第９５回月例研究会報告

No.6008　梅津尚夫

テーマ：「情報セキュリティ監査基準とシステム監査」
講師　：当協会副会長　和貝　享介　氏
（監査法人トーマツエンタープライズ　リスクサービス部　代表社員　）
日時　：２００３年3月１８日（火）
場所　：労働スクエア東京　６０１会議室

3月に経済産業省から「情報セキュリティ監査」について、中間とりまとめ報告書が出され、その後4月1日から運用が開始された。この中間報告書を作成した「情報セキュリティ監査基準研究会」のメンバーとして、システム監査人協会を代表して参加された和貝副会長により、「報告書」内容の解説を中心に、取りまとめに至った背景、今後の展望をお話しいただいた。

＜講演要旨＞

１　セキュリティ監査基準の必要性

2003年、いよいよ電子政府が本格稼動することにあわせて、セキュリティ確保の問題が焦点となってきた。情報セキュリティ対策の有効性を評価する統一的な基準の必要性が増してきている。

一方、国際取引が増える将来を見すえ、国際的にも整合性のとれたセキュリティ監査制度が必要となってきた。

２　当監査基準の対象

セキュリティ監査基準では、監査対象を情報資産とする。情報資産とは、情報システム、データ、要員などを含む範囲の広いものである。この点は、システム監査の対象が、情報システムであることと対比できる大きな特徴である。

セキュリティ監査は、情報資産に対する情報セキュリティマネジメントシステム（ＩSMS）を監査する。そのような監査を実施する場合の基準として、監査基準とは別にセキュリティ管理基準を策定した。

３　監査基準と管理基準

情報セキュリティ管理基準は、情報セキュリティ監査を行うときの「判断の尺度」となる基準、つまり監査においてどのような点を評価するかの目安であり、情報セキュリティ監査基準は、監査を行う主体の行為規範となる基準である。

４　助言型監査と保証型監査

監査の目的で分類すれば、保証型監査と助言型監査の2つになる。

保証型は、組織体が自らのセキュリティ対策について「お墨付き」を得ることを目的としておこなう監査である。この場合、保証といっても「事故が起きない」という絶対的な保証ではなく、一定の基準にそった範囲における保証であることはいうまでも無い。

一方助言型は、現状と基準とのギャップを指摘し改善の方向性を示すものである。主に外部の第三者の立場に立っての監査である。

従来のシステム監査はほとんどが助言型監査であったが、今後情報処理のアウトソーシングがすすむにつれ保証型の監査が要求されるようになるであろう。

その場合、まず助言型によって組織体のセキュリティレベルを上げていき、ある段階にまで来た時に保証型監査を行なうことになるであろう。

保証型監査報告書のひな形を提示して、内容の説明があった

５　監査基準の構成

セキュリティ監査基準は、一般基準、実施基準、報告基準の三つから構成される。一般基準は、監査の目的、監査人としての適格性、業務上の遵守事項などを規定する。実施基準は、監査計画立案、監査手続きの適用方法、監査体制など実施上の枠組みを規定する。報告基準は、報告書の記載方式や留意事項とフォローアップなどについて規定している。

６　情報セキュリティ監査企業台帳の設置

どこへセキュリティ監査を依頼したらよいかという質問に応えるため、企業台帳を作成しその

便宜を図る。

7　情報セキュリティ監査基準とシステム監査

システム監査基準も、同じく一般基準、実施基準、報告基準の三基準から成るが、こちらの実施基準は、行動規範というより、監査を行なうときの判断基準であり、少し意味合いが違う。

今回の取りまとめに至った経緯の中で、特にシステム監査との関係をどうするか、意見をまとめる苦労をお話された。新らしく策定されたセキュリティ基準の方がすっきりした体系であり、そのままシステム監査にも使用できる。

8　質疑応答

(1)　他のセキュリティ関連基準について

（質問）関連する基準とその使い方

(回答)システム監査には、このセキュリティ監査基準だけでなく、不正アクセスガイドラインなど他のいろいろな基準を合わせて使用することで、充実したシステム監査を行なうことができる。

(2)　システム監査基準との関連

(質問)　セキュリティ監査基準とシステム監査基準と重複する部分がでてくる。システム監査の存立基盤が狭くならないか、懸念している。そうならない様にシステム監査人協会としてもっと頑張って欲しい。

(回答)両者をどのように、使い分けていくのか、これからの問題である。システム監査基準も制定以来かなり時間が経つので、この機会におそらく改定されるのではないだろうか。そうすると、セキュリティ監査とシステム監査との切り分けがもっと明確になってくるものと思う。

以上