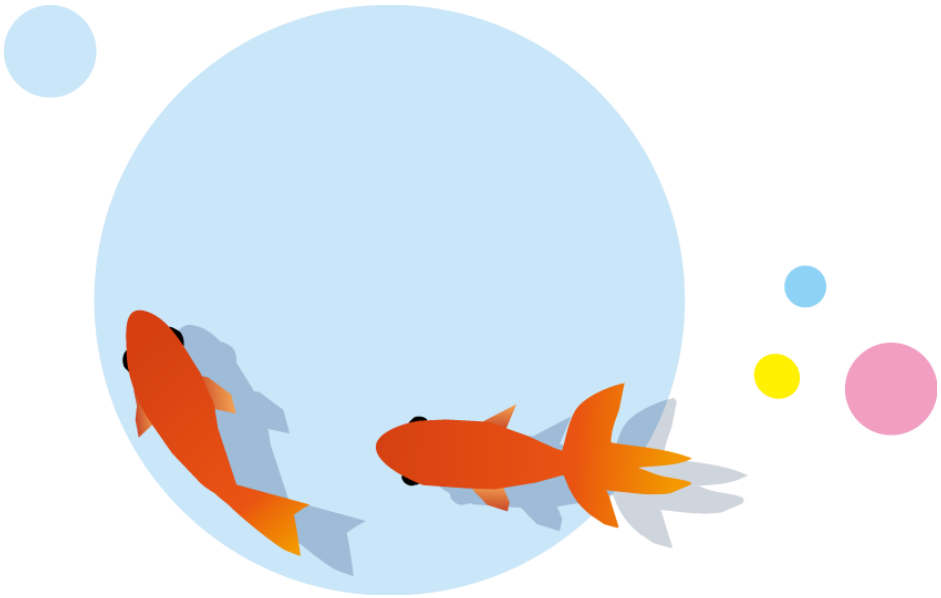
特定非営利活動法人
日本システム監査人協会報

2013年7月号
No 148

No.148（2013年7月号）＜6月20日発行＞

海開き・山開き・・・
いよいよ夏のレジャーシーズンがやってきます。

今月号も、興味ある新鮮な情報満載です。
仕事・レジャーの合間に、ぜひご一読を！



2013.06 投稿

めだか　【システム監査と他の監査との関係・連携（システム監査活性化への提言）】

“システム監査活性化への提言”をテーマに、これまで以下の２つを書いてきた。

一つは、「将を射んと欲すれば･･･」と題して、“システム監査の法制化を訴える（将を射んと欲する）のでなく、各当事者（特に「開発者」、「情報システムサービス提供者」）の説明責任遂行の必要性を訴える（まず、馬を射る）ことを通して、その説明責任遂行と不可分の、説明責任遂行に信頼性を付与し実効あらしめるシステム監査の必然的実施を導き出すのが、システム監査活性化の王道であり、また実は近道なのではないだろうか。”と書いた。

そして、もう一つは、「監査人自身が社会的使命を明確に自覚する」と題して、“システム監査人は、システム監査人の“時代の使命”を明確に自覚すべきと思う。（略）システム監査が普及しないことを嘆いて時間を潰すより、時に備え、システム監査人の足下をより強固にすることに目を向けたい。（略）まずは、システム監査人が気持ち（志）を高く持ち続け、継続的に研鑽を積み重ねることが、システム監査活性化の一丁目一番地ではないだろうか。”と書いた。

今回は本テーマの三回目（最終）として、少し見方を変えて考えてみたい。

現代は情報化社会と言われる。言葉は踊るが、これを日常の仕事の中で具体的に感じるのはどんな場面だろうか。こう考えて、はたと思った。“会社に着いて、仕事の最初にすることはPCの電源を入れること。一日の仕事の最後にするのはPCの電源を切ること”という現実かなと。つまり、今日の仕事は殆ど情報システム無しではあり得ないという現実である。言われて久しいことだが改めてそれを再認識させられた。

一方、世の中ではその仕事を対象にいろいろな監査が実施されている。会計監査、業務監査、経営監査、監査役監査、監事監査、個人情報保護監査、環境監査･･･････。これらの監査は対象や評価の視点は異なるが、情報システムの基盤の上でなされる仕事（業務・ビジネス）の在りようをその対象とするのであれば、どの監査においてもその監査対象を支える情報システムにも目を向けなければならないことは自明である。

つまり、どのような監査でも、その監査対象を支える情報システムを多少なりとも評価して、その上で各視点での監査が実施される、されている筈ということではないだろうか。

例えば会計監査において、会計システムのIT統制評価が欠かせないのはその典型的一例といえる。

とすれば、システム監査（システム監査と銘打って実施される場合の外、他の監査の中でその一部としてシステム監査が行われる場合を含む）は、今日、監査の中で一番多く実施されている筈の監査となる。例え、それがシステム監査と明確に認識されてなくても。

程度の差はあっても、情報化社会にあって全ての監査の中に組み込まれるべきシステム監査が適切にされているのか、いないのか、されてないなら我々システム監査人はそれにどう関わっていくべきなのかを考えることは、システム監査人に今課せられている重要なテーマかもしれない。

“全ての監査と不可分のシステム監査”との認識で、システム監査人は他の監査人と一層連携を強化していくことも、システム監査活性化には欠かせないのではないか。　　（広太雄志）

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

2013.06 投稿

めだか　【　So What　（システム監査活性化への提言）】

So What ： だから何、何の役に立つの

システム監査がいかに役立つか、もっともっと分かり易く伝えよう！

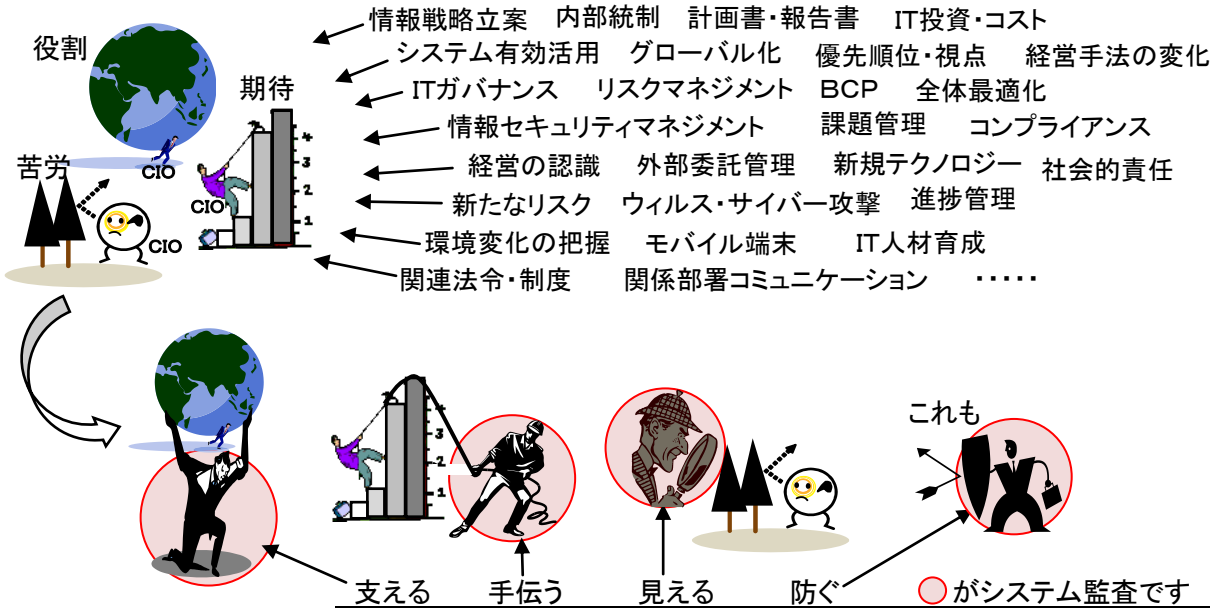
システム監査って何？ 何をするの？ 受けるとどうなる？ を言わせない

プレゼン力が新風を吹き込み、平たく語れば逆にただ者でないと分かる

目的・基準、重要性や意義、これらの説明だけでは食指が動かない

揺り動かす一歩は、難しいことを単純化して呼びかける、ではないだろうか

例えば、ＣＩＯ へアプローチしてみる



システム監査は、

- 情報システムやＩＴ利活用業務全般に利用できます。
- 「何か変だ」「どうも疑問が」の問題を明確にするのが役目です。
  - ✓ ＩＴガバナンスの改善課題が明らかになります。
  - ✓ リスクマネジメントの整備状況が把握できます。
  - ✓ 業務のリスクとコントロールの運用状況が確認できます。
  - ✓ ステークホルダーへの説明責任を果たす手段となります。
  - ✓ 重要業務を優先するなど段階的な実施が効果的です。
  - ✓ 監査結果は現場の方と認識をすり合わせてからまとめます。
  - ✓ 適否評価だけでなく改善の方向性や緊急性なども助言します。

例え話をいくつか入れる必要がある

箇条書きの多用は疑問かも

など

まだまだ工夫不足です

（山の彼方）

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

2013.06 投稿

めだか【 内部監査において重み増すシステム監査― 内部監査人の立場からのシステム監査活性化 】

「システム監査は普及していない」という話をよく聞く。しかし、金融機関の内部監査部門に籍を置いている私からすると、金融機関においてシステム監査は重視されているし、「システム監査は普及していない」というのが、どうも実感として湧いてこないところがある。そこで、システム監査がどの程度普及しているのか、調べてみた。

下の図は、日本内部監査協会が行っている「内部監査実施状況調査」において、回答企業のうち情報システムの内部監査を実施している企業の割合を時系列で表したものである。

出典：丸田起大「わが国における内部監査実務の変遷―内部監査実施状況調査結果分析」(『月刊監査研究』2012年9月号)

これによると、1995年当時2割に過ぎなかった情報システムの内部監査実施率は、パソコン・インターネット等の普及や2000年問題、個人情報保護法・J-SOXの施行など、企業におけるシステム面の課題が多く発生してきたことを背景に、着実に増加してきており、2010年には5割にまで達している。実施率5割という数字は、経理業務の内部監査実施率が5～6割程度の推移であること等を考えると、内部監査のテーマとしてはかなり高いといえる。

実施率5割をどう評価するかは別にして、内部監査において、システム監査の重みが着実に増してきていることは事実である。裏返せば、システム監査に対する経営陣からの期待もそれだけ高まっているということであろう。

それでは、われわれシステム監査を担当する内部監査人は、こうした経営陣の期待にどう応えていくのか？

まずは、「質の高い監査」を行うこと、「監査としての成果」を上げることであろう。内部監査のコンサルティング機能を発揮して、経営陣からも、被監査部門からも感謝されるような監査を目指したい。それには、SAAJの研究会活動などを大いに活用して、システム監査人としてのスキルアップを図るといった地道な努力が欠かせない。

