Tencent Cloud 日本サイバーセキュリティ規制コンプライアンスガイド

2026年4月

CONTENTS

CONTENTS

01 概要

近年、クラウドサービス技術は世界的に急速に普及し、企業の運営と政府サービスを支える重要なツールとなっています。デジタル化の推進に伴い、多くの組織や機関が、中核業務システムを従来のオンプレミス環境からクラウドプラットフォームへ移行する選択をしています。しかし、この移行は新たな課題ももたらしており、機微情報の保護、クラウドリソース設定のコンプライアンス管理、マルチクラウド・ハイブリッド環境における運用の複雑さなどが挙げられます。これらの課題に対応するため、クラウド環境の信頼性、安全性、効率性を確保する包括的な技術的・管理的メカニズムの確立が急務です。

クラウドサービス環境におけるセキュリティ課題に効果的に対応し、クラウドサービスの安全な提供と利用を促進するため、総務省（MIC）は 2021 年 9 月に「クラウドサービスを提供する際の情報セキュリティ対策ガイドライン」の最新改訂版を発表しました。このガイドラインは、クラウドサービス事業者が、自社のサービス形態、データ処理リスク、事業規模、利用可能なリソースなどの要素を考慮し、自社の事業特性に適合した情報セキュリティ対策を策定・実施することを奨励しています。

内閣サイバーセキュリティセンター（NISC）、デジタル庁、総務省、経済産業省は、サイバーセキュリティ戦略本部が策定した「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本枠組み」に基づき、政府情報システムセキュリティ管理・評価プログラム（ISMAP）を共同で運営しています。このプログラムは、政府のセキュリティ要件を満たすクラウドサービスを事前評価・登録することで、政府調達するクラウドサービスのセキュリティ水準を確保し、クラウドサービスの政府分野への円滑な導入を促進します。ISMAP 運営委員会は、登録を申請するクラウドサービス事業者に対して遵守すべきセキュリティ基準を提供し、監査・評価プロセスを完了するための指導を行い、日本政府が認める登録事業者となることを支援しています。

テンセントクラウドは、総務省および ISMAP 運営委員会の最新の規制動向を注視し、日本地域でクラウドサービスを利用する顧客が規制要件を満たすことを支援することに注力しています。本稿では、以下の規制機関のガイドラインと基準に基づき、テンセントクラウドが規制要件をどのように遵守しているかを説明します:

総務省:

- クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）

ISMAP 運営委員会:

- 政府情報システムのためのセキュリティ評価制度（ISMAP）管理基準

02

Tencent Cloud セキュリティとプライバシーコンプライアンス

コンプライアンスは Tencent Cloud の発展の基盤であり、Tencent Cloud は先進的な国際および業界のセキュリティ基準を特定し採用し、さまざまな国・地域および業界のコンプライアンス要件を遵守し、内部管理システムを絶えず改善し、Tencent Cloud のセキュリティ管理レベルを向上させ、お客様に信頼されるクラウドサービスの構築に全力を尽くしています。同時に、Tencent Cloud は業界のセキュリティ基準の策定と普及にも積極的に参加し、「コンプライアンスはサービスである」という理念を堅持し、安全で信頼性の高いクラウドエコシステムの構築と運営に取り組んでいます。

これまでに、Tencent Cloud は第三者による独立監査または評価を通じて、複数のセキュリティおよびプライバシーコンプライアンス認証または資格を取得し、Tencent Cloud のセキュリティ管理とプライバシー保護の構築が関連認証基準または業界のベストプラクティスを満たしていることを証明しています。Tencent Cloud のコンプライアンス情報の詳細については、Tencent Cloud コンプライアンスページをご覧ください。関連するコンプライアンス証明書またはレポートが必要な場合は、Tencent Cloud コンプライアンスドキュメントセンターから申請およびダウンロードしてください。

Tencent Cloud の国際的な権威ある認証、地域および業界での認定事例の一部を以下に示します:

2.1 国際的な権威ある認証

CSA STAR クラウドセキュリティ認証	STAR クラウドセキュリティ評価は、国際的な非営利組織であるクラウドセキュリティアライアンス（Cloud Security Alliance）が推進する、クラウドセキュリティ特性に特化した国際認証です。ISO/IEC 27001 情報セキュリティマネジメントシステムを拡張し、クラウドセキュリティ制御マトリックス（Cloud Control Matrix, CCM）と組み合わせることで、クラウドセキュリティ特有の課題を可視化し、ユーザーに直感的なセキュリティアーキテクチャ評価の概要を提供します。 テンセント社の長年にわたるセキュリティ実践に基づき、Tencent Cloud は CSA STAR グローバルゴールドクラウドセキュリティ認証を取得し、Tencent Cloud のセキュリティ管理システムが国際的な権威あるクラウドセキュリティ基準を満たしていることを示しています。
SOC 監査	システム・組織統制報告書（System and Organization Controls Reports、以下「SOC 報告書」）は、専門的な第三者監査法人によりアメ

	リカ公認会計士協会（AICPA）の関連基準に基づいて発行される、サービス機関の内部統制に関する一連の報告書です。SOC 報告書は独立した監査報告書として、Tencent Cloud プラットフォームの安全性、可用性、機密性に関連する統制ポイントを網羅しています。 異なる検証サービスの種類に応じて、SOC レポートはクラウドユーザーおよびその監査人に提供され、テンセントクラウドユーザーがサービス機関に関連するリスクを評価・解決するための有益な情報を提供します。

2.2 ISO/IEC システム認証

ISO/IEC 22301:2019 認証	ISO/IEC 22301:2019 は、事業継続マネジメント（Business Continuity Management、略称 BCM）をテーマとした国際規格であり、包括的かつ汎用的な BCM 手法を提供します。これにより、企業は潜在的な破壊的イベントを特定・対応し、重要業務の継続性を確保することでリスクを低減し、組織を重大な影響から保護することを目的としています。 Tencent Cloud は ISO/IEC 22301:2019 認証を取得しており、正式な事業継続管理プロセスを構築し、自社の業務の継続性と安定性を確保していることを証明しています。
ISO/IEC 27001:2022 認証	ISO/IEC 27001:2022 情報セキュリティマネジメントシステムは、情報セキュリティ分野において国際的に最も権威があり厳格で、かつ最も広く受け入れられ適用されている体系認証基準です。この認証を取得することは、企業が科学的で効果的な情報セキュリティマネジメントシステムを構築し、企業の発展戦略と情報セキュリティ管理の歩調を統一し、対応する情報セキュリティリスクが適切に管理され正しく対処されることを保証していることを意味します。 ISO 27001:2022 認証の取得は、Tencent Cloud のセキュリティへの取り組みをより明確に示すものであり、科学的で効果的な管理体制を構築し、ユーザーに安全で信頼性の高いクラウド製品とサービスを提供できることを証明します。
ISO/IEC 20000-1:2018 認証	ISO/IEC 20000-1:2018 は IT サービス管理を対象とした国際規格です。この体系は企業の情報技術サービス管理を規範化し、確立・実施・運用・監視・評価・維持・改善のモデルを通じて、企業が関連する情報技術課題を継続的に特定・管理し、ユーザーとのコミュニケーションを強化し、自己改善型の標準化されたサービス体系を構築することを支援します。

	Tencent Cloud は ISO/IEC 20000-1: 2018 認証を取得しており、認証範囲にはクラウドコンピューティングサービス、マネージドサービス、災害復旧サービスなどが含まれます。Tencent Cloud はサービス至上主義の姿勢を厳格に堅持し、顧客との情報技術サービスおよびコミュニケーションの仕組みを整備しています。
ISO/IEC 9001:2015 認証	ISO/IEC 9001:2015 は国際的に広く認知された成熟した品質マネジメントシステムです。このシステムは企業の製品またはサービス提供プロセス全体にわたる品質管理フレームワークと指針的な規範を提供し、企業が製品またはサービスを維持し、安定した一貫性のある品質を保証することを支援します。 Tencent Cloud は ISO/IEC 9001 認証を取得しており、その適用範囲はクラウドコンピューティングサービス、マネージドサービス、災害復旧サービスなどを含みます。Tencent Cloud は品質マネジメントシステムを活用することで、期待される品質目標を効果的かつ効率的に達成し、クラウド製品・サービスの品質と運用を保証しています。
ISO/IEC 27017:2015 認証	ISO/IEC 27017:2015 は ISO/IEC 27002:2013 を補完するクラウドサービス情報セキュリティの実用規格であり、クラウドサービスプロバイダーと顧客に特定のセキュリティ制御とその実施ガイドラインを提供し、クラウドコンピューティングの脆弱性に対する脅威とリスクの管理を強化します。 Tencent Cloud は ISO/IEC 27017:2015 認証を取得しており、これは Tencent Cloud が国際的に認められたベストプラクティスを常に採用していることを示すだけでなく、より包括的なクラウドセキュリティ管理システムを構築し、クラウドセキュリティサービス全体の能力を向上させたことを証明しています。
ISO/IEC 27018:2014 認証	ISO/IEC 27018:2014 は、パブリッククラウド環境における個人識別情報（PII）の処理に関する世界で最も包括的なセキュリティ基準です。この規格は、クラウドサービスプロバイダーに対し、ユーザーのプライバシーを保護する実践ガイドラインを提供し、クラウド環境下での個人データの安全性を確保することを目的としています。 Tencent Cloud が ISO/IEC 27018:2014 認証を取得したことは、Tencent Cloud の個人情報管理システムが国際的な厳格な個人情報保護法規に準拠していることを示し、Tencent Cloud のお客様にクラウドセキュリティに対するさらなる信頼と保証を提供します。

ISO/IEC 29151:2017 認証	ISO/IEC 29151 は、個人識別情報（PII）処理に関する管理措置を実施するための国際規格であり、PII 保護に関連するリスクおよびプライバシー影響評価で特定された要件を満たすことを目的としています。 Tencent Cloud は ISO/IEC 29151:2017 認証を取得しており、これは Tencent Cloud が PII 目標と業務ニーズに基づき適切なセキュリティ管理体制を構築し、クラウド上のユーザーPII に対して高水準のプライバシー保護管理を提供していることを示しています。
ISO/IEC 27701:2019 認証	ISO/IEC 27701:2019 は、ISO/IEC 27001 および ISO/IEC 27002 を拡張したプライバシー情報管理の要求事項とガイドラインであり、プライバシー情報管理システムの構築、実施、維持、継続的改善のための指針を提供し、プライバシーリスクを継続的に管理する上での重要なマイルストーンです。 テンセントクラウドが ISO/IEC 27701:2019 認証を取得したことは、テンセントクラウドが常にユーザーのプライバシー保護をサービスの核心として位置付けていることを証明し、テンセントクラウド製品のプライバシー保護の標準化と信頼性を十分に示しています。

2.3 地域・業界認証

ドイツ C5	クラウドコンピューティング適合性基準カタログ（Cloud Computing Compliance Criteria Catalogue、略称 C5）は、ドイツ連邦情報セキュリティ庁（BSI）が策定したもので、標準化された検査と報告に基づきクラウドサービスプロバイダーの情報セキュリティ適合性を検証することを目的としています。C5 はクラウドサービス分野で業界から広く認められている高水準のセキュリティ基準です。 Tencent Cloud はドイツ C5：2020 の基本および追加審査基準に合格しており、データ保護と情報セキュリティにおいてドイツ政府が設定した高水準を達成したことを意味します。
ドイツ TISAX	TISAX は、ドイツ自動車工業会（VDA）と欧州自動車産業セキュリティデータ交換協会（ENX）が共同で推進する自動車業界向け情報セキュリティ評価およびデータ交換セキュリティ基準です。TISAX により、自動車業界内の情報セキュリティ評価の相互承認が可能となり、共通の評価・交流メカニズムが提供されます。 現在、テンセントクラウドの複数のインターネットデータセンター（IDC）（北京、深センなど）は TISAX レベル 3 評価審査に合格してお

	り、当該地域に展開されているサービスはすべて TISAX の要件を満たし、完全な情報セキュリティ管理システムを構築・維持していることを意味します。
シンガポール MTCS T3 認証	シンガポール多層クラウドセキュリティ（MTCS）基準は、シンガポール情報通信開発庁（IDA）情報技術基準委員会（ITSC）の指導のもと策定されました。MTCS はクラウドの一般的な基準として、クラウドサービスプロバイダーが顧客のクラウドデータに対するセキュリティ・機密性への懸念や、クラウドサービス利用が業務に与える影響への懸念を解決するために採用できます。 Tencent Cloud はシンガポール多層クラウドセキュリティ（MTCS）T3 レベル認証を取得しました。この認証は、Tencent Cloud が健全なリスク管理メカニズムと安全なクラウドサービスを採用し、クラウド上の顧客データの安全性、機密性、および検証可能な運用透明性を保証していることを意味します。
シンガポール OSPAR	アウトソーシングサービスプロバイダー監査報告書（OSPAR）は、シンガポール金融業界におけるアウトソーシングサービスの参入基準です。この基準はシンガポール SSAE 3000 を基盤とし、シンガポールの金融機関向けサービスプロバイダーに対し、物理的レベル管理、一般的な情報技術管理、サービス管理の 3 分野における関連管理設計と運用有効性を検証することを目的としています。 Tencent Cloud の複数の製品・サービスは既にシンガポール OSPAR 監査を通過しており、ABS ガイドラインへの適合性を継続的に確保しています。本監査の通過は、Tencent Cloud のセキュリティ能力がシンガポール、ひいては東南アジアの金融サービスに対する厳格な要件を満たしていることを示しています。
DPTM シンガポールデータ保護信頼マーク	シンガポールデータ保護信頼マーク（DPTM）は、シンガポール個人データ保護委員会（PDPC）と情報通信メディア開発庁（IMDA）によって策定され、組織が責任あるデータ保護実践を示せるようにすることを目的としています。 Tencent Cloud はシンガポールデータ保護信頼マーク（DPTM）認証を取得しており、顧客、ビジネスパートナー、規制当局に対して責任あるデータ保護実践を採用し、収集した個人データを保護する能力を有していることを示しています。
Cyber Trust Mark	Cyber Trust Mark（CTM）は、シンガポールサイバーセキュリティ庁（Cyber Security Agency：CSA）が策定した国家レベルのサイバーセキ

（CTM）[シンガポール]	ュリティ認証です。CTM フレームワークはリスクベースの手法を採用しており、ガバナンス及びリスク管理、サイバーセキュリティ運用、レジリエンス、サプライチェーン及び人的セキュリティ、並びに継続的改善とリーディングプラクティスという 4 つのコア領域にわたる 22 のサブドメインを網羅しています。 テンセントクラウドは、Cyber Trust Mark（CTM）の最高レベルである Tier 5 を取得しました。本認証は、サイバーセキュリティガバナンス、リスク管理、及び運用上のレジリエンスにおけるテンセントクラウドの高度な能力を証明するものであり、アジア太平洋地域全体における規制対象分野及び高需要セクターにおいて、信頼性の高いクラウドサービスプロバイダーとしての地位を確立するものです。
韓国 KISMS 認証	韓国情報セキュリティ保護マネジメントシステム（K-ISMS）認証は、韓国政府が支援する情報セキュリティ認証であり、韓国の企業や組織が適用される韓国の情報通信技術法に基づき、情報資産を一貫して安全に保護することを支援することを目的としています。 Tencent Cloud が KISMS 認証を取得したことは、韓国のクラウド顧客が現地の法的要件への準拠をより容易に証明し、重要なデジタル情報資産を保護できることを意味します。また、Tencent Cloud の情報セキュリティ対策と脅威対応プロセスの能力がさらに強化され、セキュリティ侵害の影響をより効果的に軽減できることを示しています。
マレーシア金融業界 IT コンプライアンス監査	マレーシア中央銀行（BNM）、マレーシア証券委員会（SC）などの金融監督機関は、金融サービス業界向けの関連法規を制定し、マレーシアの銀行、保険、証券などの金融サービスにおける情報技術の利用を規制し、金融情報システムの信頼性、安全性、安定性を確保しています。 テンセントクラウドは、独立した第三者監査を通じて、マレーシアの金融顧客に提供するクラウドサービスがマレーシア金融業界の規制要件を厳格に遵守していることを証明しています。
香港金融業界 IT コンプライアンス監査	香港特別行政区金融管理局（HKMA）、証券先物委員会（SFC）、保険業監督局（HKIA）は、金融・保険・証券機関における情報技術の利用を規制するため、複数の重要な規制要件を発表しています。 Tencent Cloud は独立した第三者監査を通じて、金融業界において信頼できるクラウドサービスプロバイダーであることを証明しています。Tencent Cloud は最も厳格なコンプライアンス義務を積極的に履行するアプローチを採用しており、金融機関は安心して Tencent Cloud を基盤として次世代金融サービスを構築できます。

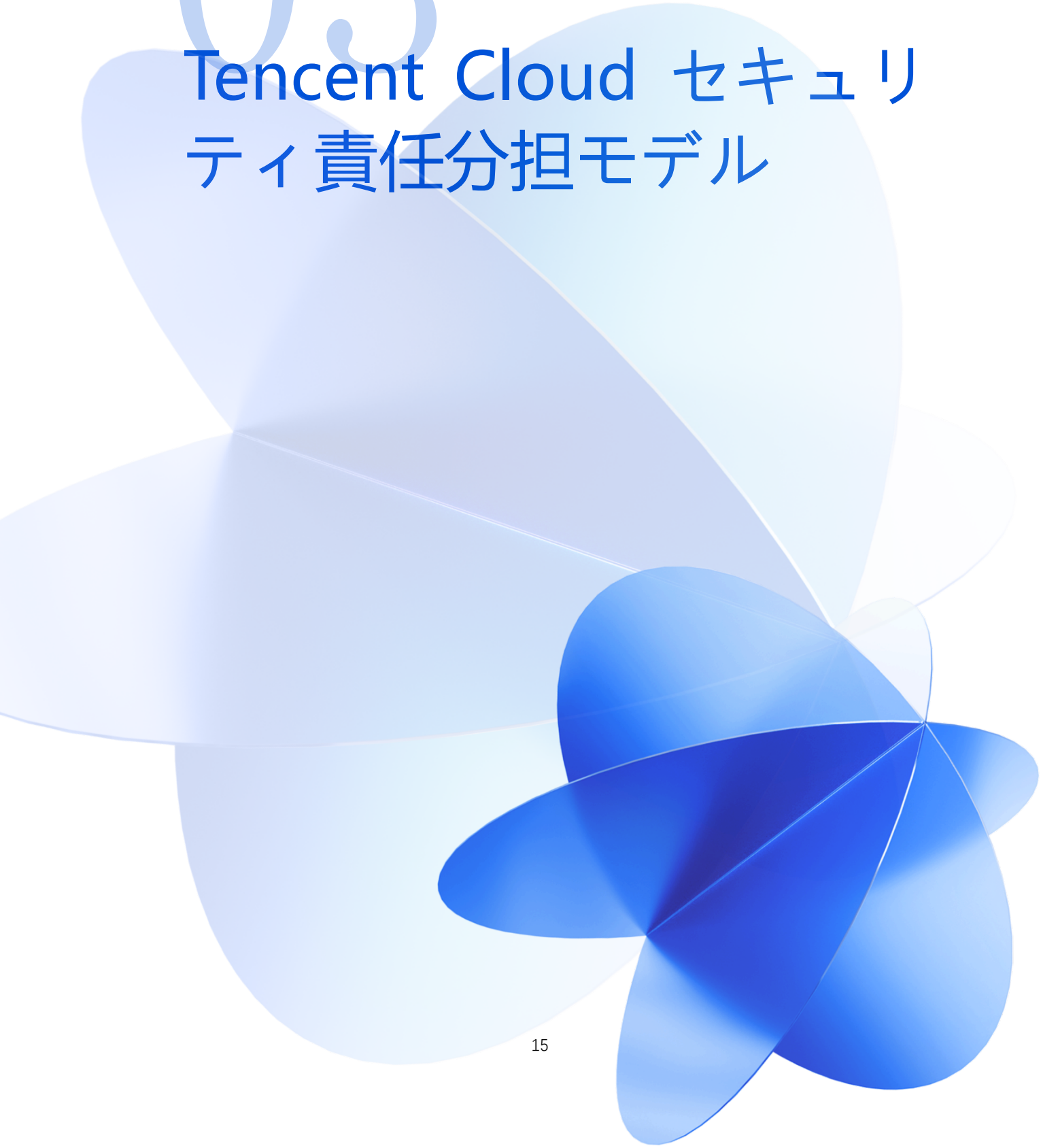
タイ金融業界における IT コンプライアンス監査	タイの金融業界機関は、タイ中央銀行（BoT）、証券取引委員会事務局（OSEC）、保険委員会事務局（OIC）などの金融監督機関および関連法定機関が公布する関連法規・条例を遵守する必要があります。その規制要件は、情報技術運用におけるリスク管理、個人情報保護、銀行・保険・電子政府システムなどにおける情報技術の応用とセキュリティ管理、電子マネー、決済システムインフラ、決済サービスプロバイダーなどをカバーしています。 Tencent Cloud は、独立した第三者監査を通じて、Tencent Cloud がタイの厳格な金融業界規制要件を遵守する能力、および Tencent Cloud がタイの金融業界顧客に高品質でコンプライアンスに準拠したクラウドサービスを提供することに尽力していることを証明できます。
インドネシア金融業界 IT コンプライアンス監査	インドネシア中央銀行（Bank Indonesia）、金融サービス庁（Otoritas Jasa Keuangan、OJK）などのインドネシア金融監督機関は、金融サービス業界向けの関連法規・規制を公布しており、その規制要件は情報技術運用におけるリスク管理、個人情報保護、銀行・保険・電子政府システムなどのシステムにおける情報技術の応用とセキュリティ管理、電子マネー、決済システムインフラ、決済サービスプロバイダーなどをカバーしています。 テンセントクラウドは、独立した第三者監査機関によるインドネシア金融コンプライアンス監査に合格し、インドネシアの金融顧客に提供するクラウドサービスが同国金融業界の規制要件を厳格に遵守していることを証明しました。
フィリピン金融業界 IT コンプライアンス監査	フィリピン金融業界機関は、フィリピン中央銀行 (BSP) などの金融監督機関および関連法定機関が制定した関連法規・条例を遵守する必要があります。その規制要件は、情報技術運用におけるリスク管理、個人情報保護、銀行・保険・電子政府システムなどのシステムにおける情報技術の応用とセキュリティ管理、電子マネー、決済システムインフラ、決済サービスプロバイダーなどをカバーしています。 テンセントクラウドは、独立した第三者監査を通じて、フィリピンの厳格な金融業界規制要件を遵守する能力、および金融業界の顧客に高品質でコンプライアンスに適合したクラウドサービスを提供するという取り組みを証明しています。
アメリカ映画協会 MPAA	アメリカ映画協会（MPAA）は、保護されたメディアコンテンツの安全な保管、処理、配信に関するベストプラクティス基準を確立しています。本実施ガイドラインは、MPAA 協会メンバーと協力関係にあるアプリケ

