

イ　基盤担当職員が実施する受入テスト仕様書作成作業を支援するために、テスト項目、使用するテストデータ、合格判定基準等を示した受入テスト仕様書（案）を作成すること。基盤担当職員は受入テスト仕様書（案）を基にして受入テスト仕様書を作成する。

ウ　基盤担当職員及びプロジェクト関係者が受入テスト計画書及び受入テスト仕様書に基づき実施する受入テストの実施支援を行う。

エ　受入テストの実施に当たり、必要に応じて本基盤の運転スケジュール、環境設定、テストデータ等の変更を行うこと。

オ　受入テストの実施に当たり、基盤担当職員からの質問に対する問合せ対応を行うこと。

カ　受入テストで発生したすべての障害が解消されている、又は問題を特定した上で対応策について基盤担当職員の承認を得ていること。

3.14. 移行に関する事項

本基盤に関する現段階での移行要件を以下に示す。

(1) 移行に関する前提条件

移行における前提条件を下表に示す。

ア　データの移行漏れを防止するため、データ移行時には本稼働中の第２期基盤を停止する必要がある。業務停止に当たっては、基盤担当職員に対して移行に係る時間や制約条件等を報告し、事前に十分な調整を行うこと。

イ　本基盤の要件等に伴い、移行対象データの作成や加工が必要な場合においては、第２期基盤運用・保守事業者と協力し、調整の上で、確実に実施すること。なお、移行実施体制と役割分担については下表を参照の上、移行作業が円滑に進むよう適宜調整すること。

表 3-12 移行に向けた作業手順及び役割分担。

項番	作業名	基盤担当職員	第２期基盤運用・保守事業者	本基盤設計・開発業務受託者	業務システム担当職員業務システム構築・運用事業者	栃木県セキュリティクラウド事業者	マロニエ21 ネットシステム管理者	個人番号利用事務認証システム事業者	庁内 LAN 管理者（クラウド接続用閉域回線管理者）
1	移行計画の作成	●、■	△	◎	◎	△	△	△	△
2	移行データ準備・提供	◎、●、■	◎	△	◎	△	△	△	△
3	移行データ分析	●、■	△	△	◎	△	△	△	△
4	移行設計	●、■		◎	◎	△	△	△	△
5	データ移行サーバ・ツールの開発	●、■		△	◎				
6	移行リハーサル	●、■	△	◎	◎	△	△	△	△
7	移行判定	◎、●、■		◎	◎、■				
8	本番移行	●、■	△	◎	◎	△	△	△	△
9	稼働判定	◎、●、■		◎	◎、■				

◎：主体者、●：確認者、■：承認者、△：支援者

ウ　本基盤上の各業務システムの移行時期については、令和 9（2027）年 7 月～令和 9（2027）年 10 月を想定する。具体的な移行時期については、本基盤の設計・開発着手後に別途定める。

エ　本番環境への移行作業は、システム停止を伴うことから、システム運用時間外の土日祝日に実施する予定である。移行作業中に障害が発生する場合も想定し、連絡体制・現場対応体制を確保すること。

オ　第 2 期基盤から本基盤のオンプレミス環境への業務システムの仮想マシン移行対象は以下を想定している。

- 移行対象となる業務システムの仮想マシン数（見込み）：約 180 台
- 総データ量：約 100TB

カ　業務データの移行対象は以下を想定している。

- 業務バックアップデータ：約 25TB

キ　各業務システムにおける第 2 期基盤から本基盤のクラウド環境への移行パスは仮想マシンの再構築を前提とする。なお、基盤設計・開発業務受託者にて仮想マシンの再構築対応をすべき業務システムの規模は以下を想定すること。ただし、以下の表の規模は令和 8（2026）年 3 月時点での見込み予測値であり、各業務システム側の事情により規模が増減する可能性に留意すること。

表 3-13　業務システムの規模

項番	項目	想定規模（見込値）
1	業務システム （インターネット非公開）	・　28 業務システム （内訳：インターネット接続系:23 システム、LGWAN 接続系:1 システム、個人番号:4 システム）
2	業務システム （インターネット公開）	・　5 業務システム
3	仮想マシン（IaaS）	・　57 台 （内訳：Windows Server 46 台、Red Hat Enterprise Linux 11 台）
4	仮想データベース（PaaS）	・　11 台 （内訳：Oracle 4 台、PostgreSQL 7 台）
5	業務用ロードバランサ	・　3 台

(2) 移行計画の作成

移行等に関しての計画をまとめた「移行計画書」を作成し、基盤担当職員の承認を得ること。「移行計画書」には、下記を含めること。なお、移行計画は本プロジェクト関係者以外の第三者にも容易に理解可能でかつ継承可能な形式で作成すること。

表 3-14　移行計画書の記載内容

項番	項目	補足
1	基盤管理者及び各事業者の移行実施体制と役割	・　移行作業は、基盤設計・開発業務受託者が主体となり実施するものとする。
2	移行に係る詳細な作業及びスケジュール	・　基盤担当職員に最終的な移行スケジュールを提示し、確定した内容を移行計画に反映させること。
3	移行対象	・　データ名称、保管環境、容量、など
4	移行環境／移行方法／移行ツール	・　移行可能期間の制約も踏まえた上で、一括移行、差分連携等の手法を組み合わせて、円滑に移行が行えるように留意すること。 ・　業務停止に当たっては、基盤担当職員に対して移行に係る時間や制

