Tencent Real-Time Communication

Protocols and Policies

製品ドキュメント

カタログ：

Protocols and Policies
セキュリティコンプライアンス認証

最終更新日：：2022-07-11 12:08:40

コンプライアンスはTencent Cloud TRTCの発展の基本です。Tencent Cloud TRTCは各国および業界のコンプライアンス要件を遵守し、提供するサービスの**セキュリティ、コンプライアンス、可用性、機密保持**および**プライバシー**を保証するほか、TRTCを使用するお客様に関連のサポートを提供することで、**企業とその顧客の様々なコンプライアンス監督管理のニーズを満たし、会社と顧客による監査業務への重複投資を削減し、監査と管理の効率を向上させます。**
TRTCは一連のSOC報告書（SOC 1、SOC 2、SOC 3を含む）、サイバーセキュリティ等級保護2.0、ISOシリーズ認証（ISO 9001、ISO 20000、ISO27001、ISO27017、ISO27018、ISO27701、ISO29151を含む）、CSA STAR、NIST CSF、BS10012およびK-ISMS認証を取得済みです。

セキュリティホワイトペーパー

最終更新日：：2023-03-13 14:47:52

1. 概要

Tencent Real-Time Communication（TRTC）は、Tencentの長年にわたるネットワークとオーディオビデオ技術上のハイレベルな蓄積を、多人数オーディオビデオ通話とローレイテンシーインタラクティブライブストリーミングの二大シナリオ化ソリューションとし、Tencent Cloudのサービスを通じて統一、標準化されたApplication Programming Interface（API）を開発者に提供するとともに、さまざまな業界およびシナリオ向けに、主要OSおよびプラットフォームに適合するSoftware Development Kit（SDK）を提供しています。開発者が低コスト、低遅延、高品質のオーディオビデオインタラクティブソリューションを迅速に構築できるよう支援します。
リアルタイムオーディオビデオPaaSクラウドサービス業界をリードするTencent Cloud TRTCにとって、データセキュリティとユーザープライバシーはサービスの根幹を成す問題です。TRTCは常にデータとユーザープライバシーの安全性を最も重要なセキュリティ原則と考え、それを日常のセキュリティ機能構築に適切に組み入れています。開発者の方にTencent CloudのTRTC製品サービスの安全保障機能についてご理解いただけるよう、TRTC PaaSサービスのセキュリティ構築およびセキュリティコンプライアンス審査について以下でご説明します。

2. セキュリティコンプライアンスとプライバシー保護

セキュリティコンプライアンスはTencent Cloud TRTCの発展の基本です。Tencent Cloud TRTCは各国および業界のコンプライアンス要件を遵守し、提供するサービスのセキュリティ、コンプライアンス、可用性、機密保持およびプライバシーを保証するほか、TRTCを使用するお客様に関連のサポートを提供することで、企業とその顧客のさまざまなコンプライアンス監督管理のニーズを満たし、会社と顧客による審査業務への重複投資を削減し、審査と管理の効率を向上させます。
TRTCは一連のSOC報告書（SOC 1、SOC 2、SOC 3を含む）、サイバーセキュリティ等級保護2.0、ISOシリーズ認証（ISO 9001、ISO 20000、ISO27001、ISO27017、ISO27018、ISO27701、ISO29151を含む）、CSA STAR、NIST CSF、BS10012およびK-ISMS認証を取得済みです。

セキュリティコンプライアンスとプライバシー保護	説明
ISO/IEC 27001: 2013　情報セキュリティマネジメントの標準規格	ISO/IEC 27001: 2013は最も基本的かつ、国際的に最も広く認知されている情報セキュリティマネジメントシステムの標準規格です。Tencent Cloud TRTCがISO 27001:2013認証を取得したことは、当社のセキュリティに対するコミットメントのあらわれです。当社の情報セキュリティ管理について一連の科学的かつ有効なマネジメントシステムがすでに確立され、信頼性の高い情報サービスをユーザーに提供可能であることを示しています。

