特定非営利活動法人
日本システム監査人協会報

2013年11月号
No 152

No. 152（2013年11月号）＜10月20日発行＞

・寒い日が多くなりました。暖かくしてゆっくりご覧下さい。
・くつろいで読める記事、身を乗り出してしまう記事、連載記事など、たわわに実っています。


2013.10 甲斐駒ヶ岳

2013. 10

【　会報テーマについてお知らせ　】

今月号から3か月間の会報テーマは**「システム監査の未来」**です。

これまでのテーマ

・今年度の年間テーマ「システム監査の普及促進」
2 ～ 4 月号テーマ「システム監査の普及促進」
5 ～ 7 月号　〃　「システム監査活性化への提言」
8 ～10 月号　〃　「システム監査の使いみち」

今年度の会報は、システム監査の普及促進に一段と拍車をかけることを趣旨に、右テーマをつど掲げて記事の収集や編集をしてきました。

今月号から第4四半期を迎えかつ年末年始を挟む時季でもあることから視野の広いテーマを設定しました。**「未来」**には、システム監査普及促進のその先にあるものやシステム監査普及促進が目指す到達点のようなものも含み、更に大所高所から俯瞰して**「未来」**を論ずることももちろん大歓迎です。

会報テーマは、会員や理事の皆様からより多くのご意見・ご提案をいただきたいと考え設けているものです。会報は、皆様がシステム監査に関して日頃お考えになっていることや、システム監査にとどまらずIT社会の健全な発展に関することなどを表明していただきたいと願っています。皆様のお仕事やご経験を通じたご意見が多くの会員の方にとって貴重な糧やヒントになり目安になることが沢山あると思います。会報はご意見とディスカッションの場になりたいと願っています。会報テーマがそのための一助になれば幸いです。

・会報への記事投稿は次の分類があります。
めだか　［匿名（めだかネーム）］
会員投稿　［実名で記名投稿］
会報投稿論文　［論文投稿規程があります］

一方で、実際に記事を投稿される方は少ないのが実情です。例えば「めだか」記事には毎号必ず数件が投稿されていますがこれらは少数の方がいつも寄せて下さるものです（同じ「めだかネーム」が毎号登場）。目まぐるしいこの世の中、皆様大変お忙しいことと存じますが、「めだかネーム」はそんな状況でも気軽に投稿をいただけるように匿名スタイルにしています。もちろん実名記事も大歓迎で毎号何件か投稿いただいているのは嬉しい限りです。この場を借りてお礼申し上げます。
皆様にとって有益な会報とは？　皆様にいつも見ていただく身近な存在になるには？　など、私ども会報委員はさらに努力いたします。皆様からのアイディアなども頂戴できればと願っています。

改めてですが、**「システム監査の未来」**が今月号からの会報テーマです。
描く**「未来」**は千差万別でバラエティーに富んでいると思います。**「未来」**は、生きる希望、創り上げるもの、感じるもの、願うもの、夢、など捉えどころがないなどと思わずに、例えば次のようなタイミングの皆様のお立場・環境・年齢等を一つの物差しに**「システム監査の未来」**を考えてみてはいかがでしょうか。

・ 3 年後 2016 年（見通せるような気もする）	・14 年後 2027 年（リニア中央新幹線）
・ 7 年後 2020 年（東京オリンピック）	・25 年後 2038 年（SAAJ 50 才−半世紀）
・10 年後 2023 年（首相目標：所得 150 万円増）	・37 年後 2050 年（65 才以上が 4 割）

会報へのご意見ご提案の投稿をお待ちしています。投稿はいつでも受け付けています。任意のテーマでも構いません。右アドレスにお願いします。E-mail：saajeditor@saaj.jp

（会報 11 月号編集担当　中山孝明）

2013.10 投稿

めだか　【　個人情報保護やプライバシー保護（システム監査の未来）　】

個人情報保護や、知られたくない権利であるプライバシー保護への筆者の考えは、次のようなものである。

a) 事業者は、個人情報を本人の同意を得た「利用目的」の範囲で利用すること。
b) 事業者は、「公」（おおやけ、パブリック）を構成する存在であって、消費者または事業の利用者の支持がなければ、事業は成立しないこと。
c) 個人情報の本人である「私」も、「公」を構成する存在で、「公」の規定に従うこと。
d) 「技術」によってセキュリティとプライバシーの両方の安全性を成立させることが可能になってきたこと。
e) 例え本人が同意しても事業者の利用が規制される共通番号等の個人情報があること。

