

いよいよ夏です。

6月に「世界最先端IT国家宣言」改定(案)と「個人情報保護法改正の大綱」という二つの重要な政府発表がありました。[注目情報](#)をご覧ください。



穂高連峰、岳沢から天狗のコルを望む

巻頭言

テーマ: 釧路市の個人情報保護対策に学ぶ

会員番号 1760 斎藤由紀子 (副会長・事務局長)

釧路市では、高齢者が行方不明になったという家族の通報を受けて、FM局から30分おきに氏名、性別、体格、服装、最後に確認された場所を放送します。個人情報保護法の例外規定を適用し「生命を守るためには、本人だけでなく家族の同意なしに第三者に提供できる」と手順を定めたことによるもので、FM局以外にも、タクシー会社、新聞販売店、ガソリンスタンドにも情報が伝達されます。この取組により2013年に釧路市で発生した55人の行方不明者のうち、情報を聞いた一般人による通報が最多で17人が発見されました。全国の行方不明の高齢者が2012年の1年間で9607人、死亡発見351人という悲惨な状況の中で、釧路市の決断は誠に尊いものがあります。

一人暮らしの高齢者が500万人を超え、若者の雇用、子供の健全な発育など社会が抱える問題は山積しています。情報システムに関わる専門職として、経験や知識をどうすれば人の生命や生活を守るために活かすことができるでしょうか。常に意識しなければならない課題と思います。

参考：「認知症行方不明者 1万人 独り暮らしに危険性」NHK2014年4月17日放映



＜目次＞

巻頭言	1
1. めだか	3
	【実現に導く力(情報化社会のためのシステム監査)】	
	【情報化社会を考える(情報化社会のためのシステム監査)】	
2. 投稿	5
	【情報化社会のためのシステム監査】	
	【橋渡しというネットワーク(情報化社会のためのシステム監査)】	
3. 本部報告	8
	【第 190 回月例研究会(2014 年 4 月開催)】	
	「第 20 回企業IT動向調査 2014(13 年度調査)」JUAS 常務理事 浜田達夫氏	
	【情報セキュリティ監査研究会だより その 15 - プライバシー・バイ・デザイン 第 10 回】(連載)	
	「ID連携トラストフレームワーク認証基準案ご紹介」	
	【「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】(連載最終)	
	「第 26 章 プライバシーマーク認定後の維持・運用ポイント」及び「おわりに」	
4. 支部報告	23
	【中部支部 中部支部研究会(5月)報告】(下記、2 件の講演の報告)	
	「特定個人情報保護評価(PIA)について」JIPDEC 電子情報利活用研究部 部長 坂下哲也氏	
	「プライバシー・バイ・デザイン」 SAAJ 情報セキュリティ監査研究会	
	【近畿支部 近畿支部第 146 回定例研究会報告】(下記講演の報告)	
	「ゴルフ場の総合基地化提言」(株)エスシーエイエヌ 代表取締役 中田和男氏	
5. 注目情報	27
	【「世界最先端IT国家創造宣言」改定(案)の公開とパブリックコメント募集(6月3日)】	
	IT総合戦略本部、個人情報保護法改正に向けたパーソナルデータ	
	に関する検討会の大綱案を了承(6月19日)	
6. セミナー開催案内	28
	【協会主催イベント・セミナーのご案内】	
7. お知らせ	30
	【新たに会員になられた方々へ】	
	【協会行事一覧】	
8. 会報編集部からのお知らせ	32
	【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】	

めだか 【 実現に導く力 】

(情報化社会のためのシステム監査)

登山のとき、勾配の路では疲れた体がザックをより重くして、弱音を吐いて立ち止まりたい時が毎回必ずある。農作業のとき、炎天で土にまみれ汗が目に沁み腰が痛くなろうとも、投げ出しちゃあダメだと懸命に気力を絞る。苦しい時にはその先を思う。そうすると自然と力が湧いてくる。苦労を凌ぐ山頂の快感と収穫の喜びがあるからだ。それはほとんど約束されたように得られる。それが信じられるからこそ、辛い歩きも作業も続けられる。これが実現する力の一例だ。例えば、イモ掘りの孫のはしゃぎは他の農作業にも元気を与える不思議な力がある。

「情報化社会のための・・・」というテーマは、システム監査の役割と課題を休みなく考えろ、頭を働かせろと言っているように思う。情報システムの活用形態が大きく変化している状況に目を向ければ、システム監査は今後さらに積極的にチェンジすることや、目標の追加や活発な活動が必要であることに気付く。

目標とそれに向けた活動はもちろんだが、さらにもっと考えるべき大切なことがある。それは「実現に導く力」の必要性だ。「実現に導く力」をお膳立てしてから進めることだ。登山や農作業を引き合いに出すまでもなく、高い目標、苦しいプロセス、実りある成果を実現するためには欠かせない力だ。単なる“頑張りましょう”や“心がけましょう”という合意や確認だけでは、目標設定も掛け声にとどまることになる。

「実現に導く力」は、流した汗と堪えた辛苦を忘れさせ“頑張ってたよかった！”“やってよかった！”と思えるものが生み出す力だ。労苦以上の満足感・喜び・充実感を信じられることが「実現に導く力」の源泉だ。これは卑しいことではない。金銭や物品などではない。心象や内的感覚に作用し影響を与えるもののことであり、ココロやハートをジーンとさせる力のことだ。必要欠くべからざるものであり、NPO の活動精神とも一致する。

NPO の活動・運営が基本的にボランティアであるからと言って、活動成果に対するご褒美や冥利が不要だということにはならない。NPO 活動においては、ややもすればひたすら奉仕を求める一方になるきらいがあるが、人間の活動に報いるものが伴うことは自然な営みといえる。それが内的なものであるなら上限さえも考える必要はない。システム監査の NPO 活動においては、目標の到達状況と活動成果が目に見える形で表れることが少ないために、達成感や満足感を実感しにくい面がある。しかしながらそのメリットが感じられる仕組みを何とかひねり出し用意する必要がある。それが、システム監査を世の中にあまねく普及させるための「実現に導く力」になると考えている。

システム監査の諸活動における「実現に導く力」としては、どのようなものがあるだろうか。いくつかの案も考えられるが、いろいろなアイデアをいただきたいと思う。筆者の意図は、モチベーションやインセンティブとも似ているがちょっとイメージが違ふし、ダニエル・ピンクのやる気や内的動機ともちょっと違ふ。そんなところから、我が身にある実感覚で「実現に導く力」とネーミングした。復唱する。山に登るのはとても苦しい／だけどそれ以上に楽しい、農作業は辛いし痛くなる／だけど孫の笑顔が見られるのなら何でもない。



(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。)

[<目次>](#)

めだか 【 情報化社会を考える 】

情報化社会において、公共機関の情報システムは、システム監査が求められるべきと思う。中でも、個人情報(personal information)を取り扱う情報システム(以下、個人情報システムという。)は、公共機関の利用者や住民個人への公的な各種サービスの提供に当って、法令等への準拠や利用目的への齟齬が生じないよう、構築や保守にシステム監査の法制化を求めたい。

個人情報のデータである個人データは、「“personal data” means any information relating to an identified or identifiable individual (data subject)」である[参考1]。つまり、個人データは、識別された又は識別される個人(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。プライバシーについて、Oxford Dictionary of English では、「privacy; a state in which one is not observed or disturbed by other people」とある。個人が他の人々に観察されたり邪魔されたりしない状況ということである。

ビッグデータは、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、利用者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[参考2]。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。利用者へサービスを提供するプロバイダー側には、解析予測によって無理なくスケジュールを組むことや、利用者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。サービス利用者へは、メリットを短いループで還元することが可能になる。公共機関が取り扱うビッグデータにおいてサービス利用者の個人データを取り扱う場合は、プライバシー侵害が起きることの無いよう対策を講じる必要がある。

公共機関の個人情報システムは、情報システムの法令等への準拠性監査はもちろんのこと、利用目的への有効性監査、情報資産へのセキュリティ監査、等々、様々な観点においてシステム監査が求められるべきである。

一方、情報システム構築の観点から、SE(システムズエンジニア)の健康管理が求められる。健全なる精神は健全なる身体から生まれると言う。情報システムの構築現場も然りである。過労死や過労自殺の防止対策を国の責務で実施する「過労死等防止対策推進法案」が5月27日、衆院本会議で可決された。法案は今国会中に成立する見込みで法案は超党派の議員連盟が提出したと伝えられている。情報システムの構築を担う企業は、過労死等の予防措置に抜本的な取組みが求められており、この分野にもシステム監査が求められるべきである。

[参考1]:「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)」堀部政男、新保史生、JIPDEC(野村至) 仮訳 (JIPDEC)

[参考2]:「ビッグデータの覇者たち」海部美知 (講談社現代新書2203)



(空心菜)

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

[<目次>](#)

投稿【 情報化社会のためのシステム監査 】

会員番号 0557 仲 厚吉 (会長)

情報化社会の昨今、インターネットで、「ドーナツの穴だけ残して食べる方法」や、“eat a donut hole” というドーナツの穴談義が流行っています。アメリカでは6月の第1金曜日がドーナツの日 (National Doughnut Day) になっています。これは、第一次世界大戦のときフランスで従軍するアメリカ人兵士たちに女性ボランティアたちがドーナツを配布したことから、彼らに感謝の意を示すため、1938年に救世軍シカゴ支部がドーナツの日を定めたということです。

ドーナツは、小麦粉に砂糖・バター・卵・ふくらまし粉などを混ぜてこね油で揚げた洋菓子で、リング・ドーナツは揚げるときに熱が通りやすいよう穴があいたいわゆるドーナツ型です。「ドーナツの穴だけ残して食べる方法」は難問で、様々な分野の人から様々な提案があります。例えば工学系だと、ドーナツを一口にかじると穴がなくなってしまうため、外周を削るように食べていく方法を提案しています。他の分野の人はそれぞれの分野の知見でこの難問の意味を問い、方法などを論じたりしています。システム監査人としてこの難問を考えてみました。

システム監査人が取り組んでいる情報システムは、ハードウェアとソフトウェア等が様々に組み合わせられて構成され、それらが相互に働くので、「システム」といわれています。「システム思考」というと、全体を要素に切り分けて把握するだけでなく、要素の相互作用に注目して全体を捉えていこうという考え方です。「システム」は複雑で目に見えないため、システム監査人は、システム管理基準によって、情報システムが、

- ・経営方針及び戦略目標の実現に貢献するか、
- ・目的を実現するように安全、有効かつ効率的に機能するか、
- ・報告する情報の信頼性を保つように機能するか、
- ・関連法令、契約又は内部規程等に準拠性があるか、

等を監査します。システム監査人は、対象になる情報システムを、システム管理基準のチェック項目 (コントロールという) で監査しますが、コントロールに切り分けて適合か不適合かを判定するだけでは、システム監査の手順として不十分だと思います。まず、対象になる情報システムがどのような利用目的で構築されたかなど、全体を捉え、システム監査の方向性や方針を定めて取り掛かる必要があります。

システム監査は、監査対象が様々になっています。情報資産へのセキュリティ監査、会計報告への信頼性監査、個人情報保護法などへの準拠性監査、情報システムの利用目的への適合性監査など、様々なシステム監査があります。システム監査の無い情報システムは穴の無いドーナツのようです。当協会では、情報化社会のためのシステム監査に対応するよう各委員会、部会・研究会、及び各支部の活動があり、ホームページや小冊子に紹介しています。会員の方々にはこれらの活動へより多くの参加をお願いしたいと思います。



