



日本金融業界向け監督規制要件 コンプライアンスガイド

2026 年 4 月

【著作権表示】

©2013-2026 Tencent Cloud All Rights Reserved

本文書の著作権はテンセントクラウドが単独で所有し、テンセントクラウドの事前の書面による許可なく、いかなる主体も本文書の内容の全部または一部を複製、改変、盗用、伝播することはできません。

【商標に関する声明】

 腾讯云 およびその他の Tencent Cloud サービスに関連する商標は、すべて Tencent Cloud Computing (Beijing) Co., Ltd. およびその関連会社が所有しています。本文書に記載されている第三者の商標は、権利者に帰属します。

【サービスに関する声明】

本ドキュメントは参考情報として提供されるものです。テンセントクラウドは、本ドキュメントに含まれる情報について、明示的または黙示的な保証を行いません。本ドキュメントは現状に基づいて作成されています。本ドキュメントに含まれる情報および意見（URL やその他のインターネットサイトへの参照を含む）は、予告なく変更される可能性があります。ご利用はご自身の責任において行ってください。

本ファイルは、テンセント製品のいかなる知的財産権についても法的権利を付与するものではありません。お客様は、内部参照目的での使用に限り、本文書の内容を複製・使用することができます。

ここに記載されている一部の例は説明のためのものであり、架空のものです。これに基づいて事実上の関連性や関連性を推測または予測することはできません。

CONTENTS

01	概要	
02	Tencent Cloud セキュリティとプライバシー コンプライアンス	
2.1	国際的な権威ある認証	4
2.2	ISO/IEC システム認証	5
2.3	地域・業界認証	7
03	Tencent Cloud セキュリティ責任分担モデル	
04	Tencent Cloud グローバルインフラストラク チャ	
05	Tencent Cloud による『金融機関等コンピ ュータシステムの安全対策基準（第 13 版）』の遵守およびお客様の対応支援につい て	
5.1	制御基準	21
5.1.1	内部の統制	21
5.1.2	外部の統制	36
5.2	実務基準	52
5.2.1	情報セキュリティ	52
5.2.2	システム運用共通	83
5.2.3	運行管理	94
5.2.4	各種設備管理	108
5.2.5	緊急時の対応	120
5.2.6	システム開発・変更	127
5.2.7	システムの信頼性向上対策	133
5.2.8	個別業務・サービス等	152
5.3	設備基準	157
5.3.1	データセンター	157
5.4	監査基準	159
5.4.1	システム監査	159
06	Tencent Cloud による「金融分野における サイバーセキュリティに関するガイドライ	

ン」の遵守及びお客様の対応支援について

6.1 サイバーセキュリティ管理態勢の構築.....	163
6.2 サイバーセキュリティリスクの特定.....	169
6.3 サイバー攻撃の防御.....	181
6.4 サイバー攻撃の検知.....	207
6.5 サイバーインシデント対応及び復旧.....	210
6.6 サードパーティリスク管理	217

07 Tencent Cloud による「資金決済に関する法律」の遵守について**08 結び****09 バージョン履歴**

01

概要

近年、ネットワーク化を伴う新技術および新サービスの急速な発展により、日本の金融機関およびその関連事業者が運用する情報システムはますます複雑化しています。また、これらの事業者に対してクラウドサービスを提供する事業者やフィンテック（FinTech）関連企業の数も増加しています。

こうした変化は新たなリスクをもたらしています。一方では、サイバーセキュリティインシデントによって引き起こされる金融システムの停止が、より広範かつ深刻な影響を及ぼす可能性があります。他方では、金融機関が保有する顧客情報などの重要データを標的としたサイバー攻撃が、ますます高度化・大規模化する傾向を示しています。

広範な金融サービス利用者の利益を守り、金融システムの安定を維持するため、日本の金融庁（Financial Services Agency, FSA）および金融業界情報システムセンター（The Center for Financial Industry Information Systems, FISC）などの規制当局は、金融分野全体におけるサイバーセキュリティ強化を積極的に推進しています。そして、サイバーセキュリティに関連する複数の基準およびガイドラインを策定・公表し、金融機関に対して、規制当局の支援を受けながら十分なセキュリティ対策を講じ、自社のサイバーセキュリティおよび健全な事業運営を確保することを求めています。

テンセントクラウドは、日本の金融庁（Financial Services Agency, FSA）および金融業界情報システムセンター（The Center for Financial Industry Information Systems, FISC）の最新の規制要求を注視し、日本の金融機関のお客様がこれらを満たすよう支援することに尽力しています。本稿では、金融機関が特に注力している以下の規制基準およびガイドラインを対象に、テンセントクラウドがお客様のコンプライアンス対応をどのように支援するかを解説します。

財団法人金融情報システムセンター(The Center for Financial Industry Information Systems (FISC))

- [金融機関等コンピュータシステムの安全対策基準（第13版）](#)

金融庁 (Financial Service Agency, FSA) :

- [資金決済に関する法律](#)
- [金融分野におけるサイバーセキュリティに関する ガイドライン](#)

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 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。

サイバートラストマーク サイバートラストマーク (CTM) は、シンガポール政府のサイバーセキュリティ庁 (CSA) が導入した国家レベルのサイバーセキュリティ認定制度です。CTM フレームワークはリスクベースの手法を採用し、ガバナンス・リスクマネジメント、サイバーセキュリティ運用、レジリエンス (強靭性)、サプライチェーン・人事セキュリティ、持続的改善・ベストプラクティスの 4 つの核心分野にわたる 22 のサブドメインを対象に評価を実施します。

テンセントクラウドは、シンガポールサイバーセキュリティ庁より最高レベル (ティア 5) のサイバートラストマーク認定を取得しました。本認定は、テンセントクラウドがサイバーセキュリティガバナンス、リスクマネジメント、運用面でのレジリエンスにおいて高い実力を有することを証明し、アジア太平洋地域における規制対象業界および高需要業界において、信頼できるクラウドサービスプロバイダーとしての地位を確立しています。

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、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	
お客様の責任	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	異なるサービスへシナリオにおける共同責任
	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	
	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	Tencent Cloud の責任
	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	
	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 による『金融機関等コンピュータシステムの安全対策基準（第13版）』の遵守およびお客様の対応支援について

金融機関等コンピュータシステムの安全対策基準（第13版）は、日本の金融業界情報システムセンター（The Center for Financial Industry Information Systems, FISC）により、2025年3月21日に公表されました。本基準は、金融機関等の関係事業者がリスク指向型のアプローチに従い、セキュリティ対策を実施するための指針を提供することを目的としています。同基準は、セキュリティ対策の要求事項を体系的に4つのカテゴリーに整理しており、それぞれ異なる管理目標および適用シーンに対応しています。「制御基準」は、情報技術ガバナンスおよび管理体制の構築に関する要求を網羅しています。「実務基準」は、金融情報システムの信頼性および安全性の向上に焦点を当てています。「設備基準」は、コンピュータシステムが設置される建物および設備を、自然災害や不正行為などの脅威から保護するための要求を定めています。「監査基準」は、制御、実務および設備に関する施策に対する監査要求を明確化しています。本章では、『金融機関等コンピュータシステムの安全対策基準（第13版）』の中から、クラウドサービスプロバイダーに関連するセキュリティ対策基準を抽出・整理し、テンセントクラウドがクラウドサービスプロバイダーとして、金融機関等がこれらの要求を遵守するためにどのように支援できるかについて説明します。

5.1 制御基準

『金融機関等コンピュータシステムの安全対策基準（第13版）』における制御基準は、主に情報技術ガバナンスを実施するために構築された規程及び管理体系、並びにこれらが正しく運用され、効果的に機能しているかどうかを確認するためのモニタリング活動を含んでいます。制御基準は、組織内の管理に向けた内部管理と、委託先・外部委託先など他組織を管理するための外部管理に分類されます。

5.1.1 内部の統制

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
統 1	方針・計画	【基礎】システムの安全対策に係る重要事項を定めた規程を整備すること。	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

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
統 1-1	方針・計 画	【基礎】サイバーセキュリティ対策に関する基本方針を整備すること。	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、クラウドセキュリティ及び情報セキュリティに関する組織体制を整備し、異なる階層のセキュリティ職能役割及び関連責任を明確化しています。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。
統 1-2	方針・計 画	【基礎】サイバーセキュリティ対策に関する規程等及び業務プロセスを整備すること。	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 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。
統 4	組織体制	【基礎】セキュリティ管理体制を整備すること。	お客様は、安全管理体制を確立し、管理者、組織、責任範囲、権限等を明確にする必要があります。 お客様の規制要求への対応を支援するため、Tencent Cloud はクラウドセキュリティおよび情報セキュリティに関する組織体制を整備し、異なる階層のセキュリティ機能の役割と関連責任を明確化し、情報セキュリティ監査および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。Tencent は、セキュリティ技術委員会および異なる機能・分野に特化した専門セキュリティチームを設置し、内部において完全な人的資源管理基準と手順を確立し、職務要件に基づく人員の採用

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			と配置を保証しています。Tencent Cloud は業界経験豊富なエキスパートサービスチームを集結させ、お客様に安全、信頼、専門的かつコンプライアンスに適った製品とサービスを提供することに尽力しています。Tencent Cloud はまた情報セキュリティ連絡員を指名し、各地域の情報セキュリティ連絡員はコンプライアンスおよび業務要件に従い、現地規制当局およびお客様と円滑なコミュニケーションを維持し、Tencent Cloud が法令、規制、契約協定を遵守することを確実にしています。
統 4-1	組織体制	【基礎】サイバーセキュリティを管理するための経営資源及び人材に関する計画を策定すること。	お客様は、サイバーセキュリティの管理に必要な経営資源を適切に配分し、サイバーセキュリティ人材の管理及び育成計画を策定し、関連人員の配置、育成及び確保を行う必要があります。 お客様の規制要求への対応を支援するため、Tencent はセキュリティ技術委員会および異なる機能・分野に特化した専門セキュリティチームを設置し、内部において完全な人的資源管理基準と手順を確立し、職務要件に基づく人員の採用と配置を確保しています。 研修及び教育の面では、Tencent Cloud は内部に情報セキュリティ研修メカニズムを構築し、正社員、コンサルタント、インターン、外部委託従業員等に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。Tencent Cloud は、全員必須研修、重要職種向け専門研修、選択専門科目研修など、多様な研修コースを提供しており、内容は基礎的なセキュリティ意識、オフィスセキュリティ、脆弱性の識別と防御、プライバシー保護、緊急対応、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。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
統 5-1	組織体制	【基礎】サイバーセキュリティリスクを特定するため、情報資産を適切に管理すること。	お客様は、情報資産の全ライフサイクル（取得、利用、保管、廃棄）に関する管理手順を策定し、情報資産の重要度に基づく階層的な分類管理を実施し、台帳等のツールを用いて情報資産を管理し、情報資産の記録が適時に更新されることを確保する必要があります。 お客様の包括的な情報資産管理を支援するため、Cloud Workload Protection Platform (CWPP)を提供しており、資産フィンガープリントの自動収集をサポートし、アカウント、ポート、プロセス、アプリケーション等の資産フィンガープリントデータを統合管理します。CWPP はまた、資産フィンガープリントに基づき、発生したセキュリティインシデントのリスク影響範囲を迅速に調査することができ、お客様のサーバーセキュリティ向上に貢献します。お客様はさらに、Cloud Security Center (CSC) は資産セキュリティセンター機能を備えており、お客様がクラウドサーバー、オブジェクトストレージ、クラウドデータベース、ロードバランサー等を含むクラウド上の資産の自動動的な棚卸しを実現し、クラウド構成リスク、脆弱性、セキュリティインシデント等、複数のセキュリティ観点から資産セキュリティリスクを統一的に管理し、クラウド上の「シャドーIT」リスクを低減します。 お客様の規制要求への対応を支援するため、Tencent Cloud は内部において情報資産管理規範及び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、ソフトウェア等の資産について、分類・階層化による管理と保護を実施しています。Tencent Cloud は資産管理システムを通じ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			て、ハードウェア機器及びソフトウェアコンポーネントの管理（資産登録及び紐付け、資産棚卸し及び情報更新、資産退役及び交換等を含む）を行い、クラウドプラットフォームの基盤システムの安定した稼働を確保し、業務システムに対して信頼性の高いサポートを提供しています。
統 5-2	組織体制	【基礎】サイバーセキュリティリスクの特定・評価及びリスク対応計画を策定すること。	顧客は、自身に関連する脅威および脆弱性情報を収集・分析し、サイバーセキュリティに関連するリスクを特定し、リスクの影響度を評価し、リスク対応計画を策定するとともに、リスク管理措置の有効性を監視する必要があります。 Tencent Cloud は、顧客のリスク管理を支援するため、Cloud Security Center (CSC)を提供しています。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ある CSC は、ポートリスク、脆弱性リスク、弱いパスワードリスク、コンテンツリスク、クラウドリソース構成リスク、サービス露出の 6 大リスクを定期的に検出し、企業のセキュリティ状況を継続的に監視します。また、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取り込み、アラートログの監査、分析、集約、一元的な表示および追跡を行います。 Tencent はさらに、お客様に Tencent Security Threat Intelligence Center (TIX)を提供しています。ワンストップのインテリジェンスサービスプラットフォームとして、脅威インテリジェンスセンターは基礎インテリジェンス、攻撃面インテリジェンス、業務インテリジェンスの 3 大インテリジェンス機能を提供し、インテリジェンス検索、IOC（侵害指標）の判定・分析、攻撃面管理などの機能をサポートし

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ます。これにより、顧客がセキュリティインシデントをより効率的に分析・判定し、企業の資産の露出面におけるリスク状況をより包括的に評価できるよう支援し、企業が効率的な多層的なセキュリティ防御体系を構築することを後押しします。 お客様の規制要件への準拠を支援するため、Tencent Cloud は社内で情報セキュリティリスク管理手順を策定し、リスク管理の全プロセス（リスクの特定、リスク分析、リスク対応計画の策定、およびリスクの追跡・監視）における業務内容を明確に定義し、指針を示しています。Tencent Cloud は少なくとも年1回リスク評価を実施し、リスクシナリオや業務・製品・サービスのプロセス分析結果に基づいてリスクを特定します。特定されたリスクに対し、テンセントクラウドは各リスクの発生可能性と影響度を評価し、リスクレベルを分類した上で、適切な対応措置を講じ、記録に残します。また、テンセントクラウドはリスク対応状況を継続的に追跡し、残存リスクを評価することで、責任者がテンセントクラウドのリスク管理要件に従って適切にリスクを管理していることを確認します。さらに、テンセントクラウドはクラウド業界の動向や内部管理の実践に基づき、リスク評価手法およびリスク登録簿の維持・改訂を行っています。
統 5-3	組織体制	【基礎】ハードウェア・ソフトウェア等の脆弱性管理に関する手続き等を策定すること。 深刻度の高い脆弱性については、クラウド事業者を含むサードパーティが保有するシステムの脆弱性対応の管理を行うことが望ましい。なお、管理に当たっては、第三者保証による報告書や契約書等を活用することが考えられる。	顧客は、ハードウェア、ソフトウェア、およびその他のコンポーネントの脆弱性管理に関する手順を策定し、脆弱性が発見された際には、システムの重要度、リスクレベル、または脆弱性の深刻度に基づき、これらの手順に従って速やかに対応措置を講じなければならない。 お客様は、Cloud Workload Protection Platform (CWPP) を利用して、Linux ソフトウェアの脆弱性、Windows システムの脆弱性、Web-CMS の脆弱性、アプリケ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ーションの脆弱性を検出・リアルタイムでアラート通知し、脆弱性修正策を取得することで、脆弱性リスクに迅速に対応することができます。 Tencent Cloud Container Security Service (TCSS) は、頻発するゼロデイ脆弱性から保護するために Tencent Cloud Security が開発した仮想パッチシステムを統合しています。脆弱性を検知・分析し、Tencent の専門知識に基づいて仮想パッチを生成し、クラウドサーバー上で自動的に適用することで、ハッカーの攻撃を効果的に阻止します。さらに、お客様は Vulnerability Scanning Service (VSS) を通じて、企業の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、セキュリティ、コンプライアンスなどについて、定期的なセキュリティスキャン、継続的なリスク警告、脆弱性検出を行うことができます。また、VSS と連携して専門的な修正提案を提供し、企業のセキュリティリスクを低減します。 お客様の規制要件への準拠を支援するため、Tencent Cloud は内部の脆弱性スキャンメカニズムと外部の脆弱性収集プラットフォームを構築し、「脆弱性報奨プログラム」を実施しています。これにより、業界のセキュリティ専門家を招き、Tencent Cloud のシステムにおけるセキュリティ脆弱性やリスクの特定を支援しています。Tencent Cloud は脆弱性スキャンシステムを使用して、クラウド環境内のセキュリティ脆弱性を定期的にスキャンしています。スキャン範囲は仮想層、システム層、アプリケーション層をカバーし、スキャン完了後、Tencent Cloud のセキュリティチームは発見された脆弱性の分析、分類、および対応を実施します。検出されたセキュリティ上の脆弱性はチケットシステムに登録

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			され、規定時間内に適切に対処されることを保証します。さらに、Tencent Cloud はホスト端末検出ツールを使用してパッチのインストール状況を定期的にスキャンし、期限を過ぎてもパッチがインストールされていないマシンについてはチケットを記録します。 さらに、Tencent Cloud は毎年、独立した第三者機関による専門的な監査を受けており、証明的な性質を持つシステムおよび組織統制レポートを提供することで、クラウドユーザー機関、独立監査人、規制当局、会社の株主、およびその他の利害関係者に、Tencent Cloud の最新のサービス組織内部統制状況を公開しています。関連するコンプライアンス証明書やレポートが必要な場合は、または Tencent Cloud コンプライアンスドキュメントセンター を通じて申請およびダウンロードしてください。また、Tencent Cloud は国際版公式サイトにて、オンライン版の Service Terms 、 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ており、Tencent Cloud が提供するサービスの内容やサービスレベル、顧客と Tencent Cloud 双方のセキュリティに関する責任と義務などを明確に定めています。顧客は、Tencent Cloud と書面による契約を締結し、契約条項や細則を協議することも可能です。
統 5-4	組織体制	【基礎】サイバーセキュリティに関する演習・訓練を行うこと。	顧客は定期的にサイバーセキュリティ演習およびトレーニングを実施し、サイバー攻撃に対するインシデント対応計画および緊急対応計画の有効性を検証し、継続的に改善を行うものとする。 お客様は、セキュリティ演習の計画と実施

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			を支援するために、の Tencent Smart Advisor (TSA) サービスをご利用いただけます。本サービスは、複数の ITOM 分野における垂直アプリケーション向けのクラウドガバナンスプラットフォームであり、Tencent Cloud の膨大な運用保守専門家の経験に基づき、リスク点検や障害演習などの多角的なガバナンスを通じてクラウドインフラストラクチャを最適化します。TSA は、各種障害注入シナリオや多業界にわたる演習経験テンプレートを提供し、アベイラビリティゾーンを跨ぐ災害対策など、多くの典型的なユースケースをカバーしています。これにより、お客様は自社のビジネスニーズに応じて、成熟したソリューションを迅速かつ効率的に再利用し、システムの可用性を向上させることができます。お客様はさらに、Penetration Testing Service (PTS) を選択することも可能です。PTS は、膨大なユーザーをシミュレートした実際の業務シナリオを通じて、システムの可用性と安定性を包括的に検証します。 お客様の規制要件への準拠を支援するため、Tencent Cloud では社内で定期的にサイバーセキュリティ関連の研修や演習を実施しています。演習では、攻撃・防御の対抗や大規模障害など、実際の典型的な災害復旧シナリオをシミュレートすることが多く、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証し、突発的な事態が発生した際にも業務を迅速に正常化できるようにしています。Tencent Cloud は演習実施時に適切な安全対策を策定し、演習がサービスに悪影響を及ぼさないよう配慮します。演習終了後、関連部門が演習報告書を作成し、改善策に基づいて是正措置を講じた上で、報告書をアーカ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			イブとして保管します。 お客様が Tencent Cloud にサイバーセキュリティ演習への参加を希望される場合、Tencent Cloud は双方で共同実施する演習活動に積極的に協力いたします。
統 5-5	組織体制	【基礎】サイバーセキュリティに係る教育・研修を行うこと。	お客様は、サイバーセキュリティ教育および研修を実施し、職務や役割に応じて従業員のサイバーセキュリティ意識を高めるとともに、職務を遂行し、インシデント対応を行うために必要な知識とスキルを向上させる必要があります。 顧客が規制要件を遵守できるよう、テンセントクラウドは社内に充実した情報セキュリティ研修体制を構築し、正社員、コンサルタント、インターン、外部委託スタッフなどに情報セキュリティ研修の受講を義務付けています。テンセントクラウドは、全従業員必修研修、重点職務向け専門研修、選択制の専門コースなど、多様な研修コースを提供しており、その内容は基礎的なセキュリティ意識、オフィスセキュリティ、脆弱性の識別と防御、プライバシー保護、研究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。
統 8	組織体制	【基礎】ネットワーク管理体制を整備すること。	顧客は、コンピュータネットワークの適切かつ効率的な運用を確保し、不正アクセスなどを防止するために、ネットワーク管理プロセスおよび体制を確立する必要があります。 顧客がネットワークセキュリティを効果的に管理できるよう、テンセントクラウドは以下のサービスを提供しています： • Virtual Private Cloud (VPC) 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、仮想化技術を用いて異なるプライベートネットワーク間の完全な論理的分離を実現し、お客様に独立かつ隔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

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			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およびネットワーク ACL ルールを設定することで、インスタンスレベルおよびサブネットの入出力トラフィックを制御し、多層的な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 による能動的な制御、IPS によるリアルタイム遮断、仮想パッチ、悪意のあるコードの検出などの機能をサポートしており、さまざまなネットワーク境界における保護を提供します。 • Web Application Firewall (WAF) は、Web 攻撃、侵入、脆弱性悪用、マルウェア注入、改ざん、バックドア、クローラーなど、Web サイトおよび Web サービスのセキュリティ保護に関する課題への対応を支援します。 • Anti-DDoS 豊富で高品質な DDoS 防御リソースと、絶えず進化する「自社開発+AI による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 攻撃への対策を実現します。 • Flow Logs (FL) は、ネットワークトラフィックのリアルタイムかつ非侵襲的なバイパス収集、保存、分析をサポートし、障害調査、アーキテクチャの最適化、セキュリティ検査、コンプライアンス監査などの課題を解決します。 Tencent Cloud 内部においても、ネットワークセキュリティ管理規範および多層防御システムを確立しています。Tencent Cloud 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の管理・制御および防御基準、ならびに対応する役割と責任を明確化し、Tencent Cloud のネットワーク上で稼働する業務の安全な運用を確保しています。Tencent Cloud は成熟し

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			たネットワークセキュリティアーキテクチャを展開しており、ファイアウォール、侵入検知/防御システム (IDS/IPS)、DDoS 防御、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迅速に検知、フィルタリング、および阻止し、Tencent Cloud のネットワークセキュリティを保護しています。 ネットワーク機器の管理に関しては、テンセントクラウド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。さらに、Tencent Cloud の本番環境には「堡垒机 (Bastion Host)」が全面的に導入されており、これを通じてネットワーク機器に関連するアカウント権限を一元管理し、権限のない者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ています。内部運用担当者が堡垒机にアクセスするには承認・許可が必要であり、許可を得た内部運用担当者は、2 段階の本人確認を経てログインする必要があります。バックエンドの運用操作記録はすべてログプラットフォームに一元的に保存され、Tencent Cloud の内部監査チームが定期的に記録の監査を行っています。
統 10	組織体制	【基礎】防災組織を整備すること。	顧客は災害対応チームを設立し、関連責任者を明確にし、災害発生時に迅速に対応できるようにすること。 顧客の規制要件への準拠を支援するため、テンセントクラウドは緊急対応に関する手順を確立し、業務復旧プロセスにおける担当者の役割を定義し、復旧プロセスにおける職務分担を明確化しています。重要なスキルや役職については、テンセントクラウドは A/B 役の相互補完メカニズムを採

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			用し、定期的な緊急対応訓練を実施することで、復旧手順の迅速かつ効果的な実行を保証し、業務中断のシナリオにおいて顧客がタイムリーに復旧できるよう支援します。
			顧客は、不正侵入、危険物の持ち込み、資産の持ち出しなど、コンピュータシステムの安全を脅かす行為を防止するための防犯組織を整備し、犯罪発生時には迅速に対応し、その影響を最小限に抑える必要があります。
統 11	組織体制	【基礎】防犯組織を整備すること。	物理環境のセキュリティに関しては、テンセントクラウドは物理セキュリティ管理制度を策定し、運用セキュリティの規範化、リスクの迅速な特定、および物理セキュリティ管理の強化を図っています。テンセントクラウドは、日本地域に2つのレンタル型データセンターを展開しています。データセンターのレジリエンスと安全性を確保するため、テンセントクラウドはデータサプライヤーの選定、契約上の制約から継続的な監視に至るまでの全プロセスにおいて、厳格な管理体系を構築しています。 物理的アクセス管理に関しては、テンセントクラウドはオペレーターに対し、データセンターへの物理的アクセスについて正式なアクセス手順を設定し、データセンターに入場する人員の身元確認を行うとともに、携行物の検査と記録を行うことを求めています。また、テンセントクラウドはオペレーターに対し、機器のサーバールームへの搬入・搬出（設置・稼働、廃棄、移設など）について、承認および検査プロセスを設定することを求めています。 セキュリティおよび監視の面では、テンセントクラウドはデータセンター運営者の警備員に対し、巡回チェックリストと巡回

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			計画に基づき各サーバールームおよび設備の状態を厳格に巡回することを求めています。各チェックポイントで署名し、点検時間を記録するとともに、インフラの故障やセキュリティインシデントを発見した場合は、直ちにデータセンターの緊急対応プロセスを起動するよう求めています。また、テンセントクラウドは運営者に対し、データセンターに 24 時間 365 日死角のないビデオ監視アラートシステムを配備し、警備室が常駐して監視記録を十分な期間安全に保管することを求めています。
統 14	要員・教育	【基礎】セキュリティ教育を行うこと。	顧客は組織内でセキュリティポリシーを周知徹底し、担当業務の内容に応じて具体的なセキュリティ対策に関する教育・研修を実施する必要があります。 顧客が規制要件を遵守できるよう、テンセントクラウドは社内に充実した情報セキュリティ研修体制を構築しており、正社員、コンサルタント、インターン、外部委託スタッフなどに情報セキュリティ研修の受講を義務付けています。関連する研修コースには、全従業員必修研修、重点職務向け専門研修、選択制の専門コースなどが含まれ、その内容は基礎的なセキュリティ意識、オフィスセキュリティ、脆弱性の識別と防御、プライバシー保護、インシデント対応、研究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 の情報セキュリティおよび個人情報保護研修は、各事業部門を対象に年 1 回以上実施されており、従業員にはセキュリティポリシーおよび手順を年 1 回以上確認し、理解していることを義務付けています。
統 15	要員・教育	【基礎】要員に対するスキルアップ教育を行うこと。	顧客は、担当者が担う業務内容に基づき教育研修を実施し、システムおよびそれが支える業務に関連する知識とスキルを向上させるものとする。 Tencent Cloud 製品の基礎知識および関連

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			する専門能力に基づく トレーニングおよび認定を提供し、公式ウェブサイトを通じてクラウド製品の操作手順、ユーザーマニュアル等をお客様に提供することで、お客様の技術力とクラウドの習熟度向上を支援しています。 顧客が規制要件を遵守できるよう、テンセントクラウドは充実した研修体制を構築し、多様なキャリアパスを設定しています。また、従業員には豊富で質の高い学習リソースを提供し、研修カリキュラムと体系を継続的に最適化することで、従業員の個人の成長とキャリア開発を支援し、職務に関連する能力と資格を確実に備えるよう努めています。
統 16	要員・教育	【基礎】障害時・災害時に備えた教育・訓練を行うこと。	顧客は、システム障害および災害をテーマとして、コンピュータシステムの運用に関連する操作等について教育・訓練を行うものとする。 お客様が規制要件を順守できるよう支援するため、Tencent Cloud の内部関連部門は、シナリオに基づいたセキュリティインシデント対応計画に関する研修や演習を定期的実施しています。また、セキュリティ技術の進展や情勢に応じてセキュリティチームの従業員に対し技術研修を行い、関係者が最新のセキュリティ規定や運用手順を理解・遵守し、最新の情報セキュリティ基準やベストプラクティスを習得することで、セキュリティインシデント発生時に迅速かつ効果的に対応できるよう確保しています。
統 18	要員・教育	【基礎】要員の人事管理を行うこと。	顧客は適切な人員管理戦略を実施し、人員の配置、ローテーションなどの人事事項を管理する必要があります。 顧客の規制要件への準拠を支援するため、Tencent Cloud は異なる職能・分野の専門チームを設置し、充実した人事管理基準および手順を確立し、職務要件に基づいた人

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			材の選定、採用、配置を確実にしています。Tencent Cloud は業界のベテラン専門家からなるサービスチームを結集し、顧客に安全で信頼性が高く、専門的かつコンプライアンスに準拠した製品とサービスを提供することに尽力しています。

5.1.2 外部の統制

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
統 20	外部委託 管理	【基礎】外部委託を行う場合は、事前に目的、範囲等を明確にするとともに、外部委託先選定の手続きを明確にすること。 委託に際しては、外部委託先を客観的に評価すること。契約期間中にも、継続的に外部委託先を評価すること。	顧客が外部委託を実施する際は、委託業務の範囲、外部委託先のサービスの性質および利用方法に基づき、金融機関と委託先との間の責任分担を明確にし、これに基づき、外部委託先の資格、業務遂行能力、内部統制およびリスク管理の状況等について総合的に評価を行うものとする。契約期間中も、顧客は外部委託先を継続的に評価しなければならない。また、委託業務の全部または一部が再委託される場合、再委託業務の内容およびリスク特性に基づき、再委託先に対する評価プロセス、ならびに委託先が再委託先に下請けを委託することを許可するための承認手続きを明確にすること。 責任の分担に関して、Tencent Cloud は国際版公式サイトにおいてオンライン版の 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ており、Tencent Cloud が提供するサービスの内容およびサービスレベル、お客様と Tencent Cloud 双方のセキュリティ責任と義務などを明確に規定しています。お客様は、テンセントクラウドと書面による契約を締結し、契約条項や細則を協議することも可能です。また、お客様が異なるクラウドサービスカテゴリ (IaaS、PaaS、SaaS サービスなど) を選択した場合、各コ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ンポーネントに対する管理権限も異なることを考慮し、テンセントクラウドはクラウド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。詳細については、本ガイド の第3章「テンセントクラウドセキュリティ責任分担モデル」 をご参照ください。 サービスプロバイダーに対するお客様の評価に関して、Tencent Cloud は専任担当者を配置し、お客様の調査および評価のニーズに対応するとともに、お客様の要求に基づき、独立した第三者監査報告書や、証明的な性質を持つシステムおよび組織の統制報告書などの関連情報を提供します。以下は、クラウドサービスプロバイダーとしての Tencent Cloud のデューデリジェンスの各側面に関する概要です： リソースと規模： テンセントクラウドの運用能力および規模は、業界においてトップクラスです。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、欧州地域など、世界中の複数の地域に展開されています。 専門性と技術力： テンセントクラウドは、強力なクラウドコンピューティング技術、ビッグデータ処理能力、AI アプリケーション、サイバーセキュリティ対策、クラウドネイティブ技術、グローバルなデータセンター展開、および業界ソリューションを通じて、業界リーダーとしての包括的な技術力を発揮しています。これらの技術力は、テンセントクラウドサービスの安定性と信頼性を確保するだけでなく、お客様に安全で信頼性の高いクラウドコンピューティング環境を提供します。また、テンセントクラウドの充実した運用セキュリティ能力により、お客

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			様にクラウド製品に関する 24 時間 365 日の技術サポートを提供することが可能です。 • 事業継続と災害復旧: テンセントクラウドは、ISO/IEC 22301 ビジネス継続性マネジメントシステムの国際規格認証を取得しています。顧客のビジネスの継続的な可用性を保証するため、テンセントクラウドはクラウド製品向けに詳細な災害復旧計画を策定し、要件に厳格に従って定期的な演習を実施することで、災害復旧計画の適時性と実行可能性を確保しています。 • データセキュリティ: 顧客データは、テンセントクラウド内部において最高レベルのセキュリティが適用されるデータとして扱われます。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。テンセントクラウドは「データの機密性」の原則を厳守し、多層的な技術的隔離手段を通じて、あるテナントが他のテナントのデータにアクセス、取得、または改ざんできないことを保証します。テンセントクラウドの多数のストレージおよびデータベース製品は、データ暗号化機能をサポートしており、安全で高強度の暗号化アルゴリズムを使用することで、データの機密性を確保しています。 • リスク管理: テンセントクラウドは、ISO/IEC 27001:2022 規格に基づき、内部リスク管理フレームワークを開発・維持し、特定されたリスクの識別、分析、および管理を行っています。Tencent Cloud は、少なくとも年 1 回、正式なリスク評価を実施し、業界のセキュリティインシデント報告、Tencent Cloud の実践経験、専門機関のリスクデータベースなどの情報源を参考に、Tencent Cloud の製品およびサービスプロ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			セスにおけるリスクを特定します。 Tencent Cloud は、資産価値、リスク発生の可能性、リスクの影響度を評価し、リスクレベルを算出します。リスク分析の結果に基づき、特定されたリスクに対する対応戦略および適切な緩和策を提供し、リスクを許容可能なレベルまで低減します。 • 下請け管理: テンセントクラウドは、国際版公式サイトにて、オンライン版の 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ています。下請け処理のシナリオに対し、契約書では、下請けの事前の同意、下請け業者の追加または変更前の通知、データ保護義務などの条項を明確に定めています。Tencent Cloud は、顧客の事前の同意なしに、契約/合意に基づき顧客に代わって行ういかなる処理業務も下請けに出しません。下請け業者の追加または変更に関する予定変更については、Tencent Cloud は電子メール等の手段を通じて顧客に通知します。また、顧客は Tencent Cloud と別途書面による合意を締結し、合意の条項や詳細を定めることも可能です。 さらに、テンセントクラウドは、厳格なサプライヤーのセキュリティ評価および参入審査、定期的な監視と評価、明確なアウトソーシングサービス契約などの措置を通じて、サプライヤーに対する効果的な管理を確保する、充実したサプライチェーンセキュリティ管理体制を構築しています。 • 監査および評価: Tencent Cloud は、定期的に独立した第三者機関による専門的な監査を受けており、証明機能を備えたシステムおよび組織統制報告書を提供することで、クラウドユーザー企業、独立監査人、規制当局、株主、その他の利害関係者に、Tencent Cloud の

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			最新のサービス組織内部統制状況を公開しています。日本地域については、Tencent Cloud は『FISC 金融機関等コンピュータシステムセキュリティガイドライン』に基づき統制状況を評価し、それに基づいて適切なシステムおよび組織統制（SOC）報告書を作成しています。さらに、テンセントクラウドは、お客様が実施する監査や評価活動に積極的に対応し、協力いたします。 • サポートおよびメンテナンス体制: Tencent Cloud の各サービスのパフォーマンス指標、測定基準、および報告要件は、各製品のサービスレベル契約（SLA）に明記されており、Tencent Cloud の公式ウェブサイトで公開されています。テンセントクラウドは、クラウドサービスのパフォーマンスと可用性を継続的に追跡し、管理コンソールを通じてお客様にリアルタイムの監視機能を提供します。同時に、テンセントクラウドは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、お客様がセキュリティ、可用性、機密性に関連する障害、インシデント、問題、苦情を報告できるようサポートします。また、お客様が適切なサービスプランを選択し、専任サポートチーム、専任テクニカル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任サポートを受けられるよう支援します。 • 通知メカニズム: テンセントクラウドは、コミュニケーションおよび通知義務を履行するため、コンソール、公式サイト、電子メールなど、多様な連絡手段を提供しています。外部環境に影響を及ぼす可能性のある製品、インフラストラクチャ、およびネットワーク構成の変更については、テンセントクラウドは公告、電子メール、テンセントクラウドコンソール、および / またはその他の適切なチャネルを通じて、速やかに顧客に通知します。お客様のセキュリティに影響を及ぼす可能性のあるインシデントについては、

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
統 21	外部委託 管理	【基礎】外部委託先と安全対策に関する項目を盛り込んだ契約を締結すること。 【クラウドサービス利用時の留意事項】 - 金融機関は、クラウドサービスの利用に係る業務の重要性及びシステム再構築に要するコスト並びに人的負担に基づき、クラウドコンピューティングサービス提供者が自己の都合によりサービスを終了する場合の事前通知期間を、あらかじめ確認すること。 - 契約を通じて、クラウドサービス提供者に対し、外部委託のサービス範囲、外部委託先のセキュリティ対策及びその実施状況の開示を求めること、又は第三者保証報告書等により再委託管理の状況を確認することが推奨される。 - 第三者保証報告書等を活用し、	Tencent Cloud 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、内部審査を経た上で、インシデントの処理および分析結果を適切な方法でお客様に通知し、対応する技術サポートを提供します。 • 契約の終了: お客様が業務の変更または将来の IT 計画の都合により契約を終了する必要がある場合、いつでもクラウド上のデータおよび本番環境のバックアップおよび移行を行うことができます。お客様のクラウドサービスが終了した後、テンセントクラウドはお客様と締結したサービス契約に基づき、厳格なデータ消去手順に従い、保存期間満了後に複製やバックアップを含むお客様データを完全に削除します。削除されたデータは復元できません。
			顧客は、外部委託先と、セキュリティ対策、機密保護、システムの安定稼働などの条項を含む契約を締結し、サービスレベル契約 (SLA) などを通じてサービスレベルについて合意すべきである。 Tencent Cloud は、国際サイト公式サイトにて、オンライン版の 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ており、Tencent Cloud が提供するサービスの内容とサービスレベル、ユーザーデータおよび知的財産の保護、顧客と Tencent Cloud 双方のセキュリティ上の責任と義務、サービス期間および契約終了の条件などを明確に定めている。顧客は、Tencent Cloud とオフライン契約を締結し、契約条項および細則を協議することも可能である。 Tencent Cloud が顧客に提供するクラウドサービスは、各サービスで定めら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、

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		直接監査の実施に代えることも検討することができる。 - 重大な影響を及ぼす事象が発生した場合に、クラウドサービス提供者に対して詳細な報告を要求できるか否か、及び当該報告をもって現地調査の実施に代えることができるか否かを、事前に確認すること。 - 第三者保証報告書等により、データ削除の実施状況を確認することができる。	および報告要件は、各製品のサービスレベル契約に明記されており、Tencent Cloud の公式ウェブサイトに掲載されています。 下請け処理のシナリオについては、テンセントクラウドが国際サイト公式サイトで提供するデータプライバシーとセキュリティ契約、下請けに関する事前の同意、下請け業者の追加または変更前の通知、データ保護義務などの条項を明確にしています。顧客の事前の同意がない限り、テンセントクラウドは 契約/合意に基づき顧客に代わって実行するいかなる処理業務も下請けに出しません。下請け業者の追加または変更に関する予見可能な変更については、テンセントクラウドは電子メール等の手段を通じて顧客に通知します。さらに、下請け業者の管理に関しては、テンセントクラウドは完備されたサプライチェーンセキュリティ管理体制を構築しており、厳格なサプライヤーのセキュリティ評価および参入審査、定期的な監視と評価、明確なアウトソーシングサービス契約等の措置を通じて、サプライヤーを効果的に管理しています。 監査およびレビューに関しては、テンセントクラウドのセキュリティチームは年1回以上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および内部システムの状態を継続的に監視することで、良好なセキュリティ態勢を維持し、関連法規およびセキュリティ管理基準の規定と要件に準拠していることを確保しています。また、テンセントクラウドは毎年、独立した第三者による専門的な監査を受け、証明的な性質を持つシステムおよび組織的統制報告書を提供することで、クラウドユーザー機関、独立監査人、規制当局、株主、およびその他の利害関係者に、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
			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。日本地域に関しては、テンセントクラウドは『FISC 金融機関等コンピュータシステムセキュリティガイドライン』に基づき、管理状況を評価し、これに基づいて対応するシステムおよび組織統制 (SOC) 報告書を作成しています。さらに、テンセントクラウドは、顧客側から発せられる監査や評価活動に積極的に対応し、協力します。 インシデント報告および通知に関しては、 Tencent Cloud は、情報セキュリティインシデントの連絡と警告管理手順を制定し、重大なセキュリティインシデントおよび重大な業務停止シナリオにおける警告・通知メカニズムを明確化しています。これにより、影響を受ける内部関係者、顧客などの関係者に対し、迅速に告知および警告を行い、すべての関係者が秩序立てて、タイムリーかつ効率的に連携・調整を行う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、その影響範囲と程度に基づき、内部審査を経た上で、セキュリティインシデントの処理および分析結果を適切な方法で顧客に通知し、損失を最小限に抑えるための是正措置を講じられるよう、適切な技術サポートを提供します。 データの削除に関しては、お客様のサービス終了後、テンセントクラウドはお客様とのサービス契約に基づき、厳格なデータ消去手順に従い、保存期間満了後に複製やバックアップを含むお客様データを完全に削除します。削除されたデータは復元できません。
統 22	外部委託管理	【基礎】外部委託先の要員にルールを遵守させその遵守状況を確認すること。	顧客は、委託業務の内容および作業範囲に基づき、外部委託先の担当者にセキュリティポリシーを含む各種規則の遵守を求め、監査の実施や外部委託先からの定期的な

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		クラウド利用の場合、金融機関等においては一般的な外部委託と異なり、クラウド事業者が金融機関等が定めたルール等をそのまま遵守することを求めるのは困難なことがあるため、クラウド事業者が公開している情報をもとに実施している安全対策やその遵守状況について自社として許容可能なのかを確認することが必要である。確認に当たっては、第三者保証による報告書等の利用も考えられる。	業務報告の受領などの措置を通じて、外部委託先の遵守状況を確認しなければならない。また、顧客は、外部委託先の担当者へのアクセス権限を、委託業務の履行に不可欠な最小限の範囲に制限しなければならない。 顧客の監査および審査要件に対応するため、Tencent Cloud は専任の担当者を配置して支援を行い、顧客側から開始される監査または審査活動に積極的に対応します。同時に、Tencent Cloud のセキュリティチームは、少なくとも年1回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および内部システムの状態を継続的に監視することで、良好なセキュリティ態勢を維持し、関連する法令およびセキュリティ管理基準の規定と要件に準拠していることを確保しています。また、テンセントクラウドは定期的に独立した第三者による専門的な監査および評価を受けています。現在、テンセントクラウドは第三者による独立した監査または評価を通じて、多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や資格を取得しており、顧客のニーズに基づき、証明的な性質を持つシステムおよび組織統制レポートを提供することで、クラウドユーザー機関、独立監査人、規制当局、会社の株主、およびその他の利害関係者に、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。 特に日本地域を対象として、Tencent Cloud は『FISC 金融機関等のコンピュータシステムセキュリティガイドライン』に基づき、管理状況の評価を実施しました。これに基づき、Tencent Cloud プラットフォームの安全性、可用性、機密性に関連する管理項目を網羅したシステムおよび組織の管理 (SOC) 報告書を作成し、Tencent Cloud の関連措置が要件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に関する