もうひとつここで述べておきたいのは、システム監査は「システム監査人」の専売特許である必要はないということである。ややもすると、システム監査は専門家に任せておけばよいとされ、一般業務の内部監査員はシステム監査を担当しないということになりがちであるが、これではいつまでたっても、システム監査に広がりはない。例えば、システム開発プロジェクトの監査で、「プロジェクトに遅延がないか、遅れている場合に責任者に報告しているか、対策を講じているか」といったことは、システム経験のない監査員でも監査はできる。監査手続書を整備したり、勉強会を開催したりして、一般業務の内部監査員もシステム監査の戦力になってもらい、システム監査人は専門性の高い分野の監査に注力することで、システム監査の質も向上するのではないかと思う。

これらの対応は、「言うは易く、行うは難し」ではあるが、内部監査におけるシステム監査活性化のために頑張っていきたい。

（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。）

2013.06 投稿

めだか　【システム監査の普及促進―デスマーチを憂いて・・その３】

筆者〔空心菜〕の2013年3月号（N0.144）の問題提起に関連して、〔健康衛生〕氏から、2013年5月号（No.146）に、「システム監査の普及促進―デスマーチを憂いて・・その2」の投稿があった。長時間労働やメンタルヘルスについて、社会的な動向と、アドバイスをする上で有益なサイトのご紹介である。感謝したいと思う。筆者〔空心菜〕は、SEのデスマーチはシステム監査上の課題であると考える同志3人で、〔健康衛生〕氏から紹介されたサイト①②を閲覧し結論を得た。ついては「システム監査の普及促進―デスマーチを憂いて・・その3」を投稿する。

システム管理基準では、この問題に関して次の項目を挙げている。

> 4. 人的資源管理 4.4 健康管理
> (1) 健康管理を考慮した作業環境を整えること。
> (2) 健康診断及びメンタルヘルスケアを行うこと。

これらは、簡単な点検項目であるが、これらに種々の点検項目を追加し、健康管理対策の実施状況を監査していけば、SEのデスマーチは「予防」できるのである。

ここで「予防」と言ったのは重要な意味がある。「抑うつ状態」と診断された時点で、「是正」のための処置を講じても、もう完全な回復は難しいということである。サイト①のSEでの問題事例を読んでも、そのような事例が多い。破断界という物理学用語がある。剛体が圧力に耐久する限界に来た時、突然壊れるその限界を言うが、同様であろう。サイト②では、「簡略版メンタルヘルス対策に係る自主点検票（事業者向け）」（中央労働災害防止協会）がダウンロードできるので事業者向けに使える。

デスマーチの主な要因は、受注→設計→プログラミング→テスト→納入後の運用という業務の流れの局面ごとに、人員不足、労務管理の甘さ、顧客対応、迫る納期、不規則な生活習慣という要因（*）が重なり、しわよせが、現場の慢性的な残業となって、このような作業環境が1年も続くと誰でも抑うつ状態になるのは当然であると思う。SE業務の流れの局面ごとに、デスマーチの主な要因となるリスクなどを認識、分析して、メンタルヘルスケアの対策を立てる、そして、その対策実施状況を監査点検項目に挙げて、監査を行うことが問われている。

*朝日新聞2013年2月1日朝刊記事の説明図（日立健康管理センターの林剛司センター長（産業医）による）

〔健康衛生〕氏から紹介されたサイト

① 厚生労働省関連サイト「こころの耳」（http://kokoro.mhlw.go.jp/）
　（社）日本産業カウンセラー協会運営サイト
② 東京都労働相談情報センターのサイト（http://www.kemkou-hataraku.metro.tokyo.jp/）

（空心菜）

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

2013.06 投稿

投稿　【　システム監査の活性化・・その２　】

会員番号 0557 仲　厚吉（システム監査活性化プロジェクト）

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

先ず、当協会が、運営組織及び事業活動が適正であって、公益の増進に資する活動を行っていることを、広く一般の人に認知してもらうことが大切です。そのためには、当協会が4万5千あるNPO法人に抜きんでた認定NPO法人であることが望まれます。旧の特定非営利活動促進法では、認定NPO法人は、国税庁長官の認定によって、寄附者への税法上の恩典という意味合いのものでした。しかし、改正された特定非営利活動促進法では、その目的に、「運営組織及び事業活動が適正であって公益の増進に資する特定非営利活動法人の認定に係る制度を設けること等」が法の条文になりました。

特定非営利活動促進法（平成24年8月1日最終改正）によりますと、第一章　総則、第一条（目的）に、この法律は、特定非営利活動を行う団体に法人格を付与すること並びに運営組織及び事業活動が適正であって公益の増進に資する特定非営利活動法人の認定に係る制度を設けること等により、ボランティア活動をはじめとする市民が行う自由な社会貢献活動としての特定非営利活動の健全な発展を促進し、もって公益の増進に寄与することを目的とする、とあります。

つまり、認定NPO法人は、運営組織及び事業活動が適正であって、公益の増進に資する特定非営利活動法人であるとして、広く一般の人に認知してもらえるわけです。当協会では、2012年度と2013年度の2年間にわたって、認定NPO法人を目指して準備をつづけています。そして、現在、新規認定申請の要件を満たしてきています。

また、当協会は、下記の定款にある事業活動(1)(2)(3)を行っています。これらの活動を通じて、システム監査の活性化のため、外部の期待を喚起してそれに応えていくこと、そして他団体との連携を強化していくことが行われています。システム監査活性化プロジェクトのメンバーとして、これらの事業活動に、より一層、取り組んでいこうと思います。

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

(1) 社会教育の推進を図る活動

(2) 国際協力の活動

(3) 前各号に掲げる活動を行う団体の運営又は活動に関する連絡、助言又は援助の活動

以上

新たに会員になられた方々へ

Welcome

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

ご確認ください

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

特典

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

ぜひ参加を

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

ご意見募集中

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

出版物

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

セミナー

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

CSA・ASA

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

会報

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

お問い合わせ

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

沼野会長からの一行メッセージ

“会報は、読むだけでなく、システム監査に関する意見をコラムで投稿頂きたい。”

2013.06 投稿

会長コラム　【　是非、会報に注目(投稿)を！　(国立国会図書館にも納められています。)　】

会員番号 0841 沼野伸生(会長)

今回は当協会の会報についてお話ししたいと思います。

協会活動の資金は基本的に会員の皆様から頂いている会費であり、協会活動に係る全ての情報の所有者は基本的に会員の皆様です。従って、最終成果ばかりでなく途中経過（中間成果物や、活動経過情報など）も含め積極的に会員に広報、還元して行かなければならないと考えています。

そこで、当協会は会報の充実化にも積極的に取組んでいます。(会報は今月号で既に１４８号になりました。)

会報は協会と会員一人ひとりを繋ぎ、協会活動情報等を定期的かつ直接的に会員に伝達し、また会員相互コミュニケーションもできる場として、当協会の重要インフラになっています。

会報は毎月２０日に発行していますが、皆さんご覧頂いていますか。

現在の会報は、概ね“協会からの情報提供”と“会員等の意見発表の場”で構成されています。

“協会からの情報提供”には、例えば、研究会等の活動情報をお知らせする「協会からのお知らせ」や、「新たに会員になられた方々に（お役立ち情報や協会活用方法)」、「注目情報」、「全国のイベント・セミナー情報」などがあります。昨年から当協会が強力に推進している会員増強ＰＴ（今年度の名称はシステム監査活性化ＰＴ）の活動状況もここで継続的にお知らせしています。

“会員等の意見発表の場”には、システム監査に関連したコラム（匿名投稿“めだか”及び記名投稿）が掲載されています。これは、システム監査に関連する自由な意見（勿論、公序良俗に反しないもの）が発表できる場です。投稿を促すために、年間、及び３ヶ月毎のテーマを設定していますが、必ずしもそれに拘らず自由に投稿できます。また、Ｗｅｂ上の会報サイトでは、会報の記事（投稿コラム等）に読者が直接コメントを投稿できるようにもしており、投稿者と読者の建設的な意見交換も可能となっています。

更に、システム監査に関連する論文の投稿も受け付けており、投稿論文は査読を経て採択されたものは会報に掲載されています。

会報は、主として当協会の会員を対象にしたものです。しかし、当協会の設立目的は“システム監査の社会への普及を通して情報社会に貢献する”というものですから、当協会の活動を広く社会に公表（アピール）することも必要です。そこで、会報部会では、当協会の会報を毎号国立国会図書館に納本し、国会図書館では“経済社会の情勢を報告する資料として有用な逐次刊行物・特別資料”として分類、登録し、国会図書館ホームページの「日本全国書誌」に掲載され、書誌データとして検索できるようにもなっています。

本コラムを読んで頂いている方は会報を見ている方々なので、その方々に会報をＰＲ（読んで下さい）というのは自己矛盾のようでもありますが、お読み頂いている方々には、是非読むだけでなくシステム監査に関連する意見をコラムで投稿頂き、また、読んでない方々に是非会報の紹介をお願いしたいと思います。

協会も、現在の会報に満足することなく、積極的に改善、レベルアップを図り、システム監査に関する活動情報の社会への発信にも努め、システム監査普及活動に引続き取組んでいきたいと思っています。

以上

2013.06 投稿

協会からのお知らせ（システム監査活性化プロジェクト）

会員番号 6027 小野　修一（システム監査活性化プロジェクト　主査）

今月の会報では、当協会の研究会や担当組織が行っている活動の中から３つの活動について、ご紹介します。いずれも、システム監査の、また当協会の活性化に資する活動となっています。

１．月例研究会

当研究会は、毎月、会員の皆様が関心をおもちの、また会員の皆様にお知らせしたいホットなテーマと講師を選任し、講演および意見交換を行っています。毎回、会員外の方も含めて 100 人以上の参加者を集める当協会の目玉の研究会の一つです。

昨年度までは開催しない月もありましたが、今年度は、まさに月例での開催を実現しようとしています。ISACA、システム監査学会をはじめとする友好関係にある組織にも、相互乗入れで開催案内をお出ししています。より一層、参加者が増え、システム監査の活性化につながることを願っています。

２．情報セキュリティ監査研究会

今月も、当研究会の中で討議、意見交換を行っているテーマの中から、会員の皆様に知っていただきたい、よろしければご一緒に議論に加わっていただきたい情報を報告します。ご関心をおもちの方がいらっしゃいましたら、お気軽にご連絡をください。お待ちしています。

３．個人情報保護監査研究会

当研究会でまとめた『PMS 実施ハンドブック』簡易版の内容を、毎月の会報で、順次紹介をしています。

ぜひ、システム監査人の主要な活動分野の一つである PMS の構築・評価を行う際の参考にしていただければと思います。このガイドブックをベースにした PMS 構築の実践ノウハウを身に付けていただくセミナーも計画しています。

