特定非営利活動法人
日本システム監査人協会報

2015年5月号
No 170

No. 170（2015年5月号）＜4月25日発行＞

気まぐれな天気に翻弄されましたが、良い季節が

確実にそこまで来ています。

システム監査人の応援歌でまとめてみました。

巻頭言

『 CSAの資格はあなたの役に立っていますか！ 』

会員番号: 281 力 利則 （副会長）

私が担当している**CSA利用推進G**の目標は、**「CSAの認定を受けて良かったと思ってもらえる活動」**です。CSA（ASA）になって良かったと思ってもらえる方が増えれば、資格の継続更新をして頂ける方が増え、その方々の活動に刺激されて、新規にCSA（ASA）になろうという方も増えると考えています。この目標達成のために、CSA利用推進Gでは、皆様にもいくつかの取組みやお願いをしていますので、ご紹介させていただきます。

続きは、投稿記事「CSAの資格はあなたの役に立っていますか！」をご覧ください。

＜目次＞

各行から Ctrl キー+クリックで
該当記事にジャンプできます。
（各記事末尾には目次へ戻るリンク有）

＜目次＞

○　巻頭言 …… 1
【 ＣＳＡの資格はあなたの役に立っていますか！】

１．めだか …… 3
【マネジメントシステム内部監査におけるシステム監査人の責任】
【心をつかみ、その気にさせる】

２．投稿 …… 5
【システム監査人の魅力】
【ＣＳＡの資格はあなたの役に立っていますか！】

３．本部報告 …… 7
【第 26 回 CSA フォーラム報告】
【「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」その８】
～ 「経済産業省ガイドライン」の読みこなしポイント ～ （最終回）

４．支部報告 …… 13
近畿支部 【地方公共団体における情報セキュリティ監査に関するガイドライン（案）】
総務省へのパブリックコメント

５．注目情報 …… 14
【情報セキュリティ 10 大脅威 2015】
【企業におけるマイナンバー制度実務」（総務編） 】
【ISMS ユーザーズガイド -リスクマネジメント編-】

６．セミナー開催案内 …… 15
【協会主催イベント・セミナー等：「月例研究会（東京）」、他】
【外部主催イベント・セミナー： 「システム監査学会 第 29 回研究大会」、他】

７．協会からのお知らせ …… 17
【新たに会員になられた方々へ】
【協会行事一覧】

８．会報編集部からのお知らせ …… 19

2015.4

めだか　【　マネジメントシステム内部監査におけるシステム監査人の責任　】

企業は、事業継続のため、収入・支出のバランスをとり、品質向上、環境配慮、情報セキュリティ、食品安全、個人情報保護などの体制に問題が無いよう継続的改善が求められる。継続的改善のため、マネジメントシステムの内部監査は、PDCAサイクルの“C”の機能を担っており、“PD”がしっかりと運用されているかを監査し、代表者に報告して代表者の見直し、すなわち“A”を導くことが役割である。システム監査人の責任は、情報システムへの監査をもとに、情報システムのリスクに応じてコントロールが適切に整備・運用されているかを点検し、代表者に報告を行うことである。

先月号で、2014年（平成26年）8月に経済産業省より伊藤レポートとして、「持続的成長への競争力とインセンティブ～企業と投資家の望ましい関係構築～」プロジェクトの最終報告書が公表されたことを紹介した。主要メッセージは5つである。

1）企業と投資家の「協創」による持続的価値創造　2）資本コストを上回るROE（自己資本利益率）、そして資本効率革命　3）全体最適に立ったインベストメント・チェーン変革　4）企業と投資家による「高質の対話」を追求する「対話先進国」　5）「経営者・投資家フォーラム（仮）」の創設

同レポートの第4章に、“マネジメントシステムと経営者のインセンティブ”についての報告がある。マネジメントシステムについては、

“企業が投資家と建設的な関係を構築し、持続的成長という共通の目的を達成するため、
どのようなマネジメントシステムが求められるのか、
取締役会の機能は現状どのように評価され、今後どうあるべきか。”　を論点としている。

上記の議論では、取締役会の機能を高めるため、取締役会の構成について、社内か社外かといったことのみならず、全体として能力や経験等のバランスが取れており価値観の多様性が確保されていること、適正な人数に保つことが求められるとしている。また、社外取締役等の非業務執行役員に関して、社外取締役に期待される役割は、取締役会およびマネジメントシステム全体の機能の中に位置づけて考えられるとしている。そして、国によって取締役会に期待される役割は異なるが、その果たすべき使命を基本方針や中長期計画等において明確にすることが重要であると提言している。

システム監査人は、企業が投資家と建設的な関係を構築し持続的成長という共通の目的を達成するため、どのようなマネジメントシステムが求められるのかを知ること、また、そのマネジメントシステムの中で、情報システム、及びシステム監査は、どうあるのか方向性を考えることが求められる。

（空心菜）

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

＜目次＞

2015.4

めだか　【心をつかみ、その気にさせる】

マネジメントシステム（以降、MS）内部監査におけるシステム監査人の責任の一つとして「MSの有効性の継続的改善のけん引役を果たすこと。」があると思います。MSをうまく活用して事業をもっと好転させるために、「経営者と現場の橋渡しをする。」とも言えます。システム監査基準には、1985年の制定当初から最新改訂版にいたるまで、「システム監査は、経営の目的達成に資する」旨の考え方が貫かれており、「情報戦略と経営戦略との整合」、「経営環境及び適用業務の変化に応じた見直し」等、監査の項目の中に、経営に関するキーワードが多く含まれています。このような考え方をマスターしているシステム監査人は、けん引役及び橋渡しとして打って付けだと思っています。

ISOの世界では、2012年に、ISO-MS規格（MSS：Management System Standard）の上位構造（HLS：High Level Structure）（＊1)を共通化することが決まり、ISO/IEC27001(ISMS)は2014年に改訂され、ISO9001(QMS)、ISO14001(EMS)も順に改訂されつつあります。

