日本総研
The Japan Research Institute, Limited

情報リスクマネジメントシステムの診断・構築

次世代の国づくり

情報リスクマネジメントの必要性

企業が事業活動を通じて取得･作成する様々な情報は、日々の業務遂行に不可欠な要素であるだけでなく、競争優位を基礎づける重要な経営資源でもあります。

しかし、企業が取り扱う情報は、常に外部に流出･漏洩するリスクに晒されています。特に、従業員や委託先等の不正･過失によって、重要な顧客情報／個人情報が外部に流出･漏洩した場合には、企業に対する信頼の失墜を招き、事業活動全体に多大なダメージを及ぼすことになります。

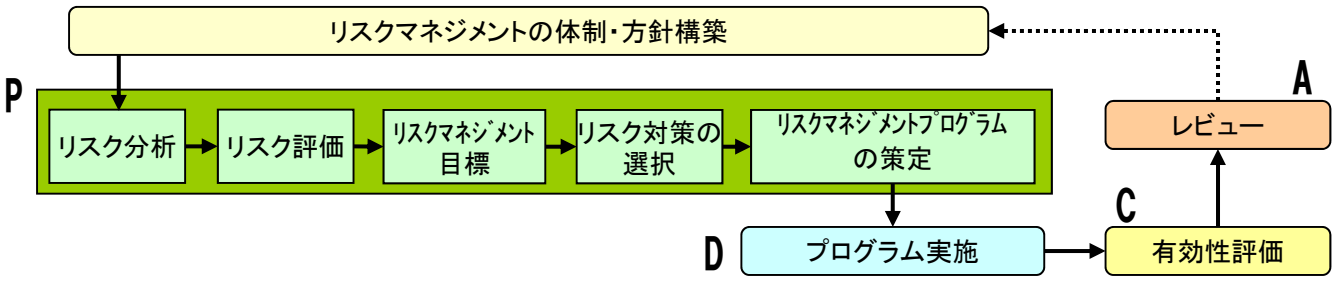
そのため、事業の安定的継続や顧客からの信頼維持･獲得のため、事業･業務の実態に即した情報リスク対策を講じ、情報漏洩等を防止するための有効性の高い統制活動を日々の業務活動に組み込むことが肝要です。

情報リスク対策の基本的考え方

有効性の高い情報リスク対策を行うためには、体系的･網羅的なアプローチによる取組みが必要です。断片的･部分的な‘対症療法’では、業務の中に眠る潜在的な情報リスクの低減には結びつきにくく、また、対策効果の持続性も不安定になります。

日本総研では、「リスクマネジメントシステム」の考え方に基づき、個別的･具体的なリスクの分析や対策立案だけでなく、それらを継続的に運用し、組織に定着させていくための体制整備までを含めてご支援します。

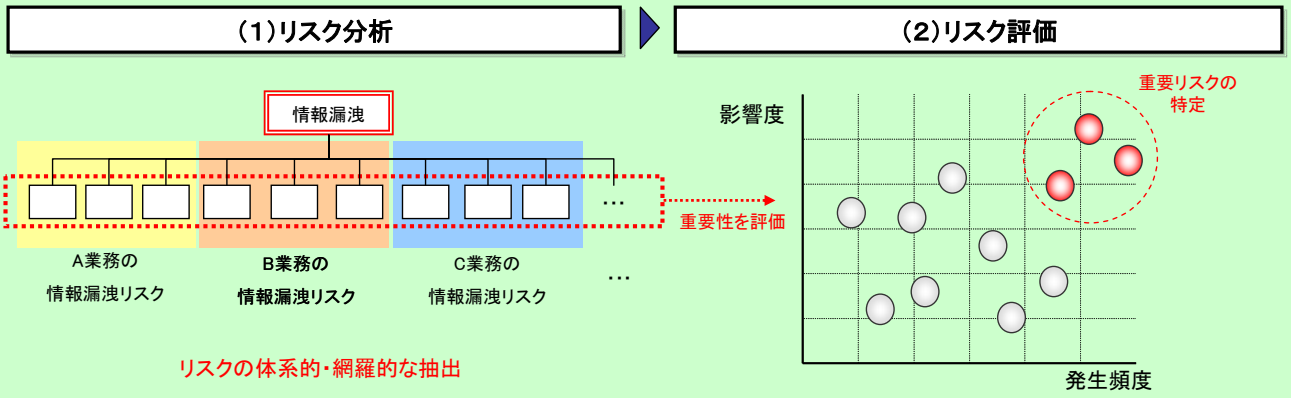
― リスクマネジメントシステムの考え方 ―



情報漏洩リスク対策の進め方

1. 情報漏洩リスクの抽出・評価

- リスク分析：企業の事業・業務の実態に基づき情報漏洩に関するリスクを体系的・網羅的に抽出・整理します。
- リスク評価：抽出された各リスクの重要性を評価し、重点的に対策を講じるべきリスクを特定します。



業務運用面での対策

2. 業務マニュアルの整備・見直し

・個別の業務に付随する情報漏洩リスクを低減させるための統制活動をデザインし、業務プロセスに組み込みます。

・統制活動を組み込んだ新たな業務の着実な運用・定着を図るため、業務の流れや統制活動を可視化した業務マニュアルを整備します。

IT面での対策

3. 情報セキュリティ対策の強化・見直し

・情報漏洩リスクを包括的に低減させるためのIT環境の整備に向けて、体系的に情報セキュリティ対策を強化します。

株式会社 日本総合研究所
リサーチ・コンサルティング部門

E-mail: rcdweb@ml.jri.co.jp