Oracle Gen 2 Exadata Database Service on Cloud@Customer Security Controls

ORACLE

Exadata Database Service on Cloud@Customer Security Controls

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

August 21, 2025 | 2.34 版

本書の目的

このドキュメントは、リリース 25.1.7.0.0.250711 および 24.1.14.0.0.250706[1]に含まれる機能および強化点の概要を説明します。25.1.7.0.0.250711 および 24.1.14.0.0.250706 へのアップグレードによ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ための一助となることのみを目的としています。

このドキュメントは、Gen 2 Oracle Cloud Infrastructure (OCI)コントロール・プレーンを介して提供される Oracle Exadata Database Service on Cloud@Customer[2] (ExaDB-C@C)のセキュリティおよびコントロール機能を要約したものです。これは、ExaDB-C@C の導入評価に携わるセキュリティ担当者を対象としています。ExaDB-C@C では、次のサービス提供方法が必要になります。

- ExaDB-C@C インフラストラクチャへの接続の許可については、オラクルが担当者を選択できるものとします
- オラクルは、ExaDB-C@C インフラストラクチャにアクセスする担当者のアイデンティティ・プロバイダとなります
- オラクルのスタッフは、オラクルが提供するソフトウェアとハードウェアを使用して、インフラストラクチャにアクセスします
- オラクルのスタッフは、定期的なスーパーユーザー(root)アクセスなど、インフラストラクチャのメンテナンスを実行します
- オラクルのスタッフは、サービスの問題の診断と解決を行うために必要なコンポーネントにアクセスします

お客様は、Oracle Operator Access Control[3]と Delegate Access Control[4]を使用して、オラクルが管理するインフラストラクチャとお客様 VM へのオラクルのスタッフによるアクセスを制御できます。これらの特権アクセス管理サービスは、エンタイトルメントを管理するための OCI インタフェース、権限を適用するための Oracle Linux セキュリティ・ソフトウェア、コマンドとキーストロークをログに記録するための Oracle Linux 監査を提供します。これらのサービスは、次のようにアクセスを提供します。

- オラクルが要求し、お客様が承認した場合に限定
- 作業を実施するために必要な期間に限定
- 一時的な最小限の権限を持つ資格証明を使用
- 一時的なネットワーク、ssh トンネル、踏み台サーバーを使用

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。本文書と本文書に含まれる情報は、オラクルの事前の書面による同意なしに、公開、複製、再作成、またはオラクルの外部に配布することはできません。本文書は、ライセンス契約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。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なさらないでください。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、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。

[1] https://support.oracle.com/knowledge/Oracle%20Database%20Products/2333222_1.html

[2] https://www.oracle.com/engineered-systems/exadata/cloud-at-customer/

[3] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-7CF13993-DB16-485A-A9FA-399E0049740B

[4] https://docs.oracle.com/en-us/iaas/delegate-access-control/doc/overview-of-delac.html

目次

図一覧

表一覧

はじめに

Exadata Database Service on Cloud@Customer (ExaDB-C@C)は、お客様のデータ・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 のすべての機能、OCI のオーケストレーション、および Oracle サポートを利用できます。このドキュメントでは、サービスに組み込まれたセキュリティ統制について説明します。これらの統制は、業界のベスト・プラクティスとオラクルの企業セキュリティ標準に従って、ユーザー・データとミッションクリティカルなワークロードを保護します。お客様の現在のセキュリティ標準が異なる場合は、お客様がポリシーを更新または調整し、必要に応じて例外を認められるように、代わりとなる統制を提示します。

役割と責任

ExaDB-C@C は、お客様とオラクルがそれぞれシステムの特定の側面を管理する共同責任モデルに従っています。責任は次のように分けられます。

お客様のサービス:

- 仮想マシン(VM)
- 仮想マシン内で実行されているデータベース

オラクルが管理するインフラストラクチャ:

- 物理サーバー(Exadata Database Server と Exadata Storage Server)
- ストレージ・ネットワーク・スイッチ

- アウト・オブ・バンド(OOB)管理スイッチ
- 配電ユニット(PDU)

オラクルが管理するクラウド・コントロール・プレーン:

- Web UI および API インタフェース
- パブリック OCI エンドポイント(サービスの API など)
- プライベート・エンドポイント(OCI Fast Connect など)
- サービスのライフサイクル管理のための OCI クラウド自動化

お客様は、VM とデータベースへのアクセスを保護、監視、管理する責任を負います。お客様は、標準的なオペレーティング・システム・ツールとデータベース・ツールを使用して、VM と Oracle Database に対する認証を管理します。[5]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 VM やデータベースにアクセスする権限はありません。ただし、Exception Workflows - Oracle Access to Customer VM で詳しく説明している特定のサポート例外を除きます。役割と責任の詳しい内訳は、表 1、「ExaDB-C@C サービスの説明」[6]と「ExaDB-C@C Explanation of Services」に記載されています。[7]

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	お客様のスタッフ	Oracle Cloud Ops	お客様のスタッフ
モニタリング	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	オラクルのインフラストラクチャのログ収集と監視をサポートするためのネットワーク・アクセスの提供	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、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 スペア部品と現場派遣	現場での診断支援(ネットワークのトラブルシューティングなど)	基盤となるプラットフォームに関連す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の管理と解決
パッチ管理	ハードウェア、IaaS/PaaS コントロール・スタックへのプロアクティブなパッチ適用	パッチ提供をサポートするためのネットワーク・アクセスの提供	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)	テナント・インスタンスのパッチ適用 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 VM の再作成	クラウド自動化の提供をサポートするためのネットワーク・アクセスの提供	お客様がアクセスできる実行中の VM の提供	オラクル独自の機能またはサードパーティの機能を使用した、お客様の IaaS データと PaaS データのスナップショット/バックアップおよびリカバリ
クラウドのサポート	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する SR の対応と解決	MOS 経由での SR の送信	SR の対応と解決	サポート・ポータル経由での SR の送信

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

[6] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/ecc-system-config-options.html

[7] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2707015.1

EXADB-C@C サービスのアーキテクチャ

図 1 は、ExaDB-C@C のアーキテクチャ・ブロック図です。このサービスは、お客様のデータ・センター内の Exadata ラックにデプロイされます。ラックには、標準的な Exadata Database Machine のすべてのコンポーネントに加えて、高可用性(HA)構成のコントロール・プレーン・サーバー(CPS)が 2 台搭載されます。CPS は、お客様とオラクルがサービスを管理できるように、Exadata ラックを OCI コントロール・プレーンに接続します。[8]

サービスは、オンプレミスの ExaDB-C@C ラックでお客様のデータを保護するのに役立ちます。お客様のデータベースへのアクセスは、お客様がコントロールするネットワーク接続を使用して行われます。お客様は、お客様の VM とデータベースを認証できる資格証明をコントロールします。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と SYS レベルのアクセス権を持ちます。お客様は、セキュリティ・ポリシーの設定、規制の遵守、エージェントのインストール、ログの転送、アイデンティティの管理を行うことができます。

お客様が選択した OCI リージョンは、オペレーティング・システムとデータベースの管理のためのクラウド自動化やインフラストラクチャのメンテナンスとサポートなどの ExaDB-C@C ライフサイクル管理機能を提供します。お客様は、OCI Identity and Access Management (IAM)を使用してクラウド自動化機能をコントロールします。OCI Audit は、データベースの作成および削除や OCPU のスケーリングなど、OCI コンソールまたは OCI REST エンドポイントを介して呼び出されたすべての管理アクションのレコードをお客様に提供します。お客様は、コントロール・プレーン・サーバーから必要な OCI 管理エンドポイントへのネットワーク・アクセスをコントロールします。「Preparing for Exadata Database Service on Cloud@Customer」[9]で、サービスのネットワーク要件が説明されています。お客様は、オラクルのスタッフによるインフラストラクチャへのアクセスをオラクルが制御することを認めることも、Operator Access Control でオラクルのスタッフをコントロールすることもできます。

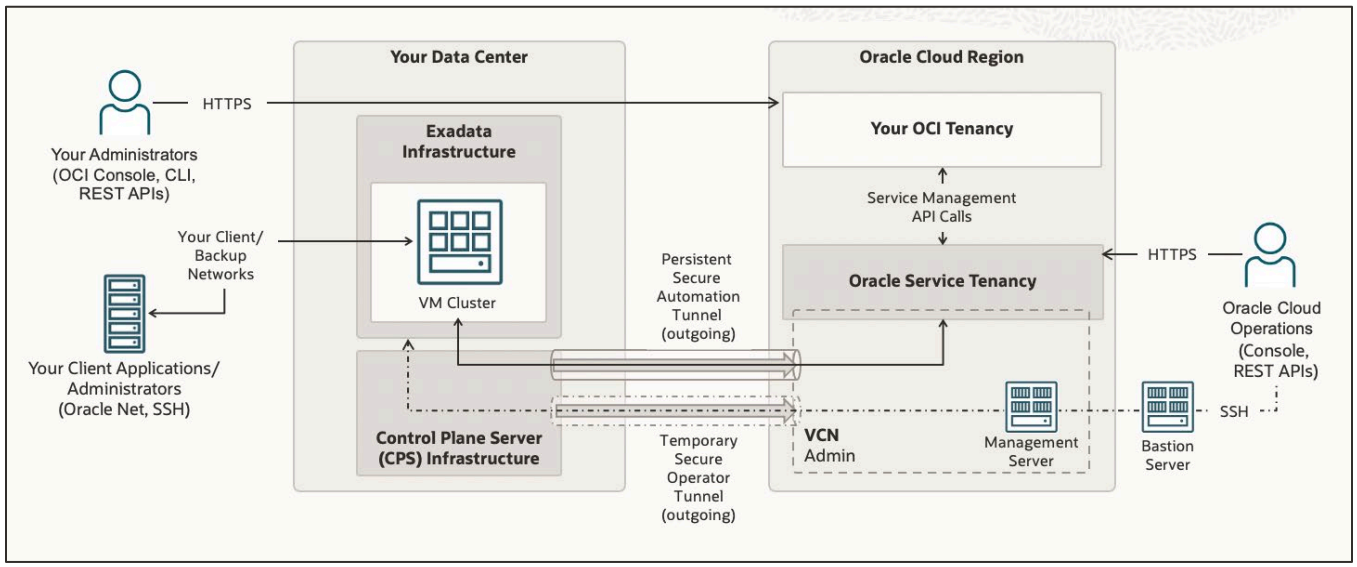

図 1: Oracle ExaDB-C@C のアーキテクチャ・ブロック図

ネットワーク・アーキテクチャ

図 2 は、物理的なネットワーク実装を示しています。[10]お客様がコントロールするコンポーネントは青色で示しています。オラクルがコントロールするコンポーネントは赤色で示しています。独立したレイヤー2 管理ネットワークがインフラストラクチャ・コンポーネントを相互接続しています(赤色)。管理ネットワークまたはストレージ・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。表面上、Exadata Database Server にはクライアント・ネットワークまたはバックアップ・ネットワーク上の IP アドレスが構成(plumb)されていません。ExaDB-C@C コントロール・プレーン・ソフトウェアは、お客様が VM クラスタ・ネットワーク・リソース [11]を作成する際に、クライアント・ネットワークおよびバックアップ・ネットワークのネットワーク検証チェックを実行するために、Exadata Database Server 上に IP アドレスを一時的に構成します。

[8] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/eccid/exacc_overview.html

[9] https://docs.oracle.com/en-us/iaas/exadata/doc/eccpreparing.html#GUID-A29A2B1C-708F-4AF2-BE6E-0B4916F6CB25

[10] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/eccid/exacc_netinterfaces.html

[11] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-setting-up-the-network.html#GUID-C1F49BDB-1249-4AE7-9ECB-7AEC406F05ED

お客様は、10Gb または 25Gb のイーサネットを使用して、Exadata Database Server のクライアント・ネットワークおよびバックアップ・ネットワークのポートをお客様のレイヤー2 スイッチに接続します。お客様は、これらのネットワークの VLAN タグをコントロールします。Exadata Database Server のホスト・オペレーティング・システムは、VM の高可用性ネットワーク接続をアクティブ/スタンバイ構成で実装します。お客様は、オプションで LACP を実装できます。

お客様の VM は、SR-IOV でマッピングされたインタフェース(黄色)を使用して、ルーティングされないプライベート・インターコネクト・ネットワーク経由で Exadata ストレージにアクセスします。物理的な Exadata Database Server と Exadata Storage Server にはそれぞれ、冗長ストレージ・ネットワーク・スイッチへの HA(アクティブ/スタンバイ)接続があります。デフォルトのストレージ・ネットワーク構成は 100.107.0.0/24 です。お客様は、必要に応じて、この CIDR ブロックを任意の IP アドレス範囲に上書きできます。

ADB-D サービスは、ExaDB-C@C サービスで実行することができます。ADB-D サービスをデプロイした場合、ExaDB-C@C サービスには次のアップデートが適用されます。

- お客様の VM は ADB-D VM となり、オラクルは ADB-D サービスをサポートするために ADB-D VM へのログイン・コントロール(名前付きユーザーとしてトークンベースの ssh)を保持します。お客様は、ADB-D のサービス定義に従い、ADB-D VM にアクセスできません。お客様は、Operator Access Control を使用して、オラクルによる ADB-D VM へのアクセスを制御できます。
- ADB-D は、ADB-D 固有の管理エンドポイントに対する 2 番目の永続的なセキュア発信トンネル・サービスを構成します。
- ADB-D は、ADB-D VM へのリモート ssh アクセス用に、ADB-D 固有のエンドポイントに対する一時的なセキュア発信トンネル・サービスを別途構成します。

オラクルでは、ExaDB-C@C インフラストラクチャの運用と ADB-D の運用の間で職務分掌を徹底しています。

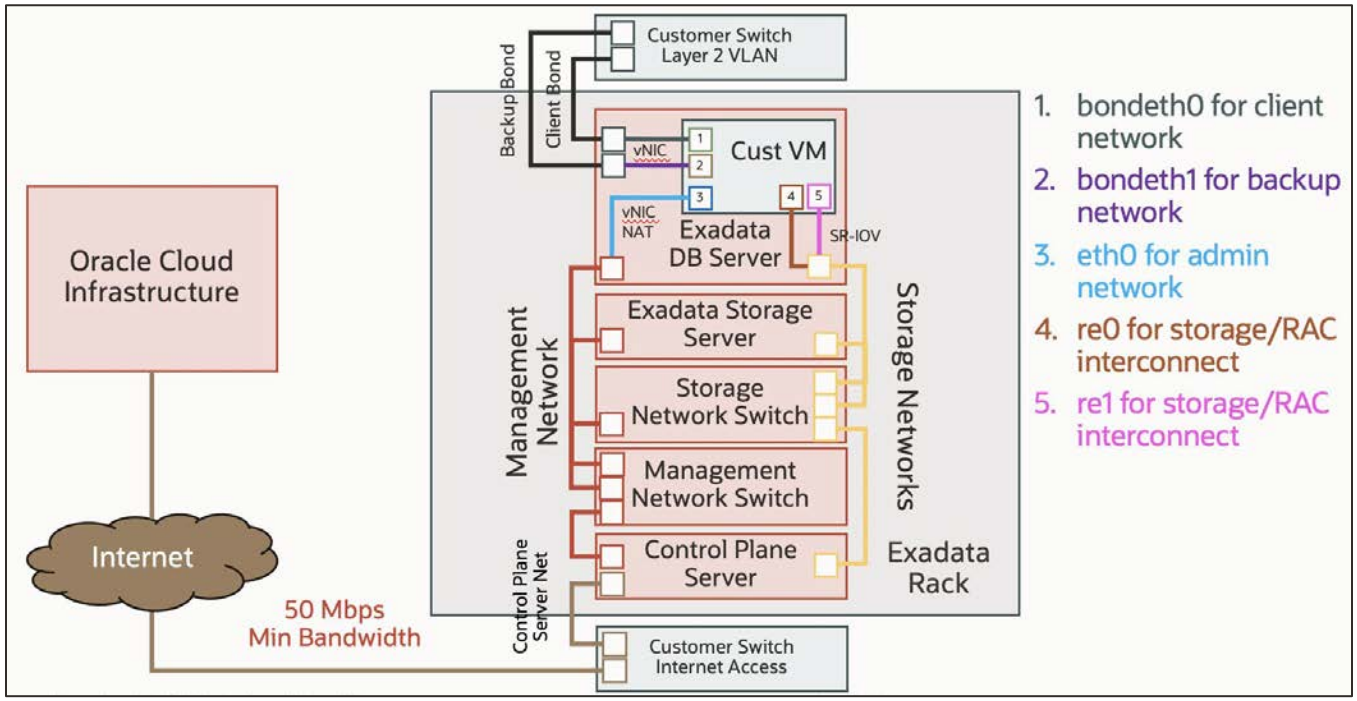

図 2: ExaDB-C@C の物理的なネットワーク実装

図 3 は、CPS のネットワーク・アーキテクチャを示しています。CPS は、お客様のスイッチ、ルーターおよびプロキシ・サーバー経由で、レイヤー2 のイーサネット接続を介してインターネットに到達します。[12]表 2 と「Exadata Cloud@Customer のネットワーク要件」[13]は、サービスの提供に必要な URL を示しています。URL へのアクセスは、ポート 443 でのアウトバウンドのみです。表には、各 URL の TLS プロトコル・バージョンと認証局が示されています。お客様は、CPS へのインバウンド・アクセスを拒否し、必要なオラクル・エンドポイントへのアウトバウンド・アクセスのみを許可するネットワーク・アクセス・ルールを設定できます。サービスは、CPS から OCI エンドポイントへの接続を管理するための http プロキシ(企業プロキシ、パッシブ・プロキシなど)をサポートしています。ExaDB-C@C は、チャレンジ・プロキシや SSL 復号(トラフィック・インスペクション)をサポートしていません。オラクルがサービスに新しい機能を追加したときに、お客様が許可した URL の更新が必要になる場合があります。IP アドレス・フィルタリングを使用している場合は、お客様の OCI リージョンに関連付けられている、該当するすべての IP CIDR 範囲へのトラフィックを許可する必要が

