

日本システム監査人協会報

新システム監査基準と SI事業者との関わり

No.148 木村 裕一

はじめに

新システム監査基準が平成8年1月30日に改訂された。昭和60年8月の制定から10年目の最初の改訂である。会報担当からの依頼により、この基準の改訂の概要を紹介し、改訂内容とSI事業者との関わりや課題についての私的な意見を述べる。

1. システム監査基準の変更点について

今回の基準改訂の狙いは次の点にある。

- ① 新しい情報システム環境への対応
- ② 災害対策の強化
- ③ 国際化への対応

新基準は旧基準と比較すると図1に示すように基準項目数が大巾に増加している。この詳細は先般 JIPDEC が主催でシステム監査基準特別講演会(8年3月14日、15日)が開催され、解説されている。ここでは概要を紹介する。

(1) 新しい情報システム環境への対応

システム監査基準の中心をなす実施基準が変更されている。

旧基準はホストコンピュータを中心とした情報システムを対象としていたが、新基準で対象とする情報システムはネットワークを含むことを強調している。

また情報システムの分散と集中の形態を検討し決定することは、企業情報システムの戦略的な部分であると重視し、企業業務に中項目「情報戦略」を設けている。

分散処理環境の構築に不可欠なネットワークに関して、システム設計の中にネットワークに関する監査項目を設け、運用業務に中項目「ネットワーク管理」を設け、同じくネットワークを含むシステムの中項目「構成管理」を設けている。

分散処理環境は、専門性の低い一般事務室も機器等の設置対象となり、システムの管理項目が広範囲になる事から、新基準では全般的に

ルールの制定を重視し、責任の明確化を図っている。

(2) 災害対策の強化

阪神大震災を踏まえ、実施基準に地震対策を中心とした災害対策をまとめた中項目「災害対策」を新設している。災害対策は、「リスク分析」、「災害時対応計画」、「バックアップ」、「代替処理・復旧」から構成されている。

(3) 国際化への対応

OECDの「情報システムセキュリティガイドライン」が情報システムの要員及び監査人の責任の明確化を求めている。これは一般基準の中に「システム監査人の責任・権限」、「職業倫理」、「守秘義務」の監査項目が追加された。実施基準においては、中項目「要員管理」を中心に基準項目の内容に取り入れられている。

(4) 実施基準の構成

以上を取り入れて実施基準とするにあたり、「システム開発取引の共通フレーム」に採用されている企画、開発、運用、保守及び共通業務という構成としている。共通フレームはISO・IECで標準化を検討中のソフトウェア・ライフサイクル・プロセス(SLCP)企画案に基づいているため、国際的な協調という観点からの対応となっている。この実施基準の構成は図2のとおりである。

(5) 一般基準

一般基準では監査計画の策定と手順について述べると共に、前記のようにシステム監査人の責任と権限、職業倫理、守秘義務を追加し明文化している。システム監査とシステム監査人の果たすべき役割を明確にし、実施基準の充実に呼応したものとなっている。

(6) その他

新基準では新たに「用語の定義」の項を設けて主要な用語を定義し、「実施基準の考え方」の項で基準の適用方法について明確に説明している。例えば実施基準は集中処理又は分散処理の

いずれにも適用出来ること、開発方法に依存せず適用出来ること、共通業務の基準の適用方法などを明示している。

(以上は、通産省情報処理振興課小森係長による「システム監査基準」改訂(システム監査学会のJSSAニュースNo. 47)を参考にさせていただいた。)

2. SI事業者とシステム監査基準の関わり

2.1 SI事業者の登録認定制度及び特定SO企業等認定制度

(1) SI事業者の登録認定

SI事業者とは情報処理業者を対象とした通産省の「システムインテグレーション(SI)登録・認定」制度に基づいて登録認定された企業である。情報システムの開発を主とするSI事業者認定の目的は、情報化に関するノウハウを持たない企業等に対して、安心して情報化投資を行い、その実現を図れるような情報サービス業者を認定することにある。ユーザーニーズとしては複数企業間、異業種間の情報ネットワークの構築、ユーザフレンドリーなシステムの構築、多くのハードウェア、ソフトウェアの組合せによる最適なシステムの構築等があり、それらを実現させ得る事業者を認定しようとするものである。

その認定申請書の記載事項の一部に次のものがあり、SI事業者として期待される要件の一端を表すと考えられる。

SIの取引先、得意とするSI分野、情報処理技術者試験合格者、人材育成の状況(カリキュラム、研修期間、研修費等)、協力会社と委託分野 等

(2) 特定SO企業等認定

「特定システムオペレーション(SO)企業等認定制度」が平成6年から施行されている。これは、ユーザ企業の情報システムを一括して管理・運用し、アウトソーシング事業としてサービスを提供する情報サービス企業を認定するものである。認定申請書では情報サービス企業の経営的、技術的基盤を審査するものであるが、同時にサービスのレベルを確保していることも審査している。申請はシステム監査に関して、次の項目を記載するようになっている。

システム監査の実施主体、内容について・監査人、・頻度、・計画の概要
SO事業の組織・体制について・部署名、・情報処理技術者試験合格者、・人材育成の状況・経験のある業務分野・守秘義務規程の有無

2.2 システム監査の実施

特定SO企業等認定制度の申請要件には、1回/年以上のシステム監査の実施がほぼ必須である。一方SI事業者の登録認定要件には、それは明示されていない。両者は主として運用と開発の相違があるが、それぞれの分野に要員、教育、組織、規定等によりユーザーニーズを満たす能力のレベルが要求されていること、及びシステム監査の目的を考慮すると、SI事業者もシステム監査の実施が求められていると考えられる。

これらのシステム監査の実施は、通産省のシステム監査基準を利用すること等が期待される。すなわち

- ① システム監査基準に基づいて実施
- ② システム監査人(システム監査基準に基づく試験合格者)がシステム監査を実施
- ③ (自社内でシステム監査が実施出来ない場合) システム監査企業(注)によりシステム監査を実施する。(注)システム監査企業台帳制度に基づく申告企業。
- ④ システム監査は年度計画を作成する等、計画的、継続的にシステム監査を実施すること等である。

3. SI業者としてシステム監査実施により期待される事項

今回のシステム監査基準改訂に伴い、当然システム監査の実施内容に対する期待も変わると考えられる。

しかしこれまでSO認定制度においても具体的にどのようなシステム監査が期待され求められるのか明文化されていない。であるからといってシステム監査を一時期に全項目全範囲にわたって詳細に実施することは實際上出来ないことである。各企業の状況を把握の上、重点を設定し、中長期的な基本計画のもとで実施することになろう。

(1) 実施事項

システム監査を実施するにあたり、まず

システム監査計画：基本計画・個別計画一等を明確にする。

計画策定は基準の改訂に起因する事項ではないが、新基準を利用することにより、分散処理形態のシステムにたいしても、計画の中でこれまでよりは明確に重点項目の設定が可能であろう。例えば基準の改訂により範囲が広がった項目に関して次のように考える。

項 目	監査の段階	内 容 例
戦略性への対応	企画	SI事業者からの提案がユーザの事業戦略等に適応した内容になっているか
個人情報保護	開発・運用	SI事業者が構築するシステムが個人情報保護の条件を満たしていること
ネットワーク	企画・開発・運用	ネットワークの障害対策、セキュリティ対策がシステム機能資源を防御するよう実施されているか
災害対策	開発・運用	ソフト、ハード、ネットワーク、運用面で災害対応が考慮されていること
外部委託	全般	SI業務を外部の力を借りて実現する際に、委託内容に関して、考慮し対策すべき事項が充たされていること

(2) システム監査の実施状況

当協会の法人部会による調査には、次のような結果が出ている。

システム監査の実施企業は、業種別に見ると、金融業は75%、情報処理・情報サービス業は31%等の結果となっている。情報処理・情報サービス企業各々の具体的なサービスの内容は不明であるが、ここに含まれるSO企業は当然として、SI事業を目指す企業の場合はより以上にシステム監査を実施する必要がある。

システム監査を実施しない理由を問う別の質問項目の回答では、「実施する必要性を感じない」という回答が約25%となっている。システム監査の効果が認識されていないという事を意味していると考えられ、システム監査人としては、重視しなくてはならない。

(3) システム監査実施の啓蒙、推進と課題

2.2項に述べたとおり、SO登録企業にはシステム監査の実施がほぼ義務付けられているが、SI事業者の申請ではその点は明文化されていない。

システム監査を実施することは、SI事業者としての業務対応(信頼性、安全性の向上、効率性の追及)力を強化し、向上させることが目的であるが、その評価尺度はない。システム監査を実施し、真面目に対応(改善)すれば事業者としての実力が向上し元が取れるという考えがある。一方、必要性が義務となっていない現在、SO登

録を考えないとすれば、評価が客観的にはつきりしないシステム監査の実施にはそれほど力が入らないという企業が多いというのが実情でないかと思われる。

これらについては、システム監査人としては経営者層に対して啓蒙、普及活動が更に必要である事を示すと共に、ユーザの役に立つシステム監査となるよう今以上のレベルアップを図ることが必要である。

またSI事業者、SO事業者の立場からは自社の体質強化を図らなければならない一方、例えば災害対策などの強化は費用負担をユーザに求める場合がでてくる。経費増はなかなかユーザに受け入れられない要因であるが、真の意味でユーザに役立つ情報システムを提供することを考えた場合、今回の改定により、基準として災害対策が明確にされたことは、負担のお願いがしやすくなる面があるのかも考えられる。

システム監査人として以上を考えた場合、内容の濃い、効果の見えるシステム監査を実施して、経営者にシステム監査の価値を認めさせることと合わせて、その効果を客観的にアピールすることも必要であるかと考えられる。

