経済産業省　クラウドサービスレベルチェックリスト

最終更新日: 2026/11/17

JENKA　運営元	項目	回答
	会社名	スターティアテクノス株式会社
	所在地	東京都新宿区西新宿２丁目３−１ 新宿モノリスビル19F
	業務内容	DX支援事業 業務の自動化ツールの開発および、導入・運用サポートによる働き方改革やテレワーク支援
	ヘルプサイト	https://help.jenka.jp
	プライバシーマークの取得有無	無 (PMS認証 JIS Q 15001準拠の第三者認証有)
	委託(再委託等含む)の有無	個人情報の管理およびサポートの外部委託はありません

1.　アプリケーション運用

No.	種別	項目	規定	単位	回答
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	【有】バージョンアップ等の計画的な停止、重要な脆弱性を検知した時には臨時メンテナンスをする場合を除き、停止時間はございません。
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】ヘルプサイトのお知らせカテゴリでの告知します。
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】2026年11月現在、サービス停止の予定はありません 終了より3ヶ月以上前にサイト上で告知します
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	【有】サービス利用約款に記載しています。サービス終了3ヶ月以上前までに通知致します。
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(%)	公開しておりません。
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	リージョン内AZレベルの冗長化を行っています。遠隔地リージョンレベルの対応はありません。
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	障害内容に応じてご報告させていただきます。
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)	なし
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】修正・更新は随時反映。サービス停止を伴う場合は、ヘルプサイトのお知らせにて通知します
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	できるだけ早急に復旧いたします。（実績：アプリケーション障害 3時間程度）
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	できるだけ早急に復旧いたします。（24時間目標）
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)	回	全体的な影響の障害: 1回 部分的な影響の障害: 1回 期間 2025年11月 - 2026年11月
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】サイトの死活監視、プログラムアラート監視、パフォーマンス監視、アクセス監視
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】規程はありませんが、できるだけ早く通知します。
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	規程はありませんが、できるだけ早く通知します。
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)	常時監視しています。
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	サービス提供状況を常時掲示する場所はありません。外部サービス連携に継続的な障害が発生した場合はヘルプサイト「お知らせ」による通知を行います。深刻である場合はお客様単位で連絡いたします
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】管理画面操作ログ, ワークフロー実行ログ サーバーシステムログは原則提供していません。
19	性能	応答時間	処理の応答時間	時間(秒)	数秒から数時間 サービス特性上、連携先・連携数・利用方法によって応答時間が異なります
20		遅延	処理の応答時間の遅延継続時間	時間(分)	数秒から数時間 サービス特性上、連携先・連携数・利用方法によって応答時間が異なります
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)	数秒から数時間 サービス特性上、連携先・連携数・利用方法によって応答時間が異なります
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	有無	【有】下記の範囲で設定が行えます。お客様独自のUIやドメインのカスタマイズは承っておりません ・ワークフロー ... 名称、ワークフロー内のコネクタ配置、ワークフロー内のメモ ・グループ ... 名称、作業ユーザーの限定、管理者設定、連携可能な外部サービスとアクションを許可 ・サービス認証 ... 名称 ・アカウント ... 名称、所属グループ、備考、有効/無効 ・セキュリティ ... IPアドレス制限、パスワードポリシー変更、多要素認証(メール)有効化
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】本サービスで用意した外部サービスへの接続機能のほか、任意のREST APIでの外部接続、本サービスが発行したWebhookおよびメールアドレスへの通知が可能です。
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)	同時接続利用者数の制限はありません。
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	ご契約時にコネクタ実行回数やファイル容量などの制限を決定します。

2.　サポート

No.	種別	項目	規定	単位	回答
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	ヘルプサイトからの問い合わせを24時間受付しております。 お電話でのお問合せは原則として承っておりません。 回答や調査対応は平日9:00 -18:00となります。
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	ヘルプサイトからの問い合わせを24時間受付しております。 お電話でのお問合せは原則として承っておりません。 回答や調査対応は平日9:00 -18:00となります。

3.　データ管理

No.	種別	項目	規定	単位	回答
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】対象: データベース 回数: 1日1回
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	日本時間午前5:30
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	7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	有無	【有】解約処理後、ただちに該当クライアントの全ユーザーのログインの権限が停止されます。 ログイン情報、ワークフロー情報は解約後90日以内に削除されます。
32		バックアップ世代数	保証する世代数	世代数	7世代(1日1回)
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】データベースおよびオブジェクトストレージに保管され、データは暗号化されています
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】お客様ごとに発行されたキーにより論理的に分離
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	【有】利用規約に定める範囲において補償をおこないます。 また、損害保険に加入しています。
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】ご解約までにお客様自身にて必要なデータはエクスポートをお願いします。
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	【有】フロントエンド、バックエンドでバリデーション処理を行っています
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】フロントエンド、バックエンドでバリデーション処理を行っています

4.　セキュリティ

No.	種別	項目	規定	単位	回答
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】ISO27001 (575952)
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1回、第三者によるソースコードの脆弱性検査を受け、評価及び対応を実施しています。
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】クラウドのアカウントは開発者ごとに可能な操作を限定し、操作ログを記録しています。本番環境は開発環境と切り離し、ルートアカウントは運用上は凍結したうえで、ログイン可能なユーザーを限定しています。
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】TLS1.3
43		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】お客様毎に内部IDを発行し、論理的に分離しています。 ワークフロー処理のリソース顧客ごとに分離されており、負荷状況に応じてスケールします
44		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	有無／設定状況	【有】本番環境と開発環境の分離, 限定されたパスワード周知, コントロールパネルの秘匿化
45		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いるか	設定状況	クライアント単位, ユーザー単位, ワークフロー単位, ワークフローの実行単位, コネクタ単位でIDを発行して管理しています。 システムログは1年間保持されていますが、お客様がダウンロード可能なデータとしては提供しておりません。ご要望の際はご相談ください。
46		ウイルススキャン	ウイルススキャンの頻度	頻度	外部からファイルを一時ダウンロードする機能において常時稼働させています。 ウィルスやマルウェアに該当するファイルは即時隔離されます。
47		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ます。