別紙1 非機能要件一覧 【Ｉ全庁的要求事項シート】

本資料は、独立行政法人情報処理推進機構が作成した「非機能要求グレード」を財団法人地方自治情報センターが地方公共団体向けに一部変更したものを基に、今回の次期システムに求める要件を整理しています。
次期システムに求める要件は、「グループ②：選択レベル」列に記載の選択レベルとなります。また、右端の「要件説明」列に適宜具体的な要件も記載していますので、併せてご確認ください。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	検収時の扱い[2]	利用ガイドの解説[3]	グループ②		レベル								備考 ［利用ガイド］第4章も参照のこと	要件説明
							選択レベル	選択時の条件	－	＊	0	1	2	3	4	5		
C.1.2.2	運用・保守性	通常運用	外部データの利用可否	外部データとは、当該システムの範囲外に存在する情報システムの保有するデータを指す（例：住民基本4情報については、住基ネットの情報がある等）。			2 外部データは利用できない	全データを復旧するためのバックアップ方式を検討しなければならないことを想定。 [－] 外部に同じデータを持つ情報システムが存在するため、本システムに障害が発生した際には、そちらからデータを持ってきて情報システムを復旧できるような場合	仕様の対象としない	ベンダーによる提案事項	全データの復旧に利用できる	一部のデータ復旧に利用できる	外部データは利用できない					
C.2.3.5		保守運用	OS等パッチ※適用タイミング	OS等パッチ※情報の展開とパッチ※適用のポリシー※に関する項目。 OS等は、OS、ミドルウェア、その他のソフトウェアを指す。	○	P29	4 緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	緊急性の高いパッチを除くと、定期保守時にパッチを適用するのが一般的と想定。 [－]外部と接続することが全くない等の理由で緊急対応の必要性が少ない場合（リスクの確認がとれている場合）。	仕様の対象としない	ベンダーによる提案事項	パッチ※を適用しない	障害発生時にパッチ※適用を行う	定期保守時にパッチ※適用を行う	緊急性の高いパッチ※のみ即時に適用を行う	緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	新規のパッチ※がリリースされるたびに適用を行う	【注意事項】 リリースされるパッチ※の種類（個別パッチ※／集合パッチ※）よって選択レベルが変わる場合がある。 セキュリティパッチ※については、セキュリティの項目でも検討すること（E.4.3.3）。	
C.4.4.1		リモートオペレーション※	リモート監視※地点	情報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。		P30	1 庁内LANを介してリモート監視を行う	庁内LANの範囲内でのみリモート監視を行い、外部（ベンダー拠点等）からの監視を行わない。 [－] サーバ機器についてもコンソールでの直接監視を行う場合 [+]外部（ベンダー拠点等）からの監視を行う場合	仕様の対象としない	ベンダーによる提案事項	リモート監視※を行わない	庁内LANを介してリモート監視を行う	ベンダー拠点等外部からリモート監視を行う				【レベル】 監視の内容については、通常運用の運用監視の項目にて確認する必要がある。	
C.4.4.3			リモート操作※時の接続方法	ベンダーがリモート監視※地点からリモート操作を実施する場合の回線接続方法。		P30	1 リモート操作※の必要時のみ接続する	ベンダーによるリモート操作はセキュリティの観点から実施を禁止していることを想定。 [+]サーバ等が複数拠点に分散する場合、または、設置場所がベンダーのサポート拠点から遠方にある場合	仕様の対象としない	ベンダーによる提案事項	リモート操作※を行わない	リモート操作※の必要時のみ接続する	常時接続環境にてリモート操作※を行う				【注意事項】 リモート操作を実施できる範囲は、あらかじめ協議し決定しておく必要がある。	
E.1.1.1	セキュリティ	前提条件・制約条件	順守すべき規程、ルール、法令、ガイドライン等の有無	ユーザが順守すべき情報セキュリティに関する規程やルール、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。 なお、順守すべき規程等が存在する場合は、規定されている内容と矛盾が生じないよう対策を検討する。 例） ・情報セキュリティポリシー ・個人情報保護法 ・電子署名法 ・IT基本法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・プライバシーマーク など	○		1 有り	セキュリティポリシー等を順守する必要があることを想定。 [－] 順守すべき規程やルール、法令、ガイドライン等が無い場合	仕様の対象としない	ベンダーによる提案事項	無し	有り					【注意事項】 規程やルール、法令、ガイドライン等を確認し、それらに従い、セキュリティに関する非機能要求項目のレベルを決定する必要がある。	
E.2.1.1		セキュリティリスク分析	リスク分析範囲	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。 なお、適切な範囲を設定するためには、資産の洗い出しやデータのライフサイクル※の確認等を行う必要がある。 また、洗い出した脅威に対して、対策する範囲を検討する。			1 重要度が高い資産を扱う範囲、あるいは、外接部分	重要情報が取り扱われているため、脅威が現実のものとなった場合のリスクも高い。そのため、重要度が高い資産を扱う範囲に対してリスク分析する必要がある。 [－] 重要情報の漏洩等の脅威が存在しない（あるいは許容する）場合 [+] 情報の移動や状態の変化が大きい場合	仕様の対象としない	ベンダーによる提案事項	分析なし	重要度が高い資産を扱う範囲、あるいは、外接部分	開発範囲				【レベル1】 外接部分とは、インターネットへの接続部分や、外部へ情報を持ち出す際に用いる媒体等を接続する部分、また、外部システムとデータのやりとりを行う部分等を意味する。 なお、以降のレベルにおいても同様の意味で用いている。 重要度が高い資産は、各団体の情報セキュリティポリシーにおける重要度等に基づいて定める（重要度が最高位のものとする等）。	
E.4.3.4		セキュリティリスク管理	ウィルス定義ファイル適用タイミング	対象システムの脆弱性等に対応するためのウィルス定義ファイル適用に関する適用範囲、方針及び適用のタイミングを確認するための項目。	○	P30	2 定義ファイルリリース時に実施	ウィルス定義ファイルは、自動的に適用する。 [－]ウィルス定義ファイルが、自動的に適用できない場合（例えばインターネットからファイル入手できない場合）。	仕様の対象としない	ベンダーによる提案事項	定義ファイルを適用しない	定期保守時に実施	定義ファイルリリース時に実施					
E.5.1.1		アクセス※・利用制限	管理権限を持つ主体の認証	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。 複数回の認証を実施することにより、抑止効果を高めることができる。 なお、認証するための方式としては、ID/パスワードによる認証や、ICカード認証、生態認証等がある。		P31	1 1回	攻撃者が管理権限を手に入れることによる、権限の乱用を防止するために、認証を実行する必要がある。 [+] 管理権限で実行可能な処理の中に、業務上重要な処理が含まれている場合	仕様の対象としない	ベンダーによる提案事項	実施しない	1回	複数回の認証	複数回、異なる方式による認証			【注意事項】 管理権限を持つ主体とは、情報システムの管理者や業務上の管理者を指す。	

