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.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。	○	3	0	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。		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	認証情報のみ暗号化	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）		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。 インターネットに直接接続せず、内部ネットワークのみに接続する情報システムの伝送において、悪意のある攻撃から重要なデータを保護するための対策。	○	2	0	インターネットに直接接続せず、内部ネットワークのみに接続する情報システムを想定。 [−] インターネットに接続していない①を満たす閉域環境における伝送データにおいて、以下の②③双方の条件も満たす場合 ①L2SW/L3SWによる通信経路の限定を行い、かつ、ファイアウォールによる通信プロトコルの限定等を行うことで必要な通信に制限していること。 ②通信ログを取得していること。 ③インシデント管理及び対応を行うこと。	○	仕様の対象としない	ベンダーによる提案事項	無し	一部のデータを暗号化（自治体の判断により暗号化対象とする伝送データを選定する）	すべてのデータを暗号化				【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。
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。	○	3	0	蓄積するデータについては、第三者に漏洩した場合でも、内容の判読ができないようすべてのデータの暗号化を実施する。		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。 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。 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。