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

以上

2013.06 投稿

【　月例研究会の活動紹介　】

会員番号 0148　木村裕一（月例研究会）

1. 月例研究会では、今年度は以下のような計画を進めております。

回	開催月日／場所	テーマ／講師
180	4月24日（水） 機械振興会館	テーマ:「企業 IT 動向調査 2013（2012 年度調査）」 講　師:社団法人日本情報システム・ユーザー協会（JUAS） 常務理事　浜田　達夫　氏
181	5月21日（火） 機械振興会館	テーマ　:『金融機関等コンピュータシステムの安全対策基準・解説書』及び 『金融機関等におけるコンティンジェンシープラン策定のための手引書』 の改訂に伴う追補版について 講師:財団法人　金融情報システムセンター 監査安全部　　西村　敏信　部長　様 鬼頭　克巳　総括主任研究員　様 岡田　昌一主任研究員　　様
182	6月17日（月） 機械振興会館	テーマ:「個人情報影響評価 PIA の要諦 PIAとシステム（情報セキュリティ）監査との関係」 講　　師:公立大学法人首都大学東京　産業技術大学院大学 教授　　瀬戸　洋一　　氏
183	7月24日（水） 機械振興会館	テーマ:「サイバー攻撃の脅威」（仮題） 講師:独立行政法人　情報処理推進機構 技術本部　セキュリティセンター 情報セキュリティ技術ラボラトリー　渡辺　貴仁　様
184	8月21日（水） 機械振興会館	テーマ:「クラウドインシデント」（仮題） 講師:独立行政法人　情報処理推進機構 技術本部　セキュリティセンター 普及グループ　河野　省二　様

以降も、毎月の開催を目指しています。ぜひ、ご都合をつけて参加くださいますようお願いします。

なお、会報に参加者の記録を掲載しておりますので、各支部などにおいてはビデオの視聴の際に参考にしてください。

2. 開催のテーマについて

テーマはシステム監査人にとって必要な情報、知識や基本的な考え方の習得を目指しています。

月例研究会担当理事が協議してテーマをきめた基本計画に沿って進めています。

その際に、年に1回程度月例研究会の参加者に行うアンケートも参考にしています。

3. 月例研究会開催の案内先

参加者の増加を図ることも月例研究会の重要な課題であり、HPにおいて掲載しているほかに、当協会の会員宛のメーリングリストによる案内（HP掲載時、及びその後にもう1度）のほか、ISACA、システム監査学会などの団体とも連携して会員向けにメールなどにより案内をしていただいております。

参加者の3割程度の方が、協会会員以外の方でもあります。

（当然、これらの方へ会員になっていただくようにご案内しています。）

4. ビデオの撮影の件

月例研究会は、原則ビデオを撮影して、各支部における研究会で活用していただくこととしております。

しかし、時期的にあるいは内容としてビデオ撮影することが適切でない場合に、講師側から承認を得られない場合があります。そのような場合には、月例研究会の配布資料のみを支部に提供しております。

このような貴重な内容の研究会もありますので、首都圏の方々、また月例研究会開催時期に首都圏に出張される方は、ぜひご都合をつけてご参加されるようにお勧めいたします。

以上

2013.06 投稿

【情報セキュリティ監査研究会だより その３】

会員番号 0056　藤野明夫(情報セキュリティ監査研究会)

はじめに

情報セキュリティ監査研究会の活動状況の会報連載は、本号で第3回になります。第一回は、研究会の雰囲気をご紹介するために、3月21日に開催されました第11回情報セキュリティ研究会の様子をお伝えいたしました。第2回は、そもそも当研究会として何を求めて活動しているかについてご説明いたしました。今回からは、テキストにもとづく議論を中心にご紹介したいと思います。本号では、テキスト第3章に関する議論と第4章の一部を抜粋してご紹介いたします。資料のURL等については文末に示します。

１．　テキスト第３章「質的に異なってきたＩＴ利用への対応」(*1)について

＜本章の議論の観点＞　本章においては、以下のことが論じられている。

インターネットを中心に、個人は意図する、意図せざるに関わらず自分の情報を提供し、また、その結果として種々の便益を得ているが、これらの多種多様なデータを単独あるいは連携することにより、同一人物の情報や行動、性向を把握することができるようになってきた。とくにソーシャルメディアやモバイルの世界ではGPSにより個人の位置情報まで把握されてしまう。さらにあらゆるデータの連携や情報の組み合わせから、意図せずに個人が特定されたり、プライバシーが侵害されたりする可能性がある。この章は、ソーシャルメディアとモバイル利用がもたらした情報の質の変化について、個人が情報を提供するという観点で論じている。

＜個別の議論＞

（1）　匿名性と仮名性

〔著者の主張〕

「情報の発信者が誰であるか」を特定できないだけでなく、「情報の発信者が誰であるかは特定できず、また、同一人物であるか否か」も特定できない場合に、「匿名」という。「情報の発信者が誰であるかは特定できないが、情報の発信者が同一人物である」ことが明らかになる場合は、「仮名」という。一般に匿名性と仮名性が混同されている。

〔研究会内の議論〕

この辺の厳密な定義を我々は普段意識していない。たしかに、仮にAという仮名を使って、いろいろな情報を提供しているうちにAという仮名でリンクづけられた多様な情報から結果的にある個人が特定できてしまう可能性がある。「匿名」という以上は、どこまでいってもある個人が特定できることは避けなければならない。たとえば、医療情報などはその典型である。

本章では触れられていないが「Ｋ－匿名」という概念がある。これは、たとえば、ある地域にXなる病気の罹患者が1名しかいなければ、かりに匿名であっても、その地域のX病の患者であるというだけで個人が特定できてしまう。これを避けるために、たとえ匿名であっても統計処理をする際の集計の最小単位を小さくすると個人が特定されてしまうような場合、すくなくとも最少単位でも同一属性をもつものがK人いることを保証するような最小単位を決めて統計処理することを「Ｋ－匿名化」という。たとえば、先のX病患者の例でいえば、すくなくともK人のX病患者が存在するように地域のサイズを拡大することである。しかし、個々のデータについてＫ－匿名化を実施したとしても、異種のデータを連携して分析することにより、結果としてＫ－匿名性が崩れ、個人が特定されることがありうる。とくにビッグデータは異種のデータを取り扱うことが一般的であるから、このようなことが起こる可能性が高い。

（2）　意図せぬ情報の提供

〔著者の主張〕

ソーシャルメディアやモバイルの世界では、利用者自身が意図せずに機微に触れる情報を提供する場合がある。これによって、思いもつかないサービスが提供される可能性もあるが、重大なプライバシーの侵害を起こす可能性もある。また、ソーシャルメディアの場合は、利用者自身によるものだけではなく、他人を介してかかる情報が提供されてしまうこともある。とくにGPSによる位置情報の提供は、種々の便益を提供する上で有効であると同時に、取り返し

のつかないプライバシーの侵害につながるおそれがあり、さらには、その被害が第三者におよぶ可能性もある。

また、投稿しないこと自身も情報になる。Twitter投稿の履歴を時系列的に分析すれば、毎日ある一定の時間に空白の時間があるのは、その時間に食事を採っている、あるいは睡眠をとっているという情報を与えることになる。

〔研究会内の議論〕

ここではソーシャルメディアの例としてTwitterしか挙げられていないが、Facebookの場合はもっと危険性が高い。たとえば写真に写りこんでいる赤の他人がFacebookの世界で流通し、完全に個人の行動が追跡されてしまう可能性がある。

また、米国では、就職活動時にソーシャルチェックを企業側がすることが普通になってきているそうである。もちろん本人の了解を得た上での調査であるが、多分、求職者がこれを拒否することは不可能であろう。また、チェックをした結果、何も発信していないということが分かると、これもまた企業側は、就職に不利な発言を消したか、主義として敢えてソーシャルメデイアに参加しない変わり者といったマイナスのイメージを持つ可能性がる。そうなると、求職者は、就職時に不利にならない当たり障りのない情報や企業側に受ける情報の発信、すなわち迎合した発言をすることになるのではないか。とすると、一般市民に、権力側と対等に世界中に情報を発信する手段を与え、民主主義の強力な道具となるはずであったインターネットやソーシャルメディアの浸透（現にジャスミン革命で独裁的権力を倒した）が、皮肉なことに、体制迎合的な極めて不自由な発言しかできないような社会もたらすのではないか。

（3）　便益と安心・安全を両立させるには蓄積や組み合わせを誰に開示するか

〔著者の主張〕

個人情報保護法では「他の情報と容易に照合して特定の個人を識別できる」場合は個人情報保護法における保護対象にしている。これを受けて総務省の「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会　第二次提言」(*3)では、「ウェブ上の行動履歴が相当程度長期間にわたって大量に蓄積される状態は、個人が容易に推定可能になる可能性がある」としている。すなわち、ビッグデータとして蓄積された結果、データ自体には個人を直接識別できる情報を含まなくても、特定の個人が推定可能になることがあるということである。

一方、情報収集側は行動履歴を長期的に蓄積し、同一属性の一群の人々のライフスタイルを分析すれば、個人を特定せずにその一群の人々にライフスタイルに合った情報を提供することができ、情報収集側、利用者側双方に利益がある。ビッグデータを用いたサービスを設計するときには、その便益性の確保とプライバシー侵害リスクの回避を両立させることが重要である。

〔研究会の議論〕

この問題には、前述の「匿名化」の議論や「意図せぬ情報提供」といった問題が深く関わってくる。システム監査人としては、そのサービスがこれらを両立する設計になっているかどうか、上述のリスクに関する深い見識と洞察のもとに監査しなければならない。

ビッグデータの領域の個人情報保護は、単なる個人情報漏えいのみではなく、異種のデータが組み合わさることで、利用者本人の意図しない情報が形成されるリスク、また、それが、利用者本人だけではなく第三者によってなされる可能性もあること等、その特殊性を深く理解することが必要である。ビッグデータの世界はまだ始まったばかりであり、今まで我々が考えも及ばなかったような問題が発生する可能性もある。継続的にウォッチするとともに深く探求すべきテーマである。

２．　テキスト第４章「ビッグデータ時代のコンプライアンスリスクと可能性」（*2）について

本章は、ビッグデータ時代のコンプライアンスリスクとビッグデータ時代の新たな可能性について枚挙している。紙数の関係で、この枚挙されたコンプライアンスリスクの紹介に留める。

ビッグデータ時代には、種々の法的・社会的リスクが存在する。これをコンプライアンスリスクというとき、これには、大量のデータの漏えいのリスク、プライバシー侵害のリスク、不正な表示のリスク、その他のリスクがある。

①　大量のデータ漏えい・消失のリスク

大量のデータ漏えいのリスクとは、大量のデータが保存され、処理に供されているときに不正侵入、内部の不正

行為等により、データの機密性が失われてしまうことをいう。大量のデータを保存している企業等は、漏えいを起こした場合の社会的な信用の失墜のリスクや損害賠償責任を負うリスクがある。

