



Oracle Exadata Database Service on Dedicated
Infrastructureのセキュリティコントロール

ORACLE

Exadata Database Service on Dedicated Infrastructureの セキュリティコントロール

セキュリティの承認者および開発者向けテクニカル・サマリー

2026年6月16日 | バージョン2.46
Copyright © 2026, Oracle and/or its affiliates
公開

本書の目的

本文書は、[Exadataリリース25.2.5.0.0.251214](#)および[24.1.19.0.0.251214](#)に含まれる機能と機能強化の概要を説明しています。本書は、読者がExadataリリース25.2.5.0.0.251214および24.1.19.0.0.251214へのアップグレードのビジネス上の利点を評価し、ITプロジェクトを計画することを支援することのみを目的としています。

本書は、Oracle Cloud Infrastructure（OCI）の[Oracle Exadata Database Service on Dedicated Infrastructure](#)（ExaDB-D）、さらに[Oracle AI Database@Azure](#)、[Oracle AI Database@Google Cloud](#)、[Oracle AI Database@AWS](#)に組み込まれているセキュリティコントロールについて説明しており、それらがお客様のユースケースに適しているかを評価する助けとなります。これらの制御は、お客様のデータやミッション・クリティカルなワークロードを保護するための業界のベスト・プラクティスに準拠しています。お客様の現在のセキュリティ標準が異なるものである場合でも、本書ではポリシーの更新や調整を行えるよう、代替となる制御を提示しています。

免責事項

本文書には、ソフトウェアや印刷物など、いかなる形式のものも含め、オラクルの独占的な所有物である占有情報が含まれます。この機密文書へのアクセスと使用は、締結および遵守に同意したOracle Software License and Service Agreementの諸条件に従うものとします。本書とここに含まれる情報は、オラクルの書面による事前の許可を得ることなく、オラクルの社外に対し、開示、複写、複製、または配布することはできません。本文書は、ライセンス同意書の一部ではありません。また、オラクル、オラクルの子会社または関連会社との契約に組み込むことはできません。

本書は情報提供のみを目的としたものであり、ここで説明する製品の機能を実装およびアップグレードする際の資料として使用されることのみを意図しています。マテリアルやコード、機能の提供をコミットメント（確約）するものではなく、購買を決定する際の判断材料にするものでもありません。本書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、オラクルの裁量により決定されます。

製品アーキテクチャの性質上、コードが大幅に不安定化するリスクなしに、本書に記載されているすべての機能を安全に含めることができない場合があります。

目次

本書の目的	2
免責事項	2
はじめに	5
役割と責任	5
OCIにおけるExaDB-D	5
マルチクラウドのための追加	6
アーキテクチャ概要	7
OCIにおけるExaDB-D	7
マルチクラウドのための追加	8
OCI子サイト	9
プライベート接続	9
OCI制御ネットワーク	10
セキュリティコントロール	11
データベースのセキュリティコントロール	12
データベース認証	12
ネットワークの暗号化	12
保管中のデータの暗号化	12
データベース・バックアップの暗号化	13
SQLを使用したデータベース管理者によるユーザー・データへのアクセス防止	13
SQLインジェクション攻撃の軽減	14
データベース・セキュリティの監視と管理	14
ExadataストレージへのVMクラスタのアクセスの制御	15
VMのセキュリティコントロール	15
VMのデフォルトのセキュリティ設定	16
VMのデフォルト・ユーザー	16
VMファイルの整合性監視	17
VMバックアップ暗号化	17
クラウド自動化によるお客様のVMへのアクセス	17
お客様のVMへのオラクルのサービスとサポートのスタッフによるアクセスの制御	17
ネットワーク・セキュリティコントロール	18
ファイアウォール機能によるIPアドレス、ポート、プロトコルの制御	18
宣言的自然言語によるIPアドレス、ポート、プロトコルの制御	18
お客様のネットワークから使用できる資格証明の制御	19
OCIの追加のセキュリティコントロール	19
テナンシー・リソースの認証を受けることができるネットワークの制御	19
テナンシー内での特定のAPIアクションの拒否	19
お客様の管理者による特権APIの使用の制御	19
ランサムウェアからのリカバリ	20
Oracleインフラストラクチャのセキュリティコントロール	20
お客様のインフラストラクチャへのオラクルのスタッフによるシールド・アクセスの制御	21
監査とロギング	22
データベース監査ロギング	22
VM監査ロギング	22
OCI監査ロギング	23
ネットワーク・トラフィックのロギング	23
Oracleインフラストラクチャ監査ロギング	23
Operator Access ControlとDelegate Access Controlの監査ロギング	24
インシデントへの対処	24
お客様による対応制御	24
オラクルのインシデント対応プロセス	24
クリティカルな問題に対する15分のサービス対応時間	24
ソフトウェアのセキュリティと更新	25

セキュリティ・テストとスキャン	25
お客様のVMのセキュリティ・テストとスキャン	25
オラクルが管理するインフラストラクチャのセキュリティ・テストとスキャン	26
カスタマイズとサード・パーティ製ソフトウェア	26
互換サービス変更	26
必要なサービス構成	26
サービスの終了とデータの破壊	27
ストレージ・メディア・ハードウェアの取扱いと破壊	27
オラクルによる顧客VMへのアクセスの例外ワークフロー	28
VMがDelegate Access Controlによって管理されている場合	28
お客様がVMにアクセスできる場合	28
お客様がVMにアクセスできない場合	29
まとめ	29
付録：技術的情報	30
ネットワーク・アーキテクチャの図	30
マルチクラウド・ネットワーク・アーキテクチャの図	31
VMのデフォルトのプロセスと証明書	32
OCIコントロール・プレーン経由でのVMシリアル・コンソールへのアクセス	35
商用関連の付録	35
準拠	35
オラクルの企業セキュリティ慣行	36
脆弱性の開示	36
Oracle Data Processing Agreement	36
Oracle Cloud Services Agreement	36
オラクルによるセキュリティ・イベント・ログの管理	37
セキュリティ・ログを少なくとも1年間保持	38
月次稼働時間99.95%の品質保証契約（SLA）	38
サービス終了後の60日間のアクセス期間	38

画像一覧

図1：ExaDB-Dアーキテクチャ	8
図2：マルチクラウド・アーキテクチャ	9
図3：Oracle AI Database@Azureプライベート接続	10
図4：マルチクラウド・インタフェースの統合	11
図5：Delegate Access Control承認ワークフロー	18
図6：APIアクセス制御承認ワークフロー	20
図7：ExaDB-DインフラストラクチャへのOracle Cloud Operationsシエル・アクセス	21
図8：ExaDB-Dのネットワーク・アーキテクチャ	30
図9：Oracle AI Database@Azureネットワークの図	31
図10：Oracle AI Database@AWSネットワークの図	31
図11：Oracle AI Database@GCPネットワークの図	32

表一覧

表1：OCIにおけるExaDB-Dでの役割と責任	6
表2：マルチクラウドでの役割と責任	6
表3：ゲストVMサービスのデフォルトのポート・マトリックス	32

はじめに

ExaDB-Dは、OCIとパートナーのデータセンターで、[Exadata](#)をマネージド・クラウド・サービスとして提供します。お客様は[Exadataの機能](#)、OCI オークストレーション、およびオラクルのサポートをすべて利用できます。このサービスは、お客様が選択したクラウド・プロバイダのデータセンターにある専用のコンピュータ・サーバーとストレージ・サーバーでデータを保護するのに役立ちます。お客様は以下を制御できます。

- データベースにアクセス可能なネットワーク
- VMとデータベースを認証可能な資格証明

お客様は、仮想マシンとデータベースに対してルートレベルおよびSYSレベルのアクセス権を持ちます。セキュリティ・ポリシーの設定、エージェントのインストール、ログの転送、およびIDの管理を実行することで、規制を遵守できます。ExaDB-Dでは、ExaDB-Dのデータベース・サーバーとストレージ・サーバーのインフラストラクチャに対する、オラクルのスタッフによるシェル・アクセスのための以下の制御モデルを選択できます。

- オラクルによる制御：アクセス権限はオラクルによる承認後に付与される
- お客様による制御：アクセス権限は[Operator Access Control](#)でのお客様による承認後に付与される

オラクルは、[オラクルの企業セキュリティ慣行](#)に基づいて、サービス・コントロール・プレーンおよびExadataインフラストラクチャを運用します。本サービスのセキュリティコントロールにより、責任共有モデルを実施できるようになり、お客様とオラクルは連携してOracle AI Databaseのサポート、保護、および監査を行うことができます。本サービスは、Oracle AI Databaseに転送中のアプリケーション・データと、Oracle AI Databaseに保管中のデータの両方を暗号化します。

役割と責任

このセクションでは、ExaDB-Dの責任共有モデルについて説明します。OCIにおけるExaDB-Dは、お客様とオラクルとの間の責任モデルの基礎となります。「マルチクラウドにおける追加事項」では、責任モデルがどのように進化して、パートナーのクラウド・サービス・プロバイダ（CSP）を組み込むかを示しています。

OCIにおけるExaDB-D

[ExaDB-Dは責任共有モデルを採用](#)しており、お客様とオラクルはそれぞれ以下のようなシステムの特定の面を管理します。

お客様の責任範囲には、以下の保護、監視、管理が含まれます。

- OCIテナンシー
- 仮想マシン（VM）
- そのVM上で稼働するデータベース

オラクルの責任範囲には、以下の保護、監視、管理が含まれます。

- 物理サーバー（Exadata Database ServerおよびExadata Storage Server）
- 内部ネットワーク・スイッチ
- 配電ユニット（PDU）
- サービスを提供するOCIリージョン

オラクルは、責任範囲内にある以下について監視し、問題が起きた場合に対応します。

- インフラストラクチャ・セキュリティとアクセス制御
- Exadataのコンピューティング、ストレージ、ネットワーク用のハードウェアとソフトウェアの監視とメンテナンス
- [Oracle Auto Service Request Qualified Engineered Systems Products](#)のイベント監視とメンテナンス

オラクルは、以下のような、責任範囲外にある要素は監視しません。

- フラッシュ・キャッシュの使用量
- VMのセキュリティとアクセス・ログ
- Oracle CRS、ASM、Database
- VMで実行中のソフトウェア

「オラクルによる顧客VMへのアクセスの例外ワークフロー」で説明されている特定のサポート例外を除き、オラクルのスタッフがお客様のVMやデータベースにアクセスすることは許可されていません。

役割と責任の詳細な内訳については、表1および[ExaDB-D on Dedicated Infrastructure - Explanation of Cloud Operations Service \(KB60969\)](#)を参照してください。

表1：OCIにおけるExaDB-Dでの役割と責任

職務	Oracleが管理するインフラストラクチャ		お客様のサービス	
	Oracle Cloud Operations	お客様のスタッフ	Oracle Cloud Operations	お客様のスタッフ
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	お客様自身によるサービスの監視をサポートするインフラストラクチャの可用性	データベース、VM、アプリの監視
インシデントの管理と解決	インシデントの管理と修復 スベア部品およびフィールド・デイスパッチ	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	お客様のアプリのインシデント管理と解決
パッチ管理	ハードウェア、IaaS制御ソフトウェア、ハイパーバイザ、およびOracleが管理するインフラストラクチャ・コンポーネント（適用可能なものに限る）へのプロアクティブなパッチ適用	該当なし	ExaDB-D on Dedicated Infrastructureのメンテナンス に関するドキュメントに従った、利用可能なパッチ（Oracle DBパッチ・セットなど）のステージング	Oracle AI Database、Grid Infrastructure、VMオペレーティング・システムのソフトウェア更新 テスト
バックアップとリストア	インフラストラクチャおよびコントロール・プレーンのバックアップとリカバリ、VMの再作成	該当なし	お客様がアクセス可能な稼働する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
クラウドのサポート	インフラストラクチャまたはサブスクリプションの問題に関連するSRの対応と解決	My Oracle Support（MOS）経由でのSRの送信	SRの対応と解決	My Oracle Support（MOS）経由でのSRの送信

マルチクラウドにおける追加事項

マルチクラウドでは、お客様のCSPが責任マトリックスに追加されます。お客様のCSPは物理的なデータセンターを管理し、OracleはExaDB-D機器へのアクセスを管理します。表2は、マルチクラウドのサポートと運用における、Oracle、CSP、お客様のスタッフの役割と責任を示しています。

表2：マルチクラウドでの役割と責任

職務	Oracleの責任	CSPの責任	お客様の責任
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	お客様による顧客サービスの監視をサポートするインフラストラクチャの可用性 Oracleのハードウェア・サービス技術者にCSPデータセンターへのアクセス権を付与 Oracleのハードウェア・サービス技術者をOracleハードウェア・ケージに案内	オペレーティング・システム、データベース、アプリケーションの監視

職務	オラクルの責任	CSPの責任	お客様の責任
インシデントの 管理と対応	インシデントの管理と修復 スベア部品およびフィールド・ ディスク	オンサイト診断支援（ネットワークの トラブルシューティング、電源、冷却 など）	お客様のアプリケーションのインシデント 管理と解決
パッチ管理	ハードウェアおよびIaaS/PaaS 制御スタックのプロアクティブな パッチ適用、利用可能なパッチの ステージング（Oracle DB/パッチ・ セットなど）		お客様のテナント・インスタンスのパッチ 適用
バックアップとリストア	インフラストラクチャおよびコンテ 이너・プレーンのバックアップと リカバリ	オンサイト診断支援（ネットワークの トラブルシューティング、電源、冷却 など）	Oracleネイティブ・バックアップまたはサード・ パーティ・ソリューションを使用した、お客 様のリソースとデータのスナップショット/ バックアップとリカバリ
クラウドのサポート	対応と解決	対応と解決	サポート・ポータル経由でSRを送信

アーキテクチャ概要

このセクションでは、ExaDB-Dのアーキテクチャの概要を説明します。「OCIにおけるExaDB-D」では、オラクルがOCIデータセンターでExaDB-Dをどのように提供しているかを示します。「マルチクラウドにおける追加事項」では、オラクルがどのようにアーキテクチャを拡張し、お客様のCSPデータセンターでサービスを提供するかを示しています。

OCIにおけるExaDB-D

図1は、[ExaDB-Dアーキテクチャ](#)を示しています。このサービスは、お客様が選択したデータセンター内の[Oracle Exadata Database Server](#)と[Oracle Storage Server](#)にデプロイされます。物理的なExadata Database ServerとExadata Storage Serverは、お客様のサービス専用となります。物理的な電力インフラストラクチャとネットワーク・インフラストラクチャは共有されています。データはOracle Exadata Storage Serverに保存され、クライアント用とバックアップ用の[Virtual Cloud Networks（VCN）](#)を経由してアクセスされます。オプションで、[FastConnect](#)または[サイト間VPN](#)を使用して、データセンター内のリソースに接続できます。[RDMA over Converged Ethernet（RoCE）ネットワーク](#)は、VLAN技術を使用してExadataストレージと[Real Application Cluster（RAC）](#)のトラフィックを分離します。

[Oracle Cloud Infrastructure](#)は、以下のものとのIDフェデレーションをサポートしています。

- Oracle Identity Cloud Service
- Microsoft Active Directory（Active Directory Federation Services（AD FS）経由）
- Microsoft Azure Active Directory
- Okta
- Security Assertion Markup Language（SAML）2.0プロトコル互換サービス

サービスの管理には、以下のようなOCIインタフェースへのHTTPS接続を使用します。

- Webユーザー・インタフェース（Web UI）：[OCIコンソール](#)経由での臨時的アクション用
- [OCI Cloud Shell](#)（Cloud Shell）：OCIコンソール内のブラウザベースのLinuxシェル
- [OCIコマンドライン・インタフェース（OCI CLI）](#)：スクリプト作成や自動化のためのコマンドライン・インタフェース
- [OCI SDK](#)/REST API：アプリケーション統合用
- [OCI Terraform Provider](#)（HashiCorp提供のドキュメントを含む）

データベースの作成やOCPUのスケーリングといったクラウド自動化機能は、[OCI Identity and Access Management（IAM）](#)を使用して制御します。[OCI監査](#)で、これらのアクションを記録しておくことができます。

