

特定非営利活動法人
 日本システム監査人協会報

2013 年 6 月号
 No **147**

— No. 147 (2013 年 6 月号) <5 月 20 日発行> —

爽やかな季節になってまいりました。

今月号も新緑の季節に相応しい
 新鮮な情報が一杯です。

ぜひ、ご一読を！



1. めだか(システム監査人のコラム)	3
【「道」の活性化……(システム監査活性化への提言)】	
【監査人自身が社会的使命を明確に自覚する(システム監査活性化への提言)】	
2. 投稿	5
【システム監査の活性化】	
3. 新たに会員になられた方々へ(お役立ち情報や協会活用方法)	6
4. 会長コラム	7
5. 協会からのお知らせ	
5.1 システム監査活性化プロジェクト	8
【情報セキュリティ監査研究会だより その2】	
【「個人情報保護マネジメントシステム実施ハンドブック」簡易版 第1章～第3章】	
【ワークショップサポートサービスのお知らせ(新サービス)】	
【システム監査事例研究会だより】	
【CSA利用推進グループの活動紹介】	
5.2 ご寄附等の報告	22
6. 注目情報(2013/3～2013/5)	23
【IPA 「標的型攻撃の防御に向けた情報共有の枠組み、J-CSIP の活動レポート」公開】	
【警察庁 13 都道府県警察に「サイバー攻撃特別捜査隊」を設置】	
【IPA 5月の呼びかけ「スマホにおけるワンクリック請求の手口に気をつけよう！」】	

7. 全国のイベント・セミナー情報	24
【協会主催イベント・セミナーのご案内】	
【月例研究会開催予定】	
8. 会報編集部からのお知らせ	28
【会報テーマについて】	
【会報記事への直接投稿（コメント）の方法】	
【投稿記事募集】	
会員限定記事	29

めだか 【「道」の活性化……（システム監査活性化への提言）】

システム監査活性化はシステム監査が歩む「道」、その「道」の姿と監査人が歩く姿のことではないだろうか。「道」は目的地への過程で、過程を活性化させることこそ重要であると思っている。ゴールテープを切るような特定地点到達が活性化ではないと思っている。

“システム監査を活性化しなければならない” “活性化が求められている” “活性化しよう！” と、「システム監査活性化」のテーマに関して、様々な観点から多くの意見や提言がこの会報に寄せられている。この「活性化」に対して、我々システム監査人は具体的に何を実施すべきか考えてみた。

【道＝^{イコール}過程】

活性化の具体策は、「道」という視点を持つことで導き出されるのではないだろうか。「道」はシステム監査の日々の歩み・プロセス・アプローチを指し、目的地ではなく過程、言い換えれば途中経過だ。活性化の具体策は、システム監査が歩む「道＝^{イコール}過程」を元気にすることと思っている。もちろん、目的や目標の姿を定めた活動は重要だがそれも途中段階の仮目標であろうと考え、それらを含めた「道＝^{イコール}過程」を重視したいと考えている。

システム監査の目的・目標（役割・期待像）はこれまでも大きく変化して来た。社会、経営、情報システム、利用者など様々な環境変化から当然の変化だ。今後も必然でそれを見通すことは実際は困難だ。

筆者の例を引いて心苦しいが、折々に目標を定めて来たがいつも漠然としていた。いつも軌道修正していた。常に途中の仮のもので最終的な目標はいつも見えない。そのようなものと思う（投げやりではない）。

さらに偉人を持ち出すのは唐突で不遜だが、アインシュタインの相対性理論も決して目的を達成した結果ではなく、仮定にもとづく研究活動の途中経過を表したものであると思う。

この枠内は大変な論理飛躍があるが、投稿テーマを考えた背景をコメントした。

改めて述べる。システム監査の活性化は、システム監査が歩む「道」をエネルギーに、そして生き生きとすることであると思う。SAAJでいえば日々の協会活動そのものが「道」だ。

【道＝^{イコール}システム監査ロード】

この「道」をワイワイと賑やかにすることが活性化と提案したい。賑やかなこの道を「システム監査ロード」と呼びたい。システム監査ロードは前後左右どの方向から歩くことがあってもいいし、繁華街のようにぶつかるような混雑こそ望ましいと思う。システム監査ロードを歩く人はシステム監査人並びに志を一にする仲間だから、システム監査について気軽な挨拶や様々な意見交換、そして難しい議論も自然と発生するだろう。

このような状態にシステム監査活性化の姿が見えてくるのではないだろうか。「道」で交わされる話題・テーマから多くの可能性が生まれるに違いない。そして、見失ってならない点は、現在のすぐ近くにシステム監査ロードがあることだと思う。半歩も踏み出せばその「道」に立てて、今すぐに歩ける「道」だと思う。



（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。）

2013.05 投稿

めだか 【監査人自身が社会的使命を明確に自覚する（システム監査活性化への提言）】

前回の私の本コラムで、情報システムは本質的に不完全性を内在するが、関係当事者（開発を指示する者、開発をする者、利用する者など）がそれを正面から受入れ、乗り越える（情報社会の恩恵を享受する）ためには、関係当事者の相互信頼関係の確立が欠かせず、そのためには各当事者（特に「開発者」、あるいは「情報システムサービス提供者」）の説明責任遂行（やるべきことはやっていることを自ら説明すること）と、その説明へ信頼性を付与するための第三者による保証（システム監査）が必然的に求められると書いた。

つまり、情報社会でのシステム監査の需要は必然だと述べた。

話は変わるが、自民党政権に代わったこともあるのか、企業及び国民の冷えた経済マインドも少しずつ変化し、平均株価は 14,000 円を超え、新聞では航空機はビジネスクラス、また豪華客船クルーズを組み込んだ高額海外ツアーの広告が1面ぶち抜きで頻繁に出され、街中では大規模ビル建設が更に加速しているようにも思える。

そして、マイナンバー法案の成立も視野に入り、関連システム開発は少なく見積もっても数千億円、民間企業のシステム改修なども見込むと、ここ数年で兆円単位のIT需要が見込まれ、IT業界は正に特需の時代に入ろうとしている。

景気が良くなれば企業活動も一層活性化し、IT投資も増え、結果、冒頭に述べた文脈で、システム監査の需要も顕在化してくると考えられる。しかし、この流れは間違いないとしても、そのスピードは様々な要素で刻々変化し読み難い。そして、システム監査に携わる方々の中には痺れを切らして、システム監査よりシステムコンサルティングの方がビジネスチャンスはありそうだと考え宗旨替する人もいて残念と前回のコラムに書いた。

システム監査人は、まず情報社会の中でのシステム監査の役割（自身の仕事の社会における役立ち）について再確認、再認識し、システム監査人の“時代の使命”を明確に自覚すべきと思う。

そして今、あるいは今年の自身のビジネスにどう結びつくかは明確でないとしても、そう遠くない将来の社会的システム監査ニーズに適格に応えられるよう準備を怠ってはならないと思うのである。システム監査が普及しないことを嘆いて時間を潰すより、時に備え、システム監査人の足下をより強固にすることに目を向けたい。

例えば、監査方法論の深化、評価基準の整備、評価基準への適合を判断するための監査要点の詳細化、調査、インタビュー実務テクニックの深化、サンプリング理論の実務への適用手法、監査実務でのIT利活用の推進、監査結果の適格な報告技術などの深化、そして変化するIT技術動向の把握などが思いつく。

組織的、政策的、また制度的な措置も勿論必要だが、まずは、システム監査人が気持ち（^{こころざし}志）を高く持ち続け、継続的に研鑽を積み重ねることが、システム監査活性化の一丁目一番地ではないだろうか。

楽観論、強い思い込み、また単なる理想論、精神論と批判されそうだと思いつつ書いてみた。

ご意見、ご指摘を是非お願いしたい。

（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。）

2013.05 投稿

投稿 【 システム監査の活性化 】

会員番号 0557 仲 厚吉(システム監査活性化プロジェクト)

システム監査活性化を考えるため、NPO活動原点に立ち帰って特定非営利活動促進法を読みかえしてみました。

第一章 総則、第一条(目的)に、この法律は、特定非営利活動を行う団体に法人格を付与すること並びに運営組織及び事業活動が適正であって公益の増進に資する特定非営利活動法人の認定に係る制度を設けること等により、ボランティア活動をはじめとする市民が行う自由な社会貢献活動としての特定非営利活動の健全な発展を促進し、もって公益の増進に寄与することを目的とする、とあります。第二条(定義)には、この法律において「特定非営利活動」とは、別表に掲げる活動に該当する活動であって、不特定かつ多数のものの利益の増進に寄与することを目的とするものをいう、とあります。当協会のNPO活動は、別表の十四の「情報化社会の発展を図る活動」に該当しています。

