ORACLE

Approaching Zero Trust Security with Oracle Cloud Infrastructure

Oracle Cloud Infrastructure が、英国国家サイバー・セキュリティ・センターの 8 つの原則で推奨されているゼロ・トラスト・セキュリティ・モデルの採用にどのように役立つかを解説します

Paul Toal
Krithiga Gopalan

2024 年 7 月、バージョン 1.3

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。この機密資料へのアクセスと使用は、お客様とオラクルとの間で締結され、お客様が遵守に同意したオラクル・ソフトウェア・ライセンスおよびサービス契約の条件に従うものとします。このドキュメントとその内容の開示、コピー、複製および配布には、オラクルによる事前の承諾を必要とします。このドキュメントはライセンス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、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、機能を提供することのコミットメント（確約）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、時期および価格については、オラクルの単独の裁量により決定されます。製品アーキテクチャの性質により、コードの大幅な不安定化を招くリスクを冒さずにこのドキュメントに記載されているすべての機能を安全に組み込むことは不可能な場合もあります。

ORACLE

目次

ORACLE

エグゼクティブ・サマリー

本書では、Oracle Cloud Infrastructure (OCI)がゼロ・トラスト・アーキテクチャのデプロイをどのように加速するかを解説します。本書では、英国国家サイバー・セキュリティ・センター(NCSC)の 8 つのゼロ・トラスト原則を、OCI のコントロールについて説明するためのフレームワークとして使用しています。このリストには、次のゼロ・トラスト原則が含まれています。

- ユーザー、デバイス、サービス、データなどのアーキテクチャを把握する。
- ユーザー、サービス、デバイスのアイデンティティを把握する。
- ユーザーの行動、サービス、デバイスのヘルスを評価する。
- ポリシーを使用して要求を認可する。
- あらゆる場所で認証と認可を行う。
- ユーザー、デバイス、サービスを重点的に監視する。
- 自分のネットワークも含めて、どのネットワークも信頼しない。
- ゼロ・トラスト用に設計されたサービスを選択する。

NCSC は英国を拠点とし、英国の最も重要な組織を保護することに焦点を当てていますが、この指針は英国企業に固有のものではなく、世界各国の組織に適用することができます。

ORACLE

はじめに

サイバー・セキュリティや IT の専門家であれば、ゼロ・トラスト・セキュリティという言葉をよくご存じでしょう。ゼロ・トラスト・セキュリティでは、組織のネットワークに接続されたユーザーやデバイスの信頼度が低いことを前提に、信頼を築いて維持するための適切なセキュリティ・コントロールの設計とデプロイメントを検討します。ゼロ・トラスト・セキュリティの背後にある考え方は、パブリック・クラウドの成長や、外部の攻撃者だけでなく内部の関係者からも生じる脅威など、いくつかの要因によってこの 10 年で拡大しました。

ゼロ・トラスト・アプローチを採用するには、膨大な時間と努力を要します。組織全体で信頼を築いて維持する技術的アーキテクチャとビジネス・プロセスを採用できるように徐々に前進していくのだという固い決意が必要です。オラクルは、Oracle Cloud Infrastructure (OCI)を通じて、ゼロ・トラスト・イニシアチブを推進する組織を支援します。OCI は、お客様のクラウドでのワークロードを素早く効果的に保護するのに役立つ、組込みのセキュリティ機能を提供するよう設計されています。

多くの組織は、パブリック・クラウドを使用してコスト効果の高いインフラストラクチャ、プラットフォーム、ソフトウェア・サービスを提供することで、業務の変革を迅速化したいと考えています。オラクルは、OCI を次世代クラウドとして設計しました。OCI は、ハイパフォーマンス・コンピューティング(HPC)能力を備えており、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 Oracle Cloud データ・センターで、または Cloud@Customer デプロイメントを通じてお客様のサイトで実行します。OCI は、オラクルの自律型サービス、統合セキュリティ、サーバーレス・コンピュートを組み合せて、エンタープライズ・アプリケーションにリアルタイムの弾力性を提供します。OCI の核となる設計原則の 1 つに、セキュリティファースト・アプローチがあります。したがって、セキュリティは後から思いつきで追加されたものではなく、最初からプラットフォームに組み込まれています。オラクルは、次の理念に従ってお客様のクラウド保護を支援しています。

- **シンプルで容易**: 使いやすく、デプロイと運用が容易なセキュリティ・コントロールを設計する。
- **完全なコントロール**: 組織のアプリケーションやデータがどこにあろうと、それらを管理できるようにする。
- **緊密な統合**: Infrastructure-as-a-Service、Platform-as-a-Service、Software-as-a-Service (Iaas、PaaS、SaaS)や分散クラウド(ハイブリッドおよびマルチクラウド)のすべてにわたって組込みの統合セキュリティを提供し、手動のセキュリティ・タスクと人的エラーを削減する。

NCSC の 8 つの原則を見ていく前に、IT 部門とクラウド・プロバイダには、クラウドのセキュリティを管理する上でそれぞれ果たすべき役割があることを明確にする必要があります。

セキュリティ管理の観点から見ると、クラウドは根本的にオンプレミスとは異なっています。IT 部門は、ハードウェアを物理的に管理する、本番環境のテクノロジ・スタックを完全に管理するなど、オンプレミスのテクノロジ・インフラストラクチャを完全に管理していますが、クラウドではクラウド・サービス・プロバイダの管理下にあるコンポーネントが使用されます。そのため、クラウドにおけるセキュリティの管理は、図 1 に示すように共同で行われます。

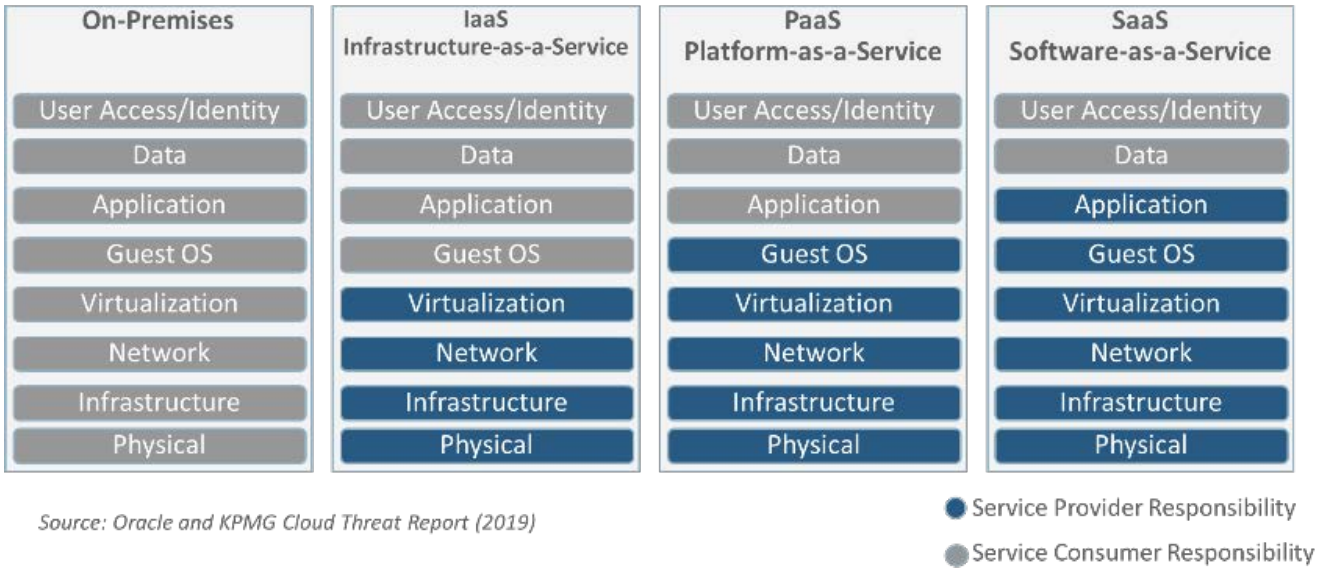


図1: セキュリティ管理上の様々な責任がお客様とクラウド・プロバイダの間でどのように分担されているかを示す概念図

OCI のセキュリティファーストの設計原則は、OCI のお客様に提供される強力なセキュリティ機能セットとともに、ゼロ・トラスト・セキュリティ・アーキテクチャの実装を支援します。

デプロイメントの中でゼロ・トラスト・アーキテクチャを目指す組織を支援するため、本書では、OCI のセキュリティ・コントロールと OCI Center for Internet Security (CIS)セキュア・ランディング・ゾーンを対応付けています。このランディング・ゾーン・テンプレートは、組織が CIS OCI Foundations Benchmark v2.0 に準拠するのに役立つ、標準化された環境を OCI テナンシにデプロイします。本書での対応付けには CIS セキュア・ランディング・ゾーンが使用されていますが、OCI オープン・ランディング・ゾーンや Oracle Enterprise ランディング・ゾーンなど、その他の OCI ランディング・ゾーンも使用可能です。
組織は、OCI にデプロイしようとしている必要なワークロードに基づいて、最適なランディング・ゾーンを評価する必要があります。

ORACLE

原則 1: ユーザー、デバイス、サービス、データなどのアーキテクチャを把握する

セキュリティ・アーキテクチャを設計するには、保護が必要なデータなど、既存のアセットを十分に理解する必要があります。NCSC の最初の 3 つの原則は検出に焦点を当てたもので、最初の原則はユーザーやデバイス、サービス、データなどの内部アーキテクチャを把握することに注目しています。

NCSC が強調しているように、アセット検出活動に取り組むことは、純粋に技術的な仕事ではない場合が多く、プロジェクトの文書や調達の記録、同僚との会話の見直しなどの作業が伴います。様々な部署や事業部門が独自のソリューションを実装しているために、アーキテクチャを把握するのが難しいこともあります。この問題は一般に「シャドウ IT」と呼ばれます。これは、Gartner によると、「IT 組織の所有権または管理が及ばない IT デバイス、ソフトウェア、サービス」を指します。

OCI には、アセット検出フェーズを迅速化する多数のツールやサービスが用意されています。これらを使用すると、表 1 にまとめたように、すでにデプロイされているものを特定して理解することができます。

表 1. アセット検出に役立つ原則 1 のコントロールと OCI ツール。

OCI コンポーネント	説明	提供される検出方法
Representational State Transfer アプリケーション・プログラミング・インタフェース(REST API)	OCI は、OCI テナンシにアクセスして管理するための REST API を提供します。各種言語向けの SDK と CLI も用意されており、これらすべてを OCI テナンシへのプログラム的なアクセスに使用できます。	OCI テナンシ内で作成されたリソースをすべて列挙するスクリプトを作成できます。OCI CLI を使用したスクリプト作成の例については、ドキュメントを参照してください。
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)**	OCI リソース・タグにより、キーと値を定義してリソースに関連付けることができます。	組織は、リソース・タグを使用して、特定のプロジェクトやシステムに使用されるリソースを整理し、リストすることができます。
Terraform	オラクルは、Infrastructure-as-Code (IaC)を介した OCI デプロイメントの実装を可能にする、Terraform 向けの OCI プロバイダを提供しています。	Terraform Discovery を使用すると、既存のデプロイ済フットプリントに基づいた IaC スクリプトを作成し、既存の OCI デプロイメントを文書化することができます。
監査	OCI が提供する Audit サービスでは、コンソール、API、SDK、CLI カスタム・クライアントや他の OCI サービスによって行われたコールなど、サポートされているすべての OCI パブリック API エンドポイントへのコールをログ・イベントとして自動的に記録します。	OCI 内の監査を使用すると、どのサービスがコールされているか、それらのコールを誰が行っているか、どのコールが成功したか、どのコールが不正であるかを理解できます。
VCN フロー・ログ	OCI 内の仮想クラウド・ネットワーク(VCN)フロー・ログは、VCN 内および VCN との間のトラフィックの接続情報を可視化します。	VCN フロー・ログを使用すると、どのようなトラフィックがどのポートを介してサービス間を流れているかを理解できます。この情報は、検出フェーズの一環としてデータ・フローを理解する上できわめて有用です。
既存のプラットフォーム・サービス	OCI には、包括的な PaaS サービスのセットが含まれており、統合、ガバナンス、アイデンティティ、セキュリティ、データ管理、分析などの幅広い機能を網羅しています。	たとえば、次のようなプラットフォーム・サービスを使用して既存のデプロイメントを理解できます。

