特定非営利活動法人
日本システム監査人協会報

2014年4月号
No 157

No. 157（2014年4月号）＜3月20日発行＞

新入生、新入社員・・・

街には、新しい息吹が生まれています。

ＳＡＡＪも、新たな体制で、

新風を吹かせていきます。

ヤマガラ（柴田幸一会員撮影）

1. めだか …… 3
【公（おおやけ）と親業（おやぎょう）】
【主客転倒と無縁のシステム監査（公(おおやけ)のためのシステム監査)】
【システム監査人としての覚悟（公(おおやけ)のためのシステム監査)】

2. 投稿 …… 6
【東日本大震災から3年】
【エッセイ:目目連】
【システム監査と税制改革(3)　「担税力に応じた新税」に関するシステム監査上の留意点】

3. 総会特集 …… 16
【会長メッセージ　2014年度活動方針について】
【第13期通常総会特別講演を聴講して】
【第13期通常総会報告】
【新役員体制】
【新任理事・新任監事のご紹介】
【2013年度会報アワード】

4. 本部報告 …… 27
【第189回　月例研究会（2014年2月開催)】
【情報セキュリティ監査研究会だより その12 ― プライバシー・バイ・デザイン　第7回】(連載)
【システム監査基準研究会】
【「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23章】

5. 支部報告 …… 43
【近畿支部第143回定例研究会報告(ISACA大阪支部共催)】

6. 注目情報 …… 45

7. セミナー開催案内 …… 46
【協会主催イベント・セミナーのご案内】
【外部のイベント・セミナーのご案内】

8. お知らせ 48
【「システム監査を知るための小冊子」発行について】
【2014年度春期　公認システム監査人及びシステム監査人補の募集】
【新たに会員になられた方々へ】
【協会行事一覧】

9. 会報編集部からのお知らせ 53
【会報テーマについて 、 会報記事への直接投稿(コメント)の方法、 投稿記事募集 】

2014.03

めだか　【　公（おおやけ）と親業（おやぎょう）　】

筆者は、公（おおやけ）のための情報システムにはシステム監査が求められるべきだと思う。また、今後、当協会がその方向で社会に働きかけていくことが必要であるとも思う。

公（おおやけ）のための情報システムとは、公共機関が取り扱う情報システムと考えて良いといえる。ウィキペディアによれは、公共機関とは、公共的な機関一般を指す概念である。具体的には、政府及び独立行政法人、特殊法人等の政府関係機関、地方公共団体及びその関係機関など行政機関全体、及び

新聞社、放送局などの報道機関、 鉄道、空港などの交通機関、
郵便局、運輸業などの輸送機関、 電気通信事業者などの通信機関、
電力会社、ガス会社、水道局などのライフライン、 病院、診療所などの医療機関、
大学、学校などの教育機関、 銀行、信用金庫などの金融機関、

などを総称した概念であるという。なお、事象により、公共機関の範囲は異なる、とある。

公（おおやけ）に対比される言葉として私（わたくし）がある。私（わたくし）が抱える課題も、社会的に解決されるべきものは公（おおやけ）の課題になりうる。今回は、「親業（おやぎょう） PET: Parent Effectiveness Training」を採り上げる。システム監査人は、「親業」のトレーニングが社会的に求められるものとして認識しておくと良いと思う。友人から、「あっ、こう言えばいいのか！ ゴードン博士の親になるための16の方法 - 家族をつなぐコミュニケーション」という本を贈呈され、一読して紹介したいと思った次第である。以下、本文から引用する。

・家族は社会の最小単位ですが、家族の形もシングルマザー、シングルファーザー、そして再婚家庭（ステップファミリー）と多様になっています。アメリカでは再婚家庭が家族形態の主流になるほど増えています。
・「助けて」の一言が言えなくて自殺してしまう人、「苦しい」の一言が言えなくて心を病んでしまう人、「やめて」の一言が言えなくていじめに苦しむ子どもなどなど、家族にさえ心の内を打ち明けることができない人が溢れています。
・血のつながりがあるにせよ、ないにせよ、夫婦、親子がさまざまな困難を乗り越え、協力し、信頼し合える関係を築くためには意識的に家族を構成する力「家族力」が必要な時代になってきました。「家族力」を身につける鍵は、ずばり、自分の思いを語り、相手の話に耳を傾け、問題が起きれば家族でその解決策を話し合うことができるという、家族一人一人のコミュニケーション能力を上げることです。

コミュニケーション能力を上げる16の方法の第1番目は、自分の気持ちを「行動の四角形」整理する、即ち、四角形に受容線を横に引き、上半分に受容できること、下半分に受容できないことに整理することから始まる。

（空心菜）

〔参考〕:「ゴードン博士の親になるための16の方法」 瀬川文子 著　親業訓練協会 監修　（合同出版）

（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。）

2014.03

めだか【　主客転倒と無縁のシステム監査　（ 公（おおやけ） のためのシステム監査）　】

主客転倒:「主人と客人の立場が逆転すること。転じて、重要なものと軽いものが逆さまになること。」
この言葉には、似た用例が数多くある。「主従逆転」、「主客逆転」、「本末転倒」、「主客混同」、「冠履転倒（かんりてんとう）」、「釈根灌枝（しゃくこんかんし）」、「舎本逐末（しゃほんちくまつ）」など。
これらは、物事が入れ替わってしまうことや、逆に取り扱ったりすることを、様々なシーンやシチュエーションに例えて表現している。個人のことでも飼い犬との主従関係の逆転など思い当たることも少なくないだろう。

情報システムの分野にも主客転倒は多くの場面で見られる。例えば、

・「情報と人間」→情報は、人間がその活動において必要なものを判断取捨し、利活用してきたが、今や、人間は情報を扱うどころか情報に右往左往させられている。情報の海で溺れている。
・「IT 部門とユーザ部門」→IT 部門は、情報システムを企画・開発・統括し、名実ともに情報システムの主役であったが、今や、従来ユーザ部と言われていた利用部門が情報システムオーナーである。
・「システム構築のリーダシップ」→自社業務のシステム構築について、自社がリーダシップを取れなくなって久しい。かなり以前から IT ベンダーに頼り、巨額の投資案件を外部に委ねる状況に移っている。

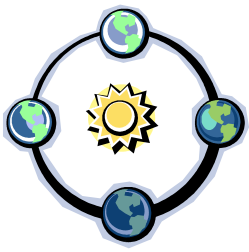
システム監査について主客転倒はあるだろうか、考えてみる。

システム監査技術者試験制度が発足した、今から四半世紀前頃の情報システムは、事務処理の機械化を電子計算課のような組織が担うことが多く、当時のシステム監査は、そのような IT 環境や開発体制のシステムリスクを対象にしていた。その後の今日までの情報システムの変遷は、ここで記すまでもなく、環境も、利用形態も、リスクの質も、それらすべての変貌が計測不能ともいえる速度で進んでいる。ドックイヤーという用語は IT の陳腐化スピードを例えたものだが、今や、その用語自体が陳腐化してしまった。

このような状況下において、システム監査は、自分の縄張りであるシステムリスクを相変わらず確実にグリップし続けているだろうか。目が届く範囲にあった可愛いシステムリスクが、いつの間にか得体のしれないリスクに変貌してしまって、そのリスクの掌中でシステム監査が踊らされていることはないだろうか。それは取り越し苦労である。システム監査とシステムリスクの主客は逆転してはいない。

「公（おおやけ）のシステム」、つまり世の中全体を動かしている情報システムは、明らかに巨大で茫漠としているが、それと向き合う「公（おおやけ）のためのシステム監査」は、常に主人の立場で毅然としていなければならない。客人または使用人である情報システムを常にコントロールしている存在である。

テーマである「公（おおやけ）のためのシステム監査」とは、そのような立場が課せられたものだと思う。システム監査においては主客転倒とは無縁であり、それを、太陽たるシステム監査と地球たる情報システムに例えるのは如何であろうか。



（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。）

2014.03

めだか　【　システム監査人としての覚悟（公（おおやけ）のためのシステム監査）　】

われわれシステム監査に携わる者にとって、嬉しくなるような調査結果がある。

システム監査は必要と思いますか。　⇒　（回答）	思う	82.0%
	思わない	8.2%
	わからない	9.3%
	無記入	0.5%

しかし、上記調査は最近の調査ではなく、今から40年ほど前の1975年に㈶日本情報開発協会が労働組合に対してアンケート(注)したものである。当時は、銀行オンラインシステム等、基幹業務のオンライン化が進められていた頃であり、通商産業省による「システム監査基準」が公表される10年も前の話である。こうした時代に、「システム監査は必要」との回答が8割を超えていることは、大きな驚きである。

当時、システム監査はどのように考えられていたのか？　㈶日本情報開発協会の1975年度調査研究「わが国におけるシステム監査のあり方」では、システム監査について、次のように述べている。

「システム監査は、情報化のメリット追求と同時に、情報処理の弊害を事前に除去しようとする問題先取り型の監査である。従来、情報化については、合理性追求のみで、デメリットについては野放しとの批判があり、こうしたことからも、情報処理に対する監査の必要性が出てきた。」

また、1975年11月7日の日本経済新聞では、「システム監査の徹底を」と題した社説を掲載し、システム監査の必要性を訴えている。

このように、当時は、これからの情報化社会の進展に向けて、システム監査への期待も大きかったようだ。

翻って、現在のシステム監査の状況を見ると、どうだろうか？　当時の期待に応えてきたといえるだろうか？

現在、システム監査の必要性について、労働組合でなくとも、企業にしろ、従業員にしろ、一般消費者にしろ、その8割が「必要」と回答してくれるかというと、甚だ心許ない。

例えば、お客様に多大な迷惑をかけるような大規模なシステム障害が発生した場合には、経営者やシステム部門に対しては、大きな非難が起こる。しかし、システム部門を監査する立場にある監査部門については、責任を問う声はあまり聞かれない。しかし、よく考えてみると、これは、システム監査に対して、社会ではそれほどの期待はしていないということの裏返しではないか？

私個人としては、システム監査は、大規模障害やセキュリティ事故・事件等の発生を防止するために、それなりの役割を果たしてきたとの自負はあるものの、その効果・功績を具体的に示すことは難しい。だからといって、システム監査についての社会の理解が拡がらないと嘆いていても、始まらない。

システム監査に対する社会の期待・信頼を高めていこうとするならば、上述のような大規模障害が発生した場合には、監査部門も、なぜ大規模障害を防げなかったのかを真摯に分析・反省し、反省すべき点は公表・謝罪するくらいの覚悟も要る。「公のためのシステム監査」には、そうした責任ある姿勢が必要であろう。

社会から「期待」されるシステム監査であるためには、期待に応えるための「責任」も伴うことを忘れてはならない。「監査はラストリゾート（最後の砦）である」との覚悟をもって、これからの監査にあたっていきたい。

（注）出典：日本情報開発協会（現.日本情報経済社会推進協会）「システム監査委員会設置について（趣旨説明書）」（1975年7月）

（やじろべえ）

（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。）

2014.03

投稿【　東日本大震災から３年　】

会員番号　1709　荒町弘　（近畿支部・BCP研究プロジェクト　主査）

1．東日本大震災から3年

2014年3月11日、東日本大震災から3年が経過しました。被災地では多数の被害にあわれた方や行方不明となられた方、今も住んでいた土地を離れての生活を送っている方がおられます。あらためて、東日本大震災により被害を受けられた方々にお見舞い申し上げますとともに、今後の更なる復興を願っております。

2．被災から復興、復旧、そして強い国づくりへ

東日本大震災は私たちから多くの物を奪い去りました。2万人近くの尊い命、被災地で暮らす人々の生活環境とインフラ、そして経済の基盤となる企業の活動。企業においては社屋自体の流失により、事業活動の歴史ともいえる記録データごと奪われてしまった例もあります。地方公共団体では住民基本台帳データの流失により災害発生時の安否確認や被害状況の確認に多大なる影響を及ぼしました。

東日本大震災後は事業継続に対する取り組みの重要性が一層クローズアップされ、都道府県や地方自治体での事業継続計画（BCP）の策定、そして防災計画と整合性を持ったIT－BCPの策定も合わせて進められています。また、都道府県が率先して地域の民間企業等の事業者におけるBCP策定のためのガイドライン整備やBCP策定支援、企業経営者への意識付けセミナー開催など、積極的な取組が実施されています。

法制面では災害が発生した場合における被害の最小化及びその迅速な回復を図ること等を基本理念とする「災害対策基本法等の一部改正」が実施されました。この中では、災害発生時または災害発生のおそれがある場合において、生命又は身体を災害から保護するために必要があると認める場合は、市町村長は避難行動要支援者の名簿情報を避難支援に必要な範囲で本人の同意を得ることなく支援機関等に提供することを可能とするなど、危機管理段階における個人情報の取り扱いについても柔軟な対応ができるようになりました。

3．システム利用形態の変化と新たな課題

東日本大震災後、企業や地方公共団体を中心とする災害に強いITの構築に向けた動きは加速されました。

ITの利用においては、「所有するIT」から「利用するIT」への変化、いわゆるクラウドコンピューティングの採用やクラウドサービスの積極的な利用が始まりました。また、データの保全というにおいては自事業所内のデータ管理に加えてデータセンター等の外部機関におけるバックアップサービスの採用も増加傾向にあります。更には、モバイルデバイスの活用や、テレワークツールの導入等も普及しつつあります。

これらは間違いなく「災害に強いIT」を実現するための有効な選択肢ではありますが、一方で従来型のIT運用管理ではカバーしきれない要素も増えています。複雑化するシステム利用形態や運用は新たなITリスクの原因にもなり得るため、今後一層、セキュリティやIT統制監査が必要となると考えます。

来年、2015年1月17日は、阪神淡路大震災から20年となります。IT基盤の上で経済活動を行う私たちにとって、「災害に強いIT」の実現は共通の課題であり、その課題に対する解決策としての万能薬というものは存在しないと思います。だからこそ、災害に対する意識を常に持ち、万が一災害が発生した場合にも、最善を尽くせる組織作りや人材育成、そして安全なIT利活用環境構築と維持への取組を続ける必要があると考えます。

（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。）

2014.03

投稿【エッセイ】目目連

会員番号 0707 神尾博

江戸時代の絵師・鳥山石燕は画集「今昔百鬼拾遺」で、ことわざ「壁に耳あり障子に目あり」を、「目目連（もくもくれん）」という妖怪として見事に視覚化している。荒廃した家屋の障子の格子毎に、2つの目が現れるといった姿で描かれており、薄気味悪くもありユーモラスでもある。

現代では、もはや画伯の時代のような絵空事ではなく、建屋や構造物、設備にまでインターネット経由でのセンサによる監視、いわゆるセンサネットワークの利用拡大が進んでいる。M2M（Machine to Machine）は、新しい概念というわけではない。FA化やCIM化の時代から、自動機やロボット等とコンピュータとのデータ連携が工場で浸透していた。ところが近年のセンシング技術の発達や通信モジュールの小型化・省電力化・量産化により、活用領域が急激に多様化してきている。

エレベーターは公衆回線を通じ、運行状態や故障停止等の情報をメンテナンス会社に送信し、状況に応じて保守作業員が遠隔操作や現地出動を行っている。また橋梁や高架道路に振動・歪みセンサを配置して、老朽化を調べるヘルスモニタリング技術も、社会インフラ保守の効率化の切り札として注目されている。DONETという地震・津波観測監視システムは、熊野灘の海底に水圧・温度・震度センサを設置し、観測データをリアルタイムで収集している。地区毎の細やかな津波到達の予測システムも開発中で、あの2011.3.11のような震災が再来しても、被害の縮小に役立つことが期待されている。

これらは社会や生活に有益な活用例だが、一方ではうろんな面々も存在する。某国製のスマートテレビが視聴情報を外部へ送信していたことが、2013年11月に英国人ブロガーの調査によって発覚した。設定を無効しても止まらなかったという。また自販機やデジタルサイネージが、当人の知らぬうちに顔データを読み取り、年齢や性別を判断し、オススメ商品や表示メッセージを変えるといった仕組も出回り始めた。JR大阪駅ビルでは、通行人の顔をカメラで撮影し追跡する実験が、2014年4月に始まる可能性もある。こうなると「Big Data」ならぬ「Bad Delicacy」とも批判されかねない。

