**外部サービス（クラウドサービス）事前確認事項**

外部サービス（クラウドサービス）におけるセキュリティ対策及びセキュリティ管理体制として以下の項目に回答するとともに必要資料を提出してください。

(1)データセンターの場所（国内かどうか）※重要情報取り扱う場合は日本国内が前提となります。

(2)【重要情報取り扱う場合】不正なアクセスを防止するために、ユーザー管理、閲覧制限、アクセス制御を実装しているかどうか

(3)クラウドサービス上に保管したデータのバックアップの取得方法、保管方法（遠隔地、別筐体等）、取得期間（同期、日次等）等

(4) 【クラウドサービスを別のサービス（PaaS）上に構築している場合※】利用しているPaaSサービス名（AWS、Azure等）

※この場合も豊中市との契約に基づき、提供するクラウドサービス全体の管理責任を負っていただく必要があります。PaaSサービスの管理範囲に帰する問題が発生した場合は、御社とPaaS事業者の契約に基づき、対処してください。

(5)クラウドサービスのセキュリティ対策として以下を実施しているか

・データセンターの災害対策や侵入対策を実施しているか

・仮想サーバなどのホスト側のOSやソフト、アプリの脆弱性の判定と対策を実施しているか

(6)通信が暗号化されているか（SSL通信を行っているか）

(7)IPアドレスの制限が可能か、利用者側で証明書のインストールが必要か

(8)国や他自治体での導入実績

(9)【LGWAN-ASP登録サービスの場合】LGWAN-AS登録番号、通信量、接続要件の有無

(10)【重要情報を取り扱う場合】約款での利用が不可のため、秘密保持契約、インシデント報告義務、損害賠償、サービスレベルを保証させるためのSLA項目を含んだ契約の締結が可能か

(11)【重要情報を取り扱う場合】管理体制を確認するために以下①～⑤のいずれかの資料の提出を提出すること

① ISMS 認証を受けていることが確認できるもの（事業者HPの掲載情報でも可）、

② ISMAPの管理基準を満たすことの確認ができる資料の提出、

③ ISMAPクラウドサービスリストへの登録が確認できること（ISMAPクラウドサービスリストの掲載情報でも可）、

④ 日本セキュリティ監査協会のSOC報告書

⑤ 上記の監査報告書や認証等の提出ができない場合は、サービス提供者及び当該サービスの信頼性が十分であることを総合的に判断するために下記すべての書類の提出を提出すること。なお、提出書類を総合的に審査し、公募要件を満たさないと判断する場合もあります。

a. 経営が安定していることを確認するための貸対照表

b. サービスを提供する基盤環境やアプリケーションに係るセキュリティ対策が適切に整備され、運用されていることを確認するために、内部で実施したセキュリティ監査や自己点検の実施状況、セキュリティ研修の実施状況の提出（いずれも実施日・実施概要等）

c. 外部サービスの開発及び運用において、本市の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていることを確認するために品質保証体制の組織体制図

d. 外部サービスに本市の意図しない変更が行われるなどの不正が見つかったときに、原因を調査・排除できる体制を整備していることを確認するため、セキュリティ管理体制の組織体制図

e. 【資本関係に海外を含む場合】資本関係・役員情報がわかる資料