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	検収時の扱い[2]	利用ガイドの解説[3]	グループ②		レベル								備考 ［利用ガイド］第4章も参照のこと	要件説明
							選択レベル	選択時の条件	－	＊	0	1	2	3	4	5		
E.5.2.1			システム上の対策における操作制限度	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、ソフトウェアにより制限するか確認するための項目。 例）コマンド実行制､ソフトウェアのインストール制限や、利用制限等、ソフトウェアによる対策を示す。			1 必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可	不正なソフトウェアがインストールされる、不要なアクセス※経路（ポート※等）を利用可能にしている等により、情報漏洩の脅威が現実のものとなってしまうため、これらの情報等への不要なアクセス※方法を制限する必要がある。 （操作を制限することにより利便性や、可用性に影響する可能性がある） [－] 重要情報等への攻撃の拠点とならない端末等に関しては、運用による対策で対処する場合	仕様の対象としない	ベンダーによる提案事項	無し	必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可						
E.6.1.1		データの秘匿	伝送データの暗号化の有無	暗号化通信方式を使用して伝送データの暗号化を行う。		P31	2 重要情報を暗号化	ネットワークを経由して送信するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [+] 外部ネットワークと接続する場合	仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化	すべてのデータを暗号化			【レベル1】 認証情報のみ暗号化とは、情報システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。 【注意事項】 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 （CRYPTREC暗号リスト：http://www.cryptrec.go.jp/list.html）。	
E.6.1.2			蓄積データの暗号化の有無	ファイル・フォルダを暗号化するソフトウェアや、データベースソフトウェアの暗号化機能を使用して暗号化を行う。		P32	2 重要情報を暗号化	蓄積するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [+]物理記録媒体の盗難・紛失の可能性が有る場合	仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化				【レベル1】 認証情報のみ暗号化とは、情報システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。 【注意事項】 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 （CRYPTREC暗号リスト：http://www.cryptrec.go.jp/list.html）。	
E.7.1.1		不正追跡・監視	ログ※の取得	不正を検知するために、監視のための記録（ログ※）を取得するかどうかの項目。 なお、どのようなログ※を取得する必要があるかは、実現する情報システムやサービスに応じて決定する必要がある。 また、ログ※を取得する場合には、不正監視対象と併せて、取得したログ※のうち、確認する範囲を定める必要がある。			1 必要なログを取得する	不正なアクセス※が発生した際に、「いつ」「誰が」「どこから」「何を実行したか」等を確認し、その後の対策を迅速に実施するために、ログ※を取得する必要がある。 （ログ※取得の処理を実行することにより、性能に影響する可能性がある）	仕様の対象としない	ベンダーによる提案事項	取得しない	必要なログを取得する					【注意事項】 取得対象のログ※は、不正な操作等を検出するための以下のようなものを意味している。 ・ログイン/ログアウト履歴（成功/失敗） ・操作ログ 等	
E.7.1.3			不正監視対象（装置）	サーバ、ストレージ※等への不正アクセス※等の監視のために、ログ※を取得する範囲を確認する。 不正行為を検知するために実施する。			1 重要度が高い資産を扱う範囲、あるいは、外接部分	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするサーバ、ストレージ※等の範囲を定めておく必要がある。	仕様の対象としない	ベンダーによる提案事項	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体					
E.10.1.1		Web対策	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	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。Webシステムが攻撃される事例が増加しており、Webシステムを構築する際には、セキュアコーディング※、Webサーバ※の設定等による対策の実施を検討する必要がある。		P32	1 対策の強化	オープン系の情報システムにおいて、データベース等に格納されている重要情報の漏洩、利用者への成りすまし等の脅威に対抗するために、Webサーバ※に対する対策を実施する必要がある。 [－] Webアプリケーション※を用いない場合	仕様の対象としない	ベンダーによる提案事項	無し	対策の強化					【注意事項】 また、実施した結果の有効性を確認するための専門家のレビューやソースコード※診断、ツールによるチェック等についても検討する必要がある。 詳細は、当センターの「地方公共団体における情報システムセキュリティ要求仕様モデルプラン」を参照の上、対策を検討すること。 Webシステムで考慮すべき項目。	
E.10.1.2			WAF※の導入の有無	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。WAF※とは、Web Application Firewallのことである。		P33	1 有り	内部ネットワークのみ接続する情報システムを想定、そのため、ネットワーク経由での攻撃に対する脅威が発生する可能性は低い。 [+] 外部ネットワークと接続する場合	仕様の対象としない	ベンダーによる提案事項	無し	有り					【注意事項】 Webシステムで考慮すべき項目。	
F.3.1.1	システム環境・エコロジー	適合規格	規格取得の有無(安全性)	提供する情報システムに使用する製品について、UL60950※などの製品安全規格を取得していることを要求されているかを確認する項目。		P33	0 規格取得の必要無し	機器の規格取得に関して指定があった場合を想定。 [－] 特に指定がない場合	仕様の対象としない	ベンダーによる提案事項	規格取得の必要無し	規格取得の必要有り						
F.3.2.1			規格取得の有無（有害物質）	提供する情報システムに使用する製品について、RoHS指令※などの特定有害物質の使用制限についての規格の取得を要求されているかを確認する項目。		P34	0 規格取得の必要無し	RoHS指令※対応の装置が指定された場合を想定。 [－] 特に指定が無かった場合	仕様の対象としない	ベンダーによる提案事項	規格取得の必要無し	RoHS指令※相当取得						
F.5.1.1		環境マネージメント	グリーン購入法対応度	環境負荷を最小化する工夫の度合いの項目。 例えば、グリーン購入法適合製品の購入など、環境負荷の少ない機材・消耗品を採用する。 また、ライフサイクルを通じた廃棄材の最小化の検討を行う。例えば、拡張の際に既設機材の廃棄が不要で、必要な部材の増設、入れ替えのみで対応可能な機材を採用するなどである。また、ライフサイクルが長い機材ほど廃棄材は少ないと解釈できる。		P34	0 対処不要	団体の方針によるものと想定。 [+]団体の方針による。	仕様の対象としない	ベンダーによる提案事項	対処不要	グリーン購入法の基準を満たす製品を一部使用	グリーン購入法の基準を満たす製品のみを使用					