		約条件等を報告し、事前に十分な調整を行うこと。 ・ 移行方式は、一括移行又は複数回の分割移行とする。
5	移行作業、移行に伴い発生する各種設定を行うための各種手順書・マニュアル	・ 移行する際の移行手順及び機能改修のリリースに係る移行手順を移行手順書としてとりまとめ、基盤担当職員の承認を得ること。具体的な移行方法や手順は、基盤担当職員と協議の上で確定し、必要に応じて手順やツールの操作方法等に関するマニュアル等を基盤設計・開発業務受託者が作成すること。 ・ 移行手順は、本基盤と連携するマロニエ 21 ネットシステム、個人番号利用事務認証システム、庁内 LAN、栃木県セキュリティクラウド及び本基盤上の業務システムの、業務連携先システム等にも影響があることを踏まえ、基盤担当職員経由で調整等を実施した上で作成すること。
6	切り戻し基準、切り戻し手順書	・ 令和 9（2027）年 10 月は、第 2 期基盤をバックアップシステムとして並行稼働させる。 ・ 本基盤から第 2 期基盤への切り戻しが必要となった場合に対応できるよう、切り戻し基準や切り戻し手順書をあらかじめ定めること。 ・ 切り戻し手順書には、切り戻した後の両システムの運用方法、データの整合性を確保する方法、再度本基盤に切替える際の移行手順等も含めること。
7	移行判定基準	・ 移行開始時に満たすべき移行判定基準を定めること。なお、移行判定基準には以下を含め詳細は基盤担当職員と協議の上決定すること。 ➢ 計画した全てのテストケースを消化し、摘出された全ての障害（バグ、不具合等を含む）が除去されていること。仮に除去されていない障害がある場合は、その対処方針が明確となっていること。 ➢ 移行計画書及び移行リハーサルの結果が適正であること。 ➢ 切り戻し基準や切り戻し手順書を定めており、基盤担当職員の承認を得ていること。 ➢ 稼働後の運用準備が整っていること。
8	連携先の外部システム	・ マロニエ 21 ネットシステム、個人番号利用事務認証システム、庁内 LAN、栃木県セキュリティクラウド及び本基盤上の業務システムの、業務連携先システム等関係者と連携すること。その際、システム連携の現状を把握し、本基盤への移行に伴うテスト計画を作成し、テストに向けた事前合意形成を行い、テストフェーズでも進捗管理、課題管理を行って、テスト結果の取りまとめを行うこと。その際に、必要な資料等の作成を行うこと。また、マロニエ 21 ネットシステム、個人番号利用事務認証システム、庁内 LAN、栃木県セキュリティクラウド及び本基盤上の業務システムの、業務連携先システム等関係者と連携し、業務システム担当職員及び業務システム構築・運用事業者に対する通知方法、通知内容の検討等について、基盤設計・開発業務受託者が主体的に実施すること。
9	移行リハーサルの実施場所（システム環境）	・ 移行リハーサルについてマロニエ 21 ネットシステム、個人番号利用事務認証システム、庁内 LAN、栃木県セキュリティクラウド及び本基盤上の業務システムの、業務連携先システム等関係者と調整の上、本番環境（クラウド/オンプレミス）で実施すること。 ・ なお、移行リハーサルにおいて本番環境を利用しない場合は、可能な限り本番環境に近い環境を準備した上で移行リハーサルを実施すること。

移行計画書に加えて下表の計画も作成すること。

表 3-15 計画の種類

項番	計画の種類	概要
1	移行リハーサル計画	移行リハーサルにおける方針、スケジュール、実施体制、実施手順、検証方法等を定めたもの

2	移行（本番）計画	本番移行時の方針、スケジュール、実施体制、実施手順、作業結果判定方法、移行作業時のセキュリティ対策等を定めたもの
3	並行稼働計画	並行稼働における方針、スケジュール、実施体制、実施手順、検証方法、切戻しを行う際のコンティンジェンシープラン等を定めたもの

移行データ準備・提供員は、第２期基盤運用・保守事業者の支援を受けつつ移行対象となるデータを整理し基盤設計・開発業務受託者に提供する。

基盤設計・開発業務受託者は、移行対象データを受領し内容を確認すること。

(3) 移行データ分析

移行対象データを分析し、データ・クレンジング等の加工作業が必要であるか確認の上、結果について基盤担当職員に報告すること。

(4) 移行設計

「移行計画書」を踏まえ、以下の点に留意して移行設計書を作成の上、基盤担当職員の承認を得ること。また、業務実施部門が本基盤を利用するために必要となる準備事項について、提案や支援を行うこと。

ア　システム移行、データ移行、稼働の方式を設計すること。

イ　本番移行等、各移行作業に関しての見込み時間を記載すること。その際は、部分的なデータを送信して所要時間を計測するなど、必ず事前に計測を行い、本番移行の見込み時間の妥当性を証明すること。

ウ　第２期基盤から本基盤へ接続切替えを実施する方法に関する設計を行うこと。なお、接続切替えを実施するために、他の情報システム等に設定変更等を依頼する場合には、依頼内容を整理した上で、各業務システム担当職員及び業務システム構築・運用事業者との調整を行うこと。

エ　データ移行を含む移行に係る作業を抽出し、システム移行フローを組み立て、タイムスケジュール化等を行うこと。

(5) データ移行サーバ・ツールの開発

円滑なシステム移行が実施できるように、必要に応じてデータ移行サーバや移行ツールの準備を実施すること。また、設計・開発業務受託者が独自開発したツール等を利用する場合は、予め基盤担当職員に報告の上、承認を取ること。

なお、業務システム個別の単位では業務データの移行が発生する可能性がある。クラウド環境への業務データの移行について、主体は業務システム担当職員及び業務システム構築・運用事業者となるが、業務データの移行に必要なセキュリティ的に問題のないネットワークを基盤設計・開発業務受託者が提供すること。

(6) 移行リハーサル

システム移行、データ移行のリハーサルでは以下の点に留意すること。

ア　移行設計書及び移行手順書の内容を最終確認し、基盤担当職員及び本基盤上の業務システムとの最終的な意識合わせを行うこと。

イ　マロニエ 21 ネットシステム、個人番号利用事務認証システム、庁内 LAN、栃木県セキュリティクラウド及び本基盤上の業務システム等連携先システムに設定変更等を依頼する場合は、依頼書を準備し、期間的な余裕を持って、基盤担当職員経由で依頼すること。