	ーションおよびクラウドサービスプロバイダーが、コンテンツセキュリティに関して遵守すべき要件を理解することを目的としています。MPAA コンテンツセキュリティテンプレートの構成要素は、関連する ISO 規格（27001-27002）、セキュリティ基準（NIST、CSA、ISACA、SANS など）、および業界のベストプラクティスを参照しています。 Tencent Cloud は、ISO 27001、ISO 27017、ISO 27018、PCI DSS、CSA STAR などの関連認証を取得しています。また、Tencent Cloud は自己評価を通じて、顧客コンテンツの管理プロセスがアメリカ映画協会（MPAA）のコンテンツセキュリティモデルガイドラインに準拠していることを確認しています。
アメリカ HIPAA	アメリカ HIPAA 法の目的の一つは、電子健康記録の利用を促進し、情報共有の強化を通じて医療システムの効率性と品質を向上させることです。HIPAA は、保護対象健康情報（PHI）の作成、受領、維持、伝送などのプロセスにおいて、事業体およびそのビジネスパートナーが PHI の安全性（可用性、完全性、機密性を含む）とプライバシーを保護することを求めています。HIPAA の規制対象となる事業体およびそのビジネスパートナーは、PHI の処理、維持、保管などの場面において、対応するセキュリティ対策を提供する必要があります。 Tencent Cloud は自己評価を通じて、ユーザーの個人情報に対するセキュリティ保護能力と管理措置の有効性が HIPAA のコンプライアンス要件に準拠していることを保証しています。
アメリカ SEC 規則 17a-4	Tencent Cloud オブジェクトストレージサービス（COS）は、アメリカ証券取引委員会（SEC）、金融業規制機構（FINRA）、商品先物取引委員会（CFTC）の技術要件に基づき、記録管理と情報ガバナンスを専門とする独立した第三者評価機関による認証を取得しています。 この認証は、高度に規制された環境（金融サービス業界など）で事業を展開する顧客に対し、Tencent COS の書き換え不可・消去不可の保存方法およびオブジェクトロック機能を保証し、Tencent Cloud が安全で業界標準に準拠したクラウド製品を提供するというコミットメントを示しています。
日本 FISC	金融機関のセキュリティ強化を目的として、「FISC 銀行及び関連金融機関コンピュータシステムセキュリティガイドライン」は、日本の銀行および金融機関が安全な情報システムを構築し、その運用を保証するための効果的な指針を提供しています。

	Tencent Cloud は独立したサービス監査人による監査を受け、これに基づきシステムおよび組織統制（SOC）報告書を作成しています。同報告書は Tencent Cloud プラットフォームの安全性、可用性、機密性に関連する統制ポイントを網羅し、Tencent Cloud の関連措置が FISC 銀行及び関連金融機関向けコンピュータシステムセキュリティガイドラインの要求を満たすことを証明しています。
英国 BS10012: 2017	BS10012: 2017 は英国規格協会（BSI）が発行し、組織にプライバシー保護のコンプライアンスフレームワークとベストプラクティスを提供し、企業が個人情報管理システム（PIMS）を構築・維持し、個人情報を保護するための十分かつ適切な管理措置を確保することを指導する。このシステムは一般データ保護規則 (GDPR) に準拠するよう更新・改訂されている。 Tencent Cloud は BS10012: 2017 認証を取得しており、Tencent Cloud の個人情報管理システムが国際基準と業界のベストプラクティスを満たしていることを示しています。これにより、お客様は GDPR のプライバシー保護要件をより適切に遵守することが可能となります。
EU CISPE	CISPE 行動規範は、EU の一般データ保護規則（GDPR）第 40 条に基づき、クラウドインフラサービスプロバイダー向けの汎欧州業界固有のガイドラインであり、欧州全域の組織が消費者、企業、機関向けに GDPR 準拠のクラウドベースサービスを迅速に開発することを支援します。 Tencent Cloud は CISPE 行動規範の「候補」マークを取得しており、これは Tencent Cloud が CISPE 行動規範の要件に基づく自己評価を完了し、文書体系と実施レベルにおけるコンプライアンスを証明したことを意味します。
NIST CSF 認証	NIST CSF は、ビジネス要因を用いてサイバーセキュリティ活動を導き、サイバーセキュリティリスクを組織のリスク管理プロセスの一部として位置付けることに重点を置いたフレームワークです。これにより、組織は自社のビジネスニーズ、リスク許容度、リソースに基づいてサイバーセキュリティ活動を調整・優先順位付けすることが可能となり、このフレームワークのリスク管理原則とガイドラインを適用することで、セキュリティとレジリエンスを向上させることができます。 Tencent Cloud は第三者機関による NIST CSF 認証を取得しました。これは Tencent Cloud のサイバーセキュリティ防御システムの能力が認められただけでなく、Tencent Cloud がセキュリティリスクを効果的に識別・防御・対応・処理し、顧客のクラウド資産とデータを保護できる

	ことを示しており、顧客の Tencent Cloud に対する安全性と安定性への信頼を強化しています。
PCI DSS 認証	ペイメントカード業界データセキュリティ基準 (PCI DSS) は、ペイメントカード業界セキュリティ基準委員会 (PCI SSC) によって策定・維持されています。カード会員のデータセキュリティ強化を目的とし、PCI DSS はアカウントデータ保護に関する技術的・運用上の要件について世界統一の基準を提供します。適用範囲は、加盟店、処理業者、アクワイアラー、発行機関、サービスプロバイダーなど、ペイメントカード処理に関わるすべての事業体、およびカード会員データを保存・処理・伝送するその他の事業体に及びます。 Tencent Cloud は PCI DSS 認証審査を通過し、PCI DSS レベル 1 サービスプロバイダーの資格を取得しました。これは Tencent Cloud が顧客に安全で信頼性の高い決済サービスを提供し、カード会員のデータを保護できることを証明しています。
GxP コンプライアンス	医療業界において、GxP は広範なコンプライアンス関連活動をカバーし、通常は医薬品、医療機器、医療ソフトウェアアプリケーションなどの医療製品の開発、製造、販売を規定する規制、ガイドライン、または業界のベストプラクティスを指します。 Tencent Cloud は GxP コンプライアンスに関するホワイトペーパーを発表し、医療業界の顧客に対し、Tencent Cloud の管理プロセスと技術的措置が顧客の GxP コンピュータ化システム要件の達成を支援すること、および Tencent Cloud がホストする顧客の業務データの機密性、完全性、可用性を確保することを説明しています。

03 Tencent Cloud セキュリティ責任分担モデル



現在、ますます多くの顧客がクラウドコンピューティングサービスプロバイダーとその製品・サービスを選択する際、セキュリティを最優先の考慮要素の一つとしています。

Tencent Cloud は、クラウドコンピューティングサービスの開放性と共有性を堅持し、クラウドプラットフォームとクラウドサービスのセキュリティ能力を継続的に向上させるとともに、お客様と協力してクラウド上のビジネスとデータのためのより良く、より完璧なセキュリティ保証システムを構築しています。クラウドサービスプロバイダーとして、Tencent Cloud はデータセンターインフラストラクチャとクラウドプラットフォームのセキュリティを担当します。お客様が異なるクラウドサービスカテゴリ（例：IaaS、PaaS、SaaS サービス）を選択する場合、各コンポーネントに対する制御権限も異なることを考慮し、Tencent Cloud はサービスカテゴリごとにクラウドセキュリティ責任分担モデルを確立しています。このモデルでは、水色部分が Tencent Cloud の責任範囲、薄灰色部分がお客様の責任範囲、薄緑色部分が Tencent Cloud とお客様が共同で責任を負う領域を示しています。

	IaaS	PaaS	SaaS	
カスタマーの責任	クラウドカスタマーのデータセキュリティ	クラウドカスタマーのデータセキュリティ	クラウドカスタマーのデータセキュリティ	
	クラウドカスタマーのアカウントおよびアクセス制御ポリシー	クラウドカスタマーのアカウントおよびアクセス制御ポリシー	クラウドカスタマーのアカウントおよびアクセス制御ポリシー	
	クラウド上セキュリティ構成ポリシー	クラウド上セキュリティ構成ポリシー	クラウド上セキュリティ構成ポリシー	異なるサービスへシナリオにおける共同責任
	クラウド上アプリケーションセキュリティ	クラウド上アプリケーションセキュリティ	クラウド上アプリケーションセキュリティ	
	クラウド上仮想化ネットワークおよびホストセキュリティ	クラウド上仮想化ネットワークおよびホストセキュリティ	クラウド上仮想化ネットワークおよびホストセキュリティ	腾讯クラウドの責任
	クラウドプラットフォームおよび製品自体のセキュリティコンプライアンス	クラウドプラットフォームおよび製品自体のセキュリティコンプライアンス	クラウドプラットフォームおよび製品自体のセキュリティコンプライアンス	
	物理的および基盤インフラストラクチャのセキュリティ	物理的および基盤インフラストラクチャのセキュリティ	物理的および基盤インフラストラクチャのセキュリティ	

図 1：Tencent Cloud 情報セキュリティ責任分担モデル

図中の各セキュリティ属性の説明は以下の通りです：

- クラウドカスタマーのデータセキュリティ：クラウド環境における顧客の業務データ自体のセキュリティ管理を指し、アップロード、保存、配信、加工、その他の方法で処理される顧客業務データなどを含む。

- クラウドカスタマーのアカウントおよびアクセス制御ポリシー：顧客が登録した Tencent Cloud アカウント情報、およびクラウドアカウントに基づくすべての認可行為（アカウント情報、パスワード、アクセス制御ポリシー、認証情報など）を指します。
- クラウド上セキュリティ構成ポリシー：クラウド製品（セキュリティ製品を含む）を適切に開発または使用するために、異なるシナリオと業務セキュリティ要件に適合したセキュリティ製品およびセキュリティ設定ポリシーを指します。
- クラウド上のアプリケーションセキュリティ：クラウドコンピューティング環境における業務関連アプリケーションシステムのセキュリティ管理を指し、アプリケーションの設計、開発、リリース、運用保守、監視運用などを含む。
- クラウド上仮想化ネットワークおよびホストセキュリティ：クラウド環境におけるホストとネットワークのセキュリティ管理を指し、ネットワーク層では仮想ネットワーク、ロードバランシング、セキュリティゲートウェイ、VPN、専用回線などを含む。ホスト層ではクラウドコンピューティング、クラウドストレージ、クラウドデータベースなどのクラウド製品の基盤管理（仮想化制御層、データベース管理システム、ディスクアレイネットワークなど）および使用管理（仮想ホスト、イメージ、CDN、ファイルシステムなど）を含む。
- クラウドプラットフォームおよび製品自体のセキュリティコンプライアンス：クラウド環境におけるクラウドプラットフォーム及び提供されるクラウド製品/サービス自体のセキュリティとコンプライアンスを指す。
- 物理的および基盤インフラストラクチャのセキュリティ：クラウド環境におけるデータセンターの安全運用、物理サーバーおよび物理ネットワーク機器のセキュリティ管理などを指します。

セキュリティ責任分担モデルに関する詳細は『Tencent Cloud Security White Paper』をご参照ください。

04

Tencent Cloud グローバルインフラストラクチャ

Tencent Cloud は世界中に複数のデータセンターを展開し、大規模なインフラストラクチャネットワークを形成しています。これにより、世界中の顧客に高速で安定した、インテリジェントかつ信頼性の高いニアサービスを提供できます。テンセントクラウドは中国本土、アジア太平洋地域、北米地域、欧州地域において 20 以上のリージョン（Region）を開設し、60 以上のアベイラビリティゾーン（Availability Zone）を運営しています。これにより、より多くの企業に強力な技術サポートを提供し、ビジネスの急速な拡大を支援するとともに、お客様が各地域の規制要件に柔軟に対応できるよう支援します。金融業界の企業におけるデータのローカルストレージとビジネスのグローバル化ニーズを満たし、データ処理のコンプライアンス、安全性、効率性を確保します。

- リージョン（Region）とは物理的なデータセンターの地理的区域を指します。Tencent Cloud の各リージョン間は完全に分離されており、異なるリージョン間で最大限の安定性とフォールトトレランスを保証します。アクセス遅延の低減とダウンロード速度の向上のため、最も近いリージョンの選択をお勧めします。
- アベイラビリティゾーン（Zone）とは、同一リージョン内で電力・ネットワークが相互に独立した物理データセンターを指します。その目的は、アベイラビリティゾーン間の障害を相互に隔離（大規模災害や大規模停電を除く）し、障害の拡散を防ぎ、ユーザーのビジネスを継続的にオンラインサービス状態に保つことです。独立したアベイラビリティゾーン内のインスタンスを起動することで、ユーザーはアプリケーションを単一ロケーションの障害から保護できます。

Tencent Cloud は現在、中国国内に 2300 以上のアクセラレーションノードを展開し、複数の通信事業者をカバーしています。海外には 900 以上のアクセラレーションノードを配置し、世界 70 以上の国と地域をカバーしています。サービスコンテンツをネットワーク全体のアクセラレーションノードに配信し、グローバルスケジューリングシステムを活用することで、ユーザーは最寄りのノードから必要なコンテンツを取得でき、アクセス遅延を低減します。

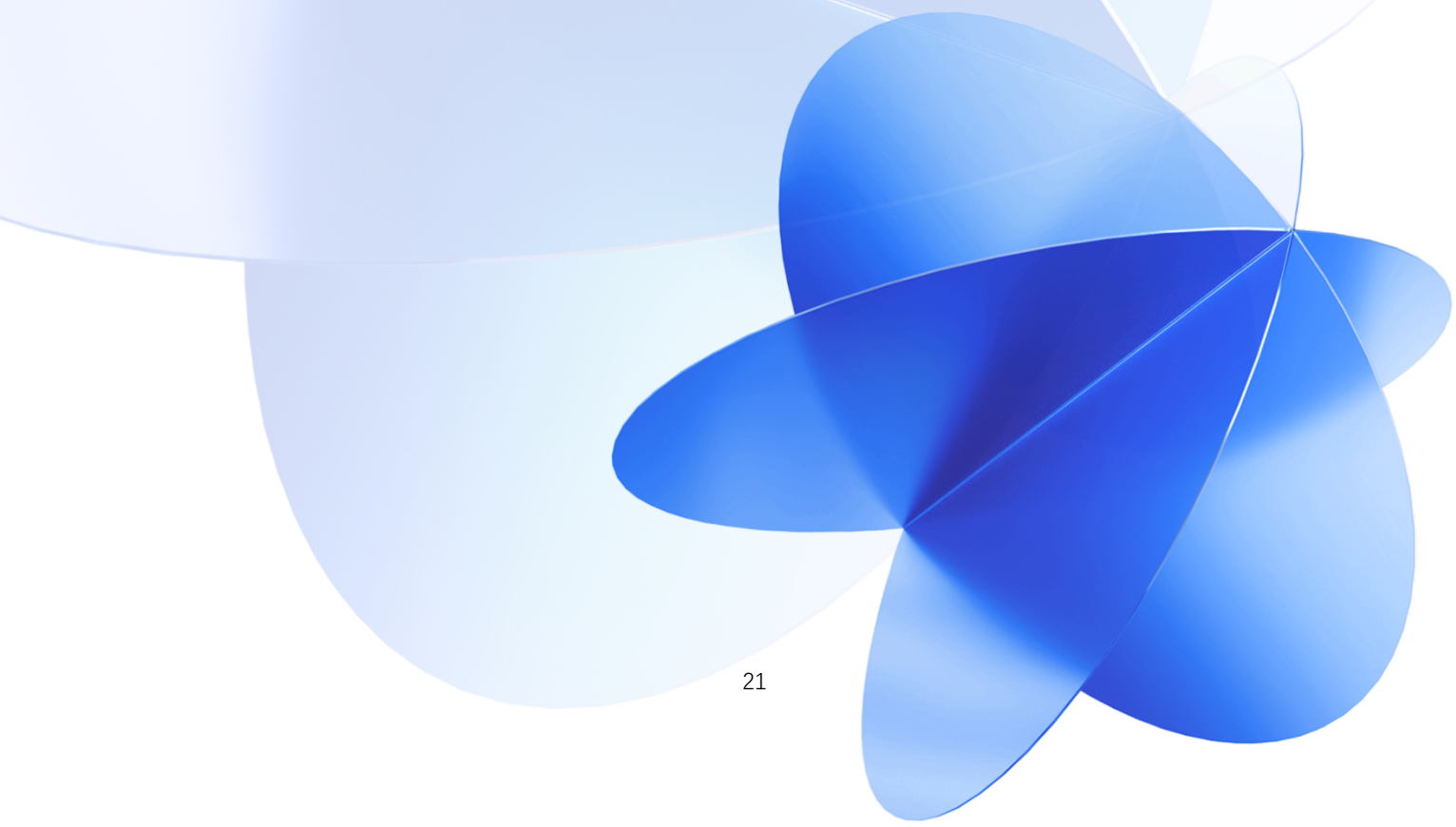
さらに Tencent Cloud は独立したサイトの設置に加え、データ暗号化、アクセス制御、監査追跡などの技術的手段を採用し、データの分離性と安全性を強化。データ

漏洩や不正アクセスを防止するとともに、データの地域的分離とコンプライアンス対応を強化しています。

Tencent Cloud のインフラストラクチャに関する詳細情報は、Tencent Cloud グローバルインフラストラクチャページをご参照ください。

05

Tencent Cloud が『クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）』に従っています



『クラウドサービス提供時の情報セキュリティ対策ガイドライン（第 3 版）』は、主にクラウドサービスプロバイダーとクラウドサービス利用者がそれぞれの責任範囲内で講じるべき情報セキュリティ対策について指針を示すものである。本ガイドラインは『クラウドサービス提供時の情報セキュリティ対策ガイドライン（第 2 版）』（2018 年 7 月）を基礎とし、政府情報システムセキュリティ管理・評価計画（ISMAP）管理基準、ISO/IEC 27017:2016、NIST SP 800-53 Rev.5 を参照して改訂され、クラウドサービスの特性に基づいた情報セキュリティ対策を包括的に網羅しています。これらの情報セキュリティ対策は、異なるクラウドサービスの種類を考慮し、共通対策、SaaS 関連対策、PaaS/IaaS 関連対策に分類され、「基本」対策と「推奨」対策の 2 つの対策レベルに区分されています。

本章では、Tencent Cloud が『クラウドサービス提供時の情報セキュリティ対策ガイドライン（第 3 版）』から関連する情報セキュリティ対策を抽出し、クラウドサービスプロバイダーとして Tencent Cloud が関連ガイドラインにどのように準拠しているかを説明します。

5.1 共通編

5.1.1 情報セキュリティへの組織的取組の基本方針

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
Ⅱ.1.1	組織の基本的な方針を定めた文書	Ⅱ.1.1.1【基本】方針の作成・承認・配布: 事業者は、組織全体での情報セキュリティに関する取組についての基本的な方針、役割、責任等を定めた文書を作成し、経営陣の承認及び署名等を経て、組織内及び関係する組織に配布すること。 Ⅱ.1.1.2【基本】方針の変更: 情報セキュリティに関する基本的な方針を定めた文書は、定期的又はクラウドサービスの提供に係る重大な変更や不適合が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。事業者は、経営陣の承認の下で方針の改定等を実施し、組織内及び関係する組織に通知すること。	**情報セキュリティ管理ポリシーに関して、**テンセントクラウドは情報セキュリティ管理ポリシーを策定しており、情報セキュリティ全体戦略、セキュリティ組織体制及びセキュリティ管理体系で構成され、クラウドプラットフォームの安全な運用とリスク管理を効果的に支援しています。テンセントクラウドの情報セキュリティポリシーは年次レビューを実施し、クラウドセキュリティ管理体系の管理目標、管理手順及び管理措置が関連するセキュリティ戦略、基準、手順及び法的要件に適合していることを確認し、情報セキュリティポリシーの十分性と有効性を保証しています。テンセントクラウドは、ISO/IEC 27001 情報セキュリティマネジメントシステム、ISO/IEC 27017 クラウドサービス情報セキュリティマネジメントシステム、ISO/IEC

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		Ⅱ.1.1.3【推奨】 文書保護: 事業者は、情報セキュリティに関する基本的な方針を定めた文書を、不正な開示による漏洩や変更等から保護すること。	22301 事業継続マネジメントシステム、ISO/IEC 20000 情報技術サービスマネジメントシステムなどの国際セキュリティ関連標準認証を取得済みです。 **文書公開と保護に関して、**情報セキュリティ管理ポリシー及び関連する体系制度などの文書は、承認後テンセントクラウド内部プラットフォームに公開され、アクセス制御と権限管理などの措置を通じて文書を保護し、不正な漏えいや変更を防止しています。関連文書管理者は文書の改訂・変更権限を有し、対応する体系文書の維持・管理を担当します。文書利用者は、当該プラットフォーム内で対応する文書を閲覧することのみ可能です。

5.1.2 情報セキュリティのための組織

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
Ⅱ.2.1	内部組織	Ⅱ.2.1.1【基本】情報セキュリティ責任者: 経営陣は、情報セキュリティに関する取組についての責任と関与を明示する。更に、組織全体にわたる情報セキュリティに責任を持つ情報セキュリティ責任者を任命し、人員・資産・予算等のリソース面で積極的な支援・支持を行うこと。 Ⅱ.2.1.2【基本】システム一覧: 情報セキュリティ責任者は、組織が保有、提供するシステム、アプリケーション及びクラウドサービスの一覧を作成し、全ての責任者を定めるとともに、個々の組織の職務記述書にセキュリティとプライバシーに関する役割と責任を記載すること。 Ⅱ.2.1.3【基本】相反する職務と責任の分離: 組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低	**情報セキュリティ管理組織体制に関して、**テンセントクラウドはクラウドセキュリティ及び情報セキュリティ関連の組織体制を構築し、職責分離などの原則に基づいて異なる階層のセキュリティ機能役割と関連責任を明確化し、情報セキュリティ監査と情報セキュリティリスク評価などの作業メカニズムを定義しています。テンセントはセキュリティ技術委員会と異なる職能・分野の専門セキュリティチームを設置し、内部に完備された人的資源管理基準及び手順を確立し、職務要件に応じた人員の採用と配置を確保しています。 **資産管理に関して、**テンセントクラウドは情報資産管理規範と全ライフサイクル管理プロセスを策定し、電子データ、ハードウェア及びその仮想デバイス、インフラストラクチャ、アプリケーションシステム、ソフトウェアなどの資産を分類・階層化して管理・保護しています。テンセントクラウドは資産管理システムを通じてハー

