ORACLE

2021年以降のクラウド・セキュリティのトレンドトップ5

自信を持って変化を導こう

妥協のない変化への適応

テクノロジーが変化し、ビジネスが優先順位を変更するなかで、変わらないのは重要な情報を保護する必要性です。パンデミックにより、業界では業務の再編成が促進されました。組織のほぼ3分の1が、クラウド・サービスの導入について、パンデミック前と比較して「重要性が大幅に増した」と述べています[1]。組織の55 %は、パンデミック後も大半の従業員が少なくとも週に1日、リモート・ワークを継続すると話しています。競争力を維持するには、企業はこういったことを考慮してセキュアなクラウドに投資する必要があります。

2020年にITリーダーは、コストを増加させず、セキュリティを犠牲にせずに、重要なインフラストラクチャをどのようにモダナイズするかという前例のない課題に直面しました。リーダーたちは、新たなレベルの責任を引き受け、システムのセキュリティを維持し、戦略的価値の向上に貢献しました。

ワークロードをパブリック・クラウドに移行する場合も、新たなレベルの自動化を実現する場合も、あるいは複雑性を低減する場合も、堅牢なサイバーセキュリティ体制は重要です。オラクルには、数十年に及びデータとアプリケーションを保護してきた経験があります。当社は、信頼性を構築し、価値あるデータを保護するOracle Cloud Infrastructure（OCI）を使用して、よりセキュアなクラウドを提供することに尽力しています。

競合他社の先を行くことは重要です。今後、極めて大きな影響を及ぼすと思われるセキュリティの傾向を共有し、オラクルが組織のセキュリティ・ニーズに対する取組みをいかに支援できるかを強調しているのはそのためです。

[1] OmdiaのICT Enterprise Insights調査（2020～2021年）

1

傾向1

リモート・ワークにより、セキュリティに対するゼロトラスト・アプローチの必要性が増加

2

傾向2

インテリジェントなセキュリティへの投資が増加

3

傾向3

DevOpsのセキュアな自動化

4

傾向4

CISOはかつてないほど多くの役割を任されている

5

傾向5

セキュリティ管理の向上には高度な可視性が必要

傾向1

リモート・ワークにより、セキュリティに対するゼロトラスト・アプローチの必要性が増加

リモート・ワークも一因となり、サイバーセキュリティ攻撃は47 %増加しました[3]。

新型コロナウイルスのパンデミックにより、すでに活発だったクラウド採用が加速しましたが、一方で、脅威アクターに新たな機会ももたらされました。在宅勤務する従業員の急増に加えて、オンラインでの会議、E-Commerceへの依存の高まりがあいまって、多くの組織は、拡大したクラウドサービスの使用を悪用するサイバーセキュリティ攻撃にさらされるようになりました。

企業の70 %は、**エンドポイント・サイバー衛生の課題を抱えており、フィッシング攻撃の試みを含むサイバーセキュリティ攻撃が**47 %増加したと報告しています。クラウド・サービスの採用が急速に広がり、環境が分散化されることで、より厳格な予防策が必要となります。しかしながら、**企業は平均で**573のシャドウITアプリケーション**を使用**しており、その多くは厳しく検証されていないため、不適切な構成や使用が監視されない状態を引き起こしている場合が多くあります。

多くの従業員が組織の物理的な壁の外で働くようになった今、悪意のある内部関係者が残す危険な兆候は容易に見逃されます。一方で、**過剰な権限が付与されたアカウントが過去24か月の**最大の脅威（44 %）であり、クラウドの誤った構成が不正行為を引き起こすおもな要因になりつつあります。

一般的なネットワーク境界線の外部にある組織のデータ・フローが増加しているため、クラウド・セキュリティに対するゼロトラスト・アプローチは、脅威を管理する上で重要な役割を果たすでしょう。
実際、組織の87 %**は、新型コロナウイルス後にゼロトラスト・アーキテクチャを実装したい**と考えています。

ゼロトラスト・アプローチでは、ユーザーや、ワークロード、デバイス、ネットワークに属する信頼レベルは事前に定義されません。このアプローチをアーキテクチャからアプリケーションに至るまでに組み込み、ユーザーID、デバイス、ロケーションといった使用可能なあらゆるデータ・ポイントに基づき、すべてのアクセス・リクエストを検証する必要があります。この追加のコンテキストは、複数の要素を使用して、2つの要素による認証をトリガーするポリシーベースのアプローチを促進します。これは、各自の具体的な職務に必要な権限とアクセス・レベルのみをユーザーに付与するという最小権限の原則に基づきます。

