Oracle OCI Exadata Database Service on Dedicated Infrastructure Security Controls

ORACLE

# Exadata Database Service on Dedicated Infrastructure Security Controls

不正なアクションの防止、検出、対応に役立ち、IT セキュリティ・ポリシーの要件に対処する機能

April 22, 2024 | 2.23 版

## 本書の目的

このドキュメントは、Exadata リリース 20.1.13.0.0.210817 に組み込まれている機能と強化点の概要を示すものです。お客様が Exadata リリース 20.1.13.0.0.210817 にアップグレードするビジネス上の利点を評価し、IT プロジェクトを計画する際にお役立ていただくことのみを意図しています。

このドキュメントは、オラクルの Oracle Cloud Infrastructure (OCI) Exadata Database Service on Dedicated Infrastructure (ExaDB-D)サービスのセキュリティおよび統制機能を要約したもので、ExaDB-D の採用評価に携わるお客様のセキュリティ担当者を対象としています。ExaDB-D の評価に携わるセキュリティ担当者は、次のドキュメントも確認する必要があります。

- Oracle Cloud Infrastructure Security Architecture[1]
- Oracle Cloud Infrastructure セキュリティ・ガイド[2]
- オラクルの企業セキュリティ慣行[3]
- Exadata Database Service on Dedicated Infrastructure Security Guide[4]
- Security Features in Autonomous Database[5]
- Security and Authentication in Oracle Autonomous Database[6]
- Oracle Cloud Infrastructure Security Testing Policies[7]
- Oracle Cloud Services Contracts[8]
- Oracle Data Processing Agreement[9]
- Oracle Cloud Services Agreement[10]

## 免責事項

このドキュメントには、ソフトウェアまたは印刷物などの形式を問わず、オラクルが独占的な権利を有する財産的情報が含まれています。この機密資料へのアクセスと使用は、オラクルとの間で締結され遵守に同意したオラクル・ソフトウェア・ライセンスおよびサービス契約の条件に従うものとします。このドキュメントとその内容の開示、コピー、複製および配布には、オラクルによる事前の承諾を必要とします。このドキュメントはライセンス契約の一部となるものではなく、オラクルおよびその子会社や関連会社との契約を構成するものではありません。

このドキュメントは情報提供のみを目的としており、記載した製品機能の実装およびアップグレードの計画を支援することのみを意図しています。このドキュメントはマテリアルやコード、機能の提供をコミットメント（確約）するものではないため、購買決定を行う際の判断材料になさらないで下さい。このドキュメントに記載されている機能の開発、リリース、および時期については、弊社の裁量により決定されます。

製品アーキテクチャの性質により、コードの大幅な不安定化を招くリスクを冒さずに本書に記載されているすべての機能を安全に組み込むことは不可能な場合もあります。

---

[1] https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf
[2] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_guide.htm
[3] https://www.oracle.com/corporate/security-practices/
[4] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/ecs-security-guide.html
[5] https://docs.oracle.com/en-us/iaas/autonomous-database/doc/security-features-adb-d.html
[6] https://docs.oracle.com/en/cloud/paas/autonomous-database/adbsa/gs-security-and-authentation-autonomous-database.html
[7] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm
[8] https://www.oracle.com/corporate/contracts/cloud-services/
[9] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
[10] https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#online

# 目次



# 図一覧

## 表一覧



## はじめに

Exadata Database Service on Dedicated Infrastructure (ExaDB-D)は、Oracle Cloud Infrastructure (OCI)データ・センターでオラクルの Exadata Database Machine をサービスとして提供します。ExaDB-D の利点は、Exadata Database Machine の機能に加えて、OCI のオーケストレーション・ツールや管理ツール、Oracle Cloud Ops によるインフラストラクチャ保守サポートも利用できることです。

ExaDB-D は、Exadata Database Machine の可用性、パフォーマンスおよび機能とセキュリティによって、クラウド・サービスの運用価値と財務価値を得ようとするユース・ケースに適したデータベース・サービスです。

ExaDB-D のサービス・デリバリ・モデルは、お客様のデータとミッションクリティカルなワークロードの保護を目的とした、業界のベスト・プラクティスに基づく標準的なサービスです。お客様が ExaDB-D のサービス・デリバリ・モデルを容易に採用できるように、このドキュメントでは、お客様が承認したセキュリティ標準が ExaDB-D のモデルと異なる可能性のあるエッジ・ケースでの補償措置として、ExaDB-D のセキュリティ統制について説明します。このドキュメントの目的は、お客様のセキュリティ・チームが統制を使用して過去の標準に対する例外を認め、統制に基づいて将来の標準を策定できるように、統制について説明することです。

## コンプライアンス

オラクルは、社内のある業務部門が 1 つ以上のサービスについて第三者による証明や認証を受けた際のフレームワークに関する情報を「アテステーション」の形で提供しています。このアテステーションは、該当する Oracle クラウド・サービスのセキュリティ、プライバシーおよびコンプライアンスの統制について独立した評価を提供しているため、コンプライアンスとレポート作成の助けとなります。この第三者によるアテステーションを検討するうえで重要なのは、それが一般的に特定のクラウド・サービスに固有の内容であり、特定のデータ・センターや地理的リージョンに固有の内容である可能性もあることを考慮することです。Oracle Cloud Compliance ドキュメント[11]にアクセスすると、ExaDB-D の特定の標準に関連する詳細情報を入手できます。この情報は変更されることがあり、頻繁に更新される可能性があり、保証なしで「現状のまま」提供され、契約を構成するものではないことに注意してください。

コンプライアンスに関するドキュメントは、オラクルの営業担当者にリクエストすることも、OCI クラウド・コンソールから直接アクセスすることもできます。[12]

## オラクルの契約

『Oracle Data Processing Agreement』[13]はオラクルが ExaDB-D を含むオラクルのサービスに関連するデータをどのように管理、保護、および処理するかを説明するもので、次が含まれます。

- 国境間データ転送
- セキュリティと守秘義務
- 監査権
- インシデント管理および侵害通知

[11] https://www.oracle.com/cloud/compliance/#attestations
[12] https://docs.oracle.com/en-us/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm
[13] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf

『Oracle Cloud Services Agreement』[14]は、Oracle Cloud Services で処理されるお客様データに関する次のような情報などを提供します。

- 所有権および制限事項
- 非開示
- コンテンツの保護
- サービスの監視と分析
- 輸出
- 不可抗力
- 準拠法および管轄裁判所

Oracle Trust Center[15]は、オラクルのセキュリティ、コンプライアンス、プライバシ、および商業契約に関するインデックスを提供します。

## オラクルの企業セキュリティ・ポリシー

オラクルのセキュリティ・ポリシーは、オラクルの社内業務とオラクルがお客様に提供するサービス(ExaDB-D サービスを含む)の両方のセキュリティ管理を対象としており、従業員や請負業者など、オラクルの全スタッフに適用されます。これらのポリシーは、ISO/IEC 27002:2013 (旧 ISO/IEC 17799:2005)規格と ISO/IEC 27001:2013 規格に準拠しており、オラクル内のあらゆるセキュリティ領域の指針となります。オラクルが公開している企業セキュリティ慣行[16]には、次の情報が含まれています。

- 目的[17] - オラクルとお客様双方のデータの機密性、完全性および可用性の保護を支援
- 人事のセキュリティ[18]
- アクセス制御[19]
- ネットワーク通信のセキュリティ[20]
- データのセキュリティ[21]
- ラップトップおよびモバイル・デバイスのセキュリティ[22]
- 物理的・環境的セキュリティ[23]
- サプライ・チェーンのセキュリティと保証[24]

## オラクルの脆弱性開示ポリシー

オラクルはポリシーとして、脆弱性の詳細について、クリティカル・パッチ・アップデートまたはセキュリティ・アラートの通知、インストール前ノート、readme ファイルおよび FAQ に記載された内容以上の追加情報を提供しません。[25]オラクルは、すべてのお客様を公平に保護するために、すべてのお客様に同じ情報を提供します。オラクルがクリティカル・パッチ・アップデートまたはセキュリティ・アラートについての事前通知もしくは「インサイダー情報」を個々のお客様にお送りすることはありません。最後に、オラクルは、弊社製品の脆弱性に関するアクティブなエクスプロイト・コード（または概念実証コード）の開発あるいは配布は行いません。

オラクルの『Critical Patch Updates, Security Alerts and Bulletins』[26]ページには、『Critical Patch Updates, Security Alerts and Bulletins』で行われたセキュリティ修正のお知らせがリストされています。これは、新しいクリティカル・パッチ・アップデート・アドバイザリ、セキュリティ・アラートおよび速報がリリースされると更新されます。クリティカル度が高いために次のクリティカル・パッチ・アップデートで配布されるまで待つことができないと見なされた脆弱性の修正については、オラクル

---

[14] https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#online
[15] https://www.oracle.com/trust/
[16] https://www.oracle.com/corporate/security-practices/corporate/
[17] https://www.oracle.com/corporate/security-practices/corporate/objectives.html
[18] https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
[19] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[20] https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html
[21] https://www.oracle.com/corporate/security-practices/corporate/data-protection/
[22] https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
[23] https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
[24] https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
[25] https://www.oracle.com/corporate/security-practices/assurance/vulnerability/disclosure.html
[26] https://www.oracle.com/security-alerts/#CVEOtherDocs

はセキュリティ・アラートを発行します。このアラートの履歴は、『Critical Patch Updates, Security Alerts and Bulletins』ページに掲載されています。

ExaDB-D などのクラウドのお客様が、クリティカル・パッチ・アップデート・アドバイザリに記載されていない情報を必要とする場合は、所定のサポート・システム内で My Oracle Support サービス・リクエスト(SR)を送信することで、情報を入手できる場合があります。

## 役割と責任

ExaDB-D は、お客様とオラクルが共同で管理します。ExaDB-D のデプロイメントは、2 つの責任領域に分けられます。

- お客様が管理するサービス: お客様が ExaDB-D のサブスクリプションの一部としてコントロールできるコンポーネント
  - お客様がアクセスできる仮想マシン(VM)
  - お客様がアクセスできるデータベース・サービス
- オラクルが管理するインフラストラクチャ: お客様がアクセスできるサービスを実行するために、オラクルが所有し運用するハードウェア
  - 配電ユニット(PDU)
  - 帯域外(OOB)管理スイッチ
  - ストレージ・ネットワーキング・スイッチ
  - Exadata Storage Server
  - 物理的な Exadata Database Server
- オラクルが管理するクラウド・コントロール・プレーン・サービス
  - お客様の Web UI および API インタフェース
  - 一般にアクセス可能なサービスとエンドポイント(OCI クラウド・サービスなど)
  - プライベートにアクセス可能なエンドポイント(OCI Fast Connect など)
  - OCI クラウド・サービスのオーケストレーションを目的とする OCI クラウド自動化

