特定非営利活動法人
日本システム監査人協会報

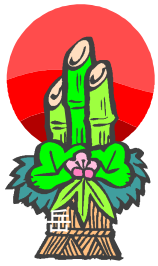
2014年1月号
No 154

No. 154（2014年1月号）＜12月20日発行＞

あけましておめでとうございます

会員各位とシステム監査人協会にとってよい年でありますように、

新年と同時に新会長が就任いたしました。まずは、ご挨拶から。



2014.1.1 投稿

就任挨拶 【 会長に就任して 】

会員番号 0557 仲 厚吉 （会長）

新年あけましておめでとうございます。本年1月1日をもって会長に就任することとなりました。事務局長職の実務経験を活かして、協会組織の充実、システム監査人の社会的評価の向上、システム監査の活性化に、イニシアティブを執らせて頂き、当協会の発展とシステム監査の普及促進に全力を尽くします。何とぞご協力を賜りますようお願い申し上げます。2年前に事務局長に就任した際に、当協会の信頼性を高めるため、認定NPO法人を目指すことを心に誓って、協会運営の質の向上に全力を尽くしてきました。また、会員の皆様から、2012年度、2013年度とつづいて、100人を超える寄付を頂いたことにより、認定NPO法人への申請準備は着々と進んでいます。この実績をもとに2014年度に東京都へ認定NPO法人への申請を行います。2014年度に当り、協会運営について、わたくしの考えを述べます。

〔2014年度の協会事業について〕

1. 信頼のブランドである「認定NPO法人」の認定取得を目指します。よって、協会事業には次の3点を挙げます。
   (1)協会組織の充実
   東京都の認定審査に合格するため協会組織を整備し、また、会員の信頼に応えるよう体制を充実させる。
   (2)システム監査人の社会的評価の向上
   「認定NPO法人」認定によって、公認システム監査人資格のブランド化を図る。
   (3)システム監査の活性化
   「認定NPO法人」認定によって、システム監査を公の活動として活性化させる。
2. システム監査の活性化の活動の一環として、次を行います。
   (1)IT－Audit等のISO化、JIS化の推進を進める。
   (2)システム監査に関連の他団体との交流を進める。
   (3)会員とのコミュニケーション向上のため、ホームページの改訂、会員ポータルサイトの導入を図る。

〔2014年度の予算編成について〕

1. 事業についての考えにもとづき次のように予算編成を考えます。
   (1)編成方針
   NPO法人の予算編成は、収益性とともに活動性をより重要とする。
   (2)事業活動
   事業活動は、収支バランスを原則とする。収支は、公認システム監査人等認定事業収支が隔年上下変動することを考え、2年タームで取り組む。事業活動によっては、重要性や緊急性を考え例外を認める。
   (3)協会体制
   協会体制の充実、会員とのコミュニケーション向上のため、ホームページの改訂、会員ポータルサイト導入に予算措置を講じる。

以上をもって、会長就任の挨拶と致します。

2013.12 投稿

退任挨拶　【　会長の任期を終えて　】

会員番号　0841　沼野伸生　（前会長）

新年、明けましておめでとうございます。

さて、私は平成24年1月に会長に就任し、2年の任期を終え平成25年12月をもって会長を退任致しました。

在任中は、会員の皆様にあたたかいご支援、ご協力を頂き、誠にありがとうございました。

厚くお礼申し上げます。

会長就任当初、私は当協会の運営方針として

（１）システム監査の普及、促進活動の一層の推進、

（２）会員サービスの一層の充実

（３）協会財政の一層の健全化

の３点を挙げ、一方、当協会の会勢の著しい減衰を踏まえ、今後のシステム監査の社会的役割の高まりに応えていくために、まずは会勢の挽回を最優先課題とし役員が一丸となって取組まなければならないとしました。

そして、会勢の挽回の基本は、会員が協会に入ってメリット感が得られるような、魅力ある協会活動を展開すること、すなわち各研究会、部会、委員会活動を一層強力に活性化し、その成果を積極的に会員へ広報、還元し、当協会の魅力を一層高め、新たな会員を呼び込み、それによって更に各研究会、部会、委員会活動を活発化していくというサイクルを回すこととし、会員増強プロジェクト（リーダ：小野副会長（当時）。後にシステム監査活性化プロジェクトに改称。）を立上げ、協会活動の活発化を徹底すると共に、長期会費未納会員の除名処理等による協会運営の効率化や大胆な経費節減による財政基盤の建直しに役員が総力を挙げて取組みました。

その結果、会員の減少傾向は取り敢えず止まり、新規会員も徐々に増加しています。また、財政基盤についても 1年目で本部現預金残高が10百万円近くになり、2年目も多少ですが更にそれに上乗せができる見込みです。

しかし、これらは協会活動に変化の兆しが見えてきたというレベルであり、予断を許さず、まだまだ、やること、やるべきことは山積みされているのが現実で、今後も息の長い努力が必要です。

私は、会長職（あるいは理事職）は適任とされる新たな人に次々に引継がれていくことで、協会の活力維持、協会活動の活性化、そしてシステム監査の社会への一層の普及促進という息の長い活動が維持できると思っています。

そこで、前任会長が後継会長を実質指名するこれまでの方式を改め、選任の透明性を一層高め、新体制での一致協力した協会運営によって会勢低迷の脱却をより確実にするため、昨年10月から理事会で選任プロセスの審議を重ね、理事の互選を経て仲新会長が誕生しました。

仲会長は、私が会長職にある時に副会長・事務局長として協会運営を支え、協会の現況を熟知した、新会長として適任の方です。会員の皆様の新会長へのご支援、ご協力をどうぞよろしくお願い致します。

私が在任した昨年までの2年間が、主として財政基盤立て直しを含む会勢挽回を中心とした守りの協会運営とするならば、今後は会勢の変化の兆しを生かし、守りと共に、攻め（システム監査普及へのより強力な攻めの施策展開）も新体制に期待できるのではと思っています。

在任中のご支援、ご協力に重ねてお礼申し上げますと共に、新会長へのご支援を心からお願い致します。

以上

2013.12 投稿

めだか　【指摘ゼロのシステム監査】

システム監査を実施する以上は、何か指摘事項や助言できなければ、という強迫観念に囚われる監査担当者は多いと思います。「折角コストをかけて監査を受けたのに指摘なしですか？」などとクライアントから言われた日には、次回から依頼は来ないだろうな（外部監査の場合）、担当役員や経営陣にどうやって報告しよう（内部監査の場合）、などと思い悩んでしまうのでしょう。

監査報告書に監査プロセスをきちんと記述して、被監査主体に説明責任を果たすことがシステム監査人の最も重要な責務です。

指摘事項や助言は必要があれば報告書に加えればよいのですが、それを記述することが最優先の課題だと考えるのは監査人の心構えとしては適切ではありません。むしろ相手の状況を正確に理解し、監査目的に沿って現状を正確に把握し、そのうえでどういった点が重要なのかを分かりやすく整理することが最も大切なことです。

報告書の中で、監査対象が抱えるリスクプロファイル、リスク認識の程度など、被監査主体が気付いていない、あるいは十分自覚的に取り組んでいないことを、監査人の見識でわかりやすく説明することは、極めて大切な技量です。報告書の趣旨をきちんと理解してもらい、被監査主体が自覚的にリスクのコントロールを行えるようになれば、監査目的の大半は達成できたといっても過言ではありません。

その意味では、良く出来ている点はきちんと評価し、さらに強化すべき点があれば、それを改善余地として、それを実施しない場合のリスクやその必要性をきちんと被監査主体に伝えることこそが優先事項です。

システム監査では必ずしも不備をみつけて指摘しなくてもよいのだ、現状を正確に理解し、被監査主体に自覚的にリスク管理に取り組んでもらうインセンティブ付けができるかどうか、がむしろ大切だと考えたいものです。報告書がそうした目的に沿って作成させていれば、監査報告を受ける被監査部門の長や経営者にとっても、システム監査をきっかけに、業務運営の適切性、資源配分の十分性についてレビューを受けたことになり、システム監査の有効性が評価されることになるでしょう。

長期的な視点でシステム監査の未来を切り開くためにも、こうした視点を大切にしながら、システム監査人諸氏とともに、地道な取り組みを続けて行きたいものだとつくづく感じています。

（拡張子）

（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。）

2013.12 投稿

めだか　【システム監査人にもっとも必要な資質は？　（システム監査の未来）】

結論を先に述べる。システム監査人にもっとも必要な資質は“情熱”であると思う。

「もっとも必要な資質」などというタイトルは尊大な感じもして気が引けるが、今月は正月号であるし会報テーマは「システム監査の未来」でもあるので、思うところを述べる。

システム監査人に必要なスキルは多々あり思いつくままでも、知識（情報システム、システム監査、関連法令や基準）、経験（情報システム、システム監査）、コミュニケーション力、計画力、ヒアリング力、文章表現力、リスク感覚、倫理感など簡単には挙げきれないほどだ（余談だがこれらのリストアップを試みるのも面白いかもしれない）。システム監査人の職務遂行に必要とされるスキルは、このように多彩かつ専門的で相応のレベルが要求されているが、それ以上に重要な資質は“情熱”ではないだろうか。

システム監査の実務で考えてみると、

・監査依頼者と初めて面談し監査目的、監査テーマなどを協議するとき、
・監査個別計画書を監査依頼者へ説明する場面で、
・現地実査や担当者へのヒアリングに接して、
・事実誤認有無確認や対応可否確認の協議の席で、
・監査結果の報告、監査報告書の提出において、

システム監査人が発揮すべき能力や発信すべき大切なことは、自らの知識や経験の披瀝などではなく、役立つシステム監査であることを表現する“情熱”（静かに伝わる熱意）であろう。また、相手方との会話・言動だけではなく、システム監査人自身の監査の品質、効率的な監査、分かり易い監査を成し遂げるための“情熱”（秘められた熱意）であろう。さらに、健全な情報化社会の発展を目指し、目先の成果や障壁に惑わされずにシステム監査の信じる道を着実に歩む“情熱”（エネルギッシュな熱意）であろう。

サミエル・ウルマン（Samuel Ullmann）の詩「青春」は人生や時節の転換点などでよく用いられるが、その一節をここで引用する。

青春とは人生のある期間を言うのではなく、心の様相を言うのだ。
優れた創造力、逞しき意志、炎ゆる情熱、怯懦を却ける勇猛心、
安易を振り捨てる冒険心，こう言う様相を青春と言うのだ。
年を重ねただけで人は老いない。理想を失う時に初めて老いがくる。
歳月は皮膚のしわを増すが、情熱を失う時に精神はしぼむ。

万能であるはずのない一人のシステム監査人の限られた能力を補い、それに留まらず新しい能力を掘り起こしてくれるもの、それが“情熱”であると、過ぎし一年と新たな一年にあれこれ思いを巡らしながら思う。

（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。）

2013.12 投稿

めだか【「情報革命時代の知恵」として学ぶシステム監査（システム監査の未来：その③)】

１０月から３ヶ月間、コラムめだかのテーマは「システム監査の未来」である。
そこで先月から、これまで私がコラムめだかで書いてきたことを振返りながら、「システム監査の未来」を私の希望、期待も込めて、**近未来像**、**中期展望**、そして**将来予想**の三段階で描いてみることにした。

第一回の１０月は、**近未来像**として、**“システム監査の監査としての Identity の確立”**を挙げた。
その趣旨は、「監査」本来への回帰、及び「織内の統制ツールから健全な情報化社会を支える社会の公器への転換」であった。

第二回の先月（１１月）は、**中期展望**として、**“監査の基盤としてのシステム監査の認知”**とした。
その趣旨は、情報社会ではどの監査においてもその監査対象を支える情報システにも目を向けなければならないとして、監査の基盤としてのシステム監査を当然のこととして認知している社会の実現を挙げた。

さて、最終回の今月は**将来予想**として、**“「情報革命時代の知恵」として学ぶシステム監査”**としたい。
以下は、私が過去の会報のコラムでこれについて書いた趣旨である。

『私たちは、農業革命、産業革命を人類史上の大変革として、学校の授業、教科書で学んだ。そして、それに匹敵する歴史上の出来事として、今、情報革命が進んでいる。

変革の時代は、変革を牽引するコア技術をその時代の人々の知恵で如何に使いこなすか、コントロールするかの試行錯誤、成功・失敗の繰返しの時代である。例えば、情報社会と言われる今日は、情報システムの“不完全性”（安全性、信頼性、効率性等の追及における避けがたい失敗リスクの存在）を受入れつつも、知恵を絞ってそれを如何に利活用するかが問われている時代と言える。

情報システムの“不完全性”は、情報革命の恩恵を享受する上で、共に受け入れなければならない現実である。そして、情報システムの“不完全性”を正面から受け入れ、かつ、利用者が積極的に情報システムを利活用していく前提は、情報システムの開発・提供者と利用者の相互信頼関係の確立にあり、この相互信頼関係の確立には、情報システムの開発・提供者の説明責任遂行が不可欠で、そして、これに呼応してこの説明責任遂行と不可分の、説明責任遂行に信頼性を付与し実効あらしめる情報システム監査が求められることになる。

将来の子供たちが、情報革命の全体、そしてその時代の人々の行動を授業や教科書で体系に学ぶ時、当時の人々の知恵、行動の一つとして、情報システム監査の導入、活用が語られる。（語られていて欲しい。)』

