近畿支部　２０１１年度研究大会　報告

№１６９　林　裕正

・日時　　２０１１年8月２０日（土）　１０時～１７時
・場所　　大阪大学中之島センター　１０階　佐治敬三メモリアルホール
・統一テーマ　「サスティナブル社会に貢献するシステム監査の実現を目指して」
・参加者数　　１１０名（発表者を含む）
・概要

本研究大会は、近畿支部の研究活動とワーキンググループの活動の報告、及び会員から応募のあった研究論文の発表を行ったものである。大会の形式は、発表者による説明、座長のコメント、及び会場の参加との質疑応答である。吉田支部長のコメントに続き、１０編の発表の報告を、近畿支部の３名の会員に分担して報告頂いた。

＜吉田支部長コメント＞

研究大会参加者の皆様
研究大会実行委員会の皆様

研究大会では、大変お世話になりました。

皆様のご協力で、概ね、順調に進行することができました。反省点もいろいろありますが、来年の開催に向けて、準備をしていきたいと考えています。

また、論文発表予定の１名の方が、やむを得ない事情で発表できなかったことは残念ですが、近畿支部の総力を挙げて、システム監査人の専門集団として、今後の指針を見出すことができたと自負しています。

当日の参加者は、ＳＡＡＪ　５７名、ＩＳＡＣＡ・一般　４８名、招待者　５名の合計　１１０名でした。懇親会も、３７名のご参加を頂きました。また、予稿集も１５０部印刷し、当日出席者及び、本部・各支部に配布しました。

今回、発表や座長の機会がなかった方も、是非、次回には、積極的にご参加下さい。

今後ともよろしくお願いします。

近畿支部長　吉田　博一

<<開会挨拶>>

今回の統一テーマを「サスティナブル社会に貢献するシステム監査の実現を目指して」としているが、サスティナブルを次の3つの意味でとらえたい。

一番目に、企業・行政等あらゆる組織でＩＴの活用が不可欠となっており、社会環境等の変化に対応できるＩＴの活用が必要となってきている。

二番目に、我々システム監査人が持続可能な能力を身に着け、社会環境の変化に耐えうる持続可能な知識を習得し、その能力を発揮する必要がある。

三番目は、今回の東日本大震災で甚大な被害を被った社会に対して、我々システム監査人の知識・経験がどのように活かせるかが問われている。近い将来、西日本でも東海・東南海・南海地震に加え、日向灘沖の4連動の巨大地震が発生し、20メートルを超える津波が襲い大阪湾にも流入するとも言われている。東日本の復旧・復興に尽くしていくと共に、我々自身の問題として、再度、大災害を前提にサスティナブル社会を構築する必要がある。

<<吉田支部長 開会挨拶>>

＜報告者　植垣　雅則（No.1380）＞

１．コンプライアンスのシステム監査研究会　報告

発表者：雜賀　努　氏（株式会社ニイタカ　監査室）

座　長：石島　隆　氏（法政大学大学院イノベーション・マネジメント研究科 教授）

【発表の概要】

情報通信技術の進歩により、情報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、一般企業の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ている。システム監査学会との共同プロジェクトであり、今回は中間報告を行う。

①研究の経緯

第一期：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。

第二期：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、第一期の成果物の見直しを行った。

第三期：2011年7月～現在進行中（2回開催）

今後の研究プロジェクトの対応方向の検討。

②研究の中間成果物（部門・業務別コンプライアンスMAP）

J-SOXの内部統制の枠組みの中ではコンプライアンスが該当し、その中でも情報システムに関連する部分を対象とした。メーカーを企業モデルとして、「部門・業務別コンプライアンスMAP」を作成した。当MAPを作成した際の考え方と記載例は以下のとおりである。

	大部門	部署	業務	関連法令	関連情報システム
説明	以下の３つに分類 1.本社管理部門（ｺｰﾎﾟﾚｰﾄ部門） 2.工場・物流・研究部門 3.営業部門	総務部、人事部等の通常企業に存在すると思われる部門を設定。	実際の業務内容が分かるレベルで記載。	関連する法令を情報システムとの関連に係りなく網羅的に記載。	使用しているまたは関連のあるシステムを網羅的に記載。
例	本社管理部門（ｺｰﾎﾟﾚｰﾄ部門）	総務部	定款管理	会社法	文書管理

③今後の対応

経済産業省のシステム管理基準及び監査基準について、コンプライアンスの観点からは以下の点が課題であると認識している。

・記載されているコンプライアンス項目は個別具体的な項目ではない。

・個別の監査現場で実際に使用できるものとはなっていない。

今後の研究では、監査目的をコンプライアンス、監査対象を企業の部門と業務で絞り込むことにより、できるだけ監査現場で使用できる基準を設定する予定である（システム監査基準及び管理基準のサブセットとの位置づけ）。

今後の研究を活性化するためにも、新メンバーを募集中であるので、奮って参加して欲しい。

【座長コメント】

・中間段階ではあるが、「部門・業務別コンプライアンスMAP」の作成は一定の成果である。

・コンプライアンスのシステム管理基準の作成・完成を目指して今後の活動を推進して欲しい。

【所感】

「コンプライアンス」という用語はよく見聞きするし、何気なく使うことも多い中で、MAPという具体的な成果物を交えての説明を受けたことにより、改めてコンプライアンスの意義や視点を考える有意義な機会となった。

＜報告者　植垣　雅則（No.1380）＞

２．システム監査法制化研究会　報告

発表者：田淵　隆明　氏（株式会社アロウズコンサルティング　マネージャー）

座　長：松田　貴典　氏（大阪成蹊大学　副学長）

【発表の概要】

１．はじめに

1.1.システムの不備に起因するトラブル：近年、プログラムの誤りなどに起因するトラブルにより、広範囲にわたる経済的損失・人的被害が多発している（鉄道事故、福島第一原子力発電所事故など）。

1.2.我が国の現状：情報システムの高度化・複雑化によりブラックボックス化が進行し、業務の属人化が進んでいる。これに伴い品質確保が困難になっている。
J-SOXの導入により、「IT全般統制」については状況が改善したが、「IT業務処理統制」は芳しくないのが現状。会計分野では、退職給付債務、償却計算、連結会計システムなど要注意である。

1.3.諸外国の事情：米国では、公共システムや医療システムについて、システム監査が既に法制化されている。韓国、台湾でも、公共システムについて、システム監査が義務化されている。システム監査が法制化されていなくても、ソフトウェアに製造物責任法が適用される先進国は多い。

