SynQ Remote シンクリモート

セキュリティチェックシート

株式会社クアンド
更新日: 2025年09月16日

本資料は経済産業省が策定した「クラウドサービスレベルのチェックリスト（2010年8月発行）」に基づき、株式会社クアンドが提供する「SynQ Remote」のセキュリティについて記載したものです。

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／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 3営業日前までにメールにて通知いたします。
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 サービス終了の1か月前までに通知いたします。
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	無 当社ではソフトウェアおよびクラウドインフラを自社で管理しており、障害発生時にはバックアップデータを用いた復旧作業を行います。外部への預託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（%）	99.85% 2024年4月～2025年3月の実績値です。
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 Azure クラウド上でシステムを運用しており、複数のデータセンターに分散配置しております。災害発生時にも冗長構成により復旧可能な体制を整えております。
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 現状、サービスが復旧不可能な場合の代替通話手段は提供しておりません。復旧作業を最優先で行い、サービス停止時間を最小化する運用体制を整えております。
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 障害発生時に代替手段としてデータ提供を行う運用は現在ございません。必要に応じて復旧後にデータアクセスを行える仕組みを用意しております。
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 定期的に更新を行っております。
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	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	公開しておりません。
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	3回 2024年4月～2025年3月の実績値です。 対応に長時間（1日以上）を要したものは0件です。
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 クラウドのモニタリング機能を用いてアプリケーションメトリクス・負荷状態・APIエラーの監視を常時行っております。
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 監視システムより担当チームへ自動通知されます。担当チームにて、障害対応プロセスを実施いたします。
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	1～5分 監視項目により異なります。
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）	1分間隔
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	稼働状況を常時公表する仕組みは現在ございません。緊急時はメールにてご案内いたします。
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 アクセスログ、操作ログ、エラーログを取得しております。重大インシデントへの調査協力など、必要に応じてログ提供を行います。
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。

QUANDO

SynQ Remote シンクリモート

セキュリティチェックシート

株式会社クアンド
更新日: 2025年09月16日

No.	種別	サービスレベル項目	規定内容	測定単位	設定
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	有 ログイン認証においてSAML2.0対応のIDPとSSO（シングルサインオン）の接続が可能です。データの外部連携は、お客様のご要望に応じ、別途ご契約のうえで対応いたします。
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）	有 1つの通話では10名までの同時通話が可能です。契約に応じて、同時に利用できる通話の数が変わります。ユーザー数に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	有 ご契約のプランに応じて、写真・動画を保存するストレージ容量の上限がございます。
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 9:00-17:00（土日祝年末年始を除く） 時間外においても障害を検知した場合、ベストエフォートで復旧対応を実施いたします。
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	平日 9:00-17:00（土日祝年末年始を除く） サポート窓口については下記でご案内しております。 https://tayori.com/q/syngremote-faq/detail/1016451/
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 Azureクラウドにてデータベースのバックアップを日次で取得しております。 復旧が必要な場合は、Azureのバックアップリストア手段を用いて対応いたします。
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	継続的バックアップおよびスナップショットの両方でバックアップを取得しており、障害発生時には概ね15分前の状態まで復旧可能です。
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	7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 サービス解約から1ヶ月後に関連データの削除を行います。
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 AES256による暗号化を行っております。
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 データベースにおいては、テナントIDを基にデータを分割管理しているため、テナントIDがない状態では他テナントのデータにアクセスできません。 ストレージ領域においても、テナントごとにコンテナを分けて保管しており、各テナントのデータは他テナントから参照できません。
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	無 補償や保険は提供しておりませんが、利用規約に従い、お客様のデータを保護するため最大限の注意を払って運用しております。
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 当社サービスでは、お客様の通話データおよび記録データを当社サービス上で保管しております。解約から1ヶ月後に関連データを削除いたします。必要に応じて、個別相談のうえでデータの引き渡しも可能です。
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 整合性検証作業や検証報告の確認作業は行っておりません。
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必須入力や文字数チェックを行っております。

QUANDO

SynQ Remote（シンクリモート）

セキュリティチェックシート

株式会社クアンド
更新日: 2025年09月16日

No.	種別	サービスレベル項目	規定内容	測定単位	設定
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 ISMS認証（ISO/IEC 27001）を取得しております。
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 毎年、外部機関による脆弱性診断を実施しております。
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 お客様の個人情報はIDサービス内に閉じて管理しております。
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以上を使用して通信を暗号化しております。
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 当社サービスはマルチテナント環境で運用しており、データはテナント情報をキーとして分離管理しております。
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 IDシステムにて利用者情報を管理しており、サービス運用上必要な担当者のみがアクセスできるよう、権限管理を行っております。
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	利用者ごとにIDを付与しており、アクセスログの検索に利用可能です。ログは適切な期間保存されており、必要に応じて調査やログ提供を行っております。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	当社サービスが利用しているプラットフォーム（Azure）側でマルウェアスキャンを実施しております。 また、全ての業務用端末にはウイルス対策ソフトを導入しており、常時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	無 当社サービスでは、バックアップメディアや外部二次記憶媒体を使用していないため、暗号化・廃棄・USB制御等の対策は実施しておりません。
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	当社サービスのデータは、Azureクラウドの東日本リージョンにて保管・管理しており、法制度および規制に基づくデータ取扱いを把握し、実施しております。

QUANDO