項番	大項目	中項目	メトリクス（指標）	メトリクス説明	レベル								備考
					-	*	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）。	仕様の対象としない	ベンダーによる提案事項	全データの復旧に利用できる	一部のデータ復旧に利用できる	外部データは利用できない				・現状はサーバー筐体内に日時で全データバックアップを取得。クライアント端末（１台）の起動時にバックアップデータをコピーしている。 ・クラウドサービスの利用も検討し、将来的にバックアップは2拠点とする。
C.2.3.5		保守運用	OS等パッチ※[4]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。	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	・（パブリッククラウドの利用など）今後利用するネットワーク次第で要求レベルは変化するが、現時点ではパブリッククラウドの利用を想定し、緊急性の高いパッチは即時適用とする。
C.4.4.1		リモートオペレーション※	リモート監視※地点	情報システムの設置環境とは離れた環境からのネットワークを介した監視や操作の可否を定義する項目。	仕様の対象としない	ベンダーによる提案事項	リモート監視※を行わない	庁内LANを介してリモート監視を行う	ベンダー拠点等外部からリモート監視を行う				
C.4.4.3			リモート操作※時の接続方法	ベンダーがリモート監視※地点からリモート操作を実施する場合の回線接続方法。	仕様の対象としない	ベンダーによる提案事項	リモート操作※を行わない	リモート操作※の必要時のみ接続する	常時接続環境にてリモート操作※を行う				
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） ・情報セキュリティポリシー ・個人情報保護法 ・電子署名法 ・IT基本法 ・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 ・プライバシーマーク	仕様の対象としない	ベンダーによる提案事項	無し	有り					・市情報セキュリティポリシーに基づくこと。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	レベル								備考
					-	*	0	1	2	3	4	5	
E.2.1.1		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。	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、あるいは、外接部分	開発範囲				・インターネットVPNを使用する想定のため、重要資産及びインターネット等との接続点において、セキュリティ診断・ペネトレーションテストを行い評価すること。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	レベル								備考
					-	*	0	1	2	3	4	5	
E.4.3.4		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。	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				
E.5.1.1		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。	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			・二要素認証とすること。
E.5.2.1			システム上の対策における操作制限度	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） コマンド実行制,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。	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※のみを許可					・現状、サーバー管理者と通常の作業者のアカウントは分かれており、権限のコントロールが可能であるため、同様とすること。
E.6.1.1		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。	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			
E.6.1.2			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。	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				

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	レベル								備考
					-	*	0	1	2	3	4	5	
E.7.1.1		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。	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					・最低限、システムログとアクセスログを取得すること。
E.7.1.3			不正監視対象（装置）	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。	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、あるいは、外接部分	システム全体				
E.10.1.1		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。	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					・パッケージ適用のため、脅威から保護されるような対策を要求する。
E.10.1.2			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。	仕様の対象としない	ベンダーによる提案事項	無し	有り					
F.3.1.1	システム環境・エコロジー	適合規格	規格取得の有無(安全性)	提供する情報システムに使用する製品について、UL60950※などの製品安全規格を取得していることを要求されているかを確認する項目。	仕様の対象としない	ベンダーによる提案事項	規格取得の必要無し	規格取得の必要有り					
F.3.2.1			規格取得の有無（有害物質）	提供する情報システムに使用する製品について、RoHS指令※などの特定有害物質の使用制限についての規格の取得を要求されているかを確認する項目。	仕様の対象としない	ベンダーによる提案事項	規格取得の必要無し	RoHS指令※相当取得					

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	レベル								備考
					-	*	0	1	2	3	4	5	
F.5.1.1		環境マネージメント	グリーン購入法対応度	環境負荷を最小化する工夫の度合いの項目。 例えば、グリーン購入法適合製品の購入など、環境負荷の少ない機材・消耗品を採用する。 また、ライフサイクルを通じた廃棄材の最小化の検討を行う。例えば、拡張の際に既設機材の廃棄が不要で、必要な部材の増設、入れ替えのみで対応可能な機材を採用するなどである。また、ライフサイクルが長い機材ほど廃棄材は少ないと解釈できる。	仕様の対象としない	ベンダーによる提案事項	対処不要	グリーン購入法の基準を満たす製品を一部使用	グリーン購入法の基準を満たす製品のみを使用				・可能な限り満たすこと。