ORACLE
Cloud Infrastructure

National Cyber Security Centre (NCSC) Cloud Security Principles - Oracle Cloudでの実装

Oracle Cloud Infrastructure

2019年1月

ORACLE

目次

I. クラウド・セキュリティ原則の使用の概要

National Cyber Security Centre (NCSC)ガイダンスは、クラウド・サービスを評価する際に検討する14の必須セキュリティ原則をまとめたものであり、これが組織にとってなぜ重要になり得るかについての背景を説明しています。

お客様は、どのNCSCクラウド・セキュリティ原則が重要であるか、またこの原則を確実に実装する必要があるとすればどの程度必要かを決定する必要があります。

クラウド・サービスのプロバイダは、自身のオファリングをコンシューマに紹介する際、NCSCクラウド・セキュリティ原則を検討する必要があります。その結果、コンシューマは、どのサービスが自らのニーズに即しているかについて十分な情報を得たうえで選択できます。

このホワイト・ペーパーでは、読者およびお客様に次の項目に関する知識を提供することを目的としています。

- セキュリティ、機密性および可用性に関連するOracle Cloud Infrastructureの管理的、物理的および技術的な予防手段がNCSCクラウド・セキュリティ原則といかに一致しているか。
- NCSCガイダンスのセキュリティおよび実装の責任が、Oracle Cloud Infrastructure (クラウド・サービスのプロバイダ)とお客様(クラウド・サービスのコンシューマ)間でどのように共有されているか。
- Oracle Cloud Infrastructureサービスを使用して、情報セキュリティ・リスク管理およびNCSCクラウド・セキュリティ原則ガイダンスの実装にお客様がどのように取り組むことができるか。

II. Oracle Cloud Infrastructureサービスの概要

Oracle Cloud Infrastructureは、パブリック・クラウドの順応性および実用性と、オンプレミス・インフラストラクチャの詳細なコントロール、セキュリティおよび予測性を組み合せて、高パフォーマンスと高可用性を備えたコスト効果の高いInfrastructure as a Service (IaaS)を提供します。

結果として、お客様は、柔軟なセルフサービスのPay-As-You-Goベア・メタル・クラウド・サーバーをプロビジョニングできます。オラクルの次世代インフラストラクチャでは、ベア・メタル・サーバーを、仮想マシン(VM)からエンジニアド・システムまであらゆるクラスのシステムと同時に実行することも可能になります。

サービスには次のものがあります。

- Archive Storage
- Audit
- Block Volumes
- Cloud Access Security Broker (CASB) Cloud Service
- Compute
- Container Engine for Kubernetes
- Data Transfer
- Database
- Database - 2ノードReal Application Clusters (RAC)
- Database - Autonomous Data Warehouse
- Database - Autonomous Transaction Processing
- Database - Exadata
- Distributed Denial of Service (DDoS) Protection
- Domain Name System (DNS)
- Email Delivery
- FastConnect
- File Storage Service (FSS)
- Identity and Access Management (IAM)
- Key Management Service (KMS)
- Load Balancing
- Object Storage
- Registry
- Storage Gateway
- Virtual Cloud Network (VCN)

Oracle Cloud Infrastructureの本部は米国のワシントン州シアトルに、オペレーション・コマンド・センターは米国のワシントン州シアトルおよびアイルランドのダブリンにあります。上記のサービスをサポートするハードウェアを格納しているデータ・センターは、米国のバージニア州アッシュバーン、米国のアリゾナ州フェニックス、ドイツ連邦共和国のフランクフルト・アム・マインおよび英国のロンドンにあります。

III. National Cyber Security Centre (NCSC)のクラウド・セキュリティ原則およびOracle Cloud Infrastructure

お客様によるOracle Cloud Infrastructureサービスの評価を支援するために、National Cyber Security Centre (NCSC)クラウド・セキュリティ原則を補完するガイダンスであるNCSCの『*Having confidence in cyber security*』に含まれているトピックに次のステートメントで対処しています。

1. サプライヤからの契約責任

オラクルには、条件、サービスの説明およびお客様へのクラウド・サービスの提供を規定した標準契約およびポリシーがあります。オラクルのHosting and Delivery PoliciesおよびPillar Documentsは、オラクルがセキュリティ、変更管理およびバックアップにどのように対応しているかなど、オラクルがクラウド・サービスをどのように提供しているかについて説明しています。

2. 独立した第三者による検証

Oracle Cloud Infrastructureは、独立した監査人および査定人に依頼し、データ保護法、規制および業界標準に関連するセキュリティ、機密性および可用性のコントロールをテストし、それに関する評価を提供しています。

オランダの認定評議会(Raad voor AccreditatieまたはRvA)によって認定された認証機関であるErnst & Young CertifyPoint (EYCP)は、Oracle Cloud Infrastructureの情報セキュリティ・マネジメント・システム(ISMS)を監査し、認定します。EYCPは、まず、2017年にISO/IEC 27001:2013証明書を発行しました。EYCPは、Oracle Cloud InfrastructureのISMSの年次調査監査を実行し、国際標準への準拠を検証しています。

QG Business Solutionsによって認定されている認証機関であるSecarma Limitedは、National Cyber Security Centre (NCSC)によって公布されたCyber Essentialsスキームに従い、Oracle Cloud Infrastructureを評価し認定します。Secarmaは、まず、2018年にCyber Essentials Plus証明書を発行し、年次評価を実行して、スキームの遵守が継続していることを検証しています。

Ernst & Young LLPは、米国公認会計士協会(AICPA)の保証業務基準書18 (SSAE 18)、および国際監査・保証基準審議会(IAASB)の国際保証業務基準3000 (ISAE 3000)に従い、Oracle Cloud Infrastructureを6か月ごとに調査し、対象のInfrastructure as a Service (IaaS)に関連するセキュリティ、機密性および可用性に関するコントロールについて、AICPAトラスト・サービス原則と基準(Trust Services Principles and Criteria)を網羅するSOC 2 (Service Organization Control 2) Type 2認証を発行します。

Schellman & Company, LLCは、クレジット・カード業界データ・セキュリティ基準(PCI DSS)に従い、年に1回Oracle Cloud Infrastructureを評価します。サービス・プロバイダ向けのOracle Cloud InfrastructureのAttestation of Compliance (AOC)は、対象のIaaSに関して、すべての12 PCI DSS要件を網羅しています。

3. 広く認められた適切な基準への準拠

Oracle Cloud InfrastructureのISO/IEC 27001:2013証明書は、その情報セキュリティ・マネジメント・システム(ISMS)を網羅しています。ISMSは、米国のワシントン州シアトルにあるOracle Cloud Infrastructureの本部から集中的に管理されます。対象のアプリケーション、システム、ユーザーおよびプロセスは、米国のワシントン州シアトル、アイルランドのダブリン、および北米と欧州、中東とアフリカなどのリージョンに拠点を置くチームによってグローバルに実装、運用されます。

Oracle Cloud InfrastructureのCyber Essentials Plus証明書は、認定された認証機関のサイバー・セキュリティ対策に対する第三者による検証を提供します。National Cyber Security Centre (NCSC)は、Cyber Essentialsスキームを策定し、一般的なインターネットベースの脅威によるリスクを緩和するためにすべての組織が実装する必要がある基本的なコントロールを明確化しています。このスキームの保証フレームワークは、整備されている技術的なコントロールをお客様および他の利害関係者に実際に示すための仕組みを組織に提供します。

Oracle Cloud InfrastructureのSOC 2 Type 2認証は、セキュリティ、機密性および可用性に関連するコントロールの設計の有効性および運用の有効性についての外部の監査人の評価を提供します。Oracle Cloud Infrastructureの対象サービスの説明、コントロールのテストおよびテスト結果がレポートに記載されており、これにより、Oracle Cloud Infrastructureのサービス・コミットメントおよび要件が適切なAICPAトラスト・サービス原則と基準に基づいて達成されていることをお客様に保証します。

Oracle Cloud Infrastructureは、全体のセキュリティ戦略の一部として、PCI DSSを通常の業務に組み入れています。このため、Oracle Cloud Infrastructureは、セキュリティ・コントロールの有効性を継続的に監視でき、年1回のPCI DSSアセスメントの間においてもPCI DSSに準拠した環境を維持するように設計されています。

4. 独立した検査機関がコントロールの実装を検証

Oracle Cloud Infrastructureは、独立した第三者機関に依頼し、パブリックIPアドレスの範囲の外部脆弱性検査を定期的に実行しています。また、Oracle Cloud Infrastructureは、非パブリックIPアドレスの範囲の定期的な内部脆弱性検査の他、パブリックと非パブリックの両方のIPアドレス範囲の内部および外部の侵入テストを実行する、情報セキュリティ専門の資格を持ったスタッフも擁しています。

5. セキュリティ・アーキテクチャのレビュー

オラクルのCorporate Security Architectは、社内の情報セキュリティの技術的な方向性の策定を支援し、オラクルの情報セキュリティの目標を推進する情報セキュリティ・ソリューションおよびアイデンティティ管理ソリューションの導入をオラクルのIT部門および事業部門に対して促します。Corporate Security Architectは、Global Information Security、Global Product Securityおよび開発のセキュリティ・リードと連携して、企業セキュリティ・アーキテクチャのロードマップを開発、検討および実装します。

Corporate Security Architectureは、多様なプログラムを管理し、オラクルのオペレーション、サービス、クラウドおよびその他のすべての事業の責任を負うリーダーおよび運用セキュリティ・チームと連携するための複数の方法を活用します。オラクルのアーキテクチャのセキュリティを管理するためのプログラムの例として、Corporate Security Solution Assurance Process (CSSAP)があります。
CSSAPは、Corporate Security Architecture、Global Information Security、Global Product Security、Oracle Global ITおよびオラクルのIT組織によって開発された、包括的な情報セキュリティ・マネジメント・レビューを提供するセキュリティ・レビュー・プロセスです。

Oracle CSSAPは、プロジェクトのライフサイクルを通じて適切なレビューを実行することで、革新的なクラウド・ソリューションおよび企業アプリケーションの提供の加速化を促進します。プロジェクトは次のレビューにより調整されます。

1. **事前レビュー**: 各事業部のリスク管理チームが、承認済のテンプレートを使用して、各プロジェクトの事前アセスメントを実行する必要があります。
2. **CSSAPレビュー**: セキュリティ・アーキテクチャ・チームが、提出された計画をレビューし、技術的なセキュリティ設計のレビューを実行します。
3. **セキュリティ・アセスメント・レビュー**: リスク・レベルに基づいて、システムおよびアプリケーションは、本番使用の前に、セキュリティ検証テストを受けます。