ISO/IEC 27017: 2015　クラウドサービス情報セキュリティ管理の実施指針を提供	ISO/IEC 27017: 2015はクラウドサービスの情報セキュリティに特化した実用標準規格であり、クラウドサービスプロバイダおよびクラウドサービスのお客様向けに特定のセキュリティ制御とその実施についてのガイドラインを提供しています。ISO 27017はISO 27002をベースに拡張された規格であり、主にクラウドベンダー向けにクラウド構築と運用保守についてのセキュリティルールを示すことを目的としています。Tencent Cloud TRTCはISO/IEC 27017認証を取得しており、このことは当社のクラウドサービスが適切な情報セキュリティ管理および保障能力を備えていることを証明しています。
	ISO/IEC 27018: 2019はパブリッククラウド内の個人情報保護に特化したガイドラインです。情報セキュリティ標準規格ISO/IEC 27001をベースに、パブリッククラウドにおける個人情報保護に適用可能な追加的制御措置を提供し、パブリッククラウドのレベルでの個人情報保護機能を強化したものです。Tencent Cloud TRTCのISO 27018認証取得は、当社が企業のデータ、知的財産権、ドキュメントの保護、クラウドITシステムのセキュリティなどの面で、業界のハイレベルなベストプラクティスを実現できていることの証明です。
CSA STAR認証	クラウドセキュリティ評価のCSA STARは、国際的な権威のある非営利団体Cloud Security Alliance（CSA）が発表したCloud Control Matrix（CCM）に基づくもので、クラウドコンピューティングセキュリティ分野の特定の要件を満たし、クラウドコンピューティングのセキュリティ特性に対応した国際認証の一つです。この認証もISO/IEC 27001情報セキュリティマネジメントシステムの拡張版であり、クラウドセキュリティ特有の問題を可視化し、クラウドサービスプロバイダのセキュリティ管理能力に対する直観的な評価の枠組みを示すものです。Tencent Cloud TRTCはCSA STAR認証の取得により、クラウドサービスのセキュリティ保障機能を有することが証明されています。
SOC審査	SOC報告書（System and Organization Controls Reports）とは、アメリカ公認会計士協会（AICPA）の定めた関連ガイドラインに基づいて、専門の第三者会計事務所が発行する、サービス機関の内部統制に関する一連の報告書のことです。 Tencent Cloudは業界をリードするクラウドサービスプロバイダとして、2017年のSOC審査プロセスにおいてすでに2017年版のトラストサービス原則を使用しており、中国国内でいち早く2017年版トラストサービス原則を遵守したクラウドサービスプロバイダです。TRTCがこのサービス認証報告書を取得していることは、当社が有効な内部統制を確立および実施すると同時に、定期的に第三者の監査を受け、各製品サービスがいずれも認証報告書の要件に確実に適合していることを証明しています。
サイバーセキュリティ等級保護認証	サイバーセキュリティ等級保護2.0（略称「等級保護2.0」）は2019年12月1日より正式に施行されました。等級保護2.0は能動的な防御に重点を置き、受動的防御に加えて事前、事中、事後の全フローに対する安全で高い信頼性かつ動的なセンシングと包括的な審査を行うもので、従来の情報システム、基本情報ネットワーク、クラウドコンピューティング、モバイルインターネット、IoT、ビッグデータ、産業管理システムといった等級保護対象をすべて網羅し

	ています。TencentパブリッククラウドTRTC PaaSサービスプラットフォームは、サイバーセキュリティ等級保護2.0の基準および関連規定に準拠し、レベル3の届出とアセスメントに合格しています。これは当社が中国のクラウドコンピューティングプラットフォームのセキュリティ構築における技術保障要件およびセキュリティ管理要件を遵守していることを示すものです。クラウドプラットフォーム上のさまざまな業界・業種の各企業ユーザーに、等級保護に準拠したサービスをご提供します。

3. データセキュリティ

データセキュリティはTencent Cloud TRTCが最も重視する点の一つです。TRTCは開発者のデータに対し適切かつ必要なコンプライアンス処理を行うことで、データの安全性を保証します。ここではTencent CloudとTencent Cloud TRTCがデータセキュリティにおいて講じている技術的制御措置と管理ポリシーについてご説明します。

3.1 データセキュリティポリシー

Tencent Cloud TRTCはデータの機密性、完全性、可用性をオーディオビデオサービスのデータセキュリティ発展の前提として堅持し、データセキュリティ管理構築の理念をオーディオビデオPaaSサービス構築のプロセスに組み入れています。Tencent Cloudは一貫して開発者データの可用性、機密性、完全性を確保します。
可用性：Tencent Cloud Virtual Private Cloud（VPC）伝送プロトコルによって、データの高可用性を保障します。
機密性：開発者からの権限承認を得ていないアクセスおよび盗聴を防止します。
完全性：開発者データの完全性を確保し、偽造を防止します。
Tencent Cloud TRTCは全従業員に対し、データセキュリティ、プライバシーとコンプライアンス、データ暗号化保護に関する定期的なセキュリティトレーニングを行っています。また、従業員との間で秘密保持契約を締結し、社内の従業員が日常の保守業務を行う上で、サービスデータの可用性、機密性、完全性を確実に保護できるようにしています

3.2 データの高可用性

TRTCは可用性の高いオーディオビデオPaaSデータサービスを開発者向けにご提供できるよう取り組んでいます。
大容量データセンター：Tencent Cloud TRTCは世界各地に多数のデータセンターを持ち、協力してサービスをご提供しています。データセンターの1つが攻撃を受けても、他のデータセンターの正常な稼働に影響せず、サービス全体にも影響しないように、パーティション隔離による保障メカニズムを備えています。
障害隔離復旧：データセンターがサービス拒否（DoS）などの、防止が困難な悪意ある攻撃に遭い、サービスに障害が発生した場合、Tencent Cloud TRTCは障害を起こした機器に対し適切な処理を行い、サービス全体の安定性と可用性を確保します。
Anti-DDoS：Tencent Cloud TRTCは使用するデータセンターにAnti-DDoSファイアウォールを設置し、DDoSのリスクをコントロールするための十分な機能とリソースを備えています。

