特定非営利活動法人
SAAJ 日本システム監査人協会報

特集　個人情報保護の実務

個人情報保護法が全面施行されて、2ヶ月3ヶ月と経過して、個人情報流出の報道が続いています。また、情報保護の管理システムや体制を構築したいという需要は強いようです。まさに、法律が起爆剤となって、これからが本格スタートです。

当協会でも、少しでも情報保護体制構築の前線で苦労されている方々を支援するため、また公認システム監査人むけの実務研鑽を兼ねて、実務経験のある有志を講師とした「個人情報保護管理者／監査責任者実務」セミナーを開催しました。

今回は、個人情報保護実務セミナーの講演を軸に、当協会が関係する活動を整理します。

1．「個人情報保護管理者／監査責任者の実務」セミナー
2．（セミナーより）JISQ 15001とプライバーマーク制度
3．（セミナーより）プライバシーマーク取得の進め方
4．（セミナーより）個人情報保護管理者の実務
5．（セミナーより）個人情報保護監査責任者の実務
6．（セミナーより）個人情報保護対応事例
7．セミナー受講報告（受講者感想）
8．地方自治体における情報保護審議委員の仕事
9．法人部会の個人情報保護セミナー
10．当協会の個人情報保護方針、個人情報告知文例

身近な話題として、期待していない郵便物は減ったでしょうか。個人の名を勝手にラベル印刷したり、DM（ダイレクトメール）は減らず、電子メールを利用した強引な歓誘メール、特にアダルトサイトへの誘導メールは増えた感じがするが、読者はいかがでしょうか。

法律の根拠ができたので、処罰を明確にすることで、このようなメールに対して自衛手段としての受信拒否設定ではなく、積極的にオプトアウト（不要との意思表示をすること）の返信メールを出すことが適切な対応であるかは難しい。ランダムに抽出または作成されたメールアドレスに対して、アクティブなメールアドレスであることが発信者にわかってしまうからです。

システム監査人の活躍の場は、ますます広がっていきます。諸兄のご活躍を期待いたします。

なお、今回の特集は、上記セミナーのテーマを題材に、追記・編集したものです。（文責・竹下）

目　次

ページ
特　集　1.～6.「個人情報保護管理者／監査責任者の実務」セミナー、7.受講報告（村上さん）……1,9
8.地方自治体の活動（蓮見さん）、9.地方公共団体セミナー報告と案内（法人部）……11,13
10.当協会の個人情報保護方針、個人情報告知文例……15,16
事例研　システム監査普及サービス（e社）、参加報告（福原さん、今野さん）……17,18
理事会　広告規程、広告掲載案内、理事会報告（H17年第4回、第5回）……19,20,21
書　評　石島隆（著）「情報システムの内部統制—ITに対応した評価の計画と手続」……25
会　報　今年度の特集テーマ計画、会報掲載、論文投稿規程と募集……26,27,28
案　内　第112回月例研究会案内、第6回実務セミナー案内……29,30

1.「個人情報保護管理者/監査責任者の実務」セミナー

このセミナーは、

① 個人情報保護法に企業としてどのように対応すべきか
② JIS Q 15001への対応とプライバシーマークを取得するには
③ 個人情報保護管理者の行うべき実務
④ 個人情報保護監査責任者の行うべき実務

を学ぶことを目的として開催されました。従って次のとおり、企業内においてすぐに役立つよう、できるだけ具体的な形で進めました。

このように「個人情報保護の実務」というテーマを、6つの異なる角度から実務的に掘り下げたセミナーは例がなく、SAAJの社会的な役割を垣間見る感じもしました。

当初予定を超える参加者のため、受講者枠を追加したため、硬いテーマにもかかわらず、2日間の会場は終始、熱気につつまれていました。確認テストで一定レベルの内容が確認された方に、後日、協会会長名の修了証が送付されました。 (主催者代表、蓮見理事)

「個人情報保護管理者/監査責任者の実務」セミナー

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)情報サービス産業協会

1. 日 程 平成17年3月5日(土)～6日(日) 9:30～16:30
2. 場 所 機械振興会館 B3研修1室 (東京都港区芝公園3丁目5番8号)
3. 内 容

＜第一日目＞

(1) 個人情報保護法と企業リスク		9:30～12:00
	弁護士	藤谷 謙人 (途中10分休憩)
(2) JIS Q 15001とプライバシーマーク制度		13:00～14:40
	公認システム監査人	一村 義夫
(3) プライバシーマーク取得の進め方		14:50～16:30
	公認システム監査人	梅津 尚夫

＜第二日目＞

(1) 個人情報保護管理者の実務		9:30～12:00
	公認システム監査人	竹下 和孝 (途中10分休憩)
(2) 個人情報保護監査責任者の実務		13:00～14:20
	公認システム監査人	芳仲 宏
(3) 個人情報保護対応事例(1)(2)		14:30～16:00
	公認システム監査人	松枝 憲司
(4) 確認テスト		16:00～16:30
(5) 個別相談会		16:30～17:00

システム監査人協会法人部会メンバーで対応します。
(小野、梅津、一村、松枝、竹下)

4. 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(12時間相当)
・日本公認会計士協会の継続的専門研修制度におけるCPE認定研修(12時間相当)
・ITコーディネータ継続教育(12時間相当)

（各講演、解説の概要）

(1) 個人情報保護法と企業リスク

藤谷護人弁護士は、現在、全国を飛び回って情報セキュリティと個人情報保護を専門にご活躍中の弁護士ですが、システム監査技術者であり当協会の会員です。

年間200回以上も講演されるというご多忙の日程の中を、無理をお願いして調整していただきました。

ご講演の内容は、弁護士＋システム監査技術者ならではのポイントばかりです。

「個人情報保護法対策30の鉄則」著者による解説は、行間を深く読み解く時間となりました。

(2) JIS Q 15001とプライバシーマーク制度

講師の一村義夫さん（公認システム監査人、ISMS 主任審査員、個人情報保護専門監査人、情報セキュリティ専門監査人）は、企業内のシステム監査責任者として、またプライバシーマーク付与認定取得、ISMS認証取得のコンサルタントとして一般企業向けの支援にご活躍中です。

多くの場合、制度の解説というテーマは、表面だけの説明に終わりがちなのですが、システム監査に長年従事されたご経験と豊富なコンサルティング経験を踏まえた情報も加わり、信頼感に溢れた講義となりました。

(3) プライバシーマーク取得の進め方

ほとんどの企業や組織は、何らかの個人情報を扱っているので、顧客情報か社員情報か、社内の情報か委託・預託された情報であるかを問わず、最低限の安全な取り扱いが必要です。全社規模で社員全員で取り組む必要があり、この活動を進めるため CP（コンプライアンスプログラム）が有効な社内規範となります。プライバシーマーク制度は JIS Q 15001 に基づき CP の適合性が審査されますが、文書審査と現地審査の2段階で行われます。

講師の梅津尚夫さん（公認システム監査人）は、システム監査技術者試験対策の重鎮で、今回もプライバシーマーク取得の進め方という合格対策の部分を担当いただきました。

(4) 個人情報保護管理者の実務

法律や JIS 規格は難解で、いきなり責任者の役割を指名されても、どのように CP を作り活動していいかわからない、という相談があります。また監査の立場で、組織の成熟度（相手の対応能力や準備レベル）に合わせて指摘しコンサルティングする悩みもありました。そこで今回は、皆で情報セキュリティ強化を考えていく状況設定で、できるだけ多くが参加し構築していけるようシナリオを設定していただきました。

講師の竹下和孝さん（公認システム監査人）は、2004 年にはプライバシーマーク審査も担当され、ISMS審査、ISMS 研修講師、情報セキュリティのコンサルタントとして活動されています。

(5) 個人情報保護監査責任者の実務

今回の2日間のテーマの中でも最も堅い部分でしたが、何度か笑いを誘った場面は、受講者の熱意で柔らかい表現に変身したようです。

講師の芳仲宏さん（公認システム監査人）は、企業内の監査人として、また技術顧問として、更には、東京地方裁判所 専門委員、民事調停委員として、幅広い分野でご活躍中です。今回は、JIPDEC の「プライバシーマーク制度における監査ガイドライン」の策定に携わられた経緯から、「個人情報保護監査責任者の実務」を担当して頂きました。

(6) 個人情報保護対応事例

受講者は、このテーマに最も関心が高かったようです。当然ながら一般には、組織の CP 構築の概要は公表していません。プライバシーマークや ISMS の認証取得企業も、どのように取得していったかの苦労話は、取得後には美化されてしまう傾向が強いため、生々しい話を聞く機会は少ないと思われます。

講師の松枝憲司さん（公認システム監査人）は、（株）ビジネスソリューションの代表取締役。「経営と情報に関するコンサルティング」と「システム監査」を多数経験されており、昨年行われたプライバシーマーク、個人情報保護対策コンサルティングの中から、事例として紹介いただきました。

2.（セミナーより）JIS Q 15001 とプライバシーマーク制度

講演者が所属する企業、およびグループ会社でのプライバシーマーク付与認定取得・更新、および、コンサルティング実績にもとづく情報を付加した講演内容であり、JIS Q 15001、プライバシーマーク制度の**詳細とその活用の考え方等**について解説された。

プライバシーマーク制度の概要

1. 概　要
2. 目　的
3. 実施体制
4. 付与の対象
5. 付与の単位
6. 有効期間
7. 手　続
8. 審　査
9. 付与可否の通知と公表
10. プライバシーマークの使用
11. 付与後の実態調査
12. 消費者相談
13. 料　金
14. 申請書類

JIS Q 15001 に基づくプライバシーマーク制度は、

① 事業者に対して、適切な個人情報保護の取り扱いを推進することにより、消費者の個人情報保護意識の高まりにこたえ、社会的な信用を得るためのインセンティブを事業者に与えること

② 消費者に対して、消費者の目に見えるプライバシーマークで示すことにより、個人情報の保護に関する消費者の意識向上を図ることを目的に制定されたものである。

2005.2 時点で 1089 社が認証取得しており、事業者からみた目的も変化している。

① 個人情報、プライバシー保護に関する社会的責任を果たすこと

② 個人情報保護法への適合性と CP 確立をアピール

③ P マークの「取得は競争有利」から「未取得は競争不利」との認識などが解説された。

（会報編集部注：2005.5 時点では、約 1500 社がプライバシーマーク認証取得し、急増している）

3.（セミナーより）プライバシーマーク取得の進め方

プライバシーマークを取得するには、コンプライアンスプログラム（CP）を作成することから開始する。

CP の構築には、いくつもの条件をクリアする必要がある。

CP の作成ステップは、JIPDEC が提供する CP 作成指針に基づくと、次の 14 ステップに分けた活動が必要である。

プライバシーマーク取得の進め方

1. プライバシーマーク制度とコンプライアンスプログラム
2. コンプライアンスプログラム(CP)の策定
   - ・CP作成準備、現状調査
   - ・JIS Q 15001構成に沿ったCP作成
   - ・安全管理措置
   - ・CPの作成ステップ
   - ・個人情報の特定
   - ・進め方のポイント
3. プライバシーマーク取得の手順
   - ・申請から認定までのステップ
   - ・取得スケジュール例
   - ・取得後の維持
4. 個人情報保護法との比較

