ログミーツのセキュリティチェックシートver.1.02

2020/11/16発行
2020/11/20改訂
時空テクノロジーズ

No.	種別	サービスレベル項目	規定内容	測定単位	設定
クラウド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日です。(計画停止を除く)
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 1週間以上前にメールで通知します。
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 3か月以上前に事前にメール/ホームページで通知します。
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（現時点では終了予定はございません。ファイルの預託も未定です。）
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 (%)	99%以上
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	有無	有 物理的に異なるリージョンからのリカバリを実施します。 リカバリには1日程度を想定しています。
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 回収できるデータをファイルを物理メディアまたはダウンロードできる環境を提供します。
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)	有 CSV,TXT, FLAC, ユーザーがアップロードしたファイル形式に従ったフォーマットで提供します。
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 1ヶ月に1～3回ほどを目安に更新。重要なアップデート情報はウェブサイトに掲載します。
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	公開しておりません。
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	24時間以内
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	障害発生はまだございません。
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 ンス監視がされています。 一定の数値を超える場合は管理者にメール通知が送信されます。
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	検討中です。 現在サービスインの直前のため、サービス開始時は緊急連絡先への連絡および、障害告知ホームページへの切り替えを想定しています。 第3者の障害監視サービスも検討中です。
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	1時間。お客様へは可能な限り早くお知らせします。
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)	5分間隔です。
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	必要に応じてサービス内、Webサイト、SNSで行います。
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 ユーザー/デバイスのアクセスログ、操作ログ、位置情報
19	性能	応答時間	処理の応答時間	時間 (秒)	UIが無応答となる時間を5秒以内とすることを目標としています。
20		遅延	処理の応答時間の遅延継続時間	時間 (分)	24時間
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)	現在ユーザー様向けへのバッチ提供は予定しておりません。
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
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)	同じアカウントに対しての同時接続は1名です。別々のアカウントによるアクセス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	契約によって可変。現在のディスク容量制限はありません。
インストールアプリケーション管理					
26	拡張性	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
27	セキュリティ	データの暗号化		有無	有 ログイン情報及び録音データ等の保存データは暗号化されています。

ログミーツのセキュリティチェックシートver.1.02

2020/11/16発行
2020/11/20改訂
時空テクノロジーズ

No.	種別	サービスレベル項目	規定内容	測定単位	設定
28		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通信の徹底
29		電子署名の有無		有無	有
30		ウイルススキャン	ウイルススキャンの頻度	頻度	無（検討中です）
31	データ管理	バックアップ世代数	保証する世代数	世代数	0 アプリケーション上に保存されたデータに関しては各種OSに依存します。 アプリケーション上のデータはすべてクラウドにアップロード後に消去前提となるので、実質クラウド側でデータ保証がされます。
32		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（障害保険加入検討中）
33	可用性	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 1ヶ月に1,2回ほどを目安に更新します。重要なアップデート情報はウェブサイトに掲載します。
サポート					
35	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	平日（祝日を除く月曜日一金曜日）午前10時から午後5時 システム停止など重大な障害発生時は、必要に応じ、上記時間帯以外でもメール対応を行います。
36		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（祝日を除く月曜日一金曜日）午前10時から午後5時。 システム停止など重大な障害発生時は、必要に応じ、上記時間帯以外でもメール対応を行います。
データ管理					
37	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 毎日バックアップを取得しています。時刻はAM5時。 バックアップは障害時の復元用です。ユーザーからの直接アクセスは想定していません。アクセスは一部の開発者に限定されます。
38		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	AM5時
39		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	2週間
40		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 サービス解約後1年間はデータを保持し、消去。 顧客の希望によっては即時消去。
41		バックアップ世代数	保証する世代数	世代数	デイリーで2週間14世代の保管です。
42		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 ストレージレベルで暗号化しています。
43		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 用途ごとに独立したキーを設定
44		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（障害保険加入検討中）
45		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 解約後はデータはサービス利用時と同様のセキュアな状態で保全。消去ルールに基づき、データも消去されます。
46		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 アクセスログや操作ログを取得しています。 ログをもとに誰が操作したかどうかの検証が可能です。
47		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 サービスが必要とするバリデーションを実行しています。
セキュリティ					
48	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 ISMS認証(ISO27001)を取得しています。 クラウドセキュリティ認証（ISO270017）も申請中で、2021年初頭に取得完了見込みです。
49		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 セキュリティ審査実施予定があります。
50		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 ISMSに準拠しています。
51		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 SSLでサービス提供されています。

ログミーツのセキュリティチェックシートver.1.02

2020/11/16発行
2020/11/20改訂
時空テクノロジーズ

No.	種別	サービスレベル項目	規定内容	測定単位	設定
52		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 ISMSには準拠しています
53		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 サービスのクリティカルポイントではSPFとなることを避けるため多重化しています
54		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 データへのアクセスは適切に制限されています。
55		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	有 ユーザーID、デバイスID,目的ごとのデータにそれぞれIDが設定されています。
56		ウイルススキャン	ウイルススキャンの頻度	頻度	サービス提供は基本的にLINUXベースのコンテナ環境となり、ウイルス対策はアクセス制限の形で実施されています。
57		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 サービスで扱うデータはクラウド上でのみ取り扱い、バックアップもクラウド上のみのためメディアでのローカルでのバックアップは実施しておりません。 バックアップデータへのアクセスは、システム責任者のみに限定しています。
58		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に対応予定です。