[3] State of Cybersecurity Report 2020（Wipro）

サイバーセキュリティ攻撃の増加率

47 %

87 %

新型コロナウイルス後にゼロトラスト・アーキテクチャを求めている割合

70 %

エンドポイントのサイバー衛生に関する課題を抱えている割合

OCIを使用したゼロトラスト・モデル（英語）

オラクルと他社との違い

Oracle Cloud Infrastructureのセキュリティ

絶えず続く脅威のリスクを軽減：

クラウド・セキュリティ・アーキテクチャに組み込まれたテナント分離と最小権限のアクセスを活用することで実現します

分離されたネットワーク仮想化によるセキュリティ：

脅威と悪意のあるアクターのラテラル・ムーブメントを防止するように設計されています

組込みのIDおよびアクセス管理：

クラウド・リソースにアクセスするユーザーを容易に制御します

セキュアなアクセス：

さまざまなデバイスやロケーションからアクセスするユーザーの認証とシングル・サインオン（SSO）、リスクベースの認証とプロアクティブなリアルタイムの不正防止によって実現します

コンテキストを認識したコンピューティング：

ID、デバイス、ロケーションを収集して活用します

傾向2

インテリジェントなセキュリティへの投資が増加

AIとMLは、マルウェアだけでなく、サイバーセキュリティ・テクノロジーの基本要件になりました。

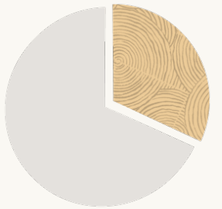
パンデミックが原因で組織は予算を引き締めていますが、セキュリティ体制の中心的な要素として人工知能（AI）と機械学習（ML）に投資することには依然として前向きです。実際、回答者の10人に9人が、クラウド・セキュリティ戦略の基盤としてこれらのテクノロジーを挙げており、組織の32％が、向こう12～18か月間の最大の投資として、AIを使用したサイバーセキュリティを優先させています。

AIとMLは、脅威（マルウェアの新規亜種、エクスプロイト、フィッシング攻撃など）を検出および防止するために幅広く使用されてきました。しかしながら、クラウド・サービスの拡大により、AIとMLの使用はマルウェアの検出にとどまらずにさらに広がっています。次世代クラウドの自動化されたセキュリティ機能は、ユーザー・アクセスを手動で管理するために必要な時間とリソースを低減できる一方で、人的エラーも削減できます。

そのような理由から、40～45％の回答者が、不正行為の特定、構成管理の保守、通常とは異なるユーザー・アクティビティの特定、セキュリティ・イベントの選別と優先順位付けにおいて、AIはセキュリティ・アナリストよりも優れている可能性があると信じています。

サイバーセキュリティの労働力不足は、2022年までに全世界で180万人という驚異的な人数に達することが予想されています。これは、今後3年以内に、高度な自動化とインテリジェント機能を活用してワークロードの88％が恐らく自律的に更新されることになるおもな理由です。

AIとMLにますます大きく依存する組織では、サイバーセキュリティ・チームは侵害を防止する重要なツールを獲得すると同時に、事業を推進させるイノベーションに集中できる時間を増加させることができます。



32％
AIを使用したサイバーセキュリティを優先する割合

40～45％
AIはセキュリティ・アナリストよりも優れている可能性があると信じている割合

88％
自律的に更新されるワークロードの割合

IDCのレポートを読む(英語)

2

オラクルと他社との違い

Oracle Autonomous DatabaseとOracle Autonomous Linux

Autonomous Database

自己保護：

データ保護とセキュリティを自動化し、データベースにパッチを自動適用するほか、“常時オン”のエンド・ツー・エンドの暗号化によって不正アクセス/攻撃の防止を支援します

自動修復：

停止時間なしでサービス停止から迅速に自動リカバリすることで停止時間を防ぎ、AIベースの自律機能が診断を実行して業務の中断を最小限に抑えます

セキュリティ管理コストの削減：

セキュリティ管理コストを最大で55 %削減します

Autonomous Linux

停止時間ゼロのパッチ適用：

停止時間のスケジューリングや再起動を行うことなく、OSカーネルと重要なユーザー・スペース・ライブラリに停止時間ゼロでパッチを適用します

“

AI/MLはコラボレーションにとどまりません。絶え間ない変化も可能にします。迅速かつ大規模に適応できることは競争上の強みであり、サイバーセキュリティにおいては、生き残れるかどうかという問題にもなり得ます。

accenture

傾向3

DevOpsのセキュアな自動化

DevOpsがますます自動化されるなかで、組織の46%は、継続的インテグレーションでセキュリティ制御を利用するために、DevSecOpsを採用したいと考えています。

