第９２回月例研究会報告

日時：平成１４年１１月５日　午後６時半より
場所：労働スクウェア東京 601 会議室
演題：「セキュリティポリシーの実効性を向上させるための運用段階のシステム監査」
講師：KPMG ビジネスアシュアランス㈱　代表取締役 IRM 事業統括（COO）　榎木千昭　氏

講演要旨

１．情報セキュリティポリシーの役割と実効性

企業が情報セキュリティを検討する場合、個別の情報セキュリティ対策を採るのではなく、情報セキュリティマネジメントを想定し、その情報セキュリティマネジメントの一環として、まずセキュリティポリシーを策定すべきである。

セキュリティポリシーは、階層的に検討され、上から第１階層が基本方針（ポリシー）として、組織の情報セキュリティに対する方針、姿勢を記述するものである。主に、組織がなぜ情報資産を保護する必要があるかを記述する。

第２階層は、対策基準（スタンダード）である。ここでは、基本方針を実現するために何をしなければならないかを記述する。

第３階層は、実施手順（プロジージャ）である。ここでは、対策基準のないようをどのような手順に従って行えば良いかを記述する。マニュアルや情報システムの設定パラメータ等が該当する。

このようなセキュリティポリシーを実現する仕組みとしての情報セキュリティマネジメントの必要性は何か。それは次のようなものである。

①事業戦略・ＩＴ戦略と整合性のとれたセキュリティマネジメント戦略が必要なこと
②戦略およびリスクに基づくセキュリティレベルの設定をすること
③マネジメント、技術対策、運用対策のバランス、および各技術同士や技術と運用との整合性が取れたセキュリティ対策をとること
④セキュリティレベルの継続的な維持と見直しの必要性
⑤効率的なセキュリティ投資とその効果測定の必要性

これらを満足すべく情報セキュリティマネジメントをシステムとして実現するものがＩＳＭＳである。

ＩＳＭＳの構築ステップは、セキュリティポリシー文書策定 → ＩＳＭＳの適用範囲決定 → リスク評価 → リスクの一覧の策定 → 対策基準の策定 → 適用宣言書の作成 である。

ＩＳＭＳのサイクルは、ＰＬＡＮ（基本方針） → ＤＯ （対策の実施）→ ＣＨＥＣＫ（モニタリング） → ＡＣＴＩＯＮ（見直し） であり、このサイクルを構築することは、経営者の責任である。

セキュリティポリシーの実効性を検討する上で、考慮しなければならないのは次の諸点である。

①セキュリティポリシーの妥当性
組織の目標とすべきセキュリティレベルの設定が妥当かどうかということである。達成不可能なレベルを設定すると、たとえそれが一部であっても、全体が不可能となってしまうこともある。

②セキュリティポリシーの遵守
セキュリティポリシーを遵守するための仕組みが整っているか、意思決定、業務の遂行、及びシステム設計、開発、運用においてセキュリティポリシーが遵守されているかということであ

る。
③見直し
事業戦略や環境の変化に伴うリスクの変化、遵守状況、および事故や事件の発生状況に応じて、セキュリティポリシーの見直しが適時に行われているかということである。

２．ISMS の監査
このアジェンダと次のアジェンダは、ISMS とセキュリティポリシーとの関係を説明するために設定されている。ＩSMSの監査の意義は、セキュリティポリシーを遵守するための仕組みが整っているかを検証することにある。
監査はモニタリングの１形態であるが、ここでＩSMSにおけるモニタリングの役割分担を考えてみる。セキュリティマネジメントの一次防御は、システム部門を含む各部門に責任がある。第２防御は、リスク管理部門である。そして、第３防御が内部監査部門である。これらの部門は各モニタリングの成果を経営陣に報告する。ここで経営陣に対するのモニタリングはどうするか。ここに外部監査としてのシステム監査の役割がある。システム監査の成果は、利害関係者等企業外部者にもたらされることもある。

内部監査としてＩSMSが確立した組織におけるシステム監査の役割を整理してみると、次のようになる。
①ＩSMSの実効性の監査が中心であり、次の内容となる。
・組織体制、役割、セキュリティポリシーの妥当性
・サンプリングによるモニタリングの適切性の監査
・リスクアプローチによる二重チェック
・セキュリティ投資の有効性・効率性の監査
②教育的効果
・すなわち監査実施および監査報告による教育的な役割である。

外部監査としてのシステム監査の内容は、次のようである。
①経営と内部監査を含むＩSMSの実効性の監査
②リスクの高い領域に対する監査
③技術者の専門知識が必要な領域の監査
④人的リソースの確保
⑤利害関係者等からの信頼性の確保

