【We

添付3. 非機能要件一覧

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
1	可用性	継続性	運用スケジュール	システムの稼働時間や停止運用に関する情報	運用時間（通常）	システム基盤の運用時間としては、24時間稼働の想定とする。オンライン提供時間については各業務システムの要件に依る。	24時間稼働を想定する。
2					運用時間（特定日）	特定日は設けない。24時間稼働を想定する。	特定日は設けない。24時間稼働を想定する。
3					計画停止の有無	予め定められた計画に沿って稼働を停止することは許容する。	予め定められた計画に沿って稼働を停止することは許容する。
4			業務継続性	可用性を保証するにあたり、要求される業務の範囲とその条件	対象業務範囲	【災害等、非常時業務機能の利用が求められる事態の発生時】 非常時業務機能は「証明書発行業務」に限定する。 【本番環境の長時間メンテナンス時】 本番予備環境を利用してすべてのオンラインおよびバッチ機能を対象とする。	特に定義しない。
5					サービス切替時間	【災害等、非常時業務機能の利用が求められる事態の発生時】 ・非常時環境利用への自動的な切替は行わない。切替にあたっては、許可含めて、手順に沿って切替を行う。災害等、非常時業務機能の利用が求められる事態が発生してから、サービスを切り替えるまでの時間を12時間以内とする。なお、インフラとしての切替時間は4時間以内（切り戻し時間は8時間以内）とする。 【本番環境の長時間メンテナンス時】 長時間メンテナンス開始前に本番環境から本番予備環境への切替を実施する。インフラとしての切替時間は2時間以内（切り戻し時間は4時間以内）とする。	特に定義しない。
6					業務継続の要求度	【災害等、非常時業務機能の利用が求められる事態の発生時】 ・非常時業務機能の利用が可能な場合、12時間以内に当日始業時時点のデータを利用して、DB更新を伴わない機能を対象として業務が継続できること。 ただし、特定の業務を行ったことを記録する目的での履歴については上記の例外とする。（例：証明書発行履歴、市民情報アクセスログ） 【本番環境の長時間メンテナンス時】 本番予備環境の利用が可能な場合、長時間メンテナンス開始前のデータを利用して、すべてのオンラインおよびバッチ機能を対象として業務が継続できること。	特に定義しない。
7			目標復旧水準（業務停止時）	業務停止を伴う障害が発生した際、何をどこまで、どれ位で復旧させるかの目標	RPO（目標復旧地点）	非常時業務機能で提供するデータは、当日始業時時点のものとする。	パブリックゾーン及びシェアードゾーンのデータは1営業日前の時点（日次バックアップからの復旧）とする。 また、本市の指定するタイミング（システム変更前後、等）で、IaaS型モデルの範囲を含めてシステムバックアップを取得し、利用者が使用できるように復旧できること。なお、プロビジョニング機能により復旧が可能な場合は、システムバックアップの取得は必須ではない。
8					RTO（目標復旧時間）	非常時業務機能を利用して、災害等発生から12時間以内に当日始業時時点のデータを利用して、DB更新を伴わない機能を対象として業務が継続できること。 ただし、特定の業務を行ったことを記録する目的での履歴については上記の例外とする。（例：証明書発行履歴、市民情報アクセスログ）	1営業日以内とする。
9					RLO（目標復旧レベル）	非常時業務機能を利用して、災害等発生から12時間以内に当日始業時時点のデータを利用して、DB更新を伴わない機能を対象として業務が継続できること。 ただし、特定の業務を行ったことを記録する目的での履歴については上記の例外とする。（例：証明書発行履歴、市民情報アクセスログ）	取得済みバックアップからのリストアが完了しているレベル、もしくはプロビジョニング機能により利用者が使用できる状態となっているレベルとする。

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
10			目標復旧水準（大規模災害時）	大規模災害が発生した際、どれ位で復旧させるかの目標	システム再開目標	■システム損害規模によって、以下の通り規定する。 【ライフライン（通信及び電気）の停止】 【設備（電源、空調など）の損壊】 ・上記の場合、7日～10日とする。 【基幹系情報システムの全壊または半壊】 ・2ヶ月～3ヶ月とする。 【札幌市施設①全壊】 ・3ヶ月～4ヶ月とする。	1ヶ月以内とする。
11			稼働率	明示された利用条件の下で、システムが要求されたサービスを提供できる割合	稼働率	計画メンテナンス時間帯を除く、閉局時間（バッチ処理、バックアップ処理、等）を含めた時間を稼働時間とし、次期インフラでは稼働率を99.9%とする。	計画メンテナンス時間帯を除き、99.9%とする。
12		耐障害性	サーバ	サーバで発生する障害に対して、要求されたサービスを維持するための要求	冗長化（機器）	基幹業務を継続するために必要な全てのサーバを冗長化する。	特に要件としない。前述の「稼働率」を満たすレベルとする。
13					冗長化（コンポーネント）	前述の「稼働率」を満たすレベルとする。用途に応じて、RAID1、RAID5、RAID6、RAID10から最適なレベルを選択可能とする。	同上
14					負荷分散方式	【WebAP兼バッチサーバ】 前段に配置する負荷分散機能による負荷分散方式とする。 【認証サーバ（リバプロサーバ、ユーザ検証サーバ）】 前段に配置する負荷分散機能による負荷分散方式とする。 【DBサーバ】 Oracle RAC(Real Application Clusters)を導入する。 【帳票サーバ】 アプリケーションフレームワークによる負荷分散方式とする。 【VDIサーバ】 利用製品で推奨される負荷分散方式とする。 【システム間連携サーバ】 前段に配置する負荷分散機能による負荷分散方式とする。 【外部連携サーバ】 OS・クラスタソフトウェア(ミドルウェア)によるフェイルオーバー方式とする。 【Webサーバ】 OS・クラスタソフトウェア(ミドルウェア)によるフェイルオーバー方式とする。 【ジョブコントロールサーバ】 OS・クラスタソフトウェア(ミドルウェア)によるフェイルオーバー方式とする。 【クライアント管理サーバ】 マスタスレーブ方式とする。 【その他のサーバ】 OS・クラスタソフトウェア(ミドルウェア)によるフェイルオーバー方式とする。	同上
15			端末	端末で発生する障害に対して、要求されたサービス	冗長化（機器）	共用の予備端末を用意し、故障時にすぐ入れ替えが可能な状態・管理とする。	同上

