

【佐倉（両備）】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	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		
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		・全データを復旧するためのバックアップ方式が確立されており、方式に沿ったデータ復旧が可能であること。（AWS Backup使用） ・データ復旧時の参照元が構築したシステム内のデータであること。	・ EC2 ・ RDS for Oracle	実機	EC2： バックアップ⇒ファイル作成（txtでもなんでも可）⇒リストアの順に作業し、作成したファイルが削除されていることで、リストアされていることを確認する。 RDS： バックアップ⇒データ追加⇒リストアの順に作業し、追加したデータが削除されていることでリストアされていることを確認する。
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。	3	緊急性の高いパッチのみ即時に適用を行う	有		OSパッチが適用可能である。 今回、閉域網ネットワークとなるため、外部からの脅威は少ないため	・ EC2	実機	正常にOSパッチ適用が実施できるか検証を実施する。
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	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、ガイドライン等がない場合	【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		佐倉市様のセキュリティポリシーに準拠していること	・ EC2 ・ セキュリティグループ ・ ACL ・ RDS	机上	佐倉市様のセキュリティポリシーと照らし合わせ、内容を確認する
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の必要がある。 [-]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		佐倉市様のセキュリティポリシーに照らし合わせ、情報資産の重要度を考慮した上で、リスク分析を行う範囲が明確になっていること	・ 情報資産	机上	佐倉市様のセキュリティポリシーと照らし合わせ、内容を確認する
5	E.4.3.4	セキュリティ	セキュリティリスク管理	ウイ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イ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	ウイ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。 [-]ウイ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		ウイルス定義ファイルがガバメントクラウド上のサーバに配信されること	・ EC2	実機	ウイルス対策ソフトから定義ファイルを更新し、バージョンが変わっ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		現行運用通り、管理権限を持つ主体の認証はID/パスワード方式でアクセスできることを確認する。	・ EC2	実機	パッケージ：ログイン画面にてパスワードを入力することでログインができることを確認。 サーバ接続認証：Windowsログイン画面にてパスワードを入力しログインできることを確認
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。 （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） [-]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		AWS Configによる変更管理・通知とセキュリティグループ、ACLによるポート制限による制限が正しく設定されているか。	・ EC2 ・ セキュリティグループ ・ ACL ・ RDS	実機	マネジメントコンソールによる設定確認。
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		認証情報が暗号化されていること。	・ 内部ネットワーク	実機	佐倉市様－ガバメントクラウド間は専用線接続による閉域網である。 今回、アプリケーションサーバーまでを暗号化通信（SSL）を行う設計し、動作検証を実施する。
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 ）。	1	認証情報のみ暗号化	有		健康管理システムのログイン時に使用するパスワードが暗号化されていること	・ RDS for Oracle	実機	ログイン時に使用するパスワードがデータベースのテーブルで暗号化されて格納されていることを確認。 その状態で、システムに正常にログインできることを確認する。
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		不正操作監視：CloudTrail 不正構成変更監視：Config 脅威検知：GuardDuty で取得されたログが確認できること	・ EC2 ・ RDS for Oracle	実機	マネジメントコンソールによる左記サービスのログを確認する。

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			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		GuardDutyで取得されたログが確認できること	・GuardDuty	実機	脅威リストに登録したIPアドレスからアクセスを行い、結果を確認する。
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		WAFの導入により、SQLインジェクション、XSSが制限されていること	・WAF	実機	WAF設定後。SQLインジェクション・XSSのテストを実施する。
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	1	有り	有	今回の環境において、インターネット接続を行うWebアプリケーションはございませんので、現行の選択レベル0で進めさせていただきます。	WAFの導入により、SQLインジェクション、XSSが制限されていること	・WAF	実機	WAF設定後。SQLインジェクション・XSSのテストを実施する。 ※（要件E.10.1.1と同様。）
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が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	AWS Backupによるバックアップとそのバックアップデータからのリストアを実施し、1営業日前のデータに復旧できていること	・健康管理システム	実機	EC2： バックアップ⇒ファイル作成（txtでもなんでも可）⇒リストアの順に作業し、作成したファイルが削除されていることで、リストアされていることを確認する。 RDS： バックアップ⇒データ追加⇒リストアの順に作業し、追加したデータが削除されていることでリストアされていることを確認する。
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がことが明らかである場合	2	12時間以内	有	AWS Backupによるバックアップとそのバックアップデータからのリストアを実施し、リストアにかかる時間が12時間以内であること	・健康管理システム	実機	1営業日前のバックアップデータからリストアを行い、リストアにかかる時間を計測する。
