「Manageクラウド」サービス品質保証／SLA 第 7 版

2021年03月08日 改定

本サービス品質保証／SLAは、経済産業省がガイドラインとして公表する「クラウドサービスレベルチェックリスト」に基づき策定しております。
ManageACクラウド、ManageOZO3クラウド、ManageOZO3クラウドプラス 各サービスの品質保証となります。

No.	種別	サービスレベル項目		測定単位	サービス保証内容
アプリケーション運用					
1	可用性	サービス時間	サービスを提供する時間帯（設備やネットワーク等の点検／保守のための計画停止時間の記述を含む）	時間帯	24時間365日(計画停止を除く)
2		計画停止予定通知	定期的な保守停止に関する事前連絡確認（事前通知のタイミング／方法の記述を含む）	有無	有： 7日前までにメール/HPにて通知
3		サービス提供終了時の事前通知	サービス提供を終了する場合の事前連絡確認（事前通知のタイミング／方法の記述を含む）	有無	有： 3ヵ月前までにメール/HPにて通知
4		突然のサービス提供終了に対する対処	プログラムの預託等の措置の有無	有無	無：
5		サービス稼働率	サービスを利用できる確率（（計画サービス時間－停止時間）÷計画サービス時間）	稼働率 (%)	99.9%を目標に運用。 (定期メンテナンス、計画停止を除く)
6		ディザスタリカバリ	災害発生時のシステム復旧／ サポート体制	有無	有： 災害時のハードウェア復旧は、西日本リージョンにて24時間後 稼働できる環境としてColdStandby環境を用意
7		重大障害時の代替手段	早期復旧が不可能な場合の代替措置	有無	有： 重大障害時においてはバックアップ規定に基づいて保管されたデータを基に別環境にシステム構築可能。 別途有償。
8		代替措置で提供するデータ形式	代替措置で提供されるデータ形式の定義を記述	有無 (ファイル形式)	無
9		アップグレード方針	バージョンアップ／ 変更管理／パッチ管理の方針	有無	有： 3ヵ月ごとの定期バージョンアップを実施予定。 バージョンアップ内容はHPにて通知。
10	信頼性	平均復旧時間(RTO)	障害発生から修理完了までの平均時間（修理時間の和÷故障回数）	時間帯	営業時間内の場合、1時間以内
11		障害発生件数	1年間に発生した障害件数／1年間に発生した対応に長時間（1日以上）要した障害件数	回	2回
12		システム監視基準	システム監視基準（監視内容／監視・通知基準）の設定に基づく監視	有無	有： システム正常稼働を24時間365日で監視、障害発生時は弊社サポートスタッフに報告メールを発信。 <監視内容> ・内部機能のよるアプリケーションプール状態監視 ・内部機能のよるColdFusion(Application Server)状態監視 ・外部サービスによる接続状況監視
13		障害通知プロセス	障害発生時の連絡プロセス（通知先／方法／経路）	有無	有： システム障害時、弊社サポートスタッフにメール送信。 ①システム責任者が障害種別、緊急度、ユーザ様への影響度を判断 ⇒復旧対応 ②サポートスタッフがメール・HPにて障害状況を通知。
14		障害通知時間	異常検出後に指定された連絡先に通知するまでの時間	時間	15分以内： 障害発生時に、システム内障害監視機能又は、外部サービスの接続状況監視機能により、15分以内に当社サポートチームにメール通知。メール通知後、サポート責任者により障害内容、重要度を鑑みて担当を設定して対応。
15		障害監視間隔	障害インシデントを収集／集計する時間間隔	時間(分)	5分以内
16		サービス提供状況の報告方法/間隔	サービス提供状況を報告する方法／時間間隔	時間(分)	随時 サービス提供状況はHPにて公開します。
17		ログの取得	利用者に提供可能なログの種類（ アクセスログ、操作ログ、エラーログ等）	有無	有： エラーログ、処理単位のトレースログ、アクセスログを取得
18	性能	応答時間	処理の応答時間	時間(秒)	平均3秒以内（データセンター内） ※集計/出力系処理は平均30秒以内
19		遅延	処理の応答時間の遅延継続時間	時間(分)	2時間以内 データセンター内の応答時間が想定値以上となる遅延の継続時間が2時間以内。
20		バッチ処理時間	バッチ処理（一括処理）の応答時間	時間(分)	4時間以内
21	拡張性	カスタマイズ性	カスタマイズ（変更）が可能な事項／範囲／仕様等の条件とカスタマイズに必要な情報	有無	無： 「システム基盤」+「アプリケーション群」で構成しているが、 別途有償にてアプリケーション単位で機能改修を伴うオプション(「OZO3 クラウドプラス」)をご用意。
22		外部接続性	既存システムや他のクラウド・コンピューティング・サービス等の外部のシステムとの接続仕様（API、開発言語等）	有無	有： csv形式でのデータエクスポート機能（エクスポート項目に制限あり）による連携が可能。 クラウドデータ連携サービス「ManageLink」利用による他システムとの連携が可能 OBC社奉行シリーズのクラウド環境構築サービス「ManageERP」による連携が可能
23		同時接続利用者数	オンラインの利用者が同時に接続してサービスを利用可能なユーザ数	有無 (制約条件)	ベストエフォート型
24		提供リソースの上限	ディスク容量の上限／ ページビューの上限	処理能力	1ユーザあたり、3GB の容量制限あり（追加容量購入可能）
サポート					
25	サポート	サービス提供時間帯(障害対応)	障害対応時の問合せ受付業務を実施する時間帯	時間帯	平日9：00-17：30 電話、メール、Webフォーム にて受付
26		サービス提供時間帯(一般問合せ)	一般問合せ時の問合せ受付業務を実施する時間帯	時間帯	平日9：00-17：30 電話、メール、Webフォーム にて受付

