ORACLE

クラウド中心のCISOのミッション

オラクルとKPMGによるクラウドの脅威レポートからの
サイバーリーダーの最優先事項と課題の解明

進化する役割の定義

組織は、情報を保存、処理、分析するためにITシステムに依存する度合いがますます高まっています。これらのリソースをデータ・センターからパブリック・クラウドに移行する量が増えるにつれ、効果的なリスク軽減プログラムを使用してこの情報の安全性を確実に維持することへの依存度が高まり続けます。

長年にわたって、この情報の安全を確保する役割は、最高情報責任者（CIO）から最高情報セキュリティ責任者（CISO）に移ってきています。このように役割の帰属が一本化されたことで、CIOが負う日々の負担の多くが軽減され、セキュリティの責任が1人の役員の手に渡りました。また、これにより、CISOの役割を担う人々にとって現実的な課題も生まれました。なぜなら、これらの役員は、全体的なデータの可用性、プライバシ、セキュリティを確保する必要があるからです。

GDPRの時代に成功を見出している組織は、セキュリティとリスクは経営幹部間で共有される責任であることを理解しています。これを裏付ける証拠は、最高個人情報保護責任者（CPO）と最高データ保護責任者（CDO）を採用していることです。
これらの責任者は、増え続けるデータの保護とコンプライアンスの確保に極めて集中した命令を下します。ビジネスの全体的な成功とセキュリティにおいて、経営幹部全員が非常に重要な役割を果たします。

経営幹部全体がこのようにセキュリティを重視しているため、単に“防止”だけでなく、実現においてもCISOが果たす役割の範囲が拡大します。1日の終わりにおけるCISOの仕事は、顧客、パートナー、組織自体のリスクを管理すること、そして、ビジネスの成功を実現できる方法でこの仕事を行うことです。

この実現は、新しいサービス、データ、ユーザー、またはインフラストラクチャの採用を予定しているすべての事業部門の担当者が席に着いたテーブルに席が用意されているCISOから始まります。これらの事業部門が最初の計画段階の議論にCISOを関与させることができないと、赤信号が灯ります。

CISOが果たすこの高度に戦略的な役割は、現在の競争の激しい情報第一の環境において極めて重要です。このような環境では、サイバー脅威がいたるところに存在し、企業は毎日のように侵害を受け、コンプライアンスが義務付けられています。
CISOは、これらのビジネスの取り組みを成功させるのに不可欠である主要な役割を果たします。ただし、最高の意思と計画にもかかわらず、多くの場合、成功を確かなものにできるチーム自体とのコミュニケーションと効果的連携という課題が生じます。

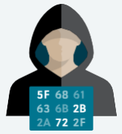
それでは、調査結果を見てみましょう。

CISOの現実

クラウド・インフラストラクチャ

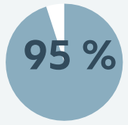
99 %
クラウド・サービスを使用してWebアプリケーション・ファイアウォールを活用することが重要/不可欠であると考えているCISOの割合

しかし、実践しているCISOの割合は**23 %**にすぎません



CISOと政府の最大懸案事項は、外国政府による攻撃/ハッキングです（Security in Age of AI）

10分の1 セキュリティ・イベント・テレメトリの75 %以上を確認できる組織の割合



クラウドが独自のデータ・センター“と同じくらい安全”または“より安全”だと述べているCISOの割合

クラウド常駐ワークロードを監視するためにクラウド・インフラストラクチャのセキュリティ制御を活用することを重視しているCISOの割合

データ管理

38 %
最も重要な課題は安全なクラウド構成の維持であると考えているCISOの割合

48 % 品質保証契約（SLA）への影響が原因でパッチ適用が遅れたCISOの割合

No. 1
組織に対して高まっているリスクの根拠のうち“人為的エラー”が占める順位

ほぼ半分（49 %）
2020年までにデータの大半をパブリック・クラウドに保存すると見込んでいる回答者の割合

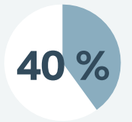
48 %
データベース環境から始めて、自動パッチ管理を導入することを計画しているCISOの割合

