**近畿支部　支部創設２５周年記念研究大会　報告**

№６４５　是松　徹

**【日時】**　　２０１３年７月６日（土）　１３時～１７時
**【場所】**　　大阪大学中之島センター　３階　講義室３０４
**【統一テーマ】**「システム監査の新領域への対応」
**【参加者数】**　９４名（発表者を含む）
**【概要】**

本研究大会は、支部創設２５周年を記念して統一テーマを掲げ、支部研究プロジェクト活動成果の報告（４編）、会員から応募のあった研究論文の発表（２編）、およびパネルディスカッションを行った。大会運営は、発表者による説明、コメンテータによる意見表明（研究論文）、およびパネルディスカッションを介した会場からの質問への回答と今後の方向性の議論という形態で実施した。成果報告と研究発表の計６編は、近畿支部の会員３名の方に記録を分担いただいた。

**<<開会挨拶：林支部長>>**

日本システム監査人協会近畿支部は、１９８８年（昭和６３年）３月４日に「関西支部」として発足しました。従いまして、本年で発足から２５年が経過したこととなります。
四半世紀の長きに渡り、支部活動が活発に継続しておりますことは、歴代の支部長、支部役員、支部サポーターの皆様を含めました支部会員の皆様の多大なるご尽力、ご協力の賜物と考えます。改めて厚く御礼を申し上げる次第です。本当にありがとうございました。また、これからも引き続きよろしくお願い致します。

さて、今回、支部創設２５周年と言う節目の時を記念して、支部会員の皆様の研究成果の発表を中心とした研究大会を開催することと致しました。情報システム産業は、技術革新によるビジネスモデルの変化や多様化が他の産業に比して早いと考えますが、ここ数年、更にその変化のスピードが速まっていると思われます。例えば、クラウド・コンピューティング／クラウドサービスの進展に伴う変化、事業継続の観点から見た「情報システム」の位置付け等、ますます多様化しており、その結果、システム監査も多様化しています。こうした状況を踏まえ、統一テーマを「システム監査の新領域への対応」と致しました。このテーマに沿って、近畿支部の研究プロジェクトの活動報告や会員の皆様の研究発表と、パネルディスカッションを行います。限られた時間の中で十分な議論ができないことも想定されますが、本研究大会の議論をきっかけに、今後のシステム監査の在り方や、目指すべき方向を皆様と考えて行きたいと存じます。

以上

特定非営利活動法人　日本システム監査人協会
近畿支部長　林　裕正


<<支部長 開会挨拶>>

**<<沼野会長からのメッセージ>>**

日本システム監査人協会近畿支部創設２５周年記念研究大会開催に当たり、一言ご挨拶いたします。

○謝辞：

本日ご参加頂いている皆様

日頃日本システム監査人協会近畿支部をご支援頂き、誠にありがとうございます。

また、本日はこの近畿支部創設２５周年記念研究大会にご参加頂き誠にありがとうございます。

本記念研究大会を後援頂く、経済産業省近畿経済産業局様,

特定非営利活動法人ＩＴコーディネータ協会様,後援頂くことを、この場を借りて厚くお礼申し上げます。

そして最後に、近畿支部林支部長をはじめメンバーの皆さん、創設２５周年、おめでとうございます。

支部創設２５周年に当たり、日頃の近畿支部の充実した活動に、改めて敬意を表したいと思います。

また、本記念研究大会の開催諸準備、いろいろご苦労様です。ありがとうございます。

○本文：

さて、少し昔の話になりますが、私たちは、農業革命、産業革命を人類史上の大変革として、学校の授業、教科書で学びました。そして、それに匹敵する出来事として、今、情報革命が進んでいると言われます。

しかし、その真只中にいると、日々の少しずつの変化の中に埋もれて、農業革命や産業革命に匹敵する変革の時代に生きている醍醐味を実感できる人はそう多くないのではと思います。きっと今から40～50 年先の子供たちが、我々が学んだ、農業革命、産業革命と同様に、20 世紀から21 世紀にかけての情報革命の全体、そしてその時代の人々の行動を授業や教科書で体系に学ぶのだと思います。

変革の時代は、変革を牽引するコア技術をその時代の人々の知恵で如何に使いこなすか、コントロールするかの試行錯誤、成功・失敗の繰返しの時代です。

例えば、情報社会と言われる今日は、ＩＴの急速、飛躍的発展、進化と共に、それと表裏一体のリスクを如何にコントロールするかの試行錯誤の時代、すなわち情報システムの“不完全性”、具体的に言えば、安全性、信頼性、効率性等の追及における避けがたい失敗リスクの存在を受入れつつも、知恵を絞って情報システムを如何に利活用するかが問われている時代と言えます。