		• **OCI Identity and Access Management (IAM)と Oracle Access Governance**: ユーザーとそのロールおよびアクセス権限を検出します。 • **Oracle Integration Cloud** と **Oracle API Gateway**: 既存のデータ・フローを特定します。 • **Oracle Data Safe**: オンプレミスとクラウドのどちらで実行されているかに関係なく、Oracle Database 内の機微なデータを特定します。 • **Oracle Data Catalog**: データとデータ・ガバナンスを管理し、既存のデータ・アセットの貴重なリポジトリを提供します。 • **Oracle Container Registry**: DevOps デプロイメント用に公開されているアプリケーションとサービスをリストします。 • **Oracle Container Engine for Kubernetes (OKE)と Oracle Resource Manager**: 実行されているアプリケーションとサービスを特定します。
OCI CIS ランディング・ゾーン・コンプライアンス・チェック・スクリプト  *CIS セキュア・ランディング・ゾーン*	このスクリプトは、テナンシの構成を CIS OCI Foundations Benchmark に対してチェックします。CIS のチェックに加えて、OCI のベスト・プラクティスに準拠しているかどうかもチェックできます。	スクリプトを使用して、テナンシのセキュリティ・ベースライン構成を業界のベスト・プラクティス(CIS のベスト・プラクティスなど)に対してチェックできます。

表 1 の OCI コンポーネントに加えて、オラクルは OCI ドキュメント・テンプレートと、検出、評価、および OCI プロジェクトの計画用のフレームワークも提供しています。

原則 2: ユーザー、サービス、デバイスのアイデンティティを把握する

クラウドへの移行が徐々に進むのに伴い、従来のネットワーク境界の侵食が加速しています。そのため、アイデンティティが新たな境界として認識されるようになりました。オラクルは、アイデンティティ・ドメインの概念を使用する、OCI Identity and Access Management (IAM)というエンタープライズクラスの Identity-as-a-Service (IDaaS)プラットフォームを提供しています。OCI IAM ドメインでは、OCI IAM と Oracle Identity Cloud サービスの機能が 1 つの統合サービスにまとめられています。OCI IAM は、OCI のクラウド・ネイティブ・サービスである Oracle Access Governance サービスと連携します。このサービスは、アイデンティティ用にクラウド環境とオンプレミス環境へのアクセスを管理するための全社規模の可視性を提供します。

OCI IAM サービスは、オラクルのクラウド・サービスへのフロント・ドアとして、また、エンタープライズ・ユーザーと消費者の双方を対象としたスタンドアロンの IDaaS プラットフォームとして機能します。これにより、OCI、サードパーティ・クラウド、および内部データ・センターで実行されているアプリケーションとサービスに重要なアイデンティティ管理機能がもたらされます。

アイデンティティは NCSC の 2 番目の原則の核となる理念であり、OCI IAM と Oracle Access Governance はこの原則を遵守するのに役立ちます。

ユーザーのアイデンティティ

OCI は、主に次のタイプのユーザー・アイデンティティを利用します。

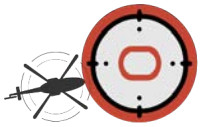
- OCI にアクセスし、OCI プラットフォーム自体の内部でネットワークの作成、Compute インスタンスのバックアップ、暗号化鍵の管理などの機能を実行する管理ユーザー。
- OCI の内部(Oracle Analytics Cloud 内など)または外部で実行されているアプリケーションにアクセスするエンドユーザー。

どちらのユーザー・タイプについても、OCI IAM はユーザーのアイデンティティ、属性、アクセス権限を管理する機能を提供します。

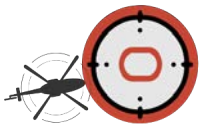
オラクルのアイデンティティ・サービスは主要なアイデンティティ・リポジトリとして機能できますが、多くの組織では、複数のアイデンティティ管理システムが特に従業員向けに導入されています。このような場合、OCI はそれらの既存のサービスと統合でき、ユース・ケースによっては既存のサービスの機能を拡張することも可能です。

表 2 は、OCI IAM および Oracle Access Governance が、NCSC がアイデンティティ・サービスで実現すべきと述べている機能にどのように対応するかを示しています。

表 2. OCI IAM で豊富なアイデンティティ機能のセットを提供する原則 2 のコントロール。

アイデンティティ・サービスの機能	説明
グループを作成する  *CIS セキュア・ランディング・ゾーン*	OCI IAM は、アイデンティティ・ドメイン内にグループを作成して管理する機能を提供します。作成したアイデンティティは、グループに割り当てたり、グループから取り消したりできます。 次のいずれかの方法を使用してグループを管理できます。 • **Web ベースのコンソール**: このサービスには、管理およびセルフサービス向けの豊富な機能を備えた Web ベースのコンソールが用意されています。 • **System for Cross-domain Identity Management (SCIM) ベースの REST API**: SCIM REST API、または SDK などの API 派生物のいずれかを使用して、管理を実行できます。 **同期**: すぐに使える多数のコネクタにより、グループやグループ・メンバーシップなどのアイデンティティをソース・システムから直接同期できます。たとえば、一般的な人材管理(HCM)クラウド・サービスやオンプレミス・リポジトリ向けのコネクタとして、Active Directory ブリッジを使用できます。

最小権限になるように構成されたロールを定義する



CIS セキュア・ランディング・ゾーン

OCI IAM はデフォルトで、OCI 内のアクセスを拒否します。管理者は、OCI 権限が付与された少なくとも 1 つのグループに割り当てられるまで、どのリソースにもアクセスできません。OCI 内の認可はすべて IAM ポリシーを通じて行われます。IAM ポリシーには、アクセス・ポリシーを作成するための使いやすいポリシー構文が用意されています。
次に例を示します。

```
Allow group OCIDBAdmins to manage database-family in tenancy
```

こうしたポリシーはグループに割り当てられ、そのグループのメンバーが権限を継承します。

OCI IAM に統合されたアプリケーションにアクセスする場合、通常はユーザーがグループに割り当てられます。グループは、1 つ以上のアプリケーションやアプリケーション・ロールにマッピングされるまで、どのサービスにアクセスする権限も持ちません。グループがアプリケーションまたはアプリケーション・ロールにマッピングされると、そのグループに割り当てられたエンドユーザーは適切な権限を持つようになります。

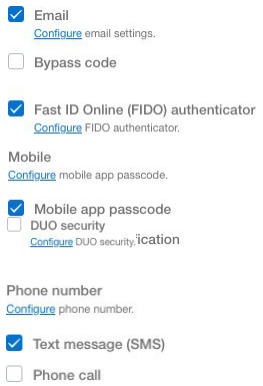
ユーザー管理の観点から見ると、あらかじめ定義されたいくつかの管理ロールが様々なレベルの管理アクセスを提供します。そのため、どの管理者にも、必要最小限の管理権限のみが付与されます。

Oracle Access Governance は、アクセス権限と OCI のポリシー・レビューに関するインサイトを提供し、異常を特定し、セキュリティ・リスクへの対策を講じることで、ロールのセキュリティをさらに強化します。

Oracle Access Governance を使用すると、属性ベース、ポリシーベース、ロールベースのアクセス制御のための動的なアイデンティティ・コレクションとアクセス・バンドルを実装できます。また、潜在的なセキュリティ侵害に関する実用的なインサイトが得られるため、アイデンティティやアクセスの課題への迅速な対処が可能になります。こうした機能により、ユーザーは自分の職務を遂行するのに必要な権限のみを持つことができます。

強力な最新の認証方式をサポートする

OCI IAM は、右に示すように、多要素認証(MFA)やパスワードレス認証、リスクベース認証などの幅広い認証ファクタをサポートしています。



サポートされている多要素方式には、時間ベースのワンタイム・パスコード(TOTP)、プッシュベースの通知、電話、SMS、電子メール、セキュリティ質問、バイパス・コード、Duo Security トークン、X.509 証明書などがあります。

業界のオープン標準である FIDO2 を使用したパスワードレス認証もサポートされているため、この標準に準拠した Yubikey や TouchID、FaceID、Windows Hello などの認証方式のサポートも可能になっています。

OCI IAM 内のリスクベース認証を使用すると、ユーザーの要求のコンテキストをいくつかのリスク要因に照らして検討、評価し、要求を許可するのか、ブロックするのか、追加の認証ファクタ(前述のファクタのいずれかなど)にチャレンジするのかを決定できます。

資格証明をユーザーに安全にプロビジョニングする	どのようにして資格証明をユーザーに安全にプロビジョニングするかは、ユーザーの作成方法によって異なります。たとえば、次の方法があります。 • **自己登録**: ユーザーが自己登録する場合、登録時に自分のパスワードを(構成可能パスワード・ポリシーに従って)作成できます。 • **管理アクション**: 管理者がユーザーのアイデンティティ・レコードを作成する場合、期限付きのリンクがユーザーにメール送信されるので、ユーザーはリンク先で自分のパスワードを設定できます。同様に、管理パスワードをリセットする場合も同じフローに従います。 • **同期**: 多くの場合、同期されたユーザーは OCI IAM に対して直接認証されるのではなく、Security Assertion Markup Language (SAML)を使用するなどの方法で、フェデレーテッド・シングル・サインオン(SSO)によって認証されます。こうしたユーザーについては、オラクルはユーザーのパスワードの格納や保守を行いません。かわりに、アイデンティティ・レコード(ユーザーのパスワードを除く)が 2 つのフェデレーテッド・プロバイダ間で同期されます。 • **委任認証**: OCI IAM は、ユーザーの Active Directory 資格証明を使用した認証をサポートしています。この場合、サービスではユーザーのパスワードを管理しません。
サービスに対して認証する	オラクルは、フェデレーテッド認証用の業界のオープン標準をサポートしています。たとえば、SAML 2.0、OAuth 2.0、OpenID Connect などです。これらの標準を使用してサービスに対して認証したり、接続されているアプリケーションへの SSO を容易にしたりすることができます。 ターゲット・アプリケーションがオープン標準をサポートしていない場合は、App Gateway をオラクルとアプリケーションの間のリバースプロキシ・ブリッジとして使用し、オープン標準トークンを、保護されたアプリケーションが理解できるヘッダー変数などの形式に変換することができます。
外部サービスでのユーザー・アイデンティティを管理する	OCI IAM は SCIM 2.0 オープン標準をサポートしています。広く使用されている一般的なターゲット・アプリケーションおよびサービスとの統合を加速するために、多くのアプリケーション・テンプレートが用意されています。SCIM テンプレートも用意されています。 このサービスでは、ターゲット・アプリケーションでアイデンティティを管理するための SCIM メッセージの生成と、信頼できるソース(源泉)からの SCIM メッセージの消費の両方が可能です。 Oracle Access Governance は、あらかじめ構築された標準ベースのいくつかのコネクタを使用して、様々な外部システムにまたがったアイデンティティのプロビジョニングをサポートしています。
ジョイナー、ムーバー、リーバー(JML)プロセスをサポートする	オラクルは、前述の SCIM インタフェース、または利用可能なその他の同期方式のいずれかによるジョイナー、ムーバー、リーバー(JML)プロセスをサポートしています。 このサービスでは、外部アイデンティティ・サービスからの JML メッセージの消費と、ターゲット・アプリケーションおよびサービスへの JML メッセージの生成が可能です。 JML メッセージを消費する際には、信頼できるソースまたは信頼できないソースとしてフィードを使用できます。つまり、ソースでは、ソースがまだ存在しないアイデンティティ・レコードを作成するか、ターゲット・システム内のアカウントを表すアカウント・レコードを作成して、アイデンティティ・レコードにリンクさせることができます。

サードパーティのフェデレーテッド ID をサポートする	JML メッセージを生成する際、OCI では、どのメッセージ・イベントが生成されるかを管理できます。どちらの場合も、一般的なソース・アプリケーションとターゲット・アプリケーション向けのアプリケーション・テンプレートが用意されています。 OCI は、SAML や OAuth、OpenID Connect などの標準による SSO と、SCIM やすぐに使用できるその他の同期機能によるユーザー管理の両方で、フェデレーテッド・アイデンティティをサポートしています。