SaaSアプリケーション

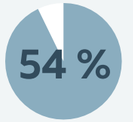
71 %
ビジネス・クリティカルなデータを保存するためにクラウドを活用している組織の割合

注目すべきことに、回答者のうち**69 %**が、使用しているクラウド・サービスのうちビジネス・クリティカルなものは12か月前よりも増えていると述べました

責任共有セキュリティ・モデルにおけるチームの役割を完全には理解していないCISOの割合

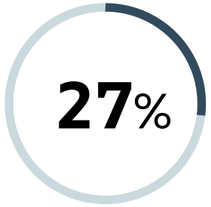


クラウド内のセキュリティ・インシデントの検出と対応という課題に直面しているCISOの割合



不正なクラウド・アプリの使用に対処しているCISOの割合。CISOのうち54 %が、この使用の結果としてマルウェアが持ち込まれていると述べています

ビジネスの実現に向けたCISOの移行



IT運用とセキュリティ運用の間の調整が欠如していると報告している組織の割合

CISOとCIOの間の不一致は、リーダー間の可視性と透明性が欠如していることを示唆しているため、問題の原因となります。

Oracle、Greg Jensen

効果的なCISOは成功を実現できます。たいていの場合、CISOは保護と実現に集中していると見なされています。これは、企業の野心と部門の目標の障害になります。CISOが効果的な存在になるには、「いいえ、あなたにはできません」と言う役員であると見なされないようにする必要があります。むしろ、CISOは、「はい、あなたにはできます。そして、それを安全に行う方法はこのとおりです」と言うことで知られる存在であるべきです。

ストレスの多いCISOの仕事には、失敗が許容される余地がほとんどありません。侵害が起こった場合、特にデータが盗まれた場合、CISOには、おそらくCIOと一緒に、厳しい処罰が下ります。このことは、CISOが「Crisis-Induced Sacrificial Offering（危機によるいけにえのささげ物）」とも呼ばれる一因となっています。成功を確実に実現するために、この責任を経営幹部全員で共有する必要性がかつてないほど高まっています。

実際的な知識のあるCISOは、変革の仲介者である必要があります。従来のリスク回避型のITスタッフとは異なり、効果的なCISOは、リスクを軽減し、脅威に対応し、コンプライアンス目標を達成しながら、ビジネスの成長をサポートするためのより優れた方法を常に模索しています。

外交的手腕のあるCISOは、IT運用チーム、セキュリティ運用チーム、開発セキュリティ運用チームの間のギャップを埋める必要があります。これは、IT運用チーム（情報管理の問題を解決する）、セキュリティ運用チーム（リスクを軽減し、データを保護し、コンプライアンスを実現する）、開発セキュリティ運用チーム（漏洩への取り組みと修復への取り組みの間のギャップを埋める）の間のギャップです。これらのチーム間の機能不全により、敵対者によって悪用される可能性があるギャップや機会が生じます。

先見の明のあるCISOは、優先順位と計画に焦点を当てます。この進取的な役割は、ビジネス・リーダーがビジネスの目標を達成する安全な方法を緻密に計画しながら、リスクを軽減し、コンプライアンスを実現するのを支援する上で不可欠です。

効果的なCISOのおもなタスク

- ビジネスを理解して、すべてのセキュリティ、リスク、プライバシ、コンプライアンス、データ整合性のニーズに関して信頼できるアドバイザーになる
- 不正、データ損失、脅威に対するリスク回避戦略を策定する
- 従業員、顧客、パートナー、データ、アプリケーション、インフラストラクチャの情報セキュリティを実装する
- 新しい脅威や出現しつつある脅威に対する検出、対応、修復、通知プログラムを開発する
- チームがクラウド・サービスとサービス・プロバイダの責任共有セキュリティ・モデルに従うよう徹底する
- 企業の情報（特に機密データ）にアクセスできる可能性があるすべてのサード・パーティ・プロバイダの査定を支援する
- 規制監視チームと連携して、コンプライアンス目標を達成する上で役に立つプロセスとテクノロジーを定義および実装する
- 企業のセキュリティ標準、ポリシー、テクノロジー・スタックを所有する
- ITチームおよび開発セキュリティ運用チームと一緒に脆弱性、構成、パッチ対応プログラムを定義および管理する

