ivanti

# サイバーリスクを客観的に評価する

## データ主導型リスク評価ガイド

目次



## この e-book について

エクスポージャー管理では、会社全体のリスク許容度に照らし合わせてセキュリティリスクを捉え、セキュリティ責任者が、経営幹部の取り組みを実現するような情報に基づいて提案を行えるようにします。

この e-book は、エクスポージャー管理の重要な要素である**データに基づくリスク評価**を行うためのツールとなります。

リスク評価を実施し、その結果を提示する簡単な方法をご紹介しましょう。ここではリスクを減らすことを選択した場合と、リスクを受け入れることを選択した場合の、ビジネスクリティカルな資産への直接的な影響を説明します。

これは、リスク評価のプロセスを様々なシナリオに適用するための手引きです。評価と緩和策を提示する際に役立つ事例とヒントを数多く提供し、リスクとエクスポージャーについて、他のビジネスリーダーたちと共通の認識を持つことができるようにします。

# はじめに

あなたは、会社がサイバー攻撃に遭うリスク、繰り返し問題を引き起こす「亀裂」、会社のセキュリティ体制を強化する取り組みについて認識しています。

業務内容を問わず、あなたの同僚はビジネスの目標とその達成のために負うべきリスクを計算し、気にかけています。

“双方が望んでいることは結局同じことなのですが、リスクについて共通の理解を持ってなければ、話は かみ合いません。”

同じ見解を得るには、詳細で客観的かつ定量的なサイバーリスク評価が必要です。

リスク評価とその結果は、他の責任者にも理解できる言葉で結論が示されます。
これによって、重要なセキュリティ対策に対する支持を集めることが可能になります。

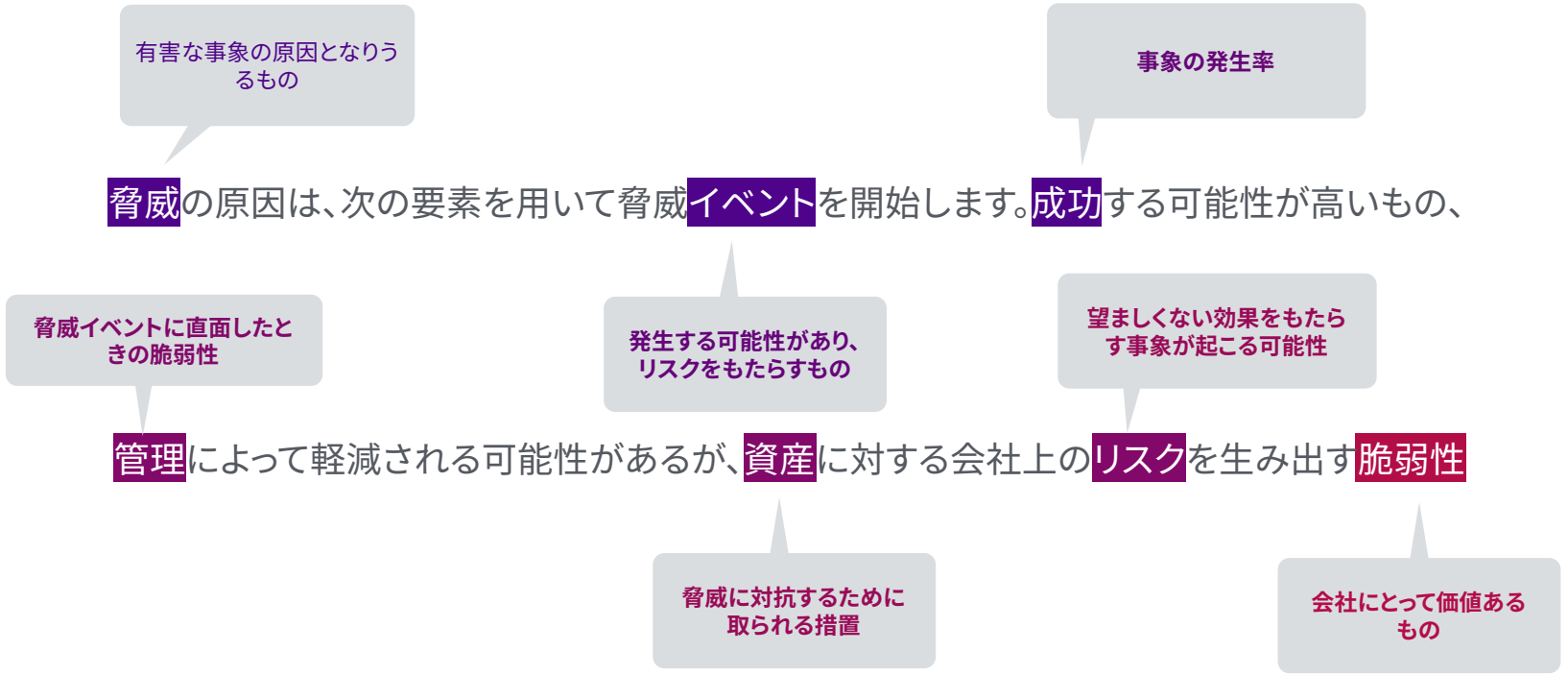
また、軽減すべきリスクや受け入れるべきリスクは、あなたが考えているものとは異なるかもしれません。

セキュリティに関わる事象を、それがまだ発生していないうちにどのように数字で表すのでしょうか？ この点を掘り下げることにしましょう。

# リスク評価

## 主要な用語と一般的なリスクモデル

一般的なリスクモデルは、次のようなものです。




現実の事象もこうしたモデルに基づいています。例を挙げましょう。

ALPHV は、**ランサムウェア攻撃**を行うグループです。攻撃は**成功**し、米国、ヨーロッパ、アジア太平洋地域の複数の企業で、**アクセス制御やユーザートレーニングの脆弱性**を悪用し、**数日間**の業務停止を引き起こしました。いくつかのケースでは、頻繁に**バックアップ**を行っていなかったために膨大なバックログが発生し、企業やその**情報**が侵害されて一般に公開されたおそれがあり、**金銭的リスク、レピュテーションリスク、法的リスク**が発生しました。

# リスク評価のステップ

リスク評価には 5 つの簡単なステップからなります。このセクションではこれらについて説明します。

1. リスク評価の対象となる資産を特定する
2. これらの資産に価値を付与する
3. 脆弱性と脅威を特定する
4. リスク（可能性 x 影響）を計算する
5. 費用利益分析を実施する

これによって、リスク評価から得られたデータに基づいたリスク対応策を提示することが可能になります。
リスク対応には4つの可能性があります（以下で詳述します）。

**回避**
危険な活動を停止させるか、脆弱なシステムを完全にシャットダウンすることによってリスクを回避します。

**受け入れ**
リスクと共存することを決定し、アクションを起こしません。

**移転**
通常、保険会社と契約して金銭的エクスポージャーをカバーします。

**軽減**
追加的な安全策を講じることでリスクを軽減します。

# ステップ 1
# 資産の特定

## 当てはまるものは？

資産は**有形のもの**（建物、人、設備）と**無形のもの**（情報、特許、ブランド、ライセンス、顧客リスト、研究開発）に分類することができます。

資産は所有権によって分類することもできます。高いレベルでは、事業資産（現金、土地、在庫、工場、従業員の専門的技能）、またはIT 資産（ソフトウェア、サーバー、ファイアウォール、ノートパソコン、監視ツール）がありますが、IT 資産は、単にそれ自体のために存在するのではなく、ビジネス資産を保護するために存在しています。あなたの会社では、サーバー（有形 IT 資産）上に営業秘密（無形営業資産）を保有しているかもしれません。この 1 台のサーバーに適用されるセキュリティ管理が、会社の存亡を左右するかもしれないのです。

