

CAA 日本システム監査人協会報

今回の会報の編集について

10月に、新しい高度情報処理技術者育成カリキュラムでの情報処理技術者試験がありました。アナリスト試験を受験された方もいらっしゃると思います。そこで、新しいカリキュラムと試験からシステム監査人の役割を再度、明らかにしていくことを編集方針としました。その為カリキュラムにも造詣の深い敦賀女子短期大学の斉藤隆氏にトップバッターとして、カリキュラム等から読みとれるシステム監査人の役割についてまとめていただきました。これを機会に会員の皆さんでもシステム監査人のアイデンティティを確立する為の議論をして頂ければと考えております。寄稿をお待ちしております。

高度情報処理技術者育成カリキュラム にみるシステム監査人の役割

No.332 斉藤 隆

1 はじめに

今後の情報化の飛躍的な推進の社会的要請に基づいて、通産省産業構造審議会より提言のあった「求められる情報化人材像」を育成するための13種類の高度情報処理技術者育成カリキュラム(以下標準カリキュラムとする)が、平成6年1月に、日本情報処理開発協会(JIPDEC)の付属機関である中央情報教育研究所(略称、CAIT)より公表されました。ここでは、標準カリキュラムにおけるシステム監査人およびシステムアナリストの位置づけを検討することにより、これからのシステム監査人の役割について、私見を述べさせていただきます。

また、今秋、当標準カリキュラムに基づいて、新試験制度のもとでの第1回目の情報処理技術者試験が実施されましたのが、その出題内容も合わせて簡単に検討させていただきます。

2 標準カリキュラムにおける考え方

標準カリキュラムにおいて、システム監査人の役割とは、情報システムを総合的に点検・評価し、関係者に助言・勧告することによって、情報システムの信頼性・安全性・効率性の向上の実効を上げ、情報システムの健全な発展を図ることであると考えられています。私はシステム監査技術者の標準カリキュラムおよびそれに準拠したCAITテキストの作成に参画しましたが、その時の作成方針としてあげられた項目の

なかに、「システム監査基準」への準拠と最新の情報技術への対応がありました。したがって、システム監査技術者カリキュラムの「第3部 システム監査の実施」、「第5部 システム監査ケーススタディ」は、それぞれ前者、後者の作成方針を反映した結果であります。

また、システムアナリストの役割とは、経営戦略の達成を情報システムの観点から支援するために、経営戦略と一体となった情報戦略、中長期の情報システム全体計画および個別の情報システム開発計画を立案することであると考えられています。そして、それぞれのテーマはシステムアナリスト標準カリキュラムの中で、それぞれ「第2部 情報戦略の立案」、「第3部 情報システムの全体計画立案」、「第4部 開発計画の立案」として扱われています。また全編にわたって、業務改善の重要性およびそれに対するシステムアナリストとしての積極的な関与が強調されています。

なお、システム監査技術者、システムアナリスト共、標準カリキュラムおよびCAITテキストの「第1部 情報システムの基本的知識」の内容は全く同じです。これは、両人材に対して、次のような育成方針があるからだと考えます。システムアナリストにとって、「第1章 経営一般」と「第2章 情報システム」の重要性は言うまでもありませんが、職務上、システムアナリストはいわゆる情報システムの効率性を重要視しがちで、したがって情報システムの信頼性、安全性の重要性を再認識するために、「第3章 情報システムの評価と監査」と「第4章 リスク

分析と情報セキュリティ]があると考えます。

システム監査人にとって、第3章と第4章の重要性は言うまでもありませんが、職務上、システム監査人は監査の視点が個々の情報システムの域に留まりがちで、したがってそれを一步踏み越えて全社的な視点、さらには経営的な点からのシステム監査の重要性を再認識するために、第1章と第2章があると考えます。

3 これからのシステム監査人の役割

システム監査人にとって、システムアナリストの業務も当然に監査対象となります。しかしながら、以下で述べるように、私はこれからのシステム監査人は自身の役割をもっと積極的に考えていく必要があると考えます。

昭和60年に「システム監査基準」が公表されて以来、システム監査技術者試験制度、システム監査企業台帳制度、システム監査実施企業に対する情報化保険の割引制度など、様々なシステム監査に関する施策が打ち出されてきました。また、今、特定システムオペレーション(SO)企業認定制度、システム開発取引の共通フレーム、ISO9000-3など、システム監査の必要性を強調するトピックスがいくつかあります。しかしながら、このような状況下にもかかわらず、過去に「システム監査で飯が食えるか」という議論もあったように、現在でもシステム監査人に対する社会的注目度は今一步の感があることは否めません。その原因として思うに、確かに「監査」というネーミングにより、対外的なイメージの悪さもあるかもしれませんが、私たちシステム監査人側も「監査」を意識し過ぎているのではないのでしょうか。特に、いわゆる「効率性」の領域において。

すなわち、今後の高度情報化社会を健全に発展させていくためには、情報システムの「信頼性」、「安全性」を独立第三者の立場から点検・評価するという機能は全体に必要不可欠です。しかしながら、この役割は今後共、金(内部監査人にとっては、経営者からの注目)にはなり難いと言えましょう。いわゆる「効率性」の領域で勝負しないと、花は開きません。そして「効率性」の領域では、私たちシステム監査人は、単に経営的な視点からのシステム監査の実施を心掛けるだけではなく、より積極的にシステムアナリストとしての役割を、特に内部監査人にとっては、果たしていかなければならないのではないのでしょうか。それも、ただ単に情報シ

テムの「効率性」の追求ではなく、「信頼性」、「安全性」に裏打ちされた「効率性」の追求です。私たちシステム監査人は、情報システムの「信頼性」、「安全性」の必要性、重要性を身をもって知っており、そのことがシステムアナリストと決定的に差別化できる点です。標準カリキュラムの第1部は、そのようなことを私たちに暗示していると思います。

今、企業経営はBPR(ビジネス・プロセス・リエンジニアリング)という名のもとに、いかに最短距離で業務を遂行していくかということに関心が集まっていますが、これは裏を返せば、チェック機能、管理機能の除去にもなりかねません。したがって、BPR後のビジネス・プロセスに対して、その正当性を保証するための監査機能が一層重要性を増してきます。このような点も考慮に入れながら、これからのシステム監査人としての役割を各自が考え直してみる必要があるのではないのでしょうか。

4 新情報処理技術者試験の概要

(1) 標準カリキュラムとの連動

標準カリキュラムの役割の1つとして、今後の高度情報化社会を担う情報処理技術者の育成指針ということをあげましたが、もう1つの役割として、情報処理技術者試験の試験科目、範囲を提示するという点もあります。したがって新試験制度下での受験者にとって最も重要な点は、標準カリキュラムに準拠した学習を行わなければならないということです。すなわち、まずは標準カリキュラムから自分が受験する人材の役割や業務内容および他の人材との関係を理解したのち、具体的な学習はCAITテキストに基づいて行っていく必要があります。特に、各章末にある「キーワード」の理解がその第1歩となります。

(2) 今秋の情報処理技術者試験の状況

システム監査技術者試験の人気減、システムアナリスト試験の人気増というおおかたの予想に反して、両試験の応募者数(受験者数、受験率)はそれぞれ、7,464人(4,151人、55.8%)、8,156人(5,073人、62.3%)でした。不幸にして合格しなかった過去の受験者がそのままシステム監査技術者試験を受験したこと、システムアナリスト試験は第1回目であるので模様眺めの受験予備軍が多かったこと、などがその理由ではないかと思われま

以下、今秋のシステム監査技術者試験とシステムアナリスト試験の問題を、試験方法別に検討してみます。

(3) 多肢選択式問題

多肢選択式問題は80問出題され全問解答となりました。また、その出題範囲は試験案内にあるように1種の範囲を含みます。

両試験とも、多肢選択式問題が非常に得点しにくくなりました。それは1種の範囲に属する出題割合が80問中60問前後と多く、しかもそれらは各問とも基本的な問題であるにもかかわらず、出題範囲が非常に広いからです。したがって、今後の受験者として、ここでの足切りをクリアするためには、午前の1種問題をいかに攻略するかが、大きなポイントとなると思われます。

