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

ORACLE

Exadata Database Service on Cloud@Customer Security Controls

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

January 9, 2024 | 2.22 版

本書の目的

このドキュメントは、リリース 22.1.17.0.0.231109.1 および 23.1.8.0.0.231109[1]に含まれる機能および強化点の概要を説明します。22.1.17.0.0.231109.1 および 23.1.8.0.0.231109 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 Gen 2 Exadata Database Service on Cloud@Customer (ExaDB-C@C)サービス [2]のセキュリティおよびコントロール機能について説明したもので、ExaDB-C@C の導入評価に携わるお客様のセキュリティ担当者を対象としています。ExaDB-C@C では、お客様が次のサービス提供要件を受け入れる必要があります。

- 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
- ExaDB-C@C インフラストラクチャへのアクセスが許可されたオラクルの担当者は、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するものとします
- オラクルのスタッフは、スーパーユーザー(root)アカウントで実行する必要があるメンテナンスを含む、インフラストラクチャのソフトウェアおよびハードウェアのメンテナンス操作を実行します
- オラクルのスタッフは、ExaDB-C@C の導入に関連するハードウェアとソフトウェアの問題の診断と解決を行うために必要なハードウェアとソフトウェアのコンポーネントにアクセスします

お客様は、オラクルの担当者による ExaDB-C@C インフラストラクチャおよび ExaDB-C@C 上の ADB-D VM へのアクセスをお客様がコントロールするための特権アクセス管理(PAM)サービスである Oracle Operator Access Control[3] (OpCtl)を使用し、オラクルの担当者が ExaDB-C@C インフラストラクチャと ADB-D VM にリモートでログインできるタイミング、および ExaDB-C@C インフラストラクチャと ExaDB-C@C 上の ADB-D VM に対する root アクセスを取得できるタイミングをコントロールできます。OpCtl はまた、お客様に対し完全なコマンド/キーストロークのロギングと、お客様による Oracle 接続の終了のコントロールを提供します。

ExaDB-C@C の評価を担当するセキュリティ担当者は、ExaDB-C@C で利用可能な追加のセキュリティ・コントロールを説明した次の関連文書も確認する必要があります。

- Oracle Cloud Infrastructure Security Architecture[4]
- Oracle Cloud Infrastructure Security Guide[5]
- Security Features in Autonomous Database[6]
- Security and Authentication in Oracle Autonomous Database[7]
- Exadata Database Service on Cloud@Customer Security Guide[8]
- Oracle Operator Access Control for Exadata Cloud@Customer[9]
- Oracle Cloud Infrastructure Security Testing Policies[10]
- Oracle Cloud Services Contracts[11]
- Oracle Data Processing Agreement[12]
- Oracle Cloud Services Agreement[13]

---

[1] https://support.oracle.com/knowledge/Oracle%20Database%20Products/2333222_1.html
[2] https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/gen2-exacc-ds.pdf
[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://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf
[5] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_guide.htm
[6] https://docs.oracle.com/en-us/iaas/autonomous-database/doc/security-features-adb-d.html
[7] https://docs.oracle.com/en/cloud/paas/autonomous-database/adbsa/gs-security-and-authentation-autonomous-database.html
[8] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/exacc-secguide.html
[9] https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/oracle-operator-access-control-tech-brief.pdf
[10] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm
[11] https://www.oracle.com/corporate/contracts/cloud-services/
[12] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
[13] https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#online

- Oracle Corporate Security Practices[14]

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。

[14] https://www.oracle.com/corporate/security-practices/

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・センターにありオラクルが所有・管理するインフラストラクチャを使用して、オラクルのパブリック Exadata Cloud Service をお客様のデータ・センターで提供します。ExaDB-C@C のメリットは、ExaDB-C@C ハードウェアをお客様が選択したデータ・センターに配置することで ExaDB-C@C ハードウェアの物理的なコントロールを保つ一方で、インフラストラクチャ・メンテナンスに対する Oracle Cloud Infrastructure (OCI)コントロール・プレーンおよび ExaDB-C@C Cloud Ops スタッフのサポートによる効率化と自動化を受けられることです。

ExaDB-C@C は、お客様がミッション・クリティカル・アプリケーションや規制の厳しい業界に適用されるポリシー、法律および規制要件を尊重しながら、クラウド実装の運用価値と財務価値の双方を得ることを目指すユース・ケースに適したデータベース・サービスです。ExaDB-C@C 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。これらの業界において、クラウド戦略の追求に関心のあるお客様は、採用したクラウド・プロバイダが提供している標準化されたサービスの中で、これらの機能が包括的にサポートされていることを確認する必要があります。

ExaDB-C@C のサービス・デリバリ・モデルは、お客様データとミッション・クリティカルなワークロードの保護を目的とした、業界のベスト・プラクティスに基づく標準化されたサービスです。ExaDB-C@C のサービス・デリバリ・モデルをお客様が容易に採用できるように、ExaDB-C@C は、お客様が承認済のセキュリティ規格が ExaDB-C@C モデルと異なる可能性があるエッジ・ケースに対する補償措置として、本書で説明したセキュリティ・コントロールを含んでいます。本書の目的は、お客様のセキュリティ・チームが、ExaDB-C@C のセキュリティ体制が適用要件を満たしていることを検証し、過去の標準に対する例外を認め、これらのコントロールに基づいて将来の標準を作成するために使用できるよう、コントロールについて説明することです。

コンプライアンス

オラクルは、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。これらサードパーティのアテステーションの検討においては、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・ドキュメントに関しては、お客様はオラクルの営業担当にリクエストすることもできますし、OCI クラウド・コンソール [15]から直接コンプライアンス・ドキュメントにアクセスすることもできます。

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)の要件を満たすために、オラクルは Oracle Cloud Infrastructure and GDPR[16]ペーパーを発行しています。

オラクルの契約

『Oracle Data Processing Agreement』[17]はオラクルが ExaDB-C@C を含むオラクルのサービスに関連するデータをどのように管理、保護、および処理するかを説明するもので、次が含まれます。

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

『Oracle Cloud Services Agreement』[18]は、Oracle Cloud Services で処理されるお客様データに関する次のような情報などを提供します。

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

Oracle Trust Center[19]は、オラクルのセキュリティ、コンプライアンス、プライバシ、および商業契約に関するインデックスを提供します。

オラクル・コーポレート・セキュリティ・プラクティス

『Oracle Corporate Security Practices』[20]では、オラクルの社内業務とオラクルがお客様に提供するクラウド・サービスのいずれのセキュリティ管理も網羅しており、従業員や請負業者をはじめとするオラクルの全スタッフに適用されます。これらのポリシーは、ISO/IEC 27002:2013 (旧 ISO/IEC 17799:2005)および ISO/IEC 27001:2013 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。Oracle が公開している企業セキュリティ慣行 [21]には次の情報が含まれます。

- 目的 [22] - オラクルのデータとお客様のデータの機密保護、整合性、可用性を守るための支援
- 人事セキュリティ [23]
- アクセス・コントロール [24]
- ネットワーク通信のセキュリティ [25]
- データ・セキュリティ [26]
- ラップトップおよびモバイル・デバイスのセキュリティ [27]

---

[15] https://docs.oracle.com/en-us/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm
[16] https://docs.oracle.com/en-us/iaas/Content/Resources/Assets/whitepapers/oci-gdpr.pdf
[17] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
[18] https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#online
[19] https://www.oracle.com/trust/
[20] https://www.oracle.com/corporate/security-practices/ and https://www.oracle.com/assets/corporate-security-practices-4490843.pdf
[21] https://www.oracle.com/corporate/security-practices/corporate/
[22] https://www.oracle.com/corporate/security-practices/corporate/objectives.html
[23] https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
[24] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[25] https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html
[26] https://www.oracle.com/corporate/security-practices/corporate/data-protection/
[27] https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html

- 物理および環境のセキュリティ [28]
- サプライ・チェーンのセキュリティと保証 [29]

オラクルがお客様の指示のもと、お客様のオフィスまたはシステムで作業している場合、オラクルのコンサルタントとサポート担当は、オラクルとお客様との合意に従い、お客様の慣習を遵守します。

役割と責任

ExaDB-C@C サービスの説明 [30]に記載され、My Oracle Support (MOS)にある ExaDB-C@C サービスの説明 [31]に関するドキュメントに詳しく記載されているとおり、ExaDB-C@C は、お客様とオラクルが共同で管理します。ExaDB-C@C のデプロイメントは、次の 2 つの責任領域に分割されます。

- お客様が管理するサービス:ExaDB-C@C のサブスクリプションの一部としてお客様がアクセスできるコンポーネント
  - お客様がアクセスできる仮想マシン(VM)
  - お客様がアクセスできるデータベース・サービス
- オラクルが管理するインフラストラクチャ: お客様がアクセスできるサービスを実行するために、オラクルが所有し運用するハードウェア
  - 配電ユニット(PDU)
  - 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

お客様は、お客様のサービスへのアクセスをコントロールおよび監視します。これには、(レイヤー2 VLAN やお客様 VM に実装されたファイアウォールを経由した)VM へのネットワーク・アクセス、VM にアクセスするための認証、VM で実行されるデータベースにアクセスするための認証が含まれます。オラクルは、オラクルが管理するインフラストラクチャ・コンポーネントへのアクセスをコントロール・監視します。オラクルのスタッフには、お客様 VM やデータベースといったお客様のサービスにアクセスする権限はありません。表 1 では、オラクルとお客様が担う役割と責任の詳細な分担を示しています。

表 1: 役割と責任

職務	オラクルが管理するインフラストラクチャ		お客様が管理するサービス	
	Oracle Cloud Ops	お客様	Oracle Cloud Ops	お客様
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

[28] https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
[29] https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
[30] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/ecc-system-config-options.html
[31] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2707015.1

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	Cloud Automation 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

EXADB-C@C サービスのアーキテクチャ

図 1 は、Gen 2 ExaDB-C@C サービスのアーキテクチャ・ブロック図です。

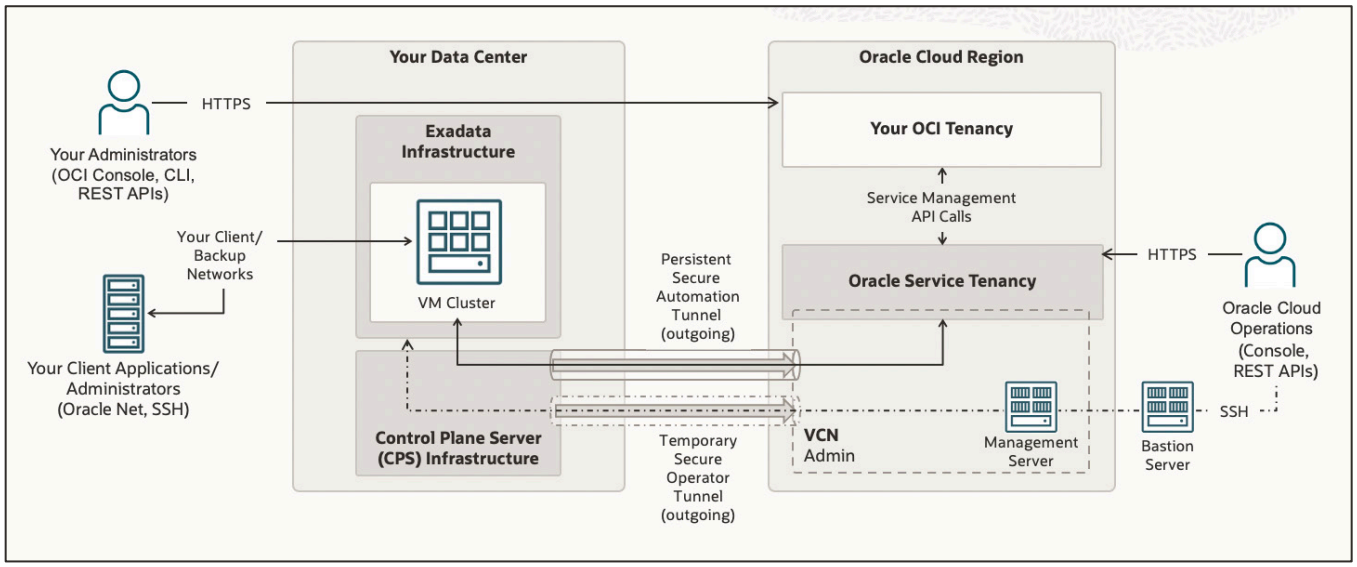

図 1: Oracle ExaDB-C@C のアーキテクチャ・ブロック図

ExaDB-C@C サービスは、お客様が選択したデータ・センター内の ExaDB-C@C ラックにデプロイされます。ExaDB-C@C 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、OCI リージョンに接続される高可用性(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。