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		減するために、相反する職務及び責任範囲は、分離すること。 Ⅱ.2.1.4【推奨】 リスク管理戦略: 情報セキュリティへの侵害が、業務、情報資産、個人、他の組織及びサプライチェーンへもたらす脅威に対するリスクを管理するために、組織全体の包括的なリスク管理戦略を策定する。リスク管理戦略は、定期的又はクラウドサービスの提供に係る変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。 Ⅱ.2.1.5【推奨】 テスト、トレーニング及びモニタリング：組織の情報システムに関連するテスト、トレーニング及びモニタリングを計画し、継続的に実施すること。また、当該計画をレビューし、組織の情報セキュリティに関する基本方針に適合しているかを確認し、必要に応じて見直しを行うこと。 Ⅱ.2.1.6【推奨】 組織内苦情管理: 組織の情報セキュリティ施策とプライバシーの取組に対する従業員からの苦情、懸念又は質問を受け取り、対応するための仕組みを構築すること。	ドウェア機器及びソフトウェアコンポーネントを管理し、資産登録及び紐付け、資産棚卸及び情報更新、資産廃棄及び交換などを含め、クラウドプラットフォーム基盤システムの安定した運用を保障し、業務システムに信頼性の高い支援を提供しています。 **リスク管理に関して、**テンセントクラウドは内部で情報セキュリティリスク管理手順を策定し、リスク管理全プロセス（リスク識別、リスク分析、リスク対応計画の策定、リスク追跡及び監視）の作業内容を明確に定義し、指針を示しています。テンセントクラウドはクラウド業界の変化動向と内部管理実践に基づき、リスク評価方法とリスク登録簿の維持及び改訂を実施しています。 **システムテストと審査に関して、**テンセントクラウドセキュリティチームは年１回以上の内部セキュリティ監査を実施し、クラウドプラットフォームと内部システムの状況を継続的に監視し、良好なセキュリティ態勢を維持し、関連法令法規及びセキュリティ管理基準の規定と要件に適合することを確保しています。逸脱が発見された場合、実際の又は潜在的な原因を分析し、是正・予防措置の必要性と優先順位を評価し、関連承認を得た後是正・予防措置を実施します。 **内部苦情管理に関して、**テンセントクラウドは内部コミュニケーション管理メカニズムを構築し、情報セキュリティマネジメントシステム運用プロセスにおいて識別された問題、並びに従業員からの情報セキュリティ又はプライバシー保護関連作業に関する提案や苦情を受付け、処理するために活用されています。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
Ⅱ.2.2	モバイル機器及びテレワーキング	Ⅱ.2.2.1【基本】モバイル機器の利用方針：モバイル機器を業務で用いることによって生じるリスクを管理するために、モバイル機器の利用方針を策定し、その方針を実施するために必要な情報セキュリティ対策を講じること。 Ⅱ.2.2.2【基本】テレワーキングでの情報保護：テレワーキングでアクセス、処理及び保存する情報資産を保護するための方針を策定し、情報セキュリティ対策を実施すること。	**モバイルデバイス管理に関して、**テンセントクラウドはモバイルオフィスセキュリティ管理関連規範を策定し、内部モバイルデバイスの安全使用基準及びモバイルオフィスアプリケーションの情報セキュリティ保証要件を明確化しています。従業員のモバイルデバイス（ノートパソコン等）に対して、テンセントクラウドはゼロトラストセキュリティ管理システムを導入し、ウイルス駆除、脆弱性修正、能動的防御などのセキュリティ機能を通じて、ランサムウェア対策、フィッシング攻撃対策、内部横断移動対策などの包括的なセキュリティ保護を実現しています。ゼロトラストセキュリティ管理システムは機微データの外部送信監視機能もサポートし、メールボックス、オンラインストレージ、リモートコントロール、ファイル転送ツールなどのファイル外部送信行為を監査・遮断し、潜在的なデータ窃取活動を防止します。 **リモートアクセス管理に関して、**テンセントクラウドは内部従業員向けリモートアクセス管理関連手順を確立し、従業員はテンセントクラウドに登録済みの信頼できるデバイスのみを使用し、暗号化通信チャネルを通じてテンセントクラウドのオフィスネットワーク及び日常業務システムにリモートアクセスできます。テンセントクラウドはリモートアクセスログを維持し、ユーザー操作行動を記録します。同時に、テンセントクラウドの内部オフィスネットワークと顧客データが存在する生産環境は完全に分離されており、テンセントクラウド従業員が顧客の同意と承認を得て顧客情報資産にアクセスする場合、必ずジャンプサーバーを経由して顧客データが存在する生産環境にアクセスする必要があり、バックエンド運用操作記録は全てログプラットフォームに集中保存され、テンセントクラウド内部監査チームが定期

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			的に記録情報を審査します。

5.1.3 サプライチェーンに関する管理

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
Ⅱ.3.1	サプライチェーン事業者間の合意	Ⅱ.3.1.1【基本】リスク対策と文書化：サプライチェーン事業者が提供するクラウドサービスについて、事業者間で合意された情報セキュリティリスク対策及びサービスレベルを文書化するとともに、サプライチェーン事業者によって確実に実施されることを担保すること。 Ⅱ.3.1.2【基本】サービスの監視：サプライチェーン事業者が提供するクラウドサービスを定常的に監視・レビューし、運用に関する記録及び報告を常に実施すること。また、定期的に監査を実施することについて、サプライチェーン事業者と合意し文書化すること。 Ⅱ.3.1.3【基本】リスク評価とレビュー：サプライチェーン事業者が提供するシステム、システムコンポーネント、クラウドサービスに関連するリス クを評価及びレビューすることについて、サプライチェーン事業者と合意し文書化すること。 Ⅱ.3.1.4【基本】関連情報の保護：システム、システムコンポーネント、クラウドサービスに関するサプライチェーン関連の情報を保護することについて、サプライチェーン事業者と合意し文書化すること。 Ⅱ.3.1.5【基本】侵害通知：サプラ	テンセントクラウドは、サプライチェーンセキュリティ管理体系を確立しており、関連するセキュリティ要件はサプライチェーン管理の全ライフサイクル（供給関係計画、サプライヤー選定、供給関係契約、供給関係管理、供給関係終了など）を網羅しています。 発注者として、テンセントクラウドは調達前に、サプライチェーンセキュリティリスク許容度に適合した調達戦略を策定し、サプライヤーに対する情報セキュリティベースライン要件を明確化します。サプライヤーを選定する際、テンセントクラウドはサプライヤーの情報セキュリティ成熟度、事業継続性計画、緊急時復旧能力などを考慮・評価します。サプライヤー選定後、テンセントクラウドはサプライヤーと関連契約を締結し、契約内容には通常、提供サービス範囲、サービスレベル、情報セキュリティ要件、情報セキュリティ責任分担、個人情報保護の役割と責任、機密保持要件、アフターサポート、変更管理、審査・監査権利などが含まれ、サプライヤーにはセキュリティインシデント関連情報のテンセントクラウドへの速やかな共有が求められます。 さらに、供給関係継続期間中、テンセントクラウドは主に定期監査と評価などの措置を通じて、サプライヤーへの効果的な管理・統制を確保しています。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		イチェーンのセキュリティ侵害に関する通知について、その手順を確立し、サプライチェーン事業 者と合意し文書化すること。 II.3.1.6【基本】変更管理：関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価に伴う、サプ ライチェーン事業者によるサービス提供の変更（現行の情報セキュリティの方針群、手順及び対応策 の保守及び改善を含む）を管理することについて、サプライチェーン事業者と合意し文書化すること。 II.3.1.7【推奨】耐タンパー性と検出: システム、システムコンポーネント、クラウドサービスの改ざん防止プログラムを実装し、情報資産の完全性を保証することについて、サプライチェーン事業者と合意し文書化すること。 II.3.1.8【推奨】システム又はシステムコンポーネントの検査：改ざんを検出して情報資産の完全性を保証するために、システム、システムコンポーネント又はクラウドサービスをランダムに検査することについて、サプライチェーン事業者と合意し文書化すること。 II.3.1.9【推奨】システムコンポーネントの信頼性：偽造されたシステムコンポーネントがシステムやクラウドサービスに侵入することを検出及び防止する手段を実装することについて、サプライチェーン事業者と合意し文書化すること。 II.3.1.10【基本】システムコンポーネントの廃棄: データ、ドキュメント、ツール又はシステムコンポーネントを廃棄する方法を確立する	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		とともに、廃棄方法についてサプライチェーン事業者と合意し文書化すること。	
Ⅱ.3.2	サプライチェーン事業者の選定	Ⅱ.3.2.1【基本】選定・契約: サプライチェーン事業者のリスクからクラウドサービスを保護するために、状況に応じて最も適した取得・調達・契約方法を採用すること。	

5.1.4 情報資産の管理

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
Ⅱ.4.1	情報資産に対する責任	Ⅱ.4.1.1【基本】管理責任者: 取り扱う各情報資産について管理責任者を定めるとともに、その利用の許容範囲 (利用可能者、利用目的、利用方法、返却方法等) を明確にした上で管理するとともに、文書化すること。 Ⅱ.4.1.2【基本】事業者間の引継ぎ: クラウドサービス利用者がクラウドサービスの利用を終了するにあたり、他のクラウドサービスへの乗換を行うことが想定される。クラウドサービス利用者によるクラウドサービス選定の自由を守るため、事業者は預託された情報を他のクラウドサービスに引き継ぐか否かに関して、予め利用者と合意し、文書化すること。 Ⅱ.4.1.3【基本】バックアップ: 情報資産、ソフトウェア及びシステムのバックアップは、利用者と合意されたバックアップ方針に従って、事業者が定期的に実施し、バックアップ内容を検査すること。また、事業者は、利用者にバックアップ機能の仕様を提供すること。 Ⅱ.4.1.4【推奨】 当初目的との一致: 時間の経過とともに、当初の目	**資産管理に関して、**テンセントクラウドは情報資産管理規範と全ライフサイクル管理プロセスを策定し、電子データ、ハードウェア及びその仮想デバイス、インフラストラクチャ、アプリケーションシステム、ソフトウェアなどの資産を分類・階層化して管理・保護しています。テンセントクラウドは資産管理システムを通じてハードウェア機器及びソフトウェアコンポーネントを管理し、資産登録及び紐付け、資産棚卸及び情報更新、資産廃棄及び交換などを含め、クラウドプラットフォーム基盤システムの安定した運用を保障し、業務システムに信頼性の高い支援を提供しています。 **クラウドサービスの終了と退出に関して、**顧客が業務変更や将来の IT 計画に伴い契約を終了する必要がある場合、任意の時点でクラウド上のデータと生産環境のバックアップ及び移行を選択できます。テンセントクラウドは、顧客が汎用的な標準フォーマットでデータをバックアップまたは移行することをサポートしており、顧客はクラウド移行段階と同様の転送方式及び転送プロトコル、又は Direct Connect

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		的や提供機能の範囲外のサービス及び機能をサポートする場合があるが、情報資産の使用目的が、当初の使用目的と一致していることを確認すること。	(DC) 、VPN Connection などのネットワークサービス製品を利用することで、クラウドからの退出段階におけるデータの安全性と信頼性を確保できます。 **バックアップ管理に関して**、テンセントクラウドはバックアップ管理手順を策定し、関連法令規範の要求に基づき、収集・処理した重要データのバックアップを実施しています。クラウド上の顧客データについては、テンセントクラウドはクラウド製品またはサービスの機能に応じて、複数のストレージレプリカとバックアップサービスを顧客に提供し、製品サービスレベル契約に定める通り、提供するデータバックアップサービスに対して責任を負います。
Ⅱ.4.2	情報の分類	Ⅱ.4.2.1【基本】資産目録：組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、機密性や重要性の観点から情報資産を分類した上で、資産目録を作成し、維持すること。 Ⅱ.4.2.2【基本】データ識別：事業者は、利用者のデータ及びクラウドサービスから派生したデータを明確に識別すること。 Ⅱ.4.2.3【基本】情報資産の取扱い：情報資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施すること。	**資産管理に関して、**テンセントクラウドは情報資産管理規範と全ライフサイクル管理プロセスを策定し、電子データ、ハードウェア及びその仮想デバイス、インフラストラクチャ、アプリケーションシステム、ソフトウェアなどの資産を分類・階層化して管理・保護しています。テンセントクラウドは資産管理システムを通じてハードウェア機器及びソフトウェアコンポーネントを管理し、資産登録及び紐付け、資産棚卸及び情報更新、資産廃棄及び交換などを含め、クラウドプラットフォーム基盤システムの安定した運用を保障し、業務システムに信頼性の高い支援を提供しています。 **データガバナンスに関して**、テンセントクラウドはデータセキュリティ関連管理手順を確立し、データ分類・階層化とデータ保護原則を明確化しています。データ所有者は、データ分類・階層化の要件に基づき、データ収集、転送、アクセス制御、バックアップ、取引保護、並びに第三者との情報転送管理の全ライフサイクルにおい

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			て、対応するセキュリティ保護措置を実施し、データの機密性、完全性及び可用性を保護することが求められます。テンセントクラウドの電子データの分類には、顧客クラウド業務データ、テンセントクラウドデータ、プライバシーデータが含まれます。顧客クラウド業務データとは顧客（クラウドテナント）のクラウド上の業務データ情報を指し、テンセントクラウドデータとはテンセントクラウドサービスの運用・保守により生成されるデータを指し、プライバシーデータとは顧客がクラウドサービス利用過程において提供する個人データを指します。 顧客データはテンセントクラウド内部において高セキュリティレベルのデータに位置付けられ、顧客は自身のデータ内容に対して唯一の所有権と管理権を有します。サービス提供や障害対応の必要性があり、かつ顧客の明確な承認を得ている場合、又は国家・地方政府機関による犯罪事件の調査など国家法令法規に適合する場合を除き、テンセントクラウド内部従業員が顧客データにアクセスすることは一切ありません。 さらに、テンセントクラウドは顧客に対し、**Data Security Governance Center (DSGC)** を提供し、顧客がデータ資産を自動的に整理し、企業のクラウド上のデータを分類・階層化及びセキュリティリスク評価することを支援しています。
Ⅱ.4.3	情報セキュリティポリシーの遵守、点検及び監査	Ⅱ.4.3.1【基本】レビュー：各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるように、定期的に及び脅威の変化や設定・構成変更等の状況変化に応じてレビュー及び見直しを行うこと。また、組織の情報セキュ	テンセントクラウドセキュリティチームは、情報セキュリティマネジメントシステムの有効性と信頼性を保証するため、内部セキュリティリスクの継続的な監視と評価を実施しています。テンセントクラウドセキュリティチームは年１回以上の内部セキュリティ監査を実施し、クラウドプラットフォームと内部システムの状況を継続的に監視し、良好なセキュリティ態勢を維

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		リティのための方針群及び標準に関し、システムや提供するクラウドサービスが、定めに従って技術的に遵守されていることをレビューすること。 Ⅱ.4.3.2【基本】点検・監査：クラウドサービスの提供に用いるシステムが、情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に検証・監査すること。システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、 慎重に計画し、実施すること。	持し、関連法令法規及びセキュリティ管理基準の規定と要件に適合することを確保しています。さらに、テンセントクラウドは年次で独立第三者の専門監査を受け、保証業務報告書（システムと組織の管理報告書：SOC 報告書）を提供することにより、クラウドユーザー機関、独立監査人、監督機関、会社株主及びその他関連利害関係者に対し、テンセントクラウドの最新のサービス組織内部統制状況を公開しています。 特に日本地域に関して、テンセントクラウドは『金融機関等コンピュータシステムの安全対策基準・解説書』に基づき統制状況を評価し、これを踏まえて対応するシステムと組織の管理（SOC）報告書を作成しています。当該報告書は、テンセントクラウドプラットフォームの安全性、可用性、機密性に関連する統制ポイントを網羅し、テンセントクラウドの関連措置が要件を満たしていることを証明するものです。
Ⅱ.4.4	アクセス管理	Ⅱ.4.4.1【基本】アクセス制御方針：アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューすること。また、情報及びシステム機能へのアクセスは、アクセス制御方針に従って、制限すること。 Ⅱ.4.4.2【基本】アクセス制御：事業者は、クラウドサービスへのアクセス、クラウドサービス機能へのアクセス及び利用者データへのアクセスを、利用者が制限できるようにアクセス制御を提供すること。 Ⅱ.4.4.3【基本】ユーティリティプログラムの使用：システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラム(データベースの中身を強制的に書き換えることが出来る機能や一時的にポートを開放す	テンセントクラウドはアクセス制御管理関連基準を策定し、クラウドプラットフォーム製品、エンドポイントシステム、ホスト OS、アプリケーションシステム、ネットワーク機器に対するアクセス制御活動を規範化しています。テンセントクラウドはユーザーアカウントに一意の識別子の使用を求め、セキュリティベースラインに基づき従業員アカウントのパスワードポリシーを設定します。テンセントクラウドはゼロトラストセキュリティ管理システムを通じて従業員の入退場認証を実施し、ユーザーが内部リソースにアクセスするには二段階認証の完了が必要です。Tencent Cloud では、アクセス制御に関する権限付与ポリシーと権限分離マトリックスメカニズムを内部で制定しており、最小権限の原則に従い、職務責任に基づいて必要な操作権限を割り当て、権限に有効期限を設定することで、権限の詳細な管理制御を実現しています。テンセントクラウドは職務役割に対応する人員の身元情報と

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		る機能等)の使用は、制限し、厳しく管理すること。また、事業者は、クラウドサービス内で利用される全てのユーティリティプログラムのための要求事項を特定すること。 Ⅱ.4.4.4【基本】プログラムソースコードへのアクセス：プログラムソースコードへのアクセスは、制限すること。 Ⅱ.4.4.5【基本】アクセス制御となりすまし対策：利用者及びシステム管理者等のアクセスを管理するために、適切な認証方法、特定の場所や装置からの接続を認証する方法等によって、アクセス制御となりすまし対策を行うこと。また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法とパスワードの有効期限を規定に含めること。	各業務システムの権限レベルの記録を維持し、定期的な内部権限審査を実施することで、権限の不正利用・誤用を防止します。 テンセントクラウドの生産環境にはジャンプサーバーを全面導入し、ジャンプサーバーを通じてテンセントクラウドバックエンドシステムコンポーネントの管理者アカウント権限を集中管理しています。内部運用要員がジャンプサーバーにアクセスするには承認が必要で、特定のテンセントクラウド内部運用要員のみがアクセス可能であり、ログインには二段階認証が必須です。運用操作記録はログプラットフォームに集中保存され、テンセントクラウド内部監査チームが定期的にログを審査します。 顧客のアクセス管理を支援するため、Cloud Access Management (CAM)サービスを提供しています。ユーザーのルートアカウントはデフォルトで配下リソースへの完全アクセス権限を有し、サブユーザーを作成してサブユーザーに ID、認証情報、権限を付与できます。ユーザーはアクセス管理コンソールを通じてサブユーザーのパスワードルール、単一ログインセッションの有効期限を変更可能です。パスワード漏えい防止のため、テンセントクラウドは顧客パスワードに対し SHA256 ハッシュ暗号化とソルト処理を施し、平文での保管を回避します。CAM は多様な二段階認証機能もサポートし、CloudAudit を通じてテンセントクラウドアカウント活動の監視、コンプライアンスチェック、操作審査、リスク審査を実施可能です。Bastion Host (BH) を提供し、ユーザー、資産、アカウント、操作権限などの次元に基づくきめ細かな権限付与をサポートし、ユーザ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ーに付与される権限が資産アクセスと業務遂行に必要な最小限であることを確保します。ジャンプサーバーも操作監査機能をサポートし、ユーザーの操作ログを記録・分析してセキュリティインシデントの効果的な追跡を可能にします。 **ソースコードアクセス制御に関して、**テンセントクラウドはプログラムソースコードをコードリポジトリに保存し、関連開発チームが権限制御を設定し、権限の定期見直しと整理を実施します。コードリポジトリへのアクセスは内部オフィスネットワークからのみ許可されます。テンセントクラウドはコードリポジトリの操作ログを維持し、定期的なログ監査を実施しています。
Ⅱ.4.5	構成管理	Ⅱ.4.5.1【基本】構成管理のポリシーと手順：目的・適用範囲・役割・責任・経営コミットメント・組織間の調整・コンプライアンスを取り扱う構成管理ポリシー及び「構成管理」対応策の実施を容易にするための手順を策定し文書化すること。 Ⅱ.4.5.2【推奨】 ベースライン構成：システムの最新のベースライン構成を把握・文書化すること。ベースライン構成には、システムコンポーネント（PC、サーバ、ネットワークコンポーネント、インストールされているソフトウェアパッケージ・OS 等の現在のバージョンとパッチ情報、設定項目等)、ネットワークの接続形態及びシステム構成内のそれらのコンポーネントの論理的な配置に関する情報を含む。 Ⅱ.4.5.3【推奨】 構成変更管理：構成管理の対象となるシステムに対する変更について定めるととも	テンセントクラウドは構成管理制度を確立し、構成管理データベースを通じて各 IT サービスコンポーネントと構成項目を一元的に管理し、構成項目（CI）及びその間の関係の管理を規範化しています。変更プロセスにおいて構成更新が含まれる場合、運用要員は変更完了後、変更案に基づき構成項目のバージョン及び関連情報を構成管理データベースに更新します。テンセントクラウドは資産の定期棚卸を実施し、構成管理データベースの監査を行い、各構成項目情報の有効性、正確性、完全性を確保しています。 **セキュリティ構成チェックに関して**、テンセントクラウド内部ではネットワークセキュリティ構成基準とセキュリティベースライン基準を整備し、スキャンツールを使用して OS、データベース管理システム、ネットワーク機器、仮想イメージの構成をスキャンし、ベースラインファイルで定義された標準構成からの逸脱を継続的に検出・修正しています。テンセントクラウドはさらにエンドポイント検知対応（EDR）ツールを導入し、全ネットワークサーバー

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		に、変更内容をレビューし、セキュリティへの影響を考慮した上で変更を許可すること。また、変更に関する関連の活動を監査し、レビューすること。 II.4.5.4【推奨】変更に対するアクセス制限：システムに対する変更に関して、物理的 / 論理的なアクセス制限を定義・文書化・承認のうえ実施すること。 II.4.5.5【推奨】 設定項目: 運用上の要求事項に適合し、最も制限された運用を実現するためのセキュリティ設定に関するチェックリストを使用して、システムに導入されている製品の設定項目を把握し文書化すること。設定項目とは、システムのハードウェアコンポーネント、ソフトウェアコンポーネント又はファームウェアコンポーネントの値を変更できるパラメータのこと。 II.4.5.6.【推奨】 ソフトウェアの使用制限：契約上の取り決めと著作権法に従ってソフトウェアと関連ドキュメントを使用するとともに、ライセンスの数によって保護されるソフトウェアと関連ドキュメントの使用をモニタリングし、それらが複製されないようにすること。 II.4.5.7【推奨】クラウドサービス利用者によるソフトウェアのインストール：利用者によるソフトウェアのインストールを管理するためのポリシーを確立するとともにポリシーが遵守されていることをモニタリングすること。 II.4.5.8【推奨】 情報の場所: 情報の場所と、情報が処理及び保存されるシステムコンポーネントを特	エンドポイント資産の包括的な監視と管理を実施しています。テンセントクラウドが採用する EDR ツールは、アンチウイルスと侵入検知、セキュリティベースラインと脆弱性スキャン、並びにコマンド操作、ログイン行動に対するセキュリティコンプライアンス監査などの機能をサポートし、マルウェアや異常行動を検知した際にアラートを発報します。 **構成変更管理に関して、**テンセントクラウドは製品及び構成変更に関する管理基準を確立し、変更プロセスの各ステップ及び関連責任者を明確化しています。テンセントクラウドは内部運用管理メカニズムを通じて変更活動を厳格に管理し、変更が生産環境投入前に適切な承認とテストを経ていることを確保し、内部運用要員によるシステムパラメータへの不正変更を制限します。顧客に影響を及ぼす可能性のある運用変更操作については、テンセントクラウドは公式サイト、サイト内メッセージなどのチャネルを通じて関連顧客に速やかに変更通知を発行します。 **ソフトウェアの使用管理に関して**、テンセントクラウド従業員は承認・審査・テストを経たソフトウェアのみのインストール、実行、更新を許可されます。調達したソフトウェアについては、テンセントクラウドは契約・合意書などにより、当該ソフトウェアの知的財産権帰属、承認使用方式、承認使用期間などを明確化し、購入したソフトウェアライセンス数に応じてソフトウェアを配布・インストールします。関連部門は承認インストールソフトウェアリストを維持し、全てのインストール済みソフトウェアが記録されていることを保証します。さらに、テンセントクラウドは顧客に対 Cloud Workload Protection

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		定して文書化すること。また、個人を特定できる情報がどのように処理されているかについて文書化すること。	Platform (CWPP)を提供し、機械学習を活用して顧客の資産管理、トロイの木馬ファイルと不審なソフトウェアの駆除などのセキュリティ保護を支援し、サーバーが直面する主要なセキュリティリスクに対応します。 **情報資産の管理に関して、**テンセントクラウドは情報資産管理規範と全ライフサイクル管理プロセスを策定し、電子データなどの資産を分類・階層化して管理・保護しています。テンセントクラウドは資産台帳システムやリストなどを通じて資産関連情報を記録し、資産保存場所（電子データが保存される物理媒体 / ストレージデータベース、ハードウェアの物理的設置場所など）を含みます。さらに、個人情報の収集と処理に関して、テンセントクラウドは事業運営を行う司法管轄区域のユーザープライバシー及びデータセキュリティに関する法令法規を厳格に遵守し、利用する個人情報及びその利用方法とプロセスを記録します。