1.4.今後の方向性：我が国の産業競争力の確保、サスティナブル社会の形成のために、システム監査の法制化の実現は極めて重要な施策である。

２．これまでの活動のまとめ

2.1.公共系のシステム監査：医療機器については「EMC規制」があり、動作確認等について情報システムに関する外部監査が法制化されている。その現状を踏まえ、以下の2点を提言する。

提言①：公共分野・医療分野におけるシステム監査の法制化を推進する。

提言②：会社法を改正し、大会社/委員会設置会社に「システム監査人」の設置と「監査役会」等への監査報告を義務付ける。

2.2.ソフトウェア：以下の2点を提言する。

提言①：製造物責任法第2条を改正し、「製造物」の中にソフトウェアを追加する。

提言②：市販ソフトウェアのリコール制度の確立。

３．我が国におけるシステム監査法制化の動き

3.1.1990年以降の状況：1990年代に金融不祥事等の経済事件が多発したことを受け、システム監査の法制化を求める提言があったが、近年はセキュリティ分野や個人情報保護以外はあまり進展がない。

3.2.J-SOXの影響：現在、J-SOX後遺症が蔓延しており、特にJ-SOXの意味の取り違えによる「3点セット」の影響は大きい。

４．システム監査を法制化する具体的方法

4.1.短期的課題への対応策：(1)有価証券報告書へのシステム監査の記述の追加。(2)SI認定制度の再開。(3)研究開発費の資産計上の再開(IFRS)。

4.2.中期的課題への対応策として以下の事項が考えられる。

(1)一定規模の計算機システム利用事業者に対するシステム監査の義務化。一定規模の業務ソフトウェアの製造事業者・販売事業者に対する品質に関するシステム監査の義務化。

(2)「ソフトウェアの品質維持に関する法律」(仮称)を制定し、市販ソフトウェアのリコール制度を確立する。一定規模のソフトウェア製造事業者・販売事業者に、情報処理試験の有資格者等の確保を義務付ける。(不動産取扱業における「宅地建物取扱主任者」などと同様の考え方。)
(3)会社法の改正：大会社/委員会設置会社はシステム監査人を置かなければならないとする。

【座長コメント】

①システム監査の法制化は古くからの課題である。これまでの取組みで実現できていない理由を明らかにすることも有用である。

②様々な問題が例示されたが、システム監査をすればこれらの問題が未然防止されたのかが疑問として残ったので、その関係を明確にすることが望まれる。

③公共・医療分野が例示されていたが、コンピュータウイルス拡散の件など社会的影響の大きさを考慮した分野についても検討が望まれる。

上記の課題はあるものの、具体例として法律の条文レベルでの改正案を示すなど、詳しく研究している点は評価できる。「システム監査の法制化」は社会として有意義であり、今後の活動に期待したい。

【所感】

「システム監査の法制化」という骨太のテーマであったが、いろんな具体例を交えての説明は分かりやすく、一人のシステム監査人として社会にどのように貢献していくべきであるか、深く考えさせられる機会となった。

＜報告者　植垣　雅則（No.1380）＞

３．ＢＣＰ研究会　報告

発表者：荒町　弘　氏（株式会社 内田洋行　官公自治体ソリューション事業部）
座　長：福本　洋一　氏（弁護士法人第一法律事務所・大阪事務所）

【発表の概要】

＜第1部　研究会発足～A社共同に至る経緯＞

〔研究会発足の経緯〕近畿支部総会後の情報交換会をきっかけにして、2010年2月17日のキックオフを経て研究会を発足し、WGを進めるにあたっての目標設定を行った。当初はメンバ8名でスタート。

〔具体的な研究内容の検討〕研究を始めると、リスク分析をどのようにすればよいか？何をベースにしたBCPがよいのか？など、研究の進め方について悩みが多い状況に…

〔リスクに対する認識の整理〕BCP策定への取組みとしては、「ビジネスインパクト分析」「リスク分析・評価」が必要と理解するも、具体的な分析を研究会メンバが行うことは不可能であった。

〔協力企業（A社）との接点・アプローチ〕上記課題を受けての検討の結果、より実効性あるBCP策定のためには、実際の企業との協同作業が最も近道であるという認識に至り、協力企業を探すことにした。取引関係にある企業からA社を紹介いただき、A社に「BCP策定の協同取組み」の趣旨説明などを行った結果、9月に承諾を得ることができた。

〔協力企業（A社）への提案内容〕以下の5点をA社に提案し、承諾を得た。

1. 取組みの目的：事業継続・企業の利益を守る
2. 取組みの内容（BCP策定に向けた活動）：IT部門と重要業務システムを対象
3. スケジュール：無理のないスケジュール
4. 成果品：既にあるガイドラインを用いた取組み
5. その他（経費等）費用は頂かない

＜第2部　A社概要とBCP策定支援活動について＞

〔A社の概要（企業とITの概要）〕化学系企業。全国に約20箇所の事業所と機械工場・化学工場・物流

拠点を持つ。全社のITは本社ICT部門（メンバ3名）が担当。
〔A社の概要（BCP策定に向け）〕本社ICT部門の3名は月に計1.5人日程度しか割けず、少ないマンパワーでの取り組みである。A社のサポートベンダからも協力を得た。活動頻度は月1回として進めた。
〔A社との契約など〕A社とSAAJの間で「ICT部門の業務継続計画（BCP）策定支援サービスに関する覚書」「機密保持契約書」を取り交わした。
〔A社のBCP策定支援活動〕「地方公共団体におけるICT部門の業務継続計画（BCP）策定に関するガイドライン」を用いて、A社が主体でBCPを策定し、SAAJは助言などの支援を行う。
＜第3部　具体的な活動内容＞
〔WGの活動経緯とキーイベント〕2010年10月にA社との合同WGを開始し、6回の合同WGを重ねて、2011年6月にドキュメントの中間確認を行った。
〔BCP策定に向けた取組み〕以下の流れで作業を行った。
「重要業務（システム）の選定」→「優先順位づけ」→「運用状況の確認」→「現地視察・サーバ室確認」→「改善ポイントの洗出し」→「ドキュメントの整理」→「BCP（簡易版）の作成」
〔東日本大震災の影響（東日本の事業所にて）〕合同WGの期間中に東日本大震災が起こった。その影響としては、人的被害は無し、関東の事業所に被害、ITへの影響は無しなどであった。
〔BCPとシステム監査〕システム管理基準における事業継続計画に関する項目について、どのように理解すればよいのか、当該項目が実現できているかの確認をどのようにすればよいのかを研究した。
〔WGとしての中間評価〕当初設定した3点の目標に対するWGとしての評価は、以下のとおりである。
1. 研究会メンバーとしてBCPに関する知識と理解を深める。→理解出来てきている。
2. ITのビジネスリスクやリスク分析について意見交換し見解をまとめる。→A社との協同活動を通じて継続中。
3. 中小企業にフォーカスしたリスク対応ケースを作る。→取組み継続中。

