特定非営利活動法人
SAAJ 日本システム監査人協会報
2011年3月発行
No 121
No.121（2011年 3月 発行）

第１０期通常総会報告と特別講演

日本システム監査人協会の第１０期通常総会は、平成２３年２月２１日（月）、東京港区の機械振興会館会議室において開催されました。総会に続き、「システムリスク　その計測・管理・監査で求められているもの」について特別講演会が開催されました。講演の要旨は後述します。

■ 第１０期通常総会の概要

通常総会は、斎藤理事の総合司会で開始され、小野副会長を議長に選任して報告および審議が行われました。

総会の議事は、平成２２年度事業報告、同会計報告、平成２３年度事業計画、同年度予算について、鈴木会長、会計担当仲理事から報告、および説明が行われました。ついで、北海道支部、東北支部、北信越支部、中部支部、近畿支部、中四国支部、九州支部の各支部長および代理者から、各支部の活動実績と次年度の計画について補足説明がなされました。今回は定年退職者が増加し、会員の退会者数が増加するなかで、予定されたシステム監査普及事業の多くが、当初予定された参加者を確保できずに規模を縮小して実施されていること。一方で、経費の節減に注力していることが報告されました。新年度の活動計画および予算のなかで、システム監査規程の国際標準化のニーズや個別企業でのオフショア化監査への支援など、効率よくシステム監査の成果を事業経営の改善に結び付けて実証していきたい、との役割を再認識しました。

会員の世代交代や入れ替わりも、システム監査の普及を加速させるために必要です。

「課題解決」というタイトルが人気を博しています。土台としてのシステム監査を、どのように定着させていくか、ここ数年、精一杯に踏ん張っていきたいという思いを強くしました。事前に議案書が公開されていたこともあり、スムーズに報告および議事は進行し、議案は採決され、議案の通り可決されました。

会報冊子版の記事　目次

総会で報告された平成２２年度事業報告、同会計報告、平成２３年度事業計画、同年度予算は、総会資料をご確認ください。総会に引き続き、特別講演会が開催され、今回は「システムリスク　その計測・管理・監査で求められているもの」について、公認システム監査人　中山孝明氏にご講演いただきました。

（ご講演中の中山さん）

（略歴）
金融機関（都市銀行）で勘定系、情報系、国際系システム企画、開発、運用、管理、および銀行子会社で業務監査、役員を歴任。2006～'10 年には金融庁 証券取引等監視委員会で、検査官として金融機関各社の情報システムの信頼性や安全性などに係る管理状況や実施状況等を担当。
現在は、中山システム監査事務所（'10 年 8 月開業～現在）。
公認システム監査人（ＣＳＡ）。日本システム監査人協会理事。

■ 特別講演会の概要

演題　　「システムリスク　その計測・管理・監査で求められているもの」
講演者　公認システム監査人（CSA）　中山孝明氏

講演目次と要旨

目次　１．システムリスクと監査
２．もとめられているもの
３．システムリスクの計測
４．システムリスクの管理
５．システム監査
６．システム監査から見たリスク管理

要旨

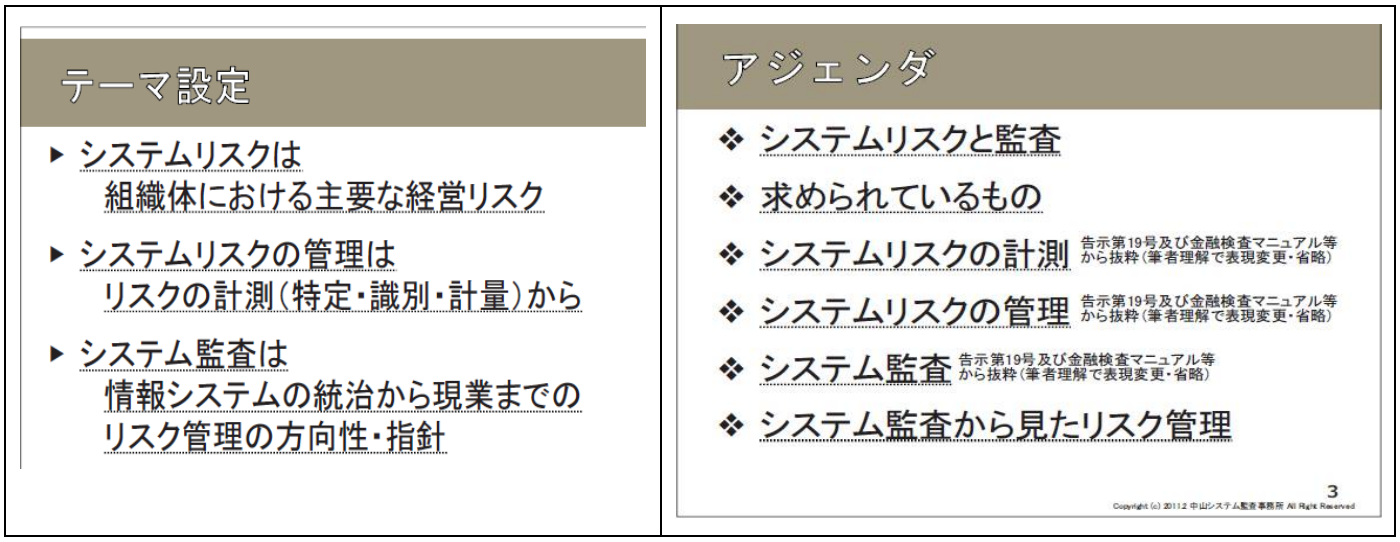
はじめに

システムリスクは対象が広いので、今回、システム監査との関係を考える時に、位置づけをきめることからスタートしたい。組織体における主要な経営リスクをどのように管理するか、というテーマを考えると、それぞれのリスクを計測できるようにすることから始めることが必要になる。つまり、リスクを特定し、識別し、計量化するという手法である。

システム監査を情報システムの統治現業までのリスク管理の方向性・指針を明らかにしていく手法とみると、両者は類似している。

金融機関としての銀行は、銀行法の規定に基づき保有する資産の充実状況が適切であるように、自主的に取り組みをすすめリスクに対応していくわけで、オペレーショナルリスクは、事務リスク、システムリスク、法務リスク、人的リスク、有形資産リスクの5種類に分類される。最近は、外部委託が増えているわけで、規定には明記されていないため、どう考えていくかの課題もあるが、証券、保険、クレジットなど業種によっても事情が違うことを考慮に加えていく必要がある。

基本的な定義をいくつかテキストに抜粋したが、金融庁の告示や金融検査マニュアル等に記載されたとおりであり、システム監査の観点から表現を変更したり、省略したものもあるので、必要な場合には後述する参照資料や URL を検索して、実際に原文を確かめて欲しい。



1．システムリスクと監査

システム監査は、業務の実施体制の整備から実際の運用、管理、評価、内部統制にいたる場面で応用できる。

準拠性や適切性を監査する場合には、方針や体制が適切であるか、故意・悪意の行為はないかなどを予防的発見的な対策の有無、さらに評価・反映の反映状況を評価していく。

2．もとめられているもの

局部的部分的な対応ではなく、全体を見通した上でのリスク対応を行うためには、システム的な対応はますます重要になってくる。リスクを管理していく方法としては、次に示すようにオペレーショナルリスク（5種類）と、リスクが現実となった場合に7種類の損失事象が考えられている。したがって、それらの定義に沿ったシステムリスク管理態勢を整備、運用するよう準備しておくことが金融機関に求められている。

❖求められているもの

オペレーショナル・リスク（5種類）

事務リスク	役職員が正確な事務を怠る、あるいは事故・不正等を起こすことにより金融機関が損失を被るリスクをいう。
システム〃	コンピュータシステムのダウン又は誤作動等、システムの不備等に伴い金融機関が損失を被るリスク、さらにコンピュータが不正に使用されることにより金融機関が損失を被るリスクをいう。
法　務〃	顧客に対する過失による義務違反及び不適切なビジネス・マーケット慣行から生じる損失・損害（監督上の措置並びに和解等により生じる罰金、違約金及び損害賠償金等を含む）など当該金融機関が法務リスクとして定義したもの
人　的〃	人事運営上の不公平・不公正（報酬・手当・解雇等の問題）・差別的行為（セクシュアルハラスメント等）から生じる損失・損害など人的リスクと定義したもの
有形資産〃	災害その他の事象から生じる有形資産の毀損・損害など有形資産リスクと定義したもの

金融検査マニュアルから抜粋（明朝体部分は原文）　10

❖求められているもの

損失事象（7種類）

内部の不正	詐欺若しくは財産の横領又は規制、法令若しくは内規の回避を意図したような行為による損失であって、銀行又はその子会社等の役職員が最低一人は関与するもの（差別行為を除く）
外部からの不正	第三者による、詐欺、財産の横領又は脱法を意図したような行為による損失
労務慣行及び職場の安全	雇用、健康若しくは安全に関する法令若しくは協定に違反した行為、個人傷害に対する支払、労働災害又は差別行為による損失
顧客、商品及び取引慣行	特定の顧客に対する過失による職務上の義務違反（受託者責任、適合性等）又は商品の性質若しくは設計から生じる損失
有形資産に対する損傷	自然災害その他の事象による有形資産の損傷による損失
事業活動の中断及びシステム障害	事業活動の中断又はシステム障害による損失
注文等の執行、送達及びプロセスの管理	取引相手や仕入先との関係から生じる損失又は取引処理若しくはプロセス管理の失敗による損失

告示第19号の別表第二（明朝体部分は原文、表形式は加工）　11

３．システムリスクの計測

システムリスクをどのように評価するかという観点では、測定手法を統一してリスクの大きさを測定する必要が出てくる。金融検査マニュアル等では、統計的な手法を用いる合理的手法で、オペレーショナルリスクの最大損失額を算出してリスクとすることが定められている。（例：VaR: Value at Risk 手法）
他にも、リスク相当額を算出する場合に、内部損失、データ、外部損失データ、シナリオ分析が適切に用いられていること、などの計測ルールが定められている。しかし、このような先進的な計測手法は、実施の運用に３年以上の内部蓄積データの整備を必要とするなど、準備にも多大な工数を要するため敷居も高い。

４．システムリスクの管理

経営陣の責任が問われる部分であるが、システムリスクを管理するためには、管理の態勢整備が必要とされ、システムリスクを把握できる役員の下で、リスク管理のための戦略方針を計画し、実際に態勢整備し、管理運用する。内部統制機能を考慮して運用、監査して状況把握する。管理するということはリスクを削減、低減するということ。そのためにリスクを測定することで、改善効果も把握できる。システムリスク管理の実効性を高めるためには、システムリスクの管理部門を定めて運用上の弱点をはっきりと把握し、速やかに対処できるようにする。

５．システム監査

システム監査を実施する場合に大切なことは、リスクの計量手法と戦略目標、業務規模・特性およびリスクとの整合性が取れていることであり、実際に実施することは結構厳しい。採用するリスク計量手法も、限界や弱点を考慮した上で適切に運営することが求められるわけです。この計量手法の検証方法には特徴がある。

経営者がシステムリスクの大きさを判断できるように計量しているわけで、その計量の方法、計量する対象や漏れが無いかなど、オペレーショナルリスクを適切に把握しているかがポイントとなる。測定することが目的ではなく、リスクを把握し削減するための計量であることを忘れてはならない。

❖システム監査

①計量手法の検証1/4

- ✓ オペレーショナル・リスク計量手法の監査を網羅的にカバーする監査プログラムが整備されていること。
- ✓ 以下の項目について、内部監査が行われていること。
  - リスク計量手法と、戦略目標、業務規模・特性及びリスク・プロファイルとの整合性
  - リスク計量手法の特性（限界及び弱点）を考慮した運営の適切性

36

①計量手法の検証2/4

- リスク計量手法に関する記録の適切な文書化と遅滞のない更新
- オペレーショナル・リスクの総合的な管理プロセスにおける変更内容の計量手法への適切な反映
- リスク計量手法によって捉えられる計量対象範囲の妥当性
- 経営陣向けの情報システムに遺漏がないこと

①計量手法の検証3/4

- ✓ 内部監査部門は、計量手法の理論的及び実証的な妥当性検証を行っていること。
- ✓ 外部損失データの使用条件・方法、それらの決定手続が定期的に検証されていること。
- ✓ シナリオ分析について、実際の損失との比較による検証が適切に行われていること。
- ✓ 内部損失データ・外部損失データの使用方法、業務環境及び内部統制要因の反映方法の適切性が検証されていること。