この点は、システム監査人に課せられた課題であるといえる。

システム監査基準の改訂に合わせて、これらについて多くのシステム監査人や企業の参加により今後議論することを提案したい。

図 1

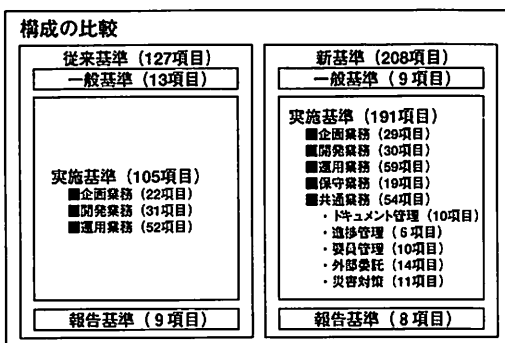
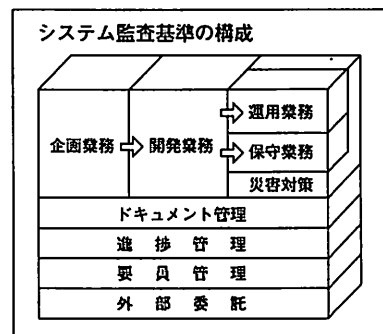


図 2



メーカーの立場から見た 改訂システム監査基準

No.239 小野 修一

今回のシステム監査基準の改訂に対して、メーカーの立場での考えおよび対応をまとめることが私に与えられたテーマである。この記事では、社としての統一された見解、対応策ではなく、メーカーに勤めるシステムエンジニアとしての立場、またシステム監査を業とする立場での改訂システム監査基準に対する考えをまとめてみた。

今回のシステム監査基準の改訂には、いくつかの重要なポイントがあるが、その中でメーカーとして対応していくべき事項、顧客がメーカーに期待している点、ビジネスライクな言い方をすれば、今回のシステム監査基準の改訂によってどのような新しいビジネスがメーカーとして創出できるか、といった観点で、私の考えを以下のように整理してみた。

1. 新しい情報システム環境への対応

今回のシステム監査基準の改訂の最も大きなポイントは、新しい情報システム環境に対応できるような基準としたことである。具体的には、

- ・ クライアントサーバシステムに代表される分散型システム環境の発展
- ・ オープンなネットワーク活用の広がり複雑化
- ・ ウォータフォール型だけでなく、RAD型、プロトタイプ型、スパイラル型などの新しいシステム開発手法の採用
- ・ 情報処理技術に精通した専門家だけでなく、業務担当者が情報システムを直接使用するEUC/EUDの浸透
- ・ ダウンサイジングやアウトソーシングを採用する企業の増加

などが、新しい情報システム環境の流れと見ることができる。

メーカーはこれらの新しい情報システム環境を顧客に提案し、顧客に導入し、顧客の業務の高度化に結びつけることを仕事としている。したがって、今回のシステム監査基準を監査項目としてだけでなく、新しい情報システム環境が進展する中で、いかにすれば顧客に満足を与える情報システムを構築し、それを取り巻く諸環境を整備することができるかといった目でシステ

ム監査基準を活用していく必要がある。

また、最新の情報処理技術に裏付けされた情報化サービス、エンドユーザまでを対象に捉えた情報システムのあり方の提案などが顧客から期待されている。

2. 上流段階におけるコンサルティングのシステム監査

従来のシステム監査基準は、システムの基本設計段階から運用段階を主な対象領域としていたが、今回の改訂では企画段階の最も上流段階までを対象としている。具体的には、経営戦略と情報戦略との整合性の確認、情報戦略の有効性の評価、システム開発の全体計画の中での情報システムの全体像の明確化、システム分析・要求定義段階におけるリスク分析や利用部門を巻き込んだ検討などが、具体的な監査項目として改訂システム監査基準の中に出てきている。

それらのシステム開発の最上流段階におけるシステム監査は、コンサルティング的色彩がかなり強い内容であり、メーカーとしては顧客の経営方針やトップマネジメントの意向をベースにした経営コンサルティング、情報化コンサルティングといった位置づけでの対応にしていけるべきである。そして、上流コンサルティングの結果として、実際のシステム開発の企画段階以降のシステム監査に結びつけていくことが、効果を上げる方法である。

3. 新たなセキュリティ要件への対応

現在、コンピュータウイルス、ソフトウェアの違法コピー、情報システムに対する不正アクセスなどが、情報システムの健全性に影響を与える深刻なセキュリティ要件となってきたが、従来のシステム監査基準ではそれらについては多くは触れられていなかった。

通産省では、それらのセキュリティ要件に対する対策をシステム監査基準とは別の基準やガイドラインとしてまとめ、システム監査基準ではそれらを併せて活用せよとしている。

メーカーとして考えるべきことは、それらのセキュリティ要件を監査項目として確認するだけでなく、セキュリティ対策の重要性の顧客への教育・啓蒙、システムを構築する段階でそれらに対するセキュリティ対策を盛り込むような指導、セキュリティ対策をパッケージ化した商品の開発・提供などによって、顧客におけるセキュリティ対策の効果を上げることである。

4. 災害対策、障害対策などの安全対策への対応

阪神大震災の教訓を踏まえ、今回のシステム監査基準の改訂では災害対策が共通業務の中の独立した監査項目になるなど、安全対策についての監査基準が具体的かつ厳しく設けられた。また、留意事項の中で、情報システム安全対策基準も併せて活用すべきとなった。

メーカはコンピュータシステムおよび関連設備を顧客に導入するにあたって、安全対策についての点検・指導を行っているが、今後は、厳しくなったシステム監査基準および情報システム安全対策基準に準拠した情報システムの安全対策に対するコンサルティングや基準への適合性の確認がサービスメニューとして重要となる。

5. 国際化に向けた対応

今回のシステム監査基準の改訂では、国際標準を基にした「ソフトウェア取引の共通フレーム」に監査基準の体系を合わせるOECDセキュリティガイドラインに則したセキュリティ対策を盛り込む、など国際化への対応が行われた。

顧客のシステム開発や運用における国際化への対応はまだ未熟であり、日本企業の国際進出の進展という現状を考えた時、メーカとして、海外においても運用するシステム開発取引のあり方、セキュリティ対策の具体化を顧客に提案していく必要がある。

新システム監査基準はシステム監査人の武器となるか

名古屋経済大学 中西 昌武

●世の中の環境が変化すると、システム管理の具体的なあり方について見直しが要求されるようになる。当然、これを対象とするシステム監査についてもその規準の見直しが必要である。このような理由でシステム監査基準が改訂されたようである。本稿は「新システム監査基準はシステム監査人の武器となるか」という観点で＜新基準＞を評価する。

●はじめに、新旧基準の内容面での継承および変更の主な点を簡単に整理する。

1. 一般基準・実施基準・報告基準の構成は従来通りだが、編集上の工夫により全体に見やすくなった。
2. 記載内容が増加し、各基準のディレクトリ階

層が増えた。マニュアル化が進んだようにも見える。

3. 伝統的なSDLCの枠組みを踏襲しているように見える。その他手法への適用方法は示されていない。
4. システム監査人の倫理、運用業務における震災対策、保守・移行・廃棄、などの記述を新設・強化した。
5. ドキュメント管理など共通業務として認識できるものを整理しモジュール化した。

●新基準は旧基準と同じく「本基準は、情報システムの信頼性、安全性及び効率性の向上を図り、情報化社会の健全化に資するため、システム監査に当たって必要な事項を網羅的に示したものである」と述べる。

●一般に、必要な事項の示し方には4つのパターンがあると考えられる。

1. 行動原理(キーワード的に示すもの)
2. マニュアル(ガイドラインとして示すもの)
3. 例示(実際の例で見せるもの)
4. しつけ(賞罰を通して身につけさせるもの)
 - 1 (行動原理)は行動全般の意味づけによって状況に対応できる応用力を与える。
 - 2 (マニュアル)は個々の状況において取りうる行動の手順・様式を提供する。
 - 3 (例示)は、実際の場面での振る舞い方を間接体験的に示す。
 - 4 (しつけ)は、条件反射に訴える定着手段である。

1～4はお互いに支えあう関係にある。行動原理が十分個人の内面に浸透すると、自身の力によって理解を深め応用力を高められるようになる。行動原理の機能を持つものだけが本来の基準の名に値する。マニュアルだけでは基準と呼べない。

●システム監査人に供給されるべき行動原理はどのようなものだろうか。

システム監査人は今、システム管理環境の流動化に耐えうる柔軟なシステム監査行動を支える行動原理を必要としている。もし伝統的なSDLCを創造的に破壊するシステム開発技術があれば、その最善に向けた統制項目を評価し指摘できるシステム監査原理が必要なのである。しかし新基準は伝統的なSDLCの枠組みを自ら解体する勇気を持てなかったようである。それどころか従来路線の中でマニュアル化を進めているように見える。そのような努力は、マニ

アルの詳細化を頼みとして行き詰まった伝統的なSDLC方法論と同じ危険をはらんでいる。

また翻ってマニュアル化をめざすのであれば、問題別・適用業務別に項目を充実させねばならない。開発業務の場合、プロトタイプ手法やCASEツール適用、RAD、EUD、アウトソーシングなどにそれぞれ対応したシステム監査マニュアルが必要となる。

「4 実施基準の考え方」の「(2)実施基準は、開発方法に依存することなく適用できる」は、柔軟な行動原理の供給を怠り、その一方で問題別・適用業務別の監査項目を具体的に用意していない点を、どう説明するのだろうか。

