ORACLE

Oracle Cloud Hosting and Delivery Policies

発効日：2024 年 2 月 Version 3.6

目次

概要

この *Oracle Cloud Hosting and Delivery Policies*（以下「本 Delivery Policies」といいます）は、お客様が注文したオラクル・クラウド・サービスについて説明しています。本 Delivery Policies は、他のオラクル・クラウドのポリシー文書を参照する場合があります。本 Delivery Policies または当該他のポリシー文書にいう「お客様」とは、お客様の注文で定義される「お客様」を指すものとみなします。別段の記載のない限り、本 Delivery Policies の全約定は本番クラウド・サービスに適用されます。

本 Delivery Policies にいうクラウド・サービスの「データ・センター地域」とは、当該対象サービスについてのお客様の注文に掲げられている地理的地域を指すか、または該当の場合においては当該対象サービスのインスタンスの有効化時にお客様により選択された地理的地域を指します。お客様により注文されたクラウド・サービスに適用されるデータ・センター地域の目的上、以下が適用されます。

- 「Europe（ヨーロッパ）」とは、欧州連合加盟国、英国およびスイスを総称したものを指します。
- 「APAC」とは、アジア太平洋地域をいいます。ただし、中国内においてはオラクルがデータ・センターを有しないため、中国を除きます。
- 「North America（北米）」とは、米国本土およびカナダから成る地理的地域を指します。ただし、クラウド・サービスを購入する団体が最初にメキシコでプロビジョニングすることを選択した場合、北米とは米国本土、カナダおよびメキシコから成る地理的地域を指します。

お客様により注文されたオラクル・クラウド・サービスについては、お客様コンテンツは、当該対象サービスに適用されるデータ・センター地域にて保管されます。オラクルは、データの冗長性をサポートするため、指定データ・センター地域内における別の場所にお客様コンテンツを複製することがあります。本 Delivery Policies における用語（英語版においては大文字で始まるもの）のうち本書内で別段の定義がなされていないものは、オラクル契約、お客様の注文書またはポリシー（場合において該当するもの）において当該用語に付与された意味を有するものとします。本 Delivery Policies は、半年ごとに更新されます。

お客様の注文またはオラクルのサービス仕様書（定義はオラクル・クラウド・サービスに関するお客様の契約のとおりとします。これには、Oracle Cloud Services Pillar ドキュメントおよび Service Descriptions のほか、Oracle Cloud Services Agreement に記載されている追加的な定義も含みます）には、特定のオラクル・クラウド・サービスに関係する追加的な詳細情報または例外事項が含まれていることがあります。オラクル・クラウド・サービスの Oracle Cloud Service Pillar ドキュメント、Service Descriptions および Program Documentation は、www.oracle.com/contracts で閲覧できます。

オラクル・クラウド・サービスは、オラクルの契約書、お客様の注文、およびかかる対象サービスに適用されるサービス仕様書の条件に基づき提供されます。オラクルによるオラクル・クラウド・サービスの提供は、お客様およびお客様のユーザーが、これらの契約および一体となるポリシーで規定されている義務と責任を遵守することを、条件としています。本 Delivery Policies、および本書において参照される文書は、オラクルの裁量により変更される場合があります。ただし、オラクルによるポリ

シーの変更は、お客様の注文のサービス期間中に提供されるオラクル・クラウド・サービスのパフォーマンス、機能、セキュリティーまたは可用性のレベルを実質的に低下させるものではありません。

オラクル・クラウド・サービスは、Oracle Cloud at Customer Services を除き、オラクルの擁するデータ・センターまたは第三者インフラストラクチャー・サービス提供者においてデプロイされます。Oracle Cloud at Customer Services は、お客様のデータ・センターまたはお客様が維持する第三者のデータ・センターにデプロイされるパブリック・クラウド・サービスです。お客様は、当該対象サービスを単体で購入することができます。また、単体購入ではなく、当該サービスを他のオラクル・クラウド・サービスの基礎プラットフォームとしてデプロイすることもできます。Oracle Cloud at Customer Services の場合、オラクルは、オラクルが当該対象サービスを運用するために必要なゲートウェイ機器を含む特定のハードウェア・コンポーネントをお客様のデータ・センターに提供します。お客様は、オラクルのハードウェア（ゲートウェイ機器を含む）をデプロイするための十分な空間、電源および冷却設備を提供する責任、ならびにオラクル・クラウド・オペレーション部門がサービスにアクセスするための十分なネットワーク接続性を確保する責任を負います。オラクルは、ゲートウェイ機器も含め、オラクルのハードウェア・コンポーネントの保守について、単独で責任を負います。

本 Delivery Policies は、Oracle BigMachines Express またはお客様の注文もしくは該当する Service Descriptions においてオラクルが指定する他のオラクル・クラウド・サービスのいずれにも、適用されません。

1. ORACLE CLOUD SECURITY POLICY

1.1 オラクルの情報セキュリティー・プラクティス – 一般

オラクルは、お客様のオラクル・クラウド・サービス内でオラクルがホストするお客様コンテンツの機密性、完全性および可用性を保護するため、かつ不正な処理行為（データ消失または不法なデータ破壊など）からお客様コンテンツを保護するために設計されたオラクル・クラウド・サービス向けセキュリティー・コントロールおよびプラクティスを採用しています。オラクルは、継続的にこれらのセキュリティー・コントロールおよびプラクティスの強化および改善に努めています。

オラクル・クラウド・サービスは、ISO/IEC 27002 に基づく情報セキュリティー管理策の実践規範に整合したポリシーのもとに運用されており、当該ポリシーから、包括的な一連の管理策の選択がなされています。オラクル・クラウド・サービスは、National Institute of Standards and Technology（以下「NIST」といいます）の 800-53 および 800-171 に準拠しています。

オラクルのクラウド情報セキュリティー・プラクティスは、オラクル・クラウド・サービスとお客様による当該オラクル・クラウド・サービスの利用とに適用可能なセキュリティー・エリアを確立し、規律するものです。

