地方自治体の業務プロセス・情報システムの 非機能要件の標準(標準非機能要件)

令和2年9月

内閣官房 情報通信技術(IT)総合戦略室 総務省自治行政局行政経営支援室 地域情報政策室

「標準非機能要件」について

「標準非機能要件」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「〇・クラウドの対象と成り得る項目」とされている項目の「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。

1. 「標準非機能要件」を用いる業務システム

・ 新経済・財政再生計画改革工程表2019」(令和元年12月19日)及び「デジタルガバメント実行計画」(令和元年12月20日閣議決定)において、地方公共団体の業務プロセス・情報システムの標準化を検討する対象とされた17業務(※)に係る、市町村が使用するシステム。

※ 住民基本台帳、選挙人名簿管理、固定資産税、個人住民税、法人住民税、軽自動車税、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、児童手当、生活保護、健康管理、就学、児童扶養手当、子ども子育支援。

2. 「標準非機能要件」の利用方法

- ○各開発ベンダ
- 「標準非機能要件」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」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」を満たしているものとはしない。

〇各市町村

- 上記17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」とする。
- ・ なお、次に示す非機能要件は「標準非機能要件」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17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」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」に優先するものとする。

「標準非機能要件」の使用方法について

- ・「標準非機能要件」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4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	メトリクス (指標)	メトリクス説明	クラウド	イドの		グル ープ ②				レ	ベル				備考 [利用ガイド]第4章も参照のこと
			(IBIA)		の扱い'	解說。	選択レベル	選択時の条件	-	*	0	1	2	3	4	5	217,000
0.1.22	運用-保守性	通常運用	利用可否	外部データによりシステムのデータが関目可能 かどうか確認するための項目。 外部データとは、当能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)。		•	の復旧に 外部デー ^{気を利} 用	全データを復用するためのバックフップ方式を検討しなければならないことを認定。 「一外部に同じデータを持つ情報システムが存在するため、本システムでは書きが発生した限けは、そちらかやデータを持ってきて情報システムを復用できるような場合	製をしない	李項	外部デー タによりシ ステムの 全データ が復旧可 能	タによりシ ステムの	システム の復日に 外部デー タを利用で きない				住店専項 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 計か優先度セレベルを下げて考えるこ とかできる。
02.35	運用·保守性	保守運用	適用タイミン グ	CS等パッチ情報の展開とパッチ適用のポリ シーは関する項目 DS等は、OS、ミドルウェア、その他のソフトウェ アを指す。 開閉付出さするセキュリティバッチなどの緊急 性の高いものは即座に適用する。	/	P29	高いパッ チは即時 に適用 し、それ 以外は足 期保守時	緊急性の高いいの手を除くと、定期保守時にいっチを適用するのが一 脈対し続き。 「一)外部と機構することが全くない等 の離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)。	奏としない	ベンダー こ よる提案 事項	バッチを適 用しない	時にバッチ	時にパッチ	高いパッチ のみ即時 に適用を	高いパッチ は即時に 適用し、そ	パッチがり リースされ るたびに	(注意事項) リリースされるバッチの種類(個別パッチ/集合/かチ)よって選択レベルが変わる場合がある。 セキュリティか・テについては、セキュリティの項目でも検討すること(E43.4)。

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

[一]は、選択レベルを1つ下げる場合の条件 [+]は、選択レベルを1つ上げる場合の条件を記載している。

活用シート【 [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	調達時	利用ガ イドの			グループ②				レ	ミル				備考 [利用ガイド」第4章も参照のこと
					の扱い ¹	解説2	選択し	レベル	選択時の条件	-	*	0	1	2	3	4	5	- 「一・「「「」が十二の一・「「「」「「」「「」「」「」
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)。	0		5	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	仕様の対象としない		によりシス テムの全 データが復	外部データ によりシー テムのデータ が復旧可 能	復旧に外 部データを 利用できな				【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、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。	0	P29	in : : : : : : : : : : : : : : : : : : :	高いパッ チは即時 に適用 し、それ 以外は定	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	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	時にパッチ	高いパッチ	は即時に適用し、そ	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)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。
E.1.1.1	セキュリティ		程、ルール、 法令、ガイド	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	0		1 7		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		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。	0		7	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		ファイル適用	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。	0	P30	-	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)。				時に実施	定義ファイルリリース時に実施				
E.5.1.1				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。	0	P31	1 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	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	10	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。