(4) 記述式問題

記述式問題は5問出題され3問解答となりました。各問題の難易度は、両試験とも、今までのシステム監査技術者試験の間4から間7と同程度ですが、長文の問題文の中に解答そのものが隠されている出題が少なくなり、類推して解答を導き出さなければならない出題が多くなりました。したがって、今後の受験者としては、今まで以上に実務試験(長文の問題文の裏に隠されている真の問題点を読取る力)が必要となると思われます。

(5) 論述式問題

論述式問題は3問出題され、1問解答となりました。ここでのポイントは、今回の試験から要求される「業務経歴書」の記述方法です。業務経歴書は事前に解答できる設問アといっても過言ではなく、したがって紙面いっぱい「業務の概要」と「私の役割」を記述しておく必要があると思われれます。

なお、両試験とも、本試験では要旨の記述が不要となりました。また、設問アの解答方法について、システム監査技術者試験では従前どおりでしたが、システムアナリスト試験では「システムの概要」に関する内容を質問形式で解答させました。

理事就任の挨拶

No.467 山田 俊明

はじめまして。本年2月から福德様の後任として近畿会の理事の重責を担う事になりました株式会社アスコットの山田です。20数年間富士通のSEとして、関西の中堅企業の情報化のお手伝いをしてまいりましたが、昨年1月退職し有志との(株)アスコット設立により企業の情報システムコンサルティングや、情報システム構築のお仕事をさせて頂いております。

まだまだ会社基盤を固める時期であり、本業での多忙な毎日です。このような状況下ではたして監査人協会へのお手伝いがどこまで出来るかが大変不安でありました。

しかし、前任の福德様からの強い押しと、これも何かのご縁と思い、お引受け致しました。微力ではありますが、協会・近畿会の活動に少しでもお役に立ちたいと思っておりますので、宜しくお願い致します。

さて、近畿会では2ヶ月に1回の割合で、定例の研究会を開催しております。ここでは、会員の方を中心にシステム監査に関するテーマで発表とディスカッションを行っております。

又、本年から監査の実践能力の習得を目指した、「実践研究会」を分科会として発足しております。定例研究会や分科会の終了後は、2次会として場所を変えて懇親会を催しており、皆さん軽くお酒を召し上がりながら、その日のテーマへの意見交換やら、情報交換を行っておられます。どうぞ近畿会の皆様、どんどんご参加下さい。お待ちしております。

第34回月例研究会感想文

日時：平成6年9月19日
 テーマ：「企業内パソコンソフト使用をめぐる違法コピー問題」
 講師：(社)日本パーソナルコンピュータソフトウェア協会
 事務局次長 佐藤文信氏
 (社)コンピュータソフトウェア著作権協会
 事務局長 久保田裕氏

さる9月19日に開催された月例研究会は、パソコンソフトを、テーマの中心においたソフトウェアの著作権保護について、上記関係協会の佐藤氏と久保田氏より、講演があった。

<講演内容>

I. ソフトウェア協会 佐藤氏

通称「パソ協」と呼ばれる本協会の概要と、協会で行っている「権利保護活動」についての概略説明があった。

本協会は、PCパッケージソフト開発会社を中心に正会員約250社から成っており、企業に対して不正コピーを無くさせる様、啓蒙活動を行っている。

「本協会の啓蒙活動実績」

(平成5年度実績)

「違法コピー対策プロジェクト」を設置。

- ① 「NOCOPY宣言」ポスターの制作と全国の業界団体等への配付・掲示の実施
- ② 違法コピー防止の啓蒙アンケート調査実施
- ③ 違法コピー被害実態調査の推計調査実施
- ④ 日本監査役協会、日本内部監査協会、日本システム監査人協会、EDP監査人協会に対して、企業内における違法コピー撲滅の協力要請・申し入れを実施等々。

(平成6年度計画)

違法コピー対策プロジェクトと法的保護委員会の合同委員会により活動予定。

- ① 企業ユーザー向け「パソコンソフト管理マニュアル」の制作・配付や管理セミナーの実施
- ② 著作権関係団体との連携強化等々。

(佐藤氏のコメント)

企業におけるパソコンの管理は、システム監

査人の仕事と認識している。

又協会として実際に使える管理を検討しているという事であった。

II. 著作権協会 久保田氏

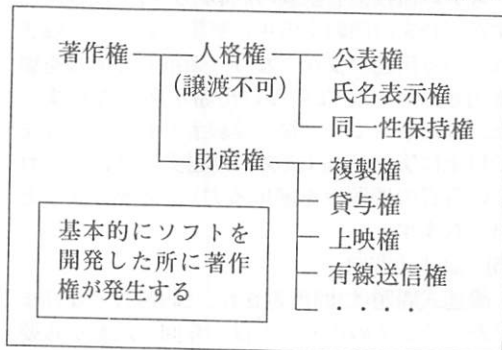
まず著作権法違反の、刑法上での罰則規定についての説明があった。

「3年以下の懲役又は100万円以下の罰金」で、これは窃盗罪より重い罰則であり又両罰規定により違反を犯した個人と企業の両者が、罰せられるという説明であった。

このような重い規定にもかかわらず、現状ではオリジナルソフトの3~5倍位は、違法コピーが稼働しているといわれている。

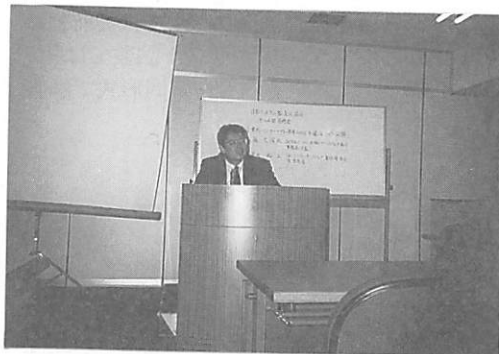
次にユーザーが著作権法に、どの様に抵触しているかを、著作権の内容を交えて説明があった。

プログラムが著作権保護の対象となる為には、「思想又は感情を創作的に表現した物であって、文学、学術、美術、又は音楽の範囲に



属する物」という要件を充足する必要がある。又「プログラムの定義」中の電子計算機には、汎用機からPC・マイコンまで含まれる。

オブジェクトプログラムは、ソースプログラムの複製物である。リバースエンジニアリングについては、現在日米間で玉虫色の状態である。



プログラムの一部であっても、「表現」に値すれば著作物として認められる。(複製不可) 同一性保持権の例外として、プログラムの利用に必要な改変を認めた。違法にコピーされたプログラムであると知って実行すれば、著作権法違反となる。現在では著作権の範囲を、プログラムだけでなくデータベースやデータの送信権等にも、ひろげている。

又著作権以外に「使用許諾契約」の契約違反(使用可能範囲・第三者譲渡の可否等)についても説明があった。使用許諾契約の内容については、実態と合っていない点や、ソフトハウスにより内容が異なり混乱の要因となっている点を認めつつも、だからと言って「違法コピーしていいんだ」とは決してならない事を、強調された。

III. Q & A

Q. 社内管理規定を作成したいが、具体的でモデルになるものがないか。

A. 協会で作成している「管理責任者の役割」がある。社内で徹底させるには、トップの意思表示が必要である。

<感想>

今回のテーマは「ソフトの違法コピー」ということで、私自身を含めて多数の人に心当たりがあるテーマであった。

ソフトパッケージの購入は、あくまでも制限付きの使用許諾権を、得ている事にすぎない事をあらためて思い知りました。

ソフトウェア業に携わる一員として、サービスを含めたソフトという価値と評価を、広く一般の人々にも認めてもらう為にも、違法コピーの問題は、積極的に解決していかなければならないと自覚した次第です。

本月例会の翌週に開催しました部内リーダー



会議において、早速この問題を取り上げ、我々自身のためにも積極的に取り組む様、今後の方針等について私からお話ししました。

又本件に関しては、システム監査人が果たすべき役割が非常に大きいものであるとも自覚いたしました。

No.555 松枝 憲司

第35回 月例研究会 感想文

日 時：平成6年10月12日

テーマ：海外のセキュリティ基準動向並びにセキュリティ基本要件

講 師：日本電気株式会社 技術企画部
標準化推進部 担当部長 菅 知之氏

概 要

平成6年6月、社団法人、日本電子工業振興協会コンピュータセキュリティ調査委員会 コンピュータセキュリティ評価基準専門委員会から公表された『コンピュータセキュリティ基本要件 機能編(第1版)、同保証編(第0.1版)』について、委員長を努められた菅講師より、海外のセキュリティ基準の動向を概観しながら、『コンピュータセキュリティの基本要件』の説明が行われた。以下、当日配付された資料を参照し、講演の概要を紹介する。