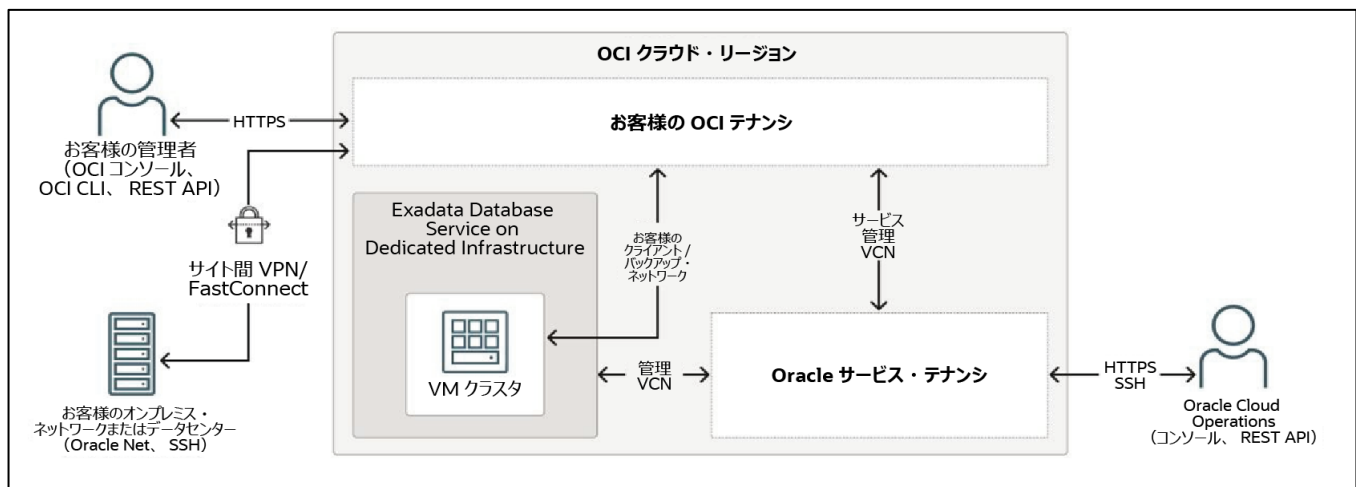


図1：ExaDB-Dアーキテクチャ

コントロール・プレーンは、オラクルの管理ネットワーク経由で、お客様の管理アクションに応じて、必要なコンポーネントに以下のようなコマンドを送信します。

データベース操作：

- VM内のエージェント・ソフトウェアへのREST APIアクセス
- mTLSによる保護
- ストレージ・ネットワーク経由での転送

VM操作：

- コントロール・プレーンのプロセスからサービス・アカウントへのトークンベースのSSH
- コントロール・プレーンが管理し、VM内のエージェント・ソフトウェア経由で配信される一時的な鍵による保護
- 管理ネットワーク経由での転送

インフラストラクチャ操作：

- インフラストラクチャ内のエージェント・ソフトウェアへのREST APIアクセス、およびコントロール・プレーンからインフラストラクチャのサービス・アカウントへのトークンベースのSSH
- mTLSおよびコントロール・プレーンが管理する鍵による保護
- 管理VCN経由で転送

互換サービスや互換ツールを使用してVMやデータベースに直接アクセスすることで、一部の管理機能を実行できます。詳細については、[Reference Guides for ExaDB-D](#)を参照してください。複雑さや運用負荷を軽減し、監査性を向上させるために、利用可能な場合はOCIインタフェースを使用することをお勧めします。

Oracle Cloud Operationsは、オラクルのサービス・テナンシーからHTTPSおよびSSHを使用してインフラストラクチャを管理します。HTTPSアクセスとSSHアクセスは、FIPS 140-2レベル3のハードウェアMFAデバイスによって認証されます。認可は、[オラクルの最小権限およびデフォルト拒否のアクセス制御慣行](#)に基づいています。オラクルのサービス・テナンシーにアクセスするには、Oracle VPNへのアクセスが必要です。商用のOracle Cloud Operationsのスタッフは、オラクルの施設外からサービスを管理する場合があります。

マルチテナント利用のためにオラクルがクラウドをどのように保護しているかの詳細については、[Oracle Cloud Infrastructure Security Architecture](#)を参照してください。

マルチクラウドにおける追加事項

[マルチクラウド](#)では、Oracle AI DatabaseのワークロードがAzure、Google Cloud、AWSのデータセンターで稼働します。マルチクラウドのためのすべてのExadataハードウェアは、クラウド・プロバイダのデータセンターに物理的に設置され、クラウド・プロバイダのネットワークでクラウド・プロバイダのサービスに接続されています。オラクルは、オラクルが管理するネットワークを通じてインフラストラクチャを管理します。これらのネットワークでは、マルチクラウド・インフラストラクチャとOCI管理ネットワークが統合されます。

図2は、マルチクラウド・アーキテクチャを示しています。ExaDB-Dは、以下の3つの追加要素によってCSPデータセンターに接続されます。

- OCI子サイト：ExaDB-D機器が設置されているCSPデータセンター内の場所
- プライベート接続：お客様のCSPのアプリケーション・ネットワークとExaDB-Dのネットワークを接続するネットワーク統合
- OCI制御ネットワーク：子サイトをOCIコントロール・プレーンに接続するネットワーク統合

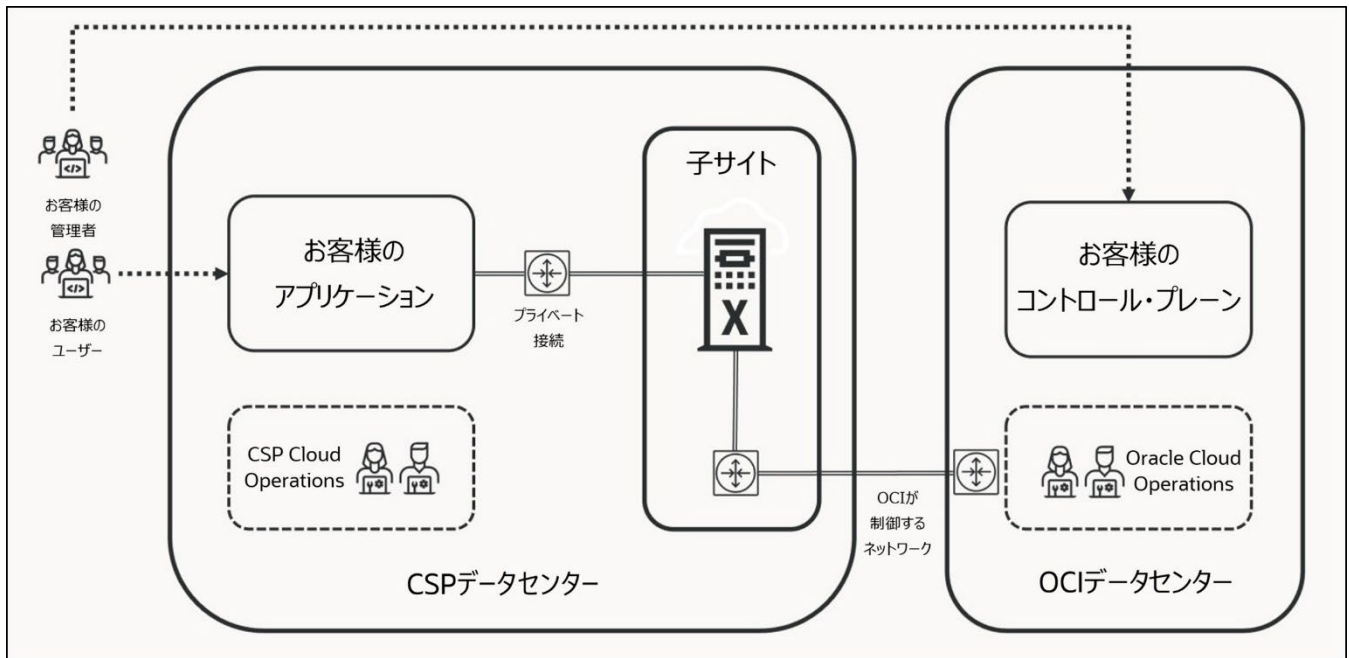


図2：マルチクラウド・アーキテクチャ

OCI子サイト

Oracle AI Databaseサービスは、CSPデータセンター内のOCI子サイトにデプロイされます。マルチクラウド・ラックには、OCIの標準のExaDB-Dのすべてのコンポーネントが含まれています。物理的な管理職務は、以下のように分離されています。

- CSPは、CSPの建物へのアクセスを制御します。
- オラクルは、子サイト内のハードウェアを保護するOracleケージへのアクセスを制御します。

[Oracle Global Physical Securityの制御](#)が、子サイトのOracleケージに適用されます。子サイトの論理セキュリティは、OCIデータセンター内のExaDB-Dの標準に従います。マルチクラウドに適用される物理セキュリティコントロールの詳細については、CSPにお問い合わせください。

プライベート接続

お客様のCSP資格証明により、CSPネットワークとExaDB-Dネットワーク間のプライベート接続がデプロイされます。ネットワーキング・ハードウェアのメンテナンスとサポートのアクセスは、CSPとオラクルのスタッフの間で以下のように分離されています。

- CSPサービスプリンシパルは、お客様のCSP APIに応じてCSPコンポーネントにアクセスします。
- OCIサービスプリンシパルは、お客様のCSP APIとOCI APIに応じてExaDB-Dコンポーネントにアクセスします。
- CSPのスタッフは、自分の資格証明を使用してCSPの機器にアクセスします。
- オラクルのスタッフは、自分の資格証明を使用してオラクルの機器にアクセスします。

マルチクラウドのExaDB-Dは、お客様のCSPネットワーク内のサブネットにデプロイされます。自動化により、お客様のCSPネットワークに一致するサブネットとIP CIDR範囲を持つOCI VCNが作成されます。このクラスタは、プライベートIPが割り当てられたVNICを使用して、OCIサブネット内で動作します。これらのプライベートIPアドレスは、お客様のCSPサブネット内でも予約されています。CSPデータセンター内でのCSPからOCIへの直接接続では、CSPネットワーク内の各プライベートIPが、VCN内の対応するVNICにマッピングされます。図3は、Oracle AI Database@Azureでの実装を示しています。オラクルは、他のCSPと同じようにこのサービスを実装しています。

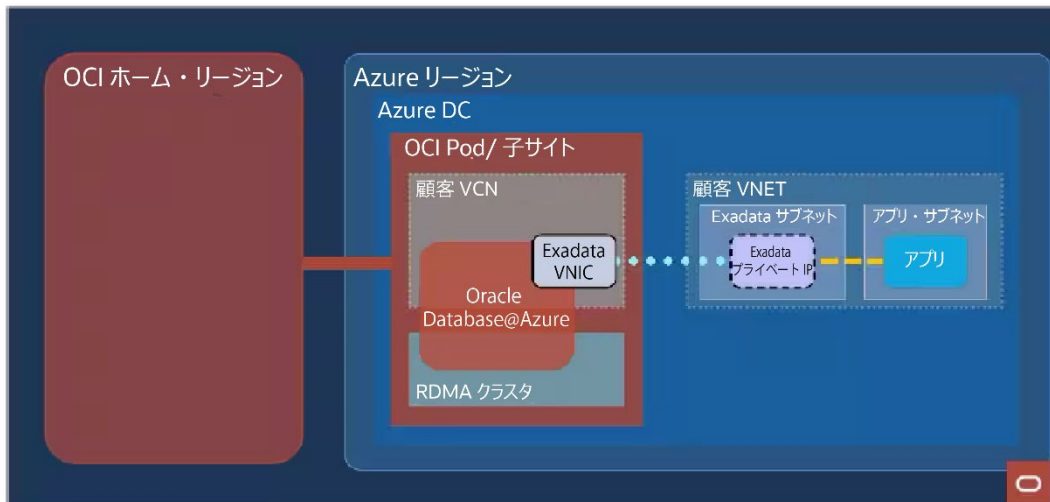


図3：Oracle AI Database@Azureプライベート接続

お客様のCSPネットワークでアプリケーションまたはユーザーが、割り当てられたプライベートIPアドレスを使用してデータベースに接続すると、仮想ネットワーク・サービスは、プライベート接続を経由してパケットを子サイト内にあるエッジ・ゲートウェイにルーティングします。OCI仮想ネットワーク・サービスは、エッジ・ゲートウェイから、Oracle AI Databaseインスタンスをホストするサーバーにパケットをルーティングします。直接プライベート・ネットワーク・リンクにより、アプリケーション、ユーザー、データベースのネットワーク・トラフィックがCSPデータセンターから流出するのを防ぐことができます。本書の「付録：技術的情報」にある図9、図10、図11は、Azure、AWS、Google Cloudにおけるマルチクラウドのネットワークキングを示しています。

どのCSPの場合でも、お客様はCSPネットワークとExaDB-Dネットワークから、お客様のデータベース（TNSリスナー・ポート）やVM（SSHポート22）へのアクセスを制御します。CSPネットワークにはCSPのネットワーク・セキュリティコントロールを、ExaDB-DネットワークにはOCIのネットワーク・セキュリティコントロールを適用できます。

OCI制御ネットワーク

OCI制御のプライベート・ネットワークにより、子サイトはOCIコントロール・プレーンに接続されます。このネットワークによって、以下を目的としたアクセスができるようになります。

- APIおよびコンソール主導のライフサイクル管理
- インフラストラクチャ・コンポーネントへのオラクルのサポート・スタッフのシェル・アクセスとAPIアクセス（必要な場合）
- お客様のビジネスの保護と運営に役立つオプションのOCIサービスへのアクセス

マルチクラウド・リソースに対してコンソールやAPIの呼出しを行う場合、それらの呼出しでは、下流のOCI APIとの認証にフェデレーションIDが使用されます。CSPコンソールを使用してExadata InfrastructureとVMクラスタを作成する場合、CSPコンソールはリソース・マネージャを呼び出し、リソース・マネージャがAPIリクエストをリソース・プロバイダにルーティングします。リソース・プロバイダは、変換、認可、認証を扱い、コントロール・プレーンを操作してデータベース・インスタンスを作成・管理します。図4は、Oracle AI Database@Azureを管理するためにOCI APIを呼び出すAzureインタフェースの統合を示しています。オラクルは、他のCSPと同じようにこのサービスを実装しています。

データベースのセキュリティコントロール

ExaDB-Dでは、Oracle AI Databaseのセキュリティ機能、互換OCIサービス、および互換鍵管理システムを利用できます。このセクションでは、一般的に使用されるソフトウェア、サービス、および鍵管理システムについてまとめています。

データベース認証

Oracle AI Databaseの認証は、[集中管理ユーザー](#)を使用して構成できます。これには、パスワード認証、[Kerberos認証](#)、または公開鍵インフラストラクチャ（PKI）認証が含まれています。集中管理ユーザーを使用すると、Active DirectoryユーザーにOracle AI Databaseへのアクセスを認可できます。[Oracle AI Databaseでは、ネイティブ・ユーザーに対して多要素認証（MFA）を構成できます。](#)これはOracle Mobile Authenticator（OMA）またはCisco Duoによるプッシュ通知、あるいは証明書ベースの認証のいずれかの形式となります。OCI IAM、MS-EI、RADIUSといった既存の外部認証方法を使用して、人間のユーザー向けのMFAを実装することもできます。

ネットワークの暗号化

ExaDB-Dは、デフォルトで[Oracle Native Network Encryption（NNE）](#)を使用して、クライアントからOracle AI Databaseインスタンスへの転送中のデータを暗号化します。[Oracle AI Databaseインスタンスはアプリケーションに暗号化接続を要求し、対応可能なアプリケーションとの間で暗号化接続を確立します。](#)暗号化接続をサポートできないアプリケーションの場合、Oracle AI Databaseインスタンスによって、アプリケーションは暗号化を使用しない接続を許可されます。この設定は、要件に応じて変更できます。