ステップ 1 ： 個人情報保護方針を定め文書化する
ステップ 2 ： CP 策定のための組織を作る
ステップ 3 ： CP 策定の作業計画をたてる
ステップ 4 ： 個人情報保護方針を組織内に周知する
ステップ 5 ： 個人情報を特定する
ステップ 6 ： 既存の個人情報取扱いシステムを評価する
ステップ 7 ： CP の構成を検討する
ステップ 8 ： CP の基本となる規程を策定する
ステップ 9 ： CP の詳細規程を策定する
ステップ 10 ： CP を文書化する
ステップ 11 ： CP に準じた体制の整備を行う
ステップ 12 ： CP を周知するための研修を実施する
ステップ 13 ： CP の運用状況を監査する
ステップ 14 ： CP の改善を実施する

なお、昨年 12 月に申請手続が一部変更され、申請費用が値上げされました。

JIS Q 15001 も制定後 5 年が経過しており、見直しが予定されているので、最新の状況は JIPDEC のホームページを検索するなどして、情報把握するよう注意していただきたい。

4.（セミナーより）個人情報保護管理者の実務

このセッションでは、実際に組織の個人情報保護管理者になって、CP 構築を進めました。

企業内のシステム監査人は、構築側か監査かの何らかの役割が回ってきます。独立系のシステム監査人には、このような立場の管理者をコンサルティングする業務も多いようです。

1) CP 構築準備

まず、情報収集から開始します。

官公庁の Web サイトを閲覧、または検索エンジンを利用して、目的とする資料を入手します。

- 個人情報保護法
- 経済産業省の個人情報保護ガイドライン
- 厚生労働省の個人情報保護ガイドライン
- 省庁の個人情報保護ガイドライン
  （業種ごとに業界特有のガイド）
- JIS Q 15001
- 監査のガイドライン（JIPDEC）

これらは公開されておりダウンロードできます。

さらに、業界団体が編纂する業界ガイドライン。小冊子は有料の場合もありますが、自社が所属する業界の細かな対応、Q&A を入手できます。

多くの場合、業界の協会に加盟する企業間では、CP 構築の進め方について情報交換したり、共同でセミナや研究会を開催しています。

2) 個人情報保護管理者の実践ステップ

さて、具体的な構築に入ります。

当日は、次のステップで構築を進め、2 時間で CP を構築しました。

1. CP 構築体制を整備する
   （情報収集、プロジェクト編成）
2. 個人情報特定とリスク認識
3. 法令・ガイドの特定
4. 社内規則を整備する
5. 社内手続
6. 教育を実施する
   （休憩）
7. CP の実践
8. CP の点検
9. 内部監査
10. レビューと継続的改善
11. 相談窓口を整備する
12. 緊急連絡体制を整備する
13. 個人情報保護法を理解する
14. （参照）経産省ガイド

個人情報保護管理責任者の悩み 1

- ✓ CPの作り方がわからない
- ✓ 情報システム管理、構築、運用経験がない
- ✓ 営業、顧客対応の経験がない
- ✓ 社内規程が整備されていない
- ✓ 社内の業務全般を知らない
- ✓ 個人情報がどこにあるか不明
- ✓ 監査のやり方がわからない
- ✓ 個人情報保護法、JIS Q 15001は難しい

個人情報保護管理（責任）者の役割

いろいろと調べた結果、次のことがわかってきた。

1.個人情報保護管理者は、次の義務を実行する
  1)社外(顧客情報)と社内(従業員情報)への対応
  2)所有する個人情報を適切に取り扱う
  3)従業員による情報流出防止のため教育監督する
  4)業務委託先から情報流出させないよう監督する
  5)第三者提供する場合には、本人同意を得る

2.請負委託と雇用者(派遣社員)の守秘契約を見直す

このため、まずは、
個人情報保護のための体制作りから始める

1．個人情報の流出防止は企業機密管理(守秘義務)
2．必要なCP(コンプライアンス・プログラム)を作る

業界ガイドライン・自主規制の一覧　2005.2調査

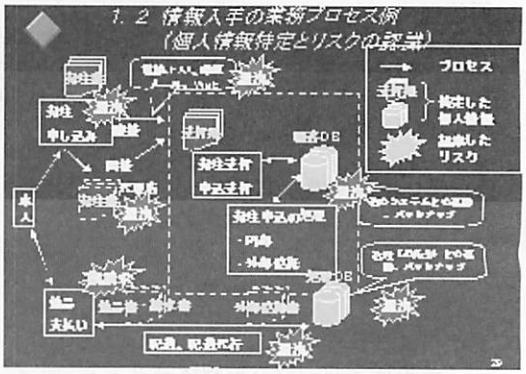
業種	ガイドライン・指針（自主規制）の名称
電気通信事業者協会	個人情報保護のための行動指針［平成11年12月7日、TCA］
財)インターネット協会	電子ネットワーク運営における個人情報保護に関するガイドライン
社)情報サービス産業	「情報サービス産業　個人情報保護ガイドライン」（第三版）（2000年5月）
日本通信販売協会	通信販売における個人情報ガイドライン[改訂 平成17年4月1日]
社)日本ダイレクトマーケティング協会	テレマーケティングにおける個人情報保護に関するガイドライン
電子商取引(ECOM)	「民間部門における電子商取引に係る個人情報の保護に関するガイドライン Ver.2.0（ECOM個人情報保護ガイドライン Ver.2.0）」
全国銀行個人信用情報センター	「信用情報機関における個人信用情報の保護に関する指針」
石油連盟・全国石油商業組合連合会	「SS等における個人情報保護法ガイドライン」2004年9月
社)日本印刷産業連合会	印刷産業における個人情報保護ガイドライン（平成16年12月）
社)日本フランチャイズチェーン協会	「個人情報保護・利用に関するガイドライン（コンビニエンスストア版）」
電子ネットワーク協議会	電子ネットワーク運営における「個人情報保護に関するガイドライン（改訂版）」

3)（セミナー後のご質問も含めて）関心の高かったテーマ

① 個人情報の洗い出しとリスクの認識

個人情報を取り扱う業務にはどのようなものがあり、誰がどのような責任で実施しているのか、全社業務を把握することは、特に大規模組織になると容易ではありません。

部門毎に情報の流れを掴み、必要に応じて図式化し、個人情報特定の手順を作成する必要があります。



・顧客との接点（直接入手・間接入手）
・取引先との接点（委託・預託・提供・共同利用）
・外部委託の接点（委託契約・選定基準）

などを把握して、リスクの認識とリスク対策を実施しているか､十分かを把握することが大切です。

・輸送／オンサイト委託／ネットワーク
・不正アプリケーション／ウイルス／リモートアクセスにも注意します。

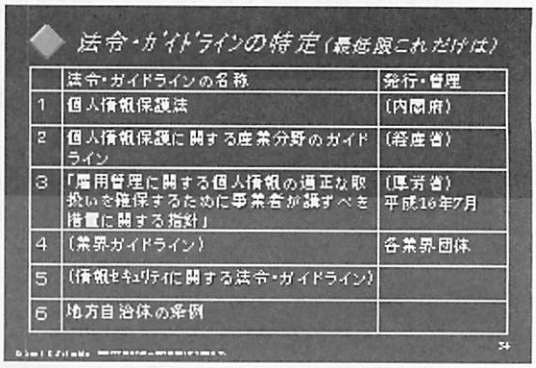
② 法令・ガイドラインの特定

意外と把握できていない部分が法令の特定です。

個人情報保護法は当然としても、その他の関連する法令・ガイドラインがでてこない。

誰がどのように抽出し、改訂の情報を入手し、社内規程に反映させていくのか、明らかにできない場合が多いようです。

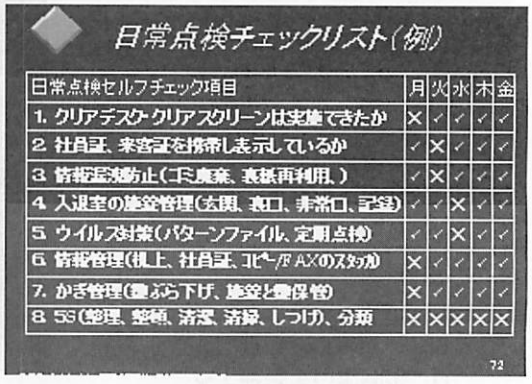
「そんな法律が私の業務に関係するの？」そう、それだけ日常業務はITに依存しており、ITになっており、IT運用・活用するために、法律の保護・遵守を必要としています。



	法令・ガイドラインの名称	発行・管理
1	個人情報保護法	（内閣府）
2	個人情報保護に関する産業分野のガイドライン	（経産省）
3	「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」	（厚労省）平成16年7月
4	（業界ガイドライン）	各業界団体
5	（情報セキュリティに関する法令・ガイドライン）	
6	地方自治体の条例	

③ 安全対策

技術的な対応も重要ですが、多くの組織では、社員に対する基本動作を習慣づけることが必要です。



日常点検セルフチェック項目	月	火	水	木	金
1. クリアデスク・クリアスクリーンは実施できたか	×	✓	✓	✓	✓
2. 社員証、来客証を携帯し表示しているか	✓	×	✓	✓	✓
3. 情報盗難防止（ゴミ廃棄、裏紙再利用、）	✓	×	✓	✓	✓
4. 入退室の施錠管理（玄関、裏口、非常口、記録）	✓	✓	×	✓	✓
5. ウイルス対策（パターンファイル、定期点検）	✓	✓	×	✓	✓
6. 情報管理（机上、社員証、コピー/FAXのスタッカ）	×	✓	✓	✓	✓
7. かぎ管理（置き忘れ、施錠と鍵保管）	×	✓	✓	✓	✓
8. 5S（整理、整頓、清潔、清掃、しつけ）、分類	×	×	×	×	×

・物理的アクセス制御
　入口・マシン室・倉庫・書庫・金庫・引出し鍵管理
・論理的アクセス制御
　クライアント／サーバへのアクセス
　暗号化、暗号鍵管理
・情報のバックアップ
　記録媒体の管理（ラベル、保管・世代管理）
・記　録
　（授受、破棄等の確認書類、管理台帳、入退室、アクセスログ等）
・オンラインによる直接収集時の対応
　収集時のSSLの使用、Cookieなどの利用時の対応 クロスサイトスクリプティング（CSS）などのセキュリティ対策

