CISOのための
内部脅威再考ガイド

内部脅威の重要性は、近年急速に高まっています。Verizon社の2024年データ侵害調査報告書(DBIR)によると、世界中のデータ侵害の68% がヒューマンエラーまたはソーシャルエンジニアリングに関連していました。この割合は2022年と比較して大幅に増加しており、当時は外部の攻撃者による侵害が80%を占め、内部者によるものはわずか20%でした。

さらに、Ponemon研究所の「2023年内部脅威による損失グローバルレポート」では、内部インシデントの55% が従業員の過失によるものであり、これに対応するために平均720万ドルものコストが発生していると報告されています。また、悪意のある内部者による侵害は全体の25%を占め、平均コストは70万1500ドル。一方で、認証情報の盗難は全体の20%を占め、対応コストは平均67万9621ドルに上ります。

内部脅威の影響は、単なる発生頻度の問題にとどまりません。例えば、内部者による侵害の中央値規模は、外部者による侵害の10倍以上に及びます。外部の攻撃者による侵害では約2億件のデータが漏えいした一方で、内部者による侵害では少なくとも10億件のデータが漏えいしています。

さらに、内部不正による侵害のコストは、2022年の1538万ドルから2023年には1620万ドルに増加しており、内部者インシデントの発生件数も1年間で44%も急増しました。

このような脅威は、内部者が複数のIDやデバイスを使用して信頼されたアクセス権限を悪用し、数ヶ月間も行動を隠蔽できるため、過少報告される傾向があります。これらの侵害が検出されないまま長引くほど、被害は深刻になります。外部の脅威は依然として存在しますが、外部者が組織に侵入することは以前より難しくなっています。

このため、外部脅威に過度に注力すると、増加する内部脅威に対する対応が後手に回り、組織全体のリスクが高まる恐れがあります。組織は、リスク要因と悪意のある意図を特定することで、内部インシデントを検知・防止するためのツールをセキュリティアナリストに提供する必要があります。

リスクやプライバシーを蓄理するCISOや経営層にとって、内部脅威を理解し、それを追跡するためのツールを備えることが緊急の課題となっています。また、この理解やツール、さらにインシデントの調査および影響緩和に関する責任を組織内の他の部門と共有することも不可欠です。その一環として、共有ガバナンス執行委員会を設立することが推奨されます。

CISOがサイバーセキュリティ全般に責任を負うのは当然ですが、内部脅威対策プログラムを単独で管理することは、組織にとって危険を伴う場合があります。特に、IT、人事、法務といった複数の部門が共同で設計した事前定義された行動計画、エスカレーション経路、コミュニケーションチャネルがない状態で対応を行わなければならない担当者にとって、そのリスクはさらに高まります。

内部要因が重要

理想的な世界では、信頼された内部者は常に信頼できるままでいるでしょう。ただし、人は複雑であり、その状況や動機は常に変化する傾向があります。CISOやセキュリティアナリストは、不審なアクティビティを監視する際に、この点を常に意識しておく必要があります。

内部インシデントはさまざまな動機によって引き起こされます。2022年には、78%が金銭的な動機によるもので、次いで個人的な恨みが9%、スパイ活動が8%、機会主義が6%となっています。しかし、近年では動機の傾向が変わりつつあります。2024年には、個人的利益が47%に急増し、内部脅威の動機として2番目に多い要因となっています。金銭的動機は依然として50%でトップを占めていますが、復讐を目的としたインシデントは45%に増加しています。妨害行為は43%から40%にわずかに減少しましたが、風評被害を目的とする動機は37%に急増しており、内部脅威の動機として公共の認識が重要であることを示しています。

多くの内部インシデントは、悪意によるものではなく、過失によるものです。以下は、脅威となり得る内部者のタイプです。

不注意による内部不正

内部インシデントの55%は、過失によるものです。セキュリティチームが認証ポリシーやアラートシステムを導入していても、従業員が許可されていないデータにアクセスをしたり、移動させたりしようとした際に、1日に何度もアラートが発生することがあります。

こうした行動は悪意ではなく、不注意や知識不足によるものです。例えばエンドユーザーがデバイスの最新パッチを適用し忘れたり、適切なセキュリティポリシーに従わなかったり、脆弱なパスワードやデフォルトのパスワードを使い続けることがあります。こうしたミスがデータ侵害につながる可能性があります。

また、従業員がセキュリテイプロトコルを生産性を妨げるものと感じると、反発することがあります。許可されたITリソースを使わず、「シャドーIT」や代替のSaaSサービスを使用することもあり、これはCISOにとって大きなストレスの原因となります。