[12] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/eccid/exacc_network.html

[13] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-network-requirements.html#GUID-F06BD75B-E971-48ED-8699-E1004D4B4AC1

あります。[14]図 5 は、インフラストラクチャのソフトウェア・プロセスが OCI エンドポイントにアクセスする方法の例を示しています。

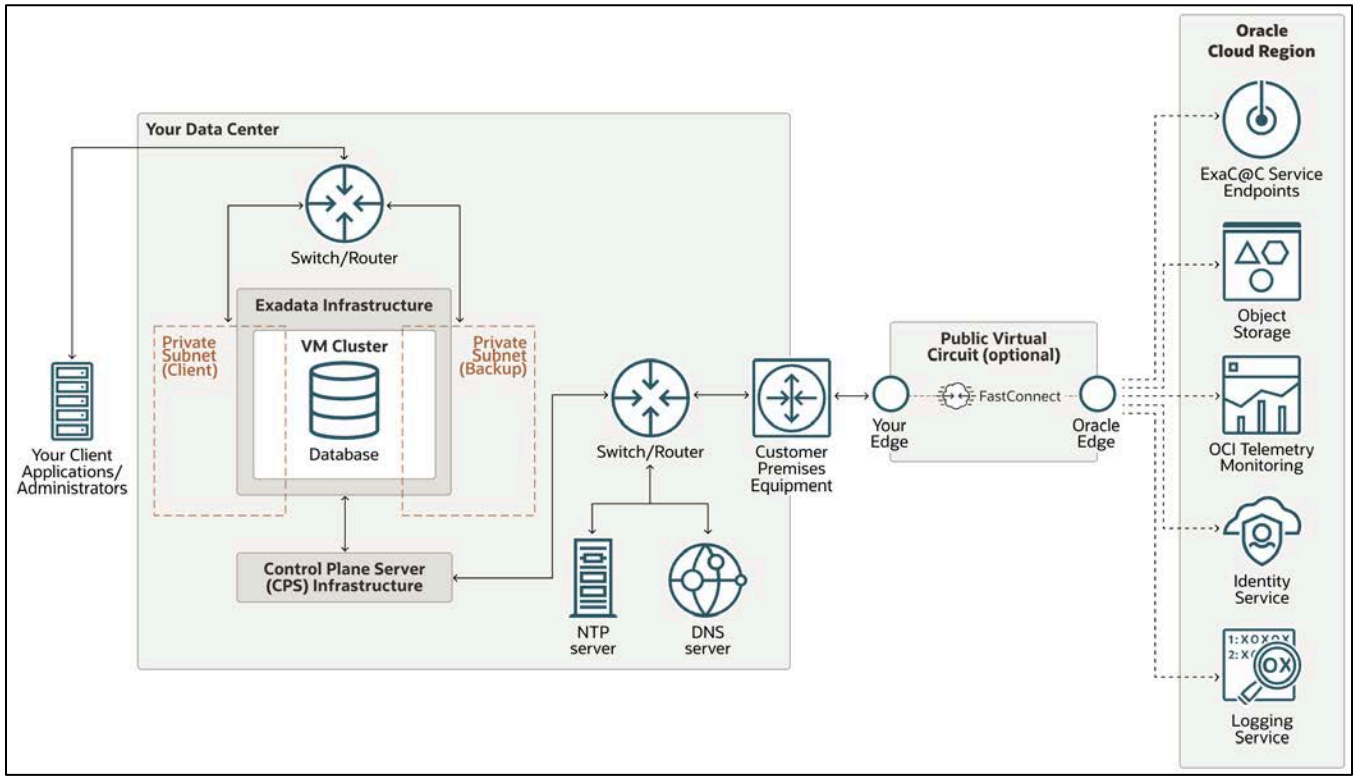

図 3: コントロール・プレーン・サーバーのネットワーク

表 2: サービスの提供に必要な URL - すべてのアクセスがポート 443 でのアウトバウンド

説明/目的	TLS バージョン	認証局	ロケーション *OCI_REGION* を自分のリージョン [15]に置き換えてください
クラウド自動化を提供するための永続発信トンネル・サービス	1.3	DigiCert	https://wss.exacc.*oci_region*.oci.oraclecloud.com
Autonomous Database Dedicated (ADB-D)のクラウド自動化を提供するための永続発信トンネル・サービス、TLS 1.3 プロトコル	1.3	DigiCert	https://wsshe.adbd-exacc.*oci_region*.oci.oraclecloud.com
ExaDB-C@C インフラストラクチャをサポートするリモートのオラクル・オペレータ・アクセス用の一時セキュア・トンネル・サービス、TLS 1.2 プロトコル	1.2	DigiCert	https://mgmthe1.exacc.*oci_region*.oci.oraclecloud.com https://mgmthe2.exacc.*oci_region*.oci.oraclecloud.com
ADB-D リソースに対するリモートのオラクル・オペレータ・アクセス用の一時セキュア・トンネル・サービス、TLS 1.3 プロトコル	1.3	DigiCert	https://mgmthe.adbd-exacc.*oci_region*.oci.oraclecloud.com

[14] https://docs.oracle.com/en-us/iaas/tools/public_ip_ranges.json.

[15] https://docs.oracle.com/en-us/iaas/Content/General/Concepts/regions.htm

システム更新取得用の Object Storage Service、TLS 1.2 プロトコル	1.2	DigiCert	https://objectstorage.*oci_region*.oraclecloud.com https://swiftobjectstorage.*oci_region*.oraclecloud.com https://*.objectstorage.oci_region.oci.customer-oci.com
インフラストラクチャ監視メトリック(IMM)の記録および処理用の Monitoring Service	1.2	DigiCert	https://telemetry-ingestion.*oci_region*.oraclecloud.com
オラクルのオペレータの名前解決用の Identity Service	1.2	DigiCert	https://identity.*oci_region*.oraclecloud.com https://auth.*oci_region*.oraclecloud.com
アプリケーションおよびセキュリティ・ログのロギング・サービス	1.2	Oracle PKISVC CrossRegion Intermediate r2[16]	https://frontend.logging.ad1.oci_region.oracleiaas.com https://frontend.logging.ad2.oci_region.oracleiaas.com https://frontend.logging.ad3.oci_region.oracleiaas.com https://controlplane.logging.ad1.*oci_region*.oracleiaas.com https://controlplane.logging.ad2.*oci_region*.oracleiaas.com https://controlplane.logging.ad3.*oci_region*.oracleiaas.com
リソース・プリンシパル・ベースの認証および Autonomous Database サービスの提供	1.2	DigiCert	https://database.*oci_region*.oraclecloud.com
VM コンソール	1.2	DigiCert	https://console1.exacc.*oci_region*.oci.oraclecloud.com https://console2.exacc.*oci_region*.oci.oraclecloud.com
インフラストラクチャ監視メトリック(IMM)リソースの記録および処理用の Monitoring Service	1.2	DigiCert	https://ingestion.logging.region.oci.oraclecloud.com
メータリングと監視	1.2	DigiCert	https://*.functions.oci_region.oci.oraclecloud.com

OCI FastConnect[17]またはサイト間 VPN[18, 19]を使用すると、ExaDB-C@C インフラストラクチャを OCI に接続できます。OCI 転送ルーティング [20]とびネットワーク・セキュリティ・リスト [21]を使用すると、OCI サービスへの ExaDB-C@C インフラストラクチャのアクセスを制御できます。OCI VCN フロー・ログ [22]を使用すると、ネットワーク・エンドポイントへのトラフィック量を監視できます。OCI Network Firewall[23]を転送用 VCN で使用すると、ExaDB-C@C サービスをサポートするために必要な URL と IP アドレスの許可リストを実装できます。図 4 は、転送用 VCN の実装を示しています。

[16] PKISVC CrossRegion Intermediate r2 は、オラクルのクラウド・コントロール・プレーン・サービス(ExaDB-C@C によって使用される内部ロギング・システムなど)向けの、オラクルが管理する Oracle Cloud Infrastructure 認証局(CA)です

[17] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/fastconnect.htm

[18] https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/overviewIPsec.htm

[19] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-network-requirements.html#GUID-E53A5DCF-CCCD-4493-B1D2-4EA6FA30B8A1

[20] https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/transitroutingoracleservices.htm

[21] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/securitylists.htm

[22] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/vcn_flow_logs.htm

[23] https://docs.oracle.com/en-us/iaas/Content/network-firewall/overview.htm

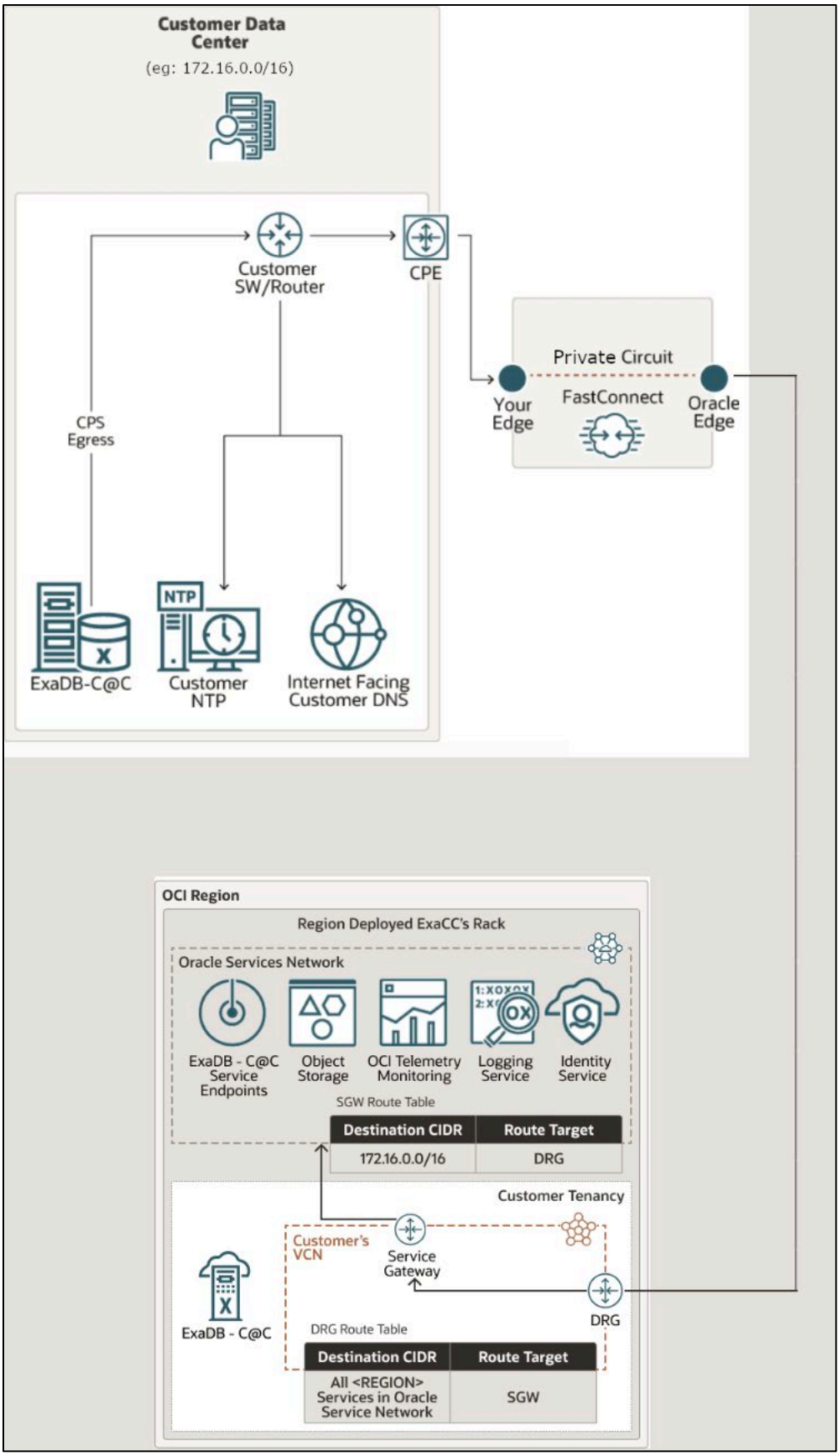

図 4: 転送用 VCN を使用したコントロール・プレーン・サーバーのネットワーク

図 5 は、ソフトウェア・プロセスが OCI とオンプレミス・ラックの間の通信を管理する方法の例を示しています。自動化を提供するための永続セキュア・トンネル・サービスは、クラウド自動化コマンド(REST API コール)を送信し、サービスの可用性を評価するための最小限の診断を返します。リモート・オペレータ・アクセス用のセキュア・トンネル・サービスは、オラクルが管理するインフラストラクチャと ADB-D リソース(該当する場合)への一時的なオラクル・オペレータ・アクセス(ssh)を提供します。これらのサービスは、ExaDB-C@C に限定されたサービスであり、OCI のパブリック・サービスの一部ではありません。OCI サービスへの接続は一時的なもので、オブジェクト・ストレージからのソフトウェア・アップデートのダウンロード、リソース・プリンシパルとサービス・プリンシパルの認証、監視レコードとロギング・レコードの送信などのサービス機能に必要な場合に、ジャストインタイムで構成されます。

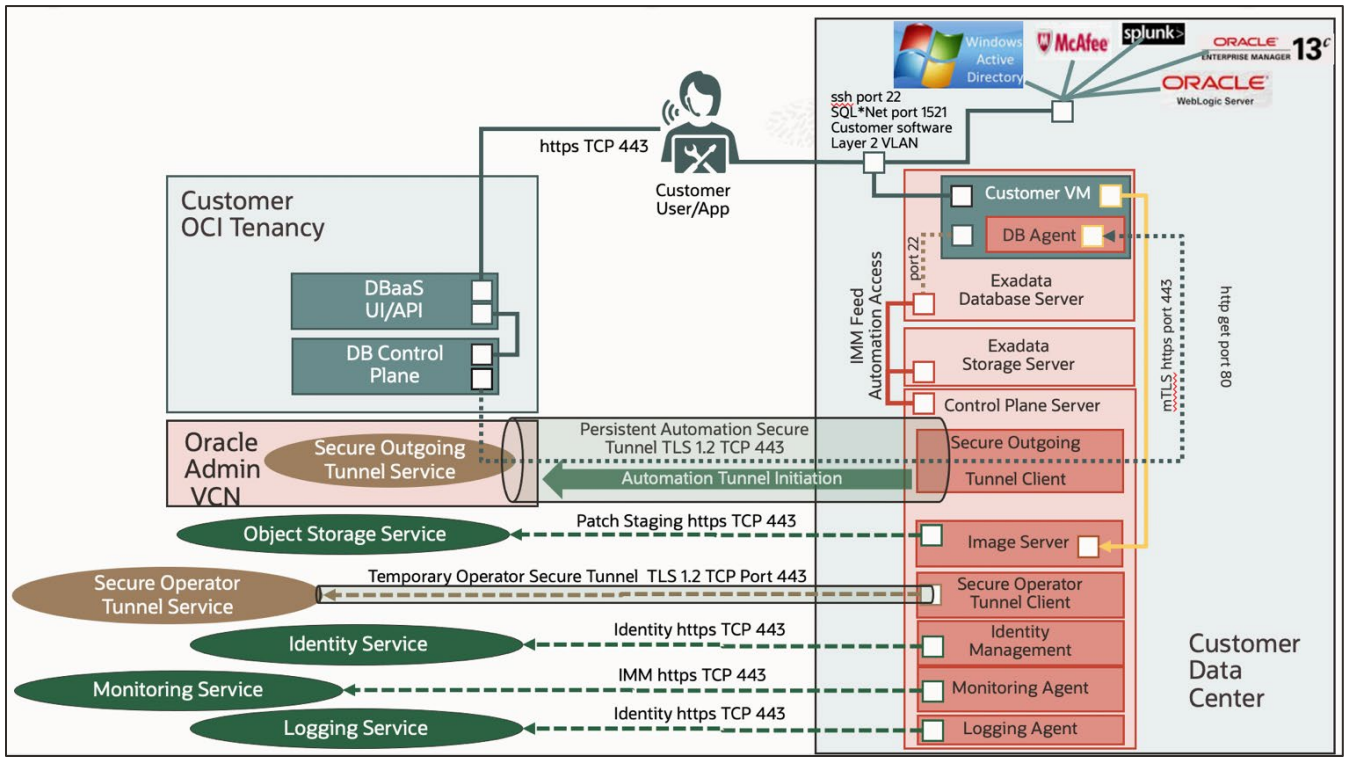

図 5: OCI サービスへのインフラストラクチャのアクセス

オラクルは、インフラストラクチャから OCI への接続のために、TLS と mTLS の証明書を独占的に管理します。オラクルは、永続セキュア・トンネル・サービスのクライアント証明書を 6 か月のスケジュールでローテーションします。オラクルは、リモート・オペレータ・アクセス用のセキュア・トンネル・サービスのクライアント証明書を 15 日のスケジュールでローテーションします。クライアント証明書は、各 ExaDB-C@C インフラストラクチャに固有です。証明書のサブジェクト代替名(SAN)には、ExaDB-C@C インフラストラクチャの Oracle Cloud アイデンティティ(OCID)が含まれています。