5.1.5 従業員に係る情報セキュリティ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
Ⅱ.5.1	雇用前	Ⅱ.5.1.1【基本】雇用契約：雇用予定の従業員(就業形態に関わらず)に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。	テンセントクラウド従業員は雇用時に任用契約及び機密保持契約への署名が義務付けられています。任用契約にはテンセントクラウドの既存のセキュリティポリシー、従業員又は第三者が履行すべき情報セキュリティ及び個人情報保護の責任が明確化され、機密保持契約には署名者の機密保持義務と責任、並びに機密条項違反後の処罰の可能性が含まれます。外部委託従業員は、テンセントクラウドと外部委託先が締結した契約に定める任用及び機密保持要件の対象となります。テンセントクラウドと従業員及び第三者間の機密保持要件は、必要に応じて法務部門による審査と更

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			新が行われます。
Ⅱ.5.2	雇用期間中	Ⅱ.5.2.1【基本】教育・訓練：全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。 Ⅱ.5.2.2【推奨】教育のフィードバック：組織のトレーニング結果を情報セキュリティ責任者にフィードバックすること。 Ⅱ.5.2.3【基本】契約違反：従業員が、情報セキュリティポリシー又はクラウドサービス提供上の契約に違反した場合の対応手続を備えること。	**教育と研修に関して、**テンセントクラウドは情報セキュリティ研修メカニズムを確立し、正社員、顧問、インターン、外部委託従業員などに対し情報セキュリティ研修コースの受講を義務付けています。テンセントクラウドは多様な研修コースを提供し、全員必修研修、重点職種向け特別研修、選択専門科目研修などを含み、内容は基礎セキュリティ意識、オフィスセキュリティ、脆弱性識別と防御、プライバシー保護、緊急時対応、開発セキュリティ規範、データセキュリティ要件などを網羅しています。 Tencent Cloud は、社内規定に違反し、いかなる手段による無断開示を行った従業員に対し、懲戒処分手続きに基づき対応する、厳格な規律処分メカニズムを確立しています。違反行為の内容に応じて、労働契約解除、法的措置の提起、刑事責任の追及を含む適切な処分措置を講じます。
Ⅱ.5.3	雇用の終了又は変更	Ⅱ.5.3.1【基本要求】アクセス権・資産の取扱い：従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続、確認項目等を明確にすること。	テンセントクラウドの退職手続きには、ユーザーアカウントと権限の速やかな無効化、及び会社資産の回収などのプロセスが含まれます。テンセントクラウドの物理的資産は全て指定責任者に割り当てられ、テンセントクラウド内部専用の資産追跡システムを通じて登録されます。Tencent Cloud は定期的に資産棚卸しを実施し、資産の実在状況を確認するとともに、棚卸し結果を記録します。

5.1.6 情報セキュリティインシデントの管理

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
Ⅱ.6.1	情報セキュリティ	Ⅱ.6.1.1【基本】組織内報告：全ての従業員に対し、業務において発	**インシデント対応と管理に関して、**テンセ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
	インシデント及びぜい弱性の報告	見したあるいは疑いをもったシステムのぜい弱性や情報セキュリティインシデント (サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等) について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続を定め、実施を要求すること。報告を受けた後に、迅速に効果的な対応ができるよう、責任体制及び手順を確立すること。 II.6.1.2.【基本】クラウドサービス事業者とクラウドサービス利用者間の報告: 事業者は、利用者が情報セキュリティ事象を事業者に報告する仕組み、事業者が情報セキュリティ事象を利用者に報告する仕組み及び利用者が報告を受けた情報セキュリティ事象の状況を追跡する仕組みを提供すること。 II.6.1.3【基本】インシデントの評価と分類: 情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定すること。 II.6.1.4【基本】フィードバック: 情報セキュリティインシデントの分析及び解決から得られた知識は、情報セキュリティインシデントが将来起こる可能性又はその影響を低減するために用いること。 II.6.1.5【基本】証拠の収集・取得: 証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用すること。	ントクラウドは情報セキュリティインシデント管理規範を策定し、情報セキュリティ報告、対応、処理メカニズム及び関連プロセスを確立しています。テンセントクラウドは内部セキュリティ運用システムを使用してセキュリティインシデントを記録します。検出・識別されたセキュリティインシデントに対して、テンセントクラウドはインシデントの性質、データの機微性、影響範囲などの要素を考慮して分析・レベル分けを行い、速やかに該当責任者に通知してインシデントのフォローアップ処理を依頼します。情報セキュリティインシデントの受付、調査評価、処理、追跡のプロセスにおいて、関連責任部門は受付けた情報セキュリティインシデントの関連記録を維持し、記録の完全性と機密性を確保します。重大なセキュリティインシデントについては、テンセントクラウドは専任チームを設置し、特別分析報告書を作成して経営層に報告します。 テンセントクラウドはさらに定期的なインシデント分析メカニズムを構築し、インシデントを多角的に分析 (インシデントタイプ、発生頻度、影響範囲及び深刻度) し、インシデントの振り返りと根本原因分析に基づいて予防措置を講じ、同様のインシデントの再発を防止します。 **インシデントのコミュニケーションと通知に関して、**テンセントクラウドは情報セキュリティインシデント対応、エスカレーション、通知などの関連手順を確立し、事故の影響を受ける可能性がある、又は既に影響を受けている会社内部関係者、顧客などの関連者に対し速やかに注意喚起又は通知を行い、各関係者が秩序立てて、迅速かつ効率的にコミュニケーションと調整を行えるようにしています。顧客に影響を及ぼす可能性のあるセキュリティインシデントについては、テンセントクラウドは情報セキュリティインシデントの影響範

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			囲と程度に基づき、内部審査を経た後、情報セキュリティインシデントの処理と分析結果を適切な方法で顧客に通知し、対応する技術支援を提供して、顧客が損失を最小限に抑えるための救済措置を講じることを支援します。 **顧客がテンセントクラウドに問題を報告又は自主的に連絡することを支援するため**、テンセントクラウドはテンセントクラウドコンソールを通じてチケットサービスを提供し、顧客がセキュリティ、可用性、機密性に関連する障害、インシデント、問題、苦情を報告することをサポートしています。さらに、テンセントクラウドはクラウドコンソールと公式サイト上でオンラインカスタマーサービス及び電話窓口を提供し、顧客がテンセントクラウドサービス利用時に直面した問題をフィードバックすることを支援します。テンセントクラウドは複数地域に相互バックアップ可能なカスタマーサービスセンターを有し、7*24 時間体制で顧客のリクエストを処理し、クラウド製品の 24 時間 365 日の技術支援、及び迅速かつ高品質なサービス対応と処理を提供します。顧客はさらに適用可能なサービスプランを選択し、専任サポートグループ、専任技術サービスマネージャー、付加価値サービスなどで構成される専用サポートを取得することもできます。

5.1.7 コンプライアンス

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
Ⅱ.7.1	法令と規則の遵守	Ⅱ.7.1.1【基本】関連法規と記録: 個人情報(特に要配慮個人情報を含む)、プライバシー情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。また、クラウドサービ	**コンプライアンスに関して、**テンセントクラウドは事業運営を行う司法管轄区域の法令法規を厳格に遵守し、セキュリティコンプライアンス関連手順を確立して、情報セキュリティ運用が関連法令、法規、基準、手順の要件に適合することを確保しています。テンセントクラウド法務チームはテンセントクラウド事業に関連するコンプ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		スの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）について、法令、契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理するとともに、利用者から求められたときには提供すること。 II.7.1.2【基本】利用可否：利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のためにシステム及び情報処理施設を利用させないこと。 II.7.1.3【基本】ソフトウェア製品：知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施すること。 II.7.1.4【基本】不正アクセス・流出からの保護：記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護すること。また、事業者は、利用者によるクラウドサービスの利用に関連して、事業者が収集し、保存する記録の保護に関する情報を、利用者に提供すること。 II.7.1.5【基本】暗号化：暗号化機能は、関連する全ての協定、法令及び規制を順守して用いるとともに、利用者が法令及び規制の順守をレビューできるように、事業者は実施している暗号による対応策を記載すること。	ライアンス要件を継続的に識別・収集し、対応する法令法規リストを作成し、定期的な維持と更新を実施しています。さらに、テンセントクラウドは年次で専門独立第三者のセキュリティ監査を受け、保証業務報告書（システムと組織の管理報告書）を提供することにより、クラウドユーザー機関、独立監査人、監督機関、会社株主及びその他関連利害関係者に対し、テンセントクラウドの最新のサービス組織内部統制状況を公開しています。 **記録管理に関して、**法令法規又は契約条項の要件を満たすため、テンセントクラウド関連部門はログなどの記録を適切に管理・保護し、記録の紛失、破損、偽造、不正アクセス又は不正削除を防止し、当該記録の保存期間を明確に定義・識別します。顧客から要請があった場合、テンセントクラウドは合理性と実現可能性を評価した上で、顧客のデジタルフォレンジック又は事後セキュリティインシデント調査などに有効な支援を提供します。 **ソフトウェア使用と著作権保護に関して、**テンセントクラウド関連部門は承認インストールソフトウェアリストを維持し、購入したソフトウェアライセンス数に応じてソフトウェアを配布・インストールし、従業員による著作権保護対象のソフトウェア、データ、コード、文書、画像などの無断複製又は使用を厳禁します。 テンセントクラウドは受容可能使用ポリシーを策定し、従業員及び第三者がテンセントクラウド会社リソース（IT システム、ネットワーク、デバイス、データなどを含むがこれらに限らない）を使用する際の責任と義務を明確化し、適切な使用行動を規範化して潜在リスクを防止します。 **暗号化統制措置に関して、**テンセントクラウド内部では鍵管理メカニズムを構築し、

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			鍵の全ライフサイクル管理を実施して、鍵の機密性、完全性、可用性を確保しています。テンセントクラウドは国際的に認められた暗号化アルゴリズムと暗号化製品を選定し、データと鍵の暗号化を実施します。

5.1.8 ユーザサポートの責任

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
Ⅱ.8.1	利用者への責任	Ⅱ.8.1.1【基本】責任：クラウドサービスの提供に支障が生じた場合には、その原因がサプライチェーンの事業者に起因するものであったとしても、利用者と直接契約を結ぶ事業者が、その責任において一元的にユーザサポートを実施すること。 Ⅱ.8.1.2【基本】SLA：事業者自身の責任範囲を SLA 等により文書化し、利用者に明確に示すこと。 Ⅱ.8.1.3【基本】情報提供：クラウドサービスの新規利用/変更を計画している利用者への情報提供にあたっては、組織のガバナンス規定を順守した上で、利用者が、必要な統制機能及び能力を有しているクラウドサービス及びこれを提供する事業者を選定できるようにすること。 Ⅱ.8.1.4【基本】クラウドサービス利用者からの苦情対応：提供しているクラウドサービスに対し、利用者からの苦情、懸念又は質問を受け取り、対応するためのプロセスを構築すること。	テンセントクラウドは国際版公式サイト上でオンラインの Terms of Service、Service Level Agreement (SLA)、データプライバシーとセキュリティ契約などの法的文書を提供し、テンセントクラウドが提供するサービスの内容とサービスレベル、ユーザーデータと知的財産権の保護、顧客とテンセントクラウド双方のセキュリティ責任と義務などを明確にしています。顧客はさらにテンセントクラウドとオフライン契約を締結し、契約中の条項と細則を協議することもできます。 テンセントクラウドが顧客に提供するクラウドサービスは、各サービスごとに合意されたサービスレベル契約（SLA）に基づいて提供されます。各サービスの性能指標、測定基準及び報告要件は、各製品のサービスレベル契約において明確化され、テンセントクラウド公式サイトに公開されています。 さらに、顧客から要請があった場合、テンセントクラウドは顧客の情報提供要請に積極的に協力します。 **クラウドユーザー苦情対応に関して、**テンセントクラウドコンソールはチケットサービスを提供し、顧客がセキュリティ、可用性、機密性に関連する障害、インシデント、問題、苦情を報告することをサポートしています。テンセントクラウドのチケッ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			トシステムは、優先度に応じた対応メカニズムを通じて顧客チケットに優先順位を割り当て、エスカレーション手順を策定してテンセントクラウドスタッフのインシデント解決と影響を受ける顧客への通知を支援します。顧客はさらに適用可能なサービスプランを選択し、専任サポートグループ、専任技術サービスマネージャー、付加価値サービスなどで構成される専用サポートを取得することもできます。
Ⅱ.8.2	保守	Ⅱ.8.2.1【基本】システム保守ポリシーと手順: システム保守の目的、適用範囲、役割、責任、経営コミットメント、組織間の調整及びコンプライアンスを取り扱う保守ポリシーを策定、文書化し、関係する組織に配布すること。 Ⅱ.8.2.2【基本】保守管理: 保守契約、保守仕様書及び要求事項に従って、保守・修理を計画、実施、文書化し、記録すること。 Ⅱ.8.2.3【基本】保守ツール: システムの保守ツールを承認・管理し、モニタリングするとともに、以前の保守ツール使用状況レビューすること。 Ⅱ.8.2.4【基本】リモート保守: リモート保守及び診断を承認のうえモニタリングする。リモート保守及び診断用ツールは、組織のポリシーに沿い、かつシステムのセキュリティ計画に記載されている通りである場合のみ、使用を許可すること。また、リモート保守及び診断のためのセッションを確立する際には、厳格な認証機能を使用するのに加え、リモート保守及び診断の記録を保管すること。リモート保守が完了したら、セッションとネットワーク接続を終了すること。	**運用管理に関して、**テンセントクラウドは運用管理規範を策定し、運用要員の日常的な運用行動に対する操作指針と要件を提供しています。テンセントクラウドは成熟したツール化・自動化された運用管理プラットフォームを採用して運用操作を管理し、内部運用管理メカニズムを通じて変更時間枠を厳格に管理し、運用リクエストが全て指定された時間内に完了することを確保しています。 **運用要員の権限管理に関して、**テンセントクラウド内部では承認戦略と権限分離マトリクスメカニズムを策定し、職務役割に対応する人員の身元情報と各業務システムの権限レベルの記録を維持しています。テンセントクラウドは定期的な内部権限審査を実施し、権限の不正利用・誤用を防止します。不要となったアクセス権限については、適切なフォローアップ行動を講じ、不要なアクセス権限を速やかに無効化します。 テンセントクラウドの生産環境にはジャンプサーバーを全面導入し、ジャンプサーバーを通じてテンセントクラウドバックエンドシステムコンポーネントの管理者アカウント権限を集中管理しています。内部運用要員がジャンプサーバーにアクセスするには承認が必要で、特定のテンセントクラウド内部運用要員のみがアクセス可能であり、ログインには二段階認証が必

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		Ⅱ.8.2.5【基本】保守要員：保守要員の認可手順を確立し、認可された保守組織又は要員の一覧を維持すること。 Ⅱ.8.2.6【基本】保守要員による保守：保守要員が付添いなしで保守を行う場合、その要員が必要なアクセス権限を有することを確認すること。また、必要なアクセス権限を持たない要員による保守活動を監督するために、必要なアクセス権限と技術的能力を有する職員を指定すること。 Ⅱ.8.2.7【基本】タイムリーな保守：システムコンポーネントに障害が発生した場合、保守サポート契約に基づき、保守サポートを行うこと。	須です。 生産環境内の操作を管理・追跡可能とするため、バックエンド運用操作記録は全て詳細に記録され、ログプラットフォームに集中保存されます。テンセントクラウド内部監査チームは定期的に運用プロセス中の不審な操作に対して問題調査と追跡を実施します。 **リモートアクセス管理に関して、**テンセントクラウド内部では従業員向けリモートアクセス管理関連手順を確立し、従業員はテンセントクラウドに登録済みの信頼できるデバイスのみを使用し、暗号化通信チャネルを通じてテンセントクラウドのオフィスネットワーク及び日常業務システムにリモートアクセスできます。テンセントクラウドはリモートアクセスログを維持し、ユーザー操作行動を記録します。

5.1.9 事業継続マネジメントにおける情報セキュリティ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
Ⅱ.9.1	情報セキュリティの継続	Ⅱ.9.1.1【基本】情報セキュリティ継続計画の策定と実施：組織は、大規模災害等における情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定するとともに、プロセス・手順・対策を確立、文書化し、実施、維持すること。 Ⅱ.9.1.2【基本】情報セキュリティ継続の検証、レビュー及び評価：情報セキュリティ継続のための対策が、大規模災害等の下で妥当かつ有効であることを確認するために、組織は、定められた間隔でこれらの対策を検証すること。	事業継続性管理に関して、テンセントクラウドは自社のクラウドコンピューティング環境に適用可能な事業継続性管理フレームワークを設計・実施し、包括的な事業継続性管理体系を構築、事業継続性管理規定を策定して、事業継続性管理関連プロセスを規範化しています。これにより、事業影響度分析、事業継続性計画、緊急時対応と災害復旧、緊急時訓練とテスト、危機管理などを網羅し、ISO/IEC 22301 事業継続性マネジメントシステムの国際標準認証を取得済みです。 テンセントクラウドは年次で事業継続性管理体系の見直しと更新を実施し、事業影響度分析の結果に基づき関連製品とサービスの事業継続性計画と災害復旧計画を審査し、必要に応じて更新します。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
Ⅱ.9.2	緊急時対応計画	Ⅱ.9.2.1【基本】緊急時対応計画の策定と手順：目的・適用範囲・役割・責任・経営コミットメント、組織間の調整及びコンプライアンスを取り扱う緊急時対応計画を策定するとともに、「緊急時対応計画」の実施手順を策定・文書化し、担当組織・要員に配布すること。 緊急時対応計画には、下記項目を盛り込むこと。 極めて重要なミッション / 業務機能と、関連する緊急時対応要件; 復旧目標 復旧の優先順位及びメトリクス；緊急時対応における役割 責任 割り当てられた個人と連絡先情報；システムの途絶又は侵害若しくは不具合が発生しても、極めて重要なミッション / 業務機能を維持できるようにすること。 Ⅱ.9.2.2【推奨】緊急時対応トレーニング：システムの利用者に対して、役割と責任に応じた緊急時対応トレーニングを実施すること。 Ⅱ.9.2.3【推奨】緊急時対応計画のテスト：緊急時対応計画の有効性を判断して計画の欠陥を特定するために、緊急時対応計画のテストを実施すること。 Ⅱ.9.2.4【推奨】 代替処理サイト: 利用者とシステムバックアップ情報の保存と取得を許可するための契約を締結するとともに、代替処理サイトを確立すること。また、代替処理サイトが一次処理サイトと同等の管理機能を提供することを確認すること。 Ⅱ.9.2.5【推奨】代替処理サイトで再開: 代替処理サイトを定め、利用者と合意した目標復旧時間内に、システムオペレーションを移転再開して、極めて重要なミッション	テンセントクラウドは内部の事業継続性管理関連規定に基づき、関連クラウド製品とサービスに対して事業影響度分析を実施します。これには、重要業務プロセスの識別、テンセントクラウド事業中断の潜在的脅威の分析、復旧時間目標（RTO）と最低サービスレベルの決定、並びに事業影響度分析結果に基づく事業継続性計画と災害復旧計画の策定が含まれます。関連計画及び計画は、場所、人員、設備、システム、情報 / データ、業務優先順位などのあらゆる側面を網羅しています。 テンセントクラウドは定期的に事業継続性計画に基づきクラウド製品の事業継続性訓練と研修を実施し、計画や計画などの実現可能性を確保します。テンセントクラウドは事業継続性計画を基に訓練計画を策定し、訓練リスク評価を実施して対応する保障措置を講じ、訓練によるサービスへの悪影響を回避します。テンセントクラウドの災害復旧訓練は、実際の典型的な災害復旧シナリオを模擬して実施され、攻防対抗や大規模障害などを含み、システムの災害復旧能力、応答速度、復旧能力を包括的に検査します。 テンセントクラウドのデータセンターは中国本土、アジア太平洋地域、北米地域、欧州地域をカバーし、リージョン (region) とアベイラビリティーゾーン (zone) で構成されています。テンセントクラウドの異なるリージョン間は完全に分離され、異なるリージョン間の最大限の安定性とフォールトトレランスを保証します。データの高可用性を確保するため、テンセントクラウドは各リージョンを複数の相互分離されたアベイラビリティーゾーンに分割します。テンセントクラウドはクラウド製品が単一リージョン内で複数のデータセンターによる冗長性メカニズムを採用することを求め、クラウドサービスの事業継続性を確保します。顧客はさらに事業発展ニーズとデータセキュリティ要件に基づき、

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		/ 業務機能を遂行できるようにすること。 II.9.2.6【推奨】 通信サービス: 一次処理サイトや代替処理サイトのいずれかにおいて一次通信サービスが利用できない場合に、極めて重要なミッションや業務機能を支援する代替通信サービスを確立すること。 II.9.2.7【推奨】 システムの復旧と再構成: システムの途絶、侵害、又は不具合が発生した場合に、システムを従前の状態に復旧し、再構成できるようにすること。 II.9.2.8【推奨】 代替通信プロトコル: 利用者が、業務の継続性を維持するために組織が定めた代替通信プロトコルを使用できるようにすること。 II.9.2.9【推奨】 代替の情報セキュリティ対策: 組織が定めた情報セキュリティ機能を実施するための主な手段が利用できない場合又は侵害された場合に、それらの情報セキュリティ機能を満たすための代替の又は補足的な情報セキュリティ対策を実装すること。	データとシステムを異なるリージョン又は異なるアベイラビリティーゾーンに柔軟に配備し、事業の災害復旧要件を満たすことができます。さらに、テンセントクラウドが提供する複数のストレージサービス及びデータベースサービスはバックアップ機能を備え、多重冗長バックアップ、遠隔地災害復旧などのニーズをサポートします。 **ネットワークレジリエンスに関して**、テンセントクラウドの各アベイラビリティーゾーンはネットワーク出口で複数の通信事業者と接続されており、通信事業者の公衆ネットワーク障害に伴う継続的な影響を効果的に低減できます。テンセントクラウドの基盤ネットワークは の冗長構築方式を採用し、ルーティング階層における経路優先度と経路到達可能性のトラフィックエンジニアリングスケジューリングと連携することで、単一デバイス障害によるネットワークサービスの中断を防止します。テンセントクラウドの計算ノードもの冗長構築方式を採用し、単一計算ノードで障害が発生した場合、スケジューラによるリアルタイム自動除外により、顧客事業の可用性を効果的に保証します。 **予備セキュリティ措置に関して**、テンセントクラウドはネットワーク多層防御体系を構築しています。テンセントクラウドは高可用性のネットワークセキュリティアーキテクチャを導入し、ファイアウォール、侵入検知 / 防御システム（IDS/IPS）、DDoS 対策、ネットワーク論理分離、Web アプリケーションセキュリティなどの多重防御メカニズムを通じて、悪意のあるネットワークトラフィックを速やかに検出、フィルタリング、遮断し、テンセントクラウドのネットワークセキュリティを保護します。

