（別紙）セキュリティ要件

1　本業務で取り扱う情報資産を目的外利用しないこと。
2　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・火災への対策が行われていること。
3　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。
4　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。
5　本システムの死活監視や障害監視を行うこと。
6　本システム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、通信機器等についての技術的脆弱性に関する情報を収集し、適宜対策を行うこと。
7　情報の盗聴・改ざん等から保護するため通信の暗号化を行うこと。
8　保存するデータは暗号化すること。
9　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。
10　アクセス記録が保存されていること。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。
11　データの消失対策として、定期的にバックアップをとり、復旧することが可能なこと。
12　保存されるデータについてサービス利用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。
13　情報セキュリティや障害に関する窓口を設置し、情報セキュリティインシデントや障害が発生した際、報告や収束に向けた対応等にかかる実施体制を確立すること。
14　本システムに関する全ての機器に対し、最新の情報をもとにウイルス対策やセキュリティパッチの適用を実施すること。
15　本システムに関する全ての機器に対し、ウイルス等の攻撃や不正侵入、個人情報を含む内部情報の流出への対策等を万全に行うこと。
16　本システムを運用するサーバは冗長化すること。また、障害が発生した場合は待機サーバに切り替わり、滞りなく運用が進められること。
17　本システムでアプリを用いる場合、サポート期間中の iOS 及び Android OS を搭載したスマートフォン等の端末で動作すること。また、各 OS のメジャー

アップデートに対応すること。

18　本システムでアプリを用いる場合、iOS 端末向けアプリケーションは「AppStore」、Android 端末向けアプリケーションは「GooglePlay」への登録申請、配信までの一切の手続きを行うこと。また、登録後の維持管理を行うこと。