●以下、本来的ではないが、新基準をマニュアルとして見たときに気づいた点をいくつか指摘する。

震災被害への対策事項は、リスクファイナンスまで踏み込んだ監査項目が用意されるとよかったように思う。

ソフトウェア／ハードウェア／ネットワークの構成管理、システムライフサイクルのフェーズ別にテーマを整理すべきであった。

保守工数の一般的増大傾向の中で、保守は、作業効率と品質保証をいかに両立するかが課題となっている。その意味で、保守業務の監査が指摘されたことは評価できる。

外部委託については、契約管理の適切性の評価を促す項目は用意されているものの、評価方法の視点は用意されていない。複雑化しつつある契約関係に対応できる監査項目が欲しいところである。

●新システム監査基準は、行動原理書としても、マニュアルとしても、システム監査人の武器としては力不足である。今後は実際レベルで柔軟に適用できるシステム監査「理論」づくりの共同研究が必要である。無原則の実践信仰は廃すべきである。さしあたっては基準を行動原理編とマニュアル編に分離することを提案する。そして行動原理編においては理論的整備を、マニュアル編においては監査ノウハウの整備による理論と実践の結合をめざすべきであろう。

システム監査基準の改訂内容について ——システム監査人の責任

No.203 馬場 要輔

今般、システム監査基準が11年ぶりに改訂された。種々の書物や専門誌で紹介されているのでご承知のことと思うが、改訂ポイントは次の

3点といわれる。

- ① 新しい情報システム環境への対応
- ② 国際化への対応
- ③ 災害対策

現時点では解説書が発行されていないこともあり(6月に刊行される予定)、内容を詳しく分析したわけではないが、内容的には、監査項目も充実し、基準が情報システムを巡る技術の進歩や、環境の変化に追いついたという点は評価されるものと思う。

基準を読んでみて感じたことは、私のような内容監査人にとっては、「実施基準」以外の所、特に「一般基準」と「報告基準」に味が出ていると思われる点である。

国際化の対応に関しての、OECDの「セキュリティガイドライン(註1)」が反映されているものと思われるが、特に、「システム監査人の責任・権限」、「職業倫理」、「報告書作成」の所である。(註1)OECDセキュリティガイドラインの関連原則として、

(1) 責任原則

情報システムの所有者、提供者、利用者その他情報システムセキュリティにかかわる者の役割と責任を明確にする必要がある。

(3) 倫理原則

情報システムおよび情報システムセキュリティは、第三者の権利と法的権益を尊重して提供される必要がある。

が、見られる。

次に、関連する基準を紹介してみると、

V. 一般基準

3. システム監査人の責任・権限・・・新設

- (1) システム監査人は、自らの判断に対する根拠を明確にすること

4. 職業倫理・・・新設

- (1) システム監査人は、客観的な評価者としての立場を堅持すること
- (2) システム監査人は、自己に対する倫理的要請を自覚し、的確かつ誠実なシステム監査の実践を通じて、内外の信頼に応えること

VII. 報告基準

1. 報告書作成

- (5) システム監査報告書は、改善勧告について提示できる改善案を記載することである。

この4つの基準から、求められているシステム監査人像をイメージしてみると、

- ① 多様で、広範囲な情報システムの各業務に対して、その正否、良否、適否を判断する根拠(知識、経験)を持ち、被監査部門(被監査者)に対して明確に示すことができること。
- ② (自身や監査部門の置かれている相対的立場に影響される事なく)いかなる被監査部門(被

監査者)に対しても客観的に評価できること。

- ③ システム監査人に対する倫理的要請がどんなものかを知っており、それを守っていること。(註2)

(註2) 当協会では、平成5年2月に12条の「倫理規定」を制定し公表すると共に、会員証の裏面には倫理規定の遵守がうたわれている。

- ④ システム監査人は、的確かつ誠実なシステム監査を実施して、監査の依頼者の信頼に応えること
(参考)

「的確」とは、的確をはずれず確かなこと。まちがいのないこと。…広辞苑

真相についていて正確なこと…岩波国語辞典
「誠実」とは、(仕事に対して)まじめで、真心がこもっていること。…広辞苑

- ⑤ 報告書で改善勧告する場合は、(情報システム部門に対して、現実的で実現性のある)改善案を記載することで、一段と高い知識や経験に加え、提案能力が求められている。(旧基準では、「必要に応じ改善案を併記」であった)
(参考)

「提示」とは、提出して示すこと…広辞苑

等々である。

これらに対応するためには、システム監査人は、今以上に情報システムや業務及びシステム監査に関しての広く深い知識、技能を備えと共に、これを維持するための不断的努力が必要となるであろう。

また、システム監査人がこのような重い責任や高い能力を求められることに対して、それを充足しているシステム監査人に対する内部的、社会的地位の向上や、職業としての保証が制度的に構築されるよう働きかける必要があるのではないかと思う次第である。

第44回月例研究会 感想文

日 時：平成8年3月6日

テーマ：「ファイアウォールとインターネット・セキュリティ」

講 師：日本ユニシス(株)
オープン企画推進部
堀越 繁明氏

No.555 松枝 憲司

さる3月6日に開催された月例研究会は、現在ブームとなっているインターネットのセキュリティについて、堀越氏より講演があった。

《講演内容》

1. インターネットの概念

インターネットが、世界中のネットワーク同志を結び付けるネットワークであるという概念について、あらためて説明があった。現在のインターネット上での主なサービス内容は以下の通りである。

① 電子メール(E-mail)

現在ユーザ数は全世界で約6,000万人である。

② ネットニュース(Net News)

ネットワーク上で情報を得たり意見交換が可能。

③ 遠隔ログイン(TELNET)

接続先のCPU、MEMORY等を借用して様々なサービスを受ける事ができる。遠隔地保守サービス等に利用。

④ ファイル転送(FTP)

データやプログラムの交換が可能。ソフトのバージョンアップ手段等として利用されている。

⑤ WWW(World Wide Web)

インターネットブームの火付け役。世界中のWWWサーバにアクセスできる。現在サーバ数は、2ヶ月半で倍増するペースである。

2. InternetとIntranetの融合

従来社内システムと対社外システムが分離していたが、統合化が進み、今後はWWWのインターフェースで社内外の情報へアクセスするいわゆるIntranetの時代を迎える。インターネットは参加者が対等の立場であり、お互いが丸見の状態である。そのため内と外の境界が必要であり、ファイアウォールの必要性が生じた。

3. ファイアウォールの概念

定義の紹介「組織において危険にさらされる計算機の数とサービスを制限し、セキュリティを向上させる技術の総称」。

「何を守るのか」、「どこに置くのか」が、重要である。

4. ファイアウォールの仕組み

① パケット・フィルタリング

【メリット】

○ 既存のネットワークを直接インターネットに接続できる。

【デメリット】

● セキュリティ強度が落ちる。

● ルータのアクセスコントロールが難しい。

② トランスポートゲートウェイ

【メリット】

○ 内側の情報が隠せる。

○ 正規アドレスを台数分持たなくてよい。

【デメリット】

● ユーザプログラムを変更する必要がある。

③ アプリケーション・ゲートウェイ

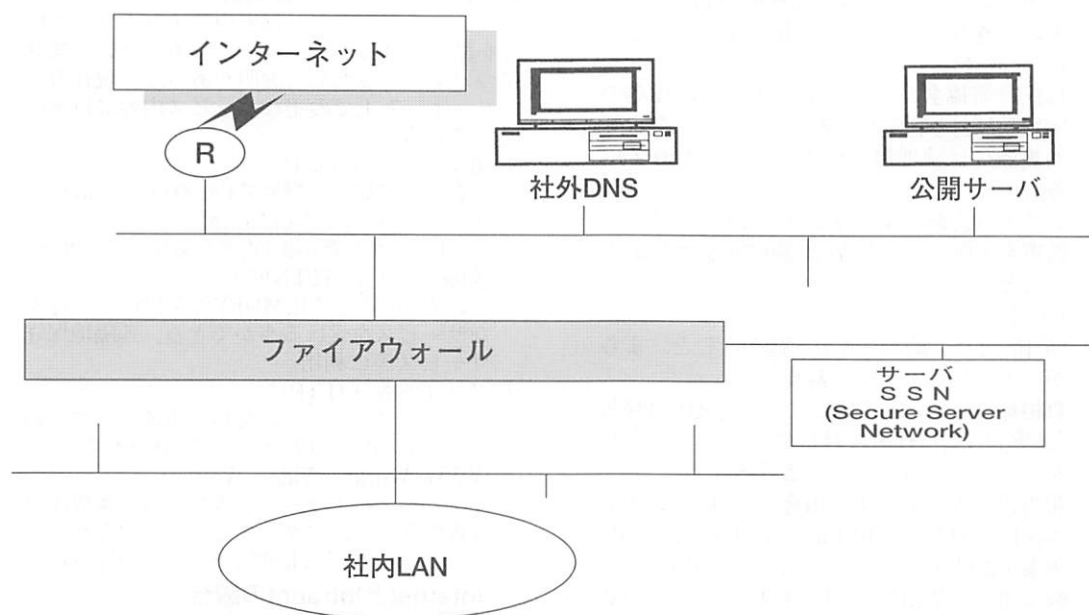
【メリット】

○ アプリケーションを変更しなくてよい。

【デメリット】

● ユーザがProxyの存在(設定情報)を知る必要がある。

最近のシステム構成例



5. 導入ステップは以下の通り。

- ① セキュリティ・ポリシーの検討
- ② 費用見積もり、体制作り
- ③ リスク分析(セキュリティ評価)
- ④ ファイアウォールの構築
- ⑤ 運用・保守
売れ筋製品の価格は、2～3M¥程度との事であった。