「参考1」の中の注釈（p.21）で、「安全性を確保する為にはセキュリティを強化し、ある程度のプライバシーの侵害を許容するという考え方がある。また、セキュリティとプライバシーの両方の安全性を成立させる、ポジティブ・サムの原則（Positive-Sum Paradigm）が提唱されている。」という記載がある。

これを考察すると、“ある程度のプライバシーの侵害を許容する”とは、社会秩序が優先される状況をいい、こうした規制は、社会的に変化し法令等に反映され、例えば米国では、テロ対策として愛国者法による検閲等が社会的に許容されている。一方、「参考2」では、「技術」がセキュリティとプライバシーの両方の安全性を成立させる要素である、といっている。事例として、プライバシーに配慮した監視カメラの画像処理技術を挙げている。

個人情報保護への法令違反とは、本人同意のない目的外利用や、漏えい、滅失、き損等の安全管理上の違反、本人同意のない第三者提供という目的外利用である。システム監査の未来として、個人情報保護マネジメントシステムや、プライバシー・インパクト・アセスメント（PIA）は、新しいシステム監査のテーマになっている。その際、規定と運用に関していえば、監査のポイントは次のように分類できる。システム監査人は、これらの監査のポイントを心得て、システム監査に当る必要がある。

a) 規定が未整備である。
b) 規定が運用されていない。
c) 運用体制が機能していない。
d) 運用しているが不十分である。

（空心菜）

参考1：「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）
参考2：「プライバシー・バイ・デザイン」堀部政男/一般財団法人日本情報経済社会推進協会（JIPDEC）編
Privacy by Design:アン・カブキアン著、JIPDEC訳　（発行　日経BP社）

（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。）

2013.10 投稿

めだか【　組織内システム監査に答がある　（システム監査の未来）　】

会報テーマ「システム監査の未来」を受けて、先ずは近未来（2～3 年後）のシステム監査を考えてみる。2～3 年後の姿の予想・想像ではなく、それまでに何を成すべきかどのようにすべきか、という点から考える。

タイトルの「組織内システム監査に答がある」に着眼しているポイントは次の 5 点だ。

・システム監査の対象は、企業などの組織がその事業目的実現のために使用する情報システムである。
・システム監査で具現化するものは、事業発展に欠かせない組織内部の課題解決である。
・組織内に定常業務として根付きさらに自発的に機能することが、システム監査の本旨である。
・我が国のシステム監査業務[※1]を現場で担っているのは、組織内のシステム監査人[※2]である。
・情報化社会の変貌と日々向き合う組織内のシステム監査人は、システム監査の未来を背負う人材である。

※1:情報システムとそれに付随する事項を点検・評価し改善する業務　※2:左記業務に従事する者

上記 5 点はシステム監査の役割遂行と目的実現の観点から最も重視すべき着眼点であり、この視点に立ってシステム監査の近未来を実現する必要があると考えている。その行動指針は、企業等の組織が取り組むべき義務と当協会（日本システム監査人協会）が果たすべき責務の両者のなかにある。システム監査の普及促進とは、取りも直さず個々別々の組織にシステム監査がしっかりと定着し実践されることであるから、上記 5 点を重視した活動は、まさに当協会が掲げる設立目的の根幹部分とも言えるだろう。

このように考えるとき、当協会の現在の活動に不足している点はあるのだろうか。今まで以上に組織内システム監査に向き合い、組織内システム監査人から頼りにされる存在になり、組織内システム監査の充実に資する具体的な活動とはどのようなものだろうか。

未来志向で考えれば、現状はもとより、組織内のシステム監査人との接触をより盛ん（能動的働きかけ）にし、その声を多数キャッチ（呼びかけと収集）し、現状認識と課題の共有をより緊密にするための施策などから着手することが考えられる。組織内システム監査人へのメリットの提供が活動の基本的な目標エリアになると思う。