当協会の定款では、第3条(目的)に、本法人は、システム監査を社会一般に普及せしめると共に、システム監査人の育成、認定、監査技法の維持・向上をはかり、よって、健全な情報化社会の発展に寄与することを目的とする、とあり、また、第4条(事業)で、本法人は、前条の目的を達成するため、次の種類の特定非営利活動を行う、とあります。

- (1) 社会教育の推進を図る活動
- (2) 国際協力の活動
- (3) 前各号に掲げる活動を行う団体の運営又は活動に関する連絡、助言又は援助の活動

あらためて NPO 活動の原点に立ち帰ると、当協会は、システム監査によって社会貢献活動を図り、もって公益の増進に寄与することを課せられていることがわかります。つまり、当協会によるシステム監査の活性化は、会員やシステム監査人のボランティア活動が、情報化社会の発展を図って公益の増進に寄与することと同義になると考えられます。

ここで、当協会のシステム監査人(CSA、ASA)資格を考えてみます。この資格は、システム監査技術者や同等の資格をレベル4と位置づけて、さらにシステム監査の職務経歴や実務経験を試問して、レベル5の認定を行っています。当協会は、この資格の取得について当協会の会員資格を前提としていません。つまり、会員の共益活動のみならず、広く一般に情報化社会の発展を図るため、社会教育の推進を図り、公益の増進に寄与する活動を行っています。

また、当協会は、システム監査基準研究会を中心にシステム監査の ISO 化の動きを支援する活動を行っています。当協会から、ISO/IEC JTC1/SC7/WG40 の会議に出席し、8月には東京で会議が開催されます。これは、国際協力の活動になりますが、システム監査を通じた公益の増進に寄与する活動になっています。

上記の他にも、当協会では、各部会、研究会、各支部において、システム監査を主題にして、広く一般に情報化社会の発展を図る活動を実施し、また他団体との連携活動を行っています。しかし、外部への広報が十分であったかを省みると、システム監査の活性化は、先ず、当協会の公益の増進に寄与する活動を広く一般の人に知ってもらうこと、期待を喚起してそれに応えていくこと、そして他団体との連携を強化していくこと、であると思います。

以上

新たに会員になられた方々へ



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.saa-j.or.jp/annai/index.html>
- ・会員規定にも目を通しておいってください。 http://www.saa-j.or.jp/gaiyo/kaiin_kitei.pdf
- ・みなさまの情報の変更方法です。 <http://www.saa-j.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.saa-j.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.saa-j.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、見学也大歓迎です。

ご意見募集

- ・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.saa-j.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.saa-j.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.saa-j.or.jp/csa/index.html>

会報

- ・PDF会報と電子版会報があります。(http://www.saa-j.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.saa-j.or.jp/members/kaihouinfo.pdf>

お問い合わせ

- ・右ページをご覧ください。 <http://www.saa-j.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

“システム監査に関わる者は、システム監査の役立ちを十分認識しておく必要がある。”

2013.05 投稿

会長コラム 【マイナンバー法案、PIA とシステム監査人】

会員番号 0841 沼野伸生(会長)

民主党政権時代に検討、議論が始まったマイナンバー制度がいよいよ正式に決まりそうです。

この原稿を書いている5月10日の朝刊には、「行政手続における特定の個人を識別するための番号の利用等に関する法案」(所謂、マイナンバー法案)が衆議院本会議で9日に可決され、今後参議院に送られ今国会中に成立する見込みとなっています。

ご承知の通り、マイナンバー制度では、国民に住民票コードを元に個人番号(マイナンバー)を付番し、まず社会保障、税、及び災害対策に関する分野で利用し、将来的には他の行政分野、また行政以外の分野での利用の可能性も想定しているものです。(尚、法人についても、識別のための番号(法人番号)が振られます。)

番号付番は情報システムでの処理を前提に考えられているものであり、その意味ではマイナンバー法の目的の実現に情報システムは欠かせません。

公表されている資料によれば、マイナンバー制度に関連し新たに開発する主な情報システムとして、個人番号生成機能、情報提供ネットワークシステム(情報連携を司る仕組み)、マイ・ポータルシステム(自身の情報の遣り取りをインターネット上で確認できる仕組み)、個人番号カード(マイナンバーカード)などが挙げられ、また、これらのシステムとの連携に伴い、住民基本台帳システム、公的個人認証サービス、また各自治体の関係業務システムの変更も必要とされています。加えて、民間企業においても「個人番号関係事務実施者」の立場で、例えば行政に提出する「給与支払報告書」などの法定調書にマイナンバーを記載することとなるため必要なシステム変更が見込まれるなど、関連情報システムの開発、変更は相当大掛かりなものです。

勿論、主要なシステムの開発では既にシステム監査の実施が計画され、正にシステム監査の出番とも言えます。会員の皆さんの中にも仕事としてそれに関わるシステム監査人の方がいるのではないのでしょうか。

さて、ここではマイナンバー制度におけるプライバシー保護への配慮の一つとして取り入れられる特定個人情報保護評価について触れたいと思います。

(因みに、“特定個人情報”とは、マイナンバーをその内容に含む個人情報のことです。)

特定個人情報保護評価は、PIA(Privacy Impact Assessment: プライバシー影響評価)に相当し、特定個人情報ファイルを取扱うに当たって(そのシステムを開発、変更するに当たって)、事前にプライバシーへの影響評価を実施し、その結果により必要な措置を事前に組み込むというものです。システム監査における企画段階の監査の考え方に似ています。

マイナンバー法案では主として行政機関の長に、また特定個人情報保護ファイルの取扱いに限って義務付けられるようですが、今後のマイナンバー利用の拡大に伴って幅広く実施されていく可能性も感じられます。

そして、このPIAの実施者の一人として、また実施したPIAの適切性評価者として、システム監査人がその役割の一端を担うことも、我々システム監査人の今後の検討テーマの一つと思っています。

尚、来月(6月17日(月))の当協会月例研究会では、このPIAをテーマに取り上げる予定です。

興味のある方は当協会HPから申し込み、ご参加下さい。

以上

2013.05 投稿

協会からのお知らせ【システム監査活性化プロジェクト】

会員番号 6027 小野 修一(システム監査活性化プロジェクト 主査)

今月の会報では、当協会の研究会や担当組織が行っている活動の中から五つの活動について、ご紹介しています。いずれも、活性化プロジェクトの活動方針に沿った活動です。会員の皆様には、各活動への積極的なご参加をお願いします。

1. 情報セキュリティ監査研究会

当研究会の中で討議、意見交換を行っているテーマについて、できるだけ生の情報をお伝えしたいという主旨で、毎号の会報でご報告しています。今号でも、最近の研究会での意見交換の内容をご報告しています。研究会に入会し、一緒に活動していただける方がいらっしゃいましたら、ご連絡をお願いします。

2. 個人情報保護監査研究会

当研究会でまとめた『PMS 構築ハンドブック』簡易版の内容を、毎号の会報で、紹介をしています。今号でも、その一部を紹介しています。

3. 事例研究会

当協会の研究会の中でも、長い歴史をもつ研究会です。システム監査普及サービスの実施によって得たノウハウを、実践セミナー、実務セミナー、課題解決セミナーなどで、会員の皆様、さらには協会外の皆様にも提供しています。本号では、そうした事例研究会の活動について、ご紹介しています。

4. WSS（ワークショップ支援サービス）

昨年度の会員増強プロジェクトから、ワーキンググループを設けて検討を行ってきたサービスが、いよいよスタートの時を迎えました。詳しくは、本会報に掲載されているチラシおよび解説記事をご覧くださいのですが、当協会がもっているシステム監査に関する専門的知識・実践ノウハウを、必要としている企業・組織に提供するという主旨です。当協会の活動理念である「システム監査の普及によって、健全な情報化社会の構築に寄与する」を体現する活動といえます。

これからスタートしようという活動ですので、いろいろな問題が出てくるかも知れませんが、一つずつ解決して成果を上げていきたいと思っています。

5. CSA利用推進グループ

当協会が認定している CSA、ASA の皆様に焦点を当てた活動を行っています。

今号では、今年度の大きな活動の1つである「CSA・ASA 全体交流会」のご案内をしています。

「CSA 継続教育セミナー」と連携し、セミナー終了後に交流会を行い、知識の習得と人的ネットワークの構築の両方の場を1日で提供しようという企画です。ぜひ、多くの方にご参加いただければと思います。

今回ご紹介した以外にも、当協会では、活性化プロジェクトを中心に、各研究会、委員会、担当組織が活発な活動を行っています。会員の皆様の活動への積極的な参加、ご意見をお願いいたします。

以上

【情報セキュリティ監査研究会だより その2】

会員番号 0056 藤野明夫(情報セキュリティ監査研究会)