VM ネットワークと CPU の分離

図 6 は、同じ Exadata Database Server (DB Server)にデプロイされた異なる仮想マシン・クラスタ(VM クラスタ)間のネットワーク分離を示しています。[24]VM は、クライアント・ネットワーク(ネットワーク 1)とバックアップ・ネットワーク(ネットワーク 2)の物理リンクを共有します。お客様は、ネットワーク・アクセスを分離するために、異なる VM クラスタの異なるネットワークに異なる VLAN タグを指定できます。ソフトウェアは、VLAN を自動的に構成して、各 VM クラスタのストレージ・ネットワーク(ネットワーク 4 および 5)を分離します。/30 vNIC 管理ネットワーク(ネットワーク 3)は、同じ Exadata DB Server 上の異なる VM の管理ネットワークを分離します。Exadata Database Server は、異なる管理ネットワーク間のルーティングを行いません。CPU コアは特定の VM に固定されるため、VM 内の方法によって他の VM の CPU キャッシュ・データにアクセスするのを防ぐことができます。VM クラスタ・ネットワークの分離の例と、VM クラスタ・ネットワークの分離が PCI DSS に準拠した運用にどのように役立つかについては、『Oracle Database Machine and Compliance with PCI DSS V3.2』[25]を参照してください。

[24] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/eccid/exacc_vmdb.html

[25] https://www.oracle.com/assets/exadata-pci-dss-compliance-wp-3157442.pdf

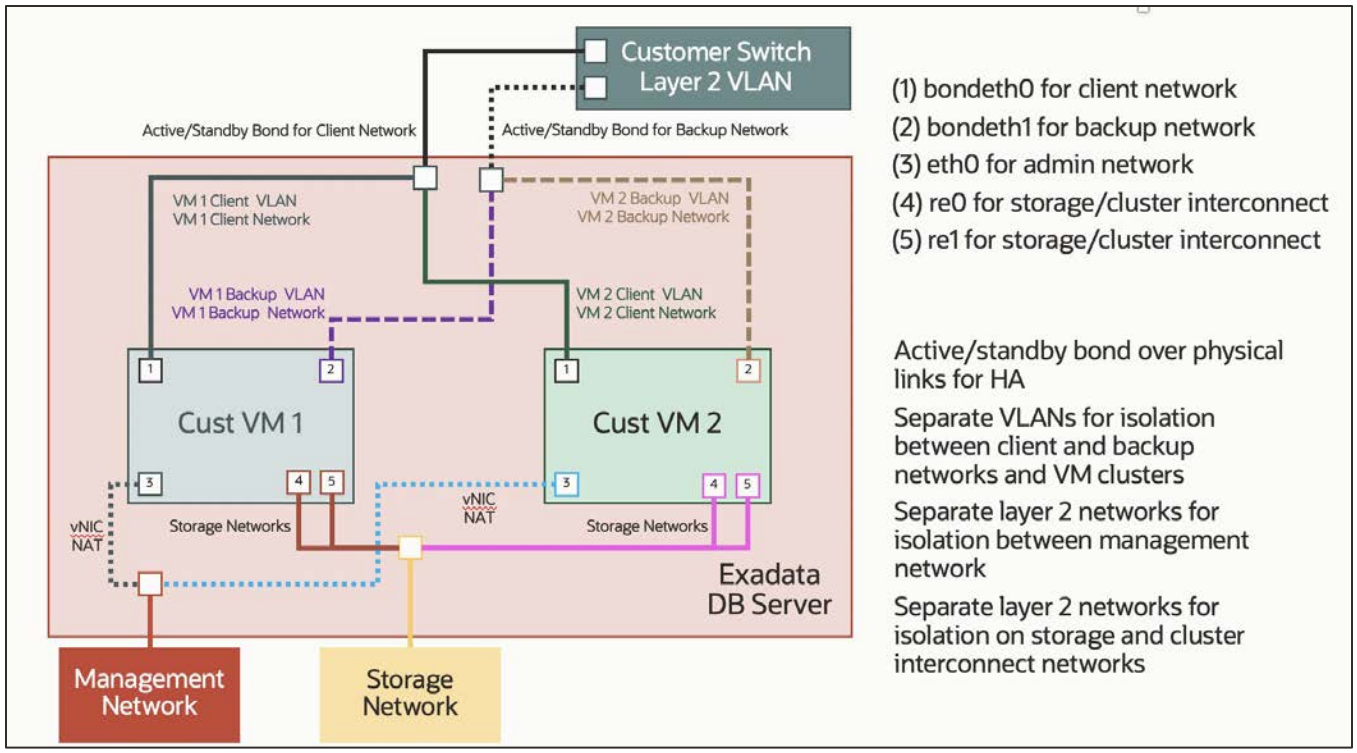

図 6: VM クラスタ・ネットワークの分離

サービスのライフサイクル管理

サービスの管理には、次のような 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 コンソール経由の非定型アクションに使用
- Oracle クラウド・シェル: 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): スクリプティングと自動化のためのコマンドライン・インタフェース
- OCI SDK/RESTAPI: アプリケーションの統合に使用
- OCI Terraform プロバイダ [26]: Hashicorp によってドキュメントが提供されています。[27]

OCI 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、コントロール・プレーンは、セキュア自動化トンネル経由で必要なコンポーネントに次のようにコマンドを送信します。

データベース操作:

- VM のエージェント・ソフトウェアへの REST API アクセス
- mTLS で保護
- ストレージ・ネットワーク上で転送

VM 操作:

- コントロール・プレーン・サーバー・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・プレーンによって管理され、VM のエージェント・ソフトウェアを使用して提供される、一時的なキーで保護
- 管理ネットワーク上で転送

インフラストラクチャ操作:

- インフラストラクチャのエージェント・ソフトウェアへの REST API アクセスと、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 とコントロール・プレーンによって管理されるキーで保護
- コントロール・プレーン管理ネットワーク上で転送

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

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

一部の管理機能は、VM とデータベースに直接アクセスして実行することもできます。複雑さと運用上の負担を軽減し、監査を改善するために、OCI インタフェースが使用可能な場合は使用することをお薦めします。

四半期ソフトウェア・アップデート

Oracle ソフトウェアの開発は、Oracle Software Security Assurance Practices[28]と Oracle Software Security Assurance[29]の基準によってコントロールされます。オラクルは、開発、テスト、品質保証およびソフトウェアのデプロイメントにおいて、職務分掌 [30]を実施しています。詳細は、次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[31]
- Exadata Cloud のソフトウェア・バージョンに関する My Oracle Support ドキュメント 2333222.1[32]
- インフラストラクチャのアップデートに関する Oracle Cloud Infrastructure メンテナンス・ドキュメント [33]
- VM、Grid Infrastructure および Oracle Database のソフトウェア・アップデートに関する Exadata Cloud@Customer のドキュメント [34]

オラクルは、Oracle Database、Grid Infrastructure および Linux オペレーティング・システムの四半期ソフトウェア・アップデートを OCI Object Storage でステージングします。これらのアップデートは、利用可能になると OCI インタフェースに一覧表示されます。お客様は、ユーザーへの影響が最も小さい期間にメンテナンスをスケジュールできます。OCI インタフェースでは、四半期メンテナンスの適用時期を表示して完全にコントロールできます。必要に応じてメンテナンスのスケジュールを変更する機能もあります。[35]

オラクルは、ローリング・メンテナンス操作を使用して、四半期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、アップデート・プロセス全体を通し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、オフラインのサーバーが常に最大でも 1 つになるように、各 Database Server を一度に 1 つずつリブートします。高可用性を考慮して設計されたアプリケーションでは、使用可能なデータベース・インスタンス間で自動的かつ透過的にデータベース接続が移行されるため、中断は発生せず、ダウンタイムをスケジュールする必要がなくなります。ストレージ・サーバーのアップデートもローリング方式で適用されます。お客様は、複数のコンポーネントが同時にアップデートされるオフライン・メンテナンスを実行して、メンテナンス期間を短縮できます。オフライン・メンテナンスの間はデータベースを使用できません。

月次インフラストラクチャ・セキュリティ・スキャンおよびアップデート

オラクルは、ExaDB-C@C インフラストラクチャに対する月次インフラストラクチャ・セキュリティ・スキャンおよびアップデート[36]を実行して、オラクルの企業セキュリティ標準へのコンプライアンスを維持します。この標準は、PCI-DSS などの各種業界標準と、FedRAMP High や ISO/IEC 27001 などの政府セキュリティ標準に準拠し、それらをサポートしています。オラクルは、インフラストラクチャのアップデートをオンラインで実行します。その際にリブートは発生せず、互換アプリケーションへの影響もありません。[37]オラクルは、ストレージ・サーバーの月次セキュリティ・アップデートをローリング方式で実行します。その際も、アプリケーションへの影響はありません。お客様は、月次セキュリティ・メンテナンスをその月の特定の時期(ただし、単一のメンテナンス期間内)にスケジュールできます。オラクルは、メンテナンス期間の開始日より 1 週間以上前に、月次メンテナンスのスケジュールを公開します。お客様は、必要に応じてスケジュールを変更できます。お客様は、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許可されておらず、監視エージェントをインストールしたり、オラクルが管理するインフラストラクチャにファイルを転送したりすることもできません。

オラクルのインフラストラクチャ監視

オラクルは、オラクルの操作責任となる次のような問題を検出して対応します。[38]

- インフラストラクチャのセキュリティとアクセス制御

---

[28] https://www.oracle.com/corporate/security-practices/assurance/
[29] https://www.oracle.com/corporate/security-practices/assurance/
[30] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[31] https://www.oracle.com/security-alerts/
[32] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2333222.1
[33] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-system-config-options.html
[34] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-update-exacc-system.html
[35] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-vw-maint-hist.html
[36] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-vw-maint-hist.html
[37] https://docs.oracle.com/en/database/oracle/oracle-database/19/racad/ensuring-application-continuity.html#GUID-C1EF6BDA-5F90-448F-A1E2-DC15AD5CFE75
[38] https://support.oracle.com/knowledge/Oracle%20Cloud/2707015_1.html

- Exadata コンピュート、ストレージおよびネットワーク・インフラストラクチャのハードウェアとソフトウェア[39]の監視とメンテナンス
- Auto Service Request Qualified Engineered Systems Products[40]イベントの監視とメンテナンス

お客様の ExaDB-C@C は、インフラストラクチャ監視メトリック(IMM)を OCI コントロール・プレーンの監視システムに自動的に送信します。Oracle サポートは、このデータをトリアージし、必要に応じてサポート・スタッフにチケットを割り当てて解決します。

オラクルは、オラクルによる対処が可能ではない、次のようなコンポーネントは監視しません。

- フラッシュ・キャッシュの使用量
- ゲスト VM のセキュリティとアクセス・ログ
- Oracle CRS、ASM および Database
- ゲスト OS で実行されているお客様のソフトウェア

お客様の VM のセキュリティ・テストとスキャン

お客様は、Oracle Cloud Testing Policies[41]に従って ExaDB-C@C のセキュリティをテストできます。OpenSCAP[42]を使用して 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。サードパーティのスキャン・ツールを使用して VM をスキャンすることもできます。サードパーティのスキャン・ツールやベンチマークは、Exadata Database Service のソフトウェア・ディストリビューションおよび構成に準拠している必要があります。任意のベンチマークで、Exadata Database Service の VM に関して重要ではないセキュリティの問題が通知される場合があります。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 ノート「Responses to common Exadata security scan findings (Doc ID 1405320.1)」[43]を参照してください。Exadata Database Service の VM が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、サービスの機能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 Database、Grid Infrastructure のアップデートなど、自動化されたソフトウェア・アップデートにより、お客様が行った変更が元に戻る可能性があるため、本番デプロイメントの前にテストする必要があります。

予防的統制

オラクルは、お客様のデータベースのデータを不正アクセスから保護するように ExaDB-C@C を設計しました。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次のように分掌されます。

- お客様は、物理的な機器へのアクセスを制御します。
- お客様は、お客様の OCI テナンシ、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。
- 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論理アクセスを制御します。お客様が Operator Access Control を使用して、オラクルが管理するインフラストラクチャへのオラクルによる論理アクセスを制御することもできます。

お客様は、3 種類の統制を使用して、お客様の OCI テナンシ、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。

認証と認可の統制

- OCI コンソール、API およびサービスにアクセスするための資格証明
- 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

データ暗号化の統制

- アプリケーションからデータベースへのネットワーク暗号化のための Oracle Native Network Encryption または TLS/SSL[44]
- ユーザー表領域の Transparent Database Encryption (TDE)[45]による保管中のデータ暗号化

ネットワークの統制

---

[39] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2875973.1

[40] https://docs.oracle.com/cd/E37710_01/doc.41/e37287/toc.htm

[41] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm

[42] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-scap-sec.html.

[43] https://support.oracle.com/knowledge/Oracle%20Database%20Products/1405320_1.html

[44] Exadata Database Service 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。

[45] Exadata Database Service 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。

- レイヤー2 および 3 での VM へのアクセスに対する、お客様のスイッチおよびファイアウォールのネットワーク・セキュリティ統制
- VM オペレーティング・システム [46]および Oracle Database[47]に実装されたネットワーク・アクセス・ルール
- Delegate Access Control 資格証明で VM に対して認証できるようにするための一時的な Delegate Access Control ネットワークおよび踏み台サーバー
- Operator Access Control 資格証明でインフラストラクチャに対して認証できるようにするための一時的な Operator Access Control ネットワークおよび踏み台サーバー。

ExaDB-C@C のソフトウェア自動化は、ファイアウォールの構成、ネットワーク・インタフェースの無効化、VM で実行されているクラウド自動化ソフトウェア・エージェントの無効化を行うためのインタフェースを提供しません。例外的なセキュリティ要件がある場合は、オペレーティング・システム・ツールを使用してこのような統制を実装できます。ただし、VM にアクセスするクラウド自動化機能を許可する際には注意が必要です。

データベースのセキュリティ統制

Oracle Database ソフトウェア、互換性のある OCI サービス、および互換性のある鍵管理システムに含まれている、次のような Oracle Database セキュリティ統制を ExaDB-C@C で使用できます。

- Oracle Database 認証
- Oracle Database ネットワーク暗号化
- Oracle Transparent Data Encryption
- Oracle Database Vault
- データベース・バックアップの暗号化
- Data Safe
- Database Security Assessment Tool

データベース認証

パスワード認証、Kerberos 認証 [48]、公開鍵基盤(PKI)認証などの Oracle Database 認証を、集中管理ユーザー[49]を使用して構成できます。集中管理ユーザーを使用すると、お客様は Oracle Database にアクセスする Active Directory ユーザーの認可を管理できます。Oracle Database では、ネイティブ・ユーザーの多要素認証(MFA)構成を、Oracle Mobile Authenticator (OMA)または Cisco Duo によるプッシュ通知と証明書ベースの認証のいずれかの形式で行うことができます。[50]MFA は、OCI IAM、MS-EI および RADIUS を使用した人間のユーザー向けの既存の外部認証方式で実装できます。

ネットワーク暗号化

ExaDB-C@C は、クライアントから Oracle Database インスタンスへ移動中のデータを Oracle Native Network Encryption (NNE)で暗号化します。NNE は、サービス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 Database インスタンスは、アプリケーションからの暗号化された接続をリクエストして [51]、対応可能なアプリケーション向けに暗号化された接続を実装します。アプリケーションが暗号化された接続をサポートできない場合、Oracle Database インスタンスはアプリケーションが暗号化なしで接続することを許可します。サービスの自動化は、Oracle Database の接続用に 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、VM にデプロイされたオペレーティング・システム・ツールを使用して TLS/SSL と mTLS を構成できます。[52]Oracle Native Network Encryption および TLS/SSL のドキュメントは、各 Oracle Database バージョンのセキュリティ・ガイドで公開されています。[53]

