特定非営利活動法人
日本システム監査人協会報

2010 年 9 月発行
No 115

～システム監査を通じて、ITと経営の融合とビジネス課題の解決を支援する～
日本システム監査人協会 電子版 http://www.saaj.or.jp/

◇◆ HOT TOPICS ◇◆

【本号の掲載内容】

◇◆ めだか ◆◇ 監査人のコラム(投稿)

〖 情報通信技術戦略の抜本的な刷新 〗

政府は5月に「新たな情報通信技術戦略」を発表した。
日本経済新聞8月18日付朝刊に、担当大臣である川端文科相兼内閣府特命担当相のインタビューが載っている。川端担当相の談話では、・・・

【続きはこちらで読めます】 http://www.skansanin.com/saaj/

〖 失敗を通して学んだシステム監査の勘所 〗

私は、約19年、さまざまなテーマ・対象でシステム監査を行ってきました。1つ1つがそれぞれに思い出深い経験であり、数を重ねるたびに少しずつですが成長している実感があります。
経験の浅いときは会社で作った手引書や市販本を参考にしながら、・・・

【続きはこちらで読めます】 http://www.skansanin.com/saaj/

コラムは、投稿者の個人的な意見表明であり、SAAJを代表する見解ではありません。

◇◆ 注目情報(9/1～9/30) ◆◇

◆ METI 経済産業省(2010/8/16)

「クラウドコンピューティングと日本の競争力に関する研究会」報告書の公表

～経済産業省はクラウドコンピューティングを応援しています！！～

【詳細はこちら】http://www.meti.go.jp/press/20100816001/20100816001.html

◆ IPA 情報処理推進機構(2010/8/13)

「インターネット上のサービスにおけるプライバシについての調査結果」を公開

【詳細はこちら】http://www.ipa.go.jp/about/press/20100813.html

◆ NISC 内閣官房情報セキュリティセンター(2010/7/31)

「重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針」

【詳細はこちら】http://www.nisc.go.jp/active/infra/siryou.html#infra_pl

◆ JIPDEC 日本情報処理開発協会(2010/7/23)

ITSMSハンドブック公開

「as a Service時代の処方箋～ITサービスマネジメントシステムとは～」

【詳細はこちら】http://www.isms.jipdec.jp/itsms/doc/JIP-ITSMS113-10.pdf

◇全国のイベント・セミナー情報◇

■『SAAJメール通信 全国版』

システム監査に関連する最新情報を収集して、毎月発行しているメルマガです。

お申し込みは無料。職場の同僚の方に是非、ご紹介下さい。(SAAJ会員は登録不要です。)

《登録はこちら⇒⇒ http://www.skansanin.com/saaj/ 》

■【東京・月例研究会9月】

「大規模システム開発におけるプロジェクト・マネジメントの実際」をテーマに、『(株)百五銀行と共同開発した、次世代オープン基幹系システムの開発プロジェクトについて、大規模プロジェクト管理・運営における重要成功要因や勘所について。また、システム稼動後の各種監査の実態について』

日本ユニシス株式会社の葛谷 幸司様に、ご講演を頂きます。

開催日は9月28日(火)18時30分より。会場は、お茶の水総評会館です。

【詳細、申し込みはこちら】http://www.saaj.or.jp/kenkyu/kenkyukai158.html

■ 公認システム監査人特別認定講習の実施についてのご案内
【詳細はこちら】http://www.saaj.or.jp/csa/tokuninannai.html

■ 平成22年度秋期 公認システム監査人およびシステム監査人補の募集について
【詳細はこちら】http://www.saaj.or.jp/csa/csaboshu.html

■【近畿支部セミナー】
日本システム監査人協会 近畿支部では、地元で参加できると好評の
システム監査の実践講座を開催しています。

企業活動の中でITの役割はどんどんと大きなウエイトを占めてきています。
内部統制という面から見てもシステム監査は重要ですね。
内部監査に携わられる役員様、ご担当様にも好評です。
システム監査入門セミナー(1日コース)は、費用面でも内容面でも
とってもお値打ちなセミナーです。
システム監査の概要が学べます。日程等の詳細は、【続き】を確認ください。

※ 9月25日-26日開催「システム監査実践セミナー」は申込受付中です。
【続きはこちら】http://www.saaj.or.jp/shibu/

◇◆ 会員限定記事(9/1～9/30) ◆◇

【本部・理事会議事録】(会員サイトから閲覧ください。パスワードが必要です)
1)7月の理事会の議事録

■発行: NPO法人 日本システム監査人協会 会報編集部
〒103-0025 東京都中央区日本橋茅場町2－8－8共同ビル6F
■ご質問は、下記のお問い合わせフォームよりお願いします。
【お問い合わせ】http://www.saaj.or.jp/

