ABeam Consulting®

URL : www.abeam.com/jp

情報セキュリティ診断サービス

今や企業においてIT化はビジネス目標を達成するための重要な要素となっています。一方で、企業活動におけるIT利用拡大に伴い、情報漏えいなどのリスクが高まり、企業存続を脅かすほど大きな問題に発展するケースも珍しくありません。情報資産を適切に管理し、情報セキュリティ管理態勢を確立・維持することは、企業活動を継続するために不可欠です。
アビームコンサルティングは、豊富な業界ナレッジを生かし、業界に合わせた柔軟かつバランスの取れた手法でセキュリティリスクを診断し、必要となるセキュリティ対策実施までをトータルに支援いたします。

情報セキュリティリスク／対策の分類

企業が直面する可能性のある情報セキュリティのリスクおよび対策は、以下の通りに分類されます。

リスク発生箇所	リスク 例	リスク対策の分類				リスク対策 例	
		人的セキュリティ	コンピュータセキュリティ	ネットワークセキュリティ	建物セキュリティ		
情報／コンテンツ	改ざん、機密漏えい、ウイルス	✓	✓			システム（技術対策）	リスク対策の導入（既存ツールの有効活用を含む）
コンピュータシステム	不正侵入、改ざん／破壊	✓	✓	✓			
ネットワーク	盗聴、外部からの攻撃	✓		✓		プロセス（運用対策）	管理方針・基準定義 リスク管理手順整備
設備(サーバ室、電源など)	不正侵入、天災／破壊	✓		✓	✓		
人(ユーザー、IT部門)	機密漏えい、不正操作	✓				組織・人材（体制対策）	体制構築（インシデント対応など） 教育・啓蒙

サービス概要

適切なリスク対策を行うためには、想定されるリスクに対して、システム（技術対策）、プロセス（運用対策）および組織・人材（体制対策）の3つの観点で検討することが重要です。
アビームコンサルティングの情報セキュリティ診断サービスは、初期診断によるセキュリティリスクの特定と、特定したリスクに対する具体的な情報セキュリティ本診断の2ステップで実施します。初期診断結果を踏まえた具体的なセキュリティ診断を実施することにより、企業のニーズに適した効率的な診断を実施することができます。

※調査範囲によって期間が前後します。

Step 1　初期診断によるセキュリティリスクの特定

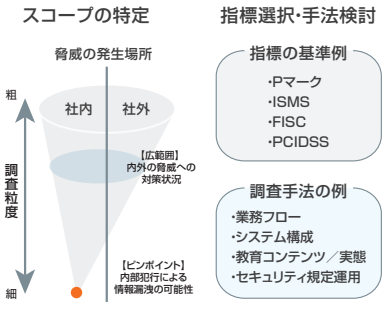
国際基準として実績のあるISO27001準拠により網羅的にリスクを特定

ヒアリング実施
↓
ヒアリング結果分析
↓
診断結果報告

Step 2　初期診断を踏まえた本診断

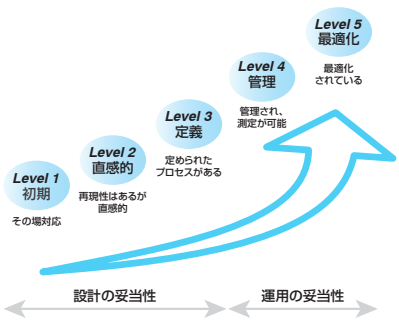
企業に合わせた調査手法の検討

アビームコンサルティングの業界知識と企業のリスク状況から、スコープを判断



成熟度モデルによるセキュリティ対策評価

対策の成熟度（設計および運用の妥当性）を5段階で数値化することにより、セキュリティ対策充実度と定着度を可視化



Step 1 : 初期診断によるセキュリティリスクの特定

現状の情報セキュリティのリスク対策状況を、国際基準として実績のある ISO27001 準拠により網羅的に評価します。

概要

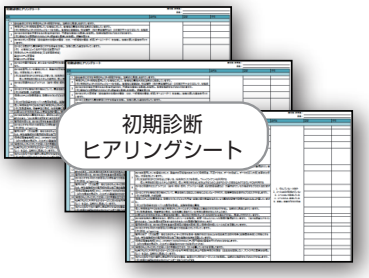
初期診断シート回答

- 現状の情報セキュリティリスクへの対策レベルを簡易調査
- 情報セキュリティリスクを網羅的に診断
- 技術対策（システム）、運用対策（プロセス）、体制対策（組織・人材）の3視点で診断

初期診断結果報告

- 初期診断の結果を報告
- 全体傾向、主要リスク、課題を簡易に評価
- 平均的な対策レベルに対する相対評価

成果物イメージ



Step 2 : 初期診断を踏まえた本診断

初期診断結果を踏まえ、リスクの大きな領域に対して詳細な診断を実施するとともに、リスク重大性を考慮した改善方向性を検討します。

概要

現状調査

- ISO27001準拠した体系に沿って現状の情報セキュリティリスクへの対応状況をヒアリング形式で調査
- 初期診断結果を踏まえた、リスクの大きな領域に対する詳細診断

成熟度診断

- 各セキュリティ要素に対して評価基準に則り成熟度を判断（レベル１～レベル５）
- リスク箇所とリスクの重大性を可視化
- リスク箇所に関する情報セキュリティ成熟度を可視化

課題抽出･改善の方向性

- 現状の情報セキュリティ対策の弱みの整理、改善方向性とりまとめ
- リスク重大性を考慮した改善方向性検討
- 早期対応と中長期対応に分けた改善施策整理

成果物イメージ