特定非営利活動法人
日本システム監査人協会報

2013年2月号
No 143

No. 143（2013年2月号）<1月20日発行> 新春特別号 別冊 同時発行

新年、明けましておめでとうございます。
皆様に役立つ“会報”に今年も一生懸命取り組みます。

会報電子版の記事　目次

新春特別記事

「新春特別号」として、次の記事2点を別冊で発行しております。ぜひご覧ください。
・新春対談（会員指向の会報を使命に）
・新年の会報テーマ（システム監査の普及促進）

〈目次続く〉

2013.1 投稿

めだか　【システム監査人自身も頭の切替えが必要では（システム監査の普及促進）】

新年の今月から３ヶ月間、会報テーマが「システム監査の普及促進」となるそうだ。
システム監査が言われて久しいが、その普及は必ずしも芳しくない。なぜ、なんだろうか。
システム監査に関わる者は皆、同じ疑問と、苛立たしさを感じているのではないだろうか。

「システム監査の普及促進」について、監査人の視点、利用者の視点、そしてその根底にある、そもそも「システム監査」とは何ものなのかの視点、認識から、思うところを綴ってみたい。
初回は、“システム監査”それ自体を他との比較で明確に識別、説明できなければ、それ自体の普及促進は難しいという根本的な問題認識から、そもそも「システム監査」とは何ものなのかの視点、認識を取り上げたい。

先日、某会合でシステム監査の話をする機会があった。そして、システム監査とシステムコンサルティングの違いについて以下のように整理して説明してみた。

	システム監査	システムコンサルティング
当事者数	3者又は4者	2者（依頼者とコンサルタント）
評価基準	関係者の合意・納得基準	コンサルタント独自の基準（ノウハウ）
結果の再現性	あり(science:科学)	なし（art：技・芸術）
成果物	適／不適の意見表明（静的）	改善提案・アドバイス（動的）

すると、後のＱ＆Ａの際に、参加者から、システム監査の成果物が、適／不適の意見表明だとすれば、システム監査にいったい何の価値があるのだろうかとの意見がだされた。この方は、コンサルタントの方のようで、今後に生かせる提案（改善に役立つ指摘事項）がシステム監査の価値と認識されているようであった。私からは、勿論監査の副次的産物としての“問題指摘（改善提案)”はあるが、システム監査の目的（価値）は客観的立場の監査人の適／不適の意見表明にあり、そこがシステム監査とシステムコンサルティングの違いと私は考えていると答えた。

システム監査の内容、価値は、時代の要請（情報化の進展）に沿って変化しているのかもしれない。例えば、情報化初期段階では、システム監査は、改善提案とそのフォローアップを特徴に、客観的立場とは言え、情報システムに対する指導的（アドバイザー的）役割も担う、組織内の統制ツールの一つと位置づけられていた。しかし、今日、システム監査は組織と利害関係者の間にあって、組織の、利害関係者に対する説明責任を担保するツール、また、利害関係者の、当該組織の情報システムに対する客観的評価情報の入手手段としての役割に、その意義が大きく拡大してきていると言える。

ここらで、改善提案・アドバイスを目的とするシステムコンサルティングと明確に異なるシステム監査の存在意義を、システム監査人自らが認識し直す必要があるのではないだろうか。

「システム監査」は「監査」ゆえに「定められた評価基準に対する、不偏的な適合性評価」がその本質であり、「システム監査」はこの「監査」本来への回帰を通し、システムコンサルティングと両輪をなす、健全な情報化社会を支える社会の公器（人間の知恵）と再認識すべきではないかと。

（広太雄志）

（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。）

2013.1 投稿

めだか　【　システム監査の普及促進－会報への一考察　】

システム監査の普及促進の観点から、会報のあり方について考察してみたい。会報は、特定刊行物として国立国会図書館へ納品され、一般の検索、閲覧に供されている。会報の記事には、匿名の「めだか」記事と、記名の投稿記事がある。「めだか」記事は、匿名投稿者の個人的な意見表明でありSAAJの見解ではないことをうたっているため、誹謗中傷でないかぎり、何でも投稿できて、外部へも思い切った発言を行うことができる。かたや、記名投稿記事は、会員番号、氏名、所属部会・研究会、支部をあきらかにしているわけで、会員やシステム監査人の履歴書に掲載する記録になりえるものである。

さて、ある会員から、当協会の本部に会員やシステム監査人が集う場がないという意見を聞いた。その意見では、システム・ストラテジストのような団体では、集いの場があって、和気あいあいと情報交換ができて楽しいとのことである。当協会では、システム監査の普及促進を主テーマとしているわけだから、システム監査が信用（credit）を取得するためにも、会員やシステム監査人が集まって、和気あいあいとした中で情報交換を行うエネルギー源としての場が必要である。会報は、デジタル化の波をうけて電子化を行い、協会ホームページ会報公開サイトからPDFファイルダウンロードする方式になっている。会報公開サイトでは、電子版も併設して、双方向性を設けている。最近の試みとして、スマホで会報の「めだか」特集記事が読めるようになった。これは、エポック・メーキングなこととして評価したい。

振り返ってみると、当協会は、会員の高齢化にともなう退会増加で会員の自然減少が生じており、会員増強プロジェクトが踏ん張っている状況である。また、残念ながらシステム監査人が資格更新を取りやめる状況が続いている。結論は、システム監査の普及促進のエネルギー源として、会員相互の情報交換を行う場が絶対的に必要であるということになる。社会一般を見ても、SNS（ソーシャル・ネットワーキング・サービス）が普及しており、会報は、会員やシステム監査人が情報交換に集う場になるような運営を目指すべきであると思う。

アダム・スミスは、人間本性の中のひとつの性向、すなわち、ある物を他の物と取引し、交換し、交易する性向（propensity to exchange）に言及し、交換の場が形成される必要性を述べている。会報の運用と同時に、リアルの世界でも、会員やシステム監査人が集う場を形成する活動が必要である。例えば、外部の企業等に対して、システム監査ワークショップ支援（WWS）の推進又は、情報交換の場を設けることが求められる。システム監査人補（ASA）は、予備的な資格になっているが、会員全員が、基本の資格としてASAを取得するよう、情報交換の場を形成する試みは、活性化につながると思う。会報は、これらのリアルな活動と連動して運営していくことになる。

「アダム・スミス『道徳感情論』と『国富論』の世界」 堂目　卓生　著（中公新書）

（空心菜）

（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。）

2013.1 投稿

めだか　【　十色・百様・千姿に向き合う付加価値（システム監査の普及促進）】

システム監査を業として見ればサービス業である。分類上の位置づけではなく、この「サービス」という部分にシステム監査の普及促進の手掛かり・足がかりがあると思っている。

改めてだが、システム監査技術者は「高度 IT 人材として確立した専門分野をもち，被監査対象から独立した立場で，情報システムや組込みシステムに関するリスク及びコントロールを総合的に点検，評価し，監査結果をトップマネジメントなどに報告し，改善を勧告する者」とされている（試験制度の対象者像）。当然だが、システム監査技術者として備えるべき技能や手続きが網羅されている。

一般的にサービスとは「一連の行為・パフォーマンス・経験などを提供し、他者へ利益をもたらすもの」とされており、サービス業の特性には「不均質性（品質が一定でない）」や、「非有形性（触ることができない、形がないため購入時に見たり試したりできない）」などがある。これらはシステム監査に良く当てはまっている。

この特性は、サービスを受ける（システム監査を受ける）側において、形のない商品を購入する際の期待性能や品質・価値の目算が一定でなく、十人十色・百人百様・千姿万態の理解と場面が発生することを示している。システム監査受ける立場の心理ともいうようなものが浮かび上がってくる。

システム監査を受ける者は、システム監査の専門性も、独立性も、技術水準も実は興味がない。購入する商品（システム監査）が役に立つか、使えるかであって、これは家電や台所用品を買う場合とあまり変わらない。形のない商品は扱いにくい存在だが、これはサービス業の一般的なことで悲観的に考えるものではない。

システム監査を受ける者が「利益」や「お得感」を得るのは、商品に付加価値を認めたときだ。

付加価値は、原材料の価格よりも製造された商品の価格が高くなった差だが、システム監査になぞらえれば、原材料（システム監査の能力）は形がなく・目に見えず・触れられず価格が不明だ。そして製造された商品（監査結果）も活字で使い心地も分からず価格は不明だ。不明・不明では付加価値はつかめない。

まして、製造された商品は監査人だけの成果ではなく、監査を受ける側も経費と時間を負担しており、しかも、こっちの方は姿かたちが明瞭で価格がハッキリしているのだから手ごわい。

しかし、しかしである。手ごわい相手を認識すれば相手を満足させる手法もコツも術も出てくる。システム監査の意義や効果の良き理解者や善意の価値判断に頼っているだけではシステム監査の定着はない。

以下はシステム監査の普及促進の定式だ。この式を満たすことによってシステム監査の魅力を高め、強固な市民権を確立し、普及促進に勢いと加速度を増したい。

（監査結果の利益・お得感）　＞　（監査を受ける側の経費・時間＋システム監査への期待）

システム監査に必要な技能は数々あるが、この定式の充足もまたシステム監査の重要な技能である。

（山の彼方）

（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。）

2013.1 投稿

めだか　【　元旦１面トップ記事の監査対象（システム監査の普及促進）　】

新年早々の記事には多少過敏になるのも“うべなるかな”と思う。
読売新聞の今年の元旦1面トップ記事は「農水機密　サイバー流出か」だった。

農林水産省がサイバー攻撃を受け、TPP交渉に関する文書が流出した疑いがあった、との報道だ。流出時期は2011年10月から2012年4月に作成された3000点以上の文書で、機密指定がされた文書もあった。約1年前に内閣官房情報セキュリティセンターから「不審な通信」の指摘を受け、内部調査を開始し、文書の外部送信の痕跡を発見し、一定の対応措置を実施した。が記事の概略だ。
このような事象については、多くの問題点、課題、対処が指摘されるのは当然で、極めて重要で大きな問題を含んでいる事件だ。

