ORACLE

Advisory: Privacy Features of Oracle Cloud Infrastructure

お客様が一般データ・プライバシー原則に準拠する上で
役立つOracle Cloud Infrastructureの機能

2023年10月、バージョン2.2

Public

免責事項

このドキュメントには、ソフトウェアまたは印刷物などの形式を問わず、オラクルが独占的な権利を有する財産的情報が含まれています。このドキュメントは契約の一部となるものではなく、オラクルおよびその子会社や関連会社との契約を構成するものではありません。

このドキュメントは情報提供のみを目的としており、お客様が各種プライバシー・フレームワークの下で適用される要件に即してOracle Cloudサービスの使用状況を評価する際にお役立ていただくことのみを意図しています。このドキュメントは、オラクルを外部委託のサービス・プロバイダとして評価する際にも役立つ可能性があります。お客様はこのドキュメントの情報を独自に評価する責任を負います。このドキュメントの情報は、法規制や規制ガイドラインの内容、解釈または適用に関して法的助言を行うことを意図しておらず、法的助言として使用することはできません。このドキュメントで述べられている法規制の適用可能性と要件については、独立した法的助言を求めてください。

このドキュメントはマテリアルやコード、機能の提供をコミットメント(確約)するものではないため、購買決定を行う際の判断材料になさらないでください。このドキュメントに記載されている機能の開発、リリースおよび時期については、オラクルの単独の裁量により決定されます。

改訂履歴

このドキュメントには、次の改訂が加えられています。

日付	改訂内容
2023年10月	バージョン2.2に更新(大きな変更はなし)
2021年11月	バージョン2.1をリリース

目次

はじめに

世界中の多くの管轄区域でデータ・プライバシー規制が導入されています。こうした規制の例として、EU一般データ保護規則(GDPR)、オーストラリアのデータ・プライバシー法、カナダの個人情報保護および電子文書法(PIPEDA)、日本の個人情報保護法、韓国の個人情報保護法(PIPA)などが挙げられます。これらの規制では、個人の個人情報の収集と処理に関するルールが定められています。

ドキュメントの目的

このドキュメントでは、世界中のデータ・プライバシー規制から発生する要件のいくつかに対応する上で、Oracle Cloud Infrastructure (OCI)の機能がどのように役立つかを説明します。

このドキュメントに記載されている情報は、法的な助言をするものではありません。お客様がプライバシー・コンプライアンス・プログラムを策定、実施する場合や、法規制上の要件に関してOCIで提供される機能を評価する場合には、ご自身で弁護士に相談することをお薦めします。

次のポリシーとドキュメントがこのホワイト・ペーパー全般で参照されています。

- Oracle Services Privacy Policy (oracle.com/legal/privacy/services-privacy-policy.html)
- Oracle General Privacy Policy (oracle.com/legal/privacy/privacy-policy.html)
- Data Processing Agreement for Oracle Services (DPA) (oracle.com/contracts/cloud-services/)

Oracle Cloud Infrastructureについて

Oracle Cloud Infrastructure (OCI)は、可用性に優れた安全なホスティング環境で幅広いアプリケーションやサービスを構築して実行できる、一連のコラボレーティブ・クラウド・サービスです。OCIは、オンプレミス・ネットワークから簡単にアクセスできる柔軟なオーバーレイ仮想ネットワークで、高パフォーマンスなコンピューティング機能とストレージ容量を提供します。OCIは、クラウド・ネイティブなエンタープライズITワークロードを実行するために、高パフォーマンスなコンピューティング能力を発揮するPlatform as a Service (PaaS)とInfrastructure as a Service (IaaS)を提供します。OCIサービスの詳細は、docs.oracle.com/iaas/Content/home.htmを参照してください。

OCIは、お客様がセキュリティとコンプライアンスのニーズにより効率的に対処できるよう支援する機能やサービスに投資し続けています。OCIのサービスと機能がコンプライアンスとレポートの要件にどのように役立つかの詳細は、oracle.com/corporate/cloud-compliance/を参照してください。

クラウド共同管理モデル

セキュリティ管理の観点から言うと、クラウド・コンピューティングとオンプレミス・コンピューティングは根本的に異なります。オンプレミスのお客様は、テクノロジ・インフラストラクチャを完全に制御しています。たとえば、ハードウェアを物理的に制御し、本稼働中のテクノロジ・スタックを完全に制御しています。一方、クラウドでは、お客様はクラウド・サービス・プロバイダが部分的に管理しているコンポーネントを使用します。そのため、クラウドでのセキュリティの管理はクラウドのお客様とクラウド・サービス・プロバイダの間の共有責任になります。

