特定非営利活動法人
日本システム監査人協会報

2013年10月号
No 151

No. 151（2013年10月号）＜9月20日発行＞

秋の野にコスモスがきれいに咲いて風に揺れています。

会報10月号は、システム監査の記事が満載です。

2013.09 投稿

めだか【 システム監査活性化の一考察～ジェロントロジーと生きがい就労に向けて～ 】

「ジェロントロジー」は、あまり聞きなれない言葉である。発達心理学から派生した比較的新しい学問領域で、「老人学」や「老年学」とも呼ばれている。「老（おい）」という言葉がつくとネガティブなイメージが強くなりますが、「加齢学」とも説明され、こちらの方がイメージとしてはるかに良い。

日本の社会では、平均寿命が男性79歳・女性85歳（平成23年：簡易生命表：厚生労働省）になり、人生80年の長寿命社会になった。また、今後の人口推計によれば、2030年には65歳以上の高齢者が人口の3分の1を占めるようになり、特に大都市部の「東京」「大阪」「神奈川」「愛知」では、「団塊の世代」の増加で地方部に比べて急速なスピードで高齢化が進むとされている。東京大学の秋山教授が20年以上にわたって追跡調査した結果によると、男性の場合は約8割の人が70歳台半ばまで自立して生活できる程に元気でいるそうである。

平成25年4月に「高年齢者雇用安定法」の改正より、高年齢者の就労機会は延長された。「システム監査の活性化」には、企業活動をリタイアしたと同時に「システム監査」の分野や協会活動から離れるのではなく、リタイア後も「システム監査」の分野や協会活動との関わり方も重要ではないだろうか。私たちの多くはこれまで何らかの形で、情報システム開発の現場や監査の業務に携わってきた「専門家」であり、企業をリタイアした後にフルタイムでなくとも、NPOやLLPへの活動参画といった多様な形態で、一人ひとりが関れるレベルの範囲と時間で、システム監査の活性化や情報システムの効率化・信頼性や安心・安全な社会構築に貢献できたら、リタイア後の人生が素晴らしい、充実したものになるのではないかと思う。もちろん、その為には、技術進歩の著しいIT分野で、新しい技術や知見の習得の自己研鑽に絶えず励んでいくことも大事になる。

加齢学の研究では、認知能力の加齢による変化は「短期記憶能力」は残念ながら40歳をピークに落ちてくるが、「日常問題解決能力」や「言語（語彙）能力」は、70歳位まで向上し続けると言われている。認知症分野の研究では、簡単な計算や音読を継続することにより、認知症の症状が改善していくそうである。さらに、外と接触を採らず家の閉じこもりがちになると、『うつ』傾向が早く進むとも言われている。

毎日、何等か形で「脳」に刺激を加え、緊張感を持ち身体を動かして生活していくことは、現役時代の就労で『お金を得る』という次元から、『生きがいを得て、楽しむ』（生きがい就労）に次元を変えることであり、健康で自立して生活できる期間を少しでも延ばすことにも繋がるのである。

企業をリタイアした後の人生を考えた時に、今まで私たちが経験してきた分野や能力を活用して、社会と繋がっていくことは幸せなことであり、社会貢献にも繋がる。人生の仕上げである高齢期を「システム監査」に関して活動をすることは、私達ひとり一人が充実した人生を全うすることになると思う。

（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。）

2013.09 投稿

めだか【「システムリスク監査」と言い換える（システム監査の使いみち）】

「システム監査」は「システムリスク監査」と説明してもいい。本質は変わらないし変えてもいない。さらに言えば「システムリスク監査」と言い換えることで分かりやすくなる。機能が明確になり名実がより一致する。広義と狭義ではなく、どちらも幅・長さ・高さ・深さなど活動領域や対象範囲・着眼点などに異なる点はないと考えている。

現況、情報システムを監査・審査・認証・点検する制度は多い。枚挙にいとまがないほど専門分野に細分化されその傾向は増している。それらの研究分野なども多々あり、監査や審査等の従事者の技術や能力を認定する資格制度もまた専門分野単位の細分化が続いている。

これらには必然性があり、背景に情報システム社会の急速な進展とそれを支える技術的な高度化と利用形態の多様化がある。点（組織単位のシステム）が面でつながりさらに重なり合っている。企業統治、内部統制、説明責任、リスク経営、コンプライアンスは情報システムと不可分だ。オフショアやクラウドなど外部委託の形態は大きく変化し、組込みシステムなど消費者個人の手許には意識されないシステムが拡散している。さらに不透明なビッグデータ活用、あきらめ感がはびこるウイルス、多大なコストをもたらす情報漏洩など、など・・・

このような環境変化のなかで、システム監査は何なのか、何をしてくれるのか、何を対象にどのような機能があるのか、細分化された専門分野とどのように差別化するかについて、システム監査を利用する側もシステム監査を実施する側も、わかり難いと思い思われている点が少なからず存在している。

本稿のタイトルは、そのわかり難さから抜け出そうとする意だ。小生の意識の中にはいつも「システムリスク監査」があり「システム監査」と全く同義語と認識して扱っている。

・システムリスクのあるところすべてがシステム監査の対象
・システムリスクを点検するのがシステム監査の役割
・被監査業務におけるリスクコントロールの状況が着眼点　など

情報システムの監査・審査・認証・点検制度がいかに専門分野に細分化されていようとも、システムリスクに真正面から向き合い、システムリスクを分野で特定せず除外せず、隠れているシステムリスクまで浮き彫りにするのがシステム監査であり、この点から「システムリスク監査」と称した。事業存続リスクに直結しているシステムリスクを、被監査組織に適応した視点で現場レベルまで点検する監査機能を再認識することが、システム監査に携わる者のスタンスを強固にするものと自らも意識している。

「システムリスク監査」というスタンスから、監査の手順・力点・着眼点などが自ずと導き出される利点も伴う。
システムリスク管理方針は明確か、情報資産のリスク評価がされているか、リスク評価に基づいた投資や管理がされているか、事業目的を阻害するシステムリスクは優先的にコントロールされているか、日常業務の仕組みにリスク認識が浸透しているか、業務遂行状況はリスク管理に反映されているか、内部監査やセルフコントロールはチェックリストに頼る単なるチェッカーではなくリスクアプローチとなっているか、など・・・

システム監査を利用する側にとって、理解されやすい、利用しやすい、納得しやすい、を重視し取り組みたい。

（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。）

2013.09 投稿

めだか【 システム監査の使いみち 】

めだかテーマ「システム監査の使いみち」も今月が最後になるようです。

これまで私は、“「報告」目的が拡大された新COSO内部統制フレームワーク”、また“IRとシステム監査”と題して「システム監査の使いみち」について思うところを書いてきた。

最終回の今回は、本年 5 月号の本会報で書いた**「将を射んと欲すれば‥‥（システム監査活性化への提言）」**の主旨を思い起こし、私の、テーマ「システム監査の使いみち」の終わりにしたい。

「将を射んと欲すれば‥‥（システム監査活性化への提言）」では、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く、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した。そして更に、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この不完全性を一層特徴付けるとも書いた。

そして、不完全性を内在するから利活用をやめるというのでなく、情報システムの健全な利活用の一層の促進には、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であると書いた。

その上で、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）が不可欠であり、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実施が必然的に求められる。

つまり、これが「システム監査の使いみち」の本質だと書いた。

システム監査は、システム監査人の介在により、当事者以外の監査人の目で評価、確認することにより、当事者では気付かなかった問題、課題が抽出できるなど、避けがたい失敗リスクの低減に寄与する可能性も持つ。しかし、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というストーリーの中では、これらはもはやシステム監査の副次的な効用に過ぎず、「システム監査の使いみち」の本質ではないのではないか。

システム監査過程での監査人による助言は「副産物に過ぎない」（監査はコンサルティングとは明確に異なる）とすることは、多くのコンサルティング志向、助言型監査志向のシステム監査人にはなかなか受入れ難いものかもしれない。しかし、コンサルティング志向、助言型監査志向は、監査とコンサルティングの違いを曖昧にし、結果的にシステム監査の何たるか（システム監査の Identity）を不明確にし、結果、情報化社会に欠かせないシステム監査の普及にマイナスの力ともなる（と思う）。

システム監査（但し、内部監査として行うシステム監査は除く。内部監査は経営者の経営のツールでありシステム監査の目的、使い方は経営者の考えにより決まる。）は、説明責任の遂行を支援し、それにより当事者間の信頼関係構築を助長し、結果情報システムの利活用を促進し、情報社会の恩恵を社会が享受する一助となる。これが「システム監査の使いみち」の本質ではないだろうか。

（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。　）

2013.09 投稿

めだか【 パーソナルデータの利活用（システム監査の使いみち） 】

大量の個人の情報を取り扱うパーソナルデータの利活用について、「パーソナルデータ利活用の基盤となる消費者と事業者の信頼関係の構築に向けて （2013年5月10日）IT融合フォーラム パーソナルデータワーキンググループ」というレポート（以下、同レポートという。）を読むと、個人の立場と、企業の立場の間に問題のあることがわかる。同レポートでは、両者の立場の間にある問題の解決のキイワードに、「分かり易さ」を挙げている。

折しも、Suica利用データ提供について The Huffington Post（2013年7月25日）の記事によれば、“JR東日本は25日、Suicaの利用データをマーケティング目的で日立に提供する件について、詳細を発表。プライバシー面で事前の説明が足りなかったことなどの批判を受け、「大変なご心配をおかけした」と謝罪した。”とあり、また、“Suicaのユーザーは希望すれば、他社に提供するデータから自分の分を除外できる。自分のSuicaの番号をjogaiyobo@jreast.co.jp へメール、または 03-5334-1655 に電話して入力すればよい。”と伝えている。

JR東日本は、Suicaの鉄道での利用データのうち、乗降駅、利用日時、鉄道利用額、生年月（日は除く）、性別及びSuicaID番号を他の形式に変換した識別番号からなるデータを統計分析用に提供しているとのことである。提供先では、データを統計的に分析し、駅の利用状況の分析データをさまざまな分類でまとめた分析リポートを作成し活用するとのことである。また、個人情報に関しては、JR東日本が提供しているデータには、氏名や連絡先など個人が特定できる情報は含まれておりませんと説明している。しかし、「個人情報の保護に関する法律」（法第2条第1項）では、個人情報は、“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。”とあるため、SuicaID番号を他の形式に変換した識別番号なるものの秘匿化の深さが問題になると考えられる。

一方、同レポートによれば、“EUと米国は、パーソナルデータの利活用の前提として、時代の要請に応じたプライバシー保護のルールに関する様々な提案を行っている。”とある。我が国においても、パーソナルデータの利活用においてプライバシー保護のルールが問われる時代になっている。同レポートの提案をはじめ、プライバシー保護のルールに関する提案への国民的合意が必要になってきている。今や、システム監査人は、関与する情報システムがパーソナルデータを利活用する情報システムである場合、プライバシー保護のルールに関する提案への国民的合意をもとに、システム監査の点検項目を整備し、システム監査に当たる時代にいると思う。

（空心菜）

（参考）

「パーソナルデータ利活用の基盤となる消費者と事業者の信頼関係の構築に向けて
（2013年5月10日）IT融合フォーラム パーソナルデータワーキンググループ」
「JR東日本、Suica利用データ提について謝罪 希望者は提供データから除外も」
http://www.huffingpost.jp/2013/07/25/jreast-suica-hitachi_n_365150.html」
「個人情報の保護に関する法律」（消費者庁）

2013.09 投稿

投稿【システム監査の使いみち】

会員番号 0557 仲　厚吉（システム監査活性化PT・個人情報保護監査研究会）

五輪・パラリンピック 2020 東京開催決定の吉報がありました。五輪・パラリンピック 2020 東京開催が日本の経済成長に良い影響を与えることを期待したいと思います。

日本政府が導入を進めている共通番号は、社会保障と税の一体改革のため、情報システムのキイコードとして、2015 年から導入予定になっています。「参考１」によれば、国民一人ひとりに番号を振り、所得や社会保障などの個人情報を管理する「共通番号制度」において、甘利明経済再生相は、6 月 11 日、個人に振る番号を「12 桁」、企業など法人に振る番号を「13 桁」にすると発表しました。番号は個人すべてに振る、さらに、法人税を納める対象になっている企業やNPOなど法人すべてにも振るということです。2015 年 10 月から番号の通知を始め、16 年以降、希望する個人には顔写真つきのICカードを配るということで、個人番号と法人番号を混同しないように桁数を変えたということです。「参考2」によれば、韓国で個人情報保護法を強化したのは、住民登録番号の不正乱用を防ぐためであり、実際、韓国では個人情報の漏えい事故は後を絶たないということです。韓国の住民登録番号は、日本政府が導入を進めている共通番号に相当します。日本においても同じ様なリスクを想定する必要があると思います。

韓国では、2014 年 8 月から、政府公共機関や一般企業が住民登録番号を収集したり利用したりできなくなり、また、個人情報漏えい事故が発生した際の企業責任が、一層厳しく問われるようになる、と伝えられています。

韓国の「個人情報保護法の改正法」は、インターネットサービスプロバイダーなどのオンラインサービス事業者が住民登録番号を収集／利用することを禁止する「情報通信網法」改正（2013 年 2 月本格施行）に続くもので、オンラインサービス以外の業種の民間企業や、公共機関に、セキュリティ対策の強化を促すというものです。これまでの公共機関や一般の民間企業は、個人の同意を得られた場合に限り、住民登録番号の収集が許されてきましたが、今後は、番号の所有者や第三者の差し迫った生命や身体の危機に関わる場合などを例外として、原則的に収集や利用が禁止となるということです。既に収集した住民登録番号は、改正法施行から 2 年以内、すなわち 2016 年 8 月までに破棄しなければならないといわれています。また、住民登録番号を漏えいした企業や機関の法的・社会的責任が重くなり、今までは安全性確保の措置を果たさなかったと認定された場合のみ企業に過怠金と刑事罰が課されてきましたが、今回の改正では、明確な因果関係の有無にかかわらず、課徴金を、最大 5 億ウォン賦課できるようにするということです。さらに住民登録番号漏えいなどの法律違反を犯した機関や企業に対しては、最高経営責任者（CEO）などの代表者や役員を対象とした懲戒勧告を行政機関が行えるようにしたということです。

システム監査人は、システム監査の使いみちにおいて、個人情報漏えい事故の事後の是正処置対応も重要ですが、事前にリスクを分析し、講じることとした予防処置の有効性を点検することが、より一層求められていると思います。

以上

参考1：朝日新聞 DIGITAL（2013.6.11）『共通番号制、個人 12 桁・法人 13 桁　15 年通知開始』
参考2：日経コンピュータ（2013.9.5）アジア最前線『韓国が個人情報保護法を改正へ　企業 CEO も懲戒勧告の対象に』

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
“引続き、会員の皆様の継続的なご支援、ご協力をお願い致します。”

2013.09 投稿

会長コラム【 日頃の協会活動へのご参加、ご支援、ご協力に心から感謝しています 】

会員番号 0841 沼野伸生(会長)

本年度も残すところ 3 ヶ月余りとなりました。また、本年は協会創設 26 年目、NPO法人化 13 年目になります。

四半世紀を超える長い間、システム監査の社会への普及促進を掲げ活動を継続できているのも、一重に会員の皆様の継続的なご参加、ご支援、ご協力の賜物です。誠にありがとうございます。