はじめに

情報セキュリティ監査研究会では、その活動状況を5月号から会報に毎号掲載することにしました。第一回は、最初でしたので研究会の雰囲気をご紹介しますために、3月21日に開催されました第11回情報セキュリティ研究会の様子をお伝えいたしました。今回は、そもそも当研究会としての課題認識は何であるか、何を求めているかについてご説明したいと思います。さらに次回以降、この課題意識にもとづいて、どのような議論が行われ、どのような結論になりつつあるかをご紹介しますと思います。

1. 現状認識

最近のデジタル・ネットワーク革命の凄まじさは、経済面だけではなく社会構造そのものを根底から覆すほどの勢いがある。今やあらゆるモノやコトはICT抜きには語ることができなくなっている。2010年ころから、北アフリカでジャスミン革命と呼ばれる現象が起こった。これはモバイルフォンによるSNSやウィキリークス等、まさにICT革命すなわち技術革新がそのまま政府転覆に繋がるという人類史上初めての経験であった。

これほどではなくても、次々と現れる様々なデジタル・ネットワーク技術によって、世の中が大きく変わっている。音楽配信によりCD売上は激減、また、新聞業界はかつて売上の半分を占めた広告料収入が三分の一になり、青森県ではこの10年で書店の数がやはり三分の一になったという。学生の就職活動もネットが基本になり、さらには企業側、学生側双方とも就職活動にSNSを利用し始めているという話も聞く。

また、一昨年の東日本大震災では、ツイッター等のソーシャルメディアが情報伝達や人々の所在地等の確認手段として大きな役割を果たした。また、ビッグデータの活用による種々の制御や購買行動のコントロール、スーパーコンピュータの活用による高度なシミュレーションや解析による新たな知見の獲得、スマホやタブレット端末の普及やソーシャルメディアの浸透による一般市民の新しい生活スタイルの確立や人間関係の変化、等々、従来の「情報処理システム」と呼ばれていた時代、ICTがビジネスプロセスに閉じていた時代とは全く異なる活用が進展し、それにとまらぬ社会革命が進行している。

一方で、昨年、ウィルスによって乗っ取られた端末の所有者が、犯罪者として誤認逮捕されたり、ネットバンキングで不正に振込みがなされたりするなど、極めて重大な事件が立て続けに起こっている。また、ネットワーク上を流れる膨大な個人情報、その収集が可能な企業に蓄積され高度な分析が行われ、結果としてその企業にアクセスする人々を自社の都合のよい方向に誘導することも可能になってきている。「ビッグデータ」は、それを取得、分析、活用できる一部の企業や政府等と、その結果、ある種の「誘導」の対象となる個人との間に圧倒的な情報の非対称性を持つ。このような負の側面あるいはリスクはますます増大している。本当にこのままでよいのかという気がしてくる。

このような大きな変化に対して、我々、システム監査人は何ができるのであろうか、また、何を期待されているのであろうか、また、何をすべきであるのか、もう一度、原点に戻って考えてみたいというのが当初の課題認識である。

2. システム監査人に求められるもの

一方で、経営者のわれわれICT専門家に対する期待は、従来とは明らかに異なっている。この点については、昨年9月の月例研究会における講演において、東京海上日動システムズ株式会社代表取締役社長 横塚裕志氏は、「現在のICTに対する経営層の期待は、従来の業務効率化から、経営戦略を踏まえたビジネスへの貢献に移っている」と指摘している(会報140号(2012年11月号)参照)。

われわれシステム監査人を含む世の中のICT専門家は、この新事態に対してどのように対応しているのであろうか。口では、データの利活用による新ビジネスの創出とか、先端的ICTの活用によるビジネスプロセスの革新といったが、それを遂行あるいはチェックする能力がどれほどあるのだろうか。はなはだ心もとない状況にあるので

はないか。

もっとも、システム監査人は、システム開発者ではなく、またコンサルタントでもないから、上述の横塚氏の期待に対して応える方法は、最新のICTを使って革新的ビジネスモデルを創出する、あるいは、提案するというのではない。むしろ、開発した新システムが適切にICT革命の成果を反映しビジネス革新に有効なものになっているかを、事後的または開発過程において検証するということを期待されているのであろう。いわば**ICTシステムのビジネスプロセス革新への有効性の監査**という側面である。

また、前述のごとく、ビッグデータやSNS等の活用においては、個人情報保護の問題を筆頭として今までのICTシステムではさほど問題にならなかったコンプライアンス上のリスクが発生し、また、このリスクに対する過度の警戒心が日本のICT革命を遅らせているという指摘もある。このようなコンプライアンスリスクに対して、当該システムが妥当な設計になっており、適正に運用されているか、ということの検証をわれわれシステム監査人は求められているのではないだろうか。**ICTシステムのコンプライアンスリスクに対する設計と運用の妥当性の監査**という側面である。

さらに、前述のごとく成りすましによる誤認逮捕に見られるように、社会インフラとしてのICTの重要性が高まるにつれて、セキュリティリスクは増大の一途を辿っている。また、国家レベルでサイバーテロを企てる例も出てきている。ネットワークを通じて様々なインフラがコントロールされるようになってくると、セキュリティ上の欠陥が人の命を直接、奪う危険性も出てきた。セキュリティリスク、とりわけ、ネットワークセキュリティリスクが適切にコントロールされているかということを検証するということも従来に比べてはるかに重要になってきている。**ICTシステムのセキュリティリスクのコントロールの妥当性の監査**という側面である。

それでは、これらの期待に応えるにはどのようにしたらよいのであろうか。それには、現在進行しつつあるデジタルネットワーク革命の実相を我々自身がきちんと把握すべきではないのか。そこで、次節に述べるようにまずは取り組むべきテーマの選定から始めることにした。

3. テーマの選定について

前述の三つの側面のすべてにわたって応えることは、短时日の間には不可能である。そこでテーマを二点目の「ICTシステムのコンプライアンスリスクに対する設計と運用の妥当性の監査」に絞ることにした。ここに絞ったのは、以下の理由による。

一点目の「ICTシステムのビジネスプロセス革新への有効性の監査」は、ICT革命の技術的要素に対する深い知識がないと実現できない。また、そのビジネスへの有効性という点に至っては、ビジネスシーンごとに大きく異なり一般論で議論するのは至難の業である。

三点目の「ICTシステムのセキュリティリスクのコントロールの妥当性の監査」については、その重要性については論を待たないが、これもまたセキュリティ技術やネットワーク技術に対する深い知識が必要になる。また、技術的には旧来の情報セキュリティ技術の延長上にあるもので、近年のデジタルネットワーク社会の発展でその重要性が増大したというのみであり、テーマとして新味のあるものではなく、要素技術としてはレガシーなものである。さらに情報セキュリティについてはシステム監査とは別に「情報セキュリティ監査制度」が存在し、よりジェネラルな役割を持つシステム監査人として深堀するにはいささか、ためられる面がある。

そこで、当研究会では、二点目のICTシステムのコンプライアンスリスクに対する設計と運用の妥当性の監査を最初に取り組むべきテーマとして選んだ。この側面は、ビッグデータやSNS等、最近のデジタルネットワーク革命の中からその重要性の面においても、また技術的にも新たな課題や対処策が検討され、また社会的にも従来にない異質の問題を提起しているという点でもシステム監査人協会の取り上げるべきテーマとして妥当なのではないかと考えたからである。

この分野は、①デジタル・ネットワーク革命で創出された革新的技術が、急速に社会インフラ化していく過程で生じた新しい問題であること、②その解決のためには、技術的側面のみならず法的側面、社会的側面、経済的側面、

あるいは心理的側面といった多方面からのアプローチが必要であり、様々なバックグラウンドを持つ多様な人材を抱える我々システム監査人協会にとって相応しいテーマであること、③その革新性ゆえに既得権とのコンフリクトが発生しがちで、既存の企業では取り組みにくく、その点では何ら既得権がなく、独立性の高い当協会に相応しいテーマであると思われること、④したがって、まさにフロンティア領域であり今から真剣に取り組めばシステム監査人協会がこの分野でリーダーシップをとることができ、システム監査人のビジネスチャンスの拡大につながる事、⑤仮にそこまでゆかなくても、この分野で適切な情報を発信し続ければ、システム監査人協会のプレゼンスが向上すること、⑥さらにそこまで行かないとしても、かかる先端分野について協会内で議論すること自体が協会の活性化につながる事、これが当研究会でこの分野をテーマとして選んだ理由である。