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
16				を維持するための要求	冗長化（コンポーネント）	端末の内蔵ディスク、電源、FAN、ネットワークカードの冗長化は要件としない。	同上
17			ネットワーク機器	ルータやスイッチなどネットワークを構成する機器で発生する障害に対して、要求されたサービスを維持するための要求	冗長化（機器）	全ての機器を冗長化する。	同上
18					冗長化（コンポーネント）	同上	同上
19			ネットワーク	ネットワークの信頼性を向上させるための要求。	回線の冗長化	基幹系サーバは回線が二重化されていること。 外部との接続点について、LAN回線は二重化されていること。WAN回線の冗長化は要件としない。	同上
20					経路の冗長化	基幹系サーバは回線が二重化されていることを前提として、経路の冗長化は行わない。	同上
21					セグメント分割	各サーバ間のトラフィック特性に基づいて、適切に分割すること。	ゾーニング（パブリックゾーン、プライベートゾーン、シェアードゾーン）の考え方を考慮の上、利用目的に応じて適切に分割すること。
22			ストレージ	ディスクアレイなどの外部記憶装置で発生する障害に対して、要求されたサービスを維持するための要求	冗長化（機器）	ストレージ機器の冗長化は要件としない。	特に要件としない。前述の「稼働率」を満たすレベルとする。
23					冗長化（コンポーネント）	コントローラ、電源、FAN、インターフェースなど機器内のすべてのコンポーネントの冗長化を行う。	同上
24					冗長化（ディスク）	用途に応じて、RAID1、RAID5、RAID6、RAID10から最適なレベルを選択可能とする。	同上
25			データ	データの保護に対しての考え方	バックアップ方式	データベースを停止せずにバックアップが可能な「オンラインバックアップ方式」とする。なお、データベースのロギング方式は、現行を踏襲し以下の環境についてはアーカイブロギング方式と想定する。 ・本番環境 ・リリース確認環境	オンラインバックアップを原則とするが、1時間以内のオフラインバックアップも許容する。
26					データ復旧範囲	以下の環境については、障害発生直前にコミットしたデータを復旧できるようにする。 ・本番環境 ・リリース確認環境 その他の環境やデータベース以外のデータ（例：リソースデータサーバ上の資源）については、前回バックアップ取得時点に復旧できるようにする。	シェアードゾーン及びパブリックゾーンのデータとする。
27					データインテグリティ	バックアップ時点でのデータインテグリティを保証すること。製品で対応できるレベルを想定している。	特に要件としない。
28		災害対策	システム	地震、水害、テロ、火災などの大規模災害時の業務継続性を満たすための要求	復旧方針	■非常時機能の利用により業務継続性を担保する。 ■システム損害規模によって、以下の通り復旧時間を想定し再構築を行う。 【ライフライン（通信及び電気）の停止】 【設備（電源、空調など）の損壊】 ・上記の場合、7日～10日とする。 【基幹系情報システムの全壊または半壊】 ・2ヶ月～3ヶ月とする。 【札幌市施設①全壊】 ・3ヶ月～4ヶ月とする。	特に要件としない。
29			外部保管データ	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、	保管場所分散度	遠隔地（1箇所）とする。	同上

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
30				データ・プログラムを運用サイトと別の場所へ保管するなどの要求	保管方法	ネットワークを利用して遠隔地（1箇所）へリモートバックアップを行う。	同上
31			付帯設備	各種災害に対するシステムの付帯設備での要求	災害対策範囲	札幌市施設①・札幌市施設②は必要な付帯設備が備わっていることとする。	日本データセンター協会制定のデータセンターファシリティスタンダードのティア3を満たすこと。
32		回復性	復旧作業	業務停止を伴う障害が発生した際の復旧作業に必要な労力	復旧作業	■システム損害規模によって、以下の復旧作業を実施すること。 【設備（電源、空調など）の損壊】 ・インフラ提供サービスの復旧確認 【ライフライン（通信及び電気）の停止】 ・インフラ提供サービスの復旧確認 【基幹系情報システムの全壊または半壊】 ・ハードウェア等の資源調達 ・セットアップ（据付調整など） ・データのリストア ・インフラ提供サービスの復旧確認 【札幌市施設①全壊】 ・ハードウェア等の資源調達 ・セットアップ（据付調整など） ・データのリストア ・インフラ提供サービスの復旧確認	特に要件としない。前述の「RTO」を満たすこと。
33					代替業務運用の範囲	「証明書発行業務」に限る。 ただし、特定の業務を行ったことを記録する目的での履歴については上記の例外とする。 (例：証明書発行履歴、市民情報アクセスログ) 上記制約内で、各業務システムがその範囲を明示的に定義すること。	特に定義しない。
34			可用性確認	可用性として要求された項目をどこまで確認するかの範囲	確認範囲	・札幌市施設内及び遠隔地に保管しているバックアップデータを使用したデータのリストア ・冗長化構成の各種機器の片側機器がダウンした際に正常に動作継続 ・非常時業務機能環境への正常切替 ・本番予備環境への正常切替 ・外部へのネットワークアクセスが不可能となった際の代替手段の正常動作 ・人事異動及び組織変更に伴う関係連絡先、要員連絡先情報 ・災害復旧作業時に必要となるドキュメントの保管場所	対象を限定した取得済みバックアップからのリストアを範囲とする。確認対象は別途本市が指定する。
35		信頼性	排他制御	システム内でデータベース等のデータ更新以外で特別な排他制御を行う必要がある場合、その内容を定義する	その他の排他制御	画面遷移をまたがる業務的な排他制御は行わない。	特に要件としない。
36		トランザクション	トランザクション単位	システムでトランザクションとして整合性を保護する粒度を定義する		一連の業務的に不可分な機能を「サービス」と定義し、この単位でトランザクション制御を行う。	特に要件としない。

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
37			トランザクション管理主体(トランザクション境界)	トランザクションを開始・終了する主体を定義する。開発対象以外の部分でトランザクションの管理を行っているものがあればその内容と連携方法を定義する		トランザクションの開始・終了は業務側の宣言的な設定に基づき、基盤フレームワークが自動的に制御する。	同上
38			トランザクション分離レベル	並行に動作するトランザクション間の分離レベルを定義する		READ_COMMITTEDとする(コミットされていない別トランザクションのデータは不可視とする)。	同上
39			2PCの必要有無	トランザクション対象が単一のリソースかどうか、複数リソース、複数トランザクションマネージャが存在するかどうかを定義する		2フェーズコミットは使用しない。	同上
40	性能・拡張性	業務処理量	通常時の業務量	性能・拡張性に影響を与える業務量	ユーザ数	現時点での想定ユーザ(エンドユーザ)数は3,500人とする。また、その他に運用保守担当者は200人程度である。	仮想デスクトップ機能を利用するユーザは100人以内とする。その他にファイルサーバ機能へのみアクセスするユーザを50人程度と想定し、合計150人程度と想定している。
41					システム利用特性	次期インフラでは、現行インフラの稼働状況をベースに、本調達仕様書に要件を整理しており、本項目に関して個別に定義することは行わない。	特に定義しない。
42					同時アクセス数	同上	同上
43					データ量	次期インフラでは、現行インフラの稼働状況をベースに、不足状況も踏まえて容量の見積もりを行っている。	「インフラ提供サービス仕様書」に明記する。
44					オンラインリクエスト件数	次期インフラでは、現行インフラの稼働状況をベースに、本調達仕様書に要件を整理しており、本項目に関して個別に定義することは行わない。	特に定義しない。
45					バッチ処理件数	同上	同上
46					業務機能数	同上	同上
47			業務量増大度	システム稼動開始からライフサイクル終了までの間で、開始時点と業務量が最大になる時点の業務量の倍率	ユーザ数増大率	厳密に増大度を算出することはせず、増大度合いに応じて、システムのキャパシティを柔軟に拡張できるようなインフラをサービス提供型で利用する。	特に定義しない。サービス提供型で利用する。
48					同時アクセス数増大率	同上	同上
49					データ量増大率	同上	同上
50					オンラインリクエスト件数増大率	同上	同上
51					バッチ処理件数増大率	同上	同上
52					業務機能数増大率	同上	同上