将来がこうあるかどうかは、まずは今後のシステム監査に関わる我々の活動、心掛け次第とも言えるが、皆さんのご意見は如何であろうか。

（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。）

2013.12 投稿

めだか　【　ストロマトライト　】

システム監査の未来を考える時、わたくしたちシステム監査人が生きている現在を考えてみます。第22回東京ミネラルショー〔国内外から340店舗が出店する鉱物・化石・隕石・宝石の“日本最大級の大展示即売会”〕で、特別展示　SPECIAL EXHIBITION（地球に酸素をもたらした生物の化石ストロマトライト）を見学しました。東京ミネラルショーのホームページによれば、ストロマトライトとは次のような生きものの化石です。

ストロマトライトは微生物の一種の藍藻類(シアノバクテリア)と泥や砂などが何層にも積み重なって出来た生物起源の岩石で、外見はマッシュルームの様なドーム型をしていますが、切断してみると層状の構造をしています。ストロマトライトを作る藍藻類(シアノバクテリア)は、地球上で最も古い生物のひとつとして、光合成により地球上に大量の酸素をもたらし生命が棲む環境をもたらしました。現在も生存しています。ストロマトライトは一番古い物で約27億年前の化石が発見されており、太古の地球で誕生し、現代でもオーストラリアのシャーク湾(ハメリンプール：世界自然遺産)他、世界中のごく限られた地域で太古の姿そのままで生存しています。日中は光合成により酸素を発生し、夜になると光合成をやめ、粘液を出してまわりの泥や砂などで体を固定します。そして再び日中になると固定した体の上(外側)で光合成を行います。長い年月それを繰り返しているうちに層状に成長し、広大な範囲に渡って群落を作っていきます。

ストロマトライトを作る藍藻類(シアノバクテリア)は、わたくしたちが住む現在の地球環境のもとを作ったと考えられます。また、歴史上、近代日本では明治維新（英: Meiji Restoration）がありました。江戸幕府に対する倒幕運動から、明治政府による天皇親政体制の転換とそれに伴う一連の改革をいいます。明治維新の中に現在の中央集権のもととなった版籍奉還（はんせきほうかん）があります。ウィキペディアによれば、つぎのようなことです。

版籍奉還は、1869 年 7 月 25 日（明治 2 年 6 月 17 日）に、日本の明治政府により行われた中央集権化事業の 1 つ。諸大名から天皇への領地（版図）と領民（戸籍）の返還。発案は姫路藩主酒井忠邦。版籍奉還は、主君（藩主）と家臣（藩士）の主従関係を否定することになるものであり、諸藩の抵抗も予想された。そこで版籍奉還の実施に際してはその意義については曖昧な表現を用いてぼかし、公議所などの諸藩代表からなる公議人に同意を求めた。更に前後して戊辰戦争の恩賞である賞典禄について定めることで倒幕に賛同した藩主や藩士を宥めて不満を逸らした。このため藩の中には「将軍の代替わりに伴う知行安堵を朝廷が代わりに行ったもの」と誤解する者もあり、大きな抵抗も無く終わった。そして版籍奉還によって各藩の中で続いていた地方知行がなくなり、蔵米知行に一元化された。また、版籍奉還と同時に旧藩主の諸侯 285 家は公卿 142 家と同時に華族に列せられ華族制度が創設され、旧藩主の諸侯は武家華族と呼ばれる。

システム監査の未来を考える時、わたくしたちシステム監査人は、現在は過去から未来へと変化しながら続いていくことに注意深くあるべきと思います。

（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。）

2013.12 投稿

システム監査の深化のために　【戦略は細部に宿る】～似て非なるものを峻別できるか?～

会員番号　1566　田淵隆明　（近畿支部法制化研究会）

これまで我が国の教育や研究の場では、「ミクロからマクロ」か「マクロからミクロ」かの優劣議論が蔓延り、時としては感情的になる場合もある。その結果、冷静に議論することができず、「似て非なるもの」の峻別が等閑になることが多い。古来より、「戦略は細部に宿る」と言われており、条約や契約における「似て非なるもの」は重大な相違をもたらすことは枚挙に暇がない。小さな相違の見落としや齟齬が悲惨な結果を惹起することも少なくない。日頃契約書法務に携わることの多い筆者としては、非常に神経を使うところである。

そもそも、「似て非なるもの」を正確に峻別するためには、議論する双方での言葉が正確に通じることが必要不可欠である。すなわち、相手の用いている用語の定義を、相互に正確に理解できていることが必要不可欠である。

【1】物理学の例

まず、筆者自身の苦い経験から述べよう。量子物理学の世界では、Transfer matrix(転送行列)が重要な位置を占めている。中でも4次正方行列で8-vertex Modelの研究は非常に重要である。しかし、この8-vertex Modelは流派により、次のように2つの異なる定義が存在する(0以外のすべてのパラメータは実数または複素数)。

$$R = \begin{bmatrix} a_1 & 0 & 0 & d_1 \\ 0 & b_1 & c_1 & 0 \\ 0 & c_2 & b_2 & 0 \\ d_2 & 0 & 0 & a_2 \end{bmatrix} \qquad S = \begin{bmatrix} a & 0 & 0 & d \\ 0 & b & c & 0 \\ 0 & c & b & 0 \\ d & 0 & 0 & a \end{bmatrix}$$

図1. Transfer matrixの2つの異なる定義

筆者の研究者グループでは8-vertex ModelはRの意味で用いていたが、他の研究者グループはSの意味で用いていた。Rは対称性を仮定しない場合であり、外部磁場のあるスピン・モデルに対応している。一方、Sは対称性の高い場合であり、外部磁場の無いスピン・モデルに対応しており、”組紐関係式”(Yang-Baxter Relations)を利用した研究の基礎となっている。筆者の研究者グループではRの定義に基づき、対称性を仮定しない広範な解を探求し一定の結果が得られ著名な学術誌にも掲載されたが、当該他の研究者グループにとっては”解決済みの問題”として全く取り合って頂けなかった。誠に遺憾なことである。

【2】国際問題の例(1)

本年の前半、シリアでは「シリアの反政府勢力・トルコ・スンニー派諸国・一部の欧米諸国 vs. シリア政府軍・クルド人勢力・シーア派諸国・ロシア」の間で深刻な紛争が発生し多くの人々が犠牲になった。誠に痛ましいことである。このように中東では長年紛争が続いているが、1967 年の第 3 次中東戦争停戦後の戦後処理の原則を定めた「国連決議 242 号」(1967 年 11 月 22 日)の解釈の齟齬から発生している重大な問題が存在している。我が国のマスコミでは「イスラエルが撤退するべき占領地の範囲があいまい」であるとのみ報道されることが多いが、詳しくは次の通りである。問題箇所は、英語及びフランス語の正文では次のようになっている。

E. withdrawal from *territories* occupied by...

F. le retrait *des territoires* occupés par...

※des＝de + les である。de は「～の」を表す前置詞(英 of, 独 von)であり、les は定冠詞の複数形。

英語正文では領域を表す territory の複数形 territories に冠詞が付いていないため、一部分を表している。一方、フランス語正文では territoire(男性名詞)複数形 territoires に定冠詞が付いているため、全部を表している。現在でも、イスラエル政府は英文をもとに 1978 年のカーター米国大統領の仲介によるエジプトとの「キャンプ・デービット合意」に基づきシナイ半島の返還をもって同決議を履行したとしている。

何故このような齟齬が発生したのか、未だに謎であるが、このことを原因として中東問題は現在でも混迷を極めている。これは、僅か定冠詞 1 個のために起こった悲劇でもあります。政治家及び外交当局には細心の注意を払ってもらいたいと思う次第である。まさに「似て非なるもの」の悲劇に他ならない。

【3】国際問題の例(2)

もう 1 つ国際問題を取り上げよう。国論を二分する騒ぎになっている TPP であるが、その重要な論点の 1 つが ISD(ISDS)条項(Investor State Dispute Settlement:投資家-国家紛争解決条項)である。経産省や TPP 推進派は「日本型 ISD」を念頭に「安全論」を説き、悪用の懸念を杞憂と一蹴している。一方、TPP 反対派は NAFTA での ISD 条項の運用実態を元に「悪用・濫用の危険」を説いている。実は「日本型 ISD」と「NAFTA 型 ISD」は「似て非なるもの」であるが、マスコミを含め、我が国ではこのことは殆ど知られていない。

例えば、提訴先の国際機関は、(米国の強い影響下にある)世銀傘下の ICSID(投資紛争解決国際センター)に限られておらず、UNCITRAL(国際連合国際商取引法委員会)、WTO(世界貿易機関)等の国際機関も使うことができる(その結果、米国政府/州政府が敗訴する可能性は十分にある)。一方、NAFTA 型では ICSID に限られている。

また、裁判管轄権についても、日本型では協議事項であり、紛争解決の国際機関への付託に際しては、当事国の文書での個別同意が必要あるが、NAFTA 型には「事前包括同意条項」があり、「国内裁判権」(司法主権)を予め包括的に放棄している。

「似て非なるもの」である両者の違いを纏めると次のようになる。これまで我が国が---迂回提訴も含めて---ISD 条項で国際提訴されたことが無いことも、NAFTA で ISD 条項が濫用・悪用され、時として「治外法権」として機能してきたたことも、読者の方々ならば、容易にお分り頂けることと思われる。これは重大な相違である。

「日本型ISD」と「NAFTA型ISD」の相違点

		日本型	NAFTA型
分類		国内手続き経由型	国内手続き省略型
国内手続き		国際機関の仲裁に委ねる場合に国内手続きによる同意が必要	国内裁判権を事前に包括的に放棄する、「事前包括同意条項」あり
裁判管轄		協議事項であり、協議不調の場合は被告国	国際機関(ICSID)のみ
仲裁を行う国際機関		ICSIDのほか、WTOとUNCITRAL	ICSIDのみ
準拠法	被告国の司法機関で審理	被告国の現地法 (州法の場合あり)	
	国際機関で審理	双方で協議し、不調の場合は「被告国法」が適用される	双方で協議し、不調の場合は「被告国法」が適用される
濫用・悪用の実態		発生しない	多発しており、国際問題になっている
備　考		米国とコロンビアなどのNAFTA以前のFTAは日本型	米韓FTAはこのタイプ

【おわりに】

システム監査においても、この「似て非なるもの」を峻別する力量を磨くことが何よりも重要であることは言うまでもない。そのためには、我々システム監査人が、汎用的な「システム監査基準」のみに依拠することなく、被監査対象の業務や用語の知見を深めるとともに、業界の慣行・業界の事情に深く精通することが必要である。その為には、公認システム監査人の認証においても、金融・保険・製造業・建設・運輸・医療などの各々の専門分野別の認証があってもよいように思われる。

SAAJ の様々な会合等で「システム監査」のあり方が話題になると、いまだに「助言型」か「保証型」の議論に留まっているケースも少なくない。確かにこの問題は"古くて新しい問題"ではあり、この論点についての検証も重要であるが、システム監査の実効性を高め、システム監査技術者や公認システム監査人の認知度を高め、社会的地位を高め、職域を拡大するためには、そろそろ、次の段階に進むと段階に来ているのではないだろうか?　日頃、筆者に様々な示唆・助言を頂く、中田和男氏、神尾博氏、横山雅義氏、吉田博一氏、力利則氏ほか皆様方に、この場を借りて深く御礼申し上げたい。(以　上)

<<Reference>>

1.「新しい「ＩＴ事業者評価制度」導入の政策提言」(中田和男、神尾博、横山雅義、田淵隆明)
http://www.saajk.org/wordpress/wp-content/uploads/saaj_20130706_thesis04.pdf
2.「システム監査の法的義務化」等のIT政策提言(神尾博、中田和男、横山雅義、田淵隆明)
http://www.saajk.org/wordpress/wp-content/uploads/23111252dd43ea67aab2e10223fd517e.pdf
3. SAP ジャパン IFRS エキスパートコラム　1-29(田淵隆明)
http://global.sap.com/japan/campaigns/2010/ifrs/expert.epx

(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。)

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。

仲 新会長からの一行メッセージ
“当協会の発展とシステム監査の普及促進に全力を尽くします。”

2013.12 投稿

【 システム監査活性化プロジェクト 】

会員番号 6027 小野　修一(活性化PT　主査)

今月の会報でも、システム監査の活性化につながる活動を行っている当協会の研究会や担当組織の中から、いくつかの活動について、ご報告しています。

１．情報セキュリティ監査研究会

今回は、情報セキュリティ監査研究会からのプライバシー・バイ・デザインご紹介の４回目として、従来単独の組織（企業、自治体、政府機関等）で行ってきたプライバシー影響評価（PIA）を、組織間の連携した活動に拡張するコンセプト、連携プライバシー影響評価（F-PIA）について紹介します。F-PIA は、組織間で共通のプライバシーポリシーやプライバシー保護のコンセプトを策定し、これに基づく影響評価を行うことで、より現実的かつ有効な PIA を実現しようとする試みです。ぜひ、ご一読ください。

２．システム監査基準研究会

システム監査基準研究会からは、先月に引き続き、IT Audit の ISO 化（ISO 30120）に関する資料の一部（目次の仮訳の一部）を紹介します。この ISO 化の活動には、当研究会メンバーが参加しています。ぜひ、ご一読ください。

