特定非営利活動法人
日本システム監査人協会報

2012 年 11 月号
No 140

No. 140(2012 年 11 月号)＜10 月 20 日発行＞

秋の夜長に記事満載の会報を

じっくりお楽しみください！

とくに月例研報告は必見です！

上高地　梓川と穂高連峰

会報電子版の記事　目次

〈目次続く〉

2012.10 投稿

めだか　【　システム監査の真の顧客は誰か（システム監査人のやりがい）　】

今月から、テーマが「システム監査人のやりがい」に変わった。
“やりがい”はひとえに主観的なもので、答えは人それぞれと思う。ここでは、システム監査人である私個人のやりがいについての考えを紹介し、皆さんのご意見もお聞きしたい。

システム監査は新たなサービスを創造するわけでなく、またその成果を直接的に金額で計ることができる分けでもない。従って、システム監査は明確な数値目標を掲げ、それを成し遂げた時に達成感、やりがいを感じる他の多くの仕事と、少し性格が異なるように思う。システム監査は情報社会の中で価値ある仕事と思うが、その価値・成果が目に見えないという意味では非常に地味な仕事と言える。

そう思っていたところ、システム監査を生業にしている友人が、監査終了時に被監査会社から、監査人の持つ知識、経験、ノウハウに基づく改善提案（アドバイス）をして貰って大変参考になったと言われ、システム監査人として大いにやりがいを感じたと話しているのを聞いた。
確かに、被監査会社が満足する監査ができたことは大変結構なことである。
しかし、この時私としてはちょっとひっかかるものがあった。

言うまでもなく、情報システムはそれ自体に効用があるのでなく、それが利用されてはじめて価値を生む。従って、情報システムの信頼性、安全性、効率性などの評価を目的とする監査では、そのサービスを利用する人が、いつでも安全に、安心して、そして最少のコストで快適に利用できることが最も重要な評価ポイントになる。私がちょっとひっかかったのは、システム監査では、システム開発者、サービス提供者の視点にも増して、システムの利用者の視点が重要と思うところから発している。
つまり、システム監査の真の顧客はシステム利用者であり、システム監査が監査人の意見表明を通し、システム利用者が安心し、満足して利用できるシステムの稼動・運用に貢献できた時（システムが何の問題もなく目的どおり活用されている時）、システム監査人のやりがいも生まれるのではと考えているからである。また、監査人の持つ知識、経験、ノウハウに基づく改善提案（アドバイス）は、コンサルティングの範疇であり、言わばシステム監査の付随的産物。それをシステム監査人のやりがいとするところにもひっかかったということである。

『システムが何の問題もなく目的どおり活用されている時システム監査人のやりがいも生まれる』とはなんともシステム監査は地味なものである。この地味な仕事にやりがいを感じるのは、何故だろうか。

情報社会の中で、システム監査人が意見表明を通しＩＴの健全な利活用促進に多少なりとも貢献している、システム監査人は情報社会を支える機能の一翼を担っているというプライドなのかもしれない。
プライド･･･、システム監査は実に地味な仕事ですね。皆さんのお考えはいかがでしょうか。

（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。）

2012.10 投稿

めだか【 システム障害管理の・・・・ホヘト（システム監査人のやりがい）】

システム障害の管理は、情報システムに関わる多くの方が従事し経験したことのある基本的な業務で、今更の感も大きいが改めて触れてみたい。さて、障害管理業務には何があるかと言えば、

① 障害管理にかかわるルール・手順を定め周知する。
② 障害発生時に必要事項を記載した障害報告書を作成する。
③ 委託先・製造元から報告書の提出を受ける。
④ 障害報告書を責任者に提出し承認を受け関係部署に回付する。
⑤ 障害管理台帳に記録し消込管理する。
⑥ 原因を追究し再発防止策を講ずる。
⑦ 重要障害を担当役員に報告する。

障害管理のイロハ

以上が障害管理の基本のイロハなら、その先のホヘトは何だろう？　いくつか挙げてみると、

⑧ 社内・顧客に影響ある障害は当該アプリの稼働日に遡及し影響調査をする。
⑨ 障害記録から一定期間ごとに原因種別・システム・製造元などで傾向分析をする。
⑩ 分析結果により発生が頻発した委託先や製品について対策を打つ。
⑪ 軽微障害でも多発傾向がある場合には重度障害に準じた対策を実施する。
⑫ 原因の記載は、表面的原因・本質的原因・根本原因・真因など曖昧な記載にせず、実効性ある再発防止のために脅威と脆弱性の両面から分析した原因を記載する。（脅威は障害を発生させた”行為・不作為”、脆弱性はそれを防げなかった”弱点”）

障害管理のホヘト

いかがだろうか。既に実施しているからと意外でなかったかも知れないし、ここまで必要かと感じたかも知れない。⑧～⑫はシステム管理基準や他の指針などにこのような表現が明確にあるわけではなく、これら12項目が必ずしも普遍的なものというわけでもない。言わんとするところはシステムリスク管理の観点からである。
重要なことは組織で必要としているリスク管理レベルに応じた管理であり、そのための障害管理がどこまでかを明確にすることである。

①～⑫を項目の字句だけでみると（システム監査の実態確認とは異なるが）、①～⑦は対症療法的な範囲にとどまり、⑧～⑫は確実な原因究明と再発防止策を示す項目といえる。仮に①～⑦の実態が対症療法にとどまっていたならば、その障害管理はリスク管理の一部などとは言えず、単に失敗の後始末をしている（本来の品質に欠けていた部分を修正しただけ）に過ぎないと評価されても止むを得ないと思う。発生した障害が別途の潜在リスクを気付かせ、新たなリスク要因になろうとしている状況については、リスク管理のPDCAサイクルのなかでマネジメントする必要がある。

障害管理業務は、情報システムの特徴（素性、近所付き合い、・・）や性格（柔軟、短気、・・）と組織の内面に直に触れる、実は奥深いものであると思う。なお、ほとんどの組織のシステムリスク管理規程では障害管理業務をリスク管理業務の一部に当然のように位置付けているのが実態ではないかと思う。

システム監査で、障害管理の適切性についてこのような観点から実務の担当者と意見交換し、健全なシステム管理のための姿を追究することもシステム監査人のやりがいとなる。

（山の彼方）

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

2012.10 投稿

めだか【情報システムの健全性について（システム監査人のやりがい）】

アダム・スミスは、人間本性を洞察し、『道徳感情論（The Theory of Moral Sentiments）』を出しており、その中で、秩序を導く人間本性、繁栄を導く人間本性、国際秩序の可能性について議論をすすめています。人間本性は、利己心の働きとともに、「同感（sympathy）」が働くとしています。人間本性は、感情や行為の「対象」について、当事者としての自分の中に、もうひとりの胸中の公平な観察者(impartial spectator)としての自分がいて、「同感」の意思やフェアプレイの態度が表われると説明しています。

マネジメントシステムにおいて、「同感」とは、教育によって、もうひとりの胸中の公平な観察者としての自分が育てられて同感し、監査によって、もうひとりの胸中の公平な観察者としての自分があらためて表われて同感することと考えられます。「システム監査人のやりがい」とは、このように人間本性を考えて、情報システムの健全性のために、システム監査をすすめていくことにあると思います。

情報システムの健全性へのシステム監査では、法令順守、情報システムの安定稼働（信頼性）、情報漏えいの防止（安全性）、また、情報システム利用状況のモニタリング（有効性）等が監査テーマの例として考えられます。これらは、内部監査のテーマとしてとりあげられ、外部監査では、内部監査の対象、内部監査自体を含めて、マネジメントシステム全体がうまく回っているかを監査することになっています。

ここで、経済産業省「システム監査基準」「システム管理基準」を考えてみたいと思います。システム監査の目的が、情報システムの健全性のために、システム監査をすすめていくことにあるとすると、例えば、情報システムの有効性のモニタリングのための管理基準（コントロール、チェックリスト）があって、情報システム利用状況のモニタリングが行われることは重要であると思います。

事業者が経営の役に立つ健全な情報システムを求めるのであれば、経済産業省「システム監査基準」「システム管理基準」は基盤であって、それぞれの事業者が、その上に、例えば、情報システムの有効性のモニタリングのための管理基準（コントロール、チェックリスト）を設計し運用することが重要であると認識することが必要です。

システム監査人は、管理基準（コントロール、チェックリスト）の設計と運用を担っていくことが責務になって、これが、システム監査人の力量向上や、システム監査人のやりがいになっていくと思います。当協会の役割とは、このような管理基準（コントロール、チェックリスト）を設計し運用する活動のセンターになることだと思います。

「アダム・スミス『道徳感情論』と『国富論』の世界」 堂目　卓生　著（中公新書）
アダム・スミス：18世紀、人間の理性を重んじる啓蒙の世紀のイギリスの経済学者・倫理学者

（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。）

2012.10 投稿

めだか【『国富論』の時代と現在】

『国富論（An Inquiry into the Nature and Causes of the Wealth of Nations）』は、1776年に刊行されました。1776年のできごとは、ウィキペディアによると、次のようなものです。

3月 － アダム・スミスが『国富論』を刊行
3月 － アメリカ独立戦争　サンピエールの戦い
4月 － 李氏朝鮮第22代国王正祖ことイ・サン即位
7月 － アメリカ独立宣言発布
　　－ 李氏朝鮮にて奎章閣（李氏朝鮮の王立図書館）設置

朝鮮（韓国）では、李氏朝鮮第22代国王正祖ことイ・サン即位が即位し、奎章閣（キュジャンガク、けいしょうかく）を設置して、改革に着手しています。これはテレビドラマになっていてファンも多いのではないでしょうか。中国では、清朝、乾隆帝の60年に及ぶ治世が終わりに近づき、乾隆帝の奢侈と十度に及ぶ大遠征の結果残された財政赤字が拡大し、官僚腐敗も進んで清の繁栄にも陰りが見え始めたという時期です。

日本では、江戸時代中後期、10代将軍徳川家治（将軍在位1760～1786）、11代将軍徳川家斉（在位1787～1837）のころになります。家治の時は田沼意次(老中在位1772～86)、家斉の時は松平定信（1758～1829）が幕政を担っていたころになります。その他に、伊能忠敬（1745生まれ）、喜多川歌麿（1753生まれ）などがいます。また、ウィキペディアによると、この時期は江戸時代において、次のように天皇名称の復活が始まった時期でした。

“光格天皇（こうかくてんのう、明和8年8月15日（1771年9月23日） － 天保11年11月18日（1840年12月11日））は、江戸時代の第119代天皇（在位：安永8年11月25日（1780年1月1日） － 文化14年3月22日（1817年5月7日））。傍系であった閑院宮家出身のためか、中世以来絶えていた朝廷の儀式の復興に熱心であった。実父慶光院と同じく歌道の達人でもあった。天保12年1月27日（1841年2月18日）、第58代光孝天皇以来1000年近く絶えていた漢風諡号選定（但し、崇徳・安徳・順徳の各天皇を除く）及び第62代村上天皇以来900年近く絶えていた天皇号（但し、安徳・後醍醐両天皇を除く）を復活させ、「光格天皇」と諡号された。それまでは「追号＋院」という形であった。天皇崩御の後、朝廷から幕府へ強く要望が出され、特例を以て許可された。さらに朝廷は「御斟酌ながら、帝位の御ことゆえ、以後は天皇と称したてまつられるべき」と天皇の名称も幕府に認めさせたのである。”

『国富論』の時代の1776年は、混沌の中に大きく次の時代が始まって、アメリカがイギリスから独立し、その100年後に南北戦争が起きています。同じ時期、朝鮮では、正祖ことイ・サンの改革が始まり、日本では、江戸時代の中後期、徳川幕府が天皇名称の復活を認め、100年後に天皇の世紀である明治へと至っています。

現在、世の中は、混沌の中にあります。アダム・スミスの『国富論』と『道徳感情論』の考え方が、あらためて見直され、研究されているのも、諾（うべ）なるかなと思います。

（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。）

投稿

■【 構築途上にあるシステムへの監査が足りない・・・なぜ？ 】　　会員番号 1143　中山 孝明

会報テーマ「システム監査のすすめ（前号まで）」「システム監査人のやりがい（今号から）」を受け投稿する。開発途上のシステムに対する監査をさらに促しつつ、取り組み甲斐のある仕事からやりがいが生まれるという観点から簡略に述べる。「すすめ」と「やりがい」は相通じる点が多い。

システム構築プロジェクトの失敗事例が多い。

某銀行と某ITベンダーとの訴訟に発展した事例は多方面に大きな衝撃を与え、「動かないコンピュータ」でも多くの事例が報告され、公表されていないことでも自身の身近で起きた、体験したという方も多いと思う。

開発工程に度重なる遅延が発生し泥沼状態に、無理な開発計画と知りつつ担当した、仕様確定を見切り発車した結果・・・になった、などは決して他人事ではなく、「システム構築プロジェクトのほとんどが失敗に終わる」などという声を一笑に付すことができない。

座右の一つのシステム監査基準とシステム管理基準を改めて開いてみると、両基準共通の前文でその目的を次のように謳っている。

> ・情報システムが、組織体の経営方針及び戦略目標の実現に貢献するため
> ・情報システムが、組織体の目的を実現するように安全、有効かつ効率的に機能するため
> ：
> （全文：http://www.meti.go.jp/policy/netsecurity/new_systemauditG.html ）

