特定非営利活動法人
SAAJ 日本システム監査人協会報

公認システム監査人特集

公認システム監査人制度発足から４年が経過いたしました。認定者数も公認システム監査人355名、公認システム監査人補238名、合計593名に達し、制度として確立された観があります。また、認定された方々も、その資格を活かし各方面でご活躍中であります。

そこで、本号では、公認システム監査人特集として、ご活躍中の方々のご報告と新認定者の抱負を掲載し、今後のシステム監査人の活動のご参考に資することにいたしました。

また、本年、公認システム監査人の更新手続きの改訂と継続教育の算定方式の改訂が行われました。あわせて本号に掲載いたしましたので、ご一読願います。

もっと気楽に、公認システム監査人

No.898 竹下 和孝

1．CSAとしての歩み

事業年度の決算報告書を印刷すると、一人前の経営者になった気がするのも不思議です。

バタバタと確定申告を終えると、やっと事業の区切りができたと思うまもなく、計算ミスの有無や仕分け方法が適切であったかなど、簿記の参考書を紐解きます。

事業計画、営業企画、日程調整、報告書、請求業務に資金繰りなど、経験してきた経営の一部を思い出すと、すでに事業者として５期目も半ばです。

投稿の要請を受けて、組織から独立して「自立」するまでの道のりを振り返る機会としてみます。50歳からの自立は、一般には厳しい選択を迫られると言われます。特に、事業資金なし、コネなし、人脈なし、営業経験なし、でスタートした個人事業主は厳しい。

同様の環境で、CSA/セキュリティ審査員/ITコーディネータなど、複数の選択肢を並べて、なんとか顧客ニーズを捉えながら好きな業務に没頭できたのではないか、と思います。

	活動分野	これまでの主な業務内容
1)	システム監査活動	監査技術者として企業診断サービス (セキュリティに関連、隣接する場合が多かった)
2)	セキュリティ活動	コンサルティング（ISMS取得、Pマーク取得)
3)	ISMS審査 Pマーク審査	①情報セキュリティマネジメントシステム（ISMS主任審査員) ②個人情報保護マネジメントシステム（Pマーク審査)

目　次

4)	教育・研修 執筆 SAAJ研究会活動	①教育・研修　研修講師としての役割も大きい。 ②執筆（受験参考書、辞書、実務書など） ③共著２冊（システム監査ハンドブック、個人情報保護）
5)	学会活動・コミュニティ活動	監査学会、セキュリティ関係コミュニティ SAAJでは　月例研究会、会報編集、個人情報保護 ITC協会、ITC埼玉、アナリスト協会、インターネット医療
6)	ITC活動 経営品質向上活動 医療情報評価活動	ITCインストラクタとしてケース研修 地域産業を支援するIT経営応援隊事業に参加 インターネットと医療情報に関する評価に参加

2．新しいタイプの監査人として

組織から独立しようと思ったきっかけには、さまざまな要素が関連しますが、情報セキュリティニーズの高まり、後輩であるITエンジニアへの期待、国際的なIT関連事業の動向が大きな影響力を持ったと考えています。

今後は、コンピュータや情報システムにとらわれない、仕組みとしての監査を目指しています。CSAの特徴は、実践経験を持つことであり、これが今後の強みとなると思います。

	活動分野	今後の興味の方向と対象
1	組織能力開発	リーダシップ、CSR、コミュニケーション
2	企業経営	技術・業務システム、管理システムへのIT活用
3	教育・研修	セキュリティ、高度IT人材育成、CIO育成、経営者研修
4	社会システム	有効性評価、セキュリティ評価、IT活用
5	環境システム	快適な生活、都市機能、自然環境に対するIT活用
6	医療システム	電子カルテ、診療情報連携、遠隔、利用者の立場

それぞれの隙間には、個人で対応できる、いや個人のほうが活動しやすいビジネスチャンスがいっぱいあるように思えます。もちろん、規制緩和や民間への業務開放が進んではいますが、企業としての実績やブランドがないと参加できない制度も実際には多いです。

このように見ていくと、どうも私が志向する監査人の姿は、監査人ではなく、監査のスキルや経験を活用した仕掛け人（実践コントローラ）だということがわかります。

実際、マネジメントシステム審査活動を重ねると、審査基準に対する判断だけでなく、どのように発展させるかに興味を持つようになり、改善のシナリオができてきます。

3．楽しみがいっぱい（CSAの可能性）

これからしばらくは、内部統制活動のもとに財務会計システムや業務管理という企業システム監査、情報システム監査が必要とされます。

多くのCSAは、情報サービス産業での経験や企業での管理職としての経験も長いので、本社部門だけでなく、グループ関連会社、海外子会社に対する管理システムの統制強化にも期待されます。国際的な活動に触れる機会でもあります。

会計監査と異なり企業の仕組みの監査が具体的に制度化されているわけではありません。

しかしながら、新会社法や金融商品取引法のもとで、連結決算やグループ経営の対象となる企業グループの関係会社に対する「業務の適切性」を確認するための内部統制は、より強制力を伴って、企業の自主的な活動として実施する環境が整いつつあります。

CSAは個人の活動に対する資格認証であり、スポンサーはついていません。

個人的には、CSAの活動支援の仕組みや交流の仕組みを作りたいと考えています。

4．自立と自律

CSAの制度が開始されて丸４年が経過したわけですが、システム監査人というだけで、どうしても重く感じるのは監査の響きと役割が理由でしょうか。

企業に属する組織人としての役割から解放され、独立した監査人としての場所を見つけるのは容易ではありません。「自立する」という表現にはあこがれますが、当然、「自律する」ことが前提で、経済的にも能力的にも、さらには経験知からも自立していることで、「公認」の名にふさわしいCSAになりたいと感じています。

監査人としての職業倫理や、所属する組織の倫理規定、契約書や誓約書に拘束されることなく、自由な振る舞いであっても許容の範囲という活動が自然にできるよう、心技体を磨く訓練は怠らないようにしたいものです。

監査は、ルール違反や不具合を発見し指摘するだけでなく、ルールを守っていることを第三者の目で評価して証明する手段でもあります。企業活動を構成する個人が「自立し自律」するときに、証明手段として監査の需要が増大すると思われます。

企業が、もっと気楽に、公認システム監査人の活動を受け入れるようになり、監査活動が企業行動のPDCAを支える役割として認知され、業績向上に寄与していることを楽しみにしております。

公認システム監査人として

みすず監査法人　片岡　学

システム監査との出会い

私とシステム監査の出会いは、昭和60年の当時の情報処理システム監査技術者試験に始まります。

金融機関の情報システム部門に配属され、プログラマーからスタートし、当時はプロジェクトを任されるようになっておりました。情報処理技術者試験も当然の如く、毎年のように受験しており、この年から始まったシステム監査の試験も受験し第1回目の合格者となりました。

生命保険会社勤務でもありましたので、このときは、まさかこの分野で将来にわたって仕事をすることになろうとは夢にも思いませんでした。

以来、情報システム部門において内部統制に関する業務や、内部監査部門においてシステム監査業務を担当し、そして、直近には監査法人において、システムレビューを担当する業務に携わることになりました。

これもひとえに、幸か不幸か、昭和60年に「システム監査」に巡りあったためによるものと思われます。

金融機関のシステム監査人として

結局12年間、生命保険会社のシステム監査人を勤めることになりました。システム監査を始めた当初から、金融機関におけるシステム監査は、他業界に比べても比較的取組が進んでおり、(財)金融情報システムセンターによって、金融機関等のシステム監査基準ができあがっておりました。

その意味から、業界内での標準を研究したり金融機関同士で情報交換させていただくことによって、実にたくさんのことを学ばせていただいた思いです。

とりわけ、都銀各行の取組には質量とも大変教えられるところがあり、そのような取組を目標としながら、自分なりの自社におけるシステム監査論を展開しつつ、日常のシステム監査業務に打ち込んできたものでした。

そこでのスタンスは、システム監査を通じて、自社のITやIT部門を世の中標準に近づけ、IT部門のために貢献すること、そして会社のシステムリスク管理に貢献することでした。そのことはいわば、IT部門で育てられたシステム監査人が果たすべき役割であるとの思いからでもありました。

12年間のシステム監査人時代に、幾つかの大きなイベントに遭遇しています。これらのイベントを通じて、システム監査人として、実にたくさんのことを学んだ気がします。またこれらの経緯を経て、世の中のシステムリスク管理やシステム監査の重要性が飛躍的に高まってきたのもまた事実であるとも思います。

ひとつは、阪神淡路大震災です。このことをひとつの契機として、システム監査基準も改定されたように記憶しています。災害対策の重要性、またコンピュータシステムの危機管理計画の重要性について、身をもって体験させられるとともに、所属していた会社も抜本的な検討を迫られた事象でもありました。

次に西暦2000年問題でした。もうすでに記憶の中に消えていってしまっている方も多いと思いますが、当時の対策や監督官庁の方針や検査を通じて、情報システムの問題はもはや経営問題であるとの認識を強くさせられた事案でもありました。システム監査を通じて経営に貢献することの大切さを思い知らされたものでした。

次は、金融検査マニュアルの登場でした。検査マニュアルの中に「システムリスク管理態勢」編があり、リスク管理のひとつの柱にシステムリスク管理が取り上げられたわけです。ここでも金融機関におけるシステム監査の実施が謳われ金融機関はもう一度体制の整備が見直されたわけです。

最後は、例のM銀行システムトラブル事件です。当時原因も含めていろいろな分析がなされましたが、金融機関のシステム監査人の一人として、この事件には二つの衝撃を覚えた記憶

があります。外からみて最強だと思っていたメガバンクのシステム開発力が必ずしも磐石ではなかったのではないかということ、そして強力な陣容を有していたと思っていたメガバンクのシステム監査機能が必ずしも当時の経営にとって有効でなかったのではないかということです。

システム開発力とシステム監査力、このふたつを弱める、なにかのIT環境の変化があるのではないか、そのことは、今後の金融機関の情報システムの信頼性や安全性に重大な影響をもたらすものにならないかなどと考えさせられた記憶があります。そのため、金融機関のシステム監査人としての最後の２年間は、金融機関の情報システムを守るために、システム監査はなにをすべきかとの観点から、監査目標を立ててシステム監査の実施にあたりました。

この間、公認システム監査人制度が発足し、発足年に公認システム監査人として認定を受け、実務を通してシステム監査人として更なる監査実績を積むとともに、協会の定例研究会などでの知識修得に努めてまいりました。

キャリア転換

2006年1月に、システム監査人としての更なる奥義を極めるため、また財務報告にかかる情報システムの統制状況のレビューアを通して各企業におけるIT統制やJ-SOX法対応のサポートを行ってみたいとの思いから、監査法人への転進を決意しました。

