

———— No. 136 (2012年6月 発行) ————

会報電子版の記事 目次

1. めだか (システム監査人のコラム)	.....	2
【システム監査人のディレンマ】		
【システム監査人の悩み—「ふしぎなキリスト教」を読んで】		
【システム監査人のなやみ】		
2. 投稿 【CSA資格の認知度は高まっています！】	.....	5
3. 会長コラム 【情報社会、システム監査、SAAJ】	.....	6
4. 研究会、セミナー開催報告、支部報告	.....	7
【第170回月例研究会報告】		
【第171回月例研究会報告】		
5. 注目情報 (5/1~6/15)	.....	15
【IPA 企業のITサービス継続の実現や強化、対策等を解説したガイドを公開】		
【IPA 標的型攻撃、スマートフォンの情報セキュリティ啓発用の映像コンテンツを公開】		
【IPA 情報処理技術者試験の「出題範囲」および「シラバス」改訂版を公開】		
【IPA 「情報セキュリティ白書 2012」を発行】		
【IPA 「Android アプリの脆弱性」に関するレポートを公開】		
6. 全国のイベント・セミナー情報	.....	16
(東京) 【月例研究会 (6月以降)】		
(事例研) 【7月例会、システム監査実務セミナー、課題解決セミナー】		
(東北支部) 【7月例会 (山形研修会)】		
(中部支部) 【7月例会】		
(九州支部) 【第255回月例会、西日本支部合同研究会】		
7. 会報編集部からのお知らせ	.....	19
会員限定記事	.....	20

**めだか 【 システム監査人のディレンマ 】**

システム監査は情報化が進むにつれて、まだまだ多いとは言えないが、社会のいろいろなところで確実にその活用が増えていると感じる。

我々、システム監査人の活躍の場が増えていくことは喜ばしい。

(ここでのシステム監査は、それ自体を単独で実施する場合の他、他の監査の中で、情報システムに係る部分にシステム監査の手法が活用される場合も含む。)

しかし、実施しているシステム監査の中味を見てみると、手放しに喜べるわけでもないように思う。中央省庁では、「業務・システム最適化指針 (ガイドライン)」などにシステム監査の導入が謳われ、情報システムの信頼性、有効性、効率性などをテーマとしたシステム監査が一部実施されている。

また、地方自治体、そして大手先進的企業でも同様な動きが見られる。

しかし、私の実感では、今日、システム監査の多くは、喫緊の問題となっているセキュリティに関する監査、I SMS、Pマークに係るマネジメントシステム監査など、セキュリティ、個人情報保護に係る監査が中心となっているのではないだろうか。

セキュリティの確保や個人情報保護は、情報システムが社会の中で機能していくために欠かせない、基本的なものである。従って、それがしっかりされていることを第三者的立場から点検、評価するシステム監査の意義は大きい。

しかし、セキュリティの確保や個人情報保護は、人の体で言えばバイタル (生命維持に必須) なもので、情報システムが社会の中で機能していく上では欠かせないが、それが確保されていればそれでよいというものでもない。人で言えば、バイタルな血圧、呼吸、体温等が良好なことは生きるうえで前提だが、その前提の上で如何に生きるか、Q O L (Quality of Life) が最も重要と言われる。

情報システムでも、セキュリティの確保や個人情報保護の上で、情報システムが如何に企業経営や国民生活の質の向上に役立つか (システムの信頼性、有効性、効率性) が問われる。

システム監査は、健全な情報化社会の発展に寄与するものとして存在するとされている。

セキュリティの確保や個人情報保護のレベルに留まっているならば、そのリスクを減らすために情報システムを使わなければいってしまうわけであるから、やはりシステム監査の本質 (最終目的) は情報システムの信頼性、有効性、効率性の評価にあるといえる。

情報システムの有効性、効率性の評価は、評価基準の整備もまだまだ不十分で、監査ノウハウの蓄積も乏しい。セキュリティの確保や個人情報保護の監査が増えるのは嬉しいが、それだけで喜んでいられるわけにもいかないのである。

(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。)

**めだか 【システム監査人の悩みー「ふしぎなキリスト教」を読んで】**

システム監査は、先の大戦後、アメリカから情報処理システム(EDPS)とともに情報処理システム監査として日本に渡来してきたと思います。情報システムは、技術革新によって、情報技術(IT)へとかわってきました。大型汎用機と端末機による情報システムから、多数のサーバーとPCやタブレット端末、スマホ等をネットワークで結んだクラウドコンピューティングなどの情報システムの利用が隆盛になってきています。このような変化は、誤解をおそれずに言えば、一神教的なシステムから、多神教的なシステムへの展開と考えてよいのではないのでしょうか。

最近、「ふしぎなキリスト教」という本を読みました。近代の考え方は、キリスト教に由来していることや、日本人の多くは、洋服を着ているものの、キリスト教に由来する近代の考え方をわからないままに、生活していることなどが書かれています。一神教では、Godのもとに、預言者、王、民があって、預言者は、Godの言葉を預かって、王や民に語りかける者として、民族の団結や独立のために警告を発し、民族の助けあいを説いたといわれています。

キリスト教では、イエスが福音を述べたあと、もう預言者はあられもないということだそうです。日本では、古来、多神教的な風土の中で、吉凶を占い、厄除けやご利益を神仏へ祈禱する巫女や陰陽師などはいても、そのような預言者はいませんでした。また、日本人は、抽象的なものより実用になるものを重んじ、しかもたんに切れるだけではない名刀をつくる匠などへの尊敬の伝統があって、現場のモノづくりに高い価値を感じていると思います。

システム監査やIT Auditは、対象となる情報システムが健全であるように、システム監査基準というフレームワークに則って、システム管理基準によって情報システムの健全性をチェックしています。システム監査基準は、トップダウンアプローチであるのに対して、システム管理基準は、現場レベルのリスク認識からリスクを分析し策定した対策をチェックリストにして監査を行うボトムアップアプローチによる部分が多いのではないかと思います。

