

【倉敷（アイネス）】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	マトリクス（指標）	マトリクス説明	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			選択レベル	検証実施有無 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 [-]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、そこ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		業務データ及びのバックアップを行い、システム内に閉じて取得するデータのみでシステムの復旧を確認する。	本番環境	実機	データベースについてはRDSバックアップからの復元を確認する。ファイルデータについてFsxに格納されているファイルをS3へバックアップしたデータを復元することで、すべてのデータ時点が復旧することを確認する。
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 [-]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）に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		ガバメントクラウド環境でOSのパッチが適用できるか確認する。	本番環境	実機	AWS SystemManager PatchManagerを利用して、OSの例月パッチが適用できて、それが適用されたAMIを保存できることを確認する。
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	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	構築する環境がガバメントクラウドのセキュリティポリシー及び倉敷市様のセキュリティポリシーに適合していることを確認する。	先行事業	机上	ガバメントクラウド上のセキュリティポリシーは、提供されたガイドラインに従ってCDKを適用することで順守できると認識している。 倉敷市様のセキュリティポリシー/ガイドラインを入手し、当該環境にて不整合がないことを確認する。	
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		データの重要度を考慮したうえで、リスク分析範囲が明らかにになっていること。	先行事業	机上	重要度が高い資産の範囲を特定し、リスクを洗い出し、各リスクへの対策を検討する。
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	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を管理セグメントのウィルスパターン配信サーバにて受渡し、各サーバに適用できることを確認する。	AWS内のEC2インスタンス全て	実機	ウィルス定義ファイルを管理セグメントのウィルスパターン配信サーバにて受渡し、AMIに反映し、インスタンスを起動することでウィルス定義ファイルが最新化された環境として起動することを確認する。
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、生体認証等がある。	1	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	AWS環境を操作するアカウントは多要素認証にて認証する。 サーバ内、DB内のアカウントは 現行通りの認証でアクセス可能であることを確認する。	AWS内のEC2インスタンス全て RDS上のSQLServer	実機	AWSの管理コンソールは多要素認証を用いる。現時点では認証アプリによる認証を想定。 EC2インスタンスへのリモート接続、及びRDSで利用するSQLServerでは現行と同じアカウントでログインできることを確認する。	
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。 [-] 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	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になってしまうため、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）	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		ネットワークアクセス経路は必要なルート及び必要最低限のポートのみが解放されていること、及びサーバ認証においては管理者アカウントのみがアクセス可能であることを確認する。	AWS内のEC2インスタンス	実機	ネットワーク設計時点では必要なアクセスルート（本庁舎⇄サーバ/VPC間）及びアクセスポートのみ開放されていることを机上確認する。 環境構築後にAWS CloudWatchを利用して不正なアクセスがないことを確認する。
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		パスワードを送受信する経路が暗号化通信経路であることを確認する。	本庁⇄AWSサーバ間	実機	業務システムは暗号化通信(SSL)を使用する。 環境構築後の各種機能検証で、業務システム以外でパスワードを送信する機能がないことを確認する。
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 [+]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		データベースのバックアップファイルが暗号化されていることを確認する。	RDSバックアップ S3、EBS、CloudWathLogs	実機	パスワードを格納するDBデータベースのバックアップファイルが暗号化されており、プレーンテキストとしてパスワードが読み取れないことを確認する。 S3、EBS、CloudWathLogsの暗号化設定を確認する。