38

①計量手法の検証4/4

- ✓ リスク計量手法の開発から独立し十分な能力のある者により、開発時点及びその後定期的に、リスク計量手法、前提条件等の妥当性について検証しているか。
- ✓ 外部業者が開発したリスク計量モデルに関してブラックボックスの部分はないか。ブラックボックスの部分がある場合には、計量モデルの妥当性について検証していること。

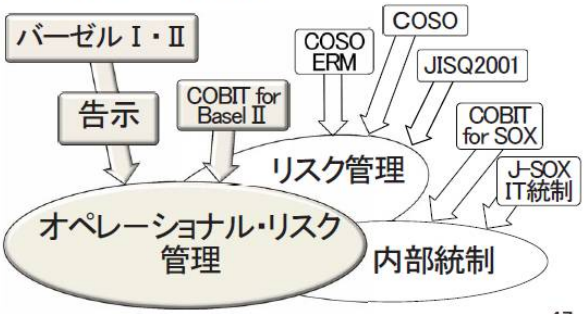
39

このあと、監査の体制、リスクの管理態勢の整備状況に対しての監査など、具体的な監査の実施状況についての評価を加えることになる。

６．システム監査から見たリスク管理

❖システム監査から見たリスク管理

リスク管理への指向



47

❖システム監査から見たリスク管理

オペレーショナル・リスクの計測手法(3種類)

規模やリスク特性等に応じ、最適な手法を選択	
基礎的手法（BIA）	粗利益に 0.15 を乗じた額
粗利益配分手法（TSA）	粗利益の業務区分ごとの掛目の合計
先進的計測手法（AMA）	任意の推計手法に基づいて予想される最大の損失額（スライドNo16参照）

BIA: The Basic Indicator Approach
TSA: The Standardized Approach
AMA: Advanced Measurement Approaches

49

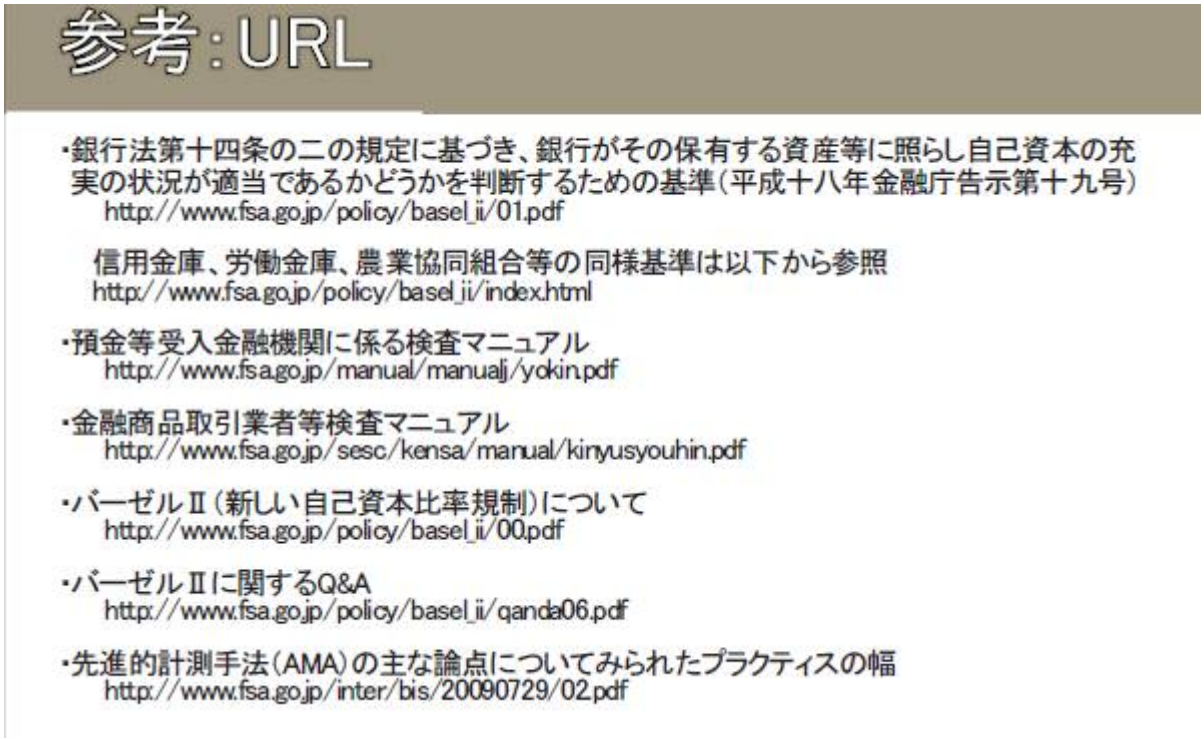
（感想）

金融検査マニュアルに沿ったシステム監査や金融機関むけの内部統制監査に関係する監査人にとっては、リスクの評価手法を振り返る機会だった、と思われます。証券監視委の検査官としての経験を交えた説明は、普段、表舞台に出ることの少ない監査人にとっても勇気付けられる内容でした。金融業や検査官としての実務を経験しないと、探し出すことも使いこなすことも容易ではない銀行協会の資料「銀行別緒比率表」の見方など、興味深く、拝聴しました。

検査にシステム監査人（CSA）の資格やノウハウが大変有用であること、具体的な点検範囲や適否の判断にあたり、システム監査と手法が似ていて、各種の基準・指針・ガイドラインを組み合わせながら、解題を分析、評価していく手法が、多くの場面で応用できることなど、金融機関むけのシステム監査にも自信を持って取り組めます。

なお、講演の中で、繰り返し説明されていましたが、告示の条文や検査マニュアルのチェックリストを引用した部分については、その逐条解説をしたものではないとのことです。

システム監査に関係する部分について、講師の判断で、膨大な量の金融検査マニュアル等のなかから適切と思われる部分を参考例示したものだということでした。正確な内容は資料末尾に紹介したURLから原文をご覧いただきたい、ということでしたので、該当の資料部分を掲載させていただきます。（報告者　竹下和孝）



【 めだかの教室 2010 年3月版 】

掲載月	タイトル・冒頭文の抜粋（投稿者、めだかネーム）
2010.07	【岡三証券知財判決で勝つ】・・・(真却辺利)
2010.07	【ネット選挙活動でのリスク】・・・(歓作人)
2010.08	【日本振興銀行メール削除事件】・・・(左平次)
2010.08	【15万台 Windows2000 サーバの行く末】・・・(唐辛子)
2010.09	【 情報通信技術戦略の抜本的な刷新 】・・・(太郎冠者)
2010.09	【 失敗を通して学んだシステム監査の勘所 】、・・・(おのおのがた)
2010.10	【 日本振興銀行破たん処理へ 】・・・(左平次)
2010.10	【 システムリスクへのアンビバレンスな思い 】・・・(KP)
2010.11	【 タイムスタンプ 】・・(じいじい)
2010.11	【 システム監査 法制化か自己規律か 】・・・(拡張子)
2010.12	【 システム監査の原点を考えよう 】・・・(“こもれび” の監査人)
2010.12	【 システム監査の専門家 】・・・(GAKU)
2010.12	【「グーグル秘録 完全なる破壊」を読む 】・・・(真却辺利)
2011.01	【保証業務に係る公表文書の調査研究と保証型システム監査の一考察（ダイジェスト版）】・・・(格物致知)
2011.01	【介護保険制度において真に見直されるべき制度上の問題】・・・(白雪姫の継母)
2011.01	【監査とコーチング】・・(やじろべえ)
2011.01	【PMS 構築の個人情報管理台帳とリスク分析表を作成目的から考えるとわかりやすくなる】・・・(お山のたぬき)
2011.02	【破産出版社の債権者集会】　・・・(左平次)
2011.03	【百貨店のカードシステム】　・・・(太郎冠者)

【 めだかの教室 2010 年3月版 】は、2010 年7月から 2011 年3月までの投稿を一覧にしたものです。
（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。 ）

めだか【岡三証券知財判決で勝つ】

201007 投稿

日本経済新聞6月11日付朝刊によれば、岡三証券グループが法人税をめぐって国（税務当局）と争っていた知財裁判で勝訴した、という。この14行の記事だけでは詳しいことがわからず、ネットで探したHP「知財情報局」によれば、次のようである。

本件は、2003年、岡三証券が業務用システムソフトの開発・運用を委託していた岡三証券情報システムから、同ソフト・関連を約30億円の著作権料を支払って取得し、アウトソーシング先の日本ユニシスに約35億円で譲渡したことに関し、税務当局が、岡三証券から同情報システムへの支払いは寄付金に当たるとし、岡三証券に約10億円の過小加算税を課し、岡三証券が課税取消しを求めていたものである。

税務当局の主張は、岡三証券が、同情報サービスにSE費用として24年間で約33億円近くを支払っていたことなどから、両社間には著作権譲渡に関する黙示の合意があり、著作権は岡三証券側にあったから、新たな著作権の支払い（経費計上）は認められず、子会社への寄付金に当たる、というのである。

著作権に関する「黙示の合意」など、そう簡単にあるわけはないが、1審の東京地裁は税務当局のいい分を認めたため、岡三証券が知財高裁に控訴していた。

知財高裁の塚原朋一裁判長は

「ソフトの著作権は原始的に開発者に帰属し、開発費用を負担した岡三証券に黙示的に譲渡されていない、ソフト開発費を出した者は、創作行為をしたいなくても当然に著作権を持つという税務当局の主張は著作権法の不適切な理解を前提としており、失当である」とし、岡三証券の勝ちとしたものである。

大昔はいざしらず、現在のソフト制作に関する著作権の扱いについては、知財高裁のいう通りであり、岡三証券は10億円の追加課税を逃れ、過年度支払い分の計18億円の法人税の修正を2010年第一四半期に計上するそうである。

残る問題もある。

岡三証券は30億円で買って35億円で売った、差額の5億円は売買手数料として、妥当であるか。

著作権を持っている岡三証券情報サービスは日本ユニシスに直接売ることもできたはずで、差額が上乗せされることを承知で、日本ユニシスは買ったのか。

ソフト制作者は、開発費を負担してもらいながら制作したソフトの著作権を持っているとしても、著作権の行使として、このソフトをだれにでも無条件で譲渡できるか。

単純な法解釈としては、できるはずであるが、開発費用を出した方の感情論としては、自由な契約の取決めとして、「第3者に譲渡する時は、開発費用負担者側の同意を得ること」くらいの条件は付したいであろう。

その「同意」を得る時、ある程度の反対給付を期待することもできる。

上の5億円は、この‘同意料’とすれば、まあまあ妥当なところか。

5億円は雑益などには計上しなければならないから、課税対象としての争いはない。　　（真却辺利）

（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。　）

めだか【ネット選挙活動でのリスク】

201007 投稿

内閣の顔ぶれが変わり、参議院議員改選に向け活発な取り組みが行われています。この選挙に向けて「ネット選挙」「選挙活動での IT 活用」が検討されました。その新たなリスクへの対応は、今回は見送りです。

投票者から見たネット選挙は、選挙日当日に都合が悪い場合の不在者投票や、不自由で投票所まで出かけられない場合に遠隔投票するなど、利便性は大きい。また若者の投票率アップにどこまで関心を集めるか期待されます。また、裁判でも課題となっている非居住者や在留外国人の選挙権についても整理する機会です。論点は、「本人確認」の方法、「なりすまし」「多重投票」など、セキュリティ上の論点をいかに防ぐか。

候補者側からみるネット選挙は、選挙活動にどこまで活用できるか、という課題でしょう。特に、米オバマ大統領が活用して成功した選挙資金の募金活動。企業団体からの募金活動を禁止する動きは、個人からの資金集めへの切り替えを意味するのでしょう。あらゆる活動に資金は必要で、選挙や政治には、大きな資金が必要となる。「政治と金」は切り離せないとすれば、どこまで適正に手続できるかという課題にこたえる解決策とクリーンな選挙運動（少なくとも、このような募金システムは追跡調査が可能です、いや可能なように設計、構築され、運用される必要があります））

しかし、twitter を利用した「成りすまし」や「悪意のあるサイトへの誘導」などの課題があることは、これまでにも報告してきました。twitter 以外にも、利用者が広がっているものとして、