NCSC が原則 2 で説明しているように、ユーザーの同意はアイデンティティ・システムの重要な要素です。OCI IAM は、次の分野での同意管理をサポートしています。

- OCI IAM 内の使用条件同意機能を使用すると、お客様は免責条項と利用規定をユーザーに提示できます。
- OAuth のサポートにより、ユーザーはアクセスの範囲を指定できます。
- エンドユーザー・トークンの使用原則により、バックエンド・リソースに対する同意をアプリケーションで証明できます。

サービスのアイデンティティ

ゼロ・トラスト・セキュリティは OCI の重要な設計原則ですが、アイデンティティも同様です。オラクルは、クラウド・ネイティブなアイデンティティ・サービスをマイクロサービス方式で構築しており、各マイクロサービスがセキュア・プロトコルを使用して相手のマイクロサービスを認証します。この設計では、これらのマイクロサービスが最初から相互に信頼できる必要はありません。

OCI は、様々なタイプのアイデンティティ向けに一貫したリポジトリを提供していますが、ゼロ・トラスト・セキュリティの実現に役立つ機能が他にもあります。

ユーザー・アイデンティティに加えて、OCI には、インスタンス・プリンシパルという Compute インスタンス向けのアイデンティティが用意されています。Compute インスタンスは、ストレージやデータベース、ネットワーキングなど、他の OCI サービスにアクセスしなければならないことがよくあります。これらのリソースへの認証済アクセスを実現するために、リソースの資格証明を Compute インスタンス内に組み込むというのが従来の方法でした。しかし、この方法では、責任を持って資格証明を管理し、定期的にローテーションする必要があるため、管理オーバーヘッドが増えます。OCI のインスタンス・プリンシパルを使用すれば、Compute インスタンス内に資格証明を組み込む必要はなくなります。OCI は、そうした Compute インスタンスの資格証明を絶えずローテーションするという複雑さに対処しています。

リソース・プリンシパルの概念はインスタンス・プリンシパルに似ていますが、サーバーレス・ファンクションなどのインスタンスではないリソースに用いることで、他の OCI リソースへのアクセスが可能になります。

OCI IAM では、インスタンス・プリンシパルとリソース・プリンシパルを使用して、長期的な資格証明を組み込むよりも安全な方法でアクセス制御を可能にしています。これらのプリンシパルに対して、ユーザー・アイデンティティ用に記述するポリシーに似た IAM ポリシーを記述します。これにより、ユーザー・アイデンティティとインスタンス・プリンシパルおよびリソース・プリンシパル用の認可ポリシーが OCI IAM 内で一元的に定義されます。

インスタンス・プリンシパルとリソース・プリンシパルの資格証明として証明書が使用されます。この証明書の管理は、作成、割当て、ローテーションも含めて OCI で自動的に行われます。

さらに、OCI 管理者は、インスタンス・プリンシパルまたはリソース・プリンシパルによって実行できる権限を決定する IAM ポリシーを記述します。Compute インスタンスは、グループ・メンバーシップ・ルールに基づいて動的グループにまとめられ、メンバーシップ・ルールに一致するすべての Compute インスタンスが、それらの動的グループに割り当てられた OCI 権限を継承します。次のインスタンス・プリンシパルの例について考えてみます。

```
Allow dynamic-group AppServersProd to inspect objects in compartment images
```

Compute インスタンスで実行されているアプリケーションまたはシステムがエンドポイント(API エンドポイントやデータベース)にアクセスするための資格証明を必要とするような状況に備えて、OCI は Secrets Management を提供しています。

このサービスでは、IPS 140-2 レベル 3 のハードウェア・セキュリティ・モジュール(HSM)に格納されている、お客様管理のマスター暗号化鍵を使用して暗号化されたシークレットを安全に格納し、取り出すことができます。このシークレットによって参照されるアイデンティティは、アイデンティティ・サービスに格納し、管理することができます。

デバイスのアイデンティティ

OCI は、デバイスのアイデンティティを管理するためのエンドポイント・セキュリティやエンタープライズ・モビリティ管理を提供しません。ただし、OCI IAM では、認証中に収集されたデバイスのフィンガープリントに基づき、リスクベースの認証方式の一部としてデバイス情報を利用できます。たとえば、ユーザーが新しいデバイスから認証しようとした場合、それに対応してユーザーのリスク・スコアを上げ、さらに強力な認証にチャレンジする、認証の試行を拒否するといった適切な措置を取ることができます。リスク要因には、サインインの失敗回数が多すぎる、疑わしい IP アドレスからアクセスした、などがあります。

原則 3: ユーザーの行動、サービス、デバイスのヘルスを評価する

原則 2 では、OCI IAM は OCI における重要なセキュリティ・コントロールとして認識されています。ユーザー、デバイス、サービスのヘルスを監視する際にも同じサービスが使用されます。

デバイスのヘルス

デバイスのヘルスは MFA の一部として監視できます。MFA 用に使用しているファクタが時間ベースのワンタイム・パスワード(OTP)でもプッシュ通知でも、Oracle Mobile Authenticator を使用できます。MFA 構成の一環として、OS バージョンのチェックや root 化されたデバイスのチェックなどのコンプライアンス・ポリシーを設定し、特定のデバイス構成設定を適用することができます(次の図を参照)。

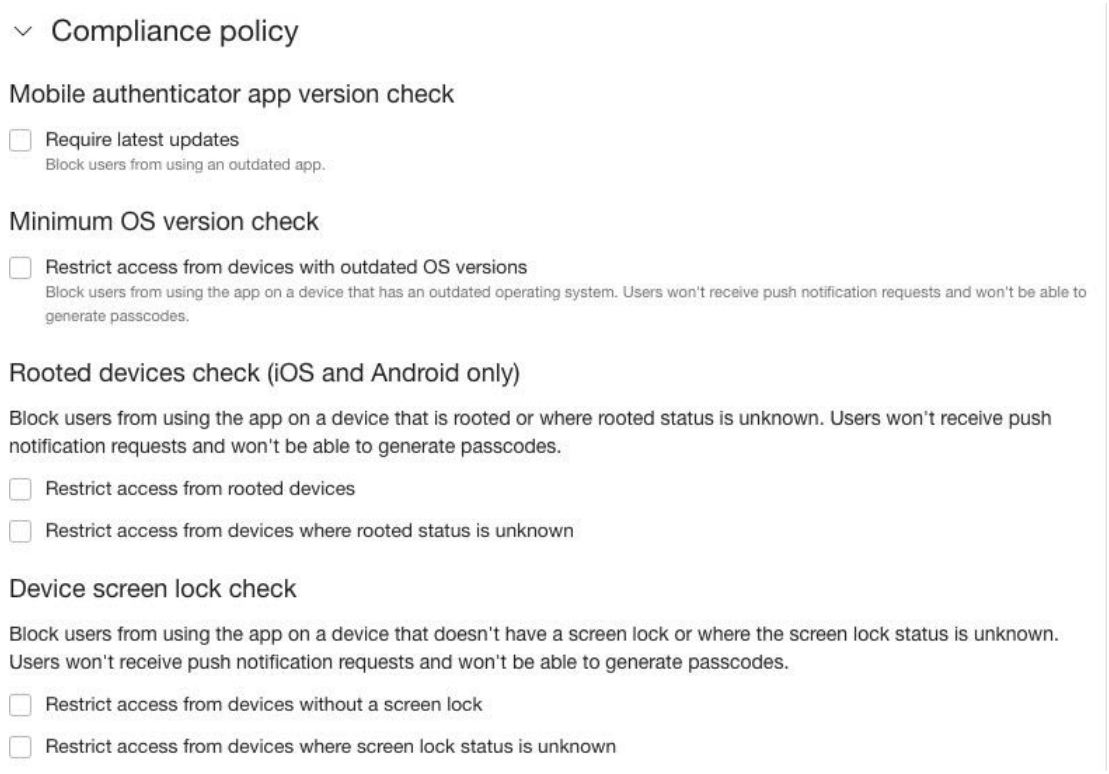


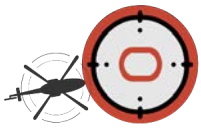
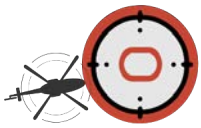
図 2: Oracle Mobile Authenticator でデバイスのコンプライアンスを確保

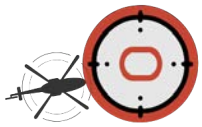
デバイスのヘルスを確認する際に考慮すべきもう 1 つのポイントは、IaaS の実行時に使用される Compute インスタンスの状態です。OCI において、サーバーやハイパーバイザをはじめとする各種インフラストラクチャ・コンポーネントの信頼度は低いとすることは、重要な理念であり設計原則です。そのため、OCI 全体にわたって多数のセキュリティ・コントロールが導入されています。たとえば、OCI ハードウェアの信頼の基点は、ハードウェアベースの信頼の基点(Root of Trust)テクノロジを使用して、OCI のお客様のテナントに対するファームウェアベースの攻撃のリスクを低減します。このテクノロジは、新しいサーバーがプロビジョニングされたり、新しいお客様のテナンシが設定されたりするたびに、ファームウェアをワイプして再インストールするように設計されています。さらに、保護インスタンスはセキュア・ブート、測定ブート、トラステッド・プラットフォーム・モジュール(TPM)を組み合せて使用し、Compute インスタンスでのファームウェアのセキュリティを悪意のあるブートレベルのソフトウェアから保護するのに役立ちます。

サービスのヘルス

OCI には、サービスのヘルスを確立するための機能がいくつか実装されています。次の表にその概要を示します。

表 3. 原則 3 のコントロール - OCI が提供するヘルス監視機能

OCI の機能	説明	ヘルス情報
自律型サービス	Autonomous Linux は、ゼロ・ダウンタイムや自動パッチ適用、既知の不正使用の検出など、核となるセキュリティ機能を提供し、複雑さと人的エラーを最小限に抑えてセキュリティと可用性を向上させます。 Autonomous Database は、自動パッチ適用、職務分掌の徹底、保存時と転送中のデフォルトでの暗号化といった自己保護機能により、機微なデータや規制対象のデータを自動的に保護します。	Autonomous Linux と Autonomous Database を使用すると、自動化と機械学習(ML)により、サービスのヘルスが向上します。
OS 管理	OS 管理では、Autonomous Linux を実行していない OCI インスタンスにおけるオペレーティング・システム環境のアップデートとパッチを管理できます。	OS 管理を使用すると、アプリケーションやサービスを実行しているオペレーティング・システムに常に最新のパッチが適用されていることを確認し、OS の既知の脆弱性が悪用されるリスクを抑えることができます。
監査とロギング  *CIS セキュア・ランディング・ゾーン*	OCI Logging サービスでは、OCI Audit やサービス・ログ、カスタム・ログなど、テナンシ内の OCI リソースで生成されたすべてのログにアクセスできます。 さらに、OCI Logging Analytics では、クラウドかオンプレミスかを問わず、アプリケーションやシステム・インフラストラクチャからあらゆるログ・データを取得して分析することができます。	OCI テナンシやテナンシで実行されているアプリケーションおよびサービス全体でログ・データと監査データを生成し、これらをコンソールで対話的に、あるいは API でプログラム的に問い合せて、データを分析することができます。
脆弱性スキャン  *CIS セキュア・ランディング・ゾーン*	OCI Vulnerability Scanning サービスでは、インストールされているパッケージやアーティファクトをスキャンし、お客様の Compute インスタンスや OCI Container Registry (OCIR) リポジトリ内のコンテナ・イメージに既知の脆弱性が存在しないか調べます。 Vulnerability Scanning は一部、ホストのスキャン用の Cloud Guard Instance Security に置き換わりました。現在、Vulnerability Scanning と Cloud Guard Instance Security をホストのスキャンに使用できますが、Vulnerability Scanning はコンテナ・イメージのスキャンにも引き続き使用できます。 また、このサービスでは、インスタンスでパブリックおよびプライベートに開かれているポートがないかスキャンし、各インスタンスの構成を特定の OS CIS ベンチマークに照らして確認します。	こうした Vulnerability Scanning での調査結果をもとに、どのパッケージにパッチを適用する必要があるか、どのようなセキュリティ強化手段を取るかを判断できます。 Vulnerability Scanning はデフォルトで Cloud Guard と統合されているため、ユーザーは自分のインスタンスやコンテナ・イメージの脆弱性の状況を 1 箇所で確認できます。

