

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
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 日提供しております(計画停止・定期保守による停止時間を除きます)。
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:計画停止を行う場合は、原則として実施 4 週間前までに管理画面およびサポートサイトに お知らせしております。
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: サービス提供を終了する場合は、少なくとも 60 日前までに管理画面およびサポートサイト等を通じてご案内しております。詳細は利用規約をご参照ください。
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:ソースコード等の預託制度は設けておりませんが、お客様データについてはサービス提供期間中いつでもエクスポート可能となるよう配慮しております。
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(%)	サービス稼働率の数値目標は対外的には公開しておりませんが、直近 1 年間の実績値は 99.9971% となっております。
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:全てのサービスを複数のデータセンターに分散配置し、1 日 1 回のデータベースバックアップおよびファイルの遠隔地保管を実施しております。
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:原則として冗長構成および復旧プロセスにより早期復旧を図っており、別途標準化された代替手段は設けておりません。長時間の停止が見込まれる場合には、お客様と協議のうえ可能な対応策を検討しております。
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)	無:上記のとおり標準の代替措置を定めていないため、代替措置時のデータ提供形式も個別協議としております。
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・改善およびセキュリティパッチの適用を順次実施しております。原則としてサービス停止を伴わない方式で行っておりますが、停止を伴う場合は No.1・No.2 に記載のとおり事前にご案内しております。
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	平均復旧時間は内部指標として計測・管理しておりますが、対外的には公開していません。
11		目標復旧時間(RTO)	障害発生後のサービスの再開に関して設定された目標時間	時間	障害発生後の目標復旧時間は内部で設定・管理しておりますが、対外的には公開していません。
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	障害発生件数については対外的に数値を公表しておりませんが、発生した障害の内容・影響・対応状況についてはサポートサイトに公開しております。 https://information.shanon.co.jp/hc/ja
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:ハードウェア、ネットワーク、パフォーマンス等について監視・アラート設定を行っております。
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	障害発生時には監視システムにて検知後、サポートサイトの障害情報ページへの掲載と、サポート登録されているメールアドレス宛への通知を行うプロセスを定めております。
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	有:サービス停止等の重大な障害を検知した場合は、原則として検知から 30 分以内に、サポート登録されているメールアドレス宛に通知しております。
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)	監視システムにより 3 分間隔で稼働状況を監視し、障害インシデントを収集・検知しております。
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	有:障害およびサービス稼働状況については、障害情報サイトに随時公開しております。 https://information.shanon.co.jp/hc/ja
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:お客様向けに生ログを直接ダウンロードいただく機能は提供しておりますが、管理画面上でログイン履歴、各種データの更新履歴、メール配信履歴などの履歴情報を確認いただけます。
19		応答時間	処理の応答時間	時間(秒)	応答時間については内部で監視・管理しておりますが、具体的な数値は対外的には公開していません。
20		遅延	処理の応答時間の遅延継続時間	時間(分)	応答遅延の継続時間については内部で監視・管理しておりますが、具体的な数値は対外的には公開していません。
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)	バッチ処理(一括処理)の所要時間については内部指標として管理しておりますが、対外的には公開していません。
22		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:管理画面からの項目追加・設定変更や、デザインテンプレートの適用などのカスタマイズが可能です。詳細はマニュアルをご確認ください。
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:外部システム連携用の Web API を提供しており、既存システムや他クラウドサービスとの連携が可能です。詳細な仕様については開発者向けドキュメントをご参照ください。
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)	同時接続可能なユーザー数については内部で管理しておりますが、対外的には公開していません。
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	有:ファイルアップロードについては 1 ファイルあたり 10MB、メールの添付ファイル総量で 5GB までを上限としております。詳細はマニュアルをご確認ください。
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	メールによる障害受付は 24 時間 365 日受け付けております。電話での障害窓口は、平日 10:00～18:00 となっております。
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	メールによる一般お問い合わせの受付は 24 時間 365 日受け付けております。回答および電話でのお問い合わせ対応時間は、平日 10:00～18:00 となっております。
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:当社では 1 日 1 回データベースのフルバックアップを取得しております。バックアップデータおよびファイルは遠隔地環境に複製して保管しており、災害時にも復旧可能な体制を整えております。
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とり、データを保証する時点	時間	原則として24時間以内のデータは保護されます。
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	30 日分を保存しております。
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、利用者に所有権のあるデータの消去方法	有無	有:契約終了後はデータを復元できない形で破棄しております。なお、バックアップデータについては保持期間満了後に自動的に削除されます。
32		バックアップ世代数	保証する世代数	世代数	30 世代(1 日 1 回のフルバックアップを 30 日分保持)を維持しております。
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:通信は TLS1.2 / TLS1.3 で暗号化しております。アプリケーションとデータベース間の通信も TLS で暗号化されております。
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:各テナント毎に論理的に分離された環境でデータを保護しております。
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	有:保険に加入しておりますが、補償内容の詳細は対外的には公開していません。
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	解約後のデータ返却は行っておりません。解約前に、管理画面よりデータをエクスポートいただく必要があります。
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:各種バリデーション機能および入力チェック機能により、データの整合性を保持する仕組みを提供しております。
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:各種入力項目に応じたバリデーションを実施しており、不正な形式のデータ登録を防止しています。
セキュリティ					
39		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 およびプライバシーマークを取得しております。詳細は以下をご参照ください。 https://www.shanon.co.jp/security/
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:専門業者による脆弱性診断を定期的に実施しております。
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:サーバにアクセス可能なメンバーは、必要最小限の運用担当者に限定しております。
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:TLS1.2 および TLS1.3 による通信の暗号化を行っております。
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、担当者以下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:現在、会計監査報告書において情報セキュリティ関連事項を個別に監査・報告する取り組みは実施しておりません。
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:テナント毎にデータを論理的に分離して保護しております。

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：サービスを利用するお客様向けには、ロールに基づいたアクセス権限設定を提供しております。当社は、障害対応など、業務上必要な場合を除き、お客様データへアクセスすることはありません。必要な際には申請に基づきアクセス権を付与する運用としております。
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	有：リクエストごとにIDを付与し、各種操作ログとともに記録・保管しております。これにより、インシデント発生時の追跡が可能となるようにしております。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	端末にはウイルス対策ソフトを導入しており、定期的なフルスキャンおよびリアルタイムスキャンを実施しております。サーバにもウイルス対策ソフトを導入しており、1日1回のスキャンを行っております。
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：バックアップデータは暗号化したうえで複数のデータセンター群に保管しております。世代管理は自動で行われており、保持期間を超過したバックアップは自動的に削除されます。 端末のUSBポートは原則として無効化しており、ストレージデバイスの接続を制限しております。
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	有：データ保存先の法制度や各種規制に基づくデータの取扱い・利用制限について把握したうえで、契約および利用規約に反映する運用としております。

※本資料に記載の機能および提供内容は、契約プランにより一部異なります。各項目に記載の内容は代表的な仕様であり、詳細はご契約プランの仕様に準じます。