特定非営利活動法人
日本システム監査人協会報

2014 年 2 月号
No 155

No. 155（2014 年 2 月号）＜1 月 20 日発行＞

CSA/ASA 資格は 1/31 が更新期限です。SAAJ 総会は 2/21 に開催されます。まだまだ寒い日が続きます。体調管理と健康に気を付けましょう。

2014.01

めだか　【　個人情報、個人データ、公（おおやけ）のためのシステム監査　】

システム監査の普及・促進を考えると、公（おおやけ）のための情報システムは、システム監査が求められるべきであると思う。一方、個人情報を取り扱う情報システム（以下、個人情報システムという。）の利活用について、システム監査の必要性を考えてみたい。個人情報システムは、顧客管理システムのようにユーザー本人へのサービスの提供だけではなく、住民個人への公的な各種サービスの提供に当っても課題を解決する方法として期待されていると思う。

〔参考1〕によれば、ビッグデータとは、人間の頭脳で扱える範囲を超えた膨大な量のデータを処理・分析して活用する仕組みであり、データ分析を活用することで仕事の効率を上げたり、ユーザーへのサービスの品質を上げたりするという考え方であるという。データ分析には多種のデータを収集し、組み合わせて活用するマッシュアップ（マッシュポテトをこね混ぜる様子を連想させる。）という手法を使う。また、膨大な量のデータを処理・分析するためにはクラウド技術が使われている。サービス提供側には、解析予測によって無理なくスケジュールを組むことや、買ってくれそうな顧客をあらかじめ絞り込んで無駄な作業を減らして、効率を上げることができるようになる。サービス・ユーザー個人へは、メリットを短いループで還元することが可能になる。

分析対象となるビッグデータは、取得時に個人情報が含まれることがほとんどであると言える。個人情報は情報システムでは個人データとして取り扱われる。個人データは、〔参考2〕によると、「“personal data” means any information relating to an identified or identifiable individual (data subject)」である。つまり、個人データは、識別された又は識別されうる個人（データ主体）に関するあらゆる情報ということである。情報システムに個人データの取扱いがある場合、プライバシー侵害の起きることが無いように取り扱う必要がある。プライバシー（privacy）は欧米から来た概念であるので、Oxford Dictionary of English を引くと、「privacy; a state in which one is not observed or disturbed by other people」ということである。日本語で言うと、個人が他の人々に観察されたり邪魔されたりしない情況ということである。

個人情報システムの利活用によってプライバシー侵害の起きることが無いように、個人情報システムの開発、又は利用に当って、プライバシー・インパクト・アセスメント（PIA）、言い換えれば、個人情報システムへのシステム監査が必要になる。個人情報の利活用に当っては、プライバシー保護（the protection of privacy）が必要である。原則的にプライバシー侵害の起きる社会は民主主義社会とは言えないからである。つまるところ、個人情報システムへ、公（おおやけ）のためのシステム監査が求められている、と言って良いと思う。

〔参考1〕:「ビッグデータの覇者たち」 海部美知 （講談社現代新書2203）
〔参考2〕:「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会報告 (2013) OECD」 堀部政男、新保史生、JIPDEC（野村至） 仮訳 （JIPDEC）

（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。 ）

2014.01

めだか【　システム監査人の責任　（ 公（おおやけ） のためのシステム監査）　】

システム監査人が果たすべき“責任”について考える。

「公（おおやけ）のためのシステム監査」という会報テーマを受け、“システム監査人の責任”という視点から述べる必要を考えた。例えば、システム監査基準において“責任”を規定している個所は下記枠内だ。改めてそれぞれの重さを確認する一方で、もう一歩踏み込んで“責任”の中身を考えてみる。

＜システム監査基準の抜粋＞

Ⅱ.システム監査の目的

システム監査の目的は、組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的な立場のシステム監査人が検証又は評価することによって、**保証を与えあるいは助言**を行い、もって IT ガバナンスの実現に寄与することにある。

Ⅲ. 一般基準　1. 目的、権限と**責任**

システム監査を実施する目的及び対象範囲、並びにシステム監査人の権限と**責任**は、文書化された規程、または契約書等により明確に定められていなければならない。

Ⅳ. 実施基準　5. 他の専門職の利用

システム監査人は、システム監査の目的達成上、必要かつ適切と判断される場合には、他の専門職による支援を考慮しなければならない。他の専門職による支援を仰ぐ場合であっても、利用の範囲、方法、及び結果の判断等は、システム監査人の**責任**において行われなければならない。

Ⅴ. 報告基準　4. 監査報告についての**責任**

システム監査人は、監査報告書の記載事項について、その**責任**を負わなければならない。

このような責任のなかで、“システム監査人の責任”として今一歩踏み込んで考えるべき重要な点は、上記矢印が示す責任＝監査目的に対する監査報告書の責任であると思う。

①踏み込む一つは、監査人がもつ専門能力で相当の注意を払い誠実な監査の報告書であれば“責任”を果たしたといえるだろうか？　②二つ目は、「保証を与えあるいは助言」への“責任”とはどのような監査報告書をいうのだろうか？　③三つ目は、IT 投資が業務の合理化から経営革新へ変貌しシステム監査が経営貢献を求められているなかで、その“責任”を果たすための監査報告書にはどのような内容が必要だろうか？

いずれも、「公（おおやけ）のためのシステム監査」の視点からの踏み込みだ。

システム監査が、公（おおやけ）から期待され、公（おおやけ）から価値を認められるには、システム監査が果たす“責任”と密接に関係している。評価は“責任”を果たすなかで生まれるものだ。因果関係であり表裏一体でもある。公（おおやけ）が求めるシステム監査は、（高邁な精神のシステム監査の意義・目的は当たり前のことでその先にある）システム監査が果たしてくれる“責任”は何か、に尽きると思う。ここで今すぐ結論めいた整理ができるものではなく、多くの方との議論の必要を感じているが、小生の考えている一端を以下に少し述べる。

前述の①については、監査報告書の品質について一定の評価を与えるアカウンタビリティーの仕組み、②については、保証型システム監査への積極的な取り組み、③については、経営に貢献する監査結果を導き出すための監査要点（チェック項目）の考案、が取り組むべき課題の一つではないかと考えている。

責任を果たすシステム監査！　響きはいいが地球を背負うような重さがある。

（山の彼方）

（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。）

2014.01

めだか　【　尊厳の監査　】

昨年2月、義父が他界した。89歳だった。82歳の頃に最初の脳梗塞で左の視野を狭めた。翌年にも脳梗塞を再発、手術も及ばず下半身不随になった。リハビリに励んだが、歩行は困難になり、会話はできるもののバルーンを付けての排尿になった。そして2年ほど前、三度目の脳梗塞で話す機能を失い、両手も口も動かせず、胃ろうで栄養補給する生活になった。91歳の義母は、今、軽い認知症で施設のお世話になっている。これまでに、義父母を通して、6ヶ所ほどの施設と何人もの入居者の状況を観てきた。

昨年 11 月のNHKクローズアップ現代で、『ウェアラブル革命　～“着るコンピューター”が働き方を変える～』が放映され、身震いする衝撃が走った。一部の映像だが、先ず　こちらをご覧いただきたい。

http://www.nhk.or.jp/gendai/kiroku/detail_3437.html

唐突に二つのこと書いた。ひとつは、急速に迫りくる高齢化社会の姿である。ウェアラブル革命は、着るだけで人がロボットのような働き方になってしまうという衝撃である。少し掘り下げよう。第一の迫りくる高齢化社会の姿は、今日の私たちを育て、支えてきた人生の先輩たちを、私たちはどう考え対応すべきか？　それは明日のあなたの姿への対応でもある。社会の仕組みとして考えねばならないテーマであるが、ほとんどの施設が、室内での食事と下の世話、入浴の世話をする範囲で、外の（五感覚を活かす）世界を遮断し、意思を持った判断、行動を閉ざし、生命力を急速に衰退させている。第二のウェアラブル革命は、経営面から見れば、未経験者でも経験者と同等以上にミスのない仕事ができるという点では経営革新の一面がある。しかし、この姿は、“人のロボット化”の印象をぬぐえない。

以前、「デスマーチを憂いて」と題して、本欄に投稿されたSEの鬱の問題－情報化に取組むSEが、異常な短納期開発やトラブル対応を続け、鬱におちいるーがあった。今度は、機械的で心や魂への働き掛けがない仕組みが招く問題提起である。多様な仕事に携わる人の仕事は、情報システムに指示され、仕事の生き甲斐や歓びが失われ、鬱に追い込まれるのでは？　そう筆者は危惧し、身震いしたのである。

人類は、長けた頭脳で先人の成果を積み増しながら、便利で多様な道具を産み出してきた。しかし、その頭脳や道具が争いに向けられ、世界の各地で、貧富・人種・宗教・国境などに関する争いが絶えない。ビジネスの場においても、情報化に伴いスピード化、広域性、正確性、生産性や効率化は限りなく進んでいるが、競争に勝利することに関心が集中し、真に大切なことを見落しているのではないか？

施設に入居している高齢者、仕事に生き甲斐を見出せない働き手には、ともに“人としての尊厳、生命力”が感じられない。システムの指示にしたがって手足を動かすだけの仕事の毎日は、鬱とその予備群を急増させるだろう。既存のルール準拠型監査、後追い型の監査には、イキイキした　みずみずしい命の喪失／覚醒の着眼点がない。組織の目標や仕組みに、今こそ“人の尊厳（魂）”に着目し、近い将来における組織への警鐘、明日の企業、行政のあるべき姿への変革を迫る監査が求められていると思う。

（日々是好日）

（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。）

2014.01

投稿　【　公（おおやけ）のためのシステム監査　】

会員番号　0557　仲　厚吉　（会長）

会報では、この 1 年のテーマとして、「○○のためのシステム監査」を掲げています。そして、2 月号からの 3 か月のテーマは、「公（おおやけ）のためのシステム監査」です。これは、下記の、〔2014 年度の協会事業について〕 (2) で、システム監査の活性化のため、「認定 NPO 法人」認定によって、システム監査を公（おおやけ）の活動として活性化させ、それを広く世の中にアピールする、という考えに関わっています。

〔2014 年度の協会事業について〕

(1)システム監査人の社会的評価の向上

「認定 NPO 法人」認定によって、公認システム監査人資格のブランド化を図る。

(2)システム監査の活性化

「認定 NPO 法人」認定によって、システム監査を公（おおやけ）の活動として活性化させる。

(3)協会組織の充実

所轄庁の東京都認定審査に適合するよう協会組織を整備し、会員の信頼に応えるよう体制を充実させる。

「漢字源」の解字によれば、「公（おおやけ）」とは、「八印（開く）＋口」で、入り口を開いて公開すること。個別に細分して隠さずおおっぴらに筒抜けにして見せる意を含む。「私」（細かくわけてとりこむ）と「公」とは、反対のことば、とあります。一方、「私」のム〈シ〉は、自分だけのものをうでででかかえこむさま。「私」は、「禾（作物）＋（音符）ム」で、収穫物を細分して、自分のだけをかかえこむこと。ばらばらに細分する意を含む、とあります。

システム監査は、いわゆる公的、又は私的な情報システムにかかわらず、その課題を明らかにして、課題解決を図ることが役割だと思います。つまり、システム監査は、情報システムにかかわる「公（おおやけ）」の活動、公益性のある活動と考えて良いと思います。ここで、情報システムのもとになる「システム思考」について考えを巡らしたいと思います。

参考資料では、“「システム思考」とは、社会や人間が抱える物事や状況を、目の前にある個別の要素ではなく、それぞれの要素とその「つながり」が持つシステムとして、その構造を理解することである。” また、“つまり、目の前にあるものだけを見続けるのではなく、物事や状況の全体像を把握し、システム自身が持つ力を活かし、小さな力でも大きく構造を動かせるポイントを見つけ、変革をデザインする方法論である。これは、社会や人間にとって、真に望ましい変化を創り出すためのアプローチなのである。”と言っています。

システム監査は、内部統制システム PDCA サイクルの Check 局面の監査の中で、情報システムにかかわるリスクを明らかにして、真に望ましい変化を創り出すためのアプローチである、と言えます。また、大切なことは、システム監査人は、目の前にある個別の要素（すなわち個々のチェック項目）とともに、より一層、それぞれの要素とその「つながり」が持つシステムとして対象になる情報システムの構造を理解する見識を持つことである、と思います。

参考資料:「入門！ システム思考」 枝廣淳子＋内藤　耕　（講談社現代新書 1895）

2014.01

システム監査と税制改革【弱者に優しい消費税】～消費税の複数税率化と物品税の復活に注意～

会員番号　1566　田淵隆明

謹賀新年。本年もよろしくお願いいたします。
賛否両論がある中、今年の 4 月 1 日から、消費税税率が引き上げられることとなったが、昨年末の「与党税制改正大綱」において、我が国の間接税の税体系に関して、システム監査上非常に重要な 2 つのことが決定したので、今回はそれを取り上げることにする。

§1. 平成 25 年度「与党税制改正大綱」

昨年 12 月 12 日に正式決定した平成 25 年「与党税制改正大綱」において、消費税に欧州のような「軽減税率」が導入されることとなった。対象品目は「食料品(外食とアルコールを除く)」、「医薬品」、「新聞」及び「書籍」となる見込みである。一部に誤解されている人がおられるようなので、正確を期すために申し添えるが、**軽減税率の制度設計は今年中に完了し、「年末の税制改正大綱」に単に盛り込まれるだけではなく、税制改正大綱の前提となることが与党間で合意**されている。正確を期すため、一部引用する。

> 「消費税の軽減税率制度については、「社会保障と税の一体改革」の原点に立って必要な財源を確保しつつ、関係事業者を含む国民の理解を得た上で、**税率 10%時に導入する。**このため、今後、引き続き、与党税制協議会において、これまでの軽減税率をめぐる議論の経緯及び成果を十分に踏まえ、社会保障を含む財政上の課題とあわせ、対象品目の選定、区分経理等のための制度整備、具体的な安定財源の手当、国民の理解を得るためのプロセス等、軽減税率制度の導入に係る詳細な内容について検討し、**2014 年 12 月までに結論を得て、与党税制改大綱を決定する**。」
> (2013 年 12 月 12 日、朝日新聞朝刊)