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
統 23	外部委託 管理	【基礎】外部委託における管理体制を整備し、委託業務の遂行状況を確認すること。 クラウド利用の場合、金融機関等においてはクラウド事業者における業務の遂行状況の確認については、一般的な外部委託先と同じ方法をとることは困難なことがあるため、クラウド事業者が公開している情報をもとに、実施しているセキュリティ対策とその遵守状況、及び各サービスの稼働実績について、自社として許容可能であるかを確認することが必要である。確認に当たっては、第三者保証による報告書等の利用も考えられる。	る詳細については、の Tencent Cloud コンプライアンス」ページ をご参照ください。関連するコンプライアンス証明書や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。 顧客は外部委託管理体制 / サプライヤー管理体制を構築し、委託契約や合意書等に基づき、委託業務の履行状況を確認しなければならない。 Tencent Cloud が顧客に提供するクラウドサービスは、各サービスごとに定められた「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、評価基準、および報告要件は、各製品のサービスレベル契約に明記されており、Tencent Cloud の公式ウェブサイトに掲載されています。Tencent Cloud は、クラウドサービスのパフォーマンスと可用性を継続的に追跡し、管理コンソールを通じて顧客にリアルタイムの監視機能を提供します。さらに、Tencent Cloud は専任スタッフによる支援を提供し、顧客が実施する監査や審査活動に積極的に対応します。 お客様の外部委託管理要件に対応するため、Tencent Cloud Observability Platform (TCOP) は、クラウド製品 / クラウドリソースのリアルタイム監視、分析、アラート機能をサポートしています。Tencent Cloud のクラウド製品が自動的に報告する各種監視指標や、お客様が独自に設定して報告する監視指標を収集し、視覚化されたグラフで表示することで、お客様がクラウド製品の稼働状況やパフォーマンスをリアルタイムで把握できるよう支援します。また、指標に対するアラート設

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			定をサポートしており、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上の異常を速やかにお客様に通知します。 さらに、Tencent Cloud は、第三者による独立した監査や評価を通じて、ISO/IEC 27001、ISO/IEC 27017、ISO/IEC 27018、ISO 22301、NIST CSF、SOC など、多数のセキュリティおよびプライバシーに関するコンプライアンス認証や資格を取得しています。Tencent Cloud のコンプライアンスに関する詳細については、「Tencent Cloud コンプライアンス」ページ（リンク）をご参照ください。関連するコンプライアンス証明書や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」（リンク）から申請およびダウンロードしてください。
統 24	クラウドサービスの利用	【基礎】クラウドサービスを利用する場合は、クラウド サービス固有のリスクを考慮した安全対策を講ずること。 1. 特定システムでクラウドサービスを利用する場合、クラウド事業者の選定時やサービス利用期間において、適用される国内外の法令や評価制度等に留意するとともに、統制対象クラウド拠点（注）やデータを保管する国又は地域を把握する必要がある。また、統制対象クラウド拠点やデータ保管場所は、実質的な統制が可能となる国又は地域に所在することが必要である。なお、通常システムにおいては、利用するサービスの内容及びリスク特性等に応じて、これらの	お客様は、クラウドサービスを利用する際、クラウドサービス固有のリスクに対処するためのセキュリティ対策を講じる必要があります。お客様は、クラウドサービスを利用する際、適用される国内外の法令に留意し、クラウドノードおよびデータの保管場所を実質的な管理が可能な国または地域に設定する必要があります。 顧客が規制要件を遵守できるよう、Tencent Cloud のインフラは世界中の複数の場所に展開されており、リージョン（region）とアベイラビリティゾーン（zone）で構成されています。各リージョンは独立した地理的領域であり、各アベイラビリティゾーンは独立した障害復旧領域であり、各アベイラビリティゾーンは物理的に分離されています。顧客は、事業の発展ニーズやデータセキュリティ要件に応じて、データやシステムを異なるリージョンやアベイラビリティゾーンに自主的

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		対策を実施する必要がある。	かつ柔軟に配置することができます。 現在、テンセントクラウドは日本に2つのデータセンターを保有し、クラウドサーバー、クラウドデータベース、CDN など、多様なクラウドコンピューティングサービスを提供しています。日本の顧客は、日本国内でデータを保存・処理することを選択できます。 Tencent Cloud は、事業運営が行われる司法管轄区域の法令を厳格に遵守し、情報セキュリティの運用が関連する法律、法規、基準、および手順の要件を満たすよう、セキュリティコンプライアンスに関する手順を確立しています。さらに、Tencent Cloud は公開性と透明性の原則を堅持しており、お客様がデータの保存場所などの情報を知りたい場合、適切なチャネルを通じて速やかに関連情報を提供します。
		2. 特定システムにおいてクラウドサービスを利用する場合、金融機関等は、統制対象クラウド拠点に対して必要となる権利（監査権等）を確保するために、クラウド事業者と交わす契約書等にその権利を明記する必要がある。なお、通常システムにおいては、利用するサービス内容及びリスク特性等に応じて、この対策を実施する必要がある。	顧客はクラウドサービスを利用する際、第三者保証報告書等の活用を通じてクラウドサービスプロバイダーに対する監査および監視を実施し、クラウドサービスプロバイダーと締結する契約書等の文書に、かかる必要な権利を明確に規定する必要があります。 クラウドサービスプロバイダーである Tencent Cloud は、国際版公式サイトにて、オンライン版の 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ており、Tencent Cloud が提供するサービスの内容とサービスレベル、ユーザーデータおよび知的財産の保護、顧客と Tencent Cloud 双方のセキュリティに関する責任と義務、サービス期間および契約終了の条件などを明確に定めています。顧客は、Tencent Cloud とオフライン契約を締結し、契約条項や細則を協議することも可能です。
		3. クラウド事業者がその責任範囲において実施する安全対策についても、統制基準に沿って管理することが基本となるが、その際には実務基準を参考にしながら確認するものの、統制上の管理方法が制約される場合もあり、その場合は第三者保証による報告書等を利用するなどの方策を講ずることが考えられる。	
		4. 監査の実施に当たっては、技術の先進性を考慮し、クラウド	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		事業者が委託した保証型監査（又は同等の効力を有する監査）の報告書を利用することが望ましい。第三者保証による報告書等は、監査以外に、クラウド事業者の要員に対するルールの遵守状況、及び業務の遂行状況の確認についても利用できるが、。	お客様のアウトソーシング監査要件に対応するため、Tencent Cloud は専任の担当者を配置し、お客様が実施する監査や審査活動に積極的に協力いたします。また、Tencent Cloud は定期的に独立した第三者機関による専門的な監査を受けており、証明機能を備えたシステムおよび組織統制報告書を提供することで、クラウドユーザー企業、独立監査人、規制当局、株主、その他の利害関係者に、Tencent Cloud の最新のサービス組織内部統制状況を公開しています。
		5.特定システムにおいてクラウドサービスを利用する場合、定期的に監査を実施する必要がある。通常システムにおいても、定期的に監査を実施することが望ましい。	特に日本地域においては、テンセントクラウドは『FISC 金融機関等コンピュータシステムセキュリティガイドライン』に基づき、統制の現状を評価し、これに基づいて対応するシステムおよび組織統制（SOC）レポートを作成しています。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。
		6.特定システムにおいてクラウドサービスを利用する場合、クラウド事業者に対する監査及びモニタリングを実効的に実施するため、クラウド事業者において採用されている技術など専門知識を有する人材を配置する必要がある。通常システムにおいても配置することが望ましい。	顧客は、クラウドサービスの異なるモデルに基づき、クラウドサービスプロバイダーとの間の責任を明確にする必要がある。
		7.クラウドサービスの利用に当たっては、新しい技術によってサービス内容及び利用形態が変化する可能性があるため、検討時点から広義の IaaS、PaaS、SaaS 等のクラウドサービスの利用形態を考慮し、金融機関等とクラウド事業者との責任分界点を明確にしたうえで利用を開始する必要がある。	Tencent Cloud は、クラウドサービスの開放性と共有という特性を堅持し、クラウドプラットフォームおよび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、顧客と共にクラウド上の業務およびデータのための、より優れた、より完全なセキュリティ保証体制を構築します。Tencent Cloud はクラウドサービスプロバイダーとして、データセンターのインフラおよびクラウドプラットフォームのセキュリティに責任を負います。顧客が異なるクラウドサービスの種類（IaaS、PaaS、SaaS サービスなど）を選択する場合、各コンポーネントに対する制御権も異なることを考慮し、Tencent Cloud はクラウドサービスの種類に基づいてクラウドセキュ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			リティ責任分担モデルを確立しました。詳細については、本ガイド をご参照ください。
			顧客は、クラウドサービスプロバイダーがアクセス権限設定の変更前に通知を行うことを確認し、アクセス権限設定または組織内部の設定変更時には、設定の妥当性を確認する必要がある。 ユーザーがクラウドリソースの権限設定を行えるよう、Tencent Cloud は「Cloud Access Management (CAM)」を提供しています。CAM は、Tencent Cloud の製品およびリソースへのアクセスを安全かつきめ細かく管理し、リソースごとに異なるユーザーに特定の権限を付与することを支援します。また、Tencent Cloud は「Bastion Host (BH)」を提供しており、ユーザー、資産、アカウント、操作権限などの観点に基づいたきめ細かな権限付与をサポートします。さらに、CAM や BH などのクラウド製品のユーザーガイドや操作手順書は文書化されており、公式サイトを通じてお客様に提供されています。お客様は関連するガイドを参照して権限設定を行うことができます。 設定ミスを迅速に特定するため、Tencent Cloud はお客様にCloud Security Center (CSC)を提供しています。CSC は、クラウド製品の設定リスクに対する自動チェックと評価をサポートしており、クラウドサーバー、オブジェクトストレージ、クラウドデータベース、ロードバランサーなど、多種多様なクラウド製品をカバーしています。これにより、クラウド製品の使用における誤ったセキュリティ設定に起因するセキュリティリスクを低減し、クラウド
		8.クラウドサービスのアクセス権限に関する仕様変更や金融機関等の誤設定により、クラウド上に保管したデータが漏えいする可能性がある。このため、特定システムにおいてクラウドサービスを利用する場合、金融機関等は、クラウド事業者に対し、クラウドサービスのアクセス権限設定に関する仕様変更が事前に通知されることを確認する必要がある。また、クラウドサービスのアクセス権限設定の仕様変更や金融機関等における設定の変更時には、設定内容の妥当性を確認する必要がある。妥当性の確認においては、専門家によるシステム監査や誤設定の自動検知等の診断サービス（CSPM 等）。	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			上のセキュリティレベル全体を向上させることができます。また、お客様は Config を通じて、クラウドリソースの集中監査とガバナンスを実現できます。これにより、お客様アカウント下の異なるリージョンにおける各種クラウドリソースの設定情報や変更履歴を継続的に記録し、Tencent Cloud のベストプラクティスに基づくルールやコンプライアンスパッケージテンプレートに基づき、企業アカウント下のクラウドリソース設定に対して継続的なコンプライアンス評価を自動的に実施し、非準拠なリソース設定を特定することで、クラウドリソースの自動監視と管理を実現します。 外部環境に影響を及ぼす可能性のある製品、インフラストラクチャ、およびネットワーク構成の変更については、Tencent Cloud は公告、電子メール、Tencent Cloud コンソール、および / またはその他の適切なチャネルを通じてお客様に通知します。 アクセス権限管理に関しては、Tencent Cloud は社内で権限付与ポリシーおよび権限分離マトリックスメカニズムを策定し、役職・役割に対応する担当者の身元情報と各業務システムの権限レベルに関する記録を維持しています。Tencent Cloud は、定期的な内部権限監査を実施することで、権限の乱用や誤用がないことを確保しています。不要となったアクセス権限については、適切な措置を講じ、不必要なアクセス権限を速やかに取り消します。 さらに、顧客データは Tencent Cloud 内部において高セキュリティレベルのデータに分類されます。顧客は自身のデータ内容に対して唯一の所有権および管理権を有します。サービスの提供やトラブルシューティングの必要性がある場合、または顧客の明確な許可を得た場合、あるいは国家・地方政府機関による犯罪事件の調査など、国の法律・法規に準拠する場合を除き、

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
統 28	サイバー セキュ リティリ スク管 理	【基礎】サプライチェーンを考慮したサイバーセキュリティリスクを適切に管理すること。	Tencent Cloud の従業員が顧客データに自発的にアクセスすることは決してありません。
			顧客は、サプライチェーン全体を網羅するサイバーセキュリティ戦略を策定し、サードパーティを含むすべての業務プロセスをカバーするサイバーセキュリティ管理体制を構築すべきである。 Tencent Cloud が顧客に提供するクラウドサービスは、各サービスで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。各サービスのパフォーマンス指標、測定基準、およびレポート要件は、各製品の SLA に明記されており、Tencent Cloud の公式ウェブサイトに掲載されています。Tencent Cloud はクラウドサービスのパフォーマンスと可用性を継続的に追跡し、管理コンソールを通じて顧客にリアルタイムのモニタリングを提供します。 また、Tencent Cloud は、クラウド製品/クラウドリソースのリアルタイム監視、分析、アラート機能をサポートするため、<u>Tencent Cloud Observability Platform (TCOP)</u> を提供しています。TCOP は、Tencent Cloud のクラウド製品が自動的に報告する各種監視指標や、お客様が独自に設定して報告する監視指標を収集し、視覚的なグラフで表示します。これにより、お客様はクラウド製品の稼働状況やパフォーマンスをリアルタイムで把握できるほか、指標に対するアラート設定も可能です。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上の異常を速やかにお客様に通知します。 Tencent Cloud は専任スタッフによる支援を提供し、お客様から依頼された評価、監査、またはデューデリジェンスなどの活動に積極的に対応します。また、お客様の要求に基づき、独立した第三者監査報告書、あるいは証明的な性質を持つシステムお

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			および組織統制報告書を提供します。 下請業者管理に関しては、テンセントクラウドは社内に完備されたサプライチェーンセキュリティ管理体制を構築しており、厳格なサプライヤーセキュリティ評価と参入審査、定期的な監視・評価、および明確なアウトソーシングサービス契約などの措置を通じて、サプライヤーを効果的に管理しています。テンセントクラウドは下請業者と正式なサービス契約を締結し、セキュリティ、プライバシー保護、機密保持、コンプライアンスなどの責任と義務を明確に定めています。また、テンセントクラウドは下請業者のサービスレベルを継続的に監視し、下請業務が安全かつ安定して運営されることを確保します。テンセントクラウドは、契約で定められたセキュリティおよび運用基準に基づき、下請業者の提供レベルを定期的に評価し、発見された問題に対しては適切な是正措置を講じ、下請業者の提供が所定のセキュリティおよび品質要件を満たすことを確保します。

5.2 実務基準

5.2.1 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
実1	データ保護	【基礎】他人に暗証番号・パスワード等を知られないための対策を講ずること。 クラウド利用の場合、クラウド事業者に対して、金融機関等で策定したセキュリティ基準を充足しているかを確認することが必要である。確認する観点としては、以下の例がある。 (1)金融機関等が使用する管理インタフェース等について、クラウド事業者が実装する暗証番号・パス	顧客は、パスワードやパスコード等の漏洩を防止するための措置を講じる必要があります。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーが実施するパスワード・パスコードの漏洩防止対策がセキュリティ基準を満たしていることを確認する必要があります。 顧客が規制要件を遵守できるよう、Tencent Cloud はアクセス制御管理に関する手順を策定しており、これにはクラウド顧客アカウントのパスワード設定および保護に関する基準が含まれています。顧客がクラウドアカウントを登録する際、各ク

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		ワードの漏えい対策 (2) クラウドサービスの仕様によるパスワードの制限 (桁数、使用可能な文字種等) 金融機関等においては、上記の確認結果をもとに漏えい対策を検討し、不足する点があれば、対策を実施することが必要である。	クラウド顧客には一意に識別可能なアカウントが割り当てられ、パスワードの複雑さや長さなどを含むパスワード設定ルール / ポリシーが設定されます。顧客が管理コンソールにログインする際、ID および認証情報、ならびに操作コマンドは HTTPS プロトコルを介して送信されます。パスワードの漏洩を防ぐため、Tencent Cloud では顧客のパスワードに対して SHA256 ハッシュ化およびソルト処理を施し、平文での保存を回避しています。Tencent Cloud は、多要素認証を利用してアカウントへのログインや、パスワード変更などの機密性の高い操作のセキュリティを強化することをサポートしています。また、Tencent Cloud ではアカウントのパスワードリセットおよび変更機能も提供しています。 Tencent Cloud はさらに、Cloud Access Management (CAM) サービスを提供しており、お客様が Tencent Cloud の製品およびリソースへのアクセスを安全に管理できるよう支援しています。 Tencent Cloud 内部でも、セキュリティ基準に基づき、従業員アカウントに対してパスワードポリシー（パスワードの長さ、複雑さ、ロック、リセットなど）を設定しています。
実 3	データ保護	【付加】蓄積データの漏えい防止策を講ずること。 クラウド利用の場合、クラウド事業者に対して、金融機関等で策定したセキュリティ基準を充足しているかを確認することが必要である。確認する観点としては以下の例がある。 (1) クラウド事業者の暗号鍵のアクセス権の確認 (2) 暗号化設定の範囲や強度の確	顧客は、重要なデータに対してデータ保護対策を講じ、ファイルの不正な複製や盗難などによるデータ漏洩を防止しなければならない。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーの暗号化の範囲と強度、および暗号化鍵へのアクセス権限管理を確認する必要がある。 顧客データの機密性と完全性を確保するため、Tencent Cloud の多くのストレージおよびデータベース製品はデータ暗号化機能をサポートしており、安全で高強度の

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		認 金融機関等は、確認結果に基づき、暗号化措置を追加する必要性を評価すること。	暗号化アルゴリズムを使用しています。また、Key Management Service (KMS)を統合することで、鍵のライフサイクル全体を管理し、データの機密性を確保しています。 Key Management Service (KMS)は、FIPS-140-2 認証を取得したハードウェアセキュリティモジュール (HSM) を使用してキーを生成・保護し、お客様の暗号化キーのライフサイクル全体にわたる管理をサポートします。KMS は、鍵の転送や配布プロセスなどを暗号化して保護し、中間者攻撃による盗難を防止します。鍵の解読や悪用リスクを低減するため KMS は鍵のローテーションをサポートし、無効化、失効、または漏洩した鍵を安全かつ確実な方法で削除します。削除された鍵は復元不可能となり、その鍵で暗号化されたデータも復号できなくなります。 お客様の規制要件への準拠を支援するため、Tencent Cloud は暗号化および鍵管理基準を策定し、データ転送や保存の過程における暗号アルゴリズムの使用、あるいは鍵管理を行う際には、国際的な暗号管理ポリシーに準拠した暗号製品および暗号化アルゴリズムを選択すべきであることを明確にしています。
実 4	データ保護	【付加】伝送データの漏えい防止策を講ずること。 クラウド利用の場合、クラウド事業者に対して、データ伝送時における重要なデータの保護対策について確認することが必要である。金融機関等においては、上記の確認結果をもとにデータ伝送時における重要なデータのデータ保護の対策を講ずることが必要である。	顧客は、重要なデータの送信に対して、暗号化などの保護対策を講じ、送信中の盗聴などによるデータ漏洩を防止しなければならない。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーに対し、データ送信中の保護対策について確認しなければならない。 データ転送の保護に関して、顧客が Tencent Cloud コンソール上で行う通信はすべて HTTPS セキュリティプロトコルによる暗号化保護の対象となります。Tencent Cloud 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、ステータス監視などの

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			セキュリティ機能を備えており、顧客の業務に対してポートレベルの通信セキュリティを保証します。さらに、顧客は以下の Tencent Cloud サービスを利用して、さまざまなシナリオにおける安全なデータ転送を実現できます： <u>Virtual Private Cloud (VPC)</u> 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、仮想化技術を用いて異なるプライベートネットワーク間の完全な論理的分離を実現し、お客様に独立した、隔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およびネットワーク ACL ルールを設定することで、インスタンスレベルおよびサブネットの入出力トラフィックを制御し、多層的なネットワークアクセス制御を実現します。 <u>Direct Connect (DC)</u>：専用性と高いセキュリティを備えた大容量のネットワーク接続を提供します。ユーザーはネットワーク回線を独占利用するため、データ漏洩のリスクがありません。 <u>VPN Connection</u>：ネットワークトンネル技術に基づき、ローカルデータセンターと Tencent Cloud 上のリソースを接続する安全な転送を実現します。VPN チャンネルは IKE（鍵交換プロトコル）と IPsec を採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することで、転送中のデータの安全性を確保します。 お客様の規制要件への準拠を支援するため、Tencent Cloud はデータセキュリティの基準を策定し、採用すべき安全なデータ転送プロトコルおよび禁止される安全でないデータ転送プロトコルを明確化する

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ことで、転送中のデータ漏洩を防止しています。
			顧客は、データへの不正アクセスを防止するため、プログラムやファイルに対するアクセス制御、アクセス権限のチェックなどの機能を設定しなければならない。クラウドサービスを利用する際は、顧客はクラウドサービスプロバイダーが提供するアクセス制御機能がセキュリティ基準を満たしているかを確認しなければならない。
			Tencent Cloud コンソールは、 Cloud Access Management (CAM) を通じて、顧客に安全な権限割り当てとサブユーザー管理機能を提供し、ユーザーやロールが具体的にどのような操作を実行し、どのリソースにアクセスできるかを容易に制御できるように支援します。顧客は CAM を利用して、メインアカウントおよび所属するサブアカウントに対して二要素認証を有効にし、アカウントのセキュリティを強化することができます。また、 CloudAudit を活用することで、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ユーザーアクティビティや API の使用状況をログに記録し、継続的に監視・保存することができます。また、Tencent Cloud は Bastion Host (BH) を提供しており、ユーザー、資産、アカウント、操作権限などの次元に基づいたきめ細かな権限付与をサポートし、ユーザーが保有する権限が、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。バスタードマシンも同様に操作監査機能をサポートしており、ユーザーの操作ログを記録・分析するこ
実5	データ保護	【基礎】ファイルに対するアクセス制御機能を設けること。 クラウド利用の場合、クラウド事業者が提供するアクセス制御機能が、金融機関等で策定したセキュリティ基準を充足しているかを確認することが必要である。金融機関等においては、クラウドサービスの機能を使用してアクセス管理を行う場合は、上記の確認結果をもとにアクセス権限のチェック機能を設計・実装・運用することが必要である。	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			とで、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。 お客様の規制要件への準拠を支援するため、データアクセス保護の面において、Tencent Cloud は社内でアクセス制御管理規範を策定し、権限管理および承認メカニズムを確立しています。Tencent Cloud は最小権限の原則を厳格に遵守し、デフォルトで最小権限制御を実施しています。Tencent Cloud は、データ資産の完全性と業務サービスの信頼性を確保するため、データアクセス権限に対して全ノードでの実名制による審査とメンテナンスを実施しています。また、異常なデータアクセス行為を検知・阻止するためのリアルタイム監視および遮断メカニズムを構築しています。さらに、定期的な内部権限監査を実施することで、権限の乱用や誤用がないことを確実にしています。不要となったアクセス権限については、適切な措置を講じ、不必要なアクセス権限を速やかに取り消します。同時に、Tencent Cloud の本番環境には「堡垒机（フォートレス）」が全面的に導入されており、これを通じて Tencent Cloud のバックエンドシステムコンポーネントに対する管理者アカウントの権限を一元管理しています。堡垒机へのアクセスには承認が必要であり、特定の Tencent Cloud 内部の運用保守担当者だけがアクセス可能です。運用保守操作の記録はログプラットフォームに一元的に保存され、Tencent Cloud の内部監査チームが定期的にログの監査を行っています。
実 7	データ保護	【付加】伝送データの改ざん検知策を講ずること。 クラウド利用の場合、クラウド事業者に対して、伝送経路のうちクラウド事業者の範囲においてどのような改ざん防止策（漏えい防止策・改ざん検知策）を実施しているのかを確認することが必要であ	顧客は、重要データの転送において改ざん検知対策を講じるべきである。 データ転送の保護に関して、Tencent Cloud コンソール上での通信はすべて HTTPS セキュリティプロトコルによる暗号化保護の対象となります。Tencent Cloud 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、ステータス監視などのセキ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		る。金融機関等においては、金融機関等 (オンプレミス環境含む) とクラウドセンターの間の伝 送データの改ざん検知策を講ずることが望ましい。	セキュリティ機能を備えており、お客様の業務に対してポートレベルの通信セキュリティを保証します。 Tencent Cloud はデータセキュリティのベースラインを策定し、採用すべき安全なデータ転送プロトコルおよび禁止される安全でないデータ転送プロトコルを明確にしています。 さらに、お客様は以下の Tencent Cloud サービスを利用して、さまざまなシナリオにおける安全なデータ転送を実現できます： Cloud Connect Network (CCN)： クラウド上のプライベートネットワーク間 (VPC)、および VPC とオンプレミスデータセンター間 (IDC) の内部ネットワーク相互接続をサポートし、ネットワーク全体のマルチポイント相互接続、ルーティングの自己学習、リンクの最適化、障害時の迅速な収束などの機能を備えています。クラウド・コネクティビティ内のネットワークインスタンス間のすべての通信データはパブリック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性を備えています。また、多段階のリンク冗長化により通信品質を保証し、データの安全性と信頼性を確保します。 Direct Connect (DC)： 専用性と高いセキュリティを備えた大容量の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回線を独占するため、データ漏洩の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、ローカルデータセンターと Tencent Cloud 上のリソースを安全に接続します。VPN チャンネルは IKE (鍵交換プロトコル) と IPsec を採用し

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			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することで、転送中のデータの安全性を確保します。
			顧客は、業務内容や接続方法等に基づき、接続元の正当性を確認する必要があります。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーに対し、クラウドサービス特有の管理対象（管理インターフェースなど）において実装されている認証機能を確認する必要があります。
			Tencent Cloud は、 Cloud Access Management (CAM) を提供し、お客様が Tencent Cloud の製品およびリソースへのアクセスを安全かつきめ細かく管理できるよう支援しています。CAM は、MFA デバイスによる認証や携帯電話の認証コードによる認証など、さまざまな方式の二次認証機能をサポートしており、ログイン時や機密性の高い操作を行う前に、本人確認と環境の安全性を確認することができます。また、Tencent Cloud は Bastion Host (BH) を提供し、お客様のユーザー管理、権限管理、認証管理、および総合的な監査を支援します。バスタードマシンは、ユーザーの実際のシナリオのニーズに応じて、静的パスワードやLDAPなど、異なるユーザーに異なるタイプの認証方法を提供できます。セキュリティを強化するため、Tencent Cloud のバスタードマシンは二要素認証をサポートしています。
実 8	不正使用 防止	【基礎】本人確認機能を設けること。 クラウド利用の場合、クラウド事業者に対して、クラウドサービスの利用における固有の管理対象において実装されている本人確認機能を確認することが必要である。多要素認証を備えていることが望ましい。固有の管理対象の例として、管理インターフェースが挙げられる。金融機関等においては、上記で確認した管理対象について、本人確認機能を設定することが必要である。	お客様が Tencent Cloud の製品およびリソースへのアクセスを安全かつきめ細かく管理できるよう支援しています。CAM は、MFA デバイスによる認証や携帯電話の認証コードによる認証など、さまざまな方式の二次認証機能をサポートしており、ログイン時や機密性の高い操作を行う前に、本人確認と環境の安全性を確認することができます。また、Tencent Cloud は Bastion Host (BH) を提供し、お客様のユーザー管理、権限管理、認証管理、および総合的な監査を支援します。バスタードマシンは、ユーザーの実際のシナリオのニーズに応じて、静的パスワードやLDAPなど、異なるユーザーに異なるタイプの認証方法を提供できます。セキュリティを強化するため、Tencent Cloud のバスタードマシンは二要素認証をサポートしています。 お客様の規制要件への準拠を支援するため、Tencent Cloud 内部でもアクセス制御管理規範を策定しており、ユーザーアカウントには一意の識別子を使用することを義務付けています。また、セキュリティベースラインに基づき、従業員アカウントに対してパスワードポリシー（パスワードの

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			長さ、複雑さ、ロックアウト、リセットなど)を設定しています。Tencent Cloud 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アクセス認証を行い、ユーザーが内部リソースにアクセスするには、まず二要素認証を完了する必要があります。さらに、Tencent Cloud の本番環境にはすでにバスターディが全面的に導入されており、バスターディを通じて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的に管理しています。内部運用担当者がバスターディにアクセスするには承認が必要であり、承認された内部運用担当者のみが二次認証を経てログインすることができます。
実 9	不正使用防止	【基礎】ID の不正使用防止機能を設けること。 クラウド利用の場合、クラウド事業者に対して、クラウドサービスの利用における固有の ID を確認することが必要である。固有の ID の例として、クラウド事業者が提供する管理者アカウント等がある。金融機関等においては、上記で確認した ID について、不正使用防止策を講ずることが必要である。	顧客は、システムやデータ等へのアクセスに使用される ID が不正に使用されるのを防止するための対策を講じるべきである。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーに対し、クラウドサービスの利用において固有の ID を確認し、確認された ID に対して不正使用を防止する措置を講じるべきである。 クラウドユーザーのアクセス制御管理に関して、Tencent Cloud はアクセス制御管理に関する手順を策定しており、これにはクラウド顧客アカウントの登録、管理、およびサポートに関する基準が含まれている。Tencent Cloud は、クラウド顧客に対しアクセス制御管理機能を提供し、顧客が自らアクセス制御ポリシーを策定し、そのポリシーを通じて購入したクラウド製品へのアクセスを管理できるようにしている。 管理コンソールは、お客様がクラウドリソースを管理・制御するためのコントロールセンターです。お客様がクラウドアカウントを登録すると、各クラウドユーザーには一意の識別可能なアカウントが割り当てられ、パスワード設定のルールやポリシーが設定されます。管理コンソールは、ユーザーアカウント名の一意性を自動的に

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			チェックします。お客様が管理コンソールにログインする際、ID や認証情報、および操作コマンドは HTTPS プロトコルを介して送信されます。お客様は、公開 API を通じてクラウドサービスとデータを一元管理できます。お客様が Open API 機能に登録する際は、各お客様に割り当てられたアクセスキーを使用して認証を行う必要があります。Tencent Cloud は、多要素認証を活用して、アカウントへのログインやパスワード変更などの機密性の高い操作のセキュリティを強化することをサポートしています。また、Tencent Cloud では、アカウントのパスワードリセットおよび変更機能も提供しています。 顧客の規制要件への準拠を支援するため、Tencent Cloud 内部でもアクセス制御管理規範を策定しています。これに基づき、ユーザーアカウントには一意の識別子を使用することを義務付け、セキュリティ基準に従って従業員アカウントのパスワードポリシー（パスワードの長さ、複雑さ、ロック、リセットなど）を設定しています。また、社内の端末、オペレーティングシステム、アプリケーション、ネットワーク機器に対しては、ログイン失敗回数の制限およびセッションタイムアウトポリシーを設定しています。
実 10	不正使用防止	【基礎】アクセス履歴を管理すること。 クラウド利用の場合、クラウド事業者に対して、管理インターフェースへのアクセス履歴の管理について確認することが必要である。金融機関等においては、上記の確認結果をもとに管理インターフェースへのアクセス履歴を定期的にチェックして正当なアクセスであるかを調査することが必要である。 クラウド利用の場合、クラウド事業者に対して、使用しているタイ	顧客は、システムおよびデータへのアクセスログを取得し、監査証拠として必要な期間保存するとともに、定期的に確認を行うべきである。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーに対し、管理インターフェースのアクセスログの内容、保存期間、保護措置、提供方法および時期、ならびにプロバイダーが使用するタイムゾーンを確認し、アクセスログを定期的に確認すべきである。 アクセスおよび操作ログの収集と保存に関しては、お客様は、CloudAudit を利用して、Tencent Cloud アカウントの活動を

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		ムゾーンを確認することが望ましい。金融機関等において、この確認結果をもとに金融機関等のシステムとクラウドシステム間のタイムゾーンの相違等による時刻のずれに留意することが望ましい。また、複数リージョンにまたがりクラウドシステムを利用する場合、複数のタイムゾーンが混在することにも留意することが望ましい。	監視し、コンプライアンスチェック、操作レビュー、およびリスク審査を行うことができます。CloudAudit では、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、イベント日時、リクエスト ID、送信元 IP アドレス、ユーザー名を含む、過去 90 日以内の Tencent Cloud コンソールおよびクラウド API の操作記録をオンラインで閲覧できます。 Tencent Cloud はさらに、ログ管理を支援するためにお客様に 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 はログの収集、保存から検索・分析、リアルタイム処理、配信に至るまで多岐にわたるサービスをサポートし、業務運用、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。Tencent Cloud CLS は、高可用性を備えた分散アーキテクチャを採用しており、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しています。これにより、単一ノードのサービス停止によるデータ利用不能を防ぎ、サービスの高可用性を確保するとともに、ログデータに対して安定かつ信頼性の高いサービス保証を提供します。 タイムスタンプに関しては、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、正確な現在の世界標準時 (UTC) を表示します。テンセントクラウドは、クラウド上のインスタンスが利用できるよう、内部ネットワーク用 NTP サーバーを提供しています。テンセントクラウド以外のデバイスについては、お客様はテンセントクラウドが提供するパブリックネットワーク用 NTP サーバーを利用できます。さらに、テンセントクラウドの各データセンター

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			では、NTP サーバーの時刻同期状況を定期的にチェックしています。 お客様の規制要件への準拠を支援するため、Tencent Cloud は社内にログ収集および管理の規範と仕組みを確立しています。ログインログ、操作ログ、システムの通常ログ、システムセキュリティイベントログなどの記録、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やリスクを検知・防止します。ログは Tencent Cloud のログ管理プラットフォームに一元的に集約され、管理されます。また、バックアップおよび厳格な保護措置を講じ、不正な改ざんや削除を防ぐよう対策しています。
実 13	不正使用 防止	【付加】電子化された暗号鍵を蓄積する機器、媒体、又はそこに含まれるソフトウェアには、暗号鍵の保護機能を設けること。 クラウドサービスを利用するに当たり、金融機関等は、クラウドサービス提供者が提供する鍵管理服务について、以下の観点から確認を行う必要がある。暗号鍵の所有権は金融機関等に帰属し、クラウドサービス提供者は無断で使用してはならないこと。鍵の使用について、適切な権限設定、アクセス管理及び監査ログ出力機能を備えていること。 クラウド利用の場合、金融機関等においては、以下の観点で暗号鍵の管理を設計・実装・運用することが必要である。 (1)暗号鍵利用権限の付与は必要最小限の要員に限定し、それにより認証及びアクセス権限を設定する。 (2)すべての暗号鍵利用に対して監	顧客は、電子化された暗号鍵を保存する機器、媒体、またはソフトウェアに、鍵保護機能を設定しなければならない。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーに対し、暗号鍵の所有権、鍵の保存方法、鍵へのアクセス管理、鍵の操作および監査ログ機能などを確認し、鍵の使用権限を必要最小限の担当者にのみ付与するとともに、すべての鍵の使用行為を記録し、ログを維持しなければならない。 Tencent Cloud は、Key Management Service (KMS) お客様が暗号化キーのライフサイクル全体にわたる管理を実現できるよう支援します。これにより、キーの生成、保存、配布、インポート、エクスポート、使用、復元、アーカイブ、破棄といった一連の操作が安全な方法で実行され、キーの漏洩を防止します。 ユーザーマスターキー (Customer Master Key、CMK) は、KMS の中核となるリソースです。CMK はユーザーの第一階層のキーに属し、主に機密データの暗号化および復号化に使用されます。ユーザーは、KMS

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		査ログを出力し、そのログを適切に保全する。	の自動生成機能を使用して CMK を生成するか、または既存のキーをインポートして CMK を作成することができます。KMS は FIPS-140-2 認証を取得したハードウェアセキュリティモジュール (HSM) を使用して、ユーザー マスター キーを保護します。 ユーザーマスターキー (CMK) には、ユーザーキーとクラウド製品キーの2種類があります。ユーザーキーは、ユーザーがコンソールまたは API を通じて作成するユーザーマスターキーです。ユーザーは、ユーザーキーに対して作成、有効化、無効化、ローテーション、権限制御などの操作を行うことができます。一方、クラウド製品キーは、Tencent Cloud の製品/クラウドサービスがキー管理サービスを呼び出す際に、自動的にユーザーのために作成される CMK です。お客様は、クラウド製品キーの照会やキーローテーションの有効化操作を行うことができます。 CloudAudit サービスは、キー管理システムサービスの関連操作イベントを記録します。お客様は、クラウド監査コンソールにログインして、関連する操作記録を確認できます。 お客様の規制要件への準拠を支援するため、Tencent Cloud は社内にキー管理メカニズムを構築し、関連基準を策定して、キーの申請、生成、保存、使用、転送、更新、破棄などのプロセスを規範化しています。鍵のライフサイクルに関わる各操作については、二重管理、厳格な引継ぎ、適切な保管、適時の更新という基本要件を遵守し、権限と責任の分離、責任者の指定、厳格な承認、詳細な記録、実名操作といった規則を確立・履行しています。また、業務用鍵の操作ログを保持し、定期的に操作監査を実施しています。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 14	外部ネットワーク	【基礎】外部ネットワークからの不正侵入防止策を講ずること。 クラウド利用の場合、クラウド事業者に対して、クラウドサービスにおける不正侵入対策のうち、金融機関等が利用することがある対策について確認し、その結果をもとに金融機関側で追加の不正侵入対策を検討することが必要である。 クラウド利用の場合、クラウド事業者に対して、クラウドサービスで提供されるアクセス履歴の確認手段や、アクセス監視機能の仕様等について確認することが必要である。金融機関等においては、クラウド事業者が公開する脆弱性の情報を入手して評価し、対応を検討することが必要である。	顧客は、外部ネットワーク（オープンネットワーク、リモートアクセス等）と内部ネットワークの接続箇所において、適切な不正侵入防止措置を講じるべきである。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーに対し、当該クラウドサービスにおいて実施されている不正侵入防止措置を確認し、その結果に基づき、金融機関側で追加の防止措置を検討すべきである。また、顧客はクラウドサービスプロバイダーに対し、クラウドサービスが提供するアクセス履歴の確認手段や、アクセス監視機能の仕様についても確認すべきである。 ネットワーク境界の保護を実施するため、 Tencent Cloud は お客様に Cloud EdgeOne (EO) を提供しています。これは、Tencent のグローバルエッジノードに基づいてお客様にセキュリティ保護およびアクセラレーションサービスを提供し、DDoS 対策、インテリジェント Web 保護、BOT/クローラー型攻撃対策、DNS 解決などの機能を備え、お客様がビジネス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もサポートしています。その機能には、DDoS 攻撃対策、インテリジェント Web 保護、BOT/クローラー型攻撃対策、DNS 解決などが含まれ、お客様がビジネス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も可能です。また、お客様は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および DDoS 攻撃対策 (Anti-DDoS) などのネットワーク境界保護ツールを選択することもできます。 Cloud Firewall (CFW) は、主に異なるネットワーク境界における保護を提供します。ファイアウォール ACL による能動的な制御、IPS による

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			リアルタイム遮断、仮想パッチ、悪意のあるコードの検出などの機能をサポートしており、従来のネットワークにおける DMZ ゾーンの要件を実現し、コア資産を重点的に保護するとともに、VPC 間のきめ細かな分離管理を実現します。 Web Application Firewall (WAF) Web 攻撃、侵入、脆弱性悪用、マルウェア注入、改ざん、バックドア、クローラーなど、Web サイトおよび Web サービスのセキュリティ保護課題に対応します。 Anti-DDoS 豊富で高品質な DDoS 防御リソースと、継続的に進化する「自社開発+AI による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 攻撃に対処します。 また、お客様は Tencent Cloud が提供するサービスを利用して、購入済みのクラウドプラットフォームリソースに対して複数の独立したネットワーク空間を構築し、ネットワークセグメントの分割や IP アドレスの割り当て、ルーティングポリシーのカスタマイズなどを行うことができます。 VPC サービスは、Tencent Cloud 上に構築された専用のクラウドネットワーク空間です。プライベートネットワーク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、仮想化技術を用いて異なるプライベートネットワーク間の内部ネットワークを完全に分離することで、独立かつ隔離された安全なクラウドネットワークを顧客に提供します。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およびネットワーク ACL ルールを設定することで、インスタンスレベルおよびサブネットの入出力トラフィックを制御し、多層的なネットワークアクセス制御を実現できます。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			Tencent Cloud は、内部のネットワークセキュリティ保護と管理に関して、ネットワークセキュリティ管理規範および多層防御システムを確立しています。Tencent Cloud 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の管理・制御および保護基準、ならびに対応する役割と責任を明確化し、Tencent Cloud のネットワーク上で稼働する業務の安全な運用を確保しています。同時に、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区分し、異なるセキュリティドメインを物理的または論理的に分離することで、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 防御、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迅速に検知、フィルタリング、および阻止し、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ています。 ログ管理に関しては、Cloud Firewall (CFW) が全トラフィックのネットワークログ分析をサポートしており、最大 6 ヶ月間保存可能です。また、高度な脅威の追跡分析をサポートし、ドメイン名の登録、解決、届出および過去の解決情報を分析できます。また、お客様は Cloud Log Service (CLS) をご利用いただけます。このサービスはワンストップのログサービスプラットフォームであり、ログの収集、保存から検索・分析、リアルタイム利用、配信に至るまで多岐にわたるサービスを

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			提供し、業務運用、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。さらに、Cloud Security Center (CSC) は、クラウドセキュリティ製品のアラートデータ、クラウド資産の構成変更データ、クラウド上のユーザー操作行動データ、および一部のクラウド製品のログデータなど、クラウド上のセキュリティ関連データを統一的に収集し、統一的な検索・調査プラットフォームを提供することで、お客様が包括的なクラウドログ監査と検索・調査を実現できるよう支援します。 また、Tencent Cloud はログ収集・管理の規範と仕組みを確立し、ログインログ、操作ログ、システムの通常ログ、システムセキュリティイベントログなどの記録、抽出、保存、保護、分析、監査などを管理・統制することで、システム活動の異常やリスクを検知・防止しています。ログは Tencent Cloud のログ管理プラットフォームに一元的に集約・管理され、関連するログ情報に対してはバックアップおよび厳格な保護措置を講じ、不正な改ざんや削除を防止しています。バックアップログの保存期間は1年以上です。Tencent Cloud は運用セキュリティ自動化監査ツールおよび内部監査チームを通じてログを監査し、システムや操作の異常を検知することで、操作リスクを防止しています。 脆弱性情報の開示については、Tencent Cloud は脆弱性の存在を確認した後、顧客の業務への影響度を評価し、チーム内部での審査を経て、速やかに公式ウェブサイトでの告知やサイト内メッセージを通じて顧客に通知します。通知内容には、脆弱性の概要、影響範囲および程度、Tencent Cloud が講じた対策、顧客への修正提案および具体的な操作手順などが含まれますが、これらに限定されません。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 14-1	外部ネット	【基礎】サイバー攻撃の端緒を検知するための監視・分析などの対策を講ずること。	お客様は、監視、分析、および報告に関する手順を策定し、サイバー攻撃の脅威レベルに応じて、攻撃を検知するために必要な監視や分析などの措置を講じる必要があります。また、データセンターやサーバールームへの出入状況および異常な活動について、継続的な監視を行う必要があります。 お客様は、の Cloud Security Center (CSC) を利用し、そのアセットセンター、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機能を通じて、事前の脅威検知、事中の対応・処置、事後の原因追跡分析というセキュリティ運用の閉ループを実現できます。クラウドセキュリティセンターは、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、クラウドリソース構成リスク、サービス露出の 6 大リスクを定期的に検出し、企業のセキュリティ状況を継続的に監視します。また、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的に取り込み、アラートログの監査、分析、集約、一元的な表示および追跡を行います。 ネットワークの監視と保護に関しては、お客様はFlow Logs (FL) を選択して利用することで、ネットワークトラフィックのリアルタイムかつ非侵襲的なサイドキャプチャ、保存、分析を実現し、障害調査、アーキテクチャ最適化、セキュリティ検出、コンプライアンス監査などの課題を解決することができます。また、Tencent Cloud はCloud EdgeOne (EO) を提供しています。これは Tencent のグローバルエッジノードを基盤として、お客様にセキュリティ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			イ保護およびアクセラレーションサービスを提供するもので、DDoS 防御、インテリジェント Web 防御、ボット/クローラー攻撃防御、DNS 解決などの機能を備えており、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も可能です。さらに、お客様は Anti-DDoS サービスを利用して、DDoS 攻撃のリスクを防ぐことができます。本サービスは、豊富で高品質な DDoS 防御リソースと、継続的に進化する「自社開発 + AI によるインテリジェント識別」洗浄アルゴリズムを組み合わせることで、DDoS 攻撃に対処し、お客様のビジネスの安定的かつ安全な運用を保証します。 お客様の規制要件への準拠を支援するため、Tencent Cloud は社内にネットワーク監視システムを導入し、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・アラートしています。また、権限制御や承認プロセスなどの多重措置を通じて、権限のない者による内部ネットワークリソースへのアクセスを厳格に禁止しています。Tencent Cloud はエンドポイント検出および対応 (EDR) ツールを導入し、ネットワーク全体のサーバー端末資産に対して包括的な監視と管理を行っています。Tencent Cloud が採用する EDR ツールは、ウイルス対策および侵入検知、セキュリティベースラインと脆弱性スキャン、ならびにコマンド操作や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ており、悪意のあるプログラムや異常な行動を検知した際にアラートを発動します。Tencent Cloud はチケットシステムを通じて、検知されたセキュリティ問題を追跡・解決します。 データセンターの監視に関しては、テンセントクラウドはデータセンター運営事業

