ORACLE CLOUD

クラウド・データベースの多層防御

クラウドとオンプレミスの
データベース・セキュリティの統合

Oracle ホワイト・ペーパー | 2017 年 3 月

著者：データベース・セキュリティ担当 PRINCIPAL PRODUCT MANAGER Dinesh Rajasekharan

ORACLE

目次

概要

クラウド・コンピューティングは、運用の柔軟性とコストによって情報技術（IT）に変革をもたらしています。組織はクラウド・コンピューティングの採用を急速に進めていますが、多くの組織ではミッション・クリティカルなアプリケーションをオンプレミスで使用し続けており、移行はまだなお進行中となっています。クラウドへの移行は費用効果に優れた選択肢ではあるものの、アプリケーションの可用性、ネットワーク待機時間、ネットワーク・スループットを懸念する組織もあります。一部の組織にとっては、さまざまなプラットフォーム・コンポーネントやアプリケーション・コンポーネントが存在するために、オンプレミスのアプリケーションを"リフト・アンド・シフト"するのは簡単なことではありません。ただし、すべての組織が"セキュリティ"という共通の懸念を持っています。データ侵害がますます増加する中で、共有のインフラストラクチャであることと、直接制御できないことが、クラウドの採用を検討している組織にとってもっとも大きな懸案事項となっています。

オンプレミスかクラウドかに関係なく、データベースは機密データのリポジトリであるため、攻撃者にとって恰好の標的となっています。さらに、EU の一般データ保護規則（GDPR）などの規則には、個人情報を保護し、悪影響の及ぶデータ侵害を個人に知らせなければならない企業の責任が規定されています。このホワイト・ペーパーでは、クラウド・データベースの機密データを保護し、さらにオンプレミスで制御を維持し続ける手法について説明します。

データベースは引き続き攻撃者の恰好の標的に

データ侵害は毎日のように報道されているため、セキュリティ研究者は、侵害は現在トップニュースとして報道されているものの、徐々に大きく扱われなくなることを心配しています。攻撃者は現在、クレジットカードや財務情報に加えて、知的財産（IP）、個人情報（PII）、および個人健康情報（PHI）を標的にしています。このような侵害で、データベースが直接標的となったこともあります。たとえば、最近では米国人事管理局から 2,150 万人分の記録が流出したり、米国有権者データベースから 1 億 9,100 万人分の記録が流出したり、バングラデシュ中央銀行から 8,100 万ドルが盗み出されています。

データベースは情報の倉庫であり、格納されているのはすべて機密情報であるため、データベースは引き続き攻撃者にとってもっとも魅力のある標的となっています。組織では、ファイアウォールや侵入検知システムなどのセキュリティを多層化することで、データベースへのアクセスを強固にしています。ただし、近年の攻撃では、ユーザー、管理者、開発者、テスト担当者、パートナー、外部委託のサービスといった、データベースへの正規のアクセス権が付与されたチャネルが利用されています。IT 環境の急速な進化やアジャイル開発手法の採用により、データベースに直接アクセスするチャネルの数が増加しており、このようなアクセスの頻度も増加しています。データベースを直接セキュリティで保護し、攻撃対象領域を減らし、攻撃者がデータベースに到達できる手段を減らすことが、ますます重要になっています。データベースを直接セキュリティで保護するには、セキュリティ制御をデータベースの近くに配置する必要があり、可能であれば、データベース自体に組み込む必要があります。

次の図は、データベース・ユーザー、データベース管理者（DBA）、テスト担当者、開発者、アプリケーション・ユーザー、サポート・ユーザーといったさまざまな脅威関係者を介して、IP、PII、PCI、PHI が保存されているデータベースを攻撃者がいかにして標的としているかを示しています。

図1：データベースは引き続き攻撃者にとって魅力的な標的に

クラウド向けのデータベース

一般にパブリック・クラウドは次の 3 つの領域に分類されます。

» Software as a Service（SaaS）

» Platform as a Service（PaaS）

» Infrastructure as a Service（IaaS）

オンプレミスの IT スタックと同様に、データベース（PaaS の一部として使用）はミッション・クリティカルなビジネス・データが格納され、クラウド・スタックの中核となっています。データベースはアプリケーション（SaaS）の基盤であるため、基盤インフラストラクチャ（IaaS）と統合する必要があります。

Oracle Database Cloud Service は、多様なデータベース構成を提供しているため、さまざまな組織のニーズに対応します。開発者は、アプリケーション・モジュールのコーディングをすぐに開始できるよう、低コストのスキーマがあれば済むでしょう。テスト担当者は、データを迅速にプロビジョニングできるデータベース・スキーマやデータベースが必要となるでしょう。書店などの小規模企業では、低コストの単一インスタンス・データベースが必要となるでしょう。大企業では、ミッション・クリティカルなアプリケーションをホストする本格的なデータベースが必要となるでしょう。次の表に、使用可能な Oracle Database Cloud Service の一部をまとめます。

Cloudデータベースのエディション	ユースケース
Live SQL	クラウド導入に適したコスト・ゼロのサービス
Exadata Express Cloud Service	中小サイズのデータを対象にしたアプリケーション開発用の完全なマネージド・サービス
Oracle Database Cloud Service	高度な機能をすべて備えた完全なOracle Database
Database Cloud Service – ベア・メタル	Oracle Database Cloud Serviceおよび専用ハードウェアとローカルNVMeストレージのパフォーマンス
Exadata Cloud Service	大規模なアプリケーションに適した世界最速のデータベース・マシン

