特定非営利活動法人
日本システム監査人協会報

2013年5月号
No 146

No.146（2013年5月号）＜4月20日発行＞

五月晴れの空に鯉のぼりが悠々と
舞い踊る季節になりました。

新しい情報が一杯です。
ぜひ、一読を！

2013.04 投稿

めだか　【　将を射んと欲すれば‥‥（システム監査活性化への提言）　】

最近、システム監査は全く普及してないという主旨をシステム監査に携わる方々からよく聞く。システム監査よりシステムコンサルティングの方がビジネスチャンスはありそうだとして宗旨替えしそうな人もいるくらいである。金融商品取引法による内部統制報告制度が定着し、IT統制の監査も明示的に謳われるようになったのに、である。

システム監査の普及は目覚しいとは言えないが、情報社会におけるシステム監査の意義、価値を忘れ宗旨替えというのも、ビジネスありきとは言いながら残念な限りである。

システム監査の活性化のためには、その実施を法制化により社会に強制するのが必要だと説く人もいる。市場での必要性の実感を基礎とした監査普及のプロセスを経ず、戦後、米国主導で法制化により公認会計士による財務諸表監査制度が導入された日本では、それも已む無い発想かもしれない。

しかし、当の米国では、自国で法制化により公認会計士による財務諸表監査制度を導入する以前から、自発的に監査が普及していた事実、現実があると聞く。

その辺の研究も十分にせず、システム監査に関わる人が法制化、法制化と言うと、自身の活躍の場を法律によって担保しようとしているとも受け取られ、足下をすくわれそうなリスクも感じる。

情報システムは、そもそも不完全性（安全性、信頼性、効率性等の追及における避けがたい失敗リスクの存在）がその特性の一つと言われる。ITの根源は自然科学であり、言うまでもなくそれ自身に意思はない。従って、ITを利用する情報システムの戦略立案、企画、開発、運用、保守、そして利用等は、その目的を前提に、全て「人」の意思、判断、行為によって実現され、そしてこの関わる「人（＝人間）」の不完全性を考えた時、ITを利用した情報システムは、本質的には不完全性を内在するとの考えである。更に、ITの急速、かつ飛躍的な発展、進化とその高い技術的専門性が情報システムの不完全性を一層特徴付ける。

しかし、不完全性を内在するから活用をやめるというのでなく、社会における情報システムの健全な利活用の一層の促進を前提とすると、関係当事者（開発を指示する者、開発をする者、利用する者など）がこの不完全性を正面から認識し、受け入れることが必要であり、そのためには、何よりも各当事者がそれぞれの役割、責任をきちっと果たしていることについての相互信頼関係の確立がその基本となる。

そして、この相互信頼関係の確立には、各当事者（特に「開発者」、あるいは「情報システムサービス提供者」）の説明責任遂行（やるべきことはやっていることを自ら説明すること）と、その説明への信頼性の担保が不可欠ではないだろうか。

つまり、システム監査の法制化を訴える（将を射んと欲する）のでなく、各当事者（特に「開発者」、「情報システムサービス提供者」）の説明責任遂行の必要性を訴える（まず、馬を射る）ことを通して、その説明責任遂行と不可分の、説明責任遂行に信頼性を付与し実効あらしめるシステム監査の必然的実施を導き出すのが、システム監査活性化の王道であり、また実は近道なのではないだろうか。　（広太雄志）

（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。　）

2013.04 投稿

めだか【 先手、先制、機先　（システム監査活性化への提言）】

新テーマの“提言“、めだか投稿としてはズシリと重いプレッシャーを感じるが、「活性化」も相当な目方があるので釣り合いは取れている。語感に眩惑されずいつもの気安さ？で、しかし新たな視点で考える。
この活性化とは、「生き生きとダイナミックに躍動する活動」という未来志向の意であって、しばしば耳にする元気になる・取り戻すなどの低調な場合からの復調を求めるものなどではない。この視点の表題だ。

「生き生きとダイナミックに躍動するシステム監査」を獲得・具体化するには、「先手・先制・機先」を基本戦略に据える必要がある。システム監査の活性化は、現在の基盤や位置を拠り所にするのではなく、明日の情報社会に求められる役割を先取りし、時流に先行するシステム監査の使命と機能に基づく活動によって見出されると考えている。「先手・先制・機先」の戦略を温故知新の教えから導き出してみる。情報処理技術者試験制度におけるシステム監査技術者像の変遷を下表に簡単にまとめた。

（語尾を省略しているのでキーワードとして見て欲しい）

	対象者像	役割・業務	技術水準
昭和61年～（1986）	・監査対象から独立 ・信頼性、安全性、効率性の観点	・関係者に助言/勧告 ・コンピュータセキュリティ確保とシステム有効活用で情報化社会を健全化	・情報処理システムの企画/開発/運用及び監査の専門分野知識 ・システム監査を行い得る
平成6年～（1994）追加項目	―	・経営に報告 ・コンピュータセキュリティの実効性担保 ・経営の内部統制の機能	・システムの全ライフサイクルの評価 ・情報処理だけでなく、経営管理の視点と関連づける ・一般的な監査技術と監査技法
平成13年～（2001）追加項目	・トップマネジメントの視点 ・可用性、機密性、保全性、有用性、戦略性の視点 ・あるべき姿と判断基準を自ら形成	・トップマネジメントへ報告 ・内部統制機能の改善を促進 ・実効性を担保し、企業経営とともに情報社会/ネットワーク社会の健全化	・情報処理の視点だけでなく、企業及び社会に貢献できる改善の促進 ・ビジネス要件や経営方針に合致した監査計画立案 ・ビジネス業務プロセスの問題点洗い出しと分析/評価の判断基準を自ら形成 ・情報技術動向や外部環境変化の把握と将来像を描く
平成21年～（2009）追加項目	・高度IT人材として確立した専門分野 ・情報システムのリスクとコントロールを評価 ・組込みシステムを点検・評価	・トップマネジメントへ報告しフォローアップ ・下位者を指導 ・ITガバナンスの向上やコンプライアンスの確保に寄与	・組込みシステムの幅広く深い知識 ・企業戦略上のリスク/コントロール/問題点の分析/評価の判断基準を自ら形成 ・ビジネス要件/経営方針/情報セキュリティ/個人情報保護/内部統制などの関連法令/ガイドライン/契約/内部規定など基づいた適切な監査

周知のことではあるが、システム監査に求められている使命と機能、期待される質量の鮮やかな変化に改めて気づく。この表からだけでも言えることが確実にある。システム監査の活性化策は、現状への充足ではなく環境変化を先取りするポジションへのギアチェンジであると思う。