上記のように「与党税制改正大綱」においては「消費税への 10%時での軽減税率の導入」が明記されたが、それと同時に「担税力に応じた新税」の検討が明記された。**「担税力に応じた新税」とは、高所得者または多額の資産保有者(以下、「富裕層」とする)に負担を求める税**と考えられ、**事実上の「物品税」や「高額飲食税」や「通行税」(グリーン車などの)など、いわゆる"贅沢税"の復活**と考えられる。

Wikipedia には、次のように「物品税」のシステムこそが、我が日本国が繁栄を謳歌していた昭和時代後半の「一億総中流社会の原動力」になったと書かれている。

<引用>

> 間接税についての伝統的な考え方は、**生活必需品に対しては課税を差し控え、贅沢品には担税力が認められるからこれを重く課税する**というものである。戦後の混乱期から高度経済成長を迎える日本においても、前述の考え方は一般的に肯定されていた。具体的には、宝石、毛皮、電化製品、乗用車あるいはゴルフクラブといったものが物品税の対象とされていた。日本の「物品別間接税」は世界に先駆けて導入され、現在欧米で導入されている間接税の物品別軽減税率は日本のこの間接税システムを真似したものである。

物品税は低所得者でも購入せざるをえない生活必需品などが非課税になっており、かわりに高所得者が購入する贅沢品には高い税率で課税されるという税制であるため、**一億総中流社会の原動力になったシステム**といえる。

</引用終わり>

今般決定した「消費税への軽減税率の導入」や「1 人 1 万円超の飲食に対して 5~6%課税される高額飲食税」の与党合意は、強い旧物品税的特徴を有しており、我々が目指すべき「一億総中流社会」の復活への第一歩であると考えられる。

間接税本来の目的である「所得の再分配」と「福祉の財源の充実」の両立のためには、**現行の消費税の体系を G7 先進国として当たり前の姿である「弱者に優しい消費税」**(生活必需品は非課税または軽減税率を適用し、宝石・毛皮などの贅沢品には重課税する間接税制度)**に改める必要**がある。その実現のためには、消費税の軽減税率の財源の確保は必須であり、**そのための「物品税」、「高額飲食税」、「通行税」などの「担税力に応じた新税」の制度設計は焦眉の急**であると考えられる。

また、この「担税力に応じた新税」の導入により、国民全体に対して「分相応の生活」を促す効果が期待される。また、高級品を得ることの「ありがたみ」の実感が強まることとなる。従って、**この新税の導入は国民全体のモラルの向上・青少年の健全育成に資するのみならず、近年急増する「カード破産」や「サラ金地獄」のような事象の発生の抑止において、一定の効果が期待**されるものである。

§2. 先進国の常識と「弱者に優しい消費税」

一部の会員の方々はご存知のように、筆者は 2012 年 6 月 13 日に衆議院の「社会保障と税特別委員会」中央公聴会に召還され、公述人として「弱者に優しい消費税」への転換を語らせて頂いた。その模様は衆議院の Web サイトや動画サイトなどで確認することができるので、ご興味のある方は是非ご覧頂きたい。

講演や執筆やメール・マガジン等で度々申し上げていることであるが、筆者は、こうした税制改革や社会保障改革を論ずる際には、絶対的な前提が 2 つある、と考えている。

①我が日本国は「アジアのリーダー」であり、国連安全保障理事会の常任理事国になる資格を有する世界に輝く先進国である。この国際的地位は、孫子の代においても、絶対に維持されなければならない。(当然のごとく、日本円は「ハード・カレンシー」の地位を維持するとともに、IMF 第 4 条の定める「自由利用可能通貨」＝4 大通貨の地位を維持しなければならない)

②先進国の国民として、我々日本人が享受している「生活水準」、「教育水準」、「モラル水準」、「食品安全・公衆衛生」、「治安水準」等は、孫子の代においても、絶対に維持されなければならない。

従って、**人口が 1000 万人に満たない小国の制度や、発展途上国や後進国などの先進国以外の制度を模倣することは全くのナンセンス**である。しかし、前政権においては、このことを理解できていない議員が少なくなかった。極めて遺憾なことである。

「弱者に優しい消費税」とは

(1)医療・学校教育・身体障害者物品には非課税を継続する。

(2)食料品などの生活必需品には軽減税率を適用する。
(3)土地や有価証券など非課税を維持することに疑問の残るものについては見直す。
(4)毛皮・宝石などの贅沢品や、高額飲食、グリーン車/グランクラス/ファーストクラスなどの贅沢なサービスには重課税する(割増税を課す)。

という、先進国の国民として、ごく普通の庶民感覚に根ざしたものである。また、同時に次のことも提言させて頂いた。

(a)中小業者の負担軽減のため、外税表示を認める(→既に実現)。
(b)簡易課税の縮小(→今回実現)。
(c)滞納を防ぐため、本則課税業者に限り、税抜き経理への一本化。

最近はあまり言われなくなったが、一部の政治家や評論家は「線引きが難しい」という妄言を発していたが、「軽減税率」は弱者対策として多くの国々で実施されており、確かな実績を有している。また、事務負担の問題をしきりに主張する人々もいるが、軽減税率制度は一部の発展途上国でも機能しており、世界に輝く先進国である我が国に出来ない筈は無い。文盲率の高いインドでも、標準税率が 12%に対し、6%と 2%の 2 種類の軽減税率が存在している。また、古代～中世にかけて繁栄した、コンスタンティノポリスを首都とする東ローマ帝国の取引高税においても、生活必需品は非課税または軽減税率であった。

この公聴会では、筆者とともに公聴会で公述した某大学教授が「軽減税率」よりも「給付付き税額控除」が優れていると力説されていた。前政権は同教授の意見を採用し、「給付付き控除」を主張していたが、筆者はこの考え方には同意しかねる。それは次の理由による。

(1)**G7 先進国において、均一税率で 7%以上の国は皆無**であり、全ての他の先進国において、食料品などの生活必需品において軽減税率が導入されている。特に、G7 のイギリス、カナダでは食料品は非課税であり、米国も多くの州において非課税である(米国は連邦レベルの消費税無し)。

※一昨年逝去されたコメンテーターの M 氏などは、テレビで「英国などは 20%だ。だから 10%ぐらい当然だ」とか「EU は付加価値税を 15%～25%にすることを加盟条件としている」と豪語していた。
しかし、EU は「均一で 15%～25%」とはしていない。現に、英国では生活必需品は 5%であり、食料品は非課税である。また、脱税防止効果のあるインボイス制度の導入も必須条件としている。マスコミの方々は、国民をミスリードすることが無いよう、正確な報道をお願いしたいところである。

(2)豪州などを加えた **OECD 加盟 34 カ国においても、均一で 10%以上の国は、韓国とニュージーランドのみ**である。しかも、両国とも「超格差社会」であり、中間層が多い我が国とは全く国情が異なる。

※韓国の社会保障費は OECD 諸国で最低水準であり、我が国の 1/3 である。

(3)**「給付付き控除」の実績はカナダとシンガポールだけであり、両国とも軽減税率併用**である。

(4)国民総背番号制など実現のために大きなインフラが必要となる。また、還付に掛かるコストが莫大であり、同時に行政の肥大化に繋がり、「天下り」ポストを増やすことになる。

(5)給付付き控除の恩恵を受けられるのは、生活保護世帯など「住民税非課税世帯」に限定されており、我が国における消費の牽引役である中間所得層に全く恩恵がない。また、金額も僅少であり、今回臨時措置として実施される「簡素な給付」でも、僅か１年間に１万円である。

(6)「レシートによる還付」は、先進国ではない韓国だけの制度であり、先進国の実績は皆無である。

(7)低所得者が「プチ贅沢」をした場合にも恩恵があり、中間所得層が全く報われず、勤労モラルの低下に繋がる。

今回、与党が「弱者対策」として、「給付付き控除」ではなく、実績のあるオーソドックスな軽減税率〝いりを選択したことは極めて賢明であり、大変喜ばしいことである。

※あろうことか、この教授はこの公聴会において「配偶者控除は究極のバラマキ」であり、全廃するべきであると力説していた。更に「専業主婦は仕事をしていない」との発言も繰り返していた。これは、全国の専業主婦に対する冒涜であり、女性蔑視の極みでもある。元々アカデミックの世界にいたものとして、ご本人の見識を疑うとともに、甚だ遺憾であると言わざるを得ない。

§3. 物品税等の「担税力に応じた新税」の制度設計

§1 で述べたように、「担税力に応じた新税」とは、**事実上の「物品税」や「高額飲食税」や「通行税」など、いわゆる"贅沢税"の復活**と考えられる。すでに「高額飲食税」については、昨年末に与党間で、「1 人当たり 1 万円を超える飲食について、(全額ではなく)超過分について、6%課税する」ことで合意している。従って、飲食業者のシステム監査を行う場合においては、注意が必要である。

以上のことから、物品税等の「担税力に応じた新税」の課税金額は、本体価格全体に課税するのではなく、次の計算式のようになると考えられる。

〔 (本体価格) － (基準金額) 〕 × (税率)　　(3.1)

設例 1: ¥300,000 のネックレスを購入する場合。物品税課税のための基準金額が¥100,000 とすると、支払い総額は次のようになる。

本体価格＝¥300,000
消費税＝¥300,000×10%＝¥30,000
物品税＝(¥300,000－**¥100,000**)×10%＝¥20,000

支払総額＝¥300,000＋¥30,000＋¥20,000＝¥350,000　　(3.2)

※このような制度設計を行うことにより、例えば基準金額が¥100,000 である場合に¥99,990 のような価格設定が大量に行われる事態を回避することができる。

ただし、鉄道のグリーン車・グランクラス・個室寝台、飛行機のファーストクラスなどの特別なサービスのための「追加料金」については、次のように全額が課税対象となる。

(追加料金部分の本体価格)　×　(税率)　　(3.3)

設例 2:鉄道でA駅からB駅まで移動する場合の乗車券が¥10,000(税抜き)、特急券が¥5,000(税抜き)、グリーン券が¥4,000(税抜き)である場合、支払い総額は次のようになる。

本体価格＝¥10,000＋¥5,000＋**¥4,000**＝¥19,000
消費税＝¥19,000×10%＝¥1,900
通行税＝**¥4,000**×10%＝¥400
支払総額＝¥19,000＋¥1,900＋¥400＝¥21,300　　(3.4)

※この新税の詳細については、次回、取り上げることとする。

§4.ポスレジ及び会計システムの現状

このように、今回の間接税の改革は、システムに大きな影響を及ぼすことになる。

〔1〕ポスレジ

現在、ポスレジの業界は、事実上大手 5 社の寡占状況にあるが、いずれも、2005 年頃までに消費税の複数税率には対応済みである。従って、この部分については、システム監査の需要が多く発生するとは考えにくい。ただし、オリジナル・メイドのポスレジ・システムにおいては大規模改修が必要になる場合がある。現実に、筆者も複数の企業から相談を受けている。

一方、**「飲食税」はロジックがやや複雑であり、システム監査上の重要なテーマ**となると考えられる。

〔2〕会計システム

会計システム分野については、我々システム監査における重要なテーマとなる。特に、一部の会計システムは税コードを持たないなど、複数税率への対応が立ち遅れている。システムのリプレース需要も増えると思われるが、**同時にシステム監査における重要なテーマとなる。**このことは、「システム監査技術者」の職域拡大のチャンスでもある。また、「システム監査法制化」への追い風ともなるであろう。

<<Reference>>

1. 衆議院「社会保障と税特別委員会」中央公聴会(平成 24 年 6 月 13 日)
https://www.youtube.com/watch?v=2ebWyoqk-EY
2. SAP ジャパン IFRS エキスパートコラム 1-29(田淵隆明)
http://global.sap.com/japan/campaigns/2010/ifrs/expert.epx

(編集者注:原稿の一部を編集および割愛させていただきました)

2014.01

【エッセイ】憑依

会員番号　0707　神尾博

神懸りや狐憑きといった憑依（ひょうい）の一部は、医学領域では解離性同一性障害、すなわち多重人格という精神疾患とされている。また憑依の中には作為的に利用されてきたケースも多いだろう。「神や霊のお告げである、もうひとりの自分がやった、まるっきり覚えていない」と主張することで、政治を操ったり近隣社会での逃げ場を作ったりと、使い道には枚挙に暇が無い。意図的かそうでないかは別にしても、たしかに憑依は我が国でも、古くから政治や文化に少なからず影響を与えてきた。邪馬台国の女王・卑弥呼は日本最古のシャーマンであり、神事を司り弟の政治を補佐したという説が有力である。また伝統芸能の一つである能では、葵上（あおいのうえ）や鉄輪（かなわ）といった演題で、女の嫉妬心が生み出す人格変換のテーマが採り上げられている。

そして我々は匿名性の高いネットの世界を手に入れ、その気になれば別人格を使い分けることが容易に行えるようになった。モバイルPCやスマホ等の、複数の端末や回線を駆使すれば、匿名掲示板等での「自作自演」が暴かれる隙も小さくなるだろう。日本でのスマホの普及率についてはいくつかのデータがあるが、2013年後半で人口比では25～30%、世帯では50%程度のようだ。今のところ私物スマートデバイスの業務利用であるBYOD（Bring Your Own Device）の採否は、事業の生産性を優先なら受容、情報漏洩のリスクを重視なら禁止といった間で、揺れ動いている模様である。しかしちょっと待って頂きたい。BYODをシャットアウトしたとしても、本当に組織側のリスクはゼロになるのだろうか？

役員等の経営幹部個人のスマートデバイスに目を向けてみれば……。特にIT企業や大手企業の場合、紛失・盗難・マルウェア等によって、組織と無関係な個人的なデータが、たとえ私物からでも漏れた場合、広範囲な炎上につながる恐れもある。「そんな脇の甘い経営陣のいる会社と取引していれば、そこに置いてあるデータだって危ない」と。この場面では、よもや「精神障害」や「人格変換」というキーワードは通用しまい。さらには、何かの拍子で私物にワクチンソフトがインストールされていないことが露見しただけでも、同様の憂き目にあうかもしれない。スキルにそれなりの自信があるなら、ユーザサポート無しの無料ワクチンソフトを使うという手もあるだろうに。

それで終わりではない。

「一方的なサポート終了には憤懣やる方ない」という声には賛同できなくもないが、WindowsXPやOffice2003もしかり。2014年4月のサポート切れ後には、セキュリティパッチが配布されないことは周知の事実ではある。あえて繰り返すが、技術的ダメージが皆無でも、風評被害が拡大し危機的状況に陥ることもあり得る。レガシーソフトを使っていることが発覚するだけも、一大事かもしれない。