他方ではプライバシーに配慮した工夫も考案されている。たとえば床に敷いたシートから発信する微弱電波の変化によって、足跡の形状や動きを検出する技術が2013年11月に発表された。人の存在や状態は手に取るように分かるが、特定人物の識別につながるデータは取得されないそうだ。科学技術は価値中立である。センサノード自体がよこしまな訳ではなく、黒幕はそれを操る人心の中に存在するのである。そもそも壁や障子のような間仕切りは、元々は「魔除切り」からきた言葉だという。魔物を呼び込むような真逆の所業などは、ご免こうむりたいものだ。

（このエッセイは、投稿者の個人的な意見表明であり、SAAJ の公式見解ではありません。 画像は Wiki より著作権保護期間満了後のものを引用しています。）

2014.03

投稿【システム監査と税制改革(3)　「担税力に応じた新税」に関するシステム監査上の留意点】

会員番号　1566　田淵隆明　(近畿支部法制化研究会)

消費税への「軽減税率」については、様々な憶測が飛び交っていたが、去る 2 月 27 日、与党税制調査会において、「5 月からの論点整理」、「9 月からの制度設計」が決定した。昨年 12 月 13 日の与党税制改正大綱において与党合意したように、2014 年末(※2014 年度では無い)の与党税制改正大綱に制度設計が書き込まれることになっているが、このスケジュールならば十分間に合うスケジュールである。

※1. 3 月 5 日の報道のように、所得税の「世帯単位の課税」の検討など、直接税の分野でも多くの制度改正が検討されており、システム監査上の要注意点は多数出てくると思われる。

※2. 財界から要請の強い法人税率の引き下げの財源については、間接税で賄うということではなく、**繰越欠損金の損金算入期間の見直しや租税特別措置の縮小など、直接税の枠内での検討**になりそうである。システム監査の観点から言えば、「税額の計算式の変更」は消費税率の引き上げに匹敵する大きなテーマである。また、**繰越欠損金の損金算入期間の縮小は、個別会計上及び連結会計上の「繰延税金資産の回収可能性の評価」において重要な論点**となる。ここまで来ると、通常のシステム設計者では正しく対応しきれなくなることもあるので、皆様方におかれては適切な監査・助言をお願いしたいところである。

前回は現行の消費税法のシステム監査上の留意点について取り上げたが、今回は、昨年 12 月 13 日の「与党税制改正大綱」の策定の際に、検討に入ることが与党間で合意された「担税力に応じた新税」に係るシステム監査上の留意点について取り上げることとする。

§1. 制度設計の基本的考え方

この新税は消費税のような「多段階の課税」ではなく、1989 年までの物品税と同様に、最終段階(小売段階)だけの課税となる見込みである。これは、確実な転嫁が困難な帳簿方式が維持される以上、当然考慮するべき事項である。

しかし、間接税の中で「仮払消費税」(資産)と「仮受消費税」(負債)の相手先別勘定が 2 個必要な「消費税」と、「売掛金/未払物品税」型の仕訳を起こし、相手先別勘定が 1 個だけ必要な「物品税」が併用されるため、システム監査上の重要なテーマとなる。

特に、**「税込経理」の場合は、運用が煩雑になるため、消費税の本則課税に関しては「税抜経理」に統一すべき**である。現在、大半の本則課税事業者は「税抜経理」を採用しており、大きな混乱は発生しないと考えられる。また、税の滞納額の約半分は消費税である。事業者による滞納防止の観点からも、「本来、仮受消費税は収益の一部を構成しない」ことを明確にするために、本則課税においては「税込経理」の選択は廃止するべきである。

※IFRS では「税込経理」は禁止である(IAS18)。

「担税力に応じた新税」は 1989 年以前の「物品税」、「サービス税」、「通行税」等が基本になる。1989 年以降のライフスタイルの変化及び物価スライドを考慮すると、例えば次のような物品・サービスが対象になると思われる。

〔1〕物品税(§2 に示すような高級な物品)
〔2〕高額飲食税　(※これについては一部既定路線)
〔3〕通行税(グリーン車、グランクラス、船舶・航空機のファーストクラスなど)
〔4〕「サービス税」及び「リゾート税」
〔5〕「ギャンブル課税」
〔6〕「遊戯場税」(※一部報道の通り、パチンコの「換金税」の導入の検討も行われている)

前々回でもご紹介したように、この「担税力に応じた新税」については、システム監査技術者の力量の問われる重要なテーマが多々あると思われる。システム監査技術者・公認システム監査人の職域拡大にも資するものである。
また、契約書における印紙税法の適用厳格化も検討されているようである。

§2. 物品税

1989 年以降のライフスタイルの変化及び物価スライドを考慮すると、例えば次のような制度設計が考えられる。

(A)衣料品
(1)本体価格が 30 万円を超える絹織物の衣服の 30 万円を超える部分
(2)本体価格が 10 万円を超える絹織物以外の衣服(※1)(下記を除く)の 10 万円を超える部分
(3)本体価格が 1 万円を超える肌着、マフラー、ベスト(チョッキ)の 1 万円を超える部分
(4)本体価格が 1 万円を超える履物、手袋、靴下、足袋、組紐、扇子等の 1 万円を超える部分
(5)その他政令で定めるもの
※1.(2)の「衣服」には、毛皮、帯(絹織物を含む)、外套(コート)を含む。

(B)住居(※1)
(1)住居のうち、延床面積で相続税法上の特定小規模宅地の特例(＝240 平米)を超える部分
(2)本体価格が 5000 万円を超える住居の 5000 万円を超える部分
(3)本体価格が 100 万円を超える造園費用の 100 万円を超える部分
(4)本体価格が 100 万円を超える門扉の 100 万円を超える部分
(5)その他政令で定めるもの
※1. いわゆる豪邸に対する特別課税である。
※2. 個人で複数の住宅を保有する「別荘」についても検討が必要であるが、法令面の整備が必要。
※3. 土地については、大規模な土地取引であっても消費税は課されないが、不動産取得税などの課税が

行われる。しかし、投機目的の土地の転売等の取引について、何らかの間接税を課すべきとの議論もある。ただし、この件については論点の整理、法令面での整備が必要。

※4. 近年、リフォーム費用について施主と施工業者の間でのトラブルが頻発している。リフォーム費用の内訳の透明化についても、早急に対策が必要である。

(C) 車両運搬具(事業用及び官公庁用及び防衛・警察関係のものは除く)

(1) 本体価格が 500 万円を超える自動車の 500 万円を超える部分
(2) 本体価格が 100 万円を超える自動二輪車(原付自転車を含む) の 100 万円を超える部分
(3) 本体価格が 20 万円を超える電動アシスト機能付き自転車の 20 万円を超える部分
(4) 本体価格が 10 万円を超える(3)を除く自転車、及び、三輪車、一輪車の 10 万円を超える部分
(5) 本体価格が 500 万円を超える航空機(ヘリコプター、人力航空機を含む)の 500 万円を超える部分
(6) 本体価格が 500 万円を超える気球、飛行船、ハングライダー等の 500 万円を超える部分
(7) 本体価格が 500 万円を超える船舶の 500 万円を超える部分
(8) その他本体価格が 500 万円を超える車両運搬具の 500 万円を超える部分
(9) その他政令で定めるもの

(D) 家具・インテリア・家電・調度品など(事業用は除く)

(1) 本体価格が 100 万円を超えるキッチンの 100 万円を超える部分
(2) 本体価格が 50 万円を超える風呂設備の 50 万円を超える部分
(3) 本体価格が 30 万円を超えるタンス・鏡台等の家具の 30 万円を超える部分
(4) 本体価格が 30 万円を超える冷蔵庫の 30 万円を超える部分
(5) 本体価格が 20 万円を超えるテレビ(※1)、ビデオ(※1)エアコンの 20 万円を超える部分
(6) 本体価格が 20 万円を超えるベッドの 20 万円を超える部分
(7) 本体価格が 10 万円を超えるマッサージ・チェアの 10 万円を超える部分
(8) 本体価格が 10 万円を超える布団の 10 万円を超える部分
(9) 本体価格が 10 万円を超えるラジオ、音響機器、洗濯機・乾燥機、エアコン、空気清浄機、加湿器、炬燵、掃除機等、パソコン、携帯電話の家電製品の 10 万円を超える部分
(10) 本体価格が 5 万円を超える石油ストーブ等暖房機器の 5 万円を超える部分
(11) 本体価格が 5 万円を超える照明器具の 5 万円を超える部分
(12) 本体価格が 5 万円を超える敷物、カーテン等の 5 万円を超える部分
(13) 本体価格が 5 万円を超える調度品の 5 万円を超える部分
(14) 本体価格が 5 万円を超える机・椅子・ソファ等の 5 万円を超える部分
(15) 本体価格が 1 万円を超える枕・毛布・電気毛布・タオル・タオルケットの 1 万円を超える部分
(16) 本体価格が 1 万円を食器(皿、茶碗、グラス等)、及び、調理器具(鍋、やかん、包丁、ナイフ等)の 1 万円を超える部分
(17) 本体価格が 1 万円を壺・花瓶・灰皿等の 1 万円を超える部分
(18) その他政令で定めるもの

※1. 今後の我が国の産業競争力強化上、4K テレビ等は重要な商品となるので基準額を 20 万円とするのが

妥当である。

(E)宝飾品・装身具・鞄(かばん)・靴(くつ)・装飾品・置物・時計等
(1)本体価格が 30 万円を超える指環(※) の 30 万円を超える部分
(2)本体価格が 10 万円を超える指環以外の宝石、及び、装身具の 10 万円を超える部分
(3)本体価格が 10 万円を超える地金の 10 万円を超える部分
(4)本体価格が 5 万円を超える鞄の 5 万円を超える部分
(5)本体価格が 5 万円を超える靴・草履の 5 万円を超える部分
(6)本体価格が 10 万円を超える時計等の 10 万円を超える部分
(7)その他政令で定めるもの

(F)書画・絵巻物・骨董品・彫刻・オブジェ・美術品・古美術品・装飾品・置物・庭園用品(灯篭など)等
(1)本体価格が 10 万円を超える書画・絵巻物・骨董・彫刻・オブジェ・美術品・古美術品・装飾品・置物・庭園用品、その他美術品等の 10 万円を超える部分
(2)本体価格が 300 万円を超える仏壇・祭壇等の 300 万円を超える部分(宗教法人の備品を除く)
(3)本体価格が 300 万円を超える墓石等の 300 万円を超える部分
(4)本体価格が 10 万円を超える数珠・持仏・位牌・ロザリオ・十字架等の 10 万円を超える部分(宗教法人の備品を除く)
(5)その他政令で定めるもの

(G)趣味用品・玩具・模型・ゲーム用品・映像・音楽等
(1)本体価格が 10 万円を超える人形・玩具等の 10 万円を超える部分
(2)本体価格が 10 万円を超える模型の 10 万円を超える部分
(3)本体価格が 10 万円を超える将棋用品・囲碁用品・麻雀・ドミノ・カルタ・カードゲーム・ボードゲーム・ダーツ・ルーレット用品等の 10 万円を超える部分
(4)本体価格が 10 万円を超える茶道具の 10 万円を超える部分
(5)本体価格が 10 万円を超える華道具の 10 万円を超える部分
(6)本体価格が 10 万円を超える映像・音楽の 10 万円を超える部分
(7)本体価格が 10 万円を超えるゲーム・ソフトウェアの 10 万円を超える部分
(8)その他政令で定めるもの

(H)スポーツ用品(学校教育(クラブ活動も含む)用の備品は除く)・釣り具等
(1)本体価格が 10 万円を超えるものの 10 万円を超える部分
(2)その他政令で定めるもの

(I)楽器(学校教育(クラブ活動も含む)用の備品は除く)
(1)本体価格が 20 万円を超えるものの 20 万円を超える部分
(2)その他政令で定めるもの

(J)動植物
(1)本体価格が 10 万円を超える動植物の 10 万円を超える部分
(2)その他政令で定めるもの
※ここでは、珍獣、高級魚、観賞用爬虫類、高額な植物・花・果実等が想定される。

(K)その他
(1)本体価格が 300 万円を超える冠婚葬祭費用の内、300 万円を超える部分
(2)本体価格が 10 万円を超える猟銃等の銃火器の 10 万円を超える部分
(3)本体価格が 10 万円を超える和弓、洋弓の 10 万円を超える部分
(4)本体価格が日本刀、甲冑等の武具の 10 万円を超える部分
(5)冠婚葬祭式場、写真館等における、本体価格が 10 万円を貸衣装及び着付け料の 10 万円を超える部分(上記の冠婚葬祭費用に含まれる場合を除く)
(6)本体価格が 3 万円を超える贈答用の花輪の 3 万円を超える部分
(7)冠婚葬祭式場、写真館等における、本体価格が 1 万円を写真(1 枚単位)の 1 万円を超える部分
(8)その他政令で定めるもの

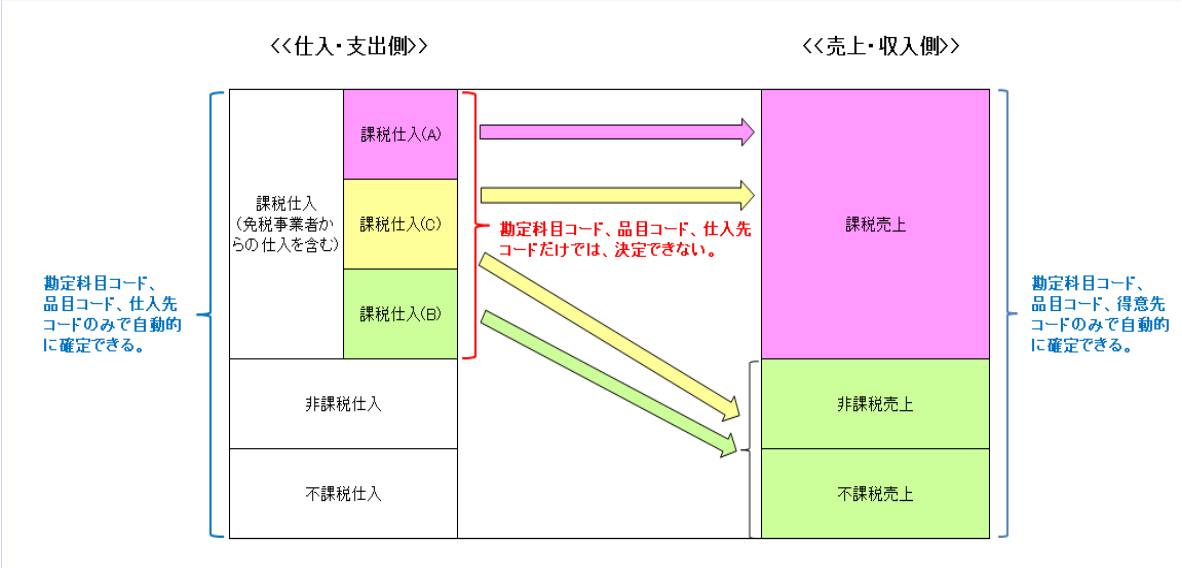
※他の税については次回以降取り上げることとし、以下は、先日の SAAJ 総会後に、複数の方々から、お問合せを頂いた件について取り上げることとする。

§3.　前回§2 の補足(個別対応方式と一括比例配分方式の相違)

前回の§2 の〔設例 1〕で指摘したように、複数税率が導入されても現行の帳簿方式(請求書等保存方式)は維持される見込みとなった。読者の方々は、本則課税の場合、「個別対応方式」と「一括比例配分方式」では納税額に大きな差異が発生することに驚かれた方々も多いと思われる。その「有利選択」は経営者にとって見逃すことのできない大きな問題である。我々「システム監査技術者」や「公認システム監査人」もシステム・コンサルタントとしての立場を求められることが少なくないが、その場合は重要なテーマとなり得る。

また、そのシステム化においては、「課税売上割合」の計算式の設定が不完全であったり、その基礎となる「非課税」と「不課税」の混同や誤謬が多く、一般のシステム設計者や SE では対応しきれていない場合が少なくない。一部には「税理士に任せておけばよい」という呑気な意見もあるが、システムに明るい税理士はまだまだ少数派であり、　ユーザの経理担当者と税理士だけに任せておくと、システムの運用設計も含めた適切な対応ができない場合も散見される。皆様方におかれては適切な監査・助言をお願いしたいところである。