4. 輪読形式での学習と討議

ICTシステムのビジネスプロセス革新への有効性の監査に取り組むにあたり、まずは、この分野において何が問題であるか、また、それはどのように解決されようとしているかを把握しなければならない。それを明らかにするため、2012年度から2013年度前半にかけては、その利活用の効果が喧伝される一方で、個人情報問題を中心に様々なリスクが存在するビッグデータの問題を研究テーマとした。テキストとして、ビッグデータの価値や意義、その基本的技術や課題、個人情報保護を含むコンプライアンスリスク、安全性、信頼性等がコンパクトにまとめられている、IPA（独立行政法人情報処理推進機構）編、2012年3月発行の「くらしと経済の基盤としてのITを考える研究会報告書 つながるITがもたらす豊かなくらしと経済 ～ ビッグデータの価値と信頼 ～」（*1）（以降、資料のURL等は、文末にまとめる）を採用した。

このテキストを月一回の定例研究会において輪読形式で読み、議論をし、また必要に応じて、適宜、別資料を参照している(*2)。次回以降は、この議論の内容と結論を紹介していきたい。

【資料】

(*1) IPA（独立行政法人情報処理推進機構）編、2012年3月発行

「くらしと経済の基盤としてのITを考える研究会報告書 つながるITがもたらす豊かなくらしと経済
～ ビッグデータの価値と信頼 ～」

URL <http://www.ipa.go.jp/about/research/2011bigdata/>

(*2) 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・エンジニアリング・センター

2012年11月13日公開の下記URLのホームページ参照

「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」

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

【情報セキュリティ監査研究会への参加について】

当研究会にご興味をもたれましたら、是非、ご参加いただきたいと存じます。毎月20日前後にSAAJ事務局で定例研究会を開催しております。参加ご希望の方、また、当会報をご覧になってご意見やご質問のある方は下記アドレスまでメールでご連絡ください。

[security ☆ saaj.jp](mailto:security☆saaj.jp) （発信の際には“ ☆ ”を“ @ ”に変換してください）

以上

「個人情報保護マネジメントシステム実施ハンドブック」簡易版 第1章

会員番号：1792 柴田幸一（個人情報保護監査研究会）

2013年5月号の[序章](#)に続き、今回は第1章、第2章、第3章をご紹介します。

第1章 プライバシーマーク取得計画

1.1 事業者の特性に合わせたPMSの確立

個人情報保護マネジメントシステム（PMS）の構築は、まず自社の業務をよく認識することから始まります。そのための効果的な取り組みとして、次のa)～c)の3要素が挙げられます。

a)	プライバシーマーク取得体制への組織的支援
b)	計画やルールの特明確化
c)	確実な実施と点検

1.2 プライバシーマーク取得計画

プライバシーマーク認証申請は、一連のPDCAを一回以上実施した記録を提出します

P	Plan	計画、体制、方針の公表、基本規程の制定
D	Do	個人情報の特定、リスク分析、対策の規定化、委託先選定、教育実施
C	Check	点検、監査
A	Act	是正処置、予防処置、代表者の見直し

1.3 認証申請

下記の指定書式を、指定審査機関のサイトからダウンロードして、書類を作成し提出します。

ご参考：JIPDEC <http://privacymark.jp/application/new/index.html>

書類名	内容
様式1	Pマーク付与適格性審査申請書（新規）
様式2	会社概要
様式3	個人情報を取り扱う業務の概要（従業員数、顧客数、DBレコード数など）
様式4	すべての事業所の所在地及び業務内容
様式5	個人情報保護体制
様式6	PMS文書（内部規程・様式）一覧
様式7	JISQ 15001 要求事項と、様式6に記載した規程、様式との対応表
様式8	教育実施サマリー（全従業員への教育100%実施結果）
様式9	監査実施サマリー（全部門の監査結果）
様式10	代表者による見直し実施サマリー
様式11	登記事項証明書（監査役が個人情報保護体制の一部を占めていないこと）
様式12	定款
様式13	会社パンフレット
事業者文書	PMS文書（様式6で記載した全文書のコピー。インデックスを忘れずに）
記録	個人情報管理台帳、リスク分析表のコピー1ページずつ

認証申請が受理されると、指定機関から「申請料5万円」の請求があります。

1. 4 文書審査

申請時に提出する「事業者文書」は、P D C Aの各段階で使用する規程や記録様式ですが、JIS Q 15001:2006の要求事項の項番をもとに、4桁～6桁の番号を付けて策定します。

例：「**3341個人情報保護体制図**」（JIS規格3.3.4 資源、役割、責任及び権限）

現地審査の1～2カ月前に、提出したPMS文書（規程類、様式）の審査結果が郵送で到着します。審査結果が「×」の項目について、現地審査までに規程を見直します。

1. 5 現地審査

現地審査の所要時間は、事業者の規模によって異なります。

現地審査時間		5時間	6時間	8時間
業種分類	規模	小規模	中規模	大規模
製造業 ・その他	資本金or出資総額	2～20人	3億円以下、又は 従業者数 21人～300人	3億円超 かつ301人～
	従業者数			
卸売業	資本金or出資総額	2～5人	1億円以下、又は 従業者数 6人～100人	1億円超 かつ101人～
	従業者数			
小売業	資本金or出資総額	2～5人	5000万円以下、又は 従業者数6人～50人	5000万円超 かつ51人～
	従業者数			
サービス業	資本金or出資総額	2～5人	5000万円以下、又は 従業者数 6人～100人	5000万円超 かつ101人～

現地審査後に、請求書が到着します。（2013年4月現在）

業種分類	小規模	中規模	大規模
審査料（新規）	20万円	45万円	95万円
審査料（更新）	12万円	30万円	65万円

1.6 指摘対応

現地審査後、約1週間で指摘事項文書が到着します。

指摘事項の項目ごとに、PMS文書で規定した「**3801 是正・予防処置報告書**」を作成し、不適合となった真の原因を追究し、3か月以内に改善報告書と改善証憑（エビデンス）を提出します。

1.7 審査会

すべての指摘事項が改善された後、1～2カ月後の審査会で、プライバシーマーク認証の最終判定がなされます。状況によっては、再度改善が必要と指示されることもあります。

1.8 プライバシーマーク取得

審査会で承認されると、1～2週間後に、事務局より付与認定通知、Pマークの使用注意などが到着します。

2年分の付与登録料は下記のとおりです。（2013年4月現在）

業種分類	小規模	中規模	大規模
付与登録料	5万円	10万円	20万円

■

2013.05 投稿

「個人情報保護マネジメントシステム実施ハンドブック」簡易版 第2章

会員番号：1792 柴田幸一（個人情報保護監査研究会）

第2章 個人情報保護方針などの公表

2.1 個人情報保護方針

代表者は個人情報保護の理念を明確にし、次の事項を含む「**3200 個人情報保護方針**」を定め、従業員に教育し、一般の人が入手できるようにホームページ等に掲載します。

a)	事業の内容及び規模を考慮した適切な個人情報の取得、利用及び提供に関し、目的外利用を行わないこと及びそのための措置を講じること。
b)	個人情報の取扱いに関する法令、国が定める指針、その他の規範を遵守すること。
c)	個人情報の漏えい、滅失又はき損の防止及び是正に関すること。
d)	苦情及び相談への対応に関すること。
e)	PMSの継続的改善に関すること。
f)	代表者の氏名
g)	制定日および最終改定日
h)	方針に関する問合せ先

ホームページを持たない企業は、リーフレットを作成して提示できるようにしてください。

2.2 個人情報の取り扱いについて

「個人情報保護法」では、利用目的（法第18条）、開示等の諸手続（法第24条）、苦情の申出先（法第24条）を、本人の知り得る状態に置かなければならないと定めています。そのため公表事項として「**3210 個人情報の取り扱いについて**」を規定し、方針とは別にホームページ上で公表します。

2.2.1 利用目的の公表

自社で取り扱うすべての個人情報について利用目的を公表します。受託、第三者提供にて取得、共同利用で取得している個人情報についても、その利用目的を漏れなく公表します。

2.2.2 開示等への対応

開示等の諸手続について公表します。

a)	開示等の求めの申出先
b)	開示等の求めの方式（提出すべき書面の様式等）
c)	開示等の求めをする者が、本人又は代理人であることの確認の方法
d)	利用目的の通知、情報開示の場合に手数料を定めた場合の手数料及び徴収方法

2.2.3 苦情・相談対応

苦情・相談対応については「個人情報保護法」だけでなく、政令においても強調されています。

a)	苦情の申出先
b)	「認定個人情報保護団体」の名称及び苦情の解決の申出先（団体所属事業者の場合のみ）

「認定個人情報保護団体」（JIPDEC など）には、Pマーク取得後申し込みをすることができます。

■

「個人情報保護マネジメントシステム実施ハンドブック」簡易版 第3章

会員番号：1792 柴田幸一（個人情報保護監査研究会）

「実施ハンドブック」原本では、「3301個人情報取扱規程」と「3430安全管理規程」の2つの規程によってPMSを構築し、PMSで使用するすべての様式を規定しています。先頭の4～6文字は、JIS 規格の項番とできるかぎり一致させています。

