特定非営利活動法人
SAAJ 日本システム監査人協会報

システム監査基準改訂について

2004年8月　会報編集部

システム監査基準は、8年ぶりに改訂され公表される見込みです。(経済産業省、2004年7月)

今回の改訂の主なポイントは、①IT革新への対応として管理基準の見直し・強化、②事業における情報システムの位置付け変化の対応、③社会に対する説明責任の高まりと保証型監査の必要性、④情報システム管理と監査人の行為規範の峻別、⑤情報セキュリティ監査制度とシステム監査は別ものであるという関係の明確化とされています。

当協会の会員諸氏にとりましても、システム監査基準は日常のシステム監査業務の基本となる基準であり、技術革新の急速な進化や企業組織の社会的責任を問う流れの中での待望の改訂です。

システム監査基準を利用する機会は、内部監査、外部監査ともに、ニーズが高まっています。今回は、改訂の流れを整理して紹介するとともに、今後の活用のあり方について考えていきます。

1. システム監査基準改訂の経緯

財団法人日本情報処理開発協会（JIPDEC）のシステム監査基準検討委員会（委員長　鳥居壮行　駿河台大学文化情報学部教授）は、システム監査基準（案）及びシステム管理基準（案）をとりまとめ、パブリックコメントを求めておりましたが、このたび、各種意見に対する対応や回答のステップを終了し、新システム監査基準およびシステム管理基準として公開されました。

財団法人日本情報処理開発協会のホームページによると、今回のシステム監査基準改訂の経緯について”システム監査基準の改訂にあたって”（2004年4月14日）と題して次のとおり説明されており、改訂の考え方を知ることができます。

【システム監査基準の改訂にあたって】

(http://www.jipdec.jp/ の掲載記事)

1. 今回の「システム監査基準」改訂の背景と意義

「システム監査基準」は、昭和60年(1985年)1月に策定されました。その後、平成8年(1996年)1月に改訂され、今回は2度目の改訂となります。前回の改訂から8年が経ちますが、その間、情報システムは、経済・社会の「神経系」ともいうべき位置付けを占めるようになり、企業経営等の根幹に大きな影響を与えるようになってきました。また、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てきました。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です。　また、2003年4月より経済産業省では「情報セキュリティ監査制

目　次

度」の運用を開始しました。現行のシステム監査においても情報セキュリティ確保の観点からの監査も行われているなど、両者の関係を整理する必要があることから、基準改訂にあたっては、情報セキュリティ監査制度を構成する「情報セキュリティ管理基準・監査基準」との関係を整理し、監査の利用者にとって選択のしやすい形にすることを目指しました。

2. 改訂のポイント

以上の背景と意義を踏まえ、以下の5点を中心とした改訂案を策定しました。

(1) IT技術の革新への対応

IT技術は日進月歩で進歩しており、数年前には考えられなかったことが現実となっています。とりわけ近年ブロードバンドが普及し世界中がインターネットでリアルタイムに接続されるようになりましたが、このネットワーク化に伴い情報システムの形態、その開発・管理手法は大きく変化しています。これと同時に、情報システムを巡るリスクは拡大するとともに、その質も大きく変化していると言えます。そのため、情報システムのライフサイクルの各段階におけるリスクを適切にコントロールすることがより必要とされており、基準にはこれらの変化に対応した新たな管理項目を追加しました。

(2) 事業における情報システムの位置づけの変化への対応

多くの企業や組織では、事業を行うに当たって情報システムが広範に用いられ、組織の戦略や目的達成に大きく関わっています。そのため、組織の経営戦略とIT戦略を整合させ、IT投資を適切に管理し、IT要員やその体制、ITに関するリスクのコントロールなどフレームワークを確立する「ITガバナンス」が極めて重要となっています。今回の改訂に当たっては、「ITガバナンス」という新たな概念を意識し、組織運営の観点から情報システムを見直すための要素を追加しました。

(3) 社会に対する説明責任の高まりと保証型監査の必要性

有効かつ効率的な組織運営のためには情報システムの活用は不可欠であり、情報システム自体の有効かつ効率的な運営が重要となっています。そのため組織の代表者は、情報システムが組織の目標及び戦略に合致していること、安全、有効かつ効率的に運営されていること、情報システム及びデータが信頼のおけるものであること、法令を遵守していることを国民、投資家、取引先を始めとする利害関係者に説明できる状態にしておくことが必要となります。そのためには、従来の助言型によるシステム監査に加え、保証型のシステム監査を行うことが必要であり、その要素を追加しました。

(4)「情報システム管理の標準」と「監査人の行為規範」の峻別

現行「システム監査基準」を、情報システム部門及びその関連部門が遵守すべき情報システム管理の標準たる「システム管理基準」と、監査人の行為規範たる「システム監査基準」に峻別しました。情報システム部門及びその関連部門は「システム管理基準」を標準として自らの組織の情報システムの管理を行い、システム監査人は「システム監査基準」に照らして監査を行うという関係（注）を明確にしました。これにより、情報システム管理は、まず経営者の責任において行われ、システム監査人はその遵守状況を保証又は遵守できていない部分が遵守できるように助言する立場にあることが明確となりました。

(5) 情報セキュリティ監査制度との関係

経済産業省は情報セキュリティ確保の観点から監査を行う「情報セキュリティ監査制度」を2003年4月から運用開始しました。「システム監査」においてもこれまでセキュリティ確保の観点からも監査が行われてきましたが、「システム監査」と「情報セキュリティ監査」とは、目的及びその成り立ちが異なり、ユーザ（被監査主体）のニーズ及び要請に応じて適切に選択されるべきものであります。改訂に当たっては、新「システム管理基準」及び新「システム監査基準」の前文に上記の趣旨を盛り込むとともに、基準の前文や項目にも関係整理を明記しているところです。

ここまでが、JIPDECのサイト（http://www.jipdec.jp/）に公表された説明です。当協会の会員の多くが監査を実施する側の立場であることからすると、もう一歩踏み込んだ内容を期待するところも大きいのが実情ではないでしょうか。

「基準解説書」への期待も膨らみますが、技術革新とともに組織のありかたや運用実態も変化していきます。

システム監査の現場では、課題に対する目的を問いながら、専門家として個々の事例への対処と経験を積み重ねることが、情報システムの多様化や複雑化への対応であり、ITを活用する上での経営課題の解決に寄与する方向であろうと思われます。

2. パブリックコメントの実施状況

平成15年6月　システム監査基準検討委員会設置
平成15年7月～9月　システム監査基準検討委員会で、基準改訂の検討開始
平成15年9月～16年3月 具体的な各基準項目の検討作業を実施（2つのWG）
平成16年4月　原案とりまとめ
平成16年4月14日（水）～5月14日　パブリックコメント実施（意見募集）
意見総数　210件（26名）
提出された意見および回答は、フィードバックとして次のサイトから参照できる。
(http://www.jipdec.jp/security/safeedback.htm)

フィードバックの内容

1「システム管理基準（案）/システム監査基準（案）に対する意見及び回答（共通）」
2「システム管理基準（案）に対する意見及び回答（全体）」
3「システム管理基準（案）に対する意見及び回答（前文）」
4「システム管理基準（案）に対する意見及び回答（基準項目）」
5「システム監査基準（案）に対する意見及び回答」
6「システム管理基準（案）新旧対照表」
7「システム監査基準（案）新旧対照表」

3. 経済産業省による公表

経済産業省は、「情報セキュリティに関する政策、緊急情報」のサイトを活用して公表している。
(http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm)

このサイトは、最近の話題となる政策をまとめたもので、情報セキュリティ総合戦略、電子署名、セキュリティ評価・認証、暗号技術評価、情報セキュリティ監査制度、などとともに「法律、ガイドライン等」という見出しの中でシステム監査制度が公示されている。

●システム管理基準（平成16年7月）【PDF形式：31KB】

●システム監査基準（平成16年7月）【PDF形式：31KB】

なお当協会では、7月27日の月例研究会の場で、発表間近の改訂システム監査基準、管理基準を取り上げ、改定作業に直接関わった委員の一人である、当協会の本田理事にご講演頂きました。

改訂システム監査基準、管理基準の発表直前（本来は直後を狙っていたのですが）の本格的な講演会となりました。

本田理事の講演内容は、第105回月例研究会報告として掲載しております。

「システム監査基準（案）」、「システム管理基準（案）」は、JIPDECサイトから公開されており、ダウンロードできます。(http://www.jipdec.jp/)

以上（文責　竹下和孝）

システム管理基準(案)

前文

今日組織体の情報システムは、それ自体経営戦略と一体となって、組織体のインフラストラクチャとして構築されている。このように重要な情報システムを脅かすリスクはますます多様化し複雑化しているが、それらを適切にコントロールすることが重要な課題となっている。システム監査は、組織体の情報システムのリスクに対するコントロールが、適切に整備・運用されていることを担保するための有効な手段となる。またシステム監査は、これらを通じて組織体のITガバナンスの実現に寄与するものである。

情報システムに対するコントロールを適切に整備・運用する目的は、以下のような範疇に分けることができる。

・情報システムが、経営方針、戦略目標の実現に貢献している。
・情報システムが、組織の目的を実現するように安全、有効かつ効率的に機能している。
・情報システムが、内部又は外部に報告する情報の信頼性が保たれるように機能している。
・情報システムが、関連法規、契約又は内部規程等に準拠している。

システム管理基準は、組織体が主体的に組織全体の戦略に沿って効果的な情報システム戦略を立てるための実践規範である。本管理基準は組織体が情報システムを導入するにあたり企画・開発・運用・保守という基本的な枠組みと具体的な管理項目を提示することにより、組織体が情報システムのライフサイクルプロセスに従って、効果的な情報システム投資と、適切なコントロールの整備と運用を導入できるように支援することを目的としている。

本管理基準は、組織体の業種及び規模等を問わず適用できるよう汎用的なものとなっている。ただし情報システムは、組織全体の戦略及び事業プロセスと、コントロールの項目が相互に結びつき合って初めて最適化され、有効に機能するものである。よって本管理基準は組織運営の戦略を司る広範なものであり、情報技術などをもって全体最適化を目指すこととなる。

情報システムのセキュリティ関連項目については、システム管理基準においても管理項目として挙げられるが、情報セキュリティ確保の観点から監査する場合は、情報セキュリティ監査制度における情報セキュリティ管理基準を活用して実施することが要請される。

システム管理基準は、本管理基準と姉妹編をなすシステム監査基準に従って監査を行う場合、原則として、監査人が監査上の判断の尺度として用いるべき基準となる。なお、組織体が属する業界又は事業活動特性等を考慮して、必要ある場合には、本管理基準の趣旨及び体系に則って、該当する関係機関などにおいて独自の管理基準を策定し活用することが望ましい。また、時々の関連技術動向、関連法令などを考慮し、それらを反映した詳細なサブコントロール項目を策定することが望ましい。

システム管理基準(270項目)

Ⅰ.情報戦略(47項目)

1.全体最適化(18)

1.1 全体最適化の方針・目標(6)

(1) ITガバナンスの方針を明確にすること。
(2) 情報化投資や情報化構想の決定における原則を定めること。
(3) 情報システム全体の最適化目標を経営戦略に基づいて設定すること。
(4) 組織体全体の情報システムのあるべき姿を明確にすること。
(5) システム化によって生ずる組織及び業務の変更の方針を明確にすること。
(6) 情報セキュリテイ基本方針を明確にすること。

1.2 全体最適化計画の承認 (3)

(1) 全体最適化計画の立案体制は、組織体の長の承認を得ること。

(2) 全体最適化計画は、組織体の長の承認を得ること。

(3) 全体最適化計画は、利害関係者の合意を得ること。

1.3 全体最適化計画の策定 (7)

(1) 全体最適化計画は、方針・目標に基づいていること。

(2) 全体最適化計画は、コンプライアンスを考慮すること。

(3) 全体最適化計画は、情報化投資の方針と確保すべき経営資源を明確にすること。

(4) 全体最適化計画は、投資効果とリスク算定の方法を明確にすること。

(5) 全体最適化計画は、システム構築・運用のための標準化を含めたルールを明確にすること。

(6) 全体最適化計画は、個別の開発計画の優先順位と順位付けのルールを明確にすること。

(7) 全体最適化計画は、外部資源の活用を考慮すること。

1.4 全体最適化計画の運用 (2)

(1) 全体最適化計画は、関係者に周知徹底すること。

(2) 全体最適化計画は、定期的及び経営環境等の変化に対応して見直すこと。

2. 組織体制 (9)

2.1 情報システム化委員会 (5)

(1) 全体最適化計画に基づき、委員会の使命を明確にし、適切な権限と責任を与えること。

(2) 委員会は、組織体における情報システムに関する活動全般について、モニタリングを実施し、必要に応じて是正措置を講じること。

(3) 委員会は、情報技術の動向に対応するため、技術採用指針を明確にすること。

(4) 委員会は、活動内容を組織体の長に報告すること。

(5) 委員会は、意思決定を支援するための情報を組織体の長に提供すること。

2.2 情報システム部門 (2)

(1) 情報システム部門の使命を明確にし、適切な権限と責任を与えること。

(2) 情報システム部門は、組織体規模・特性に応じて、職務の分離、専門化、権限付与、外部委託等を考慮した体制にすること。

2.3 人的資源管理の方針 (2)

(1) 情報技術に関する人的資源の現状及び必要とされる人材を明確にすること。

(2) 人的資源の調達及び育成の方針を明確にすること。

3. 情報化投資 (6)

(1) 情報化投資計画は、経営戦略と整合性がとれること。

(2) 情報化投資計画の決定に際して、影響、効果、期間、実現性等の観点から複数の選択肢を検討すること。

(3) 情報化投資に関する予算を適時に執行すること。

(4) 情報化投資に関する投資効果の算出方法を明確にすること。

(5) 情報システムの全体的な業績や個別のプロジェクトの業績を財務的な観点から評価し、問題点に対して対策を講じること。

(6) 投資した費用が適正に使用されたことを確認すること。

4. 情報資産管理の方針 (4)

(1) 情報資産の管理方針と体制を明確にすること。
(2) 情報資産のリスク分析を行い、その対応策を考慮すること。
(3) 情報資産の効率的で有効な活用を考慮すること。
(4) 情報資産の共有化による生産性向上を考慮すること。

5. 事業継続計画 (5)

(1) 情報システムに関連した事業継続の方針を策定すること。
(2) 事業継続計画は、利害関係者を含んだ組織的体制で立案し、組織体の長が承認すること。
(3) 事業継続計画は、従業員の教育訓練の方針を明確にすること。
(4) 事業継続計画は、関係各部に周知徹底すること。
(5) 事業継続計画は、必要に応じて見直すこと。

6. コンプライアンス (5)

(1) 法令·規範の管理体制を確立するとともに、管理責任者を定めること。
(2) 遵守すべき法令·規範を識別し、関係者に教育·周知徹底すること。
(3) 情報倫理規程を定め、関係者に教育·周知徹底すること。
(4) 個人情報の取扱い、知的財産権の保護、外部へのデータ提供に関する方針を定めること。
(5) 法令·規範および情報倫理規程の遵守状況を評価し、改善のために必要な方策を講じること。

Ⅱ. 企画業務 (23 項目)

1. 開発計画 (9)