イベント  *CIS セキュア・ランディング・ゾーン*	OCI サービスは、リソースの変化を示す、業界標準の CloudEvent 形式のイベントを発行します。 こうしたイベントに対して、次の例に示すような措置を取ることができます。 • **通知**: 電子メールや SMS 通知を送信する • **ファンクション**: 業界標準の Fn プロジェクトに基づいてサーバーレス・ファンクションを実行する • **ストリーミング**: ストリームにイベントを発行する	イベントを使用すると、リソースの変化を示し、サービスのヘルスの潜在的な変化を特定することができます。
オペレーショナル・インサイト	オペレーショナル・インサイトは、Oracle Autonomous Database のリソースの使用状況とキャパシティに関する 360 度のインサイトを提供します。	オペレーショナル・インサイトを使用すると、CPU の使用状況とストレージ・リソースを監視し、異常な動作を探すことで、セキュリティの問題を特定できます。
Cloud Advisor	Cloud Advisor は、テナンシにおける潜在的な非効率性を検出して、対処方法を説明するガイド付きソリューションを提供し、セキュリティとコスト管理の両面をカバーします。	Cloud Advisor を使用すると、コスト削減を実現できる領域や、Cloud Guard でセキュリティ・ポスチャの脆弱性が明らかになった、セキュリティの強化が必要な領域を特定して、テナンシの効率性を最大限に高めることができます。
Observability and Management Platform	Oracle Cloud Observability and Management Platform は、Logging、Log Analytics、Service Connector Hub などの一連の OCI サービスで構成されています。デプロイ先がマルチクラウド環境かオンプレミス環境かに関係なく、広範な標準ベースのエコシステム・サポートにより、クラウド・ネイティブな従来のテクノロジ全体にわたって可視性とインサイトが得られます。	Service Connector Hub では、管理者が OCI のサービス間のデータ移動や OCI のサービスからサードパーティの可観測性ツールへのデータ移動を 1 つの画面で管理、監視し、ほぼリアルタイムに対処することができます。 この統合プラットフォームは、テクノロジやクラウドの垣根を越えたフル・スタックの可視性と、統一テレメトリ、データ交換、応用機械学習などの機能を提供します。
コンテナ・イメージのスキャン、署名、検証	OCI Vulnerability Scanning では、リポジトリ内のイメージをスキャンしてセキュリティの脆弱性の有無を調べます。 イメージが公開後に変更されないことを保証するため、OCI Vault に格納されているマスター暗号化鍵を使用して OCI Registry 内のイメージに署名することができます。	イメージの署名を表示、検証して、イメージの整合性が損なわれていないことを保証します。 検証に成功したら、そのイメージを Kubernetes クラスタにデプロイできます。

ユーザーのヘルス

OCI IAM は、ユーザーのリスクやセキュリティ・ポスチャを監視するための機能を備えています。お客様が構成したリスク・プロバイダ設定に基づいて、アダプティブ・リスク・エンジンがユーザーのリスクを評価し、各ユーザーのリスク・スコアを保持します。認証のたびに評価されるこのスコアを認証プロセスの一部として使用し、アクセスを許可するのか、拒否するのか、追加のレベルの認証にチャレンジするのかを決定できます。ユーザーが 2 番目のファクタを事前に登録していない場合は、登録を必須にすることができます。

サインオン・ポリシーでユーザーからの追加のシグナル(ユーザーの場所やグループ・メンバーシップ、ユーザーがアクセスするアプリケーションなど)を考慮することもできます。認証の決定を下す際には、こうしたファクタをユーザーのリスク・スコアも含めて考慮します。図 3 に示す例では、Google Identity Provider を介して認証を行い、Federated Users グループのメンバーであるユーザーが、このサインイン・ポリシーに関連付けられたアプリケーションにアクセスしようとするたびに、もう 1 つのファクタを要求されます。

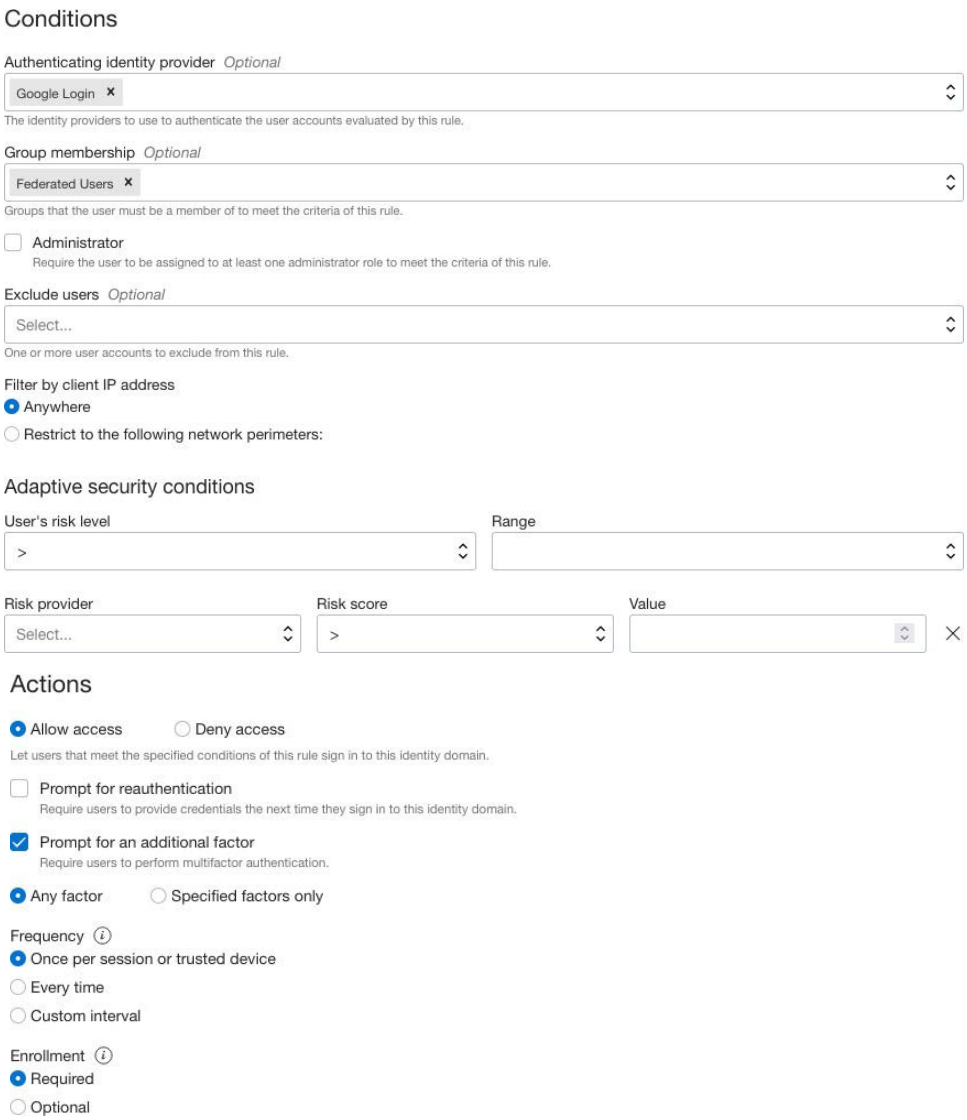


図 3: 認証中に複数のシグナルを評価

NCSC の原則 3 は、理想的な認証タイプとして FIDO2 標準によるパスワードレス認証を勧めています。OCI は、FIDO2 標準によるパスワードレス認証をサポートしています。

原則 4: ポリシーを使用して要求を認可する

認可は、多くの組織にとって長年の課題です。このテーマは次の領域に分けられます。

- **大まかな認可:** マクロレベルの認可ポリシーを参照し、通常は「ユーザーにはこのアプリケーションへのアクセス権があるか」という質問に答えます。
- **きめ細かな認可:** ユーザーがアプリケーションやサービスの内部で何を行う権限を持つかを決定します。

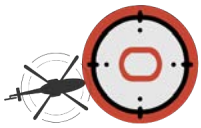
一元化された大まかな認可は多くの組織で当たり前のように実装されています。シングル・サインオンやロールベースのアクセス制御などのテクノロジを使用すれば、アイデンティティによってアクセスできるアプリケーションやサービスを制御するのは簡単です。

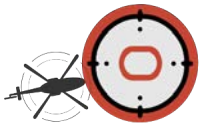
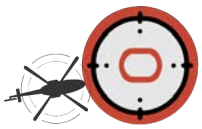
ところが、エンタープライズ規模のきめ細かな認可となると、かなり難易度が高くなります。通常、個々のアプリケーションやサービスがそれぞれ独自のきめ細かな認可を管理しています。eXtensible Access Control Markup Language (XACML)など、業界のオープン標準を使用してきめ細かな認可を一元化するためのテクノロジが利用可能です。多くの場合、こうしたテクノロジを広く採用すると、既成のアプリケーションの変更が必要になるか、カスタム・ソフトウェアの開発中にソフトウェア開発手法を変更することになります。

その結果、中央の SSO プラットフォーム内に大まかな認可を実装しながら、ターゲット・アプリケーションやターゲット・サービスがそれぞれ独自のきめ細かな認可を管理している状況は放置することになりがちです。

OCI では、リソースへのアクセスはすべて、必要な権限が割り当てられるまで拒否されます。この仕組みを提供するための機能の多くは、これまでの原則で説明しています。表 4 は、この原則の重要なコントロールをまとめたものです。

表 4. 原則 3 のコントロール - ポリシーベースの認証および認可のコントロール

OCI の機能	説明	適用可能なコントロール
OCI Identity and Access Management (IAM)  *CIS セキュア・ランディング・ゾーン*	OCI IAM は、保護の対象となる統合アプリケーション向けに、一元化された認証サービスおよび大まかな認可サービスを提供します。このサービスでは、要求に関連付けられたいくつかのシグナルを確認して、認証のレベルを決定します。 このサービスでは、ポリシーをグローバルに、または特定のアプリケーションに適用します。 OCI IAM を使用すると、エンタープライズ・ロールをアプリケーション・ロールや権限にマッピングし、ターゲット・アプリケーションにおける認可の管理に役立てることができます。 OCI IAM は、すべての OCI サービス向けに、一元的できめ細かな認可ポリシー・エンジンを提供します。このコントロールを使用すると、テナント管理者は、アイデンティティが OCI 内で OCI リソースへのアクセスと管理のために持つアクセス権のレベルを正確に決定できます。 この権限により、きめ細かな認可ポリシーを定義して、リソースに対して操作を実行する能力を制御することができます。	OCI IAM を使用すると、次のようなアイデンティティ機能のコア・セットが得られます。 • シングル・サインオン • リスクベースの適応型認証 • 多要素認証 • ロールベースのアクセス制御 様々なサインオン・ポリシーで様々なアプリケーションを保護します。 ロールのマッピングを通じてアプリケーションへの認可を制御します。OCI IAM を使用すると、「デフォルトで拒否」アプローチを利用して、ロールベースのきめ細かな認可ポリシーを定義できます。 OCI のリソースへのアクセスはすべて、インスタンス・プリンシパルとリソース・プリンシパルを介したユーザーとリソースも含め、IAM ポリシーを通じて明示的に認可される必要があります。