資料1:「ドーナツを穴だけ残して食べる方法

越境する学問一穴からのぞく大学講義」大阪大学ショセキカプロジェクト編大阪大学出版会

資料2:「システム管理基準」経済産業省商務情報政策局

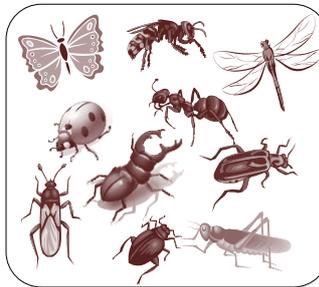
[＜目次＞](#)

投稿 【 橋渡しというネットワーク 】 (会報テーマ：情報化社会のためのシステム監査)

会員番号 1143 中山 孝明

「情報化社会のための・・・」という会報テーマは、見かけ上は情報化社会という“マス(集合体)”を相手にすることのようだが実はそうではない。逆に、マスを構成する“個々”に向き合うシステム監査こそ大切であると考えている。情報化社会と一口でいうがその内容は捉えどころがない。情報システムの利活用が社会の隅々に広まり大衆化した状態を指しているだろうが、それは一つの概念を映し出しているに過ぎない。情報化社会とは即ち“概念”であると見なすと、“個々”に向き合うことの重要性が見えてくる。＜概念:ある事物の概括的で大まかな意味内容。(大辞林)＞

専門外を恐れずに昆虫を例に引けば、昆虫は節足動物と説明されている。節足動物というのは昆虫の概念で、昆虫という言葉自体も総称なのでこれも概念だろう。昆虫観察では、昆虫という概念や総称を相手にするのではなく、個々の蝶や蜂そのものを観察対象にする。蝶や蜂の種類ではなく、個体の地域差や個体差まで含めて一つひとつについて観察する。そういうものだと思っている。たまたま昆虫を例にしたが、マスではなく個々に向き合うことに意味がある点や、右枠内のような多様性を含んでいる点など、そのままシステム監査の環境と酷似していると思う。面白いほど置き換えられるものが多いと思う。情報システムも「生き物みたいなもの」だからだろう。



昆虫観察の経験はないが、次のような多様性があると思う。

- ・種類や形や色、
- ・姿勢や動作や活動の様子、
- ・観察場所の探し方やポイント、
- ・寄生する虫や天敵など、脆弱性と脅威
- ・同種でも地域差や個体差

「情報化社会のためのシステム監査」とは、情報化社会そのものを相手にする監査ではなく、そこで生きている個々の情報システムや組織の一つひとつが、すべからず監査を実施する社会を実現しなければならない。個々のすべてがシステム監査を実施する状態にならなければ、情報化社会は実現しないといっていいたいだろう。その実現のための方策は何か、それを考える。世の中すべてにシステム監査を浸透させるということは、日本システム監査人協会(当協会)が四半世紀前の設立時から活動目的に掲げている「システム監査の普及促進」と変わらない。本質的で永続的なテーマであるが、情報化社会の変遷とあるべき姿の実現のためには力点を移すことが欠かせないと思う。

- ・業務処理の情報システムから、経営活動における情報システムの監査
- ・部門単位のシステム監査から、組織運営におけるシステムリスク管理の監査
- ・組織のためのシステム監査から、マルチステークホルダーのための監査

これらの実現のための方策の一つとして「橋渡しというネットワーク」を論題にした。この「橋渡し」には二面がある。システム監査人(個人及び法人)同士の橋渡しと、システム監査をする側と受ける側の橋渡しだ。世の中にシステム監査を浸透させるには、この橋渡しこそ重要で大きな効果がある。この橋渡しによってシステム監査の普及促進が図られる。「情報化社会のためのシステム監査」は橋渡しというネットワークを機能させることによって実現すると考える。

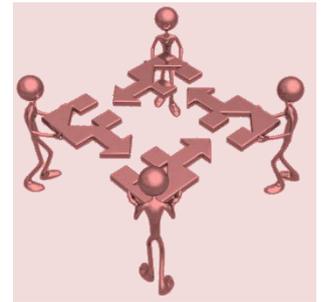
橋渡しネットワークが必要な理由は明解だ。これからの情報化社会においては、システム監査はその能力を最大限結集しなければ期待に応える監査は覚束ない。ここでいう期待とは実は気付いていない期待を含む点が重要だ。監査を受ける側がシステム監査に期待するものは、それこそ概念に留まる傾向が強くなるだろう。現状では定量面でも課題などでも期待を具体的に表現することは難しくなっている。故に、期待に応える監査とはつまり期待以上の監

査を行う必要性を伴う。これからのシステム監査では、個人の監査人や限られた経験の監査組織では手に余る場面や、期待される監査力が確保できないことが発生するだろう。システム監査がその能力を結集することは、期待に応える監査力として必要な態勢であり喫緊の課題でもある。

二面のうち、先ずシステム監査人同士の橋渡しを考える。

システム監査の実施には、例えば、情報システムやリスクマネジメントのノウハウ、意思決定の仕組みなどのマネジメントノウハウ、情報セキュリティやBCPのノウハウなどが求められる。プロジェクト監査においてはプロジェクト構築経験が重視されるかも知れない。システム監査は知識だけでなく幅広い実務経験と、それを実際の監査に結びつけられる技能が必要となる。一方で、個人や個社の監査ノウハウや監査経験には自ずと限界が伴っている。この限界に対して個々が持つ力を組織的に結集して、期待に応える監査を実現するのがシステム監査人同士の橋渡しネットワークだ。この橋渡しネットワークが機能すれば、これからのシステム監査は万能だろう。そして、その仕掛けは身近にもある。

当協会には、自営の監査人や監査企業台帳登録組織や内部監査人、民から官までの各種業種や組織の勤務経験者、実務者や研究者、監査テーマや監査領域の分野別習熟者など、きわめて多くの監査人、多彩な人材を抱えている。その人たちは日々の協会運営にも携わっている。もちろんCSA(公認システム監査人)資格者も含めて、その総力は無限ともいえる。



もう一面の、システム監査を受ける側との橋渡しを考える。

システム監査が当たり前の風土になるためには、システム監査の役割・価値を教科書的に説く前に、乗り越える壁がある。例えば、監査では何を見てどんなこと評価をするのか、監査を受けないとどうなるのか、自分たちに役立つのか、いろいろほじくられたくない、などなどの壁だ。笑って軽視できる壁ではない。この壁には様々な思惑や主張が潜んでいて、実はその見えない部分こそが重要なのだ。この壁を明らかにしつつ乗り越える取り組みが監査を受ける側との橋渡しであり、これは監査をする側の義務でもある。監査を受ける側の発意がなければ監査が実施されない現状では、要するに”その気”が必要だ。特にトップマネジメントに壁があるなら完全払拭が必須だ。監査実施を決定付ける地位にある者との戦いといってもいい。戦いとは衝突などではなく、風土醸成のための我々監査人側からのエネルギーな取り組みのことだ。監査をする側から監査を受ける側(特にトップマネジメント)への橋渡しネットワークが機能すれば、世の中へのシステム監査の浸透はより広く深く確実になるだろう。



「橋渡しというネットワーク」という論題で思うところを述べて来た。情報システムは変貌・拡散を強め、システムリスクは不確定と不明瞭を増している。この認識から、システム監査が総力を結集してことに対処する必要性を強く感じている。併せて、当協会の持つ力の大きさも認識を新たにしている。情報化社会というものをつらつら思うなかで、逆に個別に対する取り組みを考えている。

以上

第190回 月例研究会 (2014年4月開催)

会員番号 1690 梅里悦康 (月例研究会)

【講演テーマ】第20回 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

【日時】2014年4月25日(金曜日) 18:30~20:30

【場所】機械振興会館 地下2階ホール

【講演骨子】

一般社団法人 日本情報システム・ユーザー協会(略称:JUAS)は、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。

JUASのホームページ

<http://www.juas.or.jp/servey/it14/index.html> 参照

調査の内容の詳細は、JUASから「企業IT動向調査報告書2014 ユーザー企業のIT投資・活用の最新動向(2013年度調査)」(発行:日経BP社2014年4月24日)として発行されています。

I. 企業IT動向調査2014(2013年度調査)の概要**1. 調査の方法**

(1) アンケート調査

- ・実施時期 13年11月
- ・ユーザー企業IT部門 4000社対象、有効回答:1016社(回答率:25%)

(2) インタビュー調査

- ・実施時期 13年11月~14年1月
- ・ユーザー企業IT部門長:47社

2. 調査の重点テーマ

(1) 転換期に求められるIT部門の役割とは

- ・企業を取り巻く環境が激変しています。このような時代では、ユーザー企業のIT部門は、従来に増して全方位的な役割が求められています。クラウドやビッグデータなど多様化するIT環境への対応、巧妙化するセキュリティ脅威への対策、さらには、ビジネスイノベーションを誘発するIT活用の提案といった経営に直結する役割も求められるようになってきます。当然のことながら、既存のシステムの保守・安定運用なども手を抜くことはできません。
- ・しかし、こうした高度化・複雑化する要求に応えるには、課題も多いのが現状です。情報子会社やパートナー企業も含めたIT推進体制のあり方、幅広い分野の目利き力を備えた人材の育成方法、グローバル化への対応など、理想と現実のギャップを感じている企業も少なくないでしょう。
- ・こうした転換期における課題解決の一助となるために、今回の調査(2013年度調査)では調査項目を一新しました。IT投資マネジメント、システム開発の実態やIT組織、IT人材などの定点観測は残しつつ、新たな観点を追加しました。さらにビッグデータやビジネスイノベーションなどの調査項目をさらに拡充しました。

3. 調査結果の構成

- ・調査結果は、以下のように構成されています。

(1) 回答企業のプロフィール

(2)トピックス

①ITトレンド(ビックデータ)

②IT 基盤

③クライアント環境

(3)重点テーマ

①IT投資マネジメントとビジネスイノベーション

②システム開発

③IT推進組織・IT人材

(4)定点観測

①IT予算

②IT投資マネジメント

③情報セキュリティ

II. 調査結果

・調査結果の各調査項目について、特徴的な内容を抽出し、記述します。

1. 回答企業のプロフィール

・調査対象は、東証一部上場企業とそれに準じる企業の計 4000 社で、各社のIT部門長に調査票を郵送して、1016 社の回答を得ました。業種グループ、従業員数、売上高で分類すれば、次のとおりです。

(1)7つの業種グループ

・業種は、日本標準産業分類を参考に定めた「26 業種」に1業種を加え「27 業種」とし、業種の特徴を把握するため更に「建築・土木」、「素材製造」、「機械器具製造」、「商社・流通」、「金融」、「社会インフラ(※12 年度より「重要インフラ」から「社会インフラ」に変更)」、「サービス」の「7つの業種グループ」にまとめて分析しています。

(2)回答企業の従業員数

・大企業(1000 人以上)が 1/3 強(33.8%)、中堅企業(300~1000 人未満)が 1/3 強(34.2%)、中小企業(300 人未満)が 1/3 弱(32.0%)でほぼ同じ割合です。

(3)回答企業の売上高

・売上高「10 億円未満」(2.7%)、「10 億円~100 億円未満」(26.8%)、「100 億円~1000 億円未満」(47.3%)、「1000 億円~1兆円未満」(18.9%)、超大企業「1兆円以上」(4.4%)となっています。この売上高1兆円以上の超大企業(4.4%)を分析すると今後の動向が見えます。