(1) 開発計画は、組織体の長が承認すること。
(2) 開発計画は、全体最適化計画との整合性を考慮して策定すること。
(3) 開発計画は、目的、対象業務、費用、スケジュール、開発体制、投資効果等を明確にすること。
(4) 開発計画は、関係者の教育·訓練計画を明確にすること。
(5) 開発計画は、ユーザ部門と情報システム部門の役割分担を明確にすること。
(6) 開発計画は、開発、運用及び保守費用の算出基礎を明確にすること。
(7) 開発計画は、情報システムライフを設定する条件を明確にすること。
(8) 開発計画の策定に当たっては、システムの特性及び開発の規模を考慮しシステムの形態、開発方法を決定すること。
(9) 開発計画の策定に当たっては、情報システムの目的を達成する実現可能な代替案を作成し、検討すること。

2. 分析 (8)

(1) 開発計画に基づいた要求定義は、ユーザ、開発、運用及び保守の責任者が承認すること。
(2) ユーザニーズの調査は、対象、範囲及び方法を明確にすること。
(3) 実務に精通しているユーザ、開発、運用及び保守担当者が参画して現状分析を行うこと。
(4) ユーザニーズは文書化し、ユーザ部門が確認すること。
(5) 情報システムの導入に伴って発生する可能性のあるリスク分析を実施すること。
(6) 情報システムの導入によって影響を受ける業務、管理体制、諸規程等は、見直し等の検討を行うこと。
(7) 情報システムの効果の定量的及び定性的評価を行うこと。

(8) パッケージソフトウェアの使用にあたっては、ユーザニーズとの適合性を検討すること。

3. 調達 (6)

(1) 調達の要求事項は、開発計画及びユーザニーズに基づき作成し、ユーザ、開発、運用及び保守の責任者が承認すること。
(2) ソフトウェア、ハードウェア、ネットワークは、調達の要求事項を基に選択すること。
(3) 開発を遂行するために必要な要員、予算、設備、期間等を確保すること。
(4) 要員に必要なスキルを明確にすること。
(5) ソフトウェア、ハードウェア、ネットワークの調達はルールに従って実施すること。
(6) 調達した資源は、ルールに従って管理すること。

Ⅲ. 開発業務 (51 項目)

1. 開発手順 (4)

(1) 開発手順は、開発の責任者が承認すること。
(2) 開発手順は、開発方法に基づいて作成すること。
(3) 開発手順は、開発の規模、システム特性等を考慮して決定すること。
(4) 開発時のリスクを回避する手段を講じること。

2. システム設計 (14)

(1) システム設計書は、ユーザ、開発、運用及び保守の責任者が承認すること。
(2) 運用の基本方針を定め、運用設計を行うこと。
(3) 入出力画面、入出力帳票等はユーザの利便性を考慮して設計すること。
(4) データベースは、業務の内容に応じて設計すること。
(5) データのインテグリティを確保すること。
(6) ネットワークは、業務の内容に応じて設計すること。
(7) 情報システムの性能は、要求定義を満たすこと。
(8) 情報システムの保守性を考慮して設計すること。
(9) 他の情報システムとの整合性を考慮して設計すること。
(10) 情報システムの障害対策を考慮して設計すること。
(11) 誤謬防止、不正防止、機密保護等を考慮して設計すること。
(12) テスト計画は、目的、範囲、方法、スケジュール等を明確にすること。
(13) 情報システムの利用に係る教育の方針、スケジュール等を明確にすること。
(14) モニタリング機能を考慮して設計すること。

3. プログラム設計 (5)

(1) プログラム仕様書は、開発の責任者が承認すること。
(2) システム設計書に基づいて、プログラムを設計すること。
(3) テスト要求事項を定義し、文書化すること。
(4) プログラム設計書及びテスト要求事項をレビューすること。
(5) プログラム設計時に発見したシステム設計の矛盾は、システム設計の再検討を行って解決すること。

4. プログラミング (4)

(1) プログラム仕様書に基づいてプログラミングしていることを検証すること。
(2) プログラムコードはコーディング標準に適合していることを検証すること。
(3) プログラムコード及びプログラムテスト結果を評価し、記録及び保管すること。
(4) 重要プログラムは、プログラム作成者以外の者がテストすること。

5. システムテスト・ユーザ受入れテスト (14)

(1) システムテスト計画は、開発及びテスト責任者が承認すること。
(2) ユーザ受入れテスト計画は、開発及びユーザ部門の責任者が承認すること。
(3) システムテストに当たっては、システム要求事項を網羅してテストケースを設定して行うこと。
(4) テストデータの作成及びシステムテストは、テスト計画に基づいて行うこと。
(5) システムテストは、本番環境と隔離された環境で行うこと。
(6) システムテストは、開発当事者以外の者が参画すること。
(7) システムテストは、適切なテスト手法や標準を使用すること。
(8) ユーザ受入れテストは、本番同様の環境を設定すること。
(9) ユーザ受入れテストは、ユーザマニュアルに従い、本番運用を想定したテストケースを設定して実施すること。
(10) ユーザ受入れテストは、ユーザ及び運用担当者もテストに参画して確認すること。
(11) システムテスト、ユーザ受入れテストの結果は、開発、運用、保守及びユーザの責任者が承認すること。
(12) システムテスト、ユーザ受入れテストの経過及び結果を記録及び保管すること。
(13) パッケージソフトウェアを調達する場合、開発元が品質テストを実施したかを確認すること。
(14) データセンタ等のサービス提供を受ける場合、供給元でのシステムテストに係るシステム監査の実施状況を確認すること。

6. 移行 (8)

(1) 移行計画を策定し、ユーザ、開発、運用及び保守部門の責任者が承認すること。
(2) 移行作業は文書に記録し、責任者が承認すること。
(3) 移行計画に基づいて、移行に必要な要員、予算、設備等を確保すること。
(4) 移行は手順書を作成し、実施すること。
(5) 移行時のリスク対策を検討すること。
(6) 移行完了の検証方法を明確にすること。
(7) 運用及び保守に必要なドキュメント、各種ツール等は開発の責任者から引き継いでいること。
(8) 移行は関係者に周知徹底すること。

7. 旧情報システムの廃棄 (2)

(1) 旧情報システムは、リスクを考慮して廃棄計画を策定し、運用及びユーザの責任者の承認を得て廃棄すること。
(2) 旧情報システムの廃棄方法及び廃棄時期は、不正防止及び機密保護の対策を考慮して決定すること。

Ⅳ. 運用業務 (72 項目)

1. 運用の基本方針 (4)

(1) 運用管理ルール及び運用手順は、運用の責任者が承認すること。
(2) 運用管理ルールは、運用設計に基づいて作成すること。
(3) 運用手順は、運用設計及び運用管理ルールに基づいて、規模、期間、システム特性等を考慮し作成すること。
(4) 運用設計及び運用管理ルールに基づいて、担当責任者を定めること。

2. 運用管理 (16)

(1) 年間運用計画を策定し、責任者が承認すること。
(2) 年間運用計画に基づいて、月次・日次等の運用計画を策定すること。
(3) 運用管理ルールを遵守すること。
(4) 事故及び障害の影響度に応じた報告体制・対応手順を明確にすること。
(5) ジョブスケジュールは、業務処理の優先度を考慮して設定すること。
(6) オペレーションは、ジョブスケジュール及び指示書に基づいて行うこと。
(7) 例外処理のオペレーションは、運用管理ルールに基づいて行うこと。
(8) オペレータの交替は、運用管理ルールに基づいて行うこと。
(9) ジョブスケジュールとオペレーション実施記録を採り、ジョブスケジュールとの差異分析を行うこと。
(10) オペレーション実施記録は、運用管理ルールに基づいて一定期間保管すること。
(11) 事故及び障害の内容を記録し、情報システムの運用の責任者に報告すること。
(12) 事故及び障害の原因を究明し、再発防止の措置を講じること。
(13) 情報システムのユーザに対する支援体制を確立すること。
(14) 情報セキュリティに関する教育及び訓練をユーザに対して実施すること。
(15) 情報システムの稼動に関するモニタリング体制を確立すること。
(16) 情報システムの稼動実績を把握し、性能管理及び資源の有効利用を図ること。

3. 入力管理 (5)

(1) 入力管理ルールを定め、遵守すること。
(2) データの入力は、入力管理ルールに基づいて漏れなく、重複なく、正確に行うこと。
(3) 入力データの作成手順、取扱い等は誤謬防止、不正防止、機密保護等の対策を講じること。
(4) データの人力の誤謬防止、不正防止、機密保護等の対策は有効に機能すること。
(5) 入力データの保管及び廃棄は、人力管理ルールに基づいて行うこと。

4. データ管理 (10)

(1) データ管理ルールを定め、遵守すること。
(2) データへのアクセスコントロール及びモニタリングは、有効に機能すること。
(3) データを適切な状態に維持すること。
(4) データの利用状況を記録し、定期的に分析すること。
(5) データのバックアップの範囲、方法及びタイミングは、業務内容、処理形態及びリカバリの方法を考慮して決定すること。
(6) データの授受は、データ管理ルールに基づいて行うこと。
(7) データの交換は、不正防止及び機密保護の対策を講じること。

(8) データの保管、複写及び廃棄は、誤謬防止、不正防止及び機密保護の対策を講じること。
(9) データに対するコンピュータウイルス対策を講じること。
(10) データの知的財産権を管理すること。

5. 出力管理 (7)

(1) 出力管理ルールを定め、遵守すること。
(2) 出力情報は、漏れなく、重複なく、正確であることを確認すること。
(3) 出力情報の作成手順、取扱い等は、誤謬防止、不正防止及び機密保護の対策を講じること。
(4) 出力情報の引渡しは、出力管理ルールに基づいて行うこと。
(5) 出力情報の保管及び廃棄は、出力管理ルールに基づいて行うこと。
(6) 出力情報のエラー状況を記録し、定期的に分析すること。
(7) 出力情報の利用状況を記録し、定期的に分析すること。

6. ソフトウェア管理 (9)

(1) ソフトウェア管理ルールを定め、遵守すること。
(2) ソフトウェアへのアクセスコントロール及びモニタリングは、有効に機能すること。
(3) ソフトウェアの利用状況を記録し、定期的に分析すること。
(4) ソフトウェアのバックアップの範囲、方法及びタイミングは、業務内容及び処理形態を考慮して決定すること。
(5) ソフトウェアの授受は、ソフトウェア管理ルールに基づいて行うこと。
(6) ソフトウェアの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。
(7) ソフトウェアに対するコンピュータウイルス対策を講じること。
(8) ソフトウェアの知的財産権を管理すること。
(9) フリーソフトウェアの利用に関し、組織体としての方針を明確にすること。

7. ハードウェア管理 (6)

(1) ハードウェア管理ルールを定め、遵守すること。
(2) ハードウェアは、想定されるリスクを回避できる環境に設置すること。
(3) ハードウェアは、定期的に保守を行うこと。
(4) ハードウェアは、障害対策を講じること。
(5) ハードウェアの利用状況を記録し、定期的に分析すること。
(6) ハードウェアの保管、移設及び廃棄は、不正防止及び機密保護の対策を講じること。

8. ネットワーク管理 (6)

(1) ネットワーク管理ルールを定め、遵守すること。
(2) ネットワークへのアクセスコントロール及びモニタリングは、有効に機能すること。
(3) ネットワーク監視ログを定期的に分析すること。
(4) ネットワークは、障害対策を講じること。
(5) ネットワークの利用状況を記録し、定期的に分析すること。
(6) ネットワークを利用したサービスについて、組織体としての方針を明確にすること。

9. 構成管理 (4)

(1) 管理すべきソフトウェア、ハードウェア及びネットワークの対象範囲を明確にし、管理すること。
(2) ソフトウェア、ハードウェア及びネットワークの構成、購入先、サポート条件等を明確にすること。
(3) ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、影響を受ける範囲を検討して決定すること。
(4) ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、計画的に実施すること。

10. 建物・関連設備管理 (5)

(1) 建物及び関連設備は、想定されるリスクを回避できる環境に設置すること。
(2) 建物及び室への入退の管理は、不正防止及び機密保護の対策を講じること。
(3) 関連設備は、定期的に保守を行うこと。
(4) 関連設備は、障害対策を講じること。
(5) 建物及び室への入退の管理を記録し、定期的に分析すること。

Ⅴ. 保守業務 (17 項目)

1. 保守手順 (3)

(1) 保守ルール及び保守手順は、保守の責任者が承認すること。
(2) 保守手順は、保守の規模、期間、システム特性等を考慮して決定すること。
(3) 保守時のリスクを回避する手段を講じること。

2. 保守計画 (3)

(1) 保守計画は保守及びユーザの責任者が承認すること。
(2) 変更依頼等に対し、保守の内容及び影響範囲の調査並びに分析を行うこと。
(3) 保守のテスト計画は、目的、範囲、方法、スケジュール等を明確にすること。

3. 保守の実施 (3)

(1) システム設計書、プログラム仕様書等は、保守計画に基づいて変更し、保守及びユーザの責任者が承認すること。
(2) プログラムの変更は、保守手順に基づき、保守の責任者の承認を得て実施すること。
(3) 変更したプログラム仕様書に基づいてプログラミングしていることを検証すること。

4. 保守の確認 (5)

(1) 変更したプログラムのテストの実施は、保守のテスト計画に基づいて行うこと。
(2) 変更したプログラムは、影響範囲を考慮してテストを行うこと。
(3) 変更したプログラムのテストは、ユーザが参画し、ユーザマニュアルに基づいて実施すること。
(4) 変更したプログラムのテストの結果は、開発、運用、保守及びユーザの責任者が承認すること。
(5) 変更したプログラムのテストの結果を記録及び保管すること。

5. 移行 (3)

(1) 移行手順は、移行の条件を考慮して作成すること。
(2) 変更前のプログラム及びデータのバックアップを行うこと。
(3) 運用の責任者は、他の情報システムへ影響を与えていないことを検証すること。

Ⅵ. 共通業務 (60 項目)

1. ドキュメント管理 (9)

1.1 作成 (5)

(1) ドキュメントは、情報システム部門及びユーザ部門の責任者が承認すること。
(2) ドキュメント作成ルールを定め、遵守すること。
(3) ドキュメントの作成計画を策定すること。
(4) ドキュメントの種類、目的、作成方法等を明確にすること。
(5) ドキュメントは、作成計画に基づいて作成すること。

1.2 管理 (4)

(1) ドキュメントの更新内容は、情報システム部門及びユーザ部門の責任者が承認すること。
(2) ドキュメント管理ルールを定め、遵守すること。
(3) 情報システムの変更に伴い、ドキュメントの内容を更新し、更新履歴を記録すること。
(4) ドキュメントの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。

2. 進捗管理 (6)

2.1 実施 (3)

(1) 進捗計画に基づいて方法、体制等を定め、企画、開発、運用及び保守の業務の責任者が承認すること。
(2) 企画、開発、運用、保守の各業務の責任者は、進捗状況を把握すること。
(3) 進捗の遅延等の対策を講じること。

2.2 評価 (3)

(1) 業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。
(2) 評価結果は、次工程の計画に反映すること。
(3) 評価結果は、進捗管理の方法、体制等の改善に反映すること。

3. 人的資源管理 (13)

3.1 責任·権限 (3)