“あなたがデータ損失防止に関心を持っているとしましょう。対象範囲内にあるもの（業務用ラップトップ、BYOD、電話機、プリンター）を評価してその数を決定する必要し、理想的には、最新のインベントリにそれらの数を記載します。こうすることで、なぜエンドポイント数に応じたセキュリティ確保が、顧客データ、クレジットカード情報、従業員の給与といった機密情報に関わるビジネス資産のセキュリティ確保に等しいのかを説明することができます。”

このような情報が社外に流出するリスクを減らしたい。しかし、そのリスクを数値化すれば、適切な緩和策を考え出す（そして支持を得る）ための下地づくりになります。

## 「クラウンジュエル（王冠の宝石）」

**クラウンジュエルとは、最も価値ある企業資産であり、あらゆる資産の中で、その漏洩はビジネスに最大の影響を与えるものを指します。**

“あなたはおそらく、情報をクラウンジュエルと考えているでしょう。そう考えるのはもっともなことですが、他のリーダーたちの考える クラウンジュエルの定義は少し違っているかもしれません。それは、特定の業務プロセスやシステムであるかもしれませんん。ただしそこには、情報がなければその価値はゼロになってしまうという考えが欠落しています。情報はシステムの何倍も長続きするものであり、実際、保護を必要とするものです”

業務プロセスと情報システムは一体であり、結局は同じ資産を指していることになるのですが、インパクトを与えるためには、リスク分析は非常に具体的である必要があります。

会社のクラウンジュエルのひとつが顧客管理（CRM）
システムと処理される顧客情報であると想定してみましょう。
以下の2つの文の違いを見てみましょう。

「悪意のあるアクターが当社のドメインネームシステム（DNS）を詐称することによって、情報を失うことになります」

「昨年、同業他社の 45%にデータ侵害が発生し、Salesforceが処理した顧客の個人情報と取引が公開されるおそれがあります。その結果、推定45億ドルの罰金、訴訟により延々と発生する諸経費、回復に5〜10年かかるレピュテーションリスクが生じると見られています。」

後者の文の方が明らかに説得力があります。リスク評価を行うことで、このレベルまで具体性をもたせることができるようになります。

# ステップ 2
# 資産価値の決定

有形/無形の区別なく、資産の価値は明確でなければなりません。資産価値を割り当てるのは、必ずしもセキュリティチームではありません。その資産に対するセーフガードの導入について業務上の意思決定を行う際には、最重要ではなくとも、重要な考慮事項となります。

資産の価値を決定するには、以下を考慮しなければなりません。

- 資産の取得または開発に要した費用
- 資産を維持・保護するための費用
- 所有者やユーザーにとっての資産の価値
- 敵対者にとっての資産の価値
- 他人がその資産に支払おうとする価格
- 資産を紛失した場合の交換費用
- その資産が使用できなくなった場合に影響を受ける営業および生産活動
- 資産が侵害された場合の責任問題
- 会社における資産の有用性と役割

各会社の資産には所有者がいるはずです。資産価値は、その所有者が（場合によってはセキュリティチームの指導の下に）決定するべきです。

**ここで、重要な問題があります。その資産を保護しない場合、会社が負担する費用はどのくらいでしょうか？**
**この疑問に対する答えは、ビジネスインパクト分析（BIA）から始まります。**

## 理想的なビジネスインパクト分析

ビジネスインパクト分析（BIA）は通常、事業継続計画のサイクルにおける1段階に位置づけられ、テクノロジーとビジネスが一体となって活動の重要性とそれを支える資産について話し合うための重要な作業となっています。

「このプロセスが機能しなくなったらいったい何が起こるのか」と問うことで、プロセスの所有者や責任者は、財務的な影響も含めて起こりうる影響について考察することになります。これによって、リスク評価に使用できる現実に即した数値を得ることができるのです。

理想的なビジネスインパクト分析（BIA）には、以下が含まれます。

- プロセスの目的、所有者、インプットとアウトプット
- 中断の影響（金銭的影響、業務上の影響、法的／規制的影響、評判上の影響を測定）
- 最悪のシナリオと中断の回数（ピーク時など）
- 事業活動の目標復旧時間（RTO）、目標復旧時点（RPO）、最大耐久停止時間（MTD）
- このプロセスの実施/サポートに必要なリソース：他の部署、情報、人、インフラ、ベンダーのロケーション、IT 資産 これらは、プロセスの目標復旧時間（RTO）と目標復旧時点（RPO）を踏まえて、障害発生時の復旧の優先順位が設定されます。

ヒント

テンプレートは数多くあれど、万能のテンプレートはありません。以下の簡易テンプレート（編集可能なスライドをダウンロード）を出発点としてご利用ください。

事業継続性と情報セキュリティは、別の部署に属していることがあります。この場合、一貫したアプローチでリスク管理を行うために、情報を共有しておかなければなりません。

ビジネスインパクト分析（BIA）に基づいた資産の重要度割り当て

ビジネスインパクト分析（BIA）は、重要システムのうち、どれが会社の存続に必要かを特定し、許容できる停止時間を見積もります。会社が許容できる停止時間は、最大耐久停止時間（MTD）と呼ばれます。

最大耐久停止時間（MTD）のいくつかをご紹介します。

- **非重要：**30日間
- **通常：**7日間
- **重要：**72時間
- **緊急：**24時間
- **クリティカル：**数分～数時間

各業務機能と資産は、企業がそれなしで存続できる時間数に応じてこれらのカテゴリーのいずれかに分類される必要があります。これらの見積もりは、会社がこれらのリソースを活用できるようにするためにどのような管理が必要かを判断するのに役立ちます。

例えば、ウェブサーバーが4時間使えなくなると会社にとって12万ドルの損失となる場合、ウェブサーバーはクリティカルであり、ウェブサーバーを冗長化することを検討する必要があります。

これに反して、建物の稼働率を報告するツールが3週間使用できなくなり、そのために会社が負担するコストが 500ドル未満である場合、そのツールは**必要不可欠ではない**と判断して差し支えなく、ベンダーのサービスレベル契約（SLA）に頼るか、問題解決のための最善の努力で対処することができます。

T ヒント ip

プロセスおよびシステムの目標復旧時間（RTO）は、財務的損失値と相関性があり、定量的リスク分析のパラメータとして使用することができます。このような情報は、既存のビジネスインパクト分析（BIA）や災害復旧計画ですでに把握されている可能性があります。これらの情報がない場合は、範囲を絞って分析を行えば得られます。

ビジネスインパクト分析（BIA）を簡略化すると以下のようになります。

| プロセス名 | プロセスの中断 | 財務への影響 | 法的影響 | 評判への影響 |
|---|---|---|---|---|
| 当日支払い | 4時間未満 | $-$$$ | 該当なし | 該当なし |
| | 4時間～8時間 | $$$-$$$ | 該当なし | 低い |
| | 2～5営業日 | $$$-$$$$ | 中程度 | 中程度 |
| | 1～2週間 | $$$-$$$$ | 中程度 | 高い |
| | 2～4週間 | $$$$-$$$$$$ | 高い | クリティカル |
| 正当化 | ■ 評判と社会的信用の失墜…<br>■ 競争上の優位性の喪失…<br>■ 営業費用の増加…<br>■ 契約違反…<br>■ 法律および規制要件への違反…<br>■ 所得の遅延損害金…<br>■ 減収…<br>■ 生産性の低下<br>■ その他… | | | |
| 必要なリソース | スタッフ：4名以上（1週目）、6名以上（1週間経過後）<br>決済システム：利用可能でなければならず、手作業での回避策は不可<br>トークン決済：最低限2種類のトークン<br>ITシステム：決済システム（サーバー＋データベース）、インターネット、手形交換所への接続、電子メールのロケーション：初日は自宅でも可能だが、その後オフィススペースが必要となる<br>事務用品：プリンター | | | |

