特定非営利活動法人
CSA 日本システム監査人協会報

[第一特集]個人情報保護の最新トピック

個人情報漏洩事故と個人情報保護監査

個人情報保護監査研究会
No.9 蓮見 節夫

2007年3月に、大きな個人情報漏洩事故が公表されています。

一つは、大日本印刷株式会社（以下、D社と略）によるもので「個人情報流出に関するお詫びとお知らせ」が2007年3月12日に同社のホームページに掲載されました。これについては、(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より「認証取消しに次いで重い文書による「改善要請」の処分」を決定し、通知したとの発表が2007年3月23日に同協会のホームページに掲載され、さらに「大日本印刷株式会社からの個人情報漏洩事故について」とする公表文が2007年3月27日に同ホームページに掲載されました。

もう一つは、株式会社ソニーファイナンスインターナショナル（以下、S社と略）の「社員による個人信用情報機関情報の外部流出について」(2007年3月30日)と、UFJニコス株式会社（4月1日以降は三菱UFJニコス株式会社）（以下、M社と略）の「個人信用情報流出の可能性について」(2007年3月30日)とが、それぞれのホームページで発表されています。これについては経済産業省より「クレジット会社2社に対する個人情報保護法34条に基づく勧告」が行われたと同省のホームページで公表されています(2007年3月30日)。このような漏洩事故に対して、システム監査人は、どのように受け止めたらよいのでしょうか。

1．D社個人情報漏洩事故の概要と対策

以下、ホームページ上に公表されている事故の概要です。

D社が業務委託している会社の元社員が、主に販促用DMを取扱う電算処理室内で勤務しており、不正な記憶媒体によるデータ書き出しが行われ、外部に持ち出され、一部情報は詐欺にも使われたものです。持ち出されたデータは2001年～2004年に集中しており、総数7,976,790件となっています。

その間は、監視カメラの設置、生体認証による入退室管理の強化を行っていたが、内部犯行は防げなかった、2004年10月以降「ポケットのない作業服着用によるデータ等の持ち出し防止」「アクセスログの取得」を行った、としています。

個人情報流出の原因として「悪意を持った内部者による不正な記憶媒体によるデータ書き出し行為を防止する上で、結果として管理に不十分な面がありました」としています。

今後の対策として①データ記憶媒体取扱者の極小化と社員限定、また、記憶媒体への書き出しログのチェック頻度を高める、②記憶媒体の書き出し場所の分離と限定、③再発防止策の徹底教育、を行うとしています。

2．S社の事故の概要と対策

S社の発表文による概要と対策の要約です。

「弊社の社員（有期雇用）ならびに派遣社員が、個人信用情報機関の情報の一部を業務目的外で検索し外部に流出させていたことが

目次

判明しました」「これまでの調査により、複数の社員が業務時間中に弊社の情報端末を使って、前記個人情報機関から、不正に個人信用情報を取得し、これを外部の者に提供していたことが確認できました」「弊社は、改めて個人情報の管理体制を全社的に見直し、個人情報の取扱いをより厳格なものとし、社員の教育、監督を徹底してまいります。」

3. M社の事故の概要と対策

M社の発表文による概要と対策の要約です。

「弊社の元嘱託社員が、弊社の保有する個人信用情報、および個人信用情報機関から不正に照会して取得した個人信用情報の一部を特定の第三者に不正に提供していた事実が判明いたしました」「(調査結果) 元嘱託社員はアクセス権限の範囲外であるにもかかわらず、個人信用情報機関にアクセスし、不正に個人信用情報が照会、取得され、外部に流出していることが確認された」「(不正照会の数) 673名様分」「(不正照会の期間) 2004年3月から2007年3月まで」

「(発生原因) 弊社では、必要な範囲にアクセス権限を制限しています。また、指紋認証システムによる入退室管理、私物の持込・持出の禁止、監視カメラの設置、アクセスログの取得など、セキュリティ面の強化を図っており、個人信用情報機関への不正照会を防止する体制を整えておりました。しかし、今回の件については、事件発生時においては、日常業務に紛れた行動であったことから不審な行動の発見には至りませんでした。また、実際の照会業務と照会結果に不正がないか、事後的にチェックする体制が不十分でした」

「(再発防止への取り組み) 1. 信用情報の取扱いに関する緊急の再教育を実施。2. アクセス権限者および照会業務可能端末を必要最低限になるよう絞込む。3. 部署ごとに照会端末の利用記録をシステムに出力し、端末利用者の利用内容と突合させて不正利用がないか事後的にチェックする。」

4. 経済産業省の勧告の内容 (要約)

経済産業省は、S社及びM社に対し、個人情報の保護に関する法律に基づき、法違反状態を是正し法違反行為の再発を防止するよう勧告しました。特にS社については、7日以内に事実関係の追加的な調査結果等を報告するよう併せて勧告しました。認定した違反行為は、個人データの「安全管理措置義務違反」、「従業員の監督義務違反」、「利用目的による制限違反」、「適正な取得義務違反」、「取得に際しての利用目的の通知義務違反」及び「第三者提供の制限違反」です。

S社に対して

(1) 規定に違反したものを特定し、現時点における類似の違反の有無を調査し、違反が行われている場合は、当該違反行為を中止し、当該違反の再発を防止するための必要な措置を講じること

(2) ①従業者による個人データへのアクセス状況の監視の用に供することができる適切な方法により従業者による個人データへのアクセスの記録を行うこと、②個人データへのアクセス記録を確認する等の実効的な方法により従業者による個人データへのアクセス状況の監視を行うこと、③従業者の監督の具体的な実施状況を確認し、実施している安全管理措置及び従業者の監督の内容を改善すること

(3) 勧告に対して取った措置を、平成19年4月27日までに報告すること

M社に対して

(1) 従業者の監督の具体的な実施状況を確認し、実施している安全管理措置及び従業者の監督の内容を改善すること

(2) 勧告に対して取った措置を、平成19年4月27日までに報告すること

5. プライバシーマーク推進センターによる「要請」処分

D社はプライバシーマークの認定を受けている業者です。D社に対して文書による「改善要請」処分が発表されました (2007年3月23日)。その要約です。

以下の6項目に対して1ヶ月以内に改善し、その結果を報告すること。

(1) 本件事故の関連部門について個人情報の取扱いに関する臨時監査を実施すること

(2) 本件事故の原因を特定し、その原因に対して現状の対策が有効であるかの検証をすること

(3) 上記(1)(2)の結果を踏まえて現状の措置が有効でないと判断できるリスクに対して、必要な対策を検討すること。この場合、従業者の個人情報の無断・不正持出を防止する措置については特に留意すること

(4) 本件事故以外の個人情報の取扱いについて、リスク分析を実施して現状の管理の仕組みを点検し、不具合が認められたところについては、改善策を検討して講じること

(5) 以上の事項に関する見直し結果については、個人情報保護マネジメントシステム文書に適切に反映し、関連する全従業者及び委託先事業者に周知・徹底す

ること
(6) マネジメントシステムの根幹である継続的改善が有効に機能するように対応策を検討し、環境変化に応じた適切な安全管理措置が講じられるようにすること

6. プライバシーマーク推進センターの対応

プライバシーマーク推進センターでは、2007年3月27日の公表文において、以下の対応を発表しています。

制度の信頼確保に全力を尽くします：
- 公表される事故等の状況を踏まえ、注意喚起等手段を通じて情報提供を積極的に実施し、認定事業者に適切な対応を求めます
- 環境変化を踏まえた審査基準の在り方を随時検討し、その結果を審査業務に反映し、時代の要請に適切に対応した保護策の実現を図ります
- 審査員制度の下で審査員の質の向上を図り、更に審査員教育を充実する等審査能力の維持・向上に努め、審査結果の信頼性の確保を図ります
- IT等の進展を踏まえた適切な対応を促すために、セミナー、研究会の実施等によって認定事業者の啓発活動を促進します
- 苦情処理活動を通じて認定事業者の指導・監督を充実し、個人情報保護活動の充実を図ります

制度の改革を検討します：
- 認定事業者の運用状況を定期的に監視・監督する制度
- 事故や事件を起こした事業者に対して、一定期間の後に現地審査によって改善措置の実行状況を確認する制度
- 大規模な個人情報取扱い事業者に対する適正な現地審査のあり方
- 内部監査担当者の監査知識・能力を客観的に評価する仕組

7. 個人情報保護監査実施上の教訓

われわれシステム監査人は、個人情報保護監査に直接、間接にタッチすることが多い。また、プライバシーマーク推進センターの制度の改革の中で「内部監査担当者の監査知識・能力を客観的に評価する仕組」を挙げており、われわれシステム監査人に期待されている部分も多くあります。

この事故の中で、どのような教訓を得ることができるでしょうか。

JIS Q 15001 個人情報保護マネジメントシステムの中で、事故との関係で特に重要なところがあります。

(1) 目的外利用を行わないための仕組み

「事業者は、特定した個人情報について、目的外利用を行わないため、必要な対策を講じる手順を確立し、かつ、維持しなければならない」ことを求めています。ここは、2006年版になって追加された要求事項です。これを単なるお題目で終わらせないためには、更に具体化する必要があります。①個人情報の利用目的を特定し関係者に周知しておくこと。②目的外利用をさせないための技術的・物理的対策。たとえば、アクセス制限や入退室制限など。③従業者の監督。④制度的な面としては目的外利用かどうか曖昧な場合は、管理者と相談するなど。⑤事後的なチェックとしてはアクセスログの点検、入退室記録の点検などの日常点検。このとき、問題発見の感度の向上。問題かなと思ったときの報告制度など

(2) リスクなどの認識、分析及び対策の中のリスク分析の仕組み

「事業者は、特定した個人情報について、その取扱いの各局面におけるリスクを認識し、分析し、必要な対策を講じる手順を確立し、かつ、維持しなければならない」ことを求めています。これも形が整っていれば良いというものではありません。具体的に詳細に個人情報の取扱いの行われている全ての局面のリスクが洗い出される必要があります。担当者が直接タッチしていないところが抜けることがままあります。外注先、移動中、通信or通信の途上、アウトソースされたサーバの中、メールサーバの中、廃棄処理、出先の無人店舗、室、建物、周辺環境などです。

リスク分析は、コンサルタントなどの外部の者にまかせっきりというのはダメです。実際にその仕事にタッチしている人たちを巻き込んで行うことで、隠れたリスクを発見したり、取扱者の意識を高めることができます。

リスク分析をした結果は、リスク対策を行い、必要な規程に反映します。また、企業の体力との関係で100%完全な対策はできませんから、残存リスクを認識しておくことも重要です。リスク対策は、経済産業省の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」(2007年3月30日改正)、金融庁の「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」、厚労省「医療情報システムの安全管理に関するガイドライン」、日本工業標準調査会の「JIS Q 27001 情報セキュリティマネジメントシステム要求事項」の付属書A「管理目的及び管理策」などを参考にして、自社の実態に即した内容で定めます。

リスク分析は、公表された事故の情報なども、自社に当てはめて該当する問題はないか、見直すことも必要です。

(3) 安全管理措置

「事業者は、その取扱う個人情報のリスク

に応じて、漏えい、滅失又はき損の防止その他の個人情報の安全管理のために必要、かつ、適切な措置を講じなければならない」としています。ここは、リスク分析の結果としてのリスク対策が反映されるところです。目的外利用をさせないための物理的、技術的な仕組みもこの中に組み込みます。

安全管理措置は、具体的に規程等に折り込み、関係する人たちに周知しておきます。また、その通りに実施されているかをチェックするための日常点検も組み込みます。

(4) 従業者の監督

「事業者は、その従事者に個人情報を取扱わせるに当たっては、当該個人情報の安全管理が図られるよう、当該事業者に対し必要、かつ、適切な監督を行われなければならない」としています。具体的には、誓約書もありますが、上司等との日常的な、報告、連絡、相談の仕組みがあり、かつ機能していることです。監査の点からはなじみにくいのですが、縦・横のコミュニケーションができており、目標に向かって協働できている職場では、内部犯行は起きにくいものです。一人ひとりが孤立し、ぎすぎすした職場の雰囲気があるところは要注意です。

(5) 委託先の監督

個人情報の取扱いを委託する場合は、十分な個人情報の保護水準を満たしている者を選定する基準を確立すること、個人情報の安全管理が図られるよう委託先の監督を求めています。委託契約書においても、個人情報の取扱いについての条項を入れることを求めています。委託先での個人情報の取扱いについて、必要な頻度で監査・点検ができる仕組みも必要です。

委託先選定基準も、単に形式的に作成するだけではだめです。委託する業務内容や、個人情報の取扱い方によって、リスクが違いますから、取るべき安全対策も異なるものです。委託する側で、必要と思われるチェック項目を用意し、安心して個人情報の取扱いを任せられるかを判断します。プライバシーマークやISMSの認定事業者であればOKとしてしまうのではなく、具体的に一つ一つの項目をチェックすることが必要です。

