SAAJ 日本システム監査人協会報

＜特集＞
～システム監査に役立つ情報収集のノウハウ～

皆さんはシステム監査や業務をやっていて「たしかこの情報どこかに」「これに関する法律はなんだっけ」といった時，どうやって探していらっしゃいますか？普段のアンテナ雑誌は？今回は「情報収集」について考えてみました。

内　容：
- 1.1　日本システム監査人協会１２０％活用法
- 1.2　アンケート調査にみる情報収集の方法
- 1.3　インターネットお役立ち情報
- 1.4　情報収集の達人に聞く

1.1 日本システム監査人協会１２０％活用法

皆さん、SAAJ(日本システム監査人協会)を１２０％活用していらっしゃいますか？

SAAJには、この会報だけでなく、さまざまな活動や、意見交換の場があります。経験豊富なシステム監査人やいろいろな業界の会員が集まっていますから、困った時にはまず、相談してみませんか？ここでは、代表的ないくつかの得する使い方を考えてみましょう。

・ML(メーリングリスト)を活用する

皆さんML(メーリングリスト)はもう入っていらっしゃいますか？これはMLアドレス宛に電子メールを送るとリスト上のメンバー全員に送信してくれるため、全員に意見が伝えられるという便利なツールです。「XXについて教えてください。」「XXXの時どうしてますか」「参加者募集」等々、いろんな情報を聞くことが出来ます。気がついたら３つも４つも返事がついていることも。それに、このMLは登録した会員だけのクローズドなMLですから、会員以外に読まれることはありません。MLに登録していない人はさっそく次を参考に登録申し込みしましょう。

なお、新規に登録され、承認された方は、「入りましたよ」という合図を兼ねて自己紹介等の発言をお願いいたします。この時、普段から自分が集めている情報等をアピールしておいてはいかがでしょうか？

特に試験合格を目指す準会員の皆様、恥ずかしがらないで、わからないこと等どんどん質問してはいかがでしょうか？試験対策本の著者も多いこのML。きっと先輩会員からの暖かい応答があるにちがいありません。

会員用メーリングリストの登録方法は次のとおりです。

あて先　Majordomo@mla.nifty.ne.jp
本　文　subscribe saaj
同時に入会承認申請メールを出す必要があります。
あて先　owner-saaj@mla.nifty.ne.jp
題　名　SAAJML承認申請書
本　文　SAAJ会員番号、氏名、会社名、
電話番号、住所、メールアドレス
（ＭＬ事務局(岩崎)）

・月例研究会に出席する

月例研究会の葉書は届いていらっしゃいますか？

年末年始や夏を除き、毎回趣向を凝らしたテーマで一流の講師が最新の情報を教えてくれます。しかも参加費は会場設営等の実費程度。最先端を行く現場の講師に会えるのもこの時、思い切って挨拶してみてはいかがでしょうか。これに出席したくて会社の日程を調整して、わざわざ出張を兼ねて遠くからいらっしゃる方も結構いますよ。

月例研究会は会員外も参加することが出来ます。(会費は異なります)もし、業務に深く関係するテーマなら仕事仲間を誘って参加されてはいかがですか。

「私は遠いからだめだ」なんて思わないで。月例研究会は毎回ビデオが撮影されて、支部に配布されていますので、支部会等で見ることができます。

また、そのうちの一部は送料等の実費負担で貸出しもしていますから、興味のあるものはあきらめないで一度問い合わせてみてはいかが？「こんな内容でやって」「こんな人がいます」リクエストや御意見も募集しています。

ぜひ一度参加してみませんか？

・支部の活動に参加する

とは言え、月例研究会は東京で行われています。

ＳＡＡＪでは中部、近畿、中国、九州の各支部があります。各支部では定例会を開いたり、勉強会や他団体と合同セミナー等も開催したり、積極的な活動を行っていますから、ぜひ一度声をかけてみてはいかがでしょうか？より身近な会員との交流が出来ますよ。最初の参加が難しいという方は協会ＨＰ(ホームページ)でも適宜案内されていますから、セミナー等がある時に合わせて参加されてみてはいかがでしょう？

また、支部の独自のＭＬがあるところもありますから、会場に行けない時でも問い合わせてみて下さい。自分の所属が不明な方、連絡先が知りたい方はＳＡＡＪのＭＬで問いかけるか、事務局まで郵送かＦＡＸでお問い合わせを。

他にもＳＡＡＪでは事例研究会やセキュリティ部会等いろいろな活動が行われています。

これらは会員で興味があれば参加することが可能です。会報やＨＰ(ホームページ)でも案内されていますが，「こんな活動していないの？」「こういう勉強がしたいのですが」等、ＭＬで問いかけてみてはいかがでしょう？最近は電子メールでのやりとりを使い、会合への参加が困難な会員も積極的に参加していますから、自分の興味があるところへは一度お問い合わせ下さい。(募集時期等は各部会の担当者にお問い合わせ下さい)

1.2 アンケート調査にみる情報収集の方法

当協会の理事はボランティア。本業の合間をぬっていろいろな研究会や部会の調整役をしたり、理事会に出席したりしています。それだけでなく、大好きな趣味や家族サービスについても積極的です。

こんな多忙な理事の皆さん、普段どんなふうに情報収集をしているのか、アンケートをしてみました。回答のあった１２名の理事のノウハウをいただいてしまいましょう。

> Q1 日常で情報収集する場合の手段を頻度の多いものから順に３つお教下さい
> (選択肢：新聞・雑誌，本、電話帳，百科事典、図書館、知人等への電話やメール、MLや掲示板や電子会議室、専門機関のDB検索、インターネット、製造元や機関等への直接確認、TVやラジオ、その他(具体的に)

１位　新聞・雑誌(３１ポイント)
(ポイントは１位から３点２点１点)
２位　インターネット(１２)
３位　ＴＶ・ラジオ(１０)
４位　メーリングリスト(７)

