

ABeam Security® セキュリティ成熟度アセスメントサービス




情報セキュリティに係る対策の成熟度からリスクと課題の「見える化」を実施し、有効な対策となる次の一手を提案・支援

企業や組織にとって、個人情報や機密情報の活用と保護は事業活動を営む上で必要不可欠になりました。さらにデジタルテクノロジーの導入が進む過程において、個人情報や機密情報に対するセキュリティ体制が肥大化・複雑化、形骸化することで個人情報や機密情報の漏洩といったリスクが高まり、社会的信頼の失墜や事業活動への悪影響が懸念されます。アビームコンサルティングは、専門性をもったアセスメント担当部署が独立性を保ち、お客様のセキュリティ成熟度を評価することでセキュリティ対策の問題点とリスクを明確にします。また、対策の立案から実行まで支援することで、セキュリティ体制の強化に貢献します。

セキュリティ成熟度アセスメントの重要性

セキュリティ投資は事業継続性の確保や防衛力向上だけではなく、デジタルテクノロジーを活用して企業の収益を生み出す重要な戦略でもあります。セキュリティ投資を見据えたセキュリティ成熟度アセスメントを実施することで、改善に向けた投資計画がより経営層から理解を得られやすいものになります。そのため、セキュリティ成熟度アセスメントによるセキュリティ対策の現状と成熟度を知ることが改善への近道になります。

セキュリティ投資を見据えたセキュリティ成熟度アセスメントの活用観点

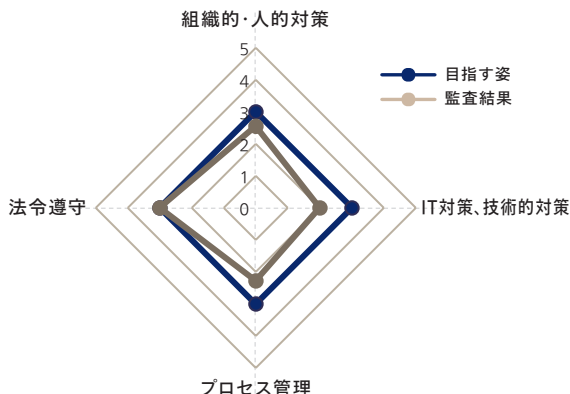
<p>社会的な責務を果たす</p>	<p>サービス向上</p>	<p>リスクの見える化</p>
 <ul style="list-style-type: none"> ☑ リスクに対応することで、顧客やステークホルダーへの責務を果たす 	 <ul style="list-style-type: none"> ☑ 対策の要点を踏まえることで、事業推進が活発化し、品質向上に寄与する 	 <ul style="list-style-type: none"> ☑ 対策が不足している点を金銭的リスク値として可視化することでビジネスインパクトを明らかにする

セキュリティ成熟度アセスメントサービス

セキュリティ成熟度アセスメントサービスは、アビームコンサルティング独自のアセスメントツールを用いて、現状のセキュリティマネジメントの問題点やリスクを明確にし、対策方針・課題を提起する助言型サービスです。情報セキュリティに係る国内外のガイドラインの核心的な共通項を「規範・法律」「プロセス」「テクノロジー」「人・組織」の4つの観点からなる評価項目に落とし込み、セキュリティマネジメントにおける成熟度を6段階で評価し、目指す姿のギャップとなる問題点とリスクを明確にします。また、対策方針・課題を提示したうえで、改善策の立案・実行まで一貫した支援が可能です。