オラクルの担当者（従業員、契約社員および派遣社員を含みます）は、オラクルの情報セキュリティー・プラクティス、および担当者の雇用または担当者からオラクルへの役務提供を規律するあらゆる追加のポリシーの適用を受けます。

オラクルでは、情報セキュリティーに対し全体的なアプローチを行っており、ネットワーク、オペレーティング・システム、データベースおよびソフトウェアのセキュリティー・プラクティスおよび手

続きが強力な内部統制、ガバナンスおよび監督によって相互に補完し合う多層防御セキュリティー戦略が実装されています。

お客様のセキュリティー態勢をお客様が構成できるようにするこれらオラクル・クラウド・サービスの場合、別段の記載のない限り、お客様は、選択された当該オラクル・クラウド・サービスのオペレーティング・システムその他の関連ソフトウェアのうちオラクル以外を提供元とするもの（お客様コンテンツも含みます）を構成し、運用し、保守し、セキュアにすることについて、責任を負います。お客様は、お客様コンテンツの適切なセキュリティー維持、保護、およびバックアップについて責任があります。これには、不正アクセスからお客様コンテンツを保護するために暗号化技術を使用すること、およびお客様コンテンツを定期的にアーカイブすることを含む場合があります。

1.2 物理的セキュリティー・セーフガード

オラクルは、お客様コンテンツのホスティング場所であるコンピューティング設備について、権限のない者によるアクセスを防止するための措置を講じています。かかる措置には、セキュリティー担当者の起用、ならびにセキュアな建物および指定されたデータ・センター施設の利用も含まれます。オラクルは、オフィス・ロケーションと本番クラウド・インフラストラクチャーの両方に対し、セキュアなコンピューティング設備を提供します。オフィス・ロケーションとオラクルが管理するコロケーション/データ・センターとの間の共通管理についての現時点での一例としては、次のとおりです。

- 物理的なアクセスについては、権限を必要とし、監視されています。
- すべての従業員と訪問者は、施設内にいる間、目視可能な公式の身分証を着用しなければなりません。
- 訪問者は、訪問者登録への署名が必要で、施設内では付添および/または監視される必要があります。
- キー/アクセス・カードの所持および施設へのアクセス機能は監視されます。オラクルを退職するスタッフは、キー/カードを返却しなければなりません。

追加の物理的なセキュリティー保護手段が、オラクルがコントロールするクラウドのデータ・センターに設置されており、現在含まれる保護手段としては、例えば、

- 敷地内はCCTVによって監視されています。
- 入口は、車両による不正侵入を防止するように設計された、物理的な障壁によって保護されています。
- 入口は、24時間365日体制で警備員によって有人警備されており、警備員は目視による身分確認を行い、訪問者の付添管理を行います。
- 環境ハザードに関する保護手段。
- 機器のいかなる物理的移動も、手渡しによる受領、その他の承認済み変更管理手順による管理の対象となります。
- ネットワーク・ケーブルは導管で保護され、可能な場合、公共エリアでの配線は避けています。

本条項は、Oracle Cloud at Customer Services には適用されません。お客様は、オラクルによる Oracle Cloud at Customer Services の提供に必要な Oracle Cloud at Customer Services 関連のハード

ウェア（ゲートウェイ機器も含まれます）のホスティングおよび運用ならびにネットワーク接続のため、自前のセキュアなコンピューティング設備を用意する必要があります。

1.3 システム・アクセス管理

オラクルのポリシーでは、次に掲げる管理体制の適用が必要とされています。すなわち、パスワードによる認証および/または複数要素認証、文書化された承認管理、ならびにアクセスのロギング。お客様コンテンツへのアクセス権を有するオラクル人員による Oracle Cloud Network へのリモート・アクセスのいずれも、複数要素認証を用いた Virtual Private Network の利用による制限の対象となります。Virtual Private Network の必須利用に加えて、Oracle Cloud Network へのアクセス権の付与をオラクル人員が受ける前に、オラクルは、デバイス・ポスチャ・チェックを実施するとともに、要塞ホストといった制御体制を整備します。オラクルは、Oracle Cloud Network およびオラクル・クラウド・サービスへのアクセスに個人所有デバイスを使用することを（ポリシーおよび技術的制御の両面で）禁止しています。

Oracle がホストするクラウド・サービスの場合：（i）クラウド・サービスへのログインの記録、および（ii）データ・センターへの論理的アクセスの制限および保護。

1.4 データ・アクセス管理

オラクルの管理するサービス・コンポーネントの場合、お客様コンテンツに対するオラクルによるアクセスは、権限のあるスタッフに限定されます。

オラクル・クラウド・サービス（オラクル・クラウド・サービス内に存するお客様コンテンツも含みます）へのオラクル人員によるアクセスについて、オラクルは、ロール・ベース・アクセス制御（RBAC）を実施するとともに、「need to know（知る必要性）」、「least privilege（最小権限）」および「segregation of duties（職務の分離）」というアクセス管理原則を採用します。また、オラクルは、オラクル・クラウド・サービスおよびお客様コンテンツへのお客様のユーザーによるアクセスをお客様側で管理することのできるメカニズムを、提供します。