1. 海外セキュリティ基準動向

機密(国防)の製品評価基準として、1985年制定された米国のTCSEC(Trusted Security Evaluation Criteria)は、その後民間システムの機密性・完全性・可用性の製品評価基準として、ITSEC(Information Technology Security Evaluation Criteria)に発展していった。(図参照)

2. 『コンピュータセキュリティ基本要件』の作成

基本要件(注1)の作成に当たっては、海外で検討されているセキュリティ評価基準を収集し、最小要件の抽出を行い、ITSECの8つの評価軸(注2)に基づき記述した。基本要件は、スタンドアロン、ネットワークを含むコンピュータシステム/製品が備えなければならないセキュリティの機能を規定した『機能要件』及びセキュリティ機能を提供するコンピュータ製品(ユーザーがシステム運用のために開発するプログラムを含む)が信頼できるものであることを示すために、その開発過程、開発環境、開

発手法等を規定した『保証要件』から構成されている。

『機能要件』に相当する基準として、既に通商産業省『電子計算機システム安全対策基準』等があるが、既存基準書では不十分と考えられる技術対策を補完する内容となっている。『保証要件』については、既存の規約としてISO 9000があり、同等の事項（製品開発に関する事項）に対する規定がある。しかし、本要件の方がISO 9000の要件に比較し、より詳細な事項を規定しているため、本要件に準拠して開発すれば、該当要件についてはISO 9000を満足することになる。

『機能要件』については完成したので、今後は業務固有の要件検討や国際標準との調整を図る。また、保証要件は更に充実を図る予定である。

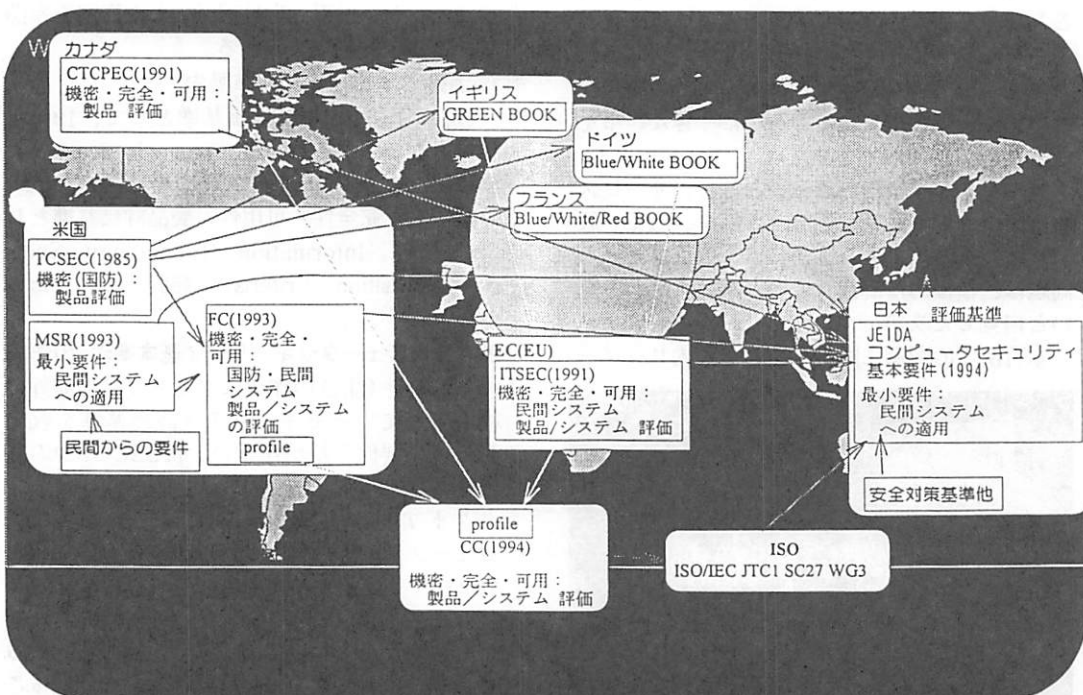
(注1) 一般商用システム及び非軍事システムの運用環境において、セキュリティを実現する上で最低限必要と考えられる要件。米国の政府機関とユーザーが共同で開発したMSR(Minimum Security Requirements)で暫定運用されているITSECの商用システム適用レベルの要件に対応するものである。

(注2) ①Identification and Authentication. ②Access control. ③Accountability. ④Audit. ⑤Object reuse. ⑥Accuracy. ⑦Reliability of service. ⑧Data exchange.

所感

1. 海外のセキュリティ基準の動向を踏まえながら、基本要件を説明される言葉の端々から、基本要件策定への情熱と作業の綿密さがうかがわれ、素晴らしい講演内容でした。
2. 保証編は、監査の立証プロセスに基づいて記述されており、まさしくシステム監査人にとって有用な内容です。今後の充実が大いに期待されます。
3. 講演終了後の懇談会において、菅講師より最近のインターネットを含めたセキュリティの現状にふれられ、セキュリティを『技術』で対応するには限界があり、結局、人間の倫理的な側面が大切である旨のご指摘がありました。情報社会における『倫理』についてはセキュリティの基本要件を構築するベースとして、今後益々重要な社会的な課題になるように感じられた次第です。

No.536 芝野 誠一



(第35回 月例研究会 配布資料より)

システムアナリスト試験研修会開催される

今年度より実施されることになったシステムアナリスト試験に向けての対策講座が、8月20・21日、27・28日にシステムアナリスト(SA)部会の主催にて実施された。月例研究会(第33回)の葉書で案内したもので、講師は当協会の会員でもある敦賀女子短大の斉藤隆先生にお願いした。従来のシステム監査試験と比較して新たに加わった試験分野を中心に、CAIT発行の94システムアナリストテキスト及びSA育成カリキュラムを主教材にして研修が行われた。8月の暑い期間、2週連続の土・日にもかかわらず、九州・大阪・名古屋・長野からの参加者も交えた23名が熱心な講師の下で“勉強”にはげんだ。

今回の参加者は、貴重な夏休みをこの講習参加に当てているだけに、取組み姿勢は全員真面目この上なく、かつ熱の入ったものであった。質問や意見表明もそれぞれの経験・考えから出され、今回のSA試験範囲として取り上げられた、企業の経営戦略や情報戦略の分野については造詣の深い斉藤先生もたじたとする程であった。初日には小宮山事務局長も来られて、合格祝贺予行演習(?)を兼ねた懇親会も開催し、厳しいながらも皆で頑張ろうという意欲を確認し合った。

研修期間後も論文添削のための演習問題が課せられ、また追加のテキストとして重要用語集(*)も配付されるなど充実した研修会となった(*SA部会荒川理事の著書。別項図書紹介記事参照)。今回参加の3人の方の感想文をいただいたので、研修会の雰囲気を感じとっていただきたいと思います。なお、本研修会は今年限りの予定で開催したものです。

システムアナリスト講習会を受講して

No.655 荒牧 裕一

高校生の頃、新幹線で名古屋から東京の有名塾に通っているある進学校の生徒の噂を聞いたことがありました。その当時は「何もそこまでしなくとも」と思ったものですが、10数年経ち、自分自身が大阪から東京の講習会に通う経験をして、その生徒の気持ちが理解できました。素晴らしい講義を受けるためならば、長距離移動の時間も手間も苦にならないものです。

斉藤先生の講義は分かり易く、かつ内容の濃いものであり、休憩と休憩の間(つまり講義時間)がとても短く感じられました。

この講習会は、私にとって、この夏最も充実した4日間であったと思います。どうもありがとうございました。

システムアナリスト講習会の感想

No.267 榎本 百合子

2週連続の土日を使用しての講習会は、集中力も記憶力も劣えかけてきた者にはやはりハードでした。

600ページあまりのテキストをどのように進めていかれるのか、不安でしたが、目新しい部分はその場で読む時間を与えられ、その他の部分は先生の方で要点をまとめて説明されたので、終了したときには全ページ読んだような気になってしまいました。

今回の講習会では、勉強の仕方や答案作成時のポイント等を教えていただき、今後の試験勉強を効率的に進めていくのに大いに役立つのではないかと思います。

アナリストセミナーを受講して

九州支部 秀嶋 弘行

まず、テキストの厚さに驚く。B5版600ページ、重さ1.3kg、カリキュラムや参考書を合わせると、その重さは2.4kgに達する。本を重さで量るのもおかしな話だが、問題はこれらをすべて“読破”して“要点を記憶”できるか、である。