このサービスでは、Oracle CA署名付き証明書が使用されて、ポート2484上でOracle TCPS（TLS/SSL）が自動的に構成されます。お客様のクライアント向けの[HA対応接続バンドル](#)は、OCIインターフェースからダウンロードできます。このサービスにより、更新やローテーションを含め、証明書が管理されます。

証明書は、[TCPS（TLS/SSL）](#) および[mTLS](#)を、VMにデプロイされたオペレーション・システム・ツールを使用して構成することで使用できます。詳細は、ご使用のOracle AI Databaseバージョンの『Oracle Databaseセキュリティ・ガイド』にある[Oracle Native Network EncryptionとTCPS（TLS/SSL）](#)の説明を参照してください。

保管中のデータの暗号化

ExaDB-Dは、保管中のデータを[Oracle Transparent Data Encryption（TDE）](#)で暗号化します。TDEは、データ暗号化鍵（DEK）とマスター暗号化鍵（MEK）で構成される2層の鍵アーキテクチャです。表や表領域データを暗号化するDEKは、MEKによってラップされます。MEKは暗号化されたデータから分離され、データベースの外部に保存されます。TDE MEKは、以下のいずれかに保存できます。

- PKCS#12ウォレット
- OCI Vault
- Oracle Key Vault
- Azure Key Vault（Oracle AI Database@Azure向け）
- AWS Key Management Service（Oracle AI Database@Azure向け）
- Google Cloud Platform Key Management Service（Oracle AI Database@Google Cloud向け）
- サード・パーティ製の互換ハードウェア・セキュリティ・モジュール（HSM）

Oracle TDEは、高いパフォーマンスを発揮するように設計されています。Intel CPUの拡張命令セット（AES-NI）を自動的に活用し、暗号化処理を高速化します。さらに、TDEの表領域暗号化は、Exadata Hybrid Columnar Compression（EHCC）やSmart Scanテクノロジーとシームレスに連携します。TDEを使用すると、機密ユーザー・データは、表領域ストレージ・ファイル、一時表領域、UNDO表領域、またはREDOログなどのファイルのいずれにあるとしても、データベース内では暗号化された状態を維持します。また、TDEでは、データベースのバックアップ全体を暗号化することもできます。Data PumpとOracle Recovery Manager（RMAN）はどちらも、TDE暗号化データと統合します。[Oracle AI Database 26ai](#)には、[量子攻撃からデータベースを保護するために必要な暗号化アルゴリズムが組み込まれています。](#)Oracle TDEの詳細については、ご使用のOracle AI Databaseのバージョンの[Advanced Securityガイド](#)を参照してください。[Oracle TDE FAQ](#)には、アーキテクチャと実装に関する一般的な質問に対する回答が記載されています。

PKCS#12ウォレットによる暗号化鍵管理

TDE MEKはデータベースの外部に保存されます。デフォルトでは、PKCS#12準拠のコンテナ（'ウォレット'と呼ばれる）に保存されます。ウォレットは、ExaDB-DのVMからアクセス可能な共有ファイル・システムに保存されます。Oracle Database 18c以降では、外部で生成した独自の暗号化鍵（Bring-Your-Own-Keyを略してBYOKと呼ばれる）を共有ウォレットにアップロードできるため、データベース管理者と鍵管理者の職務分掌を維持できます。

OCI Vaultによる暗号化鍵管理

TDE MEKの保存には、OCI Vaultを使用できます。OCI Vaultでは、以下を利用できます。

- TDEのマスター暗号化鍵を管理するための別個のハードウェア
- 信頼性が高く、耐久性に優れた、完全管理型の鍵ストレージ
- FIPS 140-2レベル3の認定を受けたハードウェア・セキュリティ・モジュール（HSM）
- コンプライアンス要件を満たすことに役立つ、TDE鍵の自動ローテーション機能と監査機能

OCI VaultでExaDB-DのTDE鍵を管理するには、お客様はまずVaultサービスにアクセスし、暗号化鍵を作成する必要があります。使用する暗号化鍵アルゴリズムは、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してください。これらの前提条件の手順が完了したら、顧客管理鍵を使用してExadataデータベースを構成します。Oracle Database 11g リリース2（11.2.0.4）以降のデータベースのみがサポートされます。

Oracle Key Vaultによる暗号化鍵管理

ExaDB-DデータベースのTDE MEKの保存には、[Oracle Key Vault（OKV）](#)を使用できます。OKVによって、すべてのTDE対応データベースと暗号化されたOracle GoldenGate証跡ファイルに継続的なオンライン鍵管理が提供されます。また、外部で生成された鍵（BYOK）を取り込む機能も提供します。[OKV永続マスター暗号化鍵キャッシュ](#)を使用すれば、OKVサーバーが利用できない場合でもデータベースを操作可能にできます。詳細については、[Migration of file-based TDE to OKV for Exadata Database Service Using Automation via REST（KB79439）](#)を参照してください。

Azure Key Vaultによる暗号化鍵管理

Oracle AI Database@Azureのサブスクリバは、[Azure Key Vault（AKV）Managed HSM、AKV Premium、およびAKV StandardをTDE MEKの管理](#)に使用できます。この統合により、アプリケーション、Azureサービス、データベースは、一元化された鍵管理ソリューションを使用できるようになり、セキュリティの強化と鍵ライフサイクル管理の簡素化を実現できます。

AWS Key Management Serviceによる暗号化鍵管理

[Oracle ExaDB-D on Dedicated Infrastructure on Oracle AI Database@AWS](#)は、[AWS Key Management Service（KMS）との統合をサポートしています](#)。この機能により、ユーザーはAWS顧客管理鍵を使用して、Transparent Data Encryption（TDE）のマスター暗号化鍵（MEK）を管理できます。

Google Cloud Key Managementによる暗号化鍵管理

[ExaDB-D on Oracle AI Database@Google Cloud](#)は、[Google Cloud PlatformのKey Management Service（KMS）との統合をサポートしています](#)。これにより、ユーザーはGCP顧客管理暗号鍵（CMEK）を使用して、Transparent Data Encryption（TDE）のマスター暗号鍵（MEK）を管理できます。

サード・パーティ製ハードウェア・セキュリティ・モジュール（HSM）による暗号化鍵管理

[Oracle AI Database](#)は、[PKCS#11準拠の鍵管理デバイスと互換性があります](#)。サード・パーティの鍵管理ベンダーとHSMベンダーは、このインタフェースを利用して、Oracle AI Database向けのTDE鍵管理機能を実装しています。実装やサポートの詳細については、[My Oracle Support（MOS）ノートのOracle TDE Support With 3rd Party HSM Vendors（KB593570）](#)を参照してください。

外部鍵マネージャを統合するには、ExaDB-D VMにPKCS#11ライブラリをインストールする必要があります。この統合の構築、テスト、ドキュメント作成、サポートは、サード・パーティの鍵マネージャやHSMのベンダーまたは実装担当者が行います。オラクルは、Oracle AI Databaseとの適合性を保証するサード・パーティ製鍵マネージャやHSMの認定プログラムを保持していません。また、Oracle Transparent Data Encryption対応のデータベース向けに鍵管理を提供するサード・パーティ製のHSMもサポートしていません。

HSMベンダーは、自社のデバイスについて自己認定を実施することで、Oracle Key Vaultに信頼の起点を提供できます。その際には、[Oracle Key Vault Root of Trust HSM Configuration Guide](#)の“Vendor Instructions for Integrating an HSM as the Root of Trust for Oracle Key Vault”を参照する必要があります。

データベース・バックアップの暗号化

[すべてのバックアップは、Transparent Data Encryptionウォレットの暗号化に使用されるものと同じマスター鍵で暗号化されます](#)。暗号化鍵はバックアップと一緒に保存されることはありません。TDEマスター暗号化鍵のバックアップとリストアを実施する責任はお客様にあります。

[Autonomous Recovery Service](#)を使用する場合、[暗号化された表領域のバックアップと、それらの表領域への変更を記述したREDOログが暗号化されます](#)。TDE暗号化データ・ブロックは、データベース上、Recovery Applianceのストレージ、テープ・デバイス、およびレプリケート先のアプライアンス上で暗号化され、ネットワーク接続経由の転送時にも暗号化されます。

SQLを使用したデータベース管理者によるユーザー・データへのアクセス防止

[Oracle Database Vault](#)は、データベース管理者によるアクセスからアプリケーション・データを保護し、プライバシー情報の取扱いと規制の要件に対応する助けになります。制御をデプロイして、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、信頼パス認可使用してデータベース内の機密操作を制御できます。さらに、Oracle Database Vaultによって既存のデータベース環境を透過的に保護することができ、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。Oracle Database Vaultのドキュメントは、ご使用のデータベース・バージョン向けに発行される[Oracle Database Vault管理者ガイド](#)に公開されています。

SQLインジェクション攻撃の軽減

[Oracle SQLファイアウォール](#)により、特定のユーザーに対して許可されたSQL文や接続のみにデータベース・アクセスは制限され、一般的なデータベース攻撃に対するリアルタイムの保護が提供されます。SQLインジェクション攻撃、異常なアクセス、および資格証明の盗難や悪用によるリスクが軽減され、潜在的なSQLインジェクション攻撃を防止または検出できます。SQLファイアウォールを使用すると、データベースにどのSQL文の処理を許可するかを制御できます。さらに、SQLファイアウォールはIPアドレスなどのセッション・コンテキスト・データを使用してデータベース接続を制限することもできます。許可されていないSQLとデータベース接続は、ログに記録してブロックできます。

SQLファイアウォールは、以下の3つのユースケースに対応できます。

- 認可されたSQL文とデータベース接続のみにデータベース・アクセスを制限することにより、リアルタイムの保護を提供
- SQLインジェクション攻撃、異常なアクセス、資格証明の盗難/乱用リスクを軽減
- 信頼できるデータベース接続パスを適用

SQLファイアウォールには、以下の利点があります。

- PL/SQLからのものを含む、すべての着信データベース接続とSQL文を検査
- 承認されていないSQLをブロックするか、ログに記録するだけとするかを選択
- SQL全体および処理コンテキストを評価
- 信頼できるIPアドレス、オペレーティング・システム・ユーザー名、またはプログラム名以外からの接続をブロック
- 標準的なデータベース・ユーザーが実行するSQL文の各データベース・ユーザーに対して許可リスト・ポリシーを構築し、予期しないSQLを検出、ブロック、ログ記録できるようにする

詳細は、[SQLファイアウォールの製品ドキュメント](#)を参照してください。SQLファイアウォールは、データベース・バージョン26aiから利用可能です。

データベース・セキュリティの監視と管理

Oracle AI DatabaseおよびExaDB-Dと互換性があるソフトウェアやサービスを使用して、データベースのセキュリティ体制の監視や管理ができます。オラクルは、ExaDB-Dデータベース向けに、Oracle Data SafeやOracle AI Database Security Assessment Tool（DBSAT）などのセキュリティ監視・管理ツールを提供しています。

Oracle Data Safe

[Oracle Data Safe](#)は、OCIクラウド・サービスであり、以下のようなことができます。

- データベースのセキュリティ構成を評価する
- 構成のずれを検出する
- 高リスクのデータベース・アカウントを特定し、そのアクティビティを表示する
- 監査ポリシーをプロビジョニングする
- 監査データを分析する（レポートの生成やアラートの生成を含む）
- 機密データを検出する（データの種類、データの量、データの場所を含む）
- 機密データをマスクして、非本番データベースのコピーからセキュリティ・リスクを排除する

[Oracle Data Safeのアーキテクチャ](#)では、実装の詳細を示しています。[Data Safe FAQ](#)には、Oracle Data Safeに関するよくある質問への回答が記載されています。1か月の監査レコードが1データベースあたり100万件を超えない限り、Oracle Data Safeの使用に追加コストはかかりません。

Oracle Database Security Assessment Tool

[Oracle Database Security Assessment Tool（DBSAT）](#)は、評価と規制コンプライアンスのプロセスを迅速化する、スタンドアロンのコマンドライン・ツールです。DBSATは関連する構成情報をデータベースから収集し、セキュリティ状態を評価するとともに、特定されたリスクを軽減する以下のような推奨方法を提案します。

- セキュリティ構成の問題とその修正方法
- ユーザーとそのエンタイトルメント
- 機密データの場所、種類、量

また、簡単な構成チェックが行われるだけでなく、ユーザー・アカウント、付与されている権限およびロール、認可制御、職務分掌、ファイナンス・アクセス制御、データ暗号化、鍵の管理、監査ポリシー、OSファイルのパーミッションも調査されます。DBSATではルールを応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緩和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。Oracle DBSATで説明されている包括的な測定と補償制御を適用することで、お客様は企業全体でデータ漏洩のリスクを軽減できます。

ExadataストレージへのVMクラスタのアクセスの制御

[ASM-Scoped Security](#)では、ストレージ・セル上の特定のグリッド・ディスクにアクセスできるOracle Automatic Storage Management (ASM) のクラスタとOracle AI Databaseのクライアントが制御されます。Oracle Exadata System Softwareでは、クライアントを識別し、グリッド・ディスクへのアクセス権を決定するためにSecurity Keyが使用されます。Oracle Exadata Storage Serverでは、アクセス権が必要とされます。クラウド自動化ソフトウェアにより、ASM-Scoped Securityと必要なSecurity Keyが自動的に構成されます。これにより、VMクラスタ内のすべてのVMが、そのVMクラスタに割り当てられているExadataストレージ（ASMディスク・グループ）にアクセスできるようになり、同時に、他のVMクラスタに割り当てられているものへはアクセスできなくなります。同じExadata Database Machine上でスコープ内とスコープ外のVMクラスタをホストするというコンテキストでのASM-Scoped Securityの例については、[Oracle Exadata Database Machine and Complies with PCI-DSS V3.2](#)を参照してください。

VMのセキュリティコントロール

[ExaDB-D VMは、セキュリティが強化されたオペレーティング・システムでデプロイされます。](#)これには以下が含まれます。

最小限のパッケージ・インストールと最小限のサービスの有効化：

- 効率的なシステムの稼働に必要なパッケージのみインストール
- システムにインストールされていたとしても、通常の操作に不要なサービスはデフォルトでは無効化
- 要件に応じてサービスは任意に構成可能

セキュアな構成：

- システムのセキュリティ体制を強化するため、インストール時に構成パラメータを設定
- SSHは特定のネットワーク・インタフェースでのみリスニングするように構成
- sendmailはlocalhost接続のみを受け入れるように構成
- grubパスワードを利用

セキュアなアクセス方法：

- 強力な暗号化を使用したSSH経由でのデータベース・サーバーへのアクセス
- 弱い暗号化はデフォルトでは無効化
- Exadata MS Webインタフェース（HTTPS）経由での診断へのアクセス

監査とロギング：

- 管理操作に対する監査が有効化
- 監査レコードは、自動化されたレビューやアラートのために外部システムに送信可能

[VMへのアクセスには、トークンベースのSSHを使用します。](#)OCI資格証明を使用して、お客様が指定した公開鍵を/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の対になる秘密鍵にアクセスできるスタッフは、opcユーザーとしてVMにアクセスできます。Oracle Cloud Automationは外部鍵管理システムとは統合されませんが、Oracle Linuxに対応したテクノロジーを使用してSSH鍵を管理できます。詳細については、該当するPAMプロバイダにお問い合わせください。[APIアクセス制御を使用してSSH鍵追加機能を制御し](#)、SSH鍵を追加しようとするOCI IDは、別のOCI IDからの承認を得なければならないようにすることができます。

Exadataソフトウェア・バージョン22.1.4.0.0.221020以降では、VMに対する認証にMicrosoft Active Directory（AD）およびLightweight Directory Access Protocol（LDAP）がサポートされています。ADとLDAPは、Linuxシステム・セキュリティ・サービス・デーモン（SSSD）を使用して構成します。Oracle Linux 8上では、SSSDサポートは、Exadata固有のセキュリティ・プロファイルと組み合わせて、Linuxのauthselectユーティリティを使用して有効化されます。[Oracle Exadata System Softwareは、システム更新中も既存のSSSD構成の詳細情報を保持します。](#)