監査法人での業務については、まだまだわかばマークがとれない状況ではありますが、いままで培ってきたシステム監査の知識を活かしつつ、またシステム監査人としての熱き思いを継続して抱きつつ、監査法人でのシステムレビュー業務に邁進したいと考えている次第です。

今後のCSAとしてのあるべき姿

システム監査技術者試験制度ができてから約20年、そして、公認システム監査人制度ができてから4年が経過しました。「システム監査技術者」を中心に、実務に応じられるシステム監査人を認定し、システム監査の実績をさらに積上げ、情報化社会の健全な発展に寄与しようとする公認システム監査人制度は大いに意義ある制度であると考えています。今後とも、CSAに対する世の中の評価をあげるための努力を、協会やCSA自らが行っていく必要があると思われます。そのためには、CSA一人ひとりが、システム監査実務を通じて、確かな実績をあげていくこと、経営や顧客のリクエストにしっかりと応えていくこと、まずこのことが当制度を支える基本であると考えます。それには、日頃の継続的な研修の場を通じて更に研鑽を積んでいくことがますます重要な環境になってきているのではないでしょうか。

昨今、J-SOXへの対応で、内部統制の議論が盛んに行われています。この中でもITへの対応が要請され、そして、IT統制への監査が必要な環境になってきています。今まさに、システム監査人、そして公認システム監査人が必要とされてきています。私たちはそのことを十分に自覚するとともに、これら社会の要請、そして環境の変化に十分に対応でき貢献できるよう、互いに研鑽し努力していきたいものだと思います。

以上のようなことを愚直にも考えている公認システム監査人の一人でありますが、システム監査や、さらに日本システム監査人協会、そして公認システム監査人制度の発展のために、少しでもお役に立てればと考えております。皆様には引き続きご指導・ご鞭撻の程、宜しくお願い申し上げます。

CSAとしての活動と今後に向けて

No.1131 須田 勉

私がCSAとして認定を受けた2003年当時は、某外資系コンピュータベンダのサーバ運用保守サービス部門にて、サーバを購入していただいた顧客（銀行業務あるいはテレコム業務のようなミッションクリティカルなシステムの購入先）に対し、運用しているITシステムの可用性、信頼性、機密性等に関するリスクアセスメントを行い、顧客のITシステム目標と整合性が取れているか否かをギャップ分析し、それを報告書としてまとめ、改善提案する仕事を行っていた。

IT運用システムの可用性アセスメントと呼んでいたが、システム監査の内容と比較すると、監査に加えてコンサルティング業務も含めた内容であった。

システム監査との類似点は、アセスメント対象顧客のシステム導入内容のプロファイルを事前に机上で調査し、必要な場合は事前にアンケート調査を行い、アセスメント実施計画を作成する。アセスメントの実施前はチェックリス

トを用意して、チーム（2～3人）での分担を決め顧客にてインタビューおよび現地調査（主としてサーバルームでの物理的設置環境調査）を数日間かけて行い、現地調査終了後、調査内容を評価した数十ページの報告書を作成し、数週間後に顧客への報告説明会を実施するものである。

アセスメントチームは、①ビジネス要求とITの整合性、②IT技術分野、③運用サポートオペレーション、④ITシステムの設置環境、⑤変更管理の仕組み、⑥情報のバックアップの仕組み等のドメインごとのリスクアセスメントを分担し、ベンダ独自のアセスメント基準に基づいて、運用プロセスを可用性、信頼性、機密性の観点から成熟度レベルを評価する。

このアセスメントの目的は顧客のビジネス目標（例えば、ITシステムのエンドユーザに対する顧客満足度を高め売上げxx%拡大に寄与する）やIT目標（システム稼働率として99.xx%の可用性を達成する）を達成するためには現状のシステムではどんなリスクが存在し、そのリスクの顕在化を防ぐための改善項目を提案することである。改善提案にあたっては、もちろんベンダなのでその結果が自社のビジネスに結びつくことができれば最高であるが、我々アセッサ（監査人）はあくまで第三者の立場で評価および改善提案することを貫くことに苦慮した。

ベンダ所属のもとでアセスメントを実施するにあたってシステム監査基準一般基準の2.1および2.2で規定されているシステム監査人の外観上の独立性と精神上の独立性が非常に重要であることが身をもって経験した。

このアセスメントでは実施工数の関係でアセスメント報告書作成から顧客への報告会までに顧客への直接的な報告内容の確認というステップが入らないために、システム監査報告の中のステップである被監査組織との意見交換無しで最終報告会に臨むことになり、報告内容の事実誤認の排除に非常に神経を使うこととなった。必要であれば電話および電子メール等で確認を取ったが、やはり、被監査組織とフェースツーフェースで意見交換を行い、報告内容の合意を取ったうえでの報告会の実施が重要なステップであると思う。

報告書の内容を被監査企業に十分に納得してもらうことがその後のフォローアップをスムーズに行ううえで重要であるからだ。

ある場合にはある改善事項について被監査部門の担当者が資源の緊急的な増強を望む観点から、こちらからの改善提案をより強調して部門の長に伝えて欲しい旨の意向を示すことは良く見受けられることである。

しかし、この場合も監査人としての独立性を保つことが第一に重要であろう。このアセスメントでは、監査手法としてアンケート法、チェックリスト法、インタビュー法および現地調査法が主体であり、運用システムの技術的な内容の調査については、運用保守サービス部門が顧客のシステム情報のデータベースで保持しており、事前にドキュメントレビュー法により十分な調査を行うことができた。

しかし、365日24時間の高可用性を要求されるITシステムの場合、コンピュータを利用した監査技法を採用し、それを顧客に導入することは顧客の業務への影響が大きすぎ、場合によっては監査ツールを導入することにより最悪、システム停止を招きかねない恐れがあり非常に難しい課題であった。

顧客によっては、運用システムと同等の試験環境を備えている場合があり、その試験環境に監査ツールを導入して他に影響がないことを確認してから本番環境に導入するステップは実施することが可能であるが、それでも現場の運用部門にとっては相当なリスクを背負うことになり、監査ツール導入への抵抗感は強いのが現実である。

今後、ますます、複雑性が増すシステムが多くなる状況のなかで、本番運用に影響を与えないで有効な監査ツールを如何にスムーズに導入して行けるかは、その監査ツールの機能や仕組みとともに非常に大きな課題になると思われる。その場合、顧客の運用システムの変更管理の仕組みとの連携を如何に取るかが大きなポイントであろう。

2003年からはITIL（IT Infrastructure Library）のフレームワークを全面的に採用したアセスメントを実施することになった。

ITILについては2005年にISO20000として規格化され、JIPDECもパイロット認証をスタートしており、今後、ITシステムの運用管理のマネジメントシステムとして認証取得する企業が本格化すると思われる。ITILベースのアセスメントも前述の実施方法と変わらないが、内容的により企業のビジネス目標とITシステムの目標の整合性を如何に取って行くかにフォーカスされており、いわゆるITガバナンスの分野のアセスメントが強化されている。

プロセス成熟度を測る管理項目として、顧客と合意したSLA(Service Level Agreement)の内容、プロセスの有効性を評価するKPI(Key Performance Indicator)およびIT目標として

のKGI(Key Goal Indicator)の策定、目標を達成するためのCSF(Critical Success Factor)の明確化などが挙げられ、運用管理プロセスを如何にPDCAサイクルとして回しているかを評価する方向となっている。

2006年からは、ISMS(ISO／IEC 27001、JISQ27001)の審査員としての活動を行っている。監査における基準性および独立性に加えて、認証性が追加されていることが審査の特徴として挙げられる。

審査員に与えられている権限は、被審査企業がISO27001の要求事項に適合しているかどうかを審査し、適合していると判定すれば認証授与できることを推薦することである。

実際の認証の可否の判定は、現場の審査員からの認証推薦を受けて、審査機関のなかで、別のレビュアーにより審査報告書の審査が別途行われ、そこでOKであれば、その後、JIPDEC等の認定機関への認証書発行の手続きに基づいて認証書が発行される手順となっている。この仕組みは審査の客観性および公平性を確保するために非常に重要である。

すなわち、現場の審査員の見方を別の角度から、より客観的に別の審査員が見ることに意義があり、また、現場の審査員が見落としがちな項目について建設的な意見を述べることにより、担当の審査員の審査スキルの向上にもつながる。

ISMSの審査を通じて感じることは、顧客にとって認証を取得することが如何に企業経営に役立つかということを理解してもらうことの難しさである。

得てして、顧客側は当面の審査を終わらせ、認証を取得できれば良いと思いがちであるが、認証取得が最終目的ではなく、取得した後もマネジメントシステムとしてPDCAを回し継続的にプロセスを改善することにより、企業経営の継続的発展につながるということを如何に理解してもらえるかである。

そのためには、審査基準や要求事項についてその1個1個を杓子定規に質問するのではなく、顧客の業務プロセスに沿って当てはめながら、その要求事項が顧客の業務にとってどんな関わりがあり、事業発展にどのようなメリットがあるのかを顧客が理解しやすいように咀嚼してインタビューして行くことが重要である。

私自身は個人的には、セキュリティは個人情報保護も含めてシステム監査におけるあくまで一分野であると考えており、このセキュリティも含めた本格的なシステム監査を手がけて行きたいと考えている。

システム監査を行うためのCSAの必要スキルとしては、①ITシステムに関するスキル、②監査に関するスキル、③経営管理に関するスキルに大別できると思う。システム監査の基本的な役割が「企業体が経営目標を達成するために必要な情報システムの安定的な運用についての保証」と考えるならば、CSAとして前述の①から③までは必須のスキルであろう。

私の課題として③のスキル強化が挙げられる。特に経営全般から見たIT投資（IT-ROI）の有効性評価を含む経営管理に関するスキルはますます必要性を増すと思われ、加えて効率性の評価手法について十分なスキルを身につける必要性を感じている。

①から③まで通して関係する、内部統制を含むITガバナンスひいてはコーポレートガバナンスに関するコントロールを十分に理解する必要性も感じている。

改定されたシステム監査基準にはシステム監査人が「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リスクアセスメントに基づいて適切に整備・運用されていることを検証・評価することによって、保証を与えあるいは助言を行う活動」と定義されており、システム監査が保証型に向かいつつある状況のなかで、CSAとして十分なこれらの力量を持つことが求められている。ISMSと同様にシステム監査においても前述のようにリスクアセスメントを実施したうえでリスクコントロールについて監査することが前提となっている。

CSAのスキルとして必要なリスクコントロールについての考え方はITILのITサービス継続性管理やCOBITにおけるサービス提供とサポート(DS4：継続的なサービスの保証)等が参考となろう。システム監査におけるスキル修得もやはり自分の現在のレベルをセルフアセスメントして、CSAとして必要なスキルマップとのギャップ分析を行い、スキル目標を明確化しPDCAサイクルのもとで継続的にキャリアアップを図って行くことが重要であり、あらゆる機会を捉えて自己研鑽を図って行きたい。