会員の皆様等の最近のご参加、ご支援、ご協力についていくつかご報告させて頂きます。

協会各研究会等への参加としては、本部主催の月例研究会、事例研究会等、また支部主催の各種研究会へ多くの会員の皆様にご参加を頂いています。特に代表的研究会である月例研究会では、最近毎回 150 名以上、時に 200 名を超える申込みを頂いており、会場の定員制限から期限前に申込みを締め切る事態も発生している状況です。また、事例研究会では毎月時々のテーマを設定し、ベテランと若手システム監査人が討論する「白熱教室」も、過去の当協会にない新しい試みとして注目を集めています。

協会主催のセミナーについては、システム監査実践・実務セミナー、課題解決セミナー等、また、CSA向け継続教育セミナーにも、会員、非会員の多くの方々にご参加頂いています。中でも課題解決セミナーは特に好評を頂き、開催回数を重ねています。

会報については、電子化を機に毎月発行とし、毎号 30 頁から時に 60 頁を超える情報を会員の皆様へ配信すると共に、システム監査人のコラム「めだか」にも、常連の投稿者に加え、新たな投稿者も少しずつですが増えてきました。協会の会報は数年前から国立国会図書館への納本も実施しています。

本年度初めて、当協会が認定するCSA（公認システム監査人）の全体交流会を開催し、多くのCSAの方々にご参加頂きました。CSAに興味を持ったCSAでない方、また非会員の方にもご参加頂いたのは大変有難いことでした。

更に、システム監査関係団体との相互情報連携を活発化させ、当協会のセミナー開催情報を関連団体のご協力を得て、それぞれの団体の会員の方々にメーリングリストで毎月ご案内頂くことにしています。例えばISACA東京支部、システム監査学会、JASA、JISA、FISAなどにご協力頂いています。これも月例研究会の参加人数が大幅に増加した一因かも知れません。

そして最後に、多くの会員の皆様から寄付を頂戴し、ご支援を頂いています。

財政基盤の拡充と協会活動の一層の活発化を狙いに、平成 24 年度の事業計画に寄付活動の検討を掲げ、平成 24 年度から会員の皆様へ当協会活動への寄付のお願いを公式に始めました。

そして、平成 24 年度は 100 名以上の方々から総額 40 万円を超える寄付を頂き、また本年度も既に 60 万円を超える寄付を頂いています。寄付については、平成 23 年度にも協会監修書籍の執筆に関った会員の方々から、執筆者が受取る印税を寄付して頂いた実績もあります。誠にありがとうございます。

SAAJは、今後も運営の効率化、体制の刷新・充実化を図り、一層協会活動を活発化し、システム監査の社会への普及促進に引続き取組み、この会員の皆様等のご参加、ご支援、ご協力に真摯に応えて参ります。

引続き、会員の皆様の継続的なご支援、ご協力をお願い致します。

以上

2013.09 投稿

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 0557 仲　厚吉（システム監査活性化PT）

今月の会報でも、システム監査の活性化につながる活動を行っている当協会の研究会や担当組織の中から、いくつかの活動について、ご報告しています。

1. システム監査基準研究会

IT-AuditのISO化について、最新の報告です。

2. 情報セキュリティ監査研究会

毎月、研究会で研究・討議している話題の中から、会員の皆様に知っていただきたい、よろしければご一緒に議論に加わっていただきたい情報をご紹介しています。今回は、前回の「新サービス創出のための課題と取り組み」に続いて「プライバシー・バイ・デザイン」についての情報提供です。タイトルだけからではお分かりになりにくいと思いますが、報告の内容をぜひお読みください。

次回に向けても、プライバシー・バイ・デザインについて研究、討議する予定です。参加されたい方は、お気軽にご連絡ください。

3. 個人情報保護監査研究会

今月も、研究会でまとめた『個人情報保護マネジメントシステム実施ハンドブック』簡易版の内容の一部を紹介しています。

システム監査人の主要な活動分野の一つである個人情報保護マネジメントシステム（PMS）の構築・評価を行う際の参考にしていただければとの考えで、ご紹介しているものです。なお、このハンドブックをベースにしたPMS構築の実践ノウハウを身に付けていただくセミナーも計画しています。セミナーの実施が決まりましたらご案内しますので、ご参加ください。

以上

2013.09 投稿

【　システム監査基準研究会　報告　】

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

○ IT-ＡｕｄｉｔのＩＳＯ化について

8/19(月)～22(木)東京の機械振興会館において、ISO/IEC JTC 1/ WG 8 の国際会議が開催されました。
本会議には、当協会から力副会長、清水理事とオブザーバーとして松尾理事と松枝副会長が参加しました。

主な参加国は、議長がイギリス、その他オーストラリア、ニュージーランド、南アフリカ、フィンランド、アメリカ、韓国、日本と ISACA の代表で、合わせて 20 数名が出席しました。

冒頭、5 月に日本から提案していた PDTR：30120（IT-Audit―IT ガバナンスの評価を支援するための監査ガイドライン）に関する国際投票結果が議長より報告されました。

投票数 10 カ国で、賛成8（原案のまま賛成6：中国・アイルランド・イタリア・マレーシア・ロシア・アメリカ、コメント付き賛成2：日本・スウェーデン）で、反対2（コメント付：フィンランド・韓国）、棄権22（コメント付き1カ国：オーストラリア、コメントなし21）でした。投票国の 8/10 が賛成でしたので、2/3 要件を満たしており投票はクリアすることができました。

大会3日目の8／22(木) の午後になり、漸くオーストラリア・フィンランド・日本・韓国・スウェーデンから提出されたコメントについて全体で討議しました。

韓国をはじめとしていろいろと意見がでましたが、日本側は松尾理事を中心に意見表明し、一応全てのコメントに対して結論をだすことができ、結果として、次のステップ（DTR）に向けて活動していくことになりました。

またこの会議では、WG8に関するいろいろな作業の提案（NWIT：New Work Item）があり審議されましたが、提案の特徴として、ISO38500（ITガバナンス）をベースにしたものが複数あったことがあげられます。欧米では、ISO38500が定着しつつあるのだなと感じました。日本においてもJIS化が予定されている来年度以降、普及していくことが期待できます。

今回出席して、あらためてこのような国際会議の場で全体の意見を取りまとめて基準を作成していくことがいかに大変なのかを知ることが出来ました。

ここまで来たのですから、基準研としても是非最後までフォローしていきたいと思っています。

なお会議の詳細な内容については、9/24(火)のCSAフォーラムで報告予定です。

2013.09 投稿

【情報セキュリティ監査研究会だより その６　－　プライバシー・バイ・デザイン　第１回】

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の活動状況の会報連載は、本号で第6回になります。今回から、新たなテーマ「プライバシー・バイ・デザイン」に移ります。当面、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」(*1)をテキスト(以下、左記の書を「テキスト」と称します)として研究を進めてまいります。単にテキストの輪読のみではなく、他の周辺情報も含め、「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いきたいと思います。

今回は、第1回として、テキスト第1章を参照しつつ、プライバシー・バイ・デザインとは何か、その意義と目的、また、国際的にどの程度受け入れられているのか等を、研究会の見解、所感を交えながら、お伝えしたいと思います。

以下の記事は、テキストの他に2009年9月に公開された「Privacy by Design Curriculum 2.0」(*2)も参考にしております。また、新テーマの第1回ということもあり、できるだけ原典の資料（例、1980年OECD勧告）に当たりました。そのため、文末の資料URL等の記述がやや長くなっておりますが、プライバシー・バイ・デザインに関する原典資料のインデックスとして、ご活用いただければと思います。

なお、本報告は、情報セキュリティ監査研究会内部の検討結果であり、日本システム監査人協会の公式の見解ではないことをお断りしておきます。また、テーマが斬新かつ理念的なものであるため、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。また、ご興味のある方は、是非ご参加ください。

(*)で示すテキスト、参考資料等の名称、URL等については、文末にまとめて記載します。

【研究テーマ】「プライバシー・バイ・デザイン」のご紹介

１．プライバシ・バイ・デザインとは何か、その定義と意義

「プライバシー・バイ・デザイン」とは、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(*3)であるアン・カブキアン博士が1990年代から提唱するコンセプトである。

「プライバシー・バイ・デザイン」は、その名の通り、設計段階からプライバシー保護を検討・実装するという考え方で、このような考慮をすれば事業者にとっても消費者にとってもポジティブサム(Win-Win)の関係をもたらすというものである。この考え方は、従来のプライバシー保護に対するマイナスのイメージ、すなわちプライバシー保護プロセスは単なるリスクに対する対応プロセスでしかなく、事業者にとっても個人情報を提供する消費者にとっても何ら付加価値を生むものではないといった概念を覆すものであり、画期的なものだと思う。

逆に言うと、従来型のプライバシーに対する考慮なしに作られたレガシーなシステムに対して、事後的に個人情報保護のためのプログラムやプロセスを追加しても、容易には実効性のあるものにならないと主張しているようである。ビッグデータやSNSの進展、拡大に伴い、システム全体、あるいは、それが機能する社会経済プロセスそのものをプライバシー保護の観点から、抜本的に、かつ、より生産的なプロセスになるように見直そうという運動とも思える。

参考のためにテキスト第1章の冒頭の部分を引用する。

「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＞－－これが、提唱者であるアン・カブキアン博士による、プライバシー・バイ・デザインの基本的な定義である。」、テキスト、P10。

プライバシー・バイ・デザインの目標とするものは、「公正な情報の取り扱い」である。

NSAによる通信記録傍受事件は情報が公正な取り扱いをされていなかった典型例であるし、いくつかのネット事業者が、提供者の許諾を得ずに個人情報を取得していた事実などもその例である。また、共通番号制度の最大の焦点は、「公正な情報の取り扱い」を如何に担保するかにある。設計段階からプライバシー問題に適切に取り組んでおけば、「公正な情報の取り扱い」が保証され、プライバシー侵害のリスクが低減するだけではなく、データ活用の面でも事業者側、消費者側双方に有益な結果をもたらすことを主張する「プライバシー・バイ・デザイン」は、IT の社会インフラ化が進展し、ビッグデータ活用とSNSが普及しつつある現代の課題に適合した優れたコンセプトだと思う。

２．プライバシー・バイ・デザインの７つの基本原則とＰＩＡとの関係

プライバシー・バイ・デザインは、以下の7つの基本原則によって「公正な情報の取り扱い（FIPs：Fair Information Practices）」を実現する。

① リアクティブではなくプロアクティブ；事後的救済ではなく予防
　プライバシー侵害が発生してから事後的に対応するのではなく、それらが発生することを事前に予防する。

② デフォルト設定としてのプライバシー保護
　個人が何もしなくても最高レベルのプライバシー保護がなされるよう、システムはデフォルトとして最高レベルのプライバシー保護の設定がなされていなければならない。

③ 設計に埋め込まれたプライバシー対策
　ITシステムやビジネスプロセスにおいて、プライバシー対策は、設計段階から、あるいは、アーキテクチャーとして埋め込まれていなくてはならない。

④ すべての機能が対象　－　ゼロサムではなくポジティブサム
　プライバシー対策は、すべての機能に渡り、かつ、他の利害関係とゼロサム、すなわち、トレードオフの関係にあってはならず、ポジティブサム、すなわち、WIN－WINの関係になることを目指す。

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に渡っての保護
　システムあるいはビジネスのライフサイクル全体に、始めから終わりまでのエンド　ツー　エンドのセキュリティ対策が埋め込まれていなければならない。

⑥ 可視化と透明性　－　オープンな状態に
　事業者は、ステークホルダーに対して、ビジネスや技術に関して、可視化と透明性を維持し、言明した約束や目標の遂行状況を、第三者検証によって保証するように努めなければならない。

⑦ 事業者からみたユーザ（個人）のプライバシーの尊重　－　ユーザー主体
　守るべきは個人のプライバシーである。プライバシー尊重の念を忘れてはならない。

この7つの基本原則は、プライバシー・バイ・デザインの根幹をなすものである。とくに、設計段階から、あるいは、アーキテクチャーとしてプライバシー対策を埋め込むことにより、「ゼロサムではなくポジティブサム」を目指すという主張は、プライバシー・バイ・デザインの核心であり、かつ、革命的な主張であり、欧米の各機関やいくつかの先進的な企業で受け入れられた要因であろう。

PIAとの関係について若干、触れる。

PIA（Privacy　Impact　Assessment）は、新システムや新プロセスの導入に際し、事前に設計段階で、プライバシー保護に関する評価を行う手法である。プライバシー・バイ・デザインでは、このPIAをツールとして用いることによって、まさに、設計段階でプライバシーリスクを洗い出すことができ、これに基づいて再設計を行ったり、開発プロセス途上におけるシステムやプロセスの適切な変更を促すことができる。

３．プライバシー・バイ・デザインに関する国際機関、ＥＵ、米国の対応状況

ここはテキスト第1章第3節の事例を基礎としているが、可能な限り原典に当たり、我々なりの検討を加えてみた。

（1）データ保護・プライバシー・コミッショナー会議(*4)(*4-2)

2010年10月の第32回データ保護・プライバシー・コミッショナー会議で、カブキアン博士提案の「プライバシー・バイ・デザインを基本的なプライバシー保護の構成要素であると認識する決議」(*5)が採択された。

（2）EU

法令レベルで個人データ保護を規定し、その第三国条項により世界中に大きなインパクトを与えた、1995年のEU95指令（directive）(*6)を強化する目的で、2012年1月25日にEU一般データ保護規則提案が公表された(*7)。今回は規則(regulation)である。「指令」は、これにもとづく国内法の制定によって実施されるが、「規則」は、EU構成国すべてに直接適用される。したがって「指令」と異なり、国内法制定過程における国ごとの相違が入り込む余地がない。この新提案にプライバシー・バイ・デザインが取り入れられている。

なお、当規則案に関しては、2012年3月にJIPDECから公表された「個人情報の安心安全な管理に向けた社会制度・基盤の研究会報告書」(*8)に、仮日本語訳が掲載されている。

（3）OECD

今日のプライバシー保護の原点になった1980年のOECD勧告(*9)が、2010年に勧告後30年を迎えるに当たり、この30年を振り返る“Thirty Years After the OECD Privacy Guidelines”(*10)という文書がまとめられた。この文書の複数個所でプライバシー・バイ・デザインに言及しており、その画期的なコンセンプトを高く評価している。

（4）米国

2012年3月26日に、連邦取引委員会（FTC：Federal Trade Commission）が、“Protecting Consumer privacy in an Era of Rapid Change”(*11)という報告書を公表した。その第Ⅳ章Privacy Frameworkに「プライバシー・バイ・デザイン」と題する一節を設け(P22-P32)、詳述している。

各地域、国、国際機関がプライバシー保護に関して、プライバシー・バイ・デザインを積極的に取り入れる方向で検討している。とくに注目すべきは、FTCが今回、プライバシー・バイ・デザインを積極的に取り入れ、EUに合わせようとしていることである。かつてEU95指令に対して、個人情報はそれを取得した事業者のものという原則を貫いていた米国が、FTCの報告とはいえ、EUと同等の概念に近づけようとしているのは画期的である。

このままだとプライバシー保護の観点で、日本が国際的に孤立してしまうおそれがある(参考資料(*4-2)参照)。

４．プライバシー・バイ・デザイン第１回報告の結論

コンセプトの革新性と納得性、現代の課題を先取りしていること、さらには、情報プライバシーコミッショナー会議、EU、FTC 等のプライバシー保護の主導権をとる組織がこぞって賛意を表明していることから、プライバシー・バイ・デザインは、今後のプライバシー保護政策の基本理念になると思われる。また、「設計段階からの、あるいは、アーキテクチャーとしてのプライバシー保護」という主張から、当然、IT システムの開発と運用に根本的変革を促すことになろう。開発段階にせよ運用段階にせよシステム監査にあたっては、プライバシー・バイ・デザインの観点での監査が必要になるはずで、システム監査人として、そのコンセプトと内容をきちんと押さえておく必要があると思う。