だが、ここで述べたいのは、これまでの報道が必ずしも明らかにしてはいないもう一つの問題だ。そもそも組織の責任者は何をしておくべきだったか、日頃の運営は適切だったか、役割と責任を果たしていたかだ。それは、この事件の経緯の一端をみるだけで明白になる。報道記事頼りだが農水省の動き（変遷）は次のとおりだ。

・昨年末以前「この問題を公表していない」 ⇒ ・元旦報道に対する説明「流出の痕跡は確認できない」 ⇒ ・1/8大臣記者会見「不審な通信のうち少なくとも1回は、意味のある情報の流出があったという報告を受けた」 ⇒ ・1/11報道「大臣指示で外部調査委員会の初会合を1/17に開催する」

この経緯から類推できることは、粗末・ずさん・低品質の組織と管理体制である、ということではないか。システム監査人の視点に依るまでもなく“歴然”で“理解できない“があらゆる人の本音と思う。報道のみが頼りではあるが、1/17に調査委員会を立ち上げるという公の発表事実が、多くのことを語って余りある。

情報セキュリティリスクを含むシステムリスクについて、どのような備えをしておくべきか、そのための権限者の役割と責任がどのようなものか、既に社会通念・常識になっているものではないか。

仮に、民間の会社で発生した事実ならば、相当な社会的制裁にさらされる事件だ。所管官庁から許認可を受けている事業をしている会社ならばどのような処分になるのか、と考えてしまう。

今回の事件について、リスク管理体制を対象にしたシステム監査を、早急に実施する方法はないものだろうか。その場合の「監査要点」（システム監査で点検・評価する小項目やチェックポイント）は下記例を始めとして、かなり広範なものになる。

・経営者（特にCIO）は、情報セキュリティを含むシステムリスク管理方針を組織全体に周知しているか。
・リスク管理の方針には、保護すべき情報資産とその責任の所在を明記しているか。
・経営者は、リスク管理の担当部門を設置し、モニタリング方法を含む適切な管理体制を整備しているか。

新たに設置されるという外部調査委員会の調査結果に、組織運営体制のシステム監査の必要性を指摘してもらえる方法はないものだろうか。きっと、多くの識者が関与する調査結果には、自ずと必要な対策が盛り込まれるはずだ。

（空遠幸）

（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。）

投稿

■【 構築途上にあるシステムへの監査が足りない④・・・腑 】

会員番号 1143　中山 孝明

連載 4 回目になる。来月の5回目で了にと考えると、もうちょっと頑張ろうという気持ちになる。いつもの曖昧な副題だが、前月号がそのまま「目からウロコ」とは正直思っていない。ウロコはそもそもしっかり付着しているし沢山あるものだ。今回は「腑」とした。前月号よりさらにソリューション的内容に近づける意図だ。

今月号では、「監査要点」について深掘りする。

システム監査実施時は、監査の目的、対象、範囲および「監査要点」を明らかにして監査手続に入るが、システム構築プロジェクトの監査の場合、どのような「監査要点」が適しているか、そこが深掘りする点だ。本連載では、システム構築プロジェクトの監査に用いる「監査要点」として、既存の基準・指針・ガイドライン等の項目では不足で補完の必要がある、ということを基調にしており既述もしている。

「監査要点」は、システム監査で確認・評価する内容であり、判断の尺度にするもの。システム管理基準（METI）やシステム監査指針（FISC）などで、「・・・しているか」「・・・すること」などと記載されている小項目やチェック項目を指す。

システム監査においては、ベースライン・アプローチによる基準対比の確認・評価や、リスクベース・アプローチによるリスク・マネジメントにフォーカスした確認・評価があり、さらに両者ともに、経営方針や事業目標、コンプライアンスの視点のポリシー・アプローチ（本稿での筆者ネーミング）が加味されることになる。現状、システム構築プロジェクトの監査では、リスクベース・アプローチを主体にし、ベースライン・アプローチとポリシー・アプローチの「監査要点」を加える手続きが基本あるいは一般的となっていると思う。筆者もリスクベースを最重視している。

リスクベース・アプローチでは、通常、リスクの洗い出し状況が最初の確認事項になる。リスク・マネジメントの実施状況なのだが、ここで、リスク・マネジメントを体系どおりに如何に忠実に実施したとしても、「計画」「認識」「分析」と進める手順は、つまりは、リスクを事前に想定・予想し特定するところからマネジメントサイクルが始まっている。この「事前に・・・」という点に、システム構築プロジェクトに用いる「監査要点」として問い直すポイントがある。

本論では、別途の重要なアプローチの必要性を提起する。（既存アプローチの補完として）

繰り返すが、事前予想のリスク事象をもとにしたリスク・マネジメントだけでは、変動要素の多様なシステム構築を成功に導く処方箋としては不足していると考えている。ここが肝心要な点であり例を引いて以下に述べる。
システム構築のQCD達成に資する技能・対応力・課題・勘所と、農業のそれの酷似例を前月号で紹介しているが、ここでも農業を例にする。実体のあるリアルな例だからだ。〔QCD（品質：Quality、予算：Cost、工期：Delivery）〕

さて、農業者が天候に関するリスク・マネジメントをしたとする。日照り、冷夏などだ。この場合例えば「水が不足した」がリスク事象の顕在化で、「作物が枯れた」がリスクの影響・結果だ。リスク分析は「枯れた場合の定量的・定性的な見積もり」で、リスク・コントロールは「水不足にならない具体的対策」になる。ここで、「水が不足した」のようなリスクを、どれほど多岐に事前予想したとしても、そしてリスク・マネジメントを継続したとしても、天候はそれこそ「お天気屋」だ。想定したリスク計画とは異なる事象に必ず見舞われる。自然環境だから当然の成り行きだ。

それゆえ農業者は、リスク計画に頼るのではなく、天候という自然環境に対して、目配り・気配りをさまざまに巡

らして繊細な五感をフルに発揮している。そしてごく普通に自らの行動を天候に順応させて農産物のQCDを達成している。「水が不足し作物が枯れた」では失格の烙印が待っているだけだ（例え僅かな作物であったとしても）。

言葉を足す。天候リスクという表現も、実は誤りだと言わなければならない。
「水が不足した」では遅いから、農業者は「お天気屋」の対象と四六時中闘っている。闘っているという表現も誤りで、正しくは”親しく付き合っている”のだ。初恋の人への感覚のような注意力で、小さな兆候を見逃すまいと神経を研ぎ澄まし、兆候を感じればそのベクトルの大小・方向を自らの行動の拠り所にしている。農業において天候はリスクではなく、多彩に変化する自然の摂理とのコミュニケーションだ。100％発生する事象というものはリスクではなく、コントロールできるようなものでもない。受け入れて行動基準に位置付けるのが本来だ。

システム構築のプロジェクトリーダー、チームメンバー、SIer、委託先それぞれが、基準・指針・ガイドラインや開発標準を遵守し、持てる力を発揮し、最善を尽くし、息切れを起こすほどに奮闘してもなお、間違い、行き違い、矛盾、狂いなどの齟齬が生じるのがシステム構築プロジェクトだ。「・・・しているか」「・・・すること」の基準に忠実な作業であっても齟齬が発生する。これは自然な姿だ。システム構築プロジェクトが人の行動様式、考え方、感情、周囲の影響などプロジェクト環境に依存不可避であるのは、農産物のQCDを左右する自然環境と同様だ。

要するに、リスク計画ではカバーできない分野で、その分野に対しては「発生した」では既に遅く、兆候を察知（兆候をつかむ前の感じて予知）した段階で、新たな行動を選択する必要がある。このような性質に左右されるのがシステム構築プロジェクトだ。例にした農業者が普通にこなしているのと同様な行動が求められている分野だ。

このような点に着眼した監査を「アクション・アプローチ」と筆者は呼び、その必要性を強調する。
このアプローチを構成する「監査要点」にもとづいた監査は、プロジェクトの成功に必ずや大きな成果をもたらすと考えている。

このアクション・アプローチは、リスクベース・アプローチ、ベースライン・アプローチ、ポリシー・アプローチを補完し、システム構築プロジェクトに向きあうシステム監査にキレとパワーを与えるものだ。

システム監査の実際においては、システム構築プロジェクトの状況（特に規模）によるアプローチの選択が求められる。小規模のプロジェクトでは依存環境が QCD に直接的に影響し易く、大規模プロジェクトでは組織的かつ規律あるチーム運営のなかで是正される部分もある一方で、大組織ならではの”生態”からの要因も多い。規模の大小でプロジェクト運営手法が異なるように、アクション・アプローチの「監査要点」も規模によって選択する。
念のため付言するが、ここで提起したアクション・アプローチは、システム構築の失敗原因として挙げられる「コミュニケーション不全」などとは全く異なる。そこで指摘される「報告が実態を示していない」や「意思疎通が図られていない」などは既存の「監査要点」で十分だ。

今月も、そして連載（次回で了）も、紙面が少なくなってきた。
「アクション・アプローチ」の監査とその「監査要点」は、システム構築プロジェクトの失敗例を聞くたびに筆者に思い浮かぶキーワードだ。
システム構築プロジェクトの成功率を劇的に向上させる手立ては、強い思いがエネルギーとなって生まれるものと信じている。

以上

新たに会員になられた方々へ

Welcome

新しく会員になられたみなさま、当協会はみなさまを熱烈歓迎しております。
先月に引き続き、協会の活用方法や各種活動に参加される方法などの一端をご案内します。

ご確認ください
・協会活動全般がご覧いただけます。 http://www.saaj.or.jp/annai/index.html
・会員規定にも目を通しておいてください。 http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・みなさまの情報の変更方法です。 http://www.saaj.or.jp/members/henkou.html

特典
・会員割引や各種ご案内、優遇などがあります。 http://www.saaj.or.jp/nyukai/index.html
セミナーやイベント等の開催の都度ご案内しているものもあります。