我々システム監査人は自身の心掛けもさることながら、何かといえば「経営に役立つシステム監査」を標榜するなら、経営幹部への新年のご挨拶で伝えましたか？「私物のPCやスマホもセキュリティ対策は万全ですか？あなたの予期していない形で、経営に悪影響が出るかも知れませんよ」と。

2014.01

第１８７回月例研究会　２０１３年１１月開催

記録者：木村裕一（会員番号0148）

講演テーマ：

2013 年版COSO内部統制フレームワークの概要

講師：森谷　博之（もりや　ひろゆき）氏

有限責任監査法人トーマツ

エンタープライズリスクサービス　シニアマネジャー

日時：2013年11月18日（月曜日） 18 時 30 分～20 時 30 分

場所：機械振興会館　地下 2 階　ホール

要旨（講師からいただいた講演骨子）

2013 年 5 月、内部統制フレームワークの事実上の世界標準の設定組織である COSO が、その最新フレームワークを公表しました。新フレームワークは、1992 年に公表された内部統制フレームワークを最新化したものであり、1992 年当時から現在までに生じた経営環境の変化や IT 技術の進化に対応したものです。

解説においては、まず COSO フレームワークが作成された背景を説明し、今回の改訂の位置づけ、構成、改定の概要を説明します。特にガバナンス、不正リスク評価など特徴的なトピックに重点を置いた説明をする予定です。COSO は、1992 年版フレームワークを適用している組織は、2013 年版フレームワークにて提示された諸原則が満たされていることを確認することを推奨しています。本セッションでは、2013 年版 COSO 内部統制フレームワークの概要を解説します。

講師紹介：森谷博之（もりや　ひろゆき）氏は、有限責任監査法人トーマツにてエンタープライズ　リスクサービス部署のシニアマネジャー。公認会計士、公認不正検査士、内部統制評価指導士、公認内部監査人

2003 年公認会計士登録。食品・飲料メーカー、IT システムベンダー、小売業を始め多くの会計監査や株式公開支援を担当。

2004 年より現部署にて内部統制構築支援、リスクマネジメント体制構築支援、内部監査支援に従事。

「内部統制実践ガイド」（ダイヤモンド社）、「内部統制報告制度実務詳解」（商事法務）等、内部統制関連の著書多数。その他、「DIAMOND ハーバード・ビジネス・レビュー」ダイヤモンド社）等、雑誌への寄稿多数。

講演の内容： まず全体を次の目次で解説します。

目次

なお、当該資料中の意見に渡る箇所は、演者の私見であり、演者の所属する組織の公式見解ではないことにご留意ください。また、本文中の訳語はすべて演者による仮訳です。

（注）スライドの注記にもありますが、講演者から「資料中の意見に渡る箇所は、演者の私見であり、演者の所属する組織の公式見解ではないこと」のお断りがありました。

1. COSO フレームワークとは何か （参照　スライド3、スライド4）

1980 年代に米国にて粉飾事件が多発した。その対応のために不正財務報告全米委員会（いわゆるトレッドウェイ委員会）が、1987 年に「不正な財務報告」レポートを上梓。同レポートは内部統制の重要性および評価基準の設定の必要性を勧告。同委員会の支援組織たる各専門職団体は、内部統制基準の設定委員会を設置した。この委員会が COSO である。「不正な財務報告」レポートの構成を、スライドの右に示す。

COSO は「”実社会”において内部統制を遂行する経営者のニーズに応えた」フレームワークを作るべく、CEO/CFO 等への面接調査やアンケートを多数実施し、その他多数のワークショップ、実地調査、ドラフトへの意見聴取等を実施し、経営実務を存分に調査・研究して、92 年に内部統制のフレームワークを公表した。これが COSO フレームワーク(以後、フレームワークを FW と標記します）である。

COSO-FW とは、簡潔にいえば組織が一定の目的を達成するために設計されるべきプロセスの体系のこと。COSO-FW は、右図のように三次元のイメージ図で概念化されている。

（スライド3）

1．COSOフレームワークとは何か

不正財務報告全米委員会とCOSO

- 1980年代に米国にて粉飾事件が多発。
- その対応のために専門職団体が立ち上げた不正財務報告全米委員会（いわゆるトレッドウェイ委員会）が、1987年に「不正な財務報告」レポートを上梓。
- 同レポートは内部統制の重要性および評価基準の設定の必要性を勧告。
- 同委員会の支援組織たる各専門職団体は、内部統制基準の設定委員会を設置。
- この委員会がCOSOである。

「不正な財務報告」レポート

1.財務報告システムと不正な財務報告の概要
2.公開会社に対する勧告

勧告の一部
➢経営者は、不正な財務報告を防止または早期発見することの重要性を認識し、財務報告に関する統制環境を確立すること。
➢内部会計統制および内部監査を充実させること。
➢社外取締役から成る監査委員会を設置し、その機能を拡大させること。
➢内部統制に関する経営者の意見等を年次報告書に記載すること。

3.公認会計士への勧告
4.証券取引委員会その他組織に対する法規制環境の改善のための勧告
5.教育に対する勧告

（出典：Report of the National Commission on Fraudulent Financial Reporting, COSO, p.v）

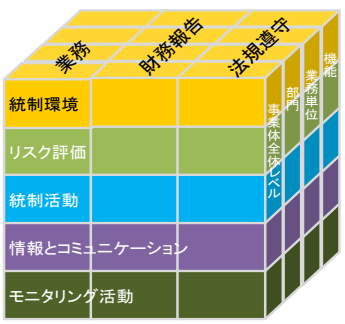
（スライド4）

1．COSOフレームワークとは何か

COSOフレームワーク

- COSOは「”実社会”において内部統制を遂行する経営者のニーズに応えた」フレームワークを作るべく、CEO/CFO等への面接調査やアンケートを多数実施。
- その他多数のワークショップ、実地調査、ドラフトへの意見聴取等を実施。
- 経営実務を存分に調査・研究し、92年に内部統制のフレームワークを公表。これがCOSOフレームワーク(以後、フレームワークをFWと標記します）。
- COSO-FWとは、簡潔にいえば組織が一定の目的を達成するために設計されるべきプロセスの体系のこと。
- COSO-FWは、右図のように三次元のイメージ図で概念化されている。

オリジナルCOSOキューブ



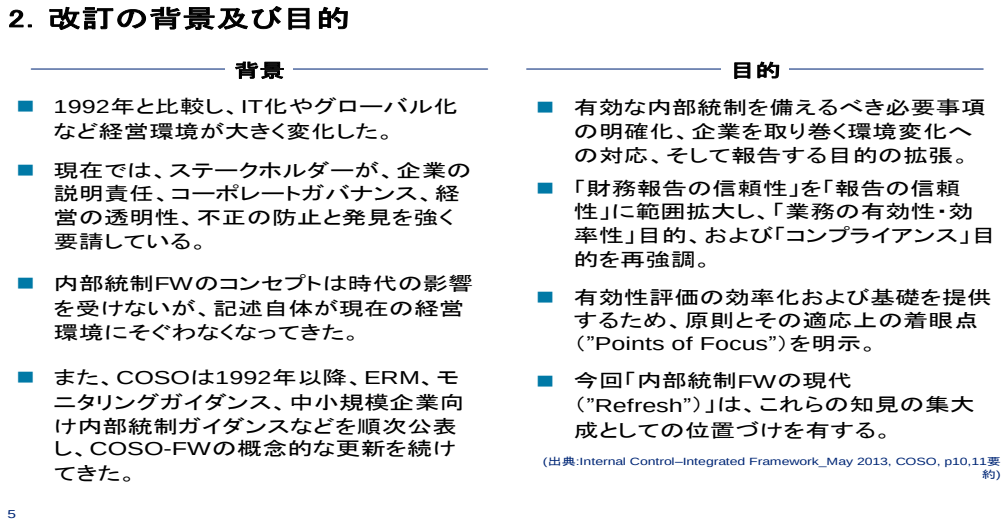
(出典:INTERNAL CONTROL – INTEGRATED FRAMEWORK,COSO, p19)

4

2. 改訂の背景及び目的　（参照　スライド5）

1992年に制定されたCOSO－FW（92年版と記す）は、広く内部統制のガイダンスとして実社会で実践的に先進的な企業を中心に適用され、これまで20年の利用実績を積み重ねてきた。
この20年間、世界中の企業や非営利組織を始め、国連や米国、日本といった公的機関においても、COSO-FW はカスタマイズされて内部統制を有効にするために利用されてきた。ただ、制定された1992年と比較して IT 関係の劇的な変化やグローバル化など事業環境の在り様が大きく変化したため、92 年版の記述は現在の経営環境にそぐわなくなってきた。このような背景から COSO は FW を見直し改訂して公表した。見直しの目的を、スライド右欄に示す。

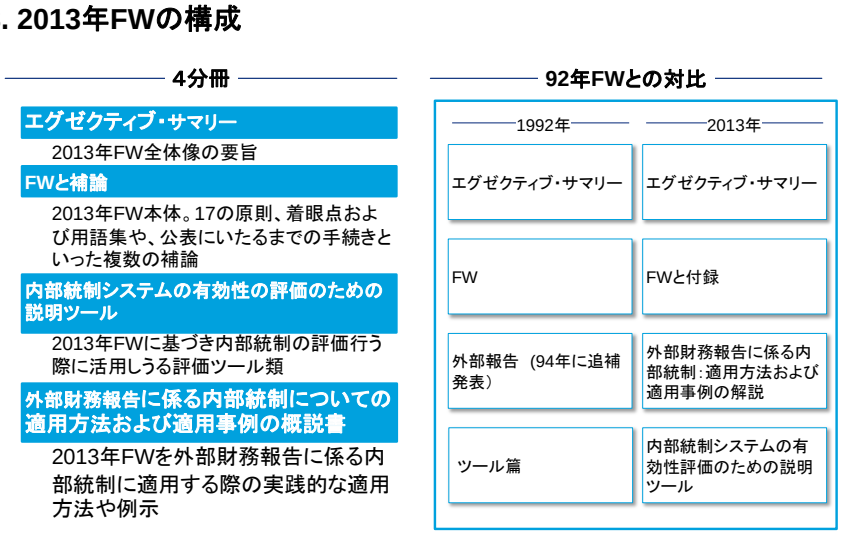
（スライド5）



3. 2013年 FW の構成　（参照　スライド6）

COSO は、92年版を発表以降も、利用を促進するために様々なガイダンス等を公表しながら、内部統制に関する様々なナレッジを蓄積してきた。今回の見直しを機にその蓄積を一気に FW に取り込み、もっと実務的に使えるようにとの観点で改訂が行われた。ただ、92年モデルの基本的考え方は依然有効であると考えられている。新しい FW の構成は次のようになる。

（スライド6）



1992 年版文書は 400 ページほどであるが、2013 年版は 600 ページ（価格 270 ドル）ほどで内容が豊富になっている。なお、エグゼクティブサマリーは、次の URL から無償でダウンロードできる。

http://www.coso.org/

http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf

(COSO Internal Control–Integrated Framework Executive Summary May 2013)

4. 改訂における変更点　（参照　スライド7）

この改訂において、変更されない部分と、変更される部分がある。

（スライド7）

4. 改訂における変更点

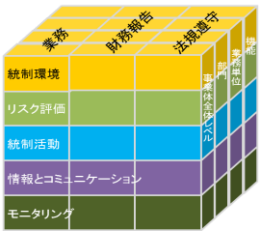
変更されない部分

1. 内部統制の定義
2. 3つの目的と5つの構成要素
3. 5つの構成要素は効果的な内部統制の必要事項であること
4. 内部統制の整備、運用及び有効性評価における、主観的判断の重要性

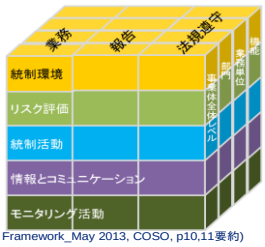
変更される部分

1. 経営環境変化への対応
2. 報告目的の拡張
3. 5つの構成要素と関連する17の原則を基本的なコンセプトとして明示
4. 適用事例の追加
5. 内部統制の有効性判断の基準

オリジナル COSO-FW



2013年版 COSO-FW



(出典:Internal Control–Integrated Framework_May 2013, COSO, p10,11要約)

7

5. 報告目的の拡張　（参照　スライド8）

スライド8に示すように92年版 FW が財務報告の外部に対する信頼性を目的にしていたことに加えて、2013年版 FW では企業内部・外部や財務・非財務を問わない報告全般へ拡張し、報告の適時性や透明性を対象にしている。

（スライド8）

5. 報告目的の拡張

報告目的の拡張

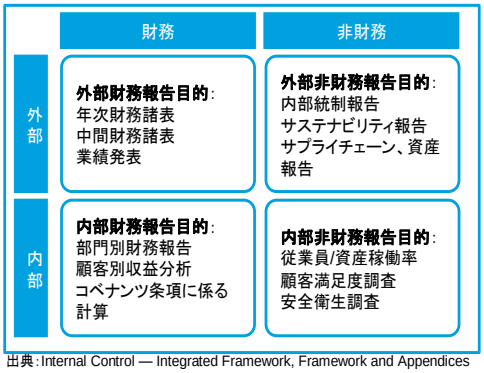
■ 1992年FWの内部統制の目的として財務報告*が挙げられていた

*財務報告とは、信頼しうる外部公表財務諸表の作成に関するもの

■ 2013年FWは社内外の別や財務・非財務の別を問わず、報告全般を対象

■1992年FWは財務報告の信頼性を対象

■2013年FWでは、報告の信頼性に加え適時性や透明性なども対象



出典:Internal Control — Integrated Framework, Framework and Appendices p9

6.　17 原則への再構成　（参照　スライド9　）

企業の内部統制が COSO－FW に適合しているかを判断する原則（原則主義）を取り入れた。各構成要素に関する記述を原則と適用上の着眼点として再構成したものである。原則は 17 項、着眼点は 75 項である。“原則は内部統制が有効と結論付けるための必須要件”である。また、“着眼点は、原則を満たすための着眼点”である。

