ABeam Consulting®
Build Beyond As One.

Cyber Attack Risk Assessment from an Attacker's Perspective

攻撃者視点の サイバー攻撃リスク診断

**サイバー攻撃シナリオを用いたリスク診断により
企業におけるセキュリティリスクを明らかにすることで、組織のセキュリティの
安全性向上を支援**

近年、サイバー攻撃による企業のビジネスへの影響として、営業活動停止や身代金支払いなどの金銭的損失、レピュテーション低下を招く事態が発生しています。また実被害を受けておらずとも自社のセキュリティ維持に努める方々は、日々新たなサイバー攻撃リスクへの対応に奔走し、見えない敵との戦いを強いられています。
ABeam Security® はサイバーセキュリティ対策をより一層強化するため、一連のサイバー攻撃の流れ(攻撃経路)を断絶できているかに着目した診断を通じて、企業におけるセキュリティリスクを明らかにします。また安全性の定量的な評価とリスクの根源となっている脆弱性要因を提言することで組織のセキュリティ向上に寄与します。

企業のサイバー攻撃対策が進まない要因

サイバー攻撃対策が進まない主な要因は、情報セキュリティを推進する部門において、サイバー攻撃対策の有効性を定量的に評価できていないことです。
また攻撃者の視点でリスクを評価できていないため、サイバー攻撃対策において対処すべきリスクを把握できていないことも要因として挙げられます。
これらの要因が解消されないまま、検出されたリスクに対して場当たり的に対策を講じた場合、サイバー攻撃対策への投資の一貫性が欠如し、期待する投資効果を得られません。
投資の一貫性を確保することで、サイバー攻撃対策をより強固なものにしていくためには、サイバー攻撃対策の有効性を定量的に評価したうえで、攻撃者視点でリスク分析・評価し、企業が行わなければならない対策を明らかにすることが重要です。

安全性の評価
診断対象となる環境を
定量的に評価できていない

攻撃者視点での分析
攻撃者の視点で対策を検討できていないため、
有効な対策が打てていない

サイバー攻撃対策への投資
場当たり的な投資は
費用対効果が低い

攻撃者視点のサイバー攻撃リスク診断サービス概要

サイバー攻撃対策を評価する方法として脆弱性診断が活用されていますが、脆弱性診断は脆弱性を特定することが目的であり、実際に攻撃が可能であるか否か判断するには十分とは言えません。また、実際に攻撃行為を実行することで診断するペネトレーションテストはサイバー攻撃時に悪用可能な脆弱性を特定することは可能ですが、企業負荷が大きいため、導入のハードルが高いのが実態です。
ABeam Security® は、診断対象の環境にて収集したデータをサイバー攻撃の手法を体系化したフレームワークである『MITREATT&CK®』に沿って分析します。これにより、診断対象組織への負荷を最小限に抑えながら企業の資産にどのように到達するか攻撃者の視点から明らかにします。
診断結果から組織の安全性を向上するための課題を提起し、課題に対する具体的な施策案を提案することで企業のサイバー攻撃対策の強化に寄与します。

他診断サービスとの比較

	診断方法	脆弱性の特定	企業への負荷	攻撃経路の特定
脆弱性診断	診断ツールを用いて企業環境の脆弱性の有無を検査	✕ 攻撃における悪用可否を考慮しない	○ 企業環境に侵入する必要が無いため、企業への負荷が小さい	✕ 実際に攻撃可能な攻撃経路を探索、特定することは難しい
サイバー攻撃リスク診断	企業環境からデータを収集 収集データから企業のリスクを分析	○ 実際のサイバー攻撃において悪用可能な脆弱性の特定ができる	○ データを収集するのみで企業環境に侵入しないので、企業への負荷が小さい	○ 実際に攻撃可能な攻撃経路を探索、特定することが可能
ペネトレーションテスト	ハッキング技術等を用いて侵入できるか検査	○ 実際のサイバー攻撃において悪用可能な脆弱性の特定ができる	✕ 企業環境に侵入して攻撃する必要があるため、企業への負荷が大きい	○ 実際に攻撃可能な攻撃経路を探索、特定することが可能 ※目標設定や実施目的から外れた場合は特定できない

アビームコンサルティングの提供価値

サイバー攻撃リスク診断においては、攻撃者視点で企業環境への侵入から実害に繋がる攻撃行為の実行可能性まで検証することで、サイバー攻撃の実行可能性を明らかにします。
また、診断結果報告書ではサイバー攻撃の実行可能性がどれほどあるかを報告するために、ABeam Security® が独自で考案したセキュリティ指標を用いて分析し、企業の安全性を定量的に評価・提示します。