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
53			保管期間	システムが参照するデータのうち、OSやミドルウェアのログなどのシステム基盤が利用するデータに対する保管が必要な期間	保管期間	ログ保管期間は以下のとおり。 ・リバプロサーバのアクセスログ：1年 ・Linuxサーバのsecureログ、シスログ：180日 ・上記以外のログ：90日 なお、重要な記録やデータの保管期間は、後述の「バックアップ保存期間」を参照。	セキュリティの観点で、本環境（ファイルサーバ機能、仮想デスクトップ機能、等）に対するアクセスログを1年保管すること。
54					対象範囲	同上	同上
55		性能目標値	オンラインレスポンス	オンラインシステム利用時に要求されるレスポンス	通常時レスポンス時間及び遵守率	現行システムから変更がないことを想定する。	特に要件としない。
56					ピーク時レスポンス時間及び遵守率	同上	同上
57					縮退時レスポンス時間及び遵守率	同上	同上
58			バッチレスポンス（ターンアラウンドタイム）	バッチシステム利用時に要求されるレスポンス	通常時レスポンス順守度合い	現行システムから変更がないことを想定する。	同上
59					ピーク時レスポンス順守度合い	同上	同上
60					縮退時レスポンス順守度合い	同上	同上
61			オンラインスループット	オンラインシステム利用時に要求されるスループット	通常時処理余裕率	アプローチとして、現行インフラの稼働状況をベースに、本調達仕様書に要件を整理しており、本項目に関して個別に定義することは行わない。	同上
62					ピーク時処理余裕率	同上	同上
63					縮退時処理余裕率	同上	同上
64			バッチスループット	バッチシステム利用時に要求されるスループット	通常時処理余裕率	同上	同上
65					ピーク時処理余裕率	同上	同上
66					縮退時処理余裕率	同上	同上
67			帳票印刷能力	帳票印刷に要求されるスループット	通常時印刷余裕率	同上 ※現行システムでは、一部のシステムの繁忙期に帳票サーバのCPUを100%消費する課題があった。次期システムでは、帳票サーバを住記系、税系、保険・福祉系と区分けすることなくプール化することで解決を図る。	同上
68					ピーク時印刷余裕率	同上	同上
69					縮退時印刷余裕率	同上	同上
70		リソース拡張性	CPU拡張性	CPUの拡張性を確認するための項目	CPU利用率	50%以上80%未満	同上
71					CPU搭載余裕有無	拡張方式（スケールアウト・スケールアップ）は指定しない。	同上

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
72			メモリ拡張性	メモリの拡張性を確認するための項目	メモリ利用率	50%以上80%未満	同上
73					メモリ搭載余裕有無	拡張方式（スケールアウト・スケールアップ）は指定しない。	同上
74			ディスク拡張性	ディスクの拡張性を確認するための項目	ディスク利用率	50%以上80%未満	同上
75					ディスク増設余裕有無	拡張方式（スケールアウト・スケールアップ）は指定しない。	同上
76			ネットワーク	システムで使用するネットワーク環境の拡張性に関する項目	ネットワーク機器設置範囲	インフラ提供サービス仕様書に記載のとおり。	同上
77			サーバ処理能力増強	サーバ処理能力増強方法に関する項目	スケールアップ	拡張方式（スケールアウト・スケールアップ）は指定しない。	拡張方式（スケールアウト・スケールアップ）は指定しない。
78					スケールアウト	拡張方式（スケールアウト・スケールアップ）は指定しない。	拡張方式（スケールアウト・スケールアップ）は指定しない。
79		性能品質保証	帯域保証機能の有無	ネットワークのサービス品質を保証する機能の導入要否およびその程度	帯域保証の設定	LAN内においては、論理環境及び論理サーバごとに帯域制御が可能なこと。 WANとの入出力の帯域については、本市用途で利用できる最大帯域幅：100Mbps以上とする。	各論理サーバ及びストレージサービスには、最大帯域幅：1,000Mbps以上、最大IOPS：8,000以上を備えること。 WANとの入出力の帯域については、本市用途で利用できる最大帯域幅：100Mbps以上とする。
80					ネットワーク帯域使用率	同上	同上
81			性能テスト	構築したシステムが当初/ライフサイクルに渡っての性能を発揮できるかのテストの測定頻度と範囲	測定頻度	次期インフラへのアプリケーション移行時に測定する。	特に要件としない。
82					確認範囲	次期インフラへ移行するすべての機能（アプリケーション）について、目標値を満たしていることを確認する。	同上
83			スパイク負荷対応	通常時の負荷と比較して、非常に大きな負荷が短時間に現れることを指す。業務量の想定されたピークを超えた状態。	トランザクション保護	現行システムでは制限しておらず、次期システムでも制限は行わない。	同上
84	運用・保守性	通常運用	運用時間	システム運用を行う時間（利用者やシステム管理者に対してサービスを提供するために、システムを稼動させ、オンライン処理やバッチ処理を実行している時間帯のこと）	運用時間（通常）	インフラとしては24時間稼働可能とする。	インフラとしては24時間稼働可能とする。
85					運用時間（特定日）	特定日として運用時間の条件を変えることは要件としない。	特定日として運用時間の条件を変えることは要件としない。
86			バックアップ	システムが利用するデータのバックアップに関する項目。	データ復旧範囲	OSやミドルウェアに関連したサーバの正常稼働に必要な最低限のファイル・業務アプリケーションの稼働に必要なファイル及び、業務の遂行に必要となるデータ(制御ファイル、表データや表定義も含むデータベースを構成するファイル)とする。	前述の「RPO」のとおり。
87					外部データの利用可否	外部データの利用はできないものとする。	特に要件としない。
88					バックアップ利用範囲	障害発生時のデータ損失防止を利用範囲とする。	前述の「RPO」のとおり。
89					バックアップ自動化の範囲	DBバックアップは、全ステップ自動で行う。 システムバックアップは、数ステップを手動で行う。	特に要件としない。

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
90					バックアップ取得間隔	個別システム単位のバックアップは以下の2つのタイミングで実施する。 [1] 夜間バッチ処理開始前 [2] 夜間バッチ処理終了後 データベース全体のバックアップは、業務終了後の指定時刻（現行システムでは2:00）に実施する。	前述の「RPO」のとおり。
91					バックアップ保存期間	リソースデータサーバ上の画像データ：10年 特定個人情報アクセス記録：7年 個人情報アクセス記録：2年 データベース：前日の業後バッチ終了時点に復旧することができるだけの保存期間	同上
92					バックアップ方式	オンラインバックアップ方式とする。	前述の「バックアップ方式」のとおり。
93			運用監視	システム全体、あるいはそれを構成するハードウェア・ソフトウェア（業務アプリケーションを含む）に対する監視に関する項目	監視情報	インフラサービス提供事業者による監視項目は以下のとおり。 [1] 死活監視、ポート監視 [2] プロセス監視（Windowsサービスを含む） [3] サービス監視（負荷分散機能によるヘルスチェックなどのサービス稼働監視等） [4] ログ監視 [5] ジョブ実行結果取得 [6] 性能監視（応答時間の確認等） [7] リソース監視	インフラサービス提供事業者による監視項目は以下のとおり。 [1] 死活監視、ポート監視 [2] プロセス監視（Windowsサービスを含む） [3] サービス監視（負荷分散機能によるヘルスチェックなどのサービス稼働監視等） [4] ログ監視 [5] ジョブ実行結果取得 [6] 性能監視（応答時間の確認等） [7] リソース監視
94					監視間隔	リアルタイム監視（分間隔） ※詳細は監視項目および監視対象に応じて適切に定義する。	特に要件としない。
95					システムレベルの監視	シナリオベースでの常時監視は実施しない。 ※ただし、負荷分散機能によるヘルスチェックは行う。	特に要件としない。
96					プロセスレベルの監視	実施する。	実施する。
97					データベースレベルの監視	実施する。	実施する。
98					ストレージレベルの監視	実施する。	実施する。
99					サーバ（ノード）レベルの監視	実施する。	実施する。
100					端末/ネットワーク機器レベルの監視	端末レベルの監視は実施しない。 ネットワーク機器レベルの監視は実施する。	特に要件としない。
101					ネットワーク・パケットレベルの監視	パケットロスやネットワーク帯域の使用率などの監視を行う。また、ネットワークへの侵入検知は行わない。	特に要件としない。
102			時刻同期	システムを構成する機器の時刻同期に関する項目	時刻同期設定の範囲	NTPサーバを利用して時刻同期を行うことする。 ※札幌市施設内の機器は既存ネットワーク内にあるNTPサーバを利用する。	NTPサーバを利用して時刻同期を行うことする。
103		保守運用	計画停止	点検作業や領域拡張、デフラグ、マスターデータのメンテナンス等、システム	計画停止の有無	計画停止は許容する。	計画停止は許容する。