---

[46] https://docs.oracle.com/en/operating-systems/oracle-linux/8/firewall/firewall-AboutPacketFilteringFirewalls.html
[47] https://docs.oracle.com/en/database/oracle/oracle-database/19/netag/configuring-oracle-connection-manager.html#GUID-AF8A511E-9AE6-4F4D-8E58-F28BC53F64E4
[48] https://support.oracle.com/knowledge/Oracle%20Cloud/2621025_1.html
[49] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/integrating_mads_with_oracle_database.html#GUID-9739D541-FA9D-422A-95CA-799A4C6F488D
[50] https://docs.oracle.com/en/database/oracle/oracle-database/23/dbseg/configuring-authentication.html#GUID-10E4F568-0FA3-4F82-99AA-14FB2947469C
[51] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-network-data-encryption-and-integrity.html#GUID-42863092-227B-437C-AFFA-623BE6AEA0EA
[52] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-using-dbaascli.html#GUID-4021F2D5-E822-470D-8570-A28EC650D905
[53] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-network-data-encryption-and-integrity.html#GUID-7F12066A-2BA1-476C-809B-BB95A3F727CF

保管中のデータの暗号化

ExaDB-C@C は、保管中のユーザー表領域データを 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)からなる 2 層の鍵アーキテクチャです。表と表領域のデータを暗号化する DEK は、MEK でラップされます。MEK 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 MEK は次の場所に格納できます。

- PKCS#12 ウォレット
- Oracle Key Vault
- 互換性のあるサードパーティの HSM

Oracle TDE は、高いパフォーマンスを発揮できるように設計されています。Intel CPU (AES-NI)の特別な命令を自動的に利用して暗号化操作を高速化します。さらに、Oracle TDE の表領域暗号化は、Exadata Hybrid Columnar Compression (EHCC)および Smart Scan テクノロジとシームレスに連携します。Oracle TDE を使用すれば、機微なユーザー・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、あるいは REDO ログなどの他のファイルのいずれにあっても、データベース全体で常に暗号化されています。さらに、TDE ではデータベース・バックアップ全体を暗号化できます。Data Pump と Oracle Recovery Manager (RMAN)はどちらも TDE の暗号化データと統合されます。Exadata Database Service での TDE 実装の詳細は、Exadata Database Machine の暗号化サービス [54]に関するドキュメントに記載されています。Oracle TDE の詳細は、実行している Oracle Database 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[55]には、Oracle TDE のアーキテクチャと実装に関する一般的な質問と回答が記載されています。

PKCS#12 ウォレットを使用した暗号化鍵の管理

TDE MEK は、データベースの外部(デフォルトでは PKCS#12 準拠のウォレットと呼ばれるコンテナ)に格納されます。ウォレットは、ExaDB-C@C の VM がアクセスできるファイル・システムに格納されます。Oracle Databases 18c 以降では、お客様は外部で生成された独自の暗号化鍵(Bring-Your-Own-Key (BYOK))を共有ウォレットにアップロードすることで、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。

Oracle Key Vault を使用した暗号化鍵の管理

ExaDB-C@C データベースを Oracle Key Vault (OKV)に移行できます。[56] OKV 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(BYOK)を取り込む機能も提供されます。オペレーティング・システム方式を使用して TDE マスター鍵を OKV に移行する手順は、製品ドキュメントの「Managing Encryption Keys on External Devices」[57]と「Migration of File based TDE to OKV for Exadata Database Service Using Automation via REST (Doc ID 2924192.1)」[58]で公開されています。OKV サーバーが使用できない場合は、OKV 永続マスター暗号化鍵キャッシュ [59]を使用して、データベースを稼働させることができます。

暗号化鍵の管理とサードパーティのハードウェア・セキュリティ・モジュール(HSM)

Oracle Database は、PKCS#11 互換の鍵管理デバイスに対応しています。[60]鍵管理と HSM のサードパーティ・ベンダーは、このインタフェースを使用して、Oracle Database 向けの TDE 鍵管理を実装しています。実装とサポートの詳細は、My Oracle Support (MOS)ノー

---

[54] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/exadata-security-features.html#GUID-FA8A2A69-AEFC-4FE3-959A-A6E584BD1F4F

[55] https://www.oracle.com/database/technologies/faq-tde.html

[56] https://docs.oracle.com/en/database/oracle/key-vault/21.2/okvag/okv_intro.html#GUID-0D169EB8-C355-459A-9ABD-325CA5B46DD0

[57] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/managing-encryption-keys-on-external-devices.html#GUID-627C83FC-D8A3-4BF2-80F6-70B11DED0C43

[58] https://support.oracle.com/knowledge/Oracle%20Cloud/2924192_1.html

[59] https://docs.oracle.com/en/database/oracle/key-vault/21.7/okvag/security_objects.html#GUID-27DA6A5A-E405-4394-BD0D-C2B213391426

[60] https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/introduction-to-transparent-data-encryption.html#GUID-2D6C5B27-8E6A-4EF7-AABF-B0FB031C8374

ト「Oracle TDE Support With 3rd Party HSM Vendors」(Doc ID 2310066.1)[61]を参照してください。ExaDB-C@C の自動化は、外部キー・マネージャを構成するためのインタフェースを提供します。[62]

外部のキー・マネージャを統合するには、お客様の Exadata Database Service の 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。サードパーティ製キー・マネージャと HSM のベンダーまたは実装業者は、こうした統合の構築、テスト、文書化、サポートを行います。オラクルは、Oracle Database でのサードパーティ製キー・マネージャと HSM の動作保証を行うプログラムを保持していません。また、オラクル・コーポレーションは、透過的データ暗号化が有効になっているデータベースの鍵管理を提供するサードパーティ製ハードウェア・セキュリティ・モジュールをサポートしていません。

HSM ベンダーは、自社デバイスの動作保証を独自に行い、Oracle Key Vault にルート・オブ・トラストを提供することができます。その場合は、『Oracle Key Vault ルート・オブ・トラスト HSM 構成ガイド』[63]の「Oracle Key Vault のルート・オブ・トラストとして HSM を統合するためのベンダーの手順」を参照してください。

データベース管理者による SQL でのユーザー・データへのアクセスを防止

Oracle Database Vault を使用すると、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することができます。このコントロール機能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。さらに、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。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』[64]で公開されています。

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、透過的データ暗号化によるウォレット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。[65]暗号化鍵はバックアップと一緒に格納されません。Autonomous Recovery Service[66]を使用すると、暗号化された表領域のバックアップと、それらの表領域の変更が記述された REDO が暗号化されます。[67]TDE 暗号化データ・ブロックが暗号化されるのは、データベース、Recovery Appliance ストレージ、テープ・デバイスおよびレプリケートされたアプライアンス上と、ネットワーク接続経由で転送された場合です。

データベース・セキュリティの自動監視および管理

Oracle Database および ExaDB-C@C と互換性のあるソフトウェアとサービスを使用して、データベースのセキュリティ体制を監視および管理できます。Oracle Data Safe は、ExaDB-C@C データベースに統合できるクラウド・サービスです。Oracle Database Security Assessment Tool (DBSAT)は、オラクルからダウンロードして ExaDB-C@C データベースで使用できるスタンドアロン・ソフトウェアです。

Oracle Data Safe

Oracle Data Safe[68]を使用すると、データベースのセキュリティを監視および管理できます。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
- レポートおよびアラートの生成を含む、監査データの分析
- 機微データの種類、量、場所などの検出
- 機微データをマスクし、本番環境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

---

[61] https://support.oracle.com/knowledge/Oracle%20Database%20Products/2310066_1.html

[62] https://docs.oracle.com/en-us/iaas/exadata/doc/manage-and-store-master-encryption-keys-on-an-external-hsm.html#GUID-C40542DB-A167-4503-B0DF-CC1C6DB04882

[63] https://docs.oracle.com/en/database/oracle/key-vault/21.3/okvhm/index.html#Oracle%C2%AE-Key-Vault

[64] 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

[65] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html

[66] https://docs.oracle.com/en-us/iaas/recovery-service/index.html

[67] https://docs.oracle.com/en/engineered-systems/zero-data-loss-recovery-appliance/23.1/amagd/data-encryption-techniques.html#GUID-3E1A521B-3B51-4D1F-BF88-27BBE41A4B03

[68] https://docs.oracle.com/en-us/iaas/data-safe/index.html

Oracle Data Safe の技術アーキテクチャ [69]は、お客様のサーバーにデプロイされたオンプレミス・コネクタをサポートして、ExaDB-C@C 上で実行されているデータベースを OCI Data Safe サービスにスムーズに接続する機能を示しています。Data Safe FAQ[70]には、Data Safe に関してよく尋ねられる質問への回答が掲載されています。監査レコードが、1 データベースあたり 100 万件/月までであれば、Data Safe の利用において追加費用は発生しません。

Oracle Database Security Assessment Tool

Oracle Database Security Assessment Tool (DBSAT)[71]は、評価と規制遵守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、オラクルからダウンロードできます。DBSAT は、関連する構成情報をデータベースから収集して、セキュリティの状態を評価し、特定されたリスクを低減する方法について、次のような推奨事項を提供します。

- セキュリティ構成の問題とその修正方法
- ユーザーとそのユーザーのエンタイトルメント
- 機微データの場所、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、認可コントロール、職務分掌、ファイングレイン・アクセス・コントロール、データ暗号化、鍵の管理、監査ポリシー、OS ファイルのアクセス権も調査されます。DBSAT で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低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低減できます。

VM のセキュリティ統制

ExaDB-C@C VM のデプロイメントには、業界のベスト・プラクティスとオラクルによるセキュリティの監督に基づく、セキュリティが強化されたオペレーティング・システムが含まれています。セキュリティ構成機能には次のものがあります。[72]

最小限のパッケージ・インストールと有効になるサービス:

- 効率的なシステムの実行に必要なパッケージのみがインストールされます。
- システムにインストールされても、通常の操作には不要なサービスは、デフォルトで無効になります。
- オプションで、要件に合わせてサービスを構成できます。

安全な構成:

- システムのセキュリティ体制を強化するため、インストール中に構成パラメータが設定されます。
- `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を行うように構成されます。
- `sendmail` は、localhost 接続のみを受け入れるように構成されます。

有効になるその他のセキュリティ機能:

- grub パスワード
- セキュア・ブート

安全なアクセス方法:

- 強力な暗号を使用して `ssh` で Database Server にアクセス
- 弱い暗号はデフォルトで無効になります。
- 暗号化された Oracle Net 接続経由でデータベースにアクセス
- デフォルトでは、サービスを使用するには暗号化されたチャネルを使用する必要があり、デフォルトの構成済 Oracle Net クライアントは暗号化されたセッションを使用します。
- Exadata MS Web インタフェース(https)経由で診断にアクセス

監査とロギング:

- 管理操作用に監査が有効になります。
- 自動レビューおよびアラート用に監査レコードを外部システムに送信できます。

---

[69] https://docs.oracle.com/en/solutions/oracle-data-safe-for-on-prem-database/index.html#GUID-07534FC6-3B10-48E5-BD49-C011D55D1070

[70] https://www.oracle.com/security/database-security/data-safe/faq/

[71] https://www.oracle.com/security/database-security/assessment-tool/

[72] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html

VM へのアクセスは、トークンベースの ssh を介して実行されます。[73]お客様は、OCI 資格証明を使用して、指定する公開鍵を /home/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、opc ユーザーとして VM にアクセスできるようになります。Oracle クラウド自動化は外部の鍵管理システムと統合されませんが、Oracle Linux と互換性のあるテクノロジを使用して ssh 鍵を管理できます。詳細は、該当する PAM プロバイダにお問い合わせください。API Access Control[74]で ssh 鍵の追加機能をコントロールして、ssh 鍵を追加しようとする OCI アイデンティティは別の OCI アイデンティティから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 ソフトウェアのバージョン 22.1.4.0.0.221020 以降、お客様は、Microsoft Active Directory (AD)と Lightweight Directory Access Protocol (LDAP)を VM に対する認証用に実装できます。AD と LDAP は、標準的なオペレーティング・システム・ツールを使用して構成できます。アイデンティティ・サービスを提供する LDAP を使用して VM へのアクセスを促進するように Linux System Security Services Daemon (SSSD)を構成できます。Oracle Exadata System Software には、SSSD をサポートする Linux パッケージが含まれており、特定の要件に従って SSSD を構成できます。SSSD のサポートは、Oracle Linux 8 で Linux authselect ユーティリティを使用することで、Exadata 固有のセキュリティ・プロファイルとともに有効になります。Oracle Exadata System Software は、システムのアップデート中、既存の SSSD 構成の詳細を維持します。[75]

トークンベースの ssh を介した 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。[76]Kerberos 認証を 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ります。

VM のデフォルト・ユーザー

ExaDB-C@C の各 VM には、オラクルがサービスの提供と維持に使用する標準の特権サービス・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。[77]サービス・アカウントには次のものがあります。

- root: Linux では必須です。ソフトウェア・アップデート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)用の権限に使用されます。
- grid: Oracle Grid Infrastructure ソフトウェアとプロセスを所有、実行、維持します。
- oracle: Oracle Database ソフトウェアとプロセスを所有、実行、維持します。
- opc: Oracle クラウド自動化で使用されます。
  - 自動化タスクを実行します。
  - 特定の特権コマンドを実行できます。
  - サービスのライフサイクル操作のためにコントロール・プレーン・エージェント・ソフトウェア(DBCS Agent と DBCS Admin)を実行します。
- dbmadmin: Exadata のコア機能を管理するために DBMCLI[78]ツールで使用されます。

セキュリティ・スキャン・ツールは、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、Exadata Database Service ソフトウェアと互換性のある LDAP または PAM ソフトウェアの構成など、管理目的で使用できます。

デプロイ済のユーザー名、ユーザーID、グループ名、グループ ID は維持することをお薦めします。Oracle ホーム・ユーザー(oracle)または Grid Infrastructure ユーザー(grid)のインストール後の変更はサポートされておらず、サービス例外の原因となります。[79]

VM のデフォルトのセキュリティ設定

ソフトウェアは、ExaDB-C@C の VM を、業界標準とオラクルのベスト・プラクティスに沿ったセキュリティ設定でデプロイします。[80, 81]これらの構成は、アクセス制御を実施し、操作上のリスクを軽減し、自動ライフサイクル管理をサポートするのに役立ちます。重要な設定には次のものがあります。

---

[73] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-connecting-to-exacc-system.html#GUID-C7C5C13C-B518-4FFC-B050-055E5C35EFA0

[74] https://docs.oracle.com/en-us/iaas/oracle-api-access-control/index.html

[75] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmso/linux-sssd-support.html

[76] https://support.oracle.com/knowledge/Oracle%20Cloud/2621025_1.html

[77] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-ACA1086F-E46D-4AFA-97B0-EFA0C280784B

[78] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmmn/using-dbmcli-utility1.html

[79] https://docs.oracle.com/en/database/oracle/oracle-database/19/cwwin/about-the-oracle-home-user-for-the-oracle-grid-infrastructure-installation.html

[80] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/security.html

[81] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-4F68D138-3778-4AED-B501-3E1108831E9C

- パスワード・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・タイムアウトに関するポリシー
- ssh によるダイレクト root ログインの拒否

技術的な構成には次のものがあります。

- `/etc/ssh/sshd_config` の `PermitRootLogin` 値。これは、root ユーザーの SSH によるログインを許可または拒否します。
  - デフォルト:PermitRootLogin は without-password に設定されます。
  - 推奨: デフォルトを維持し、OS パッチ適用などのクラウド自動化機能を許可
- `session-limit`: `/etc/security/limits.conf` の `hard maxlogins` パラメータを設定します。これは、すべてのユーザーの最大ログイン回数です。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: デフォルトを維持
- `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、プロトコル・バージョン 2 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ともに hmac-sha1、hmac-sha2-256、hmac-sha2-512
  - 推奨: デフォルトを維持
- `password-aging`: 対話型ユーザー・アカウントの現在のパスワード・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`: パスワード変更の間隔として許容される最小日数。
  - `-W`: パスワードの期限が切れる前に警告が表示される日数。
  - デフォルト:`-M 99999`、`-m 0`、`-W 7`
  - 推奨: 厳密なコンプライアンスのための`-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 のリバランスなど)に対応できるように構成されます。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・ツールで許可される必要があります。お客様には、テストとメンテナンスの労力を削減するため、また構成の変更によって生じるサービス中断のリスクを回避するために、デプロイ済の設定を維持することをお薦めします。

VM のデフォルトのプロセスおよび証明書

ExaDB-C@C の VM は、Oracle Database、Oracle Real Application Clusters (RAC)、Oracle Trace File Analyzer (TAF)、Exawatcher、Exadata Management Server (MS)など、データベース操作をサポートする Oracle ソフトウェア・プロセスを実行します。[82]表 3 は、サービスとポートを示しています。この表は、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、認証局(CA)を示しています。オラクルが管理するサービスの Oracle CA とオラクルが自己署名した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お薦めします。これらの証明書と CA は、ライフサイクル管理操作の提供を保護するために、サービスに組み込まれ、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、証明書に関連するサービスの問題のリスクを軽減し、操作の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・ポート・マトリクス

