サービス名：LogiMeets（ロジミーツ）
提供者：株式会社テクイット
最終更新日：2026年11月10日

クラウドサービスレベルのチェックリスト　回答書

本書は、経済産業省「クラウドサービスレベルのチェックリスト」の項目に沿って、LogiMeetsの対応状況を回答したものです。「有無」欄の「ー」は、有無ではなく内容で回答する項目です。目標値と記載したものは保証値ではありません。

No.	サービスレベル項目	規定内容	有無	回答
可用性				
1	**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）	ー	24時間365日（計画停止・障害発生時を除く）。サービスを停止する保守は、原則として利用の少ない深夜帯（0:00～6:00）に行います。
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	サービスを停止する保守は、原則として7日前までにサービス内のお知らせおよびメールでご案内します（緊急の対応を除く）。
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	利用規約第7条に基づき、サービスを終了する場合は事前にウェブサイトへの掲載または通知を行い、相当な周知期間を設けます。
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	無	万一サービスが停止した場合に備え、お客様はいつでもシップメント一覧（Excel形式）と書類の原本ファイル（ZIP形式で一括）をダウンロードし、手元に保存できます。なお、プログラムの第三者機関への預託（ソフトウェアエスクロー）は行っていません。
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）	ー	月間99.5%以上の稼働率の維持に努めています（計画停止を除く）。稼働率の保証（SLA）ではありません。過去1年間、サービスが停止する障害は発生していません。
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	データベースは毎日、書類・画像のファイルは随時、サーバーとは別の保管先（Amazon S3 東京リージョン）に保存しています。サーバーが被災した場合は、別のサーバーを用意してバックアップから復旧します。復旧手順を文書化し、年1回、バックアップからの復旧訓練を行います。
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	サーバーの障害で長時間ご利用いただけない場合は、ご依頼に応じて、お客様の書類の原本ファイルを当社からお届けします。書類はサーバーとは別の保管先（Amazon S3）に保存しているため、サーバーに障害が起きても書類のデータはそのまま残ります。
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	書類は、アップロードされた形式（PDF・Excel・Word・画像等）のまま、ZIP形式にまとめてお届けします。
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	機能の追加・改善は随時リリースします。利用方法に影響する変更は、サービス内のお知らせでご案内します。OS・ミドルウェア・ライブラリの更新は月1回確認して適用します。重大な脆弱性が公表された場合は、1営業日以内に影響を確認し、原則として3営業日以内に修正または回避策を適用します。
信頼性				

No.	サービスレベル項目	規定内容	有無	回答
10	**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）	―	過去1年間に障害が発生していないため、実績はありません。
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	―	通常の障害：4時間以内。サーバーの再構築を伴う場合：24時間以内（いずれも目標値）。
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	―	過去1年間：0件（対応に1日以上を要した障害：0件）。
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	監視サービス（Mackerel）で、サーバーの死活、CPU・メモリ・ディスクの使用率（80%で警告、90%で重大）、および外部からのサービス応答（https://logimeets.jp への外形監視）を24時間自動で監視し、異常を検知すると担当者に通知します。
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	お客様の業務に影響する障害が発生した場合は、サービス内のお知らせおよびご登録のメールアドレスへご連絡し、復旧時にも改めてお知らせします。
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	―	営業時間内は判明から1時間以内、営業時間外は翌営業日の午前中までにご連絡します（目標値）。
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	―	1分間隔。
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	無	定期的な報告は行っていません。障害・保守の情報はサービス内のお知らせでご案内します。
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	ご依頼に応じて、Webサーバーのアクセスログ（日時・IPアドレス・アクセス先等、直近90日分）から、お客様の会社に関する記録を抽出して提供します。他社の情報は含めません。
性能				
19	**応答時間**	処理の応答時間	―	保証値は定めていません。
20	**遅延**	処理の応答時間の遅延継続時間	―	保証値は定めていません。
21	**バッチ処理時間**	バッチ処理（一括処理）の応答時間	―	保証値は定めていません。書類のAI解析は、アップロード後に順次処理します。
拡張性				
22	**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	無	お客様ごとの個別カスタマイズは行っていません。機能のご要望は承ります。
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）	無	外部向けのAPIは公開していません。データはExcel・ZIP形式でダウンロードできます。
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	―	同時接続数の制限はありません。登録できるメンバー数・社外メンバー数は、ご契約のプランごとに定めています。