> Q2 システム監査に関して情報収集する場合の手段をQ1の選択肢から頻度の多い順に３つお教え下さい

１位　新聞・雑誌(１６)
２位　インターネット(１２)
３位　ＴＶ・ラジオ(１０)
　　セミナー，研究会への参加(１０)
５位　知人(７)

> Q3 システム監査や業務関係で情報収集する内容はどのようなものが多いですか？
> (例：製品(仕様や価格)、法律や規制、事件、試験関連、クライアントの業務関連、事例、用語、会社等)

１位は法律や規則。７名が挙げていました。

２位は新制度や新技術，事例が各６名で続きます。他には用語、試験制度、業務、会社情報、情報システム全般、製品等がありました。

> Q4 システム監査や業務関係でよく読む雑誌を２冊挙げて下さい

一番多かったのは「日経コンピュータ」次は「日経情報ストラテジー」

その他としては日経ビジネス、日経オープンシステム、ジュリスト、月刊企業診断等が続きます。

Q5 システム監査や業務関係でお薦めの本をお教え下さい(当協会発行物も含めて)

これについてはせっかくですので、御推薦のあったまま、全て掲載します。

なお、「情報システム監査実践マニュアル」は複数の方の推薦がありました。

＜記入に従いそのまま列挙＞

「著作権法」
　斎藤　博　有斐閣
「暗号」
　辻井　重雄　講談社
「金融機関等のシステム監査指針」
　FISC
「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工業調査会
「インターネット取引は安全か」
　五味　俊夫　文春新書
「図解　経営情報化１００の誤解」
「セキュリティハンドブック１，２，３」
　日科技連
「システム監査試験合格完全対策」
「システム監査基準解説書」
「監査理論の基礎」
　鳥羽　至英
「セキュリティハンドブックⅠ，Ⅱ，Ⅲ」
セキュリティマネジメント学会
「システム監査Ｑ＆Ａ」
「ＩＴマネジメント」
　ハーバード・ビジネス・レビュー編
　ダイアモンド社
「システムの運用と管理」

Q6 iモード等の携帯電話を使用したインターネット情報を活用していますか？
1よく利用する　2たまに利用する
3利用しない、持っていない

「3　利用しない，持っていない」が１１名、
「1　よく利用する」が１名でした。

インターネットについては次の章でご紹介します。

1.3 インターネットお役立ち情報

ここでは，アンケートで紹介されたインターネットのサイトをご紹介します。

Q7 日頃よく情報収集時に活用するサイトを教えてください。どんな時に活用するか教えてください。

- ご存じ「首相官邸」www.kentei.go.jp
- 検索といえば，「ヤフー」www.yahoo.co.jp「インフォシーク」http://www.infoseek.co.jp/)があります。
- 「ITSSP」
- 「通産省」は官邸からリンクで行くことが出来ます。
- 「野口悠紀夫のホームページ」「自社」を挙げる方も。　「日経ＢＰ」(ｈｔｔｐ：//itpro.nikkeibp.co.jp/)を挙げる方も何名かいらっしゃいました。

・幹事さんはこちら
ぐるなび　http://gnavi.joy.ne.jp/kanto/
・目的地に行くなら
乗り換え案内　http://ekimae2.toshiba.co.jp/
というご案内もありました。

Q8 システム監査や業務関係に役立つお薦めサイトを教えてください。

・特に多かったのは、各省庁のＨＰです。いろいろな規定等で利用されているそう。（通産省金融庁）関係団体JIPDEC,JISA,IPAにもよく立ち寄っているようですね。
・社内という人も。
・日経BP(http://itpro.nikkeibp.co.jp/)
・マーケット情報
http://www.watch.impress.co.jp/pc/
・価格.com
http://www.kakaku.com/ がこれに続いています。

1.4 情報収集の達人に聞く

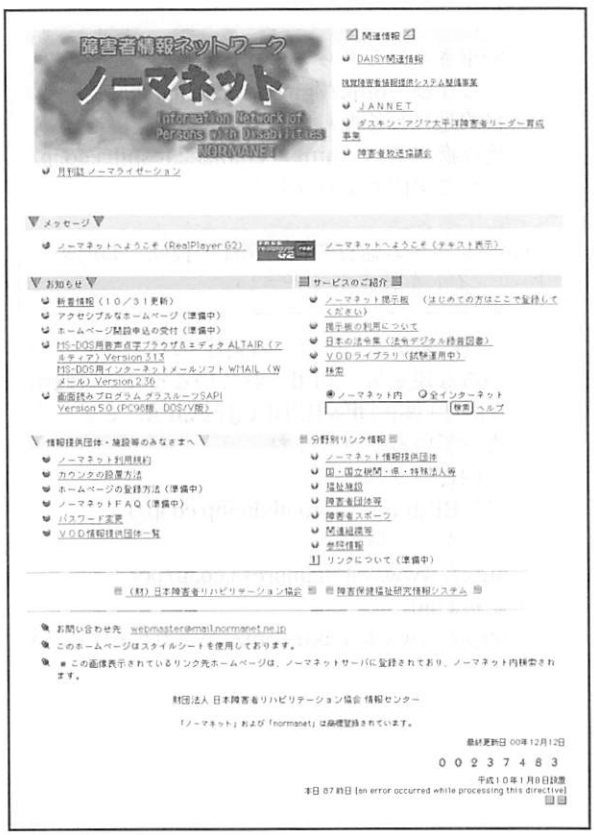
アンケートのＱ９は「情報収集の達人」をご紹介下さい。というものでした。

システム監査人協会関係で挙がったので一番の情報収集の達人と思われているのは荒川副会長。他いろいろな方が挙がりました。今回はその中のお一人、清水氏にお薦めのＨＰをご紹介いただきました。なお、氏は最近日本システムアナリスト協会も設立され、多忙な毎日をお過ごしです。御多忙の中での紹介ありがとうございました。