ウ　移行リハーサルの実施後、移行に係る作業手順、作業時間見積もり等を評価し、「移行リハーサル結果報告書」を作成すること。また、その内容について基盤担当職員に説明し、承認を得ること。

エ　移行計画書及び移行手順書に問題がないことを検証するため、最低 1 回以上移行リハーサルを実施すること。
なお、移行リハーサル実施後における使用データの扱い（移行リハーサル後に使用データを削除等）についても検討すること。

オ　移行リハーサルの結果を分析し、本番移行に向けた課題などを明確にすること。

カ　作業品質に改善及び再検証を要する問題点を確認した場合、必要に応じて移行リハーサルの再実行を検討すること。

キ　基盤担当職員の指示がある場合、修正した移行リハーサル計画書及び移行手順書を基準として移行リハーサルを再実行すること。

ク　移行リハーサル評価結果に基づき、本番移行までに解決を要する課題について整理すること。

ケ　移行リハーサルの期間においても業務システム担当職員及び業務システム構築・運用事業者による業務サーバ等のセットアップ時と同様に以下を含む必要な支援業務を実施すること。

- 基盤が提供する監視機能のチューニング支援
- 基盤が提供するネットワーク・ファイアウォール機能のチューニング支援
- 基盤が提供するログ管理機能のチューニング支援
- 基盤が提供するバックアップ機能のチューニング支援

(7) 移行判定

基盤担当職員は、移行開始判定を目的とした会議を招集し、「（2） 移行計画の作成」にて定めた移行判定基準を満たしているか確認した上で、移行判定を行う。

基盤担当職員が移行判定を適切に実施できるよう、報告には「（2）移行計画の作成」に記載した移行判定基準を満たしているか分かるような情報を含めること。

(8) 本番移行

本番移行では以下の点に留意すること。

ア　本番移行に向けて、移行リハーサルの実施結果を元に移行計画書及び移行手順書を修正すること。また、その内容について基盤担当職員に説明し、承認を得ること。

イ　移行計画書には、チェックポイントを設定し、作業の進捗度と経過時間などを元に、切り戻しの判断基準を設けること。

ウ　本番移行及び稼働に係る作業過程において作成する提出物及び成果物の内容について、基盤担当職員に説明を行い、承認を得ること。

エ　本番移行に伴う作業状況について、事前にチェックポイントを設定し、適切なタイミングで基盤担当職員に報告すること。万一、作業の実施中に不具合等を生じた場合は、速やかに基盤担当職員に報告するとともに、必要な対応を行うこと。

オ　本番移行開始判断を受け、稼働のための作業を実施し、本番稼働を開始すること。

カ　稼働関連作業の完了後、本基盤の稼働状況を確認すること。また、稼働以降安定運用までの 1 か月程度の期間、QA 対応を主体とした運用支援を行うこと。特に、本番稼働後 2 週間は、問合せ対応、インシデント対応等に手厚い対応体制をとること。

キ　本基盤に移行した後に、何らかの問題が生じた場合は、第 2 期基盤に切戻しを行うこと。切戻しできる期間については、ライセンス切れ等による第 2 期基盤の利用期限が令和 9（2027）年 10 月末のため、当該期限の前までに移行作業が収まるように設定すること。

ク　移行リハーサル、本番移行の実施結果を「移行結果報告書」として取りまとめ、基盤担当職員の承認を得ること。

(9) 稼働判定

基盤担当職員は、サービスインを判断（稼働判定）する。
その際、本基盤へ切り替えても業務に支障が生じないことを基盤担当職員が判断するための資料を提出すること。

ク　本調達機器等の納入後に本県による納入検査を行う。

ケ　納入検査の結果、本調達機器等の全部又は一部に不合格品が発見された場合には、直ちに当該機器等の修復・再設定を行うこと。当該機器の修復・再設定に長時間かかる場合には、代替機等を指定した日時までに納入・設定すること。修復・再設定及び代替機等に係る全ての費用は、基盤設計・開発業務受託者の負担とすること。

コ　納入検査には、既存の基盤運用・保守業務受託者による確認作業も含まれることに留意すること。

サ　納入検査には、基盤設計・開発業務受託者の立ち合いを伴うこと。

3.15. 引継ぎに関する事項

本基盤の運用は、別途調達する基盤運用・保守業務受託者が実施する予定である。現時点で想定する引継ぎ要件を以下に示す。

(1) 引継ぎ計画書の作成

本基盤の関連事業者に対する引継ぎの開始前に、本基盤の引継ぎに係る引継ぎ対象、引継ぎ体制、引継ぎ内容、引継ぎ方法、引継ぎスケジュール、理解度確認方法、完了条件等を記載した「引継ぎ計画書」を作成し、基盤担当職員の承認を得ること。

(2) 引継ぎ方法

ア　「引継ぎ計画書」に従い、十分な時間的余裕を持って、必要な運用引継ぎを行うこと。その際は、引継ぎ対象者の理解度を確認し、必要な場合には、「引継ぎ計画書」に記載したスケジュール等の変更を行うこと。

イ　本基盤は、その保守や将来の拡張等の業務を他事業者に引き継ぐことが可能であること（引継ぎのために必要となる各種ドキュメントを整備する等）。第三者による保守性を向上させるため、成果物等は標準的に利用されているドキュメント作成ソフトウェアを用い、編集可能な形式で納品すること。