情報システムの“不完全性”は、情報システムの開発・提供者とその利用者が、情報革命の恩恵を享受する上で、共に受け入れなければならない現実です。情報システムの“不完全性”を正面から受け入れ、かつ、利用者が積極的に情報システムを利活用していくには、情報システムの開発・提供者と利用者の相互信頼関係を確立することが重要です。そして、この相互信頼関係の確立には、情報システムの開発・提供者の説明責任遂行、即ち、やるべきことはやっていることを自らキチッと説明することが不可欠であり、これに呼応して、この説明責任遂行と不可分の、説明責任遂行に信頼性を付与するシステム監査が求められることになります。

今から40～50 年先の子供たちが、20 世紀から21 世紀にかけての情報革命の全体、そしてその時代の人々の行動を授業や教科書で体系に学ぶ時、当時の人々の知恵、行動の一つとして、システム監査の導入、活用が語られるかどうかは、今後のシステム監査の普及、また当協会を始めシステム監査に関わる関係団体、そしてシステム監査人の今の活動にかかっているのかもしれません。

本日の近畿支部記念研究大会は、「システム監査の新領域への対応」を統一テーマとし、近畿支部の研究プロジェクトの活動報告や会員の日頃の研究の発表、そして最後に経験豊富なシステム監査人によるパネルディスカッションも予定されています。まさに、日頃の近畿支部の活動・研究成果を参加者で共有し、これからのシステム監査の更なる普及の大きな契機になればと期待しています。

本日の報告、発表、そしてパネルディスカッションが、ご参加の皆様がシステム監査に取組むに当たって有意義な大会となることを心から祈念し、簡単ですがご挨拶と致します。ありがとうございました。

定非営利活動法人　日本システム監査人協会

会長　沼野伸生

＜報告者　竹下　健一（No.2083）＞

**１．コンプライアンスのシステム監査について（第Ⅲ期報告・最終）**

発表者：雜賀　努　氏（株式会社ニイタカ　監査室）

**【発表の概要】**

情報通信技術の進歩により、情報システム（ICTシステム）と密接に関連する法的問題を、コンプライアンス視点で点検・評価することが重要な課題となっている。本研究プロジェクトでは、一般企業（製造業）を対象とした情報システムを対象に、コンプライアンスのシステム監査基準の策定を目標として研究を行った。システム監査学会との共同プロジェクトであり、今回は最終報告で、実際に使用できるものへのブラッシュアップを目指した。

**①研究の活動実績**

第一期（前期）：2010年1月～2010年8月（8回開催）

コンプライアンス確保のため関連法規を一覧化し、それらの法規に関連する情報システム（ICT）のマップを作成。

第一期（後期）：2010年9月～2011年2月（5回開催）

研究活動の参考のため、有識者による情報提供を受け、研究会メンバーと討議を実施。その結果を受け、前期の成果物の見直しを行った。

第二期：2011年6月～2012年5月（9回開催）

情報システムのコンプライアンス確保のため関連法規を一覧化。それらの法規に関連する情報システムＭＡＰを作成。このＭＡＰをベースにシステム開発を例にシステム管理基準にコンプライアンスに関する脚注を追加。モデル取引、契約の工程をベースにシステム管理基準の内容についてコンプライアンスの観点から課題を抽出。今後はシステム管理基準に対するシステム監査実践マニュアルでの追記の見直しが必要と認識。

第三期：2012年6月～2013年3月（10回開催）

システム管理基準の内、企画、開発、運用、保守業務について検討した。システム管理基準に加える脚注に関して、一層の充実を図り、マニュアル的な活用を目指した。コンプライアンス視点からの具体的な監査ポイントについて議論し、一部を脚注に織り込んだ。課題として挙げられた体系上の位置付けや表現等の整合性について、脚注で可能な限り説明を加えた。

**②成果物（システム管理基準へのコンプライアンス脚注）**

1.コンプライアンスに関する脚注の作成方針

（基本項目）

・権利関係を明確にするために契約上で必要な項目

・法務部門（外部の法律専門家）の参画と連携

・外部委託を前提に委託業務の内容を明確にするための項目

・コンプライアンスリスクに関する検討項目を追加

（追加項目）
・コンプライアンス視点からの具体的な監査ポイントを追加
・体系上の位置付けや表現等の整合性に関する説明を追加
2. 検討に際して発見されたシステム管理基準上の問題点
・モデル契約とシステム管理基準の細目との用語の定義ずれ（例：要件定義と要求定義）
→　本研究プロジェクトはモデル契約にあわせた
・大規模のウォータフォールモデルの開発を対象としているため、現在の開発方法（オープン系、クラウド、パッケージ、アジャイル、中小規模等）とのかい離
→　本研究プロジェクトはウォータフォールモデルを対象とした。
・システム管理基準の細目の記載順序の不整合
→　本研究プロジェクトは現状の記載順序にあわせた。
・システム管理基準へコンプライアンス脚注を付記。斜体文字がコンプライアンス脚注。

| システム管理基準と監査のポイント | 確認すべき資料、確認方法 |
|---|---|
| 1）開発の責任者は、システム分析及び要求定義の手順を明確にしていること。 | 開発業務標準 |
| *契約上の留意点：要求定義の手順も要件定義作成支援業務に含める場合は明確に規定する。* | |
| *契約上の留意点：モデル契約では準委任契約で行うこと。* | |