会員の薦めるＨＰ

Ｎｏ．１２８　清水　順夫

障害者情報ネットワーク　ノーマネット
http://www.normanet.ne.jp/



前回の会報で、原善一郎さんに、私のページをご紹介いただいた清水順夫です。そこからのリレーというわけでもないのですが、２ヶ月ほど前に大変有り難かったＨＰがあり、今回の特集が「情報収集のノウハウ」ということでもありますので、ご紹介します。

本や雑誌の執筆をするときの情報源として、ＷＥＢは貴重です。その気になれば、けっこういろんなものが見つかります。このページもそんな仕事の中で見つけてきたものです。

このページの本来の趣旨とは違うかもしれませんが、ここのサービスの中に「日本の法令集(法令デジタル録音図書)」というコーナーがあり、ほとんどの法令の全条文が掲載されています。情報技術関係だと、あちこちに情報があるのですが、法令の情報はあまりありません。このページは、みなさんがあまり知らないような法律、たとえば、家畜改良増殖法などというのまで掲載されているのです。

２ヶ月ほど前、中小企業診断士の試験科目変更により新設となった、「経営法務」という科目の教材を書いたのですが、民法、商法から、知的所有権関連、会社更正など、いろんな分野の法律の条文を確認する必要がありました。そこで、このページに大変お世話になった次第です。

システム監査についても、契約や知的所有権など参照すべき法令は多いと思います。古い六法全書よりは遙かに価値の高い資料ですので一度ご覧ください。

今回の特集，いかがでしたか？

最後に理事の方からの「情報収集」に関するアドバイスを。

・ＳＡＡＪの月例会に出席すること

・収集も大事ですが，整理(廃棄も含めて)と活用ですね。自分も十分にはできていませんが

・好奇心

・世の中全てがインターネットの時代になります。(中略)

インターネットの活用技術が全てを決定すると思います。

・メールニュース等をこまめにチェックするのが良いかも

・たいしてありませんが，日頃のつきあいを大切にしておくことでしょうか

・検索のキーワードの設定に工夫が必要

平成12年度システム監査講演会

日　時：平成12年10月4日
場　所：東京有楽町よみうりホール
主　催：ＥＤＰユーザー団体連合会
後　援：日本システム監査人協会他

例年の情報化月間参加行事として、ＥＤＰユーザ団体連合会主催のシステム監査講演会が行われました。講演会は当協会も後援しており、今年の参加人数は６５０人余りと多く、盛会でした。冒頭にユーザー団体連合会会長長谷川氏による開会の辞のあと、通産省機械情報産業局情報セキュリティ政策室の山本課長補佐から来賓挨拶がありました。

当会からは、荒川副会長が最初に講演を行い、午後に安本副会長が監査事例発表をされました。他に事例が２件発表され、非常に有意義な講演会でした。最後に同連合会システム監査専門委員長を務めている当会理事の木村氏が閉会挨拶をされました。

以下に講演要旨を紹介します。

講演１．国際セキュリティ評価基準

ＩＳＯ１５４０８の概要
ーその企業に与えるインパクトー
講　師：株式会社アーク
　　代表取締役 荒川　幸式　氏

国際セキュリティ評価基準であるＩＳＯ１５４０８の概要について、およびこの基準の実施によって予想されるビジネスへの影響と認証制度、審査のポイントなどを説明された。

ＩＳＯ１５４０８の概要については、会報５８号の第72回研究会報告であらまし載っているのでここでは省略するが、予想されるビジネスへの影響、特に、セキュリティ基本設計書の作成手順、ＩＳＯ１５４０８の審査対象物、評価保証レベル(EAL)別の審査概要、ＥＡＬとセキュリティ強度、などは実際にこの仕事に携わっておられる講師の具体的な説明で興味深かった。

講演２．宇治市の個人情報保護についてのシステム監査から

ー地方公共団体のシステム監査取り組み事例報告
講　師：情報システム監査株式会社
　　システム監査部
　　参　与　　安本　哲之助　氏

地方公共団体のシステム監査事例について発表された。これは会報６０号第76回研究会報告に載せられている事例と同じです。(詳細内容は会報をご参照下さい。) 講演では、さらに、これからの課題として、次のような問題提起をされました。

①電子政府の整備加速化に対し、IT投資の有効性評価が重要視される
②市民サービス、市民意見の取り入れにインターネット利用も視野に入ってくる
③地方自治体のコンピュータセキュリティ基準の改定とセキュリティのレベルアップに対し安全性・信頼性評価がますます必要となる。

これに対し、外部からの評価の重要性が高まるので、評価の専門性、評価の客観性を高めるとともに、情報公開条例により監査報告書も公開の対象となることを留意する必要がある。

講演３．グローバル経営を目指した情報システムの内部統制

講　師：
マツダ株式会社情報システム本部 システム企画統括部システム統制・業務チーム
主　幹　　加島　秀郎　氏

同社は、外資提携以来国際的視野での経営環境整備を進めてきた。情報システムもフォードのグローバルネットワークと繋がり、ビジネスとシステムの緊密化を受けて情報戦略(ＩＴ Governance)強化が必要となってきた。

そこでシステム内部統制の導入活動を開始し、その一環として業務標準の整備を行った。その結果として実現できたことは

・職責分離、統制仕組みの全社展開
・セキュリティ意識の浸透
・標準／基準、文書管理の定着
・当社のシステム統制レベルの把握
・関連企業へ水平展開の基盤
・データ・センターの災害時復旧対策の導入
・システム内部統制整備の長期シナリオの策定

などである。これは、監査法人と外資親企業の業務監査を迎えるための整備であったが、監査の所感として、共通の目標設定と相互の適切

な補完の維持がシステム内部統制の成功につながる。すなわち、業務部門は業務実態を熟知し、改善仕方を知っている、効率から見た改善の優先度を知っているのに対し、監査部門は基準を熟知し、順守すべき規準の優先度を知る、社内部門間／企業間の到達バランスを知る。そこから、順守すべき規準の公開、業務部門による自己統制、経営効率と基準順守のバランス化／計画的な改善実施につながる協力関係が出来る。