お客様のデータベースのデータは、オンプレミスの ExaDB-C@C ラックで保護され、お客様のデータベースに対するすべてのアクセスは、ExaDB-C@C ラックの VM とデータベースにアクセスすることをお客様が許可したネットワーク接続(イントラネット)を介して行われます。お客様 VM とお客様のデータベースにアクセスするための資格証明は、お客様によって保持・管理されます。お客様は、お客様 VM とお客様のデータベースへの特権アクセス(root、SYS 等)を持ち、これらの資格証明を使用して VM とデータベースを保護することで、ローカルのポリシーと規制要件に対処できます。これには、エージェントをインストールする、OS とデータベースの監査ログをお客様の SIEM (Security Information and Event Management)に転送する、ExaDB-C@C のコンピュート VM OS やオラクル・データベースと互換性のあるツールを使用して、VM とデータベースに対するアクセスとアイデンティティ管理をコントロールするといった作業が含まれますが、これらに限定されません。

OCI リージョンは、お客様コントロールによるデータベースやシステム管理の Cloud Automation、インフラストラクチャのメンテナンスやサポートなどの ExaDB-C@C サービスをリモートで提供します。お客様は、OCI Identity and Access Management (IAM)サービスを使用して、Cloud Automation の管理機能へのアクセスをコントロールします。また、OCI Audit サービスによって、お客様が OCI コンソールまたは OCI REST エンドポイント経由で開始したすべての管理アクション(データベースの作成や削除など)の記録がお客様に提供されます。オラクルは、OCI リージョンからコントロール・プレーン・サーバーへのネットワーク・アクセス、およびインフラストラクチャのメンテナンスやサポートを実行するためのオペレータのアクセスをコントロールします。

物理的および論理的なネットワーク展開の詳細は、「Exadata Database Service on Cloud@Customer の準備」[32]ドキュメントで公開されています。この文書には、サービスのインストールと運用に必要な電源、スペース、冷却、その他のお客様のデータ・センターの要件も含まれています。

コントロール・プレーン・サーバーのネットワーク

ExaDB-C@C サービスでは、サービス提供、サポート、または管理を目的とするインバウンド TCP 接続は不要です。一方、リモートでのサービス提供と管理のために、ポート 443 においてオラクルのエンドポイントへのアウトバウンド TCP 接続が必要です。CPS から OCI エンドポイントへの TCP 接続が確立された後、TCP 接続は OCI から ExaDB-C@C インフラストラクチャへのペイロードの配信を許可できることに留意してください。たとえば、持続的で安全な Automation 用トンネルは OCI から ExaDB-C@C インフラストラクチャに REST API 呼出しを送信するために使用され、一時的で安全なオペレータ用トンネルは Oracle Cloud Ops が ssh プロトコル経由で ExaDB-C@C インフラストラクチャにアクセスするために使用されています。これらのエンドポイントは、表 2: ExaDB-C@C に必要なアウトバウンド URL アクセスおよび Exadata Database Service on Cloud@Customer 製品ドキュメント [33]の「Oracle Exadata Database Service on Cloud@Customer のネットワーク要件」の項 [34]に示されています。

IP アドレス・フィルタリング・ベースのファイアウォール・ルールを使用している場合、クラウド・インタフェースの動的な性質のために、https://docs.oracle.com/en-us/iaas/tools/public_ip_ranges.json で識別される OCI リージョンに関連付けられているすべての関連する IP CIDR 範囲を使用してトラフィックを許可する必要があります。

ExaDB-C@C 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。http プロキシには、デプロイメントの複雑性が伴うほか、さらなる OCI エンドポイントへのアクセスが必要となる可能性がある今後の ExaDB-C@C リリースをサポートするためのメンテナンスが必要です。お客様が特定の OCI サービスの URL に対するアクセスを選択的に許可する場合、オラクルが新たな機能やサービスを ExaDB-C@C に追加するときに、許可した URL の更新が必要になる場合があります。お客様の https、チャレンジ・プロキシおよびトラフィック・インスペクションには対応していません。

自動化を提供するための ExaDB-C@C 永続セキュア・トンネル・サービスは、Cloud Automation コマンド(REST API 呼出しのみ)をリモートで提供するために使用されます。このサービスは、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。このサービスの URL は、ExaDB-C@C インフラストラクチャを管理するように構成された OCI リージョンに固有です。

リモート・オペレータ・アクセス用の ExaDB-C@C セキュア・トンネル・サービスは、オラクルが管理する ExaDB-C@C インフラストラクチャ、および場合によっては ADB-D リソースへのオラクルのオペレータ・アクセス(ssh)に限って使用されます。このサービスは、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。このサービスの URL は、ExaDB-C@C インフラストラクチャへのオラクルのオペレータ・アクセスを許可するように構成された OCI リージョンに固有です。

ExaDB-C@C インフラストラクチャから OCI への mTLS 接続の証明書は、オラクルによって独占的に管理されます。ExaDB-C@C 永続セキュア・トンネル・サービス用の ExaDB-C@C インフラストラクチャのクライアント証明書は、オラクルによって 6 か月のスケジュールでローテーションされます。リモート・オペレータ・アクセス用の ExaDB-C@C セキュア・トンネル・サービスのクライアント証明書は、15 日のスケジュールでローテーションされます。ExaDB-C@C の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。お客様がこれらの証明書を管理したり、セキュア・トンネル接続内のトラフィックを調べたりすることは許可されていません。

CPS には、IP アドレス解決のためのお客様が提供した DNS と、時刻同期のための NTP サーバー、OCI サービス URL へのルーティングが必要です。

OCI への CPS インターネット接続に必要な最低帯域は、50/10mbs のダウンロード/アップロードです。

OCI に戻る ExaDB-C@C ネットワーク接続は、OCI FastConnect[35]または OCI サイト間 VPN によって実装されます。[36],[37]OCI 転送ルーティング [38]およびネットワーク・セキュリティ・リスト [39]は、ExaDB-C@C インフラストラクチャから OCI サービ

---

[32] https://docs.oracle.com/en-us/iaas/exadata/doc/eccpreparing.html#GUID-A29A2B1C-708F-4AF2-BE6E-0B4916F6CB25
[33] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/eccad/index.html
[34] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/eccad/eccpreparing.html#GUID-F06BD75B-E971-48ED-8699-E1004D4B4AC1
[35] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/fastconnect.htm

スへのアクセスをコントロールするために使用でき、OCI VCN フロー・ログ [40]は、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するために使用できます。

[36] https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/overviewIPsec.htm
[37] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-network-requirements.html#GUID-E53A5DCF-CCCD-4493-B1D2-4EA6FA30B8A1
[38] https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/transitroutingoracleservices.htm
[39] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/securitylists.htm
[40] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/vcn_flow_logs.htm

表 2: ExaDB-C@C に必要なアウトバウンドURL アクセス [41]

説明/目的	開放するポート	認証局	ロケーション *OCI_REGION* を自分のリージョン [42]に置き換えてください
Cloud Automation を提供するための永続発信トンネル・サービス	443 outbound	オラクル 自己署名	https://wss.exacc.*oci_region*.oci.oraclecloud.com
Autonomous Database Dedicated (ADB-D)の Cloud Automation を提供するための永続発信トンネル・サービス	443 outbound	オラクル 自己署名	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オラクルのリモート・オペレータがアクセスするための一時セキュア・トンネル・サービス	443 outbound	オラクル 自己署名	https://mgmthe1.exacc.*oci_region*.oci.oraclecloud.com https://mgmthe2.exacc.*oci_region*.oci.oraclecloud.com
ADB-D リソースにオラクルのリモート・オペレータがアクセスするための一時セキュア・トンネル・サービス	443 outbound	オラクル 自己署名	https://mgmthe.adbd-exacc.*oci_region*.oci.oraclecloud.com
システム更新取得用の Object Storage Service	443 outbound	DigiCert	https://objectstorage.*oci_region*.oraclecloud.com https://swiftobjectstorage.*oci_region*.oraclecloud.com
インフラストラクチャ・モニタリング・メトリック(IMM)の記録および処理用の Monitoring Service	443 outbound	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	443 outbound	DigiCert	https://identity.*oci_region*.oraclecloud.com https://auth.*oci_region*.oraclecloud.com

[41] https://docs.oracle.com/en-us/iaas/exadata/doc/eccpreparing.html#GUID-D3C65CB4-965E-4670-B676-5EEA4C9282C9

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

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	443 outbound	Oracle PKISVC CrossRegion Intermediate r2[43]	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	443 outbound	DigiCert	https://database.*oci_region*.oraclecloud.com

ExaDB-C@C サービスへのお客様のアクセス

お客様は、ポート 1521 の Oracle Net などの標準の Oracle データベース接続方法を使用して、お客様機器からお客様 VM で実行されているデータベースへのレイヤー2 (タグ付き VLAN)接続を介して、ExaDB-C@C で実行されている Oracle データベース(DB)にアクセスします。また、ポート 22 のトークン・ベースの ssh など、標準的な Oracle Linux の方式を使用して、Oracle データベースを実行しているお客様 VM にアクセスします。

OCPU のスケーリング、仮想マシン(VM)クラスタの作成など、インフラストラクチャ・コンポーネントを管理するアクションは、セキュリティを考慮して設計され Oracle Cloud Infrastructure でホストされるテナンシで、Cloud Automation ソフトウェアを活用するお客様によって実行されます。お客様はインフラストラクチャ・レイヤーを管理する必要はありません。オラクルが稼働時間 99.95%のサービス・レベル目標(SLO)を維持します。お客様には、ExaDB-C@C サービスのオラクルが管理するインフラストラクチャに対して直接アクセスしたり、監視エージェントをロードしたり、ファイルを直接プルまたはプッシュしたりする権限はありません。

