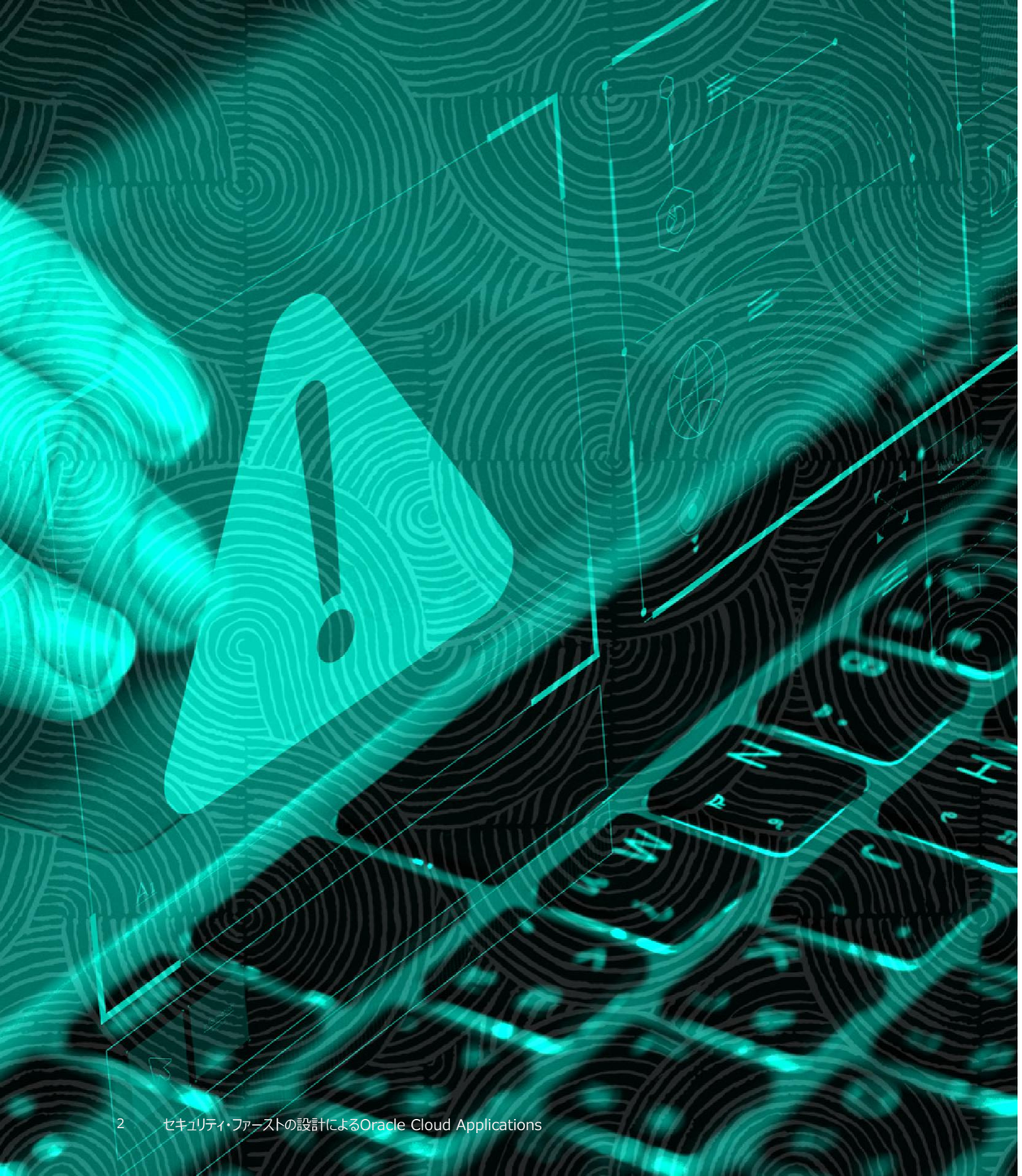
セキュリティ・ファーストの設計による Oracle Cloud Applications



セキュリティ侵害が発生していますが、その影響に気付いていますか?