また、大量のデータ消失のリスクは、障害等によって、大量に保存されていたデータが消失し、利用できなくなる状態をいう。漏えいほどではないにせよ、社会的な信用の失墜のリスクや損害賠償責任を負うリスクがある。

② プライバシー侵害のリスク

ビッグデータ時代には詳細な個人の活動に関わるデータが収集、処理されることによって、プライバシーの侵害を来す懸念がある。プライバシーに関する利益は、「宴のあと」事件（東京地裁判決 昭和39年9月28日）において、「私生活をみだりに公開されない法的保証ないし権利」と認識された。このときに法的保護のためには、以下の三要件、すなわち、個人の私生活上の事実に関する情報であること、公知になっていないこと、私人としては通常は公開を望まない内容であること、を満たすことが必要とされた。

ビッグデータ時代の問題のひとつは、この三要件を満たさないと考えられる、あるいは、個人情報保護法の対象外と考えられる各種の分析データやそれを支える個別のデータのようなものにも、ビッグデータの持つリンク付けの可能性ゆえに、プライバシー的な問題として保護が求められるべきではないかという議論があることである。すなわち、保護されるべきプライバシーの範囲が拡がっているということができる。

また、プライバシー侵害のリスクに関しては、利用者の同意を得ずに、MACアドレスやFacebookアカウントID等を収集、利用し、事件になった例もある。

③ 不正な表示のリスク

「不正な表示」とは、利用者に明示するプライバシーポリシーと、実際の情報の処理者の利用等の実態が齟齬した場合に、法的な問題が発生するのではないか、ということである。情報の処理者と利用者の間の情報の非対称性ゆえに、情報の処理者の方にモラルハザードが発生する可能性がある。

④ その他のリスク

その他のリスクの例としては、著作権などの知的財産権について、サービスの提供者が間接侵害者と認識され、訴えの対象になる可能性があることが挙げられる。本質的にはクラウドコンピューティングで議論されているものと同一の議論である。

【資料】

(*1) IPA（独立行政法人情報処理推進機構）編、2012 年 3 月発行
「くらしと経済の基盤としての IT を考える研究会報告書　つながる IT がもたらす豊かなくらしと経済
～ ビッグデータの価値と信頼 ～」）
URL　http://www.ipa.go.jp/about/research/2011bigdata/
第3章　質的に異なってきたIT利用への対応　慶應義塾大学　折田　明子　（現在は、関東学院大学）
(*2) 同上　第4章　ビッグデータ時代のコンプライアンスリスクと可能性　弁護士　高橋　郁夫
(*3) 総務省、2010 年 5 月、「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会　第二次提言」
URL　http://www.soumu.go.jp/main_content/000067551.pdf

【情報セキュリティ監査研究会への参加について】

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

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

以上

2013.06 投稿

「個人情報保護マネジメントシステム実施ハンドブック」簡易版　第４章

会員番号：0557　仲厚吉（個人情報保護監査研究会）

第４章　個人情報の特定

個人情報の特定とは、事業で利用する個人情報について、漏れなく洗い出しを行う作業です。

4．1　個人情報の特定

目的外利用を行わないため、各部門長は「3303ＰＭＳ年間計画書」に定めた時期に、自部門で取り扱う個人情報について事業の用に供するすべての個人情報を特定します。
共有サーバー上に設定したPMS用フォルダーに、作成したファイルを提出することが便利です。

4．2　業務フローの作成

各部門長は、個人情報を取り扱う業務について、様式「3311業務フロー」を用いて、個人情報の取得から廃棄に至るまでのライフサイクルについて特定します。新規事業を開始するときも同様となります。
「3311業務フロー」によって以下のことを明確にすることができます。

- 各部門で取り扱う個人情報の流れが把握でき、個人情報の洗い出し（特定）が可能となる。
- リスク分析が容易にできる。

4.3　個人情報管理台帳の作成

「3311業務フロー」で特定した個人情報を、各部門において様式「3312個人情報管理台帳」を用いて列挙し、各個人情報の取り扱いについて明確にします。

「3312個人情報管理台帳」の管理項目（ご参考）		
1	種類	ライフサイクルが同じ文書は、１行にまとめてよい。
2	媒体	紙媒体、ＰＣ上のデータ、サーバー上など、媒体ごとに特定する。
3	個人情報の内容	氏名、住所、年令、アドレス、クレジットカード情報、本籍や病歴など
4	利用目的	できる限り具体的に特定する。
5	取得・入力	本人から直接書面で取得か直接書面以外か、入力したものかなど
6	取得手段	手渡し、郵便、書留、宅配便、Ｗｅｂ、メールなど
7	件数	できる限り実態に近い数を記入。累積、年、月、回などの単位が必要。
8	社内引き渡し先	原本やコピーの引き渡し先を記入
9	開示区分	本人から直接書面で取得する場合は、原則として開示対象となる。
10	取扱権限	～担当者、役職名などを記載する。
11	保管場所	金庫、施錠キャビネット、鍵付袖机、サーバーなど保管場所を記載する。
12	保管期間	契約終了後、退職後などを起算日とする。永久保存はできるだけ避ける。
13	委託・提供先	○○印刷会社、○○データセンターなど具体的な組織名を記載する。
14	廃棄・返却	シュレッダー、廃棄業者、データ消去など
15	リスク分析表	リスク分析表（後述）のリンク先を記載。

台帳に特定すべき個人情報（ご参考）　こんなものも個人情報とは・・・・！	
1	採用応募者が提出した応募書類で、短期間であっても預かることのある情報
2	従業員が提出した、履歴書、申請書、住民票、免許証等 （本籍の記載があれば機微情報となる。機微情報の取扱いをルール化する。）
3	従業員から取得した同意書、誓約書
4	会社が、従業員から取得した情報を基に作成した、スキルシート、人事管理情報、保険、税務関係書類等
5	会社が、従業員の昇進、賞与支給等のために作成した、人事考課書類等
6	会社が、安全衛生法等に基づき作成した、従業員ごとの健診スケジュール等
7	派遣元から提供を受けた、派遣社員に関する個人情報
8	顧客が提出した、申請書、申込書、アンケート等
9	Web 入力フォームの注文や、お問い合わせ情報を保存したデータベース
10	顧客からデータ処理や印刷、加工等のため受託した個人情報
11	グループ会社と、共同利用しているグループ企業の従業員名簿
12	個人情報を取り扱うシステムのバックアップデータ
13	個人情報を取り扱うシステムのアクセスログ
14	ＰＭＳ運用で発生する個人情報。教育記録、入退室記録、訪問者記録等
15	防犯カメラによって録画した情報
16	電話や、会議を録音した情報

台帳に特定せずに「3430安全管理規程」に取扱注意ルールを定めればよい個人情報（ご参考）	
1	従業員名が記載された業務報告書、議事録、稟議書等
2	取引先と交わした契約書、見積書、請求書等のＢtoＢ文書
3	ソフトウェア開発、運用の受託業務で、常駐する客先において触れる可能性のある個人情報
4	個人が管理する名刺
5	各従業員のＰＣに到着したメール情報、アドレス帳
6	会社貸与の携帯電話に保管された電話帳
7	グループ企業のエクストラネット上で、閲覧のみ可能な他社の従業員情報

4.4　個人情報管理台帳の承認

個人情報保護管理者は、各部門から提出された「個人情報管理台帳」を承認し、事業で取り扱う個人情報がすべて特定されたかどうかを確認するため、組織全体の個人情報管理台帳を作成します。

4.5　個人情報管理台帳の見直し

各部門長は、毎年決められた時期および以下の場合に「3311業務フロー」および「3312個人情報管理台帳」の見直しを実施します。

1	個人情報の特定漏れに気付いたとき。
2	新しい個人情報取り扱い業務が発生したとき
3	業務の変更・終了など、取り扱いに変更が発生したとき
4	「3312個人情報管理台帳」の記載項目の内容に変更が生じたとき。（ただし、件数など都度更新することが実務上適当でないと判断した場合は、年一回の更新のみでもよい）

2013.06 投稿

「個人情報保護マネジメントシステム実施ハンドブック」簡易版　第５章

会員番号：0557　仲厚吉（個人情報保護監査研究会）

第５章　法令、国が定める指針その他の規範

事業者は、法令順守のため、個人情報保護法、及び政令、並びに各省庁のガイドライン等を特定し参照することが求められます。法令等は、社会情勢の変化によって改正が行われますので、改正状況を確認し内部規程に反映していくことが必要です。

5.1　法令、国が定める指針その他の規範の特定

個人情報保護管理者は、「3320 法令・指針・規範集」を自ら承認し、全従業者が常時閲覧できるよう共有ファイルサーバーに保管します。

法令・指針・規範集 ［PMS3320/2012 年 7 月 1 日更新］

実施項目		所管	制定日	最新改定日
①	個人情報の保護に関する法律　（2005/4/1 全面施行）	消費者庁	2003/5/30	2009/6/5
②	個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン	経済産業省	2004/10/22	2009/10/9
③	雇用管理における個人情報保護に関するガイドライン	厚生労働省	2012/5/14	－
④	雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項について	厚生労働省	2004/10/29	2012/6/11
⑤	個人情報保護マネジメントシステムの要求事項（JIS Q 15001：2006）	日本規格協会	1999/4/2	2006/5/20
⑥	JIS Q 15001:2006 をベースにした個人情報保護マネジメ	日本情報経済	2006/9/1	2010/9/17

5.2　法令、国が定める指針その他の規範の見直し

事業者は、個人情報保護にかかわる法令、規範等について、個人情報保護法を所管する消費者庁のホームページを閲覧し、そこに解説している法令等の改定状況を確認する必要があります。

※：消費者庁 HP　http://www.caa.go.jp/seikatsu/kojin/index.html

5.3　従業者への通知

個人情報保護管理者は、法令・規範等の改定があった場合、自社の事業にどのように影響するかの説明を含めて全ての従業者に法令・規範等の改定を通知し、法令順守を徹底する必要があります。従業者への通知は、回覧、メールなどで行い、「3320 法令・指針・規範集」は、全従業者がアクセスできる共有ファイルサーバー閲覧可能とするとよいでしょう。

次回は、「第６章　リスクなどの認識、分析及び対策」
「第７章　緊急事態への準備」をご紹介する予定です。

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

2013.06 投稿

協会からのお知らせ　【　認定ＮＰＯ法人への新規認定申請について　】

会員番号 0557 仲 厚吉(事務局長)