インタフェースのタイプ	インタフェースの名前	ポート	実行されるプロセス	認証局
クライアント VLAN のブリッジ	bondeth0	22	sshd[83]	該当なし
		1521 オプションで、お客様は 1024 から 8999 の範囲で SCAN リスナー・ポート(TCP/IP)を割り当てることができます。デフォルトは 1521 です。	Oracle TNS リスナー[84] 着信クライアント接続リクエストを受信し、Database Server へのリクエストのトラフィックを管理します。	オラクルが自己署名、お客様が管理する証明書を追加可能

[82] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-61DB809E-A676-4B11-BF45-35DB89FC87EC

[83] https://docs.oracle.com/en/operating-systems/oracle-linux/openssh/openssh-ConfiguringOpenSSHServer.html

[84] https://docs.oracle.com/en/database/oracle/oracle-database/19/netag/configuring-and-administering-oracle-net-listener.html

		注意: TNS リスナーは、既知のポート(1521、1525)への初期接続後に動的ポートをオープンします。	Transport Layer Security 認証 [85]として Oracle Native Network Encryption (NNE)と TLS/SSL をサポートしています。	
		5000	Oracle Trace File Analyzer[86] Collector	オラクルが自己署名
		7879	Jetty 管理サーバー[87]。 Oracle Exadata System Software、特に管理サーバー(MS)[88]が内部的に使用す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 オプションで、お客様は 1024 から 8999 の範囲で SCAN リスナー・ポート(TCP/IP)を割り当てることができます。デフォルトは 1521 です。	Oracle TNS リスナー	オラクルが自己署名、お客様が管理する証明書を追加可能
	bondeth0:2	1521 オプションで、お客様は 1024 から 8999 の範囲で SCAN リスナー・ポート(TCP/IP)を割り当てることができます。デフォルトは 1521 です。	Oracle TNS リスナー	オラクルが自己署名、お客様が管理する証明書を追加可能
バックアップ VLAN のブリッジ	bondeth1	7879	Jetty 管理サーバー	オラクルが自己署名
各クラスタ・ノードで実行されている Oracle	clib0/clre0	1525	Oracle TNS リスナー 各クラスタ・ノードで実行されている 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

[85] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-secure-sockets-layer-authentication.html#GUID-6AD89576-526F-4D6B-A539-ADF4B840819F

[86] https://docs.oracle.com/en/database/oracle/oracle-database/19/atnms/managing-and-configuring-tfa.html

[87] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmso/application-server-update-management-server.html

[88] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmso/management-server-database-servers.html

Clusterware[89, 90]**は、これらのインタフェースを介して通信します。**		3260	Synology DSM iSCSI	該当なし
		5054	Oracle Grid Interprocess Communication	該当なし
		7879	Jetty 管理サーバー	オラクルが自己署名
		動的ポート: 9000-65500 ポートは、オペレーティング・システムで構成されているエフェメラル範囲によって制御され、動的です。	システム・モニター・サービス(osysmond) クラスタ・ロガー・サービス(ologgerd) クラスタ・ヘルス・モニター[91]は、システム・モニター・サービス(osysmond)とクラスタ・ロガー・サービス(ologgerd)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 Interprocess Communication	該当なし
		7879	Jetty 管理サーバー	オラクルが自己署名
クラスタ・ノードは、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 エージェントにアクセスするには、ストレージ・インタフェースにアタッチされた IP/ポート 7060/7070 を使用します。	stib0/stre0	7060	dbcs-admin データベース・ライフサイクル操作を処理するためのクラウド・エージェント [92]	オラクルが自己署名
		7070	dbcs-agent データベース・ライフサイクル操作を処理するためのクラウド・エージェント [93]	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

[89] https://docs.oracle.com/en/database/oracle/oracle-database/19/cwadd/introduction-to-oracle-clusterware.html#GUID-7612C5C2-AC7C-4311-97B2-CF189268969A

[90] https://docs.oracle.com/en/database/oracle/oracle-database/19/rilin/port-numbers-and-protocols-of-oracle-components.html

[91] https://docs.oracle.com/en/database/oracle/oracle-database/19/atnms/understanding-cluster-health-monitor-services.html

[92] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-519A41E4-A97D-476E-B4BA-745C3486C779

[93] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-519A41E4-A97D-476E-B4BA-745C3486C779

コントロール・プレーン・サーバーから domU へ	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)[94]、Oracle Grid Infrastructure の一部 クラスタ同期サービス (CSS)、イベント管理 (EVM)、Oracle Notification Service (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、他のクラスタ・コンポーネント・レイヤーと通信します。	該当なし
		7879	Jetty 管理サーバー	オラクルが署名
		動的ポート: 9000-65500	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 Data Safe オンプレミス・コネクタ [95]	お客様が管理、またはオラクルが署名

VM コンソールへのアクセス

お客様は、トークンベースの ssh トンネルを使用してお客様の VM コンソールにアクセスできます。[96,97]サービスは、コントロール・プレーンを経由した、お客様の VM のハイパーバイザ・コンソールへのトンネルをコントロールします。これには 3 つの段階があります。

1. お客様の OCI IAM 資格証明により、コンソール接続が作成されます。その際、ssh プロキシ・トンネルをサポートするために、仮想マシンとコンテナがコントロール・プレーンにデプロイされます
2. お客様の ssh 資格証明により、ポート 443 のお客様デバイスから OCI エンドポイントへ、または OCI クラウド・シェルからの ssh 接続が作成されます。この接続により、OCI コントロール・プレーンを通じてお客様の VM コンソールにアクセスできるようになります
3. お客様のユーザー名とパスワード(通常は root ユーザー)を使用して、お客様の VM コンソールにログインします

ソフトウェアは、クラウド・シェルのコンソール接続を 24 時間後に自動的に終了します。コンソール接続を再度確立するには、OCI に対する認証を再度行う必要があります。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。

図 7 は、ポート 443 で OCI エンドポイントへの ssh 接続を行うためにコンソール接続を作成する、次のような手順を示しています。

1. お客様の OCI IAM ユーザーが、OCI クラウド・コンソールまたは API 経由で DBaaS コントロール・プレーンに接続し、VM コンソール接続の作成をリクエストします。API のペイロードには、コンソール・エンドポイントへの ssh セッションを確立するために使用される ssh 公開鍵を含みます

[94] https://docs.oracle.com/en/database/oracle/oracle-database/19/cwadd/introduction-to-oracle-clusterware.html
[95] https://docs.oracle.com/en/cloud/paas/data-safe/admds/create-oracle-data-safe-onpremises-connector1.html
[96] https://docs.oracle.com/en-us/iaas/releasenotes/changes/9cee8331-1a56-494c-9bcc-f0dab3eea1b4/
[97] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-manage-vm-clusters.html#GUID-34F8308B-480A-4DAE-A158-2B4856E41A90

2. お客様の OCI ユーザーが IAM ポリシーによって VM コンソール接続の作成を許可されているかどうかを OCI IAM が検証します
3. クラウド自動化ソフトウェアが、VM コンソールへの接続をサポートするターゲット・ソフトウェアにお客様の公開鍵を挿入します
4. ExaDB-C@C コントロール・プレーン・サーバー(CPS)が、お客様のデータ・センターから VM コンソールの ssh トンネルをサポートする OCI エンドポイントへの一時的なアウトバウンド接続を作成します

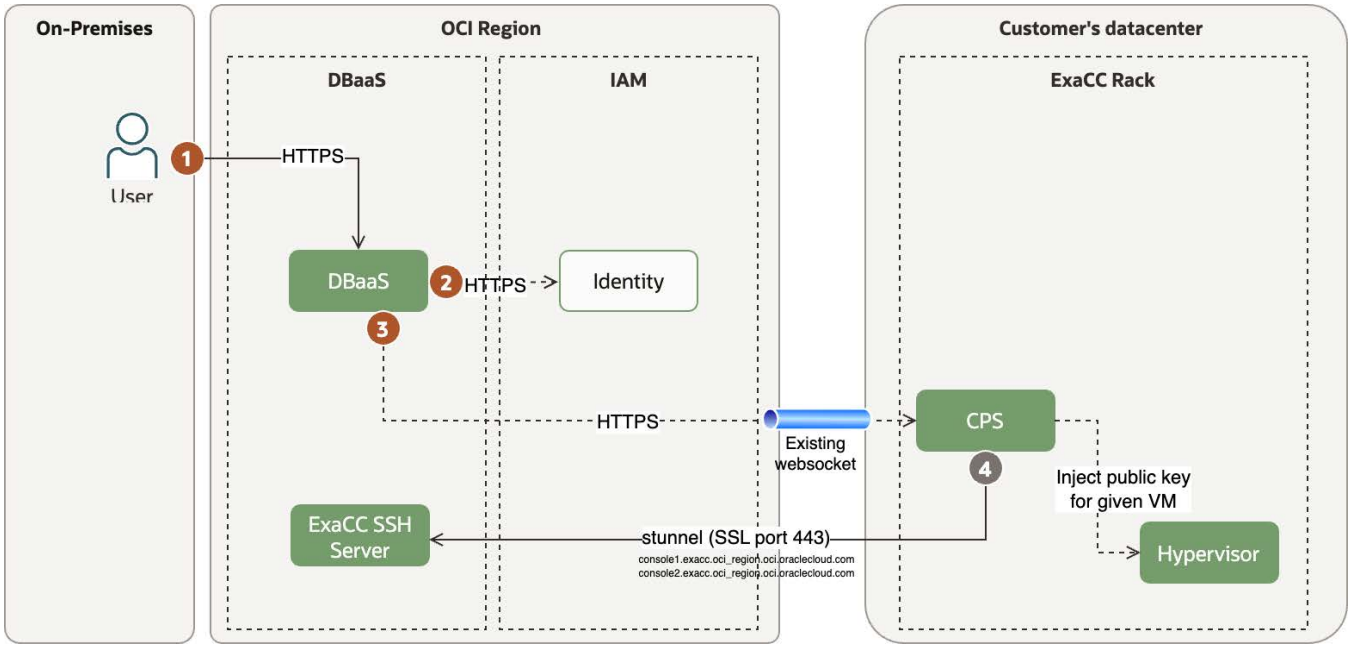

図 7: VM コンソールへの ssh トンネルを作成するワークフロー・ブロック図

図 8 は、お客様のデバイスから VM コンソールへの ssh 接続を確立する、次のような手順を示しています。

1. お客様が、OCI コンソールの API によって提供される ssh 接続文字列を使用して、ポート 443 で必要な OCI エンドポイントへの ssh 接続を開始します
2. 接続のユーザー名がリクエスト元ユーザーの IAM ユーザー名に関連付けられます
3. 接続の ssh ターゲットが ExaDB-C@C 仮想マシンに関連付けられます
4. ssh 接続に指定されたユーザー名が OCI ポリシーによってターゲット仮想マシンへの接続を許可されているかどうかを OCI IAM が検証します
5. ssh 接続が OCI コントロール・プレーンと一時的な ssh トンネルを通じて ExaDB-C@C CPS に転送されます
6. ssh 接続が CPS からハイパーバイザ上で実行されている仮想マシン・コンソールに転送されます

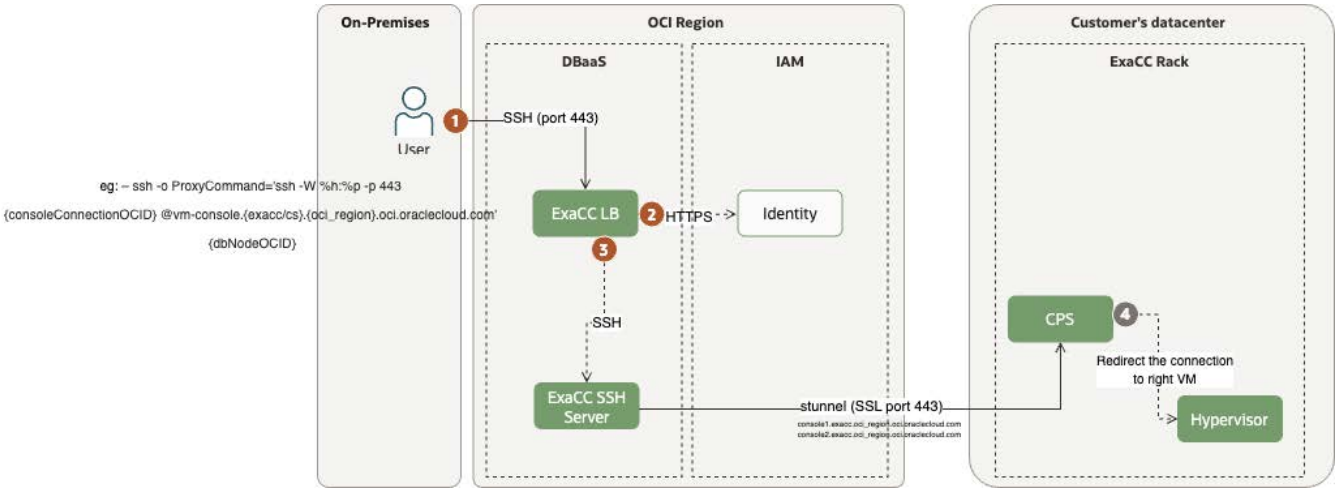

図 8: ポート 443 経由で OCI エンドポイントへの ssh 接続を確立するワークフロー・ブロック図

図 9 は、OCI クラウド・シェルを使用して VM コンソール接続を作成し、ssh 接続を確立する手順を示しています。このプロセスでは、ユーザーが提供する ssh 鍵ではなく、システム生成の保護された一時 ssh 鍵を次のように使用します。

1. お客様の OCI IAM ユーザーが、OCI クラウド・コンソールまたは API 経由で DBaaS コントロール・プレーンに接続し、OCI クラウド・シェル経由で VM コンソール接続の作成をリクエストします
2. ユーザーが OCI IAM ポリシーによって接続の作成を許可されているかどうかを OCI IAM が検証します
3. お客様の OCI IAM ユーザーがクラウド・シェル拡張機能を呼び出します
4. お客様の OCI ユーザーが OCI IAM ポリシーによって IAM 経由でのクラウド・シェルの使用を許可されているかどうかを OCI IAM が検証します
5. クラウド・シェルが ssh 鍵を作成し、DBaaS パブリック API を呼び出して、接続で使用される公開鍵を挿入します
6. CPS が公開鍵を挿入し、SSH 接続トンネルを作成します
7. CPS が ssh 接続を作成し、クラウド・シェルがシリアル・コンソールに接続します

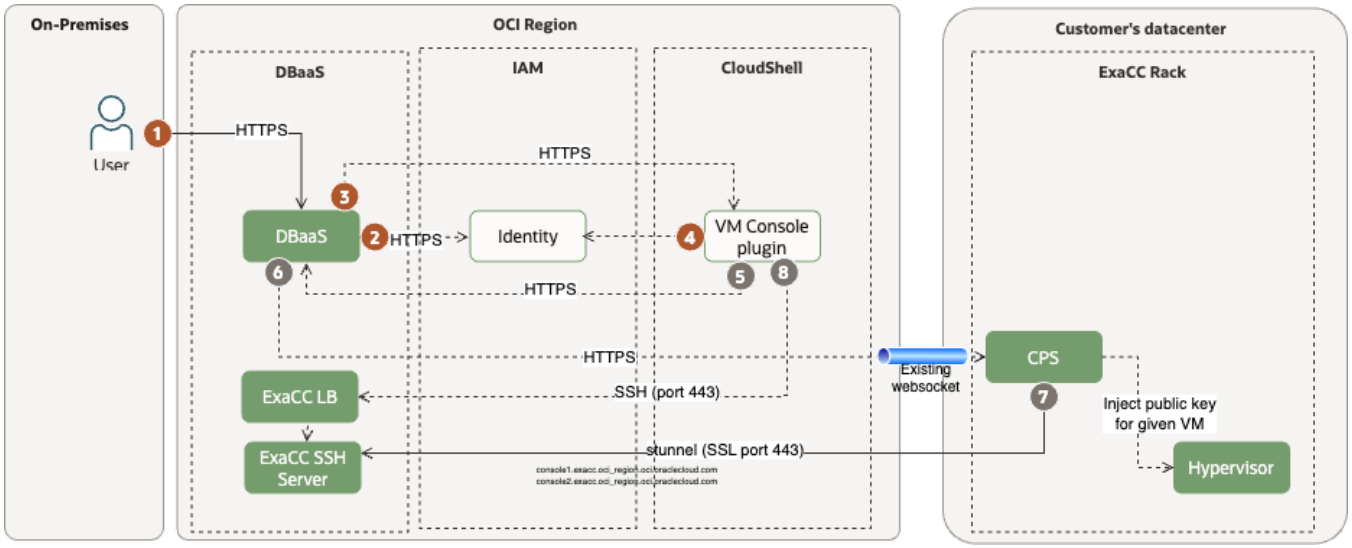

図 9: OCI クラウド・シェルを使用して VM コンソールへの ssh 接続を確立するワークフロー・ブロック図

図 10 は、VM コンソール接続を終了するワークフローを示しています

1. お客様の OCI IAM ユーザーが、OCI クラウド・コンソールまたは API 経由で DBaaS コントロール・プレーンに接続し、VM コンソール接続の終了をリクエストします
2. ユーザーが OCI IAM ポリシーによって接続の終了を許可されているかどうかを OCI IAM が検証します
3. 接続を終了する API がセキュア自動化トンネル(Web ソケット・サーバー)経由で CPS に送信されます
4. CPS が VM コンソールへの ssh 接続をサポートするセキュア・トンネルを終了します

