

No.	種別	サービスレベル項目例	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 弊社サービスの提供に影響がある変更はサービス内で告知しております。 また下記URLでも告知しております。 https://status.social-dog.net/
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	無 サービス終了時の事前連絡時期は現時点では規定しておりません。
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 現時点ではサービス提供停止を想定していないため、預託については未定となっております。
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(%)	公開しておりません。
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	有無	有 DBを日次でバックアップしており7世代分まで保存されています。 復旧のプロセスについて明文化しています。
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	無
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)	無
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 機能追加・不具合修正など随時行なっております。 また、影響が大きい変更に関してはサービス内で告知をするなどして周知しております。
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	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	主要な機能とDBに関しては12時間以内、それ以外については7日以内となっております。 主要な機能とは「SocialDogへのログイン、分析結果の表示、ユーザー情報の取得、予約投稿、キーワードモニター、いいねやフォローなどのアクション、プラン情報や請求履歴の確認、Twitterアカウントの連携や確認、SocialDogアカウントの設定確認・変更、パスワードの変更」です。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定
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	公開していません。
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	死活監視、パフォーマンス監視、障害監視、トラフィック監視を行なっております。
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	有 Slack経由で弊社担当者に通知されます。 ユーザー様への通知は必要に応じてサービス内、公式Twitterアカウントで行っています。 また下記URLでも障害発生を告知しております。 https://status.social-dog.net/
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	障害発生後数分以内に弊社担当者に通知されます。
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)	1分毎に障害監視が行われています。
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	適宜サービス内や公式Twitterアカウントによって提供状況を告知しております。 また下記URLでも告知しています。 https://status.social-dog.net/
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	無 ユーザー様にログの提供は行なっておりません。
19	性能	応答時間	処理の応答時間	時間(秒)	公開していません。
20		遅延	処理の応答時間の遅延継続時間	時間(分)	公開していません。
21		バッチ処理時間	バッチ処理(一括処理)の応答時間	時間(分)	公開していません。
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 ユーザー毎のカスタマイズ開発は対応しておりません。
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 API等は公開していません。
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ー数	有無(制約条件)	無 同時接続利用者数に制限はございません。
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	無 リソースの上限はございません。
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	平日10:00~18:00 ※日本時間(JST)での提供となります ※営業時間外は翌営業日以降のご連絡になります。 ※サポートはメールのみ対応しております。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定
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	No26と同様です。
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、利用者によるデータの取扱方法	有無/内容	有 DBデータは日次でバックアップを取得しています。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	DBバックアップは22:00~2:00(JST)の時間帯で取得しております。
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	現時点でバックアップは7日間保存しております。
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、利用者によるデータの消去方法	有無	無
32		バックアップ世代数	保証する世代数	世代数	7世代分までバックアップしております。
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 パスワードなどの機密性の高いデータは暗号化して保存しております。
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	有 ユーザー毎のIDによってデータを論理的に分離し管理しております。
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	無
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
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 入力データのバリデーションを適宜行なっております。またデータ通信にはTLSを使用し盗聴、改ざんの防止をしております。
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 入力データの形式チェックを適宜行なっております。
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認証を取得しています。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定
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	無
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 データアクセスは一部の開発者のみが行えるように制限しております。
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 TLS1.0以上を使用しています。
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」	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 アカウントIDにより情報を論理的に分離しています。
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 業務上アクセスが必要な開発者のみデータアクセスできるように制限しています。
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	ユーザー毎にIDを発行しています。IDを元にログを検索しインシデント発生原因の特定に活用可能です。 ログの保存期間は3ヶ月となっております。 ユーザー様へのログの提供は行っておりません。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	無
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 原則USBなどの持ち運び可能な二次記憶媒体の使用は禁止しております。 使用する際には社長へ申請し、暗号化やパスワードを設定するようにしております。 利用用途の終了後は速やかに削除するようにしております。
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	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。