別紙１_検証項目の検証方法（a：非機能要件_住記等）

検証方法と役割案

先行事業に協力するアプリ事業者の標準サービスのうち、標準非機能要件よりレベルが高い項目

●主○副△支援

□準備、■机上、■実機

通番	標準非機能要件項番	大項目	メトリクス（指標）	担当			先行事業における検証方法				実施工程						
				団体		ベンダ	団体	ベンダ	検証の指標	備考	構築	検証（テスト）	データリフト	検証（副本）	移行	運用保守
				主管課	情報部門											
1	A.1.3.1	可用性	RPO（目標復旧地点）（業務停止時）			●		■クラウド基盤 システム全体バックアップを行う製品を導入し、バックアップや、システム障害時の復旧手順（アーカイブログ復旧）を確立する。 ■運用保守 システム復旧手順の検証	＜レベル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）	標準：＜レベル２＞ 1営業日前の時点（日次バックアップからの復旧）	□	■実機				
2	A.1.3.2	可用性	RTO（目標復旧時間）（業務停止時）			●		■クラウド基盤 システム全体バックアップを行う製品を導入し、バックアップや、システム障害時の復旧手順（アーカイブログ復旧）を確立する。 ■運用保守 システム復旧手順の検証	＜レベル３＞ 6時間以内	標準：＜レベル２＞ 12時間以内	□	■実機				
3	A.3.2.2	可用性	保管方法（外部保管データ）		○	●	■情報部門 対応計画の検討、合意、 復旧試験実施の際の結果確認（エビデンスベース）	■クラウド基盤 保管場所を取り決め、バックアップ・リカバリ方式設計に明記し対応方針を説明。復旧試験を実施	＜レベル２＞ ＤＲサイトへのリモートバックアップ	標準：＜レベル１＞ 同一システム設置場所の別ストレージへのバックアップ	□	■実機				
4	C.1.1.1	運用・保守性	運用時間（平日）		●	●	■情報部門 運用時間の合意、延長時の申請ルールの確認	■クラウド基盤 クラウド運用変更説明資料（利用部門向け）等を用い、運用時間や申請ルールを説明する	＜レベル２＞ 定時外も頻繁に利用（1日12時間程度利用）	標準：＜レベル１＞ 定時内での利用（1日8時間程度利用）				□		■机上
5	C.1.1.2	運用・保守性	運用時間（休日等）		●	●	■情報部門 休日運用時間の合意、申請ルールの確認	■クラウド基盤 クラウド運用変更説明資料（利用部門向け）等を用い、運用時間や申請ルールを説明する	＜レベル２＞ 定時外も頻繁に利用（1日12時間程度利用）	標準：＜レベル１＞ 定時内での利用（1日8時間程度利用）				□		■机上
6	C.1.3.1	運用・保守性	監視情報			●		■クラウド基盤 ハード・ソフト（業務アプリ未起動や異常終了を含む）に対する監視、および内容や団体に応じた通報先に自動的に通報する機能を構築し、監視運用を確立する	＜レベル５＞ パフォーマンス監視を行う クラウドサービスで運用している監視およびメール等による自動通報機能を移植することを想定	標準：＜レベル４＞ リソース監視を行う	□	■実機				■実機

