第１８回研究大会　発表要旨

統一論題「システム監査の新展開と深耕」

＜基調講演＞

経済産業省の情報セキュリティ政策～システム監査基準の改訂を中心として

経済産業省　商務情報政策局　情報経済課　情報セキュリティ政策室
大崎　友和

＜発表要旨＞

「システム監査基準」は、昭和 60 年(1985 年) 1月に策定以降、平成8年(1996 年)1月に改訂され、今回は2度目の改訂である。前回の改訂から8年経つが、この間、技術革新の進展や技術的複雑性の増加により、情報システムを巡るリスクも大きく変質した。今回の改訂は、「システム監査基準」をそうした変化に対応した基準とすることを目指したもの。現在パブリックコメント（案）として公表している「システム監査基準」及び「システム管理基準」について、その背景と修正ポイントについて説明を行う。

＜特別講演＞

専門監査人資格認定制度の意義と役割

システム監査学会　会長　　鳥居　壮行

＜発表要旨＞

IT の発展により企業経営の環境が大きく変化している。そのことが、情報システムをめぐる監査にも影響を与えている。すなわち、情報システムの監査にも各分野ごとに専門分野を確立して対応しなければならなくなってきている。経産省が情報セキュリティ監査基準を発表したのも時代の流れである。このような認識のもとに、専門監査人資格認定制度を発足させることになった。この制度の背景および内容を紹介する。

＜発表1＞

セキュリティ監査の効果的実施のための課題
ーISMSと情報セキュリティ監査基準研究プロジェクト報告

ISMSと情報セキュリティ監査基準研究プロジェクト　　木村　裕一

＜発表要旨＞

「情報セキュリティ監査等の監査について、効果的、有効な監査を実施するための問題点と、それを解決するため監査人に課せられた課題」のテーマの下で、サブテーマを設定して討議した。

サブテーマ1．効果的な監査への取組み：
情報セキュリティ監査が増えることについて効率的な取組み方法はないか。現場の負担を軽減し、効果的に監査するため、どのような解決策があるか、監査人としてはどのように取り組むか

(1)　監査の実施状況
① ISO9000とISMS（またはBS7799）の認定を受けた部署がそれぞれの監査を受ける。
各制度の外部審査機関に対して監査実施の説明が必要。
② スキルが違うので、ISMSとISOの監査は一緒には出来ないと思っている。

(2) 対処・対策
① 現場に対しては監査内容を重複させないことを条件にして複数の監査を実施している。
② 情報セキュリティ監査基準は監査目的により部分的な利用や、部分的に深めての利用も可能
③ マネジメントシステムの構築　：情報システムの管理、情報セキュリティ対策、品質管理等を最初からマネジメントシステムとして意識して組織に取り入れておくことが、監査を一本化するためにも必要。

サブテーマ2．　監査人の責任はどこまであるのか。背景として外部監査が多くなるものと考えられる。
監査人として、この問題をどのようにとらえるか。

(1)対処・対策　　さまざまな項目に分けて考える
① 監査の責任を、監査人だけで考えることは適切でない。
② 監査の責任を3つの構成要素　監査基準　監査人、被監査部署に分けて、全部の問題として捉える。

その他3つのテーマについての討議を紹介する。

＜発表2＞

進化するシステム監査の新たな役割を考える
ーシステム監査体系化研究プロジェクト報告ー

システム監査体系化研究プロジェクト　松田　貴典

＜発表要旨＞

インターネットをはじめとする IT（情報技術）のめざましい進展は，豊かな情報化社会をもたらす一方で，企業や官公庁，諸組織の情報システムは多様化し，その脆弱性は複雑に顕在化している。

近年，情報システムに関連しての事故・犯罪が増加し，おおきな社会的な問題になっている。「システム監査」の重要性の認識はますます高まっているが，現在，システム監査のセキュリティ監査化，システム監査のソリューション・ビジネス化，システム監査のITガバナンス化，システム監査の公認化，システム監査の企業統治化，などなどと言われている。そこで，システム監査の関連事項が，システム監査とどう関連し，どのように解釈し，定義すればよいのか，原点にもどってシステム監査を研究報告する。

＜発表3＞

日本IBMにおけるシステム監査事例

日本アイ・ビー・エム（株）　安部川　威

＜発表要旨＞

- IBMにおける内部統制の仕組み（プログラム）、特に内部監査（オーディット）と自己点検プログラムにつて具体例を交えて紹介
- システム監査の領域および頻度を紹介し、全体像を理解いただく
- ASCA（Application Systems Control and Auditability）

内部監査に対応するプログラムの具体例として、新規アプリケーションの開発から導入までに実施されるシステム・レビューのプロセスを紹介

お断り）基調講演については、当初予定していた経済産業省　情報セキュリティ政策室　山崎琢矢氏から大崎友和氏に変更となりました。ご了承下さい。