３．個人情報保護監査研究会

個人情報保護監査研究会からは、今までに続いて、当研究会でまとめた『個人情報保護マネジメントシステム実施ハンドブック』簡易版の内容の一部を紹介します。今回のテーマは「教育」、「文書管理」、「苦情・相談対応」です。システム監査人の主要な活動分野の一つである個人情報保護マネジメントシステム（PMS）の構築・評価を行う際の参考にしていたきたく、紹介しています。ぜひ、ご一読ください。

以上

2013.12 投稿

【　システム監査基準研究会　】

会員番号 0555 松枝憲司　 0281 力利則 (システム監査基準研究会)

○IT-ＡｕｄｉｔのＩＳＯ化について

先月に引き続き、9/24(火)の CSA フォーラムにおいて報告しました ISO30120(IT-Audit)についての資料の一部を紹介します。

「IT監査-ITガバナンスの評価を支援する監査のガイドライン（ISO30120：PDTR)(仮訳)」

5.2.1 監査プログラムの概観　（ 要約: 仮々訳）

監査は、監査基準を満たすための範囲を決定して、監査証拠を取得し、それについて客観的に評価するための体系的で独立し、文書化されたプロセスである。

IT 監査の領域には、ISO/IEC 38500:2008(ITガバナンス) によって設定されている6つの原則(プリンシプル)が含まれる。これらの原則は次のとおりである。

1. 責任
2. 戦略
3. 調達・取得
4. パフォーマンス
5. 適合・準拠
6. 人的行動

各原則のための監査基準は、プロセスおよびプロダクトの2つのカテゴリに分類することができる。
つまり関連するプロセスが存在して適切な運営がされていることを確認する。
関連するプロダクト（例えば文書（活動の証拠)、各種記録、システム、および成果物)が適切な内容で存在していることを確認する。

プリンシプル1　責任

組織内の個人及びグループは、ITの供給及び要求に関してそれぞれの責任を理解し、受け入れる。
行動に責任を持つ者は、それらの行動を遂行するための権限も有している。

プロセス

1.　現状及び将来のビジネス目標の策定の為のプロセス
2.　組織のビジネス目標を達成するIT利用を方向付けするための、ITの責任を付与するプロセス
3. ITガバナンスの為の責任者のパフォーマンスをモニタリングするためのプロセス

プロダクト

1. 適切なITガバナンスのメカニズム
2. 実行責任および説明責任を達成するために必要な情報

2013.12 投稿

【情報セキュリティ監査研究会だより その９ ー プライバシー・バイ・デザイン 第４回】（連載）

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、アン・カブキアン著、「プライバシー・バイ・デザイン　プライバシー情報を守るための世界的新潮流」をテキスト(以下、左記の書を「テキスト」と称します)として、「プライバシー・バイ・デザイン」の意義、影響、PIAやシステム監査との関係などを議論しております。

前回からテキストの第2章第6節「新たな連携プライバシー影響評価(Ｆ－PIA):プライバシーと信頼できる連合体の構築」を取り上げております。なぜ、この節を取り上げたかというと、ネットワーク社会の進展にともない個人情報が複数の組織間(企業、政府機関、その他の団体)で大量に授受されることが当たりえまえになってきているなかで、未だ個人情報保護に関する種々の取り組みが単一の組織内に留まっていて、かかる状況に対応できていないと考えるからです。我が国のプライバシーマーク認証制度も単一の組織を対象としています。

この問題に対して、真正面から取り組んでいるのが、カブキアン博士の提唱するF-PIA（連携プライバシー影響評価）です。前回はF-PIA実装の前提になるFIM(連携アイデンティティ管理)をご紹介いたしました。今回は、FIMの実現形態であるアイデンティティ連合体の四つのモデルをご紹介します。次に、この連合体によって実施されるF-PIAの目的についてご説明いたします。以降のご紹介は次号の会報に継続します。

なお、本報告は、情報セキュリティ監査研究会内部の検討結果であり、日本システム監査人協会の公式の見解ではないことをお断りしておきます。また、我々の力不足のため、誤りも多々あるかと存じます。お気づきの点がございましたら適宜ご指摘いただきたいと存じます。ご興味のある方は、毎月20日前後にSAAJ本部会議室(茅場町)で定例研究会を開催しておりますので是非ご参加ください。参加ご希望の方、また、ご意見やご質問は、下記アドレスまでメールでご連絡ください。 security ☆ saaj.jp （発信の際には“ ☆ ”を“@”に変換してください）

＜テキスト＞

堀部政男／一般財団法人日本情報経済社会推進協会(JIPDEC、以下、同じ)編、アン・カブキアン著、JIPDEC 訳
「プライバシー・バイ・デザイン　プライバシー情報を守るための世界的新潮流」、2012年10月、日経BP社

【報告内容】新たな連携プライバシー影響評価（F-PIA：Federated Privacy Impact Assessment） その２
ー アイデンティティ連合体とＦ-ＰＩＡの目的 ー

１．アイデンティティ連合体について

急速なネットワーク社会の進展にともない、大量の個人識別情報(PII:Personal Identity Information)の収集、取得、管理及び活用がしばしば複数の事業者にまたがって行われている。個人識別情報に関わる複数の事業者が個人情報保護に係るそれぞれ異なる個別のポリシー、手順あるいは技術的基盤をもっているとすると、個人識別情報を提供する側にとって極めて不都合である。この問題を解決するためのFIM(Federated Identity Management、連携アイデンティティ管理)というコンセプトを前回、ご紹介した(会報153号:2013年12月号、P10-11、以下、前会報と称す)。このFIMを前提にF-PIAを実現する「アイデンティティ連合体」についてご紹介する。

F-PIAでは、参加する各企業等の組織が保有する個人情報の内容が明確に定義される。また、各企業間のデータフローが明確に文書化される。この点では、一企業内で実施される個人情報保護の方式を組織間に拡張したものといえる。次に、各参加組織は、アイデンティティプロバイダー、サービスプロバイダー、検索サービスのように、役割が定められ、それぞれが扱うことができる個人情報の種類は、連携システムの技術仕様として明確に定義される(前

会報参照)。

F-PIAでは、新たな組織やサービスが加わるたびに全体を再評価することは、現実的ではない。むしろ、新たに加わった組織やサービスと既存の組織やサービスの役割、責任及び要件を比較する方が現実的である。

アイデンティティ連合体においては、その連合体におけるプライバシー標準を策定、適用し、F-PIAを実施する。その次に行うべきことは、参加組織間でのプライバシーポリシー、手順及びプラクティスを連携させることである。

標準の策定やF-PIAの実施に当たって、どのようなアプローチがあるかは、連合体の形態によって異なる。以下の4つの連合体のモデルをご紹介する。

第一の形態は、「協力モデル」である。このモデルでは、創設者である参加組織が連合体のエコシステムを運営する事業体を形成する。いわば参加組織が同等の権限をもつことになり、柔軟性は最も高いが、無制限のメンバーシップを悪用される可能性も高く、厳格なプライバシールールと厳しいF-PIAが必要になる。

第二の形態は、「コンソーシアムモデル」である。このモデルでは、少数の創立者が形成するコンソーシアムがF-PIAの主体となり、エコシステムのルール設定とガバナンスを行う。ただし、複数の創立者には個別に自立性があるため、創立者間で異なるプライバシーモデルを利用している可能性がある。そのため連合体全体のプライバシーに関する表明は、最低限の共通項になることが多い。

第三の形態は、「集中モデル」である。このモデルでは、単一の創立者がエコシステムのルール設定とガバナンスを行う。このモデルでは、データの流通が単一の創立者によって行われるか、少なくとも把握される。それゆえ、プライバシーに関する表明や、F-PIAの結果として行う種々の施策は、単一の創立者が連合体に組み込む。

第四の形態は、「サービス指向アーキテクチャー（以降、SOA）」に基づく連合体の運営モデルである。この利点は、SOAの原則に則り、サービス要素ごとに評価すればよいことである。サービス連携の入力(サービスがアクセスした情報)と出力(利用したサービス要素の結果)について評価する。

2. F-PIAの目的

F-PIAの主たる目的は、以下の4点である。

一つ目は、連合体の参加組織がプライバシーポリシーを議論、開発及び体系化する機会を提供することである。プライバシーポリシーは、連合体によって異なる。各参加組織は、その参加する連合体のポリシーに従いつつ、自身のプライバシーポリシーを掘り下げる機会を提供する。

二つ目は、連携システムの参加組織が定着したプライバシーポリシーが守られていることを実証することである。連合体の運営者がF-PIAを実施することにより、各参加組織のプライバシーポリシーの遵守の程度が把握できる。

三つ目は、プライバシーポリシーに対する偶発的または意図的な違反を可能な限り予防するための、適切な技術的アーキテクチャーが存在することを証明することである。F-PIAは、反復的で継続的なプロセスであるべきである。プライバシー保護に関する違反の予防や発見に、参加組織のプライバシー保護システムが有効であるか否かを判定するために、F-PIAは、適宜、実施し、また、見直されるべきものである。

四つ目は、F-PIAを実施、利用、信頼するすべての当事者に利益をもたらすことである。F-PIAのプロセスにより、最終的にプライバシー保護の利益を享受するのは、個人情報の主体である個々の消費者である。しかし、F-PIAによって得られる有用な知見を組織内各層、ことにシステム設計者に与えることにより、プライバシー保護に関し、より適切で消費者に安心感を与える施策を取らせることが可能になり、結果として、その組織に競争上の優位性、消費者からの信頼性の向上等々のメリットを得させることになる。

以上

2013.12 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 17 章

会員番号：1795　藤澤　博（個人情報保護監査研究会）

第17章　教育

事業者は、個人情報を実務で取扱う従業者の啓発を図り、従業者の個人情報保護意識を徹底するためにすべての従業者に対し定期的に教育を実施します。

17.1　教育計画

1. 個人情報保護教育責任者は、すべての従業者を対象として「3451PMS 教育計画書（兼報告書）」を作成し、個人情報保護管理者および代表者の承認を得ます。
2. 同一社内で、営業職と現業職など、個人情報の取り扱いが大きく異なる場合は、職務内容と職務権限を考慮して「3451PMS 教育計画書（兼報告書）」を、複数パターン作成することがあります。

事例「3451PMS 教育計画書（兼報告書）」の前半

<table>
<tr><td colspan="3" rowspan="2">201★年度
PMS教育計画書兼報告書</td><td>承認</td><td>確認</td><td>作成</td></tr>
<tr><td>代表者
印
201 / /</td><td>個人情報保護管理者
印
201 / /</td><td>教育責任者
印
201 / /</td></tr>
<tr><td>教育区分</td><td colspan="2">定期教育</td><td>実施日</td><td colspan="2">201 年　月　日～201 年 月 日</td></tr>
<tr><td>教育目的</td><td colspan="2">個人情報保護マネジメントシステム(PMS)の運用開始にあたって</td><td>実施時間</td><td colspan="2">①本社1 ： 月 日　10:00～12:00
②本社2 ： 月 日　13:00～15:00
③〇支店 ： 月 日　10:00～12:00</td></tr>
<tr><td>対象者</td><td colspan="2">全役員、社員、嘱託、派遣社員</td><td>担当責任者</td><td colspan="2">管理部:〇〇〇〇(内線xxx)
kyoiku@xxxx.co.jp</td></tr>
<tr><td>対象人数</td><td colspan="2">60名</td><td>実施場所</td><td colspan="2">3階　第一会議室</td></tr>
<tr><td rowspan="9">内容</td><td>1</td><td>Pマーク認証取得の必要性</td><td>実施方法</td><td colspan="2">講義方式</td></tr>
<tr><td>2</td><td>PMSとは～JISQ15001 2006 の要求事項</td><td>講師</td><td colspan="2">オフィスマネジメント　斎藤講師</td></tr>
<tr><td>3</td><td>PMS導入の重要性と利点</td><td rowspan="3">テキスト</td><td colspan="2">・JISQ15001(2006) 教育テキスト</td></tr>
<tr><td>4</td><td>PMS適合の役割及び責任～体制について</td><td colspan="2">・個人情報保護方針</td></tr>
<tr><td>5</td><td>PMSに違反した時に予想される結果
就業規則、個人情報保護法違反</td><td colspan="2">・個人情報保護基本規程</td></tr>
<tr><td>6</td><td>「個人情報管理台帳」～個人情報の特定</td><td>効果確認方法</td><td colspan="2">理解度チェック(テスト)</td></tr>
<tr><td>7</td><td>「リスク分析」の実施</td><td rowspan="2">参加有無</td><td colspan="2" rowspan="2">全員必須(①②③とも定員30名、指示された時間に都合がつかない場合は事前連絡・振替可能)</td></tr>
<tr><td>8</td><td>今後のスケジュール</td></tr>
<tr><td colspan="2" rowspan="2">講義終了時の約10分間。簡単な理解度チェックテスト)を行います。</td><td>通知方法</td><td colspan="2">メール(一斉、一部個別)</td></tr>
<tr><td>費用</td><td colspan="2">無料</td></tr>
<tr><td></td><td colspan="2">①②③とも教育内容は同じです。</td></tr>
</table>