委託先に渡す個人情報は、必要な範囲に限定して渡します。

(6) 教育

教育では、a) 個人情報保護マネジメントシステムに適合することの重要性及び利点、b) 個人情報保護マネジメントシステムに適合するための役割及び責任、c) 個人情報保護マネジメントシステムに違反した際に予想される結果、を行うことを求めています。

特に、取扱っている個人情報の利用目的を理解すること、定められた手順に従って取扱うこと、それが目的外利用を阻止する仕組みでもあること、日常活動の中で、"変だな"と思ったことはいつでも上司と相談すること、など、基本的な勤務動作に繋がっています。

(7) 運用の点検

個人情報保護マネジメントシステムが適切に運用されていることが各部門及び階層において定期的に確認されるための手順の確立を求めています。

具体的には、日常点検や、チェックリストに基づく自己点検などです。最終退出時の社内点検の記録と確認、最初に出社した人と最後に退社した人の記録と確認、情報システムへのアクセスログの取得と点検などです。

ここでも点検者は、"異常"、"問題"、"普段と異なる傾向"などへの感度を高める必要があります。何年にもわたって不正アクセスが行われていたにもかかわらず、外部から指摘されなければ気が付かないというのは、記録・点検が、お座なりにしか行われていなかったのではないでしょうか。

(8) 監査

内部監査も、何年にもわたって不正アクセスが行われていたにもかかわらず、気が付かないというのは、反省すべき点が多々あるのでしょう。

当然監査人は、以上に述べてきた事柄について、すべて監査項目として、問題点を指摘できる能力を要求されています。そのためには、JISの要求事項や、内部規程のみでなく、技術の進歩や、社会の事件・事故の教訓を自ら取り入れ、不適合や不正に対する感度を高める必要があります。もちろんのこと、経験の積み重ねも必要です。

以上、システム監査人として、事故の教訓を自ら取り込むべく、自分自身の反省も含めてまとめてみました。

(記：平成19年4月17日)

「個人情報保護に関する法律についての経済産業分野を対象とするガイドライン」の改正について

個人情報保護監査研究会
会員 no.9 蓮見 節夫

平成19年3月30日に経産省ホームページに「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」の改正版が掲載されました。

ここに改正の概要をまとめましたので、ご紹介します。

1．「過剰反応」に対する見直しが行われました

本人の同意を得ることなく個人データを第

三者に提供できる事例として二つ追加されました。

(1) 法令に基づく場合の例の追加。弁護士会からの照会に基づく個人情報の提供

(2) 人の生命、身体又は財産の保護の例の追加。リコール対象製品を回収するための、販売店から製造元への顧客名簿の提供

2．個人情報取扱事業者の過剰な負担の適正化に向けた見直しが行われました

個人の権利利益の侵害のおそれが少ない個人情報の取扱に関する事例が明示されました。

(1) 安全管理措置の義務違反とならない事例として二つ明示されました。

①内容物に個人情報が含まれない荷物の宛名に記載された個人データに関する事例

②書店で誰もが容易に入手できる市販名簿に関する事例

(2)「事故又は違反への対処」を実践するための講じることが望まれる手法が例示されました

①影響を受ける可能性のある本人への連絡について、本人への連絡を省略してもかまわないものと考えられる事例が追加されました。

・紛失した個人データを、第三者に見られることなく、速やかに回収した場合

・高度な暗号化等の秘匿化が施されている場合　など

②主務大臣等への報告について、認定個人情報保護団体の対象事業者は、主務大臣への報告に代えて、認定個人情報保護団体への報告が可能になりました。ただし、特定の機微な個人情報、信用情報、クレジットカード情報が漏えいし、二次被害が発生する可能性が高い場合等は、主務大臣に速やかに報告することが必要です。

③事実関係等の公表を省略してもかまわないものと考えられる事例が明示されました。

・本人すべてに連絡が付いた場合

・高度な暗号化等の秘匿化が施されている場合　など

3．クレジットカード情報を含む個人情報の取扱に関して

別添「クレジットカード情報を含む個人情報の取扱について」が付いて、安全管理措置として講じることが望ましい事例が追加されました。

・クレジットカード情報等の保存期限の設定、保存期限経過後の速やかな廃棄

・クレジット売上伝票に記載されるクレジットカード番号を一部非表示化など

4．その他

①利用目的の特定について、業種の特定だけでは、多くの場合、利用目的をできる限り特定したことにはならない旨が明示されました。

②利用目的の通知又は公表が必要な事例として、個人情報の取扱の委託を受けて、個人情報を取得する場合が追加されました。

③個人情報に関する非開示契約は、必ずしも全ての従業者と個別に契約を締結する必要はなく、就業規則等の社内規定による包括的な契約を締結する方法でも差し支えない旨が明示されました。

④委託先の監督について、優越的地位にある者が委託者の場合に、受託者に不当な負担を課している例として、本人からの損害賠償に係る責務を、安全管理措置に係る責任分担を無視して一方的に課す場合が明示されました。

⑤開示等の求めに応じる手続きについて、事業者は本人確認のために、事業者が保有している個人データに比して過剰な情報を求めるなど、本人確認のために必要以上に多くの情報を求めてはならないことが明示されました。

「個人情報保護マネジメントシステム実践マニュアル」への追補

「個人情報保護マネジメントシステム実践マニュアル」を平成18年9月に上梓しました。その後、2006年版に基づく個人情報保護マネジメントシステム（ＰＭＳ）構築の経験の積み重ね、JIPDECの「JISQ15001:2006をベースとした個人情報保護マネジメントシステム実施のためのガイドライン」の検討、読者からの問合せやご意見、最近の重大な漏洩事故の原因分析などの経験を積みました。

こうした経験を踏まえ、ここに追補及び付録ＣＤ改訂版をお送りします。

平成１９年５月１３日

ＮＰＯ日本システム監査人協会・個人情報保護監査研究会

【本文への追補】

特に重要な文書作成上及び運用上のポイント、注意すべき事項を追加します。

1. 適用範囲

全従業者を適用範囲に定め、事業の用に供している個人情報を適用対象と定めて、運用します。倉庫業者が扱う引き受け荷物のように、事業の用に供してはいないが、お客様から機密扱いを要求されているものなどは、個人情報と同様に、リスクの認識、及びリスク対策を実施することが望ましいといえます。

2. リスクなどの認識、分析及び対策

(1) 基本規定の中などで、目的外利用を行わないため、必要な対策を講じる手順を確立し、かつ、維持することを規定します。目的外利用を起こさせないための手順は、個人情報を特定するための手順、リスクなどの認識、分析及び対策の手順、個人情報の取得、利用及び提供に関する規定、教育に関する規定、点検に関する規定、などの中に組み込みます。

(2) 特定した個人情報について、ライフサイクルに応じてリスクを洗い出し、リスク分析を実施し、リスクへの対策を講じ、残存リスクを認識する手順を規定し、運用します。この部分は特に重要で、単に形が整っているだけで済ますことなく、自社の個人情報の取扱い状況を細かく把握し、潜んでいるリスクを洗い出します。

事故事例などを分析して、次のところなどに抜けがないか、検討します。ＡＴＭなどのように外部に設置されているところ、委託先、移動中、自宅での持ち帰り作業、アウトソーシング先、通信ネットワーク、外部に置かれたウェブサーバー、送付物の宛先ミス、入れ違い、権限外のアクセス、個人情報の作業場所や保管場所などの環境（部屋、建物、周辺環境）など。

(3) リスク対策については、目的外利用を起こさせない仕組みも必要です。リスク対策については、規定、手順書、マニュアル、通達文書、教育テキストなどの中に具体的に反映されていることが必要です。

3. 計画書

教育計画書と監査計画書は、代表者の承認を得ることと、少なくとも年１回以上実施します。

4. 特定の機微な個人情報の取得、利用及び提供の制限

従業者の健康情報については、厚労省の「雇用管理に関する個人情報のうち個人情報を取扱うに当たっての留意事項について」に従います。

認証システムのために生体認証を取得する場合は、本人の明示的な同意が必要です。

5. 本人から直接書面によって取得する場合の措置

本人から直接書面によって取得する場合は、必要事項を書面により明示し、同意を得て収集します。「同意」は第三者から見て同意したことが明確でなくてはなりません。手順は、取得する手段ごと（紙に記載する場合、ウェブからの場合など）に手順を定めます。

6. 利用に関する措置

特定した利用目的の達成に必要な範囲内で個人情報を利用するという原則を規定します。

目的外利用に該当するかどうか判断に迷う場合、管理者の判断を求めるよう規定します。利用目的を変更する場合の承認手順を規定します。

7. 安全管理措置

事業者は、その取扱う個人情報のリスクに応じて、個人情報の安全管理のために必要、かつ、適切な措置を講じます。リスクに応じてとは、リスクなどの認識、分析及び対策の中で必要としたリスク対策を安全管理措置の中に組み込むことです。

何を持って「適切な措置」と見なすかは、取扱う個人情報の内容や量によって、また事業規模や業務内容によって異なるものであり、事業者自身で判断することになります。結果として問題

を起こさせないことが重要です。過去の事故事例や、他社の事故事例などを参考にして自社の「適切な措置」のレベルを判断し、実施します。

権限を持った者からの漏洩事故は、大きな事故になる可能性があります。アクセス権限の付与の範囲の絞込み、パスワードの管理、アクセスログの取得と点検などもポイントの一つです。

8. 委託先の監督

委託先選定基準は、具体的には、委託業務についての個人情報取扱の水準を評価して、委託先として適切であるかどうかを判断することです。ここでも単に形式的に手続がとられていれば良いとするのではなく、個人情報取扱のリスク分析の結果を反映して、具体的な取扱のポイントごとのチェック項目を挙げて、安心して委託できるかどうかを判定します。Ｐマーク認定事業者かＩＳＭＳ認定事業者であることは、判断の一つとしてはよいのですが、具体的なチェック項目にしたがって、評価することが大事です。委託先で講じた安全管理措置が適切であるとの判断は委託先での判断であり、委託元で必要とする安全管理措置の適切であるとの判断が一致するとき限らないからです。したがって、選定基準は、委託する業務内容によって異なるものであり、過去の事故事例なども参考にし、自社の基準で適切な水準を設定します。

委託先に個人情報を預託する場合、委託業務に必要な個人情報に限定して預託します。

9. 個人情報に関する本人の権利

個人情報保護法では、保有個人データとしていますが、JIS Q 15001 では、開示対象個人情報としていますので、その違いを認識してください。具体的に自社の開示対象個人情報は何かを認識します。

10. 是正処置及び予防処置

不適合に対する是正処置及び予防処置を確実に実施するための責任及び権限を定める手順を規定します。

この規程が適用される場面として、外部機関による審査による指摘事項、親会社や委託元からの指摘事項、リスクなどの分析において発見された不備事項、緊急事態の発生、苦情、運用の確認において発見された不備事項、監査による指摘事項、外部の事故事例からの教訓などがあります。それぞれの場面の中で、是正処置及び予防処置手順を適用することを規定します。