公認システム監査人合格とPDCAサイクル

No.1479 早川 晃由

私は、人口約８万人の中部の地方自治体に勤務しています。

情報システム部門には通算して15年程在職しています。平成15年度のことですが、上司から情報セキュリティポリシーの策定を命ぜられ、総務省のガイドラインや先行している自治体を参考にしながら完成させました。

また、平成16年４月からの運用開始に合わせ、情報セキュリティポリシーを運用するためのマニュアルや様式類を整備し、説明会を開催したことを記憶しています。

情報セキュリティポリシーの策定やそれを運用に移行させるためには、これらに関する知識や技術の習得が求められます。

その中で、情報セキュリティ対策は一過性のものではなく、PDCAサイクルで継続的に取り組まなければならないと解説されています。

PDCAサイクルは、情報セキュリティ対策に限らず情報システムの分野で適合するものが多くあります。たとえば、システムのライフサイクルや開発手法、CMM(成熟度モデル)など全体的にあるいは部分的にあてはめて捉えることができます。

情報システムの設計開発と運用に長年携わり、情報セキュリティポリシーの策定や運用も担当した経験から、次の段階として、どうしてもPDCAの「C」にあたる点検・評価の知識・技術を習得しておく必要性を強く抱くようになりました。

点検・評価には、システム監査や情報セキュリティ監査が極めて有効です。そこで、システム監査の勉強を始めました。

参考書籍を取り寄せましたが、独学に限界を感じ、まず、システム監査人補の取得をめざしました。特別認定講習を受講し、平成16年秋期に日本システム監査人協会に入会するとともに、システム監査人補の認定を受けました。

そして、実務において「住民基本台帳ネットワークシステム」や「地方公共団体情報セキュリティ」の自主点検を実施、担当しました。しかし、自主点検だけでは、システム監査自体の実務経験が不足していることに気づき、平成17年にシステム監査実践セミナーに参加しました。

たった２日間でしたが、私にとっては非常に勉強になり、システム監査の難しさを実感しました。その年は、ISACAのCISAにも挑戦しました。かろうじて合格水準に達しました。そして、総務省自治行政局が主催する地方自治体職員向けの「情報セキュリティ監査セルフチェック研修」を受講した後に、今回の平成18年春期公認システム監査人の募集で認定申請をしようと決意しました。

私が勤務しているような規模の小さな地方自治体では、人事異動でそれまでの経歴とは全く関連のない部署に異動することもあります。

もし、他の部署への異動が決まれば、認定申請は行わないことも考えていました。継続教育が困難になると判断したためです。

このため、人事異動の内示が確認できた締め切り日ぎりぎりに申請書類を郵送することになってしまいました。公認システム監査人の認定には面接試験があります。

私は、ある資格試験の面接に連続して失敗した経験があり、面接試験はとても苦手です。面接試験実施の通知を受けた日から提出した小論文を読み返し、「システム監査人倫理規定」を暗記しました。暗記をしていると、この倫理規定にはシステム監査人がシステム監査を行う上での基本的かつ重要な事項が定められていることがよく伝わってきました。そして、面接試験は相変わらず緊張しましたが、認定通知を受け取ることができました。

私のこれからのシステム監査人としての、キャリアパス、自己実現、社会貢献を目指すためにPCDAサイクルの手法をスパイラル的に自分自身にあてはめてみようと考えています。そして、公認システム監査人の名に恥じることのないよう継続的に研鑽に励みたいと思います。

公認システム監査人(CSA)利用推進の活動が始まりました！！

CSA担当理事　力　利則

公認システム監査人(CSA)になったけれど、・・その後の活動がよくわからない、認定を受けた意味やメリットは何？・・というご要望にお答えするために、本年度から複数名の担当理事を設置して検討を進めています。

第１の取り組みは、CSAの活動概要や活用のメリットなどを記載したパンフレットを作成しました(図：参考(原稿Ａ４版両面))。

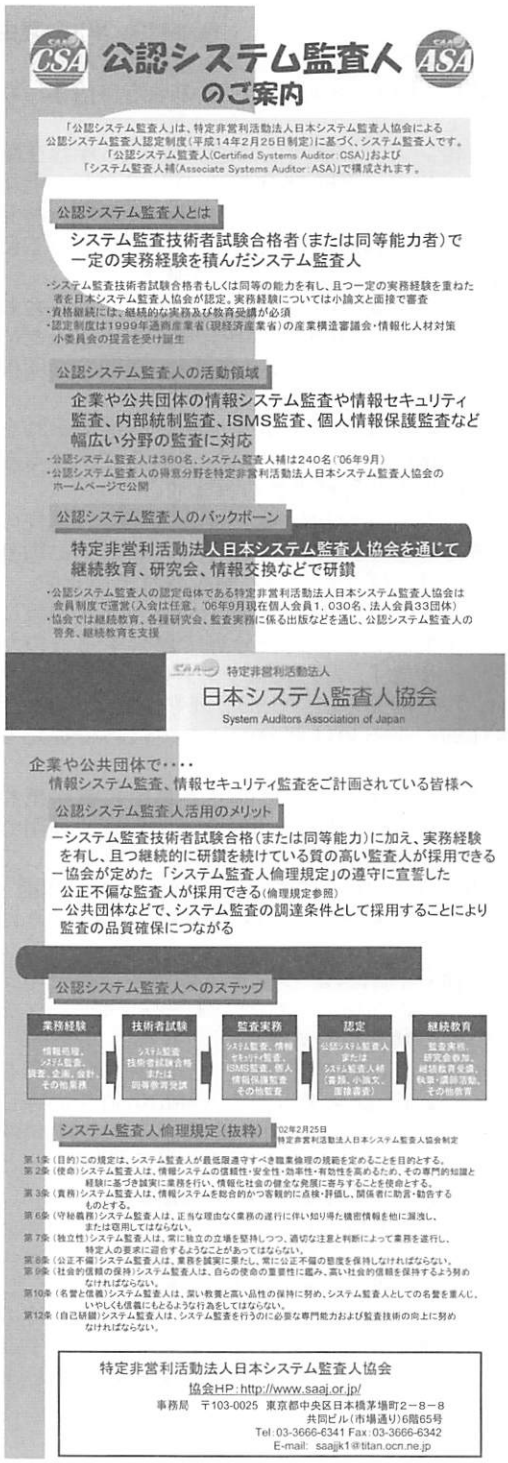
このパンフレットは協会主催の各種催しやセミナーで配布するだけでなく、システム監査講演会などの企業や官公庁・地方自治体のシステム部門等の方々が集まるイベントでも配布する予定です。CSAの皆様ももしご入用の場合はSAAJ事務局までご連絡下さい。

第２の取り組みは、各種の入札案件や資格要件にCSAを明記していただく活動があります。これはまだ検討途中ですが、CSAの設立経緯や要件などをもとにCSA資格の重要性や必要性を改めて提示していきます。依頼文書や依頼メールという形式になると思いますが、CSAの皆様からのご要望により協会名で個別に発行することも考えています。

第３の取り組みは、SAAJ認定委員会と協力してCSA認定証カードを作成する予定です。CSAとして仕事に取り組んでいる方々から、身分証明書として胸から下げる名札に使いたいというご要望に対して、理事会承認を得て推進しています。有料になる予定ですがぜひご活用下さい。

第４の取り組みは、CSAの皆様へのこうした活動の周知と活動へのご参画があります。上記の第１から第３の取り組みを知っていただくことはもちろん、それ以外にもCSA向けのセミナーや研究会の設立も考えています。しかしこれらはCSAの皆様方の積極的な参画がなければ成り立ちません。その手段としてホームページやメーリングリストの活用から始める予定です。ホームページやメーリングリストはすでにスタートしているのでこれからは中身の充実を図り活性化させることを重視します。合わせてCSA向けのセミナーや研究会の立ち上げも考えていきます。

今回、この会報で特集に取り上げられたことは、CSA利用推進について、会報編集委員会によるご協力の賜物だと思います。CSAの皆様からの貴重で役に立つ記事がたくさん記載されています。いろいろと参考にしていただいて、ご意見やご要望等あれば、会報委員あるいはCSA利用推進担当理事までご一報下さい。宜しくお願い致します。



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

公認システム監査人認定委員会

平成15年度に認定、登録された公認システム監査人及びシステム監査人補の方は、本年度末(平成18年12月31日)に認定期限が到来します。ついては、公認システム監査人制度、継続教育要項に基づき、認定の更新手続きをお願いいたします。

詳細は、当協会のホームページ(http//www.saaj.or.jp/)「認定資格更新申請手続」を参照していただき、「認定資格更新申請書」と合わせてホームページ内からダウンロードするようお願いいたします。

公　告

特定非営利活動法人日本システム監査人協会(以下、「当協会」という。)は、公認システム監査人認定制度(平成14年2月25日制定)(以下、「当制度」という。)に基づき、「公認システム監査人(Certified Systems Auditor：CSA)」及び「システム監査人補(Associate Systems Auditor：ASA)」の平成15年度の認定者について、以下の手続きにより認定の更新を行います。

平成18年10月1日
特定非営利活動法人日本システム監査人協会
公認システム監査人認定委員会

1. 新対象者

平成15年度に認定された公認システム監査人及びシステム監査人補とする。
(平成15年度の認定者の認定期限は、平成18年12月31日までとなっている。)

2. 更新申請条件

当制度に基づく継続教育の時間が次表の所定の時間を満たしている者とする。公認システム監査人及びシステム監査人補の認定の有効期間は3年であり、継続教育の受講条件をクリアすれば、認定の更新を行うことができる。認定の更新には、認定日よりの3年間及び3年間の1年ごとに、次表に定める時間以上の継続教育を受けることが義務付けられている。継続教育の範囲や認定される時間数は、「継続教育要項」に詳細に定められている。

資　格	1年間の最低義務時間	3年間の最低義務時間
公認システム監査人	30時間以上	120時間以上
システム監査人補	15時間以上	60時間以上

継続教育の算定期間は、次のとおりである。

(1) 第1年目　認定日(平成15年の日付)から平成16年12月末まで
(2) 第2年目　平成17年1月1日から平成17年12月末まで
(3) 第3年目　平成18年1月1日から平成18年12月末まで

3. 更新申請書類

公認システム監査人及びシステム監査人補の申請書類は、次表のとおりとする。

申請書類	説明
(1)認定資格更新申請書	様式1
(2)継続教育実績申告書	平成18年度分 (システム監査人の「継続教育要項(04.10.13)」による。ただし、18年7月以降の実績については、「継続教育要項(06.7.1)」による。)
(3)更新手数料振込領収書(写)	様式1の裏面に貼付する。
備考	