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			者に対し、データセンターに 24 時間 365 日死角のないビデオ監視アラートシステムを配備し、警備室での常駐体制を整えることを義務付けており、同時に監視記録が十分な期間安全に保存されることを確保しています。
			顧客は、システムのセキュリティ上の脆弱性や問題を特定し、改善するために、脆弱性スキャンおよびペネトレーションテストを実施する必要があります。
			ペネトレーションテストに関しては、
			Tencent Cloud は Penetration Testing Service (PTS) を提供しています。これは、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、制御可能かつ非破壊的な手法を用いて対象システムのセキュリティを詳細に調査します。これにより、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言を通じてシステムの安全性向上を支援するとともに、脆弱性修正後の検証もサポートします。
実 14-2	外部ネット	【基礎】脆弱性診断及びペネトレーションテストを行うこと。	脆弱性スキャンに関しては、お客様は Vulnerability Scanning Service (VSS) を利用して、企業のネットワーク資産を調査し、そのリスクを特定することができます。テンセントが長年にわたり蓄積してきたセキュリティ経験と脅威インテリジェンスに基づき、VSS は豊富かつ包括的な脆弱性ルールベースを構築し、専門的かつ効率的な 0Day/1Day/NDay 脆弱性検出機能を備えています。これにより、お客様の資産の可用性、セキュリティ、コンプライアンスなどに対して、定期的なセキュリティスキャン、継続的なリスク警告、脆弱性検出を実施し、専門的な修正提案を提供することで、セキュリティリスクを低減します。また、VSS はホストセキュリティや

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			Web アプリケーションファイアウォールなどのクラウド製品との連携をサポートし、リスク監視からリスク対応までの閉ループを実現します。 お客様の規制要件への準拠を支援するため、Tencent Cloud は社内で定期的な脆弱性スキャンおよびペネトレーションテストの仕組みを確立しています。 Tencent Cloud 内部の脆弱性スキャンには通常、Web 脆弱性、コンポーネント脆弱性、設定スキャンなどが含まれます。脆弱性スキャンシステムを通じて自動的にスキャンタスクを生成し、クラウド環境内の資産に対して脆弱性スキャンを実施するとともに、発見された脆弱性の分析、分類、および修正処理を行います。ペネトレーションテストに関しては、Tencent Cloud のセキュリティチームが定期的にエンドツーエンドの大規模なペネトレーションテストを実施しており、新製品のリリース前や重大な変更時などには、状況に応じて柔軟に絞ったペネトレーションテストを実施しています。テスト結果はセキュリティチケットを通じて関連責任部門に通知され、責任部門が速やかに脆弱性の修正やその他の是正措置を実施することで、ペネトレーションテストで発見された悪用可能な脆弱性が適切に処理されることを保証します。さらに、Tencent Cloud では定期的にレッドチーム対ブルーチームの対抗演習を行い、ネットワーク攻撃への防御を実戦形式でシミュレートしています。
実 15	外部ネットワーク	【基礎】外部ネットワークからアクセス可能な接続機器は必要最小限にすること。 クラウド利用の場合、クラウド事業者に対して、管理インタフェースに対するアクセス経路について提供方式 (GUI、CLI、API) ごとに接続元 IP アドレスを制限するこ	顧客は、不正アクセスを防止するため、外部からアクセス可能な通信経路や通信関連機器などを必要最小限に制限すべきである。 Tencent Cloud API は、Tencent Cloud 製品の各種リソースへのインターフェースを提供しており、顧客は TencentCloud

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		と等が可能か確認することが必要である。金融機関等においては、上記の確認結果をもとに管理インターフェースの提供方式ごとにアクセス経路を必要最小限にすることが望ましい。	API を通じて、クラウド製品を迅速に操作できます。顧客のアクセス保護を支援するため、Tencent Cloud が提供するクラウド API は HTTPS による通信暗号化をサポートし、複数の SDK 署名メカニズム (PHP、Python、Java、.Net、Node.js など) を通じてインターフェースの認証を行い、タイムスタンプ (Timestamp) を利用してリクエスト署名の有効期限を制限することでリプレイ攻撃を防止し、署名の暗号化もサポートしています。Tencent Cloud は、クラウド API の監視管理機能を統合しており、お客様はコンソールを通じて業務に必要な API インターフェースの状態監視を設定できます。同時に、Tencent Cloud は API インターフェースの保護機能を提供しており、クラウド API の無効化や悪用リスクを効果的に排除します。 お客様はさらに、Tencent Cloud が提供する Virtual Private Cloud (VPC) サービスを利用して、ご購入いただいたクラウドプラットフォームリソースに対して複数の独立したネットワーク空間を構築し、セグメント分割や IP アドレスのカスタマイズ、ルーティングポリシーの定義などを独自に設定することが可能です。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およびネットワーク ACL (Access Control List) ルールの設定を通じて、インスタンスレベルおよびサブネットレベルでの送受信トラフィックの制御を実現し、異なるレベルのネットワークアクセス制御を実現できます。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やネットワーク ACL ルールを設定することで、インスタンスレベルおよびサブネットレベルでの入出トラフィックを制御し、多層的なネットワークアクセス制御を実現できます。また、Tencent Cloud は

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			<u>Cloud Firewall (CFW)</u> を提供し、顧客によるインバウンドおよびアウトバウンドのアクセスフィルタリングをサポートしています。CFW のアクセス制御ルールは、ドメイン名フィルタリングや地理的位置に基づくトラフィックフィルタリングに対応しており、重要な資産の重点的な保護を実現できます。さらに、<u>Cloud</u> <u>EdgeOne (EO)</u> は、テンセントのグローバルエッジノードを基盤として、セキュリティ保護と高速化サービスを提供します。DDoS 防御 インテリジェント Web 保護 ポット/クローラー攻撃防御、DNS 解決などの機能を備え、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も可能です。 顧客の規制要件への準拠を支援するため、Tencent Cloud は成熟したネットワークセキュリティアーキテクチャを展開しています。ファイアウォール、侵入検知・防御システム (IDS/IPS)、DDoS 防御、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迅速に検知、フィルタリング、および阻止し、Tencent Cloud のネットワークセキュリティを保護します。Tencent Cloud のセキュリティチームは、ルーター、ファイアウォール、Web サーバーなどのネットワーク機器のセキュリティポリシーやパラメータ設定を定期的にレビューし、その有効性を確保しています。
実 16	不正検知策	【基礎】不正アクセスの監視機能を設けること。 クラウド利用の場合、クラウド事業者に対して、インターネット経由の不正アクセス監視についてクラウド事業者とクラウド利用者そ	顧客は、アクセス失敗および不正アクセスを監視する必要があります。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーと、不正アクセス監視に関する双方の責任範囲、およびクラウドサービスプロバイダーが提供可能な具体的な措置について確認する必要があります。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		それぞれの責任範囲を確認する。そのうえで、クラウド事業者における対応等について確認することが必要である。確認する観点としては、以下の例がある。 (1) 不正アクセスの監視対象とする機器及び資源 (2) 不正アクセスの検知時の利用者への通知 (3) 連続してアクセスに失敗したID の利用停止 (4) 外部事業者が提供する不正アクセス監視のためのツール等を導入する場合の条件や制約金融機関等においては、上記の確認結果をもとにインターネット経由の不正アクセスを監視することが必要である。また、アクセス権限の種類に不足がある場合には、ツールの導入等により機能を補うことが考えられる。	Tencent Cloud コンソールは、Cloud Access Management (CAM) を通じて、顧客に安全な権限割り当てとサブユーザー管理を提供し、ユーザーやロールが具体的にどの操作を実行し、どのリソースにアクセスできるかを容易に制御できるよう支援します。顧客は CAM を通じて、メインアカウントおよび所属するサブアカウントに対して二段階認証を有効化し、アカウントのセキュリティを強化できます。また、CloudAudit を活用して、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ユーザーアクティビティやAPIの使用状況を記録 継続的に監視および保持することができます。 また、Tencent Cloud は Cloud Log Service (CLS) を提供しており、1 つまたは複数のログトピックに対してアラートポリシーを設定できます。アラートポリシーは定期的に監視タスクを実行し、クエリ分析結果がトリガー条件を満たした場合にアラート通知を送信するため、お客様は異常を迅速に発見できます。 お客様は、Data Security Audit (DSA) を利用して、データに対する異常な操作を監視することができます。DSA は、人工知能 (AI) を基盤とした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おける各種セッション情報、アクセス操作、SQL 文の全量監査と記録をサポートしています。多様なルールベースと脅威検知エンジンに基づき、操作中の悪意ある行為を識別し、管理者に速やかに通知して適切なセキュリティ対策を講じてもらいます。また、発生済みのセキュリティインシデントに対して

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			は、数年にわたるログの監査と分析もサポートしており、インシデントの全容を再現し、責任者の特定を行うための参考資料を提供します。 クラウドサービスプロバイダーとして、Tencent Cloud は主にデータセンターの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ています。Tencent Cloud は国際サイトの公式サイト上で、オンライン版の 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ており、Tencent Cloud が提供するサービスの内容とサービスレベル、ユーザーデータおよび知的財産の保護、顧客と Tencent Cloud 双方のセキュリティ上の責任と義務、サービス期間と契約終了のシナリオ、紛争解決メカニズム、通知メカニズムなどを明確に定めています。お客様は、テンセントクラウドと書面による契約を締結し、契約条項や細則を協議することも可能です。さらに、お客様が異なるクラウドサービスカテゴリ (IaaS、PaaS、SaaS サービスなど) を選択した場合、各コンポーネントに対する管理権限も異なることを考慮し、テンセントクラウドはクラウド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。詳細については、本ガイド をご参照ください。 Tencent Cloud はアクセス制御管理規範を策定し、アクセス権限の管理要件および関連する承認メカニズムを明確にしています。Tencent Cloud は、すべてのユーザーアカウントに一意的識別子を使用することを義務付けており、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アクセス認証を行っています。Tencent Cloud は従業員アカウントのログイン状

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			態に対し、リアルタイムのセキュリティ監視を実施しており、異常なログイン行動が検出された場合、IT セキュリティシステムは直ちにアカウント所有者に連絡して確認・対応を行うとともに、関連事象を詳細に記録します。 内部の端末、オペレーティングシステム、アプリケーション、およびネットワーク機器に対し、テンセントクラウドはログイン失敗回数制限とセッションタイムアウトポリシーを設定し、不正アクセスに対してはログイン制限ポリシーを設定することで、不正アクセスを効果的に監視・警告しています。
実 19	不正発生時の対応策	【基礎】不正アクセスの発生に備えて対応策、復旧策を講じておくこと。 クラウド利用の場合、クラウド事業者に対して、不正アクセスの拡大防止のための対応策、復旧策について、クラウド事業者とクラウド利用者との間の責任範囲を確認することが必要である。クラウド事業者が実施する対応については、以下の例がある。 (1) クラウド事業者が実施する不正アクセスの拡大防止のための対応策。 (2) クラウド事業者が提供する不正アクセスに関する復旧策 金融機関等においては、上記の確認結果をもとに不正アクセス発生時の対応策、復旧策を講ずることが必要である。なお、クラウド事業者による対応策に不足がある場合には、ツールの導入等により機能を補うことが考えられる。	顧客は、不正アクセスへの対応措置および復旧プロセスを明確にすべきである。不正アクセスが発生した場合、顧客は原因を分析した上で、同様の事態が再発しないよう対策を講じる必要がある。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーと、不正アクセスの防止および復旧に関する双方の責任範囲、ならびにクラウドサービスプロバイダーが顧客に提供できる不正アクセスの拡大防止措置および関連する復旧対策 / サービスについて確認すべきである。 顧客によるインシデントの検知と迅速な対応を支援するため、Tencent Cloud はワンストップセキュリティ管理プラットフォーム および Cloud Security Center (CSC) を提供している。これらを通じて、資産管理センター、リスク管理センター、アラートセンター、高度なセキュリティ管理などの機能により、顧客が事前の脅威検知、事中の対応・処置、事後の原因追跡分析というセキュリティ運用の閉ループを実現し、セキュリティ運用の効率を向上させることを支援する。 インシデントへの対応と処理に関しては、

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			テンセントクラウドは社内で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、処理のメカニズムおよび関連プロセスを確立するとともに、社内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ています。検知・特定されたセキュリティインシデントに対し、テンセントクラウドはインシデントの性質、データの機密性、影響範囲などの要因を総合的に考慮して分析・分類を行い、速やかに担当責任者に通知してインシデントの処理を進めます。テンセントクラウドは定期的なインシデント分析メカニズムを確立しており、インシデントについて多角的な分析（インシデントの種類、発生頻度、影響範囲、深刻度）を定期的の実施しています。また、インシデントの振り返りと根本原因分析に基づき予防措置を講じ、同様のインシデントの再発を防止しています。 お客様のビジネスの継続的な可用性を確保するため、Tencent Cloud はクラウド製品および重要なプロセスに対して詳細な災害復旧計画を策定し、要件に厳格に従って定期的な演習を実施することで、その計画の適時性と実行可能性を保証しています。また、事業継続管理および災害復旧の分野において、Tencent Cloud は ISO/IEC 22301 事業継続マネジメントシステムの国際規格認証を取得しています。テンセントクラウドは包括的な事業継続マネジメントシステムを構築し、事業継続管理に関連するプロセスを標準化しています。これには、事業影響度分析、事業継続計画、緊急対応および災害復旧、緊急演習とテスト、危機管理などの側面が含まれます。また、災害発生時の内部・外部の連絡方針を明確にし、連絡先リストを整備しています。テンセントクラウドは毎年、事業影響度分析の結果に基づき災害復旧計画を見直し、必要に応じて更新を行っています。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 20	不正プログラム対策	【基礎】コンピュータウイルス等の不正プログラムへの防御対策を講ずること。 クラウド利用の場合、クラウド事業者に対して、コンピュータウイルス等の侵入及び不正プログラムによる改ざんへの防御対策について確認することが必要である。金融機関等においては、確認結果をもとにコンピュータウイルス等の不正プログラム等の侵入及び不正プログラムによる改ざんへの防御について、対策を講ずることが必要である。なお、クラウド事業者が提供する機能に不足がある場合は、ツールの導入等により機能を補うことが考えられる	顧客は、コンピュータウイルス等の悪意のあるプログラムに対して予防措置を講じる必要がある。クラウドサービスを利用する際は、顧客はクラウドサービスプロバイダーに対し、コンピュータウイルス等の侵入および悪意のあるプログラムによる改ざんに対する防御対策（クラウドサービスプロバイダーが提供する WAF、IPS、ファイアウォール、アンチウイルスソフトウェア等の保護機能を含む）を確認する必要がある。 お客様は、Cloud Workload Protection Platform (CWPP) を利用して、クラウドホストにセキュリティ保護を提供することができます。CWPP は蓄積された膨大な脅威データに基づき、機械学習を活用して、ハッキング侵入検知、脆弱性リスクアラートなどのセキュリティ保護サービスを提供します。これには、パスワードクラッキングの遮断、異常ログインの通知、トロイの木馬ファイルの検出、高リスク脆弱性の検出などのセキュリティ機能が含まれ、現在の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ます。Tencent Cloud は、お客様に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などの保護製品も提供しています。Cloud Firewall (CFW) 主に異なるネットワーク境界の保護を提供し、ファイアウォール ACL による能動的な制御、IPS によるリアルタイム遮断、仮想パッチ、悪意のあるコードの検出などの機能をサポートしています。従来のネットワークにおける DMZ エリアの要件を実現し、コア資産を重点的に保護するとともに、VPC 間のきめ細かな分離管理を実現します。 Web Application Firewall (WAF) Web 攻撃、侵入、脆弱性悪用、マルウェア注入、

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			改ざん、バックドア、クローラーなど、Web サイトおよび Web サービスのセキュリティ保護課題に対応します。 お客様の規制要件への準拠を支援するため、Tencent Cloud は多層防御システムを構築し、成熟したネットワークセキュリティアーキテクチャを展開しています。ファイアウォール、侵入検知・防御システム (IDS/IPS)、DDoS 防御、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迅速に検知、フィルタリング、阻止し、Tencent Cloud のネットワークセキュリティを保護します。 物理ホストのセキュリティに関しては、テ ンセントクラウドはエンドポイント検出・対応 (EDR) ツールを導入し、ネットワーク全体のサーバー端末資産に対して包括的な監視と管理を行っています。テンセントクラウドが採用する EDR ツールは、ウイルス対策や侵入検知、セキュリティベースラインと脆弱性スキャン、およびコマンド操作や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ており、悪意のあるプログラムや異常な行動を検知した際にアラートを発します。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事象の追跡と処理を行います。
実 21	不正プログラム	【基礎】コンピュータウイルス等の不正プログラムの 検知対策を講ずること。 クラウド利用の場合、クラウド事業者に対して、クラウドサービスにおけるコンピュータウイルス等の不正プログラムの検知対策について確認することが必要である。金融機関等においては、上記の確	顧客は、コンピュータウイルス等の悪意のあるプログラムの侵入や埋め込みの有無を検知するために、適切な検知対策を講じるべきである。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーに対し、クラウドサービスにおける悪意のあるプログラムに対する検知対策を確認し、その確認結果に基づき、適切な検知対策を講じるべきである。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		認結果をもとにクラウド事業者やセキュリティベンダー等が提供する検知対策を講ずることが必要である。	お客様は、Cloud Workload Protection Platform (CWPP) を利用して、クラウドホストのセキュリティ保護を行うことができます。CWPP は蓄積された膨大な脅威データに基づき、機械学習を活用して、ハッキング侵入検知、脆弱性リスクアラートなどのセキュリティ保護サービスを提供します。これには、パスワード解読の阻止、異常ログインの通知、トロイの木馬ファイルの検知、高リスク脆弱性の検知などのセキュリティ機能が含まれ、現在の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ます。また、Tencent Cloud はワンストップのセキュリティ管理プラットフォーム Cloud Security Center (CSC) を提供しています。これは、クラウドファイアウォールや Web アプリケーションファイアウォールからの脅威アラートやログを収集し、Tencent Cloud の脅威インテリジェンスや独自のセキュリティナレッジベースを用いてデータの自動分析と調査を行い、集中型の脅威検知、調査対応能力を顧客に提供します。 同時に、Tencent Cloud Cloud Log Service (CLS) をはじめとする複数のログ製品・サービスは、いずれも「ログダウンロード」「ログエクスポート」「ログ転送」などの機能を通じて、お客様のクラウド上のログをローカル環境にダウンロードして確認したり、指定されたサードパーティシステム（お客様のオンプレミスの SIEM/SOC プラットフォームを含む）に転送したりすることをサポートしています。 物理ホストのセキュリティに関しては、 Tencent Cloud はエンドポイント検出

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			・対応 (EDR) ツールを導入し、ネットワーク全体のサーバー端末資産に対して包括的な監視と管理を行っています。テンセントクラウドが採用する EDR ツールは、ウイルス対策や侵入検知、セキュリティベースラインと脆弱性スキャン、およびコマンド操作やログイン動作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ており、悪意のあるプログラムや異常な動作を検知した際にアラートを発します。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事象の追跡と処理を行います。
実 22	不正プログラム	【基礎】コンピュータウイルス等の不正プログラムによる被害時対策を講ずること。	顧客は、コンピュータウイルス等の悪意のあるプログラムによる被害に対処するための措置を策定すべきである。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーに対し、悪意のあるプログラムによる被害が発生した場合に利用可能な機能や手段（システムの停止および復旧の自動化が可能かどうかを含む）を確認する必要がある。
		クラウド利用の場合、クラウド事業者に対して、コンピュータウイルス等の不正プログラムにより被害が生じた場合の対応手順を作成するに当たり、金融機関等が利用できる機能や手段を確認することが必要である。金融機関等においては、上記の確認結果をもとに被害発生から復旧までの対策を講ずることが必要である。	お客様は、ホストセキュリティ (CWPP) を利用して、Linux ソフトウェアの脆弱性、Windows システムの脆弱性、Web-CMS の脆弱性、アプリケーションの脆弱性を検出し、リアルタイムでアラートを取得するとともに、脆弱性修正ソリューションを入手することができます。これにより、お客様が脆弱性リスクに迅速に対応することを支援します。Tencent Cloud Container Security Service (TCSS) は、頻発するゼロデイ脆弱性から保護するために Tencent Cloud Security が開発した仮想パッチシステムを統合しており、脆弱性を捕捉・分析し、Tencent の専門知識に基づいて仮想パッチを生成し、クラウドサーバー上で自動的に適用することで、ハッカーの攻撃を効果的に阻止します。さらに、お客様は

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			<u>Vulnerability Scanning Service (VSS)</u> を通じて、企業の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、セキュリティ、コンプライアンスなどについて、定期的なセキュリティスキャン、継続的なリスク警告、脆弱性検出を行うことができます。また、VSS と連携して専門的な修正案を提供し、企業のセキュリティリスクを低減します。 お客様の規制要件への準拠を支援し、悪意のあるプログラムによる被害を迅速に抑制するため、Tencent Cloud は内部脆弱性スキャンプラットフォームおよび外部脆弱性収集プラットフォームを導入し、内部および外部の脆弱性や脅威インシデントの報告をサポートしています。Tencent Cloud は発見されたセキュリティ脆弱性をチケットシステムに登録し、担当者に割り当てて規定の時間内に処理および修正を行います。

5.2.2 システム運用共通

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 23	マニュアルの整備	【基礎】通常時マニュアルを整備すること。 クラウド利用の場合、金融機関等においては、クラウドサービスの運用における操作及び手順をマニュアル化することが必要である。	顧客は、日常の各種操作プロセス（操作手順を含む）に関するマニュアルを作成・維持すべきである。クラウドサービスを利用する際、顧客はクラウドサービスの操作およびプロセスをマニュアル化すべきである。 Tencent Cloud 製品の操作手順、ユーザーマニュアル等は文書化され、公式ウェブサイトを通じてお客様に提供されています。また、Tencent Cloud は、Tencent Cloud 製品に関する基礎知識および関連する専門能力に基づく <u>トレーニングおよび認定</u>を提供し、お客様の技術力とクラウドの習熟度向上を支援しています。 さらに、テンセントクラウドは、24 時間 365 日対応のチケットシステム、24 時間

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			365 日対応のホットライン、AI カスタマーサービス、セルフサービスなど、複数のチャネルを通じて、お客様からの質問やフィードバックに絶え間なく対応しています。テンセントクラウドのカスタマーサービスチームと技術専門家が、迅速かつ効果的なサポートを提供します。 また、テンセントクラウドは社内で運用管理規範を策定し、運用担当者の日常業務に対する操作指針と要件を定めています。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、運用業務を管理しています。さらに、詳細な運用セキュリティの「レッドライン」を設定し、定期的に内部の運用セキュリティ監査を実施しています。
実 24	マニュアルの整備	【基礎】障害時・災害時マニュアルを整備すること。	お客様は、障害や災害発生時に使用するマニュアルを策定する必要があります。マニュアルの内容には、障害や災害発生時の代替措置、復旧手順、および対応方法を含める必要があります。 顧客のビジネスの継続的な可用性を保証するため、テンセントクラウドは自社のクラウド環境に適した事業継続管理フレームワークを設計・実装し、包括的な事業継続管理体制を構築しました。また、事業継続管理規定を策定し、関連プロセスを標準化するとともに、ISO/IEC 22301 事業継続マネジメントシステムの国際規格認証を取得しています。テンセントクラウドは、クラウド製品およびサービスの事業影響度分析結果に基づき、異なる対応戦略を策定し、クラウド製品および重要プロセスに対して詳細な災害復旧計画を策定しました。関連する戦略および計画は、施設、人員、設備、システム、情報 / データ、業務優先度など、あらゆる側面を網羅しています。テンセントクラウドは、計画などの実行可能性を確保するため、要件に従って厳格に定期的な演習を実施しています。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 25	アクセス権限の管理	【基礎】各種資源 システムへのアクセス権限を明確にすること。 クラウド利用の場合、クラウド事業者に対して、アクセス権限の設定について、内容や手段を確認することが必要である。金融機関等においては、上記の確認結果をもとに職務分掌に応じたアクセス権限の設定を行うことが必要である。なお、アクセス権限の種類に不足がある場合には、ツールの導入等により機能を補うことが考えられる。	顧客は、コンピュータシステムおよび重要ファイルへのアクセス権限の所有者を明確にし、その範囲を必要最小限に制限しなければならない。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーに対し、アクセス権限の設定内容と方法を確認しなければならない。 <u>Cloud Access Management (CAM)</u> は、顧客が Tencent Cloud の製品およびリソースへのアクセスを安全かつきめ細かく管理するのに役立ちます。ユーザーメインアカウントは、デフォルトで自身の名義のリソースに対する完全なアクセス権限を持ち、サブユーザーを作成して、サブユーザーに ID、認証情報、および権限を割り当てることができます。CAM は、<u>CloudAudit</u> を通じて、Tencent Cloud アカウントのアクティビティに対する監視、コンプライアンスチェック、操作監査、およびリスク監査もサポートしています。また、Tencent Cloud は <u>Bastion Host (BH)</u> を提供しており、ユーザー、資産、アカウント、操作権限などの次元に基づいたきめ細かな権限付与をサポートし、ユーザーが保有する権限が、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。フォートレスマシンも同様に操作監査機能をサポートしており、ユーザーの操作ログを記録・分析することで、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。 顧客の規制要件への準拠を支援するため、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。Tencent Cloud は、

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			役職・役割に対応する担当者の身元情報と各業務システムの権限レベルに関する記録を維持し、定期的な内部権限監査を実施することで、権限の乱用や誤用がないことを確保しています。同時に、Tencent Cloud の本番環境にはすでに「堡垒機」が全面的に導入されており、これを通じて Tencent Cloud のバックエンドシステムコンポーネントに対する管理者アカウントの権限を一元的に管理しています。内部の運用担当者が「堡垒機」にアクセスするには承認が必要であり、特定の Tencent Cloud 内部の運用担当者のみがアクセス可能です。また、「堡垒機」へのログインには二要素認証が必須です。運用操作の記録はログプラットフォームに一元的に保存され、Tencent Cloud の内部監査チームが定期的にログの監査を行っています。
			お客様は、利用者に注意を促す、単純なパスワードの使用を避けるなど、パスワード等の情報漏洩を防止するための措置を講じる必要があります。
			Cloud Access Management (CAM)は、 お客様が Tencent Cloud の製品およびリソースに対するアクセス制御を安全に管理するのに役立ちます。ユーザーメインアカウントはデフォルトで自身の名義のリソースに対する完全なアクセス権限を持ち、サブユーザーを作成し、サブユーザーに ID、認証情報、権限を割り当てることができます。ユーザーはアクセス管理コンソールを通じて、パスワードの複雑さ、長さ、有効期限などの情報を含むサブユーザーのパスワード規則を変更できます。パスワードの漏洩を防ぐため、Tencent Cloud では顧客のパスワードに対して SHA256 ハッシュ暗号化およびソルト処理を適用し、平文での保存を回避しています。 顧客が規制要件を遵守できるよう、Tencent Cloud は社内でアクセス制御管理規範を策定しています。これに基づき、ユ
実 26	アクセス権限の管理	【基礎】パスワードが他人に知られないための措置を講じておくこと。	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ユーザーアカウントには一意の識別子を使用することが求められ、セキュリティ基準に従って従業員アカウントのパスワードポリシー（パスワードの長さ、複雑さ、ロック、リセットなど）が設定されています。Tencent Cloud 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アクセス認証を行い、ユーザーが内部リソースにアクセスするには、まず二要素認証を完了する必要があります。
			顧客は、各種リソースおよびシステムへのアクセス権限付与の手順、ならびにアクセス権限の審査手順を定義すべきである。クラウドサービスを利用する際は、顧客はクラウドサービスプロバイダーに対し、そのクラウドサービスにおけるリソースへの権限付与に関連する機能を確認し、確認結果に基づいて社内の権限付与および審査手順を策定すべきである。
実 27	アクセス権限の管理	【基礎】各種資源 システムへのアクセス権限の付与、見直し手続きを明確にすること。 クラウド利用の場合、クラウドサービスにおける権限の付与や見直しの手続きを明確にするため、クラウド事業者に対して、クラウドサービスで提供される資源に対するアクセス権限付与に関する手続き及びそれに関する機能を確認することが必要である。金融機関等においては、上記の確認結果をもとに自社におけるアクセス権限の付与や見直しに関する手続きを定めることが必要である。	顧客は、Cloud Access Management (CAM) タグなどを通じてサブユーザーにリソース権限を割り当てることで、クラウドリソースに対するきめ細かなアクセス制御を実現できる。また、Tencent Cloud は Bastion Host (BH) を提供しており、ユーザー、資産、アカウント、操作権限などの次元に基づいたきめ細かな権限付与をサポートし、ユーザーが保有する権限が、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。さらに、CAM や BH などのクラウド製品のユーザーガイドや操作手順などは文書化されており、公式サイトを通じて顧客に提供されています。顧客は関連するガイドラインを参照して、権限の割り当てと管理を行うことができます。 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

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			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。Tencent Cloud は、役職・役割に対応する担当者の身元情報と各業務システムの権限レベルに関する記録を管理し、定期的に内部権限監査を実施することで、権限の乱用や誤用がないよう確保しています。
実 30	データ管理	【基礎】暗号鍵の運用管理方法を明確にすること。 クラウド利用の場合、金融機関等において暗号鍵管理のライフサイクル全般（生成、配布、保管、失効、更新、廃棄、保存等）の手続きを定めるため、クラウド事業者に対して、利用する暗号鍵管理サービスの内容を確認することが必要である。	顧客は、暗号鍵の生成、配布、使用、保管などのプロセスを策定し、鍵が漏洩した際の対応策を明確にする必要がある。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーに対し、提供される鍵管理サービスの内容を確認し、その確認結果に基づいて鍵のライフサイクル全般に関する内部手順を策定する。 顧客が鍵の機密性、完全性、可用性を保護できるよう支援するため、Tencent Cloud は Key Management Service (KMS) を提供しています。KMS は、顧客が鍵を容易に作成・管理できるようサポートし、多様なアプリケーションや業務における鍵管理のニーズを満たすとともに、規制・コンプライアンス要件に準拠しています。KMS はオブジェクトストレージ、分散データベース、クラウドハードディスク等のサービスの暗号化機能とシームレスに統合され、顧客が容易に活用できるようになっています。 KMS は、FIPS-140-2 認証を取得したハードウェアセキュリティモジュール (HSM) に基づいて鍵を生成・保護し、安全なデータ転送プロトコルを採用しています。また、複数のデータセンターにまたがる分散型クラスタ構成によるサービス展開とホットバックアップを採用し、基盤となる HSM デバイスは 2 つのデータセンターにまたがるコールドバックアップ構成を採用することで、鍵管理システムの高い可用

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			性を確保しています。 暗号文の安全性を確保し、鍵の解読や悪用リスクを低減するため KMS は定期的な鍵のローテーションをサポートしています。また、鍵のローテーション後も、ローテーション前に暗号化された暗号文との互換性が保たれるため、ユーザーの業務に影響を与えることはありません。KMS は、無効化、失効、または漏洩した鍵を、安全かつ確実な方法で削除します。削除された鍵は復元不可能となり、その鍵で暗号化されたデータも復号できなくなります。 お客様の規制要件への準拠を支援するため、Tencent Cloud は社内で暗号化および鍵管理基準を策定し、鍵の申請、生成、保存、使用、引き継ぎ、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にしています。鍵のライフサイクルに関わる各操作については、二重管理、厳格な引き継ぎ、適切な保管、適時更新という基本要件を遵守しています。鍵の使用過程においても、権限と責任の分離、厳格な承認、実名操作などの要件を遵守し、業務用鍵の操作ログを保持するとともに、定期的に操作監査を実施する必要があります。さらに、Tencent Cloud は、鍵の用途、鍵によって保護されるデータの機密性、鍵漏洩の可能性および影響度などの要素を総合的に考慮し、鍵のライフサイクル全体を管理しています。
実 31	オペレーション 習熟	【基礎】オペレーション習熟のための教育及び訓練を行うこと。 クラウドサービスを利用する際には、金融機関等は以下の点に留意する必要がある： (1) マニュアル改訂が、金融機関等が実施するシステムへの変更（例：業務アプリケーションの変更）といった内部要因によるものだけでなく、クラウド事業者が提供する機能等の変更といった外部要因に	お客様は、運用関連の教育およびトレーニングを実施する必要があります。クラウドサービスをご利用の際、お客様はクラウドサービスの機能変更およびそれに伴うシステム変更を考慮し、関連マニュアルを適時に改訂するとともに、必要に応じて改訂内容に基づく教育・トレーニングを実施してください。 Tencent Cloud 製品の操作手順、ユーザーマニュアル等は文書化され、公式サイトを通じてお客様に提供されています。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		よるものが増えることになる。マニュアルの改訂内容により、必要に応じて教育及び訓練を実施する。 (2) クラウド事業者から提供されるマニュアルやリファレンスに加え、クラウド事業者のホームページ上で公開されている情報を参照し、必要に応じて教育及び訓練を実施する。	また、Tencent Cloud は、Tencent Cloud 製品に関する基礎知識および関連する専門能力に基づく トレーニングおよび認定プログラム を提供し、お客様の技術力およびクラウドの習熟度向上を支援しています。 外部環境に影響を及ぼす可能性のある製品、インフラストラクチャ、ネットワーク構成の変更については、Tencent Cloud は告知、電子メール、クラウドコンソール、またはその他の適切なチャネルを通じてお客様に通知いたします。 Tencent Cloud では、社内においても包括的なトレーニングメカニズムを確立し、正社員、コンサルタント、インターン、および外部委託従業員等に対し、トレーニングコースの受講を義務付けております。Tencent Cloud は、全従業員必須トレーニング、重点ポジション向け専門トレーニング、選択専門科目トレーニングなど、多様なトレーニングコースを提供しており、基礎的なセキュリティ意識、オフィスセキュリティ、脆弱性の識別と防御、プライバシー保護、インシデント対応、開発セキュリティ規範、データセキュリティ要件などの内容を網羅しています。
実 32	コンピュータウイルス対策	【基礎】コンピュータウイルス対策を講ずること。	顧客は、コンピュータウイルスなどの侵入や感染を防ぐため、コンピュータウイルスに対する防御、検知、および復旧のプロセスを明確にすべきである。 お客様は、Cloud Workload Protection Platform (CWPP) を採用し、クラウドホストにセキュリティ保護を提供できます。CWPP は蓄積された膨大な脅威データに基づき、機械学習を活用して、ハッキング

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			侵入検知、脆弱性リスクアラートなどのセキュリティ保護サービスを提供します。これには、パスワードクラッキングの遮断、異常ログインの通知、トロイの木馬ファイルの検出、高リスク脆弱性の検出などのセキュリティ機能が含まれ、現在の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ます。 お客様の規制要件への準拠を支援するため、サーバーのウイルス対策において、Tencent Cloud はエンドポイント検出および対応 (EDR) ツールを導入し、ネットワーク全体のサーバーエンドポイント資産に対して包括的な監視と管理を行っています。Tencent Cloud が採用する EDR ツールは、ウイルス対策と侵入検知、セキュリティベースラインと脆弱性スキャン、およびコマンド操作や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ており、悪意のあるプログラムや異常な行動を検知した際にアラートを発します。 オフィス端末の利用管理については、 Tencent Cloud は社内でソフトウェアセキュリティ規範を策定し、オフィス端末（ノートパソコンやワークステーションを含む）におけるソフトウェアの使用制限を明確にしています。また、アプリケーションのホワイトリスト技術を活用し、既知の信頼できるプログラムのみの実行を許可することで、マルウェア侵入のリスクを低減しています。また、Tencent Cloud はゼロトラストセキュリティ管理システムを通じて端末を管理し、ウイルス駆除、脆弱性修正、プロアクティブ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、内部横展開対策など、全方位的なセキュリティ保護を実現しています。
実 33	外部接続管理	【基礎】接続契約内容を明確にす	顧客は、回線接続を介してデータの送受信を行う契約を締結する際、接続方式、デー

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		ること。	タ形式、データ内容などの事項を明確にする必要があります。 テンセントクラウドは、ユーザーの外部へのデータ転送のためにAPIインターフェースを提供しており、そのインターフェースでは転送プロトコル、転送形式、および転送内容が明確に定義されています。さらに、テンセントクラウドの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、ステータス監視などのセキュリティ機能を備えており、顧客の業務に対してポートレベルの通信セキュリティを保証します。
実 34	外部接続管理	【基礎】外部接続における運用管理方法を明確にすること。 クラウド利用の場合、クラウド事業者に対して、金融機関等で策定したセキュリティ基準を充足しているかを確認することが必要である。確認する観点としては、以下の例がある。クラウド事業者が提供する範囲での運用管理方法について、特にインターネット接続を伴う部分における脆弱性等が適切に対応されているか確認する。クラウド事業者が管理する範囲としては、以下の例がある。 (1) クラウド内部で使用しているネットワーク機器のバージョンアップ (2) クラウド内部で使用している仮想化やマネージドサービスで使用しているソフトウェアのバージョンアップ	顧客は、外部接続時の運用管理方法を明確にすべきである。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーがその運用管理範囲内で脆弱性問題に適切に対処しているか、ネットワーク機器および仮想化プラットフォーム関連ソフトウェアのバージョンアップを適切に管理しているかを確認する必要がある。 リモート運用保守のセキュリティ面において、Tencent Cloud は顧客に VPN Connection を提供しています。VPN 接続は、IKE (鍵交換プロトコル) と IPsec を採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することで、転送中のデータの安全性を確保します。VPN ゲートウェイは高い信頼性を備えており、下層ではデュアルマシンホットスタンバイアーキテクチャを採用することで、通信セッションの中断を防ぎ、上層のアプリケーションには影響を与えません。 また、Tencent Cloud では社内従業員のリモートアクセス管理に関する手順を確立しており、従業員は Tencent Cloud に登録済みの信頼できるデバイスに限り、暗号化された通信チャンネルを介して Tencent

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			Cloud の社内ネットワークおよび日常業務システムにリモートアクセスすることができます。Tencent Cloud はリモートアクセスログを管理し、ユーザーの操作履歴を記録します。同時に、Tencent Cloud の社内ネットワークと顧客データが格納されている本番環境は完全に分離されています。Tencent Cloud の従業員が顧客の同意と権限を得て顧客情報資産にアクセスする場合、必ずバスタードマシン (Bastion Host) を経由して顧客データが格納されている本番環境にアクセスする必要があります。バックエンドの運用保守操作記録はすべてログプラットフォームに一元的に保存され、Tencent Cloud の内部監査チームが定期的に記録情報を監査します。 脆弱性およびパッチ管理に関して、 Tencent Cloud は最新のパッチを特定し、パッチの適用前に十分なセキュリティテストを実施することで、パッチ適用の安全性を確保しています。Tencent Cloud は定期的に社内の各事業チームにパッチのアップグレードおよび適用を通知するとともに、エンドポイント検出ツールを使用してパッチの適用状況を定期的にスキャンし、期限を過ぎてもパッチが適用されていないデバイスに対しては自動的にアラートチケットを生成します。同時に、テンセントクラウドは内部の脆弱性スキャンメカニズムと外部の脆弱性収集プラットフォームを構築し、内部および外部の脆弱性や脅威の問題を報告しています。セキュリティ脆弱性に関するチケットはセキュリティ運用システムに記録され、所定の期間内に処理するよう担当者に割り当てられます。さらに、テンセントクラウドのセキュリティ研究チームは、脆弱性防御機能を仮想パッチとしてテンセントクラウドの Web Application Firewall (WAF) システムに統合し、クラウドプラットフォーム全体のセキュリティを確保しています。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ネットワーク機器の管理に関しては、テンセントクラウドはネットワークセキュリティ設定基準およびセキュリティベースライン基準を策定し、ネットワーク機器などのセキュリティ設定を標準化して管理しています。テンセントクラウドのセキュリティチームは、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のセキュリティポリシーやパラメータ設定を定期的にレビューし、その有効性を確保しています。さらに、テンセントクラウド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・アラートしています。

5.2.3 運行管理

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 35	オペレーション管理	【基礎】オペレータの資格確認を行うこと。 クラウド利用の場合、クラウド事業者に対して、金融機関等のオペレータがインターネット経由で接続することを考慮し、より強固な資格確認の手段が用意されているかについて確認することが必要である。	顧客は、コンピュータシステムの不正利用を防止するため、オペレータの資格を確認する必要があります。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーに対し、厳格な資格確認手段を提供できるかどうかを確認する必要があります。 Cloud Access Management (CAM) は、顧客が Tencent Cloud の製品およびリソースへのアクセスを安全かつきめ細かく管理するのに役立ちます。ユーザーメインアカウントはデフォルトで自身の名義のリソースに対する完全なアクセス権限を持ち、サブユーザーを作成し、サブユーザーに ID、認証情報、権限を割り当てることができます。CAM は、MFA デバイスによる認証や携帯電話の認証コードによる認証など、さまざまな方式の二次認証機能をサポートしており、ログイン時や機密性の高い操作を行う前に、本人確認と環境の安

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			全性を確認することができます。 Tencent Cloud はまた、Bastion Host (BH) も提供しており、ユーザー、資産、アカウント、操作権限などの次元に基づいた詳細な粒度での権限付与をサポートし、ユーザーに付与される権限が、資産へのアクセスや業務タスクの完了に必要な最小限の権限であることを保証します。パスションホストは同様に操作監査機能をサポートし、ユーザーの操作ログを記録・分析することで、セキュリティインシデントの効果的な追跡を確保します。 顧客の規制要件への準拠を支援するため、Tencent Cloud は社内でアクセス制御の権限付与ポリシーおよび権限分離マトリックスメカニズムを策定しました。ユーザーアカウントには一意の識別子を使用することを義務付け、セキュリティベースラインに基づいて従業員アカウントのパスワードポリシーを設定しています。Tencent Cloud 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アクセス認証を行い、ユーザーが内部リソースにアクセスする際には、まずアカウントにログインし、ゼロトラストセキュリティ管理システムによる二要素認証を完了する必要があります。同時に、Tencent Cloud の本番環境には「堡垒機（ゲートウェイ）」が全面的に導入されており、これを通じて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。内部運用担当者が堡垒機にアクセスするには承認が必要であり、特定の Tencent Cloud 内部運用担当者のみがアクセス可能で、堡垒機へのログインには二要素認証が必要です。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 36	オペレーション管理	【基礎】オペレーションの依頼・承認手続きを明確にすること。	顧客は、コンピュータシステムの不正使用を防止するため、操作依頼と承認のプロセスを明確にする必要があります。
			Tencent Cloud コンソールは、Cloud Access Management (CAM) を通じて、安全な権限割り当てとサブユーザー管理を顧客に提供し、ユーザーやロールが具体的にどの操作を実行し、どのリソースにアクセスできるかを容易に制御できるよう支援します。顧客は CAM を通じて、メインアカウントおよび所属するサブアカウントに対して二段階認証を有効化し、アカウントのセキュリティを強化できます。また、CloudAudit を活用して、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ユーザーアクティビティや API の使用状況を記録 継続的に監視および保持することができます。 お客様の規制要件への準拠を支援するため、Tencent Cloud は内部でアクセス制御管理に関する規範と対応する権限付与ポリシーを策定し、ホスト OS、アプリケーションシステム、ネットワーク機器などへのアクセスおよび操作に必要な承認手順を明確化することで、不正アクセスを防止しています。
実 37	オペレーション管理	【基礎】オペレーション実行体制を明確にすること。 クラウド事業者に対して、誤操作及び不正使用の対策が講じられていることについて確認することが必要である。確認する観点としては、以下の例がある： (1) 操作ログの取得範囲と内容 (2) オペレーション画面を録画する機能	お客様は、オペレーターのチーム構成や操作手順を含む、操作実行に関する関連メカニズムを明確にする必要があります。クラウドサービスを利用する際には、誤操作や不正使用を防止するための対策を講じる必要があります。 誤操作および不正操作の防止を支援するため、Tencent Cloud は CloudAudit を提供しています。CloudAudit は、お客様が Tencent Cloud アカウントの活動を監視し、コンプライアンスチェック、操作