ぜひ参加を
・各支部・各部会・各研究会等の活動です。 http://www.saaj.or.jp/shibu/index.html
みなさまの積極的なご参加をお待ちしております。門戸は広く、見学も大歓迎です。

ご意見募集中
・みなさまからのご意見などの投稿を募集しております。
ペンネームによる「めだか」や実名投稿があります。多くの方から投稿いただいておりますが、さらに活発な利用をお願いします。この会報の「会報編集部からのお知らせ」をご覧ください。

出版物
・協会出版物が会員割引価格で購入できます。 http://www.saaj.or.jp/shuppan/index.html
システム監査の現場などで広く用いられています。

セミナー
・セミナー等のお知らせです。 http://www.saaj.or.jp/kenkyu/index.html
例えば月例研究会は毎月100名以上参加の活況です。過去履歴もご覧になれます。

CSA・ASA
・公認システム監査人へのSTEP-UPを支援します。
「公認システム監査人」と「システム監査人補」で構成されています。
監査実務の習得支援や継続教育メニューも豊富です。
CSAサイトで詳細確認ができます。 http://www.saaj.or.jp/csa/index.html

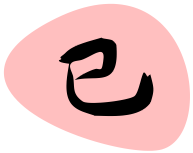
会報
・PDF会報と電子版会報があります。（http://www.saaj.or.jp/members/kaihou_dl.html）
電子版では記事への意見、感想、コメントを投稿できます。
会報利用方法もご案内しています。http://www.saaj.or.jp/members/kaihouinfo.pdf

お問い合わせ
・右ページをご覧ください。 http://www.saaj.or.jp/toiawase/index.html
各サイトに連絡先がある場合はそちらでも問い合わせができます。

沼野会長からの一行メッセージ

“当協会は、システム監査の普及促進に、引続き先頭に立ってその役割を果たします。”

■【会長コラム】



新年、明けましておめでとうございます。

会長　沼野伸生

新年、明けましておめでとうございます。

今年の元旦は大変いい日よりでした。
会員の皆様には穏やかな新年をお迎えのことと思います。

さて、私が会長に就任したのが昨年の1月ですので、今月でちょうど1年が経ちました。
昨年の主な社会的出来事を、記憶をたどって挙げてみると、1月はオウム真理教事件の平田容疑者の逮捕、2月は東京スカイツリーの完成、3月はロシアの前大統領プーチン氏が大統領に当選、4月は金正恩氏が北朝鮮トップに正式就任、5月は facebook が米ナスダック市場に上場、6月はハッカー集団 anonymous が日本政府、日本レコード協会に宣戦布告、7月はロンドンオリンピックで日本選手団が大活躍、イチロー選手がマリナーズから NY に電撃移籍、8月は消費税法の改正案可決成立、9月は橋下氏が代表を務めた新党「日本維新の会」が発足、10月は京都大学山中教授がノーベル賞受賞、11月はオバマ氏が米国大統領再選、中国では習近平氏を次期国家主席に選出、12月は衆議院解散総選挙で自民党が大勝などが挙げられます。
本当にいろいろなことがあった一年でした。

一方、当協会の活動に目を向けると、昨年1月の会長就任当初、ここ数年の当協会の会勢落込みを数値で確認し、大変な状況の中で会長を引き受けてしまったと、頭を抱えちょっと気が重くなったことを記憶しています。そこで、まずこれを何とかしなければと考え、理事会メンバーの皆さんの尽力、また、会員の皆様のご理解、ご協力も得て、会員増強PT(リーダ:小野副会長)を中心に会勢盛返し活動を積極的に展開して頂きました。PT立上げ当初、PTで具体的に何をすべきかを考えるためこれまでの協会活動を振返ると、会員増加・退会減少のための活動、会費未納者の状況確認、会員への協会各部会、研究会等の活動成果の還元徹底など、協会としての基本的な活動が十分でなかったことが明らかになりました。そこで、改めて協会運営の原点に立ち返り、十分でなかった協会運営の基本的活動を愚直に徹底、実施してきたのが昨年1年間といえます。
昨年のこの活動は、一定の成果を上げることができたと考えています。会員の皆様のご理解、ご協力に厚く感謝いたします。

会勢の盛上げはまだ途についたばかりです。本年も会員増強PTの活動成果を引継ぎ、継続して会勢の一層の盛上げに取組んで参ります。しかし、言うまでもなく会勢盛上げが当協会の最終目標ではありません。会勢を盛上げ、当協会の設立目的である、“システム監査の社会への普及”を確実に前進させ、健全な情報社会の発展に少しでも寄与していかなければなりません。
事件、事故が発生すると第三者による評価、点検を求めることが一般化し、システム監査もその一つである“第三者評価”の活用は社会的に定着しています。
このような状況の中、システム監査(システム監査人)の果たすべき役割は、情報社会の一層の進展と相俟っ

て、益々大きくなり、当協会は、システム監査の普及、促進に、引続き先頭に立ってその役割を果たして行かなければならないと思います。

本年はシステム監査に対する社会の期待、ニーズに呼応し、システム監査の普及、促進に直結する施策展開にも更に注力していきたいと考えています。

2月の総会審議を経て正式決定となりますが、現役員体制での最終年となる本年は、昨年の会員増強（会勢盛上げ）活動を引継ぐと共に、僅かですが政策予備費を予算措置し、皆で知恵を絞り、システム監査のノウハウ整理・公表など、システム監査の普及、促進に直結する施策の展開も予定したいと考えています。

守り中心の活動から、守りながら必要な攻めの施策展開も、との思いです。

本年も協会活動に会員の皆様のご理解、ご協力を引続きよろしくお願い致します。

会員の皆様にとって本年も良い年であることを心から祈念しています。

＜お願い＞

当協会の会報では、今月号から3ヶ月間、テーマを「システム監査の普及促進」として、皆様からの投稿を募集しています。このテーマは、本年度の協会活動を考える上で大変時宜を得たものになっています。

それぞれのお立場からいろいろな投稿を頂ければと期待し、また参考にさせて頂きたいと思っています。会報電子版では、投稿された内容について閲覧者がコメント入力でき、そこで筆者と読者の相互交流（意見交換）もできるようになっています。是非、積極的な投稿、議論の盛り上がりを期待しています。

＜ご案内＞

当協会の第12期総会は、本年2月22日（金）午後に機械振興会館地下会議室で開催されます。

詳細は後日ご案内させて頂きますが、今回の特別講演は、電子政府の最適化実施として順調に推移した厚生労働省職業安定局の事例（ハローワークシステム）をご担当の室長様からご紹介頂く予定です。

システム監査の視点からも興味深いものになると思いますので、是非ご参加頂きたくご案内致します。

以上

研究会、セミナー開催報告、支部報告

■ 報告１

【北海道支部創立１０周年記念講演会の結果報告】

№1068 大舘広之

日本システム監査人協会（SAAJ）では、北海道支部創立10周年記念講演会を、以下の通り開催致しましたので、ご報告致します。

土曜日にもかかわらず、総勢27名の方に参加頂き、盛会の内に開催・閉会することができました、ご後援頂いた団体のみなさま、ご講演のみなさま、及び、ご参加頂いたすべてのみなさまに感謝致します。

北海道支部創立10周年記念講演会 in SAPPORO

【日　時】平成24年12月15日(土)13:30-17:30
【場　所】かでる2．7（北海道立道民活動センター）
　　1030会議室(札幌市中央区北1条西7丁目)
【主　催】日本システム監査人協会 北海道支部
【後　援】経済産業省北海道経済産業局、
　　ITコーディネータ協会
【次　第】
　司会　日本システム監査人協会 北海道支部　菊地　圭氏
　13:30-13:45　開会挨拶　日本システム監査人協会 会長　沼野 伸生氏
　13:45-14:40　基調講演「高収益を支えるインターネット販売のシステムとは？」
　　株式会社　北の達人コーポレーション 代表取締役 木下　勝寿氏
　14:40-15:35　特別講演「システム品質から情報品質へ」
　　札幌大学経営学部教授　八鍬 幸信 氏
　15:45-16:35　支部報告「コンセントの向こう側　～電気はどのように届くのか～」
　　日本システム監査人協会 北海道支部　宮崎 雅年 氏
　16:35-17:25　本部報告「システム監査/管理基準のISO化推進状況」
　　日本システム監査人協会 副会長　松枝 憲司 氏
　17:25-17:30　閉会挨拶　日本システム監査人協会 北海道支部長　大舘　広之氏

【講演1】
【講演テーマ】「高収益を支えるインターネット販売のシステムとは？」
【講　　師】株式会社　北の達人コーポレーション 代表取締役 木下　勝寿氏
【講 演 内 容】インターネットショッピングなどのeコマースを支えるシステムを中心に「北の達人コーポレーション」の発展経緯や経験談を交えて解説された。

● システムの構成 と役割

創業当時は、ネットショッピングの同業者も少なかったが、最近は急増し、競合優位に立つには情報シ

ステムによる差異化が必要で、次のような要件に対応している。

- フロント　顧客からの受注時に様々な要望（支払者と届け先が別人。など）に対応できること。情報提供やアフターフォローで顧客満足度を上げ、リピーターを増やす。
- バックヤード　数量や鮮度などに注意し、梱包、配送を行う。業務量の増大に伴い、ミスを防止しつつ、仕事のスピードを上げる。
- データ分析　利益を上げるためにコストを削減する。このため、データを活用して効果的に投資する。たとえば、YahooとGoogleでは、どちらへの広告効果が高いか、など。

● システム開発

- システム開発は、社内で100％開発している。
- 社長が、システム開発の責任者を兼ねている。
- 何よりも、顧客対応におけるミスが怖い。システムの支援により、人為ミスを防止することが重要。システムの品質は、社長自らチェックしている。外注したことがあるが、品質が悪かった。

【所感】

木下氏は、テレビ番組などへの出演経験もあり、分かりやすく興味深かったというのが来場者の一致した感想であった。「外注では品質が悪いので内製している」というのは、情報システム業界関係者としては耳の痛い話である。システム開発・運用において、「システム監査は重要である」との締めくくりがあり、本協会の面目躍如といったところである。