低コストのデータベースを実行するか、エンタープライズ・クラスのデータベースを実行するかに関係なく、大規模な侵害が発生しているこの時代に、データ・セキュリティに関して妥協することは許されません。また、オンプレミスなのかクラウドなのかに関係なく、すべてのデータベースにわたって堅牢で一貫性のあるデータ・セキュリティ手法を適用する必要があります。このホワイト・ペーパーで説明するオラクルのデータ・セキュリティ手法は、オンプレミスの Oracle Database、およびもっともよく使用されている Oracle Database Cloud Service で採用されています。

ハイブリッド・クラウド・モデル - 現状

» パブリック・クラウド

アプリケーション、プラットフォーム、インフラストラクチャの各コンポーネントをクラウド・プロバイダーのデータセンターでホストしている場合、基盤となるリソースを複数のテナントやサブスクライバーが共有します。オラクルなどのクラウド・ベンダーは、共有プラットフォーム・モデルに加えて専用プラットフォームも提供しています。

» プライベート・クラウド

アプリケーション、プラットフォーム、インフラストラクチャの各コンポーネントは、サブスクライバーまたは顧客のデータセンターでホストされ、マルチテナント、オンデマンドの拡張、サブスクリプション・ベースの価格といったクラウドのすべての特性が適用されます。オラクルなどのクラウド・ベンダーは、完全なマネージド・サービスを通じてプロフェッショナル・サービスや技術的な専門知識を提供しています。また、オラクルは、Oracle Cloud Machine を使用してプライベート・クラウドとパブリック・クラウドのインフラストラクチャ間で移行する、追加機能も提供しています。

» ハイブリッド・クラウド

今日、さまざまな企業が開発ニーズやテスト・ニーズに対応するためにパブリック・クラウドを検討していますが、ミッション・クリティカルな本番アプリケーションは依然としてオンプレミスです。オンプレミスのアプリケーションはストレージ、データベース、アプリケーション・サーバー、Web サーバーなどの複数のコンポーネントが関連しており、その複雑さと重要性から、これらの企業では、クラウドの採用やクラウドへの移行は引き続き、検討中の項目となる見込みです。

これらの企業がクラウドを全面的に採用する場合でも、ミッション・クリティカルな本番アプリケーションにはプライベート・クラウドを使用する可能性が高いです。そのときまで、これらの企業はオンプレミス・アプリケーションとクラウド・アプリケーションが混在したハイブリッド・クラウド・モデルで運用を継続することになります。オンプレミス・プラットフォームとクラウド・プラットフォームを透過的につなぐ共通の統合フレームワークを使用すると、クラウドの採用が簡単になり、習得も最短期間で行え、移行が促進されます。

クラウドによって生じる、データ・セキュリティに関する新たな懸念

データのプライバシとセキュリティが、クラウドへの移行を検討している組織にとってもっとも大きな懸念となっている場合があります。これらのデータ・セキュリティに関する主な懸念のいくつかについて、以下トピックで概要を説明します。

クラウド・プロバイダーがデータを紛失や盗難から保護できるか

パブリック・クラウドは、データ管理、ガバナンス、コンプライアンスに複数の管理者やプロセスが関与している多くの組織にとってブラック・ボックスです。データのバックアップ、エクスポート、レプリケート、統合が頻繁に行われるため、組織はクラウド・プロバイダーがデータを紛失や盗難から保護できるのか懸念しています。

現行のデータ侵害、訴訟、政府/規制機関の関与、数百ものアプリケーションや関連コンポーネントで生成されるデータ量を考慮し、企業はクラウド内のデータを制御できないことを懸念しています。

基盤となる計算能力とネットワークの他の顧客との共有

パブリック・クラウドでは一般に、共通のサーバーを使用し、仮想マシンによって複数のテナントや顧客のアプリケーションをホストしています。DoS（サービス拒否）などの攻撃が共有サーバー・モデルにホストされているすべてのアプリケーションに波及する可能性があるため、組織はサーバーを第三者と共有することを大きく懸念しています。

誰が、いつ、どのようにデータにアクセスするか

企業では、誰が、いつ、どのようにクラウドのデータにアクセスするかが明確ではありません。たとえば、次の例が挙げられます。

» 誰がデータにアクセスするのか。エンドユーザー、クラウド管理者、サードパーティ・クラウド・プロバイダーがアクセスするのか（たとえば、提供している SaaS を別のクラウド・プロバイダーの IaaS にホストしているプロバイダーや、運用をマネージド・サービス・プロバイダーにアウトソースしているプロバイダーもあります）。

» いつデータにアクセスするのか。アクセスにどのようなチャネルを使用するのか。

» ネイティブのクラウド管理者とサードパーティのクラウド管理者が個人情報、財務情報、知的財産（IP）などの機密情報を閲覧していないことをどのように確認するのか。

» データ・アクセスのさまざまな側面をどのように監査するのか。攻撃者が監査レコードを改ざんした場合はどうなるのか。

オンプレミスとクラウドのデータを一様に保護するための戦略

オラクルのクラウド・データ・セキュリティは、クラウド・データの保護に関する主な懸念に対処する、以下の原則に基づいて構築されています。

» セキュリティが常時オン

Oracle Cloud では、暗号化や監査などの基本的なデータ・セキュリティ機能が常時オンになっています。

» セキュリティをスタック内に適用する

攻撃対象領域を縮小し、攻撃者がデータベースにアクセスできる手段を減らすためには、可能な限りデータの近くでセキュリティを適用することが重要です。また、データにセキュリティを組み込むことで、アプリケーションとデータの中断やパフォーマンスの低下を最小限に抑えています。