ヒント

編集可能なこのビジネスインパクト分析（BIA）テンプレートをダウンロードしてください。

## ビジネスインパクト分析（BIA）とリスク評価の関係

ビジネスインパクト分析（BIA）は、事業継続性に焦点を当てたリスク評価の一部となっています。可能性は低いが重要なシナリオが事業活動に与える影響に着目して、事業の優先順位を明確に示します。その結果、会社を支える情報システムを含め、会社のクラウンジュエルを決定することができます。

リスク評価は通常、式「リスク = 脅威 x **影響 x 確率」で表すことができます**。ただし、ビジネスインパクト分析（BIA）では、この式に時間という概念が加えられています。つまり、重要な業務プロセスを最も急速に混乱させる可能性のある脅威を対象としているのです。このためビジネスインパクト分析（BIA）は、情報セキュリティ3要素（CIA）、すなわち**機密性、完全性、可用性**のうち、**可用性**を保護するコントロールを決定するための重要な情報となります。

**“ランサムウェア攻撃**は、データを利用不可能にするものであり、まさに継続性のシナリオの 1 つに該当します。しかし、ただし、すべてのセキュリティリスクが **可用性**の要素に影響を与えるわけではありません。”

**データ侵害**（ランサムウェアの使用なしに流出したもの）では、システムとプロセスは通常どおり機能し、データが利用可能なままの場合があります。むしろ、データが利用可能になりすぎて、情報セキュリティ3要素（CIA）のうち**機密性**が侵害される可能性もあります。このシナリオでは、侵害されたデータを操作するプロセスが突然停止することはありません。

会社に企業秘密があるなら、それが会社のクラウンジュエルの 1 つである可能性が高く、それが悪意をもって変更されたり（**インテグリティ**構成要素）、一般に公開されたりしても、ビジネスインパクト分析（BIA）では把握されないかもしれないものの 1 例となっています。

このため、リスク評価にはさまざまな角度から取り組む必要があります。ビジネスインパクト分析（BIA）はその出発点として最適なのです。

## 情報セキュリティ3要素（CIA）のレーティング評価

ビジネスインパクト分析（BIA）を使用して、どの資産が時間的制約を受けるかを決定しました。**情報セキュリティ3要素（CIA）のレーティング評価**は、この決定事項に数値という側面を加えます。

情報通信技術に関する国際団体ISACAが提案する資産の評価と分類の方法では、資産の価値をその感応度に応じて重み付けすることが可能です。

情報セキュリティ3要素（CIA）の構成要素それぞれに、1（低）、2（中）、3（高）の値を付与します。情報セキュリティ3要素（CIA）のレーティング評価は、これら3つの値（C＋I＋A）を合計してスコア（3〜9）を割り出します。

情報セキュリティ3要素（CIA）のレーティングを企業資産のそれぞれに適用してスコアが付与され、これがリスクベースの管理実施に直結します。資産のレーティングのスコアが C3-I2-A2(7) と C1-I1-A2(4) とでは、異なる管理を必要とします。

いずれの方法も、資産に含まれる情報に対して責任を持つビジネスオーナーと協力して行うものであり、資産価値に対する共通の認識を固め、リスク意識とビジネスが志向する方向性との断絶を削減する機会となります。

ヒント

情報セキュリティ3要素（CIA）のレーティング評価は、構成項目や仮想デスクトップ（VDI）ごとに行う必要はありません。資産は、会社にとって合理的な方法（その会社が持つ共通の事業目標など）に従ってグループ化されるべきなのです。

会社としてリスク許容度を公表しているのであれば、それに基づいて、情報セキュリティ3要素（CIA）のレーティング評価で割り当てる数値について他の業務責任者と認識を一致させておきましょう。（リスク許容度を公表していない場合は、編集可能なこのテンプレートを出発点としましょう）

# ステップ 3
# 脅威モデリングと脆弱性評価

リスク分析の次のステップは、優先度の高い脅威と脆弱性を決定することです。それらが何であるかについてすでに考えをお持ちかもしれませんが、そうした仮定を検証することで、リスク評価の信頼性はさらに高まります。

## 脅威モデリング

脅威モデリングは、脅威インテリジェンスに基づいたものでなければなりません。つまり、グローバルな脅威の状況、同じ分野の他の会社に向けられた脅威の種類、自社事業の特殊性に基づいたものでなければならないのです。これによって、発生する可能性の低い脅威に労力を割くことなく、発生する可能性の高い脅威に労力を集中させることができます。

脅威モデリングを行うためには、数多くの方法があります。
**一般的な方法は 2 つあります。**

**アタックツリー：**
脅威の原因となるものには、目的に到達するために複数の手段が備わっています。アタックツリーは、脅威のさまざまな経路を枝と葉のノード（結節）に見立てた図を作成するとともに、脅威アクターが目的を達成するために満たさなければならない条件も示されます。経路のノード（結節）それぞれが持つ脆弱性が評価されます。

**低減分析：**
このアプローチは、アタックツリーをベースに、ツリーの末端のリーフ（葉）ノード間の共通点を見つけます。これにより、複数の脆弱性のそれぞれを緩和しうる管理策を特定することができます。

ヒント

脅威モデリング演習において表面化した攻撃事例は、リスク評価と軽減策の推奨事項に盛り込むことで、セキュリティ部門以外の責任者が脅威を具体的に把握するのに役立ちます。

## 脆弱性評価

脅威モデリングは、潜在的な脅威から始めて会社に侵入する方法を特定するという外側から内側へと向かうアプローチです。これに対して、脆弱性評価は内側から外側へと向かうアプローチで、脅威アクターによって悪用される可能性のある攻撃対象領域の弱点を見つけます。

“エクスポージャー管理の中核をなす原則は、攻撃対象領域を広く定義することです。攻撃対象領域における脆弱性を評価する際には、情報やシステムの脆弱性よりも広い範囲を対象とすることを忘れてはなりません。これには、プロセス（パッチ適用の遅れや不適切な適用など）、人（ソーシャルエンジニアリングのリスクの可能性、脆弱なパスワードの使用など）が含まれます”

ネットワーク脆弱性スキャナー、アプリケーションセキュリティテスト、外部攻撃対象領域管理などのソフトウェアは、潜在的な脆弱性に関する貴重な情報を表面化させます。その他の情報源として、監査報告書、リスク登録簿、コントロールテスト、侵入テスト（ペンテスト）の結果、インシデント報告書、ポリシー調査、企業文化を単に観察するなどもあるでしょう。

“システムの脆弱性に関しては、ベンダーの脆弱性評価や共通脆弱性評価システム（CVSS）などのスコアシステムが、優先度の高い脆弱性を特定するための第一歩となります。しかし、リストをさらに絞り込むには（そして、会社にとってより深刻である可能性のある低スコアの脆弱性を表面化させるには）、さらに 2 つのフィルターを重ねる必要があります。脅威のコンテキストとリスクのコンテキストです。これらはいずれも、すでに基礎が築かれていることでしょう。”

**脅威のコンテキストは、脅威の全体的な状況のことです。**
**この脆弱性は積極的に悪用されていますか？**
脆弱性が「クリティカル（Critical）」と評価されていても、それが積極的に悪用されなければ、重大性は低下します。脅威モデリング演習は、すでにあなたの会社のためにこうした調査を開始しています。

**リスクコンテクストはあなたの会社に関するものです。**
**この脆弱性が悪用された場合、会社にとってどのような影響があるでしょうか？**
**レーティング評価では脆弱性が低くとも、それが悪用された場合に重要なシステムがオフラインになるのであれば、より注意を払う価値があります。影響評価のおかげで、どの資産、システム、プロセスが侵害・中断された場合に会社に最も大きな影響を及ぼすかはすでに把握されていることでしょう。**