第3章 計画

JIS 規格の3.3を反映し、「3301個人情報取扱規程」1.1 には以下を規定しています。これにより、教育および監査の対象についても全従業員、全ての組織、すべての個人情報対象となります。

適用範囲	PMSは、当社の全従業員（役員、社員、嘱託、パートタイマー、アルバイト、派遣社員）、及び全ての組織に適用する。
適用対象	PMSは、当社の事業の用に供しているすべての個人情報を適用対象とする。

3.1 体制

代表者以下の、標準的な体制を「3341個人情報保護体制権限表」によって明確にします。

役割	権限(抜粋)
代表取締役社長	「3200個人情報保護方針」「3305個人情報保護体制」の承認 「3301個人情報取扱規程」「3430安全管理対策規程」の承認 「3303PMS年間計画書」「3451教育計画書」「3721PMS監査計画書」の承認 「個人情報保護管理者」「監査責任者」を会社内部より任命。3721監査報告書の受理 「緊急事態発生」時に対策委員長として指揮を執る。 「苦情」は緊急事態と認識し報告を受け必要な処置をとる。 「3801是正・予防処置報告書」による不適合承認、立案承認、効果の確認 「代表者による見直し」実施
個人情報保護管理者 兼 教育責任者 安全管理責任者	「3200個人情報保護方針」の策定、公表 「3210個人情報の取り扱いについて（開示手続きを含む）」の承認および公表 「3301個人情報取扱規程」「3430安全管理対策規程」3341個人情報保護体制」の周知 「3303PMS年間計画書」「3451教育計画書」の策定 「3801是正・予防処置報告書」のうち、軽微な不適合の確認、立案承認 「監査の結果を含めたPMSの運用状況」を代表者に報告する。
監査責任者	「3303PMS年間計画書」に基づく「3303監査計画書」の策定 「監査担当者」の任命、「監査の実施」「3303監査報告書」の作成 「フォローアップ監査」の実施
PMS事務局 (開示・問い合わせ ・苦情・相談窓口)	個人情報保護管理者の業務について、その指示に従う。 規程、様式、記録の管理、各部門との連絡・調整 「3303PMS年間計画書」に基づく「3456教育テキスト」の策定 「教育」の実施、「教育」の評価、「開示請求」初期対応、「苦情」初期対応 「日常点検」「次年度年間計画の立案」
システム管理責任者	情報システムの安全管理について適切なレベル維持を行う。 「3432-010システム機器・ID管理台帳」のアクセス権限設定、更新、点検 情報システムの運用監視(アクセスログ監視、バックアップ管理等)
部門管理者	「3311業務フロー」「3312個人情報管理台帳」「3313リスク分析表」の策定 「3319個人情報取得・返却・廃棄・消去管理表」による個人情報の適正管理 「3434-02委託先選定基準」による、業務委託先の選定・評価 業務委託先との契約締結、委託先の監督 「是正・予防処置」の立案、処置の実施
担当者	部門における個人情報の適正管理 部門における業務委託先の日常監視

3.2 年間計画

初年度は、「3302PMARK 取得計画表（初年度）」を策定することになります。

		PMARK認証取得スケジュール/実績表																														★
		201★年度(PMARK新規取得計画)																														
		6月					7月					8月					9月					10月					11月					
		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
準備	個人情報保護方針公表	1																														
	取扱規程	1																														
	組織・体制決定	1																														
	従業員からの同意取得		★		様式	★		同意取得																								
構築	個人情報の特定		★																	★												
	法令・指針等の特定		★																													
	リスク分析、対策の検討				★									★																		
	資源の確保					★																										
運用	安全管理規程					★																										
	教育訓練実施						★													★												
	安全管理対策運用開始	1					★																									
	委託先選定期日				★			★	契約																							
	運用の点検						★				★					★						★					★					
	監査実施							★	通知			★																				
申請	是正処置の実施													★																		
	代表者の見直し														★																	
	申請書作成、申請																★															
	現地審査																															
	PMARK取得																															
外部コンサルタント		★				★		★			★				★					★					★		★			★		

次年度のPMS年間計画は、個人情報保護管理者が策定し、代表者の見直し時に承認を受けます。

PMS年間計画は、事業年度と必ずしも合わせる必要はありません。事業の多忙な時期を避けるために、暦年（1月～12月）とすることも可能です。サンプルの「**3303PMS年間計画書**」では、予定日を上段に、実施日を下段に手書きで記入し、PMS運用の点検表を兼ねています。

201★年	1月	2月	3月	4月	5月	6月	7月	8月	9月
① 代表者の見直し(計画表の策定・承認) (状況に変化があった際には随時見直し)									
② 法令・指針・規範の改定確認 (改定を確認した際には随時見直し)					1				
③ 個人情報管理台帳の見直し (取扱に変更があった際には随時見直し)			1						
④ リスク分析表の見直し (取扱に変更があった際には随時見直し)				1					
⑤ 従業員定期教育の実施 (採用者には採用初日に教育)		15							
⑥ 監査の実施 (状況に変化があった際には臨時監査を実施)									
⑦ 全社「343401委託先管理台帳」 (「委託先調査票」が稼働化していないか点検を含む)						1			

次回は、「第4章 個人情報 の特定」

「第5章 法令、国が定める指針その他の規範」をご紹介します予定です。

個人情報保護監査研究会 <http://www.saa-j.or.jp/shibu/kojin.html> 以上

2013.05 投稿

【ワークショップサポートサービスのお知らせ（新サービス）】

会員番号 1143 中山 孝明(システム監査活性化プロジェクト)

SAAJ の新サービス、ワークショップサポートサービスのご提供とご利用申込受付が間もなく始まります。

以下は検討中の PR リーフレット(2 面)です。どうぞご覧ください。

1/2 面

- ・会員皆様へご提供する新サービスです。
- ・非会員の皆様もどうぞご相談ください。
- ・IT 利活用に関係する広範な各種業務、各種部門が対象です。
- ・皆様の日常的な様々な改善活動をサポートします。
- ・検討会、勉強会、ミーティングなど職場内の各種取組みをワークショップと称しています(形態は任意です)。
- ・これらワークショップ活動をサポートするのが、本サービスです。
- ・サービスを利用するための皆様のご準備は不要です。
- ・無料サービスです。
- ・SAAJ が持つ知識、技術、知恵、コツなどのノウハウを気軽にご利用ください。
- ・SAAJ の経験豊かなシステム監査人が対応します。

1/2 面



特定非営利活動法人 日本システム監査人協会

Systems Auditors Association of Japan

会員皆様へ ★SAAJから耳寄りなお知らせ★

非会員の皆様もお気軽にご相談ください。

皆様の職場の課題解決にお役立てください

ワークショップ サポートサービス



社内監査部門や
経営部門の方へ



情報システム
部門の方へ



利用部門
の方へ

- ・システム監査ノウハウの習得に腐心していませんか？
- ・ITや情報セキュリティの点検活動は十分でしょうか？

- ・業務改善や作業の品質向上などで懸案事項はありませんか？

- ・IT利活用の各種業務に様々な問題や悩みはありませんか？

・日常的な改善活動や対策検討をスピードアップするお手伝いです。

・皆様の主体的活動を尊重した、参考意見・アドバイスです。

・SAAJの経験豊かなシステム監査人がノウハウを提供します。



皆様のお役に

- ・システム監査やIT業務に限らずIT利活用業務に携わる皆様の活動を支援します。
- ・SAAJは、システム監査の普及を通じて健全な情報化社会の発展に寄与することを目的とし、会員サポートを充実させております。



身近な課題に

- ・システムや情報セキュリティへの要請は益々高まっています。
- ・一般的なセミナー受講では得られない、皆様固有のテーマにダイレクトに応えます。
- ・サービス利用のための事前準備は不要です。負担をお掛けしません。



使えるメニュー

- ・サービスメニューとサポートの例は、裏面をご覧ください。
- ・新サービスです。ご利用をお待ちしています。メニューのご要望もどうぞ。

利用無料

A面 2013.5

2/2 面

・利用しやすいメニュー
例も用意しています。
(右リーフレットご参照)