会報電子版の記事

目次

〖情報通信技術戦略の抜本的な刷新〗

政府は5月に「新たな情報通信技術戦略」を発表した。

日本経済新聞8月18日付朝刊に、担当大臣である川端文科相兼内閣府特命担当相のインタビューが載っている。
川端担当相の談話では、
「従来は、役所の事務処理の簡便化が主眼でしたが、今回はあくまでも利用者の利便性を追求しました」、
「また、IT戦略本部の下に関連省庁の副大臣級で構成する『企画委員会』を設け、政治主導で検討・実行できる体制を敷くことで、実施状況を厳しくチェックし、役所の壁を超えて横断的な政策をとれるようにしました」
と、ある。

すでに何回か実施されている政府の情報通信技術戦略展開の反省を踏まえてのようであり、結構なことである。

ただし、もう少し、一点集中的な設定はできないのであろうか。

例えば、今度の「新たな情報通信技術戦略」では「国民ID制度」といわれている制度設計の日限設定である。

国民IDは、所得隠しなどしなくていい立場とすれば、なるべく広い範囲で使えるものとしたい。しかし、所得隠し以外の動機として国家管理に対する反発などもあるから、適用範囲は、政治主導で決めてもらいたいが、設計推進も、政治主導でやってもらわないと、できない。

今の中央省庁すべてに関係し、他にも自治体の意見も聞かなければならない。

この根幹システムの姿が明示されれば、他の関連するシステムも構想が立てやすくなるはずである。「情報戦略」のあり方としては、このような設定もあるのではないか。

また、今度の「新たな情報通信技術戦略」の中には、国民が全国どこにいても自分の医療情報を基に診察が受けられる「どこでもMY病院」構想があるという。

一方、漏れ聞くところでは、カルテの電子化は実施が危ぶまれている。
カルテの電子化がなくて、医療情報の共有化ができるであろうか。

カルテの電子化支援も解決すべき課題は多い。

カルテ記述がどのくらい英語で、どのくらいドイツ語かは知らないが、医師の端末に、これらのフォントを搭載しなければならない。

すべての医師が、キーボードをブラインド・タッチで操作することは期待できないであろうから、入力のところで、頻出する単語については、すべてを入れなくても、いくつかの候補をすぐ表示するなど、きめ細かい支援を考えるべきであろう。

情報処理技術としては、入力の際の隘路が除かれれば、あとはラクである。

医師が他人に自分のカルテを見せたくないという心理的障壁は、電子化しなければ経済的その他の面で不利になるなど、対応策はあるであろう。

カルテ電子化の達成時期が明示されれば、「MY病院構想」は、より早く実現できる。

患者の利便とともに、医療費削減の大きな契機になるに違いない。

政府の情報通信技術戦略の組み方としては、一点集中主義を考えたいものである。　以上（太郎冠者）

（このコラム文書は、投稿者の個人的な意見表明であり、SAAJの見解ではありません。）

〖 失敗を通して学んだシステム監査の勘所 〗

私は、約19年、さまざまなテーマ・対象でシステム監査を行ってきました。1つ1つがそれぞれに思い出深い経験であり、数を重ねるたびに少しずつですが成長している実感があります。

経験の浅いときは会社で作った手引書や市販本を参考にしながら、試行錯誤でやってきましたが、いろいろと失敗をしました。そうしたとき、自分なりに考えて工夫し、また、先輩にアドバイスをもらったりしながら、自分のノウハウを高めてきました。今回は、失敗を通して学んだシステム監査の勘所のいくつかを、ご紹介します。

1．玉虫色の表現のシステム監査報告書を経営者は期待していない

システム監査を実施した結果は、システム監査報告書にまとめて報告します。システム監査報告書では、監査対象の実態が、監査基準に照らしてどのような水準にあるかを、監査人の評価として記載します。私がシステム監査を始めて間もない頃、お客様のシステムの監査でしたので、歯切れの悪い、玉虫色の評価を記載してしまいました。「･･･一部に問題と思われる状況が見受けられ、必ずしも適正な水準にあるとはいえない。」のような。報告会でお客様の経営者から、次のように言われました。これはどういう評価なのか、改善が必須なのか、改善を検討すべきなのか、改善は必要ないのか、はっきり言って欲しい。お金を払ってシステム監査を頼んでいるのは、問題をはっきりさせたいからだ。私が、経営者がシステム監査に期待していることを理解できていなかったのです。

それ以来、私は、評価は客観的に、明瞭に、端的に記述するように注意しています。3段階評価のどの水準にあるのかを明記し、その理由を、具体的証拠をもって説明するようにしました。

2．記録の提出の要求を、相手に、記録がないことの指摘と思わせてしまった

監査を実施する中で、「○○の記録があったら見せてください。」という要求をすることは、ごく一般的な手続きです。監査対象の実態を知るために記録を確認することが目的です。これも、私がシステム監査の経験があまりない頃ですが、そのように言ったところ、次のヒアリングのときに、被監査部門の方が、○○記録を作りましたから見てください、といって持ってきました。私の言ったことを、○○記録がないのは問題だから作るように、と指摘されたと理解してしまったのです。私の説明が足りなかったのです。

