

No.	種別	サービスレベル項目	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日です。(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	無 計画停止の通知は行いません。 日本時間午前4時頃実施。
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 現時点で終了の予定はありませんが、1ヶ月程度前にメール、SNSおよびWebサイトで通知する予定です。
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 現時点で終了予定はなく、プログラムやデータの預託も未定です。
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 (%)	99.87%。
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 各サーバー冗長構成によりホットスタンバイサーバーを用意し、問題があれば ALB の設定にて切り替えが可能。
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
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 RDS のバックアップ。
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 脆弱性に対する修正プログラムについては daily で自動更新、ミドルウェアが多いサーバに関しては、weekly で目視で更新確認しております。
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	1時間です。
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	6 時間以内を目標としております。
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	回数としては公開していませんが、個別の障害情報はWebサイトで公開しております。 https://status.ovice.io/
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 AWS CloudWatch によるシステム障害監視&通知を実施、対応マニュアル、管理体制を整備。
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 SNS で告知。 以後進捗があり次第随時更新。
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	弊社システム管理者への通知は検知後 1 時間以内、その後復旧まで随時監視。
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)	弊社システム管理者への通知は検知後 1 時間以内、その後復旧まで随時監視。
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	必要に応じてメール、Webサイト、SNSで行います。

No.	種別	サービスレベル項目	規定内容	測定単位	設定
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 アクセスログに関しては、管理者権限のユーザは管理者メニューの「ユーザーログ」機能で下記のような項目を確認することが可能です。 ・アクション(オンライン、オフライン等) ・名前 ・メールアドレス(ユーザID) ・IPアドレス ・日時 ※CSVファイルでダウンロードも可能です。
19	性能	応答時間	処理の応答時間	時間(秒)	3秒
20		遅延	処理の応答時間の遅延継続時間	時間(分)	1秒
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)	10秒以内(CSVダウンロードを想定)
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	有 管理者メニューによりユーザの権限設定、スペースの背景設定、スペース上の会議室、固定オブジェクト等の追加・変更が可能です。
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)	有無	有 Webhookを利用し、外部システムに通知を送ることが可能です。
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	有無(制約条件)	有 ご利用のプランにより推奨利用人数が異なります。
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	無 リソースの制限はございません。
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
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10:00-12:00、13:00-16:00 ※日本時間(JST)での提供となります。
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 日次でバックアップを取得しています(世代数は7まで)。バックアップデータへのアクセスは一部の開発者のみに制限されています。
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取り、データを保証する時点	時間	毎日深夜に実施しております。
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	時間	7日間保管しています。
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	有無	有 要請に応じてサービス解約時にデータの消去が可能です。
32		バックアップ世代数	保証する世代数	世代数	7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	無 顧客データはテナント毎にサブドメインで分離しています。
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	有無	有 サイバーセキュリティ保険に加入しています。

No.	種別	サービスレベル項目	規定内容	測定単位	設定
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	無 要請に応じてサービス解約時にデータの消去・返却が可能です。
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 通信経路はTLS1.2により盗聴、改ざんを防いでいます。
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 金額、住所、電話番号等のフォームにおいて、想定外のデータ入力ができないよう制御を実施しています。
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	有 ISMS認証(ISO27001)を取得しています。(認証番号 IA210152)
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	有 定期的(1年)に第三者機関によるセキュリティ監査を実施しております。
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 開発体制と保守体制を分離、重要情報へのアクセスは最低限の人員に制限しています。
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 すべての通信がSSLで行われており、TLS1.2以上を使用しております。
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 他利用者とはサブドメインで分離しております。
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 開発体制と保守体制を分離、重要情報へのアクセスは最低限の人員に制限しております。
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	1人1IDを発行しておりますが、ログは取得していない為、操作ログを追跡することはできません。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	ウイルススキャンは全サーバーで一日一回実施しており、パターンファイルはリアルタイムで更新しております。
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 二次記憶媒体の利用を禁止しています。
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	バックアップを含め、データ保存はAWSの東京リージョンに限定しています。

版番号	発行年月日	改訂内容
1	2021/08/26	初版
2	2021/11/27	No.33 データ保護のための暗号化要件を更新
3	2022/11/01	<ul style="list-style-type: none">・ No.12 障害発生件数のURLを更新・ No.23 外部接続性のURLを更新・ No.27 サービス提供時間帯(一般問合せ)を更新
4	2023/03/01	<ul style="list-style-type: none">・ No.14 障害通知プロセスの告知方法を更新・ No.18 ログの取得のユーザーログ項目を更新・ No.23 外部接続性のURLを更新・ No.27 サービス提供時間帯(一般問合せ)を更新
5	2023/04/12	<ul style="list-style-type: none">・ No.23 外部接続性を更新・ No.24 同時接続利用者数を更新