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	AWS Backupによるバックアップとそのバックアップデータからのリストアを実施し、1営業日前のデータに復旧できていること	・健康管理システム	実機	EC2： バックアップ⇒ファイル作成（txtでもなんでも可）⇒リストアの順に作業し、作成したファイルが削除されていることで、リストアされていることを確認する。 RDS： バックアップ⇒データ追加⇒リストアの順に作業し、追加したデータが削除されていることでリストアされていることを確認する。
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	2	一ヶ月以内に再開	有	大規模災害（疑似障害）が発生した際の、システム復旧が一ヶ月以内であること。	・健康管理システム	実機	検証方法としては、設計に従い、西日本リージョンに格納したデータを用いた復旧試験をBCP環境を用いて実施する。
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が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	99.50%	有	AWS上のサービス稼働率が99.5%を満たすこと	・EC2 ・RDS for Oracle	机上	利用するクラウドサービスにSLAが定められている場合、SLAが99.5%以上であること。
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		健康管理システムのログイン可能ユーザー数を調査する。現行環境と大きなレスポンス低下が起こっていないことを確認する。	・EC2 ・RDS for Oracle	実機	佐倉市様に一定期間で検証いただき、レスポンスの確認を行う。（特定時間に多数の職員様による操作を依頼。）
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		健康管理システムのログイン可能ユーザー数を調査する。現行環境と大きなレスポンス低下が起こっていないことを確認する。	・EC2 ・RDS for Oracle	実機	佐倉市様に一定期間で検証いただき、レスポンスの確認を行う。（特定時間に多数の職員様による操作を依頼。）
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		各事業のデータ数を集計し、データ量を把握する。	・健康管理システム	実機	現行システムにて、主要データ（各事業のデータ）量を把握する。
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		健康管理システムのアクセスログを集計し、リクエスト数（操作数）を把握する。	・健康管理システム	実機	健康管理システムのアクセスログを集計し、リクエスト数（操作数）を把握する。

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	
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		住基等、基幹システムより受領するデータの処理件数、大量処理（帳票出力）の処理件数を把握する。	・健康管理システム	実機	住基等、基幹システムより受領するデータの処理件数、大量処理（帳票出力）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	3秒以内 [+]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		通常業務量を想定した際の、レスポンス準拠が求められている業務機能において、3秒以内でのレスポンスが実現できていること。	・健康管理システム	実機	健康管理システムで以下の機能におけるレスポンスを測定する。 ①更新機能 ・個別入力画面レスポンスタイム：3秒以内 ②照会機能 ・総合照会画面レスポンスタイム：3秒以内
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 [+]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		アクセス集中時の業務量を想定した際の、レスポンス準拠が求められている業務機能において、5秒以内でのレスポンスが実現できていること。	・健康管理システム	実機	健康管理システムで以下の機能におけるレスポンスを測定する。 ①更新機能 ・個別入力画面レスポンスタイム：5秒以内 ②照会機能 ・総合照会画面レスポンスタイム：5秒以内 ※アクセス集中時のケースは同時照会件数を30以上にすることで再現する。
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	再実行の余裕が確保できる [+]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		通常業務量を想定した際の、レスポンス準拠が求められている業務機能において、再実行の余裕をもってバッチ処理が完了すること。	・健康管理システム	実機	B1.1.5において把握した処理に対し、処理時間を定め、その時間以内で処理が終了することで、再実行可能と判断する。
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	再実行の余裕が確保できる [+]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		アクセス集中時の業務量を想定した際の、レスポンス準拠が求められている業務機能において、再実行の余裕をもってバッチ処理が完了すること。	・健康管理システム	実機	アクセス集中時のケースは同時照会件数を30以上にすることで再現し、その状況でB.2.2.1で定めた処理が、再実行可能な時間で終了することを確認する。
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。	1	定時内での利用（1日8時間程度利用）	有		規定時間内にシステムが利用できること。	・健康管理システム	実機	リフト後にシステム運用テストを実施し、平日の流れを模擬した試験を実施する。
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		規定時間内にシステムが利用できること。	・健康管理システム	実機	リフト後にシステム運用テストを実施し、休日の流れを模擬した試験を実施する。
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できていること。また、バックアップの取得が日次で実行できていること。 もしくは毎日全件バックアップが取得できていること	・AWS Backup	実機	想定時間内に完了するかどうか含めて確認を実施する。
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 [+]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		システム標準のマニュアル+佐倉市様作成のマニュアルに沿って問題無く操作できること	・健康管理システム	実機	システム標準のマニュアル+佐倉市様作成のマニュアルに沿って操作を実施。
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		佐倉市様連携サーバを経由した連携を実施し、問題無くデータ更新がされること	・健康管理システム	実機	連携試験を実施。

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	
