| 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(計画停止時間を除く) |
| 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<br>毎月 第3木曜日 AM1:00からAM7:00まで(JST)<br>実施の10営業日前までに、SONAR内のインフォメーションに掲載もしくはメールにて通知 |
| 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<br>半年程度前にサービス内インフォメーションにて告知する |
| 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<br>プログラム及びデータ預託の計画無し |
| 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 (%) | 年間*使用可能時間割合99.0%を保証<br>* サービス稼働率の年間とは、1月1日から12月31日（JST）の期間を意味します |
| 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<br>Webアプリケーション・データベース・ストレージはMicrosoft Azureの複数リージョンによる地理冗長化構成とし、フェイルオーバーで復旧 |
| 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<br>バックアップ環境の西日本リージョンでサービスを再開するBCP計画を策定、年1回以上復旧テストを実施 |
| 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<br>全情報をCSV形式、物理ファイルをZIP形式でダウンロード可能 |
| 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<br>ISMS規程に準じたシステムの開発及び変更管理の運用手順（変更・リリースフロー）に従い随時アップデートを実施 |
| 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 | | 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 | | 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 | 回数は非公開<br>正確な情報提供を行うべく、サービスヘルスサイトを準備中 |
| 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<br>死活監視、パフォーマンス監視、ログ監視、エラー監視 |
| 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<br>システム稼働状態を常時リソース監視、アラートをメール及び携帯電話へ通知、ISMSで規程する緊急連絡体制に従った連絡を実施 |
| 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 | 10分以内 |
| 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 |
| 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 | 必要に応じてサービス内インフォメーション、専用ガジェットなどで告知 |
| 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<br>アプリケーションの操作ログを抽出・表示する機能を提供 |
| 19 | 性能 | 応答時間 | 処理の応答時間 | 時間 (秒) | 非公開 |
| 20 | | 遅延 | 処理の応答時間の遅延継続時間 | 時間 (分) | 非公開 |
| 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) | 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 | 有<br>画面上に表示する項目、参照可能な情報、利用可能な機能などの設定が可能 |
| 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<br>APIを公開<br>https://sonar-developers.snar.jp/ |
| 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<br>同時接続可能なユーザー数の制限無し |
| 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 | 有<br>専用ストレージに利用上限の制限あり |
| 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10:00～17:00<br>年末年始・祝日を除く |
| 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10:00～17:00<br>年末年始・祝日を除く |
| 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 | Microsoft Azure SQL Databaseで完全バックアップを毎週、差分バックアップを 12 から 24 時間ごと、そしてトランザクション ログ バックアップを 5 から 10 分ごとに作成<br>バックアップデータへの取り扱いは運用責任者および運用責任者が指名した担当者に限定 |
| 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 | 時間 | バックアップデータ保存期間の任意の時点に復元可能 |
| 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 | 35日間 |
| 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<br>サービス解約より一定の期間が経過した後データの削除を実行 |
| 32 | | バックアップ世代数 | 保証する世代数 | 世代数 | 35日分 |
| 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<br>データベースストレージの暗号化を実施、パスワード等一部のデータは不可逆の暗号化で保存 |
| 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<br>テナント固有のIDでデータを論理的に分離 |

| | | | | | |
|---|---|---|---|---|---|
| 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<br>サイバー保険加入 |
| 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<br>サービス解約より一定の期間が経過した後データの削除を実行、バックアップを含め約35日経過で完全消去 |
| 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<br>データ入力時、送信時に検証、通信経路での盗聴、改ざんを防止するためにTLSにより保護 |
| 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<br>データ入力時、送信時に検証 |
| 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<br>（ISMS、プライバシーマーク等）が取得されていること | 有無 | 有<br>ISMS (ISO/IEC 27001:2013) 認証<br>ISMS-CS (ISO/IEC 27017:2015) 認証<br>ISMS-PIMS (ISO/IEC 27701:2019) 認証<br>を取得<br>登録番号：JUSE-IR-467、JUSE-IR-467-CS01、JUSE-IR-467-PI01<br>有効期間：2020年12月21日～2023年12月20日（2021年12月20日改訂） |
| 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<br>外部診断会社によるアプリケーションの脆弱性診断を実施<br>全体：年一回<br>リリース単位：月一回 |
| 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<br>データベースへのアクセスは業務上必要な担当者へ作業申請の承認経て必要最低限のアクセス権を付与する |
| 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<br>ウェブアプリケーション上の通信はTLS1.2以上での暗号化を強制 |
| 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<br>「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<br>テナントIDによりデータを論理的に分離 |
| 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<br>データアクセス権は業務上必要最低限の開発者のみに制限 |
| 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 | IDは個人ごとに発行、管理<br>アクセスログは1年以上保管 |
| 47 | | ウイルススキャン | ウイルススキャンの頻度 | 頻度 | 全てのPCにてウイルス定義の定期更新、リアルタイムスキャンの有効化、状態の中央管理を実施 |
| 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<br>セキュリティ管理ソフトウェアのグループポリシー設定にて二次記憶媒体の利用を禁止 |
| 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る |