5.1.10 その他

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
Ⅱ.10.1	暗号と認証	Ⅱ.10.1.1【基本】 方針: 情報を保護するための暗号利用に関する方針を、策定し、実施すること。 Ⅱ.10.1.2【基本】情報提供: 事業者は、利用者に、事業者が処理する情報を保護するために、暗号を利用する環境に関する情報を提供すること。また、事業者は、利用者自らの暗号による保護を適用することを支援するために、事業者が提供する能力についても利用者に情報を提供すること。 Ⅱ.10.1.3【基本】暗号鍵の作成と管理: 組織が定めた方針に従って、システム内で使用する暗号鍵を生成・配布・保管・アクセス・廃棄すること。	テンセントクラウドはセキュリティ管理関連手順を策定し、暗号化技術の使用と管理を規範化し、鍵の申請、生成、保存、使用、伝送、更新、破棄などのプロセスにおけるセキュリティ要件を明確化しています。鍵ライフサイクルに関わる各操作は、二重管理、厳格な引継ぎ、適切な保管、速やかな更新の基本要件に従って実施されます。鍵の使用過程においても、権限と責任の分離、厳格な承認、実名確認のうえでの操作などの要件を遵守する必要があり、業務鍵操作ログを保存し、定期的な操作監査を実施します。 **データ保存時の暗号化に関して**、テンセントクラウドの複数のストレージ及びデータベース製品はデータ暗号化機能をサポートし、安全で高強度の暗号化アルゴリズムを使用し Key Management Service (KMS)との連携により鍵の全ライフサイクル管理を実現し、データの機密性を確保します。 Key Management Service (KMS)は FIPS-140-2 認証のハードウェアセキュリティモジュール (HSM) を使用して鍵を生成・保護し、顧客の暗号化鍵の全ライフサイクル管理をサポートできます。鍵の解読又は不正利用リスクを低減するため、KMS は鍵ローテーションをサポートし、無効、廃棄、又は漏えいした鍵を安全確実な方法で削除します。削除後の鍵は復元不可であり、当該鍵で暗号化されたデータも復号不可となります。 **データ転送時の暗号化に関して**、顧客がテンセントクラウドコンソール上で行う通信は全て HTTPS セキュリティプロトコル

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			による暗号化保護を受けます。テンセントクラウド製品が提供するクラウド API インターフェースも HTTPS 暗号化、署名検証、状態監視などのセキュリティ機能を有し、顧客の業務にポートレベルの通信セキュリティ保証を提供します。 顧客がテンセントクラウドプラットフォーム上に自身のアプリケーションを構築する必要がある場合、テンセントクラウドはセキュアソケットレイヤー（SSL）証明書のワンストップサービスを提供し、証明書申請、管理及び配備機能を含み、トップクラスのデジタル証明書認証局 (CA) 及び代理店と連携して、顧客の Web サイト、モバイルアプリ向けに HTTPS ソリューションを提供します。
Ⅱ.10.2	開発プロセスにおけるセキュリティ	Ⅱ.10.2.1【基本】開発プロセスにおける情報セキュリティへの取組：プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組むこと。	腾讯云内部已建立一套信息系统安全开发标准，并着力将 ISO/IEC 20000 信息技术服务管理标准、ISO/IEC27001 信息安全管理体系和 ISO/IEC 9001 质量管理体系标准融入到产品安全开发生命周期全流程中，关注需求、设计、研发、测试、交付、运维等不同环节，在产品开发各个阶段中融入信息安全和隐私保护理念，确保云产品在其生命周期内均能获得足够的安全管控。

5.2 SaaS 編

5.2.1 運用における情報セキュリティ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
Ⅲ.1.1	運用管理	Ⅲ.1.1.1【基本】情報セキュリティ監視手順の策定：情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。また、クラウドサービスの提供に用いるアプリケーションの運用・管理に関する手順書を作成すること。 Ⅲ.1.1.2【基本】運用管理端末：運用管理端末に、許可されていない	**運用管理に関して、**テンセントクラウドは 運用管理規範を策定し、運用要員の日常的な運用行動に対する操作指針と要件を提供しています。テンセントクラウドは成熟したツール化・自動化された運用管理プラットフォームを採用して運用操作を管理し。 **セキュリティ監視に関して**、テンセントク

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		プログラム等のインストールを行わせないこと。従業員等が用いる運用管理端末の全ファイルのウイルスチェックを行うこと。 Ⅲ.1.1.3【基本】稼働・障害監視：クラウドサービスの稼働監視、障害監視、パフォーマンス監視及びセキュリティインシデント監視を行うこと。また、クラウドサービスを利用者に提供する時間帯を定め、この時間帯におけるクラウドサービスの稼働率を規定すること。稼働停止や異常を検知した場合は、利用者に速報すること。また、結果を評価・総括して、管理責任者に報告すること。 Ⅲ.1.1.4【基本】追加報告：クラウドサービスの提供に用いるアプリケーションに係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告を利用者に対して行うこと。 Ⅲ.1.1.5【基本】定期報告：クラウドサービスの提供に用いるアプリケーションの監視結果、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器監視結果（障害監視、死活監視、パフォーマンス監視）について、定期報告書を作成して利用者等に報告すること。 Ⅲ.1.1.9【基本】リソース監視：要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測すること。また、事業者は、資源不足による情報セキュリティインシデントの発生を防ぐため、資源全体の容量・能力を監視すること。 Ⅲ.1.1.11【基本】マルウェア対策：	ラウド内部ではログ収集と管理規範及び関連メカニズムを確立し、ログインログ、操作ログ、イベントログなどのログデータの記録、抽出、分析、監査などを管理し、システム活動の異常とリスクの検出と防止を図っています。テンセントクラウドが顧客に提供するクラウドサービスは、各サービスごとに合意されたサービスレベル契約（SLA）に基づいて提供されます。各サービスの性能指標、測定基準及び報告要件は、各製品のサービスレベル契約において明確化され、テンセントクラウド公式サイトに公開されています。各クラウドサービスの性能と可用性は継続的に追跡され、関連指標は管理コンソールを通じて顧客がリアルタイムで監視可能です。 **セキュリティインシデント又は異常状況の報告に関して、**テンセントクラウドは情報セキュリティインシデント対応、エスカレーション、通知などの関連手順を確立し、事故の影響を受ける可能性がある、又は既に影響を受けている会社内部関係者、顧客などの関連者に対し速やかに注意喚起又は通知を行い、各関係者が秩序立てて、迅速かつ効率的にコミュニケーションと調整を行えるようにしています。顧客に影響を及ぼす可能性のあるセキュリティインシデントについては、テンセントクラウドは情報セキュリティインシデントの影響範囲と程度に基づき、内部審査を経た後、情報セキュリティインシデントの処理と分析結果を適切な方法で顧客に通知し、対応する技術支援を提供して、顧客が損失を最小限に抑えるための救済措置を講じることを支援します。 **アンチウイルスとマルウェア対策に関して、**テンセントクラウドはエンドポイント検知対応（EDR）ツールを導入し、全ネットワークサーバーエンドポイント資産の包括的な監視と管理を実施しています。テ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		マルウェアから保護するために、検出、予防及び回復のための対策を実施すること。施。	ンセントクラウドが採用する EDR ツールは、アンチウイルスと侵入検知、セキュリティベースラインと脆弱性スキャン、並びにコマンド操作、ログイン行動に対するセキュリティコンプライアンス監査などの機能をサポートし、マルウェアや異常行動などを検知した際にアラートを発報します。テンセントクラウドはさらにゼロトラストセキュリティ管理システムを通じてオフィスエンドポイントの管理を実施し、ウイルス駆除、脆弱性修正、能動的防御などのセキュリティ機能により、ランサムウェア対策、フィッシング攻撃対策、内部横断移動対策などの包括的なセキュリティ保護を実現しています。 **容量管理に関して、**テンセントクラウドは 内部容量監視プラットフォームを使用して容量使用状況をリアルタイム監視し、容量使用のトレンドを識別します。業務部門は情報システムの事業継続性を保証しつつ、前期の容量監視で得られた容量使用トレンドを参考に新規業務とシステムのニーズを考慮して容量を予測し、年次容量管理計画を策定します。
		Ⅲ.1.1.6【基本】時刻同期：クラウドサービスの提供に用いるアプリケーションの時刻同期の方法を規定し、実施すること。	テンセントクラウドはネットワークタイムプロトコル（Network Time Protocol、NTP）を通じて正確な現在の世界協定時（UTC）を表示します。テンセントクラウドはテンセントクラウド上のインスタンス向けに社内ネットワーク NTP サーバーを提供し、テンセントクラウド以外のデバイスについては、顧客がテンセントクラウド提供の公衆ネットワーク NTP サーバーを利用できます。Tencent Cloud は、NTP サーバーの時刻同期状況を定期的に確認し、ネットワーク全体の時間の統一性、正確性、信頼性を確保します。
		Ⅲ.1.1.7【基本】パスワード管理：パスワード管理システムは、対話式とすること、また、良質なパスワードとすること。パスワードの文	テンセントクラウドはアクセス制御管理規範を策定し、セキュリティベースラインに基づき従業員アカウント及びクラウド顧客アカウントのパスワードポリシー（パ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		字数等については、情報資産の機密度合いやリスクの大きさを考慮して、具体的なルールについては、組織が自主的に定めること。	スワード長、複雑さ、ロック、リセットなど）を設定しています。パスワード漏えい防止のため、テンセントクラウドはパスワードに対し SHA256 ハッシュ暗号化とソルト処理を施し、平文での保管を回避します。 テンセントクラウド顧客がユーザーアカウントを登録する際、登録画面で自主的にパスワードを設定します。テンセントクラウドは登録画面で顧客に対しパスワードポリシーを提供し、パスワード長、複雑さなどの要件を含め、顧客がパスワード設定を完了することを支援し、パスワードと顧客が入力したメールアドレスが同一であることを禁止します。テンセントクラウドアカウント登録画面は、入力ミス防止のため、顧客が設定したパスワードの再入力確認を求めます。 テンセントクラウドはさらに顧客に対 Cloud Access Management (CAM)提供 し、顧客がテンセントクラウド製品とリソースへのアクセスを管理することを支援します。ユーザーのルートアカウントはサブユーザーを作成してサブユーザーに ID、認証情報、権限を付与できます。ユーザーはアクセス管理コンソールを通じてサブユーザーのパスワードルール（パスワードの複雑さ、長さ、有効期限など）を変更可能です。
		Ⅲ.1.1.8【基本】クラウドサービスの変更管理：情報セキュリティに影響を与える組織、業務プロセス及びシステムの変更を管理すること。また、事業者は、クラウドサービス利用者の情報セキュリティに影響を与える可能性のあるクラウドサービ スの変更について、利用者に情報を提供すること。	テンセントクラウドは製品及び構成変更に関する管理基準を確立し、変更プロセスの各ステップ及び関連責任者を明確化し、変更が実施前に適切な承認とテストを経ていることを確保しています。同時に、テンセントクラウドは緊急変更の管理プロセスを定義し、緊急変更は適切な承認を得た後に実施可能です。 各タイプのプログラム変更（アプリケーションと設定ファイル、OS 及びデータベース変更を含む）は、リリース前に事業影響

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			度分析を実施し、変更のロールバック計画を策定し、関連責任者の承認を得る必要があります。テンセントクラウドの変更リリースシステムは、変更操作が承認された要員のみによって実行されることを強制し、変更関連のログを保存して定期的な監査を実施します。変更リリース後、テンセントクラウドは生産環境において変更状況の検証、監視を実施し、結果を記録します。 顧客に影響を及ぼす可能性のある運用変更操作については、テンセントクラウドは公式サイト、サイト内メッセージなどのチャネルを通じて関連顧客に速やかに変更通知を発行します。
		Ⅲ.1.1.10【基本】環境分離: 開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために分離すること。	Tencent Cloud は業界のベストプラクティスを参考に、ネットワークセキュリティアーキテクチャを設計し、業務機能とセキュリティリスクに基づいてセキュリティドメインを分割しています。異なるセキュリティドメイン間には物理的または論理的な隔離を実施し、アクセス制御や境界防御などの措置を通じて、オフィスネットワークや本番ネットワークなどの安全性を確保しています。また、開発・テスト環境において非匿名化された本番環境データの使用を禁止しています。
		Ⅲ.1.1.12【基本】イベントログの取得: 利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューすること。また、事業者は、利用者に、ログ取得機能を提供すること。 Ⅲ.1.1.13【基本】ログの保護: ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護すること。 Ⅲ.1.1.14【基本】作業記録: システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護	テンセントクラウドはログ収集と管理規範及びメカニズムを確立し、ログインログ、操作ログ、システム通常ログ、システムセキュリティイベントログなどのログの記録、抽出、保存、保護、分析、監査などを管理し、システム活動の異常とリスクの検出と防止を図っています。ログはテンセントクラウドのログ管理プラットフォームに一元的に集約され管理され、関連ログ情報にはバックアップと厳格な保護措置が講じられ、不正な変更や削除から保護されます。バックアップログの保存期間は 1 年を超えます。テンセントクラウドは運用セキュリティ自動化監査ツールと内部監査チームを通じてログ監査を実施し、システム又は操作の異常を検出して操作リ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		し、定期的にレビューすること。	スクを防止します。 テンセントクラウドは顧客に対 Cloud Log Service (CLS)を提供しています。ワンストップのログサービスプラットフォームとして、CLS はログ収集、ログ保存からログ検索分析、リアルタイム消費、ログ配信までの多様なサービスを提供し、顧客の業務運営、セキュリティ監視、ログ監査、ログ分析などの課題解決を支援します。CLS は高可用性の分散型アーキテクチャ設計を採用し、ログデータに対し多重冗長バックアップ保存を実施して単一ノード障害時のデータ利用不可を防止し、サービスの高可用性を実現してログデータに安定した信頼性の高いサービス保証を提供します。Cloud Security Center (CSC)もクラウドセキュリティ製品のアラートデータ、クラウド資産構成変更データ、クラウド上のユーザー操作行動データ及び一部クラウド製品ログデータなどの各種クラウド上セキュリティ関連データの収集をサポートし、統一検索調査プラットフォームを提供して、顧客が包括的なクラウド上ログ監査と検索調査を実現することを支援します。さらに、Elasticsearch Service (ES)サービスは、クラウドサーバー、コンテナなどの他のクラウド製品のリアルタイムログ、又は業務の既存及び増分業務データをテンセントクラウド ES クラスターに集約・転送し、データの分散保存、問合せ分析を実施します。 操作ログの収集と保存に関して、顧客は CloudAudit を利用してテンセントクラウドアカウント活動の監視、コンプライアンスチェック、操作審査、リスク審査を実施できます。CloudAudit は 90 日以内のテン

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			セントクラウドコンソールとクラウド API 操作記録のオンライン閲覧をサポートし、アクセスキー、リージョン、エラーコード、イベント ID、イベント名、イベントソース、イベント時間、リクエスト ID、送信元 IP アドレス、ユーザー名を含みます。
		Ⅲ.1.1.15【基本】ソフトウェア導入：運用システムに関わるソフトウェアの導入を管理するための手順を実施すること。	テンセントクラウドは主に自社開発ソフトウェアを使用して生産システムの運用と管理を実施しています。同時に、テンセントクラウドはソフトウェアサプライチェーンセキュリティ管理要件を策定し、外部コンポーネント導入時のセキュリティ入場審査を明確化しています。テンセントクラウドは導入製品に対し継続的なセキュリティ運用とセキュリティチェックを実施し、セキュリティ問題を速やかに解決し、製品のセキュリティ運用状況評価を通じてセキュリティリスクを識別し、サプライヤーに改善を促し、当該サプライヤーとの今後の協力戦略を見直します。
		Ⅲ.1.1.16【基本】技術的ぜい弱性：利用中のシステムの技術的ぜい弱性に関する情報は、時機を失せずに入手すること。また、そ のようなぜい弱性に組織がさらされている状況を評価すること。さらに、それらと関連するリスクに対処するために、適切な手段をとること。また、事業者は、提供するクラウドサービスに影響し得る技術的ぜい弱性の管理に関する情報を利用者が利用できるようにすること。	テンセントクラウドは脅威と脆弱性管理手順を確立し、インフラストラクチャ、情報システムなどが直面する脅威と脆弱性を速やかに識別し、改善又は修正措置を講じることを確保しています。テンセントクラウドは定期的に脆弱性スキャンを実施し、スキャン結果を各関連責任部門に通知して関連リスクに対応し、脆弱性が顧客事業に与える影響度を評価します。関連チームによる内部審査を経た後、テンセントクラウドは脆弱性関連情報を公式サイト公告、サイト内メッセージなどの方法で顧客に速やかに通知し、通知内容には脆弱性の説明、影響範囲及び程度、テンセントクラウドが講じた統制措置、顧客向け修正提案及び具体的な操作指針を含みます（ただしこれらに限りません）。
Ⅲ.1.2	システム及び情報の完全性	Ⅲ.1.2.1【基本】原本性確保：電子データの原本性確保を行うこと。 Ⅲ.1.2.2【推奨】 メモリ保護：許可されていない不正なコード実行か	**顧客データの完全性を確保するため、**テンセントクラウドはサービスレベル契約においてデータ保存の持続性、すなわち契約期間中のデータ消失防止確率を明確に定

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		らシステムメモリを保護するために、セキュリティ対策を実施すること。 Ⅲ.1.2.3【基本】セキュリティ侵害の検知：システム又はシステムコンポーネントにデータ又は機能を埋め込み、データが盗み出されたり、不適切に変更、削除されたりしたかを検知すること。 Ⅲ.1.2.4【推奨】情報の更新：不要になった情報は削除するとともに削除したことを記録するログ情報等を残すこと。 Ⅲ.1.2.5【推奨】代替情報源：主要な情報源が破損しているか利用できない場合、システム又はシステムコンポーネントが重要な機能又はサービスを実行するための代替情報源を使用すること。 Ⅲ.1.2.6【推奨】情報の断片化：一度システムに侵入されると、失われた情報を回復する方法は、通常は存在しない。組織は、情報を異なる要素に分割し、それらの要素を複数のシステム又はシステムコンポーネントと場所に分散すること。	義しています。 テンセントクラウドはデータ保存時に多重レプリカ冗長保存と消去符号技術を採用し、完全性エラーを検出した際に直ちに必要な復旧措置を講じ、データのフォールトトレランス能力を向上させます。テンセントクラウドはデータアクセス権限に対し全アクセスノードにおける実名認証と管理を実施し、データ資産の完全性と業務サービスの信頼性を保証し、リアルタイム監視と遮断メカニズムを構築して、異常なデータアクセス行動の検出と阻止を実施します。同時に、テンセントクラウドは専門チームによる 7*24 時間の運用サービスを提供し、先進的なサーバー監視と診断技術を活用してサーバーの各種障害を自動検出し、即座に自動復旧プロセスを起動します。 テンセントクラウド API の各リクエストには、ユーザー身元の検証とリクエストの完全性保証のため、公開リクエストパラメータに署名情報を含める必要があります。 テンセントクラウドはさらにアドレス空間配置のランダム化 (ASLR) などの措置を採用し、システムメモリのセキュリティを保護します。 さらに、テンセントクラウドは顧客に対 Data Security Audit（DSA）サービスを 提供しています。DSA は人工知能（AI）ベースのデータベースセキュリティ監査システムであり、企業ネットワーク内のデータベースに対する各種セッション情報、アクセス操作、SQL 文の全量監査と保存をサポートし、複数のルールベースと脅威検知エンジンに基づき操作中の悪意のある行動を識別し、管理者に対し速やかに適切なセキュリティ保護措置を講じるよう通知します。 **データ削除に関して**、テンセントクラウド

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			は安全確実なデータ削除と消去メカニズムを提供し、データの削除又は消去に関するログを保存して、処理者（インターフェース、デバイスなど）、発生時間、データオブジェクト、及び消去方法を記録することを確保します。当該ログは少なくとも 6 か月間保存されます。 **データバックアップに関して、**テンセントクラウドはバックアップ管理手順を策定し、関連法令規範の要求に基づき、収集・処理した重要データのバックアップを実施しています。内部重要情報については、テンセントクラウドはデータレベルに基づき異なるデータのバックアップ戦略を策定し、定期的に復旧テストを実施します。クラウド上の顧客データについては、テンセントクラウドはクラウド製品またはサービスの機能に応じて、複数のストレージレプリカとバックアップサービスを顧客に提供し、製品サービスレベル契約に定める通り、提供するデータバックアップサービスに対して責任を負います。
Ⅲ.1.3	媒体の保管と廃棄	Ⅲ.1.3.1【基本】媒体保管：紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。 Ⅲ.1.3.2【基本】廃棄：機器及び媒体を正式な手順に基づいて廃棄すること。 Ⅲ.1.3.3【基本】輸送：情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護すること。	テンセントクラウドは媒体に保存される情報の機微性に応じて媒体を保管・処分し、媒体管理関連手順を確立して、媒体保管と媒体処分の具体的なプロセスと基準を明確化しています。媒体処分前には関連承認が必要であり、媒体の処分に関する記録を作成します。異なる媒体の材質、保存原理及び機微情報レベルに応じて、関連チームはデータの復元不可を確保し、かつセキュリティ規範に適合する対象的な処理方法を選択します。 物理媒体を使用して情報を転送する際、テンセントクラウドはチケット形式で媒体の出庫、輸送、入庫の全プロセスを追跡します。輸送過程において、テンセントクラウドは安全確実な輸送業者を選定し、情報レベルに応じて保護措置を実施し、物理媒体に保護包装を施して輸送中の物理的損