ヒント

このチェックリストをダウンロードして、攻撃対象領域のあらゆる側面が配慮されているか確認しましょう。

# ステップ 4
# リスクの決定

ここまで、資産価値（AV）、脅威、脆弱性について見てきました。ここからはいよいよ、脅威の可能性と影響を検討し、リスクを計算することにしましょう。リスク測定には2つのアプローチがあります。**定量的アプローチ**と**定性的アプローチ**です。

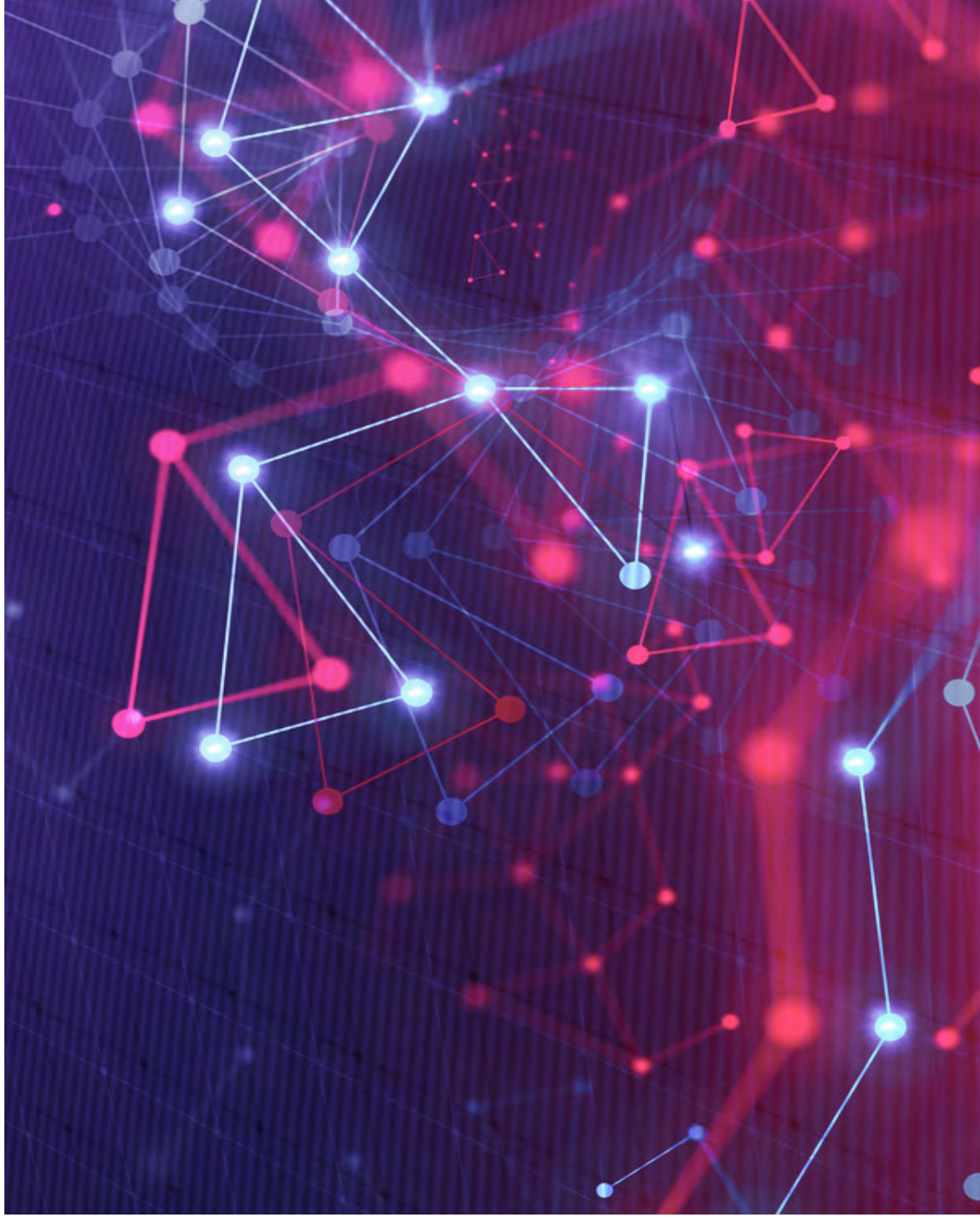
**定量的リスク分析では、分析に含まれる構成要素に金銭的価値を割り当てるために数式を使用します。**

**定性的なリスク分析では、値と評価が割り当てられます（低/中/高、1〜10、ストップランプなど）。**

あなたの会社にとって、いずれの方法が最適かを判断してください。本書では、主に定量的リスク分析に焦点を当てます。

ヒント

自動化されたリスク分析ツールを使用すると、手作業でのリスク評価の時間を短縮し、さまざまなセキュリティ対策の効果を計算することが可能になります。



## 定量的リスク分析

CEOや取締役会は、可能な限り常に金銭的、定量的な観点から実施された分析を望むことでしょう。サイバー攻撃のリスクが高いことの他にも、知っておくべきことがあります。重要なシステム上のデータの 15%を暗号化するランサムウェア攻撃が成功した場合、その企業は競争上の優位性を失うだけでなく、重要な業務が最大 4 日間中断され、1 日あたり 22万5,000ドルもの損害を被るリスクがあるということも覚えておきましょう。

リスク定量化のために広く受け入れられている式は、実は非常に単純なものです。

**年間損失予測値（ALE）= 単一損失予測値（SLE）× 年間発生率（ARO）です。ここでは、単一損失予測値（SLE）= 資産価値（AV）× エクスポージャー係数（EF）です。**

**エクスポージャー係数（EF）**は、1 つの脅威が特定の資産に与えうる損失の割合を表します。例えば、漏洩する可能性がある企業秘密を持っている場合、競争上の優位性の損失は資産価値の 10%に相当する可能性があります。企業秘密の資産価値（AV）が 400万ドルであると仮定すると、簡単な式で単一損失予測値（SLE）を算出することができます。

**AV（400万ドル）× EF（10%）= SLE（40万ドル）**

年間発生率（ARO）は、脅威が1年間で発生する推定頻度です。同じ例を用いて、あなたの会社に類する会社で起こった類似の事象を調べれば、企業秘密の漏洩は20年ごとに発生すると見積もることも可能です。つまり、年間発生率（ARO）が 0.05（1年／20年）となった場合のことです。ここから年間損失予測値（ALE）を割り出すことができます。

**単一損失予測値（SLE、40万ドル）× 年間発生率（ARO、0.05）= 年間損失予測値（ALE、2万ドル）**

**年間損失予測値（ALE）**の結果は、会社がリスクを軽減するために何らかの管理を実施すべきか、それとも単にリスクを受け入れるべきかを決定するのに役立ちます。この例では、年間 2万ドル以下のコストで管理することを合理的に正当化できます。

定量的リスク分析の結果は、リスク軽減のためのビジネスケースを構築したり、コストが年間損失予測値（ALE）を超える軽減戦略を不適格とする際に、重要な戦略ツールとなります。

## 定量的リスク分析結果の例

| 資産 | 脅威 | 単一損失予測値（SLE） | 年間発生率（ARO） | 年間損失予測値（ALE） |
|---|---|---|---|---|
| 企業秘密 | 漏洩した | 400万ドル | 0.05 | 2万ドル |
| ファイルサーバー | 破損した | 13,500ドル | 0.1 | 1,350ドル |
| 設備 | 火災 | 25万ドル | 0.1 | 25,000ドル |
| データ | マルウェア | 7,500ドル | 1 | 7,500ドル |
| お客様のクレジットカード番号 | 公開された | 30万ドル | 4 | 120万ドル |