それ以来、記録はあれば見せてください、なければそれが今の実態であり、監査報告書で○○記録を作成する必要があるという指摘をしたら作ってください、という説明をしています。監査の実施段階は実態を把握する段階であり、問題点を指摘する段階ではない、ということを説明しています。

3．プロジェクトの監査で、PMに、自分の管理能力不足を指摘されたと思わせてしまった

これも、私の説明不足に起因することでした。プロジェクト体制で進められているシステム開発段階の監査を行ったときです。進行しているシステム開発のある時点でシステム監査を行い、プロジェクトの成功に必要な改善事項（過ぎた工程の問題はあまり指摘せず、ほとんどがこれからの工程で採り入れて欲しいこと）を指摘しました。それをそのプロジェクトのPMに報告したところ、PMが自分の管理能力を問題視されたと思ったらしく、猛反発、最後には自分をPMから下ろしてくれと言い出しました。プロジェクトを成功させることが監査の目的であり、PMを含めたプロジェクトチームの不備を指摘するものでは決してないことを何回か説明し、ようやく理解してもらいました。

それ以来、監査の指摘は、システムそのもの、およびシステムに関連する仕組み・プロセスに対する指摘であり、そこに携わっている人たちに対する指摘ではないことを、折に触れて説明しています。

後の2件は、いずれも私の説明不足が失敗の原因であり、システム監査を受ける人たちは初めての経験という人が多いことを踏まえて、最初にまた途中でも、きちんと説明していくことに心がけています。

以上（おのおのがた）

（このコラム文書は、投稿者の個人的な意見表明であり、SAAJの見解ではありません。）

「東証新売買システム(arrowhead)の開発経緯について
～上流工程の取り組みとその効果～」

(SAAJ会報 2010.09)

■第153回月例研究会
「東証新売買システム(arrowhead)の開発経緯について～上流工程の取り組みとその効果～」
日時 2010年4月27日(火) 18時30分～20時30分
場所 御茶ノ水 総評会館
講師 株式会社東京証券取引所 常務取締役兼CIO 鈴木 義伯 氏

●アジェンダ
1. arrowhead開発の背景
2. 非機能要件への取組み
3. arrowhead稼動後の状況
4. プロセス改善の取組み(発注者責任の明確化)
5. arrowhead成功の鍵

●講演概要
0. はじめに
「2年前に新システム構築の取組みについて話をさせて頂いたので、今回はそのプロセスを監査されるような感じを持っています」と、冒頭の会場の雰囲気を和らげる一言で講演が始まった。また「東証に初めて行ったときは、社会インフラの障害で、あれほどバッシングされるものかということを感じたが、逆に底からのスタートであり、やりやすいということもあった」という事情や、「受注者としての経験より、発注者として遡及契約の禁止を決めて徹底した。結果、現在の東証では99%遡及契約はなくなっている。発注者側がそれをきちんと守れば、遡及契約はなくなる」といった意識変化についても冒頭に語られた。

1. 開発の背景
(1) 市場を巡る変化
株式市場における取引は、計算機からの発注の比率が大きくなり、その執行タイミングが重視され、当時の東証は1件の執行に2～3秒、世界は10ミリ秒であり、システムの性能面で、東証は世界の要求から大きく遅れていた(ニューヨーク取引所では70%～80%が計算機からの執行であった)状況であった。市場の評価は、上場企業数や規模あるいは透明性といったものから、システム(IT)の性能が重視されるように、市場を巡る環境変化が進展していた。我が国の金融資本市場を円滑に機能させるためには、取引所市場が高い流動性を確保し、高度な価格発見機能を維持し続けることが必要であり、そのためには市場を巡る要求に応える新しい情報システムが必要であった。

(2) 市場に求められるニーズ

注文・約定処理の高速化、取引注文の小口化、取引件数の急激な増加といったニーズに対応するため、次世代システム「arrowhead」を平成22年1月4日に稼動させるに至った。

(3) 基本コンセプト

基本コンセプト(コアファクタ)を以下を取りまとめて提示した。

・安全性／拡張性:拡張基準を超過した場合の拡張を1週間程度で実施する。
・高速性:注文受付通知レスポンスを10ミリ秒以下(2ミリ秒以下を実現)、また
FLEXによる情報配信のレイテンシーを5ミリ秒以下(3ミリ秒以下を実現)
・柔軟性:多様な商品や取引ルールの追加、変更に短時間で対応可能とする。
・堅牢性:99.999%以上の可溶性の確保。主要なサーバは三重化する。
セカンドサイト(バックアップセンタ)の構築、24時間以内復旧
・その他、情報配信機能強化、システム運用堅確化、セキュリティ強化

