仕様書添付資料　「情報セキュリティ対策表」

【Ⅰ　インフラ関係】

1　情報セキュリティに関して、以下の評価・認証を取得しているか

（1）ISMAP（政府情報システムのためのセキュリティ評価制度）

（2）ISO/IEC27017（クラウドサービスに関する情報セキュリティ管理策のガイドライン規格）

（3）JASA クラウドセキュリティ推進協議会 CS ゴールドマーク（クラウド情報セキュリティ管理基準）

（4）ISO22301（事業継続マネジメントシステム（BCMS）に関する国際規格）

2　日本国の法律及び締結された条約が適用される国内データセンターにおいてデータが管理され、日本国に裁判管轄権があるクラウドサービスであるか。

3　運用終了時のデータ消去方法が取り扱う情報に即した仕様になっているか。

重要度１または２に該当する情報を保存する記憶媒体については、庁舎内において情報の復元が困難な状態までデータの消去を行う。なお、抹消措置にあたっては原則として当該措置に職員が立会うとともに、書面による確認を行う。

委託事業者等は、下記のうちいずれかの方法でデータの抹消措置を実施する。

① 物理的な方法による破壊

② 磁気的な方法による破壊

③ ＯＳ等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去

④ 暗号化消去

4　不正なアクセスを防止するためのアクセス制御（ファイアウォール・IPS（不正侵入防止システム）・Web Application Firewall 等）を実施しているか。

5　DDOS 攻撃等のサービス妨害攻撃を防止（緩和）するため、CDN（コンテンツ配信ネットワーク）等を設置しているか。

6　情報の盗聴等を防ぐため、通信の暗号化対策を講じているか。

【Ⅱ　ソフトウェア関係】

1　情報処理推進機構（IPA）の「安全なウェブサイトの作り方　改訂第７版」に準拠した設計・構築が見込まれているか。

2　県庁 LAN のウイルス対策ソフトを利用するか。利用しない場合は調達製品に含まれているか。

3　取り扱う情報の機密性保護のため、サーバ内の情報を暗号化しているか。

4　「pref.saitama.lg.jp」のサブドメインを利用するか。新規にドメインを取得する場合、運用終了後のドメイン廃止費用を見込んでいるか。

【Ⅲ　運用関係】

1　ソフトウェア（OS・ミドルウェア・アプリケーション）の脆弱性対策(セキュリティパッチ適用等)の実施が仕様に含まれているか。

2　セキュリティ製品（ウイルス対策ソフトウェア等）がインシデントを検知した際の対応及び費用が含まれているか。

3　保存するログの種類を仕様に明記しているか。

4　ログの保存期間を設定しているか(1 年以上)。

5　ログを定期的に確認する運用となっているか。

【Ⅳ　アカウント管理】

1　特権によるネットワーク及び情報システムへの接続時間について、タイムアウトを設定して必要最小限に制限できるか。

2　特権を付与された ID 及びパスワードの変更を職員が実施できるか（委託事業者に行わせてはならない。）。

3　特権を付与された ID 及びパスワードは、職員端末等のパスワードよりも入力回数制限等のセキュリティ機能が強化されているか(職員端末のパスワードは 10 文字以上で英字及び数字、記号が必須。)。

4　特権を付与された ID を初期設定以外のものに変更できるか。

【Ⅴ　情報セキュリティ検査】

1　開発時の第三者による脆弱性診断の費用が含まれているか。また、運用時における脆弱

性診断の費用が見込まれているか。

【VI　生成 AI 利用時の対策】

1　生成 AI の入出力内容を生成 AI の学習に利用されないこと。

2　入出力内容が LLM サーバに保存されないこと。

3　受託者によるサーバの利用データへのアクセスが制限されていること。

4　SSL 通信等による安全な接続を行うこと。

5　日本国の法律及び締結された条約が適用される国内データセンターにおいてデータが保存され、日本国に裁判管轄権があること。