セキュリティ意識の高い従業員であっても、ミスを犯すことがあります。例えば、フィッシング攻撃などのソーシャルエンジニアリング攻撃によって、マルウェア感染や認証情報の盗難が発生するリスクがあります。また、個人的なオンライン利用のために企業の設備を不適切に使用した場合、ウォーターホール攻撃やその他の侵害につながる可能性もあります。シミュレーションツールは、サイバーセキュリティチームがこうした脅威に備えるのを支援できますが、従業員による不注意が続く限り、過失による内部脅威を完全に排除することは困難です。

侵害された内部者

侵害された内部者は、全内部インシデントの20%を占めるものの、かつて最も高額な損失を伴う内部侵害の原因となっていました。2023年には、盗まれた認証情報に関連するインシデントの平均コストが420万ドルと報告されています。これは2022年の460万ドルから減少しています。

侵害された内部者とは、組織内に存在することでサイバー犯罪者に悪用され、活動の足がかりとなってしまう人物を指します。このタイプの脅威は、信頼されていない外部者がインサイダーアクセスを取得した場合に発生し、外部と内部の脅威の境界線を曖昧にします。

ほとんどの場合、これは対象者のデバイスが知らないうちにマルウェアに感染しているか、安全でない接続を介してセッションが乗っ取られたか、ソーシャルエンジニアリング攻撃の被害に遭っていることを意味します。いずれの場合も、認証情報がサイバー犯罪者による攻撃の拠点となり、内部システムを通じた攻撃が実行されます。

もちろん、脅威行為者や競争相手から圧力を受けたり、賄賂や利益の約束によって、意図的にマルウェアをインストールしたり、認証情報を引き渡したりする場合もあります。

悪意のある内部者

悪意のある内部者は最も危険な存在であり、内部インシデントの25%を占めています。2023年には、これらのインシデントの平均コストが480万ドルに達しており、2022年の410万ドルから増加しました。

悪意のある内部者は、すべての内部脅威の中で最も破壊的な影響を及ぼします。彼らは、データ窃取、業務妨害、インフラ破壊などを引き起こす可能性があります。多くの場合、個人的な復讐心によって動機付けられていますが、他組織や国家の脅威アクターのために活動することもあります。また、自己利益を目的として行動することもあります。例えば退職時に貴重な情報を持ち出したいと考えているかもしれません。

大企業や価値の高い知的財産を持つ機閉では、就職を希望する人のうち、わずかながらも、隠れた動機を持つ人がいることはほぼ確実です。この現実は、サイバーセキュリティ分野で実際の事例に基づいて活発に議論されています。

しかし、リモートワークや分散型の働き方が普及した結果、CISOやセキュリティ運用チームにとって、悪意のある内部者を特定することが一層難しくなっています。これは、従業員が過去よりも広範なアクセス権を持つようになったためです。

紹介しました上記の3つのパターンが示すように、内部脅威は複雑かつ動的なものであり、効果的に対処するためには多面的な戦略が必要です。

内部者の行動に関するトレーニング

CISOは、人事、法務、倫理・コンプライアンス部門のリーダーやマネージャーと連携し、調査を共同で蓄理し、必要に応じて移蓄する体制を整える必要があります。
また、全従業員に対して安全な認証方法や許容される利用ポリシーについて理解を深めてもらうことも重要です。従業員には、組織のリソースが監視されていること、そして企業デバイスを使用する際にはプライバシーに一定の制約があることを認識してもらう必要があります。

もちろん、強固なセキュリティと生産性のバランスを取りながら、従業員が業務に必要なリソースへアクセスできる環境を整えることが不可欠です。しかし、意図が善意であったとしても、組織にリスクをもたらす可能性がある場合には、その行動を制限する必要があります。

この目的のため、従業員は組織のデータ保護における自分の役割を再認識できるよう、定期的な研修を受けるべきです。組織は、最低でも年に1回、サイバーセキュリティ意識を高めるためのトレーニングセッションを実施する必要があります。このトレーニングは、多くの場合、ガバナンスやコンプライアンス要件を満たす目的も兼ねています。さらに、役割ごとに特化した教育プログラムを定期的に実施することも効果的です。

内部者の行動を追跡

セキュリティ運用チームが監視の権限を十分に確立した後は、その権限を計画的かつ体系的に行使する必要があります。これは、公式なフレームワークや構造を採用し、予防策を講じ、高度な検知・対応メカニズムを導入することから始まります。

1. フレームワークの策定

サイバーセキュリティ業界には、内部脅威、アクセス、信頼に関する基準やガイドラインを提供する信頼性の高い独立機関が数多く存在します。その一例として、CISAが策定した「内部脅威緩和プログラム」が挙げられます。

ゼロトラストは独立機関によって考案されたものではありませんが、アーキテクチャ、認証、承認に関する詳細なモデルを提供しています。また、NIST、CISA、DISAといった独立機関が、このモデルをさらに発展させています。その目的は、ユーザーに適切な権限を付与し、強力かつ継続的な検証を行うことにあります。