6. 製品紹介

- ① BorderWare、
- ② FireWall-1、
- ③ Gauntlet、
- ④ Sidewinder、
- ⑤ BlackHole等。

最近の傾向としてハイブリッド型製品(FireWall+OS)が、注目されている。

7. 関連技術(ツール)紹介

- ① S/KEY
- ② SATAN(検査ツール)
- ③ TIS Firewall ToolKit
- ④ TCP Wrapper(ログ取得機能)
- ⑤ Crack(パスワード安全性検査ツール)
- ⑥ PEM
- ⑦ PGP等

8. 情報源

- ① CERT
- ② メイリングリスト
- ③ USENETニュースグループ等の紹介があった。

9. Q & A

Q1. CALS(EC)とファイアウォールの関係について。

A1. 当然切り離す事はできないが、現在は電子決済に関心が向いている。

Q2. ファイアウォールは内部の不正者に対しても有効か。

A2. 全く無防備である。

《感想》

今回のテーマは、今最も関心の高いテーマの一つであるインターネットとイントラネットのセキュリティに関するものであった。現在各企業はセキュリティ面に配慮して、インターネットと社内システムを切り離しているケースが多い。しかし今後は総合化の方向にあり、ファイアウォールに無関心ではいられない状況にある。インターネットのようなグローバルでオープンなネットワークを前提にしたセキュリティの問題に関しては、これから本番を迎える。システム監査人としても関連知識の吸収のみならず、色々な面での総合力が要求される事になるとあらためて自覚致しました。

ISCA東京支部 月例研究会 感想文

テーマ：システム監査基準の改訂について

発表者：喜入 博氏 日本ユニシス(株)

日 時：平成8年4月19日(金)

場 所：東京ガス(株)本社

No.526 富山 伸夫

講演内容の概要

本年1月に改訂されたシステム監査基準について、その経緯、背景、改訂のポイントを、改訂委員会に入って担当してこられた喜入氏から、詳しく伺うことができた。

情報システム利用形態の変化、国際的なセキュリティや監査の動向、災害対策等の要請をふまえて、それら全てを洩れなく包括的にカバーする基準を目指して、検討してきた。今後はこれを基に解説書の出版や説明会をおこなって、普及活動を行ってゆくこととなる。

改訂の経緯

情報処理開発協会の中にシステム監査普及委員会があって、今まで隔年でシステム監査白書を出したり、「システム監査のイロハ」や「モデル監査規定」など出してきた。この間に各方面にアンケート等をお願いし、旧基準の問題点を出して頂いてきた。この委員会が母体となって平成6年9月に改訂委員会が発足した。

鳥居先生が主査となり、大学の先生が4人、監査企業から4人、一般企業から6人といった構成ですが、他に通産とJIPDECから複数人が常時参加していた。

ずっと検討を続けてきたが、通産省の施策と合わせるという事もあって、去年安全対策基準・ウイルス対策基準などが出され、少し遅らせてシステム監査基準を出す事になった。

改訂の特徴

構成面では全体的に変更したが、例のシステム取り引きのプロセス(SLCP)に準拠した形に

し、保守業務の独立、共通業務の洗い出しと基準化をおこなった。

内容面では、用語の定義や実施基準の考え方を新設するとともに、ネットワーク基準を充実し、他のいろいろな基準との連動を考慮した。その結果基準項目がかなり増えることになった。

改訂基準の目玉

企画業務の監査項目の中に、経営戦略と情報化計画の整合性、全体計画と開発計画の明確化を特に意識した。

また保守業務の構成を共通フレームと同期をとって整理し、開発と保守、運用と保守の区分の明確化をはかった。

また情報技術や形態の多様化にたいしては、どのような形であれ適用できるよう表現の工夫をこらした。細かいところは解説書で各項目の趣旨と留意点というかたちでまとめたが、実は解説書の部分に随分と時間がかかってしまった。

今後の予定

3月の東京説明会のあと、順次各地方の通産局毎に説明会をやってゆく。基準と解説書を合わせた本の形で出版されるのは、多分6月中旬頃となるでしょう。

なお、CAITのシステム監査技術者のテキストは、内容的に特に問題はないので、改訂はしない方針だと聞いている。

受講後の感想

前の監査基準が出てから10年の間に情報システムの環境がどんどん変わっているが、その間の様々な議論を踏まえての新しい基準の取りまとめは、随分大変だったことと思った。

この基準が出来たとしても、実際の監査の場で適用するには、もう一段掘り下げた細目基準なり、チェックリストなりがいるわけなので、それはわれわれ監査人協会の仕事なのかなと思う。

**システム監査学会
10周年記念研究大会の報告
システム監査実施における指摘と
解決策**

No.461 橋和 尚道

掲記の統一論題のもとに研究大会が、去る5月17日に開催された。いずれシステム監査学会の機関紙・誌に詳報されるが、筆者が司会進行を担当した第2分科会の模様を中心にその概要を報告する。

開会挨拶 学会会長 宮川 公男氏

情報資源の巨大化に伴いシステムのセキュリティ(負の面)と有効性(プラスの面)が問われる。システム監査学会もこの二つの側面を意識しながら、活動を進めたいと挨拶された。

基調講演 富士通(株)専務 秋草 直之氏
「情報技術とこれからの企業経営」

最初にネットワーク・マルチメディア・パソコンなど情報技術の展望をされた。TVのように家庭に浸透するパソコン、社会のインフラに成長したパソコン通信、進展する電子店舗、インターネット利用分野の広がりから、新しい商流—Electronic Commerce—を描かれた。

企業経営へのインパクトとして、情報化投資の日米比較で日本の遅れを指摘、富士通の業務革新の取り組みを、具体的に示された。それは間接部門業務のスリム化と営業部門業務の高付加価値化で、EDI、CALSへの取り組み等である。

第1分科会(統一論題)

「ネットワークセキュリティ基準と監査」

日本電気(株) 神田 昌彦氏

「最近の大規模システムの監査ポイント」

NTTソフトウェア(株) 小橋 喜嗣氏

「ダウンサイジングの目的と効果の監査」

郷商事(株) 山口 芳彌氏

この後以上の3氏をパネリスト、アンダーセンコンサルティングの藤本邦明氏をコーディネータとするパネルディスカッションが行われた。

第2分科会(自由論題)

〔研究報告1〕

システム構築プロジェクトの構造的統制

—要件統制と自己組織統制—

名古屋経済大学 中西 昌武氏

情報システムの構築を適切に統制することが求められている。プロジェクトの運営には、資源調達、目標設定、組織統括、潜在維持の4機能をもつ要件統制が必要であるが、それには限界があり、自らの品質を望ましい方向に誘導する規制力—自己組織統制も必要となる。また両統制の一体化が課題となる。また、内部統制には、自己防衛的側面と自己革新的側面があり、システム監査は、両者を対象とするときは信頼性、安全性に、後者のときは効率性、有効性、戦略性に力点が置かれるという考え方が注目される。内部統制について自己防衛的か、自己革新的かの経営者自身の動機が曖昧なときは、システム監査がその明確化を支援する。報告者は当協会の会員(中部支部)である。

〔研究報告2〕

システム監査と管理

—両者はいかに機能すべきか

(三菱商事の実践例)—

三菱商事(株) 松下 二郎氏

情報システムの信頼性、安全性、効率性をはかるため、システム監査を充実し、併せてシステム部門のシステム及び関連業務の内部統制を強化した実践事例である。システム監査は、監査部監査と自己監査を実施し、社内規定に「システム監査基準」を設けている。内部統制も、品質と生産性向上のための品質管理チームや、システムの有効性とプロジェクトの生産性確保のための規程・基準を整備運用している。更に全開発案件対象にシステムアセスメントを実施、システム監査はそれが有効に機能しているかを検証する。今後は更に有効性面にも注力し、経営に資するよう努力している。報告書は6月に当協会に入会された。ご活躍が期待される。

〔研究報告3〕

プロセス改善指向システム監査の提案

—現場からの新たな発想—

(株)SRA 三好 武重氏

システム監査の普及率が伸びない理由に「監査人の情報技術/業務知識の不足」、「監査を実施しなくても業務に支障はあまりない」や、「監査という言葉の抵抗感」をあげられる。そこで、プロセス重視のシステム評価手法の国際的な流れと、開発現場の実情を考慮して、システムとその開発プロセスの評価、改善の枠組みを提案される。これは、品質保証のISO9000シリーズとSLCPのISO12207を考慮し、現在ISOのSPICEプロジェクトで検討継続中のSoftware Process As-

assessment(プロセス評価・改善の国際標準案)を意識してシステム監査の枠組みとする。かつ、プロセス自体の改善を被監査部門の目標とし、各プロセスの中に評価項目を組み込む方式である。

システム監査学会のシンポジウム(予告)

システム監査学会では、創立10周年記念の公開シンポジウムを11月に開催する。その概要は次のとおりで、各研究会の研究成果の発表が大いに期待されている。

〔開催要領案〕

統一論題:「システム監査研究の課題と

21世紀への展望」(仮題)

期 間:96年11月13日(水)~14日(木)

場 所:港区芝公園3-5-8

機械振興会館ホール

会 費:会員 2000円/非会員 5000円

プログラム

基調講演:宮川 公男 システム監査学会会長
研究発表:各研究会の研究成果の発表

システム監査技術研究会、システム監査実践研究会、リスクマネジメント研究会、法的リスク研究会、情報セキュリティ研究会、アウトソーシング研究会、ダウンサイジング研究会、システム監査基準特別研究会、システムコスト研究会、近畿地区システム監査研究会、北海道地区システム監査研究会、中部地区システム監査研究会(順不同)