（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。）

2013.04 投稿

めだか　【システム監査の普及促進―デスマーチを憂いて・・その２】

2013年3月号（No.144）の問題提起に関連して、長時間労働やメンタルヘルスについて、社会的な動向とアドバイスをする上で有益なサイトをご紹介したい。

2006年（平成18年）3月に厚生労働大臣によって策定された「労働者の心の健康の保持増進のための指針」は、「心の健康問題が労働者、その家族、事業場及び社会に与える影響は、今日、ますます大きくなっており、事業場において、より積極的に心の健康の保持増進を図ることは、非常に重要な課題となっている」としている。ところが、平成19年の労働者健康状況調査によると、事業所の66．4％が「心の健康問題に取り組んでいない」として、そのうち42．2％が「取り組み方がわからない」としている。特に規模の小さな事業所は取り組みが遅れている。
また、時間外や休日労働時間が長くなるほど、脳と心臓疾患の発症との関連性が高まるとも考えられている。
2006年（平成18年）3月の「過重労働による健康障害防止のための総合対策」（2011年一部改正）では、「時間外・休日労働時間の削減」「年次有給休暇の取得促進」「健康管理体制の整備」「長時間労働者への医師による面接指導制度」等の対策について定めている。

これまでの情報システムの開発場面では、長時間労働や休日出勤、不規則な勤務は当たり前であったが、前述の指針や対策が定められた動きを無視することはできない。システム管理基準の「コンプライアンス」や「人的資源管理（健康管理）」の項目に関連して、助言やコンサルティングを具体的に行えるように、メンタルヘルスに関する指針や対策、また、取り組んでいる事例を知り、アドバイスができることは、大変重要なことであると考える。

次に参考となるサイトを紹介する。
◆厚生労働省関連のサイト 「こころの耳」（http://kokoro.mhlw.go.jp/）
　※厚生労働省の委託事業として、社）日本産業カンセラー協会が運営している。
　手引・冊子・パンフレットの中には、「IT 業におけるストレス対処への支援」（平成23年）もある。
◆東京都のサイト　（http://www.kenkou-hataraku.metro.tokyo.jp/）
　※東京都労働相談情報センターの公式サイト

情報システムの開発に携わる企業は、「現場での労務管理の脆弱さ」や「品質問題や人手不足による長時間労働」の結果として、働く人の中に健康を害して長期の休業や退職となるケースがある。特に自殺に至るようなケースが発生した場合には、企業イメージを損なうだけに留まらず、裁判での敗訴や事業運営のリスクもあり、着実に取り組む必要のある重要な課題であると思う。

（健康衛生）

（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。）

2013.04 投稿

投稿　【　共通番号とシステム監査　】

会員番号 0557　仲　厚吉（個人情報保護監査研究会）

朝日新聞3月23日朝刊に、「共通番号　期待と課題」（所得や年金まとめて把握）（個人情報保護・巨額な費用）という記事がでています。また、朝日新聞朝刊4月4日朝刊にも、「共通番号消えぬ不安　利便向上の半面、不正利用も」（法案、国会審議入り）という記事がでています。

過日、米国の知人と共通番号について話す機会がありました。米国では、「social security number」という名称で、日常的に使用しているとのことです。新聞記事によれば、内閣官房の資料からとして、米国では、「social security number」は、社会保障番号制度のもとに、紙製のカードで、年金、医療、そのほか社会扶助、行政サービスの本人確認に使われていて、企業など民間での使用制限はないとのことです。

「共通番号制度」法案が成立した場合の導入スケジュールは、次のように報道されています。

2015年10月	国民一人一人に共通番号を通知。
2016年1月	税務署や日本年金機構などの各組織内に限って、共通番号をつかって情報が集められるようになる。顔写真入りの個人番号カードの交付を開始（希望者のみ）。
2016年中めど	民間企業にも共通番号の利用を認めるかどうか決める。認められれば、共通番号をつかって顧客管理などができる。
2017年1月	ほかの組織がもつ情報についても、共通番号をつかって情報が集められるようにする（地方自治体は7月から）。年金がいくらもらえるのかなどが見られるインターネットのサイト「マイポータル」の運用を開始。

共通番号導入のメリットは、所得が正確に把握しやすくなり、脱税が防ぎやすくなるということです。また、所得に応じて社会保障の給付額を変える制度を導入しやすくなることがあります。各個人にとってみれば、市町村の窓口で手当を申請する際、住民票や所得証明書などを提出する必要がなくなり、手間が省ける利点があります。デメリットは、所得や住所などの個人情報が漏れると、番号を悪用し、本人になりすまして年金を横取りするといった不正が起きるおそれがあることや、システムの開発費や運営費がかさむことが挙げられています。

2016年中めどに、民間企業にも共通番号の利用を認めるかどうか決めるスケジュールになっています。システム監査人は、共通番号をつかって顧客管理などができるという時期が来るより前に、共通番号をつかった顧客管理システム等への監査チェックリストを整備しておく必要があります。また、システム監査人の役割の重要性をアピールして出番をつくっておくことが、システム監査活性化への道につながると思います。

個人情報保護監査研究会では、先に、個人情報を取り扱う情報システム、略して、個人情報システムへのリスクアプローチの視点から、監査チェックリストを整備しました。今後は、共通番号をつかう場合の監査チェックリストの追補に取り掛ります。また、Privacy Impact Assessment 等の動向をみていきます。

以上

新たに会員になられた方々へ

Welcome

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

ご確認ください

・協会活動全般がご覧いただけます。 http://www.saaj.or.jp/annai/index.html
・会員規定にも目を通しておいてください。 http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・みなさまの情報の変更方法です。 http://www.saaj.or.jp/members/henkou.html

特典

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

ぜひ参加を

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

ご意見募集中

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

出版物

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

セミナー

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

CSA・ASA

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

会報

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

お問い合わせ

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

沼野会長からの一行メッセージ

“システム監査に関わる者は、システム監査の役立ちを十分認識しておく必要がある。”

会長コラム

会員番号 0841

みずほ証券 vs 東京証券取引所　の裁判を傍聴して

会長　沼野伸生

新規上場株JCOM株の誤発注の取消し処理ができなかったことによる損害の賠償を求め、みずほ証券が東京証券取引所を訴えた裁判の控訴審結審が3月18日（月）午後3時から、東京高等裁判所424号法廷で開かれました。

本件について、東京地方裁判所での争いの時から時間の許す限り傍聴しており、今回も午前中の仕事の後、東京高等裁判所に寄り1時間弱の法廷を傍聴してきました。

みずほ証券側は十名近い弁護士が並び、一方東京証券取引所は3名の弁護士で対応し、当日は結審であり、双方、最後の主張を展開しました。

今回の争点の最大のポイントの一つは、ソフトウェアのバグは重過失に当たるかどうかであり、みずほ証券の主張ポイントは、バグはテストでも容易に発見できたもので、重過失にあたり損害を賠償すべきとするもので、一方東京証券取引所は、合理的信頼性のあるシステムであれば、例えバグが一つあったとしても、債務不履行には当たらないとするものです。

因みに、2006年10月の第一審である東京地方裁判所の判決は、ソフトウェアのバグが重過失にあたるかどうかについては、「証拠がない」としてみずほ証券のそれに係る損害賠償請求を認めませんでした。

