特定非営利活動法人
日本システム監査人協会報

2013年3月号
No 144

No. 144（2013年3月号）<2月20日発行>

梅一輪一輪ほどの暖かさ。
春の足音が聞こえてきます。

会報電子版の記事　目次

2013.02 投稿

めだか　【システム監査人の足下は大丈夫か？（システム監査の普及促進）】

新年から3ヶ月間、会報テーマが「システム監査の普及促進」となっている。

そこで、「システム監査の普及促進」について、監査の実施者（監査人）、利用者（被監査部門）、そして、そもそも「システム監査」とは何なのかに焦点をあて思うところを綴ってみたいと考え、前回は、まずそもそも「システム監査」とは何なのかを取り上げた。

今回は、監査の実施者（監査人）に焦点をあて「システム監査の普及促進」を考えてみたい。

システム監査人、及び関係団体は自らの活躍の場を求め、システム監査の必要性をそれぞれに、またいろいろな場で訴えている。社会で第三者評価の活用が一般化していることから、情報社会の進展と相俟って、第三者評価の一つであるシステム監査の一層の普及が見込まれると説いているところもある。また、現に、行政情報システム等ではシステム監査の活用がガイドラインに謳われ、また、サイバー攻撃の脅威が現実のものとなり、システム監査の一つであるセキュリティ監査の需要も徐々に増加していると聞く。

しかし、システム監査における評価基準の整備、システム監査の実務ノウハウの集積は十分に進んでいるとは言えず、また、その前提となるシステム監査の理論の深まりも見えず、結果、システム監査人の教育の幅、厚みも広がっている（増している）とは言えないのが現状ではないだろうか。

例えば、経済産業省が公表しているシステム監査基準、システム管理基準は日本におけるシステム監査の規範的なものであるが、平成16年に改訂されて以来改定はされてなく、また深さ、幅の詳細化もあまり見られない。情報社会は保有から利用への転換も意味するクラウドサービス、また、タブレット、スマートフォンなどの新たな端末の活用を含めたBYODの動き（情報システムの利用環境の激変）、そしてサイバー攻撃の日常化など、大きな変化の中で新たな脅威も日々生まれているのに、である。例えばSAAJは、「システム管理基準 for オフショア Ver1」を策定、公開し、関係機関からの照会、活用がされていると聞く。しかし、それに続く基準の公開はなく、これも十分とは言えない。

システム監査人の中には、システム監査が普及しないのは法制化がされないことが大きな要因で、何とか法制化を進めるべきと主張する方も多い。それも必要かもしれないが、システム監査の理論の一層の深化、実践ノウハウ蓄積・体系化、システム監査実施の拠り所となる具体的評価基準の整備・拡充、そしてシステム監査人の学習の場の一層の拡大なども足下の問題として極めて重要ではないだろうか。情報社会の進展、そしてそれに伴い留めなく発生する新たな脅威の現実を考えると、スピードはともかく、情報社会の恩恵を受け続けるために必要な人間の知恵の一つとして、システム監査のニーズは間違いなく高まると思う。いざ、ではシステム監査をとなった途端にあたふたとなり、内容の乏しいアウトプットしか出せなくては、必要性を叫んでいた者として社会からの信頼は得られない。

システム監査人は、システム監査の必要性を発信すると共に、その期待に応える成果が出せるシステム監査ができるよう、自身の足下にも目を向け、日々地道な蓄積、研鑽を続けなければ、「システム監査の普及促進」はあり得ないのではないか。

（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。）

2013.2 投稿

めだか【 Ｃｙｂｅｒ-Ｐｈｙｓｉｃａｌ Ｓｙｓｔｅｍｓ】

最近のＩＴの進展は、まさに革命的といってよい。そしてその活用は、ビジネス構造そのものを根底から覆すのみならず、社会インフラに適用すれば社会構造そのものの大転換を促す可能性を秘めている。しかし、このような可能性があるにもかかわらず、多くの企業や政府、自治体もその成果を十分に活かすには未だ至っていない。

なぜであろうか。それは我々ＩＴに携わるものが現在進行中のＩＴ革命の本質を未だ正確に捉えられず、したがってそれを活用した社会変革の展望を正確に描くことができないからではないだろうか。

このあたりことを的確に展望した解説記事を見つけたのでご紹介したい。それは、情報処理学会誌「情報処理」2013 年 2 月号(2013 年 1 月 15 日発行)の解説「IT 融合社会 － 情報技術の新たな地平線 －」(PP150-155、執筆者：丸山宏、佐々木康裕)である。

この記事の主な主張は、ＩＴ革命による社会変革はまだ始まったばかりであり、これからが本番であるということである。そして、もはやＩＴは特殊な人たちが携わるのではなく全ての人々がＩＴを活用した種々の変革に携わるべきで、それによって今までとは異なる新しい社会が開けると論じている。このような社会システムを「Ｃｙｂｅｒ-Ｐｈｙｓｉｃａｌ Ｓｙｓｔｅｍｓ（ＣＰＳ)」と呼ぶ。

このネーミングは、今、現に起こりつつあり、これから起こるであろう社会変革を的確に表していると思う。その意味するところは、まさに、その言葉どおり、実世界とＩＴが緊密に連携、融合した世界である。具体例として、個々の歩行者、自動車、自転車等の動きを完全に把握し、それに基づく適切な制御や警告による交通事故のない都市の実現や、人々の好みや健康上の理由に合わせた個人別農業といったものが紹介されている。

たいへん示唆に富む内容なので、是非、ご一読いただきたい。情報処理学会誌「情報処理」の記事は情報処理学会会員以外でも同学会電子図書館の HP(http://www.ipsj.or.jp/e-library/ixsq.html)からＰＤＦ形式で入手可能(非会員は有料)である。

さて、ＣＰＳと我々システム監査人との関係である。このような社会、すなわち、ＩＴがリアルな社会と完全に融合した社会においては、その融合したシステムが、そのシステム構築の戦略目標の具現性、また、安全性、有効性、効率性、信頼性およびコンプライアンスといったシステム管理基準にうたっている事項を満足しているかを監査することが極めて重要である。なぜなら、このシステムは、人の生命、財産、さらには、社会の安全性、有効性、信頼性等にも直接、関わるからである。現在の社会におけるシステム監査の果たす役割とは比べものにならないくらい重い役割を担うことになる。

我々も、このような重責を担うであろう近未来の社会に向けて、古典的なＩＴの知識や技術、ＩＴの世界に閉じた知識や技術のみならず、その拡大する適用業務やシステムに係る知識や技術を身につけ、さらには将来の変革に対する洞察力を涵養していかないと社会の付託に応えられないことになる。また、そのような知識、技術や洞察力を身につけることにより、ＣＰＳが具体的に実現する社会において、現在とは比べものにならないほど、大きな社会的役割を担うことができるのではないか。

(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。)

2013.2 投稿

めだか【　四半世紀の変遷、監査も変化したか？（システム監査の普及促進）】

四半世紀前の1987年に日本システム監査人協会は設立されている。

1987年はFISCからシステム監査指針の初版が策定された年でもある。その1年前の1986年にシステム監査技術者試験が新設され、1985年には通産省（当時）からシステム監査基準が公表されている。システム監査にかかわる様々な仕組みの創成期に当協会は発足し、システム監査にかかわる活動が営々と積み重ねられている。

この四半世紀の情報システムの動きの一端を、極めて簡単だが振り返ったのが右表だ。

1987年：パソコン用 OS/2発表（IBM）
1989年：プリペイドカードを巡る諸問題報告
1990年代：クライアントサーバシステムが主流
1994年：自動車/携帯電話機の売り切り制
1996年「第7回通信利用動向調査（郵政省）」
・企業のインターネット利用率 11.7%
・企業の電子メール利用率 25.8%
・パスワードの採用率 61.7%
1997年：インターネットバンキング本格化
1999 年：ADSL 導入、Y2K 対応

右表によるまでもなく、情報システム環境の変化の激しさは多くの人が実感している。出来事を書き上げれば驚きで鳥肌が立つほどかも知れない。というか書ききれない量になる。右表の出来事は、当時としては最先端の話題で世間を盛んに賑わしていたものだが、現在では、これらのほとんどが「古い上着よさようなら」的な技術や知識だ。

この四半世紀にシステム監査はどのような歴史を刻んできただろうか。①システム監査人、②システム監査を受ける組織・体制、③システム監査の対象システム、④システム監査への期待、⑤システム監査の技術。システム監査を語るこの5者は、時代の趨勢と環境変化にそれぞれどのように応じてきたか、見てみよう。②と③は様変わりしていて隔世の感がある。何度も脱皮を繰り返したような感じと言っていいだろう。④は「一致」から「不一致」への変化だと思う。以前は関係者がともに価値・利益を共有していたがその共感が失われている。①と⑤は我々自身の問題で我々が一番良く分かっているはずだ。

会報テーマの「システム監査の普及促進」で言えば、どのようになるだろうか。

A. システム監査の普及は進んでいるがまだ満足できない／普及は進んでいない／普及率は低下している。

B. システム監査の認知度は向上しているが満足できない／向上していない／認知度は低くなっている。

あらゆるものが変化している中、システム監査一人が変わらなくていいということはあり得ない。四半世紀前のシステム監査への要求と、現在の要求は時代の変化とともに変わってきているはずだ。一方で、当時先端を切り開いていたシステム監査であれば、今もこれからも時代をリードする素質・資質を有しているはずだ。生まれながらの才能があるはずだ。システム監査は変わるべきだろうか。システム監査が変わる必要があるならばその前に監査人個人の変化が求められているということだろうか。システム監査を普及（一般化）させるその前にシステム監査自身の一般化がスタートラインになっているのだろうか。

いろいろなことを考えながら、システム監査の普及促進に向けた取り組みをもっと積極的に行わなければ、と考える日々だ。情報化社会の健全な発展に寄与するために。

力瘤隆々のシステム監査になろう！　エクササイズしよう！

（山の彼方）

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

2013.2 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】

当協会は、システム監査の普及促進をテーマとして、情報システムにかかわっている。最近、システム監査人として考えさせられる新聞記事があったため紹介し問題提起としたい。

2013年2月1日の朝日新聞朝刊に、「SE業界『死の行進』追いつめられて」の記事が掲載されている。電機・IT大手F社の子会社SSL社のシステムエンジニア（SE）2人の記事である。N氏は、2003年秋ごろ、2002年4月入社の1年後、テレビ局向けシステムの開発を担当し、コンピュータープログラムを期限までに仕上げるため、深夜まで作業することが多かった。N氏は、「抑うつ状態」と診断されて休職した。3カ月後に復職したが回復せず、2回目の休職の後、2006年1月、うつの治療薬を大量に飲んで死亡した。27歳だったという。もうひとりのSEも、布団から起き出せなくなり、「抑うつ状態」と診断され、2005年2月、同社をやめた。彼は、「僕たちはデスマーチ（死の行進）に巻き込まれたんだと思う。」と語っている。

N氏のお母さんは、3度にわたって労災を申請したが、国は認めなかった。2009年2月、東京地裁に提訴し、2011年3月に勝訴、判決は、「心理的負荷の程度は『過重』と評価するのが相当」として、国の不認定処分を違法だとした。SSL社も、「労働時間の短縮や、休憩設備の設置などで労働条件の改善に取り組んでいる。」と、再発防止策をとると約束した。N氏のお母さんは、「過労死防止基本法」の制定を呼びかけているという。

情報システム開発で、人員不足の中で納期に間に合わせるため、連日の残業を求められることは多い。そして、誰かが休むと残った人の負担がさらに増える。情報通信産業の労働環境に詳しい、産業医のHさん（H健康管理センタ長）によると、SEたちが働く現場で、体調を崩す人が続出する状況は、「デスマーチ」と呼ばれる。米国のSEが使い始めた言葉という。Hさんの発言として、「管理職が若い情報通信産業では、労働時間や健康面の管理が徹底されない企業がある。コスト削減を意識するあまり、デスマーチに近い状態に陥る職場が多い。業界全体の課題だ。」と話している。SEの仕事の流れの中で、受注、設計、プログラミング、テスト、納入後の運用の局面に沿って、「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」に、デスマーチの主な要因があるという。

日本でも米国でも情報システムの開発において、「デスマーチ（死の行進）」が問題になっているということは、日米の風土や文化の差異は要因ではないため、情報システムの開発という業務で、SEの仕事の流れの中の要因にリスクがあるということになる。当協会は、システム監査の普及促進をテーマとして活動している。情報システム開発に従事するSEがデスマーチ（死の行進）に巻き込まれることは、当協会が看過できるリスクではない。デスマーチ（死の行進）へのリスク軽減のモノサシである規準（システム管理基準）の設定は重要な課題であると思う。

（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

■【クラウド普及におけるシステム監査人の使命】

会員番号 0685　小坂周一郎

地元梅ヶ丘商店街は梅祭りの季節になりました。小田急線の駅の向こう側が小高い丘になっており、毎年梅が満開になります。商店街も催し物を行い観光客も集まってにぎやかになります。しかしながら商店街の実態は深刻です。これは地方の商店街や中小企業にも言えることですが、全産業縮小再生産に陥っているのではないかと思われるくらい、身を削られるように売上が低下しています。

この背景としては人口ボーナスの終了による絶対的な需要不足があると思われます。経団連のジャパンクラウドコンソーシアムではこのような状況を打開するため、全産業にクラウドを導入する計画を進めています。私は業務連携クラウドワーキングに所属していますが、クラウド導入の目的は生産者と消費者の直結です。現在の需要不足の主原因は、生産と消費の分断・流通機構および広告宣伝機構の機能不全・海外販売の難しさにあると思われます。つまり流通が非能率のため生産者価格が低く抑えられ、消費者価格が高く設定されてしまうのです。しかしながら生産者を消費者に直結するためには、生産者側に納期・品質・価格の管理が求められるため、農業や工業の生産者には生産管理クラウドの導入が求められます。富士通のJSaaSでは、そのようなクラウドが各種用意されています。

