別紙2

#	区分	事項	詳細定義
1	環境	保守環境	本番環境・ステージング環境を必須とし、大規模の改修が入る場合には、結合環境も作成できるようにしておくこと。
2	サービスレベル	システム運用時間	原則、24時間365日。ただし、不定期メンテナンス時間を除く。
3		不定期メンテナンス時間	財団と協議の上、必要に応じて不定期メンテナンス日時を決定する。 ・メンテナンス中はその旨がわかる画面を表示させること。
4		問合せ電話・メール受信	・受託者は財団からのエスカレーションを受付けた場合、インシデント対応を実施し、その結果を財団へ報告する。 ・受託者は受託者管理の管理台帳に起票し、対応ステータスを管理する。
5		アラートメール対応	・受託者は、24時間365日でアラートメールの検知を行う。 ・受託者はアラート検知後速やかに一次切り分け、初動調査、ワークアラウンド（*1）、有識者へのエスカレーション（メール&電話）を実施する。 ・受託者は調査結果を事象、原因、影響、暫定対応、本対応について財団へ報告する。 ・受託者は受託者管理の管理台帳に起票し、対応ステータスを管理する。 （*1）ワークアラウンド 策定・実施は受託者にて行う。また、ワークアラウンド手順については、財団が承認したもののみ適応すること。 標準化され、財団承認を得たワークアラウンドは、受託者にて実施する。
6		対応担当者による初期対応	システム状況確認、ログ確認等を行い既知のインシデントに対してはワークアラウンドと、必要に応じたエスカレーションを行う。
7		インシデントの管理	・受託者は受託者管理の管理台帳にてインシデントの管理を行うこととし、インシデントの検知からクローズ迄の管理活動が、適切に実施されるようにコントロールを行う。 ・受託者は受託者管理の管理台帳にてワークアラウンド対応手順を明記し、実施前後で財団へ報告を行う ・ワークアラウンド手順については、財団が承認したもののみ適応すること。
8		AI・蓄積データの取り扱い	・AIが学習した情報は、財団および別事業者へ移管する際に継続的に利用できるようにすること。 ・引継ぎの情報としての蓄積データ等は、財団および別事業者へ移管する際に継続的に利用できるようにすること。
9		定例会の開催	・受託者は定期的（毎月1回以上）に定例会議等を実施し、月次報告書の主要事項について報告すること。 ・受託者は本システムの稼働状況の調査分析等の報告を、1年に1回以上報告する。調査・分析結果に基づき、必要に応じて、改善計画を立案し、財団と協議の上、対策を実施する。
10	保守課題・要望	リリース履歴管理	ソースコード、設定パラメータのバージョン管理を行い、リリースバックが起きないようにすること。
11		リリース判定会	受託者の提示するテスト結果報告書を元に、財団にてリリース判定を実施する。
12	保守	瑕疵対応の決定方法について	システム運用開始後に発生した不具合の中で、瑕疵対応かどうか判断するまでの調査・確認対応費用については、最終的な不具合の原因に基づいて、財団と協議の上決定する。
13	セキュリティ	ネットワークセキュリティ	外部とのネットワーク境界にファイアウォールを設置し、不正アクセスを防止する。
14		アカウント管理	・パスワードは最低8文字以上とし、英語大文字(A-Z),英語小文字(a-z),数字(0,9),記号(!,#,&等)の3種以上を混在させ、固有名詞を使用しない等、容易に推測されないものを採用する。 ・自己のIDおよびパスワードを他人に開示または使用させ、もしくは他人のIDおよびパスワードを使用してはならない。 ・OS、DB、アプリの各アカウント管理、およびその他のパスワード管理は、アカウント設定後関係者に配布。配布後は受領者がセキュリティポリシーを遵守し運用を行う。
15		本番環境へのアクセス管理	システムへのリモートアクセスには、以下の要件を満たす必要がある。 ・本システムの運用保守へ携わるスタッフであること。 ・保守端末にはウイルスチェックソフトをインストールすること。またインターネットセキュリティ監視ソフトもインストールすることが望ましい。 ・踏み台サーバ及び保守端末では、操作証跡を記録する。 ・退職等により、本システムの運用保守業務から離れるスタッフのアカウントは速やかに削除する。 ・本番環境とステージング環境の操作環境誤認を防止するため、社内規定を徹底する。
16		運用作業におけるセキュリティ管理	・作業者はトラブル対応やサーバ管理目的により権限アカウントでの操作を行う場合を除き、権限アカウントでの操作を禁止する。 ・作業者は事前に承認したネットワーク経路、アクセス手法、アクセスツール以外では、いかなる手法を用いてもシステムおよびサーバへアクセスを行ってはならない。 ・個人情報及び営業秘密の含まれるデータが保存された記憶媒体について元請管理者の事前承諾（顧客から委託されたデータについては顧客の事前承諾）を得ることなく、第三者に利用又は提供してはならない。 ・機密情報と個人情報の授受については、管理台帳を作成し、授受および返却した日付、担当者、情報の内容、手段・方法を記録し管理なければならない。 ・システム上の一切のデータの移動・変更・複製・消去についても管理者の事前承諾を得ることなく実施してはならない。 ・作業者はコンソール操作にてサーバへのログオンを行い、作業終了時は必ずログアウトを行う。
17		データ管理	システムの運用に関わる全てのデータは、以下のポリシーで情報管理し、外部への漏洩を防止する ・ 運用関連の紙媒体文書は、施錠可能なキャビネットに保存する ・ 電子ファイルは運用関連スタッフのみへアクセス権を付与したファイルサーバへ保存する ・ 不要になった文書はシュレッダーにより断裁処分する ・ 許可なく受託者のオフィス外への持ち出しは禁止する ・ 社外とのメールではメール添付ファイルに読取パスワードを設定してデータ漏洩を予防する ・ 外部へのデータ持ち出し可能な媒体（CD-RやDVD-R、USBメモリ等）の利用制限をかけ、許可された場合のみ利用許可する ・個人情報のやり取りに関しては、サーバ等で管理を行う。
18		システムの管理	・受託者は、本システムのアプリケーションが正常に稼働しているかを稼働監視する。また、アプリケーションの不具合のログ情報を適宜監視する。 ・サーバーのCPU使用率等は最適な状態を保てるように選定し、運用保守の監視業務として財団と協議した閾値を超過する場合は、適宜容量の見直しを提案すること
19		機器及びソフトウェア等の維持管理	受託者は、本システム対象部分の安定稼働及び機能向上に向けて、機器、ソフトウェア、ネットワーク、データ等の維持管理に係る作業を行う。
20		セキィリティーホール、その他セキュリティ上の問題発生時の対応	開発したソフトウェアのセキュリティ・ホールや、その他セキュリティ上の問題（別紙「サイバーセキュリティ基本方針」の第三条に該当する問題）が発生した場合は、報告書を提出し、速やかな原因の究明、被害の拡散防止、再発防止策の検討を行う。
21		セキュリティ実施手順書の作成	上記、セキュリティ対応に関する手順を簡易的にまとめた書面を作成し、財団へ提出すること。
22	性能・拡張性	性能の目標値	通常業務時の情報の表示について、通信環境が最適な場合の処理速度は、ユーザーからのアクセスに対するレスポンスタイムを５秒以内の目標とすること。