2020年のビジネスの進化により、新たなアプリケーションの需要が増加しました。あまりにも急激に需要が増加したため、企業は既存のフレームワークとコンプライアンス・プログラムに新しいセキュリティ制御を導入するのが追いつかないほど速いペースでアプリを生産しており、これにより“ペースのギャップ”が生じています。

企業は、生産ライフサイクルにセキュリティの自動化を組み込んで非効率的な作業とオーバーヘッドを避けることで、このペースのギャップに対応する必要があります。また同時に、セキュリティが実装される前にサービスが本稼働した場合にサービスが公開される可能性を防ぐ必要もあります。このシナリオにより、過去数年間でアプリケーションのセキュリティは徐々に改善されました。

クラウドの刷新は、人とプロセスから始まります。そしてセキュリティは、通常“DevSecOps”と呼ばれる最高のDevOpsユースケースとして進化しました。DevSecOpsにより、サイバーセキュリティ・プロセスが自動化されるとともに、アプリケーションのライフサイクルをオーケストレートする継続的インテグレーションおよび継続的デリバリ（CI/CD）ツールチェーンが制御されます。

セキュリティは、CI/CDの自動化と統合されなければなりません。統合されなければ、製品の開発、統合、提供から取り残されてしまいます。そのため、組織の40 %が、DevSecOpsによって開発、インフラストラクチャ管理、アプリケーション所有者、サイバーセキュリティ関係者との間の高度なコラボレーションが促進されたと報告しています。さらに企業の40 %が、DevSecOpsのおかげで、自動化を通して業務効率を向上できたと述べています。

DevSecOpsの採用により、効率性とコラボレーションが向上するだけではありません。セキュリティ・インシデントへの対応からセキュリティ体制のプロアクティブな強化へと、組織の重点を変えることができます。ITリーダーは、セキュリティ制御をDevOpsプロセスに継続的に組み込むことで、日々の問題管理に費やす時間を短縮し、ビジネスに価値を与える取組みにより多くの時間を費やすことができます。

46 %

継続的インテグレーションでセキュリティ制御を利用するために、DevSecOpsを採用したいと考えている割合

40 %

DevSecOpsが以下を実現したことを報告している割合

- 高度なコラボレーション
- 業務効率の向上

Oracle Cloudセキュリティ実践ブログ(英語)

オラクルと他社との違い

自動化されたインテリジェントなセキュリティ

セキュリティを自動化：

Autonomous DatabaseとAutonomous Linuxの自動パッチ適用により、セキュリティを自動化して複雑性を低減し、人的エラーを防止し、コストを削減するとともに、Oracle Cloud GuardとOracle Identity Cloud Serviceにより脅威を軽減します

基本的なセキュリティ制御を自動化：

保管中のデータと移動中のデータの暗号化や、新機能の追加時の自動テストを含む基本的なセキュリティ制御を自動化することで、セキュリティが継続的に改善され、更新されます。

構成の選択肢を特定：

Data Safeを使用して、リスクをもたらす構成の選択肢を特定し、構成のずれを浮き彫りにします

クラウドの自動化により継続的デリバリプロセスを実現：

Oracle Cloud Infrastructureでは、オラクルのすべてのサービスがオペレーターと開発者に公開されます。オラクルのサービスは、オープンソースのプロビジョニング・ツールをネイティブにサポートすることで、DevOpsチームがコードを使用して不変なインフラストラクチャを構築できるよう支援します

クラウド・セキュリティ・ポスチャ管理の採用：

誤った構成のリソースを検出すると同時に、問題を選別して解決するための可視性を管理者に提供します

傾向4

CISOはかつてないほど多くの役割を任されている

CISOはデジタル変革とビジネス構想にますます関与するようになるため、CISOの役割には、クラウド中心の専門的知識がいっそう必要になります。

昨年は、クラウド対応の準備が整っていることの必要性とデジタル・モダナイゼーションが重視された年でした。その結果、**組織はこれまで以上に最高情報セキュリティ責任者（CISO）に大きく頼るようになっています。**より多くの役割を担うようになったCISOは、組織のチェンジメーカーになり、デジタル・トランスフォーメーション（DX）やクラウド・コンピューティングの取組みの支援を任されています。