また、「個別対応方式」を採用した場合には「仮払消費税」の 3 区分が必要となるが、そのためには「課税仕入」等の 3 分割も必要となるが、これは一般に非常に煩雑であり、一般には勘定科目コード、品目コード、仕入先コードだけでは、自動的に区分することは不可能である。



※上記の「課税仕入等」の 3 分割を行う場合、会計上の仕入だけではなく、固定資産の購入も含まれる。そして、使用目的の転用を行った場合、納税額の調整が必要になる場合があることは言うまでもない。

§4.　前回の§3(病院の損税問題)の補足

前回の〔設例 2〕と〔設例 3〕を見て頂ければお分かりのように、病院の損税問題は非常な不条理である。人間用の CT スキャンに掛かる「仮払消費税」は控除対象外消費税として医療機関の自己負担となるのに対し、動物病院用の CT スキャンに掛かる「仮払消費税」は控除対象となる。今回の増税によって、この金額が 2 倍になろうとしている。これは、経営が逼迫している地方の公立病院等にとっては極めて重い負担であり、近未来において地域医療を支える重要な病院の経営破綻が多発するものと思われる。この問題の解決には、**①医療機器を身体障害者物品と同様に「非課税物品」とする、②税率 5%の軽減税率対象品とする**などが考えられると述べたが、**保険対象医療を「非課税」ではなく「免税」とすることも検討されている**(3 月 3 日の参議院予算委員会の動画等を参照)。

※一部には「保険対象医療を課税にするべき」という暴論も存在するが、これは本末転倒であり、高齢者や身体障害者や生活保護世帯にとっては、まさに「死刑宣告」に等しい。他のG 7 先進国ではあり得ないことである。国民皆保険制度の不備により、医療難民が大量に発生している米国でさえ、このような惨い課税はしていない。

次の設例を御覧頂きたい。初めに、病院の損税問題について、何もケアが無かった場合の設例を示す。

〔設例 1〕S 外科医院(本則課税事業者)は CT スキャンを税抜 1 億円で購入した。この場合の控除対象消費税額を求めよ。S 病院の**保険対象診療(非課税)は 80%**であり、保険外医療(課税)は 20%(税抜きベース)であるので、課税売上割合は 20%である。ここで、CT スキャンの消費税率は標準税率の 10%であるとする。また、税額控除は一括比例配分方式を用いるものとする。

まず、CT スキャン購入時の会計上の仕訳は次のようになる。

機械装置　100,000,000　/　現金預金　110,000,000
仮払消費税　10,000,000　/　(4.1)

ただし、A 病院の課税売上割合 = 20%であるので、「比例一括配分」の場合、

(控除対象消費税額) = 10,000,000 × 0.2 = 2,000,000　(4.2)

従って、最終的には決算日において、次の仕訳が発生する。

控除対象外消費税　8,000,000　/仮払消費税 8,000,000　(4.3)

「控除対象外消費税額」は**営業外費用となる。つまり、800 万円は病院側が転嫁できず自己負担**することになる。これはかなり重い負担であり、この”損税”が現行の 2 倍になると経営が破たんする医療機関が続出することが懸念される。医療機関の確保は高齢者や身体障害者の方々にとって切実な問題である。

続いて、医療機器に軽減税率(5%)を適用した場合の設例を示す。

〔設例 2〕S 外科医院(本則課税事業者)は CT スキャンを税抜 1 億円で購入した。この場合の控除対象消費税額を求めよ。S 病院の**保険対象診療(非課税)は 80%**であり、保険外医療(課税)は 20%(税抜きベース)であるので、課税売上割合は 20%である。ここで、CT スキャンの消費税率は軽減税率の 5%であるとする。また、税額控除は一括比例配分方式を用いるものとする。

まず、CT スキャン購入時の会計上の仕訳は次のようになる。

機械装置　100,000,000　/　現金預金　105,000,000
仮払消費税　5,000,000　/　(4.4)

ただし、A 病院の課税売上割合 = 20%であるので、「比例一括配分」の場合、

(控除対象消費税額) = 5,000,000 × 0.2 = 1,000,000　(4.5)

従って、最終的には決算日において、次の仕訳が発生する。

控除対象外消費税　4,000,000　/　仮払消費税　4,000,000　(4.6)

「控除対象外消費税額」は**営業外費用となる。つまり、病院側が転嫁できず自己負担する金額は 400 万円に減少**することになる。これは厳しい経営環境にある地方の公立病院や中小病院にとっては朗報である。

最後に、**保険対象医療が「非課税」から「免税」に変更なった場合**の設例を示す。

〔設例 3〕S 外科医院(本則課税事業者)は CT スキャンを税抜 1 億円で購入した。この場合の控除対象消費税額を求めよ。S 病院の**保険対象診療(免税)は 80%**であり、保険外医療(課税)は 20%(税抜きベース)である。ここで、CT スキャンの消費税率は標準税率の 10%であるとする。また、税額控除は一括比例配分方式を用いるものとする。

課税売上割合の計算式は次の通り。

$$\text{課税売上割合} = \frac{\text{課税売上高(税抜き)} + \text{非課税品の海外拠点への移送}}{\text{課税売上高(税抜)} + \text{非課税売上(1)} \times 0.05 + \text{非課税売上(2)}}$$

※1.「課税売上高」には、課税物品の「輸出取引による免税売上」によるものを含む。
※2.「非課税売上(1)」は有価証券の売上を表す。「非課税売上(2)」は有価証券以外の非課税売上を表す。
※3.「不課税」は分母・分子ともに参入されないのに対し、「非課税」は分母にのみ算入される。

ここで、課税売上の計算式において、「免税売上」は「課税売上」に含まれるので、

（課税売上割合）＝　100%　　(4.7)

CT スキャン購入時の会計上の仕訳は次のようになる。

機械装置	100,000,000	/	現金預金	110,000,000
仮払消費税	10,000,000	/		

(4.8)

ただし、A 病院の課税売上割合 = 20%であるので、「比例一括配分」の場合、

（控除対象消費税額）　=　10,000,000 × 1.0 =　10,000,000　　(4.9)

従って、「控除対象外消費税額」は 0 円である。「保険対象医療」を「非課税売上」でなく「免税売上」扱いに変更することにより、患者の窓口負担を増やすことなく、病院の損税問題を解消することが可能である。

※「保険対象医療」を「非課税」ではなく「免税」とすることについては、消費税導入前の 1988 年の段階から専門家や国会において議論されてきた重要テーマであるが、「診療報酬の改定」を条件に先送りされた経緯がある。

<<Reference>>

1. 参議院インターネット審議中継
http://www.webtv.sangiin.go.jp/webtv/index.php
2. 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
3. SAP ジャパン IFRS エキスパートコラム　1-29(田淵隆明)　特に、第 20 回・第 21 回・第 24 回・第 25 回を参照。
http://global.sap.com/japan/campaigns/2010/ifrs/expert.epx
4. BS フジ「プライム・ニュース」(2013 年 12 月 3 日)
http://www.bsfuji.tv/primenews/text/txt131203.html

2014.03

総会特集【会長メッセージ】2014 年度活動方針について

会員番号 0557 仲 厚吉 （会長）

第13期通常総会が、2014年2月21日（金）13:30～15:00、会員86名の出席で、開催されました。2013年度事業報告をご承認いただきました。続いて、2014年度の協会運営に当たり、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ことを目的とした協会活動を行う等、2014年度事業計画を報告し、ご承認いただきました。また、役員選任の件、立候補者について報告し、ご承認いただきました。

会員各位から寄附を頂いた実績をもとに2014年度中に東京都へ「認定NPO法人」の申請を行うこと、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、システム監査の活性化の一環としてIT-Audit等のISO化、JIS化、システム監査に関連する他団体との交流、会員のコミュニケーション向上にホームページの整備と会員ポータルサイトの導入等を進めること等、下記のように報告しました。また、システム監査活性化委員会が、2013年度システム監査活性化プロジェクトを発展し、2014年度より新たな委員会として発足したことを報告しました。

（1）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、システム監査を公の活動として活性化させる。

3）協会組織の充実

東京都の「認定NPO法人」審査基準に従って協会組織を整備し、また、会員の信頼に応えるよう体制を充実させる。

（2）システム監査の活性化の一環として、次の活動を行う。

1）IT－Audit等、システム監査基準のISO化、JIS化を推進する。

2）システム監査に関連する他団体との交流を進める。

3）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図る。

（3）2014年度の予算編成について

1）編成方針

予算編成方針は、収益性とともに活動性をより重要とする。

2）事業活動

事業活動は、収支バランスを原則とする。収支は、公認システム監査人等認定事業収支が隔年上下変動することを考え、2年タームで取り組む。事業活動によっては、重要性や緊急性を考え例外を認める。

3）事務局

斎藤由紀子事務局長以下、事務局業務の効率化を図り、会員サービスの向上に取り組むとともに、会計（安部主査、藤澤理事、梅里理事）と協力して、協会の健全運営に努める。また、会員とのコミュニケーション向上のため、ホームページを整備し、あらたな会員ポータルサイト導入に向けて予算措置を講じる。

以上、役員一同、2014年度の活動を開始しております。会員各位のご協力をお願い致します。

2014.03

総会特集【第 13 期通常総会特別講演を聴講して】

会員番号　0557　仲　厚吉　（会長）

第13期通常総会特別講演が、2014年2月21日（金）15:20～16:20に、開催されました。会員の方々へ報告します。

演題：「リーマンショツクに立ち向うガバナンス-

新COSOの簡単な理解　-米国中央政府のGreen Reportを中心として」

講師：日本ITガバナンス協会会長　システム監査学会会長　松尾　明　氏

講演のはじめに、講演の目的である新COSOの簡単な理解として、「CLICK, CHANGE or DIE」の理解、即ち、インターネットの時代には、「インターネットから情報をクリック、ダウンロードし、そして利用し変化しなければ、死あるのみ」、これが新COSOの本質である、とのお話があった。続いて、新COSOと改訂の理由、Green Reportの定義、新COSO の17の指針、判断規準のデザイン、モニタリング、オブジェクトとCOBIT、COBITの変化、システム監査学会の取り組み、ISACA・ITGIの予定など、ITガバナンスの全般にわたる方向性について、講演があった。以下に、要約を記載する。

1．新COSOと改訂の理由

2013年5月14日に最終版が公表され、2014年12月15日までに移行を求めている。米国上場企業は対応を求められる。リーマンショツクが2008年9月15日に起きたことからして速い対応である。COSO改訂の理由を次に挙げる。

(1) ビジネスおよび業務環境の劇的な変化がある。

(2) テクノロジー主導的で国際的で複雑になることが、

組織の事業目的の達成可能性を高め、ビジネスおよび業務環境の変化に適応出来るように、

内部統制システムの有効かつ効率的な構築および維持が出来るように、

内部統制システムのインテグリテイ（誠実性と訳されているが本講演ではインテグリテイとする）に関する一層の透明性および説明責任を求めて利害関係者（Stakeholder）が関与度合いを高めている。

2．Green Reportの定義

COSO本文に無い、Green Reportの定義の幾つかを次に示す。

(1) Green book

-米国中央政府の内部統制基準である。州、市町村、NPO、社団等への適用もあり得る。ただし、これらの事業体の経営者が適切な法規やルールに従い定める。

(2) 内部統制

-内部統制（Internal Control）は、有効な内部統制システムを導入するための総括的（overall）なフレームワークを示すものであり、事業体の目的の全てをカバーする。事業体の目的には、本業業務運用、報告、法的準拠がある。

※総括的（overall）には、“全ての責任を持って”、“除外したことも記録に残す”ように運用することが求められる。

(3) 内部統制システム

-方針決定者や事業管理者は、事業体のミッションを達成するための説明責任を高めることに努めている。そのための成功要因は、有効な内部統制システムの導入である。

-有効な内部統制システムの導入により、環境変化、ディマンドの展開、新たな優先課題への対応を支援することができる。

-事業の変更が行われ、事業体が事業運用のプロセスを改善し、新たなテクノロジーを導入するのであれば、経営者は、継続的に内部統制システムを評価し、それが有効で最新化（Update）されていることを確かめることが求められる。

(4) ベースライン

-基準点ラインと訳されているが、ベースラインと本講演では定義する。内部統制システムのデザイン時の判断基準とある特定時点の状況との差異である。課題（Issue）および検出事項（Difficiencies）とも言える。

(5) 経営者（Management）

-事業体の担当者で、直接的にある組織の全ての活動に責任を負う者である。活動には、内部統制システムのデザイン、導入、有効なその運用も含まれる。

(6) 指針

-指針（プリンスパル）とは、法規やルールで従わなければいけないもの、従うことが出来るものである。原則と訳されているが、この講演では、方向性を共有することに、重みを置き、指針とした。

(7) 組織（構造）

-組織（構造）（Organizational Structure）には、本業ユニット、本業プロセス、その他の目標達成のための構造マネジメントがある。

3. 新COSO の17の指針

COSOの5要素は変わらない。合計17の指針がある。

・統制環境 5指針　・リスク評価 4指針　・統制活動 3指針　・情報と伝達 3指針　・モニタリング活動 2指針

(1) 統制環境

1) 組織は、インテグリテイと倫理観に対するコミットメントを表明する。
2) 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監督を行う。
3) 経営者は、取締役会の監督の下、内部統制の目的を達成するにあたり、組織構造、報告経路および適切な権限と責任を確立する。
4) 組織は、内部統制の目的に合わせて、有能な個人を惹きつけ、育成し、かつ、維持することに対するコミットメントを表明する。
5) 組織は、内部統制の目的を達成するに当たり、内部統制に対する責任を個々人に持たせる。

(2) リスク評価

6) 組織は、内部統制の目的に関連するリスクの識別と評価が出来るように、十分な明確さを備えた内部統制の目的を明示する。
7) 組織は、自らの目的の達成に関連する事業体全体にわたるリスクを識別し、当核リスクの管理の仕方を決定するための基礎としてリスクを分析する。
8) 組織は、内部統制目的の達成に対するリスクの評価において、不正の可能性について検討する。
9) 組織は、内部統制システムに重大な影響を及ぼし得る変化を識別し、評価する。

(3) 統制活動

10) 組織は、内部統制の目的に対するリスクを許容可能な水準まで低減するのに役立つ統制活動を選択し、整備する。
11) 組織は、内部統制の目的の達成を支援するテクノロジーに関する全般的統制活動を選択し、整備する。
12) 組織は、期待されていることを明確にした方針および方針を実行するための手続を通じて、統制活動を展開す

る。

(4) 情報と伝達

13) 組織は、内部統制が機能することを、支援する関連性のある質の高い情報を入手または作成して利用する。

14) 組織は、内部統制が機能するために必要な、内部統制の目的と内部統制に対する責任を含む情報を組織内部に伝達する。

15) 組織は、内部統制が機能することに影響を及ぼす事項に関して、外部の関係者との間での情報伝達を行う。

(5) モニタリング活動

16) 組織は、内部統制の構成要素が存在し、機能していることを確かめるために、日常的評価および/または独立的評価を選択し、整備および運用する。

17) 組織は、適時に内部統制の不備を評価し、必要に応じて、それを適時に上級経営者および取締役会を含む、是正措置を講じる責任を負う者に対して伝達する。

4. 判断規準のデザイン

判断規準のデザインには次のようなデザインが求められる。

(1) 事業情報システムのデザイン　-事業体の目的とリスクに対応させる。

(2) 適切な統制活動のデザイン　-情報システムによる統制活動を事業体の目的とリスクに対応させる。

(3) 情報テクノロジー基盤のデザイン　-情報テクノロジー基盤に対する統制活動をデザインする。

(4) セキュリテイマネジメントのデザイン　-情報システムのセキュリテイマネジメントの統制活動をデザインする。

(5) 情報テクノロジーの調達、展開、維持のデザイン　-これらのための統制活動をデザインする。

(6) 事業体の情報システムのデザイン　-業務処理統制

・完全性 ・正確性 ・正当性

(7) 情報システム活動のデザイン　-全般統制

・完全性 ・正確性 ・正当性 ・効率性

5. モニタリング

ベースラインを継続的にモニタリングすることが求められる。

(1) あるべき姿のデザインとその現状のリアルタイムに近い把握がグローバルな市場では求められている。TOGAF9があるべき姿のデザインの国際標準である。

6. オブジェクトとCOBIT

オブジェクトとは　-Objectは理解すれば、なぜ理解できないかわからなくなる。

(1) COBITとのかかわり　-1993年パリの会議でのオブジェクトの提案　-2008年LAの会議でのオブジェクトの提案

(2) 論議1 オブジェクト　-モノとしてのObject　-コンテンツはObjectか　-ソフトは、ネットはObjectか

7. COBITの変化

COBIT（Contorol Objectives for Information and related Technology）の変化は次のようなものである。

-1996 COBIT1

-1998 COBIT2　コントロール

-2000 COBIT3　マネジメント

-2005 COBIT4　ITガバナンス
-2007 COBIT4.1 VAL-IT　RISK-IT
-2012 COBIT5　Enterprise ITガバナンス
-2013 COBIT5　ビジネスト統合、エンネイブラー