4. 認定資格更新申請書の記入方法(様式1参照、本人記入欄のみを記入)

(1) 申請日

申請日を記入する。当協会において、受付順に更新手続きを行う予定であり、後記申請期間内に早めに申請することが望ましい。

(2) 写真

最近6ヶ月以内に撮影した免許書用写真を貼付する。

(縦3cm×横2.5cm胸部上半身顔写真)

(3) 申請区分(該当箇所の□にレ印または、■印をつける。以下同じ)

①公認システム監査人又は、②システム監査人補のいずれかを指定する。

(4) 認定番号

公認システム監査人は、「K」から始まる数字5桁、システム監査人補は、「H」から始まる数字5桁を記入する。

(5) 認定年月日

認定証の認定年月日を記入する。

(6) NPO. SAAJ加入の有無

①協会への加入の有無を記入する。

②会員番号

協会へ加入している会員は、会員番号を記入する。

(7) 氏名・住所・連絡先

①から⑧までの所定欄に必要事項を記入する。また、②氏名欄には捺印する。

なお、連絡先については、会社、自宅のいずれかを選択する。

(8) 添付書類

①平成18年度継続教育実績申告書を同封し、レ印をつける。ただしこの実績申告書を電子メールで提出した場合は「メールで送付」を明記すること。

②申請手数料を振り込んだ後に、更新手数料振込領収書(写)を添付し、レ印をつける。

(9) 公開する情報(公開の可否)

①新たに協会のホームページに氏名、都道府県名及び得意分野の掲載をする場合は、その可否を記入する。「公開する」、「公開しない」の何れかにレ印をつける。

②また、既に公開している場合は、「公開情報変更」「公開情報変更なし」のいずれかにレ印をつける。

(10)公開する情報(公開情報)

情報を公開する場合又は既に公開している情報を変更する場合は、公開するすべての情報について記入する。(氏名、都道府県は、必ず公開する。)

①公開する都道府県名を記入する。

②ホームページアドレス(URL:)を公開する場合に記入する。

③得意分野を公開する場合に記入する。得意分野は3項目とし、業種、専門、実績、アプリケーション等を記載できる。ただし、各項目とも全角15文字以内とする。(句読点、括弧、カタカナ、促音、長音等も全角1文字とする。)

＜得意分野の例示＞
例示１：流通業（情報戦略）
例示２：金融（情報セキュリティ監査）
例示３：ISMS、個人情報保護
例示４：ネットワークのセキュリティ監査
例示５：会計情報、人事・給与システム

5. 更新申請期間
平成19年１月１日(月)～平成19年１月３１日(水)（同日消印まで有効）

6. 更新手数料（消費税を含む）
(1) 更新手数料は、以下のとおり。
①システム監査人補の更新手数料は、10,500円とする。
②公認システム監査人の更新手数料は、21,000円とする。
(2) 更新手数料は、更新申請書提出前に当協会宛に振り込み、振込領収書の写を申請書に貼付ける。振込手数料は申請者の負担とする。
(3) 消費税の取扱いについて
認定申請手数料には消費税を含むものとする。
(4) 更新手数料振込先
会費等の振込みとの混同をさけるため、次の専用口座に振込むこと。
＜銀行振込先＞ 銀行名 三菱東京ＵＦＪ銀行 新宿西支店（０５５）
口座種別 普通預金
口座番号 １４９４７２５
名 義 日本システム監査人協会

7. 更新申請書類の送付
協会事務局あて郵送･宅配便で送付すること。持参は不可とする。
＜送付先＞ 〒１０３－００２５
東京都中央区日本橋茅場町２－８－８
共同ビル（市場通り）６Ｆ ６５号
特定非営利活動法人日本システム監査人協会 事務局
公認システム監査人認定委員会

8. 更新申請から登録までの流れ
(1) 認定資格更新申請書を受付・審査終了次第、順次更新作業を実施する。（１月～２月下旬）
(2) 更新を認定された場合は、新たに認定証を発行し送付する。また、認定されない場合は、平成19年２月末までに通知する。
なお、更新後の認定期限は、平成21年12月31日とする。

＜連絡先＞
住 所 送付先に同じ
電 話 ０３－３６６６－６３４１
ＦＡＸ ０３－３６６６－６３４２
E-mail saajjk1@titan.ocn.ne.jp

（様式１）

平成 18 年度 公認システム監査人／システム監査人補　認定資格更新申請書

（本人記入欄）		申　請　日		平成１９年１月　日		（写真貼付）
申請区分（該当にレ印）		①□公認システム監査人		②□システム監査人補		
認定番号		①Ｋ００		②Ｈ００		
認定年月日		①平成１５年　月　日		②平成１５年　月　日		
NPO.SAAJ加入の有無		①□加入、□非加入		会員番号	②No.	
氏名・住所・連絡先	ふりがな 氏　名	①ふりがな ②氏　名　印				
	連絡先選択	③　□（会社）、□（自宅）（該当にレ印）				
	〒・住所	④〒				
	所属先(会社名)	⑤				
	連絡先	電子メールアドレス（下欄↓）		電話番号	ＦＡＸ番号	
	⑥			⑦	⑧	
添付書類		①□平成１８年度継続教育実績申告書				
		②□申請手数料振込領収書（写）（振込み済み）				
公開する情報		①□公開しない	（現在公開している場合は、情報をすべて抹消する）			
		①□公開する　□新たに公開する	（新たに公開する情報を記入する）			
		①□公開する　□現在公開している	②□現在公開している情報を変更しない。 ②□現在公開している情報を変更する。（情報をすべて記入する）			
		③公開都道府県名		⑤得意分野		
		④公開ホームページ（下欄↓）		⑤得意分野		
⑥URL:				⑤得意分野		

（事務局記入欄）

	書類受付	書類審査	継続教育実績確認	最終認定
更新申請書類	月　日（　）	担当：	合　計	認定委員
申請手数料受領確認	月　日（　）	担当：	時間	
継続教育時間確認	平成１６年度	平成１７年度	平成１８年度	
	時間	時間	時間	認定委員長
認定番号	認定証書発効日	有効期限	登録確認	
No.　－２	年　月　日	年　月　日		

（注）申請手数料振込書のコピーを本申請書の裏面上部にのり付けして貼付する。

特定非営利活動法人日本システム監査人協会の「個人情報保護の取扱いについて」に同意します。

2006年7月1日

システム監査人の「継続教育要項」改定について

公認システム監査人認定委員会
継続教育部会

継続教育部会では、制度発足４年を経たあと、運用上の経緯を踏まえ、継続教育制度の内容を大幅に更新して、「継続教育要項」(06.7.1)」とし、ホームページ上に公表いたしました。詳細は、協会ホームページの左側「公認システム監査人制度」２行目の「継続教育要項」をご参照ください。主な改定点は、以下の通りです。

１．実績申告期限

申告期限到来者については、一律毎年１月１日から１月末までとした。これにより、２月１日から２月末までは審査期間とし、認定された場合は、資格は同年１月１日に遡って更新される。

２．実績申告方法

従来の郵送によるほか、電子メールによる申告も認めるものとし、この場合、署名は記名とし、押印は省略する。

毎年の継続教育申告は以上であるが、第３年目は、さらに認定資格更新申請の年にあたる。

①別途「認定資格更新申請手続」により、認定資格更新申請書を提出する、

②更新料を納付する、

③あわせて第３年目の継続教育実績申告書を提出しなければならない

(この場合、継続教育実績申告書のみを電子メールで提出する場合は、認定資格更新申請書に「継続教育実績申告書はメールで送付」と明記する。

報告先住所等は次のとおりである。

〒103-0025　中央区日本橋茅場町2-8-8　共同ビル(市場通り)6F 65

電子メール：saajjk1@titan.ocn.ne.jp

３-１．継続教育義務時間

義務時間は次のとおりである。変更なし

	１年間最低義務時間	３年間最低義務時間
公認システム監査人	30時間	120時間
システム監査人補	15時間	60時間

３-２．継続教育の範囲

●大幅に変更した。

本要項内で、「システム監査に関する」という範囲には、IT技術の最新動向を含む情報システムに関するもの、及びシステム監査に大きな影響を持つ法令、規格、基準に関するものを含む。

●種別ａで、協会主催の教育について評価を重くし、認定時間を「実時間×1.5」とした。これにより「実時間２時間のものは３時間として申告できる」

種別	分野	継続教育とみなす活動	認定時間	上限
a	当協会主催の教育	講演会、セミナー、月例研究会、支部研究会、分科会への参加、システム監査普及サービスへの参画	実時間×１．５	限度なし

(注)　当協会の支部が主催する講演会・セミナーなども同じ扱いとする。
分科会とは当協会の事例研究会や各種部会等の総称である。
申告時の記載項目は、時間のほか日時、講演会名、講師、テーマでよい。

●種別ｂ１の範囲を増やし、ｂ２、ｂ３を新設した

種別	分野	継続教育とみなす活動	認定時間	上限
ｂ１	他団体主催のシステム監査に関する講演会、研究会及びこれらに準ずるもの	システム監査学会、日本セキュリティ・マネジメント学会、経営情報学会、情報システム・ユーザ会連盟、情報システムコントロール協会、日本内部監査協会、(財)日本情報処理開発協会、日本公認会計士協会、金融情報システムセンター、システム監査普及連絡協議会、情報サービス産業協会、情報セキュリティ監査協会などが主催するシステム監査に関する講演会・研究会などへの参加。 (財)日本情報処理開発協会が認定したISMS研修機関の実施するISMS審査員研修コースの受講、同協会が実施するプライバシーマークの審査員補養成研修コースの受講。	実時間	限度なし
ｂ２	通信教育による学習及び自主学習	通信教育は本要項の趣旨に合致するものであれば、主宰者は受講者の所属の内外を問わない。 自主学習の対象は、当協会の「情報システム監査実践マニュアル」第２版（いわゆる赤本）及び「システム監査　情報セキュリティ監査　ハンドブック」。条件として、Ａ４１枚のレポート添付。	左記学習の合計実時間	10時間/年
ｂ３	情報システムベンダが主催する製品発表会等	同発表会の設営並びに説明聴取	左記設営並びに聴取の実時間	10時間/年

(注) 申告時の記載項目は、日時、主催者名、講演会名、講師、テーマとなる。保存資料としては、講演会資料の表紙・目次等申告内容を証明できるもの。(後日の当協会のサンプリング調査に該当した場合に必要となる。)上に明示がなく疑義ある場合は、種別ｆの個別審査として申告する。

●種別ｃの上限を30時間/年にのばした

種別	分野	継続教育とみなす活動	認定時間	上限
c	実　務	システム監査・検査・審査活動 ＩＴコンサルティング活動 監査活動一般	左記活動の合計実時間	30時間／年