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	本システムにおいては、不正なアクセスが発生した際に備えてOSイベントログおよび業務システムアクセスログを取得している。ガバメントクラウドにリフト後も要件レベルの変更は行わず、現行設定通りにOSイベントログが取得されることを確認する。	本番環境	実機	CloudWatchにて、OSイベントログ及びIISログ、パッチ処理ログが監視できることを確認する VPCフローログをCloudWatchに発行して、CloudWatchでログを参照できることを確認する。 業務システム内DBにて、誰がどの画面、どの個人を操作したのかのログが現行と同レベルで取得できていることを確認する。	

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	マトリクス（指標）	マトリクス説明	選択レベル		備考	選択団体記入欄（検証実施前）			検証事項	検証範囲	検証方法		
						選択時の条件	備考		選択レベル	検証実施有無 実施有無	判断理由（無の場合のみ記入）			種別	方法	
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		AWSユーザーの操作の監視、及び不正な構成変更をチェックし、警告する。	本番環境	実機	CloudTrailを使用して不正な操作アクションを監視し、アラームメールを発出できることを確認する。 不正な構成変更を検出し、アラームメールを発出できることを確認する。
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		WebシステムのコーディングについてはCookieやURLパラメータ等に宛名番号等の重要情報が格納されない設計になっており、ガバメントクラウドにリフト後も特に変更はない。Webサーバについてはシステムの正常URL以外にアクセスされた場合に表示される内容で、サーバの種類等が類推されない表示になることを確認する。	業務システム全て	実機	ブラウザの管理メニューより、Cookieに重要情報が格納されていないことを確認する。画面操作中に表示されるURLに適当なパラメータを付与してアクセスしなおした際に、システム動作に影響がないことを確認する。
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	WAFの導入は必須要件ではないため				
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膨大に発生する等業務への支障が大いことが明らかである場合	2	1営業日前の時点（日次バックアップからの復旧）	有		データベース、アプリケーション、ファイルレベルで1営業日前の状態に復元できることを確認する。	本番環境	実機	RDSバックアップ、AMIイメージのスナップショット、Fsxのスナップショットから復旧ができることを確認する。
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	2	12時間以内	有		要件「A1.3.1」の復旧テストにおいて処理時間を計測し、要求レベル時間以内に復旧できることを確認する。	本番環境	実機	要件「A1.3.1」の復旧テストにおいて処理時間を計測し、12時間以内に復旧し、顧客に公開できることを確認する。
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	2	全システム機能の復旧	有		要件「A1.3.1」の復旧テストにおいて全システムの復旧ができることを確認する。	本番環境	実機	要件「A1.3.1」の復旧テストにおいて復旧した際に、すべての機能が使用できることを確認する。
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、情報システムに基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	2	一ヶ月以内に再開	有		要件「A1.3.1」で使用する機能にて、通常稼働時とは別リージョンにシステムを復旧し、使用できることを検証する。 1か月以内に復旧できることを確認する。	本番環境/バックアップ環境	実機	要件「A1.3.1」で使用する機能にて、通常は東京リージョンで稼働しているので大阪リージョンにシステムを復旧できることを確認する。 1か月以内に復旧できることを確認する。
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。	3	99.5%	有		AWSの稼働率を含めて、業務システムとしての稼働率が選択レベルを達成できることを確認する。	本番環境	机上	要件「A1.3.1」で検証した復旧時間実績を基に、マルチAZ構成とした場合で目標の稼働率を達成できることを確認する。
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		現行同様のクライアント数からシステム接続して、画面遷移等で異常終了しないことを検証する。	本番環境	実機	負荷テストをツールにて、現行システムを利用しているクライアント台数分のアクセスを行い、正常応答を確認する。
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		現行の繁忙期と同数レベルの同時接続に対して、単独アクセスの倍程度の応答時間であることを確認する。	本番環境	実機	負荷テストをツールにて、同時アクセス数を徐々に上げていき、現行の繁忙期と同レベルの同時アクセス数まで動作させる。
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	0	すべてのデータ件数、データ量が明確である	有		移行対象のDB一覧、フォルダー一覧が作成され、それぞれ移行対象サイズが記載されていることを確認する。	本番環境	実機	初回のデータ移行時点で、移行対象DB一覧とその容量、移行対象フォルダー一覧とその容量を記録する。
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	0	処理ごとにリクエスト件数が明確である	有		現行システムのログより、平均アクセス数、時間当たりの最大アクセス数を確認する。	本番環境	実機	現行オンプレサーバのIISログ、システムのアクセスログより、時間当たり(分単位)のオンラインアクセス数の平均値、及び最大値を測定する。

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	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	