3.3 データ収集

Tencent Cloud TRTCはユーザーからの権限承認同意を得た、製品サービスに必須のデータフィールドだけを収集し、最小粒度のデータ採取の原則に厳格に従っています。またTencent Cloud TRTCの開発者が収集したプログラムログイン情報、ID認証、パスワード、支払情報、氏名と住所などのユーザーデータはすべて開発者自身が保管し、TRTCプラットフォームには保存されません。

3.4 データマスキング

開発者データのプライバシー保護のため、Tencent Cloud TRTCは公式コンソールの企業および個人情報をすべてマスキングして表示しています。このポリシーは、内部管理プラットフォーム、ログプリント、監視アラートなどの、TRTCの内部システムおよび他の製品のデータ表示チャネルにも同様に適用されています。

3.5 データの使用とストレージ

開発者の個人または企業ユーザーデータ、エンドユーザーデータ、オーディオビデオ通話データ、システム実行およびセキュリティデータに対してはカテゴリーおよびレベル別ストレージを実施し、開発者データがコンプライアンスに沿って安全に保存されることを保証します。
Tencent Cloud TRTCは開発の過程で、本番環境、テスト環境、開発環境を厳格に分離しているため、開発者のリアルデータが開発とテストに直接使用されることはありません。また、開発者とユーザーのパスワードなどの機密情報は暗号化して保存されます。
開発者とユーザーがTencent Cloud TRTCの提供するローカルサーバーのレコーディングSDKおよびクラウドレコーディング機能を使用している場合、開発者とユーザーは通話内容の一部またはすべてをレコーディングすることができます。その際、すべての録画/録音内容は開発者とユーザーが提供するストレージサーバー上に直接書き込まれ、Tencent Cloud TRTCのサーバーには保存されません。

4. Tencent Cloud TRTC PaaSサービスのセキュリティ

低遅延で高品質なリアルタイムインタラクションソリューション実現のために、Tencent Cloud TRTCサービスには厳しい要件が課されます。Tencent Cloud TRTCはオーディオビデオPaaSサービス構築の過程で、アーキテクチャ技術のセキュリティリスクを十分に評価すると同時に、コンプライアンス規格の中のセキュリティリスクコントロールシステムを最大限に遵守するとともに、その運用をオーディオビデオPaaSの各構築段階で実行することで、開発者とユーザーに高品質で安定した、セキュアな一連のオーディオビデオPaaSソリューションを提供できるよう保証します。

4.1 Tencent Cloud TRTC伝送ネットワークのセキュリティ

TRTCはTencent CloudのVPC伝送ネットワークをベースにして、超低遅延、高伝送品質かつ100万人規模をサポート可能なリアルタイムインタラクティブオーディオビデオプラットフォームを構築しています。VPC伝送ネットワークはTencent Cloud TRTC PaaSのコアサービスの一つです。オーディオビデオサービス端末シグナルの受信、ID認証、リアルタイムスケジューリング、オーディオビデオデータのリアルタイム伝送などの各段階を、コンプラ

イアンスを遵守した安全なサービスで支援します。またTencent CloudのVPC伝送ネットワークはアーキテクチャ設計において、現在のインターネット環境が直面するセキュリティ上の不安定要素を詳細に検討し、開発者とユーザーに安全かつ安定したサービスを提供するために、以下の数点からなる制御措置を実装しています。

伝送ネットワークのセキュリティ制御措置	説明
暗号化伝送	オーディオビデオデータの伝送過程での機密性を保証するため、Tencent Cloud TRTCは内蔵暗号化とカスタム暗号化という2つの方法で伝送リンクの暗号化保証を提供しています。Tencent Cloud TRTCサービスPaaSでは、全データリンクを対象とした内蔵暗号化がデフォルトでグローバルに有効になっており、データ伝送の暗号化による安全性が保証されています。
リソース隔離	Tencent Cloud TRTCは各オーディオビデオアプリケーション（SdkAppId）に専有リソースを割り当てることで、TRTCに対し、他のプロジェクトリソースから互いに独立した、安全かつ信頼性の高い演算リソースを提供できるよう保証します。開発者とユーザーにとっては、TRTCコンソールに正式登録後、コンソール（Console）上で簡単な操作を行うだけでTRTCアプリケーション（SdkAppId）を新規作成し、対応するリソースを割り当てることが可能になります。
ルーム隔離	Tencent Cloud TRTCはオーディオ、ビデオ、メッセージデータの伝送について、種類ごとに独立した隔離チャネル、すなわちRoomidを作成しています。論理上、すべてのルームは分かれており、ユーザーが同じSdkAppidのオーディオビデオインタラクティブアプリケーションおよび同じルーム名を使用している場合のみ、同じチャネルに入ることができます。ルームはセッション開始時に作成され、セッション終了（最後のユーザーが退出）後に破棄されます。この仕組みによってルームレベルでの伝送隔離を実現しています。
身分認証	ユーザーがTRTCアプリケーションを使用してTencent Cloud TRTC PaaSサービスにアクセスする際、TRTCはSdkAppid +キーによって生成された認証情報に基づいて入室検証を行うことで、開発者とユーザーが必要に応じて、自身のユーザーに対する強力な認証を実施できるようサポートします。

