システムおよび組織統制(SOC) 3 報告書
アリババクラウド
クラウドサービスシステムの
セキュリティ、可用性、機密性に係る報告書
期間: 2018 年 11 月 1 日～2019 年 12 月 31 日

(注)　日本語訳文のご利用にあたって
日本語訳文は英語版を基にした翻訳であり、参考資料としてご提供するものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。

pwc

独立受託会社監査人の報告書

アリババクラウドコンピューティング社代表取締役殿:

適用範囲

当監査法人は、「クラウドサービスシステムに関するアリババクラウドの経営陣の主張」(以下「経営陣の主張」)と題する添付書類の主張について検証を行った。この主張は、「TSP セクション 100、*セキュリティ、可用性、処理の整合性、機密保持およびプライバシーに関する Trust サービス規準の 2017 年版*」(米国公認会計士協会(AICPA)、*Trust サービス規準*)に規定されたセキュリティ、可用性、機密保持に関する Trust サービス規準(適用される Trust サービス規準)に基づいて、アリババクラウドのサービスコミットメントおよびシステム要求事項が達成されたという合理的な保証を提供するために、アリババクラウドのクラウドサービスシステム(以下「システム」)内の統制が 2018 年 11 月 1 日から 2019 年 12 月 31 日にわたり有効であったとするものである。

受託会社の責任

アリババクラウドは、アリババクラウドのサービスコミットメントとシステム要求事項が達成されたことを合理的に保証するため、自社のサービスコミットメントおよびシステム要求事項、並びにシステム内の有効な統制の設計、導入、運用について責任を負う。アリババクラウドはまた、システム内の統制の有効性に関する添付の主張も提供している。主張の作成にあたり、アリババクラウドは、その主張において適用される Trust サービス基準を選択および特定する責任、並びにシステム内の統制の有効性評価を実施してその主張に関する合理的な基準を設ける責任を負う。

受託会社監査人の責任

当監査法人の責任は、システム内の統制が当該期間にわたり有効であり、適用される Trust サービス基準に基づいて受託会社のサービスコミットメントおよびシステム要求事項が達成されたことを合理的に保証するという経営陣の主張について、調査に基づく所見を述べることである。当監査法人の検証は、米国公認会計士協会によって定められた構成証明基準に従って実施した。これらの基準により、経営陣の主張があらゆる重要点で公正に述べられているかどうかに関する合理的な保証を得るために、当監査法人には調査を計画および実施することが義務付けられている。当監査法人が得た証拠は、当監査法人の所見の合理的根拠として十分かつ適切であると当監査法人は考えている。

当監査法人の調査には、以下の内容が含まれる。

- 当該システム、並びに受託会社のサービスコミットメントとシステム要求事項を理解する
- 統制が有効でなく、適用される Trust サービス基準に基づいてアリババクラウドのサービスコミットメントとシステム要求事項が達成されなかった場合のリスクを評価する
- システム内の統制が有効で、適用される Trust サービス基準に基づいてアリババクラウドのサービスコミットメントとシステム要求事項が達成されたかどうかに関する証拠獲得手続を実施する

当監査法人の調査には、状況に応じて当監査法人が必要と考えるその他の手続の実施も含まれる。

固有の限界

内部統制のシステムの有効性については、固有の限界がある(人的ミスの可能性や統制の回避など)。

統制はその性質上、適用される Trust サービス基準に基づいて受託会社のサービスコミットメントとシステム要求事項が達成されたことを合理的に保証できるだけの有効な動作をしない場合がある。また、統制の有効性に関する結論の将来的予測は、状況の変化によって統制が適切でなくなる可能性がある、あるいは方針や手続の準拠レベルが低下する可能性があるといったリスクに影響される。

結論

当監査法人の結論では、アリババクラウドのクラウドサービスシステム内の統制は 2018 年 11 月 1 日から 2019 年 12 月 31 日の期間全体にわたり有効であり、適用される Trust サービス規準に基づいてアリババクラウドのサービスコミットメントとシステム要求事項が達成されたことを合理的に保証するという経営陣の主張は、あらゆる重要点において公正に述べられている。

PricewaterhouseCoopers

中国香港

2020 年 2 月 14 日

2018 年 11 月 1 日から 2019 年 12 月 31 日までの期間のクラウドサービスシステムに関する
アリババクラウドの経営陣の主張

当社は、アリババクラウドコンピューティング社およびその関連会社(Alibaba Cloud (Singapore) Private Limited、Alibaba.com (Europe) Limited、Alibaba Cloud US LLC、Alibaba Cloud (India) LLP、Alibaba Cloud (Malaysia) Sdn.Bhd.を含むがこれらに限定されない。アリババクラウドコンピューティング社およびその関連会社を「受託会社」または「アリババクラウド」と総称する)のセキュリティ、可用性、機密保持に関するサービスコミットメントおよびシステム要求事項が達成されたという合理的な保証を提供するため、2018 年 11 月 1 日から 2019 年 12 月 31 日の期間にわたり、アリババクラウドのクラウドサービスシステム(以下「システム」)に対して有効な統制を設計、導入、運用、維持管理する責任を負う。添付のシステム記述書には、当社の主張の対象となるシステム部分が明記されている。

