【美里（TKC）】非機能要件の標準－採択団体別検証項目

非機能要件の標準										採択団体記入欄（検証実施前）							
連番	項番	大項目	中項目	メトリクス（指標）	メトリクス説明	選択レベル		選択時の条件	備考	選択レベル		検証実施有無		検証事項	検証範囲	検証方法	
												実施有無	判断理由（無の場合のみ記入）			種別	方法
1	C.1.2.2	運用・保守性	通常運用	外部データの利用可否	外部データによりシステムのデータが復旧可能かどうか確認するための項目。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	システムの復旧に外部データを利用できない	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	【注意事項】 外部データによりシステムのデータが復旧可能な場合、システムにおいてバックアップ設計を行う必要性が減るため、検討の優先度やレベルを下げて考えることができる。	2	システムの復旧に外部データを利用できない	有		システム・データを復元するための手順を作成し、その手順通りに復元できることを確認する。	システム全般（主にデータ）	実機	AWS Backupまたは既存のバックアップツールを利用し、AMIあるいはS3を利用したバックアップから、データが復元できることを確認する。
2	C.2.3.5	運用・保守性	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。脆弱性に対するセキュリティパッチなどの緊急性の高いものは即座に適用する。	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）。	【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.4.3.4）。なお、「即時」と記載しているが、事前検証なくパッチを適用しなければならないというわけではない。	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	有		パッチの適用が自動化されていることを確認する。	システムを構成するすべてのサーバ	実機	WSUS または AWS Systems Manager 等を用い、各サーバにパッチが所定の時間（保守時間）に自動で適用されることを確認する。
3	E.1.1.1	セキュリティ	前提条件・制約事項	順守すべき規定、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） ・情報セキュリティに関する法令 ・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（総務省） ・その他のガイドライン ・その他のルール	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	【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。	1	有り	有		順守すべき法令・ポリシー・ガイドラインに沿った機能・非機能が実現できていることを確認する。	システムを構成するすべてのサーバ、ネットワーク	机上	順守すべき法令・ポリシー・ガイドラインに沿った機能・非機能が実現できていることを確認する。（情報セキュリティに関する法令、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（総務省）、LGWAN-ASPセキュリティ要綱、等）
4	E.2.1.1	セキュリティ	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	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	【レベル1】 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）。	1	重要度が高い資産を扱う範囲	有		ガバクラ化による変化（データの保管場所やライフサイクルの違い）を意識したうえで情報資産の重要性を再確認し、リスク分析範囲を明らかにする。	システムを構成するすべてのサーバ、ネットワーク	机上	ガバクラ化による変化（データの保管場所やライフサイクルの違い）を意識したうえでリスク分析を行い、結果を受けて対応を検討する。
5	E.4.3.4	セキュリティ	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。	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、ファイルが公開されるとシステムに自動的に適用されることを想定。 [-]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）。		2	定義ファイルリリース時に実施	有		ウィルス定義ファイルの適用が自動化されていることを確認する。	システムを構成するすべてのサーバ	実機	WSUS または AWS Systems Manager等 を用い、各サーバに定義ファイルが自動で適用されることを確認する。
6	E.5.1.1	セキュリティ	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。	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	【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。	3	複数回、異なる方式による認証	有		現システムで利用している認証機器を利用した二要素認証が実現できることを確認する。	システムの利用者環境、関連ミドルウェア	実機	① 顧客側：２要素認証が正常に機能することを確認する。 ※ 令和３年度事業は、回線の開通状況により、検証の幅が狭まる可能性がある。 ② 運用・保守側：AWSマネジメントコンソール等のクラウドサービス管理画面においてはMFA認証が設定されていること。