オラクルは、エンタープライズ・クラウド・サービスを保護するために、クラス最高のセキュリティ・テクノロジと運用プロセスを提供しています。しかし、お客様もオラクルのクラウド環境でワークロードを実行する際には、セキュリティとコンプライアンスに対する責任を認識し、管理する必要があります。その仕組みとしては、クラウド・オペレータのアクセス制御やインフラストラクチャへのセキュリティ・パッチの適用など、クラウド・インフラストラクチャと運用のためのセキュリティ機能をオラクルが提供します。
お客様は、自社のクラウド・リソースを安全に構成して使用する責任を負います。詳細は、クラウド・サービスのドキュメントを参照してください。

次の図は、この責任の分担を大まかに図示したものです。

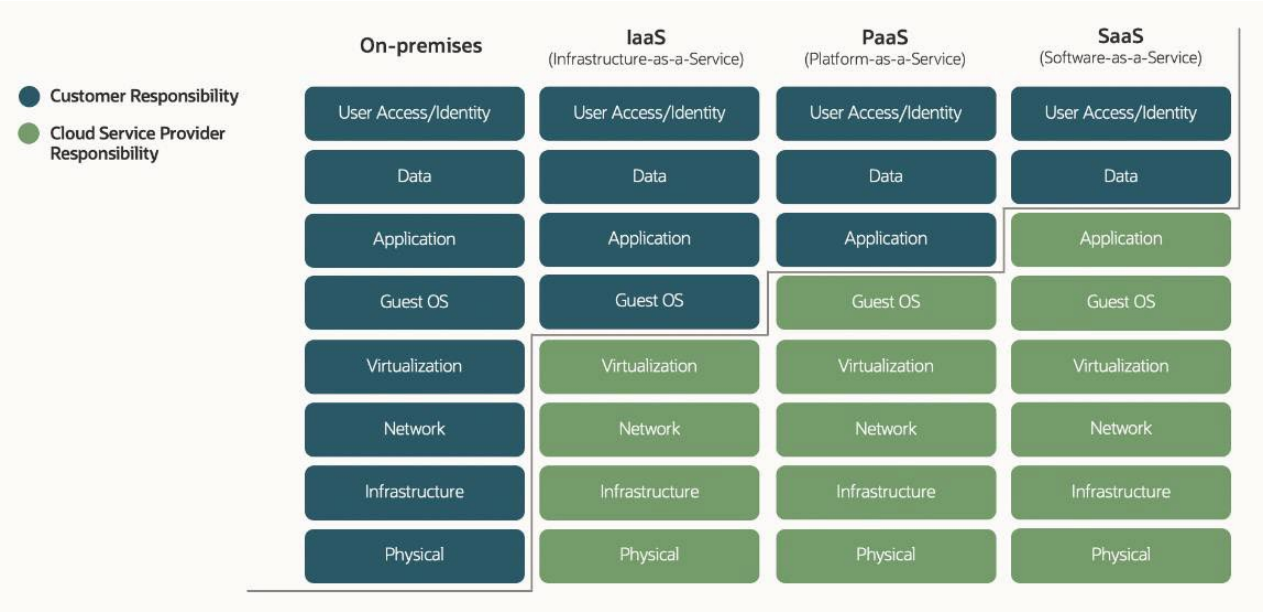

図1: お客様とクラウド・プロバイダの間の各種セキュリティ管理責任の概念図

役割

オラクルは、お客様の代理として個人情報をホスティングするクラウド・サービス・ベンダーであり、*処理者*の役割を担います。処理者は*管理者*の指示に従います。お客様はOCIの機能を使用してアプリケーションを構築するオラクルの直接の顧客であり、通常は管理者の役割を担います。管理者であるお客様はデータの処理目的を決定します。お客様の顧客は、お客様が構築するアプリケーションの*エンド・ユーザー*です。多くの場合、エンド・ユーザーは*データ主体*または*個人*とも呼ばれます。

データ主体(エンド・ユーザー) ←➔ 管理者(オラクルのお客様) ←➔ 処理者(オラクル)

サービスの範囲内では、オラクルはエンド・ユーザーまたはデータ主体(お客様が処理する可能性のある個人情報を有する個人)と直接の関係を持ちません。お客様が収集する個人情報はお客様が管理し、収集した個人情報をどのように、どのデータ・センター・リージョンで処理するかについてもお客様が決定することになります。

OCIは、データのセキュリティとデータのプライバシーに対する責任をオラクルとお客様が共有するInfrastructure as a Service (IaaS)製品です。