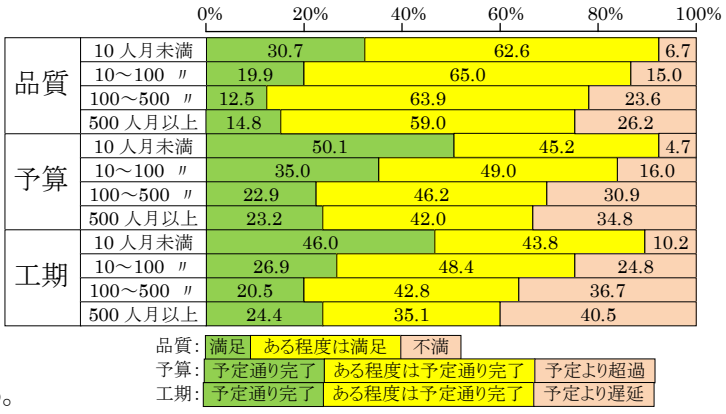
ここに引用するまでもなく、システム監査はITガバナンスの実現を通じて組織の目標実現に資するものであり、システム監査の各種基準・指針・ガイドラインにおいても同様に、経営方針・目標・目的を実現するための監査項目、監査要点が用意されている。

システム監査は、経営者や情報システムの利用者、顧客、システム接続先等々の各層・各分野に役立つものでなければならないなどと回りくどく言わず、システム監査はそこにある問題、システム構築プロジェクトを成功に導くための力を最大限に発揮する必要がある。その力をシステム監査は十分に備えている、と言いたい。

参考データを見てみよう。

システム構築の3本柱であるQCD（品質：Quality、予算：Cost、工期：Delivery）について「企業IT動向調査報告書2012」(JUAS)では右表の結果が表れている。（表はJUAS報告書から筆者作成）

私は、□の部分がそのままシステム構築の失敗事例に該当すると理解しており、さらに□の部分についてもサブシステムの単位や利用部署によっては□と同じ評価の部分が少なくないと理解している。



情報システムの信頼性、安全性、有効性、効率性を妨げるリスクのコントロールが適切であるかを点検・評価する立場のシステム監査は、システム構築プロジェクトの課題に対して何を重点にどのような関与をすべきか。

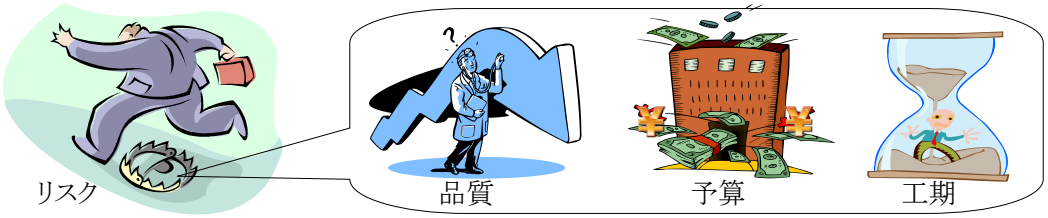
> 現状、構築途上にあるシステムに対するシステム監査が不足していると考えている。
> 急ぎ、構築途上にあるシステムにさらに踏み込んだシステム監査を実施する必要があると考えている。
> 勿論、完成後ではなく完成前に監査することの効果と必要性に疑問を挟む人はいないと思う。

この認識に同調される方は決して少なくないと考えている。

（続く）

構築途上にあるシステムに対する監査が不足しているのは、どの部分か？　なぜか？

ごく自然な感覚で、システム監査の質・量の両面に不足があり、それぞれを充実させる必要がある。そして、被監査側と監査側双方が課題を抱えていると考えている。質はシステム監査の品質、量はシステム監査の実施数だが、質・量のどちらかが被監査側・監査側の一方に起因しているという状態ではない。例えば、開発プロジェクト固有の体制や構成のなかで監査要点に迫れないケース、開発が輻輳している状況で監査に必要な資料やヒアリングが十分に得られないこと、監査対応のためのエネルギーを開発チーム側が割けないケースなどがある。通俗的だが互いに遠慮のようなものが働いていることもあると思う。



システム構築においては、規模の大・小や内製・外製等に関わらず工程管理、品質管理、費用管理など多様なマネジメントと、その下で行われている個別の作業に多くのリスクが内在しており、これらは構築途上で生成され、問題点として出現し、完成品に埋め込まれて世に出る。毎回直面する課題で避けられないものであることを情報システム関係者は不本意ながら確信しており、システム監査の必要性についてはシステム監査関係者のみならず、特にシステム構築のプランニングに関わっている者は認識しているはずである。現在、リスクコントロールが適切であるかの点検・評価についてシステム監査以外の何が担うとしているのだろうか。自問している。

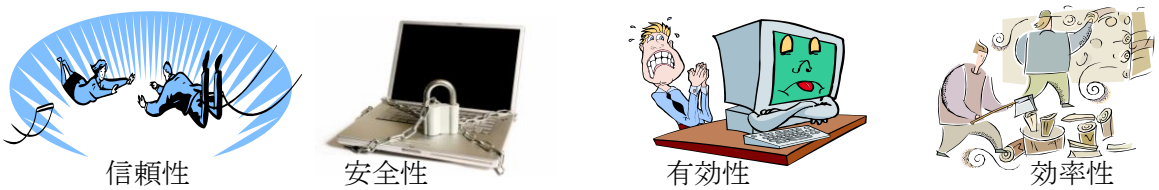
構築途上にあるシステムに対する監査を確実・適時に実施するためには、マスタースケジュールの1項目にシステム監査を挙げ、WBSにも項目を設けて他のWBSと同様に成果物まで明確にしておくことではないか。システム監査を他部署の他人の仕事としてはいけない。余りにも単純だろうか。そんなことは解っているというのだろうか。

もう1点言及する。

構築途上のシステムを監査して問題点や改善事項が表れた場合、つまりシステム構築の作業過程で内在していたリスクが顕在化した場合、それは作業者に起因するのだろうか？　それももちろんあるだろうが、多くの場合は計画や資源、方針・体制などの無理・不足・限界等によると言っても過言ではない。原因がシステム構築作業の従事者の行為ではなく与えられた環境などに起因するか否かにまで踏み込まなければならない。現象面の指摘にとどまってしまってはシステム監査の定着と評価に多くの弊害をもたらすことになると思う。

組織体の重要な経営課題、情報システムの健全な発展へシステム監査が一層貢献すること、そして難題に挑む監査でシステム監査人としてのやりがいを満喫したいと欲しつつ、自身の研鑽すべきことの高さに目が眩む。

以上



新たに会員になられた方々へ

Welcome

平成24年1月1日から9月30日の間に新しく会員になられた方は、45名いらっしゃいます。
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。 http://www.skansanin.com/saaj/
ペンネームによる「めだか」や実名投稿があります。多くの方から投稿いただいておりますが、さらに活発な利用をお願いします。この会報の「会報編集部からのお知らせ」をご覧ください。

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

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

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

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

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

沼野会長一行メッセージ：　“会員の方は、是非、ＣＳＡ、ＡＳＡの資格取得にチャレンジして下さい。”

協会からのお知らせ

■【会員増強プロジェクト（連載中）】

会員増強プロジェクトの活動は、会員の皆様のご協力もいただき、着実に成果を上げています。今月の会報では、事例研と法人部会の活動内容についてご報告します。

今後も、会員の皆様の会員増強活動へのご理解とご協力をよろしくお願いします。

【１．事例研究会の取り組み】

事例研究会の主たる目的は、「システム監査普及サービス」を通じて、会員にシステム監査の実際を経験してもらうとともに、その成果を会員のみならず、広く一般に還元するために、各種のセミナーを実施している。

本研究会では、会員増強プロジェクトの活動に協力するために、以下の施策に取り組んでいく。

1.セミナー受講料の見直し

システム監査実践セミナー（2日間コース）、システム監査実務セミナー（4日間コース）においては、システム監査に興味のある者の会員への誘導策として、従前から会員向け受講料と非会員向け受講料に差を設けてきたが、今年度から「事例に学ぶ課題解決セミナー」（半日コース） についても、会員向けの受講料を1,000円値下げし、4,000円とすることとした。

これにより、会員の同セミナーへの出席を増やすとともに、非会員を入会に誘導するきっかけとすることを期待している。

なお、あわせてリピーターを増やし、セミナー運営を安定化させるため、新規教材の作成や既存教材の見直し（経年による環境変化に伴う更新）にも積極的に取り組んでいく。

2.セミナーの周知範囲拡大

システム監査実践セミナー、システム監査実務セミナー及び事例に学ぶ課題解決セミナーについては、従来は、協会メーリングリストにて会員に周知するほか、ISACA東京支部に依頼して、同会のメーリングリストでも周知いただいていた。

今年度からは、これに加えて、以下の方法により広く周知することとした。

① 日本セキュリティ監査学会（JASA）に依頼して、同会のメーリングリストにて周知いただく。

② 一般のイベント周知掲示板（@ITなど）を利用して、システム監査に直接関与していない人への周知を図る。

③ 試行として、Facebook、Twitter等のSNS媒体を通じて周知し、効果の有無を測定する。

これまでの成果として、事例に学ぶ課題解決セミナーにおいて、従前は当協会やISACAの会員の受講がほとんどであったところ、9月開催の第7回セミナーにおいては、一般の方が@ITを見て、受講された。

3.会員の勧誘活動の実施

システム監査実践セミナー、システム監査実務セミナー及び事例に学ぶ課題解決セミナーにおいて、協会で作成している会員勧誘案内パンフを配布するとともに、クロージングの挨拶の中で、会員になっていただくよう、お願いの一言を付け加えており、新規会員の増加につながることを期待している。

以上

（理事　三輪 智哉）

【２．法人部会の取り組み】

法人部会は協会の法人会員（約30社）から構成される部会です。年間の主たる活動としては自治体や民間企業向けの情報セキュリティやシステム監査セミナーの講師派遣、このセミナーの案内DM発送、経済産業省の「システム監査企業台帳」登録企業への入会勧誘DM発送などを実施しています。また、主として首都圏の会員になりますが、月例のミーティングを実施し、ITやシステム監査に関するガイドライン等の輪読と意見交換行っています。またオフタイムの情報交換も継続して会員相互の交流を深めております。是非皆様のご参加をお待ちしております。

さて、今回会員増強の一環として法人会員をより魅力的にすべく、種々検討を重ねております。それらを以下簡単にご紹介します。

1. 法人会員としてのメリットの増強

例えば法人会員企業の社員であれば月例研究会などの協会主催のセミナーや研究会、教育を一律会員扱い価格で受講できるなどサービスの増強を検討しております。まだ検討段階ですので、是非皆様のご意見をお待ちしております。

2. 「ワークショップ支援サービス（仮称）」の提供による企業内監査等支援の強化

従来から企業や自治体への講師派遣を行って来ましたが、例えば気軽に企業に出向き、監査部門やセキュリティ部門、品質管理やISO等認証事務局などの方々が抱える悩みの相談に応ずるなどといった形のサービスはありませんでした。そこで、協会の様々な知識やノウハウを広く企業にご活用いただくべく、会員増強プロジェクトの一環で「ワークショップ支援サービス（仮称）」を構築中です（会報138号に掲載）。今後法人会員にはこういったサービスを享受いただけるよう進めて行きたいと考えています。

3. ホームページ等の活用

ホームページの会員紹介の充実を計画しています。法人の活動地域を明記したり、システム監査企業台帳、情報セキュリティ監査企業台帳へのリンクも行います。また、一定の期間になりますが、各法人会員の企業や業務紹介欄を設け、情報発信していただくことも計画しております。

以上

（理事　斉藤　茂雄）

■【ISO化推進プロジェクト（連載中）】 2012.10 投稿

投稿　【　ISO/IEC JTC1/SC7/WG40(IT ガバナンス)　Dublin 会議　参加報告　】

システム監査基準研究会ではシステム監査のISO化の動きを支援する活動を行っていますが、ISO/IEC JTC1/SC7/WG40の会議に出席しましたので、概要を報告します。

期間: 2012年9月3日～5日
場所: The O'Callaghan Davenport Hotel, Dublin, Ireland
参加国： ISACA、インド、オランダ、日本、南アフリカ、韓国、オーストラリア、ニュージーランド、アイルランド他、（一部電話参加）：19 名
議長(Convener)：Alison Holt(NZ)、Editor：原田要之助教授(日本)、Kwon, Hyung-Jin(韓国)

会議では、JTC1 の中の WG6 と SC7 (WG40(IT Audit 関係)含む)の統合・再編成、Digital Forensic Readiness、Business Information Management: BISL、ISACA の活動と ISO 関係の対応組織、IT Audit の検討とプロジェクト期間延長などの議題がありましたが、今回は IT Audit に関する、ISO:30120 に関する内容に限定して報告します。

1. ISO:30120 の WD(Working Draft)の最新案に関する検討

現タイトル： IT Audit - Audit guidelines that support the evaluation of the governance of IT

Editor より現在までの進捗と論点が整理されました。内容的には 2012 年 5 月の済州島会議の合意に基づき日本が中心となって作成した改訂版の是非に関する議論です。

しかし、一部の国が主張する「まずは Scope and Nature of IT Audit の範囲に関する合意が必要」との入口論が続き、ISO:30120 が指向する「ガバナンス」層と「マネジメント」層をカバーするガイドラインに対し、一部の国から
a.「ガバナンス」層に対する監査は不可能であり（経営層の指示が間違っていても、マネジメントの問題）、
b.「マネジメント」層でのプロセス PDCA とプロダクトの監査で十分
との主張が繰り返されました。
他の参加国からは日本提案に対する反対表明は見られなかった。 一方、「Audit(監査)」ではなく、ガバナンスがとるべき各種のタスク（EDM モデル）におけるチェックポイントの「Assessment（評価）」を実施することによりガバナンスを支援するという「より柔軟な考え方」には受け入れの可能性も見えます。 後述の OECD 文書でも「Assessment」、「Assessment Criteria」が使われています。

