コラボフロークラウド　サービスレベルチェックリスト （「クラウドサービスレベルのチェックリスト」（経済産業省）に準拠しています。）　　平成29年7月7日

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
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日としています。（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日前までにメールおよびホームページにて通知します。
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ヶ月前までにメールおよびホームページにて通知します。
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 現在預託等の措置は行っておりません。
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%以上の稼働率です。
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 ハードウェアはAmazon AWS東京リージョンのデータセンター障害対策に準じます。サービスサポートは名古屋事業所を主とし、東京および大阪事業所でフォロー体制あり。
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 現状用意しておりません。
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 軽微な機能追加・改善は1日～2週間単位で実施しています。機能追加などユーザに影響のある修正などについては、ホームページにて通知します。影響度が高い場合には、メールでの通知も行います。
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	1時間以内。
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	3時間以内。
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	0回
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 システム稼働状況を24時間365日で監視し、負荷率・各使用量およびクラウド外から正常アクセスチェックを実施しています。
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 障害発生時に弊社のクラウド運用グループに障害通知メールを送信により全体周知が行われ、その後、障害の種類に応じて担当者がアサインされます。
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	30分以内。 ただし、障害復旧の開始時期が翌営業日になる場合あり。
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
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	随時 障害等が発生した場合、弊社ホームページもしくは、メールにて確認可能です。
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	無 利用者にてログ閲覧・取得できるものは現在用意されていません。
19	性能	応答時間	処理の応答時間	時間（秒）	平均応答時間は3秒以内。（データセンタ内において）
20		遅延	処理の応答時間の遅延継続時間	時間（分）	2時間以内 データセンタ内の応答時間が3秒以上となる遅延の継続時間が2時間以内
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）	1分以内 一日1回深夜にバッチ処理を実施
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	有無	無 申請書において、承認ボタン名の変更、メール文言の変更などは、設定で変更可能。
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 弊社が用意しているモジュールによってのみ、用意している外部システム（限定されます）と連携可能。現在、API等は提供しておりません。
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	制限無し（ベストエフォート型）
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	1ユーザあたり、3GBのディスク容量制限がございます。10人で利用される場合には、30GBが制限値となります。

コラボフロークラウド　サービスレベルチェックリスト （「クラウドサービスレベルのチェックリスト」（経済産業省）に準拠しています。）　　平成29年7月7日

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
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	平日9:00～17:00（月～金）にメール、FAX、WEBより受け付けております
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	平日9:00～17:00（月～金）にメール、FAX、WEBより受け付けております
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 クラウドストレージに対し、データベースのバックアップを定期バックアップを実施しています。バックアップデータへのアクセスはクラウド運用グループのみが出来ます。添付ファイルのバックアップは現在していません。
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	時刻	1日1回、毎日午前2:00（日本時間）に定期バックアップを実施。 保守作業前に実施。
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	8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 サービス解約日の翌日から起算して31日後に全てのデータを消去します。
32		バックアップ世代数	保証する世代数	世代数	8世代分
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	無 現在、行っておりません。
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	無 ストレージキーはアプリケーションサーバーにて一括管理しています。 ただし、アップロードされたデータおよびデータベースはテナント毎に分離しています。
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	有 利用規約に定める範囲において補償を行います。
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 返却はされないが、データ消去の要件に従い、利用者のデータは全て消去します。
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	無 現在、行っておりません。
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（一部無し） 入力項目の要件に合わせて文字種や長さのチェックを行っています。 ただし、添付ファイルのデータ形式・内容には制限はありません。
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）
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 物理的な事務所の分離、運用者の制限を行っております。
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 暗号化通信にTLSv1.0以上を要求（SSL3.0は無効）し、暗号強度はAES 128bitに対応しています。なお、SHA-256で電子署名された2048bitの公開鍵を使用しています。
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 データベースを物理的に分離し、データベース利用ユーザも別々に管理している、利用会社以外のデータを参照することは、困難となっております。
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 利用者のデータにアクセスできる社員等は明確に限定しております。
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	ID付与は、情報セキュリティ管理者が認めた社員のみ。 セキュリティログの保管期間は1年となっております。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	有 ファイルアップロード時に随時、および深夜の自動メンテナンスに日次で行っています。
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 データはクラウド上でのみに保管しており、物理サーバーへのアクセスはAWSのセキュリティに準じます。
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	有 把握しております。