7	E.5.2.1	セキュリティ	アクセス・利用制限	システム上の対策における操作制限	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、ソフトウェアにより制限するか確認するための項目。 例） 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	必要最低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許可する。	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		1	必要最低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許可する。	有		対象の資産に対し、認証・許可されたユーザーからのみアクセス・操作が可能であることを確認する。	システム全般	実機	現行→ガバメントクラウドへと環境変更する点に関し、リスクの観点から検証すべきポイントを洗い出し、新たなアクセス・利用制限が必要となる個所が発生するかどうかを確認する。（例えば、S3 への直接的なアクセス、監視結果画面へのアクセス等）
8	E.6.1.1	セキュリティ	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。	1	認証情報のみ暗号化	内部ネットワークのみ接続する情報システムを想定。 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。	【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）。	3	すべてのデータを暗号化	有		庁舎⇔AWSの間の通信が、暗号化されていることを確認する。	ネットワーク	実機	庁舎⇔AWSの間の通信が、通信の特性やリスクに応じて暗号化されていることを確認する。
9	E.6.1.2	セキュリティ	データの秘匿	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。	1	認証情報のみ暗号化	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	【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）。	2	重要情報を暗号化	有		ミドルウェア及びアプリケーションの機能により、暗号化された状態で保管されていることを確認する。	システムを構成するDBサーバ	実機	保管されたデータが暗号化/符号化かれており、仮に奪取されても識別できない情報となっていることを確認。（直接的にRDB上のデータの参照しての確認）
10	E.7.1.1	セキュリティ	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）	【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	1	必要なログを取得する	有		システムを構成するサーバのOS及びミドルウェア、アプリケーションログから、必要なログが取得できていることを確認する。	ログ保管サーバ、または共有ストレージ	実機	システムを構成するサーバのアクセスログ及びミドルウェアのログ、および監査機能によるログが記録されていること、これらログファイルがログ保管サーバに収集されていることを実際に目視して確認する。
11	E.7.1.3	セキュリティ	不正追跡・監視	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	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。		1	重要度が高い資産を扱う範囲	有		同 No.10	同 No.10	実機	同 No.10

非機能要件の標準										採択団体記入欄（検証実施前）							
連番	項番	大項目	中項目	メトリクス（指標）	メトリクス説明	選択レベル		選択時の条件	備考	選択レベル		検証実施有無		検証事項	検証範囲	検証方法	
												実施有無	判断理由（無の場合のみ記入）			種別	方法
12	E.10.1.1	セキュリティ	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。	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		1	対策の強化	無	現製品において実装済みであること、および内部ネットワークで利用するシステムであることから、検証は不要と判断。				
13	E.10.1.2	セキュリティ	Web対策	WAFの導入有無	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。	0	無し	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。 [+]Webアプリケーションを用いる場合		0	無し	無	WSUSであればNAT Gateway、あるいは Sysmtes Manager経由を想定していたことから、WAF導入は必須ではない、とします。				
14	A.1.3.1	可用性	継続性	RPO（目標復旧地点）（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。	2	1営業日前の時点（日次バックアップからの復旧）	システム障害時において、障害復旧完了後、バックアップデータを使用したリストアを行うことを想定。 [-]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） [+]選択レベルの時点（1営業日前の時点）での復旧では後追い入力が膨大に発生する等業務への支障が大きいことが明らかである場合	【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。	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）	有		・業務停止（擬似障害）を伴う障害が発生した際に、障害発生直前の状態で業務継続できることを確認する。	業務システムすべて	実機	AWS DMSを用いてレプリケーションを行っている状態から、業務停止（疑似的）を発生させた際、データ同期先の環境において障害発生直前の状態で業務継続（縮退運転）ができることを確認
15	A.1.3.2	可用性	継続性	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。	2	12時間以内	窓口対応等、システム停止が及ぼす影響が大きい機能の復旧を優先しなるべく早く復旧する。 [-] 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、業務への支障が大きいことが明らかである場合	【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。	*	クラウド及びネットワークに起因する場合は３時間以内、アプリケーションに起因する場合は12時間以内	有		同 No.14	同 No.14	実機	同 No.14