【座長コメント】
BCPとシステム監査ということで、東日本大震災の後では関心の高いトピックスである。研究成果を広くアピールし、中小企業のBCP策定に貢献して欲しい。弁護士として法的な観点でのコメントを述べる。
・BCPの策定は、法的には法令遵守体制の構築（内部統制）の一環として捉えられるため、あくまで全社的な内部統制の問題として整理されるべきである。IT部門だけに限定したWG活動としているが、できるだけIT部門と他部門との関係も意識した取組みが望まれる。
・企業の経営者には内部統制としてBCP策定義務があるのかとの論点があり、これを怠ると取締役としての善管注意義務違反の責任を問われるおそれもあることから、このような観点から、BCP策定及びそのシステム監査の必要性を、経営者にアピールすることも今後取り組むべき事項である。

【所感】
東日本大震災を受けて事業継続計画を検討し整備することは、全ての企業・組織にとって喫緊の課題であると思われるが、一方で各種のリソース不足から、その推進がままならない企業等が多いとも聞く。当プロジェクトの成果物を活用して、少しでも多くの企業等が事業継続計画の整備を進めることができれば、サスティナブル社会の進展に貢献することにもなるので、非常に有用な研究であると感じた。

＜報告者　尾浦　俊行（№.1497）＞

４．クラウドコンピューティングのシステム監査（中間報告）

発表者：深瀬　仁　氏（パナソニック溶接システム株式会社）

座　長：永田　淳次　氏（桃山学院大学非常勤講師）

【研究会の目的】

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。（システム監査学会との共同プロジェクト）

【活動実績】

①クラウドの概念を学ぶ

クラウドの特性・特徴は

・On-demand self-service：オンデマンドセルフサービス

・Broad network access：広範なネットワークアクセス → ネット上の脆弱性対策が困難

・Resource pooling：地理的制約がないリソース共有 → データ保管場所の特定は困難。保管場所が海外だと日本の法律を適用できず、また消去確認も困難　※監査対応に不向き

・Rapid elasticity：利用に応じた拡張・縮小性

・Measured Service：サービス性能の測定可能

②最新動向の把握

サービス提供側（富士通、セールスフォース.ドットコム）から話を聞いた。

（富士通の場合）

・クラウド活用のためには標準化（ガバナンス）を進めることが不可欠と考え、クラウド特化ではなく全体最適の視点で企画提案している。

また、その手法として

・業務仕分けを行い、各業務に必要なサービスレベルを整理。

・必要なサービスレベル別にクラウドとオンプレミスの組み合わせを提案。

（セールスフォース・ドットコムの場合）

・Ｔｒｕｓｔサイトで稼働状況を公開。

・総務省「ＡＳＰ・ＳａａＳ安全・信頼性に係る情報開示認定制度」に基づく情報開示。

・ＳＡＳ７０TypeⅡ　監査レポートを年二回提供可能。

などの取り組みがなされていることがわかった。

【研究会としての今後の方向性・・・質疑を踏まえて】

・ＳＡＳ７０TypeⅡ等が提出された際、それをどう判断するか。

・何が監査できないのか、どうしたら監査できるのか。絞り込んで検討。

・システム管理基準にクラウド特有の部分を付加する方向で進める。

【所感】

富士通の取り組みは、顧客のシステム部門のクラウドへの過剰（安易）な期待により、のちのち顧客のユーザ部門との間で発生しうるトラブルを避けつつ、クラウドをメニューのひとつとしてビジネスを拡大・展開するために丁寧に練られた手法といえる。セールスフォース・ドットコムの取り組みは顧客内のユーザ部門よりも監査やステイクホルダからの訴追に配慮し可監査性を高める情報の提供に視点を置いているという違いはあるものの、ともに、クラウドを使ったビジネスチャンスの腰を折られないための配慮に注力しているという意味で共通していると言える。座長からも「クラウドについてはユーザとベンダーは同床異夢」という言葉があったが、同床異夢をいかにＷｉｎ－Ｗｉｎに繋げていくか。そこにシステム監査がどう貢献できるかが、今後の同研究会で解き明かされていくことを期待したい。

＜報告者　尾浦　俊行（№.1497）＞

５．セミナーWG活動報告

発表者：三橋　潤　氏（日本ユニシス株式会社）

座　長：飛田　治則　氏

【システム監査セミナーの概要】

① 初級：入門セミナー・・・「システム監査って、何？」という副題をつけ、システム監査の概要講義と簡単な模擬監査を経験できるロールプレイもあるセミナー。２２年度６月、７月、２３年度６月開催した。

（受講者のターゲット）

システム監査の言葉は知っているが､実際何をするのか「知らない→知りたい」人向けのコース。情報システムを４，５年経験している若手を想定。

⇒ 今年の受講者プロフィール：公認会計士、ＳＩ‘ｅｒの役員、情報システム部員、監査部員

（工夫・特徴）

・問題点は最初から明らかにしてある。問題点の原因究明と改善策を追求する形式。

・日本システム監査人協会のセミナーらしく、「ロールプレイ」あり！

② 中級：課題解決セミナー・・・「システム監査は、どう役に立つの？」という副題をつけ、過去に発生した重大なシステム障害を事例にしてシステム監査の有効活用を紹介するセミナー。２２年８月、２３年７月に開催した。

（工夫・特徴）

・本部事例研究会で２年前に開発された教材。

・問題事象について深堀りした内容の講義と簡易演習。

・ある団体の知識ポイントを獲得できる　→　集客力ＵＰ。

・受講者ターゲットは「情報システム部門」のベテランや管理者層。

③ 上級：実践セミナー・・・「システム監査は、どう実施するの？」という副題をつけ、１泊２日でロールプレイ中心に､たっぷりとシステム監査を体験できるセミナー。２２年９月に開催した。２３年度９月にも開催予定。