クラウドコンピューティングなどの情報システムになりますと、システム監査のありかたも、今までとは変わっていかざるを得ないと思います。これから、システム監査やIT Auditで問われるものとは、汎用的なリスク認識だけではなく、監査対象となる情報システム毎、また情報システムのライフサイクル毎にリスクを認識してシステム管理基準(監査チェックリスト)を設計し、システム監査を運用していくことにあるように思います。

システム監査人に問われる力量とは、システム監査基準をしっかりと認識した上で、システム監査人自らが、担当する情報システムに内在するリスクを現場レベルで認識し監査チェックリストを設計する能力を持ち、システム監査を運用することができる力量であると思います。システム監査人は、システム監査の匠であるべきであると思います。

「ふしぎなキリスト教」橋爪大三郎・大澤真幸著(講談社現代新書)

(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。)

**めだか 【システム監査人のなやみ】**

4月から6月のお題、「システム監査人のなやみ」の最終月になってしまった。何とかギリギリで間に合わせるべく投稿する次第である。

システム監査人の最大の悩みは、何といても「システム監査」の認知度が極めて低く、また、レスpektされていないことであろう。第二は、その認知度の低さに付随して、4月号の「めだか」にあったように、システム監査人が独立した業として成り立っていないということではないか。

後者は、第一の問題に付随するものなので、まずは、前者の問題の原因を簡単に考察してみたい。

前者の原因は、大きく二つに分けられると思う。その一つはいわゆる企業における「監査」なるものが、日本では、その機能を十分に果たしていないことにある。一般に企業の「監査役」はその企業内の財務畑の人間の上がりポストという性格が強く、その任命も実質的に社長が行なっていることが多い。監査業務に必須の独立性が確保されていないのである。この弊害による事件は、枚挙にいとまがないほどである。

したがって、日本においては、法律に定められているからやっているという程度のもので、「監査」そのものがそもそもレスpektされていないのではないかと。度重なる事件の発生によって、近年、規制が厳しくなってきたというが、オリンパス事件等、まだまだである。

今や継続的イノベーションこそが企業のみならず国の存亡を決する最重要なイシューになっている。このイノベーションを継続させるためには、規制を緩和して、企業や個人の自由闊達な経済活動や社会活動を促す必要があるが、その自由闊達さが、野放図な、社会に害を与えるものにならないためには、事後規制としての「監査」制度こそが、その保証システムとして正しく機能し、かつ、社会全体としてこれがあるから安心と思われるほどに、信頼されるものになっていなければならない。

第二の原因は、日本では「システム」の果たす役割への企業の認識が、未だ相対的に低いことにあると思う。今のICT革命の凄まじさは、すべての業界において、ICTでの優位性を確保しない限り、競争優位を維持できないほどになっているにもかかわらず、である。また、一方で近頃かまびすしいビッグデータ、SNS等においては、個人情報保護というやっかいな問題が伴う。ちょっとした認識不足、考慮不足で企業イメージに取り返しのできないダメージを与えるばかりでなく、下手をすると、長い人類の歴史の上に勝ち取ってきた基本的人権という観念をも破壊することになりかねない。

このような重大なICTに関して、企業内で十分に議論がなされているのだろうか。そもそも、このICTの重要性が正しく日本の企業内で認識されているのだろうか。大いに疑問である。システムに関する認識がこの程度だとすると、「システム監査」に関する認知度が低くても当然であろう。

縷々述べてきたが、この二つの問題とも、日本の今後の生き残りに深くかかわるものである。言いたかったことは、システム監査人の認知度の低さの原因が、そのまま、日本の今日の低迷に繋がっているのではないかと、そして、その認識の向上はそれほど簡単なことではない、ということである。

皆さんはどうお考えだろうか。私の認識は大き過ぎるだろうか。

(逍遙庵)

(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

## ■【CSA資格の認知度は高まっています！】

## CSA 利用推進グループ

昨今の官公庁の業務発注や人材募集条件に、CSA資格取得者であることが条件として加わるようになって来ていることをご存知ですか？例えば昨年12月27日公告の経済産業省の「情報セキュリティ監査等業務 一式」の入札条件には業務担当する監査人の資格としてCSA資格が入っています。また、本年1月には会計検査院のシステム監査経験者の任期付職員募集でCSAが資格要件になっています。本年2月にも財務省で同様の人材募集がありました。

CSA資格はシステム監査人としての力量を担保する資格であることは勿論ですが、上述のように企業にとってもまた個人の公的資格としても十分メリットのある資格です。

協会としてもCSA資格の更なる認知度向上に向けて種々活動が続けているところです。特に、CSA・ASA資格者向けには「CSAフォーラム」というフェイスtoフェイスの会も設けて交流しています。

## 改めて、公認システム監査人(CSA)とは・・・

日本システム監査人協会による「公認システム監査人認定制度(2002年2月25日制定)」に基づく、システム監査人です。公認システム監査人(CSA)と公認システム監査人補(ASA)で構成されます。

CSA・ASAにはシステム監査技術者試験合格者(または同等能力者)で一定の実務経験を積んだシステム監査人を認定しています。実務経験については小論文と面接で審査します。更に資格継続には、継続的な実務及び教育受講が必須です。CSA・ASAは継続的に研鑽を続けている質の高い監査人といえます。

## CSAフォーラムに登録ください・・・

CSA・ASAの方々に「システム監査に関する実務や事例研究、理論研究等を通して、システム監査業務に役立つ研究を行う場を提供」することにより、「CSA・ASA同士がフェイスtoフェイスの交流をし、相互啓発や情報交換を行い、スキルを高め、よってCSA・ASAのステータス向上を図る」ことを目的に2008年7月に開設しました。

CSAフォーラムはこれまで14回開催しました。そのうち第11回までの概要を、協会会報No.120号・121号([http://www.saaj.or.jp/members/kaihou\\_dl.html](http://www.saaj.or.jp/members/kaihou_dl.html))に掲載しております。