（スライド9）

6. 17原則への再構成

新FWの構造

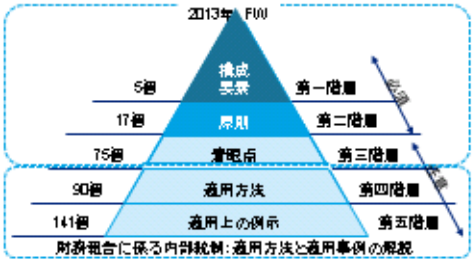
■各構成要素に関する記述を原則と適用上の着眼点として再整理。

■原則は各構成要素に関する土台となる概念であって、あらゆる組織に適合する。

■原則が有効でない場合には構成要素が有効でないと判断され、結果として内部統制が有効でないという結論に至る

原則は内部統制が有効と結論付けるための必須要件。

■着眼点とは、原則を満たすための着眼点であって、その導入は必須とまでは言えないものの、内部統制の構築やその有効性を評価することをサポートする



構成要素名	原則	着眼点	適用方法	適用上の例示（単位:個）
統制環境	5	20	25	36
リスク評価	4	15	19	27
統制活動	3	16	16	32
情報とコミュニケーション	3	14	19	26
モニタリング活動	2	10	11	20
トータル	17	75	90	141

7. ガバナンスに対する期待の高まり　（参照　スライド10）

ガバナンスについて、原則2として取り上げている。これはスライド10の記述のように、経営者から独立した立場からの視点で経営をチェックして、その問題点を指摘することが出来るようにしていることが重要である。取締役会は CEO の罷免、選任をすることが出来る。取締役会が、CEO の行うことの問題を指摘する勇気（意欲）を持つことが必要である。

原則、つまり内部統制の必須要件の中には独立とは何か、監督とは何か、の意味が明記されていない。これは、各国の法的あるいは社会的要請が異なるため一律的に必須要件として定義できないことも一因にあるが、しかしより重要なことは、法律や社会規範を基礎としつつも、取締役会が備えるべき独立性、監督義務とはどのようなものであるのかを企業自らが考え、あるべきガバナンス、内部統制を考察することを COSO は求めていると思料されるのである。そのうえで、企業の考察に多雨する COSO としての提言が、着眼点の位置づけで記述されている。

（スライド10）

7. ガバナンスに対する期待の高まり

取締役会の位置づけ

■ 1992年FWでもガバナンスの重要性は認識され、その中心的存在である取締役会について様々な記述があった

■しかし、2013年FWは、世界的なガバナンスへの関心の高まりを受けて、ガバナンスに関してさらに広範囲かつ具体化

■ たとえば、付録B「内部統制に関する役割と責務」にて、取締役会の役割について次のようにその重要性を強調

取締役会は、CEOの選解任権を通じて、内部統制に関する責任の履行において期待される誠実性や倫理的価値観、透明性、説明責任を決定付ける鍵を握っている

Internal Control – Integrated Framework, Framework and Appendices p147

【原則2】監督責任の履行

取締役会は、経営者から独立していることを表明し、かつ、内部統制の整備および運用状況についての監督を行う。

【着眼点】

監督責任の確立–取締役会はその監督責任を明確にし、受容する。

関連ある専門性の適用–取締役会は、経営陣が行おうとしている判断に対し鋭い質問を投げかけ、相応の対応を行う上で必要となるスキルや専門性を明確にし、維持し、定期的に評価を行う。

独立した運営–取締役会には、経営陣から独立し、客観的な評価や意思決定が行える取締役が十分な人数在籍している。

内部統制システムへの監督–取締役会は経営陣が整備・運用している内部統制に関する監督責任を保持している

10

8.　不正リスクの評価　　（参照　スライド11、スライド12）

また、不正リスクの評価の見直しも2013年版の重要テーマである。92 年版でも取り上げていたが、明示はしていなかった。今回 COSO が特に重視した項目の一つであり、原則として取り上げることで、不正リスク評価を有効な内部統制が備えるべき必須要件として位置づけた。

（スライド11）

8. 不正リスクの評価

これまでの扱い

- そもそもCOSO-FWは1980年代に米国で多発した粉飾事件を受けて作成されたものであるから、不正リスクをいかに低減するかはCOSOの中心的課題の一つである。
- 不正リスクの評価については、新COSO-FWにおいて初めての概念ではなく、中小規模企業向けの財務報告に係る内部統制ガイダンスの中にすでに【原則10】として登場している。

【原則10 】　不正リスク
不正に起因する重要な虚偽表示の可能性が、財務報告目的の達成を脅かすリスクを評価する際に明示的に検討されている。
(出典:Internal Control over Financial Reporting- Guidance for Smaller Public Companies Volume II_Guidance, COSO, p52)

新FWでの扱い

■原則8「不正リスクの評価」の実施に当たり、以下の点の考慮を求めている。

【着眼点】
➢不正な報告や財産の横領、汚職など、様々なタイプの不正タイプを検討すること
➢不正の誘引や動機、プレッシャーの存在の有無を評価すること
➢不正の機会がどの程度あるのかを評価すること
➢不正の正当化の余地が生まれやすい土壌があるかどうかを評価すること
(出典:Internal Control — Integrated Framework, COSO, p78)

■加えて、上記着眼点の実行にあたり、以下のアプローチを推奨している。

【推奨アプローチ】
✓不正リスクアセスメントを実施すること
✓統制活動を迂回したり無効化する方法がないか検討すること
✓内部監査において不正リスクを検討すること
✓役員報酬や給与・賞与体系において不正意欲を高めかねない誘引や圧力がないか確認すること
(出典:A Compendium of Approaches and Examples, COSO, p71-73)

11

（スライド12）

8. 不正リスクの評価

統制環境

■個人の行動は、CEOや管理職の行動が倫理的であったかどうかに大きな影響を受ける。
(出典:Internal Control — Integrated Framework, COSO, p34要約)

■行動規範への意識が希薄化する状況

- 経営者からの、規範遵守への期待に関する姿勢が従業員に伝わってこない
- 適切な監督がなく、現場の状況が経営者に伝達されない組織の分散化
- 上司等からの不正への参加の強制
- 従業員が安全に疑問や懸念を表明できるチャンネルの不存在
- 倫理的行動に妥協する動機やプレッシャーを与える業績目標
- 不正を発見し報告する能力のない脆弱な内部監査機能

(出典:Internal Control — Integrated Framework, COSO, p36要約)

9.　IT 技術への対応

IT 技術への対応は、この20年の IT 技術の発展に対応する見直しであり、スライド13に示す。

（スライド13）

9. IT技術への対応

IT技術への対応

■1992年FW公表以後、IT技術が飛躍的に発展

■内部統制とITとの関連性がさらに深化

■2013FWでは、ITに対する内部統制を重視する姿勢を強めている

■ITを適切に利用することの重要性について多くの紙面が割かれている

■その表れの一つとして、ITに関する右図にある原則を用意しています。

【原則１１】IT技術への全般統制

組織は内部統制の目的の達成を支援するIT技術に関する全般的統制活動を選択し、整備する

【着眼点】

業務プロセスにおいてどの程度テクノロジーおよびその全般統制を活用するかを決定する

関連する技術的なインフラおよびセキュリティに対する統制活動を確立する

テクノロジーの取得、開発、メンテナンスに対する統制活動を確立する

出典：Internal Control–Integrated Framework, Framework and Appendices p97

10.　内部統制が有効であるとは

13

COSO-FW を適用して、その結果企業の内部統制が有効であることを判断することは次のスライド14のように判断する。

すなわち、“5つの構成要素および関連する原則が、存在し（present）、機能して（functioning）いなければならない。”

⇒スライド14　上の網掛け

（92 年版のデザイン、インプリメンテーション、オペレーションの用語は今回変更した）

また、“5つの構成要素は統合された形で一体的に運用されていなければならない。” ⇒スライド14　中の網掛け

その判断を踏まえて、経営者が内部統制について、有効であることを表明できることになる。

（スライド14）

10. 内部統制が有効であるとは

有効性の判断基準

■内部統制が有効であるためには、5つの構成要素および関連する原則が、存在(present)し、機能(functioning)していなければならない。

- **「存在している」**…特定の目的を達成するための内部統制システムの設計と導入に際し、構成要素および関連する原則が存在していると判断されること
- **「機能している」**…特定の目的を達成するための内部統制システムの実施に際し、構成要素および関連する原則が存在し続けていると判断されること

■5つの構成要素は統合された形で一体的に運用されていなければならない。

「一体的に運用される」…5つの構成要素全体として、リスクを許容可能な水準まで軽減していると判断できること

経営者は次のような場合に構成要素が一体的に運用されていると表明することができる。

「構成要素が存在し、機能している。」

「複数の構成要素にわたって内部統制の不備を集計した結果、一つまたは複数の主たる不備ではないとの判断に至った。」

(出典:Internal Control - Integrated Framework, COSO, p18-20要約)

14

11. 改訂の概要（17 原則・ポイント）

今回取り入れた原則主義において有効性評価の基礎となる17原則を次に示す。
（当日は後半（スライド 10－18）でこの原則とポイントについて説明されたが、当記録では＜構成要素＞と 17原則を表示するのみにとどめ、説明の記述は省略する）

＜統制環境＞
1.誠実性と倫理的価値観にコミットする姿勢の明示
2.取締役会の経営者からの独立と内部統制の構築・運営についての監督
3.目的の達成には、取締役会の監督の下に、経営者による組織構造、レポーティングライン、権限と責任の確立が一般的に必要となる
4.能力ある者を採用し、教育し、効用維持することをコミットする姿勢の明示
5.内部統制に関する責任権限の明確化

〈リスク評価＞
6.リスクの識別・評価を可能にするための目的の設定
7.企業目標の達成を脅かすリスクの識別とリスク管理のための分析
8.不正リスクの評価
9.内部統制システムに重要な影響を与える変化の識別と分析

〈統制活動＞
10.企業目標の達成を脅かすリスクを許容可能な水準に低減する統制活動の選択と構築
11.企業目標の達成に寄与する IT 全般統制の選択と整備
12.方針とそれに対応する手続の整備

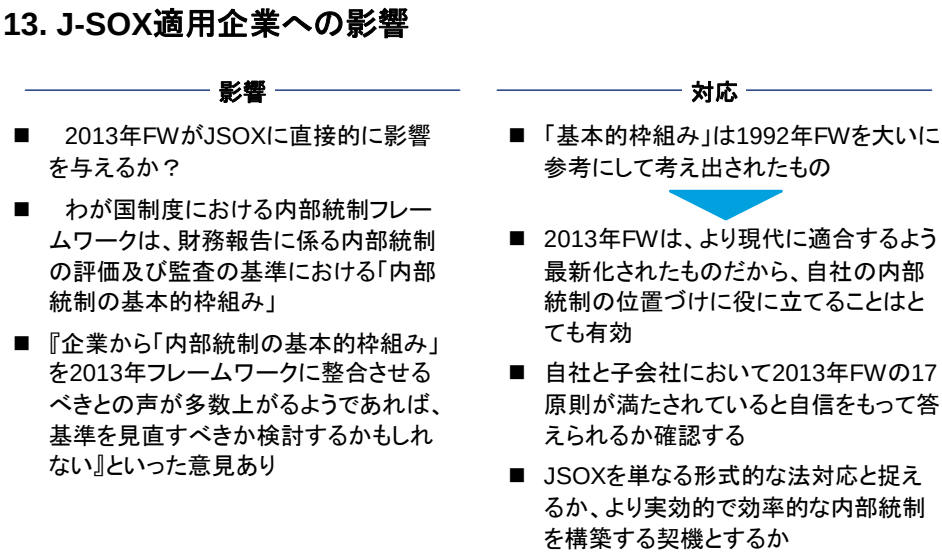
〈情報と伝達＞
13.内部統制の機能を支援する情報の発信と利用
14.内部統制の機能を支援する情報（その目的と職務を含む）の組織内の伝達
15.内部統制の機能に影響を与える事項についての外部との情報交換

〈モニタリング活動＞
16.内部統制の構成要素が存在し、機能していることを確認するための日常的及び独立的評価の選択、整備、運用
17.内部統制の不備を評価し、是正措置を講じる責任を負う者（経営者及び取締役会含む）への伝達

12.　新 COSO-FW への変更手順について　（スライド19、スライド20：略）

スライドの中で、「COSO は 2013 年度版 FW を速やかに導入するように求めており、92 年版 COSO-FW を 2014 年 12 月 15 日までを移行期間としている」（廃止する）、としている点は重要である。廃止とは、“存在しなくなる”ことであるために、移行期間後は 92 年 COSO-FW に準じていると宣言が出来なくなる。（以上記録者コメント）
（当講演記録では、92年版から2013年版 COSO－FW への変更手順について省略する。）

13.　J―SOX 適用企業への影響　（スライド21：説明は省略）



今後の COSO-FW の活用について、次のよう考える。（記録者コメント）　＜スライド21の右欄3項目＞

・2013 年版 FW は、より現代に適合するよう最新化されたものだから、自社の内部統制の位置づけに役に立てることはとても有効

・多くの企業・組織において親会社、子会社の内部監査の評価基準に利用できる。

・JSOX への対応のため（という受身）でなく、自社のために実効的で効率的な取組みの契機としてほしい。

質疑応答:

質問1：.PCAOB　AS5 の監査基準との関係はどうなるか。

（注）PCAOB：Public Company Accounting Oversight Board　公開会社会計監査委員会

講演者コメント：PCAOB で策定されている US-SOX の監査基準では COSO－FW を使えとは規定していない。しかし、COSO－FW は US-SOX でのデファクトスタンダードであり、SEC や PCAOB も COSO－FW の策定に関与しているので、結果として US-SOX 適用会社は新 FW をその評価基準として使うものになると考える。

質問2：大手監査法人で使用している3点セット（リスクコントロールマトリックス、フローチャート、業務記述書）のフォームを変更するのか。

講演者コメント：3点セットとは、内部統制評価の過程を目に見える形にしたもの。原則6＜リスク評価＞の基本の部分はこれまでと変わらないことを考えると、3 点セット自体が修正されることは想定されていないのではないか。原則8

にて示された不正リスク評価については、これまでに十分な対応をしていない企業も少なくないと思われるため、そういった企業では不正リスク評価にかかる新しいシートの準備が必要となる可能性がある。

質問3：COBIT と COSO の関係はどのようになっているか。
講演者コメント：COSO は COBIT に比べ、経営全般的なものを扱っていると考えている。その分、COSO のほうが COBIT に比べ IT 統制に関する記述が総論的であるとの印象は否めない。したがって、IT統制に関する有効性、効率性などITのFWに関しては、言葉使い、考え方などにおいてCOBIT のほうが使いやすいかと思う。COBIT は COSO との整合性を十分に検討しているとも聞いている。