・電子メール （議員候補者本人や事務所による情報発信、講演会ではメーリングリストも活用可能）
・ホームページサイト （議員候補者本人や事務所、支援者による活動報告や所信表明）
・ブログ （議員候補者本人や事務所、支援者による活動報告や所信表明）
・SNS （利用者を限定してソーシャルネットワークサービスを活用した電子掲示板）
・youtube などの動画掲載サイト（候補者本人の活動）
・Ustream などの利用者参加型の動画配信サイト（候補者本人の活動）

などがあり、それぞれに、主催する側、利用する側で注意すべきルールがあります。

ウイルス対策の未整備やライセンス更新切れ、同報メールへの個人的書き込みなど、利用者のエチケットである、最低限のルールを守らない人がいます。操作ミスならともかくとしても、規約やルールを知らないのではないか、と思われる人もいます。そのような中で、クラウドという外部環境はどんどん進化しています。

システム化の計画段階から、事業再構築の戦略企画の段階から、新しい技術やサービスをどのように取り込んでいくのか。多くのサービス利用者や参加者が、安全に気持ちよく利用できるように、ビジネスの仕組みや IT 活用の基本について、今一度、学ぶ必要性を感じています。（技術環境も大分変わっていますので、基本は知っているといわずに、その基本が変化しているのです。）

実は、その変化の場所に、セキュリティ上のリスクが現実に広がろうとしています。セキュリティ事故や事件が起こる前に、システム監査スキルを活用した計画、設計、構築を進めていくことが、安心安全な社会を維持するための予防手段の一つなのですが、まだまだ浸透が足りない。システム監査が企業のシステム全体の有効性を高める効率的な手段の一つであり、セキュリティの課題を解決する手段でもあることを、もっと知らせて行く必要があります。業績向上を実現するまで実践して、成果を確認できるようにしましょう。　　（歓作人）

（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。　）

めだか【日本振興銀行メール削除事件】　　201008 投稿

同行に関連する記事が、新聞、週刊誌にあふれている。問題は多そうであるが、金融庁の検査を忌避する手段として、銀行内メールの削除が報じられている。日本で電子メールが使われ始めた数年間は、「電子メールは改変できる、電子メールに刑事、民事上の証拠能力ありや」が議論された。

数年前、改変された電子メールにだまされた国会議員がおり、それをかばった政党の代表が辞任した事件もあった。改変された電子メールのコピーをみれば、いかにも怪しく、あるいはITに詳しくない国会議員は、多忙ではあってもIT専門家の助言を求めれば、破局には至らなかったであろう。
もっとも、当時、IT専門家でなくとも、「あれは怪しい」といっている人はいたようであるが。

今、電子メールは改変されている形跡がなければ、立派な証拠となる。
で、日本振興銀行の行内メール削除事件である。
当初の新聞報道では、検査妨害のため、多くのメールが、個々の端末からではなく、メールを制御しているサーバから削除されているといわれていた。銀行全体で故意に削除しようとすれば、そうなるであろう。

しかし、検査当局が、多くのメールが削除されていると見た根拠は何であったのだろうか。
検査対象期間の疑わしい取引の担当者のメールを時間順に並べて、通常の時間帯にあるべきメールが欠けている、などと判断したのであろうか。

しかし、こんな素朴な方法では、いかに優秀な検査官でもなかなか見つけることは難しい。
メールは、銀行から発信されても、取引先には受信されている。検査当局は、取引先への強制立ち入りはできなくても、協力要請はできよう。受信先を調べれば、発信元で削除されたメールは復元できる。
こういう方法で削除されたメールが指摘されたのか。
しかし、こういう検査工程は、新聞報道からはうかがえなかった。
その後、一部の新聞報道では、
「サーバからは、削除されていたが、取引担当者の端末の消し忘れていたフォルダから見つけた」とあった。
特定取引先の重要なメールは、一般の送受信トレイに混ぜておかず、何らかの特定フォルダにまとめておくことは、普通のビジネスマンならやるであろう。
しかし、大量のメール削除があることを解決した話としては、ややでき過ぎている。
つまり、検査当局は、大量に削除されたメールがあることを想定して、探しているように見えるのである。
一部の週刊誌の記事では、銀行の元職員からの内部告発があり、不正な取引、それを記したメールの削除などが通報されていた、という。
これなら、わかる。
法律違反の疑いのある取引をしていれば、まともに検査を受けるのは辛い。どうにかごまかそうとして、検査妨害に走れば、その方がもっと辛いことはわかっているはずであるが、「わかっちゃいるけど、やめられない」のであろう。
元都市銀行の内部刷新で活躍した人が、日本振興銀行の社長に就任した。
社長だけ代わっても、ここまで傷の深い銀行の再生は可能であろうか。　今後を見守っていきたい。　以上

（左平次）

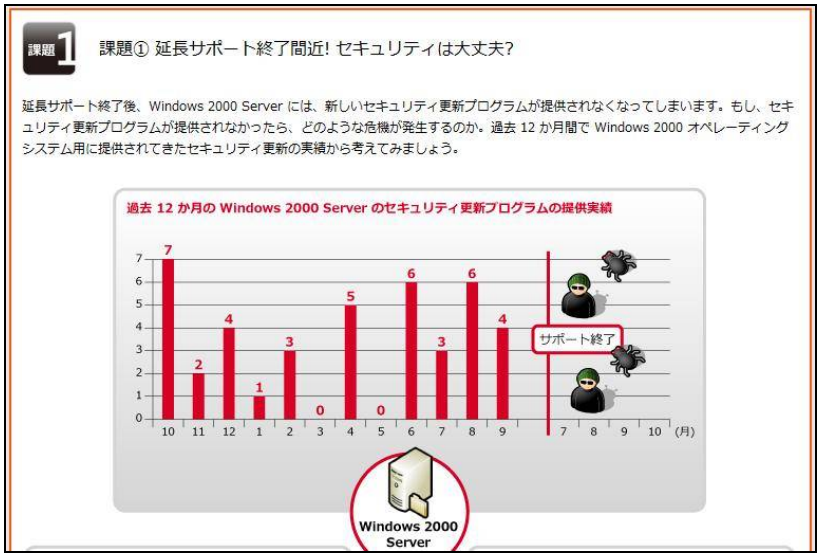
（このコラム文書は、投稿者の個人的な意見表明であり、ＳＡＡＪの見解ではありません。　）

めだか【１５万台Windows2000 サーバの行く末　】

201008 投稿

新聞社の報道によると、米マイクロソフト社がサポートを終了したWindows2000サーバの残存設置数は15万台に上るという。これだけの台数が販売中止後、またサポートの中止後も健在であるということは、優れた品質の成果である、という見方もできよう。

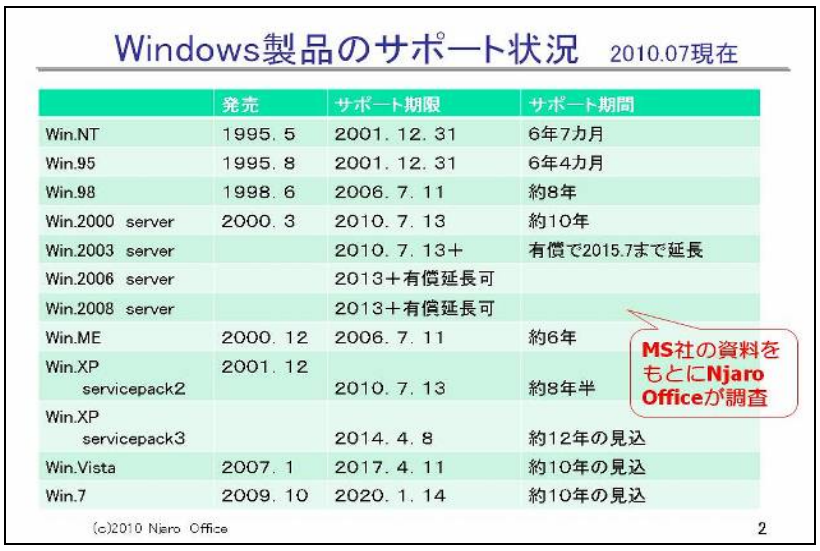
一方で、この1年間の障害発生、とくにセキュリティホールの発見に伴う修正ソフト（パッチ）の提供は次の資料の通り、ほぼ毎月、複数件の発生状況である。



マイクロソフト社の公開資料（左図）によると、Windows2000 で発生したセキュリティホールが発見されて提供されたパッチは、この１年間で４１回。現在稼働しているWindows 製品は、12種類。

（下図。NjaroOffice 資料 2010.7）

修正パッチの適用具合によって、さらに種類は増える。周辺機器を利用するためのドライバーソフトと業務ソフトウェアの組み合わせにより、業務に必要な環境を維持確保することを優先しているが、利用開始して10 年経過し、老朽化は着々と進んでいる。



	発売	サポート期限	サポート期間
Win.NT	1995. 5	2001. 12. 31	6年7カ月
Win.95	1995. 8	2001. 12. 31	6年4カ月
Win.98	1998. 6	2006. 7. 11	約8年
Win.2000 server	2000. 3	2010. 7. 13	約10年
Win.2003 server		2010. 7. 13+	有償で2015.7まで延長
Win.2006 server		2013+有償延長可	
Win.2008 server		2013+有償延長可	
Win.ME	2000. 12	2006. 7. 11	約6年
Win.XP servicepack2	2001. 12	2010. 7. 13	約8年半
Win.XP servicepack3		2014. 4. 8	約12年の見込
Win.Vista	2007. 1	2017. 4. 11	約10年の見込
Win.7	2009. 10	2020. 1. 14	約10年の見込

Windows 製品には、サーバ用、個人用とそれぞれの用途に応じて複数のバージョンが稼働している。企業のシステム管理者は、この数年間、増え続けるOS、ソフト、バージョンの種類と、それらの違いを標的にした攻撃に悩まされてきた。

今後は製造者に対応を任せることも、修復を委託できる業者や技術者を確保することも難しくなる。業務の継続に影響するシステム化の基盤として、どの技術を採用し、いつ変更、切り替えていくかという情報化戦略（経営企画）の監査は、まだまだ不十分。

変更管理どころか現状維持を続けてきて、いつまで維持できるか、秒読みに入っている企業も多いのではないだろうか。有効な対策を行わず先送りして現状維持だと思っていても、周りの環境が変化している。変化に対応していることが現状維持（サービス機能の維持）であって、変更対応できていない状態は陳腐化と言わざるを得ない。

以上（唐辛子）

（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。　）

めだか【情報通信技術戦略の抜本的な刷新】

201009 投稿

政府は5月に「新たな情報通信技術戦略」を発表した。

日本経済新聞8月18日付朝刊に、担当大臣である川端文科相兼内閣府特命担当相のインタビューが載っている。川端担当相の談話では、

「従来は、役所の事務処理の簡便化が主眼でしたが、今回はあくまでも利用者の利便性を追求しました」、

「また、IT戦略本部の下に関連省庁の副大臣級で構成する『企画委員会』を設け、政治主導で検討・実行できる体制を敷くことで、実施状況を厳しくチェックし、役所の壁を超えて横断的な政策をとれるようにしました」

と、ある。

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

ただし、もう少し、一点集中的な設定はできないのであろうか。

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

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

今の中央省庁すべてに関係し、他にも自治体の意見も聞かなければならない。

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

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

一方、漏れ聞くところでは、カルテの電子化は実施が危ぶまれている。

カルテの電子化がなくて、医療情報の共有化ができるであろうか。

カルテの電子化支援も解決すべき課題は多い。

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

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

情報処理技術としては、入力の際の隘路が除かれれば、あとはラクである。

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

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

患者の利便とともに、医療費削減の大きな契機になるに違いない。

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

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

めだか【 失敗を通して学んだシステム監査の勘所 】

201009 投稿

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

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

1. 玉虫色の表現のシステム監査報告書を経営者は期待していない

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

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

2. 記録の提出の要求を、相手に、記録がないことの指摘と思わせてしまった

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

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

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

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

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

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

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

めだか【　日本振興銀行　破たん処理へ　】

201010 投稿

9月10日、日本振興銀行は、1,800億円の債務超過をかかえて破たんした。
預金は定期預金しかないそうであるが、初めてのペイオフも実施される。

社長になったばかりの江上剛氏、本名小畠晴喜氏が頭を下げている映像が痛ましい。
同氏の話では、初めの「中小企業向け銀行」の狙いがそれていっていたというが、
いったん下り坂を転がり始めた組織の建て直しは、難しいのであろう。