	OCI のポリシー・ステートメントでは、条件と権限または API 操作を組み合せて使用し、特定の動詞(inspect、read、use、manage など)によって付与されるアクセス権の範囲を狭めることができます。	
OCI コンパートメント  *CIS セキュア・ランディング・ゾーン*	OCI コンパートメントは、リソースの論理グループを提供し、リソースに対する大まかな認可ポリシーときめ細かな認可ポリシーの定義を可能にします。	OCI コンパートメントを使用すると、特定の条件下で OCI IAM ポリシーの範囲を特定のリソース・セットに狭めることができます。
OCI プラットフォーム・サービス	OCI プラットフォーム・サービスにより、通常はサービス内の権限にマッピングされたアプリケーションレベルのロールを通じて、各プラットフォーム・サービスが独自のきめ細かな認可を提供します。	アプリケーション・ロールを OCI IAM 内のロールにマッピングすることで、ロールベースのアクセス制御がユーザー認証からターゲット・アプリケーションまで途切れることなく行われるようになります。
セキュリティ・ゾーンとセキュリティ・アドバイザ  *CIS セキュア・ランディング・ゾーン*	セキュリティ・ゾーンを使用すると、機微な OCI リソースをデプロイするためのきわめて安全で制限の厳しいコンパートメントを作成できます。制限の厳しいポリシーにより、脆弱なセキュリティ・ポスチャが構成されるのを防止できます。 セキュリティ・ゾーン・ポリシーは、人的エラーを防止し、非常に機微なデータやリソースを保護するための規範的ガードレールとなります。組織は、セキュリティ・ゾーン・ポリシーのカスタム・セットを定義することで、どのポリシーがニーズに適しているかを判断できます。 セキュリティ・アドバイザは、最大セキュリティ・ゾーン数と密接に連係し、ガイド方式のインタフェースを提供することで、お客様が OCI 内の安全なリソースを最初から正しく効率的に作成できるように導きます。	セキュリティ・ゾーンを構成すると、最も機微なリソースでも、不適切な構成によってインターネットやその他の脆弱なセキュリティ・ポスチャに公開されないことを保証できます。 セキュリティ・アドバイザを使用すると、オブジェクト・ストレージ、Compute インスタンス、ファイル・システム、ブロック・ボリュームなど、作成した OCI リソースに推奨されるセキュリティ・プラクティスを実装できます。 セキュリティ・ゾーンとセキュリティ・アドバイザは、サービスの限度内で OCI のお客様に無償で提供されます。
Web アプリケーション・ファイアウォール (WAF)	WAF は、悪意のある要求や要求者からアプリケーションを保護するように設計された、クラウド・ネイティブな Web アプリケーション・ファイアウォールを提供します。 WAF には 2 つの保護モデルがあります。 エッジ・ポリシーは、オラクル管理のエッジ・ノードにデプロイされているお客様管理のポリシーで、インターネット上に公開された Web アプリケーションのレイヤー7 保護を可能にします。 ロード・バランサ・ポリシーは、お客様が VCN 内にデプロイする OCI パブリック・ロード・バランサまたはプライベート・ロード・バランサに適用される、お客様管理のポリシーです。	要求が許可された要求者からのものであることを保証するために使用できるアクセス制御ルールで WAF を構成します。 WAF を使用して、最新のセキュリティ標準(TLS など)をサポートしないレガシー・アプリケーション向けに追加のセキュリティ・レイヤーを提供することもできます。

OCI Certificates	OCI Certificates サービスでは、Secure Sockets Layer/Transport Layer Security (SSL/TLS)証明書をお客様が簡単に作成、デプロイ、管理できます。 OCI Certificates サービスを使用すると、組織は、OCI ロード・バランサや API Gateway などの統合サービスに SSL/TLS 証明書を自動的にデプロイできます。	組織は、OCI Certificates サービスを使用して、間違いが起こりやすい手動の証明書管理プロセスを避け、証明書の監視と更新を自動的に行うことができます。 柔軟な認証局(CA)階層では、OCI Certificates サービスは、プライベート CA を作成して CA ごとにきめ細かなセキュリティ・コントロールを提供するのに役立ちます。
機密コンピューティング	OCI Confidential Computing では、使用中のデータ、RAM 内のデータ、Compute インスタンスでの計算中のデータを暗号化して保護します。	この設定により、アプリケーションを変更しなくても、リアルタイムの暗号化を使用して分離を強化できます。 暗号化鍵は、セキュア・プロセッサによってハードウェア・レベルで保護されます。

認可用のポリシー・コントロールに加えて、原則 4 では保存時と転送中のデータの暗号化について説明しています。OCI では、ベア・メタル・サーバーのローカル NVMe 一時ストレージを除き、保存時のデータはすべてデフォルトで暗号化されます。暗号化されるデータには、サービス(ブロック・ストレージ、ブート・ボリューム、オブジェクト・ストレージ、ファイル・ストレージ・サービスや各種 Oracle Database クラウド・サービスなど)の保存時のデータが含まれます。保存時のデータの暗号化は、テナント管理者が有効にする必要のある機能ではありません。OCI 全体にわたって標準で有効になります。

さらに、お客様は OCI Key Management Service (KMS)を使用して、保存時のデータの暗号化用に組織独自のマスター暗号化鍵を管理できます。このサービスでは、FIPS 140-2 レベル 3 の動作保証された HSM を使用してキー・マテリアルを格納します。OCI KMS 内の仮想ボールト、プライベート・ボールト、外部 KMS は、OCI ストレージ、データベース、Fusion SaaS との統合をサポートしています。

KMS では、非対称鍵のストレージを生成して保護することも可能です。これを KMS エンドポイントとともに署名と暗号化に使用して、ペイロードの整合性を確保することができます。お客様は、OCI での鍵の格納および管理用に KMS 内の仮想ボールトまたはプライベート・ボールトを選択できます。

さらに、OCI External KMS を使用すると、OCI の外部で格納および管理されている暗号化鍵を使用できます。External KMS は、規制要件に応じて暗号化鍵をオンプレミスまたは OCI の外部に格納しなければならないお客様や、暗号化鍵の管理を強化したいお客様にとって便利です。

OCI KMS 内のボールトでは、お客様管理の鍵がオラクル管理のシングルテナント HSM またはマルチテナント HSM に格納されるのに対し、OCI Dedicated KMS は、お客様管理のシングルテナント HSM パーティションを提供する OCI の HSM ソリューションです。このフルマネージド型サービスを使用すると、お客様は、暗号化鍵とそれを格納する HSM パーティションを全面的に管理することができ、HSM への PKCS#11 ダイレクト・インタフェースも得られます。

転送中の暗号化用には、OCI は、API エンドポイントや Oracle Cloud コンソールなどのオラクルが公開したすべてのエンドポイントに対して、TLS 1.2 で暗号化された接続を提供します。Compute インスタンスの作成中に構成することで、Compute インスタンス、ブート・ボリューム、ブロック・ボリュームの間のトラフィックも暗号化できます。

認可ポリシーを検討する際に考慮すべき最後のポイントは、ネットワーク・レベルです。ゼロ・トラスト戦略の一部としてのネットワークは、信頼できないコンポーネントです。様々なアプリケーションやサービスの間のトラフィックを制限するなど、ネットワーク・レイヤーでもコントロールを実装する必要があります。

OCI は、ネットワークのイングレス・トラフィックとエグレス・トラフィックを制御するために、セキュリティ・リストとネットワーク・セキュリティ・グループ(NSG)の両方を提供しています。セキュリティ・リストがサブネット・レベルで定義され、各 Compute インスタンスの仮想ネットワーク・インタフェース(VNIC)に対して強制されるのに対し、NSG はグループ化された一連のリソースに適用されます(図 4 を参照)。セキュリティ・リストと NSG を組み合せて使用することで、組織の要件に対応できます。

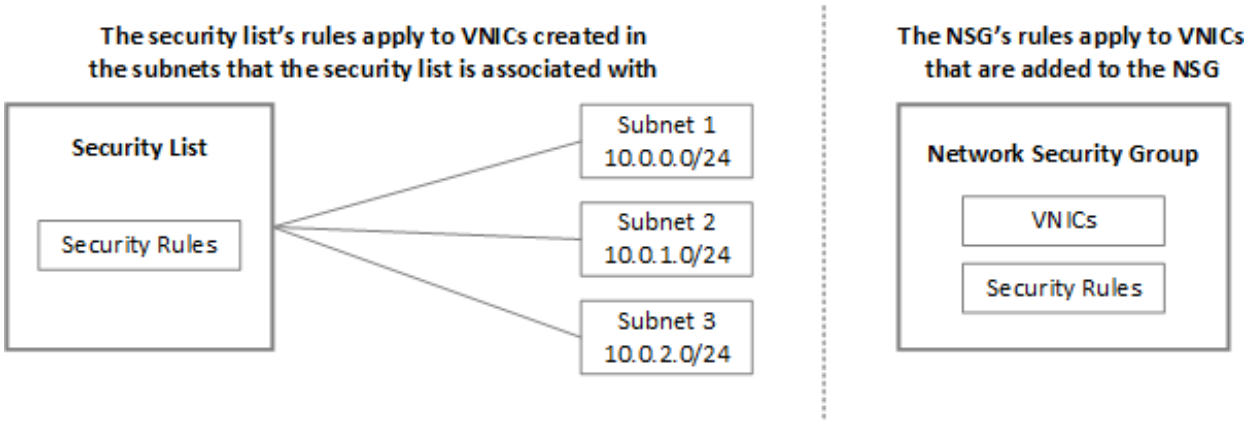


図 4: セキュリティ・リストとネットワーク・セキュリティ・グループは様々なレベルのきめ細かさで機能します。

原則 4 では、Break Glass アクセスの必要性についても説明しています。IAM ポリシーを適切に設計することで、必要な緊急アクセス権を付与できます。たとえば、一般的なアプローチとして、高度な権限を持つローカル・アカウントを作成し、このアカウントの資格証明は誰にも知らせずに、金庫などで安全に保管しておき、必要に応じて管理された状況下でのみアクセスするという方法があります。このような場合には、資格証明を使用するたびにローテーションするプロセスを用意しておく必要があります。また、高度な権限を持つユーザー・アカウントの資格証明を安全に格納するために、特権アクセス管理(PAM)ツールを使用するのも一般的です。その上で、必要に応じてそれらのアカウントを Break Glass 時のユーザーに割り当てることができます。OCI 内の監査、ロギング、監視を使用すると、必要な緊急アクセス用に追加のレベルのセキュリティを提供できます。

原則 5: あらゆる場所で認証と認可を行う

これまでの原則で詳しく説明したように、OCI は、アイデンティティ機能によって原則 5 に対応するコア・コントロールを提供しています。表 4 にそうしたコントロールの主な機能をまとめていますが、ユーザーおよびサービスの要求がすべて認証および認可されることをコントロールが保証します。その際に、アプリケーションやサービスにアクセスするエンドユーザーなのか、OCI にアクセスするパワー・ユーザーや管理者なのか、別のサービスにアクセスするサービスなのかは関係ありません。

これまでの原則との対応付けの中で、OCI IAM を使用して、構成可能な各種ファクタ(FIDO2 ベースのパスワードレス認証など)を使用した MFA を提供する方法と、要求に含まれている各種シグナル(場所、グループ・メンバーシップ、認証方式など)を使用した適応型のリスクベース認証を実現する方法について説明しています(図 4 を参照)。SAML、OAuth、OpenID Connect といった業界のオープン標準のサポートについても、それらをユーザーとサービス両方の要求に使用する方法と併せて説明しました。

ユーザーが一度認証を受けたら、資格証明を再度入力することなく他の認可済アプリケーションにシームレスにアクセスできる SSO を可能にするために、オープン標準が広く使用されていますが、すべてのアプリケーションがオープン標準をサポートしているわけではありません。ただし、OCI IAM は、そうした業界のオープン標準をサポートしていない Web アプリケーション向けに、App Gateway を使用して SSO を提供できます。

図 5 は、OCI がオープン標準をサポートする仕組みと、OCI IAM が OCI 向けだけでなく、OCI、サードパーティ・クラウド・プロバイダ、オンプレミスのいずれでホストされているかにかかわらずあらゆる Web ベース・アプリケーション向けにアイデンティティ・サービスを提供する仕組みを示しています。この図では、ユーザーは直接、または既存のアイデンティティ・プロバイダ(IdP)経由で OCI IAM に対して認証された後、認可済アプリケーションに SSO でアクセスできるようになります。アプリケーションが業界のオープン標準をサポートしているかどうかは関係ありません。