(注) 申告者の主たる職務としての実務をいう。申告時の記載項目は、外部監査、IT コンサルティングについては相手先名と活動内容（受託契約書等の写しが後日必要になる場合がある）、内部監査の場合は、申告者の所属・職務内容（職場の責任者の証明が必要になる場合がある。）となる。(省略、本文参照)

3-4．最低義務時間に達しない場合の取り扱い

●追加

(1) 第1年目に達しない場合

初年度に最低義務時間に達しない場合でも、第2年目の実績申告までに累計２年分の最低義務時間以上の継続教育の受講を条件に、公認システム監査人(CSA)、システム監査人補(ASA)の認定を維持できる。ただし、その期間は対外的に公認システム監査人(CSA)、システム監査人補(ASA)の名称を使用することはできない。

(2) 第2年目に達しない場合

第2年度に最低義務時間に達しない場合で、かつ累計２年分の最低義務時間に達しない場合は、継続教育受講の条件を果たされないことになり、それぞれの認定資格は失効となる。ただし公認システム監査人(CSA)で、システム監査人補の最低義務時間以上を実績として申告した場合は、システム監査人補(ASA)の第3年目に移行できる。上記の取り扱いについては、協会から本人宛通知する。

4．その他　　変更なし

継続教育の実績申告の受付・審査・調査は公認システム監査人認定委員会継続教育部会が担当する。

本要項についての質疑については、当協会事務局に次のメールもしくはFAXでご照会いただきたい。

電子メール：saajjk1@titan.ocn.ne.jp　ＦＡＸ：03-3666-6342

なお、継続教育実績申告書の様式は、協会ホームページの「継続教育要項」よりダウンロードしていただきたい。

平成18年度第7回理事会議事録 日本システム監査人協会

平成18年7月13日（木） 18：30－21：00
於：三井物産(株) 20F 鉄鋼製品本部第3会議室
出席者 鈴木（信）、橘和、富山、吉田（裕）、和貝、小野、馬場、岩崎、金子、蒲ヶ原、斉藤、櫻井（寛）、桜井（由）、須田、力、中山、沼野、松枝、吉田（博）、勝田（監事）、堤（中部支部オブザーバー）

1.資料

① 公認システム監査人の認定書カードの発行の件
② 日本システム監査人協会定款抜粋
③ 20周年記念事業計画実施企画（案）
④ CSAの利用推進の状況

2.審議事項

(1) 公認システム監査人等写真付認定カードの発行について（鈴木会長、馬場理事）
資料①に基づき、馬場理事より認定カードの発行についての説明があり、審議の結果承認された。発行の骨子は以下のとおりである。
・希望者に対して写真入プラスティックカードで発行する。
・受付時期は公認の認定発表時期（年2回）と更新時期（年1回）の3回
・発行手数料はSAAJ会員3,000円、非会員6,000円

3.報告事項

(1) 定款変更案の予備討議（鈴木会長）
現行の定款第27条では、「総会は、正会員総数の2分の1以上の出席がなければ開会することはできない。」と規定されているが、年々2分の1以上の出席確保が難しくなっているので、この規定の見直しが必要であり、合わせて、第16条の役員の任期、第6条の正会員の規定等の見直しが必要であり、例えば、第27条の定足数を5分の1以上、場合によっては定足数を定めずのような検討も考えられるとの提案が鈴木会長より発議された。
これに対して、様々な意見、検討点が議論され、今回は検討のための予備討議として、定款自体の相互関連性並びに定款とその他の会則との整合性も踏まえて、改めて議論を深めることとなった。

(2) 20周年記念事業の骨子案（沼野理事）
資料③に基づき、現段階におけるSAAJ20周年記念事業の実施企画案の説明が行われた。実施時期は2008年2月、コンセプトはシステム監査、及びSAAJのプレゼンス確立に向けた当協会の活動成果の発表の場とし、実施行事の概要、活動体制、スケジュール、概算費用等の案が示された。この案をベースとして、さらに検討を加え、本年の9月ごろまでに、より実行性の高いものに仕上げる。

(3) CSA利用促進プロジェクトの検討状況（力理事）
CSA の利用推進の対策として、④の資料を基にその状況が報告された。1）で審議された CSA の認定カードの発行の他、官庁等の入札、パンフレットの作成、セミナーの開催、研究会活動、出版活動その他の具体的な方策が示された。

(4) 会長及び各担当理事からの報告
1．鈴木会長
①春季の審査結果
監査人申請 22人、うち監査人認定 15名
監査人補認定 6名
失格 1名
監査人補申請 8人 全員認定
②10月7日に広島において、西日本地区合同研究会が開催される。これに、馬場理事を派遣する。
2．事務局（馬場理事）
① 事務所に冷蔵庫を設置したので、活用願いたい。
② 業務改善の一環として、月例会用の領収書作成を月例部会にお願いするために月例会用印鑑の作成を検討している。
3．メーリング（岩崎理事）
メーリングリストの新しい発信および利用方法について
4．事例研究会（吉田副会長）
7月8，9日に仙台において東北支部実践セミナーを開催した。8月、9月においては、幕張において4日間コースのセミナーを開催する予定である。
5．（斉藤理事）
先般、「情報システム・ユーザ会連盟のシステム監査専門委員会」の会合があり、出席した。

今年度のシステム監査講演会は10月5日(木)の開催となるが、例年のように後援団体を募っている。
当協会も候補に入っており、詳細が固まり次第ご案内するので、協会の対応内容を別途検討戴きたい。

6．渉外（桜井理事）
KISAA（韓国監理人協会）を招き、9月30日にセミナーを開催する。講演の後に、協会相互で情報交換会を行う予定である。
その準備窓口は渉外担当理事で行なう。

7．会報（須田理事）
8月発行の会報92号に投稿論文が掲載される予定である。
なお、原稿の締切りは7月15日となっている。

8．近畿支部（吉田理事）
7月21日に定例研究会、8月12日に情報セキュリティ、システム監査の基礎セミナー、9月2，3日に個人情報保護管理者、監査責任者の実務セミナーを大阪で開催予定である。
なお、6月の月例会は中止した。

9．法人部会（小野副会長）
新入会員報告；コガソフトウェア株式会社様
自治体セミナーのDM送付について；関東地区は発送済み。
中四国支部はご協力いただけるということで、資料送付済み。
近畿支部、中部支部はご協力いただける方向で支部内調整中。
(注) この理事会の後、九州支部からご協力いただける旨のご連絡をいただく。

10．基準研究会（松枝理事）
6月、7月のシステム監査基準研究会の定例会議について

11．月例研究会（沼野理事）
8月以降の月例研究会は、8月2日、9月21日、10月23日に予定されており、8月の研究会の講師は内閣官房よりお招きする予定である。
なお、5月22日の研究会には170名、7月3日の研究会には 240 名の参加者があった。

以 上

議　　長　鈴木信夫
議事録署名人　櫻井憲二
　　馬場孝悦

第122回月例研究会報告

No.1186　宮下　重美

日時：2006年8月2日（火）18:30～20:00
場所：中央大学駿河台記念館　281号室
演題：「政府機関の情報セキュリティ対策のための統一基準」
講師：内閣官房情報セキュリティセンター・内閣参事官補佐：佐藤慶浩氏

1．概要

「政府機関の情報セキュリティ対策のための統一基準」(2005年12月版)について、策定メンバーの「内閣官房情報セキュリティセンター」佐藤慶浩氏が、そのポイントを講演した。

2．講演要旨

① これまでは、“政府機関における情報セキュリティ対策”を問われても、政府機関により異なりますと答えざるを得なかったが、今回の統一基準により“各政府機関では最低基準が策定されており、これ以上の対策基準を追加している機関があります”と回答できる状況となった。
即ち、この統一基準は、政府各府省庁の「情報セキュリティ対策内容の整合化・共通化」を促進するために、各府省庁がとるべき情報セキュリティ対策を定めたものである。

② この統一基準は、4階層ある「政府機関統一基準文書群」の一つの階層である。
第1部から第 6 部までの構成となっている。総則、組織と体制の構築、情報についての対策、セキュリティ要件の明確化に基づく対策、情報システムの構成要素についての対策、個別事項について、となっている。詳細は、次の URL で入手できる。
http://www.nisc.go.jp/active/general/kijun01.html
＜公式ウェブページ＞
http://www.nisc.go.jp/active/general/pdf/k303-052c.pdf ＜解説書＞
前者のURLで、関連する各種情報を入手できる。
後者の解説書は、本基準の理解を助けるための参考・詳細資料であり、分り易い説明を逐条解説として追加している。

③ 政府機関統一基準文書群により、次が期待できる。
- 各府省庁においては、政府機関統一基準に準拠して、自らの情報セキュリティポリシー（省庁ポリシー）の見直しを図り、対策の底上げを図ることができる。
- 省庁ポリシーを反映した多数の実施手順書等を各府省庁が作成するうえで、手引き又は参考となり、各府省庁の利用に供することができる。
- 各府省庁自らが行う自己点検と監査に基づく評価、当該評価結果をもとに情報セキュリティ政策会議が行う勧告、これらを受けて政府機関統一基準と省庁ポリシーを見直す、というPDCAサイクルの取組みが可能となる。

④ この統一基準は政府機関用であり政府以外の利用を意図していないものであるが、政府以外の情報セキュリティ対策基準としても、取扱に注意しながら活用することも可能である。

3．講演の内容

(1) 政府機関統一基準文書群と政府機関統一基準

政府機関統一基準は、次に示すように、統一基準文書群の一つであり、4階層からなる。

①政府基本方針
②統一基準運用基準
③政府機関統一基準
④個別マニュアル群
（文書番号　K303）

なお、④は、2006年8月以降に、公開予定である。

(2) 政府機関統一基準の構成
- 第1部：総則
- 第2部：組織と体制の構築
- 第3部：情報についての対策
- 第4部：セキュリティ要件の明確化に基づく対策
- 第5部：情報システムの構成要素についての対策
- 第6部：個別事項についての対策

(3) 政府機関統一基準「第1部：総則」の構成

1.1.1 本統一基準の位置付け
構成と位置付け、個別マニュアルとの関係、各府省庁基準への反映適用対象範囲、などを述べる。

1.1.2 本統一基準の使い方
全体構成は、部・節・項－趣旨（必要性）－遵守事項（遵守事項本文・解説）となっている。
対策レベルの設定は、“当該情報システム及び業務の特性を踏まえ、リスクを十分に勘案した上で、対策項目ごとに適切な対策レベルを選択しなければならない”として、次の「基本遵守事項」「強化遵守事項」で構成している。
a)「基本遵守事項」は、保護すべき情報とこれを取り扱う情報システムにおいて、必須として基準化すべき対策事項
b)「強化遵守事項」は、特に重要な情報とこれを取り扱う情報システムにおいて、各府省庁において、その事項の必要性の有無を検討し、必要と認められるときに選択して基準化すべき対策事項