1 検収時の扱い　　○：目標（値）として扱い、長期的に測定・評価を行うべき項目

2 利用ガイドの解説　　Pxx：利用ガイドのメトリクス詳細説明ページ

3 「※」が付記された用語　　利用ガイド及び調査報告書の用語集にて解説のあるIT専門用語

別紙1 非機能要件一覧 【Ⅱ業務主管部門要求事項シート】

本資料は、独立行政法人情報処理推進機構が作成した「非機能要求グレード」を財団法人地方自治情報センターが地方公共団体向けに一部変更したものを基に、今回の次期システムに求める要件を整理しています。
次期システムに求める要件は、「グループ②：選択レベル」列に記載の選択レベルとなります。また、右端の「要件説明」列に適宜具体的な要件も記載していますので、併せてご確認ください。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	検収時の扱い[2]	利用ガイドの解説[3]	グループ②		レベル								備考 ［利用ガイド］第4章も参照のこと	要件説明
							選択レベル	選択時の条件	-	*	0	1	2	3	4	5		
A.1.3.1	可用性	継続性	RPO（目標復旧地点）※[4]（業務停止時）	業務停止を伴う障害が発生した際、バックアップしたデータなどから情報システムをどの時点まで復旧するかを定める目標値。 バックアップ頻度・バックアップ装置・ソフトウェア構成等を決定するために必要。	○	P35	3	障害発生時点（日次バックアップ+アーカイブ※からの復旧）	データの損失は許容できないため、障害発生時点までの復旧が原則。 [-] データの損失がある程度許容できる場合（復旧対象とするデータ（日次、週次）によりレベルを選定）	仕様の対象としない	ベンダーによる提案事項	復旧不要	5営業日前の時点（週次バックアップからの復旧）	1営業日前の時点（日次バックアップからの復旧）	障害発生時点（日次バックアップ+アーカイブ※からの復旧）			【注意事項】 RLO※で業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認（例えば、バックアップ時点まで戻ってしまったデータを手修正する等）は別途ユーザが実施する必要がある。	
A.1.3.2			RTO（目標復旧時間）※（業務停止時）	業務停止を伴う障害（主にハードウェア・ソフトウェア故障）が発生した際、復旧するまでに要する目標時間。 ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	○	P35	3	6時間以内	なるべく早く復旧する。故障時すみやかに利用可能な予備機を使用した復旧を想定。 [-] 業務停止の影響が小さい場合 [+] コストと地理的条件等の実現性を確認した上で、復旧時間を短縮したい場合	仕様の対象としない	ベンダーによる提案事項	1営業日以上	1営業日以内	12時間以内	6時間以内	2時間以内		【注意事項】 RLOで業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認（例えば、バックアップ時点まで戻ってしまったデータを手修正する等）は別途ユーザが実施する必要がある。	
A.1.3.3			RLO（目標復旧レベル）※（業務停止時）	業務停止を伴う障害が発生した際、どこまで復旧するかのレベル（特定システム機能・すべてのシステム機能）の目標値。 ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	○	P36	2	全システム機能の復旧	すべての機能が稼働していないと影響がある場合を想定。 [-] 影響を切り離せる機能がある場合	仕様の対象としない	ベンダーによる提案事項	規定しない	一部システム機能の復旧	全システム機能の復旧				【レベル1】 一部システム機能とは、特定の条件下で継続性が要求される機能などを指す。（例えば、住民基本台帳システムの住民票発行機能だけは、障害時も提供継続する場合等。）	
A.1.4.1			システム再開目標（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。 大規模災害とは、火災や地震などの異常な自然現象、あるいは人為的な原因による大きな事故、破壊行為により生ずる被害のことを指し、情報システムに甚大な被害が発生するか、電力などのライフラインの停止により、システムをそのまま現状に修復するのが困難な状態となる災害をいう。	○	P37	2	一ヶ月以内に再開	電源及びネットワークが利用できることを前提に、遠隔地に設置された予備機とバックアップデータを利用して復旧することを想定。機能は、業務が再開できる最低限の機能に限定する。 [+] 人命に影響を及ぼす、経済的な損失が甚大など、安全性が求められる場合でベンダーと合意できる	仕様の対象としない	ベンダーによる提案事項	再開不要	数ヶ月以内に再開	一ヶ月以内に再開	一週間以内に再開	3日以内に再開	1日以内に再開	【注意事項】 目標復旧レベルについては、業務停止時に規定されている目標復旧水準を参考とする。	
A.1.5.1			稼働率	明示された利用条件の下で、情報システムが要求されたサービスを提供できる割合。 明示された利用条件とは、運用スケジュールや、目標復旧水準により定義された業務が稼働している条件を指す。その稼働時間の中で、サービス中断が発生した時間により稼働率を求める。	○	P38	3	99.5%	ベンダーのサポート拠点から、車で2時間程度の場所にあることを想定。1回当たり6時間程度停止する故障を年間2回まで許容する。 [+] コストと地理的条件等の実現性を確認した上で、可用性を高めたい場合 [-]地理的条件から実現困難な場合。業務停止が許容できる場合。	仕様の対象としない	ベンダーによる提案事項	規定しない	95%	99%	99.5%	99.9%	99.99%	【レベル】 稼働時間（バッチ処理等を含む運用時間）を平日のみ1日当たり12時間と想定した場合。 99.99%・・・・年間累計停止時間17分 99.9%・・・・・年間累計停止時間2.9時間 99.5%・・・・・年間累計停止時間14.5時間 99%・・・・・・年間累計停止時間29時間 95%・・・・・・年間累計停止時間145時間	
B.1.1.1	性能・拡張性	業務処理量	ユーザ数	情報システムの利用者数。利用者は、庁内、庁外を問わず、情報システムを利用する人数を指す。 性能・拡張性を決めるための前提となる項目であると共にシステム環境を規定する項目でもある。また、パッケージソフトやミドルウェアのライセンス価格に影響することがある。			1	上限が決まっている	あらかじめ一定の上限値を設定する場合を想定。 [-] 特定のユーザのみ使用することを合意できた場合	仕様の対象としない	ベンダーによる提案事項	特定ユーザのみ	上限が決まっている	不特定多数のユーザが利用					
B.1.1.2			同時アクセス数	同時アクセス※数とは、ある時点で情報システムにアクセス※しているユーザ数のことである。パッケージソフトやミドルウェアのライセンス価格に影響することがある。			1	同時アクセス※の上限が決まっている	情報システムに対してどのようなピークモデル※を想定しているか確認する。	仕様の対象としない	ベンダーによる提案事項	特定利用者の限られたアクセス※のみ	同時アクセス※の上限が決まっている	不特定多数のアクセス※有り					
B.1.1.3			データ量（項目・件数）	情報システムで扱うデータの件数及びデータ容量等。性能・拡張性を決めるための前提となる項目である。			1	主要なデータ量のみが明確である	要件定義時には明確にしておく必要がある。 [+] 全部のデータ量が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	すべてのデータ量が明確である	主要なデータ量のみが明確である					【レベル1】 主要なデータ量とは、情報システムが保持するデータの中で、多くを占めるデータのことを言う。 例えば、住民基本台帳システムであれば住民データ・世帯データ・異動データ等がある。	
B.1.1.4			オンラインリクエスト件数※	単位時間ごとの業務処理件数。性能・拡張性を決めるための前提となる項目である。			1	主な処理のリクエスト件数※のみが明確である	要件定義時には明確にしておく必要がある。 [+] 全部のオンラインリクエスト件数※が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	処理ごとにリクエスト件数※が明確である	主な処理のリクエスト件数※のみが明確である					【レベル1】 主な処理とは情報システムが受け付けるオンラインリクエストの中で大部分を占めるものを言う。 例えば、住民情報システムの転入・転出処理などがある。	
B.1.1.5			バッチ処理件数	バッチ処理により処理されるデータ件数。性能・拡張性を決めるための前提となる項目である。			*	ベンダーによる提案事項	要件定義時には明確にしておく必要がある。 [+] 全部のバッチ処理件数が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	処理単位ごとに処理件数が決まっている	主な処理の処理件数が決まっている					【注意事項】 バッチ処理件数は単位時間を明らかにして確認する。 【レベル1】 主な処理とは情報システムが実行するバッチ処理の中で大部分の時間を占める物をいう。 例えば、人事給与システムや料金計算システムの月次集計処理などがある。	
B.1.2.1			ユーザ数増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とユーザ数が最大になる時点のユーザ数の倍率。			1	1.2倍	ユーザの登録・削除などのサイクルを確認する。また、将来の見通しについても確認する。 [-] 利用者が固定されている場合 [+] 利用者の増加が見込まれる場合	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 減少が予測される場合は、レベル0（1倍）を選択する。	