5.（セミナーより）個人情報保護監査責任者の実務

受講者には、システム監査人が多かったため、実際に監査業務を実践する講師の説明にも熱が入ります。

堅い話の中でのジョークが、場を和ませました。

個人情報保護監査責任者の実務

1）監査責任者の位置づけ

2）JIS Q 15001が要求する監査

3）JIS Q 15001要求事項毎の監査項目

4）監査事例の紹介

1）監査責任者の位置づけ

組織的な安全管理体制を構築するため、従業者の責任と権限を明確に定め、安全管理に対する規程や手順書を整備運用し、その実施状況を確認することが求められる。

このため、

・監査責任者を設置すること

・監査実施体制を整備すること

・監査に必要な証跡を残すような運用管理の実施が必要となる。

2）JIS Q 15001 が要求する監査

「プライバシーマーク制度における監査のガイドライン」(JIPDEC の HP からダウンロード可)に監査の進め方を解説しており、制度発足当初に制定されたものであるが、現在でも十分通用する。

個人情報を取り扱う電子計算機システムと深く関わっており、情報システムを監査対象とするシステム監査技法が参考となる。

しかし、個人情報の取り扱いは、個人情報の収集、入力データの作成と処理、出力情報の利用・提供、その保管・廃棄までが対象であり、情報主体とのかかわり（利用目的の通知と同意を得る、問い合わせ、削除要求など）も重要な監査対象である。

つまり、電子計算機システムによる処理だけではないことに注意が必要である。

3）JIS Q 15001 要求事項毎の監査項目 （抜粋）

・方針：文書化し、役員・従業員に周知させるとともに、一般の人が入手可能な措置

⇒文書には電子的な文書を含み、従業員の定義（正規・派遣など）と範囲を明らかにして周知させ、HP／会社案内／チラシ配布などの方法で外部の人も情報入手できるようにする

・計画書：内部規程を遵守するために必要な教育・監査などの計画とは、

⇒不正アクセス防止計画、ソフトウェア管理計画、セキュリティ基盤整備　などが計画される

・合理的な安全対策：

⇒経済的に実行可能な最良の技術の適用に配慮すること。想定されるリスクとその対策に要するコストとのバランスを考慮して、安全管理規程・入退管理・アクセス管理・データ管理・委託管理などのルールを制定すればよい。個人情報に関するリスクの例としては、不正アクセス、紛失、破壊、改ざん、漏洩が想定されているが、盗聴、盗難、作業ミスによる漏洩やアクセス権の無い者への開示・閲覧（これも漏洩）など、広く考える必要がある。

4）監査事例の紹介

監査という業務や役割の性格上、事例紹介は困難であるが、監査業務の進め方紹介という主旨から、

・監査計画書の作成事例

・監査実施報告の作成事例

・監査報告書の作成事例　などが紹介された。

6.（セミナーより）個人情報保護対応事例

1）小規模A社の例

（目　的）

① JIS Q 15001 の CP を自社の業務改革につなげたい

② 同業者との差別化

（経　緯）

- 一度着手したが挫折 (2002 年ごろ)
- ニーズの高まりから再挑戦 (2004 年)
- 全員参加のプロジェクトを立ち上げ
- セキュリティを確保できるよう事務所移転

A社の構築ポイント
(社長以下 6 名規模の専門サービス事務所)

社員は少なくても、クライアント数は100社。顧客の情報は、3000-4000名規模となる。

1）事務所業務の電子化
2）クライアントでも電子化の動きが進んでいる
3）従業員による情報流出を防止するため教育する
4）業務委託先から情報流出させないよう監督する

（体　制）

- 責任者を総務担当者として社長はプロジェクトオーナーとしてアドバイスに徹した
- 社員全員で分担したので、相互に協力し合って活性化していき、研修など不要だった。人の教育を重視し詳細まで記述したマニュアルを作成した。
- A社 CPには、全員がしっかりと考えを持つ手作りのよさがある。

（安全対策）

- 不正アクセス対策規程：不正アクセス対策・対処マニュアル、不正アクセス報告書など、体制整備した
- ウイルス対策規程：ウイルス対策、対処、報告書を整備した
- 施設入退管理規程：事務所見取り図を元に、インタフォン設置、施錠管理などを徹底した
- 委託先管理規程：秘密情報および個人情報の取り扱いに関する覚書を整備した

2）大規模B社の例

（目　的）

① 基幹システム再構築しサービス拡張に寄与

② 業務のスピードアップと CRM 推進にセキュリティ確保が重要な役割を果たす

（経　緯）

- 顧客情報は全国支店に分散して管理しており、店舗により管理レベルのバラツキがあった
- 2 年前から CRM の一環として顧客情報の活用を進めており、顧客データの活用が課題
- データ整備も進み、セキュリティ確保が重要

B社の構築ポイント(1000人以上の大規模事業所)

全国の販売支店・店舗を主要な窓口として、サービスを提供するために顧客情報を直接取得する。

1）個人顧客と対面する店舗を全国に持つ
2）ネットを利用した資料請求、注文入力も増加
3）ネットマガジンの配信も増えている
4）業務委託先、提携先も多様であり、分類整理を行う
5）情報システムの全国ネットワークと通信サービスは、子会社に開発運用などの処理を委託している

（体　制）

- 取締役総務部長を責任者（CPO）に指名、本社体制と全国支店 70 箇所での推進体制
- 各店舗では独立採算意識が強く、本社統制が利きにくい社風がある中で、社員の意識向上に注力
- 情報システムの開発運用、ネットワークの運用は、情報システム子会社との共同作業（業務委託）であるが、役割や責任分担が不明確な部分も多く残っていた

（顧客情報の利用目的と情報保護）

- 顧客情報の利用目的を整理して、収集・利用・預託・提供などに必要な安全管理の内容を定めた
- 個人情報の預託と預託先：預託目的に応じた預託先を整理し、安全確保できるよう体制整備した
- 「就業規則」を改訂し、社員による個人情報漏洩に関する懲罰事由を明示し誓約書を取得した

7. セミナー受講報告（感想）

「個人情報保護管理者 / 監査責任者実務」セミナー感想文

No.911 村上 進司

1. 全体の感想

平成17年3月5日から6日の2日間にわたり開催された、「個人情報保護管理者 / 監査責任者実務」セミナーに参加し、企業における個人情報の保護の支援活動を行うことを目標にしている者にとり、セミナーの内容が幅広く、実践的であり大変有意義であったと感じている。以下にその感想を述べる。

(1) セミナー全般を聴講して

3月5日（土）9:30 ～ 16:30

① 個人情報保護法と企業リスク・弁護士 藤谷 護人氏

個人情報保護法の性格や位置付け、日本における「セキュリティー文化」革命であるなど個人情報保護法の概観的なお話から、藤谷弁護士執筆の「個人情報保護対策、30の鉄則」を基にした個人情報保護法の解説及び法制の狙いなど短時間ではあったが重要法制条項を懇切に説いていただき、今後更に法制度についてより深く研鑽する際の突破口となる講義であった。特に受講するものの立場から、法制の遵守に際し、法に定められているからという、法論理的な側面だけでなく、人間としての基本的な行動指針や、道徳の観念に裏づけされたコンプライアンスの精神が必要であるとのお話を、草加市の情報破棄事件を例にしながら解説されたのが他の書籍やセミナー等に少ない、印象に残った講義であった。

② JIS Q 15001とプライバシーマーク制度・公認システム監査人 一村 義夫氏

個人情報保護法を遵守すべき企業がコンプライアンスプログラム構築の指針として或いは、企業の社会的責任の規範としてのコンプライアンスプログラムの要求事項およびプライバシーマーク制度を詳細にわたり解説いただいた。

③ プライバシーマーク取得の進め方・公認システム監査人 梅津 尚夫氏

コンプライアンスプログラムの要求事項、及びPマーク制度についての概要から個人情報保護監査、リスク分析の重要性、手順、手法、について解説された後、コンプライアンスプログラム構築の手順、Pマーク取得後の維持の重要性と PDCAのマネージメントサイクルを回す為には取得時と同等の社内緊張感が必要である旨説明された。
特に、取得までのスケジュールにおける、各実施項目の時間見積もりや、取得時、維持に必要な費用概算、個人情報保護法とコンプライアンスプログラムの要求事項の目指す目的の違い、個人情報取扱事業者に要求する内容の差を解説された点は参考になった。

3月6日（日）9:30 ～ 17:00

④ 個人情報保護管理者の実務・公認システム監査人 竹下 和孝氏

コンプライアンスプログラムの構築について実戦的に説かれ、思わず個人情報保護管理責任者の立場になりきってしまうように、抵抗感なく講義内容が受け入れられ、後は実践のみというような印象の全体の講義の流れであった。冒頭の部分では個人情報保護管理責任者誰しもが悩む「いったいどうすれば、何から手を付ければいいの？」の課題から個人情報保護法を理解する手助けとなる情報源の紹介があり、まさに、こらからコンプライアンスプログラムを構築しようとする者にとり、細切れの知識を纏めるには大いに役立ったと思う。
また、その後にPマーク取得の意義が説かれ、CP構築体制の整備から緊急連絡体制まで個人情報保護管理責任者の立場に立ちながら、ニーズ、課題は何かその解決策はといった展開は非常に理解する為に助けになった。例えば、個人情報の安全な運用例、社内規則・規定では、コンプライアンス・プログラムの要求事項と対比され解説されており、厚い参考文献や法文を理解するためにも全体を概観する為にも大いに参考になった。（参考）のISMSとPマークの違いなど、これからコンプライアンス・プログラムの構築を計画する個人情報保護管理責任者はそれではやってみようと意欲の湧く講義であり、終盤の個人情報保護法の解説も理解し易かった。

⑤ 個人情報保護監査責任者の実務・公認システム監査人　芳仲　宏氏

本講義の特徴は、Pマーク制度の監査はシステム監査とは多少異なり、JIS Q 15001の要求事項を満足しているかを監査するものであるが、基本はシステム監査に基づきコンプライアンス・プログラムが継続的に維持改善されていること、すなわちPDCAサイクルがうまく回っているかを監査することと理解できた。参考資料としての「プライバシーマーク制度における監査ガイドライン」の理解を深める解説であったことである。

JIS Q 15001が要求する監査はマネージメントサイクルの他、監査体制の独立性と客観性が要求されており、監査責任者、監査人は、監査や情報システムに習熟している人、個人情報保護やコンプライアンス・プログラムをよく理解している人を事業者の代表者が指名することと説かれている。従って、今後はシステム監査技術者や公認システム監査人の活躍の場が増大すると同時に責任も増すものと意を強くした。

⑥個人情報保護対応事例・公認システム監査人　松枝　憲司氏

本講義の内容は、個人情報保護管理者や監査責任者にとり最も貴重な情報であり、個人情報保護コンサルタントでなければ体験できない貴重な参考事例であった。

二つの事例ともそれぞれ違った角度からの参考事例であり、JIS Q 15001に対応する為に経営環境、運営面環境、IT等の設備面、経済的に人材的に限られた経営資源を企業としてどの程度割り振れるかなど、当然ながら企業により、それぞれ異なった問題や課題を解決しながら対応したであろうと想像できる内容であった。