事務局では、当協会の地位向上のため、一般の NPO 法人から認定 NPO 法人にかわることを検討する旨、理事会の承認を受け、新規認定申請について検討してきました。会報139号で報告した通り、認定 NPO 法人への要件相談のため、2012 年 8 月、飯田橋の東京ボランティア・市民活動センターを訪問し要件を確認しました。その後、要件のひとつである寄附金募集等を継続し、2013 年度 5 月現在、2012 年度と 2013 年度の 2 年間で、認定 NPO 法人への新規認定申請の要件を満たしてきています。つきましては、2014 年度に新規認定申請を行う旨を理事会に諮ります。

1. パブリック・サポート・テスト(PST)をクリアしていること

新規申請のため 2 年間で役員等を除く寄附者から3,000 円以上の寄附金を年平均100 人以上集めること(絶対値基準)で対応します。2013 年 5 月現在、2012 年度集計(118 人)と 2013 年度 5 月 22 日速報(90 人)を合わせて 208 人となり、2 年間で役員等を除く寄附者から 3,000 円以上の寄附金を年平均 100 人以上集める要件を満たしました。

2. 活動のメインが共益的な活動でないこと

会員のみの共益的活動とともに、広く一般に当協会のサービスを受けられる活動が過半であることが必要です。当協会の事業支出は、公認システム資格人等認定、システム監査 ISO 化支援、各部会研究会、支部活動等で、過半が公益的活動になっています。

3. 組織運営等が適正であること

組織運営等は、年2回、監事の監査を受けており、総会後、法務局登記、都庁へ事業報告を行っています。

4. 事業活動について一定の要件を満たしていること

定款に則って事業活動を行っています。認定のための一定の要件を満たした事業活動になるように、認定 NPO 法人に追加になる要件、例えば、寄附金の 70%以上、実際は寄附金の全部が、NPO 活動の事業費に充当になっています。

5. 情報公開が適正であること

認定申請資料について、一般の人から閲覧の請求があった場合、応じることができるように準備します。

6. 法令違反等がないこと

協会活動において法令違反等は発生しておりません。法人税の収益事業として申告する事業活動はなく、都税は免除、源泉税、消費税は法令に則って納付しています。

7. 設立から 1 年を超えていること

当協会は、2002 年度に NPO 法人として東京都の認証を受け、2013 年度に至っています。

以上

2013.06 投稿

協会からのお知らせ　【　会費納付等のお願い　】

会員番号 0557 仲 厚吉(事務局長)

事務局では 2013 年度会費請求書(2013 年 1 月 1 日付)を 3 月末日納付期限にて郵送しています。つきましては、5 月 19 日に、会費の入金が確認できていない会員の皆様へ「年会費ご納付のお願い」を下記のとおりメール送信させていただきました。また、2012 年度から会費が未納となっている会員の皆様には、2 年分の会費につきまして、納付依頼のメールを送信しています。6 月 28 日までにご納付いただけない場合は、督促状を発送させていただくこととなりますので、ご入金方、よろしくお願いします。

会員の皆様におかれましては、協会の運営に平素ご協力いただきまして誠にありがとうございます。協会ではテーマにシステム監査の普及促進を掲げて活動しております。さて、2012 年年末に事務局から、年会費請求書をお送りしておりますが、貴殿におかれましては、下記会費につきまして、ご入金が確認できておりません。

■未納分:2013 年度会費　:金 10,000 円

大変恐縮ですが、以下要領にてお急ぎお振り込みをお願いいたします。
1. 払込期限:2013 年 6 月 28 日(金)
2. 振込先:　以下のいずれかの口座にお振込お願いします。
　(振込手数料はご負担願います)
(1)郵便振替口座:00110-5-352357
　加入者名:日本システム監査人協会事務局
(2)みずほ銀行　八重洲口支店　普通2258882
　口座人名:特定非営利活動法人日本システム監査人協会
　トクヒ)ニホンシステムカンサニンキヨウカイ

お振り込みの際には、会員番号 4 桁(数字)を、お振り込み名義人の前にお付けいただきますようお願い致します。なお、入れ違いで会費をご納入済みの場合は、何卒ご容赦をお願い致します。その際には、お手数ですが、会員番号、会員名、支払日、支払名義人、銀行振込・郵便振替の別を、事務局　jimu@saaj.jp　までご連絡いただきますようお願いします。

■ご寄附のお願い

協会では会員の皆様にシステム監査の普及促進のためご寄附のお願いをしております。上記の会費納付と同じ振込先口座に、一口 3,000 円のご寄附を、お振り込みいただければ誠に幸いでございます。なお、協会から寄附者名簿を所轄庁の東京都に提出することがございます。また、御礼のため会報に寄附者氏名を公表することがございます。

■会員登録情報の変更のお願い

会員におかれて連絡先の住所やメールアドレス等の変更がある場合は、会員登録情報の変更をお願い致します。協会ホームページの「会員登録情報の変更についてご案内」の画面から変更できます。何とぞよろしくお願い致します。

http://www.saaj.or.jp/members/henkou.html

以上

2013.06 投稿

協会からのお知らせ　【　協会行事一覧　】

会員番号 0557 仲 厚吉(事務局長)

2013 年	理事会・事務局・会計・認定	部会・研究会	支部合同研究会・特別催事
7 月	(会計)支部会計報告依頼:14 日必着 (事務局)会費督促状発送〔7 月1日付〕	(月例研)「サイバー攻撃の脅威」(仮題):24 日	(支部)本部助成金収入
8 月	(認定)秋期 CSA・ASA 募集:8/1～9/30 (会計)中間期会計監査:中旬 (理事)会費督促電話:8/10～末	(月例研)「クラウドインシデント」:21 日 (基準研・ISO)「ISO/IEC 東京会議」:8/19～8/22 (事例研)「実務セミナー」:31 日	
9 月	(会計)予算実績中間報告:12 日	(事例研)「課題解決セミナー」:7 日 (CSA フォーラム)	
10 月			
11 月	(認定)CSA・ASA 更新手続案内〔申請期間 1/1～1/31〕 (認定)認定試問 (会計)2014 年度予算申請提出期限:30 日	(CSA フォーラム)	(北信越支部)西日本支部合同研究会:23 日
12 月	(会計)2014 年度予算案:1日 (理事会)2014 年度予算案・役員改選・会費未納者除名承認:12 日 (会計)2013 年度経費〆切:20 日 (事務局)通常総会・役員改選公示 (事務局)2014 年度会費請求書・寄附願い発送〔1月1日付〕		(東北支部) 支部総会・支部設立10 周年記念講演会:14 日
2014 年	**事務局・会計・認定委員会**	**部会・研究会**	**支部合同研究会・特別催事**
1 月	(認定)CSA・ASA 更新申請受付〔申請期間 1/1～1/31〕 (会計)支部会計報告依頼:14 日必着 (事務局)総会資料〆切:15 日 (会計)2013 年度決算案:中旬 (会計)2013 年度会計監査:下旬	(CSA フォーラム)	
2 月	(認定)CSA・ASA 春期募集:2/1～3/31 (理事会)通常総会議案承認:6 日 (通常総会):21 日	(通常総会特別講演)	

※定例行事予定は省略。

2013.06 投稿

研究会、セミナー開催報告、支部報告

■【第１８０回月例研究会報告】

会員番号 1690　梅里悦康(月例研究会)

日時　：2013 年 4 月 24 日(水) 18:30～20:30
場所　：機会振興会館地下 2Fホール
テーマ:第 19 回 企業IT動向調査 2013(2012 年度調査)～データで探るユーザー企業の IT 動向～
講師　：一般社団法人日本情報システム・ユーザー協会(JUAS) 常務理事浜田達夫氏

＜講演骨子＞

「企業 IT 動向調査」は、IT ユーザー企業の IT 動向を把握することを目的に、1994 年度から JUAS が実施している調査で、本年度は第 19 回目にあたります。調査テーマは、企業における IT 投資や IT 推進組織等の現状と経年変化を明らかにするとともに、年度ごとに重点テーマを設定しています。本年度は「ビジネスイノベーションへの提案(IT 部門からの提案)」と「情報セキュリティ」を取り上げています。従来は、すべての調査分析を終えた段階で調査結果を発表していましたが、前年度から IT 戦略立案や予算策定の一助となるために調査結果の一部を「速報値」として 1 月 21 日に IT 予算動向を、2 月 13 日には BCP を、2 月 27 日にはスマートフォン/タブレットの導入状況を、3 月 13 日にはビジネスイノベーションへの提案をプレスリリースしています。

JUAS のホームページ http://www.juas.or.jp/servey/it13/

調査の内容の詳細は、JUAS から「企業 IT 動向調査報告書 2013」(発行:日経 BP 社 2013 年 6 月 3 日)として発行される予定です。

Ⅰ. 企業IT動向調査 2013(2012 年度調査)の概要

1. 調査の方法

・ 調査対象は、東証一部上場企業とそれに準じる企業

(1)アンケート調査

・ 実施時期 12 年 11 月
・ ユーザー企業IT部門 4000 社対象、回答 1030 社(回答率:26%)

(2)インタビュー調査

・ 実施時期 12 年 11 月～13 年 1 月
・ ユーザー企業IT部門長、45 社

2. 調査の重点テーマ

(1)ビジネスイノベーションへの提案(IT 部門からの提案)

・ ビジネスイノベーションへの提案とは経営に直結する事項に対して IT 部門から課題解決や企業変革のための提案を行うことを指しています。近年 IT 部門に対してシステム開発・運用のみならず、全社最適視点で経営に提案を行うことへの期待が高まっています。2012 年度は、IT部門からビジネスイノベーションへの提案に関する取組み状況を調査しました。

(2)情報セキュリティ

・ 2012 年度は巧妙化が進んだ標的型攻撃により、企業のセキュリティ対策のあり方が改めて問われた年でした。

クラウドの利用、スマートデバイスの急速な普及や BYOD など、IT 環境の変化に伴い、新しいセキュリティ対策が必要となっています。その一方で、IT 部門のセキュリティ担当者でどこまで対応できるのか、また、どこまで対策を採ればよいのかが新たな課題となってきました。2012 年度は、高度化・複雑化した脅威や環境に対する新しい時代のセキュリティ対策の実態と課題を調査しました。

3. 主な調査結果

・ 調査結果は、以下のように構成されています。

(1)回答企業のプロフィール

(2)トピックス

①新規テクノジーの採用

②システム開発

③IT 基盤

④クライアント環境

(3) 重点テーマ

①ビジネスイノベーションへの提案

②情報セキュリティ

(4) 定点観測

①IT 予算

②IT 投資マネジメント

③IT 推進組織・IT 人材

④グルーバル IT 戦略

⑤BCP

Ⅱ. 調査結果

・ 調査結果の各調査項目について、特徴的な内容を抽出し、記述します。

1. 回答企業のプロフィール

・ 調査対象は、上場企業とそれに準じる企業 4000 社で各社の IT 部門長にアンケートを郵送で依頼し、1030 社の回答がありました。業種グループ、従業員数、売上高で分類すれば、次のとおりです。

