No.	要求分類		要求項目	非機能要求	No.	項目名	要求事項
1	可用性	サービスを継続的に利用可能とするための要求	継続性	■業務停止時の継続性 業務停止を伴う障害発生時は、搭載する業務システムの継続性を妨げないことを前提に、障害発生前の状態に復旧すること。 ■大規模災害時の継続性 大規模災害時は、本市の求めに応じて、設置場所から離れた遠隔地のバックアップデータを用いてシステムを復旧すること。復旧にあたっては、設置場所の電源及びネットワークが利用できる状態にあることを前提とする。 ■継続性の目標値設定 システム障害時や大規模災害時の目標復旧時間、目標復旧レベル、年間を通じたシステム稼働率など、継続性を評価するための定量的な数値目標を設定すること。	1-1	RPO（目標復旧地点）（業務停止時）	データ損失が許容できないため、障害発生時点までの復旧とすること。 （例：HA（High Availability)機能で、自動的に別のサーバ上で再起動させることで機器障害発生後も稼働を継続する、など）
					1-2	RTO（目標復旧時間）（業務停止時）	ハードウェア、ソフトウェアの障害に係わらず、障害発生から6時間以内とすること。 ※ハードメーカーの駆けつけ部品交換の時間が4時間後となり、交換後の復旧作業を2時間程度と想定し、復旧に要する時間を6時間とする。
					1-3	RLO（目標復旧レベル）（業務停止時）	すべての機能が正常に稼動するレベルまで復旧すること。
					1-4	システム再開目標（大規模災害時）	1ヶ月以内に復旧すること。
					1-5	稼働率	99.99%の稼働率とする。 ※共通基盤は重要な業務システムも稼動するシステム基盤となるため、高い稼働率が求められる。
			耐障害性	■単一障害点の排除 単一障害時は業務停止を許容せず、10 分未満の切替時間で業務を継続すること。冗長化構成を適用することで、業務を継続させる対策を講じること。	1-6	冗長化（サーバ機器）	冗長化構成を必須とする。
					1-7	冗長化（ストレージ機器）	冗長化構成を必須とする。
					1-8	冗長化（ストレージのディスク）	採用するストレージの規格により異なるが、データの消失を防止する方式を採用すること。
			災害対策	■遠隔地へのバックアップ 大規模災害時のシステム復旧を可能とするため、仮想化基盤のデータ及びプログラム等復旧に必要な情報を所定の遠隔地へ保管すること。遠隔地バックアップの実現方式は、保管先との協定に基づくことが前提であるため、コストに配慮した適度な方式を採用すること。 ■バックアップ頻度等の設定 遠隔地バックアップの対象や実施頻度、復旧方針、保管場所分散度等を設定すること。現時点では、現行通り、月次で取得したバックアップを媒体で保管する想定である。 (a) 日次バックアップ媒体：データセンタ内 (b) 月次バックアップ媒体：データセンタ外 ■システム復旧手順の整備 搭載する業務システムの復旧手順を踏まえた「仮想化基盤の復旧プロセス」の整備を構築工程の検討項目に含めること。	1-9	復旧方針	仮想化基盤の機能が提供できる構成で復旧すること。
					1-11	保管方法（外部保管データ）	仮想化基盤のデータがバックアップできるストレージ装置を採用すること。

No.	要求分類		要求項目	非機能要求	No.	項目名	要求事項
			リソース拡張性	■処理能力 仮想化技術を用いたプライベートクラウドを実現するにあたり、スケールアウトによるサーバ処理能力増強を踏まえ設定すること。	2-5	サーバ処理能力増強（スケールアップ）	仮想化基盤で要求される処理能力やデータ容量に応じて、適宜ハードウェアの処理能力やストレージ容量を拡張できること。
					2-6	サーバ処理能力増強（スケールアウト）	
3	運用・保守性	システムの運用及び保守に関する要求	通常運用	■運用時間の規定 通常運転は 24時間稼働を基本とすること。但し、法定点検やパッチ適用など、予め定められた計画に沿って稼働を停止する場合を除く。 計画停止は、搭載システムの計画に影響を考慮して、十分余裕をもって計画すること。 ■通常運用の要求設定 バックアップ、システム稼働監視、パッチ適用など、運用項目ごとの自動化範囲や対応頻度（パッチ適用の緊急対応実施有無を含む）を設定すること。設定にあたっては、搭載する業務システムの運用との役割分担に着目して整理すること。 ■監視対象の具体化 共通基盤では情報システムの構成要素全体をまとめて監視することを想定しているため、通常運用に関する要求のうち、特に監視対象の範囲については、業務システムの稼働監視やOS等のプロセス監視など具体的な監視対象を含めて明確にすること。	3-1	運用時間（平日）	開庁時間を前提とし（8時～18時）までの利用を想定しているが、繁忙期などに運用時間の延長が可能であること。
					3-2	運用時間（休日等）	週末は原則利用しないことを想定。 ※将来的に休日に開庁することなども想定されている。休日に開庁する際にも対応が可能であること。
					3-3	データ復旧の対応範囲	障害発生時に決められた復旧時点（RPO）へデータ回復ができること。
					3-4	バックアップ自動化の範囲	定期的なバックアップ処理は自動化すること。
					3-5	バックアップ取得間隔	※仮想化基盤のハードウェア構成により異なる。 日次で取得すること。
					3-6	監視情報	仮想化基盤の安定的な運用を維持するために必要な情報（システムログ等）を監視すること。
					3-7	システムレベルの監視	※仮想化基盤のハードウェア、アプリケーション構成で異なる。 仮想化基盤の安定的な運用を維持するために必要な情報（システムログ等）を監視すること。
					3-8	プロセスレベルの監視	
					3-9	データベースレベルの監視	
					3-10	ストレージレベルの監視	
					3-11	サーバ（ノード）レベルの監視	
					3-12	ネットワーク・パケットレベルの監視	
					3-13	時刻同期設定の範囲	庁内のNTPサーバと同期を行うこと。
					3-14	OS等パッチ適用タイミング	OS等パッチ適用タイミングは、月次で公開される情報に基づき適用の要否を判断し、必要に応じて適用すること。 また、適用に際してWSUSなどのパッチ適用の仕組みを用意すること。
			障害時運用	■障害時運用の目標設定 障害事象発生から所定の担当者への通知に要する時間、駆けつけに要する時間、障害検知後に所管所属へ通知するまでの時間について、定量的な数値目標を設定すること。	3-15	対応可能時間	24時間365日とする。
					3-16	駆けつけ到着時間	異常検知から4時間以内とする。 ※駆けつけが必要と判断された場合。
					3-17	障害検知通知時間	業務継続が難しい場合のみ、分かり次第速やかに通知すること。