これはすべての会社が直面する問題ですので、もし考えていなければ、考えるべきです。データ漏洩は、思っている以上に多く起こっています。Gartnerによると、全世界の企業がサイバーセキュリティ対策に投じた費用は、2022年に1704億ドルに達する見込みです。(Gartner)。[1]

健康記録から消費者の支出習慣に至るまで、オンラインでの取り組みが進むにつれ、企業が管理し維持しなければならないデータの量は天文学的に増加しています – IDCは、現在、50億人以上の消費者が毎日データとやり取りしているが、その数は2025年までに、60億人、つまり世界の人口の75%に増えるとの調査報告を発表しています。[2]このすべてのデータを保護し、ビジネスのあらゆるレベルでデータを保護することは、もはやITの責任ではありません。Identity Theft Resource Centerによると、2020年初頭だけで、80件のデータ侵害があり、約100万件の記録が漏洩しましたが、これら以外にも検知されていないケースが多数あると考えられます。[3]

ビジネス・データを安全に保つという仕事は、組織全体に広がり、企業全体の関心事になっています。今、重要な質問は、ITだけでなく、事業部門(LOB)マネージャからも尋ねられている質問です。「オンプレミスでもクラウドでも、機密データを安全に保つにはどうすればよいか?」クラウド・プロバイダーは、この質問に回答できる必要があります。

セキュリティに関しては、すべてのクラウド・プロバイダが皆同じというわけではありません。データ・セキュリティに熱心に取り組むクラウド・プロバイダー(セキュリティ・ファーストの設計のプロバイダー)が見つかった場合、セキュリティの改善がクラウドに移行する理由につながります。

「オラクルのセキュリティ・クラウド・サービスに投資して、潜在的な脅威だけでなくデータ漏洩を検出して対応し、規制要件をより適切に満たす能力を強化しました。」

大手グローバル銀行最高セキュリティ責任者（SCO）

1 https://cybersecurityventures.com/cybersecurity-market-report/

2 https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html

3 https://www.idtheftcenter.org/wp-content/uploads/2020/05/April-2020-Category-Summary.pdf

世界クラスのセキュリティ制御

オラクルにとって、お客様が規制コンプライアンスのニーズに対応できるよう支援することが重要です。オラクルのクラウド・ソリューションの多くには、次のような形式で利用できる業界標準のサード・パーティ監査レポートがあります。

- Statement on Standards for Attestation Engagements (SSAE) No. 18: SOC 1およびSOC 2

また、オラクルのクラウド・ソリューションの多くは、十分に認識されている業界標準の要件またはガイダンスに準拠しています。これらの標準の例を次に示します。

- 国際標準化機構(ISO) 27001、27002、27017、27018
- Payment Card Industry Data Security Standard(PCI DSS)
- Federal Risk and Authorization Management Program(FedRAMP)
- UK GOV Cloud - HMG Cloud Security Principles, Cyber Essentials Plus

オラクルは、業界で認められたフレームワークにおいて、クラウド・サービスに関する保証を提供することに全力を尽くしています。[4]

4 規格やレポート形式の可用性は、サービスによって異なります。お客様とオラクルの間の契約内容により、提供されるサービスの範囲および関連するセキュリティ条件が決まります。

クラウド・セキュリティを重視する理由

SaaSクラウド・アプリケーションがITから分散化されると、データの保護の責任は見過ごされがちです。

リスクにさらされているのは、機密情報や企業の秘密だけではなく、日ごろビジネスの取引で使用されるデータも同様にリスクにさらされています。

従業員/消費者データ

社会保障番号、住所、電話番号、その他の個人情報(PI)は、常に機密保持する必要があります。

多くの国では、データのプライバシーに関する規制要件があります。データを保護することは、最も価値のある資産の1つを保護するだけでなく、データが悪用される可能性のある個人情報の窃盗(およびその他の潜在的に望ましくない出来事)のリスクを軽減するのに役立ちます。

人事管理プロセス

従業員のオンボーディングとオフボーディング、および福利厚生の管理は、人事が従業員に関する多くのデータを収集することを意味します。たとえば、従業員のオンボーディングの際に、面接のメモや紹介状などの機密情報がある場合があります。同様に、従業員のヘルスケアの選択や福利厚生は、特定の診断や治療を明らかにするデータに加えて、絶対的な機密保持の必要があります。