CISOは、LOBのリーダーとの連携、ビジネス・プロセスをクラウド・コンピューティングに適合させるための調整、サイバー・リスクの未然防止、クラウド・コンピューティングに関連する脅威モデルの更新、シャドウITアプリケーションの特定などにより多くの時間を費やすようになっています。実際、**組織の73 %は、クラウド・コンピューティングに関する技術や知識をより多く備えたCISOを採用したか、採用する計画である**と回答しています。一方、**53 %はサイバーセキュリティをビジネス・プロセスに取り入れるために、ビジネス情報セキュリティ責任者（BISO）を雇用しているか、雇用する計画である**と回答しています[4]。

CISOがビジネスに集中しているなかで、オラクルは**DX CISOの台頭**も認識しています。DX CISOは、業務の遂行方法を再定義するとともに、ビジネス・プロセスを改善するよう求められるでしょう。DX CISOは、DXの取組みにサイバーセキュリティを取り入れ、ITのあらゆる側面、特にパブリック・クラウド・コンピューティングに、強力なサイバーセキュリティを埋め込む必要があります。テクノロジー・ポートフォリオを合理化するだけでなく、強固に統合されたスケーラブルなセキュリティ・スタックに変換する必要があります。これを行うには、ストリームとバッチ・データ処理用の高パフォーマンスのデータ・パイプライン、ツール間のAPI統合、データ拡充のための脅威インテリジェンスの取り込み、および即時のインシデント対応とリスク軽減のためのプロセスの自動化が必要になります。

CISOは、セキュリティをアジャイル開発、DevOps、および自動化された継続的インテグレーションおよび継続的デリバリ（CI/CD）パイプラインと統合する必要があります。また、チームにクラウド・セキュリティ共有責任モデルについて理解してもらってから、ITインフラストラクチャを全面的に網羅する相乗的なハイブリッドのセキュリティ・モデルを構築する必要があります。さらに、アカウントを停止し、権限ユーザーを管理し、機密データを保護できる最小権限のポリシーを企業と協力して策定する必要があります。

73 %

CISOを採用した、または採用することを計画している割合

53 %

BISOを雇用している、または雇用することを計画している割合

クラウド重視のCISOの資料を読む（英語）

[4] The Mission of the Cloud-centric CISO (KPMG & Oracle Cloud Thread Report)

4

オラクルと他社との違い

Oracle Cloud Infrastructure

顧客の分離と保護：

データ・レジデンシー、データ主権、クラウド・セキュリティによって実現します

フルスタックの保護：

セキュリティに対するオラクルのゼロトラスト・アプローチによって実現します。インフラストラクチャ、ユーザー、デバイス、およびアプリケーションとデータの相互作用についてはユーザーが決定します

検出の自動化：

Oracle Cloud Guardなどのツールを使用して、よくある誤ったセキュリティ構成を自動検出することで、リスクを最小化します

セキュリティ・ソリューションの提供：

脅威を検出し、エラーを修正し、攻撃から保護します

統合型クラウド・セキュリティ・シリーズの提供：

Oracle Identity Cloud Service（IDCS）を含むあらゆるOracle Fusion SaaSアプリケーションにより、一貫性のあるIDベースのセキュリティを実現します

“

DX CISOは単なる新しい役職ではありません。CISOの役割と、CISOとビジネスおよびデジタル変革との関係を進化させたものです。優先度を確保するために、DX CISOはCEOの直属となる必要があります。

KPMG

傾向5

セキュリティ管理の向上には高度な可視性が必要

多くの組織は、すべてのクラウド・ソリューションのセキュリティ・スタックを統合するために新しいツールに投資し、すべてのアプリケーションとインフラストラクチャの完全な可視化を実現しつつあります。

世界的危機を受けて企業が安定性を求めるなか、クラウドはライフラインになりました。クラウド・コンピューティングは、組織が困難に対処し、新たなビジネス機会を創出する速度を向上しましたが、複雑性が増したことで、テクノロジー・スタック全体でセキュリティと可視性についての新たな課題が発生しています。

クラウドネイティブのアプリケーションにより、新しいツール、プロセス、人員が導入されますが、多くの場合それらは成熟しておらず、運用管理のレベルは従来のアプリケーションに及びません。SaaSのオプションやアプリケーションが増加したことで、承認されていないクラウドの使用が広がりました。**各企業では現在、1,000を超える未許可のサービスが使用**されています。サプライ・チェーンはより不正行為を受けやすくなっているため、組織はビジネス全体を幅広く可視化および監査するために、ゼロトラスト・アプローチを実装する必要があります。