お客様は、お客様のサービスへのアクセスを制御し、監視します。これには、OCI 仮想クラウド・ネットワーク(VCN)[27]を介した VM へのネットワーク・アクセス、OCI ネットワーク・セキュリティ・リスト[28]、OCI VCN フロー・ログ[29]、トークンベースの ssh[30]による VM へのアクセスの認証、Oracle データベースの認証方式[31]による VM で実行中のデータベースへのアクセスの認証が含まれます。オラクルは、オラクルが管理するインフラストラクチャ・コンポーネントへのアクセスを制御し、監視します。オラクルのスタッフには、お客様のサービス(お客様の VM やデータベースを含む)にアクセスする権限はありません。表 1 は、オラクルとお客様が担う役割と責任の分担を簡単にまとめたものです。詳細は、「Exadata Database on Dedicated Infrastructure Service Description」[32]と「Exadata Database Service on Dedicated Infrastructure - Explanation of Cloud Operations Service (Doc ID 2875973.1)」[33]に記載されています。

*表 1: 役割と責任*

| 職務 | オラクルが管理するインフラストラクチャ | | お客様が管理するサービス | |
|---|---|---|---|---|
| | Oracle Cloud Ops | お客様 | Oracle Cloud Ops | お客様 |
| **監視** | インフラストラクチャ、コントロール・プレーン、ハードウェア障害、可用性、容量 | 該当なし | お客様のサービスをお客様が監視できるようサポートするためのインフラストラクチャの可用性 | お客様の OS、データベース、VM およびアプリケーションの監視 |

[27] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/overview.htm
[28] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/securitylists.htm#Security_Lists
[29] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/vcn_flow_logs.htm
[30] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/exaconnectingDB.htm
[31] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/exaconnectingDB.htm
[32] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/exa-service-desc.html
[33] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2875973.1

| | | | | |
|---|---|---|---|---|
| **インシデントの管理と解決** | インシデントの管理と是正<br>スペア部品と現場派遣 | 該当なし | 基盤となるプラットフォームに関連するあらゆるインシデントのサポート | お客様のアプリケーションのインシデントの管理と解決 |
| **パッチ管理** | ハードウェア、IaaS コントロール・ソフトウェア、ハイパーバイザ、およびオラクルが管理する対象インフラストラクチャ・コンポーネントへの予防的パッチ適用 | 該当なし | Exadata Database Service on Dedicated Infrastructure のメンテナンス[34]に関するドキュメントに準拠した使用可能なパッチ(Oracle DB パッチ・セットなど)のステージング | テナント・インスタンスへのパッチ適用<br>テスト |
| **バックアップとリストア** | インフラストラクチャとコントロール・プレーンのバックアップとリカバリ、お客様の VM の再作成 | 該当なし | お客様がアクセスできる実行中の VM の提供 | Oracle ネイティブまたはサードパーティの機能を使用したお客様の IaaS データのスナップショット/バックアップとリカバリ |
| **クラウド・サポート** | インフラストラクチャやサブスクリプションの問題に関連した SR への対応と解決 | My Oracle Support (MOS)を介した SR の送信 | SR への対応と解決 | My Oracle Support (MOS)を介した SR の送信 |

## EXADB-D サービスのアーキテクチャ

ExaDB-D サービスは、お客様が選択した OCI データ・センターにある Exadata Database Server および Storage Server の複数のラックにまたがってデプロイされます。ExaDB-D ラックには、標準的な Exadata Database Machine のすべてのコンポーネントと OCI VCN をサポートするネットワーキング・ハードウェアが含まれています。物理的な Exadata ラックとネットワーキング・インフラストラクチャは、複数のテナント(お客様)間で共有される場合があります。Exadata Database Server と Exadata Storage Server は、単一のテナント(お客様)専用です。

お客様のデータベース・データは、OCI データ・センターにある ExaDB-D Database Server および Storage Server で保護されています。また、お客様のデータベースへのお客様のアクセスはすべて、お客様が ExaDB-D ラック内の VM とデータベースへのアクセスを許可したネットワーク接続(VCN)を介して行われます。お客様の VM とお客様のデータベースにアクセスするための資格証明は、お客様が保持し、コントロールします。お客様は、お客様の VM とデータベースへの特権アクセス(お客様の VM オペレーティング・システムでの root、Oracle データベースでの SYS など)を持ち、それらの資格証明を使用して VM とデータベースを保護し、ポリシーの要件や規制要件に対応することができます。これには、エージェントをインストールする、オペレーティング・システムおよびデータベースの監査ログをお客様のセキュリティ情報イベント管理(SIEM)に転送する、ExaDB-D コンピュート VM オペレーティング・システムおよび Oracle データベースと互換性のあるツールを使用して、VM とデータベースへのアクセス制御とアイデンティティ管理を行うなどの作業が含まれますが、これらに限定されません。

お客様は、Oracle Cloud Infrastructure コンソールと REST API を使用して、ExaDB-D とデータベース・サービスをデプロイし、管理します。お客様は、OCI Identity and Access Management (IAM)[35]サービスを介して、クラウド自動化の管理機能へのアクセスを制御します。OCI Audit[36]サービスは、OCI コンソールまたは OCI REST エンドポイント経由で呼び出された、お客様が開始するすべての管理アクション(データベースの作成や削除など)のレコードをお客様に提供します。お客様は、OCI 仮想クラウド・ネットワーク[37]を介して、ExaDB-D のお客様の VM や ExaDB-D サービス上で実行されているデータベース・サービスへのネットワーク・アクセスを制御します。オラクルは、クラウド自動化とサービスをメンテナンスする必要があるオラクル・スタッフの ExaDB-D インフラストラクチャへのネットワーク・アクセスを制御します。

[34] https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/examaintenance.htm
[35] https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm
[36] https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm
[37] https://www.oracle.com/cloud/networking/virtual-cloud-network/

## ネットワーク・ブロック図

図 1 は、ExaDB-D のネットワーク・アーキテクチャのブロック図を簡単に表したものです。詳細は、「Oracle Exadata Database Service on Dedicated Infrastructure Technical Architecture」[38]製品ドキュメントに記載されています。お客様がアクセスでき、お客様がコントロールするコンポーネントは青で示しています。オラクルが管理し、特定のお客様専用(単一テナント)のコンポーネントは赤で示しています。オラクルが管理し、OCI テナント間で共有されるインフラストラクチャは緑で示しています。ExaDB-D Database (DB) Server および Storage Server (赤で表示)は、分離されたレイヤー2 管理ネットワーク(同じく赤で表示)を介して相互接続されます。管理ネットワークからお客様のクライアント・ネットワークおよびバックアップ・ネットワークへの直接のネットワーク・アクセスは発生しません。

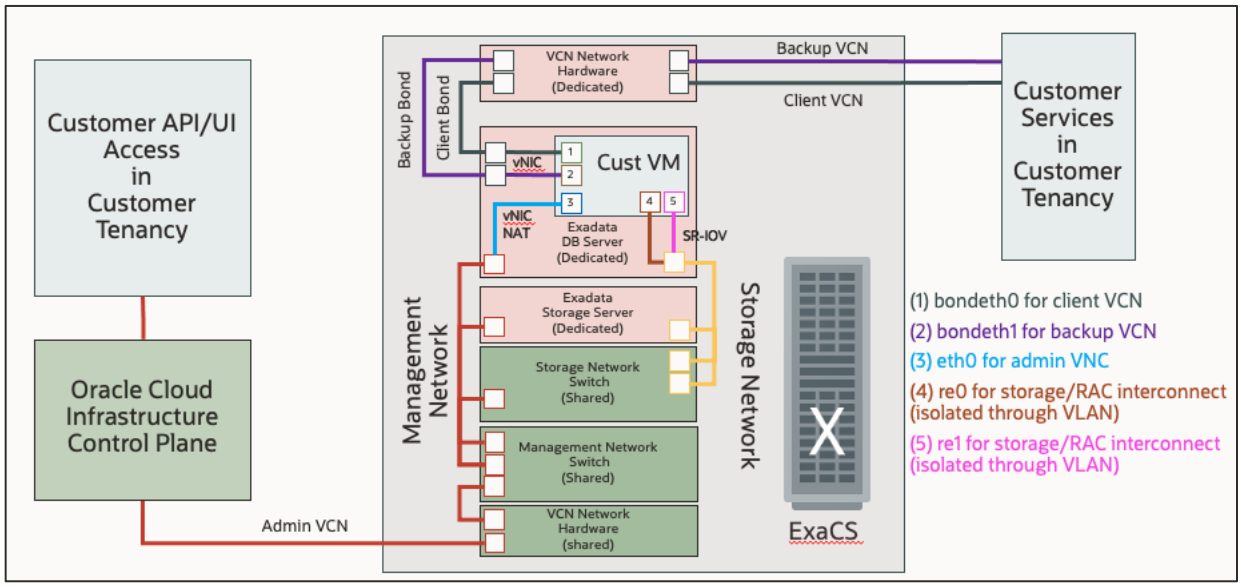


*図 1:Oracle Exadata Database Service on Dedicated Infrastructure のネットワーク・アーキテクチャのブロック図*

Exadata Database Server は、特殊な VCN ネットワーキング・ハードウェアを介して OCI ネットワーキング・インフラストラクチャに接続されます。オラクルが管理するインフラストラクチャ用のネットワーキング・ハードウェア(お客様/テナント間で共有)は緑で示し、お客様のサービス用のネットワーキング・ハードウェア(お客様/テナント専用)は赤で示しています。お客様は、OCI VCN として実装され、vNIC としてお客様の仮想マシン(お客様の VM)にマッピングされているクライアント・ネットワークおよびバックアップ・ネットワークを介して、お客様の仮想マシン(お客様の VM)にアクセスできます。物理ネットワーク接続は、高可用性を確保するために、Oracle Cloud Operations が管理するアクティブ/スタンバイ構成で実装されます。物理的なネットワーク・リンク障害が発生した場合、Oracle Cloud Operations は必要なリカバリ手順を実行してネットワーク接続を回復します。これにより、ネットワークの停止時間が短縮される場合もあります。

お客様の VM は、SR-IOV でマッピングされたインタフェース経由で、ルーティングを行わないプライベートのインターコネクト・ネットワークを介して、Exadata ストレージにアクセスします(黄色で表示)。物理的な Exadata Database Server および Storage Server はそれぞれ、冗長なストレージ・ネットワーキング・スイッチのペアへの高可用性(HA) (アクティブ/スタンバイ)接続を有しています。

Oracle クラウド自動化機能の一部が、Exadata Database Server の vNIC に実装された管理 VCN 上の NAT アドレスを介して、お客様の VM にアクセスします(青で表示)。Oracle クラウド自動化からお客様の VM へのアクセスは、トークンベースの ssh を介して制御されます。お客様が開始する管理アクションごとに、お客様の VM にアクセスするために、一時的な一意の ssh 鍵ペアが Oracle クラウド自動化によって生成されます。公開鍵は、クラウド自動化により、DBCS エージェントを通じて、お客様の VM で必要なサービス・アカウント(`oracle`、`opc`、`root` など)の`~/.ssh/authorized_keys` ファイルに挿入されます。自動化によって使用される一時的な秘密鍵は、お客様のデータ・センターにある ExaDB-D ハードウェアで実行中の Oracle クラウド自動化ソフトウェアによってメモリーに格納され、アクションの完了後に破棄されます。同様に、一時的な公開鍵は、アクションが完了すると、クラウド自動化ソフトウェアによってサービス・アカウントから削除されます。