(1)7つの業種グループ

・ 業種は、日本標準産業分類を参考に定めた 26 業種とし、業種の特性を把握するため更に「建築・土木」、「素材製造」、「機械器具製造」、「商社・流通」、「金融」、「社会インフラ(12 年度から「重要インフラ」から変更)」、「サービス」の「7つの業種グループ」にまとめて分析しています。

(2)回答企業の従業員数

・ 大企業(1000 人以上)1/3 強(34.1%)、中堅企業(300～1000 人未満)が 1/3 強(34.6%)、中小企業(300 人未満)が 1/3 弱(31.2%)でほぼ同じ割合です。

(3)回答企業の売上高

・ 売上高「10 億円未満」(2.5%)、「10 億円～100 億円未満」(27.3%)、「100 億円～1000 億円未満」(48.0%)、「1000 億円～1兆円未満」(18.0%)、超大企業「1兆円以上」(4.2%)となっています。この売上高 1 兆円以上の超大企業(4.2%)を分析すると今後の動向が見えます。

・「サービス」は、売上高 100 億円未満が半数(「10 億円未満」(6.0%)＋「10 億円～100 億円未満」(50.8%)＝

56.8%)と規模の小さな企業が多いです。

(4)業種グループとビジネスタイプ

・ 非製造業(商社・流通、金融、社会インフラ、サービス)はBtoC企業(一般消費者向け)が多いです。

2. 新規テクノロジーの採用(トピックス)

(1)新規テクノロジーの導入状況

・ 12年度は項目を入れ替えて新規テクノロジーを調査、「試験導入中・導入準備中」の割合が高い「モバイル端末管理(MDM)」(12.4%)と「ホスト型仮想デスクトップ」(7.0%)は、今後、導入率が大きく伸びると予想されます。

(2)ビックデータの取り組み状況

・ ビックデータの活用について、前向きの姿勢を示す企業が多く、3年後、大きな導入の動きが出てくると考えられます。

3. システム開発(トピックス)

(1)業務システムへのクラウド導入状況

・ 基幹系業務システムでは、導入済みが概ね 2～3%、但し、「顧客管理」では「導入済み」(4.6%)で若干高いです。「導入済み」(4.6%)、「試験導入中・導入準備中」(2.5%)、「検討中」(10.5%)、計17.6%と他の分野に比べて高く、クラウドへの関心の高さがうかがえます。

・ 情報系業務システムで本格的にクラウドが導入され、「導入済み」は「メール」(25.2%)、「掲示板、電子会議室、予定表等」(13.8%)、「社内向け広報(Web等)」(21.6%)で基幹系業務システムに比べ、情報系業務システムで本格的に導入が進んでいます。特にメールはクラウド導入の関心が高く、1/4(25.2%)が導入済み、検討中も約2割(22.4%)です。

(2)クラウド委託先選定の際に重視する点

・ クラウドの委託先選定の際は「コスト」(1位:26.3%)を最重要視します。次に重要なポイントは「クラウドベンダーの信頼度」(1位:23.4%)と「セキュリティへの取り組み」(1位:15.1%)です。「サービスの稼働時間(信頼性)」は、ある程度割り切った上(1位:6.3%)でクラウドを選択しています。

4. IT 基盤(トピックス)

(1)プライベートクラウド導入状況

・ 売上高 1 兆円以上の企業では 7 割が導入済みです。大企業を中心に導入が進みます。調達・運用形態は、データセンターは IT ベンダーから借用、ハードウェアは自社資産とする割合が高いです。

(2)IaaS、PaaS 導入状況

・ IaaS、PaaS の導入は踊り場の状況です。4 年間、導入済み企業は順調に増加するも、12 年度に初めて検討中企業が減少し、検討後見送りが増加しています。

5. クライアント環境(トピックス)

(1)スマートフォン・タブレット端末導入状況

・ 年度別導入状況:スマートフォン/タブレットを活用する企業が急激に増えています。導入企業は年々増加、12年度にはいずれも約 3 割(スマートフォン「導入済み」28.0%、タブレット「導入済み」27.0%)の企業が導入済みです。2011 年度よりスマートフォン＋9.0 ポイント増(19.0%→28.0%)、タブレット＋13.2 ポイント増(ほぼ倍増:13.8%→27.0%)しました。この 2 年間(2010 年度比)で、導入済み企業の割合はスマートフォンが約 3 倍(11.3%→28.0%)、タブレットは約 4 倍(6.2%→27.0%)に増えています。

6. ビジネスイノベーションへの提案（IT 部門からの提案）（重要テーマ）

（1）IT 部門発のビジネスイノベーション

・ ビジネスプロセス変革でミッションとして明示される企業は「明示され、かつ、応えられる」（7.1%）、「明示され、かつ、一部応えられる」（36.8％）、「明示され、どちらともいえない」（7.9％）、「明示され、応えられていない」（7.9％）、計 59.7％で、6 割の企業で既に IT 部のミッションとして明示され、業務の合理化・省力化で IT が貢献することは多いせいか、ビジネスプロセスの変革を IT 部門のミッションとしている企業は過半数を超えました。

（2）IT 部門発のビジネスイノベーション：ビジネスのタイプ別

・ ビジネスプロセス変革でミッションとして明示される企業：
  ・ ビジネスのタイプ別にてビジネスプロセス変革では大きな差がないです。
  ・ しかし、BtoC 企業のビジネスモデル変革でミッションとして明示される企業は「明示され、かつ、応えられる」（5.8%）、「明示され、かつ、一部応えられる」（24.3％）、「明示され、どちらともいえない」（7.5％）、「明示され、応えられていない」（6.9％）、計 44.5％で IT 部門ではビジネスモデル変革も視野に入れています。

（3）ビジネスイノベーション：変革を成功させる上でのポイント（1 位～3 位）

・ IT 部門発のビジネスイノベーション（ビジネスモデルの変革、ビジネスプロセスの変革）を成功させる最大のポイント（成功のポイント 1 位から 3 位まで複数回答）は、「経営と事業部門の間にあって、相互の意思疎通を緊密にすること」（1 位回答：39.2%、2 位回答：10.5%、3 位回答：9.3%、回答計 59.0％）、「社内各部門と IT 部門との意思疎通の緊密にすること」（1 位回答：18.7%、2 位回答：25.6%、3 位回答：13.4%、回答計 57.7％）でして、部門横断という IT 部門の強みを生かした部門間の関係作りが改革を左右します。

（4）自由記述より

・ 回答に寄せられた多くの具体例から、IT 部門からのビジネスイノベーション提案に際してのポイントを 10 項目にまとめました。

・ IT 部門発のビジネスイノベーションを進めるための「十か条」
  ① 実態を把握し可視化する
  ② 意識を改革する
  ③ 定期的に会合を持ち意思疎通を図る
  ④ 専門組織や担当を配置し権限を付与する
  ⑤ レポートラインを確立する
  ⑥ 経営レベルでの検討の場を設ける
  ⑦ 組織と組織の連携を図る
  ⑧ プロジェクトを設置する
  ⑨ 上流・超上流から取り組む
  ⑩ 人材を育成する

・ 多くの企業において、ビジネスイノベーションが IT 部門のミッションの一つに加えられるようになってきました。しかし、そうした、新たなミッションが重要になる一方で、社内に対する情報インフラサービスの提供など、ずっと IT 部門が担ってきた役割が重要でなくなるというわけではないです。むしろそうした従来の役割をきちんと担える IT 部門でなければ、ビジネスイノベーションという新たなミッションを担えないということを改めて認識することが必要です。

7. 情報セキュリティ(重要テーマ)

(1)情報セキュリティ対策

- 不安の割合がダントツで高いのは「ソーシャルメディアポリシーの作成」(私的利用(61.1%)、企業利用(57.5%))で、「データの暗号化等の保護策」(30.3%)に比較して、不安の大きさはほぼ 2 倍となっています。
- 標的型攻撃への対策状況を確認する目的で追加した「外部からの侵入検知防止策」(20.7%)は想定よりも不安が少ないです。従来型のファイアーウォールによる対策の実施を指した企業も少なからず含まれるのではないかと推測されます。

(2)大企業ほど標的型サイバー攻撃の標的になりやすいのは本当か

- 企業規模別標的型サイバー攻撃の有無:「全体の企業」で「攻撃を受けた」(10.2%)、「1000 人未満の企業」で「攻撃を受けた」(6.1%)、「1000 人以上の企業」で「攻撃を受けた」(19.1%)となり、大企業ほど攻撃を受けた割合が高いです。
- 攻撃を「受けていない」と回答した企業のうち、「ネットワーク境界における異常トラフィックの監視検知」を講じているのは 53.6%です。残りはどうやって攻撃を「受けていない」と判断したのか不明です。「攻撃を受けていても気づいていない」企業が含まれる可能性が否定できないです。
- 企業規模別標的型サイバー攻撃の対策実施率(複数回答):「全体」で「ネットワーク境界における異常トラフィックの監視検知」を講じているのは 56.3%です。「1000 人未満の企業」で「ネットワーク境界における異常トラフィックの監視検知」を講じているのは 49.2%です。「1000 人以上の企業」で「ネットワーク境界における異常トラフィックの監視検知」を講じているのは 70.0%です。検知は手段の導入が必要です。大企業の方が攻撃を受ける可能性が高い自覚があるがゆえに対策が進んだ結果と推測されます。

8. IT 予算(定点観測)

(1)IT 予算(開発費+保守運用費)の現状と今後の見通し

- IT 予算の増減(n=358):「増加」する割合(38.6%)から「減少」する割合(34.4%)を差し引いて求めた DI(Diffusion Index:増加割合－減少割合)値は＋4.2 ポイント、12 年度の＋1.7 ポイントから微増し、13 年度は対前年度比「増加」と「減少」が拮抗、4 社に 1 社(27.1%)は「不変」です。企業規模や業種によって傾向は変わりますが、マクロ的な視点で見ると、おおむね“横ばい”の状況になりそうです。

9. IT 投資マネジメント(定点観測)

(1)IT 部門が IT 投資で解決したい中期的な経営課題(1 位～3 位)

- 累計では「迅速な業績把握、情報把握(リアルタイム経営) 」(39.2%＝1 位:20.8%＋2 位:8.4%＋3 位:10.0%)と「業務プロセスの効率化(省力化、業務コスト削減)」(49.4%＝1 位:19.2%＋2 位:18.3%＋3 位:11.9%)が圧倒的に高く IT 投資の二本柱です。

10. IT 推進組織・IT 人材(定点観測)

(1)IT 推進体制(自社単体)

- 「現状」は「集権型」が 7 割(75.1%)、「連邦型」(23.3%)、「分散型」(1.6%)です。

11. グルーバル IT 戦略(定点観測)