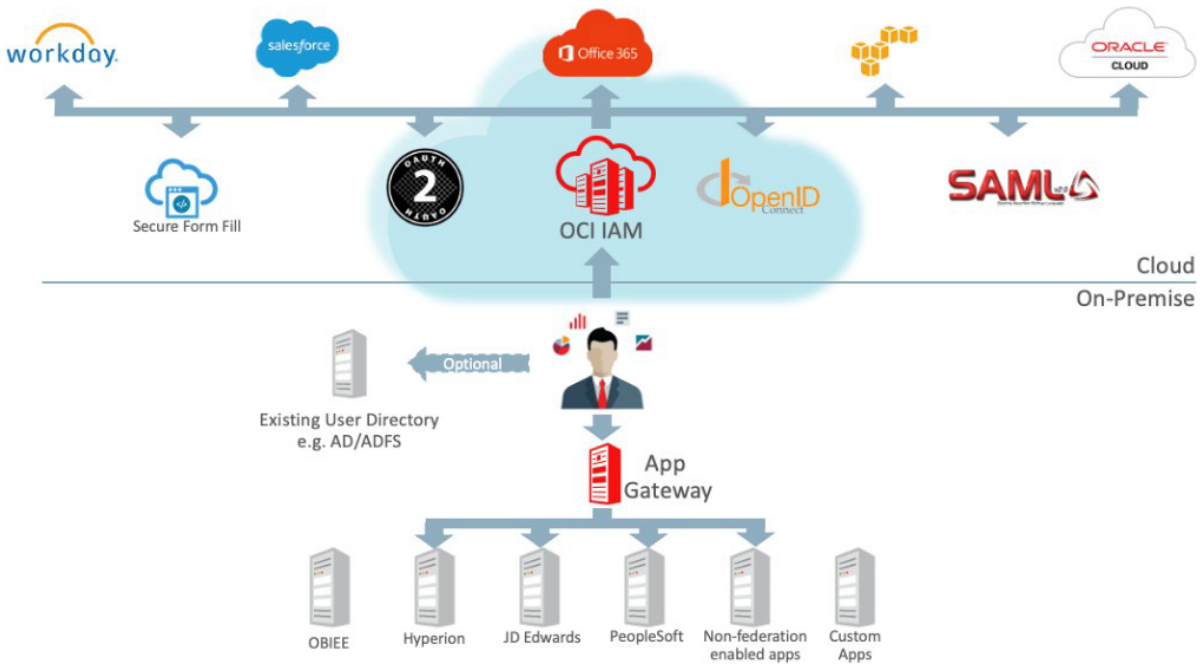


図 5: Oracle IAM をエンタープライズ・アイデンティティ・ハブとして使用。

次の概念をはじめとするサービス間通信のテーマについては、原則 2 でも説明しました。

- OCI Compute インスタンスやサーバーレス・ファンクションを他の OCI リソースに対して認証する安全なメカニズムとして、OCI のインスタンス・プリンシパルとリソース・プリンシパルを使用する方法
- OCI IAM ポリシーを使用して、OCI 内のリソースやサービスのアクセス制御を認可する方法。

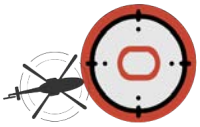
原則 6: ユーザー、デバイス、サービスを重点的に監視する

ゼロ・トラスト環境では、効果的かつ効率的な監視を行って、プラットフォームやアプリケーションで何が起こっているかを知ることが不可欠です。NCSC の原則 6 で勧められているように、ロギングと監視はネットワーク上の活動のパターンを特定するのに役立ちます。特定されたパターンはセキュリティ侵害のインジケータとなります。インシデント発生時には、ロギング・データをもとにセキュリティ侵害の発生元と範囲をより効果的に特定できます。この目的では、様々なリソースからキー・メトリックを継続的に収集し、異常な活動や定義済のセキュリティ・ベースラインからの逸脱が発生した場合には自動化されたアラームと是正措置をトリガーすることが必要になります。

サービスの監視

OCI では、テナンシのリソースとサービスを継続的かつ包括的に監視できます。OCI 内でサービスの監視を行うための 2 つの重要なコントロールについて、表 5 で詳しく説明しています。

表 5: OCI 内でのサービスの監視

OCI コンポーネント	説明	ヘルス情報
Cloud Guard  *CIS セキュア・ランディング・ゾーン*	Oracle Cloud Guard では、OCI のクラウド・セキュリティ・ポスチャ管理を一元的に確認できます。新しい Threat Detector を含む Oracle Cloud Guard は、正しく構成されていないリソースやテナントをまたがった安全でない活動、悪意のある脅威活動を検出します。さらに、クラウドのセキュリティの問題を切り分けて解決するための可視性をセキュリティ管理者に提供します。 すぐに使えるセキュリティ・レシピでセキュリティ上の不整合を自動的に修正し、セキュリティ・オペレーション・センターを効果的に拡張することができます。 Cloud Guard Instance Security は、Compute インスタンスをほぼリアルタイムに検査し、すぐに使えるディテクタを使用して MITRE-ATT&CK に準拠したランタイム・セキュリティ・アラートを提供します。	Cloud Guard を使用すると、サービスのセキュリティ・ポスチャが OCI テナンシ内の誤った構成や活動によって脆弱化していないことを保証できます。 Cloud Guard Threat Detector では、MITRE ATT&CK フレームワークに準拠したターゲット行動モデルを使用して、クラウド環境を継続的に監視できます。データ・サイエンスを適用することで、セキュリティ侵害を受けた環境を素早く検出できるので、お客様は最も重要な脅威アラートに集中できます。 Cloud Guard Instance Security では、Compute インスタンスのセキュリティ・ポスチャと、Compute インスタンスに関連するリスクおよび脆弱性を可視化できます。 Instance Security では、インスタンスのリモート問合せを可能にして脅威や疑わしい行動を検出することで、リモート・エンドポイントを可視化することもできます。
Threat Intelligence サービス	OCI Threat Intelligence は、多くの異なるソースから脅威インテリジェンス・データを収集し、そのデータを管理して、Oracle Cloud Guard やその他の OCI サービスで脅威の検出と予防を行うための実用的なガイダンスを提供します。	Threat Intelligence を起動するには、テナンシで Cloud Guard を有効にします。すると、既知の悪意ある IP に対するログの関連付けが開始されます。このサービスは、疑わしい IP 活動などの検出をデフォルトでサポートしています。

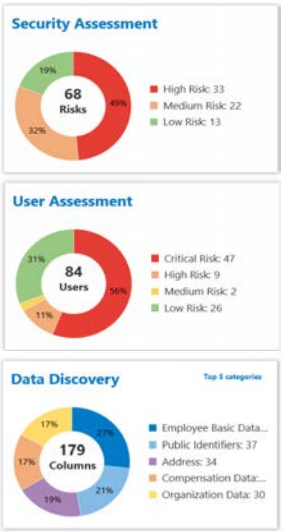
	このサービスは、オラクルのセキュリティ研究者、オラクル独自のユニークなテレメトリ、オープン・ソース・フィード(abuse.ch や Tor 出口リレーなど)から得たインサイトを提供します。	Threat Intelligence サービスは、インジケータの検索可能なデータベースも提供します。セキュリティ・アナリストはこれを使用して、インジケータに関する追加のコンテキスト情報を入手できます。
Data Safe	Oracle Data Safe は、Oracle データベースがクラウドとオンプレミスのどちらで実行されているかに関係なく、Oracle データベースのセキュリティおよびユーザー・リスク・アセスメントを提供します。 右に示すように、主要な検出結果が Data Safe 内のダッシュボードに表示されます。 	Data Safe を使用してデータベースのセキュリティ・ポスチャを監視し、セキュリティ・ポスチャの脆弱化につながる構成変更のリスクを軽減することができます。 ユーザー・アセスメントを利用すると、データベース・ユーザーのアカウントを定期的に確認して、不要な権限やデータベースに対する重大なリスクとなるユーザーを削除することができます。

表 3 および 4 に多くの機能が記載されていますが、注目すべき機能の 1 つに Web アプリケーション・ファイアウォールがあります。これは、インターネットからのトラフィック・フローや要求が Web アプリケーションに到着する前にすべて監視して検査する、リバース・プロキシの役割を果たします。この強力なサービスを使用すると、アプリケーション・サーバーへのデータを管理しながら、外部の脅威からサーバーを保護することができます。

さらに、すべての OCI サービスによってリソースのヘルス、キャパシティ、パフォーマンスに関するメトリックがパブリッシュされます。API を使用して、OCI Monitoring サービスにカスタム・メトリックをパブリッシュすることもできます。OCI Monitoring では、これらのメトリックを使用してリソースを監視します。メトリックがアラームで指定されたトリガーに一致すると、OCI Notification から通知が送信されます(図 6 を参照)。

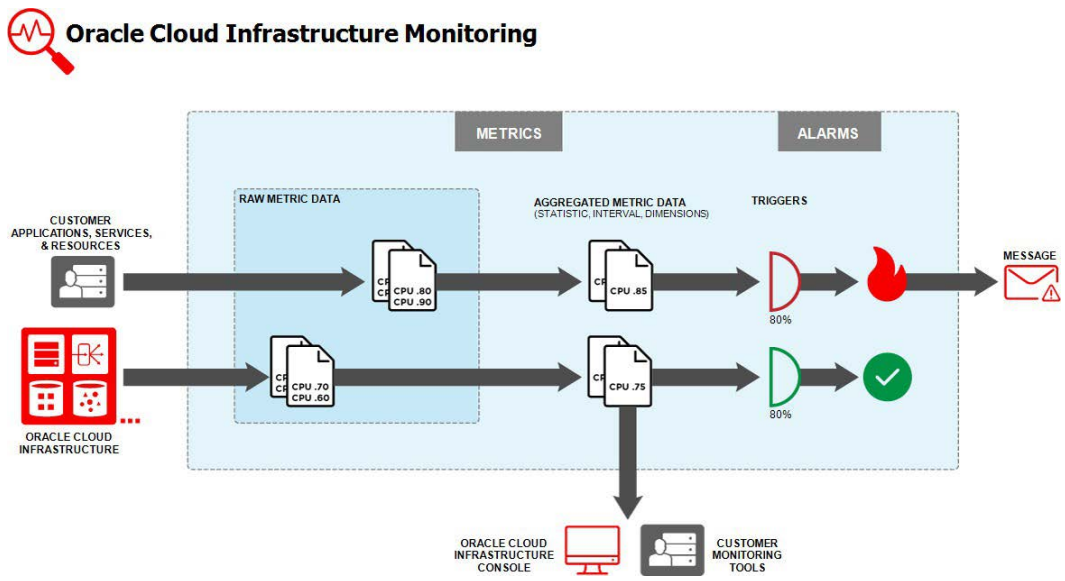


図 6: OCI の監視と通知。

ユーザーの監視

OCI IAM は、管理者およびエンドユーザーによるすべての操作(ユーザーのログイン、アプリケーションへのアクセス、パスワードのリセット、ユーザー・プロファイルの更新や、ユーザー、グループ、アプリケーションなどに対する作成、読取り、更新および削除(CRUD)など)に対応して監査データを生成します。この監査データには、SCIM 2.0 準拠の REST エンドポイントを介してアクセス可能です。これらの API を使用すると、組織の既存のセキュリティ・ツールにデータを統合できます。統合には、セキュリティ情報イベント管理(SIEM)システムを含めることができます。SIEM システムは、各種ソースからロギング・データを収集し、そのデータを照合してセキュリティ・イベントを探します。ユーザーおよびエンティティ行動分析(UEBA)システムとの統合も可能です。UEBA システムは、ロギング・データと活動データを収集し、通常の行動のパターンを作成した上で、ユーザーやその他のエンティティ(デバイスなど)の異常な行動を検出します。

デバイスの監視

エンドポイント・セキュリティとエンタープライズ・モビリティ管理は、オラクルが提供する継続的なデバイス監視用の機能の範囲を超えていることをこれまでの原則で説明しました。ただし、アイデンティティ・サービスによって収集されたデバイス・フットプリントに基づいてリスクベースの認証を実行することは可能です。OCI は、コンソールまたは API を使用した監視可能な Compute インスタンスの作成もサポートしています。

原則 6 は、信頼性の高いロギングを行うことの重要性を強調しています。OCI が提供する幅広い監査機能とロギング機能により、OCI テナンシでの活動に関して、誰がいつ何をしたかという観点から見たインサイトが得られます。OCI テナンシやテナンシで実行されているアプリケーションおよびサービス全体のログ・データと監査データが利用可能です。この情報をコンソールで対話的に、あるいは API でプログラム的に問い合せて、データを分析することができます。