【講演2】

【講演テーマ】「システム品質から情報品質へ」

【講　　師】札幌大学経営学部教授　八鍬 幸信 氏

【講 演 内 容】情報システムに対して、その中を流れる情報の質について解説された。

● 情報の品質

- 日本では、情報技術や性能に重きが置かれ、情報の品質にはあまり注意が払われていない。
- 情報品質とは、「情報の消費者による利用にとっての適合性」である。

● 医療分野での情報品質の例

- 医者の表現する情報：専門的な検査数値など。
- 患者の知りたい情報：生きるか死ぬか、酒を飲んでいいか、など。
- 社会全体で患者個々の医療情報を共有するシステムがない：救急時、病歴・手術歴・禁止医療行為は本人の申告（これも間違っている場合もあるし、本人が意識不明なら情報が得られない）によるしかない。

● 学生のデータ表現リテラシー

- ご自身のこれまでの講義経験から、数値表から適切なグラフを作成させる問題に対する学生の解答傾向を解説。
- Excelに数表を入力して、グラフ作成機能を利用すると即座にグラフが表示されるが、そもそもどう表現すべきなのかという視点が欠けている学生が多い。

【所感】

システム開発側の者にとっては、システムを作り上げることに目が向いてしまうが、システムはこれを使って、利用者へ利便を提供すること、そのためには、データの品質確保と活用が円滑に行われるように仕向けるシ

ステムが良いシステムであると、改めて考えさせられた。医療分野での話は、ご自身が救急車で搬送されたときに、情報不足からあわや手遅れということを語られ、情報品質の重要性を痛感させられた。

【講演3】

【講演テーマ】「コンセントの向こう側　～電気はどのように届くのか～」

【講　　師】日本システム監査人協会 北海道支部 宮崎 雅年 氏

【講 演 内 容】ITシステムの事業継続に不可欠な電力について、ご自身の業務経験・知識をもとに解説された。

- 電力供給における重要ポイント
  - 電力を供給するエリア内では、多数の発電機が協調して供給系統を構成している。
  - それらの発電機の周波数と位相は、ぴったり合っていなければならない。周波数と位相がずれた発電機は、供給系統から脱落し、他の発電機がそれをカバーし負担がかかる。これらが雪崩式に連鎖すると、ついには、少数の発電機で需要を支えきれず、大停電に至る。過去に東京で実例がある。
- 日本の電力事業者の構成
  - 発電量は、東京電力の約5，000万kwから北海道の約500万kwまで、大小ある。
  - 事業者間で電力を融通し合うルートはあるが、その容量は50～1000kw程度であり、限度がある。北海道がその1割を東京に融通しても、東京の1％にすぎない。
  - 50Hzと60Hzの地域に分かれており、それら地域間での電力融通は周波数変換を伴うので、意外なほど少ない。
  - 昨今の節電ニーズに対して、地域間の電力融通には限度がある。
- 北海道での電力事故
  - 北海道で今冬、暴風雪による送電鉄塔倒壊があった。
  - 懸命な復旧作業で停電から回復した。

【所感】

我々は、講演テーマどおり、普段「コンセントの向こう側」のことは忘れて、使いたいだけ電気を使っているが、供給に携わっている方々の努力が伝わってくる内容であった。日本の電力構成バランスについては、今回の選挙の争点の一つにもなったが、さまざまな新電力供給源を供給系統全体として実現するには、技術的に困難なところもあるのかと考えさせられた。

【講演4】

【講演テーマ】「システム監査/管理基準のISO化推進状況」

【講　　師】日本システム監査人協会 副会長 松枝 憲司 氏

【講 演 内 容】システム監査のISO化取組状況について、最新の状況を解説された。

【所感】

本講演は、本部研究会で発表予定の内容を一足早く披露していただいた。参加国との議論のポイントなどを分かりやすく話していただいた。

以上

■　報告２

【ISACA 大阪支部と日本システム監査人協会近畿支部合同講演会報告】

No1710　小河　裕一

1. テーマ　：「最新サイバー攻撃の脅威と富士通クラウド CERT の取り組み」
　　－ 新型攻撃に対して、今何をすべきか －
2. 講師　　：富士通株式会社
　　クラウド CERT 室長　奥原　雅之氏
3. 開催日時　：　2012年12月15日（土）　15:00～17:00
4. 開催場所　：　常翔学園大阪センター　302教室
5. 講演概要

(1) 最新サイバー攻撃の理解

「セキュリティ」という言葉が語られ始めたのは 2000 年頃で、官公庁の Web サイトが書き換えられはじめた事件以来である。毎年セキュリティ事故は発生しているが、最近は事故の質が変化してきている。最近のサイバー攻撃に関して攻撃者の観点で分類すると、低脅威多人数である個人やネットワークコミュニティレベルのものから、中脅威であるプロのハッカー集団、高脅威少人数で行われる国家レベルの防衛・諜報まで存在する。一方、攻撃動機で分類すると、興味本位や自己満足から国防のレベルまで存在する。

(2) 最新サイバー攻撃の実例

ケーススタディとして、以下の3つを簡単に説明

・Playstation Network の事件

→Playstation の機能制限を行った結果、ネットワークコミュニティとのトラブルに発展し、結果的には大規模情報漏えいに発展した

・標的型メール

→情報窃取を目的として特定の組織や個人に送られるウイルスメールによるもの。
最近では第一弾を受け取った内部の注意喚起メールの続報を装った標的型メールも存在

・制御システムを直接攻撃するマルウェア

→StuxNet,Duqu のように実際に稼動するプラントや制御システムに入り込んで活動するマルウェア。発生が特定の地域・国に偏っている傾向がある。技術的に非常に高度であり、国家レベルのプロジェクトで作成されたものと想定される。

(3) 最新サイバー攻撃に対する対策

これまでのセキュリティ脅威は一過性であり撃退すれば終わりであったが、最近の攻撃は目的達成まで繰り返し攻撃してくるパターンに変わってきている。それに伴って、対策も「DMZ をつくり、FW で内側を守る」というような水際防御では防御不可となり、総力戦で行う多層防御が必要となってきている。これからは、以下のような「総合的な対策」が必要と考えられる。

・隙をみせず、狙われにくくする。

→金のために攻撃する人は、やりにくいところを狙わない。

・多層防御等で技術的に攻撃を防ぐ。

・技術的対策に頼らず、ルール化等で「人による防御」を行う。

→「”怪しい”メールはあけない」

「怪しい」とはどのようなメールかまで決めておく。対策に万全なものはないが、やっているのとやっていないのでは全く異なってくる。

(4) 標的型メール対策訓練のケーススタディ

・演習手順

部門内の所属従業員に対して、明らかに標的型メール攻撃と思われるメールと、よく見ないとわからないメールを送信し、部員が開封するかどうかの訓練(演習)を実施した。事前に人事や法務等と調整を行い、さらに対象者にも実施2～3週間前に訓練を実施する旨を伝えた上で実施している。

・演習結果

事前に演習実施予告をしていても、わかりにくくするほど開封してしまう人が増える。明らかに標的型攻撃と思われるメールの開封率は低いが、見分けにくくすると 50%を超える開封率となった。

・演習からのフィードバック

「犯人さがし」が重要ではなく、防ぐレベルと防げないレベルを見極め、どのように対応するのか、組織のポリシーを決めることが重要である。そして、守ると決めたレベルは死守できるよう訓練を積み重ねることが必要である。

(5) 富士通のクラウドサービスとクラウド CERT の活動

・FGCP／S5

仮想化技術を用いてデータセンター内のリソースに仮想環境を割り当てて提供するサービス。

・クラウドの世界ではセキュリティがどう変わるのか？

技術的には従来の延長だが、運用面では課題が山積み状態である。

-責任分解の考え方

-インフラを共有するリスクの考え方

-データの所在明確化

-インシデント発生時のプロセス

-仮想環境に対する証拠保全

-「気がついたらサーバができている」世界の管理方法

・富士通クラウド CERT の活動

CERT＝Computer Emergency Response Team。商標登録されている。クラウド CERT の名称は世界初。One Fujitsu を実現するために、グローバルに共通化した情報セキュリティポリシーを適用している。モニタリングも 24 時間 365 日行っている。脆弱性の監視を行っているが、運用部門では無い「第三者」が実施いているということが重要ポイントである。緊急対応においては、インシデントが発生してからの対応も当然であるが、事前準備が必要でありインシデント発生前に対応ガイドラインを決めており、そのガイドラインにしたがって動くことになっている。

(6) 最新サーバ攻撃への対策として

・標的型攻撃は対策が難しく、水際防御では無く複数の対策を組み合わせる縦深防御で対処。

・ネットコミュニティは大きくなると力がある。上手く付き合う必要がある。

・最新サーバ攻撃への対策に「銀の弾丸」は無く、地道に対策を積み上げて行くことが重要。

6. 所感

一昔前と違ってサイバー攻撃も多様化してきていて、報道や記事で読むレベルや名前だけは知っているという物が多数でてきていますが、今回の講演でわかりやすく整理して頂き、どのような背景でサイバー攻撃が行われ、どのように防御すべきかを学び取ることができました。対策に関して資料の中に次のようなフレーズがありました。

「新型インフルエンザと同じでワクチンは無い。基礎体力を上げ続けることが最良の手段。」

現状わかっているサイバー攻撃への対策だけでなく、今後も次々と発生する未知の攻撃に対しても通じる事項であり、常に攻撃や対策の動きを監視した上でできるだけ先だって対策する事が重要であるということと理解しました。また、最新クラウドに対応するための富士通が行っているサービスの一端も知ることができました。さらにクラウドに限らず、新しい技術を導入してサービスを提供しはじめるときは運用面における課題解決が大変であるようにも思いました。