4.2 Tencent Cloud TRTC SDKのセキュリティ

Tencent Cloud TRTCはiOS、Android、macOS、Windows、Web、ミニプログラムなどのプラットフォームのSDKを提供し、お客様が統合を便利に行えるようにすることで、開発者の各端末プラットフォームでのTRTCインタラクション開発統合のニーズに応えます。Tencent Cloud TRTC SDKは開発者とユーザーにシンプルで統合しやすく、セキュアで安定したオーディオビデオ開発キットを提供するだけではありません。
TRTCは、コンプライアンスを遵守した、安全性が保障されたオーディオビデオPaaSサービスを開発者とユーザーに提供することで、開発者とユーザーがコンプライアンス規制および情報ソースのデータセキュリティ上の脅威に対応するために行う作業を減らせるよう尽力しています。

SDKのセキュリティサポート	説明

SDKのセキュリティとコンプライアンス	Tencent Cloud TRTC SDKの信頼性と安全性はTencent Cloud TRTCの基本的な機能保障の一つです。Tencent Cloud TRTCは機能のイテレーションの際、その前段階でコンプライアンスとプライバシーにおける機能ニーズの適正性と、セキュリティ上のリスクポイントを十分に評価することで、Tencent Cloudのコンプライアンスおよびプライバシーポリシーへの適合を確実にしています。 TRTCは機能実装の際も十分かつ必要な品質セキュリティテストを実施し、サードパーティSDK、ライブラリファイルの参照または統合を行う場合はセキュリティチェック、特にコンプライアンスの確認を実施しています。
SDKのコンテンツ暗号化	Tencent Cloud TRTC SDKはAES 128対称キーを使用した、すべてのオーディオビデオストリームおよびメッセージに対するデータレベルでの暗号化をサポートしています。暗号化されたデータはTencent CloudのVPC伝送ネットワークを通じてTRTCルーム内のノードに送信され、最終的に受信した端末でオーディオビデオデータが復号されてレンダリングされます。伝送の過程ではデータのセキュリティと機密性が保証されます。
開発者に対するSDKのセキュリティとコンプライアンスのサポート	Tencent Cloud TRTCは開発者向けに、常に高品質かつ安全で適法なオーディオビデオPaaSサービスを提供し続けています。Tencent Cloud TRTC SDKは安全なコンテンツの内蔵暗号化を提供することで、開発者とユーザーがTRTCデータのセキュリティとプライバシーコンプライアンスを徹底し、セキュリティとプライバシーに関するお客様のニーズを最大限満たし、この面での開発コストを削減できるよう支援します。

4.3 TRTCの基本コンピューティングリソースのセキュリティ

Tencent Cloud TRTCの基本コンピューティングリソースは、世界各地に分布する自社の分散型データセンター（IDC）とTencent Cloud Virtual Machine（CVM）で構成されます。これにより、TRTCの基本コンピューティングリソース環境の、高い拡張性、安全性、可用性の特性が保証されています。

コンピューティングリソースのセキュリティ	説明
自社IDC内デバイスのセキュリティ管理	Tencent Cloud TRTCのインフラのうち、自社IDC内のデバイスの日常管理について、Tencent Cloud TRTCは一連のデータセンター管理規定を整備して制定しています。この規定は管理規則とサービス実施基準を詳細に定義し、データセンターの物理環境の安全性、日常の巡回点検、異常監視報告、電力リソースの保障などを適切に反映したもので、Tencent Cloud TRTCのセキュリティコンプライアンスとインフラの安全性構築要件を満たすものとなっています。
ホスト、データベース、ミドルウェアなどのコンピューティングリソースのセキュリティ	Tencent Cloud TRTCサービスの実行に必要なリソースは、CPU、メモリ、ディスクなどのリソースを、業務の負荷に応じて適正にスケジューリングして割り当てることで対応しています。TRTCの実際のセキュリティ運用においては、適用するセキュリティベースライン、脆弱性管理ルールを制定