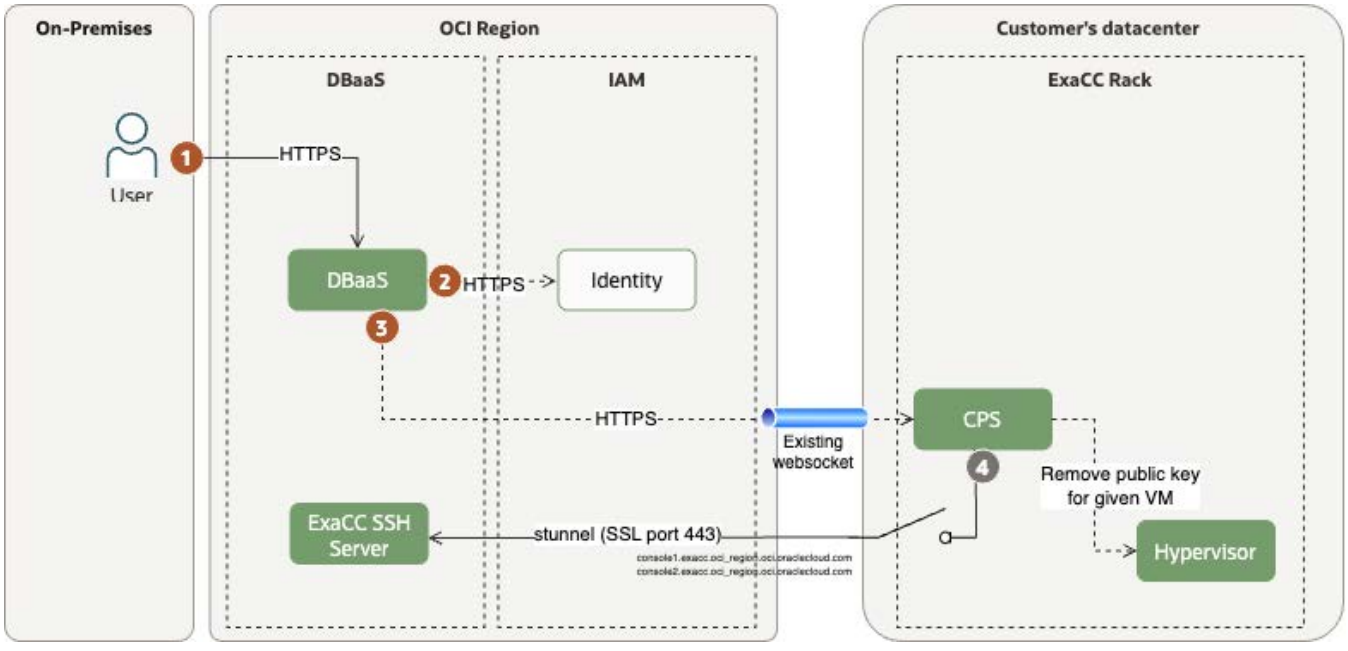

図 10: VM コンソールの ssh 接続を終了するワークフローのブロック図

API Access Control[98]で VM コンソール接続をコントロールして、VM コンソールへのアクセスを有効にしようとする OCI アイデンティティは別の OCI アイデンティティから承認を得なければならないようにすることができます。

VM へのクラウド自動化のアクセス

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 VM にアクセスします。

- ポート 443 での mTLS 認証を介して、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 を使用して、特権ユーザー(root、opc、grid、oracle)として VM にセキュアにログイン

Oracle クラウド自動化は、Exadata Database Server 管理ネットワーク上の NAT アドレスを介してお客様の VM にアクセスします。ソフトウェアは、管理アクションごとに一時的な一意の ssh 鍵ペアを生成します。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、VM で必要なサービス・アカウント(oracle、opc、grid、root など)の~/.ssh/authorized_keys ファイルに挿入されます。秘密鍵は、お客様のデータ・センターにある ExaDB-C@C ハードウェア上の暗号化ファイルに格納され、アクション完了後に破棄されます。クラウド自動化ソフトウェアは、アクションが完了すると、お客様 VM のサービス・アカウントから一時公開鍵を削除します。秘密鍵は、root アカウントが鍵にアクセスできるようにコントロールされます。

VM には、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 [99]が含まれています。コントロール・プレーンからの ssh へのアクセスをブロックすると、次のサービス機能が無効になります。

- データベースのソフトウェア・アップデート
- Grid Infrastructure のソフトウェア・アップデート
- VM オペレーティング・システムのソフトウェア・アップデート
- オラクルが管理するインフラストラクチャの四半期ソフトウェア・アップデート(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

OCPU のスケーリングは、VM への ssh アクセスを必要とせず、クラウド自動化がネットワーク・レイヤーでブロックされている場合でも引き続き機能します。

Delegate Access Control

Delegate Access Control[100]を使用すると、お客様の VM でデータベース・メンテナンス・サービスやサポート・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コントロールおよび監視することができます。お客様は、4 種類の Delegate Access Control 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 テクノロジを対象とするオラクルのカスタマ・サポート・サービス(追加料金なしで含まれる)
- Oracle Database Cloud Operation - VM にデプロイされたクラウド自動化ソフトウェアを対象とするオラクルのカスタマ・サポート・サービス(追加料金なしで含まれる)
- Oracle Engineered Systems Deployment and Infrastructure Support - Exadata Database Service のサブスクリプションとは別に交渉されるガイド付きパッチ適用およびトラブルシューティング・サービス
- Strategic Customers Program for DB Cloud Platforms - Exadata Database Service のサブスクリプションとは別に交渉されるカスタム・サポート・サービス

Delegate Access Control の予防的統制には、次のものがあります。

- オラクルのスタッフは、お客様が特定の作業リクエストを承認した後にのみアクセスします
- アクセスは、作業リクエストに関連する承認済のコンポーネントに限定されます
- アクセスはジャストインタイムの一時的なもので、所定の時間が過ぎると自動的に取り消されます
- お客様は、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タイミングをコントロールできます
- Oracle Linux の chroot jail[101]とその他のソフトウェアが権限の制限を適用します

Delegate Access Control の発見的統制には、次のものがあります。

---

[98] https://docs.oracle.com/en-us/iaas/oracle-api-access-control/index.html

[99] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-implement-sec.html#ol7-firewall-sec

[100] https://docs.oracle.com/en-us/iaas/delegate-access-control/doc/overview-of-delac.html

[101] https://docs.oracle.com/en/operating-systems/oracle-linux/8/security/security-ProtectingtheRootDirectoryUsingchrootJails.html#ol-harden-implement

- ソフトウェアは、オラクルのスタッフが VM にアクセスする必要がある場合に、お客様に通知します
- コマンドとキーストロークのログを個々のユーザーまでトレース可能になります

Delegate Access Control の対応的統制には、次のものがあります。

- ssh 接続と踏み台サーバーを終了します
- ssh 接続によって開始された Linux プロセスを終了します
- 一時的な資格証明を削除します

図 11 は、Delegate Access Control の承認およびアクセス・ワークフローを示しています。詳細は、Delegate Access Control のデモンストレーション・ビデオ [102]を参照してください。Delegate Access Control は、Operator Access Control[103]と同じ提供方法を使用し、Operator Access Control PCI-DSS Attestation of Compliance (AoC)の範囲に含まれています。

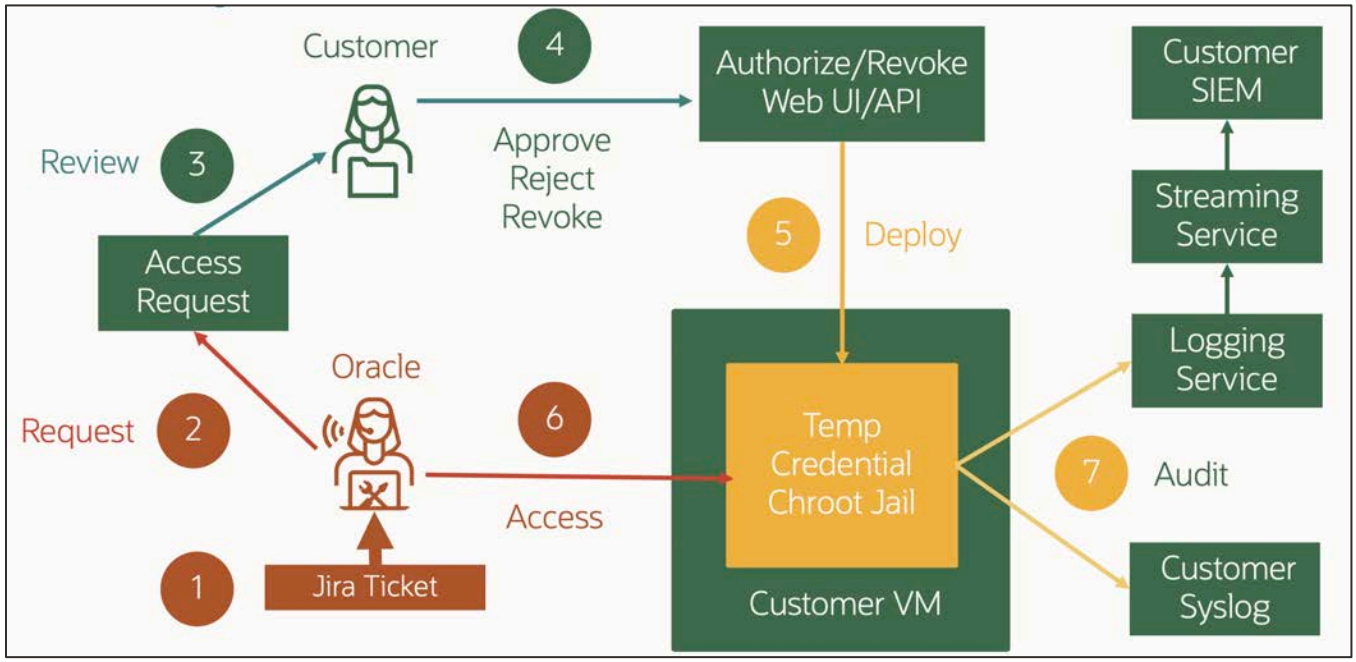

図 11: Delegate Access Control の承認ワークフロー

ネットワークのセキュリティ統制

お客様のネットワーク・セキュリティ統制を ExaDB-C@C のクライアント・ネットワークとバックアップ・ネットワークで使用できます。次のような統制により、ExaDB-C@C サービスが機能できるようにする必要があります。

- VM クラスタにおけるすべての VM 間の ICMP アクセス
- VM クラスタにおけるすべての VM 間の ssh
- 指定した管理ソースからの ssh インバウンド
- クライアントからデータベースへの SQLNet インバウンド
- DNS および NTP サーバーへのアウトバウンド DNS および NTP

OCI IAM を補完する追加の OCI セキュリティ・サービス

OCI は、ExaDB-C@C サービスとともに使用できるセキュリティ・サービスを提供しています。Network Sources と API Access Control を使用すると、認証と認可以外の特定の属性を適用して、OCI IAM を補完できます。Network Sources は、お客様のテナンシ・リソースに対する認証を、お客様が指定した IP アドレスおよび VCN から開始された接続に制限します。API Access Control は、API をターゲット・リソースに送信する前に、特権 API をインターセプトし、承認ワークフローに対してチェックします。

[102] https://www.youtube.com/watch?v=fwKtfp3aNuk

[103] https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/oracle-operator-access-control-tech-brief.pdf

Network Sources

OCI Network Sources[104]は、お客様のテナンシ・リソースに対する認証を、お客様の企業 VPN からのエグレスを許可するプロキシなど、特定の IP アドレスから開始された接続に制限します。お客様のデータ・センターから OCI リージョンへのサイト間 VPN や FastConnect を実装する場合は、OCI の転送用 VCN 経由で OCI コンソールと API の接続をルーティングできます。[105]これにより、Oracle サービスに対するオンプレミス・ネットワークのプライベート接続が可能になるため、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、トラフィックがパブリック・インターネットを通過することはなくなります。Network Sources は追加料金なしで含まれています。

API Access Control

API Access Control は、特権 OCI コンソールおよび API 機能のマルチアイデンティティ承認ワークフローを実行します。特権 API を呼び出すには、API を呼び出そうとするユーザーが自分の OCI アイデンティティでアクセス・リクエストを発行し、別の OCI アイデンティティがそのアクセス・リクエストを承認する必要があります。図 12 は、API Access Control の承認ワークフローを示しています。詳細は、API Access Control のデモンストレーション・ビデオ [106]と、Oracle Learning Center の API Access Control[107]を参照してください。API Access Control は追加料金なしで含まれています。

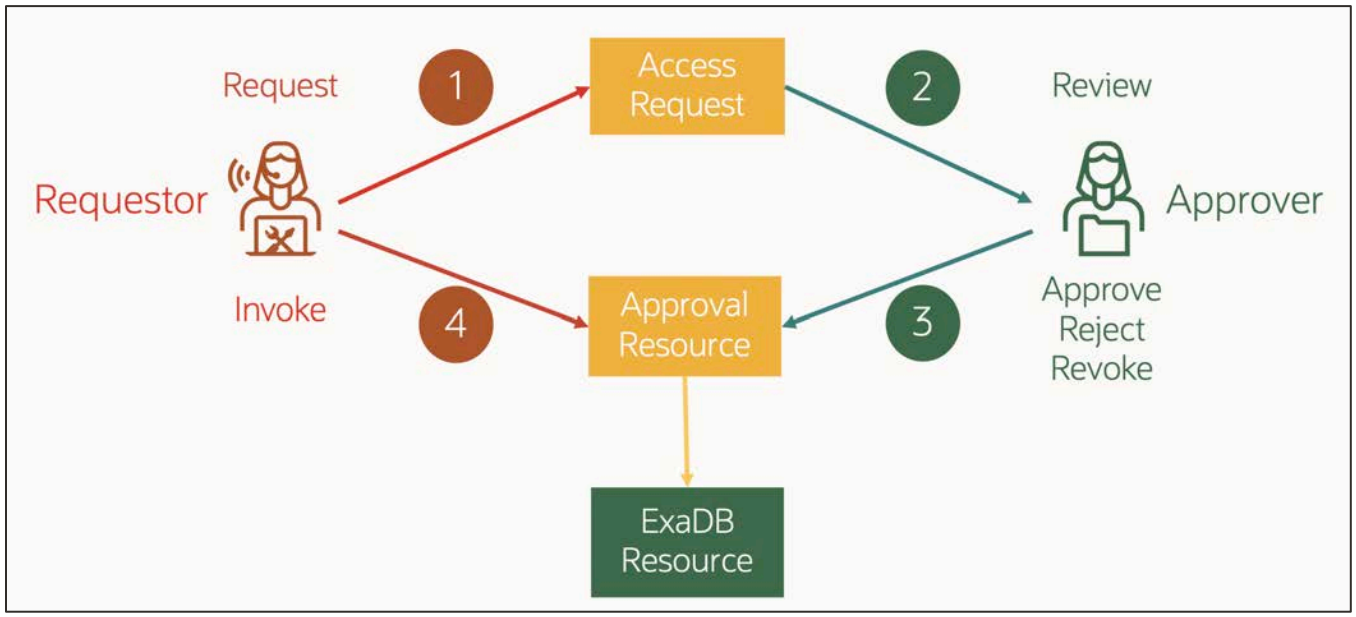

図 12: API Access Control の承認ワークフロー

インフラストラクチャ・コンポーネントに対するオラクルのアクセス制御

オラクルは、Oracle PaaS and IaaS ドキュメント [108]に記載されているように、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ます。オラクルの企業セキュリティ慣行 [109]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います。これらは、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 27002:2022 (旧 ISO/IEC 17799:2005)規格と ISO/IEC 27001:2022 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。オラクルは、自動化された人材採用プロセス、人事異動プロセス、退職プロセスを実装することで、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ています。オラクルは、Oracle Cloud Operations のアクセスを、オラクルのアクセス制御プラクティス [110]に従い、最小権限によるデフォルト拒否アプローチでさらに制御します。このアプローチでは、次のことを考慮してアクセスが提供されます。