お客様のデータ

一般的に、OCIはお客様とのやり取りの中で大きく分けて2種類のデータを扱います。

- **お客様に関するデータ:**お客様のOCIアカウントの運用とサービスの料金請求に必要な連絡先と関連する情報。オラクルがアカウント管理の目的でお客様から収集する個人情報の使用は、Oracle General Privacy Policyに従います。
- **お客様がOCIに持ち込むデータ:**お客様がOCIに持ち込むデータは、ファイル、ドキュメントまたはデータベース・エントリとして保管される可能性があります。データには個人情報が含まれている可能性がありますが、オラクルは、このデータの内容、このデータの収集方法や使用方法、このデータが特定のデータ・プライバシー規制の対象になるかどうかについて関知しません。オラクルによるこのデータの扱いについては、Oracle Services Privacy PolicyとData Processing Agreement for Oracle Servicesに記載されています。

このドキュメントでは、オラクルのお客様がOCIのサービスやテナントに保管するデータと、そのデータに含まれている可能性のある個人情報を扱う上で利用可能な機能とサービスについて、概要を示します。

データ・プライバシー原則

この後の項では、OCIのお客様がサービスの機能をどのように使用すれば多くの重要なデータ・プライバシー原則に準拠できるかを概説します。また、こうした原則に対する責任をオラクルとお客様がどのように共有するかについても説明します。各項の冒頭で示す定義は、IAPPのGlossary of Privacy Terms (iapp.org/resources/ glossary/)での定義の一部に基づいています。

透明性–開示性

透明性: 処理に関連した情報を、明確かつ平易な言葉を用いて、簡潔でわかりやすく簡単にアクセスできる形でデータ主体に提供するために、適切な措置を取ること。

処理の透明性

Oracle Services Privacy PolicyとData Processing Agreement for Oracle Servicesで、オラクルがデータを扱う際のアプローチ全般について透明性を実現しています。ただし、クラウド・プロバイダであるオラクルは一般に、お客様がOCIに保管し処理するデータについて、またそれが特定の個人に属する個人情報かどうかについて関知しません。この点において、オラクルはエンド・ユーザーと直接の関係を持たないため、データ処理のいかなる詳細についてもエンド・ユーザーに通知しません。データをどのように処理するかについてエンド・ユーザーに透明性を提供できるのはお客様のみです。

場所の透明性

OCIは、データが処理され、保管される場所についての透明性を確保しています。国境を越えたデータ移転に関する要件を定めるデータ・プライバシー規制もあるため、この透明性は重要です。お客様は、アカウントを設定する際、最初に*テナント*を配置する*ホーム・リージョン*を選択します。お客様がデータをリージョン外に移動することを選択しないかぎり、データはそのリージョン内にとどまります。OCIは、テナントまたはリージョンをまたがって機能する強力なサービスを提供します。Oracle Cloudコンソールのユーザー・インタフェースとAPIのドキュメントを使用することにより、お客様のアクションの結果としてデータが別のリージョンやテナントに移動する場合はお客様に通知されるようになります。お客様とオラクルとの契約の条件によっては、オラクルがサービスを提供する義務を遂行するためにデータをグローバルに処理する場合もあります。

リージョンと可用性ドメインについては、docs.cloud.oracle.com/iaas/Content/General/Concepts/regions.htmを参照してください。テナントの設定については、docs.cloud.oracle.com/iaas/Content/GSG/Concepts/ settinguptenancy.htmを参照してください。

データ・ローカライゼーション

データ・ローカライゼーション法(データ・レジデンシー法としても知られている)により、特定のカテゴリのデータを特定の国に保管することを求められる場合があります。お客様のデータに適用されるデータ・ローカライゼーション法や規制の規制要件をよく理解し、準拠するためにはどのような手順を踏む必要があるかを判断しなければならないこともあります。

オラクルは一般に、お客様がOCIに保管し処理するデータについて、またそれがデータ・ローカライゼーション法の適用されるカテゴリに当てはまるかどうかについて関知しません。お客様はOCI内のデータの地理的な場所を把握していることから、前の項で説明した場所の透明性がデータ・ローカライゼーションに役立つ場合があります。オラクルは、世界中の国々で新しいデータ・センター・リージョンを開設し続けているため、データを自国内に保管できるお客様がますます増えています。

OCIデータ・センター・リージョンの地図は、oracle.com/cloud/public-cloud-regions/を参照してください。

データ最小化–収集制限

データ最小化原則: 収集して保存するパーソナル・データは必要なものだけにすべきであるという考え方。

クラウド・プロバイダであるオラクルは一般に、お客様がOCIに保管し処理するデータについて、またそれがエンド・ユーザーとの間で合意した目的の達成に必要な最小限のデータかどうかについて関知しません。エンド・ユーザーから収集されたデータが最小限の量かどうかの評価を行うのは、お客様の責任です。

