

# 特定非営利活動法人 **日本システム監査人協会報**

## 特集 1 情報システム監査実践マニュアル第2版出版記念

### 情報システム監査実践マニュアル 『第2版』発刊のお知らせ

No.6027 小野 修一

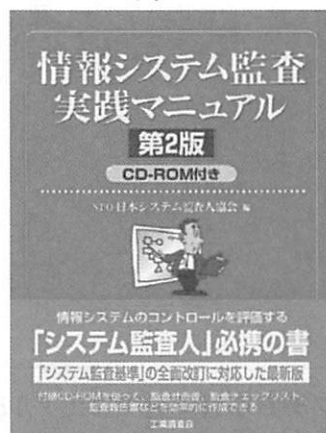
通称“赤本”という名前でシステム監査人に愛用されてきた『情報システム監査実践マニュアル』が改訂され、『第2版』として、株式会社工業調査会様から発刊されることになりました。『第2版』の発刊は、昨年10月の「システム監査基準」の改訂、「システム管理基準」の新設を受けて計画されたもので、今年度の当協会の目玉事業の1つに位置づけられていました。

システム監査基準研究会のメンバーを中心に、個人会員、法人会員も含め約15人の会員が今回の改訂作業に参加し、約半年という短い時間で、計画通りに発刊にこぎつけることができました。皆さんのご協力に感謝いたします。

また、経済産業省商務情報政策局の石飛課長補佐からは「刊行に寄せて」をご寄稿いただき、(財)日本情報処理開発協会様には「システム監査基準解説書」「システム管理基準解説書」の参考・転載についてご快諾をいただきました。改めて御礼申し上げます。

改訂されたシステム監査基準、システム管理基準に対応し、新しい時代の情報環境に適合した内容に改訂された『第2版』を、多くのシステム監査人、システム管理者の皆さんが有効活用されることで、よりよい情報環境の構築に寄与できればと願っています。

発刊までの執筆、編集活動の経緯や苦労談は松枝さん、沼野さんからの報告に譲ることにして、発刊のお知らせといたします。以下に、『第2版』の目次概要を掲載しましたので、ご参考にしてください。なお、定価は4800円(CD-ROM付き)プラス税となっています。



### 第1部 組織経営における情報システムの役割とシステム監査

- 第1章 変革する情報社会
- 第2章 システム監査の重要性と概要
- 第3章 システム監査と他監査との関係
- 第4章 システム監査と関連する諸施策

### 第2部 システム監査の実践方法

- 第1章 システム監査の導入
- 第2章 システム監査の計画
- 第3章 システム監査の実施

### 目次

|                                                  |                                 |    |
|--------------------------------------------------|---------------------------------|----|
| 特集                                               | 特集1 情報システム監査実践マニュアル第2版出版記念..... | 1  |
|                                                  | 特集2 公認システム監査人アンケート意見へのご回答.....  | 3  |
|                                                  | 特集3 支部だより.....                  | 8  |
| 会報掲載論文                                           | ソフトウェア国際取引におけるシステム監査応用の一考察..... | 15 |
| 情報システム・ユーザ会連盟主催「システム監査講演会」ー平成17年度情報化月間参加行事ー..... |                                 | 24 |
| ホームページの掲載情報を追加しました.....                          |                                 | 27 |
| 第6回システム監査実務セミナー実施報告.....                         |                                 | 31 |
| 法人部会の活動.....                                     |                                 | 34 |
| 第7回システム監査実務セミナー開催案内.....                         |                                 | 36 |
| 新刊紹介.....                                        |                                 | 37 |
| 研究会報告                                            | 第115回月例研究会報告.....               | 38 |
|                                                  | 第116回月例研究会報告.....               | 39 |
| 理事会報告                                            | 平成17年度第8回理事会議事録.....            | 42 |
|                                                  | 平成17年度第9回理事会議事録.....            | 43 |
| 編集後記.....                                        |                                 | 44 |

- 第4章 システム監査の報告
- 第5章 システム監査の改善指導（フォローアップ）
- 第6章 テーマ別システム監査のポイント
  - 6.1 データ中心アプローチにおける監査のポイント
  - 6.2 ソフトウェア国際取引における監査のポイント
  - 6.3 事業継続管理における監査のポイント
- 第3部 システム監査の事例
  - 第1章 情報システムの有効活用をテーマとした外部監査
  - 第2章 プライバシーマーク認定取得の内部監査
  - 第3章 地方自治体のシステム監査
  - 第4章 プロジェクトマネジメントの監査
- 第4部 資料
  - 第1章 様式
  - 第2章 作成例
  - 第3章 監査・評価ポイント
  - 第4章 CDの使用法

以上

## 情報システム監査実践マニュアル改訂版 出版にあたって

No.555 松枝 憲司

「赤マニュアル」の呼称で、協会関係者に広く知られている実践マニュアルのルーツは、96年協会の10周年特別プロジェクトで作成し、会員に配布した黄色い表紙の「システム監査実務手順書」です。翌97年には、システム監査の全フェーズをカバーするよう同手順書の内容を拡張させて、FDで会員に配布しました。その後、同手順書に事例その他を追加して、98年に「情報システム監査実践マニュアル」として出版に至りました。

実に3年間かけて出版にこぎつけたわけですが、今回の改訂版（ほとんど再作成です）は約半年でこぎつけました。基準研、事例研、セキュリティ監査研、法人部会、支部等協会および会員が持っているノウハウを、効率的に集大成することができたと思います。

ところで改訂版が出版できるということは、赤マニュアルが売れていることを意味しています。本が売れない時代にこの高い本が売れているのですから、監査の世界にフォローウィンドーが吹いているのは明らかです。

10年にわたって本書の編集に携わってきた者として、システム監査ビジネスの花が開き始めた時代の変化を大いに感じています。

## 情報システム監査実践マニュアル改訂版 出版にあたって

No.841 沼野 伸生

今回、当協会の重要資産である「情報システム監査実践マニュアル」（通称赤本）の改訂に関わる機会を得、執筆、取りまとめなど、時間的な負荷も大きかったのですが大変いい勉強になりました。

私は、第3部（システム監査の事例）、及び第4部（資料編）の「システム管理基準を活用した監査のポイント」の内、「共通業務」の取りまとめを担当し、また、コラムの執筆にも加わりました。私が担当した部分を中心にその一端を紹介したいと思います。

まず、第3部（システム監査の事例）については、掲載事例のほとんどを入れ替え、今日的な事例として、プライバシーマーク認定取得監査、自治体の電子調達システム監査、そして大規模プロジェクト監査などを掲載しました。どれも、掲載事例の実際の監査に中心的立場で関わった、経験豊富なシステム監査人の方々に執筆頂き、記述に当たっては、時間軸に沿って、監査の実際がより理解し易いよう心掛けて頂きました。システム監査の実務に役立つヒントが多く含まれていますので、システム監査のベテランの方も、またシステム監査未経験の方にも十分参考にして頂けるものと思います。

また、第4部（資料編）にその一部を掲載し、多くは付属のCD-ROMに収録した監査のポイント集は、システム監査（管理）基準の全項目を多くの執筆者で分担し、サブコントロール等に分解する膨大な作業であったため、その内容調整は取りまとめご担当の松枝さんを中心に大変な作業量となりました。その中で私が執筆の一部と取りまとめを担当した「共通業務」も、そのカバーする幅が広く、分担する執筆担当者も多く、また途中で担当者の変更などもあり、紆余曲折のある負荷の大きい作業となりました。しかし、ここの部分は本書の価値（システム監査のノウハウ）を多く含んだ部分であり、必要部分を適宜抜き出し、監査実務に是非活用して頂きたいと思います。

本書のコラムは、テーマ毎にそのポイントを簡潔に記載し、本書を読み進める過程で、一息入れる際の簡単な読み物になっています。それぞれの執筆者の実務経験などを基に、エッセンスを分かり易く解説しているので、これも肩の力を抜いて、一読頂きたいところです。

本書はシステム監査の理論、事例、そして実務に際し活用できるチェックポイントなどのノウハウを詰め込んだ、文字通りオールインワンタイプのシステム監査の数少ない基本書です。本書を通し、更に多くのシステム監査人の仲間が増え、今日の情報社会を支えるシステム監査が、より一層普及していくことを願っています。

## 特集2 公認システム監査人アンケート意見へのご回答

前号第87号の特集“公認システム監査人特集”の記事作成にあたって公認システム監査人にアンケートを致しました。その中で皆様から“6. 自由記入”としてご意見頂いた内容を第87号に記載致しました。その内容について理事会として真摯に受け止め一つ一つにご回答を作成しました。まだまだ十分とはいえませんが、今後とも前向きに取り組んでいく所存です。理事会からのメッセージとしてお読み頂ければ幸いです。皆様方のご理解を深めるとともに、さらにご意見ご質問等ございましたら、会報担当 saaj-kaihoh@yahoogroups.jp までお送り下さい。今後とも宜しくお願い致します。

| 分類                  | NO | アンケートでの自由意見<br>(第87号掲載)                                                                                                                                                                                                                                                                                                             | ご意見に対する回答 (理事会)                                                                                                                                                                                                                                                                                                                                   |
|---------------------|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| I. 認定資格             | 1  | ITC協会の認定資格について多くのITCは資格維持に向けて知識欲旺盛な人材群です。新規に資格を取得した場合、10P加算という制度もあります。この資格対象にシステム監査関連も入っていますが、何故か「公認システム監査人」は入っていません。「システム監査技術者」(情報処理試験合格者)「公認情報システム監査人」(ISACA)は入っております。システム監査特認講習の受講生から「何故入っていないのか?」と質問されても答に窮する状態です。仲間を増やす為に是非ともご検討のうえITC協会へのアプローチをお願いします。(注:ITCAのHPでは、「マルチエントリポイント制度運用ガイドラインの改定(V1.6)他2004.5.20」の中に入ることになっています。) | ITC協会への働きかけは3年前から実施していました。先方から正式回答を得るまでに1年以上掛かりましたが、新規加入及び更新の際のポイントについては、一定の成果を得ました。詳細については、ITC協会側のHP(マルチエントリポイント制度運用ガイドラインV1.7)をご参照下さい。                                                                                                                                                                                                          |
|                     | 2  | 資格(公認システム監査人)継続に必要な活動内容の評価について実務の評価時間が年間20時間を上限とする基準は如何にも???実務をこなす機会の増大や、実務をこなせる人材を増やしたいと願っているとは、とても思えません。                                                                                                                                                                                                                          | 監査実務の年間20時間の上限の設定について、米国CISA(公認情報システム監査人)の制度では、業務上の活動は全く認められていません。協会が経済産業省に平成13年に提出した制度の提言(会報No.63,pp.3-9)の中にCISAと提言書の相違点の一つとして「監査実務を継続教育として認める本案に、認めないCISAとの差異がある。実務経験を重視することを本案の特徴と考えたい(p.9).」として、時間上限つきですが、監査実務を継続教育に導入した点をご理解頂きたいと思います。継続教育の受講に関しては、システム監査のテーマに限らず、広く監査対象である情報システム関連のテーマで可として、時間制限はありません。実務の上限の時間については、制度の改善の議論の中で検討したいと思います。 |
| II. 公認システム監査人の認知・普及 | 3  | システム監査の啓発普及についてこの観点での協会の活動は10年前と殆ど変化していないという印象が非常に強い。外向きの活動よりも内向きの活動が中心との印象を受けます。我々は学者集団や学会活動メンバーでも無いはず。本部理事会メンバーの一新を図るなど、体質改善が必要な時期かと思えます。                                                                                                                                                                                         | 啓発普及については精々努めており、例えば、自治体の関係者の反応として、10年前は「システム監査とはなんぞや」から始めなければならなかったが、今では「システム監査を依頼したいのだが、見積査定はどうしたらいいか」「システム監査をやりたいのだが、予算がありません」というふうに変ってきています。しかしまだまだ足りないことも事実であり、協会役員として気鋭の方が出られて、さらに啓発、普及にご尽力いただくことを期待しています。                                                                                                                                  |
|                     | 4  | 公認システム監査人制度がほとんど認知されていない。大企業、情報処理会社は、法的に公認システム監査人があることを法的義務にすべきだ、そういう活動をしていただきたい。                                                                                                                                                                                                                                                   | 公認システム監査人の名が世間一般に浸透していないことはご指摘の通りです。協会としての努力不足や、広報活動の資金不足もありますが、それでも少しずつ認知され始めていることも事実です。ボランティア活動ではありますが、さらに強化していきたいと考えます。今後組織体の内部統制の整備・運用状況の評価がますます重要になります。情報システムの内部統制の評価はウエイトも高く、システム監査の重要性は高まるばかりです。組織体内におけるシステム監査人の役割も重要となり、公認システム監査人の活動が効果を発揮する場が広がるといえます。協会として組織体の内部統制の評価には、情報システムの内部統制を評価するシステム監査が不可欠であることを、機会をとらえて発言していきます。               |

| 分類                     | NO | アンケートでの自由意見<br>(第 87 号掲載)                                                                                                                                     | ご意見に対する回答 (理事会)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| II.<br>公認システム監査人の認知・普及 |    |                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                        | 5  | ①日本システム監査人協会の認知度を更に高める<br>②公認システム監査人の社会的ステータスの向上 (いわゆるブランド向上)<br>③協会の社会的貢献活動のアピール<br>④システム監査が情報システムの構築や運用に必須であることの強力なアピール<br>⑤外部システム監査実施の情報公開等による企業活動の信頼性向上など | ①協会の様々な活動を通じて認知度は高まりつつあるとは思いますが、まだ十分とはいえません。今後とも会員皆様の力を寄せていただきながら努力致します。②公認システム監査人のブランド向上については、公認システム監査人の社会的認知度をあげ、公認システム監査人の皆様のビジネスにもつなげていきたいと考えます。いろいろな広報活動や実績作りを通じて努力したいと考えます。公認システム監査人の品質を落とさないことも大切な取り組みです。いろいろな要望もお聞きしますが、ブランドを維持する意識を保って対応しています。③協会の社会的貢献のアピールについて、監査普及サ・ビス、出版物の発行など、社会への貢献はしてきていると考えますが、まだ十分とはいえません。これも今後の課題と認識しています。④システム監査のアピールの機会を伺っていますが、なかなか難関です。例えば某都市銀行のシステム障害時などにも対応を考えましたが、具体策について本格的な取り組みまではできませんでした。⑤外部監査実施の情報公開等による企業活動の信頼性向上について、システム監査が企業活動の信頼性向上に資するものであると考えています。外部監査実施時の情報公開も監査依頼者が対応すればできますが、監査人側が公開を求めるのは難しいと考えます。協会としては、外部監査で情報を公開している事例を集め、会員の参考に供したいと考えています。 |
|                        | 6  | システム監査の普及・啓発活動をもっと強化すべきと考えます。                                                                                                                                 | 協会の目的の最初に掲げたシステム監査の普及・啓発活動ですから、ご意見の通り引き続き努力します。システム監査の実施は任意監査ですから、組織体のトップの考え方や経営方針により左右されがちですが、今後は単なる任意監査として放置できなくなる情勢にあります。項目 4 でも触れましたが、組織体の内部統制の整備は重要な経営課題となり、その運用状況を含めて監査の実施は経営にとって必須の要件になりつつあります。それには、情報システムの内部統制の整備・運用状況を監査するシステム監査が絶対に必要であることを強調して行きたいと考えます。                                                                                                                                                                                                                                                                                                                                       |
|                        | 7  | 公認システム監査人という資格は、未だ社会的に認知されていない。医者、弁護士、税理士、公認会計士のような認知された職種として、将来発展することを期待します。                                                                                 | 項目 4 と同趣旨の回答になりますが、任意監査であるシステム監査が、いずれは強制監査に近い制度になるように努力したいと思えます。すでに有価証券報告書の記載内容の適正性を証する経営トップの「確証書」や情報の適時開示の「宣誓書」にはそれぞれその適切性を裏付ける社内体制(業務執行体制、内部監査体制等)の整備・運用状況の記載が求められています。これにはシステム監査の実施が前提となることを広く提言して行きたいと思えます。                                                                                                                                                                                                                                                                                                                                                                                           |
|                        | 8  | 公認システム監査人の役割について、他の制度との関連を踏まえて、役割やセールスポイントなどを明確にし、認知度を高めることが大切だと思います。この資格認定を受けることのメリットを感じられるようにしていただきたい。                                                      | システム監査技術者試験合格者は、その知識・技術が一定以上のレベルにあると認められるので、システム監査人に相応しい実務経験と継続的な能力の維持・向上に努めていることを評価して「公認システム監査人」として認定するのが本制度です。制度の創設により、市場ニーズに見合った真に実力のあるシステム監査人の育成が可能で、また試験合格者や受験者のモチベーションの維持・向上が図られることとなります。このような高度の資格であることを機会をとらえて広めていきたいと思えます。                                                                                                                                                                                                                                                                                                                                                                       |
|                        | 9  | 個人情報やセキュリティの機運の高まりもあり、協会へはシステム監査の認知度の向上および社会的役割の増す活動をますます期待したい。                                                                                               | ご意見の通り情報セキュリティ監査の問題は、組織体の存亡に係わることで注目を浴びています。それと同時に、情報システムの内部統制の評価を行うシステム監査の重要性もますます高まるものと思われます。昨年改訂されたシステム監査基準は、この情報システムの内部統制の適切な整備・運用が経営課題であると位置づけています。項目 10 でさらに言及しますが、この点を今後とも強調していきたいと思っています。                                                                                                                                                                                                                                                                                                                                                                                                         |
|                        | 10 | 最近では情報セキュリティ監査人の制度も作られ、システム監査との切り分けが難しくなっています。管理基準ではそれなりの表現をしています。協会として方向性を示唆(又は検討)していただくとありがたいです。                                                            | 昨年改訂されたシステム監査基準から、システム監査を「情報システムの内部統制が、適切に整備・運用されているかを独立かつ専門的な立場のシステム監査人が検証・評価して、保証あるいは助言する活動」と要約することができます。そしてシステム監査の実施は、IT ガバナンスの実現に寄与し、利害関係者に対する説明責任を果たすことが可能となるといえます。システム監査のあるべき姿・方向性がここにあると考え、公認システム監査人として実践と研修に励むことが必要と考えます。協会では昨年来「システム監査基準研究プロジェクト」を立ち上げ、今年は「情報システム監査実践マニュアル」の改訂版出版に挑みました。来年は種々の監査事例の積み上げを図っていきたくと考えています。是非一緒に実践にご参画を期待致します。                                                                                                                                                                                                                                                       |

