情報セキュリティリスク可視化サービス

情報セキュリティリスクを体系的に可視化し、情報セキュリティリスクに対する対策の実効性を向上させるためのサービスです。

サービスが必要とされる背景

1. 情報セキュリティ管理に対する全体最適化の要求
   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。

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、相互の依存関係を可視化します。
   ー物品の流通経路やデーターの通信経路の可視化に威力を発揮します。
2. 情報セキュリティリスクを体系的に評価します。
   ーリスク評価の枠組みは、ISO27001 に準拠しています。
   ーリ 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. 可用性インシデントに対する情報資産の被災状況、および、依存する業務の稼働状況を可視化します。

情報セキュリティリスク可視化ステップ

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影響度評価を実施します。
3	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	被災状況の可視化	可用性インシデントに対する情報資産の被災状況、および、依存する業務の稼働状況を可視化します。

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。