ログミーツ サービス基本情報及びセキュリティ情報

2020/11/16発行
2022/2/14改訂
株式会社時空テクノロジーズ

Ⅰ.基本情報				
サービス基本情報				
サービス内容				
	1	サービスの名称	○	ログミーツ（Logmeets）
	2	サービス開始年月日	○	2021年2月1日
	3	サービスの概要	○	AI自動文字起こしを用いた議事録作成・メモ作成支援及び会議の生産性向上SaaSサービス。
	4	サービスの構成要素	○	・専用モバイルレコーダー端末 ・Windows版レコーダーアプリ ・エディタ（Webブラウザ上の閲覧・編集・共有画面）
動作環境・ネットワーク環境				
	5	エディタの動作環境	○	Webブラウザ：Chrome/Edge/Firefox最新版 OS：上記ブラウザが動作するWindows/Mac/Linux
	6	Windows版レコーダーアプリの動作環境・推奨スペック	○	Windows10/11最新版 CPU：Core i5以上 メモリ：8GB以上
専用モバイルレコーダー端末の仕様				
	7	フル充電時の連続ロギング時間	○	4～5時間（動作環境やバッテリーの経年劣化により数値は変動します）
	8	フル充電までの時間	○	1～2時間（接続するUSBケーブルと充電アダプターによって変動します）
	9	使用可能ネットワーク回線	○	Docomo LTE回線/Wifi/Bluetooth
	10	Docomo LTE回線の通信速度	○	最大8Mbps
	11	ネットワーク断線時の動作	○	ネットワーク断線時にも録音を継続し、音声ファイルのアップロードは保留。ネットワーク普及後にアップロード再開し、AI文字起こしも再開。
	12	音声ファイルの取扱	○	録音して生成された音声ファイルはクラウドサーバーにアップロード後にローカルからは消去される。
	13	液晶解像度	○	240 x 320ドット
	14	タッチパネル機能	○	あり
料金体系				
	15	初期費用	○	「利用規約」を参照。
	16	月額利用料	○	「利用規約」を参照。
	17	最低契約期間	○	12ヶ月（※機材リースの場合は36ヶ月）。「利用規約」を参照。
	18	解約申請受付期限と自動更新	○	契約期間終了日から30日前まで解約申請受付。解約申請がない場合は自動更新。「利用規約」を参照。
準拠法・権利				
	19	サービスに関する準拠法	○	日本法
	20	サービスのデータ保護に関する準拠法	○	個人情報保護法
	21	サービスに登録されるデータの帰属先	○	サービス利用者
個人情報と預託データの取扱方針				
基本方針				
	22	情報セキュリティおよび個人情報保護について方針を定め、これらの方針を組織の内外へ周知している。	○	実施している。
	23	サービス提供者およびクラウドサービスが満たすべき関連法令や規制、契約上の要求事項を整理し、これらを満たすための取組を継続的に実施している。	○	実施している。
	24	セキュリティ対策が正しく実装され意図した通り運用されている。関連法令や規制、契約上の要求事項を満たしているかを社外監査など評価部門により定期的に評価している。	○	社外監査を定期実施。
個人情報保護				
	25	個人情報保護について第三社認証を取得している。	○	プライバシーマーク取得済。
	26	個人情報保護方針をサービス利用者に開示している。	○	弊社Webサイトから閲覧可能。
	27	個人情報保護に関連する法令および規制が適用される場合は、その要求に従って対応できるか。	○	対応可能。
	28	サービス内で個人情報を取得する。	○	ログインIDのメールアドレス、ログデータ、添付ファイルなど。
	29	サービス利用者の個人情報及び預託データを自社利用の有無。	○	無。サービス利用者自身の利用のみ。
	30	個人情報及び預託データは日本国内のみで扱われ、他国に移転されることはない。	○	日本国のみ。
情報セキュリティ認証				
	31	ISMS（ISO 27001）の認証を取得している。	○	取得済。
	32	ISMSクラウドセキュリティ（ISO 27015）の認証を取得している。	○	取得済。
外部委託				
	33	他の事業者/システムとの間でサービス連携を行い、受託する一部業務について外部へ再委託を行っている。	○	有。「自動文字起こしエンジンのAPI連携」と「手動清書業者」で連携。
	34	外部委託先選定基準を定め、手順に則った委託先を選定している。	○	実施している。
	35	外部委託先に対して自社と同等基準の情報セキュリティを要求、合意している。	○	実施している。
	36	外部委託先に対して定期的なセキュリティ評価を実施している。	○	実施している。
サポート・情報通知				
問合せ先				
	37	メール	○	cs@zi-ku.com
	38	電話	○	03-5488-6067
サポート受付時間帯				
	39	一般問合せの受付時間帯	○	平日（祝日を除く月曜日～金曜日）午前10時～午後5時。メール及び電話で受付。
	40	障害対応の受付時間帯	○	平日（祝日を除く月曜日一金曜日）午前10時から午後5時。メール及び電話で受付。 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実施。
サービス品質				
可用性				
	41	サービスの提供時間帯	○	365日/24時間（※計画メンテナンス時を除く）
	42	サービス稼働率	○	99%
	43	定期/不定期の保守停止に関する事前連絡通知	○	1週間以上前にメールで通知。
	44	サービス提供を終了する場合の事前連絡確認	○	3か月以上前に事前にメール及びホームページで通知。
	45	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）	○	物理的に異なるリージョンからのリカバリを実施。 リカバリには1日程度を想定。 状況把握次第サービス利用者へメールで通知。
	46	重大障害時の早期復旧が不可能な場合の代替措置	○	回収できるデータをファイルを物理メディア格納またはダウンロードできる環境を提供。
	47	代替措置で提供されるデータ形式	○	CSV、TXT、FLAC、JPEGなどアップロードされているデータ形式にて提供。
	48	クライアントアプリケーションの更新	○	1ヶ月に1～4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。
	49	クラウドのシステム更新管理/パッチ管理	○	1ヶ月に1～4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。
信頼性				
	50	障害発生から修理完了までの平均時間(MTTR：修理時間の和÷故障回数)	○	非公開
	51	障害発生からサービス再開までの目標時間（RTO）	○	24時間