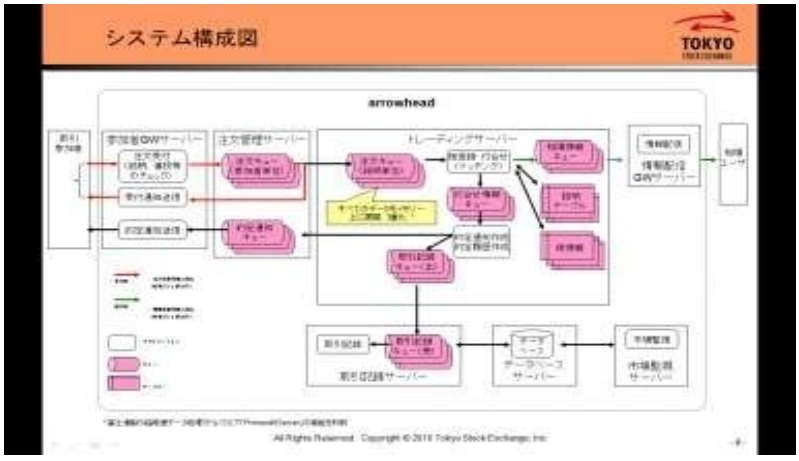
(4) arrowhead特徴

新システムの特徴を列挙すると以下のものがある。

・証券会社システムとarrowheadとのシステム間接続仕様書の変更
・市場情報の拡充
・市場監視機能の拡充 ～通常でない、または不正取引の監視機能を高速化して実現
・セカンダリサイトの構築
・arrownetの構築
・テスト環境の充実 ～セカンダリサイトを利用して本番同等のレベルで平日にテスト実施が可能であり、システムの早期の安定、信頼性向上を図るほか、開発者の労働環境の改善にもつながるものである。
・取引参加者端末はバックアップ機能に特化した端末を提供し、既存端末は使用不可。

(5) システム構成

システム構成の特徴としては、まずサーバーの三重化である。注文管理サーバー、トレーディングサーバー、取引記録サーバーは三重化されている。これだけでなく、すべてのデータをメモリ上に(三重に)展開して、高速化を図っている。三重化されたサーバーは動機をとっており、3台同時に停止しない限り機能提供が可能な構成である。また、すべてのデータをメモリ上に置くことにより、メモリとCPUの性能(およびネットワークルータの性能)が上がることで、システム性能が上がることを意味する。これにより、注文受付通知レスポンスを2ミリ秒、情報配信を3ミリ秒で実現できている。



(システム構成図、当日配布資料より)

また、東証プライマリサイト内に取引参加者のサーバを(ラック売りして)設置するコロケーションサービスという、新しいビジネスモデルが出現して、利用が進んでいる。

2. 非機能要件への取り組み

arrowheadは性能(高速性)、拡張性、信頼性といった非機能要件の実現を追及したシステム方式となっている。各要件の実現のために、要件定義／外部設計工程において各マネジメント計画書や実装規約を策定することをはじめとしたマネジメントを以下のとおり実施した。

・性能マネジメント

ミリ秒レベルの応答性能、40万件/分スループットを実現するために、各工程での性能設計・実装を評価し、目標との充分管理を行うマネジメントである。

具体的には3重化サーバの同期更新を実施した場合、情報配信に7ミリ秒かかっていたものを、詳細設計で同期更新を廃止するという方式変更を実施し、結果2ミリ秒の性能を出した、といった事例があった。

尚、性能実現は特にリスクが高いため、性能評価のチェックを第三者の専門家に依頼して実施した。このチェックなくして、本システムのレベルの性能を実現するのは難しかった。

・拡張性マネジメント

増大するトラヒックに対応して1週間でのキャパシティ拡張を実現するために、拡張手順の策定、拡張性の実装(阻害要因の排除)を目的とするマネジメントである。

実際に拡張性の検証をシステム稼動前が実施しているが、同様の例は皆無であろう。

・信頼性マネジメント

稼働率99.999%実現のために、信頼性を確保する実装の確認と信頼性定量化、障害発生時の局所化と切り替え時間の短縮を目的とするマネジメントである。

3. 稼動後の状況

arrowhead稼動後、東証自身で各種の稼動状況のデータを収集し分析を実施している。
主な指標とその傾向は以下の通りである。

(1) 注文件数／約定件数／約定率

注文件数の増加と約定件数の微増という傾向が見られる。ただし、約定率は低下傾向にあるが、これは注文の小口化が進んだ結果が要因であろうと分析している。

(2) TICK(値刻み＝約定)回数

個別銘柄毎、および全銘柄平均のTICK回数を集計しているが、全銘柄平均で2倍程度増加しており、市場が取引しやすくなったということが言え、本システム構築の目論見のひとつは達成されていると考えられる。