（工夫・特徴）

・今年度より教材を「Ｚ社」から「ｄ社」に変更。

・悩みは受講者の確保！　→　「早割り」「チラシ配り」「ＨＰ掲載」「情報バンクへの登録」等、努力していますが・・・。

【現在のセミナーの好評価な点】

・入門・実践セミナーは、ロールプレイによる「参加型セミナー」である。

・グループ討議で問題･課題を探る形式も好評。

【課題】

・実践セミナー教材の陳腐化・・・

⇒ 情報システムの構成やネットワーク環境が過去のもの。

⇒ 教材の問題点・指摘事項が、現在では常識化されている。

・しかし、教材を新規作成するには膨大なマンパワーと最新知識・技術力が必要！

⇒ 例えば：「仮想化」されたシステムを複数台有するデータセンタで、ウィルスパッチ配信用サーバの運用上に問題がある様な教材。

・もともと初級、中級、上級用として教材がデザインされていない。講義（座学）の見直しが必要。

・広報活動の強化策検討。　⇒　集客力ｕｐを目指して

・他支部でのセミナー開催支援。

⇒ 昨年度は中部支部で入門セミナーを開催。今年は九州支部で計画中。

＜報告者　尾浦　俊行（No.1497）＞

６．近畿支部サイトＷＧ活動報告

発表者：金子　力造　氏（株式会社バックス）

座　長：下田　あずさ　氏（三洋電機株式会社）

ひばりちゃんと一緒に参加した座長の下田さん
これもサスティナブル社会の実現に向けた貢献ですね･･･

【活動目的】

・支部活動（各WG、研究会、イベント）に必要なメールやメーリングリストを発行管理する。
・支部サイトを活用し、情報発信・広報活動・会員サービスなどに役立てる。
・その他、支部でのIT活用を支援する。

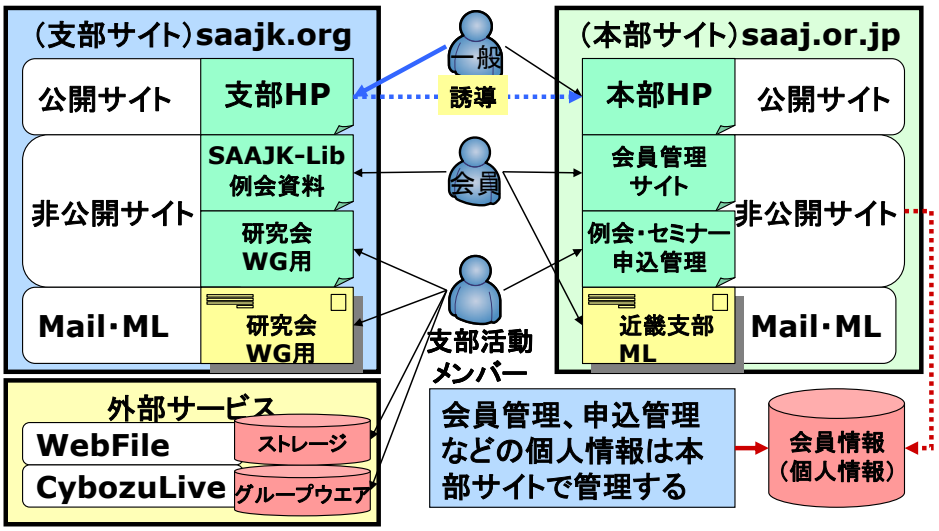
【活動前の状況】

・支部用メールアドレスが無い
・支部用メーリングリストが自由に発行出来ない
・支部用サイトが無い

そのため

・無料サービス又は個人のリソースに依存していた。
・セキュリティやサービス継続性、引継の問題があった。

現在は年間８千円のホスティングにより
ＭＬ発行可能（１０個）のメールサーバー
ＳＳＬ、ＤＢ、ＣＧＩ利用可能なＷＥＢサーバー
と、無料ストレージサービス、無料グループウェアを併用して運用している。



【今後の方向性・・・質疑を踏まえて・・・】

・サービス継続のためには、内部牽制、可監査性を高める必要がある。
・様々なメンバーが寄り集まって活動していることはＮＰＯ固有の課題であるが、逆に、だからこそＮＰＯとクラウドは相性が良いともいえ、今後ともどんどん活用していくべき。
・本部サイトの戦略とも調整しながら近畿支部サイトとしてどういうポリシーで何をするかを決めていく。

＜報告者　尾浦　俊行（№.1497）＞

７．ASP･SaaSに対する情報セキュリティ監査をふまえたクラウドコンピューティングに対する一考察

発表者：佐々木 志津香　氏（情報システム監査株式会社）

座　長：浦上　豊蔵　氏（三洋ＩＴソリューションズ株式会社）

【発表の概要】

ASP・SaaSに対する情報セキュリティ監査について監査実績を基に４つのモデルケースをあげ通常の情報セキュリティ監査との差異を検討した。各モデルにおける留意点は以下のとおり。

○モデル１ 既存システムからASPサービスへの移行

・現地調査項目の作成にあたっては、総務省「地方公共団体における情報セキュリティ監査に関するガイドライン(2007.7)」のうち「物理的セキュリティ」「技術的セキュリティ」「運用セキュリティ」から、情報システムの運用保守に関わる項目を中心に選定する。加えて、利用部門およびデータセンター側の情報セキュリティポリシー等の観点より調査項目を作成する。

○モデル２ ASP提供業者とのSLA契約の評価

・SLA評価項目の妥当性の検証にあたっては、総務省「公共ＩＴにおけるアウトソーシングに関するガイドライン(2003.3)」からSLA契約書の評価項目を洗い出し、契約書の項目評価判定を実施する。

・SLA契約書の改善案検討にあたっては、単純見直しと検討を要する項目に分け、それぞれ分析と改善案を作成する。また、SLMの構築と運営の提言を行う。

○モデル３ ASP事業者で問題が発生しているケース

システム安定稼動とセキュリティインシデントに関して、ASP事業者で実際に問題が発生している事例

・問題点の把握にあたっては、システムインフラ・アプリケーション構成・障害管理表等と過去からのシステム変更の履歴を把握し、問題発生の原因を推測する。

・現地調査項目の作成にあたっては、把握した問題点と、総務省「ＡＳＰ・ＳａａＳにおける情報セキュリティ対策ガイドライン(2008.01)」および経済産業省「ＳａａＳ向けＳＬＡガイドライン(2008.01)」をもとに「サービスの契約内容」「安定稼動」「機密保護」「アクセス権管理」等の観点から調査項目を選定する。そこに、監査人が推測した問題発生原因をふまえた調査項目を追加する。

○モデル４ インフラを借用したケース

このケースは、通常の情報セキュリティ監査の手順で行う。ただしベンダーとサービス利用者の契約関係の確認、ベンダーの監査への協力が必須である。

【必要と考えられるチェック項目】

モデルケースで示したように、情報セキュリティ監査の実施にあたっては、標準的な基準･ガイドラインと、委託契約（アウトソーシング）に関連した各種ガイドラインと組み合わせる事で一応の対応が可能である。しかし、これらの基準・ガイドラインはクラウドの特性を十分に加味して作成されたものではない。本格的にクラウド事業者のセキュリティ監査を実施するにあたっては、未整備な点が多いといえる。ここまで挙げた課題をもとに、必要と考えられるチェック項目の例を示す。

