（別　紙）

外部サービス要件

区分			要件	要否
1.外部サービス要件				
	1.1.	セキュリティ評価制度	利用しようとする外部サービス（アプリケーション）が政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））への登録が行われており、かつ利用するサービスが言明対象範囲内であること。	任意
	1.2.		1.1でISMAPへの登録が行われていない場合 利用しようとする外部サービス（アプリケーション）が政府情報システムのためのセキュリティ評価制度「ISMAP-LIU」（ISMAP for Low-Impact Use）への登録が行われていること。	任意
	1.3.	SLA	サービスレベルの保証が定められていること。 SLAには以下のような内容が定められていること。 ・情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順及び情報セキュリティインシデントの対応等の取り決め ・外部サービス利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得、保持し、定期的にレビューできること。 ・利用する外部サービス又はシステムの技術的脆弱性に関する情報は、公表された後に速やかにクラウドサービス利用者が入手できるようになっていること。	任意
	1.4.	クラウドサービス情報開示認定制度	利用しようとする外部サービス（アプリケーション）が一般社団法人日本クラウド産業協会(ASPIC)クラウドサービス情報開示認定制度への登録が行われていること。	任意
	1.5.	生成AIを利用したサービスにおける入力情報の取扱	外部サービスが生成AIを利用したサービスに該当する場合においては、同サービスへの入力情報が、本市の許可なく生成AIの学習に用いられたり、サービスを提供する事業者による監査の対象にならないことが確認できること。	必須
	1.1.でISMAPへの登録が行われている場合、1.2.でISMAP-LIUへの登録が行われている場合、または1.4.でASPICへの登録が行われている場合、以下の要件は不要			
	1.6.	資格・認証 ※アプリケーション 提供事業者(ASP)	サービス提供を行う組織(ASP)が、ISO/IEC 27001：2013認証を取得していること。	任意
	1.7.	資格・認証 ※クラウドサービス プロバイダー(CSP)	利用しようとする外部サービス（アプリケーション）が政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））に登録されているサービス上に構築されており、かつ利用するサービスが言明対象範囲内であること。	任意
	1.8.		1.7でISMAPへの登録が行われている場合、1.8～1.13の要件は不要 サーバを提供する組織(CSP)が、ISO/IEC 27001：2013認証を取得していること。	必須
	1.9.		サーバを提供する組織(CSP)が、ISO/IEC 27017：2015認証もしくはPCI DSSを取得していること。もしくはそれに相当する機能や組織体制を有していることが確認できること。	必須
	1.10.		サーバを提供する組織(CSP)が、ISO/IEC 27018：2014認証を取得していること。	任意
	1.11.	データセンター要件	データセンターは、日本データセンター協会が制定するデータセンターファシリティスタンダードのティア3相当の基準を満たした設備とすること。	必須
	1.12.	データの所在・適用法と裁判管轄	サービス上のユーザ所有データ（バックアップデータを含む。）の所在地が日本国内に限定できること。	必須
	1.13.		サービス提供事業の実施場所（事務所、運用場所）（地域（リージョン）が特定できるようにすること）を情報提供すること。提供にあたっては文書にて内容を確約すること。	必須
	1.14.		準拠法、裁判管轄を国内に指定できること。	必須
	1.15.		市が登録したデータは、本市に確実に提供でき、提供後のデータの所有権・管理権は、市が保有すること。また、市が登録したデータは、本契約に明示的に定められているところを除き、本市の承諾なく、利用できないものとすること。	任意
	1.6 と1.7もしくは、1.6と1.10の認証を取得している場合、以下の要件は不要			
	1.16.	セキュリティ対策・体制	サービス提供業務の遂行のために提供する情報（契約等の手続に付随して外部サービス事業者が知りうる利用者情報等）を、サービス提供業務の遂行目的外で利用しないこと。情報の目的外利用の禁止に対する遵守（義務）の表明をすること。	必須
	1.17.		サービス提供を行う組織若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制について提示すること。	必須
	1.18.		情報セキュリティインシデントが発生した場合に、被害を最小限に食い止めるための対処方法（対処手順、責任分界、対処体制等）について提示すること。	必須
	1.19.		障害や情報セキュリティインシデントの発生、監査結果等によって、情報セキュリティ対策の履行が不十分であると認められた場合の対処（改善の実施等）方法について提示すること。	必須
	1.20.	データ暗号化	機密性の高いデータ等については、暗号化等によって蓄積・伝送データを保護できること。	必須
	1.21.	ログ取得	外部サービス上におけるアクセスログ等の証跡に係る保存期間について、1年間以上の保存が可能であること。その手法について提示すること。	必須
	1.22.	脆弱性対策	外部サービス上の脆弱性を発見する方法があり、実施可能であること。その手法について提示すること。	必須
	1.23.	不正アクセス対策	通信内容を監視する等により、不正アクセスや不正侵入を検知及び通知できること。	必須
	1.24.	機器停止	機器に異常があった場合、検知できること。 また、機器を死活監視し、停止した場合、検知できること。	必須
	1.25.	データ取扱い時の権限管理	データの取り扱いについて、権限管理及びアクセス制御ができること。	必須
	1.26.	保守端末	保守端末は、認証管理、持出管理、施錠管理、ログ管理等によりセキュリティを確保していること。	必須
	1.27.	データ消去	データを消去する際は、ISO27001に準拠してデータを復元できないように電子的に完全に消去又は廃棄すること。また、データを消去又は廃棄した証明書を提示すること。 なお、ISO27001にデータ消去が未規定の場合、サービス終了までに規定し、認証を受けること。	必須
	1.28.	セキュリティ監査	情報セキュリティ監査の受入れが行われていること。	任意