当社は、「TSP セクション 100、*セキュリティ、可用性、処理の整合性、機密保持、プライバシーに関する Trust サービス基準 2017 年版*」(米国公認会計士協会(AICPA)、*Trust サービス基準*)に定められた、セキュリティ、可用性、機密保持に関する Trust サービス基準(適用される Trust サービス基準)に基づいて、アリババクラウドのサービスコミットメントとシステム要求事項が達成されたという合理的な保証を提供するため、2018 年 11 月 1 日から 2019 年 12 月 31 日の期間全体にわたるシステム内の統制の有効性評価を実施した。Trust サービス基準の適用に関するアリババクラウドのシステム目標は、適用される Trust サービス基準に関するサービスコミットメントとシステム要求事項に具体的に示されている。以下に、適用される Trust サービス基準に関する主要なサービスコミットメントとシステム要求事項を示す。

- アリババクラウドのコミットメントとシステム要求事項を満たすため、不正なアクセス、使用、改変からシステムを保護する
- コミットまたは合意されたとおり、機密指定された情報がシステムによって保護される
- コミットまたは合意されたとおり、システムを操作および使用できる

内部統制のシステムには、固有の制限事項(人的ミスの可能性や統制の回避など)がある。このような固有の制限事項があるため、サービスコミットメントおよびシステム要求事項が達成されていることの保証は、合理的ではあるが必ずしも絶対的とは言えない。

当社は、システム内の統制が 2018 年 11 月 1 日から 2019 年 12 月 31 日の期間全体にわたり有効であり、適用される Trust サービス規準に基づいてアリババクラウドのサービスコミットメントおよびシステム要求事項が達成されたことを合理的に保証すると主張する。

アリババクラウドコンピューティング社

2020 年 2 月 14 日

2018 年 11 月 1 日から 2019 年 12 月 31 日までの期間のクラウドサービスシステムに関する
アリババクラウドの記述書

I. 概要

事業内容

アリババグループ (NYSE:BABA) (以下「アリババ」または「グループ」)の事業部門であるアリババクラウドは、世界中の顧客、パートナー、アリババクラウド自身の e コマースエコシステムに対してグローバルクラウドコンピューティングサービスの包括的なスイートを提供している。アリババクラウドが提供するクラウドサービスは、自社開発のクラウドサービスプラットフォームおよびテクノロジーを使用している。アリババクラウドは、技術革新への多大な投資を通じてコンピューティング能力およびサービスの規模の経済を継続的に改善することで、クラウドコンピューティングを最先端のコンピューティングインフラストラクチャへと変えることを目指している。クラウドサービスは、金融、政府、ゲーム、電子商取引、モバイルサービス、医療サービス、マルチメディアといった、さまざまな業界で使用されている。アリババクラウドはクラウドサービス以外に、インテリジェントな生活、インテリジェントな都市、インテリジェントな製造、インテリジェントな農業を含む広範な分野向けにモノのインターネット(IoT)プラットフォームを提供している。アリババクラウドは、IoT インフラストラクチャの構築に全力で取り組んでいる。IoT プラットフォームのデータ保管および処理に API やその他のアリババクラウドサービスが統合され、包括的なサービススイートを利用できるようになることは、アリババクラウドの IoT プラットフォームのユーザーにとって非常に重要である。このプラットフォームには、迅速なデータの収集、保管、アプリケーション開発に役立つルールエンジンが搭載されている。アリババクラウドは、クラウドおよびデバイス端末の業界全体の統合開発プラットフォームの構築、IoT の全産業チェーンの形成、全世界的な IoT 規格策定への取り組みを通して、IoT のエコシステム、プラットフォーム、およびインフラストラクチャを引き続き構築し、現実世界とデジタル世界の統合を促進し、IoT から IoI (インテリジェンスのインターネット)への発展を進めることを目指している。

本報告書の対象のクラウドサービス

アリババクラウドは、パブリックかつオープンでセキュアなクラウドコンピューティングサービスプラットフォームの構築に取り組んでいる。本報告書の対象となったサービスは以下の通りである。

1. Elastic Compute Service (ECS)
2. Container Service for Kubernetes
3. Container Registry
4. Object Storage Service (OSS)
5. Alibaba Cloud Content Delivery Network (CDN)
6. Network Attached Storage (NAS)
7. Virtual Private Cloud (VPC)
8. Express Connect
9. NAT Gateway
10. Server Load Balancer (SLB)
11. Elastic IP
12. VPN Gateway
13. ApsaraDB RDS for MySQL
14. ApsaraDB RDS for SQL Server
15. ApsaraDB RDS for PostgreSQL
16. ApsaraDB RDS for PPAS
17. ApsaraDB for POLARDB
18. Anti-DDoS Basic
19. Anti-DDoS Pro
20. Anti-DDoS Premium
21. Web Application Firewall (WAF)
22. Security Center

23. Resource Access Management (RAM)
24. Key Management Service (KMS)
25. ActionTrail
26. MaxCompute
27. Log service
28. IoT Platform