**【所感】**

システムの開発現場においては認識が甘くなりがちな「情報システムと密接に関連する法的問題」を具体的な事例を交えて説明を受けたことで、コンプライアンスの意義を改めて認識することができた。今期の成果物である「システム管理基準へコンプライアンス脚注」は、ブラッシュアップによってより分かりやすいものへ仕上がり、システム監査の現場において有効に活用していきたいと感じた。

＜報告者　竹下　健一（No.2083）＞

**2. クラウドコンピューティングのシステム監査（最終報告）**

発表者：深瀬　仁　氏（パナソニック溶接システム株式会社）

**【研究の概要】**

クラウドコンピューティング（以下、クラウドと記載）により、これまでの外部委託形態以上に課題が潜在化し、雲のように実態をつかめない世界になってきている。本研究プロジェクトでは、クラウドの研究とともに、情報システム活用の問題、情報データの管理や所有の問題、委託契約問題など、システム監査においてどのような視点やアプローチがあるのか研究を進める。当研究プロジェクトはシステム

監査学会との共同プロジェクトであり、今回は最終報告を行う。

**【活動実績】**

第一期：2010年5月～2011年5月（全7回開催）

クラウドの概念を理解することから始め、研究会にて目指す成果物を選定した。

第二期：2011年6月～2012年5月（全9回開催）

クラウドを対象にしたシステム管理基準の適用を議論しまとめを進めた。

第三期：2012年6月～2013年5月（全6回開催）

システム管理基準のクラウドへの適用が難しいことがわかるようになりながら、クラウドに特化した留意点の考察を進め、今回の最終報告に至った。

**【システム管理基準の適用へのアプローチ】**

・クラウドを活用したシステムの管理水準を一定に保証する何かしらのマネジメント基準が必要との共通認識からスタートし、経済的観点だけでなく、クラウド選択の適正性、クラウド管理の整合性を見極めることが重要であるという視点でアプローチした。

・ システム管理基準を適用するにあたって、オリジナルの管理基準との比較を行えるテンプレートを作成し整理。システム監査ポイントは、クラウド選択の適切性、クラウド管理の整合性にポイントをおいた。

<table>
<tr><th></th><th>システム管理基準と監査のポイント</th><th>確認すべき資料、確認方法</th><th>クラウド区分</th><th>置換・追加区分</th><th>サービス提供会社へのコントロール内容</th></tr>
<tr><td>現</td><td></td><td></td><td colspan="3" rowspan="2">クラウドにおける特性として項目を付加</td></tr>
<tr><td>クラウド</td><td colspan="2">クラウドにおける管理ポイントを記述</td></tr>
</table>

・システム管理基準の適用では、情報戦略・企画、開発、運用、保守、共通の5つのチーム毎に「論点」と「まとめ」を整理した。

**【考察】**

・議論になったポイント、今後の課題

クラウド導入の場合、情報戦略・企画フェーズでのリスクの先読みが重要。短期間で経営・IT両視点で自社のリスクを把握しクラウド導入・継続を判断できるスキルが求められてくる。また、「所有」から「使用」への考えの移行に伴い、自社の情報システム現場での運用業務が減少してくる。自社の情報システム要員がよりユーザ支援を行う業務への配置が高まり、人員計画、教育への反映が必要。

・システム管理基準にて適用できなかった点

利用者が所有しない仕組みのシステム管理基準への適用は難しい。

・システム管理基準適用での総括

クラウド利用者、クラウド事業者、開発ベンダーそれぞれの間で発生するギャップを埋めるために必要なことをルール化することが重要。

・研究会開始当初と比べ、クラウドに求められる内容が大きく変化している。クラウドが今後、より重要なシステムに活用された場合、データの流出、重大事故発生リスクをあらかじめ想定しておくことが大事。クラウドに特化した選定基準、クラウドサービス決定プロセスの策定が必要である。

**【所感】**

クラウドに対するシステム監査について、これまでの研究成果を交えた詳しい説明を受け、「クラウド選択の適切性」と「クラウド管理の整合性」にポイントをおいた視点やアプローチが重要であることを理解することできた。またクラウドに対してはシステム管理基準の適用が容易でないこと、クラウドの役割が大きく変わり続ける中で今後注視すべきことについての話しをお伺いすることができ、知識を整理、補足するのに大変有意義な機会となった。

＜報告者　植垣　雅則（No.1380）＞

**３．BCPと親和性の高い情報処理システムを目指して**

発表者：永田 淳次 氏

**【発表の概要】**

**（１）はじめに**

近年、BCP/BCMの重要性の認識が高まる中、システム監査の対象としてBCP/BCMを取り上げる機会も増加している。BCP研究会では、具体的で実効性のあるシステム監査を実現すべく、複数の観点で議論を進めてきた。今回の報告では、三番目の観点「BCP策定を容易にする情報システム」での議論を通じて整理された内容を紹介する。