## 別の例を見てみましょう。

あなたは最近、急成長中の AI スタートアップ企業の IT/セキュリティ責任者に採用されました。あなたは、フィッシング攻撃が成功した場合の緊急リスクについて熟知しています。最悪のシナリオでは、あなたが開発している独自のアルゴリズムが脅威によって流出し、競争上の優位性が損なわれ、その結果、あなたの評価が下がる可能性があります。フィッシング・キャンペーンの実施を始めたところ、常に 10%の従業員がリンクをクリックしたり添付ファイルを開いたりしているという結果が出ました。

こうしたリスクを軽減するために、フィッシング対策ツールや情報セキュリティトレーニング・キャンペーンのような対策に資金を充当し、従業員を啓発する価値があることを、エンジニアリングの進歩をアピールすることに注力し続ける CEO や投資家に説明しなければなりません。ここで、定量的リスク評価の登場です。

**単一損失予測値（SLE）を決定する：**

2024年 IBM データ侵害のコストに関する調査レポートによると、フィッシング攻撃は最初の脅威としては2番目にコストが高く（悪意のある内部関係者に次いで、ビジネスメールの漏洩と同率で2番目）、その平均コストは2024年には488万ドルに達しています。これは単一損失予測値（SLE）の平均であり、あなたは自分の会社に合わせて変数エクスポージャー係数（EF）および資産価値（AV）を調整したいと考えることでしょう。

この例で、あなたの勤務先がはるかに小規模な企業であるという前提で単一損失予測値（SLE）を調整してみましょう。**エクスポージャー係数（EF）**、つまり漏洩するデータの割合は変わらないと思われますが、**資産価値（AV）**はずっと小さくなります。例えば 10%の規模になるとすると、単一損失予測値（SLE）は **488,000 ドル**となります。

**年間発生率（ARO）を決定する：**

調査の過程であなたは、業界で同等規模の企業が毎週のようにフィッシング攻撃を受けており、その数は年間 52 件に上るということを知りました。これらの攻撃が 10%の確率で成功した場合（あなたが実行してきたフィッシング キャンペーンと合致します）、**年間発生率（ARO）**は5.2となります。

**年間損失予測値（ALE）を決定する：**

**単一損失予測値（SLE、48万8,000ドル）× 年間発生率（ARO、5.2）= 年間損失予測値（ALE、250万ドル）**

（おおよその数字）

率直に言って、この年間損失予測値（ALE）のリスクを受け入れることは賢明な選択肢ではないように思われます。積極的なリスク軽減戦略のために強力なビジネスケースを作成するのがよさそうです。

## 定性的リスク分析

定性的リスク分析では、リスクを「非常に低い」から「非常に高い」まで、あるいは 1〜10 のように段階的に記述します。
こうした形式の定性的リスクマトリックス、あるいはそれに類するものを目にすることはよくあるかもしれません。

| | | 発生の可能性 | | | | |
|---|---|---|---|---|---|---|
| | | 1 稀にしかない | 2 可能性が低い | 3 可能である | 3 可能である | 5 ほぼ確実である |
| 影響 | 5 非常に高い | 5 | 10 | 15 | 20 | 25 |
| | 4 高い | 4 | 8 | 12 | 16 | 20 |
| | 3 中程度 | 3 | 6 | 9 | 12 | 15 |
| | 2 低い | 2 | 2 | 6 | 8 | 10 |
| | 1 非常に低い | 1 | 2 | 3 | 4 | 5 |

| リスク判例 | | | | |
|---|---|---|---|---|
| | 低い | 中程度 | 中程度 | 極めて高い |

先ほどのフィッシングの例に戻りましょう。あなたの定性的リスク分析では、このシナリオを「可能性が高い」と見なしています。中小企業であるため、知名度の高い大企業のように頻繁に狙われることはなくとも、フィッシングが最も一般的な脅威ベクトルの 1 つであることはご存知でしょう。あなたは、影響を中程度と判断しています。最悪のシナリオでは、あなたの会社の評判が極端に下がり、その結果、あなたの評価も下がります。より現実的なシナリオであれば、このような高いエクスポージャーは起こり得ません。分析結果は高リスクです。

過去の事象に基づいて**発生する可能性**の上限と下限を決めて幅を持たせることで、この演習の精度と再現性を高めることができます。現実味のある範囲内で両極端でないシナリオとはどのようなものでしょうか？ そして、**影響の度合い**の各カテゴリーに金銭的価値を与えます。

定量的リスク評価にも定性的リスク評価にも、それぞれ長所と短所があります。両者を組み合わせることも可能であり、規制リスクやレピュテーションリスクなど、財務リスクや運用リスクほど簡単に定量化できないものの非常に深刻なリスクを検討する機会にもなります。

**財務リスク以外のリスクに推定間接コストを割り当てたこのような表が出発点となる場合もあります。**

| 影響 | 金銭的 | 規制 | 評判 |
|---|---|---|---|
| **非常に高い** | 1,000万ドル未満 | 刑事告訴/事件、ライセンス取り消しの可能性、経営陣の個人的責任 | 信頼が完全に失われ、地元/世界規模で否定的な報道が続き、ブランドイメージが損なわれる |
| **高い** | 100万～1,000万ドル | 多額の罰金、訴訟および検察との和解、営業許可が制限される可能性 | 信頼が大きく損なわれ、完全に回復することは不可能である。否定的な報道が増加し、国際レベルにまで拡大している |
| **中程度** | 10万～100万ドル | 公的な警告および罰金、是正のための即時措置を求められる | 信頼は低下し、回復には相当のコストがかかる。否定的な報道が増える |
| **低い** | 1万ドル～10万ドル | 規制当局/監督当局からの非公開の警告 | 信頼は失われたが、時間とともに回復可能。全国的な報道があり、中立的な報道も一部ある |
| **非常に低い** | 1万ドル未満 | 規制当局や監督当局からの注意がない、あるいはほとんどない | 信頼に疑問符がつくが、短期間で回復可能。報道は地元に限定され、一時的なものである |

いずれのアプローチを採用するにしても、リスク評価には不確実性というもう 1 つの課題が待ち受けています。

定量的リスク評価も定性的リスク評価も完全な手法ではありません。数値的な評価も含め、いずれも不確実性と密接に結びついた主観レベルの評価が含まれています。

不確実性とは、ある推定に対して、どの程度確信が持てないかの度合いを指します。リスク評価を実施する際に不確実性の程度を把握することは重要です。不確実性は、結果の数字に対する信頼のレベルを示すものだからです。

純粋に客観的な分析を達成するのは困難（あるいは不可能）です。データを完全に確認するのに十分な過去の事象や調査が存在しない場合、より多くのデータを収集する時間がない場合、単にブラックスワン的な出来事を予測できない場合には、不確実性が生じます。

不確実性の領域を具体的にリストアップすると、信頼度を定義するのに役立ちます。また、不確実性を軽減できる領域を特定できるようになります。

不確実性の例として、個人デバイスの使用を認める BYOD（Bring-Your-Own-Device）ポリシーの導入を挙げましょう。

防衛産業など、セキュリティリスクの許容度が極めて低い業界で働く場合、BYOD が認められない可能性が高くなります。しかし、従業員が BYOD を要求するようになり、責任者が従業員の仕事への満足度を高めるためにこの考えに前向きに考えているとすると、リスクの増加に見合うかどうか、そのリスクを減らすためにどのような管理が必要かを見極める必要があります。

では、把握していないのは何でしょうか？

- 政府機関や請負業者の場合、将来の規制変更は貴社の方針に影響しますか？
- この方針の恩恵を享受する従業員は何人いますか？ 彼らはどのような職務を担っていますか？
- IT担当者がデバイスの登録やサポートに要する時間数は？