・例えば右リーフレットの
訪問型の場合、2H
前後のミーティング参
加をイメージしていま
す。

・身近な改善活動のお
手伝いです。小さな案
件を遠慮なくどうぞ。

・皆様が解決策を導く
ための、方向性/ポイ
ント/留意点などの参
考意見を提示します。

・どうぞお気軽にお声か
けください。

右リーフレットの E-mail
アドレスにお願いしま
す。

・リーフレットの不明点
やご要望も E-mail アド
レスにお寄せくださ
い。

・本サービスのリリース
は間もなくです。その
際は改めてご案内い
たします。

ワークショップ サポートサービス メニューとサポート例

本サービスは、皆様の日常的な小規模改善活動のお手伝いです。
ワークショップは職場内の各種検討・見直し・整備作業などの取り組みの総称です。

訪問型

(課題例: システムや情報セキュリティの監査、外部認証や内部統制)

・システム監査に取り組みたいが経験者がおらず計画が進まない。課題も
良く分からない。情報セキュリティ点検の視点に不足がないか心配。社内
にレビュー者もいない。現場の活動を活性化したいがうまく指導できない。

(サポート例) ●SAAJのアドバイザーが皆様のところへ出向き、検討会や勉強
会などのワークショップに参加します。その場でご説明を受け、
課題解決に役立つ手法や実践的なノウハウをお伝えします。
(QMS、PMS、EMS、ISMS、SMS(ITSMS)、BCMSなどにも対応)

研修型

(課題例: 研修の充実、人材育成)

・IT関係の組織内研修を充実させたい。関連知識を深めたい。

(サポート例) ●研修講師を派遣し、ご要望テーマで講演・講義などを行います。

Q&A型

(課題例: 単発的な疑問)

・IT関係で個別的な事案や単発的に発生する疑問などを解決したい。

(サポート例) ●Eメールなどで随時質問をいただき、アドバイスや参考意見を
返信します。

メニュー全般

●上記の課題例は一例です。課題例以外のIT利活用全般にかかわる諸問題を実情に
即して、システム監査の視点からアドバイスします。

例: 情報戦略、企画/開発/運用、品質管理、リスク管理、外部委託管理、Pマーク、情報管理、
BCP、障害管理、書式/様式、基準/規格、IT研修など、可能な限りご要望に対応します。

●ご相談内容や皆様の情報は守秘いたします。

特定非営利活動法人 日本システム監査人協会

事務局 〒103-0025 東京都中央区日本橋茅場町2-8-8 共同ビル(市場通り)6階

<http://www.saa-j.or.jp/> Tel: 03-3666-6341 Fax: 03-3666-6342

本サービスのお問い合わせ・お申し込み E-mail: wss@saa-j.jp

・SAAJは、システム監査技術者試験合格者が母体となって発足した団体です。
システム監査人や志している方、ノウハウ習得など、多くの方々が活動しています。(入会随時受付中)

B面 2013.5

・E-mail アドレスは既に利用可能です。皆様からのご意見をお待ちしています。

以上

2013.05 投稿

【システム監査事例研究会だより】

会員番号 0750 畠中道雄(システム監査事例研究会)

【投稿にあたって】

システム監査事例研究会(略称「事例研」)の活動の中心は、監査サービスという形で、企業・組織からシステム監査の依頼を受け、事例研のメンバーが監査を実施することにあります。これまでに30近い企業・組織の監査を行い、監査人の力量向上、監査マニュアルの出版、監査セミナー教材の作成とセミナーの開催、といった成果を残してきました。

近年、新たな監査サービスの依頼はありませんが、新しいセミナーの企画や既存セミナーの見直しを行ないながら、定例会活動の活性化を図るべく活動を続けています。

そこで、今月から、会報のページをお借りして、事例研の活動についてご報告することにいたしました。特に、システム監査白熱教室は興味ある内容に溢れています。是非ご一読ください。

【5月度事例研報告】

開催日時:2013年5月8日(水) 18:30~20:30

開催場所:八丁堀区民館、出席者6名

<事例研への参加を随時受け付けています>

・問い合わせ先: PEC01546@nifty.com (畠中)

・原則として、毎月第1水曜日の18:30から開催しています。

1. 活動報告**1.1 第24回実践セミナー終了(大西)**

5月3・4日受講者10名、講師:鈴木実・大西氏

1日目の夜が使えないため、時間配分に苦慮した。

1.2 課題解決セミナー(中山、畠中)

① 6月1日(土)に第10回開催を決定、募集開始。教材は「データセンターにおけるデータ誤消去」(久野氏)、「証券会社における大量誤発注」(濱崎氏)

② 今後の教材開発(4月27日に教材検討会を開催した)

- ・新教材の作成・充実に継続して取り組む必要性を出席者で確認した。
- ・望まれる新教材の例として、不正アクセス、医療情報、Web アプリ、ネット選挙、プロジェクト監査、自治体等や過去の監査サービス事例など。
- ・小佐野氏には今年12月開催に向けて、大西氏には来年3月開催に向けて、新たな教材作成に取り組んでいただく。

③ 今後の開催

- ・今後の開催計画は、9/7(土)、12/7(土)を候補日として、年4回の定例開催実現に取り組む。

なお、事務局の作業負担&正副担当制に関する問題提起を受け、事務局要員の増員と、手順やノウハウの明示/継承を、9月のセミナー開催計画に向けて具体化することを確認した。

1.3 監査サービス(F社)

F社としては今年度上期の再構築受注を狙っていたが、委託企業側で予算獲得ができなかったとのこと。監査サービスも延期となる。

1.4 監査サービス(S協会)

協会では、各社が利用する共同システム、および協会内のシステム運営全般を統括して管理する体制として、新たな部門を設置することになった。(4/1付で会員会社から担当部長として1名出向願い、9月を目途に組織化する予定。)

システム監査については、費用面もさることながら、この新設部門の立上げ・稼動との関係を考慮しながら、監査の実施を検討していくことになった。

1.5 活性化プロジェクト(中山、畠中)

4月26日に法人部会においてWSSの説明・検討をした。

2. システム監査白熱教室

5月テーマ「システム監査人の役割、期待される技術水準、対象者像」(発表者:中山)

〈発表概要〉

- ・配布資料はIPA「システム監査技術者試験制度」から抜粋したもの(キーワード中心)。
- ・発表趣旨は、我々システム監査人は、①自分自身に求められている役割などを正確に認識していない部分がある。②役割を漠然と意識していても明確な根拠があることをうっかりしている。③自己研鑽、切磋琢磨が必要な不足部分を明瞭にしなければならない。④間違えても「それは役割ではない」などと言ってはいけない。など。

〈意見交換〉

- ・配布資料を読むと、改めて我々が担う仕事が生易しいものではないことに正直驚く。
- ・4つの時代(①昭和61年～平成5年、②平成6～12年、③平成13～20年、④平成21年～)の経営の要請、中心となる情報技術、情報技術水準、などの影響が色濃く表われていると思われる。
- ・時代とともに、システム監査人に求められる役割が多岐にわたり、かつ難解になってきた。特に一時代前の資格試験合格者など、新たな要請に応えるために努力を要する範囲も広い。
- ・例えば、「経営の内部統制」「経営管理の視点」などは19年前からの期待水準になっており、4年前には「組込みシステムのリスク・コントロールの点検・評価」などが求められている。
- ・10年前から求められている「分析/評価の判断基準を監査人自らが形成」とは、具体的にどのような手法を指しているのか。
- ・当協会は、これらの技術水準にまで監査人を引き上げるための活動を活発にする必要がある。
- ・一つの評価が終わらないうちに、次々と新しい情報技術が現れるという時代があった。会社としては方向性を見い出せない中で、私的な探究心や費用負担で、使ってみたり触ってみたりしていた技術者が居た。
- ・組み込みシステム(「家電・自動車などの内部で電子制御を司る」と理解)にまで関与できる力量を、監査人が持たなければいけない。現実問題として出席者全員とも具体的な監査手法を持ち合わせていない。

3. 次回

6月5日(水) 18:30～ 八丁堀区民館

白熱教室テーマ①「ヒューマンエラー対策(ANAにおける事例)の伝達教育」

②「組込みシステムとシステム監査」

以上

2013.05 投稿

【CSA利用推進グループの活動紹介】

会員番号 0281 力利則 (CSA利用推進グループ)

～CSA・ASA全体交流会（6／15）参加者募集中！！**1. グループの活動とCSAフォーラム**

本グループの活動は、公認システム監査人(CSA)、公認システム監査人補(ASA)になられた方々が、この資格を取得して良かったなと思ってもらえる活動を進めています。

その代表的な活動が2ヶ月に1度程度開催しているCSAフォーラムです。CSAフォーラムは今年で5年目を迎え最近では4月23日に第17回目を開催しました。毎回、20名前後の方々のご出席を頂いて、設定したテーマに関する講師のご講演・ご説明に続いて、出席者の方々と質疑応答、意見交換に時間を掛けたフェイスtoフェイスと相互啓発の取り組みを行っています。また時間が許す方々とは毎回、懇親会を開いてフェイスtoフェイスの活動をさらに楽しく深めています。