CSAフォーラムはあらかじめフォーラムに参加登録されたCSA・ASAの方々へ開催案内しております。**現在、新規登録募集をしております(7月末締切り予定)**ので、是非皆様の事前登録をお待ちしております。

CSA資格の定期更新期限は毎年1月です。折角取得したCSA資格の失効が見込まれる方がおられます。連絡を受けた方は、今からでも復活は可能ですので更新手続きをしっかりと行い、是非一緒に活動致しましょう！



---

## 会長コラム

### 情報社会、システム監査、SAAJ

会長 沼野伸生

私たちは、農業革命、産業革命を人類史上の大変革として、学校の授業、教科書で学びました。そして、それに匹敵する歴史上の出来事として、今、情報革命が進んでいると言われます。しかし、その真っ只中にいると、日々の少しずつの変化の中に埋もれて、農業革命や産業革命に匹敵する変革の時代に生きている醍醐味を実感できる人はそう多くないのではと思います。きっと今から40～50年先の子供たちが、我々が学んだ、農業革命、産業革命と同様に、20世紀から21世紀にかけての情報革命の全体、そしてその時代の人々の行動を授業や教科書で体系に学ぶのでしょ

う。変革の時代は、変革を牽引するコア技術とその時代の人々の知恵で如何に使いこなすか、コントロールするかの試行錯誤、成功・失敗の繰り返しの時代です。例えば、情報社会と言われる今日は、ITの急速、飛躍的發展、進化と共に、それと表裏一体のリスクを如何にコントロールするかの試行錯誤の時代、すなわち情報システムの“不完全性”（安全性、信頼性、効率性等の追及における避けがたい失敗リスクの存在）を受入れつつも、知恵を絞ってそれを如何に利活用するかが問われている時代と言えます。

情報システムの“不完全性”は、情報システムの開発・提供者（ITの力を行使する者）、またその利用者（力の行使の影響を受ける者）が、情報革命の恩恵を享受する上で、共に受け入れなければならない現実です。そして、情報システムの“不完全性”を正面から受け入れ、かつ、利用者が積極的に情報システムを利活用していく前提は、情報システムの開発・提供者（ITの力を行使する者）と利用者（力の行使の影響を受ける者）の相互信頼関係を確立することです。そして、この相互信頼関係の確立には、情報システムの開発・提供者の説明責任遂行（やるべきことはやっていることを自ら説明すること）が不可欠であり、これに呼応して、この説明責任遂行と不可分の、説明責任遂行に信頼性を付与して実効あらしめる情報システム監査が求められることとなります。

考えてみれば、あるテーマについて潜在的に利害が対立する当事者間に、その当事者とは独立、かつ客観的立場の専門家（監査人）を置き、「監査」行為とその結果情報を介し、当事者間の信頼関係を醸成し、そのテーマの良好な発展を図る「監査」は、他の動物にない、人間の英知から生まれた、人間にしかない知恵の賜物かもしれません。

そして、この「監査」（情報システム監査）が、情報革命進行中の今日、情報システムの健全な利活用促進のために必要とされていると考えられます。

今から40～50年先の子供たちが、20世紀から21世紀にかけての情報革命の全体、そしてその時代の人々の行動を授業や教科書で体系に学ぶ時、当時の人々の知恵、行動の一つとして、情報システム監査の導入、活用が語られるかどうかは、今後のシステム監査の普及、また当協会（SAAJ）を始めシステム監査に関わる関係団体の活動、発展にかかっているのかもしれません。

**研究会、セミナー開催報告、支部報告****■【第170回月例研究会報告】**

会員No.355 岩崎 昭一

日時 平成24年4月25日(水) 18:30~20:30

場所 機会振興会館地下2Fホール

議題 企業IT動向調査2012(11年度調査)~データで探るユーザー企業のIT戦略~

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 原田 俊彦 氏

&lt;講演骨子&gt;

JUASでは毎年、経済産業省の委託を受け「企業IT動向調査」を実施してきました。当協会では毎年度(今まで3回)できるだけ早い時期の月例研究会において、JUASの方(去年は原田氏)をお招きして調査内容についての講演を頂いてきましたが、今年度も同様にJUASの原田氏をお招きして講演を頂きました。今年度の内容は、今までのものと少し内容・発表方法等が異なっています。

2011年4月のJUASの一般社団法人化に伴い、今回の調査は、経済産業省の委託事業としてではなく、JUASの自主事業として「企業IT動向調査」が実施されました。その結果、今までの調査以外に多くの調査項目が設けられ、発表の方法、時期もJUAS独自で決められています。既に調査内容・結果の一部は、

- ① プレスリリース(3月30日)されています。(JUASのホームページ参照)
- ② また調査の内容の詳細は、JUASから「企業IT動向調査報告書2012」(日経BP社 2012年5月28日)として発行される予定です。
- ③ 更に、日経コンピュータ(日経BP社)でも4/12発刊誌から4回にわたり“データで探る2012年度のIT戦略”と題して連載されています。

今回の月例研究会では、プレスリリースの内容のほか、この報告書の内容を先取りしたかたちで講演を頂きました。講演録を記述するに当たり、講演内容(調査結果)の詳細(図表及び数値等)は割愛し、調査のポイント、IT企業の動向について、キーワードを中心にまとめることとします。詳細な内容を知りたい方は、講演会のレジュメ、紹介した参考資料をご覧頂きたいと思います。

なお、本講演録は、当日会場で配布されたレジュメ(各支部へも送付済み)のほか、公開されているプレスリリース、日経コンピュータの内容も参考にしています。(筆者追記)

**I. 企業IT動向調査 2012(2011年度調査)の概要****(1) 調査の方法**

- (ア) アンケート調査(実施時期 11月、ユーザー企業IT部門 4000社対象、回答 1039社)、
- (イ) インタビュー調査(実施時期 11月~12年1月、ユーザー企業IT部門長、40社)