» 顧客によるデータ制御を確立する

組織は大量のデータを継続的にクラウドにアップロードしているため、オラクルは、オンプレミスから悪意のあるアクティビティを監視、検出し、データへのアクセスを拒否する、Key Vault、Audit Vault and Database Firewall などのハイブリッド・クラウド・テクノロジーを提供しています。

» データベース管理者（DBA）による機密データへのアクセスを制限する

Oracle Cloud では、クラウドのサブスクライバーとプロバイダーの DBA による機密情報へのアクセスを制限し、内部関係者による攻撃を軽減するとともに、チューニング、バックアップ、パッチ適用などの日々の操作を実行する際に使用する、Database Vault などの独自のテクノロジーを提供しています。

» オンプレミスまたはクラウドのデータを匿名化する

多くの組織が開発やテストにクラウドを使用し始めているため、Oracle Cloud では、オンプレミスまたはクラウドの機密情報を匿名化する Data Masking and Subsetting を提供しています。このアプローチは、意図的または偶発的な機密情報の漏えいを軽減し、コンプライアンスの適用範囲を最小限に抑えるものです。

» オンプレミス環境とクラウド環境間でセキュリティ・ポリシーを透過的に移行する

企業によるハイブリッド・クラウド・モデルでの運用を支援するために、Oracle Enterprise Manager は統合型のユーザー・インタフェースを備えており、オンプレミス環境とクラウド環境間でセキュリティ・ポリシーを移行、管理できます。

このホワイト・ペーパーではこれ以降、Oracle Cloud のデータ・セキュリティの原則とテクノロジーについて説明します。Oracle Cloud のネットワークとインフラストラクチャのセキュリティについては、次のホワイト・ペーパーを参照してください。

ホワイト・ペーパー：『Oracle Infrastructure and Platform Cloud Services Security』

暗号化を常時オンにし、データ紛失/盗難時の侵害を最小限に抑える

現在の IT 環境では、データが複数のデータソースにまで大幅に増加していることが多く、機密情報を追跡し続けるのが難しくなっています。

以下のシナリオについて検討します。

- クラウドでデータがバックアップされる頻度はどの程度か
- バックアップ、保存、アーカイブの場所はそれぞれどこか
- 組織からクラウドへのデータ送信に使用するチャネルとして、どのようなチャネルがあるか（ダンプのエクスポート、テープのバックアップ、クローン、メールなど）
- 古くなったバックアップ、テープ、ダンプは適切に破棄されるか
- データ・アーカイブについてはどうか
- テープ、ディスク、ダンプ、アーカイブが紛失した場合や攻撃者によって盗み出された場合、どうなるか
- 攻撃者がネットワークに侵入してデータ・パケットを盗聴した場合、どうなるか

データベース・ファイル、バックアップ、データ・ダンプ、アーカイブ、ストレージ、テープ、ネットワーク・パケットが適切に管理されていない場合、データの紛失や盗難につながる恐れがあります。

データを保存時および転送時に暗号化すると、データの紛失や盗難が発生したときに侵害を最小限に抑えるのに役立ちます。PCI-DSS や EU の一般データ保護規則（GDPR）などのデータ保護法や規格では、セキュリティ制御の一環として暗号化を義務付けています。Oracle Cloud では、保存中のデータと転送中のデータはデフォルトで暗号化され、パフォーマンスへの影響はごくわずかです。

Oracle Cloud データベースへの転送時に、データベース・ネイティブのネットワーク暗号化を使用してデータはデフォルトで暗号化されます。ネイティブのネットワーク暗号化以外に、業界標準の SSL/TLS ネットワーク暗号化も構成可能です。SSL/TLS ネットワーク暗号化を構成すると、クライアント証明書を使用した相互認証を実行できます。すべてのネットワーク暗号化オプションで、Advanced Encryption Standard（AES）や 3DES などの強力な暗号がサポートされています。整合性チェックでは、SHA-256 などの最新のハッシュ・アルゴリズムがサポートされています。

Oracle Database Cloud Service で保存中のデータは、透過的データ暗号化（TDE）を使用してデフォルトで暗号化されます。TDE では、ユーザーが作成した表領域内のデータを、SQL の CREATE TABLESPACE コマンドを使用するか任意のツールを使用して AES-128 アルゴリズムで暗号化します。必要に応じて、鍵のサイズを 192 ビットまたは 256 ビットに増やすことが可能です。また、RMAN のバックアップや Data Pump のエクスポートを暗号化することも可能です。データベースの最適化は、すでに暗号化されている表領域データにまで及び、必要に応じてデータ・ストリーム全体が暗号化されます。バックアップとエクスポートを、表領域の暗号化に使用したのと同じ鍵、パスワード、または両方を使用して暗号化できます。

データの暗号化に使用するマスター暗号化鍵は自動的に作成され、データベース・ウォレット（PKCS-12 および PKCS-5 準拠の鍵格納ファイル）ごとに保存されます。以前のマスター鍵は、今後リストアが必要となる可能性がある、暗号化されたバックアップ用のウォレットに保持されます。多数のオンプレミス・データベースとクラウド・データベースで複数の暗号化鍵、ウォレット、Java キーストアを使用する場合は、一元的な鍵管理ソリューションである Key Vault を使用することを推奨します。次の項では、Oracle Key Vault について詳しく説明します。