1.5 外部接続のためのユーザーの暗号化

お客様のオラクル・クラウド・サービスへのアクセスは、オラクルが提供する安全な通信プロトコルを経由します。アクセスが Transport Layer Security（TLS）有効化済みの接続を介している場合、その接続には少なくとも 128 ビットの暗号化がネゴシエーションされています。暗号キーを生成するために使用されるプライベート・キーは、少なくとも 2048 ビットです。TLS は、オラクルによりデプロイされるすべてのウェブベース TLS 認証アプリケーションについて、実装済みまたは設定可能です。オラクル・プログラム用に認定された、より強度の高い暗号と互換性のある、セキュリティーを向上させた、入手可能な最新のブラウザーを利用して、ウェブ対応プログラムに接続することを推奨します。オラクル・クラウド・サービスの各リリースに対する認証されたブラウザーの一覧は、お客様がアクセスできるポータル経由、または対応するオラクル・クラウド・サービスの Service Descriptions の中で入手可能です。一部事例において、お客様がオラクル・クラウド・サービスとの統合を希望する第三者（ソーシャル・メディア・サービスなど）のサイトによっては、暗号化された接続を受け付けない場合があります。第三者のサイトとの HTTP 接続がオラクルにより許可されたオラクル・クラウド・サービスに対しては、オラクルは、HTTPS 接続に加えて、当該 HTTP 接続を有効にします。

1.6 入力管理

お客様コンテンツの出所については、お客様の管理下にあることから、お客様が責任を負うものとし、オラクル・クラウド・サービスへのお客様コンテンツの統合は、お客様により管理されるものとします。

1.7 データおよびネットワークの分離

お客様コンテンツは、オラクル・クラウド・サービス内でホストされる他の顧客のコンテンツから論理的または物理的に分離されます。Oracle Cloud ネットワークのいずれも、オラクルのコーポレート・ネットワークから分離されています。

1.8 機密保持およびトレーニング

オラクル人員は、機密保持契約の対象となっており、その雇用時に情報保護に関する意識向上トレーニングを修了することが義務付けられています。その後も、全オラクル人員は、オラクルにおける該当のセキュリティーおよびプライバシーに関する意識向上トレーニング・ポリシーに基づいてトレーニングを定期的に修了する必要があります。

1.9 資産管理

オラクルは、オラクルのクラウド・サービス資産の保護および在庫管理について、責任を負います。この責任には、アクセス・リクエストをレビューし、業務上必要性がある者に対しアクセス・リクエストを許可すること、および資産目録の維持が含まれることがあります。

お客様は、お客様の管理する資産のうちオラクル・クラウド・サービスを活用またはオラクル・クラウド・サービスと統合されるものについて、責任を負います。これには、次も含まれます。すなわち、お客様コンテンツについて適切な情報種別を決定すること、また、オラクル・クラウド・サービスによって提供される文書化された管理手法がお客様コンテンツにとって適切であるか否かを判断すること。お客様は、データ主体から提供される情報の収集と使用に関し必要なあらゆる同意その他の法的根拠（オラクル・クラウド・サービスを提供するうえで必要となるあらゆる同意その他の法的根拠を含みます）を有しているか、または取得する必要があります。

1.10 Oracle Internal Information Security Policies

Oracle Cloud Information Security Policies は、オラクル・クラウド・サービスおよびお客様によるオラクル・クラウド・サービスの使用に適用されるセキュリティー・エリアを確立し規律するものです。オラクルの人員は、Oracle Corporate Information Security Policies、および人員の雇用または人員からオラクルへの役務提供を規律する他の一切のポリシーに従います。オラクルの情報セキュリティー・プログラム（以下「ISP」といいます）は、リスク要因（サイバーおよびセキュリティーに関する要因も含みます）を考慮したポリシー文書で構成されます。これには、付随する派生的な手順、基準およびガイドラインであってポリシーの効率的な運用に必要とされるものも含みます。オラクルの ISP は、効率的なセキュリティー管理のプラクティスおよび制御を通じ、お客様のオラクル・クラウド・サービス内でオラクルによりホストされるお客様コンテンツの機密性、完全性、プライバシー、一貫性および可用性を確保するためのものです。オラクルの ISP は、Oracle Security Oversight Committee による年次でのレビューを受けたうえで必要に応じて更新されます。

1.11 セキュリティーの内部レビューおよび実施

オラクルは、本条項に定める技術面および組織面でのセキュリティー措置の効果について、定期的なテスト、審査、評価および維持のための内部手順を採用しています。

1.12 外部レビュー

オラクルは、以下のエリアで、第三者を起用してオラクル・クラウド・サービスの独立したレビューを行うことができます（かかるレビューの適用範囲は、対象サービスおよび国により異なることがあります）。

- SOC 1（Statement on Standards for Attestation Engagements (SSAE) No 18 に基づくもの）および/または SOC 2 レポート（Trust Services Criteria に基づくもの）
- 業務および技術的管理手法の効果をレビューする他の独立した第三者のセキュリティー・テスト

かかるレビューに関連する情報が顧客に提供されることがあります。

1.13 Oracle Software Security Assurance

Oracle Software Security Assurance（OSSA）は、オラクルの製品（顧客がオンプレミスで使用するか、オラクル・クラウドを介して提供されるかは問いません）の設計、構築、テストおよび保守にセキュリティーを組み込むためのオラクルの方法論です。OSSA プログラムは、https://www.oracle.com/corporate/security-practices/assurance/に記載されています。

1.14 セキュリティー・ログ

オペレーティング・システムにおけるセキュリティー関連の活動について、ログが生成されます。システムは、デフォルトのセキュリティー活動、情報またはプログラムへのアクセス、アラートなどのシステム・イベント、コンソール・メッセージおよびシステム・エラーをログとして記録するように設定されています。オラクルは、フォレンジックの目的でインシデントに関するログをレビューします。検知された異常な活動については、インシデント管理プロセスの対象となります。セキュリティー・ログは、ネイティブ形式かつ変更なしの形式にて Security Information and Event Management システム（またはそれに相当するシステム）内に保存されたうえでオラクルの内部ポリシーに基づき保持されます。かかるログのオンラインでの保持期間は、少なくとも 1 年とします。かかるログは、オラクル・クラウド・サービスにおけるオラクルの内部セキュリティー業務のためにオラクルにより保持および利用されます。

