【盛岡（ICS）】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		バックアップが適切な運用設計通りの間隔で正常に取得できており、リカバリができるかを検証	システム全体	実機	・データのバックアップが正常に取得・管理できているかを確認 ・バックアップからリカバリできることを確認
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。	3	緊急性の高いパッチのみ即時に適用を行う [-]外部と接続することが全くないため	有		緊急性の高いパッチについて、事前検証などを行ったうえで、適用対象範囲に即時にパッチが適用されること	システム全体	実機	盛岡市オンプレミス環境からAWS環境への更新パッチ配布手順を確立し、手順に従って更新パッチの適用ができることを検証
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		盛岡市セキュリティーポリシーや特定個人情報保護評価とシステムの設計・設定状況の整合性確認	システム全体	机上	盛岡市のポリシーをアプリケーション開発事業者とレビューを実施し整合性を確認
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		重要資産のリスク分析範囲が明確であるかを確認	システム全体	机上	・盛岡市でデータの重要度などからリスク分析すべき対象が明らかになっているかを確認
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）。		1	定期保守時に実施 [-]ウィルス定義ファイルが、自動的に適用できない場合	有		予め手動でパッチを当てる手順を確立し、定義ファイルリリース時に手順どおり実機で実施されることを確認	システム全体	実機	盛岡市基幹系業務システム（ハウジング、自庁サーバ）はクローズド環境を前提に自動でパッチを当てる構成をとっておらず、必要に応じて手動で当てている。その手順が確立していることを確認する。
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。	1	1回	有		システム利用時にID/パスワードによる認証が行われるか確認	システム全体	実機	・業務システムにおいて、システム起動時にID/パスワードを入力する画面が表示され、登録済のID/パスワードで認証できること、また、未登録のID/パスワードで認証されないことを確認 ・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MFA認証が設定されていることを確認
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		アプリケーションが動作するのに必要な最小限のポートのみ解放されていることを確認	業務システム	実機	・仮想マシンのセキュリティグループ（ファイアーウォール）で、インバウンド側のトラフィックに対し、サービス提供に必要なポートのみ解放を行うよう設定 ・上記について許可されていない通信が行われないことを確認
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）。	1	認証情報のみ暗号化	有		クローズドネットワーク前提で認証情報が暗号化されているかを確認	業務システム	机上	・アプリケーション開発事業者にて、設計及び実装上、認証情報が暗号化されていることを確認
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）。	1	認証情報のみ暗号化	有		認証情報が暗号化されているかを確認	業務システム	実機	ユーザー登録を行い、テーブルに格納されるパスワードが暗号化されている事を確認
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		下記のログが取得できていることを確認 サーバ系：IIS,SQLServerのログ。 アプリケーション：アクセスログ（ログインしたユーザ・日時・端末、各種操作記録等）。	システム全体	実機	・業務システムにおいて、必要なログが取得されていることを確認 ・AWSマネージドサービスによりログが取得されていることを確認
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		E.2.1.1で定めた重要資産においてログの取得範囲と保存期間の明確化	システム全体	机上	・盛岡市でログの取得範囲と保存期間を定義 ・上記の定義をアプリケーション開発事業者とレビューし整合性を確認

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
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	有		セキュリティ対策が実施されているか確認する。	システム全体	実機	・アプリケーション開発事業者においてセキュアコーディング（主に、SQLインジェクション対策）が講じられていることを確認 ・アプリケーション開発事業者において、Webサーバに対してAWSマネジメントサービスを利用し、脆弱性が無いかを検証
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	インターネット経由の接続は無いため				
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。	2	1営業日前の時点（日次バックアップからの復旧）	有		前日時点のバックアップから復旧を行い、前日業務終了時点からシステムが復旧することを確認	システム全体	実機	・RPO（目標復旧地点）のタイミング（前日業務終了時点）でバックアップを取得しAWSマネージドサービスの機能でリストアできることを確認
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。	2	12時間以内	有		バックアップデータの復旧にかかる時間を計測し、実運用に耐えられるかを検証	システム全体	実機	・AWS東リージョン上のマルチAZ構成のいずれもが障害となった場合を想定し、AWSマネージドサービスを用いてバックアップの取得・保管・復旧を検証 →上記に要する時間を計測し、実運用に耐えられるかを検証 →取得されたデータを用いて全システムが利用できることを確認