CISOが内部インシデントへの検知、予防、対応能力を向上させたい場合、まず以下の要因を考慮し、自社の状況に適したフレームワークを見つけることが良い第一歩となります。

- セキュリティ
- 成熟度
- コンプライアンス要件
- 予算
- リソース

フレームワークの実現可能性を評価した上で、協調的かつ体系的な導入を開始することが推奨されます。

2. 防止策の組み込み

予防的なソリューションでは、アクセス権限を制限し、不正なアクテイビティが発生した際にセキュリティ運用チームにアラートを送信することが一般的です。これには、最小権限アクセス、役割ベースのアクセス制御、多要素認証といった標準的なゼロトラストセキュリティフレームワークに関連する多くの対策が含まれます。また、データ損失防止(DLP)ソリューションの導入も重要ですが、DLPがコンテキストを欠いている場合、不必要な警告（ノイズ）が発生し、業務の妨げになる可能性があることに留意すべきです。

実際のイベントトリガーに関する洞察がなければ、アナリストはユーザーやデバイスの行動が、不正なのか、不注意によるものなのか、偶発的なのか、それとも既存の基準からの逸脱なのかを判断できません。さらに、DLPアラートがセキュリティ運用チームに大量に通知されると、実際の内部脅威への対応が妨げられる可能性があります。そのため、認証ソリューションを含む脅威検知機能を導入することも不可欠です。

3. 検知の採用

検知とは、行動や振る舞いをその背景となるコンテキストと結びつける能力を指します。そして、優れた検知を実現するための基盤となるのは自動化です。r正常な行動」のベースラインを確立するために、行動分析は常にバックグラウンドで実行されるべきです。これにより、異常な逸脱やその原因となる状況を特定することが可能となります。

こうした異常な状況には、認証情報の不正使用や異常なアクセスパターン、大量のデータアップロード、膨大な情報のコピーなど、さまざまな事象が含まれます。強力な検知分析の仕組みが整備されていることで、アナリストは次のような迅速かつ重要な判断を行うことができます。

- この行動は異常なのか、それとも過去にも発生しているものなのか？
- この行動はピアグループ（同様の役割を持つ他のユーザー）と比較してどのように異なるのか？
- •この行動は不注意によるものなのか、それともアカウントが侵害されているのか？
- 該当アカウントは人間のユーザーか、サービスアカウントか？それによって行動の異常性はどう変わるのか？
- 侵害が検知されていない場合、この行動の裏側には何があるのか？

セキュリティ運用におけるゼロトラストや内部脅威対策のフレームワークの成熟度に関わらず、情報に基づく自動化された検知システムを活用することで、アナリストは異常なユーザーアクティピティを特定し、そのリスクに基づいて評価を行うことができます。

また、自動化された検知システムは、短期的および長期的なセキュリティプロセスを支援するために、以下のような資料の自動生成にも寄与します。

- 十分な脅威の説明：セキュリティベンダーと行動分析の両方から得られるアラートの情報
- インシデントの評価と対応を支援するタイムライン
- 将来の対応を支援するランプック
- 再現可能なプロセスを支援するプレイプック

内部脅威の対応には全社の協力が必要

前述のとおり、内部脅威の調査と対応はCISOだけの責任ではありません。IT部門や業務部門との明確なコミュニケーションおよびエスカレーション経路を確立した上で、セキュリティ運用チームが脅威を封じ込めるための権限を決定した後、他の関連部門をRACI（責任、説明責任、相談、報告）マトリックスを用いて関与させることが重要です。

重要な関係部門は次の通りです。

人事部門

人事部は、従業員の行動やその背景を監視する責任を担います。これには、業績評価が低い場合や懲戒処分といった技術的指標だけでなく、態度や感情といった非技術的指標も含まれます。

人事部は、これらの誓告サインをセキュリティ運用チームに共有し、従業員の行動に基づいた監視リストを作成し、適切な対応策を確立する支援を行うことができます。さらに、解雇が迫っている従業員や契約期間が終了間近の契約社員は、監視が必要な具体的なリスクシナリオに該当します。

法務部門

インシデントが規制やコンプライアンスに影響を与える場合、法務部門が関与する可能性があります。セキュリティ運用チームは、どのような状況でインシデントを法務部門にエスカレーションし、支援を求めるべきかを明確に理解しておく必要があります。例えば、インシデントが外部への報告を義務付けられる「違反」となる条件がどの時点で満たされるのか、といった判断基準を明確にしておくことが求められます。また、法務部はセキュリティポリシーに関連する従業員のプライバシー保護についても、専門的な助言を提供することができます。

セキュリティ部門

セキュリティ運用とは別に内部脅威対策プログラムがある場合、その責任者が最高リスク責任者（CRO)や詐欺対策チームに報告することがあります。また、大規模な組織の場合、内部脅威によって物理セキュリティチームによる対応が必要になる場合もあります。