今年はアナリスト試験の第1回で、すでに泥縄式に(?)まとめられたいくつかの受験参考書が刊行されたと聞く。しかし、このテキストは、それらの中で最も権威あるものといわれる。あとは受験者の努力如何というわけだが、すでに脳の神経細胞の相当部分が死滅している年齢の私にとっては、如何に相成りますことや、甚だ心もとない次第です。

おわりに、労を惜まず懇切丁寧にご指導くださった斉藤先生、このセミナーの企画、運営に大変お世話になった荒川さんはじめスタッフの皆さんに、心から御礼申し上げます。

中部支部活動報告

No.174 西脇 滋

- ◎ 中部支部の定義……住居地もしくは勤務地（正確には会員名簿の住所）が次の各県に属すること。愛知(26)岐阜(3)三重(0)静岡(7)長野(4)富山(4) / ()内は会員数、計44名
- ◎ 例会活動……奇数月第3土曜日15時より終了まで発表会と質疑、フリーテーマ討議
- ◎ 定期懇談会……11月例会後
- ◎ 不定期懇談会……各例会後
- ◎ 例会の内容
 - 3年度－外部講師に頼る
 - 4年度－支部メンバーで順番
 - 5年度－N社実監査の勉強
 - 6年度－ダウンサイジングとJFSP94
- ◎ 7年度活動予定－検討中
- ◎ おおまかな活動内容は上記の通りですが毎回10名程度の参加で細々と息長く活動しています。会員の方のエリアの広がりや交通事情から平日の夜に会合を持ちにくいために土曜日の午後開催しています。皆さんなかなか出にくい様子で、会の連続性を保つのに苦労しています。特に不定期懇談会はその役割を果たす上で大切な行事になっており各人各様に情報交換の場所として巧く使っています。以下参加率の高いメンバーより順に字数の許す所までメンバー紹介をします。

<原 善一郎>

岐阜県大垣地方の名士、JC、消防、ボーイスカウト、ガールスカウトその他諸々、名刺がおもしろい。仕事もガンガン、本会も影のリーダー的存在で益々盛んな30代。

<齊藤 礼三郎>

会社経営者。トライアスロンでスタミナ十分補給。本音と建前を使い分け何時もにこにこ40代。本会ではムードメーカーです。仕事柄遅刻早退をすることがお休みは少ない。

<沢 貞夫>

中部支部初代理事。今や米原に居を構え名古屋で稼ぐ一匹狼。眼鏡のしたの目が厳しい勤勉な50代、困ったときの沢頼み皆で便りにしています。

<田原 保>

メーカー系SE。一声高い声色ではっきり発言EDP経験豊富何かと教わる所が多い。メーカーの考え方、将来方向を不定期懇談会で聞くことが楽しみです。元氣な40代。

<万代 みどり>

メーカー系SE。女性会員1号、御主人に子守を任せて本会に参加します。おじさん相手にはっきりと持論を展開し女性の職場進出大歓迎の見本です。

<片寄 百合子>

コンサル会社SE。女性会員2号、仕事の都合で一時名古屋転勤になり中部支部の例会へ参加しています。これまた才女につき男性メンバーが時々厳しい追求を受けます。

<鈴木 喜博>

ソフト会社SE。温厚、只今の職種は教育担当につき調査の必要な案件は専門で引き受けてもらいます。同じ会社の上司も会員であるので我儘いえない30代。

人となりと活動内容の概要を理解できた方例会に是非参加して下さい。

連絡先

西脇 滋(セントラルシステムズ 営業推進本部)
TEL 052-204-6555 FAX 052-232-4800
外出が多いので御用はFAXが良いと思います

近畿会の活動状況報告

No.467 山田 俊明

(1)近畿会の概要

昭和62年12月に日本システム監査人協会が設立されたその2ヶ月後の昭和63年2月に早くも当近畿会が結成され、本年で丸6年を迎えています。

当時からの熱心な会員のサポートにより、2ヶ月に1回の定例研究会が行われ、着実なる研究活動が継続されている。又、これも当時からの良き伝統として、定例研究会後の懇親会も引き継がれて行われており、毎回会員諸氏の有意義なコミュニケーションの場として大いに盛り上がっています。

さて、当近畿会のエリアは名前は近畿会というものの大阪を中心に近畿2府4県に加えて、北陸の福井・石川・富山、中国の岡山・広島・鳥取・島根、及び四国4県にわたって、

130人以上の会員がおられます。しかし、残念ながら皆さんと顔を合わせての定例研究会は常に大阪市内での開催であることから、北陸や中四国からの出席は毎回1~2名と少なく、遠隔地の会員へは余り貢献できていないのが現状です。

このような観点から、平成5年から北陸地区の活動を推進する為、川端純一氏(敦賀市役所)を世話人として北陸分科会が結成された。現在会員数14名で年3回の定例研究会が開催されている。また、岡山・広島・鳥取・島根等の中国地区にも15~16名の会員がおられ、より積極的な活動推進を目指しての、中国支部独立の計画が進められており、近畿会としても出来る限りのお手伝いをしていきたいと思っております。

現在、近畿会では上記の定例研究会に加えて本年3月より、会員のシステム監査能力の育成を目指しての「実践研究会」が結成されています。ここでは模擬監査を通じてシステム監査の実践能力を身につけることと、模擬監査に参画出来ない会員の為の「監査モデル」の作成・開発チームの活動がスタートしています。(詳細は別項にて)

さて、現在の近畿会の会長は安本哲之助氏(日本生命保険)、理事として石島隆氏(センチュリー監査法人)と私(山田)が担当しています。毎回の定例研究会は大体20~30人の出席、実践分科会は10~15人の出席があり、参加者のご協力によってその都度活発な議論が展開され、有意義な会合となっているものと思っています。今後とも会員の皆様の積極的なご参加をお願いします。

最後になりましたが、近畿会の定例研究会では、会場として日本ユニシス(株)殿のご協力により、セミナー用の教室をいつもお借りしています。以前は毎回会場探しに苦労しましたが、最近では会員も開催場所に戸惑うことなく、又快適な場所での会合が出来、近畿会会員一同感謝しております。この紙面をお借りして厚くお礼申し上げます。

(2) 近畿会定例研究会の発表内容

- ① 2月25日(第36回定例研究会)
 - ・テーマ: 「BPRと情報システム」
 - ・発表者: さくら総合研究所
権野 祐二氏
- ② 4月22日(第37回定例研究会)
 - ・テーマ: 「当社における
システム監査の実施例」

・発表者: 日本ペイント株式会社
宮嶋 馨夫氏

③ 6月24日(第38回定例研究会)

・テーマ: 「情報系システムの!!!」
—当社における営業支援システムの構築と評価—

・発表者: (株)アスクプランニングセンター
日高 祐子氏

④ 8月19日(第39回定例研究会)

・テーマ: 「システム監査の評価基準」

・発表者: 九州帝京短期大学教授
システム監査人協会九州支部長
守田 昭彦氏

(3) 近畿会「実践研究会」の活動報告

日本ユニシス(株) 喜多 陽太郎

「研究会も大事だけど、実際にシステム監査をやってみたい」という話を発端に、熱心な会員10数名が集まり本年3月に実践研究会が発足しました。そして、月一回のペースでの実践的な勉強と議論を重ねるうち、嬉しい誤算とも言えるべきか、早くも6月にはクライアント(以下K社)が見つかり、「初めてのシステム監査」がスタートしました。

K社は年商約100億円、社員数約350人で全国15ヶ所に営業所・工場・研究所をもつ製造会社です。電算室要員は室長・係長と担当者2名の計4名で、オフィスコンピュータを活用して多くのシステムの開発・運用に携わってこられています。今回のシステム監査への期待として、電算室の運用管理全般について現実に即したアドバイスを求めておられる様でした。

実行メンバー4名が現地に向いて調査→その結果を分科会で報告→全員で議論した後、次回の調査項目を検討→実行メンバーが次回までに準備、というやりかたで進めていきましたが、結構負荷のかかる状況が続きました。

K社電算室の規模からは、通産省のシステム監査基準は全くといってよいほど役に立ちません。システム監査の世界では理論はあまり役には立たないこと、客観的な評価と具体的な改善提案というのが如何に難しいものであるかを再確認しました。