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		全システムが復旧できることを確認	システム全体	実機	A.1.3.2と同じ
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。	3	一週間以内に再開	有		・西リージョンでサーバが再現・復旧できることを確認 ・西リージョンでサーバが復旧するまでの間、住民の安否確認に必要なデータ（住基宛名データ等）をＣＳＶ等で自治体が利用できる形式で提供できることを確認	システム全体	実機	・AWS東リージョン障害時は、AWS西リージョンに複製されたバックアップデータを利用し、AWS西リージョン上でAWSマネージドサービスによりクラウド基盤を復旧 →上記の通り復旧できること、システムが利用できることを確認 ・住民の安否確認に必要なデータ（住基宛名データ等）は、毎日オンプレ側にデータ連携される。このデータを利用できることを確認。
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	4	99.9%	有		SLA99.9％以上であることを確認	業務システム	机上	・利用するAWSクラウドサービスにおいてSLA99.9%以上になる構成であることを確認
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		ユーザー数に上限があることを確認	業務システム	机上	・権限がある管理者のみがユーザー登録できること ・不特定多数のユーザーがアクセスできないことを確認
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		同時アクセス数を満たすサーバー構成やライセンスとなっていることを確認	業務システム	机上	B.1.1.1をもって上限とした、サーバー構成やライセンスを考慮しているかを確認
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		データ量が明確であることを確認	業務システム	机上	アプリケーション開発事業者がリフト対象業務のデータ件数とデータ量を測定し、盛岡市に提示
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		オンラインリクエスト件数を確認	業務システム	机上	アプリケーション開発事業者がログより主要業務の現状の処理件数を集計し、盛岡市に提示
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		バッチ処理件数を確認	業務システム	机上	アプリケーション開発事業者がログより主要バッチ（処理時間が30分以上の月次、年次バッチ）の現状の処理件数を集計し、盛岡市に提示

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		通常時を想定し、検索及び照会機能が概ね3秒以内に結果が返ることを確認	業務システム	実機	・現行環境下（オンプレミス）で概ね3秒以内に結果が返る処理において、設計上のサーバー性能状況下で検証 ・性能が出ない場合は、AWSマネージドサービスを利用しボトルネックを洗い出し確認 ・性能が出た場合、過剰なリソース設計となっていないことを確認
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		アクセス集中時を想定し、検索及び照会機能が概ね5秒以内に結果が返ることを確認	業務システム	実機	・DBに負荷をかけた状態で、B.2.1.4の検証を実施
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		通常時を想定した定例的なバッチ処理を実行し、再実行の余裕が確保できることを確認	業務システム	実機	設計上のサーバー性能状況下で検証 ・性能が出ない場合は、AWSマネージドサービスを利用しボトルネックを洗い出し確認 ・性能が出た場合、過剰なリソース設計となっていないことを確認
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		アクセス集中時及びピーク時のバッチ処理を実行し、再実行の余裕が確保できることを確認	業務システム	実機	・DBに負荷をかけた状態で、B.2.2.1の検証を実施
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。	1	定時内での利用（1日8時間程度利用）	有		設計通りでの利用がきるかの確認	業務システム	机上	・バックアップや夜間バッチ、その他プログラムバージョンアップ時以外は基本的にシステムが利用できる運用設計の共有
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		設計通りでの利用がきるかの確認	業務システム	机上	C.1.1.1と同じ
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		全体バックアップを週次で取得し、増分バックアップを日次で取得しているかの確認	業務システム	実機	・定期的なバックアップ作業はAWSマネージドサービスを用いて自動化されていることを確認 ・バックアップデータの保管先が要件に応じて冗長化されていることを確認
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のマニュアルを提供する	有		マニュアルの提供状況を確認	システム全体	机上	アプリケーション開発事業者が運用マニュアルを提示し、盛岡市とレビューし通常運用のマニュアルとて問題ないことを確認
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		庁内の他システムとの連携を確認	システム全体	実機	市⇔AWS間通信のDirect Connectを経由して庁内の他システムと連携できているかを検証