(1) 要員の責任及び権限は、業務の特性に応じて定めること。
(2) 要員の責任及び権限は、情報環境の変化に対応した見直しを行うこと。
(3) 要員の責任及び権限を周知徹底すること。

3.2 業務遂行 (4)

(1) 要員は、権限を遵守すること。
(2) 作業分担及び作業量は、要員の知識、能力等から検討すること。
(3) 要員の交替は、誤謬防止、不正防止及び機密保護を考慮して行うこと。
(4) 不測の事態に備えた代替要員の確保を検討すること。

3.3 教育·訓練 (4)

(1) 教育及び訓練のカリキュラムは、情報戦略に基づいて作成及び見直しを行うこと。
(2) 教育及び訓練のカリキュラムは、技術力の向上、業務知識の習得、情報システムの情報セキュリティ確保等から検討すること。

(3) 教育及び訓練は、カリキュラムに基づいて定期的かつ効果的に行うこと。
(4) 要員に対するキャリアパスを確立し、情報環境の変化に対応した見直しを行うこと。

3.4 健康管理 (2)
(1) 健康管理を考慮した作業環境を整えること。
(2) 健康診断及びメンタルケアを行うこと。

4. 外部委託・受託 (25)

4.1 計画 (3)
(1) 委託または受託の計画は全体最適化計画に基づいて策定し、責任者が承認すること。
(2) 委託または受託の目的、対象範囲、予算、体制等を明確にすること。
(3) 委託または受託は、具体的な効果、問題点等を評価して決定すること。

4.2 委託先選定 (3)
(1) 委託先の選定基準を明確にすること。
(2) 委託候補先に必要な要求仕様を提示すること。
(3) 委託候補先が提示した提案書の比較検討を行うこと。

4.3 委託契約 (8)
(1) 契約は、委託契約ルールまたは受託契約ルールに基づいて締結すること。
(2) コンプライアンスに関する条項を明確にすること。
(3) 再委託の可否について明確にすること。
(4) 知的財産権の帰属を明確にすること。
(5) 特約条項及び免責条項を明確にすること。
(6) 業務内容及び責任分担を明確にすること。
(7) 契約締結後の業務内容に追加・変更が生じた場合、契約内容の再検討を行うこと。
(8) システム監査に関する方針を明確にすること。

4.4 委託業務 (7)
(1) 委託業務の実施内容は、契約内容と一致すること。
(2) 契約に基づき、必要な要求仕様、データ、資料等を提供すること。
(3) 委託業務の進捗状況を把握し、遅延対策を講じること。
(4) 委託先における誤謬防止、不正防止、機密保護等の対策の実施状況を把握し、必要な措置を講じること。
(5) 成果物の検収は、委託契約に基づいて行うこと。
(6) 業務終了後、委託業務で提供したデータ、資料等の回収、廃棄の確認を行うこと。
(7) 委託した業務の結果を分析及び評価すること。

4.5 受託業務 (4)
(1) 受託業務の実施内容は、契約内容を遵守すること。
(2) 受託内容の進捗状況を把握し、リスク対策を講じること。
(3) 成果物の品質管理を行うこと。
(4) 契約に基づき、受託業務終了後、提供されたデータ、資料、機材等を返却または廃棄すること。

5. 変更管理 (6)

5.1 管理 (3)

(1) 変更管理ルールを定め、責任者が承認すること。

(2) 仕様変更、問題点、ペンディング事項等の変更管理案件が生じた場合、他システムの影響を考慮して決定すること。

(3) 変更管理案件は、提案から完了までの状況を管理し、未完了案件は定期的に分析すること。

5.2 実施 (3)

(1) 変更管理案件は、変更管理ルールに従って実施すること。

(2) 変更管理案件を実施した場合に、関連するシステム環境も同時に変更すること。

(3) 変更の結果は、責任者が承認すること。

6. 情報セキュリティ (1)

6.1 情報セキュリティ監査 (1)

(1) その他詳細な情報セキュリティ管理項目に関しては、情報セキュリティ管理基準を活用すること。

システム監査基準（案）

前文

今日組織体の情報システムは、それ自体経営戦略と一体となって、組織体のインフラストラクチャとして構築されている。このように重要な情報システムを脅かすリスクはますます多様化し複雑化しているが、それらを適切にコントロールすることが重要な課題となっている。システム監査は、組織体の情報システムのリスクに対するコントロールが、適切に整備・運用されていることを担保するための有効な手段となる。またシステム監査は、これらを通じて組織体のITガバナンスの実現に寄与するものである。

情報システムに対するコントロールを適切に整備・運用する目的は、以下のような範疇に分けることができる。

・情報システムが、経営方針、戦略目標の実現に貢献している。
・情報システムが、組織の目的を実現するように安全、有効かつ効率的に機能している。
・情報システムが、内部又は外部に報告する情報の信頼既が保たれるように機能している。
・情報システムが、関連法規、契約又は内部規程等に準拠している。

システム監査基準は、システム監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範である。本監査基準は、監査人としての適格性及び監査業務上の遵守事項を規定する「一般基準」、監査計画の立案及び監査手続の適用方法を中心に監査実施上の枠組みを規定する「実施基準」、監査報告に係る留意事項と監査報告書の記載方式を規定する「報告基準」からなっている。

システム監査基準は、組織体の内部監査部門等が実施するシステム監査だけでなく、組織体の外郭者に監査を依頼するシステム監査においても利用できる。さらに、本監査基準は、情報システムに保証を付与することを目的とした監査であっても、情報システムの改善のための助言を行うことを目的とした監査であっても利用できる。

システム監査の実施に当たっては、組織体における情報システムのリスクに対するコントロールの適否を判断するための尺度が必要である。システム監査は、本監査基準の姉妹編であるシステム管理基準を監査上の判断の尺度として用い、監査対象がシステム管理基準に準拠しているかどうかという視点で行われることを原則とする。しかし、システム管理基準に基づく監査に限らず、各種目的あるいは各種形態をもって実施されるシステム監査においても本監査基準を活用することができる。

システム管理基準は、組織体が情報システムを構築し運用するための標準的な対策を提供しているので参考とすることができる。

システム監査基準は、昭和60年(1985年)1月に策定されたもので、その後平成8年(1996年)1月に改訂され、今回は2度目の改訂である。今回の改訂は、昨年4月に創設された情報セキュリティ監査基準との整合性をはかり、従来の実施基準の主要部分を抜き出し、システム管理基準として独立させ、それぞれに大幅な加筆・修正を行ったものである。システム監査の目的

システム監査の目的は、ITガバナンスを通じて、情報システムが組織体の目標達成に役立つ情報及び業務処理を提供することに貢献することである。そのために、リスクアセスメントに基づくコントロールの整備、運用状況を、システム監査人が独立かつ専門的な立場から検証又は評価することによって、保証を与えあるいは助言を行うことである。

システム監査は、情報システム及びそのライフサイクルプロセスを対象とする。

一般基準

1. 目的、権限と責任

システム監査を実施する目的及び対象範囲、並びにシステム監査人の権限と責任は、文書化された規程、または契約書等により明確に定められていなければならない。

2. 独立性、客観性と職業倫理

2.1 外観上の独立性

システム監査人は、システム監査を客観的に実施するために、監査対象から独立していなければならない。監査の目的によっては、被監査主体と身分上、密接な利害関係を有することがあってはならない。

2.2 精神上の独立性

システム監査人は、システム監査の実施に当たり、偏向を排し、常に公正かつ客観的に監査判断を行わなければならない。

2.3 職業倫理と誠実性

システム監査人は、職業倫理に従い、誠実に業務を実施しなければならない。

3. 専門能力

システム監査人は、適切な教育と実務経験を通じて、専門職としての知識及び技能を保持しなければならない。

4. 業務上の義務

4.1 注意義務

システム監査人は、専門職としての相当な注意をもって業務を実施しなければならない。

4.2 守秘義務

システム監査人は、監査の業務上知り得た秘密を正当な理由なく他に開示し、自らの利益のために利用してはならない。

5. 品質管理

システム監査人は、監査結果の適正性を確保するために、適切な品質管理を行わなければならない。

実施基準

1. 監査計画の立案

システム監査人は、実施するシステム監査の目的を有効かつ効率的に達成するために、監査手続の内容、時期及び範囲等について、適切な監査計画を立案しなければならない。監査計画は、事情に応じて適時に修正できるように弾力的に運用しなければならない。

2. 監査の手順

システム監査は、監査計画に基づき、予備調査、本調査及び評価・結論の手順により実施しなければならない。

3. 監査の実施

3.1 監査証拠の入手と評価

システム監査人は、本調査においては適切かつ慎重に監査手続を実施し、保証又は助言についての監査結果を裏付けるのに十分かつ適切な監査証拠を入手し、評価しなければならない。

3.2 監査調書の作成と保存

システム監査人は、実施した監査手続の結果とその関連資料を、監査調書として作成しなければならない。監査調書は、監査結果の裏付けとなるため、監査の結論に至った過程がわかるように秩序整然と記録し、適切な方法によって保存しなければならない。

4. 監査業務の体制

システム監査人は、システム監査の目的が有効かつ効率的に達成されるように、適切な監査体制を整え、監査計画の立案から監査報告書の提出及び改善指導（フォローアップ）までの監査業務の全体を管理しなければならない。

5. 他の専門職の利用

システム監査人は、システム監査の目的達成上、必要かつ適切と判断される場合には、他の専門職による支援を考慮しなければならない。他の専門職による支援を仰ぐ場合であっても、利用の範囲、方法、及び結果の判断等は、システム監査人の責任において行われなければならない。

6. 情報セキュリティ監査

情報セキュリティ監査については、原則として、情報セキュリティ管理基準を利用しなければならない。

報告基準

1. 監査報告書の提出と開示

システム監査人は、実施した監査の目的に応じた適切な形式の監査報告書を作成し、遅滞なく監査の依頼者に提出しなければならない。監査報告書の外部への開示が必要とされる場合には、システム監査人は、監査の依頼者と慎重に協議の上で開示方法等を考慮しなければならない。

2. 監査報告の根拠

システム監査人が作成した監査報告書は、監査証拠に裏付けられた合理的な根拠に基づくものでなければならない。

3. 監査報告書の記載事項

監査報告書には、実施した監査の対象、実施した監査の概要、保証意見又は助言意見、制約又は除外事項、指摘事項、改善勧告、その他特記すべき事項について、証拠との関係を示し、システム監査人が監査の目的に応じて必要と判断した事項を明瞭に記載しなければならない。

4. 監査報告についての責任

システム監査人は、監査報告書の記載事項について、その責任を負わなければならない。

5. 監査報告に基づく改善指導（フォローアップ）

システム監査人は、監査の結果に基づいて所要の措置が講じられるよう、適切な指導性を発揮しなければならない。

討論会「新システム監査・管理基準を考える」実施報告

No.1051 京阪昌彦

日時：2004年6月12日（土）
15：00～17：30
場所：天満研修センター（大阪市）
講師兼パネラー：
三井情報開発株式会社総合研究所コンサルティング部主席コンサルタント
（内閣府CIO補佐 官、当協会理事）
本田 実氏
パネラー：
大阪市立大学大学院創造都市研究科教授
松田貴典氏
公認会計士藤野正純事務所所長 藤野正純氏
司会：当協会近畿支部長 石島 隆氏

討論会は、財団法人日本情報処理開発協会によるシステム監査基準検討委員会メンバーである本田氏からの、今回のシステム監査・管理基準の改訂のポイントとパブリックコメントの論点についての解説、パネラーの松田氏、藤野氏からの、主要な論点に関する意見表明、一般参加者を交えたディスカッション、という手順で実施された。

1. 新システム監査・管理基準の改訂のポイントとパブリックコメントの論点（本田氏）

新システム監査基準及び管理基準策定の経緯と、システム監査基準検討委員会の活動状況について述べられたあと、新システム監査基準及び管理基準の要点について解説された。

新システム監査基準及び管理基準の見直しにあたっての基本方針は、新技術及びITガバナンスを考慮し、情報セキュリティ監査制度との棲み分けを考慮した上で、より時代に適合した基準に見直すということである。特に情報セキュリティ監査との関係については、システム監査と情報セキュリティ監査は別ものという認識に立ちながらも基準のフレームについては同様の構成とすることとし、システム監査基準とシステム管理基準はワンセットで活用するものとした。また、実態として情報セキュリティコントロールに関しては情報セキュリティ監査と重複する項目も多いが、排他的にどちらかの監査に含まれるものとは扱わず、システム監査基準及び管理基準は情報セキュリティコントロールを含んでそれだけで完結するものとしている。

システム監査基準の一般基準、実施基準、報告基準は、その目的は異なるものの、情報セキュリティ監査基準のそれとほぼ同等の記述内容となっている。また、システム管理基準の項目数は280程度であり、情報セキュリティ管理基準のコントロール項目数132、サブコントロール項目数955の合計と比較すると少なく、情報セキュリティ管理基準のコントロール項目数より若干多いレベルのものである。実用に当たってはサブコントロールレベルの項目が必要であり、別途、システム監査基準解説書で説明することとする。この解説書は、拘束力に乏しい単なるガイドラインではなく権威付けを行ったものにしたい。

システム監査基準及び管理基準の制定後は、システム監査基準解説書の作成、システム監査基準及び管理基準の説明普及が課題である。

2. システム監査・管理基準を考える（松田氏）

システム監査学会システム監査体系化研究プロジェクトの中間報告をもとに、システム監査のあるべき姿について提言があった。

システム監査を取り巻く環境は変化しており、ユビキタス技術の進化とともに新たな脆弱性が発生している中で、自治体や企業の社会的責任（CSR）が求められる事故・犯罪が多発してきている。システム監査の視点については、安全性・信頼性・効率性の視点とともに、有効性・有用性・遵法性の視点、社会的責任の視点が求められるようになってきた。

具体的個別的なセキュリティ事象を扱う情報セキュリティ監査に比べ、システム監査は経営層の視点からのセキュリティ概念が含まれる。ステークホルダーへの説明責任、社会的責任を鑑み、システム監査は法定化すべきものであると考える。そのためには、システム監査は助言形ではなく保証型であるべきである。

3. 新システム監査基準・管理基準（案）に対する意見（藤野氏）

今回の見直しで、監査基準と管理基準を分離したことは評価したい。今までは管理基準レベルの議論が監査基準レベルの議論と混同されることがままあったからである。

システム監査と情報セキュリティ監査の違いについては、会計監査などとの相違に比べればそれほど明らかではなく、むしろ、システム監査基準の見直しに当たっては、情報セキュリティ監査基準の不備や欠陥を補修する試みが必要であると考えていた。今回のシステム監査基準及び管理基準案では、監査に対する行動規範が提供されていないように見えるし、内部監査と外部監査の区別、助言形監

査と保証型監査の区別などがなされていない。

また、職業倫理や守秘義務を謳った項目については、企業の就業規則に則る内部監査人や、職業倫理規定を設けた団体に属する職業的専門家の実情を鑑みると、監査基準の中に含めるレベルのものではないのではないか。