同時に、例えばコンサルを想定した場合を考慮すると、顧客提案において、事前に顧客を理解して対面しなければ、顧客のコンプライアンス・プログラムを維持する負担感が大きくプライバシーマーク制度の定着を阻害する結果にもなりかねないと、個人情報保護管理者の知恵が必要であるとの認識を持った。

(2)　「個人情報保護管理者／監査責任者の実務」セミナーに参加して

① 過去に多くのセミナーに参加してみてあるいは多数の書籍に（50冊以上購入）目を通したが、実践的な内容では本セミナが最も参考になった。
おそらく、講師の方々が実務に係わっておられるためと認識を新たにし本セミナーに参加出来たことが幸運であったと思う。

② セミナーのプログラム内容が法制面からプライバシーマーク制度、プライバシーマーク取得、個人情報保護管理者実務、監査までJIS Q 15001のPDCAの流れに沿った内容であり企画された運営委員会の方の知恵とご苦労が伺われた。

③ 確認テストは短い時間で多くの内容を集中して聴講する為に緊張感を維持するには役に立った。但し、己の理解力と、記憶力の悪さには改めてがっかりの面もあったが。

④ 個別相談会は、セミナー参加者も講師の方も多少お疲れの状態であり、時間的にも遠方に帰られる方がおられるなど制限はあるが、企画としてはユニークであり聴講者としては大いに活用したいところである。

2. おわりに

この度の「個人情報保護管理者／監査責任者の実務」セミナーは冒頭でも述べたように、「よし今度は実践だ」と意気込みが出る内容だった。更に、主催の協会や運営委員会の方々の懇切なセミナーの企画に本当に感謝したいと思う。

内容面では、各種資料を自分自身で参考にしていたが、個人情報保護とリスクマネージメントの学習が少しおろそかであることに気付いた。

4月1日より個人情報保護法が施行されたが、スタート前に想定されたこと、予想外の問題等が発生しているのでは、あるいは各企業で新たな悩み、課題があると思われる。自身でもアンテナを高くし、情報の収集に努力したいと思うが、再度本セミナーの企画があれば、付け加えていただければ、知識、実践面でのスパイラルアップにつなげられると思う。

有難うございました。

以　上

8. 地方自治体における情報保護審議委員の仕事

No. 9 蓮見 節夫

多くの地方自治体において個人情報保護条例が制定されている。私の住んでいる市においても、個人情報保護条例があり、条例に基づき審議会があって、私は1昨年より審議委員として参加している。ここで、審議委員は何をやるのかについてご紹介しようと思う。

正確には「久喜市公文書公開・個人情報保護運営審議会」という。審議会は、公文書公開制度及び個人情報保護制度の適正かつ円滑な運営を図り、この制度をより発展させていくための審議機関として設置されたものである。審議機関は、地方自治法に基づき、市長の付属機関として設置されている。審議会の委員は、10人以内で、知識経験を有するもの、市内の公共的団体を代表する者、公募による市民から成る。私は、市の広報紙を見て公募に応じて任じられた。

審議会の所管事項は条例によって次のように規定されている。

1. 審議会は、次に掲げる事項について審議し、答申する。
   ① 公文書公開制度及び個人情報保護制度の運営に関する重要事項
   ② 保護条例の規定による実施機関が審議会の意見を聴くこととされた事項

2. 審議会は、保護条例の規定により実施機関が審議会に報告することとされた事項の報告を受けるものとする。

3. 審議会は、公文書公開制度及び個人情報保護制度の運用に関する重要事項について調査審議し、市長又は実施機関に対し意見を述べることができる。

これまで審議会は、年に2～3回程度の頻度で開かれている。

最近(昨年12月)の審議会の審議事項を紹介する。

(1) 空き地の管理保全の久喜地区消防組合への個人情報の外部提供について(諮問事項)
(2) 久喜市個人情報保護条例の改正について(諮問事項)
(3) 個人情報事務取扱事務の届出について(報告事項)
(4) その他

久喜地区消防組合への個人情報の外部提供とは、空き地に雑草が生え茂っているとき、防火や衛生面から地主に雑草を刈るよう要請するが、地主の所在地が分からないとき、市に地主の住居を教えてくれと要請がある。このとき、市は地主の住所を消防組合に教えることについて良いとするかについて、審議会に諮る、という諮問事項である。

個人情報保護条例の改正についてとは、「行政機関の保有する個人情報の保護に関する法律」が施行されることに伴い、法律に合わせて、条例の一部を改正することについて、審議会に諮る、という諮問事項である。主要な改正点は、罰則規定の部分である。

個人情報事務取扱事務の届出とは、新たな個人情報の取り扱いが発生したときの手続きのことで、少ないときで数件、多いときは数十件の新取扱が発生している。

その他は、審議委員から自由に発言できるようになっている。

私はこれまで、いくつかの問題提起を行ってきた。

一つは、「久喜市情報セキュリティポリシー」についての説明と実施状況の報告を求めてきた。

特にポリシーの中では「情報セキュリティ監査の実施」が入っていたが、有名無実とならないよう求めた。

二つ目は、住民基本台帳が、現状では誰でも閲覧できるようになっていることの問題点を指摘してきた。

また、住民票等の変更時の本人確認方法の厳格化を求めて、一部実施されてきた。

審議会の議事録は、久喜市のホームページ上で公開されている。どうぞご覧になってください。

9. 法人部会　地方公共団体情報セキュリティ

法人部会では、昨年度に引き続き、「地方公共団体向情報セキュリティセミナー」を実施いたします。セミナーの内容は、最新情報を盛り込んだ有意義なものとなっています。ぜひ、関与先、お知り合いの地方公共団体の方に、ご案内・お薦めください。

セミナー名	豊島区情報セキュリティセミナー	主催団体	東京都豊島区様
開催日時	平成16年11月24、15日	参加者	合計500名（一般職員など）
担当講師	公認システム監査人（アサップ経営システムコンサルティング）梅津尚夫		
講演内容	【A. 情報セキュリティ基本コース】 ・情報セキュリティ管理の必要性 ・電子自治体と個人情報保護法 ・多発する情報セキュリティ事件・事故 ・アクセス・コントロールを中心とした情報セキュリティ対策 ・情報セキュリティ・ポリシーと個人情報保護条例		
セミナー名	第5回地方自治体セミナー （鹿児島県内自治体向け）	主催団体	（株）鹿児島頭脳センター様
開催日時	平成17年2月15日	参加者	54名（県及び県下市町村）
担当講師	公認システム監査人（システムラボNT）高井寛彦		
講演内容	【C. 情報セキュリティ監査制度】 ・情報セキュリティ監査を取り巻く動向 ・総務省提唱の「情報セキュリティ監査ガイドライン」のポイント ・情報セキュリティ監査の方法、進め方 ・関連セキュリティ情報（個人情報保護法とISMS概要）		

＜ご参考：情報セキュリティセミナーの開催事例＞
詳細はHPをご覧下さい（http://www.saaj.or.jp/chihou/johoseminar.html）

平成17年度　地方公共団体様向け

情報セキュリティセミナーの御案内

特定非営利活動法人　日本システム監査人協会
（当協会のご紹介：http://www.saaj.or.jp/）

当協会では一般職員、管理職及び専門職の皆様へ情報セキュリティの基本的な知識から専門的な実務知識までを研修していただくため「情報セキュリティセミナー」をご提案させていただきます。

ご計画されたセミナーには当協会法人部会所属で公認システム監査人の資格を有する経験豊富な講師を派遣いたします。セミナーはいくつかのコースを組み合わせてセットにてご利用いただいても結構ですし、他の団体に呼びかけて共催として参加者を募っていただいても結構です。

各コースの内容、費用のご負担は下記を、申し込み方法は次ページをご覧下さい。

コース名	A. セキュリティ対策基本コース （標準1時間）
対　象	各部門で情報セキュリティの知識を必要とする管理者、担当職員（病院、学校を含む）
内　容	1) セキュリティの必要性　（電子自治体と個人情報保護）
	2) 脅威とリスクについて（多発するセキュリティ事故、事件）
	3) セキュリティを守るための対策（全員の心構えがセキュリティの基本）
	4) 情報セキュリティをとりまく諸制度（個人情報保護法）
コース名	B. 電子自治体と個人情報保護 （標準2時間）
対　象	各部門の個人情報取扱管理者、担当職員並びにIT管理者、担当職員
内　容	1) 個人情報保護をとりまく動向（行政サービスと個人情報保護、漏洩等事故事例）
	2) 個人情報保護法（法制定の背景、法の考え方、基本法制と地方公共団体条例）
	3) 電子自治体の個人情報保護対応（漏洩防止等安全対策、教育、委託、監査）
	4) プライバシーマーク制度の概要（JIS Q 15001と同制度の概要）
コース名	C. 情報セキュリティ監査制度 （標準2時間）
対　象	セキュリティ監査管理者、担当職員並びにIT管理者、担当職員
内　容	1) 情報セキュリティをとりまく動向（今までの経緯、法体系、セキュリティ事件など）
	2) 情報セキュリティ監査制度の紹介（総務省ガイドラインを中心に）
	3) 情報セキュリティ監査の進め方（計画、準備、実施、フォローアップ）
	4) 地方自治体に求められる情報セキュリティ対策
コース名	D. 情報セキュリティマネジメントシステム（ISMS）の概要（標準2時間）
対　象	セキュリティ監査管理者、担当職員並びに関心のある職員
内　容	1) ISMSとは．認証取得のメリット（客観的な第三者評価による信頼の獲得）
	2) 認証取得の現状（多数の民間企業と自治体では2市が取得済み）
	3) ISMS構築の流れ（マネジメントシステムPDCAの構築がカギ）
	4) ISMS認証基準の解説（詳細なセキュリティの管理項目として134基準）
コース名	E. システム監査制度の概要（標準2時間）
対　象	監査委員、IT政策担当管理者並びに関心のある職員
内　容	1) 自治体にとってのシステム監査の意義（有効な情報化推進、住民への説明責任等）
	2) システム監査の進め方（システム監査基準概説）
	3) システム監査の主なテーマ（システム管理基準概説）
	4) 関連諸制度（包括外部監査、システム監査企業台帳、総務省の指導、他）

ご負担費用：セキュリティ対策基本コースは実費（資料作成費、旅費・交通費など）のみ。
それ以外のコースは実費の他、講師派遣料（2時間当たり10万円）をご負担下さい。

（裏面に続く）

＜お申し込み方法＞

情報セキュリティセミナーは下記様式にてメール、FAX または郵便でお申し込み下さい。
なお、メールでご連絡いただく場合は様式は自由ですが下記指定項目は必ずご記入下さい。

特定非営利活動法人
日本システム監査人協会　法人部会御中

情報セキュリティセミナー申込書

平成　　年　　月　　日

団体名：
所　属：
お名前：

ご希望コース名 (右記にマーク)	○A セキュリティ対策基本　○B 電子自治体と個人情報 ○C セキュリティ監査制度　○D 情報セキュリティマネジメントシステムの概要 ○E システム監査の概要			
ご希望日	(第1希望) 平成　　年　　月　　日　　(第2希望) 平成　　年　　月　　日			
特にご希望 されること				
ご連絡先	所　属		お名前	
	電　話		FAX	
	メール			

