特定非営利活動法人
日本システム監査人協会報

2013年 1月号
No 142

No. 142（2013年1月号）＜12月20日発行＞

あけましておめでとうございます。

今年も興味ある記事・新しい記事満載です。

今年一年の目標設定前に是非一読を！

羽田空港　江戸小路

会報電子版の記事　目次

〈目次続く〉

2012.12 投稿

めだか【見当識や心の理論について（システム監査人のやりがい)】　　投稿

監査において、「見当識」や「心の理論」について考えてみたいと思います。参考資料によれば、「見当識」は、次のようなものです。

“見当識とは、自分が今置かれている状況を理解する能力のことで、「今はいつ？」「ここはどこ？」「あなたは誰？」という、時間・場所・人の3つに大きく分けられます。私たちは、普段意識することはありませんが、時間の経過と場所や人を認識しながら生きています。今日は何時に起きて、午前中はどこへ行って何をして、午後はどこで誰と会ったというように、時空の中に自分を位置づけ、それを記憶しながら生きているのです。”

また、「心の理論」というものがあります。私たちが相手の心を読む、すなわち推察することができるのは、「心の理論」が発達しているからとのことです。

“男の子と女の子が、部屋の中でボール遊びをしています。しばらくすると、男の子が、ボールを青い箱の中に入れて蓋を閉め、部屋から出て行きました。すると、部屋に残った女の子が、ボールを青い箱から出して赤い箱に入れ、蓋を閉めました。その後で、男の子が部屋に戻ってきました。
あなたは、戻ってきた男の子がボールを取り出そうとして、最初にどこを探すと思いますか？”

“大人が子どもに、お菓子の箱を見せました。「中に何がはいっていると思う？」と尋ねると、子どもは「お菓子」と答えました。ところが、蓋を開けると中には鉛筆が入っていました。驚いた子どもに、大人がもう一度尋ねました。「この菓子箱をほかの人に見せて、『中に何が入っていると思う？』と尋ねたら、その人はどう答えると思う？」”

正解は、「青い箱」と、「お菓子」です。しかし、この子が正解できるかどうかは、年齢によるとのことです。また、人は、4～5歳になると心の理論が発達し、このような質問に正解できるようになるとのことです。

しかし、大人でも、見当違いなことや相手の心の読み違いは、往々にして起こります。その多くは、「感情」というものに由来すると思います。「感情」には、人にしかない、感動や、笑い、感謝あるいは嫉妬、恨みなどの複雑な感情と、ほかの動物にもある、恐怖と怒りの根源的な感情があり、これは脳の進化によるということです。

監査において、システム監査人は、常に見当を働かせ、感情的にならない心の修養と、相手に恐怖や怒りの感情を持たせないような心のゆとりが必要であると思います。そして、これができる監査人は、システム監査人のやりがいという感動を得ることができると思います。

参考資料:「認知症「不可解な行動」には理由（ワケ）がある」　佐藤眞一　ソフトバンク新書

（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。）

2012.12 投稿

めだか【　杵柄（きねづか）、年の功（とし こう）　（システム監査人のやりがい）　】　　投稿

「昔取った杵柄」、「亀の甲より年の功」。
これは尊ぶべきものだ。これほど役立つものはない。当たり前だが活用しない手はない。

巷に、基準・ガイドライン・チェックポイント・着眼点などシステム監査関係ドキュメントは数々あるが、システム監査において「**待てよ！**」とか、「**？**」とか、「**♪**」などの気付きやカン働きをリストアップしたものはない。積み重ねた経験・労苦で形成されるその人固有のものだからだ。以前のシステム業務経験（プログラミング・トラブル・悩み・失敗／成功体験など）にその源がある。それは、監査業務の経験で得られるものとは異なる。

システム監査は監査ノウハウ以前にシステム業務の経験・知識がものをいう場面が多々ある。情報システムにかかわる業務を点検・評価するのだから当然だ。**それ故**、経験済業務はもとより未経験業務の監査であっても、身に付いている座標軸（良かった、悪かった、重要だなど）を尺度に点検すれば、きっと明らかな成果を手にするはずだ。システム監査が何か特別な技能に頼らなければならないと思っていたらそれはちょっと違う。

つい最近、某製紙会社会長への長期・巨額の不正貸付事件が明るみに出た。100億円を超える額やラスベガスでのギャンブルなどまさにアンビリーバボーな出来事だった。これは経済事件だが**実は**情報システムやシステム監査に多いに関係がある。そのことをもっと論じる必要がある。私だけでなく多くの方が経験していると思うが、お金の移動や取引を処理するシステムでは、例えば次のような**管理計表**をシステムで作成・出力している。

多額取引一覧表	内部取引一覧表	例外取引管理表	異例取引発生報告	期限経過取引管理表

一例だが、金融に限らず多くの業種に同趣旨の作表システムがあり内部管理に用いられていると思う。私の時代は日常的な事務処理システムが担っていたが、昨今は内部統制に関するものと位置付けられているはずだ。

くだんの製紙会社にはこのようなものが存在していないのだろうか？　業務監査や監査役監査では例外的処理の管理計表を点検しないはずはないと思うのだが、本稿はシステム監査の観点から述べている。

システム監査において、例外的処理にかかわる管理計表の有無を点検する場面は決して少なくない。業務システムの有効性、プロジェクト監査でのシステム機能、経営支援システム、リスクアプローチやコンプライアンスの観点、内部統制監査など、このような監査に立ち会えば、個別監査計画にこのような管理計表について具体的記載がなかったとしても、現場に臨んだ際に気付きやカン働きが発揮されることが良くある。

もっと分かり易く身近な例も取り上げてみる。例えばサーバの管理状況を監査で点検する場合、UPSのバッテリーの寿命や交換については**堂々**とマイカーの経験を参考にするのがいい。バッテリー上がりや一定時期に交換しなければいざという時に車が動かない、という経験に立つことが重要だ。その上での相違点だ。

このような事例はほかにもあると思う。身に付いている**杵柄や年の功**を生かすことによって、被監査者が考慮していなかったリスクを発見し、不適切な状態を改善し、事故を未然防止することができたら、システム監査人としてこれ以上の喜びはないだろう。システム監査は杵柄や年の功が大きな力を発揮する世界だ。

（山の彼方）

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

2012.12 投稿

めだか　【　監査人の余禄（システム監査人のやりがい）　】

“システム監査人のやりがい”をテーマとしたコラム（めだか）も今月が最後のようです。
これまでの２ヶ月間は、“システム監査人のやりがい”を私なりに正面から捉えて、経験、考えを綴ってきました。
そこで、今回は最後に、少し裏口からというか、斜に構えて、監査を実施するに当たっての余禄の視点から、日頃私が考えているシステム監査人のやりがい（メリット）を紹介したいと思います。
これは、7･8 月合併号の会報に記載した「めだか【私の捉えるシステム監査の魅力（システム監査のすすめ)】」でも少し触れているものです。

私は、システム監査を含む監査業務でこれまで多くの企業を訪問してきました。そして、監査の際には、已む無い事情による例外を除き、監査実施の冒頭で、その企業の代表者と相対でお話する（お話を伺う）時間をもってきました。数人の家族経営の企業から、日本を代表する超大企業まで、規模に拘わらず、全ての監査において原則これを実施しています。その目的は、言うまでもなく監査対象企業の経営者がどのような方針、考え方で事業経営しているかをまず確認し、それを実施する監査に生かすためであり、監査において最も重要なプロセスの一つと思っています。
しかし一方、この機会はいろいろな経営者が、いろいろな考え、問題意識、ビジョンを持って経営に当たっている実態を、直接その経営者の口から聴ける、他に例を見ない私には極めて勉強になる、貴重な機会です。お会いする経営者には、私が監査人をしてない限り、会う機会はまずない筈の、極小さな企業の経営者、また、日本、世界を代表する超大企業の経営者などもいます。そして、その機会から本来の監査に関わる事項以外で学ぶことは、私にとって良い面、悪い面（反面教師）の両面で私の好奇心を満たし、また人生の糧になっています。零細企業であっても、立派な志、具体的計画をもって、顧客、従業員の心を掴み、自らが先頭に立って経営に取組んでいる経営者が現にいます。日本、世界を代表する超大企業では、大きな世界観、社会観を持ち、論理的な思考のもとに、超大組織の舵取りのポイント、醍醐味とリスクを率直に語る経営者もいます。また、ＩＴに詳しくないことから、そのリスクをどう評価し、対応するかに多くを語らず、成り行き任せ（現場任せ）で放置せざるを得ない様子の経営者もいます。更に、中には、従業員が同席する中で、監査人と取り引きをしようとする経営者もいたりして、同席している従業員のなんとも気まずそうな顔を見たこともあります。