Oracle Key Vaultを使用し、1回のクリックで攻撃者がデータを使用できなくする

暗号化の強度は、暗号化鍵を安全かつ効率的に管理できるかどうかによって決まります。攻撃者が暗号化鍵を入手したら、暗号化ソリューションは役に立たなくなります。また、鍵管理が効率的でないと、運用のオーバーヘッドが膨大になり、データ損失にもつながります。多くの組織では、データベース、アプリケーション・サーバー、ストレージ、オペレーティング・システム、アプリケーションといった複数の IT 資産にわたって暗号化鍵、ウォレット、Java キーストア、および資格証明を管理し、ローテーションを行うというのは、簡単なタスクではありません。Oracle Key Vault では、こうした課題に対処するため、暗号化鍵、ウォレット、Java キーストア、資格証明ファイルを一元管理できるようにしています。

Oracle Cloud 固有の差別化要因の 1 つに、組織がオンプレミスでデータ制御を確立できるようにするという点があります。Oracle Key Vault は、オンプレミスで暗号化鍵を管理し、疑わしいアクティビティが発生した場合は、ボタンを 1 回クリックすれば対応するクラウド・データベースへのアクセスを中断する機能を備えており、顧客がデータ制御を確立する上で重要な役割を果たします。

Oracle Key Vault は、フル・スタックで強固なセキュリティを備えたソフトウェア・アプライアンスであり、Oracle Linux および Oracle Database テクノロジーを使用してセキュリティ、可用性、およびスケーラビリティを実現します。Key Vault に保存されている暗号化データを保護する鍵階層の"信頼の起点"として、業界標準の OASIS KMIP（Key Management Interoperability Protocol）およびハードウェア・セキュリティ・モジュール（HSM）をサポートしています。ブラウザベースの管理コンソールを備えており、管理が簡素化されます。また、RESTful API を使用してさまざまな管理タスクや鍵管理タスクを自動化することが可能です。

Oracle Key Vault 12.2 以降をオンプレミスにデプロイすると、Oracle Database Cloud Service の透過的データ暗号化（TDE）鍵を管理できます。図 2 は、Key Vault のハイブリッド・クラウド管理アーキテクチャを示しています。

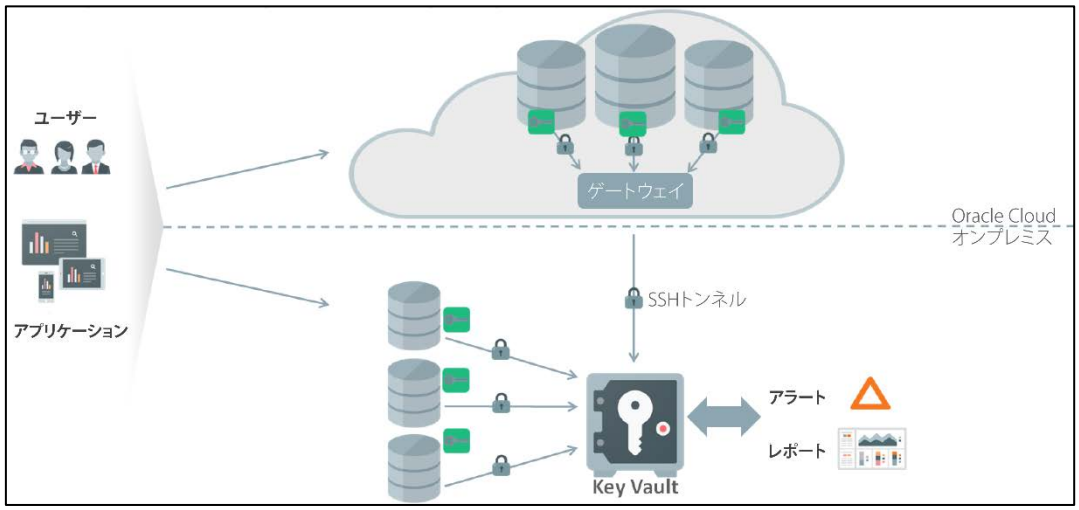

図2：Oracle Key Vaultによる、ハイブリッド・クラウド環境での鍵管理

クラウド・データベースの構成とコンプライアンスを比較する

オンプレミスとクラウドにデータベースを分散させており、各データベースにチューニング可能な構成パラメータが多数存在する場合、データベースの構成をいかに監視、同期化、保護するかが課題となります。Oracle Cloud は、構成機能とコンプライアンス管理機能を提供することで、この課題に対処します。

構成機能とコンプライアンス管理機能は、Oracle Enterprise Manager Database の Lifecycle Management Pack に含まれており、オンプレミスの Oracle Enterprise Manager が必要です。この機能は、オンプレミス・データベースとクラウド・データベースの構成を比較するのに役立ち、構成がセキュアであり、時間とともにずれることなく、最新のベスト・プラクティスが適用されていることを確認できます。すぐに使用できる 100 を超えるポリシー・チェックを Oracle Database に対して実行し、傾向を把握し、最適設定からのずれを監視できます。また、カスタム構成チェックを定義してオラクル標準のチェックを補完することもできます。Database Lifecycle Management は、Oracle Database Cloud Service の各エディションに含まれています。

自社DBAだけでなく、クラウド管理者による機密情報へのアクセスも制限する

特権ユーザー・アカウントへの偶発的または意図的な不正アクセスによるデータ侵害は、もっとも多い攻撃形態の 1 つです。通常、組織では、複数のデータベース管理者（DBA）がさまざまなアプリケーションを管理しています。Software as a Service（SaaS）やマネージド・クラウド・サービスの場合は、クローニング、パッチ適用、保守などの日々のデータベース管理タスクはクラウド・ベンダーのデータベース管理者（DBA）が行います。

