共通実施手順別表2・クラウドサービス利用基準

カテゴリー	No.	項目	要件	基準に対応できない場合のリスク	重要性分類S	重要性分類Ⅰ	重要性分類Ⅱ	チェック
コンプライアンス	1	法律について	クラウドサービスの利用にかかる法律関係は、国内法が適用されること	外国法が適用される場合、その国の法令及び規則が適用され、本市が意図せずに、クラウドサービス事業者（SaaS提供者）からその国に情報が提供されてしまう可能性がある。	必須	必須	必須	
	2	管轄裁判所について	本市との契約について紛争が生じた場合には、国内裁判所を管轄裁判所を指定可能であること	裁判を行うこととなった場合、契約で定められた管轄裁判所に出向く必要があるが、管轄裁判所に海外の裁判所を指定される可能性がある。	必須	必須	必須	
アプリケーション／通信	3	暗号化対策	通信経路(*)を適切に暗号化していること (*)SSL、 TLSによるend to end、VPN装置等による拠点間のいずれも可	デジタル庁、総務省及び経済産業省が暗号化方式について評価を行っており、安全性が確認された方式が電子政府推奨暗号リストに記載される。 このリストにない暗号化方式を利用している場合、暗号が解読され情報が漏えいしてしまう可能性がある。	必須	必須	必須	
	4		データを保存するサイバー空間(**)（バックアップ含む）において、CRYPTREC 「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」に記載の電子政府推奨暗号リスト(***)内の暗号化方式を利用していること (**)DBソフト固有の暗号化機能も可 (***)電子政府推奨暗号リストの参照URL https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022.pdf		必須	必須	任意	
	5-1	複数要素認証	SaaS提供者（ITベンダー等の管理者）及びSaaS利用者（本市、委託先または再委託先）が当該SaaSの管理画面にログインを行う際の認証方法は、複数要素認証(*)を提供していること *知識/所持/生体の３要素のうち、2つ以上を使用するもの。 *ワンタイムパスワードも所持認証として、複数要素認証に含める。	複数要素認証に比べて、パスワード認証のみといった単要素認証では、不正にログインされる可能性が高い。	必須	任意 【要件を満たすことを推奨】	任意	
	5-2		SaaS提供者（ITベンダー等の管理者）及びSaaS利用者（本市、委託先または再委託先）が当該SaaSの管理画面にログインを行う際の認証方法は、2段階認証(*)を提供していること (*)ログインする際に、ID/PWによる認証の後、追加で認証を行うもの。		-	No.5-1を満たさない場合は、No.5-2～5-3のいずれかが必須	No.5-1を満たさない場合は、No.5-2～5-3のいずれかが必須	
	5-3		SaaS提供者（ITベンダー等の管理者）及びSaaS利用者（本市、委託先または再委託先）が当該SaaSの管理画面にログインを行う際に、一定回数認証に失敗した場合、アカウントをロックする等の不正アクセス防護措置機能が付いていること		-	No.5-1を満たさない場合は、No.5-2～5-3のいずれかが必須	No.5-1を満たさない場合は、No.5-2～5-3のいずれかが必須	
サーバの設置場所	6-1	サーバ設置場所	日本国内法が適用される場所に立地していること ※データをバックアップする場所も、日本国内法が適用される場所に立地していること	電子データが国外に保存された場合、その国の法令及び規制が適用され、本市が意図せずに、クラウドサービス事業者(SaaS提供者)からその国に情報が提供されてしまう可能性がある。また、個人情報保護法第71条に抵触することとなる。	必須	任意 【要件を満たすことを推奨】	任意	
	6-2		海外サーバに個人情報を含む行政情報が保存されるが、当該個人情報の本人から同意を得ることを予定している（サービス利用時に本人から同意を得る仕様になっていること） ※同意を得る際は、必ず以下の情報をサービス利用者に提供すること （個人情報保護法第71条） ・移転先の所在国の名称 ・当該外国における個人情報の保護に関する制度 ・移転先が講する個人情報の保護のための措置 https://www.ppc.go.jp/all_faq_index/faq2-q5-8/		-	No.6-1を満たさない場合は、No.6-2～6-5のいずれかが必須	No.6-1を満たさない場合は、No.6-2～6-5のいずれかが必須	
	6-3		海外データセンターに個人情報を含む行政情報が保存されるが、日本と同等の個人情報保護法が整備されている国・地域にデータセンターが設置されていること （個人情報保護委員会が、「日本と同等の個人情報保護法が整備されている」と認める国・地域は、EU,英国限定（令和5年12月現在時点））		-	No.6-1を満たさない場合は、No.6-2～6-5のいずれかが必須	No.6-1を満たさない場合は、No.6-2～6-5のいずれかが必須	
	6-4		海外データセンターに行政情報が保存されるが、保存される情報項目が重要性分類Ⅲの項目限定であること ※重要性分類Ⅱ以上の行政情報は、原則として日本国内のデータセンターに保存する。		-	No.6-1を満たさない場合は、No.6-2～6-5のいずれかが必須	No.6-1を満たさない場合は、No.6-2～6-5のいずれかが必須	
	6-5		海外データセンターに行政情報が保存されるが、本市が本市専用の暗号鍵(SaaS利用者ごとに割り当てられた暗号鍵)によって当該データを管理すること（BYOK）(*) (*)BYOKとは：クラウドサービス事業者によって提供される暗号化サービスで使用する鍵の生成を利用者が行い、その鍵をクラウドに持ち込んでデータを暗号化すること (*)なぜ本市専用の暗号鍵であれば海外拠点にデータを置いてもよいのか：本市専用の暗号鍵でデータが暗号化され、鍵が本市自身又は国内DC内で管理されていれば、海外捜査機関等によって海外DC内のデータが国内法に拠らず接収されても、復号できず保護されるため (*)なぜ本市専用の暗号鍵が必要なのか：本市以外の利用者と暗号鍵が共通であると、データ消去に際して本市のデータのみを選択的に消去することが困難であるため		-	No.6-1を満たさない場合は、No.6-2～6-5のいずれかが必須	No.6-1を満たさない場合は、No.6-2～6-5のいずれかが必須	
サービスの品質	7	認証取得	ISMAP、ISMAP-LIU、ISO/IEC 27017又はISO/IEC27018を取得していること ※ IaaS提供者またはPaaS提供者が取得しているかどうか、ではなく、SaaS提供者が取得しているかどうか ※ISO/IEC27001は、クラウドサービス提供事業者の認証に該当しない	クラウドサービス事業者(SaaS提供者)が実施しているセキュリティ対策について第三者による認証が得られていないと、適切なセキュリティ対策となっていない可能性があり、情報漏えい等のインシデントが発生する可能性がある。	必須	任意 【要件を満たすことを推奨】	任意	
データ消去	8-1	データ消去の規格	**契約終了時**において、自社、又はIaaS事業者が実施しているデータ消去がNIST（米国国立標準技術研究所）SP800-88 Rev.1（purge、destroyのどちらか）を満たしていること	契約終了後も個人情報を含む行政情報が削除されず、情報が漏えいしてしまう可能性がある。 または、不適切な消去方法により削除されており、情報が復元されてしまう可能性がある。	※原則必須 No.8-1を満たさない場合は、No.8-2必須	任意 【要件を満たすことを推奨】 No.8-1を満たさない場合は、No.8-2必須	任意 No.8-1を満たさない場合は、No.8-2必須	
	8-2		自社、又はIaaS事業者において、本市が貸与（本市の事業のために市民等が直接入力した情報含む）した行政情報を保存したサーバ等の機器を**廃棄時**に、NIST（米国国立標準技術研究所）SP800-88 Rev.1（purge、destroyのどちらか）を満たしていること ※契約終了時点において、当該サービスの標準機能等によりデータ消去をすることが前提		必須	必須	必須	