システム監査に関するアンケート結果

日本システム監査人協会 法人部会

法人部会で昨年12月に実施しましたシステム監査に関するアンケートの集計がまとまりましたので、ご報告致します。

最終的に59社の企業からご回答をいただきました。ご協力、誠にありがとうございました。誌面を借りてお礼を申し上げます。

システム監査を実施している企業が59社中16社(27%)という結果は、システム監査白書の調査結果とほぼ同じですが、法人部会としてはシステム監査の普及にもっと私たちの努力が必要であることを感じました。とともに、情報システムの安全性、信頼性および効率性がいかに大切であり、それには妥当な費用をかける必要があることについての啓蒙活動を協力に推し進めていかなければならないと痛感しました。

今回のアンケート結果を、今後のシステム監査の普及に役立てていきたいと思ひます。

1. アンケート概要

1.1 アンケートの目的

ユーザ企業(システム監査を依頼する側の企業)に対して、システム監査の実施状況、システム監査に対して期待することなどを調査し、システム監査の啓蒙・普及、システム監査のニーズ発掘に結び付ける。

1.2 アンケートの回収状況

アンケート出状総数 289

回収総数 59(回収率:20.4%)

2. 回答企業のプロフィール

2.1 業種

・ 情報処理・情報サービス	16社
・ ソフトウェア関連製造業	8社
・ その他のサービス業	4社
・ コンピュータ関連販売業	2社
・ コンピュータ関連製造業	1社
・ 官公庁	1社
・ その他の製造業	11社
・ 金融業	8社
・ 建設業	2社
・ 教育・研究機関	2社
・ 商社・卸・小売業	1社
・ その他	3社

(注) その他の製造業は、コンピュータ関連製造業、ソフトウェア関連製造業以外の製造業、その他のサービス業は、情報処理・情報サービス業、運輸・公共サービス業以外のサービス業である。

2.2 所在地

・ 東京都	22社
・ 近畿地区	5社
・ 東北地区	3社
・ 大阪府	10社
・ 九州地区	5社
・ 関東地区	2社
・ 中部地区	8社
・ 愛知県	3社
・ その他	1社

2.3 従業員数

・ 100人以下	8社
・ 101人以上~500人以下	18社
・ 501人以上~1000人以下	10社
・ 1001人以上~5000人以下	15社
・ 5001以上	8社

- 5001人以上と回答した大規模企業(8社)の業種別内訳は、金融業が4社、コンピュータ関連製造業、その他の製造業、建設業、その他が1社ずつであった。

2.4 メインのシステム構成

- ・ 汎用機中心の集中型システム 31社
- ・ 汎用機中心の分散型システム 8社
- ・ クライアントサーバシステム 12社
- ・ ネットワークシステム 1社
- ・ その他 4社

- 回答した企業においては、汎用機中心のシステム(集中型および分散型)を使用している企業が多い(39社)結果となった。近年注目されているクライアントサーバシステムをメインで使用していると回答した企業(12社)の業種別内訳は、ソフトウェア関連製造業が4社、情報処理サービス業が3社、その他サービス業が2社、コンピュータ関連販売業、建設業、その他がそれぞれ1社であった。

3. システム監査の実施状況

- ・ 実施していない 43社
- ・ 実施している 16社(実施率:27%)

- 実施していると回答した企業(16社)の業種別内訳

業 種	全体企業数	実施企業数	実施率
金融業	8	6	75%
情報処理・情報サービス業	16	5	31%
その他の製造業	11	4	36%
その他	3	1	33%

- 実施していると回答した企業の地域別内訳

地 域	全体企業数	実施企業数	実施率
東京都	22	6	27%
近畿地区	5	4	80%
大阪府	10	3	30%
中部地区	8	2	25%
愛知県	3	1	33%

- 実施していると回答した企業の従業員数別内訳(規模)

従業員数	全体企業数	実施企業数	実施率
101人～500人	18	4	22%
1001人～5000人	15	7	47%
5001人以上	8	5	63%

- システム監査白書の調査結果では、システム監査を実施している企業は全体の約28%であり、今回の調査結果での27%もそれに近い結果となった。

- システム監査を実施している企業は大都市圏に集中しており、企業規模が大きくなるほど、実施率が高くなっており、100人以下の小規模な企業では1社も実施していない結果であった。また業種で見てもかなり偏りがあり、金融業では75%の企業が実施している結果となった。

4. システム監査を実施していない企業に対する調査

4.1 実施していない理由

- ・ 実施したいが、内部に実施するための組織がない、または実施するための人材(システム監査人)がいない。 16社
- ・ 実施したいが、経営上層部の理解が得られない。 3社
- ・ 実施したいが、実施するための予算がない。 2社
- ・ 実施を外部に委託したいが、適当な委託先が見つからない。 1社
- ・ システム監査を実施する必要性を感じない。 11社
- ・ システム監査の具体的な内容を知らない。 2社
- ・ その他 5社
- ・ 回答なし 3社

- 実施するための組織、人材がないと回答した企業(16社)の業種別内訳

- ・ 情報処理・情報サービス業: 6社
- ・ その他の製造業: 3社
- ・ 教育・研究機関: 2社
- ・ ソフトウェア関連製造業: 1社
- ・ コンピュータ関連販売業: 1社
- ・ 金融業: 1社
- ・ 建設業: 1社
- ・ その他のサービス業: 1社

- 実施するための組織、人材がないと回答した企業の従業員数別内訳

- ・ 100人以下: 1社
- ・ 101人～500人: 5社
- ・ 501人～1000人: 4社
- ・ 1001人～5000人: 5社
- ・ 5001人以上: 1社

- 実施の必要性を感じないと回答した企業(11社)の業種別内訳

- ・ ソフトウェア関連製造業: 5社
- ・ 情報処理・情報サービス業: 2社
- ・ その他の製造業: 1社

- ・建設業： 1社
- ・その他のサービス業： 1社
- ・その他： 1社
- 実施の必要性を感じないと回答した企業の従業員数別内訳

- ・100人以下： 5社
- ・101人～500人： 3社
- ・501人～1000人： 1社
- ・1001人～5000人： 1社
- ・5001人以上： 1社

- システム監査白書の調査結果では、システム監査を実施していない理由の第1位は「システム監査の実施よりもシステム化推進そのものに力点がある」であり、今回の調査で実施していない企業の業種として情報処理・情報サービス業が多いことから、システム監査白書の結果と同様に、システム監査よりもシステム開発にウェイトを置いている(置かざるを得ない)状況と言える。
- システム監査を実施する必要性を感じない、システム監査の実施を外部に委託したいが適当な委託先が見つからない、という回答に対しては、システム監査実施企業の啓蒙・普及活動、より一層の営業努力が必要である。

4.2 今後に対する考え

- ・実施する計画がある 4社
- ・実施を検討したい 22社
- ・今後とも実施する考えはない 7社
- ・その他 6社
- ・回答なし 4社

- システム監査を実施していない企業でも、今後前向きに実施する意向があるとしている企業(26社)が、今後とも実施する考えがないとする企業(7社)を大幅に上回っており、システム監査に対する関心、期待、ニーズはあると言える。

5. システム監査を実施している企業に対する調査

5.1 システム監査の実施時期

- ・半年ごとに定期的に実施 2社
- ・1年ごとに定期的に実施 6社
- ・2年ごとに定期的に実施 2社
- ・2年以上のサイクルで定期的に実施 3社
- ・不定期に実施 3社

5.2 システム監査のための年間予算(人件費を含めて)

- ・百万円以下 8社
- ・百万円以上～5百万円以下 0社
- ・5百万円～1千万円以下 2社
- ・1千万円以上～5千万円以下 3社
- ・5千万円以上～1億円以下 3社

5.3 システム監査の実施体制

- ・社内のシステム監査人のみで実施 12社
内部システム監査人の人数 平均3.5人
- ・外部のシステム監査企業に一部委託 1社
内部システム監査人の人数 平均2.0人
- ・外部のシステム監査企業に全面的に委託 1社
- ・回答なし 2社

- 実施していると回答した企業では、内部監査の一部としてシステム監査を行っているケースがほとんどという結果であった。
内部システム監査人の人数は、12人(大手銀行)、11人(大手情報処理企業)を除いてはすべて1～3人であった。
- システム監査を実施している企業でも、システム監査を外部委託している企業は少なく、システム監査企業の認知度が低い。システム監査企業のより一層の営業努力が必要である。

5.4 システム監査を実施した結果

- ・非常に満足 1社
- ・満足 11社
- ・不満 1社
- ・未評価 2社
- ・回答なし 1社

- システム監査を実施した企業では、実施した結果に対する満足度は非常に高く、実施すれば効果があるということを物語っている。
不満と回答した企業での理由は、被監査部門の協力が得られないためにシステム監査がスムーズに実施できず、満足な結果が得られなかったということであった。

5.5 外部のシステム監査企業に委託した企業に対する調査

5.5.1 委託したシステム監査の内容(複数回答)

- ・情報システムの安全性確保 1社
- ・情報システムの信頼性向上 2社
- ・情報システムの効率性向上 1社
- ・情報戦略の策定/見直しの支援 1社

5.5.2 委託したシステム監査1回当たりの実施期間

- ・ 1週間以内 1社
- ・ 2カ月以上 1社

5.5.3 委託したシステム監査1回当たりの費用

- ・ 百万円以下 2社

5.5.4 外部のシステム監査企業に委託した理由

- ・ 内部のシステム監査人の育成への期待 1社
- ・ その他 1社

6. 今後のシステム監査への期待

6.1 システム監査によって解決することを期待する課題(複数回答)