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	調達時	利用ガイドの		グループ②				レ	ヾル				備考 「利用ガイド」第4章も参照のこと
			(JEDK)		の扱い ¹	解説 ²	選択レベ	ズル 選択時の条件	-	*	0	1	2	3	4	5	
E.5.2.1	セキュリティ			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。	0		限の グライマン 操 イルアク	等)を利用可能にしている等により、 テ、コ 情報漏洩の脅威が現実のものといいのはなってしまうため、これらの情報等 作、ファ への不要なアクセス方法を制限する必要がある。 アセス (操作を制限することにより利便性 外許可 や、可用性に影響する可能性があ	仕様の対象としない	ベンダーに、よる提案事項	無し	必要のでは、 のでは、 では、 では、 では、 では、 でいました。 でいまた。					
								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	:								
E.6.1.1	セキュリティ	データの秘		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 認記 の <i>d</i> 化	正情報 内部ネットワークのみ接続する情報 外暗号 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。	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。
					0	P31											【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)。
E.6.1.2	セキュリティ			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 認記 の <i>社</i> 化	正情報 蓄積するパスワード等については 外暗号 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	仕様の対 くくない	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				【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。
					0	P32											【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)。
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。	0		1 必要 グを する	[取得 「いつ」「誰が」「どこから」「何を実行	象としない	ベンダーに よる提案 事項	取得しない	N 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 等
E.7.1.3	セキュリティ			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。	0		高し	要度が 脅威が発生した際に、それらを検知 い資産 し、その後の対策を迅速に実施する 及う範 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。	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				

活用シート【 I 全庁的要求事項シート】

項都	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		グループ②				レヘ	ドル				備考 「利用ガイド」第4章も参照のこと
					の扱い	丹山	選択レベル	選択時の条件	-	*	0	1	2	3	4	5	
E.10.	.1 セキュリティ	(Web対策	ディング、Web サーバの設 定等による対	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。	0	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。 [-] 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.	.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。	0	P33	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	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

O:クラウドの対象と成り得る項目 Δ: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

項番	大項目	中項目	メトリクス (指標)	メトリクス説明	調達時	利用ガイドの			グループ②				<i>ا</i> ما	ベル				備考 .[利用ガイド」第4章も参照のこと
			(1日1末/		の扱い ¹	解説 ²	選択	レベル	選択時の条件	-	*	0	1	2	3	4	5	. [作成のイド] 第4章 0参照のこと
A.1.3.1	可用性	継続性	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。	0	P35		前の時点 (日次バッ クアップ	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	クアップか	の時点 (日次バッ クアップか	時点 (日次バッ			【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	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。	0	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。
A.1.3.3	可用性	継続性	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。	0	P36				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		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	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。	0	P37	2	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。機能能に業務が再開できる最低限の間、パックアップデータから必要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行2時間が入った。必要なデータを持ついては、発災後72時間が用できる形式で提供すること。 [+] 人命に影響を及ぼす、経済的なれる場合でベンダーと合意できる場合		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。
A.1.5.1	可用性	継続性		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。	0	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		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14.5時間 99%・・・・・年間累計停止時間145時間

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	イドの		グループ②				V	ベル				備考 【利用ガイド」第4章も参照のこと
			(打日1)		の扱い ¹	解説 ²	選択レベル	退択時の条件	_	*	0	1	2	3	4	5	」「小川のイド」第4早も参照のこと
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 まっ ^っ る			ベンダー() よる提案 事項		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。	0		1 同時 セス(限が まって る	アク 特定のユーザがアクセスすることを O上 想定。 央 Cい	仕様の対象としない	ベンダー(i よる提案 事項	者の限ら	同時アクセ スの上限 が決まって いる	数のアクセ				
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		データ 数、ラ タ量が	での 要件定義時には明確にしておく必要件 要がある。 当一 が明 [+] 全部のデータ量が把握できている。 ない場合	象としない	ベンダーに いよる提案 事項	データ件 数、データ	主要な データ件 数、のみ 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。
B.1.1.4	性能・拡張性	業務処理量		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		0 処理 にリグ スト作 がある	エ 要がある。	象としない	ベンダーに よる提案 事項	型型ごとに リクエスト 件数が明 確である	のリクエス					【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。
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		ごとに 理件	単位 要件定義時には明確にしておく必 でをがある。 数が のて [+] 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(i) よる提案 事項	型理単位 ごとに処理 件数が決 まっている	の処理件					【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。
B.2.1.4	性能・拡張性	性能目標値	インレスポン	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)	0	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	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。
B.2.1.5	性能・拡張性	性能目標値	時のオンライ	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)	0	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	象としない		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。

項番	大項目	中項目	メトリクス (指標)	メトリクス説明	調達時	利用ガイドの			グループ②				レヘ	いし				備考 [利用ガイド」第4章も参照のこと
					の扱い ¹	解説 ²	選択	しベル	選択時の条件	-	*	0	1	2	3	4	5	
B.2.2.1	性能・拡張性	性能目標値	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。	0			余裕が確	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	間内に収	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	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)	0		2	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				
C.1.1.1	運用·保守性	通常運用	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。)	0	P40		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	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)	の利用 (1日8時間 程度利用)	定時外も 頻解に利 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。 定時:
C.1.1.2	運用·保守 性	通常運用	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。)	0	P40	1	の利用 (1日8時 間程度利	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	よる提案	規定無し(原則利用しない)	の利用 (1日8時間 程度利用)	頻繁に利 用	24時間利用			
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	0	P41	4	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	よる提案	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		同期バック アップ	