これらの質問に明確に答えることはできないかもしれません。けれども、不確実性を低減するためにできることはあります。たとえば、BYOD ポリシーを緩和した場合の受け入れ状況をよりよく予測するために、従業員にアンケートを行うことなどです。

# ステップ 5
# 費用便益分析

さて、どの程度のリスクに直面しているかの判断が行われ、軽減策の検討に取り掛かることになります。
ここではセキュリティ対策に焦点を当てていますが、ソフトウェアの脆弱性にパッチを適用したり、設定ミスを修正するなど、
あらゆる種類の緩和策にも同じ原則が適用されます。

## コスト管理

リスク対応について十分な情報に基づいた提案をするためには、重要な質問に答えなければなりません。このリスクを軽減するために、実際のコスト（隠れたコストも含む）はどのくらいかかるのでしょうか？

リスク対応について十分な情報に基づいた提案をするためには、重要な質問に答えなければなりません。このリスクを軽減するために、実際のコスト（隠れたコストも含む）はどのくらいかかるのでしょうか？

たとえその管理が金銭を必要としないものであっても、すべての緩和にはコストがかかることを忘れてはなりません。例えば、ロールベースのアクセス制御を更新する間、サーバーをオフラインにすると、新しいセキュリティツールを導入するのと同じく業務コストとなります。両者には、予算項目として計上されるか、支出項目として思い出さない限りは隠れたコストとなるかの違いしかありません。

一般的なルールとして、資産のセキュリティを確保するコストは、その資産価値よりも低くなければなりません。そうでなければ、緩和策は意味をなさないのです。

管理のコストを計算する（そして隠れたコストも明示的に考慮する）には、以下を考慮する必要があります。

- 製品コスト
- 設計および計画費用
- ダウンタイムのコストを含む導入コスト
- 環境の修正
- 他の対策との互換性
- メンテナンスの必要性
- テスト要件
- 修理・交換・更新費用
- 運営費およびサポート費（スタッフトレーニングを含む）
- 生産性への影響
- サブスクリプション費用
- 監視とアラート対応のための余剰の人時コスト

## 管理の価値

管理の価値の概念を表す式：

**（管理実施前の年間損失予測値（ALE））-（管理実施後のALE）-（年間管理コスト）= 管理の価値**

**フィッシング対策ツールとインフォセック・トレーニングキャンペーンを組み合わせて、フ**
**フィッシング攻撃**によるデータ流出に対抗することを先ほどの例で考えてみましょう。

管理の価値を決めるには、まず費用を計算しなければならなりません。
直接費と間接費をすべて考慮しましょう。

| フィッシング対策ツール | トレーニングキャンペーン |
|---|---|
| デプロイメント（単発） | デプロイメント（単発） |
| インテグレーション | インテグレーション |
| ライセンス/サブスクリプション料 | ライセンス/サブスクリプション料 |
| ユーザーのトレーニング | キャンペーン用資料 |
| メンテナンスおよびサポート | メンテナンスおよびサポート |
| 生産性の低下 | 生産性の損失（従業員がトレーニングに参加する時間） |
| **見積もり：7万ドル/年** | **見積もり：2万ドル/年** |

最初の年間損失予測値（ALE）：

**単一損失予測値（SLE、48万8,000ドル）× 年間発生率（ARO、5.2）= 年間損失予測値（ALE、250万ドル）**

（おおよその数字）

**新しい年間損失予測値（ALE）を決定するには、管理導入後の年間発生率（ARO）の減少を考慮しなければなりません。**

当初の年間発生率（ARO）では、あなたが定期的に実施していたキャンペーンに基づいて、毎週のように試みられるフィッシングが 10%の割合で成功すると想定していました。試行回数は変わりません。両方のベンダーを調査した結果、ソリューションを組み合わせることにより、成功率が 2%まで下がると見積もられたとしましょう。これにより、年間発生率（ARO）は当初の計算の5分の1、つまり 1.04 まで引き下げられます。

**これで新しい年間損失予測値（ALE）が得られました。**

**単一損失予測値（SLE、48万8,000ドル）x 新しい年間発生率（ARO、1.04）= 年間損失予測値（ALE、50万7,500ドル）**

（おおよその数字）

**ここで、管理の価値を算出することができます。**

**初期 ALE（250万ドル）- 新しい ALE（50万7,500ドル）- 年間管理コスト（9万ドル）= 管理の価値（190万ドル）**

（おおよその数字）

### 総合リスクと残存リスクの比較

セキュリティ管理を導入する理由は、会社（全体）の包括的なリスクを許容可能なレベルまで低減するためです。けれども、100%安全なシステムや環境は存在せず、対処すべきリスクは常に残されています。

管理を実施した後の年間損失予測値（ALE）は残存 ALEとも呼ばれ、残存リスクを表すことができます。

**定量的残留ALE = 残留ARO × 残留SLE**

この例では、単一損失予測値（SLE）は管理を実施した後も変化がありませんが、年間発生率（ARO）は尤度が5.2から1.04に引き下げられ、残存 ALE は初期の（本質的な）ALEよりはるかに低くなっており、積極的なリスク対応、すなわちリスク軽減のための優れた事例となっています。

以下の数式は、今後も目にして使用することがあるでしょう。

ヒント

脅威 x
脆弱性 x
資産価値 = **総合リスク**

脅威 x
脆弱性 x
資産価値 x
管理後のギャップ = **残存リスク**

総合リスク -
管理 = **残存リスク**

### 管理のメリット

管理のメリットは、多くの場合において、脅威を軽減すること（つまり先に述べたような管理の価値）だけではありません。管理を行うことで**運用コスト**を節約することもでき、こうした節約を算出することで、あなたの分析に影響を与えるかもしれません。

### 例：自動化されたパッチ適用

例えば、自動化されたパッチ適用プロセスを導入する機会を特定したとしましょう。これによって、パッチをより迅速に適用できるようになり、未解決の脆弱性や人為的ミスの可能性を減らすことができます。

しかし、それだけではありません。あなたの会社が 75 のアプリケーションを管理し、それぞれ隔週で 2 回のパッチを要しているとしましょう。それぞれパッケージ化とデプロイには平均 4 時間を要し、年間 600 時間がこの作業に費やされることになります。技術スタッフの時給を 100 ドルと仮定すると、運営コストの節約は以下のように割り出すことができます。

| | |
|---|---|
| アプリケーション数 | 75 |
| 各アプリケーションの2週ごとの更新回数 | 2 |
| アプリケーションのパッケージ化とデプロイにかかる時間数 | 4 |
| 手作業でのパッケージ化にかかる時間数 | 600 |
| 専任技術スタッフの時給 | $100 |
| **手作業でのパッケージ化の年間コスト** | **6万ドル** |

特に自動化によって時間の節約が可能になり、チームがより有意義な仕事に集中できるようになり、最終的には会社の経費削減につながります。

数値化が可能なその他のメリットの例をいくつか挙げましょう。

| メリット | 定量化 |
| --- | --- |
| **脅威検知**：異常の早期発見 | 潜在的脅威を検知する時間の短縮 |
| **インシデントレスポンス**：アラートやインシデントへの迅速な対応 | インシデント対応回数の削減 |
| **リアルタイムモニタリング**：セキュリティ情報イベント管理（SIEM）では、管理者が最近のアクティビティを確認するのを待つ必要がありません。 | 従業員の時間効率の向上 |
| **統合ビュー**：すべての対象機器が同じダッシュボードにデータを送信します。 | アプリケーション間切り替え時間の短縮、イベントの相関関係を調べる時間を節約 |
| **精度**：少ないフォールスポジティブ（偽陽性） | 事象がトゥルーポジティブ（真陽性）かどうかの評価にかかる時間の節約 |
| **コンプライアンス**：報告の強化 | 監査中のオンデマンド・レポート作成にかかる時間の節約 |
| **フォレンジック**：迅速なインシデント分析、eディスカバリ（電子証拠開示）請求がより容易に処理されるようになります。 | アクティビティログを再構築し、脅威の発生源を追跡する時間の節約 |
| **行動分析**：行動パターンを学習します。 | 通常のユーザー活動が行われているかどうかの判断にかかる時間の節約 |