(3) 時間帯別情報配信件数推移

情報配信数は一日を通して大幅に増加しており、旧システムの3倍以上の情報量となっており、データ利用価値が増大していると考えられる。

(4) 時間帯別の注文受付レスポンス推移

注文受付レスポンスは概ね公表値5ミリ秒未満の2ミリ秒で安定しており、日中を通じてほぼブレがなく、一定のレベルを保っていることがわかる。

(5) 時間帯別の情報配信時間推移

情報配信時間についても、公表値である3ミリ秒未満の2ミリ秒前後で安定している。

4. 開発プロセス改善の取組み

arrowheadにおける開発プロセス改善は以下の項目からなる。

・発注者責任の明確化
・フィードバック型V字モデル
・リスク管理

(1) 発注者責任の明確化(RFP、要件定義、国際入札)

概略のみのRFPを提示し、要件定義をベンダー任せにして、出来上がるのを待つといった従来の上流工程のあり方を改め、RFP・要件定義書を東証自身が詳細まで作成し、それを提示してベンダー選定を行うプロセスをとった。このプロセスでコストを掛け、上流工程をきちんとやることにより、結果として、下流でコストを取り戻せるという考えが根底にあった。

開発ベンダーの選定に当たっては、国際入札を実施することで(実際に国外からの応札あり)国際競争力のある価格となることを目論んだ。また、RFPで、開発工程の次工程に

進むためには、東証の承認を必要とする条件を盛り込むなど、発注者側の関与・責任を明確なものとした。

(2) フィードバック型V字モデル

従来のV字型開発モデルでは、上流工程でのミス・誤りほど、後の工程で発見され修正が行われることになり、手戻りの工数・コストが大きくなる。この改良型として、設計と並行してテスト項目を作成するW字モデルがあり、これは非常に有効であると認識している。arrowheadにおいては、Wモデルに加え、各工程で前工程における設計の不備を積極的に見つけフィードバックする「フィードバック型V字モデル」を採用した。このモデルのやり方そのものは、実際に行われている場合もあったが、それが明示化されていなかったため、今回明示して実施することとした。

フィードバック型V字モデルは大きな効果があった。特にコーディングにおいて、設計書のバグ(もしくは設計書の漏れ)を発見する部分が最も大きかった。バグ、要件定義の変更の推移を、東証で分析を実施した結果、障害(バグ検出)の推移は、コーディングでの取り組みで大きく異なることが分かった。実際に、コーティングでの設計書の不備を見つける作業を、ちゃんと実施したチームとそうでないチームの品質に大きな差が出ており、”肝はコーディング”であったという結論に達した。

(3) リスク管理

arrowheadプロジェクトにおけるリスク管理の特徴は以下の通りである。

①リスクの洗い出しとリスクスコアの算出

検出されたリスク毎にリスク発生確率レベルと影響度でスコア付けを実施し、管理対象リスクを決定する。

リスクスコアの算出方法は、「発生確率レベル(7段階) *影響度(3段階)＝リスクスコア」とし、リスクスコアが3以上のリスクを管理対象とし、リスクスコアが6以上のリスクを工程会議でモニタリングすることとした。リスクの洗い出しを、要件定義終了後、東証と開発ベンダ共同で実施した。

②リスクの低減計画と予定／実績管理

リスクスコアの低減計画を策定し、予定／実績管理を実施し、必要に応じてアクションを打つ(リスク管理におけるPDCAサイクル)。

③プロジェクト全体のリスク状況把握

管理対象の全リスクの予定スコア合計と実績スコア合計を比較することで、プロジェクト全体のリスク低減状況を把握した。リスクは可視化しやすく、まだ工夫の余地はあるはずと思われる。

また、arrowheadにおける要件変更の工程別推移を、ベンダ発見と東証発見に分けて統計をとった。

・東証発見分については83%がプログラミング前に発見している。結合テストで10%弱の発見があるが、その殆どがプログラム修正に至らない軽微な文言修正であった。これは、要件定義書、外部設計のバグは実際にそれを書いた人間でないと見つけにくいということであろう。

・ベンダ発見分については、プログラミング前までで73%を発見し、残りは製造・テスト工程において発見しており、その殆どがプログラミング修正が必要な案件であった。

5. arrowhead成功の鍵

①危機意識の共有

②発注者責任の明確化

要件定義、外部仕様まで東証の責任での作成。

要件定義書・外部設計書を一字でも変更する場合、要件変更扱いとして、CIO承認案件として発注者の責任で修正し、変更1件ごとに発注することの徹底。

③リスク管理の可視化

④経営責任者によるプロジェクト推進体制構築

⑤上流工程完璧主義

要件定義書の記述レベルの詳細化、記載内容の網羅性チェックの徹底。

受入テスト項目を上流工程で作成して、要件の充足性・要件品質の早期確保(おけるW字モデルの採用)。

⑥前工程の質は次工程で確保

フィードバック型V字モデルの採用

●所感

証券取引所の基幹業務という経済活動を支える重要な社会インフラである情報システムの開発に当たって、性能・信頼性を確保するための実際の取り組みが明快に紹介され、強い意思が伝わるインパクトのある講演であった。発注者責任の明確化、信頼性確保のためのフィードバック型V字モデルおよび開発プロジェクトの統計的分析など、ユーザ企業としてのシステム開発を進める上での理想的なありかた～多くのベストプラクティスを示したプロジェクトであったことが明確に伝わる内容であった。システム監査に携わる者のとして、こういった開発プロジェクトの姿に触れることができたことは、自身の業務への取り組みを考える上でも非常に有益なものであった。

