

クラウドサービス利用におけるセキュリティ要件

【導入・構築時の対策】

1 認証情報
提案するクラウドサービス(SaaS)について、第三者機関による保証が確認できること。 (例: ISMAP(又はISMAP-LIU)への登録、ISMS(ISO/IEC 27001)認証、プライバシーマーク) ただし、事業者がサービスを自社以外のクラウド基盤(PaaSもしくはIaaS)上で提供する場合は、当該PaaS/IaaS(利用する基盤サービス)についても第三者機関による保証が確認できること。 なお、ISMAP(又はISMAP-LIU)に登録されていない場合は、ISMS(ISO/IEC 27001)認証、プライバシーマーク、又は第三者による監査報告書・認証等により本要件と同等以上のセキュリティ水準を満たすことを示す資料を提出すること。
2 ユーザIDの管理
ユーザIDやパスワードなどの認証情報の割り当てや変更、削除がクラウドサービス提供者側で実施される場合、その管理手順等が関係法令、第三者認証、受託者の内部規程等に基づき、適切に整備・運用されていること。
3 管理者特権を有する利用者の認証
インターネットから直接管理権限を要する操作が可能となることを考慮し、不正な管理者権限利用の防止(※)が可能なこと。 ※多要素認証方式が可能な場合は実施する、不可能な場合は運用上の工夫を実施すること
4 パスワードの管理機能
パスワードの管理機能について、以下の設定が可能な機能を備えていること。 ・英大文字、英小文字、記号及び数字を含める制限 ・前回使用したパスワードを利用できないように制御 ・パスワードを暗号化した状態で保存 クラウドサービス側で機能が用意されていない場合は、代替するための運用を定めること。
5 保存する情報や機能に対するアクセス制御
クラウドサービスに保存される情報やクラウドサービスの機能ごとに、アクセス権限のない職員がアクセスできないように制限できる仕組みがあること。
6 ネットワークアクセス制限
本システムへのアクセスは、初期稼働段階において庁内LAN(自治体情報セキュリティクラウド経由)からのみ許可する。受託者はIPアドレスによるアクセス制御機能を実装し、区が指定するグローバルIPアドレス(約8アドレス)以外からのアクセスを拒否する設定を行うことができること。 なお、対象IPアドレスの追加・変更・削除については、ノーコードで設定することが可能であること。
7 多大な影響を与える操作の特定と誤操作の抑制
データベースの中身を強制的に書き換える等の多大な影響を与える操作や機能がある場合、実行可能なユーザまたは権限が制限できること。
8 仮想マシンに対する適切なセキュリティ対策の実施
仮想マシン(ソフトウェアによって仮想的に再現された物理的なコンピュータと同等の機能を有するコンピュータ)を設定する際に不正プログラム対策(必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策、ログ取得等の実施)を確実に実施できること。 SaaSを利用する場合は、これらの対応が、クラウドサービス提供事業者側でされること。
9 庁内ネットワークを経由しないクラウドサービスの利用
多要素認証方式やデバイス認証による接続端末制限等の対策をすること。
10 通信経路全般における暗号化
情報資産の保存場所及びクラウドサービス利用における通信経路において、暗号化等の機密性保護が行われていること。
11 法令や規則に対する暗号化方式の遵守
当該クラウドサービスの暗号における一連の管理策が、法令、規制及び関連する協定を遵守していること。
12 設定誤り対策
①クラウドサービス提供者による設定実施や、設定内容のレビュー等により、適切な設定を行い、設定誤りを防止することが可能であること。
②設定権限を与えるクラウドサービス利用者を限定できること。
③導入・構築時のプロセスに設定誤り防止を考慮したセキュリティ対策が組み込まれていること。
13 セキュリティ要件の異なるネットワーク間の通信の監視
クラウドサービス上のネットワークにセキュリティ要件が異なるネットワークを接続する場合、これらの間の通信(トラフィック)を監視または制御していること。なお、設定は定期的な見直しを行うこと。
14 データ容量や稼働性能の監視と将来予測
①利用実績に応じて自動的にリソースを増減させるサービスである場合、リソース不足によるサービス停止とならないよう適切に監視が行われること。 クラウドサービス提供者側で監視のためのサービスが用意されていない場合は、手動で定期的に確認する。
②リソースの利用状況の将来予測を行い設計を行うこと。
【運用・保守時の対策】
15 責任分界点を意識したクラウドサービスの利用