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			レビュー、およびリスク審査を行うことを支援するとともに、90 日以内の Tencent Cloud コンソールおよびクラウド API の操作記録をオンラインで閲覧することをサポートしています。Bastion Host (BH) も、ユーザーの運用・保守操作行動を記録および監査することができ、再生方式を通じてユーザーの操作行動を実際に再現することをサポートし、セキュリティインシデントの効果的な追跡を確保します。 さらに、Tencent Cloud 製品の操作手順、ユーザーマニュアルなどは文書化され、公式ウェブサイトを通じてお客様に提供されています。Tencent Cloud はまた、Tencent Cloud 製品の基礎知識および関連する専門能力に基づくトレーニング グおよび認定を提供し、お客様の技術力とクラウドの習熟度を向上させます。 Tencent Cloud は、内部においても運用・保守管理規範を制定し、運用担当者の日常的な運用行動に対する操作指針と要求を提供しています。Tencent Cloud は、成熟したツール化および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、内部の運用管理メカニズムを通じて変更時間ウィンドウを厳密に制御し、すべての運用リクエストが指定された時間内に完了することを保証します。Tencent Cloud はまた、詳細な運用セキュリティの「レッドライン」を設定し、定期的に内部の運用セキュリティレビューを実施しています。本番環境内での操作が制御および追跡可能であることを確保するため、バックエンドの運用操作記録はすべて詳細に記録され、ログプラットフォームに集中保存され、

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			Tencent Cloud 内部の監査チームが定期的に運用プロセス中の疑わしい操作についての問題調査と追跡を行います。
			顧客は操作を記録し、確認を行うことで、操作の正当性を検証する必要があります。
			CloudAudit は、Tencent Cloud アカун トの監視、コンプライアンスチェック、操 作監査、およびリスク監査をサポートしま す。お客様は CloudAudit を活用して、 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 を記録、継続的に監視、および保存するこ とができます。また、Data Security Audit (DSA) を選択して、データに対する異常 な操作を監視することも可能です。DSA は、AI（人工知能）を基盤としたデータベ 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おけ る各種セッション情報 アクセス操作 SQL 文の全量監査と記録をサポートします。ま た、多様なルールベースと脅威検知エンジ ンに基づき、操作中の悪意ある行為を識別 し、管理者に速やかに通知して適切なセキ ュリティ対策を講じてもらいます。発生し たセキュリティインシデントについては、 データセキュリティ監査により数年にわ たるログの監査と分析が可能であり、企業 に対してセキュリティインシデントの全 容を再現し、責任者を特定するための参考 資料を提供します。
実 38	オペレー ション 管理	【基礎】オペレーションの記録 確 認を行うこと。	顧客の規制要件への準拠を支援するため、 Tencent Cloud は運用管理規範を策定し、 運用担当者の日常業務に対する操作ガイ ドラインと要件を提供しています。また、 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、定期的に内 部の運用セキュリティ監査を実施してい

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ます。さらに、Tencent Cloud の本番環境には「堡垒機 (Bastion Host)」が全面的に導入されており、本番環境における運用操作はすべて堡垒機を経由して行わなければなりません。本番環境内の操作を確実に制御・追跡できるようにするため、バックエンドの運用操作記録は詳細に記録され、ログプラットフォームに一元的に保存されます。Tencent Cloud の内部監査チームが、運用プロセスにおける不審な操作について定期的に問題の調査と追跡を行っています。
実 39	データファイル管理	【基礎】データファイルのバックアップを確保すること。 クラウド利用の場合、クラウド事業者に対して、クラウド事業者が取得しているバックアップが業務上の障害・災害の復旧等に利用できる場合、金融機関等がみずからバックアップを取得する必要はなくなるので、クラウド事業者が実施するバックアップについて確認することが必要である。 金融機関等においては、上記の確認結果をもとにクラウド事業者が対応していない範囲について、データファイルだけでなく、利用するクラウド環境の設定情報についてもバックアップデータを取得することが必要である。	顧客は重要なデータファイルのバックアップを行い、関連する管理方法を明確にする必要がある。 Tencent Cloud 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ており、リージョン (region) とアベイラビリティゾーン (zone) で構成されています。Tencent Cloud の異なるリージョン間は完全に分離されており、各リージョンはさらに複数の相互に隔離されたアベイラビリティゾーンに分割されています。お客様は、事業の発展ニーズやデータセキュリティ要件に基づき、データやシステムを異なるリージョンやアベイラビリティゾーンに自律的かつ柔軟に展開またはバックアップすることで、事業の災害復旧要件を確保できます。さらに、テンセントクラウドは、クラウドサービスの事業継続性を確保するため、単一のリージョン内で複数のデータセンターを採用する冗長化メカニズムをクラウド製品に求めています。 Tencent Cloud が提供する各種ストレージサービスおよびデータベースサービスは、いずれもバックアップ機能を備えており、お客様のあらゆるバックアップニーズに対応しています。例えば：

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			Cloud Object Storage (COS) に保存されたデータは、リークレスレプリケーション機能を通じて複数の指定リージョンに同時に保存できます。これにより、一部のデータが予期せず失われた場合でも、冗長データを利用して完全なデータを検索・復元することが可能となり、また、あるアベイラビリティゾーンのストレージが不可抗力の災害に見舞われた際の損失を回避し、多重冗長バックアップおよび遠隔地での災害対策の効果を実現します。 Cloud Block Storage (CBS) のスナップショットバックアップ機能は、CBS の時点スナップショットを作成することでデータをバックアップし、改ざんや誤削除によるデータ損失を防ぎ、業務障害時に迅速に復旧できるようにします。 Cloud File Storage (CFS) は定期スナップショット機能を提供しており、お客様がバックアップタスクのポリシーを柔軟に設定できるようになっています。業務ごとに異なる定期スナップショットポリシーを採用することを推奨します。 Cloud Native Database TDSQL-C は、論理バックアップとスナップショットバックアップの 2 種類のバックアップタイプをサポートしています。完全なデータバックアップおよびその後の一定期間の binlog バックアップにより、TDSQL-C MySQL 版クラスタ全体または特定のデータベース・テーブルを任意の時点に復元することが可能です。 TencentDB for MySQL は、自動バックアップと手動バックアップの 2 つの方法でデータベースをバックアップで

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			き、リージョン間バックアップ機能を提供することで、お客様の災害復旧能力の向上とデータの信頼性向上を支援します。 • TencentDB for MongoDB は、データの自動バックアップとロスレス復旧メカニズムを提供し、マルチノードでのデータバックアップをサポートしています。お客様はバックアップメカニズムを通じて数日分のバックアップデータを保存でき、災害発生時のデータ復旧に役立てることができます。 Tencent Cloud 内部でもバックアップ管理手順を策定しており、関連法規の要件に基づき、収集・処理する重要データのバックアップを実施しています。内部の重要情報については、Tencent Cloud はデータレベルに応じて異なる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ています。Tencent Cloud はバックアップ戦略に基づき、サーバー、ネットワーク機器、アプリケーションシステムの設定ファイル、ログなどの情報をバックアップし、ファイルの破損が発生した場合でも速やかに復旧できるよう確保しています。
実 40	プログラムファイル管理	【基礎】プログラムファイルの管理方法を明確にすること。	顧客は、プログラムファイル（ソフトウェアパッケージ、自社開発プログラムなどのソースコードおよびロードモジュールを含む）の管理方法とプロセスを定義し、プログラムの改ざんや破壊などを防止する必要があります。 顧客のプログラムファイル管理を支援するため、Tencent Cloud は開発者ツール Cloud Native Build (CNB) を提供しています。CNB は完全な開発者ツールチェーンを提供し、要件定義からデプロイまでの開発プロセス全体を効果的にサポート・管理します。その中のアーティファクトリポジトリは、ソフトウェアビルドプロセス

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			で生成されたアーティファクトの保存、管理、配布に使用できます。 テンセントクラウド内部でも情報システムセキュリティ開発基準を確立しており、ISO/IEC 20000 情報技術サービス管理規格 ISO/IEC 27001 情報セキュリティマネジメントシステム、および ISO/IEC 9001 品質マネジメントシステム規格を、製品セキュリティ開発ライフサイクルの全プロセスに統合することに注力しています。要件定義、設計、開発、テスト、納品、運用保守などの各段階に重点を置き、クラウド製品がそのライフサイクルを通じて十分なセキュリティ管理を受けられるよう確保しています。テンセントクラウドのソフトウェア開発には DevSecOps の管理メカニズムが組み込まれており、クラウド製品の迅速かつ継続的な開発、リリース、デプロイを保証しています。 テンセントクラウドは、自社開発プロジェクトのソースコードをコードリポジトリで管理し、適切なアクセス権限管理メカニズムを設定しています。最小権限の原則に従い、各役割に応じて必要なアクセス権限を割り当てています。テンセントクラウドは、許可なくソースコードを外部へ複製、伝播、配布することを禁止しています。
実 41	プログラムファイル管理	【基礎】プログラムファイルのバックアップを確保すること。	お客様はプログラムファイルのバックアップを行い、関連する保護および管理方法を明確に定める必要があります。 Tencent Cloud が提供するコンピューティングサービス、ネットワークサービス、ストレージサービス、データベースサービス、コンテナおよびミドルウェアサービス、セキュリティサービスなど、多種多様なクラウド製品/サービスは、いずれも高可用性を備えており、対応する災害復旧計画が用意されています。例えば、Cloud Object Storage (COS) は、複数のアーキ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			テクチャやデバイスにわたるデータの冗長保存をサポートし、ユーザーのデータに対して遠隔地での災害復旧およびリソース分離機能を提供し、データの永続性を実現します。 Cloud Block Storage (CBS) のスナップショットを取得することでデータをバックアップし、改ざんや誤削除によるデータ損失を防止するとともに、業務障害時に迅速に復旧できるようにします。 さらに、Tencent Cloud は世界各国の関連国際基準および現地のセキュリティ要件に基づき、データセンターを建設またはリースしています。現在、日本国内には電力とネットワークが相互に独立した2つのデータセンターがあり、日本国内でのデータの保存、処理、およびバックアップをサポートしています。お客様は、ビジネスの発展ニーズやデータセキュリティ要件に応じて、データやシステムを異なる地域やアベイラビリティゾーンに自律的かつ柔軟に展開・バックアップし、ビジネスの災害復旧要件を確保することができます。
実 42	ネットワーク設定 情報管理	【基礎】ネットワークの設定情報の管理を行うこと。 クラウド利用の場合、クラウド事業者に対して、ネットワーク機器へのアクセスに使用する管理インタフェースの不正アクセス対策について、確認することが必要である。	顧客は、ネットワーク機器の設定情報を適切に管理し、不正な変更を防ぐ必要がある。 顧客は Config を通じて、クラウドリソースの集中監査とガバナンスを実現できます。これにより、顧客アカウント下の異なるリージョンにおける各種クラウドリソースの構成情報および構成変更を継続的に記録し、Tencent Cloud のベストプラクティスに基づくルールやコンプライアンスパッケージテンプレートに基づき、企業アカウント下のクラウドリソース構成に対して継続的なコンプライアンス評価を自動的に実施し、非準拠なリソース構成を特定することで、クラウドリソースの自動監視と管理を実現します。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			さらに、Cloud Access Management (CAM) は、そのきめ細かな権限管理機能を通じて、リソースごとに異なるユーザーに特定の権限を付与します。また、CloudAudit を利用することで、Tencent Cloud アカウントのアクティビティに対する監視、コンプライアンスチェック、操作監査、およびリスク監査を行うことができます。CloudAudit では、過去 90 日以内の Tencent Cloud コンソールおよびクラウド API の操作記録をオンラインで確認できます。 お客様の規制要件への準拠を支援するため、Tencent Cloud はネットワークセキュリティ設定基準およびセキュリティベースライン基準を確立し、ネットワーク機器などのセキュリティ設定を標準化して管理しています。Tencent Cloud のネットワーク設定情報の変更には、所定の変更および承認プロセスを経る必要があります。同時に、Tencent Cloud の本番環境には「堡垒机（フォートレス）」が全面的に導入されており、これを通じてネットワーク機器に関連するアカウント権限を集中的に管理し、未承認者による内部ネットワークリソースへのアクセスを厳格に禁止しています。内部運用担当者が堡垒機にアクセスするには承認・認可が必要であり、認可を受けた内部運用担当者は、2 段階の本人確認を経てログインする必要があります。バックエンドの運用操作記録はすべてログプラットフォームに一元的に保存され、Tencent Cloud の内部監査チームが定期的に記録の監査を行っています。 さらに、ネットワーク機器への物理的アクセス管理に関しては、テンセントクラウドはデータセンター運営事業者に対し、人員の区分およびアクセス権限に基づき、入室管理システムに完全な人員アクセス制

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			御セキュリティマトリックスを構築するよう求めており、これにより、各種人員のアクセスや操作などの行動を効果的に管理しています。テンセントクラウドは、データセンターおよびサーバールームに出入りするあらゆる来訪者やスタッフに対し、身元確認と所持品の検査を実施し、持ち込み物品を登録するようオペレーターに求めています。また、データセンターに24 時間 365 日死角のないビデオ監視アラートシステムを配備し、警備室が常駐して監視記録を安全に保管し、十分な期間保存するよう求めています。
			お客様は、ネットワーク機器の設定情報をバックアップでき、関連する管理方法を明確にする必要があります。 お客様のネットワークの高可用性を確保するため、Tencent Cloud の Virtual Private Cloud (VPC) は成熟したネットワーク仮想化技術を採用し、リンクの冗長化、ゲートウェイのアクティブ・スタンバイ構成、プライベートネットワークのマルチアベイラビリティゾーン (AZ) にわたる展開など、多様な技術によりネットワークの高可用性を確保し、リンクレベル、ネットワークレベル、データセンターレベルといったあらゆる側面からネットワークの安全性と安定性を保護します。同時に、Cloud Load Balancer (CLB) はクラスター構成で展開され、障害が発生したインスタンスを迅速に切り離すことで、高可用性を実現しています。 お客様の規制要求への対応を支援するため、Tencent Cloud はバックアップ管理手順を策定し、関連法規の要件に従って、収集・処理する重要なデータのバックアップを行っています。Tencent Cloud はバッ
実 43	ネットワーク設定 情報管理	【基礎】ネットワークの設定情報のバックアップを確保すること。	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			クアアップポリシーに基づき、サーバー、ネットワーク機器、アプリケーションシステムの設定ファイル、ログなどの情報をバックアップし、ファイルの破損時に迅速な復旧を可能にしています。
			お客様は、運用保守ドキュメント（データセンターの運用保守に必要な操作手順、操作指示書、システム関連資料、端末操作マニュアルなどを含む）を管理するための方法を明確にする必要があります。 顧客が規制要件を遵守できるよう、テンセントクラウドはドキュメント管理に関する規範および手順を策定し、ファイル識別要件（ファイル番号、バージョン番号、配布番号、公開日および実施日など）を規定することで、使用時に適切なファイルの有効なバージョンを確実に取得できるようにしています。 Tencent Cloud は主に、社内の規程管理プラットフォームを通じて規程文書の公開および管理を行っています。規程文書は、多段階の承認を経た後にのみプラットフォーム上で公開または改訂が可能となり、担当の文書管理者がメンテナンスを行います。文書管理者は規程文書の改訂・変更権限を有しており、利用者はプラットフォーム上で文書を閲覧することのみ可能です。Tencent Cloud の社内文書管理プラットフォームでは、従業員が各種業務文書を自らアップロードしたり、文書に対して読み書き権限を設定したりすることが可能です。
実 44	運用時ドキュメント管理	【基礎】運用時のドキュメントの保管管理方法を明確にすること。	
			お客様は復旧に必要なドキュメントのバックアップを行い、その管理方法を明確にする必要があります。
実 45	運用時ドキュメント管理	【基礎】災害時の復旧対応に必要なドキュメントのバックアップを確保すること。	顧客がサイバーセキュリティインシデント発生後に迅速に対応し、重要な機能を復旧できるよう、Tencent Cloud が提供する各種ストレージサービスおよ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や遠隔地での災

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			害対策などの要件に対応しています。 顧客による迅速な災害復旧を実現するため、テンセントクラウドは自社のクラウド環境に適した事業継続管理フレームワークを設計・実装し、包括的な事業継続管理体制を構築しており、ISO/IEC 22301 事業継続管理システムの国際規格認証を取得しています。データバックアップに関しては、テンセントクラウドはバックアップ管理手順を策定し、関連法規の要件に基づき、収集・処理する重要データのバックアップを実施しています。内部の重要情報については、データレベルに応じて異なる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基づき、顧客に複数のストレージレプリカおよびバックアップサービスを提供し、サービスレベル契約（SLA）の規定に従い、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。 バックアップに関する詳細については、本ガイドラインの第 5.2.3 章「実 39 データファイル管理」の条項を参照してください。
実 46	運行監視	【基礎】システムの運行状況の監視体制を整備すること。 クラウド利用の場合、クラウド事業者に対して、監視対象・内容、監視方法についてクラウド事業者が提供する監視サービスやオプション群を確認することが必要である。	顧客は、システムの稼働状況に対する監視体制を構築し、監視対象、監視内容、および監視方法を明確にする必要がある。クラウドサービスを利用する際は、顧客はクラウドサービスプロバイダーに対し、提供される監視サービスおよびオプション機能を確認し、その結果に基づいて監視体制を構築する必要がある。 システムの稼働状況を監視・管理するために、お客様は Tencent Cloud Observability Platform (TCOP) をご利用

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			用いただけます。本サービスは、クラウド製品 / クラウドリソースのリアルタイム監視、分析、およびアラートサービスを提供し、クラウドサーバーやクラウドデータベースなどのクラウド製品が自律的に報告する各種監視指標、ならびにお客様が独自に設定して報告する監視指標を収集し、視覚化グラフで表示します。これにより、お客様はクラウド製品リソースの使用率、アプリケーションパフォーマンス、およびクラウド製品の稼働状況をリアルタイムで把握できるとともに、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をお客様に迅速に通知します。 インフラストラクチャの監視と管理に関して では、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・アラートしています。また、エンドポイント検出および対応 (EDR) ツールを導入し、ネットワーク全体のサーバー端末資産に対して包括的な監視と管理を行っています。Tencent Cloud が採用する EDR ツールはウイルス対策や侵入検知、セキュリティベースラインおよび脆弱性スキャン、ならびにコマンド操作や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ており、悪意のあるプログラムや異常な行動を検知した際にアラートを発動します。Tencent Cloud はチケットシステムを通じて、検知されたセキュリティ問題を追跡・解決します。

5.2.4 各種設備管理

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 47	資源管理	【基礎】各種資源の能力及び使用状況の確認を行うこと。	顧客は、コンピュータシステムの障害や処理能力の低下を回避するため、各種リソースの能力および使用状況を監視するための適切な措置を講じるべきである。
		クラウド利用の場合、クラウド事業者に対して、資源の能力及び使用状況の把握について確認することが必要である。	Tencent Cloud Observability Platform (TCOP) は、クラウド製品 / クラウドリソースに対するリアルタイムの監視、分析、アラートサービスを提供します。クラウドサーバーやクラウドデータベースなどのクラウド製品が自動的に報告する各種監視指標や、顧客が独自に設定して報告する監視指標を収集し、可視化グラフで表示することで、顧客がクラウド製品のリソース使用率、アプリケーションのパフォーマンス、およびクラウド製品の稼働状況をリアルタイムで把握できるよう支援します。TCOP は指標に対するアラート設定をサポートしており、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上の異常状況をタイムリーにお客様に通知します。
		クラウド利用の場合、クラウド事業者に対して、管理対象資源について、以下の観点で確認することが必要である。 (1) 使用状況の監視において設定するしきい値等。 (2) 金融機関等が定義可能なスケーリングポリシー（需要の変化に応じたスケーリング方法の定義）。	お客様の柔軟な容量計画および調整を支援するため 、Tencent Cloud は Auto Scaling (AS) サービスを提供しています。AS はインスタンスのヘルス状態を自動的に検出し、お客様のビジネスニーズ、ポリシー、および事前に設定されたスケールアウト・スケールインの条件に基づいて、クラウドサーバーのコンピューティングリソースを自動的に調整し、お客様のアプリケーション負荷を処理するために常に適切な数のクラウドサーバーインスタンスを確保します。 Tencent Cloud 内部でも容量管理手順を策定しており、業務運営のニーズに基づいて容量需要を予測し、年間容量管理計画を策定しています。同時に、Tencent Cloud は内部の容量監視プラットフォームを使用して容量の使用状況をリアルタイムで監

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			視し、容量使用の傾向を把握しています。
実 48	機器の管理	【基礎】ハードウェア及びソフトウェアの管理を行うこと。 クラウド利用の場合、クラウド事業者に対して、クラウド事業者等が提供する構成管理機能について確認することが必要である。クラウド利用の場合、クラウド事業者に対して、クラウド事業者が提供する OS などの基本ソフトウェア及びソフトウェア製品（ミドルウェア含む）の変更を金融機関等で把握する方法を確認しておくことが必要である。金融機関等においては、上記で確認した内容をもとに構成管理、変更管理を実施するとともに、必要に応じて金融機関等が管理するプログラム等への対応を行うことが必要である。	顧客は、システムの導入、変更、廃止、および障害対応を円滑に実施するために、システムを構成するハードウェアおよびソフトウェアの構成管理とバージョン管理を行う必要がある。 お客様は、の Config を通じて、クラウドリソースの集中監査とガバナンスを実現できます。これにより、お客様アカウント下の異なるリージョンにおける各種クラウドリソースの構成情報および構成変更を継続的に記録し、Tencent Cloud のベストプラクティスに基づくルールやコンプライアンスパッケージテンプレートに基づき、企業アカウント下のクラウドリソース構成に対して継続的なコンプライアンス評価を自動的に実施し、非標準的なリソース構成を特定することで、クラウドリソースの自動監視と管理を実現します。 顧客が規制要件を遵守できるよう、Tencent Cloud は構成管理データベース（CMDDB）を通じてハードウェアおよび設備の詳細なリストを管理しており、このリストには各サーバーのサポート終了日（End-of-Support Date）およびプラットフォームのバージョン情報が含まれています。Tencent Cloud は定期的にサーバーの退役および交換を行い、ソフトウェアコンポーネント（OS やデータベースシステムなど）については、サポート終了前に適切なバージョンへ更新します。 構成管理の面では、テンセントクラウドは社内ネットワークセキュリティ構成基準およびセキュリティベースライン基準を確立し、ネットワーク機器、ファイアウォール、ホストサーバーの OS、データベース、およびアプリケーションシステムの

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			セキュリティ構成を標準化して管理することを目的としています。テンセントクラウドは構成スキャンツールを通じて、OS、データベース管理システム、仮想イメージの構成と基準との乖離を継続的に検出しています。検出された乖離に対しては、テンセントクラウドが自動的にセキュリティチケットを生成し、担当チームに送信して、速やかに修正を行います。 変更管理に関しては、テンセントクラウド は製品および構成変更に関する管理基準を確立しており、変更プロセスにおける各ステップおよび関連する責任者を明確化することで、変更の実施前に適切な承認とテストが行われることを保証しています。テンセントクラウドの変更リリース管理手順は、構成ファイル、オペレーティングシステム、およびデータベースの変更を網羅しています。これらの変更は、本番環境への展開前に、業務への影響分析、独立した機能テストを実施し、変更のバックアップおよびロールバック計画を策定した上で、関連する責任者の承認を得る必要があります。Tencent Cloud の変更リリースシステムでは、変更操作は権限を持つ担当者のみが実行することを義務付けており、変更に関連するログを保存し、定期的に監査を行っています。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。 さらに、顧客に影響を及ぼす可能性のある運用・保守上の変更操作については、テンセントクラウドは公式サイトやサイト内メッセージなどのチャンネルを通じて、関連する顧客に変更通知を速やかに発信します。 サードパーティ製およびオープンソース 製品の使用に関しては、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

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			要件を策定しており、外部コンポーネントの導入時にセキュリティ承認審査を実施し、本番環境への移行前にセキュリティ強化と防御措置を講じ、製品がセキュリティチェックを通過することを保証しています。製品の本番環境移行後は、継続的なセキュリティ運用とセキュリティチェックを行い、セキュリティ問題を速やかに解決するとともに、製品のセキュリティ運用状況の評価を通じてセキュリティリスクを特定し、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。
実 49	機器の管理	【基礎】機器の管理方法を明確にすること。	顧客は、コンピュータシステムの各種機器を管理する必要があります。具体的には、管理責任者の明確化、機器情報の維持管理、機器の入在庫管理などを行います。 お客様による包括的な情報資産管理を支援するため、Tencent Cloud は Cloud Workload Protection Platform (CWPP) を提供しており、資産フィンガープリントの自動収集をサポートし、アカウント、ポート、プロセス、アプリケーションなどの資産フィンガープリントデータを一元管理します。CWPP はさらに、資産フィンガープリントに基づいて発生したセキュリティインシデントのリスク影響範囲を迅速に調査することができ、お客様のサーバーセキュリティの向上を支援します。また、お客様は 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 および Cloud Security Center (CSC) を利用して、情報資産のセキュリティ管理を行うことができます。CSC は資産セキュリティセンターの機能を網羅しており、クラウドサーバー、オブジェクトストレージ、クラウドデータベース、ロードバランサーなどのクラウド資産に対する

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			自動化された動的インベントリを実現します。さらに、クラウド構成のリスク、脆弱性、セキュリティインシデントなど、多角的なセキュリティ観点から資産のセキュリティリスクを一元管理し、クラウド上の「シャドウ IT」リスクを低減します。 お客様の規制要件への準拠を支援するため、情報資産管理の面において、Tencent Cloud は情報資産管理規範およびライフサイクル全体にわたる管理プロセスを策定し、電子データ、ハードウェアおよ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に対して、分類・格付けに基づく管理と保護を行っています。Tencent Cloud は、資産管理システムを通じてハードウェア機器およびソフトウェアコンポーネントを管理しています。これには、資産の登録および紐付け、資産の棚卸しおよび情報更新、資産の廃棄および交換などが含まれ、クラウドプラットフォームの基盤システムの安定した稼働を保証し、業務システムに信頼性の高いサポートを提供します。 設備の保守および入退室管理に関しては、テンセントクラウドは通信事業者に、各レベルのエリアセキュリティ要件に基づき、データセンター向けの厳格なインフラおよび環境アクセス制御を策定するよう求めています。あらゆる種類の訪問者や従業員がデータセンターに出入りする際は、本人確認と所持品の検査を行い、持ち込み物品を登録する必要があります。同時に、テンセントクラウドは、機器のサーバールームへの搬入・搬出（設置・稼働、廃棄、移設など）について、承認および検査プロセスを設定しています。機器資産の入出庫時には、関連する現場の資産管理者が入出庫作業指示書に基づき、厳格な検査と照合を行います。機器資産の入出庫引継ぎは、カメラで監視されている引継ぎエリアで行

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			われます。すべての入出庫引継ぎについては紙の引継ぎ伝票が作成され、伝票は3年間保存されます。
実 50	機器の管理	【付加】ネットワーク関連機器の保護措置を講ずること。	お客様は、重要データを処理するシステムで使用されるネットワーク機器（MDF、IDF、ルーター、ファイアウォールなど）に対して、適切な保護措置を講じる必要があります。 顧客が規制要件を遵守できるよう、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および多層防御システムを確立しています。テンセントクラウドは、管理制度およびプロセスを通じて、ネットワークセキュリティの管理・制御および保護基準、なら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のネットワーク上で提供されるサービスの安全な運用を確保しています。同時に、テンセントクラウドは内部ネットワーク監視システムを導入し、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、権限制御や承認プロセスなどの多重措置を通じて、権限のない者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ています。
実 51	機器の管理	【基礎】機器の保守方法を明確にすること。	お客様は、コンピュータシステムを構成する機器に対して保守点検を実施し、点検内容と結果を記録する必要があります。ハードウェアの故障を防止するため、お客様は機器の特性や重要度に応じて、定期的または随時、予防保守を実施する必要があります。
実 52	機器の管理	【付加】機器の予防保守を実施すること。	顧客が規制要件を遵守できるよう、Tencent Cloud は情報資産管理規範および全ライフサイクル管理プロセスを策定し、電子データ、ハードウェアおよ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

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			います。Tencent Cloud は資産管理システムを通じて、ハードウェア機器およびソフトウェアコンポーネントの管理（資産登録および紐付け、資産棚卸および情報更新、資産の使用と修理、資産の廃棄および交換など）を行っています。テンセントクラウドは、インフラストラクチャの定期的な保守・点検を実施し、その記録を保持しています。スタッフがサーバールームに入り、機器の修理や保守を行う際は、所定の承認プロセスを遵守し、サーバールームの各種規定を厳格に遵守する必要があります。 また、テンセントクラウド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・アラートするとともに、エンドポイント検出および対応（EDR）ツールを導入し、ネットワーク全体のサーバー端末資産を包括的に監視・管理しています。 さらに、テンセントクラウドはデータセンター運営事業者に対し、現場スタッフを配置してサーバー室内の重要機器を定期的に巡回点検するよう求めています。また、あらかじめ設定された手順に従って巡回結果を記録し、異常を報告し、発見された問題を解決することで、安全上のリスクを迅速に発見・修復し、機器の安定稼働を保証しています。さらに、テンセントクラウドは運営事業者に対し、データセンターの重要機器の事前設定指標を 24 時間体制で監視するシステムを設置するよう求めています。異常が発生した場合は、自動的に現場スタッフにアラートを送信します。
実 53	コンピュータ関連設備の保守管理	【基礎】コンピュータ関連設備（コンピュータシステムに関連する電源、空調、給排水、防災、防犯、監視及び配線等の設備を含む）の管理方法を明確にすること。	お客様は、コンピュータシステムの運用に関連する電源、空調、給排水、防災、防犯、監視および配線等の設備について、管理責任者および管理方法を明確にし、定められた方法に従って管理を行うとともに、故障や災害発生時の対応方法を明確にする必要があります。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			顧客が規制要件を遵守できるよう、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、操作の安全性を規範化し、リスクを適時に特定し、物理的セキュリティ管理を強化しています。 Tencent Cloud のデータセンターは、すべて関連する国際基準および現地の安全要件に従って立地選定、建設、または賃貸が行われています。現在、Tencent Cloud は日本で2つの賃貸型データセンターを展開しています。データセンターのレジリエンスと安全性を確保するため、Tencent Cloud はデータプロバイダーの選定、契約上の制約、継続的な監視などの側面から厳格な管理体制を構築しています。Tencent Cloud は、毎年定期的に実施される内部および外部監査を通じて、オペレーターのデータセンターに対して現場検査を行い、オペレーターのデータセンターが Tencent Cloud が定める情報セキュリティ要件に準拠していることを確認しています。 テンセントクラウドは、データセンター事業者に対し、煙探知機、避雷・接地装置、火災報知器およびスプリンクラー消火システム、電源システム、分流回路システム、外気導入システム、空調システム、温度監視装置の設置を義務付けており、24 時間体制でのメンテナンスおよび設備故障の迅速な解決のための要員配置を求めています。また、物理的セキュリティに関する緊急対応計画を策定し、データセンタースタッフによる定期的なセキュリティ訓練の実施も求めています。
実 54	コンピュータ関連設備の保守管理	【基礎】コンピュータ関連設備の保守方法を明確にすること。	顧客は、コンピュータシステムの稼働に関連する電源、空調、給排水、防災、防犯、監視および配線等の設備に対し、保守点検を実施し、点検内容および結果を記録しなければならない。 顧客が規制要件を遵守できるよう、テンセントクラウドはデータセンター運営事業者に対し、電源、空調、給排水、防災、防

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			犯、監視、配線等の設備について定期的な保守点検を実施し、設備の故障を迅速に解決するための体制を整えることを求めています。また、テンセントクラウドは運営事業者に対し、警備員を配置し、点検リストおよび点検計画に基づき各サーバーームおよび設備の状態を厳格に巡回点検させ、各点検ポイントで署名および点検時刻を記録することを求めています。
実 55	コンピュータ関連設備の保守管理	【基礎】コンピュータ関連設備の能力及び使用状況の確認を行うこと。	顧客は、コンピュータシステムの稼働に関連する電源、空調、給排水、防災、防犯、監視、および配線等の設備の容量と性能限界を把握し、その使用状況を監視しなければならない。 データセンターのレジリエンスと安全性を確保するため、テンセントクラウドはデータプロバイダーの選定、契約上の制約、継続的な監督などの側面から厳格な管理体制を構築している。テンセントクラウドは、データセンター事業者に対し、電源、空調、給排水、防災、防犯、監視、配線などの設備を監視・保守し、設備の異常を速やかに発見して迅速に解決することを求めている。テンセントクラウドは、毎年定期的実施される内部・外部監査を通じて、事業者のデータセンターに対して現場検査を行い、事業者のデータセンターがテンセントクラウドが定める情報セキュリティ要件を満たしていることを確認する。
実 56	入退館（室）管理	【基礎】入館（室）の資格付与及び鍵の管理を行うこと。	顧客は、データセンターおよびコンピュータ室などの重要エリアについて、入退室管理および鍵の管理を行うものとする。 顧客が規制要件を遵守できるよう、テンセントクラウドはデータセンター事業者、エリアごとのセキュリティ要件に応じて厳格なインフラおよび環境へのアクセス制御を策定し、入退室管理および鍵管理制度を制定することを求めています。 テンセントクラウドは、オペレーターに対し、入退室管理システムを設置し、人員の区分およびアクセス権限に基づき、データ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			センターの入退室管理システムにおいて完全な人員アクセス制御セキュリティマトリックスを構築することを求めています。また、人員の入退室権限を定期的に審査し、権限の付与または取り消しの記録を保持することで、データセンターにおける各種人員のアクセスや操作などの行動を効果的に管理することを実現します。 鍵の管理に関しては、テンセントクラウドは事業者に対し、各エリアの鍵に対応する管理者または部門を適切に指定し、鍵を技術的な手段で隔離された安全な場所（パスワードロック付きの金庫や施錠可能なキャビネットなど）に適切に保管することを求めています。また、鍵の貸出申請および承認プロセスを明確にし、権限のない者が鍵を入手できないようにすることを求めています。
実 57	入退館（室）管理	【基礎】データセンターの入退管理を行うこと。	顧客は、入退館者の資格を確認することにより、データセンターへの出入りを管理し、不正侵入、危険物の持ち込み、物品の不正持ち出しなどの行為を防止しなければならない。 顧客が規制要件を遵守できるよう、Tencent Cloud はデータセンター事業者に対し、データセンターへの物理的アクセスについて正式なアクセス手順を設定し、データセンターに入る人員の身元確認を行い、携行物の検査および登録を行うことを求めています。Tencent Cloud は、データセンター事業者に対し、アクセス権限が適切に割り当てられていることを確認し、関連性がなくなった、または不要なアクセス権限を速やかに無効化するため、データセンターのアクセス権限を定期的に見直すことを求めています。 外部訪問者のデータセンターへのアクセスに関しては、テンセントクラウドは運営事業者に対し、関連する訪問者申請および承認メカニズムを確立することを求めています。承認された訪問者のみが、合意さ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			れた時間および関連スタッフの同伴の下で、データセンターの指定エリアにアクセスすることを許可します。
実 58	入退館 (室) 管理	【基礎】コンピュータ室等の入退管理を行うこと。	顧客は、コンピュータ室、データ保管室などの重要室に対し、出入管理を実施し、不正侵入、危険物の持ち込み、物品の不正持ち出しなどの行為を防止しなければならない。 顧客が規制要件を遵守できるよう、Tencent Cloud はデータセンター事業者、エリアのセキュリティレベルに応じた厳格なインフラおよび環境へのアクセス制御を策定することを求めています。また、テンセントクラウドは、オペレーターに対し、入退室管理システムを設置し、人員の区分およびアクセス権限に基づき、データセンターの入退室管理システムにおいて完全な人員アクセス制御セキュリティマトリックスを構築することを求めています。これにより、データセンターへの各種人員のアクセスや操作などの行為を効果的に管理・制御します。さらに、テンセントクラウドは、オペレーターに対し、サーバールームへの立ち入りには専任の担当者が同行すること、およびサーバールームに出入りする機器の登録を行うことを求めています。
実 59	入退館 (室) 管理	【基礎】入室後の作業を管理すること。	顧客は、コンピュータ室やデータ保管室などの重要区域への立ち入り後の業務・活動を管理する必要があります。 顧客が規制要件を遵守できるよう、Tencent Cloud はデータセンター運営事業者に対し、各レベルのエリアセキュリティ要件に基づき、厳格なインフラおよび環境へのアクセス制御を策定することを求めています。Tencent Cloud は、運営事業者に対し、入退室管理システムを設置し、人員の区分およびアクセス権限に基づき、データセンターの入退室管理システムにおいて完全な人員アクセス制御セキュリティ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			イマトリックスを構築することを求めています。さらに、Tencent Cloud は、運営事業者に対し、サーバールームへの立ち入りには専任の担当者が同行し、サーバールームに出入りする機器を登録することを求めています。
実 60	監視	【基礎】各種設備の監視体制を整備すること。	顧客は、コンピュータシステムの正常な稼働を保障するための設備（電源、空調、給排水、火災報知、監視カメラ等の設備を含む）について、相応の監視体制を確立し、監視対象、監視内容および監視方法を明確にするものとする。 顧客が規制要件を遵守できるよう、テンセントクラウドはデータセンター事業者に、電源、空調、給排水、防災、防犯、監視、および回線などの設備の監視と保守を求め、設備の異常を速やかに発見し、迅速に解決することを求めています。テンセントクラウドは、毎年定期的実施される内部および外部監査を通じて、事業者のデータセンターに対して現場検査を行い、事業者のデータセンターがテンセントクラウドが定める情報セキュリティ要件に準拠していることを確認します。

5.2.5 緊急時の対応

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 70	障害時・災害時対応策	【基礎】障害時・災害時の関係者への連絡手順を明確にすること。	お客様は、障害や災害発生時に迅速かつ正確に関係者に連絡できるよう、連絡手順を確立する必要があります。 Tencent Cloud の事業継続性に関する手順書では、災害発生時の内部・外部への連絡方針を明確化しており、コンソール上の告知、公式サイト、サイト内メッセージ、SMS、電子メールなど、多角的な連絡手段を整備し、顧客に影響を及ぼす可能性のある事象を速やかに通知できるようにしています。 Tencent Cloud は、クラウドコンソールを

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			通じてチケットサービスを提供し、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、苦情の報告をサポートしています。Tencent Cloud のチケットシステムは、段階的な対応メカニズムを通じて顧客のチケットに優先順位を割り当てます。第一線の技術チームが効果的に解決できない場合、システムは自動的にサービスエスカレーションプロセスをトリガーし、製品または技術チームが介入して共同で処理することで、顧客の要望やフィードバックが迅速に対応・処理されることを保証します。また、Tencent Cloud は公式ウェブサイト上でオンラインおよび電話による窓口を提供し、Tencent Cloud サービスの利用中に発生した問題についてお客様からのフィードバックを受け付けています。Tencent Cloud は複数の地域に相互バックアップ体制を備えたカスタマーサービスセンターを保有しており、お客様からの問い合わせや要望に 24 時間 365 日体制で対応し、高品質かつ 24 時間体制の技術サポートを提供しています。さらに、お客様は適切なサービスプランを選択することで、専用サポートグループ、専任のテクニカル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受けることができます。 現地サポートに関しては、テンセントクラウドは情報セキュリティ連絡担当者を配置しています。各地域の情報セキュリティ連絡担当者は、コンプライアンスおよび業務要件に基づき、現地の規制当局やお客様と円滑なコミュニケーションを図り、テンセントクラウドが法令、規制、および契約を遵守するよう確保します。
実 71	障害時・災害時対応策	【基礎】障害時・災害時復旧手順を明確にすること。 クラウド利用の場合、クラウド事業者に対して、金融機関等が障害	顧客は、障害または災害によりコンピュータシステムが正常に稼働しなくなった後の復旧手順を明確にし、それが緊急時対応計画と整合していることを確保しなければならない。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		時・災害時の復旧手順を作成するに当たり、金融機関等が利用できる機能や手段を確認することが必要である。金融機関等においては、障害時・災害時の復旧で必要とする要件が、クラウド事業者が提供する機能や手段では実現できない場合、金融機関等はそれを補う機能や手段を検討することが必要である。 クラウド利用の場合、クラウド事業者に対して、金融機関等が策定した稼働確認の水準を充足しているか、確認することが必要である。確認する観点としては、以下の例がある。 (1) クラウド事業者が行うクラウドサービスの障害時・災害時を考慮した切替テストの内容、頻度、テスト結果等。 (2) バックアップ機能のテスト手順	テンセントクラウドは、世界各国の関連国際基準および現地のセキュリティ要件に基づき、データセンターを建設またはリースしており、顧客に複数の地域およびアベイラビリティゾーンの選択肢を提供することで、業務の災害対策要件とサービスレベルを保証しています。 サイバーセキュリティインシデント発生後、顧客が迅速に対応し、重要な機能を復旧できるよう、Tencent Cloud が提供するコンピューティングサービス、ネットワークサービス、ストレージサービス、データベースサービス、コンテナおよびミドルウェアサービスなど、多種多様なクラウド製品・サービスはすべて高可用性を備えており、顧客のシステムやサービスの高可用性実現を支援します。例えば： • <u>Cloud Load Balancer (CLB)</u> は、安全かつ高速なレイヤー4/7 トラフィック分散サービスを提供し、トラフィック分散を通じてアプリケーションシステムの対外サービス能力を拡張し、単一障害点を排除します。CLB はクラスタ化された展開を採用しており、障害発生インスタンスを速やかに排除することで、高可用性を実現します。 • <u>Cloud Virtual Machine (CVM)</u> は、サービスの高可用性とデータの高度な信頼性を備えています。CVM に搭載されたクラウドディスクは 3 レプリカのストレージポリシーを採用しており、いずれかのレプリカに障害が発生した場合でも、データの迅速な移行と復旧を保証します。 • <u>Cloud Object Storage (COS)</u> は、複数のアーキテクチャやデバイスにまたがる冗長ストレージを提供し、ユーザーのデータに対して遠隔地での災害対策

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			やリソース分離機能を提供することで、データの永続性を実現します。 Cloud Native Database TDSQL-C (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あり、高可用性クラスターアーキテクチャを採用しています。障害が発生したノードを自動的に検出し、秒単位でのフェイルオーバーと復旧をサポートします。 TencentDB for MySQL は、データの高信頼性とサービスの高可用性を実現し、充実したデータの自動バックアップおよびロスレス復旧メカニズムを備えています。 Tencent Kubernetes Engine (TKE) は、分散型サービスアーキテクチャを採用し、サービスの障害自動復旧と迅速な移行を保証します。ステートフルサービスバックエンドの分散型ストレージと組み合わせることで、サービスとデータの安全性および高可用性を実現します。 災害復旧の面では、Tencent Cloud は包括的な事業継続マネジメントシステムを構築し、ISO/IEC 22301 事業継続マネジメントシステムの国際標準認証を取得しています。Tencent Cloud はクラウド製品および重要なプロセスに対して詳細な災害復旧計画を策定し、その実行可能性を確保するために要件に従って定期的に演習を実施しています。Tencent Cloud の災害復旧演習は、攻撃・防御の対抗演習や大規模障害など、現実的な典型的な災害シナリオを模擬して実施されることが多く、システムの災害耐性、応答速度、復旧能力を包括的に検証しています。演習で発見された問題に対しては、Tencent Cloud は演習の総括報告書で提示された改善策に基づき是正

