ivanti

# エクスポージャー管理の指標の入門書

エクスポージャー管理の登場は、組織のサイバーリスクへの取り組み方をすでに変えつつあります。この変化の不可欠な要素は、サイバーリスクの測定方法です。この入門書では、企業がエクスポージャー管理プログラムのあらゆる要素を分析し、指針を示すために使用できる各種の指標を紹介しています。

これらの指標を使用することで、セキュリティチームはリスクの優先順位付けを改善し、業務の効率と効果を向上させることができます。また、リスクを定量化し、経営幹部や取締役会、およびエクスポージャー管理に関わるその他の事業チームにリスクを周知する能力も向上します。

## 運用指標

これらの指標は、セキュリティチームが日々のエクスポージャー管理活動を行う上での指針として使用します。

| アタックサーフェス（攻撃対象領域）の可視化 | |
|---|---|
| 説明 | サイバー資産の可視化はエクスポージャー管理の基礎を成す存在です。組織には3種類のサイバー資産があります:<br>■ 既知の既知: 攻撃対象の一部であることが分かっており、何らかの形で正式に報告されているサイバー資産<br>■ 既知の未知: 攻撃対象領域の一部であることは知っているが、可視化されていないサイバー資産<br>■ 未知の未知: 攻撃対象の一部であるかどうかが不明なサイバー資産<br>アタックサーフェス（攻撃対象領域）の可視性の指標は、アタックサーフェス全体のうちどの程度 (どれくらいの量) が見えているかを示します。見えている割合を測定することで、セキュリティチームは、可視性のギャップを埋める必要がある箇所を特定し、これらの盲点を狙ったサイバー攻撃から組織をよりよく守ることができます。目標は、(おそらく達成不可能ではありますが) 100%の可視化です。 |
| 測定方法 | エクスポージャー評価に使用している製品やプラットフォームを通じて可視化できているサイバー資産の概数を、環境内の「既知の既知」および「未知の既知」の資産の概数で割り、そして100を乗じてパーセンテージに換算します。 |

なお、「未知の未知」の資産については、アタックサーフェスの可視性においては指標が計算不可能なため考慮されませんが、無視するわけにはいきません。Ivantiのアタックサーフェスチェックリストを使用して「未知の未知」を「既知の既知」に変え、アタックサーフェスの可視性を100%に近づけましょう。

## 運用資産

| | |
|---|---|
| 説明 | アタックサーフェスの可視性を算出したら、次は管理対象となる資産を算出することが重要です。この指標は従来、エンドポイント管理 (UEM) ツールを通じてアクティブに管理されているデバイスの割合を知るために使用されてきました。UEMツールとは、IT管理者によるデバイスの設定やセキュリティポリシーの制御を可能にするものです。<br><br>エクスポージャー管理の分野では、「管理対象資産」とは、セキュリティチームにエクスポージャーの調査結果・所見をもたらしている資産のことです。忘れてはならないのは、資産の可視化は最初の一歩に過ぎず、リスクを算出するにはエクスポージャーの発見が必要だということです。 |
| 測定方法 | エクスポージャー調査結果を収集するときに対象になっている資産の数を、可視資産の数で割ります (上記の「アタックサーフェスの可視性」の数値を使用)。100を掛けてパーセンテージ値にします。 |

Ivantiのエクスポージャー管理準備体制のチェックリストを使用して、すべての資産を管理下に置くためにサイバーセキュリティスタックに追加する必要があるテクノロジーを決定しましょう。