クラウドサービス利用におけるセキュリティ要件

クラウドサービス利用における責任分界点が明確であること。
16 脆弱性対策
クラウドサービス提供者が実施する脆弱性対応の範囲が明確であり、対応及び報告が迅速に行われること。
17 リソース設定を変更するユーティリティプログラムの利用制限
クラウドサービスのリソース(ネットワーク、仮想マシン等)の設定を変更するユーティリティプログラムが存在する場合、利用者を制限できること。
18 不正利用の監視
①クラウドサービスへの不正利用を検知することが可能な監視機能を有していること。 クラウドサービス側で機能が用意されていない場合は、代替するための運用を定めること。
②クラウドサービス上におけるアクセスログ等の証跡が保存され、確認できること。
19 国内法の適用
クラウドサービスの利用を通じて取り扱うデータは国内のデータセンターに保存され、国内法の適用範囲であること。
20 暗号化に用いる鍵の管理
データの暗号化や復号化を行う際に用いる符号である暗号鍵(以下、「暗号鍵」とする。)の保管場所は国内のサーバであること。
21 暗号化に用いる鍵のリスク評価
暗号鍵をクラウドサービス提供者が保管する場合、暗号鍵が窃取される可能性や安全性が低下した技術等の利用等がなく、安全に管理・利用可能なこと。
22 他のネットワークとの分離
クラウドサービス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。
23 バックアップの確実な実施
不測の事態に対してサービスの復旧を行うため、当該業務に適した頻度や範囲でのバックアップが可能であること。
24 復旧に係る手順の策定と定期的な訓練の実施
当該業務で必要となる可用性を担保するためにバックアップからの復旧が可能であること。また、定期的に訓練を実施することが可能であること。
25 データ容量、性能等の監視
利用するクラウドサービスで使用済みのデータ容量やサービスの性能について監視を行い、想定された容量・性能内で運用していることを確認できること。

【更改・廃棄時の対策】

26 移行・終了計画
クラウドサービスの移行、または、終了時の対応について、業務に与える影響を鑑みて期間や移行方法について検討すること。
27 情報の廃棄方法
①以下を例とする取り扱った全ての情報が、クラウドサービス基盤上から確実に削除可能なこと。なお、削除する対象はバックアップ等により複製されたものも含む。 ・クラウドサービスに保存された情報 ・仮想リソース(仮想マシン、仮想ストレージ、仮想ネットワーク機器など) ・ファイル(ストレージサービスに格納したファイル、各サービスのログ、開発関連ファイル、設定ファイルなど) ・暗号鍵 ・ドメイン情報
②暗号化された情報がある場合、確実な廃棄が行われること。
③廃棄の実施報告書が提出可能なこと。 ただし、提出が不可能な場合は、理由を確認して個別判断を行う。
28 基盤となる物理機器の廃棄
クラウドサービスの基盤となる装置等の処分についてセキュリティを確保した対応が行われること。 当該確認にあたっては、クラウドサービス提供事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用する。
29 管理者権限を有するアカウントの削除・返却と再利用の確認
区利用環境におけるクラウドサービス管理者アカウントは再利用されないこと。
30 特殊なアカウントの削除と関連情報の廃棄
特殊なアカウント(ストレージアカウントなど)を作成した場合は、サービス利用終了時に確実に削除できること。また、特殊なアカウントを利用して作成された情報についても確実に廃棄されること。
31 AIのセキュリティ要件
・顧客が入力したデータ(ファイル、プロンプト)および生成された結果は、基盤モデル(OpenAI等)の再学習に一切利用されないこと。 ・AIに対するプロンプトの実行履歴はユーザー単位で隔離されること。 ・AIへの攻撃に対する防御策を講じていること。 ・利用者の権限に応じて、AIからアクセス可能な情報(ユーザー情報、規約等のファイル)を制御可能なこと。