- 知る必要性のあるユーザー

[104] https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingnetworksources.htm
[105] https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/transitroutingoracleservices.htm
[106] https://www.youtube.com/watch?v=-kzyH4LzP3c&feature=youtu.be
[107] https://docs.oracle.com/en/learn/exadb-cc-api-access-control/
[108] https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf
[109] https://www.oracle.com/corporate/security-practices/corporate/
[110] https://www.oracle.com/corporate/security-practices/corporate/access-control.html

- 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 ExaDB-C@C Cloud Operations のスタッフは、Exadata Database Service 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を与えられています。これには次の機器が含まれます。

- 配電ユニット(PDU)
- アウト・オブ・バンド(OOB)管理スイッチ
- ストレージ・ネットワーク・スイッチ
- Exadata Storage Servers
- 物理的な Exadata Database Server

オラクルは、ExaDB-C@C インフラストラクチャへの Oracle Cloud Ops スタッフのアクセスを次の方法で制御します。

OCNA へのアクセス:

- ジョブ・コードに基づいて資格を付与
- FIPS 140-2 レベル 3 のハードウェア MFA を使用して認証
- ユーザー・デバイスが OCNA に接続するには、セキュリティ・スキャンに合格する必要があります。

踏み台サーバーへのアクセス:

- Exadata Database Service インフラストラクチャへの ssh アクセスは、踏み台サーバーと管理サーバーを経由します。
- 管理サーバーへのアクセスは踏み台サーバーをトンネルし、サービスをホストしているリージョンの特権管理 VCN に分離されます。
- 踏み台接続はすべてログに記録され、監視されます。

管理サーバーへのアクセス:

- スタッフは、FIPS 140-2 レベル 3 のハードウェア MFA を使用して、ssh で名前付きユーザーとしてログインします。
- アクセスは最小権限ポリシーに従って制御されます。
- 管理サーバーへのアクセスはすべてログに記録され、監視されます。

Exadata Database Service インフラストラクチャへのアクセス:

- スタッフは、トークンベースの ssh を使用して、サービス・アカウントに対して認証を行います。
- コマンドの実行は、名前付きユーザーまで監査およびトレース可能です。
- インフラストラクチャへの接続はすべてログに記録され、監視されます。

図 13 は、Oracle Cloud Operations (Cloud Ops)のスタッフが ExaDB-C@C 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。お客様は、Operator Access Control[111]を使用して、オラクルのスタッフが ExaDB-C@C インフラストラクチャおよび ADB-D VM へのシェル・アクセスを取得するタイミングをコントロールできます。

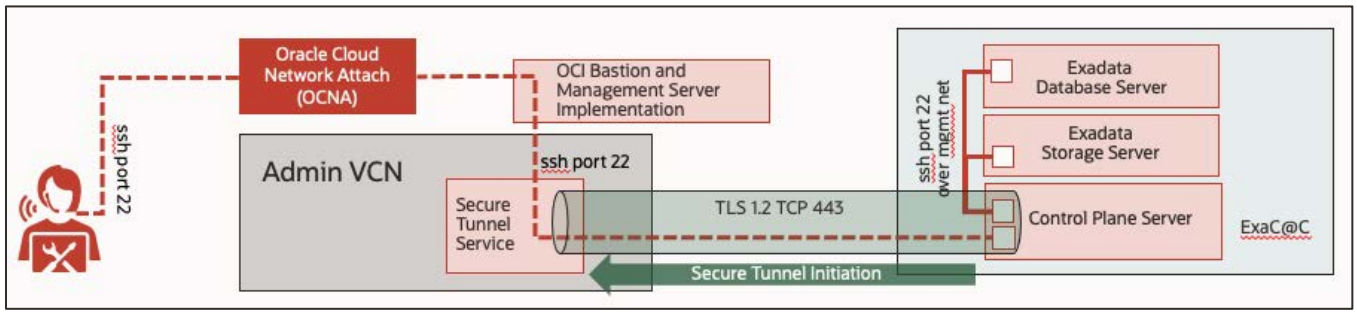

図 13: ExaDB-C@C インフラストラクチャ・コンポーネントへの Cloud Operations スタッフのアクセス

Oracle Operator Access Control

ミッション・クリティカルで高度に規制されたワークロードをサポートするアプリケーション群をクラウド・プラットフォームに移行する上で影響が現れるのが、クラウド・プラットフォームに固有の責任共有モデルです。このモデルでは、クラウド・サービス・プロバイダは、インフラストラクチャ(クラウド・プロバイダ・テナンシ)などのシステムのサブセットを管理するためのコントロールを保持し、サブスクライバは、仮想マシン、アプリケーション、データベース(お客様テナンシ)などのシステムの別の部分を管理するコントロールを保持します。ミッション・クリティカルで規制の厳しいワークロードの場合、クラウド・プロバイダ・インフラストラクチャ内のクラウド・プロバイダ・スタッフによるアクションなど、システムの任意の部分にアクセスするときに実行するアクション

[111] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html

をコントロールする責任をサブスクライバが負うことがあります。これらの要件を満たすために、お客様は、ExaDB-C@C と ExaDB-C@C 上の Autonomous Database Dedicated (ADB-D)で Oracle Operator Access Control[112]を使用できます。Operator Access Control は、たとえば銀行や金融サービスのアプリケーション、エネルギーなどの公益事業や防衛、およびリスク管理がアプリケーションの成功の重要な鍵となるような、その他のアプリケーションに最適です。

Operator Access Control は、OCI の特権アクセス管理(PAM)サービスです。Operator Access Control は、次のようなインタフェースを提供します。

- オラクルの担当者が ExaDB-C@C インフラストラクチャおよび ADB-D VM に必要なアクセスのタイミングと量をコントロールすることができます
- オラクルの担当者が ExaDB-C@C インフラストラクチャ上で実行するオラクルのオペレータ・コマンドおよびキーストロークを確認して記録することができます
- お客様の裁量でオラクルのオペレータ接続を終了することができます

これらのコントロールは ExaDB-C@C 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。Operator Access Control の予防的統制には、次のものがあります。

- オラクルの担当者は、お客様が承認した場合にかぎり、特定の Oracle 作業リクエストにのみアクセスします
- オラクルの担当者のアクセスは、規定および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ます
- オラクルの担当者のアクセスは一時的なものであり、認可されたタスクが完了するかタイムアウトに達すると自動的に取り消されます
- お客様は、オラクルの担当者がインフラストラクチャにアクセスするタイミングをコントロールできます
- ソフトウェアによる権限レベルの適用

Operator Access Control の発見的統制には、次のものがあります。

- オラクルの担当者がインフラストラクチャにアクセスする必要がある場合に、ソフトウェアによってお客様に通知します
- オラクルの担当者が実行するアクションに関するコマンドおよびキーストロークのロギング
- コマンドとキーストロークを個々のユーザーまでトレース可能
- お客様は、オラクルの担当者が入力したすべてのコマンドとキーストロークを監視できます
- コマンド実行において必要な場合、オラクルから提供されたオラクル担当者のアイデンティティの記録

Operator Access Control の対応的統制には、次のものがあります。

- お客様は、オラクルの担当者のアクセスを停止させることができます
- オラクルの担当者が開始したプロセスをソフトウェアによって終了させます
- ExaDB-C@C インフラストラクチャと ADB-D VM からリモート・アクセス可能なアカウントをソフトウェアによって削除します

お客様は、ExaDB-C@C サービスをサポートするために、オラクルの Operator Access Control アクセス・リクエスト・イベント[113]に対する継続的な監視(24 時間 365 日)と対応を確保するよう計画する必要があります。お客様は、Operator Access Control アクセス・リクエストを処理する目的で、OCI Events[114]サービスと Notifications[115]サービスを使用して、お客様のスタッフに通知するプロセスを自動化することを検討する必要があります。ServiceNow でこれを行う方法の例については、『Simple Guide to Managing OCI Alarms in ServiceNow』[116]を参照してください。継続的な監視を確保できない場合や、お客様に代わってアクセス・リクエストを自動的に承認するソフトウェアでお客様の要件を満たすことができる場合は、Operator Access Control の事前承認機能を使用できます。[117]事前承認を使用すれば、一時的なジャストインタイム・アクセスとコマンドおよびキーストロークの完全な監査ログのメリットをすべて享受でき、お客様のスタッフが OCI にアクセスしてアクセス・リクエストを承認する必要もありません。これにより、運用上の負担が軽減されるとともに、問題解決に時間がかかり、より複雑な問題やサービスの停止に発展するリスクが低下します。お客様は、あらかじめ構成したメンテナンス期間に対して事前承認を構成することで、ソフトウェア・アップデートを最適化できます。低レベルのアクセス権限を選択的に事前承認し、高レベルのアクセス権限については明示的な承認を必須にすることが可能です。[118]

---

[112] https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/oracle-operator-access-control-tech-brief.pdf

[113] https://docs.oracle.com/en-us/iaas/operator-access-control/doc/auditing-operator-access-control-lifecycle-events.html#GUID-1C819283-0660-4828-8E11-09D897211436

[114] https://docs.oracle.com/en-us/iaas/Content/Events/Concepts/eventsoverview.htm

[115] https://docs.oracle.com/en-us/iaas/Content/Events/Concepts/eventsoverview.htm

[116] https://www.ateam-oracle.com/post/a-simple-guide-to-managing-oci-alarms-in-servicenow

[117] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-49AE3FAF-95E3-4D7D-B950-9FC52C4B5FA9

[118] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-533A688A-FC75-43A8-B7DF-6481D781C872

お客様は、Operator Access Control 監査ログを互換性のあるサードパーティの性ソフトウェア製品に統合できます。これには、お客様の syslog サーバー[119]への監査ログの送信や、OCI Logging サービスと Splunk の統合 [120]が含まれます。詳細は、Operator Access Control[121]の製品ドキュメント、Operator Access Control の技術概要 [122]、および Operator Access Control Request and Audit Processing[123]ビデオを参照してください。

ソフトウェア開発および提供のセキュリティ統制

ExaDB-C@C は、Exadata Database Machine[124]のエンタープライズクラスのセキュリティ機能をクラウド・サービスとして提供します。ExaDB-C@C のソフトウェア・セキュリティには次のものがあります。

- ソフトウェア開発は、Oracle Software Security Assurance[125]のプラクティスに従って行われます
- セキュリティ・アーキテクチャは、Oracle Corporate Security Architecture[126]のプラクティスに従って実行されます
- 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-C@C インフラストラクチャにインストールされません

ソフトウェア・アップデートは、改ざんを防止するために、OCI から ExaDB-C@C インフラストラクチャへの送信前に署名され、暗号化されます。

発見的統制

ExaDB-C@C 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。サービスでは、監視に関する職務が次のように分掌されます。

- 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、監視します
- オラクルは、オラクルが管理するインフラストラクチャのロギング構成をコントロールし、監視します

オラクルには、お客様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インフラストラクチャ監査ログ情報へのアクセスをリクエストできます。お客様の監査権は Oracle Data Processing Agreement (DPA)[127]に記載されています。

お客様のサービスの監査ロギング

ExaDB-C@C は、監査とロギングのために 4 つの機能を提供します。

- OCI Audit: お客様の資格証明によって開始されたコントロール・プレーン・アクションのログ
- Oracle Database 監査: お客様の Oracle Database 資格証明によって開始されたデータベース・アクションの監査ログ
- VM オペレーティング・システム監査ログ: お客様のオペレーティング・システム資格証明によって VM で開始されたアクションの監査ログ
- Automated Intrusion Detection Environment (AIDE): ファイルの整合性監視用

お客様は、これらの監査ログを互換性のあるテクノロジに送信できます。実装の詳細は、「Ingest Oracle Cloud Infrastructure Logs into Third-Party SIEM Platforms using Log Shippers」[128]を参照してください。

OCI の監査ロギング

OCI Audit[129]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。すべてのサービスが Audit によるロギン

---

119 https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-6526ADE1-C664-4600-A62B-5993EA25134E
120 https://docs.oracle.com/en/solutions/logs-stream-splunk/index.html
121 https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-7CF13993-DB16-485A-A9FA-399E0049740B
122 https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/oracle-operator-access-control-tech-brief.pdf
123 https://www.youtube.com/watch?v=ZCLMs_kgSr4
124 https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/toc.htm
125 https://www.oracle.com/corporate/security-practices/assurance/
126 https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
127 https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
128 https://docs.oracle.com/en/learn/ocilogs-log-shipper/index.html#introduction
129 https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm

グをサポートしています。Oracle Object Storage サービスでは、バケット関連のイベントのロギングはサポートされますが、オブジェクト関連のイベントのロギングはサポートされません。Audit 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 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。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格納されます。

データベースの監査ロギング

ExaDB-C@C は、Oracle Database Unified Audit[130]を使用して、データベースの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、お客様の syslog サーバー[131]、または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。例については、SIEM へのストリーミングに関する OCI ソリューション・プレイブック [132]を参照してください。オラクルは、Oracle Database 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を各データベース・バージョンの『Oracle Database セキュリティ・ガイド』[133]で公開しています。

VM の監査ロギング

Oracle Linux 監査ログサービス(`auditd`)[134]は、オペレーティング・システム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、リモート・ログ・サーバーへの Oracle Linux 監査ログの送信も含め、自社の標準に従って `auditd` を構成できます。[135]詳細は、『Oracle Linux セキュリティ・ガイド』[136]を参照してください。お客様は、Oracle Linux 監査ログを OCI Log Analytics サービスに統合できます。[137]

ファイルの整合性監視

Exadata Database Service には、ファイルとディレクトリの整合性をチェックするための Oracle Linux Advanced Intrusion Detection Environment (AIDE)[138, 139]が含まれています。AIDE は、Linux OS で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。システムの内部的な保護を目的として、ウィルス、ルートキット、マルウェアから保護するレイヤーおよび権限のないアクティビティの検出を提供しています。これは、簡易クライアント/サーバー監視構成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、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)。この構成は`/etc/aide.conf` で変更できます。構成ファイルは、どのファイルとディレクトリを AIDE で監視するか、ロギングと出力をどのように処理するかをコントロールします。

Oracle インフラストラクチャの監査ロギング

オラクルは、インフラストラクチャ監査ログを記録、分析して対応する責任を負います。Exadata Database Service 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次のものがあります。

ILOM:

- syslog

---

130 https://www.oracle.com/database/technologies/security/db-auditing.html
131 https://support.oracle.com/knowledge/Oracle Cloud/2652319_1.html
132 https://docs.oracle.com/en/solutions/oci-aggregate-logs-siem/#GUID-601E052A-8A8E-466B-A8A8-2BBBD3B80B6D
133 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。
134 https://docs.oracle.com/en/learn/ol-auditd/
135 https://support.oracle.com/knowledge/Oracle%20Cloud/2652319_1.html
136 https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-audit-sec.html
137 https://blogs.oracle.com/ateam/post/harnessing-the-power-of-linux-logs-in-oci-logging-analytics-om
138 https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmso/aide.html
139 https://support.oracle.com/knowledge/Oracle%20Linux%20and%20Virtualization/2616282_1.html

- 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`

Exadata Database Service X8M 以降のハードウェアの監査ログには次のものがあります。

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

オラクルの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 年です。[140]インフラストラクチャ監査ログは、オラクルのセキュリティ・スタッフがアクセスできます。

対応的統制

お客様とオラクルは連携して ExaDB-C@C コンポーネント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、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は、Oracle Service Request (SR)プロセスを使用して、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。

お客様は、自身がコントロールするあらゆるサービスまたは機器に対して、あらゆる対応策を講じることができます。対応策として、Operator Access Control と Delegate Access Control のアクセス・リクエストや、お客様の VM へのネットワーク接続、CPS と OCI リソースの間のネットワーク接続を強制終了することもできます。CPS と OCI の間の接続を強制終了した場合も、お客様のデータベースは引き続き正常に機能します。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強制終了、オラクルが管理する ExaDB-C@C インフラストラクチャに対するアクセス権の取消し、OCI コントロール・プレーンからの ExaDB-C@C インフラストラクチャの切断などが含まれます。

オラクルのインシデント対応

オラクルのインシデント対応 [141]では、オラクルがセキュリティ・インシデントに対応する方法を次のように説明しています。

「オラクルが実施している、セキュリティイベント（インシデントも含む）への対応体制についてご確認ください。セキュリティインシデントとは、オラクルの社内システムおよび Oracle Cloud にホストされたデータの機密性、完全性、可用性に影響を及ぼす可能性のある、偶発的または意図的なあらゆる事象を指します。

[140] https://www.oracle.com/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf

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

Global Information Security はさらに、各 LoB におけるインシデント対応チームの役割と責任を明確に定義しています。すべての LoB は、情報セキュリティイベントの管理および迅速な是正措置の実施において、Global Information Security が定めるガイドラインに従う必要があります。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[142]では、クリティカルな問題(セキュリティ・インシデントを含む)に対するオラクルの 15 分のサービス対応時間について、次のように説明しています。

「5.3.1 重要度 1（クリティカルな停止）

オラクル・クラウド・サービスのお客様による本番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なまたは際限のない遅延が発生*
- *サービスがクラッシュし、何度か再起動を試みた後もクラッシュする状態が継続*
- *サービスの機密性、完全性または可用性に影響を及ぼす可能性のあるセキュリティー・インシデント*