1.15 その他のお客様のセキュリティー関連義務

お客様は、以下について責任を負います。

- お客様のリスクベース評価やビジネス要件に応じて、セキュリティーならびに運用の方針、基準および手続に関するお客様独自の包括的なシステムを実装すること。
- エンドユーザー・デバイスが、オラクル・クラウド・サービスにアクセスするためのウェブ・ブラウザー要件とネットワーク帯域幅の最小要件を満たすことを保証すること。
- オラクル・クラウド・サービスにデータをインポートまたはアップロードする前に、データやファイルのアンチウイルスおよびマルウェア・チェックが実施できるように、クライアント・デバイスのセキュリティー・コントロールを管理すること。

- お客様のポリシーとセキュリティーのベスト・プラクティスに従って、Customer-managed のアカウントを維持すること。
- さらに、お客様は、Oracle Cloud at Customer Services に対して、以下の責任を負います。
    - 十分な物理上およびネットワーク上のセキュリティー。
    - リアルタイムでの脅威のリスクを低減するとともにお客様のネットワークからお客様のオラクル・クラウド・サービスへの不正アクセスを防止するためのセキュリティー・モニタリング。これには、侵入検知システム、アクセス・コントロール、ファイアウォール、その他一切のネットワーク監視、およびお客様により管理されている一切の管理ツールが含まれます。

2. ORACLE CLOUD SERVICE CONTINUITY POLICY

2.1 オラクル・クラウド・サービスの高可用性戦略

オラクルは、対象サービスに影響を与えるインシデントが発生した場合でもサービス可用性および持続性を維持するために設計されたレジリエントなコンピューティング・インフラストラクチャー上に、オラクル・クラウド・サービスをデプロイします。オラクル・クラウド・サービスをホストするためにオラクルが維持しているデータ・センターには、バックアップ発電の設置された冗長電源およびコンポーネントがあり、オラクルは、ネットワーク・インフラストラクチャー、プログラム・サーバー、データベース・サーバー、および/またはストレージを含む 1 つ以上の層に冗長性を組み込むことがあります。

2.2 オラクル・クラウド・サービスのバックアップ戦略

オラクルは、インシデント時にデータ損失を最小限にするためにオラクルのみが利用することを目的として、オラクル・クラウド・サービスにおけるお客様のインスタンス内のお客様コンテンツのバックアップを定期的に行っています。バックアップは、オラクル・クラウド・サービスを提供しているプライマリー・サイトに保管され、保持を目的として別の場所に保管されます。バックアップは、通常、バックアップが作成された日から最低限 60 日後まで、オンラインまたはオフラインで保持されています。オラクルは、通常、お客様の代わりにお客様のデータの更新、挿入、削除または復元を行うことはありません。ただし、例外的に、かつ書面による承認を条件として、オラクルがお客様自身の行為の結果として喪失したお客様のデータの復元を支援する場合があります。

お客様自身のポリシーに基づくお客様によるバックアップの構成を可能にするオラクル・クラウド・サービスについては、お客様は、お客様コンテンツのバックアップおよびリストアの実行について責任を負います。また、お客様に対しては、災害発生時におけるお客様自身の業務の継続性を確保するための、事業継続計画を策定しておくことをお勧めします。

2.3 オラクルにおける事業継続性

オラクルは、オラクルの内部的処理に関係する計画であって災害、支障または不可抗力事由が生じた場合におけるサービス提供に対する一切の支障を最小化すること目的とするもの（以下「BC 計画」といいます）を、有効期間中にわたり常に維持するものとします。

BC 計画は、手続き、手順および管理体制を構築、文書化および実施することにより、BC 計画の発動時においても、オラクル・クラウド・サービスに適用されるセキュリティー条項が制限されることのないようにするものです。BC 計画の目的は、原因の如何にかかわらずオラクル・クラウド・サービスの継続性および保守に関するオラクルの内部的処理についてのレジリエンスなどを提供することにあります。

3. ORACLE CLOUD SERVICE LEVEL AGREEMENT

3.1 営業時間

オラクル・クラウド・サービスは、保守期間、テクニカル・アップグレード中、ならびにオラクル契約、お客様の注文および本 *Oracle Cloud Service Level Agreement* で定められている場合を除き、1 日 24 時間、週 7 日、1 年 365 日利用できるように設計されています。

3.2 サービス可用性

オラクルがお客様のオラクル・クラウド・サービスを有効化した時点から、オラクルは、99.9%のターゲット・サービス可用性レベルまたはターゲット・サービス・アップタイムを満たすよう努めます。これは、適用されるオラクル・クラウド・サービスのために Oracle Cloud Service Pillar ドキュメントに記載された条件（または当該ドキュメントで該当するオラクル・クラウド・サービスのためにオラクルが記載している他のターゲット・サービス可用性レベルもしくはターゲット・サービス・アップタイム）に準拠しています。

上記は、オラクル・クラウド・サービスの Program Documentation に記載されているお客様のネットワーク・インフラストラクチャーおよびお客様のユーザー作業環境から該当のオラクル・クラウド・サービスへのアクセスおよび利用のために必要なオラクルが推薦する最低限の技術的な構成要件を満たしていることが条件となります。

3.2.1 可用性の測定

該当するサービス期間の各暦月末の後に、オラクルは、月間測定期間内の合計時間（分単位）と一切の計画外停止時間（以下に定義します）との差分を、測定期間の合計時間数（分単位）で割り、その結果に 100 を掛けてパーセント値を求めることで、直前の月のサービス可用性レベルまたはサービス・アップタイムを測定します。

$$\left(\frac{\textit{月間の時間数（分単位）} - \textit{計画外ダウンタイムの時間数（分単位）}}{\textit{月間の時間数（分単位）}}\right) \times 100$$