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 72	障害時・ 災害時対応策		措置を講じ、速やかに対応する緊急対応計画を改訂するとともに、監査部門が是正状況を監督・検査します。 さらに、テンセントクラウドは定期的にバックアップ復旧テストを実施し、データの完全性と復旧可能性を検証することで、バックアップデータの保存セキュリティと利用の信頼性を確保しています。
		【基礎】障害の原因を調査・分析すること。 クラウド利用の場合、クラウド事業者に対して、クラウド事業者の責任範囲における障害発生後の調査状況を把握する手段・方法を確認することが必要である。クラウド利用の場合、金融機関等においては、クラウド利用時の障害の事前防止策を検討することが望ましい。	顧客は障害について調査を行い、発生原因を記録し、傾向分析などを通じて同様の障害の再発を防止する。 顧客が規制要件を遵守できるよう、インシデント対応および処置に関して、テンセントクラウドは情報セキュリティインシデント管理規範を策定し、情報セキュリティ報告、対応、処理のメカニズムおよび関連プロセスを確立している。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する。検知・識別されたセキュリティインシデントに対し、テンセントクラウドはインシデントの性質、データの機密性、影響範囲などの要因を総合的に考慮して分析・分類を行い、速やかに担当責任者に通知してインシデントの処理をフォローアップさせる。 テンセントは、「情報・攻防・管理・計画」からなる能動的防御セキュリティ能力体系の構築に注力しており、脅威インテリジェンス、人工知能、ビッグデータなどの技術を統合することで、セキュリティインシデントへの対応能力と効率を向上させています。 インシデントの総括と継続的改善の面において、テンセントクラウドは定期的なインシデント分析メカニズムを確立しており、定期的にインシデントを多角的に分析（インシデントの種類、発生頻度、影響範囲、深刻度）しています。また、インシデ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ントの振り返りと根本原因分析に基づき、予防措置を講じ、同様のインシデントの再発を防止しています。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立ち上げ、特別分析レポートを作成して経営陣に報告します。
			お客様は、突発的な災害、事故、障害、またはサイバー攻撃などの状況に備えた緊急対応計画を策定し、定期的に見直し、必要に応じて更新する必要があります。クラウドサービスを利用する際、お客様は緊急対応計画の発動条件やシステムの構成状況などを考慮して計画を策定する必要があります。
			お客様のビジネスの継続的かつ安定した可用性を確保するため、Tencent Cloud は世界各国の関連国際基準および現地のセキュリティ要件に基づき、データセンターを建設またはリースし、お客様にマルチリージョン (region)、マルチアベイラビリティゾーン (zone) の選択肢を提供しています。現在、テンセントクラウドは日本国内に、電力およびネットワークが相互に独立した2つのレンタル型データセンターを保有しており、日本国内でのデータの保存、処理、およびバックアップをサポートしています。お客様は、事業の発展ニーズやデータセキュリティ要件に基づき、データやシステムを異なるリージョンやアベイラビリティゾーンに自主的かつ柔軟に展開することができます。
実 73	コンティンジェンシープラン策定	【基礎】コンティンジェンシープランを策定すること。 クラウド利用の場合は、金融機関等においては以下の観点でコンティンジェンシープランを検討することが必要である。 (1) コンティンジェンシープランの発動条件; (2) システムの構成 (システムをマルチリージョン又はマルチアベイラビリティゾーンで構築することを考慮する)。	また、Tencent Cloud はクラウド製品およびサービスの事業影響度分析結果に基づき、異なる対応戦略と事業継続計画を策定しています。クラウド製品および重要なプロセスに対して詳細な災害復旧計画を策定しており、関連する戦略、計画、および対応案は、場所、人員、設備、システム、情報データなどの重要領域をカバーし、業務の優先順位に基づいて対応する災害復旧プロセスを策定し、災害対策システムの

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			完全性 秩序性 実行可能性を確保します。 さらに、テンセントクラウドは毎年、事業継続マネジメントシステム (BCM) の見直しと更新を行い、事業影響度分析の結果に基づき、関連する製品およびサービスの事業継続計画 (BCP) と災害復旧計画 (DRP) を精査し、必要に応じて更新しています。また、内部の事業継続管理規定に基づき、テンセントクラウドは緊急時対応連絡リストを管理しており、当該リストに掲載された関係者の連絡先が常に正確かつ有効であるよう、専任者を指定して管理しています。
73-1	コンティンジェンシープラン策定	【基礎】サイバー攻撃を想定したインシデント対応計画及びコンティンジェンシープランを策定すること。	顧客は、サイバー攻撃を受けた際に重大な損害が生じ、業務の遂行が困難になった場合、損害の範囲と業務への影響を最小限に抑え、迅速に復旧できるよう、サイバー攻撃に対するインシデント対応計画および緊急対応計画を策定する必要があります。 顧客が規制要件を遵守できるよう、テンセントクラウドはサイバーセキュリティ緊急対応計画を策定しており、サイバー攻撃、マルウェア、データセキュリティ、設備・施設の故障、災害事象など、多岐にわたるサイバーセキュリティ緊急事態を網羅している。テンセントクラウドは、緊急対応計画体系の確立を基盤とし、緊急対応チームの構築を支えとし、緊急対応プロセスの標準化を重点として、監視・早期警戒、通報・対応などの業務能力を継続的に強化し、サイバーセキュリティインシデントによる悪影響を予防・軽減しています。テンセントクラウドは、サイバーセキュリティ緊急対応計画の有効性を確保するため、定期的な見直し、更新、およびテストを実施しています。
実 74	)バックアップサイト	【付加】バックアップサイトを保有すること。 クラウド利用の場合、クラウド事業者に対して、金融機関等で策定	顧客は、業務の優先度を考慮した上で、異なる地域にバックアップサイトを保有すべきである。 Tencent Cloud のデータセンターは世界中の複数の地域に展開されており、顧客は二

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		したバックアップに関する基準を充足しているかを確認することが必要である。確認する観点としては、以下の例がある。 (1) 本番サイトとバックアップサイトそれぞれのゾーン、リージョンがリスク分散された距離にあるか。 (2) 被災時のサービス継続仕様。	ーズに応じてデータやシステムを異なる地域やアベイラビリティゾーンに展開できる。Tencent Cloud のデータセンターは、関連する国際基準および現地のセキュリティ要件に従って立地選定、建設または賃貸されており、高安定性の電力システムや空調システム、完備された消防システム、静電気防止設備などを備えている。また、各レベルの地域セキュリティ要件に基づき、厳格なインフラおよび環境へのアクセス制御を策定している。現在、テンセントクラウドは日本国内に、電力およびネットワークが相互に独立した2つのレンタル型データセンターを保有しており、日本国内でのデータの保存、処理、およびバックアップをサポートしています。お客様は、事業の発展ニーズやデータセキュリティ要件に基づき、データやシステムを異なるリージョンやアベイラビリティゾーンに自律的かつ柔軟に展開し、異なる事業継続モデルを採用することで、事業の災害復旧要件を保証することができます。 さらに、顧客のビジネスの継続的な可用性を確保するため、Tencent Cloud が提供するコンピューティングサービス、ネットワークサービス、ストレージサービス、データベースサービス、コンテナおよびミドルウェアサービス、セキュリティサービスなど、多種多様なクラウド製品・サービスはいずれも高可用性を備えており、対応する災害復旧計画も整備されています。

5.2.6 システム開発・変更

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 75	システム 開発・変更管理	【基礎】システムの開発・変更手順を明確にすること。 システムで利用するサードパーティのライブラリやミドルウェア、ハードウェアについては、不正侵入の経路となるバックドア等が含	顧客は、システム開発および変更内容の正当性を確保するため、開発および変更のプロセスを明確にすべきである。システムで使用されるサードパーティ製ライブラリ、ミドルウェア、およびハードウェアについては、顧客は「セキュリティ・バイ・デザイン」や「セキュリティ・バイ・デフォルト

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		まれることのないように、セキュリティ・バイ・デザインやセキュリティ・バイ・デフォルト等の安全な開発手法を製品開発に取り入れている事業者から提供される安全なプロダクトを選定することが望ましい。	ト」などの安全な開発手法を採用しているベンダーが提供する安全な製品を優先的に選択すべきである。 Tencent Cloud は、顧客の開発ライフサイクル管理を支援・サポートするために、以下の開発ツールを提供しています： • Cloud Native Build (CNB) : 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にソフトウェアを構築できるよう支援することを目的としています。CNB は、コードホスティング、高性能な開発パイプライン、AI コードレビュー、クラウド上の開発環境、アーティファクト管理、カスタムタスクセットなどの機能を備えた完全な開発者ツールチェーンを提供し、要件からデプロイまでの開発全プロセスのサポートおよびアジャイル開発管理を効果的に実現します。 テンセントクラウド内部でも情報システムセキュリティ開発基準を確立しており、ISO/IEC 20000 情報技術サービス管理規格、ISO/IEC 27001 情報セキュリティマネジメントシステム、および ISO/IEC 9001 品質マネジメントシステム規格を製品セキュリティ開発ライフサイクルの全プロセスに統合することに注力しています。要件定義、設計、開発、テスト、納品、運用保守などの各段階に焦点を当て、製品開発のあらゆる段階で情報セキュリティとプライバシー保護の理念を取り入れ、クラウド製品がそのライフサイクルを通じて十分なセキュリティ管理を受けられるようにしています。関連するセキュリティ管理措置には以下が含まれます： • セキュリティ研修: セキュアコーディング研修を通じて開発者のセキュリティ意識を醸成し、関係者にセキュリティコーディング規範の厳格な遵守を求めま

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			す; - 要件分析: 業務内容、業務プロセス、技術フレームワークについて協議し、セキュリティを組み込む最適な方法を模索します; - システム設計: システム設計に対して脅威モデリングを行い、採用するアーキテクチャのセキュリティ技術評価を実施します; - システム開発: 開発プロセスにおいて、テンセントが独自に設計したセキュア開発コンポーネントを開発担当者に提供し、テンセントクラウドのセキュアコーディングガイドラインに従ってコーディングを行う; - セキュリティ検証: コードセキュリティチェック、資産セキュリティスキャン、Web スキャン、手動によるセキュリティ評価、ペネトレーションテスト、コード監査などを通じて脆弱性を発見します; - リリース: セキュリティ部門による最終チェックと確認を経て初めて、システムは本番環境にリリースされます。これにより、セキュリティ上の脆弱性を抱えた製品が本番環境で稼働することを防ぎます。 変更管理に関しては、Tencent Cloud は製品および構成の変更に関する管理基準を確立し、変更プロセスにおける各ステップおよび関連責任者を明確化することで、変更の実施前に適切な承認とテストが行われることを保証しています。同時に、Tencent Cloud は緊急変更の管理プロセスを定義しており、緊急変更は適切な承認を得た上で実施されます。さらに、顧客に影響を及ぼす可能性のある運用・保守上の変更操作については、Tencent Cloud は公式サイトやサイト内メッセージなどのチャネルを通じて、関連する顧客に変更通知

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			を速やかに発信します。 サードパーティ製またはオープンソース製品の使用に関しては、テンセントクラウドはソフトウェアサプライチェーンのセキュリティ管理要件を策定し、外部コンポーネントの導入時にセキュリティ承認審査を実施すること、本番環境への移行前にセキュリティ強化と防御措置を講じること、および製品がセキュリティチェックを通過することを明確にしています。製品の本番環境移行後は、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するとともに、製品のセキュリティ運用状況の評価を通じてセキュリティリスクを特定し、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。
実 76	システム 開発・変 更管理	クラウド利用の場合、クラウド事業者に対して、金融機関等で策定したセキュリティ基準を充足しているかを確認することが必要である。確認する観点としては、以下の例がある。 (1) クラウドサービスで構築するシステムについて、安全に本番環境とテスト環境を分離する方法や機能; (2) 本番環境とテスト環境を分離した際のプログラムやデータ等の連携方法。	顧客は、本番環境に影響を与えないテスト環境を構築し、本番環境に影響を与えないことを前提として、システム開発および変更に関連するテストを実施すべきである。 顧客のクラウド開発を支援するため、お客様は Cloud Native Build (CNB) を利用して、開発/テスト環境を作成・利用することも可能です。CNB は数秒で起動するクラウドコンテナ環境を提供し、開発者にコーディング、コンパイル、実行、および自己テストの機能を提供することで、クラウド上での開発を支援します。CNB では、デフォルトの開発環境またはカスタム開発環境の使用が可能です。 分離要件については、Tencent Cloud は Virtual Private Cloud (VPC) も提供しており、お客様が購入したクラウドプラットフォームリソースに対して複数の独立したネットワーク空間を構築し、ネットワークセグメントの分割、IP アドレス、ルーティングポリシーなどをカスタマイズする

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ことをサポートしています。VPC サービスは、Tencent Cloud 上に構築された専用のクラウドネットワーク空間です。プライベートネットワーク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、仮想化技術を用いて異なるプライベートネットワーク間の内部ネットワークを完全に分離することで、独立かつ隔離された安全なクラウドネットワークを顧客に提供します。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およびネットワーク ACL ルールを設定することで、インスタンスレベルおよびサブネットの入出力トラフィックを制御し、多層的なネットワークアクセス制御を実現します。 お客様の規制要件への準拠を支援するため、Tencent Cloud は、開発・テスト環境と本番環境が相互に隔離されていることを保証し、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ます。
実 77	システム 開発・変更管理	【基礎】本番への移行手順を明確にすること。	お客様は本番環境への移行プロセスを明確にし、移行時には各システムの特徴を考慮して、移行プロセス中の障害を防止する必要があります。 お客様が業務を安全にクラウドへ移行できるよう支援するため、Tencent Cloud は Cloud Migration (CMG) サービスを提供しています。 Cloud Migration (CMG) は、Tencent Cloud が提供する移行ツールの統合および監視プラットフォームであり、Tencent Cloud 公式の移行ツールを提供するとともに、公式認定のサードパーティ製移行ツールを統合しており、お客様がシステムを便利かつ迅速にクラウドへ移行できるよう支援します。Tencent Cloud は、サードパーティ製移行ツールの機能と移行実績について厳格な

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			評価と認証を行い、ユーザーが選択したソリューションとツールがすべて安全かつ信頼できるものであることを保証します。クラウド移行は、すべての移行タスクの統一的な監視をサポートし、視覚的なグラフ形式で表示することで、ユーザーが移行の進捗状況を明確に把握できるよう支援します。
実 78	開発・変更時ドキュメント管理	【付加】開発・変更時のドキュメントの作成手順を明確にすること。	開発および変更に関連するドキュメントを適切に作成するため、お客様は作成すべきドキュメントの範囲を明確にし、その作成プロセスを策定する必要があります。また、お客様は開発および変更時のドキュメントの保管・管理方法を明確にし、ドキュメントの保管と管理を適切に行う必要があります。
実 79	開発・変更時ドキュメント管理	【基礎】開発・変更時のドキュメントの保管管理方法を明確にすること。	顧客が規制要件を遵守できるよう、Tencent Cloud は文書管理に関する手順とプロセスを確立しています。開発および変更期間中に作成される文書は、関連する要件に従って作成、承認、公開、使用、修正、識別、保存、および廃棄されます。
実 82	システムの廃棄	【基礎】システムの廃棄計画を策定するとともに、廃棄手順を明確にすること。 クラウドサービスを利用する場合、廃棄計画の策定及び実行のため、クラウドサービス提供者に対してデータ廃棄方法を確認する必要がある。	顧客はシステムの廃棄計画を策定し、廃棄手順を明確にした上で、承認を得て廃棄を行うものとする。顧客はシステムの廃棄を行う際、情報漏洩を防止するための対策を講じる必要がある。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーに対してデータの廃棄方法を確認する必要がある。 データの削除および破棄に関して、Tencent Cloud は安全かつ信頼性の高いデータ破棄メカニズムを提供しています。お客様のサービス終了後、テンセントクラウドはお客様とのサービス契約に基づき、厳格なデータ消去手順に従い、保存期間満了後に複製やバックアップを含むお客様データを完全に削除します。削除されたデータは復元できません。テンセントクラウドサービスの提供に使用される媒体に故障が発生し交換が必要となった場合、または
実 83	システムの廃棄	【基礎】システム廃棄時の情報漏えい防止対策を講ずること。	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			使用期限が到来し廃棄が必要となった場合、テンセントクラウドは速やかに厳格な手順に従い、徹底的な物理的破棄を行います。

5.2.7 システムの信頼性向上対策

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 84	ハードウェアの予備	【付加】本体装置の予備を設けること。	主要機器に障害が発生した場合に迅速に対応できるよう、お客様はコンピュータシステムの核心となる重要な主要機器に対して予備機器を配備する必要があります。また、重要な周辺機器に対しても予備機器または代替機能を配備する必要があります。高い信頼性が求められるファイルについては、二重化を検討する必要があります。 Tencent Cloud のデータセンターは世界中の複数の地域に展開されており、リージョン (region) とアベイラビリティゾーン (zone) で構成され、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ています。現在、Tencent Cloud は日本で 2 つの専用データセンターを展開しています。お客様は、ビジネスの発展ニーズやデータセキュリティ要件に応じて、データやシステムを異なるリージョンやアベイラビリティゾーンに柔軟に配置し、さまざまな事業継続モデルを採用することで、ビジネスの災害対策要件を満たすことができます。 また、テンセントクラウドが提供する多種多様な製品は、高い可用性を備えており、お客様のシステムやサービスの高可用性実現を支援します。例えば： • Cloud Virtual Machine (CVM) は、サービスの高可用性とデータの信頼性を備えています。CVM に搭載されたクラウドディスクは 3 レプリカのストレージ
実 85	ハードウェアの予備	【付加】周辺装置の予備を設けること。 ここの周辺装置とは、ファイル装置（磁気ディスク装置、半導体ディスク装置、光磁気ディスク装置、磁気テープ装置等）、コンソールディスプレイ等を指す。	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ージ戦略を採用しており、いずれかのレプリカに障害が発生した場合でも、データの迅速な移行と復旧を保証します。 <u>Tencent Kubernetes Engine (TKE)</u> は、分散型サービスアーキテクチャを採用しており、サービスの自動復旧と迅速な移行を保証します。ステートフルサービスのバックエンドである分散型ストレージと組み合わせることで、サービスとデータの安全性および高可用性を実現します。 <u>Cloud Load Balancer (CLB)</u> は、安全かつ高速なレイヤー4 およびレイヤー7 のトラフィック分散サービスを提供し、トラフィック分散を通じてアプリケーションシステムの対外的なサービス能力を拡張し、単一障害点を排除します。CLB はクラスタ化されたデプロイメントを採用しており、障害発生したインスタンスを速やかに排除することで、高可用性を実現します。 <u>Cloud Block Storage (CBS)</u> は、3 レプリカの分散メカニズムを採用しています。そのバックエンドのデータ複製メカニズムは、いずれかのレプリカに障害が発生した場合、データ移行などの手段を通じて迅速に新しいレプリカを複製し、常に3つのレプリカが利用可能であることを保証することで、ユーザーに安全で安心なデータストレージサービスを提供します。クラウドディスクのデータはラックを跨いで保存され、高い信頼性を確保しています。 お客様の規制要件への準拠を支援するため、Tencent Cloud は自社のクラウド環境に適した事業継続管理フレームワークを設計・実装し、包括的な事業継続管理体制を構築しました。また、ISO/IEC 22301 事業継続管理システムの国際標準認証を取

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			得しています。お客様のビジネスの継続的な可用性を保証するため、Tencent Cloud はサーバー、ネットワーク機器、セキュリティ機器などのハードウェアに冗長化またはホットスタンバイ機構を設け、ハードウェア障害時でもデータが失われず、業務を復旧できるようにしています。 ハードウェア機器の故障や問題を迅速に発見・対処するため、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などの資産を管理しています。これには、資産の登録および紐付け、資産の棚卸しおよび情報更新、資産の廃棄および交換などが含まれ、クラウドプラットフォームの基盤システムの安定した稼働を保証しています。テンセントクラウドは、データセンター運営会社の担当者に、点検リストおよび点検計画に基づき、各サーバールームおよび機器の状態について毎日厳格に点検を行うよう求めています。各点検ポイントで署名と点検時刻を記録し、インフラの障害やセキュリティインシデントを発見した場合は、直ちに対応する対応プロセスを起動します。 バックアップ管理に関しては、テンセントクラウドはバックアップ管理手順を策定しています。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基づき、顧客に複数のストレージコピーおよびバックアップサービスを提供します。テンセントクラウドは、リアルタイムのホットバックアップ、冗長ストレージ、遠隔地バックアップなどの方式を採用し、顧客のクラウド上の業務およびデータの安全性、信頼性、継続的な可用性を確保しています。バックアップに関する詳細については、本ガイドの第 5.2.3 章「実 39 データファイル管理」の条項をご参照ください。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 86	ハードウェアの予備	【付加】通信系装置の予備を設けること。	通信機器の故障発生時に迅速に対応できるように、顧客は重要な通信機器に予備機器を配備すべきである。 ネットワークのレジリエンスを保護するため、Tencent Cloud はデータセンター事業者、データセンターのネットワーク出口を複数の通信事業者と接続し、Tencent Cloud ネットワークの地域を跨ぐ災害対策能力を構築するよう求めている、通信事業者のパブリックネットワーク障害による継続的な影響を効果的に低減している。テンセントクラウドの基盤ネットワークは、冗長構成を採用しており、ルーティング階層における経路優先度およびルーティング到達可能性に基づくトラフィックエンジニアリングの調整と組み合わせることで、単一の機器障害によるネットワークサービスの中断を防止しています。さらに、テンセントクラウドは、通信機器の障害に迅速に対応できるように、ネットワーク機器などのハードウェアに対して冗長化および予備部品体制を整備しています。
実 87	ハードウェアの予備	【付加】回線の予備を設けること。	回線障害発生時に迅速に対応するため、顧客は重要な回線に対して予備回線を配備すべきである。 ネットワークのレジリエンスを保護するため、Tencent Cloud はデータセンター事業者、データセンターのネットワーク出口を複数の通信事業者と接続し、異なる通信事業者の回線をバックアップとして提供することを求めています。これにより、Tencent Cloud ネットワークの地域を跨ぐ災害対策能力を構築し、通信事業者のパブリックネットワーク障害による継続的な影響を効果的に低減します。Tencent Cloud の基盤ネットワークの冗長構成を採用しており、ルーティング階層における経路優先度およびルーティング到達可能性に基づくトラフィックエンジニアリングのスケジューリングと組み合わせることで、単一の機器障害によるネットワークサービスの中断を防止します。Tencent

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			Cloud のコンピューティングノードもの冗長構成を採用しており、単一のコンピューティングノードに障害が発生した場合、スケジューラーによってリアルタイムで自動的に除外されるため、顧客のビジネスの可用性を効果的に保証します。
			顧客は、セキュリティ・バイ・デザイン (Security by Design) を実施できる体制を構築し、システム計画段階で必要なセキュリティ機能を明確に組み込む必要があります。
			顧客が規制要件を遵守できるよう、テンセントクラウドは情報システムセキュリティ開発基準を確立し、ISO/IEC 20000 情報技術サービス管理規格、ISO/IEC 27001 情報セキュリティマネジメントシステム、および ISO/IEC 9001 品質マネジメントシステム規格を、製品のセキュリティ開発ライフサイクル全プロセスに統合することに注力しており、要件定義、設計、開発、テスト、納品、運用保守などの各段階に重点を置いています。テンセントクラウドは、製品開発の各段階にセキュリティチームを参画させ、セキュリティ要件のチェックを行い、クラウド製品がそのライフサイクルを通じて十分なセキュリティ管理と評価を受けられるよう確保し、情報セキュリティおよびプライバシーリスクを低減しています。
実 89	ソフトウェア等の品質向上対策	【基礎】必要となるセキュリティ機能を取り込むこと。	テンセントクラウドは、要件分析段階において要件のセキュリティ分析および業務リスク分析を実施します。プロジェクトマネージャーがテストチームやセキュリティチームなどの関連チームを招集し、製品要件仕様書に対するセキュリティレビューを行い、業務内容、業務プロセス、技術フレームワークについて協議し、セキュリティを組み込む最適な方法を模索します。ここでいうセキュリティ要件には ID およびアクセス管理、データセキュリティ、ネットワークセキュリティ、セキュリティ監査などの分野が含まれますが、これらに限

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			定されません。
実 90	ソフトウェア等の品質向上対策	【基礎】設計段階におけるソフトウェアの品質を確保すること。	顧客はソフトウェア設計段階において、開発の前提条件を明確にし、信頼性設計や設計作業の標準化を考慮することで、設計段階におけるソフトウェアの信頼性を向上させるべきである。 顧客が規制要件を遵守できるよう支援するため、Tencent Cloud 製品のイテレーション要件は、ユーザー、プロジェクト投資家、製品ブレインストーミング、および運用活動から得られます。Tencent Cloud は要件分析段階において、要件のセキュリティ分析および業務リスク分析を実施します。プロジェクトマネージャーがテストチームやセキュリティチームなどの関連チームを招集し、製品要件仕様書に対するセキュリティレビューを行い、業務内容、業務プロセス、技術フレームワークについて協議し、セキュリティを組み込む最適な方法を探ります。 テンセントクラウドは、正式なレビューを経た製品要件を分析し、その複雑性に基づき、詳細な技術計画の策定が必要かどうかを関係者が判断します。技術計画には、全体設計、詳細設計、実装計画、テスト計画、リソース計画、リスク管理などが含まれます。プロジェクトマネージャーは、テストチームやセキュリティチームなどの関連チームを招集し、製品設計に対するセキュリティ分析および技術リスク分析を実施する。また、システム設計に対して脅威モデリングを行い、採用するアーキテクチャのセキュリティ技術評価を行うことで、機能要件が非安全な方法で実装されることを防ぐ。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 91	ソフトウェア等の品質向上対策	【基礎】プログラム作成段階における品質を確保すること。	顧客は、プログラミングに関する仕様書に基づいてコーディングを行い、プログラミング作業の標準化および自動化対策を講じる必要があります。Web システムについては、顧客はシステム構築時に Web アプリケーションの脆弱性対策を考慮する必要があります。 <u>Cloud Native Build (CNB)</u> は、完全な開発者ツールチェーンを提供し、コードホスティング、高性能な開発パイプライン、AI コードアシスタント、アーティファクト管理などの機能を備えています。その AI コードアシスタントは、Tencent Cloud が開発者向けに特別に設計した AI プログラミング支援機能であり、多数の主要プログラミング言語をサポートし、コード補完、ユニットテスト、コード診断、インテリジェントレビュー、コード問題に関するインテリジェント Q&A などの機能を提供し、開発者のコーディング品質と効率の向上を支援することを目的としています。 顧客が規制要件を遵守できるよう、Tencent Cloud は詳細なセキュアコーディングガイドラインを策定し、社内開発者にその厳格な遵守を求めています。また、セキュアコーディング研修を通じて、開発者のインジェクション攻撃や機密情報の漏洩などのリスクに対する認識を高めています。開発者は開発プロセスにおいて、アプリケーションシステムが備えるべきセキュリティ機能を考慮し、脆弱性の発生を最大限に回避する必要があります。Tencent Cloud の内部コードセキュリティ検査・分析ソリューションは、静的アプリケーションセキュリティテスト (SAST)、オープンソースコンポーネントの検出、機密情報の検出など、多様な機能を統合しています。業務チームはパイプラインを活用してスキャン機能を自律的に導入し、コードの受け入れ段階でマージされるコードのセキュリティ評価を行うことができま

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			す。コードレビューの過程で発見された典型的な問題は記録され、業務チームのナレッジベースに集約されます。コードレビューの基準は、主に XSS、SQL インジェクション、コード実行、コマンドインジェクションなど多言語にわたる脆弱性検出、サードパーティ製オープンソースコンポーネントに存在する過去の脆弱性、機密情報の保護などを網羅しています。
			顧客は、テスト計画の策定、テスト環境および体制の整備、テスト支援機能の活用、テスト段階における各種管理の実施などの対策を通じて、テスト段階におけるソフトウェアの信頼性を向上させるべきである。
			顧客が規制要件を遵守できるよう、Tencent Cloud の開発チームが新製品の開発を完了した後、または製品に重大な変更が生じた際、テスト担当者は製品要件に基づき対応するテスト計画とテストケースを作成し、プロジェクトチームを組織してテストケースのレビューを実施します。テストケースが承認された後、テストチームはプロジェクト製品に対して機能テストを実施し、製品の機能が利用可能かつ信頼性が高く、Tencent Cloud が内部で定めた製品品質要件を満たしていることを保証します。機能テスト完了後、セキュリティチームが製品に対してセキュリティテストを実施します。テストプロセスで発見された不具合や脆弱性は、Tencent Cloud の内部脆弱性管理プロセスに従って処理され、テスト担当者はテスト結果に基づいてテストレポートを作成し、各関連チームに提出して確認を求めます。
実 92	ソフトウェア等の品質向上対策	【基礎】テスト段階におけるソフトウェアの品質を確保すること。	
実 93	ソフトウェア等の品質向上対策	【基礎】プログラムの配布を考慮したソフトウェアの信頼性を確保すること。	顧客はソフトウェアのリリース前にリリース環境を検査し、整合性を確認するとともにウイルスを排除する必要があります。 顧客が規制要件を遵守できるよう、Tencent Cloud は社内で定めたソフトウェアリリース基準およびプロセスに従って

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ソフトウェアのリリースを完了します。 Tencent Cloud はソフトウェアをリリースする際、物理ハードウェア、オペレーティングシステム、ミドルウェアに対する適合性テストを実施し、ソフトウェアが異なる環境で動作することを保証します。同時に、Tencent Cloud はソフトウェアの公開前に悪意のあるコードのスキャンを行い、ソフトウェアの安全性を確保します。脆弱性が検出された場合、自動的にチケットが生成され、開発担当チームに送信されます。開発担当チームが脆弱性の修正を完了してからリリースを行うことで、セキュリティ上の問題を本番環境に持ち込むことを防ぎます。
		【付加】オペレーションの自動化、簡略化を図ること。 クラウドサービスを利用する場合、金融機関等は、クラウドサービスにおいて操作の自動化・簡素化を実現するために提供される機能等について、クラウドサービス提供者に確認する必要がある。関連する機能の例を以下に示す。	顧客は操作の自動化および簡素化を実現すべきである。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーに対し、操作の自動化および簡素化を実現するためにクラウドサービス内で提供されている機能について確認する必要がある。 Tencent Cloud は、顧客が操作の自動化を実現できるよう、以下のサービスを含む複数のサービスを提供しています。
実 99	運用時の信頼性向上対策	(1) クラウドサービス提供者がクラウドサービス / クラウド製品に対して、起動タイミング、起動間隔、起動条件等の設定をサポートする機能。 (2) クラウドサービス提供者が提供する管理インタフェースを呼び出すアプリケーションを実装し、運用管理ミドルウェアのジョブとしてスケジューリングを行う機能。 (3) クラウドサービス提供者が提供する、操作自動化を目的としたサービスを利用する機能。	• <u>TencentCloud API</u> : クラウド API は、Tencent Cloud 製品の各種リソースに対するインタフェースを提供します。クラウド API を利用することで、顧客は少量のコードでクラウド製品を迅速に操作できます。クラウド API は互換性が高く、自動化が容易で、リモート呼び出しにも対応しています。顧客はクラウド API を通じてインタフェースを自由に組み合わせ、一般的な機能の呼び出しや機能のカスタマイズを実現できます。 • <u>Tencent Infrastructure Automation for Terraform</u> : 本製品は、世界的に広

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			く利用されている IaC ツール「Terraform」のプラグイン拡張体系に基づいており、クラウドリソースのデプロイ、実装、管理の自動化機能を提供します。Terraform の成熟したインフラ自動化ツール機能と Tencent Cloud のクラウドリソースサービス機能を相互に連携させることを目的としており、お客様が DevOps やマルチクラウド展開などのモデルを容易に実装できるようにします。Terraform HCL の宣言型構文と完全に互換性があり、インフラストラクチャのクラウドリソースをコード化して記述し、バージョン管理を行うことで、自動デプロイと運用保守の効率を向上させます。 • <u>Auto Scaling (AS)</u>: AS はインスタンスのヘルス状態を自動的に検知し、お客様のビジネス要件、ポリシー、および事前に設定されたスケールアウト・スケールインの条件に基づいて、クラウドサーバーのコンピューティングリソースを自動的に調整します。これにより、お客様のアプリケーション負荷を処理するために常に適切な数のクラウドサーバーインスタンスを確保します。 さらに、Tencent Cloud の多くのストレージおよびデータベース製品は、データの自動バックアップ機能をサポートしています。例えば、<u>TencentDB for MySQL</u> や <u>TencentDB for MongoDB</u> などは、充実したデータの自動バックアップおよびロスレス復旧メカニズムを備えており、<u>Cloud File Storage (CFS)</u> は定期的な自動スナップショット機能などを提供しています。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 100	運用時の 信頼性向 上対策	【基礎】オペレーションのチェック機能を充実すること。	顧客は、操作ミスを防ぐために、操作チェック機能を実施すべきである。クラウドサービスを利用する際は、顧客はクラウドサービスプロバイダーに対し、同社が提供する運用管理関連のサービスやツールのチェック機能を確認すべきである。 Tencent Cloud は、お客様の運用チェックや監査を支援するため、以下のようなさまざまなサービスを提供しています。 • Cloud Log Service (CLS) : 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 はログの収集、保存から検索・分析、リアルタイム利用、配信に至るまで多岐にわたるサービスをサポートし、お客様の業務運用、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。 • Cloud Security Center (CSC) : CSC は、クラウドセキュリティ製品のアラートデータ、クラウド資産の構成変更データ、クラウド上のユーザー操作行動データ、および一部のクラウド製品のログデータなど、クラウド上のセキュリティ関連データを一元的に収集し、統一された検索・調査プラットフォームを提供することで、お客様が包括的なクラウドログ監査と検索・調査を実現できるよう支援します。 • CloudAudit : 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、およびリスク監査をサポートします。お客様は CloudAudit を活用して、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記録し、継続的に監視・保存することができます。 • Data Security Audit (DSA) : DSA
		クラウド利用の場合、クラウド事業者に対して、クラウド事業者が提供するオペレーション管理に関するサービスやツールのチェック機能を確認することが必要である。	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			は、人工知能 (AI) を基盤とした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おける各種セッション情報、アクセス操作、SQL 文の全量監査と記録をサポートします。多様なルールベースと脅威検知エンジンに基づき、操作中の悪意ある行為を識別し、管理者に速やかに通知して、適切なセキュリティ対策の実施を促します。 お客様の規制要件への準拠を支援するため、Tencent Cloud は社内でログ収集および管理の規範と仕組みを確立し、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・統制することで、システム活動の異常やリスクを検知・防止しています。 さらに、テンセントクラウドの本番環境には「堡垒機 (フォートレス)」が全面的に導入されており、本番環境における運用保守操作はすべて堡垒機を経由して行わなければなりません。運用保守操作の記録はログプラットフォームに一元的に保存されます。テンセントクラウドは、運用保守セキュリティの自動監査ツールおよび内部監査チームを通じてログを監査し、操作リスクを防止しています。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 101	運用時の 信頼性向 上対策	【基礎】負荷状態の監視制御機能を充実すること。 クラウド利用の場合、クラウド事業者に対して、負荷状態における監視機能やトラフィック制御機能について確認することが必要である。金融機関等においては、上記の確認結果をもとに負荷状態における監視機能やトラフィック制御機能の導入を検討することが必要である。	顧客は、各種リソースの負荷および容量を監視し、リソースの能力や容量の限界を超えないようにする必要がある。また、コンピュータシステムの稼働状態を監視する機能も設定すべきである。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーに対し、負荷状態における監視機能やトラフィック制御機能、およびシステム稼働状態の監視に関するクラウドサービスプロバイダーとクラウドユーザー間の責任範囲を確認する必要がある。 Tencent Cloud が顧客に提供するクラウドサービスは、各サービスで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。各サービスのパフォーマンス指標、測定基準、およびレポート要件は、各製品の SLA に明記されており、Tencent Cloud の公式ウェブサイトに掲載されています。各クラウドサービスのパフォーマンスと可用性は継続的に追跡されており、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できます。
		【基礎】システム運用状況の監視機能を設けること。 クラウド利用の場合、クラウド事業者に対して、システムの運用状況の監視についてクラウド事業者とクラウド利用者との間の責任範囲を確認することが必要である。金融機関等においては、上記の確認結果をもとにシステムの監視機能を整備することが必要である。なお、クラウド事業者が提供する機能に不足がある場合には、ツールの導入等により機能を補うことが考えられる。	お客様によるクラウド製品 / クラウドサービスの監視を支援するため、テンセントクラウドは Tencent Cloud Observability Platform (TCOP) を提供しています。 TCOP は、クラウドサーバーやクラウドデータベースなどのクラウド製品が自動的に報告する各種監視指標や、お客様が独自に設定して報告する監視指標を収集し、視覚的なグラフで表示することで、お客様がクラウド製品のリソース使用率、アプリケーションのパフォーマンス、およびクラウド製品の稼働状況をリアルタイムで把握できるよう支援します。TCOP は指標に対するアラート設定をサポートしており、設定されたアラートルールに基づいて、メッセージプッシュなどの方法で業務上の異常状況を顧客に速やかに

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			通知します。 お客様が容易にキャパシティプランニングや調整を行えるよう、Tencent Cloud は <u>Auto Scaling (AS)</u> サービスを提供しています。AS はインスタンスのヘルス状態を自動的に検出し、お客様のビジネスニーズ、ポリシー、および事前に設定されたスケールアウト・スケールインの条件に基づいて、クラウドサーバーのコンピューティングリソースを自動的に調整し、お客様のアプリケーション負荷を処理するために常に適切な数のクラウドサーバーインスタンスを確保します。 ネットワークトラフィックの監視に関しては、<u>Flow Logs (FL)</u> を利用すること で、ネットワークトラフィックをリアルタイムかつ非侵襲的なバイパス方式で収集、保存、分析し、トラブルシューティング、アーキテクチャの最適化、セキュリティ検査、コンプライアンス監査などの課題を解決できます。 さらに、お客様は信頼性を向上させるために、<u>Cloud Load Balancer (CLB)</u> をご利用いただけます。CLB は、安全かつ高速なレイヤー4/7 トラフィック分散サービスを提供し、トラフィック分散を通じてアプリケーションシステムの対外サービス能力を拡張し、単一障害点を排除します。また、クラスタ化されたデプロイメントを採用しており、障害発生インスタンスを速やかに排除することで、バックエンドサーバーの業務を正常に稼働させます。 お客様が規制要件を順守できるよう、機器監視の面では、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

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			バーなどのネットワーク機器を監視・アラート通知しています。また、エンドポイント検出および対応 (EDR) ツールを導入し、ネットワーク全体のサーバーおよびエンドポイント資産を包括的に監視・管理しています。 容量計画および管理の面では、テンセントクラウドは容量管理手順を策定し、各事業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にしました。テンセントクラウドは、内部の容量監視プラットフォームを使用して、クラウドプラットフォームの基盤となるサポートサービスの容量使用状況をリアルタイムで監視し、容量使用の傾向を把握しています。
			顧客は、迅速な障害復旧を支援するため、障害検知および障害箇所の特定機能を設定すべきである。クラウドサービスを利用する際、顧客はクラウドサービスプロバイダーに対し、障害発生前の稼働状況を記録できる追跡情報を含むログ記録機能など、提供可能な障害検知および障害箇所の特定機能について確認すべきである。
実 103	障害の早期発・回復機能	【付加】障害の検出及び障害箇所の切分け機能を設けること。 クラウド利用の場合、クラウド事業者に対して、障害の検出及び障害箇所の切分け機能について、確認することが必要である。	障害検出を支援するため、Tencent Cloud はお客様に 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 はログの収集、保存から検索・分析、リアルタイム処理、配信に至るまで多岐にわたるサービスをサポートし、顧客の業務運用、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 では、1 つまたは複数のログトピックに対してアラートポリシーを設定できます。アラートポリシーは定期的に監視タスクを実行し、クエリ分析結果がトリガー条件を満たした場合にアラート通知を送信するため、お客様は異常を迅速に

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			発見できます。 また、お客様は Cloud Security Center (CSC) を利用して、クラウド上の資産に対するワンストップのセキュリティ管理を行うことができます。これには、資産の自動棚卸し、各種セキュリティリスクの検出・識別、およびセキュリティリスクに対する自動対応・処置が含まれます。クラウドセキュリティセンターは、企業のセキュリティ状況を継続的に監視し、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一元的に取り込み、アラートログの監査、分析、集約、一元的な表示および追跡を行います。また、クラウドセキュリティセンターはオーケストレーション機能を活用し、お客様が自動化された対応と処置を事前に設定できるようにすることで、対応効率の向上を支援します。 Tencent Cloud はさらに、Elasticsearch Service (ES) サービスを提供しており、クラウドサーバーやコンテナなどの他のクラウド製品からのリアルタイムログ、またはビジネスの既存および増分ビジネスデータを、Tencent Cloud ES クラスターに集約・転送し、データの分散ストレージ、検索分析を実現します。 顧客の規制要件への準拠を支援するため、Tencent Cloud は社内にログ収集・管理の規範および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・統制することで、システム活動の異常やリスクを検知・防止しています。Tencent Cloud 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の監査を行い、操作リスクを防止して

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			います。 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、エンドポイント検出および対応（EDR）ツールを導入し、ネットワーク全体のサーバーおよびエンドポイント資産を包括的に監視・管理しています。 障害への迅速な対応と処理のため、 Tencent Cloud 内部で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、処理のメカニズムおよび関連プロセスを確立しています。テンセントクラウドチームは、セキュリティインシデントを検知したり、他のインシデント発見者からの報告を受けたりすると、直ちに対応メカニズムを起動し、多角的な早期警告と防御を行います。テンセントクラウドのセキュリティチームは、24 時間 365 日のセキュリティ運用体制を基盤とし、脆弱性監視、侵入の追跡、攻撃の遮断などの核心的なシナリオに焦点を当て、セキュリティアラートにリアルタイムで対応し、攻撃の追跡と緊急対応策の策定を迅速に完了することで、セキュリティインシデントの拡大を効果的に抑制します。
実 103- 1	障害の早期発・回復機能	【付加】冗長構成・バックアップ構成が正常に機能するための措置を講ずること。	冗長構成またはバックアップ構成を採用するシステムについては、顧客はシステムの信頼性を高めるため、構成が正しく動作するよう措置を講じる必要があります。 顧客が規制要件を遵守できるよう、Tencent Cloud は包括的な事業継続マネジメントシステムを構築し、ISO/IEC 22301 事業継続マネジメントシステムの国際規格認証を取得しています。テンセントクラウドは、クラウドサービスの事業継続性を確保するため、単一リージョン内で複数のデータセンターを用いた冗長化メカニズムを採用することを求めています。また、