共通化された上位構造の中の「組織の外部・内部の課題を決定しなければならない。」及び「組織のプロセスへのMS要求事項の統合を確実にしなければならない。」等の要求事項で表されているように、MSを組織の経営（事業）活動の道具として使うように促しており、「ISOのためのISO（認証取得のための活動）をやっていてはダメですよ。」と言っているのです。

規格改訂に伴って、MSの内部監査でもルール遵守状況の確認を超えて、MSが事業に役だっているかの観点での確認が求められるのです。正に、経営に資することを強く意識しているシステム監査人の出番です。♪♪♪

（＊1）規格構成：4.組織の状況、5.リーダーシップ、6.計画、7.支援、8.運用、9.パフォーマンス評価、10.改善

私が続けているバレエのレッスンでは、必死に振り（動き）を覚えてマスターしたと思ったところで、先生によく、「皆さんは、今の振りで、発表会を見に来て下さるお客様に何を伝えたいの？」 と問われます。「振りは正しいし、一生懸命がんばっているようだけど、形どおりに順番を追うだけでは見ていてもつまらないだけです。」 と厳しいお言葉。でも確かにそうなのです。与えられた形で、順番も間違えずに、それなりの技術を身に着けて動いていても、お客様に伝えたい思いを心に秘め、その思いが伝わるように、ポールドブラ（手の運び）、足の運び、リズムの取り方等を工夫しないと、お客様の心を動かすことはできないのです。（照れくさいけど顔の表情も大事。）

経営に資する監査の実現のためには、経営者や被監査部門の人々の心をつかみ、その気にさせて、「話を聞いてみようじゃないか。」 と思わせる必要があります。そのためには、まず、自分が伝えたい思いをしっかり持った上で、事前準備、現地監査、監査報告書作成、監査報告会に臨む必要があります。関係者の心をつかみ、改善意欲を沸かせ、監査を実施したことにより、経営的に見ても組織の状況を確実に前進させることがシステム監査人の責任だと思います。

（いつかエトワール）

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

＜目次＞

2015.4

投稿【　システム監査人の魅力　】

会員番号　0557　仲　厚吉　（会長）

養老孟司先生の「「自分」の壁」という本を読みました。先生は、”最初の主題はいわゆる「自分」という問題です。”と述べています。日本は列島の国で四囲を海に囲まれており太古から人は海を渡ってこの列島にやってきました。日本人はこの列島という地理の中で「世間」というルールを暗黙知として暮らしてきたのだと思います。いっぽう、例えば、アメリカ合衆国は 240 年前に建国され、アメリカ人はフロンティアを開拓するなかで個々人の「個性」や「独創性」が重要であるという価値観を持っています。だから、それぞれの国や地域で、「自分」という問題は違っていて、日本なら日本人の自分や自分の壁を考える必要があります。

脳の中には「方向定位連合野」という分野があって、からだの境界、空間と時間をつかさどっています。「「自分」の壁」の本のなかに、ジル・ボルト・テイラー博士の「奇跡の脳」からの引用があります。博士自身、脳卒中でこの分野に損傷が起きました。「「自分」の壁」が無くなって自分が世界と一体化してここちよい状態になる、博士はそれを“涅槃（ニルヴァーナ）”と言っています。つまり、“からだの境界、空間と時間”から解放された世界を発見したということでしょうか。

さて、「「自分」の壁」という観点から「システム監査人の魅力」を考えてみます。人は性格によって、自分の壁が厚い人と薄い人があります。自分の壁が厚い人は、世間知らずと言われ、自分の壁が薄い人は、世間に合せて個性が無い人と言われます。システム監査は、システム監査を受ける人とシステム監査人の間の対話で成り立っています。システム監査人は、自分自身が、自分の壁が厚いほうか薄いほうかを知る必要があります。また、システム監査を受ける人がどちらのタイプかを判断してシステム監査を行うことはシステム監査人の魅力につながる大切なことだと思います。

当協会では、2008 年に今後の 10 年に取り組むべき課題を挙げ、2014 年に見直しを掛け、2017 年末までの残る3年間に課題を解決するべく取り組んでいます。そのなかで 2015 年度は協会運営の方向性として、システム監査の普及、促進活動の一層の推進のため協会の信頼性を高めるよう協会活動を行うこと、すなわち、会員の皆様から頂いた寄附の実績などをもとに東京都の「認定 NPO 法人」を目指すこと、認定によって協会の信頼性、システム監査人の社会的評価の向上を図ることに取り組んでいます。

また、システム監査の活性化の一環として、IT-Audit などの ISO 化、JIS 化、システム監査に関連する他団体との交流に取り組み、会員とのコミュニケーション向上のためホームページの整備、会員ポータルサイトの導入を進めています。システム監査の2大テーマとして、IT ガバナンス（Corporate governance of information technology）と IT 人材の育成をとりあげ、システム監査の活性化やシステム監査人の活用になるよう活動を進めていきます。

参考1：「「自分」の壁」 養老孟司 著　新潮新書 576
参考2：「奇跡の脳（My Stroke of Insight）」 ジル・ボルト・テイラー 著　竹内薫 訳　新潮社

以上

＜目次＞

2015.4

投稿【ＣＳＡの資格はあなたの役に立っていますか！】

会員番号 0281 力 利則 （副会長）

私が担当しているCSA利用推進Gの目標は、「CSAの認定を受けて良かったと思ってもらえる活動」です。CSA（ASA）になって良かったと思ってもらえる方が増えれば、資格の継続更新をして頂ける方が増え、その方々の活動に刺激されて、新規にCSA（ASA）になろうという方も増えると考えています。この目標達成のために、CSA利用推進Gでは、皆様にもいくつかの取組みやお願いをしていますので、ご紹介させていただきます。

(1)CSA（ASA）のことを世の中に知ってもらう方策

（皆様方にもご協力をお願いします！）

①CSA（ASA）の認定を受けている方は名刺や履歴書に記載していますか？そして名刺交換をした時にCSAの説明を少し会話に加えてみてください。

②CSA認定カードを発行しています。企業に所属せずにお客様を訪問する時や自分のことを示したい時にネームプレートとして活用できます。有料ですが使える場面も多々あります。