従来、監査規程の中に是正処置手順を規定していた場合、別にすることが望ましいといえます。

11. 事業者の代表者による見直し

事業者による見直しは、具体的に時期を明確にします。

事業者の代表者による見直しは、運用点検に伴う是正や、監査に基づく是正処置とは異なります。

【付録ＣＤ改訂版について】

1. 付録CD「すぐに使える書式・規程のサンプル集」の内容

付録ＣＤ改訂版には、次の書式、規程のサンプルを収録しています。

財団法人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編「個人情報保護マネジメントシステム実施のためのガイドライン」（日本規格協会）に対応しています。

f1	＜個人情報保護方針等＞	
f1-1	規程例 7-1	個人情報保護方針
f1-2	規程例 7-2	個人情報保護基本規程
f2	＜内部規程例＞	
f2-1	規程例 7-3	個人情報を特定する手順に関する規程
f2-2	規程例 7-4	法令、国が定める指針及びその他の規範の特定、参照及び維持に関する規程
f2-3	規程例 7-5	個人情報に関するリスク分析と対策の手順に関する規程
f2-4	規程例 7-6	事業者の各部門及び階層における個人情報を保護するための権限及び責任に関する規程
f2-5	規程例 7-7	緊急事態への準備及び対応に関する規程

f2-6	規程例 7-8	個人情報の取得・利用及び提供に関する規程（中･小規模事業社向け）
f2-7	規程例 7-9	個人情報の取得・利用及び提供に関する規程（中・大規模事業者向け）
f2-8	規程例 7-10	入退館管理規程
f2-9	規程例 7-11	入退室管理規程
f2-10	規程例 7-12	情報システム安全管理規程
f2-11	規程例 7-13	業務委託管理規程
f2-12	規程例 7-14	本人からの開示等の求めへの対応に関する規程
f2-13	規程例 7-15	個人情報保護に関する教育の規程
f2-14	規程例 7-16	個人情報保護マネジメントシステム文書の管理に関する規程
f2-15	規程例 7-17	苦情及び相談への対応に関する規程
f2-16	規程例 7-18	個人情報保護における運用の確認に関する規程
f2-17	規程例 7-19	個人情報保護内部監査規程
f2-18	規程例 7-20	是正処置及び予防処置に関する規程
f2-19	規程例 7-21	代表者による見直しに関する規程
f2-20	規程例 7-22	内部規程の違反に関する罰則の規程
f3	＜チェックリスト例＞	
f3-1	ﾁｪｯｸﾘｽﾄ例 7-1	委託先選定チェックリスト
f3-2	ﾁｪｯｸﾘｽﾄ例 11-1	部門別運用確認チェックリスト
f3-3	ﾁｪｯｸﾘｽﾄ例 11-2	安全管理措置確認チェックリスト
f3-4	ﾁｪｯｸﾘｽﾄ例 11-3	適合性監査チェックリスト
f3-5	ﾁｪｯｸﾘｽﾄ例 11-4	運用監査チェックリスト
f4	＜その他サンプル＞	
f4-1	その他 7-1	従業員、アルバイト等の誓約書
f4-2	その他 7-2	個人情報の取扱いに関する覚書
f4-3	その他 7-3	個人情報の取り扱いについての公表文例
f4-4	その他 7-4	個人情報の利用目的等の通知書兼同意書の文例
f4-5	その他 7-5	個人情報を直接書面以外の方法によって取得する場合の利用目的の公表文書の例
f4-6	その他 7-6	個人情報を直接書面以外の方法によって取得する場合の利用目的の通知文書の例

f4-7	その他 7-7	特定した利用目的の達成に必要な範囲を超えて個人情報を利用する場合の通知文書兼同意書の例
f4-8	その他 7-8	個人情報の開示請求等への回答書の文例
f4-9	その他 7-9	個人情報保護マネジメントシステム文書・書式管理台帳の記入例
f4-10	その他 8-1	従業員 100 人規模の運用体制の例
f4-11	その他 8-2	従業員 10 人規模の運用体制の例
f4-12	その他 9-1	○○年度教育計画一覧／○○年度教育計画の記入例
f5	＜様式例＞	
f5-1	様式例 7-1	個人情報管理台帳
f5-2	様式例 7-2	個人情報に関する法令および規範の一覧表
f5-3	様式例 7-3	個人情報のリスク分析表
f5-4	様式例 7-4	個人情報事故緊急連絡網
f5-5	様式例 7-5	個人情報事故報告書
f5-6	様式例 7-6	事故・事件発生速報
f5-7	様式例 7-7	個人情報新規取得申請書
f5-8	様式例 7-8	個人情報第三者提供申請書
f5-9	様式例 7-9	個人情報目的外利用申請書／アクセス利用申請書
f5-10	様式例 7-10	個人情報の授受記録
f5-11	様式例 7-11	個人情報提供記録
f5-12	様式例 7-12	個人情報保管記録
f5-13	様式例 7-13	データ送信記録受領確認書
f5-14	様式例 7-14	廃棄証明書
f5-15	様式例 7-15	預託個人情報管理台帳
f5-16	様式例 7-16	個人情報消去・廃棄記録
f5-17	様式例 7-17	預託個人情報返却届け
f5-18	様式例 7-18	受託個人情報管理台帳
f5-19	様式例 7-19	個人情報新規取得申請書
f5-20	様式例 7-20	個人情報取扱基準書
f5-21	様式例 7-21	例外的に特定の機微な個人情報を取得、利用又は提供する場合の処置について

f5-22	様式例 7-22	本人から直接書面によって取得する場合の処置について
f5-23	様式例 7-23	個人情報を直接書面以外によって取得する場合の処置
f5-24	様式例 7-24	特定した利用目的の達成に必要な範囲を越えて個人情報を利用する場合の申請書
f5-25	様式例 7-25	個人情報を利用して本人にアクセスする場合の申請書
f5-26	様式例 7-26	個人情報を第三者に提供する場合の処置について
f5-27	様式例 7-27	入退館記録（兼退館時チェックリスト）
f5-28	様式例 7-28	訪問者入退館記録簿
f5-29	様式例 7-29	サーバー室入退記録簿
f5-30	様式例 7-30	出入口開錠施錠記録簿
f5-31	様式例 7-31	アクセス用ＩＤ管理簿
f5-32	様式例 7-32	携帯用パソコンおよび磁気媒体管理簿
f5-33	様式例 7-33	個人情報格納磁気媒体管理台帳
f5-34	様式例 7-34	開示等受付報告書
f5-35	様式例 7-35	個人情報に関する申し立て申請書
f5-36	様式例 7-36	○○年度教育計画一覧／教育計画書
f5-37	様式例 7-37	教育実施記録
f5-38	様式例 7-38	個人情報保護マネジメントシステム文書・記録廃棄記録
f5-39	様式例 7-39	個人情報保護マネジメントシステム文書管理一覧表
f5-40	様式例 7-40	個人情報保護文書管理台帳
f5-41	様式例 7-41	個人情報保護記録管理台帳
f5-42	様式例 7-42	個人情報の苦情・相談お問合せ対応記録
f5-43	様式例 7-43	運用確認年度計画書
f5-44	様式例 7-44	部門運用確認結果報告書
f5-45	様式例 7-45	全社運用確認結果報告書兼改善指示書
f5-46	様式例 7-46	監査基本計画書
f5-47	様式例 7-47	監査報告書兼改善指示書
f5-48	様式例 7-48	是正処置及び予防処置の管理表
f5-49	様式例 7-49	是正処置及び予防処置の管理様式例

f5-50	様式例 7-50	是正処置及び予防処置報告書
f5-51	様式例 7-51	マネジメントレビュー議事録
f5-52	様式例 7-52	代表者による見直し実施記録

2. 付録ＣＤ「すぐに使える書式、規程のサンプル集」の使用上の注意事項
① 動作環境
付録ＣＤの内容は、米Microsoft社製のExcelファイル又はWordファイルで作られています。Microsoft Windows XPで動作確認をしています。それ以外については動作確認をしておりません。
② 付録ＣＤの内容の印刷結果については、使用するＯＳやExcel、Wordのバージョンおよびプリンタ環境などによって異なります。各自調整のうえ使用してください。
③ 付録ＣＤの著作権は、ＮＰＯ日本システム監査人協会にあります。
④ 付録ＣＤを複製し販売することを禁止します。
⑤ 付録ＣＤの内容を、組織内において使用する場合、組織の実態に合わせて、修正されることをお勧めします。

3. 付録ＣＤの編著者名
一村義夫／梅津尚夫／小野修一／力　利則／高井憲彦／仲　厚吉／蓮見節夫／
馬場孝悦／原　純江／松枝憲司（アイウエオ順）

4．付録ＣＤ「すぐに使える書式、規程のサンプル集（JIPDEC「個人情報保護マネジメントシステム実施のためのガイドライン）対応版」の申し込み方法
・「個人情報保護マネジメントシステム構築のための実務者養成セミナー」参加者に資料として配布します。
・付録ＣＤのみをご希望の方は、資料代として2,420円（税込み）を下記に振り込み、FAXで申し込んでください。
三菱東京ＵＦＪ銀行 浜松町支店　普通　口座番号　4581613
口座名義人名　日本システム監査人協会 個人情報保護監査研究会 理事 蓮見節夫
ＦＡＸ　03-3666-6342
あて先　ＮＰＯ日本システム監査人協会　PMSセミナー係
FAXには、申し込み内容、送付先郵便番号・住所、電話番号、氏名、連絡用e-mailアドレスを明記し、振込み票（または振込みを確認できる書類）の写しを添付してください。

1日でわかる 最新版

「個人情報保護マネジメントシステム構築のための実務者養成セミナー」のご案内

最近でも、個人情報の大量の漏洩事件が発生しています。セキュリティ対策に際限なく費用がかかるなど、マネジメントシステムの確立の重要性がさらに重要になっています。このセミナーは、JIPDECの「実施のためのガイドライン」、及び個人情報保護マネジメントシステム（ＰＭＳ）構築の経験を持つベテラン講師によるPMS構築・新JIS移行のポイントを中心に講義します。ＰＭＳ構築を目指す経営者、推進担当者、個人情報保護管理者、監査責任者等、すぐに役立つセミナーです。（各ご後援団体から推薦頂いています!!）

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／(社)日本印刷産業連合会／(社)コンピュータソフトウェア協会／(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／(財)日本データ通信協会／(社)東京グラフィックサービス工業会／情報システムコントロール協会東京支部／システム監査学会
1. 日程	6月27日(水) 10:00~17:00 (9:45より受付開始します)
2. 場所	機械振興会館 B3-2号室 〒105-0011 東京都港区芝公園3-5-8 案内図 http://www.jcmanet.or.jp/gaiyo/map_kaikan.htm
3. 内容 (1)	10:00 ～ 12:00 「個人情報保護マネジメントシステム実施のためのガイドライン」を中心として 講師 (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
(2)	13:00 ～ 16:30 「個人情報保護マネジメントシステム構築と新JIS対応の実務」 新JISによる申請／個人情報保護方針・個人情報保護基本規程の内容／リスクの分析・評価、および個人情報の取得、利用、アクセス及び提供／ＰＭＳ文書作成上の留意点> 講師 公認システム監査人 データリンクス株式会社 岩崎 昭一
(3)	16:30 ～ 17:00 個別相談会(希望者のみ)
4. セミナー時の必要テキスト	①「個人情報保護マネジメントシステム実施のためのガイドライン」 (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編 日本規格協会発行) セミナー参加者特別販売価格：1,596円(税込み)、 定価：1,995円)(税込み) ②「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) セミナー参加者特別販売価格：3,360円(税込み)、定価：4,200円(税込み) ③CD-ROM「すぐに使える書式・規程のサンプル集 (JIPDEC「個人情報保護マネジメントシステム実施のためのガイドライン」対応版)」受講者に配布します
5. 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 (６時間相当) ・ＩＴコーディネータ継続教育 (６時間相当)
6. 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（会員企業内の個人を含む）20,000円（消費税込み） 非会員は、 24,000円（消費税込み）
7. 募集人数	30人
8. 担当者連絡先	〒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)NPO日本システム監査人協会 担当者 蓮見節夫 E-MAILアドレス hasumi-setuo@nifty.com
9. 申し込み方法	(ＮＰＯ日本システム監査人協会ホームページ http://www.saaj.or.jp/ にも掲載しています) (1)受講料を下記に振り込んでください。 三菱東京ＵＦＪ銀行 浜松町支店 普通 口座番号 4581613 口座名義人名 日本システム監査人協会 個人情報保護監査研究会 理事 蓮見節夫 (2)申込期限 平成１９年６月２２日(金) (定員に達した場合、上記ホームページに掲載) (3)受講料を振り込んだ後、下記の参加申込書に必要事項を記入し、受講料振り込み票の写し(または振込みを確認できる書類)を添付して、下記あてＦＡＸ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 PMSセミナー係

＊　セミナーに参加できないが、CD-ROM「すぐに使える書式･規程のサンプル集（JIPDEC「個人情報保護マネジメントシステム実施のためのガイドライン」対応版)」を希望する方には、資料代 2,420 円（送料込み、税込み）で提供します。
ご希望の方は、資料代（CD-ROM）として 2,420 円（税込み）を下記に振り込み、FAX で申し込んでください。

三菱東京ＵＦＪ銀行 浜松町支店　普通　口座番号　4581613
口座名義人名　日本システム監査人協会 個人情報保護監査研究会 理事 蓮見節夫
ＦＡＸ　03-3666-6342
あて先　ＮＰＯ日本システム監査人協会　PMS セミナー係

FAX には、申し込み内容、送付先郵便番号・住所、電話番号、氏名、連絡用 e-mail アドレスを明記し、振込み票（または振込みを確認できる書類）の写しを添付してください。