(1) 1993年6月の提案
1) まとめの方向性のくくり方としてのObject 「 ・目的 ・資源(Object) ・はたらき 」
(2) COBIT1での対象範囲
1) 前向き品質の検討　-経営の有効性、効率性
2) データ管理の本質的な検討　-情報、知識への取り組み
(3) 有用性 イノベーションについて
1) プロダクトイノベーションとプロセスイノベーション
2) 不確かな、人的創造性と機会の膨大なプロセスの中から生まれる、核となるIntellectual or service competencies 廻りに戦略を高める。

8. システム監査学会の取り組み
(1) ドラッカーの遺言の勉強会 -法政大学で開催の予定
(2) オープングループセミナー -2回目を3月に予定、ソニー 所 氏　-1回目は、藤枝 氏 2月13日
(3) 30周年記念行事 -2014年に企画、来年度に実施

9. ISACA・ITGIの予定
(1) アジアCACS(ISACA) -5月に予定、5月30、31日、浅草橋
1) 基調講演 三浦雄大 氏 (三浦雄一郎 氏 長男)
2) インド政府情報戦略コンサルタント ビタルラジ 氏
(2) ITGIコンファレンス -10月開催は未定
(3) 30周年事業 -東京支部は、5月29日午後、浅草橋で予定

〔第13期通常総会特別講演を聴講して〕
日本ITガバナンス協会会長 システム監査学会会長 松尾 明 氏を来賓に仰いで、特別講演をお願いしました。講演は、講師から聴講者への質疑応答や、議論を交え、ITガバナンス全般の方向性について、初めて聴講する者にとっても、分かり易い講演であったと思います。講演の終わりに会場内から、「リーマンショツクに立ち向うガバナンス- 新COSOの簡単な理解 -米国中央政府のGreen Reportを中心として」は、日本でも適用されうるのかという質問が出ました。講師からは、金融庁の方も研究に参加しており、日本でも適用されうるとのお話しがありました。あらためて、来賓特別講演に謝辞を申し上げたいと思います。なお、Green Reportの原文については、下記のWebサイトを参照するようにとのお話でした。

http://www.gao.gov/assets/660/657383.pdf

以上

2014.03

総会特集【第 13 期通常総会報告】

事務局

第 13 期通常総会は、以下のとおり行われました。

1. 開催日時、場所等
   (1)日　時　 2014 年 2 月 21 日(金)　13:30～15:00
   (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 第1研修室
   (3)出席者数　86 名(委任状 38 名を含む)

2. 審議事項
   (1)2013 年度事業報告の件
   (2)2014 年度事業計画の件
   (3)役員選任の件

3. 議事の経過の概要および議決の結果
   互選により、中山副会長を議長に選任し、続いて上記3議案の審議を行った。
   議長より本日の議事録をまとめるにあたり、議事録署名人 2 名を選任することを諮り、互選により斎藤由紀子氏、舘岡均氏の 2 名を選任した。
   第 13 期通常総会資料に基づき、以下の通り審議及び議決が行われた。
   (1)2013 年度事業報告の件
      ① 事業報告
         沼野伸生理事より、2013 年度事業報告について説明を行った。
      ② 会計報告及び監査報告
         安部会計担当理事より、2013 年度の会計決算報告について説明を行い、続いて富山監事より、監査報告が行われた。
      以上で、審議を諮ったところ、全員異議なくこれを可決した。
   (2)2014 年度事業計画の件
      ① 事業計画説明
         仲会長より、2014 年度事業計画(案)について説明を行った。
      ② 予算の件
         安部会計担当理事より、2014 年度予算(案)について説明を行った。
      以上で、審議を諮ったところ、全員異議なくこれを可決した。
   (3)役員選任の件
      斎藤事務局長より、役員の候補者の説明を行い、審議を諮ったところ、全員異議なくこれを可決した。

以上により本日の議事を終了し、議長は会員各位の今後の協力を要請して閉会を宣言した。

第 13 期通常総会終了後、①システム監査学会会長松尾明氏の特別講演(注1)、②研究会発表(情報セキュリティ研究会藤野明夫主査「Privacy by Design ご紹介と問題提起」(注 2)、個人情報保護監査研究会斎藤由紀子主査「中小企業のための『個人情報保護マネジメントシステム実施ハンドブック』ご紹介」(注 3))が行われました。

また、その後の懇親会の席上で、新任理事紹介(注 4)、会報アワード表彰(注 5)などが行われました。

(注1)　聴講記録を P.17 に掲載しています。

(注 2)　発表内容の概要を P.36 に掲載しています。

(注 3)　説明のあった『個人情報保護マネジメントシステム実施ハンドブック』については、会報 2013 年 5 月号から内容の抜粋(簡易版)を連載中です(今回会報では P.42 に掲載)。当該ハンドブックは出版も計画中です。

(注 4)　P.24 に新任理事・監事の紹介をしています。

(注 5)　P.26 に 2013 年度会報アワードの表彰について、掲載しています。

＜総会風景＞

仲会長

質疑応答

中山議長

沼野前会長

安部会計主査

斎藤事務局長

富山監事

宮崎北海道支部長

横倉東北支部長

宮本北信越支部長

大友中部支部長

林近畿支部長

廣末中四国支部長

中溝九州支部長

2014.03

総会特集【　新役員体制　】

事務局

第 13 期は役員改選期にあたるため、総会において、以下のとおり役員が選任されました。

役員（2014年2月21日改選 ）

		役員	氏名	備考
本部	1	会長	仲 厚吉	2014/1/1就任
	2	副会長・事務局長	斎藤 由紀子	2014/1/1就任
	3	副会長	安部 晃生	2014/1/1就任
	4	副会長	小野 修一	
	5	副会長	力 利則	
	6	副会長	中山 孝明	
	7	副会長	松枝 憲司	
	8	副会長	三谷 慶一郎	
	9	理事	梅里 悦康	
	10	理事	遠藤 誠	
	11	理事	大石 正人	
	12	理事	大西　智	新任理事
	13	理事	久保木 孝明	
	14	理事	向後雅代	新任理事
	15	理事	越野 雅晴	
	16	理事	斎藤 茂雄	
	17	理事	桜井 由美子	
	18	理事	佐々野 未知	新任理事
	19	理事	清水 恵子	
	20	理事	鈴木 信夫	
	21	理事	鈴木 実	
	22	理事	高橋 典子	
	23	理事	舘岡 均	
	24	理事	西宮 恵子	
	25	理事	馬場 孝悦	
	26	理事	原 純江	
	27	理事	藤澤 博	
	28	理事	藤野 明夫	
	29	理事	松尾 正行	
	30	理事	三輪 智哉	
北海道	31	理事・支部長	宮崎雅年	新任理事
東北	32	理事・支部長	横倉正教	新任理事
北信越	33	理事・支部長	宮本 茂明	
中部	34	理事・支部長	大友 俊夫	
	35	理事	澤田裕也	新任理事
近畿	36	理事・支部長	林 裕正	
	37	理事	是松 徹	
	38	理事	荒町 弘	
中四国	39	理事・支部長	廣末浩之	新任理事
九州	40	理事・支部長	中溝 統明	
	41	監事	金子 長男	
	42	監事	木村裕一	新任監事

URL：http://www.saaj.or.jp/annai/yakuin.html

2014.03

新任理事・新任監事のご紹介

今年度から新たに役員になられる方は、以下の８名（本部３名、支部４名、監事１名）です。

本部理事	大西　智
本部理事	向後 雅代
本部理事	佐々野 未知
北海道支部理事・支部長	宮崎 雅年
東北支部理事・支部長	横倉 正教
中部支部理事	澤田 裕也
中四国支部理事・支部長	廣末 浩之
監事	木村 裕一

上記８名のうち、今回会報では、支部の新任理事４名の方に自己紹介をお願いしました。残り４名の本部理事・監事の方につきましては、次回 2014 年５月号でご紹介する予定です。

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

会員番号　1448 宮崎雅年（北海道支部 理事・支部長）

このたび理事・北海道支部長に就任した宮崎雅年です。

企業の情報システム部門に所属しており、被監査部門の立場でシステム監査と内部統制に対応している一方、監査部門の立場で社内の情報処理系システムのセキュリティを担当しております。最近では、制御系システムのセキュリティにも関心が高まっており、その対応が求められています。

日本システム監査人協会には、制御系システムのセキュリティに関わっておられる方々もおられることから、協会活動を通じて業務への気づきを得るきっかけとなればと考えております。

広い北海道には１７９の市町村がありますが、札幌市とその近郊に会員が集中しています。支部として会員が集まるには良い所ですが、北海道全体をカバーするには不十分な所でもあります。

北海道支部は、北海道のＩＴコーディネータやＩＴ技術者の組織と連携して研修会などを開催しています。北海道だけにとどまらず、広く全国の皆様と交流できれば幸いです。皆さま、今後ともよろしくお願いいたします。

会員番号　1347　横倉正教（東北支部　理事・支部長）

この度新たに理事になりました東北支部長の横倉です。　私はコンサルタントとして山形市を中心に主に山形県内で活動しています。　私は、ＩＰＡの情報処理技術者試験の上級システムアドミニストレータに合格し、その後、ＩＴコーディネータとして独立した際に、業務の幅を広げるためにシステム監査人（補）の資格を取得し、東北支部に所属して現在に至っています。システム監査人の資格取得では、故清水順夫氏から講習で指導していただきました。（清水氏とはシステムアドミニストレータ連絡会で知り合いとなっていました。）

趣味は、蕎麦屋巡りで、毎年、山形市内の蕎麦屋３８店舗を巡っています。また、神社、観光にも興味があります。東北支部の研修合宿では、そば打ち体験や蕎麦屋での昼食会、八幡神社への参拝（茅野輪くぐり体験）などのイベントを企画しました。

東北支部では、２か月ごとに例会を開催し、情報交換や研究活動を行っています。情報交換では、システム監査に関するものだけでなく、ＩＴ関連や一般の話題（最近では、消費税対応等）など会員の業務に関連すると思われることについての情報交換も行っています。研究会は、年度毎にテーマを決め、テーマに沿って討議を行っています。例会への会員の参加率はまだ十分と言えませんので、会員が参加したくなるような活動として、そば打ち体験やさくらんぼ狩りなどのイベントも行っています。

平成２５年は東北支部設立１０周年の記念の年でもあり、記念誌を製作しました。支部活動の歴史がわかる資料となっており、多くの方にみていただきたいと思っています。尚、支部活動サイトからダウンロードできるようにする予定です。

今後も、支部活動の活性化を図りたいと思っています。宜しくお願いします。

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

会員番号　1711　澤田裕也（中部支部　理事）

この度、中部支部の理事になりました。澤田裕也です。中部副支部長を務めており、主に合宿などイベントを担当しております。過去、例会や西日本合同研究会で発表しています。ユーザ系情報システム会社に所属しており、Web アプリケーションや OS のセキュリティ診断、セキュリティ監査といった業務に従事しております。

趣味は旅行(長期的な目標は日本 100 名城を制覇すること)、うさぎカフェに行ってうさぎと戯れることです。

中部支部の課題として、監査セミナーを独力で開催できるように講師のスキルを磨くことや例会以外の研究活動の充実等があげられますが、できることからコツコツと実施していたいと考えています。

微力ながら SAAJ を盛り上げていけるよう努力していきますので今後ともよろしくお願いいたします。

会員番号　1763　廣末浩之（中四国支部　理事・支部長）

今期より中四国支部の支部長に就任いたしました廣末と申します。1965 年生まれで今年 49 歳になります。私は、元々システムエンジニアとして働いていましたが、8 年ほど前に独立し、現在は個人事業主として活動しています。現在の仕事は、いろいろありますが、IT コーディネータとしての IT コンサルタント業、プライバシーマーク審査員、その他プロジェクトマネジメント支援等を実施しています。システム監査に関わる業務としては、内部統制での IT 統制内部監査支援業務を 1 社実施しておりますが業務の比率としては残念ながら少ないです。

趣味は、ゴルフ、将棋、飲み食べ歩きといったものです。近年、体重の増加が切実な課題となってきましたので、体を動かそうと思っていますが、なかなか継続は難しい状況です。しかしながら、3 年程前より友人に誘われ、地元の市民マラソン大会には参加していますので、これだけは継続していきたいと思っています。練習は直前にしか出来ていませんが。

今後、システム監査の普及に向けて微力ながら尽力していきたいと思っていますので、どうぞよろしくお願いいたします。

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

2014.03

2013 年度　会報アワード

会報編集担当

【2013年度 会報アワードの表彰について】

2013年1月から12月までの会報記事の投稿の中から、以下のとおり表彰者を選定しました。

「めだか」の部　　：沼野　伸生　様
「投稿記事、エッセイ」の部　：神尾　博　様
「部会や支部からの優良報告」：北信越支部、近畿支部

会報アワードを発表する藤澤主査

＊参考

【会報アワード】制度について

会報アワード制度は、2010 年度会報記事の投稿から「めだか」、「投稿記事、エッセイ」、「部会や支部からの優良報告」の3分野に分けてスタートし、優秀作品に対し、総会時に表彰することとしました。今回で4回目の表彰です。以前は会報記事の投稿者に薄謝として図書券を配布していた制度に変わるものです。

これからも、会報への積極的な投稿をお願いします。

次回は、あなたも「めだか」「エッセイ」「活動報告」等を投稿して、会報アワードを盛り上げていただけませんか。

（参考：2011年12月号、2012年1月号、2012年2月号会報に案内記事を掲載しています）

2014.03

第１８９回　月例研究会　（２０１４年２月開催）

会員番号 1795 藤澤 博

【講演テーマ】 :「個人情報保護法改正の方向性」

－ パーソナルデータの活用をめぐる制度見直し方針について －

【講師】:新保 史生(シンポ フミオ) 氏　慶應義塾大学 総合政策学部 教授

専門は、憲法、情報法。

経済協力開発機構 (OECD) 情報セキュリティ・プライバシー部会 (WPISP)副議長、憲法学会理事、情報通信学会監事、法とコンピュータ学会理事、(社) 日本マーケティング・リサーチ協会理事、総務省情報通信政策研究所特別上級研究員。

高度情報通信ネットワーク社会推進戦略本部 (IT 総合戦略本部)「パーソナルデータに関する検討会」、総務省「パーソナルデータの利用・流通に関する研究会」等の委員、スマートフォンの利用者情報等に関する連絡協議会議長をはじめとして、各府省庁、地方公共団体、公益法人、業界団体等の個人情報・情報セキュリティ関連の委員を歴任。

【日時】:2014 年 2 月 10 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

【講演骨子】:講演者より

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。平成 25 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。

【講演概要】:

個人情報保護法制定後、国民生活審議会個人情報保護部会、 消費者委員会個人情報保護専門調査会、経済産業省、総務省、高度情報通信ネットワーク社会推進戦略本部(IT総合戦略本部)等で、個人情報保護制度に関する検討がなされて来た。このような状況下で、本日の講演テーマである 「パーソナルデータの利活用に関する制度見直し方針」が、平成 25 年 12 月 20 日　高度情報通信ネットワーク社会推進戦略本部で決定された。 以下に、その概要について説明する。

「パーソナルデータの利活用に関する制度見直し方針」
http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/dec131220-1.pdf