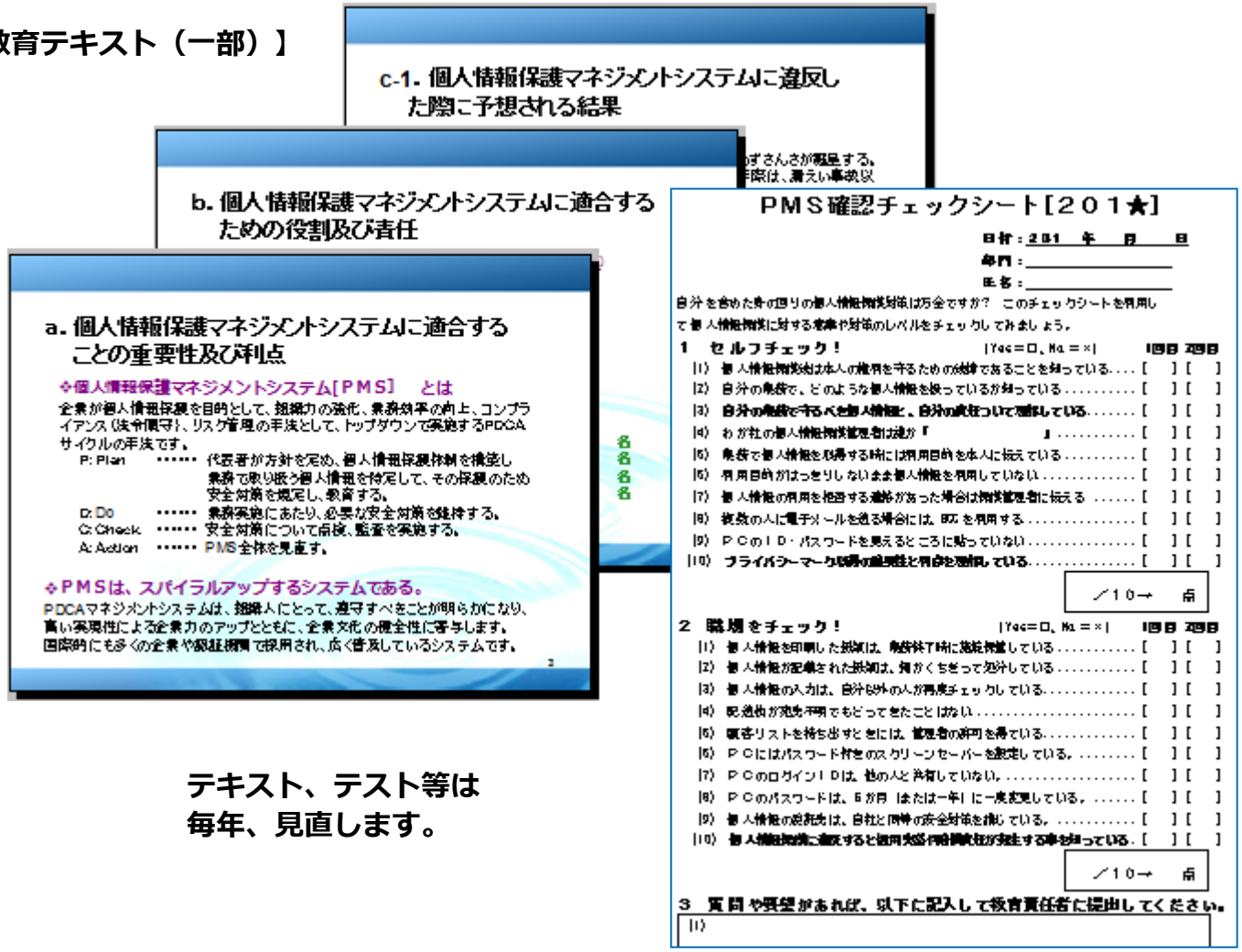
17.2　教育の実施

教育責任者は、以下のa)、b)、c)を理解させるため「3456 教育テキスト」を策定し、毎年１回以上教育を実施します。

a)	ＰＭＳに適合することの重要性及び利点
b)	ＰＭＳに適合するための役割及び責任
c)	ＰＭＳに違反した際に予想される結果

また、受講者に対して、理解度を確認することを目的として、テスト、アンケート等を実施します。

【教育テキスト（一部）】



テキスト、テスト等は
毎年、見直します。

17.3　随時の教育

以下の事例のような場合には、随時教育を実施し、「3451PMS 教育計画書（兼報告書）」を利用して記録を残します。　　【随時教育の事例】

a)	法令、国が定める指針その他の規範の改廃により、自社のＰＭＳが見直された場合
b)	施設の移転、設備の更新など、セキュリティルールの変更があった場合
c)	採用者に対する初回教育（業務に就く前に教育を実施する）
d)	事故等の緊急事態発生に関連する是正処置において、新たなルールを規定した場合
e)	他事業者で発生した事故等から、自社の予防処置としてルールを見直した場合

17.4　教育の効果確認

教育計画の意図どおりに教育が実施され、教育成果が得られたかを確認するため、受講者に対して実施したテストやアンケートの結果の分析を行います。結果は「3451PMS 教育計画書（兼報告書）」に記載、または、別紙を作成し添付資料としてもよいでしょう。

17.5　教育の実施報告

教育責任者は、受講対象者全員が受講したことを「受講者リスト」によって確認し、テスト・アンケート等の結果を含めて、「3451PMS 教育計画書（兼報告書）」に記録し、代表者に報告します。

「3451PMS 教育計画書（兼報告書）」の後半：結果報告

結果報告	
参加者	定期教育:　　名/全従業者　　不参加者のフォローアップ:201　年　月　日に実施完了
	新人教育:　　名/201★年度入社　全員完了
理解度	テスト平均点:　　点　　全員100点まで再実施した。 ◇当社従業員の理解度が弱い点: ◇対策:
次回教育への反映	◇実施時期: ◇内容
コメント	個人情報保護管理者: 代表者:

201★年度　「PMS定期教育　受講者リスト」

No.	社員番号	氏名	受講日	理解度確認結果	フォローアップ要否
1					
2					
3					
4					
5					

受講者は、社員個別に管理します。
「3451PMS 教育計画書（兼報告書）」別紙

17.6　教育記録の保持

教育の計画及び実施、結果の報告及びそのレビュー、計画の見直し並びにこれらに伴う記録は、ＰＭＳ事務局で保持します。

17.7　次年度への反映

教育の効果確認の結果は、次年度の教育計画のインプット情報として反映させることは、最も重要です。

2013.12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 18 章

会員番号：1795　藤澤　博（個人情報保護監査研究会）

第18章　文書の管理

プライバシーマーク認証審査では、ＰＭＳが適切に維持されているかどうかを客観的に確認します。確認する対象は主として文書で、第三者が見てもわかりやすく記述されていることが重要です。実施記録などはエビデンス（証憑）と呼ばれることがあります。

18.1　文書の作成

ＰＭＳの基本となるのは次の要素です。「PMS 文書体系」を策定して、維持管理します。

a)	個人情報保護方針
b)	内部規程（例：「3301個人情報取扱規程」「3430安全管理規程」）
c)	計画書（例：「3303ＰＭＳ年間計画書」「3451ＰＭＳ教育計画書」「3721ＰＭＳ監査計画書」
d)	記録（JIS Q 15001:2006が要求する記録、ＰＭＳを実施する上で必要と判断した記録）

18.2　文書の承認

個人情報保護方針、内部規程は、代表者の承認を得ます。

規程は、文書の先頭に制定年月日、改訂年月日、代表者名を記載し、記録には、作成者、作成日、承認者、承認日付欄を設置し、記入漏れのないようにします。

18.3　文書の周知

承認された文書は、全従業者がいつでも参照できるよう、文書の周知担当者を決めて迅速に、確実に周知します。閲覧される文書は最新版のみとし、紛らわしいファイルが存在してはなりません。

【周知ルールの事例】

a)	ＰＭＳ文書の制定および改定については、従業者にメールで通知する。
b)	ＰＭＳ文書の改定を行ったときは、改定内容を明確にして従業者に通知する。
c)	ＰＭＳ文書の原本は、全従業者が閲覧可能な¥共有ファイルサーバー¥PMSフォルダ¥に保管し、記録様式等は、ダウンロードできるようにする。
d)	旧版文書は、ＰＭＳ事務局のみがアクセスできるフォルダに保管する。

18.4　文書の改定

文書を改定する場合は、まず旧版文書（例：2012 年度文書）を保管し、コピーをもとに改定作業に取りかかります。改定箇所がわかるよう、訂正・追加は赤字で入力し、削除は消し線を使います。

18.5　文書（記録含む）の保管・管理

文書の保管・管理責任者は、個人情報保護管理者ですが、各部門で保管担当者を任命して紛失防止に努めてください。プライバシーマークの更新サイクルは 2 年ごとで、現地審査では、2 年間の記録を提示しますので、原本は少なくとも 2 年間保管してください。

原本は、紙でなくデータでも構いません。

18.6　ＰＭＳ文書体系（サンプル文書）

	PMS 文書を構成する規程・様式の名称	制定日	直近の改正日
1	3200 個人情報保護方針	201★年４月１日	
2	3210 個人情報の取扱い	201★年４月１日	
3	3300 個人情報保護基本規程（非公開）	201★年４月１日	….
4	3301 個人情報取扱規程	201★年４月１日	
5	3303ＰＭＳ年間計画書	201★年４月１日	
6	3341 個人情報保護体制	201★年４月１日	
7	3320 法令・指針・規範集	201★年４月１日	
8	3311 業務フロー	201★年４月１日	
9	3312 個人情報管理台帳	201★年４月１日	
10	3313 リスク分析表	201★年４月１日	
11	3371 緊急時連絡網	201★年４月１日	
12	3373 事故報告書	201★年４月１日	
13	3421 個人情報取得・変更申請書	201★年４月１日	
14	3424 通知と同意書（採用面接用）	201★年４月１日	
15	3424 通知と同意書（従業者）	201★年４月１日	
16	3424 通知と同意書（店舗用）	201★年４月１日	
17	3424 通知と同意書（その他）	201★年４月１日	
18	3425-21　適正な取得チェックリスト	201★年４月１日	
19	3425-22　電話メモ（通知事項）	201★年４月１日	
20	3430 安全対策規程	201★年４月１日	
21	3431-01 機密保持誓約書	201★年４月１日	
22	3432-010 システム機器・ＩＤ管理台帳	201★年４月１日	
23	3432-011 サーバー利用申請書	201★年４月１日	
24	3432-012 フロアマップ	201★年４月１日	
25	3432-015 情報機器「持出」許可申請書	201★年４月１日	
26	3432-016 情報機器「持込」許可申請書	201★年４月１日	
27	3432-017 携帯端末使用許可申請書	201★年４月１日	
28	3432-211 入退館安全確認記録簿	201★年４月１日	
29	3432-212 来客入退館カード貸出簿	201★年４月１日	
30	3432-213 サーバー室入退室記録簿	201★年４月１日	
31	3432-221 鍵・ID カード管理簿	201★年４月１日	
32	3432-410 個人情報返却廃棄管理表	201★年４月１日	
33	3434-01 委託先管理台帳	201★年４月１日	
34	3434-02 委託先調査票	201★年４月１日	
35	3434-03 業務委託契約書	201★年４月１日	
36	3434-04 委託業務指示書	201★年４月１日	
37	3434-05 委託業務指示書管理台帳	201★年４月１日	
38	3440-01 個人情報開示等請求書兼回答書	201★年４月１日	
39	3451PMS 教育計画書（兼報告書）	201★年４月１日	
40	3456 教育テキスト	201★年４月１日	
41	3457 理解度チェックシート	201★年４月１日	
42	3510PMS 文書体系	201★年４月１日	
43	3601 苦情・相談報告書	201★年４月１日	
44	3721ＰＭＳ監査計画書（兼報告書）	201★年４月１日	
45	3725a_JIS 適合監査チェックリスト	201★年４月１日	
46	3726b_予備調査チェックリスト（CL）	201★年４月１日	
47	3313__リスク分析表（兼監査 CL）	201★年４月１日	
48	3726d_PMS 体制の運用 CL	201★年４月１日	
49	3726e_施設設備の安全性 CL	201★年４月１日	
50	3726f_情報システム運用の安全性 CL	201★年４月１日	
51	3726g_情報システム開発の安全性 CL	201★年４月１日	
52	3726h_部門リスク分析表反映 CL	201★年４月１日	
53	3801 是正・予防措置報告書	201★年４月１日	
54	3901 代表者による見直し議事録	201★年４月１日	
55	4000PMS 例外処理申請書	201★年４月１日	

2013.12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 19 章

会員番号：1795　藤澤　博（個人情報保護監査研究会）

第19章　苦情・相談対応

事業者は、法 31 条に基づいて、個人情報の取扱いに関する苦情の適切かつ迅速な処理及び体制の整備に努める必要があります。苦情・相談が寄せられた場合は、緊急事態発生手順に準じて取扱います。

19.1　苦情

苦情を受付けた場合の、対応手順の事例を示します。

a)	電話で苦情・相談を受付けた者は、概要と電話番号をヒアリングして、「3601苦情相談報告書」に記入し、“責任ある者から折り返しする”ことについて了解を得ていったん電話を切り、苦情・相談責任者に報告する。
b)	苦情・相談責任者は、本人に電話連絡し、苦情・相談の内容を「3601苦情相談報告書」に追記して個人情報保護管理者に報告する。会社への影響度を考慮し、代表者にも報告する。
c)	個人情報保護管理者は、苦情・相談の内容を確認し、関係者に調査を依頼し、その結果および回答案を「3601苦情相談報告書」を用いて代表者に報告し、承認を得た上で、本人に回答する。ただし、軽微な苦情または相談は、個人情報保護管理者の承認のみで対応することができる。
d)	すべての「3601苦情相談報告書」は、本人の納得状況を含めた結果を記載し、代表者に報告する。
e)	個人情報保護管理者は、苦情及び相談の内容をもとに、「3801是正・予防処置報告書」を策定し、真の発生原因を追究して改善策を講じる。

本人に対し、
文書で回答が必要な場合は、
苦情の内容に応じた
「レター（一般業務文書）」
で回答します。

苦情・相談報告書

業務名		受付年月日 受付者
苦情 相談者情報 （わかる範囲でよい）	氏名	
	住所	
	電話番号 メールアドレス	
本人からの連絡	□ 来社　□ メール　□ 電話　□ 郵便　□ その他（）	
苦情・相談の区分	□ 強い苦情　□ 一般の苦情　□ その他の相談　□ 緊急	
苦情相談の内容 （本人の言葉で具体的に）		

19.2　相談

相談は、苦情の直前と捉え、苦情と同様の手順により対応します。

19.3　是正処置

苦情は、外部からの提言と捉えて、苦情を発生させた部門長に「3801 是正・予防処置報告書」の作成を指示し、苦情に至った真の原因を追究し是正処置をとります。

次回は、「第 20 章　点検」をご紹介します。＞目次へ

個人情報保護監査研究会　http://www.saaj.or.jp/shibu/kojin.html　以上

2013.12 投稿

研究会活動【「西日本支部合同研究会　in Kanazawa」 報告】

会員番号 1281 宮本 茂明 (北信越支部)

以下のとおり「西日本支部合同研究会　in Kanazawa」を開催しました.