OCI Logging サービスと OCI Audit サービスで生成されたログを分析するための効率的な SIEM を設定することで、クラウド・デプロイメントに対する脅威を検出して対応できます。OCI Functions では、こうした監査イベントを API でフェッチした後、監査データを処理し、HTTP イベント・コレクタを介して Splunk や QRadar などの SIEM にエクスポートすることができます。Splunk 向け OCI プラグインを使用すると、OCI Streaming 内のストリームから直接ログを取り込むことができます。管理者は、他の Splunk プラグインや脅威インテリジェンス・フィードなどのデータ・ソースと統合して、ログ・データからの警告を強化、拡張することもできます。

さらに、Cloud Guard Threat Detector で特定された疑わしい活動や悪意のある活動を組織の SIEM やセキュリティのオーケストレーション、自動化および対応(SOAR)システムに簡単にインポートできます。

ネットワークの監視

継続的なネットワーク監視を実行することは、VCN 内および VCN との間のトラフィックの接続情報の可視性を高める優れたサイバー・ハイジーンです。VCN フロー・ログは、VCN を通過するすべてのフローの詳細なメタデータ・レコードを保持し、このデータを OCI Logging サービスでの分析用に提示します。このデータには、トラフィックのソースと宛先に関する情報のほか、トラフィックのボリュームと、既存のネットワーク・セキュリティ・ルールに基づいて実行された承認または許可ポリシー・アクションが含まれています。この情報は、ネットワークの監視、トラブルシューティング、コンプライアンスに使用できます。Logging サービスとのクラウド・ネイティブな統合により、ログ・ファイルの表示と検索、オンプレミス SIEM へのエクスポートとストリーミングが可能です。

原則 7: 自分のネットワークも含めて、どのネットワークも信頼しない

オラクルは、クラウド・インフラストラクチャの重要な各種コンポーネント(サーバー、ハイパーバイザ、ネットワークなど)に寄せられた信頼を考慮し、これらの要素に対する基礎インフラストラクチャ内からの脅威を軽減する安全なアーキテクチャを設計しました。ハイパーバイザベースの攻撃によるリスクを減らし、テナントの分離度を高めるために、OCI では、セキュリティファーストのアーキテクチャを備えた仮想化スタックを設計し、お客様が最も重要なワークロードでも OCI を信頼できるようにしています。表 6 は、こうしたセキュリティ設計原則の一部をまとめたものです。

表 6: OCI のセキュリティファーストの設計原則

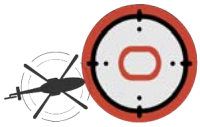
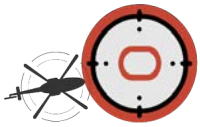
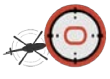
OCI のセキュリティの構成要素	説明	利点
サーバー **ハードウェアベースの信頼の基点**	OCI の主要な設計原則の 1 つに、ファームウェアベースの攻撃からテナントを保護することがあります。そのために必要なのは、サーバーを信頼しないこと、さらに具体的に言えば、サーバー上にあるファームウェアを信頼しないことです。 この方法を取る場合、新しいサーバーがテナントに対して、またはテナンシ間でプロビジョニングされるたびに、インスタンスのタイプにかかわらず、ゴールド状態のサーバー・ファームウェアをワイプして信頼できるソースから再インストールするプロセスが必要になります。	OCI ハードウェアの信頼の基点は、永続的なサービス拒否(PDoS)攻撃や、ファームウェアにバックドアを仕込んでデータを盗んだり、他の方法でデータを利用できなくする試みなど、ファームウェアベースの攻撃によるリスクを軽減するのに役立ちます。 この設計により、ファームウェアのセキュリティ侵害がすべてのお客様に広がるリスクを回避できます。
ハイパーバイザ **分離されたネットワーク仮想化**	分離されたネットワーク仮想化の基礎となる設計原則は、ネットワークの制御をハイパーバイザから排除し、OCI 内のすべてのサーバーにインストールされた別々の物理 SmartNIC に置くというものです。 このすぐに使える仮想化は、最大の分離と保護を実現し、影響範囲を限定します。	分離されたネットワーク仮想化は、ハイパーバイザの脱出やハイジャックを防止するのに役立ちます。強固な分離されたネットワーク仮想化レイヤーにより、あらゆる脅威をそのサーバー内に確実に封じ込めることができます。 この設計により、マシンがセキュリティ侵害を受けた場合のラテラル・ムーブメントが防止されるため、攻撃者がセキュリティ侵害を受けたマシンをピボット・ポイントとして使用してネットワーク上の他のマシンへ水平移動することはできなくなります。 OCI ネットワークのバックボーン全体でネットワーク・トラフィックのセキュリティを確保できます。
ネットワーク **ハイパーセグメンテーション**	OCI の物理ネットワークは、お客様とサービスを分離するように設計されています。このネットワークは、一意の通信プロファイルを持つエンクレーブにセグメント化されます。エンクレーブへのアクセスとエンクレーブからのアクセスは制御、監視されており、ポリシーに基づいています。 オラクルの従業員がサービス・エンクレーブにアクセスするには、権限を持つ担当者によって付与された明示的なユーザー権限が必要です。このアクセスは定期的な監査とレビューの対象となります。	ハイパーセグメンテーションにより、サービス・エンクレーブで実行されているクラウド・サービスのワークロードは、独自の物理ネットワークで実行されているお客様のワークロードから分離されます。 これを使用すると、OCI 基盤内でハーパーセグメント化されたエンクレーブ間のトラフィック・フローを厳密に監視および管理できます。

	サービス・エンクレーブはリージョンに対してローカルです。したがって、サービス・エンクレーブ間で必要なトラフィックは、インターネット・トラフィックと同じセキュリティ・メカニズム(インバウンドの Secure Shell (SSH)要塞ホストとアウトバウンドの SSL プロキシなど)を通過します。	エンクレーブへのアクセスとエンクレーブからのアクセスの両方を制御することで、OCI サービスのネットワークにおけるサービスの最小権限アクセスが実現します。
WAN 暗号化	OCI は、可用性ドメイン間およびリージョン間のプライベート・バックボーンでのレイヤー2 MACSec 暗号化を実装しています。 リージョン間トラフィックは、一意の鍵ペアを使用してリージョン間で認証されるため、不正なアクターが秘密鍵を盗んでリージョンを横断することはできません。	WAN 暗号化により、ネットワーク・スニッフィングが防止され、必要に応じてリージョンを信頼の対象から除外することが可能になります。
TLS パブリック・エンドポイント	オラクルが提供するエンドポイントはすべて、TLS 1.2 を使用して暗号化されます。	TLS パブリック・エンドポイントにより、中間者攻撃やネットワーク・スニッフィングの可能性が排除されます。
DDoS 保護	OCI は、一般的なレイヤー3 および 4 DDoS ボリューム攻撃(SYN フラッド、UDP フラッド、ICMP フラッド、NTP 増幅攻撃など)に対する常に有効な検出および軽減プラットフォームを提供します。この機能はデフォルトで提供され、ユーザーが意識することはありません。 オラクルは、レイヤー7 DDoS 攻撃を軽減するのに役立つ、レイヤー7 DDoS 軽減サービスを提供しています。お客様がまだ WAF を使用していない場合は、DDoS 軽減スペシャリストが WAF へのオンボーディングを支援します。	レイヤー3 および 4 DDoS 保護は、お客様のワークロードが DDoS ボリューム攻撃を受けるリスクを軽減するのに役立ちます。このサービスは、すべての OCI アカウントに対して標準で提供されます。追加のコストはかからず、構成や監視は必要ありません。 レイヤー7 DDoS 軽減サービスには価格保険プログラムがあります。このプログラムにより、お客様は DDoS 攻撃によって過大な使用量が発生した場合、クレジットの対象となることがあります。
ガバナンス **サプライ・チェーンのセキュリティ**	オラクルには、エンタープライズクラスの安全なハードウェアを開発してきた長い歴史があります。OCI サービスの提供に使用されるハードウェアのセキュリティは、ハードウェア・セキュリティ・チームが設計し、テストしています。このチームはオラクルのサプライ・チェーンと連携し、ハードウェア・コンポーネントをオラクルの厳しいハードウェア・セキュリティ標準に照らして検証します。	オラクルのサプライ・チェーン・リスク管理プラクティスでは、オラクルのダイレクト・ハードウェア・サプライ・チェーンにおける品質、可用性、供給の継続性、回復性と、オラクルの製品およびサービス全般の信頼性とセキュリティを重視しています。

表 6 で詳しく説明したすべてのコントロールは、インフラストラクチャの設計と構築の中で提供されるセキュリティの一部です。そうした設計原則以外にも、お客様が OCI 上でソリューションを構築する際に使用できる幅広いコントロールのセットが用意されています。表 7 にその概要を示します。

表 7: OCI テナンシ内のネットワーキング・コントロール

OCI の機能	説明	適用可能なコントロール
OCI DNS	OCI は、プライマリまたはセカンダリ DNS サービスとして使用できる、フルマネージド型のグローバル・エニーキャスト DNS サービスを提供します。	OCI DNS は、パブリックとプライベート両方の DNS リゾルバを提供します。 この機能は、DDoS に対する組込みのレイヤー3 および 4 保護を提供します。

セキュリティ・リストと NSG  *CIS セキュア・ランディング・ゾーン*	セキュリティ・リストとネットワーク・セキュリティ・グループを使用すると、テナンシ内のサブネットや VCN の内部で、またサブネットや VCN をまたがって、トラフィック・フローを制御できます。	セキュリティ・リストと NSG は、構成可能なルールとポリシーにより、OCI 内の VCN におけるトラフィック・フローを制限します。
OCI Bastion  *CIS セキュア・ランディング・ゾーン*	OCI Bastion は、お客様のプライベートな Oracle Compute リソース(VM や Kubernetes クラスタ、データベースなど)に対する期限付きの安全な SSH アクセスおよびポート転送通信を提供します。	OCI Bastion を使用すると、お客様は、Oracle Compute のリソースやデータベースがパブリック・エンドポイントを使用していなくても、それらのリソースにアクセスできます。 お客様は、きめ細かな IAM ポリシーを使用してアクセスを認可し、期限付きの SSH セッションを使用してアクセスを実行し、OCI Logging を使用して一元的にアクセスを監査します。
保護インスタンス	保護インスタンスは、ベア・メタル・ホストや VM におけるファームウェアのセキュリティを強化し、悪意のあるブートレベルのソフトウェアから保護します。 保護インスタンスは、セキュア・ブート、測定ブート、トラステッド・プラットフォーム・モジュール(TPM)を組み合せて使用し、インスタンスにおけるファームウェアのセキュリティを強化します。	セキュア・ブートが不正なブート・ローダーやオペレーティング・システムのブートを防止するのに対し、測定ブートはセキュア・ブートを補完し、ブート・コンポーネントの測定結果を格納することでブート・セキュリティを強化して整合性を確保します。 TPM は、測定ブートがブート測定結果の格納に使用する、特殊なセキュリティ・チップです。
ゲートウェイ • **インターネット** • **NAT** • **動的ルーティング** • **サービス** • **ローカル・ピアリング**	ゲートウェイを使用すると、VCN 外部の宛先と通信できます。	ゲートウェイを使用すると、トラフィックがどこをどのように流れるかを管理できます。たとえば、インターネット・ゲートウェイを構成しなければ、外部のトラフィックはサブネットに到達できなくなります。
プライベート・エンドポイント	プライベート・エンドポイントは、トラフィックが VCN のサブネットから VCN 外部の宛先へどのようにルーティングされるかを制御します。	プライベート・エンドポイントを使用することで、サービス間のトラフィックをプライベート・リンク経由でルーティングするのかインターネット経由でルーティングするのかなど、トラフィックが指定したとおりに流れるように構成できます。
OCI IAM  *CIS セキュア・ランディング・ゾーン*	OCI IAM では、IAM グループによって許可された、テナンシ内のリソースに対する特定のアクセスやアクションを管理できます。	OCI IAM は、不正なユーザーがテナンシ内のネットワーキング構成を表示したり変更したりできないように制限します。
プライベート・サブネットとパブリック・サブネット  *CIS セキュア・ランディング・ゾーン*	プライベート・サブネットとパブリック・サブネットを使用すると、リソースを様々なサブネット(プライベートまたはパブリック)に分離できます。	プライベート・サブネットとパブリック・サブネットは、インターネットに直接接続できないサブネットにリソースをコンパートメント化する手段となります。