本報告書の対象のデータセンターロケーション

アリババクラウドは、相互につながり合う世界を実現するため、安定した信頼できるコンピューティングおよびデータ処理能力の提供に全力で取り組んでいる。アリババクラウドは世界各地の 20 リージョンで 61 のアベイラビリティゾーンを運営している。

本報告書が対象とするロケーションには、中国(青島、北京、張家口、フフホト、杭州、上海、深圳、成都)、中国(香港)、シンガポール(シンガポール)、インド(ムンバイ)、インドネシア(ジャカルタ)、ドイツ(フランクフルト)、日本(東京)、オーストラリア(シドニー)、英国(ロンドン)、米国(シリコンバレー、バージニア)、マレーシア(クアラルンプール)、アラブ首長国連邦(ドバイ)のリージョンにあるデータセンターが含まれる。

再受託会社に割当または外部委託されたデータセンターおよび機能

アリババクラウドは、データセンターの暖房換気空調(HVAC)提供に再受託会社(以下「再受託会社」)を使用する。アリババクラウドは、消火器や CCTV (有線テレビ)などのアクセス制御および環境保全の導入によって構内を安全に保つためにこれら再受託会社を必要とする。さらに、アリババクラウドは、すべての再受託会社が情報セキュリティとビジネス継続性について特定の要求事項に従うよう要求する。

アリババクラウドは、これら再受託会社の能力および履行をレビューする責任を負う。アリババクラウドと再受託会社の間で、両当事者の責任と義務を定め、サービスの範囲とデータセンターのサービス可用性レベルを規定する契約書が署名されている。高いサービス品質を維持するため、アリババクラウドは、再受託会社が毎月提出するサービスレベルアグリーメント(以下、「SLA」)レポートに基づいて履行レビューを実施する。これら再受託会社は、毎月、主要なインシデント、指標、メンテナンスの概要を含む SLA レポートを提出するものとする。再受託会社がアリババクラウドの全要求事項を適切に満たしていることを確認するため、アリババクラウドは、データセンタープロバイダーのサービスレベルの評価を実施し、四半期毎に評価レポートを発行する。

適用される Trust サービス規準に基づいてアリババクラウドのサービスコミットメントおよびシステム要求事項を達成するには、アリババクラウドの統制に加えて、適切に設計され、効果的に運用される再受託会社の相補的な統制が必要である。本報告書の使用者は、受託会社監査人による調査の範囲に再受託会社の実際の統制は含まれないことを認知する必要がある。

II. 主要なサービスコミットメントとシステム要求事項

アリババクラウドは顧客が自社のシステムおよびデータのセキュリティ、機密性、可用性を確保できるようにするために、一貫性、信頼性、セキュリティを備え、法令を遵守したクラウドコンピューティングサービスの提供に取り組む。アリババクラウドは、アリババクラウドのサービスコミットメントとシステム要求事項が達成されたことを合理的に保証するため、システムおよびサービスに対する有効な統制の設計、導入、運用について責任を負う。アリババクラウドの顧客(委託会社)に対するサービスコミットメントは、オンラインの製品サービスレベルアグリーメント(以下「製品 SLA」)、Membership Agreement、プライバシーポリシー、アリババクラウドのサービス製品のオンライン記述書、契約書の形式で伝達される。製品 SLA、Membership Agreement、その他の法的文書の詳細については、アリババクラウドの各種規約ドキュメントセンターを参照のこと。アリババクラウドは、顧客サポートのために各種の伝達チャンネル(ライブチャット、チケット、電子メール、提案記事などを含むがこれに限定されない)を確立した。顧客に影響を与える可能性のある問題についても、確立されたメカニズムを通じてグローバルカスタマーサポートチームから顧客に伝達される。さらに、アリババクラウドは国際的な標準とベストプラクティスに従う。セキュリティと法令遵守に関する詳細は、セキュリティおよびコンプライアンスセンターで顧客に伝達される。

アリババクラウド上に構築されたアプリケーションのセキュリティについて、アリババクラウドと委託会社は共同責任を負う。アリババクラウドは基盤となるクラウドサービスプラットフォームと提供するセキュリティサービスおよび機能に対するセキュリティの責任を負い、顧客はアリババクラウドサービスに基づいて構築されるアプリケーションのセキュリティに責任を負う。アリババクラウドの顧客はサービスの選択とクラウド上アーキテクチャの設計にあたり、アリババクラウドが導入した統制とセキュリティに関して顧客が負う責任の一部として要求される構成および運用上の統制の両方を考慮に入れて目標を評価する必要がある。サービスの設計および提供時に顧客に対するサービスコミットメントを達成しながら関連する法律および規制要件を遵守するため、アリババクラウドはシステムおよび運用要件を方針、標準、マニュアル、手続の形式で規定した。これらは文書化され組織全体に伝達される。

III. 統制環境、情報と伝達、リスク評価、統制活動、およびモニタリング活動の概要

内部統制は、アリババクラウドの取締役会、経営陣、執行スタッフによって確立および維持管理されている。アリババクラウドの内部統制は、米国公認会計士協会によって定義された以下の 5 つの要素で構成されている。

