サービスレベル（チェック項目）

No.	種別	サービスレベル項目	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	時間帯	事前連絡による計画停止を除く、24時間365日
2	可用性	計画停止予定通知	定期的な保守停止に関する事前連絡	有無	（有）1週間前～1ヶ月前に管理画面内およびWebサイトにて通知
3	可用性	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	有無	（有）3ヶ月～1年程度前に管理画面内およびWebサイトにて通知
4	可用性	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）現時点で終了及び預託などの予定はございません。
5	可用性	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 (%)	2023年の1年間の実績値は99.99%になります。
6	可用性	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）本システムは、当社契約のデータセンターに構築し運用しています。 全てのサーバー、ストレージは冗長構成となっています。
7	可用性	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）日次で取得し、遠隔地での保管を実施しています。遠隔地での保管に関しても、バックアップメディア専用の保管施設にて厳重に管理を行っており、3ヶ月間保管しています。
8	可用性	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	（無）
9	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）アップグレード及び追加機能などは随時更新しております。会員への影響度合いに応じて、管理画面内およびWebサイト及びメールにて通知
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	信頼性	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	信頼性	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1日以上要した障害件数	件	非公開／0件
13	信頼性	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）死活監視、パフォーマンス監視、エラー監視を実施しております。
14	信頼性	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）弊社システム担当者へ通知され、会員への通知は、必要に応じて、管理画面内およびWebサイト及びメールにて通知
15	信頼性	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	弊社システム担当者への通知は1～3分以内に行われます。お客様への通知は可能な限り迅速に行います。
16	信頼性	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	5分間隔
17	信頼性	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、管理画面内およびWebサイト及びメールにて通知
18	信頼性	ログの取得	会員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）赤入れダウンロードログ／データ削除ログ
19	性能	応答時間	処理の応答時間	時間	非公開
20	性能	遅延	処理の応答時間の遅延継続時間	時間	非公開
21	性能	バッチ処理時間	バッチ処理（一括処理）の応答時間	時間	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）
23	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	（無）
24	拡張性	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	制限無し
25	拡張性	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	有無	プランに応じて有り／ページビューの上限は無し
			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	平日10時～12時、13時～18時※弊社休業日は除く
27	サポート	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10時～12時、13時～18時※弊社休業日は除く
			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）日次で取得し、1ヶ月間データセンターにて保管いたします。 バックアップデータへのアクセスは、一部の当社システム管理者のみがアクセス可能です。
29	データ管理	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	当日22時ごろ
30	データ管理	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	1ヶ月間
31	データ管理	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ヶ月後に自動的にデータ消去されます。
32	データ管理	バックアップ世代数	保証する世代数	世代数	日次バックアップを1ヶ月間保管（30世代）
33	データ管理	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）データは、サーバーサイドで暗号化して保存されています。 パスワードなどの情報はアプリケーションレベルにて暗号化して保存されています。
34	データ管理	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）テナントIDによりデータを論理的に分離して管理しています。
35	データ管理	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）
36	データ管理	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）サービス解約時にデータは削除されます。 データは暗号化して保存されているため、解約後の復旧はできません。
37	データ管理	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）送信時に検証を行っています。データベースのトランザクション制御や外部キー制約を利用し、通信経路はTLSにより盗聴、改ざんを防いでいます。SSLによる暗号化を行っており、TLS1.2未満の通信は無効としています。
38	データ管理	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）データ送信時に検証を行っています。
			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	（無）
40	セキュリティ	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）
41	セキュリティ	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）データへのアクセスは、システム管理者権限を有する役員または社員のみが可能のみに制限されています。それ以外の全社員は本システムのサーバーへのログイン情報を知ることができません。
42	セキュリティ	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による暗号化を行っており、TLS1.2未満の通信は無効としています。
43	セキュリティ	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	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	（有）テナントIDによりデータを論理的に分離して管理しています。
45	セキュリティ	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業務上必要な一部の開発者のみに制限されています。また、ファイアーウォールにて弊社環境からのみのアクセス制限を実施しています。
46	セキュリティ	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	IDは1会員単位で発行して管理しています。また、アクセスログは無期限で保存しておりインシデント発生時の調査が可能です。ログの提供は行っておりません。
47	セキュリティ	ウイルススキャン	ウイルススキャンの頻度	頻度	サービスコンテナの脆弱性スキャンを日次で行っています。

48	セキュリティ	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）二次記憶媒体の利用を禁止しています。
49	セキュリティ	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を把握しています。