Ⅰ パーソナルデータの利活用に関する制度見直しの背景及び趣旨

・ 我が国の個人情報保護制度については、様々な課題が指摘され、議論されてきたところであるが、具体的な解決に至っていないものもある。これまで行ってきた検討で蓄積された知見を活かし、時代の変化に合った制度の見直し、改善が求められている。

・ 今年で個人情報保護法の制定から 10 年を迎えたが、情報通信技術の進展は、多種多様かつ膨大なデータ、いわゆるビッグデータを収集・分析することを可能とし、これにより新事業・サービスの創出や我が国を取り巻く諸課題の解決に大きく貢献する等、我が国発のイノベーション創出に寄与するものと期待されている。特に利用価値が高いとされているパーソナルデータについては、個人情報保護法制定当時には想定されていなかった利活用が行われるようになってきており、個人情報及びプライバシーに関する社会的な状況は大きく変化している。その中で、個人情報及びプライバシーという概念が広く認識され、消費者のプライバシー意識が高まってきている一方で、事業者が個人情報保護法上の義務を遵守していたとしても、プライバシーに係る社会的な批判を受けるケースも見受けられるところである。また、パーソナルデータの利活用ルールの曖昧さから、事業者がその利活用に躊躇するケースも多いとの意見もある。

・ さらに、企業活動がグローバル化する中、情報通信技術の普及により、クラウド・サービス等国境を越えた情報の流通が極めて容易になってきている。国内に世界中のデータが集積し得る事業環境の整備を進めるためにも、海外における情報の利用・流通とプライバシー保護の双方を確保するための取組に配慮し、制度の国際的な調和を図る必要がある（EU:「データ保護規則」提案、米国:「消費者プライバシー権利章典」公表、OECD:「OECD プライバシーガイドライン」改正等）。

・ このような状況の変化を踏まえ、平成 25 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・データの利活用は、グローバルな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ていることから、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より民間の力を最大限引き出し、新ビジネスや新サービスの創出、既存産業の活性化を促進するとともに公益利用にも資する環境を整備する。さらに、事業者の負担に配慮しつつ、国際的に見て遜色のないパーソナルデータの利活用ルールの明確化と制度の見直しを早急に進めることが必要である。

Ⅱ パーソナルデータの利活用に関する制度見直しの方向性

このような背景・趣旨を踏まえ、個人情報及びプライバシーを保護しつつ、パーソナルデータの利活用を躊躇する要因となっているルールの曖昧さの解消等を目指して行うべき 制度見直しに関する主な方向性については、次の通り考えるものとする。

1. ビッグデータ時代におけるパーソナルデータ利活用に向けた見直し

・ 個人情報及びプライバシーの保護に配慮したパーソナルデータの利用・流通を促進するため、個人データを加工して個人が特定される可能性を低減したデータに関し、個人情報及びプライバシーの保護への影響並びに本人同意原則に留意しつつ、第三者提供における本人の同意を要しない類型、当該類型に属するデータを取り扱う事業者（提供者及び受領者）が負うべき義務等について、所要の法的措置を講ずる。

・ 共同利用やオプトアウト等第三者提供の例外措置要件の明確化、利用目的拡大に当たって事業者が取るべき手続きの整備、わかりやすいプライバシーポリシーの明示等パーソナルデータの取扱いの透明化等を検討する。

2. プライバシー保護に対する個人の期待に応える見直し

・ 適切なプライバシー保護を実現するため、保護すべきパーソナルデータの範囲、個人情報の開示及び訂正（追加

又は削除を含む。）等における本人関与の在り方、取り扱う個人情報の規模が小さい事業者の取扱い、プライバシー影響評価の導入、データ取得時等における手続きの標準化等について検討する。

・ 専門的知見の集中化、機動的な法執行の確保、及び諸外国の制度との整合を取りつつパーソナルデータの保護と利活用の促進を図るため、独立した執行機関（第三者機関）に行政処分等の権限を付与するとともに、プライバシーに配慮したデータ利活用の促進を図る観点から、罰則の在り方、法解釈・運用の事前相談の在り方等を検討する。 さらに、これらの対応と併せて、個人情報及びプライバシーの保護を有効に機能させるため、事業者が自主的に行っているパーソナルデータの保護の取組を評価し、十分な規律に服することが担保される、マルチステークホルダープロセス※の考え方を活かした民間主導の枠組みの構築を検討することにより、パーソナルデータ利活用のルールが遵守される仕組みを整備する。

※マルチステークホルダープロセス：国、事業者、消費者、有識者等の関係者が参画するオープンなプロセスでルール策定等を行う方法のこと。

3. グローバル化に対応する見直し

・ プライバシーに配慮したパーソナルデータの利活用は、グローバルに対処すべき課題であり、我が国の事業者がグローバルに適切なパーソナルデータの共有、移転等を行えるようにするため、諸外国の制度や国際社会の現状を踏まえた国際的に調和の取れた制度を検討するとともに、他国へのデータ移転の際の確実な保護対策等について検討する。

・ 国境を越えた情報流通の実態を踏まえた海外事業者に対する国内法の適用等について検討する。

以上の方向性に基づき、パーソナルデータの利活用に関する制度の見直しを進める。

Ⅲ パーソナルデータの利活用に関する制度見直し事項

1. 第三者機関（プライバシー・コミッショナー）の体制整備

・ パーソナルデータの保護と利活用をバランスよく推進する観点から、独立した第三者機関による、分野横断的な統一見解の提示、事前相談、苦情処理、立入検査、行政処分の実施等の対応を迅速かつ適切にできる体制を整備する。

・ その際、実効的な執行かつ効率的な運用が確保されるよう、社会保障・税番号制度における「特定個人情報保護委員会」の機能・権限の拡張や現行の主務大臣制の機能を踏まえ、既存の組織、権限等との関係を整理する。

2. 個人データを加工して個人が特定される可能性を低減した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

・ 個人情報及びプライバシーの保護に配慮したパーソナルデータの利用・流通を促進するため、個人データを加工して個人が特定される可能性を低減したデータに関し、個人情報及びプライバシーの保護への影響並びに本人同意原則に留意しつつ、第三者提供における本人の同意を要しない類型、当該類型に属するデータを取り扱う事業者（提供者及び受領者）が負うべき義務等について、所要の法的措置を講ずる。

3. 国際的な調和を図るために必要な事項

・ 諸外国の制度との調和

諸外国の制度や国際社会の現状を踏まえ、国際的なルール作りに積極的に参加しつつ国際的に調和の取れた制度を構築し、日本企業が円滑かつグローバルに事業が展開できる環境を整備するとともに、海外事業者に対する国内法の適用や第三者機関による国際的な執行協力等の実現について検討する。

・ 他国への越境移転の制限

グローバルな情報の利用・流通を阻害しないことと、プライバシー保護とのバランスを考慮し、パーソナルデータの保護水準が十分でない他国への情報移転を制限することについて検討する。

・ 開示、削除等の在り方

本人の自身の情報への適正かつ適時の関与の機会を確保することが、本人の不安感を払しょくするとともに、事業の透明性を確保することにもつながることから、取得した個人情報の本人による開示、訂正（追加又は削除を含む。）、利用停止（消去又は提供の停止を含む。）等の請求を確実に履行できる手段について検討する。

・パーソナルデータ利活用のルール遵守の仕組みの構築

第三者機関への行政処分等の権限の付与・一元化について検討するとともに、プライバシーに配慮したデータ利活用の促進を図る観点から、罰則の在り方等を検討し、パーソナルデータ利活用のルールを遵守する仕組を整備する。

・ 取り扱う個人情報の規模が小さい事業者の取扱い

本人のプライバシーへの影響については、取り扱うデータの量ではなくデータの質によるものであることから、現行制度で適用除外となっている取り扱う個人情報の規模が小さい事業者の要件とされる個人情報データベースを構成する個人情報の数が 5,000 件以下とする要件の見直しを検討する。その際、取り扱う個人情報の規模が小さい事業者の負担軽減についても併せて検討する。

・ 行政機関、独立行政法人等及び地方公共団体が保有する個人情報の取扱い

行政機関、独立行政法人等及び地方公共団体における個人情報の定義や取扱いがそれぞれ異なっていることを踏まえ、それらの機関が保有する個人情報の取扱いについて、第三者機関の機能・権限等に関する国際的な整合性、我が国の個人情報保護法制の趣旨等にも配慮しながら、必要な分野について優先順位を付けつつその対応の方向性について検討する。

4. 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

・ パーソナルデータの保護の目的の明確化

パーソナルデータの保護は、その利活用の公益性という観点も考慮しつつ、プライバシーの保護と同時に利活用を促進するために行うものであるという基本理念を明確にすることを検討する。

・ 保護されるパーソナルデータの範囲の明確化

保護されるパーソナルデータの範囲については、実質的に個人が識別される可能性を有するものとし、プライバシー保護という基本理念を踏まえて判断するものとする。

また、プライバシー性が極めて高い「センシティブデータ」については、新たな類型を設け、その特性に応じた取扱いを行うこととする。

なお、高度に専門的な知見が必要とされる分野（センシティブデータが多く含まれると考えられる情報種別を含む。）におけるパーソナルデータの取扱いについては、関係機関が専門的知見をもって対応すること等について検討する。

・ プライバシーに配慮したパーソナルデータの適正利用・流通のための手続き等の在り方

透明性の確保を原則として、利用目的の拡大に当たって事業者が取るべき手続きや第三者提供における本人同意原則の例外規定（オプトアウト、共同利用等）の在り方について検討するとともに、パーソナルデータ取得時等におけるルールの充実（同意取得手続きの標準化等）について検討する。

また、個人情報取扱事業者における個人情報の適正な取扱いを確保するため、個人情報の漏えい、その他のプライバシー侵害につながるような事態発生の危険性、影響に関する評価（プライバシー影響評価）の実施、公表等に

ついては、事業者の過度な負担とならないように配慮しつつ、評価事項・基準、評価対象、実施方法、評価方法等の具体化を「特定個人情報保護委員会」が行う特定個人情報保護評価の仕組みを参考に検討する。

Ⅳ 今後の進め方

- 本方針に基づき、詳細な制度設計を含めた検討を加速させる
- 検討結果に応じて、平成 26 年(2014 年)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(2015 年)通常国会への法案提出を目指す。

「個人情報保護法改正の方向性」に関連して、以下の内容の説明があった。

Ⅰ.「パーソナルデータの利用・流通に関する研究会」報告書の公表 （総務省平成 25 年 6 月 12 日）
Ⅱ. ビックデータの取扱いと責任
Ⅲ. 個人情報保護制度に関する国際的な最新動向
Ⅳ. プライバシー保護をめぐる環境の変化
Ⅴ. PIA とは

上記の概要は、以下のとおり。

Ⅰ.「パーソナルデータの利用・流通に関する研究会」報告書の公表 （総務省平成 25 年 6 月 12 日）

◎研究会報告書のポイント

- 保護されるパーソナルデータの範囲
  「実質的個人識別性」(プライバシーの保護というパーソナルデータの利活用の基本理念を踏まえて実質的に判断される個人識別性)
- パーソナルデータの利活用のルールの内容の在り方
  取得の際の経緯(コンテキスト)に沿った取扱いである場合と沿わない取扱いである場合の区分に応じた適正な取扱い
- パーソナルデータの利活用のルール策定の在り方
  「マルチステークホルダープロセス」(国、企業、消費者、有識者等多種多様な関係者が参画するオープンなプロセス)
- パーソナルデータの利活用のルールの遵守確保の在り方
  パーソナルデータの利活用のルールに関する判断の提示や、消費者と企業間の紛争解決を行うこと
- パーソナルデータの保護のための関連技術の活用
  プライバシー強化技術: Privacy EnhancingTechnologies(PETs))を最大限に有効活用すること
- 国際的なパーソナルデータの適正な利用・流通の確保
  国際的なパーソナルデータ保護の執行協力など

Ⅱ. ビックデータの取扱いと責任

- 取扱いの対象となる情報の「内容」とその取扱「手続」との関係における問題の両面に分けて検討することが必要。

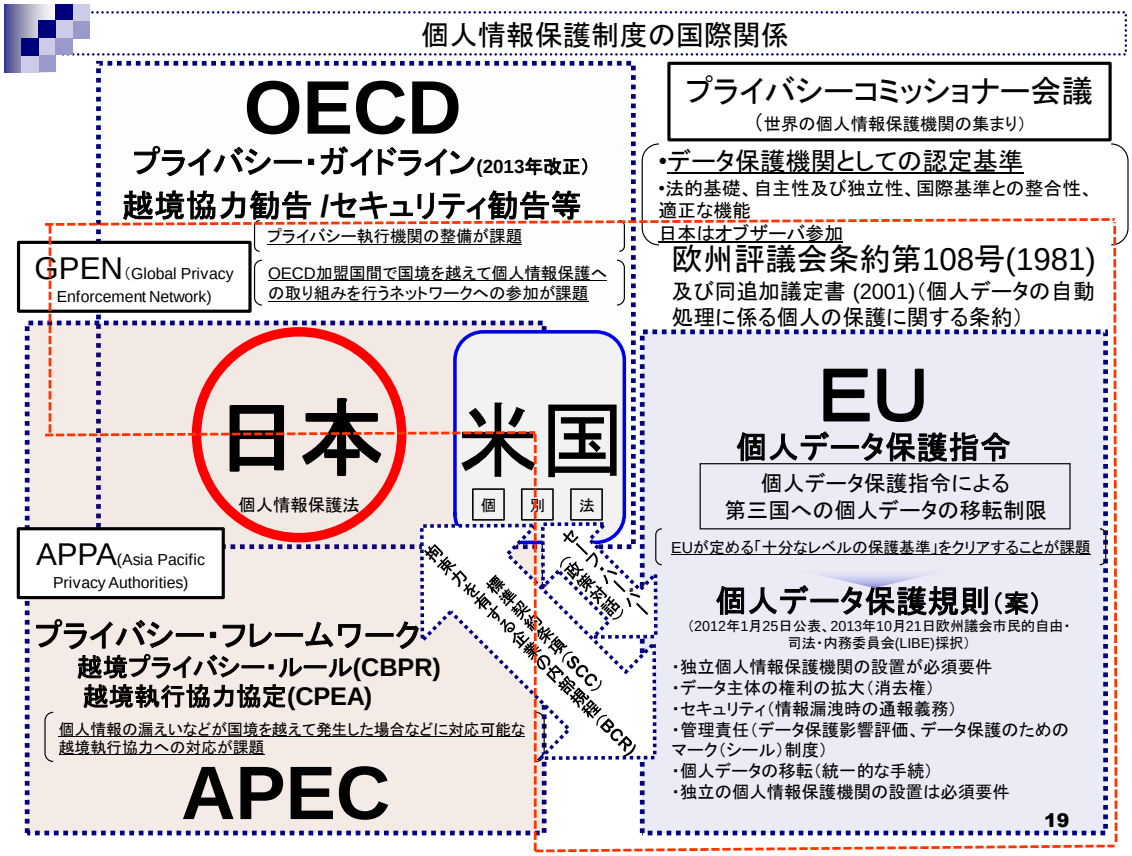
・ 前者については、ビックデータの取り扱いにおいて、情報の内容によってその取扱いが問題となる可能性がある場面としては、以下のような場合が考えられる 。

①統計情報として個人情報には該当しないと考えていた情報が、特定の個人を識別可能な情報にあたる場合
②単なる個人情報ではなく個人のプライバシー（他人に知られたくない情報）に該当する情報を取り扱う場合
③センシティブな情報など、その取扱いによって個人の権利利益を侵害する可能性が高い情報を取り扱う場合
④国家機密や企業の営業秘密にあたる情報を取り扱う場合
⑤法令において取扱いが制限されている情報を取り扱う場合（守秘義務による制限やブラックリストの保有禁止など）

ビッグデータの取扱いにあたっては、法令遵守や個人の権利利益保護への取り組みが軽視される傾向があることは否めない。

Ⅲ. 個人情報保護制度に関する国際的な最新動向

国際的な最新動向は次の図で全体の関係を表すことが出来る。



図に示された項目は次を参照。

■OECD（経済協力開発機構）

プライバシーガイドライン（2013 年改正）

＊ガイドライン本文は、堀部政男、新保史生、野村至「OECD プライバシーガイドライン日本語訳（仮訳）」〈http://www.jipdec.or.jp/publications/oecd/〉を参照されたい。