私が、企業と一定期間付き合うコンサルティングより、その都度、その都度の出会いで多くの企業と接することができる監査に軸足をおいて仕事をしている理由の一つはこれにあり、これは正に監査に関わっているからこそ恵まれる機会（余禄）で、これが私の監査人としてのやりがいにも繋がっています。
組織経営に興味があり、また好奇心が強く、人が好きなシステム監査人には、この余禄の魅力がやりがいの一つに繋がっている人も多いのではないでしょうか。

（広太雄志）

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

投稿

■【 構築途上にあるシステムへの監査が足りない③・・・ウロコ 】

会員番号 1143　中山 孝明

連載 3 回目になる。拙文と厚顔に恥じ入りながらも書き出したからには何らかのまとまりに漕ぎ着けたいと、彷徨したがる論旨を懸命に整えている。彷徨といえば青春、青春といえばサミエル・ウルマン、何気なく用いた熟語から思い出した詩に刺激され新鮮な気持ちが戻ってきた。前月・前々月号に引き続く曖昧な副題は「ウロコ」で、これまでから一歩進めてソリューション的内容に近づける意を込めた。

表題監査を実効性あるものにする監査要点（チェック項目）の考え方について論をすすめる。
いわゆる「プロジェクト監査」において、既存の基準等を違和感なく用いているだろうか。監査の品質と効率、期待に応える監査履行の面から、システム構築プロジェクトの課題に向き合える解像力のある監査要点を欲してはいないだろうか。（基準等：「システム管理基準」（METI）、「システム管理基準解説書」（JIPDEC）、「システム監査指針」（FISC）など）

もちろん既存の基準等の活用で十分な品質のシステム監査が実施できる。この場合、実際の局面では事前に次のような整理を行って監査に臨んでいると思う。（本稿の本旨は下記★以降で述べる）

・大規模システム構築では基準等のほぼ全項目を適用する（計画から投資・調達・コンプラ・建物・教育・BCPなどまで）。
・中小システムの構築では基準等から除外可能な項目もある（建物・設備やBCPなど項目単位で除外可のもの）。
・プロジェクトの全工程に適用する項目と、工程に応じて適用する項目とを明確にする。
・監査目的、テーマ、範囲に応じて監査要点を詳細化する（被監査側意思決定者の意向反映）。
・法令適用、所管官庁／業界の指針等への遵守事項を監査要点に補充する。

一端だがこのような整理をしてもなお、システム構築プロジェクトの監査には使いにくいと感じている監査人がいると思う。既に存在しているシステムではなく、無から有を生じる過程のシステムには多くの固有事項があり、そこに着眼した監査でなければ実態に迫る監査にならないと考えている。

★農業を引き合いに論を展開する。

なぜ農業か、筆者が農家出身というだけではない。実は農業との対比が最適なのだ。農業に必要な技能、諸条件への対応力、立ちはだかる難題などが、システム構築プロジェクトのそれに驚くほど当てはまる。この対比で浮かび上がることがシステム監査の勘所となりソリューションになる。

農業は技能の習熟を必要とする。品質管理・作業調整・仕上がりの見極めなどで、産物の良し悪しは費用や収入に大きく影響する。まさにシステム構築におけるQCD管理そのものだ（品質：Quality、予算：Cost、工期：Delivery）。
下記対比表は、農業の力を借りてシステム構築プロジェクトの監査の勘所を明らかにする筆者の試みだ。

（農業欄は筆者の知識不足を補うため右文献を参考にした→新潮新書「日本農業への正しい絶望法」神門善久著
なお、紙面の関係から原文に忠実な記載ができず、引用箇所を明示していない点を容赦いただきたい。）

No.	農業	システム構築プロジェクト
1	地域特性、地形、気候によって条件が異なり、不断に変化する。	組織・要員・システム環境等によって運営状況は千差万別、流動的条件への対応力が欠かせない。
2	土作りは農業の基本、良い農家は土作りに時間と労力を投入する（田んぼで5年、畑で10年）。	システム要員の育成、調達・参入・委託する人・物のスキル・性能が成否を左右する。
3	マニュアル農業は環境変化に対応できない。	指南書頼りのプロジェクト運営は行く末が見えている。

No.	農業	システム構築プロジェクト
4	自然の摂理に大きく左右される。人為的制御が効かない生産活動。カンを働かせて対処している。	個人の意思や集団の秩序に左右される。ヒューマンエラーが避けられない活動、リーダのカン働きが必要。
5	高度な農業技能者は昆虫の生態や草木の成長などから気象予測し、作業調整に反映している。	優秀なプロジェクトリーダはメンバーの動きをきめ細かく観察し、作業管理に先手を打つ。
6	天候や病害虫などの条件に恵まれればボロができない。そこそこのものが出来る。	人材に恵まれトラブルやイレギュラーの発生次第で、ある時期のプロジェクトは順調に進行する。
7	農業技能は多くの試行錯誤や関連知識の積み重ねによって得られる。	自己啓発や経験を積み、コミュニケーション能力のあるプロジェクトリーダは得難い存在。
8	病害虫発生初期に適切な対処をしないと病害虫が多発する。周辺地域に影響を及ぼす。	トラブル発生初期の対処はもちろん、ネガティブチェックで未然防止する（進捗チェックだけでは足りない）。
9	優秀な農業者も個人では限界がある。周辺土地の環境維持や水の利用など協調が欠かせない。	個人能力と小集団活動と大集団活動の複合体。それらの計画・役割・責任の全体協調をマネジメントする。
10	農産物はスーパーマーケットの消費者感覚チェックが品質維持に果たしている役割もある。	システム監査は、組織目標実現に貢献するため、被監査部門から独立して検証し経営に報告する役割を担う。

（この対比で意味があるのは動的変動項目で、例えば委託・受託における締結事項など静的な項目は、既存のチェックリストがそのまま使えるので対比に取り上げていない。）

両者の類似点の多さ、本質を突いている点、酷似の度合いに感慨さえ湧いてくる。

この対比の目的は、あるべき論・すべき論中心ともいえる既存の基準等は、環境依存・条件変化の大きいシステム構築プロジェクトには適用しにくい部分があると考えているからだ。即ち、不確定な変動要因や阻害要因に正面から向き合った監査要点を予め明確にしておかなければ実効性ある監査は高望みになる。あるべき論・すべき論のチェック項目を裏返しにしただけでは分からない監査要点がこの対比で見えてくる。

農業が、環境と変化に逆らわず調和しつつ、耕作技能を磨き良い農産物をこしらえていること、そして土地と太陽エネルギーという二つに頼りながら様々な工夫と知識を蓄積し成し遂げてきたこと、これらは対比対象の役割として十分な重みがある。（対比表の右辺には様々な項目がリストアップ可能だが、農業と対比できることが裏付けの意味を持つ）

システム監査において「有効性監査」「信頼性監査」などの言い方がある。FISCシステム監査指針では『システム監査とは「情報システムの有効性、効率性、信頼性、安全性、及び遵守性を達成できるよう、情報システムリスクを把握し・・・』と定義している。では、システム構築プロジェクトの監査の場合は「？？性」と呼称するのがいいだろうか。有効性、効率性などでは足りない気がする。筆者は「環境性」とネーミングしたい。基盤・情勢・背景・境遇・風土・個性など様々な「環境性」に着目したシステム監査が求められている。

さて、今月の紙面も尽きてきた。熱く論じてきた（つもりなので）余韻で3点つぶやく。

※農産物の顔写真で消費者の信頼を得る。情報システムの認証制度取得をアピールすることと似ているなぁー。

※農業も情報システムも生産性や後継者など構造的課題に直面している。もっと農業に学ぶ必要がありそうだ。

※情報システムは全体最適が求められている。基準等に「全体最適化」項目が縷々記載されている。システム構築プロジェクトこそ全体最適を実現する好機だが、分業が進んだ昨今の情報システム形態において、全体最適を俯瞰し実現するスーパーマンは誰か。そして、システム監査の力はどのくらいか。

システム監査の力

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。 http://www.skansanin.com/saaj/
　ペンネームによる「めだか」や実名投稿があります。多くの方から投稿いただいておりますが、さらに活発な利用をお願いします。この会報の「会報編集部からのお知らせ」をご覧ください。

出版物

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

セミナー

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

CSA・ASA

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

会報

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

お問い合わせ

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

沼野会長一行メッセージ

“新年度はシステム監査のノウハウ整理・公表などにも注力したいと思います。”

協会からのお知らせ

■【事務局からのお願い】

公認システム監査人及びシステム監査人補の更新手続きのご案内

協会では、認定委員会より、公認システム監査人、システム監査人補の皆様へ、次のご案内を行っております。

（案内文）

公認システム監査人、システム監査人補の皆様へ

公認システム監査人、システム監査人補の資格更新対象者の方にご案内させていただいております。

更新手続きの詳細は下記 HP に掲載されていますのでご参照の上、継続教育実績をつけて、２０１３年１月末までに更新手続きを行ってください。

１．２０１３年度　公認システム監査人及びシステム監査人補の更新手続きについて（１）
http://www.saaj.or.jp/csa/csakoshin.html