1 か月間（30 日間）における時間数（分単位）＝30 日×1 日あたり 24 時間×1 時間あたり 60 分

月間の計画外時間数（分単位）＝「*計画外停止時間の定義*」の項に定義された計画外停止時間の時間数（分単位）。

例：6 月は 30 日間であることから、1 か月で 30×24×60＝43,200 分

6 月に 90 分間の計画外停止時間が発生した場合の算出式：

$$(43{,}200 - 90)/43{,}200) \times 100 = 99.8\%$$

3.2.2 可用性の報告

オラクルは、お客様の注文においてお客様により購入されたオラクル・クラウド・サービスについてのサービス可用性レベルの測定値を、セルフサービス方式にて、または測定値を依頼内容としてお客様からオラクルに提出されたサービス・リクエストを通じて、お客様に提供するものとします。

3.2.3 サービス・クレジット

お客様の注文においてお客様が購入したオラクル・クラウド・サービスのターゲット・サービス可用性レベルまたはターゲット・サービス・アップタイムが、当該対象サービスに適用される所定のターゲット・サービス可用性レベルまたはターゲット・サービス・アップタイムを下回った場合、お客様は、サービス・クレジットを受領することができます。サービス・クレジットは、お客様の購入済みオラクル・クラウド・サービスに適用される Oracle Cloud Service Pillar ドキュメントまたは Service Descriptions で定義されています。本条項の定めにかかわらず、上記よりも高額のサービス・クレジットを受領する権利が、お客様のオラクルに対する注文、または特定のオラクル・クラウド・サービスの注文に適用されるサービス仕様書に定められている場合、お客様は、お客様向けのサービス・クレジットとして最も高い額を定めた規定に基づいてサービス・クレジットを受領することができます。ただし、お客様は、同一の事案について複数の規定に基づきサービス・クレジットを受領することはできません。

3.3 計画外停止時間の定義

オラクル・クラウド・サービスは、各ホスティング設備においてレジリエントなインフラストラクチャー、冗長ネットワーク接続および電源を備えたレジリエントなコンピューティング設備にデプロイされます。

「計画外停止時間」とは、オラクル・クラウド・サービスにおける問題により、お客様の接続が妨げられた時間をいいます。計画外停止時間には、オラクル・クラウド・サービスまたはオラクル・クラウド・サービス・コンポーネントが次の原因で利用できない時間は含まれません。（i）予定された保守、（ii）オラクルの支配を超える状況その他不可抗力事由（例：お客様からの依頼により開始された停止、電気設備、ネットワーク機器、電気通信機器もしくはその他の接続機器などの非オラクル製インフラストラクチャーにより引き起こされた停止、またはセキュリティー攻撃、自然災害もしくは政治上の事象など）、（iii）お客様、お客様のユーザーまたは第三者（オラクルの代理人または業務委託先であって該当のオラクル・クラウド・サービスの実施のためにオラクルにより起用された者を除きます）の作為または不作為、および（iv）お客様のオラクル契約またはお客様の注文において許容されているオラクルによる停止。また、Oracle Cloud at Customer Services について、次に該当する停止時間その他の利用不能も、計画外停止時間には含まれません。（i）お客様のデータ・センターについてのもの（例：保守が原因である場合など）、または（ii）お客様のデータ・センターでのオラクル・クラウド・オペレーション人員に関しお客様の注文で定義されたオンサイト時間の外で生じたもの。

3.4 モニタリング

オラクルは、オラクル・クラウド・サービスの可用性およびパフォーマンスならびにインフラストラクチャーおよびネットワークのコンポーネントの運用をモニターするために、さまざまなソフトウェア・ツールを利用します。オラクルは、第三者のアプリケーションなどお客様がオラクル・クラウ

ド・サービスにおいて使用するオラクル製品ではないマネージド・コンポーネントによって発生した逸脱については、モニターまたは対応のいずれもしません。

3.4.1 モニター対象コンポーネント

オラクルは、オラクル・クラウド・サービスをサポートするハードウェアをモニターし、モニター対象のネットワーク・コンポーネント（CPU、メモリー、ストレージ、データベースその他のコンポーネントなど）に対してアラートを生成します。オラクル・クラウド・オペレーション・スタッフは、オラクルが定義したしきい値の逸脱に起因するアラートをモニターし、標準的な作業手順に従って潜在的な問題を調査して解決します。

3.4.2 お客様のモニタリング・ツールおよびテスト・ツール

オラクルは、お客様のテスト・インスタンスにおけるオラクル・クラウド・サービスについての限定的な機能テストの実施をお客様に許可します。テスト実施に関する具体的な規則は、Program Documentation に掲載されていることがあります。

オラクルは、オラクル・クラウド・サービスのセキュリティー全般の検証および改善のため、オラクル・クラウドのインフラストラクチャー、プラットフォームおよびアプリケーションについて侵入テスト、脆弱性テストおよびセキュリティー評価を定期的に実施します。Oracle Cloud Services Program Documentation には、お客様がオラクル・クラウド・サービスにおいて管理または作成するコンポーネントについてお客様が評価またはテストを実施できる時期および方法が概説されています。これには、オラクル以外のアプリケーション、オラクル以外のデータベース、その他該当のオラクル以外のソフトウェア、コード、またはデータ・スクレイピング・ツールの利用も含みます。

オラクルは、本条項のガイドラインまたは該当の Oracle Cloud Services Program Documentation に違反するいかなるツールやテクノロジーについても、お客様に対して一切の責任を負うことなく削除またはアクセスを無効化する権利を有します。

4. ORACLE CLOUD CHANGE MANAGEMENT POLICY

4.1 オラクル・クラウドの変更管理と保守

オラクル・クラウド・オペレーション部門は、オラクル・クラウド・サービスの運用上の安定性、可用性、セキュリティー、パフォーマンスおよび即時性を維持するために、クラウドのハードウェア・インフラストラクチャー、オペレーティング・ソフトウェア、製品ソフトウェア、およびオラクル・クラウド・サービスの一部としてオラクルにより提供された補助アプリケーション・ソフトウェアに対する変更を実施します。オラクルは、サービスでの適用に先立ち、変更に関するレビュー、テストおよび承認を行うための正式な変更管理手順に従います。