	し、脅威に対する多層チェックのメカニズムを実行することで、基本サービスのシーンで基本演算負荷リソースの安全性を十分に確保することが可能です。
DDoS攻撃防御	分散型サービス拒否攻撃DDosはTencent Cloud TRTC PssSサービスのシステムと業務の可用性に重大な影響を及ぼします。TRTCはTencent Cloudのパブリッククラウド機能を利用し、コアサービスにAnti-DDoSソリューションをデプロイしています。このソリューションはネットワーク層、トランスポート層からのDDoS攻撃をリアルタイムに検出して防御することができます。Anti-DDoSソリューションはネットワークトラフィックをリアルタイムに監視し、攻撃を発見するとただちにスクラブし、Tencent Cloud TRTCサービスに対する保護を秒レベルで開始することができます。

4.4 Web APIのセキュリティ

開発者が自身のオーディオビデオ業務の開発を効率的に管理できるよう、Tencent Cloud TRTCはコンソールの一部の機能をRESTful API方式で開発者が呼び出せるようにしています。RESTful APIはセキュリティの面で次のような保障を提供します。

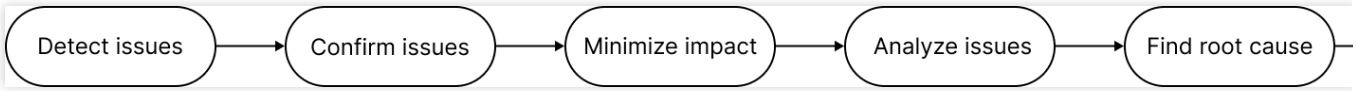
セキュリティ保障	説明
ID認証	開発者はTencent Cloud TRTC RESTful APIを使用する前にTencent Cloudコンソールにログインし、開発者専用のSecretId&SecretKeyを作成する必要があり、これによってサービス提供者のIDの一意性が確保されます。
入力の検証	開発者のリクエストのパラメータはTRTCのバックエンドサーバーで適格性の検証を行い、不正なパラメータをフィルタリングすることで、いくつかの一般的な脆弱性に対処することができます。
伝送セキュリティ	RESTful APIはHTTPSプロトコルのみをサポートし、 SSL/TLSを使用してすべてのAPI通信を暗号化することで、APIの認証情報と伝送データを保護することができます。
APIの速度制限	サーバーがAPIリクエストの速度を制限し、正常なユーザーリクエストへの応答を保証するとともに、悪意あるユーザーからのAPIリクエストを制限します。

5. セキュリティ運用

適正なセキュリティ運用ポリシーを常に堅持することは、Tencent Cloud TRTCがお客様の安全とコンプライアンス保障を実現するための基本です。Tencent Cloud TRTCはサービス自体の特性に基づき、次の方法で業務運用上の安全性を保証しています。

5.1 セキュリティ緊急対応メカニズム

Tencent Cloud TRTCはオーディオビデオPaaSというサービスの特性に基づき、さまざまなセキュリティイベント分類基準を制定し、サービスのタイプごとにカテゴリーとレベルの分類を行って、セキュリティ評価と脅威レベル分類を系統的に実施し、整備された効率的な処理フローと合わせて、セキュリティ異常のタイムリーかつ有効な処理を保証しています。
要約すると、Tencent Cloudのオーディオビデオは機能のセキュリティ異常に対し次のような処理を行っています。



5.2 業務連続性の管理

Tencent Cloud TRTCが24時間年中無休で開発者とユーザーに対しオーディオビデオサービスを提供し、低遅延かつ高品質なオーディオビデオサービスを提供できるようにするため、製品内部には、エキスパート開発運用保守チームが担当するオーディオビデオサービス可用性サポートおよび管理が組み込まれています。

緊急対応メカニズム	説明
業務の監視とアラート	Tencent Cloud TRTCの内部には24時間年中無休の高効率モニタリングメカニズムが確立されており、業務サービスおよびシステム実行の状態を監視測定しています。完全な統一モニタリングツールを構築し、業務サービスにかかわるアプリケーション、ミドルウェア、演算負荷、データベース、ネットワークデバイスなどのシステムコンポーネントの実行状態およびリソース負荷などの指標に対するイベントモニタリングと自動アラートを実現しています。また、ロボットによる当直者への通知を利用してただちに必要な処理を行い、問題をタイムリーに発見して確実にサービスを復旧させることができ、サービスの可用性を保証しています。
障害復旧と冗長性	Tencent Cloud TRTCは自社のコアIDCの冗長化アーキテクチャ上に構築されており、ソリューションの制定はデバイスの障害時の安全性を考慮し、インフラ層、演算負荷およびネットワーク構造などの観点からさまざまな極端な業務シナリオ下を考慮して行っています。Tencent Cloud TRTCの基本リソースの可用性をさらに保障するため、Tencent Cloudのパブリッククラウドサーバーを併用することで、突発的な状況でもオーディオビデオサービスの高可用性を保障できるよう配慮しています。
連続性訓練	Tencent Cloud TRTCはオーディオビデオの重要業務システムの継続的かつ有効な実行を保障するため、データセンターのネットワーク、ミドルウェア、業務システムなどについて定期的に緊急安全障害復旧訓練を実施しています。毎回の緊急対応訓練データに基づいてレビューと総括を行い、技術アーキテクチャ、運用管理フローおよび緊急対応計画を整備し、Tencent Cloud TRTCサービスの安定性を継続的に向上させています。