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
104				の保守作業の実施を目的とした、事前計画済みのサービス停止に関する項目	計画停止の事前アナウンス	【本番環境】 本番予備環境を利用する場合： ・事前アナウンスの期限は、実施日の前月の初旬とする。 本番予備環境を利用できない場合： ・事前アナウンスの期限は、実施日の3ヶ月前の初旬とする。 【その他の環境】 原則、【本番環境】と同じとする。 なお、計画停止時のシステム停止作業及び起動作業は2時間以内に完了すること。論理サーバ及び機器等の停止順及び起動順は、依存性を考慮のうえ、設計時に十分検討し、作業が正確かつ迅速に行えるように仕組みや手順書を整備すること。	事前アナウンスの期限は、実施日の2週間前とする。
105			運用負荷削減	保守運用に関する作業負荷を削減するための設計に関する項目	保守作業自動化の範囲	一部の保守作業を自動で実行する。	特に要件としないが、一部の保守作業を自動で実行することを想定している。
106					サーバソフトウェア更新作業の自動化	サーバ機器OSやストレージのファームウェア、サーバ機器上で動作するミドルウェアなどの自動更新は想定していない。	特に要件としないが、自動更新は想定していない。自動更新が行われて利用に支障が出る場合には更新前の状態に復元することを想定している。
107					端末ソフトウェア更新作業の自動化	以下の配布・更新の自動化を行う。 ・Windowsセキュリティパッチ ・AdobeReader等のソフトウェアのアップデート ・フォントの配布 ・ウィルス対策SWの検索エンジン・パターンファイルの配布 ・プリントキャプチャツールの配布 ・SSL証明書（ルート証明書）の配布 など	特に要件としないが、仮想デスクトップに対する更新の自動化を想定している。
108			パッチ適用ポリシー	パッチ情報の展開とパッチ適用のポリシーに関する項目	パッチリリース情報の提供	システム稼働に影響を与える重要問題が判明した場合、1ヶ月以内にインフラサービス提供事業者が運用保守担当者に連絡すること。	特に要件とはしないが、オンプレ型モデル側のパッチレベルに維持されることを想定している。オンプレ型モデル側のパッチレベルと相違が発生し利用に支障が出る場合には、オンプレ型モデル側のパッチレベルに合わせることを想定している。
109					パッチ適用方針	パッチ内容に応じて、運用保守担当者が判断すること。実質的な効果が得られないにも関わらず、最新化を目的とした適用は行わない。	同上
110					パッチ適用タイミング	パッチ内容に応じて、運用保守担当者が判断すること。	同上
111					パッチ検証の実施有無	本番環境適用前に、リリース確認環境等への適用・検証を行うこと。詳細は、変更・リリース管理手順に則る。	同上
112			活性保守	サービス停止の必要がない活性保守が可能なコンポーネントの範囲	ハードウェア活性保守の範囲	業務の稼働に影響を与える機器は原則活性保守が可能なこと。「活性保守」とは、装置が動作している状態のまま内部の部品を取り外して交換することが可能なことを指す。 なお、同一用途の複数サーバ機器については、そのサーバ機器上で稼働する仮想サーバを稼働させたまま別のサーバ機器に移動するなどして、業務稼働に影響を与えずに1台ずつ停止することが可能な場合は、活性保守を必須としない。 保守目的の計画メンテナンスに伴う業務停止時間は最大6時間（基本的に3時間）以内とし、事前に本市と合意すること。	特に要件としない。前述の「稼働率」を満たすレベルとする。

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
113					ソフトウェア活性保守の範囲	ソフトウェアの活性保守の例はローリングアップグレードとなるが、原則ローリングアップグレード対応が可能であること。 保守目的の計画メンテナンスに伴う業務停止時間は最大6時間（基本的に3時間）以内とし、事前に本市と合意すること。	同上
114			定期保守頻度	システムの保全のために必要なハードウェアまたはソフトウェアの定期保守作業の頻度	定期保守頻度	ハードウェアの定期保守を対象として、年1回とする。	特に要件としないが、年1回程度を想定している。
115			予防保守レベル	システム構成部材が故障に至る前に予兆を検出し、事前交換などの対応をとる保守	予防保守レベル	SNMPトラップ等で故障の予兆を検出し、事前交換などの対応をとる。なお、目視確認については、札幌市施設①設置機器は毎日1回実施し、札幌市施設②設置機器は、定期点検時に確認することとする。	特に要件とはしないが、故障の予兆を検出できることを想定している。
116		障害時運用	復旧作業	業務停止を伴う障害が発生した際の復旧作業に必要な労力	復旧製品の使用有無	復旧製品を使用することが想定されるが、復旧製品に対する特別な要件はない。	特に要件としない。前述の「稼働率」を満たすレベルとする。
117					自動復旧の可否	自動復旧に活用できる機能についても選択可(各種インフラ構成要素ごとに最適な機能を利用すること)とする。	特に要件としない。前述の「稼働率」を満たすレベルとする。
118					代替業務運用の範囲	新基幹系情報システムとしての代替業務運用の範囲は、新基幹系情報システム全体とし、代替方法は、「非常時業務システム」とする。 ※但し、非常時業務システムでは、新基幹系情報システム全体を代替するわけではない。代替運用時に必要となる機能は前述のとおり。	定義しない。
119			障害復旧自動化の範囲	障害復旧に関するオペレーションを自動化する範囲に関する項目	障害復旧自動化の範囲	自動復旧に活用できる機能についても選択可(各種インフラ構成要素ごとに最適な機能を利用すること)とする。	特に要件とはしないが、自動復旧に活用できる機能についても選択可(各種インフラ構成要素ごとに最適な機能を利用すること)であることを想定している。
120			システム異常検知時の対応	システムの異常を検知した際のベンダ側対応についての項目	対応可能時間	【ハードウェア】 本番環境および本番環境リソース共有範囲における本番環境の範囲は、24H365日対応とする。その他は、この限りではない。 【ソフトウェア】 平日9:00～17:00の問合せ対応を原則として、本番環境における業務稼働上最重要なソフトウェア(Oracle Database)は、24H365日対応可能とする。	特に要件としない。前述の「稼働率」を満たすレベルとする。
121					駆けつけ到着時間	午前8:45から午後7:30まで（土日祝は除く）は、インシデント（障害）発生から1分以内に着手できること。 上記以外の時間帯は、インシデント（障害）発生時、または札幌市運用体制からの連絡があり、対応が必要な場合は、概ね1時間を目安に札幌市運用執務室に駆けつけて作業に着手できること。	同上
122					SE到着平均時間	前述の「駆けつけ到着時間」のとおり。	同上
123			交換用部材の確保	障害の発生したコンポーネントに対する交換部材の確保方法	保守部品確保レベル	前述の「稼働率」を満たすレベルとする。	同上
124					予備機の有無	前述の「稼働率」を満たすレベルとする。	同上
125		運用環境	開発用環境の設置	ユーザがシステムに対する開発作業を実施する目的で導入する環境についての項目	開発用環境の設置有無	本番環境とは別に開発環境を用意する。	特に要件としない。本環境が開発用環境そのものである