業務連携クラウドの構想では、汎地球包含EDIを公共事業として設置し、これに農林水産業や中小企業の生産管理クラウドを設置し、小売業や商店街には販売管理クラウドを設置して、消費者動向がダイレクトに生産者に伝わるようにしてはどうかと提案されています。

ワーキングの主査の話では、クラウド計画についてEUから視察が来たそうです。EUの問題は我が国と同じく中小企業の需要不足にあるのではないかと思われます。アメリカについても同様であり、そのためTPPをなかば強引に進めようとしているのではないかと推測しています。主査の話では総務省にこの構想を説明したとき、クラウドはTPPに利用できるかという質問が出たそうです。

しかしクラウドには情報漏えいの脅威が常に付きまといます。ファーストサーバ社の大規模データ消失事故はクラウド運営の問題点を浮き彫りにしました。プライバシーマーク審査員の中でも議論があり、現在の個人情報保護（JISQ15001）を拡張してもクラウドの安全を保障すべきという意見があるのですが、その前提として事業者にシステム監査を導入する必要があるという見解が多いように思われます。この問題はかなり以前からもあり、事業者に情報セキュリティ教育を実施する機関が必要とされてきましたが、引き受ける機関がなく放置されてきた経緯があります。

クラウドは社会機構として企業情報システムを相互連結するため、従来の個別企業の情報セキュリティとは比較にならない危険性を秘めています。しかしながら独自のEDIを保有する重工業はともかく、中小企業の振興策は、リスクを取って抜本的な対策を講じなければどうにもならない状況に来ているのではないかと考えます。

そこで読者の皆様への提案ですが、システム監査人協会もクラウド推進に対して声を上げるときが来たのではないでしょうか。日々の糧を得ることも大事ですが、私たちの経済基盤の維持発展に貢献することも大切ではないかと考えます。

業務連携クラウドとシステム監査の役割については、以下のサイトに具体的な設計を乗せていますので、ぜひ一読をお願いします。http://itccomnet.blog.fc2.com/

また交流サイトとしてはフェイスブックを用意しております。http://facebook.com/itccomnet/

以上

■【時事論評：サイバー侍ジャパン】

会員番号 0707　神尾博

1. 賢者は歴史に学ぶ

IT セキュリティに携わる者は、日進月歩の攻撃への対処が要求される。これは自明の理である。敵はマネジメントシステム顔負けの継続的改善を驚異的なスピードで進め、次々と新手の手法を編み出していく。もっとも技術上は最先端に見えても、ソーシャル面では実空間での犯罪の手口との共通点も多く、それは現代に留まらないため、遡って振り返り見ることも肝要である。したがってその防御策にしても、社会システムが整備された、近世以降の太平の世のセキュリティシステムが特に参考になりそうだ。そこで平成・江戸の両時代を対比しながら、現在のサイバー空間でのセキュリティ上の未解決の課題への手立てについて、古人（いにしえびと）の知恵を拝借してみたい。

2. 入り鉄砲に出女

SYN フラッドや Smurf といった外部ネットワークからの攻撃は、ルータやファイヤウォール、ネットワーク型 IPS/IDS で検出し、パケットフィルタリングによる遮断が防御の中心になる。またマルウェア、スパムメールや危険サイトは、メールサーバや Web サーバへの対策ソフトの導入、すなわちアプリケーションゲートウェイが有効である。いわゆる入口対策と呼ばれるものだ。これらの機能を統合した UTM（Unified Threat Management）と称するアプライアンスもある。

数年前からは、重要情報を略奪するマルウェアの増加や、操作ミス・管理ミスによる個人情報漏洩の激増により、パケット監視を核とした DLP（Data Loss Protection）と呼ばれる出口対策の重要性も、認識されるようになった。以上がゲートウェイセキュリティの説明である。

一方、徳川の世では 1639 年から日米和親条約までの長期に渡り鎖国によって外交を停止し、貿易は DMZ（De Militarized Zone：非武装地帯）とも言うべき長崎の出島に制限された。また主要な街道に設置された、箱根のような関所で、デジタル証明書に相当する、印鑑が押された手形による検分が行われた。入口対策としては、特に江戸への武器弾薬の流入を厳重警戒した。また出口対策として、幕府にとって人質である大名の妻女の逃亡に目を光らせた。関所破りや役人の不正も全くなかったわけではないが、一通りの成果を収めていた。さらには江戸市中でも市街を網の目に区切り、木戸番による町毎の夜間の移動禁止の徹底が、秩序維持に一役買っていた。遊女の足抜け対策のための吉原遊郭の面番所もしかり。これらは現代 IT セキュリティにおいては物理的対策に該当する。

3. 鵜の目鷹の目

ゲートウェイでのセキュリティ対策は一定の効果があるが、それだけでは不十分である。クライアント PC やサーバにはワクチンソフトの導入が必須であり、パーソナルファイヤーウォールや、リンクやメールのスキャンのような統合型セキュリティ対策ソフトを利用しているケースも多いだろう。また暗号化によってファイル自体が流出しても、中味の情報を閲覧できないような運用を行うのも実用的だ。以上がエンドポイントセキュリティの説明であり、先のゲートウェイセキュリティも含めた様々な組み合わせは、多層防御・多段防御である。最近ではスマホ等の BYOD（Bring Your Own Device）も急速に進んでいるが、こちらに至っては組織内ネットワークの外側での利用が大半である。もはやゲートウェイ対策だけでは用をなさない。

江戸八百八町の治安のエンドポイント対策の中核を担ったのは、奉行所やその配下の岡っ引きである。2012 年に警察庁は、サイバーインテリジェンス（機密情報の窃取を目的とした、サイバー空間上での諜報活動）での被害防止を図る官民協議会を設置したが、その先駆けの官民連携であると言えよう。

幕府はのちに火付盗賊改方のような専門家集団も創設した。彼らの活動も多角的・多面的だ。日頃の巡回は脆弱性検査ツール、任意取調べはソースコード検査に該当しよう。様々な詐術の研究や整理も欠かせない。たとえばバッ

クドアやドライブバイダウンロードに当たる、大名屋敷や裕福な商家へ押し入る盗賊の引き込み役。いかがわしい画像を表示し「消してほしければカネを支払え」と要求するランサムウェアは、美人局（つつもたせ）と似たやり口である。悪党どもの変装もマルウェアのコードの難読化を髣髴する。

一方で一般庶民の打つ手は限られてくる。不用意に近づいてはいけないのは、怪しげなサイトや無許可の女郎屋。何かの時にエスカレーションできる、専門家や自身番とのパイプの確保。メールの添付ファイル同様、贈り物にも警戒すべし。収賄に巻き込まれる恐れがある。

4. いざ鎌倉

このように技術的・物理的対策にいては、犯人とのイタチごっこながら、平成・江戸のいずれの時代も、曲がりなりにも封じ込めには成功してきたと言えよう。ところが最近の IT 犯罪は、標的型攻撃や偽サイトへの巧みな誘導といった、ソーシャルな要素も取り入れられるようになった。また過去の愉快犯的なクラッキングから、金銭を目的とした犯罪の増加により、対象が官公庁や有名企業から一般市民にまで広がりを見せている。

したがって、前述のような技術的対策だけでは、心もとなくなってきた。それを補完するのは人的対策の強化である。組織内の IT セキュリティ人材といった、キーパースンの育成やスキル維持もさることながら、組織全員、あるいは国民全体への教育や啓蒙も怠れない時代になった。顧客情報を不法に提供した某携帯電話会社の女性社員のこの一言「こんな大事になるとは思わなかった」の弁に代表される、教育の不徹底などは論外だろう。

実は奉行所のような直接治安に携わる役人以外でも、全人口の 6～7%の相当する武士も、潜在的には兇徒への牽制や悪事の抑止に役立っていた。皮肉なことに武家社会の終焉機の幕末こそ、サムライの存在自体が植民地化を目論む欧米への抵抗のための、ゲリラ育成機能を持つ制度であると見せつける機会になったのである。母国からの出先機関を一歩出れば、日頃から剣術の修練を積んだ帯刀の手合が闊歩している。いつ夷敵征伐の大義名分の凶刃に見舞われるかも知れない。これでは「占領」「支配」「統治」には程遠い。政府機関が降伏しても、人民が屈服せず、財物の搾取もできなければ無意味だ。だからこそ列強は日本侵略を断念したのである。

同様に現代の IT セキュリティにおいても、弛まぬ技術力の研鑽と折れない心を持つ「サイバー侍」のダイナミックな増強は一考に値するのではないか。こちらのサムライには、もちろん女武芸者も大歓迎である。経済産業省所管の IPA 発行の「情報セキュリティ白書 2012」によれば、国内の従業員 100 人以上の企業での必要な IT セキュリティ人材は 25 万人強とされており、国民人口の 0.25%に相当する。「サイバー侍」のイメージはこれとはかなり違い、もっと広範囲なカバーを想定している。情報セキュリティスペシャリストはレベル4だが、もう少し低くても良い。職場や地域、家庭といったコミュニティでもごく普通に存在するところまで浸透し、初歩的な教育や軽微なインシデントのレスキューが出来ればよいだろう。

5. 武士は轡の音にも目を覚ます

防衛省は 2013 年度予算の概算要求の「サイバー攻撃等への対処」の項目で、新たに「サイバー空間防衛隊（仮称）」を編成することを盛り込んだ。現在のわが国のこの分野での体制は脆弱であり、予算も諸外国に比べ圧倒的に少ないことは否めず、防衛力強化自体は否定しない。

ただし地震等の災害と同様、サイバー攻撃の被害は堅牢な防衛施設以上に、一般市民の生活へ直結する危惧が大きい。そこで自衛隊法で定員が制限され、人材確保が困難なサイバー兵士を補完する「サイバー侍」の強化も視野に入れるべきだろう。彼らの調整力が、まるで「装甲車が避難民を轢き殺してでも進む」というような暴走の回避・緩和に役立つ可能性だってあるのだ。

そもそもサイバー戦争の要のパケットは、海外との IX（Internet Exchange）を経由してやってくる。さらには総務省所

管の主要な電気通信事業者のノードを通過する。たとえば電気通信主任技術者配置の員数やセキュリティ教育の義務付を強化し、非常時には協力してもらうといった方策は、大いに威力を発揮するだろう。米国ではサイバー戦争制限条約の国連での提言も検討されているらしいから、そうなればこういった仕組は平時でも必須になってくる。日頃からこうした動きを察知し、黒船来航のような異変に恐慌を起こすことのないよう、準備を怠らないことが不可欠であろう。

なお最後に、本稿作成に際して有益な助言を頂いた安本哲之助氏、横山雅義氏に対し、この場を借りて御礼を申し上げる次第である。

神尾博:クボタシステム開発株式会社勤務）

以上

■【 構築途上にあるシステムへの監査が足りない⑤(結)・・・自信 】

会員番号 1143　中山 孝明

連載最終回をあっという間に迎えた。これまでの４回を読み直してみて考えを伝えることの難しさを改めて思う。ぎこちない表現のオンパレードであったと痛感している。毎回の曖昧な副題は工夫のつもりで継続しているもが、今回の副題は「自信」とした。難関突破には「自信」の目で見通すことによってブレークスルーの道筋が開かれる。

"システム構築プロジェクトの失敗"

イメージだけで取り上げられている問題ではなく、公的機関や民間からの実態調査報告書のほか、その防止策や解決策をトラブルの予防やリスク・マネジメントの視点から述べている書籍など、この種の記事や文献は多い。この問題に敏感な筆者だから余計に目に付くのか。

システム監査がこの問題に果たすべき役割について多くの説明は不要だろう。システム監査は健全な情報化社会の発展に寄与することを目的としている。責務と言っていい。システム監査は明らかにこの問題の関係者の一員だ。この問題の背景の一つにはシステム監査自体が抱えている課題がある。という認識に立って標題テーマを設定している。昨年10月発行の号からこの連載を始めたが、毎号毎号を考えるたびに多くの見解・争点・主張が自分の中に湧き出てきた。連載3回目の書き出しで『彷徨したがる論旨を懸命に整えている』と吐露したのもそれだ。

このテーマはピラミッドの頂点に収斂させて結論づけをするものではないから、連載全体のまとまりもマイルドだ。しかし明快に意識して貫いている論旨がある。それは システム監査自身が自らやるべきことは何か だ。今月号も連載をまとめるというよりは、争点を提供することを主眼に筆を進める。

さて、システム構築プロジェクトの「特性」を整理してみる。

システム監査の視点で捉える場合の特性だ。システム監査着手時に対象の実体を有りのままに認識・把握するのはイロハだ。システム構築プロジェクトはそのスタートにおいて、能力・機能・効率・生産性が不確実・不安定な材料(人・ソフトウエア・ハードウエア・体制等)だらけの集合体だ。端的に言って、バグがぎっしり詰まったソフトウエアと、接続したことのないハードウエアと、玉石混交の要員スキルと、初顔合わせの体制と、未成熟なコミュニケーションなどがシステム構築プロジェクトに与えられたリソースだ。このことにさほどの異論はないだろう。

このような状態を足場にして、頼りにもしつつ目的実現に向けて活動するのがシステム構築プロジェクトだ。機敏で弾力的な作戦(計画と用兵)を継続させて、多くのステークホルダーに満足される逸品を作り出す事業だ。このように全くもってオリジナリティとクリエイティブに溢れた活動と思う。

システム監査は、このような特色・性質を持つ対象に対しては、稼働中システムとは全く異なるスタンスに立つ必要がある。システム構築プロジェクトと稼働中システムを同質として扱うことはできない。稼働中システムは業

