【笠置（KIP）】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		業務データおよびアプリケーションのバックアップがとれることおよびリストア可能であることを検証する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	実機	AWS Backupよるバックアップ管理 システム領域　AMI＋SnapShot データ領域　SnapShot 既存バックアップツールでのバックアップ/リストア実施可否確認 上記での実現が困難な場合、 既存の現行システムバックアップツールを使用
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		ガバメントクラウドリフト後に、現行運用通り、正常にOSパッチ適用が実施できるか検証を実施する。	ガバメントクラウド上に構築した環境（1つ以上）	実機	AWS EC2 System Managerを使ってWSUS運用管理検証 ※OS等の適用手法を確立する
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		笠置町のセキュリティポリシーを順守出来ているか検証する。	全体	机上	・笠置町セキュリティポリシーから影響範囲を確認する ・AWS側のポリシーを確認し、上記との整合を確認する https://aws.amazon.com/jp/compliance/programs/?fbclid=IwAR1JRd7pxhq98SIuRFu8BcGrtvWIuohjRLs9C1MJhhLyzGkp_4IpeuK3Nd4
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（個人情報を含む基幹業務データ）としてリスク分析する対象が明確になっているか検証する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	机上	AWS Security Hubをベースに机上検証を検討する
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		ガバメントクラウド上のサーバにウィルス定義ファイルが配信されることを検証する。	ガバメントクラウド上に構築した環境（1つ以上）	実機	既存の庁内ウィルス定義配信サーバからガバメントクラウド上のサーバにウィルス定義ファイルが配信されることを検証する。 ※最新バージョンのシグネチャが取得でき、配信されること
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		個人番号利用事務系ネットワークでは二要素認証が必須となっているため、二要素認証が正常に運用できるか確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	実機	端末に接続する装置による生体認証およびアプリケーションへID・パスワード認証ログインの二要素認証で検証する もしくは AWS Cognitoを使った、2FA及び外部認証
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		ガバメントクラウドにリフトするサーバへはサーバ管理者アカウント以外でサーバにログオンできないことを確認する。 さらに、アプリケーションの操作権限設定が正常に反映することを確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	実機	サーバ管理者アカウント以外でサーバにログオンできないことを確認する。 ■Windowsのログ ■不要ソフト監視：AWS Config で変更管理・通知。 ■ポート制御：AWS セキュリティグループ、ACL で制御。 アプリケーションの操作権限設定通りに「A業務データはアクセスできるが、B業務データへはアクセスできないこと」など、制御できていることを確認する。
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		認証情報の暗号化・伝送・複合化が正常に行えることを確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	実機	アプリケーションの認証情報（パスワード）の暗号化・伝送・複合化が正常に動作し、認証が正しく行われるかをログで確認する。 以下を利用する ・クライアント端末側のスイッチポートでパケットキャプチャ
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蓄積されているか確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	実機	アプリケーションの認証情報（パスワード）が暗号化された状態で格納されているか確認する。 AWS IAMでの暗号化、キーを作成してアクセステストをしてアクセスできるか確認

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	
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		OSイベントログおよび基幹業務システムアクセスログが取得できることを確認する。	ガバメントクラウド上に構築した環境（1つ以上） NewTRY-X/Ⅱ（基幹業務パッケージ）	実機	OSイベントログおよび基幹業務システムアクセスログから、「いつ」「誰が」「どこから」「何を実行したか」等が確認できることを検証する。 ※先行事業作業者の作業実績が追跡できることを確認する。 （AWSの機能ないしは監視装置の機能で確認） 以下に現状想定機能を記載。 OS 監視、仮想ネットワーク監視：AWS 機能 統合管理:AWS Security Hub 不正操作監視：CloudTrail 不正構成変更監視：AWS Config 脅威検知：GuardDuty
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	無	要件「E.7.1.1」を実施することで、検証項目を実施したと見なせる。 ※各機器、装置ごとにログは取得しており、内部からの攻撃等に対する不正監視装置の設置は考慮しない。				取得するログ設計（Security Hub+Cloudtrail+Cloudwatch）の検討を行う。
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		0	無し	無	[-]Webアプリケーションではないため				
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	内部ネットワークのみ接続する情報システムを想定し、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考慮しない。 （NAT Gateway想定であるため、外部から攻撃される状況にはならない）				