[43]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

物理的なネットワーク実装

図 2 では、Exadata ラックにデプロイされた ExaDB-C@C での物理的なネットワークの実装を示し、Exadata Database Service on Cloud@Customer の技術的なアーキテクチャ [44]では、アーキテクチャと実装について詳しく説明しています。お客様がアクセスおよびコントロールできるコンポーネントは青で表示され、オラクルが管理するコンポーネントは赤で表示されています。ExaDB-C@C インフラストラクチャ・コンポーネントは、同じく赤で表示されている独立したレイヤー2 管理ネットワーク経由で相互接続されています。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・ネットワークやバックアップ・ネットワークへの直接的なネットワーク・アクセスはなく、Exadata Database Server には、クライアントまたはバックアップ・ネットワークにアクセスするための 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 [45]を作成する際に、クライアント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設定します。

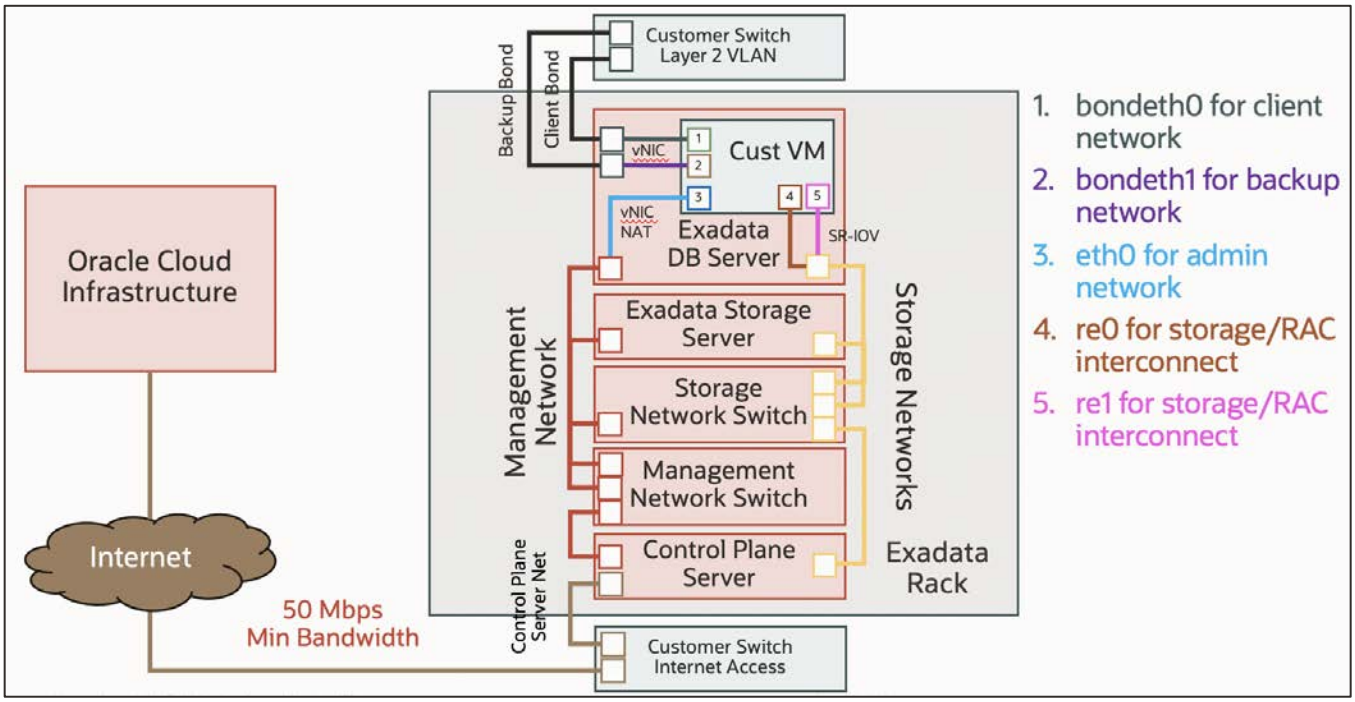

図 2: ExaDB-C@C の物理的なネットワーク実装

図 3 は、同じ ExaDB-C@C 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詳細に示しています。複数の VM クラスタが構成されている場合、お客様は各 VM クラスタの VLAN タグと IP ネットワーク構成をコントロールします。また、同じ Exadata DB Server の各 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)の同じ物理リンクを共有します。お客様は、VM クラスタへのネットワーク・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別の VLAN タグを指定できます。各 VM クラスタのバックエンド・ストレージ・ネットワーク(ネットワーク 4 および 5)は、バックエンド・ストレージ・ネットワークをサポートするコンバージド・イーサネット実装において、レイヤー2 のコントロールによって分離されているため、同じ Exadata Database Server の異なる VM がバックエンド・ストレージ・ネットワーク経由で相互にアクセスすることはできません。vNIC/NAT 管理ネットワーク・アクセス(ネットワーク 3)は、分離された/30 ネットワークとして実装されているため、同じ Exadata DB Server の異なる VM が管理ネットワーク経由で相互にアクセスすることはできません。

VM 内で実行される方法によって他の VM からのキャッシュ・データにアクセスするのを防ぐ予防的統制として、ネットワークの分離に加えて、CPU コアが特定の Exadata Database Server の特定の VM に固定されています。

---

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

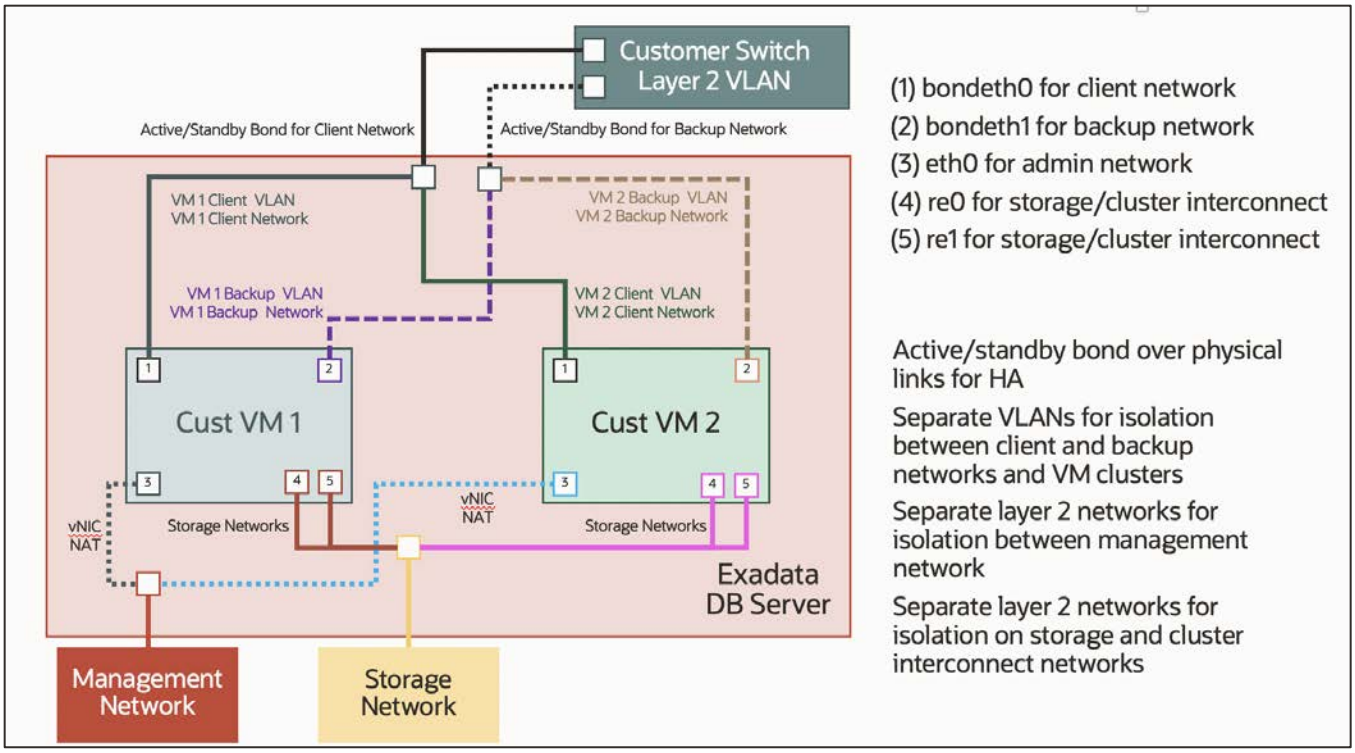

図3: VM クラスタ・ネットワークの分離

コントロール・プレーン・サーバーは、パブリック・インターネット経由で Oracle Cloud Infrastructure (OCI)コントロール・プレーンにアクセスします。また、お客様管理スイッチへのレイヤー2 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。お客様は、時刻サービス(NTP)、インターネット・ホスト名の名前解決(DNS)、およびコントロール・プレーン・サーバーが OCI コントロール・プレーンに接続するためのルーティングを提供します。コントロール・プレーン・サーバー・ネットワークに関する本書の「コントロール・プレーン・サーバーのネットワーク」の項で説明するように、コントロール・プレーン・サーバーには、インバウンド TCP 接続は不要です。TCP ポート 443 におけるオラクル IP アドレスへのアウトバウンド接続のみが必要です。お客様は、コントロール・プレーン・サーバーへのインバウンド・ アクセスを拒否し、必要なオラクルの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・ルールを設定することができ、これを設定する必要があります。CPS から OCI コントロール・プレーンへの接続に必要な最小帯域幅は、ダウンロードでは 50Mbps、アップロードでは 10Mbps です。

Exadata Database (DB)Server は、10Gb または 25Gb のイーサネット経由で、お客様管理のレイヤー2 スイッチに接続されます。お客様の仮想マシン(お客様 VM)へのアクセスには、仮想ネットワーク・インタフェース・カード (vNIC)として実装された、お客様 VM へのレイヤー2 (タグ付けされた VLAN)ネットワーク接続のペア(クライアントおよびバックアップ)を経由します。物理的なネットワーク接続は、アクティブ/スタンバイ構成で高可用性向けに実装されています。

お客様 VM は、黄色で表示されている SR-IOV にマップされたインタフェース経由で、ルーティングされないプライベート・インターコネクト・ネットワークを介して 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・スイッチのペアへの HA(アクティブ/スタンバイ)接続があります。次の CIDR の 100.107.0.0/24 は、ストレージ・ネットワーク構成における標準的な IP アドレスを示しています。これらの IP アドレスが既存の IP アドレスと競合した場合は、お客様はこの CIDR ブロックをお客様が提供する任意の IP アドレス範囲に上書きできます。

Oracle Cloud Automation は、赤で表示されている、Exadata Database Server の vNIC に実装された管理ネットワーク上の NAT アドレス経由でお客様 VM にアクセスします。Oracle Cloud Automation のお客様 VM へのアクセスは、トークン・ベースの ssh を使用してコントロールされます。Oracle Cloud Automation は、お客様が開始した管理アクションごとに、お客様の VM にアクセスするための一時的で一意の ssh 鍵ペアを生成します。公開鍵は DBCS エージェントを介した Cloud Automation によって、お客様 VM において必要なサービス・アカウントの`~/.ssh/authorized_keys` ファイルに挿入されます(`oracle`、`opc`、`grid`、`root` など)。自動化で使用される一時的な秘密鍵は、お客様のデータ・センターにある ExaDB-C@C ハードウェアで実行中の Oracle Cloud Automation ソフトウェアによってメモリーに格納され、アクション完了後に廃棄されます。同様に、Cloud Automation ソフトウェアは、アクションが完了すると、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ていますが、オラクルのオペレータの名前付きアカウントは鍵に直接アクセスできません。オラクルのオペレータの名前付きアカウントは、`root` アイデン