現在は、11月中旬に予定されている報告会のために報告書の最終調整を行っていますが、機会があれば今回実施した模擬監査について、詳細な報告をさせて頂きたいと思っております。

(4)「監査の企業モデル開発チーム」の活動報告 日本ペイント(株) 宮嶋 啓夫

① はじめに

前述の実践研究会スタート時の実行方針としては模擬監査の実施により、会員の監査能力の向上を図ることとなりましたが、現実には実際の監査の場面に参加出来ない会員の方が多い状況です。この為、今後の会員の実践的能力育成の為には、より実際に近い監査のトレーニングができる「企業モデル」の構築が必要と思われ、開発チームの活動を開始しました。

② チームの発足とモデル構築の方針

スタートからメンバー編成上の磋跌はあったものの、4名で5月からスタートしました。暗中模索ではありましたが、

- ・メンバーから提示されたモデルをベースに
- ・あまり高度な情報化レベルとはしない
- ・モデル概要構成後は、分担してサブシステムを設計する。
- ・当初は受査対象を限定、将来的には対象範囲を拡大し、監査人が計画立案できる自由度を大きくしたい
- ・ミーティングは月2回程度

等をモデル構築方針として、前進することにしました。

③ チームの活動内容と現状

- ・モデル構築：素案の業種、業態、企業体質等の具体化について、疑義討議や提示者によるレクチャーと資料学習等を実施。
- ・レベル設定：企業組織と性格、情報化レベルの設定、主たる構成員の性格付け、意識の設定
- ・サブシステム設計：販売、生産、経理システムの設計分担、入力データ、DB、出力帳票等の決定
- ・情報システム運用状況の設定：システム構成、運用スケジュール、ネットワーク、標準化の程度、諸資料の整備状況等の設定と資料作成

以上、メンバーの熱心な活動の結果、モデル構築の第1ステップは最終検証段階を残すのみとなりました。一旦、区切りをつける必要はありますが、出来れば今後共「企業モデル」の充実・拡張を続けたいと思っています。

◆近畿会会長、大阪大学の教壇に、

93/94年版のシステム監査白書によるとシステム監査に関する教育科目講座を開いているのは、全国で4年制大学で9校、大学院で2校と報告されている。近畿地区では、神戸商科大学(商経学部)・近畿大学(商経学部)・摂南大学(経営情報学部)・流通科学大学(情報学部)の4校のみであったが、今年10月から大阪大学(経済学部)でも新たに開講されることとなった。システム監査の分野について教育と研究に着手する大学が増えてきたことは大変喜ばしい限りである。

又、この開講に際して、当大学のOBである近畿会の安本会長が母校の教壇に立ち、後輩の指導にあたっておられることは重ね重ね喜ばしい限りである。

九州支部活動報告

No.374 木下 一郎

1. 緒言

九州支部の活動は、毎月1回(週の第3土曜日 15:00~17:00)の例会が中心です。平成6年は守田支部長のもと、「情報システムコンサルティングの手引」の原稿を募集し、検討、協議しています。例会には、常時10名前後の会員が集まります。会場は(株)日本システム監査の厚意により、同社の会議室を使用させてもらっています。年末(忘年会がある)や、特別な行事(事務局長との対談などが企画されたとき)の場合は、人数が増えて別の会場を手配するケースもあります。支部会員は、現在28名であり、公認会計士8名、情報システム関係17名、その外3名、という構成になっています。協会最高齢の方、夫婦で会員の方などもメンバーなので、単なる情報交換の場にはない雰囲気があります。

以下に、平成6年1月から10月までの活動について報告します。

2. 活動内容

平成6年1月の活動(第49回:12名出席)

- ・「コンサルティングの手引き」の項目の検討、協議を実施しました。既に提出された原稿の確認、及び「手引」の構成と記述の仕方について検討しました。また、「手引」を利用するコンサルタントのイメージについても統一しました。

- ・鞍馬氏からISO9000認証制度について解説していただきました。
認証制度の現状、認証取得状況、認証制度の流れ等について資料をもとに説明されました。

- ・内田氏から九州支部の93年収支決算報告及び94年予算案について提出され、承認されました。

平成6年2月の活動(第50回：9名出席)

- ・守田氏から第7回総会の出席報告をしていただきました。
前年度の活動報告、会計報告、および、前年度の事業計画について説明がありました。

九州支部は、平成5年に「システム監査ハンドブック」を作成しました。

- ・秀島氏から第32回研究会「システムコンサルティングとシステム監査」の出席報告をしていただきました。
システムコンサルティングの実施例や基本テスツ、システム監査との関係について解説していただきました。

平成6年3月の活動(第51回：7名出席)

- ・ソフトウェアの権利・保護について、著作権法、特許法などとの関係について協議しました。
- ・行武氏から携帯電話の動向について解説していただきました。
レンタルから売り切り制へ、首都圏はデジタル化へ、等の動きがあるとのこと。
- ・電話番号、テレホンカード、バンクカード、クレジットカード等のセキュリティの現状について意見交換しました。

平成6年4月の活動→中止(会場都合のため)

平成6年5月の活動(第52回：10名出席)

- ・鞍馬氏からシステム構築の際の情報化投資についての採算性をどのように検討するか解説していただきました。
情報化による効果と投資効果の算定方法、及び採算性の評価について、資料をもとに解説していただきました。
- ・鞍馬氏からソフトウェアの権利保護について解説していただきました。
ソフトウェアの権利保護の現状と、利用者としての留意事項について解説していただきました。無体財産権、著作権、特許権等の権利保護の体系と、著作権法での保護の限界についても紹介されました。

平成6年6月の活動(第53回：9名出席)

- ・行武氏から通信の機密保護はどのようになさしているか解説していただきました。
収集、利用、提供、適性管理、個人参加、責任の明確化等説明していただきました。
- ・秀島氏から監査人協会第32回月例研究会出席報告をしていただきました。

平成6年7月の活動(第54回：10名出席)

- ・監査人協会の小宮山事務局長から協会の現状報告をしていただきました。
- ・行武氏からプログラムの私的複写権について、および、システム開発における著作権の帰属について解説していただきました。
プログラムの私的複写権は認められない方針であること、システム開発を外注する場合に著作権が成立するので契約書にその明細を記載すること等、説明されました。

平成6年8月の活動→中止(出席予定者少数のため)

平成6年9月の活動(第55回：7名出席)

- ・鞍馬氏から特定システムオペレーション企業等認定制度を紹介していただきました。
システム監査人としての活躍の場が広がり、より一層の活躍が期待されるようになりました。九州支部が平成5年に作成した「システム監査ハンドブック」をもとに、チェックリスト作成し、システム監査に当たることが出来ます。
- ・守田氏から「システム監査の評価基準」について解説していただきました。
基準の分け方を、統制の水準から、基本的統制、異例事項統制、特殊事項統制、予知的統制に分けて説明されました。
- ・守田氏から第3回BSAジャパン福岡セミナーの参加報告をしていただきました。

平成6年10月の活動(第56回：5名出席)

- ・行武氏から汎用コンピュータのコンピュータウイルス対策について解説していただきました。
汎用コンピュータでもオープン化によりウイルスの脅威が増大していること、及びウイルス対策の内容について説明していただきました。

活動内容は、以上のとおりです。全国の協会会員の皆様、九州出張の折りには、例会に顔をだしてみたいかがでしょうか。12月の例会(12月17日(土曜日)の予定)終了後は忘年会を予定しておりますので飛び入り参加も歓迎いたします。

セキュリティ分科会 活動報告

日本ユニシス(株) 加藤 豊房

平成5年、セキュリティ分科会のメンバーが月1回のペースで、「情報システムの緊急時対応計画」(青山監査法人システム監査部編)の解説を開始。平成6年には、そこで学んだリスク分析手法を実際に経験するため、適当な規模の企業想定して、「情報システムへの影響想定シナリオ分析表(以下、「シナリオ分析表」と呼ぶ)を作成した。その結果は本誌1994年5月号、No.29の「セキュリティ分科会活動報告」(金子長男氏寄稿)に記載されている。この時は、仮想企業を設定しひととおりCPを試みた。したがって、「シナリオ分析表」の情報システム稼働資源、災害の種類、被災の影響度の測定は難なく完了させている。

