
~~地方公共団体の基幹業務システムの標準非機能要件~~
地方公共団体情報システム非機能要件の標準

【第1.1版】(案)

令和4年8月

デジタル庁
総務省

「標準非機能要件」「非機能要件の標準」について

「標準非機能要件」「非機能要件の標準」は、「非機能要求グレード(地方公共団体版)」（平成26年3月・JLIS作成(※)）において、業務・システムの分類「グループ②」として示された要求グレードのうち、クラウド調達時の扱いが「○:クラウドの対象と成り得る項目」とされている項目を中心に、必要と考えられる項目の「選択レベル」を基準として、最新の状況等を鑑み修正・追加をしたものである。

※ JLISが、IPAが作成した「非機能要求グレード2013年4月版」を基に、地方公共団体が業務システムを調達する際に、業務システムに共通する非機能要件として一部を改変したものの。

1. 「標準非機能要件」「非機能要件の標準」を用いる業務システム

・ 「デジタル社会の実現に向けた重点計画」（令和4年6月7日閣議決定）で定める基幹業務等システムの統一・標準化を行う業務とする20業務(※)に係る、市町村が使用するシステム。

※ 住民基本台帳、戸籍、戸籍の附票、固定資産税、個人住民税、法人住民税、軽自動車税、印鑑登録、選挙人名簿管理、子ども・子育て支援、就学、児童手当、児童扶養手当、国民健康保険、国民年金、障害者福祉、後期高齢者医療、介護保険、生活保護、健康管理

2. 「標準非機能要件」「非機能要件の標準」の利用方法

○各開発ベンダ

・ 「標準非機能要件」「非機能要件の標準」に従って、クラウドサービスによりシステムを提供する。
・ 「標準非機能要件」「非機能要件の標準」の各項目の選択レベルを下げたものが一つでもあれば、「標準非機能要件」「非機能要件の標準」を満たしているものとはしない。

○各市町村

・ 上記20業務に係る情報システム調達の際に、開発ベンダに対して示す非機能要件は、「標準非機能要件」「非機能要件の標準」とする。
・ なお、次に示す非機能要件は「標準非機能要件」「非機能要件の標準」が示す要件に従って、各市町村の業務量に応じて各市町村が具体的な値を示すこととする。
「B.1.1.1 ユーザ数」、「B.1.1.2 同時アクセス数」、「B.1.1.3 データ量(項目・件数)」、「B.1.1.4 オンラインリクエスト件数」、「B.1.1.5 バッチ処理件数」

3. 上記20業務に係る各業務システムの標準仕様と「標準非機能要件」「非機能要件の標準」の関係

・ 各業務システムの標準仕様において、非機能要件に関して独自の厳しい要件を定めた場合には、当該標準仕様の非機能要件部分が、「標準非機能要件」「非機能要件の標準」に優先するものとする。

「標準非機能要件」「非機能要件の標準」の使用方法について

- 「標準非機能要件」「非機能要件の標準」の活用シートでは、調達時に定めるべき非機能要件の項目を示しており、項目ごとにあり得るレベル(レベル0から5)を示している。
- 各開発ベンダ・市町村が調達を行う際には、各項目について「選択時の条件」における「選択レベル」として示されたレベルを使用する。

例) 項番C.1.2.2「運用・保守性」(通常運用)の「外部データの利用可否」については、選択レベル2「システムの復旧に外部データを活用できない」を使用する。
 項番C.2.3.5「運用・保守性」(保守運用)の「OS等パッチ適用タイミング」については、選択レベル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」を使用する。

利用ガイドは、「非機能要求グレード(地方公共団体版)利用ガイド」(平成26年3月・JLIS作成)のことを指す。

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			
									-	*	0	1	2	3		4	5	
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。
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 [-] 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常時適用すること。 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。	

各開発ベンダ・市町村が調達を行う際に使用する非機能要件のレベル

[-]は、選択レベルを下げる場合の条件
 [+]は、選択レベルを上げる場合の条件を記載している。

活用シート【I 全庁的要求事項シート】

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				
									-	*	0	1	2	3	4		5			
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、そこから抽出したデータによって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	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ることができる。
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座即時に適用する。	○	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くない場合(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、「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。 また、マイナンバー利用事務系のOSについては最新の修正パッチを常時適用すること。
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。
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、どの範囲を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)。
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。	○	P30	2	定義ファイルリリース時に実施	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)。	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。 最新のウイルス定義ファイル適用時に、ウイルス検索エンジンのアップデートも検討すること。

