

様式2 提案依頼事項一覧 ①非機能要件

項番	大項目	中項目	メトリクス (指標)	メトリクス説明	クラウド 調達時 の扱い ¹	利用ガイ ドの 解説 ²	選択レベル	選択時の条件	レベル							備考 「利用ガイド」第4章も参照のこと	仙台市	ベンダ回答			
									-	*	0	1	2	3	4		5	選択レ ベル	選択レ ベル	対応方針	
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 らから抽出したデータによって情報 システムを復旧できるような場合	仕様の対 象としない	ベンダー による提 案事項	外部デー タによりシ ステムの 全データ が復旧可 能	外部デー タによりシ ステムの 一部の データが 復旧可能	システム の復旧に 外部デー タを利用で きない				【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		
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、サーバー及び端末の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 性の高いものは即時に適用する。	○	P29	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）。	仕様の対 象としない	ベンダー による提 案事項	パッチを適 用しない	障害発生 時にパッ チ適用を 行う	定期保守 時にパッ チ適用を 行う	緊急性の 高いパッ チのみ即 時に適用 し、それ 以外は障 害対応時 等適切な タイミン グで適用 を行う	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	新規の パッチがリ リースされ るたびに 適用を行 う	【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)。 また、マイナンバー利用事務系のOSに ついては最新のパッチを速やかに適用 すること。 なお、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		
E.1.1.1	セキュリティ	前提条件・ 制約条件	順守すべき 規程、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	仕様の対 象としない	ベンダー による提 案事項	無し	有り					【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		
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	仕様の対 象としない	ベンダー による提 案事項	分析なし	重要度が 高い資産 を扱う範 囲	対象全体				【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		
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。	○	P30	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)。	仕様の対 象としない	ベンダー による提 案事項	定義ファ イルを適用 しない	定期保守 時に実施	定義ファ イルリリース 時に実施				【注意事項】 事前検証なく定義ファイルを適用しな ければならないというわけではない。 最新のウィルス定義ファイル適用時に、 ウィルス検索エンジンのアップデートも 検討すること。	2		
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、異なる方式による認証を実施すること により、不正アクセスに対する抑止効果を高め 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。	○	P31	3	複数回、 異なる方 式による 認証	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。 る。	仕様の対 象としない	ベンダー による提 案事項	実施しな い	1回	複数回の 認証	複数回、 異なる方 式による 認証			【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。 認証方式は大きく分けて「知識」、「所 持」及び「存在」を利用する方式があ る。 機器等(データ連携サーバー等)は多要 素認証の対象としない。	3		
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	必要最小 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 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	仕様の対 象としない	ベンダー による提 案事項	無し	必要最小 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。				【注意事項】 利用者に応じて適切に、実行可能なプ ログラム、コマンド操作、アクセス可能 なファイルを設定・管理すること。	1			

様式2 提案依頼事項一覧 ①非機能要件

項番	大項目	中項目	メトリクス (指標)	メトリクス説明	クラウド 調達時 の扱い ¹	利用ガイ ドの 解説 ²	選択レベル	選択時の条件	レベル								備考 「利用ガイド」第4章も参照のこと	仙台市 選択レ ベル	ベンダ回答		
									-	*	0	1	2	3	4	5			選択レ ベル	対応方針	
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。	○	P35	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	仕様の対象としない	ベンダーによる提案事項	復旧不要	5営業日前の時点(週次バックアップからの復旧)	1営業日前の時点(日次バックアップからの復旧)	障害発生時点(日次バックアップ+一時保存データからの復旧)			【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		
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。	○	P35	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	仕様の対象としない	ベンダーによる提案事項	1営業日以上	1営業日以内	12時間以内	6時間以内	2時間以内		【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。 目標復旧時間をSLAに定めていないクラウドサービスを利用する場合は、CSPがSLAで示す稼働率を元に業務停止時間の最大値を算出し、RTOを検討することが考えられる。	3		
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。	○	P36	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	仕様の対象としない	ベンダーによる提案事項	規定しない	一部システム機能の復旧	全システム機能の復旧				【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		
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。	○	P37	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、住民の安全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	仕様の対象としない	ベンダーによる提案事項	再開不要	数ヶ月以内に再開	一ヶ月以内に再開	一週間以内に再開	3日以内に再開	1日以内に再開	【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。	4		
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。	○	P38	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。	仕様の対象としない	ベンダーによる提案事項	規定しない	95%	99%	99.5%	99.9%	99.99%	【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		
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。	仕様の対象としない	ベンダーによる提案事項	特定ユーザのみ	上限が決まっている	不特定多数のユーザが利用					1		
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。	仕様の対象としない	ベンダーによる提案事項	特定利用者の限られたアクセスのみ	同時アクセスの上限が決まっている	不特定多数のアクセス有り					1		