| 分類                  | NO | アンケートでの自由意見<br>(第 87 号掲載)                                                         | ご意見に対する回答 (理事会)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|----|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| II. 公認システム監査人の認知・普及 | 11 | 協会は、システム監査そのものを普及・啓蒙する活動をさらに拡大していく必要を感じております。その上で、システム監査に携わる人の仕事が増えていくものと認識しています。 | システム監査の普及率は、JIPDEC調査で46.3%(05.3発表)、FISC調査で54.4%(04.12発表)です。後者は金融機関ですが、漸く5割を超えたところで、システム監査の普及はまだ十分とはいえません。しかしこれからは情報システムの内部統制の監査が組織体にとって大変重要な役割をもってきますので、それを支える公認システム監査人の役割も重要になると考え、協会としても引き続き努力したいと思っています。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                     | 12 | システム監査を広めるためには、何らかの制度化、義務化が重要だと思います。                                              | システム監査が法律で義務化されれば、システム監査が普及すると考えます。法制化までの手順を想定してみます。情報システムが社会のあらゆる部分に使われ、情報システムのあり方、及びその情報システムのあり方を問うシステム監査の重要性は認識されていますが、政治や国の行政ではシステム監査の法制化を緊急の課題としているかとなれば、まだそこには至っていないように思われます。政治や行政が考えていなければ、システム監査の専門家たちが法制化への運動を始めるしかないことになります。政治や行政に働きかければ、システム監査法制化の法案要綱くらいはまとめなければと考えます。社会制度としての制度設計が必要です。システム監査の制度設計について、政務調査会のメンバーに「なるほどそうか」というてもらわなければなりません。これはかなり労力が必要とします。会員の知恵と力を、さらにお借りしたいと考えます。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                     | 13 | もっと「公認システム監査人」を増やして、中央省庁や自治体の入札条件に指定されるように活動していただきたい。(CISAに押されればなしです。)            | CISAに押されればなしです」のお言葉ですが、具体的な事例を参照しながら、今までの経緯をご説明し回答とさせていただきます。今後とも引き続き取り組んでいくべき課題だと認識しています。最初の(1)は公認システム監査人が指定されている事例。(2)は指定されなかった事例。(3)は関連した事例について記載します。<br>(1)平成15年8月の某中央官庁のシステム監査業務請負の仕様書にある入札適合条件四つのうちの4番目の条件を引用します。「4.監査責任者となる監査人は、経済産業省が認定するシステム監査技術者試験合格者、特定非営利活動法人日本システム監査人協会(SAAJ)が認定する公認システム監査人又は情報システム監査コントロール協会(ISACA)が認定する米国情報システム監査人(CISA)のいずれかの資格を有しており、3.に実績として挙げた監査業務に中心的役割で参加していること。」とあります。これには協会名まではっきり書いていただいています。このシステム監査は7社が調達審査に合格し、10月に開札されました。<br>(2)平成16年5月に「入札条件にCISAがあって公認システム監査人が無い」との照会があり、調べた結果(1)と同じ省の別の部局のシステム監査の仕様書でした。それには「監査実施者の要件⑥監査責任者となる監査人は、ISACAが認定するCISA又は経済産業大臣が認定するシステム監査技術者の資格を有すること。」とあるのです。このときは既に入札も終了した時点でしたが、何故公認システム監査人を明示していないか、理由を知りたいと照会致しました。その時の回答は次の通りでした。「公認システム監査人の資格の存在は十分理解している。当該資格の方がCISAを包含した資格であると考えていたが、今回は公衆要件として要件を少しゆるくしたかったゆえにCISAとした。決してシステム監査人資格を有する者を公衆から外す意図はなく、包含しているものであろうからといった意識であった。公認システム監査人資格を保有していれば、よりよい。」とされ、さらに「特別認定制度にはその他の資格に「CISA」があり、論文及びプレゼンの特別講習も必要であり包含していると考えている。公認システム監査人の方は要件である「システム監査技術者」資格を取られている方が多いかと思っています。今後の要件を決める際には配慮するように致します。」との回答でした。当方としては「このような場合でも、「公認システム監査人資格の保有者はなお可」の趣旨を入れていただければ、継続教育を受けて資質の向上を図る努力をしている資格者の励みになるので、よろしくご高配を」とお願いした経緯があります。<br>(3)上の例は公認システム監査人がシステム監査技術者資格のより上位にあたる高度の資格となっていることが、逆効果だったかも知れません。現在、国の外郭団体の制度で、CISAがあって公認システム監査人が無いというのがあり、これも是正方を申し入れている事例があります。これは国家試験の上位にあたる資格だから記載がなくても含まれるということで、運用上配慮しているので問題がありませんと先方には言われていますが、公認システム監査人の記載があった方がより明確になるということで修正をお願いしてあります。その他会報の前号(No.87)に入札条件の事例(p.2)などご覧になれば、多少なりとも公認システム監査人の知名度もあがってきていると思われます。これは会員各位の努力の積み重ねが効果を発揮してきたからなのです。協会としても、なかなか気がつかないことも多いので、(2)や(3)のような事例があれば、是非事務局にお知らせいただき、協会として公認システム監査人の活用をアピールして行きたいと考えています。 |

| 分類                   | NO | アンケートでの自由意見<br>(第 87 号掲載)                                                                                                                                                                                                     | ご意見に対する回答 (理事会)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| III.<br>協会<br>ML, HP | 14 | 協会 ML<br>会員相互がもっとフランクに投稿 (受<br>発信) できる場が一般の ML と理解し<br>て居ります。当協会の ML は一般常識<br>からかなりずれた運営方針と見えま<br>す。                                                                                                                          | 現在 ML に投稿できるメールは、事務局からの会員向け情報連絡と、会<br>員からのメールのうち全会員に送付するに相応しい内容のメールに制<br>限をしています。これは、1000 人に近い会員を有している ML に、自<br>由に投稿し、自由に相互のやり取りですべて全会員に流れてしまう<br>方法は適切ではないと考えているからです。特定のテーマに賛同され<br>る会員間で又は仲間とおし任意に ML を立ち上げ自由に意見交換する<br>場を設定しているグループもあります。なお、公認システム監査人等<br>の ML については、双方向通信可能の専用のメーリングリストを開設<br>し、メーリングリスト規約も制定しています。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                      | 15 | HP の充実が必須<br>本アンケートも Web で対応できるよ<br>うにしたい。会員と一般の区別がで<br>きるようにする。会報発行を停止し<br>て Web を閲覧するなど、経費を抑えるこ<br>とで HP 充実がはかれるはずだ。                                                                                                        | (1) アンケートの収集については、初めての企画であり時間的な面か<br>ら、メールでの回収にしました。回答方法の改善は今後の課題と致し<br>ます。Web でのアンケートの実施は、一律、Web 方式にする必要はない<br>と考えます。適したアンケート企画があれば、Web での実施は可能<br>です。<br>(2) 現在のホームページは、会員と一般を区別する運用をしていま<br>せん。普及活動も兼ねており、現状は内容も一般に提供する範囲で掲載<br>しています。会員専用のページへの要望は以前からありますが、会員<br>機能を新たに構築する必要があるとともに、会員の ID 管理が運用面で<br>必要となり今の体制で難しいと考えています。今後の検討課題とさせ<br>て下さい。<br>(3) HP のデザインについては、毎年見直しはしたいと考えています。見<br>直しで欲しいことについてご提案していただければ大変有難いと存じ<br>ます。今年度の機能改善については、本会報に掲載した通りです。ま<br>たメルマガの開設については、運用体制の課題もあり、引き続き検討<br>していきたいと考えています。運用規約の制定も必要だと考えます。<br>(4) 会報を PDF 化してメールで送付する案については以前から検討し<br>ています。技術的には可能かと考えています。但し次の課題がありま<br>す。a. 現在のメーリングリスト加入者は会員の約 80% 程度であり、<br>Web よりすべての会員に情報が届くようにするためにはメーリング<br>リストの加入率を高めるための取り組みが必要です。b. メールで受<br>け取れない会員、および会報を配布している関係団体等に対しては、<br>紙媒体での提供が必要です。そうすると結局印刷が必要となり大幅な<br>コストダウンは図れなくなります。いずれにしても IT の活用は重要な<br>検討課題として取り組んでいきます。 |
| IV.<br>推薦制度          | 16 | 現在は、団体所属ですが、下記の理由<br>により将来は独立して個人営業とし<br>たいと考えています。<br>①所属する会社の営業方針に縛られ<br>る為、独立した第三者の立場が堅持で<br>きない可能性がある。<br>②高度な専門的能力を保有している<br>にもかかわらず、一般のサラリーマン<br>と比べても所得が著しく低い。その<br>際、マーケティング方法の 1 つとして<br>協会の「推薦制度」を活用したいと<br>思っています。 | 是非協会の推薦制度のご利用をお願いいたします。現在までのところ<br>推薦台帳登録者も推薦依頼者も少ないのですが、制度発足間もなく、<br>大変大きな組織体からシステム監査人の推薦依頼があり、4 名の公認<br>システム監査人を推薦し、先方から感謝された事例があります。この<br>方々は現在もそこで仕事(非常勤)を続けておられます。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                      | 17 | やはり営業活動が最大の難点です。協<br>会として紹介・仲介機能があればいい<br>のですが                                                                                                                                                                                | 推薦制度の状況は項目 16 でお答えしましたが、協会としてもさらに制<br>度の PR を積極的にしたいと考えます。まず推薦台帳への登録をお願い<br>いたします。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| V.<br>実務経験・<br>研修    | 18 | 情報セキュリティ監査、新基準に基<br>づくシステム監査の実務経験を積むた<br>めの OJT(インターン)制度があれば利<br>用させていただきたいと考えていま<br>す。若干の参加費用負担があってもか<br>まいません。                                                                                                              | 事例研究会では、システム監査実務経験の機会がない方の為、「シス<br>テム監査実務・実践セミナー」を 4 回/年開催しております。次回は、<br>2006 年 2 月に「第 7 回システム監査実務セミナー 4 日間コース」を開<br>催します。本会報にもセミナー概要が掲載されていますので、奮っ<br>てご参加ください。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                      | 19 | 本来業務(システム監査以外)で多忙な<br>ため、公認システム監査人の資格継続<br>が困難。救済措置が欲しい。                                                                                                                                                                      | 継続教育制度の見直しの一環として、制度として何らかの変更を加<br>えることはあり得ますが、それまでは現行制度の運用として考えざる<br>を得ません。セミナー参加などだけではなく、通信教育を利用した学習<br>なども認めております。継続教育の趣旨からして、何らかの学習の報<br>告をお願いいたします。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| 分類                | NO | アンケートでの自由意見<br>(第 87 号掲載)                                                                                                                                             | ご意見に対する回答 (理事会)                                                                                                                                                                                                                                      |
|-------------------|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V.<br>実務経験・<br>研修 | 20 | 現在は企業内の内部監査部門でシステム監査を担当しておりますが、できれば他社の監査も経験したいと思っております。推薦制度への応募も考えておりますが、他社の監査を請け負えるスキルが備わっているかどうかは不安です。システム監査人協会の中で、システム監査を実践したり学習し合えるような研究会のような機会があれば参加したいと思っております。 | 事例研究会では、会員の皆さんにシステム監査の実際を体験、経験頂く為に、「システム監査普及サービス」を不定期ですが、平均 2 回/年実施することを目標として活動しております。(過去約 25 回の実施実績あり) このサービスは、会員で監査チームを編成し、外部監査の形態で希望する企業団体に対して監査報酬無償でシステム監査を実施するものです。実施時期は希望企業団体があり次第ということになりますので、まずは、事例研究会の月例会 (原則第 1 水曜日夜 大手町) に参加されることをお勧めします。 |
|                   | 21 | あと数年後に定年退職を迎えますので、その後も引き続き監査業務、あるいはシステム監査の研修講師などで仕事を続けたいと思っていますので、そういうチャンスがあれば今からでも準備したいと考えております。                                                                     | 個人でシステム監査業務をする機会は、比較的小規模なシステムを対象に自分で開拓することが多いと考えます。システム監査を実施する企業が個人に応援を求める事例も見受けられますが、公募などはせず力量のわかっている人を案件のつど募ることが多いです。研修講師は講座を主催する団体などに売り込むことになります。協会のセミナー講師は、各種研究会メンバーなどから、セミナー責任者が選んでいます。協会活動を通じ、人脈を作ることをぜひお勧めします。                                |
|                   | 22 | 実務でシステム監査を経験したいが、どうすればよいでしょうか? 基本的に休日しか時間がありませんが、可能でしょうか?                                                                                                             | 項目 18 をご参照ください。「システム監査実務・実践セミナー」は土曜日及び日曜日に開催しますので、是非受講ください。                                                                                                                                                                                          |
|                   | 23 | 昨今、個人情報や情報セキュリティに関する仕事はありますが、いわゆるシステム監査の仕事をするチャンスは全くありません。システム監査について協会としてどのような展望をお持ちなのか、会報等でご披露いただけませんかでしょうか?                                                         | 個人情報や情報セキュリティ監査もシステム監査の一環として考える必要があります。しかし組織体にとって単に情報システムのセキュリティだけを確保していれば良いわけではありません。情報システムが戦略目標の実現に貢献しているか、あるいは情報システムの有効性、効率性が図られているかなどを含めて、情報システムの内部統制の評価がますます重要になってきています。新しいシステム監査基準は、このようにシステム監査のあり方・方向性を示しています。今後也会報等でこのような議論も進めていきたいと思っています。  |
|                   | 24 | システム監査、セキュリティ監査は個人では対応できない。特に、公共機関は入札が前提だから、個人は参加できない。                                                                                                                | システム監査、セキュリティ監査は、個人では活動範囲が限られます。協会名での入札もできません。入札条件に公認システム監査人を必要としている案件に関わっている法人の嘱託社員等になることによって対応できるかもしれません。あるいは協会有縁の個人を集めて有限責任事業組合(LLP)を作る案もあります。ただしこれはあくまで有志のものであり誰かキーマンが必要です。                                                                      |
| VI.<br>その他        | 25 | 制度や資格が乱立の状況は何とかならないのでしょうかね。                                                                                                                                           | 協会の理事会でもだいたい議論はしました。競争を前提とする現在の社会制度の中ではあり得る現象で、お互いが切磋琢磨していきながら世の中の評価を待つしかないと考えています。                                                                                                                                                                  |
|                   | 26 | システム監査・セキュリティ監査人などなどがいくつかの団体で認定されておりますが、統一できないのでしょうかね?                                                                                                                |                                                                                                                                                                                                                                                      |
|                   | 27 | 将来、支部で、規模の大きめのセミナーを実施する場合、金策に困った場合は相談に載って頂きたいと思っています。                                                                                                                 | 会計担当理事にぜひご相談ください。理事会の承認が必要但也有りますが、相談いただくことによって実現したこともあります。                                                                                                                                                                                           |
|                   | 28 | 東京中心の運用は、偏った活動ひいては質の高い成果の妨げになっている。ネットの時代でもあり、協会幹部はもっと創意工夫されて、関東地方以外の会員が活動し易い環境を構築すべきです。他の協会等に比べて、相当、旧態依然と遅れていると思います。今回のアンケートの運用が良い例であり、素晴らしいと思いました。                   | 東京中心の運用になりがちなのは悩みの種です。活動の中で、ネットを活用すべきところは、さらに活用していきたいと考えます。それでも協会の活動がすべてネット上で実施されるものではなく、数多いボランティアに支えられていることもぜひご理解願います。                                                                                                                              |
|                   | 29 | 潮流の先取りしたSAAJですので、今後とも他団体よりも先を走ってください。                                                                                                                                 | システム監査の新しい流れは、昨年改訂されたシステム監査基準、創設されたシステム管理基準に示されています。とりあえず従来の「情報システム監査実践マニュアル」を一新して、その『第二版』を出します。われわれとしては、それらをもとにして皆さんと一緒に、ただ新しいシステム監査の実践あるのみと考えています。ともに頑張りたいと思います。                                                                                   |

| 分類         | NO | アンケートでの自由意見<br>(第 87 号掲載)                                                                                                                                                                                                                                                                                                                                                      | ご意見に対する回答 (理事会)                                                                                                                                                                                                                                                                                                 |
|------------|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VI.<br>その他 | 30 | 私のところへはシステム開発の依頼がよく来ますが、いずれも要件定義が難しいものばかりです。システム監査といっても意見を言うだけでは企業側にメリットがありません。実際のコンプライアンスを整備してシステムを製作して実行して効果を出して初めて事業になります。協会が開発をやってみようとは思いませんか。失敗したら全責任を負うのがシステム開発で実力のない人には向かない職業ですが成功した場合の利益は大きいのです。ソフト会社は基本的にプログラムを書くだけで業務改善提案やシステム設計はやりません。そういうことができたなら、公認システム監査人を雇う明快な理由ができるわけで、役員決裁が取りやすいと思います。公認というからには、協会が事業母体で、受注があり、それを公認した人に委託するのでなければ意味ありません。政党の公認や家元制度でもそうでしょう。 | 例えば組織体の内部統制システムの構築を事業として協会が請け負うというようなことをお考えかと思えます。残念ながらコンサルティングと開発を立派にやっていた組織を別に作らないかぎり、現状の協会の定款で決められた事業範囲から外れてしまいますのでこのような業務を行うことはできません。公認システム監査人の監査の仕事は、組織体の情報システムの内部統制が適切に整備・運用されているか否かを評価し、保証あるいは助言を行うことです。そういった監査人を組織体の依頼によって推薦する制度が協会にあることはご存じのとおりです。                                                     |
|            | 31 | 形態だけで中身がないならそれでも結構ですので、資格審査は情報処理試験合格のみにしてください。教育ポイントは、ITコーディネータのポイントでも何でも認めるそうですが、ふざけた審査だと思います。                                                                                                                                                                                                                                                                                | 特認制度は、今後も運用を続けたいと考えます。厳しい条件を経て、優れた方々が公認システム監査人等に認定されており、制度の趣旨は活かされており、本人の研鑽です。研鑽の場はどこであれ、本人に蓄積が行われれば良いと考えます。協会が公認するシステム監査人の継続教育の範囲には、システム監査の対象である情報システム全般の問題に関する研修・受講等を広く考えて、IT投資・情報戦略や情報通信技術の最新動向などの問題も含まれていることを理解していただきたいと思います。ITコーディネータの組織とは、今後も協力できることは協力していきたいと考えます。継続教育の申告に対しては、協会の認定委員会として真摯な審査を実施しています。 |

### 特集 3 支部だより

#### 中四国支部活動報告

中四国支部長 高田 裕史

#### 【1】中四国支部の活動状況について

中四国支部では、講師があるテーマについて発表し、その後意見交換をするというスタイルでこの1年間活動を続けています。出席者数は会員・非会員含めて毎回10名前後になり昨年より増加傾向にあります。また、中四国支部のメーリングリストでの情報交換も少しずつですが増えてきています。

#### 【2】2005年4月～11月までの中四国支部の活動状況

| 開催日             | 講 師                    | テーマ                                      | 内 容                              |
|-----------------|------------------------|------------------------------------------|----------------------------------|
| 2005年<br>04月27日 | 株式会社エブリディ<br>フレスタ 西村さん | 個人情報保護法施行後の個人情報<br>保護対応状況                | 個人情報保護法全面施行後の企業<br>の対応状況の理解・意見交換 |
| 2005年<br>06月08日 | 中央青山監査法人<br>親泊さん       | 内部統制の基礎理解                                | システム監査を実施するにあたって<br>必要な内部統制の基礎理解 |
| 2005年<br>07月06日 | 株式会社アスベック<br>田川さん他1名   | 情報システムQ&A                                | 居酒屋でビールを片手にシステム<br>監査についての意見交換   |
| 2005年<br>08月31日 | —                      | 「財務報告に係る内部統制の評価<br>及び監査の基準」(公開草案)<br>の検討 | 2005年07月13日公表された更<br>改草案の理解・意見交換 |



| 開催日             | 講 師                  | テーマ                               | 内 容                           |
|-----------------|----------------------|-----------------------------------|-------------------------------|
| 2005年<br>10月12日 | 日立情報システムズ<br>小野さん    | 情報セキュリティ監査について・企業における情報漏洩セキュリティ対策 | 情報セキュリティ監査の現状・これからについて・意見交換   |
| 2005年<br>11月24日 | 大阪成蹊大学<br>石島さん・ビデオ鑑賞 | IT内部統制評価の計画と手続<br>(SAAJ第115回月例会)  | 情報システムの内部統制の評価についてのビデオ鑑賞・意見交換 |

### 【3】来期の活動予定

中四国支部では、システム監査の認知度の向上、普及促進を目的に、勉強会、他支部・他団体との交流等を積極的に行っていききたいと思います。特に、来年度は西日本の合同支部会の幹事支部となっており、今以上に活発な活動をしたいと思っています。

### 【4】おわりに

2005年4月の個人情報保護法全面施行をきっかけに、多くの企業・自治体等が情報システムの管理・評価に目を向けはじめています。大企業のみならず、中小企業や町村にも同様の傾向がみられます。日本の文化として評価・監査のプロセスはあまり馴染みのないものでしたが、これからは逆に、必須のプロセスとなることでしょう。また、このニーズに答えるためにも、システム監査の認知度の向上、普及促進のみならず、情報システムを評価できる人材を、多数育成することが必要となります。

我々が、上記事項を実現するためには、今以上に東京・各支部のシステム監査人の研究活動、情報共有、そして他団体との交流等が欠かせません。ここ数年をシステム監査の社会的存在価値が飛躍的に高まる千載一遇のチャンスととらえ、皆さんと様々な活動をしていきたいと思っています。

### 平成 17 年の北信越支部

No.848 森 広志

北信越支部発足後、昨年まで2ヶ年間の会員のご尽力により、各県で持ち回りしている県例会について北信越5県を全て巡回すると共に、システム監査実践セミナーや日本システムアナリスト協会中部支部との合同研究会も実施することができ、支部としての基盤を作ることができました。

今年は、支部発足3年目を迎え新しい試みとして、福井県例会のオープンセミナー化を実施しました。県例会は従来、会員を中心とした事例発表をしておりましたが、地域貢献にむけ一歩前進することができました。又、新たに上級システムアドミニストレータ連絡会と交流を持つことができました。

特に、四支部合同研究会(岐阜県)では、日本システムアナリスト協会と合同セミナーの中で「地方におけるIT技術者のネットワーク作り」についてパネルディスカッションがあり他団体との交流促進が採択されました。

北信越支部としても、他支部や他団体と交流促進を行いパワーアップしていききたいと思います。今年の北信越支部の活動は、以下のとおりです。

#### 1. 目標

- (1) 支部会員の発表・報告により、意見交換や創案の機会を作る。

- (2) 研究会ビデオをできるだけ多くの会員に活用頂く。
- (3) ホームページ(北信越支部コーナー)の掲載を充実させる。
- (4) 新システム監査基準の習得に心掛ける。