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	検収時の扱い[1]	利用ガイドの解説[2]	グループ②			レベル								備考 ［利用ガイド］第4章も参照のこと	要件説明
							選択レベル		選択時の条件	-	*	0	1	2	3	4	5		
B.1.2.2			同時アクセス※数増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点と同時アクセス数が最大になる時点の同時アクセス数の倍率。			1	1.2倍	情報システムのピークモデル※がユーザ数の増によってどのように変わると考えているかを確認する。 [-] 利用者が固定されている場合やユーザの増加とアクセスユーザの増加が相関関係でない場合 [+] 利用者の増加が見込まれる場合	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 減少が予測される場合は、レベル0（1倍）を選択する。	
B.1.2.3			データ量増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とデータ量が最大になる時点のデータ量の倍率。			1	1.2倍	業務の手順によって情報システムで扱うデータ量がどの程度増加するかを確認する。 [-] データを蓄積しないゲートウェイシステムの場合 [+] 過去のデータを長期間保存する情報システムの場合	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 減少が予測される場合は、レベル0（1倍）を選択する。	
B.1.2.4			オンラインリクエスト件数※増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とオンラインリクエスト件数が最大になる時点のオンラインリクエスト件の倍率。			1	1.2倍	情報システムの制約となるリクエスト数※の見通しを確認する。	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 オンラインリクエスト件数※は単位時間（1時間当たりの件数等）を明らかにして確認する。	
B.1.2.5			バッチ処理件数増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とバッチ処理件数が最大になる時点のバッチ処理件数の倍率。			*	ベンダーによる提案事項	情報システムの制約となる処理件数を確認する。	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 バッチ処理件数は単位時間（1日当たりの件数等）を明らかにして確認する。	
B.2.1.4		性能目標値	通常時オンラインレスポンスタイム※	オンラインシステム利用時に要求されるレスポンス※。 システム化する対象業務の特性を踏まえ、どの程度のレスポンス※が必要かについて確認する。アクセス※が集中するタイミングの特性や、障害時の運用を考慮し、通常時・アクセス※集中時・縮退運転時ごとにレスポンスタイムを決める。具体的な数値は特定の機能またはシステム分類ごとに決めておくことが望ましい。（例：Webシステムの参照系/更新系/一覧系など）	○	P39	3	3秒以内	管理対象とする処理の中で、通常時の大量データを扱わない処理がおおむね目標値を達成できれば良いと想定。 [-] 遅くても、処理出来れば良い場合。または代替手段がある場合 [+] 性能低下が、情報システムの評価低下につながる場合	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内		【注意事項】 すべての処理に適用するわけではなく、主な処理に適用されるものとする。 測定方法、調達範囲外の条件（例えばネットワークの状態等）については、ベンダーと協議し詳細を整理する必要が有る。 【レベル4】 1秒以内とした場合には、用意するハードウェアについて高コストなものを求める必要があるため、その必要性を十分に検討する必要がある。	
B.2.1.5			アクセス集中時のオンラインレスポンスタイム※		○	P40	2	5秒以内	管理対象とする処理の中で、ピーク時の大量データを扱わない処理がおおむね目標値を達成できれば良いと想定。 [-] 遅くとも、処理出来れば良い場合。または代替手段がある場合 [+] 性能低下が、情報システムの評価低下につながる場合	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内		【注意事項】 すべての処理に適用するわけではなく、主な処理に適用されるものとする。 測定方法、アクセス集中時の条件については、ベンダーと協議し詳細を整理する必要が有る。 【レベル4】 1秒以内とした場合には、用意するハードウェアについて高コストなものを求める必要があるため、その必要性を十分に検討する必要がある。	
B.2.2.1			通常時バッチレスポンス※順守度合い	バッチシステム利用時に要求されるレスポンス※。 システム化する対象業務の特性を踏まえ、どの程度のレスポンス（ターンアラウンドタイム※）が必要かについて確認する。更に、アクセス※が集中するタイミングの特性や、障害時の運用を考慮し、通常時・ピーク時※・縮退運転※時ごとに順守度合いを決める、具体的な数値は特定の機能またはシステム分類ごとに決めておくことが望ましい。 （例：日次処理/月次処理/年次処理など）	○		2	再実行の余裕が確保できる	管理対象とする処理の中で、通常時のバッチ処理を実行し、結果が不正の場合、再実行できる余裕があれば良いと想定。 [-] 再実行をしない場合または代替手段がある場合	仕様の対象としない	ベンダーによる提案事項	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる					
B.2.2.2			アクセス※集中時のバッチレスポンス※順守度合い		○		2	再実行の余裕が確保できる	管理対象とする処理の中で、ピーク時※のバッチ処理を実行し、結果が不正の場合、再実行できる余裕があれば良いと想定。 ピーク時※に余裕が無くなる場合にはサーバ増設や処理の分割などを考慮する必要がある。 [-] 再実行をしない場合または代替手段がある場合	仕様の対象としない	ベンダーによる提案事項	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる					
C.1.1.1	運用・保守性	通常運用	運用時間（平日）	業務主管部門等のエンドユーザが情報システムを主に利用する時間。（サーバを立ち上げている時間とは異なる。）		P40	2	定時外も頻繁に利用（1日12時間程度利用）	主に、開庁時間内での利用を想定 [-] 不定期に利用する情報システムの場合 [+]定時外も頻繁に利用される場合、または24時間利用の場合	仕様の対象としない	ベンダーによる提案事項	規定無し（不定期利用）	定時内での利用（1日8時間程度利用）	定時外も頻繁に利用（1日12時間程度利用）	24時間利用			【注意事項】 情報システムが稼働していないと業務運用に影響のある時間帯を示し、サーバを24時間立ち上げていても、それだけでは24時間無停止とは言わない。	業務時間の定時（8:30-17:15）以降も利用する可能性があるため、本レベルを設定。 深夜に災害対応が必要な場合は、運用保守事業者と協議のうえで、深夜も利用する可能性があるため、留意すること。
C.1.1.2			運用時間（休日等）	土日/祝祭日や年末年始に業務主管部門等のエンドユーザが情報システムを主に利用する時間。（サーバを立ち上げている時間とは異なる。）		P40	0	規定無し（原則利用しない）	週末は原則利用しないことを想定 [+] 休日出勤する職員の業務に必要なため、休日等も利用する場合	仕様の対象としない	ベンダーによる提案事項	規定無し（原則利用しない）	定時内での利用（1日8時間程度利用）	定時外も頻繁に利用（1日12時間程度利	24時間利用				休日でも災害対応が必要な場合は、運用保守事業者と協議のうえで利用する可能性があるため、留意すること。
C.1.2.5			バックアップ取得間隔	バックアップ取得間隔		P41	4	日次で取得	全体バックアップは週次で取得する。しかし、RPO※要件である、1日前の状態に戻すためには、毎日差分バックアップ※を取得しなければならないことを想定。 [-] RPO※の要件が[-]される場合 [+] RPO※の要件が[+]される場合や、複数世代を確保してバックアップの可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	システム構成の変更時など、任意のタイミング	月次で取得	週次で取得	日次で取得	同期バックアップ		