③CSA（ASA）を官公庁や自治体の入札条件の資格に加えて頂く。すでに記載して頂いていることもありますが、システム監査技術者等よりもさらに実践を踏んだ資格であることをもっと強調する必要もあります。 ④法人や企業における求人の資格条件にCSA（ASA）を加えて頂く。皆様の所属する法人や企業の求人情報にもぜひ加えてもらってください。CSA（ASA）に限定するわけではありませんが、広く世の中に知ってもらうにはいい方法です。

(2)CSA（ASA）になられた方々の交流の場、相互啓発の場、協業の場の提供

（ぜひ積極的にご参加ください。仲間が増えます。）

①この目的で始めたCSAフォーラムは先日第26回目を迎えました。2ヶ月に1回程度の開催です。フェースtoフェースを大切にということで、質疑やディスカッションの時間を十分取り集まって頂いた皆様がより主体的に参加できるようにしています。フォーラム後の懇親会も役に立つ相互啓発の場になっています。

②CSA（ASA）同士の知り合いにこの輪を広げることにより、お互いの仕事でもうまく協力できることも多くあると思います。システム監査は幅広い知識と専門的な経験が必要なので仕事としての連携や協業にもかなり向いています。

以上、CSA利用推進Gが活動していること、しようとしていることを書きました。SAAJのHPのCSA各種手続きに具体的な説明や書類が掲載されています。まだまだ十分とは言えませんが、ぜひ皆様の積極的なご参加と行動をお願い致します。皆様方からもご要望やご意見もお待ちしています。

以上

＜目次＞

2015.4

第 26 回ＣＳＡフォーラム開催【データベースの視点から考えるセキュリティ、内部統制】

会員番号 6005 斉藤 茂雄 （CSA 利用推進 G）

今回は、株式会社アクアシステムズの安澤弘子(あんざわひろこ) 様を講師に迎えました。安澤様はデータベースにおける情報セキュリティコンサルティングをお仕事にされ、「データベース・セキュリティ・コンソーシアム（DBSC）」の運営委員としてもご活躍されています。今回はデータベースとはどういったもので、セキュリティ上どんなリスクを持つのか、どう対策するのかといった広範な内容を、世の中の事例や安澤様ご自身が担当した調査結果を織り交ぜ、熱く語っていただきました。参加者からもデータベースを取り巻く諸課題について、網羅的に知ることができたといった意見があり、大変有意義な2時間でした。開催の概要は以下です。終了後講師を囲んで短時間ですが懇親会を実施しました。

タイトル：「データベースの視点から考えるセキュリティ、内部統制」

概要（当日使用スライドのコンテンツより一部抜粋）：

- DBSC（データベース・セキュリティ・コンソーシアム）について
  - ✓ データベースセキュリティに関するガイドライン
  - ✓ DBA 1,000 人に聞きましたアンケート調査 WG
- データベースの位置づけと役割
  - ✓ データベースのお話し
  - ✓ OS とデータベース
  - ✓ ビッグデータについて
- データベースのリスク
  - ✓ データベースへの脅威と対策
  - ✓ AP/WEB の脆弱性による DB 攻撃
  - ✓ 内部リスク
- データベースセキュリティの考え方
  - ✓ 境界防御偏重からの脱却
  - ✓ データベースにおけるリスクと対策
  - ✓ SQL インジェクション対策
  - ✓ 内部リスク　管理者対策
- データベース監査ログとは何か、具体的な活用方法
- クラウド時代を見据えて
  - ✓ クラウド環境で考慮すべきこと

開催日時： 2015 年 3 月 23 日（月） 18 時 30 分～20 時 30 分　　**開催場所**：（株）日立システムズ 本社

■■■■■■■■■――■■■■■■■■■

CSAフォーラムはCSA・ASAの皆様が、「システム監査に関する実務や事例研究、理論研究等」を通して、システム監査業務に役に立つ研究を行う場です。CSA・ASA同士のフェイスtoフェイスの交流を図ることにより、相互啓発や情報交換を行い、CSA・ASAのスキルを高め、よってCSA・ASAのステータス向上を図ります。ご参加のお問い合わせはCSAフォーラム事務局：csa＠saaj.jp まで（＠は小文字変換要）

■■■■■■■■■――■■■■■■■■■

CSA利用推進Gのキャッチフレーズ⇒*CSA・ASAを取得してさらに良かったと思ってもらえる資格にしましょう！！*

＜目次＞

2015.4

～「経済産業省ガイドライン」の読みこなしポイント～　　その８（最終回）

「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」

2-2-6. 苦情の処理、2-2-7. 経過措置、2-3. 研究機関等、3.「勧告」等、４. 見直し　5. 参考規格

会員番号　6005　斉藤茂雄　（個人情報保護監査研究会）

※個人情報保護監査研究会注：本稿は「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」（2014年12月12日改正部分は文中アンダーラインで表示）に沿って解説します。全文については、改正METIガイドライン本文を参照してください。

2-2-6. 苦情の処理（法第３１条関連）

法第３１条第１項

個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。

法第３１条第２項

個人情報取扱事業者は、前項の目的を達成するために必要な体制の整備に努めなければならない。

個人情報取扱事業者は、苦情処理窓口の設置や苦情処理の手順を定める等必要な体制の整備に努めなければならない。もっとも、無理な要求にまで応じなければならないものではない。

必要な体制の整備に当たっては、日本工業規格 JISQ10002「品質マネジメント－顧客満足－組織における苦情対応のための指針」を参考にすることができる。

※個人情報保護監査研究会注：JISQ10002　の序文では、苦情対応プロセスを通じて得られた情報は，製品及びプロセスの改善につながり，適切に苦情対応した場合には，組織の規模，所在地及び活動分野に関係なく，組織の評価が高まることになる。と、苦情に対する考え方の基本が述べられています。苦情は、代表者にまで報告があがる仕組みが必要です。そのため、”無理な要求”と判断する場合にも、原則として代表者に報告する必要があります。