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
126			試験用環境の設置	ユーザがシステムの動作を試験する目的で導入する環境についての項目	試験用環境の設置有無	本番環境とは別にリリース確認環境を用意する。	特に要件としない。本環境が試験用環境そのものである
127			マニュアル準備レベル	運用のためのマニュアルの準備のレベル	マニュアル準備レベル	現行のインフラ運用手順書と同等のレベルに加えて、障害発生時の一次対応等のインフラ保守に関する手順書を作成すること。	特に要件としない。サービスメニューのサービスレベルを満たすこと。
128			リモートオペレーション	システムの設置環境とは離れた環境からのネットワークを介した監視や操作の可否を定義する項目	リモート監視地点	札幌市施設外から札幌市施設内へのリモート監視は許可しない。札幌市施設内から札幌市施設外へは障害時の発報のみを許可する。	適切なセキュリティレベルを確保することを前提にリモート監視を許可する。
129					リモート操作の範囲	札幌市施設外から札幌市施設内へのリモート操作は許可しない。基本的に常駐SEによる対応とする。	適切なセキュリティレベルを確保することを前提にリモート操作を許可する。
130			外部システム接続	システムの運用に影響する外部システムとの接続の有無に関する項目	外部システムとの接続有無	外部システムとの連携は存在する。	札幌市施設①及び基幹系情報システム関係者の各拠点との接続が存在する。
131					監視システムの有無	基幹系情報システム内に監視システムを含める。次期インフラ監視機能の新規構築が調達範囲に含まれている。	インフラ監視機能が含まれる。
132					ジョブ管理システムの有無	基幹系情報システム内にジョブ管理システムを含める。次期インフラジョブ管理機能の新規構築が調達範囲に含まれている。	スケジューラー機能が含まれる。
133		サポート体制	保守契約（ハードウェア）	保守が必要な対象ハードウェアの範囲	保守契約（ハードウェア）の範囲	インフラサービス提供事業者が導入した全製品を保守範囲とする。	インフラサービス提供事業者が導入した全製品を保守範囲とする。
134			保守契約（ソフトウェア）	保守が必要な対象ソフトウェアの範囲	保守契約（ソフトウェア）の範囲	同上	同上
135			ライフサイクル期間	運用保守の対応期間および、実際にシステムが稼動するライフサイクルの期間	ライフサイクル期間	原則5年間とする。	原則5年間とする。
136			メンテナンス作業役割分担	メンテナンス作業に対するユーザ/ベンダの役割分担、配置人数に関する項目	メンテナンス作業役割分担	「運用・保守管理プロセスポリシー」および「運用・保守管理プロセス基準書」に準ずる。 インフラサービス提供事業者が導入した全製品を対象に、現状「業務運用保守業者」がアプリケーションの範囲に対して担う役割と同じ役割とする。	導入したすべての範囲を対象にインフラサービス提供事業者の担当とする。実施に当たっては本市と事前に調整を行うこと。
137			一次対応役割分担	一次対応のユーザ/ベンダの役割分担、一次対応の対応時間、配備人数	一次対応役割分担	「運用・保守管理プロセスポリシー」および「運用・保守管理プロセス基準書」に準ずる。 インフラサービス提供事業者が導入した全製品を対象に、現状「業務運用保守業者」がアプリケーションの範囲に対して担う役割と同じ役割とする。 なお、一次対応は1時間以内とする。	同上
138			サポート要員	サポート体制に組み入れる要員の人数や対応時間、スキルレベルに関する項目	ベンダ側常備配備人数	サービス提供型のため、人数は定義しない。	サービス提供型のため、人数は定義しない。
139					ベンダ側対応時間帯	前述の「駆けつけ到着時間」で定義する。	特に要件としない。前述の「稼働率」を満たすレベルとする。
140					ベンダ側対応者の要求スキルレベル	運用保守範囲の製品の専門家として、システムの運用や保守作業手順に習熟し、ハードウェアやソフトウェアのメンテナンス作業を実施できる。	運用保守範囲の製品の専門家として、システムの運用や保守作業手順に習熟し、ハードウェアやソフトウェアのメンテナンス作業を実施できる。
141					エスカレーション対応	「運用・保守管理プロセスポリシー」および「運用・保守管理プロセス基準書」に準ずる。 インフラサービス提供事業者が導入した全製品を対象に、現状「業務運用保守業者」がアプリケーションの範囲に対して担う役割と同じ役割とする。	サービス提供事業者内で適切にエスカレーション対応することを前提とし、本市の窓口は常駐SEとする。

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
142			導入サポート	システム導入時の特別対応期間の有無および期間	システムテスト稼働時の導入サポート期間	システムテスト期間はインフラサービス提供事業者が対応を行う。	システムテスト期間はインフラサービス提供事業者が対応を行う。
143					システム本稼働時の導入サポート期間	システム本稼働後はインフラサービス提供事業者が保守・運用を実施する。	システム本稼働後はインフラサービス提供事業者が保守・運用を実施する。
144			オペレーション訓練	オペレーション訓練実施に関する項目	オペレーション訓練実施の役割分担	運用保守担当者およびインフラサービス提供事業者（委託先）が協力して実施する。なお、インフラサービス提供事業者が積極的な姿勢で実施することを求める。	特に要件としない。
145					オペレーション訓練範囲	「添付6. サービスメニュー一覧」を対象範囲とする。	同上
146					オペレーション訓練実施頻度	運用体制立ち上げ時および、要員交代時に実施する。ただし、最低、年に一度、インフラサービス提供事業者主導で以下の訓練を実施すること。 ・非常時機能環境への切替、切り戻し ・本番予備環境への切替、切り戻し ・バックアップデータからのシステム復旧	同上
147			定期報告会	保守に関する定期報告会の開催の要否	定期報告会実施頻度	月1回を原則とする。	月1回を原則とする。
148					報告内容のレベル	「添付6. サービスメニュー一覧」で定義する報告内容とする。	「添付6. サービスメニュー一覧」で定義する報告内容とする。
149		ライセンス管理	ライセンス費用	ライセンスに必要な維持コストの制約を定義する		特に要件としない。	特に要件としない。
150			ソフトウェアライセンス	ソフトウェアライセンスの管理について特記すべき要求があれば定義する		同上	同上
151			ハードウェアサポートライセンス	ハードウェアサポートライセンスの管理について特記すべき要求があれば定義する		同上	同上
152			SSLサーバ証明書	SSL証明書に求める要件があれば定義する。例えば、EVSSLが必須である、等		札幌市施設内では、システムで利用するSSLサーバ証明書は、新基幹系情報システム内の認証局から発行されるものを利用すること。 以下の範囲については用途に応じて適切な証明書を利用する。 [1] 外部接続（例：自治体中間サーバ接続端末） [2] 外部DC 受託するインフラサービス提供事業者は、[2]の証明書を提供すること。	特に要件としないが、インフラ提供サービス仕様書における暗号化を求める範囲において、SSLを使用する場合は、用途に応じて適切な証明書を利用すること。
153			クライアント証明書	クライアント証明認証を使用する場合は、認証局の運営ポリシーを定義する		新基幹系情報システム利用のためにクライアント証明書は使用しない。	同上
154		変更容易性	制度変更	法改正などの制度変更時に、システム改修に対する弾力性について要件を定義する。		定義しない。制度変更に応じて、システムのキャパシティ等を柔軟に拡張できるようなインフラをサービス提供型で利用する。	定義しない。制度変更に応じて、システムのキャパシティ等を柔軟に拡張できるようなインフラをサービス提供型で利用する。
155		その他の運用管理方針	内部統制対応	IT運用プロセスの内部統制対応を行うかどうかに関する項目	内部統制対応の実施有無	定義しない。	定義しない。