## エクスポージャーリスクの格付け

| | |
|---|---|
| 説明 | サイバー資産とエクスポージャーを可視化すれば、それらのエクスポージャー関するリスク格付けの割り当てを始められます。エクスポージャーリスクの格付けにより、セキュリティチームは、組織に対して悪用される可能性が最も高い脅威を特定し、優先順位を付けて事前対策を講じることが可能となります。また、どのような脅威が経営幹部、取締役会、その他のエクスポージャー管理のステークホルダーの注意を喚起する必要があるかも測定できます。 |
| 測定方法 | エクスポージャー評価の製品およびプラットフォームは、脆弱性、設定ミス、セキュリティ管理ギャップ、その他のエクスポージャーに関するリスク格付けを、さまざまな要因に基づいて算出するプロセスを自動化します。<br><br>■ 深刻度 (例: CVSSおよび/またはベンダーのスコア)<br>■ 悪用可能性 (脆弱性インテリジェンスやEPSSなど)<br>■ 潜在的な影響 (資産の状況や事業への影響など)<br><br>包括的なリスクの格付けは、エクスポージャー管理を従来の (深刻度のみを考慮する) 脆弱性管理や (脅威のコンテキストは考慮するが、ビジネスへの影響は考慮しない) リスクベースの脆弱性管理とは異なるものにしているひとつの要因です。 |

## 意思決定指標

これらの指標は、最高経営幹部、取締役会、その他の経営ステークホルダーが、エクスポージャー管理に関して十分な情報を得た上で意思決定できるようにするものです。

| サイバーリスクレベル | |
|---|---|
| 説明 | サイバーリスクレベルとは、組織のサイバーセキュリティ状況を数値化したスコアです。組織のリスクアペタイト（ビジネス目標を達成するために許容されるサイバーリスクの水準）と組み合わせることで、組織のサイバーリスクレベルは、経営幹部によるエクスポージャー管理の意思決定における重要な判断材料となります。 |
| 測定方法 | エクスポージャー評価の製品やプラットフォームは、資産レベルから評価を開始することで、組織のリスクレベルを定量化します。これらの製品やプラットフォームは、以下のような要因に基づいて、組織環境の各資産にリスクスコアを割り当てます:<br>■ 資産に関連するエクスポージャーのリスク格付け (前述の通り)<br>■ 資産のアクセシビリティ (外部または内部の経路を通じて、資産にいかに容易にアクセスできるか)<br>■ 資産重要度 (損失や漏洩による潜在的な影響という観点からの組織における資産の重要性)<br><br>資産リスクスコアは、組織全体であれ、特定の事業部門や営業地域であれ、関連するレベルでの意思決定のためにロールアップできます。リスクスコアの範囲や意味は各ベンダーごとに異っていますが、多くのベンダーはテストやクイズに使用されるような0〜100のスケールを使用しています。数値が低いほどリスクが高く、セキュリティ状況が弱いことを意味し、数値が高いほどリスクが低く、セキュリティ状況が強いことを示します。 |

エクスポージャー管理のステークホルダーに公式データを提示する前に、このエクスポージャー管理入門書を使って、サイバーリスクレベルとリスクアペタイトについて周知してください。

| 予測されるサイバーリスクレベル | |
|---|---|
| 説明 | 組織の現在のリスクレベルは、意思決定プロセスの一部に過ぎません。何らかの決定が下されたとき、これがそのリスクレベルにどのような影響を与えるかを予測することも同様に重要です。<br><br>■ サイバーリスクレベルがリスクアペタイト（リスク許容度）を下回っており、あるエクスポージャーの修復によりリスクレベルがリスクアペタイト内に収まる（あるいはそれに近づく）と予測される場合は、修復の実施をさらに慎重に検討する必要があります。<br>■ また、エクスポージャーを放置しても組織のリスクレベルはリスクアペタイトを下回ると見込まれている場合も、修復の実行は検討に値します。<br>■ あるエクスポージャーが、プラスであれマイナスであれ、リスクに実質的な影響を与えないと予測される場合、通常はそのエクスポージャーを受け入れ、後で再評価することができます。<br><br>サイバーリスクレベルに関する指標は、一目で分析を行う際に役立ちます。これらの指標を使うことで、組織は現状を迅速に把握し、行動が必要なタイミングを把握できるようになります。一方で、重大な意思決定を行うためには、さらに高度な分析が行われます。年間予想損失額（後述）のような指標は、そうした場合に役立ちます。 |
| 測定方法 | 推奨される修復に基づいて予測されるリスクレベルの変化の予測は、一部のエクスポージャー評価の製品やプラットフォームに備わっている高度な機能です。予測は、エクスポージャーを修復することが、組織の現在のサイバーリスクレベル（上述の通り）の算出に必要となる要素にどのような影響を与えるかを見積もることによって算出されます。 |