・テーマ：**「システム監査の普及促進」**
　　-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ついて考える-
・日時：2013年11月23日(土)　13:00-17:00
・場所：ITビジネスプラザ武蔵　6階 交流室１ (石川県金沢市)
・主催：特定非営利活動法人日本システム監査人協会
　　北信越支部，中部支部，近畿支部，中四国支部，九州支部
・後援：特定非営利活動法人 ITコーディネータ協会，特定非営利活動法人福井県情報化支援協会，
　特定非営利活動法人石川県情報化支援協会，特定非営利活動法人 ITコーディネータ富山，
　日本ＩＴストラテジスト協会　中部支部
・次第：

『力強いシステム監査の実現へ』
　日本システム監査人協会 副会長 中山 孝明 様

『地域団体におけるシステム監査の価値について-社会、コミュニティ、個人のニーズに応えるシステム監査-』
　日本システム監査人協会 九州支部 中溝 統明 様

『新しい「IT 事業者評価制度」導入の政策提言』
　日本システム監査人協会 近畿支部 中田 和男 様

『民間企業におけるシステム検査の利用について』
　日本システム監査人協会 中部支部 原 善一郎 様

『金融機関におけるシステムリスク管理の取組について-経営の関与とシステム監査の活性化-』
　日本システム監査人協会 北信越支部 長谷部 久夫 様

2013 年度の西日本支部研究会を北信越支部が幹事支部として金沢で開催しました。
今回の合同研究会は、経営活動を支える情報システム環境の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ついて考えるというテーマで、本部及び西日本の 4 支部からご報告いただきました。

参加人数は、発表者 5 名を含めて総勢 27 名で、日本システム監査人協会 24 名(九州支部 2 名、中四国支部 1 名、近畿支部 1 名、中部支部 5 名、北信越支部 13 名、他支部 2 名)、後援団体 3 名でした。

◇講演Ⅰ

報告者（会員 No. 1526　國谷　吉英）

【講演テーマ】

『力強いシステム監査の実現へ』

【講師】

日本システム監査人協会　副会長　中山 孝明　様

【講演内容】

「力強いシステム監査の実現へ」という演題でシステム監査活性化に向けた協会の取り組みや、システム監査の普及促進について説明された。以下、内容を紹介する。

１．総力の活性化活動

協会全体で精力的に活動している「システム監査活性化プロジェクト」について紹介と説明があった。

① ＰＴ活動の柱；会員メリットのアップ、新たな施策、対外アピールなど

② 活動成果など；学生向けのシステム監査認知度アンケートの実施、会員向けの活性化提案の募集、月例研究会の開催案内を他の団体にも送付など最近２年間の毎月の実績や、システム監査啓発小冊子の発行など現在取り組み中の施策など

２．逞しいシステム監査人

システム監査の時代変遷に見られるシステム監査人に求められる期待像や、事務合理化からリスク指向等への情報システム環境の変遷に伴うシステム監査人の吸収力や適応力について説明があった。

また、システム監査の目的である情報システムのリスクコントロールやＩＴガバナンスの実現に向けたシステム監査人の役割発揮についてチェックリストだけに頼らない監査人自らの判断基準を持つことも重要であると説明された。

３．パワフルなシステム監査

① ワイドな領域・活動場面；有効性、リスク指向、準拠性等のアプローチや、ＩＴ統制評価や、情報セキュリティ監査、個人情報保護監査等の広範囲な活動領域の説明があった。

② 組織内システム監査の重み；事業目的実現や、組織の課題解決、組織の根付き・自発的機能、現場力、システム監査の未来を背負う等の重みについて説明があった。

③ 専門家／職業人としてのシステム監査人；知識や経験、研鑽等専門的なノウハウ、価値観、責任感、実現意欲など情報システム発展への貴重な人材資源となっている旨の説明があった。

④ 近未来への期待・貢献・課題；システム監査が会計監査や監査役監査などにも欠くことのできない位置を占めていることや、システム監査の未開拓分野への取り組み、環境変化に応じた役割の自主的開拓、システム監査の Identity などとともに、システム監査の社会的制度への定着の重要性とその実現への課題について説明があった。

４．システム監査の実施状況から

現状認識をさらなる発展策へということで一例を示し、最近実施された内部監査実施状況調査の結果から、システム監査の実施状況を自らの視点で集計・分類した内容について説明があった。

◇講演Ⅱ　　報告者（会員 No. 0947　梶川　明美）

【講演テーマ】

『地域団体におけるシステム監査の価値について
-社会、コミュニティ、個人のニーズに応えるシステム監査-』

【講師】

日本システム監査人協会　九州支部　中溝 統明　様

【講演内容】

地方団体において、システム監査がいかに価値あるものであるかについて考察された。
以下、その内容を紹介する。

１．ＩＣＴの利活用

1960 年代の汎用機の時代から始まったＩＣＴ利活用の波は、2000 年代以降モバイルの利用によるインターネットの時代へと移行している。金融、医療、自治体などにおいても、ＩＣＴの利活用は進化を遂げて現在に至っている。

２．ＩＣＴ当事者

情報システムの当事者は、データ活用の多様化に伴い多岐にわたる。ＩＤＣやクラウドでは、情報システムの委託者側としても注意しなければならない。特にクラウドシステムの中は見えないので、仕様書に注意する必要がある。今や情報システムは組織の重要なインフラとなっており、地域社会にとっても重要なものである。リスクの顕在化による新たな課題を適切にコントロールする必要性がある。そのためにシステム監査が必要になるのである。

３．イノベーションと安全問題

イノベーションは、コトの中にモノ（技術）を埋めていく。システムの複雑性が増し、想定外の事態に対する脆弱性が問題の発生源となっており、原因がどこにあるかわからない。障害を早く復旧させるレジリエンスの高いシステムがよいシステムである。

４．監査と評価

ＣＯＢＩＴやシステム監査基準は変遷している。また、情報セキュリティ監査やＩＳＯ認証監査など、様々な評価基準や評価機構がある。しかしながら、地方団体の正しい審査や評価は難しい。

５．自治体の状況

自治体クラウド、オープンデータやビッグデータ、共通番号制度の導入などこれからの自治体はいろいろなことに取り組まなければならない。また、理想的な情報システムを目指して、情報システムの最適化にも取り組んでいる。

６．システム監査の価値

「監査」という言葉を聞くと会計監査をイメージし、システム監査が何であるのか正しく理解されていない。システム監査は組織体の情報システムが適切に整備・運用されていることを担保するための有効な手段となる。システム監査の実施は組織体のＩＴガバナンスの実現に寄与し、利害関係者に対する説明責任をも果たす。情報システムを正しく評価できるのが『システム監査』である。

システム監査を担うシステム監査人は、これらの役割を担っている。

◇講演Ⅲ

報告者（会員 No. 1587　清水　尚志）

【講演テーマ】

『新しい「IT 事業者評価制度」導入の政策提言』

【講師】

日本システム監査人協会　近畿支部　中田 和男 様

【講演内容】

近畿支部ｼｽﾃﾑ監査法制化ﾌﾟﾛｼﾞｪｸﾄで検討された「IT 事業者評価制度」導入の政策提言について説明された。

1．現状の問題点と IT 業界の環境の変化

2001 年からの規制緩和として、「ＳＩ登録・ＳＯ認定の廃止」や「企業経理での研究開発費の資産計上廃止」「ソフトウェアの PL 法への適用漏れ」「システム監査の法制化の見送り」等の政策が行われた事により、IT 業界の健全な発展はおろか、システムの発注者や消費者にも損害や不満をもたらした。

こうした中、IT 業界の業界構造変化と顧客関係及び競合関係の変化をとらえ、IT 業界の再生に寄与する政策提言として、システム監査の視点から IT 事業者の力量が客観的に評価できる制度が必要であると考えた。

2．既存のＩＴ業者の評価制度

SI 登録制度や SO 認定制度など一定の長所が認められた制度が廃止された。その他の国際基準（ISO9000 等）のフレームワークがあるが、経営力や技術力の高さを表す評価ではない上に、具体性がないため評価が恣意的になる場合もある。このような既存の評価制度の中、官公需のニーズにも対応する新しい「IT 事業者評価制度」導入は必須であると考えた。

3．新しい「IT 事業者評価制度」のあり方とは

新しい評価制度の要件として①事業者全体の力量が評価できる体系、②IT 事業分野全般を網羅し適切なカテゴライズされている、③点数化により明確に順位づけする、④継続的な運用が可能である、⑤評価手続きの費用に経済性がある、などがあげられる。

IT 業者の評価に際し、建設業法の経営事項審査制度の長所を参考にし、一部を IT 産業に適合した項目に置き換えた採点方式を、一つの案として提示した。社会性等評価に管理資格者数（公認システム監査人・中小企業診断士）を設ける等、経営力・技術力等の諸項目を点数化・集計することで、順位付を可能にして客観性を確保した。

4．ＩＴ事業者評価制度導入の効果

本制度の導入によって、下記のような効果が期待でき、官公庁の発注者や IT 業界に留まらず、広く国民に受益のある制度になると考える。

①合理的な発注先選定と成果物の品質向上

②競争の透明性確保

③システム監査の開発・運用業者の力量確認の精度向上と効率化（低価格化）

④IT 業界の人材育成・技術者評価への意識向上による優良事業者の育成と国際競争力の強化

5．まとめ

この制度は、従来の諸制度の短所を補完する新しい制度である。客観性を有し、順位づけを可能とし、入札の透明性・適正性の確保、優良 IT 事業者の育成・分別、システム監査における効率化及び監査領域の拡大等の、多岐に渡り多大な効果が期待できる。制度を実現、活用定着させ、広く国民への受益につなげていく必要がある。

◇講演Ⅳ

報告者（会員 No. 1354　栃川　昌文）

【講演テーマ】

『民間企業におけるシステム検査の利用について』

【講師】

日本システム監査人協会　中部支部　原 善一郎 様

【講演内容】

グローバル化や想定外の災害や脅威対応に向けて、民間企業は積極的な経営革新や IT 体制維持/革新が必須である。IT の点検・検査・監査活動は経営革新を支える重要なツールであり、こうした活動にも破壊と創造が必要であることを発表いただいた。

1．自動車部品製造業 P 社の IT 化の歴史

自動車部品製造業、世界 7 カ国に拠点、従業員 3000 人程度、年商 1000 億円

1970 年代　電子計算機導入

1980 年代　オンラインリアルタイム処理導入、顧客との EDI 処理

1990 年代　グループ企業間での情報供給

2000 年代　本社と海外子会社間での VPN 接続

2．システム監査・システム検査利用

P 社は、1994 年に SAAJ の監査普及サービスを利用しシステム監査を受け、開発手順の整備を指摘された。その後、ISO9001・ISO27001・ISO2000 などを参考に、システムに関する各種の手順を社内に導入してきた。一方、次のような PDCA 活動を通じて、こうした手順が適切に運用されていることを確認している。次の①から③は連携していて、毎月の自己点検も最終的には法規制の一部となっている。

①毎月の自己点検

②年２回の本社による検査（検査は社外のシステム監査人に委託）

③年１回の監査法人による内部統制監査（外部監査は公認会計士）

3．維持から、積極的改善へ

現状を維持するためには、被検査対象が規定通りになっているかを確認することで「規定と実態の差異を見つけ出す検査・監査」が短期的には重要な活動となる。

一方、長期的な視点に立って経営環境変化へ適応するには、規定自体に問題があるのではないかと規定を疑う「革新を目的とした検査・監査」が重要となり、「ルール・管理の破壊と創造」が必要になる。

