No.	種別	サービスレベル項目例	規定内容	測定単位	z
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/定期保守を除く）
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	定期保守のためのダウンタイムはない
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	営業担当（Key Account Manager）はライセンスの契約終了期間４週間前に通知を行う
4		突然のサービス提供停止に対する対処	プログラムの預託等の措置の有無	有無	プログラム預託はない
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（%）	99.80%
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	遠隔地のバックアップデータセンターに毎日バックアップデータを保存、復旧時間4時間（月～金、ドイツ時間）
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	個別のソリューションについては、各々の営業担当（Key Account Manager）にお問い合わせください
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）	.docx、*.mp4
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	年1回のアップグレード、または必要に応じて実施
10	信頼性	平均復旧時間(MTTR)	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	4時間以内（基幹業務） 48時間以内（上記以外）
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	１回以内（基幹業務） １回以内（上記以外）
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	監視は行なっている
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	契約書に記載された通知プロセス、もしくは標準手順に沿って、プラットフォーム内のメッセージツールで通知
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	5分以内（基幹業務） 8時間以内（上記以外）
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）	1分以内（基幹業務） 120分（上記以外）
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	年刊にて公開
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	個別に定義する
18	性能	応答時間	処理の応答時間	時間（秒）	データセンタ内の平均応答時間3秒以内
19		遅延	処理の応答時間の遅延継続時間	時間（分）	1分以内
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）	2分以内
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	利用画面上の項目配置変更や新規項目の追加が設定画面より可能
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	APIはありません
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）	制限はありません
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	制限はありません
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	月～金 9時～18時（UTC +8）、2時間以内
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	月～金 9時～18時（UTC +8）、もしくは キーアカウントマネージャー経由の受付（電話・メール）
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	バックアップは、今後の情報量に応じて保存されます（数分から数時間 サービスにより異なります）。遠隔地のデータセンターに保存されます。 アクセス権はシステム管理者のみに制限される。復元方法、ユーザーへの開示方法は別途定める。
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	上記参照
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	30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	削除依頼は、承認/有効性をチェックされ、直ちに実行されます。また、ユーザーはいつでも自分のデータを削除することができます。
31		バックアップ世代数	保証する世代数	世代数	30日
32	データ管理	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
34		データ漏えい・破壊時の補償／保険	データ漏えい・破壊時の補償／保険の有無	有無	有
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、外部への漏えいの懸念のない状態が構築できていること	有無／内容	有、テキストか*.mp4形式
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
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	TISAX、SOC2
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	有、ネットワーク侵入テスト
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
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	AES
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	利用可能な侵入テストの管理概要
43	セキュリティ	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	SSOが利用可能
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 （ユーザーのデータにアクセスできる従業員等は、セキュリティ管理者が許可した者に限る）
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、ログの保存期間は適切な期間が確保されており、利用者の必要に応じて、受容可能に期間内に提供されるか	設定状況	権限に沿ったID管理が行われていること（1人1ID発行）
46		ウイルススキャン	ウイルススキャンの頻度	頻度	日次
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こと、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	・権限者のみアクセス可 ・廃棄時には、データを完全に抹消する ・暗号化、認証機能を用いる

改訂版号	改定日付	改定内容
2	2023/12/04	・No. 3 誤字の修正 ・No. 3「キーアカウントマネージャー」の表現変更 ・No. 8「キーアカウントマネージャー」の表現変更
1	2023/5/30	初版発行