実際の企業で具体的なリスク分析を行い、CPを作成するための準備として、以下の活動ターゲットを設定した。

1. 「シナリオ分析表」の作成の信憑性を増すために、
 - ① 「情報システム稼働資源」の分類基準を作成する
 - ② 「災害の種類」を網羅的に列挙し選択方式をとる
 - ③ 過去の実績データから「被災時の影響度」の判断基準を設定する
2. 「JRAMによるリスク分析手法」を活用するために、
 - ① JRAMについて学習する
 - ② 特にJRAM質問票の利用を検討する
 - ③ 実際にリスク分析を実施する企業で重要と考える「災害の種類」、およびその「災害による影響度」を「JRAM質問票」の質問項目に付け加えることも含めて、「JRAM質問票」の項目見直しを行う
3. 英国のリスク分析ソフトウェア「CRAMM」について調査する
4. 「CP作成の進め方」という手順書を作成する
5. 「CP作成の概要説明書」を作成し、システム監査人協会報等を通じて、試行的にCP作成を行って見たいと考えている企業を募集する
6. 応募のあった企業に対して、研究会がこの研究結果を踏まえて、CP作成のお手伝いをする

7. これら一連の経験を「活動報告書」としてまとめる

これら活動ターゲットの作業進捗状況は以下のとおりである。

1. 「シナリオ分析票」関連

① 「情報システム稼働資源」の分類基準を以下のとおり設定

- a. 設備
 - a1. 建物、事務所
 - a2. 電源設備
 - a3. 空調・給水設備
 - b. コンピュータ機器
 - b1. 本体系；CPU、メモリ、コンソール、および関連ケーブル
 - b2. 周辺系；DASD、プリンタ、テープ、OCR、スキャナ、WS、端末、および関連ケーブル
 - b3. 通信系；CCP、TDM、PBX、DSU、WAN、モデム、回線、および関連ケーブル
 - b4. CSS (LAN)；CSS上のサーバ、CSS上のクライアント、CSS上のプリンタ/ディスク/トランシーバ/ルータ、標準装備のソフトウェア、および関連ケーブル
 - b5. スタンドアロンPC；システム構成の対象となっていないPC、標準装備のソフトウェア、マウス、PCカード、および関連ケーブル
 - b6. 事務機器；電話機、FAX、コピー機、ワープロ機
 - c. ソフトウェア
 - c1. OS；OS、ミドルS/W；CASEツール
 - c2. APL；業務用ソフトウェア
 - d. サプライ
 - 帳表；指定用紙
 - e. その他
 - e1. 磁気記録物；DBファイル、磁気媒体上のデータ
 - e2. 書類；ドキュメント、マニュアル、規定
 - e3. オペレータ (SE、CEを含む)、データ、資材などの移動経費
- ② 「災害の種類」を網羅的に列挙
- A. 災害
 - A1. 震度6以上の大規模地震
 - A2. 震度4～5の中規模地震
 - A3. 火災 (全焼)

- A4. 火災 (半焼)
 A5. 火災 (ボヤ)
 A6. 落雷 (直接的な被災)
 A7. 風水害 (台風、豪雨、津波、断水)
 A8. 水漏れ
 A9. 停電
- B. 故障
 B1. ハードウェア (本体) の故障
 B2. ハードウェア (周辺機器系) の故障
 B3. ハードウェア (通信制御機器、回路系) の故障
 B4. ハードウェア (CSS系) の故障
 B5. 電源設備の故障
 B6. 空調・給水設備の故障
 B7. ソフトウェアのトラブル
- C. 過失
 オペレーション・ミス
- D. 故意
 D1. 破壊行為
 D2. 改竄
 D3. 不正使用
 D4. 意識的な怠業
- ③ 過去の実績データから「被災時の影響度」の判断基準の設定
 具体的な設定値を規定するには至っていないが、以下のキーワードに基づいて今後、「具体的な設定値」を規定していく予定である。
- Aとaが交差する欄 (災害発生時の設備障害) に関するキーワード
 Aa1; 震度と建物および情報システム機器の一般的な損傷関係を調査
 Aa2; 地盤と建物および情報システム機器の一般的な損傷関係を調査
 Aa3; 建物の建坪率と一般的な損傷関係を調査
 Aa4; 震度とライフライン (電力、水道) の強度関係を調査
 Aa5; フロアの階数と損傷関係の調査
 Aa6; 海拔
 Aa7; 地形 (崖の近く、海、川の近く)
 Aa8; 自社のビル、雑居ビルの相違
 Aa9; 落雷頻度の地域性
- Aとbが交差する欄 (災害発生時の機器損傷) に関するキーワード
 Ab1; 通産省「安対基準」の各項目との照合
 Ab2; 郵政省「データ通信ガイドライン」の各項目との照合
 Ab3; 通産省「安対基準」の事務所環境基準の各項目との照合
 Ab4; 事務所の防火、耐震、防水状況
 Ab5; 事務所の設置地域
 Aとcが交差する欄 (災害発生時のソフトウェア障害) に関するキーワード
 Ac1; ソフトウェアのバックアップ取得方法、実施
 Ac2; ソフトウェアのバックアップの保管場所 (防火区域、外部からの取り寄せ、保管場所)
 Ac3; 現状復帰の処理要否と時間
 Aとdが交差する欄 (災害発生時の重要帳表障害) に関するキーワード
 Ad1; 帳表の保管場所 (安対基準の項目と照合)
 Ad2; 帳表再取得の所要時間
 Aとeが交差する欄 (各種災害発生時のその他の障害) に関するキーワード
 Ae1; 情報の取得方法、実施
 Ae2; 情報の保管場所 (防火区域、外部からの取り寄せ、保管場所)
 Ae3; 現状復帰の処理要否と時間
 Ae4; 書類のコピーの有無
 Ae5; 移動手段に対する代替手段の状況
2. 「JRAMによるリスク分析手法」の活用
 a. JRAMについての学習
 ・ 日本情報処理開発協会発行の「JRAMによるリスク分析」を解説終了。
 JRAMによるリスク分析の概略は以下のとおりである。
- ① 主観的側面と実態的側面の2つの方法から構成されている
 ・ 主観的側面
 ・ JRAM質問票を使用する
 ・ システムの企画、開発、運用の各部署から選出された5～6名の回答者に回答してもらう
 ・ JRAM質問票を集計して評価報告を行う
- ・ 実態的側面
 ・ 業務日報、障害報告、障害復旧完了報告、損失報告を使用する。
 ・ 業務日報
 業務日報から障害原因の調査・分析を行う
 ・ 障害報告書
 障害原因の調査・分析の結果を基にして、障害の影響、障害状況、障害処理、障害の再発防止対策を記入する

- ・ 障害復旧完了報告
障害原因の調査・分析の結果と、障害復旧対応に要した費用を記入する
(直接損失、間接損失、対応費用に区分して記述する)
 - ・ 損失報告
システムを利用している各部署が被った経営上の損失を記入
 - ・ リスク分析ワークシートを作成する
 - ・ 7月11日、システム監査学会/リスク・マネジメント研究会の集会で、SATTの田場氏が駿河台予備校における教育用パソコンLANシステムのリスク分析をJRAMで実施した事例発表に我々分科会のメンバー全員が参加
 - ・ その後、田場氏のご好意により、さらに詳細な実施時の経験談等を聴取
 - b. JRAM質問票利用の検討
 - ・ 質問項目の見直し
 - ・ 質問項目の追加
 - ・ JRAM質問票集計のためのソフトウェア開発
 - c. 実際にリスク分析を実施する企業が重要と考える「災害の種類」、およびその「災害による影響度」を「JRAM質問票」の質問項目に付け加える作業
 - ・ 未着手
 - 3. 英国のリスク分析ソフトウェア「CRAMM」について調査
JRAM開発委員長を務められた明治大学の森宮康教授にお願いして、英国大蔵省の一部局であるCCTA (Central Computer Telecommunication Agency) のDen Watts氏と折衝を行い以下の事柄を調査している。
 - a. システム監査人協会/セキュリティ分科会として、CRAMMリスク分析ソフトウェアの分析評価を行うため、
 - ・ 操作マニュアル
 - ・ システム概要説明書
 - ・ 入力画面と出力帳票のサンプルを入手したい
 - b. CRAMMソフトウェアを6~12カ月借用できるか
 - c. CRAMMソフトウェアの購入価格
 - d. 日本にコンタクト先(代理店、団体名、利用者など)はないか
- 4~7. については未着手(今後の活動項目)