1.1.3 用語定義
本統一基準では、独自の用語使用があるので、もしも政府外で利用するのであれば確認が必要である。

(4) 政府機関統一基準「第2部：組織と体制の構築」の構成
- 2.1 導入　組織・体制の確立、役割の分離、違反と例外措置
- 2.2 運用　情報セキュリティ対策の教育、障害等の対応
- 2.3 評価　情報セキュリティ対策の自己点検、監査
- 2.4 見直し　情報セキュリティ対策の見直し

(5) 政府機関統一基準「第3部：情報についての対策」の構成

3.1 情報の格付け
情報セキュリティ委員会は、“行政事務で取り扱う情報について、電磁的記録については機密性、完全性及び可用性の観点から、書面については機密性の観点から当該情報の格付け及び取扱制限の基準並びに格付け及び取扱制限を明示する手順を整備すること”としている。

3.2 情報の取扱
情報の取扱について、情報のライフサイクルに沿って、作成・入手．利用．保存．移送．提供．消去．について述べている。
例えば、「情報の作成・入手」においては、“その業務以外の情報の作成又は入手の禁止、情報の作成又は入手時における格付けの決定と取扱制限の検討、格付けと取扱制限の明示、格付けと取

扱制限の継承、格付けと取扱制限の変更、など”を述べている。

(6) 政府機関統一基準「第４部：情報セキュリティ要件の明確化に基づく対策」の構成

4.1 情報セキュリティの機能：主体認証機能から暗号と電子署名など６項目
具体的には、主体認証機能、アクセス制御機能、権限管理機能、証跡管理機能、保証のための機能、暗号と電子署名について述べている。
なお、ここで述べている「遵守事項」は“if ,then 構造”により、例えば、次のような記述構造を採用している。
(a) ○○○を行う必要性の有無を検討すること
(b) ○○○を行う必要性があると求めた情報システムには、○○○を行う機能を設けること。
これは、自己点検・監査の際に問題があった場合に、(a)の検討の問題なのか、(b)の実施の問題なのかを切り分けて責任の所在を明確にするためである。

4.2 情報セキュリティの脅威：セキュリティホール対策など3項目
具体的には、セキュリティホール対策、不正プログラム対策、サービス不能攻撃対策、について述べている。

4.3 情報システムのセキュリティ要件：情報システム計画・設計など４項目。
具体的には、情報システムのライフサイクルに沿って、情報システム計画・設計．構築・運用・監視．移行・廃棄．見直し、について述べている。

(7) 政府機関統一基準「第５部：情報システムの構成要素についての対策」の構成

5.1 施設と環境　施設設備の安全区域と対策管理

5.2 電子計算機　電子計算機．端末．サーバ類の設置・運用・終了時の対策

5.3 アプリケーションソフトウェア　通信回線介在のアプリ．電子メール．ウェブの導入・運用時の対策

5.4 通信回線　通信回線．府省庁内．府省庁外回線の構築・運用時対策

(8) 政府機関統一基準「第６部：個別事項についての対策」の構成

6.1 調達・開発にかかわる情報セキュリティ対策
機器等の購入、外部委託、ソフトウェア開発

6.2 個別事項
府省庁外での情報処理の制限,支給以外の情報処理の制限

6.3 その他
府省庁外の情報セキュリティ水準の低下を招く行為の防止、事業継続計画(BCP)との整合的運用の確保など

(9) その他
統一基準作成時の配慮事項、もしも政府機関以外で活用を考える場合の方法について、講演された。
この統一基準は政府機関用に策定しているが、あえて民間事業者等が利用するとした場合、利用価値があるとのことである。
「政府機関以外での活用方法」の要点（活用ポイント・注意点）は次のとおり。

DO：
① 情報セキュリティ対策体制の修正検討
② 情報の対象の修正検討
③ 格付け・取扱制限表・明示の定義の修正検討
④ 定義用語の修正検討
⑤ 一括置換が可能である。例：行政業務→業務
⑥ 強化遵守事項の取捨選択　など

DONOT
① 部・節・項の構成を変更しない。
② 主語をセキュリティ体制上の役割以外にしない
(具体的な組織名等としないこと)
③ 述語を統合しない。

以下、省略

4．感想

①情報セキュリティ政策会議が国として策定した「政府機関の情報セキュリティのための統一基準」の取組み姿勢、概要、がわかり易く講演され理解できた。特に、我々の関心が深い部分であり、その基本的な考え方、構成、構造、編集手法について、研鑽資料を提供していただき、感謝申しあげたい。

②この統一基準を府省庁基準として使用する際の関係を“標識（＝本統一基準）と運転席（＝各府省庁）”で例えている点は興味深いものがあった。

③本統一基準において、年度計画・情報のライフサイクル・情報システムのライフサイクルを“フラクタルなPDCA”として捉えている。

この統一基準では「リスクアセスメント」という表現がでてこない。“情報の対策レベルの設定、格付けを日常業務の中で全員参加により行うことが「リスク判断」である”との意味をこめているとしている。リスクアセスメントに関わる一つの実行形式が示されたと考える。

④この統一基準の第４部・第５部の遵守事項はそのままチェックリストとして使用が可能である。即ち、教育理解度の再確認としての自己点検、オンタイム・チェックリストとしての自己点検に利用できるものであり、この便利さと活用が注目を引いた。

⑤この統一基準を活用することにより“専任監査者でなくてもある程度の監査が実施でき、監査専門家はさらに高レベル・高品質の監査業務に専念できる可能性がある”ことが示唆され、一つの活用の発想が示された、と考える。

以上、貴重なご講演に感謝申しあげたい。

平成18年度　第２回システム監査実践セミナー開催結果の報告

No.735　三輪　智哉

平成18年度第２回システム監査実践セミナーが、さる７月８～９日の２日間に渡り、宮城県富谷町の「ユアテック研修センター」において、協会東北支部との共催で開催されました。

今回は、受講者８名、講師３名、協会東北支部のメンバー３名の合計14名の参加を得て、成功裏に開催することができました。

以下、その実施結果概要についてご報告いたします。

1. システム監査実践セミナーの特色

システム監査実践セミナーの特色は、事例研究会が「システム監査普及サービス」として実際にシステム監査を実施した被監査企業の監査事例をベースとして教材を作成し、実際には４～６ヶ月かけて実施したシステム監査の実際を２日間に凝縮して、実地に体験してもらうという、極めて実践的な演習を主体としたセミナーとなっていることです。

受講者４名で１つの監査チームを形成し、システム監査個別計画書の作成からシステム監査報告会に至るまで、チームのメンバーが協業して、システム監査手順を実地に体験することになります。

システム監査の実際を体験できるだけでなく、さまざまな経験や技術を持っている他の受講者との密度の濃い協力を通して、10年来の既知の友人のような関係を創ることができ、この点だけをとっても１度参加してみる価値がありそうです。

システム監査を実際に経験したことのない方には、是非１度参加されることをお勧めいたします。

2. 今回のセミナーの日程

今回も、過去のセミナー同様、システム監査個別計画書の作成(事前学習)、予備調査、本調査、さらには監査報告書の作成を経て監査報告会までを、１泊２日(約15時間)で体験してもらいました。

第１日目の日程が終了した夜９時過ぎからは、受講生と講師が入り交じっての懇談会も催され、日ごろの業務などの話に花が咲きました。

3. 受講者について

今回は、8名の方々にご参加をいただきました。うち1名が非会員の方で、残りは協会会員の方でしたが、普段はなかなか実施する機会のないシステム監査とはどういうものなのか、体験をしていただくことができたと好評をいただきました。

受講者の受講の目的では、勉強のためとした方が5名と最も多く、実務のための準備とした方1名、経歴のためとした方2名を大きく引き離しており、会員の方々の意識の高さが伺われました。

その受講目的が達成されたかどうかについて伺ったところ、十分達成されたとする方が2名、まあまあ達成されたとする方が4名で、一応の満足は頂いたものと考えております。

4. 教材について

事例研究会が実施したシステム監査普及サービスでのシステム監査事例をベースとして教材を作成しており、今回の教材は、「現在までのシステム化・情報化の妥当性評価」及び「新情報システム企画の情報戦略と情報化計画の妥当性の評価」が監査テーマとなっている事例を使用しました。

5. 講師について

講師は、システム監査技法などに関する説明やセミナー終了後の講評を行うほか、被監査企業の役員や従業員に扮し、システム監査人となった受講生から、予備調査及び本調査時の質問に回答したり、システム監査報告会の際にはシステム監査人に質問をするなど、実践的な役割も演じました。

今回の講師は、事例研究会のメンバーの中から、次の3名が担当しました。

鈴木　実　　富山伸夫　　三輪智哉

6. 受講結果アンケートの集計結果について

今回受講された8名のうち、監査経験のある方は2名、ない方が6名となっており、またSAAJの会員が7名(法人会員を含む)、非会員の方は1名となっています。

また、ITコーディネータの資格を保有されている方が2名、公認会計士の方が1名おられ、システム監査を専門としていない方へのシステム監査の普及の意味でも重要な役割の一端を担っているという感想を得ました。

一方、本セミナーの難易度について聞いたところ、課題によっては、難しかったと回答される方が5名に達しており、今後のセミナーの内容等について、考慮しなければならない点もあろうかと思います。

一方、本セミナーを受講しての目標達成度については、十分と応えた方は2名、4名の方がまあまあであると回答しており、過半数の方がそれなりの成果を取得できたものと考えています。

受講料については、高いと回答された方が4名いたのに対し、ちょうど良いと回答された方が4名で、拮抗しております。

7．実務セミナーの今後

事例研究会が主催して実施する本セミナーは、協会の特定非営利活動法人化に伴い、これまでのセミナーをより強化して誕生してから、毎年4～5回の開催実績があり、協会の常設的な活動として定着したものと考えています。

しかし、ITの世界はシステム技術や利用形態の変化がめざましく、これに対応したシステム監査の方法も日々変化せざるを得なくなっています。

そのため、本セミナーを今後も続けていくためには、これからのシステム監査に即応した教材の改訂や製作が重要であると認識しており、「システム監査普及サービス」を受けていただく被監査企業を発掘し、新たな監査事例の実践を積み重ねていくことが不可欠です。最近、システム監査普及サービスを希望される企業の件数が少なくなっていますので、会員の皆さんから、システム監査を受けたい企業のご紹介をいただければ幸いです。ご協力をよろしくお願いいたします。

北信越支部活動報告

＜福井県例会＞
日時:平成18年6月17日(土)13:00～17:00
場所：福井県民会館　5階会議室

1. 発表
(1) 緊急時対応計画（コンティンジェンシープラン）策定ついて
発表者：角屋　典一　氏
(2)「プライバシーマーク取得」の事例紹介
発表者：伊藤　祐太郎　　氏
(3) C/Sシステムのコントロール手法について
発表者：森　広志　　氏