【情報セキュリティ監査研究会へのお誘い】

当研究会にご興味をもたれましたら、是非、ご参加いただきたいと存じます。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、会報をご覧になってご意見やご質問のある方は、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、参考資料等】

(*1) 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

(*2) “Privacy by Design Curriculum 2.0”、2009 年 9 月、カナダ　オンタリオ州・情報・プライバシー・コミッショナー事務局
http://www.ipc.on.ca/site_documents/1b-Privacy%20by%20Design%20An%20Introduction-Instructor%20Resources.pdf

(*3) **情報・プライバシー・コミッショナー**：情報・プライバシー保護に関する**責任と権限を有する、政府等と独立した「第三者機関」**。共通番号の導入に伴い日本でもいよいよ検討開始。なお、日本以外の多くの先進国では、EU、カナダ、英国、ドイツ、オーストラリア、韓国などがプライバシーコミッショナーに該当する組織、人を用意している。

(*4) **データ保護・プライバシー・コミッショナー会議**：前述の情報・プライバシー・コミッショナーの国際会議(The International Data Protection and Privacy Commissioners Conference)。同会議は、1979 年から毎年一回開催されている。下記 URL は 2013 年 9 月 23 日から 26 日にかけて開催される第 35 回ワルシャワ大会のトップページ。
URL　https://privacyconference2013.org/

(*4-2) 「個人情報保護法は世界に通用するか？」、2012 年、慶應義塾大学　総合政策学部　准教授　新保史生
日本は、国際的に認められる**「独立した第三者機関」が設置されていない**ため、上記会議への**正式参加は不可**、オブザーバー参加のみ。新保准教授は、日本のプライバシー保護対策の遅れに警鐘を鳴らしている。
URL　http://www.horibemasao.org/horibe_07/5.Prof.Sinpo_07.pdf

(*5) 第32回データ保護・プライバシー・コミッショナー会議における、プライバシー・バイ・デザインを基本的なプライバシー保護の構成要素であると認識する決議、2010 年 10 月、イスラエル　エルサレムにおいて
http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/26502/ResolutiononPrivacybyDesign.pdf

(*6) EU95指令 “DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data”
URL　http://www.icm2006.org/imgs/congresos/Directive%2095%2046%20EC.pdf
この 25 条と 26 条が、当指令と同等の法的保護がない国への個人情報の移転を禁止する「第三国条項」である。

(*7) EU一般データ保護規則提案 “Proposal for a
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)”、2012年1月25日、EU　EUROPEAN COMMISSION
URL　http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

(*8) 個人情報の安心安全な管理に向けた社会制度・基盤の研究会報告書、2012 年 3 月、JIPDEC
URL　http://www.jipdec.or.jp/project/anshinkan/doc/2011/01.pdf
(*7)の EU 個人データ保護規則案の仮日本語訳は、この P82～P186 に各項ごとに原文を付して記載されている。

(*9) OECD80 年勧告(HTML) “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”、1980 年 9 月 23 日、OECD ---- PDF 版は OECD ｵﾝﾗｲﾝﾌﾞｯｸｼｮｯﾌﾟ(http://www.oecdbookshop.org/)で入手可(有償)
URL http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

(*10) “Thirty Years After the OECD Privacy Guidelines”、2011 年、OECD
URL　http://www.oecd.org/sti/ieconomy/49710223.pdf

(*11) “Protecting Consumer privacy in an Era of Rapid Change”、2012 年 3 月、米国　FTC
URL　http://ftc.gov/os/2012/03/120326privacyreport.pdf

以上

2013.09

「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 10 章

会員番号：1792　柴田　幸一（個人情報保護監査研究会）

第10章　直接書面以外で取得する場合の措置

直接書面で取得する場合は、その利用目的を本人に書面で通知できますが、直接書面以外で取得する場合は、本人に通知し同意を得ることが困難なため、ホームページ等で利用目的を公表します。

10.1　直接書面以外で取得する場合とは

■「直接取得しない」場合の事例		
a)	受託	データ入力処理、データ出力（宛名、名刺、名簿印刷）、アンケート回収、教育研修、人事管理、顧客管理、福利・厚生サービス、健康診断
b)	提供を受ける	人材派遣、人材紹介
c)	共同利用	グループ企業の人事管理
d)	公表文書を利用	官報、市販名簿、卒業生名簿、町内会名簿、インターネット上の公開情報
■「書面で取得しない」場合の事例		
e)	口頭	店頭販売、クリーニング店
f)	電話	通信販売、デリバリーサービス
g)	電話録音	ヘルプデスク
h)	監視カメラ	来訪者、従業者、無人となったオフィスの監視など
I)	モニタリング	アクセスログ

10.2　受託業務で個人情報を取得する場合

受託業務の事業者は、委託元が適切に取得されたものかどうかを確認する必要があります。その確認方法としては、例えば下記の手段があります。

受託する個人情報が適正に取得されたことの確認方法の事例
・委託元の、契約書、ホームページの通知文書等で、同意を得たことを確認する。
・委託元との委託契約条項で、適正に取得したもののみを取得することを約している。
・委託元が適切な PMS を運用していることを、 P マーク取得事業者かどうかで確認する。
・委託元に、口頭でどんな手段で取得しているのかを聞き、問題ないと判断する。

事業者としては、委託元に確認できないこともあります。無理のない範囲で調査してください。

10.3　第三者提供で個人情報を取得する場合

第三者提供で取得する個人情報についても、適正に取得されているかどうかを確認します。もし、適正に取得されているかどうか不明な場合は、その個人情報を利用する際に、改めて本人に対し利用目的等を通知し、同意を得る必要があります。

10.4　共同利用で個人情報を取得する場合

共同利用とは、2 社以上の事業者が、あらかじめ利用目的などの取扱いを定め、本人に通知し同意を得て取得する措置のことです。本人の同意が確認できない場合は、ホームページに利用目的を公表することで、個人情報を共同利用することができます。

2013.09

「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 11 章

会員番号：1792　柴田　幸一（個人情報保護監査研究会）

第11章　利用に関する措置

11.1　利用目的の公表

直接書面取得であるか、それ以外であるかどうかにかかわらず、個人情報を取得する場合は、その利用目的を通知もしくは公表しなければなりません。また、事業者は個人情報をあらかじめ特定した利用目的の達成に必要な範囲内で利用しなければなりません。・・・　以下は<公表の事例>

(1)顧客情報
【利用目的】取引に係る業務遂行および連絡の範囲で利用します。
(2)調査、コンサルテーション、教育等の受託業務
【利用目的】顧客企業からの受託業務の範囲で利用します。
(3)講演会、講習会（以下、セミナー等という）参加者の個人情報
【利用目的】実施するセミナー等の開催に必要な連絡、出欠確認、料金請求の範囲で利用します。
(4)従業者情報
【利用目的】勤怠管理、福利厚生、報酬支払、及び事業活動における取引先との連絡調整の範囲で利用します。
(5)採用・応募者情報
【利用目的】当社が必要とする人材の採用選考業務の範囲で利用します。
(6)お問い合わせ（開示等請求、苦情・ご相談対応を含む）
【利用目的】問い合わせ対応の範囲で利用します。

※　利用目的を、公表しなければならないのは、受託事業者も例外ではありません。上記のように、受託業務を明記し、利用目的を公表します。

※　クリーニング店や、ピザのデリバリーサービスなど、受取人を特定するために、氏名、住所、電話番号等の個人情報を取得する場合は、利用目的が明らかであるとして、通知または公表を省略することができる場合があります。　　参考：経済産業省ガイドライン 2-2-2.(５)(ⅳ)

11.2　本人にアクセスする場合の措置

個人情報を直接書面による以外の方法によって取得した場合は、「公表」しただけでなく、その後本人に連絡（電話、ＤＭ送付、メール送付など）をする場合は、あらためて、本人に利用目的を通知して、同意を得る必要があります。

「本人にアクセス」の事例		
a)	PMS 導入前	退職した従業者（アルバイト、パート社員を含む）に連絡するなど。
b)	提供を受ける	紹介された人に電話連絡したり、訪問したり、面接に来てもらう場合など。
c)	共同利用	グループ企業の他社の従業者にメールを発信する場合など。
d)	公表文書を利用	市販名簿を使用して営業の電話を掛ける場合など

※　受託業務で本人にアクセスする場合は、本人への通知、同意を必要としません。本人の同意を得る義務は、委託元にあるからです。

「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　第 12 章

会員番号：1792　柴田　幸一（個人情報保護監査研究会）

第 12 章　提供に関する措置

12.1　提供に関する措置

個人情報保護法　第 23 条には、“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。”と定めています。すでに取得している個人情報でも、第三者提供について同意を得ていない場合は、あらためて第三者提供する利用目的を明示して、書面で同意を得なければなりません。

第三者提供にあたるが、見過ごされがちな事例
a) 【社員を他社に常駐させる場合】派遣、常駐、出向などの際に、プロフィールや、スキルシート、入館証発行のための個人情報を受注先に提供する場合。
b) 【ホームページに社員の顔写真やプロフィールを掲載】 ホームページは第三者が閲覧可能なため、第三者提供にあたります。

第三者提供先には、個人情報の管理について一切権限が及ばなくなる可能性があります。
従って、**第三者に提供する場合**は、以下の事項を本人に通知しなければなりません。

a)	会社名
b)	個人情報保護管理者の氏名又は職名、所属及び連絡先
c)	利用目的
d)	個人情報を第三者に提供することが予定される場合の事項
・	第三者に提供する目的
・	提供する個人情報の項目
・	提供の手段又は方法
・	当該情報の提供を受ける者又は提供を受ける者の組織の種類、及び属性
・	個人情報の取扱いに関する契約がある場合はその旨

12.2　共同利用に関する措置

共同利用とは、2 社以上の事業者が、あらかじめ共同して個人情報の利用目的などの取扱いを定め、本人に通知し同意を得て取得する措置のことです。
共同利用する場合は、本人に対し以下の通知事項を明記して本人から同意を得なければなりません。

・	共同して利用すること
・	共同して利用される個人情報の項目
・	共同して利用する者の範囲
・	共同して利用する者の利用目的
・	共同して利用する個人情報の管理について責任を有する者の氏名又は名称
・	取得方法

共同利用するにあたり、1 社を「責任を有する者」として、その事業者が共同利用することについて本人に通知し書面で同意を得ていれば、「従たる事業者」は、ホームページに上記事項を公表することで、個人情報を共同利用することができます。

共同利用は、グループ企業における従業者情報や、顧客情報の取扱いなどで活用の事例があります。しかしＰＭＳについて自社の独立性が保たれないというデメリットもあり注意が必要です。

■

次回は、「第 13 章　適正管理」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

2013.09 投稿

協会からのお知らせ　【　協会行事一覧　】

会員番号 0557 仲 厚吉(事務局長)

2013 年	理事会・事務局・会計・認定	部会・研究会	支部・特別催事
9 月	(会計)予算実績中間報告:12 日 (事務局)会費未納状況まとめ:12 日	(事例研)「課題解決セミナー」:7 日 (月例研)「システム監査の実践的な進め方」:18 日 (CSA フォーラム)「IT-Audit のISO化とIT ガバナンスのJIS化」:24 日(大崎)	(近畿支部)「システム監査体験セミナー(実践編)」:21 日～22 日
10 月		(月例研)「スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン」:22 日	
11 月	(認定)CSA・ASA 更新手続案内 〔申請期間 1/1～1/31〕 (認定)CSA 面接 (事務局)会費未納者除名通知発送:20 日 (会計)2014 年度予算申請提出期限:30 日	(CSA フォーラム)	(北信越支部)西日本支部合同研究会:23 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:28-29 日
12 月	(会計)2014 年度予算案:1日 (理事会)2014 年度予算案・役員改選・会費未納者除名承認:12 日 (認定)CSA 面接結果通知 (会計)2013 年度経費〆切:20 日 (事務局)通常総会・役員改選公示 (事務局)2014 年度会費請求書・寄附願い発送〔1月1日付〕		(東北支部)支部総会・支部設立 10 周年記念講演会:14 日
2014 年	**理事会・事務局・会計・認定**	**部会・研究会**	**支部・特別催事**
1 月	(認定)CSA・ASA 更新申請受付 〔申請期間 1/1～1/31〕 (会計)支部会計報告依頼:14 日必着 (事務局)総会資料〆切:15 日 (会計)2013 年度決算案:中旬 (会計)2013 年度会計監査:下旬	(CSA フォーラム)	(近畿支部)支部総会:17 日
2 月	(認定)CSA・ASA 春期募集:2/1～3/31 (理事会)通常総会議案承認:6 日 (通常総会):21 日	(通常総会特別講演)	
3 月	法務局登記、東京都への事業報告、変更届提出:1 日		

※注　定例行事予定は省略。

2013.09 投稿

協会からのお知らせ【 図書紹介「フェイスブック　情報セキュリティと使用ルール」】

会員番号 0109 木村 裕一（月例研究会）

図書紹介「フェイスブック　情報セキュリティと使用ルール」

著:守屋英一氏

監修：ＮＰＯ日本ネットワークセキュリティ協会　ＳＮＳセキュリティＷＧ

発行：㈱あさ出版　２０１３年７月３１日　110ページ　　定価:本体800円

2012年11月、第177回月例研究会において、「SNSの情報セキュリティを考える」のテーマにてご講演いただいた日本IBMの守屋英一氏の著書「フェイスブック 情報セキュリティと使用ルール」を紹介します。

“SNSにおけるリスクから企業を守るために”として守屋氏が作られたこの図書の一番の特徴は、教育テキストとして用いることを想定して作成され、ケーススタディ形式でSNSのリスクとその対策について解説されている点です。この背景には著者が講演等を通じて認識した次の課題があります。

1. SNSによる企業へのリスクが正しく認識されていない点
2. リスクを回避するための操作方法がまだ理解されていない点
3. SNSガイドラインが形骸化している点

この課題に対して、この図書では対策を検討するべき、あるいは解決するべき具体的な課題項目として次を設定しています。

□プライバシー流出　□情報漏えい　□リスク　□危機管理　□なりすまし
□ブランド毀損　□不正アクセス　□炎上

前記のとおり本書は教育テキストとして用いることを想定して、次のように展開しています。

まず、15問の“フェイスブック理解度チェック”を行い、これを切り口として、読者自身がどのような内容は分かっているか、分かっていないところはどれか、大まかに把握できるようにしている。