質問4：コンプライアンスが重要であるが、IT利用の不正検出についてどのように言及しているか。
講演者コメント：ITスタッフの離職率についてモニタリングをする立場の者、不正を識別する立場の者などの離職率が高いのは不正の予兆の可能性があるといった言及があるほか総務部門、退職者、ITの特性の調査、経営者の情報操作能力、などの調査に言及している。

以上質疑応答

記録者の感想：

講師の森谷氏からは2013年版COSO－FWの盛り沢山の内容について非常に精力的に講演をいただき、参加者も終始熱心に聴講していた。講師のCOSO－FW全体に精通された説明は、月例研究会の限られた時間内では収まりきれずもっと時間がほしい内容であった。日本においての採用企業はまだ少ないということであるが、このようなCOSO－FWあるいは内部統制の考え方（内部統制の充実や透明性の確保）は企業・組織の規模の大小に関わらず、必要なことである。また、第三者的な立場で物事を見ることも重要であるが、COSO－FWの原則・着眼点に表されたことが日本では基本認識としてまだ定着していないのではないかと、今回の講演を通じて（記録者として）感じられた。

システム監査人は企業の経営にはその情報システムからの切り口で関与することがほとんどであるが、森谷氏のお話にあったとおり内部統制に関する枠組みの理解と活用は、今後ともシステム監査人として研鑽が必要であると感じた次第である。有限責任監査法人トーマツのHPにもいろいろな情報が提供されているので、それらも参考に出来るようである。

当記録は、当日のセミナーの中のごく一部、森谷氏がお話された、2013年版のCOSO－FW改訂の特徴的な点についてスライドを見る導入として紹介しました。インターネットから多くの情報を得ることが出来、エグゼクティブサマリーは、誰でもダウンロードできるとのことです。皆様の必要に応じて活用をいただきたいとのことでした。　　（木村　記）

以上

2014.01

【情報セキュリティ監査研究会だより その１０ ― プライバシー・バイ・デザイン 第５回】(連載)

会員番号 0056　藤野明夫(情報セキュリティ監査研究会)

はじめに

情報セキュリティ監査研究会では、アン・カブキアン著、「プライバシー・バイ・デザイン　プライバシー情報を守るための世界的新潮流」をテキスト(以下、左記の書を「テキスト」と称します)として、「プライバシー・バイ・デザイン」の意義、影響、PIAやシステム監査との関係などを議論しております。

前々回からテキストの第2章第6節「新たな連携プライバシー影響評価(F－PIA):プライバシーと信頼できる連合体の構築」を取り上げております。なぜ、この節を取り上げたかというと、ネットワーク社会の進展にともない個人情報が複数の組織間(企業、政府機関、その他の団体)で大量に授受されることがあたりまえになってきているなかで、未だ個人情報保護に関する種々の取り組みが単一の組織内に留まっていて、かかる状況に対応できていないと考えるからです。我が国のプライバシーマーク制度も単一の組織を対象としています。

この問題に対して、真正面から取り組んでいるのが、カブキアン博士の提唱するF-PIA(連携プライバシー影響評価)です。前回、前々回とF-PIA実装の前提になるFIM(連携アイデンティティ管理)、FIMの実現形態であるアイデンティティ連合体の四つのモデル及びこの連合体によって実施されるF-PIAの目的についてご説明いたしました。今回は、F－PIAのご紹介の最後として、F－PIAにおける質問の内容、いわば、F－PIAのエッセンスというべき内容についてご紹介します。実は、F－PIAの質問の内容はかなりの部分がプライバシーマーク制度の基礎となっている個人情報保護マネジメントシステムJIS15001(以下、「PMS」)と対応がつきます。今回は、今までと趣向を変え、F－PIAについてPMSとの対応付けの形でご説明したいと思います。プライバシー・バイ・デザインというと少しばかりとっつきにくいと思いますが、PMSについては、個人情報保護に関心のある方であれば、ある程度はご存知であろうと思うからであります。

PMSについてあまりご存知ない方には、たいへん申し訳ないのですが、紙面の関係でご説明をする余裕がなく、下記の参考文献1と2をご参照いただきたいと存じます。また、下記、報告のなかのF－PIAの質問の内容は、テキストP175～178に示されております。

なお、本報告は、情報セキュリティ監査研究会内部の検討結果であり、日本システム監査人協会の公式の見解ではないことをお断りしておきます。また、我々の力不足のため、誤りも多々あるかと存じます。お気づきの点がございましたら適宜ご指摘いただきたいと存じます。ご興味のある方は、毎月20日前後にSAAJ本部会議室(茅場町)で定例研究会を開催しておりますので是非ご参加ください。参加ご希望の方、また、ご意見やご質問は、下記アドレスまでメールでご連絡ください。 security ☆ saaj.jp （発信の際には“ ☆ ”を“@”に変換してください）

＜テキスト＞　堀部政男／一般財団法人日本情報経済社会推進協会(JIPDEC、以下、同じ)編、アン・カブキアン著、JIPDEC訳「プライバシー・バイ・デザイン　プライバシー情報を守るための世界的新潮流」、2012年10月、日経BP社

＜参考文献１＞　日本工業標準調査会 審議、「個人情報保護マネジメントシステム－要求事項 JIS Q 15001:2006」、2006年5月、財団法人 日本規格協会

＜参考文献２＞　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 第2版」、2007年1月、財団法人 日本情報処理開発協会

【報告内容】新たな連携プライバシー影響評価(F-PIA：Federated Privacy Impact Assessment) その３
Ｆ－ＰＩＡの質問内容と個人情報マネジメントシステムＪＩＳ１５００１との対比

Ｆ－PIAが何を狙っているのか、より明確にするために、いささか強引であるが、Ｆ－PIAの質問内容を日本のプライバシーマーク制度の基になっているPMSの要求事項と対応付けてみたいと思う。PMSは単一の組織に対する要求であるのに対して、Ｆ－PIAは複数の組織からなる連合体に対する質問であり、その異同を示すことは、Ｆ－PIAの本質を把握する上で意義あることと考える。

Ｆ－PIAにおける質問内容は、①情報ライフサイクル、②運営方針、③実装の三つのカテゴリーに分けられる。

以下、Ｆ－PIAの質問の内容を()付きの項番+ゴシック体で示す。

１．情報ライフサイクルにおけるＦ－ＰＩＡの質問内容とＰＭＳとの対比

ここでの質問内容は、プライバシー保護に関する基本的なコンセプトに対して組織内でコンセンサスができているかを問い、また、それを実施するうえでの体制や仕組みができているかを問うものである。

（１） 適切な通知：転送される個人情報の主体は、その転送を認識しているか

第三者提供に関する本人への通知がされているかを問うものである。「JIS3.2.4.8 提供に関する措置」の「通知」の要求に該当する。Ｆ－PIAは、複数の企業、組織間で個人情報が点々流通する際のプライバシー保護、すなわち、第三者提供の際のプライバシー保護が目的であるから、この質問が筆頭に来るのは当然といえる。

（２） 適切な仕様：連合体の当事者は、情報の収集、利用、共有、保有に関する制限を適切に認識しているか

それぞれの組織に属する者が、プライバシー保護に関する基本的なルールを認識しているかを問うものである。「PMS」では、「JIS3.4.5教育」に当たるかと思う。

（３） 適切な同意：個人情報の転送は適切にユーザーの同意または選択に結びついているか

第三者提供に関する本人の同意がされているかを問うものである。「JIS3.2.4.8 提供に関する措置」の「同意」の要求に該当する。(1)と同様、Ｆ－PIAは、複数の企業、組織間で個人情報が点々流通する際のプライバシー保護、すなわち、第三者提供の際のプライバシー保護が目的であるから、当然の質問である。

（４） 適切なコントロール：ユーザーは自分の個人情報の転送を適切にコントロールできるか

「JIS3.2.4 個人情報に関する本人の権利」が該当する。JIS3.2.4全体が個人情報に対する自己コントロール権に関する要求事項であるからである。

（５） データの最小化：連合体の参加組織が収集する個人情報は、必要最小限か

「JIS3.2.4.1 利用目的の特定」が要求する「個人情報を取得するに当たっては、その利用目的をできる限り特定し、その目的の達成に必要な限度において行わなければならない」に該当する。

（６） 最小手段アクセス：連合体の参加組織が転送またはアクセスするのは、特定の取引を実行するために必要な個人情報だけか

この質問に関しては、PMSの要求にぴったり符合するものはないが、強いて言えば、「JIS3.2.4.1 利用目的の特定」、「JIS 3.2.4.7 本人にアクセスする場合の措置」及び「JIS 3.4.2.8提供に関する措置」であろう。

（７） コンプライアンス、監査、監督：プライバシーポリシーの順守を確実にするための監督機関、監査またコンプライアンスの仕組みが存在するか

「JIS3.3.4 資源、役割、責任及び権限」及び「JIS3.7.2 監査」が該当する。PMSは、前者の要求中に具体的に「個人情報保護監査責任者」という役割を要求し、また、後者では、「監査」における遵守事項や報告先を具体

的に定めている。

（８） 報告：コンプライアンスを証明するためのポリシーおよび手順の文書化が十分に行われているか

「JIS3.5 個人情報保護マネジメントシステム文書」が該当する。PMSの要求事項では、文書の種類を詳細に、個人情報保護方針、内部規定、計画書、記録に分けて、その管理レベルを規定している。

２．運営方針におけるＦ－ＰＩＡの質問内容とＰＭＳとの対比

ここでの質問内容は、連合体というF－PIA独特の体制に係るものなので、素直にPMSの要求事項に対応するものではない。しかし、その質問が問う内容のいくつかは、単一の組織に対する要求であるPMSの要求事項の拡張で対応できる。

（１） 構造と役割の割り当て：連合体の全参加組織の役割は明確に理解され、透明性を持って定義されているか。連合体の参加組織は各自の責任と義務を理解しているか

これは、Ｆ－PIA独特の連合体組織の体制に係る質問なので、PMSの要求事項に直接該当するものはない。しかし、その求めているものは、単一の組織における「JIS3.3.4 資源、役割、責任及び権限」の要求事項と同様なので、これの拡張で対応できるのではないか。

（２） ユーザーの理解：連合体の参加組織の名前や種類、役割は、ユーザーに明確になっているか

Ｆ－PIA独特の連合体に係る要求である。これについては、PMSに対応するものはない。

（３） エコシステムレベルでのアイデンティティ管理：サービスプロバイダー(*1)はユーザーの承諾を得ることなく、ユーザーのプロファイルをサービス全体にリンクすることができるか。これは、サービスプロバイダーがアイデンティティプロバイダー(*2)としての役割も兼ねている場合に懸念されることである

これは、アイデンティティプロバイダーというＦ－PIAを構成する概念に絡むものなので、PMSに該当する要求はないが、強いて近いものを探せば、JIS3.2.4.1 利用目的の特定」と「JIS3.2.4.6 利用に関する措置」が該当すると思う。前者は目的外利用を禁止しており、後者は、目的外利用が発生した場合の利用目的の変更の手順、すなわち、事前の本人への通知及び同意取得を定めているからである。おそらく、この二つの要求事項の拡張で対応できるのではないか。

〔(*1)サービスプロバイダー、(*2)アイデンティティプロバイダー：会報153号(12月号)P10－11、【情報セキュリティ監査研究会だより その8 － プライバシー・バイ・デザイン 第3回】参照〕

（４） ユーザーの関与：連合体はアカウントのリンク、トラフィック、分析をどのように予防しているか。連合体は管理策の定義において、ユーザーの関与をどのように促進しているか

これも、(3)と同様に連合体内でのアカウントのリンク、トラフィック、分析というＦ－PIA独特の課題に対する質問事項であるので、PMSに該当する要求はないが、強いて近いものを探せば、(3)と同様に「JIS3.2.4.1 利用目的の特定」と「JIS3.2.4.6 利用に関する措置」が該当し、これらの拡張で対応できるのではないかと思う。

（５） 最悪のシナリオ：「災害」が発生した場合にユーザーに通知し、被害を最小現に抑える手順を含むシナリオは検討されているか

「JIS3.3.7 緊急事態への準備」が該当する。単一の組織に対する要求を連合体に拡張すればよい。

３．実装におけるＦ－ＰＩＡの質問内容とＰＭＳとの対比

ここでの質問内容は、2. と同様に、連合体というF－PIA独特の体制に係り、さらに、実装という、より具体的なカテゴリーに関するものであるので、素直にPMSの要求事項に対応するものではない。しかし、そのいくつかは、単一

の組織に対する要求であるPMSの要求事項の拡張で対応できるのではないかと思う。

（１） 認識：連合体の参加組織は、必要な情報およびネットワークセキュリティ、また、セキュリティを強化するために実施できる手順を提供しているか

これは、「JIS3.4.3.2 安全管理措置」が適用できるのではないか。

（２） 説明責任：連合体の参加組織は、各自の役割に適した程度に、情報セキュリティについて説明責任を果たすことができるか

連合体における役割というF－PIA独特の質問内容なので、「JIS3.4.3.2 安全管理措置」がそのまま適用できる訳ではないが、ある程度の拡張をすれば対応できるのではないか。ただし、内容が技術的なので、連合体内の各組織間の技術的インフラの統一、あるいは、整合性確保といった高度な技術的問題が発生する可能性がある。

（３） 対応：連合体の参加組織がセキュリティ事故を共同で防止、検知、対応できるように、対応のための行動計画が用意されているか

F－PIA独特の連合体に係る要求である。これについては、PMSに対応するものはない。

（４） 倫理：参加組織は各自の活動または非活動が、他の連合体の参加組織に悪影響を与えることを理解しているか

F－PIA独特の連合体に係る要求である。これについては、PMSに対応するものはない。しかし、セキュリティの問題と異なり、技術的な課題ではないので、対応は比較的容易であろう。