世界中で圧倒的シェアを占め使用されているOSですら、そのパッチは延々と発行され続ける現実もある中で、不可避なソフトウェアのバグによる損害賠償をどう社会として整理するかが問われる裁判であり、我々情報システムに関わる者として7月24日（水）午後1時から予定される高裁の判決を、関心を持って待ちたいと思います。（その前に、裁判所の仲介で双方が和解する可能性もありますが。）

高裁での控訴審では、高裁の勧告により、地裁ではされなかったバグの原因となったソースコードの開示が東京証券取引所からなされ、それを基に、原告、被告双方、また双方が依頼した専門家の意見書などで主張の応酬があったと報道されています。実に興味深いですが、残念ながらその資料の閲覧まではできていません。

しかし、ソフトウェアのバグが重過失に当たるかどうかの争いでは、ソフトウェアのバグが不可避なものとすれば、開発側は、開発者として正当な注意力を持ち、開発する者としてその時の社会の技術レベルに相応した対応を実施し、それを記録などに残し自らの行為の正当性を主張できる備えがされていることが重要となります。そして、その主張について、システム監査を受けるなどでその信頼性を担保しておくことも、このような争いになった場合、裁判所の心証形成に大きく影響するものと考えられます。

今回、東京証券取引所がシステム監査についての主張をしているかどうかは定かではありませんが、我々システム監査に関わる者として、そのようなシステム監査の役立ちも十分認識しておく必要があると、一連の裁判の傍聴を通して思っています。

（本件裁判については、雑誌「日経コンピュータ 2013.4.4 号」にも詳しく報道されていますので、関心のある方はご一読下さい。）

以上

2013.04

協会からのお知らせ（システム監査活性化プロジェクト）

会員番号 6027 小野　修一（活性化PT　主査）

昨年度、当協会では会員増強プロジェクトを立ち上げ、当協会の運営・活動基盤を支える会員を増やすための活動を展開しました。結果は、プロジェクトメンバーの皆様のご努力、会員の皆様のご協力によって、会員数の減少を食い止め、会費の未収を大幅に改善し、部会・研究会・委員会・担当および支部の活動について会員の皆様に関心をもっていただくことができました。ありがとうございました。

今年度は、当協会の活動理念である「システム監査の普及を図り、健全な IT 社会の実現に貢献する」に立ち戻り、システム監査の活性化のために当協会は何ができるかを考え実践するという主旨で、システム監査活性化プロジェクトに衣替えをして活動を開始しました。システム監査の活性化は、必然的にシステム監査人の活性化、当協会の活性化・認知度向上につながり、ひいては当協会の会員増強、基盤強化にも結びつくと考えています。

会報では、システム監査の活性化を目指して、各部会・研究会・委員会・担当が行う活動を、順次、ご報告していきます。会員の皆様も、システム監査の活性化につながるご提案・ご意見がありましたら、ぜひお寄せいただきますようお願いします。

部会・研究会の掲載スケジュール
5月号：情報セキュリティ監査研究会（連載1回目）、個人情報保護監査研究会（連載1回目）
6月号：CSA利用推進・認定委員会、ワークショップ支援サービス
7月号：月例研究会、事例研究会
8月号：基準研究会、法人部会
9月号：推薦委員会、事務局・会計担当
10月号：支部、会報部会

■【情報セキュリティ監査研究会の取組み】

会員番号 0056　藤野　明夫　（情報セキュリティ監査研究会　主査）

情報セキュリティ監査研究会の活動状況を定期的に会報に掲載することを試みてみたいと思います。

第一弾として、3 月 21 日に開催されました第11回情報セキュリティ研究会の様子をお伝えいたします。3 月 21 日の研究会では、IPA（独立行政法人情報処理推進機構）編、 2012 年 3 月発行の「くらしと経済の基盤としての IT を考える研究会報告書「つながる IT がもたらす豊かなくらしと経済　～　ビッグ　データの価値と信頼　～」の第7章5節「ビッグデータ活用を支える信頼性・安全性」の輪読と討議を行いました。その概要をまとめましたのでご一読いただきたいと存じます。

■【個人情報保護監査研究会の取組み】

会員番号 1760　斎藤　由紀子（個人情報保護監査研究会　主査）

個人情報保護監査研究会では、中堅企業がプライバシーマークを取得する際に必要な基本知識をわかりやすく解説するため「個人情報保護マネジメントシステム実施ハンドブック」を策定しています。

2013年5月号の会報から、その内容の一部を抜粋し、連載でご紹介していきます。

2013.04 投稿

投稿　【情報セキュリティ監査研究会便り その１】

情報セキュリティ監査研究会　藤野明夫(会員番号：0056)

はじめに

研究会の活動状況を定期的に会報に掲載することを試みてみたいと思います。第一弾として、3月21日に開催されました第11回情報セキュリティ研究会の様子をお伝えいたします。

１．　研究テーマについて

情報セキュリティ監査研究会は、その名のとおり、「情報セキュリティ監査の研究」を主たる活動にしている。しかしながら、近年のセキュリティ事故の多発やその影響の深刻さ、ビッグデータの普及やマイナンバー制度の議論のなかでやかましくなってきた個人情報の問題等に鑑み、監査以前に、これらの深刻なセキュリティ問題（個人情報保護の問題が厳密な意味でセキュリティの問題か、という議論はあるが、とりあえずセキュリティに含めて考える）について、まずは、その問題の所在と本質の把握をすることに取り組んでいる。

2012年度から2013年度前半にかけては、その利活用の効果が喧伝される一方で、個人情報問題を中心に様々なリスクが存在するビッグデータの問題を研究テーマとした。テキストとして、ビッグデータの価値や意義、その基本的技術や課題、コンプライアンスリスク、個人情報問題、安全性、信頼性等がコンパクトにまとめられているIPA（独立行政法人情報処理推進機構）編、2012年3月発行の「くらしと経済の基盤としてのITを考える研究会報告書　つながるITがもたらす豊かなくらしと経済　～　ビッグデータの価値と信頼　～」(*1)（以降、資料のURL等は、文末にまとめる)を採用し、内容を読み合わせ、適宜、別の資料も参照しながら、議論している。

本来であれば、第1章から順次、議論の様子を紹介すべきであるが、研究会の様子を適宜紹介することを最近決めたので、途中からというよりも最終章からのご紹介になってしまった。お許しいただきたい。もっともこのテキストは各章が独立したテーマを扱っており、これからご紹介する第7章第5節は「ビッグデータを支える信頼性・安全性」というテーマで、システム監査人協会の一研究会のテーマとしてはふさわしいものかもしれない。

２．　第11回情報セキュリティ監査研究会（３月２１日、協会事務局で開催）の討議内容紹介

テキスト第7章第5節を輪読し、討議した。以下、各項目毎にテキストの概要と研究会における議論を記す。

第7章は、「（ビッグデータに関する）新サービス創出のための課題と取り組み」について論じており、第5節は「ビッグデータ活用を支える信頼性・安全性」をテーマにしている。