実行中のプロセス、TCP ポート番号、およびお客様の VM にデプロイされている実行中のプロセスのユーザーID について説明したポート・マトリックスが「Oracle Exadata Database Service on Dedicated Infrastructure のセキュリティ・ガイド」[39]で公

[38] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecsid/
[39] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/ecs-security-guide.html

開されています。このガイドは Exadata Cloud Infrastructure のセキュリティについて説明したもので、Exadata Cloud Infrastructure を保護するためのベスト・プラクティスに関する情報が含まれています。

## ExaDB-D サービスへのお客様のアクセス

お客様は、Oracle データベース(DB)の標準的な接続方法(TCP ポート 1521 での Oracle Net など)を使用し、お客様のエンドポイントからお客様の VM で実行中のデータベースへの OCI VCN 接続を介して、ExaDB-D で実行中の Oracle データベースにアクセスします。お客様は、Oracle Linux の標準的な方法(TCP ポート 22 でのトークンベースの ssh など)で、Oracle データベースが実行されている VM にアクセスします。[40]

OCPU のスケーリングや仮想マシン(VM)クラスタの作成といったインフラストラクチャ・コンポーネントの管理アクションは、OCI コントロール・プレーンでホストされているクラウド自動化を利用してお客様が実行します。Oracle PaaS and IaaS Public Cloud Pillar Documentation[41]で公表されている 99.95%のサービス・アップタイムをサポートするインフラストラクチャ管理はオラクルが実行するため、お客様がインフラストラクチャ・レイヤーを管理する必要はありません。お客様には、ExaDB-D インフラストラクチャに直接アクセスしたり、監視エージェントをロードしたり、ExaDB-D サービスでオラクルが管理するインフラストラクチャに対してファイルを直接プルまたはプッシュしたりする権限はありません。

お客様の OCI Identity and Access Management (IAM)統制は、お客様の VM とデータベースに対してお客様が Oracle クラウド自動化機能を実行できるかどうか、どのように実行するかを管理します。お客様の VM には、クラウド自動化による ssh アクセスの検出など、Oracle Linux の監査システムを介した発見的アクセス統制が実装されています。お客様は、レイヤー3 および 4 でのクラウド自動化による ssh アクセスを、お客様の VM でのファイアウォール構成によってブロックできます。ただし、これを行うと、ssh 経由でお客様の VM にアクセスする必要のあるクラウド自動化機能が動作しなくなります。この機能には次のものが含まれます。

- データベースへのパッチ適用
- Grid Infrastructure へのパッチ適用
- お客様の VM OS へのパッチ適用
- オラクルが管理するインフラストラクチャへの四半期ごとのパッチ適用(お客様の VM での CRS 再起動の検証に使用)
- Database Server Infrastructure の追加
- VM クラスタ・ノードの追加
- VM クラスタ・ノードの削除
- Storage Server の追加

Oracle クラウド自動化のアクセスは、お客様の VM とお客様のデータベースへのアクセスに必要な一部の機能をお客様が許可すれば、一時的に復旧できます。Oracle クラウド自動化は、OCPU のスケーリングを実行する際に、お客様の VM へのネットワーク・アクセスを必要としません。OCPU のスケーリング機能は、Oracle クラウド自動化によるお客様の VM へのネットワーク・アクセスをお客様がブロックしても、正常に動作します。

## OCI インタフェースへのお客様のアクセス

お客様は、OCI コントロール・プレーンへのポート 443 の https 接続を介して、OCI テナンシのクラウド自動化サービスにアクセスします。OCI コントロール・プレーンは、次の管理インタフェースを提供します。

- Web ユーザー・インタフェース(Web UI) - 通常は非定型アクションで使用
- Oracle クラウド・シェル - Oracle Cloud Infrastructure コンソールで直接使用できる Linux シェル
- OCI コマンドライン・インタフェース(OCI CLI) - 通常はオペレーティング・システム・シェルからのプログラム的なアクションで使用
- REST API (OCI ソフトウェア開発キット(OCI SDK)) - 通常はアプリケーション統合で使用

OCI Terraform プロバイダ[42]を ExaDB-D のデプロイと管理に使用できます。Hashicorp Terraform ソフトウェアのドキュメントは、Hashicorp から入手できます。[43]

---

[40] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/ecs-connect-to-service-instance.html#GUID-53DE1ED5-96D9-4F7F-B57F-4EF8D01FCDCB

[41] https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf

[42] https://docs.oracle.com/en-us/iaas/Content/API/SDKDocs/terraform.htm

[43] https://registry.terraform.io/providers/hashicorp/oci/latest/docs

すべての管理インタフェースへのアクセスは、OCI Identity and Access Management (IAM)のポリシーを介してお客様が制御します。お客様が管理するアイデンティティに、リクエストされたアクションを実行する権限がある場合、そのアクションは、適切な ExaDB-D コンポーネントに次のように提供されます。

- DBaaS UI/API が、https 経由でリクエストを DB コントロール・プレーンに送信する
- DB コントロール・プレーンが、リクエストを REST API 経由で ExaDB-D の管理 VCN に送信する
  - お客様の VM のデータベース・サービスへのアクセスを必要とするアクションは、OCI コントロール・プレーンと各 DB エージェントの間のセキュアな接続(mTLS)経由で、お客様の VM のいずれか、またはすべて(たとえば、ハーフ・ラックには最大 4 つの VM があります)で実行されている DB エージェントに送信されます。この mTLS 接続は、ExaDB-D ラック内のプライベート・インターコネクト・ネットワークを介して実装されています。お客様の VM で実行されているソフトウェア・プロセスのポート・マトリックスが「Exadata Database Service on Dedicated Infrastructure のセキュリティ・ガイド」[44]で公開されています。
  - お客様の VM へのアクセスを必要とするアクションは、Exadata Database Server からアクセスできるお客様の VM 上の NAT アドレスとして実装されている内部管理ネットワーク経由で、トークンベースの `ssh` を使用して実行されます。公開 `ssh` 鍵は一時的なもので、お客様が呼び出した管理アクションのために生成され、お客様の VM で `oracle`、`opc`、`grid` および `root` ユーザーの `authorized_keys` ファイルに格納されます。秘密 `ssh` 鍵は一時的なもので、お客様が呼び出した管理アクションのために生成され、お客様のデータ・センターにある Exadata ハードウェアで実行中の Oracle クラウド自動化ソフトウェアによってメモリーに格納されます。
  - インフラストラクチャ・コンポーネントへのアクセスを必要とするアクションは、必要なエンドポイント(Exadata Storage Server、Exadata Database Server など)への内部管理ネットワーク経由で、トークンベースの `ssh` を使用して発行されます。

オラクルは、インフラストラクチャとお客様の VM コンポーネントの管理に使用される秘密 `ssh` トークンを管理し、コントロールします。これらのトークンは、OCI コントロール・プレーンに格納され、保護されます。インフラストラクチャのトークンは一意であり、インフラストラクチャ・コンポーネント(Exadata Storage Server、物理的な Exadata Database Server、ストレージ・ネットワーク・スイッチなど)へのアクセスのみを提供します。お客様の VM やデータベースへのアクセスは提供しません。お客様の VM のトークンは特定の管理アクションに対して一意であり、お客様の VM へのアクセスのみを提供します。

## オラクルのインフラストラクチャ監視

オラクルは、Oracle Support ドキュメント 2875973.1 (Exadata Database Service on Dedicated Infrastructure - Explanation Of Cloud Operations Service)[45]に示すように、監視を行って、オラクルによる対処が可能な場合はアラートを生成します。オラクルは、Exadata Database Machine アラート・メカニズムを介して、Exadata コンピュート(Dom0)、Exadata Cell、ネットワーク・スイッチおよびコントロール・プレーン・サーバー(CPS)を含むインフラストラクチャ・レイヤーを監視します。ノードの可用性、ディスクの利用状況、ネットワーク・デバイスなどに関する追加の監視が実装されています。

オラクルは、オラクルによる対処が可能ではないパフォーマンス・メトリックは監視しません。たとえば、フラッシュ・キャッシュの使用量、IO の使用率などです。オラクルは、ゲスト VM、CRS、ASM、データベースや、ゲスト OS で実行中のその他のソフトウェアを監視しません。ゲスト VM、CRS/DB などを監視する責任はお客様が負います。

ExaDB-D インフラストラクチャ・コンポーネントは、OCI コントロール・プレーンの監視サーバーにインフラストラクチャ管理メトリック(IMM)をレポートします。Oracle Support は、ExaDB-D の実装の監視と保守を次のように実行します。

- Oracle Cloud Service インフラストラクチャ・コンポーネントの自動監視により、インフラストラクチャ監視メトリック(IMM)が OCI コントロール・プレーンの監視サーバーに送信されます。
  - シャーシの温度、ドライブのステータスなど。
  - すべての監視データの詳細は、「Auto Service Request Qualified Engineered Systems Products」[46]で公開されています。
- Oracle Support は、監視データを分析して、どのイベントの修正が必要かを判断し、サポート・チケットを作成し、サポート・チケットを OCI サポート・スタッフに割り当てます。
- チケットが割り当てられると、Cloud Ops サポート・スタッフに権限が与えられて派遣され、必要なサポート行為を実施します。

[44] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/ecs-security-guide.html
[45] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2875973.1
[46] https://docs.oracle.com/cd/E37710_01/doc.41/e37287/toc.htm

## 四半期ソフトウェア・アップデート

Oracle データベース、Grid Infrastructure、およびお客様の VM オペレーティング・システムに対する標準の四半期バンドル・パッチは、オラクルによって OCI Object Storage にステージングされます。四半期ごとのソフトウェア・アップデートは、お客様向けにクラウド自動化ユーザー・インタフェースに一覧表示され、それらのパッチの適用は、OCI のツールとポリシーを使用してお客様がコントロールします。パッチは、オラクルが管理する OCI Object Storage から直接アクセスされます。四半期ごとのパッチ情報は、オラクルの「Critical Patch Updates, Security Alerts and Bulletins」[47]で提供されます。My Oracle Support ドキュメント 2333222.1 の「Exadata Cloud Software Versions」[48]に、ExaDB-D で使用可能な現在および過去のソフトウェア・バージョンに関する情報が記載されています。Oracle Cloud Infrastructure のメンテナンスに関するドキュメント[49]には、インフラストラクチャ更新プロセスについての説明があり、「Exadata Cloud Infrastructure システムのパッチ適用および更新」ドキュメント[50]には、お客様の VM、Grid Infrastructure および Oracle データベース・ソフトウェアに対するお客様が管理する更新プロセスについての説明があります。