(No.693 福田 啓二)

■講演テーマ:　情報セキュリティ検証業務
「日本公認会計士協会　IT委員会研究報告第　39 号」の解説

講師:　有限責任監査法人トーマツ　パートナー　公認会計士　　和貝　享介　氏

講演日時:　2010　年 8 月 27 日 午後　6 時半から
場所: お茶の水 総評会館
参加者:　90　名程度

■講演の概要

保証業務の概念

協会では、厳格に財務諸表監査以外には監査(　Audit　)という言葉を使わないため、本日の話は、検証(　Examination　)という言葉を使っている。グローバルの保証業務の基準として ISAE3000　があるが、これが基になっている。日本では、協会で公表された研究報告として「監査・保証実務委員会研究報告第　20 号、公認会計士等が行う保証業務等に関する研究報告」が 2009 年 7 月に出されている。今回の情報セキュリティ検証業務は、その 20 号及び「 IT に係る保証業務等の実務指針(一般指針)」　IT 委員会報告第 5 号に関連した研究報告である。

合理的保証業務(積極的形式結論)と限定的保証業務(消極的形式結論)があるが、今回の情報セキュリティ検証業務は、前者の方である。ただし、100%保証するのではなく、許容可能な低い水準に保証業務リスクを減少させることにある。

情報セキュリティ検証業務の概要

主題に責任を負う者(検証してもらいたい人)が主題と主題情報(検証対象)について経営者の記述書を作成し、これを検証する業務実施者(公認会計士等)がいる。業務実施者は、主題を評価又は測定するための基準(情報セキュリティ評価基準)に照らして、その結果を検証報告書にし、その報告書を想定利用者が利用することになる。

その検証報告書は3つにわかれている。最初の 1 枚目が独立した監査法人の情報セキュリティ検証報告書(大きくは概要区分と結論区分の 2 つにわかれる)、　つ目には、経営者の記述書であり、経営者の評価書の対象範囲が記述される。3 つ目には、経営者の評価書(検証対象)が記述される。さらに、経営者は経営者確認書を用意する。経営者は主題と主題情報について全公開したこと等を文書で宣言し、業務実施者に経営者確認書を提出することになる。

情報セキュリティ評価基準は管理規準とコントロール規準に分け、3 階層で作成されている。経産省の情報セキュリティ管理規準に基づいて、これを委員会で編成したものである。まず、管理規準の評点水準は、0(何もしていない), 1, 2, 3(最も高い評点)に分けて評点を付けることになる。コントロール規準は、やや細かいレベルで評点を付けることにな

る。0(未実施レベル), 1, 2, 3, 4, 5(有機的改善レベル)に分けて評点を付ける。
検証手続についてもこの 39 号で言及をしている。業務実施者は検証業務リスクを合理的水準に抑える十分な証拠の入手をする。ある評価基準に複数の評価項目がある場合、その評点のつけ方については、最も低い方の評点を採用する。

情報セキュリティ検証業務の効用として以下の効用がある。

- □ 結論は管理・コントロールの良否に依存しない。たとえ、評点が低くても経営者の記述が適正であれば、適正という結論を出すことになる。
- □ 時系列比較が可能になる、前年度、今年度の比較ができる
- □ 業界比較・異業種間比較ができる

情報セキュリティ検証業務の活用として経営者が検証済みの報告書を積極的に開示すれば、信頼情報の付与、宣伝広報効果が期待されるかもしれない。また例えば、官公庁が情報セキュリティ業務契約入札業者の選定をする際に活用できることも期待される。

質疑応答

1)報告書の日付がなぜ重要なのか？

業務実施者のリスクにつながるところであり、セキュリティ事故等の後発事故が起きると、その結論の適正性に影響することになる。したがって、そのリスクを限定するために、日付を識別し、後発事象があってもその結論内容に責任を負われないことを明らかにすることになるからである。

2)結論が短いが細かなコメントを付すことはないのか？

細かな記述をすることを予定していない。適正ということの結論を言うことにあり、コメントを入れれば入れるほど、読み手が誤解をしうる余地を与えうることにもなりえる。
別途サービスとして、違う形式でコメントを文書にして出すこともあり得る。

3)ダイレクトレポーティング方式で仕事している検証、助言型の保証業務例は考えられないのか？例えば、アサーション方式のシステム監査は？

内部統制監査において　IT に係る統制は、システム監査ではなく、内部統制監査の一環であり、ダイレクトレポーティングではない。また、IT に係る業務でダイレクトレポーティング方式の保証業務例はない。