基本的な考え方

基本的な考え方として、ビッグデータ自体を一旦抽象化したブラックボックスとして扱い、ITと既存産業の融合という観点から、センサー群とシステムが統合した状態でのインフラのロバスト性（ノイズや外乱に対する堅牢性）を確保し、インフラの信頼性・安全性を客観的に開示する仕組み・制度作りを論じている。

次に、ビッグデータ自体に焦点を当てて、データ品質特性と品質確保についても検討している。

（１）社会インフラとしてのロバスト性を確保するための仕組み・制度作り

社会インフラとしてのロバスト性を確保するための仕組み・制度作りに関しては、まず、ビッグデータが社会インフラと言われるための条件として、それが使えなくなった場合の影響が社会にとって甚大かつ深刻である場合であるといい、ケースを次の二つ、すなわち、治療方法の発見に用いられる医療データのようなビッグデータが社会サービスのために使われる場合と、地図データのように、非常に多くの人が使用する場合に分けている。

この場合のロバスト性とは、一般的な高信頼システム構築技術に加え、日々の運用時の取り組みとして、システムそのものの各要素やシステムを取り巻く環境の変化の兆候把握、消費者、インフラ利用者への説明・情報開示・（事

後）対応（代替、補償等）、他サブシステムからの影響の回避等が重要であると言っている。

＜研究会の議論＞

それが使えなくなったときの影響の甚大さが、ビッグデータが社会インフラと言われる条件とした点は、我々が漠然と考えてきたことを明確にしたという点で評価できる。また、その影響の大きさゆえに、変化の兆候把握や、利用者への説明責任をロバスト性の要素として挙げたことも新鮮である。従来型のシステム監査における安全性、信頼性の概念とは一味違う観点である。

ビッグデータに限らず、ICTが社会インフラとして深く広範囲に社会に浸透していく現在、このような新たな視点でのシステム監査の役割・機能の見直しも必要ではないか。

（２）変化する利用環境の継続的モニタリングと製品・サービスの開発・運用へのフィードバックのための手法・仕組み作り

ビッグデータの利活用においては、情報やその分析の種類、精度、確度を拡大・向上させたいという本来的要求がある。ビッグデータを構成するシステムの一部の変化は、ほとんどの場合、他の要素に影響を与える。したがってサービスの内容・方法・質やそれを実現するアプリを絶えずタイムリーに進化・変更させることが必要になってくる。これを実現する開発方法論（アジャイルソフトウェア開発手法など）と変化による影響を極小化する設計手法が求められる。対応には下記二つの側面がある。

［データ類型からみた変化への対応］

データの類型は、追加蓄積型、すなわち継続的に集めることにより価値が増加していくものと、フロー型、すなわちその時点、時点での最新の情報を得るために一時的に集めて分析し、終われば不要になるものとである。

前者は、データそのものが財産であるため、アプリの互換性が重要であるのに対し、後者は、情報の精度が重要であるので、分析結果を表現する端末の互換性が重要になる。どちらの類型でもデータの持つ情報そのものが財産であるので、データの互換性を保証するためのデータ表現・構造の標準化が求められる。

［サービス類型からみた変化への対応］

サービス類型は以下の三つに分類することができる。一つは、公共サービス（気象通報、交通情報等）、この場合は、サービスの互換性・継続性が重要でサービスプロトコルの標準化が必須である。二つ目は、公務（防衛、防犯、治安等）、この場合は、機能の互換性・継続性と改善が重要で、効率的な継続開発方法、分析能力の高度化が求められる。最後は、商用サービス（株価予測、研究・開発、マーケティング等）、この場合は、新規性の競争が生命線であり、効率的かつ短納期での開発が求められる。

＜研究会の議論＞

ビッグデータにおいては変化への柔軟な対応こそが、その価値を決めるという主張は大いに頷けるものである。そのために、データ類型に応じて、アプリの互換性や端末の互換性、さらにデータ表現・構造の互換性が求められるという主張はまさにそのとおりであろう。ただし、データ類型が、単純に追加蓄積型とフロー型に割り切れるものなのか疑問である。たとえば、交通情報などは現時点の情報に基づき最短経路を求めたり、最適交通流制御を行ったりするものであり、その本質はフロー型といえるが、それとても過去の蓄積されたデータにより、機械学習的にノウハウが蓄積され、より精度の高い制御や予測が可能になっていくものである。データ類型の二分はやや単純過ぎる気がする。ここは、追加蓄積とフローを同時に満足するようなデータ表現・構造の標準化とアプリの互換性の重要性を認識すればよいのではないか。

サービス類型の分類も分類自体は正しいと思うが、その三類型ごとに開発手法への要求が異なるというのもいささか言い過ぎのような気がする。ウェイトが多少異なるという程度ではないか。

（3）業種を超えてつながったシステムにおいて信頼性・安全性を客観的に開示する制度の仕組み作り

昨今、ソフトウェアが組み込まれた機器やソフトウェアで実現するサービスがなくてはならない社会インフラになっている。このような機器やサービスが相互に連携して、業種を越えてつながった統合システムに発展してきた。これらのシステムによって利便性が向上する反面、システムの障害が利用者に及ぼす影響は、単一のシステムに比べ、はるかに大きい。

そこで、このような社会インフラ化した統合システムの信頼性や安全性を担保するする仕組みとして、「ソフトウェア品質監査制度（仮称）」（*2）が検討されている。この制度をひとことでいえば、事業者が提供する製品・サービスに対して、第三者機関がシステムそのもの、すなわち、製品・サービスのテスト結果、設計書、開発手順などをエビデンスにもとづき監査し、その結果を利用者に明示する仕組みである。

＜研究会の議論＞

本件については、テキストもソフトウェア品質監査制度の紹介に留まっているので、大きな議論はなかった。しかし、ICTが社会インフラ化していくにしたがい、従来型の事後的なシステム監査やISMSにみられるようなマネージメントシステム型の監査では不十分で、本制度にみられるような第三者機関が積極的にシステムそのもの、すなわち、製品・サービスのテスト結果、設計書、開発手順などをエビデンスにもとづき監査し、その結果を利用者に明示するというような仕組みが必要になってきたという見解には賛成である。

ただし、そもそも事業者の仕事の内容を監査し、利用者が判断の根拠にできるような信頼性のある意見を述べる能力があるような第三者機関が存在するのか、あるいはこの運営の費用を誰が負担するのか、といった制度の実現性に問題があることが指摘された。ところで、我々システム監査人が本制度の第三者機関になり得るのであろうか。

（4）データ品質特性と品質確保に関する手法・仕組み作り

［ビッグデータ時代の社会インフラにおけるＩＴサービス品質］

従来のITシステムでは、個々のシステム毎にそのITシステムで使用するデータが個別に収集され、利用されてきた。そこでは、ITサービスで要求される品質に応じて、ITシステムで使用するデータの収集方法や手順、データの精度などが決定でき、サービスに相応しいデータ品質を確保することは比較的容易であった。ITサービスの品質は、ITシステムの品質×データ品質であるが、これを確保するには、前述のごとくデータ品質は確保されているため、ITシステムの品質確保のみが課題とされてきた。