ウ　ドキュメントには設計結果のみを記載するのではなく、設計根拠等も明示し、検討経緯を可視化すること。

エ　引継ぎ期間中における本基盤の基盤運用・保守業務受託者からの問合わせに対応すること。

オ　期間内に引継ぎが完了しない場合は、原則として基盤設計・開発業務受託者の責任と負担において引継ぎを完了すること。

(3) 引継ぎ対象

本基盤の引継ぎ対象を下表に示す。なお、引継ぎに際しては基盤担当職員の指示に基づき書面又は電子媒体で行うこと。

表 3-16 本基盤の引継ぎ対象

項番	引継ぎ期間	引継ぎ先	引継ぎ内容	引継ぎ手順	補足
1	令和 9（2027）年 9 月 1 日～令和 9（2027）年 10 月 31 日	基盤運用・保守業務受託者（令和 9（2027）年度に調達予定）	・ 各種設計書・ドキュメント類 ・ 運用課題（管理簿） ・ 仕様課題（管理簿） ・ インシデント状況（管理簿） ・ 各種運用・保守作業 ・ その他成果物一式 （クラウドサービスの管理に必要なアカウントや鍵情報）	引継ぎ計画書の内容に基づいて、引継ぎ作業を行う。	

(4) クラウドサービスを利用する場合の引継ぎ

本基盤では、本調達の契約期間終了後も、クラウドサービスの契約期間終了前に契約の延長又は他の引継ぎ先事業者（運用・保守業務受託者を想定）への引継ぎ等を行うことで、クラウドサービスをそのまま継続利用することを想定している。引継ぎに際しては、必要に応じて引継ぎ先事業者及びクラウドサービスプロバイダとの間で書面による契約等を行い、しかるべく管理者権限の引渡し等を行うこと。

(5) 引継ぎ結果報告書の作成

引継ぎ作業の完了時に、本基盤の、他事業者等への引継作業の実施結果について記載した「引継ぎ結果報告書」を作成し、基盤担当職員へ報告を行うこと。

(6) 前任事業者からの引継作業

本業務を実施するために必要な情報について、第 2 期基盤運用・保守事業者からの引継ぎを受けること。引継ぎ完了後は、引継ぎ完了報告書（確認者、確認日時、完了条件の適合性等を記載）を作成し、基盤担当職員の承認を得ること。

(7) 基盤担当職員への引継ぎ

基盤担当職員向けマニュアルを作成し、操作説明を行うこと。

3.16. 教育に関する事項

(1) 教育に関する事項

本基盤の教育に関する事項は対象外とする。

3.17. 運用に関する事項

現時点で想定する運用要件を以下に示す。

(1) 運用・保守計画

運用・保守の設計で検討した内容を踏まえて、以下の要件が含まれる形で運用・保守計画書（案）及び運用・保守実施要領（案）を作成すること。

表 3-17 運用・保守計画書（案）の記載内容

項番	項目	補足
1	作業概要	・ 監視、運用・保守作業の対象範囲、管理対象、作業概要等を記載する。
2	作業体制に関する事項	・ 運用・保守業務を実施するための体制について、管理体制図、基盤運用・保守業務受託者の要員（責任者、作業者、役割分担）、連絡手段等について記載し、全体的な運用管理体制を明確にすること。
3	スケジュールに関する事項	・ プロジェクト計画書及び運用・保守の要件に基づき、運用・保守を行う上で基本とする作業内容、関係するほかの作業工程、そのスケジュール等について記載すること。 ・ 日次、週次、月次等の定型的な業務について、作業内容を記載すること。 また複数回発生した非定型業務の報告及びその定形業務化（手順書の作成等）の提案を含めること。 ・ 年次の作業内容には、運用業務の中で発生した運用上の課題、作業量の多い作業等について整理報告し、その改善（例えば自動化等）の提案を行う作業、システム運用継続計画の見直し作業、運用・保守計画書の見直し作業を含めること。
4	成果物に関する事項	・ 運用・保守業務にて納品する成果物の内容、担当者、納品期限、納品方法、納品部数等について記載する。
5	運用・保守形態、運用・保守環境等	・ 運用において採用する運用形態（オンサイト、リモート等）、運用にて利用する環境（本番環境）等を記載すること。
6	管理対象	・ 本業務で開発するシステム及びドキュメントについて保守を行うこと。
7	クラウドサービスの利用	・ 運用作業、運用手順及び運用管理用のソフトウェアも含め、可能な限り統一化を図るとともに、自動化された機能及びクラウドサービスが提供する機能等を利用し、運用に係る役務を可能な限り効率化すること。 ・ 利用しているクラウドサービスの機能や性能等に変更が発生した場合、基盤運用・保守業務受託者側でクラウドサービスの変更に伴う稼働中システムへの影響を確認し、本基盤の改修が必要な場合は、原則として対応すること。ただし、改修規模が大きい又は影響範囲が広い場合は基盤担当職員と協議の上対応を検討・実施すること。 ・ 運用 5 か年において段階的に発生する業務システムのクラウドリフトについて、本基盤からインフラ仮想リソースを払い出す等のシステム構築支援を実施すること。また、併せて本基盤のオンプレミス環境からクラウドリフト前に稼働していた同業務システムの撤去も実施すること。
8	サービスレベル	・ 運用・保守業務で達成目標とするサービスレベル項目及びサービスレベルを基盤担当職員と協議の上、決定すること。 ・ 運用におけるリソース使用状況に基づき、毎年のリソース計画を策定する。月間の運用実績を評価し、達成状況が目標に満たない場合はその要因の分析を行うとともに、サービスレベル達成状況の改善に向けた対応策を検討すること。
9	その他	・ 上記に掲げる事項のほか、運用・保守を行う上での前提条件、時間、予算、品質等の制約条件等について記載する。