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
156			サービスデスク	ユーザの問合せに対して単一の窓口機能を提供するかどうかに関する項目	サービスデスクの設置有無	サービスメニューの「ヘルプデスク」で対応する。	サービスメニューの「ヘルプデスク」で対応する。
157			インシデント管理	業務を停止させるインシデントを迅速に回復させるプロセスを実施するかどうかに関する項目	インシデント管理の実施有無	実施する。「運用・保守管理プロセスポリシー」および「運用・保守管理プロセス基準書」に準ずる。 インフラサービス提供事業者が導入した全製品を対象に、現状「業務運用保守業者」がアプリケーションの範囲に対して担う役割と同じ役割とする。	実施する。「運用・保守管理プロセスポリシー」および「運用・保守管理プロセス基準書」に準ずる。 インフラサービス提供事業者が導入した全製品を対象に、現状「業務運用保守業者」がアプリケーションの範囲に対して担う役割と同じ役割とする。
158			問題管理	インシデントの根本原因を追究し、可能であれば取り除くための処置を講じるプロセスを実施するかどうかに関する項目	問題管理の実施有無	同上	同上
159			構成管理	ハードウェアやソフトウェアなどのIT環境の構成を適切に管理するためのプロセスを実施するかどうかに関する項目	構成管理の実施有無	同上	同上
160			変更管理	IT環境に対する変更を効率的に管理するためのプロセスを実施するかどうかに関する項目	変更管理の実施有無	同上	同上
161			リリース管理	ソフトウェア、ハードウェア、ITサービスに対する実装を管理するためのプロセスを実施するかどうかに関する項目	リリース管理の実施有無	同上	同上
162	移行性	移行時期	移行のスケジュール	移行作業計画から本稼働までのシステム移行期間、システム停止可能日時、並行稼働の有無 （例外発生時の切り戻し時間や事前バックアップの時間等も含むこと）	システム移行期間	平成30年度本番環境の移行期間については現在計画中。（移行期間を確保するため、三連休以上を想定） 詳細は「移行方針書」および「移行計画書」にて定義する。	「移行方針書」および「移行計画書」にて定義する。
163					システム停止可能日時	平成30年度は、10/6～8 を想定する。 なお、コンテンジェンシー発動時は 11月を想定する。	同上
164					並行稼働の有無	本番環境にて業務を並行稼働することはない。 現行インフラのステージング環境と、次期インフラのステージング環境に相当する環境については、並行稼働を想定する。	同上
165		移行方式	システム展開方式	システムの移行および新規展開時に多段階による展開方式をどの程度採用するかの程度。	拠点展開ステップ数	「移行方針書」および「移行計画書」にて定義する。	同上
166					業務展開ステップ数	同上	同上
167		移行対象（機器）	移行設備	移行前のシステムで使用していた設備において、新システムで新たな設備に入れ替え対象となる移行対象設備の内容	設備・機器の移行内容	同上	同上

No.	非機能項目					次期インフラ〔オンプレ型モデル〕	次期インフラ〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
168		移行対象（データ）	移行データ量	旧システム上で移行の必要がある業務データの量（プログラムを含む）	移行データ量	同上	同上
169					移行データ形式	同上	同上
170			移行媒体	移行対象となる媒体の量と移行時に必要となる媒体種類数	移行媒体量	同上	同上
171					移行媒体種類数	同上	同上
172			変換対象（DBなど）	変換対象となるデータの量とツールの複雑度（変換ルール数）	変換データ量	同上	同上
173					移行ツールの複雑度（変換ルール数）	同上	同上
174		移行計画	移行作業分担	移行作業の作業分担	移行のユーザ/ベンダ作業分担	同上	同上
175			リハーサル	移行のリハーサル（移行中の障害を想定したリハーサルを含む）	リハーサル範囲	同上	同上
176					リハーサル環境	同上	同上
177					リハーサル回数	同上	同上
178					外部連携リハーサルの有無	同上	同上
179			トラブル対処	移行中のトラブル時の対応体制や対応プラン等の内容	トラブル対処の規定有無	同上	同上
180	セキュリティ	前提条件・制約条件	情報セキュリティに関するコンプライアンス	ユーザが順守すべき情報セキュリティに関する組織規程やルール、法令、ガイドライン等が存在するかどうかを確認するための項目	順守すべき社内規程、ルール、法令、ガイドライン等の有無	以下の規定に準拠する必要がある。 ・札幌市個人情報保護条例 ・札幌市個人情報保護条例施行規則 ・札幌市公文書管理規則 ・札幌市公用文規程 ・札幌市事務取扱規程 ・札幌市情報公開条例 ・札幌市情報公開条例施行規則 ・札幌市施設①管理要領 ・保守用環境運用管理要領 ・札幌市情報通信ネットワーク運用管理要領 ・札幌市情報化事務取扱要綱 ・札幌市セキュリティポリシー(*) ・危機管理マニュアル(*) ・情報セキュリティ実施手順(*) (*)の資料はセキュリティ上の理由で開示できない資料であるため、別途必要な事項を提示する。	以下の規定に準拠する必要がある。 ・札幌市個人情報保護条例 ・札幌市個人情報保護条例施行規則 ・札幌市公文書管理規則 ・札幌市公用文規程 ・札幌市事務取扱規程 ・札幌市情報公開条例 ・札幌市情報公開条例施行規則 ・札幌市施設①管理要領 ・保守用環境運用管理要領 ・札幌市情報通信ネットワーク運用管理要領 ・札幌市情報化事務取扱要綱 ・札幌市セキュリティポリシー(*) ・危機管理マニュアル(*) ・情報セキュリティ実施手順(*) (*)の資料はセキュリティ上の理由で開示できない資料であるため、別途必要な事項を提示する。
181		セキュリティリスク分析	セキュリティリスク分析	システム開発を実施する中で、どの範囲で対象システムの脅威を洗い出し、影響の分析を実施するかの方針を確認するための項目	リスク分析範囲	調達範囲全体を対象にセキュリティリスク分析を行い、その結果を札幌市に報告すること。運用保守フェーズにおいても、セキュリティリスク分析の見直しと結果の報告を年に1度実施すること。	調達範囲全体を対象にセキュリティリスク分析を行い、その結果を札幌市に報告すること。運用保守フェーズにおいても、セキュリティリスク分析の見直しと結果の報告を年に1度実施すること。
182		セキュリティ診断	セキュリティ診断	対象システムや、各種ドキュメント（設計書や環境定義書、実装済みソフト	ネットワーク診断実施の有無	事前に指定したペネトレーションテストを実施し合格すること。また、その結果を札幌市に報告すること。	事前に指定したペネトレーションテストを実施し合格すること。また、その結果を札幌市に報告すること。