2012 年 11 月 8 日に DTR 採択期限を迎える当プロジェクトを停止するのではなく、ISO:38500:2008 の枠内での IT Audit の基準作りが必要との認識は各国とも共有しているため、新たなオプションとして「Principles」、「Sub Principles」と「Outcomes」を基本とした新たなフレームワークによるアプローチで再構築してみようということになり、その土台として下記を参考として、日本が原案を作ることになりました。

a. ISO:38501: Implementation guide of Governance of IT

b. Methodology for assessing the implementation of the OECD principles of corporate governance

Principles は Responsibility, Strategy, Acquisition, Performance, Conformance, Human Behaviour と変わりません。 Outcomes との対応については Sub Principles を介在させて、より明確にしようとするものですが、どの程度の粒度と内容で定義してゆくかも重要な点です。

2. 日程の見直し

WD の第二版(現状)を 2012 年 11 月 8 日の期限内に DTR まで持ち込むことは実質不可能なため、2 年延長による再スケジュールの可能性を模索しましたが、議長見解で 1 年延長しかできないとのことで、Editor 間で下記のスケジュールを合意しました。 再構築の方式が新概念であることから、一年で計画達成に至るには早期の方向性・フレームワークの合意と、関係者の協力作業が不可欠です。 基準研でも早期に方向性を共有して協力体制を固める必要があります。

2012/10 2W-4W: 日本から新しい提案を行い(一つの Principle をたたき台に)、関係国コメント
2012/11 1W: 関係国ビデオ会議の上、12 月までに案を固める。（全 Principles）
2013/1 2W: WG40/WG6 内でコメントを求め、修正（二週間).
2013/2-4: PDTR 投票（４カ月）

3. おわりに

私は2011年初にシステム監査基準研究会に加わりましたが、当時はISO化関係の検討は初期の段階でした。現在、Working Draftは第二版ですが、次回の会合には第三版として進化させる必要があると思われます。 作業グループ(WG40)では様々な考え方の議論を経て、ドラフトができるわけですが、今回のような大幅な変更を伴うことも珍しくはないようです。 作業グループの参加者は大学、監査法人、IT企業のメンバーなど様々ですが、会合は形式的な場ではなく、どちらかといえば参加者がそれぞれの立場で意見を交換するブレーンストーミングのようなイメージでした。 言い換えれば、現段階は議論が十分煮詰まっていないということもできると思います。
会議に先立つ一か月余りはISO：30120が参照するISO関連の文書を読み、全体の構成や関連の理解に追われました。また、日本側での合同小委員会にもオブザーバーとして参加させていただき、日本側の考え方、方向性の確認をする機会をいただきました。 帰国後は、タイトなスケジュールを維持しつつ、上記の宿題処理をこなす必要があり、基準研の皆さんとの共同作業に従事しております。

（システム監査基準研究会：理事　松尾正行）
（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。 ）

■【SAAJ 会員システム(その 3)】

【事務局】

★SAAJ会員システム　https://www.saaj.or.jp/members_site/KaiinStart

「SAAJ会員システム」Topics

！！2012年10月より、会員情報変更画面のレイアウトが変更されました。

表示されている情報に誤りを発見された場合は

事務局 jimu@saaj.jp 宛にご連絡ください。

会員番号	9910	
氏名	漢字	(姓) テスト (名) 葉ナコ
	カナ	全角カタカナで入力してください。 (姓) テスト (名) ハナコ
生年月日	1960 年 2 月 24 日 生まれ	
入会年月日	2001 年 10 月 1 日	
会費納入日	2012年2月10日	
CSA/ASA認定日	2012年2月27日	
CSA/ASA認定番号	K09999	
有効期限	2014年12月31日	
所属支部	○北海道 ●東北 ○北信越 ○中部 ○関東 ○近畿 ○中四国 ○九州	
紹介会員	会員番号 氏名	
連絡・請求先	●勤務先 ○自宅	

★ＣＳＡ・ＡＳＡの「公開名簿」について

SAAJホームページでは、
CSA/ASAの名簿を公開し

氏名
得意分野
ホームページ

をご紹介しています。

城、栃木、群馬、埼玉、千葉、東京、神奈川、山梨】

	(都道府県)	(得意分野)	(ホーム
一	茨城県	ネットワーク 個人情報保護 オフィスセキュリティ	http://www.tokiw
春	栃木県		
栄	栃木県	ITコーディネータ 業務の見える化、業務改善・改革 システム導入・運用支援	http://www.imc-t
信	群馬県	金融(情報セキュリティ監査) 金融(システムリスク分析)	

公認システム監査人名簿（CSA）：　http://www.saaj.or.jp/members_site/CSAPublicList
システム監査人名簿（ASA）　：　http://www.saaj.or.jp/members_site/ASAPublicList

会員サイトにログインして「個人情報変更画面」で公開設定を変更すると、
ただちに、ホームページの「CSA／ＡＳＡ名簿」に反映されます。

左側メニューから「個人情報変更」を選択。

（マニュアル：16ページ　5【会員情報を変更する場合】）

会員情報変更画面　（最下段）

注意：

① **公開設定を行ってください。**
- **●ホームページに公開　　○非公開**
- **中心的に活動する都道府県**
- **得意分野（3行）**
- **ＵＲＬ**

② **最後に「確認画面」ボタン　→「実行」を押してください。**

公開設定	◉公開　○非公開
都道府県	宮城県
得意分野1	15文字以内　公認システム監査人
得意分野2	15文字以内　ITコーディネーター
得意分野3	15文字以内
URL	http://www.saaj.or.jp/

★次回は！！

ＣＳＡ・ＡＳＡの　資格継続のための「継続教育履歴登録機能」について！！

会員の方が、自ら継続教育履歴を登録できるよう、
システム化を進めています。
次回は、その概要についてご報告致します。

事務局理事　斎藤由紀子

■【会長コラム】

会員増強と並行し、CSA利用促進・価値向上に向けて

会長　沼野伸生

今期もあと残すところ２ヶ月余りとなりました。
協会は、本年２月に開催された第１１期総会で、協会運営の方向性として、以下の３点を挙げました。

（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

現在、この３点を目指し、各部会、研究会、委員会、及び事務局がそれぞれの所管する活動を積極的に推し進め、協会ホームページ、会員メーリングリスト、及び会報等で会員の皆様にその状況をお知らせしています。
また、本年４月に**“システム監査の一層の普及を目指してまずは会員拡大を”**と考え、会員増強PTを立ち上げ、小野副会長のリーダシップの下、ＰＴメンバーの皆さんの尽力、また会員の皆様のご協力も得て積極的に活動し、少しずつその成果も出始めています。

そこで、これに並行し、次の課題は**“大幅に減少するＣＳＡ（公認システム監査人）、ＡＳＡ（システム監査人補）の盛り返し”**と思います。（今年度のＣＳＡ、ＡＳＡ失効者は合計 140 名です。）

今般、力副会長及びＣＳＡ利用推進のメンバーの皆さんにＣＳＡ活性化の具体策を検討頂き、纏めて頂きました。
例えば、
①ＣＳＡの認知を一層高めるための広報の強化
②中央官庁等の入札案件にＣＳＡ資格保有者の配置を条件として入れて貰うようアピール
③各種資格の認定に当たりＣＳＡ取得を評価するようアピール
④システム監査人推薦制度の一層のＰＲ
⑤ＣＳＡの研修機会、相互交流機会の増強
⑥ＣＳＡの認定を受けてない当協会会員にＣＳＡ認定募集の情報をより積極的に案内
⑦ＣＳＡに対しシステム監査関連発注案件情報等の提供
などの検討が挙げられています。

力副会長のリーダシップの下、全ての部会、研究会、委員会等が協働し、会員増強と共に、ＣＳＡの認知向上、利用促進、そしてＣＳＡの増加に繋げていきたいと思っています。

引続き、会員の皆様のご理解、ご協力をよろしくお願い致します。

研究会、セミナー開催報告、支部報告

■【西日本支部合同研究会の結果報告その２　- 個別報告 -　（前号からの続き）】

【講演１】　　報告　№1053 溝田　明美

【講演テーマ】

事業継続計画とシステム監査

【講師】

北信越支部　梶川　明美　氏

【講演内容】

事業継続計画策定におけるシステム監査はいかにあるべきかについて説明された。

以下、内容を紹介する。

１．事業継続計画（BCP）の重要性と計画策定のポイントについて

大規模震災発生に備えた事業継続計画策定の重要性について、社会の意識が高まっているところである。しかしながら、その取り組み状況は組織によって様々であり、いろいろなリスクに応じた対策がある。本格的な事業継続計画の完成には更に長期間を要すると思われるが、しかし、システム復旧（ＢＣＰ発動～全面復旧まで）はシステムの新規構築ではないので、ゼロ（何もない）からのスタートではない。

２．事業継続計画(ＢＣＰ)の範囲について

情報システムに関して効率的な対策を講じるために、事業継続計画策定の３段階を積み上げる。

Ⅰ　ＢＣＰ策定の基盤づくり（ホップ）：ＩＣＴ部門独自で取り組み可能な基本的対策を実施

Ⅱ　簡略なＢＣＰの策定（ステップ）：業務部門の意向を反映した計画を策定

Ⅲ　本格的なＢＣＰの策定と全庁（全社）的な対応との連動（ジャンプ）：多額の投資判断を要する事項について、組織全体で検討を実施

３．事業継続管理（BCM）とシステム監査の役割と着眼点について

経営資源が有効に利活用され、ＢＣＰが適切に行なわれていることを検証する役割がある。システム監査は「組織は今、ＢＣＰ策定段階のどこにあるか」、「ＢＣＰの策定段階にあわせ、それぞれの段階に適合した検討がなされているか」を問う。

【所感】

事業継続計画（BCP）の重要性とリスクとの関係性、事業継続計画（BCP）の範囲や事業継続計画（BCP）のシステム監査のポイント等、非常にわかりやすくコンパクトにまとめられた講演であった。事業継続計画（BCP）の範囲は事業の全面復旧が目的であると同時にシステム監査側からの着眼点が、事業継続計画（BCP）策定段階にあわせて実施すべきであると納得できた。

事業継続計画（BCP）策定や災害シミュレーション等を業務の中で実施されているご経験に裏打ちされた大変良い講演内容だった。

以上

【講演２】　　報告　№1002 居倉　圭司

【講演テーマ】

東日本大震災を踏まえた業務継続面の課題

～ 金融機関の対応を中心に ～

【講師】

中四国支部　協会理事　大石　正人　氏

【講演内容】

2011 年は、現代日本にとって未曾有の災害に見舞われた。それを受け、「災害時における業務継続体制を同整備するのか」という観点を、中小企業ＢＣＰからすれば先進事例ともいうべき金融機関の事例・・東日本大震災の被災地にあった金融機関(東邦銀行・岩手銀行)の事例・資料、並びに日本銀行公表資料・・を基に、金融機関は今どのように取り組みどのようなことに悩んでいるのか、ということを中心に実践事例として紹介。

１．業務継続の重要性と特性

情報システムは個社、自機関の存続にかかわる。また、自らの業務継続は、重要な社会インフラや利害関係者との間で相互依存性を有する。だから、事業継続体制整備や重要な繋がりを有する先方との関係性への対処が必要である。

２．決済サービスにおける金融機関の業務継続への対応経緯

公表資料から、個々の金融機関や業界団体での継続的な取組みや日本銀行などの啓発活動や意見交換を説明され、外部環境の変化への対応状況を具体的に挙げられる。

３．東日本大震災と金融機関や決済システムへの影響

3.11 のインパクトの影響および対応を金融機関や決済システムの事例を取上げて、「初動対応」、「復旧対応」さらに「１年後の教訓」に分けて考察を挙げられる。

４．（改めて）業務継続体制整備の手順

有効で確実に実効できる業務継続体制整備の手順を次のように挙げられる。①維持体制の整備、②業務継続計画の策定、③経営資源等の確保、④意思決定・連絡体制の整備、⑤マニュアルの作成、⑥訓練の実施と計画見直し

５．東日本大震災への対処を踏まえた見直し（事例）

東日本大震災において有効に機能した事例と同震災を踏まえた見直し事例を挙げられる。

６．まとめ（試論）

まず、業務継続体制を整備する個別主体におけるＰＤＣＡサイクルを確立し、重要インフラ事業者などが主体となったストリートワイド訓練を企画・実施する。次に、知見を整理して公表するとともに個別主体における業務継続体制整備へ活用する。

【所感】

紹介された２冊の資料、頭取自ら執筆に当たったという東邦銀行公表資料「震災の総括」、行員それぞれが震災にどう立ち向かったのかという公表資料「震災の記憶」は、非常に生々しい。（この公表資料については東邦銀行 HP を参照されたし。本稿執筆時点ではダウンロード可能）

「電気が消えて、現金が引き出せるかどうかわからない・・という状況に陥ることが、社会不安を招きかねないことを改めて認識した。」（地銀頭取）。社会的使命を担った企業になればなるほど、異例の事態への対応を共有し、その使命をどう果たしていくかが重要である。