活用シート【I 全庁的要求事項シート】

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		
									-	*	0	1	2	3	4		5	
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、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、生体認証等がある。	○	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。 [+]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	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(データ連携サーバ等)は多要素認証の対象としない。
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。	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。
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。	○	P31	4 3	認証情報のみ暗号化 すべてのデータを暗号化	インターネットに直接接続せず、内部ネットワークのみをに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。	仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化	すべてのデータを暗号化			【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】 本項番の「暗号化」は「ハッシュ化」等も含む。 ガバメントクラウド及びISMAPクラウドサービスリストに登録されているクラウドサービスについては、ISMAPの認証の過程で通信のセキュリティ対策の実施を確認しているため、クラウドサービス内の伝送データの暗号化は必須ではない。 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)。
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。	○	P32	4 3	認証情報のみ暗号化 すべてのデータを暗号化	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、又は、クラウドサービスの仕様により暗号化消去を行う場合(後者については選択レベルを2上げる)	仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化	すべてのデータを暗号化			【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】 本項番の「暗号化」は「ハッシュ化」等も含む。 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)。 システム利用開始時点からの全データを暗号化すること。

活用シート【I 全庁的要求事項シート】

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				
									-	*	0	1	2	3	4		5			
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。 <i>(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)</i>	仕様の対象としない	ベンダーによる提案事項	取得しない	必要なログを取得する							【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 ・セキュリティ機器の検知ログ ・通信ログ ・DBログ ・アプリケーションログ 等
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、ネットワーク機器、端末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、ネットワーク機器、端末等の範囲を定めておく必要がある。	仕様の対象としない	ベンダーによる提案事項	無し	重要度が高い資産を扱う範囲	システム全体						
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。	○	P32	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。 [-] インターネットに接続したWebアプリケーションを用いない場合	仕様の対象としない	ベンダーによる提案事項	無し	対策の強化							
E.10.1.2	セキュリティ	Web対策	WAFの導入の有無	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。	○	P33	0	無し	インターネットに直接接続せず、内部ネットワークのみを接続する情報システムを想定。 <i>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。</i> [+] インターネットに接続したWebアプリケーションを用いる場合	仕様の対象としない	ベンダーによる提案事項	無し	有り							

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([J-LIS-4章](#)みてね)

活用シート【Ⅱ 業務主管部門要求事項シート】

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					
									-	*	0	1	2	3	4		5				
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増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。
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、GSP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。		
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。	○	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。)		
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	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。			

活用シート【Ⅱ 業務主管部門要求事項シート】

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		
										-	*	0	1	2	3	4		5	
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率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	
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					
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					
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。
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。
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。

活用シート【Ⅱ 業務主管部門要求事項シート】

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	
										-	*	0	1	2	3	4		5
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。	
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。	
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				
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				

活用シート【Ⅱ 業務主管部門要求事項シート】

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		
									-	*	0	1	2	3	4		5	
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) [-] 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	開庁時間を定時と想定。	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)	定時外も頻繁に利用(1日12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)	24時間利用	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。	
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	休日等の窓口開庁がある場合を想定。	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。	
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 [-] RPOの要件が[-]される場合 [+] RPOの要件が[+]される場合	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。	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	
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 [-] 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	運用をユーザが実施することを想定。	仕様の対象としない	ベンダーによる提案事項	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。
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(団体が管理に関与しないシステム)との接続の有無に関する項目。	○		1	他システム ・ 序内の外部システム 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 [+] 序外の 外部システムに接続して、データのやり取りを行う場合	序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 序内の 他システムが存在することを想定。	仕様の対象としない	ベンダーによる提案事項	他システム や外部システムと接続しない	他システム ・ 序内の外部システム と接続する	序外の 外部システムと接続する			【注意事項】 序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序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。	
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	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。	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				

活用シート【Ⅱ 業務主管部門要求事項シート】

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	
										-	*	0	1	2	3	4		5
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	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 が可能なることを示す。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。
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。	
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	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 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。	

活用シート【Ⅱ 業務主管部門要求事項シート】

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			
									-	*	0	1	2	3	4		5		
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 決めなどが無い場合	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。
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 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
2 利用ガイドの解説 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。
Pxx: 利用ガイドのメトリクス詳細説明ページ

活用シート【Ⅲ実現方法要求事項シート】

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	
									-	*	0	1	2	3	4		5
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。
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カ所 [+] 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から見ての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。
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	DRサイトへのリモートバックアップを想定。 [-] 媒体での保管のみによる運用を許容できる場合 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	仕様の対象としない	ベンダーによる提案事項	媒体による保管 外部保管しない	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 媒体による外部保管のみ	DRサイトへのリモートバックアップ 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				【レベル】 レベル1及び2のバックアップとは、リアルタイムにデータバックアップの取得が可能であるものを意味する。また、レベル2のDRサイトとは、システム設置場所(庁舎等の利用場所と必ずしも一致しない)と同時被災の恐れがない遠隔地を意味する。 【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、同水準を示す整合するようにレベルを選択すること。
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。