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	検収時の扱い[1]	利用ガイドの解説[2]	グループ②			レベル								備考 ［利用ガイド］第4章も参照のこと	要件説明
							選択レベル		選択時の条件	-	*	0	1	2	3	4	5		
C.3.3.1		障害時運用	対応可能時間	情報システムの異常検知時に保守員が作業対応を行う時間帯。			0	ベンダーの営業時間内（例：9時～17時）で対応を行う	[+]対応が必要な場合	仕様の対象としない	ベンダーによる提案事項	ベンダーの営業時間内（例：9時～17時）で対応を行う	ユーザの指定する時間帯（例：18時～24時）で対応を行う	24時間対応を行う					北九州市上下水道システム基盤に次期システムを構築する場合、保守対応は北九州市のデジタル市役所推進室の専用室からサーバへリモート接続することとなる。専用室の入室時間が原則業務時間の定時内（8:30-17:15）であるため、本レベルを設定している。
C.3.3.2			駆けつけ到着時間	情報システムの異常を検出してから、指定された連絡先への通知、保守員が障害連絡を受けて現地へ到着するまでの時間。	○	P42	4	保守員到着が異常検知から数時間内	[+]対応が必要な場合 [-]地理的条件・コスト等により、制限が有る場合。	仕様の対象としない	ベンダーによる提案事項	保守員の駆けつけ無し	保守員到着が異常検知から数日中	保守員到着が異常検知からユーザの翌営業日中	保守員到着が異常検知からユーザの翌営業開始時まで	保守員到着が異常検知から数時間内	保守員が常駐	夕方頃に障害が発生した場合は翌日対応とする。
C.3.3.4			障害検知通知時間	障害の発生を検知した場合に、利用者（システム運用担当者）に通知するまでの時間。	○	P42	*	ベンダーによる提案事項	本項目は、常駐保守または、サーバをデーターセンター※に設置した場合。 [+]対応が必要な場合	仕様の対象としない	ベンダーによる提案事項	障害を検知しない	24時間以内	8時間以内	3時間以内	1時間以内	30分以内		
C.4.3.1		運用環境	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。			3	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供する	緊急時にはユーザ側にて保守対応を実施することも想定し、リカバリ※作業手順などを示した保守マニュアルも作成する。 [-] 保守作業はすべてベンダーに依頼するため、通常運用に必要なオペレーション※のみを説明した運用マニュアルのみ作成する場合 [+] ユーザ独自の運用ルールを加味した特別な運用マニュアルを作成する場合	仕様の対象としない	ベンダーによる提案事項	各製品標準のマニュアルを利用する	情報システムの通常運用のマニュアルを提供する	情報システムの通常運用と保守運用のマニュアルを提供する	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供する			【レベル】 通常運用のマニュアルには、サーバ・端末等に対する通常時の運用（起動・停止等）にかかわる操作や機能についての説明が記載される。保守運用のマニュアルには、サーバ・端末等に対する保守作業（部品交換やデータ復旧手順等）にかかわる操作や機能についての説明が記載される。 障害発生時の一次対応に関する記述（系切り替え作業やログ※収集作業等）は通常運用マニュアルに含まれる。バックアップからの復旧作業については保守マニュアルに含まれるものとする。	
C.4.5.1			外部システムとの接続有無	情報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。			1	庁内の外部システムと接続する	庁内基幹系システムとして、住基と税などのように連携する庁内の他システムが存在することを想定。 [-] データのやり取りを行う他システムが存在しない場合 [+] 庁外のシステムに接続して、データのやり取りを行う場合	仕様の対象としない	ベンダーによる提案事項	外部システムと接続しない	庁内の外部システムと接続する	庁外の外部システムと接続する				【注意事項】 接続する場合には、そのインターフェース※（接続ネットワーク・通信方式・データ形式等）について確認すること。	
C.5.1.2		サポート体制	保守契約（ハードウェア）の種類	保守が必要な対象ハードウェアに対する保守契約の種類。		P43	4	定額保守（オンサイト※）	オンサイト※の定額保守が地方公共団体の標準と想定。 [-] 故障時には、公共団体職員が予備機に切り替えることで対処し、保守費を軽減したい場合	仕様の対象としない	ベンダーによる提案事項	保守契約を行わない	随時保守（センドバック※）	定額保守（センドバック※）	随時保守（オンサイト※）	定額保守（オンサイト※）			上下水道局システム基盤を利用しないハードウェアがある場合は、本要件を満たすこと。
C.5.2.2			保守契約（ソフトウェア）の種類	保守が必要な対象ソフトウェアに対する保守契約の種類。			2	アップデート※	ソフトウェアが法改正等によりバージョンアップ※した場合に、アップデートする権利を含めることを想定。 [-] アップデート※権を必要としない場合	仕様の対象としない	ベンダーによる提案事項	保守契約を行わない	問い合わせ対応	アップデート※				【注意事項】 アップデート権の範囲については、事前にベンダーと協議しておくこと。 ライフサイクル期間中に、OSやミドルウェアのバージョンアップが必要となる場合は、バージョンアップ後の情報システムの動作保障等についてあらかじめベンダーと協議しておくこと。 インターネットに公開する外部システムの場合は、最新ブラウザへの対応等についてもあらかじめベンダーと協議しておくこと。	
C.5.3.1			ライフサイクル期間	運用保守の対応期間及び、実際に情報システムが稼動するライフサイクルの期間。ライフサイクルとは情報システムの利用期間(次回のシステム更改までの期間)のことを示している。		P44	2	7年	導入するソフトウェアのサポート期間に合わせて情報システムのライフサイクル※を5年と決定したと想定。 [-] 導入するソフトウェアやハードウェアのサポート期間がもっと短い場合 [+] 情報システムで実行する業務を5年を超えて継続しなければならないため、それにライフサイクルを合わせる場合	仕様の対象としない	ベンダーによる提案事項	3年	5年	7年				【注意事項】 製品の保守可能期間よりも長い期間のライフサイクル※となる場合は、保守延長や保守可能バージョンへのアップ等の対応が必要となる。 【注意事項】 アプリケーションのパッケージソフトのライフサイクル※とは異なるので注意が必要。 通常のサポート期間は5年程度であり、それ以上の期間を求める場合には、コストの上昇を招くか、対応可能なベンダーが非常に限られるおそれがあるので注意が必要。 クラウド※の場合は、サービス提供可能期間として捉える。 【注意事項】 ライフサイクル期間中は、ソフトウェア・ハードウェアのサポート切れが発生しないようにする必要が有る。 クライアントPCとして、情報システム専用でない（例えば庁内LAN用に一括購入した）PCを使用する場合等は、更改時のOSバージョンアップ等についてあらかじめベンダーと協議しておくこと。	レベル2の「7年」を設定しているが、10年の利用期間を前提とすること（10年のレベルがないため、レベル2を設定している）。
C.5.5.1			一次対応役割分担	一次対応のユーザ/ベンダーの役割分担。			2	すべてベンダーが実施	[-]ユーザにて一次切り分けが実施できるスキルが有る場合	仕様の対象としない	ベンダーによる提案事項	すべてユーザが実施	一部ユーザが実施	すべてベンダーが実施					
C.5.6.2			ベンダー側対応時間帯	一次対応のベンダーの対応時間。			1	ベンダーの定時時間内（9～17時）	[+]運用時間帯に合わせて拡張する必要性がある場合 [-]保守契約をしない場合	仕様の対象としない	ベンダーによる提案事項	対応無し	ベンダーの定時時間内（9～17時）	ユーザの指定する時間帯	24時間対応				