技法研究会 活動報告

ソフトウェアの品質管理を輪読して

第2回 5. 品質システムの章について内容の要約

技法研究会 No.192 木村 陽一

この章では、開発の各局面での品質システムに対する要求事項が記載されている。ここでは、特定のライフサイクルモデルを意識したものでないことを明記している。(大きな意味で言えば、フェーズド・アプローチではあるが)構成としては、以下の様になっている。

- ① 契約レビュー
 - 一般
 - 品質に関する契約事項
- ② 購入者要求仕様
 - 一般
 - 相互協力
- ③ 開発計画立案
 - 一般
 - 開発計画
 - フェーズ
 - 管理(マネジメント)
 - 開発方法及びツール
 - 進捗管理
 - 開発の各フェーズへの入力
 - 開発の各フェーズからの出力
 - 各フェーズにおける検証
- ④ 品質計画立案
 - 一般
 - 品質計画の内容
- ⑤ 設計と製造
 - 一般
 - 設計
 - 製造
 - レビュー
- ⑥ テスト及び妥当性確認
 - 一般
 - テスト計画立案
 - テストの実施
 - 妥当性確認
 - フィールド・テスト
- ⑦ 検収
 - 一般
 - 検収テスト計画立案
- ⑧ 複製、引渡し及び据付け
 - 複製
 - 引渡し
 - 据付け
- ⑨ 保守
 - 一般
 - 保守計画
 - 製品の初期状態の明確化
 - 支援体制
 - 保守活動の形態
 - 星家の記録及び報告
 - リリース手順

各項目の簡単な説明と要約

「契約レビュー」とは、契約締結前に両者で契約内容について確認をすることで、契約の中に品質に関する事柄も決めておくべきであるとの主張である。

「購入者要求仕様」では、購入者が完全に決める場合と、供給者側が要求分析をして購入者側の承認を得て決まる場合がある。どちらにしても購入者側が主導権を持って決めるべき事柄であることを強調している。

「開発計画立案」では、工程をフェーズに分けてそれに対する入力と出力、フェーズごとの検証を定める時のガイドラインを規定している。また、プロジェクト全体の管理と進捗管理および開発方法とツールについて決めるべきガイドラインを示している。

「品質計画立案」では、供給者側は開発計画の一部として品質計画を定めるべきであるとする。計画の中には、品質目標の設定・各フェーズの入力および出力基準の明確化、実施すべきテストの種類、妥当性確認の明確化とそれらの詳細な実施プランと品質活動に対する責任体制を決めることを示している。

「設計と製造」では、設計・製造・レビューの各フェーズごとの品質保証の考え方が述べられている。各工程では、テストなどに頼るのではなく、きちんとした方法論を適用することで、工程で品質を作り上げていくことに重点を置くべきであるとの主張をしている。

技術研究会の議論

・全体の構成としては、どうしてもフェーズドアプローチになってしまうのですね。ダウンサイジングだとかいろいろ言われているが、まだまだ新しい開発手法が出てきていない段階では妥当なんだろうね。でも、開発手法は変わっていくのだろうね。

・本文の解説にもあるが、契約のタイミングというのは難しいのだろうね。要求がきちんと決まっていればいいのだけれどね。「在庫管理をやりたい」という要求だけで見積りも出来ないよね。営業段階での提案書での見積りやスケジュールで契約だと言われたら問題あるよ。

・システム・インテグレーションなど言われているが一括請負の技術等確立されているのかな。特に戦略的システムなど言う場合は経営的

な判断が必要でありシステム屋が要求を全部まとめられるかという問題だよ。

・ユーザーの方も判っていないじゃない。だれも判らないから、業者に丸投げしたらという無責任もあるよ。

・それは無茶苦茶だよ。でも、ダウンサイジングなど言われて経営者が情報システムはもっと安くできるんだということを聞くと、すぐに検討することになって右往左往することはあるね。そんな時には、誰も正確な要求仕様なんて判っていないんじゃないかな。

・開発計画立案のところは、そんなに議論すること無いような気がするんだけど。従来のやり方をやればいいので、結構各企業でも確立されているのではないかな。・そうだよ、でも品質計画立案では個々の品質を定義するのは難しいよ。レビューのタイミングやテストの種類等は決められるが、テスト完了基準なんかをどのように決めればよいのかなんて経験そのものだよ。バグ発見の累積カーブなんかを描いてやったりしてね。

・どうしても、これさえやればバグが無くなるという万能の方法論やツールを求めたくなるね。この本読んでても、その辺が書かれていないので欲求不満になるものね。

・でも、それを求めるのは無理だよ。絶えず、この本にあるような体系立ったやり方で絶えず品質を向上させる努力をしていくしかなんいだと思うよ。そここのところがこの品質保証の精神だと思うんだけど。

・システム監査でも同じだけど、監査という事をきちんとやりながら絶えず作業者の意識付けを行っていくことが必要なんだと思うけど。マニュアル・チェックリストで作業者が決まってることは規定して極力、一から考えることを少なくしていくことや標準化について見習うことが必要ではないかな。

・日本では、どうしても自分のところは異なっている、また、これは現状に即していない等の反発が先に来るもんね。もっと、素直になって、利用できるものはどんどん利用していいものを作り上げていくことが必要だと思うがね。

・だんだん、文化論になってきましたね。さて、この章の途中だけど、時間もそろそろで、この文化論の続きは別の場所でやりましょうか。

システム監査人日誌

第8回 No.39 川野 佳範

平成4年1月30日木曜日

結局、昨夜は食事のあと久留米の繁華街である六ツ門に社長を除いてみんなで繰り出した。最初は気が張っていて猫を被っていたが、大好きなワールドタキーが喉元を過ぎる度徐々に酔いも回ってきて11時過ぎてからはカラオケまで謡いだしてしまったようだ。酒も歌も嫌いでない私は酔いが回ると“酒を飲むのもカラオケで歌うのも仕事のうち”と勝手にうそぶき質(たち)が悪い。私どもは仕事の関係で全国各地に出張することが多く、昨夜のように関与先の人に誘われることも少なくないため、私は各地の“ご当地ソング”を予め覚えていってよく歌う。

昨夜も恥も外聞もなく

久留米餅の 機(はた)を織る
母にかさなる 筑後川
今もこの胸 やさしく洗う
清き流れよ いついつまでも
……いついつまでも

と、作詩：吉田 旺/作曲：弦 哲也 の曲を尾形大作になりすましたように“筑後川”を吟り出したようだ。

そんなことでハイネスホテルにチェックインしたのが12時過ぎとなってしまった。

今朝は予定外の久留米泊となったためジョギング・シューズとウェアの用意がなく日課にしている朝のジョギングはできなかった。

7時22分に福岡行き特急に飛び乗り福岡に。8時少し過ぎに西鉄福岡駅に着き、直ちに福岡での宿である西鉄グランドホテルに立ち寄り、慌ただしく身の回りの物を整えポストンバックに詰め込みチェックアウトスする。今週月曜日からシステム監査を始めている(株)ニコニコ・クレジットに赴いた。

今回のシステム監査は私を含め3名で実施している。トーマツ東京事務所システム監査部の山内さんと福岡事務所マネージメント・コンサルティング部門の藤田さんである。二人は、昨日私が久留米に会計監査に行っている間も(株)ニコニコ・クレジットでシステム監査を継続してやっていた。山内さんは、コンピュータセキュリティに関する監査を、藤田さんは業務処理統制の監査を担当している。

山内さんは

1. 情報セキュリティと災害復旧対策のための適切な方針および計画の策定

2. 情報セキュリティ管理者の職務権限の妥当性
3. 情報セキュリティの基準・手続き規定の有無とその適正性
4. データのオーナー、エンドユーザおよび情報システム部員に対する情報セキュリティ・レベルの適正性
5. 情報システムを取り巻く脅威に対する情報資産ごとの適切な分析
6. アプリケーション開発にあたり情報セキュリティに関するコントロール設計が適切な組み込
7. アプリケーション・プログラムの未承認変更に対する発見的コントロール機能
8. 情報資源のバックアップ体制
など20項目について監査している。