目的明確化–通知と同意

目的明確化: パーソナル・データを収集する目的は、データ収集の時点までに明確化すべきである。

クラウド・プロバイダであるオラクルは一般に、お客様がOCIに保管し処理するデータについて、またそれがエンド・ユーザーとの間で合意した目的の達成に必要な最小限のデータかどうかについて関知しません。エンド・ユーザーから収集されたデータが最小限の量かどうか(または、適切な通知が行われ、同意が得られていたかどうか)の評価を行うのは、お客様の責任です。

目的限定

目的限定: パーソナル・データを収集する目的はデータ収集の時点までに明確化すべきであり、収集したパーソナル・データのその後の使用はその目的の達成のためだけに限定される。

お客様は常に管理者のままです。オラクルは、お客様から求められた場合にデータを処理し、お客様とオラクルとの契約で規定された目的でのみデータを使用します。

クラウド・プロバイダであるオラクルは一般に、お客様がOCIに保管し処理するデータについて、またそれが収集された理由や、それがエンド・ユーザーに通知された目的の限度を超えて処理されているかどうかについて関知しません。ただし、OCIには目的限定の効果的な管理に役立つよう設計された次の機能があります。

タグ付け

オラクルは柔軟なタグ付け操作を提供しており、この機能は、リソースに(複数のコンパートメントにまたがって)ラベルを付けて、同様の目的を持つリソースを集約し、そのリソース・グループに対して一括処理を実行するのに役立ちます。テナント管理者は、リソースのタグ付け戦略を策定して実施することにより、処理対象のデータを目的に即して収集することを徹底できます。

詳細は、docs.cloud.oracle.com/iaas/Content/Tagging/Concepts/taggingoverview.htmを参照してください。

コンパートメント

オラクルは、お客様が初期ルート・コンパートメント(またはテナント)の下にコンパートメントを作成できるようにしています。管理者は、テナント内のコンパートメントをプランニングして作成することにより、クラウド・リソース(たとえば、ブロック・ボリュームやコンピュート・インスタンス)とその中に含まれるデータを整理し、特定のグループのみがそれらにアクセスできるようにすることが可能です。こうした機能は、処理の対象となる個人情報の目的限定を徹底する上でのデータ管理目標に即した方法でクラウド・リソースを整理し、分離するのに役立ちます。たとえば、企業の人事部門用にコンパートメントを1つ作成し、財務部門用にもう1つ作成することが可能です。こうすることで、クラウド・リソースが効果的に分離され、2つの部門のデータが分離された状態を保つことができます。

詳細は、docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managingcompartments.htmと docs.oracle.com/iaas/Content/Identity/compartments/managingcompartments.htm (アイデンティティ・ドメインを使用する場合)を参照してください。

仮想クラウド・ネットワーク

仮想クラウド・ネットワーク(VCN)を使用すると、インフラストラクチャの様々な部分をセグメント化し、それらのセグメント間でのリソースの通信を制御することができます。VCNアーキテクチャを事前にプランニングすることで、アーキテクチャの潜在的なネットワーク分離によって必要とされるデータのセキュリティと目的限定を強化することができます。これには次の構成を使用します。

- セキュリティ・リスト: docs.oracle.com/iaas/Content/Network/Concepts/securitylists.htm
- ネットワーク・セキュリティ・グループ: docs.oracle.com/iaas/Content/Network/Concepts/networksecuritygroups.htm
- ネットワーク・ファイアウォール: docs.oracle.com/iaas/Content/network-firewall/home.htm

VCNの詳細は、OCI Networkingのドキュメントの次のページを参照してください。

- docs.cloud.oracle.com/iaas/Content/GSG/Tasks/creatingnetwork.htm
- docs.oracle.com/iaas/Content/Network/Tasks/VCNs.htm

正確性–データ品質

正確性: 組織は、処理されるデータが正確であり、必要に応じて最新の状態に維持されていることを保証するために、あらゆる妥当な措置を取らなければならない。

クラウド・プロバイダであるオラクルは一般に、お客様が個人情報を保管するかどうかや、その個人情報が個人に関して正確かどうかについて関知しません。ただし、OCIは、データの正確なコピーを保管するのに役立つObject Storage、Block Volume、File Storageの各サービスを提供しています。