ティティを引き継ぐことも、sudo を使用してルート権限にアクセスすることもできます。Operator Access Control サービスを ExaDB-C@C サービスに適用することで、お客様は、オラクルのオペレータが ExaDB-C@C インフラストラクチャと Autonomous Database Dedicated VM にアクセスできるタイミングと、オラクルのオペレータがこれらのコンポーネントに対する root アクセスを取得できるタイミングをコントロールできるようになります。

お客様の OCI Identity and Access Management (IAM)コントロールは、お客様の OCI アイデンティティがお客様の VM およびデータベースに対して Oracle Cloud Automation 機能を実行できるかどうか、および実行する方法を管理します。お客様の VM には、Cloud Automation による ssh アクセスの検出を含む、Oracle Linux 監査システムによる検出アクセス・コントロールが実装されています。お客様は、お客様 VM のファイアウォール構成を介して、レイヤー3 および 4 で Cloud Automation の ssh アクセスをブロックできますが、これにより、ssh を介してお客様の VM にアクセスする必要がある Cloud Automation の機能が損なわれます。この機能には、次のものが含まれます。

- ASM ディスク・グループのサイズ変更
- ローカル・ストレージのサイズ変更
- お客様の VM メモリーのサイズ変更
- データベースのパッチ適用
- Grid Infrastructure のパッチ適用
- お客様の VM OS へのパッチ適用

Oracle Cloud Automation では、OCPU スケーリングを実行するためにお客様 VM にネットワーク・アクセスする必要はありません。OCPU スケーリング機能は、お客様が Oracle Cloud Automation のお客様 VM へのネットワーク・アクセスをブロックした場合も、正常に機能します。Oracle Cloud Automation のアクセスは、お客様 VM への ssh アクセスに必要な機能のサブセットを許可するために、お客様によって一時的にリストアされる場合があります。

ExaDB-C@C サービスの提供

図 4 は、ExaDB-C@C サービスを提供するために使用される TCP ポートと TCP プロトコルを示しています。[46]

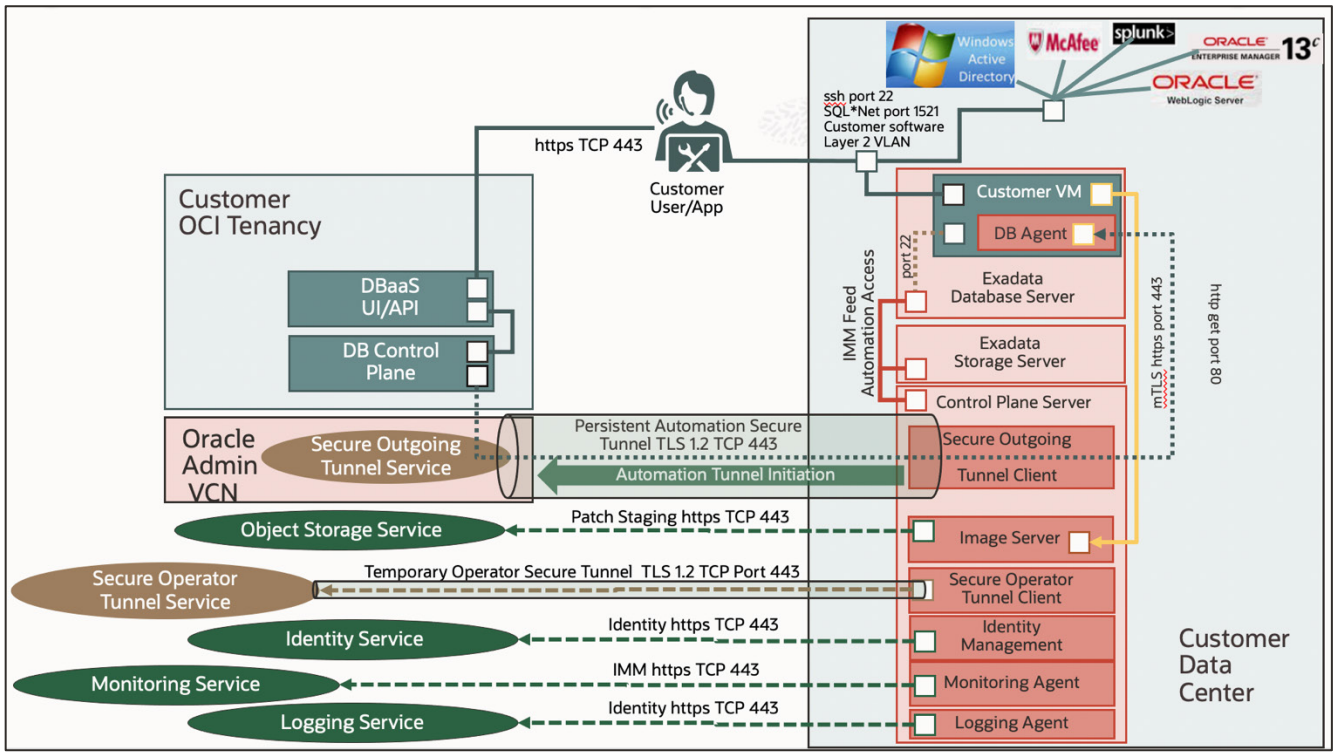

図 4: ExaDB-C@C サービス・ポートとプロトコル

[46] 図を明確化するために、サービスのエンドポイントは省略されています。URL エンドポイントの包括的なリストについては、表 2: ExaDB-C@C に必要なアウトバウンド URL アクセスと https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-network-requirements.html#GUID-F06BD75B-E971-48ED-8699-E1004D4B4AC1 を参照してください

次に示すのは、リモート・サービスを提供する上で重要なコンポーネントです。

- Oracle Cloud Infrastructure (OCI)テナンシへのお客様のアクセス
- OCI ユーザー・インタフェースおよび API へのお客様アクセスのコントロール
- リモートで自動化を提供するための、ExaDB-C@C への OCI データベース・コントロール・プレーンのアクセス
- ExaDB-C@C を OCI リージョンに接続するためのセキュアな発信トンネル・サービス
- ExaDB-C@C コンポーネントのソフトウェア・アップデートを提供するための OCI Object Storage サービス
- インフラストラクチャの監視
- Oracle Cloud Ops スタッフのアイデンティティ管理
- オラクルのオペレータ・アクセスのための一時セキュア・トンネル・サービス(リバース ssh トンネル)

ExaDB-C@C サービスでは、Oracle コントロール・プレーンと通信するために、お客様 VM にデプロイされたソフトウェアが必要です。ExaDB-C@C のお客様 VM に実装されているプロセス、ユーザーID およびネットワーク通信ポートの実装の詳細は、『Exadata Database Service on Cloud@Customer Security Guide』[47]で公開されています。

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 OpCtl を使用して、オラクルによる ADB-D VM へのアクセスをコントロールすることが可能です。
- ADB-D サービスの機能を提供するため、ADB-D 固有のエンドポイントに 2 つ目の永続的なセキュア発信トンネル・サービスが確立されます。
- オラクルの ADB-D サポート・オペレータが ADB-D VM に ssh でアクセスするために、ADB-D 固有のエンドポイントに 2 つ目の一時的なセキュア発信トンネル・サービスが確立されます。

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。

OCI インタフェースへのお客様のアクセス

お客様は、OCI コントロール・プレーンへのポート 443 の https 接続を使用して、OCI テナンシの Cloud Automation サービスにアクセスします。OCI コントロール・プレーンでは、次の管理インタフェースが提供されます。

- Web ユーザー・インタフェース(Web UI) - 通常は非定型アクションで使用
- Oracle Cloud シェル - Oracle Cloud Infrastructure コンソールに直接入力する Linux シェル
- OCI コマンドライン・インタフェース(OCI CLI) - 通常は OS シェルからのプログラム的なアクションで使用
- REST API (OCI ソフトウェア開発キット(OCI SDK)) - 通常はアプリケーション統合で使用
- Terraform - 通常は Infrastructure as Code で使用

OCI 管理インタフェースへのアクセスは、お客様が OCI Identity and Access Management (IAM)を使用して管理します。お客様が管理するアイデンティティに、リクエストされたアクションを実行する権限がある場合、アクションは、次のように適切な ExaDB-C@C コンポーネントに提供されます。

- DBaaS UI/API が、https 経由でリクエストを DB コントロール・プレーンに送信します
- DB コントロール・プレーンが、永続セキュア・トンネル・サービス管理 VCN 経由で、REST API を使用してリクエストをプロキシ・サービス(CPS プロキシ)に送信します
- OCI 管理 VCN および CPS の TLS 1.2 永続セキュア・トンネル・サービスが、ExaDB-C@C ラックの CPS で実行されている CPS プロキシに REST API リクエストを提供します
- CPS プロキシが、ExaDB-C@C コンポーネントにコマンドを発行します
  - お客様 VM のデータベース・サービスにアクセスすることが必要なアクションは、OCI コントロール・プレーンと各 DB エージェント間のセキュア接続経由で、お客様 VM のいずれか、またはすべて(たとえば、Half Rack には最大 4 つの VM があります)で実行されている DB エージェントに送信されます。この mTLS 接続は、ExaDB-C@C ラック内のプライベート・インターコネクト・ネットワークを介して実装されています。ポートの詳細は『Exadata Database Service on Cloud@Customer Security Guide』[48]を参照してください

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

- お客様 VM にアクセスすることが必要なアクションは、Exadata Database Server からアクセスできるお客様 VM に NAT アドレスとして実装されている内部管理ネットワーク経由で、トークンベースの ssh で実行されます。公開 ssh 鍵は一時的なもので、お客様が開始した管理アクションのために生成され、お客様 VM の oracle、opc、grid または root ユーザー(あるいはそのすべて)の authorized_keys ファイルに格納されます。秘密 ssh 鍵は一時的なもので、お客様が開始した管理アクションのために生成され、お客様のデータ・センターにある Exadata ハードウェアで実行中の Oracle Cloud Automation ソフトウェアによってメモリーに格納されます
- インフラストラクチャ・コンポーネントにアクセスすることが必要なアクションは、CPS から必要なエンドポイント(Exadata Storage Server、Exadata Database Server など)への内部管理ネットワーク経由で、トークンベースの ssh を使用して発行されます

インフラストラクチャの監視

ExaDB-C@C インフラストラクチャ・コンポーネントは、CPS にインフラストラクチャ管理メトリック(IMM)をレポートし、CPS は処理のためにこの情報をオラクルに中継します。IMM 接続は、ExaDB-C@C サービスの管理に使用される OCI リージョン固有のエンドポイントと、https 経由で行われます。

Oracle Support は、ExaDB-C@C の実装を次のように監視および保守します。

- Oracle Cloud@Customer インフラストラクチャ・コンポーネントの自動化された監視機能が、CPS にデプロイされたインフラストラクチャ監視ユーティリティを使用して、インフラストラクチャ監視メトリック(IMM)を OCI テレメトリ・サービスのエンドポイントに送信します
  - シャーシの温度、ドライブのステータスなど
  - すべての監視データの詳細は、『Auto Service Request Qualified Engineered Systems Products』[49]で公開しています
- アプリケーションおよびセキュリティ・ログの監視の自動化によって、アプリケーションとセキュリティ・ログが Oracle 管理の OCI ロギング・サービス・エンドポイントに送信されます。
- Oracle Support は、監視データを分析し、どのイベントの修正が必要かを判断し、サポート・チケットを作成し、サポート・チケットを OCI サポート・スタッフに割り当てます。
- チケットが割り当てられると、Cloud Ops サポート・スタッフが派遣され、必要なサポート行為を実施します。