主管課の主体作業となる項目

●主○副△支援

□準備、■机上、■実機

通番	標準非機能要件項番	大項目	メトリクス（指標）	担当			先行事業における検証方法				実施工程					
				団体		ベンダ	団体	ベンダ	検証の指標	備考	構築	検証（テスト）	データリフト	検証（副本）	移行	運用保守
				主管課	情報部門											
7	A.1.4.1	可用性	システム再開目標（大規模災害時）	●		○	■主管課 システム不通や喪失時など利用できない事象となることを想定した各種手順の検証 ・利用不可の判断 ・代替運用方法へ切替える手順 ・復旧時の対応手順	■団体支援 システム利用不可に備えた代替システムを確保し、切替手順を確立する。またそれらの実機検証の支援。 ■運用保守 復旧後の戻し手順検証	＜レベル3＞ 一週間以内に再開	ダウンリカバリを利用している団体は、Govクラウドへのリフト後も継続し、システムダウンや両回線切断時の縮退業務継続の手順を確認する想定。	□			■実機		
8	B.2.1.4	性能・拡張性	通常時オンラインレスポンスタイム	●		○	■主管課中心 現地端末でのオンライン打鍵による実機検証。 通常時日中レベルの同時打鍵台数を想定。	■団体支援 現地端末での実機検証にあたり主管課に対し、検証内容や手順、実施スケジュール等の提案・調整の実施 ■環境構築 性能テスト実施	＜レベル3＞ ３秒以内	主管課職員を中心に、通常時のアクセス台数で対象者検索を打鍵し検証を行う。（予め通常の同時アクセス台数の把握が必要）	□			■実機		
9	B.2.1.5	性能・拡張性	アクセス集中時のオンラインレスポンスタイム	●		○	■主管課中心 現地端末でのオンライン打鍵による実機検証。 3～4月繁忙期や連休明けを想定した同時打鍵台数を想定。	■団体支援 現地端末での実機検証にあたり主管課に対し、検証内容や手順、実施スケジュール等の提案・調整の実施 ■環境構築 性能テスト実施	＜レベル3＞ ３秒以内	主管課職員を中心に、ピーク時のアクセス台数で対象者検索を打鍵し検証を行う。（予めピーク時の同時アクセス台数の把握が必要）	□			■実機		
10	C.4.3.1	運用・保守性	マニュアル準備レベル	●	○	●	■主管課 ■情報部門（必要に応じ） システム運用（オンラインやバッチ処理、システム共通作業）の検証	■団体支援 マニュアル等の整備状況確認。団体のシステム運用検証にあたって操作指導等の支援 ■環境構築 変更点のマニュアル整備。その他は標準マニュアル。 ■クラウド基盤 運用テストにて当社側運用の検証	＜レベル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	システム機器更新時の動作検証やシステム運用検証と同等の内容を想定				■実機		
11	D.3.1.1	移行性	設備・機器の移行内容	●	●	△	■主管課 ■情報部門 システム移行作業の中で情報部門や主管課が移行や切替を行う作業の検討と合意、実際の移行作業（他システムや主管課端末関係など）	■団体支援 システム移行作業の計画にあたっての現地側作業の整理 ■クラウド基盤 システム移行計画書の作成にあたり現地側切替対象に関連するクラウド基盤側の作業を整理	＜レベル３＞ 移行対象設備・機器のシステム全部を入れ替える				□		■実機	

別紙１_検証項目の検証方法（a：非機能要件_住記等）

情報部門の主体作業となる項目

●主○副△支援

□準備、■机上、■実機