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			クラウド製品および重要なプロセスに対して詳細な災害復旧計画を策定し、要件に厳格に従って定期的な演習を実施することで、災害復旧計画の適時性と実行可能性を確保しています。
			障害発生時、顧客は速やかに障害に対処するための措置を講じ、機能の縮小やシステムの再構成を通じて、システム全体の停止を回避する必要があります。
			インシデントの検出および迅速な対応を支援するため、Tencent Cloud は統合セキュリティ管理プラットフォーム Cloud Security Center (CSC) を提供しています。
			その資産センター、リスクセンター、アラートセンター、高度セキュリティ管理などの機能を通じて、お客様が事前の脅威検知、インシデント発生時の対応・処置、事後の原因追跡分析というセキュリティ運用のサイクルを実現し、セキュリティ運用の効率を向上させることを支援します。
実 104	障害の早期発・回復機能	【付加】障害時の縮退・再構成機能を設けること。	顧客が規制要件を遵守できるよう、Tencent Cloud 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、処理のメカニズムおよび関連プロセスを確立するとともに、インシデント処理プロセスにおける各チームの役割と具体的な責任を明確化しています。Tencent Cloud は、内部の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ています。検知・特定されたセキュリティインシデントに対し、Tencent Cloud はインシデントの性質、データの機密性、影響範囲などの要因を総合的に考慮して分析・分類を行い、速やかに担当責任者に通知してインシデントの対応を進めます。テンセントクラウドのセキュリティチームは、24 時間 365 日のセキュリティ運用体制を基盤とし、脆弱性監視、侵入原因の追跡、攻撃の遮断といった中核的なシナリオに注力しています。セキ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			セキュリティアラートにリアルタイムで対応し、攻撃原因の追跡と緊急対応策の策定を迅速に行い、セキュリティインシデントの拡大を効果的に抑制します。 お客様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、Tencent Cloud 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、内部審査を経た上で、その処理および分析結果を適切な方法でお客様に通知します。
			お客様は、障害発生時にシステムを迅速に復旧し、業務への影響を最小限に抑えるために、必要な復旧機能を設定する必要があります。 Tencent Cloud は、世界各国の関連国際基準および現地のセキュリティ要件に基づき、データセンターを建設またはリースしており、お客様に複数のリージョンおよびアベイラビリティゾーンの選択肢を提供しています。お客様は、事業の発展ニーズやデータセキュリティ要件に応じて、データやシステムを異なるリージョンやアベイラビリティゾーンに自律的かつ柔軟に展開し、さまざまな事業継続モデルを採用することで、事業の災害復旧要件を保証することができます。同時に、Tencent Cloud が提供する各種ストレージサービスおよびデータベースサービスは、いずれもバックアップ機能を備えており、多重冗長バックアップや遠隔地での災害対策などの要件に対応しています。Tencent Cloud が提供するコンピューティングサービス、ネットワークサービス、ストレージサービス、データベースサービス、コンテナおよびミドルウェアサービス、セキュリティサービスなど、多種多様なクラウド製品・サービスは、いずれも高可用性を特徴としており、対応する災害復旧計画が整備されています。 さらに、テンセントクラウドは ISO/IEC 22301 ビジネス継続性マネジメントシス
実 106	障害の 早期発・ 回復機能	【付加】障害時のリカバリー機能を設けること。	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			テムの国際標準認証を取得しており、社内 に包括的なビジネス継続性マネジメント システムを構築し、定期的に災害復旧演習 やテストなどを実施することで、システム および業務の災害耐性、対応速度、復旧能 力を確保しています。

5.2.8 個別業務・サービス等

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
実 145	テレワー ク	【付加】テレワークで使用するハ ードウェア及びソフトウェアの管 理方法を明確にすること。	お客様は、リモートワークで使用するハ ードウェアおよびソフトウェアの管理方法 を明確にし、リモートワークを行う従業員 にその内容を周知徹底する必要があります。 また、リモートワークにおける情報漏 洩を防止するため、この過程においてデー タ保護および通信保護措置を講じる必要 があります。 お客様がいつでも、どこでも、あらゆる主 要端末を使用して、安全かつ迅速にクラウ ド業務システムにアクセスできるよう、 Tencent Cloud は SSL VPN リモートアク セス技術をサポートしています。SSL VPN は、暗号化によってインターネット上で送 信されるデータの安全性を保護し、適切な アクセス制御もサポートすることで、不正 アクセスの発生を低減します。
実 146	テレワー ク	【付加】テレワークにおける利用 者認証及びアクセス制御に関する 対策を講ずること。	お客様は、さらに VPN Connection を利 用して、オンプレミスデータセンターと Tencent Cloud 上のリソースとの接続を実 現することもできます。 VPN チャンネルは IKE (鍵交換プロトコル) と IPsec を採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することで、転送 中のデータの安全性を確保します。VPN ゲ ートウェイは高い信頼性を備えており、下 層ではデュアルマシンホットスタンバイ アーキテクチャを採用することで、通信セ ッションの中断を防ぎ、上層のアプリケー

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ションには影響を与えません。 お客様の規制要件への準拠を支援するため、モバイルデバイス管理の面において、 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に関する規範を策定し、社内モバイルデバイスの安全な利用基準およ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ました。従業員のモバイルデバイス（ノートパソコンなど）に対しては、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、セキュリティ管理を行っています。ゼロトラストセキュリティ管理システムのウイルス対策、脆弱性修正、プロアクティブ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、内部横移動対策など、全方位的なセキュリティ保護を実現しています。また、ゼロトラストセキュリティ管理システムは、機密データの外部送信監視機能もサポートしており、メール、クラウドストレージ、リモートコントロール、ファイル転送ツールなどを通じたファイルの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は、テンセントクラウドは社内従業員向けのリモートアクセス管理手順を確立しており、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に限り、暗号化された通信チャンネルを介してテンセントクラウドの社内ネットワークおよび日常業務システムにリモートアクセスすることができます。Tencent Cloud はリモートアクセスログを管理し、ユーザーの操作履歴を記録します。同時に、Tencent Cloud の社内ネットワークと顧客データが格納された本番環境は完全に分離されています。Tencent Cloud の従業員が顧客の同意と権限を得て顧客情報資産にアクセスする場合、必ずバスタードマシン (Bastion Host)

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			を經由して顧客データが格納された本番環境にアクセスしなければなりません。また、バックエンドの運用保守操作記録はすべてログプラットフォームに一元的に保存され、Tencent Cloud の内部監査チームが定期的に記録情報を審査します。
実 150	AI	【付加】AI の利用に係る方針の策定と態勢の整備を行うこと。	事業者は、人工知能（AI）の利用方針を策定し、役割と責任、利用基準および要件などを明確にし、AI の適切な利用を促進するとともに、AI の利用に関する説明責任を果たすものとする。お客様は、AI を適切に運用・管理するとともに、その透明性を確保することに努め、ユーザーや関係者の人権を侵害することを防ぎ、虚偽情報、誤った情報、偏った情報に起因する不適切かつ有害な偏見や差別を排除しなければなりません。また、お客様は、ユーザーや関係者の生命、身体、財産、精神および環境に危害が及ばないよう、AI に関連する安全対策を講じなければなりません。
実 151	AI	【付加】AI の適切な運用管理方法を定めること。	テンセントクラウドは、責任ある人工知能（AI）の発展を長期的な戦略的重点の一つと位置づけ、事業の成長を推進すると同時に、倫理と安全を AI 技術の開発および応用に組み込み、責任あるイノベーションを促進することに尽力しています。AI がもたらすセキュリティ上の課題を重視し、国際的なガバナンスの最先端動向に積極的に歩調を合わせ、AI ガバナンスの水準を継続的に向上させることで、潜在的なリスクに対処し、軽減しています。事業展開地域の法令を遵守した上で、データ品質、セキュリティコンプライアンス、および倫理を重要な考慮事項とし、AI ライフサイクルの各段階においてリスク評価を行い、一連のリスク管理措置を実施しています。また、セキュリティ分類体系、攻撃・防御対策、潜在的な有害コンテンツの検出、トレーニングデータの匿名化、社会的倫理の組み込みなどの分野に継続的に研究開発リソースを投入し、AI 製品の安全な運用を支援することで、AI 分野における新たなデータセキ
実 152	AI	【付加】AI に係る安全対策を講ずること。	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			セキュリティ、モデルセキュリティ、倫理的リスクなどの課題に対応しています。 データガバナンスの面では、テンセントクラウドはデータセキュリティ戦略を策定・徹底することで、AI データ処理のライフサイクル全体にわたる活動を包括的に規範化し、セキュリティおよびコンプライアンス要件を AI 開発の全プロセスに組み込み、信頼性の高いデータソースを厳格に審査・選定しています。さらに、先進的なアルゴリズムを用いた徹底的なデータクレンジングやセキュリティフィルタリングなどを通じて、AI データが常に有効に保護され、合法的に使用されることを保証し、ユーザーのプライバシーとデータセキュリティのために強固な防衛ラインを構築しています。同時に、コンテンツセキュリティ、プライバシー保護、モデルセキュリティなどの課題に対し、テンセントクラウドの AI セキュリティチームは社内で 1,000 人以上を動員した大規模なセキュリティテストを複数回実施し、AI セキュリティリスクを早期に発見・収束させています。 アルゴリズムガバナンスの面では、テンセントクラウドは AI アルゴリズムの安全性評価とチューニングを継続的に実施し、潜在的なセキュリティ脆弱性を定期的に特定・修正するとともに、モデルの攻撃耐性をテスト・強化し、モデル性能を最適化してバイアスを低減しています。また、部門横断的なセキュリティチームによる審査メカニズムを確立し、モデルの技術的実装およびデータ利用が業務要件とセキュリティ基準に適合していることを保証しています。 運用ガバナンスの面では、テンセントクラウドはリスクの監視、予防、対応を継続的に行い、多層的なセキュリティ対策を講じることで、モデルの出力が安全かつ正確であることを保証しています。さらに、コンテンツ識別技術を応用してリスクのある

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			コンテンツを追跡し、モデルのセキュリティレベルを継続的に向上させることで、ユーザーおよび社会に対する責任を継続的に果たしています。また、攻撃・防御の対抗演習や大規模障害など、現実的な災害復旧シナリオを定期的にシミュレートした災害復旧演習を実施し、システムの災害耐性、応答速度、復旧能力を全面的に点検することで、突発的な事態が発生した場合でも、業務を迅速に正常化できるようにしています。
実 153	AI	【付加】AI の利用に係る教育、注意喚起等を行うこと。	顧客は、ユーザーおよび関係者が AI を正しく理解し、AI を適切に使用する知識、素養、および倫理観などを身につけられるよう、AI の利用に関する教育や注意喚起を行うべきである。 お客様の規制要求への対応を支援するため、Tencent Cloud は国際版公式サイトにおいてオンライン版の『人工知能サービス利用規約』を提供し、ユーザー入力および AI 出力に関する権利と責任、AI 製品の利用制限、AI 製品 / サービスの限界等を明確化するとともに、ユーザーが苦情や改善提案を提出できるフィードバックチャネルを提供しています。 さらに、Tencent Cloud の AI 製品・サービスに関する製品紹介や利用シナリオなどは文書化されており、公式サイトを通じて顧客に提供されています。顧客は、クラウドコンソール、オンラインカスタマーサポート、電話などのチャネルを通じて、関連するサポートを受けることも可能です。 テンセントクラウドは、人工知能および機械学習の分野において、以下のような多様な製品を顧客に提供しています。 • AI 基盤製品: Face Recognition、Automatic Speech Recognition (ASR)、Text To Speech (TTS)、Tencent Machine Translation

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			<u>(TMT)</u> 、 <u>Optical Character Recognition (OCR)</u> 、 <u>Image Creation</u> 、 <u>Face Fusion</u> 。 - AI アプリケーション製品: <u>eKYC</u> 、 <u>Tencent Cloud AI Digital Human。</u> - AI プラットフォーム製品: <u>Tencent Cloud TI Platform。</u> - Tencent Cloud の大規模モデル: <u>Tencent Cloud Agent Development Platform。</u>

5.3 設備基準

5.3.1 データセンター

『金融機関等コンピュータシステムの安全対策基準』第6章「設備基準」では、金融機関のデータセンターの立地、設計及び建設等に関する基準と要件が重点的に示されています。同基準は、金融機関のデータセンターが計画及び建設に当たり、地震・津波等の自然災害に対する防護措置、データセンター内の消防設計、電力供給管理の安定性設計、温湿度等の環境制御、ケーブル配線の安全性、物理的施設及びテナント専用スペースの防護措置、設備の日常運用保守の操作性、並びに建築立地のコンプライアンス及び設計案の適合性等の重要要素を考慮し、設計上の不備がデータセンターの持続的稼働能力に影響を及ぼさないようにすることを求めています。

Tencent Cloud は、お客様が規制要求を遵守することを支援するため、世界各地のデータセンターについて、関連する国際基準及び現地のセキュリティ要件に従い、立地選定、建設又は賃借を行っています。現在、Tencent Cloud は日本地域に2つの賃借型データセンターを展開しています。データセンターのレジリエンス及びセキュリティを確保するため、Tencent Cloud はデータセンター供給者に対するアク

セス管理、契約による拘束、継続的監督の全プロセスにわたり、厳格な管理体系を構築しています。

- 供給者選定段階では、Tencent Cloud は厳格な供給者セキュリティ評価メカニズム及びアクセス基準を確立し、データセンター供給者の物理的環境の安全（入退室管理、監視、消防等）、情報セキュリティ管理システム（データ暗号化、アクセス制御等）及び事業継続性の確保能力（災害復旧案、障害復旧メカニズム等）について、包括的なデューデリジェンス及びリスク評価を実施し、選定された供給者が高いセキュリティ基準を満たすことを確保しています。
- 協定締結段階では、Tencent Cloud はデータセンター事業者と共に、標準化された契約文書を通じて双方の権利義務の境界を明確化し、データセンター事業者のサービス範囲を明確にするとともに、サービス可用性レベル等の核心的サービス基準を定量的に定義し、サービス品質に対する契約上の保証を提供しています。
- データセンター運営段階では、Tencent Cloud は定常的な監察及び評価メカニズムを確立し、定期的にデータセンター事業者の技術能力、サービス対応効率及びリスク管理効果を総合的に評価し、データセンター事業者のリスク管理上の欠陥が Tencent Cloud のお客様への核心的サービス提供能力に影響を及ぼさないようにしています。また、Tencent Cloud は双方が締結したサービスレベルアグリーメント（SLA）に厳格に従い、事業者に対して約定された周期で SLA 履行報告書を提出させており、報告書にはサービス期間中の重大インシデント処理記録、主要パフォーマンス指標達成状況及び保守作業の総括等の核心的内容を含めることを要求しています。Tencent Cloud は定期的にデータセンター事業者のパフォーマンス評価を行い、評価結果は今後の供給者との協力における重要な根拠となります。

データセンター環境セキュリティの面において、テンセントクラウドは、データセンターオペレーターに対して、高い安定性と完全冗長性を備えた電源システム、空調システム等の採用を要求し、いかなる単一障害点もデータセンターの継続性と可用性に影響を及ぼさないようにしています。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、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。

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。

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。

5.4 監査基準

5.4.1 システム監査

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
監 1	システム 監査	【基礎】システム監査体制を整備すること。	お客様は、システム監査に関する体制を構築し、監査の実施方法を選択して、コンピュータシステムの管理状況を把握・評価する必要があります。また、サイバーセキュリティに関する内部監査計画を策定し、サイバーセキュリティをテーマとした内部監査を実施するとともに、監査で発見された問題の是正状況を正確に把握する必要があります。 お客様の監査および審査要件に対応するため、Tencent Cloud は専任の担当者を 配置して支援を行い、お客様側から開始される監査または審査活動に積極的に対応します。同時に、Tencent Cloud の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確保するため、内部のセキュリティリスクを継続的に監視・評価しています。Tencent Cloud のセキュリティチームは、少なくとも年 1 回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および内部システムの状態を継続的に監視することで、良好なセキュリティ態勢を維持し、関連法規およびセキュリティ管理基準の規定と要件に準拠しています。さらに、Tencent Cloud は毎年、独立した第三者による専門的な監査を受け、証明的な性質を持つシステムおよび組織統制報告書を提供することで、クラウドユーザー機関、独立監査人、規制当局、株主、およびその他の利害関係者に、Tencent Cloud の最新のサービス組織内部統制状況を公開しています。 特に日本地域においては、テンセントクラウドは『FISC 金融機関等コンピュータシステムセキュリティガイドライン』に基づき、管理状況の評価を行い、これに基づいて対応するシステムおよび組織管理 (SOC) 報告書を作成しています。この報告書は、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
監 1-1	システム 監査	【基礎】サイバーセキュリティを対象とした内部監査を行うこと。	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			管理項目を網羅し、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。 監査で発見された問題に対し、テンセントクラウドは顧客に与える可能性のある影響を評価し、問題発生の原因を詳細に分析した上で、これに基づいて適切な是正措置を策定・実施します。関連する問題が金融機関顧客の業務運営やデータセキュリティに影響を及ぼす可能性がある場合、テンセントクラウドは速やかに関連金融機関に通知します。同時に、経営陣は是正計画および具体的な行動の実施状況を定期的に追跡・継続的に監視し、問題が効果的に解決されることを確保します。

06

Tencent Cloud による「金融分野におけるサイバーセキュリティに関するガイドライン」の遵守及びお客様の対応支援について

日本金融庁（Financial Services Agency, FSA）は、過去の金融機関に対する検査・モニタリング結果及び金融業界内外の情勢変化を踏まえ、2024年10月4日に「[金融分野におけるサイバーセキュリティに関するガイドライン](#)」を公表し、金融分野全体のサイバーセキュリティ水準の継続的な向上を推進することを目的としています。本ガイドラインは、サイバーセキュリティの観点から、ガバナンス、識別、防御、検知、対応、復旧及びサードパーティリスク管理等の各プロセスにおいて、金融機関等が履行すべき「基本対応事項」と「推奨対応事項」を明確化しています。

「基本対応事項」とは、金融機関が普遍的に実施すべき基礎的な要件を指し、「推奨対応事項」とは、金融機関の規模や特性等を踏まえ、万一インシデントが発生した場合に地域経済社会に重大な影響を及ぼす可能性がある金融機関に対して、実施が推奨される対策、参考にすべき優良事例、並びに海外の規制当局や金融機関との対話を通じて把握された先進的实践等を指します。日本金融庁は、金融機関等に対し、自社の経営環境、経営戦略及びリスク許容度等を考慮した上で、サイバーセキュリティリスクを特定・評価し、リスクに見合ったセキュリティ対策を講じることを求めています。

本章では、Tencent Cloud が『金融分野におけるサイバーセキュリティに関するガイドライン』の中からクラウドサービスプロバイダーに関連する統制要件を抽出・整理し、Tencent Cloud がクラウドサービスプロバイダーとして、金融機関等がこれらの要件を遵守することをどのように支援できるかについて説明します。

6.1 サイバーセキュリティ管理態勢の構築

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
2.1.1	基本方針、規程類の策定等	【基本的な対応事項】 ① 取締役会等は、サイバーセキュリティリスクを組織全体のリスク管理の一部として捉え、サイバーセキュリティ管理の基本方針を策定すること。 ② 取締役会等は、組織の経営目標にとってのサイバーセキュリティの確保の重要性を認識し、関係主体等からの要求事項及び法規制等の内外の状況を勘案して、必要なサイバーセキュリティ管理態勢	顧客は、サイバーセキュリティ管理の基本方針、関連戦略および実施計画を策定し、関連する組織構造を整備し、サイバーセキュリティ管理体制を構築し、サイバーセキュリティ管理体制を定期的に見直し、外部専門家を活用してサイバーセキュリティガバナンスの検証を行うものとする。顧客は、サイバーセキュリティを確保するための各種措置を積極的に推進し、サイバーセキュリティリスクをリスク管理フレームワークに組み込み、サイバーセキュリティを重視する組織文化を醸成するものとする。また、顧客は、

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		を整備すること。また、サイバーセキュリティ管理態勢について、少なくとも年1回のレビュー等を通じて、十分な検証と議論を行うこと。	サイバー攻撃に対する早期警戒情報の収集・分析メカニズム、監視メカニズム、および危機管理メカニズムを確立するものとする。
③	経営陣は、サイバーセキュリティ管理態勢を整備すること。	③ 経営陣は、サイバーセキュリティ管理態勢を整備すること。	顧客の規制遵守を支援するため、情報セキュリティ管理方針に関して、テンセントクラウドは情報セキュリティ管理方針を策定しました。これは、情報セキュリティの全体戦略、セキュリティ組織構造、およびセキュリティ管理システムで構成され、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ます。Tencent Cloud の情報セキュリティポリシーは毎年定期的に見直しが行われ、クラウドセキュリティ管理システムの管理目標、管理手順、および管理措置が、関連するセキュリティ戦略、基準、手順、およ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確保しています。また、Tencent Cloud は利用許容ポリシーを策定し、従業員および第三者が Tencent Cloud のリソース (IT システム、ネットワーク、機器、データなどを含むがこれらに限定されない) を利用する際の責任と義務を明確にし、適切な利用行動を規範化し、潜在的なリスクを防止しています。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 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的なセキュリティ関連規格の認証を取得しています。
④	経営陣は、サイバーセキュリティ管理の基本方針に基づき、サイバーセキュリティに関する戦略及び実施計画を策定し、当該実施計画の実効性及び十分性を確保すること。	④ 経営陣は、サイバーセキュリティ管理の基本方針に基づき、サイバーセキュリティに関する戦略及び実施計画を策定し、当該実施計画の実効性及び十分性を確保すること。	
⑤	経営陣は、セキュリティ・バイ・デザインを含むサイバーセキュリティ確保に向けた取り組みを推進すること。	⑤ 経営陣は、セキュリティ・バイ・デザインを含むサイバーセキュリティ確保に向けた取り組みを推進すること。	
⑥	経営陣は、サイバーセキュリティを重視する組織文化を醸成すること。	⑥ 経営陣は、サイバーセキュリティを重視する組織文化を醸成すること。	
⑦	経営陣は、サイバーセキュリティを担当する部署及び各関係者の役割、責任並びに権限を明確化すること。	⑦ 経営陣は、サイバーセキュリティを担当する部署及び各関係者の役割、責任並びに権限を明確化すること。	
⑧	経営陣は、少なくとも年1回、サイバーセキュリティリスクの状況、サイバーセキュリティに関するリスク評価結果及び実施計画の進捗状況等について、報告を求めること。	⑧ 経営陣は、少なくとも年1回、サイバーセキュリティリスクの状況、サイバーセキュリティに関するリスク評価結果及び実施計画の進捗状況等について、報告を求めること。	
⑨	経営陣は、サイバーセキュリティ管理態勢を継続的に改善すること。	⑨ 経営陣は、サイバーセキュリティ管理態勢を継続的に改善すること。	情報セキュリティ管理の組織体制に関して、Tencent Cloud はクラウドセキュリティおよび情報セキュリティに関連する組織体制を構築し、各階層におけるセキュリティ関連の役割と責任を明確化すると
		【対応が望ましい事項】 (a) 経営陣が適切な経営判断を行うための前提として重要なサイバーセキュリティに係るガバナンスの確保のため、サイバーセキュリティに関する十分な知識を利用	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		(外部専門家の利用を含む) できるようにしておくこと。 (b) 取締役会等は、サイバーセキュリティリスクを統合的リスク管理の一部として位置づけ、リスク選好度（リスクアペタイト）、リスク耐性度（リスクトレランス）を設定すること。 (c) 経営陣は、可能な範囲で、自組織のサイバーセキュリティに関する取組の意義を内外の関係者に表明するために、攻撃者の攻撃を助長する可能性を考慮の上、その内容を対外公表すること。 (d) 経営陣は、少なくとも1年に2回、以下の報告を担当部署等に求めること。 サイバーセキュリティにかかるパフォーマンス指標（KPI）及びリスク指標（KRI） (e) 経営陣は、自組織におけるサイバーセキュリティを統括管理する責任者（CISO等）としてサイバーセキュリティに関する十分な知識・経験を有し、かつ、経営陣に日常的に直接レポートできる立場の者を配置し、平時及び有事に、経営トップと直接コミュニケーションする関係を構築すること。	もに、情報セキュリティ監査や情報セキュリティリスク評価などの業務メカニズムを定義しました。Tencent はセキュリティ技術委員会および様々な機能・分野を専門とするセキュリティチームを設置し、社内に充実した人事管理基準と手順を確立することで、職務要件に基づいた人材の採用と配置を確実にしています。テンセントクラウドは、業界のベテラン専門家からなるサービスチームを結集し、安全で信頼性が高く、専門的かつコンプライアンスに準拠した製品とサービスの提供に尽力しています。また、社内に充実した情報セキュリティ研修体制を構築し、正社員、コンサルタント、インターン、外部委託スタッフなどに対し、情報セキュリティ研修の受講を義務付けています。テンセントクラウドは、情報セキュリティ管理を日常の管理業務に組み込むことを徹底し、従業員が社内の情報セキュリティ管理ポリシーおよび要件を理解し、遵守するよう確保しています。 セキュリティ監査および評価に関しては、テンセントクラウドのセキュリティチームは少なくとも年1回、内部セキュリティ監査を実施し、関連法規およびセキュリティ管理基準の規定と要件への準拠を確保しています。また、テンセントクラウドは定期的に独立した第三者による専門的な監査を受け、証明的な性質を持つシステムおよび組織的統制報告書を提供することで、クラウドユーザー機関、独立監査人、規制当局、株主、およびその他の利害関係者に、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。 リスク管理の面では、テンセントクラウドは ISO/IEC 27001:2022、ISO/IEC 27018:2014、MTCS、CSA-Star などの規格を参考に、内部リスク管理フレームワークを開発・維持し、特定されたリスクの識別、分析、管理を行っています。テンセン

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			トクラウドは少なくとも年1回リスク評価を実施し、リスクシナリオや業務・製品・サービスのプロセス分析結果に基づいてリスクを特定します。特定されたリスクに対し、テンセントクラウドは各リスクの発生可能性と影響度を評価し、リスクレベルを分類した上で、適切な是正措置を講じ、記録に残します。また、リスクの是正状況を継続的に追跡し、残存リスクを評価することで、責任者がテンセントクラウドのリスク管理要件に従って適切にリスクを管理していることを確認します。さらに、テンセントクラウドはクラウド業界の動向や内部管理の実践に基づき、リスク評価手法およびリスク登録簿の維持・改訂を行っています。 さらに、テンセントクラウドは危機管理手順を策定し、テンセントクラウドの業務製品またはサービスにおいて突発的な事象や災害が発生した場合の危機管理プロセスおよび関連する責任チームを明確にしています。
2.1.2	規程等及び業務プロセスの整備	【基本的な対応事項】 ①経営陣は、サイバーセキュリティに係る規程及び業務プロセスを整備し、少なくとも1年に1回見直しを行うこと。 ② 経営陣は、サードパーティからもたらされるリスクも含め、サイバーセキュリティリスクにかかる、組織横断的な報告・連絡・協議ルートや指揮命令系統を整備すること。	顧客は、情報資産管理、リスク評価、脆弱性管理、ペネトレーションテスト、アクセス制御、教育・研修、データ管理、ログ管理、セキュリティ設計、インシデント対応・復旧、サードパーティのリスク管理などを含む、サイバーセキュリティに関連する規程および業務プロセスを策定し、少なくとも年1回、見直しおよび改訂を行うものとする。また、顧客は、サードパーティに起因するサイバーセキュリティリスクを含むリスクに対応するため、報告・連絡メカニズムおよび関連チャネルを確立するものとする。 規則・規定および業務プロセスに関して、 Tencent Cloud は情報セキュリティマネジメントシステムを構築しており、関連する制度やプロセスを毎年定期的に見直し・更新することで、マネジメントシステムの管理目標、管理手順、および管理措置が、関連するセキュリティポリシー、基準、手

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			順、および法的要件に適合していることを確保しています。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 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的なセキュリティ関連規格の認証を取得しています。 顧客との連絡・コミュニケーションに関して、テンセントクラウドは、クラウドコンソール、電子メール、専用ホットラインなど、テンセントクラウドと外部顧客間のコミュニケーションを促進するための多様なコミュニケーションチャネルを確立しています。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ており、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。また、顧客は適切なサービスプランを選択することで、専用サポートグループ、専任のテクニカル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受けることができます。
2.1.3	経営資源の確保、人材の育成	【基本的な対応事項】 ①経営陣は、サイバーセキュリティの重要性を踏まえた上で、サイバーセキュリティ担当部署等に、専門性を有する人材を配置し、また、必要な予算を配分するなどにより、適切な資源配分を行うこと。 ②経営陣は、サイバーセキュリティ管理の基本方針と整合的な人材の育成・確保のための計画を策定すること。 ③サイバーセキュリティにかかる経営陣によるガバナンスやサイバーセキュリティ確保に向けた組	顧客は、サイバーセキュリティ担当部門等に専門能力を備えた人材を配置し、持続可能な人材導入・育成計画（管理職向けのサイバーセキュリティ関連知識研修等を含む）を策定するとともに、適切なリソースを確保し、計画的に多様な人材の確保を図るものとする。 Tencent Cloud 製品の操作手順やユーザーマニュアルなどは文書化されており、公式サイトを通じてお客様に提供されています。また、Tencent Cloud は、Tencent Cloud 製品の基礎知識および関連する専門能力に基づいた トレーニングと認定 を提供し、お客様の技術力とクラウドの習

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		織風土の醸成に資するスキルやノウハウの修得に向けて、経営陣は積極的に研修・訓練等に参加すること。 ④人材の育成については、外部人材の活用も含めて、計画的に相応の人材を確保していくこと。	熟度向上を支援しています。 さらに、テンセントクラウドは、24 時間 365 日対応のチケットシステム、24 時間 365 日対応のホットライン、AI カスタマーサービス、セルフサービスなど、複数のチャネルを通じて、お客様からの質問やフィードバックに途切れることなく対応しています。テンセントクラウドのカスタマーサービスチームと技術専門家が、迅速かつ効果的なサポートを提供します。 顧客が規制ガイドラインを順守できるよう支援するため、テンセントはセキュリティ技術委員会および様々な機能・分野の専門セキュリティチームを設置し、業界のベテラン専門家からなるサービスチームを結集させ、安全で信頼性が高く、専門的かつコンプライアンスに準拠した製品とサービスの提供に尽力しています。テンセントクラウドは社内に充実した人事管理基準と手順を確立し、職務要件に基づいた採用と人員配置を確実に実施しています。採用プロセスにおいて、テンセントクラウドは候補者の学歴や資格証明書の確認など、厳格な審査を行います。テンセントクラウドは、業界のベテラン専門家からなるサービスチームを結集し、お客様に安全で信頼性が高く、専門的なセキュリティコンプライアンス製品およびサービスを提供することに尽力しています。さらに、テンセントクラウドは多様なキャリアパスを設定し、従業員に豊富で質の高い学習リソースを提供するとともに、研修コースや体系を継続的に最適化し、従業員の個人の成長とキャリア開発を支援しています。
2.1.5	内部監査	【基本的な対応事項】 ④内部監査部門は、必要に応じて外部専門家を利用しつつ、独立した立場から、リスクベース・アプローチに基づき、サイバーセキュリティに係る内部監査計画を策定し、サイバーセキュリティ（整備状	お客様は、リスクベースのアプローチに基づき、必要に応じて外部専門家を活用し、独立した立場からサイバーセキュリティに関する内部監査計画を策定し、サイバーセキュリティ内部監査を実施する必要があります。内部監査で発見された重要な問題および関連する是正状況については、速やかに経営陣に報告する必要があります。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		況・運用状況 対応・復旧 法規制の遵守状況、サードパーティリスク管理を含む) をテーマとする内部監査を実施すること。 ②内部監査部門は、内部監査で指摘した重要な事項について遅滞なく代表取締役及び取締役会等に報告するとともに、指摘事項の改善状況を的確に把握すること。 【対応が望ましい事項】 a.内部監査部門にサイバーセキュリティに係る適切な知識及び専門性等を有する 職員を配置すること。	また、お客様は内部監査部門に、適切なサイバーセキュリティの知識と専門能力を備えた人員を配置する必要があります。 お客様の規制遵守を支援するため、Tencent Cloud 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確保するために、内部セキュリティリスクの継続的な監視と評価を行います。テンセントクラウドセキュリティチームは、少なくとも年1回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および内部システムの状態を継続的に監視することで、良好なセキュリティ態勢を維持し、関連する法令およびセキュリティ管理基準の規定と要件に準拠することを確保します。さらに、テンセントクラウドは毎年、独立した第三者による専門的な監査を受け、証明的な性質を持つシステムおよび組織的統制報告書を提供することで、クラウドユーザー機関、独立監査人、規制当局、会社の株主、およびその他の利害関係者に、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ます。 監査で発見された不適合事項に対し、テンセントクラウドは、不適合を引き起こした実際または潜在的な原因を速やかに分析し、是正・予防措置を講じる必要性と優先順位を評価した上で、関連する承認を得て是正・予防措置を実施します。是正措置の実施効果は継続的に追跡・記録されます。 さらに、顧客監査および規制当局による審査に関しては、テンセントクラウドは実際の状況および顧客との契約や合意に基づき、顧客による第三者セキュリティ監査および監督に協力し、専任の担当者を配置して支援を行うとともに、顧客が実施する監査活動に積極的に対応し、協力します。

6.2 サイバーセキュリティリスクの特定

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
2.2.1	情報資産管理	【基本的な対応事項】 ① 情報資産をライフサイクル（取得・使用・保管・廃棄）に応じて管理する手続等を策定し、必要に応じて見直すこと。 ② 情報資産は、その重要度（機密性、完全性、可用性）に応じて保護の優先度を分類し、管理すること。なお、情報資産管理については、業態ごとの監督指針等における「情報セキュリティ管理」の項目も参照すること。	顧客は、情報資産のライフサイクル管理手順を策定し、情報資産の機密性、完全性、可用性に基づいて分類および保護を行うものとする。顧客は、情報システムおよび外部システムサービス、ハードウェア、ソフトウェア、ならびにデータ等について台帳を作成し、対応する保守手順を策定するものとする。
		2.2.1.1 情報システム及び外部システムサービス 【基本的な対応事項】 情報システム及び外部システムサービスを適切に管理するための台帳等を整備し、メンテナンス手順を定めるなど、最新の状態を網羅的に把握できるようにすること。	顧客の包括的な情報資産管理を支援するため、Tencent Cloud は Cloud Workload Protection Platform (CWPP) を提供しており、資産フィンガープリントの自動収集をサポートし、アカウント、ポート、プロセス、アプリケーションなどの資産フィンガープリントデータを一元管理します。CWPP はまた、資産フィンガープリントに基づいて発生したセキュリティインシデントのリスク影響範囲を迅速に調査し、顧客のサーバーセキュリティ向上を支援します。また、お客様は 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 および Cloud Security Center (CSC) を利用して、情報資産のセキュリティ管理を行うことも可能です。CSC は資産セキュリティセンターの機能を網羅しており、クラウドサーバー、オブジェクトストレージ、クラウドデータベース、ロードバランサーなどのクラウド資産に対する自動化された動的インベントリを実現します。さらに、クラウド構成のリスク、脆弱性、セキュリティインシデントなど、多角的なセキュリティ観点から資産のセキュリティリスクを一元管理し、クラウド上の「シャドウ IT」リスクを低減します。
		2.2.1.2. ハードウェア・ソフトウェア等 【基本的な対応事項】 ① ハードウェア及びソフトウェア等を適切に管理するための手続・台帳等を整備し、メンテナンス手順を定めるなど、最新の状態を網羅的に把握できるようにすること。	データ資産管理の面では、Data Security Governance Center (DSGC) が、顧客のデータ資産の自動整理を支援し、企業のク
		【対応が望ましい事項】 a. 複合機・特定用途機器を台帳等による管理対象とすること。 b. 必要に応じて、サードパーティの資産についても管理対象とすること 24。 c. ハードウェア及びソフトウェア等に係る情報資産の分類に当たっては、重要な業務のサードパーテ	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		ィへの依存関係を考慮したリスク管理が実施できるようにすること。 d. 管理対象外となっている個人所有端末等の情報資産や未承認のクラウドサービスの利用（シャドーIT 等）を特定し、管理対象とするか使用を中止するなど、適切に対応すること。 e. 以下に掲げるものに関するソフトウェア部品表 25（SBOM、Software Bill of Materials）を整備すること。 2.2.1.3 情報（データ） 【基本的な対応事項】 ① 顧客情報や機密情報等を適切に管理するための台帳等を整備し、メンテナンス手順を定めるなど、最新の状態を網羅的に把握できるようにすること。	クラウド上のデータを分類・格付けし、セキュリティリスク評価を行います。本サービスは、機密データの発見・分類・格付け、データマップ、異常なデータアクセス分析を一体化したデータセキュリティ運用プラットフォームであり、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防御網を形成し、企業のセキュリティ効果を最大化します。企業の承認を得た上で、クラウド上のさまざまな種類のデータ資産と深く連携し、カーネルレベルからタイムリーなデータ資産情報を取得します。データの特性に基づき、企業が機密データを特定できるよう支援し、セキュリティの観点からデータ資産を整理します。国、業界、または企業のデータ分類・格付け基準に従い、企業のデータ分類・格付けを支援します。可視化機能を通じて、資産の概要、分類・格付け、アカウント権限、データストレージ、機密データなど、多角的な視点から資産のセキュリティ状況を確認できます。 お客様の規制遵守を支援するため、Tencent Cloud は社内で情報資産管理規範およびライフサイクル全体にわたる管理プロセスを策定し、電子データ、ハードウェアおよ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に対して、分類・格付け管理と保護を実施しています。Tencent Cloud は、資産管理システムを通じてハードウェア機器およびソフトウェアコンポーネントを管理しています。これには、資産の登録および紐付け、資産の棚卸しおよび情報更新、資産の廃棄および交換などが含まれ、クラウドプラットフォームの基盤システムの安定した稼働を保証し、業務システムに信頼性の高いサポートを提供します。
2.2.2	リスク管理プロセス	【基本的な対応事項】 ① 自組織の脅威情報のほか、公的機関 や情報共有機関、サードパー	顧客は、組織自身、および公的機関、情報共有機関、第三者などから、サイバー攻撃に関連する脅威情報や脆弱性情報を収集

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		ティから、サイバー攻撃の脅威情報 (他組織の事例を含む) 及び脆弱性情報を収集すること。 ② 収集した情報を整理・分析し、これらによるサイバーセキュリティリスクが自組織の事業・情報資産に与える影響を評価すること。 ③ 情報の収集元及び収集・分析の方法を少なくとも1年に1回は見直し、必要に応じて改善を図ること。 【対応が望ましい事項】 a. 自組織の業務に即して、等の専門性の高い情報共有活動や、業界横断的な団体、国際的な団体等に積極的に参画し、脅威情報や脆弱性情報等を収集し共有すること。 b. 脅威分析を行う際に、過去に発生したことがない場合でも、深刻だが現実には起こりうるサイバー攻撃の脅威を対象に含めること。 c. 新技術 (AI、量子コンピュータ等)、地政学的動向、偽情報、業界動向などの組織を取り巻く状況に留意し情報収集を行うこと。	し、収集した情報を整理・分析して、関連する脅威や脆弱性が組織の業務や情報資産に与える可能性のある影響を評価しなければならない。また、顧客は、高度な専門性を有する組織、業界横断的な団体、国際機関による脅威情報の共有活動に積極的に参加し、情報収集にあたっては、新技術、地政学的動向、偽情報、業界動向など、組織に影響を与える外部環境の変化に注視すべきである。顧客は、少なくとも年1回、脅威および脆弱性情報の収集元、収集方法、分析方法を検証し、必要に応じて改善を行うべきである。 顧客の脅威検知および分析を支援するため、テンセントは顧客に Tencent Security Threat Intelligence Center (TIX) を提供しています。ワンストップの情報サービスプラットフォームとして、脅威インテリジェンスセンターは、基礎情報、攻撃面情報、業務情報の3大情報機能を提供し、情報検索、IOCの判定・分析、攻撃面管理などの機能をサポートします。これにより、お客様がセキュリティインシデントをより効率的に分析・判定し、企業の資産の露出面におけるリスク状況をより包括的に評価できるよう支援し、企業が効率的な多層的なセキュリティ防御体系を構築することを後押しします。脅威インテリジェンスセンターは、脆弱性コミュニティ、セキュリティ機関、セキュリティツールベンダー、ソーシャルメディア、セキュリティブログなど、多様なソースから脅威インテリジェンスを収集・分析する包括的な情報収集ネットワークを構築しています。さらに、クラウド上のアルゴリズムと計算リソースを活用して誤検知を排除し、情報の正確性を保証しています。 さらに、脅威インテリジェンスセンターはSaaS化を中核とし、Web API、SDK、TIP、ミニプログラムなど多様な提供方式をサ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ポートし、様々な顧客のニーズに応えます。また、統合方式を通じて、クラウド上のインテリジェンスデータを顧客の既存のセキュリティ製品と連携させ、セキュリティ運用全体および脅威対応の効率を向上させることができます。 脅威インテリジェンスセンターの機能とサポートに基づき、Tencent Cloud は「インテリジェンス・攻撃防御・管理・計画」からなる能動的防御セキュリティ能力体系の構築に取り組んでいます。脅威インテリジェンス、人工知能、ビッグデータなどの技術を統合することで、セキュリティインシデントへの対応能力と効率を向上させるとともに、24 時間 365 日体制のセキュリティオペレーションセンターを設置し、脅威の検知、調査、対応に注力することで、セキュリティ態勢の「把握・可視化・制御」を実現しています。
	2.2.2.2. リスクの特定・評価	顧客は、サイバーセキュリティリスクの特定および評価に関連するプロセスを策定し、定期的に（少なくとも年1回）、また重大な脅威や脆弱性が発見された場合、あるいは新製品やサービスを提供する際に、サイバーセキュリティリスク評価を実施しなければならない。顧客がリスク評価を行う際は、重要な業務を特定し、重要な業務を維持するために必要な組織内の人員、設備、システム、および第三者への依存度を考慮し、シナリオ分析、机上演習、またはストレステストなどの方法を通じて組織の脆弱性を特定しなければならない。顧客は、リスク評価の結果に基づき優先順位を付け、リスク対応計画を策定する必要があります。演習 / 訓練、脆弱性検出、ペネトレーションテスト、監査、リスク評価、および実際のインシデントから得られた提言、発見事項、問題点、教訓に対し、顧客は関連手順等に従って改善を行う必要があります。さらに、顧客は少なくとも年1回、サイバーセキュリティリスク管理体制、リスク評価プロセス、および監視・検	
	【基本的な対応事項】		
	① サイバーセキュリティリスクの特定・評価に係る手順を定めること。		
	② 脅威情報及び脆弱性情報を踏まえたサイバー攻撃の発生可能性、並びにサイバー 攻撃が発生した場合の自組織の事業や情報資産に与える影響に基づき、サイバーセキュリティリスクを少なくとも1年に1回評価すること。また、重大な脅威や 脆弱性が判明した時や、新規商品又はサービスの提供時にも評価すること。		
	③ リスク評価に当たっては、境界防御型セキュリティが突破されるリスクや内部不正などの脅威も考慮し、内部ネットワークセグメントに設置したシステムへのリスクも対象とすること。		

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		【対応が望ましい事項】 a. リスク評価に当たっては、重要な業務を特定し、重要な業務を継続するために必要な組織内の人員、設備、システム、サードパーティの相互依存度を考慮すること。 b. リスク評価に当たっては、シナリオ分析、机上演習又はストレステスト等を通じて、組織における脆弱性を特定し、重要なシステム及び業務に対する潜在的な影響を考慮すること。シナリオについては、深刻だが現実には起こりうる多様なシナリオを考慮すること。 2.2.2.3. リスク対応 【基本的な対応事項】 ① リスク評価の結果に基づき優先順位付けを行い、リスク対応計画を策定すること。 ② リスク対応における例外的な取扱いやリスク受容などの取扱いに関する手続を定めること。 ③ リスク対応計画は、定期的に経営陣に報告すること。 2.2.2.4. 継続的な改善活動 【基本的な対応事項】 ① 内外の環境変化に応じてサイバーセキュリティに関するリスク評価のプロセスを少なくとも1年に1回は評価するとともに、継続的な改善活動を実施すること。 ② サイバーセキュリティリスク管理態勢の整備状況及び運用状況の有効性を少なくとも1年に1回は評価し、改善すること。 ③ 演習・訓練、脆弱性診断及びペネトレーションテスト、監査、リスク評価、及び実際のインシデント	知関連手順の有効性を評価し、継続的に改善を行う必要があります。 顧客のリスク評価および管理を支援するため、Tencent Cloud は、Cloud Security Center (CSC) を提供しています。クラウドセキュリティセンターは、クラウド上の資産に対するワンストップのセキュリティ管理をサポートしており、資産の自動棚卸し、各種セキュリティリスクの検出・特定、およびセキュリティリスクへの自動対応・処置が含まれます。クラウドセキュリティセンターは、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、クラウドリソース構成リスク、サービス露出の6大リスクを定期的に検出し、企業のセキュリティ状況を継続的に監視します。また、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的に取り込み、アラートログの監査、分析、集約、一元的な表示および追跡を行います。さらに、クラウドセキュリティセンターはオーケストレーション機能を活用し、お客様が自動化された対応と処置を事前設定できるようにすることで、脅威への対応効率を向上させます。 お客様はさらに、Performance Testing Service (PTS) を選択することも可能です。PTS は、膨大なユーザーをシミュレートした実際の業務シナリオを通じて、システムの可用性と安定性を包括的に検証します。PTS は、百万単位の同時接続と多地域からのトラフィック発生能力、ならびにトラフィック記録、シナリオオーケストレーション、トラフィックカスタマイズ、高度なスクリプトカスタマイズなどの機能を提供し、迅速にビジネスモデルに基づいて負荷テストシナリオを定義し、大規模な