・「サービス」は、売上高100億円未満が半数(53.9% = 「10 億円未満」(6.0%) + 「10 億円~100 億円未満」(47.9%))と規模の小さな企業が多いです。

(4)業種グループと主たる商品・サービスの取引形態

・非製造業(商社・流通、金融、社会インフラ、サービス)では企業向け、一般消費者向け双方にビジネスを展開している企業の割合が高いです。

(5)主たるビジネスモデルとITの位置づけ

・特に金融において「ITなしではビジネスモデルが成り立たない」と回答した割合が顕著です。

2. トピックス

(1)ITトレンド(ビックデータ)

①新規テクノロジーやフレームワークの導入状況

・「基盤系テクノロジー」「アプリケーション」「サービス」「方法論・フレームワーク」に分類しています。

②ビッグデータへの取り組み状況

・大企業中心に活用が進むと考えられます。2割(22.1%)の企業で「未検討(ニーズあり)」です。一方で約半数(52.9%)が「未検討(ニーズなし)」です。ビッグデータのニーズが必ずしも顕在化するわけではなさそうです。

・ビッグデータの活用状況:現状、今後(3年後)の予測では、「導入済み」が10.0%、「試験導入中・導入準備中」が12.0%、「検討中」が23.5%となり、検討中を含めると45.5%の企業が検討までの段階に進みます。

・売上高別ビッグデータの活用状況(現状):売上高1兆円以上の企業は検討中までの比率も極めて大きく、ビッグデータの活用も大企業から進んでいくと考えられます。

※本調査では、ビッグデータを、単にデータの量が巨大なだけでなく、多様性があり、処理の速さも求められ、処理の複雑性も高い対象(センサー情報、ソーシャルメディアの投稿、ネット上の写真や映像など)から、ビジネスへの貢献に役立つ情報を得ることと定義しました。

③ビッグデータへの取り組みでの最大の課題(1位、2位、3位)

・最大の課題は「導入する目的の明確化」(45.6%=1位:27.3%+2位:12.0%+3位:6.3%)です。なお、導入が進むにつれて課題は具体化し、「人材(データサイエンティスト)の育成」(27.3%=1位:10.7%+2位:9.5%+3位:7.1%)「データ分析・活用のための体制/組織の整備」(37.5%=1位:10.9%+2位:14.6%+3位:12.0%)の割合が高くなります。

(2)IT基盤

①クラウド導入状況

・IaaSは踊り場から利用へと加速します。一方PaaSはIaaSほどの伸びはないです。いずれも5年間、導入済み企業は順調に増加しています。

・すなわち、年度別パブリッククラウド(IaaS、PaaS)導入状況にて、IaaSでは前回調査(12年度)に比べて「導入済み」の割合が8.3ポイント(8.3%=19.4%-11.1%)、「検討中」は1.9ポイント増加(1.9%=19.5%-17.6%)しています。前回は、導入の伸びが鈍ったことから踊り場にあると見ていましたが、今回の調査では利用する方へ加速しているといえます。一方PaaSは、導入済み企業は前回より増加(1.8ポイント増加)(1.8%=12.6%-10.8%)しているものの、IaaSほどの伸びはないです。導入は進んでいるものの、勢いは鈍いです。

※自社構築できる体力があり自由度を求める場合はIaaS、コストを抑えて短期間で使用開始する場合はSaaS、と棲み分けられる一方で、その中間的な位置づけにあるPaaSは選択しづらい状況にあるのではないですか。

(3)クライアント環境

①Windows XP対応

・全体の約90%(89.2% = 「2014年4月9日までに対応完了(予定を含む)」49.1% + 「対応予定だが、2014年4月9日以降にずれ込む」40.1%)の企業が課題として真摯に受け止め取り組んでいます。多くのロードや多額の費用を要することから、全体の約40%(「対応予定だが、2014年4月9日以降にずれ込む」40.1%)の企業が2014年4月9日までは間に合いません。

・2014年4月9日に間に合わない企業からは対策として「Windows XPをサポートするウイルス対策ソフトを使用する」といった声がありますが、これだけでは十分ではないです。今後発見されるWindows XPの脆弱性の穴には対応できない可能性もあり、ウイルス対策ソフトの過信は危険です。もしもWindows XPの脆弱性を狙った攻撃を受けた場合、自社のみならず、他社にも迷惑を及ぼす可能性もあります。Windows XPをサポート終了後も使い続けることがリスクを高めることを認識した上で、もう一度リスク対策を見直し、Windows XPの移行完了時期の見直しも含め、サポートがあるOSへの早期の切り替えが必要と思われます。

②クライアントOS

- ・クライアント OS の導入割合(導入比率の単純平均)では Windows XP 以前が大幅に減少し、Windows 7 が躍進しています。最も多い OS は、初めて「Windows 7」(49.7%)が Windows XP 以前(44.9%)を上回る結果となりました。
- ・2009 年 9 月に販売開始された「Windows 7」は、過去の企業 IT 動向調査の結果によると、導入企業の割合が 09 年度は 4.1%、10 年度は 35.5%、11 年度は 62.3%、12 年度は 80.0%、13 年度は 93.2%と大幅に増加しています。
- ・2012 年 8 月に販売開始された「Windows 8」は、導入企業の割合が 12 年度は 1.9%、13 年度は 15.2%でした。

③スマートフォン・タブレット端末導入状況

- ・導入企業は年々増加し、13 年度にはいずれも 4 割弱(スマートフォン「導入済み」37.3%、タブレット「導入済み」36.3%)の企業が導入済みです。
- ・企業規模が大きいほど導入に積極的です。すなわち、「未検討」に着目すると、従業員数が大きくなるにつれて割合が下がる(スマートフォン:「300 人未満の企業」(33.2%)⇒「1000 人以上の企業」(18.6%)、タブレット:「300 人未満の企業」(30.4%)⇒「1000 人以上の企業」(9.5%))ことから、規模の大きな企業がスマートフォンやタブレット端末の導入を積極的に検討していると考えられます。
- ・ただし、別途調査した導入台数の規模を見ると、大規模な導入を行っている企業は限定的です。

3. 重点テーマ

(1) IT 投資マネジメントとビジネスイノベーション

① IT 部門が IT 投資で解決したい中期的な経営課題(1 位～3 位)

- ・IT 投資で解決したい中期的な経営課題(1 位～3 位)では、「迅速な業績把握、情報把握(リアルタイム経営)」(38.6% = 1 位:22.1% + 2 位:7.3% + 3 位:9.2%)と「業務プロセスの効率化(省力化、業務コスト削減)」(50.5% = 1 位:19.2% + 2 位:20.3% + 3 位:11.0%)が圧倒的に高く IT 投資の二本柱です。
- ・IT 投資の前提となる経営課題を見ると、「業務プロセスの効率化」(上記 50.5%)、「リアルタイム経営」(上記 38.6%)、「営業力の強化」(25.6% = 1 位:8.2% + 2 位:9.5% + 3 位:7.9%)、「IT コスト削減」(24.4% = 1 位:8.1% + 2 位:6.7% + 3 位:9.6%)、「業務プロセスの品質向上」(23.5% = 1 位:4.8% + 2 位:8.6% + 3 位:10.1%)と全業種を通じた上位 5 傑は例年と変わらないです。

② IT 投資における中期的な重点投資分野

- ・「顧客情報・営業支援(SFA、CRM等)」(40.1% = 1 位:18.6% + 2 位:11.9% + 3 位:9.6%)、「生産・在庫管理」(33.1% = 1 位:18.4% + 2 位:8.9% + 3 位:5.8%)、「販売管理」(32.2% = 1 位:15.9% + 2 位:10.7% + 3 位:5.6%)、「経営情報・管理会計」(32.2% = 1 位:12.8% + 2 位:12.0% + 3 位:7.4%)、「グループウェア・社内情報ポータル」(28.2% = 1 位:5.6% + 2 位:10.3% + 3 位:12.3%)が上位で、解決したい経営課題にほぼ対応しています。
- ・3 位に着目すると、最も回答が多いのが「セキュリティ強化(14.2%)」、「BCP(事業継続計画)12.3%」です。最優先ではないものの、重点投資分野の一つとして位置づけていると考えられます。
- ・主たる商品のビジネスモデル別に見ると、BtoB 企業と BtoC 企業では、解決したい経営課題の違いを反映して、IT 投資の重点分野においてもやはり大きな違いがあります。

③ 攻めと守りの投資配分

- ・まず、IT 予算を「現行のビジネスや業務の維持・運営のために要する(ライセンス切れや保守切れによるリプレースも含みます)情報システムの予算」(以下「ラン・ザ・ビジネス予算」と、「事業拡大や新規事業を実現するために要する情報システムの予算(以下「バリュー・アップ予算)」と分けて考えることとします。
- ・調査結果は、バリュー・アップ予算はラン・ザ・ビジネス予算を大きく下回りました。全体平均でみると両者の比率はおおよそ 2:8(平均値は、バリュー・アップ予算 20.9%、ラン・ザ・ビジネス予算 78.9%)です。企業経営にとって、情報システムとは安定した業務やビジネスの基盤であってみれば、この比率は十分理解できます。

・将来に向けては、ラン・ザ・ビジネス予算の比率を低減する中でIT投資の重心をバリュー・アップ予算に移して行こうという、明らかな意図がうかがえました。

・以上、現状は攻め(バリュー・アップ)2割、守り(ラン・ザ・ビジネス)8割で、将来に向け、厳しい予算制約の中でラン・ザ・ビジネス予算の比率を低減し、IT投資の重心をバリュー・アップ予算へ移す意向です。

④EA導入状況別ビジネスの新しい施策展開のためのIT投資割合(現状)

・IT資産の計画的管理のための方策として、ここではエンタープライズアーキテクチャー(EA)に注目する。EAを導入した企業(バリュー・アップ投資配分「EA導入済み企業」平均28.4%)とそうでない企業(バリュー・アップ投資配分「EA未検討企業」平均19.3%)の間で、バリュー・アップ投資配分に明確な差が認められ、EAは重要な役割を果たすと考えることができます。

・興味深いのは、EAを導入済または準備中の企業の方が、IT部門から経営や事業部門に対して様々な提案を行う仕組みを導入している企業の比率が大きくなるということです。ITによるイノベーションを推進するためには、その他にも様々な仕組みが必要ですが、EAを導入することはそうした仕組みづくりを推し進めることと強く関わっていることが見てとれます。

・将来的にIT予算の配分を「守り(ラン・ザ・ビジネス予算)」から「攻め(バリュー・アップ予算)」に重点をシフトするためのIT投資マネジメント基盤として「IT資産の計画的管理」、「財源確保の取組」、「ITマネジメント人材の拡充」が必要です。

⑤ITを活用したイノベーション

・従業員数別ITを活用したイノベーションへの取組状況(実施している企業の割合)では、イノベーションの実現におけるIT部門に対する期待も企業の成長と規模(従業員規模)の拡大に伴って大きくなってきます。

・企業規模が大きくなってくると効率的に業務を行うためにITは欠かせないツールとして、その提供を担うIT部門の技術力に期待が高まるのは当然と言えます。複雑化し専門分化した大企業にあつては、部門の枠を越えた業務知識や要求を明確にすること、そして内外の資源を連携することまで、期待の幅が広がってくる実態が見て取れます。

・以上、従業員規模が大きくなるにつれ、改革に取り組む企業の割合も増加し、企業の成長に伴って事務などのオペレーションのプロセスが複雑化し、変革が必要になることを示唆しています。