インフラストラクチャ・コンポーネントのソフトウェア・アップデートは、特定のソフトウェア・アップデートでの必要性に応じて、Oracle クラウド自動化とオラクルのスタッフによってデプロイされます。アップデートは、可能であれば、Linux ksplice などのツールを使用して、実行中のシステムにダウンタイムなしで適用されます。アップデートの際にコンポーネントの再起動が必要な場合(四半期ごとのパッチ・イベントでは一般的です)、オラクルはコンポーネントの再起動を Real Application Cluster (RAC)のローリング方式で実行して、アップデート・プロセスでのサービスの可用性を確保します。

## 月次セキュリティ・スキャンおよびアップデート

四半期ごとのメンテナンスと一緒に実行されるセキュリティ・メンテナンス[51]は、重要なセキュリティ・アップデートが必要な月に行われ、CVSS スコアが 0 を超える脆弱性の修正を含んでいます。

セキュリティ・メンテナンスは、必要に応じて、各月の 15 日より後に始まる 21 日間の期間中に適用するようにスケジュールされます。お客様は、月次メンテナンス期間の開始日より 7 日以上前に、スケジュール案の通知を受け取ります。月次メンテナンスは、必要に応じて、期間内の別の日にスケジュールしなおすことができます。月次セキュリティ・メンテナンスには、それまでの月のスキャンで特定されたすべてのセキュリティ脆弱性の修正が含まれます。データベース・サーバーのアップデートが Ksplice テクノロジーによってオンラインで適用されるのに対し、ストレージ・サーバーのアップデートはローリング方式で適用されます。「Oracle 管理インフラストラクチャ・メンテナンスの構成」製品ドキュメント[52]に、ExaDB-D のメンテナンスをスケジュールして実行する方法が詳しく記載されています。

## ソフトウェア・アップデートのセキュリティ・コントロール

すべてのソフトウェア・アップデートは、Oracle Software Security Assurance Practices[53]によってコントロールされます。Oracle Software Security Assurance[54]の基準が ExaDB-D ソフトウェアに適用されます。オラクルは、ソフトウェア開発、ソフトウェアのテストと品質保証、および ExaDB-D のソフトウェア・コンポーネントのデプロイメントにおいて、職務分掌[55]を実施しています。

# 予防的統制

ExaDB-D サービスは、お客様のサービスとデータベース・データを不正アクセスから隔離し保護するように設計されています。ExaDB-D サービスでは、アクセス制御に関する職務がお客様とオラクルの間で分掌されます。お客様は、お客様のサービス、データベースおよびデータベース・データへのアクセスを制御します。オラクルは、オラクルが管理するインフラストラクチャ・コンポーネントへのアクセスを制御します。

---

[47] https://www.oracle.com/security-alerts/
[48] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2333222.1
[49] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/exa-conf-oracle-man-infra.html#GUID-C4301E26-E809-438F-96D7-9C6BB02FEA7F
[50] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/ecs-patch-update.html
[51] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/exa-conf-oracle-man-infra.html#GUID-A2008207-3683-424F-9279-F632BF4C9076
[52] https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/examaintenance.htm
[53] https://www.oracle.com/corporate/security-practices/assurance/
[54] https://www.oracle.com/corporate/security-practices/assurance/
[55] https://www.oracle.com/corporate/security-practices/corporate/access-control.html

## お客様のアクセス統制

お客様は、3 種類の統制を使用して、お客様の VM、データベースおよびデータへのアクセスを制御します。

- ユーザー認証
  - OCI サービスにアクセスするための資格証明
  - お客様の VM オペレーティング・システムとデータベース管理アカウントへの資格証明
  - データベース・ユーザーがデータベースとデータベース・データにアクセスするための資格証明
- ネットワーク・アクセス
  - レイヤー2 および 3 でのお客様の VM へのアクセスを制御するための OCI VCN とセキュリティ・リスト
  - お客様の VM オペレーティング・システムと Oracle データベースに実装されたネットワーク・アクセス・ルール
- データベース暗号化
  - アプリケーションからデータベースへの暗号化[56]
  - ユーザー表領域の Transparent Database Encryption (TDE)[57]

## ExaDB-D サービスでのお客様のアクセス制御

お客様は、OCI 自動化を介して、お客様が選択した OCI リージョンの Oracle Cloud コントロール・プレーンへの https 接続を確立することで、管理アクションを実行します。お客様は、OCI Identity and Access Management (IAM)[58]の資格証明を使用して認証され、お客様のアクションは、特定のリソースに対してお客様が構成した OCI IAM の権限によってコントロールされます。お客様のユーザーに、リクエストされた管理アクションをターゲット・リソースに対して実行する権限がある場合、リクエストされたコマンドは、オラクルがコントロールするサービスの VCN によって、適切な ExaDB-D コンポーネントに送信されます。

お客様とデータベース・アプリケーションは、お客様の VM にアタッチされた OCI VNIC を介して、ExaDB-D で実行中のデータベースにアクセスします。データベースとオペレーティング・システムへのアクセスは、お客様が管理する資格証明を使用して行われます。[59]

## データ・セキュリティに対するお客様の統制

ExaDB-D は、お客様が許可する用途でデータを保護し、不正な使用からデータを守ることができるように設計されています。これにより、Oracle Cloud Ops のスタッフがお客様のデータにアクセスすることも防止されます。ExaDB-D インフラストラクチャ、お客様の VM、および Oracle データベースのデータに対する不正アクセスを防ぐよう設計されたセキュリティ対策には、以下が含まれます。

- お客様は、名前付きの特権(SYS、SYSTEM など)ユーザーの認証とお客様のデータベースへのアクセスに対する統制を保持します。
- お客様は、名前付きの特権(root、opc、oracle、grid など)ユーザーの認証とお客様のデータベースへのアクセスに対する統制を保持します。
- お客様の VM へのアクセスは、お客様の VM オペレーティング・システムによってログに記録されます。お客様はこれらのログを利用でき、お客様が選択した他のセキュリティ情報イベント管理(SIEM)システムに送信できます。
- お客様は、Linux カーネルを変更したり、Exadata の運用を阻害したりしないかぎり、任意の監視エージェントやセキュリティ統制をお客様の VM オペレーティング・システムにインストールできます。[60]
- Oracle データベースへのネットワーク接続は、クラウド自動化によって自動的に構成される Oracle Native Network Encryption によって保護されるように設計されています。

---

[56] ExaDB-D の自動化により、Oracle Native Network Encryption が構成されます。オラクルは、お客様がこの統制を維持することを強く推奨します。

[57] ExaDB-D の自動化により、Oracle Transparent Data Encryption (TDE)が構成されます。オラクルは、お客様がこの統制を維持することを強く推奨します。

[58] https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm

[59] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/exaconnectingDB.htm

[60] オラクルは、サードパーティ・ソフトウェアを ExaDB-D でテストすることもサポートすることもありません。お客様は、サードパーティ・プロバイダが自社のソフトウェアを ExaDB-D でテストし検証していること、またサードパーティ・プロバイダが自社のソフトウェアを ExaDB-D でサポートできることをサードパーティ・プロバイダに対して確認する必要があります。

- Oracle ユーザー表領域のデータベース・データは、Oracle Transparent Data Encryption (TDE)鍵によって保護されます。
  - この鍵は、クラウド自動化によって自動的に構成され、お客様の VM のファイル・システムに格納されている、パスワードで保護された PKCS12 ウォレット・ファイルに格納されます。
  - お客様は、ウォレットのパスワードを使用して TDE 暗号化鍵へのアクセスを制御します。
  - お客様は、TDE マスター鍵を OCI Vault[61]サービスに移動して保護できます
- Oracle データベース・ソフトウェアの機能である Oracle Database Vault[62]をお客様が構成して、データベース管理者がユーザー・データにアクセスしないように保護することができます。

## 移動中、処理中、保管中のデータを保護するための統制

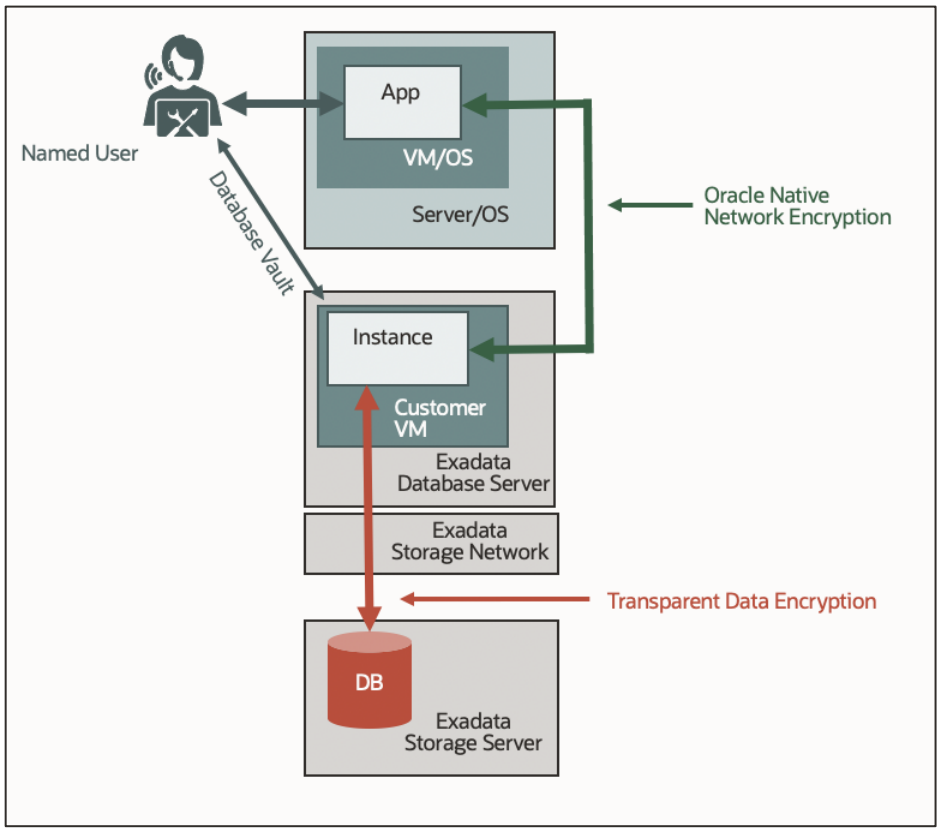


図 2 は、インフラストラクチャやお客様の VM のコンポーネントにアクセスできるユーザーやソフトウェアからお客様のデータがアクセスされないように保護する、Oracle データベース内の追加の統制を示しています。

- Oracle Native Network Encryption[63]
- Oracle Database Vault[64]
- Oracle Transparent Database Encryption (TDE)[65]