通番	標準非機能要件項番	大項目	メトリクス（指標）	担当			先行事業における検証方法				実施工程						
				団体		ベンダ	団体	ベンダ	検証の指標	備考	構築	検証（テスト）	データリフト	検証（副本）	移行	運用保守
				主管課	情報部門											
12	B.1.1.1	性能・拡張性	ユーザ数		●	△	■情報部門 各業務の利用者数の取りまとめ	■クラウド基盤 各業務の利用者数の取りまとめ支援	<レベル１> 上限が決まっている			■机上				
13	B.1.1.2	性能・拡張性	同時アクセス数		●	○	■情報部門 各業務の同時アクセス数の取りまとめ	■クラウド基盤 アクセス実績把握など取りまとめ支援	<レベル１> 同時アクセスの上限が決まっている			■机上				
14	B.1.1.3	性能・拡張性	データ量（項目・件数）		●	●	■情報部門 各業務のデータ量の合意	■環境構築 データ移行テストを行った結果から結果資料を提示	<レベル０> すべてのデータ件数、データ量が明確である			■机上				
15	B.1.1.4	性能・拡張性	オンラインリクエスト件数		●	○	■情報部門 各業務のトランザクション量の合意	■クラウド基盤 統計ログからリクエスト件数を集計し情報提供	<レベル１> 主な処理のリクエスト件数のみが明確である			■机上				
16	B.1.1.5	性能・拡張性	バッチ処理件数		●	○	■情報部門 主要バッチの件数の合意	■クラウド基盤 主要なバッチ処理についての件数情報の提供	<レベル１> 主な処理の処理件数が決まっている			■机上				
17	E.1.1.1	セキュリティ	順守すべき規程、ルール、法令、ガイドライン等の有無		●	●	■情報部門 Govクラウド利用開始にあたり、各団体のセキュリティポリシー等、影響するルールの確認と対応実施。 ・順守のための対策 ・個人情報保護委員会等の審査 ・必要に応じセキュリティポリシーやPIA等の改定	■団体支援 情報部門の支援（セキュリティポリシー等のルール確認や各種対策実施支援として情報提供を行う ■環境構築 クラウド基盤で定義したセキュリティポリシーを基に資料修正や作成を行い、団体への説明を実施する ■クラウド基盤 Govクラウド検証環境の利用手順を踏まえ、ベンダ側の新たなセキュリティポリシーを定義する	<レベル１> あり			■机上				
18	E.2.1.1	セキュリティ	リスク分析範囲		●	●	■情報部門 リスク事項洗い出しと対応策検討、関係部門やベンダとの共有と合意	■クラウド基盤 Govクラウド検証環境のシステム構成を踏まえリスク事項を洗い出し対応策と併せ提案する	<レベル１> 重要度が高い資産を扱う範囲			■机上				
19	F.1.1.1	システム環境・エコロジー	構築時の制約条件		●	○	■情報部門 Govクラウドや団体の制約条件を確認し、制約条件を取りまとめ、合意	■クラウド基盤 Govクラウドや団体の制約条件を確認し、制約条件の検討を行う	<レベル１> 制約有り（重要な制約のみ適用）			■机上				
20	F.1.2.1	システム環境・エコロジー	運用時の制約条件		●	○	■情報部音 Govクラウドや団体の制約条件を確認し、制約条件を取りまとめ、合意	■クラウド基盤 Govクラウドや団体の制約条件を確認し、制約条件を取りまとめる。またクラウド側の設備（基盤や拠点）について制約条件を取りまとめる	<レベル１> 制約有り（重要な制約のみ適用）			■机上				

