外部サービス選定基準

（第6号様式）

○外部サービスを選定する際、下記に示す要求事項を満たすサービスを選定すること。導入・構築、運用・保守、更改・廃棄フェーズ欄の要求事項は実施が確約できることを、選定時に確認すること。
○確認ができればチェック欄にチェックをつけ、外部サービス利用申請書に添付すること。
○ISMAPクラウドサービスリスト（以下、「ISMAP」とする）に登録されているサービスを利用する場合は、外部サービス提供者に対する確認は不要とする。導入事業者がある場合は、導入事業者に対して確認すること。
○ISMAPに登録されていないサービスを利用する場合は、導入事業者・外部サービス提供者ともに対して確認すること。
○実施基準・実施例欄にある数値はあくまでも目安である。利用する情報システムや取り扱う情報、非機能要件の特性に応じて、主管課において適宜数値を変更すること。
○また、本選定基準をSLAとして活用することも可能である。

No	項目	要求事項	実施基準・実施例	必須/推奨				チェック	
				ISMAPに登録されているサービス（ガバメントクラウド、LGWAN-ASPを含む）		ISMAPに登録されていない外部サービス			
				導入事業者	外部サービス提供者	導入事業者	外部サービス提供者	導入事業者	外部サービス提供者
選定基準（全般的な情報セキュリティ要件）									
認証要件									
	公的認証資格	本市が指定する公的認証資格を保有していること または同程度の水準のセキュリティ対策を実施していること	（導入事業者） ・プライバシーマーク ・ISMS/JIS Q 27001 （外部サービス提供者） ・ISMS/JIS Q 27017	必須	-	必須	推奨		
事業者要件									
	事業者体制	本市が指定する資格・実績の保有者が従事していること	・外部サービスに特化した資格及び実績 ・プロジェクトマネージャー ・情報処理安全確保支援士	必須	-	必須	推奨		
		本市からの問い合わせを受け付ける窓口があること	・事業者は、本市からの問い合わせに係る一元的な窓口を設置 ・サポート体制を構築し、体制図を本市に提出	必須	-	必須	推奨		
		本市が指定する時間帯にサポート受け付けを提供できること	平常時：平日午前9時から午後5時まで 緊急時：24時間365日（翌営業日の就業前までに対応）	必須	-	必須	推奨		
		取り扱う情報の目的外利用が禁止されていること	・外部サービス提供を通じて知り得た情報の秘密保持に関する誓約書の提出 ・NDA（秘密保持契約）の締結	必須	-	必須	必須		
		情報セキュリティ対策推進の管理体制が整備されていること	・情報セキュリティ管理体制の提出 ・情報セキュリティインシデントへの対処方法（エスカレーションルート含む）の提示 ・情報セキュリティインシデント発生から〇時間以内に、本市が指定する連絡先への連絡	必須	-	必須	必須		
		本市の情報資産に対して意図しない変更が加えられないための方策や管理体制が整備されていること	・事業者による本市の情報資産に対して意図しない変更が加えられないための方策の提示 ・その方策の管理体制の提出	必須	-	必須	必須		
		外部サービスの提供が事業者の経営状況により中断しないこと	事業者の資本関係・役員等の情報の提示	必須	-	必須	必須		
		契約の履行状況を確認できること	情報セキュリティ対策その他の契約の履行状況の確認方法の整備・提示	必須	-	必須	必須		