逮捕された元会長が起訴されれば、裁判で、問題点が明らかになる。
教訓に富む話があるのではないか。

（左平次）

（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。　）

マンジュシャゲ（曼珠沙華）　　花ことば：悲しき思いで、再会

赤い曼珠沙華と蝶、珍しい白い曼珠沙華の見事な彩りをお伝えします。

埼玉県日高市の巾着田（きんちゃくだ）は、日本有数の曼珠沙華（まんじゅしゃげ）の群生地です。
約 100 万本が高麗川の川辺を真っ赤に染め上げます。周辺にはハイキングコースも整備され、
季節の自然を満喫できます。毎年9月20頃から半月ぐらい、珍しい白い曼珠沙華も含めて
見事な彩りを見せてくれます。
今年は、暑さのために、開花が1週間程度遅れて、花にも厳しい夏だったようです。

（写真提供　榎本　吉伸）

めだか【 システムリスクへのアンビバレンスな思い 】　　201010 投稿

情報システムに関するリスクが、近年急激に増大しているのは間違いない。

ひとつには、情報システムを開発・運用すること自体の難易度があがっていることがその理由だろう。システムの構築目的が、単純なコストカットだけでなく、企業経営そのものに直結するものへと高度化していることや、システムの開発範囲が、単一企業だけでなく、複数主体間をまたがるものへ、さらにはグローバルなものへと拡大していることによって作ること自体が難しくなっている。

また、システム開発手法・環境もここ10年間くらいで大きく変わってきている。ゼロベースのスクラッチ開発ではなく、コンポーネントやパッケージの組み合わせによる、「できるだけ作らない開発」へのシフトによって、開発効率は上がってきているものの、オープンという名のブラックボックス利用を前提としている工法では、完成後の信頼性・安全性の確保はとても難しくなることは言うまでもない。

また、ユーザがシステムに求めるQCDが厳しくなってきていることも大きい。企業が提供しているサービスとシステムとが表裏一体になっている環境では、システムの品質維持は何よりも優先される。また、当然ながら重要なデータを扱うことが増えることによりそれを守ることも必要不可欠な要素となっている。同時に、企業のビジネスモデル変革スピードが加速化することにより、システム開発の工期を短縮するニーズも強くなっている。そして何よりも、右肩下がりの経営環境化では、コスト圧縮を求める経営側の要求は強くなる一方である。

統計をとっているわけではないが、システム故障・障害件数は年々増えていると思う。情報システムを提供するベンダサイドも、利用するユーザサイドも双方疲弊してきているのは間違いない

他方、日本という国は、情報システムに対して、あまりにも高い信頼性・安全性を求めすぎているのではないかという思いにも囚われてしまう。

時刻どおりに動く交通機関、極めて安定的に提供されるガス・水道・電力サービス(そういえば、「停電」って最近いつあっただろうか)。高品質なサービス提供を維持できることは日本の誇るべき長所であるという声を否定する気はないが、数分間遅れた鉄道では延々と謝罪放送を流し続けられ、数時間サービス提供がとまった企業はまるで大きな犯罪を起こしたように報道され、経営陣は謝罪会見を行うという環境。高信頼性を維持するために投入される社会コストを鑑みたとき、「過剰品質」という言葉が頭を過ぎり、このような状況自体がグローバルな視点でみたときの「ガラパゴス」ではないかという不安をどうしても覚えてしまう。

また、個人情報保護が重要な事項であることは間違いないにせよ、情報漏えいへの行き過ぎた恐怖心が、「机にワイヤーで縛り付けられて持ち歩けないノートパソコン」環境を生み、企業経営において極めて重要なはずの情報活用とは真逆の「できるだけ情報は持たないようにすぐに破棄してしまおう」という行動につながっていることはないだろうか。

システム監査とは「客観的なシステムリスクの可視化」だと考えている。

問題は、見えたリスクに対して何を提言していくかということだろう。システム監査人は、ただ「リスクがあるからこれをなくせ」とチェックリストに沿って述べるだけではいけない。先に述べたとおり、リスクを減らすことがコストを増加させ、パフォーマンスを低下させることに確実につながることを理解した上で、対象組織と組織を取り巻く環境を十分に加味した妥当なメッセージを提示しなければならない。

間違っても「角を矯めて牛を殺す」ことにならないように。　　(KP)

（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。　）

めだか【 タイムスタンプ 】

201011 投稿

検察特捜部によるFDの更新日時を改ざんするということが発覚して、検察の威信が地に落ちている。続報によればその他にも証拠の電子情報の改ざんがあったようである。

電子ファイルの更新日時をごまかしての犯罪は昔からやられており目新しいものではない。

この事件の報道を読んで10年以上前に起きたある事件を思い出した。その事件はある会社で賞与計算したファイルが改ざんされ、各従業者の支払額から小額が引かれてある情報システム部員の支払額に加算されるというものであったが、問題となったのはそのファイルの作成処理を行った時間にはその本人は休みをとっており、賞与計算の処理は定められた担当者が正規のプログラムを使用して処理されていた。このためその会社は困って使用していたコンピュータメーカーに調査依頼してきた。

調査結果わかったことは、その情報システム部員はホストコンピュータのシステムデイトを更新して自分で作成したプログラムでそのファイルを更新処理し、またシステムデイトを戻したことがログ解析で判明した。この情報システム部員は、仲間の情報システム部員のレベルが低いのでホストコンピュータのシステムデイトを更新しても他の部員はわからないと思って、この犯行を起こしたということであった。

今回の事件が今までと違うのは犯罪を起こした者が犯罪を隠すために証拠を改ざんしたのでなく、犯罪を取り調べる側が証拠を改ざんしたという点である。

たとえでいえば、試験で受検者が回答を提出した後で試験官が答案を改ざんして合格すべき受検者を不合格にさせるようなものであり、このようなことが起これば検察制度そのものが崩壊することになる。

今回の事件をきっかけに取り締まりの可視化が議論されているが、取り締まりの可視化だけでこのような事件の再発を防止できるとは思えない。取り締まりの可視化によって是正されるのは、行き過ぎた取り締まりの発見であり、証拠偽造の防止には役にたたないものと思われる。

今回の事件の教訓は、検事でも不正をするという前提にたって仕組みを作ることが必要であろうということだと思われる。

警察・検察・裁判所で証拠資料を扱う場合には原本管理の仕組みを作り、担当者から独立した組織で取扱い、担当者が調査する場合はコピーを貸与するとか、資料管理者が立会のうえで調査するなど不正ができにくい仕組みを作ることが必要であると思われる。

検察は今回の事件を、関係者の処分というトカゲのしっぽ切りで終わらせないで、2度と冤罪を発生させないという決心をもって検察捜査の仕組みの改革に取り組んでいただきたいと思う。

システム監査に関わる我々の仲間にはこのような不正をする者はいないと信じたいが、今回の事件を他山の石としてシステム監査で扱う監査証跡など資料の扱いには細心の注意を払っていきたい。

（じいじい）

（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。　）

めだか【 システム監査　法制化か自己規律か　】

201011 投稿

システム監査を法制化（あるいは制度化）すべきではないのか、について当協会でも長い間議論を行ってきています。例えば2008年の協会創立20周年を契機に実施した「システム監査これからの10年」アンケートでも（以下、紙面の都合上原文を簡略化しています）「現在は任意監査であるシステム監査ですが、（中略）システム監査の法制化・制度化は必要だと思いますか」という問いに対し、全体で3分の2の人が必要とする一方、必要とは思わない、との回答は2割となっています。そして「実際に今後法制化が進むと思いますか？」という設問には、ペースはともかく「法制化が進む」、との回答が全体の4分の3に上り、分野としては社会インフラや大企業、財務会計の分野を指摘する声がありました。

これらを踏まえ提言（4）として以下の総括を行っています。

・法制化・制度化についてはすべての業種・業態において一律ではなく、対象範囲を絞っての実施を前提に検討を行うべきである。

・その際、目的と効果を明確にすることが重要である。

・なお、規制緩和の流れに反するのではという見方があることも意識する必要がある。

ここでは最後の「規制緩和の流れに反する」のかどうか、という点を考えてみたいと思います。

このアンケートの別の箇所で、「健全な情報化環境を構築・維持していくために、システム監査の実施は必要だと思いますか？」という設問に対し、7割の人が不可欠、とする一方、残りの3割は実施がベターだが不可欠ではない、と回答しています。つまり実施の不可欠性のポイントは「健全な情報化環境」を保つことはだれのどんな責務なのか、それはどのように実現されるのか、に関わっています。

まず責務の問題ですが、結局それは、情報システムによるサービスの提供を誰から負託されているのか、に依存しています。例えば、社会的なインフラサービス事業は公共性を有しますから、法制上の要請として「健全な情報化環境」を保ったうえでサービス提供の責務があります。あとは代替可能性や競争政策上、どの範囲に例えば「社会的なインフラサービス提供事業者」などとしての認定を行うかにかかってきます。

これに対し他の事業主体は、直接間接の利害関係者（例えば上場企業であれば株主、商品・サービスの提供先等）に対して責務を負っています。いわば、市場規律のもとで、自己の事業継続性に必要な範囲で、「健全な情報化環境」を保てばよいのです。もちろん市場規律上の規制には服さなければなりませんので、財務上の要請に基づく内部統制報告などが必要なことは言うまでもありません。

問題は、各自事業者の裁量に任せて、市場の失敗や社会的被害を引き起こすような分野を事前に予測することができるのか、効果的でコストが小さい形でシステム監査の法制化・制度化をどうすれば設計、実現できるのか、といった点にかかっていると思われます。

システム監査に関わる人々はこういった点に知恵を絞り必要な提言活動を行っていきたいものです。　以上

（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。　）

めだか【　システム監査の原点を考えよう　】

201012 投稿

経済産業省（当時、通商産業省）のシステム監査基準が誕生して、早いもので20数年が経過しました。システム監査基準が制定される少し前、システム監査への関心が高まっていた当時のことを思い出しますと、当時はメインフレームが中心の情報システムでした。その後、パソコンの普及、分散処理、クライアントサーバシステム、インターネット、Webシステムというように情報通信技術が大きく進歩しました。システム監査人として、こうした技術の変化をウォッチし、新しい情報通信技術に対して、どのような監査を実施すればよいのか、苦労していたことを思い出します。

また、阪神淡路大震災によって多くの甚大な被害を受けましたが、これによってシステム監査基準が改訂され災害対策に関する監査項目が強化されました。また、個人情報保護法の制定、情報セキュリティ監査制度の創設、内部統制報告・監査制度のスタートというように社会の関心や制度が大きく変化し、それと相俟ってシステム監査の重要性が増大し、システム監査への期待も高まってきたと思います。

筆者がシステム監査の勉強を始めたころは、セキュリティとは何か、なぜセキュリティが必要なのかを経営者や監査対象部門に説明するところから始めなければなりませんでした。また、個人情報保護の必要性についても、個人情報保護の基本から説明しなければならないような状況でした。つまり、システム監査を行う前の活動に多くの時間を取られていたと思います。

最近では、経営者や監査対象部門などにシステム監査の必要性やセキュリティ、個人情報保護の重要性について説明しなくても済むようになったので、システム監査人にとって、監査をやりやすくなったと感じています。その半面、システム監査とは何か、システム監査の役割はそもそも何かとうことを考えずに、システム管理基準や自社の監査手続書に基づいて監査をしているシステム監査人も増えているような気がします。

システム監査は、もともと内部監査を中心には発展してきたものです。内部監査の役割は、経営改善や業務改善のための指摘や提言を行うことです。システム監査は、情報通信技術を企業等の目標達成に貢献させるための仕組みやプロセスがあるかどうかを点検・評価する役割を担っています。この原点を忘れてしまうと、付加価値のあるシステム監査を実施することができないのではないでしょうか。

情報セキュリティ監査制度は、外部監査を前提に考えられたものです。自組織の情報セキュリティ管理が適切に行われていることを第三者にチェックしてもらう制度なので、どうしても情報セキュリティ管理基準をベースにした準拠性の監査になってしまいます。システム監査として実施する情報セキュリティ監査では、情報通信技術を経営目標の達成に貢献するように活用する上で必要な情報セキュリティが確保されているかどうか、という視点で監査します。ですから、オーバーコントロールがあれば、それを改善するような改善提言も行うわけです。