---

[61] https://www.oracle.com/security/cloud-security/key-management/
[62] Oracle Database Vault は、Enterprise Edition Extreme Performance のサブスクリプションに含まれています。Bring Your Own License (BYOL)のサブスクリプションには含まれていません。
[63] Enterprise Edition Extreme Performance のサブスクリプションと Bring Your Own License (BYOL)のサブスクリプションに含まれています。
[64] Enterprise Edition Extreme Performance のサブスクリプションに含まれています。Bring Your Own License (BYOL)のサブスクリプションには含まれていません。
[65] Enterprise Edition Extreme Performance のサブスクリプションと Bring Your Own License (BYOL)のサブスクリプションに含まれています。

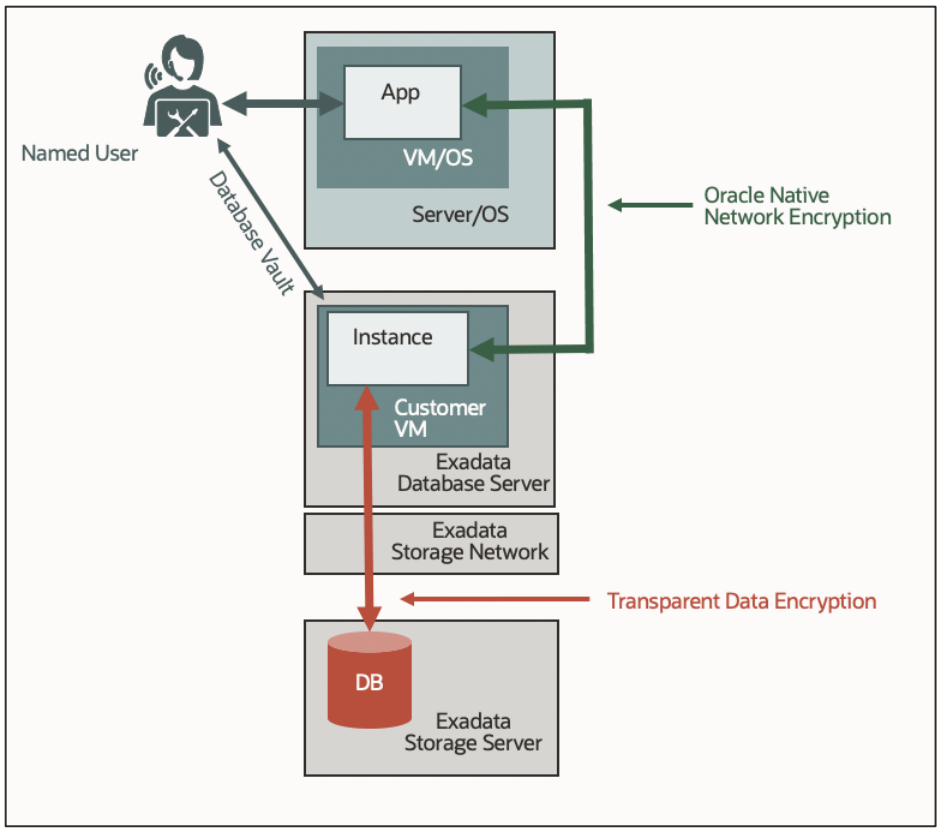


*図2:移動中、処理中、保管中のデータを保護するための統制*

### Oracle Native Network Encryption

Oracle Native Network Encryption は、アプリケーションと Oracle データベース・インスタンスの間で移動中のデータを暗号化し、ExaDB-D の自動化によって作成されたデータベース向けに自動的に構成されます。Oracle Native Network Encryption が有効になっている場合、お客様のデータは暗号化されるため、IP パケットとイーサネット・パケットを監視できるインフラストラクチャ・コンポーネントにアクセスできても、お客様のデータにはアクセスできません。Oracle Native Network Encryption および TLS/SSL のドキュメントは、各 Oracle Database バージョン向けのセキュリティ・ガイドで公開されています。たとえば、Oracle Database 19c の場合は、https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-network-data-encryption-and-integrity.html#GUID-7F12066A-2BA1-476C-809B-BB95A3F727CF を参照してください。ExaDB-D のクラウド自動化は、Oracle データベース接続用の TLS/SSL を構成するためのインタフェースを提供しません。お客様は、お客様の VM に導入された OS のツールを使用して TLS/SSL を設定することができます。

### Oracle Database Vault

Oracle Database Vault のセキュリティ統制は、データベース管理者のアクセスからアプリケーション・データを保護し、プライバシー要件や規制要件に対応できるように設計されています。統制をデプロイすることで、データベース管理者によるアプリケーション・データへのアクセスをブロックし、信頼できるパスの認可によってデータベース内部での機微な操作をコントロールできます。Oracle Database Vault では、既存のデータベース環境を透過的に保護できるため、コストと時間のかかるアプリケーション変更が不要になります。お客様は、Oracle データベース・ソフトウェアの方式によって Oracle Database Vault を構成し管理する責任を負います。Oracle Database Vault のドキュメントは、各データベース・バージョンの『Oracle Database Vault 管理者ガイド』[66]で公開されています。

### Oracle Transparent Data Encryption

Oracle Exadata Database Service on Dedicated Infrastructure (ExaDB-D)では、Oracle Transparent Data Encryption (TDE)を使用してデータベースの保管中のデータを保護します。TDE は、データ暗号化鍵とマスター暗号化鍵で構成される 2 層の鍵アー

[66] Oracle Database 19c の場合は、https://docs.oracle.com/en/database/oracle/oracle-database/19/dvadm/introduction-to-oracle-database-vault.html#GUID-0C8AF1B2-6CE9-4408-BFB3-7B2C7F9E7284 を参照してください。

キテクチャです。データ暗号化鍵は表と表領域を保護しますが、単一のデータベース・マスター暗号化鍵でラップされます。マスター鍵は暗号化されたデータから分離されて、データベースの外部に格納されます。TDE マスター鍵は、PKCS#12 規格に基づいた鍵格納ファイルである Oracle Wallet に格納できます。

Oracle TDE の詳細は、実行している Oracle データベースのバージョンの Advanced Security ガイドを参照してください。Oracle TDE の FAQ[67]には、Oracle TDE のアーキテクチャと実装に関するよくある質問への回答が用意されています。

ExaDB-D での TDE 実装の詳細は、Exadata Database Machine の暗号化サービス[68]に関するドキュメントに記載されています。

**OCI Vault を使用した ExaDB-D 向け Oracle TDE**

ExaDB-D は、Oracle Cloud Infrastructure (OCI) Vault サービスと統合されています。お客様は、セキュリティ体制の強化が求められるシステムでの追加の分離手段として、お客様の VM に格納されている Oracle Wallet ではなく、OCI Vault を使用して TDE 鍵を作成し管理できます。OCI Vault には次の利点があります。

- データベース・サービスとは別のハードウェア実装で TDE マスター鍵をコントロールし、管理
- 可用性が高く、耐久性に優れたマネージド・サービスに TDE 鍵を格納
- 連邦情報処理標準(FIPS) 140-2 セキュリティ・レベル 3 のセキュリティ認定に適合するハードウェア・セキュリティ・モジュール(HSM)で TDE 鍵を保護
- TDE 鍵のローテーションと暗号化操作の監査を自動的に行い、コンプライアンスと規制のニーズに対応

お客様が ExaDB-D の TDE 鍵を管理するには、まず Vault サービスにアクセスして、暗号化鍵を作成する必要があります。使用する暗号化鍵のアルゴリズムは AES-256 である必要があります。次に、Vault で鍵を管理するために必要な IAM ポリシーが設定されていることを確認する必要があります。前提条件となるこれらの手順が完了したら、お客様が管理する鍵で保護された Exadata データベースを作成できます。Oracle Database 11g リリース 2 (11.2.0.4)より後のデータベースのみがサポートされています。

**Oracle Key Vault (OKV)を使用した ExaDB-D 向け Oracle TDE**

お客様は、ExaDB-D データベースを、Oracle Database 資産のための唯一の鍵管理ソリューションである Oracle Key Vault (OKV)[69]に移行することも選択できます。Oracle Key Vault は、最大で 16 の OKV ノードを、地理的に分散されたデータ・センターや Oracle Cloud Infrastructure (OCI)にまたがる鍵管理クラスタに追加することで、鍵の継続的な可用性を実現します。Oracle Key Vault により、TDE 対応のすべてのデータベースと、暗号化された GoldenGate 証跡ファイルに、継続的なオンライン鍵管理機能が提供されます。外部で生成された鍵を取り込む機能(BYOK)も提供されます。

オラクルは、ExaDB-D 上で動作するデータベースの外部キー・ストアとして、Oracle Key Vault (OKV)を使用するお客様をサポートしています。OS 方式を使用して TDE マスター鍵を OKV に移行する手順は、「Migration of File based TDE to OKV for ExaDB-D Using Automation via REST (Doc ID 2924192.1)」[70]で公開されています。

OKV サーバーが使用できない場合に、OKV 永続マスター暗号化鍵キャッシュ[71]を使用して、データベースを稼働させるオプションもあります。

## お客様の VM へのクラウド自動化のネットワーク・アクセスに対する統制

Oracle クラウド自動化ソフトウェアは、2 つのアクセス方法でお客様のデータベースとお客様の VM にアクセスします。

- ポート 443 での mTLS 認証を介して、お客様の VM で実行されている Oracle DBCS エージェントへの REST API コールを実行
- トークンベースの `ssh` を介して、特権ユーザー(`root`、`opc`、`grid`、`oracle`)としてお客様の VM にセキュアにログイン

[67] https://www.oracle.com/database/technologies/faq-tde.html
[68] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/exadata-security-features.html#GUID-FA8A2A69-AEFC-4FE3-959A-A6E584BD1F4F
[69] https://docs.oracle.com/en/database/oracle/key-vault/21.2/okvag/okv_intro.html#GUID-0D169EB8-C355-459A-9ABD-325CA5B46DD0
[70] https://support.oracle.com/knowledge/Oracle%20Cloud/2924192_1.html
[71] https://docs.oracle.com/en/database/oracle/key-vault/21.7/okvag/security_objects.html#GUID-27DA6A5A-E405-4394-BD0D-C2B213391426

お客様の VM は、お客様の VM へのネットワークをブロックするための追加のデータ保護統制として、Oracle Linux のパケット・フィルタリング・ソフトウェア[72]を提供します。Oracle Linux のファイアウォールである `iptables` または `firewalld` を構成すると、レイヤー3 (IP)および 4 (TCP ポート)でのコントロール・プレーンのアクセスをブロックできます。オペレーティング・システムのファイアウォールを構成して、特定のセキュリティ要件に対応することもできます。

ファイアウォール構成のソース IP アドレスを特定するために、もしくはお客様の VM へのコントロール・プレーンのアクセスをブロックする目的でお客様の VM のファイアウォール構成をテストするために、お客様がインフラストラクチャ・コンポーネントに直接アクセスすることはできません。必要なファイアウォール・ルールを特定するには、もしくはお客様の VM のファイアウォール構成が必要に応じてコントロール・プレーンのアクセスをブロックすることを検証するには、Oracle Service Request (SR)プロセスを使用して Cloud Ops にリクエストする必要があります。