この被災地金融機関自身、地道に業務継続体制を整備していた。そのタイミングで東日本大震災のような未曾有の災害に直面した。この金融機関は災害シナリオに「震災」という項目に独立して「津波」というシナリオを持っていた。従ってそのシナリオを発動すれば対処できたのだが、それをもってしても、これほど広範囲の被災に対しては課題が残った。

広域被災、本部中枢機能不全、重要インフラの長期間消失、・・・震災の経験・記憶は、国家レベル・企業レベル、そして個人家庭レベルにおいても、十分に活かしていかなければならない、その思いを改めて認識した講演であった。

以上

【講演３】　　報告　№1167 荒添　美穂

【講演テーマ】

ＢＣＰの観点を意識したシステム監査項目の検討

【講師】

中部支部　副支部長　澤田　裕也　氏

【講演内容】

BCP を対象としたシステム監査を行なった場合に指摘事項としてあがりそうな点を、インターネットに公開されている最新事例も踏まえ検討した結果を説明された。以下、内容を紹介する。

１．計画

ＢＣＰとして計画が中長期より短期計画のみとなる傾向にある。また、経験や知識がない対応計画の作成に燃え尽き、自己満足にとどまり、分厚い資料や体制などの見直しに手が付いていない気配がある。とくに、初動対応の内容や発生時の想定に矛盾がある。

２．初動

手始めとなる危機管理本部の立上げ基準に５Ｗ１Ｈが明示されていなし、主要な関係者への連絡網が最新版に更新されていない。また、初動で必要な機材・システム、それを操作できる要員および参集する要員が被災し、欠けて回らなくなることが考慮されていない。

災害発生時に誰が何を対外報告するかシナリオが準備されていない。

３．本復旧

暫定復旧から本復旧へのストーリがないので、暫定復旧の状態で留まる事態となる。また、本復旧後に暫定側を止める段取りがなく、平常時にはアクセス不可なところが開放されたままとなる。

４．その他（備蓄・訓練・セキュリティ）

一旦揃えた備蓄材に消費期限や自然消耗があるのに管理されていない。また、災害発生時の例外処理が定まってなく、承認・決済をその時誰にするか決まっていない。特に重大なことは、そもそも訓練をしていない。

以上

【講演４】　　報告　№811　舩津　宏

【講演テーマ】

コンシューマライゼーションとその影響

－コモディティ化した商品を活用する情報システム－

【講師】

近畿支部　支部サイトWG　主査　永田　淳次　氏

【講演内容】

コンシューマライゼーションは、コンシューマ市場で展開されている技術（や製品）が企業向け（エンタープライズ向け）で利用されることである。

コンシューマライゼーションについて、３つの視点で説明された。

以下、小職の認識を紹介する。

１．ＢＣＰを容易にする情報システム

ＢＣＰとしてバックアップシステムやバックアップネットワークを構築して運用する計画がなされるが、有事の際、担当者はバックアップシステムやネットワークへの切り替えなどを考慮する必要がある。

コンシューマライゼーションとしてクラウドを考えた場合、バックアップシステムやバックアップネットワークをクラウドで構築した場合、担当者は切り替えを意識しなくてもいいようになる。

ＢＣＰとしての注意点として、事業としての業務の重要性と復旧目標を象限図にした場合、Ｗｅｂやメールなどのコミュニケーションシステムは、一般に重要度が低いが、早期復旧が必要なポジションにおかれるが、実際には、重要システム復旧のためにも必要であり、重要なシステムと位置づけ、普段より投資が必要なシステムである。

２．コンシューマライゼーション

コンシューマ市場の商品（スマホ、タブレット、ゲーム機、ツイッター、フェースブック・・・）は、企業向け商品（ＰＣ等）より機能・性能がよくなっている。製品サイクルが１／ｒ、利用者負担１／ｎ、開発力１＊ｍである。その結果、コンシューマ市場の商品は使いなれた製品となっている。

ＢＣＰは、使い慣れた製品を利用した方が有効である。ＢＣＰのコミュニケーションは、トップダウンではなく、若いデジタルエイジにまかせては。

３．ビジネスエコシステム

従来はハードウエア企業がキーカンパニーとなり、プラットフォーム企業、アプリ企業に影響を与えていた。今は、アプリ企業がバザール方式で拡大し、プラットホーム企業やハードウエア企業に影響を与えている。

ビジネスを生態系に見立てたものである。企業間のネットワークはゆるやかなつながりになり、アプリ企業、プラットホーム企　業、ハードウエア企業の三方よしのシステムが維持されることが重要である。

ＢＣＰ策定が容易な情報システムの選択、避けられないコンシューマライゼーション、健全なビジネスエコシステムの選択の時代であるとまとめられた。

【所感】

コンシューマライゼーションもビジネスエコシステムも初めての言葉であったが、非常に理解しやすい講演だった。

コンシューマライゼーションについては、最近ＢＹＯＤの話をよく聞き、当初は禁止の管理の話が中心だったが、積極利用を図る企業の話もよく聞き、時代がその方向に向かっているからと納得できた。

ビジネスエコシステムについて、汎用機メーカの凋落は周知の事実だが、ビジネスエコシステムの考え方の中で、その立ち位置を認識した上でのコンプライアンスポリシーを含めた戦略も重要とイメージした。

とても気づきの多い講演であった。

以上

【講演５】　　報告　№262 小野　哲夫

【講演ﾃｰﾏ】

インフラ系制御システムとシステム監査

～電力供給系統を支える制御系情報システムの現状とシステム監査の関与について～

【講師】

九州支部　　福田　啓二　氏

【講演内容】

インフラ系制御システムの現状とシステム監査の関与について説明された。以下、内容を紹介する。

１．電力系統と制御システムの概要

火力発電所、原子力発電所、水力発電所から工場や一般家庭への電気は、高圧変電所、送電用変電所、配電用変電所を経由して供給されるが、その系統制御システムはネットワークを用いて監視・制御されている。　電力の安定供給には停電率、電圧の安定、周波数の安定の３つの要素がある。

① 停電率

停電範囲の極小化や停電を最短で復旧させるために短絡や地絡が発生した区間を切り離す保護継電器(リレー)設備が送電網に設置されている。

② 電圧の安定

需要の増加などで電力の流れが増すと需要家側の電圧が低下する。これを防ぐために無効電力や変圧器の調整により系統内の電圧を適切に調整している。

③ 周波数の安定

周波数が変動すると電動機や制御装置、計算機等の動作が保証出来なくなる。

周波数は、生産量と消費量のバランスが崩れると変動する。また、電気は貯蔵できないので、生産量と消費量を監視しコントロールする必要がある。

以上のように電力安定供給のために各地の発電所と給電制御所・変電所間で監視・制御を行う給電システムが構築されている。この給電システムは、二重・三重のバックアップ体制がとられている。

２．大規模停電事故とシステムセキュリティ事故

1991 年以降、台風による停電、大震災による停電、自衛隊機墜落による送電線切断、変電所設備トラブル等による大規模停電事故が発生している。

一方、最近コンピュータウイルスによる鉄道会社信号管理システム停止、自動車工場の操業停止、航空機墜落事故等が発生している。

今後、情報系ネットワークシステムとの関連で電力制御システムもこのようなコンピュータウイルスによる影響を受ける可能性がある。

３．インフラ系制御システムのセキュリティとシステム監査

制御系システムの現場では、PC の持込み／持ち出し、ウイルスチェック、セキュリティソフトの最新版更新の必要性等、セキュリティに対する意識が低いのではないか。

したがって、制御系システムの運用の現場、開発の現場でのセキュリティ意識の向上とともに制御系システムのシステム監査をどうするか検討が必要と思われる。

【所感】

最近、原子力発電の停止により電力不足が発生し、計画停電が実施される見通しだが、電力制御システムの障害による停電発生の可能性については、全く話題になっていない。給電システムは、二重、三重のバックアックシステムにより強固なシステムが構築されているとのことであるが、セキュリティ面で十分な対策が施されているか早急にチェックすることが必要であると感じた。

以上

■【平成 24 年度 北信越支部長野県例会報告】

以下のとおり平成23年度 北信越支部長野県例会を開催し研究報告を行いました。

日時：2012 年 9 月 1 日（土） 13:00-17:00

会場：長野市生涯学習センター

議題:：

- ✧ 報告 1:「アジャイル開発プロジェクトにおける監査ポイント」 麻生 秀明 氏
- ✧ 報告 2:「システムリスク管理の取組について」 長谷部 久夫 氏
- ✧ 報告 3:「事業継続計画とシステム監査」 梶川 明美 氏
- ✧ システム監査研究/情報セキュリティ監査研究意見交換

【報告の概要】

◇研究報告 1

「アジャイル開発プロジェクトにおける監査ポイント」　　報告者（会員 No. 1162 麻生 秀明）

アジャイル開発手法が日本に紹介されてから１０年以上が過ぎた。開発現場でも徐々に実践事例が増え、成功経験や失敗経験の積み重ねによってノウハウが蓄積されてきている。

とはいえ主流はいまだウォーターフォール型開発である。システム開発を生業とする企業にはウォーターフォール型開発に関する膨大な経験知の地層が形成されている。ウォーターフォール型開発が相手であれば、一線を離れた人物にとっても外部からプロジェクト監査を行うのは比較的容易だ。

だがアジャイル開発が相手になると少々事情が異なる。

監査者「設計書はあるのか？」 開発者「必要なら作ります」

監査者「なんだこの右下がりの２本のグラフは」 開発者「これが計画と実績です」

監査者「バグはどれぐらい出たのか」 開発者「テストしながら開発するので数えられません。バグは０です。」

このように噛み合わない。開発者の言っていることは正しいのだろうか。品質は確保されているのだろうか。心配ごとが尽きない。

本報告は、前半でアジャイル開発手法をおさらいしたあと、後半で監査ポイントと考えられる観点を「見積り」「仕様の決め方」「品質」「生産性と進捗」「プロジェクト運営」の５点で整理したものである。理論的な研究ではなく、アジャイルプロジェクトの傍らでチームに
寄り添いながら考えていたことを、この機会にまとめてみた。

以上

◇研究報告 2

「システムリスク管理の取組について」　　報告者（会員 No.1766 長谷部 久夫）

金融機関におけるシステムリスク管理の取組事例について報告した。本年 7 月に適用された改正後の金融監督指針や金融検査マニュアルでは、昨年発生した大規模システム障害の教訓、及びその後に実施された「システムリスクの総点検」の結果を盛り込み、システムリスクに対する認識や障害発生時の対応などを従前より厳しく問うようになった。これを踏まえて、報告者が関与してきたシステムリスク管理の取組状況について発表した。

１．システムリスク管理態勢

（１）組織体制

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・改善態勢の整備に大きな役割を果たしている。またオペレーショナルリスク管理統括部署に情報集約するとともにリスク管理委員会（部長会）で情報共有し、組織横断的に連携して経営陣を支援する体制としている。

（２）規程体系

「情報資産保護方針」および「システムリスク管理方針」を定め、各方針に沿って情報資産保護に向けた安全対策を実施し、適切なシステムリスク管理のための仕組みを整備している。

２．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）

システムリスク管理については、①リスクアセスメント、②リスク管理プログラムの策定、③モニタリング、リスク把握･評価といったＰＤＣＡサイクルを回している。リスクアセスメントにあたっては、予め外部環境の変化を定義しているが、直近では、①インターネットや携帯電話を介した取引等による顧客チャネルの多様化、②システム開発・運用にかかる外部委託業務の拡大、③オペリスク管理体制の整備に向けた社会的要請の高まり（内部統制強化・個人情報保護・業務継続態勢整備）を挙げている。

（２）情報セキュリティ管理

平成１７年個人情報保護法施行に合せて、システム環境が抱える脅威の分析結果と FISC 安全対策基準をベースにセキュリティ要件を定義。その要件を満たすセキュリティ対策全体像を導出し、「セキュリティ対策マップ」に定義して対策を順次実施。

セキュリティ対策では、技術的安全対策のみでなく、開発と運用の相互牽制の確保、システム管理者への研修、および性悪説を前提とした権限の見直しなど、組織・プロセス面の強化に取り組んだ。

（３）システム企画・開発管理等

経営陣は、①開発案件の承認、②要件定義の承認、③開発リスクのモニタリング、④本番稼働の承認、⑤稼働後の評価など、さまざまな局面で開発プロジェクトに関与している。

（４）コンティンジェンシープラン

コンティンジェンシープランを整備し、経営陣による重要な意思決定および指示事項を明確にするとともに、その実効性を高めるため、定期的に取締役が自ら指揮を執る「総合訓練」を実施している。

（５）外部委託先管理

委託先と「サービス契約書」を締結し、役割分担・責任範囲を明確化するとともにＳＬＡ（Service Level Agreement)によりサービス水準を明定している。

改正後の金融検査マニュアルでは、「システムの共同化等が進展する中、外部委託先における顧客データの管理状況を、委託先が監視、追跡できる態勢を整備」することが求められている。これに対応し、セキュリティ管理に係る文書体系を整備し、セキュリティおよび個人情報保護の規程や管理要件書を制定。遵守すべき事項を明定するとともに、契約上も義務を課している。

（６）人材育成

改正後の金融検査マニュアルでは、「システムの仕組み及び開発技術の継承並びに専門性を持った人材の育成のための具体的な計画を策定し、実施」が求められている。将来にわたる技術継承とＩＴ人材の育成は重要な経営課題であり、属人化したルールを技術標準として明定するプロジェクトを立ち上げた。中堅・若手を本プロジェクトに参画させることにより人材育成に取り組んでいる。