16	A.1.3.3	可用性	継続性	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。	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	【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。）	2	全システム機能の復旧	有		同 No.14	同 No.14	実機	同 No.14
17	A.1.4.1	可用性	継続性	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。	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。また、復旧までの間、バックアップデータから必要なデータをＣＳＶ等で自治体が利用できる形式で提供（※）する。※住民記録システム等、住民の安否確認に必要なデータを持つシステムについては、発災後72時間以内に、必要なデータを自治体が利用できる形式で提供すること。 [+]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場合	【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。	2	一ヶ月以内に再開	有		これまでにAWSで発生した（公表された）大規模障害をベースに、１か月以内にシステム復旧が可能であることを確認 また、上記期間内に復旧ができない場合でも、72時間以内に必要なデータを自治体が利用可能な形式で取得可能であることを確認する。	システム全般	実機	西日本リージョンは被害をうけていないことを前提として、西日本リージョンにバックアップした情報からシステムを復旧し、顧客サイトから接続できることを確認する。 システム復旧と並行し、上記期間内に復旧ができないケースを想定して、72時間以内に住民の安否確認に必要なデータを自治体が利用可能な形式で取得・提供が可能であることを確認
18	A.1.5.1	可用性	継続性	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。一般的にサービス利用料と稼働率は比例関係にある。	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、業務への支障が大きいことが明らかである場合 [-]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。	【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	3	99.5%	有		検証機関において、システム全体で 99.5% の稼働率が達成できることを確認する。	システム全般	実機	想定ユーザーと同様のネットワーク経路・利用方法・利用時間帯・利用頻度で基幹システムに悪セスし、代表的な機能をサービス提供時間帯において、想定した稼働率以上に継続して利用できることを確認する。（RPAや検証用のツール（独自）を利用することを想定）
19	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	基幹系システムの場合は、業務ごとに特定のユーザが使用することを想定。		1	上限が決まっている	有		各業務システムの利用可能上限数を調査する。 最大人数利用時に性能面等に問題が出ていないことを確認する。	システムを構成するすべてのサーバ	実機	一定期間職員様に検証環境をご利用いただき、各業務の総利用者数が、あらかじめ許可を与えられた人数以内であることを確認する。
20	B.1.1.2	性能・拡張性	業務処理量	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	同時アクセス数の上限が決まっている	特定のユーザがアクセスすることを想定。		1	同時アクセス数の上限が決まっている	有		各業務システムで想定する同時アクセス数の上限数を調査する。 最大人数利用時に性能面等に問題が出ていないことを確認する。	システムを構成するすべてのサーバ	実機	一定期間職員様に検証環境をご利用いただき、各業務の同時利用者数が、あらかじめ許可を与えられた人数以内であることを確認する。
21	B.1.1.3	性能・拡張性	業務処理量	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。	0	すべてのデータ件数、データ量が明確である	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	【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、住民記録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。	0	すべてのデータ件数、データ量が明確である	有		各業務システムで管理するデータ総数（件数・量）を集計し、現行システムと同等であることを確認する。	DBサーバ	実機	現行システムで管理しているデータ総数と、移行後の環境のデータ総数を比較し、大きな相違がないことを確認する。
22	B.1.1.4	性能・拡張性	業務処理量	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。	0	処理ごとにリクエスト件数が明確である	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	【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、住民記録システムの転入・転出処理などがある。	0	処理ごとにリクエスト件数が明確である	有		各業務システムで受け付けるリクエスト件数を集計し、現行システムと同等であることを確認する。	Webサーバ	実機	現行システムで管理しているリクエスト数と、移行後のリクエスト数を比較し、大きな相違がないことを確認する。