特権ユーザーに対する攻撃が増加している中で、クラウド DBA のアクティビティに対する制御が限られているため、組織ではクラウドの採用に関してジレンマを抱えています。厳密な職務分離（SOD）を実施してデータ・プライバシ法や規格に準拠する必要がある金融機関や医療機関などの企業では、クラウド DBA のアクティビティを制御できないことに、さらに大きな懸念を持っています。オラクルが Database Vault を開発するまで、“データベース管理者”と“機密データのロックダウン”が両立することはありませんでした。

Oracle Database Vault は、Oracle Database に組み込まれたオラクル独自のセキュリティ制御であり、特権データベース・アカウント（クラウド DBA を含む）に対して機密情報へのアクセスを制限しながら、これらのアカウントでバックアップやパッチ適用などの日々のアクティビティを実行できるようにします。

Oracle Database Vault は、セキュリティ管理、アカウント管理、および日々のデータベース管理のアクティビティを 3 つの職務を明確に分離する制御機能を適用することで、顧客によるデータ制御を確立します。アプリケーション・スキーマ、機密テーブル、およびストアド・プロシージャのデータ・レルムを作成し、ハッカーや内部関係者が特権アカウントを悪用して機密アプリケーション・データにアクセスするのを防ぎます。Oracle Database Vault の SQL コマンド制御により、データベース内部での操作（表作成、表切捨て、ユーザー作成などのコマンドを含む）を制御できます。組込みのさまざまなファクタ（IP アドレス、認証方式、プログラム名など）を使用して、盗まれたパスワードによる攻撃を防止する複数ファクタ認可を実装できます。これらの制御機能により、誤った構成変更を防止するとともに、ハッカーや悪意のあるインサイダーによるアプリケーションの改ざんも防止できます。

Oracle Database Vault は Oracle Database Cloud Service の各エディションに含まれており、Oracle Fusion SaaS の各モジュールでフル・マネージドのサブスクリプション・サービスとしても提供されています。

マスキングとサブセット化により、機密性の高い本番データの漏えいを制限する

多くの組織は、クラウドにはコスト面と運用面でメリットがあることを認識しています。このような組織は、"クラウドとは"や"なぜクラウドなのか"といった段階はすでに通過しています。ここでは、ユースケースについて説明します。当面は開発やテストといった本番以外のユースケースでニーズがありますが、これらの組織では機密性の高い本番データをテスト目的や開発目的で使用することを懸念しています。さらに、本番データ全体をテスト環境や開発環境にコピーするというのは、コストが増加し、セキュリティ境界が広くなり、本番からテストへのプロビジョニングに遅れが生じる可能性があります。これに対して、中小企業（SMB）では、パブリック・クラウドを本番と本番以外の両方のユースケースに利用できます。プライバシやコンプライアンス上の理由から、まずは、実際のデータではなくテスト・データを使用してクラウド・インフラストラクチャを評価するというのが、もっとも可能性が高いです。

大企業か SMB かに関係なく、開発環境とテスト環境によってクラウド採用への道が開かれます。ただし、開発環境やテスト環境には本番データのコピーが含まれるため、こうした環境は攻撃の標的となる可能性があります。EU の一般データ保護規則や PCI-DSS などのデータ・プライバシ法や規格では、機密性の高い本番情報をテスト目的や開発目的に使用する場合、これらの情報を匿名化することを推奨しています。

Oracle Cloud は、機密データのマスキングとサブセット化を行えるため、組織がクラウド採用を促進しながらデータ・プライバシやコンプライアンスを確保するのに役立ちます。Data Masking and Subsetting は Oracle Cloud の差別化要因となっており、データベースからアプリケーション・データの全体コピーまたはサブセットを抽出し、個人データを匿名化および最小化できます。そのため、開発者、テスト担当者、パートナー、その他の第三者が安全にデータを共有できます。データベースの整合性が維持され、アプリケーションの継続性が確保されます。

匿名化の課題の 1 つは、適切に処理されないと、攪乱して識別不能化されたデータはテスト担当者や開発者が使えなくなる場合があることです。さらに、アプリケーションやデータベースのデータ整合性を壊す可能性があります。Oracle Data Masking and Subsetting では、こうした課題に対処するため、機密性の高い列と親子関係を再利用可能なアプリケーション・データ・モデルに取得できるようにしています。また、マスキング・フォーマット、ファンクション/変換、アプリケーション・テンプレートの包括的かつ拡張可能なライブラリを利用できます。クレジットカード番号、国民識別番号やその他の個人情報（PII）のような機密性の高い個人データは、マスク・フォーマットと匿名化フォーマットの組込みライブラリを使用して簡単にマスキングできます。

Data Masking and Subsetting は、Oracle Enterprise Manager のデータ・クローニング・ワークフローと統合されています。オンプレミス環境とクラウド環境間でデータベースをクローニングしながら、Oracle Cloud への移動前または移動後にデータをマスクできます。Data Masking and Subsetting は Oracle Database Cloud Service の各エディションに含まれており、Oracle Fusion SaaS の各モジュールでフル・マネージドのサブスクリプション・サービスとしても提供されています。