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		アプリケーション開発事業者によりアップデートが実施できるか確認	業務システム	実機	現行システムと同様にシステムのアップデートが実施されるか確認

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		システム移行を利用の少ない時間帯（土日・夜間等の閉庁時）に実施できるか確認	システム全体	実機	・ガバメントクラウド本番移行の移行計画書の作成 ・移行作業の計画段階で５日未満で実施できることを確認 ・移行計画書をもとに、移行リハーサル実施し５日未満で実施できることを確認 ・例外発生時に切り戻し作業も含めて５日未満で復旧出来ることを確認
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。	3	移行対象設備・機器のシステム全部を入れ替える	有		ガバメントクラウド上にシステムを移行できるか確認	システム全体	机上	・移行後システムが正常に動作しているか ・移行前システムと比較し、業務に影響を与える変更はないかを確認
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		現状のデータ量を把握	システム全体	机上	・アプリケーション開発事業者よりリフト対象業務のシステムのデータ量を提示 ・ログや履歴データなどの移行の必要有無や保存期間を確認
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		移行作業において，盛岡市とアプリケーション開発事業者において役割分担ができていることを確認	システム全体	机上	・アプリケーション開発事業者より役割分担に関する資料の提出 ・役割の内容を明確化していることを確認
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		構築において関係する制約の確認	システム全体	机上	・盛岡市においてシステム構築時の制約条件等を取りまとめる ・アプリケーション開発事業者において、制約条件等でシステム構築上問題ないかを確認
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		運用において関係する制約の確認	システム全体	机上	・盛岡市においてシステム運用時の制約条件等を取りまとめる ・アプリケーション開発事業者において、制約条件等でシステム運用上問題ないかを確認
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。	2	同一の構 成で情報 システム を再構築	有		復旧方針を確認する	システム全体	実機	・通常はAWS東リージョンで各種サーバ、ネットワークを構成しサービスを提供 ・AWS CloudFormationのテンプレート機能を使用し、大阪リージョンに同一構成のサーバを迅速に一貫してプロビジョニングできるかを検証 ・バックアップデータは、東京リージョンから、大阪リージョンにコピーするデータを使用
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		遠隔地へのデータ保管が実施できているか確認する	システム全体	実機	AWS西リージョンへのバックアップデータが正常に保管されているか確認
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		バックアップデータが外部に保管されていることを確認する	システム全体	実機	・AWS西リージョンにバックアップが定期的に実施されていか確認

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		障害発生時に正常な状態にデータ復旧できるか確認する	システム全体	実機	APサーバ、DBサーバともに、バックアップデータから復旧できるかを検証
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され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。	4	リソース 監視を行 う	有		リソース管理ができているかを確認する	システム全体	実機	・AWSマネージドサービスを利用し、各種監視の確立 ・監視により異常が検知された場合は、インスタンスの自動回復(別ホスト)や自動スケーリングを行うとともに、何らかの形で通知できることを確認
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。	3	四半期に1回	有		定期報告会の実施頻度を確認する	運用体制	机上	定期報告会の内容・実施時期等の保守運用ルールの合意
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		報告内容のレベルを確認する	運用体制	机上	アプリケーション開発事業者より障害報告、運用状況報告、改善提案の各報告書フォーマットを提示し盛岡市と合意
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		問い合わせ対応窓口の設置有無を確認する	運用体制	机上	現行システムの問い合わせ対応窓口を継続して設置できることを確認
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		3	1年未満	有		システム移行期間を確認する	移行計画	机上	アプリケーション開発事業者がシステム移行計画を策定し、盛岡市とレビューの上、1年未満で移行できること確認
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	平行稼働は実施しないため				
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		1	実施	有		Web診断を実施する	システム全体	実機	AWSマネージドサービスを使用し、アプリケーションのセキュリティ問題点を定期的に検査できることを確認