#### 2. 実施状況

- (1) 年度総会(富山県)3月19日(土)  
場所 アーバンビル(富山県富山市)  
① 平成17年度総会  
・平成16年度活動報告及び会計報告  
・平成17年度活動計画、その他  
② 「情報セキュリティポリシーについて」  
本部理事 馬場 孝悦 氏  
③ 「業務処理統制の向上について」  
北信越支部長 森 広志 氏  
④ 「研究会ビデオ貸出について」
- (2) 4支部研究会(岐阜県)5月28日(土)  
第一部 SAAJ四支部合同研究会・JSAG  
全国大会(平行開催)  
① 四支部合同研究会  
「電子投票のシステム監査」  
中部支部長 大野淳一氏  
第二部 JSAG & SAAJ中部合同オープン  
フォーラム  
① 『コモンズ型ネットワークと社会貢献』  
ソフトピアジャパン理事長 熊坂賢次氏  
② 『これからのIT人材の育成』  
JSAG関東・SAAJ正会員 原田奈美氏  
③ パネルディスカッション  
『地方におけるIT技術者団体のネットワーク』

石井成美 清水順夫 森広志  
福田啓二 岡田博基

(3) 福井県例会 6月18日(土)

場所 織協ビル(福井県福井市)

- ①「地方公共団体の情報セキュリティ」  
敦賀市企画部情報管理長 川端純一氏
- ②「地方公共団体の情報セキュリティ監査実施内容」  
福井ネット株式会社 角屋典一氏  
有限会社ビジネス・アイ 栃川昌文氏  
きむら経営会計 木村 善路氏
- ③「研究会ビデオ貸出について」

(4) 新潟県例会 9月24日(土)

場所 新潟トークイン

- ①「学校教育におけるシステム化の動向」  
新潟県部会長 風間 一人 氏
- ②グループ討議「セキュリティ対策の実例について」
- ③「研究会ビデオ貸出について」

(5) 石川県例会 12月17日(土)予定

場所 ITビジネスプラザ武蔵  
(石川県金沢市)

- ①「情報セキュリティ対策の最新動向」  
石川県部会長 宮本 茂明 氏

以下に、今年度発表者による発表内容を簡単に紹介します。

業務処理統制による  
アプリケーションシステムの有効性向上

No.848 森 広志

1. 行事名 北信越支部年度総会
2. 日時 3月19日(土) 13時~
3. 場所 アーバンビル(富山県)
4. 内容

(1) テーマ選定理由

昨年石川県例会で2002年7月に米国で制定された企業改革法(SOX法: Sarbanes-Oxley Act)の話題に関心が集まり、企業の内部統制について興味を持ちました。アプリケーションシステムの業務処理統制にメスを入れることでシステムの有効性を高めることができるのではと考え、当テーマを選定しました。

(2) 対象システム

対象として、業務部門システムを選択し、統制自己評価手法を志向したIT内部統制評価を行いました。

(3) IT 内部統制

ITの内部統制について、COSO(トレッドウェイ委員会組織委員会)フレームワーク、日本公認会計士協会「ITを利用した情報システムの内部統制」では以下が主眼とされています。今回は、業務処理統制(アプリケーションコントロール)を点検評価しました。

① 全般統制(ゼネラルコントロール)

- a. ハード、ソフト、ネットワークの取得及び管理運用
- b. アプリケーションシステムの開発、保守、運用に関する統制活動
- c. 情報セキュリティコントロール他
- ② 業務処理統制(アプリケーションコントロール)
- a. アプリケーションシステムの有効性と効率性
- b. 財務報告の信頼性
- c. 関連法規の遵守

(4) 現状把握

以下について現状把握を行いました。

- ①業務部門運営方針・業務処理規程
- ②アプリケーションシステム
  - ・システムの機能・データ項目の把握
  - ・マスタ、テーブル、月・年次処理
  - ・レポート、アーカイブ処理
- ③システム運営・障害対応
- ④アプリケーションコントロールにおける情報セキュリティ

(5) 点検項目

IT業務処理統制(アプリケーション)についての点検項目として、データインテグリティを重点に、③⑦については主に、テストデータ法を用いて、以下の点検を行いました。

- ①業務処理規程
- ②アクセスコントロール
- ③工程・業務間処理
- ④マスターファイル
- ⑤ポスト処理
- ⑥エラー通知と復旧
- ⑦レポート・統計情報
- ⑧データアーカイブ

(6) 改善案・箇所

点検の結果多くの改善案箇所を得ました。

守秘義務やコンプライアンスの関係で、説明は省略させていただきますが、会計情報のチェック体制、業務処理の効率化、関連法規整備に関し、多くの改善案の検討ができシステム保守・改善に役立ちました。

## 5. 評価・反省

内部統制自己評価は、システム監査の普及やITガバナンスに役立つと共に監査業務に従事していないシステム監査合格者にも役立つものと思います。又、反省として全般統制(ゼネラルコントロール)及び、関連するモジュールの影響について評価点検を十分に行えず、次回の課題となりました。

## 情報セキュリティ監査の実施について

No.9047 角屋 典一

1. 行事名 福井県例会
2. 日 時 6月18日(土) 13時半
3. 場 所 織協ビル(福井県)
4. 内 容

## (1) 背景

NPO法人福井県情報化支援協会(福井県内のITコーディネータの団体)では、昨年度から情報セキュリティ監査の事業化を計画し、協会内にシステム・セキュリティ監査委員会を設置し、検討を進めてきました。

監査実務経験を積むため、ある地方公共団体(以下A役場という)に情報セキュリティ監査の実施を打診したところ、監査の実施について承諾を得ました。但し、当協会としては監査実務ノウハウを取得する目的のため、監査料金はあくまで無料として実施しました。

## (2) 監査ニーズ

情報セキュリティ監査を打診したA役場の状況は次のとおりでした。

- ・「セキュリティポリシー」は作成したが、運用はなされていない。
- ・リスクアセスメントを行っていない。
- 一方、A役場の要望は以下のとおりでした。
- ・今後、セキュリティレベルを向上させたい。ただし、何から着手してよいか判断できないのでどのようにやっていけばよいか教えてほしい。

## (3) 監査実施内容

監査の実施にあたっては、JASAの技術部会が作成した情報セキュリティ監査助言型マニュアル(中間報告)を参考にして、監査計画、監査実施、監査報告の手順はできるだけ忠実に実施しました。

実施概要について以下に記述します。

## ① 監査計画

- a. 監査目的:セキュリティポリシーの適正な運用に着目した監査を実施し、運用における改善点を指摘し、情報漏えいなどの事故を未然に防ぐ。
- b. 監査テーマ:平成1
- c. 監査項目:情報の管理運用状況、物理的セキュリティ運用状況、人的セキュリティ運用状況、技術的セキュリティ運用状況

## ② 監査計画

- a. 実施期間と内容:監査の実施期間として1日目:ヒアリング・スコアリング、2日目:実地調査を計画
- b. チェックリスト作成:チェックリストはA役場のセキュリティポリシーを基に作成しました。

## ③ 監査の実施

- a. A役場にて2日間の期間で実施。

## ④ 監査報告書の作成

- a. 検出事項、改善提言をまとめ、被監査側に提出しました。

## 5. 評価・反省

今回、監査の実務を経験したことは今後のスキル向上につながる非常に有用な経験でした。

初歩的なレベルの感想で申し訳ないのですが、監査実務経験の少ないあるいは全くないメンバーが、拙い監査計画をたて監査を実施していく過程では、知識不足、経験不足から問題点が発生し、それらをなんとか解決しながら進めてきました。

特に、監査計画の策定や監査手続(チェックリスト作成)などは現場を意識した対応が求められ、やはり、監査実務を積みながらノウハウ蓄積の必要性を改めて認識しました。

監査手順や監査手続の設定について、被監査側の状況に適切に対応した内容にすること大切であること、その為には、基本をまずしっかり習得することの重要性を認識し、今後の研鑽すべき方向性がみえてきたと思っています。

## 教育現場の情報化について

No. 1031 風間 一人

1. 行事名 新潟県例会
2. 日 時 9月24日(土) 14時～
3. 場 所 アーバンビル(富山県)
4. 内 容

## (1) 教育情報化の状況

今年度は、「2005年度に日本を世界最先端のIT国家とする」ことを目標としたe-japan戦略の

最終年度になります。e-japan戦略の大きな柱の1つである「教育の情報化」は、IT化による効果が大きいと期待されていますが、現在のところ遅れ気味といった状況でしょうか。

そのような中、公立の小・中学校においては、PC教室や校内LANの整備に年間約2000億円の予算が使われており、インフラの整備は着々と整備が進められてきました。

今後は、本当の意味で子供たちに情報を活用できる能力の開発には何が必要かについて取組んでいく段階に入っているようです。

一方、子供たちに教える側の先生のIT環境整備は大幅に遅れています。先生へのパソコン配備がほとんど実現しておらず、学校の中で行われている事務処理、いわゆる校務については昔ながらの手書きなどの方法で行っている学校がほとんどといった状況です。

## (2) 校務の概要

校務としては、主に3つに分けて考えることができます。

- ① クラス担任が行う成績処理や時間割作成などの「教務」
- ② 事務担当が行う文書管理や備品管理などの「学務」
- ③ 養護担当が行う子供の身体情報管理や健康管理などの「保健」

また、事務作業全般を効率化させる機能として、スケジュール管理・掲示板・施設予約・電子決済などのグループウェア機能の活用も効果があると考えられています。

## (3) 校務IT化に向けた動き

文部科学省と経済産業省共管の財団法人コンピュータ教育開発センターでは、平成15年度に「教育事務負担軽減システム要件調査」を行い、平成16年度にはさらに一歩進めて「校務IT化モデル要件調査」を行いました。

「校務IT化モデル要件調査」では、モデル地区における校務IT化の効果測定や課題の抽出などを具体的にを行うと共に、校務IT化に必要な技術標準化に向けた検討も行われています。

また、平成18年度の文部科学省概算要求に「校務情報化推進事業」として新規に約9500万円の予算が要求されました。

## (4) 今後の課題

教育情報化対策は、主に地方交付税で行われます。地方交付税は、その使途について特に制限があるわけではありませんが、教育の情報化に使ってもらわなければならない内容が十分に理解し適切に執行していかなければなりません。

特に先生へのパソコン配備を早急に実現していく必要があります。

先生個人持ちのパソコンで作業を行うということは、情報管理などのセキュリティ面からも問題があると考えられます。

また、校務の情報化においては、校務時間の短縮や先生の負担軽減状況など効果性の確認方法をどのように実現するかという検討も今後していく必要があります。

「効果性の監査」という厳しい内容とまではいなくても、今後は何らかの確認方法を確立していくことになるでしょう。

今年度発表を振り返って(森)

今年度の発表は、年度目標にあるように、「支部会員の発表・報告により、意見交換や創案の機会を作る」を目的としました。発表後は、質問も良く出され意見交換の場となりました。発表・聴講者共に次の取り組みや新しい課題が発掘されたことと思います。

この火種を消さずに、支部会員一同、次の前進につなげてゆきたいと思います。

## 東北支部

No.1134 高橋 壮太

皆さん、こんにちは。東北支部は設立から約2年半が経ちましたが、この間ほぼ2ヶ月ごとに開催している月例会を中心に活動を展開して来ました。

今年のトピックは、昨年に続いてのITCみやぎとの共催セミナーです。今年は2日間のカリキュラムで、他支部との連携の一環として、中部支部原国際部長において頂き、オフショアのお話をさせて頂いたことです。更に、法人部会の支援として、個人情報のセミナーのパンフレットを、東北6県の各市への案内状送付です。今後のシステム監査普及のため、活動を継続する予定です。

以下に、東北支部の今年度の活動状況をご報告いたします。

## <平成17年度東北支部総会>

概要は以下のとおりです。

日 時：平成17年1月22日

15時00分～17時00分

場 所：(株)IT経営コンサルティング仙台事務所

出席者：9名(委任状提出16名)

講 演：

田口三郎氏(東北会員)による「福島におけるセキュリティ・個人情報保護法への取り組み」

## 議 題:

- 報告事項1 平成16年度活動内容  
 報告事項2 平成16年度収支報告  
 第1号議案 平成17年度活動計画  
 第2号議案 平成17年度予算計画  
 第3号議案 平成17年度役員選任  
 ※支部長 : 鈴木 実 (留任)  
 副支部長: 高橋典子 (留任)  
 佐藤賢一 (留任)  
 研究会 : 高橋壮太 (留任)  
 小野寺司 (留任)  
 広 報 : 佐藤直美 (留任)  
 監 事 : 田口三郎 (留任)

## &lt;平成17年3月例会&gt;

概要は以下のとおりです。

日 時: 平成17年3月5日 (土)  
 15時00分～17時30分  
 場 所: 株式会社富士通東北システムズ  
 第一会議室

出席者: 6名

## 議 事:

1. 鈴木支部長 挨拶・総会報告
2. 研究会発表  
高橋壮太氏(東北会員)による「討論材料としての最近のシステム開発事例紹介」
3. その他

## &lt;平成17年5月例会&gt;

概要は以下のとおりです。

日 時: 平成17年5月14日 (土)  
 13時30分～17時00分  
 場 所: コラッセ福島 企画展示室A  
 出席者: 8名

## 議 事:

1. 研究会発表  
小野寺 司氏(東北会員)による「情報漏洩対策ソフトウェアの機能と事例の紹介」
2. 鈴木支部長 挨拶・理事会報告
3. ITCみやぎ・SAAJ東北支部ワークショップ2005の日程及び内容についての検討
4. その他

## &lt;ITCみやぎ・SAAJ東北支部ワークショップ2005&gt;

昨年に引き続き、ITCみやぎ(ITコーディネータみやぎ会)と共催、ITコーディネータ協会後援による「ITCみやぎ・SAAJ東北支部ワークショップ」を開催いたしました。

1日目はITCみやぎが、2日目はSAAJ東北支部が担当いたしました。

概要は以下のとおりです。

日 時: 平成17年8月26日～27日  
 場 所: 1日目 仙台市青葉区中央市民センター 第一会議室

2日目 仙台市情報・産業プラザ 研修室内 容:

## 【1日目】

- ① 東北IT経営応援隊の活動状況について  
東北経済産業局  
情報製造産業課係長 中山陽輔氏
- ② 顧問ITC制度について  
日本ITイノベーション協会  
事務局長 吉田 徹氏
- ③ ハーマンモデルの活用事例について  
株式会社ハーマン・インターナショナル・ジャパン  
代表取締役会長 半沢道夫氏
- ④ 事例紹介  
ITC福島 佐藤直美氏  
FDK株式会社 須藤浩次氏
- ⑤ ITコーディネータに期待すること  
東北大学教授  
会計大学院長 安田一彦氏

## 【2日目】

- ⑥ ネットワーク監視・診断ソフトウェアSPIDERの紹介  
有限会社風土紀  
代表取締役 北村卓哉氏
- ⑦ オフショア開発について  
日本システム監査人協会  
中部支部 原 善一郎氏
- ⑧ 情報セキュリティの動向について  
クオリティ株式会社  
営業本部 三井智博氏
- ⑨ システム監査の事例～監査ポイントと効果～  
日本システム監査人協会副会長  
兼 東北支部長 鈴木 実氏

## &lt;平成17年9月例会&gt;

概要は以下のとおりです。

日 時: 平成17年9月3日 (土)  
 13時30分～17時00分  
 場 所: 山形テルサ(山形駅西口)  
 特別会議室

出席者: 9名

## 議 事:

1. 研究会発表  
市川新悦氏(東北会員)による「レガシーマイグレーションの取組み」
2. 東北支部上期会計報告
3. 個人情報保護についての意見交換
4. その他

## &lt;平成17年11月例会&gt;

概要は以下のとおりです。

日 時: 平成17年11月12日 (土)  
 14時00分～17時00分  
 場 所: 仙台市中央市民センター第一セミナー室(A)

出席者：13名

議 事：

1. 鈴木支部長 挨拶・理事会報告
2. 研究会発表  
佐藤賢一氏(東北会員)による「NPO法人  
みやぎ情報セキュリティ推進機構  
(MISEC)の活動状況について」
3. 福島市におけるシステム監査普及サービス  
についての状況報告
4. 会報の支部紹介について
5. 公認システム監査人・システム監査人補の  
更新手続きについて
6. 総会の開催について
7. その他

以上です。東北支部としましては、鈴木支部長を中心に、これからも会員相互の研鑽を目的として活動を強化してまいります。今後とも、東北支部へのご指導・ご鞭撻をよろしくお願い致します。



## 北海道支部

No.893 渡部 洋子

SAAJの皆さま、こんにちは。今年の北海道支部便りはすっかりサボってしまっていて、本当にお久しぶりで申し訳ございません。いつの間にかすっかり冬になってしまい、窓の外はもう白い世界です。

一面の緑と花が見れるのは半年後、早くも待ち遠しい毎日です。それでも例年より寒くなるのが遅かったですし、しっかり夏もありました。去年も例年より暖かくて雪が多く、年々「東北化」しているような気がします。日本全国の気候が

ちょっとずつ北にシフトしているのではないのでしょうか。

では、今年の北海道支部の状況報告です。

### (1) SAAJ 北海道支部第3回総会

1月14日(金)に、札幌市民活動サポートセンターで第3回の支部総会を開催いたしました。出席者9名、委任8名で、今年の活動計画や支部役員、予算案などを審議し、4年目のスタートを切りました。この後はもちろん新年会、今年の抱負を語り合いました。

### (2) 2月の勉強会

2月の勉強会は、2月18日(金)に実施いたしました。「e文書法案の現況と文書の電子保存について-法制度の背景と構成を中心に-」第108回研究会のビデオを上映し、ディスカッションを実施しました。会員の間でもe文書法への関心が高まっており、熱心な意見が出てきました。(株)HBA様の会議室をお借りして、参加者は会員9名でした。

### (3) 3月の勉強会

3月の勉強会は、3月18日(金)に、「地方公共団体における情報セキュリティ対策」第109回研究会のビデオ上映を実施しました。会場は久々の北海道立市民活動促進センター、参加者は会員8名、非会員2名の計10名でした。

### (4) 7月の勉強会

7月の勉強会は、7月1日(金)でした。「サイバー犯罪と情報セキュリティに関する警察の取り組み」第110回研究会のビデオを上映し、いつものようにディスカッションに続きました。(株)HBA様の会議室で、参加者は会員8名、非会員2名の計10名でした。

### (5) 9月の勉強会

9月の勉強会は、9月9日(金)に、「タイムスタンプの最新動向」第113回研究会のビデオを上映しました。(株)HBA様の会議室にて、会員7名、非会員1名の計8名の参加を得ました。

### (6) 10月の勉強会

10月の勉強会は、10月26日(水)に、「組織目標化に役立つCOSO ERM」第114回研究会のビデオを上映しました。

(株)HBA様の会議室をお借りして、参加者は会員6名、非会員1名の計7名でした。

### (7) 合同セミナーの実施(予定)

12月10日(土)午前9時から午後18時まで、ITC北海道と共催で1日セミナーを実施予定です。内容は講演4本で、それぞれのテーマは、「脅

威モデル」、「経営品質向上プログラムとは」、「北海道地域における情報産業分野クラスター事業」、「北海道のIT経営応援隊事業」となります。場所は「かでの2・7」の940研修室です。1日セミナーは初めてですが、ITC北海道と共催ですので、気楽にやっていきたいと思っています。セミナー終了後はITCとの合同忘年会の企画も同時進行中です。

こんな1年で終わりそうです。今年は役員が忙しく、なかなか企画ができずに途中ブランクがで

きてしまいました。また、テーマもオリジナルがなかなか出ずに、結局、テープ上映がほとんどでした。それでも、ちょっとマンネリ化の兆しが見られる中、とにかくにも続けてきているのは、テープがあればこそです。非常に感謝しております。いつもご配送ありがとうございます。

4年目の終わりにさしかかっている北海道支部でした。来年はどうなりますか、マンネリ脱却するか、低空飛行が続くか、乞うご期待！

## 会報掲載論文

### ソフトウェア国際取引におけるシステム監査応用の一考察

No.1195 山田 隆

はじめに

近年、ソフトウェアの開発は主としてコスト面の要請から日本国内に限らず、外国のソフトハウスに発注するケースが増加傾向にある。そして、そのような場合、国情の違いから様々な問題が生じ、ソフトウェアの開発が失敗する例も報告されている。