講演を通して最新の動向や技術を知ることができましたが、今後もこのような最新動向に常時アンテナを張って情報を仕入れることも重要であると感じました。

以上

■　報告３

【2012 年度 SAAJ 中部・北信越支部，JISTA 中部支部合同研究会報告】

北信越支部　宮本 茂明

以下のとおり 2012 年度 SAAJ 中部・北信越支部，JISTA 中部支部合同研究会を開催しました。

・日時：2012 年 11 月 23 日（金・祝）13:00～11 月 24 日（土）12:00

・会場：能美市ふるさと交流研修センター　さらい（石川県能美市）

・主催：日本システム監査人協会　中部支部，北信越支部

　　日本ITストラテジスト協会　中部支部

・参加者：17 名(SAAJ 中部支部 7 名，SAAJ 北信越支部 7 名，JISTA 中部支部 2 名，一般 1 名）

・テーマ：**「ソフトウェア品質監査制度（仮称）を受け、我々はどうすべきか」**

［1 日目：11 月 23 日］13:00-17:00

13:00～13:15　受付・会場準備

13:15～13:30　諸連絡

13:30～15:30　IPA（独立行政法人情報処理推進機構）技術本部

ソフトウェア・ｴﾝｼﾞﾆｱﾘﾝｸﾞ・センター　統合系研究員　田中和夫様による制度の説明

「ソフトウェアの品質説明強化のためのフレームワーク～ソフトウェア品質監査制度（仮称）～」

15:30～17:00　グループによる議論・成果物作成

18:30～　懇親会/意見交換

［2 日目：11 月 24 日］　9:00-12:00

9:00～10:45　グループによる議論・成果物作成

10:45～11:45　成果発表

11:45～　クロージング

Ⅰ.「ソフトウェア品質監査制度（仮称）」の概要

「ソフトウェアの品質説明強化のためのフレームワーク～ソフトウェア品質監査制度（仮称）～」について

講師：IPA 技術本部 ソフトウェア・ｴﾝｼﾞﾆｱﾘﾝｸﾞ・センター 統合系研究員 田中 和夫 様

報告者（会員 No. 1711　澤田 裕也）

田中様より「フレームワーク検討の経緯」「品質説明力とは」「フレームワークの要件と対応方針」「フレームワークおよび制度化のイメージ」「今後増えていく IT 融合システムの品質管理」「制度化に向けた他団体との連携」についてご説明いただいた。

説明後はフレームワークの内容や他の認証との棲み分け、実現に向けた課題について熱い議論が交わされた。実現・普及までに課題はあるものの、利用者にとっては安全な製品かがわかりやすい、企業にとっては製品の安全性の PR が可能になるという双方にメリットのある制度である。

私も監査人としてソフトウェア品質監査制度が始まったときに役立てるよう日々精進していきたいと考えた。

以上

Ⅱ. グループ検討の概要

「ソフトウェア品質監査制度」について4つのグループに分かれ各々テーマを決め検討を行いました。

◇Aグループ報告

報告者(会員 No.1732　田中 勝弘)

1. テーマ:「ソフトウェア品質監査制度」

社内の品質管理(監査)する人間だったら？

2. メンバー:澤田、福田、角屋、安井、田中(敬称略)

3. 検討内容

Aグループのメンバー5名は、全員 SAAJ の会員で、所属組織(立場)は、ユーザ系情報子会社、開発ベンダーの内部監査、IT コンサルタントであった。そこで、メンバー全員で議論できる「社内の品質管理(監査)する人間だったら？」をテーマとした。

議論の前に、メンバーの中で情報システム開発における設計・開発から保守にいたるプロセスを社内規定に沿って、管理(チェック)を実際に行っている者よりチェックする内容やタイミングなどの事例紹介を説明してもらい、システム開発・保守プロセスでの品質保証活動の実情を共有した。

(1) ソフトウェア品質監査制度の認識

IPA 田中様より、本制度の講演を受けて、ソフトウェア品質監査制度では、システム開発・保守プロセス工程での品質管理(品質保証)の視点と、プログラム製品(プロダクト)の品質(マニュアルや仕様書に記載された機能の動作保障、安全性などの必要機能の実装保障)の視点の二面があるのではないかとの意見があがった。そこで、この 2 つの視点での本制度の認識を議論した。

①ソフトウェア開発・保守プロセス工程での認識

上記のようにプログラム開発・保守工程でのチェックについては、現在では各社の社内規定やプロジェクトの管理ルールに沿って確認を行っているが、本制度が共通標準としてソフトウェアの開発側および利用側が”双方が同じ土俵にのる”ことで、開発工程の認識が共通化できるのではないかとの意見があがった。現在ではシステム利用者からの障害報告、不具合報告が発生した都度、その原因の説明や関連プロセスの見直しを行っていたが、適用している社内規定がプログラム品質監査制度のプロセス管理基準に準拠したものであることを保証することで、開発側としてのリスクヘッジが可能ではないかとの意見があった。しかし、単に社内規定に沿って、作業が行われているか、必要な記録が残っているかなどのマネジメントや各工程完了のチェックの視点を中心とした確認だけでは従来の ISO9001(QMS)認定などとの違い(差別化)が見つけにくい。そのため、ソフトウェア品質監査制度では、さらに成果物の内容(例えは前工程で実現するとした機能が次工程で漏れなく考慮されているか、設計・開発の整合性や技術的な妥当性の視点など)について踏み込んだ管理基準に沿った監査を行う必要が重要であるとの認識に至った。これを実現するためには、対象となるソフトウェアの内容(実装機能)に基づくチェックリストの整備が必要であるとの意見があった。

②プログラム製品(プロダクト)の品質保証での認識

田中様の講演の中で、今後の計画としてパッケージソフトについてカタログや説明書に記載された事項が適切であることを評価する旨の試行運用について説明があった。

プロダクトの品質保障ができれば業界を跨いだ基準の統一が可能になるのではないかとの意見があった。また、できるなら「建築基準法」とまでは行かなくとも、プロダクトに必要最低限の機能(例えばセキュリテ

ィ対応や誤作動防止)の実装などが保証できるのではないかとの意見があり、利用者がプロダクト選定時の比較評価の基準となりうるのではないかとの意見が出された。

(2) 本制度をどう活用するか

「社内の品質管理(監査)する人間だったら？」を視点に議論した。その結果、次のような意見がでた。

・標準化により手戻りが減る→業務負担軽減およびリスクヘッジが期待できるのではないか

・委託するベンダーとの共通の物差しができる→ベンダー間および委託元・受託先間の認識の違いが減る

特に開発側(生産者)として、上記でも述べた通りシステム利用者(顧客)とシステム開発における開発・保守プロセスが、システム開発作業を知らない顧客にも、プログラム品質や検証状況について説明しやすくなり同じ土俵にのることが出来るのではないかとの意見があった。

また、本制度を活用して、社内の内部監査人についても、

・社内プロセスをビジネス化する→対外的な監査ビジネスの創出

・システム監査人が社会で有効活用される→システム監査人の価値の認知

などの新たな活動の場が生まれるのではないかとの意見が出た。

また、既存システム開発・保守のプロセスで見る軸と、今回の制度(プログラムプロダクト)の関係を整理すると次の例示に示すマトリックスのように纏められるのではないかとのとの提案があった。

		プロダクト（今回の制度の軸）				
		業務・業界	PKG	PKG改造	新規作成	・・・
プロセス ISOなど	商談					
	要件定義		○		○	
	設計	○	○	○	○	○
	製造	○	○	○	○	○
	テスト	○	○	○	○	
	リリース		○		○	
	運用・保守		○			
	・・・					

(3) 制度化に向けた課題・意見

最後に、講演のなかで制度化していくための必要な事項について議論を行った。

・プログラム全体の品質を確保する上で、システム開発・保守を行う各プロセスでの品質作り込が確実に実施されていることを確認することが重要である。そのためには、従来の QMS 的な要素の他に、各業務やプロダクト精通者が参画して、監査対象の設計思想や確認事項を確認事項として洗い出す必要があり、そのためには、システム監査で言う管理基準策定には、業界を上げた協力体制が必要であるとの意見があった。

・監査人の育成については、対象業務の知識、経験、監査人としての技術が要求され、それを客観的に確認、維持できる仕組みが必要になると考えられる。(例えば、システム監査人協会、ソフトウェア品質監査人協会などの活用が考えられる)

・監査リスクの低減方法として、本制度で重要に応じた監査(保障)の深さについて例示があるが、例えばサ

ンプリングによる監査などについてはサンプリングの考え方など具体的な監査手続きについても指針となるものが必要になるのではないかとの意見が挙げられた。

また、本制度は、重要な分野・プロダクトにおいては任意制度ではなく、義務化に向けた関連法令等の整備も、制度定着の意味でも重要であるとの認識に至った。

以上

◇Bグループ報告

報告者（会員 No1813　大友　俊夫）

1. テーマ:「ソフトウェア品質監査制度」

自分が第三者の監査機関の担当だったら、 我々はどうすべきか

ソフトウェア開発、ソフトウェア品質管理、会計監査、内部監査など、メンバーの知見を基に、ブレーンストーミングを行い、3点の検討課題を抽出した。

(1)監 査 段 階:監査段階（プロセス）をどのように考えるか

(2)監査留意点:実際の監査にあたって、どのような留意点があるか

(3)監 査 組 織:この制度が期待する監査能力をどのように組織化し育成するか

2. メンバー:大友, 大喜、堤、宮本 （敬称略）

3. 検討結果

(1)監査段階

「製品個別監査」を行うにしても、その土壌・土台となる組織全体の「組織活動監査」を、ソフトウェア単体の製品開発プロセスの監査に先立って実施する必要があり、二段階で監査すべきと考えた。

①組織活動監査（企業風土・企業文化）

・品質マネジメント活動

・人材育成　社員の能力開発の取り組み

・顧客インタフェースのマネジメント

②製品個別監査

・個別管理基準

(2)監査留意点

ソフトウェア開発特有の課題として、ソフトウェア開発の川上から川下までの一連の流れとは別に、その後の保守・改修までを監査の対象範囲に含める必要があり、今後管理基準の制定において、「ソフトウェアのトレーサビリティの管理基準」の検討が重要な課題であると認識した。