－－－－－－－－－－－－－－－－－－ FAX 送信用 －－－－－－－－－－－－－－－－－－

ＮＰＯ 日本システム監査人協会 宛

ＦＡＸ　03-3666-6342
年　　月　　日

「個人情報保護マネジメントシステム構築のための実務者養成セミナー」申込書

①会員区分　(1)ＮＰＯ日本システム監査人協会 (2)(財)日本情報処理開発協会 (3)(社)日本印刷産業連合会 (4)(社)コンピュータソフトウェア協会 (5)(社)情報サービス産業協会	(6)(社)日本情報システム・ユーザー協会 (7)(財)日本データ通信協会 (8)(社)東京グラフィックサービス工業会 (9)情報システムコントロール協会東京支部 (10)システム監査学会
②金額の確認 受講料　20,000 円　会員区分（　　）(1)から(10)のいずれか 24,000 円　会員区分①の（1）から(10)に該当しない方 [要／不要]　1,596 円「個人情報保護マネジメントシステム実施のためのガイドライン」 [要／不要]　3,360 円「個人情報保護マネジメントシステム実践マニュアル」 合計　　円	
③所属企業名： (個人の場合は不要)	
④参加者氏名：	
⑤連絡先 e-mail アドレス：	
⑥領収書発行希望：　あり（あて先：所属企業名／参加者名）　なし	
⑦ＩＴコーディネータ継続教育として参加する方：　ＩＴＣ認定番号	
⑧受講料振込み票（または振込みを確認できる書類）を添付してください	
＊ CD－ROM の送付のみを希望する方 送付先郵便番号・住所： 電話番号： 氏名： 連絡用 e-mail アドレス：	

（この個人情報は、振り込み確認及び CD 送付のためにのみ使用します）

[第二特集]支部の活動

中部支部 2006年度 合宿報告

中部支部では11月18日、11月19日の2日間で恒例の合宿を開催しました。例年同様、今年も日本システムアナリスト協会中部支部との共同で開催しました。(以下、敬称略)

1．はじめに（当日のあいさつ）

NPO日本システム監査人協会
中部支部長　若原 達朗

恒例となったＳＡＡＪ／ＪＳＡＧ中部支部合同の合宿を今年も開催することができたことをうれしく思います。これも参加いただいたみなさま、特に開催に向けて努力いただいた合宿委員の方のおかげと、とても感謝しています。ありがとうございました。

さて、今回のテーマは「地方自治体におけるセキュリティ監査・システム監査の取り組みについて」ということで、最近では自治体でのセキュリティ監査、システム監査の事例も増えてきています。１日目の講演では、その実態を現場で実際に業務にあたっている方々からお話を伺える機会を設定していただきました。このような機会は、私達システム監査人にとって、とても貴重なものであると考えています。参加されたみなさまのお役に立てれば幸いです。

また来年、ＳＡＡＪ設立２０周年を迎えることもあり、２日目の演習ではこれからの支部運営についても検討して行きたいと思います。地方支部には地方支部の悩みがありますが、参加いただいたみなさまの知恵をお借りして、支部会員に役立つ活動としていきたいと考えています。こちらについても、合宿の中だけにとどまらず、今後さらに活発な議論を期待しています。ぜひご意見をお聞かせ下さい。

2．開催概要

(1) 日時：11月18日(土)13時～19日(日)12時
(2) 場所：岐阜県大垣市 ワークショップ24　工房2
(3) 宿泊：ワークショップ24　ソピア･キャビン
(4) テーマ:地方自治体におけるセキュリティ監査･システム監査の取り組みについて
(5) 参加人数：25名
(6) 参加費用：SAAJ/JSAG会員　10,000円

3．スケジュール

＜11月18日（土）＞

13:00　受付開始
13:30～14:15　開会挨拶、本年度活動報告、来年度計画（SAAJ/JSAG）
14:15～15:15　基調講演
『下呂市におけるISMSの取り組みについて』
下呂市企画部情報課課長補佐　桂川国男
15:30～16:30　講演(1)
『地方自治体における情報セキュリティ監査』
SAAJ中部支部　田中　勝弘
16:45～17:45　講演(2)
『岐阜県におけるITガバナンスの取り組みについて』
JSAG・SAAJ中部支部　杉山　浩一
18:00～18:15　特別報告
『第五回日中IT技術者交流会(in北京＆天津)について』
SAAJ中部支部　堤　薫
18:30～20:30　夕食／懇親会
21:00～　懇親会 2次会

＜11月19日（日）＞

8:00～9:00　朝食
9:00～10:50　グループ演習
○課題1：社会貢献活動について（地方自治体･地域企業･各種団体等への働きかけ）
○課題2：支部会員・各種団体との交流活動について（合宿、他支部・他団体交流、会員交流・啓発など）
○課題3：国際交流活動について（オフショア開発のシステム管理基準策定など）
11:00～11:50　グループ演習成果物発表
11:50～12:00　閉会挨拶
12:00　解散

4．講演

(1) 下呂市におけるＩＳＭＳの取り組みについて
発表　下呂市企画部情報課課長補佐
桂川　国男
要約＆コメント　No.877　中村　博

(要約)

本稿では地方自治体では数少ないケースとして、ISMSの認証取得に取り組まれた岐阜県下呂市(以下本市という)の事例を以下の5項目に分けて紹介する。

①ISMS導入の背景
②構築に向けた準備作業
③作業手順
④ISMS登録認証までの流れ
⑤今後の課題

①ＩSMS導入の背景

本市は2004年3月に旧下呂町を含む4町1村が合併、成立した都市である。合併により多くのネットワークシステムを抱えるようになり、インターネット・電子メールの利用増を背景に市民の個人情報保護に対する不安

を解消すべく、市長の方針によりISMSの導入決定がなされた。
②構築に向けた準備作業
構築対象部課を決定後、プロジェクトチームを設置、コンサルタントの支援を得て2004年10月に構築作業を開始した。
③作業手順
保護すべき情報資産の棚卸しから始まり、リスク分析、管理策･文書類の整備を経て、市長による「基本方針」宣言に至る。
発表者によればISMSの仕組み、思想を職員に理解させ、隅々にまで浸透させるのに相当苦労したとのことである。
④ISMS登録認証までの流れ
2005年3月の仮運用を経て、翌4月に本格運用を開始した。2回にわたる審査機関による審査を受審後、同年7月にISMS登録事業者として認証を受けた。
ちなみに、2006年初頭にはISO27001移行対応に向けて準備を開始し、同年7月に移行登録を済ませた。
⑤今後の課題
本市の課題は以下の通りである。
(a)市民サービスと機密性
例えば窓口後方の事務室に難なく入室できていたものが、ある日突然入室制限がかけられると市民と市職員との間に軋轢を生じることがある。セキュリティに対する理解を求めつつ、市民への行政サービスレベルを維持すること。
(b)職員の意識統一
認証登録後も部署間に温度差があったり、上司の理解が得られないこともある。継続的な研修等を通じた、意識統一を図ること。
(c)市民の理解
職員の更なるセキュリティマインドの向上、有効な技術的セキュリティ対策の立案･実施、内部監査の充実等により市民の理解を得ること。
(コメント)
個人情報保護の意識が高まる中、地方自治体においても情報セキュリティ維持のため様々な努力が払われている。そのような状況下で本市はISMSの導入に踏み切った。「ISMS登録事業者」としてのお墨付きは個人情報が適切に取り扱われているという安心感を市民に与える反面、例えば入室制限の実施等により行政と市民との間に新たな距離感が生じる可能性をはらんでいる。しかし、広報等を通じた市民への理解促進、市民サービスへの継続的改善活動等を通じて、セキュリティ維持と行政サービスの両立を図ることは可能と筆者は考えている。
行政サービスを受ける一個人として、今後本市のように情報セキュリティへの取り組みが明確に宣言できる自治体が増えることを期待したい。

(2) 地方自治体における情報セキュリティ監査
発表　No.6036　田中　勝弘
要約＆コメント　No.1563　松井　真一
(要約)
地方自治体の情報セキュリティポリシーの策定状況としては、総務省の指導もあり都道府県では100%、市町村でも96%を超える状況となっている。しかし、情報セキュリティ監査の実施状況となると、都道府県でも37団体（78.7%）に留まっており、市町村においては30%に達しておらず、監査が普及、浸透しているとはいえない現状である。
監査の実施が滞っている理由としては、個人的には地方自治体から以下のような意見を聞いている。
①情報セキュリティの重要性は認識している。
②財政が厳しいため、実施時期、方法を検討中
③上長説明、住民説明が困難
④近隣自治体の動きを情報収集中
そのような状況の中で、地方自治体からセキュリティ監査を依頼され実施したのでその概要を述べることとする。
監査を実施したねらいとしては、“「地方公共団体における情報セキュリティ管理基準」に基づき、情報セキュリティ対策の状況を点検・評価”することであり、助言型監査として実施している。
監査の手順としては、基本とおりに、
①事前調整
②予備調査
③本調査
④監査報告
の手順で実施したが、更に公開サーバ、ＤＮＳなど公開システムの脆弱性診断も併せて実施した。自治体が情報セキュリティ監査を依頼する場合には、今回のように、技術的脆弱性診断も同時に依頼される場合が多いようである。
監査を実施することにより、地方自治体には以下のような問題点があることがわかった。
①電子化された情報と紙の管理が別に行われていて、総括的に管理できる体制は整っていない。
②本庁と支所間でのＦＡＸ送信が残っており、誤送信による情報漏洩のリスクが潜在している。
また、自治体における今後の課題としては、情報セキュリティポリシーの実施サイクルを継続的に回すことと、職員のセキュリティ意識をいかにして向上させていくか、の2点であろうと考えている。

(コメント)
地方自治体においては、政府のe-Japan構想による住民基本台帳ネットワークの導入を契機として、セキュリティ対策の必要性が叫ばれている。それを受けて、情報セキュリティポリシーの策定および情報セキュリティ監査の実施が総務省の指導の元、普及、拡大されつつある。
しかし、地方自治体の現状をみると内部監査人による情報セキュリティ監査を実施することは、人事異動が頻繁なために監査人の育成が困難であるという問題が推測される。そこで、我々システム監査人を含めた外部監査人が、地方自治体のセキュリティレベル向上に貢献することを期待したい。

(3) 岐阜県におけるＩＴガバナンスの取り組みについて

発表　No.1276　杉山　浩一
要約＆コメント　No.1567　多田　進

(要約)
講演では、岐阜県におけるITガバナンスの取り組み状況について、行政機関としての視点も交えながら説明された。以下にその内容を説明する。
一般にITガバナンスとは、組織目標を達成するためにITにかかわる活動を統制し、ITの価値を最大化することである。さらに行政機関では、ITにかかわる活動や、その結果得られたITの価値を、議会や市民、メディアへ説明する責任もある。そのような観点で、行政機関のITガバナンス強化は重要な意義を持つ。
岐阜県では、以下のようなアプローチ(「戦略」⇒「組織運営」⇒「システム運営」⇒「説明責任」)で、ITガバナンスの構築に取組んできた。

・戦略：岐阜県IT戦略、IT活用プランなど
・組織運営：CIO設置、IT専門職員育成など
・システム運営：戦略的アウトソーシングなど
・説明責任：システム評価、監査など

これらITガバナンス構築の主な取り組み事例として、IT調達の適正化、セキュリティ対策がある。
IT調達の適正化に向けた取り組みとして、岐阜県では、情報システム導入審査委員会を設置し、予算時期やシステム調達時に、計画、実施内容を確認する体制を整備している。
また、セキュリティ対策として、ポリシーの制定、情報セキュリティ委員会の設置などに加え、第三者機関による情報セキュリティ監査を実施している。
今後のITガバナンス強化にあたっては、システム評価手法の統一化、人材の育成など様々な課題が残っているが、これらの課題を徐々に改善して、岐阜県のITガバナンス強化に努めたい。
(コメント)
一般市民として、最近の公的機関での談合や情報漏洩の問題に対するメディアの厳しい論調に同調することも多い。そのような中、行政機関としての活動が適切か否かを議会や市民などに対して説明する責任がある、というお話しは印象深かった。
実際、説明責任を果たす上で、第三者機関による監査は有効である。行政機関の監査においては、特有の環境や風土を考慮し、一般組織向けとは異なる対応も求められると考えられる。そのような観点で、SAAJが果たす役割もあるのではないかと感じた。

5. グループ演習（3グループ）

(1) グループ1（社会貢献活動）

メンバー　植野、萬代、大野、関口、早川
報告者　No.605　萬代　みどり

我々のグループは「社会貢献活動」をテーマに取り上げて討議した。
そこでは、これまで行ってきた活動を洗い出し、これから活動できる可能性のある事項を討議した。そこで挙がったのは「システム監査普及サービス」「外部向けの講演会」「他支部との交流」「他団体との交流（ＩＴＣ他）」「国際交流事業（対中国）」「地方自治体への

アプローチ（セミナー案内、講演依頼）」等である。以下に、その主な内容を報告する。

①システム監査普及サービス

SAAJ中部支部内には、「システム監査」が勤務先企業の業務であり有償で実施している会員がいる。一方で、全くシステム監査に触れる機会の無い会員もいる。システム監査普及サービスは、後者の会員にとっては有益なものであるが、前者の会員にとっては自己の業務との兼ね合いや業務上の守秘義務などとの抵触が問題となる。これが、ＳＡＡＪ中部支部の現状である。