| 年間予想損失額 (ALE) | |
|---|---|
| 説明 | 最終的には、企業の経営者は物事をビジネス用語で説明することを求めます。年間予想損失額は、エクスポージャーのリスクを金銭として定量化することで、まさにこれを実現しています。 |
| 測定方法 | ALEは以下の変数を乗じて算出されます。<br>■ SLE (単一予想損失額) は、リスクにさらされている資産の価値に、脅威がその資産に与える可能性のある損失の割合を乗じることによって1回のサイバー攻撃にドルの価値を割り当てる、ビジネスへの影響の指標です。<br>■ 年率発生率 (ARO) は、1年間という期間において脅威が発生する頻度を推定する、発生可能性の指標です。<br>現在のALEと残余ALE (リスクを軽減または修復した場合の推定ALE) を比較することで、経営幹部はコスト/便益の分析を行い、組織がリスクに対処すべきか、またはリスクを受け入れるべきかを決定できます。もちろん、ほとんどのエクスポージャー管理の決定と同様、組織のリスクアペタイトは考慮しなければいけません。 |

Ivantiのサイバーリスクの客観的評価: データドリブンなリスク評価のガイド Eブックでは、ALEやその他の指標を使用して組織におけるエクスポージャー管理の意思決定を導く方法を、ステップバイステップで説明しています。これらのリスク報告スライドを使用して、あなたが下した評価をステークホルダーに向けて提示できます。

## パフォーマンス指標

これらの指標は、エクスポージャー管理の活動結果を示しています。肯定的な影響を証明することで、エクスポージャー管理に対する組織の支援と投資を促進できます。

| 解消済みの脅威の負債 | |
|---|---|
| 説明 | セキュリティチームが組織を守るために行っている予防的な取り組みの功績が認められることはほとんどありません。セキュリティ上のインシデントが発生してチームが対応するときなど、彼らに寄せられる評価の大半はネガティブなものです。<br><br>エクスポージャー管理は、サイバーセキュリティの意思決定に経営サイドを関与させることによってこうした状況を変えることができます。ただし、経営サイドが関与するのは、「有名な」脆弱性を修正する必要があるかどうか、また、新しいセキュリティ対策の導入のために投資を行うべきかどうかといった、より重要な意思決定に限られることでしょう。解消済みの脅威負債を報告することで、セキュリティチームは、これまでに完了したエクスポージャー管理の作業の全容を示すことができます。<br><br>解消済みの脅威の負債に関する指標について留意すべき重要な点は、これらの指標は活動ベースですが、一方、エクスポージャー管理は結果がすべてであるということです。これらの指標は、チームの仕事量を伝えるのに役立ちますが、その仕事の結果を示すことの方がより重要です。 |
| 測定方法 | エクスポージャー評価の製品やプラットフォームは、解消された脅威の負債の指標を構築するために使えるデータを提供する必要があります。通常は、そのデータにフィルターをかけ、特定の情報に絞り込むことができます。いくつかの例をご紹介します。<br><br>■ 第2四半期に9,423件のマルウェアを駆除<br>■ 第1四半期にランサムウェアに伴う399件の脆弱性を解消<br>■ 重大な脆弱性の数を第4四半期に40%削減 |