１）監査の実施および監査資料の提供に関しての取り決めが契約書に明記されているか

２）データ保管場所が明確になっているか

３）データの一貫性が維持されるか（要求水準を満たすか）

４）利用者間の環境が適切に分離されているか

５）情報セキュリティに関する公的認証を取得しているか

【留意点】

・事業者の監査協力
　クラウド事業者とサービス利用者の間で監査実施に関する契約が存在しない場合、監査実施が困難となる。クラウド事業者側の監査への対応条件に関しては事前に明確にしておく必要がある。
・データの保管場所
　データの保管場所が海外である場合、そのデータは現地の法律に準拠した扱いを受けることになる。例えば、米国の通称「愛国者法」では捜査当局が米国に設置されているサーバ上のデータを調査対象とすることを認めている。また、EUのプライバシー保護に関する法律では、EUからの個人情報の持ち出しが制限されている。
・データのインテグリティ維持
　Google、Amazonをはじめとする主要なクラウド事業者においては、「分散キーバリュー・ストア（Key-Value Store）型」のデータベースが広く利用されており、データの一貫性の保証が弱いと考えられる。このことは、データ管理についてシステム管理基準に記載されている「データのインテグリティを維持すること」を満たさない可能性がある。
・委託先の監督責任
　データの管理がクラウド事業者によって行われている場合でもデータの安全性は最終的に利用者が責任を持つ必要がある。例えば、大量の個人情報を含むデータをクラウドで管理する場合、個人情報保護法第22条の「委託先の監督義務」が適用される。利用者には、クラウド事業者が個人情報の保護水準を満たしていることを評価する義務が生じる。

【まとめ】
　ASP提供業者への監査は、通常のセキュリティ監査と同様に進めていく事ができるといえる。ただし、基準・ガイドラインは監査対象システムの特性・課題に応じて柔軟に選択する必要がある。また、ASP事業者とサービス利用者の間で監査実施に関する契約が存在しない場合、監査実施が困難となる事が想定される。弊社の監査事例においても、ASP事業者側が監査実施に強い拒否反応を示したケースがあった。最終的には、サービスの利用企業（監査依頼者）からの強い働きかけにより監査を実施することができたが、監査の実施を確実に行うためには監査実施に関する契約が不可欠である。

＜報告者　大塚　一志（No.1700）＞

８．多様な基準によるシステム監査の可能性

　発表者：吉田　博一　氏（大阪府）
　座　長：小山　俊一　氏（株式会社マネジメント総研）

【研究の背景】

・システム監査は法制度的に強制ではない。
　法制化が必要か、クラウドに適用するには、という議論が出ている。
・システム監査によりシステムの完全無欠性を保証はしていない。
　システム監査に対する投資が、経営者とプロジェクトマネジャーで相違がある。
・金融機関では、行政当局による監査で規制されている。
・企業の内部統制のルールとして法制化されたものとして、J-SOX（日本版 SOX 法）がある。
　ただし、対象は財務諸表に対する監査であり、システム全般に対するものではない。
・情報セキュリティ分野に特化した監査として、保証型情報セキュリティ監査がある。
　システム監査が経営者の言明を基に行われる。

以上より、従来のシステム監査基準からシステム監査の必要性を考える。具体的には、経済産業省が示す「情報システム・モデル取引・契約書」「共通フレーム」を基にシステム監査の必要性を考察する。

【発表の概要】

○情報システム・モデル取引・契約書におけるシステム監査の役割

・証券取引における誤発注事件（みずほ証券のトラブル）などの事故事例を受け、情報システム障害の社会的影響が日々深刻化していることが懸念されている。

・経済産業省より情報システムの信頼性向上に関するガイドラインが提示された。ガイドラインではシステムライフサイクルプロセス全体に対する第三者によるレビューが示されている。

・第三者評価では、情報システムの企画や要件定義段階において、システム監査人を含むレビュアーに監査を依頼することとされている。

○共通フレーム

・共通フレームはソフトウェア・ライフサイクル・プロセスの国際規格（ISO/IEC12207）に適合した国内基準であるが、国際規格に対して「企画プロセス」「システム監査プロセス」が追加されている。

・共通フレームを適用しながら、システム監査を実施していくこととなるが、システム監査プロセス活動を適切に実施するためには、監査対象から独立したシステム監査人が本プロセスの実施に当たることが必要とされる。

○Ｊ－ＳＯＸと保証型情報セキュリティ監査

・上場会社は内部統制について評価した報告書（内部統制報告書）を有価証券報告書と合わせて提出することが義務付けられ、経営層の意識が変わってきた。

・ＪＡＳＡが提唱する保証型セキュリティ監査がより具体的に保証型情報セキュリティ監査の概念について提示している。

・監査対象を経営者が言明した範囲とするシステム監査の実現の可能性があるが、その手法は確立していない。

【座長コメント】

システム監査に言及されている、あるいは、システム監査に関連のある３つの基準・視点で、システム監査の位置づけ・必要性の認識について考察されており、基準を拠り所としたシステム監査の普及のための次の一手を考える上で、有意義な整理になっている。

例えば、世の中の認知として、

・システム監査というものがある

・システム監査をするのが望ましい

・システム監査をすべきである

・システム監査をしなければならない

という段階を考えた場合に、「システム監査をしなければならない」という段階にどのように持っていくかについて、論文の第２弾にも期待したい。

【質疑応答】

Ｑ：限られた字数で網羅的には表現することはできない状況でしょうが、どのような基準でこの３つの基準を考慮されたのか。

Ａ：経営者の視点で、実際に証券取引所、株式取引の事故事例を基に、行政が発する情報を基に絞り込んだ結果、この３つに絞り込まれた。

Ｑ：モデル契約・契約書では、システム監査が関与することと、システム監査が関与しないことを区別されているのか。

Ａ：厳密には区別せずにモデル契約書の中でもシステム監査が取り上げられている。あまり厳密に区別していない。

Ｑ：会計的には内部統制報告書は言明では無い。なぜ言明という言葉が保証型情報セキュリティ監査で使用されたと考えるのか。

Ａ：言明については、内部統制報告書と区別せず使用している。このような類似した手法を今後のシステム監査で利用できるのではないかと考え使用した。

Q：７６ページの共通フレームについて、システム監査人は明確な資格として明記していないため、どのような方を想定しているのか。
A：技術者の例示として、ＩＴの専門家として列挙している内容であり、特定の資格ではなく、代表名として記載した。
Q：ＪＡＳＡでは保証型セキュリティ監査を進めている。保証型監査を取り組むにあたって計画はあるのか。芳仲先生からの示唆はどのような内容か。
A：東京本部ではＪＡＳＡと定期的な意見交換をしている。ＪＡＳＡでとりきめる保証型監査と一緒に出来るように調整を進めている。芳仲先生からの示唆は基準等の内容である。