**(2) 調査の重点テーマ**

- (ア) BCP(事業継続計画)への取組み

2011年3月11日の東日本大震災で、事業やITの継続性に対する企業の意識が改めて問われていることを受けて、BCPへの取組みの変化を調査するとともに、IT部門として長期的な事業継続に向けた取組みへの指針を探っている。調査の結果、大震災を契機にBCPへの関心が高まり「BCPを定期的に見直す」との回答が急増し、リスク管理に対する意識変化がうかがえる。

## (イ) 超上流・IT利活用の実態と課題

企業におけるIT部門の役割は、より高度なものに変化している。今回の調査では、事業や業務の検討から始まり、システム化の方向性を定めるまでの「超上流」、そして開発後の「IT利用推進」に焦点を当て、現在のIT部門の実態と課題を調査し、今後のあり方を検討している。今回の調査でもシステム開発、運用の実務は外部委託している様子が見えてくる。

## (ウ) 定点観測

今までの調査において、以下の項目を継続的に調査しているため、これらの項目についても調査し、その後の変化の状況を把握することにした。特徴的な変化については、説明の都度、特記している。

- |         |             |            |
|---------|-------------|------------|
| ①IT推進組織 | ②IT人材       | ③グローバルIT戦略 |
| ④システム開発 | ⑤情報システムの信頼性 |            |

## (3) 主な調査結果

調査結果は、以下のように構成されている。いわば調査報告の目次と同様のものと思われるものである。講演会においては、レジュメを活用し、順を追って説明があった。

## 1. 回答企業のプロフィール

## 2. 最新トピックス

- |              |                 |
|--------------|-----------------|
| ①新規テクノロジーの採用 | ②IT予算の現状と今後の見通し |
| ③IT投資マネジメント  | ④ソフトウェアの採用と評価   |
| ⑤情報セキュリティ    |                 |

## 3. 重点テーマ

- |                    |
|--------------------|
| ①BCP(事業継続計画)への取り組み |
| ②超上流・IT利用活用の実態と課題  |

## 4. 定点観測

- |         |             |            |
|---------|-------------|------------|
| ①IT推進組織 | ②IT人材       | ③グローバルIT戦略 |
| ④システム開発 | ⑤情報システムの信頼性 |            |

## II. 調査結果

調査結果の詳細については割愛して、各調査項目(上記の表題)について、特徴的な内容を抽出し、2、3記述のこととする。より詳細な内容を知りたい方は、最初に記述した参考資料を入手し、読まれることをお勧めします。

## 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部門長に調査票を郵送で依頼し、1039社の回答があった。業種、従業員数、売上で分類すれば、次のとおりである。

- (1) 業種は、日本標準産業分類を参考に定めた26業種とし、更に建築・土木、素材製造、機械器具製造、商社・流通、金融、重要インフラ、サービスの7つの業種グループに分けられている。
- (2) 回答企業の従業員数は、大企業(1000人以上)1/3強、中堅企業(300~1000人未満)が1/3強、中小企業(300人未満)が1/3弱でほぼ同じ割合である。
- (3) 売上高については、超大企業(1兆円以上)4.6%、1000億円~1兆円未満:19.0%、100億円~1000億円未満:



50.0%、10億円～100億円未満:23.7%、10未満:2.8.0%となっている。

なお、この調査内容は、ITのユーザー企業として、日本の中核企業の調査結果と判断することができ、調査結果の信頼性は高いと思われる。(筆者追記)

## 2. 新規テクノロジーの採用(最新トピックス)

- (1) 導入率が最も高い「仮想化(サーバー)」は過半数以上の企業が使用する成熟した技術となっている。
- (2) 「タブレット端末」と「スマートフォン」は、今後導入率が大きく伸びると予想される。
- (3) IT基盤としてのクラウドの利用が本格的に立ち上がりつつある。特に、ユーザーが独自に構築・運用する「プライベート・クラウド」は一般的なIT基盤になりつつあると言える。
- (4) SaaSの導入済み割合は、「メール」が2割、「SFA・CRM」「その他」が1割前後であるが、アプリケーションの調達方法として無視できない存在になりつつある。
- (5) 懐疑的だったクラウドの導入が一気に積極的導入に変化してきている。特に売上高1000億円以上の企業で顕著な変化が見られる。

## 3. IT予算の現状と今後の見通し(最新トピックス)

- (1) 12年度のIT予算を「増やす」企業が4割弱、「減らす」企業が約3割となっている。増減の内訳で見ると、「増加」と「減少」が減り、「不変」が増加している傾向にある。
- (2) IT予算のDI値(Diffusion Index: 増加割合－減少割合)の次年度予測の推移を見ると、IT予算は、2010年度(▲4ポイント)を底に、回復基調だが(11年度: +6.4、12年度: +8.1)であり劇的な回復は見込めない。
- (3) すべての業種で12年度のIT予算のDI値がプラス、又はイーブンであるが、DI値が最も高かったのは、「重要インフラ(48.1、+29.6)」でDI値がマイナスからプラスに転じたのは、震災復興への期待が大きい「建築・土木」であった。
- (4) 売上高に対するIT予算の比率は、2年連続で減少している。売上の伸びにIT予算の伸びが追いついていない。売上高に占めるIT予算の比率は、全体平均では1.04%であり、「金融」が5.18%と突出している。平均以上は、重要インフラ(1.45%)、サービス(1.08%)のみである。

## 4. IT投資マネジメント(最新トピックス)

- (1) IT投資で解決したい中期的な経営課題については、上位から「業務プロセスの効率化」(50.0%)、「迅速な業務把握、情報把握(リアルタイム経営)」(42.3%)である。また、「IT開発・運用コストの削減」(25.5%)となっている。
- (2) IT投資マネジメントにおいて、最も重要な観点がIT投資に対する効果の評価であるが、事前評価を「常に実施」している企業は4割、事後評価を「常に実施」している企業は、わずか14.0%であり、なかなか進んでいない。
- (3) 「業務効率」「業務スピード」「業務品質・精度」についてのIT投資の「効果あり」としている企業が7から9割に達しているのに対し、「市場のシェア拡大」「製品・サービス開発力」については、IT投資の「効果なし」としている企業が7割強も存在している。