まとめとして、システム内部統制の整備は業務の効率化に貢献するとともに、ビジネスのグローバル化やＥ－ビジネスの推進のために避けて通れない。整備には多大の投資を伴うが先行投資的な面を含むと共にプロセス改善による効率向上や顧客の信用向上などから必須のものである。監査部門にはその実現の支援を期待している。

講演４．

日本生命保険相互会社におけるシステム監査事例とシステム監査人の課題

講　師：
日本生命保険相互会社　検査部
検査役　　片岡　学　氏

１．システム監査の実施体制

システム監査人は、検査部(８４名)内の本部検査チームに、公認情報システム監査人２名が担当している。基本方針として「銀行と同レベルのコントロールの確立」を掲げ、準拠する基準は、ＦＩＳＣのシステム監査指針に拠っている。

２．監査対象システム

情報システム関連部門および分社した情報システム子会社である。システム子会社に対しては、システム監査に関する条項を盛り込んだ基本契約書を締結している。２つのコンピュータセンター、ホスト系４９システム、EUC系約４００システムあり、これを部門別監査、業務システム別監査、テーマ別監査に仕分けて実施している。

３．監査実施例

今回は、外部委託業務の監査として、開発委託に関する監査、運用委託に関する監査を事例として説明された。

以上の事例説明の後、金融検査環境の変化、ＦＩＳＣの動きに触れ、今後のシステム監査に求められるものとして

・企業内の内部統制システムの重要サブシステムとして経営のマネジメントシステムにくみこまれること

・システム監査は第一義的には内部監査部門の役割であるとの認識を経営・内部監査部門と共有すること

・会計監査人・監査役監査との相互協力体制の確立

・急激に変化する情報処理環境に対応したシステムリスク管理への適切な対応の実現

・金融検査対応 等などがある。

最後に、システム監査の更なる充実に向けて、経営層への更なる・不断の働きかけ、システム監査人としての更なるスキルアップ、システム監査人の分業化(外部の専門業者)検討、他の監査領域との連携強化、準拠性から有効性へ、システム監査の有効性を常に意識しアピールできるものにすること、などを提言された。

以　上

第76回研究会報告

日時：平成12年9月21日(木)18：30～20：30
場所：労働スクエア東京 704号室
講師：情報システム監査株式会社
システム監査部参与 安本 哲之助 氏
演題：地方公共団体のシステム監査の取り組み事例報告
(宇治市の個人情報保護についてのシステム監査から)

NO.792 前橋 雅夫

講演要旨

１．システム監査の概要

昨年５月、宇治市の住民情報２１万件がホームページで販売されるという事件が発生した。この事件の後、宇治市より個人情報保護についてのシステム監査の公募があり、８社からの応募があったが当社が落札した。

依頼者側のシステム監査要件は「システム監査業務仕様書」というかたちでまとめられており、それには、監査範囲は電子データだけでなく手書きの情報も含めた事務システム全般であること、個人情報流出防止策を技術面、設備面、組織・機構、要員体制、委任契約のあり方の観点

から提言してもらいたいことが指定されていた。

監査基準は、自治省の「地方公共団体コンピュータセキュリティ対策基準」を中心として、通産省の「情報システム安全対策基準」「システム監査基準」、宇治市の「個人情報保護条例」「個人情報取扱事務登録制度」を使用し、監査項目は、運用業務に関する基準の準拠性、共通業務(要員管理、外部委託)に関する基準の準拠性の2項目とした。

2．システム監査の実施要領

今回のシステム監査は、平成11年12月までの「本調査」と、平成12年3月までの「追加調査・フォロー監査」という2段階に分けて実施した。監査を2段階に分けた理由は、問題に対して一刻も早く改善に着手したいという依頼者側の意向があったことと、平成12年度予算に対策関連費用を盛り込みたかったことの2点によるものである。

3．本調査

本調査は次のような手順で実施した。

(1) 事前準備
- ・資料の収集
- ・アンケートの作成、配布、回収、分析
- ・調書の作成

(2) 本調査
- ・インタビュー
- ・職場視察

(3) 調査結果の検討
(4) システム監査結果中間報告書の作成
(5) システム監査コンサルティングレポートの作成(第1次分)
(6) 意見交換会
(7) 報告書提出
- ・システム監査結果中間報告書
- ・システム監査コンサルティングレポート

(システム監査結果中間報告書に基づく第1次改善事項)

報告書はセキュリティを考慮して、総合編と詳細編の2種類に書き分けた。「宇治市情報公開条例」では「システム監査結果報告書」は公開対象になっている。そのため、セキュリティの弱点や具体的な場所や内容を特定できないような記述に止めた総合編を公開対象とし、問題点を全て記述した詳細編については、市民の情報資産の安全性を損なうものとして非公開にした。

コンサルティングレポートでは、パソコン利用環境の再構築に関する提案、中間報告書に基づく改善提案とその実施に関する見積り金額提示などの内容について報告した。

4．追加調査・フォロー監査

追加調査・フォロー監査は次のような手順で実施した。

(1) 追加調査の準備
- ・追加アンケート作成(改善定着状況確認)

(2) 追加調査(フォローと実査未着手領域の追加実施)
- ・重要諸規程の精査
- ・追加インタビュー
- ・個人情報取扱事務登録簿の視察
- ・書庫の視察
- ・フォローアップ監査

(3) 追加調査結果の検討会
(4) システム監査結果最終報告書の作成
(5) システム監査コンサルティングレポートの作成
(6) 意見交換会
(7) 報告書提出
- ・システム監査結果最終報告書
- ・システム監査コンサルティングレポート

(システム監査結果最終報告書に基づく第1次改善事項)

最終報告書と中間報告書との違いは、フォローアップ監査にて改善が確認された項目は指摘事項から取り除いていること、中間報告書提出後の取り組み状況について記述していることなどの点で異なっている。