務形態も作業基準もマネジメントも、手法やルールが明確でシンプルな日常業務だ。共通点は少なく「まったく別の生き物」と言ってもいい。仮に、システム監査だけがひとり単一の視点を引きずり、対象の本質に切り込まなければ、既成のチェック項目を消し込むだけの自己満足に終わってしまう恐れがある。

それは、システム構築プロジェクトの生成を考えると良くわかる。つまりITによって事業を刷新・改革するための新規ビジネスの創作活動であるという点だ。システム監査もイノベーションを共有しなければ役に立たない。

効果的な　システム監査形態についても述べる。

システム構築プロジェクトのシステム監査は、内部監査の充実による実施が最も効果的と考えている。内部監査は、組織体が組織の独自の判断に基づいて経営目標の効果的な達成を目的として行われるもので、従事する監査人は与えられた職制と職責の下で業務を遂行する。そこではアシュアランスとコンサルティングは有機的に併用されて目標達成に貢献する点検・評価・助言が行われる。もちろん監査人は独立性や客観性を保持しつつ作業することになる。組織内部に必要な監査要員が不足している場合は、外部の監査人を活用して内部監査を充実させることができる。

これは、外部監査におけるコンサルティング領域への踏み込み不足や保障型監査の限界などが生じる点があることと対比している。監査とコンサルティングを混同しているのではない。クリエイティブな仕事はルールが曖昧なもので、問題解決策がしばしば予想外なものになることがある。立ち入ったヒアリングと助言・アドバイスの重要度が高いと考えている。

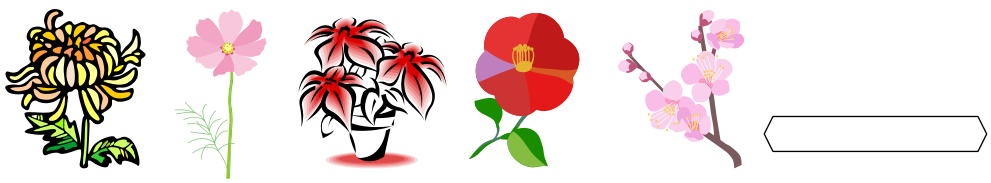
外部の監査企業等に委託してシステム監査を受ける場合であっても、内部監査業務の一部または全部の委託であれば内部監査に位置づけられ、内部監査と同様の形態の監査作業となる。例えば、2012年7月1日から適用された改正後の「金融検査マニュアル」に「システム関係に精通した要員による内部監査の実施や、システム監査人等による外部監査の活用を行っているか。」というチェック項目が新たに追加されているが、ここでいう外部監査は内部監査の業務委託を否定しているものではなく、外部監査人の視点の重要性を指していると私は理解している。達成目標はシステム構築プロジェクトの完成その1点にあるのだから、システム監査もまたその完成を目標に据えた価値観と行動基準に立つ必要がある。

システム監査は　価値ある技術を有している。入り組んだ状況を整理し複雑多岐な要素を解きほぐして核心に迫る仕事をしている。この自信を背景に世の中の困難な問題に立ち向かっていきたい。そのための技術を我々システム監査人は常に磨き続けている。

いよいよ、　連載の紙面が尽きてきた。

この問題には今後検討すべきことが残っている。一つはシステム構築プロジェクトが抱えているリスクのリストアップだ。要件定義、品質、スケジュール、体制などなど、プロジェクトのワーク項目のすべてに内在するリスクだ。もう一つはシステム構築プロジェクトで発生しているトラブル事例の洗い出しだ。事例を経験に学ぶ重要性は言うまでもない。いずれも材料はあるし無限の作業量でもないと思っているのだが、さて‥‥。

5か月にわたり貴重な会報の紙面を頂戴したことに感謝申し上げる。



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

“システム監査ワークショップ支援サービス」の試行受入れ先を募集中です。”

■【会長コラム】

当協会が検討している「システム監査ワークショップ支援サービス（仮称）」のご紹介

会長　沼野伸生

当協会の設立目的を一言で言えば、システム監査の社会への普及です。そして、この目的を達成するために協会内の各研究会、部会、委員会が、毎月いろいろ知恵を絞り、活動しています。

そのような活動の中から、今回このコラムでは、平成24年度の会員増強PT（リーダ：小野副会長）でアイデアが出され検討が進められている「システム監査ワークショップ支援サービス（仮称）」について紹介したいと思います。
（仮称）と付いていることからも分かるように、まだ完成版として提供できるレベルまで確立はしていませんが、当協会の新たな活動の形を模索したものとして、是非皆さんにも知っておいて欲しいと思い紹介するものです。

「システム監査ワークショップ支援サービス（仮称）」は、組織内のシステム監査、あるいはもう少し広く、ITガバナンス関連業務に関する検討会、勉強会、研修会など（総称して“ワークショップ”）を支援するサービスです。
当協会の経験あるCSAなどのシステム監査人が、「相談コーナー型」、「出張アドバイザー型」、「企業内研修型」など、対象組織のニーズに合う方式で、その組織の“ワークショップ”を支援するというものです。
日頃組織内でシステム監査、ITガバナンス関連のご担当として悩み、苦労されている方々に、SAAJの知識、ノウハウ、各種情報を提供し、また、相談対応も行い支援すると共に、私たちSAAJも新たな気づき、学びを得、双方にメリットのあるものにしていこうと考えています。

当協会は、このサービスを「システム監査普及の草の根運動」と捉えており、このサービスを通し、“役に立つSAAJ”の評価をまずは組織のご担当者、管理者から得て、システム監査の理解者（裾野）を広げ、システム監査の一層の普及、会員増強に繋げたいと考えています。

現在、このサービスは「出張アドバイザー型」を中心に試行準備を進めており、試行受入れ先を募集中です。
試行受入れ先は、過去に当協会の各種セミナーに参加頂いた受講者の所属組織を中心に打診していますが、その他の組織でも調整がつけば可能です。是非、検討頂ければと思います。

当協会の新たな活動の形の模索に関心を持って頂くと共に、会員の皆様のご支援・ご協力もお願い致します。

（「システム監査ワークショップ支援サービス（仮称）」は平成24年9月号の会報でも中山理事から紹介されています。）

以上

研究会、セミナー開催報告、支部報告

■　報告 1

第 178 回　月例研究会報告

会員番号 1795 藤澤　博

講演テーマ及び講師 ：

予兆型システムリスクに挑む

― これからのシステムリスク管理、監査を提案する ―

T. M. A パートナーズ(株) 代表取締役社長 遠藤 誠氏

日時 ： 2012年12月17日（月）18:30～20:00

場所 ： 機械振興会館 地下2階 ホール

講演概要:

「これからのシステムリスク管理、監査を提案する。」をテーマとして、以下のレジメに沿って講演された。

1. 今日のシステムリスク、リスクマネジメントとは
2. 金融庁が定義するシステムリスクと検査指摘事項
3. システムリスクと品質管理の関係を考える
4. 予兆型システムリスク管理態勢を整える
5. 予兆型システムリスク管理を実践する
6. 予兆型システムリスク管理を提案する
7. 予兆型システム監査の課題
8. 予兆型システム監査実践への提言

1. 今日のシステムリスク、リスクマネジメントとは

①今日のリスクとは

ISO31000のリスクの定義が、2002年版の“事象の発生確率と事象の結果の組み合わせ”から、2009年に、“目的に対して不確さが与える影響”に変更された。

リスクの定義を『目的に対して不確さが与える影響』と定めた。

参考:ISO31000:2009 ;「Risk management-Principles and Guidelines-リスクマネジメント-原則及び指針」規格は、あらゆる組織が利用できるリスクマネジメント、安全分野、内部統制等を含む汎用的なリスクマネジメントのためのガイドラインの国際規格。

リスクには、損失の発生のみに帰結するリスクと、利得につながるリスクがある。

システム関連で考えると

1) 損失発生のみに帰結するリスク

・災害、サイバーテロ、システム障害、不正・誤謬、個人・機密情報漏えい

2) 利得につながるリスク（損失と利得が一体のリスク）

・システム開発、アライアンス、シェアードサービス、システム統合、グループ統合、IT部門の子会社統合、業際またぐシステム連携等

②今日のリスクマネジメントとは

損失に帰結するリスクを最小化し、同時に、利得を最大化するためのコントロールをうまく組み合わせながら適用してゆくことである。
リスクマネジメントを経営意志徹底のための仕組みとして位置づけ、定めた経営目標の達成の妨げや不確かさをリスクと認定して最適化を図ることとしている。

2. 金融庁が定義するシステムリスクと検査指摘事項

事例として、金融庁が定義するシステムリスクについて説明があった。

① 金融庁が定義するシステムリスク

・平成14年12月での定義

システムリスクとは、システム統合における事務・システム等の統合準備が不十分なことにより、顧客サービスに混乱をきたす、場合によっては金融機関等としての存続基盤を揺るがす、さらには決済システムに重大な影響を及ぼすなど、顧客等に損失が発生するリスク、また統合対象金融機関等が損失を被るリスクをいう。

・平成24年6月での定義

システムリスクとは、コンピュータシステムのダウン又は誤作動等、システムの不備等に伴い金融機関が損失を被るリスク、さらにコンピュータが不正に使用されることにより金融機関が損失を被るリスクをいう。

上記の定義には、企業文化・経営陣による組織・人的要因・急激な変化等、真の根本的なリスクについて何も定義をしていない。

② 金融検査で指摘しているシステムリスクを分析

・システム企画の局面から経営者層が関与する必要があるという指摘がある
・経営戦略、システム投資計画の整合性などに踏み込んだ指摘がある(当局が定義している、システムリスクの定義よりもより拡大した解釈をしていることになる)。
・経営者が取るべき対応としては単に執行部門からの報告を受けているだけでは不十分としている、積極的な関与、適切な指揮を求めている。
・システム移行判定基準、稼働判定に対する経営者の指示が的確でないという指摘がある。
・グループ全体のコンティンジェンシープランの実効性がないという指摘がある。
・全社的な視野でシステムリスク管理ができていないという指摘もある。
・システムリスク管理部門による進捗管理、事後検証、現場への指導、具体的な問題把握とその検討などが足りないという指摘がある。
・指摘内容をよく見ると、企業文化・経営陣による組織・人的要因・急激な組織・システム環境の変化等によって惹起された問題について指摘をしている。

金融庁が目指しているシステムリスクの管理態勢は、単に静的、物理的な、あるいは技術的な問題としてのみ捉えているのではなく、システムのライフサイクル、リスクのマネジメントサイクルを動的なプロセスとして捉え、問題点を指摘している。
リスクの両面を具体的指摘事項で示している。
したがって、定義だけが古いのであって、検査マニュアル及び検査の実務は、多角的にリスクを捉え、本源的な

問題点を指摘していると解釈される。

3. システムリスクと品質管理の関係

次の各視点から見た品質管理（当たり前の品質、前向きの品質）について説明する。

・顧客の視点

・組織の視点

・プロセスの視点

①当たり前の品質 VS 前向きの品質

視点	当たり前の品質	前向きの品質
顧客の視点 コンシューマ（顧客）側の評価基準	・サービスの継続性、可用性 ・情報の正確性、信憑性、機密性が高い。 ・情報改ざんされない、漏洩しない情報の発生・更新履歴保持、説明能力がある。 ・低コストでサービス利用できる新サービスを早く市場に出す、享受できる。	・見やすい、わかりやすい、表現力 ・必要な情報及び情報サービスを必要な時に必要な顧客に提供することができる。 ・分かりやすい、操作性が良い、処理結果がすぐ得られる。 ・個人のライフスタイル及び情報ニーズに最も適した情報の提供、蓄積、周知、共有ができる。
組織の視点、経営者側の評価基準	·経営目標とシステム開発案件の開発目的が整合する ·開発案件の優先度が経営計画と整合する ·サービスの継続性、可用性、情報の正確性、信憑性、機密性が高い ·情報が改ざんされない ·情報の発生・更新履歴保持、説明能力がある。 ·無駄なシステムコストが発生していない。 ·必要なIT資源に費用が適正に投下されている。 ·経営計画と整合するスケジュールで事が進んでいる。 ·遅延による他への影響を最小限にとどめている	·新たな技術とビジネスモデルを採用した結果、新たな顧客層を獲得できる、新たなニーズを発掘し、新サービスを展開できる ·システム導入により、競に比して、差別化できて合する他社いる。 ·情報提供の場所、時間に依存しない、グローバルワイズな対応が可能 ·必要に応じて、情報提供相手を使い分けできる。 ·無駄な業務プロセスが減る ·部門間の情報連携が円滑になる ·意思疎通の活発化、知識、ノウハウの質的向上に寄与する
プロセスの視点、システム運営者側の評価基準	·しかるべき責任者によってプロセスで生成されたドキュメントが承認されている。 ·情報の正確性、信憑性、機密性が高い ·情報が改ざんされない ·情報の発生・更新履歴保持、説明能力	·求めているシステム寿命に応じた、適切なシステムソリューションを選択し、リスクテークを実施している ·システムライフサイクル全体から見た、システム更改時期を決定している

	がある。 ·システム障害件数が目標レベルを下回っている ·システムSLA（開発・運用）が目標値を達成している ·必要なスキルが定義され、適材適所の人が配置され、作業をしている ·ルールが標準化され、統一されている ·しかるべき責任者がコスト管理をし、適正にモニタリングしている。必要に応じて、対処策を実施している ·限られた予算枠で適正なコスト配分をしている ·しかるべき責任者が重要な作業タスクについて進捗管理をし、適正にモニタリングしている。必要に応じて、対処策を実施している	·適切なシステムソリューションを選択、導入した結果、業務のプロセスが改善されている ·冗長な開発、運用業務プロセスが減っている ·重要度に応じたシステム開発・運用リスクを採用している ·システム開発・運用プロセスを常に自己点検し、改善につなげている ·意思疎通の活発化、知識、ノウハウの質的向上に寄与する ·システム開発・運用業務で学んだ教訓、蓄積されたヒヤリ・ハット事例を共有させ、働く人の質的向上につなげている