■EU（欧州連合）

EU 個人データ保護指令（1998 年制定）

EU 個人データ保護規則案、法執行指令案（2013 年 10 月 21 日欧州議会市民的自由・司法・内務委員会

■APEC（アジア太平洋経済協力）

APEC プライバシーフレームワーク（2004 年 10 月 29 日採択）

APEC 越境プライバシー規則（APEC Cross-Border Privacy Rules (CBPR)）

プライバシー・フレームワーク（越境執行協力協定(CPEA)）

■欧州評議会（Council of Europe）

個人データの自動処理に係る個人の保護に関する条約第 108 号(1981 年）改正案

■米国

消費者プライバシー権利章典（2012 年）

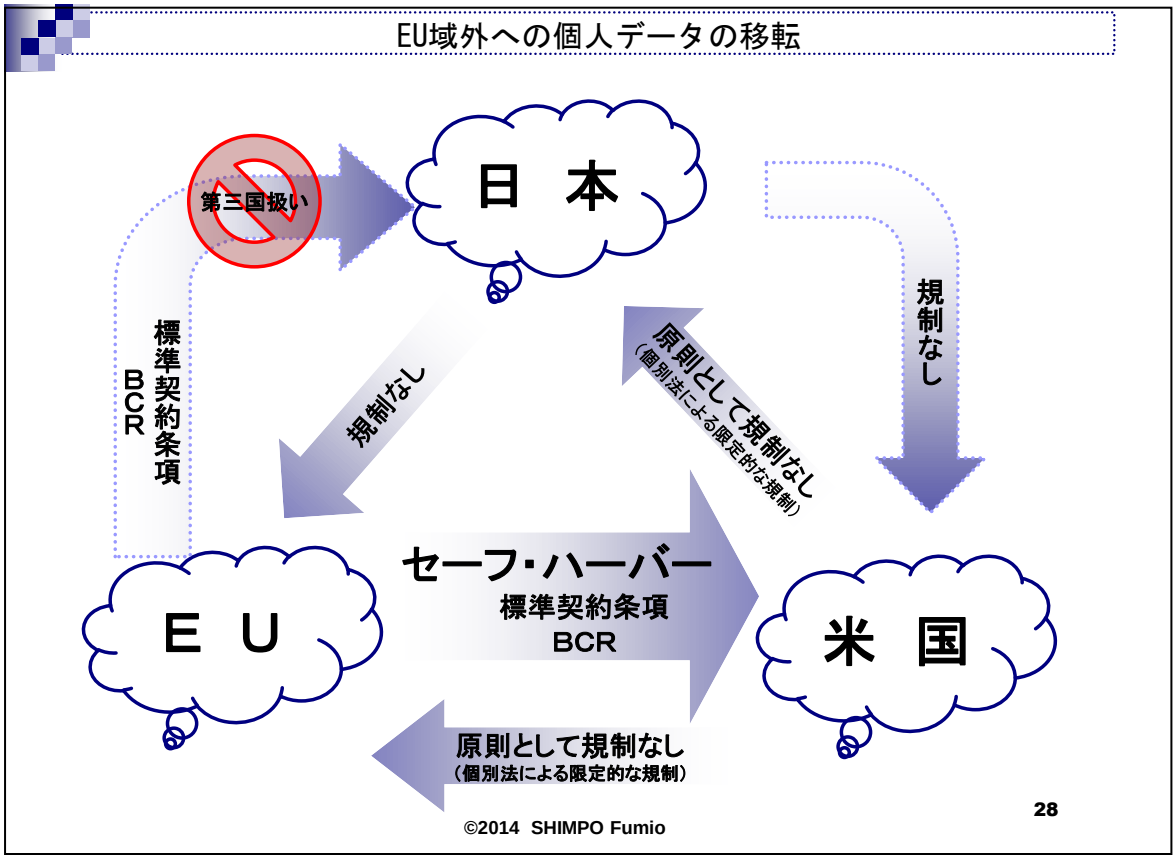
■日本

「パーソナルデータの利活用に関する制度見直し方針」高度情報通信ネットワーク社会推進戦略本部決定

（平成 25 年 12 月 20 日）

＊　EU 区域外への個人データの移転

日本と EU、米国とは次の関係にある。



Ⅳ. プライバシー保護をめぐる環境の変化

①個人のプライバシーに対する様々な脅威の増大

・SNS（ソーシャルネットワーキングサービス）の利用者数の増加

・スマートフォンの普及

・クラウド・サービスの利用

・新たなサービスの出現やネットワークの利用環境の変化

②プライバシー保護への新たな対策や取り組み

・プライバシーへの脅威となりかねないサービスの増加に対抗

③「プライバシー」という概念は、抽象的であるとともに個人の主観にも左右される

・プライバシー保護のための「仕組み」そのものが、抽象的かつ曖昧な概念（イメージ）として受け止められる傾向がある

・プライバシーとは、主観的要素に影響される抽象的な概念

・プライバシー侵害に対しては、事後的な救済によらざるを得ない

・事後救済では手遅れ（原状回復は困難）

これらを解決するために考案されたのが

「プライバシー・バイ・デザイン（PbD）」

④PbD とは

・プライバシー保護を目的として利用される技術および対策を、システム設計およびその構築段階から検討・実装し、個人情報の取扱いに関するライフサイクル全般において、体系的かつ継続的にプライバシー保護に取り組むための仕組み

⑤PbD の目的

・公正な情報処理（FIPs：Fair Information Practices）の達成

・プライバシー保護に向けた取り組みを事前に計画し、それを実施すること

・七つの基本原則と六つのプロセスから構成

【七つの基本原則】

1. リアクティブ（事後）でなくプロアクティブ（事前）：事後の措置でなく事前に予防
2. デフォルト設定でプライバシー保護
3. 設計時に組み込むプライバシー対策
4. すべての機能に対してーゼロサムではなくポジティブサム
5. エンドツーエンドのセキュリティ：ライフサイクル全体の保護
6. 可視化と透明性：オープン化
7. 個人のプライバシー尊重：個人を主体に考える

Ⅴ．PIA とは

①PIA（プライバシー影響評価）とは

・行政情報システムにおける個人情報の適正な取扱いを確保し、個人のプライバシーを保護するために最適な方策を講ずるために実施する評価手法のこと

・諸外国においては新たな行政システムの構築にあたって、事前に実施することを義務づける国がある

②PIAの実施が求められる背景

・行政事務や行政サービスなど行政の電子化+個人情報を電子的に取得し処理をする新たな情報システムの構築

・個人情報を扱うシステムの構築等を行う場合に、事前に個人の権利利益の侵害を防ぐための対策が必要との考え

・PIAを実施することで、新たな情報システムの導入によって個人のプライバシーが脅威にさらされることがないようにすることが可能

質疑応答:

【質問1】:OECD8 原則に記載されているデータ管理者とは？

【講演者コメント】:OECD8 原則に記載されているデータ管理者とは、各原則を実施するための措置に従う責任を有する者で、個人情報保護法でいう個人情報取扱事業者に該当する。

【質問 2】:日本の第三者機関(プライバシー・コミッショナー)の国際的位置づけについて？

【講演者コメント】:日本は、残念ながらプライバシーコミッショナー会議(世界の個人情報保護機関の集まり)の正式メンバーではないが、この会議は意思決定機関でなく、各国の代表者やステークホルダーが集まって意見を交換する重要な会議であります。このプライバシーコミッショナー会議に堀部先生は、永年、日本を代表しオブザーバとして参加されており、事実上のコミッショナー的な役割を担っておられる。

【質問 3】: EU と日本では、個人情報保護に関して根本的に何が異なるのか？

【講演者コメント】:EU の保護制度は枠組みがしっかりしていて理想的である。しかし、一例で言うと、英国ではデータ管理者の登録制度があるが関連する企業すべてが登録されているか疑わしいところがある。一方、日本では、業法(電気通信事業法等)で事業者の登録義務があるが、登録していない事業者はない。このように EU と日本では、法令遵守のギャップが存在する。

本件の内容については、雑誌「ジュリスト」(有斐閣)3 月号に掲載しているので参考にして戴きたい。

上記以外の質問もあり、活発な質疑応答の時間を持つことが出来ましたが、紙面の都合で割愛させて戴きました。

【講演終了】

【記録者の感想】

講師の新保史生氏からは、「個人情報保護法改正の方向性」と海外における個人情報保護の動向等について、熱のこもった講義を戴き、参加者は終始注目し拝聴していた。

新保史生氏が、平成 27 年(2016 年)通常国会への法案提出に向け、パーソナルデータの利用・流通の可能性とその課題の整理等について精力的に活動されていることが、ひしひしと感じました。また、個人情報保護制度に関する国際的な最新動向として、OECD プライバシーガイドライン、EU の個人情報保護指令及び個人データ保護規則、APEC のプライバシー・フレームワーク及び米国のセーフ・ハーバーについても説明を戴き、世界の動きを感じることができました。今後の「個人情報保護法」改正の動きについて、注目したいと思います。 (藤澤 記)

【本講演に関する参考文献】

・「パーソナルデータの利活用に関する制度見直し方針」
http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/dec131220-1.pdf
・世界最先端 IT 国家創造宣言 http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20130614/siryou1.pdf
・「OECD プライバシーガイドライン日本語訳(仮訳)」 http://www.jipdec.or.jp/publications/oecd/
・雑誌「ジュリスト」(有斐閣)3 月号(2014 年 2 月 25 日発売)P.38-44
特集 ビッグデータの利活用に向けた法的課題 ーパーソナルデータ保護法制の展望ー
「EU の個人情報保護制度」(新保史生氏)

以上

2014.03

【情報セキュリティ監査研究会だより その１２ ― プライバシー・バイ・デザイン 第７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。

この議論の概要を、2月21日に開催された日本システム監査人協会第13期総会の後の特別講演会において、「Privacy by Design ご紹介と問題提起」と題し、主査である藤野が発表しました。今回は、この発表の概要をご報告いたします。当日は時間が短かったために割愛した部分があります。この報告では、その部分を補っておりますことをご承知おき下さい。なお、テキストの他に下記の資料を参考にしております。

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

＜参考資料＞ 「6. 先行事例 DNT:Do Not Track」の参考資料

Mozilla Japan、「DO NOT TRACK 実装ガイド」、2012.05.01
http://www.mozilla.jp/static/docs/firefox/dnt-guide.pdf

【報告内容】第13回総会(2月21日)後の特別講演会での発表、「Privacy by Design　ご紹介と問題提起」

１．プライバシー・バイ・デザインとは何か

提唱者であるカナダ・オンタリオ州の情報・プライバシー・コミッショナー、アン・カブキアン博士の定義によれば、プライバシー・バイ・デザインとは、「プライバシー情報を扱うあらゆる側面においてプライバシー情報が適切に取り扱われる環境をあらかじめ作り込もうというコンセプト」である。しかし、これは、単にコンセプトというレベルではなく、フレームワーク、さらにいえば、ムーブメント(運動)と言うべきものではないか。デジタルネットワーク技術が社会インフラとして深く浸透し、社会全体に革命的な変化が起こりつつある現在、「プライバシー・バイ・デザイン」は、その変化の方向を左右する力を持つものであると考える。このようなコンセプトを、インターネットが普及し始めた1990年代半ばに提唱した、アン・カブキアン博士の先見性に、深く敬意を表するものである。

プライバシー・バイ・デザインの目指すものは、以下の三点である。

①公正な情報処理(FIPs:Fair Information Practices)
②プライバシー保護に向けた取り組みを事前に計画し、実施
③制度的方策だけでなく技術的に深く踏み込んだ対策も検討

後に紹介するように、③の技術的に深く踏み込んだ対策も検討するというところに、従来のこの種のコンセプトあるいはフレームワークにない斬新さがある。従来この種のものは、一般的な標準として取り込まれることを狙うために、

ベンダー無依存あるいはベンダー独立性を貫く必要があり、敢えて個々の技術に踏み込むことを避けてきた。しかし、今日の技術の発展と社会への浸透の速さは、技術的に深く踏み込まないと問題が解決できず、そのような自己規制を許さなくしている。

２．プライバシー・バイ・デザイン、七つの基本原則

プライバシー・バイ・デザインの骨格をなすもの、それは、以下に示す七つの基本原則である。

①プロアクティブ、事後的救済ではなく予防： 事後的な救済策ではなく、予防的に事前に作用する。

②デフォルト設定としてのプライバシー保護： プライバシー保護機能は、システムに最初から組み込まれ、初期状態で有効化されている。したがって、ユーザーが意識せずにプライバシー保護機能が働く。

③設計に埋め込まれたプライバシー対策： プライバシー保護の仕組みは、IT及びビジネス慣行のデザイン及び構造に組み込まれる。付加機能として追加されるものではない。ITシステムおよびビジネス慣行に不可欠な中心的機能である。ITに閉じた話ではない。

④ゼロサムではなくポジティブサム： プライバシー保護の仕組みの構築によって、安全性や利便性を損なうなどのトレードオフの関係をつくってしまうゼロサムアプローチではなく、すべてに対して利益をもたらすポジティブサムを目指す。

⑤情報のライフサイクル全体に渡っての保護： プライバシー情報は、発生から廃棄までのライフサイクル全体に渡って適切な保護がなされなければならない。

⑥可視化と透明性、オープンな状態に：すべての関係者の信頼を得るために、可視化と透明性を確保する。

⑦ユーザー（個人）主体のプライバシーの尊重：プライバシー情報を取り扱う側の利益ではなく、プライバシー保護の主体たるユーザー（個人）の利益を最大限に尊重する。

以下、プライバシー・バイ・デザインに関連する、PIA、FIM、F－PIA、DNTをご紹介する。

３．ＰＩＡ：Privacy Impact Assessment

プライバシー・バイ・デザインの実現のためには、システムの設計段階でプライバシー影響評価、PIAが必要である。PIAとは、情報システム稼働に伴うプライバシーへの影響を評価する手法であり、あらかじめ定めたフレームワークに適合しているか否かを評価する。さらに、プライバシーへの影響を低減する制度的方策と技術面の検討を行う。技術面の検討では、プライバシー保護強化技術（PETs：Privacy Enhancing Technologies）を利用する。

なお、PIAは、元来、電子政府等の行政情報システムが対象であったが、その内容ゆえ、実施対象は行政組織に限定されない。とくに民間企業でも行政機関に匹敵する個人情報を保有し、また、ビッグデータとしての活用の動きが活発化する現在、重要なアクティビティになっているのではないか。

４．ＦＩＭ：Federated Identity Management

FIM（連携アイデンティティ管理）は、複数の事業者間で取り扱われる個人識別情報に関する事業者間の新たな連携モデルの構築によって、個人識別情報提供者から見れば、自身の個人識別情報が異なる事業者間で授受されることで不適切な取扱いを受けるリスクを減じ、また、個人識別情報を利用する事業者側から見れば、煩雑で危険な個人識別情報を取り扱うことのリスクを減ずる。

そのために、一般のサービスプロバイダーから独立して個人認証等を行う、アイデンティティプロバイダーという機関を設ける。以下の図1に示す事例により、その機能を紹介する。