「ルール・管理の破壊と創造」を行なう際には、次のようなことを参考にしている。

①ISO などの最新版　　②経営環境変化　　③社内の経験、外部の経験

4．最新の知識を作り出し・発信する

「ルール・管理の破壊と創造」のためには、特に外部の経験者が持つ知見に期待しており、知見を持つ者のコミュニティが新しい知識を作り出すと考えている。また、知見を高めるためには「現地・現物・現認」の考えが重要となる。

SAAJ 中部では、こうしたことを目的に海外視察を通じて国際交流を進めている。

◇講演Ⅴ

報告者（会員 No. 1766　長谷部 久夫）

【講演テーマ】

『金融機関におけるシステムリスク管理の取組について
－経営の関与とシステム監査の活性化－』

【講師】

日本システム監査人協会　北信越支部　長谷部 久夫

【講演内容】

金融機関の事業ではＩＴへの依存度が益々高まり、ＩＴ利用の高度化によってシステムリスクは多様化し、業務停止、訴訟、事業破綻等のリスクへと連鎖するコアリスクになっている。これに伴い、ＩＴのコントロール構築、及び当該コントロールが効果的かの第三者検証である「システム監査」は重要性を増している。

本講演では、報告者が関与したシステムリスク管理の取組をご紹介し、リスク管理態勢の要となる経営陣の関与とシステム監査について発表した。

１．銀行システムの概要（位置づけ）

金融機関には、社会的な責任を基軸とする経営理念のもと、新たな経営戦略を展開し、かつ信頼できる金融サービスを提供することが求められている。情報システムは、そのための中核的な手段であり、ＩＴ戦略自体が経営戦略と一体となっている。

２．システムリスク管理態勢

経営陣は、①方針の策定、②内部規程・組織体制の整備、③評価・改善態勢整備に大きな役割を果たす。リスク情報をリスク管理統括部署に集約するとともに、部長会において情報共有し、組織横断的に連携し経営陣を支援する体制としている。内部監査部署はリスク管理の有効性を検証し経営へ報告している。

３．システムリスク管理の現状

（１）定期的なリスク評価（ＰＤＣＡサイクル）

外部環境の変化を定義したうえで、①リスクアセスメント（リスク洗い出し→リスク評価→改善計画の策定）、②改善プログラムの決定、③モニタリング・リスク把握のＰＤＣＡサイクルを回している。

（２）情報セキュリティ管理

物理的セキュリティ、および論理的セキュリティに加え、開発と運用の相互牽制、セキュリティ教育、および性悪説を前提とする権限の見直し等を実施し、組織・プロセス面の強化を図っている。

（３）システム企画・開発管理等

経営陣及びシステムリスク管理部署は、さまざまな開発局面において開発プロジェクトに関与する。内部監査部署はそれらの関与状況を含め、適時に開発プロジェクト監査を実施している。

（４）コンティンジェンシープラン

障害発生の初期対応、暫定対応、および復旧対応の各フェースにおける経営陣による重要な意思決定及び指示事項を緊急時対応計画に定め、当該計画の実効性を確保するための訓練を実施している。

（５）外部委託先管理

外部委託契約締結にあたり、委託先と役割分担・責任範囲を決め、ＳＬＡ（Service Level Agreement）でサービス水準を明定。セキュリティ管理要件等に基づき継続的に運用状況をモニタリングしている。

４．まとめ

経営陣、および内部監査部署が関与する態勢でリスク管理のＰＤＣＡサイクルを実践することにより、リスク抑制の実効性は着実に向上しつつある。今後もリスク管理の取組を継続的に実施していきたい。

◇西日本支部合同研究会を振り返って

報告者（会員 No.1281　宮本 茂明）

［合同研究会］

今回で 11 回目となる西日本支部研究会を関係者のご協力のもと金沢で開催することができました。

テーマについては「システム監査の普及促進」に設定し、様々な角度からご講演いただきました。

参加者それぞれが、テーマについて考え、気づきを得るよい機会になったと思います。

- 力強いシステム監査の実現に向けてどう取り組むべきか
- システム監査の価値についてどう社会、コミュニティ、個人のニーズに応えていくか
- 「IT 事業者評価制度」導入の政策提言をどうシステム監査に活かしていけるか
- システム監査とシステム検査をどう活用していくか
- システムリスク管理のためには、どう経営の関与とシステム監査の活性化を図っていくか

講演いただいた方々に、深く感謝いたします。

［懇親会］

研究会終了後、会場近くの「座いっく」にて、22 名の参加で懇親会を開催しました.

全員の自己紹介とともに参加者が熱く語り合う場になりました。今回の研究会・懇親会を通して参加者の皆様に有益な情報提供・情報交換の場になったのではないかと思います。

［観光］

懇親会終了後、ちょうど金沢城・兼六園ライトアップ～秋の段～が開催されていて、ご希望のみなさんと兼六園、ひがし茶屋街に分かれライトアップされた金沢を散策しました。

また翌日観光として、ひがし茶屋街～金沢城公園～尾山神社～武家屋敷をご案内しました。金沢は 11 月に入り天候の悪い日が続いていたのですが，合同研究会が開催されて土日は、天候に恵まれ幸いでした。

［ご協力お礼］

講演者の皆様、西日本各支部の合同研究会準備にご協力いただいた皆様、合同研究会の進行・運営にあたりご協力いただいた皆様ありがとうございました。

北信越支部も今年で支部開設 10 年を迎えることができました。今後も継続し皆様と情報交流を進めていきたいと思いますので，よろしくお願いいたします。

以上

2013.12 投稿

セミナー開催報告【近畿支部主催　システム監査体験セミナー（実践編）開催結果について】

会員番号 1345 広瀬 克之（近畿支部）

近畿支部では、2013 年 9 月 21 日(土)、22 日（日）大阪産業創造館を会場として、システム監査体験セミナー（実践編）を開催しました。

1 日目は 10 時から 18 時 30 分、2 日目は 10 時から 17 時 00 分までの 2 日間コースで実施しました。建築会社を事例企業として、システム監査のケーススタディを主とした内容で、4 名の方にご参加いただきました。最少催行人数 8 名で案内していましたが、当協会の使命およびセミナーの継続性確保の観点で、開催決定といたしました。

●講義 ＆ 経営者インタビュー

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、「システム監査実施手順・手法」の講義を行いました。

その後、本日のケーススタディで学習する内容を監査手順に従って説明し、受講者はチーム作業を開始し、経営者インタビューの準備に入りました。

●予備調査 ＆ 監査個別計画作成

1 日目の午後は、経営者インタビューを行い、その結果を受けて予備調査で使用する質問項目検討・予備調査・まとめ・調査報告を体験いただきました。

1 日目の最後は、2 日目で実施する本調査の準備として、予備調査で得た情報を参考に、本調査でインタビューする項目を含めた監査個別計画作成を行いました。

●本調査 ＆ 監査報告

2 日目は、本セミナーのメインとなる本調査を実施しました。受講者は準備した質問項目に従って、対象会社の管理職・一般職、および事例企業のシステムアウトソーシング先企業の管理職・一般職にインタビューしました。短い時間の中で簡潔・的確なインタビューを実施されていました。

続いて、本調査のまとめから報告書作成まで実施いただきました。報告書作成は、どのような事実について指摘をするか、その分類・指摘内容等、議論を重ね適切な内容にまとめていただきました。

最終的には、今回の監査依頼者である事例企業の経営者を含めた被監査部門への監査報告会を行いました。被監査部門からの質問に対して、これまでの議論を重ねた内容を背景に適切な回答で対応されていました。最後に、今回の体験セミナーで事例企業の問題をどのように分析していくのがよいかの、考え方の例を紹介し、

一連のケーススタディの終了となりました。

●監査体験の感想

受講された三人の受講者から感想文を頂戴しました。

私はシステム監査技術者の資格を取得したものの、監査の経験は全くありませんでした。実際のシステム監査業務が自分のイメージどおりの物か確かめたい、という動機が本セミナーへの参加のきっかけとなりました。

参加して一番感じたことは、チームで作業する事の難しさです。資料の読込みや被監査部門へのインタビューの過程で色々な細かいリスク事項はチーム内で浮かんで来るのですが、メンバー同士で興味分野が発散する傾向があり、意見の集約に難航する場面がありました。また、監査手続を進めるに従って新たなリスクの発見もあり、最終的な監査報告書は、当初の監査計画書の監査項目から外れた指摘事項を多く含む物となってしまいました。

本セミナーでは、このようなシステム監査業務の実践的な難しさについて気付き得たことが、何よりも成果であったように思います。　　五野　友裕

最初の感想としては、1組だけだったので、驚きました。セミナー参加人員より、講師の数
が多いセミナーは珍しいと思います。日頃システム監査を実際に行うことはないですが、
今回のセミナーは実践力がついた気がします。同じ組の松井さんの的確なアドバイスもあり、有意義なセミナーでした。ただ、4 人参加でしたので、8 人くらいいれば、もっと他の人の考え方を参考にできたと思いますので、不満としては、人数が少なかったことです。
協会へのお願いとしましては、やはり、システム監査の法制化を目指していただいて、公認システム監査人として報酬を得る機会を増やしていただきたいと思います。そうなれば、セミナーの参加者も自然と増えると思います。　　村阪　浩司

・今回の会社の要望が「ＩＳＯ系以外の観点によるシステム監査の実践的演習の受講」だったため、その内容に違わぬ貴重な機会となりました。

・ＩＳＯ基準の枠外のところ（いわゆる非機能要件や、サービスマネジメントの有効性測定等）で、どういう取っ掛かりから着手するかの悪戦苦闘する過程を事前に実感できたことが大きな収穫でした。実際のＩＳＯ系監査よりは会社法系・業務監査系の色合いが近い印象を受けました。

・実例に即している部分は説得性があり、確かにメインフレーム系という古びた技術でありますが、講師の方

からご指摘があったように「ブラックボックス化した最新技術と同等に考えてみる」という視点にははっとさせられました。貴重な教材だと思います。あとはマニュアル共々、ＩＰＡさんの最新知見なども加味したアップデートを期待します。

・参加者が多い方が、他チームとの比較という点でより理解が深まった気がします。もっとも今回も、人数以外の要素では格安な料金設定なのに高品質の演習だと感じました。

・ＭＥＴＩやＩＰＡ、その他他のプライマリベンダー等の協力を得た開催回数の積極増を期待します。また、ＩＳＭＳやＩＳＯ２０００との関係をすっきり説明頂くとなおありがたいです。（今回、ＩＳＯ１９０１１の上に重ねて、さらに赤本やシステム監査基準の知識素養が必須なのか、どこまで重なる要素があるのかも関心事でした）　　石崎　大介

今回受講されたみなさんは、将来も見据えて何らかの形で監査業務に関与されておられるわけですが、今回の学習を通じて、さらに、システム監査に必要な手順・インタビュー方法の気付きや再確認につなげていただけたと思います。

以　上

2013.12 投稿

セミナー開催報告【 近畿支部主催 「事例に学ぶシステム監査の基本と応用」開催結果について 】

会員番号 1710 小河裕一 （近畿支部セミナーグループ）

近畿支部では、2013年11月16日（土）13時から常翔学園大阪センターにて「事例に学ぶシステム監査の基本と応用」と題してセミナーを開催いたしました。

総勢12名の受講者を迎えて、システム監査の経験に長けた近畿支部スタッフ4名が、実際の業務を通じての経験やWGでの研究を通して得られた情報に関して1人45分を持ち時間として講演を行いました。

●各事例・講義について

近畿支部が開催しているセミナーの中で唯一「座学のみ」のセミナーですが、「現場に近い」講義内容のため、参加された受講者の皆様も興味を持って聴講しておられたようです。

1．内部監査よもやま話（講師：是松徹）

長年、講師が業務で担当している「内部監査」において、業務を通じて感じている課題とその対応策例をいくつかの具体例を交えながら紹介しました。監査として要求される事柄と実態とのギャップ、それを埋めるための案など参考にして頂けたと思います。

2．外部監査としてのシステム監査事例（講師：植垣雅則）

委託されて実施する内部監査の事例や金融機関への監査の実態をご自身の経験を交えながら紹介しました。

いかに「外部監査を有効に利用してもらうか」等、外部の力をいかに使うか及び監査・審査への対応実態を参考にして頂けたと思います。

3．個人情報保護マネジメントシステムとISOマネジメントシステム　―文書と記録の管理を主体として―

（講師：吉谷尚雄）

ISOの認証審査員の経験を通しての、最近の ISO 動向と ISO 要求規格に対して「有効な」対応方法を紹介しました。「共通テキスト」としてまとめられる等、2013 年以降のISO改版のポイントや規程に準拠して活動する上での「文書と記録の残し方」、システム監査と「システムの監査」の違いなど盛りだくさんな内容で興味をもって聞いて頂けたと思います。

4. システム監査のBCP監査ポイントについて（講師：荒町弘）

BCPの中でも「大災害発生時」に関して、東日本大震災における自治体の動きを中心にした事例と、今後の復旧手法やそのシステムに対する監査の事例案を研究成果も交えて紹介しました。

●受講者の皆様からの声

受講者の皆様からは以下のような声をいただきました。評価頂いた意見として、次のようなものがありました。

・実体験に基づいたお話で、具体的事例も多くわかりやすかった。
・現場におけるシステム監査の例が参考になった。（悪い例が役に立った）
・「外部監査を活用する」ということをもっと取り入れていきたいと感じました。（活用のポイントを踏まえ）
・文書化に関する合理的な考え方（ムダなものは作らない）が大変勉強になりました。
・BCPだけでなく日常トラブルや不測の事態に対応していくための事前チェックや自主監査をどう進めるべきかを考えさせる内容で刺激を受けました。