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	検収時の扱い[1]	利用ガイドの解説[2]	グループ②			レベル								備考 ［利用ガイド］第4章も参照のこと	要件説明
							選択レベル		選択時の条件	-	*	0	1	2	3	4	5		
D.1.1.2	移行性	移行時期	システム停止可能日時	移行作業計画から本稼働までのシステム停止可能日時。（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。）			4	利用の少ない時間帯（夜間など）	業務が比較的少ない時間帯にシステム停止が可能。 [-] 停止を増やす場合	仕様の対象としない	ベンダーによる提案事項	制約無し（必要な期間の停止が可能）	5日以上	5日未満	1日（計画停止日を利用）	利用の少ない時間帯（夜間など）	移行のためのシステム停止不可	【注意事項】 情報システムによっては、システム停止可能な日や時間帯が連続して確保できない場合がある。（例えば、この日は1日、次の日は夜間のみ、その次の日は計画停止日で1日、などの場合。） その場合には、システム停止可能日とその時間帯を、それぞれ確認すること。 【レベル】 レベル0は情報システムの制約によらず、移行に必要な期間のシステム停止が可能なことを示す。 レベル1以上は、システム停止に関わる（業務などの）制約が存在する上での、システム停止可能日時を示す。レベルが高くなるほど、移行によるシステム停止可能な日や時間帯など、移行計画に影響範囲が大きい制約が存在することを示している。	年末年始等の長期休暇でのシステム切替を想定。
D.3.1.1		移行対象（機器）	設備・機器の移行内容	移行前の情報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。		P44	4	移行対象設備・機器のシステム全部を入れ替えて、さらに統合化する	業務アプリケーションも含めた移行がある。 [-] 業務アプリケーション更改が無い場合 [+] 業務アプリケーションの更改程度が大きい場合	仕様の対象としない	ベンダーによる提案事項	移行対象無し	移行対象設備・機器のハードウェアを入れ替える	移行対象設備・機器のハードウェア、OS、ミドルウェア※を入れ替える	移行対象設備・機器のシステム全部を入れ替える	移行対象設備・機器のシステム全部を入れ替えて、さらに統合化する		【レベル】 移行対象設備・機器が複数あり、移行内容が異なる場合には、それぞれ合意すること。	次期システムでは、現行の調査入力システムを廃止し、現行台帳システムとともに再構築する想定のため、本レベルを設定している。
D.4.1.1		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）。		P45	1	1TB未満	10TB（テラバイト）未満のデータを移行する必要がある。 [-] 1TB未満の場合 [+] 10TB以上の場合	仕様の対象としない	ベンダーによる提案事項	移行対象無し	1TB未満	10TB未満	10TB以上				・現行データの内容は仕様書本編の「図表14 移行対象データ」を参照 ・データ容量の多くを占めると想定される画像・動画の次期システムにおける取り扱いは以下を想定しているが、システム動作の遅延防止やデータ容量の増加を抑制できるより良い方法があれば提案すること。 【画像】 共有フォルダ等のファイルサーバにアップロードし次期システムから共有フォルダへのリンクをクリックすることで参照可能に 【動画】（調査委託時の撮影動画等） 共有フォルダ等にはアップロードせず、納品されたDVD等にある動画を必要なときに再生 ※ただし、急を要する場合の対応状況を機能要件4.3のチャット機能でやりとりする際には、撮影から1ヶ月程度限定で動画も保存することを想定
D.5.1.1		移行計画	移行のユーザ/ベンダー作業分担	移行作業の作業分担。			1	ユーザとベンダーと共同で実施	移行結果の確認等、一部を自治体職員が実施する形態を想定。 [+] 移行データの確認を自治体が実施しない場合	仕様の対象としない	ベンダーによる提案事項	すべてユーザ	ユーザとベンダーと共同で実施	すべてベンダー				【注意事項】 最終的な移行結果の確認は、レベルに関係なくユーザが実施する。なお、ユーザデータを取り扱う際のセキュリティに関しては、ユーザとベンダーで取り交わしを行うことが望ましい。 【レベル1】 共同で移行作業を実施する場合、ユーザ/ベンダーの作業分担を規定すること。特に移行対象データに関しては、旧システムの移行対象データの調査、移行データの抽出/変換、本番システムへの導入/確認、等について、その作業分担を規定しておくこと。 【注意事項】 ベンダーに移行作業を分担する場合については、既存システムのベンダーと新規システムのベンダーの役割分担を検討する必要がある。	
F.1.1.1	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庁内基準や法令、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。 例） ・J-SOX法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・FISC ・プライバシーマーク ・構築実装場所の制限 など			1	制約有り（重要な制約のみ適用）	庁内規約などが存在する場合を想定。 [-] 法や条例の制約を受けない場合、もしくは業界などの標準や取り決めなどがない場合	仕様の対象としない	ベンダーによる提案事項	制約無し	制約有り（重要な制約のみ適用）	制約有り（すべての制約を適用）				【注意事項】 情報システムを開発する際に、機密情報や個人情報等を取り扱う場合がある。これらの情報が漏洩するリスクを軽減するために、プロジェクトでは、情報利用者の制限、入退室管理の実施、取り扱い情報の暗号化等の対策が施された開発用環境を整備する必要が生じる。 また運用予定地での構築が出来ず、別地に環境設定作業場所を設けて構築作業を行った上で運用予定地に搬入しなければならない場合や、逆に運用予定地でなければ構築作業が出来ない場合なども制約条件となる。	
F.1.2.1			運用時の制約条件	運用時の制約となる庁内基準や法令、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。 例） ・J-SOX法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・プライバシーマーク ・リモートからの運用の可否 など			1	制約有り（重要な制約のみ適用）	設置に関して何らかの制限が発生するセンターやマシンルームを前提として考慮。ただし条件の調整などが可能な場合を想定。 [+] 設置センターのポリシーや共同運用など運用に関する方式が制約となっている場合	仕様の対象としない	ベンダーによる提案事項	制約無し	制約有り（重要な制約のみ適用）	制約有り（すべての制約を適用）					
F.2.2.1		システム特性	クライアント※数	情報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※（端末）の数。 専用端末、共用端末問わず、当該システムで使用するクライアント数を示す。			1	上限が決まっている	あらかじめ一定の値を決めて合意することを想定。 [+] 上限台数を設定できない場合	仕様の対象としない	ベンダーによる提案事項	特定クライアント※のみ	上限が決まっている	不特定多数のクライアント※が利用					
F.2.5.1		システム特性	特定製品の採用有無	ユーザの指定によるオープンソース※製品や第三者製品（独立系ソフトウェア会社/独立系ハードウェア会社）などの採用の有無を確認する項目。採用によりサポート難易度への影響があるかの視点で確認を行う。		P45	0	特定製品の指定がない	構成する機器に関して固有の製品が指定された場合を想定。 [-] 特に指定がない場合	仕様の対象としない	ベンダーによる提案事項	特定製品の指定がない	一部に特定製品の指定がある	サポートが困難な製品の指定がある					