四半期ソフトウェア・アップデート

オラクルとお客様が協力して Exadata Database Service on Cloud@Customer ソフトウェア・アップデートを行う方法の詳細は、Exadata Database Service on Cloud@Customer サービスのメンテナンス[50]に関するドキュメントで公開されています。My Oracle Support ドキュメント 2333222.1 (Exadata Cloud Software Versions[51])には、ExaDB-C@C で利用可能な現在とこれまでのソフトウェア・バージョンの情報が記載されています。

Oracle Database、Oracle Grid Infrastructure、およびお客様 VM OS の四半期ごとのバンドル・パッチは、オラクルによって OCI Object Storage から CPS にステージングされます。四半期ごとのソフトウェア・アップデートは、お客様向けに Cloud Automation ユーザー・インタフェースに一覧表示され、それらのパッチのアプリケーションは、OCI のツールとポリシーを使用してお客様がコントロールします。パッチは、お客様 VM から CPS で実行中のイメージ・サーバーへのアウトバウンド http (ポート 80)接続を介して、アプリケーションのためにアクセスされます。

インフラストラクチャ・コンポーネントの四半期ごとの標準パッチ・バンドルとソフトウェア・アップデートは、個別のソフトウェア・アップデートで定められているように、Oracle Cloud Automation とオラクルのスタッフによってデプロイされます。アップデートは、可能な場合は、Linux ksplice などのツールを使用して停止時間なしで実行中のシステムに適用されます。アップデートの際にコンポーネントの再起動が必要な場合は、オラクルはローリング方式でコンポーネントの再起動を実行して、アップデート・プロセス中のサービスの可用性を確保します。

---

[49] https://docs.oracle.com/cd/E37710_01/doc.41/e37287/toc.htm
[50] https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/examaintenance.htm
[51] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2333222.1

月次セキュリティ・スキャンおよびアップデート

四半期ごとのメンテナンスと一緒に実行されるセキュリティ・メンテナンス [52]は、重要なセキュリティ・アップデートが必要な月に行われ、CVSS スコアが 7 を超える脆弱性の修正を含んでいます。

セキュリティ・メンテナンスは、必要に応じて、各月の 15 日より後に始まる 21 日間の期間中に適用するようにスケジュールされます。お客様は、月次メンテナンス期間の開始日より 7 日以上前に、スケジュール案の通知を受け取ります。月次メンテナンスは、必要に応じて、期間内の別の日にスケジュールしなおすことができます。月次セキュリティ・メンテナンスには、それまでの月のスキャンで特定されたすべてのセキュリティ脆弱性の修正が含まれます。データベース・サーバーのアップデートが Ksplice テクノロジによってオンラインで適用されるのに対し、ストレージ・サーバーのアップデートはローリング方式で適用されます。

スキャン結果はオラクルの内部で保護され、セキュリティ上の理由から一般に公開されたり、お客様と共有されたりすることはありません。オラクルの Software Security Assurance Practices[53]には、オラクルがソフトウェアの脆弱性をどのように扱い、どのように伝えるかについての詳細が記載されています。

ソフトウェア・アップデートのセキュリティ・コントロール

ExaDB-C@C サービス向けにオラクルが管理する初期ソフトウェア・デプロイメント・パッケージとすべてのソフトウェア・アップデートは、サービスへの提供前に署名されます。ExaDB-C@C サービスでは、これらのソフトウェア・アップデートに有効な署名があるかどうかを自動的にチェックし、検出された署名が無効である場合は、ソフトウェア・アップデートが拒否されて、オラクルにアラートが送信されます。Oracle Software Security Assurance[54]の基準が ExaDB-C@C ソフトウェアに適用されます。

予防的統制

ExaDB-C@C サービスは、お客様のサービスとデータベース・データを不正アクセスから保護するように設計されています。ExaDB-C@C サービスでは、お客様とオラクルの間で職務が分掌されます。お客様は、お客様のサービス、データベース、データベース・データへのアクセスをコントロールします。オラクルは、オラクルが管理するインフラストラクチャ・コンポーネントへのアクセスをコントロールします。

お客様のアクセス・コントロール

お客様は、次の 3 種類のコントロールを使用して、お客様 VM、データベース、およびデータへのアクセスをコントロールします。

- 認証
  - OCI サービス [55]、お客様 VM OS およびデータベース [56]、およびデータベース・データ [57]にアクセスするための資格証明
- ネットワーク
  - お客様 VM にアクセスするためのレイヤー2 VLAN[58]
  - お客様 VM OS[59] および Oracle データベース [60]に実装されたネットワーク・アクセス・ルール

---

[52] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-vw-maint-hist.html#GUID-A2008207-3683-424F-9279-F632BF4C9076
[53] https://www.oracle.com/corporate/security-practices/assurance/
[54] https://www.oracle.com/corporate/security-practices/assurance/
[55] https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm
[56] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/ecc-connecting-to-exacc-system.html
[57] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-privilege-and-role-authorization.html#GUID-89CE989D-C97F-4CFD-941F-18203090A1AC
[58] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/ecc-setting-up-the-network.html
[59] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-implement-sec.html#ol7-firewall-sec

- 暗号化
  - アプリケーションからデータベースへの暗号化 [61]
  - データベースからストレージへの暗号化 [62]

ExaDB-C@C ソフトウェアは、お客様がファイアウォールを設定したり、ネットワーク・インタフェースを無効にしたり、お客様の VM で実行されている Cloud Automation ソフトウェア・エージェントを無効にしたりするためのインタフェースを提供しません。特別なセキュリティ要件があるお客様は、OS ツールを使用してこのような制御を実装することができますが、この操作により、お客様の VM にアクセスする Cloud Automation 機能が無効になります。お客様は、これらの制御を解除し、OS ツールを使用して Cloud Automation ソフトウェア･エージェントを有効にし、お客様の VM にアクセスする Cloud Automation 機能を復元する必要があります。

ExaDB-C@C サービスにおけるお客様のアクセス・コントロール

お客様は、OCI 自動化機能によって、お客様が選択した OCI リージョンの Oracle Public Cloud コントロール・プレーンに対して https 接続を確立することで、管理アクションを実行します。お客様は OCI Identity and Access Management (IAM)の資格証明を使用して認証され、お客様のアクションは、特定のリソースに対してお客様が構成した OCI IAM 権限によってコントロールされます。お客様ユーザーに、リクエストされた管理アクションをターゲット・リソースで実行する権限がある場合、リクエストされたコマンドは、永続セキュア・トンネル・サービス経由でローカルのコントロール・プレーン・サーバー(CPS)に送信され、適切な ExaDB-C@C コンポーネントに提供されます。

お客様とデータベース・アプリケーションは、お客様 VM でホストされるレイヤー2 (タグ付けされた VLAN)ネットワーク接続を介して、ExaDB-C@C で実行中のデータベースにアクセスします。データベースと OS へのアクセスは、お客様が管理する資格証明を使用して行われます。

---

[60] https://docs.oracle.com/en/database/oracle/oracle-database/19/netag/configuring-oracle-connection-manager.html#GUID-AF8A511E-9AE6-4F4D-8E58-F28BC53F64E4

[61] ExaDB-C@C の自動化機能により、Oracle Native Network Encryption が構成されますが、お客様はこのコントロールをオーバーライドできます。オラクルは、お客様がこのコントロールを維持することを強く推奨します

[62] ExaDB-C@C の自動化機能により、オラクルの透過的データ暗号化(TDE)が構成されます。オラクルは、お客様がこのコントロールを維持することを強く推奨します

データ・セキュリティに対するお客様のコントロール

Oracle ExaDB-C@C は、適切なお客様によって正当に使用されるようにデータを保護し、不正アクセスからデータを守ることができるように設計されています。この設計により、Oracle Cloud Ops スタッフ・メンバーがお客様のデータにアクセスすることも防止されます。ExaDB-C@C インフラストラクチャ、お客様 VM、および Oracle Database のデータに対する不正アクセスを防ぐよう設計されたセキュリティ対策には、次のものが含まれます。

- お客様は、名前付きの特権ユーザー(sys、system など)の認証とお客様のデータベースへのアクセスに対するコントロールを保持します
- お客様は、名前付きの特権ユーザー(root、opc、oracle、grid など)の認証とお客様 VM へのアクセスに対するコントロールを保持します
- お客様 VM へのアクセスは、お客様 VM OS によってログに記録されます。お客様はこれらのログを利用でき、任意の Security Information Event Management (SIEM)システムに送信できます
- お客様は、マルウェアの検出を目的としてお客様の VM にスキャン・エージェントをインストールできます。お客様は、お客様の VM をスキャンする前に、Exadata セキュリティ・スキャンの一般的な発見に対する回答(My Oracle Support Doc ID 1405320.1)[63]を確認してください。お客様のセキュリティ・スキャン/テストは、『Oracle Cloud Security Testing Policy』[64]に準拠する必要があります。
- お客様は、Linux カーネルへの悪影響や Exadata 運用の阻害にならなければ、任意の監視エージェントやセキュリティ・コントロールをお客様 VM OS にインストールすることができます
- Oracle Database へのネットワーク接続は、Cloud Automation によって自動的に構成される Oracle Advanced Security Network Encryption によって保護されるように設計されています
- Oracle Database のデータは、保管時にオラクルの透過的データ暗号化(TDE)によって保護されます
  - Cloud Automation で自動構成され、パスワードで保護された PKCS#12 ウォレット・ファイルが、Exadata ストレージ上の ASM Cluster File System (ACFS)[65]に保管され、お客様 VM からアクセス可能となります
  - お客様は、ウォレットのパスワードを使用して TDE 暗号鍵へのアクセスをコントロールします
  - お客様は、TDE マスター鍵を Oracle Key Vault などの外部のキー・ストアに移動できます
- ユーザー・データがデータベース管理者からアクセスされないようにするために、Oracle Database Vault[66]が実装される場合があります

図 5 は、インフラストラクチャ・コンポーネントやお客様 VM コンポーネントへのアクセス権を取得できるユーザーやソフトウェアからお客様のデータがアクセスされないようにする、Oracle Database 内の次の補完的統制を示しています。

- Oracle Native Network Encryption[67]
- Oracle Database Vault[68]
- Oracle Transparent Database Encryption (TDE)[69]

---

[63] https://support.oracle.com/rs?type=doc&id=1405320.1
[64] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm
[65] https://docs.oracle.com/en/database/oracle/oracle-database/19/ostmg/overview-acfs-advm.html
[66] https://docs.oracle.com/en/database/oracle/oracle-database/19/dvadm/introduction-to-oracle-database-vault.html#GUID-0C8AF1B2-6CE9-4408-BFB3-7B2C7F9E7284
[67] Enterprise Edition Extreme Performance サブスクリプションと Bring Your Own License (BYOL)サブスクリプションに含まれます
[68] Enterprise Edition Extreme Performance サブスクリプションに含まれ、Bring Your Own License (BYOL)サブスクリプションには含まれません
[69] Enterprise Edition Extreme Performance サブスクリプションと Bring Your Own License (BYOL)サブスクリプションに含まれます