[トークンベースのSSH経由のOracle Cloud Automationセキュア・ログインは、Kerberos認証と互換性がありません。](#)VM内でKerberos認証を実装し、[特権ユーザー・アカウント](#)（root、oracle、grid、opc、およびdbmadmin）への認証に追加のチャレンジを要求するようにした場合、SSHでVMにアクセスするOracle Cloud Automation機能は失敗します。Oracle DatabaseのユーザーにはKerberos認証を使用できます。

VMのデフォルトのセキュリティ設定

お客様のExaDB-D VMは、業界標準およびオラクルのベスト・プラクティスに準拠したセキュリティ設定でデプロイされています。この構成は、アクセス制御の実施、運用リスクの低減、および自動化ライフサイクル管理のサポートに役立ちます。主要な設定には以下のようなものがあります。

- パスワードのエージングと複雑さ
- アカウント・ロックアウトとセッション・タイムアウトのポリシー
- SSH経由でのrootによる直接ログインの拒否

技術的な設定には以下のようなものがあります。

- `/etc/ssh/sshd_config`内の`PermitRootLogin`値。rootユーザーによるSSH経由のログインを許可/拒否します。
 - デフォルト：`PermitRootLogin`は`without-password`に設定されています。
 - 推奨：OSパッチ適用などのクラウド自動化機能が許可されるように、デフォルトのままにしておいてください。
- `session-limit`：`/etc/security/limits.conf`内の`hard maxlogins`パラメータ。全ユーザーの最大ログイン数を示します。この制限は`uid=0`のユーザーには適用されません。
 - デフォルト：`hard maxlogins 10`
 - 推奨：デフォルトのままにしておいてください。
- `ssh-macs`：使用可能なメッセージ認証コード（MAC）アルゴリズムを指定します。
- MACアルゴリズムは、バージョン2のプロトコルでデータの整合性を保護するために使用されます。
 - デフォルト：サーバーとクライアントの双方で、`hmac-sha1`、`hmac-sha2-256`、`hmac-sha2-512`
 - 推奨：デフォルトのままにしておいてください。
- `password-aging`：対話型ユーザー・アカウントの現在のパスワードのエージングを設定または表示します。
 - `-M`：パスワードを使用できる最大日数
 - `-m`：パスワードを変更できるようになるまでの最小日数
 - `-W`：パスワードの有効期限が切れる前に警告が出される日数
 - デフォルト：`-M 99999`、`-m 0`、`-W 7`
 - 推奨：厳格にコンプライアンスを維持するために、`-M 60`、`-m 1`、`-W 7`

シェルのタイムアウトは、長時間実行される自動化タスク（ASMリバランスなど）に対応できるように構成されています。これらの値はサービス構成の一部であり、セキュリティ・スキャン・ツールで許可する必要があります。

一部のクラウド自動化機能には、`PermitRootLogin=without-password`が必要です。その場合、`PermitRootLogin=no`に設定すると、クラウド自動化機能のアクションは失敗します。アクションを実行するには、`PermitRootLogin=without-password`に設定する必要があります。`PermitRootLogin`は、オペレーティング・システムのツールを使用して、独自の基準に合わせて管理できます。

テストやメンテナンスの手間を減らし、構成変更によるサービス中断のリスクを回避するために、デプロイ済みの設定を維持することをお勧めします。

VMのデフォルト・ユーザー

各ExaDB-D VMには、オラクルがサービスの提供やメンテナンスに使用する特権サービス・アカウントが含まれています。トークンベースのSSHログインが必要です。パスワードベースのSSHログインは無効になっています。サービス・アカウントには以下が含まれます。

- `root`：Linuxでは必須です。ソフトウェアの更新や一部のバックグラウンド・プロセス（Oracle Trace File Analyzer AgentやExaWatcherなど）に使う権限として使用されます。
- `grid`：Oracle Grid Infrastructureのソフトウェアとプロセスを所有、実行、メンテナンスします。
- `oracle`：Oracle AI Databaseのソフトウェアとプロセスを所有、実行、メンテナンスします。
- `opc`：Oracle Cloud Automationで使用されます。
 - 自動化タスクを実行
 - 特定の特権コマンドを実行可能
 - サービス・ライフサイクル操作のためのコントロール・プレーン・エージェント・ソフトウェア（DBCS AgentとDBCS Admin）を実行
- `dbmadmin`：[DBMCL](#)ツールと組み合わせて、Exadataのコア機能を管理するために使用されます。

セキュリティ・スキャン・ツールでは、これらのアカウントをサービス・アカウントとして分類する必要があります。`opc`アカウントは、ExaDB-Dソフトウェアと互換性のあるLDAPやPAMソフトウェアの構成など、管理目的で使用できます。

デプロイ済みのユーザー名、ユーザーID、グループ名、グループIDは、そのままにしておく必要があります。[インストール後にOracleホーム・ユーザー（oracle）やGrid Infrastructureユーザー（grid）を変更することはサポートされておらず、サービスの例外が発生する原因となります。](#)

VMファイルの整合性監視

ファイルとディレクトリの整合性をチェックするために、ExaDB-Dには[Oracle Linux Advanced Intrusion Detection Environment \(AIDE\)](#) が組み込まれています。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、コンパクトながら強力な侵入検出ツールであり、事前定義されたルールを使用してファイルとディレクトリの整合性をチェックします。これは、ウイルス、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備えることで、システムを内部的に保護することを意図しています。これは、簡素化されたクライアント/サーバー監視構成用の独立した静的バイナリです。AIDEはオンデマンドで実行されます。変更を報告する時間は、`/etc/aide.conf`で設定されたシステム・チェックに応じて異なります（通常は1日1回以上）。この構成ファイルでは、AIDEによって監視されるファイルやディレクトリ、およびロギングや出力の処理方法が定義されます。詳細については、[Oracle Linux : Advanced Intrusion Detection Environment \(AIDE\) Usage and HOWTO \(KB385603\)](#) を参照してください。

VMバックアップ暗号化

物理的なデータベース・サーバーの障害からリカバリできるように、[オラクルはExaDB-Dインフラストラクチャ・ラック内のコンポーネントにVMのイメージをバックアップします](#)。オラクルはこのバックアップを暗号化し、バックアップ暗号化鍵を管理します。バックアップを保存しているラック内のコンポーネントにアクセスできれば、オラクルはそのイメージをリストアできます。

クラウド自動化によるお客様のVMへのアクセス

Oracle Cloud Automationソフトウェアは、以下の2つの方法でお客様のデータベースとVMにアクセスします。

- ポート7060と7070でのmTLS認証を介した、VMで実行されているOracle DBCSエージェントへのREST API呼出し
- トークンベースのSSH経由で特権ユーザー（root、opc、grid、oracle）としてVMに安全にログイン

コントロール・プレーンは、各管理アクションに対して一時的かつ一意のSSH鍵ペアを生成します。公開鍵は、DBCSEージェントによってVMにおいて必要なサービス・アカウントの`~/.ssh/authorized_keys`ファイルに追加されます。秘密鍵は、コントロール・プレーンのインフラストラクチャ内に保存されます。アクションの完了後、コントロール・プレーンは秘密鍵を破棄し、一時的な鍵を削除します。

VMは、VMへのネットワークをブロックする追加のデータ保護制御として、[Oracle Linuxパケット・フィルタリング・ソフトウェア](#)を提供します。コントロール・プレーンからのSSHアクセスをブロックすると、以下のサービス機能が動作しなくなります。

- データベース・ソフトウェアの更新
- Oracle Grid Infrastructureのソフトウェア更新
- VMオペレーティング・システムのソフトウェア更新
- オラクルが管理するインフラストラクチャの四半期ごとのソフトウェア更新（VMでのCRS再起動の検証に使用）
- データベース・サーバー・インフラストラクチャの追加
- VMクラスタ・ノードの追加
- VMクラスタ・ノードの削除
- ストレージ・サーバーの追加

OCPUのスケールングにはVMへのSSHアクセスは不要であり、ネットワーク層でVMへのクラウド自動化アクセスをブロックした場合でも機能し続けます。

お客様のVMへのオラクルのサービスとサポートのスタッフによるアクセスの制御

[Delegate Access Control](#)を使用すると、お客様のVMでデータベースのメンテナンスとサポートのサービスをサブスクライブし、サービス・プロバイダのスタッフによるアクセスを制御・監視できます。以下の5つのサービスをサブスクライブできます。

- Oracle Database Cloud Customer Support : データベースとOracle Linuxテクノロジーのサポート・サービス（追加料金なしで付属）
- Oracle Database Cloud Operations Support : VMにデプロイされたクラウド自動化ソフトウェアのサポート・サービス（追加料金なしで付属）
- Oracle-Managed Software Updates for Database Cloud Services : VMソフトウェアの更新に関するサポート・サービス（追加料金なしで付属）
- Oracle Engineered Systems Deployment and Infrastructure Support : ご利用のサービスに対するパッチ適用とトラブルシューティングの支援（別途購入）
- Strategic Customers Program for DB Cloud Platforms : カスタム・サポート・サービス（別途購入）

Delegate Access Controlを使用する場合、以下が適用されます。

- オラクルのスタッフは、お客様の承認をいただいた後のみお客様のVMにアクセスします。
- [アクションの適用](#)により、アクセスは作業リクエストに関連する承認済みコンポーネントに限定されます。

管理者はデータに対して特定のアクセス経路を定義できます。ポリシーで明示的に許可されていないトラフィックはネットワークを通過できないため、セキュリティが向上し、セキュリティ・チーム、ネットワーク・チーム、監査チームの業務は簡素化されます。

お客様のネットワークから使用できる資格証明の制御

ExaDB-Dサービスで、[サービス・ゲートウェイ](#)の代わりに[Private Service Access \(PSA\)](#)を使用することで、サービス単位でのきめ細かなネットワーク・アクセス制御が可能になります。PSAは、OCIサービスAPIに到達するための経路として、そのAPIのパブリックIPではなく、お客様のネットワークのプライベートIPを使用します。PSA経由でサービスにアクセスする際は、テナンシー内の資格証明が適用され、クロステナンシーの資格証明の使用とクロステナンシーのオブジェクト・ストレージPARIによるアクセスはブロックされます。

[ExaDB-Dをサポートするには、以下のPSAを作成する必要があります。](#)

- データベース・サービス：リソース・プリンシパル認証とサービス・メタデータへのアクセスに使用
- Oracle Identity and Access Managementのデータ・プレーンAPI：サービス認証に使用
- Object StorageサービスAPI：ソフトウェア更新やカスタム・イメージのダウンロードに使用
- ファンクション・サービスの呼出し：サービス監視に使用
- OCI Monitoringによる取込み：サービス監視に使用
- ロギング取込みAPI：サービス監視に使用

また、PSAを構成したネットワークから、ポート443でサブネットへのインバウンド・アクセスを許可するネットワーク・セキュリティ・ルールを作成する必要があります。

OCIの追加のセキュリティコントロール

OCIは、ExaDB-Dをサポートするその他のセキュリティ・サービスも提供しています。このセクションでは、一般的に使用される制御についてまとめています。

テナンシー・リソースの認証を受けることができるネットワークの制御

[ネットワーク・ソース](#)を使用すると、テナンシー・リソースから認証を受けることができる接続を、特定のIPアドレス（企業VPNからの通信を許可するプロキシなど）を起点とする接続に限定できます。データセンターからOCIリージョンへのサイト間VPNやFastConnectを実装している場合、OCIコンソールとAPI接続を[トランジットVCN](#)経路でルーティングできます。これにより、オンプレミス・ネットワークからオラクルのサービスへのプライベート・アクセスが可能になります。そのため、オンプレミスのホストはプライベートIPアドレスを使用できるようになり、トラフィックはパブリック・インターネットを経由しなくなります。

テナンシー内での特定のAPIアクションの拒否

[IAM Deny](#)ポリシーでは、denyステートメントが導入されています。これによりポリシー管理が簡素化され、リソースへのアクセス制限をより簡単に実施できるようになります。コンソールのガイド付きワークフローを通じてdenyポリシーを有効化できるのは、デフォルトのドメイン内のデフォルトの管理者グループのメンバーのみです。セットアップ時には、以下のデフォルトのルートレベル・ポリシーによって、どのユーザーがdenyステートメントを管理できるかが制限されます。これにより、IAM Denyを有効化したテナンシー管理者とデフォルトの管理者グループのメンバーだけが、denyポリシーの作成を許可されます。デフォルトのドメイン内のデフォルトの管理者グループのメンバーは、常にdenyポリシーの適用対象外となり、最上位レベルでの継続的なアクセスが保証されます。

リスクを管理するために、管理者はdenyポリシーの変更に関する通知を有効にすることができます。denyポリシーはセキュリティと柔軟性を高めますが、子コンパートメントの管理者はdenyポリシーを使用して親のアクセスをブロックすることができるため、慎重に管理する必要があります。denyポリシーは、許可ポリシーよりも優先されます。

お客様の管理者による特権APIの使用の制御

[Oracle API Access Control](#)により、特権APIに対して必須の承認ワークフローが追加されます。これをCloud Exadataインフラストラクチャで有効にすると、関連するクラウドVMクラスターやコンテナ・データベースにも保護が拡張されます。具体的には、以下の[特権OCIコンソールとAPI機能](#)に対して、複数のIDによる承認ワークフローが強制されます。

- データベース、VMクラスター、インフラストラクチャの削除
- Oracle Database、Oracle Grid Infrastructure、オペレーティング・システム・ソフトウェアの更新
- Data Guardのスイッチオーバー
- VMコンソール接続の作成
- VMへのSSH鍵の追加

特権APIを呼び出す前に、そのAPIを呼び出そうとするユーザーは、自身のOCI IDを使用してアクセス・リクエストを出す必要があり、そのアクセス・リクエストは別のOCI IDで承認する必要があります。図6は、APIアクセス制御承認ワークフローを示しています。詳細については、[API Access Control at the Oracle Learning Center](#)を参照してください。Oracle API Access Controlは追加料金なしで利用できる付属機能です。

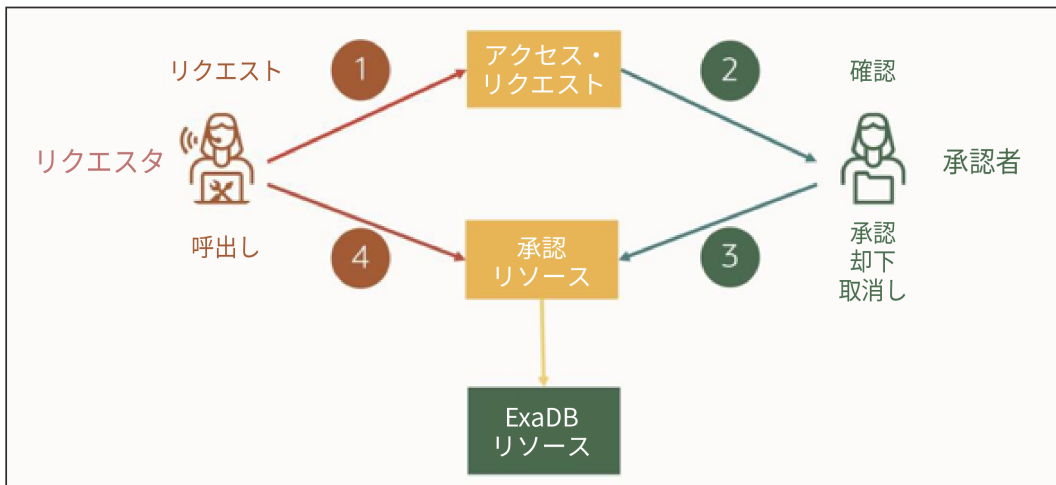


図6：APIアクセス制御承認ワークフロー

ランサムウェアからのリカバリ

[Oracle Database Autonomous Recovery Service](#) (Recovery Service) は、完全管理型でスタンドアロンの一元化データベース保護サービスであり、OCI、マルチクラウド、オンプレミスにデプロイされたOracle AI Database向けとなっています。データベースをランサムウェアから保護するように設計されており、以下の4つの主要な技術的柱で構成されます。