No.	要求分類		要求項目	非機能要求	No.	項目名	要求事項
			運用環境	■マニュアル整備レベル 開発業者以外のシステム事業者がシステム運用を行えるように通常運用、保守運用のマニュアルを整備すること。 操作マニュアル等のドキュメント類は、可読性の高さ（職員にとってのわかりやすさ）に特に配慮して作成すること。 ■外部システムとの接続要求 基本的には、各業務システムの間の連携を中継する役割を持つ。 印刷データを印刷業者に渡すなど外部とのやり取りが発生する想定の上、要求仕様を設定すること。 ■その他運用環境の要求設定 リモート監視の有無など、システム構築の調達に向けて上記以外に予め設定すべき項目があれば、該当する項目とその要求仕様を設定すること。	3-18	マニュアル準備レベル	仮想化基盤の運用に必要となるマニュアルは全て整備すること。
					3-19	リモート操作時の接続方法	外部からのリモート操作は行えない設定とすること。
					3-20	外部システムとの接続有無	庁内の外部システムのみ接続できる設定とすること。 ※庁外のシステムとの接続については、業務システムを介した間接的な接続は想定される。
			サポート体制	■保守契約、ライフサイクル期間 機器及びソフトウェアの費用は5年リースとし、5年毎に機器更新を想定している。 ■導入サポート 仮想化基盤は、多数の業務システムが利用又は搭載することから、テスト時、本稼働時の導入サポートを行うこと。 また、サポートは、現地（新潟市役所など）で対応すること。 ■その他サポートの要求設定 一次切り分けの役割分担、報告会の規定など、運用保守事業者のサポート体制に関する要求仕様を設定すること。	3-21	保守契約（ハードウェア）の種類	定額保守（オンサイト）とすること。
					3-22	保守契約（ソフトウェア）の種類	保守契約に基づき、アップデートが提供されること。
					3-23	ライフサイクル期間	本番運用から5年をライフサイクルタイムとすること。
					3-24	一次対応役割分担	運用保守を担当する事業者で対応すること。
					3-25	運用保守事業者側対応時間帯	開庁時間内での対応とすること。
					3-26	定期報告会実施頻度	月1回実施すること。
					3-27	報告内容のレベル	仮想化基盤の運用状況および障害報告等を実施すること。
4	セキュリティ	情報システムの安全性に関する要求	制約条件	■遵守する規定類 次期住記システムの構築や運用を進めるにあたっては、以下に示す規程類を順守すること。 ・新潟市情報セキュリティポリシー ・新潟市個人情報の保護に関する法律施行条例	4-1	順守すべき規程、ルール、法令、ガイドライン等の有無	順守すべき規定類に従い対応すること。
			セキュリティリスク対策	■セキュリティリスク対策の要求設定 セキュリティリスクの分析範囲、Webサーバ等のセキュリティ診断実施有無やウイルス定義ファイルの適用タイミングなど、セキュリティリスク対策に関する要求仕様を明確化すること。また、セキュリティリスク対策の緊急対応の実施有無を定義すること。	4-2	リスク分析範囲	重要度が高い情報資産を扱う範囲および庁外と接続する部分を対象とする。
					4-3	ウイルス定義ファイル適用タイミング	ウイルス定義ファイルは自動で適用されること。
			不正追跡・監視	■アクセスログの記録 不正アクセス発生時の追跡確認などの用途に、いつ・誰が・どの情報を・どうしたかを記録し、閲覧できる仕組みを設けること。 ■不正追跡・監視の要求設定 その他、サーバ等への不正アクセス監視など、新潟市のセキュリティポリシーに従い、必要な不正追跡・監視の要求を設定すること。	4-4	ログの取得	セキュリティインシデントが発生した際に、「いつ」「誰が」「どこから」「何を実行したか」が確認できるログを取得すること。
					4-5	不正監視対象（装置）	重要度が高い情報資産を扱う範囲および庁外と接続する部分を対象とすること。
5	システム環境	情報システムの設置環境等に関する要求	制約条件	■制約条件の要求設定 情報システムの設置環境に関して、庁内基準や法令、各地方公共団体の条例などの制約がある場合、その要求を明確化すること。	5-1	構築時の制約条件	構築時の制約条件となる情報については、別紙で提供すること。

No.	要求分類		要求項目	非機能要求	No.	項目名	要求事項
					5-2	運用時の制約条件	運用時の制約条件となる情報については、別途提供すること。