財務レポートのシステム

機密性の高い従業員や顧客データなどの財務情報を機密保持することは、CFOだけでなく、すべてのビジネス・リーダーにとって最優先事項です。範囲の制御、高度なロール分析、職務分掌、ビジネス・ユニット全体の監査と評価のためのデータ・プライバシ・ツールを使用して、財務システム内でデータ・セキュリティ・リスクを低減できます。

報酬および給与

報酬および給与計算データは、きわめて機密性の高い情報です。データ漏洩によって、従業員の士気が下がったり人事の問題が発生する可能性があります。また、給与が自動振込の従業員も多いため、個人の銀行口座情報も格納されることがよくあります。

顧客オーダーおよび契約情報

顧客データの整合性を維持するだけでなく、顧客アカウントに関する情報を機密に保持することもできます。

アカウントのプランや戦略に関する情報(特にモバイル・デバイスの情報)は、セキュリティが不十分な場合に、簡単に悪用される可能性があります。

業界固有の要件

企業によっては、HIPAAとFISMAなどの業界の特定の規制や制限を遵守する必要があります。クラウド・プロバイダを選択する際には、対応が必要な規制を考慮することが重要です。[4]

リージョン別データのホスティング

クラウド・サービス契約の一環として、クラウド・プロバイダーは、データ・センター・リージョン内のデータの場所を指定する必要があります。特定のデータ・ロケーション要件がある場合、クラウド・プロバイダがサポートする場合があります。

また、ビジネスで必要な場合は、クラウド・プロバイダーがバックアップおよびリカバリ・データ用のリージョン・ストレージを提供できる必要があります。クラウド・プロバイダは、お客様の指定したリージョン以外でデータのホスティングを移行しません。

グローバル・アクセス制御

従業員が他の従業員の機密情報にアクセスできないようにする必要があります。そのため、クラウド・プロバイダがビジネス全体で統一されたグローバル・アクセス制御を提供することが重要です。

最小権限の原則に従い、アクセス拒否のデフォルト設定を行い、適切なユーザーが適切なシステムおよびデータに適切なレベルのアクセス権を持ちます。

ロールおよびテリトリの表示

営業担当は、データ(顧客、リードおよび商談を含む)と自分のジョブを実行できる機能にアクセスする必要がありますが、テリトリ定義へのアクセス権を付与する理由はありません。営業マネージャは、チーム全体の活動を測定するために各担当者のアカウントを表示する必要があり、セールスオペレーションには独自のアクセス権があります。

統合されたセキュリティ制御により、役割ベースのアクセスが可能になり、チームは機密データへのアクセスを制限しながら作業を行うことができます。

4 規格やレポート形式の適用性は、サービスによって異なります。お客様とオラクルの間の契約内容により、提供されるサービスの範囲および関連するセキュリティ条件が決まります。

クラウド・プロバイダに必要なもの

貴重なデータを保護し、データ侵害のリスクを軽減しましょう。セキュリティに関しては、次を提供するプロバイダを探しましょう。

- クラウド・プロバイダの継続性
- セキュアなデータ分離アーキテクチャ
- グローバルな統合アクセス制御
- コンプライアンスとGDPR管理
- グローバルなクラウド運用
- 高度なデータ・セキュリティ

これらの重要な考慮事項は、セキュアなクラウド・プロバイダの選択に役立ちます。次のページでは、各考慮事項が企業にどのように役立つかについて説明します。

セキュリティ・ファーストの設計

Oracle Cloud Applicationsスイートは、セキュリティ・ファーストに重点を置いて開発され、安全な分離アーキテクチャで設計されています。不要なアクセスからデータを保護し、スタックの複数のレイヤーに組み込まれます。