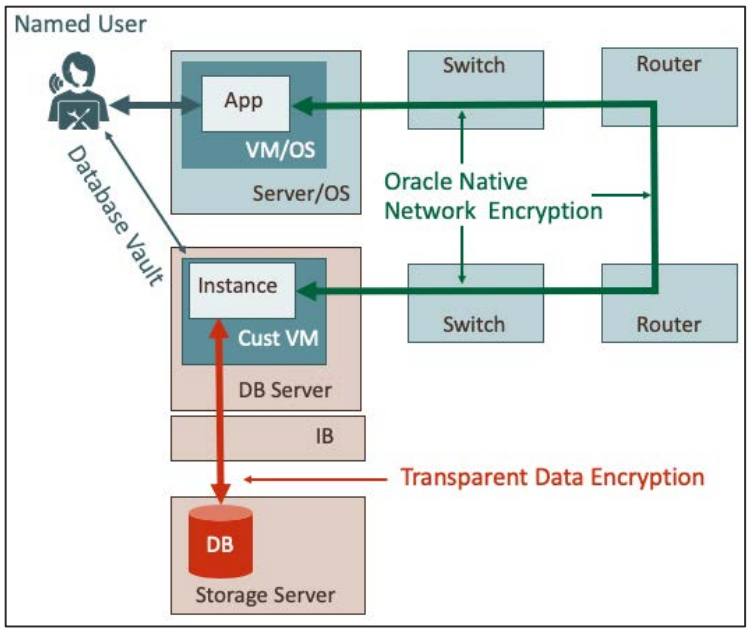

図5: 転送中、処理中、保管中のデータを保護するためのコントロール

Oracle Native Network Encryption

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

Oracle Database Vault

Oracle Database Vault のセキュリティ・コントロールは、特権アカウントからアクセスされないようにアプリケーション・データを保護し、プライバシ要件や規制要件に対処できるように設計されています。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。お客様は、Oracle データベース・ソフトウェアの方式によって Oracle Database Vault を構成および管理する責任を担います。Oracle Database Vault のドキュメントは、各データベース・バージョン向けの『Oracle Database Vault 管理者ガイド』で公開されています。たとえば、Oracle Database 19c の場合は、https://docs.oracle.com/en/database/oracle/oracle-database/19/dvadm/introduction-to-oracle-database-vault.html#GUID-0C8AF1B2-6CE9-4408-BFB3-7B2C7F9E7284 を参照してください。

オラクルの透過的データ暗号化と Oracle Key Vault

オラクルの透過的データ暗号化(Oracle TDE)は、Oracle Database のユーザー表および表領域を暗号化します。権限のあるアプリケーションやユーザーが暗号化を意識する必要はありません。データはストレージに書き込まれる前にデータベースによって自動的に暗号化され、ストレージから読み取られる際に自動的に復号されるためです。データベースにデータを保管する権限とデータベースのデータを検索する権限のあるアプリケーションが参照するのは、復号された(すなわち“平文”の)データのみです。Oracle TDE は、特権のある OS ユーザー、ネットワーク、およびストレージ管理者(あるいはストレージ管理者を装った者)がデータベース・コントロールを迂回してデータに直接アクセスするのを防止します。権限のあるデータベース・ユーザーとアプリケーションは、暗号化されたデータを処理する際に復号鍵を提示する必要はありません。かわりに、データベースではこれまでの章で説明したアクセス・コントロール・ルールによって、データにアクセスする権限がないユーザーのアクセスが拒否されます。

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。

Oracle TDE では、マスター暗号鍵で暗号化されたデータ暗号鍵で構成される 2 層鍵アーキテクチャを使用しています。このマスター暗号鍵は、データベースの外部に保管されます。デフォルトでは、ACFS ファイル・システム内にある、PKCS#12 に準拠した「ウォレット」と呼ばれるコンテナに保管されます。お客様 VM OS では、Oracle RAC に対応したデータベースの両方のインスタンスにアクセスできる共有のウォレット・ロケーションが提供されます。さらに、Oracle Databases 18c 以降では、お客様は外部で生成された独自の暗号鍵(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。お客様は、ExaDB-C@C データベースを、Oracle Database 資産のための唯一の鍵管理ソリューションである Oracle Key Vault (OKV)[70]に移行することも選択できます。Oracle Key Vault は、最大で 16 の OKV ノードを、地理的に分散されたデータ・センターや Oracle Cloud Infrastructure (OCI)にまたがる鍵管理クラスタに追加することで、鍵の継続的な可用性を実現します。Oracle Key Vault により、Oracle TDE 対応のすべてのデータベース・リリースと、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。

Oracle TDE の詳細については、お客様が実行している Oracle Database のバージョンにおける、『Oracle Database Advanced Security ガイド』を参照してください

- TDE for Oracle Database 19c[71]
- TDE for Oracle Database 18c[72]
- TDE for Oracle Database 12.2.0.1[73]
- TDE for Oracle Database 12.1.0.2[74]
- TDE for Oracle Database 11.2.0.4[75]

Oracle TDE の FAQ[76]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。

オラクルは、ExaDB-C@C 上で動作するデータベースの外部キー・ストアとして、Oracle Key Vault (OKV)を使用するお客様をサポートしています。ExaDB-C@C は OKV[77]と統合されているため、お客様はクラウド・オートメーション・インタフェースを使用して TDE 鍵を OKV に移行したり、TDE 鍵をローテーションしたりできます。OS 方式を使用して TDE マスター鍵を OKV に移行する手順は、My Oracle Support ドキュメント 2823650.1 (Migration of File based TDE to OKV for Exadata Database Service on Cloud at Customer Gen2[78])で公開されています。オラクルは、ExaDB-C@C でのサード・パーティ製ハードウェア・セキュリティ・モジュール(HSM)の使用をサポートしていません。

ExaDB-C@C での TDE 実装の詳細は、Exadata Database Machine の暗号化サービス [79]に関するドキュメントに記載されています。

---

[70] https://docs.oracle.com/en/database/oracle/key-vault/21.2/okvag/okv_intro.html#GUID-0D169EB8-C355-459A-9ABD-325CA5B46DD0
[71] https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/introduction-to-transparent-data-encryption.html#GUID-62AA9447-FDCD-4A4C-B563-32DE04D55952
[72] Oracle Database 18c の TDE
[73] Oracle Database 12.2.0.1 の TDE
[74] Oracle Database 12.1.0.2 の TDE
[75] Oracle Database 11.2.0.4 の TDE
[76] https://www.oracle.com/database/technologies/faq-tde.html
[77] https://docs.oracle.com/en-us/iaas/exadata/doc/manage-encryption-keys-on-external-devices.html#GUID-B1EE94A4-2852-4376-949D-25E6E286B932
[78] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2823650.1
[79] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/exadata-security-features.html#GUID-FA8A2A69-AEFC-4FE3-959A-A6E584BD1F4F

お客様 VM への Cloud Automation のアクセス・コントロール

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

- トークンベースの ssh を使用して特権ユーザー(root、opc、oracle)としてお客様 VM にセキュアにログイン
- mTLS 認証を使用し、お客様 VM で実行中の Oracle ソフトウェア・エージェントに対する REST API 呼出しを実行。『Exadata Database Service on Cloud@Customer Security Guide』[80]にポート・マトリクスとソフトウェア・プロセスの記載があります。

お客様 VM では、コントロール・プレーン・ソフトウェア・アクセスをブロックするなど、お客様自身がお客様 VM へのネットワーク・アクセスをコントロールするための補完的統制として Oracle Linux ファイアウォール・ソフトウェア [81]が提供されます。お客様は、Oracle Linux OS の管理ツールを使用してパケット・フィルタリング・ソフトウェアを構成することができます。ExaDB-C@C の自動化には、Oracle Linux パケット・フィルタリング・ソフトウェアを構成する機能やインタフェースは含まれていません。

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

トークンベースの ssh を使用した Oracle Cloud Automation のセキュアなログインは、Kerberos 認証と互換性がありません。お客様がサービス・アカウントを制御するためにお客様 VM に Kerberos 認証を実装すると、Oracle Cloud Automation が機能しなくなる可能性があります。詳細については、Oracle サポート・ドキュメント 2621025.1 (「ExaCC VM's Support Kerberos Authentication」)[82]を参照してください。

Exadata ソフトウェア・バージョン 22.1.4.0.0.221020 では、お客様 VM に対する Microsoft Active Directory (AD)認証および Lightweight Directory Access Protocol (LDAP)認証を、お客様が ExaDB-C@C 上に実装することが可能です。この構成の場合、ExaDB-C@C の Cloud Automation がサポートされません。ExaDB-C@C のお客様 VM に直接アクセスして AD と LDAP を実装すると、AD および LDAP を構成できます。ExaDB-C@C のお客様 VM の更新 [83]は、Exadata Database Machine イメージの更新プロセス [84]と同じように、イメージの更新として実行されるため、お客様は、AD または LDAP 実装がイメージの更新プロセスにより、どのような影響を受けるかをテストして検証する必要があることに注意してください。パッチ適用サイクルの間、AD または LDAP の一時的な無効化や削除が必要になる可能性を念頭に置き、AD または LDAP の実装と、イメージの更新プロセスに互換性がない場合は、パッチの適用後に、AD または LDAP を元の状態に戻してください。

---

[80] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html
[81] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-implement-sec.html#ol7-firewall-sec
[82] https://support.oracle.com/knowledge/Oracle%20Cloud/2621025_1.html
[83] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-update-exacc-system.html
[84] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmmn/updating-exadata-software.html#GUID-E6090FA9-13B4-4BEF-A28D-73BDC3729C58

お客様 VM へのお客様スタッフのアクセス・コントロール

お客様 VM へのアクセスは、トークンベースの ssh[85]を使用して実装されます。お客様は、OCI クラウド・テナンシの資格証明とコントロール機能を使用して、お客様が指定する公開鍵を、opc ユーザーの /home/oracle/opc/.ssh/authorized_keys ファイルに追加します。説明は、Exadata Database Service on Cloud@Customer インスタンスへのアクセス [86]に関するドキュメントにあります。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担当者は、トークンベースの ssh を使用してお客様 VM にアクセスできるようになります。Oracle Cloud Automation は、お客様の鍵管理システムと統合されません。お客様は、Oracle Linux と互換性のあるテクノロジを使用して、ssh 鍵を管理できます。

データを窃盗から防御するためのコントロール

ExaDB-C@C で実行されているデータベースのユーザー表および表領域に格納されるデータは、オラクルの透過的データ暗号化(TDE)によって暗号化されます。暗号化されたデータを窃盗しても、データの復号が技術的に困難であるため、データの使用は限定されます。アメリカ合衆国の国防総省(DoD)と国家安全保障局(NSA)は、データ保護に AES 暗号化規格を推奨しています。

『Oracle Corporate Security Practices』[87]は、オラクルの社内業務とオラクルがお客様に提供するサービス(ExaDB-C@C サービスを含む)のいずれのセキュリティ管理も網羅しており、従業員や請負業者をはじめとするオラクルの全スタッフに適用されます。これらのポリシーは、ISO/IEC 27002:2013 (旧 ISO/IEC 17799:2005)および ISO/IEC 27001:2013 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。

[85] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/ecc-connecting-to-exacc-system.html
[86] https://docs.oracle.com/en/cloud/cloud-at-customer/exadata-cloud-at-customer/exacc/connect-ssh.html#GUID-C5DAB5B8-1FFA-4122-9181-189561F6E0F1
[87] https://www.oracle.com/corporate/security-practices/corporate/