（５） リスク評価：すべての連合体の参加組織は個別および連合レベルで、リスク評価および最小化プロセスを実施しているか

「JIS3.3.3 リスクなどの認識、分析及び対策」が比較的素直に適用できるのではないか。

（６） セキュリティの設計と実装：セキュリティは情報システムの不可欠な要素として設計されているか

まさにプライバシー・バイ・デザインらしい質問である。これについては、PMSに対応する要求事項はないが、強いていえば、「JIS3.4.3.2 安全管理措置」か。

（７） セキュリティ管理：連合体はセキュリティ管理に対して包括的な取り組みをしているか

「包括的」という部分をうまく盛り込めば、「JIS3.4.3.2 安全管理措置」の拡張で対応できるのではないか。

（８） 再評価と学習：連合体および連合体の参加組織は、セキュリティ対策を再評価し、必要に応じて変更を実施するためのスケジュールを確保しているか

連合体の合意形成過程の問題はあるが「JIS3.8 是正処置及び予防処置」の拡張で対応できるのではないか。

まとめ

F－PIAが質問形式であるのに対して、PMSは規格であるから要求という表現形式になるという相違はあるが、求めていることは上述のとおり、かなり似た内容である。ただ、F－PIAは、「連合体」を前提にしているので、連合体ゆえに満たすべき内容があり、すべてが対応づけられるわけではない。また、ここに記載されているF－PIAの質問の内容は、あくまでも例示であり、適用される連合体の性格により、また、プライバシー保護システムの成熟度により、自ずと変わるべきものである。したがって、ここで掲げたPMSとの対応づけも、あくまでひとつの試みにすぎない。

PMSになじみのある方に限られた話しではあるが、何か遠い世界のように思われていたF－PIAが、身近なものに感じられたのではないだろうか。

以上

2014.01

【　システム監査基準研究会　】

会員番号　0555　松枝憲司　　0281　力利則　（システム監査基準研究会）

○IT-ＡｕｄｉｔのＩＳＯ化について

先月に引き続き、9/24(火)の CSA フォーラムにおいて報告しました ISO30120(IT-Audit)についての資料の一部を紹介します。

「IT監査-ITガバナンスの評価を支援する監査のガイドライン（ISO30120：PDTR)(仮訳)」

5.2.1　監査プログラムの概観　（要約: 仮々訳）（続き）

プリンシプル2　　戦略

組織のビジネス戦略は、現状および将来のIT能力を考慮する。

ITの戦略計画は、組織のビジネス戦略の現状および継続的なニーズを満たすこと

プロセス

1. 適切なリスク評価策を策定するためのプロセス
2. ビジネス戦略を立案するためのプロセス
3. IT戦略計画を策定するためのプロセス
4. ITの利用から得られる便益をモニタするためのプロセス

プロダクト

1. ITのリスク評価報告
2. ビジネス戦略
3. IT戦略計画
4. 業務継続計画(BCP)
5. IT継続計画

プリンシプル3　　調達・取得

IT調達・取得は、適切かつ継続的分析に基づいた明確で透明な決定により、正当な理由づけで実施される。便益、機会、費用およびリスクの間には、短期および中期双方からの適正なバランスが存在する。

プロセス

1. IT調達のオプションを評価するためのプロセス
2. IT調達部署およびサプライヤをモニタするためのプロセス

プロダクト

1. IT投資計画
2. 情報資産管理に関するポリシー
3. アウトソーシングに関するポリシー
4. 提案依頼(RFP) に関するポリシー
5. 契約
6. IT資産(システムおよびインフラ)に関する報告書

2014.01

「個人情報保護マネジメントシステム実施ハンドブック」簡易版　第 20 章

会員番号：1760　斎藤由紀子（個人情報保護監査研究会）

第20章　点検

点検とは、事業者自らが構築したＰＭＳの有効性を確認するために行う重要な機能です。
点検には、２通りの手段があります。

運用の確認	個人情報保護管理者以下、全社、各部門、各階層の管理者が、自ら行う日常点検
監査	個人情報保護監査責任者が、組織から独立して第三者的な視点で行う点検

20.1　運用の確認

あらかじめ「3303 年間計画表（兼点検表）」にＰＭＳ運用の確認時期と確認項目を設定し、計画どおり実施されているかどうかを確認します。　上段に予定日、下段に実際に実施した日を記入し、進捗管理をすることになります。実施日は手書きでもかまいません。

201★年度「3303ＰＭＳ年間計画書」

	201★年	１月	２月	３月	４月
①	代表者の見直し（計画表の策定・承認）				
	（状況に変化があった際には随時見直し）				
②	法令・指針・規範の改定確認				
	（改定を確認した際には随時見直し）				
③	個人情報管理台帳の見直し			1	
	（取扱に変更があった際には随時見直し）			/	
④	リスク分析表の見直し				1
	（取扱に変更があった際には随時見直し）				/
⑤	従業者定期教育の実施		15		
	（採用者には採用初日に教育）		/		
⑥	監査の実施				
	（状況に変化があった際には臨時監査を実施）				
⑦	全社　「343401委託先管理台帳」				
	（「委託先調査票」が陳腐化していないか点検を含む）				

各記録の点検は、
毎月実施した日付を記入します。

⑧	各部門「3319　個人情報返却廃棄管理表」点検	/
⑨	3432-010「システム機器・ID管理台帳」点検	/
⑩	3432-015 情報機器「持出」許可申請書(OUT)点検	/
⑪	3432-016 情報機器「持込」許可申請書(IN)点検	/
⑫	3432-017「携帯電話使用申請書」点検	/
⑬	3432-211「入退館安全確認記録簿」点検	/
⑭	3432-212「来客入退館カード貸出簿」点検	/

開示請求、苦情などの
件数も記録します。

⑲	開示等請求の件数	計：　件	件	件
⑳	苦情・事故・ヒヤリ・ハットの発生	計：　件	件	件

20.2　監査

監査は、毎年以下の２つの観点から実施します。

監査目的	監査の内容	監査対象
適合性監査	法令、国が定める指針その他の規範および、個人情報保護マネジメントシステム－要求事項（JIS Q 15001:2006）に合致しているかどうかを監査する。	内部規程（PMS責任者、事務局など）
運用監査	自社のＰＭＳにおいて、リスク分析の結果講じるとした対策の運用状況の監査	全社、全部門（PMS運用、および各部門責任者など）

20.2.1　監査計画

全社を対象にした監査の時期については、大枠を「3303PMS 年間計画書（兼点検表）」に定めます。監査の実施時期は、事業の繁忙期を避ける必要があります。また定期的な全社員教育が実施され、個人情報の特定とリスク分析が実施され、運用が開始された後に行います。

監査計画書には、監査テーマ、部門ごとの実施時期、時間、監査担当者など、具体的な計画を立案します。
監査時間は業務の規模にもよりますが、被監査部門の意見を聴取する場でもあることを認識し、
少なくとも２時間程度は、確保するとよいでしょう。

サンプルの
監査計画書は、
監査報告書を兼ねています。

監査計画書は、代表者の承認が必要です。

201　年度　PMS監査計画書　兼報告書

（201×年4月1日～201×年3月31日）

標題の件、個人情報保護監査規程　第××条に基づき、下記のとおり実施致したくご承認願います。

監査責任者：取締役　○○○○室長

監査目的	1. JIS等の適合監査	当社ＰＭＳの、JIS Q 15001：2006など利用した	
	2. PMS運用監査	当社ＰＭＳにおいて、リスク分析の結果講ずるとし	
被監査部門 監査日程	1. JIS等の適合監査	個人情報保護管理者	1. 実施予定:
	2. PMS運用監査	全社および全部門	2. 実施予定:
特記事項	（予算、外部からの協力要請等）		

全部門を対象とすること　　監査担当者は被監査部門でないこと　　以下は、監査実施

	被監査部門	監査担当者		監査実施日
☆	ＪＩＳ等の適合性監査	○○○○部	○○○○○	２０１　／
①	ＰＭＳ体制	○○○○部	○○○○○	２０１　／
②	施設・設備の安全管理	○○○○部	○○○○○	２０１　／
③	情報システムの安全管理	○○○○部	○○○○○	２０１　／
④	○○○○部	○○○○部	○○○○○	２０１　／
⑤	○○○○部	○○○○部	○○○○○	２０１　／
⑥	○○○○支店	○○○○支店	○○○○○	２０１　／
監査結果	【監査責任者の所見】 1. JIS等の適合監査について 2. PMS運用監査について			

20.2.2　監査体制

個人情報監査責任者は、全部門の監査を実施する権限を持ちます。
代表者や個人情報保護管理者は、監査責任者を兼務することはできません。自分を監査してはならないというルールがあるからです。ただし、２名しかいない小規模事業者の場合、代表者は個人情報保護管理者を兼務し、監査責任者は他の者を指名します。
同様に、監査担当者は、自部門を監査することはできません。２名しかいない小規模事業者では、相互に監査担当者として監査を実施してください。
なお、企業の監査役は、内部統制上の機能制限により監査責任者だけでなく、個人情報保護体制に参加することはできませんので注意してください。

20.2.3　適合性監査

適合性監査は、規程を更新する時が最も有効な時期です。監査報告書を代表者に提出し、不適合があれば、見直しを経て規程が承認されるという手順で行ってください。

下記の「チェックリスト JISQ15001 適合性監査」のサンプルは、各項目の指摘事項、および全体の【不適合】の概観を記入して代表者に報告する様式になっています。このハンドブックで使用するチェックリストは、すべて報告書を兼ねています。

201y 年度　ＰＭＳ監査チェックリスト[JIS Q 15001 適合性」兼報告書

	代表者	監査責任者	被監査者	監査実施日	201y/mm/dd
				被監査部門	個人情報保護管理者
監査報告に当たっては、手書きのままでよい。 ①適合欄：○× ②規程欄：条項番号まで記載すること。	確認受領	報告	確認	監査担当者	○○部○○課 ○○○○○
				保存期間	３年後年度末
				廃棄予定	201y/mm/dd
	/ /	/ /	/ /	主管	個人情報保護監査責任者

【不適合】の概観

○×（業務がなければ　－）

JIS 要求事項	チェック内容	適合	規程および条文、使用する様式	指摘事項
1適用範囲	①下記の全従業者を人的範囲に定めているか。（正社員、契約社員、嘱託社員、派遣社員、パート社員、アルバイト社員、取締役、執行役、理事、監査役、監事、等を含む。）		3301 取扱規程 1.1	
	②全社を適用対象としているか。		3301 取扱規程 1.1	

20.2.4　運用監査

被監査部門の職場に出向き、部門長や、業務担当者に対するヒアリングや現場目視を行います。 事業の内容や取り扱いに応じて準備した「監査チェックリスト」を用い、エビデンス（証拠書類）や実態を確認して、「監査チェックリスト」に書き込んでいきます。

	運用監査チェックリストの種類	監査対象
b)	「3726b_予備調査チェックリスト」	被監査部門の事前準備用
c)	「3313c _リスク分析表（兼監査チェックリスト）」	【必須】
d)	「3726d_PMS体制の運用チェックリスト」	個人情報保護管理者および事務局
e)	「3726e_施設・設備の安全性チェックリスト」	施設ごとの管理部門
f)	「3726f_情報システム運用の安全性チェックリスト」	システム運用部門
g)	「3726g_情報システム開発の安全性チェックリスト」	システムのオーナー部門
h)	「3726h_部門ＣＰチェックリスト」	

a)～h)のうち、c)「3313c リスク分析表（兼監査チェックリスト）」を用いての監査は必須です。

部門	管理部	業務名　「従業員管理」								
業務フロー	採用から従業員管理および退職に至る従業員情報管理業務								/ /	
ライフサイクルおよび業務名		台帳	個人情報管理台帳に記載の個人情報名	取得手段 入力	媒体	コピー	想定されるリスク	リスク対策	規程・様式	監査 ○×	監査確認結果
取得	採用業務	1 2 3	履歴書 職務経歴書 成績証明書	本人・直接手渡し	紙	禁止	利用目的の通知漏れ 書面による同意の取得漏れ	1. 面接キット「同意書（応募者用」	「個人情報取扱規程」3.4.2.4		
							漏洩（紛失）	1. 保管管理者の限定	「安全管理規程」4		
								2. 施錠管理	「安全管理規程」4		
		4	応募者からの同意書		紙	禁止	漏洩（紛失）	1. 保管管理者の限定	「安全管理規程」4		
								2. 施錠管理	「安全管理規程」4		
移送		－	（応募者類の返却）	－	紙	－	漏洩（誤送付）	1. 簡易書留で送付	「安全管理規程」9		
								2. 送付表の保管	「安全管理規程」9		
利用		5	応募者リスト 採用結果票	面接者が記入	紙	禁止	目的外利用（期限を超える保管）	「廃棄記録」による確認	「安全管理規程」4		

各部門で取り扱う個人情報について、リスク分析した結果の対策＝規程について監査を実施するため、実務的で、効率的な監査を実施することができます。
他の「監査チェックリスト」は、被監査部門が抱えるリスクに応じ、追加で監査を実施してください。

※　施設や設備は、部門にまたがるため、総務部や支部長などを対象に、「3726e_施設・設備の安全性チェックリスト」で監査します。　　（以下は e）の一部）

3.4.2.2 適正な取得	①あらたな個人情報を取得することとなった場合には、「同意書」を添付して、ＰＭＳ管理責任者の承認を得ているか。	施設安全	「個人情報取扱申請書」
	②監視カメラによって社員および来訪者を録画している場合は、「監視カメラ設置」パネルを掲示しているか。	施設安全	目視

※　全社の基盤としての情報システムがある場合は、f)「3726_情報システム運用の安全性チェックリスト」によって、システム運用部門の責任者を対象に監査します。　（以下は f）の一部）

不正アクセス防止	①ネットワークのログインＩＤは、一人ずつ個別に与えているか。	SYS	「ＩＤ管理表」		
	②人事異動・退職者が発生した際に、速やかにＩＤを削除しているか。	SYS	目視		
	③パスワードは、英数字混合で８文字以上に制限しているか。	SYS	目視		
	④ネットワークのログインパスワードは、６か月以内に（強制的に）パスワードを変更しているか。	SYS	「ＩＤ管理台帳」		
	⑤一般利用者のＰＣログインは、ユーザ権限としているか。	SYS	目視		

※　サンプルのチェックリストは、取り扱う個人情報に応じて、不要な行を削除するなど、整理してご使用になってください。

20.2.5　運用監査の評価

監査担当者は、ヒアリングや目視した事実に基づき、チェックリストに以下の評価を記入します。

	評価	記述	状況	是正処置
a)	適合	○	問題なし	不要
b)	観察事項	○’	直ちに改善され、再発はしないと評価できる状況	不要
c)	不適合	×	是正しなければ、本人の権利を侵害し、企業の存続に係わるリスクとなる状況	必要