- データベース保護：これにはリアルタイムのトランザクション保護、エンドツーエンドのランサムウェア保護、および不変性が含まれます。
- リカバリの保証：これには継続的なバックアップ検証、データベース保護の監視、専用ネットワーク経由での高速データベース・リストア機能が含まれます。
- レジリエンスがあるアーキテクチャ：Oracle Exadataエンジニアド・システムの設計手法を基本とする、コンピュート・サーバーとストレージ・サーバーの基盤上に構築されています。ユーザー・モデルは職務分掌が図られており、データベース、Recovery Appliance、関連アプライアンスの役割はそれぞれ互いから分離されています。そのため、どのユーザーも、権限を持たない他のシステムにアクセスすることはできません。
- 不変のバックアップ：侵害を受けたシステム上にあるバックアップそのものが、内部プロセスや外部ユーザーによって消去または削除されるのを防ぎます。

Recovery Serviceは、サイバー攻撃に対する回復力と復旧能力を備えています。本番データベースから障害分離されるように設計されており、本番データベースがサイバー攻撃を受けた場合でも、Recovery Serviceが侵害されることはありません。オラクルは、ランサムウェアからOracle AI Databaseを保護するために、Recovery Serviceを使用することを推奨しています。

Oracleインフラストラクチャのセキュリティコントロール

オラクルは、[Oracle PaaSおよびIaaSのドキュメント](#)で説明しているとおり、インフラストラクチャのセキュリティと可用性を独占的に管理しています。[オラクルの企業セキュリティ慣行](#)は、オラクルの社内業務とクラウド・サービスにおけるセキュリティ管理を対象としています。これは、従業員や契約業者を含むすべてのオラクル関係者に適用されます。これらのポリシーは、ISO/IEC 27002:2022（旧称ISO/IEC 17799:2005）およびISO/IEC 27001:2022標準に準拠しており、オラクル社内におけるセキュリティのすべての領域で指針となります。オラクルは自動化されたHRの入社/異動/退職プロセスを実装し、それによってインフラストラクチャへのアクセス権限と、従業員のジョブコード、トレーニング記録、雇用ステータスの更新との整合性を確保しています。オラクルは、[オラクルのアクセス制御](#)に従って、最小権限およびデフォルト拒否のアプローチによってクラウド運用へのアクセスをさらに厳格に管理しています。このアプローチではアクセス権は以下のように付与されます。

- 知る必要性のあるユーザー
- 業務を行うための最小権限
- 利害の対立を防止するための職務分掌

Oracle Cloud Operationsのスタッフは、以下を含むサービス・インフラストラクチャのコンポーネントにアクセスし、それをサポートします。

- 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
- Oracle Exadata Storage Server
- 物理Exadata Database Server

図7は、Oracle Cloud OperationsのスタッフがExaDB-Dインフラストラクチャ・コンポーネントにどのようにアクセスするかを示しています。オラクルは、ExaDB-DインフラストラクチャへのOracle Cloud Operationsスタッフのアクセスを次の方法で制御します。

OCNAアクセス：

- ジョブコードとトレーニング記録に基づいて権限を付与
- FIPS 140-2レベル3のハードウェアMFAデバイスを使用して認証
- OCNAに接続するにはユーザー・デバイスはセキュリティ・スキャンにパスすることが必須

Bastionホストへのアクセス：

- ジョブコードとトレーニング記録に基づいて権限を付与
- OCNAへのアクセスが必要
- サービスをホストしているリージョンの特権管理VCNに分離
- FIPS 140-2レベル3のハードウェアMFAデバイスを使用して認証
- 接続ロギングと監視は名前付きユーザーまで追跡可能

ExaDB-D管理サーバーとインフラストラクチャへのアクセス：

- ジョブコードとトレーニング記録に基づいて権限を付与
- Bastionホストへのアクセスが必要
- FIPS 140-2レベル3のハードウェアMFAデバイスを使用して認証
- 接続ロギングと監視は名前付きユーザーまで追跡可能

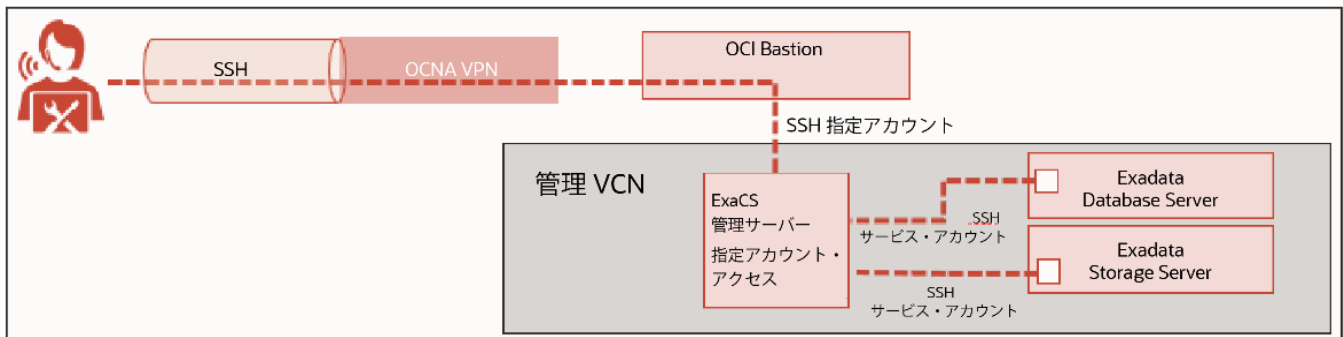


図7：ExaDB-DインフラストラクチャへのCloud Operationsシェル・アクセス

オラクルの商用のOracle Cloud Operationsのスタッフは、世界全体でフォロー・ザ・サン・モデルで勤務し、24時間365日体制のサポートを提供しています。商用のOracle Cloud Operationsのスタッフは、オラクルの施設外からサービスを管理する場合があります。

お客様のインフラストラクチャへのオラクルのスタッフによるシェル・アクセスの制御

責任共有モデルが理由で、ミッション・クリティカルなワークロードや規制対応が厳しいワークロードをクラウドで運用することは困難である場合があります。この手法では、クラウド・プロバイダがインフラストラクチャを管理し、お客様が仮想マシン、アプリケーション、データベースを監督します。お客様がご自身の環境内で行われるすべての操作に対して責任を負う場合（お客様の専用インフラストラクチャに対するクラウド・プロバイダのスタッフによる操作を含む）、[Oracle Operator Access Control](#)がその監視ニーズへの対応を支援します。これは、リスク管理が極めて重要な組織（銀行、金融サービス、エネルギー、防衛、その他の厳格な管理が求められる環境）向けに設計されており、ExaDB-D、およびExaDB-D上のAutonomous Database Dedicated（ADB-D）で使用できます。

Operator Access Controlは特権アクセス管理（PAM）サービスであり、変更管理プロセスや変更管理システムと統合して以下を行うことができます。

- オラクルのスタッフが、お客様のExaDB-Dの物理データベース・サーバーとストレージ・サーバーのインフラストラクチャ、およびADB-D VMにアクセスするタイミングと範囲を制御する
- オラクルのスタッフが、お客様のExaDB-Dの物理データベース・サーバーとストレージ・サーバーのインフラストラクチャ上で実行するオラクル・オペレータ・コマンドとキーストロークを監視し、記録する
- お客様の判断でOracle Operatorの接続を終了する

これらの制御はExaDB-Dサービスの標準機能であり、追加費用なしで利用できます。お客様がOperator Access Controlを使用する場合、以下のようにアクセスを制御できます。

- アクセスは、オラクルからリクエストがあり、お客様が承認した後に許可される
- 作業リクエストごとに固有の一時アカウントを使用して実施され、実行したスタッフを特定できる
- 承認されたユーザーの一時的なネットワーク・アクセスで実装される
- 指定された特定の作業リクエストに関連する、明示的に承認されたコンポーネントに限定される
- 作業リクエストの期間に限定される
- タスクの完了後またはタイムアウトとなった場合は自動的に取り消される

Operator Access Controlの[アクションの適用](#)制御特権は、オラクル・オペレータに制限を適用します。[Operator Access Control Audit Logs](#)は追跡可能で、実行したスタッフを特定できます。調査やコンプライアンス上の理由で必要な場合、オラクルはスタッフのID詳細情報を提供できます。

オラクル・オペレータのアクセス権は取り消すことができます。Operator Access Controlを取り消すと、以下のようになります。

- SSHセッションが終了する
- 一時アカウントによって開始されたプロセスが終了する
- ExaDB-DインフラストラクチャとADB-D VMから一時アカウントが削除される

ExaDB-Dサービスをサポートするには、[Operator Access Controlアクセス・リクエスト](#)を24時間365日体制で監視し、対応する必要があります。[OCI Events Service](#)および[OCI Notifications](#)を使用すると、新しいリクエストが発生した際に、お客様のスタッフに自動的にアラートで通知できます。[Splunk](#)や[ServiceNow](#)などのシステムを統合し、対応プロセスを効率化できます。

すべてのリクエストを監視したり対応したりすることができない場合や、自動承認がニーズに適している場合は、[Operator Access Controlの事前承認機能](#)を使用してください。事前承認機能を使用すれば、スタッフはOCIで個々のリクエストを承認しなくても、一時的なジャストインタイムでのアクセスと完全な監査ログの取得ができます。これにより、運用負荷が軽減され、遅延に起因して重大な問題やサービス停止が生じるリスクを低減できます。メンテナンス期間に合わせて事前承認を設定すると、更新作業を効率化できます。リスクと運用効率のバランスを取りやすくするために、選択的に[低い権限については選択的に事前承認し、高い権限については明示的な承認を求める](#)ように設定することもできます。

Operator Access Controlの監査ログは、互換サード・パーティ・ソフトウェア製品と統合できます。これにより、[OCIロギング・サービス](#)と[Splunk](#)が統合されます。詳細については、[Operator Access Controlの製品ドキュメント](#)および[Operator Access Controlの技術概要](#)を参照してください。

監査とロギング

ExaDB-Dにより、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し、監査とロギングが提供されます。このサービスでは、監視の職務が以下のように分離されています。

- お客様が、ご自身のサービスのロギング構成を制御および監視します。
- オラクルが、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制御および監視します。

監査ログは、互換テクノロジーに送信できます。実装の詳細については、[Ingest Oracle Cloud Infrastructure Logs into Third-Party SIEM Platforms using Log Shippers](#)を参照してください。監査ログの監視はオラクルの責任範囲には含まれておらず、オラクルがお客様の監査ログを監視することはありません。お客様はOracle Service Request（SR）プロセスを通じて、該当するOracleインフラストラクチャの監査ログ情報へのアクセスをオラクルにリクエストできます。Operator Access Control監査ログとDelegate Access Control監査ログは、お客様とオラクルの双方が利用可能です。

データベース監査ロギング

ExaDB-Dは、[Oracle AI Database Unified Audit](#)を使用して、データベースに対する包括的な監査ロギングを提供します。これらの監査レコードは、syslogサーバーや互換性のある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。オラクルは、各データベース・バージョンの[Oracle AI Database Security Guide](#)で、Oracle AI Database監査ログの構成、管理、監視に関するドキュメントを公開しています。詳細については、[Oracle AI Database Unified Audit: Best Practice Guidelines](#)を参照してください。

お客様は[Database Vault](#)を使用して、データベース管理者からOracle AI Database統合監査証跡を保護できます。

VM監査ロギング

[Oracle Linuxの監査ログ・サービス（auditd）](#)は、VM内でオペレーティング・システムの資格証明によって実行されたアクションを記録します。お客様は、独自の基準に従って[auditdを構成](#)できます。これには[Oracle Linux監査ログをリモート・ログ・サーバー](#)に送信することも含まれます。[Oracle Linuxの監査ログ](#)はOCI Log Analyticsサービスに統合できます。

OCI監査ロギング

OCI監査は、サポートされているすべての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呼出しをログ・イベントとして自動的に記録します。すべてのサービスが監査によるロギングに対応しています。Object Storageサービスはバケット関連イベントのロギングには対応していますが、オブジェクト関連イベントのロギングには対応していません。監査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）、独自のカスタム・クライアント、および他のOracle Cloud Infrastructureサービスによって行われたAPI呼出しが含まれます。ログの情報には以下のものが含まれます。

- APIアクティビティが発生した時刻
- 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

監査イベントには、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、レスポンス・データが含まれます。OCI監査サービスによってログ記録されたイベントは、OCIコンソール、API、またはJava用のSDKを使用して表示できます。イベントからのデータは、診断の実行、リソース使用率の追跡、コンプライアンスの監視、セキュリティ関連イベントの収集に使用できます。監査ログは、APIのターゲット・リソースのコンパートメントに保存されます。これらのログは、互換システムに転送できます。

ネットワーク・トラフィックのロギング

VCNフロー・ログを使用してネットワーク・トラフィック情報をキャプチャし、監視やセキュリティのニーズをサポートできます。VCNフロー・ログには、VCNを通過するトラフィックの詳細が記録され、トラフィックの監査に役立ちます。キャプチャ・フィルタを使用して、トラフィックを評価したり、フロー・ログに含めるトラフィックを選択したり、ロギング・サービスを活用してログ情報を指定のログ・グループに送信したりできます。

Oracleインフラストラクチャ監査ロギング

インフラストラクチャ監査ログの記録、分析、対応は、オラクルの責任範囲となります。

ExaDB-D X8以前のハードウェアのインフラストラクチャ監査ログには、以下が含まれます。

ILOM :

- syslog
- 物理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Exadata Database Server :

- /var/log/messages
- /var/log/audit.log
- /var/log/secure
- /var/log/xen/xend.log

Oracle 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

ExaDB-D X8M以降のハードウェアにおけるインフラストラクチャの監査ログには、以下が含まれます。

ILOM :

- syslog
- 物理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Exadata Database Server :

- /var/log/messages
- /var/log/secure
- /var/log/audit/audit.log
- /var/log/clamav/clamav.log
- /var/log/aide/aide.log

Oracle Exadata Storage Server :

- /var/log/messages
- /var/log/secure
- /var/log/audit/audit.log

Oracleインフラストラクチャ監査ログの保存期間は少なくとも1年間です。インフラストラクチャ監査ログには、オラクルのセキュリティ・スタッフがアクセスできます。

Operator Access ControlとDelegate Access Controlの監査ロギング

Operator Access ControlとDelegate Access Controlのログには、オラクルのスタッフによるシェル・アクセス時のコマンドとキーストロークが記録されます。これらのログはOracle Linuxのauditdによって生成されます。これらのログは、お客様のローカルSIEMシステムやOCIロギング・サービスに送信できます。また、ログを互換性のあるシステムに転送し、互換技術で処理することも可能です。どちらのサービスも、人間が読み取り可能なHTMLファイルを生成できるAPIとOCIコンソール・インタフェースを提供しています。これらのファイルには、キーストローク（TTY）とコマンドの記録が要約され、実行された操作とその順序が示されます。このサービスでは、ログ・ファイルから、ユーザー・パスワードなどの機密情報がリダクションされます。

インシデントへの対処

お客様とオラクルは連携して、ExaDB-Dコンポーネントへのアクセスを保護し、監視します。いずれかの当事者が不正なアクションを検出した場合、その当事者は相手方に通知する前に、直ちに対応アクションを取ることができます。お客様が不正なアクションを検出した場合は、そのアクションと対応について、Oracle Service Request（SR）プロセスを使用してオラクルに通知してください。

お客様による対応制御

お客様は、自身が管理するサービスに対して任意の応答アクションを実行できます。これには、顧客VMとOracle AI Databaseへのネットワーク接続の終了、およびOperator Access ControlとDelegate Access Controlのアクセス・リクエストの終了が含まれます。

オラクルのインシデント対応プロセス

オラクルのインシデント対応プロセスでは、以下に示すとおり、オラクルがセキュリティ・インシデントに対してどのように対応するかが説明されています。

“セキュリティ・インシデントとは、オラクルの企業システムおよびOracle Cloud上でホストされているデータの機密性、完全性、または可用性に影響を与える可能性がある、偶発的または意図的なあらゆる事象を指します。