- ・ 情報システムの安全性確保 19社
- ・ 情報システムの信頼性向上 23社
- ・ 情報システムの効率性向上 29社
- ・ 情報戦略の策定/見直しの支援 13社
- ・ その他 2社

- 従来、システム監査を実施する目的としては安全性確保、信頼性向上の占める割合が高かった。しかし、今回の調査結果では情報システムの開発・運用コストの削減や費用対効果の増大を目指す効率性(有効性、経済性とも言える)が多くの割合を占め、情報戦略の策定/見直し支援というコンサルティングに近い分野にもその期待が寄せられていることが大きな特徴となった。

6.2 システム監査が効果を発揮することを期待する分野

6.2.1 システム構成(複数回答)

- ・ クライアントサーバシステム 34社
- ・ ネットワークシステム 21社
- ・ 汎用機中心の集中型システム 12社
- ・ 汎用機中心の分散型システム 12社

- クライアントサーバシステムやネットワークシステムに対する期待が大きく、情報化環境の新しい流れを反映した結果となった。

6.2.1 システムライフサイクルについて(複数回答)

- ・ 企画段階 27社
- ・ 開発段階 21社
- ・ 運用段階 25社

- 情報システムの複雑化、多様化に伴い、システムライフサイクルの上流工程でシステム監査を実施し、さまざまなニーズを正しく反映した情報システムを企画し、開発の手戻りをなくすことへの期待感が見られる。

6.3 システム監査の実施体制

- ・ 内部で組織を作り、システム監査人を育てて実施 33社
- ・ 内部システム監査とともに、外部のシステム監査企業にも委託 17社
- ・ すべてを外部のシステム監査企業に委託 2社
- ・ どのようにしたら良いか不明 2社
- ・ その他 3社
- ・ 回答なし 2社

- 一部を外部監査企業に委託すると回答した企業(17社)の業種別内訳は、その他の製造業が6社、ソフトウェア関連製造業が2社、情報処理・情報サービス業2社、金融業が2社、建設業が2社、それ以外は1社ずつであった。

また、すべてを外部監査企業に委託すると回答した企業(2社)の業種は、その他の製造業とその他のサービス業であった。

6.4 システム監査を外部委託する場合に考慮すること

- ・ 会社の方針、ニーズに合っているか 32社
- ・ 費用が妥当か 13社
- ・ 委託先のシステム監査企業の実績 9社
- ・ その他 1社
- ・ 回答なし 4社

6.5 システム監査を外部に委託する場合の、1回のシステム監査実施における費用

- ・ 百万円以下 19社
- ・ 百万円以上～3百万円以下 22社
- ・ 3百万円以上～5百万円以下 7社
- ・ 5百万円以上～1千万円以下 1社

- 1回のシステム監査を外部委託する場合の費用としては、3百万円までと考えている企業が大多数という結果であった。百万円以下と回答した企業が19社もあつが、百万円以下では実のあるシステム監査の実施は困難であり、システム監査企業としては、妥当な費用負担が必要であることの啓蒙・普及が必要である。

7. システム監査を実施する上で必要と考 えるもの

- ・ 通産省 システム監査基準 49社
- ・ 通産省 情報システム安全対策基準 37社
- ・ 通産省 コンピュータウイルス対策基準 20社
- ・ FISC 金融機関等のシステム監査指針 9社
- ・ 公認会計士協会 内部統制質問書 7社
- ・ 情報処理サービス業電子計算機システム
安全対策実施事業所認定制度 7社
- ・ 通産省 システム監査企業台帳 4社
- ・ 特定システムオペレーション企業等認定制度 3社

8. その他の意見

回答企業から寄せられたシステム監査について
の意見の中に、システム監査の制度化を望む
声が多くあった。今回のアンケート調査の対象
が情報システム担当管理者ということで、シス
テム監査を実施したいが、どうしてもシステム
開発業務などが優先されてしまうという悩みが
現れた意見と言える。

- 通産省はシステム監査の普及のためにいろ
いろな施策を講じており、今後、その効果が現
れることを期待するとともに、日本システム
監査人協会としても、それに対応した活動
を行っていく必要がある。

近畿会活動報告

「片山津温泉で合宿研修会開催」

No.299 安本 哲之助



近畿会の合宿スナップ

かねてから計画の北陸分会との合同研究会は
阪神・淡路大震災のため延期となっていました
が、ようやく実現でき、3月1日(金)から2日
(土)に1泊で合宿研修が実現しました。

何分、超多忙な会員ばかりであり当日の業務
終了後出発のスケジュールで石川県片山津温泉
「加賀観光ホテル」に勇躍駆けつけ、夜8時から
の宴会開始となりました。東京からは橘和会
長、中尾事務局長と中部支部代表の西脇さん
にもご参加いただけ総員17名が夜のふけるまで本
音で議論をいたしました。翌日はまじめにも早
朝から「新システム監査基準の目指すもの」の
テーマで研究会をはじめ、解散時よくもまじめ
にお互いやったなど成果を振り返りつつ帰路に
つきました。なお、本会開催にあたりまして地
元の川端さん、諏訪さんには大変お世話になり
ました。中部の西脇さんからは「先日は楽しいひ
とときをありがとうございました。中部も刺激
されて火を消す事なく勉強をしていく事にしま
す。こちらは実監査をターゲットにして活動し
ております。今までに2企業実施し、今年度は
2つの予定です。」と声を寄せていただいており
ます。お互いのレベルアップのためにこのよう
な機会がもうけられたらと思います。

また、この研究会を機に会員の意見交換をよ
り積極的に行い、論議する場として喜多さん
のお骨折りでニフティに近畿会のホームパ
ーティを開設いたしました。これからはこれをつ
かって会員の連絡を密にし、出来れば定例研
究会の出欠確認をここですることで、手間・コ
ストの削減を目指したいと考えております。

すべては紙面の都合でできませんが合宿で
の声を一部紹介します。

Kさん 「現状はただでさえ進んでいないシス
テム監査への取組ぶりで、急激に進むオー
プンシステム化のなかで改訂はシステム監査普
及のチャンスであるはずである。」

Yさん 「基準の改訂を期待していたが、まだ
未解決の課題が多いようだ。肉付けは我々が
する方向でとりくまねばならない。」

Kさん 「月例研究会は基本的には一方通行な
わけですが、合宿では皆さんの本音の議論が聞
けたように思います。そういう意味であの合宿
は私にとって新鮮でした。開発の立場・コンサル
タントの立場・監査の立場それぞれの本音の
意見が聞けたように思います。そういう意味で
合宿は毎年1回やりたいですね。」

Oさん 「基準の文言が、「～は適切か」という
表現から、「～は行われているか」という表現に
変わったことについて、内容のチェックから、
形式的なチェックに変わってしまったというこ
とで、かなりの議論がありました。この基準は、
内部監査を想定しているとのこと。だとすれ

ば、今回の表現の変更は、それなりに適切ではないか。今回の表現の変更は、主観的なチェックから客観的なチェックに変わったということだと考えられるからです。」

Nさん 「内部監査としてのシステム監査はあくまでもその内容にまで入ったチェックをするべきだ。」

Yさん 「そのためには外部監査の場合永いクライアントとの付き合いの中で、その置かれた状況を熟知した上で適切な助言をする必要があるし、そうであればビジネスとして成り立つことも考えられる。」

Kさん 「実際に監査部門でシステム監査をしておられる方々はそうはいかない。実際にシステム監査をやっておられる方々の意見を是非お聞きしたい。」

等々でした。

新しい基準をベースに、そういった議論ができればと思います。

皆さん こんにちは 中部支部です。

No.124 中部支部 原 善一郎

今年度が始まってすでに半年が過ぎました。中部支部も例年通り活動をしています。1月、3月、5月と例会を行いました。例会では、ゼミ形式で会員が持ち寄ったテーマについて話し合っています。そして、ついに恒例になってしまった懇親会も継続しています。

さて、今年はぜひ実際にシステム監査を独力でやってみたいとの希望で意気こんでいますが、なかなか不慣れなこととて、スタートしません。去年の長野合宿の成果をフィールドで示そうとしているのですが…。

事例研究会のご指導で進めようとしています。もちろん、報告書を出すときは「日本システム監査人協会」と言う名称で出すのですから、理事会の承認も必要です。

現在、2社が希望を出されていて、少しずつ進んでいます。そのための監査計画の話し合いを5月の例会として行いました。もちろん、例会への参加者は「守秘義務」を負います。そして、少なくとも中部支部の中では「サポートチーム」には入って頂きます。従って、中部支部の例会は当分の間は「実査検討会」になってしまいますので、フリーの方は入れないことになってしまいます。(また、中部支部通信もつまらないものになります。例会の議事録もマル秘扱い

です。パソコン通信部会のパティオへも大まかな概略しかアップできません。)

この実査の中では電子メールを利用します。ある会社の実査で使ってみて、その威力を実感したからです。支部通信も電子メールのみにさせて頂こうと思っています。爆発的に電子メールを使える方が多くなってきました。この現象は「革命的」だと思います。それはちょうど「ファクシミリ」の普及期のような現象だと思います。

このように技術進歩は加速度的に進んできました。そして、私たちが取り扱うべき「対象システムなど」は従来のホストシステムから、大衆化したコンピュータ、大衆化したネットワークも入ってきているのではないのでしょうか。今どきのパソコンはカタログスペックでは10年前のメインフレームです。そして、フロッピーだけで扱っていた時代と違って、ソフトの複雑さも10年前のメインフレームを思い起こさせる程の規模になっています。「10年前のシステム監査」ではなく「現在・未来のシステム監査」を考えると、きが来たようです。

中部支部の状況は折に触れて、ニフティサーブにあるパソコン通信部会(パティオで構成)にアップして行きます。皆さんも入って下さい。また、中部支部へのご希望は電子メールにてお願いします。

