comomo
2022/8/25更新

「クラウドサービスレベルのチェックリスト」（経済産業省）に基づき、comomoの提供する音読さんのセキュリティについてまとめたものです。
お客様フォーマットのチェックシートへの回答をご希望の場合は、別途有料オプションを提供しております。詳細はお問い合わせください。

経産省 クラウドサービスレベルのチェックリスト

No.	種別	サービスレベル項目例	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／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	有無	30日前にメール／ホームページで通知
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ヶ月程度前にサービス内インフォメーションにて告知します。
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 プログラム及びデータ預託の計画無し
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（%）	現状、SLAの保証提示しておりません。 SLO未定義ながら、現状での回答可能範囲は下記となります。 稼働目標：99.9% 昨年稼働実績（平均）：99.99%以上、提供環境により異なる
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 国内遠隔地のデータセンターにデータをバックアップ 遠隔地に予備システムの構築はございません。
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 構成ネットワークで単一障害点がないようにサーバを冗長化。データの日次バックアップを別環境に7世代保管。 災害発生時は復旧可能な最新のバックアップを使用して、別環境に24時間以内に復旧見込み。ただし、災害範囲が広範囲に及び、複数拠点のデータセンターを跨ぐ場合などはこの限りではありません。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定
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 完全に現行環境が活きない状態の場合、データアクセスに対する認証・セキュリティを同程度に保った上での提供が望ましく、それ故にバックアップデータから復旧させる事が優先的に考えられます。しかしながらそれは環境復旧を指しますので、この場合代替という提供を想定しておりません。
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 お客様に影響のある機能変更等を伴うアップデートは、サイト上で事前に告知しております。 サービスのソースコードレベルの変更管理はGitを利用して行なっています。 Googleのマネージドベースイメージをしよう。このイメージでは最新のセキュリティパッチが自動適用されます。
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	障害＝サーバ・ネットワーク接続障害としての回答です。 平均10分以下
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	12時間以内の復旧を目標
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	回	長時間障害0回（数分単位の通信障害を除く）
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 アクセス・負荷・使用量等を別環境のシステムにてチェックを行っております。
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 障害内容をホームページの障害発生状況ページに掲載。特定のユーザーへ障害が発生している場合はメールで連絡。
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	営業時間内：1営業日以内に通知。 営業時間外：状況把握から1日以内に通知。
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）	営業時間内/外に関わらず、監視対象項目によって、数秒～5分で収集。
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	ホームページにて随時確認いただけます。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定
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 アクセス状況確認等サービス提供上ログを取得しておりますが、あくまで当社の管理・サービス提供の可用性を目的としており、あいにく任意に操作ログをご覧いただく機能は準備がございません。 ただし、裁判所からの命令、警察からの調査への協力の場合この限りではありません。
19	性能	応答時間	処理の応答時間	時間（秒）	平均2秒未満。 対象とするページ・ご登録いただくデータ量・接続されている端末のネットワーク環境に
20		遅延	処理の応答時間の遅延継続時間	時間（分）	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は3時間以内を目標としております。
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）	定期的なバッチ処理はございません。
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	無 サービス自体のカスタマイズには未対応となっております。
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	無
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 接続上限に達した場合スケールアウトで対応を行うため基本的に制限はございません。
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	無 容量上限に達した場合スケールアウトで対応を行うため基本的に制限はございません。
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	基本的には一般問い合わせと変わらず平日10:00-16:00（メール）を予定。 障害発生状況ページで状況は随時更新予定
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	メールで受け付けており、受付は24時間365日、対応は平日10:00-16:00となります。
データ管理					

No.	種別	サービスレベル項目例	規定内容	測定単位	設定
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 • データベース: 日次でフルバックアップ、 IaaS 機能によりフルバックアップを随時取得 • 書類ファイル: 随時遠隔地にレプリケーション • ログ: 随時レプリケーション アクセス権はデータベース、ログ、書類ファイル：インフラチームのみ
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	データベースは IaaS機能により当日10分前まで保証 ファイル、ログは随時レプリケーションしているので直前まで保証
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	バックアップはクラウド上に保持しており、外部媒体へ は保管しておりません。 保存期限は以下の通りです。 • データベース: 7日間 • ログについて: 最低1年間保管 サービスの性質上、書類ファイルについては無期限に 保存いたしております。
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 削除機能より、随時履歴の削除可能。データベース、ログは保管期間経過後に削除
32		バックアップ世代数	保証する世代数	世代数	3世代
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 データベースストレージの暗号化を実施、パスワード等一部のデータは不可逆の暗号化で保存
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 複数のキーを使用することで、不正アクセス等の影響範囲を限定します。
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。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定
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 データ出力は機能範囲で契約者側にて行っていただきます。 報告は、削除を行った旨をメールでご案内しております。削除後の非存在の証明は難しいですが、ご希望いただきましたら出力結果が存在しないという出力はご案内可能です。
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	有 データ入力時、送信時に検証、通信経路での盗聴、改ざんを防止するためにTLSにより保護
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 テキストボックスに入力するテキストは、プレーンテキストである必要があります。 アップロードされるファイルは適切なPNG, JPG, JPEG, WEBP形式のデータである必要があります。
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	無 今後取得を検討
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	有 外部企業による脆弱性診断を半期に一度実施し、指摘事項について対応しております。
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 運用者は限定されております。
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 ユーザーとサービス間の通信はTLS1.2 以上を利用しております。
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

No.	種別	サービスレベル項目例	規定内容	測定単位	設定
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 分離した権限を発行し領域ごと提供しており、データベース含め分離した構成をとっております。が、コントロールにおいては非公開情報とさせていただいております。
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 アクセス可能な従業員は限定され、その権限・認証を認知する者を限るとともに構成・経路は非公開とさせていただきますがロケーション・認証を設けております。
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	1従業員1IDで管理システムの認証を行います。 契約者へログの提供はあいにく行っておりませんが、万が一セキュリティインシデント発生の際には当然に影響範囲特定に必要な情報提供・調査にあたる認識でおります。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	以下のようになっております。 サーバ → ウイルス対策ソフト導入なし 運用者端末 → 随時スキャン
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 バックアップはクラウド上に保持しており、持ち出し可能な外部媒体への保管は行わないようにしております。
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	データセンター、当社ともに日本国法に準拠します。