変更管理手順を通してなされる変更には、システムおよびサービスについての保守作業、アップグレードおよび更新ならびにお客様固有の変更が含まれます。オラクル・クラウド・サービスの変更管理手順は、変更実施中のサービス中断を最小限に抑えるように策定されています。

オラクルは、保守期間中にオラクル・クラウド・サービスの中断が必要となりうる変更には、特別な保守期間を確保します。オラクルは、アクセス量の少ない時間帯と地域特有の要件を考慮し、予定さ

れた保守期間中（当該期間についてはオラクルが事前に通知するものとします）に変更管理手順が確実に実行されるよう取り組みます。

オラクルは、保守期間の予定変更について事前に通知します。実行可能なお客様指定の変更およびアップグレードに関して、オラクルは、お客様と保守期間の調整をします。

サービス中断を引き起こすと予想される変更の場合、予定された保守のための保守期間は、サービス可用性レベル（上記「*Oracle Cloud Service Level Agreement*」を参照）の月次評価期間における計画外停止時間（分単位）には算入されません。オラクルは、これらの確保された保守期間を最小限にし、かつサービスの中断を発生させる保守作業時間を最小限にするよう、商業上合理的な努力をします。

お客様が自身で保守活動を実施できるオラクル・クラウド・サービスの場合、お客様は、オペレーティング・システムおよびその他の関連ソフトウェアの構成および保守について責任を負います。

4.1.1 クリティカル・セキュリティー保守

オラクルにおいて、オラクル・クラウド・サービスのセキュリティー保護のためにクリティカル・セキュリティー保守を実行する必要が生じることがあります。クリティカル・セキュリティー保守は、オラクル・クラウド・サービスまたはオラクル・インフラストラクチャーにおける急迫状況（例えばセキュリティー脆弱性など）のうち、緊急対応以外による対処が不可能であるものに対処するために、必要とされます。オラクルは、クリティカル・セキュリティー保守の利用の最小化に努めるとともに、合理的な範囲で、予定された保守期間外でのサービス中断が必要となる一切のクリティカル・セキュリティー保守について、24 時間前に通知するよう努めます。

4.1.2 データ・センターの移行

オラクルにより必要と判断された場合、または災害復旧の場合には、オラクルは、オラクルの維持するデータ・センターにデプロイされているお客様のオラクル・クラウド・サービスを、同一のデータ・センター地域内の異なる本番データ・センターに移行する場合があります。災害復旧以外の目的のデータ・センターの移行については、オラクルは、少なくとも 30 日前にお客様に通知します。

4.2 ソフトウェアのバージョン管理

4.2.1 ソフトウェアの更新

オラクルは、いずれのオラクル・クラウド・サービスの顧客に対しても、当該オラクル・クラウド・サービスのソフトウェア・バージョンを、当該オラクル・クラウド・サービスのサポート対象リリースとしてオラクルにより指定されているソフトウェア・バージョンと同一の最新の状態に維持することを求めます。ソフトウェアの更新は、そのオラクル・クラウド・サービスに対するバージョンの最新性を維持するために必要とされるものです。*Oracle Cloud Service Continuity Policy*、*Oracle Cloud Service Level Agreement* および *Oracle Cloud Support Policy* も含め、本 Delivery Policies に基づくオラクルの義務は、お客様がご自身のオラクル・クラウド・サービスについて現在のサポート対象バー

ジョンを維持することに依存します。オラクルは、古いバージョンを実行した結果として生じるオラクル・クラウド・サービスのパフォーマンス、機能性、可用性またはセキュリティーの問題に対する責任を負いません。

4.2.2 End of Life

オラクルは、オラクル・クラウド・サービスのサポート対象リリースのみをホストし、サポートします。オラクル・クラウド・サービスの他のバージョンはすべて、「End of Life（EOL）」であるとみなされます。お客様は、特定のバージョンの EOL に先立ち、最新バージョンへのオラクル・クラウド・サービスの更新を完了することが必要となります。お客様は、オラクル・クラウド・サービスのバージョンの EOL に先立つ更新を完了しなかった場合には、オラクルにより自動的に更新が実施されるかまたはオラクル・クラウド・サービスが停止される場合があることを了承します。オラクル・クラウド・サービスのバージョンが EOL となり、オラクルが更新されたバージョンを利用可能としない状況においては、オラクルは、後継のオラクル・クラウド・サービスを指定し、お客様がそれに移行することを要請する場合があります。

5. ORACLE CLOUD SUPPORT POLICY

本 *Oracle Cloud Support Policy* に記載されているサポートは、オラクル・クラウド・サービスのみに適用され、お客様の注文に基づき当該オラクル・クラウド・サービスの一部としてオラクルにより提供されます。オラクルは、オラクル・クラウド・サービスについてオラクルを提供者とする追加のサポート・サービスを提供することがあり、お客様は当該サポート・サービスを追加料金にて注文することができます。

5.1 オラクル・クラウド・サポート条件

5.1.1 サポート料金

お客様の注文に基づいてお客様によりオラクル・クラウド・サービスに対して支払われる料金には、本 *Oracle Cloud Support Policy* に記載されているサポートが含まれています。お客様が購入する追加オラクル・サポート・サービスには、追加料金が適用されます。

5.1.2 サポート期間

オラクル・クラウド・サポートは、オラクル・クラウド・サービス開始日より利用可能となり、対象サービスの満了日または終了日をもって終了します（以下「サポート期間」といいます）。オラクルは、かかるサポート期間終了後においては、本 Oracle Cloud Support Policy に記載されているサポートを提供する義務を負いません。

5.1.3 技術担当者

お客様の技術担当者は、オラクル・クラウド・サービスに対するオラクル・サポートに関するお客様とオラクルとの間の唯一の連絡窓口となります。当該技術担当者は、少なくとも初期の基本的なトレーニングを受けていなければならないとともに、必要に応じて特定の役割または導入フェーズ、特別なサービス/製品の使用方法、および移行に適した補足トレーニングを受けていなければなりません。システム上の問題の解決を促進するため、ならびにサービス・リクエストの内容の分析および解決についてオラクルを支援するため、お客様の技術担当者は、オラクル・クラウド・サービスに精通していなければなりません。サービス・リクエストを提出する際、お客様の技術担当者は、問題の診断お