改善に向けた提言として、次のようなものがありました。

・ISO，MSS共通テキスト等の全体フレームや位置付けについて冒頭にある程度説明があればその後の解説が理解しやすかったと思う。

今後もさまざまなテーマを選定し、スタッフの経験を交えて紹介していくセミナーが開催できればと考えております。

以上

2013.12 投稿

支部活動　【　システム監査の法制化等のロビー活動報告（2013 年度）　】

会員番号　1566　田淵 隆明 （近畿支部・システム監査法制化プロジェクト主査）

1. 新機軸

システム監査法制化研究プロジェクトは、当協会・近畿支部における公式活動の一つです。2010年度から数人のメンバによって相互研鑽を続け、いくつかの研究論文や講演等の成果を上げて来ました。ところが活動を続けるうちに、従来型の「論文やコラム執筆・講演により広く社会に訴える」という手法のみでは、システム監査の法制化や普及促進には限界があるのではないかという疑念が、徐々に大きくなってきました。

そこで2012年度あたりから、業界団体や政治家に直接接触し「システム監査とは何か？」の啓蒙から始まり、国策としての必要性をアピールするといった、いわゆる「ロビー活動」にまで行動範囲を広げてきています。2012年6月の衆議院公聴会の席上では、冒頭でシステム監査の法制化の必要性について言及させて頂き、この模様はテレビ中継もされました。

また最近では「システム監査人のみならず、IT技術者全体を元気にする！」をスローガンに、新しいIT事業者評価制度の創設等、システム監査の周辺の政策提言にまで研究対象を拡大中です。今回は2013年度における我々の活動実績の概要を報告させて頂きます。

2. 主な請願内容

システム監査やITに関連の深いもののみを記載します。なお**太字下線**の項目は、当プロジェクトにおいて、当協会での研究論文やコラム執筆、講演といった具体的な成果物があるものです。他の項目については目下、研究の深耕を進めています。

(1)システム監査の法的義務化、会社法での「システム監査人」の選任義務化

すでに米国・韓国・台湾では、重要な公共システム等については、システム監査の実施が法的に義務付けられている。安全性・信頼性・効率性の担保のためには、第三者によるチェックの制度化が不可欠である。

(2)新しいIT事業者評価制度の創設

SI（システムインテグレータ）やSO（同オペレータ）の認定・登録制度が徐々に縮小されてきた。建設業における「経営事項審査制度」のような客観的なIT事業者評価制度があれば、システム監査の実施に際しても十二分に役立つ。

(3)企業経理における研究開発費の資産計上の復活

米国IT企業はイスラエル等、世界各国の技術力に注目しM&Aも進んでおり、スルーされるようでは技術立国の名が廃る。わが国の国際競争力倍返しのため、研究開発に意欲的な企業を後押しする財務・税制上の優遇制度の検討が急務である。

(4)ソフトウェア(コンピュータプログラム)に対する製造物責任法(PL法)の適用

インターネットの普及、クラウド化、コモデティ化等により、ITサービスはグローバル、ボーダーレスになってきた。ITの品質に関する規制基準のハードルを上げることで、他国を凌駕する技術力強化を促し、海外需要を取り込む効果が見込める。

(5)技術競争力強化やサイバー犯罪対策を考慮した電力エネルギー改革

安全な新エネルギーの普及や省エネ(SiCデバイス等)、蓄電技術の強化をめざすべきである。関連するデバイスや装置、ITに携わる技術者等の雇用創出にもつながる。また発送電分離だけではなく、送配電分離についても議論が必要である。

(5)データセンター(DC)等での電気通信主任技術者の配置義務の強化

(6)原発・食品衛生・ISO等、マネジメント系審査制度の「推進」と「審査」の組織の完全分離

3. 主な活動実績

先に述べたように、政策実現のためには不特定多数だけではなく、関連するキーパースンにピンポイントで訴えていくことも、極めて重要であると考えています。なお相手の団体や個人に迷惑がかかる恐れがあるため、名称・時期の記載については特定できないような表現にとどめています。

(1)議員との懇談

「3月下旬:某国会議員(元大臣)」

「9月下旬:某国会議員」

「9月中旬、9月下旬:某国会議員」

「5月上旬、9月中旬、11月上旬:某世田谷区議会議員」

(2)業界団体での講演・ディスカッション・懇親会等

「1月下旬:秋田市」

「2月上旬:札幌市」

「2月下旬:宮崎市」

「3月上旬:新潟市」

「3月中旬:甲府市」

「6月下旬:水戸市」

「7月上旬:福島県郡山市」

「11月下旬:仙台市」

(3)マスコミ関係者との懇談

「10月中旬:フリージャーナリスト(元某放送局報道局長)」

5. 謝辞

こうしたロビー活動には際立った説得力のある資料が不可欠であり、その作成にはどうしても私一人の知識や時間では限界があります。当プロジェクト副主査の神尾博氏、メンバの中田和男氏、横山雅義氏には、日頃から不足部分を補って余りあるご支援を頂いています。また近畿支部理事の方々も、近畿支部25周年記念行事等、研究成果の発表の機会については、殊の外ご配慮を賜りました。この場を借りて厚くお礼を申し上げます。当PTメンバ一同、2014年度もさらに成果が上がるよう邁進したい。

※注記:本稿の「システム監査の法的義務化」以外の部分については、執筆者個人の意見でありSAAJの公式見解ではありません。

2013.12 投稿

注目情報（2013.11～2013.12）※各サイトのデータやコンテンツは個別に利用条件を確認してください。

■ＩＰＡ（独立行政法人情報処理推進機構）

Microsoft Office 等の脆弱性(CVE-2013-3906)を悪用する国内の組織に対する標的型攻撃を確認
～不審メールへの警戒、緊急対策の実施を～　(2013.11.20)
http://www.ipa.go.jp/security/topics/alert20131120.html

■ＩＰＡ（独立行政法人情報処理推進機構）

Adobe Flash Player の脆弱性対策について(CVE-2013-5331 等)（2013.12.11）
http://www.ipa.go.jp/security/ciadr/vul/20131211-adobeflashplayer.html

■ＩＰＡ（独立行政法人情報処理推進機構）

Microsoft 製品の脆弱性対策について(12 月)（2013.12.11）
http://www.ipa.go.jp/security/ciadr/vul/20131211-ms.html

■ＩＰＡ（独立行政法人情報処理推進機構）

Microsoft Office 等の脆弱性対策について(CVE-2013-3906)（2013.12.12）
http://www.ipa.go.jp/security/ciadr/vul/20131106-ms.html

■ＮＩＳＣ（内閣官房情報セキュリティセンター）

重要インフラ1 0 分野が一堂に会してＩ Ｔ 障害対応のための演習「分野横断的演習 CIIREX 2013(注)」を実施（2013.12.02に報道資料公開）
http://www.nisc.go.jp/active/infra/pdf/ciirex2013_press.pdf
(1) 実施日時・場所：平成25年12月9日（月）12：00～18：30、株式会社三菱総合研究所 会議室
(2) 参加予定機関等：
【重要インフラ事業者】10分野：情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流
【政府機関】重要インフラ所管省庁(金融庁、総務省、厚生労働省、経済産業省、国土交通省)、NISC等
（注）「CIIREX」（シーレックス）は「重要インフラにおける分野横断的演習」の略称。以下の英文の頭文字。
CIIREX：Critical Infrastructure Incident Response Exercise

■警察庁

平成 26 年 4 月のサポート終了後に Windous XP を使用することの危険性 （2013.12.25、報道資料公開）
http://www.npa.go.jp/cyber/kanminboard/siryou/report_xp.pdf
全国自治体のPCの 13.1%が、サポート期間内に後継OSに更新できない可能性が高いことが判明し、情報セキュイティ上の重大な問題であることが改めて認識された。継続して使用すると、コンピュータウイルスや不正アクアセスの攻撃に遭い、PCが乗っ取られ、遠隔で操作される、PC内の情報流出、D－DOS 攻撃の踏み台にされる、パスワードが盗まれインターネットバンキングで不正な送金がされてしまう等々の危険が極めて高くなる。

以上

2013.12 投稿

協会からのおしらせ　【　第 13 期通常総会のご案内　】

日本システム監査人協会(SAAJ)会員各位

■第 13 期通常総会のご案内

日本システム監査人協会の第 13 期通常総会を、下記の通り開催致します。

万障お繰り合わせの上ご出席をお願い申し上げます。

記

1. 日時:　2014 年 2 月 21 日(金)13 時 30 分　～　15 時

2. 場所:　東京都港区芝公園 3 丁目 5 番 8 号 機械振興会館　地下 3 階　研修 1 室

アクセス:http://www.jspmi.or.jp/kaigishitsu/access.html

3. 第 13 期通常総会議事

13:30 開　会

(1) 2013 年度　事業報告の件

(2) 2014 年度　事業計画の件

(3) 2014 年度　予算の件

(4) 理事選任の件

(5) その他

15:00 閉　会

(休　憩)

4. 特別講演及び研究会発表

15:20 開　場

(1) 特別講演

(2) 情報セキュリティ監査研究会発表

(3) 個人情報保護監査研究会発表

17:00 閉　場

5. 懇親会

17:30 開　場

20:00 閉　場

※懇親会場は機械振興会館地下 3 階の別室です。懇親会費は 3,000 円です。

※総会、懇親会の参加申込は 2014 年 1 月中旬より、協会ホームページにて受け付けます。

以上

2013.12 投稿

協会からのお知らせ【2014 年度 公認システム監査人及びシステム監査人補の更新手続きについて】

「2014年度　公認システム監査人及びシステム監査人補の更新手続きについて」が協会のホームページに掲載されています。2014年度に更新が必要な方は、更新手続きをお願いします。
掲載の概略は下記の通りですが、申請書等の資料のダウンロードなどは、ホームページからお願いします。
（http://www.saaj.or.jp/csa/csakoshin.html）

---------- 記 ----------

2013年12月1日
特定非営利活動法人日本システム監査人協会
公認システム監査人認定委員会

2014年度　公認システム監査人及びシステム監査人補の更新手続きについて（1）

特定非営利活動法人日本システム監査人協会（以下、当協会という。）は、公認システム監査人認定制度（2002年2月25日制定）（以下、当制度という。）及び継続教育要項（2004年10月13日制定）に基づき、「公認システム監査人(Certified Systems Auditor：CSA)」及び「システム監査人補(Associate Systems Auditor：ASA)」の認定期限が2013年12月31日（暫定有効期間2014年2月28日）で満了となる認定者について、認定の更新を行います。

更新申請書等の資料の入手方法は、以下のとおりです。

＜資料の入手方法＞
個人情報の取扱いについて、「同意する」を押した後に、以下が表示。

公認システム監査人及びシステム監査人補の更新手続きについて（2）

（1）「認定資格更新申請手続」の　ダウンロード：PDF 形式
（2）更新申請書等様式一式のダウンロード
「認定資格更新申請書」（様式1）：Word 形式
「継続教育実績申告書」（様式2）：Word 形式
（3）「CSA／ASA認定資格者の更新申請時期」
http://www.saaj.or.jp/csa/keizoku.html
（4）「継続教育要項」の参照
http://www.saaj.or.jp/csa/2nen_koushin.html
（5）「公認システム監査人認定制度」のダウンロード：PDF 形式

以上

2013.12 投稿

協会からのおしらせ　【　事務局からのお願い　】

日本システム監査人協会(SAAJ)会員各位

■会費納付のお願い

平素は協会の運営にご協力いただきまして誠にありがとうございます。

2014 年度会費の請求書を送付いたしますので、ご納付の方よろしくお願い致します。

なお、会費の未納が続きますと協会の規定により会員資格を継続できないことになります。協会の趣旨をご理解の上、ご対応よろしくお願い致します。

＜金額＞　2014 年度会費　　￥10,000－　　(年会費は、消費税非課税です。)

＜払込期限＞2014 年 3 月 31 日

＜振込先＞　郵便振替口座:00110-5-352357

加入者名:日本システム監査人協会事務局

銀行振込口座:みずほ銀行八重洲口支店(普通)2258882

口座人名:特定非営利活動法人日本システム監査人協会

トクヒ)ニホンシステムカンサニンキヨウカイ

※銀行振込の際は、≪会員№≫4桁の数字を氏名の前に付けて下さいますようお願い致します。

(会員番号が付けられない場合は、メールまたは FAX で振込内容をお知らせください。)

■ご寄附のお願い

協会では、運営基盤のより一層の改善を図りたく、一口 3,000 円のご寄附をお願い申し上げます。ご寄附は、協会会費に合わせてお振込みいただければ、会費とは別に寄附金の取扱いにさせていただきます。