そして基本事項として“フェイスブックとは何か”を解説している。

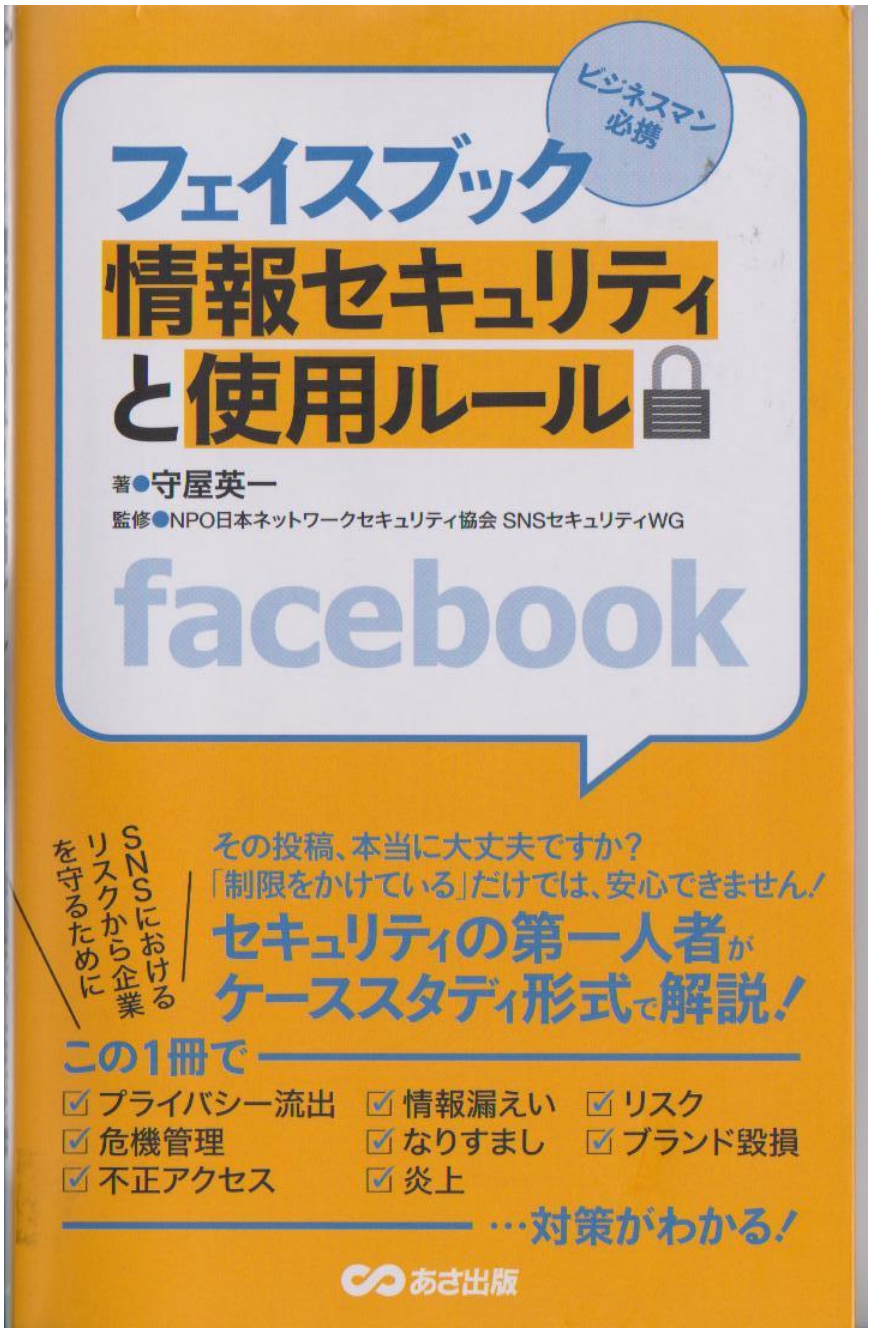
次いで、理解度チェックの回答を取り掛かりにして、次のように分類され1問1答形態で用意されたcase（事例）を中心に、それぞれ用語解説や、対策（操作方法つき）を確認、習得するようにしている。

・人間関係における対策 （3事例）
・ブランド毀損対策 （3事例）
・情報漏えい対策 （6事例）
・セキュリティ対策 （3事例）

例えば、・人間関係における対策では、①SNSにおける上司と部下の適切な関係、②お客様の信頼を失うSNSの行動、③お客様からの「友達リクエスト」、が事例であり、これを確認するという構成になっている。必要に応じて実際の対策の操作画面を示しているため、説明が具体的で誰でもが迷わずに利用できる内容である。

各項目は、著者のSNS利用や講演活動、取材の経験を基にしてまとめられたCaseで、仮想事例ではあるが、よく考えられた内容になっていて、解説も分かりやすい、かつ意味のあるものになっている。

本書の使い方は個人で読み進めるほか、前記のとおりワークショップテキストとして利用することを意識した作りとなっていて、その手順の解説もしているので、ご自身での習得のほか、教育担当の方や、その助言をする立場の方はぜひ一度手にとって見られることを薦めます。



以上

2013.09 投稿

【第183回 月例研究会 報告】

会員番号 1750 舘岡 均(認定委員会)

日時 2013 年 7 月 24 日(水曜日) 18 時 30 分～20 時30 分
場所:機械振興会館 地下 2 階 ホール
講演テーマ:「実演によるサイバー攻撃の仕組み解説」
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
研究員 渡辺 貴仁 氏

＜講演骨子＞

今年 3 月韓国で銀行や放送局を狙ったサイバー攻撃により大規模システム障害が発生し、日本でも今年 4 月から 1,000 件以上ものウェブサイトが改ざんされている。
これらサイバー攻撃の事例を紹介するとともに、どのような問題により被害が生じたのか、特に重大な被害に結び付く新しいタイプの攻撃について、ウイルスによる攻撃を実演し、その仕組みや対策を解説した。

(講師から頂いた講演骨子)

＜講演概要＞

講演の内容は、配布資料「実演によるサイバー攻撃の仕組み解説」に基づき、大項目は次のとおりである。

1. サイバー攻撃の傾向
2. 韓国へのサイバー攻撃
3. 日本で最近多発している攻撃
4. 標的型攻撃(新しいタイプの攻撃)
5. 対策へのアプローチ

さらに、講演のなかでは、直接に見て理解できるように、実際のサイバー攻撃の実演PC環境を用い、PC画面をマルチスクリーンに表示して、実際の攻撃、被害状況が良く解るように解説した。

＜講演内容＞

詳細な内容を講演して頂いたが、本報告では講演内容のポイントを報告するので、詳細は配布資料を参照願いたい。
(本報告では、講演資料の項番を再設定している)

1. サイバー攻撃の傾向

(1)サイバー攻撃の事例

2011 年には、国の政府・省庁に頻繁な攻撃が多かった。2012 年 1 月から 2013 年 7 月において、メディアで報道された攻撃は次のとおり。

2012／1 : JAXA 職員のパソコン感染、無人補給機情報など流出か(毎日新聞等) : 標的型攻撃、
・
2012／9 : 「中国紅客連盟」の標的か・・・総務省統計統計局サイト(読売新聞等): DDoS、不正アクセス
・

2013／7 ： 企業の監視強化迫られる 任天堂不正アクセス、手口巧妙に（日経新聞）： 不正アクセス等々の17事例があり、政府機関、金融機関、多岐にわたる業種の企業において、サイバー攻撃がされている。

(2)サイバー攻撃とは

サイバー攻撃には様々な攻撃があるが、情報窃取・流出、情報破壊、サービス妨害、物理破壊（制御システムを止めるなどによる）、を目的としている。

(3)情報セキュリティの変遷(1)

	2001～2003 年	2004～2008 年	2009～2012 年
時代背景	ネットワークウイルスの全盛	内部脅威・コンプライアンス対応	脅威のグローバル化
IT 環境	コミュニケーション手段	e-コマースの加速	経済・生活基盤に成長
セキュリティの意味合い	サーバやPCの保護	企業・組織の社会的責任	危機管理・国家安全保障
攻撃の意図	いたずら目的	いたずら目的 金銭目的	いたずら目的、金銭目的、 抗議目的、諜報目的
攻撃傾向	ネットワーク上の攻撃	人を騙す攻撃の登場	攻撃対象の拡大
攻撃対象	PC, サーバ	人、情報サービス	スマートデバイス、 重要インフラ
対策の方向	セキュリティ製品中心	マネジメント体制の確立	官民・国際連携の強化 セキュリティ人材育成強化

(4)情報セキュリティの変遷(2)

・不正アクセス事案、
・情報漏洩事件
・日米サイバー対話
・ミサイル技術の窃取　など。

(5)情報セキュリティにおける領域の整理

情報セキュリティにおける領域は次のように整理できる。

	内部統制・コンプライアンス	**サイバーセキュリティ**	**サイバー空間防衛**
分野	企業統治	サイバー犯罪	国家安全保障
脅威	情報漏洩、不正防止 ガバナンス強化	フィッシング詐欺 ウェブサイトへの攻撃　etc	重要インフラへの攻撃 政府機関への攻撃
対応者	システム監査人、経営層	セキュリティベンダー、 システム管理者	日本国政府 重要インフラ事業者
関連制度	ISMS、Pマーク、 個人情報保護法	ウイルス作成罪 不正アクセス禁止法	日米サイバー対話 サイバー防衛隊新設 日本版NSC設立

(6)サイバー空間における攻撃者

様々な目的をもった攻撃者がサイバー空間に潜んでおり、その攻撃者のタイプは、社会を騒がせる、金銭型、諜報活動型（サーバースパイ）、ハクティビスト（自分たちの主義・主張に反する政府や企業を攻撃）がある。

現実世界と異なり、攻撃者は捕まるリスクが小さく、容易に攻撃を行うことが出来るのが特徴である。

（7）金銭を目的とした攻撃

個人をターゲットにした金銭情報の窃取を目的とした攻撃が行われている。サイバー犯罪の実態としては、被害額は世界で 1100 億ドル（約 8.6 兆円）、国内 4 億 4200 万ドル（約 348 億円） であり、被害者数は国内では 920 万人／年、世界では 150 万人／日である。狙われる情報としては、金銭に直結する情報、本人になりすませる情報であり、具体的には、クレジットカード番号、ID／PW、個人情報などである。代表的な攻撃例としては、スパイウェア、スピアメール、フィッシングサイト、等々がある。

（8）対立する組織への抗議・報復　攻撃

現実世界の活動家がサイバー空間でデモを実施している。攻撃者像としては、サイバー攻撃によって自身の主張・抗議を行う人達、掲示板やソーシャルメディアによる攻撃の呼び掛けに呼応した人達である。攻撃事例としては、日本における著作権法改正に伴うアノニマスの攻撃、イスラム諸国から米国への攻撃などある。代表的な攻撃例では、ウェッブサイト改ざん、DDos　等々があり、攻撃の成果を目に見える形にして自分たちの主張を強調する、あるいは現実世界における落書き、デモに似た構図である。

（9）諜報活動を目的とした攻撃

気づかれないように情報を盗む攻撃者がいるが、その目的は、企業や政府機関の機密情報の窃取、知的財産情報や組織の活動情報の収集である。狙われた情報には、国家機密情報、ソースコード、メールアーカイブ、交渉計画、新規油田・ガス田開発に関する詳細な調査結果、ドキュメントストア、契約書、システム設計図面などがある。

業種別の攻撃数は、政府・行政機関：22組織、工業関連：6組織、通信関連：13組織、軍需関連：13組織となっている。代表的な攻撃例は、標的型メールを中心とした複合的な攻撃をし、静かに気づかれないように情報を盗んでいく攻撃である。

2. 韓国へのサイバー攻撃

（1）韓国へのサイバー攻撃のあらまし

2013 年 3 月 20 日（14 時過ぎ）に、韓国の放送局や金融機関へのサイバー攻撃があり、放送局や金融機関の業務が停止する等の大きな被害があった。被害を受けた組織は、放送局 3 社、金融機関 3 社、保険会社 2 社で、社内のネットワークに接続していたパソコンやサーバなど合わせて 4 万 8700 台余りが被害を受けた。その結果、銀行業務（ATM）や窓口の停止、オンラインバンキングが一時的に利用不能になった。また、Windows Vista 以降の PC は、マスターブートレコード破壊により復旧不可能（PC が起動不能）な状態になる被害、接続されている全てのハードディスク全消去になる被害、天気予報サイト（改ざん）を利用してウイルス感染サイト化し、韓国の国民の PC600台が感染する等の被害を受けた。

（2）攻撃の手口と分析

攻撃は、資産管理サーバを乗っ取り、ソフトウェアアップデート機能を利用して、ウイルスを組織内の PC に拡散し、同時に多発被害を誘発させるような手口であった。

攻撃を分析すると次のとおり。

・敵はターゲットの電算システムの運用環境を徹底分析していた。

・資産管理サーバには、アカウント情報を奪取された痕跡があった。

・管理者 PC、ウェブサーバー、資産管理サーバに存在した脆弱性を利用した。

・上記は、ウイルスが仕込まれたウェブサイトの閲覧や、標的型メールの添付ファイル参照によって、ウイルスに感染していった。

さらなる分析の結果、中国・米国・欧州からは間接的なものであり、北朝鮮内部の PC6 台から直接および海外間接により、1590 回接続があり、金融社向けに流布用悪性コード 3 種がアップロードされたことが判明した。2013 年 2 月 22 日には、被害直前までの予行演習がされていた。

(3)対応と問題点

韓国における対応は、国家サイバーセキュリティ危機管理の警報を、5 段階中 3 番目に相当する「注意」に引き上げ、かつ官民軍の合同組織「サイバー危機対策本部」を設置して 2 次攻撃に備えた。民間等での対応は、ワクチンソフト、復旧プログラムの提供等を行うが、完全な復旧は難しいと言われている。

被害機関の問題点はとしては、セキュリティの観点で杜撰なシステムであったことが判明している。具体的には、非セキュアーナサーバ設定、脆弱な認証、パッチ不十分、管理者以外からも可能なサーバ接続、セキュリティの甘いネットワーク構成、等々があげられる。また、管理者 PC は、重要情報に対して不十分な管理、パッチ不十分な状況であった。経営者と管理者の意識の低さが見られた。関連性は不明だが、同時期に韓国に対して、さらに他の攻撃もあった。

3. 日本で最近多発している攻撃

(1)日本でもサイバー攻撃が多発

・2013 年 4 月頃からウェブサイト改ざんが多発している。

ウェブサイトを閲覧しただけで、PC がウイルスに感染する。

・いわゆるガンブラーの手口

①アカウント情報などを窃取するウイルスが確認されている。(FTP／SSH クライアントの ID・パスワード、)

②更なる攻略の手口

・ウェブアプリケーション(ApacheStruts2)が古く脆弱性が内包

・CMSに、容易に推測可能な管理者パスワードを設定

・ウェブサーバのアカウント情報を委託業者と共有していた。

(2)いわゆるガンブラーの手口とは(おさらい)

ガンブラーの手口は次のようにステップを踏んで行われる。

① **「ウェブサイトの管理者(Aさん)」**のパソコンに**ウイルス**が侵入。

② **ウイルス**によりftpのアカウント情報が**「悪意のあるもの」**に送られる。

③ **「悪意のあるもの」**が入手したftpのアカウントを使って侵入し、**「Aさんのウェブサイト」**を改ざん＆ウイルスの配置。

④ **「一般利用者」**が、改ざんされた**「Aさんウェブサイト」**を閲覧。

⑤ **「一般利用者」が「悪意のあるもの」のウェブサイトに誘導され、ウイルス**がダウンロードさせられる。

・ガンブラーの最近の傾向は、ウイルス感染の悪循環を構築して、新たに管理者がウイルス感染する方法が実行されている。

(3)改ざんを防ぐためのサイト管理方法

1)システム側の対策

管理方法としては、アクセス制限、パスワードの強化、ウェブサイトの管理者は更新専用パソコンの導入、

外部のウェブサイト管理者はscpコマンド、FTPSなどを使用、VPNなどによるアクセス制限、等が挙げられる。

2)クライアントパソコンの対策

クライアントパソコンにおける対策は次のとおり。

①ウイルス対策ソフトの導入と適切な運用

ウイルス定義ファイルを最新に保つこと、統合型セキュリティ対策ソフトの使用、有害サイトのブロック機能を使用すること等々がある。

②脆弱性の解消

・OS、その他ソフトを最新に保つようこまめなアップデートが必須である。

・ウェブブラウザのオートコンプリートを無効にする。

4. 標的型攻撃(新しいタイプの攻撃)