2-2-7. 経過措置（法附則第２条～第５条関連）

（本人の同意に関する経過措置）

法附則第２条

この法律の施行前になされた本人の個人情報の取扱いに関する同意がある場合において、その同意が第１５条第１項の規定により特定される利用目的以外の目的で個人情報を取り扱うことを認める旨の同意に相当するものであるときは、第１６条第１項又は第２項の同意があったものとみなす。

※個人情報保護監査研究会注：個人情報保護法の施行（2003年5月30日公布・施行）前に、本人から「利用目的を極端に制限しない条件で同意を得ていた場合」には、法第15条1項（利用目的の特定）、法第16条第1項（利用目的の範囲内で取り扱うこと）、同第2項（承継において利用目的の範囲内で取り扱うこと）について、本人の同意があったものとみなされるのが、「経過措置」です。

> **法附則第３条**
> **この法律の施行前になされた本人の個人情報の取扱いに関する同意がある場合において、その同意が第２３条第１項の規定による個人データの第三者への提供を認める旨の同意に相当するものであるときは、同項の同意があったものとみなす。**

第三者への提供に関しても、個人情報保護法の施行前に本人から同意を得ていれば、法施行後も引き続き、第２３条第１項（第三者提供に係る同意）があったものとみなされます。

> **（通知に関する経過措置）　法附則第４条**
> **第２３条第２項の規定により本人に通知し、又は本人が容易に知り得る状態に置かなければならない事項に相当する事項について、この法律の施行前に、本人に通知されているときは、当該通知は、同項の規定により行われたものとみなす。**

第三者提供について、法施行前に通知または公表していれば、第２３条第２項（第三者提供に係る通知・公表）は行われたものとみなされます。

※個人情報保護監査研究会注：個人情報保護法が施行されて10年以上経過した現在、「経過措置」の拡大解釈は許されません。利用目的をできる限り特定して、通知または公表しなければならないという原則に従うことが重要です。

2-3. 民間団体付属の研究機関等における個人情報の取扱いについて

> **法第５０条第１項第３号**
> **個人情報取扱事業者のうち次の各号に掲げる者については、その個人情報を取り扱う目的の全部又は一部がそれぞれ当該各号に規定する目的であるときは、前章の規定は、適用しない。**
> **一　放送機関、新聞社、通信社その他の報道機関（報道を業として行う個人を含む。）報道の用に供する目的**
> **二　著述を業として行う者　著述の用に供する目的**
> **三　大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者　学術研究の用に供する目的**
> **四　宗教団体　宗教活動（これに付随する活動を含む。）の用に供する目的**
> **五　政治団体　政治活動（これに付随する活動を含む。）の用に供する目的**

民間研究機関等において、その活動が学術研究の用に供する目的である場合、第四章（個人情報取扱事業者の義務等）の適用除外となります。ただし、「○○研究所」との名称を有していても、単に製品開発を目的としているものについては、本法の「学術研究を目的とする機関又は団体」には該当しません。

※個人情報保護監査研究会注：2003年の個人情報保護法の制定にあたっては、報道機関、著述業者、宗教団体等から、法制化に強い反対がありました。憲法第21条で保障する「表現の自由」との関連による主張です。当研究会では、適用除外とされる、全文を掲載しましたが、経済産業省ガイドラインでは、三のみに触れています。

3.「勧告」、「命令」及び「緊急命令」についての考え方

> **法第３４条第１項**
> **主務大臣は、個人情報取扱事業者が第１６条から第１８条まで、第２０条から第２７条まで又は第３０条第２項の規定に違反した場合において個人の権利利益を保護するため必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる。**

※個人情報保護監査研究会注:法34条第1項では、以下の違反が対象となります。
第16条(利用目的による制限)、第17条(適正な取得)、第18条(利用目的の通知等)、第20条(安全管理措置)、第21条(従業者の監督)、第22条(委託先の監督)、第23条(第三者提供)、第24条(保有個人データの公表)、第25条(開示)、第26条(訂正等)、第27条(利用停止等)、第30条第2項(手数料の額)

法第34条に規定される経済産業大臣の「勧告」「命令」及び「緊急命令」については、事業者がガイドラインに沿って必要な措置等を講じたか否かにつき判断して行われます。

ガイドライン中、「しなければならない」とされている規定に従わなかった場合は、規定違反と判断され得ます。一方、「望ましい」とされている規定に従わなかった場合は、規定違反と判断されませんが、個人情報保護の推進の観点からできるだけ取り組むことが望まれます。

「命令」は、個人の重大な権利利益の侵害が切迫していると認められ、かつ「勧告」に従わないときに発せられます。「緊急命令」は、緊急に措置をとる必要があると認められるときに、「勧告」を前置せずに行われます。

※個人情報保護監査研究会注:勧告や命令の判断に、ガイドライン中の「しなければならない」「望ましい」という記述が重要になりますが、本稿ではガイドライン本文の割愛、要約、表現変更などを行っていますので、正確には改正METIガイドライン本文を参照してください。

> **法第５６条**
> **第３４条第２項又は第３項の規定による命令に違反した者は、６月以下の懲役又は３０万円以下の罰金に処する。**

第34条第2項(命令)又は第3項(緊急命令)については、措置を講ずべき期間が設定され、当該期間中に措置が講じられない場合に、「罰則」が適用されます。

４．ガイドラインの見直し

本ガイドラインは、法の施行後の状況等諸環境の変化を踏まえて毎年見直しを行うよう努めるものとする。

５．個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・規格

※個人情報保護監査研究会注:今回のガイドライン改定で、「個人情報保護のためのマネジメントシステム」の構造がより明確にされました。

（１）個人情報保護のためのマネジメント体制の確立

体制の整備に当たっては、JIS Q 15001「個人情報保護マネジメントシステム」を、

安全管理措置の実施に当たっては、JIS X 5070「情報技術セキュリティの評価基準」、JIS Q 27001「情報セキュリティマネジメントシステム」、JIS Q 27002「情報セキュリティ管理策の実践のための規範」、情報処理推進機構（IPA）の「組織における内部不正防止ガイドライン」、総務省・経済産業省の「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」、ISO/IEC 18033（暗号アルゴリズム国際規格）等を、安全管理措置の実施状況の確認に当たっては、経済産業省の「情報セキュリティ監査制度」を、それぞれ参考にすることができます。