- **統制環境** - 標準的な要求事項およびシステム構造を提供するとともに、従業員の内部統制に対する意識に影響を及ぼす、内部統制を導入するうえでの基盤である。
- **情報と伝達** - 情報および伝達システムを介して、実施する必要のある内部統制に関する情報を従業員が確実に入手および伝達するようにするとともに、情報伝達活動の運用を管理する。
- **リスク評価** - 事業活動において内部統制の目的の達成に悪影響を与える可能性のある関連するリスクを識別して体系的に分析し、リスクに対応するための合理的な戦略を策定する。
- **モニタリング活動** - 内部統制手続全体をモニタリングし、必要に応じて是正を行う。また、状況が許す場合、内部統制システムの適時対応を確実にするために、対応する統制手続を調整する。
- **統制活動** - 経営陣によって設計された統制が、リスクに対処して会社の統制目標を達成するために有効であり、効果的に運用されていることを確認するための方針、手続、標準、作業指示を規定および実施する。

以下にこれら 5 つの要素について概説する。

1. 統制環境

アリババグループの一事業部門であるアリババクラウドは、組織としてアリババグループ(以下「アリババ」または「グループ」)全体の統制環境に従う。アリババの経営陣は、組織のコアバリューと社風、アリババ社員の意識を定めている。全体的な統制環境には、アリババクラウドの経営陣および従業員の内

部統制に対する姿勢および認識と、統制の有効性を支える活動が反映される。これにより、その組織にとっての統制活動の重要性と、従業員が組織の方針、手続、標準に向ける注目の大きさが定まる。アリババクラウドは内部統制を定義および実施するために、グループと足並みを揃えたコアバリューおよび行動規範を定め、各事業部の組織構成、役割、責任を明確に定義し、方針、手続、標準を組織内で文書化および伝達する。

アリババクラウドには組織の構成と各事業部が定義されている。各事業部の役割と責任は組織レベルで割り当てられる。

アリババクラウドはグループのスタッフ向け採用、オンボーディング、トレーニングプログラムに従う。人材管理要求事項を達成するための方針および手続に従って、正式なメカニズムが規定された。

2. 情報と伝達

アリババクラウドは、アリババクラウドとその従業員間、ならびにアリババクラウドとその顧客間の効果的な情報伝達を確実にするため、確立された方針および手続に則って、内部および外部の伝達経路を確立した。

3. リスク評価

アリババクラウドは、企業内のリスクおよび提供サービスに関連するリスクを識別し、分析し、管理するためのリスク管理フレームワークを確立した。リスク管理フレームワークには、経営陣レベルまたは執行部レベルの要員が関与しており、セキュリティ、可用性、機密保持のリスクを含む戦略的および運用的リスクを対象とする。

アリババクラウドは、ISO/IEC 27001:2013 および関連する業界標準に従って、総合的な情報セキュリティ管理システムを確立した。リスクの識別、分類、脅威のモニタリングと分析、統制施策の評価、リスクの解消などを対象とする、情報セキュリティリスク評価を年 1 回実施することを義務付けている。

アリババクラウドの情報データセンターチームは、各データセンターのリスクインベントリを維持管理し、リスクインベントリを対応するリスクマネージャーに伝達する。

4. モニタリング活動

アリババクラウドは、情報セキュリティ管理について総合的かつ体系的な検査および評価を毎年実施し、情報セキュリティ方針、規格、要求事項の履行と、セキュリティ統制の適切性を評価する。さらに、アリババクラウドの情報セキュリティ管理は、定期的に内部監査を受ける。これらにより、情報セキュリティ方針の遵守と統制の運用の有効性が検証される。監査結果は、経営陣に直接報告される。

IV. 統制活動

アリババクラウドは統制活動を策定するための方針、手続、標準、作業指示を規定する。これらは適用される Trust サービス規準を有効に達成するために導入されている。アリババクラウドの内部統制の構成要素には、組織に、または特定の手続とアプリケーションに幅広い影響を与える統制が含まれる。

1. 情報セキュリティのガバナンスとリスク管理

アリババクラウドは、すべての部署および要員に対し、その日常業務および管理手続についての指針を提供するため、情報セキュリティおよび IT 運用リスクを統制および管理するための方針および手続を確立した。すべての方針は、アリババクラウドの内部プラットフォームで従業員による参照が可能である。

2. 人事

アリババクラウドは、人材管理について以下の方針および行動規範を確立した。新しく入社した従業員は、労働契約、秘密保持契約、宣誓書に署名することが要求される。これらの中には、情報セキュリティに関する従業員の責任と義務が明確に定義されている。

アリババクラウドは従業員の役割と責任に加えて指揮命令系統に関する情報を、全社員に公開されている社内ポータル上で文書化および維持管理した。業績評価が定期的に実施される。情報セキュリティおよび行動規範要件に対する従業員の違反があった場合、対応する罰則の決定とともに社内ポータルで公表される。