5.3 セキュリティモニタリングと侵入防止

Tencent Cloud TRTC PaaSサービスは多層防御を確実に実行することで脅威の基本的な側面に対応しており、セキュリティチームは最小権限の範囲でセキュリティログの分析を行っています。各業務で毎日生成されるログデータにおいて、特定したセキュリティ異常イベントについて速やかにアラートを発出し、セキュリティ運用担当者がさらに関連付けと遡及分析による確認を行います。すでに確認されている潜在的なリスクポイントについては、Tencent Cloud TRTCの緊急対応メカニズムによる処置と追跡を行って、業務システムの安全性と安定性を保障します。

6. 従業員のセキュリティ

Tencent Cloud TRTCでは、内部の従業員1人1人が、日常の運用と管理のプロセスにおいてデータと情報の安全性保証という原則を厳格に確実に遵守することを基本としています。Tencent Cloud TRTCは、セキュリティレベル全体における要員セキュリティの重要性を十分に認識しており、採用、入社、トレーニング、退職などのフローの中で、従業員の職業倫理と基本的な資質、Tencent Cloudの価値観との一致、セキュリティとコンプライアンスの要件ならびに業務発展の必要性を満たすかどうかを十分に考慮しています。

フローの段階	説明
採用	Tencent Cloud TRTCは従業員採用の事前段階で、人的資源の専門家が候補者の学歴、業務経験の確認を行い、条件に適合する専門スキルを確実に備えた従業員を採用しています。
入社	新規従業員は入社後、Tencent Cloudのセキュリティとコンプライアンスの認識要件を満たすための従業員安全行動規範を学びます。また、各従業員とはレベルごとに秘密保持契約を締結しています。重要なデータに触れる職場の従業員に対しては、より厳格なセキュリティコンプライアンス規定の研修を行い、評価に合格しなければTRTCの日常の構築業務に関与できないようにしています。
在職中	在職中の従業員は、セキュリティとプライバシー保護に関するトレーニングに定期的に参加し、評価に合格することが義務付けられています。また、Tencent Cloud TRTCでは内部のセキュリティとプライバシーに関する活動を不定期に開催し、全従業員のセキュリティ意識を常に向上させる取り組みを行っています。
退職時	退職する従業員は定められた退職フローに従って、引継ぎとアクセス権限の無効化を完了しなければなりません。Tencent Cloud TRTCは従業員と締結した秘密保持契約に基づき、退職後の秘密保持期間中の遵守状況を審査し、従業員に対し退職後の情報セキュリティ秘密保持義務について告知します。特に重要な職場の従業員とは、状況に応じて競業避止契約を締結します。退職する従業員は業務の引継ぎ、データクリーンアップを完了し、審査に合格してからでなければ退職できません。

7. セキュリティ責任の共同負担

Tencent Cloud TRTCはリアルタイムインタラクティブオーディオビデオPaaSのクラウドサービスプラットフォームであり、TRTCはクラウドサービスプラットフォームとSDKのセキュリティに対する管理を行います。それと同時に、サービスへのアクセス者である開発者にも、ご自身のアプリケーションとシステム環境のセキュリティを管理するとともに、Tencent Cloud TRTCの提供するセキュリティ管理機能をご自身のニーズに応じて適切に使用し、ご自身の情報、プラットフォーム、プログラム、システム、ネットワークの安全性を保障していただく必要があります。

8. まとめ

お客様にセキュリティとコンプライアンスを遵守した安定的なオーディオビデオサービスPaaSをご提供することは、Tencent Cloud TRTCが考える最も大切な要素の一つです。Tencent Cloud TRTCは要員、技術、管理フローなどのさまざまな面から、情報セキュリティソリューションの実行、コンプライアンス監督管理義務の履行を系統的に推進し、これらを日常的な運用のルールとして製品サービス開発を指導しています。また、より効率的で安全性の高い、自動化されたセキュリティ保護措置の実現に向けて、新技術の研究にも積極的に取り組んでいます。TRTC PaaSサービスの高可用性を継続的に保障し、エンドユーザーの合法的な権益を守るため、Tencent Cloudはこれからもセキュリティとコンプライアンスを保証したリアルタイムインタラクティブオーディオビデオクラウドサービス製品の開発に全力を尽くしていきます。