さらに踏み込めば、活動リソースのほとんどをその方向に投入しても良いのではないだろうか、と思っている。（現役を卒業している者相互間での研究や研鑽は当然必要だが）現場の第一線で働く者との課題解決テーマを研究や研鑽の場のほとんどにして、且つ現場の第一線で働く者の参加比率を過半とするなどの活動方法まで考える必要がでて来るかも知れない。

未来志向の創意工夫の具体化には、それなりのハードルが有るかも知れないしあるいは無いかも知れない。（システム監査の）未来は行く先の方向や歩程をデザインすることであり、希望的・楽観的にあれこれ考えを巡らしつつイメージすることからいい着想もでてくると思う。

（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。）

2013.10 投稿

めだか【　システム監査の監査として Identity の確立　（システム監査の未来：その①）　】

今月から3ヶ月間、コラムめだかのテーマは「システム監査の未来」となった。

そこで、これまで私がめだかで書いてきたことを振返りながら、「システム監査の未来」を私の希望、期待も込めて展望してみたい。未来の展望は、近未来像、中期展望、そして将来予想の三段階で描いてみよう。

第一回の今回は、近未来像として、**“システム監査の監査として Identity の確立”**としたい。

現在の「システム監査」は、企業・組織の経営管理（内部統制）の一環として実施される場合が多く、「システム監査」は改善提案とそのフォローアップを特徴に、客観的立場とは言え、情報システムに関する指導的（アドバイザー的）役割を担い、また、「システム監査」の依頼者である組織体の長（経営者）も、実質求めているのは情報システムの安全性、信頼性、有効性等について抱える課題へのシステム監査人からのアドバイスや提案が中心と思う。所謂、助言型監査中心であるということである。従って、「システム監査」は、実質的にはシステム監査人の個人的力量に依存したシステムコンサルティングとして機能している部分が大きいと言えるのではないだろうか。

しかし、このようなシステムコンサルティング機能はその過程の副産物としてはあっても、情報化社会の中で果たすべきシステム監査の役割は、**“監査としての本来の機能の発揮”**ではないだろうか。

すなわち、情報社会の進展を踏まえ、これからの「システム監査」の意義を考える時、「システム監査」は「監査」であり、「コンサルティング」と明確に峻別され、情報システムに関する、組織の、利害関係者に対する説明責任を担保するツール、また、利害関係者の、当該組織の情報システムに対する客観的評価情報の入手手段としての、本来の役割を担わなければならないと私は思う（期待する）のである。

これが私の言う**“システム監査の監査として Identity の確立”**ということである。

これまでのコラムめだかでも以下の主旨を述べてきた。

「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（開発者、利用者など）が、ITの急速、かつ飛躍的な発展、進化などによる情報システムの不完全性を正面から認識し、受入れることが必要であり、そのためには、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説明責任を果たすことが不可欠で、その説明責任遂行に信頼性を付与し実効あらしめる役割をシステム監査が担う」と。

つまり、私の期待する「システム監査」の近未来像は以下が実現され、社会に定着している状態である。

①「監査」本来への回帰

「システム監査」と「システムコンサルティグ」を峻別し、「システム監査」は「定められた評価基準に照らし適合／不適合を判断し、その結果に基づき監査目的を踏まえ意見表明を行なう、再現性のある、不偏的な適合性評価」として機能する。

②組織内の統制ツールから、健全な情報化社会を支える社会の公器へ

「システム監査」は、情報システムに関し、組織内の統制ツールに留まらず、組織の、利害関係者に対する説明責任を担保するツールとして、情報社会に必須の重要な機能を果たす。

上記二点を実現し社会に定着させる道程はなかなか険しいが、システム監査に関る者として避けては通れないのではと思う。皆さんのご意見は如何であろうか。

（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。）

2013.10 投稿

投稿　【　システム監査の未来　】

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）

システム監査の未来のあり姿について、過去から現在を見て、それを未来に投影（プロジェクト）して考えてみました。システム監査において過去の画期的な出来事は、平成 16 年 10 月 8 日に、「システム監査基準」と「システム管理基準」が策定されたことだと思います。