よびトリアージについてオラクルを支援するために、発生した問題について根本的に理解しているとともに、問題を再現する能力を有している必要があります。オラクル・クラウド・サービスに対するオラクル・サポートが中断することがないよう、お客様の技術担当者が変更になった場合には、直ちにオラクルに連絡する必要があります。

5.1.4 オラクル・クラウド・サポート

オラクル・クラウド・サービスに対するオラクル・サポートは以下により構成されます。

- オラクル・クラウド・サービスの問題または不具合の診断
- 関連するサービス仕様書に記載されるとおり、オラクル・クラウド・サービスがすべての主要な点において機能するように、オラクル・クラウド・サービスで報告された検証可能なエラーを解決するための合理的な範囲の商業的努力
- *Oracle Cloud Change Management Policy*（上記を参照のこと）に記載される変更管理の作業中のサポート
- 24x7x365（1日24時間/週7日/年365日体制）でのテクニカル・サービス・リクエストの支援
- 24x7x365（1日24時間/週7日/年365日体制）でのアクセスが可能な、オラクルにより指定されたクラウド・カスタマー・サポート・ポータル、およびサービス・リクエストを登録するためのライブ電話サポート
- コミュニティー・フォーラムへのアクセス
- 現地国におけるオラクルの通常営業時間内（午前8時～午後5時）の技術的な内容以外のカスタマー・サービス

5.2 オラクル・クラウド・カスタマー・サポート・システム

5.2.1 オラクル・クラウド・カスタマー・サポート・ポータル

オラクルは、お客様により取得されたオラクル・クラウド・サービスについて、注文に基づき、当該オラクル・クラウド・サービス向けに指定されたクラウド・カスタマー・サポート・ポータル（サポート・ポータル）を通じて、サポートを提供します。オラクル・クラウド・サポートおよびポータル（これらにより提供されることのある対象サービスのあらゆる部分も含みます）は、お客様の注文の一部となっている場合もありますが、オラクル・クラウド・サービスの提供内容ではなく、グローバルに提供されることのあるものであり、それに対するアクセスについては、該当のポータル・ウェブサイトに掲載されている使用条件により規律されることになります（かかる使用条件は、変更されることがあります）。かかるポータルにおいてお客様による情報のアップロードが可能である場合、お客様は、政府発行の身分証番号、健康情報、財務情報、支払カード情報、管理対象非機密情報その他のセンシティブな個人情報がお客様およびお客様のユーザーのいずれからも、当該ポータルに提出されることのないようにする責任を負うものとします。ただし、サポート・ポータルにおける使用条件により、またはお客様における該当のクラウド・サービス注文により別段の明示的な許可がなされている場合は、この限りではありません。サポート・ポータルにアクセスできるのは、オラクル・クラウド・サービスについてのお客様における指定技術担当者その他の認定ユーザーに限られます。該当の場合、サポート・ポータルにおいて、サポートの詳細がお客様の指定技術担当者に提示されるとともに、オラクル・クラウド・サービスについてオラクル・サポートの使用が可能となります。お客様のサービス・リクエストに関係するサポート上の通知およびアラートは、サポート・ポータルに掲載されます。

5.2.2 ライブ電話サポート

お客様の技術担当者は、オラクルのサポート・ウェブサイト（https://www.oracle.com/support/contact.html）で参照できる電話番号および連絡先を介して、ライブ電話サポートを利用することができます。

5.3 重要度の定義

クラウド・サービスに関するサービス・リクエストは、サポート・ポータルを通じて、お客様の技術担当者が提出するものとします。サービス・リクエストの重要度は、お客様からの提供情報に基づいて割り当てられるものであり、以下に規定する重要度の定義に基づくものとします。

5.3.1 重要度 1（クリティカルな停止）

オラクル・クラウド・サービスのお客様による本番利用が停止しているか、またはお客様において合理的に業務を継続することができない程度に当該利用が深刻な影響を受けている。サービスが完全に停止している。さらに、影響を受ける業務運用がビジネス上ミッション・クリティカルであり、緊急を要する。重要度 1 のサービス・リクエストには、次の特徴が 1 つ以上含まれます。

- データが損傷
- 文書に記載されたクリティカルな機能が利用不能
- サービスが長期間にわたり停止し、リソースまたは応答に許容不能なまたは際限のない遅延が発生
- サービスがクラッシュし、何度か再起動を試みた後もクラッシュする状態が継続
- サービスの機密性、完全性または可用性に影響を及ぼす可能性のあるセキュリティー・インシデント

オラクルは、重要度 1 のサービス・リクエストについては 15 分以内に応答するよう合理的な努力をします。重要度 1 サービス・リクエストの対処にオラクルが取り組んでいる全期間にわたり、お客様は、お客様の技術担当者を 1 日 24 時間/週 7 日体制にて対応可能な状態に置く旨に、同意します。オラクルは、重要度 1 サービス・リクエストが解決するか、妥当な回避方法が用意されるか、承認済みのアクション・プランが用意されるか、またはお客様における 1 日 24 時間/週 7 日体制の担当窓口が機能しなくなるまで間、1 日 24 時間/週 7 日間対応で取り組みます。お客様は、データ収集、テストおよび修正適用を支援するために、オラクルに対して 1 日 24 時間週 7 日間対応の技術担当者を整備する必要があります。お客様は、重要度 1 である事態に際してオラクルから必要なリソース配分が得られるよう、オラクルに対して重要度分類を慎重に提示する必要があります。