23	B.1.1.5	性能・拡張性	業務処理量	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。	0	処理単位ごとに処理件数が決まっている	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	【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。	0	処理単位ごとに処理件数が決まっている	有		各業務システムで受け付けるバッチ処理数を集計し、現行システムと同等であることを確認する。	APサーバ	実機	現行システムで管理しているバッチ処理数と、移行後のバッチ処理数を比較し、大きな相違がないことを確認する。

非機能要件の標準										採択団体記入欄（検証実施前）							
連番	項番	大項目	中項目	メトリクス（指標）	メトリクス説明	選択レベル			備考	選択レベル		検証実施有無		検証事項	検証範囲	検証方法	
								選択時の条件				実施有無	判断理由（無の場合のみ記入）			種別	方法
24	B.2.1.4	性能・拡張性	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）	3	3秒以内	管理対象とする処理の中で、通常時の照会機能など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 [+]コストと実現性を確認した上で、業務への支障が大きいことが明らかである場合	【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。	3	3秒以内	有		原則として、アプリケーションの改修をせずに、現行システムと同等のレスポンスが返ってくることを確認する。	システム全般（Webレスポンス、バッチ処理時間、印刷時間等）	実機	令和３年度は、代表的なシステム・よく使われる機能にフォーカスし、現行環境と同等レベルのレスポンスが継続して得られることを確認する。 ※ 令和３年度事業は、限定された環境（データ、回線、負荷の面において）の中での簡易検証となる予定。
25	B.2.1.5	性能・拡張性	性能目標値	アクセス集中時の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）	2	5秒以内	管理対象とする処理の中で、ピーク時の照会機能など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 [+]コストと実現性を確認した上で、業務への支障が大きいことが明らかである場合	【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。	2	5秒以内	有		同 No.24	同 No.24	実機	同 No.24
26	B.2.2.1	性能・拡張性	性能目標値	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） ※「通常時」とは、運用保守期間のうち、繁忙期間（住基業務であれば転入・転出の多い年度末・年度当初、個人住民税業務であれば確定申告時期・当初課税時期等）及び想定量を超える処理が発生した期間を除いた期間をいう。	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、エラーが発生するなどして処理結果が不正の場合、再実行できれば良いと想定。 [-]再実行をしない場合または代替手段がある場合		2	再実行の余裕が確保できる	有		同 No.24	同 No.24	実機	同 No.24
27	B.2.2.2	性能・拡張性	性能目標値	アクセス集中時の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、ピーク時のバッチ処理を実行し、エラーが発生するなどして処理結果が不正の場合、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		2	再実行の余裕が確保できる	有		同 No.24	同 No.24	実機	同 No.24
28	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。）	1	定時内での利用（1日8時間程度利用）	開庁時間を定時と想定。 [-]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	【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。	2	定時外も頻繁に利用（1日12時間程度利用）	有		運転スケジュール通りにシステムが利用できることを確認する。	システム全般	実機	運転スケジュール通りに定期タスク等が起動し、システムが利用できることを確認する。
29	C.1.1.2	運用・保守性	通常運用	運用時間（休日等）	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。）	1	定時内での利用（1日8時間程度利用）	休日等の窓口開庁がある場合を想定。 [-]休日の窓口開庁や休日出勤がない場合 [+]定時外も頻繁に利用される場合		1	定時内での利用（1日8時間程度利用）	有		同 No.28	同 No.28	実機	同 No.28
30	C.1.2.5	運用・保守性	通常運用	バックアップ取得間隔	バックアップ取得間隔	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		4	日次で取得	有		業務システムの要件として求められるバックアップが実現できることを確認する。	データ	実機	S3に対するバックアップと世代管理、冗長化が図れていることを確認する。また、バックアップ済みデータから、世代を指定して戻すことができることも確認する。
31	C.4.3.1	運用・保守性	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。	2	情報システムの通常運用と保守運用マニュアルを提供する	運用をユーザが実施することを想定。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	【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。	2	情報システムの通常運用と保守運用マニュアルを提供する	有		通常運用と保守の範囲を明確にしたうえで、マニュアル通りに運用ができることを確認する。	システム全般	実機	アプリケーション開発事業者より運用・保守マニュアルを提示し、２町に確認いただいたうえで、内容に問題がないことを確認いただく。