こう捉えると、中部地区のシステム監査需要を「システム監査普及サービス」のみで賄うには限界がある。このことや、有償サービスとしてのシステム監査を認識してもらうために、今後は業務としてのシステム監査の普及を推進する方向に向きそうである。

支部は、システム監査を求める立場の人と、システム監査を業務として行える人とを仲介する立場にシフトしていくのではないか。そのためには、今後、支部が主体となって、システム監査台帳やＳＡＡＪ本部への登録を推進していくべきである。それを通じて、結果として、中部地区のシステム監査企業の育成に貢献していけるだろう。

②セミナーや講演会

中部地区の企業・自治体向けのセミナーや講演会においては、他地区とは異なる中部地区の特殊事情がある。つまり、関連法令や技術的なセミナーなどは、ソフトピアジャパンその他の公的機関が無料で質の高いものを提供している。そのため、有料のセミナーへの需要は他地区に比べて低い。

したがって、セミナーや講演会を企画するにあたっては、このような事情を踏まえた上で、適切な企画を検討する必要があるだろう。

③提言

合宿最終日の各チームの成果発表時に、他チームの方から次の助言があった。曰く、健全なコンピュータシステムを守るために、世間で稼動するさまざまなコンピュータシステムに対して、相手方から求められなくても評価や提言を積極的に行っていく社会的責任を負うべきというのである。

確かにそうだと思った。我々は自分たちの枠の中でどのような活動ができるかを考えていたが、もっと広く社会に目を向けていくべきである。これからの我々はそのような意識で活動していくべきである。

(2) グループ２ (支部会員･各種団体との交流活動)

メンバー　下谷、佐野、若原、川合、福田、杉山

報告者　No.027　佐野　雅哉

当グループは、「支部会員・各種団体との交流活動について」について、特に支部活動のあり方に着目して議論し、その上で各種団体との交流のあり方について議論した。

①支部活動のあり方について

はじめに日本システム監査人協会中部支部及び日本システムアナリスト協会中部支部の現状について報告した。

両支部とも最近は、例会の進め方･発表テーマ、遠隔地会員の存在等を原因として、例会出席者が固定化する傾向にあり、支部活動の活性化が課題であると認識しているとのことであった。

そこで、支部活動の活性化について議論することとし、まずは、私達会員がなぜ各協会に加入したのかという原点に立ち返り、次に支部活動の目的を明確にする必要があるのでないかと考えた。

当グループでは、「私達は、異なる業種の人達との交流を通じて、幅広い見識を持ち、技術研鑽に努めるために協会に加入し、支部例会などに出席している。」という認識を確認して、支部活動では、そうした意欲に応える活動が必要であると考えた。

具体的には、「会員に対するニーズ調査を行い支部例会の内容を見直す。」、「毎回時宜に合った講演会を開催し著名な講師を招く。」、「本部で開催している月例研究会のビデオ鑑賞を行う。」といったことを挙げて議論した。

とりわけ、ニーズ調査の実施に関しては、九州支部では実施したことがあり、「さまざまな情報が得られる。」ということが最も支部活動に期待することであるとの紹介もいただいた。

②各種団体との交流のあり方について

次に、各種団体との交流にあり方について議論し、上級システムアドミニストレータ連絡会、ＩＴコーディネータ協会、日本技術士会等の中部支部など、同じＩＴ関連の団体との交流を深める必要性について検討した。

また一方で、システム監査あるいはシステムアナリストという専門性を持った集団である特性を活かして、経営情報学会等いわゆるユーザ団体との交流についても推進して行ってはどうかという議論になり、対象団体、アプローチ方法等について検討を行った。

③まとめ

限られた時間の中で、支部活動のあり方及び各種団体との交流のあり方について議論し、結論とは言えなくとも一定の方向性・可能性を拾い上げることができたと考えている。

今後、支部例会等を通じ、実効性のあるものにできるよう議論を重ね、魅力ある支部活動を展開したい。

(3) グループ３ (国際交流活動)

メンバー　原、堤、田中、山田、石井

報告者　No.678　堤　薫

グループ検討概要は以下の通りであった。

山田さんが作成した次の２種の資料をもとに今後の活動方針を検討した。

○システム管理基準（for ｵﾌｼｮｱ開発）課題（天津発表と質疑と今後の課題）

○オフショア開発技術者教育の一考察

①活動方針のポイント

(a) システム管理基準に適用に関する優先順位付け
優先付け（shall、should）を行い、適用に関する解説（説明）を付加していく。

(b) 適用・普及に関する働きかけ
まず、中国側への普及のアイディアとして、プリモスおよび関連会社に採用企業となってもらう。そして、マスコミへのＰＲの核として利用する。
また、日本側への普及のアイディアとして、ＮＥＣなどに中国ビジネスにおいて標として採用してもらう。そして、中国側にそれを提示し、他の企業へも採用を促す。

(c) 管理基準に適用した運用標準の策定
…管理基準を利用するところにて作成
ＮＥＣなど中国ビジネスにおいての標準として採用してもらう企業に協力してもらいながら、管理基準に準拠した運用標準を策定してもらう。そして、中国側にそれを提示し、他の企業へも採用を促す。

(d) オフショア開発技術者教育
…日中両技術者に管理基準を教える必要がある！
中国側技術者および日本側技術者の双方のブリッジＳＥの育成が望まれる。

(e) 著作権について（案）
中部支部の研究開発部（本部理事の方も参加）と山田さんとの共同著作権利と設定したい！。

著作権表記は以下のようにする。

Copyright 2003-2006 NPO 法人 SAAJ
中部支部研究開発部 & 山田隆
Copyright 2003-2006 t.yamada and
NPO-SAAJ_chubu_R&D

公共目的　または　利用企業のソフト取引を円滑に行う目的でその会社自身のために利用する限りにおいて、無償で適用することを認める権利は権利者おのおのが他の権利者に断りをしなくても行使できる。この基準を普及するために有償でビジネスを行う場合の使用権料は山田さんが 50%、SAAJ 中部支部研究開発部が 50%を受ける。この際の使用許可は両者の合意に基づく。

上記のケースは、変更権を認めない、上記のケース以外は、両者の合意を要する。なお、SAAJ 中部支部研究開発部は SAAJ 中部支部長が代表権を行使する。中国科学院計算技術研究所ファン所長と連携して著作財産権と著作人格権に関して検討する。

②今後の展望

国際取引の共通基準への発展させるために、日中にかぎらず、ベトナム、フィリピン、韓国、米国などを含む外国間でのソフト

6. 合宿に参加して（感想）

(1) ＳＡＡＪ／ＪＳＡＧ中部支部２００６年度合同合宿に参加して

No.1479　早川　晃由

合宿に今回初めて参加しました。今年度の中部支部の年間活動計画を目にした時に、合宿がイベントとして企画されていることを知り、どのようなことが行われるのか興味を抱いていました。

合宿の開催が迫ってきた１０月上旬、合宿参加者募集の案内メールをいただきました。テーマは「地方自治体におけるセキュリティ監査・システム監査の取組みについて」ということで、私が現在抱える業務と関連が深く、ぜひとも参加したいと思いました。

泊まり掛けの研修は、１年前のシステム監査実践セミナー以来久しぶりでした。参加者のために駐車場も確保されていて、合宿会場に車で行くことができました。会場に入ると早速、SAAJ と JSAG の活動報告及び来年度計画の説明が始まりました。１日目はセミナーが中心でした。まず、ISMS の認証を取得し、ISO27001 に移行登録された下呂市の取組みが講演されました。市長のトップダウンで取組みを進めておられ、地方自治体としてかなり先進的である印象を受けました。次の「地方自治体における情報セキュリティ監査」の講演では、「なぜ、この管理策を選んだのかリスク分析と管理策が紐付けされていないと乖離する。」という言葉が深く記憶に残りました。３つ目の講演では、岐阜県におけるセキュリティ対策の取組みについて特に「情報セキュリティ対策の実施体制」に関心

を持ちました。県と市町村では異なるところがありますが、とても勉強になりました。特別報告では、映像を中心に中国との交流の深まりを拝見できました。

セミナー終了後、懇親会に引き続き二次会も開催されました。仕事の話を持ち出すのは差し控えていたのですが、抱えている課題について話題にしたところ適切なアドバイスやヒントを色々聞くことができました。

二日目は、グループ演習の「課題1」に取組みました。予習しておらずあまり発言ができませんでしたが、発表に役立ててもらおうとパソコンに討議内容を整理しながら打ち込みました。

この合宿は、職場や家庭を離れ、宿泊すれば家に帰る心配もせず、会員同士が歓談し交流を深める機会を与えてくれるものだと思いました。懇親会や二次会では、雑談しながら様々な話題が飛び交い、そんな雰囲気の中から仕事上の課題も糸口が見出せてくると感じました。それぞれの分野で専門性を深め高い技術を有する先輩会員の方々と二日間過ごせたことは、私にとってとても有意義なひとときとなりました。事務局幹事の皆様、参加者の皆様ありがとうございました。

(2) 合宿の感想

No.6037　大野　淳一

毎年、ＳＡＡＪ中部の合宿に参加していますが、今回は、普段の仕事にも関係したテーマであり、興味を持って参加することができました。講演については、講師それぞれの立場での考え方や取り組んできたことについて丁寧に説明していただき、私にとっては大変有意義な時間でした。

グループ演習では、それぞれのグループで課題に沿って真剣に討論する様子が印象的でした。社会貢献活動のあり方、他団体との交流、オフショア開発のシステム管理基準の研究などについて、来年以降の具体的な活動を見据えた議論、発表が行われました。ＳＡＡＪやＳＡＡＪ中部支部の今後１０年を見据えた活動の方向性について考えるとてもよい機会であったと思います。

例年のように、今回も他支部や他団体から多くの方に参加していただき、懇親会やグループ演習の場で積極的に発言していただきました。こうしたオープンな雰囲気が中部支部の特徴であり、支部活動の幅を広げているのだと改めて感じました。

最後になりましたが、多忙な業務の中で、合宿の会場手配からテーマ設定まで非常に多くの作業について快く対応していただいた合宿担当の方、多くの刺激を与えていただいた参加者の皆様に心より感謝いたします。

(3) ＳＡＡＪ／ＪＳＡＧ中部支部２００６年度合同合宿に参加して

No.1233　栗山　孝祐

私は、システムベンダに勤務し、２００６年度からシステム監査部門に所属しております。そして、システム開発やシステム運用の監査をしています。その為、東海地区での各企業、自治体の動向を把握し、自社の参考にしたく合宿に参加しました。

また、会員の皆様との人的ネットワークを築き、情報交換の場としたいと思いました。

参加した結果は、自分が期待した以上の成果があったと思います。仕事の関係があり、２日目の朝までになったことは残念でした。

①１日目の講演

基調講演では、下呂市は市長の理解のもと、東海地区で先駆けてＩＳＭＳ取得に取り組んでおり、トップの強い意志と判断が必要であることがわかりました。

また、新しいものを導入する時の現場の抵抗や、それに負けずに突き進む推進担当者の目的意識が印象的でした。

講演１「地方自治体における情報セキュリティ監査」では、監査を請け負った立場の話しであった。プロとしてストーリー性が重要でそれを持って推進されていることが判りました。

講演２「岐阜県におけるＩＴガバナンスの取り組みについて」では、今回の事件の影響や知事が交代するとＩＴに対する取り組みが大きく変わることがよくわかりました。

その他、日中交流については、中部支部が推進していますが、継続と拡大していくことを望みます。

②懇親会

会社のメンバーとは異なる方との懇親会であり、それぞれの自治体や会社、立場が異なる方とのシステム監査やシステム開発の取り組み、さらに、中国のシステム開発の話しなど、最新情報やウラ話等も聞け大変有意義な会でありました。

最後に、若原様、杉山様はじめ皆様にお世話になったことにあつく御礼を申し上げます。

7．おわりに（当日のあいさつ）

日本システムアナリスト協会 中部副支部長
No.1224 石井 成美

初日の講演、夜遅くまで続いた懇親会、そして、二日目のグループ演習では、時間が足りなくなる程白熱した合同合宿も無事終了する事が出来ました。

幹事を担当して頂いた杉山さんの労に、感謝申し上げます。

今回のＳＡＡＪ／ＪＳＡＧ中部支部の合同合宿には、中部支部の会員だけでなく北信越、関東、九州地区からも参加者を迎え、他団体や他地域との交流活動にもなったと思います。

今後、例会活動を一層充実させ、本合宿での検討課題を継続検討していきたいと考えます。

最後に、いつまでも自己を向上させ様とする熱意を持った皆様と、ご一緒させて頂いたことに、この場を借りて感謝申し上げます。

また、来年も本合同合宿が開催されることを期待します。

平成 19 年北信越支部年度総会

No.848 森広志

北信越支部では、平成 19 年年度総会を富山市で行いました。今年度は、ＳＡＡＪ創立２０周年ということで、本部の情報セキュリティ監査研究会から山内講師をお招きし実施することができました。以下、報告を述べます。

