（別紙１）

外部サービス選定基準

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	当局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	当局が指定する資格・実績の保有者が従事していること	・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		
		当局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、当局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、体制図を当局に提出	必須	-	必須	推奨		
		当局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	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24時間以内に、当局が指定する連絡先への連絡	必須	-	必須	必須		
		当局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	・事業者による当局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		
		当局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、当局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当局に報告	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	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、当局に監査結果を提出	必須	-	必須	必須		
データ要件									
	所有権	データの所有権は当局が保有できること	契約書にデータの所有権は当局が保有と明記	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	当局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	当局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	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	SSLによる通信経路の暗号化	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整備が確認できること	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	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	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報告すること	必須	-	必須	必須		
更改・廃棄時の要件									
	データ廃棄	当局に関する電子データ・媒体・書類すべてを廃棄できること	事業者が責任をもって、事業者環境から廃棄	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		