２．継続教育要領
・3 年更新版
http://www.saaj.or.jp/csa/3nen_koushin.html
・2 年更新版
http://www.saaj.or.jp/csa/2nen_koushin.html

３．ＣＳＡ／ＡＳＡ認定資格更新に関するご注意
http://www.saaj.or.jp/csa/keizoku.html

日本システム監査人協会　認定委員会

■【会長コラム】

新年を迎えるにあたって

会長　沼野伸生

一年は早いものです。
本年も、会員の皆様には協会活動にご理解、ご協力を頂き誠にありがとうございました。

今年の協会運営の方向性は、以下の３点としました。
（１）システム監査の普及、促進活動の一層の推進
（２）会員サービスの一層の充実
（３）協会財政の一層の健全化

特に、これらの実現には会員増強（会勢の盛上げ）が欠かせないとして、会員増強ＰＴを立上げ、小野副会長のリーダシップの下、会員の皆様のご協力も得ながら、ＰＴメンバーが一丸となって活動してきました。

その主な活動内容は、会員紹介運動の展開、会費未納者への状況確認のための理事による電話連絡の実施、会報の充実化（協会活動情報の会報による広報の徹底、システム監査人のコラム“めだか”等への投稿の勧奨推進）、月例研究会の講師・テーマの一層の充実化と参加費の値下げ、システム監査ワークショップ支援サービス（企業へのシステム監査導入の草の根支援活動）の検討、学生会員制度の検討、そしてシステム監査基準ＩＳＯ化への支援活動などが挙げられます。各研究会等協会活動への参加を勧奨するＰＲスライドを作成し、月例研究会や各種イベントの開始前の時間帯に投影するなども秋頃から始めました。

一方、全国の支部の活動も活発に展開されました。例えば、各支部における定例研究会開催の他、６月には福岡市で西日本支部合同研究会が開催され、１１月には仙台市で東北支部が友好団体との共催でワークショップを、石川県能美市では中部支部、北信越支部が友好団体との共催で合同研究会を開催し、１２月には札幌市で北海道支部創立１０周年記念講演会が開催されるなどがありました。

また、今年は当協会が運営する公認システム監査人制度の２年毎の更新対象に当たる公認システム監査人、システム監査人補の方々が大量にあり、多くの方々の更新処理を円滑に実施しました。

社会に目を転じてみると、引続き、事件、事故が発生すると第三者による評価、点検を求めることが一般化し、システム監査もその一つである“第三者評価”の活用は社会的に定着しています。
このような状況の中、システム監査（システム監査人）の果たすべき役割は、情報社会の一層の進展と相俟って、益々大きくなり、当協会は、システム監査の普及、促進に、引続き先頭に立ってその役割を果たして行かなければならないと思います。

今年の活動は、会員、役員の皆様のご理解、ご協力、尽力でそれなりに成果を上げることができました。

しかし、会勢の盛上げはまだ途についたばかりであり、一方ではシステム監査に対する社会の期待、ニーズに呼応し、システム監査の普及、促進に直結する施策展開にも更に注力していく必要があります。

新年は、今年の会員増強（会勢の盛上げ）活動を引継ぐと共に、システム監査のノウハウの整理・公表などにも一層力を注いでいきたいと考えています。

会員の皆様の、ご理解、ご協力を引続きよろしくお願い致します。　どうぞ良い年をお迎え下さい。

研究会、セミナー開催報告、支部報告

■【近畿支部　第１３６回定例研究会報告】

報告　№1687 小宮　弘信

日時　　2012 年 11 月 16 日　18:30～20:30
会場　　大阪大学 中之島センター　2 階 講義室 201
テーマ　「“JIS Q 20000-1 の改正のポイント”と“ITSMS の本当の効果”」
講師　　株式会社マネジメント総研　代表取締役　小山俊一氏

【講演概要】

近年ますます情報システムの重要度は高まっており、システム運用サービスへの要求も高度化して来ています。そのため、IT サービスのマネジメントに関する国際規格である ISO20000 とこれに基づく IT サービスマネジメントシステム（ITSMS）への関心は高まっています。ISO20000 は ITIL V2 をベースにした BS15000 を基に策定され、ITIL の思想や概念から大きな影響を受けていますが、2007 年に ITIL は V3 で大きく変わりました。それに伴って ISO20000 も 2011 年に改正されました。そして ISO/IEC 20000-1 を基に作成された日本工業規格である JIS Q 20000-1 も 2012 年 9 月に改正されました。そこで今回は JIS Q 20000-1 について、2007 年に発行された旧版との違いなど、改正のポイントを小山氏に解説していただきました。

講師の小山俊一氏は中小企業診断士やシステム監査技術者、PMP,CISA,ITSMS Provisional Auditor など多くの資格を持たれています。そして基幹システムの構築やコンサルティングファームの経験を経て、現在は株式会社マネジメント総研の代表取締役として、情報セキュリティや IT サービスマネジメント、知的資産経営などのコンサルティング事業を展開されています。

講演の内容は「JIS Q 20000-1 の改正のポイント」として、「そもそも JIS Q 20000-1 とは？」という基本的な部分と「改正のポイント」についてお話いただきました。そして「ITSMS の本当の効果」として、「取組みの効果」と「成果につながる勘所」について講演していただきました。

「そもそも JIS Q 20000-1 とは？」では ISO や ITIL との関係、ITSMS 認証取得組織数、「IT サービス」と「IT サービスマネジメント」「マネジメントシステム」の定義と関係性、サービスマネジメントプロセスの概要についてお話いただきました。その中で、ITIL の V2 では「サービスサポート（青本)」と「サービスデリバリ（赤本)」が中心であったものが、V3 ではライフサイクル（サービスストラテジ、サービスデザイン、サービストランジション、サービスオペレーション、継続的サービス改善）の観点でまとめ直されたことや、「IT サービスマネジメント」は個々のサービスをマネジメントすることであり、その「IT サービスマネジメント」をマネジメントする枠組みが「マネジメントシステム」であることなどについて説明していただきました。また顧客からの要求事項をインプットとし、要求された IT サービスをアウトプットするためのサービスマネジメントプロセス（サービス提供プロセス、関係プロセス、解決プロセス、統合的制御プロセス等）の概要についても講義していただきました。

「改正のポイント」では JIS Q 20000-1:2007 と JIS Q 20000-1:2012 との新旧規格の違いを章ごとに説明

していただき、ISO 9001 や ISO/IEC27001 など、他の国際標準との整合性が図られたこと、文言や用語定義の見直しが図られたこと、適用範囲の定義に関する要求事項が追加されたこと、他の関係者（供給者だけでなく顧客や適用範囲外の社内組織）によって運用されるプロセスのガバナンスに関する要求事項が追加されたことなどを解説していただきました。

「取組みの効果」では JIPDEC より紹介されている ITSMS の構築・運用メリットや ITSMS 認証の取得メリット、認証取得組織へのアンケート調査結果についてご説明いただくとともに、小山氏がコンサルティング支援の現場で実際に目にして来られた導入時点での効果や運用の中で得られる効果についてもご紹介いただきました。

「成果につながる勘所」では①組織体制、②文書体系、③構築手順、④プロセスアプローチ、⑤内部監査、⑥マネジメントレビューの切り口で勘所をお話いただきました。

質疑応答では、ITSMS 認証取得組織数が 2012 年 11 月 9 日現在、累計で 171 件と年間 20 件ペースでの増加に留まっていることに対する驚きと、認証が少ない理由について質問がありました。小山氏の見解として、規格の適用対象が ISO9001 や ISO/IEC27001 に比べて限定される（IT サービスに限定され、システム開発そのものは対象外）ため絶対数が少ないことと、ITIL を意識して管理している企業は少なくないが認証取得の必要性がまだまだ温まっていないことが考えられると述べられました。また、認証の返上が見られる規格もある中で ITSMS については返上しているところは今のところ見られないこと、取組まれている組織はその有用性を実感されていること、クラウドサービスが一般化する中で IT サービスマネジメントはますます重要性が増していることなども補足されました。

昨今のサーバ障害等の事象を鑑みても、IT サービスマネジメントの仕組みの普及と、その切り口でのシステム監査の必要性は高まっており、IT サービスの品質を向上させ、継続してサービスを提供して行くためにも、もっと JIS Q 20000-1 の浸透を図って行かなければならないと感じました。