# リスク対応

あなたはこれまで関連情報を収集し、リスク評価を実施してきました。
これで、いよいよデータに基づく対応策を提案することができます。

## 対応策のオプション

前述したように、リスク対応には4つのタイプがあります。

### 回避

リスクを負っている事業／プロセス／システム／ロケーションを閉鎖することにより、リスクを回避します。

### 移転

リスクを保険に委ねます。このオプションは財務上のリスク移転に過ぎず、会社は依然として顕在化したリスクに対する責任を負い、評判の低下などの他の種類の損失に対処する必要があることに注意してください。

### 受け入れ

リスクを受け入れます。この決定は、定期的に再検討する必要があることに注意してください。

### 軽減

リスクが現実化した場合に発生するコストが管理コストよりも高いことを認識し、リスクを軽減します。

フィッシング攻撃によるデータ流出対策の例に再び立ち帰りましょう。
私たちは、総合リスク、管理の導入コスト、管理導入後の残存リスクの計算を見てきました。

「**リスクを回避するには**外部との電子メールのやりとりを停止する必要がある」といった対応は、明らかに実現不可能です。

資産価値がそれを保護するためのコストが正当化されるほど高くない場合、**リスクを受け入れる**ことは理にかなっています。この例では、リスクが顕在化した場合のコスト、つまり年間損失予測値（ALE）を250万ドルと算出しました。この額は、年間9万ドルを管理に費やすことで約80%削減できます。
これはリスクを受け入れることに反対するための強力な論拠となります。”

リスクを保険会社に**移転する**ことは、初期コストは低いかもしれませんが、この事例ではあまり良い選択肢ではありません。サイバーリスクに対する賠償責任補償は金銭的なコストをカバーする可能性は高いですが、他の種類の影響については対象とされていません。この事例では、次の資金調達ラウンドへの影響が懸念されます。第三者にリスクを移転しても対処できないレピュテーションリスクのことです。

最終的には、セキュリティ管理を適用することでリスクを**軽減**できるようになります。このケースでは、フィッシング対策ツールと情報セキュリティに関するトレーニングキャンペーンを組み合わせています。これは、私たちが行ったリスク評価に明確に合致しています。

## リスク許容度を取り入れる

リスク評価によって必ず明確な対応策が得られるとは限りません。管理コストが、顕在化したリスクのコストよりも明らかに低い場合であっても、です。リソースは常に限られており、緩和戦略には常に**機会費用**が伴うためです。選択肢は必ずしも、行動を起こすか、リスクを受け入れるかのいずれかであるとは限りません。一方を行うか、他方を行うかの中間となる場合が多いのです。

会社のリスク許容度を理解することは、リスク軽減戦略がリスク評価に基づくものであっても、機会費用が大きいエッジケースを解決するのに役立ちます。

リスク許容度とは、会社がその目的を遂行するために受け入れるリスクのレベルのことです。リスク許容度が高いということは、より大きな利益を得るために大きなリスクを受け入れる用意があることを意味します。一方、リスク許容度が低いということは、その会社がリスクを可能な限り減らすことを好むことを意味します。

リスク許容度は、業種、会社の規模、成長目標などによって大きく異なります。リスク許容度にはまた、複数の側面があります。会社によっては、運用リスクに対する選好度は高くとも、コンプライアンスリスクに対する許容度が低いこともあります。

高いレベルでは、リスク許容度のステートメントは通常、以下のような形をとります。

| 一般的なリスク許容度<br><br>[XYZ 社]は、リスクに対してバランスの取れたアプローチを採用し、すべてのリスクが等しいわけではなく、<br>戦略目標を達成するためにはある程度のリスクが必要であることを認識しています。 | |
|---|---|
| イノベーションリスク | 私たちは、競争環境において製品を差別化する先進技術や革新的なソリューションへの投資に対して、高いリスク許容度を備えています。そのためには、研究開発や製品開発においてある程度の不確実性を受け入れる必要があることを、私たちは理解しています。 |
| 運用リスク | 私たちは、低〜中程度のリスク許容度を維持しています。オペレーショナル・エクセレンスを追求する一方で、私たちは提供基準を損なうことなく効率性とサービス品質を向上させる取り組みを優先しています。 |
| セキュリティリスク | セキュリティ上の脅威や侵害に対する私たちのリスク許容度は極めて低くなっています。ネットワーク・セキュリティとデータ保護に対する当社のコミットメントは最重要であり、当社のシステムとお客様のデータを保護するために多額の投資を行っています。 |
| コンプライアンスリスク | 私たちは、法的・規制的要件に対するコンプライアンス違反に対するリスク許容度を低くしています。すべての業務分野において、関連する法律、基準、ベストプラクティスを確実に遵守することが重要です。 |

これらの側面のそれぞれには、考慮すべき重要な要素がいくつかあります。

- **リスクキャパシティは**、会社が許容できる最大リスク量であり、通常は財務上のリソース、運営能力、規制上の制約によって決まります。
- **リスク許容度は**、目標に対して許容可能な偏差のことです。
- **リスク閾値は**、戦略の変更が必要であることを示す「越えてはならない一線」です。

リスク許容度とキャパシティの間のしきい値、または異なる許容度間のしきい値は、受け入れと緩和のいずれが適切な対応策であるのかわかりにくい「エッジケース」を整理するのに役立ちます。

フィッシングの例に戻ると、成長著しい新興企業ではリスク許容度が高く、サイバーセキュリティ予算が限られているため、管理が比較的安価であるにもかかわらず、フィッシング攻撃が成功した場合のリスクは許容範囲内であるというシナリオが考えられます。

ヒント

あなたの会社に専門のリスク部門がある場合は、その部門に指示を仰ぎましょう。通常、リスク管理の枠組みの一部としてリスク許容度が文書化されているはずです。

会社にリスク許容度ステートメントがない場合、編集可能なこのリスク許容度ステートメント テンプレートを使用して開始することができます。

# 例

これまでのところ、資産に価値を割り当て、脅威と弱点を評価し、定性的手法を使って脅威が発生する可能性と影響を判断し、年間損失予測値（ALE）を使用してリスクを判断し、管理コスト（および管理を行わない場合のコスト）を見積もってきました。

データを入手できたので、エンドツーエンドの例で考えてみましょう。

ヒント

編集可能なテンプレートをダウンロードし、このフォーマットを使ってあなた独自の評価を示しましょう。

## 例1：BYOD による情報漏洩対策

**問題文：**

BYOD（Bring-your-own-device）ポリシーを活用して個人デバイスを使用する社員が増えています。現時点では、BYOD には企業所有のデバイスと同じセキュリティ管理は適用されておらず、機密データの流出が懸念されています。

こうした管理が行われていないため、従業員は個人の電子メールやクラウド、データ転送ウェブサイト、AI ツールなどにデータを転送するなどして、社内の環境外で企業情報を処理することがあります。

**提案：**

現在、会社のデバイスに適用されているエンドポイント DLP（情報漏洩対策）を BYOD にも適用することで、（誤操作または意図的な）データ漏洩のインシデントを最小限に抑え、コンプライアンスを強化することができます。

**リスク評価**

**資産価値（AV）**：当社のビジネスインパクト分析（BIA）で、会社の機密データの資産価値は 100万ドルと算出されました。
**エクスポージャー係数（EF）**：データ漏洩の場合、機密データの価値の 60%を失う可能性があると想定されます。
**年間発生率（ARO）**：リスク登録とヘルプデスクチケットを分析した結果、危険なインシデントは年に 2 回発生する可能性が高いと結論づけられました。