この問題は、外国のソフトハウスに開発を依頼する場合は、日本のソフトハウスとは様々な開発環境条件が異なることから生じていると考えられる。一例として、「仕様どおりに完成できなかった」「性能が不足している」などの問題が最終段階になって発覚し、プロジェクト全体が失敗する例もある。この問題は、本来、正確に提示すべき事項を実行していないと、同じ日本の国内において外注を行う場合においても発生する問題である。しかし、日本国内であれば、要求事項を詳細に明確にしなくても、受注側組織の日本独特の気配りでなんとかでき上がることも多い。しかしこれは、日本国内の場合にのみ通じることである。日本国内であれば通用した曖昧性が、国外への発注の場合に通用せず、それを単なる文化の違いという一言で片付けてきたことが、問題の解決を遅らせてきた一つの要因である可能性もある。これらの問題を回避し開発を成功させるためには、外国との取引であるからこそ、曖昧さを確実に排除して、かつ、外国の法制度等に関係する各種の対策や注意すべき事項への配慮が必要である。

本論文では、外国のソフトハウスに発注してソフトウェアを開発する(以下「ソフトウェア国際取引」という)組織体に対してシステム監査を行う場合の留意点や確認すべき事項について、国際取引で特に重要な分野である、「システム管理基準」の「情報戦略」「企画業務」「開発業務」「共通業務」について示す。なお、本検討は対中国の場合を中心に一般的な国際取引に拡張して考察を進めたものである。

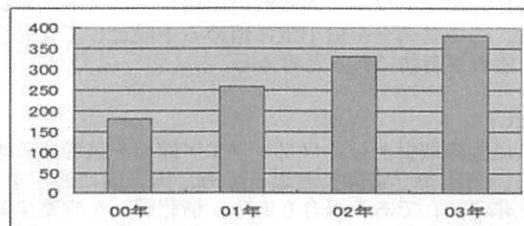
#### 1. ソフトウェア国際取引の背景

日本側から見たオフショア開発の全体像は定かではないが、外国から見た日本のオフショア開発の動向として、中国から見たソフトウェア国際取引の状況を以下に示す。

##### (1) 北京ソフトウェア産業の動向

中国では、ソフトウェア産業の発展に力を入れている。この傾向は中国に留まらず、インド、フィリピンなどでも顕著である。特に中国では日本へのソフトウェア輸出に尽力している。図-1. 1は昨年の3月にSAAJ中部支部が中国(北京)の科学院を訪問した時に、示されたデータである。

図-1.1 北京ソフトウェア産業(2003)(中国科学院) (億元)



これを見ると、2003年北京市のソフトウェア産業規模は前年度より14%増加しており、そのときの説明では、中国全体のソフトウェア産業規模は約1000億元(1.4兆円)であるから、全国の30%を占めている。

## (2) 国際比較

ソフトウェア産業規模における、外国へのソフトウェア輸出(外国からの発注による外国へのソフトウェア納入)動向を、表-1.2に示す。これによると、年々の増加率が大い上、日本向けのソフトウェア輸出が全世界の7割近くを占めていることを示している。

ここから、中国でのソフトウェアの輸出総額は北京だけでも、年間で1億数千万ドル(百数十億円)に達しており、このうち、日本における中国へのオフショア開発の規模は9490万ドル(約100億円)あることがわかる。

表-1.2 北京市ソフトウェアの国別比較輸出額(単位：万ドル)

| 年    | 輸出総額  | 伸び率 | 日本向輸出額 | 割合  | 伸び率 | 米国向輸出額 | 割合  | 伸び率   |
|------|-------|-----|--------|-----|-----|--------|-----|-------|
| 2001 | 6958  | —   | 4676   | 67% | —   | 979    | 14% | —     |
| 2002 | 9314  | 34% | 6274   | 67% | 34% | 868    | 9%  | — 11% |
| 2003 | 13800 | 49% | 9490   | 69% | 51% | 1484   | 11% | 71%   |

## 2. ソフトウェア国際取引における問題点とシステム監査の必要性

## 2.1 ソフトウェア国際取引における問題点

各種の雑誌、論文、セミナー資料などを参考に整理するとソフトウェア国際取引における問題点は以下の通りと考える。

## (1) コミュニケーション不足

ソフトウェア開発の目的、計画から始まって、仕様定義、設計、製造、テスト、納入、品質、権利など、あらゆる工程で発注側の条件(意思)が国際取引先に正確に伝わらない事に起因する問題が発生する。このコミュニケーション問題は、いわゆる「文化の違い」、「常識の違い」に始まって、言語の問題なども関係すると考えられる。

例として、仕様条件を「入力データ条件は英数字8桁」と規定した場合、発注側は規定以外の入力が合った場合はエラーメッセージ処理を当然のこととして期待しているが、受注側は仕様として規定していないから単なるエラー処理だけで、メッセージ出力はしないかもしれない。結果として納入時に不具合の問題として表面化する。(参考文献3)

対策としては仕様書を丁寧に細かくドキュメント記述し、発注元の明確な意思と的確な伝達及び受注側の正確な理解と実行が必要であり、この種の対策は、仕様定義だけでなく、あらゆる工程において必要である。

## (2) 文化の違い

上記で述べた問題と対策は異文化の国々と国際取引を行う場合だけでなく、日本国内での取引においても基本的には必要な事項であると考えられる。しかし、同じ日本国内での受発注であれば省略できる詳細情報でも、異文化の国々との間ではいわゆる「日本の常識」は通用しないため、省略せず丁寧にドキュメント化して伝える必要がある。

## (3) 距離

物理的な距離が遠いことは、実際の開発現場の人々とのコミュニケーション不足の原因になる。関係者同士の信頼感醸成のためには、時間と費用のコストがかかっても最低限の相互訪問が重要である。

## 2.2 国際取引におけるシステム監査の必要性

システム監査の本来の目的を達成するためには、開発段階まで遡って監査することが必要である。(参考文献2)それも、開発終了時点で監査するよりは、開発着手時点と途中段階で監査・助言したほうが効果的であると考えられる。特に、ソフトウェア国際取引の場合、コスト削減のメリットの裏側には開発完了のリスクが存在している。このリスクを最小限に留める手段として受発注双方に関して以下に述べる留意点を考慮したシステム監査が有効であると考ええる。

## 3. 情報戦略における監査のポイント

外国のソフトウェアハウスに国際取引としてソフトウェア開発を依頼する場合、国による文化的な相違を十分考慮する必要がある。日本で「常識」と思っても、国際的に通用するとは限らない。むしろ、日本の「常識」は国際での「非常識」である場合もある。情報戦略を立案する場合、国際取引先の国と日本との歴史、経済的関係の見通しなど、当該国の特徴に配慮の上で、国際取引を採用することについて



て、組織経営の中長期視点から、目的や狙い・コスト・リスクなど、戦略的に総合評価し最終的な方向を結論付けていく必要がある。

### (1) 全体最適化計画策定時の考慮点・留意点

ITガバナンスの方針は国際取引の目的・コスト・リスクに関する評価を十分実施した上で明確化する必要がある。単に経済面だけでなく、国際取引先との2国間の政治動向、国際的な地域全体の中長期動向を十分勘案した戦略の方針を、以下の着眼点の基に監査する必要がある。

(a)組織体としてのITガバナンスの内容の国際取引を含む明確な定義はあるか。

(b)国際取引に理解ある情報システム担当の最高責任者(CIO: Chief Information officer)の選任をしているか。

### (2) 開発体制確立時の考慮点・留意点

国際取引を含む組織体制を確立するとき、国際取引先と発注元の日本企業との連携のモデルを確立する必要がある。連携モデルは開発の関与度合いに応じて様々なケースが考えられる。ここでは、開発体制と、国際取引先での開発工程に関して典型的なモデルを示す。

#### (a) 開発体制モデル

国際取引を含む開発体制の代表例として、国際取引先に関連する日本法人が日本国内に存在し、かつ、開発を行う企業が国際取引先の本国にあるケースをモデルとする。この場合、通常、契約は発注元の日本企業と国際取引先の日本法人との間で交わされる。また、仕様の確定、技術的諸条件の調整、問題対応などは、ブリッジSEと呼ばれる技術者が対応する。ブリッジSEは日本の発注側企業が供出する場合、国際取引先が供出する場合、もしくは双方が供出する場合が考えられる。国際取引先が中国の場合、中国企業が供出している場合が多い。

開発体制モデル図を図-3.1に示す。

図-3.1 開発体制モデル図



#### (b) 工程モデル

開発工程のうち、どの工程を国際取引先に発注するかについては各種のケースが考えられる。監査のポイントとしては、すべてのケースに対応できるよう抽出しているが、一つの代表例として、詳細設計以降を発注する場合の工程モデルを図-3.2に示す。

図-3.2 工程モデル

国際取引によるソフトウェア開発の工程範囲例



このモデルの特徴は、開発体制モデルでの各部門や開発工程の各所に国際取引先との接点関係してくる点にある。これらの接点でのインタフェースを国際取引先と確実に構築する必要がある。以下、開発体制に関する監査のポイントを示す。

- (a)情報システム化委員会本体を発注元企業で日本国内において構成する場合でも、ソフトウェア開発に国際取引を活用する場合、情報システム化委員会に国際取引先の責任者を含める等の対応について十分配慮しているか。
- (b)情報システム部門には、国際取引に関する基本的な理解と専門知識をもつ人材が参加しているか。
- (c)人的資源管理面では、発注元の人的資源だけではなく、国際取引先の人的資源の面に十分な配慮をしているか。

例えば、中国人技術者の流動性が問題になっている。せっかく研修を受けさせたのに、研修が終わると会社を退職し、別の会社によりよい条件で移ってしまう例が多くある。これを抑制するために、研修を受けさせる条件として例えば3年以上の勤務継続を事前に契約事項として定め、もし、会社を辞める場合は、研修費用を請求する、などの対策を考慮している必要がある。

#### (3) 事業継続管理の考慮点・留意点

ソフトウェア国際取引を行った場合のリスク評価と対応策の事前検討が必要である。

例えば、取引先が倒産または、開発不能状態になるリスクをどの程度見積もって、その場合のプロジェクト全体への致命的な影響を最小限にするために何を考慮しておくか検討し、準備しておく。監査ポイントの例としては、以下が考えられる。

- ① ソフトウェアエスクロー（ソフトウェアのライセンスを行う場合に、そのソフトウェアのソースコードや技術情報を第三者「エスクロー・エージェント」に預託しておく制度）を利用しているか。
- ② 納期を最終締め切りに十分余裕をもって設定しているか。

#### (4) コンプライアンスの考慮点・留意点

遵守すべき法令・規範として、個人情報保護法など日本の法令が外注先の外国に影響する場合適切に対応しているか、の監査が必要である。また、日本の法令・規範だけでなく、国際取引先の法令・規範を考慮する必要がある。特に著作権をはじめとする産業財産権に関して国際取引先と正式な契約を締結する必要がある。以下、中国の法令の例を示す。

- (a)知的財産権関連の中国側法令を考慮しているか。

- ① 中華人民共和国著作権法
- ② 中華人民共和国著作権法实施条例
- ③ コンピュータソフトウェア保護条例

- (b)ソフトウェア特許関連として「中華人民共和国特許法」を考慮しているか。

- (c)中国国内のソフトウェア関連として「中華人民共和国技術輸入輸出管理条例」「外商投資商業領域管理弁法（新）」を考慮しているか。

### 4. 企画業務における監査のポイント

#### (1) 開発計画の考慮点・留意点

- (a)開発計画は、日本のソフトハウスを使う場合と基本的には変わらないが、中国等の外国のソフトハウスを使う場合は、より綿密に計画を立てている必要がある。計画は外国のソフトハウスを使うことを決める前の事前調査と意識合わせを十分に行うことから始め、契約内容を十分つめてから業務を始める必要がある。「とりあえず」始めて、「詳細は」後から決めればよい、というのは日本の企業相手の場合だけに通じることである。
- (b)仕様が最初から詳細には決められず、プロトタイプを作成・確認しながら、スパイラルに設計して行く場合、具体的な作業方法や仕様、納期等の条件を詳細に定める必要がある。さらに、インターネット経由もしくは媒体郵送・納入先への持参などのファイル授受などの条件を決めて、アウトプットを提示してもらう方法を採用するのか、それとも、派遣社員に対するのと同じ扱いで、毎日作業指示を出し、発注側の指示ですべてを進めて行くのか、などによって進捗管理方法は大幅に異なる。それぞれに最適な進捗管理方法を定めている必要がある。
- (c)発注元および国際取引先で国際取引に関係するプロジェクトリーダーや技術者などに対する教育方針の骨子はこの段階で明確にし、双方の合意形成が必要である。国際取引の場合は技術内容・技術用語だけでなく、日本の開発の進め方、進捗管理の方法、コミュニケーション手段などマネジメントに必要な最低限の教育が必要である。これは、国際取引先だけでなく、日本側の関係者に対しても相手先との意思疎通に必要な事項を十分検討し、該当者への教育・訓練が必要になる。
- (d)国際取引の場合、相手国との距離が遠いことを十分配慮する。通信手段が発展した今日においても、人と人との直接の接触の重要性は変わらない。全体的なコスト計画の中に、計画的に相互訪問を行うコストを考慮してある必要がある。

## (2) 分析の考慮点・留意点

「分析」での国際取引に関する重要課題は要求仕様の定義である。国際取引先に仕様を確実に伝えるためには、国内の場合よりも丁寧に、詳細に記述した文書で示す必要がある。

本来、第三者にソフトウェア開発を発注する場合は、機能、性能条件など客観的な条件を明確に記述すべきであるが、国内では、この程度書いておけばあとは「常識」で分かるとして、詳細・明確に記述しない例もある。このようなことは、仮に国内では通用する場合があっても、国際取引の場合は誤解を生じ、プロジェクトが失敗する原因になるため、避けねばならない。

主な監査ポイントは以下の通りである。

### (a) 外部仕様は要求事項を含めて網羅的に記述し文書化しているか。

日本では、この程度記述してあればあとは「常識」で分かるはずであるから省略するということは国際取引では誤解を生む可能性がある。日本にとって「常識」でも国際取引先では「常識」でないことも多い。国際取引先では「記述していることを実現すればよい」と考える。すなわち「記述していないことに対応する必要はない」ことになる。できる限り文書として記録に残る形で網羅的に記述する必要がある。

### (b) 内部仕様は外部仕様に基づいて詳細に文書化しているか。

複数のソフトウェアモジュールを組み合わせてシステムを実現する場合で、その一部のソフトウェアモジュールを国際取引先に発注するときは、関係するソフトウェアの外部仕様（動作環境条件、開発環境条件、機能条件、性能・実時間条件、保守・運用関係条件、マンマシンインタフェース条件など）を明確にした上で、入出力条件、エラー発生時の対処条件、その他、実現すべき条件を明確に文書で示す必要がある。

逆の表現をすれば、「文書に記述していない内部仕様は、国際取引先の判断に任せる」ということであると考える必要がある。

### (c) 仕様書のレビューに国際取引先の中核要員は参加しているか。

仕様書、特に内部設計仕様書のレビューを実施する場合、国際取引先のブリッジSEや設計・製造の責任者が参加することが望ましい。できれば、レビュー計画当初から参画してもらい、レビューの目的・進め方等を十分理解してもらい、レビューの実施に当たって要員の確保や遠隔からの出張スケジュールがスムーズに実現できるよう配慮してもらうことが望ましい。

また、レビューした結果は、確実に設計・製造作業やソフトウェアに反映するよう、その後の計画再調整（仕様調整または体制強化・再試験・試験リソース増強など各種の選択肢から総合判断が必要）を含めてレビュー直後に確認できるようにするなど、国際取引先を含むレビュー体制や計画などの事前の準備・確認が重要である。

レビューは工程の区切りだけでなく、中間においても効果的であるが、国際取引先の外国で行うことも非常に有効である。担当者同士の相互理解を深める効果もある。

### (d) 技術的・専門的な用語は定義し・用語集などにまとめているか。

開発に必要な専門用語はなるべく多く定義し、用語集にまとめて、国際取引先との正確なコミュニケーションに役立てることが望ましい。

特に、国際取引先が中国である場合、「カタカナ用語」が難しく感じられるといわれている。「カタカナ用語」の場合、原文の英語表示を併記すれば、より性格にコミュニケーションできる。

## 5. 開発業務における監査のポイント

### (1) 開発手順の考慮点・留意点

開発手順はプロジェクトによって大幅に異なる場合が多い。一方、開発を開始する前には開発手順を関係者全員が理解し実行できる状態にする必要がある。

国際取引を行う場合は、相手が外国であるため、なおのこと、開発手順の理解が求められる。

主な監査ポイントは以下のとおりである。

#### (a) 開発手順は国際取引という条件を十分配慮して明確に詳細に定めているか。

#### (b) 開発手順を日本側と国際取引側双方の責任者が承認しているか。

#### (c) 開発手順は、開発手法（スパイラルやウォーターフォールモデルなど）、開発規模、システム特性（ネットワークシステム、端末システム、組込み型システム、データベースシステムなど）に対応した最適な開発手順になっているか。

#### (d) 開発時のリスク評価として国際取引固有のリスクを評価しているか。

国際取引が初めてである場合、納期直前でのキャンセルなど重大な問題を未然に防止することが重要である。そのためには、考えられる脅威、脆弱性、全体リスクを検討し、対策を開発手順の中に盛り込

む必要がある。また、万一リスクが発生してもプロジェクト全体に致命的な問題にならないような配慮(重要部分の早期レビュー、発注元での技術掌握による代行を可能としておくなど)が必要である。

(2) システム設計の考慮点・留意点

前段の仕様の明確化を受けて、国際取引先でのシステム設計を的確かつ最適に実施するためには、責任者による設計書の承認、入出力画面、データベース、ネットワーク、性能、障害対策などに関するきめ細かい管理が必要となる。

以下に主な監査ポイントを示す。

(a) システム設計書は国際取引先の責任者も承認しているか。

国際取引先の分担分のシステム設計書は、国際取引先の責任者やブリッジ SE の承認が必要である。担当者任せで放任されているではない。また、国際取引先の分担分と直接インタフェースを有するソフトウェアモジュールとの間のインタフェースや機能分担の正確性をレビュー等により確認した記録も同時に存在することが好ましい。

(b) 運用設計との整合性を確認しているか。

システム設計で入出力画面がユーザの利便性を確保しているか、また、データベースと業務内容の整合性はとれているかについて、レビューを通して確認する必要がある。

「利便性」や「業務内容」に関する要求は、設計仕様として具体的に記述してある必要がある。

(c) ネットワーク構成と業務内容の整合性がとれているか。

ネットワーク構成を検討するとき、開発環境としてのネットワーク構成と、ターゲットシステムとしてのネットワーク構成を区別し検討し、かつ全体整合を考慮する必要がある。

国際取引での開発環境を考える場合、開発環境を設置する場所(国)が日本の場合はシステム管理基準に準じて検討すればよいが、外国で開発環境を構築する場合、日本を含む全体での情報環境の最適化が必要である。特にセキュリティ面での配慮と、国際間にゲートウェイ装置がある関係上、性能問題にも配慮が必要である。

ネットワークの設計を行う場合も前記同様の配慮を加えて、当該国固有の開発条件(国産品の利用など)に配慮が必要である。このため、要求仕様条件(機能、性能、品質、外部条件、保守条件その他)を詳細に文書化して相互承認を確実に実行していく必要がある。

(d) 要求性能の実現性が確保されているか。

① 要求性能規定：要求性能が明確でなく、プロジェクトが危機に陥ることは多い。また、性能条件が最終システムでの条件のみ規定されており、中間段階での規定がない場合もリスクが大きい。特に、国際取引でシステム全体でない、一部のモジュールのみ発注するような、部分設計・製造の場合は、当該部分における性能条件の規定が重要である。部分システムの性能仕様の規定は難しいこともあるが、大規模システムの場合は特に、性能シミュレーション等も検討し、この性能仕様の規定内容の妥当性の可否を検討する必要がある。代替方法として、重要モジュールを組み込んだプロトタイプシステムで事前確認する方法もある。

② 実時間性能条件：性能といっても、単位時間あたりの処理トランザクション数や、通信システムでは、処理パケット数、処理呼数などだけでなく、レスポンスタイム条件などを、実時間条件と背景となるトラヒック条件やその他の外部環境条件(例えば無線での電波伝搬特性としてのフェージング条件と誤り・消滅条件など)の前提の下で明確にするなど、詳細な規定と国際取引先との相互承認が必要である。

③ 品質条件：下記の障害対策や、上記の外部環境条件とも関連するが、エラー発生率、呼損率、パケット紛失率、パケット誤り率、などの品質条件がある。これらの条件はシステムの基本構造に影響するため、早い時期での明確化が必要である。国際取引先に詳細に提示し、相互承認をとる必要がある。