2. 研究会ビデオの貸出

発表内容：

(1)「金融機関におけるコンティンジェンシープランの策定（FISC版）
福井ネット株式会社　角屋典一

・コンティンジェンシープラン策定の必要性について2004年7月、福井豪雨による弊社の被災状況や福井市のハザードマップによる被害の説明を行い、弊社におけるコンティンジェンシープラン策定の必要性を説明した。
・現在、注目を浴びている事業継続計画(BCP)の各省の対応状況について経済産業省、内閣府、および中小企業庁の「事業継続ガイドライン」の概要と、中小企業庁「中小企業 BCP 策定運用指針」の「チェックシート」により、BCP策定の重要性を説明した。
また、JISQ27002における事業継続管理の定義、また、NIST　SP800－34(NIST:米国国立標準技術研究所)の「IT緊急時対応計画」の概要を説明して、コンティンジェンシープランや事業継続計画に関係する資料を紹介した。
・事業継続管理(BCP)と危機管理計画(CP)の違いについて経済産業省の BCP の定義、FISC の定義などを紹介しながら、FISCのコンティンジェンシープランの範囲はシステムリスクを対象として策定されていることを説明した。
・FISCのコンティンジェンシープラン策定の流れについて各工程に沿って具体的に説明を行った。
第1工程：必要性の認識と推進組織の編成
第2工程：予備調査と基本方針の決定
第3工程：具体的なコンティンジェンシープランの立案
第4工程：コンティンジェンシープランの決定
第5工程：コンティンジェンシープランの維持管理

(2)「プライバシーマーク取得事例」
北銀ソフトウエア　伊藤祐太郎

北銀ソフトウエアのプライバシーマーク（PM）取得活動の事例発表
・2005年8月プライバシーマーク取得プロジェクト結成(12名)
プロジェクト人数を多くし、各部門に情報管理の重要性認識の徹底を図った。
2006年6月認証取得
・個人情報は、各部門単位で取扱・管理の責任を持つ。
・情報管理に関する取扱規定などは従来から決めており、これを一旦2003年に集大成していた。
・さらに2004年個人情報保護法施行に際して、社内組織を変更し情報の取扱・管理、リスク管理・統括を行う部署として、リスク統括部を設置し活動を開始していた。これらを活かし、PM要求に沿った規定などを整備した。
・ISMS要求事項なども確認したが、オーバーラップする部分があるものの ISMS 規定とは相容れない部分も多く、この後考えている ISMS 認証取得時には、改定も必要と思う。
・質疑応答でもこの点の質問があった。
Q: ISMSとPMどちらを先に進めればよいか。
A: 詳細確認していないが、ISMSを先にした方ががよいのでないかとの認識である。

(3)「ITガバナンスに役立つC/Sシステムのリスクコントロールについて」
No.848　森　広志

昨今の情報システムの構成はC/Sシステムとレガシーシステムとの混在となっていると

考え、C/SシステムがITガバナンスに役立つためのリスクコントロール手法を調査した。

JIPDEC平成10年3月発行「クライアントサーバシステム環境下におけるリスクコントロールに関する調査研究報告書」では、「オブジェクト志向モデル」が紹介されている。

業務システムでイベントが発生する都度、KPIの各項目にデータがモニタリングされ、経営指標の達成度を評価し経営活動の統制を行うことで、ITガバナンスに役立つことができる。この「オブジェクト志向モデル」にCOSOモデルを反映し内容の充実を図ったのが、ITガバナンス協会(ITIG)「エンタープライズ・ガバナンス・モデル(Control Objectives for Enterprise Governance)」と考えており、概要について紹介を行った。

私は、このモデルの中にある「ネット中心テクノロジー管理ガイドライン(CONCT)」を不慣れながらインターネットを利用した業務システムの改善に利用したことがあったが、今年に入り「エンタープライズ・ガバナンス・モデル」を知りようやく全体像の把握ができた。今回、COSOモデルの概要を学ぶ機会ができ、内部統制の構成要素である組織コミュニケーションの重要性を認識することができた。今後、システム管理基準と合せ、他基準・ガイドラインの理解に努めていけるようにしていきたいと思います。

＜長野県例会＞

日時　9月16日（土）14：00～17：00
場所　ホテル信濃路（長野市）
内容
1. 近況報告
2. 発表
(1) 金融機関における情報セキュリティ対策について　藤原　康弘　氏
(2) ITガバナンスのためのクライアントサーバシステムの統制について　森　広志　氏
3. ビデオの貸出他

発表内容：

(1) 金融機関における情報セキュリティ対策について

藤原　康弘　氏

金融機関を取り巻く情報セキュリティの中でも、特にキャッシュカードに関する犯罪について傾向と対策について解説された。

欧米と比較して日本では、多額の現金をATMで引き出すことが当然となっていることから、キャッシュカードの盗難や偽造による犯罪が増大し、大きな社会問題となった。

技術的な対策として暗証番号のゼロ暗証化が実施されたほか、ICカード化、生体認証の採用などが進められているが、決め手はまだないのが現状である。

制度的な対策としてキャッシュカードの利用限度額の引き下げ、犯罪防止の取組についての関係機関の連携がある。

また、情報セキュリティ監査によるリスクの洗出しによる対応も必要となっている。

完璧と言える対策はまだないが、預金者がセキュリティについてもっと関心を持ち、技術的・制度的な対策とのバランスを取ってこの問題に対応していくことが大切ではないだろうか。

(2) ITガバナンスのためのクライアントサーバシステムの統制について

森　広志　氏

システム監査の目的として、ITガバナンスへの役立ちが求められるようになってきた。この考えは世界の標準となりつつある。

近年の情報システムは、インターネットを活用した電子商取引もそうだが、基幹システムについてもERPサーバを利用するなど、ネットワークを中心とした情報技術が活用されている。

これらネットワークを中心とした情報技術についてITガバナンスに役立てるためのシステム監査技法の一つに、日本情報処理開発協会が示したオブジェクト指向モデルがあり、更にCOSOフレームワークを基本として発展させたエンタープライズ・ガバナンス・モデルがある。

これらの情報システムの統制方法とITガバナンスへの貢献について検討・提案した。

今後、ITガバナンスに役立ってゆくためには、IT面以外にもビジネス面の理解が必要との認識を得た。

(雑感)

季節によりいろいろな表情を見せてくれる日本海が水平線まで青く続いている。富山の県境を過ぎ直江津（なおえつ）で信越本線に乗り換えた。米どころ新潟の黄金の稲穂が棚田までつづいていて神々しく、収穫の秋に思わず感謝する。緑深い山を超えるとまだ9月だというの

に真っ赤なりんごがあちこちになっている。ようやく長野だ。すっきりした冷気で深呼吸し、きれいに掃除された歩道を行くと目的のホテルに着いた。

当日はいつもより蒸し暑いとのことでおどろいた。

いろいろな人とのご縁を楽しみ、刺激をもらって自分の不勉強を反省するいつもながらの勉強会であるが、ちょっとした旅行気分を味わえるのも地方支部のよさかもしれない。

日本システム監査人協会近畿支部 第97回定例研究会講演録

日時：平成18年7月21日（金）18:30～20:30
場所：国際カンファレンスプラザ17F（大阪本町）
テーマ：「JIS Q 15001:2006改定のポイントと対応策」
講師：キープライバシーソリューションズ代表 芹生　幸治郎（近畿支部会員）

冒頭、吉田支部長より、平成18年度近畿支部総会決定事項（近畿支部会計細則の制定、本年度の活動スケジュール紹介等）について報告があった。引き続き、氏により「JIS　Q 15001：2006」と題する講演が行われた。その要旨は以下の通りである。

1. 改正の概要

今回のJISの主な改正点は、①個人情報保護法で導入された概念の導入・明確化、②個人情報保護法の用語への統一、③マネジメントシステム（PDCAサイクル）の明確化、の3点である。この結果、旧1999年版と新2006年版を比較すると、規格のページ数は5頁から11頁へ、要求事項は25項目から38項目へと増加した。

2. 主な改正点

改正の概要で述べた3つの改正点が、新2006年版のどの項番でどのように表現されているか、要求事項を確認しながら解説された。

3. 改正点とプライバシーマーク（更新）対応

個人情報保護マネジメントシステム（PMS）を構築する目的は何か。それは、「個人の権利・利益を保護するため」であり、また「個人情報の取扱いにおける事故を防止するため」である。プライバシーマークは、そのための手段であることをしっかり認識することが大切である。

では、事業者がPMSを構築し、プライバシーマークの認定を受けるために、特に留意すべきポイントは何か。これを、上記の改正点をふまえて、

①「個人の権利・利益を保護する」観点
②「個人情報の取扱い事故を防止する」観点
③「マネジメントシステムを確立する」観点

の三つにまとめて、自身の豊富なコンサルティング経験をベースに説明された。主なポイントは、個人情報保護の理念、拡大されたリスク概念、個人情報保護管理者の報告義務、計画と目標管理、見落としやすい報告先機関、教育の位置づけと教育内容、従業者や委託先の管理方法、記録を管理する意味、文書管理の方法、ルールを守らせるコツ、運用の確認と監査の関係、是正処置から予防処置への展開、事業の代表者による見直し方法などである。いずれも論点は明快で、具体的事例を交えてわかりやすく説明された。

4. 事故防止の為に

JIPDECが公表した「平成17年度の個人情報の取扱いにおける事故報告にみる傾向と注意点」をもとに、注意すべきポイントとその対策、事故防止に役立つPMS構築の必要性が論じられた。

最後に、個人情報の取扱いにおける事故には、「個人」という被害者が存在するという事実をしっかり認識し、個人情報の有用性に配慮しつつ、個人の権利利益を保護（尊重）しなければならない。事故を防ぐために、継続的かつ組織的に取り組むことが大切である、と締めくくられた。

質疑応答では、参加者の具体的な質問に対して、氏が個人情報保護法の理念を正しく理解すれば判断を大きく誤ることはないという点を強調され、他の参加者にも有意義な議論がなされた。

「個人情報保護管理者／監査責任者の実務」セミナー案内書（富山開催分）

主催　NPO日本システム監査人協会
後援　(財)日本情報処理開発協会／(財)日本データ通信協会／(社)情報サービス産業協会／
(社)日本情報システム・ユーザー協会／情報システムコントロール協会東京支部／
(社)東京グラフィックサービス工業会／システム監査学会／
上級システムアドミニストレータ連絡会