		情報セキュリティ対策の履行が不十分な場合に改善できること	情報セキュリティ対策の履行が不十分な場合の対処方法の整備・提示	必須	-	必須	必須		
		SLA保証が契約内容に含まれること		必須	-	必須	必須		
		本市対策基準を遵守すること		必須	-	必須	-		
	再委託	事業者からの再委託が発生する場合、本市の選定条件で求める条件を再委託事業者にも求められること	・再委託事業者への情報セキュリティ対策の担保 ・再委託事業者の情報セキュリティ対策の確認状況を本市に報告	必須	-	必須	必須		
	事業者環境	必要最小限の従事者のみが執務室や保守環境に入室できること	・ICカードや生体認証で運用従事者以外の入室を制限 ・入退室のデータを管理していること	必須	-	必須	必須		
		その他設備が整っていること	・有人監視 ・友連れ防止扉 ・フロア全体が網羅的に監視できるカメラの設置	必須	-	必須	必須		
セキュリティ要件									
	通信	取り扱う情報の重要性に応じて、通信経路の暗号化が適切に実施できていること	・端末とサーバ間の通信は、SSL（TLS）を利用 ・通信回線は、VPNを利用 ・本市向けのサービスは、本市が指定するIPアドレスからの通信のみを許可	必須	-	必須	必須		
	監査	第三者機関のセキュリティ監査を実施していること	・年1回以上の監査実施 ・事業者は、監査後、本市に監査結果を提出	必須	-	必須	必須		
データ要件									
	所有権	データの所有権は本市が保有できること	・契約書にデータの所有権は本市が保有と明記	必須	-	必須	必須		
データセンター要件									
	建物	気象災害等に耐えられる構造であること	・耐震構造または免震構造 ・震度７以下に耐えうる構造	-	-	-	必須		
	非常用電源設備	停電時に電気を配給できる無停電電源装置・自家発電装置が設置されていること	設置 （24時間365日の無瞬電無停電） バッテリーが尽きていないか確認できていること	-	-	-	必須		
	設置場所	本市のデータが該当国の準拠法・裁判管轄により、情報開示や差し押さえがされない国でデータセンターが所在していること	・日本国内 ・準拠法・裁判管轄に基づいても情報開示や差し押さえがない国・地域	-	-	-	必須		
その他要件									
	情報開示請求	本市が指定する情報を開示できること	・平常時のリソース状況 ・インシデント発生時に係る各種ログの提供 ・インシデント原因調査のための環境設定の開示	-	-	-	必須		
導入・構築時の要件									
セキュリティ要件									
	アクセス制御	不正なアクセスを防止するためにアクセス制御が実施されていること	・管理画面に対する接続元IPアドレスの制限 ・ID認証含めた多要素認証	必須	-	必須	必須		
	暗号化	取り扱う情報が暗号化して保存されること	・外部サービス内での暗号化 ・外部サービスへの通信経路上での暗号化 ・CRYPTREC暗号リスト搭載の暗号強度の遵守	必須	-	必須	必須		
	開発時	開発時のセキュリティを保つための開発手順等が整備されていること	開発時のセキュリティを保つための開発手順等の提示	必須	-	必須	必須		
		調達するソフトウェアのライセンスが規定違反しないこと	他ベンダが提供するソフトウェア等を導入する場合のライセンス管理方針の提示	必須	-	必須	-		
	設計・設定	設定の誤りを見出すための対策が整備されていること	・設定の誤りを見出すための対策の提示 ・テスト結果報告書の提出	必須	-	必須	必須		