３．まとめ

（１）リスク評価（ＰＤＣＡサイクル）によるリスク管理の成果

属人的になりがちなリスクの洗い出し、評価、および改善活動について経営陣が関与する態勢でＰＤＣＡサイクルを実践することにより、①リスクコミュニケーションの円滑化、②予防的な対応策の検討、③費用対効果を勘案した有効な対策実施などの成果が出ている。

（２）今後の取組

システムリスク管理態勢の整備は、システム部門における課題の範ちゅうではなく、主たる経営課題に位置づけられる。リスク管理のＰＤＣＡサイクルの定着化を図り、今後、更に強固なリスク管理態勢となるよう努めていきたい。

今後とも、本会の有識者の皆様方にはご指導の程、よろしくお願い申し上げます。

以上

◇研究報告 3

「事業継続計画とシステム監査」　報告者（会員 No. 0947　梶川 明美）

東日本大震災から 1 年以上が経過し、大規模災害発生に備えた事業継続計画（ＢＣＰ）策定の重要性について、社会の意識が高まっているところである。しかしながら、その取り組み状況は組織によって様々であり、本格的なＢＣＰの完成には更に長期間を要すると思われる。このことを踏まえ、情報システムに関して効率的な対策を講じるために、ＢＣＰ策定の各フェーズにおけるシステム監査はいかにあるべきかを考察する。

１　ＢＣＰ策定の現状

ＢＣＰとは、事故や災害等の発生時にいかに事業を継続させるかについてあらかじめ定めたものであり、組織が危機に陥った場合、影響を最小限に押さえこみ組織存続の生命線となりうるものである。まさに危機管理そのものである、と言える。

ＢＣＰが重要なものであるという認識があるにもかかわらず、なかなか策定が進まない理由として、何をどんな手順で作ればいいのかよく分からない、また策定には大きなコスト（ヒト、モノ、カネ、時間）が必要なことがあげられる。

２　ＢＣＰ策定指針

ＢＣＰは想定するリスクに応じた対策となるが、リスクとその影響の発現箇所は様々である。東日本大震災は、考え得るリスクを広範囲に網羅しているため、対象事象として検討を始めるのが有効であると思われる。

また、最初から完璧なＢＣＰの策定を目指すのは困難である。早急に対策すべきことについて、できるところから始めることがポイントである。

３　ＢＣＰとシステム監査

システム監査は、経営資源が有効に利活用され、組織存続のための事業継続管理が適切に行われていることを検証するための有効な手段である。

「ＢＣＰが適切に策定され、維持管理されているか」をシステム監査の着眼点とし、組織は今、ＢＣＰ策定フェーズのどこにいるのか、それぞれのフェーズに適した検討がなされているかについて監査を実施していく。

(1) フェーズ１（ＢＣＰ策定の基盤づくり）～すぐできること、なすべきことを実施しているか～
体制が作られているか
現状を調査し、問題点を把握しているか
初動対応計画は決められているか
簡易な初動対応訓練を行ったか

(2) フェーズ２（簡略なＢＣＰの策定）～必要なところに、効果的な経営資源の割り当てをしていることを、担保できるか～
組織全体の協力体制はとられているか
被害想定は妥当か

(3) フェーズ３（本格的なＢＣＰ策定）～事業継続管理が機能しているか
組織全体の検討体制はあるか
ＰＤＣＡサイクルの仕組みがあるか

以上

■【近畿支部活動のご紹介】

１．初めに

今年度より近畿支部の支部長をしております林です。今回は、近畿支部の活動についてご紹介させて頂きます。

２．定例活動

近畿支部では、以下の2つの勉強会を定期的に開催しています。

(1)定例研究会

近畿支部会員の方を中心に講師をお願いし、講演会形式で研究会を開催しています。奇数月の第三金曜日の18時半から2時間の講演と、食事をしながらの講師の方を交えた情報交換会の2部構成としています。毎回、講師の選定に苦労していますが、応諾頂いた講師の方には、いつも非常に興味深いテーマで講演をして頂いており、参加人数も毎回、40名前後です。今年の11月の定例研究会で第136回目の開催となります。

(2)システム監査勉強会

本部の月例研究会のDVDを視聴する勉強会です。偶数月の第三土曜日に開催しています。毎回、2本のDVDを視聴していますが、関西在住の会員の方は、中々東京の月例会に参加する機会が少ないため、参加者からは好評です。システム監査勉強会は、今年の10月で第34回目の開催となりました。

３．支部会員向けサービス

近畿支部では、以下の2つのテーマで会員向けサービスを実施しています。

(1)システム監査セミナーの実施

東京で開催されているシステム監査セミナーの教材を中心に、支部独自の資料も使用したシステム監査セミナーを毎年開催しています。セミナーは、体験セミナー(半日)、実践セミナー(2日)、事例セミナー(半日)の3種類です。今年は、実践セミナーが最少遂行人数に達せず、止む無く中止致しました。セミナーWGの皆さんには、事前準備に多くの時間を費やして頂きましたが、残念でした。来年度の開催に向け、今後対応を検討する予定です。

(2)近畿支部サイト(URL:http://www.saajk.org/)の運営

近畿支部会員向けに独自のホームページを開設して、情報提供をしています。支部サイトWGの皆さんのおかげで、今年は内容を充実することができました。具体的には、支部会員へのインタビュー記事の掲載、過去の研究会の資料の掲載等です。また、今年の9月には、支部会員向けのメルマガも発刊しました。地道な活動ですが、今後とも支部会員向けのサービス向上に努めていきます。

４．研究会活動

近畿支部では、現在以下の4つの研究会を開催しています。其々、主査の方を中心に、研究テーマに沿った活動をしています。これらの研究の成果は、昨年度の近畿支部の研究大会等で報告を致しました。来年度以降は、テーマの追加等も含め、更に活性化を図りたいと考えています。

(1)コンプライアランスのシステム監査研究会(システム監査学会との共同研究プロジェクト)

(2)クラウドコンピューテングのシステム監査研究会(同上)

(3)システム監査法制化研究会

(4)BCP研究会

５．関係団体との協力関係

近畿支部では、以下のような団体と連携して活動を進めています。今後は、関西に拠点を置く他の団体とも連携した活動をしたいと考えています。

(1)ISACA大阪支部殿

近畿支部の会員の方には、ISACA大阪支部殿の会員の方も多くおられます。同じシステム監査を中心とした団体として、相互の研究会の参加費を、自組織の会員価格と同じ設定にし、参加し易くしています。セミナーの案内も相互のメーリングリストで案内をしています。また、セミナーの開催日も重複しないような設定にしています。更に、数年前より、12月には合同で特別講演会を開催し、会員相互の交流も図っています。

(2)システム監査学会殿

前述のように、研究会活動においてシステム監査学会殿と2つの共同研究プロジェクトを実施中です。

(3)経済産業省近畿経済産業局殿

近畿経済産業局殿には、近畿支部で開催するシステム監査セミナーの後援をお願いしています。また、セミナーの案内についても、近畿経済産業局殿の関係団体へ案内をして頂いています。近畿支部の活動報告も定期的に実施しています。

(4)ITコーディネータ協会(ITCA)殿

近畿支部のセミナーについて、ITコーディネータ資格の継続に必要な知識ポイントの認定をお願いしており、毎回、認定を頂いています。ITコーディネータの方も、システム監査の知識は必要であり、当支部のセミナーを受講して頂くことで、知識ポイントの獲得に貢献しています。

(5)一般財団法人関西情報センター(KIIS)殿

一般財団法人関西情報センター(KIIS)殿は、1970年に情報化の推進拠点として、関西の財界が中心となり、経済産業省、大阪府、大阪市、地元大学等の支援を受けて設立された団体です。関西地域の産業の発展と地域の活性化に寄与するべく、情報通信技術に関する調査研究、行政・地域の情報化やまちづくり等地域振興に関する調査研究、さらには、国の情報化施策の普及および推進を図るためのシンポジウムやセミナー、健康保険関連業務のシステム開発、情報処理事業等、幅広い活動を展開されています。そのため、当支部のシステム監査セミナーの案内をホームページに掲載して頂き、またKIIS殿のセミナーで近畿支部のセミナーのチラシを配布して頂いています。また、KIIS殿が主催するPマーク審査員研修の案内を、近畿支部の会員に案内するなど、協力関係を築いています。

６．近畿支部設立２５周年に向けて

近畿支部は、1988年3月に設立されました。従いまして、2013年に25周年を迎えることになります。2008年度には、「20周年記念シンポジム」を開催し、また、2011年度には「研究大会」も開催致しました。25周年目である来年度にも、記念となるシンポジウムを開催したいと考えています。開催にあっては、近畿支部の会員の皆様を始め、日本システム監査人協会各位のご協力も頂きたいと考えますので、何卒よろしくお願い申し上げます。

以上

(理事　林　裕正)

近畿支部　第１３３回定例研究会報告　　報告者：No 169　林　裕正

１．テーマ　：　マイナンバー法案によって変わる事業者における個人情報管理

２．講師　：　弁護士法人第一法律事務所　弁護士　福本　洋一　様

３．開催日時　：　２０１２年５月１８日（金）　１８：３０～２０：３０

４．開催場所　：　大阪大学　中之島センター　２階　講義室２０１

５．講演概要

（講師の福本先生より頂いた講演概要を、先生の了解を頂いた上で引用致します。）

「マイナンバー法案」（行政手続における特定の個人を識別するための番号の利用等に関する法律）は、本年 2 月 14 日に閣議決定され、第 180 回国会に提出されている。

同法案は、行政機関等が国民を識別するための「個人番号」を利用することで、社会保障・税に関する行政事務において効率的な情報の管理・利用・授受を実現する「社会保障・税番号制度」を導入するものである。同制度については、従前より国家による個人のプライバシー侵害のおそれに関して議論がなされているが、同法案によって、事業者の行政に対する届出・報告事務（例えば、従業員の健康保険や厚生年金の加入届出の事務等）における「個人番号」の利用及びそれに伴う事業者の「個人番号」を含む個人情報の取扱いに関する新たな義務が事業者に対して課されることに関してはあまり注目されていない。しかしながら、同法案の定める事業者の義務は、「個人番号」を含む個人情報について個人情報保護法よりも厳格な取扱規制であり、事業者による「個人番号」を含む個人情報のデータベース作成も原則禁止されている。その結果、同法案は、事業者における個人情報管理や個人情報を取り扱うシステムの利用に対して重大な影響を及ぼすおそれがあり、従業員・顧客情報に関するシステムに対する監査において新たな視点が求められる。以上のように、「マイナンバー法案」は、4 月 16 日時点においては未だ法律として成立していないが、事業者の個人情報管理に重大な影響を及ぼすおそれが高いことから紹介する次第である。

６．感想

福本先生は、現役の弁護士でありながら、システム監査技術者試験に合格され、また日本システム監査人協会に加盟され近畿支部の一員として研究活動に参加されています。近畿支部の研究会活動の中では、法律の専門家の立場から有益な意見やアドバイスを頂いています。

今回の講演テーマは、概要にもあるように、マイナンバー法案に含まれている一般事業者の個人情報管理に関わる影響を解説されたものでした。一般的には、マイナンバー制度は、地方自治体を中心とした行政組織の情報システムへの影響が大きいと理解されていると思われますが、今回の解説で、その影響範囲がかなり広範囲になることが想定されることが分かりました。もちろん、各事業体の戦略も踏まえ、個人番号の利活用をどの程度まで行うかにより、情報システムへの影響範囲は様々であると考えられます。まだ、法案の成立は不透明な状況ですが、今後の動向をシステム監査人としても注目していく必要があると改めて感じました。

以上

近畿支部　第１３４回定例研究会報告　　報告者：No985　山中修治

１．　テーマ　：ＦＩＳＣ『システム監査指針』（第３版）改訂に向けたヒアリング結果について

２．講師　　：公益法人金融情報システムセンター(FISC)監査安全部
主任研究員　市川千尋　氏

３．開催日時：　２０１２年７月２０日（金）　１８：３０～２０：３０

４．開催場所：　大阪大学　中之島センター　２階　講義室 201

５．講演概要

Ⅰ.「システム監査指針」について

① 金融機関等の「システム監査指針」とは、監査実施時の参考となる手引書の位置付けで、自主基準だが、スタンダードガイドラインとして広く活用されている。但し、「監査指針」のチェックポイントを順守せねばならないとはされておらず、反対に、それらを全てクリアしたからと言って、情報システムリスクの管理体制を保証するものでもない。

② 全体として、エグゼクティブサマリー、フレームワーク、チェックポイント集から構成されている。

・「エグゼクティブサマリー」は、経営者の為のガイドに相当。

・「フレームワーク」は、システム監査の概念、監査の実践及びその実施上のポイントから成り、主に、新任監査人の学習と、ベテラン監査人の知識・理論の整理を想定して記述されている。なお、フレームワークの概念図は、COSO のキューブに対し、三角形で表現されている。

・「チェックポイント集」は、標準ポイント総数 1,101 項目（要点項目、大項目、小項目）で、各金融機関の実情に合わせて、実際の利用に際し増減が行われる。

Ⅱ.「システム監査指針」発刊の背景と経緯

① 昭和 50 年代のオンラインシステム利用の不祥事件多発を契機に、昭和 59 年に FISC が設立、昭和 62 年に米国金融機関検査協議会（FFIEC）作成の「EDP 検査ハンドブック」を基に「システム監査指針」初版が発行（チェックポイント数 560 項目）。