①現状の問題（トレーサビリティの重要性）

・ソフトウェアの流用性

・ソフトウェアの世代管理

・保守、改修段階の課題

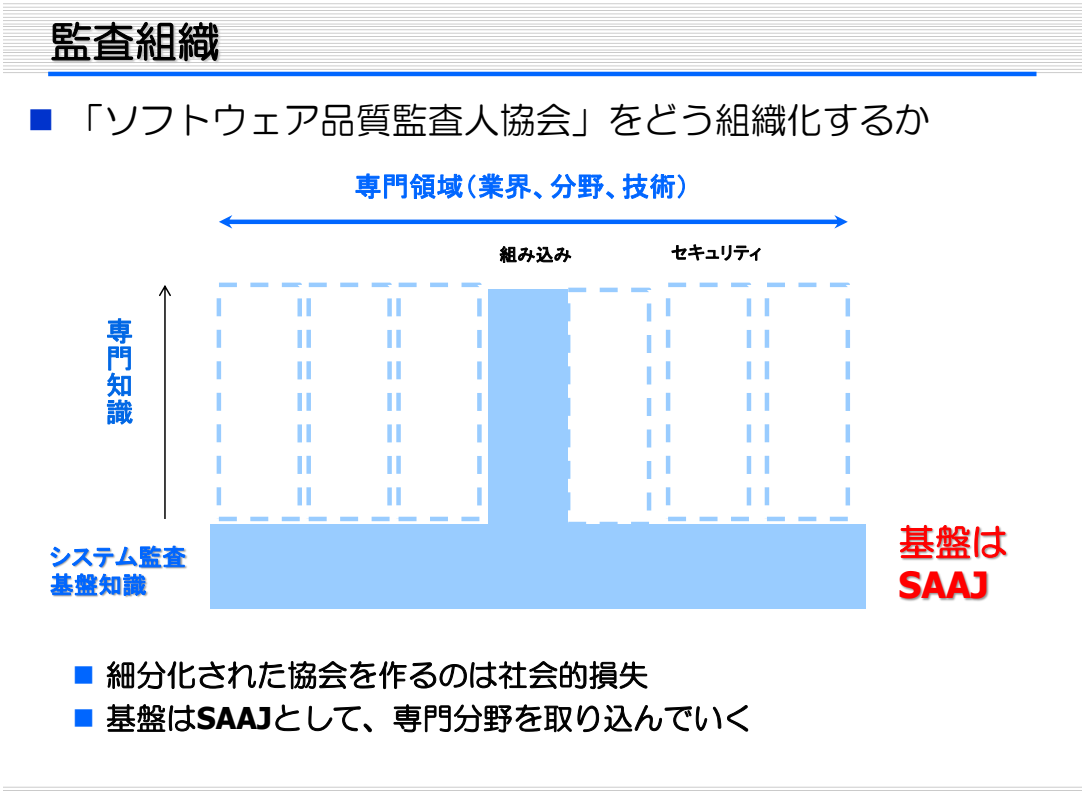
- 改修時の影響範囲の特定が困難
- トレーサビリティの組み込みがされていないケースも多い

②問題解決の方向性

製造業におけるすぐれた部品管理ノウハウをソフトウェア品質管理にも取り入れる

(3)監査組織

「ソフトウェア品質監査制度」においては、監査人の母体として「ソフトウェア品質監査人協会」を想定しているが、この組織の在り方、人材養成について、社会的な組織活動の効率性の観点から、SAAJという既存組織を基盤として活用することが重要で、下図に示す取組の必要性を指摘した。



以上

◇Cグループ報告

報告者(会員 No.1502　木村　武志)

1. テーマ:「ソフトウェア品質監査制度」

自分が社内の品質管理担当だったらどう活用する？

2. メンバー:栃川、石黒、中谷、木村(敬称略)

3. 検討内容

(1) 感想・意見の共有

テーマは、メンバーに品質管理者と開発担当者が多く、議論のし易さから選定しました。

初日は、特に議論の範囲を決めずに意見交換を行いました。制度への理解が漠然とした状態なので、メンバーとの話し合いの中で、どのような意見や疑問点を各自持っているかを情報共有する時間としました。

最初に挙がった話題は、“審査基準書”の策定から運用についてでした。この基準の具体的な内容が分からない状態で、この制度の活用を考えるのは難しかったのですが、どの範囲でどの深さまでを対象とするかが重要との意見がありました。品質に対する要求は、業種・業態・規模といった多くの要因により異なります。製品・システム開発の現場では、人や組織の経験値に基づいた品質指標等はありますが、その根拠となると説明が難しいのが実状です。

次に ISO9001 との関係についての話題も挙がりましたが、“審査基準書”での話題からも組織単位の活

動だけでなく、本制度は業種・業態・規模に応じた品質要求への対応となります。また ISO9001 については、形骸化している組織体が多く、この制度も同じ道を歩むのではという意見もありました。それに対しては、ISO9001 を経営の道具として活用している組織も多くあり、それらの事例を元に有効な制度としなければいけない意見がありました。

1日目の議論は“審査基準書”に話題が集中しました。基準が無ければ監査、評価、認証といった活動が実施できないことから、内容が見えない“審査基準書”についての話題が多くなりました。

(2) 現状の問題・課題からの制度の活用

2日目は、1日目の感想・意見の共有を踏まえて、各自の現場でどのような問題や課題があり、その対策として本制度の何が活用できるかを議論しました。制度自体の活用方法としては、いわゆる“お墨付き”としての活用もありますが、グループとしては製品・システムの本質的な品質向上と、複数業界で共有・支持できるものに範囲を絞って検討しました。また、必要性の観点としてはプロセス、ビジネス、人・組織の大きな範囲で検討しました。

検討結果を“表　現場の課題・問題に対する制度の活用方法”にまとめました。プロセスの観点では業界別、現場に適合した品質基準としての活用です。ビジネス面では発注・購買時における関係会社に対する品質確保の手段として活用です。また、人・組織においては、とかく品質よりもコストと納期が優先されてしまうことが現場では多いので、トップダウンとボトムアップの両方向から社会的な必要性と制度としての要求から品質の重要性を周知する手段としての活用です。表では観点毎にまとめましたが、検討の場では、プロセス面での活用は、ビジネスや人・組織に面での活用に共通する点もあるなど、表の縦の境界は特に無いのとのことで意見が一致しました。

表の中に“基準”、“共通言語”、“物差し”といった単語があるように、定量化が難しいソフトウェア品質のスタンダードとして活用し、継続可能な制度に育てなければいけないという意見に至りました。

表　現場の課題・問題に対する制度の活用方法

必要性の観点	プロセス	ビジネス	人・組織
課題・問題点	品質を確保するための明確なプロセスがない。 QMS より業界別、現場に適合した基準が必要である。	品質を確保するための共通言語が無い。	品質意識を持った人材が育たない。 経営層に品質意識が無い。 (コスト、納期が優先)
活用方法	自社の製造の基準として活用する。(段階的な改善) 鏡として活用する。(自分達の日頃の活動の振り返り時の基準)	仕入先の選定基準として活用する。	人材育成の物差しとして活用する。 トップダウンの品質活動するために活用する。(品質活動への経営資源の確保)

4. 所感

私の業務は、設計書の検証、品質データの収集から分析、実機検証といった地道な作業です。しかし、開発者に対して品質向上に有効な指摘がなかなか出来ていないのが実状です。しかも、IT システムは複雑で巨大化しており、問題が発生した場合の影響度も大きくなっています。今回の研究会で他社の方にも

お話を伺うと、同様の問題意識を持っているとお聞きしました。このソフトウェア品質監査制度は、まだまだ多くの課題がありそうですが、日本の IT 産業におけるソフトウェア品質の底上げのために必要な制度と思いました。今後は制度の状況を注視して、引き続き有効なソフトウェア品質の向上策を考えて行きたいと思います。

以上

◇Dグループ報告

報告者(会員 No.848　森 広志)

1. テーマ:「ソフトウェア品質監査制度」 **企業の品質管理担当だったらどう取組めばよいか？**
2. メンバー:若原(発表)、栗山、國谷、森 (敬称略)
3. 検討内容

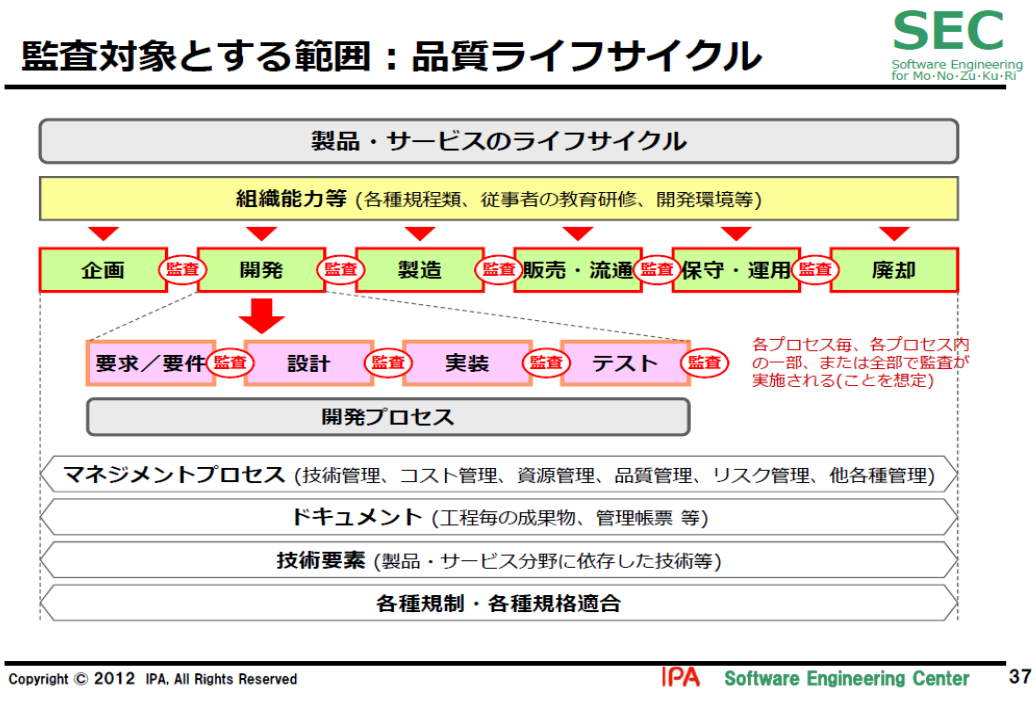
(1)導入とリスク

Dチームでは、企業が「ソフトウェア品質監査制度」にどのように取組めば良いか検討しました。導入に際しては、政府機関による「ソフトウェア品質監査制度」導入促進の外圧を利用することで、企業の製品・サービスの品質向上を高めるよう働きかけることが効果的と考えます。特に、当制度が顧客価値を創造し、企業価値貢献に役立つことが真に重要であり、形だけの導入で責任回避に使われることを防止することも必要です。