パソコン通信部会は ニフティ:MHE02226
蓮見理事へ電子メールを下さい。

中部支部へは ニフティ:PXP12756 原 善一郎へ電子メールを下さい。

「中国支部」だより

No.387 中国支部 安原 節男

平成8年も、前半が過ぎようとしています。が、支部活動の方は、やはり遅れがち。

今年の話・活動として、

① 会員異動等。この度、井口光浩さんが入会され、支部構成員が1名増となり大変喜ばしいことです。また、従来からの会員の方で、鳥取から広島市内への異動がありました。

② 公開研修会の実施。今年に入って、研修会を公開形式で実施。

* 広島県情報産業協会殿との共催

テーマ「クライアント／サーバシステムとシステム監査」

* 一般への公開形

テーマ「INSネット64の利活用」

その他、昨年度の活動状況(会報No.37)でもご紹介しましたとおり、当支部では、会員の広域分散の問題がありますが、岡山・松江でも研修会を実施すべく計画中です。

- ③ 定例研修会の実施。今年から、偶数月の第二(または第三)水曜日に研修会を実施することとしており、第1回を4/17日に実施、次回は6/19を計画しています。
などがあります。

今年は、このほか、中国通産局・機械情報産業課殿と連携した活動も、是非実現させたいと考えております。

九州支部活動状況(1月～4月)

No.307 行武 郁博

九州支部の活動の中心は毎月の例会です。会員のシステム監査関連事項の研究、報告や情報交換等を行なっています。以下主な事項について述べます。

1月

1. 活動方針の決定

九州支部95年度収支計算書および96年度予算案の提示が赤塚氏より提示があり承認した。九州支部の96年度活動は、毎月の例会の開催と例会での研究成果の取りまとめを行うこととした。

2. 「ソフトウェア管理者養成講座」(主催JPSA)受講報告(秀嶋氏)

秀嶋氏より講座内容、使用テキストの紹介があった。

3. 「ソフトウェア管理ガイドライン」について(行武)

平成7年11月15日付通産省公報で公表された。内容をみると、ここでいう「ソフトウェア」はパソコンで稼働しているパッケージソフトウェアという限定されたソフトウェアである。また「ソフトウェア監査」という新語が登場しておりシステム監査とは異なるものだと説明されているが、内容と用語の隔たりが大きすぎるので概念上、無用の混乱が起これると思われる。当初から内容に合った用語を使用すべきであろう。

2月

1. 第9回日本システム監査人協会通常総会出席報告(行武)

2月16日に開催された日本システム監査人協会の総会に出席したのでその内容につき報告を行った。

2. 「デジタルキャッシュについて」(行武)

総会で行われた特別講演「デジタルキャッシュ」(セキュリティの応用技術)―大田和夫氏一の内容について説明した。

3月

1. 例会の研究成果のとりまとめについて

例会での発表原稿を各人がフロッピーに記録して鶴岡氏へ提出し、鶴岡氏がとりまとめることとなった。

4月

1. 「情報システムアウトソーシングとシステム監査」守田氏

表記の論文を守田氏が学会誌に発表されたので例会で説明していただいた。

アウトソーシングされたシステムについてはユーザ企業のシステム監査人は通常のシステム監査ができないとされる。したがって、ユーザ企業については委託に関連する監査として、監査項目を設定しておこなうこととなる。一方、ベンダー(アウトソーシング事業者)のシステム監査はベンダーのシステム監査人が行うこととなる。この両者のシステム監査のポイントについて説明があった。

また、アウトソーシング発生の経緯、定義(特に外注との相違点)、実例の紹介がありアウトソーシングについてまとめた勉強をすることが出来た。

今まで例会のレギュラーメンバーとして活躍していただいた木下氏の突然の転勤は大きなショックであった。現在では、毎月4～5名の出席者となってしまったが今後とも頑張って例会を続けてゆく所存です。

「ソフトウェア管理ガイドライン」についての疑問

No.307 行武 郁博

平成7年11月14日付で通産省は「ソフトウェア管理ガイドライン」を発表した。その主旨にも明記されているようにソフトウェアの違法複製等を防止するために設けられたガイドラインであり、ここで用いられている「ソフトウェア」とは、「パーソナルコンピュータで稼働し一般に市販流通しているシステムプログラム、アプリケーションプログラム、ユーティリティ等のパッケージソフトウェアをいう」と定義されている。一般的な意味でのソフトウェアとは違い、限定されたソフトウェアである。そうであれば、なぜ「パソコンパッケージソフトウェア」といったソフトウェアを限定した意味の用語とならなかったのか、疑問を持ったのである。

また、ソフトウェアの使用状況についての監査として「ソフトウェア監査」が規定されている。これは、解説書によると、システム監査でのソフトウェアの監査とは異なりソフトウェアの監査者もシステム監査人ではない。システム監査とは別の次元の問題として認識されているようである。（「コンピュータウイルス対策基準」ではシステム監査が規定されている。）

ところで平成8年1月30日付で「システム監査基準」が改訂公表された。実施基準・運用管理として「ソフトウェア管理」が設定されている。ここでは、前記「ソフトウェア管理ガイドライン」と類似する項目も規定されている。留意事項では、（ソフトウェアの利用状況の監査については、「ソフトウェア管理ガイドラインを活用すること」と記述されている。）

システム監査基準では「ソフトウェア」の定義はない。勿論、一般的な意味での「ソフトウェア」であろうが、前記の限定された意味でのソフトウェアも使用されていることとなる。

このように内容の異なる「ソフトウェア」、「ソフトウェア管理」や「ソフトウェア監査」が存在している。混乱をさけるためにも、内容を適切に表した用語とすべきである。また、今後、用語を含めて各種基準、ガイドライン相互の調整と統一を図るべきであると思う。

当協会所有図書貸出手続きのご案内

担当理事 馬場要輔

当協会でも所有（購入、受贈）している図書（参考図書、ビデオ、資料等）の貸出手続きについてご紹介致しますのでご利用下さい。

(1) 基本事項

- ① 貸出は当協会会員（含む法人会員、準会員）に限定します。（グループ使用も可）
- ② 会員と事務局との連絡は、所定の書式によるFAX通信で行って頂きます。
（事務局の負担を軽減するため電話による申込はご遠慮下さい）
- ③ 貸出期間は2週間以内とします。場合により継続貸出もできることとします。
- ④ 図書の送付（貸出・返却）は宅急便または郵便を使用し、送料は会員の負担とします。

(2) 借出手続

1) 借 出

- ① 借出希望者は、添付の「図書借出・継続借出申込書」をA4版に拡大コピーの上、所定事項を記入し事務局にFAXで申し込んで下さい。
（注）図書の特定は「図書番号」によることとします。（万一「図書番号」と「図書名」が符号しない場合は、「図書番号」のものが指定されたものとして扱います。類似する図書名が多いので、ご注意ください）
- ② 事務局では、借出希望の図書が手元にある場合、「料金受取人払い」の宅急便または郵便により借出希望者に送付します。
- ③ 事務局は、借出希望の図書を他の会員に貸出中の場合や、所蔵していない等の理由で貸出ができない場合は「図書貸出不能連絡書」によりその旨借出希望者にFAXで連絡します。

2) 継続借出

- ① 借出者が借出期間終了前に、「図書借出・継続借出申込書」を事務局宛FAXで提出した場合、他に借出希望者がいない場合に限り、更に2週間以内の借出期間の延長ができます。
- ② 事務局は、他に借出希望者がいる時は、「図書貸出不能連絡書」により、借出希望者に継続借出できないことを連絡します。

3) 保管・管理

- ① 「図書」を借出した会員は、返却まで、善管注意義務を負って頂きます。
- ② 紛失、汚損
貸出した「図書」が、万一、紛失、汚損された場合には、事情により、再購入価格を限度に、費用の負担をして頂きます。

4) 返却

- ① 借出者は使用後（借出期間内）、速やかに、借出図書を「料金差出人払い」の宅急便または郵便で事務局に返却して下さい。

(F A X 5 3 5 0 - 9 2 6 9)