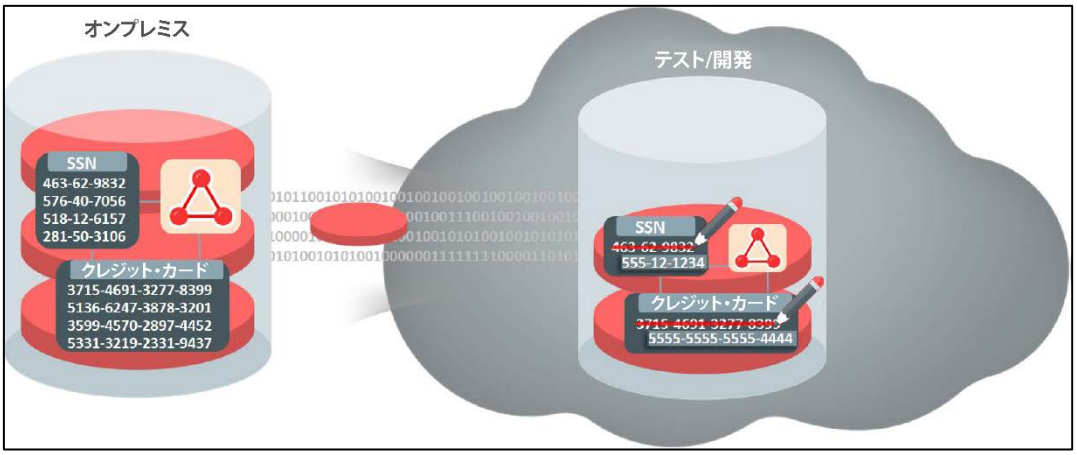

図3：Oracle Data Masking and Subsettingで、オンプレミスまたはクラウド内のデータを保護

オフサイトの統合により、脅威を検出して監査データの改ざんを軽減する

攻撃はますます高度になっており、境界セキュリティをバイパスし、信頼されている中間層を利用し、さらには特権を持つ内部関係者になりすましています。また、攻撃者は通常、攻撃を隠すために監査レコードの改ざんを試みます。多数のセキュリティ・インシデントの調査から、監査データをタイムリーに審査すれば、不正なアクティビティを早期に検知して結果として生じる経済的な打撃を軽減できることが分かっています。暗号化と同様に、監査は重要なデータ・セキュリティ要件となっており、データ・プライバシ法や規格で義務付けられています。

Oracle Cloud では、包括的できめ細かい統合型の監査機能を Database Cloud Service の一部として提供しています。暗号化と同様に、監査機能もデフォルトで有効になります。また、オンプレミスの Audit Vault and Database Firewall で監査レコードを保存、管理できるため、顧客による監査データの制御が確立されます。

Oracle Audit Vault and Database Firewall（AVDF）はソフトウェア・アプライアンスであり、データベース、オペレーティング・システム、およびディレクトリのデータベース・アクティビティ監視イベントと監査データを統合するのに役立ちます。AVDF 12.2 では、クラド・データベースの監査データを一元化された場所に統合することも可能です。AVDF により、一貫性のあるポリシー、統合型のレポート、共通のアラート管理など、オンプレミス・データベースとクラウド・データベースに対応した、企業全体にわたる統合型の監査インフラストラクチャが容易になります

AVDF には、PCI-DSS、SOX、HIPAA といったさまざまなデータ・プライバシ規格に対応した、事前構成のレポートが用意されています。これらのレポートを使用すると、監視対象システムの監査データを集計できます。傾向を詳しく分析する場合、クラウドとオンプレミスの監視対象システムのイベント・データを組み合わせてフィルタリングし、対話形式で表示するか静的な PDF や Excel 形式で表示できます。管理者は、データベースで不正アクセスやシステム権限の乱用が試みられたことを示すアクティビティに対して、しきい値に基づいたアラートを定義できます。

Oracle Key Vault と同様に、AVDF もフル・スタックで強固なセキュリティを備えたソフトウェア・アプライアンスであり、Web ベースの管理コンソールが用意されています。すべてのネットワーク接続に暗号化と認証が適用され、管理職務がそれぞれの管理ロールごとに分離されます。次の図は、AVDF のハイブリッド・クラウド管理アーキテクチャを示しています。

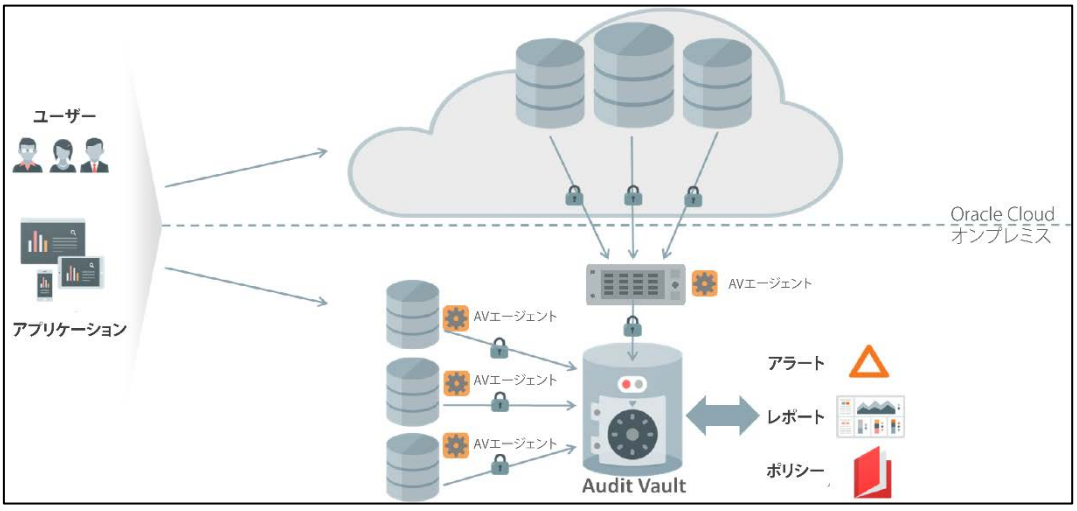

図4：Oracle Audit Vault and Database Firewallによる、オンプレミとクラウド内のデータベースの監視

セキュリティ・ポリシー管理を一元化および統合する

ハイブリッド・クラウド・モデルで運用している大企業か、オンプレミス・アプリケーションをクラウドに"リフト・アンド・シフト"しようとしている SMB かに関係なく、ポリシー管理を一元化、統合して共通のユーザー・インタフェースを使用すると、全体的な複雑さが軽減され、セキュリティ・インシデントの可能性も低減されます。Oracle Key Vault と Oracle Audit Vault では、Web ベースのユーザー・インタフェースを使用して暗号化鍵や監査レコードを管理できます。また、'Oracle Enterprise Manager Cloud Control'では、共通のインタフェースを使用してオンプレミスの Oracle Database と Oracle Cloud のデータ・セキュリティ・ポリシーを管理できます。