32	C.4.5.1	運用・保守性	運用環境	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 [+]庁外の外部システムに接続して、データのやり取りを行う場合	【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。	1	庁内の外部システムと接続する	有		業務上必要となる連携処理が、機能面・非機能面で現状と同等レベルで実現し、かつコスト面でも課題が出ないことを確認する。	システム全般（基幹システム＋連携対象となるシステム）	机上	多数の連携処理があることから、令和３年度事業で検証可能な範囲で、連携可否（プロトコル、通信の方向、性能、コスト等）について確認を行う。 ※ 令和３年度は机上中心とし、すべての動作検証は令和４年度とする。
33	C.5.2.2	運用・保守性	サポート体制	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	ソフトウェアがバージョンアップした場合に、ベンダーがアップデートすることを想定。 [-]アップデート権を必要としない場合		2	アップデート	有		ガバメントクラウドへのライセンス持ち込め可否や、アップデートに必要な設備（回線等）を準備できるかどうかを確認する。	OS、ミドルウェア	机上	OS、ミドルウェアの関連ベンダーにヒアリングし、運用保守に必要な構成をガバメントクラウド上で構築できるかについて確認する。 ※ 令和３年度は机上確認とし、実機検証は令和４年度とする。

非機能要件の標準										採択団体記入欄（検証実施前）							
連番	項番	大項目	中項目	メトリクス（指標）	メトリクス説明	選択レベル			備考	選択レベル		検証実施有無		検証事項	検証範囲	検証方法	
								選択時の条件				実施有無	判断理由（無の場合のみ記入）			種別	方法
34	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	【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。	4	利用の少ない時間帯（夜間など）	有		業務終了後、翌営業日までにシステム移行が完了することを確認する。	システム全般	実機	夜間作業にてシステム移行が完了できる移行計画を複数策定し、机上シミュレーションにて実現性について比較検討する。 ※ 令和３年度は机上確認とし、実機検証は令和４年度とする。
35	D.3.1.1	移行性	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。	3	移行対象設備・機器のシステム全部を入れ替える	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	【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。	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	有		同 No.34	同 No.34	実機	同 No.34
36	D.4.1.1	移行性	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、移行データに含まれるPDFなどの電子帳票類を含む）。	*	ベンダーによる提案事項	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	【注意事項】 データベースの使用量をそのまま使用すると、ログデータなど移行には必要のないデータも含まれる場合がある。	*	ベンダーによる提案事項	有		同 No.34	同 No.34	実機	同 No.34
37	D.5.1.1	移行性	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。 [+]標準仕様準拠のシステムから標準仕様準拠のシステムに移行する場合	【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。	1	ユーザとベンダーと共同で実施	有		同 No.34	同 No.34	実機	同 No.34
38	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 ・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（総務省） ・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	【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。	1	制約有り（重要な制約のみ適用）	有		ISMS、政府機関の情報セキュリティ対策のための統一基準、ISMAP、Pマーク、社内セキュリティポリシー等に従い、環境構築が行えることを確認する。	オペレーションルーム	実機	令和３年度においては、回線契約が間に合わない可能性があるため、令和４年次事業で検証すべき手順やルール整備や製薬事項の確認を行う。
39	F.1.2.1	システム環境・エコロジー	システム制約/前提条件	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 ・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（総務省） ・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		1	制約有り（重要な制約のみ適用）	有		同 No.38	同 No.38	実機	同 No.38
40	A.3.1.1	可用性	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。	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	【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。 DR（Disaster Recovery）サイトとは、災害などで業務の続行が不可能になった際に、緊急の代替拠点として使用する施設や設備のこと。	3	限定された構成をDRサイトで構築	有		業務停止（擬似障害）を伴う障害が発生した際に、障害発生直前の状態で業務継続できることを確認する。	業務システムすべて	実機	AWS DMSを用いて、庁舎内に設置した縮退運転サーバに、直前のデータがレプリケートされることを確認する。 DX切断などの障害を疑似的に発生させ、縮退環境で業務が継続できることを確認する。