Oracle Software Security Assurance (OSSA)は、製品開発のライフサイクルのすべての段階にわたり、製品がお客様によってオンプレミスで使用されるのか、Oracle Cloudを通じて提供されるのかに関係なく、製品の設計、構築、テストおよびメンテナンスにセキュリティを組み込むオラクルのメソドロジです。オラクルの目標は、オラクルの製品が、最もコスト効果の高い所有経験を提供するだけでなく、お客様がセキュリティ要件を満たせるように、その支援となることです。

IV. National Cyber Security Centre (NCSC)のクラウド・セキュリティ原則およびOracle Cloudでの実装に関連するドキュメント

NCSCのクラウド・セキュリティ原則についての完全なガイドについては、次のドキュメントを参照してください。

- Implementing the Cloud Security Principles

次のOracle Cloud Infrastructureドキュメントは、セキュリティ機能およびベスト・プラクティスに関する情報を含む、各サービスの構成および管理についての技術的な説明およびガイダンスを提供します。これらの情報は、Oracle Cloud Infrastructureのコントロールおよび機能をNCSCのクラウド・セキュリティ原則にマッピングする次の第5項で使用されます。

- Oracle Cloud Infrastructureドキュメント
  - 主な概念および用語
  - セキュリティ・ガイド
  - セキュリティ機能
  - セキュリティ・ベスト・プラクティス

オラクルは、オラクルの内部オペレーションおよびサービスのお客様へのプロビジョニングのためのセキュリティ、安全性およびビジネスの継続性に関連するすべての機能を包含する企業セキュリティ・プラクティスを保有しています。これには、一連の内部情報セキュリティ・ポリシーの他、様々なサービスに適用される様々な顧客対応のセキュリティ・プラクティスが含まれます。

Oracle Cloud Security Practicesは、Oracle Cloudでホストされている、またはクラウド・サービスの提供時にアクセスされる(あるいはその両方の)お客様データおよびシステムの機密性、完全性および可用性を保護するために設計されたオラクルのコントロールを説明しています。この情報は、次の第5項でも使用され、Oracle Cloud Infrastructureのコントロールと機能をNCSCクラウド・セキュリティ原則と併せて示しています。

詳細は、次のドキュメントを確認してください。

- Oracle Corporate Security Practices

Oracle Cloud Infrastructureは、Infrastructure as a Service (IaaS)製品であり、セキュリティの責任は、Oracle Cloud Infrastructureとお客様の間で共有されます。

Oracle Cloud Infrastructureでワークロードを安全に実行するには、お客様はそのセキュリティおよびコンプライアンスの責任を認識している必要があります。目的をもって、オラクルはクラウド・インフラストラクチャおよびオペレーションのセキュリティを提供し(クラウド・オペレータのアクセス制御、インフラストラクチャ・セキュリティ・パッチ適用など)、お客様は自身のクラウド・リソースを安全に構成する責任を負います。

詳細は、次のドキュメントを確認してください。

- Oracle Cloud Infrastructure Security

同様に、プライバシ・コンプライアンスも、Oracle Cloud Infrastructureとお客様の間での共同責任です。次のドキュメントは、お客様が一般データ保護規則(GDBR)要件を満たす際に、Oracle Cloud Infrastructureの特性や機能がどのように役立つかを説明しています。

- Oracle Cloud Infrastructure and the GDPR

オラクルには、条件、サービスの説明およびクラウド・サービスの提供を規定した標準契約およびポリシーがあります。詳細は、次のドキュメントを確認してください。

- Oracle’s New Data Processing Agreement for Cloud Services
- Oracle Cloud Services Contracts
- Cloud Services Hosting and Delivery Policies

V. NCSCクラウド・セキュリティ原則: お客様の考慮事項およびOracle Cloud Infrastructureの実装

次の項は、NCSCが説明している14の各クラウド・セキュリティ原則の詳細な内容を示しています。

お客様の考慮事項とOracle Cloud Infrastructureの実装の両方に関する情報が、各原則に対して詳細に示されており、次の領域にまとめられています。

- ***クラウド・セキュリティ原則の名称および説明***: NCSCによって定義されています。
- ***考慮事項***: NCSCガイド『*Implementing the Cloud Security Principles*』内で、これらの考慮事項は、ユーザー(お客様)がクラウド・サービスを分析および使用する際に自信を持てるという"目標(goal)"として定義されています。
- ***Oracle Cloud Infrastructureのコントロールまたは機能***: 各クラウド・セキュリティ原則の特質に固有のセキュアなアーキテクチャを実現する、様々なプロセス、セキュリティ・コントロール、内部標準およびユーザー(お客様)に提供される追加機能の詳細。

指定された各クラウド・セキュリティ原則の考慮事項に応じて、Oracle Cloud Infrastructureコントロールまたは機能は、セキュリティ機能が実装されているサービス(該当する場合)に重点を置きます。

クラウド・セキュリティ原則1: 転送中のデータの保護

ネットワーク転送中のデータは、改ざんおよび傍受に対し適切に保護される必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
お客様は次の方法を考慮する必要があります。 - 転送中のデータが、お客様のエンドユーザー・デバイスとサービス間でどのように保護されるか。 - 転送中のデータが、サービス内で内部的にどのように保護されるか。 - 転送中のデータが、サービスと他のサービス間でどのように保護されるか(例: APIが公開されている場合)。	Oracle Cloud Infrastructureは、転送中のデータに対する複数の暗号化形式を提供します。 **API(Application Programming Interface)暗号化** すべてのOracle Cloud InfrastructureのAPI (Application Programming Interface)リクエストは、HTTPSおよびSSLプロトコルTLS 1.2をサポートする必要があります。 **仮想プライベート・ネットワーク(VPN)** Oracle Cloud Infrastructureは、IPSec仮想プライベート・ネットワーク(VPN)のトンネル・モードをサポートしています。各Oracle IPSec VPNは、静的ルートを使用してトラフィックをルーティングする複数の冗長IPSecトンネルで構成されます。Border Gateway Protocol (BGP)は、Oracle IPSec VPNではサポートされていません。 **プライベート接続** Oracle Cloud Infrastructure FastConnectは、お客様のデータ・センターとOracle Cloud Infrastructure間で専用のプライベート接続を提供します。FastConnectは、高帯域幅のオプションを提供し、インターネットベースの接続と比較して、より信頼性が高く一貫したネットワーキング・エクスペリエンスを提供します。 FastConnectでは、プライベート・ピアリング、パブリック・ピアリングまたは両方の使用を選択できます。 • プライベート・ピアリング: 既存のインフラストラクチャをOracle Cloud Infrastructure内の仮想クラウド・ネットワーク(VCN)に拡張します(例: ハイブリッド・クラウドまたはリフト・アンド・シフト・シナリオの実装)。コネクション全体での通信には、IPv4プライベート・アドレス(通常、RFC 1918)が使用されます。

クラウド・セキュリティ原則1: 転送中のデータの保護

ネットワーク転送中のデータは、改ざんおよび傍受に対し適切に保護される必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	• パブリック・ピアリング: インターネットを使用しないOracle Cloud Infrastructure内のパブリック・サービスへのアクセス。たとえば、Object Storage、Oracle Cloud Infrastructureコンソールおよび API、またはお客様のVCNのパブリック・ロード・バランサなどです。接続間の通信には、IPv4パブリックIPアドレスが使用されます。FastConnectがない場合、パブリックIPアドレスへのトラフィックはインターネット上でルーティングされます。FastConnectがある場合、そのトラフィックはプライベートの物理接続上で移動します。 お客様のコンピュートおよびストレージ・リソースのすべては、お客様が構成し制御するVCNの中に含まれます。VCNは、ソフトウェア定義ネットワークであり、お客様がそのワークロードの実行に使用するオンプレミスの物理ネットワークに類似しています。VCNセキュリティ・アーキテクチャの編成には、次のようなタスクが含まれます。 • ネットワーク・セグメンテーションのためのVCNサブネットの作成 • VCNセキュリティ・リストを使用した、VCNおよびロード・バランサ・ファイアウォールの編成 • 高可用性およびTLSのためのロード・バランシングの使用 • VCN外部接続のタイプが、インターネット、オンプレミス・ネットワーク、ピアリング済VCNまたはこれらの組合せのいずれであるかの決定 • 仮想ネットワーク・セキュリティ・アプライアンスの使用(たとえば、次世代ファイアウォール、ID) • DNSゾーンおよびマッピングの作成。ロード・バランサにおける重要なセキュリティ考慮事項は、お客様のTransport Layer Security (TLS)証明書を使用した、お客様のVCNへのTLS接続の構成です。

クラウド・セキュリティ原則1: 転送中のデータの保護

ネットワーク転送中のデータは、改ざんおよび傍受に対し適切に保護される必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	お客様のVCNは、サブネットにパーティション化でき、それぞれは可用性ドメインにマップされます。プライベート・サブネット内のインスタンスは、パブリックIPアドレスを持てません。パブリック・サブネット内のインスタンスは、オプションとして、お客様の裁量でパブリックIPアドレスを持つことができます。 **セキュリティ・リスト** セキュリティ・リストは、ステートフルおよびステートレス・ファイアウォール機能を提供し、お客様のインスタンスへのネットワーク・アクセスを制御します。セキュリティ・リストはサブネット・レベルで構成され、インスタンス・レベルで実施されます。複数のセキュリティ・リストをサブネットに適用できます。ネットワーク・パケットは、セキュリティ・リスト内のいずれかのルールと一致する場合に許可されます。 ゲートウェイによって、VCN内のリソースとVCN外の宛先が通信できます。ゲートウェイには次が含まれます。 • **インターネット・ゲートウェイ:** インターネット接続用(パブリックIPアドレスを含むリソース用) • **NATゲートウェイ:** 受信インターネット接続へのリソースの公開なしのインターネット接続用(プライベートIPアドレスを含むリソース用) • **動的ルーティング・ゲートウェイ(DRG):** VCNリージョンの外のネットワークへの接続用(たとえば、IPSec VPNまたはFastConnectによるオンプレミス・ネットワーク、または別のリージョンのピアリング済VCN) • **サービス・ゲートウェイ:** Object StorageなどのパブリックOracle Cloud Infrastructureサービスへのプライベート接続用 • **ローカル・ピアリング・ゲートウェイ(LPG):** 同じリージョン内のピアリング済VCNへの接続