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			傷を回避します。

5.2.2 アプリケーション

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
Ⅲ.2.1	アプリケーションの情報セキュリティ対策	Ⅲ.2.1.1【基本】ウイルス対策：クラウドサービスの提供に用いるアプリケーション（データ・プログラム等）についてウイルス等に対する対策を講じること。 Ⅲ.2.1.2【基本】公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮：公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護すること。 Ⅲ.2.1.3【基本】アプリケーションサービスのトランザクションの保護：アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護すること。不完全な通信; 誤った通信経路設定; 認可されていないメッセージの変更；認可されていない開示；認可されていないメッセージの複製又は再生。 Ⅲ.2.1.4【基本】プラットフォーム変更後のアプリケーションの技術的レビュー：プラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験すること。 Ⅲ.2.1.5【基本】パッケージソフトウェアの変更に対する制限：パッ	テンセントクラウドはアプリケーションサーバーにエンドポイント検知対応（EDR）ツールを導入し、アンチウイルスと侵入検知、セキュリティベースラインと脆弱性スキャン、並びにコマンド操作、ログイン行動に対するセキュリティコンプライアンス監査などの機能をサポートし、マルウェアや異常行動などを検知した際にアラートを発報します。テンセントクラウドは定期的に EDR ツールのセキュリティポリシー（ユーザー権限ポリシー、システムアクセスポリシーなど）を検査・更新します。 公衆ネットワーク上のアプリケーションサービスのセキュリティを保護し、ネットワーク通信過程における通信情報の機密性と完全性を確保するため、テンセントクラウドは定期的に手動又は自動のアプリケーション脆弱性セキュリティ評価ツールを使用して公衆向けネットワークアプリケーションの脆弱性スキャンを実施し、公衆向け Web アプリケーションの前方に Web アプリケーションファイアウォールなどの Web ベース攻撃を検査・防御可能な自動化技術ソリューションを設置します。同時に、顧客がテンセントクラウドコンソール上で行う通信は全て HTTPS セキュリティプロトコルによる暗号化保護を受けます。テンセントクラウド製品が提供するクラウド API インターフェースも HTTPS 暗号化、署名検証、状態監視などのセキュリティ機能を有し、顧客の業務にポートレベルの通信セキュリティ保証を提供します。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		ケージソフトウェアの変更は、必要な変更だけに限ることが望ましい。また、全ての変更を厳重に管理すること。	**変更に関して、**テンセントクラウドは製品及び構成変更管理基準を確立し、変更プロセスの各ステップ及び関連責任者を明確化し、変更が実施前に適切な承認とテストを経ていることを確保しています。各タイプのプログラム変更（アプリケーションと設定ファイル、OS 及びデータベース変更を含む）は、リリース前に事業影響度分析を実施し、変更のロールバック計画を策定し、関連責任者の承認を得る必要があります。テンセントクラウドの変更リリースシステムは、変更操作が承認された要員のみによって実行されることを強制し、変更関連のログを保存して定期的なログ監査を実施します。変更リリース後、Tencent Cloud の運用チームは本番環境において変更内容の検証、監視、および結果記録を実施します。
Ⅲ.2.2	データの保護	Ⅲ.2.2.1【基本】バックアップ：利用者のデータ、アプリケーションの管理情報及びシステム構成情報の定期的なバックアップを実施すること。 Ⅲ.2.2.2【基本】バックアップ情報の完全性：バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認すること。	テンセントクラウドはバックアップ管理手順を策定し、関連法令規範の要求に基づき、収集・処理した重要データのバックアップを実施しています。内部重要情報については、テンセントクラウドはデータレベルに基づき異なるデータのバックアップ戦略を策定し、定期的に復旧テストを実施します。クラウド上の顧客データについては、テンセントクラウドはクラウド製品またはサービスの機能に応じて、複数のストレージレプリカとバックアップサービスを顧客に提供し、製品サービスレベル契約に定める通り、提供するデータバックアップサービスに対して責任を負います。
Ⅲ.2.3	セッション管理	Ⅲ.2.3.1【基本】セッションのライフサイクル管理：セッションのライフサイクルの制御(生成、破棄、タイムアウト検知)を行うこと。 Ⅲ.2.3.2【基本】セッションの真正性：通信セッションの真正性を保護すること。パケットレベルではなくセッションレベルでの通信の保護によっ て、通信セッションの	テンセントクラウド開発チームは、テンセントクラウド内部のアプリケーションセキュリティ管理規範の関連要件に従い、アプリケーション開発過程においてアプリケーションが備えるべきセキュリティ機能（アプリケーションのセッション管理を含む）を考慮します。テンセントクラウドは適切なセッションタイムアウト閾値を設定し、セッションハイジャック、リプレ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		両端で通信相手の身元及び伝送される情報の有効性に関して信頼の根拠をもたらす。 Ⅲ.2.3.3【基本】同時セッションの制御：同時処理されるアカウントの割り当て数又はアカウントタイプの割り当て数は、システムが定めた各セ ッションの割り当て数まで制限すること。 Ⅲ.2.3.4【基本】セッションのロック：定められたアイドル時間を経過した場合又は利用者から要求された場合、システムがセッションをロックすることによって以降のアクセスを遮断すること。なお、認証手順として確立された手順を用いたユーザによってアクセスが再確立されるまで、セッションをロックすること。	イ攻撃、不正アクセスのリスクを低減します。テンセントクラウドは製品リリース前にセキュリティ評価と検査を実施し、適切なセッション管理機能が設定されていることを確認します。 セッションセキュリティを保証するため、顧客がテンセントクラウドコンソール上で行う通信は全て HTTPS セキュリティプロトコルによる暗号化保護を受けます。テンセントクラウドのクラウド製品が提供するクラウド API インターフェースは HTTPS 暗号化、署名検証、状態監視などのセキュリティ機能を有し、顧客の業務にポートレベルの通信セキュリティ保証を提供します。

5.3 PaaS/IaaS 編

5.3.1 運用における情報セキュリティ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
IV.1.1	運用管理	IV.1.1.1【基本】情報セキュリティ監視手順の策定：情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。また、クラウドサービスの提供に用いる管理機能を持つアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の運用・管理に関する手順書を作成すること。 IV.1.1.2【基本】運用管理端末：運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。従業員等が 用いる運用管理端末の全ファイルのウイ	**運用管理に関して、**テンセントクラウドは運用管理規範を策定し、運用要員の日常的な運用行動に対する操作指針と要件を提供しています。テンセントクラウドは成熟したツール化・自動化された運用管理プラットフォームを採用して運用操作を管理し。 **セキュリティ監視に関して**、テンセントクラウド内部ではログ収集と管理規範及び関連メカニズムを確立し、ログインログ、操作ログ、イベントログなどのログデータの記録、抽出、分析、監査などを管理し、システム活動の異常とリスクの検出と防止を図っています。テンセントクラウドは

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		ルスチェックを行うこと。 IV.1.1.3【基本】稼働・障害監視：クラウドサービスの提供に用いる管理機能を持つアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の稼働監視、障害監視、パフォーマンス監視を行うこと。稼働停止や異常を検知した場合は、利用者に速報すること。また、結果を評価・総括して、管理責任者に報告すること。 IV.1.1.4【基本】追加報告：クラウドサービスの提供に用いる管理機能を持つアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器に係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告をクラウドサービス利用者に対して行うこと。 IV.1.1.5【基本】定期報告：クラウドサービスの提供に用いる管理機能を持つアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の監視結果（障害監視、死活監視、パフォーマンス監視）について、定期報告書を作成して利用者等に報告すること。 IV.1.1.6【基本】時刻同期：クラウドサービスの提供に用いる管理機能を持つアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の時刻同期の方法を規定し、実施すること。 IV.1.1.7【基本】パスワード管理：パスワード管理システムは、対話式とすること、また、良質なパスワ	ログをログ管理プラットフォームに一元的に集約し管理し、関連ログ情報にはバックアップと厳格な保護措置が講じられ、不正な変更や削除から保護されます。テンセントクラウドは運用セキュリティ自動化監査ツールと内部監査チームを通じてログ監査を実施し、システム又は操作の異常を検出して操作リスクを防止します。 テンセントクラウドが顧客に提供するクラウドサービスは、各サービスごとに合意されたサービスレベル契約（SLA）に基づいて提供されます。各サービスの性能指標、測定基準及び報告要件は、各製品のサービスレベル契約において明確化され、テンセントクラウド公式サイトに公開されています。各クラウドサービスの性能と可用性は継続的に追跡され、関連指標は管理コンソールを通じて顧客がリアルタイムで監視可能です。 **アンチウイルスとマルウェア対策に関して、**テンセントクラウドはエンドポイント検知対応（EDR）ツールを導入し、全ネットワークサーバーエンドポイント資産の包括的な監視と管理を実施しています。テンセントクラウドはさらにゼロトラストセキュリティ管理システムを通じてオフィスエンドポイントの管理を実施し、ウイルス駆除、脆弱性修正、能動的防御などのセキュリティ機能により、ランサムウェア対策、フィッシング攻撃対策、内部横断移動対策などの包括的なセキュリティ保護を実現しています。 **セキュリティインシデント又は異常状況の報告に関して、**テンセントクラウドは情報セキュリティインシデント対応、エスカレーション、通知などの関連手順を確立し、事故の影響を受ける可能性がある、又は既に影響を受けている会社内部関係者、顧客などの関連者に対し速やかに注意喚起又は通知を行い、各関係者が秩序立て

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		ードを確実にするものとすること。 IV.1.1.8【基本】クラウドサービスの変更管理：情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更を管理すること。また、事業者は、クラウドサービスに悪影響を与える可能性のあるクラウドサービスの 変更について、利用者に情報を提供すること。 IV.1.1.9【基本】リソース監視：要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測すること。また、事業者は、資源不足による情報セキュリティインシデントの発生を防ぐため、資源全体の容量・能力を監視すること。 IV.1.1.10【基本】環境分離：開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために、分離すること。 IV.1.1.11【基本】マルウェア対策：マルウェアから保護するために、検出、予防及び回復のための対策を実施すること。 IV.1.1.12【基本】イベントログの取得：利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、 保持し、定期的にレビューすること。また、事業者は、利用者に、ログ取得機能を提供すること。 IV.1.1.13【基本】ログの保護：ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護すること。	て、迅速かつ効率的にコミュニケーションと調整を行えるようにしています。顧客に影響を及ぼす可能性のあるセキュリティインシデントについては、テンセントクラウドは情報セキュリティインシデントの影響範囲と程度に基づき、内部審査を経た後、情報セキュリティインシデントの処理と分析結果を適切な方法で顧客に通知し、対応する技術支援を提供して、顧客が損失を最小限に抑えるための救済措置を講じることを支援します。 **容量管理に関して、**テンセントクラウドは 内部容量監視プラットフォームを使用して容量使用状況をリアルタイム監視し、容量使用のトレンドを識別します。業務部門は情報システムの事業継続性を保証しつつ、前期の容量監視で得られた容量使用トレンドを参考に新規業務とシステムのニーズを考慮して容量を予測し、年次容量管理計画を策定します。 **時刻同期に関して、**テンセントクラウドは ネットワークタイムプロトコル (Network Time Protocol、NTP) を通じて正確な現在の世界協定時（UTC）を表示します。テンセントクラウドはテンセントクラウド上のインスタンス向けに社内ネットワーク NTP サーバーを提供し、テンセントクラウド以外のデバイスについては、顧客がテンセントクラウド提供の公衆ネットワーク NTP サーバーを利用できます。 **変更管理に関して、**テンセントクラウドは 製品及び構成変更管理基準を確立し、変更プロセスの各ステップ及び関連責任者を明確化し、変更が実施前に適切な承認とテストを経ていることを確保しています。顧客に影響を及ぼす可能性のある運用変更操作については、テンセントクラウドは公式サイト、サイト内メッセージなどのチャネルを通じて関連顧客に速やかに変更通

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		IV.1.1.14【基本】作業記録：システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューすること。 IV.1.1.15【基本】ソフトウェア導入：運用システムに関わるソフトウェアの導入を管理するための手順を実施すること。 IV.1.1.16【基本】技術的ぜい弱性：利用中のシステムの技術的ぜい弱性に関する情報は、時機を失せずに獲得すること。また、そのようなぜい弱性に組織がさらされている状況を評価すること。さらに、それらと関連するリスクに対 処するために、適切な手段をとること。また、事業者は、提供するクラウドサービスに影響し得る技 術的ぜい弱性の管理に関する情報を利用者が利用できるようにすること。	知を発行します。 **環境分離に関して、**テンセントクラウドは 業界の実践を参考にネットワークセキュリティアーキテクチャを設計し、業務機能とセキュリティリスクに基づいてセキュリティドメインを分割し、異なるセキュリティドメイン間で物理的又は論理的分離を実施し、アクセス制御と境界防御などの措置を通じてオフィスネットワーク、生産ネットワークなどのセキュリティを確保しています。 **脆弱性管理に関して**，テンセントクラウド は定期的に脆弱性スキャンを実施し、スキャン結果を各関連責任部門に通知して関連リスクに対応し、脆弱性が顧客事業に与える影響度を評価します。関連チームによる内部審査を経た後、テンセントクラウドは脆弱性関連情報を公式サイト公告、サイト内メッセージなどの方法で顧客に速やかに通知し、通知内容には脆弱性の説明、影響範囲及び程度、テンセントクラウドが講じた統制措置、顧客向け修正提案及び具体的な操作指針を含みます（ただしこれらに限りません）。 運用管理に関連する追加情報については、本ガイド第 5.2.1 章「運用における情報セキュリティ」内の「Ⅲ.1.1-運用管理」を参照してください。
IV.1.2	システム及び情報の完全性	IV.1.2.1【基本】原本性確保：電子データの原本性確保を行うこと。 IV.1.2.2【推奨】 メモリ保護：許可されていないコードの実行からメモリを保護するための、セキュリティ対策を実施すること。 IV.1.2.3【基本】 セキュリティ侵害の検知：システム又はシステムコンポーネントにデータ又は機能を埋め込み、データが盗み出されたか、不適切に削除されたかを判断	顧客データの完全性を確保するため、テンセントクラウドはサービスレベル契約においてデータ保存の持続性、すなわち契約期間中のデータ消失防止確率を明確に定義しています。 テンセントクラウドはデータ保存時に多重レプリカ冗長保存と消去符号技術を採用し、完全性エラーを検出した際に直ちに必要な復旧措置を講じ、データのフォールトトレランス能力を向上させます。テンセントクラウドはデータアクセス権限に対

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		すること。 IV.1.2.4【推奨】 情報の更新: 不要になった情報は削除するとともに削除したことを記録するログ情報等を残すこと。 IV.1.2.5【推奨】 代替情報源: 主要な情報源が破損しているか利用できない場合、システム又はシステムコンポーネントが重要な機能又はサービスを実行するための代替情報源を使用すること。 IV.1.2.6【推奨】 情報の断片化: 一度システムに侵入されると、失われた情報を回復する方法は、通常は存在しない。組織は、情報を異なる要素に断片化し、それらの要素を複数のシステム又はシステムコンポーネントと場所に分散すること。	し全アクセスノードにおける実名認証と管理を実施し、データ資産の完全性と業務サービスの信頼性を保証し、リアルタイム監視と遮断メカニズムを構築して、異常なデータアクセス行動の検出と阻止を実施します。同時に、テンセントクラウドは専門チームによる 7*24 時間の運用サービスを提供し、先進的なサーバー監視と診断技術を活用してサーバーの各種障害を自動検出し、即座に自動復旧プロセスを起動します。 テンセントクラウド API の各リクエストには、ユーザー身元の検証とリクエストの完全性保証のため、公開リクエストパラメータに署名情報を含める必要があります。 テンセントクラウドはさらにアドレス空間配置のランダム化 (ASLR) などの措置を採用し、システムメモリのセキュリティを保護します。 システム及び情報の完全性に関連する追加情報については、本ガイド第 5.2.1 章「運用における情報セキュリティ」内の「Ⅲ.1.2-システム及び情報の完全性」を参照してください。
IV.1.3	媒体の保管と廃棄	IV.1.3.1【基本】 媒体保管: 紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。 IV.1.3.2【基本】廃棄: 機器及び媒体を正式な手順に基づいて廃棄すること。 IV.1.3.3【基本】輸送: 情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護すること。	テンセントクラウドは媒体に保存される情報の機微性に応じて媒体を保管・処分し、媒体管理関連手順を確立して、媒体保管と媒体処分の具体的なプロセスと基準を明確化しています。媒体処分前には関連承認が必要であり、媒体の処分に関する記録を作成します。異なる媒体の材質、保存原理及び機微情報レベルに応じて、関連チームはデータの復元不可を確保し、かつセキュリティ規範に適合する対象的な処理方法を選択します。 物理媒体を使用して情報を転送する際、テンセントクラウドはチケット形式で媒体の出庫、輸送、入庫の全プロセスを追跡します。輸送過程において、テンセントクラウドは安全確実な輸送業者を選定し、情報レベルに応じて保護措置を実施し、物理媒

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			体に保護包装を施して輸送中の物理的損傷を回避します。

5.3.2 プラットフォーム、サーバ・ストレージ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
IV.2.1	プラットフォーム、サーバ・ストレージの情報セキュリティ対策	IV.2.1.1【基本】ウイルス対策：クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージについてウイルス等に対する対策を講じること。	テンセントクラウドはエンドポイント検知対応（EDR）ツールを導入し、全ネットワークサーバーエンドポイント資産の包括的な監視と管理を実施しています。テンセントクラウドが採用する EDR ツールは、アンチウイルスと侵入検知、セキュリティベースラインと脆弱性スキャン、並びにコマンド操作、ログイン行動に対するセキュリティコンプライアンス監査などの機能をサポートし、マルウェアや異常行動などを検知した際にアラートを発報します。テンセントクラウドはチケットシステムを通じてアラートイベントのフォローアップと処理を実施します。さらに、テンセントクラウドは定期的に EDR ツールのセキュリティポリシー（ユーザー権限ポリシー、システムアクセスポリシーなど）を検査・更新します。
IV.2.2	プラットフォーム、サーバ・ストレージの運用・管理	IV.2.2.1【基本】可用性：クラウドサービスを利用者に提供する時間帯を定め、この時間帯におけるクラウドサービスの稼働率を規定すること。また、プラットフォーム、サーバ・ストレージの定期保守時間を規定すること。 IV.2.2.2【基本】リソース：クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。	**サービスのレベルと性能についてです**，テンセントクラウドが顧客に提供するクラウドサービスは、各サービスごとに合意されたサービスレベル契約（SLA）に基づいて提供されます。各サービスの性能指標、測定基準及び報告要件は、各製品のサービスレベル契約において明確化され、テンセントクラウド公式サイトに公開されています。各クラウドサービスの性能と可用性は継続的に追跡され、関連指標は管理コンソールを通じて顧客がリアルタイムで監視可能です。 テンセントクラウドはさらに顧客に対 Tencent Cloud Observability Platform (TCOP)を提供し、ユーザーがクラウド製

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			品 / クラウドリソースのリアルタイム監視、分析、アラート設定を実施することをサポートします。TCOP はクラウドサーバー、クラウドデータベースなどのクラウド製品が自主報告する各種監視指標と顧客がカスタマイズ設定した監視指標を収集し、可視化グラフで表示し、顧客がクラウド製品リソースの使用率、アプリケーション性能、クラウド製品の稼働状況をリアルタイムで把握することを支援します。TCOP は指標に対するアラート設定をサポートし、設定されたアラートルールに基づき、メッセージプッシュなどの方法で業務異常状況を顧客に速やかに通知します。 さらに、テンセントクラウドはインフラストラクチャの定期保守と点検を実施し、保守点検記録を保存します。テンセントクラウドはデータセンター事業者に対し、要員を配置して日次で厳格に点検リストと点検計画に基づき各機械室とデバイスの状況を点検し、インフラストラクチャの障害又はセキュリティインシデントを速やかに発見、対応、処分することを求めています。 **容量計画と管理に関して、**テンセントクラウドは容量管理手順を策定し、各業務部門が関連業務システムの容量予測と計画を担当することを明確化しています。テンセントクラウドは内部容量監視プラットフォームを使用して容量使用状況をリアルタイム監視し、容量使用のトレンドを識別します。業務部門は情報システムの事業継続性を保証しつつ、前期の容量監視で得られた容量使用トレンドを参考に新規業務とシステムのニーズを考慮して容量を予測し、年次容量管理計画を策定します。
IV.2.3	データの保護	IV.2.3.1【基本】バックアップ：利用者のサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施するこ	テンセントクラウドはバックアップ管理手順を策定し、関連法令規範の要求に基づき、収集・処理した重要データのバックアップを実施しています。内部重要情報については、テンセントクラウドはデータレベ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		と。 IV.2.3.2【基本】バックアップ情報の完全性：バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認すること。	ルに基づき異なるデータのバックアップ戦略を策定し、定期的に復旧テストを実施します。クラウド上の顧客データについては、テンセントクラウドはクラウド製品またはサービスの機能に応じて、複数のストレージレプリカとバックアップサービスを顧客に提供し、製品サービスレベル契約に定める通り、提供するデータバックアップサービスに対して責任を負います。

5.3.3 ネットワーク

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
IV.3.1	ネットワークにおける情報セキュリティ対策	IV.3.1.1【基本】ネットワーク構成：ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。 IV.3.1.2【基本】管理者の権限：情報セキュリティ責任者は、システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。 IV.3.1.3【基本】不正アクセス防止：外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。 IV.3.1.4【基本】パケット検知：不正な通過パケットを自動的に発見、若しくは遮断する措置を講じること。 IV.3.1.5【基本】実施基準：外部ネットワークを利用した情報交換に	**ネットワークセキュリティ保護と管理を実施するため、**テンセントクラウドはネットワークセキュリティ管理規範とネットワーク多層防御体系を構築しています。テンセントクラウドは管理制度とプロセスを通じてネットワークセキュリティ管理と保護基準、並びに対応する役割と責任を明確化し、テンセントクラウドネットワークが担う業務の安全な運用を確保します。同時に、テンセントクラウドは業界の実践を参考にネットワークセキュリティアーキテクチャを設計し、業務機能とセキュリティリスクに基づいてセキュリティドメインを分割し、異なるセキュリティドメイン間で物理的又は論理的分離を実施し、アクセス制御と境界防御などの措置を通じてオフィスネットワーク、生産ネットワークなどのセキュリティを確保しています。テンセントクラウドはファイアウォール、侵入検知 / 防御システム (IDS/IPS)、DDoS 対策 Web セキュリティ保護などの多重防御メカニズムを通じて、悪意のあるネットワークトラフィックを速やかに検出、フィルタリング、遮断し、テンセントクラウドのネットワークセキュリティを保護します。 テンセントクラウドはさらにネットワーク攻撃、データセキュリティ、デバイス・

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		おいて、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。 IV.3.1.6【基本】通信の暗号化：外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。 IV.3.1.7【基本】サーバ証明書：第三者が当該事業者のサーバになりすますこと (フィッシング等) を防止するため、サーバ証明書の取得等の必要な対策を実施すること。 IV.3.1.8【基本】情報セキュリティ特性：利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。 IV.3.1.9【基本】障害監視：外部ネットワークの障害を監視し、障害を検知した場合は管理責任者に通報すること。 IV.3.1.10【推奨】 クロス・ドメイン・ポリシーの実施：論理的に接続するセキュリティドメインの物理インターフェイスやネットワークインターフェイス間にポリシー施行メカニズムを実装すること。 IV.3.1.11【推奨】 統制管理のための代替通信パス：指揮統制のために代替通信パスを確立すること。 IV.3.1.12【推奨】 検出機器の再配置：攻撃者が目標を達成する能力を妨げるために、センサー又は監視機能を新しい場所に再配置すること。	施設障害、災害的イベントなどの異なるネットワークセキュリティ緊急時シナリオに応じて、緊急時対応計画と対応計画を策定・維持し、内部におけるネットワークセキュリティ緊急事態の秩序立てた速やかな処分を確保し、ネットワークセキュリティインシデントがテンセントクラウドに与える悪影響を軽減します。 **ネットワーク通信保護に関して、**顧客がテンセントクラウドコンソール上で行う通信は全て HTTPS セキュリティプロトコルによる暗号化保護を受けます。テンセントクラウドのクラウド製品が提供するクラウド API インターフェースは HTTPS 暗号化、署名検証、状態監視などのセキュリティ機能を有し、顧客の業務にポートレベルの通信セキュリティ保証を提供します。 **ネットワークレジリエンスを保護するため、**テンセントクラウドのデータセンターは世界中の複数地域に分散し、各アベイラビリティーゾーンのネットワーク出口は複数の通信事業者と接続され、テンセントクラウドネットワークの跨地域災害復旧能力を構築し、通信事業者の公衆ネットワーク障害に伴う継続的な影響を効果的に低減します。テンセントクラウドの基盤ネットワークは の冗長構築方式を採用し、ルーティング階層における経路優先度と経路到達可能性のトラフィックエンジニアリングスケジューリングと連携することで、単一デバイス障害によるネットワークサービスの中断を防止します。 **ネットワークデバイスセキュリティに関して、**テンセントクラウドはネットワークセキュリティ構成基準とセキュリティベースライン基準を整備し、ネットワークデバイス、ファイアウォール、ホストサーバーOS、データベース、及びアプリケーションシステムのセキュリティ構成を標準化

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		IV.3.1.13【推奨】 ハードウェア/ソフトウェアによる分離とポリシーの施行セキュリティドメイン間にハードウェア/ソフトウェアによる分離とポリシーの適用メカニズムを実装すること。 IV.3.1.14【推奨】 ハードウェアベースの書き込み保護：システムファームウェアコンポーネントにハードウェアベースの書き込み保護を採用すること。	管理しています。テンセントクラウドのセキュリティチームは定期的にルーター、ファイアウォール、ネットワークサーバーなどのネットワークデバイスのセキュリティポリシーとパラメータ設定を見直し、ポリシーとパラメータの有効性を確保します。テンセントクラウドはさらに内部ネットワーク監視システムを設置してネットワークデバイスを監視・アラートし、チケットシステムを通じて識別されたセキュリティ問題のフォローアップと解決を実施します。さらに、テンセントクラウドは権限管理、承認プロセスなどの多重措置を通じて、非承認要員による内部ネットワークリソースへのアクセスを厳禁します。 **マルチテナントデータ分離に関して、**テンセントクラウドは「データの機密性」の原則を厳格に遵守し、仮想化制御層リソースアクセス制御ポリシー、クラウドプラットフォーム内部プライベートネットワーク間分離ポリシー、Web コンソール権限割り当てと身元認証、インターフェースセッション ID とアクセスキーなどのセキュリティメカニズムを含む多層的な技術的分離手段を通じて、顧客データが相互に不可視であることを確保し、技術的にテナントが他テナントのデータにアクセス、取得、又は改ざんできないことを保証します。 **データ漏洩防止の面では、**テンセントクラウドはデータアクセス権限に対し、全ノードでの実名制による審査と管理を実施し、データ資産の完全性と業務サービスの信頼性を確保しています。また、リアルタイムの監視および遮断メカニズムを構築し、あらゆる異常なデータアクセス行為を検知・阻止しています。さらに、テンセントクラウドは従業員の業務端末にデータ漏洩防止（DLP）ツールを導入し、データの持ち出しを効果的に制限するとともに、潜在的なデータ窃取活動を監視、検知、防止