②前向きの品質に関わる評価基準、監査プログラムを作る必要性

〈組織・経営者レベルで品質が劣化傾向にある例 〉

・系統的な取組の欠如、システム担当部門に任せっきり
・重要性に応じた第三者意見を取り入れていない
・掘り下げた分析が行われないシステム障害と本源的な問題追及をしない
・人的資源のミスマッチ放置
・違反件数の増加
・未処理是正処置の増加
・企画または開発・保守作業の重要プロセスにおける経営者の参画がほとんどない
・なかなか取上げられない従業員のシステムリスクに対する意識
・システム上の技術問題への片寄った注力
・ケアーミスの報告求めない。教訓を学ぼうとする教育をしていない
・自己点検・評価プロセスの欠如、
・経営に報告を求める情報の整理整頓ができていない

品質管理の劣化傾向はシステムリスクの高まりの兆しであり、相関関係がある。
リスクが高まる兆しに注目する必要がある。

4. 予兆型システムリスク管理態勢の構築

①リスクが高まる兆しに注目した管理体制・態勢を構築する

リスクが高まる兆しに注目した管理体制・態勢を構築するということは、最大の予防対策であり、また、リスク・フォワ

ード・ルッキング・アプローチそのものである。リスクを動態的にとらえ、流れ、変化に敏感になる。

〈一企業としてできること〉

1) リスク管理を行う専担部署を設置する。あるいは、システムリスク委員会を常設して定期的に活動する。

2)プロジェクトの管理手法、予算に関わる管理業務責任も持たせる。あるいはこれらの決定プロセスに関与する。

3)リスク分析の結果を内部統制機能の設計構築構想に盛り込むよう指示をする権限を与える。

4)時代の流れを読み、将来の経済環境、金融資本市場、技術動向等の変化に対する研究、分析を行う役割を与える。

5)他社事例、失敗・成功事例を研究し、自社でも将来起こるかもしれない事例に注目し、自己点検（CSA）をする。

6)把握されたリスク情報を迅速に組織内で共有し、経営陣やシステム関係部門と迅速に共有する。

〈業界としてできることは〉

1)民間企業、非営利団体が、自発的に、予兆的リスク管理に成功した事例、失敗した事例をデータベース化し、公開できるようにする。ナレージを共有する。

2)ITの力を利用して、企業事業体が適切に事に対処したことにより、その事業体及びその関係者が利得を経済的にあるいは非経済的に（例：社会貢献）もたらすものを業界全体で研究する、例えば非営利団体を支援する、などなど。

5. 予兆型システムリスク管理を実践する

①これから発生するリスクを以下の環境から何かを考える。

組織文化、プロセス、関係者、顧客市場

②リスクの継続的モニタリング

個々の評価項目の有効性をモニタリングするのではなく、全体的に品質が前回より向上しているか、劣化しているか傾向をつかむ。

6. 予兆型システムリスク管理の提案

･伝統的システムリスク管理と予兆型システムリスク管理の比較を下記に示す。

伝統的システムリスク管理	予兆型システムリスク管理
損失に結びつくリスクのみ対象にしている	損失及び利得に結びつくリスクを対象にする
技術のリスク、オペレーション可能なレベルのリスクが中心と経営者が認識している	技術、オペレーションの問題が経営レベルのビジネスリスクに連鎖しうるリスクと経営者が認識している
情報システム部門の課題であり、情報システム部門中心の体制であった。	情報システム部門にとどまらず、組織全体の課題になりうると考える。（専門性を持っているCIO、システムリスク専門部署、オペレーショナルリスク統括部門などの創設）
事が起これば対応するといった「リアクション型」が中心の活動であり、静態的な棚卸型の	兆しを予想して先回りする「予兆型」の活動であり、動態的に見直し策を講じる

見直し策を講じる	
新たな情報技術がもたらす危うさを中心に置いて対応策を講じる。	新たな情報技術がもたらす危うさと事業機会創出の二律背反関係を考慮して、対応策を講じる
経営戦略を達成するために、最低限必要な対策レベルを分析し、費用対効果を分析し、対応策を選択する	経営戦略を達成するために、許容できるリスクのレベルを分析し、積極的にリスクテイクをすることも検討する。
潜在的な損失額とリスクが発生する確率を分析し、対応策を講じる	確率にこだわらず、テールリスクを評価し、対応策を講じる
伝統的システムリスク管理	予兆型システムリスク管理
失敗を防ぐ、失敗を罰する文化、管理手法を構築する	失敗を学び、教訓を生かし、再挑戦をする文化、管理手法を構築・導入する
過去の出来事を分析、評価し、対応策を講じる 過去のパフォーマンスを評価する	傾向、環境変化などを察知して、今後発生しうる兆しを特定し、評価し、対応策を講じる 兆しを評価する
リスク発生の原因・事象に注力した未然防止対策を講じる	未然防止策のみならず、リスクが発生した場合の結果にも注目して、影響軽減対策を講じる
リスク管理規定・計画の見直しは定期的に行う	リスクプロファイルが変われば、見直しは随時行う。

7. 予兆型システム監査の課題

これまでに多くの企業の内部監査部門がシステム監査を実施してきているが、なぜシステム開発プロジェクトの上流工程の監査が十分に実施できていないのだろうか 疑問である。

①本社の中枢部門が、経営陣に諮りながら練り上げた構想そのものを監査するとは
「畏れ多いこと」という意識、本社の企画・業務部門や管理部門への内部監査の実施は、直ちに経営への監査を行うことと同義語になる。

②企画構想段階の監査については、監査の常道である、「明確なエビデンス」が
なかなか提示できないという根本問題がある。さまざまな問題（将来大きなリスクを惹起させそうな検討不足や仕組みの不備など）の兆しを発見しても、それが発現する絶対的な確証が得られない。

③上流工程の監査を本社の中枢部門に対して行うためには、システム部門に在籍して
大きな開発プロジェクトのプロジェクトマネージャーの経験があることや、本社の中枢部門に在籍して、会社の戦略や方針を検討してきたといった経験が必要になるが、そのようなスキルセットを持ったシステム監査人が少ない。

④画構想段階やシステムのカットオーバー段階のリスク評価手法および監査手法が
確立していない。標準的な開発過程の監査チェックポイントを採用しても、実際には実態に即したチェックポイントが生まれてきて、大規模な開発プロジェクトを多数経験をしたり、本社部門でこういう企画・構想を実際に練った経験がないと、なかなか出てはこない着眼点がある。また、将来のシステムリスクを先取りして評価するフォワード・ルッキングの意識づけが監査人自身できていない。

⑤カットオーバー段階の監査にはこの段階特有の困難さもあるため、この監査を躊躇する傾向がある。カットオーバー直前の監査を行う場合、本社部門もシステム部門も通常は大変な激務の真っ只中にある。このため、監査を受

ける余裕がないのが普通であり、「どうして、こんな時期に監査をするのか」という批判を受けることが多い。

8. 予兆型システム監査実践への提言

予兆型システム監査の実践を以下に示す。

①IT戦略目標の設定内容そのものが正しいかという評価は、定めた経営目標の達成を阻害しているか、または貢献しているか否かが焦点となる。兆しに関わる明確なエビデンスがないため、是正に向けての提言をすることになるが、早い段階で判断ミス？を指摘する効果が最も高いため、実施の意義は大いにある。システム担当役員と事前の評価基準とのすり合わせをし、十分な意見交換をし、理解を求める。（システム担当役員に意見を述べ、是正を求める権限を監査部門に与えることが前提になる。）

②経営戦略目標、システム戦略目標のPDCAサイクル、プロセスを監査する。戦略目標策定・展開のプロセス（十分な分析と検討をした上で計画され、決定され、周知されているか、整合性を持続させているか、プロジェクトの計画は経営戦略目標と整合しているか、等の観点）から監査を実施する。

③「上流工程監査を受ける文化」を本社部門およびシステム部門に意識づけさせる。あらかじめ、重要な大規模プロジェクトは、カットオーバーをする前にシステムリスクの専門部署および内部監査部門が確認するプロセスがあることをルール化したらどうか、また、事前に認知させる段取り作業をしたらどうか？例えば、役員および本社部門およびシステム部門の管理責任者の意識を高めてもらうため、システム企画・開発検討のタイミングで双方が参加できる勉強会を適宜開催し、当プロジェクト監査の着眼点の見方などを議論する。

④システムの上流工程監査ができる人材を登用する。経営企画、システム企画、大規模開発案件経験者を一定期間ジョブローテンションし、内部監査業務に従事してもらう方法、外部から専門家を雇用する、等の方法が考えられる。また、複眼的な監査要点を洗い出すためには、様々な経験を有した人のチーム編成をする、その場合、過去に関わった業務、システム開発業務の監査をする立場になる監査人が発生した時には、まったく関わっていない人を加えた混成チームで監査をすることにより、被監査部署への遠慮や独立性などの問題に対処できるのではないか

⑤システム企画立案時点でこれから起こるかもしれないシステムリスクの兆しを学ぶ。監査人自らが、システム稼働前にどんなリスクが生じうるか勉強し、早い段階で被監査部門との意見交換をする。

⑥そして何より、経営者がリーダーシップを発揮する。経営企画、システム企画、情報処理部門等の担当役員自らが自分達が管掌する業務について監査を受けることを許容することとその必要性を理解し、部員に教育する。

予兆型システム監査実践への提言（まとめ）

①前向き品質追求を前提としたシステム監査を実施しよう。前向き品質管理に関わるシステム監査基準を開発しよう。

②システム企画・開発プロセスにおけるシステム監査の主題には、システム化構想、開発検討の段階から監査範囲に含めて計画・実施しよう。

③品質劣化の兆し、技術環境変化の兆しからリスクを識別しよう。

④定めた経営目標の達成の妨げにつながっている、無作為の行為についてもコメントしよう。

⑤リスクをとってシステム開発を決定した場合に、リスクをとることについての妥当性を評価しよう。

⑥リスクにうまく対処できた事例を監査報告に盛り込み，好事例として称賛しよう。

⑦経営者をうまく誘導しよう。

＜感想＞

今回の講演テーマ「予兆型システムリスクに挑む ― これからのシステムリスク管理、監査を提案する ― 」は、これからのシステム監査がどうあるべきかを金融庁が定義するシステムリスクを事例として講演を戴いた。これからのシステム監査は、前向き品質追求を前提としたシステム監査を、システム企画・開発プロセスでは、システム化構想を開発検討の段階から監査範囲に含めて計画・実施する。また、経営者をうまく誘導する等、今後のシステム監査のあり方について、非常に興味ある内容で講演を戴きました。

遠藤様から、金融庁のシステム監査の実績経験を活かし、現状を解り易く説明して戴いたことに感謝し、感想とさせて戴きます。

＜本講演者の問合せ先＞

T. M. A パートナーズ株式会社
代表取締役 社長 遠藤 誠 電話: 090-4813-0691
e-mail:makotoen@kamakuranet.ne.jp
URL: http://tmapartners.web.fc2.com/index.html

以上

■　報告２

第 179 回　月例研究会報告

会員番号 0555 松枝憲司

日時 2013 年 1月22 日（火） 18:30～20:30

会場　　機械振興会館地下2Fホール

テーマ「IT Audit ISO化推進状況」

IT Audit －Audit guidelines that support the evaluation of the Governance of IT－

講師　日本システム監査人協会　システム監査基準研究会

力利則氏（NECフィールディング株式会社、SAAJ副会長）

松枝憲司（株式会社ビジネスソリューション、SAAJ副会長　研究会主査）

松尾正行氏（株式会社商船三井、SAAJ理事）

【システム監査基準研究会の紹介】

講演に先立ち、主査の松枝より当研究会について紹介した。

- 活動内容：システム監査/管理基準の活用についての研究及び情報を発信。
  現在は、IT Audit の ISO 化を目指した ISO30120 の原案作成を支援しています。
- 活動形態：
  （定例会開催頻度）：原則として1回/月ですが必要に応じ臨時開催
  （開催場所）：茅場町または麻布十番 （活動時間帯）：原則午後6時半から
- 活動成果例：
  - 情報システム監査実践マニュアル(赤本)出版
  - J-SOX 対応IT統制監査実践マニュアル(黄本)出版
  - システム管理基準 for オフショア Ver1 公開　等

ご興味のある方は、松枝までお気軽にご一報ください。（メール：kmatsueda@nifty.com）

【講演概要】

力氏より、ISOプロジェクトの背景とこれまでの経緯等について、以下の説明があった。

Ⅰ．背景とこれまでの経緯

1．会議の経過

- 2011年5月　パリ会議（力出席）
  基準研メンバが中心になり原案を作成したNP（New work item Proposal）を提案し、国際投票の結果プロジェクトとして成立した。
- 2011年8月：「Pre-WD」を作成。 文書番号が「ISO/IEC TR 30120」に決定。
  → 今回はIS（国際規格）ではなく、TR（Technical Report 技術報告書）を目指す。
  Pre-WD版（ANNEX等はサンプル）を各国に提示しコメントを収集
- 2011年9月　ロンドン会議（力出席）
- 2012年1月　ロンドン会議の結果を受けて基準研メンバを中心に「ISO/IEC TR 30120 WD1」版を作成
- 2012年5月　チェジュ島会議
- 2012年8月　チェジュ会議の結果を受けて「ISO/IEC TR 30120 WD2」版の作成

- 2012年9月　ダブリン会議（松尾出席）
- 2012年11月　ダブリン会議の結果を受けて、日本の改訂案を作成
- 2012年11月　ISOのWGの統合（WG40とWG6がWG8に統合）があり、議長が交替。
  → 今後の進め方及びスケジュールに関して現時点で未定。

2. タイトルとスコープの議論

続いて、ISO化作業においてキーとなる「タイトルとスコープ」の議論の変遷についての説明があった。

○ これまでの検討の経緯「タイトルとスコープ」

年月	タイトル	スコープ
～2011年7月	IT Audit	This guideline provides high level guidance on adopting appropriate frameworks for the management and governance of IT and guidance on auditing against adopted framework.
2011年8月ロンドン会議への提案	Guidelines for IT Management Systems Audit	This guideline provides guidance on auditing the IT management systems based on the requirements of ISO/IEC 38500. It includes guidance on management of audit programmes, conduct of audit, as well as the competence and evaluation of auditors.
2011.9～2012.5 ロンドン会議	IT Audit - Guidelines for Governance of IT -	This technical report provides guidance on auditing to support the evaluation of the governance of IT based on the principles of ISO/IEC 38500.
2012.6～チェジュ会議	IT Audit – Audit guidelines that support the evaluation of the Governance of IT –	This technical report provides guidance on the auditing of IT that supports the evaluation of the governance of IT based on the principles of ISO/IEC 38500: 2008.