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		『ガバメントクラウドで提供されるPaaS機能ないしはECインスタンスのSnapShot等を利用したバックアップ/リストアを想定。 またバックアップの取得は下記の２種類を想定。 ①データベース/アプリケーション/ファイルレベル ②OSイメージレベル 両方の方式で最新バックアップを取得した時間点への（日次バックアップであれば１営業日前へ）復元が可能であるか確認する。』	①NewTRY-X/Ⅱ（基幹業務パッケージ） ②ガバメントクラウド上に構築した環境（1つ以上）	実機	データベース/アプリケーション/ファイルの前日バックアップを利用したリストアを実施し、データ件数の一致確認（バックアップ＝復旧後環境）、および前日時点からの運用再開が可能な状態となっているか、システム操作・システム連携等の確認を行う。 バックアップには 全体確認だとAWS Backup システム領域　AMI＋SnapShot データ領域　SnapShot 等を検討。
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。	3	6時間以内	有		①データベース/アプリケーション/ファイルレベル	①NewTRY-X/Ⅱ（基幹業務パッケージ） ②ガバメントクラウド上に構築した環境（1つ以上）	実機	以下の対応が時間内に可能かを総合的に検証する。 ・バックアップからのリストアおよび復旧後システム動作確認時間（実機） ・リストア不可の場合の縮退環境への切替および縮退システム動作確認時間（実機）
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		②OSイメージレベル	①NewTRY-X/Ⅱ（基幹業務パッケージ） ②ガバメントクラウド上に構築した環境（1つ以上）	実機	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。
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		両方の方式で最新バックアップを取得した時間点への（日次バックアップであれば１営業日前へ）復元が可能であるか確認する。	①NewTRY-X/Ⅱ（基幹業務パッケージ） ②ガバメントクラウド上に構築した環境（1つ以上）	実機	AWS Backupを用いた形でのマルチAZ構成でAZ故障時の復旧確認検証を実施する。大規模障害時の復旧フローについて確認。 ※大阪リージョンについては、バックアップのみを想定しているため範囲外 ーーー マルチAZ構成の弊社の懸念事項 ・Zone自体の障害などSPOF（単一障害点）の状態に陥る恐れがあり復旧時間の確約が困難になります。 ・アプリケーション設定でIPアドレス固定値しか入力できない懸念があります。 ・ファイル連携時の遅延の影響があります。
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		AWSの利用サービスでSLAが定義されているものについて、SLAを満たすか確認する。	AWS上のサービス	机上	既存の非機能要件を基に記載している。AWSの利用サービスでSLAが定義されているものについては、算出可能だとは考える。責任範囲を抽象化した状態でSLAを算出し、机上検証する。 例） 　Direct Connect、Direct Connect Gateway、TransitGWのみを設定するAWSアカウントの中でのSLAは、単純にその機能のSLAの掛け算となる。

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
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		利用ユーザ数以上のライセンスがあることを確認する。 ※ライセンスの数で利用ユーザ数の上限が決まっていることを確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	机上	現行システムのユーザ登録やアクセスログから「利用ユーザ数」を確認。 現行システムの利用ユーザ数以上のOracleライセンス等があることを確認する。 補足 利用ユーザ（職員数）は現行と変わらない前提。
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		同時利用ユーザの上限以上のライセンスがあることを確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	机上	現行システムのユーザ登録やアクセスログから「同時利用ユーザ数の上限」を確認。 現行システムの同時利用ユーザ数以上のOracleライセンスがあることを確認する。 補足 利用者数も少なく、AWS EC2インスタンスの最小サイズでも動作すること想定している。
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		現行システムデータとガバメントクラウドシステムデータが同一であること（データに欠落がないこと）を検証する。	①NewTRY-X/Ⅱ（基幹業務パッケージ） ②G-Trust（障がい者福祉システム）	実機	各業務システムのデータ件数、データ量を比較し検証する。 ・各テーブルデータ件数の確認および現行との一致確認 ・エクスポートデータサイズが現行との一致確認
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する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	実機	アプリケーション開発事業者が現行システムのアクセスログからオンラインリスエスト件数を確認する。
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。	1	主な処理の処理件数が決まっている	有		現行システムとガバメントクラウドシステムで同等の処理時間、同一の処理件数、処理結果となることを確認する。	①NewTRY-X/Ⅱ（基幹業務パッケージ） ②G-Trust（障がい者福祉システム）	実機	現行システムのテスト環境（ある時点の凍結データ）とガバメントクラウドシステムのデータを同一のものとし、同じバッチ処理を実行。 処理時間と処理結果を比較検証する。
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	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		現行システムとガバメントクラウドシステムで同等のレスポンス時間となることを確認する。 ※現行システムSLAでは「5秒以内」だが、デジタル庁様の示す「3秒以内」を目標として検証する。	①NewTRY-X/Ⅱ（基幹業務パッケージ） ②G-Trust（障がい者福祉システム）	実機	現行システムのテスト環境（ある時点の凍結データ）とガバメントクラウドシステムのデータを同一のものとし、同じ操作を実行。 レスポンスタイムを比較検証する。
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	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		ネットワーク経路上に一定のトラフィックを流している状態でシステム利用に影響が出ないかを検証する。	NewTRY-X/Ⅱ（基幹業務パッケージ）		ネットワーク経路上に一定のトラフィックを流している状態でシステム利用に影響が出ないかを検証