(e) 障害対策を検討しているか。

システムの内外の要因に起因するエラーや障害時の復旧機能について規定する。国際取引の場合は特に詳細に規定し相互承認が必要である。復旧条件は機能面だけでなく、実時間面も規定する。さらに、保守担当者への通知機能など、あいまいにするとトラブルの要因になるので注意が必要である。

(f) レビュー計画を立てているか。

レビュー計画は各工程単位で実施することが好ましい。特に国際取引の場合、直接技術者とコミュニケーションがとれる機会でもあり、なるべく頻繁に実施するとリスクを減少させる効果がある。

重要な点は、事前の計画と確実な実行、および、報告と対策実施・管理である。

国際取引先や、ブリッジSEに任せきりで、計画の遅れのためレビューを省略したり、先方の報告確認だけで済ませてはならない。

### (3) プログラム設計の考慮点・留意点

コーディングに入る直前のドキュメントとしての「プログラム設計書」の体系・形式・記述内容について明確な基準を定め、発注側と受注側で内容のレビュー・確認が必要である。プログラム設計書は、機能条件、入出力条件、エラー処理条件(メッセージ有無含む)性能条件、など、詳細に記述していることが望ましい。

作業効率の観点から、このドキュメントが省略される時があるが、その場合は、システム設計書に基づいてコーディングすることを許容することを承認する必要がある。この場合、機能の実現方法の担当部分について、プログラム設計側に委ねることになるので、中間でのレビューで、発注側の意図するプログラム設計になっているか確認が重要になる。

受注側でプログラム設計書を作成する場合は、プログラム設計書は発注側によってレビュー・承認していることが必要である。

### (4) プログラミングの考慮点・留意点

プログラミングに入る前にコーディング規約を確立する必要がある。国際取引を行う場合、最低限の品質を確保するためにも極力詳細に定めることが望ましい。単に、形式的な事項だけでなく、プログラムの機能や構造上、注意事項、その他、使用する命令の特徴に対応した注意事項などがあれば、それも含めたほうがよい。単に形式的なルールだけに留まると、簡単なコーディング規約確認ツールを用いて、コーディングレビューは不必要であるかのような実態になる恐れがある。

プログラミング後ソースコードレビューは必須条件である。しっかりとしたレビュー計画を立てて、必ず実施している必要がある。

### (5) システムテスト・ユーザ受け入れテストの考慮点・留意点

(a)単体のモジュールテスト、モジュール結合試験、システム単体試験、システム結合試験、総合試験、移行試験、運用試験、性能試験など、関係するソフトウェア、ハードウェア、周辺システム環境、運用人員環境、運用時間条件、地理的・設備的環境条件その他あらゆる条件を国際取引先に明示して最終的なシステム全体試験を要求仕様条件に基づいて確実に完了させていく必要がある。

ユーザ受け入れテストの条件もなるべく詳細に提示していることが望ましい。十分詳細に提示できる場合は、このテスト条件を事前に国際取引先に提示し、国際取引先での出荷テストの試験項目に取り込んでおいてもらうと良い。この場合、ユーザ受け入れテストはサンプリングで実施する方法も可能である。

(b)国際取引の場合、性能に起因する問題が、最終的なシステムテストで表面化するケースがある。工程の最終段階での、この種の問題はプロジェクトに致命的な問題となる。これを避けるためには、システムテストに入る前の製造工程でのモジュールテストの段階で、目標の明確化と測定・評価方法の確立が重要である。システムテストの段階では、一番早い段階での測定・評価を実施していることが重要である。

## 6. 共通業務における監査のポイント

### (1) ドキュメント管理の考慮点・留意点

(a)ドキュメント管理の体系化と、国際取引先に作成してもらう部分の明確な取決めが必要である。各工程単位で必要なドキュメントの種類と作成環境、日本語ドキュメント作成に使用するソフトウェア、フォントの条件なども、決める必要がある。詳細設計書、ソースコードへの日本語コメントの挿入、進捗報告書などが関係する。

(b)ソフトウェア開発手法として、例えばUML(Unified Modeling Language)を採用する場合は、開発・維持のためのツールなどの環境を統一している必要がある。

### (2) 進捗管理の考慮点・留意点

進捗管理を行う場合、どこまで細かく日本流に管理させるか注意が必要である。具体的なやり方まであまり細かく管理すると、「文化問題」が出てくる。粗すぎると、こちらが心配になって信頼関係が崩れる要因になる。

進捗管理は、結局は「人」である。「日本と国際取引先の国に通じた優秀な人材こそが重要である」とことは正しい。しかし、すべて、その人任せではプロジェクト責任者として、客観的な進捗管理はできない。優秀な「人」に加えて、客観的なチェックポイントを押さえ、評価・管理ができるようにしている必要がある。

### (3) 品質管理

(a) 品質管理は定量的に行う必要がある。詳細設計以降、バグ件数、バグを数える基準、バグ密度、「バグ」や「バグ密度」の定義、目標バグ数、性能目標、性能の評価基準など、具体的に定めている必要がある。

(b) 品質の責任範囲を明確にする。特に、システム全体の中での一部を国際取引する場合、システム全体の性能責任は発注側にある。国際取引先が担当する部分の性能の要求と確認方法を明確にしている必要がある。

### (4) 人的資源管理の考慮点・留意点

#### (a) 要員の流動対策

国際取引先の要員の教育を行いスキルレベルが向上しても、当の技術者がよりよい条件の別会社に移ってしまうことが多くある。例えば中国ではスキルの高い人は高い年収で雇用される。発注側で教育した結果としてスキルが上がった場合、そのスキルレベルに応じた待遇をしないと、他社に移る。この現実を踏まえた対応をしている必要がある。

(b) 仕事の割当てを能力に見合ったものであるかの観点が必要である。レベルの高い人にだれでも出来る仕事(将来的な価値が低い場合など)を割り当てると、不満が高まる。逆に、能力以上の仕事を割り当てるときは、断ることをしないため、できないことがプロジェクトの後半に出てくる恐れがある。

(c) プロジェクトを開始する前に日本側の責任者や主だったメンバーが国際取引先の現地を訪問し、現地のスタッフ全員とコミュニケーションすることが好ましい。そこで、直接どのような仕事を要求するのか、また、現地の事情など、話し合っていることが好ましい。

### (5) 委託・受託の考慮点・留意点

(a) 全体のシステムの中で何を委託するか、委託範囲を明確にし、契約を結ぶ場合、コンプライアンス、再委託、知的財産、特約および免責事項を明確にしている必要がある。

(b) 契約内容は、国際取引側の責任者と内容を確認するだけでなく、中国専門の法律事務所に確認するなどの注意をしている必要がある。

### あとがき

以上、ソフトウェア開発に外国のソフトハウスを活用する時の留意点について、「情報戦略」、「企画業務」、「開発業務」、「共通業務」について概略を示した。なお、ここでのポイントは、国際取引でない国内での開発の場合もあてはまるポイントも多いが、国際取引の場合、特に注意すべきポイントとして掲載してあります。

なお、本論文は、まえがきでも述べたとおり、対中国を中心に考察を進めたものであり、その他の国々に関して必ずしも当てはまらない事項もあると思われる。システム管理基準のサブコントロールとしての充実の検討も必要であり、これらは今後の研究課題として残っていると考えます。

### 謝辞

本検討は昨年SAAJ中部支部が中国(中華人民共和国)の中国科学院計算技術研究所とシステム監査を通じた交流会に向けての検討結果が母体となっている。大野支部長、原国際部長をはじめとする関係各位に感謝します。

#### 注記

なお、ここで述べた留意点に基づくシステム監査のチェックポイントの詳細については、近日発行予定の情報システム監査実践マニュアル(日本システム監査人協会編)に掲載してありますので、合わせて参考にして頂ければ幸いです。

### 参考文献

- 1 (北京科学院)
- 2 情報システム監査実践マニュアル(日本システム監査協会編)
- 3 中国でのソフト開発成功法(日経システムプロバイダ 2002/3.1)

### 会報掲載論文募集要項

会員の皆さんより、会報掲載論文を募集します。

1. 論文の内容

システム監査・セキュリティ監査(関連を含む)の実務の裏づけのある内容で、システム監査・セキュリティ監査(関連を含む)の啓発、普及、理論深化、情報提供、実践、手法開発等に役立つ論文。既発表論文は除く。

2. 字数 6千字以上、17千字以内(図表を含める)

3. 提出方法 ms-wordで作成し、フロッピーディスクで会報編集委員会あて送付する。  
(メールに添付する場合は、パスワードを設定する)

4. 審査

会報編集委員会内に設ける論文審査委員会にて、審査を行い、掲載に値するか、及び内容の優劣を判断し、掲載する場合は、2万円以上、6万円の範囲で原稿料を支払う。審査の内容は公表しない。

5. ここに掲載した論文は、公認システム監査人(補)継続教育で、10時間/1稿として認める。

6. 掲載論文募集締め切り

常時受け付けとし、会報編集委員会より打ち切りのお知らせがあるまで継続する。

### 会報掲載論文審査要綱

理事会提案 2003.7

最終改訂 2003.10 判定基準(点数)改訂

1. 論文審査委員会

応募論文が提出されたら、編集委員長は、応募条件を満たしているかを判断する。

応募条件を満たしていない場合、直ちに却下する。

(応募条件: 字数の制限、応募者は会員であること)

応募条件を満たしている場合、直ちに、編集委員の中より、2名の審査委員を任命する。

編集委員長を含めて3名で審査委員会を構成する。

論文提出者を、審査委員に加えることはできない。

編集委員長が論文提出者の場合、編集委員長を除いた編集委員会で3名を選出し、審査委員会を構成する。

審査委員名は公表しない。

2. 審査委員は、提出した論文を査読し、判定基準表に基づき、点数を出す。

判定基準は、会員からの要望があれば公表する。

以上

# 情報システム・ユーザ会連盟主催「システム監査講演会」

## —平成17年度情報化月間参加行事—

日時：平成17年11月2日（水）

場所：きゅりあん（東京・品川区立総合区民会館）

**演題：「情報セキュリティガバナンスによる  
内部統制の強化と企業価値の向上に  
向けた政府の取組」**

**講師：経済産業省 商務情報政策局  
情報セキュリティ政策室  
田辺 雄史 氏**

■報告者 株式会社日立情報システムズ  
No.6005 斉藤 茂雄

### ■所感

本講演は基調講演に相応しく、ウィルス被害、不正アクセスなど近年の情報セキュリティ脅威とこれに対応した経済産業省ないしは政府全体の動向を概観し、更には本題の情報セキュリティガバナンスの解説に至る内容であり、システム監査に携わるものばかりではなく、情報セキュリティに係わる多くの人々にとって、包括的に情報セキュリティの課題と方向性を理解する絶好の機会となったと思う。

情報セキュリティに係る脅威については、ウィルスやワームに留まらず、最近ではスパイウェア・フィッシングといった経済的利得を目的とした情報搾取やボットといった組織化・分業化した複合的な手法による攻撃まで出現し、より手口が悪質化している。そのため、従来の技術的対策レベルから組織的・社会的対策レベル、国家的対策レベルといった広範な対策が必要とされて来ている。このような背景から政府一丸となった取組みが要請され、2004年7月から根本問題について議論を開始、2005年4月には内閣官房の体制を強化し、官民の専門家を集約し、「内閣官房情報セキュリティセンター(NISC)」を設置したとのことである。また、同5月には「情報セキュリティ政策会議」を設置し、国家レベルのセキュリティ対策に係わる行動計画作りを進めつつあるとのことであった。

一方経済産業省では企業を中心とした社会的対策レベルの指針として2005年3月に「情報セキュリティガバナンスの確立に向けた報告書」を取り纏め、企業における情報セキュリティガバナンスの方向性を提言している。

現代の企業にとって情報セキュリティ対応は極めて喫緊の経営課題であるが、リスクの不明確さに対して、対策の費用効果も不明確で、情報セキュリティを高めることそのものが事業目的でないことから、その取組みには頭の痛い課題が多くあるのではないだろうか。

情報セキュリティガバナンスの報告書は、

- ① 企業の情報セキュリティ対策レベルを測定するための指標である「情報セキュリティ対策ベンチマーク」
  - ② 企業自らの対策の実施状況等について対外的に公表するためのモデル「情報セキュリティ報告書モデル」
  - ③ 企業がIT事故発生時にも事業運営を継続的に維持するための計画(BCP)の策定手順等を述べた「事業継続計画策定ガイドライン」
- の3点セットからなる。これらは、企業における情報セキュリティを自律的・継続的に改善・向上するための組織的・包括的アプローチの導入が必要との立場から作成されたものである。企業経営の中にどういった「力学」を働かせると情報セキュリティが確保されるか、どうしたら「ちゃんとやったところが評価される」のかといった疑念があり、3点セットがセキュリティ対策の一つの尺度として活用されることを望んでいるとのことであった。更にはこれらの尺度が企業における情報セキュリティ対策の格付けや表彰制度に発展することを希望しており、政府の調達への活用が取組みが必要との田辺氏のご意見であった。

情報セキュリティ監査に携わる者として、上記3点セットは監査視点の一つとして大いに活用すべきと考える。その前に各社、自社の情報セキュリティ対策レベルの確立と向上のために積極的な適用を進めるべきであろう。

### ■講演内容

- ・情報セキュリティを取り巻く状況
- ・情報セキュリティに係る脅威等の変遷と経済産業省の施策
- ・情報セキュリティ対策のレベル
- ・情報セキュリティ対策の考え方
- ・環境分野と情報セキュリティ分野の歴史の流れ
- ・政府全体の動き—経緯
- ・情報セキュリティ政策会議及び内閣官房情報セキュリティセンター(NISC)の設置
- ・情報セキュリティ政策会議において検討中の課題
- ・「政府機関の情報セキュリティ対策のための統一基準」について
- ・「重要インフラの情報セキュリティ対策に係る基本的考え方」について
- ・経済産業省の情報セキュリティ政策
  - 情報セキュリティ政策の歴史、技術的手段の適用推進、企業経営への組込み、人材育成等
- ・情報セキュリティガバナンスの確立に向けて
  - 事業活動の「神経系」となったIT



- 事業リスクとしての情報セキュリティ～ IT 事故の実態～
- 経営課題としての情報セキュリティの位置付け
- 情報セキュリティ対策の現状
- 企業における事業継続計画 (BCP) 策定動向
- 情報セキュリティガバナンス：行動のためのフレームワークに向けて
- セキュリティ文化と企業のあるべき姿
- 情報セキュリティガバナンスの概念
- 情報セキュリティ対策ベンチマーク
- 対策ベンチマークに係るセルフチェックのための Web サイト
- 情報セキュリティ対策ベンチマーク～国際標準との関係
- 情報セキュリティ報告書モデル
- 事業継続計画策定ガイドライン
- 今後各主体に求められる取組み

- ・ 監査実施の流れ－米国企業改革法対応監査の場合
  1. 個別監査計画書の作成
  2. キックオフレターの発信
  3. キックオフミーティング
  4. リスク分析評価
  5. 監査プログラムの準備
  6. フィールドワーク
  7. 発見事項の説明
  8. テストレポート / テストステータスの作成
  9. レスポンスの確認
  10. フォローアップ

**演題：「IT ガバナンスの確立と事業継続マネジメント (BCM) の構築」**

**講師：KPMG ビジネスアシュアランス株式会社  
常勤顧問 喜入 博 氏**

**演題：「在日 AIG カンパニーズにおけるシステム監査への取組みについて」**

**講師：AIG 株式会社 システム監査部  
シニア・システムズ・オーディター  
朝川 充 氏**

#### ■報告者

SAAJ 理事、株式会社日立情報システムズ  
No.6005 一村 義夫

#### ■所感

通常監査、個人情報保護法対応監査、米国企業改革法対応監査等、複数の監査を並行して実施している、或いはそのような状況を控えている組織の監査人にとっては、大変参考になったのではないかと。とくに米国企業改革法対応監査に関しては事例発表がまだ少ない中での発表であった。システム監査人にとっても米国企業改革法対応監査あるいは日本版 SOX 法対応監査など、業務の拡充機会が出てきたということであり、研鑽を積み、その機会を活かし、活躍の場を広げていくべきであろう。

#### ■講演内容

##### ・ 会社概要

AIG グループは、世界の保険・金融サービス業界のリーダー。130 以上の国・地域で事業展開。

- ・ 在日 AIG カンパニーズのシステム監査体制
- ・ 年度監査計画の立案
- ・ 監査の種類
- ・ 監査実施の流れ－通常監査の場合
- ・ 監査実施の流れ－個人情報保護法監査の場合

#### ■報告者

SAAJ 理事、株式会社日立情報システムズ  
No.6005 一村 義夫

#### ■所感

今年3月に経済産業省の「企業における情報セキュリティガバナンスのあり方に関する研究会」(座長：土居 範久 中央大学 理工学部 教授)から報告書が発表された。講師の喜入氏は同研究会の委員であり、「事業継続計画策定ガイドラインワーキンググループ」の主査を務められるなど、我が国第一級の BCM 専門家である。今年に入り、経済産業省、内閣官房、内閣府のほか、コンピュータメカ系、損保系、コンサルタント系等の代表企業からさまざまな場で事業継続にかかわる提言、提案が相次いだ。そうした流れに押されるように大手企業においては、BCP、BCM 導入が経営課題であるとの認識が広まりつつあるように思われる。喜入氏の講演は、これから BCP、BCM の導入を企画しようとしている者にとり、BCP、BCM の導入の背景、目的他を整理する上で大変役に立つ内容だったと思われる。喜入氏の講演に先立って行われた経済産業省の田辺 雄史氏の講演「情報セキュリティガバナンスによる内部統制の強化と企業価値の向上に向けた政府の取組み」と相俟って BCM の構築の重要性がよく理解できる内容であった。喜入氏が所属する KPMG 社が2004年に調査した業務中断理由や BCP 策定状況の日米比較は、日本の経営者に BCM 導入・強化を説得する上で大変貴重な調査データである。業務中断理由の調査(重複回答)では、日本では2割程度の企業が機器故障、ソフトウェア障害、通信の故障を挙げ、これらが業務中断理由のトップを占めており、米国では8割程

度の企業が停電を挙げ、6割前後の企業が自然災害、機器障害、ソフトウェア障害、人的ミス、通信の故障、ウイルス感染・不正アクセス行為を挙げている。このような業務中断の経験の差が、日本のBCP策定済み企業は22%、米国のそれは67%という結果につながっているようである。しかし、今後、日本の大規模停電、大規模自然災害、その他のリスクのポテンシャルが、米国のそれよりも低いと言い切れる状況にはないというのが報告者の昨今の実感であり、予感である。現在、日本企業の取り組みは、米国のそれに大きく水を空けられている。しかし、今回の調査データは、日本の企業にとって、早期のBCP策定・強化は、他社との差別化の有効な武器になることを裏付けるものである。また、BCMにおいて監査或いはシステム監査が担うべき役割が明確にされている。これは、システム監査人の業務拡充の機会であり、われわれシステム監査人はその責任を果たすべくますます研鑽、実績を積むことが社会的にまた組織内で期待されるにちががなく、我々はその期待に応えなければならないと思う。喜入氏には、次の発表機会には、是非、事例発表をお願いしたいと思った。

#### ■ 講演内容

- ・情報セキュリティ対策のこれまで
- ・個人情報保護法の本格施行への対応
- ・個人情報保護と情報システムのガバナンス
- ・経済産業省の「システム監査基準」の改定
- ・ITガバナンスの構成要素
- ・ITガバナンスにおける八つの管理要素と管理の仕組み
- ・企業を取り巻くリスク(リスクの企業外および企業内の起因を整理)
- ・事業継続計画策定ガイドラインの背景と目的(経済産業省の発表引用)
- ・経済産業省：事業継続計画策定のガイドラインの構成(経済産業省の発表引用)
- ・業務中断理由(日米比較。KPMG調査)
- ・BCP策定状況(日米比較。KPMG調査)
- ・政府における事業継続の必要性の提言等(内閣府、経済産業省、内閣官房)
- ・ISO：事業継続計画の標準化動向
- ・BCPとBCM(出所：BSI)
- ・BCMのPDCAサイクルと主な作業
- ・ビジネスインパクト分析・リスク分析(出所：経済産業省)
- ・BCP発動時の段階(出所：経済産業省)
- ・BCM構築のポイント
- ・BCMのシステム監査の視点
- ・事業継続計画の管理基準と監査の視点