当初のタイトル「IT　Audit」に始まって、直近の内容に至るまでの経緯が説明された。

最新の内容は以下のとおりである。

○「ISO/IEC TR 30120 WD2」のタイトルとスコープ（和訳）

・タイトル　:IT監査 – ITガバナンスの評価を支援するための監査ガイドライン–

・スコープ：本報告書は、ISO/IEC38500：2008の原則に基づくITガバナンスの評価を支援するIT監査のガイドラインを提供する。

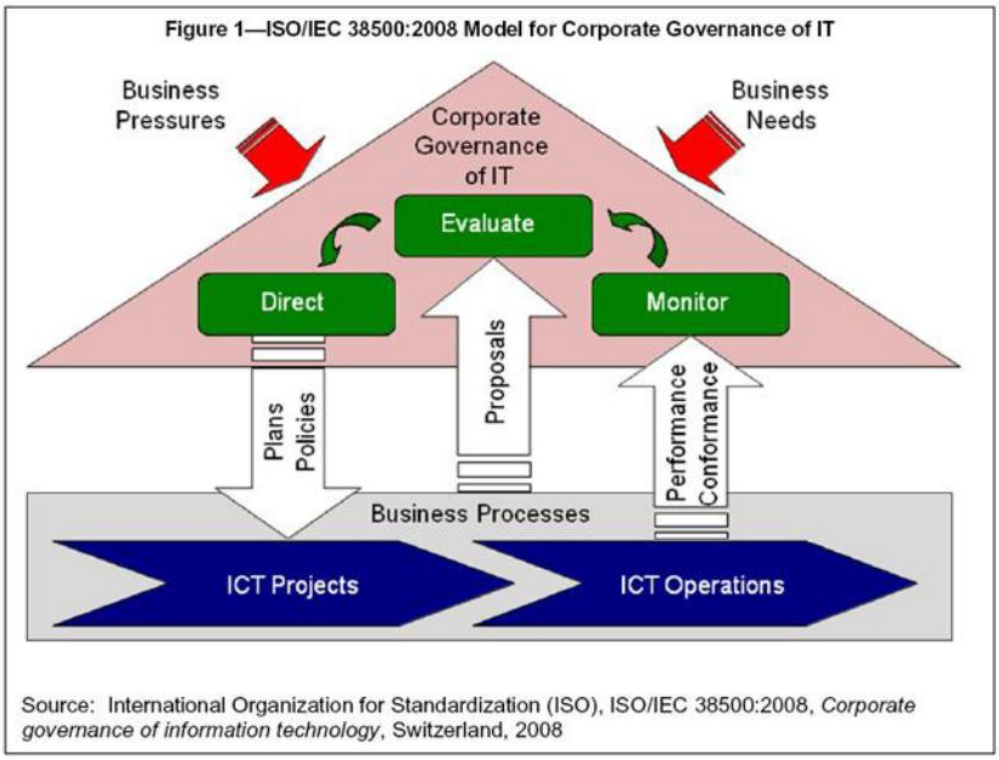
※ 実際の講演では力氏が継続して、各会議で検討したポイントについての説明があったが、本報告書を読まれる方により理解しやすいよう「ISO/IEC38500：2008」の説明を先に挿入しました。

Ⅱ．ISO/IEC38500：2008の概要

上記スコープからもわかるように、ISO/IEC 30120は「ISO/IEC38500：2008」に基づいているため、ISO/IEC38500：2008の理解が前提となる。松枝より「ISO/IEC38500：2008」の概略について説明があった。

1．ISO/IEC38500：2008におけるITガバナンスモデルについて

ISO/IEC38500におけるITガバナンスのモデル



ガバナンスボディ(GB：経営者層)は、ビジネス環境からの要求や市場に合わせて、企業としての方針を決定する。企業の執行部門からの活動をモニタして、目標との乖離を調べ、その結果と執行部門からの提案を統合的に評価して、実施部門に対して指示を行う、というモデルである。

(1)オーストラリアの国内基準であるAS8500がベースとなり国際標準となった。

(2)企業の経営者が実施するべき行動として、①指示（Direct）、②評価（Evaluate）、③モニタ（Monitor）がある。

(3)重要なことは、経営者は、IT の投資や利用について決定し、その結果をモニタして、改善を行うことが求められている。

(4)組織のガバナンスを実施する組織のオーナ、ボード メンバ、パートナー、上級幹部は以下を実行すること

①現在と将来のITの利用について評価する

②ITの利用が組織のビジネス目標に合致するように 計画とポリシを策定し、実施する

③ポリシへの準拠と計画に対する達成度をモニタする としている。

2. ISO/IEC38500による IT ガバナンスを実現するための6つの原則

ISO/IEC38500では、以下の6つの原則を定めている。

① Responsibility（責任） ITに対する責任を明確にする原則

② Strategy（戦略） ITは組織の目的を最大限に支援する原則

③ Acquisition （調達・取得） ITの有効性を高める適用原則

④ Performance （パフォーマンス） ITの可用性を高める性能原則

⑤ Conformance（適合・準拠） ITが法令や企業内部の取決めに準拠する準拠原則

⑥ Human behaviour（人的行動） ITは人的要素を考慮する人的行動原則

Ⅲ. 会議における重点ポイント

1. ロンドン会議とチェジュ会議のポイント

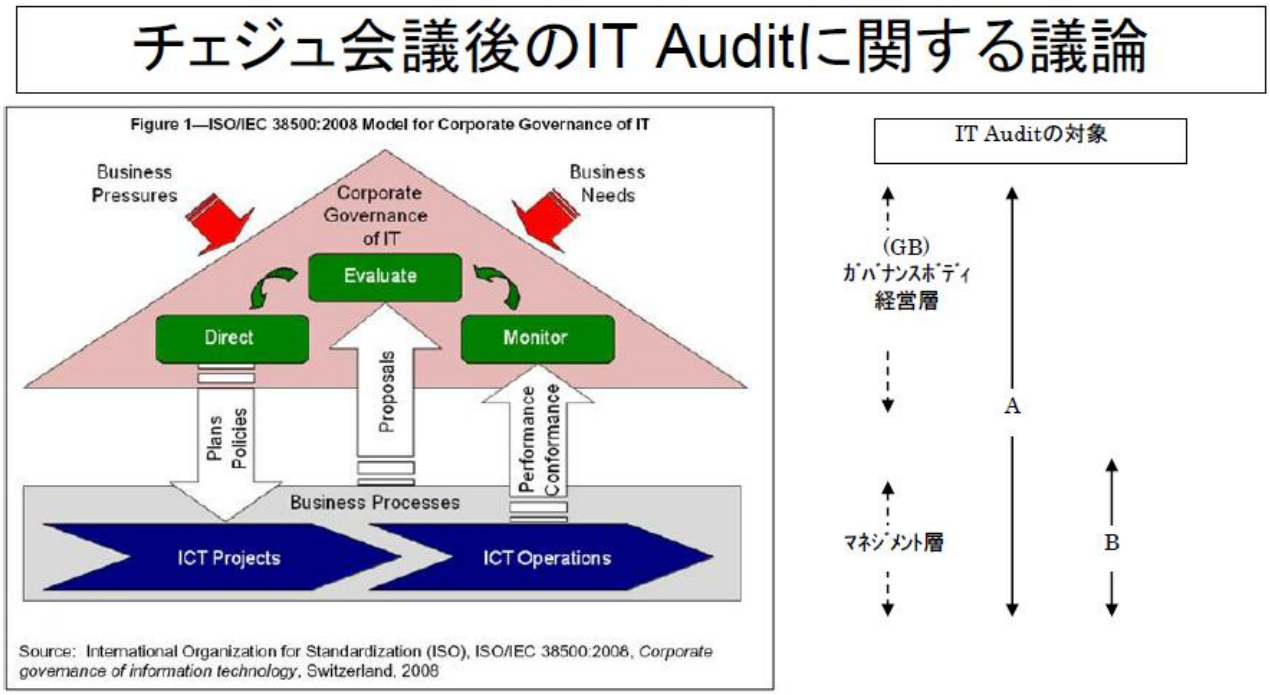
スコープについては、このガイドラインとITガバナンスの基準であるISO/IEC38500との関係が、大きな議論となった。

・ITガバナンスとの関係で、6つの原則に基づくのか、ITガバナンスに基づくのかの観点で議論となり、当面は、6つの原則に基づくこととした。

・次に、ITのマネジメントを評価するのか、評価を支援するのかが大きな論点となった。

監査人が、ITのマネジメントを評価するのではなく、ITのマネジメントを評価するGBの支援として、監査人による監査意見を述べるということでコンセンサスを得た。

2.チェジュ会議のポイント



・IT Auditが対象とする範囲は、GBとマネジメントの両方の活動を含むものとの理解であった（図のA）。 しかし会議後に、IT Auditが対象とする範囲からGBは外すべきとの意見がでた。 あくまでもGBの指示を受けて実施しているビジネスプロセスが対象であり、また、このプロセスはマネジメント層が対象なので、PDCAサイクルに沿ったAuditCriteriaとすべきではないかというものである（図のB）。

3.ダブリン会議のポイントと今後の予定等

(1)「まずはScope and Nature of IT Auditの範囲に関する合意が必要」があり、ISO30120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て、

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 十分との主張があった。

一方で「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た。

(2)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。

(3)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、次の資料を参考として、 日本が原案を作ることになった。

Ⅳ.「ISO/IEC TR 30120 WD2」内容の紹介

1. ISO/IEC TR 30120 WD2の構成

次に「ISO/IEC TR 30120 WD2」の全体の構成について松枝より説明があった。

ISOにおける監査の規格として「ISO/IEC19011:2011」があり、全体の構成としてはこれを踏襲している。

また「19011」の内容をそのまま適用できる項目が多く存在しており、その箇所については「ISO 19011:2011, Clause X apply」と記述している。

ISO/IEC30120の目次は以下のとおりである。

INTRODUCTION

1. SCOPE

2. NORMATIVE REFERENCES

3. TERMS AND DEFINITIONS

4. Principles of Audit Guidelines for Governance of IT

4.1 GENERAL →ISO 19011:2011, Clause 4.1, apply

5. Managing an Audit Programme

5.1 GENERAL → ISO 19011:2011, Clause 5.1, apply.

5.2 ESTABLISHING THE AUDIT PROGRAMME OBJECTIVES

5.3 ESTABLISHING THE AUDIT PROGRAMME

5.4 IMPLEMENTING THE AUDIT PROGRAMME

5.5 MONITORING THE AUDIT PROGRAMME

5.6 REVIEWING AND IMPROVING THE AUDIT PROGRAMME

原則として ISO19011:2011 を適用し、異なる箇所のみ記載

以下次頁

6. Performing an IT Audit
- 6.1 GENERAL
- 6.2 INITIATING THE AUDIT
- 6.3 PREPARING AUDIT ACTIVITIES
- 6.4 CONDUCTING THE AUDIT ACTIVITIES
- 6.5 PREPARING AND DISTRIBUTING THE AUDIT REPORT
- 6.6 COMPLETING THE AUDIT
- 6.7 CONDUCTING AUDIT FOLLOW-UP

原則として ISO19011:2011 を適用

7. Competence and Evaluation of Auditors
- 7.1 GENERAL
- 7.2 DETERMINING AUDITOR COMPETENCE TO FULFIL THE NEEDS OF THE AUDIT PROGRAMME
- 7.3 ESTABLISHING THE AUDITOR EVALUATION CRITERIA
- 7.4 SELECTING THE APPROPRIATE AUDITOR EVALUATION METHOD
- 7.5 CONDUCTING AUDITOR EVALUATION
- 7.6 MAINTAINING AND IMPROVING AUDITOR COMPETENCE

原則として ISO19011:2011 を適用

ANNEX A

Practice Guidance for IT Auditing
- A1. Responsibility（責任）
- A2. Strategy（戦略）
- A3. Acquisition（調達・取得）
- A4. Performance（パフォーマンス）
- A5. Conformance（準拠性・適合性）
- A6. Human Factors（人的要素）