（２）個人情報保護を推進する上での考え方や方針の策定等

方針には、以下に掲げる点を考慮した事項を盛り込みます。

●事業の内容及び規模を考慮した適切な個人情報の取扱いに関すること。

(ア)取得する個人情報の利用目的

(イ)＜個人データの取扱いの委託を行う場合＞

(ウ)＜本人の同意なく第三者提供する場合＞

(エ)＜共同利用する場合＞

(オ)以下の保有個人データに関すること

(カ)開示等の求めに応じる手続に関すること

(キ)問い合わせ及び苦情の受付窓口に関すること

●個人情報の保護に関する法律を遵守すること。

●個人情報の安全管理措置に関すること。

●マネジメントシステムの継続的改善に関すること。

（３）消費者等本人に対する分かりやすい説明の実施

事業者は、消費者等本人に対して、個人情報保護を推進する上での考え方や方針等について、消費者等本人に誤解を与えることなく分かりやすい表現で表示することが望ましい。

分かりやすい説明の実施に際して参考とすべき基準

1. 記載事項

(1)必要十分な記載事項

1 個人情報の取扱いに関する情報として、以下の7項目が記載されていること

1)提供するサービスの概要

2)取得する個人情報と取得の方法

3)個人情報の利用目的

4)個人情報や個人情報を加工したデータの第三者への提供の有無及び提供先

5)消費者等本人による個人情報の提供の停止の可否、訂正及びその方法

6)問合せ先

7)保存期間、廃棄

2. 記載方法

(1)取得する個人情報とその取得方法に係る記載方法

2 取得する個人情報の項目とその取得方法について、可能な限り細分化し、具体的に記載していること

3 取得する個人情報の項目やその取得方法のうち、消費者等本人にとって分かりにくいものを明確に記載していること

(2)個人情報の利用目的に係る記載方法

4 取得する個人情報の利用目的を特定し、具体的に記載していること

5 個人情報の利用目的が、取得する個人情報の項目と対応して記載されていること

6 取得する個人情報の利用目的のうち、消費者等本人にとって分かりにくいものを明確に記載していること

(3)第三者への提供の有無及び個人情報や個人情報を加工したデータの提供先に係る記載方法

7 事業者が取得する個人情報や個人情報を加工したデータを第三者に提供する場合、その提供先及び提供目的が記載されていること

8 加工したデータを第三者に提供する場合、その加工方法が記載されていること

(4)消費者等本人による個人情報の提供の停止の可否及びその方法に係る記載方法

9 事業者による個人情報の取得の中止又は利用の停止が可能であるかが記載され、可能である場合には取得の中止方法又は利用の停止方法を明示して記載していること

上記の「参考とすべき基準」は、「パーソナルデータ」を利活用してサービスを行う事業者が、消費者から「パーソナルデータ」を取得し利用する際に、消費者に対して行う説明文書等の内容について、その適切性を、第三者評価するツールとして、経済産業省策定「評価基準」を基に作成されたものです。
評価方法等については、経済産業省ホームページの「個人情報保護」のページに掲載されています。

URL:http://www.meti.go.jp/policy/it_policy/privacy/index.html

・・・・・・―*・・・・・・―*・・・・・・―*・・・・・・―*・・・・・・―*・・・・・・―*

2014年8月号から連載開始した、～「経済産業省ガイドライン」の読みこなしポイント～ は、今回をもちまして完結となります。途中12月にガイドラインの改定があり、編集に苦慮する場面もありましたが、有益な活動となりました。皆様には長期間ご愛読ありがとうございました。(主査 斎藤由紀子)

バックナンバー目次 http://1.33.170.249/saajpmsMETIGL/000METIGL.html

(↑バックナンバー目次のURLが変更となりました。)

担当執筆者のコメント(斉藤茂雄):

私は2014年4月に当研究会に参加し、保護法の勉強のために連載第3回から執筆を担当させてもらいました。執筆とはいうものの、METIガイドライン原文を取捨し、会報のスタイルに整形することが主で、研究会メンバーに校閲をお願いし、特に斎藤由紀子主査には大幅な加筆訂正をいただきました。今回無事連載を終了することが出来たのは研究会メンバーのご支援と読者の皆様のご理解の賜物と御礼申し上げます。

以上

＜目次＞

2015.4

【活動報告】「地方公共団体における情報セキュリティ監査に関するガイドライン（案）」（総務省）へのパブリックコメント

会員番号 1566 田淵隆明 （近畿支部･システム監査法制化推進プロジェクト主査）

2015年2月に総務省がパブリックコメント募集を開始した「地方公共団体における情報セキュリティ監査に関するガイドライン（案)」に対し、我々は当SAAJの設立目的や規約に記載のある「システム監査の普及」に則った意見を、同省の地域力創造グループ・地域情報政策室へ表明（Emailで連絡）した。内容は以下の通りである。

1.情報セキュリティといった、安全性に特化した監査では、部分最適に陥る可能性がある。むしろ信頼性・効率性等も含めた大局高所からのシステム監査の中での、情報セキュリティ項目のチェックの方が良いのではないか。たとえばオープンソースの一部利用による、特定OSへの攻撃の被害回避や、信頼できる無料ソフト活用による費用削減等、総合的に評価を下すべきである。
2.自治体等の官公庁のIT関係の監査は、有資格者（システム監査技術者、公認システム監査人、CISA等）のみに限定すべきである。なお、情報セキュリティ中心の監査の場合は、電気通信主任技術者や情報セキュリティスペシャリストも選択肢に加えるべきである。

