

## コラボフロックラウド サービスレベルチェックリスト

第 11 版 改定日：2022 年 8 月 8 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 日です。（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 定期的な保守停止の場合は、7 日前までにサポートサイトでの通知と、担当者へのメール通知が行われます。 ※ただしシステム運用面・セキュリティ面の影響から対策が必要と判断された場合は、数日から数時間以内に事前通知の上、緊急メンテナンスを実施する場合があります。
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 ヶ月前までにサポートサイトでの通知と、担当者へのメール通知が行われます。
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柳橋市場ラボを主としてフォロー体制を組んでいます。
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 現状代替手段の用意はありません。
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、サポートサイトでの事前通知と、担当者へのメール通知が行われます。
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クラウド外から 24 時間 365 日で監視し、正常アクセスチェックを実施しています。その他、負荷率・各使用量、発生している例外などについても監視を行い、必要に応じて対策を行っています。
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	サポートサイトにて、発生日時、解決日時、障害原因、今後の対策が随時公開されます。
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	障害等が発生した場合、弊社サポートサイトにて、発生日時、解決日時、障害原因、今後の対策について随時公開しています。障害情報の購読者にはメールでの通知も行われます。
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	有 監査ログにより、システムへのログイン/ログアウトを記録し、お客様自身で参照・ダウンロード可能です。

19		クロックの同期	システムで使用しているクロックの同期対応	有無	有 Amazon AWS が提供する NTP サーバーと同期しています。
20	性能	応答時間	処理の応答時間	時間 (秒)	平均応答時間は 3 秒以内と定義しています。(データセンター内において)
21		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 3 秒以上となる遅延の継続時間が 2 時間以内と定義しています。
22		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しています。
23	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 REST API と JavaScript API によるカスタマイズが可能。カスタマイズに必要な仕様などの情報は、サポートサイトにてリファレンスとナレッジを公開。また、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、設定で変更可能です。
24		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 オプションによる kintone 連携の他に、REST API と JavaScript API、及び Webhook による外部連携カスタマイズが可能。カスタマイズに必要な仕様などの情報は、サポートサイトにてリファレンスとナレッジを公開しています。
25		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)
26		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、5GB のディスク容量制限があります。(10 人で利用される場合には、合計で 50GB が制限値です。)
サポート					
27	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、WEB より受け付けています。
28		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、WEB より受け付けています。
データ管理					
29	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 クラウド全体を独自形式で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実施できます。
30		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。 保守作業前に実施しています。
31		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	60 日間
32		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お客様データは 30 日間、バックアップデータは 60 日間保持し、保持期間経過後速やかに対象データを削除します。
33		バックアップ世代数	保証する世代数	世代数	60 世代分
34		バックアップからの復元	利用者要望によるバックアップからのデータ復元の対応有無	有無	無 利用者の希望によるバックアップからの復元は受け付けていません。
35		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 データベースの暗号化を行っています。
36	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。	

37		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 利用規約にて定義しています。詳細はクラウドサービスご利用規約を参照ください。
38		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 データの返却はされませんが、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。データ消去要件の詳細については本チェックシート内「データ消去の要件」を参照ください。
39		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 申請データの作成日時・作成者・データ変更履歴が記録され、お客様により参照できます。
40		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。
41		データ資産の管理主体と範囲	預託データの所有権、利用権(事業者への委譲を含む)が明確に定義されている	有無	有 クラウドサービスご利用規約にて、コラボスタイルはお客様データに関するいかなる権利も取得しない事を定義しています。
42		装置の処分又は再利用	装置の処分又は再利用時の対応について明確にされているか	対応状況	装置の破棄及び再利用については、Amazon AWS の方針に従って実施されています。
セキュリティ					
43	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 認証を取得しています。(登録番号: IS 670172)
44		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 セキュリティホールの有無等について、第三者の脆弱性検証ツールにより継続的な確認を行い、重要な問題がある場合は速やかに対処する体制を構築しています。
45		Web アプリケーションの保護	Web アプリケーションへの不正な侵入、操作、データ取得等に対し、対策を行っていること	有無実施状況	有 ・OS、その他ソフトウェアのパッチ更新情報を常に収集し、必要なパッチは検証後速やかに適用する体制を整えています。 ・Web アプリケーションに対する多方面からの攻撃に備えるため、ファイアウォールや DDos 攻撃への対策に加え、WAF による防御を行っています。
46		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います。
47		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 TLSv1.2 以上を要求し、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。
48		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
49		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 ・必要に応じて、テナント毎に IP アドレス制限や、BASIC 認証を利用する事で、利用者間の情報隔離を強化できます。 ・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ますので、利用会社以外のデータを参照することは困難です。
50		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います。
51		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が付与しています。 ・セキュリティログの保管期間は 1 年です。 ・セキュリティログは関係者のみにアクセス権を割り当てています。
52		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。

53		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のみ保管されます。物理サーバーへのアクセスは Amazon AWS のセキュリティに準じます。
54		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 把握しています。 当サービスを提供するために、以下のサービスを利用しています。 ・Master Hub：連携オプションサービスでの API 連携利用のため ・New Relic：アプリケーション監視のため
55		セキュリティインシデント発生時の対応	・情報セキュリティインシデント発生時の、責任体制及び手順、及び通知の有無	有無	有 ・インシデントレベルの判断方法、対応方法、責任体制、対応後の記録の作成方法などを定義し、情報セキュリティインシデントが発生した場合に迅速に対応できる体制を構築しています。 ・利用者に広く注意喚起が必要な、重大なセキュリティインシデントが発生した場合、弊社サポートサイトにて、発生日時、解決日時、障害原因、今後の対策が随時公開されます。
56		専門組織との連絡	・情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持しているか。	有無	有 情報セキュリティコンサルタントと定期的に情報交換を行い、また必要に応じて随時連絡が取れる体制を構築しています。
57		セキュリティに配慮した開発方針	セキュリティに配慮した開発方針の有無	有無	有 提供サービスは、各種ガイドライン及び社内開発方針に従って開発されます。 また品質認証制度である PSQ-Lite の認定を取得しています。
58	認証	パスワード管理	セキュリティに配慮したパスワードが設定できる	有無	有 ・最低文字数、複雑さの制御、前回と同じパスワードを設定不可とする設定が可能です。 ・パスワードの有効期限を設定可能です。
59		接続時間の制限	一定の使用中断時間が経過したときは、使用を中断しているセッションを遮断する	有無	有 指定期間を経過すると、自動的にセッションを遮断するように設定可能です。

※「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。