(1)企業のグローバル化

- 業種グループ別ビジネスのグローバル化の状況:上場企業(全体:n＝1004)の 53.8%は既に海外進出済みです。業種グループ別では「機械器具製造(n＝256:72.5%)」と「素材製造(n＝189:75.8%)」の比率が高く、「金

融（n＝57：24.8％）」の比率は低いです。

12. BCP（定点観測）

（1）全社的な BCP の策定状況

・ システム障害や自然災害など、想定するリスク別の BCP（事業策定計画）の策定状況では、東日本大震災をきっかけに、BCP の策定に取り組む企業が着実に増えています。地震（直下型地震、または、大規模地震）を想定した BCP の「策定済み」企業は約半数です。「策定中」や「検討中」を含めると約 8 割に達しました。

Ⅲ. 質疑応答

1. IT 部門発のビジネスイノベーションを進めるための「十か条」

Q：調査結果においてビジネスイノベーションを進めるための「十か条」があります。「「十か条」は企業においてきちっとできているか？」がシステム監査する者のテーマです。これを確認しながら進めていくことになると思いますが、有効に機能していますか？

A：「十か条」は回答の自由記述からまとめたものです。例えば IT 利活用について作った IT がどう活用されているか、改善の仕組みがあるか、改善の仕組みはどういう形で行われているか、Exit（出口：記録者注記）としてシステムは廃棄しまうのか、その基準・対策、それが見える化されているか、という状況を今回調査しています。それを IT 利活用でまとめています。

・ IT 利活用の基準・体制作りをしている企業ほどむしろ「攻め」、IT 投資、ビジネスイノベーションに積極的です。わりとそういう企業は「守り」で従来型でないかといわれていますが、人材が揃っていますので、そういうところがビジネスイノベーションにいち早く対応できています。調査結果をクロスでみるとわかります。そういったことについて PDCA を回すべきと報告書に書くことにしています。

2. ビジネスイノベーションのための人材育成

Q：ビジネスイノベーションの一番の問題は人材育成です。ビジネスの者に IT 知識をつけさせる、IT 部門の者に企画の知識をつけさせる、中途採用、外部リソース・コンサルタントを活用する等、人材育成はどのような企業が多いですか？今回の調査で出ていますか？

A：調査では数字で出てくるほどはないです。今回は自由記述が中心です。加えて 50 社インタビューの結果から引用しています。今後発刊される「企業 IT 動向調査報告書 2013」に各社こんな取組をしていますと入れてあります。例えば、ビジネスと IT との融合ということですから、各社によってはビジネス側に IT を寄せたり、IT 側にビジネスを寄せたり、ミッションを与えプロジェクトにして混成チームをさせたりしますが、最近はビジネスと IT との混成チームが多いようです。混成チームからお互いに人が育つことが多いです。従来は、その領域の分担を決めていましたが、今は互いに領域を超えて行います。たとえば、ある会社では CIO が IT 部門とビジネス部門のサービス企画を2つ担当しており、その CIO 配下のビジネスと IT とで課長・部長クラスで週次にて 1 時間から 2 時間議論します。おかげで、最近は自然体で IT とビジネスがコミュニケーションできるようになってきた。もちろんそのため互いに勉強しなければなりません。また、ある会社ではビジネスの業務企画と IT 企画を意図的に同じフロアにするというシンプルな方法を採っています。いろいろな事例を集めていますが、ビジネスイノベーションの人材育成に必ず必要なものはミッションと意識改革です。ミッションは明示しなければなりません。意識改革は待っていてはダメで、出なさいです。この意識改革は CIO と IT 部門長の仕事です。詳しくは今後発刊される「企業 IT 動向調査報告書 2013」をお読みください。

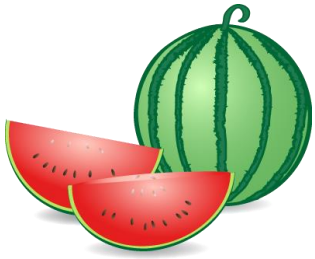
Ⅳ. おわりに

・ 今回の講演は、ビデオの撮影はしていません。資料は配布されたレジュメのみです。講演の中で、レジュメのほかに未公開資料が示されましたが、これらの内容についてもこの講演録には含まれていません。

・ 前年度の講演録【第 170 回月例研究会報告】(開催日:2012 年 4 月 25 日(水)、議題:「企業 IT 動向調査 2012 (2011 年度調査)～データで探るユーザー企業の IT 戦略～」＝2012 年 6 月発行会報№136 に掲載)を合わせてお読み下さると経年変化等について、より理解が深まります。

・ 詳細の内容は、今後発刊される「企業 IT 動向調査報告書2013」をお読みいただきたいと思います。(記録者追記)

以上



■【近畿支部　第１４０回定例研究会報告】

会員番号 2089　阪口博一（近畿支部）

１. テーマ　：「あなたのへそくり、奥様にばれていませんか」
～身近なテーマで、セキュリティをユーザに分かりやすく伝えよう～

２. 講師　：NTT西日本　大阪支店　粕淵　卓氏

３. 開催日時　：2013 年 5 月 17 日(金)　18:30～20:30

４. 開催場所　：大阪大学中之島センター　3階　講義室301

５. 講演概要　：

(1)アジェンダ

講義いただいた内容は以下のとおりである。

a. セキュリティとは　b. リスクマネジメント　c. 暗号　d. 認証　e. 脅威　f. PKI　g. まとめ

(2)内容

a. 「へそくり」の事情

本講義の導入部として、「複雑なセキュリティを身近なテーマでユーザにわかりやすく伝える」というコンセプトから、現在の「へそくり」事情を様々なWeb(ホームページ)の情報をもとに、へそくりを持っている人の割合、その金額、どうやって貯めたか、その隠し場所は、などの統計について紹介があった。

b. セキュリティとは

へそくりにおいて大切なことは、①バレないこと、②配偶者などに使われてしまわないこと、③自分が使いたいときにいつでも使えることである。これを情報セキュリティに例えるなら、それぞれ機密性、完全性、可用性(＝情報セキュリティの3要素)ということができる。

c. リスクマネジメント

リスクは（資産の重要性）×（脆弱性）×（脅威）で表すことができる。へそくりに例えるなら、（へそくりの額）×（隠し場所の危険性）×（見つかる可能性）ということになる。どんなリスクがあるのかを分析し、損失額と発生頻度を予測して評価し、その大きさによって対応策を考えることがリスクマネジメントになる。

リスク対応策には、①リスク低減、②リスク回避、③リスク移転、④リスク受容の 4 つがある。へそくりの場合は、それぞれ、①足のつかないオンラインバンク系に預けて言動にも注意する、②使ってしまう、親③に預ける、④見つかったらしょうがないと割り切る、といったものになる。

d. 暗号

「旧日本軍の暗号は米軍に比べて劣っていたか」、「同じ鍵で開く玄関の2重鍵は意味があるか」といった話題をもとに、暗号のアルゴリズムについての解説があった。また、「天才数学者が解読に何十年もかかる暗号は安全か」という話題から暗号方式の寿命、「100人の社員が10台の自転車をシェアする方法」という話題から公開鍵暗号方式についても説明された。

e. 認証

上記「暗号」と同様に、「ホテルでの鍵の受取り」、「銀行ATMでの4桁の暗証番号」といった話題から、認証に使われる情報についての説明、また「顔認証」や「生体認証」の問題点について説明があった。

f. 脅威

不正アクセスの攻撃者の目的（いやがらせ、営利目的など）、営利の場合はどれくらい儲けるのか、といった話題や、脅威の分類、企業が受ける損害額などの説明があった。

g. PKI（Public Key Infrastructure：公開鍵暗号基盤）

Web上での安全な通信基盤として、自分が証明する「デジタル署名」と、公的機関に証明してもらう「電子証明書」についての説明があった。

h. まとめ

まとめとして、BCM（事業継続性管理）の重要性について説明があった。要は、災害時を想定した計画をたて、リスクを分散し、継続的に活動することである。最初の話題「へそくり」に例えると、バレたときのことを想定し、隠し場所を分散させ、その対策を継続的に行うということになる。

6．所感

私は、現在、品質管理やリスク管理の事務局を仕事にしています。年に数回は情報セキュリティの教育研修の計画をたてて、時には自分で講師も行います。様々な階層の社員に機密性、完全性、可用性に脆弱性、脅威を説明するのも重要な仕事なのです。今回の講演内容の連絡をいただいたとき、「これだ！」と思い、早速申し込みました。社員の皆さんの次第に重くなってくる目を見ずに、情報セキュリティの研修ができるのであれば、本当に魅力です。

身近な「へそくり」を例にして、リスクマネジメントを説明するというのは、今回の講師である粕淵氏のオリジナルとのこと。セキュリティ対応策は、リスクを軽減するためのもので、すごくシンプルなもの、というか常識的であたりまえのことであるということが受講者に理解しやすいものとなっていると感じました。へそくりだけでなく、暗号や認証、不正アクセスなどの話題もわかりやすく興味をひく事例で説明されていて、私にとってはとても満足のいく講演でした。

以上

2013.06 投稿

注目情報　(2013.5～2013.6)

■【警察庁、「総合的なサイバー攻撃対策の強化について」公表】

2013 年 5 月 16 日　警察庁

警察庁は、サイバーテロの脅威の増大、サイバーインテリジェンス事案の続発に対応するため、サイバー攻撃対策の強化を図る通達を発出した。 主な内容としては、以下の 3 つを柱とするものとなっている。

(1) 司令塔機能の強化 － サイバー攻撃分析センターの設置 －

サイバー攻撃の実態解明等を進めるため、全国警察による捜査、情報収集、分析等の司令塔として「サイバー攻撃分析センター」を設置する。

(2) 現場対応力の強化

専門捜査員制度を活用し、サイバー攻撃特別捜査隊およびサイバー攻撃捜査に関する高度な専門的知識、技能等を有する警察職員を都道府県の枠を超えて広域的に運用する。そのほか、技術支援等の機能強化、捜査部門と技術部門の協同対策推進などを行う。

(3) 被害の未然防止および拡大防止のための官民連携の強化

事業者との情報共有枠組みの拡大および情報交換の活性化を進める

警察庁プレスリリース本文　http://www.npa.go.jp/keibi/biki3/250516kouhou.pdf

■【ＪＮＳＡ、「2012 年度　情報セキュリティ市場調査報告書」公開】

2013 年 5 月 31 日　NPO 日本ネットワークセキュリティ協会

NPO 日本ネットワークセキュリティ協会(JNSA)では、2004 年度以来継続して、日本国内の情報セキュリティ市場の調査を実施している。2012 年度調査は、アンケート調査、個別推計調査、インタビュー調査、全体集計・推計調査等を踏まえ、途中見直し等もはさんで実施し、2013 年 5 月にとりまとめた。