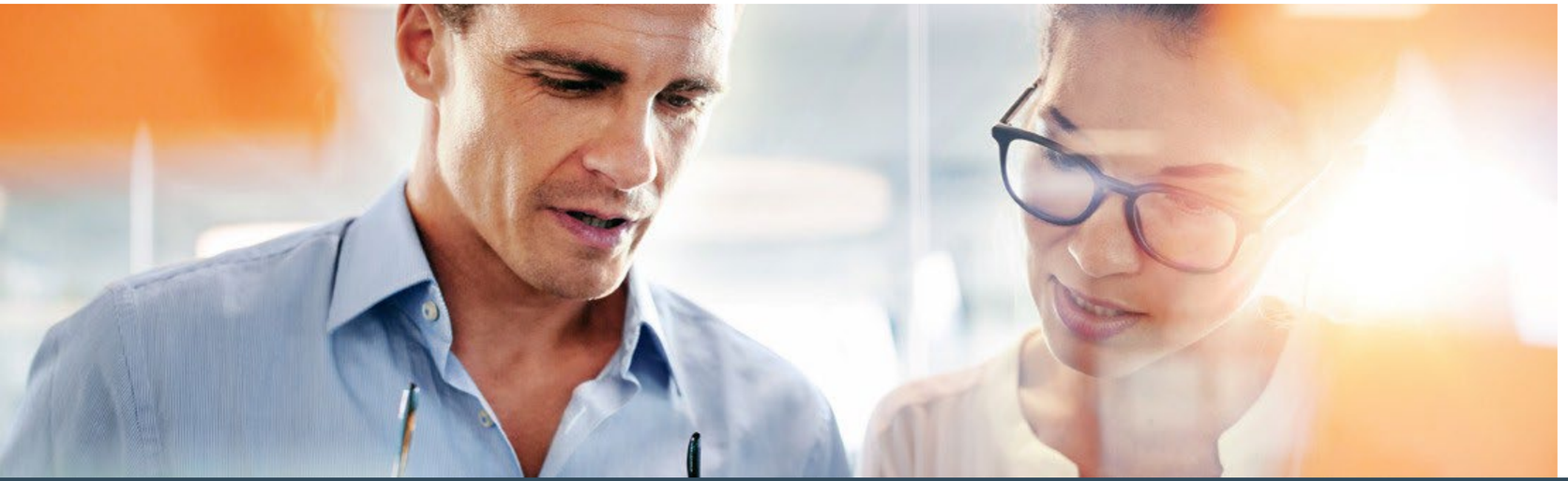
インシデントの防止、検出、対応、リカバリ

92%

確立されているセキュリティ・ポリシーに違反する、クラウド・サービスの認可されていない使用または不適切な使用を含むシャドウITに起因するデータ損失または侵害を心配しているCISOの割合

インシデントのリスクを下げ、攻撃の影響を軽減するには、効果的なリーダーシップが必要です。

Oracle、Laurent Gil



CISOは皆、事後対応型のインシデント検出よりも事前対応型のインシデント防止に焦点を当てることを好むことに疑いを挟む余地はありません。ただし、組織は24時間365日、攻撃を受けるリスクに晒されています。これは、多くの場合、緊急の検出と対応の方が予防的手段よりも重要であることを意味します。

企業の保護を成功させる鍵となるのは、クラウド・サービス、データ・センター、インフラストラクチャ、エッジの極めて重要なパッチ適用と構成管理です。これには、

エンドポイント・システム、モバイル・デバイス、サーバー、モノのインターネット（IoT）が含まれます。

しかし、組織のCIOの48 %は、品質保証契約（SLA）に影響を及ぼす停止時間やソフトウェアの非互換性が原因で、管理者が時間どおりにパッチを適用できないと報告しています。また、ITチームの51 %には、パッチ適用の優先順位が原因でその他のプロジェクトを遅らせざるを得なかった経験があります。