セキュリティ指標	概要
安全性評価スコア	■ サイバー攻撃に対する安全性を100点満点で評価
実行可能な攻撃手法	■ 攻撃者が企業環境に対してどれだけ攻撃しやすいか判別するための指標 ■ 攻撃動機要素※に到達するための攻撃経路の構成要素を集計
有効な攻撃経路	■ 攻撃動機要素にどれだけ到達しやすいか判別するための指標 ■ 攻撃経路のうち、攻撃動機要素に到達できる経路数を集計
到達可能な攻撃動機要素の割合	■ 実態として攻撃が成功する可能性を測るための指標 ■ 攻撃動機要素のうち、攻撃者が到達可能と判定された割合
攻撃経路の成立に必要な攻撃手法の平均	■ 攻撃経路を成立させるためにどれだけ労力を要するか把握するための指標 ■ 攻撃動機要素に到達するまでに必要な攻撃手法の平均を算出

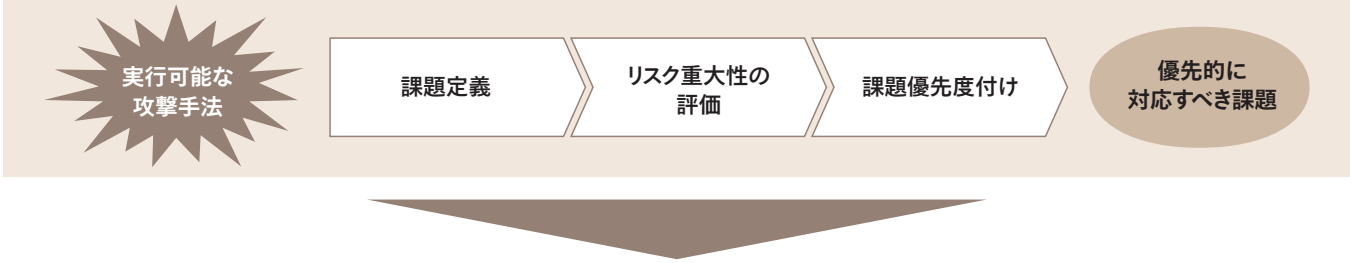
※ 攻撃動機要素:攻撃者が最終目標(診断対象が保有する資産の窃取、破壊、暗号化 等)を達成するために悪用する、機密性の高いデータや強い権限を有するユーザー

サービス導入によってもたらされる効果

セキュリティ指標を用いて診断した結果をもとに、攻撃手法が実行される可能性を低減するために必要となる対応を課題として定義します。さらに課題をリスク重大性の観点から評価し、課題優先度を付けることで企業は重大性の高い課題から対応することが可能となります。
しかしながら、定量的な診断結果と課題の優先度付けだけでは、課題に対処するための具体的な対策を立てることができず、リスクの低減につながりません。そこで診断結果の考察に加え、課題に対する施策案をABeam Security® が提唱するセキュリティ対応策整理のためのフレームワーク「Security Quadrat」に基づいて策定し、企業におけるリスク低減の達成を支援します。

なお、セキュリティ対策の意思決定に向けては、セキュリティ全体戦略とロードマップ、それに至る根拠とコスト算出が必要となります。
ABeam Security® ではこれらの業務を支援するサービス『セキュリティ投資計画策定サービス』を有しており、施策にかかる費用並びに管理会計上で計上される管理コストを含めたトータルコストを可視化することができます。これにより意思決定に向けた活動へスムーズに移行することが可能です。

課題定義および課題優先度付け



Security Quadrantに基づいた施策案

Organization（人・組織）

人や組織の改善、必要とされるスキルの獲得とあわせ、社会の変化に合わせた意識改革に取り組みます。

Technology（テクノロジー）

デジタルを活用した、脆弱性の把握や検知機能の追加、改善を実現します。
また、ログの解析や証跡の保存等、運用分野の要望も、デジタルで解決します。

Regulation（規範・法律）

新たに策定され、または変化する法律や規制への継続した対応が求められます。
CSR を遵守するためにも、法律と規制について常に知見を更新する対応が不可欠となります。

Process（プロセス）

正しい意思決定を支える業務遂行手順は、環境の変化に合わせて更新しながらの運用が必要です。
抜け漏れのない手順が正しく実行されているかも定期的に確認します。

アビームコンサルティング株式会社
www.abeam.com