当監査制度を企業に導入した場合、監査業務の労務量、品質標準や監査標準の整備・作成に係わるコスト、外部調達コスト(委託先にも同様の活動を遵守頂く)等が経営圧迫要因となると考えます。加えて、監査人も保証型監査の責務を負い監査品質の確保を図る必要がありますが、上記の全コストを上回る価値創造が求められます。

(2)「ソフトウェア品質監査制度」運営のための工夫

当監査制度の監査対象範囲は、下図のように、製品・サービスの企画から廃棄までライフサイクル全体を網羅し各工程の全てまたは一部を監査する必要があります。



当監査制度の品質を確保し効率的に運営してゆくためには、先ず、各プロジェクト件名が適切にマネジメントされると共に、監査に必要な工程毎の成果物が整備されている必要があります。一般的な企業のプロジェクト管理は、現実には不十分な点が多々あると考えられるため、PMO(Program Management Office)を設置し、プロジェクトマネージャの養成、優先順位・全体進捗管理、規定基準・成果物管理、プロジェクト技術支援を実施し、全社内での効果的効率的なプロジェクト運営を行い、更に、これらが整った上でAMO(Audit Management Office:仮称)を設置し、監査人養成、全体進捗管理、規定基準・成果物管理、監査技術支援を実施することで、頻繁に発生する監査業務の効率的処理を目指すことを提案したいと思います。

以上

Ⅲ. 合同研究会を振り返って

報告者(会員 No.1281　北信越支部　宮本 茂明)

SAAJ 中部支部からの呼びかけで SAAJ 中部・北信越支部、JISTA 中部支部合同研究会を合宿形式で実現することができました。

研究会テーマについては、現在制定に向け検討が進められている「ソフトウェア品質監査制度(仮称)」についてシステム監査人、システムアナリストの立場から考えてみる機会とすると良いのではないかということで設定しました。

研究会実施に当たり「ソフトウェア品質監査制度」を知るため、IPA(独立行政法人情報処理推進機構)殿に制度説明をお願いし、IPA 技術本部ソフトウェア・エンジニアリング・センター統合系研究員　田中和夫様に講演いただけることになりました。

研究会では、はじめに IPA 田中様から「ソフトウェアの品質説明強化のためのフレームワーク～ソフトウェア品質監査制度(仮称)～」の説明をいただき、その後グループに分かれて検討テーマを決め議論を深めました。

各グループに SAAJ 中部支部、北信越支部、JISTA 中部支部所属の人が各々分かれる組み分けとし、各支部の研究会とは違ったメンバーで議論できるようにしました。初対面の方もいらっしゃいましたが、システム監査人、ITストラテジストとしてベースが共有できていたこともあり、最初から活発な議論が行われました。

懇親会でも活発に意見交換が行われ、懇親終了後も宿泊棟ロビーでシステム監査や今回のテーマも含め夜が更けるまで議論が行われました。

IPA 田中様には講演だけでなく、グループ討議への参加、夜の懇談会への参加、クロージングのグループ発表への総評をいただくことができ、研究会として充実したものとなりました。田中様はじめ IPA 関係者の皆様に感謝いたします。

システム監査人として、今回グループで検討したことも踏まえ、ソフトウェア品質監査制度について今後とも動向をウォッチしていきたいと思います。

今回の研修会場は、九谷焼の地元である石川県能美市の「能美市ふるさと交流研修センターさらい」を利用しました。落ち着いた雰囲気で、部屋表示や洗面台も九谷焼という、日常と少し違う空間で、研修に集中することができました。

研修最終日は、秋晴れとなり、研修終了後、近くの那谷寺や兼六園等で紅葉を楽しんでリフレッシュされた方々もいらっしゃったようです。

今回の合同研究会を盛会のうちに終えることができ、参加された皆様に感謝いたします。ありがとうございました。

［参考情報］

「ソフトウェア品質監査制度部会活動報告書及び関連委託事業報告書」

独立行政法人情報処理推進機構 技術本部 ソフトウェア・エンジニアリング・センター

2012 年 11 月 13 日公開

http://sec.ipa.go.jp/reports/20121113-2.html

以上

■　報告４

【第１７７回 月例研究会受講報告】

会員番号 1792 柴田　幸一

講演テーマ及び講師 ：

1.「SNSの情報セキュリティを考える(フェイスブックが危ない)」:

日本アイ・ビー・エム　経営品質・情報セキュリティ　情報セキュリティ推進室

シニア・セキュリティ・アナリスト　守屋　英一氏

日時 ： 2012 年 11 月 21 日(金)18:30～20:30

場所 ： 機械振興会館 地下 2 階 ホール

講演概要:

1. サイバー攻撃事例

・サイバー攻撃の傾向

攻撃者の変化:標的型から諜報行為型へ、コンシュマー向けの愉快犯から企業・国家の機密情報を盗む攻撃へと変化している。

国家間のサイバー攻撃:安価にダメージを与えることが出来るため、軍事力が低くても可能であることから兵器として利用されている。

・国内におけるサイバー攻撃の分類

H24 上期:標的型攻撃が 1.8 倍と増加した。

政府機関への攻撃が 25%と最も多かった。

2.攻撃の手法

・攻撃の準備:攻撃対象に関する情報の収集し、収集した情報は攻撃対象を騙し、信頼させるために悪用される(ソーシャルエンジニアリング)。

・初期潜入:協力会社や関係者しか知りえない情報を用いて、ウイルスに感染させる等の攻撃を開始する。本人は感染したことに気づかない。

・攻撃基盤構築:ウイルスに感染したパソコンを遠隔操作し、周辺システムに不正アクセスを行う。

・内部情報の収集:組織内のシステムに潜伏し、社内の情報を収集する(認証サーバへのアクセス等)

・最終目的の遂行:機密情報の詐取を実行する、情報を消去する(6 ヶ月程気づかない)。

・サイバー攻撃は電子メールを利用することから SNS 経由へ変化している。

3.講演者からの質問

・現在フェイスブックを利用している方？:出席者の半数が挙手

4.SNS(Social Networking Service)とは

・SNS の種類:LINE, Facebook、Google プラス、mixi 等

・Facebook と他の SNS との違い:Facebook は他の SNS と違いハンドルネーム、ニックネームではなく実名で登録するため安心感、信頼性高い。

5. Facebook とは(実例の紹介)

・撮影した写真を位置情報付でアップ出来る。

・遠隔地の家族に近況の報告をすることが出来る。

・登録している本人の出身校や勤務先等の属性で音信不通の旧友と連絡が出来る。

6. Facebook の登録の変化

・2011 年 1 月 200 万人であったが、2012 年 4 月には 1500 万人へと急増している。

7. Facebook へ加入の動機

・友人に勧められ、皆が話しかけてくれる、コメントに回答をくれるから。

・皆がやっているから、自分もやってみたい。

8. Facebook に関するリスク認識

・実名登録に伴って発生する危険性を認識していない。

・個人情報がどこまで公開されているか知らない。

・登録項目を制限する方法を知らない。

・皆が実名で公開しているから安心している。

9. Facebook の危険性

・事例 1

不倫がバレる:写真に名前をつける機能から、相手が公開した写真から Facebook につながり個人情報が公開され、本人が隠していても関係がバレる。(アメリカで離婚裁判の証拠として採用された事例がある。)

・講演者からの質問

画面の安藤美姫、越直美、北川景子の写真から共通点を見つける。

回答:本人が登録した Facebook でなく、なりすましの画面である。

・事例 2

なりすまし登録:ある調査で全世界登録者の 8.7%(9300 万人)がなりすまし

実名登録の信頼性を逆手にとって、商品の販促目的で口コミを登録する。

著名人になりすまし、偽の投資話を持ちかける。

自分が Facebook に登録していなくてもなりすましの事例がある。

本人確認はメールアドレスであることの落とし穴。

・事例 3

逗子ストーカー事件:「質問コーナ」、「ジオタグ」を利用し、本人の住居をつきとめる。

・事例 4

ターゲット広告:公開された個人情報を利用し、ターゲットを絞り込んで効率的に宣伝をする。広告料が Facebook の収入となっている。

・事例 4

ステルスマーケッティング:あたかも客観的な評判を装い特定な商品の好評・悪評を投稿する(実名登録の悪用例)。

・事例 5

求人会社の素行調査：面接時の参考とするため、本人の Facebook を検索し、過去の記事を取得する。公開された情報は問題ないが、作為的に取得すると職安法に抵触する恐れがある。

過去の情報をリセットしても「ソーシャルインテリジェンス」は過去 7 年の情報をビジネスとして保存している。（古い情報保存を業務にしている。古い情報も消すことが出来ない。）