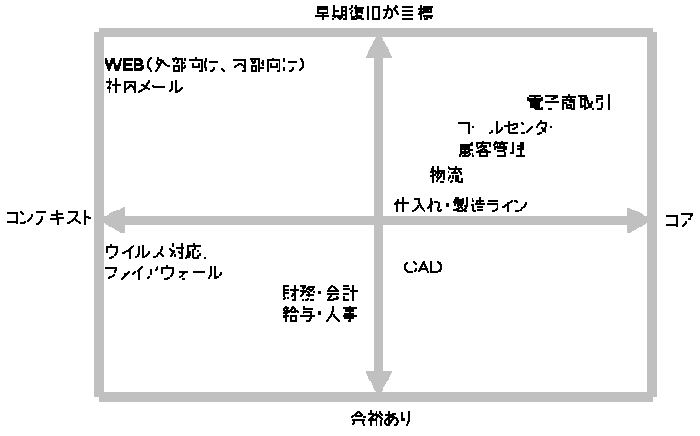
**（２）BCP/BCM**

内閣府の事業継続ガイドラインによると、事業継続計画（BCP）は危機管理や緊急時対応の要素を含む重要なものである。BCPを実践することで、最低限の操業度を確保し、重要業務の操業度を早期に復旧させ、ビジネスへの影響度を小さくしようというものである。BCP/BCMの重要性の認識は高まりつつあるが、大規模大震災の後であってもその策定が十分進んでいるとは言えない。

これらの要因となっているのは、BCP策定方法が分からないだけでなく、人手、時間、コストが不足している等のケースが多いためとみられる。BCP策定には困難さを伴っているため、BCPが簡単で低コストに策定できることが望まれている。

**（３）情報システム**

企業が遂行する業務にはコア業務とコンテキスト業務がある。情報システムも同様に、コア業務用の基幹系システムとコンテキスト業務用の情報システムの二種類がある。BCP策定では、コア業務の情報システムのみが対象となりがちである。しかし、インシデント発生時はコンテキスト業務の情報システムも復旧優先度が高い。復旧の優先度の一例を図に示す。




コンテキスト業務の情報システムは正確な情報収集には必須であるが、対象がコアでないため、軽んじられる傾向にある。図の左上に位置される情報システムが課題を内在しており、十分な投資がされていない場合、柔軟性がなく、融通が利かない情報システムとなり、これを前提にBCPの策定を行うと、膨大な計画書が必要となり、作成や維持に大きな労力が必要となる。

**（４）BCPと情報システム**

BCP策定においても、発展するインターネット技術（クラウドサービス）を活用することが出来るようになってきている。クラウドサービスを利用した情報システムでは、平常時とインシデント発生時でも、その操作に大きな違いはない。これはBCP策定の簡単化につながり、クラウドサービスや共通のネットワークを利用することで操作の複雑性を減少させている。クラウドサービスには他にも多くの特長があり、BCPの策定や維持、改良において、多くのメリットが考えられる。

**（５）事例**

BCP/BCMの浸透度は斑であるが、一部では着実に整備が始まっている。例えばマイクロソフト社は「そして誰もいなくなった」という刺激的なタイトルで震災時のテレワークの実践を紹介し、チャットの有効性と普段使いツールの効果について報告している。幾つかの企業の事例から、コミュニケーションを支援する道具がインシデント発生後の復旧・復興時には核となることが、改めて認識できる。

**（６）まとめ**

BCP策定の重要性は高まっているが、その策定が十分進んでいるとは言えない。その原因の一つに人手、時間、コストがあるため、BCP策定を容易にする情報システムの必要性があると考えた。インシデント発生時はコミュニケーションを司るITがより重要になるが、ノンコア業務であるため、十分な投資は望めない。そこでクラウド等の外部サービスを利用することで、BCP策定に適するITシステムを低コストで構築することができることを示した。

今後、BCP/BCMの存在そのものが、競争力のある戦略となりうる。研究会の活動を通じて、具体的提案となるよう精錬化していきたいと考えている。

**【所感】**

東日本大震災を受けて企業・組織の規模を問わずBCPの整備は重要な課題と認識されているが、その進展は思わしくないのが実情である。本報告は、コンテキスト業務の情報システムとクラウドサービスを結び付けて実例を示し、簡易かつ低コストでの構築のヒントとして有用であると感じた。

＜報告者　金子　力造（№.1531）＞

**４．新しい「IT 事業者評価制度」導入の政策提言**

発表者：中田　和男　氏

SAAJK システム監査法制化プロジェクト：中田和男氏、田淵隆明氏、神尾博氏、横山雅義氏


**【発表の概要】**

現在、IT 事業者の経営力・技術力の諸項目を総合的・客観的に評価する制度・基準は存在しない。そこで新たな「IT 事業者評価制度」の導入を一つの案として提示し、政策提言とする。