Oracle Enterprise Manager Cloud Control 12.1.0.5 以降では、RMAN、Data Pump、プラガブル・データベース（PDB）、スナップ・クローンなどのさまざまなデータ・プロビジョニング手法を使用し、オンプレミス環境とクラウド環境間でデータベースおよび関連するセキュリティ・ポリシーを透過的に移行できます。暗号化設定、監査ポリシー、アクセス制御、行レベルのセキュリティ制御といったセキュリティ設定やポリシーを、アプリケーションやデータベースを停止させずにオンプレミスからクラウドへ、またはクラウドからオンプレミスへ透過的に移行できるため、クラウドへの移行作業が大幅に簡素化されます

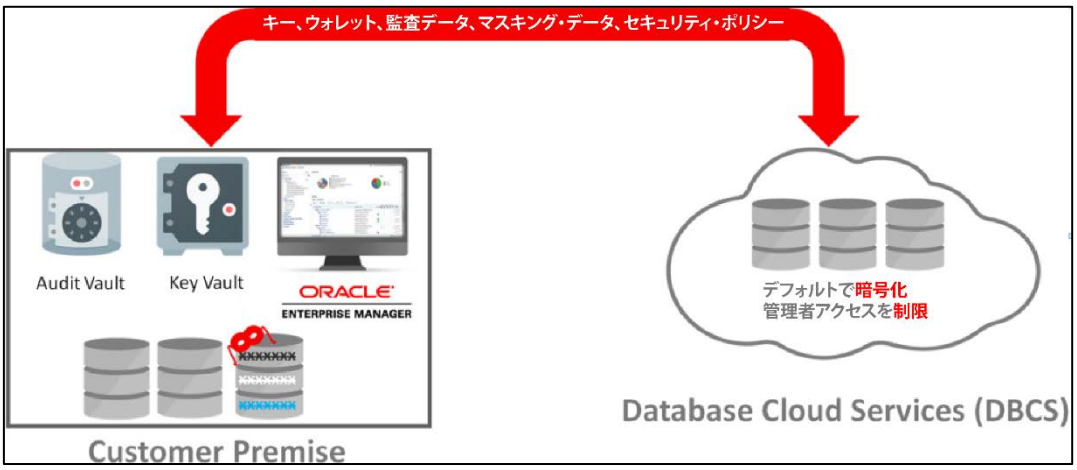

図5：統合型ユーザー・インタフェースにより、ハイブリッド・データセンター全体を可視化

透過性、正確性、パフォーマンス、拡張性を備えた多層防御を実現する

最新アプリケーションは、Web ゲートウェイ、Web プロキシ、Web サーバー、アプリケーション・サーバー、データベース・サーバーといった複数の基盤となるコンポーネントから構成されています。多層的な環境においてすべてのセキュリティ制御を定義し、実装することは難しい作業です。オラクルのデータ・セキュリティ・テクノロジーでは、こうした課題に対処するために、制御をデータの近くに配置し、データベース内にセキュリティを適用しています。Oracle が提供するデータ保護制御機能の大半は、Oracle Database に組み込まれています。データを発生元で保護することで設計や展開が容易になるだけでなく、保護の精度が向上し、攻撃対象領域が縮小します。

Oracle Key Vault と Oracle Audit Vault and Database Firewall では制御と管理を一元化することで発生元のデータ保護を補完します。何千もの暗号化鍵や何百万もの監査記録があろうと、セキュリティ・ポリシーの種類がさまざまであろうとも、これらのコンポーネントは一元管理できるため管理に関連する作業が大幅に簡素化されます。機密データを保護するために、Oracle Database のセキュリティ制御機能はすべて相互に統合されています。

オラクルは、数十年にわたってデータ・セキュリティ分野で第一人者として認められており、ここ数年はセキュリティ製品の開発によって、さまざまな脅威ベクトルによる攻撃に組織が対処できるよう支援しています。オンプレミスかクラウドかに関係なく、Oracle Database は評価、予防、および検知が可能な、数多くの高度なセキュリティ制御機能を備えています。行レベルのセキュリティや監査といった基本的なセキュリティ制御機能は、10 年以上にわたって提供されています。Data Redaction や Real Application Security といった次世代のデータ中心型のセキュリティ制御機能は、開発者がアプリケーションの変更をゼロまたは最小限に抑えながら、データ・セキュリティをアプリケーションに組み込むのに役立ちます。多層防御のセキュリティを実現する Oracle Database のセキュリティ制御機能については、次のホワイト・ペーパーを参照してください。

ホワイト・ペーパー：『Oracle Database 12c のセキュリティとコンプライアンス』

次の表は、オラクルの各種データ・セキュリティ・テクノロジーがさまざまな脅威ベクトルをどのようにして軽減するかを示しています。

リスク	軽減方法
テスト/開発/パートナーでの機密データの漏えい	クラウドへの移行前にマスキングとサブセット化を実行
クリアテキスト・データの紛失	データをデフォルトで暗号化
暗号化鍵への不正アクセス	オンプレミスのKey Vaultで鍵を制御
クラウドDBAによる不正アクセス	DBAによるアクセスをDatabase Vaultで制限
侵害を迅速に検出できない	オンプレミスのAudit Vault and Database Firewallで監査と監視を実行