1. 北信越支部平成 19 年年度総会スケジュール

(1) 日時；3 月 24 日（土）13:30 から 17:00
(2) 場所；富山駅北口アーバンビル 5 階
(3) 内容；
①北信越支部年度総会 13:30 ～ 14:00
昨年度行事報告･今年度行事計画（森）、
昨年度予算報告･今年度予算計画（坂井）
② 20 周年記念行事について（森）
14:00 ～ 14:20
③北信越支部システム監査・情報セキュリティ監査研究チームの報告（森､宮本）
14:20 ～ 14:50
④発表「情報セキュリティ監査について」
15:00 ～ 16:15（質疑応答時間含む）
SAAJ 本部情報セキュリティ監査研究会
講師 山内 美佐子 氏
⑤情報セキュリティ監査に関する意見交換
16:30 ～ 17:00（内容；北信越支部情報セキュリティ監査研究プロジェクトチームの意見交換会と山内氏からアドバイス）
参加者；山内講師、合田、伊藤、坂井、高瀬、白井、宮本、角屋、栃川、森田、尾島、國谷、河村、清水、神田、森

2. 発表趣旨「情報セキュリティ監査について」

SAAJ 本部 情報セキュリティ監査研究会
講師 山内 美佐子 氏

情報セキュリティ監査は、情報セキュリティにかかわるリスクマネジメントの確立・維持を独立かつ専門的な立場から点検・評価し、保証あるいは助言を行うことを目的としている。

監査範囲として、情報セキュリティのリスクマネジメントであり、具体的にはセキュリティ基本方針、組織・資産管理・人的・物理的及び環境的セキュリティ、通信及び運用管理、アクセス制御、システム開発保守、事業継続管理、適合性が監査範囲になる。

情報セキュリティ監査人は、監査業務を行うにあたり、リスクの識別と評価、リスク軽減のために必要なコントロールを判断しなければならない。

今回、JISQ27001 管理項目実施の解釈と考慮点に関する知識をコメントデータとして蓄積しリスクを体系的に漏れなく洗い出しリスク認識やセキュリティ対策見直しに役立てる発想からＷｉｋｉサーバを利用しシステムを開発、山内氏よりコメント例などを交えて、詳細に説明を頂いた。

3. 情報セキュリティ監査に関する意見交換について（概要）

リスク分析とコントロールの知識は、情報セキュリティ監査の骨格になるものであり、非常に重要な研究だと考えます。今回の、Ｗｉｋｉサーバを利用したシステムは、JISQ27001 管理項目によりリスクの洗い出しを行っていますが、情報システムの規模や構成からリスク分析を行う方法も必要ではないかとのご意見がありました。

又、情報セキュリティインシデントについて、インシデント発見時点で対応を取ることが求められますが、インシデントは将来、現在よりも多様になると考えますが、運用管理者が適切な処置が取れるよう、あらかじめ対策を整備する必要があると認識が図られました。

事業継続管理について意見交換があり、事業継続管理を作成していない企業も多いとの認識ですが、過去に良く検討された災害対策計画を現在の情報システムに対応したリニューアルやブラッシュアップができれば良いのではないかと思います。又、災害対策計画に限らず、過去の優れたマニアル、基準なども同様と考えます。

北信越支部として情報セキュリティ監査研究チームが発足し、この機会に運営について意見交換を行い、次の方向性で推進することになりました。

a．推進方法：チームメンバが１人あるいは複数名で１テーマを受け持つ
b．研究：テーマに関する事例研究
c．テーマ案：
・情報セキュリティ監査技法関連
・セキュリティ・マネジメント関連
・セキュリティ技術関連

本部の情報セキュリティ監査研究会の活動を参考にさせていただくと伴に、少しでも役立つことがあれば、ご協力してゆきたいと思います。今後ともよろしくお願いいたします。

北信越支部年度総会に参加して

No.1587　清水　尚志

３月２４日に、富山で開催された北信越支部年度総会に出席させていただきました。

あこがれのシステム監査人協会に加入させていただき始めての総会でしたので、とても楽しみにしていました。

終始和やかな雰囲気の中にも、専門家としての深い洞察からくる鋭い意見が活発に交わされ、とても有意義な総会でした。

総会の内容は、ＳＡＡＪ創立２０周年事業の支部行事として「情報セキュリティ」の研究を通じてメンバーのスキル向上を目指すと同時にシステム監査の普及を企図したものでした。

昨今は、ＩＴの高度化と利用範囲の広がりから益々情報セキュリティの分野は重要になり、監査のニーズも高まっていることを感じているところです。今後私自身も、情報セキュリティ監査研究チーム活動に何らかの形で参加させていただき成果物の作成への協力通じて自己研鑽に励みたいと思います。

２０周年事業の基調講演として山内先生から情報セキュリティ監査の研究内容について、ご講演を頂きました。この中で情報セキュリティ監査の基準作りが極めて重要かつご苦労が多いことを実感しました。また、公認会計士やＩＴコーディネータなど様々な専門家が現場感覚を交えた質疑を熱心に交わされているのを聞かせていただき大変勉強になりました。

又、各方面のスペシャリストの方々が真剣に、かつ和やかな雰囲気で討議される場は大変に貴重なものであり、今後も参加させていただきたいと思います。微力ながら支部運営のお手伝をさせていただきながら皆様と親交を深めて行ければうれしいと思っています。

今後ともよろしくお願いします。

（雑感）

今年の年度総会は、例年に無く多くの参加者を得ることができました。システム監査の可能性は、対象ではマイクロロボットのようなミクロから、広域情報システムのようなマクロまで、技術・知識では、セキュリティから経営まで、

実に幅広く感じます。今回、ｗｉｋｉサーバを拝見させて頂きました。

未来のシステム監査には、システム監査人がナレッジデータベースの支援を得て行うようになるかもしれないと思いました。支部としても地道に技術・知識の習得に努め未来のシステム監査に役立って行ければと思います。

第９回システム監査実務セミナ開催報告

事例研　清瀬秀隆

2007年3月24日、25日および3月31日、4月1日の4日間、幕張・OVTAにおいて第9回システム監査実務セミナを実施した。

例年は２月に実施する４日間実務セミナであるが、今年は内部統制セミナの開催があり、時期を３月にずらすこととなった。年度末ということもあり、受講生が集まるか危惧されたが、結果として12名の受講者での実施となった。

講師は４名で、受講生を３名ずつの４グループに分けて講義を進めていく。４日間のタイムテーブルを別表に示す。初日は座学中心となる。10時の講義開始から昼食まで途中休憩なしで進めていく。午後からは、グループ別のワークを中心とした実習に入っていく。前半２日間は、監査を行うための準備段階（個別計画の策定、調査資料の収集）までを実習する。このため、どちらかというとデスクワークが中心となる。

２日目の最後に資料を受講生に配布し、後半２日間までの宿題を課す。通常、中１週間あけて後半２日間を実施するが、今回は会場の都合で２週連続での実施となる。受講生は宿題をこなす時間を捻出することが大変だったのではないかと思う。

後半２日間は、事例研究会のセミナの最大の特徴である「ロールプレイ」が集中する。３日目に予備調査と本調査が一気に来る。４日目は調査結果のまとめを行い、監査報告会を行う。前半に比べるとかなりハードになる。しかし、受講生にとっては座学ばかりでなく、自分で行動する「実習」が多いため、時間が足りないと思うほど、あっという間に時が過ぎていくようだ。

４日目、監査報告会の実習が終わった後、

事後課題の説明をして解散となる。講師はこの後の提出された課題の評価と添削が大変なのだが、今回は非常に短期間で修了の認定がなされた。受講生の方々の真摯な取り組みが、良い結果に結びついたものと考える。

セミナそのものは、うまく運営できたのではないかと考えている。

さて、その一方で筆者は事務局も担当していた。セミナ運営事務については、反省すべき点がいくつかある。まず、事務局の業務手順書がない。今までは固定されたメンバが担当していたことと、実践・実務は日数が違うだけで事務局業務は同一だったことがあり、これで済んでいた。しかし、内部統制セミナが開始され事務局を担当する事例研メンバが増えていくことも考えると、「口伝」では限界がある。筆者として、今回の経験を手順書としてまとめようと思っているのだが、本業が忙しく少し時間がかかりそうだ。

テキストについても、セミナのロールプレイに用いる事例ごとに「直し」を入れなければならない部分があるが、テキストのデータそのものが一元管理できていないために、実際にセミナを開始してから未修正で配布したことが判明することがある。現在運用に乗せている事例ごとに教材管理CDなどを作成して管理するなどの策が必要かと考えている。今回のd社アウトソースについては、仮作成版として筆者がCDを作ってみようかと思う。

ところで、3日目(後半初日)の朝。筆者が事務局としてOVTAのフロントで「日本システム監査人協会ですが」と告げたところ、「どちらの日本システム監査人協会さまでしょうか？」と問われてしまった。目を白黒させていたところ、二つ予約が入っていることがわかり、予約番号でチェックインは完了した。しかし、いやな予感はしていた。。。。。

予想通り、受講生の方のうち何名かは別の方に行ってしまったようだった。

セミナで使っていることがわかっているのだから、後付でOVTAを使う方は、必ず「セミナではない」ことがわかるように予約を入れるようにしたい。協会外の一般の方に受講して「いただいている」という意識を持ち、二度とおきないようにしなければならない。

事務局業務部分では、私が業務で海外出張に出てしまったこともあり、滞った部分があることは否めない。今後はよりスムースな運営とできるよう、改善に取り組んでいきたい。

以上

日本システム監査人協会システム監査実務セミナー　(2007.3.24 ～ 2007.3.25　於.幕張)

セミナースケジュール表（前半２日間分）

第一日目			（グループ別…７～８名＝２チーム　チーム別…３～４名）				
時間			内容	形式	場所	a	b
from	to	時間(分)				グループ	グループ
10:00	10:30	30	開会セレモニー	全体	大部屋	3014	←
			・開会挨拶、コース紹介				
			・セミナー全体スケジュール説明				
			・講師・受講者自己紹介				
10:30	11:30	60	システム監査動向と技法解説	全体	大部屋	↓	
11:30	12:00	30	演習課題説明	全体	大部屋	↓	
12:00	13:00	60	昼食休憩	全体	レストラン	－	－
			【チーム別演習開始】				
13:00	13:30	30	チーム内自己紹介	チーム別	中部屋	3020	3021
			役割分担決定				
			＜課題１＞				
13:30	14:00	30	監査依頼者の意向確認（ロールプレー）	チーム別	中部屋	↓	↓
			＜課題２＞				
14:00	15:30	90	被監査企業情報の検討及び	チーム別	中部屋	↓	↓
			トップインタビュー準備				
			＜課題３＞				
15:30	16:30	60	トップインタビュー（ロールプレー）	チーム別	小部屋	4020	4021

16:30	17:00	30	*講師コメント｛トップインタビュー後｝*	グループ別	中部屋	3020	3021
			＜課題４＞				
17:00	18:00	60	監査テーマ設定検討	チーム別	中部屋	↓	↓
18:00	19:00	60	夕食休憩		レストラン		
19:00	19:40	40(20/チーム)	監査テーマ発表	グループ別	中部屋	3020	3021
19:40	20:00	20	*講師コメント（監査テーマ発表後）*	グループ別	中部屋	↓	↓
20:00			明朝のチェックアウト手続等説明し一日目終了	グループ別	中部屋	↓	↓
20:00	21:00	60	（懇親会）	全体	中部屋	3020	

第二日目

時間 from	時間 to	時間（分）	内容	形式	場所	a グループ	b グループ
9:00	9:10	10	当日予定等事務連絡	グループ別	中部屋	3020	3021
9:10	9:30	20	*講師コメント｛個別計画作成前｝*	グループ別	中部屋	↓	↓
			＜課題５＞				
9:30	11:00	90	監査個別計画作成･検討	チーム別	中部屋	3020	3021
			＜課題６＞				
11:00	11:30	30(15/チーム)	監査個別計画発表（ロールプレー）	グループ別	中部屋	↓	↓
11:30	12:00	30	*講師コメント｛個別計画発表後｝*	グループ別	中部屋	↓	↓
12:00	13:00	60	昼食休憩		レストラン	－	－
			＜課題７＞				
13:00	14:00	60	予備調査・本調査の為の	チーム別	中部屋	↓	↓
			資料収集検討				
14:00	14:30	30(15/チーム)	資料収集内容発表	グループ別	中部屋	↓	↓
14:30	15:00	30	*講師コメント｛資料収集発表後｝*	グループ別	中部屋	3020	3021
			・配布資料説明				
			・宿題説明（予備調査質問項目リスト作成説明）				
15:00			事務連絡･アンケート記入後、前半終了（受講生解散）		中部屋	3020	3021