グローバル情報セキュリティは、各事業部門（LoB）内のインシデント対応チームの役割と責任をさらに詳細に定義します。すべてのLoBは、情報セキュリティ・イベントの管理と適時の修正アクションの実施に関するグローバル情報セキュリティ・ガイダンスを遵守する必要があります。各LoBのインシデント対応プログラムには、以下の要件が含まれます。

- セキュリティ・イベントが発生したことの調査および検証
- 関係者との連携および適切な通知の実施
- 証拠およびフォレンジック関連情報の保存
- セキュリティ・イベントまたはインシデントおよびそれに関連する対応活動の記録
- セキュリティ・イベントまたはインシデントの封じ込め
- セキュリティ・イベントまたはインシデントの根本原因への対応
- セキュリティ・イベントのエスカレーション

セキュリティ・イベントが発見されると、オラクルのインシデント対応計画は、迅速かつ効果的な初期対応（トリアージ）を支援します。これには、調査、対応、修正、復旧、および事後分析が含まれます。LoBのインシデント対応チームは、セキュリティ・インシデント管理ポリシーに則り、セキュリティ・ポスチャと多層防御の強化につながる合理的な対策を特定するために、イベント後の分析を実施します。LoB内では、イベントの調査中に「Chain of Custody（証拠保全）」を維持するために、情報収集のための正式な手順とシステムが利用されます。また、オラクルは必要に応じて、法的に認められるフォレンジック・データ収集を支援します。”

クリティカルな問題に対する15分のサービス対応時間

Oracle Cloud Hosting and Delivery Policiesには、セキュリティ・インシデントを含むクリティカルな問題に対して、オラクルはサービス対応時間を15分とするという規定が以下のように記載されています。

“5.3.1 重要度1（クリティカルな停止）

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

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

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

ソフトウェアのセキュリティと更新

オラクルのソフトウェア開発は、[Oracle Software Security Assurance Practices](#)によって制御されます。オラクルは、ソフトウェアの開発、テスト、品質保証、およびデプロイメントにおいて、[職務分掌を実施](#)しています。詳細は、以下のドキュメントを参照してください。

- [Oracle Critical Patch Updates for Security Alerts and Bulletins](#)
- [Exadata Database Service Software Versions](#)
- [Configure Oracle-Managed Infrastructure Maintenance](#)
- [Patch and Update an ExaDB-D System](#)
- [ExaDB-D Interim Software Updates](#)

オラクルは、Oracle AI Database、Grid Infrastructure、およびLinuxオペレーティング・システムのソフトウェア更新を、OCI Object Storageにステージングします。これらの更新は、利用可能になるとOCIインタフェースにリストされます。お客様のスタッフがこれらの更新を適用するタイミングについては、お客様が管理します。四半期ごとのインフラストラクチャ更新は、ユーザーへの影響が最小限となる期間にスケジュールします。OCIインタフェースから、オラクルによる四半期ごとのインフラストラクチャ更新の適用時期を完全に管理し、把握できます。必要に応じて、メンテナンスのスケジュールを変更できます。

オラクルは、ローリング・メンテナンス操作を実施することで、四半期ごとのメンテナンスがお客様のアプリケーションに与える影響を最小限に抑えます。これにより、更新プロセス全体を通じてデータベースの可用性が維持されます。ローリング・メンテナンスでは、各データベース・サーバーを1度に1台ずつ再起動し、オフラインのサーバーがどの時点でも最大1台に限定されるようにします。高可用性を実現するように設計されたアプリケーションでは、データベース接続は使用可能なデータベース・インスタンス間で中断なく自動的に移行されるため、ダウンタイムをスケジュールする必要はありません。ストレージ・サーバーの更新もローリング方式で適用されます。お客様はオフライン・メンテナンスを実行することもできます。その場合は複数のコンポーネントが並列で更新されるため、メンテナンス期間は短縮されます。オフライン・メンテナンス中は、データベースは利用できません。

どのCVEがどのCritical Patch Update AdvisoryまたはSecurity Alertの対象となっているかは、[Oracle Map of CVE to Advisory/Alert](#)で確認できます。VMまたはExadata Infrastructureのソフトウェア・リリースによって解決されるCVEは、以下のように特定できます。

- VMクラスタの更新（OS）または更新履歴にアクセスし、ソフトウェアのバージョン（例：24.1.18.0.0.251115）を記録する
- [Exadata Database Machine and Exadata Storage Software Supported Versions \(KB153930\)](#) にアクセスする
- ソフトウェアのバージョンを確認し、CVE Release Matrixをダウンロードする

データを調査するための開発ツールやデバッグ・ツールは、ExaDB-Dインフラストラクチャにはインストールされていません。

セキュリティ・テストとスキャン

VMのセキュリティ・テストとスキャン

お客様は、[Oracle Cloudのテスト・ポリシー](#)に従ってExaDB-Dのセキュリティ・テストを実行できます。お客様のサービスには、コンプライアンス確認のためにVMをスキャンする[OpenSCAP](#)が含まれています。

サード・パーティ製のスキャン・ツールを使用してVMをスキャンすることもできます。お客様が使用するサードパーティ製スキャン・ツールやベンチマークは、ExaDB-Dのソフトウェア・ディストリビューションや構成と互換性がある必要があります。場合によっては、恣意的なベンチマークによって、ExaDB-D VM上にセキュリティ問題があると指摘されることがありますが、それらは重大なリスクではありません。Exadataで機能するように一般的なベンチマークを調整する方法の詳細については、[Responses to common Exadata security scan findings \(FAQ3926\)](#) を参照してください。

Oracleが管理するインフラストラクチャのセキュリティ・テストとスキャン

Oracleは、Oracle製品に対するセキュリティ分析とテストを義務付けています。

Oracleは、Oracleの企業セキュリティ標準を遵守するため、ExaDB-Dインフラストラクチャに対して毎月インフラストラクチャのセキュリティ・スキャンと更新を実施しています。これらの標準は、PCI-DSSなどの各種業界標準や、FedRAMP HighおよびISO/IEC 27001などの政府セキュリティ標準に準拠し、それらをサポートするものです。Oracleはインフラストラクチャの更新を、オンラインで、再起動なしに実施し、互換アプリケーションに影響を与えないように計画しています。また、ストレージ・サーバーへの月次セキュリティ更新はローリング方式で適用し、これもアプリケーションに影響を与えないように計画しています。月次セキュリティ・メンテナンスの実施は、その月内の特定の時間帯にスケジュールできます。ただしスケジュールできるメンテナンス期間は1つだけです。Oracleは、メンテナンス期間開始の少なくとも1週間前に、月次メンテナンスのスケジュールを公開します。必要に応じてスケジュールは変更できます。お客様によるインフラストラクチャ・コンポーネントへの直接アクセス、監視エージェントのインストール、またはOracle管理インフラストラクチャへのファイル転送は許可されていません。

カスタマイズとサード・パーティ製ソフトウェア

ExaDB-Dではお客様に、ゲスト・オペレーティング・システムへのrootアクセスやOracle AI DatabaseへのSYSDBAアクセスなど、お客様の環境に対する特権アクセスが付与されます。このレベルの管理により、お客様は構成の変更やソフトウェアのインストールができます。こうした変更や追加を行うと、時間の経過とともにスタック内の別の場所で例外や問題が発生する可能性があります。

Oracleは、Oracle以外のソフトウェアに対する技術サポートは提供していません。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が責任を負います。Oracle以外のすべてのソフトウェアについては、Oracle Linux環境またはExadata環境（あるいはその両方）での使用についてベンダーによる認定を受けており、お客様によってターゲット環境で徹底的なテストが実行されたものをご利用になることを強くお勧めします。ExaDB-Dでのサード・パーティ・ソフトウェアのサポートに関する詳細については、[My Oracle SupportドキュメントのInstalling Third-Party Software on Exadata Components \(KB144164\)](#) で公開されています。

問題が発生した場合、OracleのサポートはOracle Service Request (SR) プロセスを通じて診断を支援します。問題によっては、Oracleは変更を元に戻すよう推奨する場合もあります。特にサード・パーティ・ソフトウェアが関係しているケースなど、状況によっては、Oracleの標準サポート・ポリシーに従い、サード・パーティ・コンポーネントがない状態で問題を再現してみようお客様にお願いすることがあります。Oracleのサポートは、お客様のデータベース・サービスのサブスクリプションに含まれており、追加料金なしでご利用いただけます。

互換サービス変更

セキュリティ基準に準拠するように、お客様はVMの特定の面を変更できます。これには以下のものがあります。

- ファイアウォール/パケット・フィルタリング・サービス（クラウド自動化機能が許可されていることが条件）
- ログイン・バナー
- sudoログ・ファイル、オペレーティング・システムの監査ログ、およびリモート・ログ・サーバーへの監査ログ送信
- パスワードのエージング、複雑さ、履歴、有効期限
- systemdジャーナルのアップロードとリモートsyslogサーバーへの送信
- システム全体の暗号化ポリシー（MAC）の設定
- fs.suid_dumpableの構成

必要なサービス構成

サービス運用をサポートするため、お客様はVMの特定の面を変更せず維持する必要があります。これには以下のものがあります。

- /tmp、/dev/、/var/tmp、/var/logに対するexec権限
- /dev/shmに対するexecおよびsuid権限
- デプロイ済みのcrontab構成
- デプロイ済みのsudo構成
- デプロイ済みのシェルのタイムアウト
- デプロイ済みのumask
- デプロイ済みのnet.ipv4.conf.all.rp_filter構成
- デプロイ済みのドット・ファイル・アクセス
- rdsカーネル・モジュール
- 暗号化ライブラリ構成
- デプロイ済みのユーザー名、ユーザーID、グループ名、グループID

VM pam.d構成には、認証失敗時のための[default=die]が含まれています。これはrequiredやrequisiteと同じように機能します。

シェルのタイムアウトは、長時間実行される自動化タスク（ASMリバランスなど）に対応できるように構成されています。これらの値はサービス構成の一部であり、セキュリティ・スキャン・ツールで許可する必要があります。

一部のクラウド自動化機能には、PermitRootLogin=without-passwordが必要です。その場合、PermitRootLogin=noに設定すると、クラウド自動化機能のアクションは失敗します。アクションを実行するには、PermitRootLogin=without-passwordに設定する必要があります。PermitRootLoginは、オペレーティング・システムのツールを使用して、独自の基準に合わせて管理できます。

ベンチマークに準拠するようにVMを変更する場合は、本番デプロイメントの前に変更をテストし、サービス機能が損なわれてい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 AI Database、Grid Infrastructureの自動更新によって、お客様が加えた変更が元に戻される場合があります。オラクルは、提供時の設定でサービスを使用することを推奨しています。規定のサービス設計に従うことで、変更により必要となる広範なテスト、検証、トラブルシューティングを低減できます。

サービスの終了とデータの破壊

お客様はExaDB-Dを終了させることができます。終了すると、[Exadata Secure Eraser](#)ユーティリティが起動し、ハード・ドライブ、フラッシュ・デバイス、永続メモリ、内部USB上のデータが安全に消去されます。また、ILOMも工場出荷時の設定にリセットされます。Secure Eraserは、ユーザー・データ（サービスに保存されたOracle AI Databaseデータ）だけでなく、オペレーティング・システム、Oracle Exadata System Software、ユーザー構成を含むすべてのコンテンツをサニタイズします。Exadata Secure Eraserは、各ストレージ・デバイスのハードウェア機能を自動的に検出し、サポートされている最適な消去方法を選択します。セキュリティと処理速度の向上のために、可能な場合は必ず暗号化消去が使用されます。ExaDB-Dで使用されるハードウェアは、暗号化消去をサポートしています。Secure Eraserで使用される暗号化消去方法は、[NIST SP-800-88r1標準](#)に準拠するように設計されています。My Oracle Support（MOS）でService Request（SR）を開くことで、オラクルから安全な消去の認定を取得できます。

オラクルは、ExaDB-Dインフラストラクチャ・ハードウェアをオラクルのデータセンター間で移動させる場合があります。ハードウェアを移動させる前に、オラクルはインフラストラクチャ・コンポーネントに対してExadataの安全な消去を実行し、お客様のデータがオラクルのデータセンターから外部に出ないようにします。ハードウェアの耐用期間の終了時には、オラクルはお客様のデータが記録されたすべてのメディアを破壊します。

ストレージ・メディア・ハードウェアの取扱いと破壊

お客様のExaDB-Dサービスのストレージ・メディアには、[オラクルの情報および資産の分類慣行](#)が適用されます。オラクルが実行するストレージ・メディア・ハードウェアのメンテナンスと破壊は、PCI DSS、ISO 27001、CSA STARに準拠しています。関連する制御には、以下が含まれます。

ISO 27001に準拠する制御：

- A.8.3.2 – メディアの廃棄:メディアが不要になった場合は、正式な手順に従い、安全に廃棄する必要がある。
- A.8.3.3 – 物理的なメディアの輸送:輸送中はメディアのトレーサビリティを確保し、メディアを保護する必要がある。
- A.11.2.7 – 機器の安全な廃棄または再利用：機器（ディスクを含む）は、再利用または破壊する前に、すべての機密データが確実に消去されていることを検証する必要がある。

PCI DSSに準拠する制御:9.4.7 カード会員データが保存されている電子メディアが業務上または法律上の理由で不要になった場合、以下のいずれかの方法で破壊するものとする。

- 電子メディアを破壊する。
- カード会員データを回復不可能な復元できない状態にする。
- 9.4.7.a メディア破壊ポリシーを調べ、電子メディアが業務上または法律上の理由で不要になった場合の電子メディアの破壊手順が、そのポリシーの要件に規定されているすべての項目に従って定義されていることを確認する。
- 9.4.7.b メディア破壊プロセスを観察し、担当者と面接して、カード会員データが保存されている電子メディアが、そのポリシーの要件に規定されているいずれかの方法で破壊されることを確認する。

CSA STARに準拠する制御：

- DCS-01.1 組織の施設外で使用される機器を安全に廃棄するためのポリシーと手順が確立、文書化、承認、伝達、実施、維持されているか。
- DCS-01.2 機器が物理的に破壊されない場合でも、情報の回復を不可能にするデータ破壊手順が実施されているか。

ISO 27001とPCI DSSのコンプライアンス文書は、お客様のOCIテナンシーからダウンロードできます。「[Identity and Security](#)」->「[Compliance](#)」を選択してください。詳細については、[Consensus Assessment Initiative Questionnaire \(CAIQ\) v4.0 for Oracle Cloud Infrastructure \(OCI\)](#) を参照してください。

お客様のサービスに利用されているストレージ・メディア・ハードウェアへの物理的なアクセスと交換については、以下の手段で通知されます。

- オラクルが、ExaDB-Dの顧客通知（CN）をサブスクライブしているお客様のスタッフ宛てにCNを発行する。
- お客様のOracle ASMアラート・ログに、ストレージ・メディアのオフライン/オンライン・ステータスの変化とASMディスクのライフサイクル・イベントが記録される。
- お客様のOracle ASM監査ログに、ASMディスクのライフサイクル・イベント（ASMディスクの削除や追加など）が記録される。
- お客様のOracle Linuxオペレーティング・システム・ログに、ストレージ・デバイス（ASMディスク）のステータスの変化が記録される。

オラクルは、ExaDB-Dのディスクとフラッシュ・メディアを、厳格な取扱いと破壊手順を必要とする機密資産に分類しています。以下の要件が適用されます。

- アクセス制御：これらのパーツにアクセスするには、2名の人員による検証プロセスが必要です。
- オンサイトでの取扱い：いかなる状況においても、これらのパーツをデータセンターから持ち出してはなりません。
- 破壊：これらのパーツは、オラクルが承認した破壊方法（破碎、消磁気など）を用いて、データセンターの施設内で破壊する必要があります。
- ドキュメント：破壊のプロセスと検証については文書化し、コンプライアンスと監査の目的で記録を保持する必要があります。

オラクルによる顧客VMへのアクセスの例外ワークフロー

ExaDB-Dのサポートには、Break-Glass例外ケースが含まれます。そのケースでは、VMの障害を解決するためにオラクルのスタッフがお客様のVMにアクセスすることが必要とされます。オラクルのスタッフによるお客様のVMへのアクセス方法を制御するプロセスと技術的制御は、以下の状況に応じて異なります。