活用シート【Ⅲ実現方法要求事項シート】

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	
									-	*	0	1	2	3	4		5
C.1.3.1	運用・保守性	通常運用	監視情報	<p>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べきかを決定することを目的としている。</p> <p>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。</p>	○	P51	4	<p>レベル3に加えてリソース監視を行う</p> <p>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。</p> <p>[-] 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</p>	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	<p>【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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>【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。</p>
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	<p>四半期に1回</p> <p>[-] 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</p>	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	<p>【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。</p>
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	<p>障害及び運用状況報告に加えて、改善提案を行う</p> <p>障害発生時など改善提案が必要な場合を想定</p>	仕様の対象としない	ベンダーによる提案事項	無し	障害報告のみ	障害報告に加えて運用状況報告を行う	障害及び運用状況報告に加えて、改善提案を行う			
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。	○	P52	1	<p>ベンダーの既設コールセンターを利用する</p> <p>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</p> <p>[-] 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</p>	仕様の対象としない	ベンダーによる提案事項	問い合わせ対応窓口の設置について規定しない	ベンダーの既設コールセンターを利用する	ベンダーの常駐等専用窓口を設ける				<p>【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。</p>
C.6.3.1	運用・保守性	その他の運用管理方針	インシデント管理の実施有無	システムで発生するインシデントの管理を実施するかどうかを確認する。インシデント管理の実現方法については、有無の確認後に具体化して確認する。	△		1	<p>既存のインシデント管理のプロセスに従う</p> <p>運用管理業務のうちインシデントに対する管理として求める内容。</p> <p>[-]運用管理契約を行わない場合 [+]新たにプロセスを作成する必要がある場合(既存のプロセスを見直す場合を含む)</p>	仕様の対象としない	ベンダーによる提案事項	インシデント管理について規定しない	既存のインシデント管理のプロセスに従う	新規にインシデント管理のプロセスを規定する				

活用シート【Ⅲ実現方法要求事項シート】

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		
									-	*	0	1	2	3	4		5	
C.6.4.1	運用・保守性	その他の運用管理方針	問題管理の実施有無	インシデントの根本原因を追究するための問題管理を実施するかどうかを確認する。問題管理の実現方法については、有無の確認後に具体化して確認する。	△		1	既存の問題管理のプロセスに従う [-]運用管理契約を行わない場合 [+]新たにプロセスを作成する必要がある場合(既存のプロセスを見直す場合を含む)	仕様の対象としない	ベンダーによる提案事項	問題管理について規定しない	既存の問題管理のプロセスに従う	新規に問題管理のプロセスを規定する					
C.6.5.1	運用・保守性	その他の運用管理方針	構成管理の実施有無	リリースされたハードウェアやソフトウェアが適切にユーザ環境に構成されているかを管理するための構成管理を実施するかどうかを確認する。構成管理の実現方法については、有無の確認後に具体化して確認する。	△		1	既存の構成管理のプロセスに従う [-]運用管理契約を行わない場合 [+]新たにプロセスを作成する必要がある場合(既存のプロセスを見直す場合を含む)	仕様の対象としない	ベンダーによる提案事項	構成管理について規定しない	既存の構成管理のプロセスに従う	新規に構成管理のプロセスを規定する					
C.6.6.1	運用・保守性	その他の運用管理方針	変更管理の実施有無	ハードウェアの交換やソフトウェアのパッチ適用、バージョンアップ、パラメータ変更といったシステム環境に対する変更を管理するための変更管理を実施するかどうかを確認する。変更管理の実現方法については、有無の確認後に具体化して確認する。	△		1	既存の変更管理のプロセスに従う [-]運用管理契約を行わない場合 [+]新たにプロセスを作成する必要がある場合(既存のプロセスを見直す場合を含む)	仕様の対象としない	ベンダーによる提案事項	変更管理について規定しない	既存の変更管理のプロセスに従う	新規に変更管理のプロセスを規定する					
C.6.7.1	運用・保守性	その他の運用管理方針	リリース管理の実施有無	承認された変更が正しくシステム環境に適用されているかどうかを管理するリリース管理を実施するかどうかを確認する。リリース管理の実現方法については、有無の確認後に具体化して確認する。	△		1	既存のリリース管理のプロセスに従う [-]運用管理契約を行わない場合 [+]新たにプロセスを作成する必要がある場合(既存のプロセスを見直す場合を含む)	仕様の対象としない	ベンダーによる提案事項	リリース管理について規定しない	既存のリリース管理のプロセスに従う	新規にリリース管理のプロセスを規定する					
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	仕様の対象としない	ベンダーによる提案事項	システム移行無し	3ヶ月未満	半年未満	1年未満	2年未満	2年以上		
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	仕様の対象としない	ベンダーによる提案事項	無し	有り						【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。
E.3.1.2	セキュリティ	セキュリティ診断	Webアプリケーション診断実施の有無	Webアプリケーション診断とは、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、インターネットに接続したWebアプリケーションを用いない場合	仕様の対象としない	ベンダーによる提案事項	不要	実施						

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

2 利用ガイドの解説 2x:利用ガイドのメトリクス詳細説明ページ