確認結果欄には、確認した記録（エビデンス）の名称、目視したモノやヒアリング内容を明記し、不適合があれば、　“～を実施していない”、“～を記録していない”　など、具体的に記入します。

準備した監査項目のすべてについて、監査結果を記入した後、
チェックリストの１ページ目の「【不適合】の概観」欄に、被監査部門ごとに特徴的な問題点や事情について記述し、代表者が一見してその部門の状況が理解できるようにします。
監査の終了時に「講評会」を実施し、被監査部門に不適合について納得が得られるよう説明し、確認印もしくはサインを得ます。

20.2.6　監査報告

監査責任者は、監査担当者から各部門の監査結果について「チェックリスト」によって報告を受け、結果のサマリーとして「3721 監査計画書（兼報告書）」を作成します。
「3721 監査計画書（兼報告書）」には、監査責任者が，ＰＭＳに対して改善すべき提言が盛り込まれている必要があります。

20.2.7　是正処置

監査において発見した不適合については、「3801 是正・予防処置報告書」を用いて、是正処置を実施します。監査責任者の責務は、不適合の報告迄で、是正処置の責任者は個人情報保護管理者となります。

次回は、「第 21 章　是正処置及び予防処置」をご紹介します。＞目次へ

個人情報保護監査研究会　http://www.saaj.or.jp/shibu/kojin.html　　以上

2014.01

支部報告　【　２０１３年　大分合同セミナーの開催報告について　】

会員番号　1035　梶屋　博史　（九州支部）
会員番号　0465　藤平　実　　（九州支部）

1. 開催日時、場所

日時:2013年11月9日(土)　13:30～17:30
場所:ホルトホール大分　410会議室
主催:大分県中小企業診断士協会、日本システム監査人協会
　　システム監査学会、大分IT経営推進センター、ITC大分　　計5団体
参加者:19名(懇親会参加:15名)

2. 議題、内容・感想

(1)開講挨拶(13:30)
　　一般社団法人　大分県中小企業診断士協会　　会長　清成　真一

(2)第一部:セミナー主催団体会員による発表(13:40～16:00)
　1)「WindowsXPサポート切れ問題と消費税増税対策」(13:40～14:45　)
　　講師:大分県中小企業診断士協会・大分IT経営推進センター　阿部芳久　氏

①　消費税増税対策
消費税改正のシステム対応に対し以下の考慮事項を提起。
●価格表示の問題
・総額表示義務の時限的撤廃(H29.3 末)
　一定の条件を満たした場合には、税抜きでの表示可能。
・移行期間の取扱い

●消費税転嫁の問題
・消費者との取引
・事業者間取引

●消費税引上げ経過措置
・製造請負等の消費税経過措置対応
　請負工事等の契約日、引渡し日を個別に管理し、
　適用税率を自動判定・手動選択できる仕組みが必要。
　(請負金額が変更した場合の考慮も)
・通信販売等の経過措置
　税率の確定時期、指定日前の取引、指定日以降の取引

② WindowsXPサポート切れ問題

2014 年 4 月 9 日サポート終了。

ある日突然、取引先に被害をあたえるかもしれない・・・・。

サポート終了に伴う、セキュリティのリスク。

（例. 知らず知らずの間に、攻撃型の操作で、取引先の PC を攻撃。）

⇒ 感想:

消費税改正への経過措置に関しては、出席者の関心も高く、”この場合はどうなるのですか”など具体的な内容の質問も飛び、一旦講師が宿題として預かり、その後に回答するとの場面もあった。

2)「情報セキュリティ　～多様な攻撃からどう守る？～」(15:00～16:05)

講師:日本システム監査人協会九州支部　福田啓二 氏

不正アクセスサイバー攻撃に関する事例などの紹介があった。

・フィッシング

・標的型攻撃／APT 攻撃

標的型攻撃の典型的手法:

フィッシングメール(偽装メール)＋不正プログラム

・水飲み場攻撃

・遠隔操作

例.遠隔操作ウィルス事件 2012

・ID／パスワード漏えい

・Web 改ざん

・Dos／DDoS 攻撃

・大規模サイバー攻撃

・個人情報保護／SNS

パーソナルデータ:位置情報や購買履歴など広く個人に関する情報。

SNS-facebook の注意点、企業としての SNS の利用。

⇒ 感想:

専門的な難しい事柄を、話題となった具体的な事例を織り交ぜることなどの工夫を行うことで、身近なこととして捉えることが出来る様ご説明いただいた。

(3)第二部:特別講演(16:20～17:25)

1)「第六次産業の現状について」＜仮＞

講師:株式会社みらい蔵　代表取締役　山村恵美子　氏

⇒ 講演内容、感想:

みらい蔵の山村社長のお話は、農業のIT化といっても、一番の問題はよい農作物を作るための「水資源」の確保だということが、さすが現場でお仕事されている人の意見だと勉強になりました。そのための国・役所との交渉も大変だという話も、なるほどと感じました。

また、農家の人(生産者)とITを含めた支援者(流通・小売業者も含む)がWin－Winの関係になるように努めることが大事だという言葉も印象に残りました。

(4)終講挨拶(17:25～17:30)

特定非営利活動法人　大分IT経営推進センター　副理事長　田邉　祐治

3. 所感:

今年の合同セミナーは、大分駅周辺総合整備の一環として設置されたばかりのまだ真新しい匂いがする“ホルトホール大分”にて行いました。

この会場において、今年も5団体の方々が集い、講師の方の話を熱心に聞き入り、またその後の懇親会においてもセミナー出席者の多くの方が参加され有意義な時間を持つことが出来ました。

これも、システム監査人協会の代表として福田さんが来ていただきご講演をしていただくなど、多くの方々のご協力によるものであり感謝申し上げます。

※ホルトホール大分 http://www.horutohall-oita.jp/

2014.01

支部報告【近畿支部　第１４２回定例研究会　報告】

会員番号 2419　馬場秀樹

1.　テーマ　:「データセンター運用におけるシステム監査の有用性」
2.　講師　　:西日本電信電話株式会社　京都支店　横山　雅義　氏
3.　開催日時:2013年11月15日（金）　18:30　～　20:30
4.　開催場所:大阪大学中之島センター　2階　講義室201
5.　講演概要:

講師が日頃のデータセンター誘致活動をする中で生じた疑問を、システム監査技術者の視点で、システム監査法制化プロジェクトの方々との意見交換を経てまとめた内容を、講演していただきました。

データセンター事業は、古くは一般的な建物に設置することが困難な、超重量、高発熱なメインフレームを設置・運用するための事業として存在していたが、ダウンサイジング、IT の高度化、インターネット拠点化、クラウド化等により、求められる機能、位置づけが大きく変化している。また、2011 年 3 月 11 日の東日本大震災以降、「セキュリティ対策」よりも「災害対策」としてのニーズが顕著になり、データセンター事業者の市場は増加傾向にある。

ユーザーから、「どの事業者のサービスも似たり寄ったりでどう選定すべきか分からない」という声を聴くことがある。事業者がどこまでの運用をリスクコントロールするのか分からない、何を拠り所に事業者・サービスを選定すべきなのか、結局は価格で決めるしかないのか、メニューの有無だけでは、真にサービスレベルを評価することができず、事業者がどこまで品質の担保、リスクコントロールしているのか明確でない。

データセンター業界で活用されている基準として、ISO9000、ISMS、ITSMS では、国際性はあるが、具体性客観性に弱く、建物設備運用やコネクティビティ運用に関する評価ができない。また、FISC、JDCC-FS では、適合証明により具体性客観性は確保できるが、コネクティビティ運用や情報システム運用に関する評価はできない。
現在のところ、データセンター事業を総合的に評価する基準は存在せず、ユーザーは担保に不足するサービス品質を、自らが評価し契約協議によって担保する必要がある。
データセンター事業者の評価基準を明確にし、その評価基準に基づいて、システム監査の査証により公にその品質の担保とすることで、ユーザーが客観的にデータセンターサービスを評価・選定することでき、消極的なコスト重視の潮流からサービス品質・技術の重視へと移行することも可能と考える。

6. 所感

データセンター業界で活用されている基準である、ISMS、ITSMS、JDCC-FS 等、それぞれだけでは不十分であり、データセンター事業を総合的に評価する基準を明確にして、システム監査を行うことが必要であること、データセンター事業者のサービス品質を評価する上で、どのような運用業務が存在するか、それに対応する要求事項を、建物設備運用、コネクティビティ運用、情報システム運用で整理され、データセンター事業の運用を業務とする私には、考えさせられる点があり、参考となりました。

以上

2014.01

注目情報（2013.12～2014.01）※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。

■特定個人情報保護委員会が正式に発足、委員長に堀部政男一橋大学名誉教授が就任

内閣府は、特定個人情報保護委員会が2014年1月1日に正式に発足し、委員長に堀部政男一橋大学名誉教授が就任したと発表した。特定個人情報保護委員会は、2016年の共通番号制度開始にともなう個人j情報保護のための第三者委員会として機能するもので、堀部氏は日本初のプライバシーコミッショナーになることになる。

詳細は、以下のホームページを参照されたい。

http://www.cao.go.jp/bangouseido/ppc/index.html

以下、内閣府のホームページにおける特定個人情報保護委員会の説明を掲載する。

特定個人情報保護委員会

特定個人情報保護委員会は、個人番号その他の特定個人情報の有用性に配慮しつつ、その適正な取扱いを確保するために必要な措置を講ずることを任務とする内閣府外局の第三者機関です。具体的には、特定個人情報の取扱いに関する監視・監督（立入調査、報告要求、指導、助言、勧告、命令等の権限の行使）、情報保護評価に関すること（指針の策定や評価書の承認）、特定個人情報の保護についての広報・啓発、これらの事務のために必要となる調査・研究及び国際協力等を行います。

■ＩＰＡ、昨年発生した情報セキュリティに関する事案で一般利用者に影響が高いもの４点を発表

IPA(独立行政法人 情報処理推進機構)は、1月7日に、昨年発生した情報セキュリティに関する事案の中で、金銭被害につながる可能性が高いという点で、特に一般利用者に影響が高いと考えられるもの4点を発表した。

(1)インターネットバンキング利用者を狙った不正送金
(2)過去の流行時の約 2 倍の件数に上るウェブ改ざん
(3)偽の警告画面を表示させ有償版の購入を促し、クレジットカード番号を入力させる
「偽セキュリティソフト」などの手口
(4)従来の対策では見抜くことが難しい、スマートフォンのワンクリック請求アプリ

このうち、(1)、(3)及び(4)は、1年前の“呼びかけ”で紹介したものと重複しているが、2012年に既に存在していたこれらの手口が、2013 年に入りさらに深化、巧妙化している。これら 4 点の手口について、下記のホームページで詳細に報告されているので、参照されたい。

https://www.ipa.go.jp/security/txt/2014/01outline.html

被害に遭わないためには、以下の対策を漏れなく行うことが必須であるが、それに加えて「自分は大丈夫だ」という思いこみを捨て、日ごろから用心することが重要である。

(1)セキュリティソフトを導入し、ウイルス定義ファイルを常に最新に保つ。
(2)パソコンやスマートフォンの OS（オペレーティングシステム）やアプリケーションソフトを最新版に更新する。
(3)年に一度は、普段使用しているメーカー以外の無料ツールでウイルスチェックを行う。

■ＪＰＣＥＲＴ／ＣＣ　　ＩＭＥ のクラウド関連機能に関するセキュリティ上の注意

最近の日本語入力に使われる IME には、学習履歴を複数の端末で共有するために外部サーバに履歴を保存したり、変換精度を向上させるために外部サーバと通信したりする、クラウド関連機能が実装されている製品があります。

このような機能を持つ IME は、一部のメーカー製 PC にプリインストールされていたり、他のアプリケーションと一緒にインストールされたりする場合があります。

クラウド関連機能は、ユーザーが端末で入力した内容を外部サーバへ送信することによって実現されていますが、ユーザーの意図しない通信を行っている事例が指摘されています。

IME のクラウド関連機能を使う場合は、入力内容が外部に送信される可能性があることを認識しておきましょう。

http://www.jpcert.or.jp/tips/2014/wr140101.html

（編集者注：IME (Input Method Editor)
日本語などのマルチバイト文字を入力するとき、
入力履歴を学習して変換効率を高める機能）

2014.01

【　協会主催イベント・セミナーのご案内　】

■月例研究会（東京）

第189回月例研究会	日時:2014 年 2 月 10 日(月)18:30～20:30　場所:機械振興会館　地下2階ホール	
	テーマ	個人情報保護法改正の方向性
	講師	慶應義塾大学　総合政策学部 教授　博士(法学)　新保　史生　氏
	講演骨子	内閣官房IT総合戦略本部のパーソナルデータに関する検討会において、「パーソナルデータの利活用に関する制度見直し方針」が示された。2013 年 6 月に決定された「世界最先端 IT 国家創造宣言」において、 IT・データの利活用がグローバル競争を勝ち抜く鍵であり、その戦略的な利活用により、新たな付加価値を創造するサービスや革新的な新産業・サービスの創出と全産業の成長を促進する社会を実現するものとされ、個人情報及びプライバシーの保護を前提としつつ、パーソナルデータの利活用に必要な制度の見直しを実施することに基づくものである。 平成 26 年 6 月までに、法改正の内容を大綱として取りまとめ、平成 27 年通常国会への個人情報保護法の改正案提出を目指すことが示された。見直し案において示された検討事項として、第三者機関(プライバシー・コミッショナー)の設置、個人が特定される可能性を低減した個人データの個人情報及びプライバシー保護への影響に留意した取扱い、国際的な調和を図るために必要な事項、プライバシー保護等に配慮した情報の利用・流通のために実現すべき事項について解説する。
	お申し込み	別途、HP でご案内します。

■公認システム監査人特別認定講習（東京・大阪）

開催中	公認システム監査人(CSA:Certified Systems Auditor)およびシステム監査人補(ASA:Associate Systems Auditor)の資格制度にもとづく認定条件を得るための講習です。	
	概要	・システム監査技術者試験と関連性のある各種資格の所有者については、特別認定制度に基づく本講習により、CSA・ASA 認定申請に必要な資格要件を満たすことができます。 ・特別認定制度の詳細はHPで公開しています(http://www.saaj.or.jp/csa/shosai.pdf)。
お申し込み		講習開催スケジュールと申し込み先をHPでご案内しています。 (http://www.saaj.or.jp/csa/tokuninannai.html)