**（１）現状の問題点の整理と政策提言のテーマ選定**

政策提言のテーマ選定にあたり、現状の問題点を「規制緩和」の負の側面に焦点を当て総括した。無制限な規制緩和の拡大は、IT の分野においてもネガティブな影響としてソフトウェアの品質悪化や国際競争力の低下に繋がった。今日新たな業界構造変化をとらえ、IT 業界の再生に寄与する政策を提

言できないかと考えた。

**（2）既存の IT 事業者の評価制度の調査 ～当事者の外部からの目線での検証～**

既存の評価制度について考察した結果、SI 登録、SO 認定はすでに廃止されており、ISO、CMMI など国際性はあるが具体性、客観性に弱く、利益相反の疑念を払拭できない。よって新しい IT 事業者評価制度の導入は必須であるとの結論に至った。

**（3）IT 産業の定義と分類**

IT 産業は多岐にわたり、合理的なカテゴライズが必要である。日本標準産業分類に準拠し、情報サービス業およびインターネット付随サービス業の二つとし、さらに小分類において、システム監査業、情報セキュリティ監査業を別枠として新設し、「IT 産業の分類（案)」を提示した。

**（4）新しい「 IT 事業者評価制度」の在り方とは？**

新しい「IT 事業者評価制度」の要件として、以下の 5 点を抽出した。

①技術力のみではなく経営力や社会性等の項目も合わせ事業者全体の力量が評価できること
②IT 事業分野全般を網羅し、適切なカテゴライズがされていること
③認定・非認定の二分法でなく、点数化により各事業者を明確に順位付する相対的評価であること
④制度自体が持続性・柔軟性に優れており、継続的な運用が可能なこと
⑤評価手続きの費用の経済性があり、実務上、申請者の負担にならないこと

さらに実績のある建設業法による経営事項審査制度のフレームワークを活用しつつ、IT 業界の特性・実情を踏まえた採点方式を採用し、綜合評点の算出式及び採点シート（案）を提示した。

**（5）期待される効果～広く国民に受益のある制度～**

本制度の導入により以下の効果が期待できる。

①官公需入札での条件化による、合理的な発注先選定及び成果物品質の向上
②客観的な点数評価及び可視化による（官民問わず)、競争の透明性の確保
③システム監査に際して、関連する開発・運用業者の力量確認の精度向上及び大幅な効率化
④IT 業界の技術者評価への意欲の向上による優良事業者の育成、及び国際競争力の強化

**（6）今後の検討課題**

本研究の課題として、政策実現するためのロビー活動やシステム監査の効率化のための活用方法、SOHO 事業者の取り扱い、高度情報処理技術者のアサインなど検討すべき点は残っている。

**（7）まとめ**

「IT 事業者評価制度」の導入により、IT 事業者を総合的・客観的に評価することが可能になり、システムの発注者側だけでなく、優良 IT 事業者の育成及びシステム監査の分野においても多大な効果が期待できると考える。本制度を実現定着させ、広く国民への受益につなげていく必要がある。

**【所感】**

本研究発表の補足資料として、総合評定通知書の書式サンプル、算出式、採点テーブル、審査項目から評価方法まで、きわめて詳細かつ具体的に提示されていた。システム監査の分野でも、このような定量的な評価基準があることは、監査の効率性や客観性において大いに活用できると思われる。また IT 技術者全体が元気になる、正当に評価される社会を目指すべきであるという提言の理念は素晴らしく、今後の法制化に向けての取り組みに期待したい。

＜報告者　金子　力造（№.1531）＞

**５．対策型監査の効果と重要性**

発表者：木村　修二　氏
情報システム監査株式会社：木村 修二氏、深瀬 知寛氏
コメンテータ：松田　貴典　氏

【発表の概要】

（1）はじめに

ある中央省庁の一機関において実施した新しい対策型監査の手法を素材に、今後の地方自治体における監査のありかたを考える。まず、どうすれば監査が事故（情報漏洩）防止に有効な手段となりえるのか？というのが問題意識としてあった。そこで対策型監査を考え、その具体的な適用例として認証システムを考察した。

（2）情報セキュリティ事故と監査

事例から、規程類が完全に遵守されていれば事故は起きないのか？という疑問が生まれた。内部、外部にかかわらず攻撃者（予備軍）が存在し、攻撃を企て、攻撃が可能な環境なら情報セキュリティ事故は起きる。我々がコントロール出来るのは環境だけ。そこで事故が起きない環境を作り出していくには、攻撃が可能な環境かどうか調査し、事故に直結する具体的な脅威を示し、攻撃の容易さを評価し、事故防止に直結する改善策と、脅威を受容した意思決定を明確にする必要がある。