(2)システム開発

①システム開発への事業部門の参画度

・システム開発への事業部門の参画に関するIT部門の評価として高かったのは「テストへの参加」(5点満点にて平均3.0点)です。逆に、低いのは「要件定義に関する主体性」(5点満点にて平均2.3点、レベル1:「部門が手取り足取り」⇔レベル5:「事業部門が主体的に実施」と「事業部門の要件定義スキル」(5点満点にて平均2.3点、レベル1:スキル不十分⇔レベル5:必要なスキルを充足)でした。

・開発成否に影響を及ぼす、事業部門の参画に関する事項(1位~3位)では、「現行業務仕様の把握」(1位:38.7%)、「要件定義に関する主体性」(1位:34.2%)が1位の割合が高いです。

・以上、IT部門は事業部門の要求を正しく把握し、システム開発を行う必要がありますが、そのためにはまず事業部門がしっかり要件に主体性を持って提示できるかがカギとなります。

②開発手法の活用状況

・全般的にウォーターフォール型の開発手法が依然として主流(「基幹系」:75.5%、「業務支援・情報系」:64.1%、「Web・フロント系」:55.1%、「管理業務系」:72.7%)です。

・「プロトタイプング・反復型」は、いずれの業務システム分野でも2割以上(「基幹系」:20.1%、「業務支援・情報系」:28.8%、「Web・フロント系」:33.0%、「管理業務系」:21.7%)の採用です。WEBサイトの構築や、小規模な業務システム開

発案件では適用が広がっていると推察します。

・各開発手法に期待する効果として、品質重視であれば手堅くウォーターフォール(「品質向上」:68.4%)です。開発スピードの向上に期待がかかるアジャイル(「開発スピードアップ」:52.0%)です。「プロトタイピング・反復型」は、その中庸策(「品質向上」:30.0%、「開発スピードアップ」:42.0%)です。

・以上、ウォーターフォール型開発手法が依然として主流ですが、「プロトタイピング・反復型」の適用もみられ始めています。アジャイル手法の活用はまだ限定的です。

(3)IT推進組織・IT人材

①今後の IT 機能別の役割分担

・今後、従業員 1000 人以上の大企業では、IT 戦略策定(「IT 部門」:85.8%)と戦略実行の役割分担が進むと予測されます。従来の業務を情報子会社やベンダーに移管し、IT 部門の時間をより戦略策定に割けるようにするとみられます。

・「③設計・開発・テスト」(「IT 部門」:31.5%)、「⑤システム運用」(「IT 部門」:34.7%)、「⑥システム保守」(「IT 部門」:34.0%)、「⑨ヘルプデスク」(「IT 部門」:37.1%)に加え、「⑩情報セキュリティリスク管理」(「IT 部門」:76.7%)、「⑪その他 IT マネジメント」(「IT 部門」:79.1%)などにおいても、情報子会社やベンダーへの委託が進んでいくことが見受けられます。

・また、情報子会社は IT 部門の一部として、今後は IT 部門の役割を共に担う存在になっていきます。

②情報子会社の保有状況

・全体の傾向は、際立った変化はないです。6年前の08年度からあまり変化はなく、全体では約2割(19.9%＝「情報子会社あり(経営権あり)」:17.2%+「情報子会社あり(経営権なし)」:2.7%)、従業員数 1000 人以上の企業では約4割(38.8%＝「情報子会社あり(経営権あり)」:35.4%+「情報子会社あり(経営権なし)」:3.4%)が情報子会社を保有している状況です。

③IT 部門の年齢構成

・4人に1人が65歳以上という超高齢化社会の中、IT部門でも高齢化が進行中です。現状に危機感を抱き、新規採用や人事ローテーション等の対策を講じている企業との差が明確になりつつあります。

・IT部門「40代以上の層が多い(シニア中心型)」:52.3%、情報子会社「40代以上の層が多い(シニア中心型)」:30.9%で、最も比率が高かったのは、40代以上の層が厚いシニア中心型です。

④業種グループ別 IT 部門の年齢構成と設立年数別 IT 部門の年齢構成

・業種グループ別 IT 部門の年齢構成では、金融(65.2%)、建築・土木(59.5%)、素材製造(58.2%)、機械器具製造(55.7%)、社会インフラ(53.7%)では、「シニア中心型」が半数を超えています。

・設立年数別 IT 部門の年齢構成では、40代以上の層が多い(シニア中心型)は「設立して5年以上30年未満」(31.9%)、「設立して30年以上60年未満」(50.2%)、「設立して60年以上90年未満」(56.5%)、「設立して90年以上」(61.8%)です。

・いずれの業種グループでも40代以上の層が多い「シニア中心型」が高い比率を占めています。会社の設立年数と IT 部門の年齢構成の相関性も強く、設立年数が長い企業ほどシニア中心型の割合が増加しています。

⑤人材タイプ別 IT 部門要員

・開発、運用の現場が情報子会社へシフトしたり、クラウドなどの利用により「作らずに使う」システムが増加する中、IT部門でも IT 部門要員に求められる役割が変わりつつあります。

・「①業務改革推進担当」のDI値は21.6、「②IT戦略担当」はDI値21.1、「③システム企画担当」はDI値21.0と増加志向が明らかです。(※記録者注:DIとはDiffusion Indexの略で「増加割合」-「減少割合」です。)

・一方で、「⑤開発担当」のDI値は▲4.3、「⑥運用管理」はDI値▲6.1、「⑦運用担当」はDI値▲11.2、「⑧ヘルプデス

ク担当」はDI値▲5.9と減少志向でした。

・全体の傾向として、今後、IT部門の要員を業務改革や戦略・企画領域にシフトさせようとする企業の意向が顕著に表れています。

・今後の方向性は人材タイプごとに異なり、業務改革推進、IT戦略担当、システム企画を増加させ、開発、運用、ヘルプデスクは減少を志向します。IT部門をより上流へシフトさせようとする意向です。

⑥従業員数別業務改革推進担当の今後の方向性

・業務改革推進を担う人材をいかに増やすかが大きな課題です。規模に比例して増員意欲は顕著で、従業員数1000～4999人の企業は40.2%、5000～9999人の企業では54.3%、10,000人以上の企業は60.6%が各々増加しています。

・それでは実際にどうやって育成を行うのか別途調査しました、「①業務改革推進担当」の育成に有効な施策としては、「事業部門への異動による実務経験付与」を挙げる企業が多い(57.3%)です。

・なお、情報子会社を持つ企業では開発の現場に近い部分を担当するタイプ(開発担当、運用管理、運用担当など)の育成方法として「情報子会社との人材ローテーション」の占める割合が高くなります。

4. 定点観測

(1) IT予算

①IT予算の現状と今後の見通し

・14年度の予測のDI(※記録者注:DI:Diffusion Index:「増加割合」-「減少割合」)値12.6は2008年のリーマンショック以降、最大の値となっています。予測のDI値の動きは、10年度のDI値▲4.0を底に、13年度は4.2と減少するものの、漸増傾向(10年度:▲4.0、11年度:6.4、12年度:8.1、13年度:4.2、14年度:12.6)が続いています。IT予算の実績を反映している計画値の推移を見ても09年度以降、IT予算の増加傾向(10年度:▲9.0、11年度:6.0、12年度:1.7、13年度:13.5、14年度:-)は確認できます。

・以上、13年度の計画のDI値は13.5、IT予算を増やす企業が大幅に増加しています。14年度の予測のDI値は12.6、IT予算を増やす企業数は引き続き増加が見込まれます。

②売上高に対するIT予算比率

・単純平均で12年度1.20%、13年度1.23%です。13年度は売上高の伸び以上にIT予算を伸ばした年です。IT予算比率はIT装置産業といわれる「金融」が12年度5.04%、13年度5.07%と突出しています。

(2) グローバルIT戦略

①企業のグローバル化

・売上高別ビジネスのグローバル化の現状:海外市場の開拓は、幅広い層の企業にとって成長を維持するために不可欠な戦略となっています。

・業種グループ別業務プロセスの共通化の状況:目指すべき姿は企業規模や事業内容によって異なりますが、グローバルでの業務プロセスの共通化は、短期に解決できるものでもなく、長期に渡る課題といえます。

・上場企業の51.2%は既に海外進出済みです。売上高1000億円以上の企業では4社に3社(1000億円以上～1兆円未満:73.4%、1兆円以上:74.4%)が海外へ進出しています。そのうち、業務プロセスの「共通化」または「共通化の予定」は約6割(57.5%＝「全世界で共通化済み」:5.9%+「全世界で共通化の予定」:12.6%+「地域ごと(中国、アジア、米州、欧州など)に共通化済み」:15.1%+「地域ごとに共通化の予定」:23.8%)です。

②グローバルでのITガバナンス

・現状は「海外の事業拠点に任す」「特に行わない」が大半です。

・今後はセキュリティ(69.4%＝「グローバルで管理・標準化」:53.0%+「地域ごとに管理・標準化」:16.4%)やコンプライアンス(69.5%＝「グローバルで管理・標準化」:52.4%+「地域ごとに管理・標準化」:17.1%)、次にIT戦略(64.9%＝「グローバ

ルで管理・標準化」:44.7%+「地域ごとに管理・標準化」:20.2%）、予算(56.5%＝「グローバルで管理・標準化」:32.4%+「地域ごとに管理・標準化」:24.1%)、さらには IT 基盤(60.3%＝「グローバルで管理・標準化」:35.0%+「地域ごとに管理・標準化」:25.3%)、業務システム(57.7%＝「グローバルで管理・標準化」:30.8%+「地域ごとに管理・標準化」:26.9%)・情報(マスターやコード体系)(58.3%＝「グローバルで管理・標準化」:36.9%+「地域ごとに管理・標準化」:21.4%)を目指します。

・ビジネスのグローバル展開を IT の活用で推し進めようとする中、従来の個別最適からグローバル、もしくは地域での全体最適へ向けた筋道を描いているようです。

・以上、セキュリティやコンプライアンスで「グローバルで管理・標準化」または「地域ごとに管理・標準化」の傾向が強いです。まず守りの領域をしっかり固め、最低限の企業ブランドを保護する意思表示ですか。

(3) 情報セキュリティ

① 情報セキュリティ対策

・標的型攻撃の手口は従来のメールを発端とする攻撃にとどまらず、攻撃対象の利用者がよく利用する Web サイトにウイルスを感染させた上で待ち伏せるなど、多様化しています。高度化する攻撃への対策を実行推進する人材の確保や社内ネットワーク上の怪しいデータの挙動を分析・検知するソリューションの導入等が大きな課題となっていると思われます。

・以上、不安が大きい情報セキュリティ対策の自己評価です。ほとんどの項目に対して対策が大幅に不足しています。

② 情報セキュリティ対策の企業グループでの取り組み

・情報セキュリティ対策の企業グループでの取り組みでは、「完全にグループ全体を対象としている」は約 4 割(39.6%)です。

・情報セキュリティ事故の影響度別に情報セキュリティ対策の企業グループでの取り組みを見ると、「完全にグループ全体を対象としている」は、「部分的に影響がある」:26.3%、「大きな影響がある」:43.6%、「企業の存続に関わる影響がある」:55.6%です。同じグループでも、企業によって規模やセキュリティリスクは異なります。体力的に親会社や大規模な企業と同じ対策を打てない企業もあるでしょう。しかし、セキュリティ問題が顕在化すると、グループ全体に波及します。今後、グループ全体でセキュリティ対策を進めていくことがさらに求められてくるでしょう。

・以上、「完全にグループ全体を対象としている」は約 4 割(39.6%)です。情報セキュリティ事故の影響度別に見ると、インパクトが大きいほどグループ全体での取り組みが進みます。

Ⅲ. 質疑応答

1. IT 部門の欠かせないものは若手人材の確保育成

質問:調査結果において IT 部門の一番かかせないものは何ですか?