表 3-18 運用・保守実施要領（案）の記載内容

項番	項目	補足
1	コミュニケーション管理	・ 運用・保守業務を実施する上で必要となるコミュニケーション手段について、会議体（会議体の名称、開催目的、開催スケジュール、出席者、報告内容等）、インシデント発生時の報告ルート等について記載し、効率的かつ円滑なコミュニケーションを実現すること。
2	体制管理	・ 運用・保守に携わる事業者における作業体制の管理手法等について記載すること。
3	作業管理	・ 運用・保守作業及びその品質の管理手法等について記載すること。
4	リスク管理	・ 運用・保守における作業を阻害する可能性のあるリスクを適切に管理するため、リスク認識の手法、リスクの管理手法、顕在時の対応手順等について記載すること。
5	課題管理	・ 運用・保守において解決すべき問題について、発生時の対応手順、管理手法等について記載すること。
6	システム構成管理	・ 運用・保守における情報システムの構成（ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、施設・区域、公開ドメイン等）の管理手法等について記載すること。
7	変更管理	・ 運用・保守により発生する変更内容について、管理対象、変更手順、管理手法等について記載すること。
8	情報セキュリティ対策	・ 平常時のセキュリティ運用として、継続的な脆弱性管理、構成管理及び変更管理を行い、不正アクセス等のセキュリティ脅威に対する監視運用を行うための具体的な方法を記載すること。 また、セキュリティインシデント発生に備えた体制や手順、発生時の被害極小化、速やかなサービス復旧を行うための具体的な方法を記載すること。

(2) 運用・保守準備

運用・保守に当たって、以下の準備作業の実施等を行うこと。

ア 監視設定

運用業務を効率的に実施するため、監視、アラートについて、本基盤の特性、各種アラート発生時の重要度に応じたチューニング（マッチング文字列、閾値、アラート検知結果の重要度など）を行い、定量的な計測に基づいて監視を行うこと。また、アラートの通知先、通知手段等は基盤担当職員と協議の上、決定すること。

イ バックアップサービス

本基盤の故障復旧に必要なデータのバックアップを定期的に取得すること。また、故障復旧時における必要なデータのリストア作業の手順、役割分担等を事前に決定し、故障発生時には実施すること。

ウ 運用・保守手順書

運用・保守実施要領及び運用・保守計画書に基づき、運用・保守手順書を作成すること。

(3) 共通的な要件

ア 運用・保守期間

稼働後、令和 14（2032）年 10 月 31 日まで運用・保守業務受託者にて運用・保守を実施する。

イ　運用・保守報告書の作成

運用・保守業務の実施結果を運用・保守報告書として取りまとめ、基盤担当職員が指定した日時までに納品すること。

ウ　情報セキュリティ対策の実施

「3.10.情報セキュリティに関する事項」を踏まえて実施した情報セキュリティ対策の対応結果を情報セキュリティ対策実施報告書に取りまとめ、基盤担当職員が指定した日時までに納品すること。

(4) システム稼働要件

本基盤の本番稼働に係る要件は「1.4 業務実施の時期・時間」を参照すること。

(5) 主な運用作業一覧

現時点で想定する主な運用作業の一覧について、以下に示す。以下の内容を基に、本基盤の設計・開発時に、運用・保守計画書（案）及び運用・保守設計書（案）を作成すること。

表 3-19 主な運用作業一覧

項番	運用作業の分類	主な運用作業の内容
1	パッチ適用管理業務	・ 保守におけるパッチ適用要否の判断結果に基づき、パッチを適用の上、適用後の稼働確認を行うこと。
2	ログ管理業務	・ 操作ログやアクセスログ等のシステムログ、例外事象の発生に関するログを取得すること。 ・ 取得したログ情報を活用し、適切なキャパシティ管理を行うこと。キャパシティの改善が必要と判断された場合、キャパシティ改善提案を行うこと。 ・ 収集したログを一元的に管理し、不正侵入や不正行為の有無の点検・分析を効率的に実施すること。 ・ ログの正確性を担保するため、適切なアクセス制御を行い、ログの改ざんを防止すること。
3	ジョブ管理業務	・ ジョブの登録・更新、ジョブの起動スケジュールを登録し、ジョブの実施結果を確認、報告すること。 ・ 基盤担当職員が必要性を認めた際は、基盤担当職員の指示に従い、ジョブの手動実行を行うこと。
4	システム監視業務	・ 本基盤の運用状況を監視し、障害の発生又はその兆候を検知するとともに、障害を検知した際には重要性等が分類された通知メールを受け障害調査の対応ができること。 監視には、例として以下のものがある。 ジョブ監視、死活監視、性能監視、リソース監視、障害監視、ログ監視（監視対象のログを監視し、特定の文字列パターンと一致した場合に障害とする方式）、セキュリティ監視、クラウドの構成監視（クラウドサービスを構成する要素を監視する方式）、外形監視（本基盤を利用するユーザと同じ方法でアクセスし正常に動作しているか監視する方式）等 なお、セキュリティ監視に当たっては、取得ログやセキュリティ製品のアラート等を用いて、不正アクセスやマルウェア感染等のセキュリティ脅威により引き起こされる異常な状態の監視等を行い、セキュリティインシデントやその兆候を早期に検知すること。 ・ 各種監視結果を定期的に集計・分析し、監視方法や閾値、通知の見直し等が必要な場合は、基盤担当職員の承認を得た上でこれに係る設計を行い、対応を実施すること。※システムサイジングについても定期的に分析を行い、基盤担当職員の承認を得た上で見直すこと。
5	問題管理業務	・ 本基盤に対し、重大な影響を与えるインシデントや将来的に重大なインシデントに発展する可能性がある問題について影響評価を行った上で、緊急度及び優先度を定め、根本原因の調査及び解決策の立案を行うこと。
6	変更管理業務	・ 課題管理機能の活用を前提として、適切な変更管理を実施すること。 ・ 構成要素を追加、変更又は廃棄する場合は、変更依頼書を起票すること。 ・ 機密情報の不要な公開等の意図しないセキュリティインシデントを防止するため、本基盤の設定変更等に当たっては、情報セキュリティ関連の設定に影響しないことを確認すること。

