

No.	種別	サービスレベル項目	規定内容	測定単位	設定
アプリケーション適用					
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/定期保守除く) サーバーの冗長構成により、点検/保守に伴う計画停止時間は発生しません。
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： 大規模な変更および定期メンテナンスの少なくとも48時間前までに電子メールでお客様に通知いたします。 小規模な変更については必要に応じて通知を行い、実施します。
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	無： 現時点でサービス終了予定および当該規定はございませんが、サービス終了の際は事前に電子メールでお客様に通知いたします。
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	有： ISL Onlineは、最先端グリッド技術で連結(冗長化)されたグリッドネットワークを利用して、世界中のどこからでも目的のPC/サーバまでの最適ルートを自動選択し、高速かつ安定した接続を提供するサービスです。グリッドネットワークには特定のサーバに集中したアクセスを他のサーバに分散処理する負荷分散機能と、接続サーバの偶発的トラブルの際にも他のサーバがセッションを維持する機能を備えていることで、安定したサービスを提供します。グリッドネットワークを構成するサーバ(主に日本、ドイツ、アメリカ)は常に同期されており、障害時は他のサーバからデータをリストアできます。
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(%)	2019年度(1月～12月)の実績は99.9846%です。
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： 万が一、日本のサーバ群(2020年4月23日現在10台)が災害や高負荷に見舞われても、他国の低稼働サーバ群からリソースをもらい安定稼働を維持します。
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： 個別のサーバのバックアップ周期や保管世代は公開しておりませんが、専用施設(ISMS、FISC準拠のデータセンター)に設置されたグリッドネットワークを構成する90台以上のサーバは常に同期されており、障害時は他のサーバからデータをリストアできます。
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： 代替措置で提供されるデータはございません。
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： 世界中に90台以上存在するサーバの冗長構成で順次アップデートを行います。バージョンアップ時のサービス停止時間はありません。 非公開です。
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	非公開です。
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	非公開です。
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	0回(1日以上対応を要した障害は発生していません)
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	有： システム監視には社内開発の監視ソフトを使用し、OSリソース、サービス、通信ポート等に対して実施されています。
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： 情報を有り次第、登録メールアドレスへの通知及びHPでの告知になります。
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	サポート提供時間帯は、1時間以内での通知を目標としています。
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)	非公開です。
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	障害発生時等、必要に応じてホームページ上に情報を掲載いたします。
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： サーバのログファイルは提供していませんが、製品の利用履歴はサーバからダウンロードすることができます。
19	性能	応答時間	処理の応答時間	時間(秒)	非公開です。
20		遅延	処理の応答時間の遅延継続時間	時間(分)	非公開です。
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)	非公開です。
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：
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等の公開はございません。	
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数	有無(制約条件)	無： 全世界で数万ユーザーが同時にサービスを利用しています。	
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	非公開です。	

No.	種別	サービスレベル項目	規定内容	測定単位	設定
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	月曜日～金曜日の9:30～11:45 13:00～17:30 (祝日・弊社休業日を除く) ※メール受付は24時間、対応は営業時間内に順次対応いたします。
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	月曜日～金曜日の9:30～11:45 13:00～17:30 (祝日・弊社休業日を除く) ※メール受付は24時間、対応は営業時間内に順次対応いたします。
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	非公開です。
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	非公開です。
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	非公開です。
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、保管媒体の破壊の実施有無/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： GDPR（EU一般データ保護規則）およびISO27001認証の要求に基づいたルールで、データ消去を行っております。解約時にご連絡いただいた場合、EU法によって保護される購入履歴等の一部例外を除くすべてのデータが消去可能です。物理メディアやその他の記憶媒体に関しましても、ISO27001認証の基準で安全に消去または物理破壊されます。
32		バックアップ世代数	保証する世代数	世代数	非公開です。
33		データ保護のための暗号化要件	データを保護するに当たり、暗号化要件の有無	有無	有： ISL Onlineで通信されるすべてのデータは、SSL（2048ビットRSAキーによるハンドシェイクとAES 256bitセッションキーを使用）で暗号化されているため、セッション開始後にデータを盗聴される心配はありません。また、一度セッションを終了すると同一セッションに再接続することはできません。ISL Onlineのプログラム自身もコードサイン証明書によりデジタル署名されており、非常に高いセキュリティで安心してお使いいただけます。
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： 2段階認証により、他ユーザーによる不正アクセスの影響範囲を限定します。
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： 開発元（XLAB社：スロベニア）の過失によりデータの漏洩や破損があった場合は、支払い済みの1年間の料金を上限として補償します。
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： GDPR（EU一般データ保護規則）に基づき、ユーザーに関連するデータの消去や返却要求に応じることが可能です。購入履歴等のEU法によって保持期間が定められているデータに関しては、要求があった場合も削除できかねますためあらかじめご了承ください。
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： データ修正者/日時が自動で記録されるため、ログとの比較により正規操作の検証が可能です。
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： 想定外のデータは格納できない仕様となっています。
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： サーバー管理を行うXLAB社は、ISMS認証(ISO27001)を取得しています。
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： ペネトレーションテストの実績はございますが、内容および結果は非公開です。セキュリティ対策における第三者機関の評価を得て、XLAB社はISO27001認証を取得しています。
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： ISO27001認証の要求に基づいたルールで運用されており、データへのアクセスは運用者を限定するほか、作業スペースへの入室管理を行うことで物理的にも制限しています。
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： TLS 1.2に対応しています。
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： データ認証のアクセス制御により、論理的にデータを隔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： 利用者データにアクセスできる社員は許可を得た者のみに限定されます。
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	OSのログは冗長化された各サーバー上、または監視ツール上で保管し、4週間保存されます。マルチテナントの性質上、保管期間の延長やログの提供はできません（シングルテナントによるプライベートクラウドライセンスでは可能です）。ソフトウェアログは、監視ツールに集約した上で1年間保存。製品の利用履歴、ユーザーIDごとのログイン履歴は無期限で保存され、検索が可能です。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	中継サーバーのウイルススキャンは未実施ですが、サービスや通信ポートを常時監視することでウイルス対策を行っています。 Online ScreenAssist/Online ScreenView及び両サービスのベースサービスとなるISL Online以外のサービスの実行や、Online ScreenAssist/Online ScreenView及び両サービスのベースサービスとなるISL Onlineで使用するポート以外でのインターネット接続は許可しておりません。
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	非公開です。
49		データの外部保存方針	データ保存時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	開発元（XLAB社：スロベニア）及びXLAB社の正規販売業者の株式会社オーシャンブリッジは制約条件を把握しています。