＜研究会の議論＞

従来のシステムでは、データ品質は確保できていたという指摘は新鮮であった。当然といえば当然である。しかし、従来もデータ品質は十分に確保されてきたわけではなく、確保できるデータ品質のレベルにあわせてサービス品質を決めてきたのが実態ではなかったか。データ品質を見誤ったためにシステム稼働後トラぶったという例は結構あるのではないか。もっともデータ品質を見誤ったのは、システム設計者の責任であり、システム設計者のコントロールの範囲内である。その意味で次に述べられるビッグデータ時代のデータ品質の問題とは次元が異なるとも言える。

［ビッグデータ時代のＩＴサービス品質を支えるデータ品質の確保］

ビッグデータにおいては、ある目的で収集されたデータを、その後、他の目的でも利用される場合があるほか、特定の利用目的を想定せず大量のモニタリングデータを収集・蓄積し、その集積度や網羅性に応じて後から利用目的が決まるような利用形態もある。また、データを収集することなく流れ（フロー）において処理される場合もある。

こうした中、高品質なITサービスを提供するためには、データの品質がそのサービスの要求水準に適合しているかどうか、確認して利用することが重要になる。そのためには、データの品質を示す情報が付加される仕組みと同

時に、高品質なITサービスへの活用を想定したデータの高品質化が重要になる。

以上の観点から、ビッグデータ時代には、ITシステムの品質に係る技術と同様な技術のデータ品質確保への適用が必要になる。すなわち、データ品質の見える化、データ取得プロセスの標準化、データの標準化といったものである。これらは追加蓄積型データ、フロー型データといったデータのタイプによっても異なるものになるであろう。

このほかにもデータ「品質」には様々な観点がある。ビッグデータの分析では“パターン”の発見を目指す。パターンとは、情報の典型性という語と同等である。典型性には、信用性と専門性が大きく作用すると言われている。何らかの指標を設定して、信用性や専門性を評価することが必要になろう。

また、ビッグデータ特有の解決すべき技術的・社会的課題がある。一次データに著作権がないことの確認、一次データ中への個人情報の混入の確実な除去、二次データの著作権保持者の明確化等である。

＜研究会の議論＞

ビッグデータ時代のシステムでは、データありきという観点でシステムの設計やサービス品質の確保を行わなければならないという指摘は、その通りである。むしろ、信用性も専門性も異なる雑多なデータの集積から新たな知見を得るということがビッグデータ分析の本質的な価値であるから、データ品質の確保に拘泥することは、本来のメリットを放棄することになる。むしろテキストが指摘するように、データ品質の見える化に注力し、そのサービス品質に対する保証とすることが肝要であろう。

たとえば、3．11の際にツイッターが大いに活躍したが、その半分は悪意でないにせよガセネタであったという話がある。しかし、それでツイッターの価値がないということになるわけではない。このおかげで助かった人たちも多数いたのだから。かといってガセネタを放置するのも問題である。ビッグデータについてはデータ品質およびその結果としてのサービスの品質に関する何らかの標準化されたレイティング技術が必要になる。

ビッグデータの品質問題は結構、奥が深く、最終的にはその有用性との見合いで判断することになるであろう。また、最後の著作権の問題や個人情報の問題等、従来型の「品質」では括れない新たな問題もある。

これらの種々の問題の解決にシステム監査人がどれだけ関与すべきか、また、どのような形で関与できるか、「ソフトウェア品質監査制度（仮称）」への関与も含め、今後、議論していきたい。

３．　情報セキュリティ監査研究会への参加について

初めて研究会の様子を紹介させていただきました。その雰囲気が伝わりましたでしょうか。もし、ご興味をお持ちになりましたら是非、研究会にご参加ください。毎月20日前後にSAAJ事務局で定例研究会を開催しております。参加ご希望の方は右記アドレスまで、メールでご連絡ください。　　security@saaj.jp

【資料】

(*1) IPA（独立行政法人情報処理推進機構）編、2012 年 3 月発行
「くらしと経済の基盤としての IT を考える研究会報告書　つながる IT がもたらす豊かなくらしと経済
～　ビッグデータの価値と信頼　～」）
URL　http://www.ipa.go.jp/about/research/2011bigdata/

(*2) IPA（独立行政法人情報処理推進機構）技術本部 ソフトウェア・エンジニアリング・センター
2012 年 11 月 13 日公開の下記URLのホームページ参照
「ソフトウェア品質監査制度部会活動報告書及び関連委託事業報告書」
URL　http://sec.ipa.go.jp/reports/20121113-2.html

以上

2013.04 投稿

「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　　序章

個人情報保護監査研究会　主査　斎藤　由紀子

個人情報保護監査研究会では、中堅企業がプライバシーマークを取得する際に必要な基本知識をわかりやすく解説するため「個人情報保護マネジメントシステム実施ハンドブック」を策定しています。
2013年５月号の会報から、その内容の一部を抜粋し、連載でご紹介していきます。

序章　はじめに

１．個人情報保護の歴史

1980年９月23日にOECD理事会勧告が採択された後、1989年経済産業省「個人情報保護ガイドライン、1998年4月「プライバシーマーク」制度発足、2003年5月30日「個人情報の保護に関する法律 」の一部施行を経て、2005年4月1日「個人情報の保護に関する法律」が全面施行となりました。

２．個人情報保護マネジメントシステム（PMS)とは

事業者が自社の事業のために利用する個人情報の取扱について、PDCAサイクルを実行する仕組みです。

３．JIS Q15001：2006　個人情報保護にマネジメントシステム－要求事項

JISQ15001:2006規格は、プライバシーマークの認証基準です。　**１適用範囲**　から、**3.9事業者の代表者による見直し**　まで、事業者がしなければならないPMS(＝PDCA）が規定されています。

４．最近の情報漏えい事故

NPO日本ネットワークセキュリティ協会（JNSA）が、2011年1月1日から12月31日の間に、新聞やインターネットニュースなどで報道されたインシデントについて　「2011年 情報セキュリティインシデントに関する調査報告書」（2012/12/7版）を公表しています。

	2010 年度	2011 年度
漏えい数	557 万 9316 人	628 万 4363 人
インシデント件数	1679 件	1551 件
想定損害賠償総額	1215 億 7600 万円	1899 億 7379 万円
一件当たりの平均漏えい人数	3468 人	4238 人
一件当たり平均損害賠償額	7556 万円	1 億 2810 万円
一人当たり平均損害賠償額	4 万 3306 円	4 万 8533 円

情報漏えいインシデントを起こした組織が、積極的にインシデントを公表する姿勢が定着し、緊急事態発生時の社内ルール（対応手順）の明確化および社内周知の重要性が認識されてきています。