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
183				ウェアのソースコードなど)に対して、セキュリティに特化した各種試験や検査の実施の有無を確認するための項目	Web診断実施の有無	基盤担当者によるソースコードインスペクションで担保する。	基盤担当者によるソースコードインスペクションで担保する。
184					DB診断実施の有無	データベース構築に関するセキュリティ診断は、基盤担当者による設計インスペクションで担保する。SQLに関するセキュリティ診断は、アプリケーションFWで提供するSQLインジェクションが適切に利用されていることを、ソースコードインスペクションで担保する。 不正・不審操作に関するセキュリティ診断は、DBMS固有のログ出力機能を用いてアクセスを監視する。	データベース構築に関するセキュリティ診断は、基盤担当者による設計インスペクションで担保する。SQLに関するセキュリティ診断は、アプリケーションFWで提供するSQLインジェクションが適切に利用されていることを、ソースコードインスペクションで担保する。 不正・不審操作に関するセキュリティ診断は、DBMS固有のログ出力機能を用いてアクセスを監視する。
185		セキュリティリスク管理	セキュリティリスクの見直し	対象システムにおいて、運用開始後に新たに発見された脅威の洗い出しとその影響の分析をどの範囲で実施するかを確認するための項目	セキュリティリスク見直し頻度	前述の「セキュリティリスク分析」のとおり。	前述の「セキュリティリスク分析」のとおり。
186					セキュリティリスクの見直し範囲	前述の「セキュリティリスク分析」のとおり。	前述の「セキュリティリスク分析」のとおり。
187			セキュリティリスク対策の見直し	対象システムにおいて、運用開始後に発見された脅威に対する対策の方針を確認するための項目	運用開始後のリスク対応範囲	前述の「セキュリティリスク分析」のとおり。	前述の「セキュリティリスク分析」のとおり。
188					リスク対策方針	前述の「セキュリティリスク分析」のとおり。	前述の「セキュリティリスク分析」のとおり。
189			セキュリティパッチ適用	対象システムの脆弱性等に対応するためのセキュリティパッチ適用に関する適用範囲、方針および適用のタイミングを確認するための項目	セキュリティパッチ適用範囲	システム全体	システム全体
190					セキュリティパッチ適用方針	パッチ内容に応じて、運用保守担当者が判断すること。実質的な効果が得られないにも関わらず、最新化を目的とした適用は行わない。	特に要件とはしないが、オンプレ型モデル側のパッチレベルが維持されることを想定している。オンプレ型モデル側のパッチレベルと相違が発生し利用に支障が出る場合には、オンプレ型モデル側のパッチレベルに合わせることを想定している。
191					セキュリティパッチ適用タイミング	パッチ内容に応じて、運用保守担当者が判断すること。	同上
192		アクセス・利用制限	認証機能	資産を利用する主体(利用者や機器等)を識別するための認証を実施するか、また、どの程度実施するのかを確認するための項目	管理権限を持つ主体の認証	アプリケーションの認証には「ユーザ名」「PINコード」「ワンタイムパスワード」の3点を用いる。 端末、サーバOSでの認証は「ID/パスワード」による認証とする。	「ID/パスワード」による認証を最低限の要件とし、より強固な認証方式を採用することを想定する。認証情報の管理は本市、もしくは本市が委託するものが行う。
193					管理権限を持たない主体の認証	同上	同上
194			利用制限	認証された主体(利用者や機器など)に対して、資産の利用等を、ソフトウェアやハードウェアにより制限するか確認するための項目	システム上の対策における操作制限度	【サーバ】 ・サーバやミドルウェアへのアクセスは、利用者毎の役割に応じた範囲でのみ操作可能とする。 【端末】 ・ソフトウェアのインストールは、端末管理ツールで制限する。 ・USBポートの利用制限を行う。 ・アクセスするデータのセキュリティレベルに応じて端末は分離する。	開発環境のうち、アプリケーションの開発環境(＝情報の持ち出しを制限する範囲)については、仮想デスクトップ機能を介してのみアクセス可能とする。また、ファイルのダウンロードは不可とする(アップロードは可)。これは、本市が提供するテストデータ(データ秘匿化によって個人を特定不能としたデータ)が不特定多数によって閲覧可能となることを防ぐためである。
195					物理的な対策による操作制限度	【サーバ】 ・入退室制限された区画に設置する。 ・サーバラックは施錠する。鍵はキーボックス内に保管し、認証された要員のみが取り出し可能とする。 【端末】 ・市民情報にアクセス可能な端末は、入退室制限された区画に設置する。	日本データセンター協会制定のデータセンターファシリティスタンダードのティア3を満たすこと。

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
196			管理方法	認証に必要な情報（例えば、ID/パスワード、指紋、虹彩、静脈など、主体を一意に特定する情報）の追加、更新、削除等のルール策定を実施するかを確認するための項目	管理ルールの策定	PINコードはユーザに紐付く4桁の数字であり、本人しかしらない想定である。ワンタイムパスワードはユーザごとに配布するトークン発行機で生成する。アカウントの追加・変更・削除は、管理手順についても基盤の運用保守メニューで定義する。 【サーバ・ミドルウェア】 Windows系及びLinuxサーバは、ActiveDirectoryによる統合管理を行う。それ以外は個々の製品・ミドルウェアごとに設定する。 【端末】 ActiveDirectoryによる統合管理を行う。 【ファイルの持出】 ・外部への持出は所定の申請に基づき可能とする。持出を希望する者は、対象ファイルをファイルサーバ（外部からのアクセス不可）に一時保管し、市へ申請する。市職員は、個人を特定する情報が含まれていないことを確認のうえ、外部アクセス可能なストレージ（WebDAV）にコピーする。コピー完了後、希望者は任意のタイミングで取得する。 【ファイルの持込】 ・持込に伴う事前申請やチェックはしない。ただし、ウィルスチェックおよびマルウェア対策は実施すること。	ID/パスワード認証などのアクセス管理、アカウント管理、アクセス制御等を統合的に管理できるようにすること。使用する製品の指定は行わない。 アプリケーションの開発環境（＝情報の持ち出しを制限する範囲）からのファイルの持ち出し（ダウンロード）は不可とする。アプリケーションの開発環境（＝情報の持ち出しを制限する範囲）へのファイルの持ち込み（アップロード）は許可するが、ウィルスチェック及びマルウェア対策は実施すること。
197					ユーザ管理対象者	【Webアプリケーション】 原局職員に加え、運用保守用途のアカウント。 【サーバ・ミドルウェア】 運用保守用途のアカウント。 【運用保守端末】 運用保守および開発（テスト）用途のアカウント。 Webアプリケーションについては、基盤機能により対象アカウントの有効期間や認可情報などを管理する。 【開発端末】 開発用途のアカウント。主に開発業者ごとに発行。	パブリックゾーンに配置するファイルサーバ機能、構成管理サーバ及び仮想デスクトップ機能を利用するアカウント。
198		データの秘匿	データ暗号化	機密性のあるデータを、伝送時や蓄積時に秘匿するための暗号化を実施するかを確認するための項目	伝送データの暗号化の有無	端末とDMZセグメント間の通信はSSL等の暗号化を必須とする。サーバルーム内で完結する通信については暗号化は要件としない。 なお、札幌市施設外との通信については暗号化を必須とする。	利用者各自の拠点に存在する端末とパブリックゾーンに配置するファイルサーバ機能、構成管理サーバ及び仮想デスクトップ機能との間の通信は暗号化を必須とする。アプリケーションの開発環境（＝情報の持ち出しを制限する範囲）内で完結する通信については暗号化は要件としない。

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
199					蓄積データの暗号化の有無	盗難、流出のリスクに備え、蓄積データの暗号化を実施する。 【ストレージ】 ディスクの物理的な盗難、紛失リスクを鑑みて、ストレージの暗号化を行なう。 【ファイルシステム】 OSデータや個々の業務ファイルの暗号化は原則実施しない。 【ミドルウェア】 Oracle Database は、データファイルやDatapump ツールによって生成したダンプファイルを暗号化する。	個人情報が含まれないため、蓄積データの暗号化は要件としない。
200					鍵管理	暗号化データと鍵は保管先を分け、適切な管理を行うこと。	特に要件としない。
201		不正追跡・監視	不正監視	不正行為を検知するために、それらの不正について監視する範囲や、監視の記録を保存する量や期間を確認するための項目	ログの取得	基盤ではシステム上の各機器でアクセス記録を採取すると共に、市民情報の閲覧履歴を記録・照会する仕組みを提供する。	本環境（ファイルサーバ機能、仮想デスクトップ機能、等）に対するアクセスログを1年保管すること。
202					ログ保管期間	前述の「バックアップ保存期間」を参照。	同上
203					不正監視対象（装置）	基幹系のインフラを構成する装置のうち、ログイン認証を要する装置を対象とする。	不正アクセス等の監視のためにログを取得すること。
204					不正監視対象（ネットワーク）	不正アクセスの検知が可能なこと。	不正アクセスの検知が可能なこと。
205					不正監視対象（侵入者・不正操作等）	札幌市施設内には監視カメラ等による対策が備わっている。	日本データセンター協会制定のデータセンターファシリティスタンダードのティア3を満たすこと。
206					確認間隔	危険性の高いアクセスを検知した場合には速やかに本市に報告をすること。その他は、少なくとも月に一度、不正監視の結果を確認し、本市に報告すること。	危険性の高いアクセスを検知した場合には速やかに本市に報告をすること。その他は、少なくとも月に一度、不正監視の結果を確認し、本市に報告すること。
207			データ検証	情報が正しく処理されて保存されていることを証明可能とし、情報の改ざんを検知するための仕組みとしてデジタル署名を導入するかを確認するための項目	デジタル署名の利用の有無	デジタル署名は利用しない。	特に要件としない
208					確認間隔	デジタル署名を利用しないため、デジタル署名の確認間隔は非機能要件として定義しない。	同上
209					ファイル改ざん検知	以下の理由により、ファイル改ざん検知は原則行わない。 ・改ざん検知の対象となる、業務アプリケーションが扱うデータは原則 RDBMS に保管されていること。 ・過去、基幹系においてファイル改ざん検知用ツールを導入したものの、対象ファイルの変更頻度が高く、都度ツールを無効化する運用としており、運用の手間がかかることや実体として検知の意味をなさないこと。 一方、DB監査機能を有効化し、業務アプリケーション以外からの不正な改ざん行為を検知する。	同上
210		ネットワーク対策	ネットワーク制御	不正な通信を遮断するための制御を実施するかを確認するための項目。	通信制御	外部ネットワークとの境界にファイアウォール等を設置し、不正な通信を制御する。また、札幌市施設内に設置するNW機器においても、不要な通信は遮断する。	ファイアウォール機能により、不正な通信を制御する。
211			不正検知	ネットワーク上において、不正追跡・監視を実施し、システム内の不正行為や、不正通信を検知する範囲を確認するための項目	不正通信の検知範囲	前述の「不正監視対象（ネットワーク）」を参照。	前述の「不正監視対象（ネットワーク）」を参照。