以上

■【近畿支部セミナー実施報告】

報告者：No1345 広瀬 克之

日時　　2012 年 11 月 17 日　13:00～17:00
会場　　常翔学園大阪センター
テーマ　「事例に学ぶシステム監査の基本と応用」
講師　　是松理事、荒町理事、三橋氏、吉谷氏（共に支部サポーター）

【講演概要】

近畿支部では、１１月１７日（土）１３時から、常翔学園大阪センターで、「事例に学ぶシステム監査の基本と応用」と題したセミナーを開催しました。１４名の受講生を迎え、近畿支部スタッフ４名がシステム監査の現場で発生している諸問題について、それぞれ４５分を持ち時間として講演しました。

【内容】

１．テーマ監査／業務監査としてのシステム監査事例
－J-SOX・IT 統制評価と棲み分けて－

グローバル企業で、内部監査室に勤務し幅広く内部監査を実践している支部会員の講演です。年間を通して、どのように監査を実施し、効果をあげているか、また何を課題認識しているかについて、実際に利用しているチェックリストなども交えてご紹介しました。

２．ファイル共有ソフトによる情報漏洩事故の事例

大手ハード・ソフトベンダーでシステム監査室に勤務中に遭遇した事件について、どのように問題をとらえ解決していったかを紹介しました。協力会社による情報漏洩という身近な事象に、興味を持って頂けたと思います。

３．システム管理基準等を用いたＢＣＰ（事業継続計画）監査について

近年数々の災害・事件に見舞われ、ＢＣＰはすべての組織にとって大きな経営課題となっています。その中で近畿支部が取組んでいる実企業へのＢＣＰ策定支援やＢＣＰの監査に関する考察などを紹介しました。

４．マネジメントシステム規格の統合的な運用　－内部監査の効率的な運用事例－

講師が長年外部監査の専門家として環境、品質、プライバシー監査に携わってきた支部会員であり、最近話題となっている統合監査のホットな話題を、具体的な条文も引用しながら紹介しました。多くの企業が複数の認証に向けて今後取組む指針を与えるものと思います。

それぞれの講演をみなさん興味深く聴講され、講演後、積極的に質疑もされて、テーマの関心の高さがうかがえました。今回のセミナーは、システム監査の場面では何が起こっているのか、興味・関心を持って頂くことをねらいとして、支部会員の経験・考えをご紹介するものでした。受講生の皆さまからは次のような声を頂きました。

・「テーマ監査／業務監査としてのシステム監査事例　－J-SOX・IT 統制評価と棲み分けて－」は実際の内部監査事例で、具体的で大変参考となった。
・「ファイル共有ソフトによる情報漏洩事故の事例」の起こってしまった監査の事例として参考となった。
・当社でもＢＣＰ監査を実施しているが、システム管理基準等を用いたＢＣＰ（事業継続計画）監査について」を聞いて、アプローチの仕方が間違っていなかったことがわかった。

・「マネジメントシステム規格の統合的な運用」にあった「具体的な確認事項」は参考にしたい。

また、今回は事例を気軽に聞いて頂こうという企画のため、資料は当日配付としましたが、「事前に学習しておきたかった」「実用的なシートだったので利用してみたい」などの意見も頂きました。これらを参考に、今後も会員の経験を有効活用できるような機会を作りたいと考えています。

以上

■【第１７６回月例研究会受講報告】

報告者　梅里　悦康

日時　　2012 年 10 月 26 日　18:30～20:30
会場　　機械振興会館地下２Ｆホール
テーマ　「コーポレート・ガバナンスと IT ガバナンス～監査役の視点から～」
講師　　アリアンツ生命保険.監査役　河邊（こうべ）精一　氏
CGEIT, CISM, CISA, CIA, MBA

【講師紹介】
河邊氏は、某割賦販売会社の在職中に、慶応ビジネススクールで MBA を取得された。
その後、米国系の船会社で IT 部長を経て、
1991 年から米国系保険会社グループで内部監査に従事。その後、システム監査部長として SOX スペシャリストとして活躍されました。
2006 年から米国系コンサルティング会社で IT ガバナンスのコンサルティング業務に従事され、
2009 年から火災共済・中小企業共済組合の顧問をされ、
2008 年にアリアンツ生命保険.社外監査役に就任し現在に至る。

【講演概要】
『昨年は、オリンパス、大王製紙とトップの不祥事が相次ぎ、今年に入ってもインサイダー取引などの不祥事で、日本企業のガバナンスが問われています。本講演では、先ず企業のガバナンスについて、会社法の見直しなどの最近の動向や欧米のガバナンスとの違いについてお話したいと思います。
そのような現状を踏まえて、企業のＩＴについてのガバナンスの動向を見ながら、システム監査人の果たすべき役割と監査役の立場で見たＩＴに係るガバナンスの監査のポイントなどを監査役の視点からお話いたします。
なお、講演内容の一部はＩＳＡＣＡ東京支部の８月の月例会でお話したことと重複いたしますが、今回は、監査役として企業のガバナンスの向上にシステム監査をどう役立ててもらいたいかということに重点を置いて、事例なども交えながらお話しするつもりです。』

【内容】
➢コーポレート・ガバナンスの要点
企業のガバナンスが話題になるのは、不祥事が起きた時が圧倒的に多く、また、いわゆる SOX に見られるような不祥事からの制度の変更があるかと思います。いずれにしろ、マイナスなイメージが強く、前向きな企業の発展とは逆のブレーキとしてのイメージです。しかし、ガバナンスはもっと企業経営にとってその目標達成に不可欠な概念と考えます。

➢企業経営とガバナンス
〇海賊にもガバナンスは必要不可欠？
→海賊という極端な例を用いてガバナンスの意味を考えてみます。海賊は、商船を襲い金品を略奪する、その行為自体は無法ですが、無法だからと言って海賊船の船員がそれぞれ勝手なことをやっていたらうまく行かないのです。映画パイレーツ・オブ・カリビアンでコードという言葉が何度か出てきます。コードは**掟**と訳されていますが、コード（掟）という規則があって、目的達成（略奪を最大限にする）ためにはその掟を守らせる

ガバナンスが必要です。“ガバナンス“という言葉からは政府のような公的なイメージがありますが、なにか目的を成し遂げるためには海賊でも必要なことです。そして、このコード（掟・規程）は海賊船の船長と船員の双方、すなわちステークスホルダー全員が規程を理解して契約するとともに、船長・オフィサーがいて船員同士も互いに監視し、その遵守状況をチェックするガバナンスが存在します。

このことは企業経営においても同様で、企業の収益性を確保することがガバナンス実践の目的です。

〇経営の強さ

→有効なガバナンスの構築には、アカウンタビリティ（説明責任）と透明性の確保が不可欠です。ステークホルダーに対する説明責任がきちんと果たせて、経営に透明性があることでガバナンスの実践が可能となり、安定した強い経営基盤ができると考えます。

➢不祥事とガバナンス

→不祥事の発生によりガバナンスが問われています。

〇不祥事の構造

→不祥事の起こる背景にはいろいろな理由があります。不正検査では、不正のトライアングルという概念があるといわれています。

「動機・プレッシャー」、「機会」、「行為の正当化」の 3 要素、この３つが揃うと不正がおきます。逆にいうとどれか一つでも欠けると不正は起きません。

→オリンパス事件では、「動機・プレッシャー：財テクにおける投資の失敗にて、当事者に損出しカバーのプレッシャーがあります。」、「機会：監査役が主導しましたが、監査役を含めて全ての役員を含めて仲間内でできてしまう。」、「行為の正当化：損が出た場合株価が下がり株主に迷惑をかける。」の 3 要素がありました。この例は、本来監視役である監査役が首謀者の一人であるということで、後に述べる日本企業の制度でチェック機能が不完全であるという問題点が出た典型です。

〇IT に係る不祥事

→東日本震災直後のみずほ銀行のシステム障害では、経営者のガバナンスの問題とも言われています。また、個人情報漏えいの多くはコントロールの不備ですが、その背景にはガバナンスの問題があるように思います。ある米国での調査では、CIO は不正の兆候を見つけてもなかなか報告しないケースが多いという報告がありましたが、IT に限らず不祥事故を隠ぺいしないで報告する風土が必要です。

〇ガバナンスの強化で不祥事はなくなるか？

→事前に不正の兆候を見つけることで罪を犯させない仕組み、モニタリングや監査により不正を早期発見できる仕組みが必要です。

８０年代アメリカではスーパーマーケットの収益圧迫の最大の要因は従業員の不正と言われていました。不正を早期発見できる仕組みは収益にも影響します。

ただし、ガバナンス実践は不祥事を無くすのが目的ではないことに留意。

➢会社法の見直しにおけるガバナンス

〇今回の会社法見直しの対象

→先月の法制審議会に諮られました会社法の見直し案は「企業統治の在り方」ということ「親子会社に関する規律」が主な改正点ですが、またここで、ガバナンスの強化というとして監査役の権限強化と社外取締役の厳