1 検収時の扱い　　○：目標（値）として扱い、長期的に測定・評価を行うべき項目

2 利用ガイドの解説　　Pxx：利用ガイドのメトリクス詳細説明ページ

3 「※」が付記された用語　　利用ガイド及び調査報告書の用語集にて解説のあるIT専門用語

別紙1 非機能要件一覧 【Ⅲ実現方法要求事項シート】

本資料は、独立行政法人情報処理推進機構が作成した「非機能要求グレード」を財団法人地方自治情報センターが地方公共団体向けに一部変更したものを基に、今回の次期システムに求める要件を整理しています。
次期システムに求める要件は、「グループ②：選択レベル」列に記載の選択レベルとなります。また、右端の「要件説明」列に適宜具体的な要件も記載していますので、併せてご確認ください。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	検収時の扱い[2]	利用ガイドの解説[3]	グループ②		レベル								備考 ［利用ガイド］第4章も参照のこと	要件説明
							選択レベル	選択時の条件	-	*	0	1	2	3	4	5		
A.2.1.1	可用性	耐障害性	冗長化※[4]（サーバ機器）	サーバ機器を物理的に複数用意し、1台が故障しても他方で稼働が可能な状態にすること。ハードウェア構成を決定するために必要。		P47	2	すべてのサーバで冗長化※	特定のサーバで冗長化※ [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	非冗長※構成	特定のサーバで冗長化※	すべてのサーバで冗長化※			【レベル1】 特定のサーバで冗長化※とは、情報システムを構成するサーバの種別（DBサーバ※やAPサーバ※、監視サーバなど）で冗長化の対応を分けることを意味する。 また要求としてサーバの単位ではなく、業務や機能の単位で冗長化※を指定する場合もある。	上下水道システム基盤を利用しない場合は、本要件を満たすこと。
A.2.5.1			冗長化（ストレージ※機器）	ディスクアレイ※などの外部記憶装置を物理的に複数用意し、1台が故障しても他方で稼働が可能な状態にすること。ハードウェア構成を決定するために必要。		P47	0	非冗長構成※	特定の機器のみ冗長化※ [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	非冗長構成※	特定の機器のみ冗長化※	すべての機器を冗長化※			【レベル1】 特定の機器のみとは、導入するストレージ※装置に格納するデータの重要度に応じて、耐障害性の要求が装置ごとに異なる場合を想定している。	上下水道システム基盤を利用しない場合は、本要件を満たすこと。
A.2.5.3			冗長化（ストレージ※のディスク）	ハードディスクを物理的に複数用意し、1台が故障しても他方で稼働が可能な状態にすること。ハードウェア構成を決定するために必要。		P48	1	RAID5※による冗長化※	RAID5※による冗長化※ [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	非冗長構成※	RAID5※による冗長化※	RAID1※による冗長化※			【レベル2】 性能での要件からRAID0※との組み合わせを検討する。	上下水道システム基盤を利用しない場合は、本要件を満たすこと。 なお、レベル1を設定しているが、上下水道局システム基盤と同等の構成を要求したいため、「RAID6」とすること。
A.3.1.1		災害対策	復旧方針	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代替の機器として、どこに何が必要かを決める。		P48	2	同一の構成で情報システムを再構築	災害発生後に調達したハードウェア等を使用し、同一の構成で情報システムを再構築することを想定 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	復旧しない	限定された構成で情報システムを再構築	同一の構成で情報システムを再構築	限定された構成をDRサイト※で構築	同一の構成をDRサイト※で構築		【レベル】 レベル1及び3の限定された構成とは、復旧する目標に応じて必要となる構成（例えば、冗長化※の構成は省くなど）を意味する。 【注意事項】 データセンター等の庁舎外にサーバを設置する場合は、庁舎がDRサイトの位置づけとなる場合もある。	
A.3.2.1			保管場所分散度（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、データ・プログラムを運用サイトと別の場所へ保管する。			2	1ヶ所（遠隔地）	遠隔地1ヵ所 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	外部保管しない	1ヶ所（近隣の別な建物）	1ヶ所（遠隔地）	2ヶ所（遠隔地）			【注意事項】 ここで遠隔地とは、サーバ等の設置場所から見ての遠隔地であり、庁舎等の利用場所から見ての遠隔地では無い。	
A.3.2.2			保管方法（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、データ・プログラムを運用サイトと別の場所へ保管するための方法。		P49	0	媒体による保管	媒体による保管を想定。 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	媒体による保管	同一システム設置場所内の別ストレージ※へのバックアップ	DRサイト※へのリモートバックアップ※					
B.1.3.1	性能・拡張性	業務処理量	保管期間（データ）	情報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。必要に応じて、データの種別ごとに定める。保管対象のデータを選択する際には、対象範囲についても決めておく。			3	5年	税制などの対応で保管期間が規定されているという想定。 [-] 参照期間が限られていて、バックアップ媒体に吸い上げることが可能な場合 [+] ディスク容量に余裕がある場合	仕様の対象としない	ベンダーによる提案事項	6ヶ月	1年	3年	5年	7年	10年以上有期	【レベル】 それぞれの情報システム（住民情報、税等）でデータの保管期間が異なる場合は、それぞれの対象データについて決めること。	
C.1.2.3	運用・保守性	通常運用	データ復旧の対応範囲	データの損失等が発生したときに、どのような事象に対して対応する必要があるかを示す項目。		P50	1	障害発生時のデータ損失防止	障害発生時に決められた復旧時点（RPO）へデータを回復できれば良い。 [-] 障害時に発生したデータ損失を復旧する必要がない場合 [+] 職員の作業ミスなどによって発生したデータ損失についても回復できることを保証したい場合	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	障害発生時のデータ損失防止	変更・削除したファイルの復旧				【注意事項】 職員の入力ミスを想定した変更・削除したファイルの復旧の場合、情報システムとしては正常に完了してしまった処理を元に戻さなければならないため、ファイルサーバ以外の情報システムでは実現できないと考えて良い。	
C.1.2.4			バックアップ自動化の範囲	バックアップ自動化の範囲。 バックアップ運用には、 ・スケジュールに基づくジョブ起動※ ・バックアップ対象の選択 ・バックアップ先メディアの選択（外部媒体交換） ・ファイル転送 などといった作業ステップが存在する。別地保管を媒体搬送で行う場合の、外部媒体交換はここには含まない。		P50	2	1ステップのみ手動で行う（外部媒体交換のみ）	バックアップに関するオペレーション※はバックアップ管理のソフトウェアを導入して自動化するが、ハードウェアが対応していないためメディア管理（外部媒体交換）だけは手動にて実施する必要がある。 [-] 手間は増えるが、障害発生時の影響範囲を少なくするため、複数の作業単位に区切ってスクリプト※化する場合 [+] メディア管理も自動で行いたい場合	仕様の対象としない	ベンダーによる提案事項	全ステップを手動で行う	数ステップを手動で行う（外部媒体交換とバックアップ開始コマンド※の入力）	1ステップのみ手動で行う（外部媒体交換のみ）	全ステップを自動で行う				