項番	大項目	中項目	メトリクス (指標)	メトリクス説明	調達時	利用ガイドの			グループ②				1 /	ベル				備考 [利用ガイド」第4章も参照のこと
			(JE DA)		の扱い ¹	解説 ²	選択	レベル	選択時の条件	-	*	0	1	2	3	4	5	
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。	0		1	テムの通 常軍 保マニュ アルする 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	象としない	ベンダーに よる提案 事項	準のマニュ	情報システムの通常運用のマニュアルを提供する	テムの通 常運用と 保守運用 のマニュア	ユーザの システール にタマール にタマたれ ニュア に 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。
	運用·保守性		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。	0		ļ;	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	仕様の対象としない	ベンダーに よる提案 事項	外部シス テムと接続 しない	庁内の外 部システム と接続する	部システム				【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。
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。	0			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				
D.1.1.2	移行性	移行時期	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 前パックアップの時間等も含むこと。)	0		;	ない時間 帯(夜ど)	[-] 停止を増やす場合	象としない	事項	(必要な期間の停止が可能)				ない時間 帯(夜間な ど)	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】 レベルの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、システム停止で割約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、システム停止可能は日や時間帯など、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)		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。	0	P44		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	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	設備・機器 のハード ウェアを入 れ替える	設備・機器 のハード	設備・機器 のシステム 全部を入 れ替える	設備∙機器		【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。

項番	大項目	中項目	メトリクス (指標)	メトリクス説明	調達時	利用ガイドの			グループ②				ν·	ベル				備考 _[利用ガイド」第4章も参照のこと
			(12)		の扱い ¹	解説2	選护	マレベル	選択時の条件	-	*	0	1	2	3	4	5	
D.4.1.1	移行性	移行対象 (データ)		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)。	0	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	が 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		移行のユー ザ/ベンダー 作業分担	移行作業の作業分担。	0		1	ユーザーと実施	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	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。
	境・エコロジー	システム制 約/前提条 件	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	0			(重要な制 約のみ適 用)	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	象としない	よる提案事項		(重要な制 約のみ適 用)	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。
		システム制 約/前提条 件	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				(重要な制	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	象としない	ベンダーに よる提案 事項		約のみ適用)	(すべての 制約を適 用)	l'order to			

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

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	調達時	利用ガイドの			グループ②				レ	ベル				備考 」 [利用ガイド]第4章も参照のこと
			(TH PA)		の扱い ¹ 	解説 ²	選択	マレベル	選択時の条件	-	*	0	1	2	3	4	5	[[]]]
A.3.1.1	可用性	災害対策		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。	0	P48		成で情報	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 事項	復旧しない	た構成で 情報シス	同一の構 成で情報 システムを 再構築	限定され た構み 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】 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		散度(外部保	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。	0		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	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 (遠隔地)			【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。
A.3.2.2			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。	0	P49		テム所入りのアップ	[+] コストと実現性を確認した上で、 可用性を高めたい場合	象としない	ベンダーに よる提案 事項	る保管	テム設置 場所内の 別へいクアッ ブ	アップ				
C.1.2.3	性性		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。	0	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) ヘ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	よる提案	プを取得し	時のデー	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	調達時	利用ガイドの			グループ②				ν	ベル				備考 「利用ガイド」第4章も参照のこと
			VIII DAV		の扱い ¹	解説 ²	選択	レベル	選択時の条件	-	*	0	1	2	3	4	5	[1],130 [1] [3], 14 05],130 = 2
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。	0	P51	4	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	象としない	ベンダーに よす 事項	監視を行 わない	死活監視を行う	エラー監視を行う	エラー監視(トレース含む) う	視を行う	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監視とは、対象が出力する立ち合む。トレース情報のこと。トレース情報のこと。トレース情報についても判断することができ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に対し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ーク帯監視のこと。パフォーマンス監視とは、対象が出力するにといったリソースの使用状況を判断するにといったリソースに使用が必要するパフォーマンス監視とは、対象が出力するによったり、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ことでは、常の入出力、ネ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。
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。	0		3	10	[-] 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	象としない		無し	年1回	半年に1回	四半期に1回	月1回	週1回以上	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。 【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。
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。	0			障害及び 運用状況 報告に改 き提 を 表 そ そ そ そ そ そ で 、 変 を そ う で 、 変 を う で 、 き た う る う う う う う う う う う う う う う う う う う	障害発生時など改善提案が必要な 場合を想定	象としない	ベンダーに よる提案 事項		障害報告 のみ	障害報告 に加えて 運用状況 報告を行う	運用状況 報告に加			
C.6.2.1			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。	0	P52		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	象としない	よる提案	せ対応窓 口の設置	の既設 コールセン ターを利用	ベンダー の常駐等 専用窓口 を設ける				【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。
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。	0		4		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	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	

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		グループ②				レ^	ベル				備考 [利用ガイド]第4章も参照のこと
					071120	77-10-6	選択レベル	選択時の条件	-	*	0	1	2	3	4	5	
D.1.1.3	移行性			移行作業から本稼働までのシステムの並行稼働の有無。	0		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			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。	0		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	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 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