5. 用語の定義

個人情報保護法など法令・規範と、プライバシーマーク認証基準（JIS）の比較を説明しています。今回は紙面の都合で、経済産業省ガイドラインとの比較は省略しています。

JIS		引用：JIS Q 15001:2006（骨子）	条	法令・規範等
2.1	個人情報	JIS：“生存する”の定義はなく、死者の情報も含まれる。 また、“保有期間”、”件数”の定義は無く、一瞬、1件でも個人情報として取り扱う。 上記の他は、法律と同じ	2条	生存する、個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。 政令：過去６カ月以内のいずれの日においても５０００件を超えないものは除外
2.3	事業者	事業を営む法人その他団体又は個人。 JIS：単に事業者と呼ぶ	2条3	「個人情報取扱事業者」個人情報データベース等を事業の用に供している者をいう。
2.6	本人の同意	JIS：本人が個人情報の取扱いに関する情報を与えられた上で，承諾する意思表示が必要。 法律では単に同意を得るとし、手段まで言及していない。	16条	あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。
3.2	個人情報保護方針	事業者の代表者が，個人情報保護の理念を明確にし、規格が要求する６項目を含めて公表する文書。	基本方針	基本方針６：事業者が行う措置の対外的明確化
3.3.1	特定	法：利用目的の特定 JIS:個人情報の特定 自らの事業の用に供するすべての個人情報を漏れなく特定すること。	15条	利用目的をできる限り特定しなければならない
3.3.3	リスク等の認識	漏えい，滅失又はき損については、法律と同じ概念。 JIS：法令等に対する違反，経済的不利益、社会的信用失墜，本人への影響を考慮する。	20条	漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。
3.4.2.1	利用目的の特定	法とほぼ同じ概念 取得する個人情報の利用目的をできる限り特定し、利用目的の達成範囲内で取り扱わなければならない。	16条1	あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。
3.4.2.2	適正な取得	法とほぼ同じ概念 適法、かつ、公正な手段によって個人情報を取得しなければならない。	17条	偽りその他不正の手段により個人情報を取得してはならない。
3.4.2.4	明示	法とほぼ同じ概念 本人から，書面に記載された個人情報を直接に取得する場合には，少なくとも規格が定める事項を，あらかじめ書面によって本人に明示しなければならない。	18条2	契約書その他の書面に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。
3.4.2.5	公表	法とほぼ同じ概念 個人情報を直接書面以外（3.4.2.4 以外）の方法によって取得した場合に，広く一般に自己の意思を知らせること。	18条	個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。
3.4.2.6	目的外利用	取得時に特定した利用目的の達成に必要な範囲を超えて個人情報を利用すること。書面によって本人に通知し、本人の同意を得る必要がある。 JIS：書面で通知し同意を得なければならない。	18条3	利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。
3.4.2.8	提供	法と同じ概念 個人情報を、委託、第三者提供、共同利用、合併に伴う提供を行う場合は、本人の同意が必要。	23条	あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

—	オプトアウト	JIS：法ではオプトアウトでも可。 JIS では不適合となる	23条	あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。
3.4.3.1	正確性の確保	法と同じ概念 利用目的の達成に必要な範囲内において、個人情報を、正確、かつ、最新の状態で管理すること。	19条	利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければならない。
3.4.3.2	安全管理措置	法と同じ概念 取扱う個人情報のリスクに応じて、漏えい、滅失又はき損の防止その他の安全管理のために必要かつ適切な措置を講じること。	20条	取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。
3.4.3.3	従業者の監督	法と同じ概念 従業者に個人情報を取扱わせるに当たって、安全管理が図られるよう、監督すること。	21条	従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。
3.4.3.4	委託先の監督	個人情報を委託する場合に，十分な個人情報の保護水準を満たしている者を選定し、監督すること。 JIS：選定しなければならない。 法では監督のみ	22条	個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。
3.4.4	本人の権利	本人から求められる開示，内容の訂正，追加又は削除，利用の停止，消去及び第三者への提供の停止の求めのすべてに応じることができる権限を有するものに関して，本人から利用目的の通知，開示，内容の訂正，追加又は削除，利用の停止，消去及び第三者への提供の停止を求められた場合は，遅滞なくこれに応じなければならない。 JIS：法のような理念までは規定していない。	3条	個人情報は、個人の人格尊重の理念の下に慎重に取り扱わなければならない。
3.4.4.1	開示対象個人情報	法とほぼ同じ概念 事業者が，本人から求められる開示，内容の訂正，追加又は削除，利用の停止，消去及び第三者への提供の停止の求めのすべてに応じることができる権限を有するもの。 JIS：消去までの期間を問わない。	2条5	「保有個人データ」とは、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データをいう。 政令：6か月以内に消去するものは除外する。
3.4.4.2	開示等の求め	法とほぼ同じ概念 本人から、当該本人が識別される個人情報について、利用目的の通知，開示，内容の訂正，追加又は削除，利用の停止，消去及び第三者への提供の停止を求めること。	24～27条	第 25 条：開示 第 26 条：訂正等 第 27 条：利用停止等 第 28 条：理由の説明 第 29 条：求めに応じる手続
3.4.4.3	周知	法とほぼ同じ概念 開示等の求める場合に提出する様式、手数料の支払い方法など、手順を公表すること。	24条	保有個人データに関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。
3.6	苦情	苦情は、責任ある者まで報告が上がる仕組みが必要である。 JIS：責任ある者とは代表者もしくはその代理の者をいう。	31条	個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。 ２～前項の目的を達成するために必要な体制の整備に努めなければならない。

次回は、「第１章　プライバシーマーク認証取得計画」をご紹介する予定です。

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

以上

2013.04 投稿

注目情報　(2013.3～2013.4)

■【「2013 年版 10 大脅威　身近に忍び寄る脅威」を公開】

最終更新日 2013 年 3 月 12 日
独立行政法人情報処理推進機構
技術本部 セキュリティセンター

本公開資料は、情報セキュリティ分野の研究者、企業などの実務担当者など 117 名から構成される「10 大脅威執筆者会」メンバーの知見や意見を集めながら、近年の情報システムを取り巻く脅威について解説しています。資料は、下記の 3 章構成となっています。

第 1 章　情報セキュリティの変遷

1 章では、情報セキュリティの変遷として、情報セキュリティが定着してきた 2001 年から 2012 年までのセキュリティの変化を振り返っています。

第 2 章　2013 年版 10 大脅威

2012 年において社会的影響が大きかったセキュリティ上の脅威について、「10 大脅威執筆者会」の投票結果に基づき、1 位から 10 位に順位付けしています。

第 3 章　今後対策が重要となる脅威

今後、社会的影響が大きくなると予想される脅威について、「10 大脅威執筆者会」の投票結果に基づき、3 つのテーマについて解説しています。

http://www.ipa.go.jp/security/vuln/10threats2013.html

■【社会保障・税番号制度の導入】

内閣官房

平成25年3月1日 ： 番号法案及び関係法律の整備等法案が閣議決定・国会提出されました。
第 183 回 通常国会 議案番号4 衆議院で審議中 (2013.4.3 現在)
平成25年3月1日 ： 資料「番号制度導入によるメリット」を掲載しました。
http://www.cas.go.jp/jp/seisaku/bangoseido/

■【〈日本公認会計士協会〉「お知らせ」】

平成25年3月27日：
金融庁：「監査基準の改訂及び監査における不正リスク対応基準の設定に関する意見書」の公表について
http://www.hp.jicpa.or.jp/ippan/jicpa_pr/news/post_1728.html

2013.04 投稿

全国のイベント・セミナー情報

■北信越支部　「2013 年度 北信越支部総会・研究会 報告」

会員 No.1281　北信越支部 宮本 茂明

以下のとおり2013年度 北信越支部総会・研究会を開催しました.