以上

所感(筆者)

本件は、IT に関する非監査業務である保証業務についてはじめて実務的な試みをしたものであり、ある意味では斬新であたらしい試みであったと思います。今後セキュリティ検証業務が我が国で実務として根付いていくかどうかについては、今後の展開を見ないとわかりませんが、何かのきっかけが必要な気がします。きっかけとは、先進事例としてどこかのブランドのある会社がこのサービスを享受して価値を見出しているという事例が生まれること、または不謹慎ながら、セキュリティ事故による本件サービスに対するニーズが顕在化すること等が頭に浮かびます。

遠藤 誠(筆)

近畿支部主催 システム監査入門セミナー（2回目）を開催して

No.1411 岡谷 亨

平成22年　7 月10日土曜日、大阪駅から歩いて10分強にある常翔学園で、近畿支部で今年度2回目となるシステム監査入門セミナーを開催しました。10時から17時までの1日コースで、スーパーに対するシステム監査のケーススタディです。受講者は11名と演習に適切な人数でしたが、入門セミナーという名称に似合わず、システム監査の経験者が6名参加されていました。また、残りの方も3名は内部監査部門の方で、監査のベテラン揃いといった陣容でしたので、初めてシステム監査に触れられる受講者の方とレベルが違いすぎないか、受講者の全員に満足頂けるかどうかを心配していました。

最初にセミナーの説明やスタッフ及び受講者の自己紹介を行った後、三橋氏が「システム監査概要」の講義を行いました。次に、金子氏が演習の説明を行い、受講者が3チームに分かれてチーム単位での演習に入りました。金子氏の説明は、予備調査の結果からシステム管理基準にどのように結びつけてインタビューの確認項目（チェックポイント）を決定するか具体的な紐解きのヒントを含んでおり、大変わかりやすい説明でした。第1回目の反省を踏まえた改善点でしたが、入門者に対してチェックリスト作成のポイントがわかりやすく伝えられたのではないかと感じました。

午前中チェックリストの作成を行った後、作成したチェックリストを用いて午後一にインタビューの演習を実施しました。第1回目と異なり、今回は3チームでしたので、被監査部門役を3名に増やしての演習でした。受講後のアンケートで、“ヒアリングを受ける側のみなさんの演技力には脱帽です。”と書かれていましたが、部長役の荒町氏、課長役の是松氏とも、役になりきって名演技をされていました。かくいう私も今回は課員になりきってインタビューを受け、サービス残業の実態まで吐露するはめになりました。（もちろん架空です。笑）

インタビューが終了すると、監査結果を監査報告書にまとめて頂き、監査報告会で報告頂きました。この入門セミナーの面白いのは、監査報告会も体験の場としている所です。スーパーの広瀬専務及び、監査依頼者である関西内部監査室長等に対してチーム単位で監査報告して頂きましたが、いずれの監査チームとも、関西室長からの執拗な質問に上手く回答されていました。

監査経験者が多いということでかなりレベルの高い演習となりましたが、受講者の皆さんから有意義なセミナーであったとの感想を頂き、スタッフ一同安心しました。手前味噌ながら、この入門セミナーは、「この内容で、この面白さで、この値段？！」を地でいくセミナーではないかと思います。この入門セミナーというショートコースにご満足頂いたら、ぜひ、実践セミナーというフルコースにも参加頂きたいものです。

セミナーワーキンググループのスタッフの皆様、当日都合が悪かったにも関わらず顔を見せて頂いた吉田支部長様、講義資料の改良にご助言頂いた藤野副支部長様、皆様どうもお疲れ様でした。ぜひ来年も実施したいですね。尚、今回のセミナーでは、関西氏がツイッターで常時セミナーの状況をつぶやく試みも実施されました。皆様ぜひ探してみて下さい。

「システム監査入門セミナー」に参加させていただいて

情報技術開発㈱ 監査室 堀畑 行彦

7/10 開催の「システム監査入門セミナー」に参加させていただき、ありがとうございました。

今回の感想を聞かせてほしいとのご依頼をいただき、少し書かせていただきます。

「堀畑くん、このセミナー参加してみないか？」それは、5 月のある日上司の一言より始まりました。

4 月に監査室に配属され、監査が何かということで日々戸惑っている最中なのに、監査室の業務にシステム監査があるからといって、IT企業に勤めながら、開発経験ゼロの私には絶対無理！と思い最初はお断りいたしました。しかし、上司の「何事も経験」というお言葉で、めでたく参加が決定しました。それからの不安な日々・・。システム監査の資料を読んだり、事前資料をいただいてからはケーススタディのシステムについて、わからないなりに理解しようと悪戦苦闘の毎日でした。

いよいよセミナー当日、不安で睡眠不足気味のまま突入です。まず参加者の方々の自己紹介があり、お聞きしているとシステム開発経験者の方が多数参加されておられ、益々不安は増すばかりです。