CSA&ASAの皆様にはこのCSAフォーラムのご案内は届いていますか？実は当初より20～30名前後で開催したいという趣旨から、事前登録を行って頂いた方に絞ってご案内を差し上げています。年に1度程度しか届いていない方は、事前登録者の拡大を狙ってCSA・ASA全員にメールリストを使って配信しているからです。もしCSA・ASAの方で、CSAフォーラムのご案内を毎回欲しいという方は、SAAJ事務局までその旨をご一報くだされば事前登録を行います。ぜひご連絡ください。

2. 第1回CSA・ASA全体交流会の開催

今年は、CSAフォーラムの活動に加えて、第1回CSA・ASA全体交流会を開催することにしました。今、ちょうど、SAAJのHPから申し込みができます。CSA・ASA継続教育の後に行います。受講ポイントが付与される継続教育を受講した後に全体交流会でお互いの人を知ろうというのが趣旨です。ただ当日、継続教育には時間的に出席できない方や受講ポイントは他で確保できているという方は、全体交流会だけに出席することもできます。ぜひ大勢のCSA・ASAの方々と知り合って交流を深めることによって、自分の仕事へのフィードバックやビジネスのチャンスにつなげていただければと考えています。

第1回 CSA・ASA全体交流会のご案内

- ① 日時 2013年6月15日(土)PM5～7 (継続教育 同日 PM1:30～4:45)
- ② 場所 東京都港区 機械振興会館本館 (継続教育と同じ会館)
- ③ 会費 2500円
- ④ 申込み方法 SAAJのHPより (継続教育の案内ページ)
- ⑤ 幹事 CSA利用推進グループ

CSA利用推進グループのキャッチフレーズ

****CSA・ASAを取得してさらに良かったと思ってもらえる資格にしましょう！！**

2013.05 投稿

協会からのお知らせ 【ご寄附等の報告】

会員番号 0557 仲 厚吉(事務局長)

■2012 年度ご寄附の集計報告

2012年度から会費請求書に同封して会員の皆さまにご寄附をお願いしております。お蔭さまで、会員の皆さまからご寄附が集まり、2012年度の協会財政状況に大きく貢献していただきました。誠にありがたく御礼を申し上げます。寄附金は、寄附金収入として計上しております。それぞれの皆さまに御礼状をさしあげるべきですが、この報告にて、御礼状に代えさせていただきます。失礼をお許してください。なお、特定非営利活動促進法に基づいて、「寄附者名簿」を所轄庁の東京都に提出することがございます。何とぞご了承を賜りたくお願い申し上げます。

〔2012年度集計〕

人数	金額
124人	410,100円
(役員等以外でかつ3,000円以上の方:118人)	

2013年度のご寄附については、速報として3月末現在、次の状況になっております。重ねて御礼を申し上げます。

〔2013年度速報〕

人数	金額
103人	576,536円

■2012 年度の印税収入報告

2012年度において、「情報システム監査実践マニュアル第2版(赤本)」の印税収入が、70,434円ありました。そのうち、執筆者分(80%)の印税収入53,644円について、理事活動等に関する規程に基づき執筆者の方の同意を得て、協会の印税収入に繰入れさせていただいております。あらためて御礼を申し上げます。

人数	金額
18人	53,644円

理事活動等に関する規程

(謝礼金)

第4条 謝礼金については、下記のとおり定める。

4. 協会出版物の原稿料、印税等の扱い

協会が監修等を行った出版物の原稿料、印税等があった場合は、原則として20%を協会に納付し、80%を執筆者に分配する。なお納付率については、出版担当者と会計担当者が協議して変更できるものとする。

以上

注目情報 (2013. 3～2013. 5)**■【IPA、「標的型攻撃の防御に向けた産業界との情報共有の枠組み、J-CSIPの活動レポート」公開】**

2013 年 4 月 17 日 独立行政法人情報処理推進機構 技術本部 セキュリティセンター

IPAでは、2012 年 4 月から活動を開始した標的型攻撃の防御に向けた産業界との情報共有の枠組み「サイバー情報共有イニシアティブ」(以降、J-CSIP(ジェイ シップ))において、これまで 5 業界、39 組織で運用体制を確立している。2012 年度の活動では、参加組織から 246 件の情報提供を受け、IPAによる分析を経て、参加組織へ 160 件の情報提供を行った。これら J-CSIP の活動状況を「サイバー情報共有イニシアティブ 2012 年度 活動レポート」としてまとめ、公開した。参加組織において以下の様な成果があった。

- (1) 業界を狙った同一もしくは類似の攻撃が行われていることを組織間で相互に共有し、対策に寄与した。
- (2) NDA下での情報管理を前提とし、また、情報の匿名化などの情報共有ルールを適用することで、情報の共有可否に対する迅速な判断と、詳細な内容の情報共有を可能とした。
- (3) 複数組織に行われた攻撃間の相関についての分析結果を共有することにより、今後想定される攻撃に対する各組織での対策立案に繋がった。

ホームページ <http://www.ipa.go.jp/about/press/20130417.html>プレスリリース本文 <http://www.ipa.go.jp/about/press/pdf/130417press.pdf>**■【警察庁、13 都道府県警察に「サイバー攻撃特別捜査隊」を設置】**

2013 年 3 月 28 日 警察庁

平成25年4月1日付けで、13 都道府県警察(北海道、宮城、警視庁、茨城、埼玉、神奈川、愛知、京都、大阪、兵庫、広島、香川、福岡)に「サイバー攻撃特別捜査隊」を設置し、全国で約 140 人の専任捜査員が対策を推進する体制を構築する。当捜査隊の任務は、サイバー攻撃から個人の生命、身体及び財産を保護し、公共の安全と秩序を維持するため、次に掲げる業務を遂行することを任務とする。

- (1) サイバー攻撃に対する警備情報の収集、整理その他サイバー攻撃に関する警備情報に関すること。
- (2) サイバー情報に関する警備犯罪の予防に関すること。
- (3) サイバー情報に関する警備犯罪の捜査に関すること。

警察庁プレスリリース本文 <http://www.npa.go.jp/keibi/biki3/20130328kouhou.pdf>**■【IPA、5月の呼びかけ「スマホにおける新たなワンクリック請求の手口に気をつけよう！」】**

2013 年 5 月 1 日 独立行政法人情報処理推進機構 技術本部 セキュリティセンター

IPAセキュリティセンターでは、毎月、情報セキュリティに関する注意を促す「今月の呼びかけ」を行っているが、5 月は、「スマホにおける新たなワンクリック請求の手口に気をつけよう！」と題して、「請求画面が消えない」といったスマホにおける新たなワンクリック請求の手口と対処方法を紹介している。スマホが生活必需品として浸透するに従い、悪質な手口が次々と現われるおそれがあり、警戒が必要である。

5 月の呼びかけ本文 <http://www.ipa.go.jp/security/txt/2013/documents/summary1305.pdf>

2013.05 投稿

【協会主催イベント・セミナーのご案内（東京開催その1）】

会員番号 0557 仲 厚吉(事務局長)

■CSA・ASA継続教育セミナー

公認システム監査人認定委員会・CSA利用促進Gの、CSA・ASA継続教育セミナー「フィッシング攻撃の実態ならびに警察による摘発事例を語る講演会」をご案内します。また、セミナー終了後、「CSA・ASA交流会」を開催しますので、ぜひ、ご参加をお願いします。協会ホームページからお申込みができます。

<http://www.saa-j.or.jp/kenkyu/keizoku20130615.html>

「フィッシング攻撃の実態ならびに警察による摘発事例を語る講演会」

1. 日時：2013(平成25)年6月15日(土) 午後1時30分から午後4時45分
2. 場所：東京都港区 機械振興会館本館 地下3階 第1研修室（電話 03-3434-8211 港区芝公園 3-5-8）
3. テーマ・講師：
①「フィッシングに関する最新動向について」 フィッシング対策協議会事務局 山本健太郎氏
②「フィッシング摘発、警察の取り組みについて」 警察庁生活安全局 情報技術犯罪対策課 警視 吉田光広氏
4. 参加費：協会会員 ¥3,000 非会員 ¥4,000
5. 継続教育認定時間：6時間(実時間×1.5(種別a))

6. 第1回CSA・ASA交流会

〔懇親会〕：機械振興会館本館 午後5時から午後7時 会費 ¥2,500 ※交流会だけの参加も受け付けます。
申込み方法 SAAJのHPより（継続教育の案内ページ）
幹事 CSA利用推進グループ