ちなみに2015年1月から施行された「サイバーセキュリティ基本法」の第5条では、地方公共団体におけるサイバーセキュリティに関する自主的な施策の策定と実施が、責務として記載されている。これによりセキュリティポリシーの策定が必須となった。ポリシーガイドでは監査・自己点検の項で独立かつ専門的知識を有する専門家によって情報セキュリティ監査や自己点検を行うと定められている。すなわち、情報セキュリティ監査を実施しなければ結果的にポリシーに背くことになり、結果的に法令違反になると判読できる。

また、2015年4月から施行された、内閣官房によるIT総合戦略本部「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書」では、セキュリティ監査から脱皮して本来のシステム監査として、一過性でなく体系的な取り組みが必要と、政府機関でもシステム監査3年計画を標榜している。たとえば「運用・保守業務の効率性及び経済性をテーマとしたシステム監査を実施する」とある。「安全性（特に機密性)」のみならず「信頼性」「効率性」も含めた、全体最適を目指したシステム監査が不可欠であることが、ようやく理解され、浸透し始めたと解釈される。

以上により、我々のコメントは時期および当を得たものであると自負している。なお私事にてなかなか時間を裂けない中、メンバの意見を集約しコメントの文章をまとめて頂いた神尾博氏、システム監査に関する政府・行政の動向の有益な情報を提供頂いた安本哲之助氏には、主査としてこの場を借りて一言お礼を申し上げたい。

（この報告書は、近畿支部･システム監査法制化推進プロジェクトにおける意見表明であり、SAAJ全体の見解ではありません。）

＜目次＞

2015.4

注目情報（2015.3～2015.4）※各サイトのデータやコンテンツは個別に利用条件を確認してください。

■情報セキュリティ10大脅威 2015

2015年4月3日　　独立行政法人情報処理推進機構　セキュリティセンター

IPAが毎年公表している解説書です。本資料は、情報セキュリティ分野の研究者、企業の実務担当者など64組織99名から構成される「10大脅威執筆者会」メンバーの審議・投票によってトップ10を選出し、各脅威についてメンバーの知見や意見を集めて解説したもので、資料は、下記の3章構成となっています。

・第1章　情報セキュリティ対策の基本

パソコンやスマートフォンなどを利用する上で、実施しておくべき情報セキュリティ対策の基本について解説しています。

・第2章　情報セキュリティ10大脅威 2015

「10大脅威執筆者会」の投票結果に基づき、1位から10位に順位付けして解説しています。

・第3章　注目すべき課題や懸念

社会に影響を与える可能性が高く、注目しておきたい課題や懸念について解説しています。

http://www.ipa.go.jp/files/000044680.pdf

■企業におけるマイナンバー制度実務」（総務編）【日本商工会議所・JIPDEC主催セミナーより】

10月から通知開始が、スケジュールされている「個人番号」その取扱いに関する影響は、マイナンバーが適用される税務・社会保障領域で、行政各所との手続き事務で関わりをもつ、企業にも及びますので、以下を参考にして下さい。

http://heartrock-noma.com/contents_798.html

■ISMS ユーザーズガイド

-JIS Q 27001:2014(ISO/IEC 27001:2013)対応　-リスクマネジメント編-　2015 年 3 月 31 日

一般財団法人　日本情報経済社会推進協会（JIPDEC）情報マネジメント推進センター

ISMS ユーザーズガイドを補足し、リスクアセスメント及びその結果に基づくリスク対応についての理解を深めるために必要な事項について、例を挙げて解説しています。

ISMS 認証取得に関する文書は、次のサイトから PDF 版をダウンロード、および申請できます。

http://www.isms.jipdec.or.jp/std/index.html

＜目次＞

2015.4

【協会主催イベント・セミナーのご案内】

■月例研究会（東京）

第201回	日時:2015 年 4 月 28 日(火)　18:30～20:30　場所:機械振興会館　地下2階多目的ホール	
	テーマ	「企業 IT 動向調査 2015(14 年度調査) ～データで探るユーザー企業の IT 動向～」
	講師	一般社団法人　日本情報システム･ユーザー協会 常務理事　浜　田　達　夫　氏
	講演骨子	一般社団法人　日本情報システム･ユーザー協会（略称:JUAS)は、「企業 IT 動向調査 2015」を実施し、その成果を 4 月に発表いたしました(調査期間:2014 年 10 月～11 月、経済産業省　商務情報政策局　監修)。 1000 社の IT ユーザー企業の回答から、定点観測と重点テーマを通して IT 投資や IT 戦略方針など、世の中の最新動向を俯瞰していきます。
	お申し込み	http://www.saaj.or.jp/kenkyu/kenkyukai201.html
第202回	日時:2015 年 5 月 29 日(金)　18:30～20:30　場所:機械振興会館　地下2階多目的ホール	
	テーマ	「三井住友信託銀行における システム統合に対する内部監査の概要」(仮題)
	講師	三井住友信託銀行株式会社　内部監査部 審議役兼システム監査チーム長　辻本　要子　氏
	講演骨子	詳細確定次第、HPでご案内いたします。
第203回	日時:2015 年 6 月 16 日(火)　18:30～20:30　場所:機械振興会館　地下3階　研修2号室　※場所注意	
	テーマ	「個人情報保護法及び番号利用法の改正 － パーソナルデータの利活用をめぐる制度の見直し －」(仮題)
	講師	講師 :慶應義塾大学　総合政策学部　教授　新保　史生　氏　博士(法学)
	講演骨子	詳細確定次第、HPでご案内いたします。
第204回	日時:2015 年 7 月 14 日(火)　18:30～20:30　場所:確定次第、HPでご案内いたします。	
	テーマ	テーマ:「情報セキュリティの最新の脅威の動向」(仮題)
	講師	独立行政法人　情報処理推進機構　(IPA) 技術本部　セキュリティセンター　情報セキュリティ技術ラボラトリー 主任研究員　渡辺　貴仁　氏
	講演骨子	詳細確定次第、HPでご案内いたします。 ※資料注意:講師承諾により電子データ資料配布のみ紙資料配布なし （協会HPに資料配布電子データ化への方針をアップ済み）
第205回	日時:2015 年 8 月 24 日(月)　18:30～20:30　場所:確定次第、HPでご案内いたします。	
	テーマ	「CSMS(サイバーセキュリティマネジメントシステム)認証と ISMS 認証の今後」(仮題)
	講師	一般財団法人　日本情報経済社会推進協会(JIPDEC) 情報マネジメント推進センタ　センター長　高取敏夫　氏
	講演骨子	詳細確定次第、HPでご案内いたします。