### 演題：「サイバー犯罪・サイバーテロの現状と対策」

講師：警察庁サイバーテロ対策技術室

伊貝 耕 氏

#### ■ 報告者

SAAJ理事、株式会社日立情報システムズ

No.6005 一村 義夫

#### ■ 所感

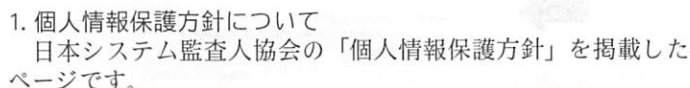
サイバー犯罪が身近に感じられる今日である。国の警察機関である警察庁は、広域組織犯罪に対処するための警察の態勢、犯罪鑑識、犯罪統計等警察庁の所掌事務について都道府県警察を指揮監督している。講演の内容は、通り一遍の犯罪の紹介ではなく、犯罪の実態および警察庁の犯罪に対する現状把握と認識を踏まえており、なかなか興味深い内容があった。国や地方自治体における犯罪防止体制についても理解を深める上で大変役立った。警察の活用の訴えがあった。サイバー犯罪に対処するために技術者集団400名、うち専従者300名だそうである。わが国の犯罪対策としてこれで十分かどうかは分からないがその規模には正直驚いた。我々システム監査人としては、より現実差し迫っているサイバー犯罪に対応できるよう監査項目の見直しなど積極的に対応すべきであろう。

#### ■ 講演内容

- ・サイバー犯罪の現状：検挙件数は年々増えているが、犯罪事案件数に対する検挙率が増えているかどうかという意味では、懸念される。
- ・サイバー犯罪に関する警察への相談件数は、うなぎのぼりである。
- ・サイバー犯罪の現状(phishing、サイバー脅迫などに犯罪組織が関与ほか)
- ・情報システムをとりまく情勢(インターネットへの接続の拡大ほか)
- ・情報セキュリティ事案と背景(個人情報漏洩に対する包括的な禁止規定の欠如ほか)
- ・各種有害活動(功名心から金銭的利益へ、個人から組織へ、Malware(有害ソフトウェア)の利用ほか)
- ・情報セキュリティポリシーの必要性
- ・PDCAループの要諦
- ・適切な対処のために(発生を前提とした体制が必要)
- ・インシデントレスポンス(基本的な流れ。想定される情報セキュリティ事案への対処、対処手段を規定)
- ・警察の活用(「警察が来た!」のショック療法ほか)

本年度の機能改善として、当協会のホームページ(<http://www.saa.or.jp/>)に、以下情報掲載を追加しました。時々確認し、有効に活用してください。(HP担当)

1. 個人情報保護方針について（新設）
2. 公開情報登録・変更・削除フォーム、会員登録情報の変更フォーム（新設）
3. サイトマップ（新設）
4. ML 規約（新設）
5. 発信メール履歴（新設：メールが届かない場合、アドレス変更をしていない可能性があります。発信メール履歴を確認し、アドレス変更手続き（2 項参照）をお願いします）
6. 「協会全般のお知らせ」を「研究会等のお知らせ」と「協会からのお知らせ」に分割
7. 広告掲載（新設：有料広告の掲載）



2. 公開情報登録・変更・削除フォーム、会員登録情報の変更フォーム

公開情報の登録・変更・削除や、会員登録情報の変更をホームページからできるようにしました。

公開情報登録・変更・削除フォーム、会員登録情報の変更フォーム、いずれも「個人情報の取扱いについて」に同意していただいてから入力するようになっております。従来からある「入会申込みフォーム」も「個人情報の取扱いについて」に同意していただいてから入力するようになっております。

具体的な画面の流れは、以下の通りとなります。

(1) 公開情報登録・変更・削除フォーム

「個人情報の取扱いについて」画面

公開情報への査読・変更・削除(非公開)

■公開情報への査読・変更・削除(非公開)

個人に関する以下の事項に同意いただくことが必要です。

「同意する」をクリックすると「公開情報への査読・変更・削除(非公開)」フォーム  
(5/11/2012)が 表示されますので、お申し込みください。

個人情報の取得について

(1) 当会では、個人情報保護政策を定め、活動の推進を図ります。また、活動に同意したものとします。  
(2) 当会では、収集した個人情報を活動の目的に必要範囲で利用します。  
(3) 当会では、下記の場合、第三者等に個人情報を提供する場合もあります。  
a) 本会が主催する活動の開催  
b) 本会が主催する活動の開催と、活動  
c) その他、当会が活動の推進に必要と判断した場合  
(4) 当会では、名称、ホームページ、メールのアドレスと連絡先を明記して、本会を意図した個人を特定し  
ておきます。  
(5) 当会では、お電話、Eメール、郵便物、等で取得する個人情報に訂正、削除を希望  
する権利があります。この場合、当会では必要に応じ対応いたします。

個人情報保護の取組について

個人情報保護法に基づき、当会では  
特定個人情報保護官  
日本NPO法人協会個人情報保護  
推進センターに個人情報保護法第4条  
第四項に定める監視官の申請  
TEL:03-3593-4141 FAX:03-3593-4142  
E-mail: info@npo-jp.org

(議事録参照) 2018年6月(予定)

Copyrighted Material

「同意する」  
をクリック



(「同意しない」をクリックすると、トップページに戻ります)

公開情報登録・変更・削除フォーム

※印刷機能は、印刷フォームにてご利用ください。

**日本システム監査人協会 公開情報登録・変更・削除フォーム(公開システム監査人等)**

---

|       |                                                                                                                     |  |  |
|-------|---------------------------------------------------------------------------------------------------------------------|--|--|
| 入力年月日 | 10/7/2013                                                                                                           |  |  |
| 登録内容  | <input type="radio"/> 登録 <input checked="" type="radio"/> 登録 <input type="radio"/> 削除 <input type="radio"/> 更新(非公開) |  |  |

**※現在協会に登録しているデータを入力してください。**

|           |                                                                           |                                          |  |
|-----------|---------------------------------------------------------------------------|------------------------------------------|--|
| 属性(必須)    | <input checked="" type="radio"/> 公開システム監査人 <input type="radio"/> システム監査人様 |                                          |  |
| 登録証番号(必須) | <input type="text"/> ※内5桁数字入力                                             |                                          |  |
| 氏名        | 姓 <input type="text"/> 名 <input type="text"/>                             | カナ <input type="text"/> ※内5桁カナを入力してください。 |  |

**※登録または変更する項目を入力してください。**

|      |                                               |                                          |  |
|------|-----------------------------------------------|------------------------------------------|--|
| 新氏名  | 姓 <input type="text"/> 名 <input type="text"/> | カナ <input type="text"/> ※内5桁カナを入力してください。 |  |
| 新連絡先 | <input type="text"/>                          |                                          |  |
| 得意分野 | <input type="text"/>                          |                                          |  |
| 得意分野 | <input type="text"/>                          |                                          |  |
| Eメール | <input type="text"/>                          |                                          |  |

入力データの登録が必要な方は登録画面を印刷して保存してください。

## (2) 会員登録情報の変更フォーム

「個人情報の取扱いについて」画面

[illegible]

「同意する」  
をクリック



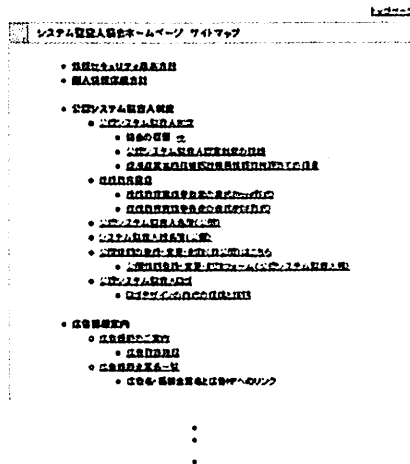
(「同意しない」をクリックすると、トップページに戻ります)

## 公開情報登録変更フォーム(会員・非会員用)

[illegible]

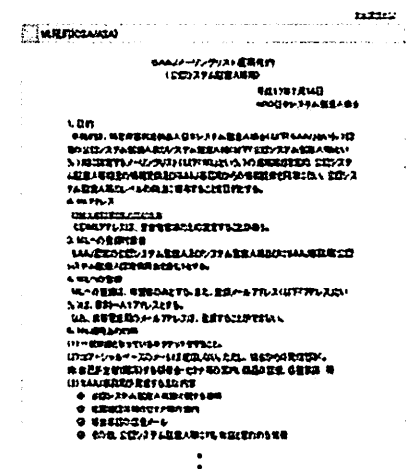
## 3. サイトマップ

サイトマップを掲載しております。



## 4. ML 規約

SAAJ メーリングリスト運用規約を掲載しております。



## 5. 発信メール履歴

2005年7月1日以降に発信したメールのメール番号、タイトル、発信年月日を掲載しております。

メールが届いていない方は、メーリングリストに登録されていないか、アドレスが間違っている可能性があります。

メールアドレスの登録・変更処理をお願いします。(ホームページからできます。)

| 発信メール履歴 (2005年7月1日以降) |                                         |            |
|-----------------------|-----------------------------------------|------------|
| メール番号                 | タイトル                                    | 発信年月日      |
| reprsaas-01           | (再) 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」 | 2005/11/10 |
| reprsaas-02           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-03           | (再) 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」 | 2005/11/10 |
| reprsaas-04           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-05           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-06           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-07           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-08           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-09           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-10           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-11           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-12           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-13           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-14           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-15           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-16           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-17           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-18           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-19           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |
| reprsaas-20           | 2005年11月17日の研究発表<br>「電子技術情報誌誌名について」     | 2005/11/10 |

トップページの「協会全般のお知らせ」を「研究会等のお知らせ」と「協会からのお知らせ」に分割し、見やすくしています。

- 地方自治体向け(平成17年度)情報セキュリティセミナーのご案内  
0005/11/17 (FRI) 11:00
- 第11期月間研究会「電子政府構築に向けた取組について」  
0005/11/17、日・東京府のご案内 0005/11/02 19:00
- プロ大分・日本システム監査人協会九州支部合同セミナーのご案内  
0005/11/18、日・大分 0005/11/01 09
- 「個人情報保護管理者/監査責任者の養成」セミナーのご案内  
0005/11/19、日・東京 0005/11/02
- システム監査実習セミナー(大阪コース) 0005/11/25-27、日・大阪府  
のご案内を掲載しました。0000-00
- 第11回月報発表会と総会の冒しへ(来月おこなう) 0005/11/0

---

**協会からののお知らせ**

- 法人会員の紹介ページの更新 0005/11/17 (FRI) 11:00
- 発信メール機能の実装 0005/11/17 (FRI) 11:00
- 法人向け情報通信研究会(学会)へ募集のご案内 0000-00
- システム監査実習についてと主催者・システム監査人協会へ加入をお願い  
日本システム監査人協会へ加入のお願い(事務局より) 0005/11/02 19:00

## 「広告掲載企業名一覧」ページ

[illegible]

広告掲載企業名一覧  
 広告掲載企業名一覧  
 特設ページ掲載法人  
 日本システム製造人協会  

| 企業名 | 企業名 |
|-----|-----|
|     |     |

 (C)2014年(日)  
 Japanese Auction Association of Japan

本会報が届く頃には完成しておりますので、確認してみてください。

**第6回システム監査実務セミナー実施報告**

No.1060 太田 香

去る9月、第6回システム監査実務セミナーが延べ4日間にわたり開催されました。

今回は過去の受講者の方々からの要望が多かったセキュリティ監査の事例をベースに、新しく開発された教材を初めて取り上げたセミナーとなりました。

また、事例に基づき、今回のセミナーでも財団法人金融情報システムセンター(FISC)殿で発行されている「金融機関等のシステム監査指針」をテキストの一部として使用させて頂きました。

以下に実施内容をご報告させていただきます。

**I. 実施概要****1. 日程**

9月 3日(土)～ 4日(日) (前半)  
9月 17日(土)～ 18日(日) (後半)

**2. 場所**

幕張OVTA (海外職業訓練センター)

**3. 受講者数**

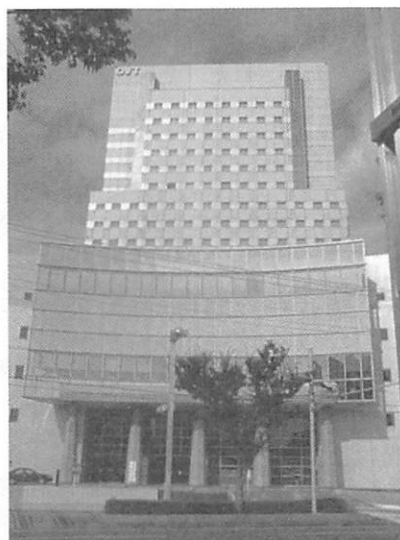
18名

**4. 講師**

鈴木 実 沼野 伸生  
森本 哲也 成田 佳應  
中山 孝明 太田 香 (事務局兼務)  
今井 孝至 (講師支援)

**5. 研修概要**

- 1) システム監査の動向と技法解説
- 2) 演習課題説明
- 3) 監査依頼者の意向確認
- 4) 被監査企業情報の検討
- 5) トップインタビュー
- 6) 監査テーマ設定
- 7) 個別計画作成
- 8) 資料収集検討
- 9) 予備調査準備
- 10) 予備調査
- 11) 予備調査まとめと本調査方針検討
- 12) 本調査準備
- 13) 本調査
- 14) 監査報告書作成
- 15) 被監査部門との事実誤認有無確認
- 16) 監査報告会



(会場：幕張OVTA)

**II. 実務セミナーの特色**

既に会報にて何度も紹介されているかと思いますが、簡単にまとめると次の通りです。

**1. 事例を基にしたケーススタディ**

教材は事例研究会で「普及サービス」として実施した事例を元にして作成されています。

もちろん実際の被監査企業名等はわからないように資料や名称をアレンジしておりますが、事実をベースにした現実味溢れる内容となっております。

さらに講師側が被監査企業の担当に扮し、ロールプレイング形式で予備調査、本調査を体験して頂き、座学のための研修と比べて臨場感を伴った体験を得ることができます。

**2. 監査の一通りを体験**

公認システム監査人制度のみなし経験として申告できるよう、監査の一通りの流れを学んで頂けます。監査依頼者の意向確認から始まり、監査報告会までの流れが4日間に凝縮されています。実践セミナー(2日間)は内容をさらに凝縮し、予備調査準備の段階から体験して頂けるように構成されています。

**3. 受講者同士で監査チームを編成**

実際の監査も複数のメンバーでチームを編成して行われることが多いと思われます。このセミナーでも受講者の方同士で監査チームを編成し課題に取り組んで頂きます。

さまざまな分野で活躍し、経験をお持ちの受講者同士のコミュニケーションもこのセミナーならではの醍醐味といえるでしょう。

### III. セミナー概況

#### 1. FISC 殿と橘和副会長のご参画

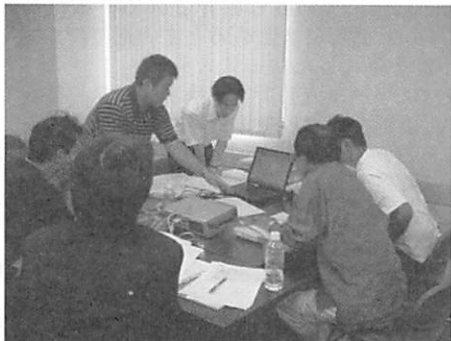
冒頭にご紹介させて頂きましたが、今回は FISC 殿にて発行された「金融機関等のシステム監査指針」をテキストとして使用させて頂きました。そのご縁もあってか FISC 殿より本セミナーのオブザーバーとして合計 4 名のご担当の方々にご参画頂きました。さる方は監査チーム内メンバーとして積極的にご発言され受講者と共にセミナーをご体験して頂けたようです。

また、当協会の橘和副会長も FISC 殿と共にご参画頂き、監査チームの熱い討議に聞き入っておられました。

ご参画頂きました FISC 殿ならびに橘和副会長には大変お疲れ様でした。

#### 2. 演習課題

受講者の方々もそれぞれの分野でご活躍の経験豊富な方々です。ご自身で培われた視点を元にお互いに意見を交換し(ぶつけ合い?)、監査業務は進んでいきます。中でも議論の余地がある課題では、制限時間内に成果物をまとめ上げることはかなり大変な様子でした。



(討議風景：身の入った議論)



(討議風景：プロジェクターを使用して)

#### 3. 監査報告会

演習の最後に被監査企業のトップに監査報告を行う「監査報告会」を行います。監査チームはこの報告会でトップの理解を得るために監査業

務を精魂込めて実施しているわけです。当然説明にも力がこもります。今回の報告会は被監査企業の経営陣も納得のいく内容だったようです。



(監査報告会：経営陣への最終報告)

また、監査報告会終了後、講師より全体講評が行われます。受講者の方々の努力の成果が講師からの高い評価へとつながりました。



(講師講評：中には厳しい指摘も!)

#### 4. 懇親会

当日の研修が終了した後は受講者、講師を交えての懇親会です。仕事の話やら監査の話やら、果ては歴史、哲学に至る話なども。



(懇親会：時の経つのも忘れて...)

中には「演習課題より役に立った」なんていう声もあったとか、なかったとか...



## 5. 受講者の方々の声

先日、受講者の方からのアンケートを集計致しました。システム監査技術者試験に合格されている方が約半数、ITC(ITコーディネータ)にご登録されている方が4分の1、他に公認会計士や技術士、中小企業診断士の方もいらっしゃいました。

やはり「難しかった」という回答が多かったのは「監査テーマの設定」の課題でした。これは実務セミナーを開催するたびに共通しており、実際の監査でも時間を費やした所でもあります。

また、今後は内部統制に関する監査(セミナー)をやりたいというご希望も複数頂き、最新の事例を基にしたセミナーを実施することの重要性を事務局としても認識致しました。

## 6. 新教材を使用して

初めての教材に対して受講者の方々からの反響はどのようなものか、講師他、教材化に参画された方々が気になっていた所でした。「指摘事項に至る情報が不足していないか」、逆に「冗長な内容の資料が多すぎるのではないか」、自問自答しつつも今回の監査報告会での受講者の方々からの報告内容にて、それらはすべて杞憂と化したと感じました。

その反面、資料不足を受講者の方からご指摘を頂き、さらなるブラッシュアップの必要性も感じている次第です。

また、今回は受講者の方々に「金融機関等のシステム監査指針」を通常使用している「システム監査実践マニュアル」に追加する形でご準備頂き、費用面での負担を懸念しておりました。

しかし、当指針の内容の充実度や実務に即した内容が受講者の方に好評だったせいか、アンケートにもその点でのご指摘はありませんでしたので胸をなでおろした心境です。

## IV. 実務セミナーの今後

昨今の監査ニーズである情報セキュリティ監査を事例研究会の「システム監査普及サービス」にて実現でき、なおかつそれをセミナーの教材として会員各位と共有できることは大変有意義なことであると感じております。今後もさらに最新の事例を基にした教材を使用してのセミナーを実施していきたいと考えております。

受講された方々にもセミナーの最後でお願いさせて頂きましたが、会員の皆様からもぜひシステム監査の実施を検討されている企業、団体のご紹介をお願い致します。「システム監査普及サービス」なら通常の監査では費用的に難しいと考えておられる企業、団体等の方々でもご納得できる形で実現できる仕組みを整えております。

当協会のHPの「協会からのお知らせ」に連絡先等記載されておりますので、よろしくお願い致します。

## セミナー体験記

岩下秀樹

私は今春のシステム監査技術者試験に合格したものの、これまでの勉強だけでは腑に落ちない部分が残っており、実践を通して理解することの必要性を感じていました。会社の先輩に相談したところこのセミナーの紹介を受けて早速申込みをしたものです。4日間のプログラムは非常に充実しており、演習を通じた理解力の向上を果ただけでなく、このような実践的セミナーの進め方についても多くを学ぶことができました。それではこのセミナーに対する私の感想をご紹介します。

### ■ システム監査の全プロセスを一通り実践的に演習できる

“監査依頼者の意向確認”から“システム監査報告会”までのプロセスを実践と理論を通して体得できたことが非常に有益でした。まず実践することで疑問点が明確になり、理論補強で理解が一層深まりました。私のような監査未経験者には極めて有効です。

### ■ チーム単位による模擬監査の取組

セミナーでは1チーム4・5名を単位として監査チームを編成します。演習ではこの監査チーム内で意見交換をしながら作業を進めます。様々な経歴を持つメンバーとの意見交換を通して、模擬監査の作業品質を高めることができました。

### ■ 教材の充実度が高い

今回の教材は、(1)「金融機関等のシステム監査指針」(FISC)、(2)情報システム監査実践マニュアル(日本システム監査人協会)、(3)模擬監査用資料、(4)解説用資料、の4種類です。被監査部門の資料やインタビュー結果をFISCの監査指針に照らし合わせながら模擬監査を進める...というスタイルは、他のセミナーと比較して極めて本格的な試みです。このような本格的かつ実践的なセミナーこそ私が求めていたものでした。