協会活動の改善のため、何とぞご協力をお願い致します。

＜2014 年度ご寄附(一口)＞￥3,000-　　ご寄附は、何口でも結構でございます。

＜振込先＞　※ご寄附は、協会会費に合わせてお振込みいただければ幸いです。

ご寄附についてのお問合せは、下記宛にご連絡いただきますよう、お願い致します。

協会事務局メール　jimu@saaj.jp　電話　03-3666-6341　FAX 03-3666-6342

※寄附者名簿は、法令に基づき所轄庁の東京都へ報告させていただきます。

※また、御礼のため氏名等を会報等に掲載することがあります。会報掲載を拒否される場合は、事務局宛に事前にお申し出ください。

2013.12 投稿

協会からのおしらせ　【　協会主催イベント・セミナーのご案内　】

■月例研究会（東京）

第189回月例研究会	日時:2014 年 2 月 10 日(月)18:30～20:30　場所:機械振興会館　地下2階ホール	
	テーマ	個人情報保護法改正の方向性
	講師	慶應義塾大学　総合政策学部 教授　博士(法学)　新保　史生　氏
	講演骨子	内閣官房IT総合戦略本部のパーソナルデータに関する検討会において、「パーソナルデータの利活用に関する制度見直し方針」が示された。平成 25 年 6 月に決定された「世界最先端 IT 国家創造宣言」において、 IT・データの利活用がグローバル競争を勝ち抜く鍵であり、その戦略的な利活用により、新たな付加価値を創造するサービスや革新的な新産業・サービスの創出と全産業の成長を促進する社会を実現するものとされ、個人情報及びプライバシーの保護を前提としつつ、パーソナルデータの利活用に必要な制度の見直しを実施することに基づくものである。 平成 26 年 6 月までに、法改正の内容を大綱として取りまとめ、平成 27 年通常国会への個人情報保護法の改正案提出を目指すことが示された。見直し案において示された検討事項として、第三者機関(プライバシー・コミッショナー)の設置、個人が特定される可能性を低減した個人データの個人情報及びプライバシー保護への影響に留意した取扱い、国際的な調和を図るために必要な事項、プライバシー保護等に配慮した情報の利用・流通のために実現すべき事項について解説する。
	お申し込み	別途、HP でご案内します。

■公認システム監査人特別認定講習（東京・大阪）

開催中	公認システム監査人(CSA:Certified Systems Auditor)およびシステム監査人補(ASA:Associate Systems Auditor)の資格制度にもとづく認定条件を得るための講習です。	
	概要	・システム監査技術者試験と関連性のある各種資格の所有者については、特別認定制度に基づく本講習により、CSA・ASA 認定申請に必要な資格要件を満たすことができます。 ・特別認定制度の詳細はHPで公開しています(http://www.saaj.or.jp/csa/shosai.pdf)。
お申し込み		講習開催スケジュールと申し込み先をHPでご案内しています。 (http://www.saaj.or.jp/csa/tokuninannai.html)

■中堅企業向け「６ヶ月で構築するＰＭＳ」セミナー（東京）

申し込み常時受付中	概要	個人情報保護監査研究会著作の規程、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。 詳細をHPでご案内しています。(http://www.saaj.or.jp/shibu/kojin.html)
	基本コース	月 1 回(第 3 水曜日)14 時～17 時(3 時間)×6 ヶ月 ※他に、月 2 回の応用コースなどがあります。
	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 本部会議室(茅場町)
	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)

■システム監査サービス（全国）

申し込み常時受付中	情報システムの健康診断をお受けになりませんか？　実費のみのご負担でお手伝いいたします。	
	概要	・経験豊富な公認システム監査人が、皆様の情報システムの健康状態を診断・評価し、課題解決に向けてのアドバイスをいたします。これまでに多くの監査実績があり、システム監査サービスを受けられた会社等は、その監査結果を有効に活用されています。 ・システム監査の普及・啓発・促進を図る目的で実施しているものです。監査にかかる報酬は無償で、監査の実施に要した実費（通信交通費、調査費用、報告書作成費用等）のみお願いしております。 ・ご相談内容や監査でおうかがいした情報等は守秘します。
お問い合わせ		システム監査事例研究会主査　畠中（Email：PEC01546@nifty.com）

協会からのおしらせ　【　外部のイベント・セミナーのご案内（会報担当収集分）】

■青山学院大学大学院　第 8 回公開シンポジウム

日時、場所	2013 年 12 月 21 日（土）14:00～17:30（開場 13:30） 青山学院大学　青山キャンパス 17 号館　6 階　本多記念国際会議場
テーマ	メディアが問う　わが国の会計および監査の課題
詳細、申し込み先	http://www.aoyama.ac.jp/sp/info/event/2013/01466/

■一般財団法人　日本情報経済社会推進協会（JIPDEC）　第 35 回電子情報利活用セミナー

日時、場所	平成 25 年 1 月 10 日（金）14:00～16:20（受付開始 13:30） 六本木ファーストビル 1 階　JIPDEC 第 1、2、3 会議室
趣旨	経済産業省の平成 26 年度 IT 関連施策について紹介するとともに、データ利活用によるイノベーション創造に向けた経済産業省の取組について紹介する。
講演テーマ及び講師	◆「経済産業省の平成 26 年度 IT 関連施策（仮）」 経済産業省　商務情報政策局　情報政策課長　間宮　淑夫　氏 ◆「データ利活用によるイノベーション創造に向けた経済産業省の取組について」 経済産業省　商務情報政策局　情報経済課長　佐脇　紀代志　氏
詳細、申し込み先	http://www.jipdec.or.jp/dupc/forum/faudi/event/faudi_seminar35.html

以上

2013. 12 投稿

協会からのおしらせ　【　協会行事一覧　】

2013 年	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
9 月	12 日 会計:予算実績中間報告 12 日 事務局:会費未納状況まとめ	7 日 事例研:「課題解決セミナー」 18 日 第 185 回月例研究会 24 日 CSA フォーラム	21-22 日 近畿支部:「システム監査体験セミナー(実践編)」
10 月	10 日 会計:9 月末予算実績対比表の理事会報告	22 日 第 186 回月例研究会	
11 月	14 日 理事会:次期会長選任 14 日 会計:予算申請提出依頼(11/30〆切) 16 日 事務局:2014 年度役員改選準備開始 20 日 事務局:会費未納者除名通知発送 30 日 会計:2014 年度予算申請提出期限	16 日 認定委員会:CSA 面接 18 日 第 187 回月例研究会 20 日 認定委員会:CSA・ASA 更新手続案内〔申請期間 1/1～1/31〕 21 日 CSA フォーラム 28 日 第 188 回月例研究会 28 日 認定委員会:CSA 面接結果通知	16 日 近畿支部:「事例に学ぶシステム監査の基本と応用」 23 日 北信越支部:西日本支部合同研究会 28-29 日 東北支部:支部設立 10 周年記念システム監査実践セミナー
12 月	1日 会計:2014 年度予算案策定 12 日 理事会:2014 年度予算案、会費未納者除名承認 13 日 会計:支部会計報告依頼(1/11〆切) 20 日 会計:2013 年度経費提出期限 26 日 事務局:2014 年度会費請求書・寄附願い発送〔1月1日付〕	7 日 事例研:「課題解決セミナー」 9 日 認定委員会:更新手続きのご案内メール発信 11 日 CSA 認定証発送	6 日 北海道支部:支部総会 14 日 東北支部:支部総会・支部設立 10 周年記念講演会
2014 年	**理事会・事務局・会計**	**認定委員会・部会・研究会**	**支部・特別催事**
1 月	10 日 通常総会開催案内掲示・メール配信 10 日 役員改選公示 11 日 会計:支部会計報告期限 15 日 事務局:総会資料〆切 20 日 会計:2013 年度決算案 25 日 会計:2013 年度会計監査 31 日 償却資産税・消費税申告	認定委員会:CSA・ASA 更新申請受付〔申請期間 1/1～1/31〕 20 日 認定委員会:春期公認システム監査人募集 案内 〔申請期間 2/1～3/31〕 (CSA フォーラム)予定	中部・近畿支部会計監査 17 日 近畿支部:支部総会
2 月	6 日 理事会:通常総会議案承認 **21日 通常総会 (特別講演)** 新役員	認定委員会:CSA・ASA 春期募集(2/1～3/31) 10 日 第 189 回月例研究会	
3 月	1 日 事務局:法務局登記、東京都への事業報告、変更届提出	(CSA フォーラム)予定	
4 月	1 日 認定 NPO 法人申請準備開始	認定委員会:新規 CSA/ASA 書類審査	

※注　定例行事予定の一部は省略。

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 年度の年間テーマは「システム監査の普及促進」、また、11 月号から 1 月号の四半期テーマは「システム監査の未来」でした。次号の会報2月号からテーマが変わります。2014 年度年間テーマは、「○○○のためのシステム監査」、2 月号から 4 月号までの四半期テーマは、「公(おおやけ)のためのシステム監査」です。皆様から様々なご意見ご提案を会報に寄せていただき、会報がシステム監査を活性化する議論の場となれば幸いです。

□■ 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」)

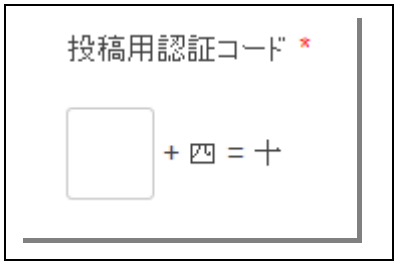
(2013.12.20 追記)

最近、コメントスパマーが多すぎるので、簡単な認証方式を導入しました。

これまでの方式では、スパマの入力を防止することができませんでしたので、毎日、数百件もスパムコメントが投稿されてしまい、削除の作業を必要としていました。そこで、簡単なクイズ形式の認証を導入しました。

2－1. コメント入力時の認証

この方式では、足し算、引き算、掛け算などの計算式が、ランダムに表示されます。



お手数ですが、コメント投稿する場合には、
画面に表示されるガイドにそって、
認証コードを入力してください。
回答の入力には、算用数字を入力してください。

数値を日本語(漢字)で表示しているのは、スパムコメントの送信元である日本語を理解しないスパマーからのコメントを入力できなくするためです。

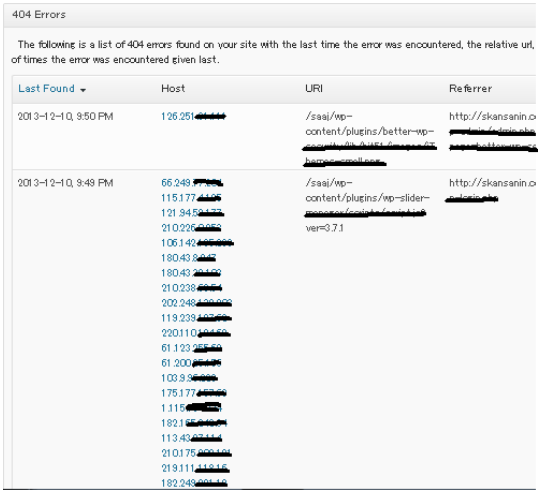
2-2. 会報サイトへの急増アクセスの正体

先月、12月号を公開した後には、次のような集中アクセスが記録されています。

世の中に報道される攻撃は、決して他人のことでないことを紹介するために、公開して紹介します。

次のログファイルのキャプチャ画像を見てください。

(画像1右⇒)



このキャプチャには、攻撃に利用された端末機器のIPアドレスが記録されています。所有者をトレースすると、以前には中国籍のものが圧倒的に多かったのですが、最近では、多国籍に広がっているようです。(一部にマスクをかけています)

1秒間の間に、このように画面に収まりきれないほどの集中的なアクセスがあるのは、組織化された、またはプログラム化された攻撃の現れでしょう。BOTの一例とも推定されます。
私たちもいっそうの自衛に努める必要があるのでしょう。

2-3. 会報サイトへのスパムコメント

2013年の夏も終わるころから、会報サイトへのアクセスが増えてきました。記事が充実して外部からのアクセスが増えてきたのかと喜ぶのも早すぎたようです。会報サイトの記事内容とは無関係な、勝手な記事を投稿する、いわゆるスパムコメントだったのです。たとえば、会報を発行した翌日のアクセスは、増えます。

しかし、全国の1000名会員のアクセス、会員ではないけどシステム監査に関心を持つ一般閲覧者のアクセスより、別の種類のアクセスが圧倒的に多い。その別の種類の人とは、スパムコメントを書き込む人でした。

次のログファイルのキャプチャ画像を見てください。

(画像2右⇒)

会報発行後、ほんの3－4日の経過後にこのような多くのアクセスがあるのは、通常はうれしいことです。でも、その内容が、スパムだとすれば決して穏やかではありません。もう一度、画像1の画面の上部をご覧ください。

スパム(1708)という画像を確認いただけますか。
1708 件ものアクセス＝スパム書き込みがあったことの記録です。

しかし、同時に管理人として、悩みの種は、無用なコメントの削除に費やす時間とエネルギーの浪費です。
国際的な資源管理の観点では、資源の無駄です。これは、アクセスではなく、セキュリティ上の被害です。
多くのサイト運営者が、類似の被害を受けているにも係らず、自分が被害にあっていることを知らないのです。

先に、スパマーによる 1708 件ものアクセスを報告しました。今度は、具体的なコメントの例を紹介しましょう。

前回よりも数値は減りますが、
今日もまたお疲れ様です。
スパマー(217件)。
先日、履歴を消去したばかりなのに。

スパムコメントも英文だけではなく、日本語に翻訳されて表示される場合もあります。
かなり怪しい日本語ですが、翻訳機能の性能はだいぶ向上していることがわかります。

今後も、会報サイト運用に関連する有用な情報をレポートさせていただきます。　（サイト管理人　竹下和孝）

□■ 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）

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/
■会報は会員への連絡事項を含みますので、会員期間中の会員へ自動配布されます。
会員でない方は、購読申請・解除フォームに申請することで送付停止できます。
【送付停止】 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）
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━