クラウド・セキュリティ原則1: 転送中のデータの保護

ネットワーク転送中のデータは、改ざんおよび傍受に対し適切に保護される必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	ルート表は、お客様のVCNのサブネットからVCNの外の宛先にトラフィックをルーティングする方法を制御します。ルーティング・ターゲットは、VCNゲートウェイまたはVCN内のプライベートIPアドレスとなります。 詳細は、次を参照してください。 • Virtual Cloud Network Overview and Deployment Guide • NAT Instance Configuration • Deploying VPN IPSec Tunnels with Cisco ASA/ASAv VTI on Oracle Cloud Infrastructure • Bastion Hosts: Protected Access for Virtual Cloud Networks

クラウド・セキュリティ原則2: 資産の保護とレジリエンス

ユーザー・データ、保存または処理する資産は物理的な改ざん、損失、損害または占拠に対して保護される必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
お客様は次を考慮する必要があります。 - どの国でデータが格納、処理および管理されるか。 - お客様のクラウド・サービスの使用が、関連する法律(例: データ保護法2018および一般データ保護規則)の遵守にどのように影響するか、およびサービス・プロバイダが運用している法域が許容可能かどうか。	**管轄のコントロール** データ管理者としての立場では、お客様は、どのリージョンまたは可用性ドメインにサービスをデプロイし、そのデータをどこに格納するかを決定します。 データの処理者としての立場では、Oracle Cloud Infrastructureはお客様のデータ主体とは直接の関係はなく、お客様がデータ主体から収集したデータへのインサイトも保有しません。 データ保護原則およびコンプライアンスの詳細は、『Oracle Cloud Infrastructure and the GDPR』を参照してください。 **データ・センターの保証** コロケーション施設は、自らのISO/IEC 27001:2013証明書またはSOC 2 Type 2認証(あるいはその両方)を所有しています。Oracle Cloud Infrastructureは、各施設の有効な証明書および保証報告書の年次評価および定期的なオンサイトの適合性調査を実行しています。Oracle Cloud Infrastructureの独立した監査人は、定期的なオンサイト・ウォークスルーを実行し、データ・センター・コントロールが確実に実施され運用されるようにしています。

クラウド・セキュリティ原則2: 資産の保護とレジリエンス

ユーザー・データ、保存または処理する資産は物理的な改ざん、損失、損害または占拠に対して保護される必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
- データを含むストレージ・メディアが認可されていないアクセスから保護されているかどうか。 - リソースが移動または再プロビジョニングされたとき、お客様がサービスの使用を終了したとき、または消去をリクエストしたときに、データが消去されるかどうか。 - 保留の顧客データを含むストレージ・メディアが認可済か、製品の寿命の最後に安全に破棄されるかどうか。	すべてのオラクルの建造物の個別の要件のガイダンスについては、*Oracle Global Facility Physical Security Technology and Design Manual*に記載されています。*Oracle Supplier Information and Physical Security Standard*は、サードパーティ・サプライヤが従う必要がある、物理的、管理的および技術的な予防手段に対する要件の詳細を説明しています。 **保存データの保護: デフォルトで暗号化** デフォルトでは、Oracle Cloud Infrastructure Block Volumesおよび関連するバックアップが、AES-256を使用して保存時に暗号化されます。お客様が、dm-crypt、veracryptおよびBit-Lockerなどのツールを使用して、データ・ボリュームを暗号化することもできます。 Oracle Cloud Infrastructure Object Storage内のすべてのデータは、AES-256を使用して保存時に暗号化されます。暗号化はデフォルトでオンであり、オフにできません。各オブジェクトは、その暗号化鍵で暗号化され、オブジェクト暗号化鍵はマスター暗号化鍵で暗号化されます。さらに、お客様は、オブジェクトをオブジェクト・ストア・バケットに格納する前に、クライアント側の暗号化を使用して、暗号化鍵でオブジェクトを暗号化できます。 ユーザーが作成した表領域は、Oracle Cloud Infrastructure Databaseでデフォルトで暗号化されます。これらのデータベースでは、ENCRYPT_NEW_TABLESPACESパラメータはCLOUD_ONLYに設定され、Database Cloud Service (DBCS)データベースで作成された表領域は、異なるアルゴリズムが指定されている場合を除き、AES128アルゴリズムによって透過的に暗号化されます。 Oracle Cloud Infrastructure File Storageは、NFSv3エンドポイントを各お客様のVCNサブネット内のマウント・ターゲットとして公開します。すべてのファイルシステム・データは、AES-128を使用して保存時に暗号化されます。

クラウド・セキュリティ原則2: 資産の保護とレジリエンス

ユーザー・データ、保存または処理する資産は物理的な改ざん、損失、損害または占拠に対して保護される必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
- 顧客データ、資格証明またはサービスの構成情報を含んでいる可能性のある機器が、その寿命の終了時に(またはリサイクルする前に)確認されるかどうか。 - 機微データを含むコンポーネントが、必要に応じてサニタイズ、削除または破棄されるかどうか。 - 停止状態からの回復能力など、サービスの可用性のコミットメントがビジネス・ニーズを満たしているかどうか。	**保存データの保護: 暗号化鍵の管理** Oracle Cloud Infrastructure Key Managementは、データの暗号化の集中管理を提供します。お客様は、Key Managementを使用して、マスター暗号化鍵とデータ暗号化鍵の作成、鍵のローテーションによる新しい暗号マテリアルの生成、暗号操作で使用する鍵の有効化または無効化、鍵のリソースへの割当て、および暗号化と復号化への鍵の使用を行えます。 Oracle Cloud Infrastructure Object StorageおよびOracle Cloud Infrastructure Block Volumeは、Key Managementと統合されており、バケットおよびブロックまたはブート・ボリューム内のデータの暗号化をサポートしています。Oracle Cloud Infrastructure Identity and Access Management (IAM)との統合により、お客様はどのユーザーおよびどのサービスが、どの鍵にアクセスでき、その鍵で何を実行できるかを制御できます。Oracle Cloud Infrastructure Auditの統合により、鍵の使用状況を監視する手段がお客様に提供されます。監査は鍵およびボールトについての管理アクションを追跡します。 鍵は、連邦情報処理規格(FIPS) 140-2セキュリティ・レベル3のセキュリティ証明を満たす、可用性および耐久性の高いハードウェア・セキュリティ・モジュール(HSM)に格納されます。Key Managementでは、その暗号化アルゴリズムおよびその鍵がAES対称鍵であるため、Advanced Encryption Standard (AES)が使用されます。 **データのサニタイズおよび機器の処分** オラクルの*Media Sanitization and Disposal Policy*は、システムの寿命、システムの修復と再利用、およびベンダーの変更などの状況に対応するための情報のサニタイズおよび処分など、電子記憶装置からの情報削除の要件を、関連する安全なデータ処理と併せて説明しています。

クラウド・セキュリティ原則2: 資産の保護とレジリエンス

ユーザー・データ、保存または処理する資産は物理的な改ざん、損失、損害または占拠に対して保護される必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	Oracle Cloud Infrastructureは、データが意図せず公開されることがないように、米国標準技術局(NIST)の *Special Publication 800-88 Guidelines on Media Sanitization* (媒体のサニタイズに関するガイドライン)に従っています。このガイドラインは、電子的サニタイズと物理的サニタイズの両方を網羅しています。 **物理的なレジリエンスおよび可用性** Oracle Cloud Infrastructureは、リージョンおよび可用性ドメインでホストされます。リージョンはローカライズされた地理的地域であり、可用性ドメインは、リージョン内に配置された1つ以上のデータ・センターです。リージョンは、いくつかの可用性ドメインで構成されます。ほとんどのOracle Cloud Infrastructureリソースは、VCNなどのリージョン固有、またはコンピュート・インスタンスなどの可用性ドメイン固有のいずれかです。 可用性ドメインは、互いに独立していて耐障害性があり、故障の同時発生に備えて設計されています。可用性ドメインは、電源や冷却装置、内部の可用性ドメインネットワークなどのインフラストラクチャを共有していないため、1つの可用性ドメインの障害が、他の可用性に影響しないように設計されています。 リージョン内のすべての可用性ドメインは、低レイテンシで高帯域幅のネットワークに相互に接続されているため、インターネットおよび顧客設備への可用性の高い接続の提供、複数の可用性ドメイン内でのレプリケートされたシステムの構築を可能にし、高可用性と障害回復の両方を実現しています。 リージョンは、他のリージョンから完全に独立しており、国または大陸をまたぐなど、間隔を大きく開けて分離できます。一般的に、近くにあるリソースを使用する方が、距離の離れたリソースを使用するよりも高速であるため、お客様は最も使用量の多い場所にアプリケーションを配置します。

クラウド・セキュリティ原則2: 資産の保護とレジリエンス

ユーザー・データ、保存または処理する資産は物理的な改ざん、損失、損害または占拠に対して保護される必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	ただし、次の目的のために、アプリケーションを異なるリージョンにデプロイすることもできます。 • 規模の大きい気象状況または地震など、リージョン全域にわたる事象のリスクの緩和 • 法的な管轄区域、税域およびその他のビジネスまたは社会的な条件に対する様々な要件への対応 お客様は、ビジネス・ニーズ、社内の方針、および業界または規制遵守の要件に応じて、高可用性および障害回復を設計および実装する責任を負います。詳細は、『Best Practices for Deploying High Availability Architecture on Oracle Cloud Infrastructure』および『Best Practices for Disaster Recovery in Oracle Cloud Infrastructure』を参照してください。