回答:いろいろありますが品質等がやはりポイントです。経営、ビジネスにイノベーションの提案することがいわれています。どう対応するか人材の問題があります。人員の年齢構成高いことです。従来型で若手が入らないです。IT 部門長に話を聞くと、「ベテラン層は過去の言われた通り開発をした成功体験があり、どうやって意識改革をするのか、併せて若手人材を確保育成するかが課題」です。

2. IT 部門の一元的把握と理解力不足を補完しイノベーションするために内部・外部とのコラボレーション

質問:経営者はイノベーションを実現する IT 人材を必要としています。しかし、IT 人材のスキルはプログラム開発、ネットワークのスキルです。ビッグデータに係わるデータサイエンティスト人材とビジネスイノベーションに係わる人材は、従来までの IT 人材のスキルと異なります。両者のギャップを企業側はどう解決していますか。

回答:調査データによると、IT 部門は技術力、要求定義力に強みがありますが、情報の一元的把握と理解力が弱いです。本来、社内要求と社外要求を理解することとこれらを分析して事業にどうゆうふうに使われるべきかを把握すること

が求められています。これが弱いのです。これに対していろいろ模索しています。提案するため他の部門と共同組織を作ること、社外と連携し外部とコラボレーションして生み出すことが行われています。このように IT 部門は内部・外部とコラボレーションしています。今後、そのうち成果がでて、成功事例が出てきます。コラボレーションがキーです。

3. 要件定義は業務要件のこと、要件定義の決定は CIO と IT 部門長の仕事、トップの考え方を反映すること

質問: 要件定義は、業務の要件ですか。それとも、システム要件ですか。IT がうまくいかないのは、業務部門の管理で業務要件がきちんとできているか、そもそもどのような要件定義をするかにかかっています。QTC がくずれ、普通、プロジェクト開始してから要件が変わってしまいます。要件定義はそもそも正しいか分析していますか。

回答: 要件定義は、業務の要件です。要件がそもそも正しいのか、業務要件、そこに戻る必要があります。確定した内容がビジネス部門の部門長の決裁を受けたものでしょうか。とりあえず、システム開発し最後土壇場に「こんなシステムを何で作ったのか。」と言われる。これにより開発が振出しに戻ることがあります。結果から見るとオーソライズしていない要件定義で開発が始まるのが問題です。これは CIO と IT 部門長の仕事です。ビジネス部門・業務部門の役員の決裁を受けること、ステアリングコミティにビジネス部門の部門長を、プロジェクトメンバーにビジネス部門のキーパーソンを専任にてアサインすること、トップの考え方を反映すること、いろいろ必要です。

4. 経営目的に合致しているか否か監査することに重要性増加

質問: 監査の面で、私どもは準拠性監査がメインです。経営目的とりわけ目的型監査の重要性が増してきましたか。

回答: 今後、経営目的に合致しているか否か監査することに重要性が増しています。経営と IT が近くなっています。このシステムの評価は経営目的の観点で、経営とどこまで合致しているかです。まさしくその通りだと思います。

IV. おわりに

・当講演録は配布資料と対比してみるように記述しました。月例研究会に参加されなかった方は、ぜひ配布されたレジュメを取り寄せてご覧ください。なお、今回の講演は、ビデオの撮影はしていません。資料は配布されたレジュメのみです。講演の中で、レジュメのほかに配布されていない資料が示されましたが、これらの内容についてもこの講演録には含んでいません。

・前年度の講演録【第 180 回月例研究会報告】(日時: 2013 年 4 月 24 日(水)、議題: 「企業IT動向調査 2013(12 年度調査)～データで探るユーザー企業のIT戦略～」)を合わせてお読み下さると経年変化等について、より理解が深まります。

SAAJのホームページ:

http://skansanin.com/saaj/201307/201307SAAJKaihoNr148_monthly.pdf 参照

・詳細の内容は、発刊されている「企業IT動向調査報告書 2014」をお読みいただきたいと思います。(記録者追記)

以上

【情報セキュリティ監査研究会だより その15 - プライバシー・バイ・デザイン 第10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な潮流」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、2013年8月から議論しております。

本年度5月号から、「プライバシー・バイ・デザイン」の一実現形態であり、また、システム監査人の新たな活躍の場になる可能性がある「ID連携トラストフレームワーク」のご紹介を開始し、5月号は、その概要、6月号は、日米の先行事例をご紹介いたしました。本号では、3月にJIPDECが発表したトラストフレームワーク参加事業者の認証基準案をご紹介したいと思います。このなかで、システム監査人の新たな活躍の場として期待される、認証にあたる「審査人(監査人)」の能力基準についてもご紹介いたします。

なお、6月号でご紹介した米国における先行事例、Identity Credential and Access Management、“ICAM”の紹介の図に、誤りがありましたので訂正させていただきます。会報6月号の9ページ、図3、TFP(トラストフレームワーク・プロバイダ)がRP(リライディング・パーティ)である政府機関を認定する矢印が出ていますが、政府機関は認定する必要がありません。この矢印を削除していただきたいと存じます。誤った情報を提供しましたこととお詫び申し上げます。

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と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思います。ご興味のある方は、毎月20日前後に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](mailto:security☆saaj.jp) (発信の際には“☆”を“@”に変換してください)

【参考資料等】**<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な潮流」、2012年10月、日経BP社

<資料1> 経済産業省「ID連携トラストフレームワーク概要」

http://www.meti.go.jp/policy/it_policy/id_renkei/tf_gaiyou.pdf

<資料2> 2014年3月14日開催、経済産業省主催シンポジウム「アイデンティティ連携が生み出す社会」資料

http://www.meti.go.jp/policy/it_policy/id_renkei/0314symposium.pdf

<資料3> 平成25年度電子経済産業省構築事業：「ID連携トラストフレームワーク」の構築のための実証事業

第2回戦略委員会資料：「本事業で策定した基準案について(基準案の検討概要)」、平成26年3月6日、JIPDEC
なお、本資料は、下記の参考ホームページの「『ID連携トラストフレームワーク』の構築のための実証事業」内の「第2回ID連携トラストフレームワーク戦略委員会(平成26年3月6日)」の「配布資料(ZIP形式)」の中にあります。

<参考ホームページ>

・経済産業省「ID連携トラストフレームワーク」のホームページ：http://www.meti.go.jp/policy/it_policy/id_renkei/

【報告】「ID連携トラストフレームワーク」ご紹介その3 —— 事業者認証基準案について**1. ID連携トラストフレームワークの概要**

事例のご紹介の前に、今回、初めてご覧になる方のために、ID連携トラストフレームワークを再度、ご紹介する。この部分は、会報2014年5月号の記事に若干、補足を加えたものであり、既にご存知の方は飛ばしていただきたい。

ID連携トラストフレームワークとは、異なる組織間での信頼性を確保したID(アイデンティティ)連携を実現することによって、インターネットサービスの課題を解決し、サービスに係るあらゆる活動をオンライン上で完結できるようにする仕組みである。なお、ここでいう“ID”の意味は、ユーザID等、個人の識別に用いるための“Identifier”ではなく、“Identity”、すなわち、利用者である個人に関する属性の集まりのことである。

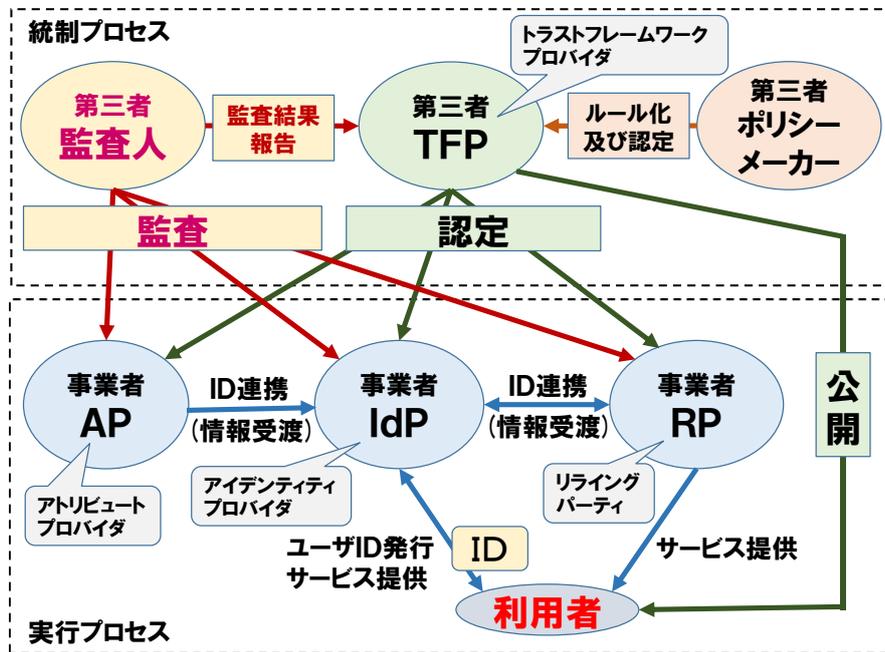


図1. トラストフレームワークによるID連携のイメージ

図1に、トラストフレームワークによるID連携のイメージを示す。各プレイヤーの役割の紹介を通じて、トラストフレームワークの機能を説明する。なお、これらの認定/認証業務は、ISO Guide 65の基準に則して行われる。

(1) 統制プロセス:ポリシーメーカー、TFP及び監査人の三種のカテゴリーの「第三者」から構成される。

- ① **ポリシーメーカー**(政府や業界):トラストフレームワークにおける要求事項やルール及びトラストフレームワーク・プロバイダの認定基準を策定する。
- ② **TFP**(トラストフレームワーク・プロバイダ): ポリシーメーカーが策定したルールに基づき、保証レベルを定義し、保証レベル毎に事業者が満たすべき技術、運用面での監査要件を作成する。
また、監査を行う監査人(アセッサー)を認定し、アセッサーの監査結果に基づき、事業者を認定する。
- ③ **監査人**(アセッサー):トラストフレームワーク・プロバイダが作成した監査要件に基づき、参加事業者に対して監査を実施する。

(2) 実行プロセス:利用者とIdP、RP及びAPの三種のカテゴリーの「事業者」から構成される。

- ① **利用者**:サービスを受ける主体。自分自身を証明する情報を、認証する主体に渡す必要がある。
- ② **IdP**(アイデンティティ・プロバイダ):利用者を認証する主体。利用者の登録や確からしさの確認を行う。
- ③ **RP**(リライング・パーティ):IdPから、必要な属性情報のみを受け取り、利用者サービスを提供する。
- ④ **AP**(アトリビュート・プロバイダ):利用者が求めるサービスを提供するにあたり、IdPが保有する属性情報だけでは足りない場合に、該当する属性情報を、IdPやRPに提供する。

上記の仕組みのなかで、TFP(トラストフレームワーク・プロバイダ)は、利用者に対して、このフレームワークの仕組みやルール、参加事業者、保証レベル等を公開する。これにより、利用者は、自身のデータがどのように取り扱われているかを知ることができる。また、この仕組みに参加すれば、一般事業者(RP:リライング・パーティ)は、個別に個々の一般事業者と契約を交わすことなく利用者の情報を受け取り、自らのサービスに活用することができる。

