別紙１－５

仕様書別紙４

クラウドサービスの利用に関する特記事項

（クラウド基盤）

第１条　発注者との契約については、日本国の法令に準拠するものでなければならない。また、契約に係る訴訟については、発注者の事務所の所在地を管轄する日本国の裁判所を専属的管轄裁判所とする。

第２条　データセンタの設置場所は、日本の法令の範囲内で運用できる場所でなければならない。

第３条　サービス内容を発注者に共有し、サービスにおいて発注者が管理する範囲と受注者が管理する範囲について発注者と確認しなければならない。

第４条　受注者が原因で発注者が損害を受けた場合は、受注者がその損害を賠償しなければならない。

第５条　受注者の責任範囲における事件または事故の発生時の対応に関する情報（以下の事項等）を発注者に提出しなければならない。

・システム障害時の連絡手段、連絡先、連絡を受け付ける時間帯等
・システム障害の原因究明と恒久対策を行う為の体制や対応時間帯
・システム障害で被害を受けたシステム、サービスの復旧を行うための体制や対応時間帯

第６条　事業者やサービス利用者（または障害を自動検知する仕組み）からの障害報告等を通じて、障害範囲の特定をしなければならない。

第７条　受注者への問い合わせ先（氏名、メールアドレス、電話番号）を発注者に提出しなければならない。

第８条　受託した事務に係る各種情報資産を受託した事務以外の用途で利用してはならない、また第三者に提供又は譲渡してはならない。契約満了後又は契約解除後も同様とする。

第９条　提供サービスに関するアクセスログについて、保存期間やアクセスログの参照及び提供方法を発注者に提出しなければならない。

第１０条　区と合意した内容でアクセス制御（例：グローバル IP アドレスによるアクセス制御等）を実施しなければならない。

第１１条　サービス終了に伴いクラウド内に保存したデータを消去する際は、対象のデータを復元不可能になるようにし、対応結果を区に報告しなければならない。

第１２条　ID・パスワードは第三者から推測困難となるよう設定・管理しなければならない。

第１３条　端末やサービスにおけるアクセス制御機能について、多要素認証、もしくは同等の代替措置を実装しなければならない。

仕様書別紙４

第１４条　以下の暗号化機能及び仕組みを実装しなければならない。
・データ暗号化に利用した暗号化鍵を管理する仕組み
・サービス内で保管する情報資産の暗号化
・区が利用する環境とクラウドサービスの間の通信経路の暗号化　※危殆化していない暗号化通信プロトコルを利用すること
・（複数システムが連携する場合）システム間の通信経路の暗号化

第１５条　受注者が責任対象となる障害について以下の要件を満たさなければならない。
・事業者側で障害を検知する機能があること
・障害時の障害検知、原因追及、復旧作業における対応ルートを発注者に提供できること
・障害時の連絡先等（担当者の氏名、電話番号、メールアドレス）となる連絡ルートを発注者に提供できること

第１６条　受注者は、提供するサービスを変更する際には、事前協議を実施しなければならない。

第１７条　事前に発注者と協議して定めたサービスレベルの保証・サービス提供の前提条件・保証対象となるサービスの内容や責任範囲・サービスの品質基準（利用時間・停止時間等の定量的な数値）・取り決めを守れなかった場合に課せられるペナルティを遵守しなければならない。

第１８条　障害の発生時は、事前に協議した発注者の連絡先に連絡し、発注者と連携して再発防止策を講じる為の支援をしなければならない。

以下の条文はリモート保守(※)について適用する。

※リモート保守とは、クラウド上の業務システムを受注者の保守拠点から保守することを指す。

第１９条　以下２０条～２９条に係るセキュリティ対策が問題なく実施されていることを区が監査可能でなければならない。発注者による監査ができない場合は、理由を発注者に書面で提出しなければならない。

第２０条　ユーザアカウントについて、以下観点での制御を実施しなければならない。
・アカウント数が適正量であること
・定期的にアカウントの棚卸を実施すること
・異常なログインを検出する仕組みがあること

第２１条　作業場所のセキュリティ対策として、以下と同等の対策を実施しなければならない。
・社内業務の作業場所とは分離した保守・運用エリアにて作業を実施すること
・保守・運用エリアもしくは受注者オフィスビルに入退出時、IC カード等を用いた認証が実施されること

仕様書別紙４

第２２条　事業者のリモート保守専用端末のアクセス制御について、多要素認証、もしくは同等の代替措置を実装しなければならない。
第２３条　受注者は、リモート保守時に利用する端末について、以下と同等の対策を実施しなければならない。
・ウイルス対策ソフトやエンドポイントセキュリティを導入すること
・のぞき見防止フィルムの使用等の策を講じること
第２４条　入退室や操作のログの取得及び定期的なバックアップ管理をしなければならない。
第２５条　受注者は、データの管理に関して、以下の事項を遵守しなければならない。
・原則データの持ち出しは禁止すること
・やむを得ず、データを持ち出しする必要がある場合は、必要となる手続きを実施の上、持ち出しすること
第２６条　インバウンド・アウトバウンド共に必要最小限のアクセスのみ許可するよう制御可能でなければならない。
第２７条　IDS 等による異常アクティビティの監視をしなければならない。
第２８条　保守事業者の利用環境とクラウドサービスの間の通信を暗号化しなければならない。
第２９条　通信のログの取得及び定期的なバックアップ管理をしなければならない。