### ■ 講師の方々の熱意

私が感嘆したのがこのセミナーに対する講師の方々の熱意です。監査の専門性は勿論のことですが、模擬監査のインタビューとしての参画(臨場感が溢れます)、懇親会の手配(2次会でもお世話になりました)など、4日間のセミナーの効果を高めるための熱意を至るところで感じ取ることができました。この場をお借りして改めて御礼申し上げます。

今回のセミナーで体得した知識やスキルを活かすべく、さらに研鑽を深めたいと考えております。

### 私が「システム監査実務セミナー」から得たもの

情報システム監査株式会社  
齊木 孔二

私がこのセミナーに参加したのは、システム監査人の資格を得ることよりも、システム監査の実務経験を積むことが目的でした。

数ヶ月前に会社のシステム監査事業部門へ異動となり、某金融機関のシステム監査案件に参画しましたが、実務経験がないことの辛さを実感するばかりでした。そこで、私には経験によるノウハウがない分、システム監査の「定石」を学ぶ必要があると考え、会社からの薦めもあって、このセミナーに参加することになりました。

教材については、実例をアレンジして監査対象企業の資料を作成しているためか、調査している実感がわくものでした。現地調査の代わりに施設のフロア地図を使用するなど、さまざまな工夫もされていました。

ロールプレイについては、インタビューを体験する貴重な機会になりました。スタッフの方々と、社長や部長を演じながら質問に答えるのは大変だったと思います。

スケジュールについては、討議や発表の時間が限られているため、チーム内で役割分担して効率よく作業を進める必要があり、かえって「限られた時間内でアウトプットを作成する」訓練になりました。

チーム作業については、作業を進めるうちに、みんなで1つのアウトプット(計画書や報告書)を作成していくという共同作業の中で、自分の果たせる役割を考えることができるようになりました。また、私が所属したチームは優秀な方々ばかりで、さまざまな場面で助けていただきました。

私自身の課題としては、初日の監査テーマ発表を担当した時に、ほぼ資料の棒読みになっていたことなどから、プレゼンテーション能力の向上が大きな課題となりました。同時に、他の方々による発表やインタビューが大いに参考になりました。

冒頭にもありましたとおり、今回のセミナーはシステム監査の「定石」を学ぶ良い機会となりました。このような機会を与えていただいたスタッフの方々に、深くお礼を申し上げます。また、今回のセミナーでは、システム監査という共通項を

持った、さまざまな方々にお会いすることができました。このようなご縁や人脈も、システム監査の実務経験と同様に大切にしたいと考えています。ありがとうございました。

### 法人部会の活動

副会長 小野修一

法人部会は、本協会の法人正会員をメンバーとして活動している部会です。現在、下の一覧表にある34社が法人正会員として登録されています。34社というと、経済産業省が公表している「システム監査企業台帳」登録企業の約1/3に当たります。システム監査を業としている企業の集まりとしては、国内で最大規模といっても過言ではありません。

| 法人名                     | 所在地  |
|-------------------------|------|
| 株式会社 アーク                | 東京都  |
| 有限会社 アイ・エス・ソリューション      | 兵庫県  |
| アイビスジャパン株式会社            | 東京都  |
| 有限会社 アサップ経営システムコンサルティング | 千葉県  |
| あずさ監査法人                 | 東京都  |
| 株式会社 イースティル             | 東京都  |
| 有限会社 インターギデオン           | 東京都  |
| ウッドランド株式会社              | 東京都  |
| エヌ・アイ・コンサルティング株式会社      | 大阪府  |
| NECネクサソリューションズ株式会社      | 東京都  |
| 有限会社 オフィス・あん            | 広島県  |
| 株式会社 管理工学研究所            | 石川県  |
| 共立コンピュータサービス株式会社        | 岐阜県  |
| KPMG ビジネスアシュアランス株式会社    | 東京都  |
| 株式会社 ジーシーシー             | 群馬県  |
| 株式会社 ジェイマック             | 新潟県  |
| システムラボNT                | 神奈川県 |
| 情報システム監査株式会社            | 大阪府  |
| 株式会社 ソフトコム              | 北海道  |
| ダイヤモンドデータ株式会社           | 東京都  |
| T & D 情報システム株式会社        | 埼玉県  |
| 中央青山監査法人                | 東京都  |
| 株式会社 中電シーティーアイ          | 愛知県  |
| 監査法人 トーマツ               | 東京都  |
| 日本システムディベロップメント株式会社     | 大阪府  |
| 日本ユニシス株式会社              | 東京都  |
| ビーエー東京監査法人              | 東京都  |
| 有限会社 ビジネス情報コンサルティング     | 埼玉県  |
| 株式会社 ビジネスソリューション        | 東京都  |
| 株式会社 ビジョンクリエイト          | 大阪府  |

| 法人名                | 所在地 |
|--------------------|-----|
| 株式会社 日立情報システムズ     | 東京都 |
| 株式会社 富士通ラーニングメディア  | 東京都 |
| 前橋システムコンサルティング株式会社 | 千葉県 |
| 有限会社 山口システム監査      | 千葉県 |

この一覧表から分かるように、法人会員企業の所在地は全国に展開しています。この所在地以外にも支店、営業所をもった法人企業も多く、法人会員企業のネットワークは、まさに全国レベルとすることができます。

法人部会の活動の目的は、日本国内にシステム監査を普及させ、システム監査をビジネスとして成立させ、自分たちがそのシステム監査ビジネスの担い手となることです。

わが国のシステム監査の普及状況はまだまだであり、法人会員企業は、企業としてビジネスチャンスの獲得に努めていますが、当協会の法人会員になることによって、法人会員同士が連携・協力することで、新しいビジネスチャンスの発掘を目指しています。

そうしたことを狙いとして昨年度から法人部会で行っている活動が、地方自治体を対象にした情報セキュリティセミナーの企画・実施です。この活動については、すでに会報で何度かご報告していますので、ここでは詳しくは触れないことにします。

法人部会では、原則月1回、定例会を開催しています。仕事で忙しい法人会員企業メンバーですが、月1回集まって、システム監査を何とかビジネスにしたいということで、さまざまな検討や具体的な作業を協力して行っています。最近では、先にも触れた地方自治体向け情報セキュリティセミナーの内容の充実に取り組んでいます。

また、集まった法人会員同士が、システム監査に関連した世の中の動向、それぞれの会社における取組みや苦労談などを、話し合っています。会社の話については、もちろん話せる範囲は限られますが、他の法人会員からアドバイスももらえることもあり、非常に貴重な情報が得られる機会となっています。ときには、定例会の後、懇親会の場に席を移して、話題が盛り上がることもあります。

法人部会では、さらに会員企業を増やし、システム監査の普及活動に努めたいと思っています。それが、結果として、それぞれの企業のビジネス創造になると考え、活動を行っています。

最後に、最近法人正会員となられた2社の方には会社紹介をお書きいただきましたので、ご紹介します。

#### ●T&D情報システム株式会社（北清氏）

T&D情報システム株式会社はT&D保険グループ(太陽生命・大同生命・T&Dフィナンシャル生命)の情報処理会社として、大型汎用コンピュータやオープン系システムを利用し、業務アプリケーションの開発や保守・運用管理、システムインフラの整備、新技術の調査等を中心に業務を行っています。

当社は個人情報の保護に万全を期するとともに、コンピュータ室・建物のセキュリティ管理、安全な建物構造などにより、高い信頼性、安全性を誇るシステムを運用し、平成17年5月にはプライバシーマーク認定を取得しています。

平成17年7月より日本システム監査人協会法人部会に入会し、より専門的な内部監査を実現するために内部監査部門に公認システム監査人を配属しています。

#### ●株式会社イースティル（源口氏）

健全な証券市場を創り維持するためには、信頼性・安全性・効率性を満たした証券情報の流通が不可欠です。イースティルは、証券情報サービスのアウトソーシングおよびASPを中心に事業を営んでいます。

証券情報は、為替や株価等の市況データや市況ニュースといったリアルタイム性のあるデータと、財務データのようなデータベース処理が必要な時系列データが中心です。これらのデータを蓄積・加工・分析して投資判断に有意義な証券情報を生成し、証券市場に流通させるためのシステム・インフラを構築し、サービス全体を運営する事がイースティルの仕事です。証券会社のほか出版業や報道機関等が提供する証券情報サービスの構築・運用、自社データセンターにお客様名義の証券情報サービスを構築して提供するなど、24時間連続稼働の証券情報サービスのシステムを、証券情報の専門知識と自社開発のソフトウェア・エンジンを使って提供しています。

当社では、内部監査の必要性からシステム監査の専門家を育成していますが、監査や各種コンサルティングへのご要望があり、証券業等を中心としたシステム監査を専門家と協働して推進する事業を計画中です。

今後とも、法人部会の活動にご協力をお願いします。

## 第7回システム監査実務セミナー開催案内

システム監査の実際を体験してみませんか!!

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、毎年数回、実践的なセミナーを開催しています。

今回のセミナーは、当協会が既に6回の開催実績を重ねる、「システム監査実務セミナー」(4日間コース 1泊2日×2回)です。このセミナーは、当協会の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て、実践で得たノウハウを皆様と共有することを目標にしています。

システム監査の実際を体験してみたい方や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参加機会のない方は、この機会を利用してシステム監査の実際を経験し、システム監査能力の向上を図りましょう。

なお、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1年間経験したものとみなされます。

本セミナーは、ITコーディネータ協会の「専門知識研修コース」(5.5ポイント相当)及び日本公認会計士協会の「継続的専門研修」(29単位相当)に認定されております。

### 記

- |               |   |                                                                                                                                            |
|---------------|---|--------------------------------------------------------------------------------------------------------------------------------------------|
| 1. 日          | 時 | 平成18年2月4～5日(前半)、平成18年2月11～12日(後半)<br>(前半)第1日目 10:00～20:00 第2日目 9:00～15:00<br>(後半)第1日目 10:00～20:30 第2日目 9:00～15:00                          |
| 2. 場          | 所 | 財団法人 海外職業訓練協会(OVTA)<br>〒261-0021 千葉市美浜区ひび野1-1(JR京葉線 海浜幕張駅 徒歩7分)                                                                            |
| 3. 費          | 用 | 168,000円(宿泊費、食費を含む。会員以外の方は189,000円)<br>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」(2005年11月改訂版)が別途必要となります。<br>(お持ちでない方には、割引価格で販売します)              |
| 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。セミナー用にアレンジした「システム監査依頼書および企業情報」を教材として、3～5名程度のグループにわかれて、トップインタビュー、監査計画書作成、予備調査、本調査、監査報告の実際を体験して頂きます。 |
| 5. 講          | 師 | 事例研究会のシステム監査普及サービス経験者4～6名(予定)<br>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担当                                                                             |
| 6. 問合先及び受講申込先 |   | 日本システム監査人協会 システム監査実務セミナー<br>事務局担当 三輪智哉 E-Mail:t_miwa@strim.or.jp<br>※下記の申込内容を記入の上E-Mailでお申込下さい。                                            |
| 7. 申し込み期限     |   | 平成18(2006)年1月16日(月) <span style="float: right;">以上</span>                                                                                  |

日本システム監査人協会 第7回システム監査実務セミナー参加申込書

月 日

会員区分：SAAJ会員(会員NO. 記載下さい)または非会員

氏 名

資料送付先

住 所 〒 -

自 宅 電話No.

FAX-No.

勤務先 電話No.

FAX-No.

E-MAIL アドレス

システム監査実践/実務セミナーに参加した経験 あり ( 年 月開催 ) / なし

システム監査経験： あり / なし

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」(2005年11月改訂版)をお持ちでない方には、市販価格の2割引で頒布いたしますので、購入申し込み下さい。)

## 新刊紹介

No. 355 岩崎 昭一

SEならこれだけは知っておきたい  
「個人情報保護とリスクマネジメント」  
～体制構築から漏洩時の対応まで～

著者：東京海上日動リスクコンサルティング株式会社  
発行所：ソフト・リサーチ・センター

企業において、個人情報保護法に対する対策を何も検討していないことこそ最大のリスクである。本書は、そのようなリスクの対策に 대응することができる新刊書である。多少とも個人情報保護に関するコンサルティングや監査等に携わる者として、常時携帯しても重くない一書である。その理由は、個人情報保護法に関する内容がコンパクトにまとめられており、説明会や顧客との対応において正確性を求められた場合、索引・用語集として利用することができると思われるからである。また、個人情報の漏洩をリスクマネジメントの観点から、同一書籍の中に含めていることも特徴である。本書の紹介が当協会の会員の活動の一助となれば幸いである。(本書の代表執筆者は、当協会理事の指田朝久氏)

まず、目次は次のとおりである。

- 第1章 個人情報保護の基本
- 第2章 個人情報保護法の理解
- 第3章 個人情報保護体制構築の全体像
- 第4章 個人情報保護対応の課題
- 第5章 個人情報保護の実務
- 第6章 JIS Q 15001 とプライバシーマーク
- 付録 個人情報保護法の全文

## ミニ知識

「オプトインとオプトアウト」  
「定量的評価と定性的評価」  
「個人情報漏洩のリスクカーブ」  
「フレーズの頭文字を取ってパスワードを作成する方法」  
「盗難防止用ワイヤー(セキュリティワイヤー)」

ミニ知識も役に立つと思われる。

第1章「個人情報保護の基本」では、個人情報保護の原則(OECDの8原則)と個人情報保護法のルーツについて解説されている。他の市販本を見ると本書と同一内容をかなりのスペースを割いて解説しているが、本書は、僅か6ページである。要点のみが用語集のようにコンパクトに記されており、個人情報保護の教育研修や説明会に活用することができる。

第2章「個人情報保護法の理解」では、個人情報保護法の内容が法の適用範囲、構成、目的、定義、個人情報取扱事業者等に亘って、民間事業者として必要な部分が抽出され、また、詳細な内容

については、「経済産業省のガイドライン」を引用し、解説している。個人情報保護法を整理して理解するのに役立てることができる。

第3章「個人情報保護体制構築の全体像」では、個人情報保護法を満ちし、個人情報漏洩の発生を防止するために必要な取組みについて、組織整備から個別の対策まで順を追って解説している。個人情報保護のために、自分たちが何をしなければならぬか纏められている。本書を受身の立場(事業者)で捉えると実施に移すことは大変であるが、例えば、コンサルタントやSEとして、顧客に説明する場合には、十分に余る内容が盛込まれている。キーワードを取り上げるだけでも十分な内容である。

第4章「個人情報保護の対応の課題」では、個人情報保護に対する2つの大きな課題である個人情報保護法の要求事項への対応、及び個人情報漏洩の防止について詳しく解説している。前者については、法への対応である関連する各分野のガイドラインが取り上げられ、後者では、個人情報漏洩をリスクと捉えてリスクマネジメントの観点から対策が考察されている。いわば本書のタイトルの後段の目玉である。

リスクマネジメントを理解するのは、大変なことであるが、図解、例示を用いて簡潔に説明している。リスク分析や評価の一部を経験した者には、整理して理解することができる。また、後段では、4つのリスク対策(リスク「保有」、「低減・予防」、「回避」、「移転」)のうちの「リスク移転」について、言及しており、個人情報漏洩賠償金額の算定の考え方が解説されている。(当社においても既に個人情報漏洩保険(通称)に加入しているが興味のあるところである。)

第5章「個人情報保護の実務」では、個人情報保護対応で求められる主な手順(文書)を具体的に解説している。個人情報保護のための各種の手順、文書・様式の事例が解説されており、自社の文書等の雛形として活用すれば、個人情報保護対応を完成させることが可能と思われる。また、コンサルタントやSEとしても、十分活用することができる内容である。

第6章「JIS Q 15001 とプライバシーマーク」では、個人情報保護法とJIS Q 15001との比較について一部述べられている。本書の本来の目的ではないので、本書からプライバシーマーク制度を理解することはできないが、幾つかの相違点について纏められている。

最後に、個人情報保護法、プライバシーマーク制度、リスクマネジメントについて、20冊余の市販本を購入したが、全体の理解が進むにつれてどれも同じであり役に立たなくなってきた。最近では、原本を参照するようにしている。本書は、入門書でないで個人情報保護法に関し、初めての者には難しいかもしれないが、ある程度のレベルの者には、大変役立つものと思われる。本書を一読し、この本1冊とJIS規格本等により、説明

会などに関連資料を沢山持ち運びしなくてもよいと思っている。本書のサブタイトルにあるように、コンサルタントやSEにとっては、必携の書として推薦する次第である。

## 第115回月例研究会報告

No.557 仲 厚吉

日 時：2005年9月27日 18:30～20:30

場 所：中央大学駿河台記念会館 2階会議室

講 師：大阪成蹊大学現代経営情報学部助教授・

公認会計士 石島 隆 氏

演 題：[IT内部統制評価の計画と手続き

ー財務報告に係る内部統制の観点からー]

### 【はじめに】

新会社法が平成17年6月29日に国会可決され平成18年4月施行予定であり、「財務報告に係る内部統制の評価及び監査の基準」の公開草案が出された昨今、システム監査人であれば内部統制システムやIT内部統制とは何かを語れるべきであろう。しかし、今日現在、的確に語れる人は少ないと思われる。

講師の石島先生は、その数少ない人のひとりであり、今回の講演では、「関西のお笑いの会社」の事例を使い、内部統制の基本的要素を分りやすく話された。

研究会会場は、時節柄、聴講する人々で満席の状況であった。

### 【講演目次】

#### 1. IT 内部統制とは何か

- (1) コーポレート・ガバナンスと内部統制との関係財務報告に係る内部統制の評価及び監査の基準（公開草案）
- (2) IT ガバナンスと IT 内部統制との関係
- (3) コーポレート・ガバナンスと IT 内部統制との関係

#### 2. IT 内部統制評価の計画と手続き

- (1) 財務諸表監査における内部統制評価の位置づけ
- (2) 監査要点と IT のコントロール目標との関係
- (3) IT 内部統制評価の実務的実施手順
- (4) 情報システムの概要把握
- (5) 全般統制の評価
- (6) 業務処理統制の評価

### 【講演概要】

#### (IT内部統制とは何か)

システム監査技術者にとってIT内部統制は重要な考え方である。

今回の講演では、財務報告の信頼性の確保を目的とした内部統制及びIT内部統制について説明している。

従来の内部統制概念は、会計統制(①資産の保全、②会計資料の正確性と信頼性の確保)及び経営統制(③経営能率の増進、④経営方針の遵守)の組合せとし、共通に関わるものとして内部牽制(Internal check)及び内部監査を挙げていた。

これに対して、本講演では、新しい内部統制の概念をベースとした「財務報告に係る内部統制の評価及び監査の基準(公開草案)」について解説がなされた。

「財務報告に係る内部統制の評価及び監査の基準(公開草案)2005年7月13日 企業会計審議会内部統制部会」

1. 内部統制の基本的枠組み
2. 財務報告に係る内部統制の評価及び報告
3. 財務報告に係る内部統制の監査

上記1.は、内部統制の基本的枠組みについての解説である。上記2.は、経営者の責任において、財務報告に係る内部統制の評価及び報告を正しく行うこと、また、上記3.は、監査人の責任において、経営者が作成した財務報告に係る内部統制の評価に関する監査を正しく行うことを求めている。

これらの内部統制の評価及び監査の基準は、システム監査基準での管理基準と監査基準に対比して考えるとイメージしやすいと思われる。

なお、上記の公開草案には、コーポレートガバナンスという言葉は出てこないようであるが、講師による講演中の図示により、内部統制が、コーポレートガバナンス及びマネジメントシステムに関係付けられているイメージの説明がなされた。

公開草案においては次のように「内部統制の定義」がなされている。

「内部統制は、基本的に、企業等の4つの目的(①業務の有効性及び効率性、②財務報告の信頼性、③事業活動に関わる法令等の遵守、④資産の保全)の達成のために企業内のすべての者によって遂行されるプロセスであり、6つの基本的要素(①統制環境、②リスクの評価と対応、③統制活動、④情報と伝達、⑤モニタリング、⑥ITの利用)から構成される。」

なお、「⑥ITの利用」について公開草案には、「財務報告の信頼性に関しては、IT環境を度外視しては考えることのできない今日の企業環境を

前提に、財務諸表プロセス自体に組み込まれたIT及び財務報告プロセスに重要な影響を及ぼすITの状況を適切に考慮し、財務報告の信頼性を担保するために必要な内部統制を整備することが必要になる。」

と述べられている。

#### (IT内部統制評価の計画と手続き)

##### (1) 財務諸表監査における内部統制評価の位置づけ

まず、監査の基本概念(委託者、受託者、監査人及び監査に対する監視)、会計情報の質的特性(意思決定有用性)の説明があり、続いて、財務諸表監査について、財務諸表と二重責任の原則(経営者と監査人の責任)の説明があった。