4. 討論 （司会：石島氏）

パネラー3氏の発表の後、下記のテーマについて一般参加者を含め、積極的な討論が行われた。

① システム監査と情報セキュリティ監査の目的・対象・観点の相違について

本田氏から「システム監査は、情報システムの目的達成のリスクに対するコントロールの有効性確保についての保証または助言（目的）であり、情報システムやSLCP（対象）に対して、効率性、有効性、信頼性、遵守性を含めて（観点）実施するものであるのに対し、情報セキュリティ監査は、情報資産のセキュリティ確保の保証または助言（目的）のために、情報資産（対象）に対して、機密性、完全性、可用性（観点）について実施するもの」という私見が示された。それをもとに、情報システムと情報資産という用語の定義を明確にすべきといった意見や、情報セキュリティ監査では、本来必要なセキュリティ設計に関する領域がカバーしきれていない、等の議論が交わされた。

② システム監査基準への職業倫理の記載について

内部監査人や外部監査人の倫理規定は、所属企業の就業規則や所属団体の規程で定めるべきであり、監査基準に職業倫理を記述する必要はないのではないか、という藤野氏の意見に関して議論が交わされた。

③ システム管理基準におけるコントロールに関するフレームワーク・情報戦略に関する記載について

内部統制の評価自体の監査に関する事項や、情報戦略に関する事項については、今回のシステム管理基準にはあまり記述されていないという意見があった。本田氏からは、コントロールに関するフレームワークについては、今後の課題である旨のコメントがあった。また、情報戦略に関しては、定義が明らかでないが、今後のEAの動向を踏まえながら整理する必要があるという議論があった。

④ 内部監査と外部監査の関係について

内部監査と外部監査の定義について、実施主体で定義する考え方（企業内部者が実施するものを内部監査、外部委託するものを外部監査）と、報告先で定義する考え方（経営者に対して報告するものを内部監査、第三者に対して報告するものを外部監査）のどちらなのかという問いかけがあった。後者が妥当ではないかという議論があった。

⑤ 保証型監査の必要性とそのための条件整備について

保証型監査については、市場ニーズの可能性に関する意見や、法定化するのであれば保証型監査である必要があるといった意見があった。また、保証型監査の実施にあたって拠り所となるシステム管理基準を早急に整備（詳細化）する必要があるという意見に対しては、解説書の改訂等によりフォローしていく等、皆の叡智を集めて作成していく必要があるというコメントがあった。

また、一般参加者から、保証型では、実質的に経営者から内部監査人に対する担保要求が厳しくなってしまうのではないかという危惧が寄せられた。これに対しては、内部監査に限らず、経営者には保証の意味〔事故がないことを保障する（Guarantee）のではなく、基準通りであることを保証する（Assurance）こと〕を説明し、完全ではないことを理解してもらう必要があるというコメントがあった。

最後に、本田氏から、システム監査基準及び管理基準については今回規定されても、まだまだ先があり、課題については解説書でフォローしながら、皆で前向きにどんどんよくしていこう、というコメントがあり、盛会のうちに討論会を終えた。

参加された方々の高い問題意識を感じた討論会であり、これから皆で、システム監査を盛り上げていかなければならないことを認識した場でありました。

改訂されたシステム監査基準・管理基準の解説（第105回月例研究会報告）

No.1060 太田 香

日時：2004年7月27日（火） 18：30～20：30
場所：中央大学駿河台記念館 280号会議室
講師：特定非営利活動法人 日本システム監査人協会理事 本田 実 氏
演題：「改訂されたシステム監査基準・管理基準の解説

●はじめに

この講演が行われた時点ではまだ経済産業省からの発表が行われていないため、演題を「改訂された」から「改訂される」と理解して頂きたいとの説明とともに講演が開始された。講師は当協会の理事であり、また内閣府ＣＩＯ補佐官である本田氏である。システム監査基準検討委員会委員として改訂システム監査基準・管理基準の両ワーキンググループにてご活躍された。氏に委員会内部での検討経緯を交えながらご解説頂いた。

●講演内容

以下の項目に従って講演が行われた。

Ⅰ．前段
1. システム監査基準改訂の経緯
2. システム監査基準検討委員会の活動状況、ワーキンググループのメンバー構成

Ⅱ．主題
1. 改訂システム監査基準・管理基準の基本方針
2. 情報セキュリティ監査とシステム監査の位置づけ
3. 現行「システム監査基準」との対比
4. 改訂システム監査基準の概要と内容
5. 改訂システム管理基準の概要と内容

Ⅲ．まとめ
1. 今後の課題

～質疑応答～

Ⅰ－1. システム監査基準改訂の経緯

1985年1月に当時の通産省にて「システム監査基準」が作成され、1996年1月に「改訂」が行われ、現在に至っている。2000年以降において、当協会にてシステム監査にかかわるさまざまな提言を行ってきている。

Ⅰ－2. システム監査基準検討委員会の活動状況、ワーキンググループのメンバー構成

省略（筆者記：JIPDECのホームページ等でご参照頂きたい。）

Ⅱ－1. 改訂システム監査基準・管理基準の基本方針

以下の5点をシステム監査基準改定の基本方針とした。
1. 新しい技術革新への対応
2. 事業における情報システムの位置付けの変化への対応
3. 社会に対する説明責任の高まりと保証型監査の必要性
4. 「情報システム管理の標準」と「監査人の行為規範」の峻別
5. 情報セキュリティ監査制度との関係明確化

また、以下の3点については、今回の改訂では行わないこととした。
(1)「用語の定義」は基準に入れず、別途定めることを検討する。
(2) 個別の対象システムの規模、状況等に大きく依存するものは、個別に設定されるものとし、基準では触れない。
(3) 活用範囲を広く保つため、特定の定義はしない。

Ⅱ－2. 情報セキュリティ監査とシステム監査の位置づけ

図1をご参照頂けるとより明確となるが、システム監査は「情報システムに対する構築・運用の全体最適化」を目的とし、情報セキュリティ監査は情報システム以外を含めた「情報資産」を範囲としている。また、判断の尺度についてはシステム監査の場合は「効率性・有効性」も尺度に含ま

れるが、情報セキュリティ監査についてはこの判断基準は適用されない。さらにシステム監査において情報セキュリティ確保の観点が必要とされる場合は「情報セキュリティ管理基準」を活用するという位置付けとしている。

Ⅱ－3. 現行「システム監査基準」との対比

大きく改訂されたのは、「システム監査基準」と「システム管理基準」の2本立てで構成したことである。これは基本方針の「4」で挙げられている通りで、「情報セキュリティ監査制度」の構成に合わせたものである。システム監査基準、システム管理基準のそれぞれの章立てについては現行の「システム監査基準」を基本的に踏襲し、そこに新たな項目を追加する形をとっている。(図2、図3を参照)

Ⅱ－4. 改訂システム監査基準の概要と内容

「一般基準」、「実施基準」、「報告基準」に先立ち「前文」と「目的」を掲げ、そこに先ほどの「基本方針」を盛り込んでいる。「前文」についてはシステム管理基準にも同様の観点のものを追加している。この「前文」についてはパブリックコメントでも意見が多く、訂正している所がある。意識して盛り込んだ内容として、内部監査部門による実施だけではなく、組織体の外部者の監査にも利用できるものとしたこと、保証型監査と助言型監査の存在を明記したなどがある。

「目的」に「リスクアセスメントに基づくコントロールの整備·運用状況」と明示することにより、リスクアセスメントの必要性を強調した。リスクの例として「目的・目標が実現できないリスク」「安全·有効・効率的に機能しないリスク」「提供する情報の信頼性が低いリスク」「関連法制度に準拠していないリスク」というものが挙げられる。システム監査はこれらのリスクのコントロールが適切に整備・運用されていることを確認するための有効な手段である。システム監査さえ行えばリスクコントロールがうまく行えるというものではないことにご注意いただきたい。

「一般基準」、「実施基準」、「報告基準」で説明を要する部分として、「監査人の独立性、客観性」についての程度はさまざまな状況が考えられるため、あえて監査基準には明記しなかった。本基準を広範囲に使えることを目指したことにより、文言の厳密性をあえて追求していない。「システム監査人は、職業倫理に従い～」という文章でも内部監査人はシステム監査を職業としているものではないが「職務上の倫理」と読み替えて理解していただくなどの点も同様である。また監査の手順の項を設け「予備調査・本調査」を挙げているが、これらは情報セキュリティ監査基準には存在しない。これは現実に実施されている状況を踏まえ、あえて残したものである。ただし、予備調査と本調査の違いを明確にすべきとの意見がある。これについては基準では定義を行わず、別途定めることを検討中である。

Ⅱ－5. 改訂システム管理基準の概要と内容

「前文」については監査基準のものと同様の観点で記述されている。特に明記する点はこの管理基準を「原則として、監査人が監査上の判断の尺度として用いるべき基準」と明示している点である。また「全体最適化」という考え方は「EA」と共通するものであり、改訂作業において意識はしたが、あえて用語として文言化はしていない。

管理基準の内容についてだが、大きな変更点は「情報戦略」が追加されたことである。この「情報戦略」のかなりの部分で前出の「全体最適化」という文言を用いている。またここで現在の情報技術の潮流(トレンド)を取り込んでいる。「企画業務」については「調達」の項目を追加、「開発業務」についてはほぼ同じ。「運用業務」については一部項目を追加し、今まで「保守業務」に位置づけられていた大規模保守については開発業務へと移動した。「共通業務」については品質管理と変更管理を追加した。また外部委託を「委託・受託」として受託の項目も追加した。

Ⅲ－1. 今後の課題

これは私見をかなり含んでいるが、経済産業省、JIPDEC、IPAとして

①システム監査基準、管理基準の説明·普及
②システム監査基準解説書の作成
③システム監査技術者試験の対応等

また、日本システム監査人協会として

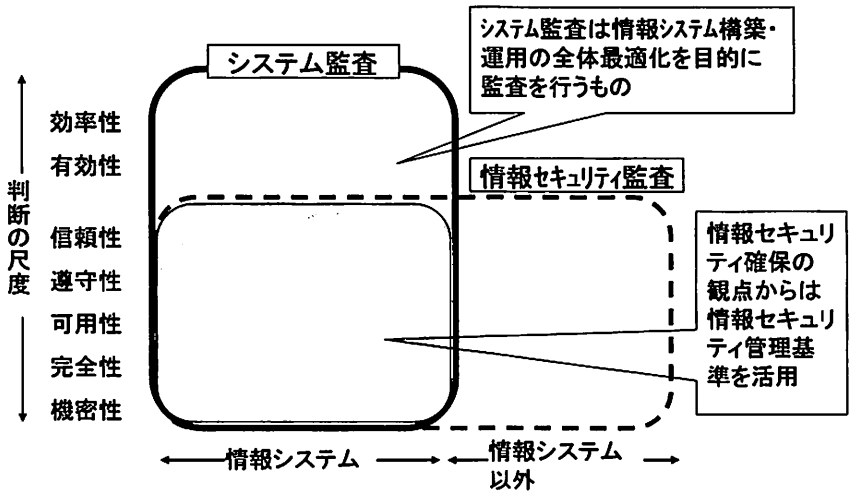
①システム監査基準、管理基準の研究、ガイドラインの作成
②情報セキュリティ監査との連携の研究、ガイドラインの作成

③システム管理基準の各項目ごとのコントロール及びサブコントロールの作成
④業種·業界ごとのシステム管理基準ガイドラインの作成
⑤システム監査事例の蓄積・公開等
以上の点の必要性が感じられる。

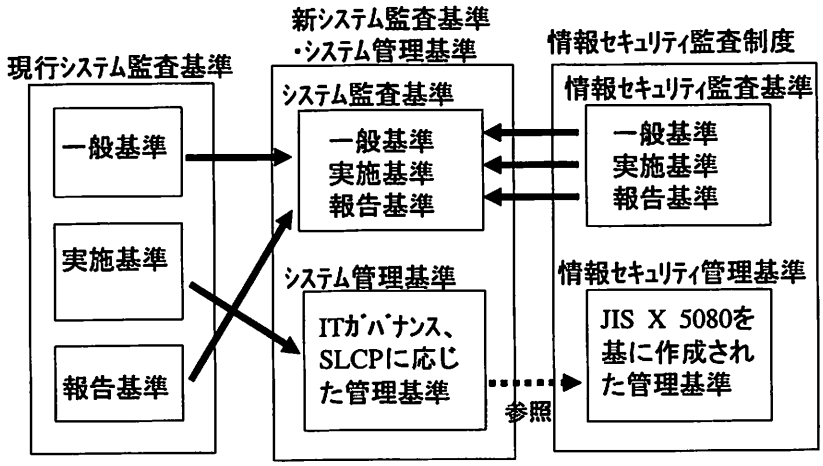
～質疑応答～
一通りご説明いただいた後で、限られた時間ではあったが質疑応答が行われた。質問内容は用語の定義やあいまいさが残るような文章への質問、また改訂の方向性に対する意見なども挙げられた。それらに対する回答の中で、用語の定義を含めなかった経緯などは詳細にご説明され、パブリックコメントにも挙げられた「IT ガバナンス」についての定義を明確化することによる範囲の矮小化への懸念、また全体に「EA」の概念を基礎として取り入れているものの「EA」そのものの用語化は避けることになったなどの説明があった。
また、デファクトスタンダードに準拠しすぎると、それらが改訂された場合には本基準も改訂せざるを得なくなるなど、日本の文化で育てられた「システム監査基準」の独立性を損なう懸念も説明されていた。
新しい概念をどこまで取り入れ、また、用語化するか、他の基準との整合性、デファクトスタンダードへの準拠程度などについての委員の方々の意見の交錯があったことも説明され、決定しづらいことについても成果物として纏め上げなければならないもどかしさも窺い知れた。

●おわりに
当日は 130 余名、会場を埋め尽くすほどの参加者があり、ただでさえ熱気の立ち込める東京都内でも場内の熱気はひとしおのものであった。
講演の端々にて、委員会、ワーキンググループ内部でもパブリックコメントへの対応に対する意見が分かれた事などをご説明され、パブリックコメントを提出した方も参加されているであろう今回の研究会でその経緯をご説明頂き、納得された方も多いのではないだろうか。
今回の研究会は IT 環境の変化の早さと可能な限り齟齬のない改訂にしようと検討を重ね続けられた委員会のメンバーの方々のご苦労が拝察される講演内容であった。

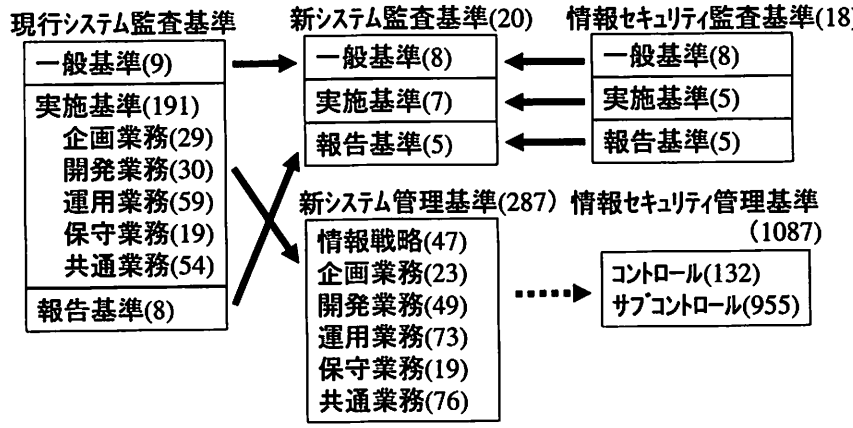
3. 2 情報セキュリティ監査とシステム監査



3．3 現行システム監査基準との対比（1）



3．3 現行システム監査基準との対比（2）



（注）システム監査基準、管理基準の項目数は、発表予定のものである。

システム監査実践セミナーを開催して

NO.848 森 広志

システム監査実践セミナーは、今年2月初旬に、吉田理事より検討依頼がありました。

北信越支部の今年度計画では、システム監査実践セミナーの開催を検討することにしていましたので、早速、役員メールに諮ったところ、多数の賛成同意を得て開催することとしました。