■中堅企業向け「6ヶ月で構築するPMS」セミナー（東京）

申し込み常時受付中	概要	個人情報保護監査研究会著作の規程、様式を用いて、6 ヶ月でPMSを構築するためのセミナーを開催します。 詳細をHPでご案内しています。(http://www.saaj.or.jp/shibu/kojin.html)
	基本コース	月 1 回（第 3 水曜日）14 時～17 時（3 時間）×6 ヶ月 ※他に、月 2 回の応用コースなどがあります。
	料金	9 万円/1 名～（1 社 3 名以上割引あり）
	会場	日本システム監査人協会 本部会議室（茅場町）
	テキスト	SAAJ『個人情報保護マネジメントシステム実施ハンドブック』

【外部主催イベント・セミナーのご案内】

■システム監査学会　第２９回研究大会（東京）

申し込み受付中	統一論題	レピュテーションリスクマネジメントとシステム監査
	日時	2015 年 6 月 15 日（金） 大会：10:00～16:55　懇親会：17:00～19:00
	会場	機会振興会館ホール 他
	基調講演	「レピュテーションリスクマネジメントとこれからの経営」 講師：特定非営利活動法人日本リスクマネジャー＆コンサルタント協会 副理事長 前田 泉 氏
	詳細	http://www.sysaudit.gr.jp/taikai/2015taikaiyoshi.html

■ＩＳＡＣＡ東京支部 2015 年　月例会予定（東京）

日時： 2015 年 5 月例会 5/27（水）開催予定 18:30-20:10(受付開始：18:00) 2015 年 6 月例会は年次総会開催のためお休みです。	
詳細	http://www.isaca.gr.jp/education/

＜目次＞

2015.4

新たに会員になられた方々へ

新しく会員になられたみなさま、当協会はみなさまを熱烈歓迎しております。
先月に引き続き、協会の活用方法や各種活動に参加される方法などの一端をご案内します。

ご確認ください
・協会活動全般がご覧いただけます。 http://www.saaj.or.jp/index.html
・会員規程にも目を通しておいてください。 http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・皆様の情報の変更方法です。 http://www.saaj.or.jp/member/henkou.html

特典
・会員割引や各種ご案内、優遇などがあります。 http://www.saaj.or.jp/nyukai/index.html
セミナーやイベント等の開催の都度ご案内しているものもあります。

ぜひ参加を
・各支部・各部会・各研究会等の活動です。 http://www.saaj.or.jp/shibu/index.html
皆様の積極的なご参加をお待ちしております。門戸は広く、見学も大歓迎です。

ご意見募集中
・皆様からのご意見などの投稿を募集しております。
ペンネームによる「めだか」や実名投稿があります。多くの方から投稿いただいておりますが、さらに活発な利用をお願いします。この会報の「会報編集部からのお知らせ」をご覧ください。

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

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

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

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

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

＜目次＞

2015.4

【　ＳＡＡＪ協会行事一覧　】	※注　定例行事予定の一部は省略。	赤字：前回から変更された予定	
2015 年	**理事会・事務局・会計**	**認定委員会・部会・研究会**	**支部・特別催事**
4 月	9 日 理事会 末日 法人住民税減免申請	認定委員会:新規 CSA/ASA 書類審査 中旬 認定委員会:新規ASA認定証発行 28 日第 201 回月例研究会	19 日 2015 年春期情報技術者試験
5 月	14 日 理事会 29 日 会費未納者チェック	中旬 認定委員会:新規 CSA 面接 29 日第 202 回月例研究会	
6 月	1 日 会費未納者督促状発送 11 日 理事会 12 日～会費督促電話作業(役員) 末日 支部会計報告依頼(〆切 7/14) 末日 助成金配賦額決定(支部別会員数)	10 日 認定委員会:CSA 面接結果通知 16 日 第 203 回月例研究会	
7 月	8 日 支部助成金支給 9 日 理事会	1 日 秋期公認システム監査人募集案内〔申請期間 8/1～9/30〕 14 日 第 204 回月例研究会 20 日 認定委員会:CSA 認定証発送	14 日 支部会計報告〆切
8 月	(理事会休会) 29 日 中間期会計監査	秋期公認システム監査人募集開始～9/30 24 日 第 205 回月例研究会	
9 月	10 日 理事会		5～6 日 西日本支部合同研究会 (開催場所:岐阜)
	以下は、2014 年に実施した行事一覧です。		
10 月	9 日 理事会	30 日 第 196 回月例研究会	25 日 近畿支部:IT-BCP 体験セミナー
11 月	13 日 理事会 14 日 予算申請提出依頼(11/30〆切) 支部会計報告依頼(1/10〆切) 18 日 2015 年度年会費請求書発送準備 20 日 会費未納者除名予告通知発送 30 日 予算申請提出期限	中旬 認定委員会:CSA 面接 19 日 第 197 回月例研究会 20 日 CSA・ASA 更新手続案内〔申請期間 1/1～1/31〕 28 日 認定委員会:CSA 面接結果通知	29 日 西日本支部合同研究会 (開催場所:大阪市)
12 月	1日 2015 年度年会費請求書発送 2015 年度予算案策定 11 日 理事会:2015 年度予算案、会費未納者除名承認 12 日第 14 期総会資料提出依頼(1/9〆切) 19 日 会計:2014 年度経費提出期限	6 日 法制化検討 PT 事前打合せ 6 日 事例研:第 16 回課題解決セミナー 10 日 CSA/ASA 更新手続案内メール 16 日 第 198 回月例研究会 20 日 CSA 認定証発送 21 日 第 25 回 CSA フォーラム	13 日 東北支部:支部総会
2015 年	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
1 月	7 日 16:00 総会資料(〆) 8 日 理事会:通常総会資料原案審議 9 日 総会開催案内掲示・メール配信 19 日 会計:2013 年度決算案 24 日 会計:2013 年度会計監査 26 日 総会申込受付開始(資料公表) 31 日 償却資産税・消費税	認定委員会:CSA・ASA 更新申請受付〔申請期間 1/1～1/31〕 20 日 第 199 回月例研究会 20 日 春期公認システム監査人募集案内〔申請期間 2/1～3/31〕	10 日 会計:支部会計報告期限 16 日 近畿支部:支部総会
2 月	5 日 理事会:通常総会議案承認 20 日 第 14 期通常総会・特別講演 25 日 法務局:資産登記、活動報告書提出 28 日 年会費納入期限	CSA・ASA 春期募集(2/1～3/31) 28 日-3 月 1 日 事例研:第 25 回システム監査実務セミナー(前半)	
3 月	2 日 東京都への事業報告書提出 2 日 年会費未納者宛督促メール発信 4 日 認定 NPO 法人東京都による調査 12 日 理事会	4 日 第 200 回月例研究会 14-15 日 事例研:第 25 回システム監査実務セミナー(後半)	