内部統制報告・監査制度におけるIT統制の評価では、財務報告の信頼性確保に係る部分の有効性だけしか評価あるいは監査しません。企業にとって最も重要である、経営目標（利益目標・販売目標など）を達成するためのIT統制が有効かどうかについては、評価・監査を行いません。経営者や監査対象部門が喜ぶような改善提言、つまり、内部統制報告・監査制度は、営業支援システムが顧客獲得に役立っているか、顧客サービスの向上につながっているか、というような視点での改善提言は行わない制度になっています。今後のシステム監査の発展を考えると、一度、原点に立ち返ってシステム監査を考えることが必要なのではないでしょうか。　　“こもれび”の監査人

（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。　）

めだか【　システム監査の専門家　】

201012 投稿

お読みになった方もおられると思われるが、「システム監査の専門家」ということについて、大変考えさせられる記事を発見した。それは、当方にとって、システム監査の大先輩にあたる方がお書きになられた「専門家の専門性放棄」というタイトルの意見である。お言葉によれば、およそ次の通りである。

日本の社会で大変心配なことが起こっている。それは専門家の専門性放棄である。たとえば、裁判員制度を導入した司法の世界、内部統制の評価を極力企業の自主判断、自己対応そして自己申告の報告に任せようとしている会計監査の世界、更にはスポーツ選手や芸能人を引っ張り出した政治の世界などなど、それぞれ専門性が求められる分野で、専門性の放棄が起きている。そして、情報セキュリティについても、「(担当者が)企業においてセキュリティを推進したいと思っても、トップが考え方を変えない限り何時まで経ってもセキュリティは改善されない」との話があるが、組織の中で、必要なセキュリティレベルを提案し実現するのは、専門家である担当者の責務であり、トップの所為にして専門家としての能力を発揮できていない。経営者を説得できないのは、担当者の専門性の不足または熱意不足ではないか。専門家は専門性を発揮してこそ、専門家なのである・・・。

担当者の一人である当方にとっては、少し辛口の大先輩のコメントであったが、十分に同意できるものであり、またシステム監査の世界は、はたしてどうなのだろうと考えさせられるものとなった。

システム監査基準が制定されてから、早20数年たった現在。そして、いまや経営者自身も、パソコンを操作し、またIT分野の経験があるひともいるという環境にある。しかし、企業の中にあって、もし仮にシステム監査の重要性を説明しシステム監査の普及(もう、「普及」という時代を過ぎているのではないか、そして過ぎていてほしいが)及び充実を果たせていないとすれば、それは、システム監査の専門家としての役割を果たしていないか、もしくは専門性を持っていないかのどちらかということになる。

日本情報処理開発協会が、隔年で「システム監査普及状況調査」を実施している。平成18年の調査結果によれば、システム監査の実施において、最も問題だと思われるのは、「システム監査人が不足している」の回答が最も多く、「トップマネジメントのサポートが得られない」は僅かの回答であった。この調査結果だけで、システム監査の専門家がしっかりと経営者のその重要性を認識させているとはいえないが、少なくとも調査開始(確か平成2年頃)当初よりは、システム監査人等は、経営者のITリスクやコントロールに対する理解や啓発を促す役割を、専門家として担ってきていると考えたい。

冒頭の記事を読んでいて、また、あることを思い出した。当方が、かつて内部監査の世界に初めて足を踏み入れた頃、ある先輩内部監査人に、心構えとして、「マージャンのサンシキ」ならぬ「監査人のサンシキ(＝三識)」を教わった。それは、「知識」「常識」「見識」である。先輩は、これに「胆識」(腹の据わった考えであるという)を加え、「ヨンシキ」だと教えてくれた。システム監査の専門性の発揮も、実はこれに通じるところが多く、とりわけ、トップマネジメントへのアピールする場面についても、ITの技術的領域及びシステム監査技術領域の専門性の発揮のみならず、この「ヨンシキ」を専門家として十分発揮することが重要ではないかと考えるがどうであろうか。

そして、あらためて、日本システム監査人協会の「システム監査人倫理規定」を読み返してみた。そこには、「ヨンシキ」の精神が十分に反映されていると感じた。　　以上(GAKU)

(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。　)

めだか【「グーグル秘録　完全なる破壊」を読む】　　201012 投稿

大部の本であるが、数百人のインタビューによる軽妙な受け答えで構成されており、途中で放り出すことなく読み終えた。

グーグルの2人の若い創業者は、初め、なぜ活字本なのか、ネットに載せればいいではないか、活字本を作ることに協力するのは時間のむだだといって取材に応じなかった、という。
筆者の説得で創業者がインタビューに応じたあとは、同社員100人以上がインタビューに応じているが、1人の副社長だけは最後まで拒否したそうである。拒否の理由は明らかではないが、拒否した人がいるのが面白い。

グーグルの創業者は「学生」と呼ばれたりしているが、正確には「コンピュータ科学のエンジニア」であり、「エンジニア」が作り、大きくした組織がグーグルである。

ある程度社員数が多くなったとき、社内のミーティングで、「自分たちはどうなりたいか」を議論した、とある。
とにかく検索ユーザの利便のために奉仕するという考え方でやってきても、ある程度大きくなって社会的に影響力が出始め、衝突も出てくれば、社員全員が立ち止まり、目指す方向を意思統一する必要が出てきたのであろう。
まとまった結果が「われわれは邪悪にならない」である。

「ユーザ本意をさらに徹底する」など、凡庸ないい方ではなく、「邪悪にならない」という表現は、
評者にいわせれば、エンジニアらしい生真面目さにあふれている。
あるいは、IT業界では、大きくなり過ぎて「邪悪になった」ところがあるのかもしれず、「おれたちは、そうはならない」という決意表明が新鮮にひびくのであろうか。

社員食堂を始めたきっかけは、メンバーが食事に出て、並んだりする時間がもったいないからである、という。経費はすべて会社持ちで、利用者は無料である。一時は100種類のメニューがあったが、経費見直しで50種類になった、著者は「それでも他社より50種類多い」といっている。つまり、他では、まねできないのである。

もちろん大きな主題は、グーグルによって、既存のメディア、というよりそれまでの世の中の多くの部分が変えられたか、にある。

翻訳本の題名は「秘録」とやや古めかしいが、原著の題名は「Googled」である。
少しネットなれした人は、「グーグルで検索する」を、短く「ググる」という。

世の中がどれだけググられたか、どれだけググられていくのか、また、グーグルそのものがどこまで変貌していくのか、だれも簡単に解を提出できない。

多くの本は読み終わった場合、一種のカタルシスがあるが、本書の場合は、上の問いがのしかかってきて、衝撃が残ったままなのである。　　（真却辺利）

（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。）

めだか　　201101投稿

【 保証業務に係る公表文書の調査研究と保証型システム監査の一考察（ダイジェスト版）】

日本システム監査人協会では、長年わが国におけるシステム監査の普及・向上に努力をしてきたが、創立 20 周年を記念して「システム監査のこれからの 10 年」が発表された。ここでは、協会が取り組むべき 10 の提言が公表され、その 5 項目で「保証型監査についての見解の明確化と公表」が公表された。

これを機会に、筆者も「財務情報等に係る保証業務の概念的枠組みに関する意見書（以下、意見書という）」金融庁企業会計審議会（2004 年 11 月 29 日）、IT委員会報告第 5 号「ITに係る保証業務の実務指針（一般指針）」日本公認会計士協会（2009 年 9 月 1 日）等の保証業務に係る公表 20 文書について調査研究し、『保証型システム監査のフレームワーク』について考察した。レポートは A4 で 100 数ページにも及ぶために、本コラムでは、その「ダイジェスト版」として主に結論だけを簡単に紹介したい（以下、レポートより抜粋の上、一部コラム用に変更）。

本考察の目的は、意見書・研究報告書等の保証業務に係る公表文書を十分に研究した上で、保証型システム監査のフレームワークを一つのモデルとして明確にすることである。ご批判を恐れずに申し上げると、保証業務に係るシステム監査について制度として必要な監査基準や監査手続等の基本的要件は、これらの公表文書で十分に議論が尽くされていると考える。従って、本レポートの主題は既に議論されてきた保証型システム監査の要件を一つのフレームワークとしてまとめることである。今後必要なのは、保証型システム監査の豊富な実績の積み重ねとその成果としての社会への普及、浸透であると考える。

本レポートでは「保証型システム監査に係るフレームワーク」について、システム監査で信頼と実績のある経済産業省「システム監査基準」に準拠して、公表文書に見てきた保証業務に係る議論を整理すると共に、特に保証業務に係るシステム監査の担保要件等について重点的に追補し、これを定義し明確化する。

結論を簡単に述べると、保証型システム監査で特に重点を置くべき論点は、意見書で定義されている保証を担保する 5 つの要件のうち、「適合する基準」と「適切で十分な証拠」の 2 項であると筆者は考える。それぞれについての提案は次の通りである。

保証型システム監査における「適合する基準」では、システム監査の目的におけるコントロールを適切に整備・運用するための目標である戦略性、安全性・有効性・効率性、信頼性、遵守性の各目標において、信頼性、遵守性については適用可能であるが、有効性や効率性を目的とする監査では経済産業省のシステム管理基準が適切かどうかという疑問が残る。これらに対する適合する基準については、個別に今後の開発を期待する。

また、保証型システム監査における「適切で十分な証拠」については、監査手続における運用状況の評価において内部統制の実施基準で採用された「サンプリング試査」を採用したい。質、量ともに適切で十分な証拠を客観的に担保するためにはこれで十分すぎることはない。

保証型システム監査の実績として、2009年11月に当協会近畿支部においてシステム監査普及サービスで実施された「i社システム監査サービス」は意欲的な試みである。簡単なレポートや2010年7月16日付けの近畿支部定例研究会の講演資料等がホームページ上で紹介されているが、更に詳細を研究する機会を見つけ、今後の参考としたい。

以上、紙面の都合上、ダイジェスト版でレポートの概要を紹介したが（それも結論のみですが）、別の機会に本レポート全文を紹介したい。今後の保証型システム監査の議論における一つのたたき台としていただければ幸いである。

（格物致知）

（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。）

めだか【介護保険制度において真に見直されるべき制度上の問題】

201101 投稿

2010年12月9日の日経新聞に「第3次ベビーブームは望み薄」という衝撃的な見出しが出ていたことは記憶に新しい。さらに12月22日開催「第15回社会保障審議会医療部会」で発表された資料82ページでは、2030年には高齢者1人をささえる労働者人口が、1.7人と予測されている。

介護保険制度については、2012年の見直しによって介護利用料、保険料の値上が予定されているが、一般には知られていない根本的な制度上の問題がある。

介護事業者

サービス種類	2009年4月
【訪問介護】	26,741
【訪問入浴介護】	2,407
【訪問看護】	64,955
【訪問リハビリテーション】	53,105
【通所介護】	24,188
【通所リハビリテーション】	33,447
【短期入所生活介護】	7,653
【短期入所療養介護】	5,789
【特定施設入居者生活介護】	3,047
【居宅療養管理指導】	154,870
【福祉用具貸与】	7,319
【居宅介護支援事業者】	31,907
【指定介護老人福祉施設】	6,134
【介護老人保健施設】	3,603
【指定介護療養型医療施設】	2,329
【特定福祉用具販売】	7,175

最も見直されるべきは、介護報酬請求業務の複雑さである。診療報酬は全国共通の「診療点数表」により単価（1点＝10円）が明確であるのに対し、介護報酬はサービスの種類、内容、提供回数、提供時間、利用者の要介護度、および地域に応じて単価が異なっている（1単位＝10円～10.72円）。訪問介護サービスでは従来3級ヘルパーが行ったサービスは70%に減額されていたが、2010年4月以降は請求できなくなったし、40歳以上の難病（指定16疾病）患者への訪問介護には、地方自治体によっては全額公費で補助がでるケースもある。個々のサービスの単純な積算が不可能であるため、膨大なチェック機能を備えたアプリケーションやASPサービスを利用する事業者がほとんどである。特に複雑な処理が発生するのが、訪問介護事業者で、その数は左表に示されるとおり全国に26,741事業者あるが、その多くが中小規模事業者である。

介護事業者は、翌月からすぐに〆処理に取りかかり10日までに国保連（介護報酬請求先）に伝送で請求しなければならないが、その主流は未だにISDN回線経由であることにも驚く。（独立行政法人福祉医療機構2009/12/1発表資料より抜粋）

