情報セキュリティリスク評価・対応支援

情報セキュリティリスクを体系的に評価し、その結果に基づいた対応策を実装するためのお手伝いをいたします。

サービス概要

1．業務と業務で使用している情報資産、および、相互の依存関係を洗い出すお手伝いをします。

2．情報セキュリティリスクを体系的に評価するお手伝いをします。

－リスク評価の枠組みは、ISO27001 に準拠しています。

－リ スク評価手法は、某中央官公庁や大手企業でも採用されている実績のある評価手法です。

3．評価結果に基づく対応策を実装するためのお手伝いをします。

サービスの特徴

情報セキュリティの維持・向上のためには、全社を対象とした体系的な管理が必要となりますが、現状では、例えば、共有サーバーのアクセス権等のスポット的な対策に重点を置いているところが、少なからず見受けられます。このような個別対応は、一般的に特定の部分に過剰な対策を取ってしまう傾向があり、対策費用がオーバースペックぎみになりがちで、かつ、他の部分の脆弱性が残されたままになりがちです。これに対して、本サービスでは、全社にわたるリスクを俯瞰することができるので、これに基づいた全体を最適化した管理が容易になり、対策費用の配分も最適化され、結果としてコストの削減、および、情報セキュリティ対策に対する実効性の向上が期待できるようになります。

情報セキュリティリスク評価・対応ステップ

1	業務、情報資産の洗い出し	対象とす る部門の業務活動と業務活動で取り扱う情報資産を洗い出します。
2	情報資産分析	洗い出した情報資産に対して、相互依存関係の特定と情報セキュリティ事故が起こった場合の影響度評価を実施します。
3	詳細リスク分析、管理策検討	洗い出し た情報資産に対する脅威や脆弱性の評価を実施し、脆弱性を低減するような管理策を検討します。
4	ギャップ分析、管理策検討	ISO27001 の付属書 A の管理策に対するギャップ分析を実施し、ギャップを低減するような管理策を検討します。
5	規定策定、システム実装	検討した管理策を実施するための規定や手順の策定およびシステムの実装を行います。

プロジェクト完了までのエ 数とスケジュール

1．各ス テップごとに 1 回の訪問と次のステップまでのメールでの問合せに対応します。

2．各ステップごとの間隔は、１～２週間を想定しています。

3．お客様の 規模（部門数や拠点数など）によって、同じステップを複数回実施する場合があります。