セキュリティ・ファーストの設計により、データ保護、スケーラビリティおよびパフォーマンスが向上します。

クラウド・プロバイダの継続性

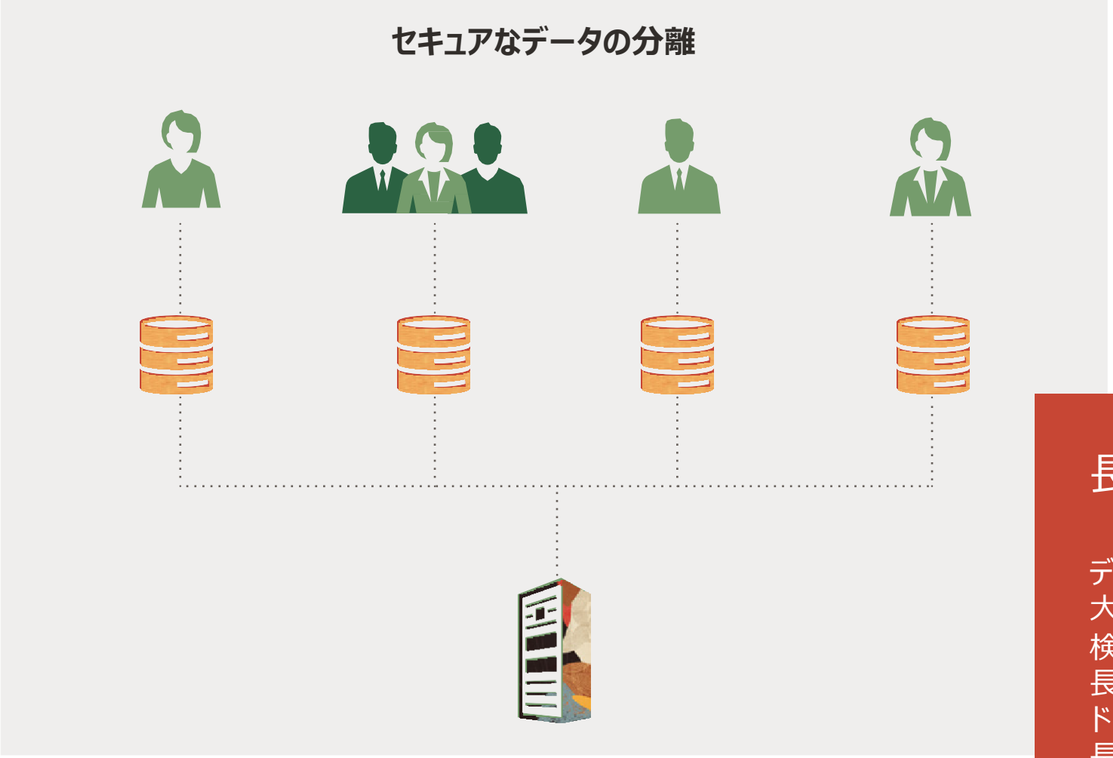
そのクラウド・プロバイダは安定したサービス提供を継続することが可能ですか。明日なくなるようなものではないですか。クラウド・アプリケーションに関する意思決定はビジネスにとって非常に重要であるため、プロバイダがクラウドを保護する長きにわたる実績があるかどうかを調査します。プロバイダの財務状況と、安全性と、イノベーションに投資する能力を調べます。クラウド・プロバイダは、長期的に優れたサービスを提供できるプロバイダーがいいでしょう。

セキュアなデータ分離アーキテクチャ

Oracle Cloudを使用すると、クラウド全体で共有リソース(ハードウェアなど)を利用して、コストを低く抑えることができます。一方で、オラクルのセキュリティ・ファーストの設計とセキュアなデータ分離アーキテクチャにより、オラクルはデータを分離してリスクを軽減し、高パフォーマンスのスケーラビリティを実現します。

お客様のデータを他のお客様から分離する、セキュアなデータ分離を使用するプロバイダを選びます。

理にかなった場所ではリソースを共有、そうでない場所では分離



Oracle Cloudを使用すると、お客様は独自の仮想ネットワークや分離されたストレージなど、独自のデータベース・インスタンスをクラウド内に保有できます。このアーキテクチャにより、ノイジー・ネイバー（noisy neighbors）に関する懸念はありません。