41	A.3.2.1	可用性	災害対策	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	【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。	2	1ヶ所（遠隔地）	有		同 No.40	同 No.40	実機	同 No.40
42	A.3.2.2	可用性	災害対策	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。	1	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	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		2	DRサイトへのリモートバックアップ	有		同 No.40	同 No.40	実機	同 No.40

非機能要件の標準										採択団体記入欄（検証実施前）							
連番	項番	大項目	中項目	メトリクス（指標）	メトリクス説明	選択レベル			備考	選択レベル		検証実施有無		検証事項	検証範囲	検証方法	
								選択時の条件				実施有無	判断理由（無の場合のみ記入）			種別	方法
43	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、どのようなデータ損失に対して対応する必要があるかを示す項目。	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コストと実現性を確認した上で業務への支障が起きることは明らかな場合	【注意事項】 職員が一度正常に処理したデータについては、回復するデータには含まれない。	1	障害発生時のデータ損失防止	有		同 No.14	同 No.14	実機	同 No.14
44	C.1.3.1	運用・保守性	通常運用	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。	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 [+]通常よりも処理が集中することが予想できパフォーマンス監視が必要な場合	【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。 また、定期報告会には、リソース監視結果、パフォーマンス監視結果の報告は必須ではない。	5	パフォーマンス監視を行う	有		現在実施している監視方法およびマネージドの機能を利用し、リソースの利用状況を監視し、閾値を超えた場合のアラート発信ができることを確認。	システム全般、既存環境（現行データセンター）の運用拠点	実機	現状の監視ツールあるいはCloudWatchを利用し、各種監視や報知ができることを確認。 ※ 令和３年度は机上確認とし、実機検証は令和４年度とする。
45	C.5.9.1	運用・保守性	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。	3	四半期に1回	[-]保守に関する報告事項が予め少ないと想定される場合 [+]保守に関する報告事項が予め多いと想定される場合	【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。	4	月1回	有		報告頻度に関する契約上の取り決めがなされていることを確認。	システム全般	机上	現契約（最低月に１度）に従い実施する。
46	C.5.9.2	運用・保守性	サポート体制	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	障害発生時など改善提案が必要な場合を想定		3	障害及び運用状況報告に加えて、改善提案を行う	有		同 No.45	同 No.45	机上	同 No.45
47	C.6.2.1	運用・保守性	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。	1	ベンダーの既設コールセンターを利用する	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を設置する必要がない場合 [+]コストと実現性を確認した上で、常駐作業員がいないと適切な保守・運用ができないと考えられる場合	【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。	1	ベンダーの既設コールセンターを利用する	有		システム移行に際して想定される呼量の増加と、コールセンターのキャパシティを検討し、既設設備を利用するか新たな窓口を準備する必要があるかを確認する。	システム全般	机上	これまでのシステム移行の知見をベースに、どの程度の呼量が想定されるかについてのシミュレーションを行う。
48	D.1.1.1	移行性	移行時期	システム移行期間	移行作業開始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		4	1年未満	有		役所の繁閑期やベンダー側のリソース、環境構築・システム移行に係る負担を勘案しながら、現実的な移行期間を検討する。	システム全般	机上	これまでのシステム移行の知見をベースに、アプリケーション事業者で移行計画案を立て、まずは机上レベルで、ユーザーと一緒に移行シミュレーションを行う。
49	D.1.1.3	移行性	移行時期	並行稼働の有無	移行作業から本稼働までのシステムの並行稼働の有無。	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	【レベル1】 並行稼働有りの場合には、その期間、方法等を規定すること。	0	[-]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	無	並行稼働はしない予定。				
50	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		0	無し	無	閉域網で利用するサービスであることと、利用者庁舎内（職員）からに限られることから、「内部犯を想定する必要がない場合」に相当すると考える。				