良いニュースは、CISOの89 %が、データベースを管理対象の第一環境として、自動パッチ管理ソリューションを現在採用している、または採用する予定である、と述べていることです。

それ以外の良いニュースは、機械学習と行動分析のおかげで、組織が、準拠していないか構成が正しくないクラウド・サービスのために企業データがどれくらいリスクに晒されている可能性があるかをより効果的に特定できることです。

実際に、機械学習と高度な自動化により、ここ数年の間に、組織がリスク・ポイントを特定し、修復またはリスク軽減プロセスを自動化する作業の支援が大幅に強化されました。

この機能のおかげで、IT運用チーム、セキュリティ運用チーム、開発セキュリティ運用チームは、現在行っている事後対応型の消火活動を行うのではなく、戦略的な計画策定により関与しやすくなります。

人的リスク要素

53%

IT運用組織とセキュリティ運用組織のサイバーセキュリティ・スキルの不足を報告している組織の割合

セキュリティ運用チームのために十分に有能なスタッフを採用、トレーニング、維持することはできません。私たちは、人を雇うことでこの問題を解決することはできず、組織が直面しているサイバーセキュリティの課題に対処するためにテクノロジーと自動化に頼る必要があります。

Oracle、Fred Kost

現在のビジネスは、IT運用チームとセキュリティ運用チームの有能なスタッフの慢性的な不足に直面しており、この問題はますます悪化しています。セキュリティで保護すべきサービス、トレーニングすべきユーザー、パッチを適用すべきシステム、処理すべきイベントは増え続けています。多数の大規模な侵害の原因を探ると、人的エラーや、リスクを特定して管理するのに役立つツールとプロセスの不足の結果として生じる、誤った構成のクラウド・サービスにたどり着きます。

オーバーロードのおもな原因の1つは、ログ・ファイルやリアルタイム・アラートなどのデータ（特にイベント駆動型データ）が多すぎることです。人間はどうしても、そのような大量の情報をただちに分析して対応することができません。あるいは、一切できません。現在の人員配置には、イベントの流れを分析し、誤った構成を事前対応的に計画して監視し、膨大な課題に対処するための能力、時間、知識が欠如しています。

厄介な問題：パブリック・クラウド・インフラストラクチャとプラットフォーム、およびミッション・クリティカルなSaaSソリューションには、潜在的な不正とデータ損失を特定するのに役立つイベント駆動型情報が豊富に含まれています。すべてのセキュリティ・イベント・テレメトリを収集し、オンプレミス・イベントと相互に関連付け、異常な動作の徴候について分析する必要があります。

組織内では、これが人的エラーの影響と組み合わされることで、誤って構成されたこれらの誤った構成のクラウド・サービスにおける

機密ビジネス・データの漏洩につながります。この種のデータ侵害は防止できる可能性が高いですが、多くの場合、スタッフがアクセスと構成の管理の責任を見落としたときに見逃されてしまいます。

私たちは、情報を守る方法の優先順位を付け直し、この方法について再考する必要があります。私たちには新しいシステムが必要です。これを、私たちの人材と敵対者のコンピュータとの戦いにすることはできません。それでは、私たちはその戦いに負けてしまいます。これは、私たちのコンピュータと敵対者のコンピュータとの戦いにする必要があります。そして、間違いを犯さないことです。これは戦いなのです。