項番	運用作業の分類	主な運用作業の内容
7	リリース管理業務	・ 基盤担当職員とリリース作業の日程、作業内容、依頼事項等の調整を行い、実施の計画をリリース計画書に記載すること。 ・ リリースを実施した際、リリースに関する情報を「リリース管理台帳」にて管理すること。 ・ 「リリース管理台帳」には以下の項目を管理し、履歴を確認することとし、その管理が必要な項目についても管理する仕組みとすること。 ➢ 実施計画の内容 ➢ リリーステストの実施有無及び結果 ➢ リリース時期 ➢ 各種レビューの実施有無及び結果 ➢ リリース内容 ・ リリース計画書については、リリース予定日より十分な期間を確保の上、前もって基盤担当職員の承認をもって提出すること。なお、緊急なリリースを要する場合は基盤担当職員と協議すること。
8	システム構成管理	・ 本基盤に係る全ての構成品目について、適切な構成管理を実施すること。 ・ システム構成管理対象を特定し、管理レベルを定めること。なお、システム構成管理対象は、本基盤を構成するクラウドサービス、ソフトウェア（製品名、開発元、バージョン、ライセンス、依存関係等）、アプリケーション、通信回線、公開ドメインのほか、本基盤の運用・保守に係る全てのドキュメント及びデータとすること。ただし、本基盤の外部から提供を受けるものであり、運用・保守において変更を行わないものは、システム構成管理の対象外とする。 ・ システム構成管理対象の変更について、変更履歴を追跡可能であること。 - 本番環境・検証環境の維持管理を行うこと。
9	バックアップ	・ システムバックアップ、データバックアップを取得すること。 ・ 必要に応じてシステムリストア、データリストアを実施すること。
10	業務支援	・ 基盤担当職員の指示に基づき、基盤利用者の利用状況のデータを集計し、基盤担当職員に定期的に報告すること。 ・ 必要に応じて、データベースやディレクトリ等に施されるアクセス制御の設定変更を実施すること。 ・ 運用に必要な端末は基盤設計・開発業務受託者が用意すること。
11	障害対応	・ 障害発生時は、発生から解決までの一連の作業（受付、問題判別、業者間調整、調査解析、修復方法の検討、障害原因アプリケーションの再設計・製造・試験、再発防止・品質向上作業、報告書作成・報告実施、環境（本番環境）反映）を行うこと。 ・ 本基盤の連携先システムにおいて障害が発生し、業務影響が発生した場合においても、連携先システム担当が実施する原因調査、代替策、解決策の検討及び処置を必要に応じて支援すること。 ・ システム障害と想定される連絡を受け付けた際、別途、基盤担当職員より指示する担当者へ速やかにエスカレーションすること。
14	インシデント管理	・ 情報セキュリティインシデントが発生した場合は、「運用・保守実施要領」等に定めた手順に従ってインシデント対応を行うこと。対応に当たっては、基盤担当職員、関係事業者と適宜調整の上で対応を行うこと。 ・ インシデント対応手順の実効性を担保するため、定期的にインシデント対応手順の見直しやインシデント対応訓練を実施すること。
15	バージョンアップ対応	・ 保守におけるバージョンアップ対応要否の判断結果に基づき、バージョンアップ対応を実施し、稼働後の動作確認を行うこと。
17	運用改善	・ 本基盤の状況を基盤管理者が定期的に把握できるように仕組みを整えること。 ➢ プロジェクトの目標とする指標、基盤利用者の利用状況 ➢ クラウドのリソース等、本基盤の利用状況・コストの発生状況 ・ 本基盤の利用状況については、少なくとも以下の項目に記載した項目を実施し、利用状況の分析とその後の改善策に資する項目を含めること。 ➢ 運用管理・保守業務の作業別の所要時間 ➢ 自動化や効率化が可能と思われる作業の洗い出し ➢ 本基盤及び運用・保守業務の改善提案 ・ アイドリングなどの無駄／過剰なリソースを発見し、コスト削減につながる仕組みを整え、改善

項番	運用作業の分類	主な運用作業の内容
		提案を行うこと。 ・ 本基盤の利用拡大や利便性向上のため、実績に基づいた定量的なデータや利用者からの問合せ内容等を分析し、多くの基盤利用者が操作方法に迷う部分や誤操作を誘発する部分を把握した上で本基盤の改善策を検討すること。また基盤担当職員と協議の上、本基盤の改善を実施すること。
18	サービスオペレーション支援	・ 計画停止、保守作業、障害対応等により基盤利用者への影響が生じる場合、業務システム担当職員への周知連絡を行うこと。 ・ 作業影響を生じる範囲について、不測の運用障害を回避する観点から、メンテナンス機能を利用してサービス閉塞・閉塞解除運用を実施すること。
19	情報セキュリティ監査	・ 基盤担当職員が情報セキュリティ監査を実施する場合がある。その際はセキュリティ監査事業者との調整・ヒアリングへの協力を行うこと。
20	アカウント管理	・ 基盤運用・保守業務受託者は、基盤担当職員からの指示に基づき、ユーザID（特権ID含む）の払い出し、削除、パスワード再発行を実施すること。 ・ アカウントの利用状況の棚卸を実施すること。実施するタイミングは、年 1 回程度を想定しているが、具体的な時期については基盤担当職員と協議の上、決定すること。
21	基盤リソース払出業務	・ 「1.2 業務内容」を参照し、業務システム担当職員からの申請に基づいて、リソースの新規払出、変更、削除を実施すること。
22	その他業務	・ サーバ証明書の更新、ドメインの管理等を行うこと。

3.18. 保守に関する事項

以下の保守要件も踏まえて保守設計を実施すること。基盤運用・保守業務受託者が、運用・保守計画書及び運用・保守実施要領に基づき以下の作業を適切に実施できることを想定している。また、サービスレベルで規定された時間以内に、対応を開始できる体制下で実施されることを要件としている。なお、以下の保守要件は現時点のものであり、保守設計において具体的な作業等を確定の上で基盤運用・保守業務受託者の調達を行う予定である。