## 5. ソフトウェアの採用と評価(最新トピックス)

- (1) Windows7の導入については、11年度は、10年度の2倍であったが、12年度に若干遅延している。移行に当たった最大の課題は、「業務アプリケーションの互換性に問題がある」であり、「必要となるテストの範囲が不明」は大きく減少している。

(2)クライアントOSについては、「WindowsXP」が減少傾向にあり「Windows7」の導入が大幅に増加している。

#### 6. 情報セキュリティ(最新トピックス)

- (1)サイバー攻撃の現状については、この1年間に、「受けた」企業が1割強、「受けていない企業」が8割、「わからない」企業が1割弱であった。攻撃を受けた企業で「被害を受けた」企業は3割弱であった。
- (2)セキュリティ対策が進んでいないのは「ソーシャルメディアポリシーの作成」が2/3でダントツであり、次いで「データの暗号化等の保護対策」「情報資産のレベル分けによる適切な管理」「USBメモリ/CD-ROM等の書き出し・持ち出しの制限」がそれぞれ約3割程度ある。

#### 7. BCP(事業継続計画)への取組み(重点テーマ)

- (1)東日本大震災による被害と見えてきたリスクについては、直接間接に被害を被った企業は6割(直接の被害:4割弱、間接の被害:2割強)で、IT部門として対策が必要なリスクは、「多くのシステムが一箇所に集中している」ことであった。
- (2)導入済みの多い対策は、「外部のデータセンターの活用(4割)」と「ネットワークの多重化(3割)」である。今後は、「クラウド・コンピューティングへの転換(検討中:4割)」や「バックアップセンターの準備(検討中:3割)」が増加すると考えられる。
- (3)BCPを策定済みの企業は半数にも満たない状況であり、「システム障害」でも5割弱である。また、「風評被害」や「サイバーテロ」については、ほとんど進んでいない。今後は、大震災、大規模な自然災害のBCPを策定する企業が大幅に増加することが想定される。
- (4)「BCPは実践で機能したのか」の質問に対しては、2/3の企業がBCPが機能(十分機能した:1割強、おおむね機能した:5割強)したとしているが、別の見方をすると、9割弱の企業ではBCPに何らかの問題を抱えており、見直しが求められていことがわかる。

#### 8. 超上流・IT利活用の実態と課題(重点テーマ)

- (1)代表的な基幹業務システムの寿命は、「全体」では、14.6年となっている。07年度調査では、13.8年なので、この5年間で寿命が約1年伸びたことになる。事業環境の変化サイクルが短くなる一方で、システムの寿命は長くなる傾向にある。
- (2)超上流工程への取組みについて、システム開発以前の超上流に注力することが、システム化プロジェクトが成功し、運用でその目的を達成する大きな要因となる。しかし、この領域は属人的で標準的な方法論が少ない等の課題も多い。
- (3)超上流活動の充実を示すアプリケーション・オーナー制度を採用している企業は、5社に1社しかないが、売上高1兆円以上では8割に達している。業種グループ別では「金融」「重要インフラ」で採用が進んでいる。
- (4)超上流への取組みについては、全体として組織的な取組みがまだまだ不足している。「組織的に実践できない」が半数を超える項目が10/17にもなり、実施すべき課題として認識はあっても実践する困難さを示している。

#### 9. IT推進組織(定点観測)

- (1)情報子会社の6割が売上の50%以上を親会社に依存しているが、その一方で、「外販比率が50%以上」の子会社も増加している。また、開発委託先(情報子会社をもつ親会社)からみる(推測すると)、子会社の6割が開発を4割が保守運用を主な事業としている。

(2)経営層からIT部門への期待領域が広がってきている。最近では、IT部門の6割が「ビジネスモデルの変革」を期待され、8割が「ビジネスプロセスの変革」を期待されている。

#### 10. IT人材(定点観測)

(1)IT要員に必要な能力と現状については、自社IT部門内で確保・育成する必要性が高い能力として、上位は、「業務システムの改善提案」と「IT戦略策定・IT企画」となっている。11年度は「情報セキュリティ・リスク管理」も重要視されているのが特徴である。

(2)CIOの形態とミッションについては、「IT担当役員が経営トップとIT部門の間に位置する」形態が4割(大企業では過半数)であり、中小企業では、IT担当役員が不在の企業が6割ある。今後は、CIOは経営戦略に近いミッションに傾注していくと思われる。

#### 11. グローバルIT戦略(定点観測)

(1)既に半数以上が海外に進出し増加傾向にある。業種グループ別では「機械器具製造」3/4と「素材製造」:2/3)の比率が高い。また大企業では7割が、中堅企業でも約半数が海外に進出している。

(2)IT投資の最重点テーマに「グローバル化への対応」を掲げる企業が増加している。特に目立つのは「素材製造」「機械器具製造」などの製造業である。注目すべきは、ここに来て中堅中小企業にも及んでいる兆しが見られる点である。

#### 12. システム開発(定点観測)

(1)システム開発における工期・予算・品質の状況について、500人月以上の大規模プロジェクトの「工期」は、07年度から改善傾向にあり、工期の延長は40.5%で、07年度から16.1ポイント改善はしたものの、まだまだ改善の余地は大きい。

(2)日本では工期や予算より品質を重視したプロジェクト管理が主流となっている。不満の割合は年々改善しているものの、工期や予算に比べると改善幅は小さい。品質に対する要求レベルが高くなりつつあるのもその要因の1つかもしれない。日本の品質要求(信頼性への要求)は、海外と比較すると、10倍近い差がある。

