repsona セキュリティチェックシート

2021年12月2日版

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／方法の記述を含む）	有無	有 実施5営業日前までにお知らせで通知します
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 利用規約に基づいて行われます
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 現状、Repsona開発システム・サービス提供を司る運営システム・現顧客データ管理の第三者委預託の予定はありません。
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（%）	最新の稼働率は https://repsona.com/status でご確認いただけます。
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 1日1回以上のバックアップを行い、データはサービスが稼働している環境とは異なるデータセンターへ保管。
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 世代管理されたバックアップデータからの復旧。
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 公開していません
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	継続的なバージョンアップを実施しています。リリース後、お知らせにて報告します。サービス稼働に影響が出るようなアップグレードの場合は事前に告知します。
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	公開していません
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	公開していません
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	ダウンタイムが発生した障害は https://repsona.com/status で履歴をご確認いただけます。
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 ハードウェア／ネットワーク／パフォーマンス監視
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 障害発生時は速やかに担当者に通知され、対応を行います。ユーザーへはTwitter等で速報を出します。
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	10分以内
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）	対象により異なります。1～5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	https://repsona.com/status で稼働状況をご確認いただけます。
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 アクセスログ・操作ログ・エラーログなどを収集しています。
19	性能	応答時間	処理の応答時間	時間（秒）	平均1秒未満
20		遅延	処理の応答時間の遅延継続時間	時間（分）	公開していません
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）	公開していません
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 個別のカスタマイズはありません。
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 APIは公開していません。
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 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	プランに応じて、利用可能なストレージ容量の上限があります。
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	24時間365日（問い合わせフォーム）
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	平日（月曜日～金曜日） 10:00～16:00
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 定期的にバックアップを行っています。データ領域のバックアップは、サービスが稼働している環境とは異なるデータセンターへ保管しています。
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	24時間以内
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、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 180日経過後に削除作業を開始し、開始から10日以内に削除を完了します。
32		バックアップ世代数	保証する世代数	世代数	7世代

No.	種別	サービスレベル項目例	規定内容	測定単位	設定
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
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 ユーザーへのキー提供は行っていません。S3内の分離した領域に保存しています。スペース単位でのストレージは物理的には必ずしも分離していません。
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。
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 限定的になりますが現在サービスで提供しているデータ出力機能を使い、ユーザー自身で行っていただく形となります。
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
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
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 ISMS認証を取得しています。
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	無 脆弱性検査を定期的に実施しています。
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 サーバーにアクセスする事が出来るのは、システム運用担当のスタッフに限定しています。また、ファイアーウォールで弊社環境からのみアクセスできるように制限しています。
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 TLSv1.2以上で通信を暗号化しています
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
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 スペース毎にデータを論理的に分離しアクセスコントロールされています。
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 サーバーにアクセスする事が出来るのは、システム運用担当のスタッフに限定しています。また、ファイアーウォールで弊社環境からのみアクセスできるように制限しています。
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	保管しているログから調査可能です。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	定期的にスキャンしています。
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 二次記憶媒体を使用せず、データセンター間でバックアップを取っております。
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	把握しています