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 [+]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		現行システムの処理の中で最長の処理時間を持つバッチジョブとその処理件数を把握する。	本番環境	実機	現行オンプレサーバのバッチジョブログより、直近1年間で最長時間のジョブを把握し、その処理件数を把握する。
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	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ある。 【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		現行システムとガバメントクラウドに移行後のシステムで比較して、オンラインレスポンスタイムが著しく劣化しないこと、及び3秒以内という基準を満たすことを確認する。	本番環境	実機	顧客環境から接続可能になった後で、顧客環境からシステムにアクセスして、レスポンスタイムを計測すること、及び現行システムと比較して操作性として著しく遅延していないことを確認する。
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	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ある。 【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		負荷テストにて、実際のピーク時アクセス数に達した時のレスポンスタイムが5秒以内であることを確認する。	本番環境	実機	負荷テストをツールにて行う中で、実際のピーク時のレスポンスタイムを確認する。 ピーク時アクセス数は、現行システムのアクセスログから、過去1年以内のピークを抽出する。
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	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		夜間バッチ処理が現行と比べて著しく遅延しないことを確認する。 再実行の余裕が確保できる時間であることを確認する。	本番環境	実機	各業務の月次処理、年次処理等負荷の高いバッチ処理を現行システムとガバメントクラウドに移行後の環境で処理時間比較を行い、著しく劣化しないことを確認する。 再実行の余裕が確保できる時間であることを確認する。
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	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		夜間バッチ処理が現行と比べて著しく遅延しないことを確認する。 再実行の余裕が確保できる時間であることを確認する。	本番環境	実機	各業務の月次処理、年次処理等負荷の高いバッチ処理を現行システムとガバメントクラウドに移行後の環境で処理時間比較を行い、著しく劣化しないことを確認する。 再実行の余裕が確保できる時間であることを確認する。
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） [-]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		現行運用と同じ時間設定でのサイクル運用テストを行い、不具合が発生しないことを確認する。	本番環境	実機	現行運用と同じ時間設定でのサイクル運用テストを行う。
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		現行運用と同じ時間設定でのサイクル運用テストを行い、不具合が発生しないことを確認する。	本番環境	実機	現行運用と同じ時間設定でのサイクル運用テストを行う。
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		現行運用と同じ時間設定でのサイクル運用テストを行い、不具合が発生しないことを確認する。	本番環境	実機	現行運用と同じ時間設定でのサイクル運用テストを行う。
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 [+]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		情報システムの通常運用マニュアルは変更ない見込み。保守マニュアルについてはガバメントクラウドのサーバ管理等のマニュアルを更新する。	本番・検証環境	机上	保守マニュアルに、ガバメントクラウド上での運用設定、及び障害復旧に関する事項を追記する。
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 [-]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		庁内の連携基盤との接続を確認する。	本番・検証環境	実機	外部システム（情報提供ネットワーク含む）とは庁内設置の共通基盤システムを介しての連携を行っている。全ての連携について共通基盤システムとの接続を確認する。

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	マトリクス（指標）	マトリクス説明	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			検証実施有無	実施有無	判断理由（無の場合のみ記入）			種別	方法
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		SEが実施する業務システムの更新リリースを確認する。	本番・検証環境	実機	ガバメントクラウド移行後も本要件に変更はない。ミドルウェアの更新が必要な場合に手動で実施することとしている。業務システムのアップデートについては、ガバメントクラウド上での方式としてAMIを更新してからインスタンスを再起動する方式で適用を確認する。
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）	業務が比較的に少ない時間帯にシステム停止が可能。 [-]停止を増やす場合	4	利用の少ない時間帯（夜間など）	有		移行作業時間を測定し、業務利用がない時間内で実施できることを確認する。	本番環境	実機	環境構築、及びデータ移行試験時に、システムの運用時間外の範囲で移行できることを確認する。