(1) 保守業務の実施

保守業務として以下を実施すること。

ア 問合せの受付時間は、「1.4 業務実施の時期・時間」に記載のとおりとする。ただし、基盤担当職員が緊急かつ業務に支障を来すと判断した場合はこの限りではない。

イ 受け付けた問い合わせをインシデントとして管理し、インシデントのクローズまで、対応を継続すること。

ウ 障害について対応したときは、障害報告書を作成し、基盤担当職員に報告すること。

エ 保守業務の実施に当たっては、保守体制を用意すること。
保守体制とは、問い合わせ受付対応窓口とハードウェア及びソフトウェア保守対応の総称を示すものとする。また、基盤システム運用保守体制と連携しサービスレベルに影響がないよう本県及び基盤運用・保守業務受託者と十分に協議を行うこと。

オ 保守期間は、賃貸借期間が終了するまでとする。
なお、保守期間中にハードウェア及びソフトウェアのサポート期間が終了しないこと。

カ　本調達機器について、技術的サポートを行うこと。
また、今後の運用中に本調達機器と他の機器との接続や別途調達するソフトウェアを本県がインストールする場合、本県と連絡が取れる体制をとり支援すること。

キ　保守対応は日本語で実施すること。

(2) 保守設計
保守設計として、以下を実施すること。

ア　役割分担の整理
役割分担を行う際に以下の点に留意すること。
・　保守業務の設計に際し、基盤運用・保守業務受託者の責任範囲及びクラウドサービスを含めた関連事業者間の役割分担を整理すること。
・　本基盤がクラウドサービス上で稼働することを踏まえ、各業者間の役割分担を考慮した上で、保守設計を行うこと。

イ　クラウドサービスの利用
クラウドサービスを利用する際に以下の点に留意すること。
・　保守設計を実施する上で、クラウドサービスの標準機能を可能な限り活用すること。
・　クラウドサービスによる自動化等により、省力化を実施すること。
・　運用・保守実施要領、運用・保守計画書及び運用・保守手順書については、クラウドサービスが提供する各サービスを活用することにより、作業のみならずドキュメント類についても効率的に作成すること。
・　利用するクラウドサービスにおいて、提供サービスの仕様上必要となるアップデートパッチの適用やメンテナンス等の対応に際して、本基盤への影響度に鑑み、基盤担当職員と協議の上対応を行うこと。又は、自動適用を行う等の対応が可能となるよう、必要な仕組み（検知、適用、等）を準備すること。

(3) クラウドサービスの保守
クラウドサービスの保守として以下を実施すること。

ア　利用しているクラウドサービスにおいて脆弱性及び不具合が確認された場合は、その対応について基盤担当職員と協議し、パッチ適用要否を判断すること。

イ　クラウドサービスにおいてバージョンアップ等の情報が公開された場合には、バージョンアップに伴う影響調査を実施した上で、基盤担当職員と協議し、適用等の可否を決定すること。なお、実施することとなったバージョンアップに伴う機器・サービス等の停止は計画停止に準ずるものとして扱う。また、バージョンアップに起因して改修が必要な場合には、対応について別途基盤担当職員と協議すること。

(4) ハードウェアの保守
ハードウェアの保守として以下を実施すること。

ア　保守対応時間は、24 時間 365 日とする。

イ　保守形態は、当日オンサイト保守とする。
・　障害受付時より２時間以内に保守作業に着手すること。

・　休日及び夜間等の作業の場合は、本県と協議し対応時間の調整を行うこと。

ウ　年 1 回程度休日に、本県庁舎設備のメンテナンスを目的とした全庁停電作業が予定されている。
その作業に伴い障害が発生した際には、保守作業を行うこと。
なお、障害復旧に係る OS やデータのバックアップ及びリストア作業は、基盤運用・保守業務受託者が実施する。

エ　各ハードウェア障害発生時には、当該機器又はそれを構成する部品等の調達・交換・修理等を迅速に行うこと。

オ　本調達機器等の保守に関して、製造元等が提供するハードウェア保守サービスに準ずる安定したサポート及び保守サービス品質の維持を図ること。
なお、ハードウェアの保守サービスレベル対応時間は、24 時間 365 日の当日オンサイト保守とする。

カ　本調達機器等に障害が発生した場合、保守サービス対応時間の範囲で、ハードウェア障害と判断された時点から、原則 2 時間以内に技術者を派遣し、障害装置の修復、故障部品の交換修理に当たるものとすること。
なお、賃貸借期間中は、必要な交換部品を必ず提供すること。

キ　休日及び夜間等の作業の場合は、本県と協議し対応時間の調整を行うこと。

ク　保守サービスは保守作業に必要な出張費用や技術料、部品代等全ての費用が含まれていること。
ただし、各種災害や本県に原因があり障害が発生した場合には本県と協議し決定する。

ケ　ハードウェアの修理又は交換を行う際に、サーバラックからの取り外しや、据え付け・調整作業等の必要な作業を実施すること。
また、必要に応じて、本県と協議の上、必要な設定内容の再投入等、設定作業を行うこと。

コ　障害箇所の修復後、システムが適切に機能するか動作確認を行い、正常動作を確認すること。

サ　保守期間中、ハードウェアに対する修正ファームウェアの適用要否に関する情報を提供すること。

シ　修正ファームウェアの適用に関しては本県と協議し決定すること。

ス　本調達機器に搭載された SSD 又は HDD に障害が発生し当該 SSD 又は HDD を交換した場合、交換した SSD 又は HDD については、情報漏えい対策を実施し本県の承認を得てから、本県外へ持ち出すこと。
なお、本県が求める場合にはデータ消去証明を発行し提出すること。