- **Object Storage**を使用すると、多くのコンテンツ・タイプの非構造化データを保管できます。Object Storageは、データが複数のストレージ・サーバーや複数の可用性ドメインにまたがって保管される、リージョン単位のサービスです。Object Storageでは、破損データを自動的に検出して修復するチェックサムを使用して、技術的なデータの完全性を能動的に監視します。データの冗長性も能動的に監視し、維持します。Object Storageでは、冗長性の喪失が検出されると、追加のデータ・コピーを自動的に作成します。**Archive Storage**は、長期間保存しておく必要があるが、アクセス頻度がきわめて低いデータ・オブジェクトに使用できる、もう1つのストレージ・クラス層です。詳細は、docs.cloud.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htmとdocs.cloud.oracle.com/iaas/Content/Archive/Concepts/archivestorageoverview.htmを参照してください。
- **Block Volume**を使用すると、ブロック・ボリュームがコンピュート・インスタンスにアタッチされ、接続されているときに、それを通常のハード・ドライブとして使用できます。データを失うことなくボリュームを切断して、別のコンピュート・インスタンスにアタッチすることが可能です。ボリュームを自動的にレプリケートしてデータ損失から保護することで、データの耐久性が強化されます。詳細は、docs.cloud.oracle.com/iaas/Content/Block/Concepts/overview.htmを参照してください。
- **File Storage**を使用すると、共有ファイル・システムおよびマウント・ターゲットの管理とファイル・システムのスナップショットの作成が行えます。File Storageでは、同期レプリケーションと高可用性フェイルオーバーを使用して、回復力に優れたデータ保護を実現しています。詳細は、docs.cloud.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htmを参照してください。

可用性

可用性: データは、組織またはデータ主体が必要に応じてアクセスできる場合に"使用可能"であると言える。

次のOCI機能は、データの可用性を確保するのに役立ちます。

可用性ドメインとフォルト・ドメイン

お客様のテナントは、お客様が選んだ使用可能なホーム・リージョンに作成されます。多くのOCIリージョンは、物理的に分離されたフォルトトレラントな可用性ドメインで構成されます。お客様は、この可用性ドメインを使用してレプリケートされたシステムを構築できます。

フォルト・ドメインとは、可用性ドメイン内のハードウェアとインフラストラクチャをグループ化したものです。オプションで、新しいコンピュート・インスタンスの作成時にそのフォルト・ドメインを指定できます。これにより、コンピュート・インスタンスを分散させることが可能となり、複数のインスタンスを1つの可用性ドメイン内の同じ物理ハードウェアに配置しなくてすみます。

詳細は、docs.cloud.oracle.com/iaas/Content/General/Concepts/regions.htmと docs.cloud.oracle.com/iaas/Content/Compute/Tasks/edit-fault-domain.htmを参照してください。

バックアップ

次に示す柔軟なデータ・ストレージ・バックアップ・オプションをご利用いただけます。

- **Block Volume**:Block Volumeのバックアップは手動で行うか、スケジュールすることができ、増分バックアップと完全バックアップの2種類があります。クロス・リージョン・バックアップは、ビジネス継続性、ディザスタ・リカバリ、アプリケーションの移行と拡張の目的で使用できます。ポリシーベースのバックアップには、様々なバックアップ頻度と保存期間が用意されています。これらのバックアップはObject Storageで暗号化されます。詳細は、docs.cloud.oracle.com/iaas/Content/Block/Concepts/blockvolumebackups.htmを参照してください。
- **Object Storage**:Object Storageのレプリケーションはディザスタ・リカバリ作業を支援し、データ冗長性関連のコンプライアンス要件に対処します。同じリージョン内で、または複数のリージョンにまたがって、オブジェクトのコピーを他のバケットに作成できます。詳細は、docs.cloud.oracle.com/iaas/Content/Object/Tasks/usingreplication.htmと docs.cloud.oracle.com/iaas/Content/Object/Tasks/copyingobjects.htmを参照してください。
- **Base Database Service**: バックアップはObject Storageまたはローカル・ストレージに保存できます。データを保護し、可用性を確保するために、Data Guardも使用できます。詳細は、docs.oracle.com/iaas/dbcs/doc/backup-and-recovery.htmlと docs.oracle.com/iaas/dbcs/doc/use-oracle-data-guard-db-system.htmlを参照してください。
- **Exadata Cloud Service**:Exadataデータベースのバックアップは Object Storageに保存され、管理対象にも管理対象外にもできます。データを保護し、可用性を確保するために、Data Guardも使用できます。詳細は、docs.oracle.com/iaas/exadatacloud/exacs/ecs-managing-db-backup-and-recovery.html (オラクルが管理するバックアップとユーザー構成バックアップの両方が使用可能)と docs.oracle.com/iaas/exadatacloud/exacs/using-data-guard-with-exacc.htmlを参照してください。