- VMがDelegate Access Controlによって管理されているか
- サービスの例外が発生したのはお客様がVMにアクセスする前か
- サービスの例外が発生したのはお客様がVMにアクセスした後か

これらのケースにおけるプロセスと技術的制御については、この後のセクションで説明します。

VMがDelegate Access Controlによって管理されている場合

[Delegate Access Control](#)を実装し、Oracle Cloudカスタマー・サポートとOracle Cloud Operationsをサブスクライブしている場合、Oracle Cloud SupportとOracle Cloud Operationsのサポート・スタッフから、お客様に対してDelegate Access Controlアクセス・リクエストが発行されます。お客様が承認すると、オラクルのサポート・スタッフは作業を行うために、[アクションの適用](#)によって制御されている資格証明（最小権限アクセスのための、一意で一時的なジャストインタイムの資格証明）を使用してVMにアクセスします。Oracle Linuxの監査サービスは、OCIロギング・サービスによって、コマンドやキーストロークのログをお客様に提供します。お客様は、Oracle Linuxの監査ログをお客様のsyslogサーバーに送信することもできます。

お客様がVMにアクセスできる場合

お客様がサービスにアクセスできるようになる前にお客様のサービスに例外が発生した場合、そのサービス例外に関連するOracle Service Request（SR）でのオラクルのアクセス要請に“はい”と応答すれば、オラクルのスタッフにお客様のサービスへのアクセスを許可できます。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の障害が含まれます。オラクルのスタッフは、次の情報を入力して既存のSRでの許可を求めます。

- ExaDB-Dに関連するセキュリティ・ポリシーにより、オラクルのスタッフがお客様の明示的な許可なしにお客様のdomU¹にアクセスすることは禁止されています。オラクルがこのポリシーを遵守するためには、オラクルのスタッフが次の質問を尋ねて、domU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、オラクルによるお客様のdomUへのログインを認める、お客様の明示的な許可が必要です。domUへのアクセスを明示的に許可することにより、お客様のdomUまたは関連データベースに保存されている機密データがないことを確認していることになり、お客様のセキュリティ・チームは、オラクルによるこの問題の修正を支援するために、オラクルがお客様のdomUにアクセスすることを許可していることとなります。domUにアクセスするための明示的な許可をオラクルにいただけますか。”

お客様がSRで“はい”と回答した場合、オラクルは、オラクルのスタッフがVMにアクセスできるように、プロセスおよびセキュリティコントロールを一時的に調整します。SRがクローズされるか、お客様がオラクルにSRでアクセスを中止するよう指示するまで、オラクルのスタッフによるVMへのアクセスは許可されます。Operator Access Controlを実装している場合、オラクルは問題解決のためにOperator Access Controlアクセス・リクエストを開きます。オラクルのスタッフが該当のシステム・コンポーネントにアクセスすることを許可するには、お客様がこのOperator Access Controlアクセス・リクエストを承認する必要があります。

¹ domUは、ExaDB-DにデプロイされたVMを表現するオラクルの用語です。この用語は、オラクルのスタッフによるExaDB-Dサービス内のVMへのアクセスを管理するプロセス制御の一部として必要です。

お客様がVMにアクセスできない場合

お客様がVMにアクセスできない場合、またはインフラストラクチャ・ネットワークからのリモート・ログインでVMにアクセスできない場合（VMがクラッシュしているなど）は、特定のプロセスと技術的制御によって、オラクルのスタッフがインフラストラクチャからお客様のVMにアクセスすることを許可できます。このアクセスは、Oracle Service Request（SR）プロセスと（実装されている場合は）Operator Access Controlを通じて、お客様とオラクルによって制御されます。この方法のユースケースには、次のものが含まれます。

- VMの起動失敗の原因となるエラー
- VMへのお客様のSSHが失敗する、またはお客様の資格証明が失われる原因となるエラー
- その他のサポート・エラー状態

お客様が直接監視していない状況でもオラクルのスタッフがVMにアクセスすることを許可して構わない場合には、以下の表現でService Request（SR）を開きます。

- SRのタイトル：
 - オラクルにExaDB-DのゲストVM（VM名<DBサーバーの詳細ページ>リソース→仮想マシンに表示されているVM名を挿入>）にアクセスできる明示的な許可を与えるためのSR
- SRの内容：
 - サポートがSR# 1-xxxxxxxに記載されている問題を解決するための支援を目的として、オラクルにゲストVMへのアクセスを明示的に許可するためにこのSRを開いています。この許可を与えることにより、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にアクセスできるようになると理解していることを認めます。さらに、上記のSRに記載されている問題を解決するために、セキュリティ・チームが、ゲストVMへのアクセスをオラクルに許可している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サーバーの詳細ページ>リソース→仮想マシンに表示されているVM名を挿入>

お客様がオラクルに対して、オラクルのスタッフによるアクセスを直接監視できるように共有画面の表示を求める場合には、以下の表現でService Request（SR）を開きます。

- SRのタイトル：
 - オラクルにExaDB-DのゲストVM（VM名<DBサーバーの詳細ページ>リソース→仮想マシンに表示されているVM名を挿入>）にアクセスできる明示的な許可を与えるためのSR
- SRの内容：
 - サポートがSR# 1-xxxxxxxに記載されている問題を解決するための支援を目的として、オラクルに共有画面セッションでのゲストVMへのアクセスを明示的に許可するためにこのSRを開いています。この許可を与えることにより、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にアクセスできるようになると理解していることを認めます。VMへのこのアクセス許可は、オラクルが実行するすべてのアクティビティを当社の担当者が画面共有セッションを通じてリアルタイムで監視できることが条件となります。さらに、上記のSRに記載されている問題を解決するために、セキュリティ・チームが、共有画面セッションでゲストVMへのアクセスをオラクルに許可している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サーバーの詳細ページ>リソース→仮想マシンに表示されているVM名を挿入>
- Operator Access Controlを実装している場合、オラクルは問題解決のためにOperator Access Controlアクセス・リクエストを開きます。オラクルのスタッフが該当のシステム・コンポーネントにアクセスすることを許可するには、お客様がこのOperator Access Controlアクセス・リクエストを承認する必要があります。
- Operator Access Controlは、コマンドとキーストロークのロギングを、ほぼリアルタイム（60秒未満）でお客様のテナンシー内のOCIロギング・サービスに提供します。

お客様が新しいSRを作成し、オラクルがその新しいSRを受け取ると、オラクルはプロセスとセキュリティコントロールを一時的に調整し、オラクルのスタッフがVMにアクセスすることを許可します。SRがクローズされるか、お客様がオラクルにSRでアクセスを中止するよう指示するまで、オラクルのスタッフによるVMへのアクセスは許可されます。

まとめ

ExaDB-Dでは、お客様がVM全体のセキュリティ機能を制御します。Oracle AI Databaseの暗号化によりデータは暗号化されますが、暗号化鍵を管理するのはお客様です。Oracle AI Databaseのセキュリティ機能は、データベース内のデータに対する認証とアクセスを制御します。ただし資格証明や認可に対する制御を保持するのはお客様です。Oracle Linuxの認証機能は、VMへのアクセスを制御します。ただし資格証明や認可に対する制御を保持するのはお客様です。

ExaDB-Dのオラクル管理コンポーネント全体にわたるセキュリティおよび監査機能は、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の防止に役立ちます。セキュリティ対策には、名前付きユーザーの多要素認証と、オラクルが管理するインフラストラクチャ・クラウドへのFIPS 140-2レベル3準拠のトークンベースのSSHアクセスによる厳密認証が含まれます。

このセクションでは、複数の可用性ゾーンがあるOracle AI Database@Azure（図9）、単一の可用性ゾーンがあるOracle AI Database@AWS（図10）、単一の可用性ゾーンがあるOracle AI Database@GCP（図11）のネットワーク図を示します。リージョンが構成に対応できれば、これらのサービスはいずれも、単一または複数の可用性ゾーンにデプロイできます。

- ネットワーク・セキュリティ・グループ
- セキュリティ・リスト
- ゼロトラスト・パケット・ルーティング
- Private Service Access



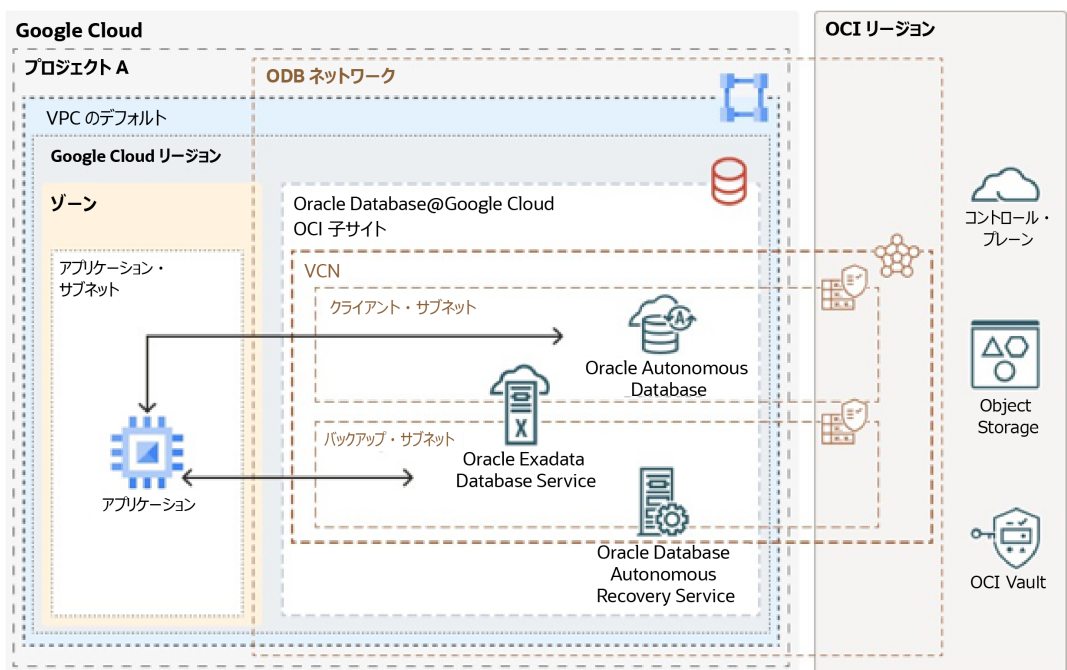


図11：Oracle AI Database@GCPネットワークの図

VMのデフォルトのプロセスと証明書

ExaDB-DのVMでは、データベース運用をサポートするOracleソフトウェア・プロセスが実行されます。これには以下が含まれます。

- Oracle AI Database、Oracle Real Application Clusters (RAC)
- Oracle Trace File Analyzer (TAF)
- ExaWatcher
- Exadata Management Server (MS)

表3は、各プロセスのネットワーク・インタフェース、ポート番号、プロセスの説明、および認証局（CA）を示しています。オラクルでは、オラクルが管理するサービスに対してOracle CAおよびオラクル自己署名証明書を受け入れるようにセキュリティ・スキャナを構成することを推奨しています。これらの証明書とCAはサービスに組み込まれ、ライフサイクル管理操作の提供を保護するためにオラクルによって管理されます。証明書とCAを受け入れることで、サービスの問題のリスクが低減し、運用負荷を最小限に抑えることができます。

表3：ゲストVMサービスのデフォルトのポート・マトリックス

インタフェースのタイプ	インタフェース名	ポート	実行されるプロセス	認証局
クライアントVLAN上のブリッジ	bondeth0	22	sshd	該当なし
		1521、2484 オプションで、お客様はSCANリスナー・ポート（TCP/IP）を1024～8999の範囲内で割り当てることができます。 デフォルトは1521です。 注意：TNSリスナーは、ウェルノウン・ポート（1521、1525）への初期接続後に動的ポートを開きます。	Oracle TNS Listener 着信するクライアントの接続リクエストを受け取り、データベース・サーバーへのそれらのリクエストのトラフィックを管理します。 Oracle Native Network Encryption (NNE) および トランスポート・レイヤー・セキュリティ認証としてのTLS/SSL をサポートします	オラクルが内部CA署名。 お客様独自の証明書を追加可能

		TLS/SSLはポート2484を使用します。		
		5000	Oracle Trace File Analyzer Collector	オラクルが自己署名
		7879	Jetty Management Server Oracle Exadata System Software、特に Management Server (MS) で内部的に使用されるアプリケーション・サーバー・エンジン。	オラクルが自己署名
	bondeth0:1	1521、2484 オプションで、お客様はSCANリスナー・ポート（TCP/IP）を1024～8999の範囲内で割り当てることができます。 デフォルトは1521です。	Oracle TNS Listener	オラクルが内部CA署名。 お客様独自の証明書を追加可能
	bondeth0:2	1521、2484 オプションで、お客様はSCANリスナー・ポート（TCP/IP）を1024～8999の範囲内で割り当てることができます。 デフォルトは1521です。	Oracle TNS Listener	オラクルが内部CA署名。 お客様独自の証明書を追加可能
バックアップVLAN上のブリッジ	bondeth1	7879	Jetty Management Server	オラクルが自己署名
各クラスタ・ノードで実行されるOracle Clusterwareは、これらのインタフェースを介して通信します。	clib0/clre0	1525	Oracle TNS Listener 各クラスタ・ノードで実行されるOracle Clusterwareは、これらのインタフェースを介して通信します。	該当なし
		3260	Synology DSM iSCSI	該当なし
		5054	Oracle Gridプロセス間通信	該当なし
		7879	Jetty Management Server	オラクルが自己署名

		動的ポート：9,000～65,500 ポートはオペレーティング・システムで構成済みの一時的な範囲によって制御され、動的なものとなります。	システム監視サービス（osysmond） クラスタ・ロガー・サービス（ologgerd） Cluster Health Monitor は、System Monitor（osysmond）サービスとCluster Logger（ologgerd）サービスを使用して診断データを収集します。	オラクルが自己署名
	clib1/clre1	5054	Oracle Gridプロセス間通信	該当なし
		7879	Jetty Management Server	オラクルが自己署名
クラスタ・ノードでは、これらのインタフェースを使用してストレージ・セル（ASMディスク）にアクセスします。 ただし、コントロール・プレーン・サーバーからDBCSエージェントへのアクセスには、ストレージ・インタフェースに接続されたIP/ポート（7060/7070）が使用されます。	stib0/stre0	7060	dbcs-admin データベースのライフサイクル運用を処理するクラウド・エージェント	オラクルが自己署名
		7070	dbcs-agent データベースのライフサイクル運用を処理するクラウド・エージェント	オラクルが自己署名
	stib1/stre1	7060	dbcs-admin	オラクルが自己署名
		7070	dbcs-agent	オラクルが自己署名
コントロール・プレーンからdomU	eth0	22	sshd	該当なし
ループバック	lo	22	sshd	該当なし
		2016	Oracle Grid Infrastructure	該当なし
		6100	Oracle Notification Service (ONS) 、Oracle Grid Infrastructureの一部 Cluster Synchronization Service（CSS）、Event Management（EVM）、およびOracle Notification Services（ONS）の各コンポーネントは、同じクラスタ・データベース環境内の他のノードにあるクラスタ・コンポーネント・レイヤーと通信します。	該当なし

		7879	Jetty Management Server	オラクルが署名
		動的ポート：9,000～65,500	Oracle Trace File Analyzer Collector	オラクルが署名
お客様が管理	お客様が管理	お客様が管理	オプションの Oracle Data Safe オンプレミス・コネクタ	お客様が管理、またはオラクルが署名

OCIコントロール・プレーン経由でのVMシリアル・コンソールへのアクセス

お客様はトークンベースのSSHトンネル経由でVMシリアル・コンソールにアクセスします。コントロール・プレーンを経由して、VMのハイパーバイザ・コンソールにトンネル接続します。アクセスは以下の3つの手順で制御します。

