第103 回月例研究会報告
「JIPDEC リスクマネジメントシステム（JRMS）の狙いと適用」
東京海上リスクコンサルティング株式会社
リスクコンサルティング室
主席研究員　指田　朝久　氏
2004 年5 月27 日（木）
機械振興会館　B3F　第1 研修室

No.557　仲　厚吉

ISMS 認証制度、昨年発足した情報セキュリティ監査・管理基準、最近、パブリックコメントがなされたシステム監査・管理基準、等々百花繚乱にある中で、JRMS が新たに設けられ、それら基準の相互のあり方がよくわからない受講者である私に、この90 分は誠に有意義な時間でした。
ISMS 認証制度等のPDCA マネジメントサイクルで、P の計画段階におけるリスク分析にJRMS を使い、C の監査段階には、情報セキュリテイ監査基準またはシステム監査基準を使えば、うまくいくと理解しました。
先ず、JRMS の狙いをお聞きしました。
◎情報リスクを企業全体のリスクマネジメントの中のひとつのリスクとして捉える
・企業全体のリスクマネジメントができているかがまず重要
・情報リスクの優先順位は企業全体としてどの位置にあるか
・「はじめに対策ありき」ではなくリスク分析を実施しリスクの軽重を判断し、リスク度合いに応じた対策を検討する
安全対策を「はじめに対策ありき」で一律に決めつけるのではなく、情報リスクを企業全体のリスクマネジメントの中のひとつのリスクとして捉えるわけです。
JRMS の構成は、
Ⅰ　経営とリスクの関係
Ⅱ　JRMS におけるリスクマネジメント計画
Ⅲ　情報システムのリスク分析
Ⅳ　情報システムにおけるリスク対策
となっています。
Ⅳの情報システムにおけるリスク対策まで導くツールですので非常に便利なすぐれものという印象です。
JRMS では成熟度モデルが採用されていて、
レベル0　未認識
　組織内で全く意識されておらず、何もしていない
レベル1　初期
　組織内で部分的にしか実施されていない
レベル2　反復可能
　組織内で大体実施されているが、標準がない
レベル3　定義
　組織内で標準が作られ、大体それに従って実施されている
となっています。
分析のためのレーダチャートは、各項目ごとに、レベル0 ～レベル3 まで分析結果が表示されるので勘どころをつかむのに便利になっています。
バラツキ、ギャップ分析、分析結果のとりまとめ、評価まで対応できるツールというように理解しました。

まとめとして、
・情報リスク、情報セキュリティを企業経営、自治体経営全体に関わるリスクマネジメントの一環としてとらえる
・「はじめに対策ありき」ではなくリスクを把握し、そのリスクの度合いに応じて対策をとる
・リスクマネジメントは組織と人で実践する。そのための脆弱性分析にJRMS は有効である
・JRMS はISMS などの制度と対立するものではなく、相互に補完できる
という言葉で結ばれました。

引き続き、約30 分の質問時間には、活発な質疑応答がなされました。
Q １．JRMS は、企業の情報システムにおけるリスク分析、リスク対策を導くツールと思うが、例えば、受注工事のリスク、見積もりミスのリスクのような、プロジェクト管理上のリスク分析にも使用できるのか？
A １．JRMS はリスクマネジメント（JIS Q 2001）の視点に基づき、情報リスクへの対応について開発したもの。情報システムにかかわるもの以外のものには対応していない。

Q ２．コンサルタントが１本購入して、多数

のクライアント用に利用できるのか？
A ２．そのような利用方法は、著作権上の問題が生じると考えられる。

Q ３．ギャップ分析の方法論はあるのか？
A ３．レーダチャートによる視覚で分析するため実務に耐えられるものと考えている。利用者の経験則になる。

Q ４．分析する際の項目へのウェイトのかけ方だがアドバイスはあるか？
A ４．それぞれの企業の事情によりウェイトのかけ方が変わるので、クライアントと合意することが必要と思う。ツールにはデフォルト値があるが考えて使用すること。

Q ５．金融機関に勤めているが、金融検査マニュアル、FISC のシステム監査基準、ISMS、JIS X 5080、JIS Q 2001、情報セキュリティ監査基準、システム監査基準など様々な基準があり、それぞれ少しちがう。何を使えばよいのか？
A ５．各要求項目を包含したカバー範囲の確認が有効。JRMS は各基準から重要と思われるものを抽出し情報リスク対応用に開発した。

Q ６．ケーススタディ「X 社のリスクマネジメント」にある質問対象者の数は、経営者層3 名、リスクマネジメント部門5 名、情報システム部門5 名、ユーザ部門4 名であるが、それくらいの質問対象者数で妥当なのか？
A ６．妥当と思う。中堅企業を対象に事例としている。質問項目が1004 項目あるので、あまり人数を増やすと入力作業がたいへんになることもある。

Q ７．実際事例は集まっているか？　うまい使い方はあるか？
A ７．まだ未集計の段階であると思う。特定のシステムを対象として適用することも可能であるのでうまく使ってほしい。
最後に、講師に対して受講者から満場の拍手で謝意が述べられました。

―