コンサルティングレポートでは、セキュリティポリシー策定に向けての提案、中間報告書で提案したセキュリティ対策製品とその後に発売されたWindows2000のセキュリティ機能の比較検討情報を追加した。

5．改善事項

改善事項は、平成12年度中に改善が望まれる第1次改善事項と、将来的に改善が望まれる第2次改善事項とに分けて報告した。

第1次改善事項では、以下のポイントについて指摘した。

(1) 組織・規定の整備	セキュリティ関係
(2) 運用管理	パスワード
(3) 入力管理	入力時チェック
(4) データ管理	複写
(5) 出力管理	出力管理規定

(6) ソフトウェア管理	ソフトウェア管理規定
(7) ハードウェア管理	パソコンの保管管理
(8) ネットワーク管理	ネットワーク管理規定
(9) 保守業務	変更履歴
(10)ドキュメント管理	作成基準
(11)要員管理	セキュリティ教育
(12)外部委託	作業者の明確化
(13)システム監査	継続的な監査

第２次改善事項では、以下のポイントについて指摘した。

(1) 運用管理	アクセス分析
(2) データ管理	暗号化
(3) 建物・関連設備管理	耐火金庫
(4) ドキュメント管理	ドキュメント整備

６．これからの課題

ＩＴ革命により電子政府の整備が加速化し、市民サービスや市民意見の取り入れにインターネット利用が視野に入ってきている今日、自治体のコンピュータセキュリティ基準の改定とセキュリティのレベルアップは必須である。このような背景のもと、今回のシステム監査のような外部からの評価の重要性は、ますます高まっていくものと思われる。その際に、評価の専門性、評価の客観性がポイントとなってくる。今回、我々は上記のような改善指摘をしたが、他の監査会社が監査しても同じような報告になるのか、この点についての検討が必要ではないかと考えている。

質疑応答

Q1. 外部委託についてはどのような指摘をおこなったのか。

A1. 今回の事件は、開発テストで本番データを使用していたものが、アルバイトから漏れたという経緯がある。具体的には再委託禁止等の指摘を行った。

Q2. 他の自治体に与えたインパクトはどのようなものか。

A2. 他の自治体からもシステム監査の引合いはきている。自治体側も「何もしないでいて何かあったら...」という危機感がでてきているのだろう。また、この８月２８日に自治省からだされた「ＩＴ革命に対応した地方公共団体における情報化施策等の推進に関する指針」により、システム監査にとってはフォローの風が吹き始めている。

Q3. 今後はシステム監査でコンサルティングまで求められてくるのか。

A3. 組織体のＩＴ体力によって違ってくるのではないか。自己革新的組織に対しては問題指摘だけでよいと思うが、それが充分でない組織に対しては具体的な対策まで求められるであろう。

Q4. システム監査の結果、個人情報保護のレベルは上がったのか。

A4. 徐々に改善してきている。アクセス分析と暗号化が実現するまでは完全とはいえないが、レベルは格段に上がってきている。

第７７回研究会報告

日時：平成１２年１０月２７日
場所：労働スクエア東京
演題：「金融機関等のシステム監査について
～システム監査指針改訂を通して～」
講師：(財)金融情報システムセンター
監査安全部研究員　山田　巌 氏

No526 富山伸夫

講演要旨

Ⅰ．ＦＩＳＣの活動紹介

ＦＩＳＣ(The Center for Financial Information Systems)は財団法人金融情報システムセンターの略称で、昭和５９年設立、金融機関、保険会社、証券会社、コンピュータメーカ、監査法人等の８５１機関を会員とするシンクタンクである。

職員は４９名、大半は会員企業からの出向者であり、金融情報システムの安全性確保、業務推進における情報システムの効果的活用等の重要な問題について調査・研究、必要に応じて、指針の提示、その他の提言を行うことを目的としている。

最近の活動として

* 金融機関等における個人データ保護のための取扱指針(Ｈ１１．４改訂)
* 金融機関等コンピュータシステムの安全対策基準(Ｈ１２．７改訂)
* 金融機関等のシステム監査指針(Ｈ１２．７改訂)

などを提示する他、「統合的リスク管理研究会」「電子決済研究会」「金融ＥＤＩ、貿易金融ＥＤＩ研究会」などを行っている。

Ⅱ．金融機関等のシステム監査

一般的に、金融機関等では、検査部という部門に、情報システムを専門的に監査するセクション(あるいは人)を配置するケースが多いが、監査人の数では大手行で１０名程度、その他では１～２名というところが多い。

検査と監査の違いについては、検査が定められた規定・マニュアルへの準拠性の側面が強いのに対し、監査は準拠性に加え、規定・マニュアルそのものを含めリスクがコントロール出来ているかを評価するところがある。

金融機関等のシステム監査は、情報システムの規模と役割が肥大化してくるなかで、データのインテグリティやコンピュータシステムの健全な運営という視点に留まらず、情報システム戦略の達成やリスク管理の実践といった視点にまで進化してきている。

リスクをコントロールする具体的な仕組みが内部統制システムであって、これの枠組みとしてＣＯＳＯレポートによる５つの構成要素がある。この５つの要素には、

１)統制環境、２)リスクの評価、３)統制活動、情報と伝達、５)監視活動、があって、指針作成のバックボーンとなっている。

金融機関等のシステム監査環境は、市場環境の変化、金融監督行政の変化を受けて大きく変わってきた。

Ⅲ．「金融機関等のシステム監査指針」について

・改訂の経緯とポイント

平成１０年より「新しい金融環境におけるシステム監査研究会」発足させ、指針改訂を睨んだ論点整理を行い、具体的な改訂作業は、平成11年7月より着手した。そして、平成１２年７月に「システム監査指針(改訂版)」を出版した。

改訂のポイントとしては、システム監査に関わる当事者の役割と責任を明確にすること、情報システムにリスクとコントロールという概念を導入し、システム監査の機能を定義した。また、本指針の位置付けとしては、基準ではなく指針(ガイドライン)であるので、監査実施のための参考書として使われるべきものとしている。