項番	大項目	中項目	メトリクス (指標)	メトリクス説明	クラウド 調達時の扱い ¹	利用ガイ ドの解説 ²	選択レベル	選択時の条件	レベル								備考 「利用ガイド」第4章も参照のこと	仙台市	ベンダ回答	
									-	*	0	1	2	3	4	5		選択レ ベル	選択レ ベル	対応方針
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	仕様の対象としない	ベンダーによる提案事項	すべてのデータ件数、データ量が明確である	主要なデータ件数、データ量のみが明確である					【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。 なお、適切な構成でクラウドサービスを利用することで、拡張性を容易に確保することが考えられる。	1		
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	仕様の対象としない	ベンダーによる提案事項	処理ごとにリクエスト件数が明確である	主な処理のリクエスト件数のみが明確である					【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。 なお、適切な構成でクラウドサービスを利用することで、拡張性を容易に確保することが考えられる。	0		
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	仕様の対象としない	ベンダーによる提案事項	処理単位ごとに処理件数が決まっている	主な処理の処理件数が決まっている					【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。 なお、適切な構成でクラウドサービスを利用することで、拡張性を容易に確保することが考えられる。	1		
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)	○	P39	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	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内	【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		
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)	○	P40	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	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内	【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		
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	仕様の対象としない	ベンダーによる提案事項	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				2		

項番	大項目	中項目	メトリクス (指標)	メトリクス説明	クラウド 調達時の 扱い ¹	利用ガイ ドの 解説 ²	選択レベル	選択時の条件	レベル								備考 「利用ガイド」第4章も参照のこと	仙台市	ベンダ回答		
									-	*	0	1	2	3	4	5		選択レ ベル	選択レ ベル	対応方針	
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	仕様の対象としない	ベンダーによる提案事項	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				2			
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。)	○	P40	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、頻繁ではないが計画された稼働延長がある場合	仕様の対象としない	ベンダーによる提案事項	規定無し (不定期利用)	定時内での利用 (1日8時間程度利用)	繁忙期は定時外も頻繁に利用 (1日12時間程度利用)	定時外も頻繁に利用 (1日12時間程度利用)	24時間利用		【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。 一般的に、クラウドサービスにおいては、仮想サーバやコンテナなど、サービス起動時間に対して費用が発生する。運用時間を必要最低限に留め、サービスを停止させることでクラウドにかかるコストの削減が見込まれる。	1		
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。)	○	P40	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	仕様の対象としない	ベンダーによる提案事項	規定無し (原則利用しない)	定時内での利用 (1日8時間程度利用)	定時外も頻繁に利用 (1日12時間程度利用)	24時間利用		【注意事項】 一般的に、クラウドサービスにおいては、仮想サーバやコンテナなど、サービス起動時間に対して費用が発生する。運用時間を必要最低限に留め、サービスを停止させることでクラウドにかかるコストの削減が見込まれる。	1			
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	○	P41	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	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	システム構成の変更時など、任意のタイミング	月次で取得	週次で取得	日次で取得	同期バックアップ		4		
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の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	仕様の対象としない	ベンダーによる提案事項	各製品標準のマニュアルを利用する	情報システムの通常運用のマニュアルを提供する	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	ユーザのシステムの運用ルールに基づくカスタマイズされたマニュアルを提供する			【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。 なお、クラウドサービス上でのメンテナンス(一部サービスの提供終了や廃棄を含む)への対応に関するマニュアルについても想定される。	2		
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他システムや外部システム(団体が管理に関わらないシステム)との接続の有無に関する項目。	○		1	他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 [+] 外部システムに接続して、データのやり取りを行う場合	仕様の対象としない	ベンダーによる提案事項	他システムや外部システムと接続しない	他システムと接続する	外部システムと接続する				【注意事項】 庁外の民間クラウド等で稼働する場合でも、内部ネットワークで接続する場合は庁内のシステムと位置づけること。 また、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		
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	仕様の対象としない	ベンダーによる提案事項	保守契約を行わない	問い合わせ対応	アップデート				2			