日本中の企業で事務処理のコストパフォーマンスが叫ばれ、PCが一斉に導入されてから久しい。しかし国が定めた介護報酬請求の仕組が複雑であるためもあり、そのシステムの完成度は高いとはとても言えない。介護業界では劣悪な労働条件とともに劣悪なIT環境の二重苦に陥っているのである。

2000年の介護保険制度、2005年の障害者支援費制度と、措置から契約の流れで社会福祉の仕組みは統合に向かい、官から民へと移行してきた。民間の事業であればなおさら制度が簡略化されなければ、事業者の体力はついて来られないのに国は全く無責任である。システム開発に携わる多くの人たちが、介護保険請求システムに興味を示して来なかったのも、今後どのように変わるのか解らないという先の見えない制度であると言うことなのだろう。こうした資源が整備されていないことに疑問を持つ余裕もなく、声を上げる暇も無く訪問介護に走り回る介護事業者を見て見ぬふりで放置しておいて、我々の老後は豊かになろうはずもない。何かできることはないかと思う日々である。　　以上

（白雪姫の継母）

（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。　）

めだか【 監査とコーチング 】　　201101 投稿

「改善すべきと監査人が思ったこと指摘して、何が悪いのですか？」

これは、数年前、監査部門に配属されて間もない後輩が、ある指摘をしようとして、被監査部門から実態に合わないと反発されたため、先輩であった私に、その不満をぶつけた一言である。

この質問に、私は一瞬口籠ってしまったが、当時、あるセミナーでコーチングの話を聞いた直後だったこともあって、「監査もコーチングが重要だよ。こちらが問題点だと思っても、それを相手に押しつけてはダメで、気付かせるようにすることが必要なんだ。」とアドバイスした。

しかし、私自身はというと、被監査部門に問題点をどう伝えたら納得してもらえるのかに、いろいろと悩んではいたものの、実はそれまで、監査にコーチングの考えを取り入れるなどとは考えてもいなかった。

そこで早速、「監査におけるコーチング」に関して調べてみたところ、以下のとおり、一般にはその重要性についてあまり意識されているとは言えない状況であった。

①インターネットで検索しても、監査においてコーチングが重要であるという意見は、いくつかあるものの、数えるほどしかない。

②「監査におけるコーチング」について解説した書籍は、ほとんどない。

だが、最近は状況が変わってきた。監査の世界でもコーチングへの注目度が高まってきているようだ。

＜事例1＞

昨年10月に株式会社プロティビティジャパンが公表した『内部監査に必要な能力のサーベイ』(注)において、向上の必要性が高い監査人のスキル・能力として、「コーチング／メンタリングスキル」が、「外部とのネットワーキング」に次いで第2位となり、前年調査の第10位から大幅に順位を上げている。

その事情について、同サーベイでは「内部監査部門内での人材教育・育成や被監査部門に対する指導・改善などの局面で、必要性が高まっているもの」としている。

（注）日本の内部監査担当役員、内部監査部門長、マネージャー、その他の専門職の計191人に対する調査結果。
http://www.protiviti.com/ja-JP/Downloads/IA_Survey_2010.pdf

＜事例2＞

「監査におけるコーチング」について解説した書籍は、ほとんどなかったが、ここにきてやっと出会えた。

昨年10月に発売された戸村智憲氏著『監査コミュニケーション技法"疑う流儀"－監査心理学による監査を通じた幸せづくり－』(税務経理協会)が、それである。

被監査部門とどうコミュニケーションしていくのがよいのかについて、具体的実践例を示しながら様々な解説がなされており、非常に得るところの多い本である。

皆さんも、「コーチングを取り入れた監査＝被監査部門に問題点・改善策を気付かせる監査」について、ちょっと考えてみませんか？　　以上　（やじろべえ）

（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。　）

めだか　　201101 投稿

【PMS 構築の個人情報管理台帳とリスク分析表を作成目的から考えるとわかりやすくなる】

プライバシーマーク（Pマーク）の審査に携わり、また、PMS（個人情報保護マネジメントシステム）の構築相談に携わっている経験から記します。

PMS構築において（またPマーク審査において）、個人情報の特定とリスク認識、分析および対策（リスク分析）は、一般的に理解しにくく、結果として申請事業者も、コンサルも苦労しているようである。

＜個人情報の特定について＞

個人情報を特定する「個人情報管理台帳」は、どのような個人情報を保護対象とするか社内の関係者に明確に示し、また場合によってはお客や個人情報の本人に対して説明のために示す資料でもある。この台帳では、まず、何が個人情報保護の対象か明確にするのであるが、例えば沢山ある個人に関する書類（人事管理用書類、取引伝票や社内の掲示物など文書名ごとに分けると膨大な数になる）をどのように整理して記載するか、名刺のように複数の所有者に分散する情報はどのようにこの台帳に記載するか、顧客から預かった情報などがさまざまな媒体にコピーがなされる状況をどのように記載するか、迷うところである。また、この台帳では管理者、保管場所、保管期間、委託の有無など管理要件を明確にする。

事業者が個人情報を特定し「個人情報管理台帳」に記載するため、さまざまに思考し、コンサルに指導を受けたりして、これで良いかと作った台帳について、プライバシーマークの審査員からいろいろな指摘をされ、特定のしなおし、また台帳の手なおし、作り直しを要求されることが多いようである。このことから、台帳作成は厄介な事項と悩んでいる事業者が多いのではないかと思われる。

この原因のひとつとして、台帳は個人情報を特定するために作成することはわかっているが、何のためにこの台帳を作るのかという視点が抜けているための混乱が少なからずあるのかとおもわれる。

この台帳の役割は、事業者が自社で責任を持って扱う個人情報を明らかにして、その管理要件を明確にするのであり、その視点から考えるべきである。つまり、「社内の関係者に何が個人情報保護対象であることを周知徹底する」ために十分な精度を持たせ、また、万一の事故などの場合に「顧客などに自社の個人情報保護システムを説明する」ことが出来るようにする。このような視点で考えると、どの程度の精度や表現が必要であるか、自分たちで判断が出来ることになる。要は、社内の関係者が明確に対象をもれなく認識でき、また顧客にも説明できるものであればよい。決して形式的に何かの要件を満たすことではないのである。

＜リスク分析について＞

次にリスク分析の結果作成する「リスク分析表」は、取り扱いの局面ごとにどのようなリスクが存在するか、個人情報保護のためそのリスクに対してどのような対策をしなければならないか、明確にするものである。このリスクをどのように洗い出し資料としてまとめるかの方法は、普段事業者はあまりなじみがないため理解しにくく結果として申請事業者は苦労しているようである。

したがって、管理者などがその考え方をコンサルタントや資料から得たり、Pマークの審査において要求されて

知ることが多いようである。一方、実際のリスクの洗い出しは個人情報の取扱いの局面ごとに、つまりデータフロー、業務フローに沿って考えてゆく必要がある。これは現場の実態をよく知っている者が分析にあたる必要があり、従って、本当のリスクを考え、リスク対策を認識し、対策が適切であるか内容を検討出来るのは現場の管理者、担当者である。また、その対策を実施するのは偏に現場に依存することになるので、明らかにした保護対策は個人情報保護の管理者は当然であるが、それを扱う現場の者が良くその内容を熟知していなければならない。したがって「リスク分析表」を作成するには、方法を知る管理者などが考え方をサポートし、現場が主体で考えることになる。

このときにリスクや対策をどのように表現するかなどは、個人情報の特定と同じように、「社内の関係者にリスクと保護対策を正確に周知徹底できるように表現し、また、万一の事故などの場合に顧客などに自社の個人情報保護システムを説明することが出来る」ようにすることが目的となる。また、「時間が経過しても担当者が異動し状況がかわっても、分析内容が引き継がれるように分かる内容で記載する。」ことが必要である。このような「リスク分析表」となっているか、判断基準にすることである。

＜作成した資料の活用＞

このような台帳と、リスク分析表は、作成するのに貴重な時間を費やして作成することになる。したがって出来上がった台帳とリスク分析表を、十分に利用しないということは大変な無駄づかいということになる。ところが、上記の目的を十分に意識しないと、せっかく作成したものを、プライバシーマークの審査が終わってしまうと、年1度の見直し、次回審査までそのままに放置してしまうことになる。この無駄遣いがかなりの割合であるのでないか懸念する。

PMSは継続的に運用することが必要であり、このため運用ルールを担当者、関係者にわかりやすく示す（「見える化」する）こと、そして周知させていることが重要である。

個人情報を保護するためにPMSを構築しているにもかかわらず、そのことが忘れられて、「個人情報管理台帳」、「リスク分析表」の形式的な要件を満たすことに重点を置きすぎてしまうことが多いようである。繰り返すが、何のためにこの書類を作るのか、決して整理して審査員に提示して確認してもらうためではない。作成したものを社内で関係者が利用してこそ意味があり、そのために作成するものである。記載された管理要件が間違っていないこと、その特定した狙いに沿って管理していること、そのため現場の教育の材料として、活用しなければならないものでもある。

このように活用していれば、内容の定期的な見直しは容易に行うことができる。しかし、前に書いたように書類が作成されてそのままになっているのでないか懸念される。

以上はプライバシーマーク認定を取得した事業者としては、その「個人情報管理台帳」と「リスク分析表」を上記の目的に沿って作成するとともに、利用することを心がけ、そしてコンサルにあたる者としては、意味を間違えた作成を指導しないこと、事業者に無駄をさせないように気をつけることが必要であると考える。

（お山のたぬき）

以上

（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。）

201102 投稿

めだか【 破産出版社の債権者集会 】

著書を出したことのある出版社の債権者集会に出席した。
担当裁判官、裁判所の選任した管財人（弁護士）、破産者（前社長）、破産者代理人（弁護士）、債権者（著書執筆者、元社員など）数十人である。

集会は裁判所が開催したもので、集会の仕切り、司会は担当裁判官である。
管財人が、就任以降の債権の回収状況など、財産目録、収支計算書を中心に説明する。
「現金」は簿価が￥5,491,491、評価額が￥5,404,971、とある。大きな差ではないが、「現金」で簿価と評価額（現にあった金額か）に違いがある。

事業が継続されていれば、この種の差はどこかでなくなるが、活動が止まったところを生々しく、映し出している。
「預貯金」は、100万、200万と大きく残っているところも借入と相殺で回収見込みなしとか、6万足らずの口座が国税差押とあったりで、こちらも大変である。
「受取手形」は6件、450万円余で、これは全額回収されている。手形を振り出した先がしっかりしていれば、回収可能なのであろう。

「在庫商品」の書籍は借りた倉庫に置いてあった。
倉庫料なども滞納しており、倉庫側からは速やかな撤去を求められている中で、元社員の応援も得て、購入希望者などを倉庫に集め、ギリギリ売り払った経緯などが説明される。

「出資金」は、信用金庫や信用組合への出資分である。
「平成23年2月4日6月以降でないと脱退手続がとれない」という注釈のところは最終的には回収できそうであるが、大口の300万円分は、「現時点では出資金買取希望者が現れず、換金不能」という。
脱退で出資金を返還してくれるところと代わりの出資者を見つけなければならないところとあるようである。
少しであるが、株式もある。
簿価￥11,000のものが￥90,000で回収されているが、簿価￥6,000のものは株券不明とある。
管財人の説明は、収支計算書の収入の部で終わった。
　合計￥32,664,507。
同支出の部は
　事務費￥351,935、
　（破産）財団債権￥24,312,572、
　簡易配当金￥0、
　管財人報酬￥8,000,000、
　合計￥32,664,507。

支出のうち、破産財団分は自治体へ納入しなければならない住民税などを指しているから、回収されたもののうち、事務費を除けば、あとは管財人の報酬という構図である。

もちろん管財人の働きがなければ、回収そのものが成り立たないわけであるし、担当の弁護士も1人ではないようであるから、800万でも足が出そうであるが、これも一つの現実なのであろう。

債権者として出席した人は、著作の執筆者や元社員が多いようであった。
自分の本を出してくれた出版社の倒産など、経験した人は少ないようで、執筆者から、「書籍の著作権はどうなる」という質問があった。

管財人の答えは、「出版社側には何の権利も残っていない。書籍の原稿や印刷版型は印刷所が持っている。印刷所側は債権のかたに押さえているので、管財人と話をしてくれない。執筆者ご自身が印刷所と交渉し、他の発行元があれば、そこに移管してもらったらどうか」である。