52	1年間に発生した障害件数	○	0件
53	1年間に発生した、復旧まで1日以上かかった障害件数	○	0件
54	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。ハードウェア／ネットワーク／パフォーマ ンスの監視。一定の数値を超える場合は管理者にメール通知。
55	障害発生時の通知プロセス	○	メールとウェブサイトにて通知。
56	異常検出後に指定された連絡先に通知するまでの時間	○	1時間
57	障害インシデントを収集/集計する時間間隔	○	5分
58	サービス提供状況を報告する方法	○	必要時にサービス内の通知エリアとメールで報告。
59	サービス利用者に提供可能なログの種類	○	ログの作成日時、編集ログ、ログイン履歴など。
性能			
60	処理の応答時間	○	UIの無応答時間5秒未満。
61	処理の応答時間の遅延継続時間	○	24時間
62	バッチ処理(一括処理)の応答時間	○	現在サービス利用者用のバッチ処理機能なし。
拡張性			
63	カスタマイズが可能な機能	○	ユーザー辞書機能。
64	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)	○	外部連携のAPI機能なし。
65	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	○	原則、同一IDに対しては同時に1ログイン。別IDの同時接続制限数なし。
66	ディスク容量の上限/ページビューの上限	○	現在はクラウド保存容量及びページビューの制限なし。(将来変更の可能性あり)
Ⅱ.セキュリティ			
セキュリティ			
セキュリティー般			
67	サービスに対する不正な侵入、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。	△	2022年度早期に第三者機関の監査を計画。
68	提供者側でのデータ取扱環境が適切に確保されている。	○	ISO27001 / ISO27015で定めた方針に準拠。
69	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。	○	ISO27001 / ISO27015で定めた方針に準拠。
70	異なる利用企業間の情報隔離、障害等の影響の局所化。	○	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。
71	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。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。	○	利用者からの依頼があった場合に、システム責任者のみ利用者のデータにアクセス可能。
72	ウイルススキャン対応。	○	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。
73	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。	○	日本国の個人情報保護法に準拠して運用。
74	弊社オフィスの入退室記録。	○	実施している。
ログ			
75	サービス利用者の利用ログを保存している。	○	有。
76	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を利用者ログ検索に利用できる。	○	ユーザーID、デバイスID,目的ごとのデータにそれぞれIDが設定されており、トレース可能。
77	システム運用に関するログを保存している。	○	有。
暗号化			
78	通信の暗号化レベル。	○	SSL暗号通信。
79	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。	○	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でのみ扱うため、ローカルメディアへのバックアップは実施なし。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。
80	データベースへの暗号化措置の有無。	○	有。
アクセス制限			
81	サービス利用者の接続元IPアドレスによる接続経路制限の有無。	○	有。(※サービス利用者が希望した場合)
82	ログイン後一定時間以内に操作が無かった場合には、セッションを切り再度ログインを要求しているか。	○	有。
83	利用者自らによるパスワード変更を可能としているか。	○	可能。
84	多要素認証やシングルサインオン、2段階認証等の適切な認証機構を用いているか。	X	今後実装予定。
Ⅲ.データ管理			
データ保守・管理			
バックアップ			
85	バックアップ周期と時刻(RPO)	○	毎日AM5時。
86	バックアップ保存期間と世代数。	○	2週間、14世代。
87	バックアップデータへのサービス利用者のアクセス。	○	利用者はアクセス不可。バックアップは障害対策用で弊社の限られたエンジニアのみアクセス可能。
データ管理			
88	データを保護のための暗号化要件の有無。	○	有。ストレージレベルで暗号化。
89	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。用途ごとに独立したキーを設定。
90	データ漏えい・破壊時の補償/保険の有無。	○	有。サイバー保険加入済。
91	入力データ形式の制限機能。	○	有。サービスが必要とするバリデーションを実行。
データ消去			
92	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。	○	解約後、一定期間経過後に該当データがクラウドサーバーから消去される。
93	データ消去証明書の発行の可否。	○	発行可能。
94	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の有無。	○	有。