項番	大項目	中項目	メトリクス (指標)	メトリクス説明	クラウド 調達時の 扱い ¹	利用ガイ ドの 解説 ²	選択レベル	選択時の条件	レベル							備考 「利用ガイド」第4章も参照のこと	仙台市	ベンダ回答			
									-	*	0	1	2	3	4		5	選択レ ベル	選択レ ベル	対応方針	
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	仕様の対 象としない	ベンダー による提 案事項	制約無し (必要な期 間の停止 が可能)	5日以上	5日未満	1日 (計画停止 日を利用)	利用の少 ない時間 帯(夜間な ど)	移行のた めのシス テム停止 不可	【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 が可能であることを示す。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		
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。	○	P44	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	仕様の対 象としない	ベンダー による提 案事項	移行対象 無し	移行対象 設備・機器 のハード ウェアを入 れ替える	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	移行対象 設備・機器 のシステ ム全部を 入れ替え る	移行対象 設備・機器 のシステ ム全部を 入れ替え て、さらに 統合化す る	【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			
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)。	○	P45	*	ベンダー による提 案事項	移行前システムのデータを抽出し たうえで、移行対象データを決定す る必要がある。	仕様の対 象としない	ベンダー による提 案事項	移行対象 無し	1TB未満	10TB未満	10TB以上			【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。	*		
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	仕様の対 象としない	ベンダー による提 案事項	すべて ユーザ	ユーザと ベンダーと 共同で実 施	すべてベ ンダー				【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		
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	仕様の対 象としない	ベンダー による提 案事項	制約無し	制約有り (重要な制 約のみ適 用)	制約有り (すべての 制約を適 用)				【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		
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	仕様の対 象としない	ベンダー による提 案事項	制約無し	制約有り (重要な制 約のみ適 用)	制約有り (すべての 制約を適 用)					1		

1 クラウド調達時の扱い

○:クラウドの対象と成り得る項目 △:クラウドの対象となる場合がある項目 -:通常クラウドの対象とならない項目

なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。

2 利用ガイドの解説

Pxx: 利用ガイドのメトリクス詳細説明ページ

様式2 提案依頼事項一覧 ①非機能要件

項番	大項目	中項目	マトリクス (指標)	マトリクス説明	クラウド 調達時の 扱い ¹	利用ガイ ドの 解説 ²	選択レベル		選択時の条件	レベル								備考 「利用ガイド」第4章も参照のこと	仙台市	ベンダ回答		
										-	*	0	1	2	3	4	5		選択レ ベル	選択レ ベル	対応方針	
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。	○	P48	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	仕様の対象としない	ベンダーによる提案事項	復旧しない	限定された構成で情報システムを再構築	同一の構成で情報システムを再構築	限定された構成をDRサイトで構築	同一の構成をDRサイトで構築		【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			
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	仕様の対象としない	ベンダーによる提案事項	外部保管しない	1ヶ所(近隣の別な建物)	1ヶ所(遠隔地)	2ヶ所(近隣の別な建物と遠隔地)	2ヶ所(遠隔地)		【注意事項】 ここで遠隔地とは、主系サーバ等の設置場所と同時被災の恐れがない遠隔地であり、庁舎等の利用場所から見ての遠隔地では無い。 A.3.2.2(保管方法(外部保管データ))と合わせて考慮し、整合するようにレベルを選択すること。	2			
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。	○	P49	2	ネットワーク経由でストレージへのリモートバックアップを含む	A.3.2.1と同じ拠点へのリモートバックアップを想定。 [-]媒体での外部保管のみによる運用を許容できる場合	仕様の対象としない	ベンダーによる提案事項	外部保管しない	媒体による外部保管のみ	ネットワーク経由でストレージへのリモートバックアップを含む				【注意事項】 A.3.2.1(保管場所分散度(外部保管データ))と合わせて考慮し、整合するようにレベルを選択すること。	2			
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。	○	P50	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	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	障害発生時のデータ損失防止	職員の作業ミスなどによって発生したデータ損失防止				【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			
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。	○	P51	4	レベル3に加えて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	仕様の対象としない	ベンダーによる提案事項	監視を行わない	死活監視を行う	レベル1に加えてエラー監視を行う	レベル2に加えてエラー監視(トレース情報を含む)を行う	レベル3に加えてリソース監視を行う	レベル4に加えてパフォーマンス監視を行う	【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			
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	仕様の対象としない	ベンダーによる提案事項	無し	年1回	半年に1回	四半期に1回	月1回	週1回以上	【注意事項】 業務ごとの定期報告会の頻度を指す。また、障害発生時に実施される不定期の報告会は含まない。	4			