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		から得られた推奨事項、発見事項、教訓については、関連手続等に従って改善すること。 【対応が望ましい事項】 a. 脅威環境の変化、技術の進歩、得られた教訓に応じて、監視・検知に係る関連手続を少なくとも1年に1回は評価し、改善すること。 b. パフォーマンス指標 (KPI) 及びリスク指標 (KRI) を測定・評価し、経営陣に報告する仕組みを整備すること。また、具体的な目標及び達成指標を設定し、改善の状況及び課題を特定すること。	業務アクセスシナリオを現実的に即して再現することで、お客様が事前にアプリケーションのパフォーマンス問題を特定することを支援します。 お客様の規制遵守を支援するため、Tencent Cloud は内部で情報セキュリティリスク管理手順を策定し、リスク管理の全プロセス（リスクの特定、リスク分析、リスク対応計画の策定、およびリスクの追跡・監視）における業務内容を明確に定義し、指針を示しています。 リスクの特定: Tencent Cloud は少なくとも年1回リスク評価を実施し、業界のセキュリティインシデント報告、Tencent Cloud の実践蓄積、専門機関のリスクデータベースなどの情報源から、Tencent Cloud に適用されるリスクシナリオを特定します。また、リスクシナリオや業務製品・サービスのプロセス分析結果に基づいてリスクを特定します。 リスク評価: テンセントクラウドは、資産価値、リスクシナリオの発生可能性、リスクの影響度を評価し、リスクレベルを算出します。 リスク対応: リスク分析の結果に基づき、特定されたリスクに対して、テンセントクラウドは対応戦略および適切な緩和措置を講じます。高リスクについては、リスク責任者がリスク対応計画（リスク移転またはリスク低減措置）を策定し、リスク管理表を更新します。中リスクについては、リスク責任者が実際の環境に基づき、リスク対応計画の策定が必要かどうかを判断します。低リスクは許容可能なリスクとみなされます。残存リスクについては、テンセントクラウドが

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			年1回レビューを行い、その状態とリスク値を監視します。 ・ リスクの監視、レビュー、および報告: Tencent Cloud はリスク評価結果を集約し、リスク評価報告書を作成して経営陣に報告します。また、リスク管理表を維持管理し、リスク条件の変化やリスク対応計画の状況を監視し、リスク管理計画をリアルタイムで調整します。 さらに、テンセントクラウドは主要リスク指標を定義し、定期的に主要リスク指標を測定し、許容リスク基準と照合して、発見された問題の根本原因を分析し、改善の提案と案を提示する。
2.2.3	ハードウェア・ソフトウェア等の脆弱性管理	【基本的な対応事項】 ①ハードウェア・ソフトウェア等の脆弱性管理に係る手続等を策定し、必要に応じて見直すこと。 ②入手した脆弱性情報は、ハードウェア・ソフトウェアの脆弱性管理に係る手続等に基づき、対応の要否を判断すること。 ③システムの重要度、リスク又は脆弱性の深刻度に基づいたパッチ適用等の対応期限を設定するとともに対応実績を管理すること。 ④深刻度の高い脆弱性が判明した場合、情報システム及びハードウェア・ソフトウェア等に関する台帳等に基づき、影響を受ける情報システム等を特定し、速やかに対応すること。 ⑤深刻度の高い脆弱性については、グループ会社、海外拠点が保有するシステムについても、脆弱性対応の範囲に含めること。 ⑥深刻度の高い脆弱性については、重要なサードパーティが保有するシステム（共同利用型のシ	顧客は、ハードウェア/ソフトウェアの脆弱性管理に関連する手続を策定し、取得した脆弱性情報を評価した上で、システムの重要度、リスク、または脆弱性の深刻度に基づいて対応措置を講じ、管理を行うべきである。顧客は、対応措置を実施しない例外的な状況に対して、関連する承認手続を確立すべきである。深刻度の高い脆弱性については、顧客はクラウドサービスプロバイダーなどの第三者が保有するシステムの脆弱性対応措置を管理すべきである。管理の過程では、第三者保証報告書(SOC2 報告書など)や契約書などの文書を活用することを検討できる。 顧客の脆弱性およびリスク管理を支援するため、Tencent Cloud は、Cloud Security Center (CSC)を提供しています。 クラウドセキュリティセンターは、クラウド上の資産に対するワンストップのセキュリティ管理をサポートしており、資産の自動棚卸し、各種セキュリティリスクの検出・識別、およびセキュリティリスクに対する自動対応・処置が含まれます。テンセントの情報分析能力を基盤として、ク

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		テムを含む)の脆弱性対応の管理を行うこと。なお、管理にあたっては、第三者保証による報告書(SOC2 など)や契約書等を活用することが考えられる。 【対応が望ましい事項】 a. 深刻度の高い脆弱性については、クラウド事業者を含むサードパーティ(上記⑥のサードパーティを除く)が保有するシステムの脆弱性対応の管理を行うこと。なお、管理にあたっては、第三者保証による報告書や契約書等を活用することが考えられる。	クラウドセキュリティセンターはお客様に最新の脆弱性情報をプッシュ通知し、脆弱性の影響範囲や対処策の提案などを含む詳細なレポートを提供することで、高リスクな脆弱性に対する迅速な検知と対応を支援します。また、クラウドセキュリティセンターはオーケストレーション機能を活用し、お客様が自動化された対応策を事前に設定できるようにすることで、脅威への対応効率を向上させます。 顧客の規制遵守を支援するため、テンセントクラウドは脅威および脆弱性管理に関する手順を確立し、情報システムが直面する脅威や脆弱性を迅速に特定し、改善または修正するための措置を講じます。テンセントクラウドは情報システムに対して定期的に脆弱性スキャンおよびペネトレーションテストを実施し、テストプロセスにおいて過去に発見された脅威や脆弱性を再検証するとともに、テストを繰り返し実行することで脆弱性の修正状況を確認します。スキャンまたはテストの過程で特定されたセキュリティリスクは、セキュリティチケットを通じて関連部門に通知され、評価およびフォローアップ処理が行われます。評価の結果、脆弱性が顧客の業務に影響を及ぼす可能性があることが判明した場合は、公式サイトでの告知やサイト内メッセージを通じて、速やかに脆弱性に関する情報を顧客に通知します。通知内容には、脆弱性の説明、影響範囲および程度、Tencent Cloud が講じた管理措置、顧客への修正提案、具体的な操作手順などが含まれますが、これらに限定されません。 さらに、Tencent Cloud は定期的に独立した第三者による専門的な監査を受け、証明的な性質を持つシステムおよび組織統制レポートを提供することで、クラウドユーザー機関、独立監査人、規制当局、会社の株主、およびその他の利害関係者に、Tencent Cloud 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

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			においては、Tencent Cloud は『FISC 金融機関等コンピュータシステムセキュリティガイドライン』に基づき、管理状況の評価を行い、これに基づいて Tencent Cloud プラットフォームの安全性、可用性、機密性に関連する管理項目を網羅した、対応するシステムおよび組織管理（SOC）報告書を作成しています。
2.2.4	脆弱性診断及びペネトレーションテスト	【基本的な対応事項】 ① システムの脆弱性対策やセキュリティの問題点を特定し、改善するために、リスクの大きさやシステムの重要度等も考慮した上で脆弱性診断及びペネトレーションテストを定期的実施すること。また、関連する手続等を策定し、必要に応じて見直すこと。 【対応が望ましい事項】 a.脆弱性診断及びペネトレーションテストは、インターネットに直接接続していない VPN 網、内部環境も対象とすること。 b.定期的に脅威ベースのペネトレーションテスト（TLPT）を実施すること。 c.自組織のシステム環境を熟知する内部人材によるペネトレーションテスト。 d.ペネトレーションテストの方法及び結果を定期的にレビューし、新たな独立した視点を得るためにテストベンダーの交代要否を検討すること。	顧客は、脆弱性検査およびペネトレーションテストに関する手順を策定し、定期的に脆弱性検査およびペネトレーションテストを実施し、発見された問題の優先順位付けを行い、対応方法と対応期限を決定し、対応状況をフォローアップしなければならない。 ペネトレーションテストに関しては、Tencent Cloud はお客様に Penetration Testing Service (PTS) を提供しています。これは、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、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のセキュリティを詳細に調査します。これにより、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言を通じてお客様のシステムセキュリティ向上を支援するとともに、脆弱性修正後の検証もサポートします。 脆弱性スキャンに関しては、お客様は Vulnerability Scanning Service (VSS) を利用して、企業のネットワーク資産を調査し、そのリスクを特定することができます。テンセントが長年にわたり蓄積してきたセキュリティ経験と脅威インテリジェンスに基づき、VSS は豊富かつ包括的な脆弱性ルールベースを構築し、専門的かつ効率的な 0Day/1Day/NDay 脆弱性検出能力を備えています。これにより、お客様の資産の可用性、セキュリティ、コンプライアンスなどに対して、定期的なセキュリティ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			スキャン、継続的なリスク警告、脆弱性検出を実施し、専門的な修正提案を提供することで、セキュリティリスクを低減します。また、VSS はホストセキュリティや Web アプリケーションファイアウォールなどのクラウド製品との連携をサポートし、リスク監視からリスク対応までの閉ループを実現します。 お客様の規制遵守を支援するため、Tencent Cloud では社内で定期的な脆弱性スキャンおよびペネトレーションテストの仕組みを確立しています。 Tencent Cloud 内部の脆弱性スキャンには通常、Web 脆弱性、コンポーネント脆弱性、設定スキャンなどが含まれます。脆弱性スキャンシステムを通じて自動的にスキャンタスクを生成し、クラウド環境内の資産に対して脆弱性スキャンを実施するとともに、発見された脆弱性の分析、分類、および修正処理を行います。ペネトレーションテストに関しては、Tencent Cloud のセキュリティチームが定期的にエンドツーエンドの大規模なペネトレーションテストを実施しており、新製品のリリース前や重大な変更時などには、状況に応じて柔軟に絞ったペネトレーションテストを実施しています。テスト結果はセキュリティチケットを通じて関連責任部門に通知され、責任部門が速やかに脆弱性の修正やその他の是正措置を実施することで、ペネトレーションテストで発見された悪用可能な脆弱性が適切に処理されることを保証します。さらに、Tencent Cloud では定期的にレッドチーム対ブルーチームの対抗演習を行い、ネットワーク攻撃への防御を実戦形式でシミュレートしています。
2.2.5	演習・訓練	【基本的な対応事項】 ①組織におけるサイバーインシデント対応計画及びコンティンジェンシープランの実効性を確認し、課題を把握した上で継続的に改善	顧客は、組織のサイバーセキュリティインシデント対応計画および緊急時対応計画の有効性を確認するため、定期的に演習および訓練を実施し、演習中に発見された問題等に基づいて計画および対応策を改訂

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		するために、定期的な演習・訓練を実施すること。また、必要に応じて、演習・訓練への外部委託先の参加を検討するほか、業界横断的な演習に参加すること。 ②経営陣、サイバーセキュリティを統括管理する責任者（CISO 等）及び業務部門の責任者が自らサイバー演習・訓練等に関与し、その結果を把握すること。 ③演習・訓練のシナリオには、顧客に深刻な影響を与え、かつ現実起こりうるシナリオを含めて検討すること。 ④演習・訓練を通じて、業務継続等の観点でサイバーインシデント対応計画及びコンティンジェンシープランの有効性を定期的に検証し、演習・訓練で得られた課題や教訓等を踏まえ見直すこと。 ⑤演習・訓練の手法・シナリオ等について、最新の脅威動向等に応じて見直しすること。 【対応が望ましい事項】 a. 実機等を用いた復旧訓練においては、システム及びデータの復旧手順の適切性並びに復旧目標（目標復旧時点（RPO）、目標復旧時間（RTO））の妥当性の確認を含めること。 b. 自組織に大規模かつ長期間にわたる影響を及ぼすインシデントや、金融システム全体に深刻な影響が波及するシナリオを用いた演習・訓練を実施すること。 c. 演習・訓練を通じて判明した課題に対する改善内容については、再度演習等を実施してその有効性を検証すること、又は残存リスクを許容することについて経営陣等	しなければならない。復旧訓練を行う際、顧客はシステムおよびデータ復旧プロセスの適切性、ならびに目標復旧時点（RPO）および目標復旧時間（RTO）の妥当性を確認しなければならない。顧客は各種の訓練および演習を組み合わせて実施し、必要に応じて外部委託業者を演習に参加させることを検討しなければならない。 お客様は、の Tencent Smart Advisor (TSA) サービスを活用し、事業継続性テストの計画および実施を支援することができます。本サービスは、複数の ITOM 分野における垂直アプリケーションに対応したクラウド上のガバナンスプラットフォームであり、Tencent Cloud の膨大な運用保守専門家の経験に基づき、リスク点検や障害演習などの多角的なガバナンスを通じてクラウドインフラストラクチャを最適化します。Tencent Cloud Advisor は、IaaS から PaaS に至るまでの各種障害注入シナリオや、多業界にわたる演習経験テンプレートを提供します。アベイラビリティゾーンを跨ぐ災害対策など、多くの典型的なユースケースを網羅しており、お客様が自社のビジネスニーズに応じて、成熟したソリューションを迅速かつ効率的に再利用し、システムの可用性を向上させることを支援します。 顧客の規制遵守を支援するため、Tencent Cloud では、緊急対応および災害復旧の訓練・テストを定期的に行っています。訓練計画についてはリスク評価を行い、訓練がサービスに悪影響を及ぼさないように対策を講じています。Tencent Cloud の災害復旧演習は、攻撃・防御の対抗演習や大規模障害など、現実的な典型的な災害シナリオを模擬して実施されることが多く、システムの災害耐性、応答速度、復旧能力を包括的に検証します。演習終了後、関連部門は演習報告書を作成し、改善策に基づい

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		の承認を得ること。	て是正措置を講じ、報告書をアーカイブして保管します。
		d. 訓練・演習等 については、それぞれの規模・特性を踏まえ、これらを組み合わせて実施すること。	Tencent Cloud は毎年、事業継続マネジメントシステム (BCM) の見直しと更新を行い、事業影響分析の結果に基づき、関連製品およびサービスの事業継続計画 (BCP) と災害復旧計画 (DRP) を精査し、必要に応じて更新します。 適切な状況下では、テンセントクラウドはお客様のセキュリティ演習に対し、関連する技術サポートを提供することも可能です。

6.3 サイバー攻撃の防御

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			お客様は、サイバー攻撃を防ぐために多層防御措置を講じる必要があります。 ネットワーク境界の保護を実施するため、 Tencent Cloud はお客様に Cloud EdgeOne (EO) を提供しています。これは Tencent のグローバルエッジノードを基盤として、セキュリティ保護と高速化サービスを提供するもので、DDoS 防御、インテリジェント Web 防御、ポット/クローラー攻撃防御 DNS 解決などの機能を備えており、お客様は業務ニーズに応じて独自のアクセス制御ルールを設定することも可能です。また、お客様は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、および Anti-DDoS などのネットワーク境界保護ツールも選択可能です。 Cloud Firewall (CFW) 主にさまざまなネットワーク境界の保護を提供し、ファイアウォール ACL による能動的な制御、IPS によるリアルタイム遮断、仮想パッチ、悪意のあるコードの検出などの機能をサ
2.3	サイバー攻撃の防御	【基本的な対応事項】 ①サイバー攻撃に備え、不正侵入を防止するための境界ネットワーク対策、内部ネットワークでのシステム不正利用を防止するための対策、外部への情報漏洩対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じる こと。	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ポートしています。従来のネットワークにおける DMZ エリアの要件を実現し、コア資産を重点的に保護するとともに、VPC 間のきめ細かな分離管理を実現します。 Web Application Firewall (WAF) Web 攻撃、侵入、脆弱性悪用、マルウェア注入、改ざん、バックドア、クローラーなど、Web サイトおよび Web サービスのセキュリティ保護課題に対応します。Anti-DDoS 豊富で高品質な DDoS 防御リソースと、継続的に進化する「自社開発 + AI による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 攻撃に対処します。 ネットワーク通信セキュリティの面では、 Tencent Cloud コンソール上での通信は HTTPS セキュリティプロトコルによる暗号化保護を受けています。お客様がいつでも、どこでも、あらゆる主要な端末を使用して、安全かつ迅速にクラウド上の業務システムにアクセスできるよう、Tencent Cloud は SSL VPN リモートアクセス技術をサポートしています。SSL VPN は、インターネット上で転送されるデータのセキュリティを暗号化によって保護するほか、適切なアクセス制御をサポートし、不正アクセスの発生を低減します。さらに、お客様は Cloud Connect Network (CCN) を利用して、クラウド上のプライベートネットワーク間 (VPC) や、VPC とオンプレミスデータセンター間 (IDC) の安全な内部ネットワーク相互接続を実現できます。 お客様の規制遵守を支援するため、Tencent Cloud はネットワークセキュリティ管理規範および多層防御システムを確立しています。 Tencent Cloud 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の管理・制御および保護基準、ならびに対応する役割と責任を明確化し、

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			Tencent Cloud のネットワーク上で稼働する業務の安全な運用を確保しています。同時に、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区分し、異なるセキュリティドメインを物理的または論理的に分離することで、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 防御、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迅速に検知、フィルタリング、および阻止し、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ています。 マルチテナント環境におけるデータ分離 については、テンセントクラウドは「データの機密性」の原則を厳守し、仮想化制御層の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のプライベートネットワーク間の分離ポリシー、Web コンソールの権限割り当てと認証、インターフェースのセッション ID とアクセスキーなどの多層的な技術的分離手段を通じて、テナントが他のテナントのデータにアクセス、取得、または改ざんできないように確保しています。 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

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			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、防止しています。
2.3.1	認証・アクセス管理	【基本的な対応事項】： ①認証及びアクセス権の付与に係る方針及び規程等を策定し、定期的に見直すこと。 ②システムへのアクセス権限は、正当な業務上の要請があり、承認され、適切に教育・研修を受け、管理されている個人に対してのみ付与すること。また、ユーザによる機器及びシステムへのアクセス権限は、システムや情報の重要度を考慮して付与すること。 ③機器 (API に認証情報を組み込むことを含む) 及びユーザの ID 及び認証情報を適切に管理すること。 ④ID を認証し、システムへのアクセスを許可する前にユーザのアクセス権限の適切性を検証すること。また、アクセスしたユーザを特定できる措置を講じ、処理内容をログに記録し、ユーザの操作内容と対応させること。 ⑤システムや情報の重要度に応じて、認証要件を決定すること。特に、重要なシステムへのリモートアクセスには、多要素認証を使用すること。 ⑥第三者による不正行為を阻止するための仕組みや取組みを活用すること (メールの送信ドメイン認証 (SPF/DKIM/DMARC)、安全なファイル交換機能、顧客へのサポートと啓発活動 (注意喚起やセミナー) 等)。	顧客は、認証およびアクセス権限の付与に関する規範と手順を策定し、定期的に権限の見直しを行うものとする。顧客は、機器およびユーザの認証情報を適切に保管し、ユーザがシステムにアクセスする前に、アクセスするユーザを識別し、そのアクセス権限を検証し、ユーザの操作および処理内容をログに記録するための措置を講じるものとする。さらに、顧客は、高度に機密性の高い区域およびコンピュータ室、データ保管室などの重要な部屋への物理的アクセスを管理、保護、記録するものとする。 アクセス制御管理の面において、Cloud Access Management (CAM) は、お客様が Tencent Cloud の製品およびリソースへのアクセスを安全かつきめ細かく管理し、リソースごとに異なるユーザーに特定の権限を付与することを支援します。その中で、ユーザーメインアカウントはサブユーザーを作成し、サブユーザーに ID、認証情報、および権限を割り当てることができます。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規則を変更することができます。CAM は、MFA デバイスによる認証や携帯電話の認証コードによる認証など、さまざまな方式の二要素認証機能をサポートしており、ログイン時や機密性の高い操作を行う前に、本人確認と環境の安全性を確認できます。また、CAM は CloudAudit を通じて、Tencent Cloud アカウントのアクティビティに対する監視、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しています。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		⑦シングルサインオンや外部認証連携等、システム間又はセキュリティ境界にまたがる認証及び認可における機密性、完全性及び真正性等を確保すること。 ⑧機密性の高い区域及びコンピュータ室、データ保管室等重要な室への物理的アクセスを管理し、保護し、記録すること。	また、Tencent Cloud は Bastion Host (BH) を提供しており、ユーザー、資産、アカウント、操作権限などの次元に基づいたきめ細かな権限付与をサポートし、ユーザーが保有する権限が、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。フォートレスマシンも同様に操作監査機能をサポートしており、ユーザーの操作ログを記録・分析することで、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。 顧客の規制遵守を支援するため、Tencent Cloud は社内でアクセス制御管理規範を策定し、ユーザーアカウントには一意の識別子を使用することを義務付け、セキュリティベースラインに基づいて従業員アカウントのパスワードポリシーを設定しています。Tencent Cloud 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アクセス認証を行い、ユーザーが内部リソースにアクセスするには、まず二要素認証を完了する必要があります。 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。Tencent Cloud は、役職・役割に対応する担当者の身元情報と各業務システムの権限レベルに関する記録を管理し、定期的な内部権限監査を実施することで、権限の乱用や誤用がないよう確保しています。さらに、テンセントクラウドの本番環境には「堡垒機 (Bastion Host)」が全面的に導入されており、堡垒機を通じてテンセントクラウドの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的に管理していま

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			す。堡垒機へのアクセスには承認が必要であり、特定のテンセントクラウド内部の運用保守担当者のみがアクセス可能で、堡垒機へのログインには適切な本人確認が必要です。運用保守操作の記録はログプラットフォームに一元的に保存され、テンセントクラウドの内部監査チームが定期的にログの監査を行っています。 物理的なアクセス制御に関しては、テンセントクラウドの各データセンターは、異なるレベルの地域セキュリティ要件に基づき、厳格なアクセス制御ポリシーを策定しています。あらゆる種類の訪問者や従業員がデータセンターに出入りする際は、本人確認と所持品の検査を行い、持ち込み物品を登録する必要があります。テンセントクラウドは、人員の区分とアクセス権限に基づき、データセンターの入退室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ックスを構築し、データセンターにおける各種人員のアクセスや操作などの行動を効果的に管理しています。さらに、テンセントクラウドの金融専用エリアの物理サーバールームでは、専用ケージを用いて異なる顧客の機器を物理的に隔離するとともに、生体認証入退室管理システムを導入しており、権限のない者が顧客の機器に接触することを効果的に防止しています。
2.3.2	教育・研修	【基本的な対応事項】 ①経営陣を含むすべての役職員に対して、役割と責任に応じたサイバーセキュリティの意識向上に係る教育・研修を定期的実施すること。 ②サードパーティ在籍の担当者が、業務を適切に行う上で必要となるサイバーセキュリティの教育・研修を受講していることを確保すること 32。なお、本対応には、	顧客は、全従業員に対して定期的に必要な教育・研修を提供し、関連する従業員のスキルと知識レベルを維持・向上させるとともに、第三者の担当者がその職務を遂行するために必要なサイバーセキュリティ教育・研修を受講していることを確認しなければならない。さらに、顧客は、必要に応じて、自組織の顧客に対し、サイバー攻撃の脅威を理解し、サイバーセキュリティ意識を向上させるのに役立つ措置を実施しなければならない。 Tencent Cloud 製品の操作手順、ユーザー

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		サードパーティによる社内教育・研修が実施されていることを金融機関等が確認することをもって受講を確保することも含まれる。 ③顧客に対し、必要に応じ、サイバー攻撃の脅威及びサイバーセキュリティの意識向上に資する取組みを実施すること。 ④IT 又はセキュリティを所管する部門の役職員に対して、脅威及び対策の変化等、最新の知識とスキルを維持するための教育・研修を定期的実施すること。 ⑤すべての役職員に対して、自身がインシデントの当事者となった場合に適切な対応を行うために、必要な教育・研修等の機会を確保すること。また、インシデント対応及び復旧計画における役割及び運用手順に係る教育・研修を、関係する役職員に対して、定期的実施すること。 【対応が望ましい事項】 a.フォレンジック調査等を内部の役職員で実施する場合は、該当する役職員のスキルと知識を維持・向上させること。 b.脆弱性診断やペネトレーションテストを内部の役職員で実施する場合は、該当する役職員のスキルと知識を維持・向上させること。	マニュアル等は文書化され、公式ウェブサイトを通じてお客様に提供されています。また、Tencent Cloud は、Tencent Cloud 製品の基礎知識および関連する専門能力に基づくトレーニングおよび認定を提供し、お客様の技術力とクラウドの習熟度向上を支援しています。さらに、Tencent Cloud は、24 時間 365 日対応のチケットシステム、24 時間 365 日対応のホットライン、AI カスタマーサービス、セルフサービスなど、複数のチャネルを通じて、顧客からの質問やフィードバックに絶えず対応しています。テンセントクラウドのカスタマーサポートチームと技術専門家は、お客様に迅速かつ効果的なサポートを提供します。 顧客が規制ガイドラインを順守できるよう、テンセントクラウドは研修体制を構築し、正社員、コンサルタント、インターン、外部委託スタッフなどに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、全従業員必修研修、重点職務向け専門研修、選択制の専門コースなど、多様な研修コースを提供しており、その内容は、基本的なセキュリティ意識、オフィスセキュリティ、脆弱性の特定と防御、プライバシー保護、インシデント対応、研究開発のセキュリティ基準、データセキュリティ要件などを網羅しています。
2.3.3	データ保護	【基本的な対応事項】 ①情報の重要度と、使用される技術環境における固有のリスクに応じて、データの管理方針を策定すること。管理方針には、データの管理、データの保存、適切な暗号化方式を採用することや、暗号鍵と電子証明書を、そのライフサイクルを通じて管理し、保護すること。	顧客は、データのライフサイクルを通じてデータを保護・管理するため、データ管理方針 / ポリシー、外部記憶媒体の保護および使用管理手順、バックアップ手順などを策定し、実施する必要があります。顧客は、従業員や外部関係者によるデータ漏洩を監視・防止するため、データ漏洩防止 (DLP) または同等の機能を有するシステムを導入する必要があります。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		と、危殆化時の対応などを含めること。	データストレージの保護に関しては、 Tencent Cloud の多くのストレージおよびデータベース製品がデータ暗号化機能をサポートしており、安全で高強度の暗号化アルゴリズムを使用しています。また、 Key Management Service (KMS) を統合することで、キーのライフサイクル全体にわたる管理を実現し、データの機密性を確保しています。<u> </u>は、FIPS-140-2 認証を取得したハードウェアセキュリティモジュール (HSM) を使用してキーを生成・保護し、顧客の暗号化キーのライフサイクル全体にわたる管理をサポートします。鍵の解読や悪用リスクを低減するため KMS は鍵のローテーションをサポートし、無効化、失効、または漏洩した鍵を安全かつ確実な方法で削除します。削除された鍵は復元不可能となり、その鍵で暗号化されたデータも復号できなくなります。さらに、Tencent Cloud はデータの保存において、マルチレプリカ冗長ストレージとエラー訂正コード (ECC) 技術を採用しており、整合性のエラーを検出した際には直ちに必要な復旧措置を講じることで、データの耐障害性を大幅に向上させています。 データ転送の保護に関しては、 Tencent Cloud コンソール上での顧客の通信はすべて HTTPS セキュリティプロトコルによる暗号化保護の対象となります。Tencent Cloud のクラウド製品が提供するクラウド API インターフェースも、HTTPS 暗号化、署名検証、ステータス監視などのセキュリティ機能を備えており、顧客のビジネスにポートレベルの通信セキュリティ保証を提供します。さらに、顧客は以下の Tencent Cloud サービスを利用して、さまざまなシナリオにおける安全なデータ転送を実現できます：
		②情報の重要度に応じてデータを分類し、分類に応じた管理方針に従ってデータを保護すること。	
		③外部記憶媒体の保護と使用に係る管理手続を策定し、実施すること。	
		④ライフサイクル全体を通じて、データを適切に管理すること。	
		⑤システム及び情報の重要度に応じたバックアップ要件、バックアップデータの隔離と保護、整合性の検証、復旧テストの実施等を含む、バックアップに関する規程等を整備し実装すること。	
		【対応が望ましい事項】	
		a. DLP 又はそれに相当するものを導入し、役職員や外部関係者によるデータ漏えいを監視し、保護すること。	
		b. 法令上の責任や組織の資産としての情報の重要性に従って、データ・ガバナンスに関する方針及び規程等を策定すること。	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			<u>Direct Connect (DC)</u> : 専用性と高いセキュリティを備えた大容量の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回線を独占するため、データ漏洩のリスクがありません。 <u>VPN Connection</u> : ネットワークトンネル技術に基づき、ローカルデータセンターと Tencent Cloud 上のリソース間を安全に接続します。VPN トンネルは IKE (鍵交換プロトコル) と IPsec を採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することで、転送中のデータの安全性を確保します。 <u>Cloud Connect Network (CCN)</u> : クラウド上のプライベートネットワーク間 (VPC) 、および VPC とローカルデータセンター間 (IDC) の内部ネットワーク相互接続をサポートし、ネットワーク全体のマルチポイント相互接続、ルーティングの自己学習、リンクの最適化、障害時の迅速な収束などの機能を備えています。クラウド・コネクティビティ内のネットワークインスタンス間のすべての通信データはパブリック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、および低遅延、低パケットロス率などの特性を備えています。また、多段階のリンク冗長化により通信品質を保証し、データの安全性と信頼性を確保します。 データバックアップに関しては、Tencent Cloud はクラウド製品またはサービスの機能に基づき、顧客に複数のストレージレプリカおよびバックアップサービスを提供し、サービスレベル契約 (SLA) の規定に従い、提供され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。Tencent

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			Cloud が提供するコンピューティングサービス、ネットワークサービス、ストレージサービス、データベースサービス、コンテナおよびミドルウェアサービスなど、多様なクラウド製品・サービスは、お客様が自身のシステムおよびデータのバックアップ戦略を設定することをサポートし、お客様のあらゆるバックアップニーズを満たします。バックアップに関する詳細については、本ガイドの第 5.2.3 章「実 39 データファイル管理」の条項をご参照ください。 データ漏洩防止に関して、Tencent Cloud はお客様に 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おける各種セッション情報、アクセス操作、SQL 文の全量監査と記録をサポートします。また、多様なルールベースと脅威検知エンジンに基づき、操作中の悪意ある行為を識別し、管理者に速やかに通知して、適切なセキュリティ対策を実施できるようにします。 データの削除および破棄に関しては、 Tencent Cloud は安全かつ信頼性の高い データ破棄メカニズムを提供しています。お客様のサービス終了後、テンセントクラウドはお客様とのサービス契約に基づき、厳格なデータ消去手順に従い、保存期間満了後にレプリカやバックアップを含むお客様データを完全に削除します。削除されたデータは復元できません。また、テンセントクラウドサービスの提供に使用される媒体に故障が発生して交換が必要になった場合、または使用期限が到来して廃棄が必要になった場合、テンセントクラウドは厳格な手順に従い、速やかに完全な物理

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			的破棄を行います。 お客様の規制遵守を支援するため、テンセントクラウドはデータセキュリティに関する管理手順を確立し、データの分類・格付けおよびデータ保護原則を明確化しています。データ所有者に対し、データの分類・格付け要件に基づき、データの収集、転送、アクセス制御、バックアップ、取引保護、および第三者との情報転送管理といった全ライフサイクルにおいて、相応のセキュリティ保護措置を実施し、データの機密性、完全性、可用性を保護することを求めています。顧客データは Tencent Cloud 内部において高セキュリティレベルのデータに分類され、顧客は自身のデータ内容に対して唯一の所有権および管理権を有します。サービスの提供やトラブルシューティングの必要性がある場合、または顧客の明確な承認を得た場合、あるいは国家・地方政府機関による犯罪事件の調査など、国家の法律法規に準拠する場合を除き、Tencent Cloud の従業員が顧客データに自発的にアクセスすることは決してありません。 さらに、テンセントクラウドはデータアクセス権限に対し、全ノードでの实名制による審査および管理を実施し、データ資産の完全性と業務サービスの信頼性を確保するとともに、リアルタイムの監視および遮断メカニズムを構築し、異常なデータアクセス行為を検知・阻止しています。また、テンセントクラウドは従業員の業務端末に、データへの外部エクスポートを制限できるデータ漏洩防止 (DLP) ツールを導入し、潜在的なデータ窃取活動を監視・検知・防止しています。
2.3.4	システム のセキュ リティ対 策	【基本的な対応事項】 ①必要な機能のみを提供するようにシステムを構成すること。 ②システムの保守におけるサイバ	顧客は、システムに必要な機能のみを提供するように構成し、システムの運用・保守プロセスにおけるサイバーセキュリティを確保するための手順を策定し、システムをマルウェアの感染から保護しなければ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		ーセキュリティを確保するための 手続を定めること。 ③サポートの終了に伴うハードウェア・ソフトウェアの廃止・更改を計画的かつ安全に実施すること。ソフトウェアについてサポート対象バージョンへの更新が困難な場合には、補完的な措置を講じるとともに、迅速にサポートが得られるソフトウェアを利用したシステム・ビジネスプロセスへの移行計画を立て、着実に実行すること。 ④システムをマルウェアの感染から保護すること。 【対応が望ましい事項】 a. システムで利用するサードパーティのライブラリやミドルウェア、ハードウェア については、不正侵入の経路となるバックドア等が含まれることのないように、セキュリティ・バイ・デザインやセキュリティ・バイ・デフォルト 34 等の安全な開発手法を製品開発に取り入れている事業者から提供される安全なプロダクト を選定すること。 b. サプライチェーンのリスク評価の中で、ハードウェアに関するサイバーセキュリティリスクを評価対象とすること。 c. ハードウェア（機器、ファームウェア、UEFI 又は BIOS 等）の真正性を確保し、また、不正な書き換えを防止するための対策（改竄検知など）を導入すること。 d. ハードウェアの調達基準等にセキュアな調達のための基準を設けること。調達基準や取引基準の中	ならない。サポート終了となるハードウェア / ソフトウェアについては、顧客は安全な廃棄または更新の計画を策定しなければならない。また、顧客はハードウェア調達のための安全な調達基準を策定し、サプライチェーンリスク評価においてハードウェアに関連するサイバーセキュリティリスクの考慮を組み込まなければならない。 お客様は、Cloud Workload Protection Platform (CWPP) を採用することができます。このサービスは、テンセントが蓄積した膨大な脅威データに基づいており、お客様のベースラインセキュリティ管理を支援します。CWPP は、ワンクリック検出や定期検出などのオプションモードを含むベースライン検出をサポートし、ベースラインの合格率や修正提案の確認も可能です。また、CWPP はテンセントクラウドのデフォルトベースラインポリシーも提供しており、お客様がサーバーのベースラインセキュリティをより適切に管理するのに役立ちます。 Cloud Security Center (CSC) は、クラウド製品の設定リスクに対する自動検査・評価機能を提供します。クラウドサーバー、オブジェクトストレージ、クラウドデータベース、ロードバランサーなど、多種多様なクラウド製品をカバーし、クラウド製品の利用における誤ったセキュリティ設定に起因するセキュリティリスクを低減し、クラウド上のセキュリティレベル全体を向上させます。 また、お客様は Config を通じて、クラウドリソースの集中監査とガバナンスを実現できます。これにより、お客様アカウント下の異なるリージョンにおける各種クラウドリソースの設定情報や変更履歴を

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		で、調達先又は取引先の法令順守、自組織のセキュリティ基準又は倫理基準などの社内基準の遵守を求めること。法令、社内基準、国連制裁等を踏まえたサプライヤーリスト又は制裁対象リストを作成、維持し、これらを踏まえた調達を実施すること。	継続的に記録し、Tencent Cloud のベストプラクティスに基づくルールやコンプライアンスパッケージテンプレートに基づき、企業アカウント下のクラウドリソース設定に対して継続的なコンプライアンス評価を自動的に実施し、非準拠なリソース設定を特定することで、クラウドリソースの自動監視と管理を実現します。 顧客が規制当局の指針を遵守できるよう、Tencent Cloud は構成管理データベース (CMDB) を通じてハードウェアおよび設備の詳細なリストを管理しており、このリストには各サーバーのサポート終了日 (End-of-Support Date) およびプラットフォームのバージョン情報が含まれています。Tencent Cloud は定期的にサーバーの退役および交換を行い、ソフトウェアコンポーネント (OS やデータベースシステムなど) については、サポート終了前に適切なバージョンへ更新します。退役したハードディスクについては、Tencent Cloud は安全な物理的破棄方法を採用し、ハードディスクが完全に破棄されることを保証するとともに、破棄記録にその旨を登録します。 ホストセキュリティの面では、テンセントクラウドはエンドポイント検出・対応 (EDR) ツールを導入し、ネットワーク全体のサーバー端末資産に対して包括的な監視と管理を行っています。テンセントクラウドが採用する EDR ツールは、ウイルス対策や侵入検知、セキュリティベースラインおよび脆弱性スキャン、ならびにコマンド操作やログイン動作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ており、悪意のあるプログラムや異常な動作を検知した際にアラートを発動します。 セキュリティ開発の面において、テンセントクラウドは情報システムセキュリティ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			開発基準を確立し、ISO/IEC 20000 (情報技術サービス管理)、ISO/IEC 27001 (情報セキュリティマネジメントシステム)、および ISO/IEC 9001 (品質マネジメントシステム) の各規格を、製品のセキュリティ開発ライフサイクル全体に組み込むことに注力しています。具体的には、要件定義、設計、開発、テスト、納品、運用保守といった各段階に重点を置いています。テンセントクラウドはアジャイル開発手法を採用し、必要なソフトウェア開発ライフサイクル (SDLC) の原則およびセキュリティ・バイ・デザイン (Security-by-Design) の原則を取り入れることで、クラウド製品がそのライフサイクルを通じて十分なセキュリティ管理を受けられるよう確保しています。 ベースラインおよび構成管理の面では、テンセントクラウドは、ネットワーク機器、ファイアウォール、ホストサーバーのオペレーティングシステム、データベース、およ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して管理することを目的とした、一連の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確立しています。Tencent Cloud はスキャンツールを使用して、オペレーティングシステム、データベース管理システム、ネットワーク機器、および仮想イメージの設定をスキャンし、ベースラインファイルで定義された標準設定からの逸脱を継続的に検出します。標準からの逸脱が検出されると、システムは自動的にセキュリティチケットを生成し、責任部門に送信します。責任部門はこれに対し、速やかに対処します。 ソフトウェア / ハードウェアのセキュリティに関する詳細については、本ガイドの第 5.2.4 章「各種デバイスの管理」を参照

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			してください。
			お客様は、ログの取得、監視、保存の手順を策定し、定期的に見直す必要があります。また、情報システムのイベントログや運用担当者の作業ログについても、定期的に、または必要に応じて都度確認する必要があります。
			Tencent Cloud はお客様に 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 はログの収集、保存から検索・分析、リアルタイム利用、配信に至るまで多岐にわたるサービスを提供し、お客様の業務運用、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、ログデータを多重に冗長バックアップして保存することで、単一ノードのサービス停止によるデータ利用不能を防ぎ、サービスの高可用性を実現し、ログデータに対して安定かつ信頼性の高いサービス保証を提供します。 Cloud Security Center (CSC) は、クラウドセキュリティ製品のアラートデータ、クラウド資産の構成変更データ、クラウド上のユーザー操作行動データ、および一部のクラウド製品のログデータなど、各種クラウドセキュリティ関連データの収集をサポートしています。また、統一された検索・調査プラットフォームを提供し、お客様が包括的なクラウドログ監査と検索・調査を実現できるよう支援します。さらに、 Elasticsearch Service