情報セキュリティの説明

最終更新日：：2023-03-13 14:49:06

説明：
このドキュメントについて、ここに次のように表明します。
1. このドキュメントはお客様にTencent Real-Time Communication（TRTC）製品、サービスのセキュリティの概要についてご説明し、情報管理とお客様およびエンドユーザーのデータセキュリティ保護をどのように行っているかについて述べることを目的としたものです。セキュリティに対し強制的な要件をお持ちの場合は、Tencent Cloudとの間で書面の商用契約（SLA）によって取り決めを行うことをお勧めします。契約がない場合、Tencent Cloudはこのドキュメントの内容についていかなる明示的または黙示的なコミットメントまたは保証も行いません。
2. セキュリティ特性の範囲は幅広いため、ここでは技術セキュリティの要点の「一部」のみに言及します。
3. このドキュメントを国家または業界情報セキュリティ関連規格、要件の参考文書とすることはできません。
4. この文章は可読性向上のための加工を行っています。記述が不正確な部分が存在する場合は1点目をご参照ください。
5. ドキュメントの解釈権はTencent Cloudに帰属します。

1、概要

Tencent Cloud TRTCライブラリは下記の認証を取得し、下記の認証のセキュリティ要件に適合しています。
ISO 9001認証
ISO 20000認証
ISO 27001認証
ISO 27017認証
CSA STAR認証
GDPR
その他のセキュリティコンプライアンス認証をクリックして表示

2、情報セキュリティ保障の説明

Tencent Cloud TRTCの管理セキュリティおよび技術セキュリティ要件はGDPR基準に適合しています。

2.1 情報データセキュリティ

ユーザーとTRTCサーバー間の通信はTencent Cloud VPC伝送プロトコル、TLS、Web Socket Secureなどのプロトコルによって保護されます。TRTCは伝送の過程で、伝送する情報を復号可能なキーを一切持ちません。通話内容

の情報は端末デバイス上（クライアントappやローカルサーバーのレコーディングサーバーなど）で、お客様が権限を承認したキーによってのみ復号が可能です。

2.2 データ可用性

大容量データセンター：Tencent Cloud TRTCは世界各地に多数のデータセンターを持ち、協力してサービスをご提供しています。データセンターの1つが攻撃を受けても、他のデータセンターの正常な稼働に影響せず、サービス全体にも影響しないように、パーティション隔離による保障メカニズムを備えています。
障害隔離復旧：データセンターがサービス拒否（DoS）などの、防止が困難な悪意ある攻撃に遭い、サービスに障害が発生した場合、Tencent Cloud TRTCは障害を起こした機器に対し適切な処理を行い、サービス全体の安定性と可用性を確保します。
Anti-DDoS：Tencent Cloud TRTCは使用するデータセンターにAnti-DDoSファイアウォールを設置し、DDoSのリスクをコントロールするための十分な機能とリソースを備えています。

2.3 データ分類保存

個人情報	用途	法的根拠
コンソール設定データ： TRTCアプリケーションID、アプリケーション名、記録が有効化されているか、リレー機能が有効化されているか、選択した課金方式	課金に必要なため、当社はこれらの情報を使用してこの機能の使用状況を確認します。 これらのデータは当社のElasticsearch Service (ES)機能に保存されることにご注意ください。	これらの情報は、当社がお客様と締結した契約を履行し、お客様にこの機能を提供するために不可欠な情報であるため、処理を行います。
バックエンドログデータ： ライブストリーミング活動のあらゆる参加者に関連するユーザーID、ルームナンバー、ライブストリーミング活動のあらゆる参加者に関連するクライアントIP、クライアントのSDKバージョン、ライブストリーミング活動のあらゆる参加者に関連するOSのタイプ	当社はこの機能を要件に従って実行し、故障を排除することを確実にするために、これらの情報を使用します。 これらのデータは当社のES機能に保存されることにご注意ください。	これらの情報は、当社がお客様と締結した契約を履行し、お客様にこの機能を提供するために不可欠な情報であるため、処理を行います。
ダッシュボード情報： 通話中のオーディオとビデオの品質に関する情報：エンドユーザーのAPPID、エンドユーザー制御機能に関するデータ（ビデオの有効化、ビデオの無効化、オーディオの有効化、オーディオの無効化）、入室、退室、ルームID、ミュート機能、CPU使用率、メモリ使用状況、ネットワーク遅延、データパケットロス、解像度、ビットレート、フレームレート、 音量	当社はこの機能を要件に従って実行し、故障を排除することを確実にするために、これらの情報を使用します。 これらのデータは当社のES機能に保存されることにご注意ください。	これらの情報は、当社がお客様と締結した契約を履行し、お客様にこの機能を提供するために不可欠な情報であるため、処理を行います。