新しいタイプの攻撃について、事例、手口、分析を以下に示す。

(1)国内の大手総合重機メーカー(防衛産業)に対する標的型攻撃(2011 年 9 月)

関係組織の職員のPCをウイルスに感染させ、大手総合重機メーカとのやりとり後の 10 時間後に、関連企業に標的

型攻撃メールを送付した。被害状況としては、ウイルスは広域に社内拡散(11事業所、83 台のPCやサーバ、外部通信)、原発・防衛関連情報が攻撃者に窃取された

組織内に巧妙なルートで侵入し、組織内拡散、組織内調査、重要サーバへの不正アクセスによって、組織の重要情報(知的財産、顧客情報等が)を狙う事件が顕在化した例である。

(2)攻撃された後に、外部への攻撃に使われた例。

EMC　Corporation のセキュリティ事業部門である RSA のSecureIDに関する情報が窃取され、攻撃者はそれを使用してさらに外部サーバの情報を窃取した。その後に外部サーバから痕跡が消去された。RSAから盗んだ情報を利用し、ロッキード・マーチンへの攻撃に使用したとの報道もある。

(3)韓国農協に対する攻撃(2011 年 4 月)

韓国農協ネットワークシステムの外部委託業者がウェブサイト経由でマルウェアに感染し、電算ネットワークのデータが大量に破壊され、数日にわたって業務不能状態になった。農協のバックアップされたデータも削除され、一部のデータは復旧不可能な状況となった。

(4)「新しいタイプの攻撃」その手口

段階的な手続き、0段階〔事前調査〕、1 段階〔初期潜入段階〕、2段階〔攻撃基盤構築段階〕、3 段階〔システム調査段階〕、4 段階〔攻撃最終目的の遂行段階〕で攻撃する手口がある。

0 段階〔事前調査〕： 攻撃ターゲットの環境調査、関係機関の情報窃取活動。

1 段階〔初期潜入段階〕： 各種初期攻撃(標的型攻撃メール添付ウイルス、ウェッブ改ざんによるウイルスダウンロードサーバへの誘導、外部メディア(USB 等)介在ウイルスなど

2 段階〔攻撃基盤構築段階〕： バックドアを使った攻撃基盤構築。

3 段階〔システム調査段階〕： 組織のシステムにおける情報取得、情報の存在箇所特定。長期間(数か月～数年単位)発見されないように潜伏して行う。

4 段階〔攻撃最終目的の遂行段階〕： 組織の重要情報(知的財産、個人情報等)の窃取、組織情報(アカウント等)を基に目標を再設定し、何度も攻撃を行う。

(5)「新しいタイプの攻撃」の分析

「新しいタイプの攻撃」の流れを分析してみると、共通的な攻撃手法があることが分った。すなわち、構築した攻撃基盤は発見されなく、再利用され、時間をかけて何度もしつこく行うこと等が分かった。

(6)共通攻撃手法の分析

共通攻撃手法を詳しく見ていくと、バックドア通信機能、システム内拡散機能、一斉バージョンアップ機能、USB利用型情報収集機能の 4 つの機能が存在する。

5. 対策へのアプローチ

(1)セキュリティ対策の特徴と弱点

不正侵入を阻止する方法には、FireWall、IDS、Anti-Virus 等があるが、外から内への侵入に備える境界防御の概念であり、完全に侵入を防ぐのは困難である。また、セキュリティパッチ適用対策があるが、エンドポイント(PC)へのパッチ適用では利用者主導による対策の為に漏れの可能性があるとか、サーバ機器等へのパッチ適用では互換性の問題で適用できないとか、システム停止が許容できない等の問題がある。また、啓発活動による対策があるが、不審メールを開かないという啓蒙活動では 1 人でも感染すると組織に侵入されるとか、ルールによる制限対策では、USBメディアの持ち込み禁止のルールがある、しかし実際の業務に支障をきたす可能性がある。

いずれも、完全な対策は難しい。

(2)新しい発想による対策

従来の対策は、「脅威を入れない」対策であり、侵入されることを前提とした対応であるが、「実害を防ぐ」対策という新しい発想の対策が必要である。具体的には次のとおり。

①入口と出口に二重のセキュリティ対策を行う。

入口対策では外部からの脅威をブロックし、出口対策では情報を外部に持ち出されないようにする。

②共通的な攻撃手法への対策ポイント

外部通信の検知と遮断による攻撃基盤構築を阻止をし、さらにウイルスのシステム内拡散防止による攻撃の最終目的への到達回避をする。

③出口対策の考え方

バックドア通信の検知と抑止として、プロキシサーバーとFWの設定を行う。感染予防策は、アクセス区間の整理(VLAN 構築、VLAN 間の通信を制限、マルウェアの偵察行為を阻止。)、浸食予防(VLAN毎に通信を監視、感染発覚時には VLAN を切り離す)がある。さらに、早期発見のための対策として、ログの監視がある。

(3)8つの出口対策における設計対策

具体的には、次のような8項の設計対策がある。

① サービス通信経路設計、
② ブラウザ通信パターンを模倣とするhttp通信検知機能の設計、
③ RATの内部 proxy 通信(CONNECT 接続)の検知遮断設計、
④ 最重要部のインターネット直接接続の分離設計、
⑤ 重要攻撃目標サーバの防護、
⑥ SW 等での VLAN ネットワーク分離設計、
⑦ 容量負荷監視による感染活動の検出、
⑧ P2P 到達範囲の限定設計

参考として、サービス経路設計、最重要部のインターネット直接接続の分離設計、VLAN ネットワーク分離設計、設計実装図例を示す。(配布資料参照)

(4)対策製品を選定する上で重要なポイント

対策製品を選定する上で重要なポイントは次のとおり。

①出来ることと出来ないことをしっかり見極めること。

全てを防ぐことの万能製品は存在せず、ハコを置いただけで防げる攻撃は単純な攻撃だけである。

②運用をしっかり考えること。

その製品を運用する場合、どの程度工数が必要かを真剣に考えなければならない。

(5)対策の考え方の整理

対策の考え方を整理すると、次のとおり。

①攻撃による組織への損失を見極めること。

何が発生すると組織にとって脅威なのか、特に情報の窃取を考慮する必要がある。

②システム全体を見渡したトータルな対策をすること。

一部分の対策では、対策の漏れや、効率的・効果的な対策が行えなくなる。さらに、入口対策に偏らず、出口対策にも視点を当てたバランスの取れた対策が重要である。

③組織の運用形態に合った対策をすること。

万全のセキュリティ対策設備を備えても、運用が出来なければ効果は無いので、運用が出来ることを念頭に置いた対策検討が必要である。

とにかく、他組織の脅威をそのまま自組織の脅威にあてはめて考えるのではなく、自組織の影響を分析して対策することが重要である。

6. 参考となるIPAがウェブにアップしている情報

次のような情報がウェブにアップされているので、ご参考にされたい。

・『新しいタイプの攻撃』の対策に向けた設計・運用ガイド

http://www.ipa.go.jp/security/vuln/newattack.html

・Windows　XP　サポート終了について

2014 年4月9日にWindows　XPのサポートが終了するので、新たな脆弱性が発見されてもセキュリティ更新プログラムが提供されなくなり、ウイルスや不正アクセスの脅威にさらされたままの状態になり可能性が高まる。

http://www.ipa.go.jp/security/announce/winxp_eos.html

・5分でわかるITパスポート

『ITパスポート試験』はIT化された社会で働くすべての方に必要な基本的能力を証明する国家試験である。

http://www.jitec.ipa.go.jp/ip/

・IPA 独立行政法人 情報処理推進機構　セキュリティセンター(IPA／ISEC)

http://www.ipa.go.jp/security/

＜実演＞

新しいタイプのサイバー攻撃の例として、ウイルスによる攻撃を実演して、その仕組みを解説した。

攻撃とその被害状況が良く解るように、攻撃用PCと被害用PCを用意し、それぞれのPC画面をマルチスクリーンに表示しした実演が行われた。

(1)実演1

メールの文面にて誘導されて、添付ファイルを開く。

これによって、ウイルスに感染し、被害者のPCは完全に攻撃者にコントロールされる。

被害者のPCカメラを通してその表情などが攻撃者に見え、さらにデスクトップ／内部のデータが見える。

・・・感染すると被害者のPCを初期化して復旧対策をするしかない。

感染した理由は、ソフトウェア（MS Word）が最新の状態ではなかった、及びウイルス対策ソフト（定義ファイル）が最新でなかったことによる。

（2）実演2

攻撃者が被害者PCを踏み台にして、ディレクトリーサーバおよび重要書類格納サーバの内容を窃取できる。

＜主な質疑応答＞

Q1：企業において出口対策などをどのようにしたら効果的に実現出来るか？

A1：早期発見のためには、ログの監視をすることが有効であるので、企業においては、日常的に専任者がツールを活用して怪しい動きを監視することはできる。専門的な知識も必要とされるので、ネットワークセキュリティベンダーのサービスを受ける選択もある。いずれにしても、どのように具体的に対策をするかは、自身の脅威を明らかにして、どの程度工数、費用をかけるかを考慮して対策することが大切である。

Q2：IPAはセキュリティについてコンサルタント業務をしているか？

A1：IPAは直接のコンサルタント業務をビジネスとしていないが、様々な事例の紹介、対策の取組みに関してのアドバイス等は出来るので、困った場合はご相談下さい。

＜報告者所感＞

本講演には通常の約２倍近い多くの方々が参集し、「サイバー攻撃」についての関心の高さが伺われた。とくに実際に攻撃用PCと被害用PCを用いて、実際の攻撃状況、被害状況をマルチスクリーンに投影して、臨場感のある実演が行われた。その状況を目の当たりにすると、今後ますます注力して新しい発想による対策を含めたセキュリティ対策を実施すべきであることを肝に銘じた。さらに最新かつ実践的なセキュリティ対策についての講演内容は、セキュリティ活動のレベルアップに大いに役立つものであった。セキュリティ事故は、頻繁に起きており、その攻撃手口は変化し巧妙化しているので、われわれの対策も進化させなければならず、常に高度な専門的知識を習得して対策すべきであることを痛感した。

２台の重いデモ用PCを運び込んでご来場を頂き、さらに盛会なる月例研究会講演にして下さった、講師の渡辺貴仁氏には、改めて深くお礼を申し上げます。有難うございました。

以上

2013.09 投稿

【 近畿支部 創設２５周年記念研究大会 報告 】

会員番号 0645 是松 徹(近畿支部)

【日時】 2013年7月6日(土) 13時～17時

【場所】 大阪大学中之島センター 3階 講義室304

【統一テーマ】「システム監査の新領域への対応」

【参加者数】 94名(発表者を含む)

【概要】

本研究大会は、支部創設25周年を記念して統一テーマを掲げ、支部研究プロジェクト活動成果の報告(4編)、会員から応募のあった研究論文の発表(2編)、およびパネルディスカッションを行った。大会運営は、発表者による説明、コメンテータによる意見表明(研究論文)、およびパネルディスカッションを介した会場からの質問への回答と今後の方向性の議論という形態で実施した。成果報告と研究発表の計6編は、近畿支部の会員3名の方に記録を分担いただいた。

<<開会挨拶:林支部長>>

日本システム監査人協会近畿支部は、1988年(昭和63年)3月4日に「関西支部」として発足しました。従いまして、本年で発足から25年が経過したこととなります。

四半世紀の長きに渡り、支部活動が活発に継続しておりますことは、歴代の支部長、支部役員、支部サポーターの皆様を含めました支部会員の皆様の多大なるご尽力、ご協力の賜物と考えます。改めて厚く御礼を申し上げる次第です。本当にありがとうございました。また、これからも引き続きよろしくお願い致します。

さて、今回、支部創設25周年と言う節目の時を記念して、支部会員の皆様の研究成果の発表を中心とした研究大会を開催することと致しました。情報システム産業は、技術革新によるビジネスモデルの変化や多様化が他の産業に比して早いと考えますが、ここ数年、更にその変化のスピードが速まっていると思われます。例えば、クラウド・コンピューティング／クラウドサービスの進展に伴う変化、事業継続の観点から見た「情報システム」の位置付け等、ますます多様化しており、その結果、システム監査も多様化しています。こうした状況を踏まえ、統一テーマを「システム監査の新領域への対応」と致しました。このテーマに沿って、近畿支部の研究プロジェクトの活動報告や会員の皆様の研究発表と、パネルディスカッションを行います。限られた時間の中で十分な議論ができないことも想定されますが、本研究大会の議論をきっかけに、今後のシステム監査の在り方や、目指すべき方向を皆様と考えて行きたいと存じます。

特定非営利活動法人　日本システム監査人協会

近畿支部長　林　裕正

〈〈支部長 開会挨拶〉〉

〈〈沼野会長からのメッセージ〉〉

日本システム監査人協会近畿支部創設25周年記念研究大会開催に当たり、一言ご挨拶いたします。

〇謝辞:

本日ご参加頂いている皆様

日頃日本システム監査人協会近畿支部をご支援頂き、誠にありがとうございます。

また、本日はこの近畿支部創設25周年記念研究大会にご参加頂き誠にありがとうございます。

本記念研究大会を後援頂く、経済産業省近畿経済産業局様,

特定非営利活動法人ITコーディネータ協会様,後援頂くことを、この場を借りて厚くお礼申し上げます。

そして最後に、近畿支部林支部長をはじめメンバーの皆さん、創設25周年、おめでとうございます。

支部創設25周年に当たり、日頃の近畿支部の充実した活動に、改めて敬意を表したいと思います。

また、本記念研究大会の開催諸準備、いろいろご苦労様です。ありがとうございます。

〇本文:

さて、少し昔の話になりますが、私たちは、農業革命、産業革命を人類史上の大変革として、学校の授業、教科書で学びました。そして、それに匹敵する出来事として、今、情報革命が進んでいると言われます。

しかし、その真只中にいると、日々の少しずつの変化の中に埋もれて、農業革命や産業革命に匹敵する変革の時代に生きている醍醐味を実感できる人はそう多くないのではと思います。きっと今から40～50 年先の子供たちが、我々が学んだ、農業革命、産業革命と同様に、20 世紀から21 世紀にかけての情報革命の全体、そしてその時代の人々の行動を授業や教科書で体系に学ぶのだと思います。

変革の時代は、変革を牽引するコア技術をその時代の人々の知恵で如何に使いこなすか、コントロールするかの試行錯誤、成功・失敗の繰返しの時代です。

例えば、情報社会と言われる今日は、ITの急速、飛躍的発展、進化と共に、それと表裏一体のリスクを如何にコントロールするかの試行錯誤の時代、すなわち情報システムの“不完全性”、具体的に言えば、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を受入れつつも、知恵を絞って情報システムを如何に利活用するかが問われている時代と言えます。