＜目次＞

2015.4

会報編集部からのお知らせ

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

□■ 1. 会報テーマについて

2015 年度の年間テーマは、「システム監査人の魅力」です。これまでは「システム監査」に焦点を当ててきましたが、今年度は「システム監査人」に焦点を当てて考えてみたいと思います。5 月号から 7 月号までは、「マネジメントシステム内部監査におけるシステム監査人の責任」をテーマといたします。皆様の幅広いご意見をお待ちしています。

会報テーマは、皆様のご投稿記事づくりの一助に、また、ご意見やコメントを活発にするねらいです。会報テーマ以外の皆様任意のテーマももちろん大歓迎です。皆様のご意見を是非お寄せ下さい。

□■ 2. 会報の記事に直接コメントを投稿できます。

会報の記事は、

1)PDF ファイルの全体を、URL(http://www.skansanin.com/saaj/)へアクセスして、画面で見る

2)PDF ファイルを印刷して、職場の会議室で、また、かばんにいれて電車のなかで見る

3)会報 URL(http://www.skansanin.com/saaj/)の個別記事を、画面で見る

など、環境により、様々な利用方法をされていらっしゃるようです。

もっと突っ込んだ、便利な利用法はご存知でしょうか。気にいった記事があったら、直接、その場所にコメントを記入できます。著者、投稿者と意見交換できます。コメント記入、投稿は、気になった記事の下部コメント欄に直接入力し、投稿ボランをクリックするだけです。動画でも紹介しますので、参考にしてください。

(http://www.skansanin.com/saaj/ の記事、「コメントを投稿される方へ」)

□■ 3. 会員の皆様からの投稿を募集しております。

分類は次の通りです。

1. めだか (Word の投稿用テンプレート(毎月メール配信)を利用してください)
2. 会員投稿 (Word の投稿用テンプレート(毎月メール配信)を利用してください)
3. 会報投稿論文 (「会報掲載論文募集要項」及び「会報掲載論文審査要綱」があります)

□■ 会報投稿要項 （2015.3.12 理事会承認）

・投稿に際しては、Wordの投稿用フォーム（毎月メール配信）を利用し、会報部会（saajeditor@saaj.jp）宛に送付 して下さい。
・原稿の主題は、定款に記載された協会活動の目的に沿った内容にして下さい。
・特定非営利活動促進法第2条第2項の規定に反する内容(宗教の教義を広める、政治上の主義を推進・支持、又は反対する、公職にある者又は政党を推薦・支持、又は反対するなど)は、ご遠慮下さい。
・原稿の掲載、不掲載については会報部会が総合的に判断します。
・なお会報部会より、表現の訂正を求め、見直しを依頼することがあります。また内容の趣旨を変えずに、字体やレイアウトなどの変更をさせていただくことがあります。

会報記事は、次号会報募集の案内の時から、締め切り日の間にご投稿ください。
バックナンバーは、会報サイトからダウンロードできます（電子版ではカテゴリー別にも検索できますので、ご投稿記事づくりのご参考にもなります）。
会報編集部では、電子書籍、電子出版、ネット集客、ネット販売など、電子化を背景にしたビジネス形態とシステム監査手法について研修会、ワークショップを計画しています。研修の詳細は後日案内します。

会員限定記事

【本部・理事会議事録】（当協会ホームページ会員サイトから閲覧ください。パスワードが必要です）

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

■発行： NPO 法人　日本システム監査人協会　会報編集部
〒103-0025　東京都中央区日本橋茅場町2－8－8共同ビル6F

■ご質問は、下記のお問い合わせフォームよりお願いします。
【お問い合わせ】 http://www.saaj.or.jp/toiawase/

■会報は会員への連絡事項を含みますので、会員期間中は、会員へ配布されます。
会員の所属や登録メールアドレス等の変更は、当協会ホームページ会員サイトより変更してください。
会員でない方は、購読申請・解除フォームに申請することで送付停止できます。
【会員でない方の送付停止】 http://www.skansanin.com/saaj/register/

■□■SAAJ会報担当
編集委員： 藤澤博、安部晃生、久保木孝明、越野雅晴、桜井由美子、高橋典子、西宮恵子、藤野明夫
編集支援： 仲厚吉 （会長）
投稿用アドレス： saajeditor ☆ saaj.jp （☆は投稿時には＠に変換してください）

＜目次＞