

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。(定期メンテナンス等の計画停止を除く)
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 年間メンテナンススケジュールの通知及び1週間以上前の事前通知を実施しています。現状、メール及びサポートサイトにて通知しています。
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ヶ月間以上の予告期間において、お客様に事前通知いたします。メール及びサポートサイトにて通知する想定です。
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 (%)	99.6%/年(サーバ保守のための本サービス停止時間を除く。)
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 サーバーは冗長化して運用しています。
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	有 日次でデータをバックアップを行い世代管理をしデータセンターに保管しています。またシステム構成はコード化して管理しており、迅速な復旧が可能です。
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	有無 (ファイル形式)	有 万が一に備えお客様側で管理画面よりデータをCSV形式でダウンロードすることが可能です。
9		アップグレード方針	バージョンアップ/変更管理/ バッチ管理の方針	有無	有 機能追加やバッチ適用は随時行っております。お客様への影響が大きい変更については、事前にメール及びサポートサイトで告知を行います。
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	4時間
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	公開しておりません。
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	有 死活監視、パフォーマンス監視、エラー監視を行っております。
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 メールにて弊社担当者に通知されます。お客様への通知は必要に応じてメール、サポートサイトで行います。
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	時間	弊社担当者への通知は数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		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)	5分間隔です。
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	個別の報告はしておりませんが必要に応じてメール、サポートサイトで行います。
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)	有無	有 重要なリソースへの操作を監査ログ機能として提供しております。
19	性能	応答時間	処理の応答時間	時間 (秒)	公開しておりません。
20		遅延	処理の応答時間の遅延継続時間	時間 (分)	公開しておりません。
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)	公開しておりません。

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	有 設定画面より一部の設定画面より項目追加・編集・計算式設定などが可能です。
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 現状一般向けのAPIは公開しておりませんが、各種クラウドサービスとの連携強化は図っていく予定です。 https://kinrou44.jp/faq/
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)	無 同時接続利用者数の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	(電話) 10:00～18:00 ※土日祝日及び当社が定める休日を除く (メール)24時間365日受付
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	(電話) 10:00～18:00 ※土日祝日及び当社が定める休日を除く (メール)24時間365日受付
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 週次でフルバックアップ、日次で差分バックアップを取得しデータセンターに保管します。復旧方法については定められた手順に基づいて行います。バックアップデータへのアクセスは限定された管理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	午前4時
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	1週間分
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 利用契約の終了後1ヶ月以内に保存データを削除します。
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 ご要望に応じて、暗号化データベースをご利用いただけます(有償対応)
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 法人コード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 損害保険に加入しています。
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	有無/内容	有 利用契約の終了後1ヶ月以内に保存データを削除します。 必要に応じてサービスの契約終了前にデータをCSV形式でダウンロードいただけます。
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 データの整合性検証を行っております。通信経路はTLS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 入力項目の要件に合わせて形式や長さのチェックを行っています。

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	有 ・プライバシーマークを取得しています。登録番号:10822550 ・ISMS認証(ISO27001)を取得しています。認証番号:IS609954
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 クラウド型脆弱性診断ツールを使用した脆弱性診断を定期的の実施しています。
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 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。
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 基本的にサービスとの通信はTLS 1.2にて暗号化しています。 ※打刻専用機の一部で、TLS1.0、1.1を利用しておりますが、今後禁止にしていく予定です。
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 法人コードによりデータを論理的に分離して管理しています。
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 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。
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	保管しているログから調査可能です。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	開発・運用に利用するマシンはリアルタイムスキャンを有効化し随時検索しています。
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	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。