ORACLE HCM CLOUDのORACLE CASB

背景:

多くの企業は、Oracle HCM Cloudなどのビジネスクリティカルなアプリケーションを利用して、ビジネス・プロセスを向上させ、従業員や契約社員とのエンゲージメントを高めています。これらのアプリケーションは、ビジネスクリティカルで機微な機密情報を含み、セキュリティは最重要課題です。

ビジネス上の観点から、HCM Cloudへの移行が進むと、すべてのサービスのすべてのアクティビティを積極的に監視し、ロール、構成およびビジネス・オブジェクトなど全体の変更を追跡できるようにすることが重要です。これにより、組織は、ビジネス・プロセスのベースラインやユーザー権限をより速く構築し、異常を早期に修正できます。コンプライアンスの実現は予測可能なものとなり、費用も抑えられます。

セキュリティ上の観点から、Oracle HCM Cloudはそれ自体本質的に安全ですが、ユーザーの行動を組織のクラウド領域全体で追跡することは重要です。セキュリティ・チームが関心を持つ側面の一部を次に示します。

- クラウド・アプリケーションのセキュリティ構成に行われる変更
- ユーザー権限の変更
- データ抽出の試行
- 悪意のあるアクセス
- 資格情報の漏洩

他のクラウド・サービスと同様に、セキュリティは、クラウド・サービス・プロバイダと顧客組織の共同責任です。オラクルは、その共同責任を遂行することで、安全で安定したHCM Cloudソリューションを確実なものとしています。HCM Cloudによって提供される基礎となるセキュリティの一部を次に示します。

- クラウド・インフラストラクチャ(ネットワーク、コンピュート、ストレージなど)の保護
- 保存中または移動中の暗号化を提供することによる機微データの保護
- モジュール全体のHCM Cloud機能へのきめ細かなアクセス