19

所有図書一覧表

8.5.28現在

図書番号	図 書 名	発行者名・出版社名
KS001	システム監査白書(93-94)	JIPDEC、システム監査学会・(株)コンピュータ・エージ社
KS002	情報システム監査に関する一般基準 及び情報システム監査基準書	ISACA
KS003	情報システムの内部統制質問書	日本公認会計士協会
KS004	情報システムの内部統制	日本公認会計士協会・第一法規出版
KS005	システム監査技術者育成カリキュラム	JIPDEC・中央情報教育研究所
KS006	同 標準テキスト(上)	JIPDEC・中央情報教育研究所
KS007	同 標準テキスト(下)	JIPDEC・中央情報教育研究所
KS008	システム監査技術者受験研究[上](基礎編)	(株)技術評論社
KS009	システム監査技術者受験研究[下](基礎編)	(株)技術評論社
KS010	情報システムの監査とコントロール (SACレポート)	日本内部監査協会・日経BP社
KS011	金融機関等のシステム監査実践例集(I)	金融情報システムセンター
KS012	金融機関等のシステム監査実践例集(II)	金融情報システムセンター
KS013	システム監査企業台帳に関する規則	通産省
KS014	システム監査白書(95-96)	JIPDEC、システム監査学会・(株)コンピュータ・エージ社
KS015	SACレポート(英文) 第1分冊(Executive Summary)	IIA(米国内部監査人協会)
KS016	同 第2分冊(Audit & Control Environment)	同上
KS017	同 第3分冊(Using IT in Auditing)	同上
KS018	同 第4分冊(Managing Computer Resources)	同上
KS019	同 第5分冊(Managing Information & Developing Systems)	同上
KS020	同 第6分冊(Business systems)	同上
KS021	同 第7分冊(End-user & Departmental Computing)	同上
KS022	同 第8分冊(Telecommunications)	同上
KS023	同 第9分冊(Security)	同上
KS024	同 第10分冊(Contingency Planning)	同上
KS025	同 第11分冊(Emerging Technologies)	同上
KS026	同 第12分冊(Master Index)	同上
KS027	同 第13分冊(Advanced Technology)	同上
KS028	同 別冊(C/S Implementation)	同上
KS029	金融機関等コンピュータシステムの 安全対策基準解説書	金融情報システムセンター
KS030	金融機関等のシステム監査指針	金融情報システムセンター
KS031	コンピュータウイルス対策基準解説書	通産省機械情報産業局・JIPDEC
SC001	ハッカーズ大辞典	Eric S.Raymond編。アスキー出版局
SD001	データベース白書1955	(財)データベース振興センター編
SK001	金融機関におけるコンティンジェンシー プラン策定のための手引書	金融情報システムセンター
SK002	コンティンジェンシーマニュアル(翻訳版)	金融情報システムセンター
SK003	コンピュータとオフィス防災マニュアル	工業調査会
SK004	防災・震災管理ハンドブック	産労総合研究所編 経営書院
SK005	企業と自治体のための総合地震対策指針	FEMA(Federal Emergency Management Agency : 米国連邦緊急事態管理庁)住友海上リスク総合研究所監訳)
SK006	日本列島・地震アトラス 活断層	イミダス特別編集 集英社
SK007	実践 企業危機管理読本	東京海上火災保険(株)安全技術サービス部 プレジデント社
SK008	金融機関等におけるコンティンジェンシー プラン策定要綱	金融情報システムセンター
SK009	金融情報システム(増刊35号) ー阪神・淡路大震災における個別金融機関等 の対応状況調査	金融情報システムセンター
SN001	通信サービス利用ガイドブック	日経コミュニケーション別冊・日経BP社
SS001	システム開発取引の共通フレーム(1994年版)	通産資料調査会
SS002	ソフトウェアの品質保証 ISO9300-3 対訳と解説	(財)日本規格協会

所有ビデオ一覧表

8.5.28現在

図書番号	タイトル	作成者・発売元
VS005	第5回総会ビデオ(2本:含む分科会報告)	平成4年2月開催
VS006	第6回総会ビデオ	平成5年2月開催
VS008	第8回総会ビデオ	平成7年2月開催
VS009	第9回総会ビデオ	平成8年2月開催
VT037	「ネットワーク構築の考慮点について」	第37回 月例会ビデオ 平成7年1月開催
VT038	「コンピュータのバックアップについて」	第38回 月例会ビデオ 平成7年4月開催
VT039	新開発手法「クリーンルーム」について	第39回 月例会ビデオ 平成7年5月開催
VT040	新開発手法Mai Dvo Clu につて	第40回 月例会ビデオ 平成7年6月開催
VT041	「PL法とソフトウェア」について	第41回 月例会ビデオ 平成7年7月開催
VT042	Unicode その光と影	第42回 月例会ビデオ 平成7年10月開催
VT043	CALSの概要と情報システムに与える影響	第43回 月例会ビデオ 平成7年12月開催
VT044	ファイアウォールとインターネットセキュリティ	第44回 月例会ビデオ 平成8年3月開催
VK015	「システム監査計画の立案と効果を補足する 施策の実施について」	第15回 近畿月例会ビデオ 平成2年7月開催
VK016	「システム監査の実施手順とサポートシステム」	第16回 近畿月例会ビデオ 平成2年9月開催
VK017	「コンサルタントから見たシステム監査」	第17回 近畿月例会ビデオ 平成2年9月開催
VK018	「銀行業におけるシステム監査」	第18回 近畿月例会ビデオ 平成3年1月開催
VK019	「アメリカ大手企業のシステム監査の 最新状況について」	第19回 近畿月例会ビデオ 平成3年3月開催
VK020	「システム開発・保守における効率性の 意識について」	第20回 近畿月例会ビデオ 平成3年5月開催
VK021	「経営者のためのシステム監査」	第21回 近畿月例会ビデオ 平成3年7月開催
VK022	「KPMGにおけるEDPコントロールに 関する考え方」	第22回 近畿月例会ビデオ 平成3年9月開催
VK024	「当社(関西日本電気ソフトウェア、株)に おけるシステム監査への取組について」	第24回 近畿月例会ビデオ 平成4年1月開催
VZ001	「システム監査企業登録台帳制度」	平成4年2月 第5回総会特別講演
VZ002	「模擬監査事例についてのディスカッション」	平成5年2月 第6回総会行事
VZ003	「クライアントサーバーシステムとシステム監査」	平成7年2月 第8回総会特別講演
VZ004	「映像記録 阪神大震災」	平成7年1月 毎日放送

創立10周年記念行事開催

来年は、当協会が発足して10周年にあたりますので、下記のとおり、設立10周年記念行事を行います。会員各位のご参加をお願い致します。なお、かつこ書内は、実施主体です。

記

1. 設立10周年記念論文の募集(論文審査委員会)
2. 設立10周年記念号会報の発行
3. 新システム監査基準のチェックシートの出版(システム監査基準プロジェクト)
4. 情報システムの地震対策の研究(セキュリティ分科会)
5. ロールプレイによるシステム監査体験合宿(監査事例研究会)
6. SI/SO登録制度におけるシステム監査の実態調査(法人部会)

設立10周年記念論文の募集のお知らせ

当協会の設立10周年にあたり下記の要領で、記念論文を募集致します。また、今回は当協会発足に尽力されました初代副会長故石上氏にちなみ石上賞を設けました。
会員各位のふるってのご参加をお願い致します。

記

1. テーマ
①システム監査の普及策について

- ②システム監査の有効性について
- ③システム監査の経済性について
2. 執筆の様式および量
35文字/行 30行/頁 最大8頁以内
3. 締切
10月末日事務局必着のこと
4. 参加資格等
会員に限らずシステム監査に関心のある者。共同執筆も可。(詳細は荒川副会長まで)
5. 発表等
年次総会において発表する。
6. 賞金
石上賞 10万円(最優秀賞に併与する)
最優秀賞 10万円 1名
優秀賞 10万円 1名
佳作 5万円 2名
なお、該当論文がない場合は、欠賞とすることがある。
7. 石上賞
故石上氏(当時富士通(株))は、当会の発起人の1人でありましたが、設立直前に急死されました。当協会は、石上氏を初代副会長に選任し1年間副会長を空席とすることでそのご尽力に感謝の意を表明しました。
ご遺族より10万円を当会発展のためとお申し出がありましたので、今回特に石上賞を設けることと致しました。

「インターネット上に協会の ホームページを開設」

日本システム監査人協会では、インターネット上に協会のホームページを開設することになりました。協会の主要目的の一つであるシステム監査の啓蒙と普及を目指した活動の一環です。

ホームページの構成は、5部編成として次のように考えています。

- 第1部 日本システム監査人協会の案内、システム監査に関するニュース、お知らせ等
- 第2部 システム監査に関するトピックスや論文など
- 第3部 監査受託企業紹介(法人会員案内)
- 第4部 システム監査受験対策情報
- 第5部 読者(視聴者?)とやりとり、ご意見、Q&Aなど

ここに載せる情報はすべて会員からのものです。是非とも、積極的に情報をお寄せ下さい。

ホームページで発進する情報はHP編集委員が常時受け付けています。Nifty Surve上の協会の会員向けPATIOに書き込んで下さい。あるいは、担当理事の蓮見あてご連絡下さい。(Nifty ID MHE02226)

第4部のシステム監査受験対策情報は、これからシステム監査試験を受けようという人に試験に合格するノウハウを教えようというものです。そして合格したら協会の会員になってもらおうというものです。最近合格したばかりの方は合格体験記や合格のノウハウをお寄せ下さい。

また理事会では、記事を集めて、編集し、ホームページに載せる作業を行うHP編集委員を募集しています。条件はインターネット及びNiftyにアクセスができる環境を持っている方です。

ホームページは現在編集委員の手によって準備中です。うまくいけば、この記事が読者に届くころには出来上がっています。次号では正式のアクセス名をお知らせします。

新規入会個人会員

番号	氏 名	勤 務 先 ・ 所 属
721	中田茂	ブラザー工業(株)
722	渡辺敏之	(株)東芝
723	黒田賢三	さくら総合研究所
724	市丸信子	日本ユニシス(株)
725	奥田浩二	大阪ガス(株)
726	松下二郎	三菱商事(株)
727	石戸康博	

発行所 日本システム監査人協会

発行人 川野 佳範

事務局 〒151 東京都渋谷区笹塚2-1-6
笹塚センタービル5F
(株)産能コンサルティング内
TEL. 03(5350)9268 FAX. 03(5350)9269

※ご連絡はなるべく郵便または、FAXをお願いします

会報担当(ご投稿、ご意見、ご要望は下記まで)

三谷慶一郎 (株)NTTデータ経営研究所

TEL. 03(5467)6321 FAX. 03(5467)6322

金子 長男 (財)公営事業電子計算センター

TEL. 03(3343)4560 FAX. 03(3343)6742

富山 伸夫 (株)データ総研

TEL. 03(5695)1651 FAX. 03(5695)1656

木村 陽一 共同VAN(株)

TEL. 03(5321)3208 FAX. 03(5321)3201

山内 美佐子 伊藤忠テクノサイエンス(株)

TEL. 043(285)1892 FAX. 043(285)1889