ご記入いただいた個人情報は上記セミナー開催の準備、運営の目的ためにのみ利用いたします。

＜お申し込み先＞
メール：　saajjk1@titan.ocn.ne.jp
FAX：　03-3666-6342
郵　便：　〒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
特定非営利活動法人　日本システム監査人協会　法人部会

10. 当協会の個人情報保護方針、個人情報告知文例

個人情報保護方針

制定 平成17年4月1日
特定非営利活動法人
日本システム監査人協会
会長 宮川 公男

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」といいます。）は、自ら保有する個人情報を適正かつ安全に管理することが重要な責務と考え、ここに個人情報保護方針を定めて、当協会のすべての会員がこれを遵守し、実践することを宣言します。

1．当協会は、個人情報の収集・利用・提供に関して収集時に、情報主体（本人）に通知又は公表します。

2．当協会は、個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えいなどの予防ならびに是正に努めます。

3．当協会は、個人情報に関する法令及びその他の規範を遵守します。

4．当協会は、個人情報保護に対し継続的な改善に努めます。

以 上

個人情報の取扱いに関する問合せ先
特定非営利活動法人
日本システム監査人協会事務局
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
TEL:(03)3666-6341 FAX:(03)3666-6342
E-mail: saajjk1@titan.ocn.ne.jp

個人情報の取扱いに関する同意処理について

平成17年5月12日
NPO日本ｼｽﾃﾑ監査人協会
事務局（HP担当）

1. 既登録者への同意処理について
既に個人情報を収集（当協会に登録）している者については、次のとおりとする。
(1) メーリングリストで、個人情報保護方針を制定しホームページに掲載した旨及び下記の内容を送信し同意を得る。
(2) 会報、ホームページに個人情報保護方針及び下記の内容を掲載し、同意を得る。
2. 今後の取扱いについて
下記文例をホームページから申込むときの画面に挿入し、個人情報の取扱いについて同意を得る。また、書類についても、同様の主旨を記述のこととする。

2.1 会員用／公認システム監査人（補）（申込みを含む）用の文例

個人情報の取扱いについて

(1) 当協会の個人情報保護管理者は、当協会の事務局長です。また、連絡先は下記記載のとおりです。
(2) 当協会は、収集した個人情報を当協会の活動に必要な範囲で利用します。
(3) 当協会は、下記の場合、第三者に個人情報を提供する場合があります。
a）法令に基づき請求された場合
b）本人（会員等）が公開を同意した場合
c）その他、協会活動に必要な場合（会報掲載など）
(4) 当協会は、会報、ホームページ、メーリングリストなどの業務を委託しており、必要な個人情報を預託しております。
(5) 当協会が管理している個人情報に関して開示を求める権利や、誤りのある場合に訂正／削除を要求する権利があります。この場合、当協会の事務局にご請求ください。

個人情報の取扱いに関する問合せ先
特定非営利活動法人
日本システム監査人協会事務局
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
TEL:(03)3666-6341 FAX:(03)3666-6342
E-mail: saajjk1@titan.ocn.ne.jp

2.2 セミナー（月例研究会・実務セミナーなど）用の文例

個人情報の取扱いについて

(1) 当協会の個人情報保護管理者は、当協会の事務局長です。また、連絡先は下記記載のとおりです。
(2) 当協会は、収集した個人情報を申し込まれたセミナー実施に必要な範囲で利用します。また、当協会の継続教育などの確認に利用する場合があります。
(3) 当協会は、下記の場合第三者に個人情報を提供する場合があります。
a）他団体に受講証明などをご希望される方はその証明に必要な事項
b）法令に基づき請求された場合
c）本人（会員等）が公開を同意された場合
d）その他、協会活動に必要な場合（会報掲載など）
(4) 当協会は、会報、ホームページ、メーリングリストなどの業務を委託しており、必要な個人情報を預託しております。
(5) 当協会が管理している個人情報に関して開示を求める権利や、誤りのある場合に訂正／削除を要求する権利があります。この場合、当協会の事務局にご請求ください。

（連絡先は、上記に同じ）

2.3 同意の方法
個人情報の収集時に、入力画面の最初（上部）に上記文例（告知文）を表示し、「同意する」をクリックして、入力画面に入る（次に進む）ことができるようにする。

以　上

「システム監査普及サービス実施報告（e社）」

システム監査事例研究会
（畠中道雄）

2004年10月から2005年3月にかけて実施した、e社監査普及サービスについてご報告します。

1. 今回のシステム監査のテーマ

今回のシステム監査では「e社のセキュリティへの取り組みに関する現状を把握して、問題点・課題を明確にする。」ことを監査目的としました。e社の提供するシステムは、システムの置かれた特殊事情や重要性により、機密保持を中心にセキュリティの確保が、設計段階からの重要テーマであり、依頼者としては安定運用段階に入った現在の運用実態を把握し、万事に遺漏のないことを確認したいとの希望をもっていました。

従って、監査項目は、①機密漏えい対策、②システム継続のための安全性対策、③効率的な保守を実現するための設計とし、監査テーマとしては情報セキュリティ、その中で特に機密漏えい対策を中心に据えました。

2. システム監査の範囲

上記監査目的に沿うために、①機密漏えいに対する、ハードウェア・ソフトウェア・ネットワークにおける設計上の留意点と運用実態、②発注業務の主体であるe社、および実質的な利用者である各商社における運用実態および情報セキュリティに関する規定類・手順書の整備状況と利用者教育、③開発・保守委託先における運用実態、④現実に行われているオペレーションの規定類への適合状況、⑤アウトソーシング先との契約条項の妥当性を監査対象としました。

3. システム監査実施の手続き

管理状況の評価にあたって、ヒヤリングのチェックリストとして情報セキュリティ管理基準を使用しました。監査チームはリーダーに打矢隆司氏、サブリーダーに沼野伸生氏、畠中道雄氏、監査メンバーに今野匡氏、福原幸太郎氏、成田稔氏、海上幸宏氏、太田香氏が参加しました。

監査手続きは、e社監査依頼者に対する意向確認、経営トップヒヤリング、予備調査、本調査を実施しました。監査の進め方として、まず、今回採用しました評価基準である「情報セキュリティ管理基準」のサブコントロールレベルで、e社、委託先、システムセンター、利用部門における実態（管理基準との差異）を調査しました。委託先・システムセンターにはそれぞれ2回訪問し、詳細な確認を行ってきました。管理基準に述べられているあるべき姿に対して実態はどうか、その結果、どのようなリスクが想定されるか、具体的な事例としてどのような事件・事故が起きているか、といった観点で評価を行い、実査やヒヤリングで得た情報を元に問題点・課題を絞りこんでいきました。調査はヒヤリング、要求仕様書・設計資料・運用手順書の閲覧、運用委託先の実査・ヒヤリング、開発・保守委託先のヒヤリング・資料閲覧、利用商社の実査・ヒヤリングによって行いました。

監査経過は下表の通りです。

年月日	自	至	実施内容
2004.10.24	18:00	19:00	依頼者の意向確認
2004.11.22	18:30	20:30	トップヒヤリング
2004.12.03	15:00	19:00	e社ヒヤリング
2004.12.14	18:45	21:15	委託先ヒヤリング
2004.12.22	15:00	18:15	システムセンター実査ヒヤリング
2005.01.20	18:00	20:00	e社利用者ヒヤリング
2005.01.31	13:30	18:00	委託先実査ヒヤリング
2005.02.10	18:00	19:00	商社利用者ヒヤリング
2005.02.23	15:00	17:30	システムセンター実査ヒヤリング
2005.03.04	15:00	16:40	委託先ヒヤリング
2005.03.28	18:45	20:30	監査報告会

4. 監査結果

4.1 評価できる事項として、①e社が示したセキュリティ要件を、開発受託したベンダーが的確にブレークダウンして、セキュリティを重視したシステム設計・開発が行われていること、②運用管理者のセキュリティ教育重視の考え方に基づき、協力会社も含めてシステム利用者の教育を積

極的かつ継続的に行っていること、③低コスト運用を実現していること、④手順書・チェックリストに基づく運用が実現していること、を挙げました。

4.2 指摘事項と改善案

監査の重点を機密漏洩対策、システム継続のための安全性対策に置いていることから、複数ある指摘事項の中でも、遠隔操作端末の取扱と、データの隔地保管を緊急改善提案として報告しました。

遠隔操作端末については、設置環境の改善、アクセス記録の監視強化を提案しています。

データの隔地保管については、事業継続計画の検討や非常時の体制整備を提案する中で、e社としてすばやく業務を復旧させるために不可欠な改善策として提案しています。

この他の改善提案として以下の点を指摘し改善提案を示しました。

① 委託先や利用会社の良識と自主性に依存せず、e社独自で情報セキュリティの重要性を明文化すること。

② セキュリティ組織の中心的組織として開発・保守・運用状況を正確に把握し対応するため、月1回の報告会や障害報告を活用すること。

③ 委託先や利用会社の協力を求め、情報資産の管理状況についての報告を求めること。

④ アクセス制御をさらに強化するため、URLフィルタリング、パスワードの変更ルールの改善、スクリーンロックの設定、などを行うこと。

5. 終わりに

本システム監査事例につきましては、e社のご好意により、機密保持に十分留意することを前提に、システム監査の研鑽のため「システム監査実践・実務セミナー」の教材として整備していきますので、その際には是非セミナーに参加頂き、今回のシステム監査で得たノウハウを協会全体で共有していきたいと考えます。

「システム監査普及サービス（e社）に参加して（その1）」

福原幸太郎

私はユーザー企業の情報処理部門に二十数年従事し昨年検査部門に配属になり、システム監査を担当することになりました。今回の監査は、初めての外部監査であり、被監査組織とのコミュニケーションへの不安と監査チームとしての指摘事項の合意形成方法について興味を持って参画しました。

監査がスタートして被監査組織と再委託先（アウトソーシング先）への監査ヒアリングおよび実査が進む中で、再委託先との監査範囲に対する見解の相違により、深く掘り下げることが時間的制約を受けることになりました。しかし、監査人リーダーの的確なる決断と指示により無事予定通り監査を終えることができたように思います。

私はこの監査で、監査証跡（事実）と管理基準（尺度）の結びつきを明確にした上で、指摘事項（案）を導き出し、この指摘事項（案）を被監査組織にとっての重要度（優先度）を踏まえた指摘事項とするという監査人リーダーからの徹底した指導を受け大変良い勉強をさせて頂きました。また、私が所属する組織においても今回のような再委託先との監査見解の相違というようなものをどう解消していくかという良い経験をさせていただきました。今後、この経験を生かして一層の研鑽を積んでいこうと思います。

最後に、今回ご一緒させて頂きました監査人リーダー、メンバーの方々、ご指導有難うございました。

「システム監査普及サービス（e社）に参加して（その2）」

今野 匡

内部監査人としてのシステム監査は3年経験していますが、外部監査人としては初めての経験でした。特に、メンバーにはCSAの講師の方がいらっしゃると聞き、更に興味が高まりました。