格化があります。

〇今回の会社法見直しの是非

→これは、オリンパスや大王製紙の不祥事のようなものを想定したものと思われますが、このような体制面だけのものでは、企業の活力を失わせるブレーキとしてのガバナンスの強化だけになると考えます。何度も述べますが、安定した強い経営で企業の収益性を確保することがガバナンス実践の目的であり、不祥事を無くすのが目的ではありません。

➢日本企業のガバナンス

→先程の法制改革の背景には、日本のコーポレート・ガバナンスが機能していないとの外国（欧米）の投資家からの言われ続けていることがあります。その中には、日本独特の監査役制度そのものが、欧米、特に米国の制度と違っていて判りにくい、それに加えて投資家に対する英語での説明のまずさもあって、不信感を抱かせてきました。

余談ですが、今まで監査役の英語訳は Corporate Auditor でしたが、やっと先日、日本監査役協会で Audit & Supervisory Board Member という新しい呼称の諮問がなされました。

ここで、英語の問題もさることながら、その背景にある組織や歴史的な経緯、文化的な違いが、よりガバナンスというものの本質を誤解させているところがあるのではないかと考える。

〇欧米企業との対比

・組織の違い

→米国の一般的な組織では経営は執行役員に任され、取締役・取締役会はその監視ということで分れていますので、少なくとも建前上はガバナンスが効きます。しかし、日本の場合では取締役が執行役を兼務しているために、この監視機能が不十分です。監視役は社外取締役と監査役ということになりますが、実際は社長が選任し決定していますので、欧米の投資家からみるとガバナンスが効いていないことになります。

・歴史の違い

→法律の違いがありますが、その法律の成立や企業の成立の歴史的背景の違いもあります。

・文化の違い

→米国は全てが契約の契約社会で、経営者と株主は契約関係にあり、経営者には説明責任があり、取締役は経営者の契約（職務）履行を監視することがガバナンスの基本となりますが、日本ではそのような考えは馴染まず、そこに食い違いが生じてきます。

➢IT ガバナンスの動向

〇ISACA /ITGI: COBIT 5 で、呼び方が IT ガバナンスから Governance of Enterprise IT と変わりました。

→図を見ていただくと対象領域の発展（Evolution of scope）がわかります。

最初 1996 年：COBIT1 では システム監査（Audit） の指針でした。

それが 1998 年：COBIT2 では コントロール、内部統制（Control）という監査だけでない拡がった言い方、概念となりました。

2000 年：COBIT3 では更に Management に広がり、

2005 年 7 月：COBIT4.0/4.1 では IT Governance という表現になり、IT 投資（ Val IT 2.0（2008））と IT リスク（ Risk IT（2009））が後に出されました。

2012 年： COBIT5 では、 Governance of Enterprise IT となり、SOX における COSO を意識して、次第に対象

領域が広がり、IT 内部におけるガバナンスから企業のガバナンスの一部としての IT 部分を見てゆくという形に変わってきて、IT 投資価値と IT リスクの評価が統合されています。

➢ISACA/ITGI: COBIT 5

〇GEIT（ガイトと読みます）のガバナンス活動の５つのプロセス

1. Ensure governance framework setting and maintenance.（ガバナンス・フレームワークの設定と維持）
2. Ensure benefits delivery.（成果の提供） →IT から何が生み出されるか？
3. Ensure risk optimization.（リスクの最適化） →リスクの最適化プロセス。
4. Ensure resource optimization.（資源の最適化） →資源は何に使われるか？
5. Ensure stakeholder transparency.（利害関係者への透明性）→説明責任が果たせるか？

各プロセスには、EDM（Evaluate:評価、Direct:指揮、Monitor:モニター）が定義される。

→EDM は IT に限らず企業のガバナンス活動と共通の概念です。

➢ISACA: CGEIT （シーガイト）

→ISACA の資格として 2008 年から認定が始まりました。

〇CGEIT 専門領域（ドメイン ）

→CGEIT シーガイトでは 6 個のドメインが定義されています。

・Domain 1 - IT Governance Framework（IT ガバナンスの枠組）
・Domain 2 - Strategic Alignment（戦略との整合）
　→IT 戦略が企業の戦略に沿ったものかどうか。
・Domain 3 - Value Delivery（価値の提供）
・Domain 4 - Risk Management（リスク管理）
・Domain 5 - Resource Management（リソース管理）
・Domain 6 - Performance Measurement（成果の測定）

→成果測定は IT プロジェクトの成果のコントロールに近い考え方ですが、そのプロセスはステークホルダーに対して透明で、説明責任を果たさなければいけません。

→COBIT５のガバナンス活動に近いものになっています。

➢監査役と IT ガバナンス

→昨年、日本監査役協会から「監査役に期待される IT ガバナンスの実践」という報告書が出されましたが、報告書が出されること自体、今までになく IT ガバナンスが経営に大きな影響があることの表れです。いわゆる J-SOX では本家の US－SOX より IT が強調されていますが、日本では経営者の IT 意識が低いことから明示されたようです。IT が専門家に任せで済んだ時代とは違い、現在は PC なしでは仕事にならず、最近ではクラウドや BYOD などが話題になっています。監査役も、IT ガバナンスに無関心ではいられません。

➢IT ガバナンスの定義

（日本監査役協会による定義です）

〇「IT ガバナンスとは、コーポレート・ガバナンスの一側面であって、企業価値の向上を目指しつつ企業の社会的

責任を果たし、かつ事業継続と業務の有効性及び効率性を達成するために、IT の戦略的利活用とそれに伴うリスクに対して、全社的に対処するための取締役の職能と責任の明確化、及びそれを独立した立場から監視・検証する監査役の職能と責任を通じて、企業グループ全体としての IT 利活用の適切な推進と IT 利活用をめぐるリスク対処を効果的にするための仕組みないしは活動をいう。」

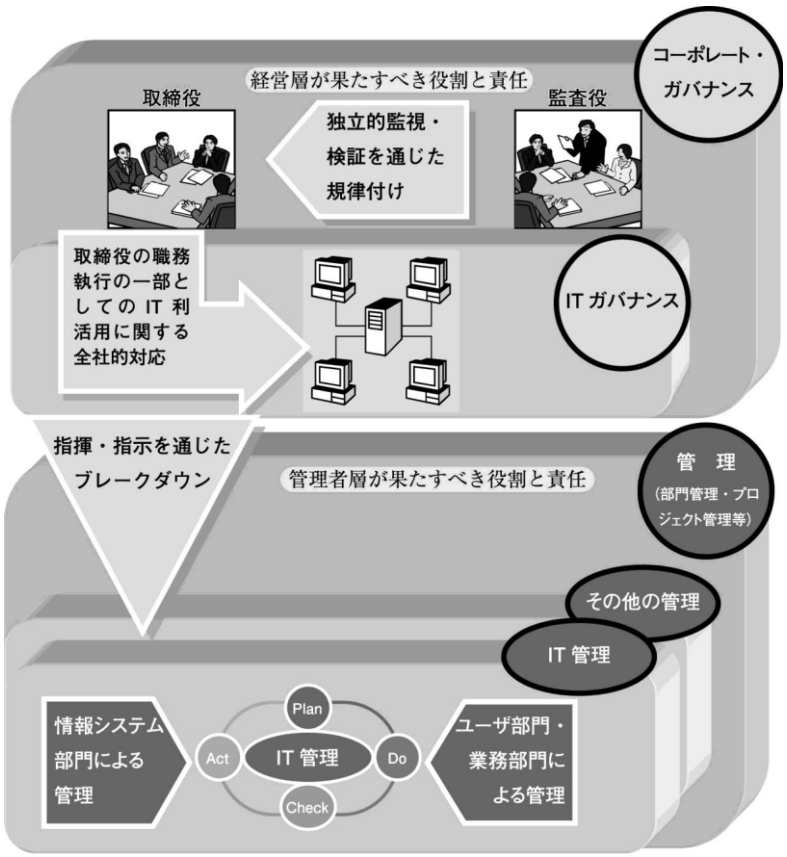
（監査役に期待される IT ガバナンスの実践、 2011 年 8 月）

→「取締役の職能と責任の明確化」がキーワードです。収益を最大にする IT 利活用は取締役の責任です。IT は専門家任せでは、取締役の職務をまっとうしているとはいえません。

〇ガバナンスと管理（マネジメント）の関係

「監査役に期待される IT ガバナンスの実践」 2011 年 8 月

図 1 ガバナンスと管理（マネジメント）の関係（P. 4）より転載



図の上部はガバナンスで、上半分は監査役の領域です。日本では、取締役の職務に対するものをシステム監査で見るのは難しいと思われます。米国の教科書では、内部監査は、取締役会の監査委員会へ報告し、独立しています。