2. ID連携トラストフレームワーク認証基準案

以下に、JIPDECが今年3月6日に、「『ID連携トラストフレームワーク』の構築のための実証事業(以下、「実証事業」)」第2回戦略委員会で報告した、「本事業で策定した基準案について(基準案の検討概要)」(資料3)の一部をご紹介します。ご紹介する内容は、ID連携トラストフレームワークに参加する事業者の認定のための評価基準(案)と、これらの認証にあたって信頼付与機関(TFP)からの依頼で審査を担当する審査人(監査人)の能力基準である。

なお、紙面の都合上、概念レベルに留める。詳細は、資料3をご覧ください。

(1) 実証事業で検討した基準の範囲

図2に、実証事業で検討した基準の範囲を示す。

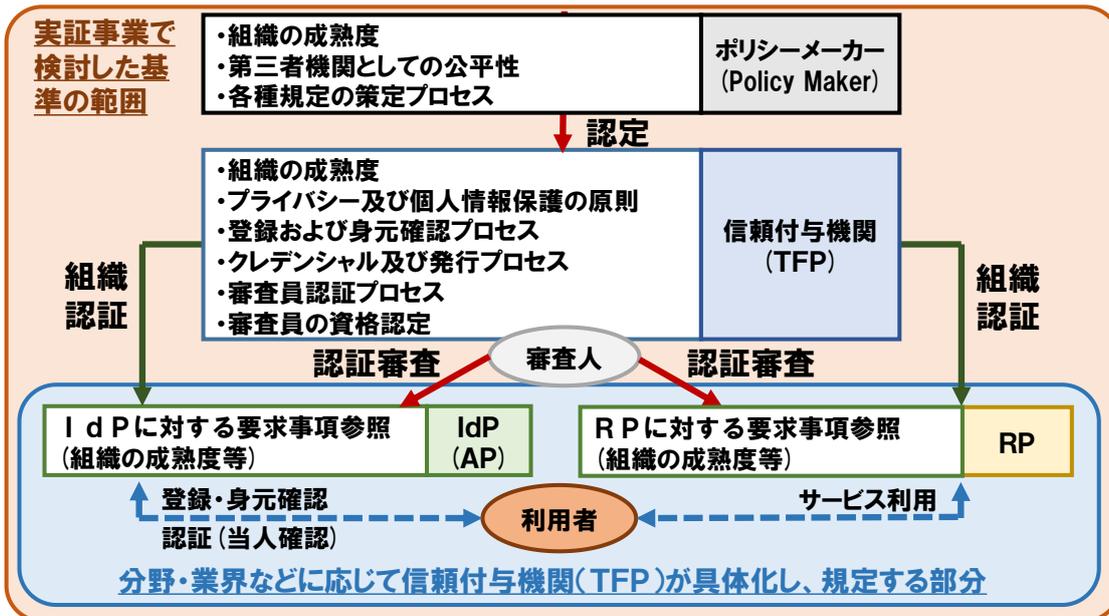


図2. 実証事業で検討した基準の範囲

図2に示すように、実証事業では、ポリシーメーカーが信頼付与機関(TFP)を認定する際に必要となる要件を検討し、基準案を作成した。この基準案は、適用される分野・業界など、個別の要件を含まない汎用的な基準である。

IdP、RPやAPを認証するための個別の要件を含む詳細な基準は、分野毎、業界毎等に設置される信頼付与機関(TFP)が、当該分野や業界等の固有の要件を取りこんで規定するのが原則であるが、分野毎あるいは業界毎等の個別の要件を含まない汎用部分について、IdP及びRPを認証するための評価基準(案)を参考として検討した。

(2) IdPサービス及びRPサービスの評価基準(参考)

以下に、IdP及びRPの認証基準(汎用部分のみ)の要求事項と認証の流れ(図3)を示す。

i) IdPサービス評価基準(参考)

IdPに対して、信頼付与機関が策定した要求事項に則り、アイデンティティ管理、個人情報の保護が適切に行われているかを評価する。IdPに対する要求事項は以下のとおりである。

- ・組織の成熟度: 法的実在性、法務遂行と法令遵守、財務規定、情報セキュリティマネジメントと監査、外部委託、運用管理
- ・プライバシー及び個人情報保護の原則: ISO 29100 プライバシー原則 (①同意と選択 ②目的適法性と規定 ③収集の制限 ④データの最小化 ⑤利用、保持、開示の制限 ⑥正確性と質 ⑦公開、透明性及び通知 ⑧個人参加とアクセス ⑨責任 ⑩情報セキュリティ ⑪法令遵守)に則った対策が行われているか
- ・身元確認の基準: 登録
- ・本人確認の基準: クレデンシャル管理(発行・管理)、トークン、認証プロセス、アサーション

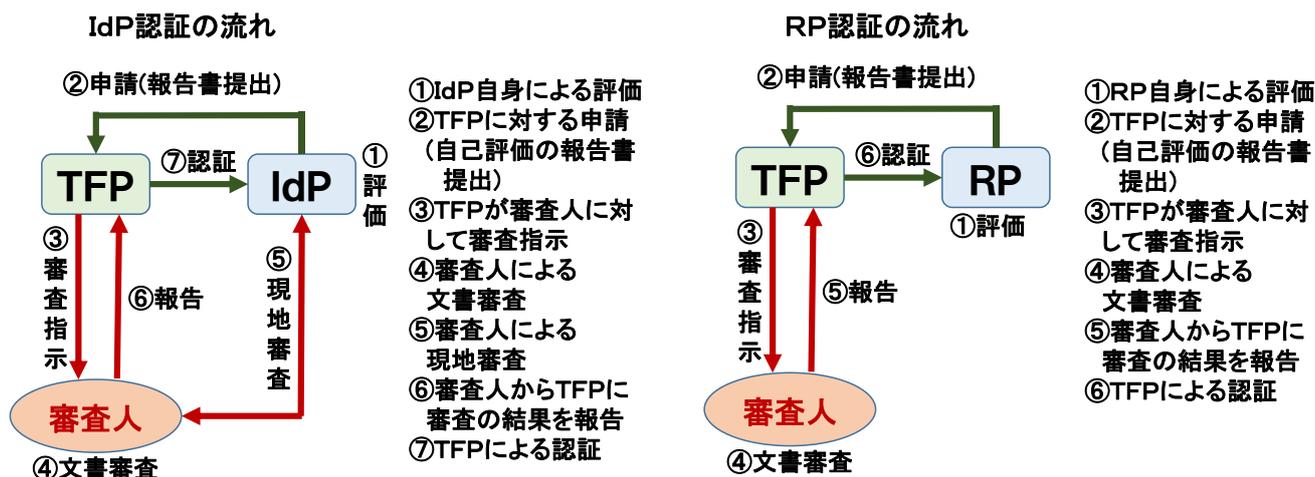


図3. IdP及びRP認証の流れ

ii) RPサービス評価基準(参考)

RPに対して、信頼性付与機関(TFP)が策定した要求事項に則り、個人情報の保護が適切に行われているかを評価する。RPに対する要求事項は以下のとおりである。

- ・組織の成熟度: i) IdPサービス評価基準と同様
- ・プライバシー及び個人情報保護の原則: i) IdPサービス評価基準と同様
- ・プライバシー及び個人情報保護の原則の遵守証明: 個人情報保護基準に則った対策をしているかを証明する程度(プライバシー影響評価の実施、JIS Q 15001やISO27001の遵守)

(3) 審査人(監査人)の能力基準

審査人(監査人)に求められる能力の基準を以下に示す。

分類	内容
個人的資質(努力規定)	・人格的に優れていること
知識及び技能(努力規定)	以下について知識及び技能があること ・審査の原則、手順及び方法、審査先の組織の概要 ・法的及び契約 ・マネジメントシステム及びID連携トラストフレームワーク基準文書
資格(義務規定)	・高校卒業程度の学力 ・情報処理及びセキュリティの専門家である(例えば、公認情報システム監査人(CISA)、ITスキル標準のレベル4以上など) ・情報技術分野において4年以上の実務経験がある。このうちの2年以上は、情報セキュリティに関連した役割又は職務についている。 ・これらの経験は、すべて合理的な範囲で最近のもの
教育(努力規定)	・定期的な教育を受ける

おわりに

本稿により、ID連携トラストフレームワークにおけるシステム監査人の活躍シーンがおぼろげながらイメージできたのではないかと思います。今後、一層、情報収集に努め、我々システム監査人の果たすべき役割を明確にしていきたい。

以上

[<目次>](#)

「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26章

会員番号：1795 藤澤 博（個人情報保護監査研究会）

第26章 プライバシーマーク認定後の維持・運用のポイント

プライバシーマークの認定を受けたことで、個人情報保護マネジメントシステム（PMS）が完成しました。しかし、PMSの維持・運用は、資格認定を受けてからがスタートです。

26.1 PMSの維持・運用

構築したPMSを維持・運用するポイントは以下のとおりです。

26.1.1 個人情報保護体制の維持

個人情報保護管理者、監査責任者、教育責任者、苦情対応窓口責任者、情報システム管理者等が不在にならないよう、組織変更、人事異動、退職等が予定されている場合は、速やかに任命し、引き継ぎを行ってください。

26.1.2 PMS年間計画書に基づいた運用

個人情報管理台帳の見直し、リスク分析表の見直し、法令等の改廃確認、委託先の再評価、定期教育の実施、運用の確認、定期監査の実施、代表者による見直し等、PMS年間計画書に基づいて実施してください。2年後のプライバシーマーク更新審査では、PMS運用が計画どおり実施されているかが、審査の対象となります。

各種記録には、実施日や報告日、承認日等の日付、承認印やサインなどの証跡が必要です。

26.1.3 内部規程の見直し

PMSの運用の積み重ねを行い、点検、是正、見直しの結果を内部規程に着実に反映して、PMSの継続的改善を図ることが重要です。

26.2 付与機関、指定機関による実態調査等**26.2.1 指定機関による更新審査**

プライバシーマーク認証取得以降、2年毎の更新審査においてPMSの運用状況を確認します。

26.2.2 付与機関、指定機関による実態調査

JIPDECなどの付与機関や指定機関は、プライバシーマーク制度に対する社会からの信頼を維持するために、認定事業者に対して立ち入り調査を求めることがあります。

26.2.3 改善の勧告及びプライバシーマークの認定取消し

プライバシーマーク制度の運用に問題があった認定事業者に対し、プライバシーマーク制度委員会における審議に基づいて、改善の勧告・要請がなされ、それに従わない事業者に対しては、プライバシーマーク付与認定の取り消しとなる場合があります。

日々の着実な積み重ねによって、PMSを維持・運用していただきますよう、お願い致します。

「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 おわりに

会員番号：1760 斎藤 由紀子（個人情報保護監査研究会）

2014年5月29日時点で、プライバシーマーク取得事業者は13,648社となりました。もう特定の事業者だけがPMSを運用する時代ではなくなったと言っても過言ではありません。「PMS実施ハンドブック」簡易版が、あらたにプライバシーマークを取得する事業者だけでなく、更新される事業者にとっても、あらためて確認していただける内容となっていれば幸いです。

■ 規程と様式のサンプル

「個人情報取扱規程」と「安全管理規程」、および一連の様式があれば、それを利用して、簡単に導入していただけるのではないかと考え、この簡易版ではその一部をご紹介します。実際のセミナー等ではサンプル全体を使用して研修をしています。