長期的な視点を持つ

データ・セキュリティに関しては、長期的な視点を持つことが大切です。5年後のセキュリティのニーズは?
検討しているセキュリティ・ソリューションは、お客様とともに成長し、新しい要件や変化する要件に適応できますか?クラウド・プロバイダの選び直しはしたくありません。データを保護し、長期的にイノベーションを実現できるクラウド・プロバイダーを選びましょう。

グローバルな統合アクセス制御

権限のないユーザーがビジネス・クリティカルなデータにアクセスできると、問題が発生する可能性があります。理想的なクラウド・プロバイダにより、アクセス制御をグローバルに管理できます。

たとえば:

- ユーザーが企業に入社した際は正しいアクセスレベルを判断して付与し、適切でなくなった場合はそのアクセスを取り消すことができます。
- 承認したユーザーのみが、エンタープライズ全体の一元化されたアイデンティティ管理とフェデレーテッド・シングル・サインオン(SSO)により、クラウドとオンプレミスの両方で関連データにアクセスできます。
- ロールベースのアクセス制御(RBAC)が導入され、職務分掌(SOD)が可能になり、機密情報への不正アクセスを防ぎます。
- ユーザーには、ジョブ固有の職務に関連するデータのみが表示されます。管理者は、ジョブ機能およびデータ権限にマップするジョブ・ロールを構成します。

コンプライアンスとGDPR管理

最新のクラウド・プロバイダーは、GDPRやその他のプライバシー法によるコンプライアンスのニーズに対応するために、リスク管理ソフトウェアなどのコンプライアンスの管理に役立つ多くのグローバル・データセンター・リージョンとソフトウェア・ソリューションを備えている必要があります。

グローバルなクラウド運用

オラクルのグローバル・ネットワーク・オペレーション・センターには、クラウド・セキュリティをプロアクティブに監視するエキスパートが配置されています。Oracle Fusion Cloud Applicationsの運用は、24時間365日の「follow the sun」体制でお客様をサポートします。

クラウド・プロバイダには、最先端の物理的なデータ・センターの保護、論理的なデータ・セキュリティ、およびデータのプライバシー保護ポリシーがすでに適用されている必要があります。さらに、適切なクラウド・プロバイダは、先行的なセキュリティ・エンゲージメントと監視、および最先端のディザスタ・リカバリを実現します。

高度なセキュリティ・オプション

世界クラスのクラウド・プロバイダは、ビジネスに追加のセキュリティ対策が必要な場合に、高度なセキュリティ・オプションをクラウドで提供します。高度なデータ・セキュリティ・サービスの一部:

- Oracle Transparent Data Encryptionにより、機密データの不正使用を防止します。[6]
- Oracle BreakglassとDatabase Vaultは、データおよび管理者アクセスに対する追加の制御を提供し、従業員情報の不正使用、表示または共有を防止します。オラクルのお客様が「鍵」を握っていて、クラウド環境にアクセスする必要がある場合、クラウド・プロバイダへのアクセス権を付与する必要があります。[6]
- Oracle Cloud Access Security Broker (CASB) Cloud Serviceを使用すると、SaaSのセキュリティ監視を自動化することで、さらなる保護を実現できます。クラウド・アプリケーションとクラウド・プロバイダの脅威検出を組み合わせたものです。
- Oracle Identity Cloud Service (IDCS)は、セキュアで適応性の高い認証およびアクセス制御(SSO、オンプレミスおよびSaaSアプリケーションのユーザー・プロビジョニング、およびハイブリッド・アイデンティティ管理機能を含む)を提供します。
- アイデンティティ管理ソリューションをハイブリッド・クラウド・モデルのクラウド・アプリケーションに拡張する機能。[6]

6 選択したクラウド製品で利用可能

セキュリティ・ファーストの設計による Oracle Cloud Applications

オラクルは、グローバル・データ・センター・リージョンの全体的な設計の一環として、クラウド・セキュリティ・ファーストをすべてのレイヤーに継続的に投資しています。現在は、リスクを軽減し、エラーを削減し、コンプライアンスと監査を改善し、生産性を向上させる自律型機能を構築しています。