■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」(非売品)

■システム監査サービス（全国）

申し込み常時受付中	情報システムの健康診断をお受けになりませんか？　実費のみのご負担でお手伝いいたします。	
	概要	・経験豊富な公認システム監査人が、皆様の情報システムの健康状態を診断・評価し、課題解決に向けてのアドバイスをいたします。これまでに多くの監査実績があり、システム監査サービスを受けられた会社等は、その監査結果を有効に活用されています。 ・システム監査の普及・啓発・促進を図る目的で実施しているものです。監査にかかる報酬は無償で、監査の実施に要した実費（通信交通費、調査費用、報告書作成費用等）のみお願いしております。 ・ご相談内容や監査でおうかがいした情報等は守秘します。
お問い合わせ		システム監査事例研究会主査　畠中（Email：PEC01546@nifty.com）

【　外部のイベント・セミナーのご案内（会報担当収集分）】

情報セキュリティ月間 キックオフ・シンポジウム開催	日時：2014 年 2 月 3 日（月）13：00～16：30	
	場所	一橋講堂　東京都千代田区一ツ橋 2-1-2 学術総合センター2 階
	テーマ	「日本の成長を支えるサイバーセキュリティ」
	概要	2月は情報セキュリティ月間です。内閣官房情報セキュリティセンター（NISC）では、キックオフ・シンポジウム「日本の成長を支えるサイバーセキュリティ」を、平成 26 年 2 月 3 日（月）に開催します。 活力あふれ国際競争力ある社会に向け、ますます注目され、広がりを見せるサイバー空間。その安全・安心な利活用のためには、しっかりとしたセキュリティ対策が不可欠です。あなたの組織の成長戦略に、サイバーセキュリティはきちんと位置付けられていますか？急速に普及したクラウドや SNS 等のサービスと、便利さの一方で生じる情報流出や事業中断のリスク。企業経営で見落としがちな、身近に潜む危険とその対策について解説・議論します。 情報セキュリティをご担当されている方はもちろん、企業や団体の経営に携わっている方など、皆様の積極的なご参加をお待ちしております。
	参加費	無料（事前登録制）
	お申し込み	詳細、申込み等は以下の HP をご覧ください。 情報セキュリティ月間 キックオフ・シンポジウム 「日本の成長を支えるサイバーセキュリティ」 http://www.nisc.go.jp/security-site/files/symposium_140203.pdf

2014.01

協会からのおしらせ　【　第 13 期通常総会のご案内　】

日本システム監査人協会(SAAJ)会員各位

■第 13 期通常総会のご案内

日本システム監査人協会の第 13 期通常総会を、下記の通り開催致します。

万障お繰り合わせの上ご出席をお願い申し上げます。

記

1. 日時:　2014 年 2 月 21 日(金)13 時 30 分 ～ 15 時
2. 場所:　東京都港区芝公園 3 丁目 5 番 8 号 機械振興会館　地下 3 階　研修 1 室

アクセス:http://www.jspmi.or.jp/kaigishitsu/access.html

3. 第 13 期通常総会議事

13:30 開　会

(1) 2013 年度　事業報告の件

(2) 2014 年度　事業計画の件

(3) 2014 年度　予算の件

(4) 理事選任の件

(5) その他

15:00 閉　会

(休　憩)

4. 特別講演及び研究会発表

15:20 開　場

(1) 特別講演

(2) 情報セキュリティ監査研究会発表

(3) 個人情報保護監査研究会発表

17:00 閉　場

5. 懇親会

17:30 開　場

20:00 閉　場

※懇親会場は機械振興会館地下 3 階の別室です。懇親会費は 3,000 円です。

※総会、懇親会の参加申込は 2014 年 1 月中旬より、協会ホームページにて受け付けます。

以上

2014.01

協会からのお知らせ【2014 年度 公認システム監査人及びシステム監査人補の更新手続きについて】

「2014年度　公認システム監査人及びシステム監査人補の更新手続きについて」が協会のホームページに掲載されています。2014年度に更新が必要な方は、更新手続きをお願いします。
掲載の概略は下記の通りですが、申請書等の資料のダウンロードなどは、ホームページからお願いします。
（http://www.saaj.or.jp/csa/csakoshin.html）

---------- 記 ----------

2014年1月1日
特定非営利活動法人日本システム監査人協会
公認システム監査人認定委員会

2014年度　公認システム監査人及びシステム監査人補の更新手続きについて（1）

特定非営利活動法人日本システム監査人協会（以下、当協会という。）は、公認システム監査人認定制度（2002年2月25日制定）（以下、当制度という。）及び継続教育要項（2004年10月13日制定）に基づき、「公認システム監査人(Certified Systems Auditor：CSA)」及び「システム監査人補(Associate Systems Auditor：ASA)」の認定期限が2013年12月31日（暫定有効期間2014年2月28日）で満了となる認定者について、認定の更新を行います。

更新申請書等の資料の入手方法は、以下のとおりです。

＜資料の入手方法＞
個人情報の取扱いについて、「同意する」を押した後に、以下が表示。

公認システム監査人及びシステム監査人補の更新手続きについて（2）

（1）「認定資格更新申請手続」の　ダウンロード：PDF 形式
（2）更新申請書等様式一式のダウンロード
「認定資格更新申請書」（様式1）：Word 形式
「継続教育実績申告書」（様式2）：Word 形式
（3）「CSA／ASA認定資格者の更新申請時期」
http://www.saaj.or.jp/csa/keizoku.html
（4）「継続教育要項」の参照
http://www.saaj.or.jp/csa/2nen_koushin.html
（5）「公認システム監査人認定制度」のダウンロード：PDF 形式

以上

2014.01

協会からのおしらせ　【　事務局からのお願い　】

日本システム監査人協会(SAAJ)会員各位

■会費納付のお願い

平素は協会の運営にご協力いただきまして誠にありがとうございます。

2014 年度会費の請求書を送付いたしますので、ご納付の方よろしくお願い致します。

なお、会費の未納が続きますと協会の規定により会員資格を継続できないことになります。協会の趣旨をご理解の上、ご対応よろしくお願い致します。

＜金額＞　2014 年度会費　　￥10,000－　　(年会費は、消費税非課税です。)

＜払込期限＞2014 年 3 月 31 日

＜振込先＞　郵便振替口座:00110-5-352357

加入者名:日本システム監査人協会事務局

銀行振込口座:みずほ銀行八重洲口支店(普通)2258882

口座人名:特定非営利活動法人日本システム監査人協会

トクヒ)ニホンシステムカンサニンキヨウカイ

※銀行振込の際は、≪会員№≫4桁の数字を氏名の前に付けて下さいますようお願い致します。

(会員番号が付けられない場合は、メールまたは FAX で振込内容をお知らせください。)

■ご寄附のお願い

協会では、運営基盤のより一層の改善を図りたく、一口 3,000 円のご寄附をお願い申し上げます。ご寄附は、協会会費に合わせてお振込みいただければ、会費とは別に寄附金の取扱いにさせていただきます。

協会活動の改善のため、何とぞご協力をお願い致します。

＜2014 年度ご寄附(一口)＞￥3,000-　　ご寄附は、何口でも結構でございます。

＜振込先＞　※ご寄附は、協会会費に合わせてお振込みいただければ幸いです。

ご寄附についてのお問合せは、下記宛にご連絡いただきますよう、お願い致します。

協会事務局メール　jimu@saaj.jp　電話　03-3666-6341　FAX 03-3666-6342

※寄附者名簿は、法令に基づき所轄庁の東京都へ報告させていただきます。

※また、御礼のため氏名等を会報等に掲載することがあります。会報掲載を拒否される場合は、事務局宛に事前にお申し出ください。

新たに会員になられた方々へ

Welcome

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/annai/index.html
・会員規定にも目を通しておいてください。 http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・みなさまの情報の変更方法です。 http://www.saaj.or.jp/members/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
　みなさま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

・みなさま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。

2014.01

【　協会行事一覧　】

2013 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
9 月	12 日 会計:予算実績中間報告 12 日 事務局:会費未納状況まとめ	7 日 事例研:「課題解決セミナー」 18 日 第 185 回月例研究会 24 日 CSA フォーラム	21-22 日 近畿支部:「システム監査体験セミナー(実践編)」
10 月	10 日 会計:9 月末予算実績対比表の理事会報告	22 日 第 186 回月例研究会	
11 月	14 日 理事会:次期会長選任 14 日 会計:予算申請提出依頼(11/30〆切) 16 日 事務局:2014 年度役員改選準備開始 20 日 事務局:会費未納者除名通知発送 30 日 会計:2014 年度予算申請提出期限	16 日 認定委員会:CSA 面接 18 日 第 187 回月例研究会 20 日 認定委員会:CSA・ASA 更新手続案内〔申請期間 1/1～1/31〕 21 日 CSA フォーラム 28 日 第 188 回月例研究会 28 日 認定委員会:CSA 面接結果通知	16 日 近畿支部:「事例に学ぶシステム監査の基本と応用」 23 日 北信越支部:西日本支部合同研究会 28-29 日 東北支部:支部設立 10 周年記念システム監査実践セミナー
12 月	1日 会計:2014 年度予算案策定 12 日 理事会:2014 年度予算案、会費未納者除名承認 13 日 会計:支部会計報告依頼(1/11〆切) 14 日 事務局:第 13 期通常総会資料提出依頼(1/8〆切) 20 日 会計:2013 年度経費提出期限 27 日 事務局:2014 年度会費請求書・寄附願い発送準備〔1月1日付〕	7 日 事例研:「課題解決セミナー」 9 日 認定委員会:更新手続きのご案内メール発信 11 日 CSA 認定証発送	6 日 北海道支部:支部総会 14 日 東北支部:支部総会・支部設立 10 周年記念講演会
2014 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	10 日 通常総会開催案内掲示・メール配信 10 日 役員改選公示 11 日 会計:支部会計報告期限 15 日 事務局:総会資料(完) 20 日 会計:2013 年度決算案 25 日 会計:2013 年度会計監査 31 日 償却資産税・消費税申告	認定委員会:CSA・ASA 更新申請受付〔申請期間 1/1～1/31〕 20 日 認定委員会:春期公認システム監査人募集　案内 〔申請期間 2/1～3/31〕 (CSA フォーラム)予定	中部・近畿支部会計監査 17 日 近畿支部:支部総会
2 月	6 日 理事会:通常総会議案承認 **21日 通常総会 (特別講演)** 新役員	認定委員会:CSA・ASA 春期募集(2/1～3/31) 10 日 第 189 回月例研究会	
3 月	1 日 事務局:法務局登記、東京都への事業報告、変更届提出	(CSA フォーラム)予定	
4 月	1 日 認定 NPO 法人申請準備開始	認定委員会:新規 CSA/ASA 書類審査	20 日:2014 年春期情報技術者試験

※注　定例行事予定の一部は省略。

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

2014 年度年間テーマは、「○○○のためのシステム監査」、2 月号から 4 月号までの四半期テーマは、「公(おおやけ)のためのシステム監査」です。皆様から様々なご意見ご提案を会報に寄せていただき、会報がシステム監査を活性化する議論の場となれば幸いです。

□■ 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を利用してください。会報サイトからダウンロードできます)
2. 会員投稿 (Word の投稿用テンプレートを利用してください)
3. 会報投稿論文 (論文投稿規程があります)

いつでも募集しております。 気楽に投稿ください。 特に新しく会員となられた方(個人、法人)は、システム監査への想いやこれまで活動されてきた内容で、システム監査にとどまらず、IT 化社会の健全な発展を応援できるような内容であれば歓迎いたします。

次の投稿用アドレスに、テキスト文章を直接送信、または Word ファイルで添付していただくだけです。

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)

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。

2014.01

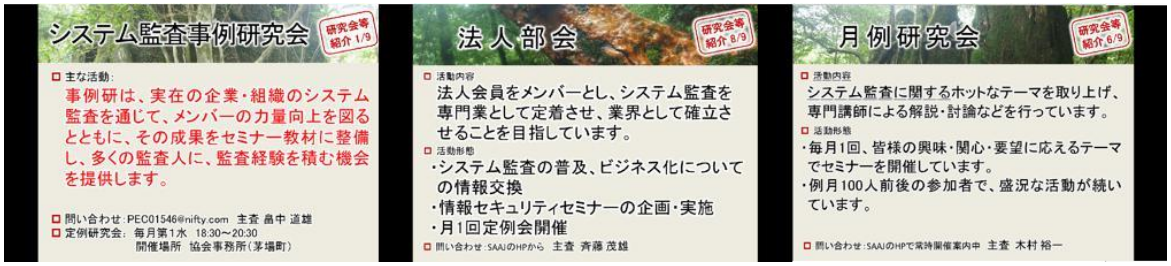
【 2014 年の会報サイト　ビジュアル化について 】

すでにお気づきの方も多いと思いますが、会報サイトのトップ画面の印象を大きく変えました。

表示例1

表示例 2

表示例 3



現状では、この3つのパターンをランダムに表示するようにしています。
気分を和らげるための季節の草花や自然の風景も、組み合わせることで、サイトの品位もアップします。

昨年より開始したプレゼンツールの Prezi も、写真をベースとしています。
興味深い写真を背景にすると見栄えもよく、注目してしまいます。
SAAJ の活動に参加したい、覗いてみたいと思うような全国支部の活動を紹介する写真や掲示も、価値が高いと思われます。たとえば上記の画像は、月例研究会の開催前に紹介している PR 画像です。

腕をみがいているカメラ愛好家、いつもデジカメを持ち歩いて、スクープ写真を保存しているあなた！
ぜひ、会報サイトのトップ画面を飾りませんか。

ということで、会報サイト用写真、画像を募集しています。ただし、画質がよすぎる(高解像度)場合には、サイトの動作(画像表示)が遅くなるので、画素を調整して表示させていただく場合があります。

以上　会報サイト管理人　竹下和孝

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)

会報編集担当の役割を変更しました。
より良い会報作りに邁進したいと考えます。
今後とも、どうぞよろしくお願い致します。(会報主査　藤澤)

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

■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、会員期間中の会員へ自動配布されます。
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。
【送付停止】 http://www.skansanin.com/saaj/

■□■SAAJ会報担当━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
編集：藤澤 博、安部 晃生、越野 雅晴、桜井 由美子、仲 厚吉、中山 孝明、藤野 明夫
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）
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━