■ 電子版の制作

個人情報保護監査研究会メンバーの情報共有のため、Web上で閲覧できるよう電子版（Web版）を先に作りました。最終的にはハンドブック本文（35ファイル）と、規程および様式（77ファイル）となりましたが、使用したツールのAdobe「DreamWeaver」は絶大な威力を発揮しました。ファイル名を変更しても、各文書に記述した様式へのリンク先が自動的に修正されます。

■ セミナーやコンサルティングの実績を反映

電子版をもとにセミナーやコンサルティングの実績をもとに、ユーザーの反応から得た結果を逐次反映してきました。

簡易版では規程や様式の一部をご紹介しますだけでしたが、その全容を皆さんにご利用いただけるよう、2014年内を目標に出版を計画しています。また、2015年に予定されている、個人情報保護法改正の「PMS実施ハンドブック」への反映や、改定した様式の提供など、Webサイトからダウンロードを可能にする予定です。ぜひともご期待いただきますよう、お願い致します。

2013年5月号から2014年7月号まで、1年6か月間お読みいただきありがとうございました。

以上

「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 [目次へ](#)

個人情報保護監査研究会 主査 斎藤由紀子

<http://www.saa-j.or.jp/shibu/kojin.html>[＜目次＞](#)

中部支部報告【中部支部 研究会（5月）】

会員番号 1694 安井秀樹（中部支部）

■2014年度中部支部 研究会（5月）報告

以下のとおり、2014年度SAAJ中部支部 研究会（5月）を開催しましたので報告いたします。

日時：2014年5月24日（土）13:30～17:00

会場：名古屋市市政資料館 第2集会室

内容：

- | | |
|--|-------------|
| (1) 協会連絡事項など | 13:30～13:40 |
| (2) 「プライバシー・バイ・デザイン」
SAAJ 情報セキュリティ監査研究会 藤野理事 | 13:40～14:40 |
| (3) 質疑応答 | 14:40～15:05 |
| ＜ 休憩 ＞ | |
| (4) 「特定個人情報保護評価(PIA)について」
一般財団法人日本情報経済社会推進協会（JIPDEC）
電子情報利活用研究部 坂下部長 | 15:15～16:15 |
| (5) 質疑応答 | 16:15～16:50 |
| (6) その他、連絡事項 | 16:50～17:00 |
| ＜ 移動 ＞ | |
| (7) 懇親会
・場所 ウィルあいち（市政資料館向い）内 レストランウィル | 17:10～ |

◇テーマ1「プライバシー・バイ・デザイン」 ～ご紹介と問題提起～

(1) 概要

- プライバシー・バイ・デザインとは何か
- プライバシー・バイ・デザインの七つの基本原則
- プライバシー・バイ・デザインの実現形態
 - P I A : Privacy Impact Assessment (プライバシー影響評価)
 - F I M : Federated Identity Management (連携アイデンティティ管理)
 - F - P I A : Federated P I A (連携プライバシー影響評価)
 - D N T : Do Not Track (行動追跡拒否)
 - I D (アイデンティティ) 連携トラストフレームワーク
- システム監査人の新たな役割

(2) 所感

プライバシー・バイ・デザインの七つの基本原則と、実現における上流工程での影響評価について、とても解りやすくご説明頂いた。さらに I D 連携トラストフレームワークのご紹介と我々システム監査人の役割について、貴重な提言を頂いた。システム監査人として、世の中の動向を踏まえつつ、我々にできることは何か、また、今後身に付けるべきスキルは何か、について深く考えさせられた。

◇テーマ2「特定個人情報保護評価(PIA)について」 ～試行から見る対策と課題～

(1) 概要

- 特定個人情報保護評価の規定と実施手順
- 特定個人情報保護評価の支援を始めた経緯
- 特定個人情報保護評価は何をすればいいのか
- 試行の実施
- 地方公共団体へ助言していること（試行を行った体験から）
- 当協会（JIPDEC）で地方公共団体へ支援している内容
- 今後に向けて

(2) 所感

特定個人情報保護評価の世界的な動向と J I P D E C 様が地方公共団体向けに実施している支援(助言含む)について、大変にわかりやすい説明を頂いた。また、実際に地方公共団体において試行した当事者として、貴重なご意見も沢山頂いた。内容については、どれもこれも臨場感に満ち溢れ、参加者全員がとても感銘を受けた。さらに、参加者からの具体的、かつ、専門的な質問に対しても、丁寧な対応を頂いた。システムベンダーに身を置く者としてだけでなく、居住する地方公共団体の一市民としても、無関係ではすまされないことを痛感させられた。

◇懇親会

場所を移して行われた懇親会では、会場の人数制限で残念ながら研究会に参加できなかったメンバも加わり、闊達な意見交換が行われた。また、立食形式であったこともあり、初めて参加のメンバも含め多くの方々が活発な交流をされていた。さらに、アルコールも入ったことで、発表資料に載せられていない(載せられない?) 貴重な内容の話が講師より飛び出したりして、参加メンバ全員で大いに盛り上がった。



(名古屋市市政資料館概要)

煉瓦造りの大正末期の建物で国の重要文化財「旧名古屋控訴院地方裁判所区裁判所庁舎」を保存、公開。市の公文書館として市政資料を保存、閲覧、展示。また、研修室、展示室など市民活動の場を提供するとともに、映画やドラマ、また、結婚記念など、撮影スポットとしても活用されています。

※上記は、今回の研究会会場の名古屋市市政資料館です。

以上

近畿支部報告 【 近畿支部第146回定例研究会報告 】

会員番号 2520 松本拓也 (近畿支部)

1. テーマ : 「ゴルフ場の総合基地化提言」
2. 講師 : 株式会社 エスシーエイエヌ 代表取締役
中田 和男氏
3. 開催日時 : 2014年5月16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 :**

講師は、ゴルフ場が有する膨大な資産と、水源涵養、環境保護、気候変動緩和等の貴重な機能に着目し、その有効活用を図ることが、国土保全上、環境保護上有意義であると考えた。今回は、その活用方策として、ゴルフ場の総合基地化について講演していただいた。

(1) ゴルフ場の総合基地化とは

講師は、ゴルフをプレイするというゴルフ場本来の機能を残しつつ、ゴルフ場の有する資産・機能を活用して後述の3つの基地機能を構成し、活用していくことを想定されている。このゴルフ場の総合基地化の提言は、システム監査人にとっても、総合基地化に関連する情報システムの整備、管理を通じて社会に寄与する機会を得ることになり、大いに意義を有するものと考えている。

(2) 基地機能の概要**①国土保全及び自然エネルギー基地**

全国各地に広く分布するゴルフ場の広大な敷地の有する水源涵養、環境保護、気候変動緩和等の機能を維持し、更に、敷地を有効活用し、太陽エネルギー、風力、バイオマス(刈草等の活用)等の自然エネルギーを活用するエネルギー基地としても利用する。なお、ゴルフ場の総合エネルギー基地化は、スマートグリッド化によるエネルギーの地産地消を目指すものである。

②防災支援基地

東南海地震等の広域災害に際し、ゴルフ場の有する施設(管理棟、食堂、浴場、洗面所等)を開放して避難者の一時滞留を支援するほか、救難用ヘリポート等の支援用地の提供、支援資材の貯蔵箇所の提供等、広大な敷地を活用して防災支援の重要な役割を果たす。また、上記①のように自然エネルギー基地化することで、非常用のエネルギー基地としても威力を発揮できる。

③近隣センター基地

今日、限界集落の増大等、地域の居住環境の悪化が懸念されているが、ゴルフ場の施設を活用して、近隣住

民の生活改善に寄与する余地が大いにある。場合によっては、近隣集落と連携して、食堂、ゴルフコース周辺の景観、浴場等を近隣に開放する近隣センター基地も有力なゴルフ場活用策となる。

(3) 総合基地化と IT との関連

- ・エネルギー管理システム他の監視制御システムは、自動制御系統であり、その信頼性、安全性、可用性の確保が焦点になる。そこで、フェイルセーフ機能に着目して、開発・運用に関与していくべきである。
- ・防災支援のための各種管理システム、通信システムにおいては、情報セキュリティ、プライバシー保護への配慮が必要となる。運用時の可用性確保にも重点を置くべきと考える。
- ・近隣センター機能を発揮するためには、近隣住民等の顧客管理システムの充実が必要となるが、ここでは、プライバシー保護について考慮することが必要となる。
- ・ゴルフ場は、上記の IT への対応について、必ずしも有用な人材を有していない。このため、各種情報システムの開発・運用・監査について有効な対応が取れるとは限らない。そこで、システム監査人は、他の IT 専門家(中小企業診断士、IT コーディネータ等)と連携して、ゴルフ場の IT 強化について支援を行う必要が出てくる。
- ・一つの方策として、中小企業の会計参与の如き、情報参与といった人材の配置を提言したい。又、このような人材配置に対してインセンティブを与える等の施策も必要と考える、

(4) 今後の取り組みの方向性

- ・ゴルフ場の総合基地化については、国の助成、ゴルフ場の条件整備のいずれを見ても、計画的な取り組みが必要で、本提言は、今のところ、まったくの提案段階に過ぎない。これから、各位のご支援を得て、提言の充実、各方面への働きかけ等を行っていききたい。尚、現在、再生可能エネルギーの普及を促す各種助成策が政府をはじめ、各自治体において講じられているが、これらの活用も考慮する必要がある。

(5) まとめ

下記の理由により、ゴルフ場の総合基地化を提言する。

- ・ゴルフ場は、貴重な国土資産であり、その機能の維持を図ることは、国民経済上大いに意義を有している。
- ・ゴルフ場の総合基地化を図ることによって、再生可能エネルギーの導入等国民経済にも貢献でき、又、その広大な敷地を活用して、防災支援においても重要な位置を占めることができる。
- ・近隣と連携することにより、地域住民に資する近隣センター機能を発揮することができる。

6. 所感

大きな資産・敷地を有するゴルフ場を、ゴルフプレイ以外にも有効に活用できないかという点に着目されており、私はゴルフをプレイしないのですが、共感できる内容だと思います。ただ、今回の提言にあるような3種の機能については、ゴルフ場の立地、近隣住民の世帯構成、交通アクセス等、ゴルフ場の周辺環境により、その需要は異なると感じます。そのため、日本国内にあるゴルフ場のうち、この機能を導入することに効果がある施設がどの程度あるのかについては、今後の課題となると考えます。

以上

■「世界最先端IT国家創造宣言」改定(案)の公開とパブリックコメント募集(6月3日)

政府の世界最先端IT国家創造宣言の公開から1年を経、改定案の検討が進んでいる。6月3日に改定案が公開され、6月17日までパブリックコメントの募集が行われた。SAAJに深く関係する主な改定部分は以下のとおり。

1. III.1.(1)「②ビッグデータの利活用による新事業・新サービスの創出の促進」に、以下が追加された。
・「**パーソナルデータの利活用に関する制度見直し方針**」(2013年12月IT総合戦略本部決定)を踏まえ、2014年6月までに**法改正の大綱**としてとりまとめ(次の記事参照)、2015年通常国会に関連法案提出
2. III.1.に「(6)東京オリンピック・パラリンピック等の機会を捉えた最先端のオープンデータ、次世代放送・通信サービス、IT利活用による『おもてなし』の発信」が追加された。この取り組みの一環として、**ID連携トラストフレームワーク**(P17の記事、『情報セキュリティ監査研究会だより』参照)が明記されている。