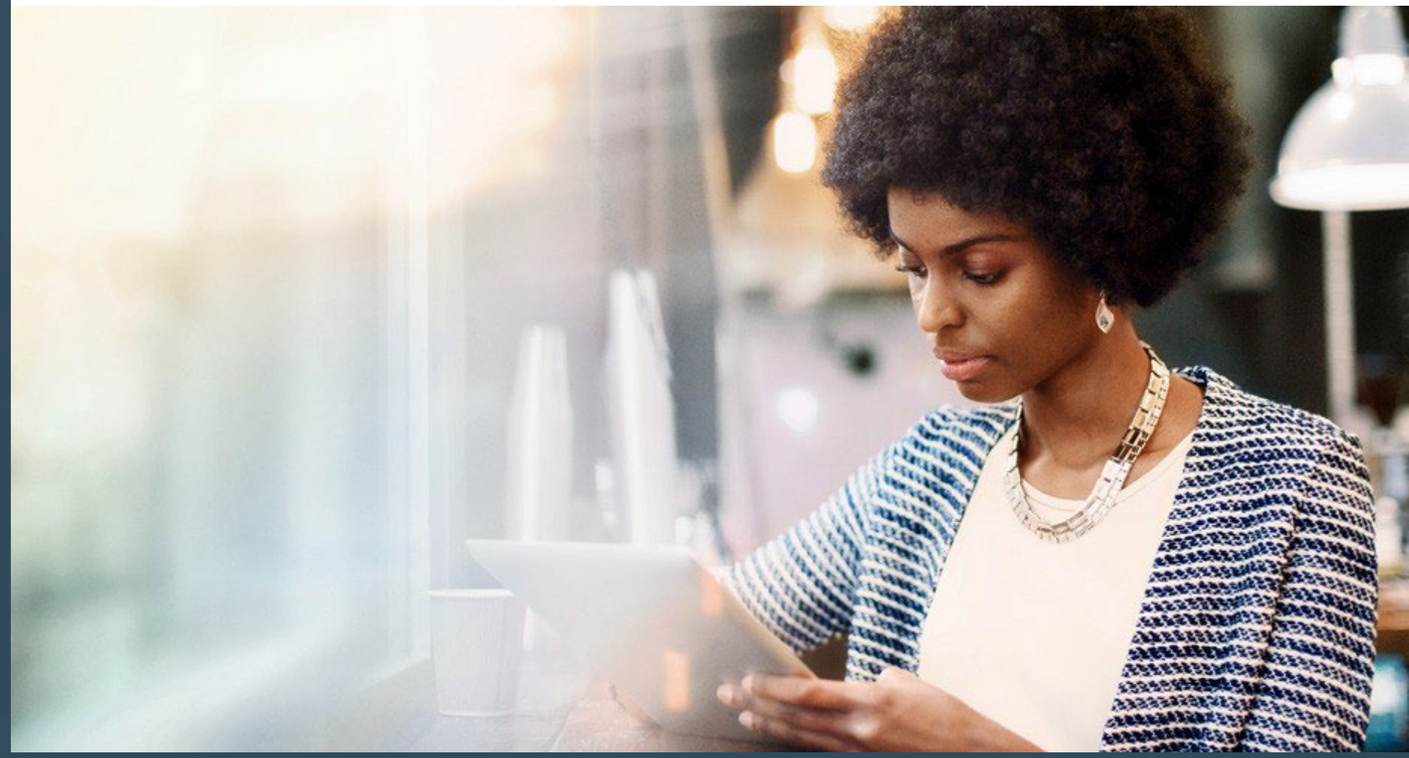
Oracle、Larry Ellison

幸いにも、自動化により、過度なイベント・ノイズや反復的なタスクが排除され、セキュリティ担当者が新しい戦略的取り組みを実現できるようになります。

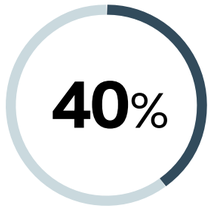
セキュリティ担当者が新しい戦略的取り組みを実現できるようになります。

一方、人工知能、特に機械学習と深層学習により、数百（または数千）の異なるログと情報フィードを相互に関連付けることで、変異と異常を素早く見分けることができるパターンが特定されます。

これにより、現在のCISOは、リスクの高い構成、行動、応答を特定するのに必要なツールを備えるようになりました。サイバー犯罪と内部関係者による脅威に対する戦いにおいて、最高の組織に属するCISOは、可視性が必要な領域で可視性が高まります。



CISOの機会



最優先のサイバーセキュリティの課題はクラウド内のセキュリティ・インシデントの検出と対応であると言っているCISOの割合

多層防御はサイバーセキュリティのベスト・プラクティスですが、その実装には困難が伴う場合があります。成功するには、使いやすく、クラウドのワークロードを保護するためのプロセスに組み込みやすい包括的な多層防御にアクセスする必要があります。