OCIの高可用性ソリューションの詳細は、docs.oracle.com/en/solutions/design-haを参照してください。

セキュリティ・セーフガード

セキュリティ・セーフガード: パーソナル・データは、適切なセキュリティ・セーフガードにより、データの損失または不正アクセス、破壊、使用、改ざん、または漏洩などのリスクから保護すべきである。

お客様は、ワークロードの保護とサービス(Compute、Network、Storage、Databaseなど)の安全な構成に対して責任を負います。共同セキュリティ・モデルに関する情報(docs.cloud.oracle.com/iaas/Content/Security/Concepts/security_overview.htm)を参照してください。

OCIの多くのセキュリティ・サービス、機能および推奨プラクティスについては、次の参考資料に記載されています。

- セキュリティ・サービスおよび機能 (docs.cloud.oracle.com/iaas/Content/Security/Concepts/security_features.htm)
- OCIのセキュリティ・アーキテクチャ (oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf)
- サービス固有のセキュリティ・ベスト・プラクティス (docs.cloud.oracle.com/iaas/Content/Security/Reference/configuration_security.htm)

機微情報

機微な個人情報: 医療情報や財務情報など、プライバシーの合理的な期待の概念にとって、より重大に関連するデータ。

クラウド・プロバイダであるオラクルは一般に、お客様がOCIに保管し処理するデータについて、またそれが機微情報かどうかについて関知しません。データに機微情報が含まれるかどうか、データの特殊な処理を実施する必要があるかどうかの評価は、お客様の判断に委ねられます。そのような評価と併せて、特定のサービスやリージョンがお客様のワークロードとデータに適しているかどうかの評価も行う必要があります。ただし、オラクルはデータ(適切な場合、機微データを含む)を保護するのに役立つ、暗号化機能と鍵管理サービスを提供しています。

暗号化

この項で説明する暗号化は、基礎となるデータの性質にかかわらず、デフォルトで行われます。OCIは、データの性質、つまりデータがパーソナル・データなのか、機微データなのか、それ以外なのかについて関知しません。

- **Block Volume**:データはデフォルトで保存時に暗号化され、バックアップもObject Storageで暗号化されます。詳細は、docs.cloud.oracle.com/iaas/Content/Block/Concepts/overview.htmを参照してください。
- **Object Storage**:各オブジェクトが専用の鍵で暗号化されます。暗号化はデフォルトで有効になっています。詳細は、docs.cloud.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htmを参照してください。
- **File Storage**:お客様のデータはデフォルトで保存時に暗号化されます。詳細は、docs.cloud.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htmを参照してください。
- **Base Database Service**: 透過的データ暗号化(TDE)を使用することにより、ユーザーが作成した表領域の暗号化がデフォルトで有効になります。詳細は、docs.oracle.com/iaas/dbcs/doc/network-time-protocol-and-transparent-data-encryption.htmlを参照してください。
- **Exadata Cloud Service**:Exadata Cloud Serviceデータベースに作成した新しい表領域はすべてデフォルトで暗号化されます。詳細は、docs.oracle.com/iaas/exadatacloud/exacs/exa-conf-db-features.htmlを参照してください。

Vault

Vaultキー管理サービスは、お客様のデータの暗号化を、お客様が管理する鍵によって一元的に管理できるようにします。これは次のタスクに使用できます。

- マスター暗号化鍵とデータ暗号化鍵を作成する
- 鍵をローテーションして新しい暗号化マテリアルを生成する
- 暗号化操作で使用する鍵を有効化または無効化する
- 鍵をリソースに割り当てる
- 鍵を使用して暗号化と復号化を行い、データを保護する

Block Volume、Object Storage、File Storage、Streamingの各サービスがVaultと統合され、これらのサービスでのデータの暗号化がサポートされています。VaultとIdentity and Access Management (IAM)との統合により、鍵へのアクセス権を持つのは誰か、どのサービスかを制御できます。Auditサービス(次の項を参照)を使用すると、鍵とボールトに対する管理アクションを追跡できます。Vaultの詳細は、docs.cloud.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htmを参照してください。

漏洩通知–インシデントレスポンス

漏洩の開示: 組織は、パーソナル・データの機密性とセキュリティに影響を及ぼすインシデントについて、規制当局または被害者(あるいはその両方)に通知するものとするという要件。

オラクルは、送信、保管、その他の方法で処理されたオラクル管理のお客様データの破壊、損失、改ざん、不正な開示またはアクセスが疑われるか、それらが発生したことを示すインシデントを検出して速やかに対応するための統制とポリシーを導入しています。オラクルのInformation Security Incident Reporting and Response Policyに、イベントやインシデントのレポートと対応に関する要件が定められています。詳細は、oracle.com/corporate/security-practices/corporate/security-incident-response.htmlを参照してください。