今回はセキュリティ監査と事前に聞いていましたが、途中でJISX5080との比較という条件が入り、楽しみにしていました予備調査におけるコントロールの整備状況の確認から監査手続の策定、またそれに対するメンバーでの議論は行われず、コントロール項目ごとの分担になったのが残念でした。この点については是非別の監査で経験したいものです。

先日のシステム監査技術者試験の論文でも「システム監査の品質」の問題が出たようですが、ステークホルダーからの納得性の確保は重要な課題と認識しています。中でも監査手続が肝心で、これを蔑ろにすると被監査部門との十分な意見交換に繋がらず、実効性の低い独り善がりの監査結果に終わります。報告を受ける経営も納得しかねると思います。

「システム管理基準」や「情報セキュリティ監査基準」など、益々監査実施に用いる基準が整備される一方、被監査部門はこうした動向を理解しているとは言い難いものです。システム監査人の技量は被監査部門の改善意欲を如何に引き出せるかに掛っているのではないでしょうか。

広 告 取 扱 規 程

特定非営利活動法人
日本システム監査人協会

(目　的)

1. 本規程は、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。）の会報及びホームページ等へ広告を掲載する場合の取扱いについて規定し、当協会の会員及び当協会が認定した公認システム監査人並びにシステム監査人補（以下「公認システム監査人等」という。）の活動を支援することを目的とする。

(広告掲載基準)

2. 当協会は、当協会の会報およびホームページ等に、以下の条件を満たす広告を掲載することができる。
   (1) 広告の内容は、当協会の定款、倫理規定などに照らし、広告を掲載することが、当協会の目的、信用、品位の保持に反しないもの。
   (2) 意見広告など、当協会内に賛否両論があることが想定されないもの。
   (3) その他、広告媒体を含め広告を掲載することが妥当であると判断したもの。
   2) 理事会は、上記広告掲載条件を判定するための担当役員（以下「広告掲載担当」という。）を、3名を限度として指名する。

(広告媒体)

3. 広告媒体は、当協会の会報、ホームページ（以下「HP」という）、メーリングリスト（以下「ML」という。）等とする。

(広告出稿者)

4. 広告出稿者（広告を掲載できる者。以下「出稿者」という。）は、その住所、氏名（社名）、業種、連絡先（電話番号等）が明らかであり、料金の支払いが確かである者とする。
   なお、広告掲載に当たっては、会員および会員から推薦のあるものを優先する。

(広告料金)

5. 広告料金は、下表のとおりとし、広告掲載が確認でき次第速やかに支払いを受けるものとする。

(単位：万円)

広告媒体	広告単位（期間・回数）	出稿者		記　事
		会　員	会員外	
会　　報	1号あたり（1ページ）	8	10	
	1号あたり（半ページ）	4	5	
ホームページ	2ヶ月間（A4版1ページ）	8	10	(注1)
メーリングリスト	1回（30行1000文字以内）	2	3	(注2)

(注1) HP広告の場合、出稿者の依頼により、1回に限りHP広告と同一内容（文字のみ）をMLにも流すことができる。また、掲載期間内に募集等を締切った場合には、「締切」の文言をHP広告に追加掲載することができる。(いずれも無料)

(注2) MLについては、初回と同一内容を1週間毎に最大3回まで送信することができる。(いずれも有料)

   2) 出稿者が公益団体などの場合、広告掲載担当が発議し理事会の承認により、料金を減免することができる。

(運用細則)

6. 本規程の運用細則（事例を含む）は、広告掲載担当において別途定める。

(施行日)

7. 本広告取扱規程は、平成17年5月12日から施行する。

以　上

広告掲載ご希望の皆様へ

平成17年5月12日

広告掲載のご案内

特定非営利活動法人
日本システム監査人協会

はじめに

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」といいます。）の会員及び当協会が認定した公認システム監査人並びにシステム監査人補の活動を支援することを目的とした広告を、当協会の会報及びホームページ等に掲載することができます。

1. 広告出稿者の範囲

広告出稿者（広告を掲載できる者。以下「出稿者」といいます。）は、出稿者の住所、氏名（社名）、業種、連絡先（電話番号等）が明らかであり、料金の支払いが確かである者とします。

なお、広告掲載に当っては、会員および会員から推薦のあるものを優先します。

2. 広告掲載基準

(1) 当協会の定款、倫理規定などに照らし、広告を掲載することが、当協会の目的、信用、品位の保持に反しないものとします。

(2) 意見広告など、当協会内に賛否両論があることが想定される広告は掲載することができません。

(3) 掲載の可否については、当協会の「広告掲載担当」が判定します。

3. 広告媒体

広告媒体は、当協会の会報、ホームページ（以下「HP」といいます。）、メーリングリスト（以下「ML」といいます。）等とします。

4. 広告料金

広告料金は、下表のとおりです。

（単位：万円）

広告媒体	広告単位（期間・回数）	出稿者		記　事
		会　員	会員外	
会　　報	1号あたり（1ページ）	8	10	
	1号あたり（半ページ）	4	5	
ホームページ	2ヶ月間（A4版1ページ）	8	10	（注1）
メーリングリスト	1回（30行1000文字以内）	2	3	（注2）

（注1）HP広告の場合、出稿者の依頼により、1回に限りHP広告と同一内容（文字のみ）をMLにも流すことができます。また、掲載期間内に募集等を締切った場合に、「締切」の文言をHP広告に追加掲載することができます。（いずれも無料）

（注2）MLについては、初回と同一内容を1週間毎に最大3回まで送信することができます。（いずれも有料）

2）出稿者が公益団体などの場合、広告掲載担当が発議し当協会の理事会の承認により、料金を減免とすることができます。

5. 料金の支払い

請求書払いとし、請求書受領後（広告掲載を確認後）1週間以内に支払うものとします。

6. 申込み先（連絡先）

特定非営利活動法人
日本システム監査人協会事務局
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
TEL:(03)3666-6341 FAX:(03)3666-6342
E-mail: saajjk1@titan.ocn.ne.jp

以　上

平成17年度第4回理事会議事録

日本システム監査人協会

平成17年4月9日（水）18：30～20：00
於　　：三井物産（株）会議室
出席者：橘和、富山、鈴木（信）、鈴木（実）、小野，蓮見、岩崎、沼野、
大石、竹下、喜多、吉田、松枝、指田、木村、芳仲、桜井、馬場

1. 審議事項

(1) 個人情報保護法関連の件

SAAJは個人情報保護法の個人情報取扱事業者ではないが、（東京都の条例では5000人という制限がないこともあり、）入会申込，研究会申込などで個人情報の収集時に利用目的などの通知文を入れることについて蓮見理事より提案された。

提案内容について承認され、通知文などについては岩崎理事を中心に事務局に一任することにした。

2. 報告事項

(1) 近畿支部（喜多理事）

・近畿支部担当理事1名の海外出張による理事2名体制などもあり、昨年度は若干支部活動が停滞気味であったと思う。5月の帰国を待ち、中部支部や九州支部と同じように支部総会を開催し、支部活動の活発化を目指したい。

・3月12日に個人情報保護セミナーを開催して、98名の参加があった。

(2) 法人部会（小野副会長）

・自治体向けセミナーを16年度は2件実施できたので、17年度の案内状やセミナーの内容を見直している。6月にDM発送の予定。

(3) 監査基準プロジェクト（本田理事主査，小野副会長が代理報告）

・新「赤本」の発刊にむけて活動しており、チェックポイントを新基準にあわせていく。また北信越支部会員が作成した国際取引における監査ポイントを入れる。また、事例研と提携して進めている。

次回4／26に開催予定。

(4) 月例研究会（沼野理事，桜井理事）

・3月に企画会議を開催し、今年度のテーマ、講師候補の検討を行なった。

・今年度は5月からスタートし、例年夏休みとしている8月も開催し、年9回の開催を予定する。

・第1回（木村理事が責任理事）は、「システム監査基準の改訂とその経営的意義
ーシステム監査人に求められる経営監査の視点ー」をテーマとして
5月23日（月）に開催する。
講師は橘和副会長にお願いしている。

・第2回（桜井理事が責任理事）は、6月28日（火）に開催予定。
システム監査人が知っておくべきセキュリティ技術の最新動向について、NTTコムウェアの方に講師をお願いする。

(5) 会報（竹下理事）

・次回の会報は5／15〆で6月発行、個人情報保護に関する特集を予定

・その後は8月，10月，12月，2月と予定している。

(6) 認定委員会（鈴木（信）副会長）

・（審査部会）春の申請件数は、公認システム監査人 33名，システム監査人補 18名。5月に面接し、6月認定の予定。

・（継続教育部会）継続教育の未報告者に連絡をする。

(7) 事例研究会（吉田理事）

・e社の普及サービスが3／28報告会を開催して終了した。(10月開始)
メンバー8名で、情報セキュリティ管理基準で実施

・6月4日，5日幕張で実践セミナーを実施。

・9月3日，4日，17日，18日に金融をテーマにした実務セミナーを予定している。FISCに協力依頼状をだした。
（5月25日にFISC第一部会にc社の報告会を予定）

(8) セキュリティ監査研究会（木村理事）

・情報セキュリティ監査基準のツール化を検討している。

(9) 個人情報保護監査研究会

・出版の件は、出版社の目途がつき4月8日再スタートした。

(10) その他

・本田理事が城西国際大学の教授に就任された。

・3月19日の北信越支部総会に馬場理事が出席した。

以 上

議長 橘和尚道
議事録署名人 馬場孝悦
岩崎昭一

＜次回理事会開催予定＞

平成17年5月12日（木）18:30～
三井物産（株）15階金属A会議室（地下鉄大手町C5出口）

平成17年度第5回理事会議事録

日本システム監査人協会

平成17年5月12日（木） 18：30～20：30
於 ：三井物産（株）会議室
出席者：富山、小野、吉田、松枝、大石、竹下、馬場、岩崎、金子

1. 審議事項

(1) 理事会開催日変更の件
理事会の定例開催日を第2木曜日とする旨事務局から提案が出され、提案どうり決定した。

(2) 広告取扱規程の件
①提案事項：「広告取扱規程（案）」及び「広告掲載のご案内（案）」について提案が出された。（岩崎理事）
②「広告取扱規程（案）」の修正箇所
・2項の（1）項中、定款の前に「当協会の」を加える。
・2項の2）項中、「担当役員（以下「広告掲載担当」という。）を3名まで指名する。」を「3名を上限として担当役員（以下「広告掲載担当」という。）を指名する。」に修正する。
・5項の1項中、「支払うものとする。」を「支払いを受けるものとする。」に修正する。
・5項の2）項中、「料金を無料とすることができる。」を「料金を減免することができる。」に修正する。
・その他、表現を判りやすく修正した。
③「広告掲載のご案内（案）」の修正箇所
・省略（前記②と同様の趣旨で修正）
④決定事項
・広告掲載担当役員は、岩崎理事及び鈴木（信）副会長とする。
・修正後の本規程は本日（平成17年5月12日）から実施する。