・日時:2013 年 3 月 16 日(土)13:00～17:00　　参加者:16 名

・会場:富山県民会館(富山市)

・議題:

- ✧ 年度支部総会
  - 2012 年度活動/会計報告
  - 2013 年度活動/会計計画
  - 2013 年度西日本支部合同研究会 in Kanazawa テーマ検討
- ✧ 本部総会報告
- ✧ 研究会:「ソフトウェア品質監査制度」を考える

◇研究会 :「ソフトウェア品質監査制度」を考える

「ソフトウェア品質監査制度(仮称)/ソフトウェア品質説明のための制度」は, 今後システム監査を進める上でのフォローアップしていくべき事項と考え, 昨年の中部支部との合同研究会に続き, 支部内で理解を深めるために, 該当の本部月例会ビデオ視聴と意見交換を行った.

１．「ソフトウェア品質監査制度（仮称）」の概要確認

本部の第 171 回月例研究会(2012 年 5 月 21 日)ビデオを視聴し, 参加者で「ソフトウェア品質監査制度(仮称)」の概要確認を行った.

- ➢ 「ソフトウェア品質監査制度(仮称)～ソフトウェアの品質説明力強化の取り組み～」
  独立行政法人情報処理推進機構／IPA 技術本部 SEC 統合系プロジェクト(兼)組み込み系プロジェクト
  サブリーダー 工学博士 田丸 喜一郎 氏

また、昨年の月例研究会以降に IPA から報告されている下記の関連情報について概要を確認した.

- ➢ 「ソフトウェア品質説明力強化の普及・推進のための調査」報告書 IPA SEC 2013 年 2 月 15 日公開
  http://sec.ipa.go.jp/reports/20130215.html
  - この報告書では,「ソフトウェア品質説明のための制度」の具体化に向け, 制度の対象候補となりうる産業分野の状況(現状, 将来展望, その産業分野の日本企業のグローバル市場におけるポジショニング等), 諸外国の産業育成の取組み(産業育成施策、規制、国際標準化への取組み等), 過去の国内 IT 関連施策/制度に関する調査結果が報告されている.
    - ✧ 対象産業分野:

重要インフラ 10 分野，主要輸出産業分野，将来の産業分野，広く社会生活、国民生活に影響のある分野

- ✧ 国内 IT 関連施策に関する現状把握
  システム監査制度,プライバシーマーク制度,ISMS 適合性評価制度,ITSMS 適合性評価制度,BCMS 適合性評価制度，Trust サービス

➢ ソフトウェア品質説明力強化に向けた実験報告書　IPA SEC　2013 年 3 月 8 日更新
http://sec.ipa.go.jp/reports/20130215-2.html

➢ SEC journal 第 31 号(Vol8.No.4)「ソフトウェアの品質説明力強化に関する実験を実施」
IPA SEC　2012 年 12 月 14 日公開
http://sec.ipa.go.jp/users/secjournal/SEC_journal_No31web.pdf

- この報告書では，ソフトウェアの品質を説明するためのフレームワークが実際に現場で機能するか具体的なモデルを設定した実験結果が報告されている.
- 12 分野の実験の中から「パッケージソフトウェア製品認証仮想実験」について概要確認を行った.
  - ✧ CSAJ:一般社団法人コンピュータソフトウェア協会の「パッケージソフトウェア品質認証制度について」以下の実験が，監査レベル 1,2 について実施された.
    - ✓ JIS-X-25051(ISO/IEC 25051)準拠レベルでのフィージビリティ評価
    - ✓ IPA-SEC ソフトウェアの品質説明力強化のための制度フレームワークの監査スキームを認証制度に導入した場合のコスト評価
      - 監査レベル 1:重要項目に対するサンプル監査
        ⇒サンプリング精度が向上，認証制度としてコストバランスが成立
      - 監査レベル 2:全項目に対するサンプル監査
        ⇒サンプリング精度が低下，コストバランスが不成立
  - ✧ 結果:監査レベル1が適当と判断

2．「SAAJ 中部・北信越支部，JISTA 中部支部合同研究会」参加報告

昨年の「SAAJ 中部・北信越支部，JISTA 中部支部合同研究会:ソフトウェア品質監査制度(仮称)を受け、我々はどうすべきか」に参加の方々から，合同研究会での各グループでの検討結果を報告いただいた.

➢ 日本システム監査人協会 会報 No.143(2013 年 2 月号)
「2012 年度 SAAJ 中部・北信越支部，JISTA 中部支部合同研究会報告」
http://skansanin.com/saaj/201302/201302SAAJKaihoNr143_hokushinetsu.pdf

3．意見交換

「ソフトウェア品質監査制度(仮称)/ソフトウェア品質説明のための制度」について，参加者で意見交換を行った.

[主な意見]

- 保証型監査の場合，業界毎の詳細基準が必要．どのレベルまで詳細基準を作っていくかが課題ではないか．
- 社会インフラ関連の制御システムの品質は重要だが，関係者以外には見えない／分からない状況にあるのではないか．
- あるソフトウェア開発の現場に加わった際，1 か月間に約 50 人体制で進められたプロジェクトで，プログラミング工程においてプロパ数名，残りが協力会社社員で，月単位で人が入れ替った現場もあった．こういった開発の中で，どう品質を第三者として見ていくか難しいと感じた．
- この制度が，コスト圧迫でなく，ソフトウェア品質を説明できることのメリットを享受できる制度にならないといけないと考える．
- 小さなソフトウェア開発企業の場合，品質部門を持つ体力がないところも多い．
- 負担が多く，日本だけの制度であれば，競争力が落ちる懸念もある．

・統合システムが現実のものとなってきている．家電のインターネット接続が進み，複数メーカ製品の接続とリモコン操作の複雑さにより，特定の人しか使えないシステムになっているのではないか．
ユーザインタフェースが重要であり，こういった分野での，ユーザビリティ（実際に使用できること/使いこなせること）に関する監査も重要ではないか．

４．今後に向けて

この研究会後，3 月末に IPA から「ソフトウェア品質説明のための制度ガイドライン（案）」のパブリック・コメントが募集された．「ソフトウェア品質監査制度（仮称）/ソフトウェア品質説明のための制度」について，今後も引き続き支部例会でフォローしていきたいと考えている．

- 「ソフトウェア品質説明のための制度ガイドライン（案）
  ～パブリック・コメント募集のお知らせ～ 」IPA SEC 2013 年 3 月 29 日公開
  http://sec.ipa.go.jp/pubcom/20130329.html