アリババクラウドは、行動規範、情報、データセンターに関するグループの要求事項に沿ったトレーニングスキームを規定した。

3. データセキュリティ管理

アリババクラウドは、データの収集、転送、処理、交換、保管、破棄を含むデータライフサイクルを通じて、データセキュリティの管理および統制を徹底するため、データセキュリティライフサイクル管理プロセスを規定した。データセキュリティガイドラインに定義された関連要求事項に従って、セキュリティ対策および統制メカニズムが設計および導入された。また、データのバックアップおよび冗長性に関連する統制が規定および導入された。当該統制の設計および実施の有効性を確保するためのモニタリングプロセスが導入されている。

4. インフラストラクチャと仮想化セキュリティ

アリババクラウドのインフラストラクチャセキュリティ対策および仮想化テクノロジーにより、内部ネットワークと物理サーバーはセキュアに保護される。これにより、テナントのクラウドリソースへの不正アクセスを防ぎ、仮想化コンピューティング、ストレージ、ネットワークの分離を通じて、同じクラウドコンピューティング環境内でテナント間を分離する。

アリババクラウドはオペレーティングシステムとイメージの保護に対する保護標準を規定した。アリババクラウドのホストサーバーに採用されるオペレーティングシステムおよびイメージは、標準に従って構成する必要がある。

5. ID およびアクセス管理

アリババクラウドの ID およびアクセス管理は、情報資産を不正アクセスから保護するために、アクセス制御管理方針に記載された最小権限および職務分掌の原則に従って、アリババクラウド環境内のリソースおよびシステムへのアクセスを適切に管理および制限する。

アカウントの作成、変更、削除を管理するために、アカウントおよびアクセス管理の方針ならびに手続が導入されている。従業員のアクセスが適切であることを確認するために、定期的アクセスレビューが実施されている。従業員による単純なパスワードの設定を防止するため、パスワードポリシーがアカウント管理プラットフォームに組み込まれている。

6. 資産管理

アリババクラウドは、クラウドサービスの提供に使用されるアリババクラウド環境内の情報資産に適切な保護レベルを適用するため、情報資産を識別、インベントリ記録、分類、管理する。情報資産を識別、分類、管理するための方針および手続が規定された。また、情報資産の取得、配置、廃棄の手続を統制するためのガイドラインが規定された。新しい資産の取得には適切な担当者による認可が必要である。新しい資産を運用環境に配置する前にテストを実施し、テスト結果を文書化する必要がある。データセ

ンター外への資産の転送要求には適切な承認が必要であり、転送された資産は承認後に適切な方法で廃棄する必要がある。

7. 顧客認証およびアクセス管理

アリババクラウドは、顧客が各自のリソースへのアクセスをセキュアに認可し、顧客環境へのアクセスが適切に制限されるようにするため、ユーザーID 管理およびリソースアクセス制御機能を顧客に提供する。

アリババクラウドはアリババクラウド公式 Web サイトに関する Web サイトサービス契約を定めている。この契約には、アリババクラウドが提供するサービスのレベル、機密保持およびデータ開示の条件を含め、顧客アクセス管理に関する顧客とアリババクラウドそれぞれの責任と義務が定義されている。アリババクラウドのアカウント登録プロセスにおいて、顧客はサービス契約の受諾に合意し、確認する必要がある。アリババクラウドの Web サイトでの登録が正常に完了すると、顧客専用のアリババクラウドアカウントが割り当てられる。顧客がセルフサービス式のパスワードリセットを実行すると、確認済みの携帯電話に送られた SMS 確認コードによって顧客の ID が検証される。

Resource Access Management (RAM)は、アリババクラウドが提供する集中型のユーザーID 管理およびリソースアクセス制御サービスである。RAM を使用することで、1 つのアリババクラウドアカウントに独立した複数の RAM ユーザーを割り当てることができる。アリババクラウドのアカウント所有者は RAM 内に、従業員、システム、アプリケーション用の個別 RAM ユーザーアカウントを作成できる。RAM では、RAM ユーザーごとに異なるパスワードまたは API アクセスキーを割り当てることができるため、アリババクラウドアカウントの資格情報を共有することで発生するセキュリティリスクが排除される。それぞれの RAM ユーザーはクラウドリソースへの操作を実行するため、個別のログオンパスワードまたはアクセスキーを使用してアリババクラウドコンソールにログインするか、サービス API を呼び出すことができる。既定では、新しく作成された RAM ユーザーアカウントにはリソースに関する権限が何も付与されない。顧客は最小権限の原則に従って、最小限の操作権限をそれぞれの RAM ユーザーに割り当てることができる。

アリババクラウドの O&M 担当者が顧客のアリババクラウドリソースに一時的にアクセスする必要が生じた場合、顧客リソースへのアクセスには顧客による認証および承認が必要になる。

8. 暗号化およびキー管理

アリババクラウドの暗号化およびキー管理は、最先端の暗号化を効果的に使用することで機密データの機密性、信ぴょう性、整合性を確保する。機密データの暗号化が実施されているなど、保護対策に関する方針およびガイドラインが規定された。

Key Management Service (KMS)はアリババクラウドが提供するセキュアな管理サービスで、セキュアなキーホスティングや暗号操作などの基本機能を提供し、キーローテーションなどのセキュリティ手法を組み込む。他のクラウドサービスで管理されるユーザーデータを暗号化するために、KMS をそのクラウドサービスに統合することができる。