#### 13. 情報システムの信頼性(定点観測)

(1)システム障害の「見せる化」が進み、重大障害の減少に貢献している。役員以上に報告する「システム障害の見せる化」が浸透し、そのプラス効果として、「中断障害が減少する」結果をもたらしていると考えられる。

(2)事業が中断した障害原因は例年と同じく「ハードウェア故障」「ネットワーク(キャリア)の障害」「ネットワーク(自社)の物理的故障」がトップ3で年次別に見ると減少傾向にある。ネットワーク系の障害は、事業中断に繋がりがやすい。

#### III. おわりに

今回の講演は、ビデオの撮影はしていない。資料は配布されたレジюмеのみである。講演の中で、レジюмеのほかにも幾つかの未公開資料が示されたが、これらの内容についてもこの講演録には含まれていない。本講演録は、今後発行される「企業IT動向調査報告書2012」の紹介としての位置づけであると理解してほしいことを付記しておく。

(筆者追記)

以上

## ■【第171回 月例研究会報告】

会員 No.2090 遠藤 誠(理事)

日時:平成24年5月21日(月)18:30~20:30

場所:機械振興会館地下2階

議題:ソフトウェア品質監査制度~ソフトウェアの品質説明力強化の取り組み~

講師:独立行政法人情報処理推進機構 技術本部ソフトウェア・エンジニアリング・センター

統合系プロジェクト&amp;組込み系プロジェクトサブリーダー 工学博士 田丸 喜一郎 氏

参加者数:112名

## 〈講演骨子〉

我が国の製品・システムは品質が高いと言われている。しかしながら、米国を中心に第三者による検証・妥当性・確認等の裏づけをもって、その品質を説明できる能力(品質説明力)が求められている。このような品質に対する市場の考え方の変化に対応するため、経済産業省とIPAにて「ソフトウェア品質監査制度(仮称)」の検討を進めているところである。2010年度から、ソフトウェア品質管理に精通した有識者、開発企業及び検証サービス事業者などの代表を交え、国際市場における我が国製品の品質に対する正しい評価を確立するための制度のあり方について議論してきた。保証型の監査制度として利用者に対して合理的な保証を与え、適切な品質が保たれていることを広く知らしめる制度にしていくことを目指している。

(本セミナーでは、本制度の背景や狙い、枠組み、監査制度等についてご説明をしていただきました。)

## 〈講演内容〉

## ●本制度の背景や狙い

社会的な背景として、高度情報ネットワーク社会の登場である。どの家庭でも使われている電化製品(テレビ、冷蔵庫等)や自動車などには、組込みソフトウェアが存在する。電化製品で約3,000万行にも上り、自動車に至っては、将来1億行のソフトウェアが記述されることになりつつある。そして、これら組込みソフトウェアが至る所で使われ、全体的に統合化され、統合的につながったシステム、サイバーフィジカルシステム(米国)、スマートデジタルシステム(欧州)とも呼ばれるようになってきている。

このような中で、個々のアイテムをそれぞれつなげていった時に、全体のシステムが正常に動くか検証する仕組みがないことが問題となってきている。どこかの部分でソフトウェアのミスがあれば、火災にとどまらず、装置故障により有害物質を出すことになったり、耐震強度を劣化させることになったり、広く利用者にとって被害が及ぶ可能性があり、リスクが拡大することにもなりかねない。

統合システム実現の課題について調査をすると、「全体の品質確保」、「利用者、利用目的、利用シーンの定義が不十分であること」、「他産業、他分野の文化や技術の理解」等が課題として挙げられている。製品出荷後の不具合の発生製品率が2009年ごろから上がってきている。また、製品出荷後の1製品当たりの不具合件数の推移を見ても、繰り返し同製品に不具合が出るケースがあり、一向に減ることがない状況である。製品出荷後に発生した不具合の原因を調べると、「ソフトウェア」が約28%で一番多く、利用者を含めた、「操作・使用環境等の利用者」、「他製品・他システムとの接続」、「取扱説明書・表示」等の原因が増えつつあることに留意したい。

一方、第180回国会に消費者庁が「消費者安全法の一部を改正する法律案」を提出している。この改正には身体・生命に関わる事故の原因究明をするために、強い調査権限を持った事故調査委員会を設置することが含まれている。ソフトウェアのミスで身体・生命に関わる事故が発生すれば、事故原因究明対象となりソフトウェアの品質説



明が事業者に求められることも想定される。

このようなことを踏まえ、利用者から見て安心・安全なソフトウェアソフトウェア、装置であると云えるような制度づくりとして、ソフトウェア品質監査制度(仮称)を検討しているところである。利用者に対して、高い品質を客観的に説明できること、業界自らがその必要性を認識していることが本制度を進める上で後押しになっている。

### ● 枠組み

このように、第三者による検証、妥当性確認による品質説明力強化の必要性が高まっていることから、制度づくりに向けて進んでいる。業界からは、本制度について、以下のような要望が示されている。

- ・国際的な制度
- ・先端開発にも適用できる高い機密保持性を持つ制度
- ・コストとのバランスが取れる制度
- ・義務ではなく、任意の制度
- ・既存の規格認証との重複が少ない/しない制度
- ・システムに関係する複数の業界で共有・支持できる制度
- ・品質向上に有効な制度

### ● 監査制度

すでに確立された公認会計士等による財務諸表監査制度を参考に枠組みを作っているところであるが、本制度にはいくつかの特徴がある。たとえば、審査基準を策定する機関を設けるが、審査基準は一つではない。様々な分野に適した複数の審査基準を作る予定である。利用者・利用情報、障害情報を収集する。利用品質も考慮した品質監査のための基礎情報であり、産業・製品別の審査基準の策定と維持に貢献する情報として参照できる仕組みを考えている。また、監査人協会を設置し、監査人の業務査察、能力維持のための継続的な教育研修を提供する場も設置したいと考えている。

