別紙３

データセンタ要件

１　認証取得

システムを利用するデータセンタは、国内に所在地を置き、国内法の適用を受け、ファシリティ条件は以下の項目を満たすこと。また、日本データセンタ協会（ＪＤＣＣ）制定の「データセンタファシリティスタンダード」における「ティア３」相当のサービスレベルを有し、クラウドセキュリティ（ＣＳ）ゴールドマーク取得をしていること。

２　セキュリティ対策

(1) データセンタへの入退管理は、セキュリティ管理システム等により、２４時間３６５日実施されていること。

(2) サーバ室等への入退室を管理・記憶するため、バイオメトリクス認証システム等の本人認証を実施していること。

(3) 入退室者が記憶媒体（メモリカード、メモリスティック等）を不正に所持し、持出持込することができない体制であること。

(4) 複数の監視カメラを設置し、撮影された映像を一定期間保存すること。監視カメラの設置に当たっては、死角のないように設置されていること。

(5) サーバ室への出入口には十分な強度を持つ防火扉等を設置し、破壊等による不正侵入が防止されていること。

(6) サーバ室は外部から内部を見通せない窓なしとする等の対策を講じられていること。

(7) 警備員を常駐させていること。

３　災害対策について

(1) 停電や電力障害が生じた場合に電源を確保するための対策が講じられていること。

(2) 受電設備は法定点検時も完全無停止であること。

(3) 無停電電源装置（ＵＰＳ）や定電圧定周波数装置（ＣＶＣＦ）、自家発電装置を備えていること。また、発電設備使用中

も燃料補給継続運転を可能とし、完全無停止であること。

(4) ２系統以上の給電経路・方式にて電源の引き込みを図り、施設内は二重化等の冗長性を確保していること。

(5) 火災報知機・通報システム及び消火設備が設置されていること。加えて、消火設備による汚損の対策が講じられていること。また、避雷、静電気からの防護のための対策が講じられていること。

(6) 地震・水害に対する対策が講じられており、地震リスクに対する安全性の確保として、ＰＭＬによる評価の場合１０～２０％未満であること。

(7) 震度６相当以上に耐えうる耐震構造であること。

4　通信について

(1) ネットワークは、不正アクセスなどのセキュリティインシデント予防の観点から、暗号化及びＶＰＮなどを用いた独立した閉域網とすること。侵入検知（ＩＤＳ）を導入するなど、安定運用のための対策が取られていること。

(2) データセンタ側の回線は、ＬＧＷＡＮ－ＡＳＰアプリケーションが快適に稼働する帯域を確保すること。

5　運用について

(1) ２４時間３６５日体制で稼動するオペレーターによる常駐監視（機器監視、ウイルス検知等）を行うこと。

(2) 障害発生時早急にサービス復旧に向けた対応をすること。

6　バックアップについて

(1) システムを構築する仮想サーバ内のデータベースについては、同一データセンタ内にバックアップ用の仮想サーバを用意し、日次バックアップを７世代（１週間分）以上実施すること。さらに、遠隔地のデータセンタにて同一のバックアップデータを保持し、冗長化をはかること。

7　その他

(1) ＪＩＰＤＥＣやＪＱＡ等で認定している情報処理管理に関する公的認証（ＩＳＭＳ、プライバシーマーク等）が取得されていること。

(2) クライアントパソコンのＯＳのバージョンアップ等に対応できること。
(3) その他必要な関連機器については、過不足なく選定すること。
(4) システム入れ替えの際に、容易に新規に導入しうるシステムにインポートするためのデータエクスポートが行えること。