(3) 個人情報保護方針の件
①提案事項：「個人情報保護方針（案）」、「個人情報の取扱いに関する同意処理について（案）」について提案が出された。（岩崎理事）
②「個人情報保護方針（案）」の修正箇所：
・前文中、「役員及び個人情報を取り扱う全ての者がこれを遵守し」を「当協会の全ての会員がこれを遵守し」に修正する。
・1項中、「情報主体に告知し、同意を得ます。」を「情報主体（本人）に通知又は公表します。」に修正する。
③「個人情報の取扱いに関する同意処理について（案）」の修正箇所
・1項の（5）項を削除する。
（論議内容：プライバシーマーク制度では記載することになっている内容ではあるがプライシーマーク制度の認証を受けるわけではないため、そこまで厳密にしなくともよい。入会受付においては、必須項目がないと入会を受理しないことになっているため、とりあげて協会への参加お断りなど言う必要はない。該当する局面としては氏名の会報掲載拒否があるが、本人の意思に基づき匿名を許す等の運用で対処できる。ーーーー等々、論議した結果、削除することに決定した。）
・1項の（6）項中、なおがきを削除する。
・2項についても前記と同様に修正する。
・4項の（1）項を「会報、ホームページ、メーリングリストで会員に周知する。」に修正する。
・4項の（2）項を削除する。

④決定事項:
・制定日を平成17年4月1日とする。
・個人情報保護管理者は事務局長とする。
・修正後の本文書はすみやかにホームページに掲載する。

2. 報告事項
(1) 事例研究会(吉田理事)
・2日間コースの実践セミナーを6月4日、5日にOVTAに於いて実施する。
受講申込者12名、講師4名の予定。
・4日間コースの実践セミナーを9月3日、4日、17日、18日にOVTAに於いて実施する。
最近実施した普及サービスで新教材を開発し、FISC監査基準を使用したセミナーとなる予定。
(2) メーリングリスト(岩崎理事)
・現在のメーリングリストを法人契約に切り替える予定。
・運用作業を順次メーリングリスト担当(金子理事)に切り替えてゆく。
(3) 新システム監査基準研究会(小野副会長)
・赤本改定について、記載内容のテーマが固まってきた、5月31日の会議で概ね決定できる。
・チェックリストについては、パーツごとに担当を決め作成中であり、5月31日には第一次原稿を出し、6月にレビューする計画である。
(4) 法人部会(小野副会長)
・自治体セミナーーについて、昨年は2回実施したが、今年も実施を計画中である。
・6月には、自治体向けDMを出したい。
(5) 会報(竹下理事)
・次回会報の編集方針を設定した。
・メインテーマは、3月実施した個人情報保護の講演会とする。
・協会の活動を宣伝する内容を含めたい。
・本日の理事会で審議した「個人情報保護方針」及び「広告掲載規程」を会報に掲載する。
・会報の発送は、これまで普通郵便で発送していたが、次回から大口扱いの発送方法に変更し経費の節減を図る。
(6) 各支部への依頼(馬場理事)
・近畿支部以外の支部で実施する講演会の講師謝礼などで源泉徴収税の納付が必要で本部から納付しなければならない場合は、納付期限までに間に合うように発生の都度本部事務局(会計担当)に連絡ください。
・現時点で未報告のものがあれば早急に報告ください。(近畿支部は従来とおり支部で納付をお願いします。他の支部は発生することがほとんどないため、代行納入しています)

以　上

議長　富山伸夫
議事録署名人　金子長男
小野修一

<次回理事会開催予定>
平成17年6月9日(木)18:30～
三井物産(株)15階金属A会議室(地下鉄大手町C5出口)

石島 隆(著)「情報システムの内部統制—ITに対応した評価の計画と手続」

A5判 280頁 本体価格2800円
(税込価格2940円)(2005/02/16発行)
出版社:中央経済社;ISBN: 4502250309;

著者略歴
大阪成蹊大学現代経営情報学部助教授。公認会計士,税理士,システム監査技術者,ITコーディネータ。日本公認会計士協会情報システム委員会(現IT委員会)委員・専門研究員,同業種別会計委員会建設業研究部会幹事,同近畿実務補習所講師等などを歴任。

著者は,公認会計士であるとともにシステム監査人でもあり,また会計やシステム監査についての教育にも長く携わっておられる。本協会の会員の中でも著者のテキストでシステム監査を勉強された方はたくさんおられると思う。本書は財務諸表監査に従事する公認会計士や内部監査人,経理部門や情報システム部門などにおいて内部統制の構築と見直しに携わっている人を対象に,財務報告の信頼性という目的に関連したIT内部統制評価の役割とそのあり方について書かれている。まず,各章を概観しよう。

第1章から第3章までは,情報システムの内部統制についての基礎知識が整理されている。「第1章 IT内部統制とは何か」では,コーポレート・ガバナンスと内部統制との関係,ITガバナンスとIT内部統制との関係,コーポレート・ガバナンスとIT内部統制との関係をそれぞれ比較しながら,IT内部統制とは何かについて説明されている。「第2章会計情報システムの位置付けと仕組み」では,企業における情報システムの全体像および会計情報システムの位置付けについて,会計情報の内容と会計データの処理プロセス,および会計情報システムの設計基準について説明されている。「第3章 税法上の電子帳簿保存制度」では,電子帳簿保存法の概要および承認申請,会計情報システムの対応要件について説明されている。

「第4章 IT内部統制評価の計画と手続」では,財務諸表監査におけるIT内部統制の位置付けとその評価の考え方がとりあげられている。IT内部統制に依拠するかどうかの判断,内部統制の理解と統制リスクの評価,統制評価手続きの計画と実施,IT内部統制の有効性評価の結論と報告などについて説明されている。

第5章から第7章は,内部統制評価の実務についてとりあげられている。「第5章 全般統制とは何か」では,IT内部統制における統制活動のなかで,個々のアプリケーション・システムの統制活動である業務処理統制の有効性を確保するための基盤となる全般統制について説明されている。「第6章 業務処理統制とは何か」では,財務情報の信頼性を直接的に保証する役割をになう業務処理統制について説明されている。「第7章 IT内部統制評価の具体例と留意点」では,IT内部統制評価を実際に行う際の実務的な実施手順と留意すべき事項について,具体例に基づいて説明されている。付録として,IT内部統制に係わる基準・ガイドライン・報告書などが付けられている。

本書のサブタイトルである「ITに対応した評価の計画と手続」からうかがわれるように,本書の中心となっているのは第4章である。財務報告の信頼性確保におけるIT内部統制評価についての基本的な考えがここで示されている。ITに大きく依存する現代企業の財務報告の信頼性確保においては,従来の組織や業務手続に焦点をあてた内部統制評価とは別に,IT内部統制評価の重要性が増しているとする。なお,「IT内部統制」とは著者によって用いられた用語である。ITを利用した情報システムの内部統制のことであり,財務諸表監査において評価の対象とする財務報告のための内部統制の一部をさす。実際の情報システムはコンピュータを中心にしながらも手作業の領域も多く含まれている。そのため,情報システムは,コンピュータ処理に限定されない情報処理・活用のシステムとして理解されている。著者はこのような広義の「情報システム」の意味と対比するかたちで,情報及び通信技術を使用した情報処理・活用のシステムの部分,言い換えれば純粋にITに依存した領域を分けて,その領域における内部統制を「IT内部統制」と定義している。

以上のように情報システムの内部統制について,財務報告の信頼性という観点から取り扱われており,その点で本書はまず公認会計士や内部監査人向けに書かれていると言えるだろう。いわば公認会計士や内部監査人が財務諸表にかかわるITについてより知識を深めることを目的としている。しかし,米国企業改革法(SOX法)や資本市場のグローバル化を背景に,コーポレート・ガバナンスや内部統制の強化要請は世界的潮流となっており,我が国の企業においても内部統制の強化は今や喫緊の課題となっている。そのような中において,システム監査人や情報システム部門の責任者においてもIT内部統制の強化に果たす役割が求められており,本書はまさに最適な参考書といえよう。是非御一読をお薦めしたい。なお著者にはSOX法が求めるグローバルレベルでの内部統制の強化など,本書のテーマをさらに発展していかれることを望みたい。

会報部会・活動報告

会報主査　竹下和孝

1. 概　要

会報部会は、会員とのコミュニケーションに寄与しようと活動しております。これらの会報編集の一部を紹介します。

2005年度会報担当委員

竹下和孝（主査）、富山伸夫、吉田裕孝、仲厚吉、力利則（以上、会報担当理事）

池島晃、須田勉、木村陽一、藤野明夫、山田正寛　（以上、編集委員）

2. 2005年会報の特集計画

2005. 4 . 4に開催した会報編集会議で、2005年どの大まかな特集方針と編集担当の分担を調整しました。各担当は記事の仕込みをはじめますので、執筆要請がありましたらご協力ください。

定例テーマの例

・本部理事会、事例研究会、月例研究会など本部を中心とする活動報告

・支部を中心とする活動の報告

・新入会員紹介、会員が執筆した本の紹介

また、会報掲載論文、投稿は期限の定めなく受け付けております。

号　数	発行月 (頁数)	編集担当	主な記事
84号	2005. 4 (48p)	吉田	(特集)第4期総会 システム監査実務セミナ、自治体向けセミナ
85号 今　号	2005. 6 (p)	竹下 山田	(特集)個人情報保護 セミナ報告、SAAJ会員管理の告知・ポリシ
86号 予　定	2005. 8 (p)	木村陽 藤野	(特集)セキュリティ技術
87号 予　定	2005.10 (p)	富山 池島	(特集)自治体の情報セキュリティ対策（法人部会） 公認システム監査人の活動 II
88号 予　定	2005.12 (p)	力 須田	(特集)赤本改訂 2005支部活動特集①
89号 予　定	2006. 2 (p)	仲	(特集)研究部会 2005支部活動特集②
90号 予　定	2006. 4 (p)	吉田	(特集)第5回総会

3. 会報編集の経過

SAAJ会報は年6回、2ヶ月ごとに発行していますが、これまで発行のプロセスを紹介する機会はありませんでしたので、概略の流れを紹介します。

① 会報編集会議
当番の編集担当、副担当を中心に、特集記事の企画や編集日程を練ります。

② 原稿依頼
特集記事の内容に合わせて各部会長、支部長、会員に執筆依頼をします。

③ 締め切り前後の原稿フォロー
各位のご協力を頂いて、現行の全体を組み合わせて、全体バランスと量を把握します。

④ 編集開始
当番の編集担当、副担当は、会報記事の掲載順序や見出しを決めます。

⑤ 原稿案を印刷会社に送付して、入稿、初稿作成
毎回お世話になっている印刷会社にファイルを送付します。

⑥ 初稿の校正
入稿後、レイアウトされた初稿（PDF形式）に対し校正します。(編集担当、副担当)