BIBLIOGRAPHY

Ⅴ. Managing an Audit Programmeの紹介

続いて、ダブリン会議後に作成した日本の改定案について、松尾氏より説明した。

まず改定案の参考としたISO-38501の概要説明があった。

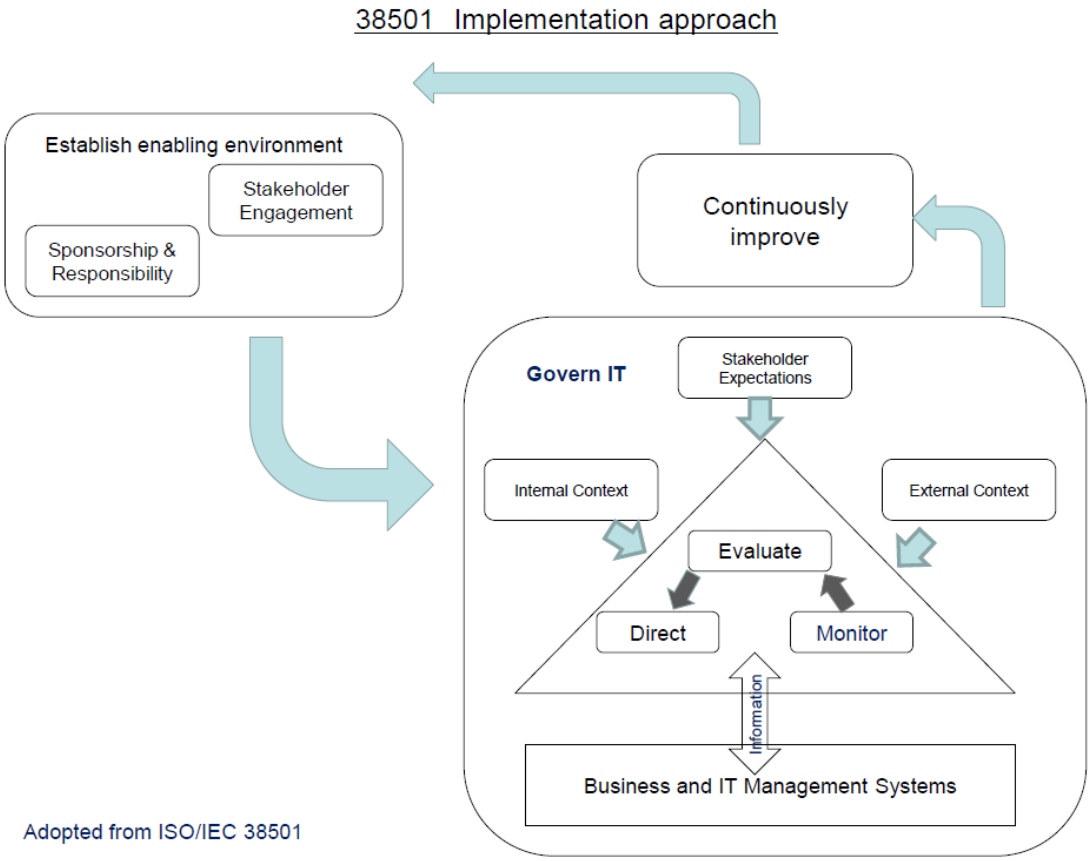
ISO-38501：PDTR 38501-WD3v2: For WG6 comment 2012-07-06「ITガバナンス導入のガイドライン」

※これ以降の日本語訳については以下の用語を参照している：

①ISO/IEC専門業務用指針、第一部 統合版ISO補足指針-ISO専用手順（第9版2012年版）：MSSの開発プロセスおよび校正に関する手引き:

Appendix-4（上位構造、共通の中核となる共通テキスト並びに共通用語および中核となる定義に関する手引き

②情報セキュリティガバナンス導入ガイダンス：経済産業省 平成21年6月



1．38501 実施のアプローチの紹介

上記モデルに基づき以下の説明があった。

①IT統治(Govern IT)の概観

・38500フレームワークの適用にはプロセス・管理を基にしたものではなく、アウトカム基準のアプローチの適用が重要である

・このアプローチはGB*が「How to」ではなく、「What need to be achieved」を決めることが容易となり、組織がITの利用について適切に方向づけできる。 *GB: Governing Body(経営陣)

②3つの主要な行動

ア） 評価 (Evaluate)

・関連付けの整理

-内部環境: ビジネス戦略、リスク許容度、戦略的変革プログラム、組織の文化、成熟度、スキルのレベル

-外部環境: 法制、技術の進展、一般のトレンド、入手可能なスキル、競争力、ステークホルダの要求

・基本線の策定

-IT統治の考え方: キービジネスファクターがITの導入と利用にインパクトを与えるか？

≫戦略、リスク、コンプライアンス、企業文化、決定権と権限委譲

-ISO38500 成熟度の評価: 6つのプリンシプルに対してアウトカムズの達成度を評価する

≫明確かつ適切な責任(Responsibility)の付与

≫組織の戦略(Strategy)への集中の重要性

≫バランスの取れた調達・取得(Acquisition)の必要性

≫パフォーマンス(Performance)と監視(Monitoring)、管理(Control)の関連付けの設定

≫適切なレベルの内部、外部準拠性・適合性(Conformance)の設定

≫人的要素(Human Behaviour)の影響、扱いの理解の重要性

・ギャップ分析：プリンシプル毎に現状とあるべき成熟レベルの分析

イ) 方向づけ(Direct)：

・ギャップ分析の結果に基づき、GBは識別された変更行動が適切に実施されることを支援する

・ITガバナンスの事務局：変更行動の進捗管理と必要な管理業務の実施

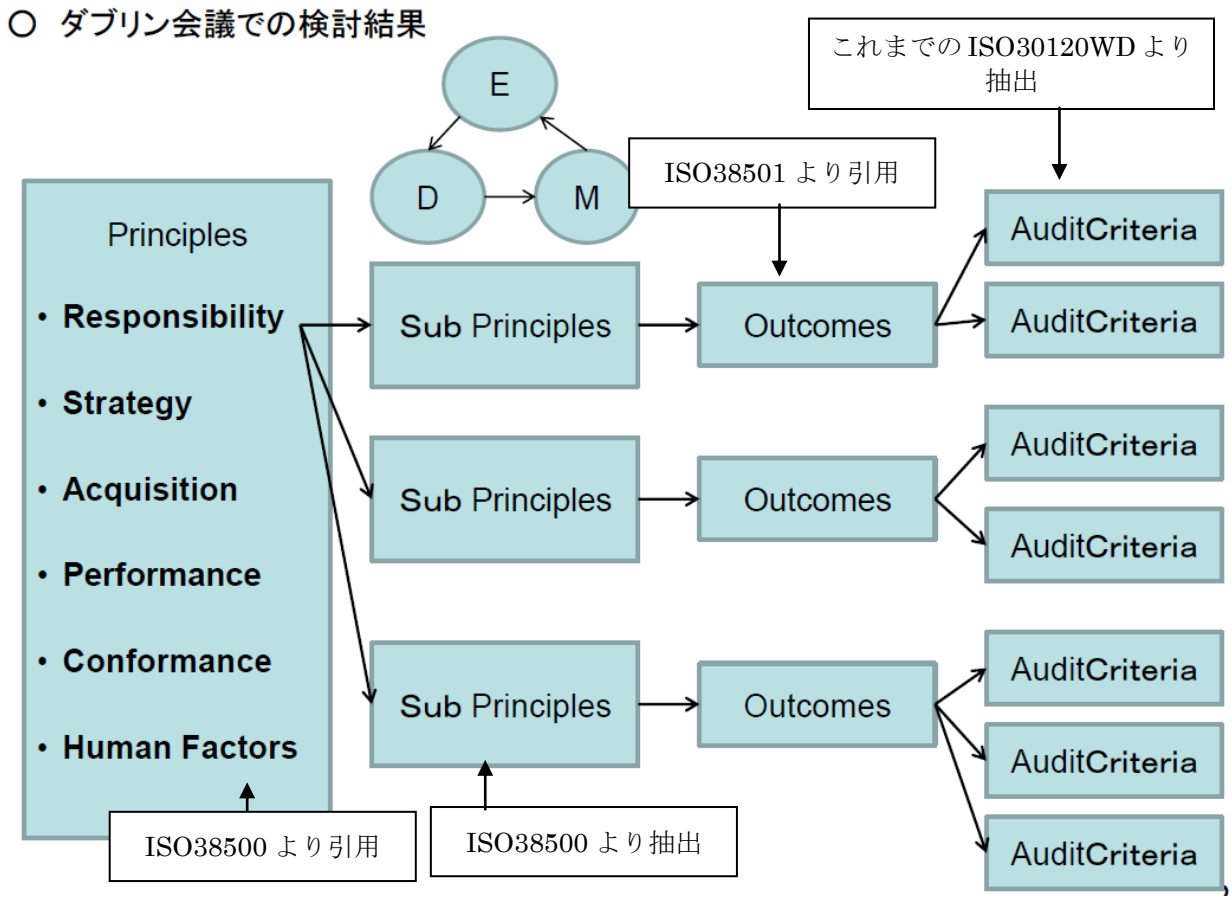
ウ) モニタリング (Monitor)

・ITの重要な部分においてパフォーマンスと準拠性・適合性を監視し、組織のIT関連のアウトカムズの達成度を監視すること

・監視の結果は、次のサイクルの基本線アセスメントにおける成熟度の現状評価となる

2. ダブリン会議後の改定案のモデル紹介

上記38501のOUTCOMES等を参照して、以下のような構成を、改定案のモデルとした。



3.日本の改定案の紹介

プリンシプル-1 責任	
組織内の個人及びグループはITの供給及び要求に関してそれぞれの責任を理解し、受け入れる。 行動に責任を持つ者はそれらの行動を遂行するための権限も有する。	
サブプリンシプル	
1.組織の現在及び将来のIT利用に関する責任の付与オプションを評価すること 2.ITに関する決定責任を与えられる者はその実行責任と説明責任に対応するための情報を受け取ることが保証されること 3.適切なITガバナンスのメカニズムが設定され、責任を付与された者の受け入れ、理解及びパフォーマンスが監視されること	
アウトカムズ	
1.組織はITによって可能となるビジネスの変革を成功裏に導入する 2.ITによって組織の価値が生成される 3.組織は最適なコストで高品質なITを受容できる	
Audit Criteria (監査の基準)	Audit Practice Guide (監査実践ガイド)
1.1 現状及び将来のビジネス目標が決定され、効果的、有効かつ受容可能なITの使用及び導入が確保され、責任決定プロセスが存在すること	1. ITガバナンスに関する方針が存在することを確認する
1.2 ITに関する責任項目が設定され、ビジネスの価値とプロセスを理解するIT専門家の支援により責任者が指名されること	1. ITの責任に関するIT専門家の報告書を確認する 2. ビジネス及びIT環境の変化に対応した、個人の役割と責任を検証する 3.方針からの逸脱度の計測を含む、IT利用の計画に関する管理およびITステアリング委員会に是正措置が提案されることを検証する 4. ITの利用または利用計画に関する会議報告を検証し、IT利用の責任が適正に考慮されていることを確認する
1.3 個人の責任と権限が明確に定義され分離される; 責任項目はITの供給側及び要求側に関係する	1. 権限の枠組みと役割を検証し、それらの責任項目が適正であることを確認する 2. 権限、責任の枠組みに関する情報が明確で公知であることを検証する 3. 組織図から、IS戦略を決定する専門委員会が設立され、職務が指定され、最適化計画が導入されている事を確認する

1.4 ITに関する諸決定を行う責任を負うものは、その実行責任及び説明責任に合致するための、情報を受けられることが保証される	4. ビジネス及びIT環境の変革に応じて、個々人の役割と責任項目を検証する 5. 方針からの逸脱度の計測を含む、IT利用の計画に関する統制を検証する。そのうえでITステアリング委員会に矯正措置が提案されることを確認する 6. IT利用またはIT利用計画に関する打ち合わせ報告を評価し、説明責任及び実行責任が適正に考慮されていることを確認する
1.5 ITガバナンスにおける責任者のパフォーマンスが報告され、GBによって監視される	1. IT利用またはITのパフォーマンスに関する報告がITステアリング委員会になされていること

プリンシプル-2 戦略	
組織のビジネス戦略は現状及び将来のIT能力を考慮する; ITの戦略計画は組織のビジネス戦略の現状及び継続的なニーズを満たすこと。	
サブプリンシプル	
1. ITおよびビジネスプロセスの進展はITが現状及び将来のビジネス要求事項への支援を行うことを確保する。 それは関連の国際・国内標準に記述された、適切なリスクの査定と評価に準じること。 2. 計画及び方針はITの諸活動が、変化する諸環境に対する組織目標と整合し、よりよい実践および重要なステークホルダーの他の要求を満足させることを考慮する。 3. 計画と方針の準備と利用は組織がITの諸開発から便益を受けることを確保する。	
アウトカムズ	
1. 組織のオペレーションが、ITシステムにより効果的に支援され戦略的変革が容易かつ迅速に可能となる 2. 深い組織上の内情がマネジメント情報システムにより提供される 3. ITイノベーションを通じて、組織の競争優位が駆動される	
Audit Criteria (監査の基準)	Audit Practice Guide (監査実践ガイド)
2.1　ITの諸活動は現状及び将来のビジネス要求事項および変化する環境に対する組織目標と整合すること。 また、よりよい実践例を考慮しかつステークホルダーの他の要求を満足するものであること	次の点を評価、確認する 1. 戦略的IT計画の標準運用手順が文書化され、伝達され、維持されている 2. ビジネス改善要求事項の識別方法論が存在する 3. ビジネス改善要求事項を支援するITの潜在力調査を支援する技術とプロセスが存在する 4. 代替案の選択における評価基準が設定されている 5. 戦略的IT計画プロセスにおいて、経営層、管理者層およびステークホルダーからの意見やフィードバックを組み入れる方法論が配慮されている 6. ビジネス戦略の実施の中で、ITパフォーマンスの計測プロセスが存在する