監査には、助言型監査もあるが、本制度は、助言型ではなく、保証型の監査であり、「主題情報はすべて重要な点において適正に表示されている」という意見表明をする。また、監査人は、外部監査人と企業内部の監査人との間で、その役割と責任範囲を分けて作業を行う。事業会社においては、依然として機密性が高い企業秘密情報の領域を守る必要があるため、情報開示ができない領域については内部監査人が行う。意見表明するためには、直接機密情報に触れなくても内部監査人が行った作業内容・結果についての検証をして外部監査との連携をとる等の工夫をすることになるだろう。

監査へのコストはどの程度が適切であるかという議論がある。一つのベースラインとしてソフト開発費用の10%程度が適切ではないかという考えがある。わが国のソフト開発費用は約3兆円であり、約3,000億円程度の市場と概算している。

### ● 今後のスケジュール

平成24年夏ごろ、IPAは第二次中間報告を公開する予定、また同年度に、品質監査制度推進部会(消費者団体や大学教授等中立的な立場の方のみ選定)を設置し、制度適用先行分野を選定し、そこから実験的に模擬実験をしてもらう。その実験報告を踏まえて、制度評価改善を25年度に行い、26年度から監査業務開始というスケジュール感で取り組んでいこうとしている。



**(主な Q&A)**

1. これまでの認証制度はプロセス中心に審査・評価をしてきているため、対象そのものを評価すると云うことになっていない。あまり、有益な制度だと思っていない。これと本制度は同じことにならないのか？どこが違うのか？

——>プロセスの確認のみではなく、機能、要件定義書の設計内容、ニーズの内容の妥当性等上流工程の内容についても確認が必要である。また、トレーサビリティを調べて、確認をしたり、一般社団法人TERAS に登録された仕様書、要求書に対応できているのかの形式確認も含まれる。

2. ギャランティの保証ではなく、アシュアランスの保証ということで、保証の限界があると云うことで、理解するが、実務的にどこまで合理的な保証の線が引けるのか疑問がある

——>たしかにギャランティはできない、合理的な保証である。事故・障害についての保証はしない。被害者に対する保証とは何か、たとえば、何かあった場合には損害賠償をするようなシステムを検討する必要がある。

3. 本制度の監査人とはどんなバックグラウンドがある人を想定しているのか？

——>ある程度その業界、分野で経験を積んだ熟練者の方、監査や認証審査業務に長年携わった方などに先陣を切ってやってもらいたいと考えるが、具体的な資格要件はこれから決まることになるだろう。

4. 認証マークについてどんな考えを持っているのか？

——>取得した企業の一覧を公開するとか、マークの表示をするとかこれから議論することになるだろう。

5. ISO化を考えているか？

——>検討課題である。国際社会で通用する制度にすべきである。さらに、業界では、さまざまな認証システムを一つにまとめて、全てが含まれていると云った認証をしてもらえるような最終形が求められてもいる。これから議論することになる。

以上

**注目情報 (2012/5/1~6/15)****■【IPA 企業のITサービス継続の実現や強化、対策等を解説したガイドを公開】 (2012/5/8 発表)**

IPA(独立行政法人情報処理推進機構、理事長:藤江 一正)技術本部 ソフトウェア・エンジニアリング・センター(以下、SEC)は、一般企業等における「IT サービス継続(\*1)」の実現や強化に向けた基本的な考え方や、必要な対策の選択・実施の方法についてまとめたガイドを公開しました。

URL: <http://sec.ipa.go.jp/reports/20120508.html>

**■【IPA 標的型攻撃、スマートフォンをテーマにした情報セキュリティ啓発用の映像コンテンツを公開】 (2012/5/9 発表)**

IPA(独立行政法人情報処理推進機構、理事長:藤江 一正)は、「標的型攻撃(\*1)」および「スマートフォン」をテーマにした情報セキュリティ啓発用の映像コンテンツを2種制作し、2012年5月9日から「IPA Channel(\*2)」にて公開するとともに、情報セキュリティ研修用DVDの配布受付を開始しました。

URL: <http://www.ipa.go.jp/security/keihatsu/videos/>

**■【IPA 情報処理技術者試験の「出題範囲」および「シラバス」改訂版を公開】 (2012/5/22 発表)**

IPA(独立行政法人情報処理推進機構、理事長:藤江 一正)情報処理技術者試験センターは、「共通キャリア・スキルフレームワーク」の「知識体系(BOK:Body of Knowledge)」の最新版に対応するとともに、ITの新しい技術動向やビジネス環境の変化等をより的確に反映することを目的として、全試験区分の「出題範囲」および「シラバス(情報処理技術者試験における知識・技能の細目)」について見直しを実施し、その改訂版を公開しました。

URL: [http://www.iitec.ipa.go.jp/1\\_04hanni\\_sukiru/\\_index\\_hanni\\_skill.html](http://www.iitec.ipa.go.jp/1_04hanni_sukiru/_index_hanni_skill.html)

**■【IPA 「情報セキュリティ白書2012」を発行】 (2012/6/1 発表)**

IPA(独立行政法人情報処理推進機構、理事長:藤江 一正)は、ITの専門家や技術者だけでなく、一般の利用者にも情報セキュリティの現状を周知することを目的に、国内外の注目すべき情報セキュリティ事件・事故や、新しいサービス・情報機器の利用拡大による新たな脅威など、広く情報セキュリティに関する出来事や状況をまとめ、「情報セキュリティ白書2012」として、2012年6月1日から販売を開始しました。

URL: <http://www.ipa.go.jp/security/publications/hakusyo/2012/hakusho2012.html>

**■【IPA 『Androidアプリの脆弱性』に関するレポートを公開】 (2012/6/13 発表)**

IPA(独立行政法人情報処理推進機構、理事長:藤江 一正)は、IPAに届け出られるAndroidアプリの脆弱性関連情報が2011年後半から増加していることを踏まえ、それらを分析して脆弱性を作り込みやすいポイントをまとめ、技術レポート「IPAテクニカルウォッチ」として公開しました。