アリババクラウドはデータセキュリティを確保するため、転送中の暗号化、保管中の暗号化、ハードウェアベースのメモリ暗号化を含めたエンドツーエンドの暗号化を使用する。アリババクラウドは包括的なデータ暗号化ソリューションの一部として、HSM ベースのデータ暗号化サービスと SSL Certificates Service を提供する。

9. 物理的および環境的セキュリティ

アリババクラウドは、アクセスセキュリティ管理と環境制御を統制するための物理的および環境的セキュリティ管理に関する方針と手続を確立した。アクセス権の付与は最小権限の原則に従う。

アリババクラウドのデータセンターは物理環境のセキュリティを確保するため、必要な環境的保護とモニタリングの統制およびメカニズムを備えている。データセンターサービスプロバイダーのパフォーマンスがモニターされ、定期的に評価される。

10. エンドポイントセキュリティ

アリババクラウドは、ソフトウェアのインストール、ウイルス対策ソフトウェア、データ漏洩保護に加え、モバイルデバイスの不適切管理または誤用に起因するセキュリティインシデントおよび脆弱性から運用システムを保護するためのモバイルデバイス関連のネットワークへの参加を統制するために方針および手続を規定した。また、Bring-Your-Own-Device (BYOD)デバイスとウイルス対策ソフトウェアのインストールを管理およびモニターしてエンドポイントセキュリティを確保するため、統制ならびに技術的措置が確立された。エンドポイントのデータセキュリティをモニターするため、データ漏洩保護(以下「DLP」)ソリューションが確立された。

11. 脅威および脆弱性管理

アリババクラウドの脅威および脆弱性管理は、システムの不具合と不正な行為を検出し、是正措置または軽減措置を適時に取ることで、アリババクラウドと同社の顧客環境のセキュリティを確保する。アリババクラウドは、セキュリティ脆弱性の分類や対応メカニズムを含むセキュリティ脆弱性管理を統制するための方針およびガイドラインを規定した。脅威および脆弱性管理プロセスは、関連する方針およびガイドラインの要求事項に従って運用される。例外的な運用はセキュリティ部門によって追跡調査され、必要な措置が講じられる。クラウドプラットフォームは毎日スキャンされ、スキャン結果が脆弱性管理プラットフォームに収集されモニターされる。

12. セキュリティインシデント管理

アリババクラウドのセキュリティインシデント管理は、セキュリティイベントのモニタリングと検出、検出されたイベントに対する適切な対応の適時実行を通じてセキュアな運用とシステム保護を実現する。アリババクラウドはセキュリティインシデントの分類、エスカレーション、通知プロセスを統制するため、セキュリティインシデント対応標準およびガイダンスを規定した。クラウドプラットフォームのセキュリティはセキュリティインシデントを検出するためにモニターされ、プラットフォームリソースが攻撃されるとインシデントを適切に処理するためのセキュリティインシデント対応プロセスがトリガーされる。クラウドプラットフォームで実行された活動のログは中央のロギングプラットフォームを介して収集され、リアルタイムコンピューティングプラットフォームとオフラインコンピューティングプラットフォームにインポートされる。異常の分析と検出のため、各コンピューティングプラットフォームでセキュリティモニタリングアルゴリズムを介してログが処理および分析される。インシデントを適時に分析、追跡し、対応を調整する責任はセキュリティチームが負う。セキュリティインシデントが確認された場合、複数の伝達チャンネルを介して影響が及ぶ顧客に通知される。

13. 問題管理

アリババクラウドは誤動作の分類、誤動作に対する適時対応の要件、リスクレベルに基づく誤動作のエスカレーションおよび解決を統制し、問題または誤動作が適時に識別、評価、エスカレーション、解決されるようにするため、誤動作管理基準および手続を確立した。各種チャンネル経由で発見される誤動作を識別、統合、追跡、モニターするため、誤動作管理プラットフォームが開発および利用された。誤動作が発見された場合、これに責任を負う要員によって適時に追跡調査が行われる。影響を受ける顧客には複数の伝達チャンネルを介して通知が送られる。

14. 変更管理

アリババクラウドは、クラウドプラットフォームで行われたすべての変更を記録、評価、テスト、承認し、必要な場合は運用環境への実装前に正式な方針および手続に従って伝達するため、標準化された変

更管理プロセスを規定した。運用システムへのアクセスが最小権限および職務分掌の規則に従うことを確認するため、変更管理プロセスに関するアクセス制御が規定および導入された。開発、テスト、運用別に分離された環境が実装されており、各種環境へのアクセスは制御され、認可された要員に制限される。

アリババクラウドは、製品開発ライフサイクルの各ステージにセキュリティを組み込むことで、セキュリティ機能を強化し、クラウド製品のセキュリティリスクを軽減するため、クラウド製品に特化した SPLC ソリューションを実装した。製品がクラウドコンピューティング向けの厳格な要件を満たすようにするため、製品の開発開始から、セキュリティアーキテクチャレビュー、セキュアな開発、セキュリティの検証、製品のリリース、インシデント対応までの 6 ステージにわたり、包括的なセキュリティ開発メカニズムが導入されている。

