Digima クラウドサービスセキュリティチェックシート

更新日: 2026年09月01日

No.	種別	サービスレベル項目	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	サービス自体は24時間365日提供（バージョンアップ等の計画停止を除く）されます。
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	有り。 定期メンテナンスやバージョンアップ等の計画停止が発生する場合は、事前にサポートサイトへの掲載やシステム画面上（プロダクト上）などでユーザーへ通知・連絡を行っております
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	無し。
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（%）	保証・目標値の定めなし。
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	無し。
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	無し。
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）	定義無し。 なお、代替措置としてではなく、通常の運用において「ユーザー自身によるデータのバックアップ」や「解約時のデータ引き渡し」を行う際には、システムのエクスポート機能が対応している一部のデータ（顧客データなど）に限り、CSVファイル形式でダウンロードして取得することが可能です。
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	有り。 バージョンアップ、システムの変更管理、およびセキュリティパッチの適用に関する方針や運用体制は、サービス提供元（株式会社コンベックス）において定義され、適切に実施・管理されています。
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	非公開
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	非公開
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	非公開
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	有り。 監視体制や報告プロセス自体はルール化され運用されていますが、具体的な監視項目は非公開としております。24時間・365日体制でネットワーク監視が実施されており、監視データは1分ごとに収集されております。
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	有り。 障害発生時に、サポート窓口から利用者に発生事実や原因、被害状況を速やかに報告するルールがあります。具体的な通知先や通知方法などの詳細な手順は非公開となります。
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	定義無し
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）	未定義
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	定義無し
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	無し
19	性能	応答時間	処理の応答時間	時間（秒）	非公開
20		遅延	処理の応答時間の遅延継続時間	時間（分）	非公開
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）	非公開
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	無し
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	無し
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）	制限なし
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	各機能ごとに制限あり
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	受付時間帯：平日 10:00～12:00 ／ 13:00～17:00
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	受付時間帯：平日 10:00～12:00 ／ 13:00～17:00
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	有り。 バックアップ：事業者側で毎日完全バックアップ、および1分ごとに増分バックアップを実施しています（AES-256で暗号化）。 保管場所：機密データはすべて日本国内（東京）のデータセンターで保管されます。 アクセス権：システム利用者はアクセスできません。 ポータビリティ：一部データ（顧客データなど）のみシステムからCSV形式でエクスポート可能です。
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	1分（バックアップ取得間隔） 毎日実施される完全バックアップに加えて、1分ごとに対象データの増分バックアップを取得していますが、障害発生時にデータをどこまで遡って保証するかという公式な目標復旧時点（RPO）の定めはありません。
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	クラウドサーバーを利用しているため弊社での媒体管理は行っておりません。
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	有り。 サービス解約後のデータ削除については、利用規約にしたがって削除されます。
32		バックアップ世代数	保証する世代数	世代数	35世代（日次バックアップを35日間保存）
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	有り。
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	有り。 アプリケーションによって制御されていますが詳細は非公開となります。
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	無し
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	一部有り。 顧客データなどシステム側でエクスポート機能が提供されている一部のデータのみCSVファイル形式で引き渡しが可能
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	一部有り。 一部のサービスにおいて監査ログおよびチェックサム機能がデータ整合性を検証する手法として実装されています。
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	機能によって異なります
セキュリティ					
39		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	有り。 プライバシーマーク（Pマーク）を取得
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	有り。 脆弱性診断を年に1回実施しております。
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	有り。 データベースへの直接アクセスおよび変更は、社内運用ルールにより開発・運用担当のSRE管理者のみに制限されています。
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	有り。 クラウドサービスとユーザーが操作する端末との間でやりとりされるすべての通信、およびデータ転送の経路において、SSL/TLS証明書の検証を伴うHTTPS経由での接続のみが強制されています。
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	無し

44	セキュリティ	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	一部有り。 ユーザー権限に応じてアクセスできる情報が分かれるシステム仕様となっております。 物理的な隔離や障害影響の局所化はございません。
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	有り。 ユーザー権限によってアクセスできる情報が別れる仕様となっております。 IPアドレスを利用してクラウドサービスへのアクセス元自体を制限する手段も備わっております。
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	一部有り。 ユーザー単位でのID付与に対応しております。利用者へのログの提供はございません。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	ウィルススキャンは実施しておりません。 ウイルススキャン自体は未対応ですが、システムの安全性維持を目的としたマルウェア対策は実施されています。
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	一部有り。 システム上で取得される完全バックアップデータは、保管時にAES-256規格により常に暗号化されています。物理的なデバイス管理やその検証については、すべてクラウド事業者（データセンター）側の厳格なセキュリティ統制に依存し、同事業者によって実施・担保されています。
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	把握している。 お客様の機密データはすべて日本国内（東京）のデータセンターに保管されることが保証されており、国内の各種法制度（個人情報保護法等）を遵守した環境で適切に取り扱われています。