クラウド・セキュリティ原則3: ユーザー間の区分

悪意のある、または不正利用されているサービス・ユーザーによって、他のユーザーのサービスまたはデータが影響を受けないようにする必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
お客様は次を考慮する必要があります。 - サービスまたはプラットフォームを共有するユーザーのタイプ。 - 顧客データおよびサービスが、サービスの他のユーザーから十分に分離されているか。 - サービスのお客様のインスタンスの管理は他のユーザーからどのように分離されているか。	Oracle Cloud Infrastructureのテナンシのセキュリティは、ファクタの組合せに基づいています。次のステップは、テナンシのセキュリティの構成に関する大まかなガイドラインを示しています。 **ユーザー認証および認可** テナンシを安全に構成するための最初のステップは、最小の権限でテナンシ・リソースにアクセスするユーザーの認証および認可のメカニズムを作成することです。このステップには、Oracle Cloud Infrastructure Identity and Access Management (IAM)の作成、IAMグループの作成、作成したIAMユーザーの認証メカニズムの編成(たとえば、パスワードを使用したコンソール・アクセス、API鍵を使用したAPIアクセスおよびオブジェクト・ストアの認証トークン)、論理グループへのコンパートメントを使用した顧客テナンシ・リソースのグループ化、テナンシまたはコンパートメント・リソースへのIAMグループのアクセスを認可するIAMセキュリティ・ポリシーの編成が含まれます。企業にとって、オンプレミスのユーザーおよびグループのテナンシへのフェデレーションは重要な考慮事項です。IAMでは、お客様がユーザー、グループ、セキュリティ・ポリシーおよびフェデレーション・メカニズムを作成できます。 **ネットワーク・セキュリティ・アーキテクチャ** IAMユーザー認証および認可を編成したら、次のステップとして、お客様のアプリケーションの実行およびテナンシへのデータの格納を安全に行うためのネットワーク・セキュリティ・アーキテクチャを作成します。お客様のコンピュートおよびストレージ・リソースはすべて、各お客様用に作成された仮想クラウド・ネットワーク(VCN)内に含まれます。VCNは、ソフトウェア定義ネットワークであり、お客様がそのワークロードを実行するために使用するオンプレミスの物理ネットワークに類似しています。

クラウド・セキュリティ原則3: ユーザー間の区分

悪意のある、または不正利用されているサービス・ユーザーによって、他のユーザーのサービスまたはデータが影響を受けないようにする必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	VCNセキュリティ・アーキテクチャの編成には、次のようなタスクが含まれます。 • ネットワーク・セグメンテーションのためのVCNサブネットの作成 • VCNセキュリティ・リストを使用した、VCNおよびロード・バランサ・ファイアウォールの編成 • 高可用性およびTLSのためのロード・バランシングの使用 • VCN外部接続のタイプが、インターネット、オンプレミス・ネットワーク、ピアリング済VCNまたはこれらの組合せのいずれであるかの決定 • 仮想ネットワーク・セキュリティ・アプライアンスの使用(たとえば、次世代ファイアウォール、ID) • DNSゾーンおよびマッピングの作成。ロード・バランサにおける重要なセキュリティ考慮事項は、お客様のTransport Layer Security (TLS)証明書を使用した、お客様のVCNへのTLS接続の構成です。 **コンピュート・インスタンスのセキュリティ構成** お客様のアプリケーションは、お客様のVCN内で、ベア・メタル(BM)・インスタンス、仮想マシン(VM)インスタンスおよびGPUなど、コンピュート・インスタンス上で実行されます。コンピュート・インスタンスは、基本的なコンピュート・ビルディング・ブロックです。ベア・メタル・インスタンスでは、Oracle管理ソフトウェアは実行されていないため、結果として、インスタンスおよび(メモリーおよびローカル・ドライブ内に)格納されているデータは、お客様によって完全に管理されます。VMインスタンスは、最小権限メカニズムおよび業界をリードする企業向けハイパーバイザ・セキュリティのベスト・プラクティスを使用して設計されています。 セキュリティおよびパフォーマンス要件に応じて、お客様はテナンシのアプリケーション・ワークロードを実行するインスタンスとして、BMインスタンスおよびVMインスタンスを選択できます。

クラウド・セキュリティ原則3: ユーザー間の区分

悪意のある、または不正利用されているサービス・ユーザーによって、他のユーザーのサービスまたはデータが影響を受けないようにする必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	インスタンスで実行されるお客様のアプリケーションのセキュリティを維持するために、コンピュート・インスタンスを安全に構成することが必須です。 **データ・ストレージ・セキュリティの構成** 必要なデータおよびアクセスの種別に応じて、お客様はデータを(コンピュート・インスタンスにアタッチされた)ローカル・ドライブ、リモート・ブロック・ボリューム、オブジェクト・ストア・バケット、データベースまたはファイル・ストレージに格納できます。これらのデータ・ストレージ要件に対応するために、Oracle Cloud Infrastructureは、Block Volume、Object Storage、DatabaseおよびFile Storageなど、複数のデータ・ストレージ・サービスを提供しています。データ・セキュリティ要件を満たすために、お客様は、データをテナンシに格納するためのテナンシ・データ・ストレージ・アーキテクチャを編成し、サービスで使用するストレージを安全に構成する必要があります。コンプライアンスおよび規制要件は、適切なデータ・ストレージ・セキュリティ・アーキテクチャを決定するための重要なファクタです。 API監査ログは、APIへのコール(コンソール、SDK、CLIおよびAPIを使用したカスタム・クライアント)をログ・イベントとして記録します。API監査ログは、デフォルトで常にオンであり、オフにできません。このログは、90日間お客様に対して有効であり、最大365日間保持されます。API監査ログの情報は、APIアクティビティの発生時間、アクティビティのソース、アクティビティのターゲット、アクションの内容およびレスポンスの内容です。OCI API監査ログを定期的にレビューし、テナンシ・リソースに行ったアクションと一致していることを確認することをお薦めします。 詳細は、Oracle Cloud Infrastructureのセキュリティ機能を参照してください。

クラウド・セキュリティ原則4: ガバナンス

サービス・プロバイダは、そのサービスおよび情報の管理を統合し、指示するセキュリティ・ガバナンス・フレームワークを保有している必要があります。このフレームワークの範囲外で導入される技術的なコントロールは、根本的に弱体化します。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
お客様は次を考慮する必要があります。 - サービスに、適切なガバナンス・フレームワークおよびプロセスがあるかどうか。	オラクルは、組織の目標に沿ったセキュリティ・コントロールおよびプロセスを明らかにしグローバルに実装するためのITセキュリティの監視およびガバナンス機能を提供しています。Oracle製品は、次のセキュリティ・グループによってサポートされています。 **Oracle Security Oversight Committee (OSOC)** オラクルのSecurity Oversight Committee (OSOC)では、事業部およびセキュリティ組織から上級役員が集まり、世界中のオラクルの組織でセキュリティ戦略について情報を交換する機会を持っています。OSOCの役割は次のとおりです。 • グローバル組織の企業セキュリティ要件を明らかにし、対応します。 • 世界規模のセキュリティ標準、慣例およびポリシーを提供するために、事業部門(LOB)、組織およびチームの任命および委任を行います。 • すべてのLOBにわたり、推奨事項およびアクション・プランを上級役員に伝えます。 **Oracle Global Information Security (GIS)** Oracle Global Information Security (GIS)は、セキュリティの監視、コンプライアンス、実施、情報セキュリティ・アセスメントの遂行、情報セキュリティのポリシーと戦略、および会社レベルの研修と意識向上プログラムの開発推進の責任を負っています。従業員は、GISポリシー・ポータルを通じてGISセキュリティ・ポリシーを参照できます。

	また、GISは、セキュリティ・インシデント対応の主たる窓口であり、インシデントの防止、識別、調査および解決の全体的な方向性を指示します。 **Oracle Cloud Infrastructureセキュリティ最高責任者** Oracle Cloud Infrastructureでは、LOB内のセキュリティ組織および情報セキュリティ管理システム(ISMS)を管理するセキュリティ最高責任者が任命されています。セキュリティ最高責任者は、LOB内で次の役割を監督します。 • セキュリティ・アーキテクチャ • 攻撃的セキュリティ • 検出および対応チーム(DART) • セキュリティ・サービス開発 • アクセス制御エコシステム • セキュリティ製品 • 脅威および脆弱性管理(TVM) • 継続的セキュリティ統合サービス(CSIS) **Oracle Cloud Infrastructure Risk Management** Oracle Cloud Infrastructure Risk Managementは、リスク管理の慣行のガバナンスおよびオペレーションへの組込み、最新かつ重要な、新たに出現したリスクのオペレーションおよび指導者チームへの伝達、リスクの検知および管理、ベスト・プラクティスのアドバイス、リスクの評価および関連チームへのアドバイス、セキュリティ戦略の設計、システムおよびソリューションのアーキテクチャ・レビュー、脅威インテリジェンス、およびコンポーネント・グループおよびテクノロジの技術的アセスメントを行います。

クラウド・セキュリティ原則5: 運用セキュリティ

サービスは、攻撃を妨げ、検出し、阻止するために安全に運用し管理する必要があります。優れた運用セキュリティは、複雑で官僚的、また時間を要したり費用がかさんだりするプロセスを必要とするべきではありません。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
お客様は次を考慮する必要があります。 - 構成および変更の管理 - システムへの変更が適切にテストされ認可されていること、およびその変更が予期せずセキュリティ・プロパティを変更しないことの確認。 - 脆弱性管理 - 構成するコンポーネント内のセキュリティの問題の識別と緩和。	**変更管理** Oracle Cloud Infrastructureは、セキュリティ、可用性および機密性へのコミットメントの中核的な要件として、包括的な変更管理プロセスを備えています。変更管理プロセスは、少なくとも毎年見直され、各変更に対して従うべきプロセスおよびプロシージャの要点を示します。 変更管理プロセスは、職務の分離(SOD)を組み込んでおり、実装前に変更の承認およびテストを要求します。すべての変更リクエストは、電子的にアクセス制御されるチケッティング・システムに記録されます。ワークフローにより、クローズ状態の子チケットの必須のレビューおよび承認が行われることなく、チケットが、スケジュール済または実装フェーズに進まないようにできます。 すべての変更は、実装前に、同僚による評価を受ける必要があります。レビューアは、通常、対象システム・サービスの知識を持った同じチームのメンバーであり、正確性および潜在的な問題について、変更を技術的にレビューできます。お客様に重大な影響を及ぼす可能性のある変更も、サービスを管理するチームのマネージャによる文書化された承認を必要とします。 Oracle Cloud Infrastructureは、すべての変更が24時間以内または変更フリーズ中に実装される緊急変更プロセスを実装しており、この変更プロセスにおいても、変更の実装前にオペレーション・チームのメンバーおよび上級管理者により承認を得ることを必須としています。