Operator Access Control による特権アクセス管理

Operator Access Control (OpCtl) [88]は、オラクルのスタッフが ExaDB-C@C インフラストラクチャと ADB-D VM にアクセスできるように管理するためにお客様が使用できる特権アクセス管理(PAM)サービスです。OpCtl は、ExaDB-C@C インフラストラクチャと ADB-D VM からリモート・アクセス可能なすべてのログイン・アカウントを無効にし、お客様が OpCtl アクセス要求を承認した後に、オラクルのスタッフのために特定のコンポーネントに固有の一時的な資格情報をデプロイすることで機能します。『Oracle Operator Access Control for Exadata Cloud@Customer』[89]では、ExaDB-C@C と ADB-D の OpCtl を評価するお客様のセキュリティ・スタッフ向けに詳細を説明しています。

Oracle Data Safe

Oracle Data Safe[90]は、Exadata Cloud at Customer サブスクリプションに含まれるセキュリティ・クラウド・サービスです。Data Safe によって次のことが可能になります。

- データベースのセキュリティ構成の評価
- 構成ドリフトの検出
- リスクの高いデータベース・アカウントを特定し、そのアクティビティを表示
- 監査ポリシーのプロビジョニング
- 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

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 Data Safe の技術アーキテクチャ [91]には、お客様が管理する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への接続をスムーズにし、OCI リージョンの OCI Data Safe サービスに接続する機能があります。

Oracle Database セキュリティ評価ツール(DBSAT)

Oracle Database Security Assessment Tool (DBSAT)[92]は、スタンドアロンのコマンドライン・ツールです。適切な種類の構成情報をデータベースから収集し、現在のセキュリティ状態を評価することで、評価プロセスと規制遵守プロセスを迅速化させるとともに、特定されたリスクを低減する方法を提案します。

DBSAT は追加費用なしで提供されており、次の情報をすばやく確認することができます。

- 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

DBSAT はデータベースとリスナーの構成に関する情報を分析し、不必要にリスクを招く可能性がある構成設定を特定します。また、簡単な構成チェック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の漏洩リスクを低減できます。

---

[88] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html
[89] https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/oracle-operator-access-control-tech-brief.pdf
[90] https://docs.oracle.com/en-us/iaas/data-safe/index.html
[91] https://docs.oracle.com/en/solutions/oracle-data-safe-for-on-prem-database/index.html#GUID-07534FC6-3B10-48E5-BD49-C011D55D1070
[92] https://www.oracle.com/database/technologies/security/dbsat.html

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

『Oracle Access Control Practices』[93]では、ExaDB-C@C インフラストラクチャを把握し、ExaDB-C@C インフラストラクチャにアクセスする必要があるオラクルのスタッフにアクセス権が制限されており、さらに次の詳細が定められています。

- ExaDB-C@C インフラストラクチャにアクセスする権限は、オラクルのポリシーに従ったジョブ・コードとトレーニング・レコードを持つ特定のサポート・スタッフに限定されます。技術的なセキュリティ対策によってこのポリシーは強化されます
- 人材採用、人事異動、退職の各プロセスを自動化することで、お客様のインフラストラクチャにアクセスする権限と、従業員のジョブ・コード、トレーニング・レコード、従業員ステータスへの更新との整合性が確保されるようにします

Oracle Cloud Operations のスタッフには、次の機器を含む ExaDB-C@C インフラストラクチャ・コンポーネントにアクセスし、サポートを提供する権限があります。

- 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

図 6 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。

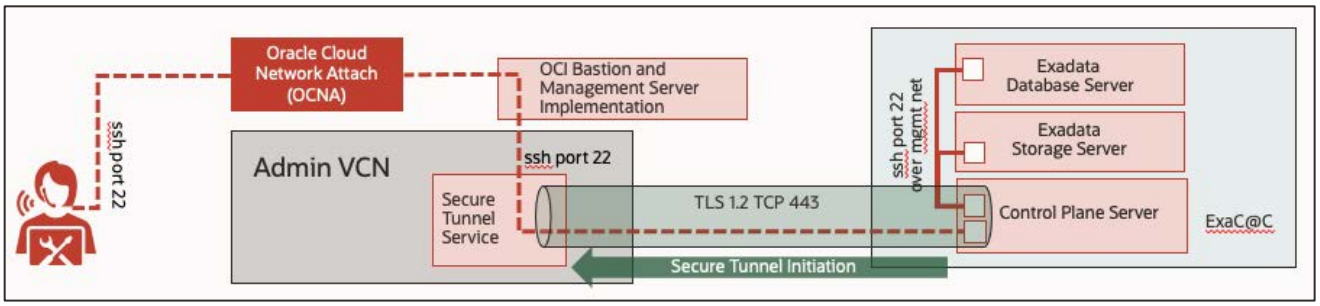

図 6: ExaDB-C@C インフラストラクチャ・コンポーネントへの Cloud Operations スタッフのアクセス

オラクルは、次の手順でクラウド・サービス・インフラストラクチャ・コンポーネントへの Oracle Cloud Ops のスタッフのアクセスをコントロールします。

- Oracle Cloud Network Attach (OCNA)へのアクセスは、Oracle Access Control のプラクティスに従い、ジョブ・コードに固有の資格に基づいて FIPS 140-2 レベル 3 のハードウェア MFA (Yubikey)を使用します
- ExaDB-C@C インフラストラクチャへのプロキシされた ssh トンネル・アクセスを目的とした、踏み台および管理サーバー経由のアクセス
  - サービスをホストする OCI リージョンにある OCI の特権管理 VCN 内で分離された踏み台および管理サーバーを介したアクセス、Oracle Access Control プラクティスによって制御される管理サーバーおよび踏み台サーバーによるアクセスおよびトンネルのエンタイトルメント
  - 踏み台サーバー経由の接続は、オラクルによって記録および監視されます
- FIPS 140-2 レベル 3 ハードウェア・トークン(Yubikey)で実装された MFA を使用して、ssh トンネル経由で名前付きユーザーとして ExaDB-C@C インフラストラクチャにログインします
  - コマンドの実行は、ExaDB-C@C インフラストラクチャに実装された監査ロギングを使用して、特定の名前付きユーザーにまで遡ることができます
  - インフラストラクチャ・コンポーネントに対する接続はオラクルによって記録および監視されます
- 管理タスクの実行において、サービス・アカウントの ID、sudo を使用したサービス・アカウントの認証取得を受け入れます
  - コマンドの実行は、特定の名前が指定できる Oracle 従業員まで辿ることができます
  - 許可されたアクションが実行され、不正なアクションが強制終了されるよう、インフラストラクチャ・コンポーネントに対する接続はオラクルによって監視されます

[93] https://www.oracle.com/corporate/security-practices/corporate/access-control.html

お客様は、Operator Access Control (OpCtl)[94]を適用して、ExaDB-C@C インフラストラクチャと ADB-D VM に対する Oracle スタッフのアクセスをさらに制御することができます。

Exadata インフラストラクチャ・ソフトウェアのセキュリティ

ExaDB-C@C は、Exadata Database Machine を基盤としており、オンプレミスのクラウド・モデルで、Exadata Database Machine に備わるエンタープライズクラスのセキュリティ機能を提供します。ExaDB-C@C のセキュリティ機能には、次のものが含まれます。

- ExaDB-C@C インフラストラクチャにデプロイされるソフトウェアは、お客様のサービスを実行するための最低限のソフトウェア・コンポーネントに限定されます
- 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
- 必須でない OS ツールやパッケージは、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
- ソフトウェア開発は、Oracle Software Security Assurance のもとで行われます [95]
- セキュリティ・アーキテクチャは、Oracle Corporate Security Architecture のもとで実行されます [96]

Exadata Database Machine のセキュリティ機能について詳しくは、オラクルの https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/toc.htm を参照してください。

発見的統制

ExaDB-C@C では、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おいて堅牢な発見的統制(監査およびロギング)が提供されます。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、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管理します。オラクルには、お客様のサービスの監査ログにアクセスする権限はありません。お客様は、オラクルのサービス・リクエスト(SR)プロセスを通して、該当するオラクルの監査ログ情報へのアクセスをリクエストできます。お客様は、https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf で Oracle Data Processing Agreement (DPA)の監査権限を確認することができます。

お客様アクセスのお客様監査ロギング

ExaDB-C@C では、お客様のアクションの監査とロギングのために、次の 3 つの領域を提供します。

- OCI Audit サービス [97]: お客様の OCI IAM 資格証明を使用して開始されたコントロール・プレーンのアクション(Web UI、OCI CLI、OCI REST API など)の監査ログ
- Oracle Database の監査 [98]: お客様の Oracle Database 資格証明を使用して開始されたデータベース・アクションの監査ログ
- お客様 VM OS の監査ログ [99]: OS の資格証明を使用してお客様 VM で開始されたアクションの監査ログ

Oracle Cloud Infrastructure Audit サービスにより、サポートされるすべての Oracle Cloud Infrastructure のパブリック・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が、ログ・イベントとして自動的に記録されます。現在は、すべてのサービスで監査ロギングによるロギングがサポートされます。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 サービスによって記録されるログ・イベントとして、Oracle Cloud Infrastructure コンソール、コマンドライン・インタフェース(CLI)、ソフトウェア開発キット(SDK)、独自のカスタム・クライアント、あるいはその他の Oracle Cloud Infrastructure サービスによって実行された各 API 呼出しが挙げられます。ログには、次の情報が含まれます。

- 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

---

[94] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html
[95] https://www.oracle.com/corporate/security-practices/assurance/
[96] https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
[97] https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm
[98] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/introduction-to-auditing.html#GUID-94381464-53A3-421B-8F13-BD171C867405
[99] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-implement-sec.html#ol7-audit-sec

- 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。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、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。OCI Audit サービス[100]のドキュメントを参照してください。

Oracle Database の監査では、データベース・ユーザーと非データベース・ユーザーが Oracle データベースに加えた変更が追跡されます。お客様には、Oracle Database の監査ログを構成・管理する権利と責任があり、これには、監査ログをリモート・ログ・サーバーに送信する作業も含まれます。Oracle Database の監査ログの構成、管理、監視についてのドキュメントは、各データベース・バージョン向けの『Oracle Database セキュリティ・ガイド』で公開されています。[101]

お客様 VM OS の監査ログは、お客様 VM で実行中の Oracle Linux (OL) OS の監査ログ・サービスとして実装されます。Oracle Linux 監査ログ・サービスにより、OS の資格証明(`root`、`oracle`、`grid`、`opc` など)およびお客様が構成した名前付きユーザーによって実行されたアクションが記録されます。お客様には、自社の標準に従って Oracle Linux 監査ログを構成する責任があります。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作業も含まれます。ドキュメントは、お客様 VM で実行されている OS の特定バージョン向けの『Oracle Linux セキュリティ・ガイド』[102]で公開されています。

お客様は、CPS とインターネット間のネットワーク・アクセス、お客様 VM へのネットワーク・アクセス、お客様 VM からお客様のデータ・センターへのネットワーク・アクセスなど、自身がコントロールするネットワーク・アクセスをどの時点でも監視できます。

Oracle アクセスのお客様監査ログ

お客様は、オラクル・スタッフの ExaDB-C@C インフラストラクチャと ADB-D VM へのアクセスに対する追加の発見的統制として、Oracle Operator Access Control[103]を使用することができます。Operator Access Control は、オラクル・スタッフが ExaDB-C@C インフラストラクチャと ADB-D VM にアクセスする際に入力したすべてのコマンドとキーストロークのログを記録します。Operator Access Control の監査ログは、OCI Logging サービスおよび CPS からお客様指定の syslog サーバーへの直接送信により利用可能です。詳細は『Oracle Operator Access Control for Exadata Cloud@Customer』[104]をご覧ください。