特に昨年は、中部支部で開催された、システム監査実践セミナーに、梶川副支部長が参加し内容を実際に把握して頂いた事が早々の開催に繋がったと考えています。

研修会場は、第一開催希望の5月15日（土），16日（日）について、伊藤支部理事より富山駅前のCICビルに確保頂くことができました。

2月23日には、SAAJ年度総会に出席し、吉田理事、沼野理事にお会いし、システム監査実践セミナーの全体スケジュールや集客や講師、宿泊などについて教えていただきました。

ホテル予約では、システム監査実践セミナーの当日、他の学会の大きなイベントと重なり、富山の主要なホテルは満室のため、いろいろ探すのに苦労しました。何とか、CICビル近くのビジネスホテルを確保しました。

又、集客については、締切日の直前近くまで開催にこぎつける人数が確保できず気を揉みました。募集については、支部会員にそれぞれご協力願いました。私は、地元の情報産業協会や地元ITコーディネータ団体に募集をかけました。それでも募集人数が満たず、大野中部支部長からも中部地区のITコーディネータに呼びかけを行って頂き、何とか開催人数を確保することが出来ました。やはりITコーディネータは、会員数が多いことや知識ポイント取得の必要性があるため頼るところが大きかったと思います。

開催当日は、沼野、森本両講師の説明を参考にさせていただく予定でおりましたが、ホテルの予約部屋割りや写真撮影、レストランの手配などの作業もあり、ゆっくりしていることが少ない状況でした。伊藤理事も、当日準備や富山県名物鱒の寿司のおみやげ手配などご尽力頂きました。

特に圧巻だったのは、第1日目終了後の懇親会で、梶川副支部長が短時間で用意して頂いた蛍烏賊料理でした。これには期待以上の効果があり、皆さんで富山県名物の蛍烏賊料理を食べ、本当に疲れが吹っ飛んだ感がありました。

今回のシステム監査テーマは、両チームともに有効性の監査を選択されました。私は、企業経営者は、準拠性監査よりも企業目的に役立つ有効性、効率性の監査を好むということを改めて再確認しました。

私は、米国など世界で普及しているシステム監査は、監査計画にリスクアセスメントや内部統制レビューがあり、準拠性監査に入ってゆきやすく、又、テーマ選定も行いやすくなっていると考えています。このため世界で普及しているシステム監査の多くは、準拠性監査が主流だと思っています。逆に、日本のシステム監査の場合は、トップインタビューを重視するため有効性の監査を選択することが多くなると思います。しかし、投資対効果や有効性評価方法のノウハウが蓄積向上、工夫されることは、今後のシステム監査普及に役立つと考えます。

受講者の皆さまは、それぞれ熱心に研修に取り組まれ、監査手順、ヒヤリングやプレゼンテーションを経験、習得され成果が上がったようにお見受けしました。

今回、富山開催を計画していただいた吉田理事ほか事例研究会の皆様方、沼野理事、森本講師、北信越支部の梶川副支部長、伊藤理事、遠くからおいで頂きました受講者の皆様方、まことにありがとうございました。次回の開催時も楽しみにお待ちしております。

スケジュールと雑感

No.947 梶川 明美

1. 日程　2004年5月15日・16日
2. 場所　富山駅前CiCビル3 F
「とやま市民交流館」市民学習コーナー
3. スケジュール
15日（土）
13:00 ～ 13:20　開会セレモニー
（開会挨拶、スケジュール説明、自己紹介等）
13:20 ～ 13:50 【講義1】
システム監査実施手順及びシステム監査基本技法解説
13:50 ～ 14:20　ケース及び演習課題説明
14:20 ～ 15:40　＜課題1＞
監査計画・予備調査項目まとめ
15:40 ～ 16:10　監査計画発表
16:10 ～ 16:40 【講義2】
予備調査インタビューのテクニック他
16:40 ～ 17:40　＜課題2＞
予備調査インタビュー（ロールプレー）
17:40 ～ 19:00　夕食
（エクセルホテル東急「松や」）
19:00 ～ 19:40　＜課題3＞
予備調査結果まとめと本調査方針検討
19:40 ～ 20:20　予備調査結果と本調査方針の発表

20:20～20:45 【講義3】
本調査インタビューのテクニック他
21:00～22:00 懇親会（ホテル佐渡）

16日（日）
7:30～8:00 朝食（ホテル佐渡）
8:30～9:45 ＜課題4＞本調査質問事項検討
10:00～11:30 ＜課題4＞
本調査質問事項検討
11:30～12:35 ＜課題5＞
本調査インタビュー（ロールプレー）
12:40～13:30 昼食（CiCビル「花みくら」）
13:30～15:00 ＜課題6＞監査報告書作成
15:00～16:00 ＜課題7＞
監査報告会（ロールプレー）
16:00～16:20 講師講評、事後課題説明
16:20～16:40 閉会セレモニー／解散

4. 雑感

活発で緊張感のある討論や講義の中にも、終始なごやかに実践セミナーのスケジュールを進められた講師と受講生の皆様の姿が印象的でした。

てきぱきと段取りされる講師の先生方と森支部長のもと、特にこれといった仕事もなかった私はもっぱら添乗員としておみやげや懇親会担当をしていました。セミナースケジュールはかなりのボリュームなのでシステム監査漬けでしたが（当然ですが）、次回富山にお越しの際は是非ゆっくりと観光していってください。

システム監査実践セミナー受講感想

No1354 栃川 昌文

私は、中小企業を対象に中立的な立場で（システム販売は基本的に行わないで仲介や紹介を行う）、システムコンサルを行っています。独立して5年になりますが、以前からお客様のシステムに対するニーズ把握や現状分析、お客様への問題点の提示方法などにおいてシステム監査の視点や手法が役に立つのではないか、と感じていました。

そこで、昨年、特別認定制度を利用してシステム監査人補になったのですが、実務経験が無いために、システム監査を経験してみようと思い、今回のセミナーを受講しました。実は、今年2月に行われた4日間コースに申し込んだのですが、開催3日前に虫垂炎（いわゆる盲腸）になり、ドタキャンしました。そんな経緯もあり、今回のセミナーを楽しみにしておりました。

今回のセミナーでは、ニーズの把握という点は範囲に入っていませんでしたが、予備調査、本調査、監査報告のまとめ、と体験することができました。

受講して感じたのは、似ているようで違う、コンサル業務と監査業務の違いでした。対象も手法も似たようなことをやりますが、ゴール＝成果物に違いがあるために、視点もおのずと異なってくるのかな、というものです。演習においては、こういった違いからチーム内で議論が噛み合わない場面もありました。一方、コンサル業務に参考になることも多いにあり、これからの仕事に役立てると確信しています。

まだまだ未熟ですのでこういった感想を持つことが間違っているかもしれません。今後もセミナーなどを通して監査技術を磨きたいと考えています。

最後になりましたが、2日間講師をしていただきました、森本さん、沼野さんにお礼を申し上げます。また、会場や宿泊、懇親会のお世話をしていただきました北信越支部の皆様にも感謝申し上げます。

●セミナー参加報告

No. 1184 山田 和夫

はじめに、参加の動機ですが、この春にシステム監査人補の申請を機に、会社ではシステム監査業務を行なう機会が無いことから、セミナーで模擬体験をするために応募しました。

受講前には、配布された資料を見て、その量の多さとセミナー・スケジュールがタイトであることに驚きました。受講案内に従い、事前学習は行なったものの、セミナーを受講してから振り返れば、量・質ともに準備不足でした。私のような経験の無い受講者にとっては、事前学習に相当の時間を充てることが必要なようです。

セミナーでは、チームが編成され、与えられた監査テーマについて、監査計画・予備調査・本調査・監査報告を、ロールプレー形式で演習します。こうした実習の中で、特に難しく感じたのはインタビューでした。これは、単にコミュニケーション能力の優劣が問題なのではなく、各種資料や回答者の答をもとに、論理的に思考し、仮説を立て、それを検証し、事実を導き出すことを、短時間で的確に行なう必要があるからで、そうした訓練が不足している私にとっては難関でした。セミナーを通して、監査のインタビューが経験できることは、大変有意義であると思います。

また、セミナーの事後課題として、監査報告書を提出することになります。私は、セミナー翌週から出張を控えていたので、何とかそれまでに完成をと思い、睡眠時間を削って事後課題

に取り組むはめになりました。その人の能力により格差があるのでしょうが、私の場合、報告書作成に約16時間もかかってしまいました。今回のセミナー参加を通して、私にとっては難関の連続でしたが、日常の業務では得ることのできない大変貴重な経験が得られと感じています。

最後に、講師の方々をはじめ、事務局の方々、参加者の方々には、大変お世話になりました。この場を借りてお礼を申しあげます。

平成16年度第1回システム監査実践セミナー(in 富山)に参加して

No.1281 宮本 茂明

今回の実践セミナーには、外部システム監査のスキルをつけることを目的に参加しました。仕事としてのシステム監査は、社内監査が主のため、本セミナーは外部システム監査を擬似体験するよい機会となりました。

ケーススタディは、システムの有効性に関するもので、経営トップへ現状システムの有効性をシステム監査の切り口で報告するものでした。セキュリティ監査等で行う規定への準拠性確認等でなく、その進め方の難しさを実感しました。

講師の先生から、「予備調査では、調査対象に対する網羅性が必要。このための情報を広く収集。次に魚を追い込むように、問題点のターゲットを絞り込む。」というアドバイスを受けましたが、論理的にはわかっていても、ロールプレーイングで得た直後の情報に目が行きがちで、全体を見てポイントをつくという形に充分にもっていけなかった点が、セミナーでの反省点です。

有効性を主体においたシステム監査について、システム監査で事実を整理し、取組むべき方向性を客観的に提示し、その後ITコーディネータのアプローチに繋げていくのが効果的ではないかと感じました。

2日間充実したセミナーでした。講師の森本先生、沼野先生、受講者の皆様、会場・懇親会準備等ご尽力いただいた北信越支部の森様、伊藤様、梶川様、ほんとうにありがとうございました。

システム監査実践セミナーin富山に参加して

No.1381 斉藤 哲生

一泊二日の缶詰セミナーとう事でかなり緊張感を持って参加しました。というのも私は実務経験がなく「まず、何を決めるのか？」「何から調べるのか」など皆目検討がつかない状況だったからです。

講習のスタートは事前配布された「ケーススタディ」の資料から始まります。当然ですが資料は事前に熟読されていることが前提ですから要注意です。私は読むには読んだのですが「ああ、こんな内容のことが書いてあるのか」程度にしか読んでおらずかなり焦りました。その資料には事前課題も設定されています。参加された皆様はきちんと課題をこなされておりましたが、実は私は白紙でした。そんなこともあり冒頭から頭は120%のフル回転、私にとっては波乱の幕開けです。

それでも講師の方の実例を基本とした解りやすい説明は私の体（頭？）に自然に吸収されていきました。「概念」ではない「実例」は解りやすく説得力がありました。それをグループでの実践演習で整理していきます。まずは講義の内容をグループで「討議」して、方針を決め作戦を立てます。そして「ロールプレイング」(講師の狸ぶりに脱帽)、「まとめ」、「発表」を繰り返しながら予備調査、本調査といった課題を消化して行きます。グループ形式の討議は他のメンバーからの自分では気が付かない観点の指摘に「偏りのない監査」の重要性を感じました。最終日の監査報告会の「ロールプレイング」は本気で監査した気になり、モデル企業「Z社」に愛着すら沸いてきました。

あっという間の2日間、今は最後の事後課題に悪戦苦闘中ですが貴重な経験が出来ました。最後になりましたが開催に当り会場その他の手配をして頂いた北信越支部の皆様に感謝致します。(ほたるいか 美味しかったです)

以 上

「中部北陸地区情報処理団体研究会（in 富山）2004」

次の通り、地域の情報処理団体と交流を深め、かなり密度の濃い研究会を開催しましたので報告いたします。各テーマの報告書は分担しました。

No.947 梶川明美

●日 程

1. 日 時 6月19日（土）13：30～20：30
2. 場 所 JR富山駅前CiCビル3 F 会議室
3. スケジュール
   ・開催の挨拶
   NPOシステム監査人協会北信越支部
   森 広志支部長

・セミナー1
「日中ソフトウエア産業発展に向けての提言～システム監査の視点より～」
SAAJ中部支部長　大野　淳一氏
(共立コンピュータサービス株式会社)
・セミナー2
「リスクアプローチによる監査」
SAAJ北信越支部副支部長
白井　正氏（監査法人トーマツ）
・セミナー3　「情報戦略とITガバナンス」
日本システムアナリスト協会
中部支部長　岡田　博基氏
(東邦ガス株式会社)
4. 懇親会　かまど料理　ごんべい舎

●セミナー1

No.395　田原　保

「日中ソフトウエア産業発展に向けての提言～システム監査の視点より～」
NPO日本システム監査人協会
中部支部長　大野　淳一氏

富山駅前のCIC会議室は、28名の参加者でほぼ万杯状態。大盛況の中、緊張を和らげるような語りで大野氏の講演が始まった。北京で実際プレゼンしたPPTで説明され、論文作成チームの河田リーダーも同席された。冒頭に訪中となった経緯を説明。そのきっかけは、軽いノリで始まったこと、昨秋のファン副所長との会食から一気に実現に至ったこと、直前まで続いた論文作成の苦労話など話された。

現在の中国での情報処理資格は3種あり、2002年1月から日本での資格（システムアナリスト試験、ソフトウエア開発技術者試験、基本情報技術者試験）と相互認証を実施中であるが、日本でのシステム監査技術者試験にあたる資格が無いことに着目。中国での同資格の必要性と創設を願い、さらに相互認証できるようにし、両国の発展に寄与しようとする主旨・狙いを披露した。

また資料に基づき、日中ソフトウエア取引の現状や特徴、問題点、日本側の背景、問題解決に向けた方向性と視点、今後の展望について説明した。

最後に長期を見据えた両国の発展と交流のために我々が少しでも寄与したいとの熱い思いで締めくくられた。

その後の質疑応答の中で訪中団のメンバである若原氏と田原より、実際の緊張した会議の様子や懇親会でのエピソードなどについても紹介した。聴講された方々は皆、真剣に聞かれた様子であり、上々の評価であったようだ。

今回の参加者の方にも今後の交流活動に参加を期待表明して予定時間の講演を終了した。

●セミナー2

「リスクアプローチによる監査」

No.1281 宮本　茂明

講　師：NPOシステム監査人協会
北信越支部副支部長　白井正　氏

＜概要＞

会計監査（財務諸表監査）におけるリスクアプローチについて，公認会計士の立場から，会計士協会の指針をもとに具体的事例も交え説明された。

1. 財務諸表監査業務におけるリスク評価

財務諸表監査において意見表明を誤る可能性(監査リスク)を監査計画立案前に評価する。監査において全てを見ることができないことから，重要なところにフォーカスして，監査リスクの評価結果を監査計画に反映する。