Oracle、Johnnie Konstantas

クラウドは魔法ではありません。クラウドとは、サービスとしてのソフトウェアであろうとサービスとしてのインフラストラクチャであろうと、サーバー、データベース、ネットワーク・インフラストラクチャ、アプリケーション、IDプラットフォーム、暗号化方法論、エンタイトルメントを表します。これらすべてが連携して、規制コンプライアンスの目標を確実に達成します。安全なクラウド・アプリケーションとクラウド・データに関する責任は、クラウド・サービス・プロバイダとそのビジネス顧客との間で共有されます。

CISOはたいてい、クラウド・コンピューティング用の責任共有セキュリティ・モデル（SRSM）をその他の経営幹部、IT運用チーム、事業部門マネージャーに説明するという苦しい戦いに直面しています。これは、戦って勝つ必要がある戦いです。なぜなら、より多くの部門がワークロードをクラウドに移行しており、残念ながら、場合によってはクラウドにたどり着くために認可されていないサービスを活用しているからです。

未査定のサプライヤの使用であろうと承認済みサービスの不正な使用であろうと、クラウドは、CISOにとってのセキュリティ上の課題であると同時に組織にとっての機会でもあります。CISOの93 %は、組織内で不正なクラウド・アプリケーションの使用が見つかったと報告しています。

もちろん、CISOの最大懸念事項はこれで終わりではありません。一般的なメール・フィッシングや、ターゲットを絞ったスピアフィッシングは増加傾向にあり、エンドユーザーのトレーニングを行ったりメール・セキュリティ・ツールを使用したりしたとしても、機密ネットワークやデータ・リソースに侵入する拠点を築く上で効果を発揮する場合があります。セキュリティ運用チームは、永遠に注意深く監視する必要があります。

また、セキュリティ運用チームは、オペレーティング・システムからネットワーク・スイッチまで、オープンソース・ライブラリからモバイル・アプリまでのあらゆるレベルのスタックで、ソフトウェア（およびハードウェア）にパッチを適用することで、ゼロデイ脅威による漏洩を制限するためにIT運用チームが最新の状態を維持できるよう徹底する必要があります。

もう1つの課題は、大規模な変化に対応することです。大半の組織は、セキュリティ・イベント・データの小さな一部のみを監視しているため、マルウェアや悪意のある攻撃者に拠点を築く機会を与えています。デバイスとアプリケーションの数が増加するのに伴い、CISOとセキュリティ運用チームは、新しいクラウド中心の戦略なしでこれらの脅威を特定して対応するという課題に直面し続けます。

これは戦いなのです。サイバー攻撃者がAIを採用し、深層学習および機械学習アルゴリズムを使用して、マルウェアやターゲットを絞った攻撃をより高度化させてその機能を拡張する可能性がますます高まっています。このため、CISOが火をもって火を制することに焦点を当てるよう徹底する重要性がかつてないほど高まっています。

オラクルは、ビジネス・クリティカルなデータとサービスをセキュリティで保護することに関して確固たる評価を得ています。セキュリティは、オラクルが提供するあらゆる製品およびサービスのDNAの一部であり、Oracle Cloud Infrastructure（OCI）のおもな設計の原則と機能にまで及びます。OCIは、増加の一途をたどるビジネス・クリティカルなワークロード用のスケーラビリティ、安全性、性能の高い環境を提供します。
CISOとCIOは皆、リスクと脅威への露出を減らすためにこの環境に価値を見出す必要があります。

ORACLE

貢献者

Oracle、Senior Technology Writer
Alan Zeichick

Oracle、Senior Director of Cloud Security
Greg Jensen

オラクルのセキュリティ、およびセキュリティ・リーダーとITリーダーがクラウド戦略を最大限に活用する方法について詳しくは、以下でオラクルをフォローしてください。

または、www.oracle.com/securityをご覧ください。

詳しくは、オラクルとKPMGによるクラウドの脅威レポートをお読みください。このレポートでは、ビジネス・クリティカルなクラウド・サービスへの移行において明らかになったセキュリティ上のギャップが浮き彫りになっており、CISOとセキュリティ運用チーム向けの主要な実践事項が提案されています。