| サイバーリスクレベルの変化 | |
|---|---|
| 説明 | 現在および予測されるサイバーリスクレベルは、エクスポージャーを修復するかどうかの短期的な意思決定の指針として使用できるが、時間の経過に伴うサイバーリスクレベルの変化は、その意思決定が及ぼす長期的な影響を示します。セキュリティチームが自分たちのエクスポージャー管理業務の成果を証明する一つの方法は、組織のサイバーリスクレベルをリスクアペタイトの範囲内に維持する能力、あるいは必要に応じてレベルを改善する能力を実証することです。<br><br>現在および予測されるサイバーリスクレベルを経営幹部のステークホルダーと定期的にレビューすれば、時間の経過に伴う変化やその欠如を報告する際に驚くようなこともありません。むしろ、サイバーリスクレベルの変化に関する報告は、エクスポージャー管理が設計通りに機能していることを強調する機会となり得ます。 |
| 測定方法 | サイバーリスク レベルの変化は、さまざまな方法で測定および報告できます。<br><br>■ 絶対的な変化 (2つの異なる時点におけるサイバーリスクレベルの正確な数値の差、例えば、サイバーリスクレベルが1月1日に72で、12月31日に83であった場合、暦年で+11の変化となります)。<br>■ パーセンテージポイント (2つの異なる時点におけるサイバーリスクレベルの差のパーセンテージ。上記の例でいえば、リスク・レベルが0〜100の尺度で測定されていると仮定した場合、その変化は15.3%となります)。<br>■ 折れ線グラフ (様々な時点におけるサイバーリスクのレベルを示し、一般的にレベルが上がっているか下がっているか等の傾向を示します)。<br><br>エクスポージャー評価を行う一部の製品やプラットフォームでは、このデータは自動的にダッシュボードに表示されます。 |

| セキュリティ投資利益率 (ROSI) | |
|---|---|
| 説明 | 繰り返しになりますが、企業の経営者は物事をビジネス用語で説明することを求める傾向にあります。その点、投資利益率 (ROI) ほどはっきりとしたビジネス指標はないでしょう。<br><br>セキュリティ投資利益率（ROSI）はROIのセキュリティチームバージョンであり、エクスポージャー管理レポートのツールボックスの中で最も強力なツールといえるかもしれません。エクスポージャー管理の取り組みをドルという金額で表すことで、セキュリティチームは、個々の投資の価値だけでなく、一定期間におけるすべてのエクスポージャーの管理の取り組みの累積価値も報告することができます。 |
| 測定方法 | セキュリティ投資利益率（ROSI）は、投資コストに対する投資の財務的利益を測定する従来のROIとは異なり、投資のおかげで回避された財務的損失の予測をそのコストに対して測定します。それらの予測損失は、組織の過去のデータと業界調査を組み合わせ、合理的な精度で見積もることができます。<br><br>従来のROIは、現在の価値から投資にかかったコストを差し引き、そのコストで割ってから100を掛けてパーセンテージを算出して得られます。この方程式を一つ修正することにより、つまり、投資の現在価値を、投資により回避される損失の予測値に変更することによって、組織は、セキュリティ投資利益率 (ROSI) を計算し、エクスポージャー管理投資の財務的影響を測定することができます。 |

## Ivantiについて

Ivantiは、ITおよびセキュリティ向けに包括的なクラウドベースプラットフォームを提供するエンタープライズソフトウェア企業です。Ivantiは、顧客のニーズに合わせてスケーラブルなソフトウェアソリューションを提供し、ITとセキュリティが運用効率を改善し、コストを削減しながら、セキュリティリスクをプロアクティブに低減できるよう支援します。Ivanti Neuronsプラットフォームはクラウドネイティブで、一貫した可視性、スケーラビリティ、セキュアなソリューション提供を実現するための、統一されたサービスとツールの基盤として設計されています。Ivantiのエンドツーエンドのソリューションは、Fortune 100社のうち85社を含む34,000以上の顧客によって採用されています。Ivantiは、すべての視点が聞き入られ、尊重され、評価される環境づくりに尽力し、顧客、パートナー、従業員そしてよりサステイナブルな未来を実現するために取り組んでいます。詳細については、ivanti.com/jaや@GoIvantiをフォローしてください。

ivanti

詳細については
ivanti.com/ja
をご覧ください。