2. 監査リスク

監査リスクは，次のように定義されている．「監査リスク」＝「固有リスク」×「統制リスク」×「発見リスク」

・「固有リスク」：関連する内部統制が存在していないとい仮定の上で，財務諸表に重要な虚偽の表示がなされる可能性。
　－企業内外の経営環境により影響を受けるリスク。
　－特定の勘定や取引が本来有する特性から生ずるリスク。
・「統制リスク」：財務諸表の重要な虚偽の表示が，企業の内部統制によって防止または適時に発見されない可能性。情報システムの内部統制も含まれる。
情報システムのコントロール目標としては，準拠性，網羅性，可用性，機密性，正確性，維持継続性，正当性がある。
・「発見リスク」（監査手続き上のリスク）：企業の内部統制によって防止または発見されなかった財務諸表の重要な虚偽の表示が，実証的手続きを実施してもなお発見されない可能性．監査リスクへの対応は，発見リスクの程度に適合した実証手続の実施にあることに留意する。

3. リスクアプローチ

「 監査リスク」を，常に一定水準以下のレベルにする必要がある。
「固有リスク」「統制リスク」は，被監査会社側の問題で，所与のリスクであり，所与のリスクが大きければ「発見リスク」を小さくす

るよう監査実施手続を計画・実施する必要がある。これが監査におけるリスクアプローチである。

リスクアプローチにおいて，リスク評価に漏れがないよう進めることが必要である。講師の所属する監査法人では，リスク評価を支援するシステムが活用され，リスク評価の網羅性チェックが実施されている。なお，リスク評価において，会計士としての経験に基づく「勘」も大事な要素であることを忘れてはならないとのことであった。

リスク評価の具体的な事例説明もあり，監査業務のリスクアプローチ概要を理解することができた。今回の講演を参考に，システム監査の計画立案時に監査リスクについて客観的に評価し，監査計画に反映するよう活動していきたい。

●セミナー3

No. 947　梶川明美

「日本システムアナリスト協会中部支部によるパネルディスカッション」

コーディネータ：岡田

パネリスト：関口、下谷、鈴木、若原、河田

コーディネータ

今年の活動テーマ「アナリストになろうよ！」を追求するため、企業のアナリストって何だろう、コンピュータでは何が出来るんだろう？というところからアプローチを開始した。今日は皆さんからも意見を頂戴したい。今企業のIT投資はどうなっているのだろう？

パネリスト A

数年前までは効率化でシステムを導入するところがほとんどだったが、今は経営判断をしたいというところが増えている。自分が今携わっている小売業のお客様。会社が急激に大きくなって、社長はいろいろなことにチャレンジしたいと思っている。具体的には社長が居ながらにしていろいろな情報を利用できるコックピット経営をしたいという意向である。基幹業務と経営情報を同時に進めている。

パネリスト B

行政分野ではコストで綿々と基幹業務をしているところもあるし、e-Japan計画に押されているところもある。優先順位をつけてやっているというよりは、導入期日に基づいた仕事の進め方が多いようである。

会場参加者 C

上流工程からシステム構築に入るケースは少ない。絞り込まれた要件でのアプローチが多い。お客様によってそれぞれ違う。システムの目的が社内ではっきりしているところはいいが、とにかく○○システムを入れたいというところはしっかりと構築できない。

パネリスト D

システムアナリストは企業内のCIO補佐官である。システムアナリストがまともに経営陣に意見を言えるのは、はっきりした経営方針を持っているところである。

会場参加者 E

コンピュータは以前から使っていたが、ECなどが出てきてお客さまと連携を取らなければならない部分があるので、どう進めていけばいいのかアナリストに教えて欲しい。また、血のめぐり（情報の流れ）が悪いような気がする。社長の意見など組織の末端にうまく流れていないのでは、と思うことがある。

コーディネータ

アナリスト育成の視点から見るとどうだろうか？

会場参加者 F

一般企業ではアナリスト的な人がうまく検討していることもあるし、そうでない場合もある。アナリスト的な人達には船頭的な視点でやってもらえるといい。ベンダーと一緒に進歩していければいい。一言で言うと人間力。パソコンオタクのいるところは絶対失敗する。

パネリスト G

教育担当からアナリスト育成を考えると、ITスキル標準が有効である。集合研修でカバーできるのはレベル3から4くらいまでである。一緒に仕事をしていく中から力を高めていくのがいい。

パネリスト H

最近の若い人は言われたことはきちんとするが、自分からアイデアを出してくることが少ない。それでは我々の社会が成り立っていかない。先ほど会場から意見があったように、アナリスト候補として「船頭的な視点」を持って自分から行動できる人を育てたい。

会場参加者 I

アナリストは誰を相手に仕事をするのか？どこへいって何をするか、誰を相手にするのか教えて欲しい。

コーディネータ

経営総を相手に仕事をするというものと理解しているが実際には、経験上も、開場からの意見からみても、経営層に直接提案できているような企業内アナリストは少ないのではないかと思われる。今後、この巾を広げてい

くためにはどうすればいいか、も課題である。

会場参加者 J

コードの不統一にあるようなIT活用の混乱があるので、ITガバナンスが必要である。ITガバナンスを実現するにはPDCAを廻していけることが大切。ITガバナンスをやらないとITが統一できない。

コーディネータ

ITガバナンスという視点でアナリストの役割を整理してみることも必要であろう。

パネリスト D

アナリストとITコーディネータの機能は幅広くかつ 重なるところが多い。立場は違うものであるが、アナリストとITコーディネータの協業を考えるべきだ。

●セミナー参加報告

NO.632 尾島記

今回の中部・北陸合同研究会を一言で表すとしたら「人間力あふれる会」だったと思います。人間力については、研究会第3部パネルディスカッションについてのご紹介文の中にも記載されていますが、簡単にいうと、個人のパーソナリティ・知識・能力を余すところなく発揮しようとする意志と言えます。(田原さん、みなさん、この認識でいいですよね？)

パネルディスカッションの中で、求められるIT人材は「人間力あふれる人」であるという結論を得て、みな納得し、いざ懇親会となりました。ちょっと身びいきですが、富山の海の幸と旨い酒を堪能し、おおいに盛り上がりました。

というのも、懇親会の会場には著名な政治家、アスリート、芸能人の色紙が多数飾ってあり、わたしたちの足跡を残さないわけにはいかないということで、「人間力」を込めて寄せ書きしてきました。次回の富山での研究会終了後、また2枚目の色紙を書きにいきましょう。

第103回月例研究会報告

「JIPDECリスクマネジメントシステム（JRMS）の狙いと適用」

東京海上リスクコンサルティング株式会社
リスクコンサルティング室
主席研究員 指田 朝久 氏
2004年5月27日（木）
機械振興会館 B3F 第1研修室

No.557 仲 厚吉

ISMS認証制度、昨年発足した情報セキュリティ監査・管理基準、最近、パブリックコメントがなされたシステム監査・管理基準、等々百花繚乱にある中で、JRMSが新たに設けられ、それら基準の相互のあり方がよくわからない受講者である私に、この90分は誠に有意義な時間でした。

ISMS認証制度等のPDCAマネジメントサイクルで、Pの計画段階におけるリスク分析にJRMSを使い、Cの監査段階には、情報セキュリテイ監査基準またはシステム監査基準を使えば、うまくいくと理解しました。

先ず、JRMSの狙いをお聞きしました。

◎情報リスクを企業全体のリスクマネジメントの中のひとつのリスクとして捉える

・企業全体のリスクマネジメントができているかがまず重要
・情報リスクの優先順位は企業全体としてどの位置にあるか
・「はじめに対策ありき」ではなくリスク分析を実施しリスクの軽重を判断し、リスク度合いに応じた対策を検討する

安全対策を「はじめに対策ありき」で一律に決めつけるのではなく、情報リスクを企業全体のリスクマネジメントの中のひとつのリスクとして捉えるわけです。

JRMSの構成は、

Ⅰ 経営とリスクの関係
Ⅱ JRMSにおけるリスクマネジメント計画
Ⅲ 情報システムのリスク分析
Ⅳ 情報システムにおけるリスク対策

となっています。

Ⅳの情報システムにおけるリスク対策まで導くツールですので非常に便利なすぐれものという印象です。

JRMSでは成熟度モデルが採用されていて、

レベル0 未認識
組織内で全く意識されておらず、何もしていない

レベル1 初期
組織内で部分的にしか実施されていない

レベル2 反復可能

組織内で大体実施されているが、標準がない
レベル3　定義
組織内で標準が作られ、大体それに従って実施されている
となっています。

分析のためのレーダチャートは、各項目ごとに、レベル0～レベル3まで分析結果が表示されるので勘どころをつかむのに便利になっています。
バラツキ、ギャップ分析、分析結果のとりまとめ、評価まで対応できるツールというように理解しました。

まとめとして、
・情報リスク、情報セキュリティを企業経営、自治体経営全体に関わるリスクマネジメントの一環としてとらえる
・「はじめに対策ありき」ではなくリスクを把握し、そのリスクの度合いに応じて対策をとる
・リスクマネジメントは組織と人で実践する。そのための脆弱性分析にJRMSは有効である
・JRMSはISMSなどの制度と対立するものではなく、相互に補完できる
という言葉で結ばれました。
引き続き、約30分の質問時間には、活発な

質疑応答がなされました。
Q1．JRMSは、企業の情報システムにおけるリスク分析、リスク対策を導くツールと思うが、例えば、受注工事のリスク、見積もりミスのリスクのような、プロジェクト管理上のリスク分析にも使用できるのか？
A1．JRMSはリスクマネジメント（JIS Q 2001）の視点に基づき、情報リスクへの対応について開発したもの。情報システムにかかわるもの以外のものには対応していない。

Q2．コンサルタントが1本購入して、多数のクライアント用に利用できるのか？
A2．そのような利用方法は、著作権上の問題が生じると考えられる。

Q3．ギャップ分析の方法論はあるのか？
A3．レーダチャートによる視覚で分析するため実務に耐えられるものと考えている。利用者の経験則になる。

Q4．分析する際の項目へのウェイトのかけ方だがアドバイスはあるか？
A4．それぞれの企業の事情によりウェイトのかけ方が変わるので、クライアントと合意することが必要と思う。ツールにはデフォルト値があるが考えて使用すること。

Q5．金融機関に勤めているが、金融検査マニュアル、FISCのシステム監査基準、ISMS、JIS X 5080、JIS Q 2001、情報セキュリティ監査基準、システム監査基準など様々な基準があり、それぞれ少しちがう。何を使えばよいのか？
A5．各要求項目を包含したカバー範囲の確認が有効。JRMSは各基準から重要と思われるものを抽出し情報リスク対応用に開発した。

Q6．ケーススタディ「X社のリスクマネジメント」にある質問対象者の数は、経営者層3名、リスクマネジメント部門5名、情報システム部門5名、ユーザ部門4名であるが、それくらいの質問対象者数で妥当なのか？
A6．妥当と思う。中堅企業を対象に事例としている。質問項目が1004項目あるので、あまり人数を増やすと入力作業がたいへんになることもある。

Q7．実際事例は集まっているか？　うまい使い方はあるか？
A7．まだ未集計の段階であると思う。特定のシステムを対象として適用することも可能であるのでうまく使ってほしい。

最後に、講師に対して受講者から満場の拍手で謝意が述べられました。

第104回月例研究会報告

開催　平成16年6月22日（火）
場所　中央大学駿河台記念会館
講師　日本システム監査人協会会長
　　宮川　公男氏
演題　「統計学でリスクをマネージする」

No.898　竹下和孝

(はじめに)

“あなたの数字の読み方は正しいか”と問われると応えに困るのが大方の反応ではないでしょうか。ましてやリスクを統計学で評価するとなると、溜息だけ。

当初の心配とは裏腹に、すっきりした気分になった講演で、出席者130名でした。

(講演要旨)

1. 統計学は難しくない

統計学は数学の一部ではなく、記号と数式を恐れる必要はない。教える人には数学の先生が多い、というだけのことである。

統計学は日常生活の中で利用されている。

我々は本当に必要なものが何かわかっていないと、2種類の間違いをしてしまう。

①必要なものを捨ててしまう誤り ②不要なものを取っておく誤り

数値の変動の大きさを過剰に伝えてしまうことが多いので、比率の使い方にも注意が必要である。

50%down したものを元に戻すには、 100%の up が必要である

この場合、元に戻ったに過ぎないのに、短期的にみると倍増したようにみえる。これらは、日常生活に多くみられる事象そのものであり、貿易統計や新聞報道でも誤用と思われる事件が発生している。

2. 数値の読み方

比率の使い方には注意が必要である。

50%下がった株価が元に戻るためには100%上がらなければならない。

40%下がった株価が元に戻るためには67%上がらなければならない。

1）前月比増減率

新聞の統計記事に小売売上高を見かけるが、季節調整済み前月比増減率として表示されており、誤解を招きやすい。対前月比という値は売上高の時系列変化ではない。ここに使われている数　字は正しくても、対前月売上高増減のような間違った印象を与えてしまうからである。

2）70のルール

金利が7%の場合は、10年で倍になる。
これが0.5%の場合は140年かかる。
現在の0.1%の状況では700年もかかる。

3）構成比率

比率は正しく使わないと内容の異なるものを混在して間違って判断してしまう。

例えば、構成比率（ある特性を持つものの割合）、対立比率（2つの量を対比させて相対的な大小や高低を比較する）は別の指標である。つまり、自己資本比率（＝自己資本／総資本）は構成比率であるが、負債比率（＝他人資本／自己資本）は対立比率である。

4）ダウ平均と日経平均

ダウ式平均株価は、株価の連続性を保つために、ダウ式という計算方式で株価を除している。これは株式の分割による株価の低下が株価合計に影響しないように考慮された計算方法である。

しかしながらダウ式を採用していた日経平均は200/4に銘柄を入れ替えたことにより、除数、倍率ともに大きく変動し、日経平均の連続性を損ない、株価指標としての有用性を失っていると判断される。これは単にダウ式という計算手法の議論ではない。

3. 標準偏差

平均値は同じでもばらつきによって差があることを示したものが標準偏差であり、平均点からどれだけ離れているかを示す。

1）仮説検定法

心配事の統計で常識的な判断そのもの。

日常ほぼ定時に帰宅する几帳面な人の帰宅時間の遅れは、何かあったのではないか心配されるが、不規則な人は午前様でも心配されない。これは仮説検定の判断である。

2）2種類の誤り

コンビニでの仕入れ（1個増やすかの判断）

	＋1個が売れる	1個が売れない
＋1個	正しい決定	オーバーストック（誤り）
そのまま	アンダーストック（誤り）	正しい決定

職場検診（検診結果で異常が発見できるか）

		真　実	
		異常なし	異常あり
検診結果	異常なし	正	誤り
	異常あり	誤り	正

4.意思決定の黄金則

“もうはまだなり、まだはもうなり”という格言がある。

意思決定は、1か0の判断ではあるが、結果に至るまでには、安心と諦めがある。

科学を知っていると、事象を見たときにより正しく理解できる。

決定＝客観＋主観
決定＝計算＋直感
決定＝数学＋判断
決定＝科学＋決断

例）囲碁のルールを知っていると、黒白の棋譜から優劣や軌跡が読める。

(Q&A)