オラクルによって処理された情報が関わる確認済のセキュリティ・インシデントが発生したと判断した場合、オラクルは、Data Processing Agreement for Oracle Servicesに定められた契約上、規制上の責任に従い、影響を受けるお客様やその他の第三者に速やかに通知します。
悪意のある試みや疑わしいインシデントに関する情報とインシデント履歴は、外部と共有されません。エンド・ユーザーのいずれかまたは規制当局に、個人情報の漏洩について通知する必要があるかどうかは、管理者であるお客様が判断しなければなりません。

お客様は、自身が管理するセキュリティ環境内でインシデントや個人情報の漏洩を検出する責任を負います。たとえば、OCIでは、お客様のテナントに対するユーザーのログインが不正であるかどうかを見抜くことはできません。Cloud GuardとAuditサービス(次の項を参照)は、OCIでお客様が設定した環境を監視するのに役立ちます。OCIプラットフォームに実装した機能に応じて、他の監視ソフトウェアを実装することもできます。

Cloud Guardの詳細は、docs.oracle.com/iaas/cloud-guard/home.htmを参照してください。

Audit

Auditサービスは、OCI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)に対するコールを、そのコールがコンソール、ソフトウェア開発キット(SDK)、コマンド・ライン・インタフェース(CLI)のいずれから行われたかに関係なくログに記録します。監査ログの内容には、イベントのタイプ、イベントを開始したユーザー、リクエストの日時、リクエストの説明、レスポンスが含まれています。こうしたログに記録されたイベントのデータを使用すると、テナント内のアクティビティを監視できるようになり、データの保護に役立ちます。このロギングは自動的に行われます。お客様は監査ログの保存期間を設定できます。

詳細は、次の参考資料を参照してください。

- docs.cloud.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm
- docs.oracle.com/iaas/Content/Audit/Reference/logeventreference.htm
- docs.cloud.oracle.com/iaas/Content/Audit/Tasks/settingretentionperiod.htm

最小権限

最小権限: 機能の実行に必要な最低限のレベルでアクセス権が付与されるセキュリティ統制。

OCIにおけるアクセス制御は、最小権限という概念に基づいています。新しいリソース(ブロック・ボリュームやコンピュート・インスタンスなど)はデフォルトで制限されています。つまり、当初は管理者グループのユーザーのみにリソースに対するアクセス権が付与されます。管理者のみが、既存または新規のポリシー、グループおよびコンパートメントを通じて、リソースに対するアクセス権を他のユーザーに付与できます。ポリシーは、お客様のテナントにあるリソースへのアクセスを*許可する*のみです。拒否することはできません。アクセス制御には、暗黙的な拒否というものがあります。これは、デフォルトではユーザーは何もすることができず、ポリシーを通じてアクセス権を付与される必要があることを意味します。

ポリシーの詳細は、docs.oracle.com/iaas/Content/Identity/Concepts/policygetstarted.htmとdocs.oracle.com/iaas/Content/Identity/Concepts/policies.htmを参照してください。

保管制限

保管制限: パーソナル・データはデータ主体の識別が可能な形で保管しなければならず、保管期間はそのパーソナル・データを処理する目的に必要な期間を超えてはならないという原則。

クラウド・プロバイダであるオラクルは一般に、お客様がOCIに保管し処理するデータについて、またそのデータを処理する目的が終了したかどうか、データを削除する必要があるかどうかについて関知しません。お客様がデータを削除しなければならないと判断した場合、OCIはデータを完全に削除するよう設計されたサービスを提供します。

データ削除

OCIは、すべてのデータ・ストレージ・サービスで削除機能を提供しています。各サービスの詳細は、次の参考資料を参照してください。

- **Block Volume**: docs.cloud.oracle.com/iaas/Content/Block/Tasks/deletingavolume.htm
- **Object Storage**: docs.cloud.oracle.com/iaas/Content/Object/Tasks/managingobjects.htmと docs.cloud.oracle.com/iaas/Content/Object/Tasks/managingbuckets.htm
- **コンピュート・インスタンスとNVMeストレージ**: docs.cloud.oracle.com/iaas/Content/Compute/Tasks/terminatinginstance.htm
- **File Storage**: docs.cloud.oracle.com/iaas/Content/File/Tasks/managingfilesystems.htm

Object Lifecycle Management

オラクルは、データ・オブジェクトのアーカイブと削除を自動化するのに役立つObject Lifecycle Managementを提供しています。docs.cloud.oracle.com/iaas/Content/Object/Tasks/usinglifecyclepolicies.htmを参照してください。