■日本システム監査人協会近畿支部　「第１３９回定例研究会報告」

会員 No1710　小河裕一

１．テーマ　　：「マネジメントシステム規格の統合的な利用と効果的な認証審査」
２．講師　　：　有限会社吉谷コンサルティング事務所　吉谷　尚雄氏
３．開催日時　：　２０１３年　3月15日（金）　１８:３０～20:３０

４．開催場所　：　大阪大学中之島センター　2階　講義室201
５．講演概要
（1）アジェンダ：　講義いただいた内容は以下の通りである。
①　マネジメントシステム規格の動向について
②　マネジメントシステム規格共通文書化
③　複数のマネジメントシステムの統合的な構築と運用
④　効果的な認証審査
⑤　個人情報保護監査研究会のご紹介　（本報告では省略）

（2）内容

①マネジメントシステム規格の動向について

マネジメントシステム規格の認証とは、依頼企業と直接的に利害関係の無い認証機関が、依頼企業のマネジメントシステムに対する適合性を証明することである。認証機関は JAB や JIPDEC 等の認定機関から認定を受けている。現在認定を受けている認証機関は、QMS:46 機関、EMS:42 機関、ISMS:26 機関であり、日本の認定機関から認定を受け、認証している総数は全体の 50%程度である

マネジメントシステムには、以下のようなものがある。

・**品質マネジメントシステム（QMS）**:「顧客満足」が最大目的である。改正の予定は 2013 年に作業原案（WD）が提出され,2015 年に正式改正する予定である。

・**環境マネジメントシステム（EMS）**:「環境に及ぼす影響を最小限にとどめる」が最大目的である。2013 年 2 月に改正案が委員会原案に移行することが決定した。他のマネジメントシステムとの整合性向上も内容に含んでいる。EMS は QMS と比較すると改正が順調である。

・**情報セキュリティマネジメントシステム（ISMS）**:「情報セキュリティ」が最大目的である。現状の改正は基本的に 2005 年版を引き継ぐ形で 2005 年以降の動向に対応したものであり、2013 年には改正される予定である。

・**労働安全衛生マネジメントシステム（OHSAS）**:これは働く人々の健康を精神的な側面を含めて守るマネジメントであり”ISO”ではない。このため日本の認証機関は海外の認定機関から認定を受けている。前回の改定は 2007 年。2012 年現在で定期改正作業を実施中である。

・**個人情報保護マネジメントシステム（PMS）**

JIS Q 15001 であり、改正動向は不明である。国内の関連情報として、以下のものがある。

個人情報保護法・・・・改正には消極的
マイナンバー法案・・・・いったん廃案
個人情報保護省庁ガイドライン・・・・省庁間の整理が進んでいない。
JISQ15001 と法律における不整合の合致作業・・・・すすんでいない。

マネジメントシステム認証の現状として以下の事項が挙げられる。

・JAB 非認定の認証機関から適合認証をうける「プライベート認証」が増加している。

・ISO認証について、社会からの信頼性が叫ばれている。

②規格の共通文書化

複数あるマネジメントシステム規格の標準化が目的である。

例として、9001,14001,27001 の「教育」の要求事項は以下のようになっている。

9001: 力量、教育訓練及び認識

14001:力量、教育訓練及び自覚

27001:教育・訓練、意識向上及び力量

このような共通部分に関して曖昧さを排除して、できるだけ具体化した表現となるようにして統一化することが目的である。共通文書化することにより変わる規格の解釈として、以下があげられる。

・組織の事業プロセスへマネジメントシステムの要求事項との統合を求められる。

・マネジメントシステムの計画において、「リスクと機会」を見定めて取り組むことが求められる。

・「リスク」という概念が共通で導入される結果、共通部分に「予防処置」の規定がなくなる。

③複数のマネジメントシステムの統合的な構築と運用

規格の共通文書化に組織として対応するためには、プロシージャが複数存在し整合性がとれない場合がでてくる。この状況を未然に防ぎ、認証企業側で統合して運用していくために以下の手順を薦める。

・部署毎に自部門の現状業務に関する仕組みを調査し、仕事のプロセスを意識した「業務記述書」を作成。

・5W1Hを意識して、「業務記述書」を仕事の「手順書」に書き換える。

・手順書にマネジメントシステム共通の要求事項や法令規制の要求事項を付加していく。

・作成した「手順書」に基づいて運用を開始し、日々の業務を行っていく。

この「手順書」を元にして内部監査を実施する場合、「手順書通りの運用か否か」を見る形となる。重要なことは「手順書通りに業務が運用されているか？」であるので必要に応じて手順書を現状の仕事に合わせて改訂することも必要となる。ただし、実際の手順が手順書だけではなく、「法令・規制」に反している場合は実際の作業手順を修正する必要がある。

④効果的な認証審査

企業がマネジメントシステムの認証をうけるメリットとは

・認証を受けていることで、一般消費者や取引先に組織の信頼性をアピールすることができる。また取引条件となっている場合もある。

・定期的な認証審査によって、マネジメントシステムの継続的な維持・改善が図れる。

という点があげられる。

6. 所感

企業が認証取得している代表的なISO 規格として9001/14001/27001 があります。お話の前半では、これらの「マネジメントシステム」をご存知無い方にもわかりやすくするために、「マネジメントシステムとは」と「どのような改訂動向なのか」を説明していただき、状況が把握できたと思います。後半では、これらマネジメントシステムにおける共通テキスト化が、どう影響を与えるのか？また、それに対応するにはどのようにすればいいのか事例をあげて話をしていただき、非常に内容の濃い講演であったと感じました。

以上

2013.04

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

2013 年の最初の会報テーマは「システム監査の普及促進」です。

この「システム監査の普及促進」は、4月号までのテーマとしたのちは今年の”基調テーマ”として、3か月ごとのテーマとは別に1年間継続し、皆様と幅広く深く意見交換して行きたいと考えています。

5 月号からの 3 ヶ月間の会報テーマは「システム監査活性化への提言」としました。おりしも、協会の重点施策である「会員増強プロジェクト」の名称も平成 25 年 4 月から「システム監査活性化プロジェクト」に変更したばかりです。協会の部会、研究会、支部などの活動の場でも白熱した議論をお願いいたします。

□■ 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)

これらは、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。

ワークショップのお知らせ

今月末から始まる連休中に、スキルアップしませんか。会報サイトでも採用している次のテーマでワークショップを開催します。実際に構築する、有効性やセキュリティを評価するには実際に操作するのが一番。会報サイトに詳細案内しますので関心をお持ちの方は申し込みください。

１．ビジュアル、ズーミングプレゼンテーション　Prezi　（プレジ）を使おう

２．世界で最も普及している CMS ツールのワードプレス

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/

■会員でない方が送付停止を希望される場合、購読申請・解除フォームに申し込んでください。

【送付停止】 http://www.skansanin.com/saaj/

■□■SAAJ会報担当━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

編集：仲 厚吉、安部 晃生、越野 雅晴、桜井 由美子、中山 孝明、藤澤 博、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）

━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━