こんな監査も新人、システムも素人が参加していいのかって思ってしまいました。

最初は、システム監査に関する概要の講義、事前に資料を見ていたので、理解はしやすく、またゆっくりとわかりやすくご説明いただいたので、少しほっとしました。

いよいよチームに分かれての演習です。私はM氏、U氏とともに、Cチームです。なにやら舞上がっている間にリーダーということになってしまい、いよいよ混乱する私。

演習は、ケーススタディに沿って、各自の役割分担を決め質問項目をまとめる作業になりました。

お二人はどうやらシステム開発経験者らしく、落ち着いて質問項目の要点をまとめていく。私は、あせりながら、必死でない知恵をしぼって質問を考える。そうしている間に、昼食になりました。

午後からは、いよいよ監査のロールプレイングの開始です。講師の方々の見事な役者ぶりに感心しつつ、必死で質問とその答えを聞いて、問題点を検討しようとするが、システム素人の悲しさで、なかなか考えつかない。質問も途切れてしまい、お二人に続きをお願いしてしまう始末。チームメイトと講師の方々にも助けていただきながら、なんとか質問の演習は終了。

「リーダーの方に、監査報告を発表していただきます。」エー、またまた難題だ。生来の緊張症の私が、監査報告の発表なんて・・・。報告内容は、チームメイトのお力でなんとかまとめあげて、いざ発表です。緊張で頭の中がカラッポになりながら、なんとか発表しました。改善点もご指導いただき、なんとか終了です。その後ケーススタディの解説をいただき、なるほどそういうことかと納得したり、そういう視点でみるのかと感心したり、とシステム監査の難しさを感じながら、無事セミナー終了です。

今回セミナーに参加させていただき、本当に貴重な経験をさせていただきました。わからないなりにシステム監査を少し体験できたことは非常に有意義でこれからの監査の業務に活かしたいと思います。また、こんなできの悪い生徒を、講師の先生方や参加者の皆さんは、非常に暖かく迎えてくださり、感謝の気持ちでいっぱいです。本当にありがとうございました。また、ご一緒させていただく機会がありましたら、こんな私ですがよろしくお願い申し上げます。

以上

7 月 10 日（土）システム監査入門セミナー　　1 日コース 感想文

オルタネート　水内　一九昌

今回のセミナーは、資料を一読する事無く、目を通しただけで参加しました。

テキストは、熟読してません。 今、私の中では、 Web に集中中です。

ケーススタディは、Aチームに参加しました。

演習1:チェックリストの説明と作成
担当の決定
　リーダー、システム課長担当メンバー、システム課員担当メンバー、店舗営業部部長担当メンバー の担当を決めました。
　チェックリスト作成は30分位の感覚です。

　昼食も30分位で引き上げ、休憩無く、チェックリストを検討してました。

演習2:監査の実施
　各回メンバー全員参加で行い、1回目はまだ余裕が有りましたが2・3回目は余裕も無く、時間も足らないくらいで、監査報告の纏めの事も頭を過ぎりました。

演習3:監査報告のまとめ
検出事項・改善提言は全員で作成しましたが、総評は報告者が纏めた方が報告しやすいと考えほぼリーダー任せでした。

　監査報告のまとめの終了までは、頭を使いぱなしで胃に血液が流れず気が付けば、消化不良のようでした。

　リーダーの監査報告、他のチームの報告の時は、ホッとしてました。

　経産省「システム監査基準」から、資料～ケーススタディへの展開は、納得です。

ケーススタディ解説
なるほどなぁ～　　て、感じです。

　Aチームの他のメンバーは、テキストを熟読しているようでした。
　感想文を書くのに資料は、よく読みました。セミナー参加前に熟読していればと考えています。
　これからも、テキストに目を通すようにします。

　受講者自己紹介は、チーム分け後の方が良いのではないでしょうか？
　チェックリストの作成時間は、もう少し時間が欲しいです。

　IBM ユーザー会の関西研の「 H18T2 内部統制」に参加して、
　　2004 年 経産省「システム監査基準」改定公表　　（平成 16 年度版）

2007 年 経産省「システム監査基準」追補版 （財務報告に係わる IT 統制ガイダンス ）
目を通すぐらいは、行っていました。

もともと、プライバシー・マーク、ISMS の情報収集は行っていました。

セミナーも、いろいろ参加してます。

07.07.17 SAALK
09.07.17 SAALK IFRS
09.12.19 ISACA IFRS
10.05.21 SAALK ソフトウェア資産管理

ケーススタディ自体は、抵抗感も無く難易度の高いものでは有りません。

入門セミナー位のペースの仕事では、余裕が無さそうです。
もっと、じっくり考えて出来る仕事がしたい物です。
私のビジネスモデルは、助言的監査からのシステム構築です。
システム再構築のシステム監査には、今回の体験は有効に活用します。

各チームの監査報告に、コメントして配布してもらえないでしょうか？
ホットな内に理解を高めます。

よろしく 御願いします。