5.3.2 重要度 2（重大な障害）

サービスに深刻な障害が生じている状態。容認できる回避策がなく、オラクル・クラウド・サービスの重要な機能が利用できないが、限定された方法での業務運用は継続可能である。

5.3.3 重要度 3（技術的な問題）

サービスに軽微な支障がある状態。影響は不便な程度であるが、機能を修復するための回避策が必要な場合がある。

5.3.4 重要度 4（一般的なガイダンス）

お客様からはオラクル・クラウド・サービスに関する情報、機能拡張またはドキュメントによる説明を求めるが、当該サービスの運用に影響がない状態。サービス上の障害は生じていない状態。

5.4 サービス・リクエストの重要度レベルの変更

5.4.1 初期の重要度レベル

オラクルは、サービス・リクエストが作成された時点で、上記の重要度の定義および/またはお客様からの提供情報に基づき当該サービス・リクエストの初期の重要度レベルを記録します。サービス・リクエストが作成され次第、オラクルは、まず、当該サービス・リクエストを発生させた不具合を解決することに焦点を当てます。サービス・リクエストの重要度レベルは、以下のとおり調整される場合があります。

5.4.2 サービス・リクエスト・レベルの引き下げ

根本的な不具合に対する作業の進捗に応じて、不具合の重要度が、オラクル・クラウド・サービスの稼働に対する現在の影響度に基づき現在割り当てられている重要度よりも低くなった場合、重要度は、現在の影響度を最も適切に反映する重要度へ引き下げられます。

5.4.3 サービス・リクエスト・レベルの引き上げ

サービス・リクエストの処理中に、オラクル・クラウド・サービスの本番稼働に対する現在の影響度に基づき現在割り当てられている重要度よりも高い重要度を不具合に割り当てる必要が生じた場合、重要度は、現在の影響度を最も適切に反映する重要度へ引き上げられます。

5.4.4 重要度の定義の遵守

お客様は、重要度の割当ておよび調整が、オラクル・クラウド・サービスの本番稼働に対する現在の影響度に基づいて正確であることを保証するものとします。

5.5 サービス・リクエストのエスカレーション

お客様によりエスカレーションされるサービス・リクエストについて、オラクルのサポート・アナリストは、エスカレーションの管理を担当するオラクル・サービス・リクエスト・エスカレーション・マネージャーと連携します。オラクル・サービス・リクエスト・エスカレーション・マネージャーは、お客様と協力して、アクション・プランを策定し、適切なオラクルのリソースを割り当てます。サービス・リクエストを発生させた不具合が未解決のままになっている場合、お客様は、サービス・リクエスト内容をレビューし、オラクル・サービス・リクエスト・エスカレーション・マネージャーに連絡し、必要に応じてそれをオラクル内の次のレベルにエスカレーションするよう要請することができます。エスカレーションされたサービス・リクエストの解決を容易にするために、お客様は、当該サービス・リクエストがエスカレーションされたオラクル内のレベルと同レベルの担当者を、お客様の組織内に配置する必要があります。

6. ORACLE CLOUD SUSPENSION AND TERMINATION POLICY

6.1 オラクル・クラウド・サービスの終了

オラクル・クラウド・サービスのサービス期間終了から 60 日間、または該当する場合は、お客様が Pay as You Go 方式で購入したクラウド・サービスの利用をお客様が終了し、関連するサービス期間終了から 60 日間、オラクルは、お客様によるデータ回収を目的として、セキュアなプロトコルを介し、かつ構造化された機械可読形式のフォーマットにて、オラクル・クラウド・サービスに存在するお客様コンテンツを利用可能にするか、またはサービス・システムをアクセス可能な状態に維持します。

オラクル・クラウド・サービスの無料トライアルおよびパイロットに関し、オラクルは、当該トライアルまたはパイロットの終了後 30 日間にわたり、お客様コンテンツを利用可能な状態にします。この回収期間中、オラクルの Cloud Service Level Agreement は適用されず、いかなる本番業務にもサービス・システムを使用することはできません。オラクルには、この回収期間後は、お客様コンテンツを保持する義務は一切ないものとします。

お客様がお客様コンテンツについてアクセスまたはコピーをするためにオラクルの支援を必要とする場合には、お客様は、サポート・ポータルにおいてサービス・リクエストを作成する必要があります。

オラクルによるデータ回収および関連する支援は、お客様コンテンツを保管しないオラクル・クラウド・サービスには適用されません。お客様は、かかるオラクル・クラウド・サービスがデータ保存の面で別個のオラクル・クラウド・サービス（Storage Cloud Service または Database Cloud Services など）に依存するものである場合においては、データ回収が可能となるよう終了対象のオラクル・クラウド・サービスの終了時まで当該別個のオラクル・クラウド・サービスが有効期間内である状態を確保する責任、またはサービス期間の終了に先立って本番オラクル・クラウド・サービスが有効である間に他の何らかの態様にて適切な措置を講じることによりお客様コンテンツのバックアップもしくは個別保存を行う責任を、負うものとします。

回収期間の満了後、オラクルは、オラクル・クラウド・サービスからお客様コンテンツを削除します。ただし、適用法による別段の義務付けがある場合は、この限りではありません。

Oracle Cloud at Customer Services については、お客様は、適切な使用による合理的な消耗を前提とし、オラクルが提供したあらゆる Oracle Cloud at Customer Services 関連のハードウェア・コンポーネント（ゲートウェイ機器も含みます）を、正常に使用できる状態で、かつ Oracle Cloud at Customer Services の開始時と同じ状態で、オラクルが回収できるようにする必要があります。

7 対象サービスの使用

お客様は、取得済みのオラクル・クラウド・サービスそれ自体および当該クラウド・サービスから受ける便益についてのアクセスおよび使用が、Oracle Global Trade Compliance Policy（記載場所：https://www.oracle.com/corporate/security-practices/corporate/governance/global-trade-compliance.html）に基づく国におけるユーザーによりまたは当該ユーザーのために行われる状況を、確保する責任を負います。