事故の様態を、情報の入手段階と持ち出し段階に分解して単純化すると対策を実施すべき場所が明確になる。同時に対策が不可能な部分も明確になる。正当権限者の不正行為はアクセス制御でコントロール出来ない。また電子媒体だけでなく脳も外部記憶媒体である。人的対策も出口対策として考慮する必要がある。そこで出口対策を意識した監査のあり方として、

①セキュリティシステムから期待されている機能を洗い出し「期待値」を監査基準に含める。

②「期待値」を含め、受容した脅威を明確化、具体化する。

③「期待値」を実現するための手法を提案する。（改善策の提案）

④新たな脅威を把握する手続きを明文規定する。

このような準拠性監査の拡大を「対策型監査」とした。

（3）認証の課題

認証については、個体認証、主体認証、意図認証、利用目的認証と４つに分類できる。なりすまし対策として主体認証を考えると、例えばWindowsのアクセス制御は、ID、パスワードをかけてもLinuxで起動してデータを回収すれば認証は回避できる。規程類を守ってもこの認証回避は防げない。セキュリティのポイントとしては、受容したリスクの一覧、どこで事故が起きる可能性があるのか、どんな事故が起きる可能性があるのかを一覧表で整理しておくことが重要であると考える。

（4）今後の課題

標的型など新しいタイプの攻撃による出口対策の重視、セキュリティ報告書による関係者への説明、スマホ等の普及による持込規制の無力化など、情報セキュリティは大きな転換点を迎えている。今回認証システムだけを例にしたが、今後さらに範囲を拡大して検討を進めたい。

【コメント】松田　貴典　氏


事故発生の可能性の箇所や認証回避の問題などに着眼し、出口対策の重要性や対策型監査として提言された。実務者として実践的に新しい手法や概念を検証されているところは成果であった。

セキュリティの機能について入口出口の話を主にされていたが、本来は防止制御機能、検知機能、回復機能など３つの機能があり、さらにセキュリティのレイアｰ構造がある。それと入口出口の関係がわかりにくい。また対策提言は、監査ではなくコンサルではないのか？助言型の監査と書かれているが、むしろ保証型ではないのか？論文としては、そのような言葉の意味や定義についてより検討し、論理展開の関連づけをもう少し整理されれば良い論文になると思う。

**【所感】**

日々現場でセキュリティ事故やその防止に直面されている方ならではの臨場感のある発表であった。監査が事故防止に有効な手段であるのか？という問いは､情報セキュリティ監査だけの問題ではなく、システム監査についても同様であり、特に保証型であればその効果や実効性について常に問われる部分である。セキュリティや IT を取り巻く環境は急速に変化しており、監査のあり方について再考しなければならない時期であると痛感した。

＜報告者　植垣　雅則（№.1380）＞

**６．保証型システム監査を可能にするアプローチ**

発表者：松井 秀雄 氏

コメンテータ：中野 節子 氏


**【発表の概要】**

**（１）保証型システム監査とは**

・システム監査の分類：「保証」を与えるものと「助言」を与えるものの２つのタイプが存在する。「助言型」は多く実施されてきたが、「保証型」の事例は少ないのが実情である。

・何を「保証」するのか：被監査組織の情報システム自体やそのガバナンスに関する整備状況や運用

状況自体に対して絶対的な保証を与えるような監査意見を表明する事は極めて困難であり、システム監査人にとってリスクが大きい。しかし、次のような状況を設定すれば、可能と考えられる。

イ．監査対象組織のＩＴ統制状況に関する「言明書」が当該組織の代表者から表明されること

ロ．システム監査人は監査対象組織の統制状況がその言明書に記載されているレベルに達しているかを監査し、達成していると判断した時に保証を与える監査意見を表明する

・保証型システム監査の難しさ：「助言型」に比べて「保証型」のシステム監査においては、監査要点の網羅性、可監査性、根拠の明示、説明責任と言った点でより難しさを伴う。

**（2）保証型システム監査の必要性とその背景**

・システム監査基準に「保証型」が導入された主因として、情報システムが適切に管理されていることについて、ステークホルダー（広義・狭義）への説明責任がより増大したことが挙げられる。

・保証型監査を依頼する側の視点でそのニーズを分類すると、以下の４つが考えられる。システム監査人は依頼者のニーズに対応した保証型システム監査のあり方を考える必要がある。