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			しています。 **ネットワーク攻撃の検出に関して**、テンセントクラウド内部では、ログ収集および管理の規範とメカニズムを確立しています。ログインログ、操作ログ、イベントログなどのログデータの記録、抽出、分析、監査などを管理し、システム活動の異常やリスクを検知・防止します。また、Tencent Cloud は内部ネットワーク監視システムを設置し、ルーター、ファイアウォール、ネットワークサーバーなどのネットワーク機器を監視・アラート通知するとともに、チケットシステムを通じて特定されたセキュリティ問題を追跡・解決しています。同時に、Tencent Cloud は詳細な運用セキュリティの「レッドライン」を設定し、異常行動監視における長年の経験をもとに充実したルールベースを構築し、信頼性の高い運用セキュリティ自動監査ツールを開発しました。これにより、異常行動を即座に識別し、リアルタイムのアラートを自動的にトリガーすることが可能です。 **テンセントクラウドはさらに顧客がネットワークセキュリティを効果的に管理するため、以下の複数のサービスを提供しています:** • EdgeOne (EO) platform、テンセントのグローバルエッジノードに基づき、顧客にセキュリティ保護と加速サービスを提供します。DDoS 対策、インテリジェント Web 保護、BOT/クローラー攻撃対策 DNS 解析などの機能を有し、顧客が業務ニーズに応じてカスタムアクセス制御ルールを設定することをサポートします。 • Virtual Private Cloud (VPC)はトンネル技術に基づき、物理ネットワーク上に仮想ネットワークを構築し、仮想

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			化技術を使用して異なるプライベートネットワーク間の完全な論理分離を実現し、顧客に独立・分離された安全なクラウドネットワークを提供します。プライベートネットワーク内のクラウドサーバーについては、セキュリティグループ及びネットワーク ACL ルールを設定することで、インスタンスレベル及びサブネットの出入りトラフィックを制御し、異なる階層でのネットワークアクセス制御を実現します。 • Cloud Firewall (CFW)は、ファイアウォール ACL の能動的管理、IPS リアルタイム遮断、仮想パッチ、マルウェア検知などの機能をサポートし、顧客に異なるネットワーク境界での保護を提供します。 • Web Application Firewall (WAF)は、Web 攻撃、侵入、脆弱性悪用、マルウェア埋め込み、改ざん、バックドア、クローラーなどの Web サイト及び Web 業務セキュリティ保護課題に対応します。 • Anti-DDoS は、十分かつ高品質な DDoS 対策リソースと、進化を続ける「自社開発+AI インテリジェント識別」洗浄アルゴリズムを組み合わせ、DDoS 攻撃問題に対応します。 • Flow Logs は、ネットワークトラフィックのリアルタイム、非侵入型のパススルー収集、保存、分析をサポートし、顧客の障害調査、アーキテクチャ最適化、セキュリティ検知、コンプライアンス監査などの課題解決を支援します。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
IV.3.2	情報の転送	IV.3.2.1【基本】情報転送の方針及び手順：あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び対策を備えること。 IV.3.2.2【基本】情報転送に関する合意：組織と外部関係者との間で、業務情報のセキュリティを保った転送について、合意すること。 IV.3.2.3【基本】秘密保持契約又は守秘義務契約：情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、 定めに従ってレビューし、文書化すること。	テンセントクラウドはデータセキュリティ関連管理手順を確立し、データ分類、転送などの活動を規範化し、第三者との情報転送管理に関する要件を明確化しています。 テンセントクラウドは国際版公式サイト上でオンラインの『データプライバシーとセキュリティ契約』を提供し、テンセントクラウドが提供するサービスに関連するデータ処理及び転送に適用されます。当該契約には顧客とテンセントクラウド双方のセキュリティ責任と義務などが明確に規定されています。顧客はさらにテンセントクラウドとオフライン契約を締結し、契約中の条項と細則を協議することもできます。 **情報転送関連の保護措置に関して**、顧客がテンセントクラウドコンソール上で行う通信は全て HTTPS セキュリティプロトコルによる暗号化保護を受けます。テンセントクラウド製品が提供するクラウド API インターフェースも HTTPS 暗号化、署名検証、状態監視などのセキュリティ機能を有し、顧客の業務にポートレベルの通信セキュリティ保証を提供します。顧客はさらに以下のテンセントクラウドサービスを利用して、異なるシナリオでのデータ安全転送を実現できます： • Direct Connect (DC): 専用性と高セキュリティ性を備えた大容量ネットワーク接続を提供します。ユーザーがネットワークリンクを占有するため、データ漏えいリスクがありません。 • VPN Connection：ネットワークトンネル技術に基づき、ローカルデー

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			タセンターとテンセントクラウド上のリソース間の安全な転送を実現します。VPN トンネルは IKE (鍵交換プロトコル) と IPsec を使用して転送データを暗号化し、インターネット上に安全で信頼性の高いデータトンネルを構築して、転送途中のデータセキュリティを保証します。 • Cloud Connect Network (CCN): クラウド上のプライベートネットワーク (VPC) 間、VPC とローカルデータセンター (IDC) 間の社内ネットワーク相互接続をサポートし、全ネットワーク多点相互接続、ルーティング自動学習、リンク最適化、障害高速収束などの能力を備えます。クラウド相互接続内のネットワークインスタンスの全通信データは公衆ネットワークを経由せず、優れた通信品質とネットワーク可用性、低遅延、低パケットロス率などの特徴を有し、多重リンク冗長性により通信品質を保証し、データを安全確実にします。 **機密保持責任に関して、**テンセントクラウド法務部門は機密保持契約の策定と更新を担当します。テンセントクラウドが第三者会社（サプライヤーなど）又は個人（従業員など）と締結する機密保持契約には、契約の有効期間、機密保持契約署名者又は署名会社の責任 / 義務、保護すべき情報、契約終了時の情報の書庫化と消去要件、契約違反の結果などが明確に規定されています。
IV.3.3	セッション管理	IV.3.3.1【基本】セッションのライフサイクル管理：セッションのライフサイクルの制御(生成、破棄、タイムアウト検知)を行うこと。 IV.3.3.2【基本】セッションの真正性: システムは、通信セッションの	テンセントクラウド開発チームは、テンセントクラウド内部のアプリケーションセキュリティ管理規範の関連要件に従い、アプリケーション開発過程においてアプリケーションが備えるべきセキュリティ機能（アプリケーションのセッション管理を含む）を考慮します。テンセントクラウド

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		真正性を保護すること。 IV.3.3.3【基本】同時セッションの制御：同時処理されるアカウントの割り当て数又はアカウントタイプの割り当て数は、システムが定めた各セッションの割り当て数まで制限すること。 IV.3.3.4【基本】セッションのロック：定められたアイドル時間を経過した場合又は利用者から要求された場合、システムがセッションをロックすることによって以降のアクセスを遮断すること。なお、認証手順として確立された手順を用いたユーザ によってアクセスが再確立されるまで、セッションをロックすること。	は適切なセッションタイムアウト閾値を設定し、セッションハイジャック、リプレイ攻撃、不正アクセスのリスクを低減します。テンセントクラウドは製品リリース前にセキュリティ評価と検査を実施し、適切なセッション管理機能が設定されていることを確認します。 セッションセキュリティを保証するため、顧客がテンセントクラウドコンソール上で行う通信は全て HTTPS セキュリティプロトコルによる暗号化保護を受けます。テンセントクラウドのクラウド製品が提供するクラウド API インターフェースは HTTPS 暗号化、署名検証、状態監視などのセキュリティ機能を有し、顧客の業務にポートレベルの通信セキュリティ保証を提供します。

5.3.4 建物、電源

現在、日本地域のデータセンターは、国際標準化機構（ISO）による一連の認証を含む、複数の国際的に権威あるセキュリティおよびプライバシーコンプライアンス認証を全面的に取得しています。具体的には、ISO/IEC 27001 情報セキュリティマネジメントシステム認証、ISO/IEC 27017 クラウドサービス情報セキュリティ認証、ISO/IEC 27018 パブリッククラウドにおける個人識別可能情報（PII）保護認証、ISO/IEC 27701 プライバシー情報マネジメントシステム認証、および ISO/IEC 29151 個人識別情報保護認証を含みます。さらに、クラウドセキュリティアライアンス（CSA）STAR セキュリティ信頼性保証認証、Payment Card Industry Data Security Standard（PCI-DSS）国際パブリッククラウド認証、並びに SOC Type 2 監査にも合格しており、情報セキュリティ、プライバシー保護、クラウドサービスコンプライアンス、決済データセキュリティを網羅する全次元のコンプライアンス体系を構築し、国際的なベストプラクティスと業界の厳格な管理要件を厳格に順守しています。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
IV.4.1	建物の災害対策	IV.4.1.1【基本】建物：クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等のシステムが設置されている建物（情報処理施設）については、物理的及び環境上の危険を考慮して、システムが存在する施設の場所を計画すること。また、地震・水害に対する対策が行われていること。 IV.4.1.2【基本】電源：クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等のシステムを設置する場所には、停電や電力障害が生じた場合に電源を確保するための対策を講じること。 IV.4.1.3【基本】空調：クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等のシステムを設置する場所では、設置されている機器等による発熱を抑えるのに十分な容量の空調を提供すること。	クラウドサービスプロバイダーとして、テンセントクラウドは顧客に安全、安定、継続的、信頼性の高い物理施設基盤を提供することに努めています。テンセントクラウドはデータセンター関連の国際基準と監督要件に基づき、計画-実施-チェック-改善（PDCA）のセキュリティマネジメントシステム汎用プロセスモデルに従い、包括的なセキュリティ管理体系を確立し、厳格な監査とともに継続的改善を通じてクラウドコンピューティングデータセンターの物理的及び環境的セキュリティを保証しています。 テンセントクラウドは世界中の各データセンターを関連国際基準と現地のセキュリティ要件に従って立地、建設又は賃貸し、環境脅威を十分に考慮して高確率の環境リスク地域を回避しています。現在、テンセントクラウドは日本地域に2つの賃貸式データセンターを配備しており、テンセントクラウドはデータセンター事業者に対し、高安定性の全冗長電源システムと空調システムなどを採用し、単一障害点がデータセンターの継続性と可用性に影響を与えることを回避するよう求めています。 加えて、テンセントクラウドの日本地域におけるデータセンターは、立地選定段階において、地域の地質学的・気象学的リスクを十分に考慮しています。津波リスクを根源的に回避するため、標高が比較的高く、海岸線から離れ、地質構造が安定した場所を優先的に選定しています。建築物の基礎高さの嵩上げ、完全な排水システムなどの設計により、洪水被害への耐性を強化しています。建築主体は高い耐震性を備えた構造体系を採用し、耐震能力を全面的に強化して地震リスクを効果的に軽減し、インフラの持続的かつ安定的な稼働を保証しています。
IV.4.2	火災、雷、静電気からシ	IV.4.2.1【基本】汚損対策：サーバルームに設置されているクラウドサービスの提供に用いるサーバ・	テンセントクラウドは事業者に対し、データセンターに完全な消防システム（特定区域火災検知システム、自動消火システム、

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
	ステムを防護するための対策	ストレージ、情報セキュリティ対策機器等のシステムについて、放水等の消火設備の使用に伴う汚損に対する対策を講じること。 IV.4.2.2【基本】火災対策：クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等のシステムを設置するサーバルームには、火災検知・通報システム及び消火設備を備えること。 IV.4.2.3【基本】雷対策：情報処理施設に雷が直撃した場合及び誘導雷が発生した場合を想定した対策を講じること。 IV.4.2.4【基本】静電気対策：クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等のシステムについて、作業に伴う静電気対策を講じること。 IV.4.2.5【基本】緊急遮断：緊急時に、システム又は個々のシステムコンポーネントの電源を遮断できる機能を提供するとともに、緊急時に電源を遮断する機能が、不正に起動されないようにすること。 IV.4.2.6【基本】非常用電源：一次電源が失われた場合に、長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用意すること。 IV.4.2.7【基本】非常用照明：停電が発生した場合や、電力が途絶えた場合に作動し、施設内の非常口と避難経路を照らす自動非常用照明をシステムに導入し、維持すること。 IV.4.2.8【推奨】電磁パルス保護対策：システム及びシステムコンポ	緊急時手動消火装置を含む）を設置することを求めています。 テンセントクラウドは事業者に対し、データセンター内部に静電気防止床を設置し、キャビネット、配線ダクトなどに接地線を設置して、静電気によるデバイス損傷を防御することを求めています。 テンセントクラウドは事業者に対し、データセンターに避雷システム、防放射システム、給配電システム、UPS システム、照明システムなどの機械室正常稼働に必要な施設を設置することを求め、データセンターの保守要員が交代勤務で 24 時間 365 日の保守を実施し、デバイス障害の迅速な解決を確保することを求めています。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		ーネントの電磁パルス損傷に対して保護対策を講じること。	
IV.4.3	装置の対策	IV.4.3.1【基本】 サポートユーティリティ: 装置は、サポートユーティリティの不具合による、停電、その他の故障から保護すること。サポートユーティリティ (電気、通信サービス、給水、ガス、下水、換気、空調等) は、次の条件を満たすこと。 a) 装置の製造業者の仕様及び地域の法的要求事項に適合している。b) 事業の成長及び他のサポートユーティリティとの相互作用に対応する能力を定期的に評価する。 c) 適切に機能することを確実にするために定期的に検査及び試験する。 d) 必要であれば不具合を検知するための警報装置を取り付ける。 e) 必要であれば物理的な経路が異なる複数の供給元を確保する。 IV.4.3.2【基本】ケーブル配線のセキュリティ: データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護すること。 IV.4.3.3【基本】 装置の保守: 装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守すること。 IV.4.3.4【基本】資産の移動: 装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出さないこと。 IV.4.3.5【基本】構外にある装置及び情報資産のセキュリティ: 構外にある情報資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、 セキュリティを適用するこ	**デバイスなどの資産管理に関して、**テンセントクラウドは資産管理システムを通じてデバイスなどを管理し、資産登録及び紐付け、資産棚卸及び情報更新、資産廃棄及び交換などを含め、クラウドプラットフォーム基盤システムの安定した運用を保障し、業務システムに信頼性の高い支援を提供します。デバイスが機械室に出入りする際（設置・稼働又は廃棄・移出）は、対応する承認と検査プロセスに従います。関連要員は機械室で稼働するデバイスの物理的設置場所を速やかに資産管理システムに入力します。 テンセントクラウドは定期的にサーバーなどの廃棄と交換を実施します。テンセントクラウドサービス提供に使用される媒体に障害が発生し交換が必要な場合、又は使用期限に達し廃棄が必要な場合、テンセントクラウドは速やかに厳格なプロセスに従って完全な物理的破壊を実施し、消去記録に登録します。 **デバイス保守と監視に関して、**テンセントクラウドはデータセンター事業者のセキュリティ要員に対し、日次で厳格に点検リストと点検計画に基づき各機械室とデバイスの状況を点検し、各検査ポイントで署名と検査時間を記録し、インフラストラクチャの障害又はセキュリティインシデントを発見した際に直ちにデータセンター緊急事態対応プロセスを起動することを求めています。テンセントクラウドは事業者に対し、データセンターに 7*24 時間の死角なしビデオ監視アラートシステムを設置し、警備室で監視し、監視記録が安全に十分な期間保存されることを確保することを求めています。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		と。 IV.4.3.6【基本】装置のセキュリティを保った処分又は再利用：記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを全て消去していること、若しくはセキュリティを保って上書きしていることを検証すること。事業者は、装置のセキュリティを保った処分又は再利用を行うための取決めについ て、利用者と合意していること。 IV.4.3.7【基本】無人状態にあるクラウドサービス利用者装置：利用者は、無人状態にある装置が適切な保護対策を備えていることを確実にすること。 IV.4.3.8【基本】クリアデスク・クリアスクリーン方針：書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用すること。	**ケーブル配線セキュリティに関して、**テンセントクラウドはデータセンター事業者に対し、強電ケーブルと通信ケーブルを分離して配備し、干渉を回避することを求め、情報処理施設に接続する電源と通信回線を地下又はラック内に配備して、電力及び通信ケーブルのセキュリティを保護することを求めています。 **オフィス環境セキュリティに関して、**テンセントクラウドは従業員に対し、機微情報を含む紙文書を適切に収納することを求め、会議室及び研修室などの共有エリア使用後は、ホワイトボード上の機密及び機微情報を速やかに消去し、プロジェクターを閉じ、会議資料を持ち帰り、機密及び機微情報の漏えいを防止することを求めています。テンセントクラウド従業員のエンドポイントにはロック画面ポリシーが設定され、従業員がエンドポイントデバイスから離れる際にデバイスをロックします。コピー機、ファクシミリ、シュレッダー、プリンターなどの無人デバイスは、オフィスエリア内の監視下にある適切な場所に設置され、不正使用と侵入を回避します。
IV.4.4	建物の情報セキュリティ対策	IV.4.4.1【基本】オフィス、部屋及び施設のセキュリティ：オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用すること。 IV.4.4.2【基本】セキュリティを保つべき領域での作業：セキュリティを保つべき領域での作業に関する手順を設計し、適用すること。 IV.4.4.3【基本】入退室記録：重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室の手順書と記録を作成し、適切な期	テンセントクラウドは物理的セキュリティ管理制度を策定し、操作セキュリティを規範化し、リスクを速やかに識別し、物理的セキュリティ管理を強化しています。 **セキュリティ区域のアクセス管理に関して、**テンセントクラウドはデータセンター事業者に対し、人員カテゴリーとアクセス権限に基づき、入退館管理システムに完全な人員アクセス制御セキュリティマトリクスを構築し、各種人員のアクセス、操作などの行動を効果的に管理することを求めています。テンセントクラウドは事業者に対し、データセンターに出入りする各種訪問者又は作業員の身元確認と携帯品検査を実施し、持ち込まれた物品を登録する

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		間保存すること。 IV.4.4.4【基本】監視カメラ：重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像をあらかじめ定められた期間保存すること。 IV.4.4.5【基本】破壊対策ドア：重要な物理的セキュリティ境界の出入口に破壊対策ドアを設置すること。 IV.4.4.6【基本】警備員：重要な物理的セキュリティ境界に警備員を常駐させること。 IV.4.4.7【基本】鍵管理：サーバルームやラックの鍵管理を行うこと。 IV.4.4.8【基本】受渡場所：荷物の受渡場所などの立寄り場所及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理すること。また、認可されていないアクセスを避けるために、それらの場所を情報処理施設から可能な限り離すこと。 IV.4.4.9【基本】搬入と搬出：施設に搬入・搬出されるシステムコンポーネントに対して許可・未許可、モニタリング及び管理を行い、それらについての記録を保管すること。	ことを求めています。 **警備と監視に関して**、テンセントクラウドは事業者に対し、セキュリティ要員を配置して厳格に点検リストと点検計画に基づき各機械室とデバイスの状況を点検し、各検査ポイントで署名と検査時間を記録し、インフラストラクチャの障害又はセキュリティインシデントを発見した際に直ちにデータセンター緊急事態対応プロセスを起動することを求めています。テンセントクラウドはさらに事業者に対し、データセンターに 7*24 時間の死角なしビデオ監視アラートシステムを設置し、警備室で監視し、監視記録を安全に保存して十分な期間保存することを確保することを求めています。 **引継区域と物品の出入り管理に関して**、テンセントクラウドはデータセンター事業者に対し、データセンター機械室引継区域（機械室に入室せずにアクセス可能な区域）を設置することを求めています。引継区域内部の通路が開放されている間、引継区域外部の通路には対応するセキュリティ保護が適用されます。テンセントクラウドはさらに事業者に対し、関連チームを配置して引継区域に入る物品の検査と登録を実施し、搬入物品と搬出物品を分離して保管し、物品の損傷を発見した際に直ちに物品責任者に連絡して対応処理を行うことを求めています。

06

Tencent Cloud の「政府情報システムセキュリティ管理・評価計画(ISMAP)管理基準」への対応

政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program, ISMAP）は、日本政府が公共クラウドサービスの安全性を評価する制度であり、政府クラウドサービス調達におけるセキュリティ水準を確保することを目的としています。同制度は、内閣官房サイバーセキュリティ戦略本部の「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」に基づき、内閣サイバーセキュリティセンター（NISC）、デジタル庁、総務省、経済産業省が連携して運営しています。ISMAP は、クラウドサービスプロバイダーが遵守しなければならないセキュリティ要件を規定し、クラウドサービスプロバイダーの安全性を評価することで、日本政府のセキュリティ要件を満たすプロバイダーを登録し、政府機関が登録リストから迅速に調達・外部委託を行えるようにしています。ISMAP 登録プロバイダーとなるためには、クラウドサービスプロバイダーは ISMAP が承認した第三者評価機関による評価を受けなければなりません。

同制度の下、ISMAP ガバナンス委員会は「政府情報システムのためのセキュリティ評価制度（ISMAP）管理基準」を策定し、クラウドサービスプロバイダーが ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリストに登録申請する際に実施すべきセキュリティ措置を明示することを目的としています。「政府情報システムのためのセキュリティ評価制度（ISMAP）管理基準」は、ISMAP 評価 / 監査の前提となる基準でもあります。当該管理基準は、「クラウド情報セキュリティ管理基準 2016（JIS Q 27001：2014、JIS Q 27002：2014、JIS Q 27017：2016 に基づく）」に基づき、「政府機関におけるサイバーセキュリティ対策の統一基準（2023）」、NIST SP 800-53 rev.4、JIS Q 27014：2015 を参考に策定されました。

政府情報システムのためのセキュリティ評価制度（ISMAP）管理基準は、ガバナンス基準、管理基準、管理対策基準で構成される。ガバナンス基準は組織の情報セキュリティ活動を指導・管理する枠組みであり、管理基準は情報セキュリティ管理の確立・実施・運用・監視・維持・改善に関する基準を規定し、組織の情報セキュリティ活動に対する指揮統制を調整する。管理対策基準は、組織が情報セキュリティ管理構築段階でリスク対応方針に基づき選択可能な管理対策を提供する。

クラウドサービスプロバイダーとして、Tencent Cloud は事業運営所在の司法管轄区域の法令を厳格に遵守し、安全・安定・持続的・信頼性の高いクラウドサービス

の提供に努めています。Tencent Cloud は「政府情報システムのためのセキュリティ評価制度（ISMAP）管理基準」に基づき、管理状況の評価と改善を実施しました。現時点ではお客様からの関連要請を受けていないため、ISMAP 認証は取得しておりません。今後お客様から関連要求があった場合、Tencent Cloud は実情に応じて対応いたします。