デジタル・エコシステムが拡大するにつれ、企業は新しいツールを利用して、データのプライバシと規制に伴う増加し続ける負担に対処する必要があるでしょう。データの量と種類が増えれば、データの検出と分類は困難になり、セキュリティ・チームが一貫性のあるセキュリティ・ポリシーを施行することも難しくなります。実際、**組織の30 %が、パスワード、暗号化鍵、API鍵を含む“クラウドのシークレット”がクラウドベースのサーバーに保管されている**ことを発見しました。コンプライアンスと業界規制は進化しており、コンプライアンスの遵守を徹底するためのより良い仕組みが求められています。

リモート・ワークがきっかけとなり、クラウドの採用が急速に進みましたが、アクティビティの監視も行っているセキュリティ・チームにとって、クラウドのアクセスと権限を把握することはますます困難になっています。企業は、クラウド環境を保護する複雑性を事前に予測して対処する必要があります。

多くの大企業は、複数のIaaS、PaaS、およびSaaSプロバイダを利用しており、各プロバイダには独自の共有責任モデルがあるため、誤った構成、ソフトウェアの脆弱性、人的エラー、プロセスの冗長性などの影響を受けやすくなります。リスクを低減し、継続的な保護を促進するには、企業はデータベースとアプリケーションのセキュリティ、企業セキュリティとプライバシ、IDおよびアクセス管理とともに、インフラストラクチャを検討する必要があります。

1000以上

日常的に使用される未許可サービスの数

30 %

クラウドのシークレットがクラウドベースのサーバーに保管されていることを発見した割合

データ・セキュリティと保護のeBook (英語)

Oracle Cloudでのセキュリティの監視、管理、緩和

完全なSaaSセキュリティ制御：

Oracle Identity Cloud ServiceおよびOracle Risk Management Cloudを通してアプリケーション所有者、監査担当者、セキュリティ運用チームに完全なSaaSセキュリティ制御を提供

レスポンスと修復の提供：

Oracle Identity Cloud Serviceにより、行動の監視とセカンダリ認証を提供

自己保護の自律型データベース：

Oracle Data Safeを使用してデータベース全体でセキュリティを管理することで、アクティビティを分析し、監査ポリシーを管理し、構成のずれを検出し、テストと開発の各プロセスからリスクを排除します

クラウド・セキュリティ・ポスチャ管理：

Oracle Cloud Guardにより、Oracle Cloud Infrastructureの顧客テナント全体に対するクラウド・セキュリティ・ポスチャの統一ビューが提供されます。

Oracle Cloud Guardによる誤構成のリソースと非セキュアなアクティビティの検出：

テナント全体で誤った構成のリソースとセキュアでないアクティビティが検出され、セキュリティ管理者に、クラウド・セキュリティ問題を選別して解決するための可視性が提供されます。一貫性のないセキュリティは、設定不要のセキュリティ・レシピを使用して自動的に修復されるため、セキュリティ運用センターの規模を効果的に拡大または縮小できます

今後の傾向

2020年が業務の遂行方法を永遠に変えたことはもはや明白です。もう1つ明らかになったのは、セキュリティを優先するアプローチが、複雑性を低減しながらイノベーションを促進する上で大きな役割を果たす可能性があることです。

組織は適切なツールを導入することで、セキュリティを自動化し、人的エラーを防止し、コストを低減できます。リモート・ワークとクラウド・コンピューティングは新たな標準になりつつあります。

IT部門のトップは、この先何年も続くより安全な企業の未来を形成する上で、非常に重要な役割を担うでしょう。

変化に対応できる
Oracle Cloudの詳細を
知る

さらに詳しく

Oracle Cloudが
お客様に選ばれる
理由を知る

事例を見る

クラウド・インフ
ラストラクチャ・
セキュリティの
詳細を確認する

詳細情報

オラクルのクラウド・セキュリティについての詳細はこちら
https://www.oracle.com/jp/security/cloud-security/

オラクルのクラウド・プラットフォームについての詳細はこちら
https://www.oracle.com/jp/cloud/

【オラクルの製品・ソリューションに関するお問い合わせ先】
https://www.oracle.com/jp/corporate/contact/

ORACLE