15. ビジネス継続性管理

アリババクラウドは中断発生時に重要業務を適時に回復できるようにするため、ビジネス継続性管理に関する方針およびガイドラインを規定した。ビジネス継続性計画が開発され、年次でテストされた。

アリババクラウドは容量のボトルネックを防止するため、容量の予測、計画、モニタリングに関して規定された手続に従う。アリババクラウドは容量管理のベースラインを規定し、容量の制約により可用性が損なわれるリスクを評価する。容量はリアルタイムでモニターされ、予測使用量が許容容量を超えるとフォローアップ対策が取られる。

サービス可用性レベルが定義され、公式 Web サイトで顧客に公開されているサービスレベルアグリーメント内に明記された。

16. ベンダー管理

アリババクラウドは、第三者サービスプロバイダーが合意されたセキュリティおよびサービス提供レベルに準拠することを確認するため、ベンダーおよび第三者従業員の現場作業中ならびにその前後の管理を統制するための方針および手続を規定した。

すべてのベンダーには、作業開始前にアリババクラウドによる経歴調査を受け、契約書と機密保持契約に署名することが要求される。提供されるサービスは定期的な評価の対象である。

17. 監査および法令遵守

アリババクラウドは、内部統制の継続的モニタリング、高いセキュリティ基準および品質の確保、有効な認定および認証の維持、関連する法令、規制、契約要件の遵守を目的に、監査および法令遵守管理に関する方針と手続を規定した。

経営陣によってレビューおよび承認された監査計画に従って、内部監査が年 1 回以上実施される。内部監査の調査結果は内部監査チームによって定期的に追跡調査され、修正措置と予防措置が統制環境およびシステムに導入される。

アリババクラウドは新しい業界標準に従うため、内部統制システムの継続的改善に取り組む。世界中で運営および管理されるアリババクラウドは、国際情報セキュリティ標準に従うとともに、クラウド製品およびサービスの提供地域における国内情報セキュリティ標準に従う。アリババクラウドは国際的ベストプラクティスへの準拠に取り組んでおり、独立した立場から業界標準の遵守を定期的に検証されている。詳しくは、アリババクラウドセキュリティおよびコンプライアンスセンターを参照のこと。

18. 委託会社の相補的な統制

共同責任モデルの対象となるアリババクラウド内のアプリケーションおよびデータのセキュリティは、アリババクラウドとその顧客が共同で責任を負う。アリババクラウドは自社システムの設計にあたり、

適用される Trust サービス規準を満たすため、委託会社によって一定の相補的な統制が導入されることを意図した。適用される Trust サービス規準は、アリババクラウドの統制のみによっては効果的に達成できない。そのため、アリババクラウドの統制とともに各委託会社の内部統制も評価する必要がある。
このセクションでは、アリババクラウドが委託会社(すなわち顧客)の責任と考える統制領域について説明する。したがって、委託会社がこれらの相補的な統制を検討して開発する必要がある。以下の統制リストに、適用される Trust サービス規準を達成するために顧客が導入しなければならない可能性がある追加の方針、手続、統制を示す。適用される Trust サービス規準は、相補的な統制が適切に設計され、効果的に運用された場合に限り達成可能である。各委託会社は、各自で設定した内部統制を評価し、統制が適切に設計され、効果的に運用されているかどうかを判断する必要がある。以下の表は、委託会社の基礎となる統制を網羅した一覧ではなく、またそのような一覧を記載することを意図したものではない。効果的な管理を実現するために、委託会社は特定の事例ごとの必要性に応じて、その他の統制活動を導入しなければならない場合がある。

領域	適用製品	委託会社(顧客)の責任
組織のセキュリティ	すべて	• 委託会社はアリババクラウド内に配置されるアプリケーションとデータに関する相補的な統制の設計にあたり、リスク管理プロセスを構築し、リスクに対処する統制目標を評価する必要がある。 • 委託会社は組織内の情報セキュリティ管理および運用の指針となる方針、手続、標準を規定する必要がある。 • 委託会社は相補的な統制の設計と運用有効性を評価するにあたり、相補的な統制のモニタリングメカニズムを確立する必要がある。
アプリケーションの統制	すべて	• 委託会社は、アプリケーションレベルの統制(職務分掌、統制の自動化、システム演算、レポートの生成、システムインターフェイス)が適切に設計され、有効に動作するよう、適切な統制を導入する必要がある。
アクセスセキュリティ	すべて	• 委託会社はクラウドインスタンスを保護するため、セキュリティグループ、RAM ロール、アクセス制御リストなどのアクセス制御を導入する必要がある。 • ユーザーID は、提供される連絡先情報を介して検証される(委託会社が自身のクラウドアカウントに対してセルフサービスのパスワードリセットを実行するときの SMS 確認コードなど)。そのため委託会社は、アリババクラウドから要求される連絡先情報(携帯電話番号など)を正確に登録して適時更新し、検証チャンネル(携帯電話、電子メールなど)を安全に維持するために、関連する統制を導入する必要がある。 • 委託会社は自社のクラウドリソースにアクセスするために多要素認証手法を使用する必要がある。パスワードポリシーの複雑さを考慮に入れてパスワードポリシーを規定する必要がある。 • アクセスキーを適切に保護し、機密保持する必要がある。 • 委託会社は強化したインスタンスのファイアウォールポリシーを導入する必要がある。 • 委託会社は、ユーザー認証システムの整合性をサポートし、不正アクセスを防止するため、適切なセキュリティ構成を導入する必要がある。