トークンベースの `ssh` を使用した Oracle クラウド自動化のセキュアなログインは、Kerberos 認証と互換性がありません。お客様が Kerberos 認証をお客様の VM に実装すると、Oracle クラウド自動化機能の一部が機能しなくなる可能性があります。オラクルは、お客様がお客様の VM で Kerberos オペレーティング・システム認証を構成することをサポートしていません。これを行うと、クラウド自動化が無効になるためです。Oracle データベースのユーザー認証用に Kerberos 認証を構成することは可能です。詳細は、Oracle Support ドキュメント 2621025.1 (Does ExaCC VM's Support Kerberos Authentication)[73]を参照してください。

## お客様の VM へのお客様のスタッフのアクセスに対する統制

お客様の VM へのアクセスは、トークンベースの `ssh`[74]を介して実行されます。お客様は、OCI クラウド・テナンシの資格証明と統制を使用して、お客様が指定する公開鍵を `opc` ユーザーの`/home/oracle/opc/.ssh/authorized_keys` ファイルに追加します。インストールされた公開鍵に関連付けられた秘密鍵にアクセスできるお客様のスタッフは、トークンベースの `ssh` を介してお客様の VM にアクセスできるようになります。Oracle クラウド自動化は、お客様の鍵管理システムと統合されません。お客様は、Oracle Linux と互換性のあるテクノロジーを使用して `ssh` 鍵を管理できます。

Exadata ソフトウェアのバージョン 22.1.4.0.0.221020 以降では、お客様の VM に対する Microsoft Active Directory (AD)および Lightweight Directory Access Protocol (LDAP)認証を、ExaDB-D でお客様が実装できます。ExaDB-D は、この構成でのクラウド自動化サポートを提供しません。お客様は、ExaDB-D のお客様の VM に直接アクセスして AD と LDAP を実装することで、AD と LDAP を構成できます。ExaDB-D のお客様の VM のアップデート[75]は Exadata Database Machine のイメージ・アップデート・プロセス[76]を使用してイメージ・アップデートとして実行されること、およびイメージ・アップデート・プロセスがお客様の AD または LDAP の実装に及ぼす影響についてはお客様がテストし、検証する必要があることに注意してください。AD または LAP の実装がイメージ・アップデート・プロセスに対応していない場合は、パッチ・サイクル中に AD または LDAP を一時的に無効化するか削除し、パッチの適用後に AD または LDAP を復元する必要が生じる可能性があるため、お客様はこれを踏まえた計画を立てる必要があります。

## データの盗難を防ぐための統制

ExaDB-D データベースのユーザー表領域のデータは、Oracle Transparent Data Encryption (TDE)によって保護されます。暗号化されたデータを盗んでも、データの復号が技術的に困難であるため、あまりメリットはありません。米国国防総省(DoD)と国家安全保障局(NSA)は、データ保護に AES 暗号化規格を推奨しています。詳細は、NSA のガイドライン[77]と NIST 規格[78]を参照してください。

オラクルの企業セキュリティ慣行[79]は、オラクルの社内業務とオラクルがお客様に提供するクラウド・サービス(ExaDB-D を含む)のセキュリティ管理を対象としており、従業員や請負業者など、オラクルの全スタッフに適用されます。これらのポリシー

---

[72] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-implement-sec.html#ol7-firewall-sec
[73] https://support.oracle.com/knowledge/Oracle%20Cloud/2621025_1.html
[74] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/ecs-connecting-to-service-inst.html#GUID-53DE1ED5-96D9-4F7F-B57F-4EF8D01FCDCB
[75] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-update-exacc-system.html
[76] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmmn/updating-exadata-software.html#GUID-E6090FA9-13B4-4BEF-A28D-73BDC3729C58
[77] https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm
[78] https://www.nist.gov/publications/advanced-encryption-standard-aes
[79] https://www.oracle.com/corporate/security-practices/corporate/

は、ISO/IEC 27002:2013 (旧 ISO/IEC 17799:2005)規格と ISO/IEC 27001:2013 規格に準拠しており、オラクル内のあらゆるセキュリティ領域の指針となります。オラクルのセキュリティ慣行は公開されています。

## Oracle Data Safe

Oracle Data Safe[80]は、Exadata Cloud at Customer のサブスクリプションに含まれているセキュリティ・クラウド・サービスです。Data Safe によって、次のことが可能になります。

- データベースのセキュリティ構成の評価
- 構成ドリフトの検出
- リスクの高いデータベース・アカウントを特定し、そのアクティビティを表示
- 監査ポリシーのプロビジョニング
- 監査データの分析(レポートの作成とアラートの生成を含む)
- 機微データの検出(データの種類、量、場所を含む)
- 機微データをマスクし、本番以外のデータベースのコピーからセキュリティ・リスクを排除

監査レコードの数が 1 データベース当たり 100 万件/月を超えなければ、Data Safe の利用において追加費用は発生しません。

Oracle Data Safe のテクニカル・アーキテクチャ[81]には、お客様がコントロールするサーバーにデプロイされたオンプレミスのコネクタをサポートする機能が含まれており、ExaDB-D で実行されているデータベースを OCI リージョン内の OCI Data Safe サービスに簡単に接続できます。

## Oracle Database Security Assessment Tool (DBSAT)

Oracle Database Security Assessment Tool は、スタンドアロンのコマンドライン・ツールです。適切な種類の構成情報をデータベースから収集し、現在のセキュリティ状態を評価することで、評価プロセスと規制遵守プロセスを迅速化するとともに、特定されたリスクを軽減する方法を提案します。

DBSAT は追加費用なしで提供され、お客様が次の情報をすばやく確認できるように設計されています。

- セキュリティ構成の問題とその修正方法
- ユーザーとその資格
- 機微データの場所、種類、量

DBSAT は、データベースとリスナーの構成内の情報を分析し、不必要にリスクを招く可能性がある構成設定を特定します。また、簡単な構成チェックだけでなく、ユーザー・アカウント、付与されている権限およびロール、認可統制、職務分掌、きめ細かなアクセス制御、データ暗号化と鍵の管理、監査ポリシー、OS ファイルのアクセス権も調査します。DBSAT は、ルールを適用してデータベースの現在のセキュリティ・ステータスを迅速に評価し、上記の全領域で検出されたリスク箇所を出力します。そして、それぞれのリスク箇所について、リスクを削減または軽減するために必要な修正措置を、ベスト・プラクティスに沿った形で提案します。DBSAT によって提供される包括的な測定結果と補完的統制を適用することで、お客様は企業全体でデータ漏洩リスクを削減できます。Oracle DBSAT は、オラクルからダウンロードできます。[82]

# インフラストラクチャ・コンポーネントへの Cloud Operations のアクセスに対するオラクルの統制

Oracle Cloud Ops のスタッフには、通常の運用条件[83]の下でお客様の VM、データベースまたはデータベース・データにアクセスする権限はありません。ExaDB-D インフラストラクチャ・コンポーネントにアクセスしてサポートする権限はあります。これには次の機器が含まれます。

- 配電ユニット(PDU)
- 帯域外(OOB)管理スイッチ
- ストレージ・ネットワーク・スイッチ
- Exadata Storage Server
- 物理的な Exadata Database Server

---

[80] https://docs.oracle.com/en-us/iaas/data-safe/index.html
[81] https://docs.oracle.com/en/solutions/oracle-data-safe-for-on-prem-database/index.html#GUID-07534FC6-3B10-48E5-BD49-C011D55D1070
[82] https://www.oracle.com/database/technologies/security/dbsat.html
[83] オラクルのスタッフがお客様の VM にアクセスできる例外条件については、「Exception workflows - Oracle Access to Customer VM」で説明しています。

## オラクルの技術的なアクセス制御

図 3 は、Oracle Cloud Operations (Cloud Ops)のスタッフが ExaDB-D を管理するために、どのようにインフラストラクチャ・コンポーネントにアクセスするかを示しています。

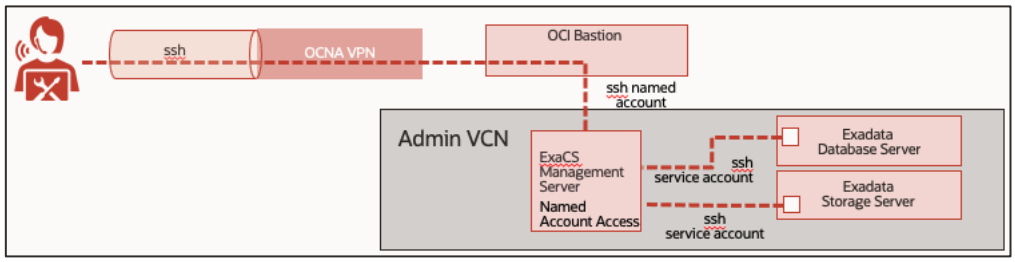


*図 3:Cloud Operations のスタッフによる ExaDB-D インフラストラクチャ・コンポーネントへのアクセス*

オラクルは、Oracle Cloud Ops のスタッフによるクラウド・サービス・インフラストラクチャ・コンポーネントへのアクセスを次の方法で制御します。

- ジョブ・コードに固有の資格に基づき、FIPS 140-2 レベル 3 のハードウェア MFA (Yubikey)を使用して、Oracle Cloud Network Attach (OCNA)にアクセス
- ExaDB-D インフラストラクチャへの ssh アクセスを目的に、踏み台サーバーと管理サーバーにアクセス
  - ExaDB-D 管理サーバーへのアクセスは、分離された踏み台サーバーを介して、サービスをホストする OCI リージョンにある OCI の特権管理 VCN に接続するトンネルとして実装されます。
  - 踏み台サーバーを介した接続は、オラクルによってログに記録され、監視されます。
- FIPS 140-2 レベル 3 のハードウェア・トークン(Yubikey)で実装された MFA を使用して、ssh による名前付きユーザーとして、ExaDB-D インフラストラクチャ管理専用の管理サーバーにログイン
  - 管理サーバーへのアクセスは、公開されているオラクルの最小権限アクセス・ポリシー[84]に基づいて制御されます。
  - ExaDB-D インフラストラクチャへの接続は、オラクルによってログに記録され、監視されます。
- トークンベースの ssh による必要なサービス・アカウントを使用して、ExaDB-D インフラストラクチャにログイン
  - コマンドの実行は、ExaDB-D インフラストラクチャに実装された監査ロギングを介して、特定の名前付きユーザーまで辿ることができます。
  - インフラストラクチャ・コンポーネントへの接続は、オラクルによってログに記録され、監視されます。

## オラクルのプロセスのアクセス制御

オラクルのアクセス制御[85]に関するセキュリティ慣行では、知る必要と ExaDB-D インフラストラクチャにアクセスする必要があるオラクル・スタッフにアクセスを制限しています。次のポリシーがあります。

- ExaDB-D インフラストラクチャにアクセスする権限は、オラクルのポリシーに準拠したジョブ・コードとトレーニング・レコードを持つ特定のサポート・スタッフに限定されます。技術的なセキュリティ対策がこのポリシーを強化しています。
- 人材採用、人事異動、退職の各プロセスを自動化することで、お客様のインフラストラクチャにアクセスする権限と、従業員のジョブ・コード、トレーニング・レコード、雇用状況の更新との整合性を確保します。