1）健康管理について　（省略）

2）標準偏差、素値の使い方について

科目の中での得点比較、複数科目の合計点による比較は、意味が異なるものである。

3）重大な意思決定を迫られた時に、冷静に判断するための工夫があるか。

情報収集や代替案の検討など、出来るだけのことはやった、という状況になると、安心して判断できる。

(感想)

日常生活や業務の中で、出てきた数値を考えも無く鵜呑みにしていないだろうか。

身近な事例をわかりやすく解説する形で進められた講演を拝聴して標準偏差の意味を正しく理解した、というより、誤った数値の見方や見せられ方について考え直す機会を得た。

自分なりの判断基準を持つことが重要で、意思決定のタイミングで納得いくまで（努力してあきらめるほど）リスク対応計画を練る。軽減・受容と考えて“人事を尽くして天命を待つ”という中国の諺を思い出した。確率にとらわれることなく精一杯努力するところも意思決定の要素である。

参考著作）「統計学でリスクと向き合う」
宮川公男著　東洋経済新報社　1600円＋税

平成16年度第6回理事会議事録

平成16年6月9日（水）18：30～20：00　於：三井物産（株）会議室
出席者：小野、橘和、鈴木（信）、富山、和貝、木村、金子、佐藤、竹下、仲、沼野、蓮見、馬場、原、本田、松枝、山口（忠）、吉田、石島

1. 審議事項

吉田理事、富山副会長等複数の理事から次の事項が、審議事項として提案され、議題とすることが承認され審議した。なお、複数の理事の要求による提案事項も事前に提案出来るものは期限内に案内することが了承された。

(1) システム監査普及サービスの監査チームリーダーに対する報酬
- チームリーダは普通の担当者と比べ5倍から10倍の作業が必要となり、担当した場合の作業負荷がとても大きいので、作業時間に対する報酬が支払えるようにできないか。
- 普及サービスは無料であり、企業からは実費のみ負担をお願いしている。
- 実費には交通費、食事代、作業場所費などが含まれる。
- 普及サービスの趣旨から、監査チームリーダに対して作業時間に応じた報酬を支払うことは難しい。

＞上記を踏まえて、担当理事が報酬に関するルール案を検討して再審議する。

2. 報告事項

(1) 法人部会
- 地方自治体向け「情報セキュリティセミナー」の運用体制と運用手順を制定したので、その説明を行った。
- セミナーの目的はシステム監査の啓蒙普及と法人会員のビジネス機会創造の両面がある。
- 無料セミナーと有料セミナー（講師派遣に対して基本設定として2時間で10万円）がある。
- 有料セミナーの講師を行った法人会員は2割をロイヤルティとして協会へ支払うとともに、作成した資料、アンケート結果を法人部会にフィードバックする。

(2) システム監査人推薦委員会
- 前回理事会で報告したNY社より、監査評議委員について正式な推薦依頼を受けた。
- 台帳に登録された立候補者より選定する予定。
- NY社では、人事関連システムの構築をA社が行っており、B社がプロジェクト監査を行っている。
- 監査評議委員はプロジェクト監査のレビューを行う。

(3) 公認システム監査人
- 6月12日、19日、26日に面接を行う。

(4) JASA情報セキュリティフォーラム
- 情報セキュリティ監査協会より、6月29日に開催する「2004年度JASA情報セキュリティフォーラム」での後援依頼を受け、了承した。

(5) ISACA総会
- ISACAより、6月25日実施の総会について会長宛の案内を受け取った。

(6) 月例研究会
- 5月27日に第103回月例研究会を開催した。
- テーマは「JIPDECリスクマネジメントシステム(JRMS)の狙いと適用」で、参加者は76名だった。
- 次回は6月22日に中央大学駿河台記念館で、宮川会長の講演を予定している。
- テーマは「統計学でリスクをマネージする」で、現在65名くらい受け付けている。
- 7月はシステム監査基準の改定について予定している。
- 会計規定が変更されており、5月開催の月例研究会から理事も参加費を支払うことになった。尚、開催手伝いの担当理事については、報酬規定に従った報酬が支払われる。

(7) システム監査基準の改定
- 現在、パブリックコメントに回答中である。
- 監査基準、管理基準について200以上のコメントを受け付けた。
- 6月中にはめどがつき、7月には発表できる予定である。

(8) 広報
- 協会パンフレットのレイアウトを印刷所に依頼中である。

(9) 会報
・第79号を発送した。
・79号は地方支部の活動報告が多いが、今後も継続する予定。
・次回原稿は7月15日締め切りである。
・新システム監査基準が間に合えば、載せる予定である。
・今後のテーマを検討するために、会報内容についてアンケートを行う予定である。
(10) 普及サービスの状況
① 大手SI企業（c社）
・6名で金融システムのシステム監査を行っている。監査チームリーダーは、成田氏である。
・予備調査まで完了した。
・7月13日に監査報告会を予定している。
② 大手ゼネコン（d社）
・アウトソーシングと個人情報保護の観点での監査を行っている。
・監査チームは9名（他にd社から2名）で、監査チームリーダーは、打矢氏である。
・6月1日にトップヒアリングを行った。
・これから予備調査を開始する予定である。
・9月中旬に監査報告書としてまとめる。
(11) 実務セミナー、実践セミナー
・5月15日、16日に、富山での実践セミナー2日間コースが、北信越支部にご協力頂き、無事終了した。
・8月21、22日、9月4日、5日に幕張OVTAで開催予定の実務セミナー4日間コースの教材の改善を準備中で、現在事例研究会のタスクフォースとして作業中である。
・中四国支部との共催で、10月23日、24日に、広島市で実践セミナー（2日間コース）を行う。
(12) セキュリティポリシー
・情報資産調査が完了した。
(13) 会計
・4半期ごとの報告を行う必要があるが、まだ3月期が完了していない。
・まとまり次第理事会メールで報告する。
(14) 北信越支部
・北信越支部、中部支部、及び日本システムアナリスト協会中部支部と共催で、「中部北陸地区情報処理団体研究会 (IN富山2004)」を実施する。
・日本システム監査人協会HPに掲載について、HP担当で検討して回答する。
(15) 近畿支部
・6月5日に、SAAJ、ISACA大阪支部、システム監査学会の共催、近畿経済産業局、ITコーディネータ協会他の後援で「最新システム監査セミナー」を開催した。120名弱の参加（半分はITコーディネータ）があった。
・6月12日にシステム監査基準の討論会を予定している。
(16) 東北支部の総会
・11日金曜日がITCで、12日土曜日がSAAJである。
・2名の理事が前泊して対応する。
(17) 中部支部
・5月15日（土）岐阜県大垣市のソフトピアジャパンにて例会を開催した。
・3月の中国科学院計算技術研究所との交流会に関する発表及び議論を行った。
・参加者は19名だった。
講演1「日中ソフトウェア産業の発展に向けての提言
ーシステム監査の視点よりー」 若原達朗 氏
講演2「北京訪問団の4日間」 植野真由美 氏
(18) HP
・新HPの準備として、一部を除いてテストが完了した。
・OCNからBIGLOBEへの切り替えは、2週間くらいの内に完了する。
・切り替えが終了したら、WEBマスタのメールアドレスも合わせて連絡する。

以 上

議長 橘和尚道
議事録署名人 富山伸夫、山口忠男

＜次回理事会開催予定＞
平成15年7月14日（水）18:30～
三井物産（株）16階金属会議室（地下鉄大手町C5出口）

平成16年度第7回理事会議事録

平成16年7月14日（水）19：00～20：30　於：三井物産（株）会議室
出席者：橘和、鈴木（信）、富山、小野、蓮見、三谷、藤野、大石、片岡、仲、
沼野、芳仲、本田、力、吉田、岩崎、馬場

1.審議事項

(1) 推薦委員選任の件

小野委員の辞任に伴い、岩崎氏を推薦委員に選任することが提案され、承認された。

(2) システム監査普及サービスの監査チームリーダに対する報酬の件

前回の理事会決定に基づき、吉田理事より報酬に関するルールが下記のように提案され承認された。また、蓮見副会長より監査チームリーダの報酬に関して会計規定を修正することが提案され承認された。

報酬案；チームリーダが被監査企業に訪問し、打ち合わせ・インタビュー・報告等を実施した時間数に1時間当たり3500円を乗じた金額とし、10万円を上限とする。

2.報告事項

(1) 推薦委員会

・6／22の推薦委員会にて、小野委員長の辞任、橘和委員長の新任を決めた。
・6／1に1号推薦の依頼を受けたYK社に6／28付で4名の推薦をした。

(2) 法人部会

・自治体向けセキュリティセミナーのDMを関東地区中心におこなう。
各支部については、支部長と相談の上、支部から発送してもらう。
・公認システム監査人の特別認定講習会の広告を検討いただきたい。
→広報担当で検討する。

(3) 月例研究会

・第104回月例研究会（講師：宮川会長、テーマ：統計学でリスクをマネージ）は、6／22に予定通り開催され130名を超える参加者があった。
・第105回月例研究会（講師：本田理事、テーマ：新システム監査基準管理基準について）は、7／27に開催予定であり、会場は中央大学
駿河台記念館である。
（新システム監査基準・管理基準の公表が遅れており、月例研究会当日に間に合うか不確定の状況にある。）
・7／26に月例研究会の平成16年第二回企画会議を開催する予定である。今年後半の月例研究会のテーマ、講師候補、及び担当理事を決める予定である。

(4)（公認システム監査人）認定委員会

・認定作業が完了した。申請者30名中公認システム監査人内定者は21名であった。

(5) 広報

・（株）秀和システムより、「システム監査・情報セキュリティ監査ハンドブック」（仮）が発刊されることになり、橘和副会長をはじめとして理事数名に執筆等協力いただいた。
・（社）日本電気協会より出稿依頼があった。→芳仲理事にお願いする。

(6) システム監査基準研究会

・システム監査基準がまだ公表されていない。月例研究会に間に合えばいいが。

(7) HP

・7／1に切り替えをおこない、月例研究会がHPから申し込みできるようになった。
・公認システム監査人の公開情報項目の追加について報告があり、
既存取得者の追加受付締切が検討され、8／15までとした。

(8) 事例研

・c 社のシステム監査普及サービスに関するシステム監査報告会を 7 ／ 13 に実施した。
この監査報告会をもって、c 社向け監査普及サービスは完了した。
・d 社のシステム監査普及サービスは 9 ／ 20 ごろ監査報告予定で、予備調査を進めている。

(9) 会計

・監事より 9 ／ 12（日）13：30 より会計監査・システム監査をおこなう旨の通知を受けた
→事務局長，会計担当，岩崎理事，金子理事で対応する。
・NPO の役員登記の更新がまだ完了していない。(一部理事の住所誤りがあったため)

(10) その他

・事務局の PC トラブルがあり、53 通のメールが読めなかった。また現行の回線能力
等の問題もあり、金子理事・岩崎理事に支援いただき、対応していきたい。
・事務局より、会員数・会費納入状況について報告があった。

(11) 監事より

・会員数も増大しているので、問題が生じた際には、会員へのサービスを全うできることを最
優先に考え、それぞれの担当で判断して進めていくようにされてはどうか。
・監事による監査には煩わしい点もあるかと思うが、協力いただきたい。

以 上

議長　　橘和尚道
議事録署名人　馬場孝悦、岩崎昭一

＜次回理事会開催予定＞
平成 16 年 9 月 8 日（水）18:30 ～
三井物産（株）16 階金属 C 会議室 (地下鉄大手町 C5 出口)

支部だより

「中四国支部の活動報告」

報告者　高田裕史

最近の中四国支部の活動内容を報告いたします。2004年6月24日（木）広島県立体育館にてNPO法人ITC広島理事溝下博氏を招き「個人情報保護のための内部管理体制の整備」について2時間ご講演いただきました。同氏はシステム監査技術者試験合格者であり、会員との質疑応答にて個人情報保護についての具体的な方策やシステム監査との関係等の意見交換ができました。次に、7月21日（水）個人情報保護に実際に取り組まれている会員により会社としての取組みについてご講演いただきます。中四国支部の会員で支部会に出席されていない方は是非これからの支部会にご出席いただければと思っております。

「中部支部7月例会のテーマ発表の紹介」

7月の中部支部の例会で発表されたテーマ発表の1つ「バランスド・スコア・カードの有効性」を紹介します。発表者は、関口幸一氏（会員No.737）です。

これを読んで参加したくなった方、9月18日の浜松例会、11月27～28日合宿にふるって参加ください。浜松例会の後の懇親会は、地ビールレストランです。また、合宿は、愛知県の健康増進のための施設での開催なので、健康に気を使う方のもおすすめです。

＜発表＞

「バランスド・スコア・カードの有効性」

No.737　関口氏

Sec1. BSCの基本的な考え方

社長の嘆き

- 社長の年度方針を展開できていますか？
- 社員は自分のテーマを実行できていますか？
- 中間管理職は、苦しんでいませんか？

これらは、戦略や目標も具体的実施計画にできてないため「絵に描いたもち」に終っています。

このためBSCは、財務指標だけでなく、顧客の視点、社内プロセスの視点、学習と成長の視点で指標を作ります。つまり顧客に対して、自分をどう位置づけ、どうアプローチするのか戦略を立案することです。その結果として、財務指標が向上します。

4つを総合的に計画立案することをBSCは提唱します。

Sec2.BSC特徴

2つの特徴は

- 戦略と日々の業務の結びつけるツール
- 組織業績のモニタリング指標や評価指標の策定を効果的に支援するフレームワークであり、キーポイントは戦略を日々の具体的な行動に結びつける「社員も含めた総力戦にすること」です。

続いて手順や事例照会、質疑応答や意見交換も活発に行なわれました。

総務省主催行政情報システム技術研究会で橘和副会長講演

2004年6月30日、総務省行政管理局が主催する行政情報システム技術研究会（第7回）で、橘和副会長が「行政情報システムにおけるシステム監査の導入について」と題して講演された。同研究会は、中央省庁の情報システム担当者を対象に総務省行政管理局が開催している(霞ヶ関の経済産業省別館8階、午後2時から3時30分まで)。

講演の内容は、システム監査とは、システム監査の意義、システム監査基準と情報セキュリティ監査基準の関係、システム監査はどう行われるか、行政情報システムの監査主体の要件、大阪府電子調達システム開発のシステム監査、宇治市のシステム監査の事例など、である。

当日の出席者は、事務局を入れて50名で、普段の研究会出席者が30名前後とのことで、関心の高さがうかがえた。

質問は、文部科学省の方から「システム監査の頻度はどれくらいか、一回やれば当分やらなくて済むのか」、会計検査院の方から「開発中のプロジェクトへの監査だが、計画案の策定からか、実行計画が決定された後なのか」などであった。なお、広報担当として、鈴木（信）も同行し、質疑応答に参加かつNPO法人としての活動のPRも行った。

会員の書いた書籍紹介

『女性ITプロフェッショナルのホンネ会議』
著者：Tea Time
出版社：日経BP社
定価：本体1400円＋税

No.239　小野修一

本書の著者は「Tea Time」というIT業界で働く女性エンジニアの私的グループであり、メーリングリストを中心に活動しているとのこと。その中の16名の共同執筆で、SAAJの会員も数名含まれている。しかし、執筆者は全員がペンネームなので誰だかは分からない。記事を読んで、これはきっとあの人だ！と想像するのも楽しみの1つかもしれない。