2.2　IT及びビジネスプロセスの進展に置いて、関連する国際・国内標準に記載された、適正なリスク査定と評価が実施されること	1. リスク査定方針を吟味する 2. リスク査定方針がリスクのレベルに応じた、リスク分析の頻度、受容可能なリスクの定義責任及びリスク軽減のための統制の実施期限を明示していることを確認する 3. ITの利用に関して、リスク査定プロセスが適用されること 4. リスク査定報告を吟味し、リスク査定に基づいてITリスクの為の計画が実施されていることを確認する 5. BCP計画が設定され承認され実施されていること 6. BCPに関する従業員の教育及び訓練が設定され実施されていること 7. BCPテストの最低限の周期が規定され、テスト結果は文書化され、結果に基づいた計画の更新が行われること
2.3　組織が新たな機会または挑戦、新規ビジネスまたはプロセス改善を確保するための、革新的なIT利用に関する提案が奨励される	1. ITステアリング委員会が最適化計画を承認する 2. 情報システムの全体最適化計画の目標及びビジネス戦略との整合を確認する 3. IT利用、IT投資配分の原則がビジネス要求事項と合すること 4. 組織の情報システムモデルが適用されていること 5. 新システムの導入による組織の構造及びビジネスプロセスの変更に関して方針が適用されること 6. 情報のセキュリティに関する方針が設定され実施されていること
2.4　ITが意図された便益を達成していることを確認するため、ITの利用が監視される	1. ITの利用に関するパフォーマンスがGBにより監視され、IT利用のパフォーマンスがビジネス要求事項を達成していない場合は適切な行動がとられていることを確認する

プリンシプル-3 調達・取得	
IT調達・取得は、適切かつ継続的分析に基づいた、明確かつ透明な決定に基づき、正当な理由づけで実施される。 便益、機会、費用及びリスクの間には、短期及び長期双方の適正なバランスが存在する。	
サブプリンシプル	
1. 承認された提案を実現するためのITオプション、提案された投資の金額に対する価値とリスクのバランスを基に評価される。 2. IT資産は、必要な能力が提供される前提において、適切な文書の準備を含む適正な手法で調達される。 3. 組織及びサプライヤーは、IT調達における組織の意図について共通の理解を維持する	
アウトカムズ	
1. ITの投資はビジネスへの貢献の度合いに基づいて優先度付けされる 2. ビジネス要求事項は選択されたITソリューションによって全面的に支援される 3. 導入プログラムは計画に基づいて実施され、ビジネス上の便益を達成する	
Audit Criteria (監査の基準)	Audit Practice Guide (監査実践ガイド)
3.1 IT投資は短期及び長期におけるビジネスへの貢献に必要な機能を実現することと看做される	1. 短期及び長期のビジネス戦略に合致したIT投資計画が設定されていることを確認する 2. 提案された投資金額に対する最適なリスクと価値のバランスを取って、複数のIT投資計画案が評価されていることを確認する
3.2 IT資産の管理方針および関連する手順は、必要な機能が準備できる前提で、IT資産が、文書化の準備を含む適切な方式で調達されるために、設定される	1. IT資産の調達に関し、方針、関連の手順及び関係する統制を吟味する 2. 情報資産のリスク査定及び統制手続きを吟味し、必要な時は適正な方策がとられることを確認する 3. IT資産の利用について、効果的、効率的な方針と手続きがあるかを吟味する
3.3 供給の手配(内部及び外部の供給手配)が組織のビジネスニーズを支援する	1. IT投資の方針が設定されていることを確認する 2. IT投資に対する収益見積りの標準的手法が設定されていることを確認する 3. 全てのIT資産及び個別プロジェクトの財務的パフォーマンス、および、問題発生時には必要な対策が取られていることを査定する 4. IT調達のパフォーマンスを確認するために、IT投資に関する報告、委員会の議事録を吟味する
3.4 IT調達実施に関し、サービスプロバイダの選定に関わる方針及び手続きが設定されている	1. IT調達において、サービスプロバイダの選定のための方針及び手続きが設定されていることを確認する 2. サービスプロバイダの選定基準は、関連するビジネス要求事項と整合していることを確認する 3. サービスプロバイダ候補に対する、現在の要求仕

	様は組織のビジネスニーズに整合していること
3.5 組織のビジネス要件を確保するため、供給体制（内部及び外部供給体制）を含む、策定プロセスの継続的な分析を拡張する	1. IT投資報告および委員会議事録を査閲し、ITのパフォーマンスを確認する 2. IT投資の収益見積もりの標準的な手法を設定する 3. 全ての情報システム及び個別プロジェクトの財務的パフォーマンスおよび問題があれば必要な行動を取っていることを査閲する。 4. IT投資が適切に実施されていることを査閲する 5. サービスレベルの設定に関する方針が定義されていることを確認する

プリンシプル-4 パフォーマンス	
ITは、サービスの提供、現状及び将来のビジネス要求事項に合致するサービスレベル及びサービス品質の提供を支援する、組織の目的に適合する。	
サブプリンシプル	
1. ITは必要とされる機能と能力において、ビジネスプロセスを支援する 2. ビジネスの正常な運用継続、情報及びIT資産の保護の完全性、関連する知的財産及び組織の記憶及びITの利用にともなるリスクの扱いに関わるリスクが十分に配慮されること 3. ITが合意された優先度と予算上の制約に従って、組織のニーズに対応できるよう、十分な資源が配分される	
アウトカムズ	
1. 全てのステークホルダーは必要な時はITと交流し、処理できる 2. ITシステム中の情報は完全、正確かつ安全である 3. 情報システムの支援が必要な時は、ステークホルダーは効果的に支援が受けられる	
Audit Criteria (監査の基準)	Audit Practice Guide (監査実践ガイド)
4.1 ITの機能と能力は、効率的、有効かつ受け入れ可能なITの利用と供給を確保しつつ、ビジネスの目的と要求事項に適合すること	1. ITの方針、最適化計画及び情報システムの開発計画に関するガバナンスを入手する 2. 情報システムの開発計画に関するIT委員会の議事録を吟味し、情報システム開発計画が最適化計画及びIT利用に関わるリスクに適合していることを確認する 3. IT委員会が次の諸点を検討するため、適時に開催されている事を確認する ・ ITが要求される機能と能力によりビジネスプロセスを支援する能力があること ・ ITに関連する活動によりビジネスオペレーションが中断されるリスク

	・組織の現状及び継続的なビジネス目標を支援するITプロセスへの支援がある ・将来のIT機能を提供するためのプロセスが適正に導入されている 4. ITの方法付けはIT管理者によってサポートされている 5. IT利用のパフォーマンスは監視され、必要に応じて改善されていることを確認する 6. ソフトウェア、ハードウェアおよびネットワークに関する運用手順書があることを確認する
4.2　データの正確性及び効率的なITの利用のような方針が適切に守られる	1. データ管理規則が存在すること 2. データ管理報告により、正確で最新のデータが喪失や誤使用から保全され、正確性、秘匿性を確保するためのデータオペレーションが適切であることを確認する
4.3　過大な需要及び/または災害時にITシステムは適正に反応し、可用性が確保されること	1. 災害復旧計画及びコンティンジェンシープランが開発され、GBにより承認され、それらは適切なリスク分析により作成・更新されていることを確認する 2. それぞれのビジネスプロセスに対する受容可能な回復時間に関する査定が設定され、優先付けされていることを確認する 3. 教育及び訓練計画が存在し、適切に実施されていること 4. 災害復旧計画は、事業継続に必要な、最も重要なシステム及びシナリオに合致していること 5. システム、データ及び必要な資源のバックアップ方式及び手続きが、ビジネスの回復目的に対して割り当てられていること 6. バックアップの方式と手順はITオペレーションの責任者によって承認され理解されていること
4.4　システムの変更や更新によるビジネスの停止を引き起こさない	1. 変更管理ルール及び手続きが設定、承認、実施されていることを確認する 2. 変更管理案件の結果はIT部門の責任者によって入手され、承認されていること
4.5　情報システムは無許可のアクセス及びデータ変更から保護されている	1. データ管理のルールが存在すること 2. データ管理報告を査閲し、データの使用がその正確性、秘匿性を適正に維持されていることを確認する

4.6　ビジネスの正常なオペレーションの継続や情報の完全性及び知的財産及び組織の記憶を含むIT資産の保護に対するリスクおよびIT利用にともなるリスクの扱いに関して考慮されている	1. 情報セキュリティ方針及び統制が定義され文書化されている 2. 情報セキュリティ統制の有効性を査閲する 3. 情報セキュリティ統制は外部組織及び/または関連のサービスプロバイダにより同意され実施されている 4. 情報セキュリティに関する事故は、事故管理手順を用いて、情報セキュリティリスクの優先度に基づいて、管理されている 5. 情報セキュリティに関する事故は、改善の機会を識別するために報告され査閲されている

プリンシプル-5 適合・準拠	
ITは、義務的な法律及び規則に適合する。 方針および実務指針が明確に定義、導入及び施行される	
サブプリンシプル	
1. ITは様々な義務（規則、法制、慣習法、契約）、内部の方針、標準及び職業指針を満足すること 2.ITプロセスと統制が導入され、組織の方針、サービス要求事項及びリスク受容度への適合を確保する 3.関連法制、必要なITプロセスの実施及び個別保証の統制及び規則の継続的な監視がなされる	
アウトカムズ	
1. 組織の方針、規則及び義務が、そのITシステムの中に正確に導入される 2. 法的、規則的要求に対する違反を防止するため、組織はその情報と取引を適切に管理する	
Audit Criteria (監査の基準)	Audit Practice Guide (監査実践ガイド)
5.1　ITは義務（規則、法律、慣習法、契約）、内部の方針、標準及び関連する職業規範を満たす	1. 下記のIT準拠性・適合性を分析する ・準拠性・適合性 ・ステークホルダーの要求事項 ・組織文化及びトップの考え方 2. 情報セキュリティ事故のインパクト報告を査閲し、改善の機会を識別する 3. IT委員会議事録及びITの適合性報告を査閲する
5.2　ITの利用が関連する義務(規則、法律、慣習法、契約)に適合することを確認する定期的かつルーティン化されたメカニズムが存在する	1. ITが義務を満たすための策定プロセスが存在する 2. トレーニングシステムが存在する 3. トレーニング計画が存在する 4. IT委員会議事録及びITの適合性報告を査閲する 5. 準拠性に関する手続きおよびガイドラインが存在する 6. 要員に関するIT倫理が定義されている

5.3　適時、包括的かつ適切なビジネス満足度を評価するメカニズムが存在する	1. 監査報告を査閲する 2. ビジネスの満足度調査報告を査閲する 3. ITのコンプライアンス及び準拠性が、資産・データの廃棄、環境、プライバシー、戦略的知的財産管理を含む、ビジネス満足度の評価に適切である事を確認する

プリンシプル-6 人的行動	
ITに関する方針、実践及び決定は、「プロセスに関わる人々」の現状及び進化するニーズをふくむ、人的要素を尊重すること	
サブプリンシプル	
1. ITの諸活動は、人的要素を識別し適切に配慮する 2. 人的要素に関わるリスクが管理され、これらのリスクは、公知の方針、手続きに基づき、関連の決定権者にエスカレートされる 3. 組織のITシステムの全分野におけるすべてのユーザに対し、継続的な教育、訓練及び力量のテストが考慮される	
アウトカムズ	
1. ステークホルダーは受容可能なマナーにおいて、組織のITシステムを利用する 2. スタッフがITシステムを生産的かつ効果的に活用して、ビジネスの効率及び価値を生成する	
Audit Criteria (監査の基準)	Audit Practice Guide (監査実践ガイド)
6.1　ITの諸活動は、人的要素を識別し適切に配慮する	1. 人的資源の管理方針が存在する 2. 方針および手続きは適切である 3. IT策定プロセスが存在する
6.2 人的要素に関連したITリスクに対するプロセスが管理されること	1. 委員会議事録を査閲する 2. キャリアーパスプログラムを査閲する 3. 社員が物理的、精神的に適正である報告書を査閲する 4. 人的要素に関わるITリスクに対する策定プロセスがあることを確認する
6.3　全てのユーザに対する教育、訓練及び力量テストが存在し、それらは一貫した組織の方針を基にしている	1. 人的資源管理方針に沿った教育、訓練計画及びカリキュラムを確認する 2. 教育及び訓練に関する報告書を査閲する

Q&A

Q1. 今回のIT-AuditのISO化がシステム監査人に与える影響についてどのようなことが考えられるか

A1. IT-AuditがISO化された場合、恐らく現在の経済産業省のシステム監査基準・管理基準にとって代わるのではないかと思われる。そうなれば日本におけるシステム監査の新たな基準として、企業から注目を集めることになると思う。またISO30120のベースになっているITガバナンスの規格である「ISO/IEC38500:2008」のJIS化も動き出していると聞いており、この両者が揃うことで、ITガバナンスに関する日本におけるシステム監査ビジネス拡大の切掛けとなるのではないかと期待している。

Q2. WDにおける他国との意見調整の目途はついているのか。

A2. 現時点で具体的な調整は進んでいない。現在ISOのWGの再編に伴い、第三国のメンバにより今後の進め方等に関する勧告がでているので、それに従っていくことになると思われる。但し、今後の具体的なスケジュールは未定である。

Q3. ダブリン後の見直し案について、サブプリンシパルとアウトカムズとは1対1に対応しているのではないのか。

A3. 現在の案では、ISO38501からアウトカムズを参照しているため1対1までの対応はしていない。

【感想】

IT-AuditのISO化というテーマは、システム監査人にとって非常に関心の高いテーマである。

参加された方も熱心に聞いていただいたようであった。しかしながら、ISO化作業そのものの進捗は芳しいといえず、定められた期限内に成果がまとまらない（参加国の合意が得られない）場合は、本プロジェクトが中止となってしまう可能性も残されている。ISOのWGの再編及び議長の交替のため、今後のスケジュールについて現時点で未定という状況からも一層懸念される。