1. お客様のOCI IAMの資格証明を使用して、シリアル・コンソール接続を作成します。これには、SSHプロキシ・トンネルをサポートするために、一時的なBastionホストや、コントロール・プレーンに仮想マシンとコンテナをデプロイすることが含まれます。
2. お客様のSSH資格証明を使用して、お客様のデバイスまたはOCI Cloud ShellからVMコンソールへのSSH接続を作成します。
3. お客様はユーザー名とパスワード（通常はrootユーザー）を使用して、VMシリアル・コンソールにログインします。

コントロール・プレーンは、作成から24時間後にコンソール接続を終了します。コンソール接続を再確立するには、OCIから再認証を受ける必要があります。コンソール接続は、OCIコンソールまたはAPIインタフェースを使用して、いつでも終了できます。VMシリアル・コンソールは、[APIアクセス制御](#)によって制御できます。

商用関連の付録

このセクションでは、ExaDB-Dの一般的なセキュリティの質問に関連する、オラクルの公開商用コンテンツについてまとめています。オラクルのセキュリティ、コンプライアンス、プライバシー、および商用契約に関するドキュメントの索引については、[Oracle Trust Center](#)をご覧ください。

準拠

オラクルは、オラクルの事業部門が、サード・パーティの認証またはそのサービスの1つ以上について認定を"認証"の形式で取得しているフレームワークに関する情報を提供します。これらの認証はコンプライアンスとレポート作成に役立てることができ、該当するOracle Cloud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管理を独立して評価できるようになります。これらのサード・パーティ認証をレビューするには、それらが一般に特定のクラウド・サービスに固有であることに加え、特定のデータセンターまたは地理的地域に固有である場合があることを考慮することが重要です。ExaDB-Dの特定の標準に関連する詳細については、[Oracle Cloud Complianceドキュメント](#)をご覧ください。この情報は変更される場合があり、頻繁に更新される可能性があり、“現状のまま”提供され、保証はなく、契約には組み込まれないことに注意してください。

ExaDB-Dのサービス提供において準拠するフレームワークと標準には、以下が含まれます。

- C5
- CSA STAR Level 2
- Canada Protected B
- DESC (UAE)
- DoD IL5
- ENS High
- FSI (韓国)
- FedRAMP High – JAB ATO
- G-Cloud Marketplace
- GxP
- HIPAA
- HITRUST CSF
- Héberge des Données de Santé (HDS)
- IRAP
- ISMAP
- ISMS
- ISO/IEC 20000-1
- ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 27018

- ISO/IEC 27701
- ISO/IEC 9001
- MeitY
- NCSC
- NISC
- PCI DSS
- SAMA
- SOC 1
- SOC 2
- SOC 3
- Saudi Arabian National Cybersecurity Authority
- Three Ministries
- UK Cyber Essentials
- UK Security and Data Protection Toolkit

コンプライアンス・ドキュメントについては、オラクル営業担当者にリクエストすることも、[OCIコンソールから直接アクセスすることもできます](#)。

[Advisory: Oracle Cloud Infrastructure and the General Data Protection Regulation \(GDPR\)](#) を参照すると、OCIサービスの利用において欧州連合（EU）の一般データ保護規則（GDPR）要件を満たすのに役立ちます。FedRAMPの詳細については、[FedRAMP Marketplace](#)を参照してください。

オラクルの企業セキュリティ慣行

[オラクルの企業セキュリティ慣行](#)は、オラクルとお客様のデータの機密性、完全性、可用性を保護するのに役立ちます。これらの慣行は、オラクルの社内業務と、クラウド・サービスのセキュリティ管理を対象としており、従業員や契約業者などのオラクルのすべてのスタッフに適用されます。これらのポリシーは、ISO/IEC 27002:2022（旧称ISO/IEC 17799:2005）およびISO/IEC 27001:2022標準に準拠しており、オラクル社内におけるセキュリティのすべての領域で指針となります。これらの慣行には以下が含まれます。

- [目的](#)
- [人事管理セキュリティ](#)
- [アクセス制御](#)
- [ネットワーク通信セキュリティ](#)
- [データ・セキュリティ](#)
- [ノートパソコンとモバイル機器のセキュリティ](#)
- [物理的および環境的セキュリティ](#)
- [サプライ・チェーンのセキュリティと保証](#)

脆弱性の開示

ポリシーとして、[オラクルは、Critical Patch UpdateまたはSecurity Alertの通知、インストール前の注意事項、Readmeファイル、およびFAQで提供される内容を超える、脆弱性の詳細に関する追加情報を提供しません](#)。オラクルは、すべてのお客様を平等に保護するために、すべてのお客様に同じ情報を提供します。オラクルは、Critical Patch UpdateまたはSecurity Alertに関する事前通知や"インサイダー情報"を個々のお客様に提供することはありません。オラクルが、オラクル製品の脆弱性を悪用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"）を開発または配布することはありません。

[Oracle Critical Updates, Security Alerts, and Bulletins](#)ページには、Critical Patch Update Advisory、Security Alert、Bulletinで行われたセキュリティ修正の発表が掲載されており、新しいCritical Patch Update Advisory、Security Alert、Bulletinがリリースされると更新されます。オラクルは、脆弱性修正が次のCritical Patch Updateでの配布を待つことができないほど重大であるとみなされる場合、Security Alertを発行します。これらのアラートの履歴は、『Oracle Critical Updates, Security Alerts, and Bulletins』ページに保持されます。

Oracle Data Processing Agreement

[Oracle Data Processing Agreement for Oracle Services](#)は、お客様のサービス契約に規定されているサービスを提供するにあたり、処理者であるお客様に代わってオラクルが行う個人情報（PI）の処理に適用されます。以下のような個人情報をオラクルがどのように制御、保護、処理するかを説明しています。

- 国境を越えたデータ転送
- セキュリティと機密保護
- 監査権
- インシデント管理と侵害通知

ExaDB-Dの利用の一環として、お客様は、オラクルが本Data Processing Agreementに基づき義務を遵守していることを、年1回を上限として監査できるものとします。さらに、適用されるデータ保護法により要求される範囲において、お客様または規制当局はより頻繁に監査を実施する場合があります。

Oracle Cloud Services Agreement

[Oracle Cloud Services Agreement](#)では、Oracle Cloud Servicesにおいてお客様のデータが、以下のような点でどのように処理されるかを説明しています。

- 所有権と制限事項
- 非開示
- コンテンツの保護
- サービスの監視と分析
- エクスポート
- 不可抗力
- 準拠法と管轄権

Oracle Cloud Services Agreementに関する重要な情報は以下のとおりです。

"5.1 対象サービスの提供の一環としてオラクルに提供されるお客様コンテンツを保護するため、オラクルは、該当の手段面、物理面、技術面その他における安全対策、ならびにシステムおよびコンテンツの管理に関する他の該当の側面（掲載場所：

<https://www.oracle.com/jp/contracts/cloud-services/>）を、遵守するものとします。

11.1. オラクルは、オラクルによる対象サービスの運用を円滑化するため、お客様のサービス・リクエストの解決を支援するため、対象サービスの機能、セキュリティ、完全性または可用性に対する脅威および対象サービスにおけるコンテンツ、データまたはアプリケーションに対する脅威を検出してそれに対処するため、ならびに違法な行為またはAcceptable Use Policyへの違反を検出してそれに対処するために、対象サービスを継続的に監視します。オラクルの監視ツールは、かかる目的で必要となる場合を除き、対象サービス内に存するお客様コンテンツのいずれも収集せず、その保存もしません。オラクルは、お客様またはお客様のユーザーから提供された非オラクル製のソフトウェアのうち対象サービス内に保存されているか、対象サービス上で動作するかまたは対象サービスを介して動作するものについて、監視を行わず、問題への対処も行いません。オラクルの監視ツールにより収集された情報（お客様コンテンツを除きます）は、オラクルの製品およびサービスのポートフォリオの管理を支援するため、オラクルの製品およびサービスの不備への対処においてオラクルの助けとするため、また、ライセンス管理の目的のために、使用されることもあります。

11.2. オラクルは、（a）対象サービスのパフォーマンス、運用および使用に関連する統計その他の情報を蓄積することができるとともに、

（b）セキュリティおよび運用の管理のため、統計分析を作成するため、ならびに研究および開発の目的で、対象サービスからのデータを集計形式にて使用することができるものとします（（a）および（b）を総称して以下「サービス分析」といいます）。サービス分析についてのいかなる知的財産権も、オラクルに留保されるものとします。"

オラクルによるセキュリティ・イベント・ログの管理

[オラクルの通信・運用管理](#)では、Oracleサービスに関連するセキュリティ・ログ情報をオラクルが制御および管理する方法について、次のように説明しています。

"オラクルでは、システム・オーナーがオペレーティング・システム、アプリケーション、データベース、ネットワーク機器における特定のセキュリティ関連活動についてログを取得・保持することを義務付けています。システムは、オラクルのシステムおよびアプリケーションへのアクセスの記録に加えて、システム・アラート、コンソール・メッセージ、システム・エラーなどもログに記録する必要があります。オラクルは、ログ・ファイル媒体の容量枯渇、イベント記録の失敗、ログの上書きなどの運用上の問題を防止するための制御を実施しています。

オラクルのポリシーでは、各事業部門がセキュリティ・イベントの調査およびフォレンジックを目的としてログを監視することが求められています。検出された異常なアクティビティは、そのシステムを所有する事業部門のセキュリティ・イベント管理プロセスに取り込まれる必要があります。セキュリティ・ログへのアクセスは、必要性（need-to-know）と最小権限（least privilege）の原則に基づいて提供されます。可能な場合、ログ・ファイルは強力な暗号化やその他のセキュリティ管理策によって保護され、アクセスも監視されます。インターネットにアクセス可能なシステムによって生成されたログは、インターネットにアクセスできないシステムに移動させる必要があります。"

[Oracle Consensus Assessment Initiative Questionnaire \(CAIQ\)](#) には、オラクルがセキュリティ・ログを管理する方法の詳細が以下のように記載されています。

"CCC-07.1 確立されたベースラインから逸脱した変更が行われた場合にプロアクティブに通知する検出手段が実装されていますか。

変更管理に関するOCIクラウド・コンプライアンス標準では、OCIを開発、管理、サポートするオラクルの従業員およびプログラムのための手順（不正な変更の防止を含む）を概説しています。OCIサービスは、予期しない変更や不正な変更がないか監視し、影響を受けるホストでの逸脱をログに記録して、検知および対応チーム（DART）に必要な応じて通知します。

DCS-02.2 移設または転送のリクエストには、書面または暗号手法により検証可能な認可が必要ですか。

OCIサービスは、資産の取得、開発、利用、保守、廃棄の際に、情報資産とインベントリ記録簿の資産の場所に加えられた変更をログに記録します。

LOG-01.1 ロギングおよびモニタリングのポリシーと手順が確立、文書化、承認、伝達、適用、評価、維持されていますか。

ロギングおよびモニタリングのポリシーは、Oracle Corporate Securityによって確立、文書化、承認、伝達、適用、評価、維持されています。オラクルは、オペレーティング・システム、アプリケーション、データベース、およびネットワーク・デバイスにおける特定のセキュリティ関連活動を記録しています。Oracleプログラムへのアクセス、システム・アラート、コンソール・メッセージ、システム・エラーなどのログを記録するようにシステムを構成しています。オラクルは、ログ・ファイルのメディアを使い切る、イベントを記録できない、ログが上書きされるなど運用上の問題から保護するために、設計されたコントロールを実装しています。

詳細は、oracle.com/corporate/security-practices/corporate/communications-operations-management.htmlを参照してください。

ロギングとアラートに関するOCIクラウド・コンプライアンス標準では、監査ログの収集、維持、レビューの要件を規定しています。

LOG-09.1 情報システムでの監査レコードは、不正なアクセス、変更、削除から保護されていますか。

ロギングとアラートに関するOCIクラウド・コンプライアンス標準では、不正なアクセス、変更または削除からログを保護するための複数レイヤーのセキュリティについて説明しています。これには、次の手段が含まれます。

- ログ構成機能へのアクセスを、特権アクセスを持つ個人に制限する
- 転送中のログ・データを暗号化する
- 情報保護ポリシーに従ってログ・レコードを分類する
- 自動化されたツールでログ・データを継続的に監視する”

セキュリティ・ログを少なくとも1年間保持

[Oracle Cloud Hosting and Delivery Policies](#)では、オラクルによるセキュリティ・ログの処理と保持について、以下のように説明しています。

”1.14 セキュリティ・ログ

オラクルは、オペレーティング・システム、アプリケーション、データベースおよびネットワーク・デバイスにおける特定のセキュリティ関連の活動について、ログを作成します。システムは、デフォルトのセキュリティ活動、情報またはプログラムへのアクセス、アラートなどのシステム・イベント、コンソール・メッセージおよびシステム・エラーをログとして記録するように設定されています。オラクルは、セキュリティ・イベントの調査およびフォレンジックのためにログをレビューします。検出された異常なアクティビティは、セキュリティ・イベント管理手順の対象となります。セキュリティ・ログは、ネイティブ形式かつ変更なしの形式にてSecurity Information and Event Managementシステム（またはそれに相当するシステム）内に保存され、たとえばオラクルの内部ポリシーに基づき保持されます。セキュリティ・ログのオンラインでの保持期間は、少なくとも1年とします。かかるログは、オラクルの内部セキュリティ業務のためにオラクルにより保持および利用されます。”

月次稼働時間99.95 %の品質保証契約（SLA）

[Oracle PaaS and IaaS Public Cloud Services Pillar Document](#)では、以下に示すとおり、オラクルのサービスが99.95 %の稼働率で提供されなかった場合のOracleサービス・クレジットによる救済措置について説明しています。

”可用性サービス・レベル合意 このサブセクションの可用性サービス・レベル合意が適用される上記のクラウド・サービスに関して、オラクルは商業的に合理的な努力を尽くして、おのおののサービスが99.95 %以上の月次稼働時間率（下で定義します）ですべての暦月において使用可能となるように努めます（“サービス・コミットメント”）。該当する上記のクラウド・サービスがこのサブセクションで示す可用性サービス・レベル合意のサービス・コミットメントを満たさない場合、お客様はそうした不適合サービスに対するサービス・クレジットを、次のように決定されるサービス・クレジット率に従って受け取る資格があります。

月次稼働時間率：	サービス・クレジット率
• 99.95 %未満99.0 %以上：	10 %
• 99.0 %未満95.0 %以上：	25 %
• 95.0 %未満：	100 %”

サービス終了後の60日間のアクセス期間

[Oracle Cloud Hosting and Delivery Policies](#)では、サービス終了後の、サービスからお客様のデータを取得できるアクセス期間について、以下のように説明されています。

”6.1 Oracle Cloud Servicesの終了

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

るサービス仕様書の条件に基づいて認められている場合を除き、かかる対象サービスを使用するお客様の権利は、サービス期間の終了時に失効します。”

CONNECT WITH US

+1.800.ORACLE1までご連絡いただくか、oracle.comをご覧ください。
北米以外の地域では、oracle.com/contactで最寄りの営業所をご確認いただけます。

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2026, Oracle and/or its affiliates. All rights reserved. 本文書は情報提供のみを目的として提供されており、ここに記載されている内容は予告なく変更されることがあります。本文書は、その内容に誤りがないことを保証するものではなく、また、口頭による明示的保証や法律による黙示的保証を含め、商品性ないし特定目的適合性に関する黙示的保証および条件などのいかなる保証および条件も提供するものではありません。オラクルは本文書に関するいかなる法的責任も明確に否認し、本文書によって直接的または間接的に確立される契約義務はないものとします。本文書はオラクルの書面による許可を前もって得ることなく、いかなる目的のためにも、電子または印刷を含むいかなる形式や手段によっても再作成または送信することはできません。

OracleおよびJavaはOracleおよびその子会社、関連会社の登録商標です。その他の名称はそれぞれの会社の商標です。

IntelおよびIntel XeonはIntel Corporationの商標または登録商標です。すべてのSPARC商標はライセンスに基づいて使用されるSPARC International, Inc.の商標または登録商標です。AMD、Opteron、AMDロゴおよびAMD Opteronロゴは、Advanced Micro Devicesの商標または登録商標です。UNIXは、The Open Groupの登録商標です。0120

Exadata Database Service on Dedicated Infrastructureのセキュリティコントロール