図の下部はマネジメントです。下半分は、システム監査にて今までマネジメントとして見ています。

図 1　ガバナンスと管理（マネジメント）の関係

営業部門、生産部門、管理部門などがあり、その上にガバナンスとして取締役会があります。ガバナンスはそれらをひっくるめて企業活動があり、監査は、スコープを定めてみていきます。役員レベルへの監査は大変難しいと思います。

通常、システム監査は下半分ですが、監査役監査では上半分が対象になります。

「監査役に期待される IT ガバナンスの実践」 2011 年 8 月
図２監査役によるガバナンス機能発揮の必要性（ P. ６）より転載

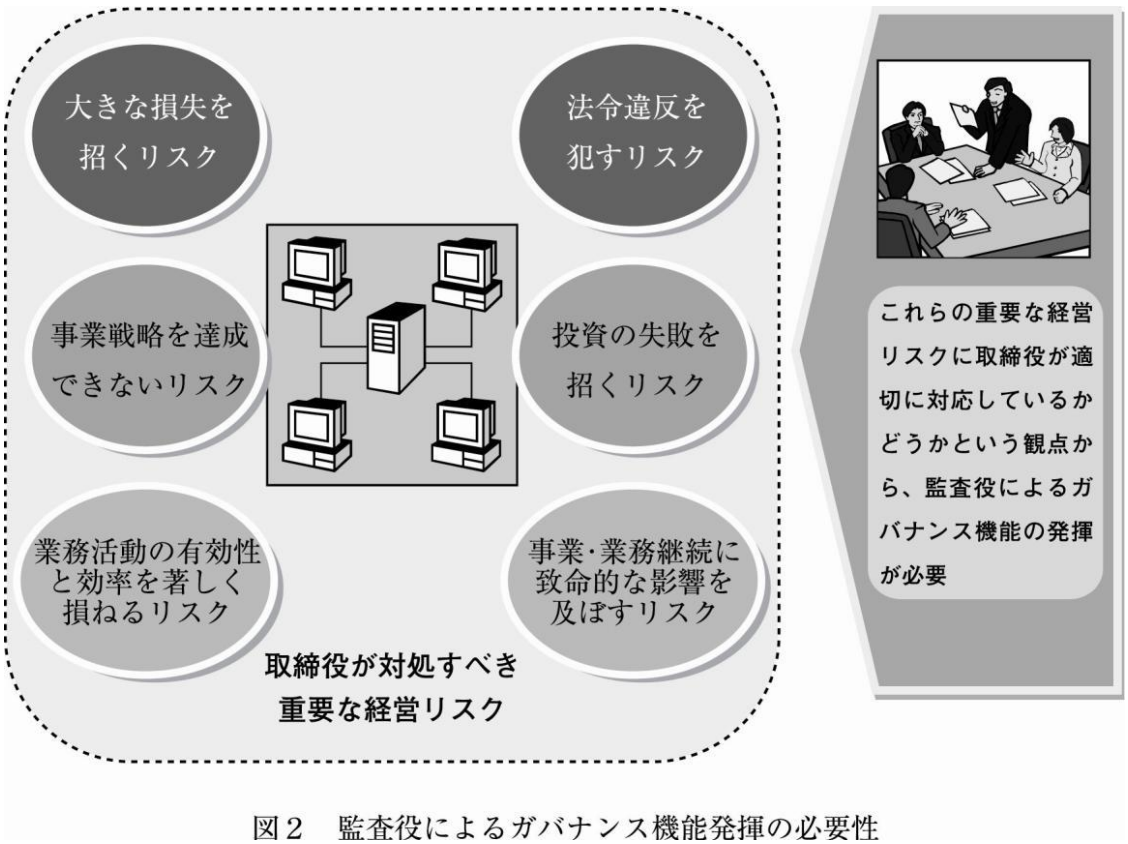


図２　監査役によるガバナンス機能発揮の必要性

→隅々まで IT が浸透し利用されている現在、経営リスクと IT リスクを分離できない状況です。
→経営リスクのなかの一つとして IT リスクを見ていかねばなりません。

➢IT ガバナンスが目指すもの
「監査役に期待される IT ガバナンスの実践」
2011 年 8 月
図３IT ガバナンスの４つの目的（P. 11）より転載

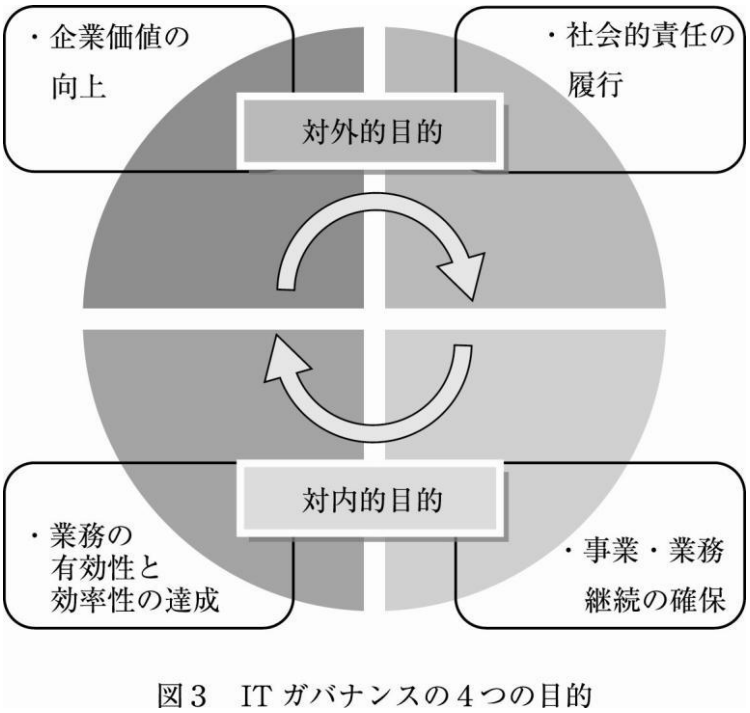


図３　IT ガバナンスの４つの目的

→IT ガバナンスはが特別なものではなく、IT 以外とまったく同じ企業活動の一部になってきています。対外的目的には、先ほどお話しましたステークホルダーに対するアカウンタビリティが含まれます。

➢システム監査と IT ガバナンス

→システム監査と IT ガバナンスを先ほどの Cobit5 や CGEIT のドメインの定義を参考に監査のスコープ的に見て行きます。

〇IT プロジェクトの管理

→IT プロジェクトの各段階での効果測定ができていますか？

IT ガバナンスを意識したシステム監査で、最初のステップとして重要です。

〇IT 資源の管理

→IT に係わるリソース、人、モノ、金、時間の適切な配分と管理がされていますか？

IT 資源が最適に配分されていることの説明責任と資源配分の透明性のための情報管理がなされている必要があります。

〇IT リスクの管理

→IT だけの問題でなく全社的な観点からのリスクの把握、測定できていますか？

適切なリスクの低減策、許容範囲を超えるリスクの管理、許容範囲の決定の適切性を見る必要があります。

〇IT の企業業績への貢献

→IT 投資は企業活動に価値をもたらしていますか？

常に IT 投資が企業活動に価値をもたらすかどうかを考えて決定されているかを見る必要があります。

〇企業戦略と IT 戦略の整合性

→企業戦略と IT 戦略は一体でなければなりませんが、往々にして IT 戦略を監査しようとしたときに、企業戦略の方も明確でないことがあります。これは、IT ガバナンス以前の問題です。

〇IT ガバナンスのフレームワーク

→SOX 対応で、規則と役職だけは出来ているが実質的に機能していない例があります。組織の規模や特徴に応じた体制があり、実質的に機能していることが大切です。

以下、個別に詳しく見ていきます。

➢IT プロジェクトの管理

〇個々のプロジェクトは IT 戦略と矛盾していないか。

〇プロジェクトのリスク管理（進捗、予算、その他の資源、プロセス、モニタリング、報告）は適切に行われているか。

〇成果の測定は予め決められた通りに行われ、適切に報告されているか。

〇成果物は事前に決められた要件を満たしているか。

➢IT 資源の管理

〇IT 投資の最適性

→計画の段階で投資効果を測定する指標を作成し、管理できる体制となっている必要があります。従って、途中でリクエストが変わるなどの変更があった場合には、その都度、測定指標の変更される必要があります。

〇要員の確保（量・質・教育訓練）

→十分な知識・経験のある必要なマンパワーを確保する要員計画が将来にわたってできているか。特に、大きなプロジェクトが考えられる場合には、的確な要求定義やプロジェクト全体を管理できる要員を確保することが重要です。