クラウド・セキュリティ原則5: 運用セキュリティ

サービスは、攻撃を妨げ、検出し、阻止するために安全に運用し管理する必要があります。優れた運用セキュリティは、複雑で官僚的、また時間を要したり費用がかさんだりするプロセスを必要とするべきではありません。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
- 保護的監視 - サービスに対する攻撃および許可されていないアクティビティを検出するための基準の設定。 - インシデント管理 - インシデントに対応し、安全で使用可能なサービスを回復する能力の確保。	**脆弱性管理** システムの侵入テストは少なくとも年に1回実施されます。商用脆弱性スキャン・ツールは、すべての外部IPアドレスおよび内部のノードを少なくとも年4回スキャンするように構成されています。脆弱性スキャンおよび侵入テストの結果は、管理部門によってレビューされます。脆弱性および脅威は、評価され、チケットに記録されて、解決まで追跡されます。 **セキュリティ・イベントおよび情報監視** Oracle Cloud Infrastructureは、インフラストラクチャ内のネットワーキング・デバイス、ホストおよび他のコンポーネントのセキュリティ関連のログおよびアラートを取り込み格納するセキュリティ情報およびイベント監視(SIEM)ソリューションを導入しています。Oracle Cloud Infrastructureの検出および対応チーム(DART)は、SIEMでイベントの相関関係およびその他の関連する検出シナリオを24時間365日ベースで監視し、本番環境での認可されていない侵入およびアクティビティから防御および保護するように設計されています。 **インシデント管理** お客様のアカウント・マネージャに直接報告されるインシデントを含むインシデントは、内部のアクセス制御された電子的なチケッティング・システムにより記録されます。インシデントのルーティング、伝達およびエスカレーションは、緊急性およびお客様への影響などのファクタの数によって異なります。重大度の定義の詳細を次に示します。My Oracle Support (MOS)または外部のユーザー・インシデント報告プロセスを介して報告されたインシデントは、Oracle Cloud Infrastructure担当者に転送され、内部で識別されたインシデントと同じ方法で、電子的なチケッティング・システムで追跡されます。

クラウド・セキュリティ原則5: 運用セキュリティ

サービスは、攻撃を妨げ、検出し、阻止するために安全に運用し管理する必要があります。優れた運用セキュリティは、複雑で官僚的、また時間を要したり費用がかさんだりするプロセスを必要とするべきではありません。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	セキュリティ・インシデントの場合、Oracle Cloud Infrastructureは、GIS、Global Product SecurityおよびPrivacy & Security Legalなどの合意した手続きを必要に応じてアクティブ化し、スペシャリストに、インシデントに対応するための技術的な専門知識を提供します。オラクルが、個人情報違反を含むインシデントをお客様に報告する必要があると判断した場合、影響を受けるお客様に迅速に通知します。

クラウド・セキュリティ原則6: 個人のセキュリティ

サービス・プロバイダの従業員が、データおよびシステムにアクセスできる場合、顧客は、サービス・プロバイダの信用性に対する高いレベルの信頼を必要とします。適切なトレーニングにより裏付けされる徹底的な審査により、サービス・プロバイダの従業員による偶発的または悪意のある漏洩が発生する可能性が削減されます。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
お客様は次を考慮する必要があります。 - 情報へのアクセス権またはサービスに影響を及ぼす能力を持つサービス・プロバイダ・スタッフに実施されるセキュリティ審査のレベルが適切であること。 - 情報へのアクセス権が必要な従業員またはサービスに影響を及ぼすことができる従業員の最少人数。	**顧客データへのアクセス** Oracle Cloud Infrastructureは、お客様の仮想クラウド・ネットワーク(VCN)、アプリケーション、ワークロードまたはデータへのアクセス権を持ちません。お客様が、Oracle Cloud Infrastructureサービスの使用中、データへのアクセスおよびその使用を制御します。 **Oracle Human Resources** Human Resources (HR)は、オラクルの企業業務の1つです。このセクションのコントロールは、Oracle Cloud Infrastructureの従業員を含む、世界中の従業員グループに適用されます。HR担当者は、オラクル内の事業領域に割り当てられます。HRは、その業務に数多くのOracle Human Resources Management Systemおよびツール(HRシステム)を活用します。従業員の手順は、各地域のオラクルの方針、法律および規制に従って異なります。 新規従業員の採用(従来の新規採用または合併または買収による採用)には正式な手順があり、会社の指示および国内の規制およびプロセスに従います。新しい従業員を必要としているマネージャは、HRセルフサービス・アプリケーションにアクセスし、求人を作成して採用チームに転送し、各地域のプロセスに従ってレビューおよび承認を依頼します。

クラウド・セキュリティ原則6: 個人のセキュリティ

サービス・プロバイダの従業員が、データおよびシステムにアクセスできる場合、顧客は、サービス・プロバイダの信用性に対する高いレベルの信頼を必要とします。適切なトレーニングにより裏付けされる徹底的な審査により、サービス・プロバイダの従業員による偶発的または悪意のある漏洩が発生する可能性が削減されます。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	面接の候補者を選択する前に、履歴書がレビューされます。採用マネージャおよび採用担当者(マネージャにより要求された場合)は、最初に有力な候補者と面接します。次に、候補者は、経験、役割および専門知識に基づき選択された複数の面接担当者との面接プロセスを続けます。 候補者の特定が完了したら、オファー・プロセスが開始されます。オラクルの候補者の場合、取引条件(ポジション、給与など)に基づいて、オファーおよび異動に必要な承認レベルを示した正式な承認マトリックスがあります。 **経歴チェック** 経歴チェックは、各地域の法律および規制ならびに各地域のオラクル・ポリシーに従って、採用のために選択された候補者に対して実行されます。オラクルのサプライヤ契約では、個人をオラクルに配属させる前に、各地域の法律および規制ならびに各地域のオラクル・ポリシーで許可された範囲で、サプライヤの契約社員に非直接雇用オラクル雇用者(請負業者)の経歴審査を受けることを求めています。非直接雇用者が直接オラクル従業員として採用された場合、その採用地で必須のオラクル経歴チェックを受ける必要があります。 **トレーニング**

クラウド・セキュリティ原則6: 個人のセキュリティ

サービス・プロバイダの従業員が、データおよびシステムにアクセスできる場合、顧客は、サービス・プロバイダの信用性に対する高いレベルの信頼を必要とします。適切なトレーニングにより裏付けされる徹底的な審査により、サービス・プロバイダの従業員による偶発的または悪意のある漏洩が発生する可能性が削減されます。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	新規従業員には、新規採用Webサイトおよびオリエンテーション・コースが用意されています。オリエンテーションは、多くの形式で提供されています。オリエンテーションは、採用地に応じてオンラインeコース、ライブWeb放送を通じて、または対面のオンボーディング・セッションで行われます。 現在提供中のトレーニングは、Webラーニング、Oracle Universityおよび外部コースを通じて提供される様々なコースで、すべての従業員が利用可能です。各従業員のトレーニングは、個人の職務内容をサポートするようにカスタマイズされます。

クラウド・セキュリティ原則7: セキュアな開発

サービスは、セキュリティに対する脅威を特定し緩和するように設計され、開発されている必要があります。そうではない場合、セキュリティの問題に対して脆弱になる可能性があり、データの漏洩、サービスの損失またはその他の悪意のある行動が発生する場合があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
お客様は次を考慮する必要があります。 - 新しく進化している脅威がレビューされ、サービスがそれに合わせて改善されていること。 - 安全な設計、コーディング、テストおよびデプロイメントに関する業界の優れた慣行に沿って、開発が行われていること。 - 構成管理プロセスが整備され、開発、テストおよびデプロイメントを通じてソリューションの整合性が確保されていること。	**Secure Coding Standards** オラクルは、コードを記述する際に既知のセキュリティ欠陥タイプが含まれないようにする方法について、ソフトウェア開発者向けのガイドラインを示した*Secure Coding Standards*を文書化しています。Secure Coding Standardsは、幅広いOracle Software Security Assurance (OSSA)プログラムの一部であり、Software Engineering Institute Computer Emergency Response Team (SEI CERT)のルールおよびオラクル社内の指示に基づいています。 **ソフトウェア開発ライフサイクル** すべてのOracle Cloud Infrastructureソフトウェア開発チームは、OSSAおよびOracle *Secure Coding Standards*の要件に従う必要があり、ソフトウェア開発のライフサイクル(SDLC)を文書化する必要があります。これには、安全なコード開発の慣行、相互評価、新規コードを本番に組み込むための変更管理、および年1回の安全なコード開発トレーニングなどが含まれます。Oracle Cloud Infrastructureソフトウェア開発チームは、少なくとも年1回SDLCをそれぞれレビューし更新する必要があります。 **Continuous Integration/Continuous Deployment** Oracle Cloud InfrastructureのContinuous Integration/Continuous Deployment (CICD)チームは、最適な開発およびテスト慣行を具現化するエンジニアリング環境の構築を支持し、エンジニアが継続的な統合およびデプロイメント・モデルを使用して、高い品質、安定性およびパフォーマンスを備えたIaaS製品を定量的に提供できるようにします。

クラウド・セキュリティ原則7: セキュアな開発

サービスは、セキュリティに対する脅威を特定し緩和するために設計し開発する必要があります。そうではない場合、セキュリティの問題に対して脆弱になる可能性があり、データの漏洩、サービスの損失またはその他の悪意のある行動が発生する場合があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	ソフトウェア開発チームを持つCICDパートナは、Oracle Cloud InfrastructureのIaaSソリューションのアーキテクチャ、設計および実装の責任を負い、製品の開発サイクルを通じて、コード・リリースの速度および品質を高めます。 **構成管理** Oracle Cloud Infrastructureは、業界標準の構成管理ツールを使用して、長寿命のホストのパッケージ、システム構成およびサービス構成を管理します。