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	3	移行対象設備・機器のシステム全部を入れ替える	有		現行システムの機器について、移行先に対応する機器又は機能が存在する設計になっていることを確認する。	本番・検証環境	机上	機器の新旧対応表を作成して、移設漏れがないことを確認する。
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	2	10TB未満	有		現行データが全て移行できることを確認する。	本番・検証環境	実機	移行試験の中でデータ量を確認し、最終移行にて適切な移行手段を検討する。
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	1	ユーザとベンダーと共同で実施	有		本番運用切り替えに向けた移行計画書を作成する。検証期間中に本番移行リハーサルを実施し、移行計画自体の検証を行う。	本番・検証環境	実機	本番運用切り替えに向けた移行計画書を作成する。検証期間中に本番移行リハーサルを実施し、移行計画自体の検証を行う。
38	F.1.1.1	システム環境・エコロジ	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がない場合	1	制約有り（重要な制約のみ適用）	有	要件「E.2.1.1」を実施すること で、検証項目を実施したと見なせる。	・順守すべき制約が明らかになっていること。 ・順守すべき制約に沿った、システム設計・構築を行っていること。	先行事業	机上	移行計画や構築作業が、遵守すべき規則等に沿ったものとなっているか確認する。
39	F.1.2.1	システム環境・エコロジ	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		・順守すべき制約が明らかになっていること。 ・順守すべき制約に沿った、システム運用を行っていること。	先行事業	机上	運用方法が、遵守すべき規則等に沿ったものとなっているか確認する。
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定める。	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	2	同一の構成で情報システムを再構築	有		災害対策として大阪リージョンに環境を復旧できることを確認する。	本番環境/バックアップ環境	実機	要件「A.1.3.1」で実施するテストにて確認できる見込み。 クロスリージョンバックアップを利用して大阪リージョンに退避したファイルからシステムを復旧する。

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		
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	【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		大阪リージョンにバックアップする	本番環境/バックアップ環境	実機	クロスリージョンバックアップを利用して大阪リージョンに退避する。
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		要件「A.3.2.1」を実施することで、検証項目を実施したと見なせる。	本番環境/バックアップ環境	実機	要件「A.3.2.1」を実施することで、検証項目を実施したと見なせる。
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ある場合 [+]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		要件「A.1.3.1」を実施することで、検証項目を実施したと見なせる。	本番環境	実機	要件「A.1.3.1」を実施することで、検証項目を実施したと見なせる。
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まない。「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		監視設定を行い、監視対象のリソース異常時に通報が実施できることを確認する。	本番環境	実機	CloudWatchにて監視設定を行い、異常時にメール通報できること、システム管理者(倉敷市様、アイネス双方)が受信できることを確認する。
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可否。	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		月次で保守定例会議を開催すること	本番運用時	机上	保守定例会議は現行月次開催である。ガバメントクラウドヘリフト後も保守定例会議を開催する。
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		定例保守会議にて、障害報告、運用状況報告が報告事項として存在すること、障害報告時には改善提案が記載されていることを確認する。	本番運用時	実機	定例保守会議にて、障害報告、運用状況報告が報告事項として存在すること、障害報告時には改善提案が記載されていることを確認する。
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ある。	1	ベンダーの既設コールセンターを利用する	無	現行と変わらないため。				
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 [+]さらに長期間が必要な場合		4	2年未満	有		予定の期日に稼働できることを確認する。		机上	要件「D.5.1.1」で実施する移行リハーサルにて、移行期間の達成度を確認する。
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、方法を規定すること。	0	無し	無	要件「D.5.1.1」で実施する移行リハーサル後の動作確認にて移行後の運用確認が可能であり、ガバメントクラウドへ業務システムをリフトするうえでの並行稼働期間は設けない。				
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		AWSConfig,SecurityHubを利用して診断を実施する。	本番環境	実機	AWSConfig、SecurityHubを利用してセキュリティ診断を実施する。診断結果で、設定手順等を変更する必要がある場合は構築手順書にフィードバックする。