趣旨

このセミナーは、
① 個人情報保護に企業としてどのように対応すべきか
② 新JIS Q 15001個人情報保護マネジメントシステムとは、旧JISとの違い
プライバシーマーク制度の概要と、取得するには
③ 個人情報保護管理者の行う実務
④ 個人情報保護監査責任者の行う実務
を学ぶものです。企業内においてすぐに役立つよう、演習問題も取り入れました。

1. 日程　平成18年11月11日(土)～12日(日)　10時半～17時半
2. 場所　(富山駅前) CICビル3階市民会議室（第4学習室）
〒930-0002　富山市新富町1-2-3　電話076-444-0001
3. 内容

第一日目
1．企業の内部統制と個人情報保護法対応　10:30～12:30
㈱筑波総合研究所　代表取締役　公認システム監査人　打矢　隆司
2．新JIS Q 15001解説とプライバーマーク制度　13:30～15:20
(財)日本情報処理開発協会　プライバシーマーク推進センター
副センター長　関本　貢
3．個人情報保護のための安全管理の実務　15:30～17:30
㈱ビジネスコミュニケーション　代表取締役
公認システム監査人　松枝　憲司

第二日目
1．個人情報保護管理者の実務　10:30～14:00(途中1時間休憩)
んじゃろ監査事務所　代表　公認システム監査人　竹下　和孝
2．個人情報保護監査責任者の実務　14:10～16:50
㈱日立情報システムズ　CSR本部　副本部長
公認システム監査人　一村　義夫
3．確認テスト　16:55～17:30
4．個別相談会　17:30～18:00

4. 参考資料として、JIS Q 15001:2006(日本規格協会発行)を受講者に配布します。
5. 参考資料として、出版物「個人情報保護マネジメントシステム実践マニュアル」
(NPO日本システム監査人協会監修　㈱工業調査会出版)を格安にて提供します
6. 確認テストで一定レベルの内容が確認されたものには、後日、協会会長名の修了証を送ります。
7. 継続教育等の認定
・公認システム監査人・システム監査人補における継続教育時間として認定(12時間相当)
・(依頼予定)ITコーディネータ継続教育（12時間3ポイント分)
8. 受講料　NPO日本システム監査人協会会員及び後援団体の会員　21,000円（消費税込み）
非会員　25,200円（消費税込み）
9. 募集対象人数　30人
10. 担当者連絡先　担当者　蓮見節夫　E-MAILアドレス　hasumi-setuo@nifty.com
11. 申し込み方法
(1)受講料を下記に振り込んでください。

みずほ銀行　北沢支店　普通　口座番号 1053488
口座名義人名　日本システム監査人協会事務局
(2) 申し込み期限　平成１８年１１月８日(水)
(3) 受講料を振り込んだ後、下記の参加申込書を記入し、受講料振り込み票(または振込みを確認できる書類)を添付してFAXで下記あて送付してください。
FAX　03-3666-6342
送付先の宛名　NPO 日本システム監査人協会

ＮＰＯ日本システム監査人協会
「個人情報保護管理者／監査責任者の実務」セミナー申込書（富山開催分）

年　月　日

①会員区分
(1) ＮＰＯ日本システム監査人協会会員
(2) (財)日本情報処理開発協会会員
(3) (社)情報サービス産業協会会員
(4) (社)日本情報システム・ユーザー協会
(5) (財)日本データ通信協会
(6) 情報システムコントロール協会東京支部
(7) (社)東京グラフィックサービス工業会
(8) システム監査学会
(9) 上級システムアドミニストレータ連絡会
(10) いずれの会員でもない

②所属企業名：

③参加者氏名：

④連絡先E-Mailアドレス：

⑤領収書発行希望：あり(あて先：所属企業名／参加者名)　なし

⑥ITコーディネータ継続教育として参加する方：ＩＴＣ認定番号

⑦受講料振込み票(または振込みを確認できる書類)添付

(以上の個人情報は、セミナー受講処理に必要な範囲でのみ使用します)

書籍紹介

『個人情報保護マネジメントシステム　実践マニュアル―JIS Q 15001:2006対応―』

＜CD-ROM「すぐに使える書式・規程のサンプル集」付き＞

日本システム監査人協会　監修

平成18年5月に発表された新JISに対応した個人情報保護の仕組みづくりと運用を平易に解説しています。プライバシーマークの取得と運用のポイントが分かります。

・個人情報保護の仕組みをつくる。
・何から始めるか、どう運用するか、プライバシーマーク取得と取得後のポイントは何か、新JISに対応したマネジメントシステムの実務を網羅。
・CD-ROM「すぐに使える書式・規程のサンプル集」付き。

など、実務者に役立つ「実践マニュアル」として事例を多く取り入れています。
当協会の個人情報保護監査研究会メンバが中心となり執筆しました。(代表　蓮見節夫)

(主要目次)

なお、次のミスが見つかりました。お詫びして、訂正させていただきます。

ページ	正誤の内容
本文39ページ（3）	【誤】4.3.7 ⇒ 【正】3.3.7 【誤】4.4.2.7 ⇒ 【正】3.4.2.7 【誤】4.4.2.8 ⇒ 【正】3.4.2.8 【誤】4.4.3.3 ⇒ 【正】3.4.3.3 【誤】4.7.1 ⇒ 【正】3.7.1 【誤】4.8 ⇒ 【正】3.8
本文123ページ 4.14（1）　2行目	【誤】要求事項3.9は、今までのJIS Q 15001規格になく、JIS Q 15001:2006で新たに設けられた要求事項です. 【正】要求事項 3.9 内の考慮しなければならないとする a) ～ g) 項は、JIS Q15001:2006で新たに加えられた項です.
本文209ページ（2）	【誤】4.3.7 ⇒ 【正】3.3.7
本文209ページ（3）	【誤】4.4.2.8 ⇒ 【正】3.4.2.8
本文209ページ（3） 1行目	『「オプトアウト」の機能が、』の後ろに「一部の例外について」を挿入する
付録CD-ROM	【誤】規程例7-16「苦情及び相談への対応に関する規程」は、内容が、規程例7-20と同じ。 【正】(提供方法を検討中)

新刊紹介

内部統制を高める
ＩＴ統制と監査の実務のＱ＆Ａ

あずさ監査法人 IT監査部（編）

本書は、題名にもあるとおりIT統制における監査について、Q&A方式で書かれた実務書である。

現代の企業において、企業ガバナンス、とりわけ財務報告に係わる内部統制を語るとき、ITによる統制環境を無視することはできない。それどころか、IT統制の欠陥は、そのまま内部統制の欠陥にストレートにつながる可能性が十分にありうる。

内部統制の理解には、まずIT統制の包括的理解が必要不可欠であり、内部統制の評価はIT統制の評価に大きく依存することとなる。本書は、このような認識のもと、内部統制におけるIT統制の役割とその構築のポイント、また、IT統制の評価および監査の進め方とその要点について、実践的な面から解説と実務ノウハウを取り上げている。

アメリカのSOX法を受けて、わが国においても内部統制の重要性が急速に認識されるようになり、日本版SOX法の制定が具体化してきている。そして、内部統制におけるITの活用も重要視されるようになり、IT統制なる用語も頻繁に使われている。このような状況の中で、われわれシステム監査人がどのような役割を果たし、またどのように活動すべきかまだ十分理解できていないのが現実と思われる。

本書は、このような疑問に応えるため48個のQ&A形式で構成されている。本書によりIT統制の中でのシステム監査をどのように位置づけ、どのように対応していけばよいのか一つのヒントを与えてくれる書籍としてここに紹介することとしたい。

本書の構成（目次）は次のとおりである。

第Ⅰ章　IT統制とは（Q1～Q15）
第Ⅱ章　IT統制監査とは（Q16～Q27）
第Ⅲ章　IT全般統制とその監査実務（Q28～Q33）
第Ⅳ章　業務処理統制とその監査実務（Q34～Q41）
第Ⅴ章　その他のIT監査（Q42～Q48）

48個のQ&Aは、最初に題名と同じであるQの部分があり、それに対する回答がAの部分で示され、続いて解説が記述されている。そのため自分の疑問に対するQの題名を探せば、簡単に回答を得ることが可能であり、また、本書の全体を通して読むことにより、IT統制と監査についての手掛かりを得ることも可能である。

第Ⅰ章では、IT統制全般について解説されている。IT統制を「会社レベルのIT統制」、「IT全般統制」、「業務処理統制」に位置づけ、どのように構築すればよいかポイントが解説されている。第Ⅱ章以降は、これらの統制とその監査について、実務に役立つよう監査上の留意点が述べられている。個々のQについては、耳慣れた用語も出ているが、監査に必要な重要ポイントを把握するのには、大変役立つものと思われる。

幾つかのキーワード的なQを紹介すれば、IT統制、SOX法、COSO、日本版SOX法、IT統制の整備計画の策定、IT統制におけるモニタリング、IT統制監査人の要件（当然、公認システム監査人も含まれている）、日本公認会計士協会のIT委員会報告第３号（巻末資料に詳細を掲載）、ITガバナンス監査等々である。

最後に、本書の執筆者の代表は、あずさ監査法人 代表社員 IT監査部長であり、当協会理事の櫻井憲二氏であることを紹介しておきたい。

（データリンクス株式会社　監査室長　岩崎　昭一）

《編集後記》

公認システム監査人特集ということで、今、現場で実践されている方の原稿を頂戴することができました。これで思い出すのが、アメリカ第35代大統領ジョン・F・ケネディの就任演説です。

『わがアメリカ国民諸君、国家が諸君のために何をしてくれるかを問うな。諸君が国家のために何をなし得るかを問いたまえ。』

この言葉のアメリカ国民を日本のIT従事者、国家を公認システム監査人資格に読み替えてみたい気持ちになります。資格というのは、それだけでは何ももたらさないと思います。その資格を育てて、羨望の眼差しで見られるようにするのは、資格者の日々の活動と成果だと思います。

CSAを社会にとって価値あるものにしている投稿していただいた方々や、この制度を育てている協会の方々に敬意を払うとともに、日々活動されている方に、後に続くものに対しての投稿をお願いする次第です。

発行所　特定非営利活動法人 日本システム監査人協会
発行人　鈴木　信夫
事務局　〒103-0025
東京都中央区日本橋茅場町2-8-8
共同ビル（市場通り）6階65号室
TEL. 03(3666)6341 FAX. 03(3666)6342
事務局メール：saajjk1@titan.ocn.ne.jp
ホームページ　http://www.saaj.or.jp/

会報担当委員
竹下　和孝　富山　伸夫
須田　勉　吉田　裕孝
木村　陽一　仲　厚吉
藤野　明夫　森本　哲也
山田　正寛

※会員のみなさまからの投稿（連載、随筆等何でもOK）を募集します。記名記事は謝謝進呈します。書籍紹介欄もありますので、執筆されたかたはお知らせ下さい。
会報担当メール：saaj-kaihoh@yahoogroups.jp