		取り扱う情報の重要性に応じて、冗長化が構成されていること	・冗長化の構成 ・障害発生時から〇分以内のサービス再開	必須	-	必須	必須		
		正確に時刻同期がされていること	時刻同期の方法の提示	必須	-	必須	必須		
		構築・開発した環境・プログラムに脆弱性が残存していないこと	・脆弱性診断の実施 ・診断結果に基づく脆弱性解消のための対策の実施 ・脆弱性が解消されたことを示す報告書の提出	必須	-	必須	必須		
運用・保守時の要件									
運用要件									
	提供時間	本市が指定する時間帯にサービスを提供できること	計画停止を除き、平日（土日及び祝日、12月29日から1月3日を除く）の午前8時から午後8時まで	必須	-	必須	必須		
	計画停止	定期点検など、計画的なサービス停止の手順が定められていること	・事業者は30日前までに本市の許可を得る ・原則、平日の午後8時以降もしくは土日に実施 ・計画停止の際は、サービスのトップ画面に掲載	必須	-	必須	必須		
	稼働率	本市が指定する稼働率を維持できること ※稼働率：（提供時間-（停止時間-（計画停止時間＋本市起因の停止時間））） ÷提供時間	・99.5%以上 ・事業者は毎月5日までに、本市が指定する連絡先に前月分の稼働率を報告	必須	-	必須	必須		
	改修方針	プログラムの欠陥に対応すること	事業者は、欠陥の発見後、1時間以内に本市が指定する連絡先に一報し、翌日までに対応を無償で実施	必須	-	必須	必須		
		法律改正に対応すること	事業者は、全ての法律改正に係る改修を適切な期限までに無償で実施	推奨	-	推奨	推奨		
		利用者の要望に対応すること	事業者は、本市を含む全ての利用者の要望のうち、乙が決定したものを年2回無償で実施	推奨	-	推奨	推奨		
	障害監視	本市が指定する間隔で、機器・ネットワーク・サービスの性能・障害を監視でき、異常時に連絡できること	・5分ごとに実施 ・事業者は、以上を検知した場合は、15分以内に、本市が指定した連絡先に連絡	必須	-	必須	必須		
	障害復旧	本市が指定する時間で、障害発生から復旧完了できること	・原則、1時間以内 ・事業者は、障害復旧後3日以内に障害に係る報告書を本市に提出	必須	-	必須	必須		
	応答時間	本市が指定する時間で、端末から操作して応答できること	・平常時：3秒以内 ・ピーク時：5秒以内	必須	-	必須	必須		
	バッチ処理	本市が指定する時間で、バッチ処理が完了できること	4時間以内	必須	-	必須	必須		
	同時接続利用者数	本市が指定する利用者数が、同時に利用できること	500ユーザ	必須	-	必須	必須		
	サービス終了告知	本市が指定する期限までにサービス終了案内を本市に連絡できること	・前年度の5月まで ・事業者は、事前告知後、サービスのトップ画面に掲載	必須	-	必須	必須		
	サービス変更告知	本市が指定する期限までにサービス変更案内を本市に連絡できること	・変更の3か月前 ・事業者は、事前告知後、サービスのトップ画面に掲載	必須	-	必須	必須		
	コールバック時間	問い合わせに即答できなかった場合の連絡期限	1時間以内	必須	-	必須	必須		
	問題解決時間	問い合わせを受けてから問題解決までの時間	1営業日以内	必須	-	必須	必須		
セキュリティ要件									
	ウイルス対策	サーバのウイルス対策を実施できていること	・ウイルス対策ソフトのリアルタイムスキャンを有効化しておくこと ・ウイルス定義ファイルを以下の間隔で最新化すること 　配信後、緊急性を要するもの：2時間以内 　それ以外：24時間以内 ・ウイルススキャンを1週間に1回実施すること	必須	-	必須	必須		
	セキュリティパッチ適用	OS、ソフトウェアのセキュリティパッチを速やかに適用できること	緊急性を要するもの：24時間以内 それ以外：7日以内	必須	-	必須	必須		
	ログ管理	アクセスログ・操作ログ・エラーログが取得・保存できること	・利用者ごとの記録（アクセスログ・操作ログ・エラーログ） ・利用者ごとの利用記録をサービス管理画面から閲覧 ・利用者ごとの利用記録は、1年間以上保存 ・ログは改ざん防止措置が実施されていること	必須	-	必須	必須		
	データ分離	利用者間で適切にデータが分離され、他の利用者に本市のデータが漏えいしないこと	・本市専用のエリア（リージョン）の設置 ・暗号化キーの適切な配置	必須	-	必須	必須		
	バックアップ	バックアップデータを取得し、保存できること	・毎週金曜日の午後11時にフルバックアップを行い、1年間保存 ・毎日午後11時（金曜日は除く）に差分バックアップを行い、2週間保存 ・暗号化の上保存 ・随時ネットワーク経由で別のデータセンターに保存	必須	-	必須	必須		
	データ復旧	復旧までの期間	・平常時の障害に起因する場合：1日以内 ・想定外の大災害などに起因する場合：2週間以内	必須	-	必須	必須		
	データ出力	本市職員が速やかに全データを出力できること	サービスの管理画面からCSVで出力	推奨	-	推奨	推奨		
	アクセス制御	不正なアクセスを防止するためにアクセス制御が実施されていること	・権限付与の操作履歴の確実な記録 ・不正アクセスを監視できること 　もしくは防止する装置（ファイアウォール、リバースプロキシ、IDS・IPS、WAFなど）が導入されていること	必須	-	必須	必須		
	暗号化	取り扱う情報が暗号化して保存されること	・暗号化に用いる鍵の管理者と鍵の保管場所の整備 ・鍵管理手順と鍵の種類お情報の要求とリスク評価の整備 ・鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価の整備	必須	-	必須	必須		

	通信制御	利用している他のネットワークと分離されていること	利用する外部ネットワークのネットワーク基盤が他のネットワークと分離されていることの確認	必須	-	必須	必須		
	設計・設定	設定の誤りを見出すための対策が整備されていること	・設定の誤りを見出すための対策の提示	必須	-	必須	必須		
	事業継続	外部サービスを利用して事業継続できること	・バックアップの実施および遠隔地保管	必須	-	必須	必須		
更改・廃棄時の要件									
	データ廃棄	本市に関する電子データ・媒体・書類すべてを廃棄できること	・物理的破壊もしくは暗号化キーの廃棄 ・事業者が責任をもって、事業者環境から廃棄 ・廃棄後、証明書を本市に提出	必須	-	必須	必須		
	アカウント廃棄	利用者アカウントをすべて廃棄できること		必須	-	必須	必須		
		管理者アカウントを削除・返却できること		必須	-	必須	必須		