[改定案の URL] http://www.kantei.go.jp/jp/singi/it2/dai64/siryou2_2.pdf

[改定案の概要(改定部分のピックアップ)の URL] http://www.kantei.go.jp/jp/singi/it2/dai64/siryou2_1.pdf

■IT総合戦略本部、個人情報保護法改正に向けたパーソナルデータに関する検討会の大綱案を了承(6月19日)

政府のIT総合戦略本部は、6月19日に開催された第12回パーソナルデータに関する検討会で、「パーソナルデータの利活用に関する制度改正大綱(検討会案)」を了承した。以下に、大綱の趣旨を示す。

個人情報保護法制定から10余年が経過し、情報通信技術が飛躍的に進展している。なかでも、個人の行動・状態等に関する情報に代表され、利用価値が高いパーソナルデータは、高度な情報通信技術を用いた方法により、利活用が可能になってきている。しかしながら、この新たなイノベーションを適用するに際し、現行の個人情報保護法では、さまざまな課題がある。これを可能な限り、事業者にとっても、個人情報を提供する利用者にとっても使いやすく、また、安全・安心を得られるものに変えていこうというのが、この制度改正の主たる目的である。

検討案における課題解決のための法的措置の基本的な枠組みは、以下のとおり。

1. 本人の同意がなくてもデータの利活用を可能とする枠組みの導入等
多種多様かつ膨大なパーソナルデータを、分野横断的に利活用することによって生まれるイノベーションや、それによる新ビジネスの創出が期待されるが、その際に、目的外利用や第三者提供に当たって、本人の同意を必要とする現行法の仕組みは、事業者にとって負担が大きい。そこで、本人の同意がなくてもこれらを行うことを可能にする枠組みを導入する。具体的には、「個人の特定性を低減したデータ」への加工と、本人の同意の代わりとしての取扱いに関する規律を定める。
2. 基本的な制度の枠組みと、これを補完する民間の自主的な取り組みの活用
法的規制では避けることが難しい、いわゆるグレーゾーンの問題に対応するため、法律では大枠を定め、具体的な内容は政省令、規則及びガイドライン並びに民間の自主規制ルールにより対応することとする。
3. 第三者機関の体制整備等による実効性ある制度執行の確保
パーソナルデータの促進に向けて、法令や民間の自主規制ルールを実効性あるものとして運用するため、独立した第三者機関の体制を整備する。

「パーソナルデータの利活用に関する制度改正大綱(検討会案)」のURLは以下のとおり。

<http://www.kantei.go.jp/jp/singi/it2/pd/dai12/siryou1.pdf>

[<目次>](#)

【 協会主催イベント・セミナーのご案内 】

■月例研究会（東京）

第192回	日時:2014年7月3日(木) 18:30~20:10 場所:機械振興会館 地下2階多目的ホール
	テーマ クラウドサービス利用のための 情報セキュリティマネジメントガイドラインの概要及び改訂について
	講師 経済産業省 商務情報政策局 情報セキュリティ政策室 室長補佐 上坪 健治氏 特定非営利活動法人 日本セキュリティ監査協会(JASA)事務局長 永宮 直史氏
	講演骨子 本年3月、経済産業省では「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」を改訂しました。 本ガイドラインは、JIS Q 27002:2006 (ISO/IEC 27002)における実施の手引をベースに、クラウドサービス利用における情報セキュリティ管理の確立、導入、運用、監視、見直し、維持及び改善のために必要な情報を提供するものです。本講演では、本ガイドラインの趣旨と概要について中心に解説するとともに、改訂によって生じた主要な変更点についても紹介します。
お申し込み	ご案内とお申し込み方法を HP でご案内しています。 (http://www.saa.or.jp/kenkyu/kenkyukai192.html)
第193回	日時:2014年7月22日(火) 18:30~20:30 場所:機械振興会館 地下2階多目的ホール
	テーマ 「情報セキュリティの最新の脅威の動向」(仮題)
	講師 独立行政法人 情報処理推進機構(IPA)技術本部 セキュリティセンター 情報セキュリティ技術ラボラトリー 主任研究員 渡辺 貴仁 氏
	講演骨子 詳細確定次第、HPでご案内いたします。
お申し込み	
第194回	日時:2014年8月20日(水)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 特定個人情報保護評価指針について - マイナンバーにおけるPIA実施の対策と課題等 -
	講師 一般財団法人 日本情報経済社会推進協会(JIPDEC) 電子情報利活用研究部 部長 坂下 哲也 氏
	講演骨子 詳細確定次第、HPでご案内いたします。
お申し込み	

■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.saa.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)

[<目次>](#)

■公認システム監査人特別認定講習の実施(東京・大阪)

計 画 中	◎情報システムに関する知識コース(2日コース)	2014年7月3日～4日 2014年7月13日～14日
	◎システム監査に関する知識コース(2日コース)	2014年7月1日～2日 2014年7月12日～13日 2014年7月20日～21日 2014年8月10日～11日 2014年9月14日～15日
	◎論文およびプレゼンテーションコース(1日コース)	2014年6月30日 2014年7月7日 2014年7月19日 2014年8月3日 2014年9月3日
概 要	本講習は、SAAJが認定した特別認定講習実施機関が、CISA、ITコーディネータ、情報セキュリティスペシャリスト、プロジェクトマネージャ等の資格取得者に対し、SAAJの定めるカリキュラムに基づき講習を実施するものです。講習を修了した場合には、「公認システム監査人」、「システム監査人補」の申請の資格要件が得られます。	
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.saa-j.or.jp/csa/tokubetsu_nintei.html)	

■システム監査普及サービス(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。
	<p>概要</p> <ul style="list-style-type: none"> ・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、システム監査普及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。 <p>詳細はHPでご案内しています。(http://www.saa-j.or.jp/topics/hukyuservice.html)</p>
お 問 い 合 わ せ	システム監査事例研究会主査 大西 (Email: jireiken@saa-j.jp)



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.saa.or.jp/index.html>
- ・会員規定にも目を通しておいてください。 http://www.saa.or.jp/gaiyo/kaiin_kitei.pdf
- ・皆様の情報の変更方法です。 <http://www.saa.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.saa.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.saa.or.jp/shibu/index.html>
皆様の積極的なご参加をお待ちしております。門戸は広く、見学も大歓迎です。

ご意見 募集中

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

出版物

- ・協会出版物が会員割引価格で購入できます。 <http://www.saa.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.saa.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.saa.or.jp/csa/index.html>

会報

- ・PDF会報と電子版会報があります。 (http://www.saa.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.saa.or.jp/members/kaihouinfo.pdf>

お問い合わせ

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

[< 目次 >](#)

【 SAAJ 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
11月	14日 理事会:次期会長選任 14日 予算申請提出依頼(11/30〆切) 16日 2014年度役員改選準備開始 20日 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 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 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 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 総会開催案内掲示・メール配信 10日 役員改選公示 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〕	11日 会計:支部会計報告期限 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	CSA・ASA 春期募集(2/1~3/31) 1-2日 事例研:第23回システム監査実践セミナー(前半)、22-23日(後半) 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	1日 事例研:第13回課題解決セミナー 25日 CSA フォーラム	
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 25日 第190回月例研究会	20日 2014年春期情報技術者試験(9:30~16:30)
5月	8日 理事会 29日 会費未納督促メール	認定委員会:新規 CSA/ASA 面接 15-16日 事例研:第26回システム監査実践セミナー 22日 第191回月例研究会	
6月	12日 理事会 末日 支部会計報告依頼(〆切 7/14) 末日 助成金配賦額決定(支部別会員数)	7日 事例研:第14回課題解決セミナー 10日 新規 CSA/ASA 承認 10日 CSA フォーラム	28日 近畿支部:システム監査体験セミナー(入門編):
7月	1日 会費未納者督促状発送 初旬 支部助成金支給 10日 理事会	1日 秋期公認システム監査人募集案内〔申請期間 8/1~9/30〕 3日 第192回月例研究会 22日 第193回月例研究会	14日 支部会計報告〆切
8月	(理事会休会) 会費督促電話作業(役員) 中旬 中間期会計監査	秋期公認システム監査人募集開始~9/30 20日 第194回月例研究会	30~31日 東北支部:合宿研修会 30~31日 近畿支部:システム監査体験セミナー(実践編)
9月	11日 理事会		
10月	9日 理事会		

※注 定例行事予定の一部は省略。

[＜目次＞](#)

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 年度の年間テーマは、「〇〇〇のためのシステム監査」とし、四半期ごとに「〇〇〇のための」について具体的なテーマを設定して、システム監査に関する皆様からのご意見ご提案を募集しています。

8月号から10月号までの3か月間のテーマは、「次世代のためのシステム監査」です。次世代に向けてのシステム監査について、皆様からの幅広いご意見をお待ちしています。

過去5月号から7月号までのテーマは、「情報化社会のためのシステム監査」でした。様々なご意見ご提案、ありがとうございました。

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

□■ 2. 会報の記事に直接コメントを投稿できます。

会報の記事は、

- 1)PDF ファイルの全体を、URL (<http://www.skansanin.com/saaj/>)へアクセスして、画面で見る
- 2)PDF ファイルを印刷して、職場の会議室で、また、かばんにいれて電車のなかで見る
- 3)会報 URL (<http://www.skansanin.com/saaj/>)の個別記事を、画面で見る

など、環境により、様々な利用方法をされていらっしゃるようです。

もっと突っ込んだ、便利な利用法はご存知でしょうか。気に入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、投稿ボタンをクリックするだけです。動画でも紹介しますので、参考にしてください。

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

□■ 3. 会員の皆様からの投稿を募集しております。

分類は次の通りです。

1. めだか (Word の投稿用テンプレート(毎月メール配信)を利用してください)
2. 会員投稿 (Word の投稿用テンプレート(毎月メール配信)を利用してください)
3. 会報投稿論文 (論文投稿規程があります)

会報記事は、次号会報募集の案内の時から、締め切り日の間にご投稿ください。システム監査にとどまらず、情

報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します。ただし、投稿された記事については、表現の訂正や削除を求め、又は採用しないことがあります。また、編集担当の判断で字体やレイアウトなどの変更をさせていただきますことがあります。

次の投稿用アドレスに、次号会報募集案内メールに添付されるフォーマット(Word)を用いて、下記アドレスまで、メール添付でお送りください。

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)

バックナンバーは、会報サイトからダウンロードできます(電子版ではカテゴリー別にも検索できますので、ご投稿記事づくりのご参考にもなります)。

会報編集部では、電子書籍、電子出版、ネット集客、ネット販売など、電子化を背景にしたビジネス形態とシステム監査手法について研修会、ワークショップを計画しています。研修の詳細は後日案内します。

会員限定記事

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



■発行: NPO 法人 日本システム監査人協会 会報編集部

〒103-0025 東京都中央区日本橋茅場町2-8-8共同ビル6F

■ご質問は、下記のお問い合わせフォームよりお願いします。

【お問い合わせ】 <http://www.saaj.or.jp/toiwase/>

■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/>

Copyright(C)2014、NPO 法人 日本システム監査人協会

掲載記事の転載は自由ですが、内容は改変せず、出典を明記していただくようお願いします。

■□■SAAJ会報担当

編集委員: 藤澤博、安部晃生、久保木孝明、越野雅晴、桜井由美子、中山孝明、藤野明夫

編集支援: 仲厚吉 (会長)

投稿用アドレス: saajeditor ☆ saaj.jp (☆は投稿時には@に変換してください)