クラウド・セキュリティ原則8: サプライ・チェーン・セキュリティ

サービス・プロバイダは、サービスが実装を要求するすべてのセキュリティ原則をそのサプライ・チェーンが十分にサポートするように保証する必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
お客様は次を考慮する必要があります。 - 情報が、サードパーティ・サプライヤおよびそのサプライ・チェーンとどのように共有され、アクセスが許可されているか。 - サービス・プロバイダの調達プロセスでサードパーティ・サプライヤに対するセキュリティ要件がどのように整備されているか。 - サービス・プロバイダが、サードパーティ・サプライヤからのセキュリティ・リスクをどのように管理しているか。	オラクルのコロケーション施設プロバイダは、Oracle Cloud Infrastructureの電源、物理的なセキュリティおよび環境管理のみを提供します。コロケーション施設プロバイダは、Oracle Cloud Infrastructureのサービスまたはアプリケーション、ワークロードまたはデータへのアクセスが許可されていません。 オラクルのサプライヤ・セキュリティ・プログラムは、ISO 27000シリーズに沿っており、オラクルによって使用されるサプライヤの情報セキュリティ・リスクを識別、管理および緩和するように設計されています。サプライヤ・セキュリティ・アセスメントは、サプライヤ・セキュリティ・プログラムの一環として実行され、オラクルの情報および物理セキュリティ標準に対するサプライヤのコンプライアンスのレビュー、相違の特定、および改善についての助言を行います。 **コロケーション施設のセキュリティ** 各コロケーション施設は、自らのISO/IEC 27001:2013証明書またはSOC 2 Type 2認証(あるいはその両方)を所有しています。Oracle Cloud Infrastructureは、各施設の有効な保証報告書の年次評価および定期的なオンサイトの適合性調査を実行しています。Oracle Cloud Infrastructureの独立した監査人は、定期的なオンサイト・ウォークスルーを実行し、データ・センター・コントロールが確実に実施され運用されるようにしています。 すべてのオラクルの建造物の個別の要件のガイダンスについては、*Oracle Global Facility Physical Security Technology and Design Manual*に記載されています。*Oracle Supplier Information and Physical Security Standard*は、サードパーティ・サプライヤが従う必要がある、物理的、管理的および技術的な予防手段に対する要件の詳細を説明しています。

クラウド・セキュリティ原則8: サプライ・チェーン・セキュリティ

サービス・プロバイダは、サービスが実装を要求するすべてのセキュリティ原則をそのサプライ・チェーンが十分にサポートするように保証する必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
- サービス・プロバイダが、そのサプライヤによるセキュリティ要件の適合性をどのように管理しているか。 - サービス・プロバイダが、サービスで使用されているハードウェアおよびソフトウェアが本物であり、改ざんされていないことをどのように検証しているか。	**ハードウェア・セキュリティ** Oracle Cloud Infrastructureは、Oracle (Sun)、Arista、Juniper、Caviumなど広く知られたハードウェア・ベンダーおよびその他の有名なベンダーからハードウェアを調達しています。ハードウェア・ベンダーは、個人情報を誤用や偶発的、違法または未許可の破棄、損失、変更、公開、取得またはアクセスから保護するために設計された適切な技術的または組織的な対策を実装し維持することが求められます。加えて、 オラクルへのサプライヤは、*Oracle Supplier Information and Physical Security Standards (OSSS)*および*Oracle Supplier Code of Ethics and Business Conduct (OSCoE)*に記載されている、IT、物理的な環境および人材面のセキュリティ、機密性、トレーニング、コンプライアンスと監査、ビジネスの継続性、障害回復、さらにセキュリティ・インシデントおよび報告要件に準拠していることが求められます。進化するビジネス・リスク、セキュリティ標準および規制遵守要件に対応するために、オラクルは、少なくとも年に1回OSSSおよびOSCoEをレビューし、必要に応じて、いつでも更新しています。

クラウド・セキュリティ原則9: セキュアなユーザー管理

サービス・プロバイダは、顧客がサービスの使用を安全に管理するために使用できるツールを提供する必要があります。管理インタフェースおよび手順は、不正アクセスおよび顧客のリソース、アプリケーションおよびデータの変更を阻止するセキュリティの壁の極めて重要な部分です。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
お客様は次を考慮する必要があります。 - 管理インタフェースおよびサポート・チャネルに対するユーザーの認証。 - 管理インタフェース内の区分およびアクセス制御。	**認証および認可** お客様が、アプリケーション、ワークロードおよびデータへのアクセスおよび使用を管理します。Oracle Cloud Infrastructure Identity and Access Management (IAM)サービスは、企業の要件を満たすように構築されており、すべてのOracle Cloud Infrastructureリソースおよびサービスに対する認証および認可を提供します。企業は、セキュリティ、分離およびガバナンスを維持しながら、様々なビジネス・ユニット、チームおよび個人によって共有される単一のテナンシを使用できます。 お客様がOracle Cloud Infrastructureに参加すると、テナンシが作成されます。テナンシは、お客様に属しているすべてのOracle Cloud Infrastructureリソースを含む仮想的な概念です。テナンシの管理者は、ユーザーおよびグループを作成して、コンパートメントにパーティション化されているリソースに最小権限アクセスを割り当てることができます。 **区分および分離** コンパートメントは、単一の論理ユニットとして管理できるリソース・グループであり、規模の大きいインフラストラクチャを合理的に管理する手段を提供します。たとえば、コンパートメント(HRコンパートメント)を作成し、HRアプリケーションをホストするために必要なクラウド・ネットワーク、コンピュート・インスタンスおよびストレージ・ボリュームの特定のセットをホストできます。

クラウド・セキュリティ原則9: セキュアなユーザー管理

サービス・プロバイダは、顧客がサービスの使用を安全に管理するために使用できるツールを提供する必要があります。管理インタフェースおよび手順は、不正アクセスおよび顧客のリソース、アプリケーションおよびデータの変更を阻止するセキュリティの壁の極めて重要な部分です。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	コンパートメントは、クラウド・リソースを編成、分離するための、Oracle Cloud Infrastructureの基本的なコンポーネントです。 お客様はコンパートメントを使用して、分離の目的でリソースを明確に区分します(リソースをプロジェクトまたはビジネス・ユニットごとに区分します)。一般的な手法として、組織の各主要部分に対してコンパートメントを作成します。地域ごとに範囲が定められているほとんどのOracle Cloud Infrastructureサービスと異なり、IAMサービス・リソースは世界全体が対象です。お客様は、複数のリージョンにまたがる単一のテナンシを保有できます。 次に、主要なIAMを示します。 • **リソース:** 会社の従業員が、Oracle Cloud Infrastructureサービスとやりとりする際に作成および使用するクラウド・オブジェクト。たとえば、コンピュート・インスタンス、ブロック・ストレージ・ボリューム、仮想クラウド・ネットワーク(VCN)、サブネットおよびルート表などがあります。 • **ポリシー:** テナンシ内のリソースへのアクセスを定義する認可ルールのセット。 • **コンパートメント:** セキュリティ分離およびアクセス制御を目的とした、リソースの異種コレクション。 • **テナンシ:** 組織のリソースをすべて含むルート・コンパートメント。管理者は、テナンシ内で、1つ以上のコンパートメントの作成、1人以上のユーザーとグループの作成、およびコンパートメント内のリソースを使用する権限をグループに付与するポリシーの割当てを行えます。

クラウド・セキュリティ原則9: セキュアなユーザー管理

サービス・プロバイダは、顧客がサービスの使用を安全に管理するために使用できるツールを提供する必要があります。管理インタフェースおよび手順は、不正アクセスおよび顧客のリソース、アプリケーションおよびデータの変更を阻止するセキュリティの壁の極めて重要な部分です。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	• **ユーザー:** リソースを管理するためにアクセスする必要がある個人またはシステム。ユーザーがリソースにアクセスするためには、グループに追加される必要があります。ユーザーは、Oracle Cloud Infrastructureサービスへの認証に使用する必要がある資格証明を1つ以上保有します。フェデレーテッド・ユーザーもサポートされています。 • **グループ:** 類似したアクセス権限セットを共有するユーザーのコレクション。管理者は、テナンシ内のリソースを消費または管理するグループを認可するアクセス・ポリシーを付与できます。グループ内のすべてのユーザーは、同じ権限セットを継承します。 • **アイデンティティ・プロバイダ:** フェデレーテッド・アイデンティティ・プロバイダとの信頼関係。Oracle Cloud Infrastructureコンソールに対して認証を試みるフェデレーテッド・ユーザーは、構成済のアイデンティティ・プロバイダにリダイレクトされます。認証が成功したら、フェデレーテッド・ユーザーは、ネイティブIAMユーザーと同様に、コンソール内のOracle Cloud Infrastructureリソースを管理できます。現在、Oracle Cloud Infrastructureは、Oracle Identity Cloud ServiceおよびMicrosoft Active Directory Federation Service (ADFS)をアイデンティティ・プロバイダとしてサポートしています。フェデレーテッド・ユーザーに適用されるポリシーを定義するために、フェデレーテッド・グループは、ネイティブIAMグループにマップされます。 Oracle Cloud Infrastructureリソースにアクセスするすべてのお客様のコールは、まず、IAMサービス(またはフェデレーテッド・プロバイダ)によって認証され、次にIAMポリシーに基づいて認可されます。お客様は、テナンシ内のコンパートメント内のインフラストラクチャ・リソース(ネットワーク、コンピュート、ストレージなど)にアクセスする権限を一連のユーザーに付与するポリシーを作成できます。

クラウド・セキュリティ原則9: セキュアなユーザー管理

サービス・プロバイダは、顧客がサービスの使用を安全に管理するために使用できるツールを提供する必要があります。管理インタフェースおよび手順は、不正アクセスおよび顧客のリソース、アプリケーションおよびデータの変更を阻止するセキュリティの壁の極めて重要な部分です。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	これらのポリシーは柔軟であり、理解および監査が簡単な、人間が読み取れる形式で記述されています。 **認証の資格証明** 各ユーザーは、Oracle Cloud Infrastructureに対して自身を認証するために次の資格証明を1つ以上保有しています。ユーザーは、自らの資格証明を生成し、ローテーションできます。加えて、テナンシのセキュリティ管理者は、テナンシ内のユーザーの資格証明をリセットできます。 • **コンソールのパスワード:** Oracle Cloud Infrastructureコンソールに対するユーザーの認証に使用されます。 • **API鍵:** すべてのAPIコールは、ユーザー固有の2048ビットRSA秘密鍵を使用して署名されます。ユーザーは、公開鍵のペアを作成し、コンソール内で公開鍵をアップロードします。 • **認証トークン:** 認証トークンはオラクルが生成するトークン文字列であり、お客様はこれを使用して、Oracle Cloud Infrastructureのシグネチャ・ベースの認証をサポートしていないサードパーティAPIで認証できます。たとえば、認証トークンを使用して、OpenStack Swiftクライアントで認証します。十分な複雑性を確保するにために、トークンは、IAMサービスによって作成され、お客様が指定することはできません。 • **顧客秘密キー:** Object StorageサービスのS3準拠のAPIにアクセスするためにAmazon S3クライアントによって使用されます。十分な複雑性を確保するにために、パスワードは、IAMサービスによって作成され、お客様が指定することはできません。

