

はじめに

情報システムの構築にセキュリティという要素が欠かせなくなってから、ほぼ10年が経過した。その間にテクノロジーの進歩や規則整備の努力によりアカデミック機関における情報セキュリティ対策は一巡した。しかし一方で、情報システムをとりまくセキュリティ情勢は厳しさを増している。このような状況のもとでは、最新のテクノロジーを理解するにとどまらず、情報セキュリティマネジメントという視点からセキュリティ対策を継続していかなければ、リスクの激しい変化や増大する業務に対応していくことは困難である。

本WGは、実現可能なセキュリティ対策を設計、実装、検証するために役立つマネジメント・ノウハウをわかりやすくまとめることを目標に、2007年1月より2009年1月まで活動してきた。活動は、準備会と計8回の会合（8回目は合宿）、メーリングリストで交換した約400通のメール、WebコンテンツマネジメントソフトPOESYの利用の3本柱からなっている。2年間の第一期と第二期に分けて、各期で成果レポートを作成した。本報告書には、第二期、第一期の順番で二つの成果レポートをおさめている。両方の期で「組織・人間に関わるテーマ」、「実用的なテーマ」および「先進的なテーマ」の三つを選択し、合計で六つのテーマに取り組んだ。成果レポートでは、それぞれのテーマについての議論をレジメの文章とスライド形式にまとめている。第一期の特徴については第一期成果レポート中の「はじめに」で紹介した。ここでは第二期で選んだテーマについて簡単に紹介する。

第二期には、「人間・管理・インシデントハンドリング」、「状況確認のためのセキュリティアプライアンス」および「エンドポイント」をテーマに選んだ。いずれのテーマにおいても最終結論を模索するのではなく、現時点における最善の実践とはなにかを考えた。最初のテーマでは、情報セキュリティにおいて最も脆弱な存在である人間をどう管理するのか、セキュリティ体制をどのように良質に保っていくのか、実際にセキュリティ事故の発生に対して組織と人間はどう振る舞うべきなのか、について議論した。二つ目のテーマでは、最新のセキュリティテクノロジーを実装するアプライアンスについて考察した。具体的な事例としてP2Pファイル交換ソフトウェアを取り上げ、セキュリティマネージャとしての考え方をまとめた。このテーマのもと10の組織にセキュリティ・アンケートを実施させていただき、回答を頂いた。アンケート結果をまとめたので参照して欲しい。三つ目のテーマでは、これまで利用者側にまかされていた「エンドポイントセキュリティ」をどうマネージしていくのかについて、松竹梅の三つのソリューションを用意し議論した。それぞれの特徴を表形式で示したので、エンドポイントシステムの設計に役立てていただければ幸いである。

まとめ役
湯浅富久子