＜報告者　大塚　一志（№.1700）＞

９．システム監査とその類似概念

発表者：木村　安寿　氏（関西学院大学　経営戦略研究科教授）
座　長：庫本　篤　氏（近畿職業能力開発大学校　生産情報システム技術科）

発表者が欠席されたため、座長のコメントと質疑応答の報告とする。

【座長コメント】

内部監査の中で部分的監査が許されるのではないかという考察があるが、システム監査の中で上位概念に対する検証を含んだ一体としてプロジェクト監査を行うことは同意できる。

今回の統一テーマであるサスティナブル社会におけるシステム監査との関連においては、今回の発表はシステム監査の概念を全体として説明している。

【会場からの意見】

会場意見１（雑賀氏）：
・システム監査は内部統制の保証である。
・内部統制というのは、目的と基本的に合致していれば保証される。
・部分的な意見表明は、上位概念が保証されていれば保証されている。上記概念を保証すれば、下位の監査を実施する。
・実際に内部監査をしていると、上位概念で監査して、下位の部分を輪番で数年毎に実施している。部分的な表明が出来ないといわれても、実際には部分的表明で進めるしかない。

会場意見２：
・ＩＳＡＣＡから参加したものであるが、経産省の管理基準、プロジェクトマネジメントをどうすればよいかということはＰＭＢＯＫに書かれている。

座長意見：
・システム開発フェーズに着目すると、システム監査は運用フェーズに重点を置いている。

＜報告者　大塚　一志（№.1700）＞

１０．自治体のクラウドコンピューティングを活用した共同アウトソーシングの企画業務に関するシステム監査

発表者：津田　博　氏（近畿大学　経営学部准教授）
座　長：是松　徹　氏（オムロン株式会社　グローバル監査室）

【研究の背景】

全国には人口１０万人以下の市町村が１５００余りある。それらの市町村での基幹システムを対象としたシステム再構築をテーマとした研究を進めている。複数市町村の共同利用を

目的としたシステム再構築の調査研究を行った。
【発表の概要】
○はじめに
・基礎自治体（市町村）は、地域における行政の自主的かつ総合的な実施の役割を担っている。例えば、子供手当では、国レベルの議案であるはずが、日本では市町村が提供する仕組みとなっていることが象徴的な特徴である。
・ＩＴに関して、国が市町村をコントロールするという関係にないため、各市町村は、自助努力によって仕組みを構築しなければならない。
・ＩＴ経費は小規模市町村では年間予算の１％近くに上るところがあり、逼迫した財政難の中で、経費の縮減が課題になっている。他にも、標準化の問題、震災からの安全性の要求の高まりが議論されている。
・基礎自治体のシステム共同化の必要性は過去から認識され、総務省も進めてきたが、十分に展開できているとはいえない。
・ＩＴに関して、被災地においても、他自治体からのＩＴ利用に関する支援は、自治体ごとに仕組みが異なるため、十分な支援ができなかった。
○共同アウトソーシングが功奏した事例
・山形県長井市：仙台のｉＤＣ利用により地震によるサーバー損壊を免れた。
○省電力の事例
・宮崎県都城市：サーバー仮想化による節電（市のサーバーを２台に統合）。
○複数自治体による共同化組織の形成
・企画を一本化するが、費用は各自治体で予算化する。調達は共同化組織が担う。
・システム監査は各首長に監査報告書を提出する。
・共同化の経緯は、東大阪市・大東市の２市が最初に実施し、他の市町村に展開された。1982 年にピークに達したが、その後、共同導入から単独導入へ移行する団体が増えたため、共同化組織は減少した。
○共同化が困難な理由
・業務手順の変化が大きく、担当部署には短期的メリットが見出せない。
・リース期間が揃わない。
・データ移行やシステム連携が個別にベンダーと調整しがちである（単独自治体では個別ＩＴベンダーと随意契約となりがちなため）。
（複数の共同化組織での企画段階の検討・実施内容例）
◆ 現在の内部開発よりも単体で外部委託したほうがコストが増大する場合がある。従って共同化へ。
◆ 首長同士で合意の調整が必要となる。
◆ 事前デモが１業者４０回近く行われた事例がある（４社であれば、４×４０回）。そのため、合意形成に非常に時間がかかった
◆経費分担は、どの市町村も納得できる金額にするのは困難である。このことは、「コンドルセのパラドックス」として知られている。
・自治体ごとにパッケージ構成が異なる。
○共同アウトソーシングにおけるシステム監査
・計画に関する監査
◆ 開発計画は、全首長が承認しているのか。ミドルの管理者がどれだけ熱心なのか、で変わる。
◆ 役割分担が明確であるのか（自治体には、情報部門がない場合がある）。
・分析に関する監査
◆ 現状の経費の分析（ユーザーニーズが正しいか判断が必要）。
◆ パッケージのカスタマイズに掛かる費用は適切なのか。
◆ユーザーニーズとの適合性。

