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	選択レベル	選択時の条件	[+][-]条件	レベル						備考
									-	*	0	1	2	3	4	5	
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	1回	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。 [+] 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】 重要度が高い資産は、各自治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）。
						2	0				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				
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。	○		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】 定義ファイルを適用する際には事前検証を実施した上で速やかに適用することが望ましい。 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。