「経営者のニーズ」「システム委託者のニーズ」「システム受託者のニーズ」「社会のニーズ」

**（3）保証型システム監査と助言型システム監査**

・助言型監査は主に組織内部の改善目的として、保証型監査は主に組織外部の利害関係者を守るため、もしくは判断の材料として利用することを想定していると思われる。

・保証型システム監査の手順においては、助言型と比べると以下のような点で特徴がある。

「言明書」「監査目的」「可監査性要求レベル」「成熟度レベル」「報告内容」

**（4）保証型システム監査の分類定義**

・誰が、何の目的で依頼するのかを考えると、保証型システム監査は次の４分類が考えられる。

①経営者主導方式：経営者が自組織の情報システムの管理レベルを把握したい

②委託者主導方式：委託者が委託先の情報システムの管理レベルを把握したい

③受託者主導方式：受託者が委託元に自組織の情報システムの管理レベルを報告したい

④社会主導方式　：広く社会に自組織の情報システムの管理レベルを表明したい

**（5）類似するその他の保証型監査**

・類似するものとして「保証型情報セキュリティ監査」「委託業務における18号監査（日本公認会計士協会監査基準委員会報告書第18号）」「Trustサービス」がある。

**（6）保証型システム監査の実施手順**

・保証型システム監査の実施手順について、「実施フロー例」と留意点を図示して説明する。

・システム監査人は、以下のプロセスで監査証拠の分析を行い、合意することによって保証意見を表明することが可能である。

検出事項総覧の作成→検出事項総覧の抽出→検出事項の合意→指摘事項の整理→監査意見形成

**（7）まとめ**

・これまで実施されたシステム監査では「助言型」が多く、「保証型」は圧倒的に少ない。当論文は、こうすれば保証型システム監査を実施できるのではないかという可能性を示すべく、成果を纏めたものである。今後も改善を図り、保証型システム監査の事例を増やしていきたい。

**【コメント】**中野 節子 氏

同じシステム監査人の立場としてこのような研究に取り組まれたことに敬意を表する。

保証型システム監査を複数例実施したが、被監査組織が作成する言明書の内容をどうするかで苦労した。公表資料に詳細内容を記載するとセキュリティ上の問題が生じる可能性があることから、概要版と詳細版の2種類の言明書を作成したケースもある。業種業態別の言明書の詳細サンプルを充実させるべく、研究に継続して取り組んでもらいたい。

**【所感】**

保証型システム監査はシステム監査人であれば誰もが取り組んでみたいテーマであると思われる。助言型との比較を通じて特長や留意点、事例を示した本研究報告は、多くのシステム監査人の役に立つものであると感じた。一人のシステム監査人として、保証型システム監査の事例が増えるように努めようと改めて感じた。

＜報告者　是松　徹（№.645）＞

**7．パネルディスカッション　－システム監査 2.0 への進化は可能か－**

モデレータ：吉田　博一　氏

パネラー：浦上　豊蔵　氏、雜賀　努　氏、田淵　隆明　氏、永田　淳次　氏、深瀬　仁　氏

**【概要】**

本パネルディスカッションでは、支部の 4 つの研究プロジェクトから各 1 名と客観的な立場の方 1 名の計 5 名をパネラーに迎え、実際の研究活動成果をパネラー相互や参加者と共有しつつ、吉田前支部長をモデレータとして今後の方向性に関する検討を行った。

冒頭に、モデレータから、支部 20 周年記念シンポジウム（2008 年 7 月）以降、2011 年 8 月開催の研究大会までの支部イベントで採り上げたテーマを振り返り、さらに内外の環境変化を踏まえ、Web2.0 等にちなんだ仮称「システム監査 2.0」への進化が可能かとの問題提起がなされた。

これを受け、各パネラーからは、先に発表のあった研究プロジェクト活動成果に関するコメントが概ね次の流れで提示された。

・研究プロジェクト報告①（コンプラ研）／②（クラウド研）対するコメント：浦上氏
・研究プロジェクト報告③（BCP 研）／④(法制化研)に対するコメント： 雜賀氏
・コメントに対する見解： 雜賀氏、田淵氏、深瀬氏、永田氏

その後、 休憩時間中に回収した研究成果発表に対する会場からの質問票について、該当する研究プロジェクト所属のパネラーから回答を行った。(雜賀氏、田淵氏、深瀬氏、永田氏)

最後にパネラー全員から、システム監査の進化を見据え、最も期待する研究プロジェクトや今後の方向性についてのコメントを提示し、終了となった。


≪モデレータ≫


≪全体風景≫

**【所感】**

今回のパネルディスカッションは、単に一般動向での目新しい事項について議論するのではなく、あくまで実際に活動を行ってきた研究プロジェクトに軸足を置き、その成果と限界を確認しつつ今後の方向性を検討する姿勢であった。J-SOX 本番初年度であった 20 周年記念シンポジウムの時期から 5 年が過ぎ、監査では効率化が求められ、その一方でより対象が多様化してきており、このタイミングで「システム監査の新領域への対応」について検討できたのは時期に適ったものであったと思う。

また、４つの研究プロジェクトのうち２つはプロジェクト終了の位置づけであり、今回のパネルディスカッションを総括として次の新しい研究プロジェクトに成果をつなげていただきたいと考える。

なお、パネラーの数や検討項目の内容等からパネルディスカッションの時間がまだまだ足りないきらいがあったため、「システム監査 2.0 への進化は可能か」は、今後も会員全員で継続して問い続けていきたいテーマであると感じている。