■中堅企業向け「6ヶ月で構築するPMS」セミナー

個人情報保護監査研究会の中堅企業向け「6ヶ月で構築するPMS」セミナーの開催をご案内します。当研究会では、当研究会著作の規程、様式を用いて、6ヶ月でPMSを構築するためのセミナーを開催します。

詳細は、個人情報保護監査研究会主査 斎藤(saa-jk7@saa-j.jp)までお問い合わせください。

中堅企業向け「6ヶ月で構築するPMS」セミナー

- ・基本コース：月1回(第3水曜日)14時～17時(3時間)×6ヶ月
- ・料金：9万円/1名～(1社3名以上割引あり)
- ・会場：日本システム監査人協会 茅場町オフィス
- ・テキスト：SAAJ「個人情報保護マネジメントシステム実施ハンドブック」(非売品)
2013年5月号 SAAJ 会報より、[「個人情報保護マネジメントシステム実施ハンドブック」簡易版](#)を公開開始！
- ・セミナーのお申込が多い場合、最大6ヶ月お待ちいただくことがあります。
- ・基本コースの他に、月2回の応用コースなどがあります。

以上

2013.05 投稿

【協会主催イベント・セミナーのご案内（東京開催その2）】

会員番号 0735 三輪 智哉(システム監査事例研究会)

**第10回「事例に学ぶ課題解決セミナー」受講者募集のご案内
実際の事故事例をもとに未然防止策のポイントを学びます！**

情報システムの事故・障害で、企業や顧客が損失を被る事例が後を絶ちません。システム監査の専門家が事故・障害の原因を解き明かし、システム監査の観点から見た有効な解決策を示します。

事故・障害の原因は報道だけでは分かりません。事故・障害事例をリスクとコントロールの視点で分析して、皆様の課題解決に役立つ説明をします。

情報システムの利用者から運営者、経営者から担当者まで多様な階層・職種の方のキャリアアップに、当セミナーをご活用下さい。

事故・障害を未然に防ぐシステム監査の役割とその有効性の理解向上にも役立ちます。

自社システムの信頼性・安全性をさらに高めたいと考えておられる経営者、役員の方、IT 部門長の方など、多くの皆様の参加をお待ちしています。

受講修了後、受講証明書をお渡ししています。

なお、当該企業がどのように問題を解決したかについての解説セミナーではありませんので、ご注意ください。

記

1. 日程及び会場

開催日:2013 年 6 月 1 日(土)

時間 :13:00~17:00(進行状況により若干の変更が生じる場合があります。)

会場 :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 (最寄り駅 都営地下鉄大江戸線勝どき駅下車徒歩8分)

2. 費用 : 4,000 円(日本システム監査人協会会員)、6,000 円(一般)(費用には、教材費・消費税が含まれます。)

3. 内容 : 事例を用いて次の順で講義(受講者も一部参加)します。

STEP1:事故・障害事例を把握する

STEP2:問題事象を考える

STEP3:リスク(脅威・脆弱性)を考える

STEP4:リスク対策(コントロール)を考える

STEP5:システム監査による評価

事例講義:「データセンタにおけるデータ誤消去」(新規ケース)

簡易演習:「証券会社における大量誤発注」

なお、教材は、当日配布します。

4. 受講していただきたい方

どなたでもお申し込みいただけます。特に、経営者、役員、IT 部門長の皆様の参加を歓迎いたします。

5. 募集人員 : 定員20名(最小催行人員12名)

6. 受講申し込み方法 : 右記 URL からお申し込み下さい。 http://www.saa-j.or.jp/kenkyu/kadaiseminar_10.html

以上

2013.05 投稿

【協会主催イベント・セミナーのご案内（大阪開催）】

会員番号 0169 林裕正(近畿支部)

■システム監査セミナー**1. システム監査体験セミナー（入門編）**

- ・日時:2013 年 6 月 22 日(土)10:00～17:00 場所:常翔学園大阪センター
- ・内容: 内容は、システム監査入門講義(座学)、3～4 名のグループでシステム監査プロセスの一部を体験いただくグループワーキング(演習)、及びワンポイント監査実話です。システム監査に関連する事前知識は必要ありません。ITコーディネータ知識ポイントを1P付与致します。
- ・費用:日本システム監査人協会会員 4,000 円、 その他の方 5,000 円
- ・定員:16 名(最小催行人員 8 名)
- ・申込方法:協会ホームページから、お申込みください。 <http://www.saa.or.jp/index.html>

2. システム監査体験セミナー（実践編）

- ・日時:2013 年 9 月 21 日(土)・9 月 22 日(日) 場所:大阪産業創造館
- ・費用:日本システム監査人協会会員 16,800 円、 その他の方 21,000 円
- ・定員:16 名(最小催行人員 8 名)
- ・申込方法:申込み準備中

■第 37 回システム監査勉強会

- ・日時:2013 年 6 月 15 日(土)10:00～12:00 場所:大阪大学中之島センター
- ・内容: 2013 年 2 月 22 日の SAAJ 第 12 期通常総会特別講演の DVD の視聴。
テーマ「職業安定行政におけるシステムの刷新について」
講師 厚生労働省職業安定局労働市場センター業務室長 村上竹男様
- ・費用:日本システム監査人協会会員 無料、 ISACA大阪支部会員 無料、 両協会の会員以外の方 1,000 円
- ・申込方法:協会ホームページから、お申込みください。 <http://www.saa.or.jp/index.html>

■近畿支部創設 25 周年記念研究大会

- ・日時:2013 年 7 月 6 日(土)13:00～17:00 場所:大阪大学中之島センター
- ・統一テーマ:システム監査の新領域への対応
- ・内容: 近畿支部は、1988 年(昭和 63 年)3 月 4 日に「関西支部」として発足しました。今年は、創設 25 周年の節目の年となることから、これを記念して研究大会を開催致します。従来、システム監査が対象とした「情報システム」の位置付けがクラウドサービスの拡大や事業継続の観点から多様化しており、その結果、システム監査も多様化しています。こうした状況の中で、「システム監査の新領域への対応」を統一テーマとして、近畿支部の研究プロジェクト活動報告や会員の研究発表と、会員によるパネルディスカッションを行います。
- ・費用:日本システム監査人協会会員 1,000 円、 ISACA大阪支部会員 1,000 円、
両協会の会員以外の方 3,000 円
- ・申込方法:申込み準備中

以上

2013.05 投稿

【月例研究会開催予定】

会員番号 0148 木村裕一(月例研究会)

■2013 年 5 月・第 181 回月例研究会

- 1.日時:2013 年 5 月 21 日(火)18:30～20:30
- 2.場所:機械振興会館 地下 2 階多目的ホール
- 3.講演テーマ:「FISC 安全対策基準第8版追補、コンティンジェンシープラン手引書第3版追補3の内容」(仮)
- 4.講師:金融情報システムセンター 監査安全部長 西村敏信氏、鬼頭克巳氏、主任研究員 岡田氏

■2013 年 6 月・第 182 回月例研究会

- 1.日時:2013 年 6 月 17 日(月)18:30～20:30
- 2.場所:機械振興会館 地下 2 階多目的ホール
- 3.講演テーマ:「PIA(Privacy Impact Assessment)について」(仮題)
- 4.講師:首都大学東京 産業技術大学院大学教授 瀬戸洋一氏

■2013 年 7 月・第 183 回月例研究会

- 1.日時:2013 年 7 月 24 日(水曜)18:30～20:30
- 2.場所:機械振興会館 地下 2 階多目的ホール
- 3.講演テーマ:「サイバー攻撃の脅威」(仮題)
- 4.講師:独立行政法人 情報処理推進機構 渡辺貴仁氏

■2013 年 8 月・第 184 回月例研究会

- 1.日時:2013 年 8 月 21 日(水曜)18:30～20:30
- 2.場所:機械振興会館 地下 2 階多目的ホール
- 3.講演テーマ:クラウドインシデント
 - ・利用者側:攻撃発生事例
 - ・事業者側:標準化、国際動向 (仮題)
- 4.講師:独立行政法人 情報処理推進機構
技術本部 セキュリティセンター 普及グループ 研究員 河野省二氏

以上



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。

この「システム監査の普及促進」は、4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、3か月ごとのテーマとは別に1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。

5月号からの3ヶ月間の会報テーマは「システム監査活性化への提言」としました。おりしも、協会の重点施策である「会員増強プロジェクト」の名称も平成25年4月から「システム監査活性化プロジェクト」に変更したばかりです。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、投稿ボタ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】(当協会ホームページ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/>

■送付停止は、購読申請・解除フォームに申し込んでください。

【送付停止】 <http://www.skansanin.com/saaj/>

Copyright(C)2013、NPO 法人 日本システム監査人協会

掲載記事の転載は自由ですが、内容は改変せず、出典を明記していただくようお願いします。

■□■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、藤澤 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)