一方で、これだけリスクコントロールという言葉が叫ばれるようになったにもかかわらず、それに反比例するかのように、我が国のシステム監査に関する活動は低調を極めている。 IT-AuditのISO化が、このような状況を打破する切掛けとなることを期待しており、システム監査基準研究会としては、極力支援を継続していく予定である。

より多くの皆様の協力をお願いしたい。

以上

■　報告３

日本システム監査人協会近畿支部　第１３８回定例研究会報告

No.1428　中田　和男

1. テーマ　　「システム監査事例からシステム監査について考える」

2. 講師　　三橋ITコンサルタント(代表)　三橋　潤氏

3. 開催日時　　2013 年 1 月 18 日(金)19:00～20:30

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

三橋氏の多年に亘る勤続経験に根差した監査実施事例2事例につき、監査実態を発表頂いた上、事例に基づき考慮すべき論点につき提起を頂いた。

(1)事例1:情報漏洩事故を起こしたシステム開発会社に対するシステム監査の実施事例

情報漏洩事故の概要:過去に作成した開発関連資料が数年後に情報漏洩事故を起こした。

①情報漏洩の経緯;

・2005 年発足の内閣官房情報セキュリティセンター(NISC)が、2007 年にサイバー空間を調査した結果、Winny 空間に官公庁関係のシステム開発に関する一部資料が漏洩している事が判明。

・漏洩の状況は、当該官公庁関係某システムの開発請負業者 A の開発体制において、一部の開発を外注した下請け開発業者 B の1開発員の所有する個人パソコンに放置されていた開発情報が、後日そのパソコンが Antinny に感染したことにより、Winny 空間に流出したと判明。

・開発請負業者 A は、漏洩した情報に関するモジュールやプログラムを迅速に再作成して入れ替えている。

・以上の状況を踏まえ、下請け開発業者 B に対するシステム監査を実施した。

②システム監査実施の状況;

・B 社のシステム漏洩事故に対する、問題発覚後の対応と再発防止策の実施状況と現状を監査する。

・システム監査の項目は、情報セキュリティ管理基準と FISC システム監査基準から抜粋して選定した。→全項目数95項目。

・実施の環境は、監査実施時点と開発時点とでは、相当変化している。

③システム監査実施報告;

・B 社の再発防止策の実施状況は評価できる。

・監査報告会は、A 社と B 社に分けて実施した。

・A 社に対しては、今回の漏洩事故の遠因となる課題があったことを指摘、今後一層のセキュリティ強化を提案した。

・B 社に対しては、セキュリティ対策状況の一層の改善策を提案した。

(2)事例2:毎年システム監査を実施している事例:

事例2の概要;

・A 社の金融機関向けアウトソーシングシステムに対するシステム監査を本番開始から毎年定期的にシステム監査を実施している。このシステム監査により、顧客に対しシステムの健全性をアッピールしている。顧客(複数の金融機関)との契約には、顧客が A 社のシステムを監査できる条項が含まれている。この結果、A 社の内部監査の他に、顧客 2 社からの外部監査が実施されることとなった。

・当該アウトソーシングシステムの状況:2003 年に本番開始、この年より内部監査を実施している。本番開始後、ソフトのバグが多発し、運用面でも指摘事項が多くあった。しかし、年 3 回の監査での指摘事項への対処で急速に改善している。

・1, 2 年目は、システム管理基準に則り、網羅的に実施、3 年目には障害分析に重点を置いて実施。4 年目にハードウェアの更改作業があり、「移行準備作業について」という監査テーマがあった。5 年目の監査テーマとしては、「昨年度から1年間の作業状況に問題は無かったかを監査する。」とした。

・システム監査を毎年実施する場合は、監査テーマの選定に難渋し、被監査システムについて深堀りする監査となっていく。そこで、被監査システムについて精通する監査メンバーが必要であり、あるいは、システムに精通する専門部署の応援が必要となる、

(3)以上の 2 事例の説明の上で、システム監査の論点につき、発表者より論点の提起を頂いた。

① 事例1から

・システム監査は、本事例の如く重大事故のケースで、再発防止策を第 3 者の視点で客観的に検証することにも使える。

② システム監査に利害関係がつきものか

・利害関係がないシステム監査はない。極力、客観性を意識した監査が必要。

③ 指摘事項がないといけないか

・重要な指摘事項がないとか、指摘事項が少ないと監査の内容に不安を感じる。この解消のためには、監査項目、資料やデータを精査して自信を深めるとともに、他の監査報告を閲覧できるなら、指摘事項を参照して、当てはめてみることも有効である。

④ システム監査で障害は防げるか。

・システム監査で障害を完全に防ぐことはできないが、開発段階の不具合発見率や単体・結合・システムテストの記録確認は必要である。障害が発生したモジュールの開発チームやリーダーの共通性に関する調査も必要である。他システムに発生した障害の状況や対応策の確認も必要である。これらを勘案して、障害防止のため、システム監査は必要である。

⑤ まとめ

以下の条項の提起があった。

・システム監査基準前文;「システム監査は、組織体の情報システムにまつわるリスクに対するコントロールが適切に整備・運用されていることを担保する。・・」

・監査チームには、被監査部門が洗い出したリスクとそのコントロールを評価できる高い技術力が必要である。

・被監査組織が管理基準の「Ⅰ.情報戦略からⅥ.共通業務」に亘る各管理項目を概略的に理解し、絶えず PDCA を回して日々業務遂行していく土壌を育成しているかが重要である。

以上の研究報告に基づき質疑応答を行い定刻散会した。　　以上

■　報告４

千葉県香取市職員向け情報セキュリティセミナー実施報告

法人部会　No.6008　梅津尚夫

平成 25 年 2 月 1 日、香取市役所において「平成24年度情報セキュリティ研修会」が開催され、法人部会の「地方自治体向け情報セキュリティセミナー」の活動として、「情報セキュリティ事故を起こさないために」と題し、約 1 時間の講義を 2 回行いました。当日は「情報セキュリティの日」2 月 2 日の前日でもあり、総勢約 100 名という大勢の職員の方が出席されました。

出席者が市民の情報を扱う立場ということもあり、最近の情報漏えい事件や市のセキュリティ施策内容について説明を行いました。質疑には、外注委託先の漏えい事故を防ぐ対策についての切実な質問もあがり、情報漏えい事件を起こさないためには、どういった対策が必要なのかという点を意識していただけたことと思います。

セキュリティセミナーの講演内容は、次の通りです。

1. 情報セキュリティの必要性 （電子自治体と個人情報保護）
2. 脅威とリスクについて （多発する情報セキュリティ事件・事故）
3. 情報セキュリティを守るための対策 （全員の心構えが情報セキュリティの基本）
4. 情報セキュリティを取り巻く諸制度 （個人情報保護関連の法制度）
5. 地方公共団体における情報セキュリティの取組み状況

窓口になっていただいた香取市総務部総務課情報管理班の皆様、ありがとうございました。

香取市研修の風景

以上

注目情報（2013/1～2013/2）

■【〈IPA〉「情報セキュリティエコノミクスシンポジウム 2013」開催のご案内】（2013/1/31 発表）

IPA では、情報セキュリティエコノミクスと呼ばれる分野における取り組みとして、「組織の内部不正防止ガイドライン」の作成や「日本的経営と情報セキュ リティ研究会」における活動を行ってきました。これらの取り組みを紹介し、情報セキュリティエコノミクスの意義を広めることおよび国内における活動を推進するためのイベント「情報セキュリティエコノミクスシンポジウム 2013」を開催いたします。

URL： http://www.ipa.go.jp/security/event/2013/eco_sympo/index.html

■【〈IPA〉テクニカルウォッチ「社会インフラとしてのクラウドに求められる信頼性とサービス継続のための条件について」レポート】（2013/1/31 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、クラウドコンピューティングの停止のリスクと、その回避のための方策に関する検討を行い、技術レポート「テクニカルウォッチ」としてとりまとめ、公開しました。

URL：https://www.ipa.go.jp/about/technicalwatch/20130131.html

■【〈IPA〉「 毎年 2 月は情報セキュリティ月間です！ 」】2013/2/1 発表）

スマートフォンの不正アプリや遠隔操作ウイルス感染など、国民生活に影響を及ぼす情報セキュリティに関する事案について多数報じられています。誰もが安心して IT の恩恵を享受するためには、国民一人ひとりがこれまで以上に情報セキュリティについて関心を持ち、これらの問題に対応していく必要があります。このため政府では 2010 年から毎年 2 月を、情報セキュリティに関する普及啓発強化のための「情報セキュリティ月間」としています。

URL： http://www.ipa.go.jp/security/txt/2013/02outline.html

全国のイベント・セミナー情報

■【事例研　第９回　課題解決セミナー】

情報システムの事故・障害で、企業や顧客が損失を被る事例が後を絶ちません。システム監査の専門家が事故・障害の原因を解き明かし、システム監査の観点から見た有効な解決策を示します。事故・障害の原因は報道だけでは分かりません。事故・障害事例をリスクとコントロールの視点で分析して、皆様の課題解決に役立つ説明をします。

情報システムの利用者から運営者、経営者から担当者まで多様な階層・職種の方のキャリアアップに、当セミナーをご活用下さい。事故・障害を未然に防ぐシステム監査の役割とその有効性の理解向上にも役立ちます。自社システムの信頼性・安全性をさらに高めたいと考えておられる経営者、役員の方、IT 部門長の方など、多くの皆様の参加をお待ちしています。

受講修了後、受講証明書をお渡ししています。

なお、当該企業がどのように問題を解決したかについての解説セミナーではありませんのでご注意下さい。

（現在、当セミナーの企業様等団体向け出張セミナーも承っております。）

http://www.saaj.or.jp/kenkyu/jirei_semi_panf.pdf

1. 日程及び会場

2013 年 3 月 2 日(土)

時間 ：　13:00～17:00

（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　6,000 円（一般）

4,000 円（日本システム監査人協会会員）

（費用には、教材費・消費税が含まれます。）

3. 内容

事例を用いて次の順で講義(受講者も一部参加)します。

STEP1：事故・障害事例を把握する

STEP2：問題事象を考える

STEP3：リスク（脅威・脆弱性）を考える

STEP4：リスク対策（コントロール）を考える

STEP5：システム監査による評価

事例講義：「大手銀行の基幹システム障害」

事例講義：「証券会社の個人情報漏洩事故」

なお、教材は、当日配布します。

4. 受講していただきたい方

どなたでもお申し込みいただけます。

特に、経営者、役員、IT 部門長の皆様の参加を歓迎いたします。

5. 募集人員　　定員18名（最小催行人員12名）

6. 受講申し込み方法

以下の URL からお申し込みください。

http://www.saaj.or.jp/kenkyu/kadaiseminar_9.html

■【東京・法人部会】

【民間企業・団体様向け情報セキュリティセミナー】 http://www.saaj.or.jp/hojin/minkan_seminar.html

【地方自治体様向け情報セキュリティセミナー】 http://www.saaj.or.jp/hojin/chihou_seminar.html

■【東京／大阪・ＣＳＡ（公認システム監査人）資格取得関係セミナー】

【公認システム監査人特別認定講習】（継続開講中）

システム監査技術者試験と関連性のある資格の所有者については、この講習を履修・修了することにより、システム監査技術者試験合格と同様の取り扱いにより、CSA資格を取得する道が用意されています。

詳細は下記URL参照 （SAAJホームページでもお知らせ中）

http://www.saaj.or.jp/csa/tokuninannai.html（公認システム監査人特別認定講習の実施について）

■【月例研究会　2013年の開催について】

2013 年の月例研究会は、4 月の開催をはじめとして、年間 10 回を予定して進めてゆきます。

開催条件としては、原則昨年と同様で以下により進めます。

開催日：毎月中・下旬の平日夜間　18.30 から 2 時間

開催場所：機械振興会館（港区芝公園3－5－8）地下 2 階　ホール

機械振興会館へ地下鉄神谷町駅から無料バスが利用できます。会館の HP をご覧ください。

http://www.jspmi.or.jp/kaigishitsu/access.html

資料配布：紙の印刷物として参加者に配布（ファイルの公開は予定していない）

参加費：会員 1000 円、会員外 3000 円

開催予定の連絡：会員にはメール、他に協会の HP に掲載

申し込み：事前に HP から行っていただく

ビデオ提供:研究会の様子をビデオで撮影して、各支部の研究会に提供します(昨年同様)

開催内容については、システム監査関連の動向などを取り入れて、テーマ、講師を選定して決めていきます。また、毎年あるいは隔年で定例のテーマで報告していただくものがあります。
(過去のテーマについては、HP に掲載しています。)

2013 年のテーマと日程については、現時点で折衝中などの状況です。会報が出される時点では具体的にご案内できると思いますが、この原稿作成時では、開催条件などをお知らせすることに止まります。なお、参加いただきました皆様には年 1 回程度アンケートを行っていますが、テーマや運営方法などについてご意見があれば、随時事務局にお寄せください。 (主査:木村　裕一)

以上

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 年の最初の会報テーマは「システム監査の普及促進」です。

本テーマは、システム監査にかかわるすべての方々の最大の関心事であり、切望している情景でもあると考えてテーマに選びました。

システム監査を社会一般に普及させて健全な情報化社会の発展に寄与することは、当協会の設立目的でもあります。新しい年の初めに相応しいテーマと思いますので、皆様からのいろいろなご意見を会報に寄せていただきたいと願っております。

この「システム監査の普及促進」は、四月号までのテーマとしたのちは今年の”基調テーマ”として、三か月ごとのテーマとは別に一年間継続し、皆様と幅広く深く意見交換して行きたいと考えています。皆様の職場で、そしてご友人と日常的な話題に採り上げるのはいかがでしょうか。また、協会の部会、研究会、支部などの活動の場でも白熱した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/

■会員でない方の送付停止は、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/

■□■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、藤沢 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）