〇外注管理

→戦略として外注利用の是非が検討されているか。セキュリティを含めて外注管理体制ができているか。

契約を SLA（報告者注：Service Level Agreement)や SLS（報告者注：Service Level Specification)で管理し、報告・分析・ペナルティ・契約の見直しを行う体制があるか。

課題は適宜解決しているか。

〇ハードウェア・インフラの管理

→IT の場合は技術の進歩が速いので、それまでの知識や経験が役に立たないこともあります。技術の陳腐化が早いので、将来に向けた教育と人材の育成がなされているかが重要です。また、リニューアルのタイミングや外注化の検討、会社の将来の規模や方向性を考えた対応が出来る体制になっているかを見る必要があります。

（河邊さんが所属する）アリアンツ生命では、今年 1 月から「変額年金」の新規営業を中止しましたが、それまでは営業を拡大する方針で、右肩上がりの計画でした。しかし、年金原資の運用環境の悪化から営業停止を決定し、それに合わせてこれは、IT も要員の削減や経費の削減という 180 度の方向転換が必要となりました。このように計画外の事態に対応を迫られた時には、経営者とのコミュニケーションがガバナンス上重要になります。

➢IT リスク管理

〇リスクアセスメント

・IT システム特性

・コントロールの不備、脆弱性の特定

・可用性の判断

・影響度の分析

→これらの見地からリスク事象の発生頻度、影響額を定量化してあるかどうか。

〇リスク軽減策

・技術的対応、管理的対応、運用的対応がある

リスクの許容限度の決定がどのようになされ、それは経営者のリスク選好を反映しているかどうかです。

ここで、監査をする場合、リスク軽減策そのものの是非を見るのではなく、その軽減策を採用するに至った意思決定のプロセスで、十分な情報の収集と検討がなされたかを見るべきです。一般に、ガバナンスの監査で経営者の意思決定の結果は監査の範囲外で、意思決定者（経営者）が正しい情報収集の努力をして検討を重ねたかどうかが監査の範囲内です。

〇定期的な見直しと文書化

→リスクは刻々と変わります。文書化は透明性の確保のため必要です。

➢IT の企業業績への貢献

〇システムの効果の測定

→後になって何をもってシステムの効果を測定するか不明？ではおかしいです。

リクエストの段階、戦略計画できちんと何を持って測るのか予め決めておくことです。

〇ステークホルダーのニーズに合ったシステムの提供

→ユーザ部門がいいましたので、それを作りましたでは不可。

→CIO が、取締役レベルか？システム委員会戦略メンバーレベルか？

優先順位をつける点で、コントロールされているか？そのコントロールを決めるのは取締役レベルか？

〇透明性とアカウンタビリティ

→業績への貢献、取締役の責任を明確にする必要がある。

➢企業戦略と IT 戦略の整合性

〇企業の方針・戦略・事業計画などと IT 開発・運用に矛盾はないか？

→企業の戦略立案時には IT 部門が入っているべきで、そうであれば矛盾はないはずです。しかし、現実は立案後に IT 部門に伝えられるために、開発・運用計画は IT 部門が独自に策定することから、矛盾する場合が出てきます。

〇システム開発の戦略や計画は経営者により十分検討されているか？

→システム戦略委員会がある会社は多いです。ユーザ部門とシステム部門だけで行うのではなく経営者が優先順位付に参加することが必要で、効果の測定、成果は報告されて経営者がその責任を自覚している必要があります。

〇IT 開発は企業の事業計画・戦略等の変更を反映しているか？

→事業計画の変更の十分な情報が IT 部門に入ってこない、あるいは計画変更に際して考慮するべき IT が十分検討されていないことのないようなコミュニケーション体制が必要です。

〇IT 責任者（CIO）は、経営者に十分な情報提供を行なっているか？

→CIO は、例えば無理な開発スケジュールなどを押し付けられ事などが無いように、IT の知識・情報とともに十分な権限を持っていることが大切です。また経営の感覚を持って、経営者が判断するのに必要十分な情報を提供できていなければなりません。

ガバナンスを考えたとき、システム監査は CIO や IT 部門と経営者のコミュニケーション状況を見る必要があります。

➢IT ガバナンスのフレームワーク

〇組織体制、責任者の職務と権限、プロセスの構築

〇方針・規程類・規則の文書化と定期的な見直し

→J-SOX では当たり前ですが、文書は見直しの経緯がわかるようになっていること。

〇方針・規程類・規則の周知徹底

→ガバナンスは海賊の例でみたように、当事者が契約概念をもって方針・規程類・規則を遵守することです。周知徹底とは、こういうことであり、当然、違反した場合には罰則も適用されるということです。

〇法令・規制等の遵守体制

→コンプライアンスということで、いわゆる脱法行為など社会通念上許されない行為も違反と認識されます。

〇新技術などへの対応

→IT の特徴として、常に新しい有効な製品や技術の導入にも積極的である必要があります。IT ガバナンスもそれに対応できる体制が必要です。

➢監査役監査と IT ガバナンス（１）

監査役協会の報告書では、監査役のガバナンス監査として以下のものを挙げています。

〇情報保存管理体制の監査

〇損失危険管理体制の監査

〇効率性確保体制の監査

〇法令等遵守体制の監査

〇企業集団内部統制の監査

「監査役に期待される IT ガバナンスの実践」 2011 年 8 月

＜付録＞「会社法施行規則」に基づく IT ガバナンス・チェックリスト（ P.48）

➢監査役監査と IT ガバナンス（２）

〇監査役監査のポイント

→取締役会、執行役員会、IT 関連委員会などで、 IT リスクに関しての十分な議論が行われているか？

〇取締役の IT ガバナンスへの認識

→専門家にまかせているから大丈夫ではこまります。

〇CIO は十分な知識と権限を持っているか？

→ガバナンス確保のためには大事です。

〇モニタリング体制は組織に組み込まれているか？

→監査役として是非ともみなければなりません。監査役・内部監査部門は状況を見て報告する体制－組織体制が何らかの形で必要です。

➢システム監査人と監査役の連携

→システム監査人と監査役の連携は、今日、是非とも皆様にお話ししたかった事の１つです。

システム監査人の立場では監査役とはあまり話をする機会がないのではないかと思います。オフィシャルなコミュニケーションの体制があるべきですが、監査役と内部監査人との連携は大切であるが、なかなか難しいのが現状です。

米国では、内部監査人が直接、取締役のなかの audit committee（報告者注：監査委員会）に報告するので、経営者も監査の対象になりますが、日本では社長へ報告しますので、経営者のガバナンスの不備は指摘しにくいことになります。そのためにも、経営者の監視役である監査役との連携が不可欠です。

〇監査役に対する IT の啓発

→残念ながら監査役で IT に明るい方が大変少ないことから、最近の IT リスクの問題について監査役への啓蒙が必要です。監査役はまじめな人が多く、監査役は極めて勉強家ですので、話をすれば間違えなく聞いてくれると思います。IT リスクに懸念を持つ監査役は非常に多くいます。例えば、最近の事件では遠隔操作ウィルス問題になっていますし、新テクノロジとして、クラウド、ソーシャルネットワーク、スマートフォン、タブレット端末があり、話題になっています。

例えば、ソーシャルネットワークにて顧客情報を集める、あるいは新しい携帯デバイスを導入するなどという営業からの提案を取締役会で議論することになったと考えてみてください。最新の IT を正しく理解していないと、その提案に懸念があったとしても、リスクがわからず、取締役会での議論に質問も出来ません。結果、

声の大きな者に押し切られることになります。

〇監査役への情報提供

→システム監査人の方は自社システムの現状、問題点などの情報を監査役に提供していただきたいと思います。特に社外監査役はそうですが、自社のシステムの状況を知らないことが多く、また、それを自分で調べることは困難です。基本的なところから、ハードウェア・ソフトウェア・セキュリティについて最低限の情報の提供を是非お願いしたいと思います。

「監査役に報告すると細かいことを聞いてくるので鬱陶しい」という話をときどき聞きますが、基本的な情報を持っていなくて報告を正確に理解するとなると次々と疑問点が出てくるのです。日頃、出来るだけコミュニケーションをとって、些細なことでも、いろいろ情報をお願いいたします。

〇監査役の有効利用

→システム監査人では言いにくいこと、言えない問題は、監査役を使って言ってもらうということも可能です。先ほどお話ししましたように、日本の会社の組織・制度ではガバナンスに関わるような問題を指摘しにくい環境ですので、経営に重大な影響を及ぼす懸念がある場合には、大いに監査役を利用してください。監査役はこのようなときのために存在し、法律で強い権限を持っています。

逆に監査役は問題を薄々感じていることもありますが証拠がないと言えないことも多くあります。システム監査人の目にしたことをどんどん話して、監査役と議論していただければと思います。

