



本資料は、「クラウドサービスレベルのチェックリスト」(経済産業省)に基づき、Xtra株式会社の提供するQlingoのセキュリティについてまとめたものです。
独自のチェックリストへの回答をご希望の場合は、別途有料オプションを提供しております。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定(記入欄)
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日となります。(計画停止/定期保守を除く)
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】実施3日前までにページ上部の告知欄にて通知致します。
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	【有】終了1ヶ月前までに公式サイトにて事前に通知致します。
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	【無】預託等の措置は行っておりません。
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(%)	稼働率99.9%以上を目標と定義しています。
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】過去1週間のデータを復元できるよう、日次でバックアップを行っております。また物理的に離れたデータセンターでの冗長構成をとっています。
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】システムが利用できない場合の代替手段は準備していません。即座に復旧が可能なよう、データセンターの冗長化、及びバックアップの世代管理を行っております。
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】システムが利用できない場合の代替措置を未提供のため、定義していません。
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】軽微な機能追加・改善は随時実施します。影響が予想される大幅なバージョンアップを行う場合は、事前にサイトやメールで告知します。影響が予想されないアップデートに関しては、原則事前告知は行わずリリース後にサイトで告知をいたします。
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	これまで、サービスが利用できなくなる程度の障害の発生事案はありません。
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	営業時間内に発生した障害については、目標復旧時間を5時間以内としています。営業時間外に発生した障害については、目標復旧時間を24時間以内もしくは翌営業日の午前12時までのどちらか早い方としています。
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	これまで、サービスが利用できなくなる程度の障害の発生事案はありません。
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】システム稼働状況を24時間365日で監視しています。(ハードウェア/ネットワーク/パフォーマンス/エラー発生状況等)
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】障害発生時は、弊社担当者にアラートが通知されます。お客様にはサイト上にて報告します。
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	定めはございませんが、できるだけ早く通知します。(営業時間外の場合は、翌営業日になることがあります。)
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)	5分間隔で監視しております。
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	定期報告は行っていません。
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	ログの取得は行っていますが、ログ提供は行っていません。	
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	【無】機能・デザインの個別カスタマイズは承っておりません。
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】現在、API等は提供しておりません。
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】同時接続利用者数の制限はありません。
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】ご利用のプランに応じて、人数の上限があります。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定(記入欄)
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	24時間365日となります。(メール・問い合わせフォーム)
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	通常のサポート業務の対応時間は、月～金曜日 10:00～17:00(祝日、年末年始等は除く)となります。原則、2-3営業日以内にご返答いたします。内容によってはそれ以上のお時間をちょうだいする場合もあります。
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】過去1週間のデータを復元できるよう、日次でバックアップを行っております。(アクセス権はシステム管理者のみ。)データはクラウド上に冗長化し保管しています。システムトラブル時のみ復旧を行います。
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とり、データを保証する時点	時間	具体的な時点は公開しておりませんが、24時間以内のデータを保証致します。
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	バックアップデータの保存期間は最大で1週間となります。
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】サービス解約後、一定期間経過後に削除します。
32		バックアップ世代数	保証する世代数	世代数	7世代分を保証します。
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】TLSv1.2にて通信を暗号化しています。また保存データおよびデータベースの暗号化を行っています。
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	【無】ストレージに対してお客様が直接アクセスすることはありません。
35		データ漏えい・破壊時の補償/保¥險	データ漏えい・破壊時の補償/保険の有無	有無	【有】利用規約に定める範囲において保証を行います。(損害賠償保険には加入)
36		解約時のデータ可用性	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】サービス解約後、一定期間経過後に削除します。
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	【無】データの預託は行っていません。
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	【無】取得していません。
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】脆弱性検査を定期的実施しております。
41		情報取扱い環境	提供者側でのデータ取扱い環境が適切に確保されていること	有無	【有】サーバにアクセスする事が出来るのは、システム運用担当のスタッフに限定しています。また、ファイアーウォールで弊社環境からのみアクセスでき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】TLSv1.2にて通信を暗号化しています
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】実施していません。
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】お客様の契約スペースごとにデータを管理し、アクセス制限を行うことでデータ利用を制限しています。
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】サーバにアクセスする事が出来るのは、システム運用担当のスタッフに限定しています。また、ファイアーウォールで弊社環境からのみアクセスできるように制限しております。
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	個人単位でIDを付与しており、ログに記録されています。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	リアルタイムにウイルスチェックを行っております。
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	有無	【有】二次記憶媒体を使用せず、データセンター間でバックアップを取っております。
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】把握しております。	