オラクルは、重要度 1 のサービス・リクエストについては 15 分以内に応答するよう合理的な努力をします。重要度 1 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。」

カスタマイズとサードパーティ・ソフトウェア

ExaDB-C@C は、お客様に対し、お客様の環境への特権アクセスを提供します。提供されるアクセスには、ゲスト・オペレーティング・システムへの root アクセスと、Oracle Database への SYSDBA アクセスが含まれます。このレベルの統制により、お客様は構成の変更やサードパーティ・ソフトウェアのインストールを行うことができます。このような変更や追加は、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を引き起こす可能性があります。

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、認証、およびエラー解決などが含まれます。カスタム/サード・パーティのソフトウェアのテクニカル・サポートについては、そのソフトウェアの供給者が責任を負うものとします。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推奨されます。Exadata Database Service 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 ドキュメント「Installing Third Party Software On Exadata Components (Doc ID 1593827.1)」[143]で公開されています。

問題が発生した場合は、Oracle Service Request (SR)プロセスを通じて、Oracle サポートが問題を診断します。問題によっては、変更を元に戻すようにお薦め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場合には、標準のサポート・ポリ

[142] https://www.oracle.com/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf

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

シーに従って、サードパーティ・コンポーネントなしで問題を再現するようお願いすることがあります。[144] Oracle 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追加料金なしで含まれています。

サービスは提供された状態で使用することをお薦めします。Exadata Database Service の設計には、Oracle Corporate Security Architecture[145]と Oracle Software Security Assurance[146]による監督が組み込まれています。所定のサービス設計に従うことで、変更のテスト、検証およびトラブルシューティングを広範囲に行う必要性を軽減できます。

商用リファレンス情報

この項には、ExaDB-C@C のセキュリティについてよくある質問に関連してオラクルが公開している商用コンテンツがまとめられています。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、商業契約に関するドキュメントのインデックスについては、Oracle Trust Center[147]を参照してください。

コンプライアンス

オラクルは、オラクルの事業部門が 1 つ以上のサービスに関して、サードパーティによる認証または認定資格を取得したフレームワークに関する情報を、「アテステーション」という形で提供しています。これらのアテステーションは、コンプライアンスとレポートをサポートし、該当する Oracle クラウド・サービスのセキュリティ、プライバシおよびコンプライアンスのコントロールを個別に評価できます。これら第三者のアテステーションを検討する際には、一般的に特定のクラウドサービスに特化していること、また、特定のデータ・センターや地域に特化している可能性があることを考慮することが重要となります。https://www.oracle.com/cloud/compliance/#attestations にアクセスすると、特定の規格の関連する詳細情報を確認できます。この情報は現時点のものですが、変更される可能性があり、頻繁に更新される可能性があり、保証をするものではありません。かつ、契約には組み込まれていないことに注意してください。

ExaDB-C@C は、次の一般的な規格に準拠して運用されます。

- ISO 27001
- System and Organization Controls 1 (SOC 1)
- System and Organization Controls 2 (SOC 2)
- System and Organization Controls 3 (SOC 3)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)

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。[148]お客様が OCI サービスを利用して EU 一般データ保護規則(GDPR)の要件を満たせるよう、オラクルは Oracle Cloud Infrastructure and GDPR[149]ペーパーを発行しています。

オラクルの企業セキュリティ・ポリシー

オラクルの企業セキュリティ慣行 [150]は、オラクルとお客様のデータの機密性、完全性、可用性の保護を支援します。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 27002:2022 (旧 ISO/IEC 17799:2005)および ISO/IEC 27001:2022 の各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。これらの慣行には以下が含まれます。

- 目的 [151]
- 人事のセキュリティ [152]
- アクセス制御 [153]
- ネットワーク通信のセキュリティ [154]

---

144 https://support.oracle.com/knowledge/Oracle%20Cloud/1593827_1.html
145 https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
146 https://www.oracle.com/corporate/security-practices/assurance/
147 https://www.oracle.com/trust/
148 https://docs.oracle.com/en-us/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm
149 https://docs.oracle.com/en-us/iaas/Content/Resources/Assets/whitepapers/oci-gdpr.pdf
150 https://www.oracle.com/corporate/security-practices/corporate/
151 https://www.oracle.com/corporate/security-practices/corporate/objectives.html
152 https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
153 https://www.oracle.com/corporate/security-practices/corporate/access-control.html
154 https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html

- データのセキュリティ [155]
- ラップトップおよびモバイル・デバイスのセキュリティ [156]
- 物理的・環境的セキュリティ [157]
- サプライ・チェーンのセキュリティと保証 [158]

脆弱性の開示

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、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。[159]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。オラクルは、Oracle 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』[160]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-C@C 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。

Oracle Data Processing Agreement

Oracle Data Processing Agreement for Oracle Services[161]は、オラクルがデータを制御、保護、および処理する方法を説明するもので、以下が含まれます。

- 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

ExaDB-C@C の一環として、お客様は、オラクルが Data Processing Agreement に基づく義務を遵守していることを、年に 1 回を限度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って要求される範囲において、お客様またはお客様の規制当局は、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[162]では、お客様のデータが Oracle Cloud Services でどのように処理されるかを次のように説明しています。

- 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

Cloud Services Agreement の重要な情報を次に示します。

---

155 https://www.oracle.com/corporate/security-practices/corporate/data-protection/
156 https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
157 https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
158 https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
159 https://www.oracle.com/corporate/security-practices/assurance/vulnerability/disclosure.html
160 https://www.oracle.com/security-alerts/#CVEOtherDocs
161 https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
162 https://www.oracle.com/contracts/cloud-services/

「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、該当の手続面、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/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（上記(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」[163]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目的で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フィードされなければなりません。セキュリティログへのアクセスは、最小権限の原則に基づき、それを知る必要がある人にのみ付与されます。可能な場合、ログファイルは他のセキュリティ統制に加えて強力な暗号化によって保護され、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)[164]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次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）に必要に応じて通知します。

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。

---

[163] https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html

[164] https://www.oracle.com/a/ocom/docs/oci-corporate-caiq.pdf

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[165]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、次のように説明しています。

「1.14 セキュリティー・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ー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ー活動、情報またはプログラムへのアクセス、アラートなどのシステム・イベント、コンソール・メッセージおよびシステム・エラーをログとして記録するように設定されています。オラクルは、セキュリティー・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ーは、セキュリティー・イベント管理手順の対象となります。セキュリティー・ログは、ネイティブ形式かつ変更なしの形式にて Security Information and Event Management システム（またはそれに相当するシステム）内に保存されたうえでオラクルの内部ポリシーに基づき保持されます。セキュリティー・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ー業務のためにオラクルにより保持および利用されます。」

99.95%の月次稼働時間サービス・レベル・アグリーメント(SLA)

Oracle PaaS and IaaS Public Cloud Services Pillar Document[166]では、提供された Oracle サービスの稼働時間率が 99.95%に達しなかった場合の Oracle サービス・クレジットの修正について、次のように説明しています。

「可用性サービス・レベル・アグリーメント このサブ項目の可用性サービス・レベル・アグリーメント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、どのカレンダー月においても、かかるサービスのそれぞれを 99.95%以上の月次稼働時間率(定義は後述)で使用可能な状態に維持するよう、商業的に合理的な努力をします(以下、「サービス・コミットメント」といいます)。該当する上記のクラウド・サービスが、このサブ項目の可用性サービス・レベル・アグリーメントに対するサービス・コミットメントを満たさない場合、お客様はかかる非準拠のサービスに対してサービス・クレジットを受け取る権利を得ます。その際のサービス・クレジット率は次のように決定されます。

月次稼働時間率: *サービス・クレジット率*

- *99.0%以上 99.95%未満:* *10%*
- *95.0%以上 99.0%未満:* *25%*
- *95.0%未満:* *100%」*

サービス終了後の 60 日のアクセス期間

Oracle Cloud Hosting and Delivery Policies[167]では、サービス終了後の 60 日のアクセス期間(お客様がサービスからお客様データを取得できる期間)について、次のように説明しています。

「6.1 オラクル・クラウド・サービスの終了

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

---

165 https://www.oracle.com/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf

166 https://www.oracle.com/contracts/docs/paas_iaas_pub_cld_srvs_pillar_4021422.pdf

167 https://www.oracle.com/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf

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-C@C サービスのサポートには、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 VM にアクセスする必要があるような例外的なケースも含まれます。オラクルのスタッフがお客様の VM にアクセスする方法を決定するプロセスと技術的な統制は、お客様が VM にアクセスできるかどうかによって異なります。これらのケースに対応するプロセスと技術的な統制について、この後の項で説明します。

VM が Delegate Access Control で制御されている場合

お客様が Delegate Access Control[168]を実装し、Oracle Cloud Customer Support と Oracle Cloud Operation をサブスクライブしている場合、Oracle Database クラウド・サポートまたは Oracle Cloud Operations のサポート・スタッフは、Delegate Access Control アクセス・リクエストをお客様に対して発行します。お客様が承認すると、Oracle サポート・スタッフは、一意の一時的なジャストインタイム資格証明を使用して VM にアクセスします。この資格証明は、Linux chroot jail に実装されている最小権限アクセス用にデプロイされたものです。Oracle Linux 監査サービスは、OCI Logging サービスを介して、コマンド/キーストロークのログをお客様に提供します。お客様は、オプションで、Oracle Linux 監査ログをお客様の syslog サーバーに送信できます。

お客様 VM にお客様がアクセスできる場合

お客様 VM にお客様がアクセスできる場合、リモート・コラボレーション・テクノロジ(Zoom、Webex、Skype など)を使用して、お客様 VM へのアクセスをオラクルの担当者と共有できます。このアクセスは、SR プロセスによって次のようにコントロールされます。

- お客様は、障害を示すサービス・リクエスト(SR)をオープンします
- お客様またはオラクルは共有セッションを開き、SR でセッション情報を示します
- お客様とオラクルの担当者は、SR から共有セッション情報にアクセスします
- お客様は、お客様の資格情報を使用して VM にアクセスします
- オラクルの担当者の指示に従って、問題を解決するためのコマンドをお客様が入力するか、オラクルの担当者が VM セッションのキーボード入力をコントロールすることを許可します
- お客様は、診断情報をもとに SR を更新します
- オラクルの担当者は、SR に解決情報を記載し、更新します

リモート・ログイン経由で VM にアクセスできない場合

お客様がお客様 VM にアクセスできないか、インフラストラクチャ・ネットワークからのリモート・ログイン経由で VM にアクセスできない場合(VM がクラッシュした場合など)、特定のプロセスと技術的コントロールにより、オラクルの担当者がインフラストラクチャからお客様 VM にアクセスすることが許可されます。このアクセスは、Oracle Service Request (SR)プロセスと Operator Access Control(実装されている場合)を通じて、お客様とオラクルが次のようにコントロールします。

- Oracle Cloud Ops が直接の監督なしにお客様 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:
    - 「SR granting Oracle explicit permission to access a Guest VM of ExaCC with VM Name <*「DB サーバー詳細」ページ→「リソース」→「仮想マシン」にリストされているとおりに VM 名を記入*>」
  - SR の内容:
    - We are opening this SR to grant explicit permission to Oracle to access our Guest VM in order for support to help resolve the issue described in SR# 1-xxxxxxxx.We acknowledge that by providing this permission, we understand that Oracle will have access to all files and memory that are part of the Guest VM.In addition, we also agree that the customer security team has authorized Oracle to have access to the customer Guest VM in order to resolve the issue described in the above SR.
    - DB サーバーの OCID: <*ここに VM をホストしている DB サーバーの OCID を記入*>
    - VM 名: <*「DB サーバー詳細」ページ→「リソース」→「仮想マシン」にリストされているとおりに VM 名を記入*>
- Oracle Cloud Ops によるアクセスを直接監督できるよう、オラクルに画面の共有を求める場合、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:
    - 「SR granting Oracle explicit permission to access a Guest VM of ExaCC with VM Name <*「DB サーバー詳細」ページ→「リソース」→「仮想マシン」にリストされているとおりに VM 名を記入*>」
  - SR の内容:
    - We are opening this SR to grant explicit permission to Oracle to access our Guest VM in a shared screen session in order for support to help resolve the issue described in SR# 1-xxxxxxxx.We acknowledge that by providing this permission, we understand that Oracle will have access to all files and memory that are part of the Guest

[168] https://docs.oracle.com/en-us/iaas/delegate-access-control/doc/overview-of-delac.html

VM. This permission to access our VM is contingent on our representative being able to monitor in real-time via a screen-sharing session all activities performed by Oracle. In addition, we also agree that the customer security team has authorized Oracle to have access to the customer Guest VM via this shared screen session in order to resolve the issue described in the above SR.

- DB サーバーの OCID: *<ここに VM をホストしている DB サーバーの OCID を記入>*
- VM 名: *<「DB サーバー詳細」ページ→「リソース」→「仮想マシン」にリストされているとおりに VM 名を記入>*

- Operator Access Control が実装されている場合、オラクルは問題を解決するために Operator Access Control アクセス・リクエストをオープンします。お客様は Operator Access Control アクセス・リクエストを承認して、オラクルのスタッフに適切なシステム・コンポーネントへのアクセスを許可する必要があります。
- Operator Access Control では、お客様の syslog サーバーまたはお客様のテナンシの OCI Logging サービス(あるいはその両方)に、コマンドやキーストロークがほぼリアル・タイム(60 秒未満)で記録されます。

オラクルとお客様の両方が共有セッションにアクセスしている状態で、オラクルが問題の解決に当たります。適切な技術プロセスの決定はケースバイケースであり、SR に示された障害モードに固有のものです。

サービスの終了とデータの破壊

お客様は、ExaDB-C@C を終了させることができます。[169]サービスを終了させると、そのサービスで実行されているデータベースとデータはすべて、Exadata Database Machine Secure Erase を使用して永久に削除されます。[170]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、サポートされる最適な消去方法を選択します。より高いセキュリティと高速性を実現するために、可能なかぎ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 標準に完全に準拠しています。[171]お客様は、My Oracle Support (MOS)サービス・リクエスト(SR)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。

デバイスおよびデータの保持

Oracle Customer Data and Device Retention for (DDR) Oracle Cloud at Customer[172]は、ExaDB-C@C のオプションのアドオン・サービスです。Oracle DDR は、ExaDB-C@C から取り外された、機微、機密または極秘のお客様データを含む可能性のある適格なハードウェア・アイテム(保持されたハードウェア)をお客様が保持することを許可します。DDR を目的とする場合、保持されたハードウェアとは、Exadata データベース・サーバー、ストレージ・サーバーおよびコントロール・プレーン・サーバーの次のコンポーネントを指します。

- ハード・ディスク・ドライブ(HDD)
- ソリッドステート・ドライブ(SSD)
- パーシステント・メモリー(PMEM)

169 https://docs.public.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/ecc-manage-databases.html#GUID-76C7A374-7E40-4E65-A6F1-AEE63D01CFE7

170 https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/exadata-secure-erase.html#GUID-6C9FD30C-FF88-4ABA-9249-93E183784B0D

171 https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization

172 https://www.oracle.com/assets/customer-data-device-retention-sd-4419287.pdf

まとめ

お客様 VM とデータベース全域の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 Database の暗号化機能によってデータが暗号化され、お客様が暗号鍵のコントロールを保持します。Oracle Database のセキュリティ機能によって、データベース内のデータに対する認証とアクセスがコントロールされ、お客様がこの認証とアクセスのコントロールを保持します。Oracle Linux の認証機能によってお客様 VM へのアクセスがコントロールされ、お客様がこの認証とアクセスのコントロールを保持します。

オラクルが管理する ExaDB-C@C 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-C@C 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、該当する監査ログが VM、Oracle Database、OCI サービスおよび Oracle Service Request (SR)プロセスを通じてお客様に提供されます。

お客様が管理するコンポーネントとオラクルが管理するコンポーネントのセキュリティ体制と監査体制を組み合わせることで、職務が分掌され、高度なセキュリティを備えたオンプレミス・デプロイメントのメリットと、クラウドの利便性と経済性が実現されます。お客様と Oracle Cloud Operations は連携してシステムのセキュリティを構成し、お客様のデータの不正アクセスと盗難を防止します。Oracle Cloud Operations のスタッフは、ExaDB-C@C サービスを提供するためにお客様のネットワークやサービス、データにアクセスすることはありません。またお客様は、オラクルが管理するインフラストラクチャにアクセスして ExaDB-C@C サービスを利用することはありません。ExaDB-C@C 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を得ながら、クラウドの経済性、俊敏性、スケーラビリティを享受できます。

.

CONNECT WITH US

お問い合わせ先：+ 1.800.ORACLE1 もしくは oracle.com にアクセスください。
北米エリア以外にお住まいの場合は、oracle.com/contact で最寄りのオフィスをご確認ください。

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

Exadata Database Service on Cloud@Customer
Security Controls
November 2525