今回調査の基準年度とした 2011 年度は、ゲーム機ベンダ、防衛産業企業、国の機関などでサイバー攻撃被害が相次いだこと、リーマンショック以降投資が抑制されていた反動などにより市場はプラス成長を取り戻し、「情報セキュリティツール」が 3,648 億円(対前年度比成長率+3.0%)、「情報セキュリティサービス」が 3,278 億円(同+5.7%)で、合計 6,926 億円(同+4.3%)となった。

2012 年度については、引き続き標的型攻撃を中心とするサイバー脅威に対する備えを抜本的に見直す動き、IT 投資サイクルの循環、企業収益力の持ち直し等を背景に回復の動きが継続したと見られる。その結果「情報セキュリティツール」は 3,846 億円(同+5.4%)、「情報セキュリティサービス」は 3,463 億円(同+5.6%)となり、合計では 7,309 億円(同+5.5%)と、再び 7,000 億円台に達したものと推定される。

ホームページ　http://www.jnsa.org/result/2013/surv_mrk/

調査報告書　http://www.jnsa.org/result/2013/surv_mrk/2012fymarketresearchreport.pdf

2013.06 投稿

【協会主催イベント・セミナーのご案内（東京開催）】

■システム監査実務セミナー

今回ご案内するセミナーは、COSO-ERM モデルが提唱する、企業のリスク低減を図るためのシステム監査を目指す、「システム監査実務セミナー」(4 日間コース 1 泊 2 日×2 回)です。

企業の経営戦略及び業務の有効性と効率性の向上を図るためには、情報システムの活用が必須であり、その評価・改善を進めるためには、システム監査を実施することが有効です。

これまで実施されてきた業務監査(システム監査)では、現場の業務評価の視点を重視した監査が多く見受けられています。

今後は、コーポレートガバナンス、内部統制の面から、業務評価の視点に加えて、経営リスクに対する業務システムの有効性、効率性、安全性の向上の観点からの評価・改善提案が重要になってきます。

本セミナーは、当協会のシステム監査事例研究会で実施した、「システム監査サービス」の実際の監査事例を教材として、ロールプレイを中心とした演習ベース のきわめて実践的なコースで、全社的リスクマネジメントの枠組み(①経営戦略への貢献、②業務の有効性と効率性、③報告の信頼性、④関連法規の遵守)に ついてよりよく理解し、経営に役立つシステムの実現に資するシステム監査の方策を理解・修得することを目標にしております。

なお、本セミナーを受講した後、事後課題を提出頂き、その内容が適切であると判断された場合には、当協会が認定する公認システム監査人の認定に必要なシステム監査実務を 1 年間経験したものとみなされます。

また、本セミナーは、IT コーディネータ協会の「専門知識研修コース」(5.5 ポイント相当)に認定されています。

記

1. 日程及び会場

2013 年 8 月 31 日(土)～9 月 1 日(日)

2013 年 9 月 14 日(土)～15 日(日) ＜1 泊2日×2＞ どちらか一方のみの参加は不可

時間:土曜は 10:00～19:30、日曜は 09:00～15:00(進行状況により若干の変更が生じる場合があります。)

会場:晴海グランドホテル　〒104-0053 東京都中央区晴海 3-8-1 電話番号: 03-3533-7111

(最寄り駅 都営地下鉄大江戸線勝どき駅下車徒歩8分)

2. 費用

168,000 円(日本システム監査人協会会員)

189,000 円(一般)　　＊費用には、教材費・宿泊費・食事代・消費税が含まれます。

3. 副教材

情報システム監査実践マニュアル(第 2 版) 森北出版社 5,460 円

4. セミナーの概要

前半2日間 8/31 10 時～19 時 30 分、9/1 9 時～15 時

・システム監査実施手順及びシステム監査技法説明(座学)

・監査依頼者意向確認(ロールプレイ)

・トップインタビュー(ロールプレイ)

・監査テーマ決定(チーム作業)

・監査個別計画作成(チーム作業)
・資料収集の検討(チーム作業)

後半2日間　9/14　10 時～19 時 30 分、9/15　9 時～15 時
・予備調査(ロールプレイ)
・本調査(ロールプレイ)
・監査報告書作成(チーム作業)
・事実誤認有無等確認(チーム作業)
・監査報告会(ロールプレイ)

全 33 時間

教材　金融機関のデータセンターに関する監査

5. 受講していただきたい方

情報処理技術者(システム監査)資格保有者もしくは同等の知識を有する方、または内部監査、システム監査の経験がある方(上記条件に当てはまらない方は、お問合せください)

6. 募集人員

定員20名(最小催行人員10名)

7. 受講申込み等

問合せ先:日本システム監査人協会　セミナー事務局　miwa-toshiya@saaj.jp

受講申込み:http://www.saaj.or.jp/kenkyu/jitsumuseminar22.html　より申込みください。

■中堅企業向け「６ヶ月で構築するＰＭＳ」セミナー

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

詳細は、個人情報保護監査研究会主査　斎藤(saajjk7@saaj.jp)までお問い合わせください。

中堅企業向け「６ヶ月で構築するＰＭＳ」セミナー

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

■月例研究会

前述「5．1 システム監査活性化プロジェクト」の「月例研究会の活動紹介」の中でも掲載していますが、7 月および 8 月の月例研究会の開催予定は、以下のとおりです。

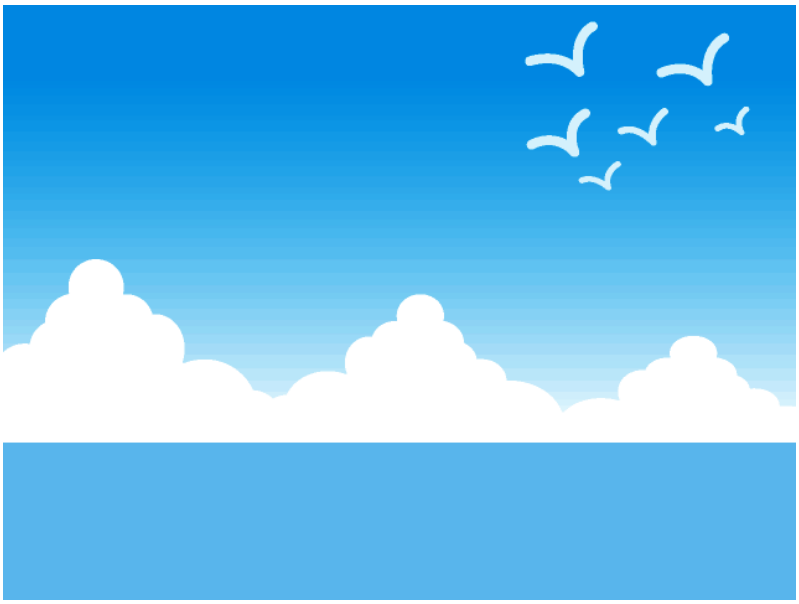
2013 年 7 月・第 183 回月例研究会

日　時　　：　2013 年 7 月 24 日(水)18:30～20:30
場　所　　：　機械振興会館　地下 2 階多目的ホール
講演テーマ：　「サイバー攻撃の脅威」(仮題)
講　師　　：　独立行政法人　情報処理推進機構　　渡辺貴仁氏

2013 年 8 月・第 184 回月例研究会

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

以上



2013.06 投稿

【協会主催イベント・セミナーのご案内（大阪開催）】

■近畿支部創設 25 周年記念研究大会（統一テーマ:システム監査の新領域への対応）

近畿支部は、1988 年(昭和 63 年)3 月 4 日に「関西支部」として発足しました。今年は、創設 25 周年の節目の年となることから、これを記念して研究大会を開催致します。

従来、システム監査が対象とした「情報システム」の位置付けが、クラウドサービスの拡大や事業継続の観点から多様化し、その結果、システム監査も多様化しています。こうした状況の中で、近畿支部の研究プロジェクト活動報告や会員の研究発表を行い、統一テーマである「システム監査の新領域への対応」について議論致します。多くの皆様の参加をお待ちしています。

記

1. 日時　　2013 年 7 月 6 日(土)13:00～17:00　懇親会 17:30～19:30

2. 場所　　大阪大学中之島センター　3階　講義室304
大阪市北区中之島 4-3-53　TEL 06-6444-2100(京阪中之島線　中之島駅より　徒歩約5分)

3. 参加費

日本システム監査人協会会員	1,000 円
ISACA大阪支部会員	1,000 円
一般	3,000 円
懇親会費(希望者のみ)	4,000 円

4. 定員　　80 名

5. プログラム

13:00～13:10	開会挨拶
13:10～13:30	コンプライアンスのシステム監査(雑賀努氏)
13:30～13:50	クラウド・コンピューティングのシステム監査(深瀬仁氏)
13:50～14:10	BCPと親和性の高い情報処理システムを目指して(永田淳次氏)
14:10～14:30	新しい「IT事業者評価制度」導入の政策提言(中田和男氏)
14:30～14:40	(休憩)
14:40～15:10	対策型監査の効果と重要性(木村修二氏　深瀬知寛氏)
15:10～15:40	保証型システム監査を可能にするアプローチ(松井秀雄氏)
15:40～15:50	(休憩)
15:50～16:50	パネルディスカッション「システム監査 2.0 への進化は可能か？」 (モデレータ:吉田博一氏　パネラー:研究プロジェクト報告者　他)
16:50～17:00	閉会挨拶
17:30～19:30	懇親会

6. 申込方法

http://www.saaj.or.jp/shibu/kinki/kinki_taikai2013.html　より申込みください。

申込締切:2013 月 6 月 21 日(金)

以上

2013.06 投稿

会報編集部からのお知らせ

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

□■ 1． 会報テーマについて

2013 年の会報の基調テーマは、「システム監査の普及促進」であり、3 か月ごとに「システム監査の普及促進」に関連するテーマを取り上げ、皆様と幅広く深く意見交換していきたいと考えています。

5 月号から今月号までの会報テーマは「システム監査活性化への提言」です。協会においても、「システム監査活性化プロジェクト」を中心に、システム監査活性化に向けて取り組んでいるところです。会報記事が、協会の部会、研究会、支部など、皆様の活動の場での議論の契機となれば幸いです。

次回 8 月号から 3 か月間の会報テーマは「システム監査の使いみち」です。皆様の投稿をお待ちしています。

□■ 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】（当協会ホームページ会員サイトから閲覧ください。パスワードが必要です）

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

■発行： NPO 法人　日本システム監査人協会　会報編集部

〒103-0025　東京都中央区日本橋茅場町2－8－8共同ビル6F

■ご質問は、下記のお問い合わせフォームよりお願いします。

【お問い合わせ】 http://www.saaj.or.jp/toiawase/

■会報は会員への連絡事項を含みますので、会員期間中の会員へ自動配布されます。

会員でない方は、購読申請・解除フォームに申請することで送付停止できます。

【送付停止】 http://www.skansanin.com/saaj/

■□■SAAJ会報担当━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

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

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

━━