AV x EF = SLE => $1M x 0.6 = $600K|
SLE x ARO = ALE => 600万ドル x 2 = 120万ドル

**不確実性**：データの信頼度は 85%です。
このレベルは、以下の要因に影響されます。

- 漏洩した機密データの性質と範囲
- 不満を持つ従業員が存在する可能性
- 啓発トレーニングを受講していない新入社員がいる可能性（現在それに代わる措置を実施中）

<table>
<tr><th colspan="4">リスク対応</th></tr>
<tr><th>オプション</th><th colspan="2">実現可能性</th><th>残存リスク</th></tr>
<tr><td>回避</td><td colspan="2">可能：回避すればリスクは 0になりますが、BYOD　ポリシーを終了しなければならず、従業員の不満につながるおそれがあります。</td><td>0</td></tr>
<tr><td>受け入れ</td><td colspan="2">可能：受け入れは可能ですが、リスク許容度の範囲外かもしれません。リスクの受け入れとは、直接的な金銭的コストと、風評被害、訴訟、罰金、規制当局の監視、ネガティブなソーシャルメディアなどの間接的コストも受け入れることを意味します。</td><td>年間損失予測値（ALE）= 120万ドル</td></tr>
<tr><td>年間損失予測値（ALE）= 120万ドル</td><td colspan="2">可能：保険にリスクを移転すれば、一定額まではカバーすることができます。サイバーリスクに対する賠償責任の補償限度額は、1件あたり通常50万～500万ドルです。ただし、<br>■ 評判の低下、規制当局からの罰金、顧客が起こす訴訟などのコストは、保険ではカバーされません。<br>■ 緩和策が実施されない場合、再発の際に保険は補償を停止する可能性があります。</td><td>不確実性が残ります。保険料とイベントの回数によって差があります。軽減されるのは財務リスクだけです。</td></tr>
<tr><td rowspan="7">軽減（推奨）</td><td colspan="3">可能（下記参照）</td><td rowspan="7">年間発生率（ARO）を80%削減すると、新しい ARO は 0.4 となります。残存する単一損失予測値（SLE）は変化がありません。<br><br>“新しい（残存）年間損失予測値（ALE）= 60万ドル x 0.4 = 24万ドル”</td></tr>
<tr><td colspan="2">費用</td><td>メリット</td></tr>
<tr><td>追加ライセンス</td><td>3万ドル</td><td rowspan="5">見積もり 社内脅威インシデントの可能性を 80%削減</td></tr>
<tr><td>デプロイに必要な人時</td><td>10,000ドル</td></tr>
<tr><td>ユーザーのトレーニング</td><td>10,000ドル</td></tr>
<tr><td>初年度合計</td><td>5万ドル</td></tr>
<tr><td>翌年度以降合計</td><td>3万ドル</td></tr>
</table>

## 例2：ロールベースのアクセス制御の見直し

### 問題文：

CRM（顧客関係管理）システムのロールベースのアクセス制御は、5年間更新されていません。その間に会社の構造は大きく変化し、役割の種類とそれぞれの権限は、システムにアクセスする個人の実際の役割と一致しなくなっています。脅威アクターが認証情報を入手するために悪用される可能性のある不必要な権限が提供されていることが多くあります。

### 提案

ロールベースのアクセスを再マッピングするには、部門横断的な膨大な労力が必要ですが、このような変更を行う場合、システムのダウンタイムは必要ありません。ユーザーが新しいロールに慣れるまで、生産性が短期間低下しますが、これはすぐに解決されます。これらのコストは、年間損失予測に比べるとかなり抑えられた額となるため、私たちはこの取り組みを進めることを推奨し、営業、マーケティング、オペレーションの同僚たちの支援を求めています。

### リスク評価

**資産価値（AV）**：当社のビジネスインパクト分析（BIA）で、会社のCRM（顧客関係管理）内データの資産価値は 150万ドルと算出されました。
**エクスポージャー係数（EF）**：ロギングやモニタリング、多要素認証など、私たちが導入している他の管理策を踏まえると、攻撃が成功した場合にアクセスして流出させることができる機密データは 10%程度と見られます。
**l年間発生率（ARO）**：異なる範囲で 1 年に 2 回行うペンテスト（侵入テスト）の過去 5 年間の結果を見ると、特権アクセスを使用したインシデントは 1 年に 1 回発生すると予想されます。

AV x EF = SLE => $1.5M x 0.1 = 15万ドル
SLE x ARO = ALE => 15万ドル x 1 = 15万ドル

**不確実性**：データの信頼度は80%です。このレベルは、以下の要因に影響されます。

- 漏洩した顧客データの性質と範囲
- 不満を持つ管理者がいる可能性
- 別の侵害による認証情報の流出
- 特権アクセスを迂回する攻撃手法を進化させている脅威アクター

<table>
<tr><th colspan="5">リスク対応</th></tr>
<tr><td>オプション</td><td colspan="3">実現可能性</td><td>残存リスク</td></tr>
<tr><td>回避</td><td colspan="3">なし：回避すればリスクは 0 になりますが、CRM（顧客関係管理）システムで特権的なアクションを実行することはできません。</td><td>0</td></tr>
<tr><td>受け入れ</td><td colspan="3">可能：受け入れは可能であり、リスク許容度の範囲内であると見られます。ただし、評判の低下や規制による監視といった間接的なコストも考慮する必要があります。</td><td>年間損失予測値（ALE）<br>= 15万ドル</td></tr>
<tr><td>移転</td><td colspan="3">可能：保険にリスクを移転させると、事故発生時の直接費用がカバーされます（単一損失予測値（SLE）= 15万ドル）。サイバーリスクに対する賠償責任の補償限度額は、1件あたり通常50万〜500万ドルです。けれども、緩和策が実施されない場合、再発の際に保険は補償を停止する可能性があり、</td><td>不確実性が残ります。<br>保険料とイベントの回数によって差があります。</td></tr>
<tr><td rowspan="5">軽減<br>（推奨）</td><td colspan="3">可能（下記参照）</td><td rowspan="5">年間発生率（ARO）は変化がありません。<br><br>エクスポージャー係数（EF）が50%減少すると、残存する単一損失予測値（SLE）は75,000ドルになります。<br><br>新しい（残存）<br>年間損失予測値（ALE）= 7万<br>5,000ドル x 1 = 7万5,000ドル</td></tr>
<tr><td colspan="2">費用</td><td>メリット</td></tr>
<tr><td>IT、運営、マーケティング、営業部門を通じて、スタッフの時間を新しい役割に割り当てる</td><td>10,000ドル</td><td rowspan="3">見積もり 攻撃成功イベントへのエクスポージャーを50%削減。</td></tr>
<tr><td>CRM（顧客関係管理）ユーザーが新しい役割に適応する間の生産性の低下</td><td>5,000ドル</td></tr>
<tr><td>合計</td><td>15,000ドル</td></tr>
</table>

# 結論

データに基づいてリスク評価を行い、その結果を提示するために必要なツールをあなたは手に入れたことになります。ビジネスレベルの目標とセキュリティ目標を整合化させ、リスクに対する共通の理解の構築に向けて大きな一歩を踏み出したのです。

また、CEO や取締役と同じ用語を用いて話すことで、目先の目標以上の成果を達成することができます。つまり、注目を得られ、認知度、スポンサーシップの獲得にもつながるのです。

こちらをクリックしてダウンロードしてください：


事業影響評価テンプレート


リスク許容度ステートメント テンプレート


攻撃対象領域チェックリスト


リスクアセスメント（評価）レポートテンプレート

成功をお祈りします！

## 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、またはIvanti
へのお問い合わせは、ivanti.com/ja
にアクセスしてください。