・事例 6

アカウントの乗っ取り：毎日 60 万件のアカウントが乗っ取られている。

本人の確認はメールアドレスとパスワードであり、パスワードは各システム共通して使用している事例が多い。

ID/パスワードが盗まれても対策として端末を識別する「mTAN」認証技術を導入する。

・事例 7

遠隔操作ウイルス：Facebook では、友人・知人からのメールは気にせずクリックする傾向が強く、感染したユーザからのメッセージを開けてしまい感染した。

10.企業の責任

・企業が注意すべき点

勤務時間中の Facebook の利用の監視

誹謗中傷、プライバシー−侵害、名誉棄損等の投稿に関する監視

情報漏えいの監視

・Facebook 利用に関するガイドラインの策定

総務、法務担当等に限定せず技術的観点から IT 部門を加え策定する。

3 つの基本：①ルールを守る　②発言内容　③責任をもつ。

免責を明示させる（企業でなく個人の発言であることを明示する）

ガイドラインを公開することで抑止効果がある。

11.質問

・Facebook に登録した 6 ヵ月後、メールアドレス帳に登録したメンバーに Facebook 参加勧奨のメールが配信されたが原因は何か？

・ANS:：Facebook 登録時にアドレス帳のインポートを許可する項目があり、停止していてもスマホのバージョンアップ時に許可するように移行する事例がある。

所感

インターネットを用いた便利なコミュケーションツールとして電子メール、ブログ、ツイッター等、次々と提供され、その利便性に誘われ利用者は増加していることに薄々リスクを感じており、フェイスブックの利用は躊躇していました。講演で具体的事例を紹介しながら、連絡先の判らない旧友と再会できたり、著者自身が出版の機会得るなどの有用性があるが、反面、個人情報やメールアドレスを収奪されプライバシーを公表されたり思わぬ攻撃を受けたりする危険性を理解出来ました。「フェイスブック」が危ないのではなく、「フェイスブックの使い方を知らない」ことが危ないのであり、リスクを理解した上でツールとして使いこなすことが重要であることを感じました。事前に資料を配布せず、講演の途中でクイズを織り込む等、肩の凝らない解り易い内容の講演でした。

以上

注目情報（2012/12～2013/1）

■【〈IPA〉年末年始における注意事項】（2012/12/19 発表）

IPA（独立行政法人 情報処理推進機構）は、年末年始の長期休暇中における情報セキュリティに関する注意喚起を発表しています。この注意喚起は、長期休暇中のサービス妨害攻撃や顧客へのウイルス感染、情報漏えいなどのインシデントが起きないよう、また起きた場合の被害が拡大しないことを目的として、(1)システム管理者を対象とした長期休暇前の対応、(2)企業でのパソコン利用者を対象とした長期休暇明けの対応、(3)家庭でのパソコンやスマートフォン、タブレット利用者を対象としたセキュリティ対策、で構成されています。

URL： http://www.ipa.go.jp/security/topics/alert241219.html

■【〈IPA〉2011 年度情報セキュリティ事象被害状況調査報告書の公開】（2012/12/20 発表）

IPA（独立行政法人 情報処理推進機構）は、最新の情報セキュリティ関連の被害実態および対策の実施状況等を把握し、情報セキュリティ対策を推進するため、「2011 年度 情報セキュリティ事象被害状況調査」を実施し、その報告書を IPA のウェブサイトで公開しています。

URL： http://www.ipa.go.jp/security/fy23/reports/isec-survey/index.html

■【〈IPA〉「安全なウェブサイトの作り方」に「ウェブ健康診断仕様」を追加】（2012/12/26 発表）

IPA（独立行政法人 情報処理推進機構）は、「安全なウェブサイトの作り方」に、別冊「ウェブ健康診断仕様」を加えた改訂第 6 版を IPA のウェブサイトで公開しています。

URL： http://www.ipa.go.jp/security/vuln/websecurity.html

■【〈IPA〉「ウイルスの ゴールをゆるすな たよれるキーパー セキュリティ」】（2013/1/7 発表）

IPA（独立行政法人 情報処理推進機構）は、IPA のウェブサイトで、2013年1月の呼びかけとして、「ウイルスのゴールをゆるすな たよれるキーパー セキュリティ」を公開しています。なお、このタイトルは小学生が作成したもので、最優秀賞の標語とのことです。

URL： https://www.ipa.go.jp/security/txt/2013/01outline.html

全国のイベント・セミナー情報

■【東京・月例研究会】

過去履歴はこちら→ http://www.saaj.or.jp/kenkyu/getsurei.html

回	日時	テーマ	講師
第 179 回 月例研究会	1 月 22 日(火) 18:30～20:30	「IT-Audit の ISO 化推進に関する状況報告 (ISO/IECTR30120)」	日本システム監査人協会 システム監査基準研究会

開催場所:東京都港区芝公園 3-5-8　機械振興会館　地下 2 階ホール

案内図　http://www.jcmanet.or.jp/gaiyo/map_kaikan.htm

■【東京・システム監査事例研究会】

【第21回 システム監査実務セミナー】**※本セミナーは募集を終了いたしました。お申込みありがとうございました。**

〈日時〉 2013年2月2日(土)～3日(日)＆2月9日(土)～10日(日)

1泊2日×2回の4日間コース

〈場所〉 晴海グランドホテル(〒104-0053 東京都中央区晴海3-8-1　電話番号03-3533-7111)

〈内容〉 システム監査人の実務能力の維持・向上のため、毎年数回開催しています。

本セミナー受講後の事後課題の内容が適切である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認定に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。

【第9回 事例に学ぶ課題解決セミナー】

〈日時〉 2013年3月2日(土)予定　13:00～17:00

〈場所〉 未定(都内)

〈費用〉 日本システム監査人協会会員　4,000円、その他の方　6,000円

〈定員〉 18名(最小催行人員12名)

詳細は近々SAAJのホームページでお知らせ予定です。

■【東京・法人部会】

【民間企業・団体様向け情報セキュリティセミナー】　http://www.saaj.or.jp/hojin/minkan_seminar.html

【地方自治体様向け情報セキュリティセミナー】　http://www.saaj.or.jp/hojin/chihou_seminar.html

■【東京／大阪・ＣＳＡ(公認システム監査人)資格取得関係セミナー】

【公認システム監査人特別認定講習】(継続開講中)

システム監査技術者試験と関連性のある資格の所有者については、この講習を履修・修了することにより、システム監査技術者試験合格と同様の取り扱いにより、CSA資格を取得する道が用意されています。

詳細は下記URL参照 (SAAJホームページでもお知らせ中)

http://www.saaj.or.jp/csa/tokuninannai.html(公認システム監査人特別認定講習の実施について)

会報編集部からのお知らせ

１．会報テーマについて
２．会報記事への直接投稿（コメント）の方法
３．投稿記事募集

□■ １．　会報テーマについて

2013 年の最初の会報テーマは「システム監査の普及促進」です。

本テーマは、システム監査にかかわるすべての方々の最大の関心事であり、切望している情景でもあると考えてテーマに選びました。

システム監査を社会一般に普及させて健全な情報化社会の発展に寄与することは、当協会の設立目的でもあります。新しい年の初めに相応しいテーマと思いますので、皆様からのいろいろなご意見を会報に寄せていただきたいと願っております。

この「システム監査の普及促進」は、四月号までのテーマとしたのちは今年の”基調テーマ”として、三か月ごとのテーマとは別に一年間継続し、皆様と幅広く深く意見交換して行きたいと考えています。皆様の職場で、そしてご友人と日常的な話題に採り上げるのはいかがでしょうか。また、協会の部会、研究会、支部などの活動の場でも白熱した議論をお願いいたします。

□■ ２．　会報の記事に直接コメントを投稿できます

会報の記事は、
1）PDF ファイルの全体を、URL（ http://www.skansanin.com/saaj/ ）へアクセスして、画面で見る
2）PDF ファイルを印刷して、職場の会議室で、また、かばんにいれて電車のなかで見る
3）会報 URL（ http://www.skansanin.com/saaj/ ）の個別記事を、画面で見る

など、環境により、様々な利用方法をされていらっしゃるようです。
もっと突っ込んだ、便利な利用法はご存知でしょうか。

気にいった記事があったら、直接、その場所にコメントを記入できます。著者、投稿者と意見交換できます。
コメント記入、投稿は、気になった記事の下部コメント欄に直接入力し、投稿ボランをクリックするだけです。
動画でも紹介しますので、参考にしてください。
（ http://www.skansanin.com/saaj/ の記事、「コメントを投稿される方へ」 ）

□■ ３．会員の皆様からの投稿を募集しております

分類は次の通りです。

１．めだか　（Word の投稿用テンプレートを利用してください。会報サイトからダウンロードできます）

２．会員投稿　（Word の投稿用テンプレートを利用してください）

３．会報投稿論文 （論文投稿規程があります）

これらは、いつでも募集しております。 気楽に投稿ください。

特に新しく会員となられた方（個人、法人）は、システム監査への想いやこれまで活動されてきた内容で、システム監査にとどまらず、IT 化社会の健全な発展を応援できるような内容であれば歓迎いたします。

次の投稿用アドレスに、テキスト文章を直接送信、または Word ファイルで添付していただくだけです。

投稿用アドレス:saajeditor ☆ saaj.jp （☆は投稿時には＠に変換してください）

会報編集部では、電子書籍、電子出版、ネット集客、ネット販売など、電子化を背景にしたビジネス形態とシステム監査手法について研修会、ワークショップを計画しています。研修の詳細は後日案内します。

会員限定記事

【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）

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

■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、ご要望等は、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/toiawase/

■この会報は会員の期間中、登録アドレスへ配信されます。

会員以外の方は、送付を希望・停止する場合、次の購読申請・解除フォームから手続ください。

【購読申請・停止】　http://www.skansanin.com/saaj/

■□■ＳＡＡＪ会報担当――――――――――――――――――――――――――――――

編集： 仲 厚吉、安部 晃生、越野 雅晴、桜井 由美子、中山 孝明、藤沢 博、藤野 明夫

投稿用アドレス: saajeditor ☆ saaj.jp（☆は投稿時には＠に変換してください）

――――――――――――――――――――――――――――――――――――