・システム監査の定義

「金融機関等のシステム監査とは、情報システムの有効性、効率性、信頼性、順守性及び安全性の達成を妨げようとする情報システムリスクの管理体制が適切かつ効果的であるかを、監査対象から組織的に独立したシステム監査人が把握、評価し、その結果を経営者に報告するものである。」

・ 情報システムの目的と情報システムリスク(省略)
・ 情報システムのコントロール目標(省略)
・ システム監査の対象領域は殆んど全社・全階層
・ システム監査の種類(省略)
・ 実施体制

システム監査人の独立性を確保し、ＩＴに通じたシステム監査人を確保することが必要として、システム監査人に求められる資質として、①ビジネス能力、②公正不偏な判断と職務上の秘密の厳守、③専門知識とスキル(監査技術、ＩＴ、監査対象業務)を挙げている。

・ 実施手順は、次のように設定している

経営者からの指示

1 st Step

リスクの識別、評価(何がリスクなのか？)

2 nd Step

チェックポイント設定(何を診ればよいか？)

3 rd Step 監査実施(証拠、テスト)

4 th Step

チェックポイントの判定(従前の検査はここで終わっていたのではないか)

5th Step

リスクのコントロール状況の評価
(最終的にここにたどりついて監査となるのではないか)

経営者への報告(監査報告書の提出)

・チェックポイント集

１３の要点項目が、６０の大項目に分かれ、さらに１７６の小項目に分けて、１０２２のチェックポイントの構成となっている。

一般的なリスクを想定してのものなので、大方の監査実施の際には掘り下げブレークダウンが必要であるが、そこは、各金融機関の情報システムの規模や運営形態、また監査人の力量による部分も大きいのではないかと感じて次第である。

Ⅳ．今後の課題

海外の動向調査や、金融庁での「金融機関などにおける実効性のある内部監査・外部監査体制の確立に向けて」といったワーキンググループの立上げなど、を睨んで今後継続的に改訂のスキーム構築や情報収集の仕組み作り、リスクの評価や計量化方法の研究が必要で、ＩＳＡＣＡ，内部監査人協会、システム監査人協会などとの繋がりを持ってゆきたい。

質疑

Q：システム監査人の資質・専門能力はどこまで拡充が必要か
A：内部監査が前提となるが、どこまでを求めるかは個々の金融機関の課題と考える。
Q：システムリスクの評価は情報システム部門の役割と思うが
A：監査部門はリスクのコントロール状況を評価するうえで、独自のメジャーを持つべきではないかと考える。(勿論、被監査部門のリスク評価の内容を評価し、それを是とするのであれば、使うことも可能と思う。)
Q：関連会社監査の根拠形成はどうする
A：外部委託契約に監査の権利を盛り込むような形を考えている。
Q：取締役を監査の対象外とするのは奇異な感じがする
A：監査部門が、欧米では経営ボードの監査委員会に属するのに対し、日本では1ライン組織になっているので、経営者の意思決定そのものは内部監査の対象領域ではないと考えている。
Q：「金融機関等のシステム監査指針」をＦＩＳＣ会員外が入手できるか
A：会員には1部無償配布、余部1万円。会員外は1部2万円で出せる。
詳しくは、ホームページ
http://www.fisc.or.jpにて
Q：「指針」の位置付けは
A：金融機関等における有益なシステム監査実施のための参考書である。
Q：金融監督庁の参画や同庁「検査マニュアル」との関係は
A：金融庁はオブザーバーとして、作業部会そのものには出席された。但し、本指針が、即「金融検査マニュアル」対応という捉え方は、FISCとしては考えていない。
Q：リスクの識別評価が難しいと思うが、なにかガイドがあるか
A：銀行により千差万別で難しい。(強いてあげるとすれば)棚卸的な網羅的な洗出し等が具体的な方法としては考えられるのではないか。
Q：日米で意識差はあるか
A：FISCとしても今後の研究課題と考えている。具体的には、今年の１１月に海外調査を計画している。

(感想)ここ２～３年、金融業界の激変には驚き放しであるが、金融検査、内部監査、内部統制、システム監査などの動向をしっかり受け止めて、指針改訂につなげて来られたＦＩＳＣのご努力に感服しました。必要に迫られてのことでしょうが、システム監査の世界で一歩先に出た感じで、これからも実践例などをお聞きしたいものです。

近畿支部特別寄稿

「逆もまた真なり」

Ｎｏ．７０７　神尾博

今夏は世界最大の墳墓である仁徳天皇陵の特別参拝がおこなわれた。

通常は、第３堤(一番外側の濠、仁徳陵には３濠ある)、そして第２堤までしか見られないが、私が訪れた日には、白熱の陽光を浴びた高温の砂利を踏んで第２堤の内側まで入り、鳥居の向こうの第１濠も拝観出来た。

近辺には仁徳陵以外にも古代の古墳群が点在しており、航空写真でこれらを探し出すことはたやすい。コンクリート製のビル群やアスファルトで舗装された道路等の、白やグレー系の色が多い中では古墳の緑色がひときわ目立つからだ。

全体が木々や雑草に覆われている古墳は、宅地化・都市化に対する緑地の防波堤的役割を果たしている存在とも言えよう。事実、ランドサットから大阪市の地表温度を調べてみると、川や池、そして緑地は相対的に温度が低かったという結果が得られている。堺市の仁徳陵の辺りでも同様の傾向であろう事はまず間違いない。

ところが、これらの古墳の建設当時の風貌は、現在の様子と大きく異なっていたらしい。当時は灰白色の石が敷き詰められ、赤茶色の土器や埴輪でふちどりがなされていたと言う。古墳の回りは自然が豊かでほとんど緑１色だったから、すこぶる人目を引く存在だったであろう。