ベンダ主体、団体は副担当や支援となる項目

●主○副△支援

□準備、■机上、■実機

通番	標準非機能要件項番	大項目	メトリクス（指標）	担当			先行事業における検証方法				実施工程						
				団体		ベンダ	団体	ベンダ	検証の指標	備考	構築	検証（テスト）	データリフト	検証（副本）	移行	運用保守
				主管課	情報部門											
21	A.3.1.1	可用性	復旧方針		○	●	■情報部門 対応計画の検討、合意、 復旧試験実施の際の結果確認（エビデンスベース）	■クラウド基盤 Govクラウドの仕様を確認のうえ、災害時復旧フロー、手順を整備し対応方針を説明。復旧試験を実施	<レベル２> 同一の構成で情報システムを再構築 制約有り（重要な制約のみ適用）		□	■机上				
22	A.3.2.1	可用性	保管場所分散度（外部保管データ）		○	●	■情報部門 対応計画の検討、合意、 復旧試験実施の際の結果確認（エビデンスベース）	■クラウド基盤 保管場所を取り決め、バックアップ・リカバリ方式設計に明記し対応方針を説明。復旧試験を実施	<レベル２> 1ヶ所（遠隔地）	【2022/4/28変更】 変更理由：記載誤り（レベル） 変更前：レベル1（遠隔地）	□	■実機				
23	C.1.2.3	運用・保守性	データ復旧の対応範囲		○	●	■情報部門 対応計画の検討、合意、 復旧試験実施の際の結果確認（エビデンスベース）	■クラウド基盤 データ・ファイルを分類し、復旧方針を取りまとめ対応方針を説明。復旧試験を実施	<レベル１> 障害発生時のデータ損失防止		□	■実機				
24	C.4.5.1	運用・保守性	外部システムとの接続有無	○	○	●	■主管課 ■情報部門 他システム連携一覧の情報収集と合意、切替にあたっての調整。連携テスト実施にあたり他社システム調整	■団体支援 システム構成図、連携一覧の整備。連携テスト実施にあたっての他社システム調整の支援 ■環境構築 他システム連携テストの実施	<レベル１> 庁内の外部システムと接続する		□			■実機		
25	C.5.9.1	運用・保守性	定期報告会実施頻度		○	●	■情報部門 定例会の実施	■運用保守 定例会の実施（通常の運用）	<レベル３> 四半期に１回					□		■机上
26	C.5.9.2	運用・保守性	報告内容のレベル		○	●	■情報部門 定例会の実施	■運用保守 定例会の実施（通常の運用）	<レベル３> 障害及び運用状況報告に加えて、改善提案を行う					□		■机上
27	C.6.2.1	運用・保守性	問い合わせ対応窓口の設置有無	○		●	■主管課 コンタクトセンター（問合せ窓口）の利用者整理、緊急連絡網についての整理	■運用保守 コンタクトセンター（問合せ窓口）の利用準備、緊急連絡網についての整理	<レベル１> ベンダーの既設コールセンターを利用する					□		■机上
28	D.1.1.1	移行性	システム移行期間	○	○	●	■情報部門 システム移行計画の検討、合意	■団体支援 システム移行計画の策定、説明実施	<レベル４> ２年未満						■机上	
29	D.1.1.2	移行性	システム停止可能日時	○	○	●	■主管課 ■情報部門 移行作業後の動作確認など主管課作業の検討と合意	■団体支援 移行作業計画にあたっての現地作業の整理 ■クラウド基盤 本番移行の計画作成と本番移行リハーサルや本番移行作業の実施	<レベル３> １日（計画停止日を利用）				□		■実機	
30	D.1.1.3	移行性	並行稼働の有無	○	○	●	■情報部門 システム移行計画の検討、合意（並行稼働はなし）	■環境構築 システム移行計画の策定し説明（並行稼働はなし）	<レベル０> 無し	【2022/4/28変更】 変更理由：記載誤り 変更前：レベル1（有り）					■机上	
31	D.4.1.1	移行性	移行データ量	△	△	●	■情報部門 移行データ量の合意	■クラウド基盤 本番移行リハーサルや本番移行を行い移行結果確認シートにて移行データ量を提供する	＊ ベンダーによる提案事項				□		■実機	
32	D.5.1.1	移行性	移行のユーザ/ベンダー作業分担	○	○	●	■情報部門 役割分担の検討、合意 システム移行作業における確認作業等の実施	■団体支援 移行作業計画にあたっての現地作業の整理 ■クラウド基盤 移行計画書を作成し、役割分担を明確化 本番移行リハーサルや本番移行を行う	<レベル１> ユーザとベンダーと共同で実施				□		■実機	