３、ISMS の監査ポイント
監査ポイントの第一は、遵守における義務と罰則の明確化である。セキュリティポリシーの遵守にかかわる署名や違反に対する懲罰規定の適用の明文化は、遵守率の向上に影響する。また、懲罰規定等の適用以外に、個々のセキュリティ項目の違反に対する罰則等を規定する必要がある。具体的には、上司への通知、始末書等の軽微な罰則の適用、利用停止等の処置、人事評価制度への反映などである。
第二のポイントとして、セキュリティ教育が挙げられる。内容として次のような事項に留意が必要である。
①継続的なセキュリティ教育の実施とセキュリティポリシーの遵守およびセキュリティ事故や事件の発生率の相互関係
②シニアマネジメント、ミドルマネジメント、従業員、派遣社員、外部委託先、取引先、顧客等全ての関係者全員への教育が必要

③教育を定期的に実施する必要がある。トータル時間が同じでも、回数を増やすことが効果的
④複数の方法を組合わせる。パンフレット配布、集合記養育、セルフアセスメント、監査、ｅラーニング等
⑤全員が受けること、教育受講時の署名や受講しない場合の派ッ則を徹底

第三のポイントは、費用対効果の高いインシデントマネジメントである。下記のような内容をもつ。
①情報セキュリティ事故・事件の迅速な発見体制
②明確な基準による経営者等への報告体制
③システムの停止やネットワークの遮断等の緊急対応
④顧客や取引先への迅速な情報提供
⑤メディアからの問合せに対する適切な回答
⑥法的手段や抗議等に対する対応

４．セキュリティポリシーの遵守状況の監査
このアジェンダはセキュリティポリシーを根付かせるための有効な手段として必要である。すなわち意思決定、業務の遂行、及びシステム設計、開発、運用においてセキュリティポリシーが遵守されているかどうかを検討する監査である。
セキュリティポリシーの有効性をチェックする監査手続として、コントロールテストの実施があり、次のような事項を対象とする。
①システムの利用や情報の取扱い
②システム設計や業務設計へのコントロールの取組み状況
③ソフトウェアや機器の調達、外部委託
④システム設定
⑤システムの開発業務、運用業務

これらをチェックする方法として、次のような手続を実施する。
①インタビューや観察による業務実施状況のチェック
②設計文書、契約書等のチェック
③実施履歴のチェック（申請書類、議事録、システムログ等）
④ツールやオペレーションによるシステム設定状況のチェック

上記のテスト結果の分析により、セキュリティポリシーが遵守されていない場合には下記のようなものがあり、それぞれ改善を要する。
①個人的な怠慢、意思の欠如 → 罰則、自動化を要す
②全体的に浸透していない → 啓蒙、教育を要す
③セキュリティレベルが高すぎる → セキュリテイポリシーの見直しを要す
④手順が明確でない → 実施手順の整備、教育、自動化を要す
⑤業務との不整合 → ポリシー、実施手順の見直し、例外措置と手順の明確化を要す

コントロールのテストとして、実証性テストも肝要である。実証性テストは、セキュリティ事故（可能性）の実態を把握することにより、コントロール（対策）の有効性を確認するものである。実証性テストを行った上で、コントロールテストを実施すべき範囲を決定する場合もある。
実証テストの例として、次のようなものがある。
①ネットワークや建物への侵入（ペネトレーション）

②セキュリティ事故の分析
③コンティンジェンシープランのテスト（ウォークスルー等）
④未承認プログラムの発見

５．情報セキュリティ監査の動向

現在実施ないし実施が検討されている情報セキュリティ制度を概観する。

先ず、経済省の情報セキュリティ監査研究会である。電子商取引や電子政府の信頼性・安全性を確保するためには情報セキュリティの確保が不可欠であり、そのために第三者による技術面、運用面の情報セキュリティ対策の実効性の監査が望まれるとの趣旨で、２００２年研究会が開始された。情報セキュリティ化監査のあり方や、情報セキュリティ監査基準及び標準的な実施事項の検討がなされている。

次に、ＢＳ７７９９認証制度およびＩSMS適合性評価制度である。前者は、２００２年１０月２１日現在、グローバルに１４９組織の認証取得事業者が存在する。このうち日本は１１組織で２位である。　後者は、２００２年１０月２１日現在、３８組織が認証取得している。

最後に、米国公認会計士協会のＴＲＵＳＴサービスを紹介する。このうち SysTrust は、情報システムのコントロール（可用性、セキュリティ、インテグリティ、保守性）の有効性に関わる評価である。また、WebTrust は、e-Commerce のためのコントロール（プライバシー、セキュリティ、トランザクションインテグリティ、可用性、機密性等）の有効性に関わる評価である。このＴＲＵＳＴサービスは日本公認会計士協会により、わが国でも展開される予定である。

（感想）

約 70 名という参加者の多さが、「セキュリティ」ないし「セキュリティポリシー」に関するテーマへの関心の高さを示していた。榎木氏の講義は、「情報セキュリティとは何か」という基本から、主要アジェンダである「セキュリティポリシ」を経て、今日的動向である「情報セキュリティ監査」までをカバーしており、受講者全員、時間いっぱい熱心に聴講していた。最後に話された「情報セキュリティ監査の普及と課題」は、今回のテーマに対する、わが国の監査体制制度への提言とも言える結論となった。

（Ｎｏ．１８　和貝享介）