筆者が書いたものは、版型が残っていても再び印刷には付したくないからいいのであるが、中には我が子の葬式を出すような気持ちの人もいるのであろうか。
債権者集会には、債務者も出席しなければならないようで、破産者席には前社長の姿があった。
多くの執筆者を送り出した人柄のいい人で、集会終了後、何人かが話しかけていた。
筆者も「大変でしたね」とかいうつもりであったが、敗軍の将に声をかけるのもやや辛いのである。

（佐平次）

（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。）

201103 投稿

めだか　【百貨店のカードシステム】

失くしたときの面倒くささを考え、カードはなるべく持たないようにしているが、いきさつがあって、A、B二つの百貨店のポイント・カードを持っている。

買い物のたびにポイントをつけてもらえば、少ない額とはいえ、正価からいくらか割り引いて買ったことになる。外商を利用するほどの取引はないから、百貨店で値切って買い物をする機会にはなる。

一方、百貨店側も抜け目なく、持合わせがなくとも多額な買い物ができますからとクレジット機能付にさせるから、簡単には失くせない。

中元、歳暮で使っている粕漬け店が百貨店に出た。売り場の女性店員と何か話そうと、「詰合せは直営店で買っても同じだよね」などといえば、「直営店ではポイントがつかないから、百貨店で買う方がトクですよ」という。なるほど、そんな使い方もあるのか。

百貨店のポイントの還元の仕方は同じで、一定期間のポイントに対し、店内での買い物券を出す。これが、なかなか面倒だと思っていたら、A店では、紙の買い物券をやめて、電子の世界で、貯まっているカードから、直接引き出せるようにしたという。

カードシステムの中には顧客別の台帳があるわけだから、売り場の端末から、そのデータを見れば、わざわざ買い物券を介在させる必要はない。やぼな買い物発券機はどうなったかと見れば、客が現在のポイントを確認できるものとして置いてある。

ただし、一定期間のポイントだけを使用可能対象とすれば、データとしては、使用可能ポイント数と蓄積中のポイント数を持たなければならない。買い物をした際の領収証に、両方が印刷されて出てくるが、大した金額でもないのに、客としては一々両方を確認しなければならない。

ところが、そのうち、一定期間のしばりがなくなり、現在蓄積されているポイント数が全部使えるというのである。
これは便利になった。小額の買い物で、ほかに待っている客もいる中で、小銭を出すは、カードを出すは、品物を受け取りはでは、両手がふさがって不便であるが、カードだけで済めば、簡単である。領収証のポイント残は、すなわち使用可能数で、もう一つ、二つ買っていこうかということにもなる。

仕組みの進歩は、すなわちカードシステムに対し、継続して投資していることを示している。端末などの機能も向上させているはずである。

A店で、このような展開があったのに、B店の方では、何の変化もない。

ある日行けば、「カードシステムでポイント整理のため、カードの利用ができません」などというお知らせが出ている。システムを改善しておらず、する気もないように見える。

B店の店員がA店のカードを持ってはいないであろうから、他店がどれほど変化しているかはなかなかわからないのかもしれない。

B店から、親展のハガキが来た。ハガキを出す経費もばかにならない。

ポイント付与商品の一部について、今まで「8%」のポイントを付けていたが、これを「1%」にするというあいさつである。「利幅が縮小する中で、やっていけないから」という。そうもあろうかと思うが、「8%」なら意味のある値引きであったが、「1%」では、形の上で値引きしてますというお印だけになる。手間ひまを考えれば、経営的には、いっそ「0%」の方がいいのではないか。中途半端はいけない。

百貨店という業態が他業種からの挑戦を受けて、昔ほどの元気がないことは、新聞雑誌を見ても、店の売り場を歩いてもわかるが、百貨店全部がダメになるわけではない。

店全体の売上が伸びなければ、システム投資に回せる金が出てこないことはわかるが、どこに集中と選択の原則を働かせるのか。IT関係者は、どのような論理をもってシステム投資への必要性をいうのか。むずかしさはますます増すのであるが、どうにか知恵をしぼらなければならない。

（太郎冠者）

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

監査人のコラム「めだか」は、会員の方、どなたでも投稿できます。
これまでの投稿例をご覧いただき、原稿を次のアドレスへ送信ください。

saaj-kaihoh ☆ yahoogroups.jp　（☆は投稿時には＠に変換してください）

なお、編集者の判断で、調整をお願いする場合もありますが、原則、投稿された内容をそのまま掲載します。
また、一般投稿も歓迎します。

(CSA 報告)　　【 (CSA 報告) CSA フォーラム　開催報告まとめ 】後半

2011年CSAフォーラム新年会資料

CSAフォーラム（第8回～第11回）開催結果について

2011年1月26日

NPO日本システム監査人協会
CSA利用推進G

目　次

CSAフォーラム開始の背景
CSAフォーラムのコンセプト
第1回から7回までCSAフォーラム開催一覧
第8回から第11回までの開催ご紹介
－概要
－発表者プロフィール
－発表内容

 1

CSAフォーラム開始の背景

CSAに係わる問題意識と対応

◆CSAの位置付けについての課題

- CISAやその他の監査人資格に比して知名度が低く、入札資格・人材募集要件などに殆どCSAが現れない
- CSAの連帯感の醸成、コミュニケーションを深める場が少ない
- SAAJにCSAが監査人としての力量を高める場が少ない

- ・公認システム監査人（CSA）案内リーフレット作成、配布
- ・CSA入札条件依頼文例の作成、配布
- ・協会HPにCSA専用ページを作成
- ・CSAフォーラムの開始（'08年9月第1回開催）

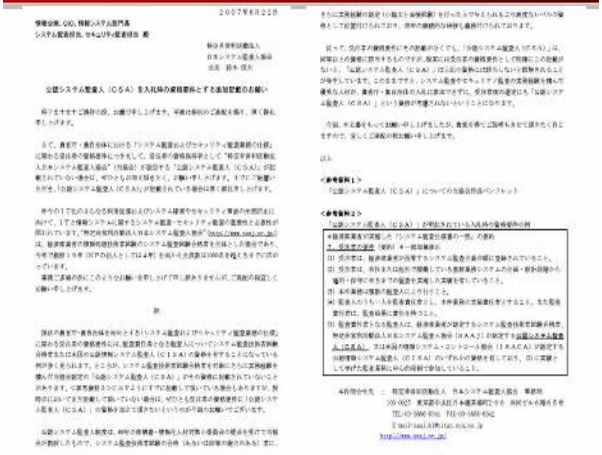
著作、情報発信等、更にCSAのステータス向上のための施策が必要

 2

公認システム監査人のご案内

 3

CSA入札条件依頼文例



 4

CSAフォーラムのコンセプト

●CSAフォーラムはCSA・ASAを対象にシステム監査に関する実務や事例研究、理論研究を通して、CSA・ASAの*システム監査業務に役に立つ研究*を行うことを目的にします。

●本活動を通じCSA・ASA同士の*フェイスtoフェイスの交流*を図ることにより、相互啓発や情報交換を行い、CSA・ASAのスキルを高め、よってCSA・ASAのステータス向上を図ることも狙いにしています。

●フォーラムの開催は*隔月で1回30名程度*の参加とします。

 5

第1回から7回まで CSAフォーラム開催一覧

回数	開催日	講師	タイトル
1	08/9/30	竹下 和孝 氏	CSAの成功法則
2	08/11/26	三谷 慶一郎 氏	CSAに求められる新たな役割
3	09/1/27	松枝 憲司 氏	CSA実践報告＆基準研紹介
4	09/3/5	島田 祐次 氏	内部監査から見たシステム監査
5	09/6/1	桜井 由美子 氏	組織人を幸せにするマネジメントシステムを目指して
6	09/7/23	小野 修一 氏	システム監査の実践を通してのCIOの役割・課題への貢献
7	09/9/24	山田 隆 氏	オフショア開発成功のためのシステム監査

 6

第8回CSAフォーラム － 概 要

項 目	内 容
発表者	福田 啓二 氏 （株式会社アンヴィックス取締役）
タイトル	地方在住CSAの活動とスキル維持向上策
発表者コメント	システム開発の現場を主な業務としながらシステム監査にも従事している活動状況をご紹介するとともに、SAAJ九州支部をはじめとする地域コミュニティへの関与を通じたシステム監査人としてのスキル維持・向上策についての考えと実践についてお話しさせて頂きます。
開催日・場所	2010年1月25日 於、日立情報システムズ 会議室

 7

第8回CSAフォーラム
– 発表者プロフィール

発表者	福田　啓二　氏
プロフィール	福岡市在住。通信、製造、画像処理等のシステム開発に従事。 現在は電力系統制御システム開発プロジェクトに関与するかたわら、 システム監査／セキュリティ監査等でもご活躍中。
資格・所属団体等	システム監査技術者、公認システム監査人、CISA、情報セキュリティ専門監査人、個人情報保護専門監査人、システムアナリスト、　テクニカルエンジニア（情報セキュリティ）、ネットワークスペシャリスト他。 NPO日本システム監査人協会 九州支部長（2001-2009）、　日本システムアナリスト協会理事（2008-2009）、システム監査学会会員、情報システムコントロール協会会員、セキュリティとんこつ・ばりかた勉強会スタッフ。
著書（共著）	「個人情報保護士試験公式テキスト」（日本能率協会マネジメントセンター）、「IT業界がわかる」（技術評論社）

 8

第8回CSAフォーラム
– 発表内容（主なスライドタイトル）

- 支部活動について
  - 九州支部のご紹介
  - これからの支部活動について
- スキルについて
  - 主にIT技術のスキル
- スキル維持・向上について
  - スキル維持・向上のツールとしての試験
  - パブリックコメント
  - 仕事への波及
- システム監査の事例

 9

第9回CSAフォーラム
－ 概　要

項　目	内　　容
発表者	萩原　栄幸　氏 （株式会社ピーシーキッド　上席研究員）
タイトル	目からウロコの情報セキュリティと様々な雑感
発表者コメント	防衛省や海上保安庁などのセキュリティ教育や銀行協会への講演会などを通じて、最近の情報セキュリティにおける様々な犯罪事例やちょっとした知っていると便利な事、そしてグーグルの中国撤退やハッキングデモを通じて警鐘を行い、今後どう世の中が変化していくかを文字通り目からウロコが落ちるように意識変革を目指して講演を行います。 また今年設立した社団法人についても驚くべき事実を基に解説していきます。絶対に見逃せない講演だと自負しております。
開催日・場所	2010年4月26日　於、日立情報システムズ会議室

 10

第9回CSAフォーラム
－ 発表者プロフィール

発表者	萩原　栄幸　氏
プロフィール	●情報処理技術者試験で最難関である「特種」に日本最年少で合格。早稲田大学システム科学研究所に通学後、プロジェクト・リーダーとして、多数のシステムを担当。日本セキュリティ・マネジメント学会（JSSM）の「先端技術・情報犯罪とセキュリティ研究会」などで講師経験を積む。NHKやフジテレビなどにも出演し、活動範囲を広めている。2008年6月まで三菱東京UFJ銀行システム部に在籍。
資格・所属団体等	●日本セキュリティ・マネジメント学会　理事、社団法人 コンピュータ・ソフトウェア著作権協会　技術顧問、ネット情報セキュリティ研究会　相談役、CFE公認不正検査士、一般社団法人（非営利型）「情報セキュリティ相談センター」事務局長、金融ニュービジネス＆テクノロジー研究会　常任アドバイザー
著書	●「経営戦略としての個人情報保護と対策」（工業調査会、2002年、共著　・「名探偵ハギーの世界一やさしい　情報セキュリティの本」（日科技連出版、2004年）・「45分でわかる個人情報保護」（日経BP社、2005年,共著）　・「個人情報はこうして盗まれる」（KKベストセラーズ、2005年）　・「デジタル・フォレンジック事典」（日科技連出版、2006年、編集責任＋共著）　・「NHK達人に学ぶ人間力アップ」（日本文芸社、2007年10月発行、共著扱い）　他