(5) ソフトウェア保守
ソフトウェアの保守として以下を実施すること。

ア　ソフトウェア最新化
本基盤を構成する全てのソフトウェアについて、製品不具合や情報セキュリティに関する脆弱性を修正するため、基盤担当職員と協議の上、ソフトウェアを最新化すること。なお、ソフトウェアの最新化に当たっては、本基盤のシステム構成等に考慮すること。

イ　修正プログラムの適用
修正プログラム適用の際は以下の点に留意すること。

・ 情報セキュリティや安定稼働の観点から緊急性が高いと考えられる修正プログラムについては、緊急適用を計画すること。緊急性が低い修正プログラムについては、定期保守作業の中での適用を計画すること。
・ 使用しているクラウドサービスの内容に変更が発生する際には、クラウドサービスより提供する情報を元に本基盤への影響範囲を調査の上、修正プログラムの適用可否を基盤担当職員へ報告すること。適用が必要と判断された場合、クラウドサービスより提供されるソフトウェアに対する修正プログラムの適用作業を実施すること。

ウ 検証・デプロイ

検証・デプロイを行う際は、ソフトウェア保守に伴い、本基盤の安定稼働に影響が生じる事態が予測される場合、バージョンダウンもしくは、リストア手順を確立した上で実施すること。

エ 設計書への反映

ソフトウェア保守によりソフトウェア構成に変更が生じた場合、設計書等へ変更内容を反映すること。

オ 保守条件の決定

保守条件は、「製品の導入や使用方法」、「製品の互換性や相互操作性」、「製品資料の解釈」、「構成サンプルの提供」、「修正策の情報提供」、「製品プログラム、製品コードに起因する障害」等の保守が提供されることを想定しているが、最終的な保守条件は、基盤担当職員と調整の上、保守設計において決定すること。

カ 脆弱性管理

ソフトウェアに関する脆弱性に対処するために、以下の対応を行うこと。

・ 脆弱性管理基準の作成と運用

脆弱性管理の方針を定めた脆弱性管理基準を、保守設計において基盤担当職員と調整の上で作成し、運用すること。

脆弱性管理基準には、以下の項目を含めること。

- 個別対応の要否判断の基準
  情報システムの「脅威」、「脆弱性」、「重要度」からの観点からのリスクの評価基準と対応優先度、個別対応又は定期保守でのどちらで対応するかの方針、目標とする脆弱性対処の対応期限を取り決めたもの。
- 定期アップデート規則
  ソフトウェアの定期アップデートを実施する頻度、実施条件、回帰テストの範囲を取り決めたもの。
- ソフトウェア採用判断の基準
  提供元の信頼性やサポート条件、脆弱性の情報開示やパッチ提供など、脆弱性対応を円滑に行うための基準を取り決めたもの。
- 脆弱性管理の対象と管理方式
  クラウドの責任共有モデルを含む情報システムの脆弱性管理の対象と、ソフトウェア構成や脆弱性を管理するツールやサービスなどの管理方式を取り決めたもの。

・ 脆弱性管理手順の作成と運用

脆弱性に対処する手順を定めた脆弱性管理手順を、保守設計において基盤担当職員と調整の上で作成し、運用すること。

脆弱性管理手順には以下の項目を含めること。

- ソフトウェア構成の管理

情報システムで使用するソフトウェアの製品名、開発元、バージョン、ライセンス、依存関係などを容易に参照できるよう構成管理及び変更管理を行うこと。

- 脅威情報の収集、自システムへの影響分析
  日々出現するセキュリティ脅威や脆弱性に対処するため、定常的に脅威情報や脆弱性情報を収集し、情報システムへの影響を含めてリスク分析を行うこと。
- リスクに応じた脆弱性対応及び定期アップデート
  情報セキュリティや安定稼働の観点からリスク評価を行い、即時もしくは優先的な対応が望ましいと判断される脆弱性については、緊急対応を計画すること。即時対応が不要もしくは対応の必要性が低い脆弱性については、定期保守作業の中での対応を計画すること。

キ　OS 等のバージョンアップや修正プログラムの提供を行うこと。

ク　ソフトウェアの脆弱性や修正プログラムの情報提供を行うこと。

ケ　基盤システムで障害が発生した場合には、障害の復旧等に協力すること。

コ　本調達機器がマルチベンダ構成になる場合、納入及び保守を確実に実現するために、関係する業者間で十分な合意を得るとともに、問い合わせ窓口を一本化する等、実施のための体制を整備し本県に報告すること。

サ　マルチベンダ構成における保守業者間の各種調整等については、基盤設計・開発業務受託者の責任と負担のもとに実施することとし、本調達機器の導入に当たり、その調整等による不都合、負荷等が発生しないようにすること。

(6) 保守実績の評価及び改善

保守実績の評価及び改善として以下を実施すること。

ア　本基盤の運営に関わる関係者間で本基盤の保守に係る情報や問題認識を共有し、保守業務の品質を継続的に維持・向上させること。

イ　本基盤が使用するクラウドサービス、ソフトウェア等の保守実施状況について、日々の保守業務の中で収集する定量的な管理指標を定め、基盤担当職員と合意すること。

ウ　ログ解析機能等を活用し、指標値の収集、評価及び管理を効率的に行うこと。

エ　管理指標の達成状況を評価し、未達の場合は原因分析を行い、改善措置を検討すること。また、これらの実績、評価、改善措置について、定期報告すること。

オ　モニタリング及び運用過程を通じて得られた利用状況を分析することにより、ライフサイクルコスト低減の観点から、利用するクラウドサービスの所要量及びソフトウェアライセンスの削減可能性を検討すること。また、利用状況の実績、評価、コスト削減可能性について、定期報告すること。

(7) ドキュメントの保守

設計・開発関連ドキュメント及び運用・保守関連ドキュメントが、基盤運用・保守業務受託者の契約期間において、最新の状態であるよう維持・更新等を行うこと。