監査人による試査のために、試査の前提となる「母集団の均質性」を保証するのが「内部統制」であり、言い換えれば、財務諸表の信頼性を支える総合的な基盤としての内部統制が要求されることである。

次いで、下記の事項についての説明がなされた。

- (2) 監査要点とITのコントロール目標との関係
- (3) IT内部統制評価の実務的実施手順
- (4) 情報システムの概要把握
- (5) 全般統制の評価
- (6) 業務処理統制の評価

内部統制のうちIT内部統制以外の部分は、手作業の部分であり、財務報告における内部統制は、IT内部統制と手作業による内部統制が統合されたものである。

財務報告の信頼性確保のためのITのコントロール目標として、会計データの信頼性、会計情報システムにおけるプログラムの信頼性及び会計情報システムの可用性が挙げられる。

#### 【さいごに】

講師は、締めくくりとして、2点を挙げている。

- ・ 内部統制の基本的要素としての「ITの利用」は、ITの技術的な側面を考慮しながらも、他の基本的要素と一体のものとして評価するべきである。
- ・ 仕組みの構築と文書化だけではなく、組織のケイパビリティの向上にも目を向けるべきである。

以上を聴講し、私見ではあるが、財務諸表プロセスはどの組織体にも存在していることを考えると、投資家などへの説明責任の一環に、今後、

当協会会員が監査人チームとして内部統制に関わる機会は多くなると思われる。その意味で本日の研究会は基本的な知識を得るための意義のあるものと思う。

#### 第116回月例研究会報告

No.56 藤野 明夫

日時：2005年10月19日(水) 18:30 ~ 20:10  
場所：中央大学駿河台記念館 285号会議室  
講師：監査法人トーマツ エンタープライズ  
リスクサービス部 パートナー  
達脇 恵子 氏  
演題：「CSRと内部監査」

#### ■講演内容

- 1. CSRとその動向
  - 2. CSRと企業内諸活動
  - 3. CSRと内部監査
- ～質疑応答～

##### 1. CSRとその動向

CSRとは、企業の社会的責任 (Corporate Social Responsibility)のことである。欧州委員会の定義によれば、「責任ある行動がビジネスの持続的な成功をもたらすとの観点から、企業やステークホルダーズとの交流の中に、自主的に社会や環境への配慮を組み込むこと」となっている。すなわち持続的な成功、成長(サステナビリティ)のために、目先の利益にとらわれずに、周囲(ステークホルダー)に対して責任ある行動をとることである。

CSRがクローズアップされてきた背景には、①ネット社会の進展(地球の裏側のできごとが瞬時に伝わり、悪いニュースが隠せない)、②環境等への危機感(企業活動の影響力が増大し、環境破壊に直接影響するようになった)、③行き過ぎた資本主義への反省(自己中心的な企業行動が周囲の反発を招く)がある。企業のステークホルダーには、株主・投資家、グループ会社、顧客、取引先、金融機関、政府・政府機関、従業員、労働組合、地域社会、NGO/NPOがあるが、近年、企業は、従来よりも地域社会、NGO/NPO、株主・投資家を重視する傾向が強くなっている。

CSRに対する各国の考え方や動向には特長がある。欧州では、「社会の発展のためには企業は経済以外にも役割を担うべきである」という基本的な考えがあり、これに対して、欧州委員会や各国政府が企業への期待を明示している。米国では、民間主導で、NGO/NPOを始めとする市民の

活動が企業に対し社会的責任を要求する動きが強い。

日本では、環境問題、コンプライアンス(不祥事の多発による)等を出発点に、自主的に取り組みを始める企業が急増している。2004年から従来の「環境報告書」から「サステナビリティ報告書」、「CSR報告書」に発展させる企業が多数でできており、2004年が日本のCSR元年である。また、日本ではリスクマネジメントとしてのCSRという観点が強い。経済産業省の「リスク新時代の内部統制」(注1)には、「環境問題の深刻化、消費者意識の向上、事業の国際化等により、企業の社会的責任は増大しており、広範なステークホルダーに対する企業責任を果たさない場合の社会からのペナルティというかたちでのリスクが増大してきている」と書かれている。

CSRに関する国際基準、ガイドラインには以下のものがある。

- ① コーポレート会議企業行動指針(1994年):「共生」を目指す日米欧企業家の自主行動指針
- ② 国連グローバルコンパクト(2000年):国連による人権、労働、環境等に関する企業の行動原則。これに同意する企業は支持表明と年次報告が必要。
- ③ 持続可能性報告ガイドラインGRIガイドライン(2002):GRI(Global Reporting Initiative)による開示のガイドライン
- ④ AA1000(1998年):英国アカウンタビリティによる、開示プロセスの基準
- ⑤ SA8000(1997年、2001年改訂):米国SAIによる、途上国労働者の保護基準あり。
- ⑥ ISO26000:2008年規格化を目前に検討中。認証を前提としないガイドラインとする案。

表に②グローバル・コンパクトの例を示す(注2)。

## 「グローバル・コンパクト」の10原則

(2004年6月に腐敗防止に関する原則が追加され、現在10原則)

### 人権

原則1. 企業はその影響の及ぶ範囲内で国際的に宣言されている人権の擁護を支持し、尊重する。

原則2. 人権侵害に加担しない。

### 労働

原則3. 組合結成の自由と団体交渉の権利を実効あるものにする。

原則4. あらゆる形態の強制労働を排除する。

原則5. 児童労働を実効的に廃止する。

原則6. 雇用と職業に関する差別を撤廃する。

### 環境

原則7. 環境問題の予防的なアプローチを支持する。

原則8. 環境に関して一層の責任を担うためのイニシアチブをとる。

原則9. 環境にやさしい技術の開発と普及を促進する。

### 腐敗防止

原則10. 強要と賄賂を含むあらゆる形態の腐敗を防止するために取り組む。

表 国連グローバル・コンパクト(注2)の10原則

「財務分析+企業の社会的責任評価(環境対応、社会的責任対応)」により、投資対象会社を決定する社会的責任投資(SRI: Social Responsible Investment)という手法がある。すでにこのSRIにもとづくファンド(SRIファンド)も住友信託などから発行されている。

## 2. CSRと企業内の諸活動

CSRの導入の目的は、それぞれの企業におけるCSRの意義によって定まる。目的の例としては、①経営理念の再確認(松下電器創業者「企業は社会の公器である」等)、②経営活動の再整理、③ブランドの価値向上(資生堂等、多くの企業)、④リスクマネジメントの充実、⑤経営変革のきっかけ、⑥外国人株主の比率向上(に対応した透明性確保)等がある。日本経団連の2005年10月21日の報告「CSR(企業の社会的責任)に関するアンケート調査結果」(注3)の最後の頁によると、CSRを推進するにあたって、「現在も将来(2から3年後)も優先的に取り組んでいる(と思われる)分野」のトップに立ったのは「コンプライアンス・法令遵守」である。また「現在重要な分野」の2番目は「環境」、3番目は「個人情報保護」。



情報セキュリティ」であるが、後者は、「将来」は重要度が低下している。これに反し、「リスクマネジメント」は、「将来」において重要度が増している。

CSRはすべてのステークホルダーの期待を満たす必要があるが、そこには自ずと優先度がある。ジョンソン・アンド・ジョンソンでは、かつて自社の薬品に毒物が混入し死者が出るという大事件が発生した。このとき、ステークホルダーに①顧客、②従業員、③株主という優先度をつけていたので、顧客第一の行動、すなわち、当該薬品の全品回収という行動が俊敏にとれ、逆に同社に対する評価が上がった、ということである。

コンプライアンスはCSRの大前提である。とくに日本の企業においては、コンプライアンスの意義が大きい。しかし、コンプライアンスも単に法令遵守に留まるべきではなく、①法令を遵守した行動、→②社内諸規定、マニュアル等に準拠した行動、→③倫理・社会規範を遵守した行動、→④経営ビジョンに適った行動、というようにより高次のコンプライアンスに発展していくべきである。

また、CSRも、ステークホルダーとの対話を軸にPDCAサイクルを回し、マネジメントシステムとして企業に根付かせる必要がある。今やCSRは、取組み内容だけではなく、その実効性が問われている。さらに、会社単体から、企業グループ、サプライチェーンへと、より広範な企業活動全体の統一的な活動へ展開していかなければならない。

### 3. CSR と内部監査

CSR マネジメントのPDCAサイクルにおける内部監査の役割のひとつは、コンプライアンス等個別テーマ及び、全体のCSRマネジメントの有効性を評価することである。いまひとつは、経営者のアカウンタビリティ(説明責任)において、企業内の活動に関する客観的な情報を経営者に提供することである。

ここで改めて、「内部監査」について考えてみたい。内部監査人協会の定義によれば、「内部監査は、独立した客観的な保証活動とコンサルティング活動であり、これらの活動を通じて、組織運営に付加価値を与え、それを改善する。」となっている。体系的かつ規律あるアプローチにより、①リスク・マネジメントの有効性、②内部統制の品質、③ガバナンスのプロセスの3点を評価・改善することによって、組織目的の達成を支援する。このなかの内部統制とは、基本的に、①財務報告の信頼性、②コンプライアンス、③業務の有効性・効率性、④資産の保全の4つの目的の達成のために、業務に組み込まれ、組織内のすべての者によって遂行されるプロセスをいう。

昨今CSR監査と呼ばれているものの実態を見てみると、①CSRの各テーマの推進状況や活動の有効性に関する監査、②倫理監査(コンプライアンス監査)、③取引先に関する監査(海外の工場における労働環境の監査等)、④ステークホルダーアンケート等を指している場合が多い。取引先の監査の例では、取引先に遵守してもらう規定と監査がセットになっている。たとえばイオンでは、サプライヤーコードオブコンダクトが監査とセットになっている。

システム業界において多い委託業務について触れたい。個人情報保護法では、個人情報に係る委託業務について、委託元に対して委託先を「必要かつ適切に監督」することが義務付けられているが(同法22条)、本条に関する経済産業省のガイドラインでは、この「必要かつ適切な監督」の内容として、委託内容が遵守されていることを定期的に確認することを要求している。

多くの委託元から「定期的確認」を受けることが義務付けられるこのような事態は、委託先にとって大きな負担になる。この問題は個人情報保護法のみならず、委託先まで含めたCSRを実践しようとするれば常に発生する問題である。これに対するひとつの解として、米国監査人協会が策定した監査基準第70号(SAS70)がある。これは独立監査人が、委託先であるサービス機関の内部統制および有効性に関し、意見表明する報告書を受領する指針である。その基準に従って受領される報告書を含めてSAS70という。これによって、サービス機関としては、委託元ごとの監査を受けなくても良くなる。また、委託元監査人にとっては、SAS報告書を検討すれば直接監査に出向く必要がなくなる。

日本においても、上記基準を参考にして、2000年3月に日本公認会計士協会から「業務委託に係る内部統制の有効性評価」が公表された。

### ■ 所感

CSRというたいへん時宜を得た話題を、われわれシステム監査人の立場も踏まえてご説明していただいた。講師はかつてIT業界に身をおかれ、また、公認システム監査人とCISAの資格を持たれているためか、コンプライアンスや内部統制といった専門性の深い内容であるにもかかわらず、受講者にとって、たいへん分かりやすいご講演であった。

講師に深く感謝したい。また、講演内容の性格上、あまり省略すると意味が伝わらなくなってしまうので、いささか長い報告になったことをお詫び申し上げる。

最後に講演中に言及された主な資料の参照先を以下に記す。

(注1)「リスク新時代の内部統制」経済産業省

<<http://www.meti.go.jp/kohosys/press/0004205/1/030627risk-hokokusyo.pdf>>

(注2)「国連グローバル・コンパクト」国際連盟

<<http://www.unic.or.jp/globalcomp/>>

(注3)「CSR(企業の社会的責任)に関するアンケート調査結果」日本経団連

<<http://www.keidanren.or.jp/japanese/policy/2005/066.pdf>>

## 平成17年度第8回理事会議事録 日本システム監査人協会

日 時:平成17年9月14日(水)18:30~20:00

於 :三井物産(株)会議室

出席者: 橋和、富山、鈴木(信)、蓮見、岩崎、指田、金子、吉田、松枝、仲、力、原、梶川(北信越支部長代理)、馬場

### 1. 審議事項

- (1) 平成14年度認定者の認定更新申請案内の件  
平成14年に認定された公認システム監査人・システム監査人補の更新案内について提案され、字句修正などの提案があり修正は事務局に一任することで承認された。

### 2. 報告事項

- (1) 個人情報保護監査研究会(蓮見副会長)  
「個人情報保護管理者/監査責任者の実務」セミナーを下記のように開催する。  
日時 11月12-13日  
後援 (財)日本情報処理開発協会、(社)情報サービス産業協会  
詳細は 後日ホームページに掲載
- (2) 会計担当(蓮見副会長・馬場理事)  
・上期の会計監査は9月18日に協会事務局で実施される。  
・会計業務マニュアルを作成し、交通費・飲食費に対して会計の確認事項を定めた。  
・交通費の請求様式を若干修正した。
- (3) 月例研究会(仲理事)  
・今後の月例研究会の予定  
<9月27日>  
テーマ:「IT内部統制評価の計画と手続き」  
講師:日本システム監査人協会 石島副会長  
場所:中央大学 駿河台記念館  
<10月19日>  
テーマ:「CSRとシステム監査(仮題)」  
講師:監査法人トーマツ  
エンタープライズリスクサービス部  
パートナー 達脇 恵子 氏  
場所:中央大学 駿河台記念館

<11月7日>

テーマ:「電子政府構築に向けた取組みについて」

講師:総務省行政管理局行政情報

システム企画課

課長補佐 澤田 稔一氏

場所:中央大学 駿河台記念館

(4) 北信越支部(梶川北信越支部長代理)

・支部研究会の開催

(9月24日(土) 14:00~17:00)

場所:新潟トークイン

内容:事例発表

「学校教育におけるシステム化と

今後の動向」

発表 新潟県協会長 風間 一人 氏

その他グループ討議など

(5) 事例研究会(松枝理事)

・実践マニュアルの原稿を9/8に入稿した。  
CD部分は9月末に持ち込む予定。

・出版は11/15~20の予定(11月に大阪で開催する実践セミナーに使用)

(6) 情報セキュリティ監査研究会(金子理事)

・実践マニュアルのCDに入れる「情報セキュリティ監査基準のツール」を作成中。

(7) 会報(富山副会長)

・87号は公認システム監査人の特集で10月上旬発行予定。

(8) 事例研究会(吉田理事)

・スモールf社普及サービス、10/7中間報告で12月末までに完了予定。

事例研から9名、東北支部から3名が参加。

・実務セミナー(9/3-4, 9/17-18)を実施中。18名が参加。

・11月27日、28日に近畿支部と共同で実践セミナーを開催予定。

講師は事例研から2名、近畿会から5~6名。

・2006年2月4日-5日、11日-12日に第7回実務セミナーを開催予定。

(9) 法人部会報告(メールで小野副会長)

・新たに2社が法人会員として入会。

T & D 情報システム(株)様

(株)イースティル様

・次回の部会で、今年度の監査企業台帳登録企業への入会案内を発送予定

・自治体向セミナーのコンテンツ見直し中

(10) その他

・システム監査学会・秋季大会を後援する。

以上

議長 橋和尚道  
議事録署名人 馬場孝悦  
岩崎昭一

平成 17 年度第 9 回理事会議事録  
日本システム監査人協会

日 時:平成 17 年 10 月 13 日(木)18:30~20:30

於 :三井物産(株) 会議室

出席者:橘和、鈴木(信)、蓮見、金子、吉田、  
仲、力、桜井、馬場

## 1. 審議事項

- (1) 平成 17 年 7 月末会計中間報告の件  
平成 14 年 7 月末現在の会計中間報告と 9 月 18 日に実施された監事による  
会計監査の結果の報告があり、了承された。

## 2. 報告事項

- (1) 会計担当(蓮見副会長・馬場理事)  
・会計監査の指摘事項実施のため、今後理事に対する交通費などの振り込みは個人口座に切り替える。また、今年度の経費が次年度処理にならないように協力いただきたい。
- (2) 事例研究会(吉田理事)  
・スモールIT普及サービスは 12 月末までに完了予定。  
その次の普及サービス希望会社があれば連絡いただきたい。  
・11 月 27 日、28 日に近畿支部と共同で実践セミナーを開催するが、現時点での参加申込は 5 名。
- (3) 個人情報保護監査研究会(蓮見副会長)  
・「個人情報保護管理者/監査責任者の実務」セミナーを下記のように開催する。  
日時 11 月 12-13 日  
後援 (財)日本情報処理開発協会、  
(社)情報サービス産業協会  
・個人情報保護の出版は JIS の改定が遅れているため、それに合わせて遅くなる見込み。
- (4) HP(桜井理事)  
・NEC のウエーブ・コンポーネント・サービスを利用しているが、オフィス・コンポーネント・サービスに統合される。
- (5) 情報セキュリティ監査研究会(金子理事)  
・「情報セキュリティ監査基準のツール」を使用した情報セキュリティ監査を実施した。半日 2 日で 14 ページの報告書となった。
- (6) 認定事業(鈴木(信) 副会長)  
・公認システム監査人の申請は計 32 名(東京 24、大阪 4、名古屋 3、福岡 1)、システム監査人補の申請は、計 35 名である。
- (7) 月例研究会(仲理事)  
・今後の月例研究会の予定  
<10 月 19 日>

テーマ:「CSR とシステム監査(仮題)」

講師:監査法人トーマツ

エンタープライズリスクサービス部

パートナー 達脇 恵子 氏

場 所:中央大学 駿河台記念館

<11 月 7 日>

テーマ:「電子政府構築に向けた取組みについて」

講師:総務省行政管理局行政情報

システム企画課

課長補佐 澤田 稔一氏

場 所:中央大学 駿河台記念館

## (8) 会報(力理事)

- ・87 号は公認システム監査人の特集で本日送付した。システム監査人からの意見をそのまま掲載したが、この意見に対する回答を次号以降に掲載していく。

## (9) 法人部会報告(メールで小野副会長)

- ・監査企業台帳登録企業で協会未会員の企業あてに、入会案内の DM を発送した。約 90 社。
- ・自治体向けセキュリティセミナーのコンテンツをレビュー中。
- ・次回の会報に法人部会活動を紹介予定。

## (10) システム監査基準研究会(メールで小野副会長)

- ・実践マニュアル改訂  
現在、初校中。11 月 20 日頃の発刊予定。

## (11) 中部支部(メールで大野支部長)

- ・昨年に続き、中国科学院計算技術研究所との交流会を中国上海市で開催する。  
11 月 3 日~6 日で、中部支部から 9 名が参加予定。

## (12) 九州支部(メールで福田支部長)

- ・ITC 大分・日本システム監査人協会九州支部合同セミナーを 11 月 12 日(土)に開催する。  
開催案内を協会ホームページに掲載。

## (13) その他

- ・FISA(情報システム・ユーザ会連盟)システム監査専門委員会によるシステム監査講演会 11/2(水)開催され、SAAJ も後援する。

以上

議長  
議事録署名人

橘和尚道  
馬場孝悦  
吉田裕孝

## 《編集後記》

今号の特集では「情報システム監査実践マニュアル第2版出版記念」「公認システム監査人アンケート意見へのご回答」そして「支部特集」の3つを取り上げました。

特集1については、初版発行時の大変な苦勞が偲ばれ、それがあったからこそ今回の改訂版発行では半年という短期間で全面的な改訂が成し遂げられたのだと思います。関係者の皆さんの努力に敬意を表したい。この通称赤本第2版の利用によりシステム監査のより一層の普及につながることを望みたい。

特集2については普段、協会会員と理事の間でのコミュニケーションがなかなか取りにくい状況のなかで、このような双方向のやり取りの機会が作れたことに意義が有ると言えます。各項目に対し真摯な回答をして下さった各理事の方に謝意を表したい。

特集3については今回は4支部の報告を掲載した。原稿作成のご協力に感謝します。他の支部の活動内容については次の機会に譲りたいと思います。

今年も残りわずかとなりましたが、来年もこの広報の内容を充実させシステム監査の今後の一層の啓発と協会の発展につながるよう努力したい。(T.S.)

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 〒103-0025

東京都中央区日本橋茅場町2-8-8

共同ビル(市場通り)6階65号室

TEL. 03(3666)6341 FAX. 03(3666)6342

事務局メール: [saajjk1@titan.ocn.ne.jp](mailto:saajjk1@titan.ocn.ne.jp)

ホームページ <http://www.saa.or.jp/>

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@yahoo.co.jp](mailto:saaj-kaihoh@yahoo.co.jp)