② その後の「COSO」レポート発行や、金融情報システムの小型・分散化、オープンネットワーク化の動きに対応する為に、平成 12 年に第 2 版を発行（チェックポイント数 1,022 項目）。リスクとコントロールの概念を導入し、また、新たにエグゼクティブサマリーを追加した。

③ 現在の第 3 版は平成 19 年に発刊。第 2 版と内容的に大きな変更はないが、その後の環境変化（個人情報保護法、J-SOX）に合わせて内容を見直し。更に、使いにくいバインダー形式から 1 冊製本形式に変更。

Ⅲ.「システム監査指針」を取巻く現状と動向

① 国内では、東日本大震災、サイバー犯罪増加、スマートフォン普及等の動きにより、監査のより厳しい実施が要求され、また、海外では、COSO の改訂があり、実装でのより厳しいチェックが求められる動きがある。

Ⅳ.「システム監査指針」改訂に向けたヒアリング調査の実施

① 平成 21 年調査時の個別ヒアリング実施対象先、及び地域金融機関会員、システム監査セミナー参加会員等に対し、前回改定からの環境変化に伴って、監査指針改定の必要性について意見調査。地方銀行 18 行、信用金庫 8 行、証券、IT ベンダー、等、計 31 社。

② 調査結果

・取捨選択や内容変更を行う等、そのままの形の利用ではないが、「システム監査基準」は広く使用されている（特に、チェックポイント集）。

・東日本大震災等の大規模な障害への対策や、クラウドを始めとする、外部委託サービスの多様化等への対応が、次回の改訂の主要な要因と考えられる。

Ｖ．「システム監査指針」改訂に向けて

① フレームワークは、COSO 改訂、ISO19011:2011、バーゼルⅢを考慮の上、改訂が必要。

② チェックポイント集についても、項目追加（安全対策、外部委託等）、リスク見直し、コントロールの代替案記載、チェックポイントの網羅性向上と重要度付け、及び、リスク、コントロール、チェックポイントの相互の関連性明示等、検討が必要

③ 平成 25 年中を目途に改訂を予定。

６．所感

金融機関の業務において情報システムの重要度が極めて大きいことや、万一、障害が発生した場合の、社会全般や市民生活に対する影響度が大きいことが、一般に認知されている為、金融機関等のシステム監査に否定的な意見は殆ど無いと考えられる。

また、金融機関の情報システムの規模は、一般企業と較べて、格段に大きいことが普通と考えられるが、一方、その業務手続内容や処理の流れは、取扱商品の種類が多彩とは言え、その個々のものについては、国際的にみても、共通性が高く、高度に標準化・定型化されていると考えられるので、監査手続き的には、監査を受ける側も、監査する側にとっても、ある程度、こなれたものになると想像できる。

更に、金融機関は、一定以上の規模が必要な業種であり、例外を除いて、資金的にも、人材的にも比較的恵まれているケースが多く、監査はかなり効率的に実施が可能で、結果として、費用対効果面で考えても高いのではないかとの印象を持っている。監督官庁の強い指導力もあって、金融機関のシステム監査はやはり、別格と思われる。

これに対して、システム監査一般で考えてみれば、日本でシステム監査が提唱されてから、相当の年数になるが、大企業を除けば、未だに、システム監査が十分な市民権を得ているとは思われない。

全くの個人的意見で恐縮だが、システム監査の制度化については、法令による強制実施化推進はもちろん重要だが、監査を受ける主体やその利害関連者に対して、効果・メリットが判り易い客観性や計量化（金額評価、確率やカバレッジ）によって、有用性を具体的にアピールできることも重要ではないかと思う。

以上

近畿支部　第１３５回定例研究会報告　　報告者：No1709　荒町　弘

１．テーマ：　地方自治体の基幹システム再構築におけるＳＬＡ（サービスレベル・アグリメント）について

２．講師：　　近畿大学経営学部　津田　博　先生

３．開催日時：２０１２年9月２１日（金）　１８：３０～２０：３０

４．開催場所：大阪大学　中之島センター　２階　講義室２０１

５．講演概要

平成の大合併を経た地方自治体ではここ数年の間に基幹システムの再構築の動きが活発になっており、自治体クラウドによるシステム構築事例が増えつつあります。従来からも自治体における基幹システムの安定的な運用は常に最優先の課題ですが、システムの構築形態（自己開発・パッケージ導入）や運用形態の多様化、そしてＩＴ部門職員の人員構成やスキルなども変わっていく中、その課題はより一層大きなものになっていると考えられます。

自治体が運用するＩＴシステムの品質維持と向上のためのツールとしてＳＬＡ導入があり、今回、津田先

生が自治体に対して実施したアンケート結果とその分析結果をもとに、ご講演をして頂きました。

ご講演の内容は、主に、「調査の背景」「自治体のＳＬＡ導入について」「アンケート調査と結果の分析・集計」「ＳＬＡの定義」「ＳＬＡに関する成熟度モデル」「まとめ」という流れで行って頂きました。

自治体クラウドの採用は、正に「所有」するＩＴから「利用」するＩＴへの移行であり、標準的なパッケージソフトを複数団体で利用することで３割のＩＴコスト削減が期待されているとのこと。その一方で、業務を標準ソフトにどれだけ合わせられるかという利用部門における問題と、ＩＴサービスとしてのレスポンス等の品質保証をどのように行うかというＩＴ部門が担当する課題が可視化されてきていること。そして、ＳＬＡを細かく定義した場合の利用団体、サービス提供企業双方のメリットやデメリット等についても具体的に説明して頂きました。

実際にＳＬＡを導入し運用している自治体はまだ数が限られており、管理する自治体側にも相応の負荷がかかることから、実際には人口規模で１５万人以上の自治体でないとまだＳＬＡの導入は負担が大きいのではないかというコメントや、西日本では努力目標型のＳＬＡが多く、東日本ではペナルティ有の目標保証型のＳＬＡの方が多い傾向にあること等も教えて頂き、大変参考になりました。

質疑では、「全国の自治体に一律に適用できる標準的なＳＬＡを策定して欲しい」という希望や、「コスト削減に逆行しない程度のＳＬＡのコスト感について」の質問、「ＳＬＡを細かくすることで対応できるベンダーが限られるというベンダーロックの恐れはないか」等の各種質問が出ました。

是非とも津田先生には、更に多くの情報の分析をして頂き、全国に標準適用が可能なＳＬＡの基準について、ご教示頂きたく思いました。ありがとうございました。

以上

■【第１７４回月例研究会受講報告】

会員 No. 6005　斉藤 茂雄

日時　　2012 年 8 月 29 日　18:30～20:30
会場　　機械振興会館地下２Ｆホール
テーマ　事業継続マネジメントの現場・現実とは
講師　　株式会社　富士通総研（ＦＲＩ）
　　執行役員　第二コンサルティング本部　ＢＣＭ事業部長　伊藤　毅　氏

【講演骨子】

3.11 の東日本大震災を被災し、日本企業の被った被害は物理的被害やビジネス停止による機会損失などに加え、グローバルな視点からは日本企業の事業継続能力に対する信用低下にまで繋がり、その影響は甚大である。このような状況から形式的な BCP の策定ではなく、真の「事業継続能力」が求められるが、調査によると BCP に取組まない理由として「（自企業内に）策定に必要なスキル・ノウハウがない」という声が多い。これは事業継続の真の意味を理解しないまま、形式的な手続きだけを求められているといった誤解からきている。

BCP が無いとどうするか。10 年前には大概の企業は BCP を持っていなかった。この状況で被災したら何もしないでいた訳はなくて、皆が集まり、何を優先しやらなければいけないかを考え、対処したはずである。これは当たり前のことである。ただ、昔はこれで良かったが今は平常時のビジネススピードが速くなり、ビジネスが停止した時の影響が格段に大きくなってしまった。従ってその時に集まってでは遅く、事前に準備しておかざるを得なくなった。この当たり前のことを頭に置いて、準備し、訓練する、これを繰り返すことが事業継続能力を高めることであり、そのための管理プロセスが BCM である。

（報告者要約）

【講演概要】

１．経営を取り巻く危機環境の変化

世界の自然災害と経済損失をまとめた資料があるが、1995 年の阪神淡路大震災、2005 年のハリケーンカトリーナ、今回の東日本大震災・タイ水害で突出して経済的損失が発生している。ここで考えておかなければいけないのは、被害には直接被害と間接被害があることである。設備・建物の復旧、再調達、取引先・委託先変更による追加費用、緊急節電対応による機器・拠点移転などといった直接被害は比較的分かり易い。また、ビジネス停止により発生した売上減、機会損失や納期遅延によるペナルティといった間接被害までは比較的想像がつく部分である。ところが実は非常に大きい間接被害というのが、「日本企業の事業継続能力に対する信用低下」である。

10 年ほど前、海外で BCM についての要求事項をヒアリングして回ったことがあるが、日本は地震国で、英語にまでなった「津波」という言葉がある国で、素晴らしい工業国なのだから、既に優れた対策をしているだろうというのが海外の認識だった。ところが今回そうでない事象が露呈してしまった。この事実が非常に大きいと感じている。

帝国データバンクの「BCP についての企業の意識調査（2012 年 3 月 27 日）」によると、5,990 社の調査で 1 ヶ月以内に復旧は 2,680 社（44.7%）、復旧に 1 ヶ月以上かかったが 3,310 社（55.3%）、復旧に半年以上かかった企業は 1,617 社（26.9%）である。日本人の感覚ではあれだけの災害の中でよく 1 ヶ月で再開したと思ってしまうが、停止期間だけ見たらひどい状況である。ビジネスの世界はドライであり、1 ヶ月もビジネスが止まったという事実を考えなければならない。実際、海外の取引先から BCP の状況を問い合わせて来ており、日本でも取引先全てを集め、各社に真の意味の BCP を提示させる企業が出てきた。形式的な BCP ではなく事業継続のパフォーマンスを求める動きが、昨今の経営環境（危機環境）となりつつある。

2. BCM とは何か

内閣府が出している平成 23 年 11 月調査の「BCP の策定状況」では、大企業の 72.3%、中堅企業の 35.7%が取り組んでいるという数字になっている。BCP については定義がはっきりしていない側面があり、色々な数字がありすぎるが、72.3%という数字には本当にそうだろうかという疑念もある。

同じ調査に「BCP に取り組まない理由」というのがあり、「策定に必要なスキル・ノウハウがない」というのがトップで、回答企業 284 社の約 50%を占める。これはおかしなことだと思う。被災した時、どうやって業務を再開するか分からないはずがない。BCP がないからと黙って見ているビジネスマンは居ない。こういう回答が出るのは BCP についてのお作法を言い過ぎているコンサルタントの責任かも知れない。このことが問題であり、この誤解をいかにほぐすのかが BCM の普及にとって必要なことだと考えている。

ISO22301 が正式発行されたが、マネジメントシステムを構築したからとか認証を得たからそのことで BCM のパフォーマンスが十分とは言えない。特にいざという時に使うかどうか分からない文書を沢山作ったり、ゆっくりした PDCA は本来の BCM の目的ではない。「事業継続能力＝目標時間内に再開できる力（パフォーマンス）」が重要であることを忘れてはならない。

BCM の本質は「事業継続力の強化」にある。つまり、災害や事故、突然の業務停止、その他急激な経営環境の変化などの、①危機的状況が発生することを前提に②事前にどのように行動するかを明らかにし③迅速な合同ができるように準備をしておくことがすなわち BCM の取組みである。

次に、リスク管理と BCM は違う概念であると考えている。リスク管理は「想定内」を前提とし、発生確率と影響度の評価から対応を決める。リスク管理は「想定内」を対象とするため、リスク管理の対象を定めたとたんに「想定外」が生ずる。BCM の領域は、発生確率は低いが損失の大きいものが主に管理の対象となる。対象には「想定外」も含む。原因や発生事象に不確定要素が多いため、発生を前提に損失の減少・早期再開に重点を置く。「想定外」に対しては代替手段を持つことが効果的である。

3. 富士通の対応事例

富士通の工場では、デスクトップパソコンの製造工場である富士通アイソテック（FIT）が震度6弱の地震に被災した。富士通では、富士通アイソテックの被害が甚大であったため、ノートパソコン専門工場の島根富士通で代替製造行うことを決定した。それでは富士通の BCP はどうなっていたのか。

それぞれの工場は、デスクトップパソコンとノートパソコンの専門工場であるが、当然ながらパソコンという事業を考えた時、コスト的に双方の工場に代替生産できるような設備は用意していない。しかし、もしそれぞれの工場が代替しなければならない時、何をしなければいけないかは分かっていた。富士通アイソテックでは 2007 年に BCP を策定し、役員から現場まで過去 40 回以上の実働とシミュレーションを織り交ぜた切替え訓練を実施していた。

3.11 では被災してすぐに、福島と川崎と島根の3箇所に対策本部が立ち上がった。実際は4tトラックに支援物資を積んで福島へ向かわせ、福島から設備を島根に運んだ。この時何を島根に運べばよいのか、何を新たに調達しなければならないかは分かっていた。情報システムは二つ別々だということも分かっており、データは移行出来ないので手入力が必要だと分かっていたので、即日川崎から島根に要員が派遣できた。この何をしなければならないかということが明快になっていたのが富士通の BCP である。特別にお金をかけていない。代替手段というのは金を掛けて別の場所に同じ設備を用意するということだけが答えでないということである。