サービスの終了

お客様がOCIサービスのサブスクリプションを終了する場合、オラクルは、クラウド・サービスの本番環境に存在するデータをお客様が取り出せるようにします。取出し期間が過ぎると、データは完全に削除されます。この取出し期間の詳細は、Oracle Cloud Hosting and Delivery Policies (oracle.com/contracts/cloud-services/)の第6項「Oracle Cloud Suspension and Termination Policy」に記載されています。

データ主体(エンド・ユーザー)の要請

データ主体: 特定された、または特定可能な自然人。

クラウド・プロバイダであるオラクルは一般に、お客様がどのような個人情報をデータ主体(エンド・ユーザー)から収集してOCIで処理するかについて関知しません。ただし、Data Processing Agreement for Oracle Servicesの「Privacy Inquiries and Requests from Individuals」の項に、データ主体の特定の個人情報のアクセス、削除または消去、制限、修正、受信および送信(データポータビリティ)、または処理に対する異議の申立てといった要求への対応に関してオラクルが行う支援について記載されています。

国境を越えたデータ移転

国境を越えたデータ移転: ある管轄区域から別の管轄区域への個人情報の移転。

Data Processing Agreement for Oracle Servicesの「Cross-Border Data Transfers」の項に、国境を越えたデータ移転を伴う処理をサポートするためにオラクルが導入しているデータ移転メカニズムの説明があります。

サブプロセッサ

アウトソーシング: 個人情報の処理を含む場合もあるビジネス・プロセスを第三者に委託すること。

Data Processing Agreement for Oracle Servicesの「Oracle Affiliates and Third Party Subprocessors」の項に、オラクルがその関連会社と第三者サブプロセッサに対し、オラクルがData Processing Agreement for Oracle Servicesに基づいて行っているのと同じレベルのデータ保護およびセキュリティに準拠するよう求めていることも説明されています。オラクルは、OCIサービスの履行を支援するために個人情報を処理する関連会社および第三者サブプロセッサについての透明性を確保しています。

プライバシーオフィサー

プライバシーオフィサー: 多くの組織でプライバシーのコンプライアンスおよび業務の責任者を指す一般用語。

OCIはOracle Services Privacy Policyの対象となっており、このポリシーには、プライバシーの問題について現場からの問合せに対応するグローバル・データ保護責任者が任命されているという説明があります。このポリシーは次の情報も提供します。

- オラクルのグローバル・データ保護責任者に連絡する方法
- データ・プライバシー問合せフォーム
- プライバシーおよびセキュリティ・プラクティスに関する苦情の解決プロセス

Oracle Cloud Infrastructureのコンプライアンス

オラクルは、お客様が急速に変化するビジネス環境でグローバルに事業を展開し、ますます複雑化する規制環境の課題に対処できるよう支援することに注力しています。そのために、オラクルは、社内のある業務部門が1つ以上のサービスについて第三者による証明や認証を受けた際のフレームワークに関する情報を「アテステーション」の形で提供しています。このアテステーションは、該当するOracle Cloudサービスのセキュリティ、プライバシーおよびコンプライアンスの統制について独立した評価を提供しているため、コンプライアンスとレポート作成の助けとなります。

さらに、オラクルはクラウド・サービスの使用に関する一般情報と技術的な推奨事項を「アドバイザリ」の形で提供しています。このアドバイザリを提供する目的は、お客様が特定のOracle Cloudサービスを使用することの適合性を判断できるように、またコンプライアンスの義務を果たすのに役立つ特定の技術統制を実装できるように支援することです。

詳細は、Oracle Cloud Complianceサイト(oracle.com/corporate/cloud-compliance/)を参照してください。

その他の参考資料

- OCIの ドキュメント(docs.cloud.oracle.com/iaas/Content/GSG/Concepts/baremetalintro.htm)
- Oracle Services Privacy Policy (oracle.com/legal/privacy/services-privacy-policy.html)
- Oracle Cloud Servicesの契約(oracle.com/contracts/cloud-services/)

結論

Oracle Cloud Infrastructureは、オラクルのグローバルなパブリック・クラウド・リージョンで、あるいはお客様のデータ・センター内で、自律的な運用、統合されたセキュリティ、真に弾力性に優れたサーバーレス・サービスを提供します。Oracle Cloud Infrastructureは、各種規制フレームワークの下での運用に必要な技術統制を実装するのに役立つ、組込みのセキュリティ機能やプライバシー機能をいくつか備えています。

CONNECT WITH US

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

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