（エンドユーザーの）SDKログデータ：ユーザーID、ルームナンバー、クライアントSDKバージョン番号、TRTCルームのOSタイプ	当社はこの機能を要件に従って実行し、故障を排除することを確実にするために、これらの情報を使用します。 これらのデータは当社のES機能に保存されることにご注意ください。	これらの情報は、当社がお客様と締結した契約を履行し、お客様にこの機能を提供するために不可欠な情報であるため、処理を行います。
UIN	当社はこれらの情報を使用してこの機能の使用状況を確認します。 これらのデータは当社のES機能に保存されることにご注意ください。	これらの情報は、当社がお客様と締結した契約を履行し、お客様にこの機能を提供するために不可欠な情報であるため、処理を行います。
SDK APPID（UINを使用して異なるアプリケーションを作成）	この機能の一部として、当社はこれらの情報を使用してお客様のアプリケーションの使用状況を確認します。 これらのデータは当社のES機能に保存されることにご注意ください。	これらの情報は、当社がお客様と締結した契約を履行し、お客様にこの機能を提供するために不可欠な情報であるため、処理を行います。
故障排除データ：エンドユーザーのAPPID、エンドユーザー制御機能に関するデータ（ビデオの有効化、ビデオの無効化、オーディオの有効化、オーディオの無効化）、入室、退室、ミュート機能、ルームID、CPU使用率、メモリ使用状況、ネットワーク遅延、データパケットロス、解像度、ビットレート、フレームレート、音量	当社はこれらの情報を使用してエンドユーザーの問題の検出と特定を行い、故障を排除します。 これらのデータは当社のES機能に保存されることにご注意ください。	これらの情報は、当社がお客様と締結した契約を履行し、お客様にこの機能を提供するために不可欠な情報であるため、処理を行います。

TRTCはローカライズレコーディングおよびクラウドレコーディング機能を提供し、お客様は通話内容の一部またはすべてをレコーディングすることができます。クラウドレコーディングサービスを使用する際、オーディオビデオ通話の録音/録画はすべてお客様のクラウドストレージサービスに保存され、TRTCではオーディオビデオファイルの保存は行いません。
TRTCは国内サイトのお客様の上記のデータは中国大陸で、グローバルサイトのお客様の上記のデータはシンガポールデータセンターでそれぞれ保存することで、データセキュリティコンプライアンスのストレージに関する

要件を満たしています。

2.4 アクセス権限承認

エンドユーザーがTRTCルームに入室する際、動的署名によるID認証を行い、悪意ある攻撃によってお客様のクラウドサービス使用権が不正利用されることを阻止する必要があります。詳細についてはセキュリティ保護署名UserSigの説明をご参照ください。

2.5 アクセス制御

TRTCは内部の全システムに対し厳格なアクセス制御管理を実行しています。全ユーザーが独立した内部アカウントと権限承認システムを持ち、さらに2段階認証を経る必要があります。アクセスレコードはすべて記録として保存されます。
ユーザーデータサービスにかかわるすべての機器は厳重に審査され、保護されています。TRTCは必要な場合以外はユーザーのサーバーにアクセスしません。安全上の理由からユーザーサーバーへのアクセスが必要な場合も、TRTCは一時的な権限を取得してユーザーサーバーにアクセスし、かつその一連のプロセスをスクリーンキャプチャし、すべての操作記録を維持します。

2.6 内部セキュリティ審査

当社はこの機能によって処理した個人データを保存します。具体的には以下のとおりです。

個人情報	保持ポリシー
お客様の一時キー情報： SDK APPID、ユーザー名、秘密鍵	当社はお客様によるこの機能の使用期間中、これらのデータを保持します。お客様がこの機能の使用を終了されるか、またはアカウントが削除された場合、当社は7日以内にこれらのデータを削除します。
アプリケーションに関連するお客様のログデータ： SDK APPID、アプリケーション名、タグ、サービスステータス、作成時間、操作	当社はお客様によるこの機能の使用期間中、これらのデータを保持します。お客様がこの機能の使用を終了されるか、またはアカウントが削除された場合、当社は7日以内にこれらのデータを削除します。

これらの個人データはDPSAリクエストによって削除することができます。

2.7 従業員セキュリティ意識トレーニング

Tencent Cloud TRTCは全従業員に対し情報セキュリティ意識およびセキュリティコンプライアンストレーニングを定期的に実施しています。また、全従業員が毎年定期的に情報秘密保持意識に関する講義とトレーニングを受講しています。

2.8 違反処理

Tencent Cloud TRTCの従業員は要件に従って秘密保持契約および内部セキュリティ制度を遵守することが義務付けられています。従業員が上記の要件に違反した場合、状況の重大性に応じて相応の違反処理措置が課せられます。これにはトレーニングと教育の強化、労働契約の解除、その他の法的責任の追及などが含まれますが、これらに限定されません。

2.9 潜在的なセキュリティ上の脆弱性

お客様がTRTCプラットフォームで潜在的なセキュリティ上の脆弱性を発見された場合は、チケットを提出して直接フィードバックをいただければ、当社の専門技術者がただちに処理とフィードバックを行います。ご協力に感謝申し上げます。
脆弱性の検証と特定のため、以下の関連内容をご提出ください。
ご連絡先
発見された潜在的な脆弱性機能の記述
必要な特定方法、問題再現の手順についてもあわせてご提供ください。