アセスメント報告書

■成熟度を4つの観点から6段階で評価



対策方針・課題

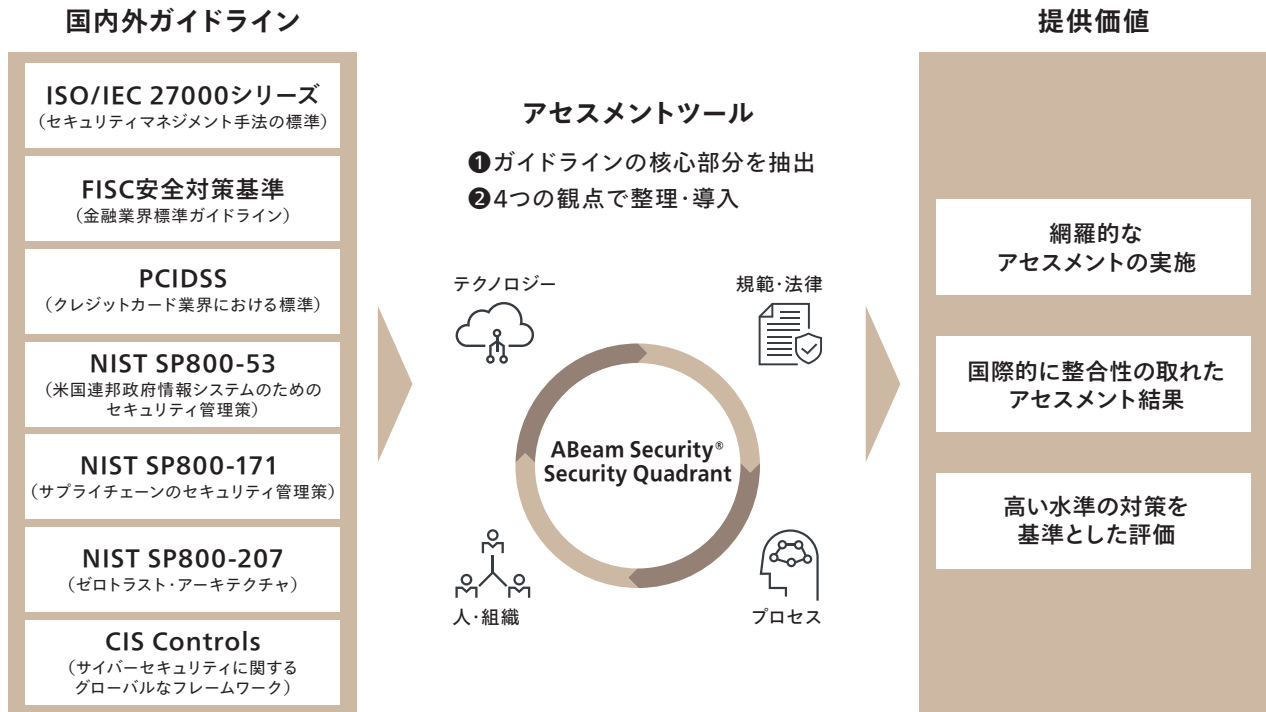
■アセスメント結果と整合性が取れた改善策を提案

- ☑ 改善策
- ☑ 概要
- ☑ 詳細
- ☑ アセスメント対応項目
- ☑ 重要度の評価指標
- ☑ 金銭的リスク値
- ☑ セキュリティインシデント発生率



アビームコンサルティングの提供価値

セキュリティ成熟度アセスメントは、アビームコンサルティング独自のアセスメントツールを用いて実施します。アセスメントツールは、国内外のガイドラインの核心的な共通項を当社が提唱する4つの観点 (Security Quadrant) で整理しているため、セキュリティ上必要な評価観点を網羅しています。加えて、金融業界の基準を採用することで一定レベルの対策水準を担保しています。これらの理由から、業界・業態を問わず全ての企業が事業を営む上で、必要な評価観点を網羅し、お客様固有の事情に合わせたアセスメントの提供が可能です。



情報セキュリティ対策について経営層に説明する際、対策の投資対効果を説明することが非常に重要です。なぜなら、対策を実現するために必要なコスト (時間、費用、人員等) の妥当性を経営層が判断する際、対策による脅威への効果を示すことが有効であるためです。本サービスによるアセスメントの結果は、実施されている情報セキュリティ対策の有効性だけでなく、次期セキュリティ投資計画において講じるべき対策の立案、および対策の実現に必要なコストの妥当性の評価にもご活用いただけます。

アセスメントの結果では、現状の情報セキュリティ対策への評価を踏まえ次に講ずべき対策を提示します。その際、実現に必要なプロセス、Quality (品質) Cost (コスト) Delivery (納期) によって評価した実施の優先度、さらに対策の効果を「見える化」して提示するため、経営層に向けた説得力のある説明材料として重要な役割を果たします。

実施プロセス

セキュリティ成熟度アセスメントは5段階のフェーズで実施します。

アセスメント実施フェーズにおいては、「セルフチェック」を中心に「ヒアリング」、「レビュー」といった技法を用いることで、回答者同士でドキュメント等に対する運用状況や課題の認識合わせが可能になります。