＜アンケート結果＞

（1）アンケート回収結果

| | |
|---|---|
| 参加者数 | 94 |
| アンケート回収数 | 50 |
| アンケート回収率 | 53.2% |

| | | |
|---|---|---|
| 無記名 36 | コメントあり | 14 |
| | コメントなし | 22 |
| 記名あり 14 | コメントあり | 8 |
| | コメントなし | 6 |

（2）評価結果

| 【全体】 | 期待通り | ほぼ期待通り | どちらとも言えない | 多少期待外れ | 期待外れ | 未記入 |
|---|---|---|---|---|---|---|
| 全体の印象 | 13 | 23 | 11 | 1 | 0 | 2 |

| 【報告・発表等】 | 非常に良い | 良い | 普通 | 悪い | 非常に悪い | 未記入 |
|---|---|---|---|---|---|---|
| コンプライアンスのシステム監査 | 9 | 18 | 18 | 3 | 0 | 2 |
| クラウドコンピューティングのシステム監査 | 13 | 17 | 19 | 1 | 0 | 0 |
| BCPと親和性の高い情報処理システムを目指して | 11 | 24 | 13 | 2 | 0 | 0 |
| 新しい「IT事業者評価制度」導入の政策提言 | 9 | 23 | 14 | 4 | 0 | 0 |
| 対策型監査の効果と重要性 | 9 | 21 | 18 | 1 | 1 | 0 |
| 保証型システム監査を可能にするアプローチ | 11 | 25 | 11 | 1 | 0 | 2 |
| パネルディスカッション | 10 | 21 | 7 | 2 | 1 | 9 |
| 記念誌 | 15 | 20 | 10 | 0 | 0 | 5 |

| 【大会運営】 | 非常に良い | 良い | 普通 | 悪い | 非常に悪い | 未記入 |
|---|---|---|---|---|---|---|
| 日程・時間の設定 | 16 | 22 | 11 | 1 | 0 | 0 |
| 時間配分 | 14 | 20 | 12 | 3 | 1 | 0 |
| 募集方法 | 16 | 20 | 13 | 0 | 0 | 1 |
| 参加費用 | 16 | 21 | 10 | 2 | 1 | 0 |

（3）本研究大会を知ったルート

| 【その他】 | メーリングリスト | ホームページ | パンフレット | 友人・知人 | その他 | 未記入 |
|---|---|---|---|---|---|---|
| 情報入手方法 | 29 | 13 | 1 | 2 | 3 | 6 |

（注）複数回答ありのため、合計がアンケート回収人数である50名よりも大きくなっている。

## （4）アンケートの主なコメント

### a）全体の印象

・記念誌をベースに説明があったのでわかりやすかった。テーマも興味深いものだった。
・今後も関西でのシステム監査の活性化の為、尽力していただきたい。
・コンプライアンスＭＡＰ、クラウド選定のポイント、ＢＣＰ策定のポイント等、具体的に為になる発表が多かった。
・論文発表会のような色彩が強く、事例等を期待したのでわかりづらい面があった。パネルディスカッションは良かった。
・実業務への適用方法、効果が読みにくい。ex. 会社法、J-SOX 法、内部監査にどこまで有効に使えるのかが読めない。
・発表者の主張を可能な限り聞けるよう発表時間を長くして欲しい。現行の人数で 2 日間の開催を希望します。(可能であれば)

### b）個別評価

・いずれも中味の濃い内容だったと思います。これだけ深掘りされた皆様に敬意を表します。
・(コンプラ研) 時間が足りなかったように思う。
・(対策型監査) 対策型監査の効果と重要性については、体験型（実務型）の主張と、大学の先生による学問的な観点の両方からの意見があり、非常に分かりやすかった。
・(保証型監査) 保証型に関する発表については、“その時点の状況”を保証することで被監査団体や社会にどのようなメリットがあるのかについて、もう少し深く考察して欲しい。(たとえば、クラウド事業者で実施するとユーザへの説明責任を果たす上で有効になるか等)
・(パネルディスカッション) システム監査 2.0 の意味や方向性がわからなかった。コメントや質問対応とテーマに沿った議論を分けた方が良かったのではないか。

### c）大会運営

・せっかくの開催なので、半日でなく１日とし、１編ごとの発表時間をもう少し長くしても良かったと思う。あるいは、発表に際してポイントを絞る必要があるのでは。
・テーマが多く非常に勉強になったが、講師の方があわただしく説明されており、時間が足りなかったのではないか。
・各報告に対するコメントも報告直後にした方がよかったと思います。(聴取者も印象に残っていますので)

### d）その他

・他に比べてやや発表内容に起承転結がないように思うので、その点の改善が進めば、よりわかりやすい発表になるでしょう。
・記念誌のエッセイはまとめていただいた方が読みやすいと感じました。
・動画サイト等への投稿も考えてはどうか。
・ISO 審査員が助言することがあるように、監査人がコンサルを必要に応じて行うことも必要と考えている。

以上