情報システムの“不完全性”は、情報システムの開発・提供者とその利用者が、情報革命の恩恵を享受する上で、共に受け入れなければならない現実です。情報システムの“不完全性”を正面から受け入れ、かつ、利用者が積極的に情報システムを利活用していくには、情報システムの開発・提供者と利用者の相互信頼関係を確立することが重要です。そして、この相互信頼関係の確立には、情報システムの開発・提供者の説明責任遂行、即ち、やるべきことはやっ

ていることを自らキチッと説明することが不可欠であり、これに呼応して、こ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するシステム監査が求められることになります。

今から40～50 年先の子供たちが、20 世紀から21 世紀にかけての情報革命の全体、そしてその時代の人々の行動を授業や教科書で体系に学ぶ時、当時の人々の知恵、行動の一つとして、システム監査の導入、活用が語られるかどうかは、今後のシステム監査の普及、また当協会を始めシステム監査に関わる関係団体、そしてシステム監査人の今の活動にかかっているのかもしれません。

本日の近畿支部記念研究大会は、「システム監査の新領域への対応」を統一テーマとし、近畿支部の研究プロジェクトの活動報告や会員の日頃の研究の発表、そして最後に経験豊富なシステム監査人によるパネルディスカッションも予定されています。まさに、日頃の近畿支部の活動・研究成果を参加者で共有し、これからのシステム監査の更なる普及の大きな契機になればと期待しています。

本日の報告、発表、そしてパネルディスカッションが、ご参加の皆様がシステム監査に取組むに当たって有意義な大会となることを心から祈念し、簡単ですがご挨拶と致します。ありがとうございました。

特定非営利活動法人　日本システム監査人協会
会長　沼野伸生

＜報告者　竹下　健一(No..2083)＞

1. コンプライアンスのシステム監査について(第Ⅲ期報告・最終)

発表者:雑賀　努　氏(株式会社ニイタカ　監査室)

【発表の概要】

情報通信技術の進歩により、情報システム(ICTシステム)と密接に関連する法的問題を、コンプライアンス視点で点検・評価することが重要な課題となっている。本研究プロジェクトでは、一般企業(製造業)を対象とした情報システムを対象に、コンプライアンスのシステム監査基準の策定を目標として研究を行った。システム監査学会との共同プロジェクトであり、今回は最終報告で、実際に使用できるものへのブラッシュアップを目指した。

①研究の活動実績

第一期(前期):2010年1月～2010年8月(8回開催)

コンプライアンス確保のため関連法規を一覧化し、それらの法規に関連する情報システム(ICT)のマップを作成。

第一期(後期):2010年9月～2011年2月(5回開催)

研究活動の参考のため、有識者による情報提供を受け、研究会メンバーと討議を実施。その結果を受け、前期の

成果物の見直しを行った。

第二期：2011年6月～2012年5月（9回開催）

情報システムのコンプライアンス確保のため関連法規を一覧化。それらの法規に関連する情報システムMAPを作成。このMAPをベースにシステム開発を例にシステム管理基準にコンプライアンスに関する脚注を追加。モデル取引、契約の工程をベースにシステム管理基準の内容についてコンプライアンスの観点から課題を抽出。今後はシステム管理基準に対するシステム監査実践マニュアルでの追記の見直しが必要と認識。

第三期：2012年6月～2013年3月（10回開催）

システム管理基準の内、企画、開発、運用、保守業務について検討した。システム管理基準に加える脚注に関して、一層の充実を図り、マニュアル的な活用を目指した。コンプライアンス視点からの具体的な監査ポイントについて議論し、一部を脚注に織り込んだ。課題として挙げられた体系上の位置付けや表現等の整合性について、脚注で可能な限り説明を加えた。

②成果物（システム管理基準へのコンプライアンス脚注）

1.コンプライアンスに関する脚注の作成方針

（基本項目）

・権利関係を明確にするために契約上で必要な項目

・法務部門（外部の法律専門家）の参画と連携

・外部委託を前提に委託業務の内容を明確にするための項目

・コンプライアンスリスクに関する検討項目を追加

（追加項目）

・コンプライアンス視点からの具体的な監査ポイントを追加

・体系上の位置付けや表現等の整合性に関する説明を追加

2.検討に際して発見されたシステム管理基準上の問題点

・モデル契約とシステム管理基準の細目との用語の定義ずれ（例：要件定義と要求定義）

→　本研究プロジェクトはモデル契約にあわせた

・大規模のウォータフォールモデルの開発を対象としているため、現在の開発方法（オープン系、クラウド、パッケージ、アジャイル、中小規模等）とのかい離

→　本研究プロジェクトはウォータフォールモデルを対象とした。

・システム管理基準の細目の記載順序の不整合

→　本研究プロジェクトは現状の記載順序にあわせた。

・システム管理基準へコンプライアンス脚注を付記。斜体文字がコンプライアンス脚注。

システム管理基準と監査のポイント	確認すべき資料、確認方法
1）開発の責任者は、システム分析及び要求定義の手順を明確にしていること。	開発業務標準
契約上の留意点：要求定義の手順も要件定義作成支援業務に含める場合は明確に規定する。	
契約上の留意点：モデル契約では準委任契約で行うこと。	

【所感】

システムの開発現場においては認識が甘くなりがちな「情報システムと密接に関連する法的問題」を具体的な事例を交えて説明を受けたことで、コンプライアンスの意義を改めて認識することができた。今期の成果物である「システム管理基準へコンプライアンス脚注」は、ブラッシュアップによってより分かりやすいものへ仕上がり、システム監査の現場において有効に活用していきたいと感じた。

＜報告者　竹下　健一(No..2083)＞

2. クラウドコンピューティングのシステム監査(最終報告)

発表者:深瀬　仁　氏(パナソニック溶接システム株式会社)

【研究の概要】

クラウドコンピューティング(以下、クラウドと記載)により、これまでの外部委託形態以上に課題が潜在化し、雲のように実態をつかめない世界になってきている。本研究プロジェクトでは、クラウドの研究とともに、情報システム活用の問題、情報データの管理や所有の問題、委託契約問題など、システム監査においてどのような視点やアプローチがあるのか研究を進める。当研究プロジェクトはシステム監査学会との共同プロジェクトであり、今回は最終報告を行う。

【活動実績】

第一期:2010年5月～2011年5月(全7回開催)

クラウドの概念を理解することから始め、研究会にて目指す成果物を選定した。

第二期:2011年6月～2012年5月(全9回開催)

クラウドを対象にしたシステム管理基準の適用を議論しまとめを進めた。

第三期:2012年6月～2013年5月(全6回開催)

システム管理基準のクラウドへの適用が難しいことがわかるようになりながら、クラウドに特化した留意点の考察を進め、今回の最終報告に至った。

【システム管理基準の適用へのアプローチ】

・クラウドを活用したシステムの管理水準を一定に保証する何かしらのマネジメント基準が必要との共通認識からスタートし、経済的観点だけでなく、クラウド選択の適正性、クラウド管理の整合性を見極めることが重要であるという視点でアプローチした。

・　システム管理基準を適用するにあたって、オリジナルの管理基準との比較を行えるテンプレートを作成し整理。システム監査ポイントは、クラウド選択の適切性、クラウド管理の整合性にポイントをおいた。

<table>
<tr><th></th><th>システム管理基準と監査のポイント</th><th>確認すべき資料、確認方法</th><th>クラウド区分</th><th>置換・追加区分</th><th>サービス提供会社へのコントロール内容</th></tr>
<tr><td>現</td><td></td><td></td><td colspan="3" rowspan="2">クラウドにおける特性として項目を付加</td></tr>
<tr><td>クラウド</td><td colspan="2">クラウドにおける管理ポイントを記述</td></tr>
</table>

・システム管理基準の適用では、情報戦略・企画、開発、運用、保守、共通の5つのチーム毎に「論点」と「まとめ」を整理した。

【考察】

・議論になったポイント、今後の課題

クラウド導入の場合、情報戦略・企画フェーズでのリスクの先読みが重要。短期間で経営・IT両視点で自社のリスクを把握しクラウド導入・継続を判断できるスキルが求められてくる。また、「所有」から「使用」への考えの移行に伴い、自社の情報システム現場での運用業務が減少してくる。自社の情報システム要員がよりユーザ支援を行う業務への配置が高まり、人員計画、教育への反映が必要。

・システム管理基準にて適用できなかった点

利用者が所有しない仕組みのシステム管理基準への適用は難しい。

・システム管理基準適用での総括

クラウド利用者、クラウド事業者、開発ベンダーそれぞれの間で発生するギャップを埋めるために必要なことをルール化することが重要。

・研究会開始当初と比べ、クラウドに求められる内容が大きく変化している。クラウドが今後、より重要なシステムに活用された場合、データの流出、重大事故発生リスクをあらかじめ想定しておくことが大事。クラウドに特化した選定基準、クラウドサービス決定プロセスの策定が必要である。

【所感】

クラウドに対するシステム監査について、これまでの研究成果を交えた詳しい説明を受け、「クラウド選択の適切性」と「クラウド管理の整合性」にポイントをおいた視点やアプローチが重要であることを理解することできた。またクラウドに対してはシステム管理基準の適用が容易でないこと、クラウドの役割が大きく変わり続ける中で今後注視すべきことについての話しをお伺いすることができ、知識を整理、補足するのに大変有意義な機会となった。

＜報告者　植垣　雅則(No.1380)＞

3. BCPと親和性の高い情報処理システムを目指して

発表者:永田　淳次　氏

【発表の概要】

(1)はじめに

近年、BCP/BCMの重要性の認識が高まる中、システム監査の対象としてBCP/BCMを取り上げる機会も増加している。BCP研究会では、具体的で実効性のあるシステム監査を実現すべく、複数の観点で議論を進めてきた。今回の報告では、三番目の観点「BCP策定を容易にする情報システム」での議論を通じて整理された内容を紹介する。

(2)BCP/BCM

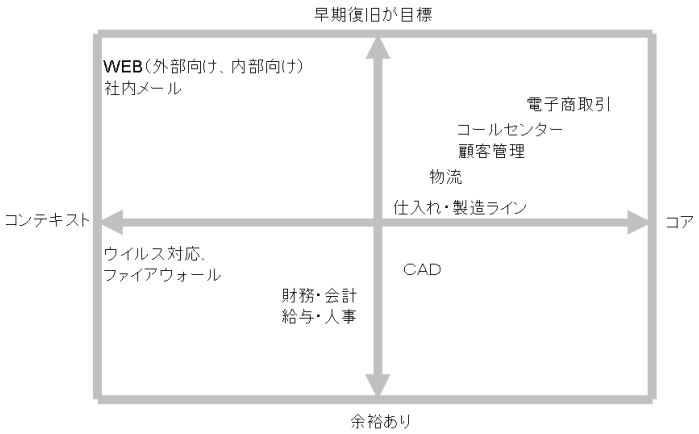
内閣府の事業継続ガイドラインによると、事業継続計画(BCP)は危機管理や緊急時対応の要素を含む重要なものである。BCPを実践することで、最低限の操業度を確保し、重要業務の操業度を早期に復旧させ、ビジネスへの影響度を小さくしようというものである。BCP/BCMの重要性の認識は高まりつつあるが、大規模大震災の後であってもその策定が十分進んでいるとは言えない。

これらの要因となっているのは、BCP策定方法が分からないだけでなく、人手、時間、コストが不足している等のケースが多いためとみられる。BCP策定には困難さを伴っているため、BCPが簡単で低コストに策定できることが望まれている。

(3)情報システム

企業が遂行する業務にはコア業務とコンテキスト業務がある。情報システムも同様に、コア業務用の基幹系システムとコンテキスト業務用の情報システムの二種類がある。BCP策定では、コア業務の情報システムのみが対象となりがちである。しかし、インシデント発生時はコンテキスト業務の情報システムも復旧優先度が高い。復旧の優先度の一例を図に示す。

コンテキスト業務の情報システムは正確な情報収集には必須であるが、対象がコアでないため、軽んじられる傾向にある。図の左上に位置される情報システムが課題を内在しており、十分な投資がされていない場合、柔軟性がなく、融通が利かない情報システムとなり、これを前提にBCPの策定を行うと、膨大な計画書が必要となり、作成や維持に大きな労力が必要となる。



(4)BCPと情報システム

BCP策定においても、発展するインターネット技術(クラウドサービス)を活用することが出来るようになってきている。クラウドサービスを利用した情報システムでは、平常時とインシデント発生時でも、その操作に大きな違いはない。こ

れはBCP策定の簡単化につながり、クラウドサービスや共通のネットワークを利用することで操作の複雑性を減少させている。クラウドサービスには他にも多くの特長があり、BCPの策定や維持、改良において、多くのメリットが考えられる。

(5)事例

BCP/BCMの浸透度は斑であるが、一部では着実に整備が始まっている。例えばマイクロソフト社は「そして誰もいなくなった」という刺激的なタイトルで震災時のテレワークの実践を紹介し、チャットの有効性と普段使いツールの効果について報告している。幾つかの企業の事例から、コミュニケーションを支援する道具がインシデント発生後の復旧・復興時には核となることが、改めて認識できる。

(6)まとめ

BCP策定の重要性は高まっているが、その策定が十分進んでいるとは言えない。その原因の一つに人手、時間、コストがあるため、BCP策定を容易にする情報システムの必要性があると考えた。インシデント発生時はコミュニケーションを司るITがより重要になるが、ノンコア業務であるため、十分な投資は望めない。そこでクラウド等の外部サービスを利用することで、BCP策定に適するITシステムを低コストで構築することができることを示した。

今後、BCP/BCMの存在そのものが、競争力のある戦略となりうる。研究会の活動を通じて、具体的提案となるよう精錬化していきたいと考えている。

【所感】

東日本大震災を受けて企業・組織の規模を問わず BCP の整備は重要な課題と認識されているが、その進展は思わしくないのが実情である。本報告は、コンテキスト業務の情報システムとクラウドサービスを結び付けて実例を示し、簡易かつ低コストでの構築のヒントとして有用であると感じた。

＜報告者　金子　力造(No.1531)＞

4. 新しい「IT 事業者評価制度」導入の政策提言

発表者:中田　和男　氏

SAAJK システム監査法制化プロジェクト:中田和男氏、田淵隆明氏、神尾博氏、横山雅義氏

【発表の概要】

現在、IT 事業者の経営力・技術力の諸項目を総合的・客観的に評価する制度・基準は存在しない。そこで新たな「IT事業者評価制度」の導入を一つの案として提示し、政策提言とする。

(1)現状の問題点の整理と政策提言のテーマ選定

政策提言のテーマ選定にあたり、現状の問題点を「規制緩和」の負の側面に焦点を当て総括した。

無制限な規制緩和の拡大は、IT の分野においてもネガティブな影響としてソフトウェアの品質悪化や国際競争力の低下に繋がった。今日新たな業界構造変化をとらえ、IT 業界の再生に寄与する政策を提言できないかと考えた。

(2)既存の IT 事業者の評価制度の調査 ～当事者の外部からの目線での検証～

既存の評価制度について考察した結果、SI 登録、SO 認定はすでに廃止されており、ISO、CMMI など国際性はあるが具体性、客観性に弱く、利益相反の疑念を払拭できない。よって新しい IT 事業者評価制度の導入は必須であるとの結論に至った。

(3)IT 産業の定義と分類

IT 産業は多岐にわたり、合理的なカテゴライズが必要である。日本標準産業分類に準拠し、情報サービス業およびインターネット付随サービス業の二つとし、さらに小分類において、システム監査業、情報セキュリティ監査業を別枠として新設し、「IT 産業の分類(案)」を提示した。