別紙１_検証項目の検証方法（a：非機能要件_住記等）

ベンダのみの項目

●主○副△支援

□準備、■机上、■実機

通番	標準非機能要件項番	大項目	メトリクス（指標）	担当			先行事業における検証方法				実施工程					
				団体		ベンダ	団体	ベンダ	検証の指標	備考	構築	検証（テスト）	データリフト	検証（副本）	移行	運用保守
				主管課	情報部門											
33	A.1.3.3	可用性	RLO（目標復旧レベル）（業務停止時）			●		■クラウド基盤 システム全体バックアップを行う製品を導入し、バックアップや、システム障害時の復旧手順を確立する。 ■運用保守 システム復旧手順の検証	<レベル２> 全システム機能の復旧	クラウドサービスで運用しているシステム全体のバックアップ・復旧の機能を、Govクラウドで利用できる製品で再構築することを想定。	□	■実機				
34	A.1.5.1	可用性	稼働率			●		■クラウド基盤 稼働率の母数について基準を決め、測定方法を決定する	<レベル３> 99.5%			■机上				
35	B.2.2.1	性能・拡張性	通常時バッチレスポンス順守度合い			●		■団体支援 バッチ実行検証にあたり主管課に対し、検証内容や手順、実施スケジュール等の提案・調整の実施、必要に応じバッチ運用設計の見直し作業の実施も想定。 ■環境構築 バッチ事前検証の実施	<レベル２> 再実行の余裕が確保できる	通常処理のバッチ実行時間の検証を行う。	□			■実機		
36	B.2.2.2	性能・拡張性	アクセス集中時のバッチレスポンス順守度合い			●		■団体支援 バッチ実行検証にあたり主管課に対し、検証内容や手順、実施スケジュール等の提案・調整の実施、必要に応じバッチ運用設計の見直し作業の実施も想定。 ■環境構築 バッチ事前検証の実施	<レベル２> 再実行の余裕が確保できる	ワースト処理時間のバッチ実行時間の検証を行う。	□			■実機		
37	C.1.2.2	運用・保守性	外部データの利用可否（バックアップとシステム復旧）			●		■クラウド基盤 システム全体バックアップを行う製品を導入し、バックアップや、システム障害時の復旧手順を確立する。	<レベル２> システムの復旧に外部データを利用できない	クラウドサービスで運用しているシステム全体のバックアップ・復旧の機能を、Govクラウドで利用できる製品で再構築することを想定。	□	■実機				
38	C.1.2.5	運用・保守性	バックアップ取得間隔			●		■環境構築 システム全体バックアップを行う製品を導入し、バックアップや、システム障害時の復旧手順を確立	<レベル４> 日次で取得	クラウドサービスで運用しているシステム全体のバックアップ・復旧機能を、Govクラウドで利用できる製品で再構築することを想定	□			■実機		
39	C.2.3.5	運用・保守性	OS等パッチ適用タイミング			●		■クラウド基盤 OS等のパッチ適用のため、Govクラウド上にWSUS機能を構築し運用を確立する	<レベル４> 緊急性の高いパッチは即適用し、それ以外は定期保守時に適用を行う	WSUSによるパッチ配付機能を構築することを検討する。。アプリ互換問題を想定しパッチによるタイミング制御検討	□	■実機				■実機
40	C.5.2.2	運用・保守性	保守契約（ソフトウェア）の種類			●		■クラウド基盤 リリースのフローや手順を策定しPTF保守作業の検証	<レベル２> アップデート		□					■実機
41	E.3.1.2	セキュリティ	Web診断実施の有無			●		■クラウド基盤 内部ネットから考え得る脅威を整理し対策を策定	<レベル１> 実施	変更理由：CSPのサービスの利用含めて実施方法を検討 変更前：机上検証	□	■実機				
42	E.4.3.4	セキュリティ	ウィルス定義ファイル適用タイミング			●		■クラウド基盤 ウイルス対策製品の導入と、ウイルス定義ファイルの更新運用を確立する	<レベル２> 定義ファイルリリース時に実施	クラウドサービスで運用しているウイルス対策およびウイルス定義を配付する仕組みの移植を想定	□	■実機				■実機
43	E.5.1.1	セキュリティ	管理権限を持つ主体の認証			●		■クラウド基盤 RDゲートウェイ構築。RDGWとサーバの2段階ログインを確認。オンライン利用制限やパスワードポリシー決定	<レベル３> 複数回、異なる方式による認証	ベンダ側の作業環境はクラウドサービスで運用しているRDゲートウェイを構築することを想定	□	■実機				
44	E.5.2.1	セキュリティ	システム上の対策における操作制限			●		■運用保守 稼働後を想定した運用操作の中で、制限された利用者権限で問題なく作業できるか検証 ■クラウド基盤 ActiveDirectoryを構築し、構築時以外は接続ユーザーはインストール等が制限されていることを確認	<レベル１> 必要最小限のプロフラムの実行、コマンドの操作、ファイルへのアクセスのみ許可する	ActiveDirectoryの構築を想定	□	■実機				
45	E.6.1.1	セキュリティ	伝送データの暗号化の有無			●		■クラウド基盤 SSLアクセラレータの利用を想定し業務システム設定を変更。通信パケットから認証情報が暗号化されていることを確認する	<レベル１> 認証情報のみ暗号化	SSLアクセラレータの利用を想定	□	■実機				
46	E.6.1.2	セキュリティ	蓄積データの暗号化の有無			●		■クラウド基盤 暗号化の範囲を明確に示し、直接参照できないことを確認する	<レベル２> 重要情報を暗号化	【2022/4/28変更】 変更理由：CSPのサービス利用 変更前：レベル１（認証情報のみ暗号化）	□	■実機				
47	E.7.1.1	セキュリティ	ログの取得			●		■クラウド基盤 Zabbixを構築しRDGWやFWのログを取得する。ログの取得範囲を明確化し適切に保管できることを確認	<レベル１> 必要なログを取得する		□	■実機				
48	E.7.1.3	セキュリティ	不正監視対象（装置）			●		■クラウド基盤 ログの取得範囲を明確に示し、適切に保管できることを確認する	<レベル１> 重要度が高い資産を扱う範囲			■机上				
49	E.10.1.1	セキュリティ	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			●		■クラウド基盤 共通制御の脆弱性対策について明確化。業務システムでパスワードポリシー有効期限を定めるなど対策実施	<レベル１> 対策の強化			■実機				
50	E.10.1.2	セキュリティ	WAFの導入の有無					対象外	<レベル０> 無し	【2022/4/28変更】 変更理由：対象外と判断 変更前：レベル1（対策の強化）						