クラウド・セキュリティ原則10: アイデンティティと認証

サービス・インタフェースへのすべてのアクセスは、認証および認可された個人に制限する必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
お客様は次を考慮する必要があります。 - アイデンティティおよび認証コントロールにより、個々のインタフェースにアクセスする権限がユーザーに付与されていることが保証されているかどうか。	**認証および認可** お客様が、アプリケーション、ワークロードおよびデータへのアクセスおよび使用を管理します。Oracle Cloud Infrastructure Identity and Access Management (IAM)サービスは、企業の要件を満たすように構築されており、すべてのOracle Cloud Infrastructureリソースおよびサービスに対する認証および認可を提供します。企業は、セキュリティ、分離およびガバナンスを維持しながら、様々なビジネス・ユニット、チームおよび個人によって共有される単一のテナンシを使用できます。 お客様がOracle Cloud Infrastructureに参加すると、テナンシが作成されます。テナンシは、お客様に属しているすべてのOracle Cloud Infrastructureリソースを含む仮想的な概念です。テナンシの管理者は、ユーザーおよびグループを作成して、コンパートメントにパーティション化されているリソースに最小権限アクセスを割り当てることができます。 **区分および分離** コンパートメントは、単一の論理ユニットとして管理できるリソース・グループであり、規模の大きいインフラストラクチャを合理的に管理する手段を提供します。たとえば、コンパートメント(HRコンパートメント)を作成し、HRアプリケーションをホストするために必要なクラウド・ネットワーク、コンピュート・インスタンスおよびストレージ・ボリュームの特定のセットをホストできます。 コンパートメントは、クラウド・リソースを編成、分離するための、Oracle Cloud Infrastructureの基本的なコンポーネントです。

クラウド・セキュリティ原則10: アイデンティティと認証

サービス・インタフェースへのすべてのアクセスは、認証および認可された個人に制限する必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	お客様はコンパートメントを使用して、分離の目的でリソースを明確に区分します(リソースをプロジェクトまたはビジネス・ユニットごとに区分します)。一般的な手法として、組織の各主要部分に対してコンパートメントを作成します。地域ごとに範囲が定められているほとんどのOracle Cloud Infrastructureサービスと異なり、IAMサービス・リソースは世界全体が対象です。お客様は、複数のリージョンにまたがる単一のテナンシを保有できます。 次に、主要なIAMの概念を示します。 • **リソース:** 会社の従業員が、Oracle Cloud Infrastructureサービスとやりとりする際に作成および使用するクラウド・オブジェクト。たとえば、コンピュート・インスタンス、ブロック・ストレージ・ボリューム、仮想クラウド・ネットワーク(VCN)、サブネットおよびルート表などがあります。 • **ポリシー:** テナンシ内のリソースへのアクセスを定義する認可ルールのセット。 • **コンパートメント:** セキュリティ分離およびアクセス制御を目的とした、リソースの異種コレクション。 • **テナンシ:** 組織のリソースをすべて含むルート・コンパートメント。管理者は、テナンシ内で、1つ以上のコンパートメントの作成、1人以上のユーザーとグループの作成、およびコンパートメント内のリソースを使用する権限をグループに付与するポリシーの割当てを行えます。 • **ユーザー:** リソースを管理するためにアクセスする必要がある個人またはシステム。ユーザーがリソースにアクセスするためには、グループに追加される必要があります。ユーザーは、Oracle Cloud Infrastructureサービスへの認証に使用する必要がある資格証明を1つ以上保有します。フェデレーテッド・ユーザーもサポートされています。

クラウド・セキュリティ原則10: アイデンティティと認証

サービス・インタフェースへのすべてのアクセスは、認証および認可された個人に制限する必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	• **グループ:** 類似したアクセス権限セットを共有するユーザーのコレクション。管理者は、テナンシ内のリソースを消費または管理するグループを認可するアクセス・ポリシーを付与できます。グループ内のすべてのユーザーは、同じ権限セットを継承します。 • **アイデンティティ・プロバイダ:** フェデレーテッド・アイデンティティ・プロバイダとの信頼関係。Oracle Cloud Infrastructureコンソールに対して認証を試みるフェデレーテッド・ユーザーは、構成済のアイデンティティ・プロバイダにリダイレクトされます。認証が成功したら、フェデレーテッド・ユーザーは、ネイティブIAMユーザーと同様に、コンソール内のOracle Cloud Infrastructureリソースを管理できます。現在、Oracle Cloud Infrastructureは、Oracle Identity Cloud ServiceおよびMicrosoft Active Directory Federation Service (ADFS)をアイデンティティ・プロバイダとしてサポートしています。フェデレーテッド・ユーザーに適用されるポリシーを定義するために、フェデレーテッド・グループは、ネイティブIAMグループにマップされます。 Oracle Cloud Infrastructureリソースにアクセスするすべてのお客様のコールは、まず、IAMサービス(またはフェデレーテッド・プロバイダ)によって認証され、次にIAMポリシーに基づいて認可されます。お客様は、テナンシ内のコンパートメント内のインフラストラクチャ・リソース(ネットワーク、コンピュート、ストレージなど)にアクセスする権限を一連のユーザーに付与するポリシーを作成できます。これらのポリシーは柔軟であり、理解および監査が簡単な、人間が読み取れる形式で記述されています。

クラウド・セキュリティ原則10: アイデンティティと認証

サービス・インタフェースへのすべてのアクセスは、認証および認可された個人に制限する必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	認証の資格証明 各ユーザーは、Oracle Cloud Infrastructureに対して自身を認証するために次の資格証明を1つ以上保有しています。ユーザーは、自らの資格証明を生成し、ローテーションできます。加えて、テナンシのセキュリティ管理者は、テナンシ内のユーザーの資格証明をリセットできます。 • **コンソールのパスワード:** Oracle Cloud Infrastructureコンソールに対するユーザーの認証に使用されます。 • **API鍵:** すべてのAPIコールは、ユーザー固有の2048ビットRSA秘密**鍵**を使用して署名されます。ユーザーは、公開**鍵**のペアを作成し、コンソール内で公開**鍵**をアップロードします。 • **認証トークン:** 認証トークンはオラクルが生成するトークン文字列であり、お客様はこれを使用して、Oracle Cloud Infrastructureのシグネチャ・ベースの認証をサポートしていないサードパーティAPIで認証できます。たとえば、認証トークンを使用して、OpenStack Swiftクライアントで認証します。十分な複雑性を確保するにために、トークンは、IAMサービスによって作成され、お客様が指定することはできません。 • **顧客秘密キー:** Object StorageサービスのS3準拠のAPIにアクセスするためにAmazon S3クライアントによって使用されます。十分な複雑性を確保するにために、パスワードは、IAMサービスによって作成され、お客様が指定することはできません。

クラウド・セキュリティ原則11: 外部インタフェースの保護

サービスの外部インタフェースまたは信頼度の低いインタフェースはすべて特定し、適切に防御する必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
お客様は次を考慮する必要があります。 - どの物理および論理インタフェースから情報が提供されるか、およびデータへのアクセスはどのように制御されるか。 - サービスが、これらのインタフェース上で適切なレベルに対してユーザーを識別し認証するかどうか。	お客様が、自身の運用環境内のコンピューティング・リソースの物理的なセキュリティの責任を負います。論理インタフェース・セキュリティに関して、お客様のコンピュートおよびストレージ・リソースのすべては、お客様が構成し制御する仮想クラウド・ネットワーク(VCN)で囲まれます。さらに、Oracle Cloud Infrastructure Domain Name System (DNS)サービスは、企業のお客様向けに動的、静的および再帰的DNSソリューションを提供します。このサービスは、訪問者をお客様のWebサイトおよびアプリケーションに高速で安全なサービスを通じて接続します。 DNSサービスは、グローバルなエニーキャスト・ネットワーク上で、5つの大陸のPOP (Points Of Presence)により運用されており、完全に冗長化されたDNS構成およびPOP当たり複数のTier 1トランジット・プロバイダを提供しています。このソリューションは、DNSベースのDDoS (分散型サービス拒否)からの保護、および1日当たり2400億超のデータを収集し分析する広大なセンサー・ネットワークを活用したインハウスのセキュリティ専門知識を提供しています。また、DNSサービスは、セカンダリDNS機能も完全にサポートしているためお客様の既存DNSサービスを補完し、DNSレイヤーにおけるレジリエンスを提供しています。 VCNは、ソフトウェア定義ネットワークであり、お客様がそのワークロードの実行に使用するオンプレミスの物理ネットワークに類似しています。VCNセキュリティ・アーキテクチャの編成には、次のようなタスクが含まれます。 • ネットワーク・セグメンテーションのためのVCNサブネットの作成 • VCNセキュリティ・リストを使用した、VCNおよびロード・バランサ・ファイアウォールの編成 • 高可用性およびTLSのためのロード・バランシングの使用 • VCN外部接続のタイプが、インターネット、オンプレミス・ネットワーク、ピアリング済VCNまたはこれらの組合せのいずれであるかの決定

クラウド・セキュリティ原則11: 外部インタフェースの保護

サービスの外部インタフェースまたは信頼度の低いインタフェースはすべて特定し、適切に防御する必要があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	• 仮想ネットワーク・セキュリティ・アプライアンスの使用(たとえば、次世代ファイアウォール、ID) • DNSゾーンおよびマッピングの作成。ロード・バランサにおける重要なセキュリティ考慮事項は、お客様のTransport Layer Security (TLS)証明書を使用した、お客様のVCNへのTLS接続の構成です。 お客様の仮想クラウド・ネットワーク(VCN)は、サブネットにパーティション化でき、それぞれは可用性ドメインにマップされます。プライベート・サブネット内のインスタンスは、パブリックIPアドレスを持てません。パブリック・サブネット内のインスタンスは、オプションとして、お客様の裁量でパブリックIPアドレスを持つことができます。 セキュリティ・リストは、ステートフルおよびステートレス・ファイアウォール機能を提供し、お客様のインスタンスへのネットワーク・アクセスを制御します。セキュリティ・リストはサブネット・レベルで構成され、インスタンス・レベルで実施されます。複数のセキュリティ・リストをサブネットに適用できます。ネットワーク・パケットは、セキュリティ・リスト内のいずれかのルールと一致する場合に許可されます。 ゲートウェイによって、VCN内のリソースとVCN外の宛先が通信できます。ゲートウェイには次が含まれます。 • インターネット・ゲートウェイ: インターネット接続用(パブリックIPアドレスを含むリソース用) • NATゲートウェイ: 受信インターネット接続へのリソースの公開なしのインターネット接続用(プライベートIPアドレスを含むリソース用) • 動的ルーティング・ゲートウェイ(DRG): VCNリージョンの外のネットワークへの接続用(たとえば、IPSec VPNまたはFastConnectによるオンプレミス・ネットワーク、または別のリージョンのピアリング済VCN) • サービス・ゲートウェイ: Object StorageなどのパブリックOracle Cloud Infrastructureサービスへのプライベート接続用 • ローカル・ピアリング・ゲートウェイ(LPG): 同じリージョン内のピアリング済VCN

