No.	種別	サービスレベル項目	規定内容	測定単位	設定
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 遅くとも1週間前にWebページに掲載
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 おおよそ3ヶ月前を目安にWebページに掲載
4		突然のサービス提供停止に対する対処	プログラムや、システム環境の各種設定データ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 (%)	非公開（99.9%以上を目標）
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	有無	有 複数のデータセンターによる冗長構成にて運用
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	無
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 ダウンタイムが発生しないアップデートは、予告なく随時実施 ダウンタイムが発生するアップデートは、遅くとも1週間前にWebページに掲載して計画的に実施
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	非公開
11		目標復旧時間(RTO)	障害発生後のサービス提供の再開に関して設定された目標時間	時間	非公開
12		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	回数は非公開 障害情報はWebページに掲載
13		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 ネットワーク/ハードウェア/ソフトフェアの死活監視およびパフォーマンス監視、システムエラー監視を実施
14		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 軽微な障害においては、Webページに掲載 ユーザに重大な影響を与える障害においては、Webページに掲載および利用ユーザにメール連絡
15		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	72時間以内を目標
16		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分間隔
17		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	必要に応じてWebページに掲載
18		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 BOT実行ログ（コンソールから閲覧可能） コンソールへのアクセスログ（要求に応じて部分的に開示可能）
19	性能	応答時間	処理の応答時間	時間 (秒)	非公開
20		遅延	処理の応答時間の遅延継続時間	時間 (分)	非公開
21		バッチ処理時間	バッチ処理(一括処理)の応答時間	時間 (分)	非公開
22	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	有 自動化処理（BOT）を作成可能
23		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 APIを公開 外部iPaaSサービスとの連携機能を提供 kintoneとの連携プラグインを提供
24		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)	無 制限無し
25		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	契約プランによる ・ディスク容量 ・月間BOT実行可能時間 ・同時BOT実行可能数 ・月間トランザクション量 作成可能なBOT数は無制限
サポート					
26	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	メールにて常に受付（回答は3営業日以内）
27		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	メールにて常に受付（回答は3営業日以内）
データ管理					
28	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 日次でユーザデータをバックアップ（一部のデータは随時バックアップ） バックアップデータへのアクセスは一部の開発者のみに制限
29		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	AM3:00(JST)までにバックアップ完了 （一部のデータは随時バックアップ）
30		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	10日間
31		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	有 サービス解約後、11日以内にユーザデータを削除
32		バックアップ世代数	保証する世代数	世代数	10日間
33		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 データは暗号化して保管
34		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 契約毎のユニークIDによりデータを論理的に分離
35		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	無
36		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 サービス解約後、11日以内にユーザデータを削除
37		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	有 アプリケーションによる入力値の検証 TLS暗号化による改ざん防止
38		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 アプリケーションによる入力値の検証 WAFによる入力値のセキュリティ検証
セキュリティ					
39	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(ISO27001)を取得 ISMSクラウドセキュリティ認証(ISO27017)を取得 プライバシーマークを取得
40		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
41		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 データへのアクセスは業務上必要な一部のオペレータ・開発者のみに制限
42		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 RSA-2048 (SHA256)
43		会計監査報告書における情報セキュリティ関連事項の確認	会計監査報告書における情報セ キュリティ関連事項の監査時に、担当者へ以下の資料を提供する旨 「最新のSAS70Type2監査報告書」「最新の18号監査報告書」	有無	無
44		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 契約毎のユニークIDによりデータを論理的に分離
45		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 契約内においてユーザロールを設定可能
46		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	契約毎・ユーザ毎にIDを付与 アクセスログ(個人情報は含まない)は1年間保管し、契約ID・ユーザIDによる検索が可能。要求に応じて部分的に開示可能
47		ウイルススキャン	ウイルススキャンの頻度	頻度	開発・運用に利用するPCはセキュリティソフトによるリアルタイムスキャンを常時有効
48		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	有 二次記録媒体の使用は原則禁止
49		データの外部保存方針	データ保存地の各種法制度の下におけるデータ取扱い及び利用に関する制約条件を把握しているか	把握状況	データはAWS東京リージョンに保管 制約条件を把握している