OCI Network Firewall	OCI Network Firewall は、Palo Alto Networks の次世代ファイアウォール・テクノロジ(NGFW)を利用して構築された、クラウド・ネイティブなマネージド型のファイアウォール・サービスを提供します。機械学習を利用したファイアウォール機能によって OCI のワークロードを保護するこのサービスは、OCI 上で簡単に使用できます。 OCI ネイティブの Firewall-as-a-Service サービスである OCI Network Firewall を使用すると、組織は、他のセキュリティ・インフラストラクチャを構成して管理することなく、ファイアウォールの機能を活用し始めることができます。	OCI Network Firewall を使用すると、柔軟なポリシー施行が可能になり、組織は、インバウンド(North-South)、アウトバウンド、水平方向(East-West)のトラフィックに関するきめ細かなセキュリティ・ルールをアプリケーションやネットワークのワークロードに簡単に適用できます。 VCN ルーティング・ルールを使用してトラフィック・パスに透過的に挿入し、OCI ゲートウェイや VCN サブネットなどの他のネットワーク機能と一緒に構成して、任意のネットワーク・トポロジでセキュリティを確保することができます。
仮想テスト・アクセス・ポイント(VTAP)	OCI VTAP は、トラフィック・ミラーリング・サービスです。ネットワークの特定のポイントを横断するトラフィックをコピーし、ミラーリングしたトラフィックをネットワーク・パケット・コレクタまたはネットワーク分析ツールに送信して、後で詳細な検査や追加の分析を行えるようにします。	OCI VTAP を使用すると、ネットワーク・トラフィックを包括的に可視化して、細かな異常を特定することができます。 必要なトラフィックをネットワーク・モニタリング・アプライアンスにミラーリングすることで、特定のトラフィックの監視とロギングを義務付けるコンプライアンス要件に準拠することもできます。
ネットワーク・ソース	ネットワーク・ソースとは、一連の定義済 IP アドレスです。IP アドレスは、パブリック IP アドレス、またはテナンシ内の VCN の IP アドレスです。ネットワーク・ソースを作成すると、それをポリシーまたはテナンシの認証設定で参照して、発信元の IP アドレスに基づいてアクセスを制御できるようになります。	ネットワーク・ソースにより、ネットワーク位置に基づいてリソースをさらに保護することが可能になります。

ネットワーク固有のコントロールに加えて、セキュリティ・ゾーンや Cloud Guard、Web アプリケーション・ファイアウォールなどのその他のコントロールについても、すでに本書のこれまでの項で詳しく説明しています。

原則 8: ゼロ・トラスト用に設計されたサービスを選択する

原則 7 で勧められているように、ゼロ・トラスト・アーキテクチャではネットワークが信頼されていないため、サービスがそれ自身を保護するように設計する必要があります。前の項の表 6 で、OCI のセキュリティファースト・アプローチにおけるセキュリティ設計原則の一部について詳しく説明しています。

OCI は、セキュリティ侵害を前提とし、最小信頼原則に基づいて設計されており、その結果として生まれたのがゼロ・トラスト・アーキテクチャです。分離特性には次の要素があります。

- 他のテナントからの分離
- クラウド・プロバイダのスタッフからの分離
- テナンシでの事業部門間の分離を構成できること
- 外部の脅威アクターからの分離を構成できること

OCI では、これらのセキュリティ機能をアーキテクチャに組み込み、この 4 つの脅威アクターからの分離を徹底しています(図 7 を参照)。このような分離の 1 つの例として、OCI コンパートメントを OCI 内の最高クラスのリソースとして使用することが挙げられます。表 4 で説明したように、コンパートメントは OCI リソースの論理コンテナです。コンパートメントにアクセス制御ポリシーを適用することで、テナンシ内でのポリシー主導の分離が可能になります。

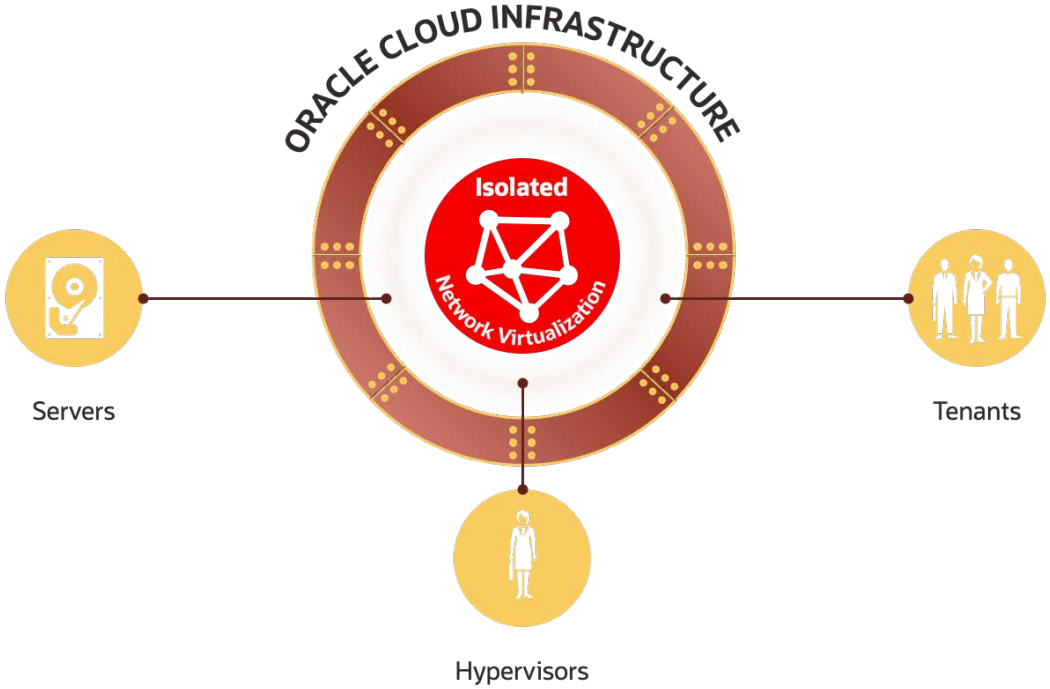


図 7: OCI のセキュリティ侵害を前提とした最小信頼設計。

原則 8 は、標準を使用することの重要性も強調しています。OCI では、お客様とパートナーがオープン・エコシステムの標準に従うことで、クラウド・ベンダー・ロックインを回避できます。これまでの原則との対応付けの中で、SAML、OAuth、OpenID Connect、SCIM といった業界のオープン標準のサポートについて、それらをユーザーとサービス両方の要求に使用する方法と併せて説明しています。

これまでの項で、アイデンティティ・サービスがこうしたオープン標準のサポートとともに提供されていることも説明しました。そのため、このアイデンティティ・サービスは、OCI で使用できるだけでなく、OCI やサードパーティ・クラウド・プロバイダ、オンプレミスでホストされている任意の Web ベース・アプリケーションで使用できます。本書で説明しているように、App Gateway を使用すると、オープン標準をサポートしていない Web アプリケーション向けに SSO を有効にできます。さらに、組織の認証の標準を Active Directory にしたい場合は、委任認証が可能です。

ORACLE

OCI CIS セキュア・ランディング・ゾーンと NCSC ゼロ・トラスト原則の対応付け

次の表の空欄は、ランディング・ゾーンを適用できないか、その領域のコントロールがまだ実装されていないことを示します。

機能	説明	8 つのゼロ・トラスト原則への適用可否							
		1	2	3	4	5	6	7	8
OCI Identity and Access Management	ランディング・ゾーンは、グループ、コンパートメント、ポリシーを作成し、最小権限とテナンシ内での職務分掌を有効にします。	✓	✓	✓	✓	✓	✓	✓	✓
ネットワーキング	ランディング・ゾーンは、複数のサブネットや VCN にわたって様々なリソースを分離し、テナンシ内のリソースを論理的に分離するために必要な構造を適用します。	✓			✓		✓	✓	✓
鍵管理(KMS)	ランディング・ゾーンは、Vault サービスと統合された OCI サービスが使用できる仮想ボールトと鍵を作成します。		✓		✓				✓
Cloud Guard	ランディング・ゾーンは、ルート・コンパートメントですべてのディテクタとレスポンダを使用して、OCI Cloud Guard を有効にします。						✓	✓	✓
脆弱性スキャン	ランディング・ゾーンは、脆弱性スキャン・ターゲットを 1 つ作成します。レシピは、提供されているすべてのターゲットに割り当てられます。								✓
踏み台	ランディング・ゾーンは、Terraform 構成での定義に従い、ターゲット・サブネットに接続するための踏み台のインスタンスを 1 つ作成します。							✓	✓
イベント(監査)	ランディング・ゾーンは、IAM ポリシーの変更、VCN の変更、IAM グループの変更、IAM ユーザーの変更など、複数の OCI イベント・ルールを作成します。	✓	✓				✓		✓
通知	ランディング・ゾーンは、それぞれがサブスクリプションを持つトピックを少なくとも 2 つ作成します。すべての IAM 関連イベントが送信されるセキュリティ・トピックおよびサブスクリプションと、すべてのネットワーク関連イベントが送信されるネットワーク・トピックおよびサブスクリプションです。	✓							
セキュリティ・ゾーン	ランディング・ゾーンは、定義済のコンパートメントごとにレシピを 1 つ作成し、関連するレシピを持つ定義済のコンパートメントごとにセキュリティ・ゾーンを作成します。				✓			✓	✓

ORACLE

結論

ゼロ・トラスト・セキュリティは、製品でもなければ、アプリケーションにおいて特定の時点で何かを有効にするためのチェックボックスでもありません。ゼロ・トラストは単独の行動ではなく、アプローチであり、採用するには時間と労力と投資が必要になります。

ゼロ・トラスト・セキュリティは、セキュリティ侵害を受けてデバイスやユーザーを信頼できないネットワークの原則に基づき、組織のユーザー、サービス、デバイス、データを理解した上で、適切なコントロールを実装することに重点を置いています。これにより、要求を適切に認証し、複数のシグナルに基づいて要求を認可すると同時に、すべてのアクセスを監視します。ワークロードを配置する場所を決める際には、ゼロ・トラスト・セキュリティ戦略に従い、ゼロ・トラスト・プログラムを加速するのに必要なコントロールを提供できるクラウド・プロバイダを選択することが重要です。

オラクルは、セキュリティファーストの設計原則に基づいて OCI を構築し、ハードウェアベースの信頼の基点、分離されたネットワーク仮想化、ハイパーセグメンテーションなどのコントロールを通じて、核となるゼロ・トラスト・セキュリティを一から実装しています。すべての原則は、クラウド・インフラストラクチャの重要なコンポーネント(サーバー、ハイパーバイザ、ネットワークなど)に対する最小信頼アプローチを使用して設計されています。OCI のセキュリティファースト・アプローチの詳細は、OCI セキュリティ・アーキテクチャの技術概要を参照してください。

オラクルは、セキュリティの自動化と強化に役立つセキュリティ・コントロールを OCI 内で提供することに力を注いできました。オラクルは、デフォルトでの暗号化を可能にし、問題を自動的に修正する機能を備えたクラウド・セキュリティ・ポスチャ管理を提供しています。オラクルの戦略は、簡単に実装できるコスト効果の高いソリューションを提供し、組織がクラウド・セキュリティの責任を効果的に果たせるよう支援することです。

ゼロ・トラスト・セキュリティは、購入する製品でもなければ、アプリケーション内で有効にするチェックボックスでもありません。ゼロ・トラストは、採用するには時間と労力と投資が必要になるアプローチです。

ゼロ・トラスト・セキュリティ戦略に従い、ゼロ・トラストに基づいたプログラムを加速するのに必要なコントロールを提供できるクラウド・プロバイダを選択してください。

ORACLE

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