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		現行システムとガバメントクラウドシステムで同等の処理時間、同一の処理件数、処理結果となることを確認する。 ※エラーが発生した場合、再実行の余裕があることを確認する。	①NewTRY-X/Ⅱ（基幹業務パッケージ） ②G-Trust（障がい者福祉システム）	実機	現行システムのテスト環境（ある時点の凍結データ）とガバメントクラウドシステムのデータを同一のものとし、同じバッチ処理を実行。 処理時間と処理結果を比較検証する。 ※エラーが発生した場合、再実行可能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	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		観点が、バッチ処理の処理能力に関する項目であると考えられます。実際に、人口が少なく、高負荷となることがなく、バッチ処理のレスポンスについても影響が出ないことが想定されるため、バッチ処理の正常動作の検証とします。 ※エラーが発生した場合、再実行の余裕があることを確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	実機	バッチ処理は、通常3処理同時までで基幹系システム制約をかけているが、検証のため5つ同時処理などでサーバへの負荷をかける検証を実施する ※エラーが発生した場合、再実行可能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）	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	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、問題が発生しないことを確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	実機	現行運用と同じ時間設定で、サーバタスク予約、アプリのバッチ処理予約等を設定し、利用時間に問題が発生し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
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		2	定時外も頻繁に利用	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、問題が発生しないことを確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	実機	現行運用と同じ時間設定で、サーバタスク予約、アプリのバッチ処理予約等を設定し、利用時間に問題が発生しないことを確認する。
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		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、問題が発生しないことを確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	実機	現行運用と同じ時間設定で、バックアップ取得ツールを予約し、正常にバックアップが取得できることを確認する。また、週次バックアップも行う。（AWS Backupの設定を想定）
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		保守運用マニュアルをガバメントクラウド運用に合わせる形に更新する。 ※通常運用マニュアルに変更はない見込み。	NewTRY-X/Ⅱ（基幹業務パッケージ）	机上	保守運用マニュアルについて、ガバメントクラウドのIaaSサーバ管理、及びPaaS機能利用分、縮退環境の変更点等を更新する。
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	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		庁内の外部システム等と連携（疎通）ができることを確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	実機	庁内の戸籍システムと連携（疎通）確認を行う。 京都府共同利用クラウドのシステムと連携（疎通）確認を行う。
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		システムのアップデート作業が現行とほぼ同じ手順でできることを確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	実機	現行システムのアップデート作業（法改正対応等）は1~2ヶ月に1回の頻度で発生しているため、先行事業期間内に発生するアップデートを1回以上実施する。なお、ベンダー側でアップデート作業を実施する。
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		移行作業で必要な作業内容を洗い出し、夜間ないしは土日祝の開庁時間外で作業完了することを机上検証する（想定するダウンタイムを測定する）。	NewTRY-X/Ⅱ（基幹業務パッケージ）	机上	本番環境の切替作業タイムスケジュール表を作成し、想定されるダウンタイムを机上測定する。
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。	2	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	有		京都府共同利用クラウドからガバメントクラウドクラウドへ現行システムを移行する際に、R2（DBをRDS利用）での構築を検証する。 ※R2での構築が実現困難と判断した場合、R1での構築で実施予定。	NewTRY-X/Ⅱ（基幹業務パッケージ）	実機	京都府共同利用クラウドからガバメントクラウドクラウドへ現行システムを移行する際に、R2（DBをRDS利用）での構築を検証する。 ※R2での構築が実現困難と判断した場合、R1での構築で実施予定。
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。	2	10TB未満	有		移行対象のデータ量を確認の上、欠落することなく全て移行できることを確認する。	①NewTRY-X/Ⅱ（基幹業務パッケージ） ②G-Trust（障がい者福祉システム）	実機	移行対象のデータ容量・件数を確認し、移行後に完全一致することを確認する。
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	【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		ガバメントクラウドへの本番移行計画の内、役割分担案を作成する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	机上	ガバメントクラウドへの本番移行で必要となる作業を洗い出し、各役割分担を整理、役割分担表の案を作成する。

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
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		AWSの基準で笠置町の規定上問題となるものがないか確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	机上	AWSの基準で笠置町の規定上問題となるものがないか確認する