この事例は、A銀行に口座を持つユーザーが、B銀行のATMを用いて、X円を引き出す処理である。

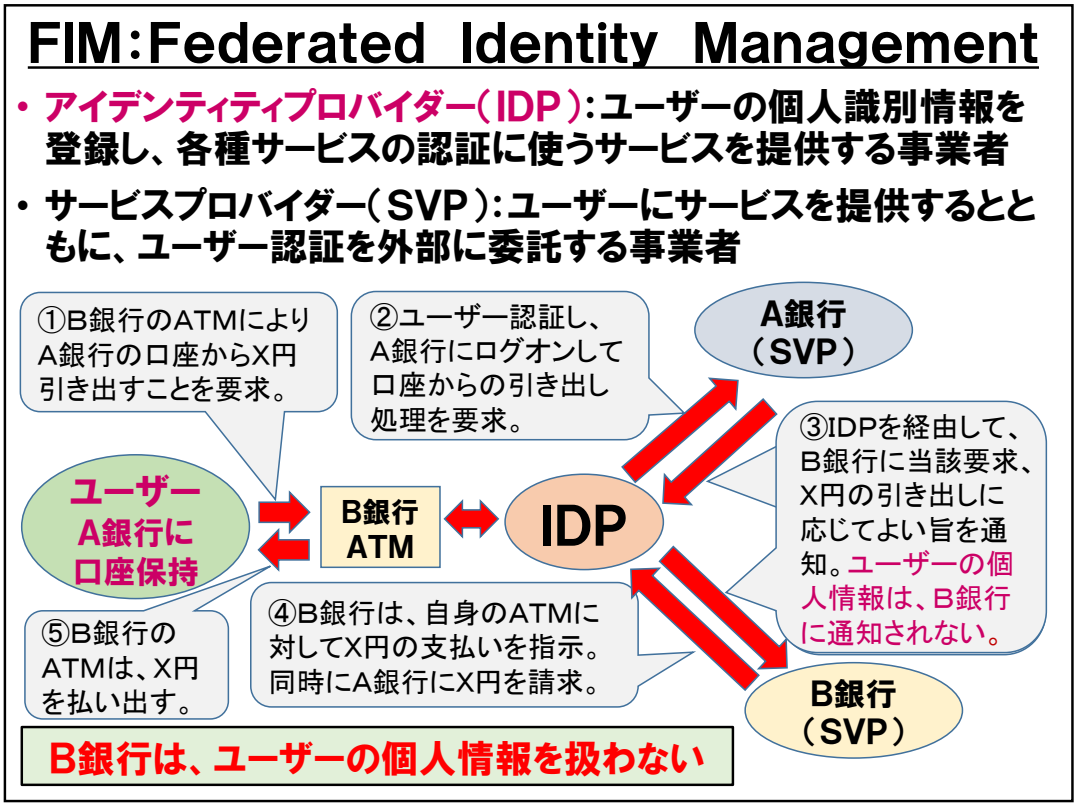


図１．ＦＩＭの機能について

①ユーザーは、B銀行のATMに対して、A銀行の口座からX円を引き出すことを要求する。

②B銀行のATMは、アイデンティティプロバイダー(以下、IDP)に接続し、IDPは、入力されたユーザーの個人情報により個人を識別、認証して、A銀行にログオンし、A銀行に対してX円の引き出しを要求する。

③A銀行は、ユーザーの残高を調べ、引き出し可能であれば、IDPを経由して、B銀行に当該要求、X円の引き出しに応じてよい旨を通知する。このとき、A銀行とB銀行の間では、ユーザーの個人情報は一切、授受されない。

④A銀行から通知を受けたB銀行は、自身のATMに対してX円の支払いを指示し、同時にIDPを介してA銀行にX円を請求する。

⑤B銀行のATMは、ユーザーにX円を払い出す。

上述のごとく、B銀行は、ユーザーの個人情報を一切扱わないので、このユーザーの個人情報を管理する必要はない。一方、A銀行はB銀行に対してユーザーの個人情報を渡す必要がなく、第三者提供の事態が発生しない。

５．Ｆ－ＰＩＡ：Federated ＰＩＡ

Ｆ－PIA(連携プライバシー影響評価)とは、個人情報が流通する複数の組織の連合体に対するPIAである。

異なる組織間で大量の個人情報が流れるデジタルネットワーク社会では、ある組織が取得した個人情報は、ネットワークを通じて転々と異なる組織間を移動し、各組織は異なる利用目的に活用する。単一の組織を前提にするPIAでは対応できない。

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(個人情報保護マネジメントシステム:JIS　Q 15001)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。情

報ライフサイクルの質問、ここでは、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が、そのうちの三点について対比してみる。Ｆ－PIAの質問の内容を（）付きの項番+ゴシック体で示す（出典:「テキスト」P175）。

（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、複数の企業等の組織間で個人情報が転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)と同様である。

６．先行事例 ＤＮＴ：Ｄｏ Ｎｏｔ Ｔｒａｃｋ

DNT(行動追跡拒否)は、Cookie等によるユーザー(個人)の行動の追跡を、本人側の意思によって拒否する技術である。自分の行動がCookie等により過去、現在、未来に渡って追跡され、購買履歴、友人関係、情報検索履歴などが、個人を識別できる履歴として残り、自分の性向、思想、行動パターン等が何者かに握られてしまう。インターネット社会の大きな負の側面である。この個人の行動の追跡を本人側の意思によって拒否する技術がDNTである。

DNTは、Webブラウザ（以下、ブラウザ）とWebサイト（以下、サイト）側に以下の仕組みを導入することで実現できる。ブラウザ側には、まず、ユーザーがDNT機能のオン／オフを設定する仕組みを作る。次にオンと設定した場合、ブラウザが作成するHTTPヘッダーに“DNT:1”という行を含めてサイト側に送信する。サイト側では、“DNT:1”を含むHTTPヘッダーを受け取ると、あらかじめサイト側が定めた、ユーザーの個人情報を取り扱わない措置をとる。

サイト側は、あらかじめDNTオン設定のユーザーに対して、どのような措置をとるかを決定し、それをプライバシーポリシーとして公開し、かつ、それを実現するプログラムをインプリメントする。例えば、Twitterは、DNTをオンに設定したユーザーに対しては、ユーザーにカストマイズしたお勧めや助言の表示などで使われるWebサイトのアクセス履歴情報の収集を停止し、同様に、お勧め広告の表示で使われるTwitterの広告パートナーのWebサイトのアクセス履歴情報の収集も停止する等の措置をとることを宣言している。

DNTの機能は、DNTオンの設定をしたユーザーが、自己のプライバシー保護に対する要求と合致するプライバシーポリシーを宣言したサイトを選択してアクセスすることで実現する。

しかし、DNTには以下の問題点がある。一点は、プライバシーポリシーの異なるサイトを個人情報が転々流通し、DNTの実効性が失われることである。二点目は、ユーザーはサイト側が公開するプライバシーポリシーの技術的内容を理解できるかという問題である。Cookieの意味を理解しているユーザーはどのくらいいるのであろうか。

７．プライバシー・バイ・デザインが突きつけるもの

デジタルネットワーク技術が社会インフラ化した今日、単一の組織では、プライバシーの実効的保護は不可能である。とくに、最近、脚光を浴びているビッグデータの活用は、複数の組織における異種の個人情報を解析することで、従来、得られなかった新たな知見を得るところに最大の効果がある。Ｆ－PIAに見られるように、この点に着目して、早々と取り組む姿勢は評価すべきであるが、前述のDNTのごとく大きな解決困難な問題があるのではないか。

そもそもＦ－PIAが提案する複数の組織の連合体は実現可能であろうか。複数の業種あるいは同一業界のライバ

ルどうしが、手を組めるものなのか。また、この実現には、社会全体のコンセンサスと大きな投資が必要になる。

DNTについても、広告業の場合は、ユーザーがカストマイズされた広告の提供を望まなければ、そのユーザーのアクセスログの取得を止めればよいが、金融業では、不正行為追跡と証拠の確保のために個人情報を含むアクセスログの取得は必須であろう。業種により、利便性や安全性に対する要求は異なり、プライバシーポリシーも異なる。

これらを解決するためには、制度作りだけでは限界があり、社会的要求に対して技術をマッチングさせる社会技術的アプローチが必要になり、技術に対する深い洞察と新たなアーキテクチャ構築が必要になる。

さらに、プライバシー・バイ・デザインは、ユーザーと組織との間のトレードオフの関係をWinWinの関係にすることを目指しているようであるが、知る権利等の他のコンプライアンスとのトレードオフの問題は、未解決である。

加えて日本独特の問題がある。それは、欧米諸国に比較して、一般の人がプライバシーに関する認識が低いことである。基本的人権の確保のために、文字どおり血を流してきた欧米諸国との歴史の違いが原因かもしれない。一言で言えば、何を守るべきか、なぜ守られるべきかについて、我が国では、コンセンサスがない。おそらく、プライバシー・バイ・デザインを推進するにあたり、なぜ、そのような大掛かりなことをしなければならないのかということに、多くの国民が疑問を持つのではないか。

８．システム監査人の新たな役割

前述のごとく、急速に社会インフラ化するデジタルネットワーク技術に対応し、そこからプライバシー保護を筆頭とするコンプライアンスの問題に対応するためには、この時代に相応しい、技術と制度の融合による新たな社会アーキテクチャ作りが必要となる。社会に大きなインパクトを与えることになる、この変革は誰が担うべきであろうか。

ITベンダー、ユーザー企業であろうか。まさにこれからビッグデータ等の個人情報を活用し、ビジネスチャンスを拡げようとしているこれら企業は、自らの行動に制約を課すことになりかねないプライバシー・バイ・デザインに対して消極的なのではないか。一方、行政はどうであろうか。行政が主導権をとるということは、権力を行使することである。権力を行使するためには、法的裏付けが必要であるが、新たな法律を作るには国民の間のコンセンサスが必要になる。急激に進歩するITと、それに伴う急速な社会の変化は、コンセンサスを得る余裕を与えないのではないか。

時々刻々変化する事態に柔軟に対応でき、かつ、コンプライアンスと相性がよいのは、監査プロセスではないか。監査プロセスは、監査対象との対話のプロセスであり、合意形成の可能性がある。

システム監査人は、技術的バックグラウンドがあり、他のIT技術者に比べれば、法律や社会的制度にも通じているが、残念ながら、この大変革を主導するほどのパワーは、我々にはない。しかし、かつてのY2Kのときのように、これらの問題に対して警鐘を鳴らすことは可能であろう。また、変革の方向性、あるいは、フレームワークの提案は可能かもしれない。

情報セキュリティ研究会は、プライバシー・バイ・デザインを軸に、上記活動を目指す。

【今後の活動について】以下は、特別講演会の発表では触れなかった当研究会の今後の活動予定である。

上記発表の「7. プライバシー・バイ・デザインが突きつけるもの」及び「8. システム監査人の新たな役割」を深く追求し、時代の要求に対応するシステム監査人の新たな活躍の場を検討したい。現段階では、問題点を枚挙したレベルであるが、3月、4月は、この問題を論理的に整理し、自らの能力を考量して解決のための優先付けを行い、5月には新たなテーマによる検討を開始したい。ご興味のある方は、冒頭に記したご案内にしたがって、是非、当研究会にご参加いただきたい。

以上

2014.03

【　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１ＳＯ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-4　パフォーマンス ITは、現状及び将来のビジネス要求事項に合致するサービスレベル及びサービス品質の提供を支援するという組織の目的に適合する。
プロセス 1. ITがビジネス目標の達成を支援しているか評価の為のプロセス 2. 文書管理の評価の為のプロセス 3. プロジェクト管理の評価の為のプロセス 4. 品質管理の評価の為のプロセス 5. 変更管理の評価の為のプロセス
プロダクツ 1. ビジネス要求およびIT要求分析に関する報告書 2. ITの変更管理サービス 3. 災害復旧サービスおよび代替運用計画 4. システム運用サービス 5. ITインフラの保守および管理サービス 6. 古い情報システムの廃棄サービス 7. 情報セキュリティ管理サービス

プリンシプル-5　適合・準拠 ITは義務的な法律及び規則に適合する。 方針および実務指針が明確に定義され、導入及び施行される。
プロセス 1. 組織がITガバナンスの為のシステムに適合しているか否かの評価の為のプロセス 2. ITの利用が関連法律、規則に準拠しているか否かの評価の為のプロセス
プロダクト 1. IT利用が関連する義務、標準、ガイドライン、ポリシーおよび手順に適合させる為の仕組 2. 専門家の為のポリシーおよび関連のガイドライン 3. コンプライアンス(準拠性)およびコンフォーマンス(適合性)に関する報告書 4. 環境、プライバシー、戦略的知識管理に関する報告書

2014.03

「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 23 章

会員番号：1760　斎藤由紀子（個人情報保護監査研究会）

第23章　例外処理について

23.1　例外処理について

個人情報の取得・利用･アクセス・提供において、例外的な処理が発生した場合は、
「4000PMS 例外処理申請書」によって、その理由を明記し、個人情報保護管理者の承認を得ます。

「4000PMS例外処理申請書」を使用する場面	
3.4.2.1	個人情報管理台帳に特定しない場合。
3.4.2.3	特定の機微な個人情報の取得に際し、同意を省略する場合。
3.4.2.4	本人から直接書面取得に際し、同意を省略する場合。
3.4.2.5	個人情報を3.4.2.4以外の方法によって取得した場合、本人に通知または公表を省略する場合。
3.4.2.6	本人からの同意を省略して、利用目的の範囲を超えて利用する場合。
3.4.2.7	本人にアクセスする場合に、本人への通知・同意を省略する場合。
3.4.2.8	個人情報を第三者に提供する際に,本人の同意を省略する場合。

「4000PMS例外処理申請書」(一部)

↓該当する項目		↓　に☑すること	201 /　/	201 /　/	201 /　/
□	□ 3.4.2.1 個人情報管理台帳に特定しない場合。(3.4.2.1)	□ 業務マニュアルに取得から廃棄までの手順を規定している。			
		□ BtoBで取得し、利用目的があきらかである。			
		□ その他:			
□	3.4.2.3 特定の機微な個人情報の取得に際し、同意を省略する場合。	□ a)法令に基づく取得である。			
		□ b)人の生命、身体、又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難である。			
		□ c)公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難である。			
		□ d)国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることによって当該事務の遂行に支障を及ぼすおそれがある。			
□	3.4.2.4 本人から直接書面取得に際し、同意を省略する場合。	3.4.2.5のただし書き			
		□ a)利用目的を本人に通知し、又は公表することによって本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある。			
		□ b)利用目的を本人に通知し、又は公表することによって当社の権利又は正当な利益を害するおそれがある。			
		□ c)国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することによって当該事務の遂行に支障を及ぼすおそれがある。			
		□ d) 取得の状況からみて利用目的が明らかであると認められる			
		3.4.2.6のただし書き			
		□ a)法令に基づく取得である。			
		□ b)人の生命、身体、又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難である。			
		□ c)公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同			

■

次回は、「第 24 章　マネジメントシステムの統合化」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

2014.03

支部報告　【　近畿支部第１４３回定例研究会報告（ISACA 大阪支部共催）　】

会員番号　0645 是松　徹(近畿支部)

１．テーマ　：「サポート期限切れＯＳの守り方」

２．講師　　：ネットエージェント株式会社　代表取締役
**　　杉浦　隆幸　様**

３．開催日時：2013 年 12 月 14 日（土）　15:00 ～ 17:00

４．開催場所：大阪大学中之島センター　講義室 301

５．講演概要：

XPサポート終了間近で行うこととして、次の 5 通りの視点から解説いただいた。

真のデッドラインは、2014年4月のサポート終了直後ではなく、クリティカルな脆弱性が顕在化すると見込まれる時点(7 月頃か)と認識すべきとのことである。

① 新しいOSに移行する。
② 互換機能を利用する。
③ 制限利用、隔離利用にする。
④ なんとかしてみる。
⑤ あきらめる。

（１）新しいＯＳに移行する。

ブラウザ、メール、Office2007 以上を利用し特別なソフトはなしという標準的な利用環境では実施が容易で確実な対処方法である。OS移行の選択対象となる Windows8 と Windows7 では、操作の変更が大きいもののサポート期限の長さを含めたセキュリティ面の強度から Windows8 が推奨できる。

OS移行時のチェクポイントとして、専用ハードや旧式ハード等のドライバが動作可能か、アプリケーションやドライバが 64 ビット対応できているか等に留意が必要である。

また、Office2003 も同時期にサポート期限切れとなることを忘れてはならない。

（２）互換機能を利用する。

アプリケーションの互換モード(XPモード)や仮想化環境下で VMware を利用する方法である。VMware 上で動作させる場合には、ネットワーク機能はオフとしOSとのデータ交換をクリップボード経由とすることがセキュリティ面からの留意点である。

（３）制限利用、隔離利用にする。

インターネット、USBメモリを使用不可にする等の制限をかけ、外部からのデータ取り込みは、たとえば書き込み不可であるCDR、DVD－Rを利用するという方法である。隔離環境でのみ利用し、使用終了後も他の環境に移動しないようにする考え方である。

（４）なんとかする。

不要なサービスの停止を徹底する、代替の最新サービスに置き換える、不要なコマンドを削除する等の方法がある。

また、攻撃者が苦手とする傾向にあるパーソナルファイアウォールの活用は効果的な方法であるが、IEや Office2003 以前が存在すると、その脆弱性が狙われる可能性がある。