何とも面白いことに、古代人が目にした「緑のベース(地)にセラミックのアクセント」は、現在の「セラミックのベースに緑のアクセント」と正反対の関係にある。すなわち、ビット演算で言うところの反転処理(riverse)、いわば「00010000」から「11101111」への変化である。

完全無欠な対称に見えるこれら二つのビット

列にも、ひとつの共通点がある。

「１個だけが他の７個と違う」という点だ。古墳においても同様、古代・現代を通じて周囲から引き立つ存在であること自体には変わりがない。

われわれビジネスマンやエンジニアは、ややもすると世の中の変化にばかり目が行きがちである。しかし「何が変わるか」だけではなく「何が変わらないか」の見極めも大切なのではないか。むしろ「何が変わらないか」を見極めることが、「何がどう変わっていくか」を見通すための近道ではないか。

企業にしても「変わらない」部分こそが安定事業となり得る。あるいは技術者の能力にしても、バックボーンがしっかりしていなければ急激な変化への対応は難しいだろう。などといった考えが暑気で朦朧とした脳裏をよぎった。

ところで、ひょっとすると古代人は未来におけるセラミック色からの反転を見越して、緑のタイムカプセルを現代人に託してくれたのかも知れぬ。しかしながら、彼らの未来への想いは永遠に時空の彼方を漂う謎である。

中国支部便り

No.３８７　安原節男

毎年のことながら、過ぎてしまうと早いもので、今年も残り一月半となりました。

今年の中国支部の活動をまとめてみました。

※近畿会、システム監査普及サービスの「Ｃプロジェクト」に参加。今年２月から６月まで小生と藤原会員が参加して貴重な経験をさせていただきました。外部監査として、予備調査から監査結果報告までの、一連の作業を実施できる機会はなかなか得られません。

※システム監査実践セミナー、大阪コースへの参加。関西では初めての「システム監査実践セミナー」が大阪市内で５月中旬に開催され、

当支部から藤原、西村両会員が参加されました。

※広島西南ロータリークラブで「システム監査」についての卓話。８月下旬、小生が約３０分間でしたが、卓話のお時間をいただきました。

なお、当支部の桑原副支部長(公認会計士)が同クラブのメンバーであることから実現しました。

※「電子認証・電子公証の関連動向と今後の展望」研修会の実施。当支部としては初めての本部から講師(本部理事、三谷慶一郎氏)を招聘しての研修会を９月８日に広島市内で開催しました。

参加者は約４０名、会員の参加は数名でしたが、一般募集を行ったこともあり、まずまずの参加者数となりました。

※おわりに、当支部の会員動向ですが、今年は、平さん・日名さん・新田さんの３名の入会をえて、総会員数は２４名となりました。内訳をみると、岡山３・広島１１・鳥取１・島根３・愛媛１・香川４・高知１と広範囲に亘っています。

以上

中部支部合宿セミナー企画

No.124 原　善一郎

中部支部は恒例のセミナーを一般公募もして、実施しました。

募集のときには次の通りに意気込んでおります。

実施報告は次号でお知らせします。

<セミナー募集要項>

情報化に関するプレゼンテーション能力向上セミナー開催について

日本システム監査人協会中部支部

情報化技術(ＩＴ)の進歩は政治・経済・行政或いは文化等、社会の隅々迄にその影響を及ぼしています。これはまさしくＩＴ革命といってもよいでしょう。技術の進歩はそれを利用し、活用するのは組織であり人であります。

組織体にあっては、ＩＴを利用した仕組みが組織を効率的に働かすことを認識し実施にいたるまでには多くコミュニケーションが行われます。

特に決裁権限者の理解を得るための説明はＩＴ技術者の大切な責務であります。しかしＩＴ技術者の説明は専門用語が多すぎる・省略語多すぎる・横文字が多すぎると言われます。これはＩＴ技術者のコミュニケーション能力の不足を指摘したものといえるでしょう。

今般、通産省の戦略的情報化投資活性化プロジェクト(通称ITSSP)のその中核となる人材であるＩＴコーディネータの能力にコミュニケーション能力を求めています。

私ども日本システム監査人協会中部支部では年間テーマを決め議論してきたことの総まとめとして合宿形式による意見交換をしてきました。高いレベルとシステム監査にとどまらない議論は、飛び入りの方からも好評でした。

今回よりこの企画を公開し、ＩＴ技術者のコミュニケーション能力の向上特にプレゼンテーション能力の向上を目指したセミナーとしました。

この種のセミナーは他でも開催されておりますが、全てにそのまま適用できるものではありません。実地での応用は受講者自身が行うものであります。

多くの方の参加を期待するものであります。

記

１．実施日時	２０００.１１.１８(土)－１９(日)
２．場　　所	岐阜県大垣市ソフトピアジャパン
３．参加予定人数	５０名(内　非会員は２０名程度とする)
４．参加資格	通産省の高度情報処理技術者試験合格者
	もしくは同程度の能力を有し紹介者の推薦がある人
５．世話人	日本システム監査人協会会員が当たる
６．費用(宿泊費込み)	２５，０００円（会員　１５，０００円)
７．紹介者	日本システム監査人協会中部支部(紹介した人)

８．内容(予定)

(１)ビジネスから見た情報化をテーマとし　たゲストスピーカーによる講演、事例発表

(２)上記ケースを元に、グループ別の討論形式での意見交換、検討

(３)グループ別に成果物のプレゼンテーション

９．参加申込方法　紹介者にお尋ね下さい

コラム：会員のちょっと良い話
「秘湯の秘」

No.18　和貝　享介

温泉が趣味の一つ。

夏に家内とみちのくの秘湯に行く。姥湯(うばゆ)温泉。

スイッチバックをご存知だろうか。険しい山道を列車で行きつ戻りつ登るあれである。ここではクルマのスイッチバックがある。１台やっと通れる山道を多少の不安を覚えながら行くと突然立看板が現れる。絵のとおりＮ字型にローで前進→バックに入れて斜めに登りつつ後進→再びローに入れ前進、というふうにギアを入れ替えて進む。スイッチバック運転ができないと、姥湯には行けない。