さて、内容はというと、社会で働き生活する中で直面するさまざまな問題に、まさにホンネで悩み・思い・主張を語ってくれている。女性という枕言葉が付いているが、それぞれのテーマは男女を問わないものがほとんど、女性の視点からの指摘・提案となっている。

実際の章立てからいくつか項目を抜き出してみると、

第1章　ピンチ！どうやって切り抜ける？
- 作ったプログラムがバグだらけ！
- 英語ができないのに海外出張！
- イヤな仕事を与えられた！
- 有給休暇を使い切ってしまった！
- 産休明けたら席がなかった！

第2章　チャンス！どうやってモノにする？
- 5回の転職で違う世界を体験
- 国際企業の経営者に
- 文系を私が学会で発表
- おじさんと上手につき合う
- いつの間にか、書いた本が60冊

第3章　オフ！どうせなら徹底的に
- 趣味の仲間を持とう
- 子供とパソコンを使う楽しさ
- ストレスの予防と対応八カ条
- ボーナスで自分にごほうび
- 子供を持って人生が豊かに

ほとんどの項でなるほど！と思ったが、私には第2章の「チャンス！」が特に印象的であった。男性だ、女性だ、は関係ない。力一杯仕事をして、仕事以外の時間を大事にして、家族や仲間との交流を大事にして成長する。改めて、そんなことの大切さを認識させてくれる1冊である。皆さんもどうぞご一読を。

第4回システム監査実務セミナーのご案内

NPO法人日本システム監査人協会

NPO法人日本システム監査人協会では、設立目的のひとつである「システム監査人の実務能力の維持・向上」のため、下記の日程で第4回目のシステム監査実務セミナー4日間コースを開催いたします。

本セミナーでは、当協会事例研究会で実施したシステム監査普及サービスの事例を教材とし、実践で得たノウハウを会員の皆様と共有することを目標にしています。また、このセミナーを受講後に事後課題を提出頂き、その内容が適切と判断された場合には、公認システム監査人認定に必要なシステム監査実務を1年間経験したものとみなされます。

システム監査技術者試験には合格したもののシステム監査を経験されていない会員の皆さん、この機会を利用してシステム監査の実際を体験し、システム監査能力の向上を図りましょう。非会員の方も大歓迎です。多くの皆さんの参加をお待ちしています。

尚、本セミナーは、以下の資格をお持ちの方の認定セミナーともなっております。

・ITコーディネータ対応専門知識研修コース
(獲得知識ポイント5.5ポイント　22時間)
・日本公認会計士協会の継続的専門研修制度におけるCPE認定研修
(履修単位：29単位)

記

1. 日　　時（前半）平成16年8月21日（土）～22日（日）
第1日目10：00～20：00
第2日目9：00～15：00
（後半）平成16年9月4日（土）～5日（日）
第3日目10：00～20：45
第4日目9：00～15：00
＊参加は、前半、後半の通しとし、どちらか一方のみの参加は出来ません。

2. 場　　所　幕張OVTA（海外職業訓練センタ）
(最寄駅：JR京葉線海浜幕張駅徒歩5分)
〒261-0021　千葉市美浜区ひび野1丁目1番地
電話番号：043-276-0211

3. 受講費用　SAAJ会員：　168,000円、非会員：　189,000円
（費用には、宿泊費、食費、消費税を含みます。）
※テキストとして日本システム監査人協会編「情報システム監査実践マニュアル」(4,200円税別）を使用しますので、お持ちで無い方は別途必要となります。

4. セミナー内容
事例研究会が実施したシステム監査普及サービスをケーススタディとして取り上げます。
4～5人程度のグループにわかれ、監査依頼事項の確認、
トップインタビュー、監査テーマ・監査計画の作成、
予備調査、本調査、監査報告の実際を、
前半、後半の4日間のセミナーを通し体験して頂きます。

5. 講　　師　事例研究会メンバーのシステム監査普及サービス経験者8名（予定）講師は監査手順の解説・指導の他、被監査企業の社員の役割も演じます。

6. 募集対象者および人員
日本システム監査人協会会員（法人会員を含む）、
システム監査技術者試験合格者あるいは同等の能力を持つ方、
システム監査に従事される予定の方、
システム監査を業務に役立てたい方、
システム監査技術者試験受験予定の方、
ITコーディネータ、公認会計士の方など。
定員20名（最小催行人員10名）

7. 申し込み先　NPO法人日本システム監査人協会
第4回システム監査実務セミナー事務局担当
三輪智哉
※　下記の申込内容を記入の上E-Mailでお申込下さい。
(E-Mail：t_miwa@st.rim.or.jp)

8. 申し込み期限　平成16年7月30日（金）

NPO法人日本システム監査人協会
第4回システム監査実務セミナー参加申込書

平成16年　　月　　日

①会員No..（法人会員の場合は法人名、会員で無い方は「非会員」)：
②氏　名：
③勤務先名称：
④勤務先所属：
⑤資料送付先住所：
⑥資料送付先宛名：
⑦資料送付先TEL：
⑧連絡先E-MAILアドレス：
⑨システム監査実施経験：　あり　／　なし
⑩当協会主催のシステム監査実践セミナー参加経験：　あり（　年　月）／　なし
⑪当協会主催のシステム監査実務セミナー参加経験：　あり（　年　月）／　なし
⑫テキスト購入希望：　あり　／　なし
（テキスト：日本システム監査人協会編「情報システム監査実践マニュアル」をお持ちでない方には、割引価格（3,600円税込み）で頒布し、事前資料と共に発送致します。）

以　上

平成16年度第2回システム監査実践セミナー（in 広島）受講者募集のご案内
システム監査未経験の皆様へ
システム監査実践セミナーに参加し、システム監査の実際を体験してみませんか !!

NPO法人日本システム監査人協会では、設立目的のひとつである「システム監査人の実務能力の維持・向上」のため、下記の日程で平成16年度第2回目のシステム監査実践セミナーを開催いたします。

このセミナーは、当協会が既に13回の開催実績を重ねる、「システム監査実践セミナー」（1泊2日コース）です。

本セミナーでは、当協会事例研究会で実施したシステム監査普及サービスの事例を教材とし、実践で得たノウハウを会員の皆様と共有することを目標にしています。また、このセミナーを受講し、事後課題を提出頂きその内容が適切と判断された場合には、当協会が認定する公認システム監査人の必要なシステム監査実務を6ヶ月間経験したものとみなされます。

従い、システム監査技術者試験には合格したもののシステム監査を経験されていない会員の皆様、この機会を利用してシステム監査の実際を体験し、システム監査能力の向上を図りましょう。 多くの皆さんの参加をお待ちしています。

本セミナーについては、以下の資格をお持ちの方の認定セミナーでもあります。

・ITコーディネータ対応専門知識研修コース
（1年度間上限なしで換算できる学習時間12時間。知識ポイント：3ポイント相当）
・日本公認会計士協会の継続的専門研修制度におけるCPE認定研修（予定）

記

1. 日　　時　平成16年10月23日（土） 13：00より
平成16年10月24日（日） 16：00まで

2. 場　　所　RCC文化センター
http://www.rccbc.com/
広島市中区橋本町5-11
電話番号：082-222-2277

3. 費　　用　会員： 80,000円、非会員： 100,000円
（費用には、教材費、宿泊費、食事費を含みます。）
テキストとして日本システム監査人協会編「情報システム監査実践マニュアル」（工業調査会 定価4,200円税別）が別途必要となります。

4. セミナー内容　事例研究会が実施したシステム監査普及サービスをケーススタディとして取り上げます。4～5人程度のグループにわかれ、予備調査、本調査、監査報告などの演習をロールプレイング形式をまじえ、2日間のセミナーを通し体験して頂きます。

5. 講　　師　事例研究会メンバーのシステム監査普及サービス経験者6名（予定）
講師は監査手順の解説・指導の他、被監査企業の社員の役割も演じます。

6. 募集対象者および人員

日本システム監査人協会会員（法人会員を含む）、
システム監査技術者試験合格者あるいは同等の能力を持つ方、システム監査に従事されている方
定員 20 名（最小催行人員 10 名）

7. 申し込み先　NPO 法人日本システム監査人協会
システム監査事例研究会　事務局担当　沼野伸生　宛
※下記の申込内容を記入の上 E-Mail でお申込下さい。
(E-Mail：fwgc5762@nifty.com)

8. 申し込み期限　平成 16 年 10 月 1 日（金）

9. 問い合わせ　NPO 法人日本システム監査人協会
システム監査実践セミナー事務局担　沼野伸生
E-Mail：fwgc5762@nifty.com

以　上

NPO 法人　日本システム監査人協会
平成 16 年度第 2 回システム監査実践セミナー in 広島　参加申込書

平成 16 年　月　日

① 会員 No.（法人会員の場合は法人名）：
② 氏　名：
③ 資料送付先：
（住所）〒
（宛名）
④ 連絡先　E-MAIL アドレス：
（電話 No.　FAX-No.　）
⑤ 当協会主催の
システム監査実践又は実務セミナー参加経験：　あり（　年　月）／　なし
⑥ システム監査実施経験：　あり　／　なし
⑦ テキスト購入希望：　あり　／　なし
（テキスト：日本システム監査人協会編「情報システム監査実践マニュアル」をお持ちでない方には、当日会場にて市販価格の 2 割引（3,600 円税込み）で頒布いたします。）

以　上

公認システム監査人及びシステム監査人補に関する公開情報の追加について

公認システム監査人、システム監査人補　各位

平成16年7月23日

特定非営利活動法人 日本システム監査人協会

公認システム監査人及びシステム監査人補に関する情報は、現在、当協会のホームページの公認システム監査人名簿（http://www.saaj.or.jp →公認システム監査人→「公認システム監査人名簿（公開）」）に掲載していますが、この公開情報に「得意分野」を追加して掲載することができるようになりました。

下記により、「得意分野」に掲載する情報を受付けますのでご通知ください。

記

1. 掲載できる項目（希望者のみ）
   <旧（現行）>　氏名、都道府県、ホームページ
   <新　　>　氏名、都道府県、得意分野（追加）、ホームページ

2. 追加掲載する項目
   得意分野3項目とする。
   得意分野は業種、専門、実績、アプリケーション等とし、各項目とも全角15文字以内とする。
   （句読点、括弧、カタカナ、促音、長音等も全角1文字とする）
   ＜得意分野の例示＞
   例示1：流通業（情報戦略）
   例示2：金融（情報セキュリティ監査）
   例示3：ISMS、個人情報保護
   例示4：ネットワークのセキュリティ監査
   例示5：会計情報、人事・給与システム

3. 掲載（開始）時期
   平成16年度春期公認システム監査人の公開時期と同じとする。
   掲載予定時期は、平成16年9月中旬の見込み。

4. 受付期限
   平成16年8月15日とする。
   （受付期限を過ぎても、情報の追加・変更はできますが、事務局の作業の都合上遅れる場合があるのでご了承願います。）

5. 通知方法
   日本システム監査人協会事務局 (saajjk1@titan.ocn.ne.jp) あて、以下の内容のメールで通知する。
   (1) 氏名、都道府県名、認定番号
   （※注意：認定番号は、認定証内のKまたはHに続く6桁の英数字のこと。
   協会会報郵便物の氏名に沿えてある数字だけの協会会員番号ではない）
   (2) 得意分野
   ①××××××××××××××××　（全角15文字）
   ②××××××××××××××××　（全角15文字）
   ③××××××××××××××××　（全角15文字）
   ＜15文字を超過した場合は、16字以降切捨て＞

6. その他
   公開情報の詳細、連絡先等は、ホームページ上の「平成16年度秋期公認システム監査人募集要項」をご参照ください。

以　上

新規入会者一覧

会員番号	氏　名	勤務先名	勤務先所属	支部/地域
1390	新井　浩一	関西電力(株)	監査役室	近畿
1391	黒沢　兵夫	日本電気(株)	ナショナルセキュリティ・ソリューション事業部	関東
1392	杉本　一郎	(株)リコー	ネットワークシステム推進部 コンサルティング事業グループ	関東
1393	松崎　雅之	(株)富士総合研究所	業務管理部	関東
1394	大川　秀喜	光陽無線(株)	システム技術課	九州
1395	田村　丈夫	オフィスアコード		九州
1396	黒川　俊雄	株式会社シーエーシー	会計ソリューション構築センター	関東
1397	近森　健三	東京海上リスクコンサルテイング株式会社	リスクコンサルテイング室	関東
1398	山内　英樹	山之内製薬株式会社	情報システム部	中部
1399	奥山　順子	日本アイ・ビー・エム株式会社	ibm.Comセンター事業部	関東
1400	磯部　勤	花王株式会社	ヘルスケア第2研究所	関東
1401	阿漕　和司	インターネットセキュリティシステムズ株式会社	プロフェッショナルサービス部	関東
1402	向田　弘	三菱電機情報ネットワーク(株)	OSD事業部	関東
1403	竹村　徹也	株式会社シーイーシー	北陸システム部	北信越
1404	鶴　恒芳	松下電器(株)PSS社	本社　情報システムG	関東
1405	梅原　伸行	有限会社サイラス		関東
1406	掘　泰史	株式会社アイ・ティ・フロンティア	システム・アカデミィ	関東
1409	金児　智子	(株)MHトラストシステムズ	公共法人システム部	関東
1410	永井　和彦	NECシステムテクノロジー(株)	ソリューション事業統括本部	近畿
1411	岡谷　享	グローバルセキュリティエキスパート株式会社	コンサルティング事業部	近畿
1412	堀田　雅寛	株式会社HBA	経営管理本部品質管理部	北海道

＜編集後記＞

新しいシステム監査基準がやっと公表される見込みです。会報80号は、8/4に開催される経済産業省による説明会をターゲットとして、できるだけ多くの情報ソースを織り込みました。関係者のご尽力に感謝します。ISMSをはじめとする情報セキュリティ関係の需要は、来年春の個人情報保護法の完全施行の後押しを受けて、今後も急増すると見込まれています。

新基準と共にシステム監査も本格出動です。当協会に期待される役割や会員諸氏の活動範囲も着実に広がりを見せています。それぞれの立場でのご活躍を祈念いたします。(K.T)

発行所　特定非営利活動法人 日本システム監査人協会
発行人　宮川　公男
事務局　〒163-0716
東京都新宿区西新宿 2-7-1
新宿第一生命ビル 16階 16W4 号室
TEL. 03(3348)4415 FAX. 03(3348)4416
事務局メール：saajjk1@titan.ocn.ne.jp
ホームページ　http://www.saaj.or.jp/

※ 会員専用メーリングリストで様々な情報提供を行っています。ご加入はowner-saaj@mla.nifty.ne.jpにお問い合わせください。また受信アドレスの変更時も手続が必要になりますので、上記アドレスまで連絡してください。

会報担当委員
竹下　和孝　池島　晃
富山　伸夫　須田　勉
吉田　裕孝　木村　陽一
仲　厚吉　藤野　明夫
力　利則　山田　正寛

※会員のみなさまからの投稿（連載、随筆等何でもOK）を募集します。記名記事は薄謝進呈します。書籍紹介欄もありますので、執筆されたかたはお知らせ下さい。

会報担当メール：saaj-kaihoh@yahoogroups.jp