クラウドサービス調達仕様

1(1) 預託データの取扱いに関する規程等において，目的外の利用を禁じていること。
(2) 利用者の個人情報をサービス提供以外の目的で利用していないこと。
(3) 預託データの利用に当たっては，約款や規約等により利用目的を全て明記していること。
(4) 預託データをサービス提供以外の目的で利用していないこと。
(5) 情報資産の取扱いに関する規程等が定められており，適切に管理していること。
(6) サービス利用終了時におけるデータの取扱いを定めていること。
(7) 利用者の求めに応じた預託データや利用者が作成したデータ等の取扱いについて定めていること。
(8) 情報資産を消去又は廃棄する際の取扱いに関する規程等を定めていること。
(9) 外部記憶媒体の管理方法（保管や廃棄方法等）に関する規程等を定めており，これら規程等を遵守していること。
(10) やむを得ず外部記憶媒体を利用する場合は，一定のセキュリティ対策を講じていること。
(11) 持ち運び可能な外部記憶媒体の利用を禁じる設定又は規程等を定めていること。

2(1) 情報資産の暗号化方針やルールを定めていること。
(2) サービス提供者が当該サービスに対して通信する際は，暗号化などのセキュリティ対策を講じていること。
(3) 外部サービスやツールを利用する場合，セキュリティ水準を確認していること。
(4) 意図しない変更や不正利用に対する対策を講じていること。
(5) サービスの開発・保守・運用の各フェーズにおいて，機能要件やセキュリティ要件を確認していること。
(6) 外部及び内部からの不正アクセスを防止するためにファイア

ウォールを設置していること。
(7) 不正なパケットを自動的に発見又は遮断するための仕組みを導入している（又は導入予定である）こと。
(8) 各サーバの用途に応じた論理的分離により境界を保護する仕組みを設けていること。
(9) 暗号化するためのキーやパスワードにアクセスできる人を限定していること。
(10) サービスの開発・保守・運用の各フェーズにおいて、データの漏えいを防止する対策を実施していること。
3 (1) クラウドサービスの開発や保守，運用において，アクセス制御の方針やルールを定めていること。
(2) クラウドサービスの開発や保守，運用において，特権アカウントによるアクセスを記録し，適切な利用であることを監視していること。
(3) サービス提供事業者のアクセス制御について，適切な認証方式により実施していること。
(4) 他サービスと連携する機能がある場合，サービス利用者の管理者権限で該当機能の使用可否の設定変更ができないこと。
(5) サービス利用者のアクセス制御を複数の仕組みを用いて実施していること。
(6) サーバへのリモートアクセスを制限していること。
(7) 従業員やシステム管理者が預託データへアクセスした場合の操作ログを監視していること。
(8) 組織内のアカウントのログイン履歴や操作ログを確認できること。
(9) 組織内のアカウントを削除又は利用停止できること。
(10) 従業員に対する情報セキュリティ及び重要情報の取扱いに関して定期的に教育を実施していること。
(11) 従業員及び契約相手との契約が終了又は変更となった場合，アクセス権の変更や削除，貸与資産の返却等を実施していること。
(12) クラウドサービスの開発や保守，運用において，不要アカウントの適切な管理を実施していること。

(13) アクセスログは複数取得し，一定の期間において保存されていること。

4 (1) サービスのリリース作業は，特定の従業員のみが実施できること。
(2) サービスの内容を変更する場合は，事前にテストし，変更後の影響や不具合がないことを確認していること。
(3) アプリケーションを変更する場合，事前に本番環境と同等の開発環境でテスト等のリリース手順の確認を実施していること。
(4) サービスのインフラやネットワークを変更する場合は，事前に非機能要件をテストし，変更後の影響や不具合がないことを確認していること。

5 (1) サービス提供に係る脆弱性を管理し，状況に応じて適宜対処していること。
(2) 脆弱性診断やペネトレーションテストを実施していること。
(3) 使用するソフトウェア等のパッチ更新やアップデートを適宜実施していること。
(4) Webアプリケーションの脆弱性を悪用した攻撃等を防止するための仕組みを導入している（又は導入予定である）こと。

6 (1) 外部委託先が預託データを取り扱う場合には，セキュリティ水準や情報の取扱方法等に関する定めについて確認し，合意されていること。
(2) 外部委託先の選定や管理について，方針や基準等を定めていること。
(3) 外部委託先に対してセキュリティ対策やインシデント発生時の対応，関連法令の遵守，情報の消去などの要求事項について定めていること。
(4) 外部委託先との合意内容が正しく履行されていることを定期的に確認し評価していること。

7 (1) セキュリティインシデントやシステム障害を複数の視点で監視し，検知する仕組みを設けていること。
(2) セキュリティインシデントやシステム障害が発生した場合の役割分担や責任が明確になっていること。
(3) セキュリティインシデントやシステム障害が発生した場合の体制や手順が確立されていること。
(4) 過去の事例等を参考としたセキュリティインシデント対応の改善につなげていることが望ましい。
(5) 直近２年間で対外的に向けた公表又は監督省庁や認証機関等への報告に相当するセキュリティインシデントが発生していないこと。ただし，発生していた場合には，契約締結前にインシデント内容及び対応状況を確認する。
(6) 地震や火災等の災害又は大規模なシステム障害に備えたリカバリ計画やコンティンジェンシープランを策定していること。
(7) 地震や火災等の災害又は大規模なシステム障害に備えたシステム構成となっていること。
(8) データセンターの入退室管理や自然災害への対策等，物理的なセキュリティ対策を確認していること。
(9) 自然災害やセキュリティインシデントへの対策として，可用性を高める対策を実施していること。

8 (1) サービスレベルや責任範囲に関して，稼働目標や目標復旧時間などの定めを複数以上設けていること。
(2) クラウドサービスのデータやアプリケーション，環境構成情報などのバックアップを取得していること。
(3) バックアップが正しく取得できており，適切に復旧できることを確認していること。

9 (1) 関連法令や規制，契約上の要求事項を満たす取組を継続的に実施していること。
(2) 定期的な監査を実施していること。
(3) 契約や規約等において日本法に準拠していること。
(4) 個人情報の保護に関する法律（平成１５年法律第５７号）に

対応していること。

(5) 情報セキュリティ又は個人情報保護に関する第三者認証や評価を取得していること。

(6) 預託データを他国に保管していないこと。ただし，他国に保管されていても日本の法令の範囲内で運用できる場合には差し支えない。

１０(1) クラウドサービスの時刻を同期させていること。

(2) サービスが何らかの事情で利用できない場合には，利用者に対して通知できること。