今回の場合 12 時間後に島根工場に切替える BCP を発動できた。その時島根工場の何を停止しなければいけないかの優先順位のカテゴリも決めていた。このように 12 時間で判断したので、12 日間で業務再開できたが、もし BCP が無く初動が 24 時間 遅れて 36 時間後に発動していたら、災害時行動記録分析結果により、再開に 30 日はかかったと予測できる。初動の 1 時間の遅れは再開の 1 日の遅れに繋がる。なぜなら皆で経営資源を奪い合うからであり、それは水やガソリンの不足で社会生活面でも経験したことである。つまり BCM の初動はタイムマネジメントとも言える。

4. BCM の4つのポイント

BCM でやるべきことは次の4つに集約できる。

① ボトルネックへの集中的な事前対策

壊滅的な被害を受けた時に、普及にどの位時間が掛かるかを普段から考えておくことが重要。考えたなら復旧を長期化させるボトルネックを見つけ、ボトルネックをいかに短縮するか、ボトルネックへの集中的な事前対策が重要である。半導体製造工場であればクリーンルームかもしれない。製造工場であれば金型かもしれない。情報システムの場合はデータの復旧など。

② 復旧のみでない代替戦略オプション

ボトルネックを含め壊滅的にやられたらどうするか。完璧な代替手段は用意できなくとも、少なくとも対応スピードを速めることを考えておくことは出来る。状況に柔軟に対応するため、複数の戦略オプションを常に準備する。対策が未実施でも、継続方法と課題が明確になっていれば、対応時間は大きく短縮する。なんでもかんでも2重化は出来ない。災害対策は費用対効果策でもある。事業において「お客様に提供すべきは価値」と考えれば代替手段は沢山出てくる。極端な話、お客様やライバル企業で代替してもらう方法もある。いずれにせよ、そのときになって考えるのでは遅いので、事前に準備しておくことが重要である。

③ 発災 24 時間以内の初動と意思決定

24 時間以内の初動と 24 時間以降は考え方が違うことを知らなければならない。24 時間以内は被害状況が違っていても対応は共通的である。初動は出たとこ勝負という考えは通用しない。必要業務量に対して人的資源が大きく枯渇するのがこの段階なので、優先順位付けと訓練による特定の人に依存しない共通的な対応が出来る備え、つまり動ける人材とルールつくりが重要である。

24時間以降は、状況変化に応じて適宜柔軟な対応が必要となる。先のことはどんどん変わるので、決めておいても使えないことがある。

④ 現場主体の訓練と改善の繰り返し

どんな状況でその時何をしなければならないのか、その対応時間を短くするにはどうするのか、いわばチェックとアクションの繰り返しを徹底的に訓練するのが重要である。富士通ではそのための実践的な訓練（シミュレーション訓練）を提唱している。シミュレーション訓練では、事前に訓練シナリオを知らせない。次から次と災害時の事象を提示し、それをやるには今の状況で何が出来るか、どの位時間がかかるのか、何がネックになるのかをひたすら考えさせる。これにより、危機発生時及びその後の対処方法の計画性が「必要かつ重要なこと」であることの気付きを促す。

5. 情報システムへの対応

3.11 で明らかになった IT 部門の課題は色々出てきているが、当たり前の最低限の対策ができていなかったということが大きい。物理的対策としてデータの外部保管の問題、免震床などの構造対策などもあるが、大きな問題は業務継続観点での IT 構成管理が出来ていない点である。事業継続すべき重要な業務で使っている情報システムの範囲が明確か、重要業務のアプリケーションが何か分かっているか、そのアプリケーションを動かす構成は？サーバが色々なところにあって、何をどこで使っているか分からなくなり、何から手をつけたら良いかわからなくなっていないか。サーバのみならず、クライアント PC は、そこで動くローカルアプリケーションは、その PC のセキュリティは、LAN は、ネットワークは。つまりこれらの関係性（構成）を明確にしたトータルに考えた構成管理が必要である。

また、システムの復旧についてデータのバックアップは当たり前になっているが、しかしバックアップが目的化していないだろうか。バックアップはデータ保全のためではなく、システムの停止状態から業務を再開するためにある。そのためにはバックアップからの戻しの訓練が必要であるが、どの程度実施されているだろう。こういった当たり前のことが出来ていないことが、3.11 で明らかになった課題である。

3.11 以降新たに発生した課題として、今まで BCP が出来ていなかったので BCP を作ろうとすると現場の業務再開に対するシステム要件が勝手にどんどん定義されてしまい、情報システム部門ではとても対応できない事態が起こるというケースが想定される。これについては CIO がイニシアティブを取り、情報システム部門が仮説ベースの対

策コストを算出するなどあらかじめ IT－BCP を策定し、業務部門と調整することにより課題解決すべきである。

6．ポスト 3.11 の BCM

事業継続に形は無いと考えている。どうやるかは企業により異なるので、BCM や BCP という形を与え、それに企業が合わせるのは間違いである。監査の視点でもそのように見て欲しい。BCM、BCP を監査するとするなら形を見るのではなく、いかにその企業が速く事業再開ができるかという点に着眼すべきである。これは丁度その企業の経営が正しいかを評価するのと同じくらい難しいことだと思う。

次に BCM への取り組みの視点として、これまでも話したが、How（どうやってやるのか）から入ってしまい、ガイドラインやハウツウ本に頼ると BCM は出来ない。Why（なぜ取組むのか）から入り、What（何を目的にするのか）、Who（誰がやるのか）Where（何を対象とするのか）When(いつまでにやるのか)そして How（どうやってやるのか）でないと BCM は出来ない。なぜならば、その企業ごとに BCM は違うからである。

最後にまとめると、組織がやらなければならないことは、事業継続能力すなわち速く復旧回復できる能力を身に付けることである。それを実現するには3つの要素がある。一点目は「ハード」で、なるべく壊れないようにしておく、壊れたときでも被害が少なくなるようにするということ。例えば情報システムでは二重化やバックアップである。二点目は「ソフト」で、いざという時に速く動けるよう体制・役割分担、マニュアルや手順を準備しておくということ。三点目は残念ながらいくらそういうことを決めておいても被災時には異なる事象が起きてしまうので、その時に柔軟に判断して速く動ける組織の能力、個人の能力を磨くことをやっておくということである。

いままではハードを強化し、それに伴うソフトを作り、その下に人が動けるようにトレーニングするというアプローチだったが、今日申し上げたアプローチはその逆で、いざという時にどんなことが起きるのかみんなで発想し、その時自分たちがやらなければならないことは何か、そしてそれを速くやるにはどんなソフト・ハードが必要なのかという具合に考えることである。そして危機というのは災害事象だけではなく、今日の非常にスピード化した経営環境そのものでもあり、このような激変する経営環境の変化に対する取り組みもやはり BCM なのだと理解すべきである。

【感想】

3.11 以降 BCM、BCP の事例はいくつか聴講したが、今回ほどしっくりと身についたお話は無い。身近な事象も含め、いかに 3.11 に BCP が機能しなかったか。例えば多くの会社で非常時の水や食料・備品を備蓄しながら、「BCP の発動者不在のため」にそれが供給されず不自由したという話を聞く。これなども BCM が一部の担当者の形ばかり仕組みとなっている結果であろう。恐らくそういった企業では BCP は機能しなかったのだと思う。今回のお話を通じ、何故このようになり、何を反省しなければならないか、監査人として何を見ていかなければいけないか理解出来た。

終わりに、今回のご講演はお話が多岐に亘り、非常に情報量に溢れた内容であった。報告者の力不足で、この内容をうまく皆様にお伝えできないことをここでお詫びいたします。

以上

■【第１７５回月例研究会受講報告】　　会員 No. 1690　梅里 悦康

講演テーマ：　「新しい時代のシステム監査を考える」
講師：　東京海上日動システムズ株式会社　代表取締役社長　横塚 裕志 氏
日時：　2012 年 9 月 27 日(木)18：30～20：00
場所：　機械振興会館　地下 2 階　ホール

■講師紹介：
1972 年：東京海上火災保険株式会社入社、一貫して情報システム部門に従事して、情報システム部長、執行役 IT 企画部長等を歴任
2006 年 7 月：東京海上日動システムズ株式会社　代表取締役社長
現在、東京海上日動火災保険株式会社　常務取締役でしたが、同社を退任しシステムズの社長に専念
著書として「ＳＥよ大志を抱こう」、「日経コンピュータ」の連載記事の掲載があります。

＜講演骨子＞

情報システムの目的が、「効率化」から「ビジネスへの貢献」に大きく変化している。「エンタープライズＩＴ」とスマホを中心とした「コンシューマＩＴ」とが連動を始めた。この新しい時代において、情報システムに関するリスクの捉え方、情報システムによる価値創造の考え方など、情報システムを取り巻く価値観が大きく変化している。変化の激しいアメリカでの最新動向を取り入れながら、新しい視点から、システム監査の新しい役割を考えてみようと思います。

＜講演概要＞

システム監査への期待

ここ最近ビジネス環境は大きく変わり、内部監査・システム監査と経営との関係は大きく違ってきています。従来、システム監査は、情報システムの安全・リスクについてチェックをかけ、ブレーキをかけています。新しいシステム監査は情報システムを有効に活用することで、アクセルを踏みます。2012 年 7 月 IIA（報告者注：The Institute of Internal Auditors／内部監査人協会）国際カンファレンスで、内部監査、システム監査は経営戦略を推進する Catalyst:触媒、応援団たるべきとされています。IT ガバナンスカンファレンスでは、Cobit5 の IT に係るリスクについては、大きく考えを変えてきています。新しい技術・新しい IT にチャレンジしないことが最大のリスクです。

東京ガールズコレクション×システム監査＝　？

企業サイドがいい製品と思って作りこれを買うビジネスモデルから、お客様が自分の好きなものを選んで買うビジネスモデルに変わっています。ソニーのウォークマンとアップルの iPod では、ウォークマンは音を聞くという品質では上かも知れません。しかし、そういうことではないです。iPod は聞きたい曲を 1 曲ずつダウンロードして聞くことにお客様は価値を見出し、世界を席巻しました。

大きな変化

世界で名だたる企業はシステムを武器として使っています。システム監査はそういうことに貢献していかなければなりません。お客様に選んでもらう観点からは、システムの目指す品質はバグがなくなっているかでは

なく、いかにお客様にウケるシステムか、いかにスピードがあるかに品質が変わっています。

業務効率化→ビジネスへの貢献

業務効率化からビジネスへの貢献が世界のトレンドです。先週、セールスフォースコンファレンスでは、大きな企業のビジネスサイトの CMO、CEO で、ビジネスモデルをこう変えたので、ビジネスを拡大したと話をしています。

社内→コンシューマー

ついに、コンシューマー向けスマホアプリを作ることになりました。要件→外部設計→プログラムテスト→システム出来上がりでは開発できません。ウォーターフォール開発はできず、アジャイル開発しかありません。

情報システムのリスクとは何か？情報システムの価値とは何か？

お客様にどう価値を感じていただくか、保険銀行がスマホアプリを開発しています。情報システムが決定的に違ってきています。情報システムをいかに経営戦略として使うか、企画、情報システム部門、営業部門が一致団結していかなければなりません。システム監査はシビアなことを求められます。情報システムの価値を新しい時代のなかで考え直していくことから始める必要があります。

システム監査も大きく変化する必要がある。情報システムが経営にとって効果的であるか？システム監査の新しい視点

情報システムが経営にとって効果的であるかどうか？重大なポイントです。効果的であるようにシステム監査は触媒として経営にアドバイスします。内部監査、外部監査は経営者のモニタリング機能として大事な機能です。

開発テーマの優先順位は、経営戦略と一致しているのか？優先順位を決めているのは誰か？声の大きな部門を優先していないか？

開発にノミネーションされたテーマが、経営戦略と一致しているのか？はかなり難しいです。どういうプロセスで、どう経営戦略と照合し、一致させるか問題です。最終的には取締役会で決定していますが、声の大きな部門を優先していないか？　リソースの大きな部分が意外と優先順位が低いです。決まっているもの、開発規模を見積しやすいものを優先しがちです。

会社のなかに優先順位を決める仕組みがあるか？その仕組みが機能しているか？そこが基本です。経営戦略と一致していない開発案件はマネジメントがうまくいって、トラブルなく完了しても経営にとって意味がないです。システム監査にそこをモニタリング機能にて機能しているかみてもらうことです。

当社は 2004 年から 10 年かけて全面再構築しました。全面再構築はリスクが高いと評価され、案の定、プロジェクトは遅延し、プロジェクトは予算オーバーしました。遅延したのを現場の方に申し上げたときに、「システム構築は 1982 年以来 20 何年ぶりなので、何年遅れても、使いやすいシステムを使えることは価値が高く、少しの遅延は何でもないです。」と現場の方にいわれました。

開発テーマ・要件は、ビジネスに効果的か？ビジネスサイドの関与が行われているか？シンプルな要件になっているか？

開発テーマ・要件は、ほんとうにビジネスに中味で重要で効果的か？　よく要件をみているとビジネスに貢献していないのでは？　政府が作っている情報システムはほとんど有効に機能しないといわれ方をしています。

IT になるとビジネスサイトは IT 部門にまかすということになるから IT 部門としてきちっとしたものがないと IT 部門が IT ベンダーに丸投げ、スマホ、タブレットで作っておいて丸投げで、IT ベンダーがそれぞれの思いで作ります。誰も使わないシステム、まったく意味のない経営的に効果のないシステムになります。

ビジネスサイドの関与が行われているか？IT をどう使ってビジネスをするかは極めて重要な仕事です。クラウドをどう使うかビジネスサイドで考えているのと考えていないのとではどっちが強いか明白です。IT をビジネスの道具としてどう使っているか監査してほしいです。