結論

クラウドのデータ・セキュリティに対するオラクルのビジョンは、以下の原則に基づいています。

» セキュリティが常時オン

» セキュリティをスタック内に適用する

» 顧客がデータを制御できる

» オンプレミスとクラウドでセキュリティ・ポリシーが同じである

上記の原則を実施するために、Oracle Database Cloud Service は次のことを実現する、他社とは異なる独自のテクノロジーを提供しています。

» 暗号化鍵と監査レコードを物理的に統合、管理、制御する

» 特権ユーザーによる機密データへのアクセスを Database Vault で制限する

» オンプレミスまたはクラウドの機密情報をマスキングおよびサブセット化する

» 統合されたブラウザベースのユーザー・インタフェースでセキュリティ・ポリシーを管理および移行する

また、セキュリティを最大限に高めるために、オンプレミスかクラウドかに関係なく、Oracle Database は評価、予防、および検知が可能な包括的な制御機能を提供しています。

クラウドの採用やクラウドへの移行を進めている大企業と SMB（中小企業）は、Oracle Cloud で提供されているデータ・セキュリティ・テクノロジーを利用すると、データ・プライバシやセキュリティに関する懸念が軽減され、クラウドへの移行を促進できます。

参考資料

» Oracle Cloud

» Oracle Database Cloud Service

» オラクルのデータ・セキュリティ

» ホワイト・ペーパー：『Oracle Database 12c のセキュリティとコンプライアンス』

» ホワイト・ペーパー：『Oracle Infrastructure and Platform Cloud Services Security』

付録

Oracle Database Cloud Serviceと他のクラウド・プロバイダーとのデータ・セキュリティの比較

次の表は、Oracle Database Cloud Service のデータ・セキュリティを、Amazon Web Services（AWS）および Microsoft Azure のデータベース・サービスと比較したものです（本ホワイト・ペーパーの発行時点）

	AWS AURORA	AZURE SQL DB	ORACLE CLOUD DB
データの暗号化	✓	✓	✓
オンプレミスでの暗号化鍵の制御			✓
DBAによる機密データへのアクセスの制限			✓
テスト/開発時の機密データのマスキング			✓
オンプレミスでの監査レコードの収集			✓
クラウドとオンプレミス間でのセキュリティ・ポリシーの移行			✓

- **鍵管理の比較**
  - Oracle Key Vault をオンプレミスにデプロイして、オンプレミスと Oracle Cloud データベースのデータベース暗号化鍵を一元的に収集および管理できます。また、ボタンを 1 回クリックすれば暗号化鍵を停止できるため、データベースを停止させずにアプリケーション・データを使用不可にできます。
  - これに対して、Amazon Key Management および Azure Key Vault のサービスは、それぞれのクラウドに制限されています。顧客がこれらの鍵管理ソリューションをオンプレミスにデプロイして暗号化鍵を制御することはできません。直接所有できないというのは、企業にとって大きな問題です。
- **特権ユーザーのアクセス制御の比較**
  - Oracle Database Cloud Service では、Database Vault を使用して DBA（Oracle Cloud 管理者を含む）による機密情報へのアクセスを制限できます。
  - これに対して、AWS と Azure では、Database Vault 同等のテクノロジーは提供されていません。
- **データのマスキングおよびサブセット化の比較**
  - Oracle Database Cloud Service では、Data Masking and Subsetting を使用してオンプレミスまたは Oracle Cloud の機密性の高い本番データを検出、マスキング、およびサブセット化できます。
  - これに対して、AWS と Azure では、Data Masking and Subsetting 相当のテクノロジーは提供されていません。

» **クラウド・データベースの監査と監視の比較**

  » Oracle Audit Vault をオンプレミスにデプロイして、オンプレミスと Oracle Cloud に配置されている Oracle Database の監査情報を一元的に収集および管理できます。データベース監査情報をオフサイトで管理できるため、攻撃者が監査レコードを改ざんする可能性が最小限に抑えられます。

  » これに対して、Amazon CloudWatch（監視サービス）、Amazon CloudTrail（API 監査サービス）、および Azure Security Center は、オンプレミスにデプロイしてデータベース監査レコードをオフサイトで保持することはできません。

» **セキュリティ・ポリシー管理に使用するユーザー・インタフェースの比較**

  » Oracle Enterprise Manager、Key Vault、および Audit Vault では、統合型のユーザー・インタフェースを使用して、暗号化鍵、ウォレット、監査レコード、監査ポリシー、マスキング・ルール、Database Vault のポリシー、行レベルのセキュリティ・ポリシーといった、オンプレミスと Oracle Cloud に配置されている Oracle Database のデータ・セキュリティ・コンポーネントとポリシーを管理できます。顧客は、オンプレミス環境と Oracle Cloud 環境間でデータ・セキュリティ・コンポーネントやポリシーをクローニング、移行、転送できます。

  » これに対して、AWS と Azure では、オンプレミス・データベースとクラウド・データベース間でデータ・セキュリティ・コンポーネントやポリシーをクローニング、移行、転送できるような、統合型のユーザー・インタフェースは提供されていません。

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

海外からのお問い合わせ窓口
電話：+1.650.506.7000
ファクシミリ：+1.650.506.7200

CONNECT WITH US

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

Integrated Cloud Applications & Platform Services