※原則、契約終了時に本市基準によるデータ消去を必須としますが、クラウドサービスの仕様により当該要件を満たさない場合は、他セキュリティ要件等を総合的に検討の上、サーバ等の機器廃棄時に本市基準によるデータ消去を実施する仕様でも可とします。

★参考：各重要性分類の例示　※注　あくまでも一例です。業務内容等により必ずしも以下の場合に当てはまらない可能性もございます。

分類	定義	例
重要性分類S	重要性分類Ⅰに分類される行政情報のうち、滅失又はき損した場合、行政の円滑な執行に重大な支障をきたす恐れのある行政情報	特定個人情報、住基・税・障害等の基幹系システムに保存されている機密情報
重要性分類Ⅰ	・仙台市情報公開条例（平成12年仙台市条例第80号）第7条第1号から第4号に定義されている不開示情報。 ・情報システムの運用管理に関する情報で，情報セキュリティを維持するため，機密の取扱いを要する情報。 ・上記に掲げる場合のほか，情報管理者が，情報の機密性，完全性及び可用性その他の事情を考慮して，重要性分類Ⅰとして管理することが適当と認める行政情報。	個人情報（氏名・住所・年齢・性別）、重要な情報システムに係るPWやシステム設定
重要性分類Ⅱ	・仙台市情報公開条例第7条第5号及び第6号に定義されている不開示情報。 ・上記に掲げる場合のほか，情報管理者が，情報の機密性，完全性及び可用性その他の事情を考慮して，重要性分類Ⅱとして管理することが適当と認める行政情報	議事録や予算執行、見積もりの情報等
重要性分類Ⅲ	重要性分類S，Ⅰ及びⅡ以外の行政情報。	HPに公開している情報