ただし、ビジネス・オブジェクトまたはユーザー、ならびにユーザーのセキュリティの構成、カスタマイズおよび変更は組織の責任です。

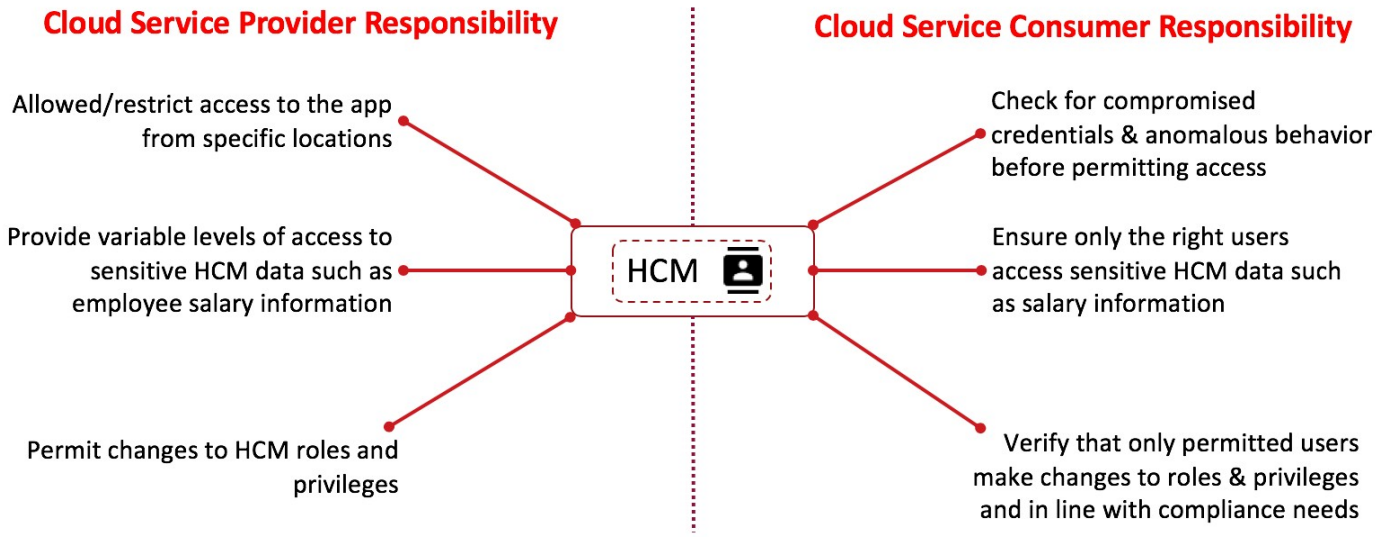

図1: HCM Cloudの共同責任モデル

Oracle CASBは、組織が共同のセキュリティ責任を遂行できるよう支援します。この資料では、Oracle HCM Cloudが本来備えているセキュリティ・ポスチャの強化という点におけるOracle CASBのビジネス価値を紹介します。

ビジネス価値:

- **Oracle HCM Cloudの使用状況の可視化:** ユーザーおよび使用目的を詳細に把握します。これにより、必要十分なサービスの使用が促進されます。
- **継続的なコンプライアンスの実現:** 構成、ロールおよび権限の変更によって、監査の失敗や法の不履行が発生しないようにします。
- **不正の早期検知:** 不正の可能性を示すビジネス・オブジェクトへの変更について通知が送信されます。
- **危険性のあるユーザーの識別:** ユーザー行動分析により、クラウド資産全体のリスクにネットワーク効果を活用します。

ORACLE HCM CLOUDのセキュリティの強化にORACLE CASBが適している理由

- **Oracle HCM Cloud**にアクセスしているユーザーを可視化: Oracle CASBは、緊密な統合により、アプリケーションを誰が使用しているか、また時間や場所などのアクセス属性に関する詳細な情報を提供します。
- **積極的な監視:** Oracle CASBは、管理ユーザーのアクティビティ、および個人、給与、その他の関連する個人識別可能情報(PII)の変更などの機微データの変更の積極的な監視を提供します。
- **高リスク・ユーザーの識別:** Oracle CASB Cloudは、機械学習とユーザー行動分析を活用して、特定のユーザーのリスク・スコアを計算し、そのユーザーのアクティビティやジオロケーションなどのコンテキスト・データに基づいて高リスク・ユーザーを識別します。
- **ビジネス・オブジェクトの変更に対する詳細かつ積極的なインサイトの獲得:** Oracle CASBは、ビジネス・オブジェクト・レベルの属性を調査し、そのビジネス・オブジェクトへの変更に対する単一のインサイト・ポイントを提供します。
- **ロールおよび権限への変更の追跡:** Oracle CASBは、主要ロールの変更をすべて監視します。これには、あらゆるロール変更についての特権およびメンバーシップの変更が含まれます。
- **すべてのクラウド・ソリューションに対する単一の可視化ポイント:** 組織が複数のクラウド・アプリケーションを使用している場合、Oracle CASBでは、Oracle HCM Cloud、ERP Cloud、およびOracle以外のアプリケーション(Office 365やSalesforceなど)を含むすべてのアプリケーションを監視する一括管理機能(single pane of glass)を提供します。