(4)新しい「 IT 事業者評価制度」の在り方とは？

新しい「IT 事業者評価制度」の要件として、以下の 5 点を抽出した。

①技術力のみではなく経営力や社会性等の項目も合わせ事業者全体の力量が評価できること

②IT 事業分野全般を網羅し、適切なカテゴライズがされていること

③認定・非認定の二分法でなく、点数化により各事業者を明確に順位付する相対的評価であること

④制度自体が持続性・柔軟性に優れており、継続的な運用が可能なこと

⑤評価手続きの費用の経済性があり、実務上、申請者の負担にならないこと

さらに実績のある建設業法による経営事項審査制度のフレームワークを活用しつつ、IT 業界の特性・実情を踏まえた採点方式を採用し、綜合評点の算出式及び採点シート(案)を提示した。

(5)期待される効果～広く国民に受益のある制度～

本制度の導入により以下の効果が期待できる。

①官公需入札での条件化による、合理的な発注先選定及び成果物品質の向上

②客観的な点数評価及び可視化による(官民問わず)、競争の透明性の確保

③システム監査に際して、関連する開発・運用業者の力量確認の精度向上及び大幅な効率化

④IT 業界の技術者評価への意欲の向上による優良事業者の育成、及び国際競争力の強化

(6)今後の検討課題

本研究の課題として、政策実現するためのロビー活動やシステム監査の効率化のための活用方法、SOHO 事業者の取り扱い、高度情報処理技術者のアサインなど検討すべき点は残っている。

(7)まとめ

「IT 事業者評価制度」の導入により、IT 事業者を総合的・客観的に評価することが可能になり、システムの発注者側だけでなく、優良 IT 事業者の育成及びシステム監査の分野においても多大な効果が期待できると考える。本制度を実現定着させ、広く国民への受益につなげていく必要がある。

【所感】

本研究発表の補足資料として、総合評定通知書の書式サンプル、算出式、採点テーブル、審査項目から評価方法まで、きわめて詳細かつ具体的に提示されていた。システム監査の分野でも、このような定量的な評価基準があることは、監査の効率性や客観性において大いに活用できると思われる。また IT 技術者全体が元気になる、正当に評価される社会を目指すべきであるという提言の理念は素晴らしく、今後の法制化に向けての取り組みに期待したい。

＜報告者　金子　力造(№.1531)＞

5. 対策型監査の効果と重要性

発表者:木村　修二　氏

情報システム監査株式会社:木村　修二氏、深瀬　知寛氏

コメンテータ:松田　貴典　氏

【発表の概要】

(1)はじめに

ある中央省庁の一機関において実施した新しい対策型監査の手法を素材に、今後の地方自治体における監査のありかたを考える。まず、どうすれば監査が事故(情報漏洩)防止に有効な手段となりえるのか？というのが問題意識としてあった。そこで対策型監査を考え、その具体的な適用例として認証システムを考察した。

(2)情報セキュリティ事故と監査

事例から、規程類が完全に遵守されていれば事故は起きないのか？という疑問が生まれた。内部、外部にかかわらず攻撃者(予備軍)が存在し、攻撃を企て、攻撃が可能な環境なら情報セキュリティ事故は起きる。我々がコントロール出来るのは環境だけ。そこで事故が起きない環境を作り出していくには、攻撃が可能な環境かどうか調査し、事故に直結する具体的な脅威を示し、攻撃の容易さを評価し、事故防止に直結する改善策と、脅威を受容した意思決定を明確にする必要がある。

事故の様態を、情報の入手段階と持ち出し段階に分解して単純化すると対策を実施すべき場所が明確になる。同時に対策が不可能な部分も明確になる。正当権限者の不正行為はアクセス制御でコントロール出来ない。また電子媒体だけでなく脳も外部記憶媒体である。人的対策も出口対策として考慮する必要がある。そこで出口対策を意識した監査のあり方として、

①セキュリティシステムから期待されている機能を洗い出し「期待値」を監査基準に含める。

②「期待値」を含め、受容した脅威を明確化、具体化する。

③「期待値」を実現するための手法を提案する。(改善策の提案)

④新たな脅威を把握する手続きを明文規定する。

このような準拠性監査の拡大を「対策型監査」とした。

(3)認証の課題

認証については、個体認証、主体認証、意図認証、利用目的認証と4つに分類できる。なりすまし対策として主体認証を考えると、例えば Windows のアクセス制御は、ID、パスワードをかけても Linux で起動してデータを回収すれば認証は回避できる。規程類を守ってもこの認証回避は防げない。セキュリティのポイントとしては、受容したリスクの一覧、

どこで事故が起きる可能性があるのか、どんな事故が起きる可能性があるのかを一覧表で整理しておくことが重要であると考える。

(4)今後の課題

標的型など新しいタイプの攻撃による出口対策の重視、セキュリティ報告書による関係者への説明、スマホ等の普及による持込規制の無力化など、情報セキュリティは大きな転換点を迎えている。今回認証システムだけを例にしたが、今後さらに範囲を拡大して検討を進めたい。

【コメント】松田　貴典　氏

事故発生の可能性の箇所や認証回避の問題などに着眼し、出口対策の重要性や対策型監査として提言された。実務者として実践的に新しい手法や概念を検証されているところは成果であった。

セキュリティの機能について入口出口の話を主にされていたが、本来は防止制御機能、検知機能、回復機能など3つの機能があり、さらにセキュリティのレイアー構造がある。それと入口出口の関係がわかりにくい。また対策提言は、監査ではなくコンサルではないのか？助言型の監査と書かれているが、むしろ保証型ではないのか？論文としては、そのような言葉の意味や定義についてより検討し、論理展開の関連づけをもう少し整理されれば良い論文になると思う。

【所感】

日々現場でセキュリティ事故やその防止に直面されている方ならではの臨場感のある発表であった。監査が事故防止に有効な手段であるのか？という問いは、情報セキュリティ監査だけの問題ではなく、システム監査についても同様であり、特に保証型であればその効果や実効性について常に問われる部分である。セキュリティやITを取り巻く環境は急速に変化しており、監査のあり方について再考しなければならない時期であると痛感した。

＜報告者　植垣　雅則(№.1380)＞

6. 保証型システム監査を可能にするアプローチ

発表者:松井 秀雄 氏

コメンテータ:中野 節子 氏

【発表の概要】

(1)保証型システム監査とは

・システム監査の分類:「保証」を与えるものと「助言」を与えるものの2つのタイプが存在する。「助言型」は多く実施されてきたが、「保証型」の事例は少ないのが実情である。

・何を「保証」するのか:被監査組織の情報システム自体やそのガバナンスに関する整備状況や運用状況自体に対して絶対的な保証を与えるような監査意見を表明する事は極めて困難であり、システム監査人にとってリスクが大きい。しかし、次のような状況を設定すれば、可能と考えられる。

イ. 監査対象組織のIT統制状況に関する「言明書」が当該組織の代表者から表明されること

ロ. システム監査人は監査対象組織の統制状況がその言明書に記載されているレベルに達しているかを監査し、達成していると判断した時に保証を与える監査意見を表明する

・保証型システム監査の難しさ:「助言型」に比べて「保証型」のシステム監査においては、監査要点の網羅性、可監査性、根拠の明示、説明責任と言った点でより難しさを伴う。

(2)保証型システム監査の必要性とその背景

・システム監査基準に「保証型」が導入された主因として、情報システムが適切に管理されていることについて、ステークホルダー(広義・狭義)への説明責任がより増大したことが挙げられる。

・保証型監査を依頼する側の視点でそのニーズを分類すると、以下の4つが考えられる。システム監査人は依頼者のニーズに対応した保証型システム監査のあり方を考える必要がある。

「経営者のニーズ」「システム委託者のニーズ」「システム受託者のニーズ」「社会のニーズ」

(3)保証型システム監査と助言型システム監査

・助言型監査は主に組織内部の改善目的として、保証型監査は主に組織外部の利害関係者を守るため、もしくは判断の材料として利用することを想定していると思われる。

・保証型システム監査の手順においては、助言型と比べると以下のような点で特徴がある。

「言明書」「監査目的」「可監査性要求レベル」「成熟度レベル」「報告内容」

(4)保証型システム監査の分類定義

・誰が、何の目的で依頼するのかを考えると、保証型システム監査は次の4分類が考えられる。

①経営者主導方式:経営者が自組織の情報システムの管理レベルを把握したい

②委託者主導方式:委託者が委託先の情報システムの管理レベルを把握したい

③受託者主導方式:受託者が委託元に自組織の情報システムの管理レベルを報告したい

④社会主導方式　:広く社会に自組織の情報システムの管理レベルを表明したい

(5)類似するその他の保証型監査

・類似するものとして「保証型情報セキュリティ監査」「委託業務における18号監査(日本公認会計士協会監査基準委員会報告書第18号)」「Trustサービス」がある。

(6)保証型システム監査の実施手順

・保証型システム監査の実施手順について、「実施フロー例」と留意点を図示して説明する。

・システム監査人は、以下のプロセスで監査証拠の分析を行い、合意することによって保証意見を表明することが可能である。

検出事項総覧の作成→検出事項総覧の抽出→検出事項の合意→指摘事項の整理→監査意見形成

(7)まとめ

・これまで実施されたシステム監査では「助言型」が多く、「保証型」は圧倒的に少ない。当論文は、こうすれば保証型システム監査を実施できるのではないかという可能性を示すべく、成果を纏めたものである。今後も改善を図り、保証型システム監査の事例を増やしていきたい。

【コメント】中野　節子　氏

同じシステム監査人の立場としてこのような研究に取り組まれたことに敬意を表する。

保証型システム監査を複数例実施したが、被監査組織が作成する言明書の内容をどうするかで苦労した。公表資料に詳細内容を記載するとセキュリティ上の問題が生じる可能性があることから、概要版と詳細版の2種類の言明書を作成したケースもある。業種業態別の言明書の詳細サンプルを充実させるべく、研究に継続して取り組んでもらいたい。

【所感】

保証型システム監査はシステム監査人であれば誰もが取り組んでみたいテーマであると思われる。助言型との比較を通じて特長や留意点、事例を示した本研究報告は、多くのシステム監査人の役に立つものであると感じた。一人のシステム監査人として、保証型システム監査の事例が増えるように努めようと改めて感じた。

＜報告者　是松　徹(No..645)＞

7. パネルディスカッション　ーシステム監査 2.0 への進化は可能かー

モデレータ:吉田　博一　氏

パネラー:浦上　豊蔵　氏、雜賀　努　氏、田淵　隆明　氏、永田　淳次　氏、深瀬　仁　氏

【概要】

本パネルディスカッションでは、支部の 4 つの研究プロジェクトから各 1 名と客観的な立場の方 1 名の計 5 名をパネラーに迎え、実際の研究活動成果をパネラー相互や参加者と共有しつつ、吉田前支部長をモデレータとして今後の方向性に関する検討を行った。

冒頭に、モデレータから、支部 20 周年記念シンポジウム(2008 年 7 月)以降、2011 年 8 月開催の研究大会までの支部イベントで採り上げたテーマを振り返り、さらに内外の環境変化を踏まえ、Web2.0 等にちなんだ仮称「システム監査 2.0」への進化が可能かとの問題提起がなされた。

これを受け、各パネラーからは、先に発表のあった研究プロジェクト活動成果に関するコメントが概ね次の流れで提示された。

・研究プロジェクト報告①(コンプラ研)／②(クラウド研)対するコメント:浦上氏
・研究プロジェクト報告③(BCP 研)／④(法制化研)に対するコメント: 雑賀氏
・コメントに対する見解: 雑賀氏、田淵氏、深瀬氏、永田氏

その後、 休憩時間中に回収した研究成果発表に対する会場からの質問票について、該当する研究プロジェクト所属のパネラーから回答を行った。(雑賀氏、田淵氏、深瀬氏、永田氏)

最後にパネラー全員から、システム監査の進化を見据え、最も期待する研究プロジェクトや今後の方向性についてのコメントを提示し、終了となった。

≪モデレータ≫

≪全体風景≫

【所感】

今回のパネルディスカッションは、単に一般動向での目新しい事項について議論するのではなく、あくまで実際に活動を行ってきた研究プロジェクトに軸足を置き、その成果と限界を確認しつつ今後の方向性を検討する姿勢であった。J-SOX 本番初年度であった 20 周年記念シンポジウムの時期から 5 年が過ぎ、監査では効率化が求められ、その一方でより対象が多様化してきており、このタイミングで「システム監査の新領域への対応」について検討できたのは時期に適ったものであったと思う。

また、4つの研究プロジェクトのうち2つはプロジェクト終了の位置づけであり、今回のパネルディスカッションを総括として次の新しい研究プロジェクトに成果をつなげていただきたいと考える。

なお、パネラーの数や検討項目の内容等からパネルディスカッションの時間がまだまだ足りないきらいがあったため、「システム監査 2.0 への進化は可能か」は、今後も会員全員で継続して問い続けていきたいテーマであると

感じている。

＜アンケート結果＞

（1）アンケート回収結果

参加者数	94
アンケート回収数	50
アンケート回収率	53.2%

無記名 36	コメントあり	14
	コメントなし	22
記名あり 14	コメントあり	8
	コメントなし	6

（2）評価結果

【全体】	期待通り	ほぼ期待通り	どちらとも言えない	多少期待外れ	期待外れ	未記入
全体の印象	13	23	11	1	0	2

【報告・発表等】	非常に良い	良い	普通	悪い	非常に悪い	未記入
コンプライアンスのシステム監査	9	18	18	3	0	2
クラウドコンピューティングのシステム監査	13	17	19	1	0	0
BCPと親和性の高い情報処理システムを目指して	11	24	13	2	0	0
新しい「IT事業者評価制度」導入の政策提言	9	23	14	4	0	0
対策型監査の効果と重要性	9	21	18	1	1	0
保証型システム監査を可能にするアプローチ	11	25	11	1	0	2
パネルディスカッション	10	21	7	2	1	9
記念誌	15	20	10	0	0	5

【大会運営】	非常に良い	良い	普通	悪い	非常に悪い	未記入
日程・時間の設定	16	22	11	1	0	0
時間配分	14	20	12	3	1	0
募集方法	16	20	13	0	0	1
参加費用	16	21	10	2	1	0