セミナースケジュール表（後半２日間分）

第一日目　（グループ別…７～８名＝２チーム　チーム別…３～４名）

時間 from	時間 to	時間（分）	内容	形式	場所	a グループ	b グループ
10:00	10:30	30	後半開会セレモニー	グループ別	中部屋	5014	5015
			・セミナー後半スケジュール説明				
			・後半二日間の演習内容説明				
			＜課題８＞				
10:30	12:00	90	予備調査準備	チーム別	中部屋	↓	↓
12:00	13:00	60	昼食休憩		レストラン	－	－
			＜課題９＞				
13:00	14:00	60	予備調査（ロールプレー）	チーム別	中部屋	↓	↓
14:00	14:30	30	*講師コメント｛予備調査後｝*	グループ別	中部屋	↓	↓
			＜課題１０＞				
14:30	15:30	60	予備調査結果纏めと本調査方針検討	チーム別	中部屋	↓	↓
15:30	16:00	30(15/チーム)	予備調査結果と本調査方針の発表	グループ別	中部屋	↓	↓
16:00	16:30	30	*講師コメント｛本調査前｝*	グループ別	中部屋	↓	↓
			＜課題１１＞				
16:30	18:00	90	本調査準備	チーム別	中部屋	↓	↓
18:00	19:00	60	夕食休憩		レストラン	－	－

			＜課題１２＞				
19:00	20:00	60	本調査（ロールプレー）	グループ別	中部屋	↓	↓
20:00	20:45	45	*講師コメント［本調査後］*	グループ別	中部屋	↓	↓
20:45			明朝のチェックアウト手続等説明し一日目終了	グループ別	中部屋	↓	↓

第二日目							
時間			内容	形式	場所	a	b
from	to	時間（分）				グループ	グループ
9:00	9:10	10	当日予定等事務連絡	チーム別	中部屋	5014	5015
			＜課題１３＞				
9:10	10:40	90	監査報告書作成	チーム別	中部屋	↓	↓
			＜課題１４＞				
		随時	被監査部門に事実誤認有無等確認（ロールプレー）	チーム別	中部屋	↓	↓
			＜課題１５＞				
10:40	11:40	60	システム監査報告会準備	チーム別	中部屋	↓	↓
11:40	12:40	60	昼食休憩		レストラン	－	－
			＜課題１６＞				
12:40	14:00	80(20/チーム)	システム監査報告会（ロールプレー）	全体	大部屋		
			（各チーム：発表：１５分、質疑：５分）				
14:00	14:30	30	講師全体講評	全体	大部屋		
14:30	14:40	10	事後課題説明	全体	大部屋		
14:40	14:50	10	受講生アンケート記入	全体	大部屋		
14:50	15:00	10	閉会セレモニー	全体	大部屋		
15:00			セミナー終了				

第９回システム監査実務セミナーに参加して（2007年３月24日、25日と３月31日、４月１日）

No.1609　藤岡長道

桜便りの季節、私は、海浜幕張駅北口に出ると、フランスから進出したカルフールの大規模店舗を横目に歩き、海外職業訓練センターにおいて開催された「システム監査実務セミナー」に初参加した。参加者は12名で３名づつの４チームに分かれ、外部監査を依頼してきた企業に監査に入るという想定で、１泊２日のコースを２週続ける４日間で行われた。

私が参加した動機は、公認システム監査人の資格申請に向けてスキルアップしたいのと、システム監査のプロから実務的なヒントを得たいという二つの目的があった。参加メンバーは、システム開発にかかわるSEの方、コンサルタントの方、システム監査を担当している方が中心だった。いずれの方も、システム監査の重要性を認識されており、グループワークやロールプレイの質問役にも積極的で、多面的な議論を進めることができた。特に、最終日の監査報告のプレゼンテーション準備においては、各チームとも講師の先生方からの指導ポイントを参考に、「情報システム監査実践マニュアル」（赤本）を参照しながら、締め切り時間を意識してパワーポイントを作成し、緊張感のある雰囲気であった。

監査対象となるケースは架空のものではなく、実際のケースを匿名にしているものだけに、事例が具体的で、講師の先生方のロールプレイにおける迫真の演技（？）とあいまって臨場感があふれる充実した研修だった。次々と新しい課題が出されていくので、テンポが良く、監査の標準プロセスを４日間で体験することができた。特に、監査ヒアリングのための質問項目の整理、予備調査段階での「見通しのつけ方」等、監査プロセスにおける「計画性」と「想像力」が重要であることを強く認識した。研修チームの監査プロセスにおける「弱点」、「改善点」も遠慮なくずばりと指摘していただけるので素直に反省できて良かった。

また、夕食後の懇親会では、ベテランの講師陣からシステム監査の苦労話や面白さを聞くことがためになり、日米文化の比較、大阪と東京の慣習の違い、企業経営のポイントまで幅広いテーマを語り合って有意義で楽しい時間をすごすことができた。研修を企画した協会の方々と土日を使って私たちを指導してくださった講師の先生方に、改めて深く感謝したい。この研修は本当に有意義だった。

CSA（公認システム監査人）活動報告 2007/06

No.898 竹下和孝

私はCSA（公認システム監査人）です。

しかし、多くの場合、ISMSコンサルタントとかPマークコンサルタントと呼ばれています。企業でプログラマとしてソフト開発を始めた頃、「SE」とか「コンサルタント」に憧れました。コンサルティング会社に勤務すると、その日からコンサルタントという名刺を使う場合が多い昨今では、どうしてもその呼ばれ方には馴染めません。でも、お客様は、そう呼ぶほうがわかりやすいようです。

私はCSAですと名乗っても、「何ですか、それ」と言われる場合が多く、「公認システム監査人」のほうが、まだなんとなく価値がありそうです。早く社会的な信頼と存在価値を高めて、有名になりましょう。

私はシステム監査は、情報システムの開発や利用に限らず、もっとあらゆる分野でのCSAの守備範囲をもっと広めていきたいと考えています。システム監査は仕組みの監査であり、内部統制、内部監査、業務監査、あるいはセキュリティや各種ISOの認証審査など、監査・審査・検査と名前のついたものの基盤であり、基本的なスキルであると考えています。

「自立」した独立系CSAのメリット

さて、私は著名なソフトウェア会社からも、ハードウェア会社からも、コンサルティング会社からも独立しています。したがって、多くの会社や組織を、客観的・公平に評価できると思っています。元勤務していた会社も、卒業すれば一定の守秘義務はあっても、利害関係はありません。

しかし現実には、何らかのブランド会社の名刺という実績（または、組織のバックアップという保険）がないと、相手にしてもらえない場合が多いのです。企業側も、早くベンダー依存の構造から脱却して、自立して計画作成、ベンダー評価ができるようになると、経営の意思決定がスピードアップします。ITを経営の中に組み込んで活用して行くのであれば、自らが活用する技術と経営について、自ら判断できるようになると素晴らしいですね。

CSAのセキュリティ診断

さて、ISMS構築、認証取得の支援やPマークの体制構築、認証取得の支援に関する、いわばセキュリティの仕事が最近の主要な業務です。この仕事は、審査、監査、構築支援（コンサルティング）のどの分野でみても、縁の下の力持ち。いつも舞台裏で活動し、問題が起きると、さあ大変です。子供のころ、蟻の巣をつついて悪戯したことを思い出します。

安全な運用を請け負って自らの責任で顧客が望むレベルの安全策を作り上げるのだから、当然といえば当然のこと。しかし、多くの場合、顧客は、依頼したことや約束とおりに実践していないのです。

これが組織全体に蔓延するまでもなく、パソコンを利用している社員の一人でも操作ミスで情報漏えいすると、組織は硬直してしまいます。私は、「これが情報セキュリティの怖さで、組織の心筋梗塞だ」と説明しています。

ほんの一瞬の隙、たった一人のために、これまで蓄積してきた信頼は消滅してしまいます。

だから「セキュリティホール」と言われる重大な欠陥を見逃さないように、日夜、気を配ります。

この「組織のセキュリティホール」は、実は、経営者の中に潜んでいる場合が多い。

CSAの経営診断

セキュリティ系のCSAは、このセキュリティホールを事前に見つけては、リスクの顕在化（＝セキュリティ問題が現実に発生する）を未然に防ぐ対策の立案、実施を主要な業務としています。

では、経営系のCSAは、その組織が課題を認識しているか、不足や過剰にならないようにコントロールしているか、また不足していることを早く発見して適切な追加の経営資源をタイムリーに投入するようなやり繰り（だから、マネジメント）ができているかを判断し実践することを支援します。経営者には判断力、実行力（組織を動かす力）が必要で、組織の構成員が行動できるように指示しなければなりません。

最近は、リスク対応の現場（http://risk.livedoor.biz/）から、エクセレントを目指す（http://njaro.exblog.jp/）方向へシフトしようと情報発信しています。

自社の様子が気になる場合には気軽にCSAに相談できる、という場や環境を作りたいと思います。組織経営にも健康診断は必要で有効です。またCSAは個人としての活動が中心ですので、大手ファームに比べると安価にサービス提供できます。私の場合も、セキュリティに関する相談が多いのですが、お蔭様で引っ張りだこです。但し、せっかくパフォーマンスを評価頂いているのであれば、相応の報酬をいただけるほうがうれしいなと思います。このようなCSAのビジネスモデルを作りたいと願います。

月例研究会報告の記録（テーマ、講師、報告書、協会会報より）

会報記事の投稿に、ご協力いただき、ありがとうございます。
会報の報告記事として好評の月例研究会報告は次の方々に執筆いただいております。
お礼とあわせて、ご報告させていただきます。

月例研究会報告の記録

2007.6.1 現在

回	日時	テーマ	講師（肩書きは、当時のもの）	報告者
127	07.04.23	金融機関等のシステム監査指針（第３版）改訂について	財団法人　金融情報システムセンター(FISC)監査安全部長　　郡山　信　氏	馬場　孝悦
126	06.12.22	J-SOX の基準と IT の位置づけ	監査法人トーマツ エンタープライズリスクサービス部パートナー 公認会計士、公認情報システム監査人　　伊藤　哲也　氏	蓮見　節夫
125	06.11.30	IT サービスマネジメント(ISO20000)の概要と事例から学ぶ構築のポイント	(株)IP イノベーションズ　コンサルタント　津村　正彦　氏	三橋　潤
124	06.10.23	FISC の安全対策基準とコンティンジェンシープラン策定手引書の改訂について	財団法人　金融情報システムセンター(FISC)監査安全部長　　郡山　信　氏	本田 実
123	06.09.21	事業継続とシステム監査	東京海上日動リスクコンサルティング株式会社情報グループ・グループリーダー NPO 事業継続推進機構 副理事長　指田朝久 氏（前当協会理事）	鈴木 実
122	06.08.02	政府機関の情報セキュリティ対策のための統一基準	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	宮下　重美
121	06.07.03	システム監査と JSOX	日本大学商学部教授　　堀江正之氏	渡部　洋子
120	06.05.22	新 JIS の概要とシステム監査	(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　関本貢氏	一村　義夫
119	06.01.30	ISO/IEC27001:2005 の最新動向	財団法人日本情報処理開発協会情報セキュリティ部 ISMS 制度推進室長　高取敏夫氏	松枝　憲司
118	05.12.16	ソフトウエア国際取引に関するシステム監査について	合資会社アジア経営システム監査研究所社長 山田隆氏	竹下　和孝
117	05.11.07	電子政府構築に向けた取組について	総務省行政管理局行政情報システム企画課課長補佐　澤田稔一氏	成田　佳應
116	05.10.19	CSR と内部監査	監査法人トーマツエンタープライズリスクサービス部パートナー　達脇恵子氏	藤野 明夫氏
115	05.09.27	IT 内部統制評価の計画と手続き	大阪成蹊大学現代経営情報学部助教授 石島隆氏	仲　厚吉
114	05.08.22	組織目標達成に役立つ COSO ERM	日本内部監査協会常務理事 淑徳大学兼任講師　山本明知氏	高井　憲彦