私は、ニコニコ・クレジットの監査執務室に入る暇もなく山内さんに

「山内さん進捗状況はどうですか。何か指摘すべき事項がありますか？」と質問する。

「そうですね、今のところは……そう、特権命令を利用できる人が4名もいまして問題ではないかと思えます。特権命令はセキュリティ管理者のみに限定すべきだと思います。それに人事異動があってもアクセス権限テーブルがメンテナンスされていないようです。人事異動の情報が的確に情報システム部門に流れていないようです。」

「そのかほに何か有りますか？」と私。

「はい、アプリケーション・ソフトのバックアップ体制が良くありません。データについては外部にバックアップ保管しているのに、アプリケーション・ソフトについては外部保管されていません。この建物以外の安全な場所に保管しておく必要があると思います。」と山内さん。「それに情報セキュリティと災害復旧対策のための適切な方針や計画も策定されていません。当社の業務は情報システムに大きく依存しているのでセキュリティ・レベルについて全社的に考えておく必要があります。」と何時もまじめで固い表情の山内さんが今は笑みを浮かべながら報告してくれた。

「藤田さんの方はどうですか。」と私。

「今のところ順調で特に報告しておくことはありません。」と藤田さんがちよつとぶっきらぼうな言い方で答えた。藤田さんは頭の回転が速いので話にも無駄がなく、また鋭いためぶっきらぼうに聞こえることがある。

その時、監査室長の力久さんが監査室に静かに入ってきて「川野先生……。急なことですみませんが今日10時から経営委員会がありまし

て、今日のテーマは「わが社の今後の情報システムのあり方」についてなのです。そこで社長が言いますのは、折角川野先生が来ているのなら川野先生にも経営委員会に出席してもらって意見を述べてもらったらいいだろうということなのです。先生どうでしょう……。」と例の揉み手をするような感じの姿勢で話す。

「そうですね。監査人はインデペンデントでなければなりませんから経営の意思決定の場に出席することはどのようなものかと思えますね。どうでしょう……？」と腹の中では今回のこの業務が会計監査ではなく業務監査の側面からのシステム監査であるので、それほど独立性に関して神経質になる必要はないと思っていながら、取って監査室長にはもったいぶって、じらすような言い方をした。

「そうですね。……そうですね。独立性は大事ですね。独立性は……。わかりました社長にはその旨……。」

「ちょっと待って……力久さん。」私の言葉を真に受けたのに私があわてて。

「行きますよ！～。勿論委員会の席に。行きますよ～。」と。そして“それじゃ～。アウトソーシングについて一席ぶってこようか”

(つづく)

新刊紹介

「システムアナリスト試験重要用語集」

日本能率協会マネジメントセンター刊

約250頁 2500円

荒川幸式(システムアナリスト部会担当理事)編・著

これまでの情報システム構築は、個々の要求に対して、その都度に個別に対応してきたといつてよい。その結果、情報システムは各所で不整合を起こして保守は困難を極め、新規開発力を失わせる大きな要因となっている。

さらに重要なことは、経営戦略とはあまり関係なく開発が進められてきたことである。経営戦略に一致しない情報システムは、効果の点において有効なものとはなり得ない。費用ばかりかかって十分な効果が上がらないことに、情報システム部門は厳しい反省を今日迫られている。

このようになった原因は、情報システム部門に開発のエンジニアはいても、経営戦略が理解でき情報戦略や情報システム開発の全体計画を立案できるシステムアナリストがほとんど育っていないことによる。

経営戦略が情報戦略に影響を与えることは当然であるが、情報戦略が経営戦略に影響を与え

るようになった今日、企業にとっては、その橋渡しができる人材であるシステムアナリストの養成が重要なテーマとなってきた。

そこで平成4年12月に「情報化のための人材像」と題する中間報告が、通商産業省産業構造審議会情報産業部会人材対策小委員会より公表され、さらにこの報告に基づいて本年度よりシステムアナリスト試験が実施された。

この本は、システムアナリスト試験の出題範囲である旨が公表されている標準カリキュラムで示されている重要用語350余について、その簡潔な定義を示し説明を加えている。

収録した用語は、システムアナリストとして理解して置くべき重要な用語でもあるが、システムアナリストの担当する業務も、システム監査の対象領域に当然含まれることから、同時にシステム監査人にとっても理解が望まれる用語にもなっている。

目次は次のとおりである。

第1部 情報システムの基本的知識

第1章 経営一般

第2章 情報システム

第3章 情報システムの評価と監査

第4章 リスク分析と情報セキュリティ

第2部 情報戦略の立案

第1章 企業環境の把握

第2章 情報戦略の策定

第3部 情報システムの全体計画立案

第1章 全体計画の必要性

第2章 全体計画立案の方法

第3章 業務モデルの定義

第4章 情報システム体系モデルの定義

第5章 情報システム開発課題の分析

第6章 情報システムの中長期計画の立案

第7章 計画の評価・承認

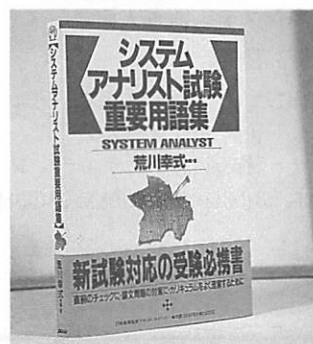
第4部 開発計画の立案

第1章 開発計画の進め方

第2章 システム化の目的とその範囲の定義

第3章 システム化計画

第4章 開発計画書の作成



新規入会個人会員

番号	氏名	勤務先・所属
668	島 潟 与 明	秋田職業能力開発短期大学校 情報処理課
669	永 田 仁	(株)プライムシステム開発
670	大河内 実	日本電気(株) インフォメーションシステム部
671	早 川 正 彦	ライオン・アクゾ(株) 管理部
672	兵 藤 浩	
673	古 井 伸 幸	(株)エー・シー・エー 経営企画室
674	奥 居 裕 明	安田火災海上保険(株) システム開発部第2PJ室

事務局からのお知らせ

I) 中国支部が開設されました

日本システム監査人協会規約第3条の規定により、平成6年10月13日の理事会で、以下のとおり中国支部の開設が決議されましたのでお知らせいたします。

連絡先：〒734 広島市南区翠5-10-18

(有)オフィス・あん 内

Tel 082(255)5138 FAX 082(505)0199

支部役員：支部長 安原 節男(会員番号387)(有)オフィス・あん 代表取締役

副支部長 桑原 英明(会員番号295) 桑原公認会計士事務所 公認会計士

II) ISACA(旧、EDPAA東京支部)月例研究会への参加が可能になりました

システム監査関係諸団体との交流の成果として、日本システム監査人協会とISACAとの月例研究会の相互乗り入れが実現しました。今後、日本監査人協会会員はISACAの月例研究会にメンバー料金で参加できることになりました。

なお、この月例会の案内は、時間的また財政的理由から会員宛に直接通知することができません。当面、協会運営のパソコン通信(ニフティー・サーブのホームパーティー)上で日時等のお知らせを行う予定です。当協会員である旨を明記してご参加下さい。

[ISACA-イサカとは]

ISACAは米国のInformation Systems Audit & Control Associationの略で、今年から名称が変わったものである。今までは、EDPAA(EDP監査人協会)で知られていた協会、日本には東京支部の他に、大阪支部、名古屋支部がある。

米国のCISA(Certified Information Systems Auditor)試験の合格者を中心にした団体であり、システム監査とコントロールに関する啓蒙と教育を目的に月例会などを活発に開いている。

昨年はシステム監査学会などと「システム監査アジア太平洋会議」を主催したように、国際的な活動がその性格上も活発である。(編集部注)

発行所 日本システム監査人協会

発行人 川野 佳範

事務局 〒151 東京都渋谷区笹塚1-64-8

笹塚サウスビル7F

(株)産能コンサルティング内

TEL 03(5350)9268 FAX 03(5350)9269

※ご連絡はなるべく郵便または、FAXをお願いします

会報担当(ご投稿、ご意見、ご要望は下記まで)

徳武 康雄 富士通(株)

TEL 03(3778)8281 FAX 03(3778)8106

金子 長男 (財)公営事業電子計算センター

TEL 03(3270)7471 FAX 03(3270)3998

橘和 尚道 システム監査コンサルタント

TEL 0423(69)0639 FAX 0423(69)0639

木村 陽一 日本レジホンシステムズ(株)

TEL 03(5286)7231 FAX 03(5286)7203

山内 美佐子 伊藤忠テクノサイエンス(株)

TEL 043(285)1892 FAX 043(285)1889