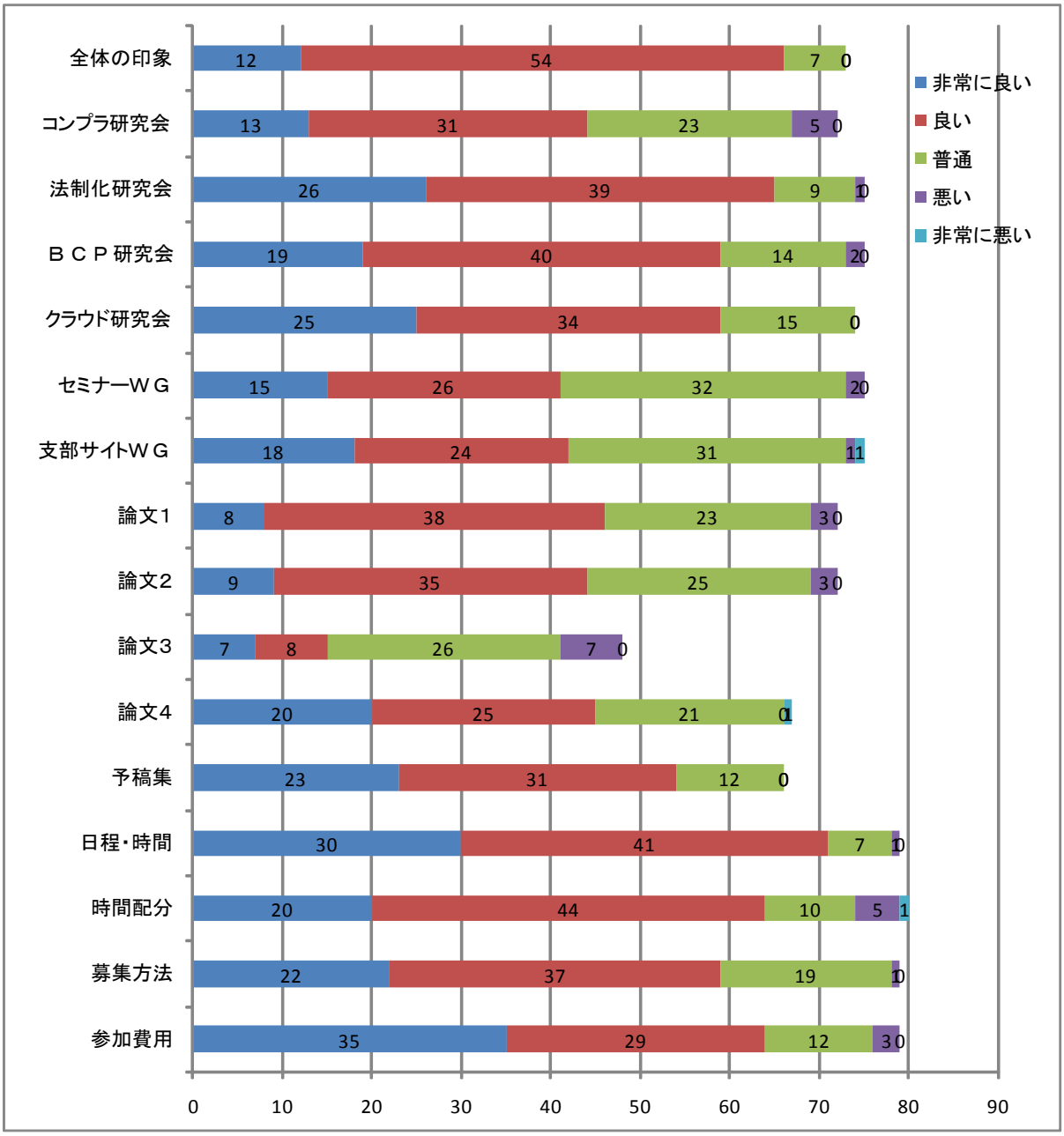
・調達に関する監査
◆ 調達方法はルールに従っているか。
◆ 調達仕様書は適切か。
○まとめ
・明らかになったこと
◆ 共同アウトソーシングは、全首長の合意が必要となる。
◆ 関係者の合意対象は、多方面、多階層に及ぶ。
◆ ユーザーニーズは、その本質を掴む必要がある。
◆ 独立した第三者のシステム監査は、共同アウトソーシングの透明性・公正性を高める上で必要である。
○今後の課題
・多くの共同化組織を分析して類型化する。
・概要だけでなく、より深い検討を行う。
【質疑応答】（Q：会場、A：発表者）
Q：共同アウトソーシングが進まない事情は？
A：現場が手順変更に抵抗している。一般的には強いリーダーシップが必要。現場では、強制的調整手段が発揮しがたい。
Q：その対策は？
A：関係者との合意形成がキーとなる。合意形成には、合理的な前提を示した説明を行う。合理的説明の裏づけに監査報告を生かす。企画業務で合理的な説明をするには、経費削減できることや、効率化、安全性向上を監査でどのように示していけるのか、検討事項となる。
Q：自治体に対する厳しい指摘もあった。９７ページのシステム監査がＩＴガバナンスに寄与するという主張は、９４ページの記載では、共同アウトソーシングはリスクを伴う、とも書かれている。ガバナンスを確立できるというという主張はどういった根拠で示されているのか。
A：国際関係と同じで自治体は平等な関係があるという前提がある。独立した組織の中で共通した意識で実施することをガバナンスと呼んでいる。
Q：システム監査が必要であるという根拠をもう少し明確に示して頂きたい。
A：合意に至らないこと等が問題と認識している。その内容を把握するのは、表面化しないために困難である。成功要因から逆説的に推定するなど、今後検討していきたい。全国で共同アウトソーシングを展開するには、基準が必要となる。今後共同アウトソーシングした場合、ＩＴベンダーが倒産することもあることを念頭におく必要がある。そのためには第三者チェックが必要ではないか。
Q：論文で書かれているシステム監査とは、本当にシステム監査を指しているのか。これは依頼者が誰であるのか、監査費用はどのように負担しているのか、監査を行う上で何を保証するのか思い浮かばない。
A：監査の依頼、費用負担については、協議会が担うと考える。
意見：外部監査と見ることもできるが、共同アウトソーシングを進めるに当たりどういうところに課題があるのか。千葉県のような実例を見た上でより良い研究を進めて頂きたい。