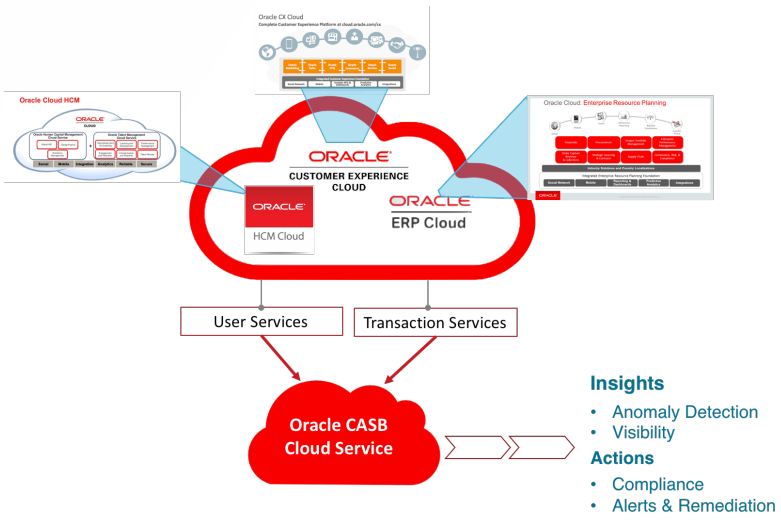

図2: Oracle CASBによるOracle Cloud Applicationsの補完

使用事例

使用事例1 - ユーザーアクセス監視(可視性とセキュリティ):

CASBは、どの時点においても誰がOracle HCM Cloud にアクセスしているかを識別します。個別の組織のすべてのOracle HCM Cloudユーザーの情報をOracle CASBで追跡できます。IPアドレス、ログイン日時、デバイス・タイプ(モバイル、デスクトップなど)、OS、ブラウザ種別、成功/失敗ログイン/ログアウトなどの情報をOracle CASBから取得できます。さらに、総当たり攻撃などのパスワードベースの攻撃、Torなどの匿名プロキシからのログイン攻撃も監視できます。詳細なログイン成功/失敗レポート、およびログイン回数が最も多いユーザー、ログイン失敗回数が最も多いユーザーについての主要セキュリティ・インジケータも提供されます。

使用事例2 - ロール変更の識別(セキュリティとコンプライアンス):

CASBは、Oracle HCM Cloudで行われたロール、権限およびメンバーシップの変更を積極的に監視します。Oracle CASBは、Oracle HCM Cloud内のロール作成、メンバーの追加/削除などのすべてのロール変更を、発生元が管理者かユーザーかに関係なく監視し、インシデントおよびアラートを通じて通知を送信します。特にOracle HCM Cloudの場合、お客様は事前にシード済のロールをコピーしてロールを作成できます。このコピーしたロールへの変更により、ダウンストリームに重大な影響が出る可能性があります。監視を行っている場合、この変更は、迅速な影響分析の実行に役立ちます。ロール変更、および最もロール変更が多いユーザーなど主要セキュリティ・インジケータの包括的なレポートも提供されます。

使用事例3 - 機微なビジネス・オブジェクトへの変更の識別(不正の検出):

CASBは、Oracle HCM Cloud内の個人および給与情報などの機微なビジネス・オブジェクトへの変更を監視します。Oracle CASBは、個人、給与など、Oracle HCM Cloud内の重要なビジネス・オブジェクトを監視し、変更が発生するとアラートを発します。このオブジェクト属性の変更に対する詳細レポートおよび主要セキュリティ・インジケータが提供されます。

使用事例4 - 異常なユーザー行動の識別(セキュリティ):

CASBは、ユーザーとエンティティの行動分析(UEBA)を使用して異常なアクティビティを識別します。Oracle CASBは、機械学習に基づいて、ユーザーの一般的な行動のプロファイルを構築します。たとえば、あるユーザーは通常サンフランシスコからログインしているとします。この場合、ニューヨークから行われるログイン試行は、ユーザーの通常の行動からの逸脱を意味し、潜在的なリスクとなり、セキュリティ・チームにアラートが通知されます。同様に、Oracle CASBは、通常のトランザクション量からの逸脱を識別し、セキュリティ・チームにアラートを通知します。

結論

Oracle HCM Cloud固有のセキュリティは、組織に快適さの層を提供します。しかし、ほとんどの組織の運用形態であるマルチクラウド環境の場合、情報セキュリティ・チームがOracle HCM Cloudの複数の側面を他のクラウド・アセットとともに監視することが必要不可欠です。Oracle CASBは、Oracle HCM Cloudなどの重要なビジネス・アプリケーションで求められる必須の可視性と追加セキュリティの層を提供します。