さらに、Tencent Cloud は第三者による独立監査または評価を通じて、ISO/IEC 27001、ISO/IEC 27017、ISO/IEC 27018、ISO22301、NIST CSF、SOC など、複数のセキュリティおよびプライバシーコンプライアンス認証または資格を取得しており、Tencent Cloud のセキュリティ管理とプライバシー保護の構築が関連認証基準または業界のベストプラクティスを満たしていることを証明しています。特に日本地域においては、テンセントクラウドは『金融機関等コンピュータシステムの安全対策基準・解説書』に基づき、 管理の現状を評価し、これに基づいて対応するシステムおよび組織管理（SOC）レポートを作成しました。このレポートは、テンセントクラウドプラットフォームの安全性、可用性、機密性に関連する管理ポイントを網羅しています。テンセントクラウドのコンプライアンス情報の詳細については、本ガイドの第 2 章 Tencent Cloud セキュリティとプライバシーコンプライアンスをご参照ください。

07 Tencent Cloud の顧客向けクラウド製品サービス

Tencent Cloud はクラウド＋AI 技術を融合し、豊富で使いやすいフルスタック製品を構築。インフラストラクチャ層、プラットフォーム製品・ソリューション層からアプリケーション製品・ソリューション層に至るまで、企業の多様なニーズを満たし、デジタル化アップグレードを支援します。卓越した製品群を基盤に、安定性・信頼性・効率性に優れたサービスを提供し、企業の業務成長と競争力強化を実現。基礎セキュリティや業務セキュリティのあらゆるシナリオ要求を十分に満たし、企業がデジタルセキュリティ免疫システムを構築するのを支援します。以下では、テンセントクラウドの製品・サービスをカテゴリー別に簡潔にご紹介します。より包括的かつ詳細な情報は、テンセントクラウド公式サイトの「製品とサービス」ページでご確認ください。

7.1 セキュリティ関連製品

- **Web Application Firewall (WAF)**

Web Application Firewall (WAF) は、AI ベースのワンストップ Web 業務運営リスク保護ソリューションです。その保護原理は、Web 業務サイトに直接アクセスするトラフィックをまず Tencent Cloud WAF 保護クラスタノードに誘導し、クラウド上の脅威洗浄・フィルタリングを経て安全なトラフィックを業務サイトに返送することで、顧客の業務サイトに到達するトラフィックの安全性と信頼性を確保します。Tencent Cloud WAF は、SQL インジェクション、XSS（クロスサイトスクリプティング）、マルウェアアップロード、不正アクセスなどの OWASP 攻撃を効果的に防御できるほか、CC 攻撃のフィルタリング、0day 脆弱性パッチの提供、ウェブページ改ざんの防止など、多様な手段でウェブサイトのシステムと業務の安全を包括的に保護します。

- **Cloud Firewall (CFW)**

Cloud Firewall (CFW) は、パブリッククラウド環境向けの SaaS 型ファイアウォールです。主にインターネット境界防御を提供し、クラウド上のアクセス制御の統一管理とログ監査のニーズに対応します。従来のファイアウォール機能を備えつつ、クラウド上のマルチテナントおよび弾力的な拡張機能をサポートし、顧客のビジネスクラウド移行におけるネットワークセキュリティインフラストラクチャです。

- **Anti-DDoS**

Anti-DDoS は包括的・効率的・専門的な DDoS 防御能力を備え、企業組織向けに DDoS 高防御パッケージや DDoS 高防御 IP など多様な DDoS ソリューションを提供し、DDoS 攻撃問題に対応します。十分な高品質な DDoS 防御リソースと、継続的に進化する「自社開発＋AI インテリジェント識別」洗浄アルゴリズムを組み合わせ、顧客ビジネスの安定かつ安全な運用を保証します。

- **EdgeOne(EO)**

EdgeOne (EO) platform Tencent のグローバルエッジノードを基盤に海外市場向けにセキュリティ保護と高速化サービスを提供し、DDoS 防御、インテリジェント Web 保護、BOT/クローラー攻撃防御、DNS 解決などの機能を備えています。 お客様の業務ニーズに応じたカスタムアクセス制御の設定をサポートし、多様な業界の企業顧客を保護し、利用体験を向上させます。

- **Tencent Cloud Container Security Service (TCSS)**

Tencent Cloud Container Security Service (TCSS) は、コンテナ資産管理、イメージセキュリティ、ランタイム侵入検知などのセキュリティサービスを提供し、イメージ生成・保存から実行までのコンテナライフサイクル全体を保護し、企業のコンテナセキュリティ防御体系構築を支援します。

- **Vulnerability Scanning Service (VSS)**

Vulnerability Scanning Service (VSS) は、企業ネットワーク資産を自動検出・リスク識別する製品です。テンセントが 20 年近く蓄積したセキュリティ能力を基盤に、ネットワーク機器やアプリケーションサービスの可用性・安全性・コンプライアンスを定期的にスキャンし、継続的なリスク警告と脆弱性検出を実施。VSS と連携した専門的な修復提案により、企業のセキュリティリスクを低減します。

- **Penetration Testing Service (PTS)**

Penetration Testing Service (PTS) は主に Web アプリケーション、モバイルアプリのセキュリティペネトレーションテストを提供し、脆弱性の発見、悪用、修正、修正後の検証を含む脆弱性ライフサイクル全体をカバーします。PTS はハッカーが使用する可能性のある攻撃技術や脆弱性発見技術を完全にシミュレートし、対象シ

ステムのセキュリティを深く探査してシステムの最も脆弱な部分を発見します。ペネトレーションテストは、お客様の承認を得た上で、制御可能かつ非破壊的な方法と手段を用いて、対象システムやネットワーク機器に存在する弱点を発見し、セキュリティ強化の提案を行い、お客様のシステムセキュリティ向上を支援します。Tencent Cloud ペネトレーションテストサービスは、Tencent Security Lab のセキュリティ専門家によって実施され、ブラックボックス、ホワイトボックス、グレーボックスなど多様なテストソリューションを提供し、お客様の潜在的なリスクをより包括的かつ深く発見します。

- **Cloud Workload Protection Platform (CWPP)**

Cloud Workload Protection Platform (CWPP) はマルチクラウド環境向けホスト保護製品です。テンセントが蓄積した膨大な脅威データに基づき、機械学習を活用して資産管理、トロイの木馬ファイル駆除、侵入検知、脆弱性リスク警告、セキュリティベースラインなどの保護サービスを提供。サーバーが直面する主要なサイバーセキュリティリスクを解決し、企業のサーバーセキュリティ防御体系構築を支援します。

- **Cloud Security Center (CSC)**

Cloud Security Center (CSC) は、Tencent Cloud のワンストップセキュリティ管理プラットフォームです。資産センター、リスクセンター、アラートセンター、高度なセキュリティ管理を通じて、事前の脅威検知、事中の対応処置、事後の追跡分析というセキュリティ運用の閉ループを実現します。

- 資産センター：Tencent Cloud の 34 種類のクラウド資産を自動同期し、非 Tencent Cloud IP や非 Tencent Cloud ドメインを手動追加して統一管理。
- リスクセンター：ポートリスク、脆弱性リスク、脆弱なパスワードリスク、コンテンツリスク、クラウドリソース設定リスク、サービス公開リスクの 6 大リスクを検知し、分類管理します。
- アラートセンター：クラウドファイアウォール、Web アプリケーションファイアウォール、ホストセキュリティのログデータを統合し、アラートログの分析・集約に基づき、3 層防御のアラートを一元表示・処理します。

- 高度なセキュリティ管理：グループアカウントの統一管理をサポートし、模擬攻撃による防御検証を実施。

- **Key Management Service (KMS)**

Key Management Service (KMS) は、セキュリティ管理サービスであり、顧客が容易に鍵を作成・管理し、鍵の機密性、完全性、可用性を保護します。複数のアプリケーションやビジネスにおける鍵管理ニーズを満たし、規制やコンプライアンス要件に準拠します。KMS は FIPS-140-2 認証のハードウェアセキュリティモジュール（HSM）を基盤に鍵を生成・保護し、安全なデータ転送プロトコルを採用。複数データセンターに分散配置されたクラスタ型サービスとホットバックアップを実現し、基盤となる HSM デバイスは二重データセンターでのコールドバックアップ構成により、KMS の高可用性を確保します。KMS はオブジェクトストレージ、分散データベース、クラウドディスクなどのサービスの暗号化機能とシームレスに統合され、顧客が容易に適用できるようにします。

- **Data Security Governance Center (DSGC)**

Data Security Governance Center (DSGC) は、機密データの発見・分類・格付け、データマップ、異常データアクセス分析を統合したデータセキュリティ運用プラットフォームです。企業がデータ資産を自動的に整理し、クラウド上のデータを分類・格付け・セキュリティリスク評価を行うことを支援し、Tencent Cloud の各セキュリティ機能と連携して閉じたデータセキュリティ保護網を形成し、企業のセキュリティ効果を最大化します。

7.2 クラウドコンピューティング及びネットワーク製品

- **Cloud Virtual Machine (CVM)**

Cloud Virtual Machine (CVM) は高速・安定性を備えたクラウド仮想ホストであり、Tencent Cloud の主要製品の一つとして、クラウド上でスケーラブルな計算リソースを提供します。CVM は以下の優れた特徴を有します：

- 効率的-迅速な作成：一部のクラウドサーバーは 10 秒以内に作成が完了し、単一リージョンで毎分数千台のクラウドサーバー作成をサポート。

- 易用性-可用域間ホットマイグレーション：同一リージョン内の異なる可用域間でサーバーのホットマイグレーションが可能で、サービスの中断を防止します。
- 信頼性 - 高効率な災害対策：Tencent Cloud 独自のユニバーサルホスティンググループは、単一リージョン内で複数のアベイラビリティゾーンを提供するだけでなく、アベイラビリティゾーン内において物理マシン間、ラック間、スイッチ間の 3 層災害対策を実現し、包括的な災害対策次元を備えています。

- **Cloud Bare Metal (CBM)**

Cloud Bare Metal (CBM)は自動スケーリング可能なハイパフォーマンス CVM インスタンスであり、物理マシンのパフォーマンスを損なわないこと、リソースを安全に隔離できることなどのメリットがあります。このサービスを利用することで、物理サーバーを取得する時間が数分に短縮されます。CBM はパブリッククラウド VPC ネットワーク内で完全に実行され、クラウド上でのリソース利用の利便性と安全性を確実に保証します。各製品間の VPC 通信のパフォーマンスにボトルネックはありません。

- **Auto Scaling (AS)**

Auto Scaling (AS) は、コンピューティングリソースを効率的に管理する戦略を提供します。お客様は、管理戦略を時間周期で実行するように設定したり、リアルタイム監視戦略を作成したりして、CVM インスタンスの数を管理し、インスタンスへの環境デプロイを完了させ、ビジネスの円滑な運用を保証できます。需要がピーク時には、Elastic Scaling が自動的に CVM インスタンス数を増やし、パフォーマンスへの影響を防止します。需要が低い時には CVM インスタンス数を減らし、コストを削減します。Elastic Scaling 戦略は、需要が安定しているアプリケーションの自動化管理を実現するだけでなく、業務急増や CC 攻撃などの問題も解消します。また、毎日、毎週、毎月の使用量が変動するアプリケーションに対しては、業務負荷に応じて分単位での拡張が可能です。

- **Tencent Kubernetes Engine (TKE)**

Tencent Kubernetes Engine (TKE) はネイティブ Kubernetes を基盤とし、コンテナを中核とした高度にスケーラブルな高性能コンテナ管理サービスを提供します。

TKE はネイティブ Kubernetes API と完全互換であり、Tencent Cloud のクラウドディスク（CBS）、ロードバランサー（CLB）などの Kubernetes プラグインを拡張。コンテナ化されたアプリケーションに対し、効率的なデプロイ、リソーススケジューリング、サービスディスカバリー、動的スケーリングなど一連の完全な機能を提供します。開発、テスト、運用プロセスにおける環境の一貫性問題を解決し、大規模コンテナクラスタ管理の利便性を向上。顧客のコスト削減と効率化を支援します。

- **Tencent Container Registry (TCR)**

Tencent Container Registry (TCR) は、安全で専用かつ高性能なコンテナイメージのホスティング・配布サービスを提供します。お客様は複数のリージョンで同時に専用インスタンスを作成でき、コンテナイメージの近接取得を実現することで取得時間を短縮し、帯域幅コストを節約できます。TCR は細粒度の権限管理とアクセス制御を提供し、顧客のデータセキュリティを保証します。P2P 高速配布をサポートし、大規模クラスタでの同時大容量イメージ取得時の性能ボトルネックを解消。顧客の オンライン業務の迅速な拡張・更新を支援します。カスタムイメージ同期ルールとトリガーをサポートし、既存の CI/CD ワークフローと柔軟に連携可能。コンテナ DevOps の迅速な実現を支援します。

- **Virtual Private Cloud (VPC)**

Virtual Private Cloud (VPC) は Tencent Cloud 上に構築された専用クラウドネットワーク空間であり、Tencent Cloud 上の顧客リソースにネットワークサービスを提供します。異なる VPC 間は完全に論理的に分離されています。顧客のクラウド専用ネットワーク空間として、ソフトウェア定義ネットワーク（SDN）方式で VPC を管理でき、IP アドレス、サブネット、ルーティングテーブル、ネットワーク ACL、トラフィックログなどの機能設定が可能です。プライベートネットワークは、Elastic IP や NAT ゲートウェイなど、インターネット接続のための複数の方法もサポートし、複数の課金方式と帯域幅パッケージを提供してコストを節約します。同時に、VPN Connection or Direct Connect (DC) を通じて Tencent Cloud とローカルデータセンターを接続し、柔軟にハイブリッドクラウドを構築することもできます。

- **VPN Connection**

VPN Connection は、ネットワークトンネル技術に基づく伝送サービスであり、ローカルデータセンターと Tencent Cloud 上のリソースを接続します。これにより、インターネット上で安全かつ信頼性の高い暗号化チャネルを迅速に構築できます。VPN 接続は設定が簡単で、クラウド側の設定がリアルタイムで有効になり、信頼性が高いという特徴を持ち、ゲートウェイの高可用性を実現し、安定した継続的な業務接続を保証します。これにより、遠隔地での災害復旧やハイブリッドクラウド展開などの複雑な業務シナリオを容易に実現できます。

7.3 ストレージとデータベース関連製品

- **Cloud Log Service (CLS)**

Cloud Log Service (CLS) は、Tencent Cloud が提供するワンストップログサービスプラットフォームです。ログ収集、ログ保存からログ検索分析、リアルタイム消費、ログ配信まで、複数のサービスを提供し、お客様の業務運営、セキュリティ監視、ログ監査、ログ分析などの課題解決を支援します。CLS は高可用性の分散アーキテクチャを採用し、ログデータに対して多重冗長バックアップストレージを実施。単一ノードのサービス停止によるデータ利用不能を防止し、サービスの高可用性を実現。ログデータに安定した信頼性の高いサービス保証を提供します。

- **Cloud Object Storage (COS)**

Cloud Object Storage (COS) は、Tencent Cloud が提供するディレクトリ階層構造なし、データ形式制限なし、膨大なデータ容量に対応し、HTTP/HTTPS プロトコルアクセスをサポートする分散型ストレージサービスです。Tencent Cloud オブジェクトストレージは、 のマルチアーキテクチャ・マルチデバイス冗長ストレージを提供し、遠隔地災害復旧とリソース分離機能によりデータの永続性を実現します。COS はさらに盗用防止設定機能を備え、ブラックリストとホワイトリストを設定可能で、悪意のあるソースからのアクセスを遮断します。

- **Cloud Block Storage (CBS)**

Cloud Block Storage (CBS) は、CVM 向けの永続的なブロックレベルストレージサービスを提供します。クラウドディスク内のデータは、利用可能なゾーン内で自動的に複数レプリカによる冗長化ストレージされ、データの単一障害点リスクを回避

し、高い信頼性を実現します。クラウドディスクは、安定した低遅延のストレージ性能要件を満たす、複数のタイプと仕様のディスクインスタンスを提供します。同一アベイラビリティゾーン内のインスタンスへのマウント/アンマウントをサポートし、数分以内にストレージ容量を調整できるため、弾力的なデータ需要に対応します。

- **Cloud File Storage (CFS)**

Cloud File Storage (CFS) は、安全で信頼性が高く、スケーラブルな共有ファイルストレージサービスを提供します。CFS はクラウドサーバー、コンテナサービス、バッチコンピューティングなどのサービスと連携し、複数の計算ノードに容量とパフォーマンスが弾力的に拡張可能な高性能共有ストレージを提供します。CFS 標準ファイルストレージは 3 重冗長化により、極めて高い可用性と信頼性を実現します。CFS はユーザー分離、ネットワーク分離、およびアクセス許可リスト（ホワイトリスト）によりクライアントの操作権限を制限できます。

- **Cloud-Native Database TDSQL-C (TDSQL-C)**

Cloud Native Database TDSQL-C は、Tencent Cloud が独自開発した次世代クラウドネイティブリレーショナルデータベースです。従来のデータベース、クラウドコンピューティング、新ハードウェア技術の利点を融合し、高い弾力性、高性能、大容量ストレージ、安全で信頼性の高いデータベースサービスを提供します。クラウドネイティブデータベース TDSQL-C は、オープンソースデータベースエンジン MySQL および PostgreSQL と完全互換性を持ち、秒単位の障害切り替えと復旧をサポートし、データの安全性と信頼性を保証します。

- **TencentDB for MySQL**

TencentDB for MySQL は、クラウド上での MySQL データベースの簡単なデプロイと利用をサポートします。クラウドデータベース MySQL を利用すれば、お客様は数分でスケーラブルな MySQL データベースインスタンスをデプロイできます。クラウドデータベース MySQL は、バックアップロールバック、監視、迅速なスケールアウト、データ転送など、データベース運用保守の包括的なソリューションを提供し、IT 運用業務を簡素化することで、お客様がビジネス発展に集中できるようにします。

- **Tencent Cloud Distributed Cache (Redis ® OSS-Compatible)**

Tencent Cloud Distributed Cache (Redis ® OSS-Compatible) は、Tencent Cloud が提供する Redis プロトコル互換のキャッシュおよびストレージサービスです。豊富なデータ構造により、様々なタイプのビジネスシナリオ開発を支援します。マスター/スレーブホットスタンバイをサポートし、自動災害復旧切り替え、データバックアップ、障害移行、インスタンス監視、オンラインスケーリング、データロールバックなど、包括的なデータベースサービスを提供します。

- **TencentDB for MongoDB**

TencentDB for MongoDB は、世界的に人気の高い MongoDB を基盤に構築された高性能 NoSQL データベースです。MongoDB プロトコルに互換性があり、安定した豊富な監視管理機能、弾力的な拡張性を提供します。完全な自動データバックアップとロスレス復元メカニズムを備え、各インスタンスクラスターはデフォルトで毎日 1 回バックアップされます。リアルタイムのデュアルマシンホットスタンバイ、5 日間のコールドバックアップデータダウンロードが可能です。

- **Data Transfer Service (DTS)**

Data Transfer Service (DTS) は、MySQL、MariaDB、PostgreSQL、Redis、MongoDB など、複数のリレーショナルデータベースおよび NoSQL データベースの移行をサポートします。業務を停止させることなく、クラウドへのデータベース移行を容易に完了できます。リアルタイム同期チャネルを利用して高可用性データベース災害復旧アーキテクチャを簡単に構築し、データサブスクリプションを通じてビジネスデータマイニングや業務の非同期デカップリングなどのシナリオ要件を満たします。

7.4 開発・運用関連製品

- **Cloud Access Management (CAM)**

Cloud Access Management (CAM) は、Tencent Cloud が顧客に提供するユーザーおよび権限管理システムであり、Tencent Cloud 製品およびリソースへのアクセスを安全かつ詳細に管理することを目的としています。顧客は CAM 内でユーザーやロールの作成・管理・削除が可能で、ID 管理とポリシー管理を通じてユーザー/ロ

ールが実行できる操作やアクセス可能なリソースを制御できます。また、既存の社内アカウント体系を持つ企業や組織向けに、CAM はフェデレーション認証をサポートし、企業内ネットワークアカウントとの相互運用を実現します。顧客は CAM を通じて既存の認証体系を活用し、従業員やサービス提供者に Tencent Cloud サービスとリソースへのアクセス権限を付与できます。

- **CloudAudit**

CloudAudit は、Tencent Cloud アカウントの監視、コンプライアンスチェック、操作監査、リスク監査をサポートするサービスです。CloudAudit を活用することで、お客様はログを記録し、Tencent Cloud インフラストラクチャ全体における操作に関連するアカウント活動を継続的に監視・保持できます。CloudAudit は、Tencent Cloud 管理コンソール、API サービス、コマンドラインツール、その他の Tencent Cloud サービスを通じて実行された操作を含む、Tencent Cloud アカウント活動の履歴を提供します。これらの履歴は、セキュリティ分析、リソース追跡、問題調査の簡素化に役立ちます。

- **Bastion Host(BH)**

BH（Bastion Host）は、顧客の IT 資産に対するプロキシアクセスとインテリジェントな操作監査サービスを提供します。BH を統一的な入口として内部資産の管理・保守を行う場合、ユーザーは複数のアドレスやアカウント・パスワードを記憶する必要がありません。BH はユーザー、資産、アカウント、操作権限などの次元に基づく細粒度な権限付与をサポートし、ユーザーが持つ権限が資産へのアクセスや業務タスクの遂行に必要な最小限の権限であることを保証します。同時に、タイムスタンプ、コマンド文、ダウンロード/アップロード操作、アクセス IP、サーバー、ユーザー名など多角的な分析により異常行動を検知・アラートし、内部悪意のある事象を効果的に防止します。

- **Tencent Cloud Observability Platform (TCOP)**

Tencent Cloud Observability Platform（TCOP）は、Tencent Cloud クラウド製品が自動報告する各種監視指標と、顧客が独自に設定して報告する監視指標を収集し、グラフで表示します。同時に、指標に対するアラート設定をサポートします。立体的なクラウド製品データ監視、インテリジェントなデータ分析、リアルタ

イム異常アラート、カスタマイズ可能なデータレポート設定を提供し、顧客が業務と各クラウド製品の健全性をリアルタイムかつ正確に把握できるようにします。

- **Cloud-Native Build (CNB)**

Cloud Native Build (CNB) は、コードホスティング、クラウドネイティブビルド、クラウドネイティブ開発、AI コードアシスタント、アーティファクトリポジトリなどの機能を提供します。CNB は Docker エコシステムを基盤とし、環境、キャッシュ、プラグインを抽象化し、宣言型構文を採用することで、開発者がより効率的な方法でソフトウェアを構築することを支援します。

08 結び

Tencent Cloud は、Tencent グループが注力して構築したクラウドコンピューティングブランドであり、Tencent の長年にわたる技術蓄積とセキュリティ実践能力を継承しています。Tencent Cloud は、お客様に安全で信頼性が高く、知的なクラウドを継続的に提供し、より多くの企業がデジタル化の波に効率的に対応し、企業の安全な発展を推進することを支援することに尽力しています。

本ガイドは、日本の総務省および ISMAP 運営委員会の重要な指針と基準に基づき、Tencent Cloud がどのように顧客のクラウド上システムとデータのコンプライアンス実現を支援し、企業顧客が安心してシステムとデータをクラウドに託すことを可能にするかを、包括的かつ透明性をもって示します。Tencent Cloud は本ガイドを通じて、企業顧客が日本の総務省および ISMAP 運営委員会のコンプライアンス要件を効果的に満たすと同時に、デジタル化アップグレードとビジネスの革新的発展を効率的に実現することを支援したいと考えています。

本ガイドは参考情報です。記載内容については、お客様の実情に応じて適切にご利用いただき、Tencent Cloud サービス利用時の規制コンプライアンス確保にご活用ください。

09 バージョン履歴

日付	バージョン	詳細
2026 年 4 月	V0.1	初版発行