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			<u>(ES)</u> サービスは、クラウドサーバーやコンテナなどの他のクラウド製品のリアルタイムログ、あるいは業務の既存データおよび増分データを、Tencent Cloud の ES クラスターに集約・転送し、データの分散型ストレージ、クエリ分析を行います。 操作ログの収集と保存に関しては、お客様 は <u>CloudAudit</u> を活用し、Tencent Cloud アカウントのアクティビティに対する監視、コンプライアンスチェック、操作監査、およびリスク監査を行うことができます。CloudAudit では、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、イベント日時、リクエスト ID、送信元 IP アドレス、ユーザー名を含む、過去 90 日以内の Tencent Cloud コンソールおよびクラウド API の操作記録をオンラインで確認できます。 Tencent Cloud 内部では、ログ収集および管理に関する規範と仕組みを確立しており、ログインログ、操作ログ、システムの通常ログ、システムセキュリティイベントログなどの記録、抽出、保存、保護、分析、監査などを管理・統制し、システム活動の異常やリスクを検知・防止しています。ログは Tencent Cloud のログ管理プラットフォームに一元的に集約され、管理されます。また、関連するログ情報に対してはバックアップおよび厳格な保護措置を講じ、不正な改ざんや削除を防止しています。バックアップログの保存期間は 1 年以上です。Tencent Cloud は、運用セキュリティ自動化監査ツールおよび内部監査チームを通じてログの監査を行い、システムや操作の異常を検知することで、操作リスクを防止しています。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			顧客は、金融商品およびサービスの設計段階で「セキュリティ・バイ・デザイン」を実施し、自組織にシステムを提供する重要なサードパーティがセキュリティ・バイ・デザインを実施できる体制を備えていることを確認すべきである。顧客は、セキュリティ・バイ・デザインに関連する管理プロセスを確立し、運用すべきである。 顧客の開発ライフサイクル管理を支援するため、Tencent Cloud は開発者ツール Cloud Native Build (CNB) を提供しています。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にソフトウェアを構築できるよう支援することを目的としています。CNB は、コードホスティング、高性能な開発パイプライン、AI コードレビュー、クラウド上の開発環境、アーティファクト管理、カスタムタスクセットなどの機能を備えた包括的な開発ツールチェーンを提供し、要件定義からデプロイまでの開発プロセス全体をサポートし、アジャイル開発管理を効果的に実現します。 テンセントクラウド内部でも、情報システムセキュリティ開発基準を確立しており、ISO/IEC 20000 情報技術サービス管理規格、ISO/IEC 27001 情報セキュリティマネジメントシステム、および ISO/IEC 9001 品質マネジメントシステム規格を製品セキュリティ開発ライフサイクルの全プロセスに統合することに注力しており、要件、設計、開発、テスト、納品、運用保守などの各段階に焦点を当て、製品開発のあらゆる段階で情報セキュリティとプライバシー保護の理念を取り入れ、クラウド製品がそのライフサイクルを通じて十分なセキュリティ管理を受けられるようにしています。関連するセキュリティ管理措置には以下が含まれます： • セキュリティ研修: セキュアコーディン
		【基本的な対応事項】 ① 金融商品・サービスの企画・設計段階から、セキュリティ要件を組み込む「セキュリティ・バイ・デザイン」を実践すること。サービス全体の流れの中で、重要なサードパーティも含めてリスクを検証し対策を講ずること。 ② 自組織にシステムを提供する重要なサードパーティにおいて、セキュリティ・バイ・デザインを実施できる体制となっているかを確認すること。 【対応が望ましい事項】 (a) セキュリティ・バイ・デザインに係る管理プロセスを確立し、運用すること。	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			グ研修を通じて開発者のセキュリティ意識を醸成し、関係者にセキュリティコーディング規範の厳格な遵守を求めます; - 要件分析: 業務内容、業務プロセス、技術フレームワークについて協議し、セキュリティを組み込む最適な方法を模索します; - システム設計: システム設計に対して脅威モデリングを行い、採用するアーキテクチャのセキュリティ技術評価を実施します; - システム開発: 開発プロセスにおいて、テンセントが独自に設計したセキュリティ開発コンポーネントを開発担当者に提供し、テンセントクラウドのセキュリティコーディングガイドラインに従ってコーディングを行う; - セキュリティ検証: コードのセキュリティチェック、資産のセキュリティスキャン、Web スキャン、手動によるセキュリティ評価、ペネトレーションテスト、コード監査などを通じて脆弱性を発見します。 - リリース: セキュリティ部門による最終チェックと確認を経て初めて、システムを本番環境にリリースします。これにより、セキュリティ上の脆弱性を抱えた製品が本番環境で稼働することを防止します。 さらに、Tencent Cloud は物理的および論理的な分離メカニズムにより、開発環境と本番環境を厳格に分離しており、非本番環境での非マスキング済み本番データの使用を禁止しています。
		【基本的な対応事項】 ① 不正侵入を防止するため、外部ネットワーク と内部ネットワーク の接続部分に適切な不正侵入防止策 を講ずること。また、外部ネ	お客様は、内部ネットワークと外部ネットワーク間のデータ交換に対して侵入防止措置を講じ、専用回線や暗号化技術などを通じてネットワークの安全性を確保する必要があります。また、ネットワークセグ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		ットワークと内部ネットワークとの間のデータ授受に対する不正侵入防止策を講ずること。 ② ネットワーク機器の設定 を定期的及びシステム環境の更新時に点検し、必要に応じて更新すること。ファイアウォールは必要な通信のみを許可する設定とすること。 ③ 情報の機密性や完全性等を保護する観点から、専用線や暗号技術の活用等を通じてネットワークのセキュリティを確保すること。 ④ 無線 LAN ネットワークへのアクセスは、適切な認証機能及びアクセス制御機能を実装し、不正利用を防止すること。 ⑤ テレワークやベンダーによる保守等においてリモートアクセスの対象とするシステムを制限し、適切に管理すること。また、重要なシステムについては、多要素認証や暗号化接続を使用すること。 【対応が望ましい事項】 a. DDoS/DoS 攻撃対策、DNS に係るサイバーセキュリティ対策、代替通信経路の制御などによって、組織の通信及びネットワークサービスの耐性度を強化すること。 b. 開発環境及びテスト環境を本番環境から分離するとともに、不正アクセスや情報資産の不正な変更を防止すること。 c. ネットワークセグメントを細分化し、マルウェアの水平移動（ラテラルムーブメント）を阻止することなどにより、サイバー攻撃の被害拡大防止を図ること。	メントを細分化し、DDoS/DoS 攻撃対策、DNS 関連のネットワークセキュリティ対策、予備通信経路の管理などを通じて、組織の通信およびネットワークサービスのレジリエンスを強化する必要があります。さらに、リモートワークやベンダーによるメンテナンスなど、リモートアクセスが必要なシステムについては、制限と管理を行う必要があります。 ネットワーク通信セキュリティの面では、 お客様が Tencent Cloud コンソール上で行う通信はすべて HTTPS セキュリティプロトコルによる暗号化保護を受けています。Tencent Cloud 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、ステータス監視などのセキュリティ機能を備えており、お客様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。また、お客様は以下の Tencent Cloud サービスを利用して、さまざまなシナリオにおけるデータの安全な転送を実現できます： • Direct Connect (DC)：専用性と高いセキュリティを備えた大帯域幅の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回線を独占するため、データ漏洩の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、ローカルデータセンターと Tencent Cloud 上のリソースを安全に接続します。VPN チャネルは IKE（鍵交換プロトコル）と IPsec を採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することで、転送中のデータセキュリティを保証します。 ネットワークのレジリエンスを確保するため、Tencent Cloud のデータセンターは

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			世界中の複数のリージョンに展開されており、各アベイラビリティ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ています。これにより、Tencent Cloud ネットワークのリージョン横断的な災害対策能力を構築し、通信事業者のパブリックネットワーク障害による継続的な影響を効果的に低減します。Tencent Cloud の基盤ネットワークは、冗長構成を採用しており、ルーティング階層における経路優先度とルーティング到達可能性に基づくトラフィックエンジニアリングのスケジューリングと組み合わせることで、単一の機器障害によってネットワークサービスが中断しないことを保証します。 また、テンセントクラウドは、お客様がネットワークセキュリティを効果的に管理できるよう、以下のサービスを提供しています： • <u>Virtual Private Cloud (VPC)</u>：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ます。仮想化技術を活用し、異なるプライベートネットワーク間の完全な論理的分離を実現することで、独立かつ隔離された安全なクラウドネットワークを顧客に提供します。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およびネットワーク ACL ルールを設定することで、インスタンスレベルおよびサブネットの入出力トラフィックを制御し、多層的なネットワークアクセス制御を実現します。 • <u>Cloud EdgeOne (EO)</u>：テンセントのグローバルエッジノードを基盤として、顧客にセキュリティ保護およびアクセラレーションサービスを提供します。DDoS 防御、インテリジェント Web 防御、ボット/クローラー攻撃防御、DNS

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			解決などの機能を備え、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。また、顧客は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、および Anti-DDoS などのネットワーク境界保護ツールを選択することも可能です。 Cloud Firewall (CFW) ファイアウォール ACL による能動的な制御、IPS によるリアルタイム遮断、仮想パッチ、悪意のあるコードの検出などの機能をサポートし、さまざまなネットワーク境界における保護を提供します。 Web Application Firewall (WAF) は、Web 攻撃、侵入、脆弱性悪用、マルウェア注入、改ざん、バックドア、クローラーなど、Web サイトおよび Web サービスのセキュリティ保護課題への対応を支援します。 Anti-DDoS 豊富で高品質な DDoS 防御リソースと、絶えず進化する「自社開発+AI による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 攻撃への対策を実現します。 Flow Logs (FL) は、ネットワークトラフィックのリアルタイムかつ非侵襲的なバイパス収集、保存、分析をサポートし、障害調査、アーキテクチャの最適化、セキュリティ検査、コンプライアンス監査などの課題を解決します。 お客様が規制当局の指針を順守できるよう、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および多層防御システムを確立しました。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の管理・制御および保護基準、ならびに対応する役割と責任を

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			明確化し、テンセントクラウドのネットワーク上で稼働する業務の安全な運用を確保しています。同時に、テンセントクラウド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区分し、異なるセキュリティドメインを物理的または論理的に分離することで、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および本番ネットワーク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 防御 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迅速に検知、フィルタリング、および阻止し、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ています。 ファイアウォールの使用および管理に関して では、テンセントクラウドのファイアウォールルールは、テンセントクラウドの生産ネットワークへのアクセスを制限するように設定されています。ファイアウォールルールへの管理アクセスは、セキュアシェル (SSH) プロトコルと二要素認証を使用する権限のある管理者に限定されており、ファイアウォールルールの変更は、展開前に関連する審査および承認プロセスを経ます。テンセントクラウドは定期的にファイアウォールルールの包括的な監査を実施し、ルールの使用状況を重点的に確認しています。 ネットワーク機器のセキュリティに関して では、テンセントクラウドはネットワークセキュリティ設定基準およびセキュリティベースライン基準を確立し、ネットワーク機器、ファイアウォール、ホストサーバーのオペレーティングシステム、データベ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ース、およびアプリケーションシステムのセキュリティ設定を標準化して管理しています。テンセントクラウドのセキュリティチームは、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のセキュリティポリシーやパラメータ設定を定期的にレビューし、その有効性を確保しています。また、テンセントクラウドは内部ネットワーク監視システムを導入し、ネットワーク機器の監視とアラート発信を行っており、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。 リモートアクセス管理に関しては、テンセントクラウドは社内従業員向けのリモートアクセス管理手順を確立しており、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にのみ使用を限定し、暗号化された通信チャネルを通じてテンセントクラウドの社内ネットワークおよび日常業務システムにリモートアクセスします。テンセントクラウドはリモートアクセスログを維持し、ユーザーの操作行動を記録します。同時に、テンセントクラウドの社内ネットワークと顧客データが存在する本番環境は完全に分離されています。テンセントクラウドの従業員が顧客の同意と権限を得て顧客情報資産にアクセスする場合、必ずバスタードマシン（堡垒機）を経由して顧客データが存在する本番環境にアクセスしなければならず、バックエンドの運用保守操作記録はすべてログプラットフォームに一元的に保存され、テンセントクラウドの内部監査チームが定期的に記録情報を監査します。
		【基本的な対応事項】 ① 利用するクラウドサービスの仕様を確認し、理解を深めること。 ② 責任共有モデル 36 を理解し、クラウド事業者との責任範囲等を	顧客は、利用するクラウドサービスの仕様および責任分担モデルを把握し、責任分担に基づき、サービス仕様の変更時にその影響を確認しなければならない。顧客は、クラウドサービスの各構成・設定の適切性を確保しなければならない。顧客は、関係

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		明確にすること。 ③ 情報公開等の設定にミスがないか確認すること。設定の妥当性の確認においては、必要に応じて、専門家によるシステム監査や誤設定の自動検知等の診断サービス等を利用すること。 ④ 責任分界に応じて、サービス仕様が変わる際には影響を確認すること。 ⑤ 多岐にわたる関係主体等を把握し、情報共有体制・インシデント対応体制を構築すること。 ⑥ クラウドサービスの利用終了時における、クラウドサービス上のデータの取扱いについて確認すること。	する関係者との間で情報共有およびインシデント対応体制を構築しなければならない。クラウドサービスの利用終了時には、顧客はクラウドサービス上のデータの取り扱い方法を確認しなければならない。 Tencent Cloud がお客様に提供するクラウドサービスは、各サービスで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。各サービスのパフォーマンス指標、測定基準、およびレポート要件は、各製品の SLA に明記されており、Tencent Cloud の公式ウェブサイトに掲載されています。Tencent Cloud は、クラウドサービスのパフォーマンスと可用性を継続的に追跡し、管理コンソールを通じてお客様にリアルタイムの監視機能を提供します。 責任分担の面において、テンセントクラウド はクラウドサービスの開放性と共有という特性を堅持し、クラウドプラットフォームおよび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業務およびデータのための、より優れた、より完備されたセキュリティ保証体制を構築します。Tencent Cloud はクラウドサービスプロバイダーとして、データセンターのインフラストラクチャおよびクラウドプラットフォームのセキュリティに責任を負います。お客様が異なるクラウドサービスカテゴリ（IaaS、PaaS、SaaS サービスなど）を選択する際、各コンポーネントに対する管理権限も異なることを考慮し、Tencent Cloud はクラウド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。詳細については、本ガイドをご参照ください。 ユーザーの設定チェックとリスク管理を支援するため、Cloud Security Center (CSC) は、クラウドサーバー、オブジェク

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			トストレージ、クラウドデータベース、ロードバランサーなど、多種多様なクラウド製品を対象とした、クラウド製品の設定リスクに対する自動チェック・評価機能を提供しています。これにより、クラウド製品の利用における誤ったセキュリティ設定に起因するセキュリティリスクを低減し、クラウド上のセキュリティレベル全体を向上させることを支援します。また、お客様は Config を通じて、クラウドリソースの集中監査とガバナンスを実現できます。これにより、お客様アカウント下の異なるリージョンにおける各種クラウドリソースの設定情報や変更履歴を継続的に記録し、Tencent Cloud のベストプラクティスに基づくルールやコンプライアンスパッケージテンプレートに基づき、企業アカウント下のクラウドリソース設定に対して継続的なコンプライアンス評価を自動的に実施し、非標準的なリソース設定を特定することで、クラウドリソースの自動監視と管理を実現します。 クラウドユーザーとのコミュニケーション に関しては、Tencent Cloud は、クラウドコンソール、電子メール、専用ホットラインなど、Tencent Cloud と外部顧客間のコミュニケーションを促進するための多様なチャネルを確立しています。Tencent Cloud コンソールはチケットサービスを提供しており、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。Tencent Cloud のチケットシステムは、段階的な対応メカニズムを通じて顧客のチケットに優先順位を割り当てます。第一線の技術チームが効果的に解決できない場合、システムは自動的にサービスエスカレーションプロセスをトリガーし、製品または技術チームが介入して共同で処理を行うことで、顧客の要望やフィードバ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ックが迅速に対応・処理されることを保証します。また、顧客は適切なサービスプランを選択することで、専用サポートグループ、専任のテクニカル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受けることができます。 変更通知に関しては、外部環境に影響を及ぼす可能性のある製品、インフラストラクチャ、およびネットワーク構成の変更リクエストについて、テンセントクラウドは公告、電子メール、テンセントクラウドコンソール、および / またはその他の適切なチャネルを通じて顧客に通知します。 インシデント対応および通知に関しては、Tencent Cloud は、情報セキュリティインシデントの連絡と警告管理手順を制定し、重大なセキュリティインシデントおよび重大な業務停止シナリオにおける警告・通知メカニズムを明確化しています。これにより、影響を受ける内部関係者、顧客などの関係者に対し、迅速に告知および警告を行い、すべての関係者が秩序立てて、タイムリーかつ効率的に連携・調整を行う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セキュリティインシデントについては、Tencent Cloud は、当該インシデントの影響範囲および程度に基づき、内部審査を経た上で、インシデントの処理および分析結果を適切な方法で顧客に通知し、損失を最小限に抑えるための是正措置を講じられるよう、相応の技術サポートを提供します。 クラウドサービスの終了および離脱に関して、お客様がビジネス変更または将来のIT 計画に基づき契約合意を終了する必要がある場合、いつでもクラウド上のデータおよび本番環境のバックアップおよび移行を行うことを選択できます。Tencent Cloud は、お客様が汎用的な標準フォーマットを使用してデータのバックアップま

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			たは移行を行うことをサポートしており、お客様はクラウド導入フェーズと同様の転送方法および転送プロトコル、Direct Connect (DC)、VPN Connection などのネットワークサービス製品を利用して、クラウド離脱フェーズにおけるデータの安全性と信頼性を確保できます。お客様のクラウドサービス終了後、Tencent Cloud は厳格なデータ消去方法に従い、保存期間満了後にコピーおよびバックアップを含むお客様のデータを完全に削除し、削除後のデータは復元できません。

6.4 サイバー攻撃の検知

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
2.4	サイバー攻撃の検知	【基本的な対応事項】 ① アノマリ (異常値)、IoC (侵害の痕跡) などのサイバー攻撃の端緒の検知のための監視・分析・報告に係る手続等を策定し、必要に応じて見直すこと。なお、利用するクラウドサービスがサイバー攻撃の端緒となるリスクを踏まえ、責任分界に応じて、監視の対象には、クラウドサービスも含めること。 ②サイバー攻撃に対するリスク低減を図るために、サイバー攻撃の脅威に応じて、必要な監視・分析などの対策を講ずること 2.4.1. 監視 【基本的な対応事項】サイバー攻撃の端緒を検知するために、以下について継続的な監視を実施すること: 1 ハードウェア・ソフトウェアについて。	顧客は、異常値や攻撃の痕跡 (IoC) などのサイバー攻撃の初期兆候に対する監視、分析、および報告手順を策定し、サイバー攻撃の脅威レベルに応じて、必要な監視、分析等の措置を講じなければならない。顧客は、クラウドサービスを監視範囲に含めなければならない。また、顧客は、異なる種類のサイバー攻撃に対応したインシデント対応計画および緊急復旧計画を策定し、定期的または必要に応じて見直しを行わなければならない。 お客様は、Cloud Log Service (CLS) をご利用いただけます。本サービスはワンストップのログサービスプラットフォームであり、ログの収集、保存から検索・分析、リアルタイム利用、配信に至るまで多岐にわたるサービスを提供し、業務運用、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、1 つまたは複数のログトピックに対してアラートポリシーを設定することをサポートしています。アラートポリシーは定期的に監視

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		② ネットワークについて。	タスクを実行し、クエリ分析結果がトリガー条件を満たした場合にアラート通知を送信するため、お客様は異常を迅速に発見できます。お客様はさらに、Cloud Security Center (CSC) を利用して、その資産センター、リスクセンター、アラートセンター、高度セキュリティ管理機能を通じて、事前の脅威検知、事中の対応・処置、事後の原因追跡分析から成るセキュリティ運用のクローズドループを実現することが可能です。クラウドセキュリティセンターは、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、クラウドリソース構成リスク、サービス公開の6大リスクを定期的に検出し、企業のセキュリティ状況を継続的に監視します。また、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一元的に取り込み、アラートログの監査、分析、集約、一元的な表示および追跡を行います。さらに、お客様は Elasticsearch Service (ES) サービスを利用し、クラウドサーバーやコンテナなどの他のクラウド製品のリアルタイムログ、あるいは業務の既存データおよび増分データを、Tencent Cloud ES クラスターに集約・転送し、データの分散型ストレージ、検索・分析を行うことができます。 ネットワークトラフィックの監視に関しては、Flow Logs (FL) を選択することで、ネットワークトラフィックのリアルタイムかつ非侵襲的なバイパス収集、保存、分析を行い、障害調査、アーキテクチャの最適化、セキュリティ検査、コンプライアンス監査などの課題を解決できます。 お客様の規制遵守を支援するため、テン
		③ 役職員によるシステムへのアクセスについて。	
		④ 外部のサービスプロバイダによるシステムへのアクセス（保守作業等）について監視をすること。	
		⑤ サイバー攻撃の端緒がインシデントに該当するかどうかを分析（影響範囲・重要度を含む）し、速やかにしかるべき責任者に報告すること。	
		⑥ サイバー攻撃の端緒を検知するためのアラート基準や閾値等の妥当性を定期的に検証すること。	
		⑦ データセンターやサーバ室への出入や不審な活動を監視すること。	
		【対応が望ましい事項】	
		a. おとりアカウントやサーバを用いて、攻撃の初期段階に検知するための仕組みを導入すること。	さらに、お客様は Elasticsearch Service (ES) サービスを利用し、クラウドサーバーやコンテナなどの他のクラウド製品のリアルタイムログ、あるいは業務の既存データおよび増分データを、Tencent Cloud ES クラスターに集約・転送し、データの分散型ストレージ、検索・分析を行うことができます。 ネットワークトラフィックの監視に関しては、Flow Logs (FL) を選択することで、ネットワークトラフィックのリアルタイムかつ非侵襲的なバイパス収集、保存、分析を行い、障害調査、アーキテクチャの最適化、セキュリティ検査、コンプライアンス監査などの課題を解決できます。 お客様の規制遵守を支援するため、テン
		b. 顧客サービスの提供内容を踏まえた常時監視（24 時間 365 日）を行うこと。	
		c. SIEM 等のツールを活用して、複数の監視情報（ソーシャルメディア、ダークウェブ等の外部情報を含む）を集約し、情報の相関関係を含めて、リアルタイムにサイバー攻撃の端緒がインシデントに該当するかどうかを分析すること。	

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。 パッチ管理に関しては、テンセントクラウドは最新のパッチを特定し、インストール前に十分なセキュリティテストを実施して、パッチの安全性を確保します。テンセントクラウドは定期的に各内部業務チームにパッチのアップグレードとインストールを通知し、エンドポイント検出ツールを使用してパッチのインストール状況を持定期的にスキャンします。また、期限を過ぎてもパッチがインストールされていないデバイスに対しては、自動的にアラートチケットを生成します。 物理的なセキュリティと監視に関しては、テンセントクラウドはデータセンター運営事業者に対し、データセンターに 24 時間 365 日死角のないビデオ監視アラートシステムを配備し、警備室が常駐して監視記録を十分な期間安全に保管することを義務付けています。また、テンセントクラウドは、オペレーターに対し、セキュリティ担当者が点検リストおよび点検計画に

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			厳格に従って各サーバルームおよび機器の状態を点検するよう求めています。各点検ポイントで署名と点検時刻を記録し、インフラの障害やセキュリティインシデントを発見した場合は、直ちにデータセンターの緊急インシデント対応プロセスを起動する必要があります。

6.5 サイバーインシデント対応及び復旧

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
2.5.1	インシデント対応計画及びコンティンジェンシープランの策定	【基本的な対応事項】 ④サイバー攻撃を想定したインシデント対応計画及びコンティンジェンシープラン（復旧計画まで含む）を、サイバー攻撃の種別ごとに策定すること。その中で対応の優先順位や目標復旧時間、目標復旧水準を定めておくこと。左記について、定期的あるいは必要に応じて見直しを実施すること。 【対応が望ましい事項】 a.コンティンジェンシープランにおいては、資金清算インフラや決済インフラ等におけるインシデントや、データセンターやクラウド等を含めたサードパーティが提供するサービス等が長期間利用できないようなインシデントなど、大規模な被害が生じるサイバーインシデントに対応するためのコンティンジェンシープランも整備すること。	顧客は、異なる種類のサイバー攻撃に対応するため、適切なインシデント対応計画および緊急復旧計画を策定し、対応の優先順位、目標復旧時間（RTO）および目標復旧ポイント（RPO）を明確にし、定期的または必要に応じて見直しを行うものとする。顧客が策定する緊急対応計画には、大規模なサイバーインシデントへの対応計画を含めるものとする。 インシデントへの対応および処理に関して、Tencent Cloud は社内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、処理のメカニズムおよび関連プロセスを確立するとともに、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ています。検知・特定されたセキュリティインシデントに対し、Tencent Cloud はインシデントの性質、データの機密性、影響範囲などの要因を総合的に考慮して分析・分類を行い、速やかに担当責任者に通知してインシデントの処理を進めます。 事業継続および緊急対応計画に関しては、テンセントクラウドは包括的な事業継続マネジメントシステムを構築し、ISO/IEC 22301 事業継続マネジメントシステムの国際規格認証を取得しています。テンセントクラウドは、クラウド製品およびサービスに対して事業影響度分析を実施し、各業

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			務の復旧時間目標（RTO）および復旧時点目標（RPO）を明確化しています。また、事業影響度分析の結果に基づき、異なる対応戦略と事業継続計画を策定し、クラウド製品および重要プロセスに対して詳細な災害復旧計画を策定しています。関連する戦略、計画、および対応案は、場所、人員、設備、システム、情報データなどの重要領域をカバーし、業務の優先順位に基づいて対応する災害復旧プロセスを策定し、災害対策システムの完全性、秩序性、実行可能性を確保します。 また、テンセントクラウドはサイバーセキュリティ緊急対応計画を策定しており、サイバー攻撃、マルウェア、データセキュリティ、設備・施設の故障、災害事象など、多岐にわたるサイバーセキュリティ緊急事態を網羅しています。確立された緊急対応計画体系を基盤とし、緊急対応チームの構築を支えとし、緊急対応プロセスの標準化を重点とすることで、監視・早期警戒、通報・対応などの業務能力をさらに強化し、サイバーセキュリティ事象がテンセントクラウドに及ぼす悪影響を予防・軽減しています。
2.5.2	インシデントへの対応及び復旧	インシデント対応計画及びコンティンジェンシープランにおいては、以下の事項を考慮すること： 2.5.2.1. 初動対応（検知・受付、トリアージ） 【基本的な対応事項】 ① 各種システムの監視や、顧客等からの問合せ、セキュリティ対応機関など外部組織からの連絡により、インシデントを検知すること。 ② 検知・受付時に収集した情報を基に、事実関係を確認のうえ、インシデント対応の要否を判断すること。 ③ インシデントは、業務影響等に	顧客は、様々な手段を通じてセキュリティインシデントを検知・検証し、インシデント対応を開始すべきかどうかを判断しなければならない。対応が必要なインシデントについては、顧客はログ等の証拠、およびインシデント対応の各段階に関する記録を保存しなければならない。インシデント発生時には、顧客は法令やインシデントの実際の影響等に基づき、監督機関等の関係者に速やかに報告し、適切な場合にはインシデントを適切に公表しなければならない。顧客は、サイバー攻撃による被害の拡大を防ぐための抑制措置を講じ、被害の原因を排除しなければならない。また、顧客は復旧手順に従って復旧を行い、復旧後のシステムおよび業務の状態を確認するとともに、復旧後に当該インシデントの発

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		応じた優先順位付けを行い、あらかじめ定められた基準に従い、インシデント対応組織の管理者や、サイバーセキュリティを統括管理する責任者（CISO 等）、経営陣に報告すること。 2.5.2.2. 分析 【基本的な対応事項】 ① 対応が必要と判断したインシデントについて、攻撃の手口や原因・経路、システムへの影響、現在発生している業務影響及び今後発生しうる業務影響等について分析すること。特に、分析を行う際は事前にログ等の証拠を保全し、分析は保全したログ等に対して行うこと。 ② インシデントの検知・受付から復旧までのフェーズに関し、記録。 2.5.2.3. 顧客対応、組織内外の連携、広報 【基本的な対応事項】 ① インシデント対応計画やコンティンジェンシープランに基づき、サイバーセキュリティを統括管理する CISO 等の責任者や担当者、各コンティンジェンシープランの関係者が、それぞれの役割、必要な連絡先、必要な対応手順について習熟すること。 ② 情報漏えい等により顧客に二次被害などの影響がある場合は、影響範囲や注意事項、対応方法等を当該顧客に伝達すること。 ③ インシデント発生時は、法令等に従い、規制当局等に速やかに報告をすること。 ④ 法令等に基づき、公表が必要な	生原因を分析・評価し、必要に応じてインシデント対応計画や緊急時対応計画などの関連するネットワークセキュリティ管理メカニズムを改善する必要があります。 お客様のインシデント検知および迅速な対応を支援するため、Tencent Cloud はワ ンストップセキュリティ管理プラットフォーム および Cloud Security Center (CSC) を提供しています。これらプラットフォームの資産管理センター、リスク管理センター、アラートセンター、高度なセキュリティ管理などの機能を通じて、事前の脅威検知、事中の対応・処置、事後の原因追跡分析というセキュリティ運用の閉ループを実現し、セキュリティ運用の効率を向上させます。 サイバーセキュリティインシデント発生後、お客様が重要な機能を迅速に復旧できるように、Tencent Cloud が提供する多くの製品は高可用性を備えており、システムやサービスの高可用性を実現します。例えば： • Cloud Load Balancer (CLB) は、安全かつ高速なレイヤー4/7 トラフィック分散サービスを提供し、トラフィック分散を通じてアプリケーションシステムの対外サービス能力を拡張し、単一障害点を排除します。CLB はクラスタ化された展開を採用しており、障害発生時のインスタンスを速やかに排除することで、高可用性を実現します。 • Cloud Virtual Machine (CVM) は、サービスの高可用性およびデータの高信頼性という特長を備えています。CVM に搭載されたクラウドディスクは

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		場合や、二次被害防止、顧客保護等の観点から公表が適切な場合は、サイバー攻撃による被害、対応状況、復旧見込み等の判明している事実について、顧客や自組織等のセキュリティ上のリスクを配慮した上で、適切かつ速やかに公表すること。 ⑤ 攻撃者の TTP (Tactics (戦術)、Techniques (技術)、Procedures (手順)) 等、他機関にとっても有効となる攻撃技術情報について、機密情報を除いた上で、必要に応じ、金融 ISAC や JPCERT/CC 等の情報共有機関に共有すること。	3 レプリカのストレージ戦略を採用しており、いずれかのレプリカに障害が発生した場合でも、データの迅速な移行と復旧を保証します。 • Tencent Kubernetes Engine (TKE) は、分散型サービスアーキテクチャを採用しており、サービスの障害に対する自動復旧と迅速な移行を保証します。ステートフルサービスのバックエンドである分散型ストレージと組み合わせることで、サービスとデータの安全性および高可用性を実現します。
		2.5.2.4. 封じ込め 【基本的な対応事項】 ① サイバー攻撃の被害拡大を防ぐための封じ込め措置を講じること 【対応が望ましい事項】 a. 封じ込めの際には、対応によって影響が生じる可能性のあるサードパーティに適切に通知を行うこと。	インシデント関連の証拠の収集、集約、および分析を支援するため、Tencent Cloud は 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 はログの収集、保存から検索・分析、リアルタイム処理、配信に至るまで多岐にわたるサービスを提供し、業務運用、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。さらに、の Elasticsearch Service (ES) サービスは、クラウドサーバーやコンテナなどの他のクラウド製品からのリアルタイムログ、あるいは業務の既存データや増分データを、Tencent Cloud の ES クラスターに集約・転送し、データの分散型ストレージ、クエリ分析を行います。
		2.5.2.5. 根絶 【基本的な対応事項】 ① サイバー攻撃により被害が発生した原因を除去すること（マルウェアの駆除、パッチの適用等による脆弱性の修正等）。	バックアップに関しては、Tencent Cloud が提供する各種ストレージサービスおよびデータベースサービスはいずれもバックアップ機能を備えており、お客様のあらゆるバックアップニーズに対応します。お客様がクラウドに保存したデータについては、Tencent Cloud はデータのリアルタイムホットバックアップ、冗長ストレージ、遠隔地バックアップなどの方式を採用
		2.5.2.6. 復旧 【基本的な対応事項】 ① 復旧計画において、復旧完了し業務再開を判断する際には、判断権限者を明確にしておくとともに、判断要素を整理しておくこと。 ② 復旧作業においては、被害を受けた機器の初期化、システム再構	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		築等を行い、システムを通常の運用状態に戻して正常稼働を確認すること。 ③ バックアップからの復旧の際には、攻撃の手法に応じて、既にバックアップデータ等が改ざんされている可能性や、マルウェア等に感染している可能性に留意すること。 ④ 被害を受けたシステムと他システムを再接続する前に、システムの正常な稼働や接続がなされていることを確認すること。 ⑤ 復旧作業に際しては、重要な業務が適切な手順で復旧され、通常どおりの業務が稼働していることをシステム責任者と共に確認するなど、復旧が適切に行われたことを確認すること。 ⑥ インシデントからの復旧後、当該インシデントの発生原因や被害の拡大に関する原因等を分析し、対応の評価を行うこと。また、当該評価を基に、インシデント対応計画やコンティンジェンシープランを含むサイバーセキュリティ管理態勢の見直しや改善を行うこと。	し、クラウドに保存された業務データの安全性、信頼性、および継続的な可用性を確保しています。Tencent Cloud はさらに、物理的セキュリティ、アクセス制御、論理的分離など、多岐にわたる保護措置を実施しており、<u>お客様が Key Management Service (KMS)、および Cloud Access Management (CAM)</u> を利用することをサポートし、お客様のバックアップデータが不正アクセスや改ざんを受けるのを防止しています。バックアップに関する詳細については、本ガイドの第 5.2.3 章「実 39 データファイル管理」の項目をご参照ください。 インフラの復旧能力に関しては、Tencent Cloud のデータセンターは世界中の複数のリージョンに展開されており、そのうち 3 つのデータセンターは香港内に設置され、お客様が選択・展開できるようになっています。各アベイラビリティ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ており、Tencent Cloud ネットワークのリージョン間災害対策能力を構築することで、通信事業者のパブリックネットワーク障害による継続的な影響を効果的に低減しています。Tencent Cloud の各データセンターの電力システムおよび空調システムは、いずれも高安定性の完全冗長システムを採用しており、単一障害点によるデータセンターの電力および冷却供給の継続性への影響を回避しています。Tencent Cloud の基盤ネットワークおよびコンピューティングノードは、いずれも N×N の冗長構成を採用しており、ネットワークサービスおよび顧客ビジネスの有効性を確保し、単一障害点による中断が発生しないようにしています。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			顧客の規制遵守を支援するため、インシデントへの対応および処置に関して、テンセントクラウドは情報セキュリティインシデント管理規範を策定し、情報セキュリティ報告、対応、処理のメカニズムおよび関連プロセスを確立するとともに、インシデント処理プロセスにおける各チームの役割と具体的な職責を明確化しています。 テンセントクラウドは、内部の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ています。検知・特定されたセキュリティインシデントに対し、テンセントクラウドはインシデントの性質、データの機密性、影響範囲などの要因を総合的に考慮して分析・分類を行い、速やかに担当責任者に通知してインシデントの対応を進めます。インシデント対応プロセスの有効性と迅速性を確保するため、テンセントクラウドの内部業務部門は定期的にセキュリティインシデント緊急対応計画に関する演習を実施しています。また、セキュリティ技術の発展や情勢に基づき、セキュリティチームの従業員に対して技術トレーニングを行い、最新のセキュリティ規定や運用プロセスを理解・遵守させるとともに、最新の情報セキュリティ基準やベストプラクティスを習得させるよう努めています。 お客様がコミュニケーションおよび通知義務を効果的に履行できるよう支援するため、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、インシデントのエスカレーション、インシデント通知などの関連手順を確立しています。これにより、インシデントの影響を受ける可能性のある、または既に影響を受けている社内関係者やお客様などの関係者に、速やかに警告や通知を行い、各関係者が秩序正しく、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ます。

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			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、その影響範囲と程度に基づき、内部審査を経た上で、インシデントの処理および分析結果を適切な方法で顧客に通知します。また、顧客が是正措置を講じ、損失を最小限に抑えられるよう、相応の技術サポートを提供します。 インシデント管理および証拠収集に関し ては、テンセントクラウドは社内セキュリティインシデントの証拠収集に関する基準を明確に定めています。情報セキュリティインシデントの受付、調査・評価、処理、追跡の過程において、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に関する記録を維持し、その完全性と機密性を確保します。テンセントクラウドは、お客様のニーズに基づき、合理性と実現可能性を評価した上で、お客様のデジタルフォレンジックおよび事後のセキュリティインシデント調査・分析に対して効果的な支援を提供します。 また、テンセントクラウドはログ収集・管理の規範および仕組みを確立し、ログインログ、操作ログ、システムの通常ログ、システムセキュリティインシデントログなどの記録、抽出、保存、保護、分析、監査などを管理・統制しています。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・管理され、関連するログ情報に対してはバックアップおよび厳格な保護措置が講じられます。 インシデントの総括と継続的改善に関し て、テンセントクラウドは定期的なインシデント分析メカニズムを確立しており、インシデントを多角的に分析（インシデントの種類、発生頻度、影響範囲、深刻度）し、事後検証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。重大なセキュリティインシデ

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
			ントについては、テンセントクラウドは専任チームを編成し、特別分析レポートを作成して経営陣に報告します。

6.6 サードパーティリスク管理

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		【基本的な対応事項】	
		①サイバーセキュリティに係る戦略、取組計画を策定する際にはサプライチェーン全体を考慮すること。また、サードパーティを含む業務プロセス全体を対象としたサイバーセキュリティ管理態勢を整備すること。	顧客は、サプライチェーンのセキュリティを自社のサイバーセキュリティ戦略、計画および関連メカニズムに組み込み、サードパーティのサイバーセキュリティリスク管理システムおよび組織体制を構築し、サードパーティを特定して管理台帳を維持するとともに、サードパーティとの取引終了時の管理プロセスを確立しなければならない。サードパーティと取引を行う場合、顧客は事前に設定した基準に基づいてデューデリジェンスを実施し、サードパーティとの契約またはサービスレベル契約 (SLA) において、双方の責任分担等の内容を明確にしなければならない。顧客は、第三者に対するリスク評価を実施し、第三者およびその製品・サービスがもたらすサイバーセキュリティリスク、契約履行状況、ならびに第三者自身のサプライチェーンリスク管理状況を継続的に監視しなければならない。重要なアウトソーシング業務については、顧客は撤退戦略または代替案を策定すべきである。
2.6	サードパーティリスク管理	② サードパーティのリスク管理のライフサイクル全体を通じ、サードパーティに起因するサイバーセキュリティリスクを管理するために必要な態勢を整備し、サードパーティリスク管理の方針を策定すること。	クラウドサービスプロバイダーとして、Tencent Cloud は国際版公式サイトにおいてオンライン版の Terms of Service 、
		③ サードパーティリスクを管理するための組織体制の整備（一元的に管理する統括部署の設置や、関係部署間の連携を含めた各部署の役割及び責任の明確化）、組織内規程の策定を行うこと。	Service Level Agreement (SLA) 、『データ処理およびセキュリティ契約』などの法的文書を提供しており、Tencent Cloud が提供するサービスの内容およびサービスレベル、ユーザーデータおよび知的財産権の保護、お客様と Tencent
		④ サードパーティを特定し、サードパーティやサードパーティが提供する商品・サービスの自組織業務における位置づけ・役割・重要度、重要な情報（個人情報や営業機密等）の取扱いの有無、組織内システムへの接続状況（インターネット接続等の外部からのアクセスの容易さ）などをふまえ、サードパーティのリスク評価を行い、そのリスクに応じた対応をす	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		ること。	Cloud の双方のセキュリティ責任と義務、サービス期間と契約終了シナリオ、紛争解決メカニズム、通知メカニズムなどについて明確に規定しています。お客様はさらに、Tencent Cloud とオフラインでの契約締結を選択し、契約中の条項および細則を協議することも可能です。
		⑤ サードパーティを管理するための台帳等を整備し、維持すること。	下請け処理のシナリオについては、上記の契約書に、下請けの事前の同意、下請け業者の追加または変更前の通知、データ保護義務などの条項が含まれています。顧客の事前の同意がない限り、テンセントクラウドは、契約に基づき顧客に代わって実行するいかなる処理業務も下請けに出しません。下請け処理業者の追加または変更に関するいかなる予定変更についても、テンセントクラウドは電子メールなどの手段を通じて顧客に通知します。
		⑥ サイバーインシデント対応計画やコンティンジェンシープランにおいては、インシデント対応等を行うサードパーティを含めた態勢を整備すること。	下請業者の管理に関しては、テンセントクラウドは完備されたサプライチェーンセキュリティ管理体制を構築しており、厳格なサプライヤーのセキュリティ評価および参入審査、定期的な監視・評価、明確なアウトソーシングサービス契約などの措置を通じて、サプライヤーを効果的に管理し、下請けがテンセントクラウドの顧客へのサービス提供能力、顧客情報処理プロセスの機密性および完全性、ならびに金融機関の監督および監査権限に影響を与えないことを確保します。
		⑦ サードパーティとの取引開始に当たっては、事前に定めた基準に基づき、デューデリジェンスを行うこと。	お客様のアウトソーシング評価、監視、および管理要件に対応するため、Tencent Cloud はお客様からの要請に応じて関連情報を提供し、専任担当者を配置して、お客様の評価、監査、および調査活動に積極的に対応・協力します。さらに、Tencent Cloud は毎年、独立した第三者による専門的な監査を受けており、証明的な性質を持つシステムおよび組織統制報告書を提供することで、クラウドユーザー機関、独立監査人、規制当局、会社
		⑧ サードパーティが遵守すべきサイバーセキュリティ要件を明確化の上、重要度に応じ、サードパーティ等との契約や SLA（サービスレベルアグリーメント）等において、例えば、以下の項目を明記すること。	
		⑨ サードパーティ及びその製品・サービスによってもたらされるサイバーセキュリティリスク並びに契約の履行状況等について、リスクの重大性に応じて、継続的にモニタリングすること。	
		⑩ サードパーティとの取引終了時の管理プロセス（データ廃棄、組織内システムへのアクセス遮断措置など）を整備すること。	
		【対応が望ましい事項】	
		a. サードパーティリスク管理に係る統括部署に適切な知識等を有する人員の配置をすること。	
		b. サードパーティリスク管理において、重要な業務のサードパーティへの依存関係、サードパーティの集中リスク、地政学リスクの影響、フォースパーティの影響を	

番号	制御領域	具体的な制御要件	Tencent Cloud の応答
		考慮すること。	の株主、およびその他の利害関係者に、Tencent Cloud の最新のサービス組織内部統制状況を公開しています。
		c. 重要なサードパーティがそのサードパーティ（2以上のサードパーティ（自組織から見たフォースパーティ、フィフスパーティ及びN番目のパーティ）を含む）を管理する能力及びそのサプライチェーンリスク、集中リスク等について、定期的にモニタリングすること。	お客様が業務の変更や将来のIT計画により契約を終了する必要性が生じた場合、いつでもクラウド上のデータおよび本番環境のバックアップおよび移行を行うことができます。Tencent Cloud は、お客様が一般的な標準フォーマットを使用して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いるため、お客様はクラウド移行時と同じ転送方式や転送プロトコルを採用するか、または Direct Connect (DC)、VPN 接続 (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、クラウドからの移行段階においてもデータの安全性と信頼性を確保できます。お客様のサービス終了後、Tencent Cloud はお客様とのサービス契約に基づき、厳格なデータ消去手順に従い、保存期間満了後に複製やバックアップを含むお客様データを完全に削除します。削除されたデータは復元できません。
		d. 重要なサードパーティの事業撤退や業務停止、契約関係の終了に備えて、適切なコンティンジェンシープランと出口戦略を事前に策定し、定期的に代替手段のテスト等を行うこと。	アウトソーシングに関する詳細については、本ガイドの第 5.1.2 章「外部管理」をご参照ください。

07

Tencent Cloud による「資金決済に関する法律」の遵守について

支払及び決済サービスの適正な実施を確保し、利用者を保護し、当該サービスの提供を促進するとともに、支払及び決済システムの安全性及び利便性の向上を図るため、日本の金融庁（Financial Services Agency, FSA）は「[資金決済に関する法律](#)」（Payment Services Act）を策定・公表しました。本法案は、プリペイド型支払手段の発行、預金取扱機関以外の者による資金移動取引、電子支払手段取引、暗号資産取引、資金移動取引の分析及び預金取扱機関間の資金移動取引の決済等に関して、規定及び要件を設けています。情報セキュリティに関しては、本法案はプリペイド型支払手段の発行者、暗号資産交換業者等に対し、業務関連情報を管理するために必要な措置を講じ、当該情報の漏えい、紛失又は毀損を防止することを求めています。

クラウドサービスプロバイダーとして、Tencent Cloud は事業運営が行われている法域の法令を厳格に遵守し、お客様に対して安全で安定的、継続的かつ信頼性の高いクラウドサービスを提供することに努めています。Tencent Cloud は、「資金決済に関する法律」（Payment Services Act）に基づき、コントロール状況の評価および改善を実施しました。情報管理および保護の観点において、お客様のデータはTencent Cloud 内部において高セキュリティレベルのデータとして位置付けられ、お客様は当該データの内容に対して唯一の所有権および管理権を有しています。お客様情報の安全性を確保するため、Tencent Cloud はデータセキュリティに関する管理手順を整備し、データ保護原則を明確化しており、アクセス制御、物理インフラのセキュリティ保護、ネットワーク防御、データ暗号化、データバックアップ、データ漏洩防止等多面的な保護措置を講じています。また、Tencent Cloud はお客様のデータの機密性、完全性及び可用性を保護するため、データ暗号化やバックアップ機能を備えたストレージおよびデータベース製品、通信及びネットワーク防御関連製品など、複数のクラウド製品・サービスを提供しています。Tencent Cloud の情報セキュリティ対策および関連クラウド製品・サービスに関する詳細は、本ガイドの[第5章](#)および[第6章](#)をご参照ください。

さらに、Tencent Cloud は第三者独立監査または評価を通じて、ISO/IEC 27001、ISO/IEC 27017、ISO/IEC 27018、ISO 22301、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に関する認証・資格を取得しており、Tencent Cloud のセキュリティ管理およびプライバシー保護の仕組みが、関連する認証基準または業界の良好な実践に適合していることを示しています。特に日

本地域においては、Tencent Cloud は『金融業界情報システムセンター（FISC）金融機関等コンピュータシステムの安全対策基準』に基づき、コントロール状況の評価を実施し、その結果に基づき、Tencent Cloud プラットフォームの安全性、可用性及び機密性に関するコントロールポイントを含むシステム及び組織管理（SOC）報告書を作成しています。Tencent Cloud のコンプライアンスに関する詳細は、本ガイド第2章「Tencent Cloud のセキュリティおよびプライバシーコンプライアンス」をご参照ください。

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、日本の金融庁（Financial Services Agency, FSA）および金融業界情報システムセンター（The Center for Financial Industry Information Systems, FISC）の重要な規制要求に基づいて作成されています。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