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		AWSの基準で笠置町の規定上問題となるものがないか確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	机上	AWSの基準で笠置町の規定上問題となるものがないか確認する
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		『ガバメントクラウドで提供されるPaaS機能ないしはECインスタンスのSnapShot等を利用したバックアップ/リストアを想定。 またバックアップの取得は下記の２種類を想定。 ①データベース/アプリケーション/ファイルレベル ②OSイメージレベル 両方の方式で最新バックアップを取得した時間点への（日次バックアップであれば１営業日前へ）復元が可能であるか確認する。』	ガバメントクラウド上に構築した環境	実機	システム領域　AMI＋SnapShot データ領域　SnapShot もしくは 既存バックアップツールでのバックアップ実施可否確認。 各バックアップ拠点（大阪、東京リージョン）からのデータを用いて復旧する際のフローについて確認する。 ただし、マルチAZが構成できない場合は、レベル3の「限定された構成をDRサイトで構築」となる。
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		ガバメントクラウドから庁舎へのバックアップデータ転送を検証する。 ※「C.1.2.2」にて検証する。	ガバメントクラウド上に構築した環境	机上	災害時を想定し、AZ レベルの障害ケースと、リージョンレベルの障害ケースでのバックアップ、リストアの際のフローについて机上検証を実施。 ＜利用する機能＞ 大阪リージョンにAMI+SnapShot をコピーする（デジタル庁方針に従う(東西2 センタにバックアップ)）
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		「C.1.2.2」にて検証する。 ※既存の非機能要件を基に「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」記載としております。 DRサイトへのリモートバックアップが確認できれば非機能要件グレードを上げる想定でおりますため、「２：DRサイトへのリモートバックアップ」を目標とした検証を想定しております。	ガバメントクラウド上に構築した環境	机上	災害時を想定し、AZ レベルの障害ケースと、リージョンレベルの障害ケースでのバックアップ、リストアのフローについて机上検証を実施。 ＜利用する機能＞ 大阪リージョンにAMI+SnapShot をコピーする（デジタル庁方針に従う(東西2 センタにバックアップ)）
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		『ガバメントクラウドで提供されるPaaS機能ないしはECインスタンスのSnapShot等を利用したバックアップ/リストアを想定。 またバックアップの取得は下記の２種類を想定。 ①データベース/アプリケーション/ファイルレベル ②OSイメージレベル 両方の方式で最新バックアップを取得した時間点への（日次バックアップであれば１営業日前へ）復元が可能であるか確認する。』	ガバメントクラウド上に構築した環境	机上	データベース/アプリケーション/ファイルの前日バックアップを利用したリストアを実施し、データ件数の一致確認（バックアップ＝復旧後環境）、および前日時点からの運用再開が可能な状態となっているか、システム操作・システム連携等の確認を行う。また、各バックアップ拠点（大阪、東京リージョン）からのデータを用いて復旧する際のフローについて確認する。 バックアップには 全体確認だとAWS Backup システム領域　AMI＋SnapShot データ領域　SnapShot 等を検討。

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
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		現行運用の監視ツールを利用し、リソース監視（CPU、メモリ、Disk、トラフィック等）が可能であることを確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	実機	AWSのコンポーネントないしは監視ツールを利用して実現可否を検討 ※AWS Security Hub等
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		京都府共同利用クラウドからガバメントクラウドへ運用変更されることが、自治体への定期報告会頻度に影響するとはあまり考えていないが、責任分界点（AとBを繋いでいる回線については、誰が報告するのか）が明確となった際にはアプリケーション事業者からの報告すべき内容により、頻度を再検討する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	机上	定期報告会の内容・頻度等の保守運用ルールについて関係者（自治体・協議会・アプリケーションベンダ）で検討する。
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		「C5.9.1」でアプリケーション事業者の責任範囲となった部分については、現行でも「障害及び運用状況報告に加えて、改善提案」を行っているため、同様の運用が継続できることを確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	机上	「障害及び運用状況報告に加えて、改善提案」を定例会報告資料にまとめる。
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有る。	1	ベンダーの既設コールセンターを利用する	有		先行事業に関する問い合わせ窓口も現行の問い合わせ窓口と変更なく運用できることを確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	机上	先行事業に関するお問い合わせを現行のお問い合わせ窓口で対応し、その内容をまとめる。
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 [+]さらに長期期間が必要な場合		4	2年未満	有		移行設計から移行完了までに想定される作業内容を洗い出し、2年未満に収まることを確認する。	NewTRY-X/Ⅱ（基幹業務パッケージ）	机上	移行設計から移行完了までの作業内容を洗い出し、想定されるWBSを作成する。
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	並行稼働は実施しない予定。				
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	・通信の方向を制限しているため（基幹系データのダウンロード不可）内部犯を想定する必要がない。 ・アプリケーションがWebアプリケーションではないため				