お客様によるお客様 VM のセキュリティ・スキャン

お客様は OpenSCAP[105]を使用して、お客様 VM でセキュリティの脆弱性をスキャンできます。

お客様は、Oracle Linux Advanced Intrusion Detection Environment (AIDE)[106]を使用してファイルおよびディレクトリの整合性をチェックできます。AIDE は、Linux 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。オンデマンドで実行され、変更をレポートする時間はシステム・チェックに依存します(通常は 1 日に 1 回以上)。このユーティリティは、多数のアルゴリズム(md5、sha1、rmd160、tiger など)を使用して動作し、一般的なファイル属性をサポートし、スキャンに含める、あるいは除外するファイルの正規表現パーサーもサポートしています。

---

100 https://docs.cloud.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm
101 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。
102 https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-audit-sec.html
103 https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html
104 https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/oracle-operator-access-control-tech-brief.pdf
105 https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-scap-sec.htm
106 https://support.oracle.com/knowledge/Oracle%20Linux%20and%20Virtualization/2616282_1.html

お客様は、スキャン・ソフトウェアを含むサード・パーティ・ソフトウェアを ExaDB-C@C のお客様 VM にインストールすることができます。オラクルは、オラクル以外のソフトウェアに対する技術サポートは行いません。これには、インストール、テスト、認証、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 および、または Exadata 環境での使用が認定されており、お客様によって対象環境でのテストが徹底的に実施されていることが強く推奨されます。ExaDB-C@C でのサード・パーティ・ソフトウェアのサポートの詳細は、My Oracle Support の「Installing Third Party Software On Exadata Components」(Doc ID 1593827.1)[107]で公開されています。

お客様による ExaDB-C@C のお客様 VM のセキュリティ・テストは Oracle Cloud のテスト・ポリシー[108]に従って実行される必要があります。

[107] https://support.oracle.com/knowledge/Oracle%20Cloud/1593827_1.html
[108] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm

オラクルの監査ロギング

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

- ILOM
  - `syslog`
  - 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 `syslog`
- 物理的な Exadata Database Server
  - `/var/log/messages`
  - `/var/log/audit.log`
  - `/var/log/secure`
  - `/var/log/xen/xend.log`
- Exadata Storage Server
  - `/var/log/messages`
  - `/var/log/audit.log`
  - `/var/log/secure`
- ストレージ・ネットワーク・スイッチ
  - `/var/log/messages`
  - `/var/log/audit.log`
  - `/var/log/secure`
  - `/var/log/opensm.log`

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

- ILOM
  - `syslog`
  - 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 `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`

Oracle infrastructure 監査ログの保存期間は 13 か月です。インフラストラクチャ監査ログは、オラクルのセキュリティ・スタッフがアクセスできます。疑わしいセキュリティ・インシデントが発生した場合は、オラクルの担当者とお客様担当者が協力して、Oracle Incidence Response[109]に従って問題を解決します。

対応的統制

お客様とオラクルは連携してお客様のサービス、データベース、データベース・データ、VM、インフラストラクチャへのアクセスを保護、監視します。お客様とオラクルのいずれかが不正なアクションを検出した場合、検出した側は、セキュリティ・ポリシーや不正アクションの詳細と状況に応じて、相手側に通知する前に、即座に対応策を講じることができます。お客様が不正なアクションを検出した場合は、お客様は Oracle SR プロセスを通して、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。一方オラクルも、検出した不正アクションとオラクルの対応をお客様に通知します。

お客様は、自身がコントロールするあらゆるサービスや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、お客様 VM へのネットワーク接続や、CPS と OCI リソース間のネットワーク接続を強制終了することもできます。お客様が CPS と OCI リソース間の接続を強制終了した場合も、データベース・サービスとデータベースは引き続き正常に機能し、お客様のこの対応によって強制終了された権限のあるアクションはすべて再開できます。

お客様は、Operator Access Control[110]を使用して、ExaDB-C@C インフラストラクチャおよび ADB-D VM へのオラクル・スタッフのアクセスを終了させることができます。

---

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

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、CPS における接続の強制終了、ExaDB-C@C リソースに対するアクセスの取消しなどが含まれます。

サービスの終了

お客様は、ExaDB-C@C ライフサイクル管理業務の一環として、ExaDB-C@C インスタンスを終了させることができます [111]。Exadata Cloud Service のリソースを終了させると、そのリソースとその上で動作しているすべてのデータベースは永久に削除されます。サービスの終了機能は、Exadata Database Machine Secure Erase[112]として実装されています。Exadata Secure Eraser は、ストレージ・デバイスのハードウェア機能を自動的に検出し、デバイスでサポートされる最適な消去方法を選択します。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。Secure Erase の証明書は、My Oracle Support (MOS)リクエストをオープンして、オラクルから取得できます。

例外ワークフロー - お客様 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お客様の 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。オラクルの担当者によるお客様 VM へのアクセス方法を管理するプロセスと技術的なコントロールは、お客様がお客様 VM にアクセスできるか、そうでない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コントロールについては、次の項で説明します。

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可能な場合、オラクルの担当者はオラクルが管理するインフラストラクチャ・コンポーネントからお客様 VM へのアクセスを許可されることはありません。かわりにお客様の担当者は、お客様の資格情報を使用してお客様 VM にアクセスする必要があり、その後、お客様の担当者は画面共有の技術(例: Zoom、Webex、Skype など)を使用して、お客様 VM へのアクセスを共有することができます。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
- オラクルとお客様担当者は、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お客様 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

お客様 VM にお客様が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場合、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 Technology (実装されている場合)を通じて、お客様とオラクルが共同で次のようにコントロールします。

- お客様が直接監督していなくても、Oracle Cloud Ops がお客様 VM にアクセスしてかまわない場合は、お客様が、次の内容でサービス・リクエスト(SR)をオープンします。
  - SR のタイトル:

---

[110] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html
[111] https://docs.oracle.com/en/cloud/cloud-at-customer/exadata-cloud-at-customer/exacc/delete-exadata-service-instance.html
[112] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/exadata-secure-erase.html#GUID-6C9FD30C-FF88-4ABA-9249-93E183784B0D

        - 「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 名を入力します>
    - 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: <ここには、VM をホストしている DB サーバーの OCID を入力します>
        - 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 名を入力します>
- Oracle Cloud Ops によるアクセスを、お客様が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は、お客様が、次の内容でサービス・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 名を入力します>
    - 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 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: <ここには、VM をホストしている DB サーバーの OCID を入力します>
        - 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 名を入力します>
- 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 Access Request を開きます。お客様は Operator Access Control Access Request 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、お客様のデータ・センタ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)のお客様が指定した syslog サーバーに、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場合、オラクルは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。

DATA PROCESSING AGREEMENT の監査

ExaDB-C@C サービスの一環として、お客様は、オラクルが Data Processing Agreement (DPA)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。『Data Processing Agreement for Oracle Services』[113]には、お客様が監査を要求する方法と監査が行われる方法が詳しく記載されています。

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[114]は、ExaDB-C@C のオプションのアドオン・サービスです。Oracle DDR は、お客様が、お客様の ExaDB-C@C サブスクリプションのためにお客様のデータ・センターにオンサイトで設置された ExaDB-C@C のハードウェア・システムから削除された、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)を保持することを許可します。

[113] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
[114] https://www.oracle.com/assets/customer-data-device-retention-sd-4419287.pdf

DDR を目的とする場合、保持されたハードウェアは次のものを指します。

- 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)

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、お客様は、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・テナンシ内のクラウド・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をコントロールする責任をお客様が負うことがあります。これらの要件を満たすために、オラクルのお客様は、Exadata Database Service on Cloud@Customer (ExaDB-C@C)および ExaDB-C@C 上の Autonomous Database Dedicated (ADB-D)で Oracle Operator Access Control[115] (OpCtl)を使用することができます。

OpCtl は、ExaDB-C@C の Oracle Cloud Infrastructure (OCI)の特権アクセス管理(PAM)サービスです。OpCtl は、次のお客様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時期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、オラクルのお客様は追加コストなく利用することができます。

OpCtl は、お客様が Oracle Cloud Ops のスタッフによるインフラストラクチャへのログインをコントロールし、お客様が管理するシステムにお客様担当者がアクセスする際に適用されている基準と同一にしなければならないユース・ケースに適した機能です。OpCtl 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。

OpCtl の予防的セキュリティ・コントロール機能には、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時期をコントロールできます
- ソフトウェアによるオラクルの担当者の特権エスカレーションの実施

OpCtl の発見的セキュリティ・コントロール機能には、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のお客様への通知
- 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
- 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に対するお客様によるセキュリティ監視
- コマンド実行において必要な場合、オラクルからお客様に提供されたオラクル担当者のアイデンティティの記録

OpCtl の対応的セキュリティ・コントロール機能には、次のものがあります。

- オラクル・スタッフのアクセスを停止させるお客様のコントロール
- オラクル・スタッフが開始したプロセスを終了させるためのお客様のコントロール
- 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削除するためのお客様のコントロール

---

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

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 [116]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、OpCtl アクセス・リクエストを処理する目的で、OCI Event[117]および Notifications[118]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』[119]を参照してください。

お客様は OpCtl サービスと互換性のあるサード・パーティのソフトウェア製品に OpCtl 監査ログを統合することができます。これには、OpCtl 監査ログのお客様指定の syslog サーバー[120]への送信や、OCI Logging サービスと Splunk の統合 [121]が含まれます。

ExaDB-C@C インフラストラクチャの OpCtl サービスに関する詳細な説明は、Operator Access Control[122]製品のドキュメントに記載されています。OpCtl サービスの概要は、『Oracle Operator Access Control for Exadata Cloud@Customer』[123]に記載されています。

まとめ

お客様 VM およびお客様の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 サービス・コンポーネント全域にわたるセキュリティ機能と監査機能により、Oracle Cloud Operations のスタッフが、権限のあるアクションのみを ExaDB-C@C のインフラストラクチャ・コンポーネントで実行することが保証されます。セキュリティ対策として、名前付きユーザーの多要素認証、定期的にローテーションされる強力なパスワード、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トークンベースの SSH アクセスが使用されます。監査とロギングはスタック全体に実装され、お客様はオラクルのサービス・リクエスト(SR)プロセスをとおしてリクエストを行うことで、監査ログを入手できます。

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確保し、お客様データの不正アクセスと窃盗を防止します。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。

---

[116] https://docs.oracle.com/en-us/iaas/operator-access-control/doc/auditing-operator-access-control-lifecycle-events.html#GUID-1C819283-0660-4828-8E11-09D897211436
[117] https://docs.oracle.com/en-us/iaas/Content/Events/Concepts/eventsoverview.htm
[118] https://docs.oracle.com/en-us/iaas/Content/Events/Concepts/eventsoverview.htm
[119] https://www.ateam-oracle.com/post/a-simple-guide-to-managing-oci-alarms-in-servicenow
[120] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-6526ADE1-C664-4600-A62B-5993EA25134E
[121] https://docs.oracle.com/en/solutions/logs-stream-splunk/index.html
[122] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-7CF13993-DB16-485A-A9FA-399E0049740B
[123] https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/oracle-operator-access-control-tech-brief.pdf

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
February 2424