URL: <http://www.ipa.go.jp/about/technicalwatch/20120613.html>

**全国のイベント・セミナー情報****■【東京・月例研究会（6月以降）】****【6月・第172回月例研究会】**

- 1.日時:2012年6月20日(水)18:30~20:30
- 2.場所:機械振興会館 地下2階多目的ホール
- 3.講演テーマ:「社会保障と税に関わる番号制度について」
- 4.講師:内閣官房 社会保障改革担当室 参事官補佐、弁護士 水町 雅子 氏

**【7月・第173回月例研究会】**

- 1.日時: 2012年7月20日(金)18:30~20:30
- 2.場所: 機械振興会館 地下2階多目的ホール
- 3.講演テーマ:「不正アクセス防止対策に関する行動」(仮題)
- 4.講師: 警察庁生活安全局情報技術犯罪対策課 専門官(防犯対策) 人見友章 氏(予定)

**【8月・第174回月例研究会】**

- 1.日時: 2012年8月29日(水)18:30~20:30
- 2.場所: 機械振興会館 地下2階多目的ホール
- 3.講演テーマ:「BCP発動の実際と見直しポイント」(仮題)
- 4.講師: 株式会社 富士通総研 第二コンサルティング本部 BCM事業部長 伊藤毅 氏

**【9月・第175回月例研究会】**

- 1.日時: 2012年9月27日(木)
- 2.講師: 東京海上日動システムズ 横塚 裕志 氏(代表取締役社長)  
日経コンピュータ掲載の講座「SEを鍛える開講横塚塾」他の連載記事の著者
- 3.内容: 調整中

※ 会員サービス向上の一環として、  
今年度は、会員会費を2,000円から1,000円に値下げいたします。  
また、開催場所がこれまでと変更になっておりますので、ご注意願います

**■【事例研究会】****【7月例会】**

- 1.日時：7月4日(水) 18:30- (第2水曜になります。ご注意ください)
- 2.場所：中央区立八丁堀区民館  
[http://www.pb-k.jp/city.chuo.7kuminkan/hachobori\\_map.html](http://www.pb-k.jp/city.chuo.7kuminkan/hachobori_map.html)
- 3.内容：監査ノウハウ白熱教室：「開発プロジェクトにおける監査」野田氏

**【システム監査実務セミナー】**

- 1.日程：(前半)8月25日(土)、26日(日)  
(後半)9月8日(土)、9日(日)
- 2.場所：いずれも晴海グランドホテル(宿泊は、隣接の東京海員会館)を予定
- 3.内容：近日中に開催案内をHPに掲載予定

**【課題解決セミナー】**

- 1.日程：9月1日(土)
- 2.場所：未定
- 3.内容：近日中に開催案内をHPに掲載予定

**■【東北支部】****【月例会(山形研修会)】**

- 1.日時：平成24年6月23日(土) 14時～17時  
平成24年6月24日(日) 9時～12時
- 2.場所：ホテル サンチェリー(山形県寒河江市本町1-2-23)会議室
- 3.内容：(1日目)  
研修1：講演「システム監査法制化研究会の提言」(田淵隆明氏)  
研修2：システム監査法制化についての意見交換  
(2日目)  
研修3：スマートフォン・クラウドのセキュリティについての意見交換  
(※イベントとして、1日目の研修前に「そば打ち体験兼昼食会」、1日目の研修後に「懇親会」、  
2日目の研修後に「さくらんぼ狩り」を計画)

**■【中部支部】****【7月例会】**

1. 日時: 7月21日(土)14:00~17:00
2. 会場: 東桜第1ビル
3. 内容: (1) 協会連絡事項など
  - ・本部理事会報告(2) 西日本合同研究会(6月30日)の参加報告
- (3) 中部支部 SAAJ・JISTA 合同研究会(11月)の進め方について(意見交換)
- (4) 研究会
  - ・スマートコミュニティに関する動向について(その2)
  - ・3月テーマの続編 若原さん(5) 懇親会

**■【九州支部】****【第255回月例会】**

- ・日時: 2012年6月23日(土)15:00-17:00
- ・場所: 早良市民センター 第2会議室
- ・内容: - 報告/連絡事項(15:00~15:30)
- 発表研究事項(15:30~17:00)

**【西日本支部合同研究会】**

- ・日時: 2012年6月30日(土)13:00~17:00
- ・場所: 福岡県 Ruby・コンテンツ産業振興センター(福岡市)
- ・内容: - テーマ『災害に備えたシステム監査』



## 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4月～6月発行の会報テーマは「システム監査人としての悩み」でした。如何でしたでしょうか？ システム監査人は、そのミッションが高いが故に「悩み」も尽きないと思われれます。SAAJにはそんな悩みを持ちながらも未来に向かって羽ばたこうとしている仲間が大勢います。研究会、月例会、CSA フォーラム、支部活動、及び懇親会等を通じて大いに語り合い、活力を養いましょう。7～9月号のテーマは、「システム監査のすゝめ」です。会員増強プロジェクトと歩調を合わせて活動します。他にも議論したいテーマ等がございましたら是非会報担当へご連絡ください。

### □■ 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。

気に入った記事があったら、直接、その場所にコメントを記入できます。著者、投稿者と意見交換できます。コメント記入、投稿は、気になった記事の下部コメント欄に直接入力し、投稿ボタンをクリックするだけです。動画でも紹介しますので、参考にしてください。

( <http://www.skansanin.com/saaj/> の記事、「コメントを投稿される方へ」 )

### □■ 3. S A A J 会報編集担当より お知らせ

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](mailto: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/toiwase/>

■送付停止は、購読申請・解除フォームに申し込んでください。

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

Copyright(C)2012、NPO 法人 日本システム監査人協会

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

■□■ S A A J 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、藤沢 博、藤野明夫

投稿用アドレス: [saajeditor ☆ saaj.jp](mailto:saajeditor@saaj.jp)