クラウド・セキュリティ原則11: 外部インタフェースの保護 サービスの外部インタフェースまたは信頼度の低いインタフェースはすべて特定し、適切に防御する必要があります。	
考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	ルート表は、お客様のVCNのサブネットからVCNの外の宛先にトラフィックをルーティングする方法を制御します。ルーティング・ターゲットは、VCNゲートウェイまたはVCN内のプライベートIPアドレスとなります。 詳細は、Oracle Cloud Infrastructureのセキュリティ機能を参照してください。

クラウド・セキュリティ原則12: セキュアなサービス運営

クラウド・サービスの管理に使用されるシステムは、そのサービスへの高い特権付きのアクセス権を保有します。これが漏洩すると、セキュリティ・コントロールを省略する、大量のデータを盗むまたは操作する手段になるなど、多大な影響を及ぼす場合があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
お客様は次を考慮する必要があります。 - サービスを管理するためにサービス・プロバイダによってどのサービス管理モデルが使用されているか。 - 使用しているサービス管理モデルによってサービスのデータまたは使用にもたらされるリスク。	**オラクル担当者による基礎となるスタックのセキュアな管理** サービスをサポートしているネットワーク・デバイス、サーバーへのアクセスでは、Oracleユーザーは、マルチファクタ認証を使用し、3つのレベルのアクセス制御を通過することが求められます。認証パスの最初のステップは、Oracle Cloud Network Access (OCNA) VPNです。OCNAは、専用のエクストラネット内の多層のDMZ (非武装地帯)環境であり、オラクルの内部企業ネットワークおよび非クラウド・サービス用のVPNから分離されています。これは、ユーザーとターゲット・デバイス間の安全なアクセス・ゲートウェイとして機能します。OCNAは、オラクルのDMZに配置されているゲートウェイ・サブネット、ツール・サブネットおよびネットワーク・サブネットで構成され、ファイアウォールで保護されます。 有効なOCNAアカウントを持つ承認済のエンジニアのみがOCNAにアクセスできます。OCNAに対する認証には、2要素認証が必要です。ユーザー・アカウントの作成時、ユーザーにアクセス権が付与される個々の資格を説明する属性が定義されます。ユーザーは、接続時、そのリソースにアクセスが制限されます。ユーザーのアクセス権は、アクセスがプロビジョニングされる前に、適切な承認者によって承認される必要があり、ユーザーの雇用が終了したら、アクセス権は取り消されます。OCNAは、エンドポイントで最新のウィルス対策ソフトウェアが実行されているか、ローカル・ファイアウォールが有効であるか、およびソフトウェア更新に関するオラクルのポリシーに合致しているかを判断するセキュリティ・ポスチャ・チェックを完了してから、VPNへの認証をエンドポイントに許可するように構成されています。 認証パスの2番目のステップは、関連する要塞サーバーに対する認証です。オペレータ・アクセスは、要塞サーバーからのみ許可されます。要塞サーバーは、OCNAのサブネットからの接続のみを受け入れます。要塞サーバーへのアクセスは、2つの方法で制御されます。

クラウド・セキュリティ原則12: セキュアなサービス運営

クラウド・サービスの管理に使用されるシステムは、そのサービスへの高い特権付きのアクセス権を保有します。これが漏洩すると、セキュリティ・コントロールを省略する、大量のデータを盗むまたは操作する手段になるなど、多大な影響を及ぼす場合があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	• Oracle Identity Manager (OIM) - 必須のOIM資格を持つ承認済のエンジニアのみが、要塞サーバーにアクセスできます。ユーザーのアクセスは、資格がプロビジョニングされる前に、適切な承認者によって承認される必要があります。 • SSH鍵 - 権限のあるユーザーの公開/秘密SSH鍵が、ユーザーのUNIXユーザー名と組み合せて使用され、LDAPを介して認証されます。ユーザーの秘密鍵は、アクセスに2要素認証を必要とするユーザーのトークン上の仮想スロットに格納されます。対応するユーザーの公開鍵は、アクセスのプロビジョニング・プロセス中に適切な要塞サーバーで構成されます。 要塞サーバーに対して認証するには、ユーザーは両方の前提条件を満たしている必要があります。要塞サーバーへのアクセスは、四半期ごとにレビューされます。レビュー時に特定された不適切なアクセスは、調査され無効になります。 **お客様によるクラウド・サービスのセキュアな管理** お客様は、次の方法でクラウド・サービスのリソースを作成および管理できます。 • Oracle Cloud Infrastructureコンソール: このコンソールは、ユーザーおよび権限だけではなく、インスタンス、クラウド・ネットワークおよびストレージ・ボリュームの作成および管理を促進する直感的なグラフィカル・インタフェースです。

クラウド・セキュリティ原則12: セキュアなサービス運営

クラウド・サービスの管理に使用されるシステムは、そのサービスへの高い特権付きのアクセス権を保有します。これが漏洩すると、セキュリティ・コントロールを省略する、大量のデータを盗むまたは操作する手段になるなど、多大な影響を及ぼす場合があります。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	• Oracle Cloud Infrastructure Application Programming Interfaces (API): Oracle Cloud InfrastructureのAPIは、通常、HTTPSリクエストおよびレスポンスを使用するREST APIです。 • ソフトウェア開発キット(SDK): SDKは、Oracle Cloud Infrastructure APIとの簡単な統合に使用でき、Java用のSDK、RubyおよびPythonなどが含まれます。 • コマンドライン・インタフェース(CLI): お客様は、一部のサービスでCLIを使用できます。 詳細は、Oracle Cloud Infrastructureのセキュリティ機能を参照してください。

クラウド・セキュリティ原則13: ユーザーの監査情報

サービスおよびその中で保有されているデータへのアクセスの監視に必要な監査レコードを顧客に提供する必要があります。顧客に提供可能な監査情報のタイプは、妥当な時間スケール内で不適切または悪意のあるアクティビティを検出し対応する能力に直接影響します。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
お客様は次を考慮する必要があります。 - 提供される監査情報、その情報がどのように、いつ利用可能になるか、データの形式および関連付けられている保存期間。 - 利用可能な監査情報が、誤用またはインシデントの調査ニーズを満たしているか。	Oracle Cloud Infrastructure Auditサービスは、サポートされているすべてのOracle Cloud Infrastructureパブリック API (Application Programming Interface)エンドポイントへのコールをログ・イベントとして自動的に記録します。現在、すべてのサービスは監査によるロギングをサポートしています。Object Storageサービスは、バケット関連イベントのロギングをサポートしていますが、オブジェクト関連のイベントはサポートしていません。 Auditサービスによって記録されるログ・イベントには、Oracle Cloud Infrastructureコンソール、コマンドライン・インタフェース(CLI)、ソフトウェア開発キット(SDK)、お客様独自のカスタム・クライアントまたは他のOracle Cloud Infrastructureサービスによって行われるAPIコールが含まれます。ログの情報は、APIアクティビティの発生時間、アクティビティのソース、アクティビティのターゲット、アクションの内容およびレスポンスの内容です。 各ログ・イベントには、ヘッダーID、ターゲット・リソース、記録されたイベントのタイム・スタンプ、リクエスト・パラメータおよびレスポンス・パラメータが含まれます。お客様は、コンソール、APIまたはJava SDKを使用して、監査サービスによって記録されたイベントを表示できます。イベントの分析や別々の格納だけではなく、イベントの表示、個々のイベントの詳細のコピーも行えます。イベントのデータは、診断の実行、リソースの使用状況の追跡、コンプライアンスの監視およびセキュリティ関連のイベントの収集に使用できます。 詳細は、Oracle Cloud Infrastructureのセキュリティ機能を参照してください。

クラウド・セキュリティ原則14: セキュアなサービスの利用

クラウド・サービスのセキュリティおよびその中で保持されているデータは、顧客がサービスを不完全な方法で使用した場合、弱体化する可能性があります。結果として、データを適切に保護するには、サービスを使用する際、顧客が一定の責任を負います。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能

お客様は次を考慮する必要があります。
 	
- 使用可能なサービス構成のオプションおよび一般的に好まれるセキュリティ関連の事項。
 	
- お客様によるサービスの使用に関するセキュリティ要件。
 	
- サービスを使用および管理するお客様の従業員が、それをどのように安全かつ確実に行えるようにするか。
	Oracle Cloud Infrastructureの起動、構成、管理および使用のためのドキュメント
	
	Oracle Cloud Infrastructureサービスの起動、構成、管理および使用に関する詳細は、次のドキュメントを参照してください。
	
	• Oracle Cloud Infrastructureドキュメント
	  ○ 主な概念および用語
	  ○ セキュリティ・ガイド
	  ○ セキュリティ機能
	  ○ セキュリティ・ベスト・プラクティス
	
	セキュリティの共同責任
	
	Oracle Cloud Infrastructureでワークロードを安全に実行するには、お客様はそのセキュリティおよびコンプライアンスの責任を認識している必要があります。目的をもって、オラクルはクラウド・インフラストラクチャおよびオペレーションのセキュリティを提供し(クラウド・オペレータのアクセス制御、インフラストラクチャ・セキュリティパッチ適用など)、お客様は自身のクラウド・リソースを安全に構成する責任を負います。

クラウド・セキュリティ原則14: セキュアなサービスの利用

クラウド・サービスのセキュリティおよびその中で保持されているデータは、顧客がサービスを不完全な方法で使用した場合、弱体化する可能性があります。結果として、データを適切に保護するには、サービスを使用する際、顧客が一定の責任を負います。

考慮事項	Oracle Cloud Infrastructureのコントロールまたは機能
	詳細は、次のドキュメントを確認してください。 • Oracle Cloud Infrastructure Security

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services