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
212			サービス停止攻撃の回避	ネットワークへの攻撃による輻輳についての対策を実施するかを確認するための項目	ネットワークの輻輳対策	ネットワークの負荷を継続的にモニタリングすることで、対策とする。	サービス停止攻撃に対する予防及び検知のセキュリティ対策を備えること。
213		マルウェア対策	マルウェア対策	マルウェア（ウィルス、ワーム、ボット等）の感染を防止する、マルウェア対策の実施範囲やチェックタイミングを確認するための項目	マルウェア対策実施範囲	現状の規約により、新基幹系情報システムに関わる全てのコンピュータ(サーバ・端末)を対象とする。	範囲内のすべての論理サーバを対象とする。
214					リアルタイムスキャンの実施	クライアント端末・サーバにおいて常時リアルタイムスキャンを実施する。	常時リアルタイムスキャンを実施する。
215					フルスキャンの定期チェックタイミング	クライアント端末は週1回実施する。 サーバは不定期とする。運用・保守管理プロセスにおいて、必要と判断した場合。	週1回以上実施する。
216		Web対策	Web実装対策	Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目	セキュアコーディング、Webサーバの設定等による対策の強化	他項目で定義済のため、本項目は非機能要件として定義しない。	他項目で定義済のため、本項目は非機能要件として定義しない。
217					WAFの導入の有無	WAFの導入は要件としない。	特に要件としない。
218	使用性・操作性	画面設計ポリシー	HTMLフレームの利用可否	HTMLフレームの利用可否について定義する		後述のサポートブラウザで規定するブラウザでの動作が保証されること	特に要件としない。
219			JavaScriptの利用ポリシー	Webの画面上で使用するクライアントJavaScriptについて使用可否・利用目的(バリデーション、Ajax等DHTML、画面遷移等)について定義する		後述のサポートブラウザで規定するブラウザでの動作が保証されること	同上
220			サポートブラウザ	システムのクライアントとして想定するOS、ブラウザを定義する		以下のブラウザを前提とする ・Internet Explore 11 または Microsoft Edge ・Firefox Ver26.0以降	以下のブラウザを前提とする ・Internet Explore 11 または Microsoft Edge ・Firefox Ver26.0以降
221			携帯サポート有	携帯電話のブラウザをサポートするか定義する		携帯電話ブラウザのサポートは不要	特に要件としない。
222			想定画面解像度	システムが標準的に想定する画面解像度を定義する。フルスクリーン使用を前提とするか、なども定義する		横1024×縦768ピクセル以上とする。 フルスクリーンモードとするかは、利用者に委ねる。	同上
223			使用色の制約	画面上で利用できる色を限定する場合にはその内容を定義する (例：色弱のエンドユーザが色を識別できる必要がある、等)		制約なし	同上

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
224			ブラウザプラグインの使用可否	ブラウザ上で動作するプラグイン(Flash、SilverLight、任意のActiveXプラグイン等)の使用可否及びバージョンを定義する。使用が前提の場合は当該プラグインがインストールされていない環境でどのように振る舞うべきかを定義する		Flash および 任意の Active X プラグインを使用可とする。 その他のプラグインについても、前述のサポートブラウザに記載したブラウザに対応したものであれば、札幌市の許可を得たうえで可能。	同上
225			Cookieの使用ポリシー	HTTP Cookieについて使用の可否及び使用目的、有効期間等について定義する		利用可	同上
226			その他画面設計ポリシー	上記以外に画面上の設計ポリシーがある場合はその内容を定義する		制約なし	同上
227	システム環境・エコロジー	システム制約/前提条件	構築時の制約条件	構築時の制約となる社内基準や法令、各地方自治体の条例などの制約が存在しているかの項目	構築時の制約条件	以下の規定に準拠する必要がある。 ・札幌市個人情報保護条例 ・札幌市個人情報保護条例施行規則 ・札幌市公文書管理規則 ・札幌市公用文規程 ・札幌市事務取扱規程 ・札幌市情報公開条例 ・札幌市情報公開条例施行規則 ・札幌市施設①管理要領 ・保守用環境運用管理要領 ・札幌市情報通信ネットワーク運用管理要領 ・札幌市情報化事務取扱要綱 ・札幌市セキュリティポリシー(*) ・危機管理マニュアル(*) ・情報セキュリティ実施手順(*) (*)の資料はセキュリティ上の理由で開示できない資料であるため、別途必要な事項を提示する。	以下の規定に準拠する必要がある。 ・札幌市個人情報保護条例 ・札幌市個人情報保護条例施行規則 ・札幌市公文書管理規則 ・札幌市公用文規程 ・札幌市事務取扱規程 ・札幌市情報公開条例 ・札幌市情報公開条例施行規則 ・札幌市施設①管理要領 ・保守用環境運用管理要領 ・札幌市情報通信ネットワーク運用管理要領 ・札幌市情報化事務取扱要綱 ・札幌市セキュリティポリシー(*) ・危機管理マニュアル(*) ・情報セキュリティ実施手順(*) (*)の資料はセキュリティ上の理由で開示できない資料であるため、別途必要な事項を提示する。
228			運用時の制約条件	運用時の制約となる社内基準や法令、各地方自治体の条例などの制約が存在しているかの項目	運用時の制約条件	運用時についても構築時と同様の規定に準拠すること。	運用時についても構築時と同様の規定に準拠すること。
229		システム特性	ユーザ数	システムを使用する利用者(エンドユーザ)の人数	ユーザ数	前述の「ユーザ数」のとおり。	前述の「ユーザ数」のとおり。
230			クライアント数	システムで使用され、管理しなければいけないクライアントの数	クライアント数	Active Directoryの管理対象クライアント数は1,000台程度。XenApp利用クライアントは2,600台程度。	仮想デスクトップ機能を利用するため、管理しなければいけないクライアントは0台。
231			拠点数	システムが稼働する拠点の数	拠点数	区役所など約20拠点。	開発業者の拠点を含め、約20拠点と想定している。
232			端末・プリンタ等	端末やプリンタの設置場所、及び台数		同上	端末は開発業者の拠点など各利用者の拠点に設定される。プリンタは存在しない(0台)。

No.	非機能項目					次期インフラ 〔オンプレ型モデル〕	次期インフラ 〔オフプレ型モデル〕
	大項目	中項目	小項目	小項目説明	詳細項目		
233			複数言語対応	システム構築の上で使用が必要、またはサービスとして提供しなければならない言語	言語数	原則として日本語対応を行うこと。	原則として日本語対応を行うこと。