セキュリティ要件

【情報セキュリティポリシー】
想定される脅威を整理し、契約後に示す「三重県電子情報安全対策基準（情報セキュリティポリシー）」に従った対策ができること。
【前提】
・ISMAP（政府情報システムのためのセキュリティ評価制度）クラウドサービスリストに登録されたクラウドを利用するか以下のア~シの条件を満たすクラウドを利用すること。 ア　本業務で取り扱う情報資産を目的外利用しないこと。 イ　本業務で利用するサーバ・ストレージ、情報セキュリティ対策機器等の情報システムが設置されている建物（以下データセンターという）は、地震・水害・火災への対策を行っていること。 ウ　本業務で利用するデータセンターは、日本の法令が適応されること。また、管轄裁判所に関しては、日本国内の裁判所を合意管轄裁判所とできること。 エ　情報セキュリティや個人情報保護に係る第三者認証等のレポートにより、その管理水準が適正と認められていること。 オ　本業務に用いるアプリケーション、サーバ、ストレージ、情報セキュリティ対策機器、通信機器の死活監視・障害監視について監視を行っていること。 カ　本業務に用いるアプリケーション、サーバ、ストレージ、情報セキュリティ対策機器、通信機器についての技術的脆弱性に関する情報を収集し、適宜対策を行っていること。 キ　不要なサービスを停止すること。また、利用する通信プロトコル、ポートは必要最小限とし、利用していない通信プロトコル、ポートはファイアウォール等にて遮断すること。 ク　不正なアクセス等を検知・防御するためのIPSを導入すること。 ケ　サービス仕様の変更やサービス終了等について、対応策を検討する期間を確保するため、それらを行う場合は事前に通知を行うこと。 コ　サービスの稼働率や、サポート・問い合わせ窓口等に関して明示すること。 サ　情報セキュリティに関する窓口を設置し、情報セキュリティインシデントが発生した際、三重県への報告、 収束に向けた対応等にかかる実施体制を確立すること。 シ　本業務を行う上で利用上問題となる免責事項等がないこと。
【通信の暗号化】
すべてのページ要求に対して、TLS1.2以上を使用し、SHA-2(256）以上のSSLサーバ証明書を使用すること。
【アクセスログの管理】
・アクセス記録及び作業内容等の記録を保存すること。なお、アクセス記録にはログイン成功だけでなくログイン失敗の記録も行うこと。
・ログの内容をチェックし、異常が見受けられる場合は直ちに委託者に報告すること。
【アカウントの管理】
・パスワードの有効期限、最小文字数、必要文字種別の設定ができること。
・ユーザーの操作履歴を保存し、誰がいつ何を登録・編集等したか、初心者でも簡単に該当箇所を確認できること。
・一定時間操作がないユーザIDに対して自動でログオフを行うこと。また、自動ログオフまでの時間の設定ができること。
・システム利用端末を紛失または盗難等で第三者が使用する可能性が生じた場合など、該当する IDを停止することで、第三者のログインを防止できること。
【データベースの暗号化】
・保存されるデータは全て暗号化を行うこと。
【OS、ソフトウェア、アプリケーションにおける脆弱性の判定と対策】
・ソフトウェア等に対するセキュリティパッチの適用やバージョンアップを適切に行うこと。
・ウイルスに感染しないよう厳格なウィルス対策を行うこと。
【監視体制】
・クラウドの監視を行い、異常を検知できる体制を整えること。
・情報セキュリティ侵害が発生した場合には、直ちに職員へ報告し、受託者の責任及び負担において、情報セキュリティ侵害の内容及び影響範囲を調査の上、当該情報セキュリティ侵害への対応策を実施すること。
【データ消去】
・保存したデータについて契約終了時に適切に消去すること。なお、暗号化したデータの暗号鍵を無効化することでもデータ消去措置と見なす。