【経済産業省】クラウドサービスレベルのチェックリスト　　最終更新：2024/7

https://warp.da.ndl.go.jp/info:ndljp/pid/8658576/www.meti.go.jp/press/20100816001/20100816001-4.pdf

No.	種別	サービスレベル項目例	規程内容	測定単位	回答内容
アプリケーション運用					
1	可用性	サービス停止時間	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） 障害調査、回答は弊社が定める休日を除く平日の９時から１７時までで対応します。（日本時間）
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】 計画停止の２週間前までにメールもしくはサービス内の機能で通知
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】 メールもしくはサービス内の機能で通知 通知時期は定めていません。
4		突然のサービス提供停止時の対処	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】 環境委託は行っていません。
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（%）	99.0%以上を目標としています。
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】 バックアップはＡＷＳの別リージョンに転送しています。 復旧は東京で行います。
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	【有】 サービスを稼働しているリージョンが使用できなくなった場合、別リージョンで復旧できます。
8		代替処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】 サービスを利用しない場合での代替措置は定義していません。
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】 年に２回のバージョンアップを予定しています。 脆弱性対応や不具合対応などにより緊急パッチリリースを行う場合もあります。 変更内容をリリースノートで公開します。
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	事例は取得中です。
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	目標を８時間以内としています。
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	事例は取得中です。
13		システム監査基準	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】 弊社が定める休日を除く平日の９時から１７時まで（日本時間）に死活監視、や資源（ＣＰＵ、メモリ、ディスク）監視を行います。異常が発生した場合は、同時間帯で調査・対応を行います。
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】 お客様の管理責任者にメール、または本サービス内にてお客様に通知します。
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	弊社が障害を検出した時点を起点として、１時間以内を目標とします。 ※弊社が定める休日を除く平日の９時から１７時までの対応とする。 　上記時間帯以外で検出した場合は、翌稼働日の開始後１時間以内を目標とする。
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分間隔で監視しています。
17		サービス提供状況の報告/間隔	サービス提供状況を報告する方法／時間間隔	時間	毎月稼働状況に関する報告をします。
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】 ログイン履歴、操作履歴、データ更新履歴はサービス内で確認できます。 サービスのシステムログは確認できません。
19	性能	応答時間	処理の応答時間	時間（秒）	定義していません。 登録データ数によっては応答時間が長くなる可能性があります。最大１時間でクライアントーサーバ間がタイムアウトします。ただし、クライアントーサーバ間がタイムアウトされたときでもサーバ側の処理は継続されます。実行状態はサービス内で確認可能です。 お客様のネットワーク環境（プロキシサーバなどの設定）によっては、１時間より前にタイムアウトする（クライアント側にエラーが返る）可能性があります。mcframe X以外のリソースでタイムアウトした場合、想定外のエラーが返却され、ブラウザ側でリトライが行われる場合があります。リトライが行われると２重登録される可能性があります。そのため、ネットワーク環境の設定変更をお願いする可能性があります。
20		遅延	処理の応答時間の遅延継続時間	時間（分）	定義していません。
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）	定義していません。 登録データ数によっては応答時間が長くなる可能性があります。 非同期で実行させることも可能です。実行状態はサービス内で確認可能です。
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】 カスタマイズ環境（Developer Platform）を提供しています。
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	【有】 CSVファイル連携（SFTP）やAPI連携が可能です。 APIドキュメントを提供しています。 ※CSVファイル連携（SFTP）を利用する場合、SFTPのポート（22）を開放していただく必要があります。
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）	【有】 購入されたライセンスで制御されます。ログインしている同時接続数で制御されます。
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	定義していません。
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	時間帯	ヘルプデスクでの受付は24時間365日可能です。 障害調査・回答は弊社が定める休日を除く平日の９時から１７時までで対応します。（日本時間）
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	ヘルプデスクでの受付は24時間365日可能です。 障害調査・回答は弊社が定める休日を除く平日の９時から１７時までで対応します。（日本時間）

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】 1日1回データベースのフルバックアップを行います。 稼働しているリージョンで保管するとともに、別リージョンに転送します。 お客様はバックアップデータにアクセスできません。
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	時間	データベースの復旧時点は２４時間以内とします。 復旧作業に伴い、損失されたデータについては何ら保証せず、また責任を負わないものとします。 データのリストアはB-EN-Gの判断で行います。お客様のリクエストによる対応はしないものとします。
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	ログイン履歴、操作履歴、データ更新履歴は１か月以内のデータを参照できます。
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	解約後１か月以内で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	データベースのバックアップデータは３世代分（３日分）保存します。
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】 httpsによる暗号化通信を行っています。ファイル連携ではsftpで暗号化通信を行っています。 データベースのデータ暗号化は行っていません。
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	【有】 データベースはPostgreSQLを利用しています。Row Level Securityを利用してテナントごとのデータが管理されます。
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	【無】 定義していません。
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】 データの返却については定義していません。データ消去の方法は定義しています。
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	【有】 サービスの機能としてチェック機能があります。登録したデータはお客様がサービス内で確認できます。
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】 サービスの機能ごとに定義されています。定義内容によってチェックされます。
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	【有】 プライバシーマークの認定済みです。（https://www.b-en-g.co.jp/jp/p-policy.html） mcframe XはAWSのファンデーショナルテクニカルレビューを通過しています。 ※ファンデーショナルテクニカルレビューは２年ごとに通過することにしています。
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】 1年に2回、第三者機関によるウェブアプリケーション脆弱性診断を実施しています。
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】 顧客環境へのアクセス方法は社内文書で定義しています。社内規定に従って適切に管理されます。
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】 httpsによる暗号化を行っています。ファイル連携はsftpで暗号化を行っています。 ※SHA-256 with RSA(2048) また、AWS WAFを導入しています。
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】 提供していません。
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】 シングルテナント環境： VPCをわけ、ネットワークレベルで分離しています。データベースもテナントごとに作成しています。 マルチテナント環境： 外部ファイルストレージはテナントごとに分離され、別テナントのデータにはアクセスできません。 データベースはPostgreSQLのRow Level Securityを利用してテナントごとのデータが管理されます。
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】 顧客環境へのアクセス要件は社内文書で定義しています。社内規定に従って適切に管理されます。顧客環境には権限が与えられたユーザが承認後にアクセスできることにしています。
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	AWSアカウントのアクセス状況はCloudTrailで管理しています。CloudTrailのデータは１年間保存します。 ＡＷＳアカウントは個人のＩＤを付与しています。共有ＩＤは使用していません。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	sftpで外部からアップロードされたファイルはアップロードの都度ウイルスチェックしています。
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】 バックアップはAWS Buckupサービスを利用して管理しています。 外部への保管は行っていません。
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	稼働中のデータはＡＷＳの東京リージョンでのみ管理しています。 ※東京リージョンで問題が発生したときはシンガポールリージョンで運用する可能性がある