シンプルな要件になっているか？例外操作極めて細かい。情報システム部門はことわりにくいです。シンプルでコストを下げスピードを上げ、現場が最初はシンプルでいいのではといってもらえるとありがたいです。3 年でなく半年で提供し、反応を見て改善する、アジャイル開発しかないです。システム監査にアクセルを踏んでもらいたいです。

現場で使われているか？

どのようなふうに使われているか、システム監査でモニタリングしてください。現場に 1 通のみの通達では伝わらないです。実際にシステムを使用する代理店さんの販売店 46,000 店に「新しいシステムできました。」とどのように伝えるかです。現場に行って、どの様に使われているか、なぜ使われていないのか経営に報告してほしいです。

会社全体として、新しい技術情報にチャレンジしているか？

リスクコントロールは重要ですが､新しい技術にチャレンジしていかないと会社はものすごく損失となります。個人個人にてチャレンジではなく、組織としてチャレンジ、組織として新技術の取り込みに遅れます。プロセスとして、個人個人にチャレンジを課していますでは機能しません。会社として進化がないです。

あなたの会社は IT を活かそうとする文化がありますか？

IT を活かそうとしない、会社は世界で戦えないです。IT をどう使うか、より IT を使ってどうビジネスをするか。ビジネスサイトが真剣に考えます。そういう文化の醸成を経営はやっていかなければなりません。システム監査により会社の競争力が上がっていきます。

＜主な質疑応答＞

1.　システム監査の実施タイミング

Q：お話いただいたシステム監査は、従来のシステム監査とはイメージが大きく変わっている。従来は、企画工程が終わったなど、ある区切りでシステム監査をするのが普通であった。今日うかがったシステム監査はどのようなタイミングで実施することになるか。

A：改善のフォローアップも効果が上がらないと思うので、年中実施（いつでもモニタリング）をしていただきたいです。

2. BCM/BCP

Q：貴社のグループで BCM/BCP はどのように構築しているか、実際はどうなさっていますか？

A：データセンターのバックアップ、ネットワークバックアップはシステム部門が当然にしています。ビジネスプロセス側を災害に強いものにするかはビジネスサイトとシステム部門がコラボして作っています。当社は多摩センター、千葉センターを持っています。東京電力計画停電に対応する自家発電は面倒です。データセンターを持つことはできれば避けたいです。基幹系システムを全部委託することは、経営上議論が必要です。

3. システムが使われているか否かの検討する主体

Q：これまでのシステム監査とは大きくイメージが異なる。システムが使われているかどうかは、システム企画部門、経営企画部門と違って、なぜシステム監査人なのでしょうか？

A：もちろん主体は経営がやるべきですが、システム監査人にモニタリングして、応援してほしいです。経営がきちっとやっていないことが多いです。

4. クラウド、スマホで、システム監査にて注意していなければいけない視点

Q：クラウド、スマホにテクニカルなところで、システム監査にて注意していなければいけない視点、観点でなにかあれば、お聞かせください。

A：リスクは２つで、安定稼働と顧客情報（セキュリティ）です。クラウド、スマホは同じです。委託先が安定的に稼働しないとき監査ができるかチェックすべきです。クラウド、スマホはいかに顧客情報が漏えいしないかです。委託先選定に課題があります。

5. クラウドに対する監査

Q：クラウドは、監査が非常にやりづらいです。SAS70 で ASP 業者が監査したものをお客様に提供すべきでしょうか。団体の動きはどうなっていますか

A：クラウドの監査は課題です。難しいと思います。データセンターのデータ消失事故もあります。セールスフォースに委託して、現地調査、調査権を留保して契約しています。政府関係の団体がチェックし、そこのお墨付きがあればよろしいかと思います。

6. システム監査人の育成、経営企画、マーケティング等の経験

Q：提言があります。システム監査人の育成の根幹にかかわった問題を含んでいると思います。伝統的に、システム監査人は経営企画、システム企画、マーケティング戦略、そういう経験を持っていません。経営戦略、経営企画の経験を持たせ､権限責任を持たせ､育てる意識づけしないと実現できないです｡システム監査人は、ほとんど大きなシステム開発プロジェクトを経験していなく、企業経営の経験もなく、CIO は名ばかりで財務企画と一緒になってやっています。人の問題が多いです。

A：内部監査部はそういった経験がなくとも円滑に進むと思います。人材は東京海上システム監査、SE 経験だけで、マーケティング経験はありません。ヒヤリング、モニタリングで実践が能力を育成します。そういう方向感でやっていいと経営が承認すればいいです。そういう分野に徐々に入っていくことが自然です。

7. システム監査の具体的事例―使われていないシステム

Q：東京海上システム監査の具体的事例があれば、システム監査の内容、テーマ、監査の結果、経営者への報告の事例があれば、お聞かせ下さい。

A：あるシステムを取り出して使われ方が想定通りか否か検討しました。発注部門、現場にモニタにしてシステムは使われていない。ビジネス部門はなぜか検討し、今後どうしたいのかヒヤリングしました。システム部

門にシステム監査にこないでいっています。すごく有効です。ビジネスサイドに緊張が走っていました。

8.　経営者と内部監査とのコミュニケーション方法

Q：従来の守りの監査・本日の攻めの監査にて経営者とシステム監査人は共通に認識をいかにとるか、監査すべき項目をどうとるか、御社において経営者とシステム監査人はコミュニケーションをどうとっていますか？お話しをお聞きしたいです。

A：内部監査の方向感として、ビジネスサイドの変化により監査が影響を受けて変わってきていると思っています。守りの監査から、攻めの監査に内部監査が変わってきています。　経営と内部監査とどういうコミュニケーションをしているかはわかりません。

＜感想＞

講演テーマ「新しい時代のシステム監査を考える」は、システム監査の新しい役割を触媒・応援団とし、その役割に対する経営者からの期待でした。「エンタープライズＩＴ」とスマホを中心とした「コンシューマＩＴ」とが連動する新しい時代において、システム監査への期待が、経営にとって大変高いことに、驚きました。

以上

注目情報（2012/9,10）

■なりすましウイルスによる誤認逮捕

インターネット上に犯罪予告の書き込みをしたとして逮捕された人がその後、なりすましウイルスによる誤認逮捕であったとして釈放される事件があいついで発生した。

一件は、ホームページに無差別殺人を予告する書き込みをしたとして、偽計業務妨害罪で8月26日に逮捕され、起訴後に、別人がなりすまして遠隔操作した可能性があることが判明し、勾留が取り消され、9月21日に釈放された事件である。もう一件は、伊勢神宮の破壊予告をネットの掲示板に書き込んだとして逮捕されたが、一週間後に釈放された事件である。

個人情報漏洩事件とは異なる、たいへんおそろしい事件である。

この事件の怖いところは、誤認逮捕された本人が、自ら、犯人ではないことを証明する手立てがないことである。これから一億総スマホ時代になったとき、類似の事件が発生する可能性がある。

■ＩＰＡ：セキュリティセンター　「２０１０年１０月の呼びかけ」　（2012/10/1 発表）

「 SNS におけるサービス連携に注意！ 」　～　あなたの名前で勝手に使われてしまいます　～

最近、インターネット上のサービスである“Twitter（ツイッター）”などのミニブログサービスや、“mixi（ミクシィ）”、“Facebook（フェイスブック）”、“Google+（グーグルプラス）”などの SNS（ソーシャルネットワーキングサービス）が人気である。これらのサービスは、今の自分の行動や考えを簡単にインターネット上に発信できることや、同じ趣味や考えを持つ利用者同士の交流の場として利用できることが特徴となっており、多くの利用者を集めている。その反面、悪意ある者からサービス利用者が狙われるようになった。例えば、「自分では何もしていないのに、Twitter 上で勝手に投稿された」といった相談などが複数寄せられている。Facebook では悪意あるサイトへのリンクを含む投稿が確認されている。

IPA で調査した結果、SNS 間のサービス連携機能を悪用された場合に、こうした被害が発生し得ることを確認した。

対策としては、①SNS の不要な連携サービスの取り消し、②他社の投稿（ツイートなど）に書かれている URL を安易にクリックしない、③口コミなどで連携先のサービスの評判を確認する、等がある。

詳しくは、下記 URL を参照。

http://www.ipa.go.jp/security/txt/2012/10outline.html

また、怪しいメールや DM（ダイレクトメール）が届いた、怪しいリンク先が書かれている SNS やブログなどの投稿文を見つけた、などがあったなら、IPA 安心相談窓口まで連絡してほしい。

E-mail:　anshin@ipa.go.jp

■ＩＰＡ：プレス発表　（2012/10/1 発表）

クラウドの浸透実態と緊急時対応における課題に関する調査結果を公開

～機能停止を回避するための条件・課題を提起～

IPA（独立行政法人情報処理推進機構、理事長：藤江　一正）は、社会インフラとしての重みを増しつつあるクラウドコンピューティング(*1)の実態と、その停止の影響、ならびに機能維持のための条件について実態調査と課題抽出を行い、その結果を、2012 年 9 月 28 日（金）から、IPA のウェブサイトで公開した。下記 URL を参照。

http://www.ipa.go.jp/security/fy23/reports/cloud/index.html

全国のイベント・セミナー情報

■【東京・月例研究会】

※ 会員サービス向上の一環として、今年度から会員会費を 2,000 円から 1,000 円に値下げしております。

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

回	日時	テーマ	講師	
第 176 回 月例研究会	10 月 26 日(金) 18:30～	コーポレート・ガバナンスとITガバナンス ～監査役の視点から～	アリアンツ生命保険株式会社 監査役　河邊　精一　様	開催場所は、本表下の欄外のとおりです。
第 177 回 月例研究会	11 月 21 日(水) 18:30～	SNS の利用とその危険性について	日本アイ・ビー・エム(株) 経営品質・情報セキュリティ推進室 シニアセキュリティアナリスト 守屋 英一様	
第 178 回 月例研究会	12 月 17 日(月) 18:30～	「金融機関のシステムリスクに挑む、コンティンジェンシープランの見直しが必要になった今日」（仮題）	ＮＰＯ法人 日本システム監査人協会 理事　遠藤 誠 様	

開催場所：東京都港区芝公園 3-5-8　機械振興会館　地下 2 階ホール
案内図　http://www.jcmanet.or.jp/gaiyo/map_kaikan.htm
（ご注意）昨年までと会場が変わっております。

■　【大阪・近畿支部主催セミナー】

「事例に学ぶシステム監査の基本と応用」　（ITコーディネーター知識ポイント1P付与）
〈日時〉 2012年11月17日（土）13:00～17:00、
〈場所〉 常翔学園　大阪センター　http://www.josho.ac.jp/facility/osakacenter.html
大阪市北区梅田 3-4-5　毎日インテシオ 3F　TEL：06-6346-6367
〈費用〉 日本システム監査人協会会員　4，000円、　その他の方　5，000円
〈内容〉 監査の実体験から生じた事例講演を3題と、BCPにおけるシステム監査の考察を講義形式で行う。
事例講演
・「テーマ監査／業務監査としてのシステム監査事例　－J-SOX・IT 統制評価と棲み分けて－」
・「ファイル共有ソフトによる情報漏洩事故の事例」
・「マネジメントシステム規格の統合的な運用　－内部監査の効率的な運用事例－」
BCP監査考察：「システム管理基準等を用いたBCP（事業継続計画）監査について」
〈テキスト〉 オリジナル資料
〈講師〉 近畿支部のシステム監査サービス等経験者
〈定員〉 20名（最小催行人員8名）
〈申込方法〉 右のホームページからの申込み　http://www.saaj.or.jp/index.html
〈申し込み期限〉 2012年11月9日（金）締切り
〈問い合せ〉 日本システム監査人協会 近畿支部 セミナー係　（E-mail: semi2012@saajk.org　E-mail のみ ）

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

2012 年 11 月～1 月発行の会報テーマは「システム監査人のやりがい」です（4 月～6 月のテーマは「システム監査人の悩み」、7 月～10 月発行の会報テーマは「システム監査のすすめ」でした）。

近年、情報処理技術者試験のシステム監査の受験者が低迷していると聞きます。また、当協会の会員数も減少傾向にあります。その理由は、システム監査という仕事の意義と面白さが世間に知られていないためであると思います。そこで、今回は、システム監査人としての実務経験が豊かな会員諸氏に、システム監査の意義と面白さを語っていただきたいと思います。もちろん、否定的なご意見も大歓迎であります。

専門職として働く者にとって一番大事なこの点について、議論が盛り上がることを期待します。

・・・・・今月号も多くの方にシステム監査にかかわる記事の投稿をいただきました。・・・・・
・・・・・ありがとうございました。・・・・・

みなさまのご意見等を引き続きお寄せ下さい。また、協会の部会、研究会、支部などの活動の場でも大いに議論をお願いいたします。

□■ ２．　会報の記事に直接コメントを投稿できます

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

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

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

□■　３．会員の皆様からの投稿を募集しております

分類は次の通りです。

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

２．会員投稿　(Word の投稿用テンプレートを利用してください)

３．会報投稿論文 (論文投稿規程があります)

これらは、いつでも募集しております。 気楽に投稿ください。

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

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

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

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

会員限定記事

【本部・理事会議事録】(会員サイトから閲覧ください。パスワードが必要です)

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

■発行：　NPO 法人　日本システム監査人協会　会報編集部

〒103-0025　東京都中央区日本橋茅場町２－８－８共同ビル６F

■ご質問は、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)

━━