⑦ 初校を印刷会社に送付して、校正入稿、2稿作成
第2稿（PDF形式）に対し校正します。（編集担当、副担当）
⑧ 2稿を校正（省略する場合もあります）
第2稿（PDF形式）に対し校正します。（編集担当、副担当）
⑨ 2稿を印刷会社に送付して、印刷、封入、発送
⑩ 次回、編集会議

4. 最近発行した会報の内容

号 数	発行月 (頁数)	主な記事
78号	2004. 4 (48p)	(特集) 第3期総会 藤谷弁護士、本田理事による記念講演と総会内容を紹介
79号	2004. 4 (48p)	(特集) 中部支部中国訪問団報告 3 /18から21にかけて訪中、中国科学技術院での交流報告
80号	2004. 8 (44p)	(特集) システム監査基準改訂について 基準改訂の敬意、監査基準・管理基準（ドラフト版）
81号	2004.10 (24p)	(特集) 公認システム監査人の活動報告 組織へのシステム監査のアプローチ、事業例を3例紹介
82号	2004.12 (40p)	(特集) 協会支部の活動、付録システム監査基準、管理基準 地域のIT関連団体と相互協力し活動展開する様子を紹介
83号	2005. 2 (28p)	(特集) 研究会活動

5. 今後の活動計画
① 今年度好評だった特徴のある特集が編集できるよう目指しています。
理事会議事。月例研究会、研修会の報告。支部の活動報告。会員紹介などの定例テーマに加え、会員投稿や応募論文を増やしていきたいと考えていますので、会員各位の積極的な投稿を期待しています。
② 実務に有益な会報を目指し、活動報告と掲載論文の募集を継続します。
(編集委員を拡充し、活動の範囲を拡大する)
③ 会員から、編集委員を募集して会報活動の充実にむけて協力をいただきました。
今年度は多くの会員と支部の協力を頂いた特集に対し、会員から評価のフィードバックを頂いております。地道な活動に対する編集担当への激励に感謝しております。

6. 会報担当から意見募集
① 会報の電子化について
電子化することで、会報発行の大きな部分をしめる郵送費が節約できます。
しかしながら、印刷された会報も必要であり、会員の勧誘や活動を説明するときに有効であるとの強い要望もあります。通信が高速化されてきたとはいえPDFの送信では自宅で印刷して見るのは大変、との意見もあります。
また会員の登録住所がタイムリーに更新されないことによる、発送済み会報の返却が発生しています。(会員諸氏は、どのような会報や特集を期待しておられますか)

② 内容を分類して、メルマガ形式によるタイムリーな情報伝達を試行したいとの企画案があります。しかしながら、専任者もいない現在の編集委員の工数では、とても定期的な発行は難しい状況です。何度か編集会議での議題にもでておりますが実現できていません。(会員諸氏は、どのような会報やメルマガを期待しておられますか)

以 上

2005. 6. 1. SAAJ 会報編集部

会報掲載論文募集要領

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)の啓蒙、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　ms-wordで作成し、フロッピーディスクで会報編集委員会あて送付する。
(メールに添付する場合は、パスワードを設定する)

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. ここに掲載した論文は、公認システム監査人(補)継続教育で、10時間/1として認める。

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綱

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

第112回月例研究会「システム監査で押さえておくべき情報セキュリティ技術のポイント」のご案内

特定非営利活動法人
日本システム監査人協会

個人情報保護法やe-文書法の施行及びISMS認証取得等に伴って、システム監査人には、これまで以上に情報セキュリティ対策の妥当性を監査する機会が増えてくると思われます。一方、情報セキュリティ技術は日進月歩であり、最新の情報を的確に把握するのが非常に困難になってきております。

そこで、今回は、最新の情報セキュリティ技術の動向と、その技術の組合せや選択のポイント、並びに情報セキュリティ技術に対する監査のポイントについてご説明いただくことを企画いたしました。

個人情報保護法20条で要求されている安全管理措置のポイントを皮切りに、最新ウイルス・ハッカー対策、生体認証、暗号化及びe-文書法関連の話題やIP電話やICタグのセキュリティ等まで最新情報満載です。ご期待ください。

記

1. テーマ
「システム監査で押さえておくべき情報セキュリティ技術のポイント」

2. 日　時
2005年6月28日（火）
18時30分～20時30分

3. 場　所
中央大学　駿河台記念館　280号会議室

4. 講　師
NTTコムウェア㈱
セキュリティコンサルタント
木村　歳修　氏
（ISMS審査員、ITコーディネータ、プロジェクトマネージャ／
情報セキュリティアドミニストレータ情報処理技術者　等）

5. 会　費　会　員2,000円
非会員3,000円

6. 参加申込
日本システム監査人協会ホームページの申し込みフォーム（SSL対応）にて、2005年6月21日（火）までにお申し込みください。

7. 申込み受理
お申込みの受付ができた場合、特に確認メールは発信いたしませんので、ご了解願います。定員超過で、参加いただけない場合は、メールでその旨お知らせいたします。
申し込み確認画面をプリントし当日受付へご提示下さい。

8. 参加費の授受
参加費は、当日受付で、現金でお払いいただき、同時に領収書をお渡しいたします。
（請求書は発行いたしません）。

9. 会場案内
所在地　〒101-8324
東京都千代田区神田駿河台3-11-5
中央大学駿河台記念館

以　上

第6回システム監査実務セミナー受講者募集のご案内

システム監査未経験の皆様へ、
そして
金融機関システムの監査体験を希望される皆様へ

システム監査実務セミナーに参加し、システム監査の実際を体験してみませんか！
本セミナーでは、
金融機関システムの監査を通じて数多くの貴重な監査実務を学ぶことが出来ます！

NPO 法人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、下記の日程で第6回（平成17年第2回目）のシステム監査実務セミナーを開催いたします。

このセミナーは、当協会が既に16回の開催実績を重ねる、「システム監査実践セミナー」（1泊2日コース）の内容を拡張・充実し、前半（1泊2日）、後半（1泊2日）の延べ4日間で実施する、日本では数少ないロールプレイング形式の監査セミナーです。

セミナーでは、当協会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、実践で得たノウハウを会員の皆様と共有することを目標にしています。

特に今回のセミナーでは、金融機関システムの外部監査を事例としており、現在求められているリスク管理や情報セキュリティの厳しい要求に応える監査の視点と監査手法を学んでいただきます。

貴重な監査事例をもとにした他に例を見ない本セミナーの体験は、皆様の監査ノウハウをさらに幅広く、そして価値あるものにいたします。

また、**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申請に必要なシステム監査実務を1年間経験したものとみなされます。**

システム監査の知識はお持ちであるものの、システム監査の実務経験が少ない会員の皆さん、この機会を利用してシステム監査の実際を体験し、システム監査能力の向上を図りましょう。 非会員の方も大歓迎です。多くの皆さんの参加をお待ちしております。

本セミナーは、以下の資格をお持ちの方の認定セミナーでもあります。

- **ITコーディネータ対応専門知識研修コース**
  （1年度間上限なしで換算できる学習時間22時間。知識ポイント：5.5ポイント相当）
- **日本公認会計士協会の継続的専門研修制度におけるCPE認定研修（予定）**

記

1. 日　　時　（前半）　平成17年9月3日（土）～4日（日）
　　第1日目 10：00～20：00　　第二日目9：00～15：00
　　（後半）　平成17年9月17日（土）～18日（日）
　　第1日目 10：00～20：30　　第二日目9：00～15：00
　　＊参加は、前半・後半の通しとし、どちらか一方のみの参加は出来ません。

2. 場　　所　幕張 OVTA（海外職業訓練センタ）
〒 261-0021　千葉市美浜区ひび野 1 丁目 1 番地（℡：043-276-0211）

3. 費　　用　会員：168,000 円、非会員：189,000 円（宿泊費、食事費、消費税を含む）
＊他に以下のテキストが必要になります。
①日本システム監査人協会編「情報システム監査実践マニュアル」
（工業調査会　定価 4,200 円税別）
②（財）金融情報システムセンター殿発刊「金融機関等のシステム監査指針」
（定価 20,000 円税別）

4. セミナー内容　事例研究会が実施したシステム監査普及サービスをケーススタディとして取り上げます。
4 ～ 5 人程度のグループに分かれ、監査依頼事項の確認、トップインタビュー、監査テーマ・監査計画の作成、予備調査、本調査、監査報告の実際を、4 日間のセミナーを通し体験して頂きます。
システム監査基準は「金融機関等のシステム監査指針」を使用します。

5. 講　　師　事例研究会メンバーのシステム監査普及サービス経験者 6 名（予定）
講師は監査手順の解説・指導の他、被監査企業の社員の役割も演じます。

6. 募集対象者および人員
日本システム監査人協会会員（法人会員を含む）、
システム監査技術者試験合格者あるいは同等の能力を持つ方、
システム監査に従事されている方及び今後予定されている方
定員 20 名（最小催行人員 10 名）

7. 申し込み先　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　太田　香
※下記の参加申込書の形式で E-Mail でお申し込みください。
(E-Mail：otamail@pop21.odn.ne.jp)

8. 申し込み期限　平成 17 年 8 月 12 日（金）

9. 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　太田　香
(E-Mail：otamail@pop21.odn.ne.jp)

以　上

NPO法人日本システム監査人協会
第6回システム監査実務セミナー参加申込書

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、郵便番号、宛名）

5. 連絡先（E-MAILアドレス、電話 No、FAX-No）

6. 請求書発行希望有無（あり（宛先名称）／なし）

7. 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）

8. システム監査実施経験（あり／なし）

9. テキスト①「情報システム監査実践マニュアル」の購入希望（あり／なし）
＊購入希望の方には、市販価格の2割引（3,600円税込み）で頒布いたします。受講料にテキスト費用を加えてお振込み下さい。

10. テキスト②「金融機関等のシステム監査指針」の購入方法問い合わせ（する／しない）
＊ご自身で事前に準備をお願いします。購入方法はお問い合わせいただければ事務局よりご案内します。

以　上

（注：記入頂いた個人情報は、セミナー受講管理の目的で利用いたします）

（編集後記）

昨年来、地震、集中豪雨、大規模事故、個人情報漏洩など事業の継続を揺るがすような事件が続き、事業継続計画の作成が話題になっています。

2000年を迎えるときのY2K対応の時に、緊急連絡網の整備は出来ていたのではないか、その後、利用していなかったので陳腐化したり、解散したり、個々の組織で事情は違う。緊急連絡網は、責任者の名前と電話番号を載せておくことが目的ではなく、非常時の意思決定を伝達する手段の一つである。電話が通じない状況でどうするのか、リスクマネジメントとクライシスマネジメント（危機管理）を今一度、平常時のうちに考えておきたい。（KT）

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　宮川　公男
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　池島　晃
富山　伸夫　須田　勉
吉田　裕孝　木村　陽一
仲　厚吉　藤野　明夫
力　利則　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