エッセイ、論文の募集

会員の皆様
SAAJ 会報の読者の皆様

会報編集部では、次の通りエッセイ（論文募集要項に該当しない投稿）、論文を募集しています。会員の皆様の積極的な投稿をお願いいたします。

今年は、SAAJ 創設 20 周年にむけて、記念講演会や論文集の発行など、各専門部会および支部ごとに、活動の成果をまとめていく機会も多いかと思われます。

会員、読者の皆様も、是非、手記にまとめて気楽に投稿いただき、システム監査の歴史に記録を残しませんか。会報編集部が支援させていただきます。

論文については、次の投稿要領を用意しております。　エッセイの投稿には記名をお願いすること以外には、特に制約はなく、自由な創意工夫が反映できます。

会報掲載論文募集要項

会員の皆さんより、会報掲載論文を募集します。

1．論文の内容：
　システム監査・セキュリティ監査（関連を含む）の実務の裏づけのある内容で、システム監査・セキュリティ監査（関連を含む）の啓発、普及、理論深化、情報提供、実践、手法開発等に役立つ論文。既発表論文は除く。
2．字数：　６千字以上、１７千字以内（図表を含める）
3．提出方法：　原稿は、ms-word で作成し、パスワードを設定し、メールに添付して送付する。フロッピーディスク等で会報編集委員会あて送付する場合、媒体は返却しない。
4．審査：　会報編集委員会内に設ける論文審査委員会にて、審査を行い、掲載に値するか、及び内容の優劣を判断し、掲載する場合は、２万円以上、６万円の範囲で原稿料を支払う。審査の内容は公表しない。
5．CSA 継続教育：掲載論文は、10 時間 /1 稿として公認システム監査人（補）継続教育の実績とする。
6．掲載論文募集締め切り：　常時受け付けとし、会報編集委員会より打ち切りのお知らせがあるまで継続する。

会報掲載論文審査要項

理事会提案　2003.7
最終改訂　2003.10　判定基準（点数）改訂

1．論文審査委員会
　応募論文が提出されたら、編集委員長は、応募条件を満たしているかを判断する。
　応募条件を満たしていない場合、直ちに却下する。
　（応募条件：字数の制限、応募者は会員であること）
　応募条件を満たしている場合、直ちに、編集委員の中より、２名の審査委員を任命する。
編集委員長を含めて３名で審査委員会を構成する。
　論文提出者を、審査委員に加えることはできない。
　編集委員長が論文提出者の場合、編集委員長を除いた編集委員会で３名を選出し、審査委員会を構成する。
　審査委員名は公表しない。

2．審査委員は、提出した論文を査読し、判定基準表に基づき、点数を出す。
　判定基準は、会員からの要望があれば公表する。　以上

会報編集委員募集

２００７年度、会報編集委員を募集します。
応募を希望される方は、会報編集委員会までご連絡ください。
E-mail： saaj-kaihoh @ yahoogroups.jp （記事の投稿先と同じです）

ＳＡＡＪ会報の編集活動に参加するメリット
毎回の特集や編集に参加して他の編集委員と意見を交換することにより、システム監査の理論や技術、実務に関する最新の情報に接することができ、自分自身の考え方、活動方法の整理、そして新しい切り口を発見することができます。

条件１
・東京都内で行われる編集委員会（２ヶ月に一度程度の頻度で行われる）に参加できること（主として、茅場町の協会事務所で行います）
・e-mail を利用できる環境を持ち、Word、PDF ファイルなど論文編集に利用される文書ファイルの受信、送信および読み書きなどの編集ができること。
編集作業の大半は、e-mail のやり取りで行われる。

条件２
・会報投稿論文への応募があった場合、論文査読をお願いする場合があります。
・e-mail を利用できる環境を持ち、Word、PDF ファイルなど論文に応募される文書ファイルの受信、送信および読み書き、および査読に協力いただける方。
論文査読を委託する場合には、日程調整と守秘手続を行って、委託します。

その他
・編集主（副）担当、および査読担当の場合に、薄謝を支給します。
・交通費等の実費は協会で負担します。
・会報編集委員は、公認システム監査人（補）継続教育で、
普及啓発　協会の運営を支援する活動
合計実時間　上限２０時間／年
が認められます。

第 10 回システム監査実務セミナー受講者募集のご案内

システム監査の実際を体験してみませんか!!
日本システム監査人協会では、設立目的のひとつである「システム監査人の実務能力の維持・向上」のため、毎年数回、実践的なセミナーを開催しています。
今回のセミナーは、当協会が既に９回の開催実績を重ねる、「システム監査実務セミナー」（４日間コース１泊２日 X2 回）です。
このセミナーは、当協会の事例研究会で実施したシステム監査普及サービスの事例を教材として、実践で得たノウハウを皆様と共有することを目標にしています。
システム監査の実際を体験してみたい方やシステム監査技術者試験には合格したもののシステム監査参加機会のない方は、この機会を利用してシステム監査の実際を経験し、システム監査能力の向上を図りましょう。
なお、このセミナーを受講し、事後課題を提出頂きその内容が適切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)に認定されております。

1.	開催日時	平成 19 年9月1日(土)～2日(日) 平成 19 年9月8日(土)～9日(日) ＜1泊2日×2＞ どちらかのみの参加は 不可時間：土曜は 10:00 ～ 21:00、日曜は 09:00 ～ 15:00 (進行状況により若干の変更が生じる場合があります。)
2.	場所	海外職業訓練協会(OVTA) 〒 261-0021 千葉市美浜区ひび野1丁目1番地 電話番号：043-276-0211
3.	費用	168,000 円 (日本システム監査人協会会員)、189,000 円 (一般) (費用には、教材費・宿泊費・食事代・消費税が含まれます。)
4.	内容	事例研究会が実施したシステム監査サービスをケーススタディとして取り上げます。セミナー用にアレンジした「システム監査依頼書および企業情報」を教材として、3～5名程度のグループにわかれて、トップインタビュー、監査計画書作成、予備調査、本調査、監査報告の実際を体験して頂きます。
5.	講師	協会の事例研究会メンバーでシステム監査普及サービス経験者2～4名(予定)。
6.	対象者	情報処理技術者(システム監査)資格保有者もしくは同等の知識を有する者。 定員20名(最小催行人員10名)
7.	申込み	NPO法人日本システム監査人協会 システム監査実務セミナー事務局担当 三輪智哉 (e-mail：t_miwa@st.rim.or.jp) ※下記の参加申込書を記入の上 E-Mail でお申込下さい。
8.	申込期限	平成19年8月10日(金)
9.	問合せ	NPO法人日本システム監査人協会 システム監査実務セミナー事務局担当 三輪智哉 (e-mail：t_miwa@st.rim.or.jp)

NPO法人日本システム監査人協会

第10回システム監査実務セミナー参加申込書

申込日： 年 月 日

①会員NO. (法人会員の場合は法人名)：
②所属企業名：
③参加者氏名： 男／女
④資料送付先：
(住所) 〒
(宛名)
⑤連絡先 E-MAIL アドレス：
(電話 No. FAX-No.)
⑥教科書 (情報システム監査実践マニュアル(第2版)) 購入希望の有無 □あり ／ □なし
⑦請求書発行希望：□あり (宛先：□所属企業名／□参加者名) ／□なし
⑧現在担当している業務の概要：

⑨当協会主催のシステム監査実践又は実務セミナー参加経験：□あり (年 月) ／□なし
⑩システム監査実施経験：□あり／□なし

以上

「第４回　内部統制セミナー in 札幌」受講者募集のご案内

Ｊ－ＳＯＸ対応の内部統制の構築方法及び評価のポイントを実際に体験してみませんか‼
ＮＰＯ法人日本システム監査人協会では、内部統制構築に関する知識と実践能力を修得するための内部統制セミナーを北海道（札幌市）で開催します。
当セミナーは、システム監査事例研究会で３０回近くの開催実績を積んだシステム 監査実践・実務セミナーのノウハウをベースとして、実行段階に来ている J-SOX の
内部統制の理論と実践を、ロールプレイング方式で実際に体験頂く、実務に即役立 つセミナーです。
内部統制の構築担当者、評価担当者及びその支援をされるコンサルタント、監査人 に対して、書籍や他のセミナーではえられない「業務処理と IT の内部統制に関する 総合知識及び実務の進め方」を実体験できる他に類をみないセミナーです。
システム監査の知識、経験を実務に生かす絶好の機会が到来しておりますので、本 セミナーを受講して、この機会を皆さんのビジネスに生かしていきましょう！！！

記

１．開催日時：平成１９年９月１５日（土）～１６日（日）
　　平成１９年９月１６日（日）は AM9:00 ～ PM4:30
　　（進行状況により終了時間に若干の変更が生じる場合があります。）
２．場　　所：道特会館
　　〒 060-0002 札幌市中央区北２条西２丁目 26 番地
　　（交通機関：札幌市地下鉄「大通駅」下車徒歩５分
　　札幌駅からも徒歩５分程度）
　　電話番号：011-251-8506
３．費　　用：73,500 円（日本システム監査人協会会員）、94,500 円（一般）
　　（費用には、教材費・昼食代・消費税が含まれます。）
４．内　　容：基礎知識を学ぶ座学と事例企業に関する演習課題への取組み、企業へのヒアリング（ロールプレイング）、改善提案のまとめ演習、発表（ロールプレイン グ）、講評など。
５．講　　師：協会の事例研究会メンバーでシステム監査普及サービス経験者３～４名（予定）。
６．対 象 者：Ｊ－ＳＯＸ対応担当者、内部統制の構築、評価に関わる実務担当者及びその支援者。
　　定員２０名（最小催行人員１０名）
７．申込み・問合せ：ＮＰＯ法人日本システム監査人協会
　　内部統制セミナー事務局担当
　　沼野伸生（e － mail:numano_associates@nifty.com）
　　※下記の参加申込書にご記入の上 e-mail でお申込下さい。
８．申込期限：平成 19 年８月 27 日（月）

以　上

－ －

ＮＰＯ法人日本システム監査人協会
第４回　内部統制セミナー参加申込書

申込日：　　年　　月　　日

①会員ＮＯ．（法人会員の場合は法人名）：
②所属企業名：
③参加者氏名：
④資料送付先：
（住所）〒
（宛名）
⑤連絡先　e-mail アドレス：
（電話 No.　　FAX-No.　　）
⑥請求書発行希望：□あり（宛先：□所属企業名／□参加者名）／□なし
⑦現在担当している業務の概要：

⑧当協会主催のシステム監査実践又は実務セミナー参加経験：□あり（　　年　月）／□なし
⑨システム監査実施経験：□あり／□なし

以上

（この個人情報は、セミナーの運営管理のためにのみ使用します）

図書推薦

会員番号555　松枝憲司

「企業リスクとIT統制　-会社法、JSOX、ISMS、BCMが求めているもの」
指田朝久　他共著株式会社アスキー　2,400円＋税

本書は、企業を取り巻くリスクに焦点をあてている。
特徴としては、会社法、JSOX(金融商品取引法)、ISMS(ISO27001)、BCM(事業継続ガイドライン)を取り上げ、それぞれの視点から企業に求められている事項について解説している点である。
上記法律やガイドラインに対する従来の取り組みかたは、「ベストプラクティス」や「基準」、「ガイドライン・チェックリスト」といったものを参考に、どのような対策を打てばよいか、最低限何をすればよいのか、といったアプローチで施策を実施しているケースが多い。このやり方は「コントロールアプローチ」であり、効率的な対応が行える場合もあるが、各企業の状況に応じたリスクの度合いを考慮せずに実施すると、場当たり的な対応や過剰な対応となってしまうケースがある。
これを防止するためにも、本書では「リスクアプローチを採用し、最終的に影響を及ぼす業務の視点でITリスクを共通化することにより、対策の論理的な統合が可能となり、また各コントロールの相互補完関係を明らかにすることができる」としている。
付録として、「IT(情報システムに関する)リスク」「IT統制チェックリスト」を、各50個ずつ例示している。
当協会の「システム監査基準研究会」でも、現在IT統制に関する研究を行っており、非常に参考になる本である。
会員の方にとっては必携の書である。是非手に取っていただきたいと思います。

●本書の構成

《編集後記》

IT先進国インドに行ってきました。といっても、デリー、ニューデリーという首都圏だけです。

そこで見たもの感じたものは、ITインフラの拡充よりも電力、道路、上下水道という社会基盤の整備を必要とする場所が多いということでした。

10億人以上の人を抱え、人やものの運搬に、らくだ、水牛、自転車、二輪車、三輪(自動)車、四輪車が往来しています。鉄道に加え、最近、地下鉄が開業しました。英国の旧植民地が連携したコモンウェルスオリンピックが2010年にデリーで開催される計画で、再開発が加速しているそうです。

以前、台湾を訪問して、表通りは近代日本と同じで、裏通りは終戦直後の日本が混在していると感じました。

ここデリーでは、人類の歴史が始まって以来の伝統的インドと、ITを取り込んだ先端インドが、同時進行していると感じました。

だから、ドリームを目指して活気あふれるインドがあり、貧富の差はますます拡大します。

この街では、社会の仕組みをデザインする、実践モニタリングする、成果を評価することで、社会資本や投資の無駄を省くことができると思われます。

社会システムの効率性、有効性を評価する監査が有益です。(KT)

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 須田 勉
富山 伸夫 木村 陽一
吉田 裕孝 藤野 明夫
仲 厚吉 山田 正寛
森本 哲也

※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。記名記事は薄謝進呈します。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