（５）あきらめる。

OSのセキュリティをあきらめただけで、すべてをあきらめるわけではなく、狙いを絞った対策を打つ考え方である。たとえば機密性確保に主眼を置き、不正侵入があることを前提に、多くの偽情報を本物の情報と混在させて判別を難しくする、デスクトップ・マイドキュメントは空にして TrueCrypt で暗号化したドライブのみ使用する、ネットワーク利用を制限する等により情報流出のリスク低減を図る方法がある。

最終的には、利用者にサポート期限切れのXPを使い続けることは不便であり、Windows8 に移行する方が簡単・便利であると認識してもらうことが重要であると考える。

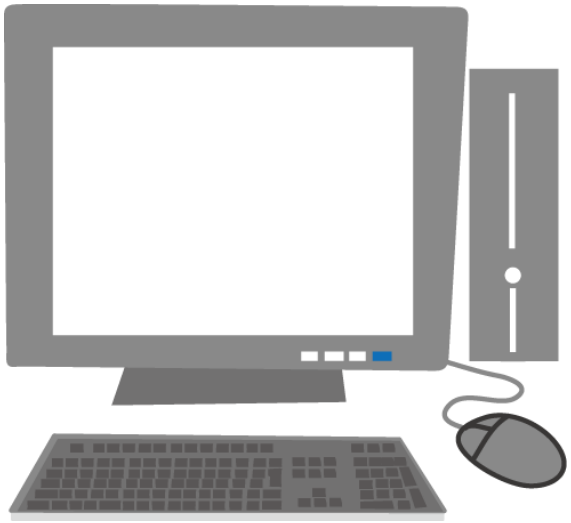
６．所感

間近に迫ったXPのサポート期限切れに向けた具体的な対処方法をセキュリティ確保の観点から多面的にお話いただき、広く普及し情報インフラとなったOSのサポート期限切れ発生時の課題について考える良いきっかけとなりました。

現実として、サポート期限切れまでに新機種への置き換えやOS移行という対策を 100%はとれないという問題があると思います。個人用はもちろんのこと、企業用でもオフィスは比較的順調に対策が進みますが、たとえば工場の生産ラインで使用しているPCの置き換えが進まない等があると思います。この場合、「なんとかする」「あきらめる」の内容が、非常に参考になると感じました。

真に守るべきものを明確にして身の丈にあった対策をとる、リスク受容できるものは受容する割り切りを持つ等のセキュリティの基本的かつ現実的な考え方に立ち戻り、脆弱性満載と言われる環境下でもとるべき手段は多々あることに改めて思い至った次第です。

以上



2014.03

注目情報（2014.02～03）※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。

■警察庁：「平成 25 年中のサイバー攻撃の情勢及び対策の推進状況について」公表

警察庁は、「2013(平成 25)年中のサイバー攻撃の情勢及び対策の推進状況について」を公表しました。

同資料によると、標的型攻撃は、「ばらまき型」攻撃の減少により、前年比大幅に減少したものの、「やりとり型」攻撃の増加、不正な外部接続の発覚を免れようとする手口の出現等、手口が巧妙化・多様化すると共に、周到な準備による計画的な攻撃が見られたとしています。

https://www.npa.go.jp/keibi/biki3/260227kouhou.pdf

■ＩＰＡ：「増加するインターネット接続機器の不適切な情報公開とその対策」公開

独立行政法人情報処理推進機構（IPA）は、オフィス機器、家電製品のインターネット接続に伴う新たな脅威や、不用意な外部公開を SHODAN で確認する手順をまとめたレポート「増加するインターネット接続機器の不適切な情報公開とその対策」を IPA のウェブサイトで公開しました。

http://www.ipa.go.jp/security/technicalwatch/20140227.html

■ＦＩＳＣ：金融機関におけるサイバー攻撃対応に関する有識者検討会報告書のＨＰ掲載

FISC金融システム情報センターでは、「金融機関におけるサイバー攻撃対応に関する有識者検討会」において昨年 6 月から今年 2 月まで、金融機関とその利用者が対応すべき事項の方向性について幅広く議論を行ってきました。今般、当該検討会での報告書をホームページに掲載することにしました。

当センターでは、本検討会での議論ならびに報告書を受けて、今後、関係者と連携して、各種ガイドラインの改訂や金融業界全体のサイバー攻撃対応の促進に向けた実務的な検討を行っていくとしています。

https://www.fisc.or.jp/isolate/?id=686&c=topics&sid=136

■ビットコイン　不正アクセスにより消失相次ぐ

インターネット上の仮想通貨ビットコインの取引所を運営するマウントゴックス社が、不正アクセスにより利用者から預かったビットコインを失ったとして経営破綻し、2 月 28 日、東京地裁に民事再生法の適用を申請しました。

他の業者でも、サイバー攻撃を受けて、ビットコインを失ったとの発表が続いています。

http://www.nikkei.com/article/DGXNASGC2802C_Y4A220C1MM8000/

http://www3.nhk.or.jp/news/html/20140305/k10015721921000.html

■ＩＰＡ：「平成 26 年度春期情報処理技術者試験」の応募者数公表

独立行政法人情報処理推進機構（IPA）。情報処理技術者試験センターは 4 月 20 日（日）に実施する「平成 26 年度春期情報処理技術者試験（経済産業省所管）」の応募者数を公表しました。

それによると、春期試験の応募者数は、前年同期比 94.2%の 182,569 人であり、システム監査技術者試験の応募者数は、前年同期比 91.7%の 4,087 人でした。

http://www.ipa.go.jp/about/press/20140310_2.html

2014.03

【　協会主催イベント・セミナーのご案内　】

■月例研究会（東京）

第190回	日時:2014 年 4 月 25 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	企業 IT 動向調査 2014(13 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(JUAS)　常務理事　浜田達夫氏
	講演骨子	JUAS は、経済産業省 商務情報政策局の監修を受け、「企業 IT 動向調査 2014」を実施いたしました(調査期間:2013 年 10 月～11 月)。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、世の中の動向を俯瞰していきます。
	お申し込み	ご案内とお申込み方法を HP でご案内しています。 (http://www.saaj.or.jp/kenkyu/kenkyukai190.html)

■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/tokubetsu_nintei.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)

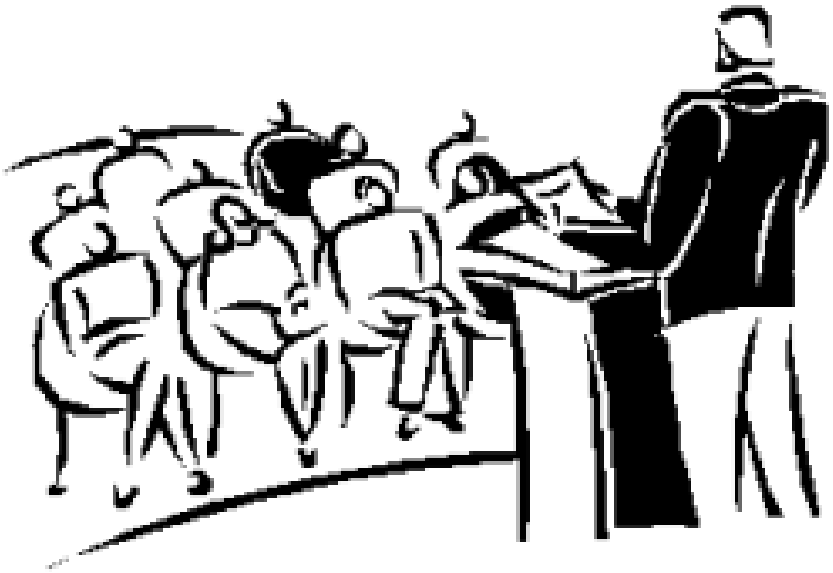
■システム監査サービス（全国）

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　大西(Email:oonishi-satoru@saaj.jp)

2014.03

【　外部のイベント・セミナーのご案内（会報担当収集分）】

システム監査学会　2014 年度第 28 回研究大会	
日時:2014 年 6 月 6 日(金)	
場所	機械振興会館
主催者	システム監査学会
統一論題	IT の進化とシステム監査
参加受付	4 月を予定
案内	http://www.sysaudit.gr.jp/のイベント案内より



2014.03

協会からのお知らせ【「システム監査を知るための小冊子」発行について】広くご活用下さい

会員番号　6005　斉藤　茂雄　（法人部会）

法人部会では、この度システム監査活性化委員会と連携して、「システム監査を知るための小冊子～情報社会に不可欠なシステム監査～」を編集し発行いたしました。

この小冊子の発行は、昨年の「システム監査活性化に向けた提言募集」に法人部会から提案し、採用されたことで実現しました。提案主旨は「システム監査についての疑問、意義、効果、事例などを分かり易く紹介した小冊子を発行することで、システム監査の理解を助け、活性化に繋げる。併せて協会の知名度を向上させる。」でしたが、今回皆様のご協力で、まだまだ改善すべきところはあるものの、概ね意図した小冊子ができあがったと考えております。

小冊子は A5 版表紙込み 36 ページ、中綴じカラー印刷です。全体を「入門編」と「応用編」に分け、右の17のコンテンツを掲載しました。気軽に読んでいただけるよう、なるべく文字を少なめに、様々な視点からシステム監査を述べたつもりです。システム監査初心者から経営層まで、多くの方に読んでいただけるとありがたいと思っております。皆様には、セミナー会場や企業内など、様々な場面で広くお配りいただくと、システム監査の普及、協会の知名度向上に役立つものと考えます。

目　次

入門編

✔ 監査とは　1
✔ システム監査とは　3
✔ システム監査に適用される基準とは　5
～システム監査における判断の拠りどころ～
✔ システム監査人に求められる能力とは　7
✔ システム監査人の思考回路（一例）　9
～チェックリストを超える柔軟さを身近な事例から～
✔ システム監査人を目指すということ　10
～システム監査経験を通じ、将来の能力発揮場面を拓く～
応用編
✔ システム監査への期待　11
✔ 身近な“システム障害管理”　その目的を今一度　13
～システム監査の視点で、経営に貢献する障害管理へ～
✔ システム監査による経済的メリット　15
～東日本大震災の教訓は、具体的な実践になっている～
✔ システム監査は、世の不正とも戦えるでしょうか？　17
～システム監査の知られざる力～
✔ システム開発プロジェクトの成功にシステム監査を　19
～価値観も方法論もPMが実現したいものと合致～
✔ 組織から独立した外部監査の有効活用　21
～大手証券会社の誤発注事例から学ぶ外部監査の必要性～
✔ 個人情報保護とシステム監査　23
～開発と運用の両面で厳しい監査が求められる時代に～
✔ システム監査人の新たな活躍の場としての　25
プライバシー・バイ・デザイン
✔ 情報漏えい防止に有効なシステム監査　27
～自分たちでは気が付かない情報漏えい 防止対策がある～
✔ 効果的かつ安心してSaaSを利用するためのシステム監査の実施　29
～SaaSを利用したビジネスプロセスの整備にもつながる～
✔ 組織内のシステム監査人へ、SAAJからの応援メッセージ　31
～情報システムの点検や改善に取り組むすべての方へ～

最後に、ご執筆いただいた方々、編集にご協力いただいた方々のお名前を記させていただいて、感謝申し上げます。

【執筆・編集ご協力者（五十音順、敬称略）】
梅津尚夫、小野修一、勝田敦彦、
木村裕一、斉藤茂雄、斎藤由紀子、中山孝明、沼野伸生、濱崎元伸、藤野明夫

【編集ご協力者（五十音順、敬称略）】　安部晃生、大石正人、大西智、加佐見明夫、苅田朝子、佐藤京子、
舘岡均、力利則、仲厚吉、早川淳一、松枝憲司

※小冊子は協会 HP からもご覧いただけます。
URL：http://www.saaj.or.jp/csa/system_audit_booklet.pdf

以上

2014.03

協会からのお知らせ　【２０１４年度春期　公認システム監査人及びシステム監査人補の募集】

2014年度春期　公認システム監査人及びシステム監査人補の募集の〔公告〕が協会のホームページに掲載されています。資格取得を企図されている各位はご参照願います。〔公告〕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も、ホームページからお願い致します。

（http://www.saaj.or.jp/csa/csaboshu.html）

---------- 記 ----------

2014年2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年度春期
公認システム監査人及びシステム監査人補の募集について

〔公告〕

特定非営利活動法人日本システム監査人協会（以下、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、制度という）に基づき、「公認システム監査人(Certified Systems Auditor：CSA)」および「システム監査人補(Associate Systems Auditor：ASA)」を認定するため、2014 年度春期公認システム監査人およびシステム監査人補の募集を行います。募集の概要と申請書等の資料の入手方法は、以下のとおりです。

1．認定資格

公認システム監査人およびシステム監査人補とする。

2．申請条件

（1） 認定申請者は、経済産業省が実施するシステム監査技術者（旧情報処理システム監査技術者）試験に合格していること。（制度2（5）特別認定制度に基づく特別認定講習の修了により、上記試験の合格者と同様に取り扱う者を含む）

（2） 公認システム監査人の申請者は、申請前直近6年間のシステム監査実務経験（実務経験みなし期間）が2年以上あること。

3．認定申請

（1） 申請書類（記入方法は、募集要項参照）

公認システム監査人およびシステム監査人補の申請書類は、次表のとおりとする。

申請書類	公認システム監査人	システム監査人補	記事
(1)認定申請書	○	○	様式1
(2)監査実務経歴書	○	－	様式2
(3)小論文	○	－	様式3
(4)宣誓書	○	○	様式4
(5)資格証明（写）	○	○	
(6)申請手数料振込書（写）	○	○	
(7)面接試験	□	－	別途通知

（注1）〇印の資料一式を申請書類として提出する。

（注2）□印については、面接試験を実施する。

備考:公認システム監査人とシステム監査人補を同時申請する場合は、公認システム監査人用の申請書類を提出する。

（2） 面接試験

申請書類審査後、認定委員会が別途指定・通知する日時場所において、面接試験を受ける。

4. 募集期間

2014年2月 1 日（土）～2014年 3 月 31 日（月）（同日消印まで有効）

5. 認定申請手数料

申請手数料	協会会員	非会員
(1) 公認システム監査人認定申請手数料 （注1）システム監査人補と同時申請する場合も手数料は同じです。	21，000円	31，500円
(2) システム監査人補が申請する場合の公認システム監査人認定申請手数料	10，500円	15，750円
(3) システム監査人補認定申請手数料	10，500円	15，750円

6. 資料の入手方法

【個人情報の取り扱いについて】　同意

（1）「公認システム監査人、システム監査人補　募集要項」

ダウンロード（PDF 形式）

（2） 申請書等様式一式

·認定申請書（様式1）:Word 形式

·監査実務経歴書（様式2）:Word 形式

·小論文（様式3）:Word 形式

·宣誓書（様式4）:Word 形式

（3） 公認システム監査人認定制度のダウンロード

·PDF 形式

（4）「公認システム監査人制度」創設のお知らせ（2002 年7月1日）のダウンロード

·PDF 形式

（5） 特別認定講習に関する情報

（・特別認定講習機関認定については参照）

以上

2014.03

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/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。

2014.03

【　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
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	9 日 理事会:通常総会議案審議 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(〆) 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	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〕	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	認定委員会:CSA・ASA 春期募集(2/1～3/31) 5 日 CSA フォーラム 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 13 日 理事会:理事担当	25 日 CSA フォーラム	
4 月	1 日 認定 NPO 法人申請準備開始 10日 理事会	認定委員会:新規 CSA/ASA 書類審査 25 日 第 190 回月例研究会	20 日:2014 年春期情報技術者試験
5 月	8日 理事会	認定委員会:新規 CSA/ASA 面接	

※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」とし、3 か月ごとに「○○○のための」について具体的なテーマ設定して、システム監査に関する皆様からのご意見ご提案を募集いたします。

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」でした。この 3 か月間にご投稿いただいた様々のご意見ご提案、皆様のご参考になりましたでしょうか？

次回発行の 5 月号から 7 月号までの会報テーマは「情報化社会のためのシステム監査」とします。システム監査は情報化社会発展のためにいかにあるべきか等、皆様、いろいろとご意見があろうかと思います。皆様からのご投稿をお待ちしています。

□■ 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。

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、久保木孝明、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）
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━