		• 委託会社は、自身のカスタムイメージを不正アクセスから保護するためのアクセス制御を実装する必要がある。 • 委託会社はネットワークセキュリティ標準を規定し、自社の仮想プライベートネットワークが適切な内部ネットワークのみに接続されるようにする必要がある。 • 委託会社は自社の各種 ECS インスタンスのアクセスセキュリティを保護するため、承認されたセキュアな更新のみがセキュリティグループの規則に適用されるようにする統制を導入する必要がある。 • 委託会社は、自社のインスタンスを不正アクセスから保護するため、IP ホワイトリストを確立して維持管理する必要がある。 • 委託会社は、バケットおよびオブジェクトを不正アクセスから保護するため、ストレージアクセスに対して有効なアクセス制御を確立する必要がある。 • 委託会社は自社のクラウドリソースに対して許可されたアクセスおよび IP の定期的レビューを規定する必要がある。 • 委託会社は統制モニタリングプロセスとインシデント対応プロセスをサポートするため、該当する場合は機密情報に関わるアクティビティ、システムエラー、データ変更などをログに記録する機能を有効にして設定する必要がある。
	IoT 製品のみ	• 委託会社は、自身の IoT デバイス、サーバー、ゲートウェイ端末のセキュリティを確保するため、適切なアクセス制御を実装する必要がある。 • 委託会社は、自身が開発した IoT ファームウェアアップグレードパッケージのローカルセキュリティを確保するため、適切なアクセス制御を実装する必要がある。
データセキュリティ	すべて	• 委託会社は、アリババクラウドによって提供されるデータ転送サービスを利用する場合に越境データ転送要求事項が考慮されるよう、適切な統制を導入する必要がある。 • 委託会社はアリババクラウドとのすべてのインタラクションに対して暗号化(TLS/SSL)接続を使用する必要がある。高いデータ転送セキュリティレベルを必要とする委託会社(PCI DSS の遵守が必要な場合など)は、TLS 1.2 を採用する必要がある。委託会社は必要に応じて自社の CMK のローテーションを設計する必要がある。 • 委託会社は自社固有の要件に応じた暗号化オプションを導入し、維持管理する必要がある。
	IoT 製品のみ	• 委託会社は、自身の IoT デバイス、アプリケーション、サーバー、ゲートウェイ端末の間で転送されるデータに対して適切な保護手段を講じ、これを評価する必要がある。 • 委託会社は、機密データ(ローカルにダウンロードされる deviceSecret など)のセキュリティと、ローカルに保存されるその他のデータのセキュリティを確保するため、適切な統制を導入する必要がある。
変更管理	すべて	• 委託会社はアリババクラウド上にホストされる自社のアプリケーションおよびデータに対して、適切な変更管理統制を導入する必要がある。

		• 委託会社は必要に応じて自社インスタンスに最新パッチを適用する必要がある。 • 委託会社は開発活動から運用システムを切り離すため、分離された環境をセットアップする必要がある。
	IoT 製品のみ	• 委託会社は、アリババクラウドによって提供されるソフトウェア(SDK、モバイルアプリケーション、AliOS Things など)の再開発時のセキュリティを確保し、適時にセキュリティパッチアップグレードを行うため、適切な変更管理統制を導入する必要がある。
問題管理	すべて	• アリババクラウドが提供する製品およびサービスに固有の誤動作またはセキュリティインシデントがあった場合、委託会社はこれをアリババクラウドに通知し、アリババクラウドとのインシデント対応プロセスに適時に対応する必要がある。
ビジネス継続性管理	すべて	• 委託会社は、自社のニーズに合った適切なバックアップおよびリストア戦略と計画を策定する必要がある。これらはその有効性を確保するためにテストする必要がある。アリババクラウドはデータバックアップ機能を顧客に提供しており、委託会社は適時のバックアップおよびリストア目標を達成するための該当メカニズムを確立できる。 • 委託会社は自社のニーズに合わせたディザスタリカバリ計画およびビジネス継続性計画を規定する必要がある。定期的に実践訓練を行う必要がある。 • 委託会社は必要な冗長性レベルと高可用性アーキテクチャを実現するため、マルチゾーンおよびマルチリージョンオプションを利用し、冗長システムを設計および実装する必要がある。
	IoT 製品のみ	• アリババクラウドは、自社の IoT 製品およびサービスシステムでデバイスモニタリング機能を提供している。委託会社は、自身の IoT デバイスとゲートウェイの状態をモニターするため、適切な統制を導入する必要がある。 • 委託会社は、自身の IoT デバイスとゲートウェイに保存されたデータが有効にバックアップされるよう、適切な統制を導入する必要がある。