Oracle Cloudでは、次のようなメリットがあります。

- **クラウド・プロバイダの継続性。**オラクルの経験がすべてを物語っています。40年以上にわたる安全なデータ管理、エンタープライズレベルのクラウド運用において長年の経験があり、何百万人ものユーザーを日々サポートしています。
- **セキュアなデータ分離アーキテクチャ。**理にかなった場所ではリソースを共有し、そうでない場所では分離します。安全で信頼性の高いパフォーマンスを実現するために、お客様ごとに分離したデータベースが用意されています。
- **グローバルな統合アクセス制御。**企業全体では、承認されたユーザーのみがクラウドおよびオンプレミス・システムのデータにアクセスできます。フェデレーテッドSSOおよびRBACによる一元的なアイデンティティ管理により、不正アクセスを防止します。
- **グローバルなクラウド運用。**オラクルは、冗長性の高いインフラストラクチャと高可用性を備えたエンタープライズ・グレードのクラウド・データ・センターを運営しています。
- **コンプライアンス、GDPRおよびRisk Management。**最新のクラウド・プロバイダーは、現在のコンプライアンス、GDPR、データレジデンシー要件に対応できる多くのグローバル・データセンター・リージョンとソフトウェア・ソリューションを備えている必要があります。
- **高度なセキュリティ・オプション。**オラクルは、ビジネスに追加のセキュリティ・ニーズがある場合に、高度なセキュリティ・オプションを提供します：Oracle Transparent Data Encryption[6]、Oracle Break Glass、Oracle CASBおよびOracle Identity Cloud Service[6](ハイブリッド・モデルのアイデンティティ管理ソリューションを含む)。

信頼できるクラウドパートナー

オラクルは、エンタープライズレベルのクラウド運用において長年の経験を持ち、完全なクラウド戦略を有しており、何百万人ものユーザーを日々サポートしています。

40年以上のセキュアなデータ管理経験を持つオラクルのみが、スタックのすべてのレイヤーでセキュリティを設計しています。そして、最近のこの取り組みを証明するものとして、オラクルは世界初の自己稼働、自己保護、自己修復ができる自律型データベースを開発しました。

6選択したクラウド製品で利用可能

オラクル：信頼できるクラウドパートナー

オラクルは、信頼できる戦略的なビジネス・イノベーションおよび変革のパートナであり、安全なクラウド・イノベーションを継続的に投資および開発するための取組みを担っています。Oracle Cloud Applicationsスイートは、セキュリティ・ファーストに重点を置いて、開発されました。設計が分離されているため、データ保護、スケーラビリティ、およびパフォーマンスが向上します。このスイートは、グローバル・エコシステムの一部として、マルチクラウド環境などのシステムにセキュアに接続できます。

オラクルによる投資とイノベーション

オラクルは、すべてのお客様のニーズが同じではないことを認識しています。グローバル要件への対応や、別の国のローカル・データ・セキュリティ要件への対応が必要なお客様もいれば、業界固有の規制コンプライアンス要件があるお客様もいます。

お客様のニーズが高まる中、オラクルは引き続き投資とイノベーションを行い、ビジネスに必要なレベルで安全なデータ管理サービスを提供します。

仕組み

Oracle Cloudサービスのユーザーになると、サービス・レベルとセキュリティ標準がクラウド・サービス契約で提示されます。

何百万人ものオラクルのユーザーが、日々Oracle Cloudを使用しています。オラクルは、ユーザーのインプットに基づいて、自己修復が可能な自立型機能を開発し続け、リスクの低減、手作業によるエラーの削減、コンプライアンスと監査の向上、生産性の向上を実現する最先端のセキュアなイノベーションを提供します。

ビジネスに追加のセキュリティ・ニーズがある場合、オラクルは高度なデータ・セキュリティ・オプションを備えており、将来のニーズに合わせてイノベーションを継続します。

お問い合わせ先

詳しい情報については、+1.800.ORACLE1でオラクルの担当者にお問い合わせください。または、oracle.com/applicationsにアクセスしてください。

北米以外では、oracle.com/corporate/contact/global.htmlにアクセスしてお近くのOracleオフィスの電話番号を検索してください。

Connect with Us