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 [-]アップデート権を必要としない場合		2	アップデート	有		ミドルウェア（Office）のバージョンアップが必要と認められた場合、正常に対応できるかを確認する。	・EC2	実機	Officeのパッチを適用する。
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） [-]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		連携を含め、システムの移行・検証に3日間はかかることが想定されるため、土日祝日も視野に入れ、業務が比較的少ない時間帯で移行計画に沿った、スケジュールで移行できること	・EC2 ・RDS for Oracle ・健康管理システム	実機	移行リハーサルを実施し、移行時間の測定を行う
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		移行後、システムが問題無く動作すること	・EC2 ・RDS for Oracle ・健康管理システム	実機	移行リハーサルを実施し、移行手順の確認・動作検証を行う
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。	1	1TB未満	有		移行データ量が適切であること	・健康管理システム	実機	システム稼働に必要なデータ（アプリケーション実行環境、OracleDumpデータ等）に限り移行され、システムが正常に動作することを検証する
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 [+]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		移行計画によって、役割分担が明確になっていること	・移行計画書	机上	移行計画書にユーザが担当する工程、ベンダーが担当する工程が明示されていること
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） [-]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	【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ある。 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		弊社内の構築作業室におけるセキュリティが担保されていること	弊社内の構築作業室	机上	弊社内の構築作業室における、セキュリティに関する資料を提示し、問題無いことを確認する。
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		弊社内の構築作業室におけるセキュリティが担保されていること ※構築作業室とリモート運用を行う部屋が同じであるため、「F.1.1.1」と同じ内容で検証を実施する。	弊社内の構築作業室	机上	弊社内の構築作業室における、セキュリティに関する資料を提示し、問題無いことを確認する。
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 [+]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		用意した復旧手段により、障害発生前と同様のシステムを再構築できること。	・AWS Backup ・CloudFormation	実機	西日本リージョンにバックアップされたデータから、東日本リージョンにシステムの再構築が可能であること。 CloudFormationを使用し、インフラを再構築できることを確認。
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ヶ所 [+]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		西日本リージョンにEC2、RDSの情報がバックアップされていること	・AWS Backup	実機	AWSBackupにより、西日本リージョンにバックアップファイルが作成され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	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	
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」と同様。	要件「A.3.2.1」と同様	実機	要件「A.3.2.1」と同様。
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		AWS Backupによるバックアップとそのバックアップデータからのリストアを実施し、1営業日前のデータに復旧できていること（要件「A.1.3.1」と同様。）	・健康管理システム	実機	EC2： バックアップ⇒ファイル作成（txtでもなんでも可）⇒リストアの順に作業し、作成したファイルが削除されていることで、リストアされていることを確認する。 RDS： バックアップ⇒データ追加⇒リストアの順に作業し、追加したデータが削除されていることでリストアされていることを確認する。
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		・リソースの使用状況を把握できること。 ・閾値（CPU使用率、メモリ使用量、ディスク容量など）を設定し、それを超えた場合に、あらかじめ定められた連絡先にアラート通知が出来ること。	・CloudWatch（EC2・RDS・ELB）	実機	CloudWatchによるリソース監視が設定されて、マネジメントコンソールから状況が確認できること。 ELBによるWebサービスの死活監視が正常に動作しているかも監視対象とする。
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。	3	四半期に1回	有		現状の保守契約に含まれていないが、別途対応方法を検討し、定例会が開催されることを確認する。	運用体制	机上	現状の契約から変更されて、定例会の開催が契約に含まれることを確認する。
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		「C.5.9.1」で開催する定例会での報告内容について、障害の状況及び改善提案が報告内容に含まれることを確認する。	運用体制	机上	現状の契約が変更され、障害発生時の報告内容に改善提案までが含まれることを確認する。
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	有		コールセンターが設置されているか、問い合わせ先が公開されているか。		机上	コールセンターのリーフレットを公開、展開する。
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		移行計画に記載されているスケジュールで実施できること	・移行計画書	実機	移行計画に記載されているスケジュールで実施できること
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	無し	無		移行のためのシステム停止時間は3日あれば可能と考えており、既存環境とガバメントクラウドの並行稼働はしない。			
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		0	不要	無		外部から「内部ネットワーク経由での攻撃」については、個人情報系ネットワークでは考えにくく、「内部犯を想定する必要がない場合」に相当すると考えられるため、選択レベルを下げ、0で進めさせていただきます。			