研究大会参加者アンケート集計結果

１．アンケート回収結果

参加者数	110	無記名	コメント無し	45
アンケート回収数	80		コメント有り	28
アンケート回収率	72.7%	記名有り		7

２．評価結果



＜補足＞

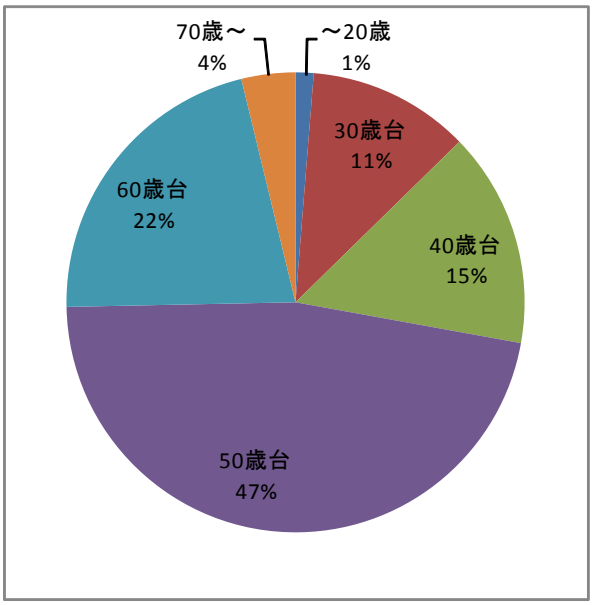
＊　横軸は回答数であり、未記入はカウントしていない。

＊　「論文３」は、発表者が不在であったため、未記入が多くなっている。

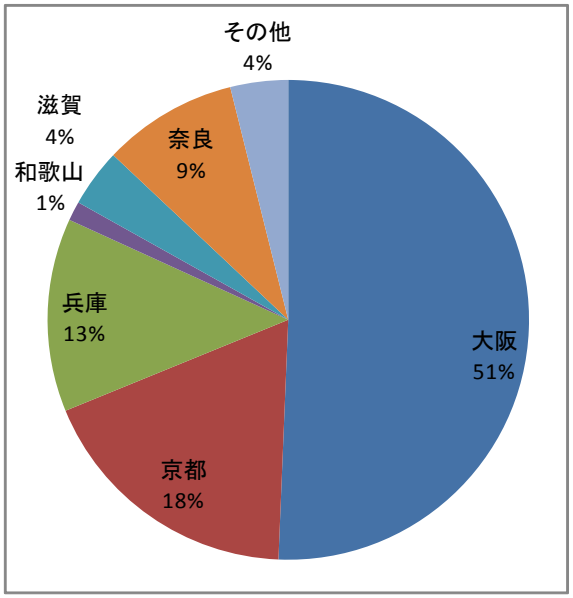
＊　途中退席者／途中参加者は、参加していない発表の評価は未記入であった。

３．参加者情報

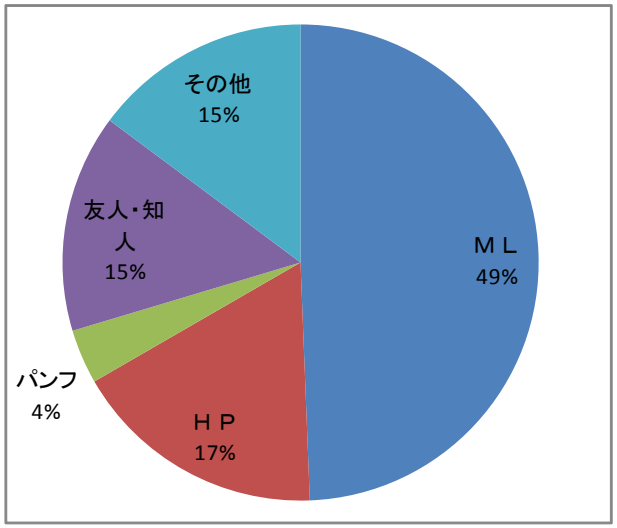
（１）年齢



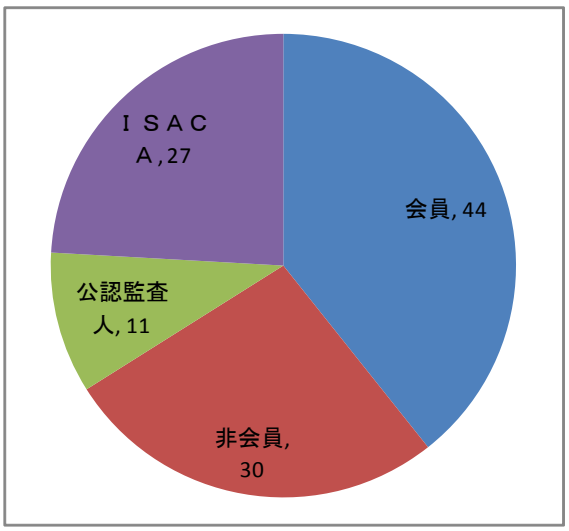
（２）住所



（３）情報入手方法



（４）資格情報



＜補足＞

＊　「住所」の「その他」は、福井県、山梨県、沖縄県。

＊　「情報入手方法」は、アンケートの記述が一部曖昧な部分があった。

＊　「資格情報」は、複数回答があったため、比率表示ではなく回答数を表示した。
「非会員」の回答欄は不要であった。

４．アンケートのコメント

（１）全体の印象

・発表に対する座長コメント方式は有益でした。座長の選任に注力されたと思います。全員、素晴らしいコメンテータでした。
・雑誌や新聞と言ったメディアからの知識より、実際に取り組まれていることを肉声で得る知識の方が得るところは大きく、期待通りでした。
・積極的な議論が出来ているので思考を深めることができました。
・テーマに沿った内容、時間に応じた深度であった。
・理論や、あるべき論だけでなく、実例に即した発表もあって勉強になった。
・活動途中の報告が多かったので、是非、完成の報告会、研究大会を開催して頂きたい。
・システム監査も経営者の目線をもっと取り上げてやっていく方向で推進された方がいいと思う。
・テーマ、及び討議に余り新しさがない。

（２）個別評価

・(コンプラ研）コンプライアンスの捉え方の差、それを受けての研究会のスタンスについて説明があると良かった。
・(クラウド研）座長の発言が長かった。もっと、参加者に時間を振るべきであった。
・(セミナーWG)セミナー参加者が少ないですね。ロールプレイが支持されているとの分析でしたが、ロールプレイがあるから参加しない、という考えの方もいるかもしれません。入門コースで２種類（ロールプレイの有る無し）やってみるのも面白いのではないでしょうか？
・(論文２）経営方針に沿ったシステム監査の基準・手法の提案が明確であった。
・(論文４）実務に裏打ちされて面白かった。同じテーマで定例研究会でも発表して欲しい。
・(予稿集）予稿集には書けないことがあるためか、実際の発表の方が良かった。
・各発表や報告の概略（半ページ程度）があれば、予め聴くポイントが分かってより活発な意見交換ができると思います。
・活動実績が報告に占める割合が高い報告があるが、何のために何をやって何を得たのか本論をもっと重視して報告頂きたい。
・前半は活動報告であり、ある意味しかたないですが、後半の論文発表のように今一歩内容により踏み込んで説明して頂けたら良かったです。
・内容が、ややマンネリの感がある。

（３）大会運営

・座長による講評を入れると言うのは斬新で面白い。発表者の気づかない視点での意見の広がりが得られる。
・土曜日の開催は、ｇｏｏｄです。毎月はきついですが、半期に１回はＯＫです。
・テーマを絞って「クラウドコンピューティングのシステム監査」にもっと時間を取っても良かった。
・時間が短い中でテーマが多すぎたため、表面的な説明になるきらいがあった。
・論文については、質疑の時間をもう少し長くして欲しい。
・ややテーマ数が多く、発表時間、質疑時間が十分でない場合もあったように思う。

（４）その他

・今後も開催を検討して欲しい。
・定期的にこのような企画で活動を振り返ることが大事だと思う。
・電気通信主任技術者の活用などの話題もあり、保有スキルの活用、強化という自己啓発のきっかけとなりました。
・質問等、いつも同じ人の意見に終始している感がある。
・育児同伴参加は問題ありません。新鮮でした。
・記念すべき第一回の研究大会で、泣き声は残念でした。

以上