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	検収時の扱い[1]	利用ガイドの解説[2]	グループ②			レベル								備考 ［利用ガイド］第4章も参照のこと	要件説明
							選択レベル		選択時の条件	-	*	0	1	2	3	4	5		
C.1.3.1			監視情報	情報システム全体、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。 監視とは情報収集を行った結果に応じて適切な宛先に発報することを意味する。本項目は、監視対象としてどのような情報を発信するべきかを決定することを目的としている。 セキュリティ監視については本項目には含めない。「E.7.1 不正監視」で別途検討すること。		P51	4	リソース監視を行う	夜間の障害時にも、管理者に状況を通知し、すぐ対処が必要なのかどうかを判断するため、詳細なエラー情報まで監視を行うことを想定。 [-] 障害時は管理者がすぐに情報システムにアクセスできるため、詳細なエラー情報まで監視する必要がない場合 [+] エラー情報だけでなく、リソース使用状況も監視して、障害発生を未然に防ぎたい場合	仕様の対象としない	ベンダーによる提案事項	監視を行わない	死活監視を行う	エラー監視を行う	エラー監視（トレース情報を含む）を行う	リソース監視を行う	パフォーマンス監視を行う	【レベル】 死活監視とは、対象のステータス※がオンラインの状態にあるかオフラインの状態にあるかを判断する監視のこと。 エラー監視とは、対象が出力するログ等にエラー出力が含まれているかどうかを判断する監視のこと。トレース情報※を含む場合は、どのモジュール※でエラーが発生しているのか詳細についても判断することができる。 リソース監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいてCPUやメモリ、ディスク、ネットワーク帯域といったリソースの使用状況を判断する監視のこと。 パフォーマンス監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいて、業務アプリケーションやディスクの入出力、ネットワーク転送等の応答時間やスループット※について判断する監視のこと。 【運用コストへの影響】 エラー監視やリソース監視、パフォーマンス監視を行うことによって、障害原因の追求が容易となったり、障害を未然に防止できるなど、情報システムの品質を維持するための運用コストが下がる。	
C.4.1.1		運用環境	開発用環境の設置有無	開発用環境とは、本番環境とは別に開発専用に使用することのできる機材一式のことを指す。 本番移行後に本番環境として利用される開発フェーズの環境は、本項目に含めない。			0	情報システムの開発用環境を設置しない	ベンダーの開発用環境（案件専用でない）による開発を想定。 [+] 庁舎内に開発用環境を設置した方が開発の効率が良いため短期間で大規模の開発を実施する場合や、セキュリティ上庁舎外にて開発することが難しいソフトウェアの場合	仕様の対象としない	ベンダーによる提案事項	情報システムの開発用環境を設置しない	運用環境より機器構成を縮小した開発用環境を設置する	運用環境と同一の開発用環境を設置する					
C.4.2.1			試験用環境の設置有無	試験用環境とは、本番環境とは別に試験専用に使用することのできる機材一式のことを指す。本番移行後に本番環境として利用される試験フェーズの環境は、本項目に含めない。		P52	2	専用の試験用環境を設置する	専用の試験用環境を設置する。 [-] 開発環境と試験用環境を併用する場合、または、情報システムの試験環境を設置しない場合	仕様の対象としない	ベンダーによる提案事項	情報システムの試験用環境を設置しない	情報システムの開発用環境と併用する	専用の試験用環境を設置する					
C.5.9.1		サポート体制	定期報告会実施頻度	保守に関する定期報告会の開催の要否。	○		4	月1回	[-] 報告の必要が無い場合。 [+] 運用業務委託をしている場合や、SLAを設定している場合、必要に応じて。	仕様の対象としない	ベンダーによる提案事項	無し	年1回	半年に1回	四半期に1回	月1回	週1回以上	【注意事項】 障害発生時に実施される不定期の報告会は含まない。	
C.5.9.2			報告内容のレベル	定期報告会において報告する内容の詳しさを定める項目。			3	障害及び運用状況報告に加えて、改善提案を行う	[+] 運用業務委託をしている場合や、SLA※を設定している場合、必要に応じて。	仕様の対象としない	ベンダーによる提案事項	無し	障害報告のみ	障害報告に加えて運用状況報告を行う	障害及び運用状況報告に加えて、改善提案を行う				
C.6.2.1		その他の運用管理方針	問い合わせ対応窓口の設置有無	ユーザの問い合わ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。		P52	2	ベンダーの常駐等専用窓口を設ける	サポート契約を締結するベンダーの既設コールセンターが問い合わせ対応窓口となることを想定 [-]問い合わせ対応窓口設置しない場合 [+] 常駐するベンダー作業員が問い合わせ対応窓口となる場合等	仕様の対象としない	ベンダーによる提案事項	問い合わせ対応窓口の設置について規定しない	ベンダーの既設コールセンターを利用する	ベンダーの常駐等専用窓口を設ける				【注意事項】 ここでは、ユーザとベンダー間における問い合わせ窓口の設置の有無について確認する。問い合わせ対応窓口機能の具体的な実現方法については、別途に具体化する必要が有る。	
D.1.1.1	移行性	移行時期	システム移行期間	移行作業計画から本稼働までのシステム移行期間。			4	2年未満	年度を跨いで移行を進める必要がある。 [-] 期間短縮の場合 [+] さらに長期期間が必要な場合	仕様の対象としない	ベンダーによる提案事項	システム移行無し	3ヶ月未満	半年未満	1年未満	2年未満	2年以上		
D.1.1.3			並行稼働の有無	移行作業計画から本稼働までの並行稼働の有無。			1	有り	移行のためのシステム停止期間が少ないため、移行時のリスクを考慮して並行稼働は必要。 [-] 移行のためのシステム停止期間が確保可能であり、並行稼働しない場合	仕様の対象としない	ベンダーによる提案事項	無し	有り					【レベル1】 並行稼働有りの場合には、その期間、場所等を規定すること。	現行システムを令和9年3月末まで利用可能な状態としておく想定。
E.3.1.2	セキュリティ	セキュリティ診断	Web診断実施の有無	Web診断とは、Webサイトに対して行うWebサーバ※やWebアプリケーション※に対するセキュリティ診断のこと。			1	実施	内部ネットワーク経由での攻撃に対する脅威が発生する可能性があるため対策を講じておく必要がある。 [-] 内部犯を想定する必要がない場合、Webアプリケーション※を用いない場合	仕様の対象としない	ベンダーによる提案事項	不要	実施					【注意事項】 詳細は、当センターの「地方公共団体における情報システムセキュリティ要求仕様モデルプラン」を参照の上、対策を検討すること。	

1 検収時の扱い　　○：目標（値）として扱い、長期的に測定・評価を行うべき項目

2 利用ガイドの解説　　Pxx：利用ガイドのメトリクス詳細説明ページ

3 「※」が付記された用語　　利用ガイド及び調査報告書の用語集にて解説のあるIT専門用語