 11

第9回CSAフォーラム
－ 発表内容

――ボットの本当の怖さってご存知ですか？

――本当に業者を信用してもいいですか？

――裁判所がしてしまった「情報漏洩」の非常識

――金融機関のコンピュータシステムでの日米の違い

――便利ツール

――健全な情報セキュリティ社会に貢献しませんか？

 12

第10回CSAフォーラム
－ 概　要

項　目	内　容
発表者	大石　正人　氏 （日本銀行金融機構局企画役（システム・業務継続担当）。2000年代以降相次いだ大手金融機関のシステム統合の調査やシステムリスク管理手法の高度化に向けた作業に従事。特定非営利活動法人　日本システム監査人協会　理事。
タイトル	金融機関のシステムリスク管理－中央銀行の立場から
発表者コメント	中央銀行にとって、決済システムの円滑かつ安定的な運行を確保し、金融システムの安定を確保することは、物価の安定と並んで重要な役割の一つです。日本銀行はわが国唯一の中央銀行として、日本銀行当座預金を通じて取引先金融機関間の決済インフラを提供するとともに、金融機関の業務や事務処理体制に問題がないかを、考査やオフサイトモニタリングを通じて目配りをしています。今回のフォーラムでは、そうした観点から決済の安全性や効率性の確保に向けた活動内容をご紹介します。
開催日・場所	2010年7月26日　於、日立情報システムズ会議室

 13

第10回CSAフォーラム
－ 発表内容

1. 金融機関と決済サービス
2. 決済サービスの概要
3. 考査・オフサイトモニタリングでの対応
4. システムリスク管理の観点・項目
5. リスク・ファクターの変化
6. システム共同化の現状と課題
7. プロジェクト管理の現状と課題
8. 決済サービスと事業継続管理

 14

第11回CSAフォーラム
－ 概　要

項　目	内　容
発表者	中山　孝明　氏（中山システム監査事務所代表）
タイトル	システムリスク、その計測・管理・監査で求められているもの
発表者コメント	情報システムのリスクとコントロール、リスクの計測と評価、システム監査などに、法的な要求事項が及んでいる部分があります。それは、オペレーショナル・リスクの管理として金融機関に課せられているものの中にあり、システム監査人にはこれらを踏まえた監査が求められております。これはさほど目新しい話ではありませんが、多くの業種や システム分野の専門家に関係する事柄でもあると思います。 また、システムリスクの把握や管理については試行錯誤の状況が多いのも現実と理解しております。 発表の後、システム監査人の役割などを含め意見交換をさせていただきたいと考えております。
開催日・場所	2010年11月26日　於、日立情報システムズ会議室

 15

第11回CSAフォーラム
– 発表者プロフィール

発表者	中山 孝明 氏
略歴等	●都市銀行における、勘定系・情報系・国際系システムなどの企画・開発・運用の各部門の業務、システム子会社の業務、コンピュータセンターの管理業務などに従事 ●銀行子会社における、業務監査本部、事務集中本部などの業務及び役員を歴任 ●金融庁(証券取引等監視委員会)における、金融機関のシステムリスク管理態勢などの検査官(2010年7月退官) ●現在、中山システム監査事務所代表 ●公認システム監査人(CSA)、日本システム監査人協会 理事

 16

第11回CSAフォーラム
– 発表内容

――システムリスクと監査

――オペレーショナル・リスクの登場

――要求事項(告示第19号)←オペレーショナル・リスク管理

――システムリスクの理解

――要求事項(検査マニュアル)←システムリスクの管理

――リスク管理への取り組み

 17

会報電子版(メール、PDF、個別記事)の見方について

会報の電子化を進め、都度、読みやすいように調整を加えています。　2011.3 時点で、電子化された会報といっても、３つの種類がご覧になれますので、それぞれの関係について説明させていただきます。

１）電子メールで送信する会報メール
　メールでお届けするのは、タイトル、記事の抜粋など、一部です。

２）会報メールの指定された URL をクリックすることで、会報 PDF 版をダウンロードできます。
　画面上で閲覧するだけでなく、全体の会報をダウンロードしてみる、印刷することもできます。

３）同様に、会報メールに記載された URL（http://skansanin.com/saaj/）では、個別記事を閲覧できます。
　記事は、前回分、先月分と蓄積し、比較することで価値が高まるものもあります。
　「めだか」、「月例研究会」、「基準研究会」、「支部報告」、「投稿、ニュース」などの
　2010 年以降に発行した会報は、テーマごとに、アーカイブ記事として閲覧できます。

まず、会報の記事を編集終了すると、メール版の案内を送付します。送付先は、会員の登録アドレス宛です。

１．会報発行のメール案内を受信後、メールに記載された該当の記事へリンクをたどって、
　１）画面で見る　２）PDF の記事なので、印刷してみる　ことが可能です。

２．会報サイト（個別記事検索）

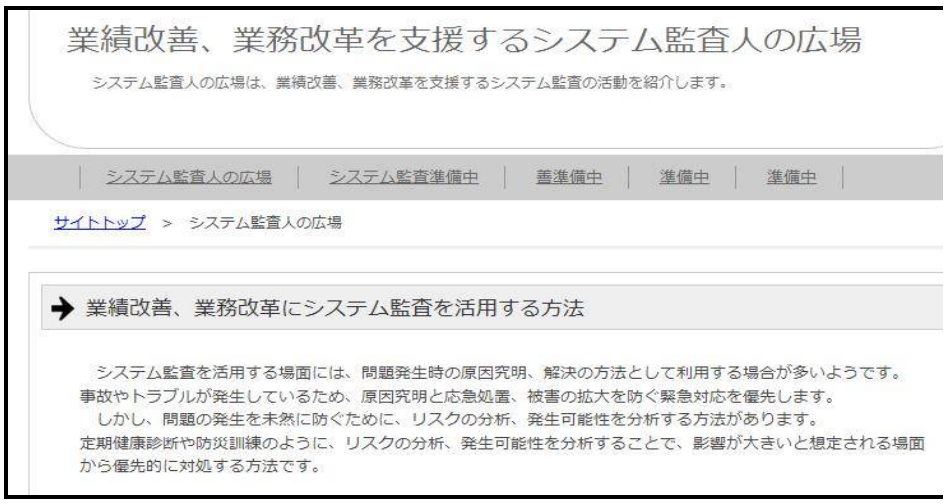
１と同様の電子版記事は、会報サイトでは、記事ごとに検索することができます。
（電子化を始めた２００９．１２号以降の記事が保管されています。
今後、それ以前の記事についても、電子版として対応可能な場合に、掲載していく予定です）

サイト構成

１）http://skansanin.com　　システム監査人の広場　（SAAJ、LLP-CSAJ など共通利用）

２）http://skansanin.com/saaj/　SAAJ 会報の掲載サイト（情報発信の拠点として活用予定です）

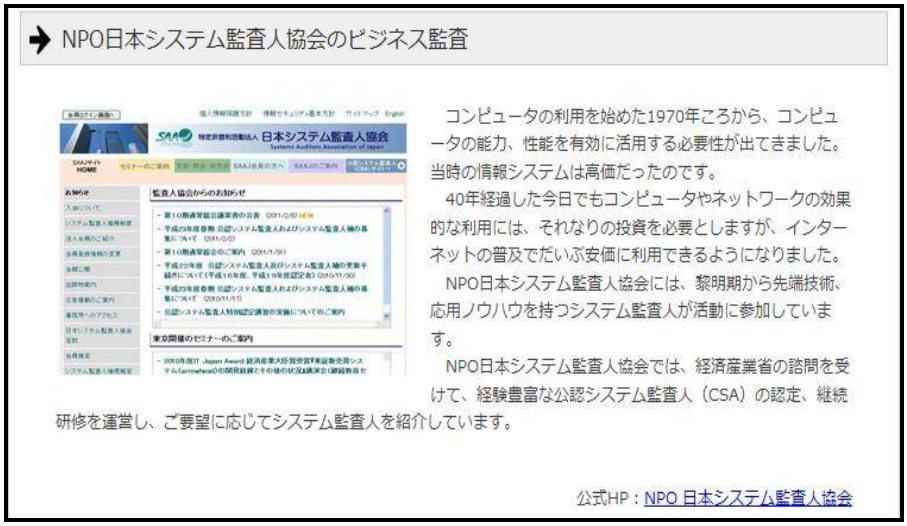
１）システム監査人の広場 http://skansanin.com



システム監査を進めるシステム監査人の情報交換、交流の場として、サイトを運営しています。

システム監査を調査、研究、普及活動を実務的に推進しているのは、業務改善や改革の実効性を高め、加速するためです。

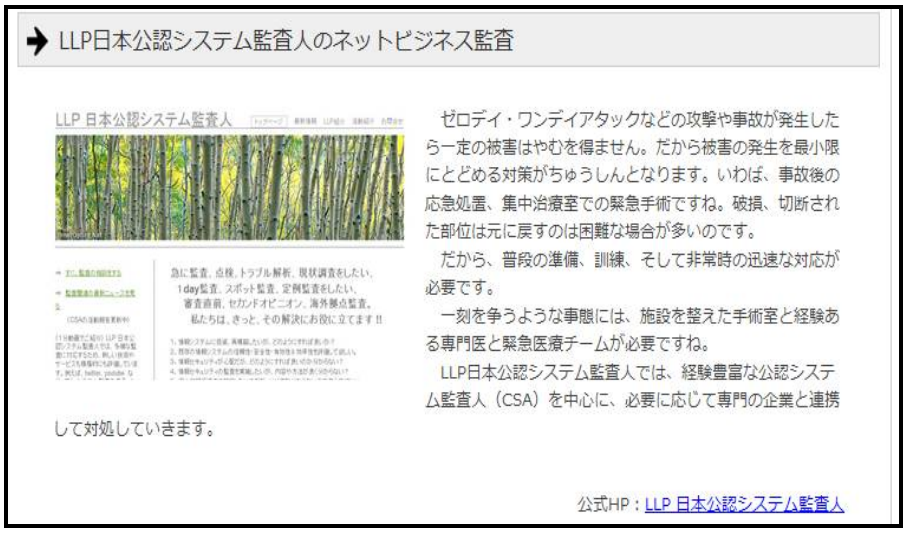
1）－2　システム監査を推進する組織　SAAJ



SAAJ 公式サイトと LLP 日本公認システム監査人サイトへリンクをたどれるようにしてい

SAAJ の公式サイトを中心として、システム監査というキーワードへの検索を容易にするよう、紹介しています。

1）－3　システム監査を推進する組織　LLP-SKANSANIN



http://skansanin.com/con5/
LLP 日本公認システム監査人のサイトとの相互連携で、システム監査への個別ニーズにこたえる体制を整備して利便性を高めようとしています。

LLP サイトでは、一般からの個別相談にも応じています。

1）－4　http://skansanin.com/saaj/ のめだか記事を紹介

公認システム監査人や CSA のブランドつくりを支援するため、情報発信の拠点として活用を始めています。

今後は、個人の記名記事を編集する予定です。

これにより、システム監査人のブランドも高まるよう期待しています。

２）http://skansanin.com/saaj/ では、会報の個別記事と過去記事（アーカイブ）を閲覧できます。

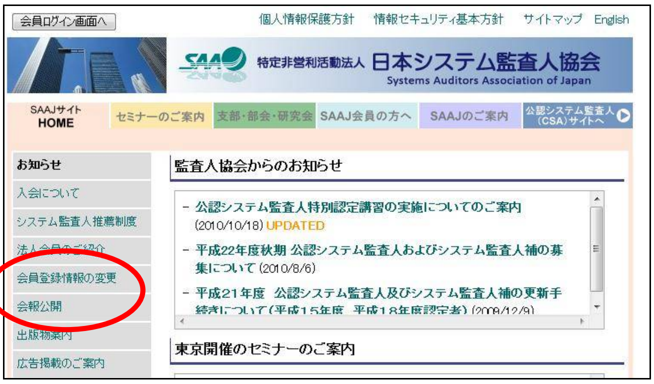
３．SAAJ 公式サイト　（http://www.saaj.or.jp/）

SAAJ の公式ページには、会報の電子版を公開しています。

メール送信のほうが伝達速度が速いため、記事を更新して掲載するタイミングは約１日遅れます。

公式サイトでの閲覧方法は、2010.12 月号にも詳細の閲覧方法を解説しています。

SAAJ 公式サイトのトップページ



会報公開をクリックすると、閲覧可能な月別会報を案内します。会員限定情報にはパスワードが必要です。

以上

■□■ＳＡＡＪ会報担当

編集：竹下和孝、仲　厚吉、安部晃生、成　楽秀、桜井由美子、山田　隆、片岡　学、
　木村陽一、藤野明夫　　投稿用アドレス：saaj-kaihoh☆yahoogroups.jp（☆は安全対策）