ありがとうございました。(大きな拍手)

参考情報

「海賊の経済学」ピーター・ T・リーソン著　エヌティティ出版　 2011

「監査役に期待される IT ガバナンスの実践」　公益社団法人日本監査役協会　2011

http://www.kansa.or.jp/support/library/misc/it.html

質疑応答：

→Q：最後の方、「監査役監査と IT ガバナンス（２）」「CIO は十分な知識と権限を持っているか？」について質問があります。

私のみるところでは、日本と米国では CEO、CFO は違いがないと思えます。

CIO はその組織の IT の指令塔でないといけないはずです。

情報システム部門担当役員と CIO とは違いがあると思いますが、

監査役が当該 CIO は十分な知識・権限を持っていない判断されると

監査役としてはどうしたらいいか？

CIO は個人の問題、知識を持っていない場合、かなり言い方が難しいと思います。

どういう風に申し上げたらいいのでしょうか？

→A: 情報システム担当役員では兼任が多く、知識を持っていないケースが多いと思います。逆に CIO と名前がついているが名前がついても課長レベルのケースもあると思います。また、日本の企業では CIO が居ないケ

ースもあります。
CIO が必ずしも十分な知識がない、あるいは取締役レベルの権限をもっていないと絶対ダメではありません。IT 戦略委員会というものがあって、そのなかできちっとした議論して、担当役員が出てきちっと理解できる体制になっていて、例えばシステム部長、システム部門のスタッフが委員会で IT について説明する、組織として戦略・リスクを判断できる体制ができていればいいです。
また、CIO 個人でやらなければいけない場合は、情報収集の努力をしてもらわなければなりません。自分で判断できなければ、外部コンサルを利用しても判断できれば十分可能です。
努力をしていなければ問題であり、そのような CIO を任命したのであれば、それは取締役全員の責任です。取締役会として、もし担当者に能力が足りない場合、これを補う仕組みが必要となると思います。監査役としては、CIO や個人ではなく、取締役会にこの問題を提起すべきと思います。

＜感想＞

ガバナンス全てに IT ガバナンスが入り込んでいること、監査役のシステムに係る情報取集に困難性があること、システム及びその IT リスクについて正しく理解していないと監査役が取締役会で質問もできずに大きな声に押し切られてしまうおそれがあること、システム監査人と監査役との連携がいかに重要であるかということが、強く印象に残りました。

また、河邊さまから、システム監査人と監査役が接触する機会は、従来は中々なかったですが、現在ではメールを利用することができるようになり、連携方法として有効に利用できるようになったということを伺い、大いに参考に出来ることと受け取りました。

以上

注目情報（2012/11～12）

■ＩＰＡ：セキュリティセンター　「２０１２年１２月の呼びかけ」　（2012/12/3 発表）

「 ネット銀行を狙った不正なポップアップに注意！ 」

～　“乱数表”や“合言葉”の正しい使われ方を知り、自己防衛を　～

パソコンでインターネットバンキングにログインしようとすると、ウイルスが不正なポップアップ画面を表示して、合言葉や乱数表を利用者に入力させ、これらの情報を窃取しようとする新たな手口の犯行が発生しているとして、警察庁と各金融機関が注意を呼び掛けています。

従来のフィッシング詐欺は、利用者を「見た目はそっくりだが完全に別の偽サイト」へ巧みに誘導して、個人情報や金銭に関わる情報を窃取するケースが大部分でした。また 2011 年 9 月には、銀行を装った偽メールにウイルスが添付されていて、そのウイルスを実行するとログイン情報や乱数表の内容の入力を促す偽の画面が出現するといった手口も出現しました。

今回の新たな手口では、「本物のサイトにアクセスしたら、”途中から”偽の画面が出現する」という点で、今までのフィッシング詐欺の手口と決定的に異なります。本物のサイトのログイン後の表示であるために利用者が信用してしまい、情報を入力して被害が広がったと推測されます。

詳しくは、下記 URL を参照。

http://www.ipa.go.jp/security/txt/2012/12outline.html

■ＩＰＡ：プレス発表　（2012/12/11 発表）

「2012 年度 情報セキュリティの脅威に対する意識調査」報告書を公開

～ 適切なパスワード設定を含む情報セキュリティ対策の基本が浸透せず

IPA（独立行政法人情報処理推進機構、理事長：藤江　一正）は、情報セキュリティに関する対策情報の発信、普及啓発等の活動に役立てることを目的として、インターネット利用者を対象とした「2012 年度　情報セキュリティの脅威に対する意識調査」を実施し、その報告書を 2012 年 12 月 11 日（火）から、IPA のウェブサイトで公開しました。

詳しくは、下記 URL を参照

http://www.ipa.go.jp/security/fy24/reports/ishiki/index.html

全国のイベント・セミナー情報

■【東京・月例研究会】

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

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

回	日時	テーマ	講師	
第 178 回 月例研究会	12 月 17 日(月) 18:30～	予兆型システムリスクに挑む― 先進的なこれからのシステムリスク管理、監査を提案する ―	ＮＰＯ法人 日本システム監査人協会 理事　遠藤 誠 様	開催場所は、本表下の欄外のとおりです。
第 179 回 月例研究会	1 月 22 日(火) 18:30～	システム監査基準のＩＳＯ化について（仮題）	日本システム監査人協会 システム監査基準研究会	

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

■【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）

■【東京・事例研究会】

「システム監査実務セミナー」

「システム監査人の実務能力の維持・向上」のためのセミナーです。

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。

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。
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。
〈日　時〉 2013 年 2 月 2 日(土)～ 3 日
2013 年 2 月 9 日(土)～10 日(1 泊 2 日×2)
〈場　所〉 晴海グランドホテル
中央区晴海 3-8-1　TEL:03-3533-7111
〈費　用〉 日本システム監査人協会会員　168,000 円、　その他の方　189,000 円
〈定　員〉 20 名(最小催行人員 10 名)
詳細は下記URL参照 (SAAJのホームページでもお知らせ中)
http://www.saaj.or.jp/kenkyu/jitsumuseminar21.html

■【大阪・近畿支部主催セミナー】

「2013年度近畿支部総会・第138回定例研究会」

〈日　時〉 2013 年1月18 日(金)
18:30～19:00　2013年度近畿支部総会
19:00～20:30　第138回定例研究会
〈場　所〉 大阪大学中之島センター　2階　講義室201
http://www.onc.osaka-u.ac.jp/others/map/index.php
大阪市北区中之島4－3－53
電話:06－6444－2100
京阪中之島線　中之島駅より 徒歩約5分
〈内　容〉「システム監査事例からシステム監査について考える」
〈講　師〉 三橋ITコンサルタント(代表)　三橋　潤　様
公認システム監査人　公認情報セキュリティ主任監査人　公認情報
システム監査人　電気主任技術者(第三種)　電気工事担任者
〈費　用〉 日本システム監査人協会会員/ISACA大阪支部会員　1,000 円、　その他の方　3,000 円
懇親会 4,000 円
詳細は下記URL参照 (SAAJのホームページでもお知らせ中)
http://www.saaj.or.jp/shibu/kinki/kenkyukai138.html

会報編集部からのお知らせ

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

□■ １．　会報テーマについて

2012 年 11 月～2013 年 1 月発行の会報テーマは「システム監査人のやりがい」です（4 月～6 月のテーマは「システム監査人の悩み」、7 月～10 月発行の会報テーマは「システム監査のすすめ」でした）。

11 月からの会報テーマ「システム監査人のやりがい」如何だったでしょうか。皆様思い思いのやりがいについて貴重な体験、意見が紹介されました。共感できる部分、反論がある部分などあったかと思います。また、これからシステム監査人を目指す方にとっては貴重な情報であったと思います。

今後も会報編集部としては、さまざまなご意見やコラムを募集しております。否定的なご意見も大歓迎であります。会報を通して議論が盛り上がり、協会活動が活発となることを目指したいと思います。

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

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

□■ ２．　会報の記事に直接コメントを投稿できます

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

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

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

□■ ３．会員の皆様からの投稿を募集しております

分類は次の通りです。

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

２．会員投稿　（Word の投稿用テンプレートを利用してください）

３．会報投稿論文 （論文投稿規程があります）

これらは、いつでも募集しております。 気楽に投稿ください。

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

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

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

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

会員限定記事

【本部・理事会議事録】（会員サイトから閲覧ください。パスワードが必要です）

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

■発行：　NPO 法人　日本システム監査人協会　会報編集部

〒103-0025　東京都中央区日本橋茅場町２－８－８共同ビル６F

■ご質問は、下記のお問い合わせフォームよりお願いします。

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

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

会員でない方は、購読申請・解除フォームに申請することで送付停止できます。

【送付停止】　http://www.skansanin.com/saaj/

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

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

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

━━