これらのリーダーや部門間で十分な連携がとれていない場合、プロセスの管理が複雑化し、インシデントによる業務の混乱やコストも増大します。内部脅威対策の取り組みが社内で十分に周知されていない場合、インシデント対応の調整が不十分となり、結果的に対応が遅れる可能性があります。また、CISOが自分の特定の職務権限を超えてしまうと、同僚との関係を損なう可能性があります。

こうした問題を防ぐためには、役割を明確にし、責任の範囲を定めた透明性の高い憲章を策定することが、内部脅威に関する効果的なセキュリティ運営の鍵となります。この憲章は以下の重要な役割を果たします：

CISOの権限強化

CISOがサイバーセキュリティ全責任を一手に担うと見なされることは、悪意ある内部者の行動を増長させる恐れがあります。

一方で、サイバーセキュリティのルールと責任がステアリングコミッティによって共有され、それを従業員に明確かつ効果的に伝えることで、従業員に共同責任の意識を持たせることができます。このアプローチは、従業員の組織に対する信頼感を向上させる効果が期待されます。

予防の強化

既知のインサイダー脅威の指標（たとえば、争議や意見の不一致、否定的なフィードバック、経済的困窮、過度の熱意や不誠実な熱意）に関連する従業員は、人事部によって内部監視リストに追加される可能性があります。

不正行為の疑いがある限り、上級従業員もこの例外ではありません。このため、CISO、人事部、法務部、そして経営層の間で、明確なコミュニケーションラインを確立することが極めて重要です。

検知能力の強化

CISOは、セキュリティアナリストが収集したデータを基に、内部者の「正常な行動」とr異常な行動」を定義し、その情報を他部門と共有することで、従業員の機密性を保ちながら調査を支援できます。

要するに、最良の内部脅威プログラムは、セキュリティ運用をはるかに超えており、以下の主要な特性によって定義されます。

- 協力的かつ学際的であること
- 明確に定義されたプレイブック、ランブック、憲章によって運営されていること
- 参加者間で共同出資されること
- 複数年にわたる一貫した計画に基づき、継続的に最適化されること
- 一貫した計画にはどのような要素が必要でしょうか？

タッチポイント

経営層レベルでは、この憲章に基づき、四半期または半年ごとに会合を開くことが推奨されます。チームリーダーレベルでは、より頻繁に会合を行い、直近のインシデントやベストプラクティスに関する情報を共有します。

成果物

理想的には、これらのタッチポイントから、簡潔なインテリジェンスレポートなどの資料が作られ、毎年、経営執行役会長に提出されるべきです。年末の報告書には、サンキーダイアグラムなどのデータ視覚化を含めて、調査のトリガーとインシデントの解決プロセスを示す必要があります。内部脅威対策のプロセスを最適化することで、組織はインシデント対応において卓越した成果を達成できます。

組織一内の信頼関係の再構築

コミュニケーションは、CISOが内部脅威を軽減するための活動の基盤です。その主なポイントは次のとおりです。

- 組織全体とのコミュニケーション：組織全体に積極的に働きかけることで、リスク意識を共有し、全従業員が自身のサイバーセキュリティへの役割を理解する文化を醸成します。
- リーダー間の意思疎通：同僚とのコミュニケーションにより、リーダーはインシデント対応において組織が成功している点や失敗している点を理解できるため、集合的に能力を高め、高度なセキュリテイプログラムを構築できます。
- アナリストとのコミュニケーション：セキュリティ運用全体でのデータ収集を強化しつつ、アナリストと継続的に情報を共有することで、「正常な行動」のベースラインが確立できます。これにより、ユーザーの行動について迅速かつ情報に基づいた判断が可能になります。

ゼロトラストアーキテクチャの基本原則である「決して信頼せず、常に検証する」だけでなく、ユーザーの行動と権限を積極的に監視する基準を確立することで、このフレームワークは組織内の相互信頼を大幅に向上させ、より堅牢なセキュリティ環境を実現します。現在、一部のセキュリティコミュニティでは、内部者を暗黙の「脅威」として抑制・管理すべき存在とみなす従来のアプローチを離れ、組織全体に求められる多様な信頼レベルに注目する傾向が強まっています。

最新の協調的なセキュリティ運営は、この文化的変革を推進し、組織全体で責任を共有する意識を醸成します。これにより、内部リスクが内部脅威に発展するのを防げます。

About Exabeam

Exabeamはインテリジェンスとオートメーションの分野をリードし、世界有数の企業のセキュリティ運用を支えています。グローバルなサイバーセキュリティ革新企業として、Exabeamは実績豊富でセキュリティに特化した柔軟なソリューションを提供し、脅威の検出・調査・対応（TDIR）をより高速かつ正確に実現します。

Learn more at www.exabeam.com →