クルマはここまで、という片側深い谷の空き地に駐車し、谷を見下しながら１００メートルほど急坂を徒歩で宿まで。荷物は、お猿が２匹乗れる程度の宿自家製の荷物用ロープウェイで谷越えさせるか、持って登る。途中の山肌を清水が滴り小滝となっている。木もれ陽の山風が涼しい。

標高1250メートルの１軒宿。夏休み時期とて満室の表示。山小屋風で天井が低い。聞くと、「春から秋まで」で、冬は宿のオーナーも山を降りるという。

ほろ酔いの夕食後風呂に行く。裂けた岩山にガッ、ガッ、ガッとノミを入れて作ったような露天風呂。青みがかった白濁の湯。勇気ある若い女性が入ってくる。混浴である。

夜空に満天の星。ぼんやりと天の川も見える。目を閉じると何もない。ただ、心地良いぬくもりだけ。

新入会員の声

No.９１５　千原　俊夫

私は都市銀行の国際部門に所属しており、国際業務でのシステム関連企画を担当しております。

昨今、金融機関のシステムリスクに対する取組の要請が高まっており、金融監督庁検査をはじめとして、銀行内の検査に於いても重要な項目となって来ております。

また、海外拠点においては多数の国に拠点展開している関係上、先進国から途上国までそれぞれの国のシステムセキュリティガイドラインに準拠した対応が必要となります。

このような環境の中でシステムリスクに対しての自己流の取組とはならないよう、基本から忠実に対応する為にとシステム監査について関心を深め、この度皆様方のお仲間に加えて頂きました。

現在は、海外拠点でのシステムリスクへの取組とその管理体制の構築に関しての対応を行っておりますが、お話出来るレベルではなくお恥ずかしい限りの内容です。

皆様方が交わされておられる事項は、参考になることが多く有り難く思っております。

銀行業務と云う仕事柄、セキュリティにつきましては守秘義務の観点から充分な注意を払わねばなりません。

しかしながら、業務上の生産性を向上する観点からは、モバイル環境で社内情報のアクセスを認める必要性にも迫られ、安全性と利便性のバランスが必要となります。

また、グローバルなネットワーク構築を行うと、海外で生じたセキュリティ上の問題も、重要情報の流出となりかねず、ゆるがせには出来ません。

職場だけで検討した対策ですと、ともすると独善的な対応に陥る懸念がありますので、皆様方との情報交換をさせて頂き、より良い対応にしたいと思っております。

今後とも宜しくお願い致します。

森 伸之

ＳＡＡＪ新会員の森 伸之といいます。よろしくお願いします。

私は川鉄情報システム(株)で会計システムのコンサルをしておりますが、システム監査、品質管理の領域について、初めて主体的かつ具体的に直面したのは、今から6年位前に、ある大手企業のシステム案件の入札条件として、ＩＳＯに準拠した品質システムについての取り組みを明記する必要があり、その件について社内調整を行った時でした。

当時、当社はＩＳＯ９００１認証をまだ取得しておらず、私は会社の品質システムへの取り組み強化を、品質管理の担当者に強く申し入れたことを覚えています(その後１９９６年１１月に、当社はＩＳＯ９００１認証取得)。

ＩＴ技術の進歩に伴い、電子帳簿法制化やＥＣ／ＥＤＩによる取引の増大など、システム監査人の存在意義は益々高まっている昨今ですので、初心を忘れずにやっていこうと思っています。

新規入会個人会員

番号	氏　名	勤務先・所属
960	神谷　勝典	(株)日立システムアンドサービス
961	寺下　厚二	(株)日本システムディベロップメント
962	山崎　敏夫	ヤマハ発動機(株)
963	野見山雅史	デトロイトトーマツコンサルティング(株)
964	田中　邦明	オムロン(株)
965	今津　忠夫	ゼネラリ保険会社
966	齋藤　淳	三井造船システム技研(株)
967	加賀谷久美子	アシストマイクロ(株)
968	西嶋　達男	(株)第一勧銀情報システム

編集後記

さて、今回の特集いかがでしたでしたか？
皆さんはSAAJ(日本システムス監査人協会)を120%活用されていたでしょうか？
今はインターネットや携帯端末等での情報も多く、ML等を活用し、遠くに離れている会員が双方やりとりをして執筆したり、意見交換をしたり様々な活動の可能性があります。
遠いから、忙しいからと思わずに、一声かけてみてはいかがでしょうか？
21世紀はどんな世の中になるのでしょうか？
会報担当一同皆様のますますの御活躍をお祈りいたします。(か)

＜会計より＞

当協会の会計は１月から12月です。平成13年度用の年会費の振込用紙が年明けにも届くと思いますのでお忘れ無く。

発行所 日本システム監査人協会
発行人 橘和　尚道
事務局 〒144-0054
東京都大田区新蒲田２－１－３
第１８ハネハビル７階
情報システム監査株式会社 内
TEL. 03(5711)3831 FAX. 03(5711)3832
ホームページ http://www.saaj.or.jp/
※ご連絡はなるべく郵便または、FAXでお願いします

会報担当(ご投稿、ご意見、ご要望は下記まで)
三谷慶一郎 (株)NTTデータ経営研究所
TEL. 03(5467)6331 FAX. 03(5467)6332
QZG07732@nifty.ne.jp
原田　奈美 日本アイ・ビー・エム(株)
TEL. 03(5644)6431 FAX. 03(3664)4968
QZE10566@nifty.ne.jp
富山　伸夫 富山システム監査事務所
TEL. 043(489)8754
GFF00037@nifty.ne.jp
片寄早百合 横浜市総務局
TEL. 045(671)2118 FAX. 045(664)9386
HGA01347@nifty.ne.jp
吉田　裕孝 三井物産(株)
TEL. 03(3285)2058 FAX. 03(3285)9939
Hi.Yoshida@xm.mitsui.co.jp