## Exadata インフラストラクチャ・ソフトウェアのセキュリティと統制

ExaDB-D は、Exadata Database Machine を基盤としており、Exadata Database Machine のエンタープライズクラスのセキュリティ機能[86]をオンプレミスのクラウド・モデルで提供します。ExaDB-D のセキュリティ機能には次のものがあります。

- ExaDB-D インフラストラクチャにデプロイされるソフトウェアは、お客様のサービスを実行するための最小限のソフトウェア・コンポーネントに限定される
- お客様のデータを調査するための開発ツールとデバッグ・ツールは、ExaDB-D インフラストラクチャにインストールされない
- 必須でないオペレーティング・システム・ツールとパッケージは、ExaDB-D インフラストラクチャにインストールされない

---

[84] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[85] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[86] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/toc.htm

- ソフトウェア開発は、Oracle Software Security Assurance[87]の下で行われる
- セキュリティ・アーキテクチャは、Oracle Corporate Security Architecture[88]の下で実行される

## 発見的統制(ロギングと監査)

ExaDB-D は、お客様のサービスとオラクルが管理するインフラストラクチャに対する堅牢な発見的統制(監査とロギング)を提供します。お客様は、お客様のサービスのロギング構成をコントロールし、オラクルは、オラクルが管理するインフラストラクチャのロギング構成をコントロールします。オラクルには、お客様のサービスの監査ログにアクセスする権限はありません。お客様は、Oracle Service Request (SR)プロセスを通じて、該当するオラクルの監査ログ情報へのアクセスをリクエストできます。また、Oracle Data Processing Agreement (DPA)[89]で監査権限を確認できます。

## お客様の監査ロギング

ExaDB-D は、お客様のアクションの監査とロギングのために、3 つの機能を提供します。

- OCI Audit サービス:[90] お客様の OCI IAM 資格証明を介して開始されたコントロール・プレーン・アクション(Web UI、OCI CLI、OCI REST API など)の監査ログ
- Oracle データベースの監査:[91] お客様の Oracle データベース資格証明を介して開始されたデータベース・アクションの監査ログ
- お客様の VM オペレーティング・システムの監査ログ:[92] オペレーティング・システムの資格証明を介してお客様の VM で開始されたアクションの監査ログ

OCI Audit サービスにより、サポートされるすべての Oracle Cloud Infrastructure パブリック・アプリケーション・プログラミング・インタフェース(API)エンドポイントへのコールが、ログ・イベントとして自動的に記録されます。現在、すべてのサービスが監査ロギング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、オブジェクト関連イベントのロギング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・イベントとして、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)、独自のカスタム・クライアント、その他の Oracle Cloud Infrastructure サービスによって実行された API コールが挙げられます。ログの情報には次のものが含まれます。

- API アクティビティが発生した時間
- アクティビティのソース
- アクティビティのターゲット
- アクションの種類
- レスポンスの種類

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。OCI Audit[93]サービスによってログに記録されたイベントは、コンソール、API、または Java の SDK を使用して参照できます。イベントのデータは、診断、リソース使用率の追跡、コンプライアンスの監視、およびセキュリティ関連イベントの収集を行うために使用できます。

Oracle データベースの監査では、データベース・ユーザーと非データベース・ユーザーが Oracle データベースに加えた変更が追跡されます。お客様は、監査ログをリモート・ログ・サーバーに送信する作業も含め、Oracle データベースの監査ログの構成と管理を行うことができます。Oracle データベースの監査ログの構成、管理および監視についてのドキュメントは、各データベース・バージョンの『Oracle Database セキュリティ・ガイド』[94]で公開されています。

---

[87] https://www.oracle.com/corporate/security-practices/assurance/
[88] https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
[89] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
[90] https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm
[91] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/introduction-to-auditing.html#GUID-94381464-53A3-421B-8F13-BD171C867405
[92] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-implement-sec.html#ol7-audit-sec
[93] https://docs.cloud.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm.
[94] Oracle Database 19c の場合は、https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/introduction-to-auditing.html#GUID-94381464-53A3-421B-8F13-BD171C867405 を参照してください。

お客様の VM オペレーティング・システムの監査ログは、お客様の VM で実行されている Oracle Linux (OL)オペレーティング・システムの監査ログ・サービスとして実装されます。Oracle Linux の監査ログ・サービスにより、オペレーティング・システムの資格証明(root、oracle、opc など)とお客様が構成した名前付きユーザーによって実行されたアクションが記録されます。お客様は、Oracle Linux の監査ログをリモート・ログ・サーバーに送信する作業も含め、自社の標準に従って Oracle Linux の監査ログの構成を行うことができます。『Oracle Linux セキュリティ・ガイド』[95]でドキュメントが公開されています。

## お客様の VM のお客様によるセキュリティ・スキャン

お客様は、OpenSCAP[96]を使用してお客様の VM をスキャンすることで、コンプライアンスを確保できます。

お客様は、Oracle Linux Advanced Intrusion Detection Environment (AIDE)[97]を使用して、ファイルおよびディレクトリの整合性をチェックできます。AIDE は、Linux オペレーティング・システムとともに自動的にインストールされる、小さいながら強力な侵入検出ツールです。このツールでは、事前定義のルールを使用してファイルおよびディレクトリの整合性をチェックします。ウィルス、ルートキット、マルウェアからの保護と不正なアクティビティの検出を行うレイヤーを提供し、システムを内部的に保護することを目的としています。これは、簡易的なクライアント/サーバー監視構成のための独立した静的バイナリです。オンデマンドで実行され、変更をレポートする時間はシステム・チェックに依存します(通常は 1 日に 1 回以上)。このユーティリティは、多数のアルゴリズム(md5、sha1、rmd160、tiger などがあるが、これらに限定されない)を使用して動作し、一般的なファイル属性をサポートします。さらに、スキャンに含めるか除外するファイルの正規表現パーサーもサポートします。

お客様は、スキャン・ソフトウェアを含むサードパーティ・ソフトウェアを ExaDB-D のお客様の VM にインストールすることができます。オラクルは、オラクル以外のソフトウェアに対する技術サポートは行いません。これには、インストール、テスト、認定、エラー解決が含まれます。カスタム/サードパーティ・ソフトウェアの技術サポートについては、そのソフトウェアのサプライヤーが責任を負います。オラクル以外のすべてのソフトウェアは、ベンダーによって Oracle Linux または Exadata 環境(あるいはその両方)での使用が認定されており、お客様とサードパーティ・プロバイダによって対象環境でのテストが徹底的に実施されていることが強く推奨されます。ExaDB-D でのサードパーティ・ソフトウェアのサポートの詳細は、My Oracle Support の「Installing Third Party Software on Exadata Components (Doc ID 1593827.1)」[98]で公開されています。

サード・パーティのスキャン・ツールとサード・パーティ提供のベンチマークを使用しているお客様は、必ずベンチマークをアップデートして、ExaDB-D のソフトウェア配布および構成と互換性を持たせる必要があります。任意のベンチマークで、ExaDB-D のお客様 VM に関するセキュリティの問題が通知される場合がありますが、これはベンチマークが認識していない ExaDB-D サービスでの補完コントロールによるもので、重大なリスクではない可能性があります。一般的なベンチマークを調整して Exadata に対応させる方法については、My Oracle Support Note の「Responses to common Exadata security scan findings (Doc ID 1405320.1)」[99]を参照してください。ExaDB-D のお客様 VM が、サード・パーティのベンチマークやお客様が設計したベンチマークに適合するように変更されている場合は、その変更をテストし、ExaDB-D のソフトウェア自動化が変更によって損なわれないことを検証する必要があります。オペレーティング・システム、Oracle データベース、Grid Infrastructure のアップデートなど、自動化されたソフトウェアのアップデートにより、サード・パーティ提供のセキュリティ・ベンチマークに合せて実装されたお客様の変更が元に戻る可能性があります。

ExaDB-D のお客様の VM に対してお客様が行うセキュリティ・テストは、Oracle Cloud Testing Policies[100]に従って実行される必要があります。

## ExaDB-D のお客様 VM でのお客様によるサード・パーティ・ソフトウェアの使用

お客様は、スキャン・ソフトウェアを含むサードパーティ・ソフトウェアを ExaDB-D のお客様の VM にインストールすることができます。オラクルは、オラクル以外のソフトウェアに対する技術サポートは行いません。これには、インストール、テスト、認定、エラー解決が含まれます。カスタム/サードパーティ・ソフトウェアの技術サポートについては、そのソフトウェアのサプライヤーが責任を負います。オラクル以外のすべてのソフトウェアは、ベンダーによって Oracle Linux または Exadata 環境(あるいはその両方)での使用が認定されており、お客様によって対象環境でのテストが徹底的に実施されていることが強く

[95] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-audit-sec.html
[96] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-scap-sec.html.
[97] https://support.oracle.com/knowledge/Oracle%20Linux%20and%20Virtualization/2616282_1.html
[98] https://support.oracle.com/knowledge/Oracle%20Cloud/1593827_1.html
[99] https://support.oracle.com/knowledge/Oracle%20Database%20Products/1405320_1.html
[100] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm

推奨されます。ExaDB-D でのサードパーティ・ソフトウェアのサポートの詳細は、My Oracle Support の「Installing Third Party Software On Exadata Components (Doc ID 1593827.1)」[101]で公開されています。

## オラクルの監査ロギング

オラクルが所有する ExaDB-D インフラストラクチャで実行されたアクションの監査ロギングは、オラクルの責任で行われます。オラクルは、ExaDB-D X8 以前のハードウェアについて、次のインフラストラクチャ監査ログを保持します。

- ILOM
  - syslog
  - 物理的なインフラストラクチャ・コンポーネントの syslog にリダイレクトされた ILOM syslog
- 物理的な Exadata Database Server
  - /var/log/messages
  - /var/log/audit.log
  - /var/log/secure
  - /var/log/xen/xend.log
- Exadata Storage Server
  - /var/log/messages
  - /var/log/audit.log
  - /var/log/secure
- ストレージ・ネットワーク・スイッチ
  - /var/log/messages
  - /var/log/audit.log
  - /var/log/secure
  - /var/log/opensm.log

オラクルは、ExaDB-D X8M 以降のハードウェアについて、次の監査ログを保持します。

- ILOM
  - syslog
  - 物理的なインフラストラクチャ・コンポーネントの syslog にリダイレクトされた ILOM syslog
- 物理的な Exadata Database Server
  - /var/log/messages
  - /var/log/secure
  - /var/log/audit/audit.log
  - /var/log/clamav/clamav.log
  - /var/log/aide/aide.log
- Exadata Storage Server
  - /var/log/messages
  - /var/log/secure
  - /var/log/audit/audit.log