No.	サービスレベル項目	規定内容	有無	回答
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	―	書類の保存容量に上限は設けていません（通常の業務利用が前提。利用規約第9条）。1ファイルあたりのアップロードは20MBまでです。
サポート				
26	**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	―	平日9:00～19:00（土日祝日・年末年始を除く）。お問い合わせフォームまたはメール（support@logimeets.jp）で受け付けます。
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	―	平日9:00～19:00（土日祝日・年末年始を除く）。通常1～2営業日以内に回答します。
データ管理				
28	**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	データベースは毎日バックアップを取り、Amazon S3（東京リージョン）に保存しています。書類・画像のファイルはAmazon S3に保存し、AWS Backupで毎日バックアップを取っています。あわせてバージョニング（版の保持）を設定しているため、誤って上書き・削除された場合も以前の状態に戻せます。復旧は当社が行います。
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	―	データベース：24時間（毎日午前3時にバックアップ）。書類・画像のファイル：バージョニングにより、変更・削除の直前の版まで復旧できます。
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	―	データベースのバックアップ：30日間。書類・画像のバックアップ（AWS Backup）：14日間。書類・画像の以前の版：30日間。いずれも経過後は自動的に消去します。
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	退会後は、取引内容の確認や法令に基づく保存等に必要な期間データを保持し、その後削除または匿名化します。ご依頼があれば、法令上保存が必要なもの等を除き削除します。バックアップ内のデータは30日以内に自動的に消去されます。
32	**バックアップ世代数**	保証する世代数	―	データベース：30世代（1日1世代）。書類・画像：14世代（1日1世代）。
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	通信はTLS 1.2／1.3で暗号化しています。書類・画像のファイルとバックアップは、保管先（Amazon S3）で保存時に暗号化しています。パスワードはハッシュ化して保存しています。クレジットカード番号は決済代行（Stripe）が管理し、当社では保持しません。
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	無	お客様ごとの暗号鍵の管理は行っていません。保管先での暗号化には、Amazon S3が管理する鍵を使用しています。
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	無	サイバー保険には加入していません。損害賠償の範囲は利用規約の定めによります。
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	解約前に、シップメント一覧（Excel）と書類の原本ファイル（ZIP）をお客様ご自身でダウンロードできます。退会後のデータは、ご依頼に応じて削除します。

No.	サービスレベル項目	規定内容	有無	回答
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	書類はアップロード時にファイルのハッシュ値（SHA-256）を記録し、版ごとにアップロードした利用者・日時とともに保持しています。定期的な検証報告は行っていません。
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	アップロードできる書類は、PDF・画像・Excel・Word・CSV・テキスト・ZIP・メール形式に限っており、実行形式のファイルは受け付けません。1ファイルあたり20MBまでです。各入力項目は形式を検証しています。
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	無	ISMS（ISO/IEC 27001）、プライバシーマークは取得していません。
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	無	第三者による脆弱性診断は実施していません。
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	当社がお客様のデータを確認するのは、お問い合わせ・不具合への対応など、サービスの提供に必要な場合に限ります。運営の管理画面は許可した固定IPアドレスからのみ接続でき、ログイン前の追加認証を設け、ログインをすべて記録しています。サーバーへのリモート接続（SSH）も許可した固定IPアドレスに限っています。サーバー事業者の管理パネルと、書類の保管先であるAWSの管理画面へのログインには二要素認証を設定しています。
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	TLS 1.2／1.3のみに対応しています（TLS 1.0／1.1は無効）。暗号方式はAES-256-GCM等を使用しています。
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」	無	SOC報告書等の監査報告書は提供していません。
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	データは会社ごとに分けて管理し、すべての画面・ダウンロードで閲覧権限を確認しています。他社のデータを閲覧することはできません。書類のファイルは外部から直接開けるURLを持たず、権限の確認後にのみ取り出せます。
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	会社の管理者が、メンバーの招待・権限設定・利用停止を行えます。書類は「自社のみ」「連携先と共有」を書類ごとに選べ、共有したものだけが取引先に表示されます。社外メンバー（通関業者等）は招待されたシップメントのみ閲覧でき、権限は「閲覧のみ」「編集」から選べます。
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、受容可能な期間内に提供されるか	有	IDは利用者ごとに付与しています。ログイン時の端末・IPアドレス・日時、書類の版ごとのアップロード者・日時を記録しています。Webサーバーのアクセスログは90日間、管理画面のログイン記録は1年間保存します。調査が必要な場合は、ご相談に応じて提供します。

No.	サービスレベル項目	規定内容	有無	回答
47	**ウイルススキャン**	ウイルススキャンの頻度	無	アップロードファイルのウイルススキャンは行っていません。実行形式など業務書類以外の形式のアップロードを拒否し、Excel・Wordのプレビューはファイル内のプログラムが動作しない形で表示しています。
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	バックアップはAmazon S3に暗号化して保管しており、物理的な記録媒体は使用していません。お客様のデータを外部記憶媒体（USBメモリ等）に保存することを禁止し、業務端末には画面ロックを設定しています。
49	**データの外部保存方針**	データ保存時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	有	サーバー（エックスサーバーVPS）と書類の保管先（Amazon S3 東京リージョン）は日本国内です。書類のAI解析（OpenAI、Google Cloud Vision）、決済（Stripe）、コンテナ追跡、画面のリアルタイム更新（Pusher）では海外の事業者に必要な情報を送信するため、各国の制度を把握したうえで利用しています。AIサービスは、送信した情報がAIの学習に利用されない条件で利用しています。

関連資料

- セキュリティへの取り組み：https://logimeets.jp/security
- 情報セキュリティ基本方針：https://logimeets.jp/security/policy
- 利用規約：https://logimeets.jp/terms　／　プライバシーポリシー：https://logimeets.jp/privacy-policy

お問い合わせ：support@logimeets.jp