データ管理					
27	データ管理	バックアップの方法	バックアップ内容（回数、復旧方法など）、データ保管場所／ 形式、利用者のデータへのアクセス権など、利用者に所有権のあるデータの取扱方法	有無／内容	有 一日一回データベースバックアップ及び添付ファイルのバックアップを実施。 バックアップデータへのアクセスは、サポートチームメンバのみ許可。
28		バックアップデータを取得するタイミング(RPO)	バックアップデータをとり、データを保証する時点	時間	AM 02:00 ～ 04:00時点のデータを保証
29		バックアップデータの保存期間	データをバックアップした媒体を保管する期限	時間	3日
30		データ消去の要件	サービス解約後の、データ消去の実施有無／タイミング、保管媒体の破棄の実施有無／タイミング、およびデータ移行など、利用者に所有権のあるデータの消去方法	有無	解約日の翌日から30日後に全データを削除します。
31		バックアップ世代数	保証する世代数	世代数	3世代
32		データ保護のための暗号化要件	データを保護するにあたり、暗号化要件の有無	有無	有
33		マルチテナントストレージにおけるキー管理要件	マルチテナントストレージのキー管理要件の有無、内容	有無／内容	有： データ及びデータベースはテナント毎に分離して管理しています。 （ストレージキー自体はアプリケーションサーバーにて一括管理しています。）
34		データ漏洩・破壊時の補償／保険	データ漏洩・破壊時の補償／保険の有無	有無	利用規約の範囲で補償
35		解約時のデータポータビリティ	解約時、元データが完全な形で迅速に返却される、もしくは責任を持ってデータを消去する体制を整えており、外部への漏洩の懸念のない状態が構築できていること	有無／内容	有： 解約日から30日後に、全データの削除を行います。 (データ削除までの間の利用者登録データは利用規約の秘密保持義務に準拠するものとして取り扱います) 登録データの返却は行いませんが、基本情報(ユーザ情報、役職情報、グループ情報まで)は、解約前にユーザー操作によりcsvファイルとして出力可能です。 それ以外の登録データの抽出を希望される場合は、「データ抽出サービス(別途有償)」にて対応します。
36		預託データの整合性検証作業	データの整合性を検証する手法が実装され、検証報告の確認作業が行われていること	有無	無
37		入力データ形式の制限機能	入力データ形式の制限機能の有無	有無	有： 入力項目ごとに整合性チェックを実施。 整合性チェック抵触の場合、アラートメッセージを表示。
セキュリティ					
38	セキュリティ	公的認証取得の要件	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	有無	有： ISMS(ISO/IEC 27001)並びに、ISMSクラウドセキュリティ認証(ISO/IEC 27017)を取得しています。
39		アプリケーションに関する第三者評価	不正な侵入、操作、データ取得等への対策について、第三者の客観的な評価を得ていること	有無／実施状況	無
40		情報取扱い環境	提供者側でのデータ取扱環境が適切に確保されていること	有無	有： 実データ及び運用環境へのアクセス制限を行い、サポートスタッフのみの限定を行っています。
41		通信の暗号化レベル	システムとやりとりされる通信の暗号化強度	有無	有： TLS1.2以上にてデータを暗号化しています。
42		システム監査への資料提供	システム監査時に、担当者へ以下の資料を提供する旨明示「SAS70認定の取得有無」「18号監査報告書の提示可否」	有無	無：
43		マルチテナント下でのセキュリティ対策	異なる利用企業間の情報隔離、障害等の影響の局所化	有無	有： テナント毎にデータベースを分離、利用会社以外のデータの閲覧は不可。
44		情報取扱者の制限	利用者のデータにアクセスできる利用者が限定されていること、利用者組織にて規定しているアクセス制限と同様な制約が実現できていること	有無／設定状況	有： 実データ及び運用環境へのアクセス制限を行い、サポートスタッフのみの限定を行っています。
45		セキュリティインシデント発生時のトレーサビリティ	IDの付与単位、IDをログ検索に利用できるか否か	設定状況	IDは一社員：一IDとして、利用者様のシステム管理担当者が付与します。 IDにより、セキュリティインシデント発生時のアクセス履歴を検索可能です。
46		ウィルススキャン	ウィルススキャンの頻度	頻度	有： 以下日程にてウィルススキャンを実施。 ①システム更新等のファイルアップデート時 ②週次(夜間メンテナンス時)
47		二次記憶媒体の安全性対策	バックアップメディア等では、常に暗号化した状態で保管している。廃棄の際にはデータの完全な抹消を実施し、また検証していること、USBポートを無効化しデータの吸い出しの制限等の対策を講じていること	有無	有： 利用者の登録データはクラウドサーバーのみに保存。 クラウドサーバー(登録データ含む)へのアクセス制限(サポートスタッフ限定)の運用をしております。