インフラストラクチャの監査ログの保存期間は 13 か月です。インフラストラクチャの監査ログは、OCI SIEM サービスと OCI Logging サービスに格納され、Oracle Incident Management チームと OCI のセキュリティ・チームによるアクセスが可能です。お客様は、Oracle Service Request (SR)プロセスを通じて、インフラストラクチャの監査ログへのアクセスをリクエストできます。お客様が疑わしいアクティビティを検出した場合は、セキュリティのサービス・リクエストを登録し、該当するログを提供するという手順を踏みます。これにより、Oracle Security Operations Center (SOC)の関与が開始されます。このレビューは、お客様と協力してイベントの調査にあたる独立チームによって実施されます。

## 対応的統制

お客様とオラクルは連携して、お客様のサービス、データベース、データベース・データ、VM およびインフラストラクチャへのアクセスを保護し、監視します。お客様とオラクルのいずれかが不正なアクションを検出した場合、検出した側は、セキュリティ・ポリシーや不正なアクションの詳細と状況に応じて、相手側に通知する前に、即座に対応策を講じることができます。お客様が不正なアクションを検出した場合、お客様は Oracle Service Request プロセスを通じて、そのアクションと対応をオラクルに通知する必要があります。オラクルは、確認された不正なアクションとオラクルの対応をオラクルの Incident Response Policy[102]に従ってお客様に通知します。

---

[101] https://support.oracle.com/knowledge/Oracle%20Cloud/1593827_1.html

[102] https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html

お客様は、自身がコントロールするあらゆるサービスに対して、あらゆる対応策を講じることができます。対応策としては、お客様の VM へのネットワーク接続、お客様がコントロールする Oracle データベースへのネットワーク接続の終了などがあります。

オラクルの対応的統制には、OCI の踏み台サーバーにおける接続の終了、オラクルが管理する ExaDB-D インフラストラクチャのリソースに対するアクセス権の取消しなどが含まれます。

## サービスの終了とデータの破壊

お客様は、ExaDB-D ライフサイクル管理業務[103]の一環として、ExaDB-D インスタンスを終了させることができます。Exadata Database Service on Dedicated Infrastructure のリソースを終了させると、そのリソースとその上で実行中のすべてのデータベースが永久に削除されます。サービスの終了機能は、Exadata Database Machine Secure Erase として実装されています。[104]Exadata Secure Eraser は、ストレージ・デバイスのハードウェア機能を自動的に検出し、デバイスでサポートされる最適な消去方式を選択します。セキュリティの強化と高速化のために、可能な限り暗号化消去が使用されます。Secure Eraser で使用される暗号化消去方式は、NIST SP-800-88r1 規格に完全に準拠しています。[105]お客様は、My Oracle Support (MOS)リクエストをオープンすることで、オラクルからセキュアな消去の認定を受けることができます。

## 例外ワークフロー - お客様の VM へのオラクルのアクセス

ExaDB-D サービスでは、オラクルのスタッフが通常の運用条件の下でお客様の VM にアクセスすることを許可していません。お客様の VM で障害が発生し、問題解決のためにオラクルのスタッフがアクセスしなければならない例外ケースがあります。オラクルのスタッフがお客様の VM にアクセスできるタイミングと方法を決定するプロセスと技術的な統制は、例外が発生したのが、お客様がお客様の VM にアクセスする前か後かによって異なります。

### ケース 1:お客様がお客様の VM にログインする前のサービス例外

お客様がサービスにアクセスする前に、お客様のサービスで例外が発生した場合、お客様は、サービス例外に関連するサービス・リクエスト(SR)でオラクルのアクセス要請に対して「はい」と答えることにより、オラクルのスタッフがお客様のサービスにアクセスすることを許可できます。この方法のユース・ケースには、クラウド自動化によって作成される VM の障害などがあります。

オラクルのスタッフは、既存の SR で許可を求めるために、次の情報を入力します。

- ExaCC サービスに関連するセキュリティ・ポリシーにより、オラクルの担当者は、お客様の明示的な許可なくお客様の DomU にアクセスすることを禁じられています。このポリシーを遵守するために、オラクルのスタッフは、次の質問をすることで、DomU[106]にアクセスする許可をお客様から得る必要があります。
- 「この SR に記載されている問題を解決するには、オラクルがお客様の DomU にログインすることを認める、お客様の明示的な許可が必要です。DomU への明示的なアクセス許可を与えることで、お客様は、お客様の DomU や関連するデータベースに格納されている機密データがないこと、また、オラクルがこの問題を修正できるように、お客様のセキュリティ・チームがオラクルに対してお客様の DomU へのアクセスを許可することを確認したことになります。DomU への明示的なアクセス許可をいただけますか。」

お客様が SR で「はい」と答えた場合、オラクルのプロセスおよびセキュリティ統制は、オラクルのスタッフがお客様の VM にアクセスすることを許可するように一時的に調整されます。オラクルのスタッフによるお客様の VM へのアクセスは、SR がクローズされるか、お客様が SR でアクセスを中止するようオラクルに指示するまで、許可されます。

---

[103] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/examanagingDBsystem.htm
[104] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/exadata-secure-erase.html#GUID-6C9FD30C-FF88-4ABA-9249-93E183784B0D
[105] https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization
[106] DomU とは、ExaDB-D サービスにデプロイされたお客様の VM を指すオラクルの用語です。この用語は、ExaDB-D サービス内のお客様の VM に対するオラクル・スタッフのアクセスを管理するプロセス統制の一部として必要です。

## ケース 2:お客様がお客様の VM にログインした後のサービス例外

お客様がサービスにアクセスした後、お客様のサービスで例外が発生した場合、お客様は、アクセスを許可する新しい SR をオープンすることにより、オラクルのスタッフがお客様のサービスにアクセスすることを許可できます。

この方法のユース・ケースには次のものがあります。

- VM が起動できなくなるエラー
- お客様の VM への ssh が失敗したり、お客様の資格証明が失われたりするエラー
- その他のサポート・エラー条件

オラクルがお客様の VM にアクセスすることを許可するには、お客様は次の文言で新しい SR をオープンする必要があります。

- Oracle Cloud Ops がお客様の直接の監督なしにお客様の VM にアクセスすることを許可しても構わない場合、お客様は次の文言でサービス・リクエスト(SR)をオープンします。
  - SR のタイトル:
    - オラクルに ExaCC のゲスト VM (VM 名<DB サーバー詳細ページ→「リソース」→「仮想マシン」の下に表示されている VM 名を挿入>)への明示的なアクセス許可を与える SR
  - SR の内容:
    - サポートが SR# 1-xxxxxxxx に記載されている問題を解決できるよう、オラクルにゲスト VM への明示的なアクセス許可を与えるために、この SR をオープンします。この許可を与えることで、オラクルがゲスト VM に含まれるすべてのファイルとメモリーにアクセスできることを理解することを認めます。加えて、前述の SR に記載されている問題を解決するために、顧客のセキュリティ・チームがオラクルに対して顧客のゲスト VM へのアクセスを許可したことにも同意します。
    - DB サーバーの OCID:<VM をホストしている DB サーバーの OCID をここに挿入>
    - VM 名:<DB サーバー詳細ページ→「リソース」→「仮想マシン」の下に表示されている VM 名を挿入>
- 共有画面を提供して、Oracle Cloud Ops のアクセスをお客様が直接監督することを許可するようオラクルに求める場合、お客様は次の文言でサービス・リクエスト(SR)をオープンします。
  - SR のタイトル:
    - オラクルに ExaCC のゲスト VM (VM 名<DB サーバー詳細ページ→「リソース」→「仮想マシン」の下に表示されている VM 名を挿入>)への明示的なアクセス許可を与える SR
  - SR の内容:
    - サポートが SR# 1-xxxxxxxx に記載されている問題を解決できるよう、オラクルに共有画面セッションでのゲスト VM への明示的なアクセス許可を与えるために、この SR をオープンします。この許可を与えることで、オラクルがゲスト VM に含まれるすべてのファイルとメモリーにアクセスできることを理解することを認めます。この VM へのアクセスの許可は、弊社の担当者がオラクルによって実施されるすべてのアクティビティを画面共有セッション経由でリアルタイムに監視できることを条件とします。加えて、前述の SR に記載されている問題を解決するために、顧客のセキュリティ・チームがオラクルに対して、この共有画面セッションを介した顧客のゲスト VM へのアクセスを許可したことにも同意します。
    - DB サーバーの OCID:<VM をホストしている DB サーバーの OCID をここに挿入>
    - VM 名:<DB サーバー詳細ページ→「リソース」→「仮想マシン」の下に表示されている VM 名を挿入>

お客様が新しい SR を作成し、オラクルが新しい SR を受け取ると、オラクルのプロセスおよびセキュリティ統制は、オラクルのスタッフがお客様の VM にアクセスすることを許可するように調整されます。

## まとめ

Exadata Database Service on Dedicated Infrastructure では、お客様の VM とお客様のデータベースの全体にわたるセキュリティ機能はお客様によってコントロールされます。Oracle データベースの暗号化機能によってデータが暗号化され、お客様が暗号鍵の統制を保持します。Oracle データベースのセキュリティ機能によって、データベースのデータに対する認証とアクセスが制御され、お客様がこの認証とアクセスの統制を保持します。Oracle Linux の認証機能によって、お客様の VM に対するアクセスが制御され、お客様がこの認証とアクセスの統制を保持します。

オラクルが管理する Exadata Database Service on Dedicated Infrastructure のコンポーネント全体にわたるセキュリティ機能と監査機能は、ExaDB-D のインフラストラクチャ・コンポーネントに対する不正なアクションを防止するのに役立ちます。セキュリティ対策には、名前付きユーザーの多要素認証や、オラクルが管理するインフラストラクチャ・コンポーネントに対する FIPS 140-2 レベル 3 準拠のトークンベースの ssh アクセスを使用した強力な認証などがあります。監査とロギングはスタック全体に実装され、Oracle Service Request (SR)プロセスを通じてリクエストを行ったお客様に該当する監査ログが提供されます。

Exadata Database Service on Dedicated Infrastructure は、高度なセキュリティを備えたオンプレミス・デプロイメントの利点を、使いやすく経済的なクラウドで提供します。お客様と Oracle Cloud Operations は連携してシステムのセキュリティを確保し、お客様のデータへの不正アクセスやお客様のデータの盗難を防止します。Oracle Cloud Operations のスタッフがサービスを提供するためにお客様のネットワーク、サービス、データにアクセスすることはなく、お客様がサービスを利用するためにオラクルが管理するインフラストラクチャにアクセスすることはありません。Exadata Database Service on Dedicated Infrastructure のデプロイメント・モデルでは、お客様は、オンプレミス・デプロイメントのセキュリティと、クラウドの経済性、俊敏性、スケールの利点を同時に享受できます。

## CONNECT WITH US

+1.800.ORACLE1 にお電話いただくか、oracle.com にアクセスしてください。
北米以外のお客様は、oracle.com/contact でお近くの営業窓口を参照いただけます。

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



Exadata Database Service on Dedicated Infrastructure
Security Controls