（3）本研究大会を知ったルート

【その他】	メーリングリスト	ホームページ	パンフレット	友人・知人	その他	未記入
情報入手方法	29	13	1	2	3	6

（注）複数回答ありのため、合計がアンケート回収人数である50名よりも大きくなっている。

（4）アンケートの主なコメント

a）全体の印象

・記念誌をベースに説明があったのでわかりやすかった。テーマも興味深いものだった。
・今後も関西でのシステム監査の活性化の為、尽力していただきたい。
・コンプライアンスＭＡＰ、クラウド選定のポイント、ＢＣＰ策定のポイント等、具体的に為になる発表が多かった。
・論文発表会のような色彩が強く、事例等を期待したのでわかりづらい面があった。パネルディスカッションは良かった。
・実業務への適用方法、効果が読みにくい。ex. 会社法、J-SOX 法、内部監査にどこまで有効に使えるのかが読めない。
・発表者の主張を可能な限り聞けるよう発表時間を長くして欲しい。現行の人数で 2 日間の開催を希望します。（可能であれば）

b）個別評価

・いずれも中味の濃い内容だったと思います。これだけ深掘りされた皆様に敬意を表します。
・（コンプラ研）時間が足りなかったように思う。
・（対策型監査）対策型監査の効果と重要性については、体験型（実務型）の主張と、大学の先生による学問的な観点の両方からの意見があり、非常に分かりやすかった。
・（保証型監査）保証型に関する発表については、“その時点の状況”を保証することで被監査団体や社会にどのようなメリットがあるのかについて、もう少し深く考察して欲しい。（たとえば、クラウド事業者で実施するとユーザへの説明責任を果たす上で有効になるか等）
・（パネルディスカッション）システム監査 2.0 の意味や方向性がわからなかった。コメントや質問対応とテーマに沿った議論を分けた方が良かったのではないか。

c）大会運営

・せっかくの開催なので、半日でなく１日とし、１編ごとの発表時間をもう少し長くしても良かったと思う。あるいは、発表に際してポイントを絞る必要があるのでは。
・テーマが多く非常に勉強になったが、講師の方があわただしく説明されており、時間が足りなかったのではないか。
・各報告に対するコメントも報告直後にした方がよかったと思います。（聴取者も印象に残っていますので）

d）その他

・他に比べてやや発表内容に起承転結がないように思うので、その点の改善が進めば、よりわかりやすい発表になるでしょう。
・記念誌のエッセイはまとめていただいた方が読みやすいと感じました。
・動画サイト等への投稿も考えてはどうか。
・ISO 審査員が助言することがあるように、監査人がコンサルを必要に応じて行うことも必要と考えている。

以上

2013.09 投稿

【 2013年度 SAAJ中部・北信越支部 JISTA中部支部 合同セミナー 報告 】

以下のとおり、2013年度 SAAJ中部・北信越支部 JISTA中部支部 合同セミナーを開催しました。

日時:2013 年 7 月 20 日(土) 13:00～7 月 21 日(日)15:00
会場:名古屋市
テーマ:**「システム監査体験セミナー(実践編)」**

[1 日目:7 月 20 日] 13:00-21:00
13:00～13:30 開会セレモニー 開会挨拶、コース紹介 受講生・講師自己紹介 他
13:30～14:00 システム監査実施手順および システム監査基本技法解説
14:00～14:30 ケース及び演習課題説明
14:40～14:50 チーム内自己紹介 役割分担
14:50～16:10 ＜課題1＞ 予備調査の準備
16:10～16:50 ＜課題2＞ 予備調査(インタビュー)
16:50～17:30 ＜課題3＞ 予備調査の纏め
17:30～19:20 ＜課題4＞ 監査個別計画の作成
19:20～20:20 ＜課題5＞ 監査個別計画の発表
19:20～20:20 講師コメント 事務連絡
20:20～20:45 ＜課題6＞ 本調査準備
21:00～22:45 懇親会

[2 日目:7 月 21 日] 9:00-15:00
9:00～9:50 ＜課題6＞ (続き)本調査準備
9:50～10:50 ＜課題7＞ 本調査(インタビュー)
10:50～13:00 ＜課題8＞ 本調査の纏めおよび監査報告書の作成
13:00～14:20 ＜課題9＞ システム監査報告会(発表)
14:20～14:50 報告会の講師コメント座談会(受講生感想や意見交換)
14:50～15:00 閉会挨拶

■セミナーの概要

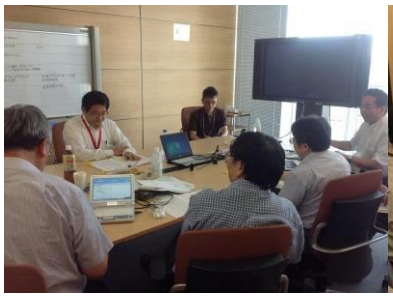
報告者(会員 No. 1711 澤田 裕也)

7 月 20,21 日に「システム監査体験セミナー(実践編)」を SAAJ 中部／北信越支部、JISTA 中部支部の合同で開催しました。このセミナーは監査事例に基づいて設定された仮想企業を対象に監査を体験するものです。

当日は最初に栗山中部支部長の開会挨拶の後、12 名の受講者およびスタッフの自己紹介でセミナーが始まりました。その後、講師である近畿支部の三橋さんより監査の流れや具体的な実施方法の説明を頂き、実際の監査を体験するグループワークに入っていきます。まずは予備調査です。三橋さんと

SAAJ 中部支部スタッフ扮する被監査者にインタビューし、現状を把握していきます。結果をもとに監査個別計画を作成し、各グループの代表が発表します。講師のアドバイスをもとに本調査の準備をキリの良いところまで進めたところで初日のセミナーが終了し、懇親会へつづいていきます。

２日目は本調査の準備の続きから入り、メインイベントである本監査を予備調査と同様に行い、結果を報告書にまとめ被監査者に報告していく流れです。最後に講師、受講者交えて意見交換でセミナーは終了です。2 日間で約 14 時間、監査を一通り体験いただきました。



■セミナーに参加して

◇Aグループ

報告者（会員 No.1281　北信越支部　宮本　茂明）

今回システム監査体験セミナー（実践編）を通し、チームとしてシステム監査を疑似体験でき、課題の本質をどう見極めていくか改めて見直す契機となりました。

1チーム3人で予備調査準備から本調査まで、バックグラウンド（経験、知識領域）が違う3人が、それぞれが意見を出し合うことで、深みのあるシステム監査体験ができました。バックグラウンドが違うメンバーにより監査対象を異なる視点で見ていくことで、視野が広がり大きく捉えることができより効果的な監査ができることを実感しました。

仕事での内部監査業務では、予備調査部分の視点が固定化される傾向にありますが、セミナーでの気づきを活かし、定期的に監査チーム編成を見直し新たなバックグラウンドの違うメンバーで予備調査部分の視点に柔軟性を持たせていきたいと考えています。

今回のセミナー運営にあたっては、近畿支部、中部支部事務局の皆様に大変お世話になり、感謝いたします。ありがとうございました。

以上

◇Bグループ

報告者（会員 No.1732　田中　勝弘）

今回の体験セミナーは、被監査組織の情報セキュリティにスポットを当てて実施するものであった。当グループでは、演習開始に当たり、当日配付されたトップインタビュー(議事録)の内容を元に、システム監査の実施および監査を依頼した顧客(経営者や管理者)に対して、どのような視点で報告をするのが望ましいかという点についてメンバーで議論が行われた。当然、システム監査実施に先立ち監査を依頼した事業者経営陣の監査に対する期待(現状の是非など確認したい事項)について確実に実施することが必要である。しかし、システム監査人として、それ以外にも監査報告を求めるクライアントに対して、今後の改善に役立つ情報や改善活動へアドバイスやポイントなども必要ではないかとの意

見が出された。そこで、予備調査、監査計画、本調査を通して、情報セキュリティ以外にも、本教材で対象となった業務の運用、体制(責任分担)、委託先契約などロールプレイ内のインタビューで気が付いた点などを盛込む監査結果を報告することとした。限られた時間および資料での検討、ヒアリングによる実査であったが、模擬システム監査の一連の体験ができた。また、本体験セミナーでは「システム管理基準」を監査基準としたが、システム監査実施の場面においては、監査を受ける側(披監査事業者)においても、システム監査実施の必要性や有効性を高める上でも、当該する管理基準を事前に理解して頂くことも必要不可欠であると感じた。

以上

◇Cグループ

報告者(会員 No.808　若原　達朗)

私はこれまでに二度、中部で開催されたシステム監査セミナーを、事務局としてお手伝いしたことがあるのですが、実際に受講するのは初めてです。グループ内の白熱した議論や、他グループの方々の参考になる発表、講師コメントと、とても勉強になりました。例え事務局としてでも、見るのと受講するのとでは大違いです。また、個人的にも北信越支部やJISTA中部の方々との議論を通して、リスク対策の世間水準をどう把握するか、という問題を改めて意識することができ、有意義なセミナーだったと実感しています。

さらに驚かされたのは、そのコストパフォーマンスの高さです。有意義なセミナーの間に出てくる食事、場所を変えて行われた懇親会、宿泊と、これらすべてが例年とほぼ変わらない金額の参加費に含まれていました。事務局の皆様の努力に本当に感謝したいと思います。ありがとうございました。そして、今度はぜひ、事務局ではなく、受講者として参加していただければと思います。

以上

◇Dグループ

報告者(会員 No. 2446　甲斐　正彦)

Dグループのメンバー3名は、ユーザ系情報会社、公共機関、SI開発ベンダというバラバラのバックボーンであったが、各自の視点と経験を基に、非常に活発な議論が図れ有意義な教育となった。

今回は監査のRPG形式演習で有り、限られた時間で相手に如何に話をさせ、実態を聞き出すかということの難しさを学んだ気がする。ともすれば作業効率を優先し、確認したい項目を連続してYES／NOの質問形式でヒアリングしてしまったが、真の実態把握と隠れている原因抽出には、インタビュー形式で会話を進めることが重要と感じた。次回の教育では逆にインタビューされる側のRPGも行い、どのように聞かれると話がしやすいか？また会話が弾むのか？というところのスキルアップにも繋げられれば良いと感じている。

また今回立場は違えど、監査対象をあるべき姿／求められるべき姿へ導くように、日々努力されている多くの仲間の生の声が聞けたのが、私としては特に印象に残っており、翌日からのモチベーションアップにも役立てている。

以上

■合同セミナーを振り返って

報告者（会員 No.1711　澤田　裕也）

今回のセミナーに事務局として初めて参加しました。まずは無事にセミナーを終えることができて一安心です。講師の三橋さん、中部支部スタッフ、受講者の協力があってのことです。皆様ありがとうございました。

また、かなり時間の無い状況にもかかわらず、どのグループも的確な監査指摘事項をまとめあげ報告していたこと、懇親会が遅い時間の開始にもかかわらずシステム監査や普段の仕事の話等でとても盛り上がったのが印象に残っています。

今後は合同セミナーや合宿は継続しつつ、中部支部独力で監査セミナーが開催できるようスキルアップしていきたいと考えております。

以上

2013.09 投稿

注目情報　(2013.8～2013.9)

■IPA(独立行政法人情報処理推進機構、理事長:藤江　一正)は、昨今のウェブサイト改ざんの一因となっている、脆弱性が含まれる古いバージョンの CMS(*1)を使い続けているウェブサイトの届出が、6 月からの累計で 42 件寄せられているのを受け、ウェブサイト運営者へ早急な対策を呼びかける為、注意喚起を発することとしました。

https://www.ipa.go.jp/security/topics/alert20130913.html

(*1)Content Management System の略。Web コンテンツを統合・体系的に管理し、配信など必要な処理を行うシステムの総称

■IPA(独立行政法人情報処理推進機構、理事長:藤江　一正)および JPCERT/CC(一般社団法人 JPCERT コーディネーションセンター、代表理事:歌代　和正)は、ウェブサイト改ざん等のインシデントの急激な増加を受け、ウェブサイト運営者及び管理者に対し、改めて点検と備えを呼びかけます。

https://www.ipa.go.jp/security/topics/alert20130906.html

■(平成 24 年度)消費者相談受付対応概要　平成 25 年 8 月 29 日
一般財団法人日本情報経済社会推進協会(JIPDEC)プライバシーマーク推進センター

当協会プライバシーマーク事務局内の「消費者向け相談窓口」および認定個人情報保護団体の相談窓口である「個人情報保護苦情相談室」(以下、両相談窓口を総称し「相談窓口」)が、平成 24 年度に受付けたプライバシーマーク付与事業者等の個人情報の取扱いに係る苦情・相談等(以下「相談」)の概要について取りまとめましたので、ご活用下さい。

http://privacymark.jp/news/2013/0830/index.html

■(平成 24 年度)「個人情報の取扱いにおける事故報告にみる傾向と注意点」について　平成 25 年 7 月 12 日
一般財団法人日本情報経済社会推進協会(JIPDEC)プライバシーマーク推進センター

平成 24 年度中に当協会(JIPDEC)および指定審査機関(平成 24 年度末現在 18 機関)に報告があったプライバシーマーク付与事業者(以下、付与事業者)の個人情報の取扱いにおける事故についての概要を報告する。

http://privacymark.jp/news/2013/0712/index.html

2013.09 投稿

【　協会主催イベント・セミナーのご案内　】

■中堅企業向け「６ヶ月で構築するＰＭＳ」セミナー

個人情報保護監査研究会の中堅企業向け「6ヶ月で構築するPMS」セミナーの開催をご案内します。当研究会では、当研究会著作の規程、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。

詳細は、個人情報保護監査研究会主査　斎藤(saajjk7@saaj.jp)までお問い合わせください。

中堅企業向け「6ヶ月で構築するPMS」セミナー

・基本コース:月 1 回(第 3 水曜日)14 時～17 時(3 時間)×6 ヶ月
・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　茅場町オフィス
・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)
　2013 年 5 月号 SAAJ 会報より、「個人情報保護マネジメントシステム実施ハンドブック」簡易版を公開開始！
・セミナーのお申込が多い場合、最大 6 ヶ月お待ちいただくことがあります。
・基本コースの他に、月 2 回の応用コースなどがあります。

■月例研究会

- 第 186 回月例研究会のご案内(速報)[2013/10/22, 於・東京]

テーマ ：「スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン」(*)に関して、
①これらの報告書・ガイドラインの概要
②背景にある危険なアプリの実態紹介　(仮題)
(*)(モバイル・コンテンツ・フォーラム:MCF)が 2012 年 11 月に発表

日時 ： 2013 年 10 月 22 日(火曜)18:30～20:30
場所 ： 機械振興会館　地下2階ホール

講師 ： 株式会社オプト　海外事業本部
　北京欧芙特信息科技有限公司　董事長　　寺田　眞治　氏
(MCF の常務理事。スマートフォンのプライバシー対応 WG のリーダー)

以上

2013.09 投稿

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
4. おわび

□■ 1． 会報テーマについて

2013 年の会報の基調テーマは、「システム監査の普及促進」であり、3 か月ごとに「システム監査の普及促進」に関連するテーマを取り上げ、皆様と幅広く深く意見交換していきたいと考えています。

10 月号までの会報テーマは「システム監査の使いみち」です。協会においても、「システム監査活性化プロジェクト」を中心に、システム監査活性化に向けて取り組んでいるところです。会報記事が、協会の部会、研究会、支部など、皆様の活動の場での議論の契機となれば幸いです。

□■ 2． 会報の記事に直接コメントを投稿できます。

会報の記事は、

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

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

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

など、環境により、様々な利用方法をされていらっしゃるようです。

もっと突っ込んだ、便利な利用法はご存知でしょうか。

気にいった記事があったら、直接、その場所にコメントを記入できます。著者、投稿者と意見交換できます。

コメント記入、投稿は、気になった記事の下部コメント欄に直接入力し、投稿ボランをクリックするだけです。動画でも紹介しますので、参考にしてください。

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

□■ 3．会員の皆様からの投稿を募集しております。

分類は次の通りです。

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

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。研修の詳細は後日案内します。

□■ ４．おわび

本号掲載のペンネーム「健康衛生」のめだか投稿【システム監査活性化の一考察～ジェロントロジーと生きがい就労に向けて～】は、本来は、会報147号（2013 年6月号）に掲載されるべきものでした。この投稿が、正しい投稿用アドレスに募集期間内に投稿されたにもかかわらず、担当の編集部会員の誤りにより見落としておりました。この事実を８月末に発見いたしまして、投稿者のご了解を得て、本号に掲載させていただきました。

まことに申し訳ございませんでした。

なお、今後、このような誤りが発生しないよう、編集部会内でチェックシステム確立等の是正処置をとりましたことをご報告させていただきます。

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：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）
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━