「システム監査基準」の「Ⅰ．前文」には、“今日、組織体の情報システムは、経営戦略を実現するための組織体の重要なインフラストラクチャとなっている。さらに、それぞれの情報システムがネットワーク化されることにより、社会の重要なインフラストラクチャとなってきている。・・・。システム監査は、組織体の情報システムにまつわるリスクに対するコントロールが適切に整備・運用されていることを担保するための有効な手段となる。また、システム監査の実施は、組織体の IT ガバナンスの実現に寄与することができ、利害関係者に対する説明責任を果たすことにつながる。” とあります。

当時、システム監査に並んで、情報セキュリティの確保の観点から監査を実施する場合に、情報セキュリティ監査制度に基づく情報セキュリティ監査を行うことが求められました。「システム管理基準」においても情報セキュリティの確保に関連する項目が挙げられており、「システム管理基準」にあるそれぞれの項目について、情報セキュリティ管理基準を活用して監査を実施することが望ましいとなっています。また、時々の関連技術動向、関連法令、及び社会規範などを考慮し、それらを反映した詳細なサブコントロール項目を策定することが望ましいとなっており、実際、「システム管理基準 追補版（財務報告に係る IT 統制ガイダンス）」が、平成 19 年 3 月 30 日に追補になりました。

当協会定款第 3 条（目的）には、“本法人は、システム監査を社会一般に普及せしめると共に、システム監査人の育成、認定、監査技法の維持・向上をはかり、よって、健全な情報化社会の発展に寄与することを目的とする。”とうたっています。定款第 4 条（事業）には、その目的を達成するための事業活動に、社会教育の推進を図る活動、国際協力の活動、それらの活動を行う団体の運営又は活動に関する連絡などの活動を挙げています。現在、当協会は、公認システム監査人等の育成、認定を担っており、国際協力の活動の一環として、ISO30120（IT-Audit）の推進、及び ISO38500（IT ガバナンス）の JIS 化に参加し、また、システム監査関連団体との連携強化を図ろうとしています。

関連技術動向、関連法令、及び社会規範などは、時々変化しています。現在、システム監査、情報セキュリティ監査、財務報告に係る IT 統制監査に加えて、個人情報保護監査などが求められています。「技術」が進歩し、「関連法令」、「社会規範」などが変わっても、それらにかかわる「人」は、未来においてもその強みと弱みは変わらないものと思います。アダム・スミスは国富論の中で、「人」には、交換性向（propensity to exchange）と説得性向（principle to persuade）があると説いています。「システム監査人」が持つべき情報交換のスキルや、説得の力量につながるものと思います。

システム監査の未来は、「システム監査人」の未来であるといえます。

参考：「アダム・スミス 『道徳感情論』と『国富論』の世界」堂目卓夫著　中央公論新社刊（中公新書 1936）

以上

2013.10 投稿

エッセイ【瓜子姫】

会員番号 0707、神尾博(クボタシステム開発株式会社勤務)

小柄な妖怪・天邪鬼(あまのじゃく)が瓜子姫(うりこひめ)に化けて、長者屋敷への輿入れを企むという民話が、日本各地に伝承されている。瓜子姫は可憐で機織りの達人、現代でも美貌で手に職を持つ女性なら引く手数多だろう。天邪鬼は老夫婦が留守なのを見計らい、瓜子姫を言葉巧みに家の外へ連れ出すのに成功するが、その後の展開では彼女を木に縛り付ける、顔の皮を剥いで被る、命を奪うといったバリエーションが存在する。

こうした「なりすまし」は変身願望のみならず、利益目的である場合も少なくない。オリジナルと見た目が微妙に違う偽ウルトラマンの正体は、地球侵略を目論むザラブ星人だった。偽水戸黄門はハナ肇、小松政夫、笹野高史といった名優が演じ、歓待での珍味や美酒に舌鼓を打っていた。一方、我々システム監査人の活動分野であるITの世界でも、他人のIDを使って内部ネットワークに侵入し機密情報を盗み出したり、個人への偽装メールでクレジット情報を騙し取ったりと枚挙に暇がない。

アカウント乗っ取り系のなりすまし対策には、一般に認証システムが有効だ。パスワード認証の場合はフレーズの使い回しの禁止、またICカードやトークンを併用する多要素認証で、リスクは更に減少する。最近ではアクセス端末や場所、時間帯等のふるまいを監視し、警報を出したりアクセス禁止にしたりするリスクベース認証も普及し始めた。偽物の瓜子姫は機織りの音がぎこちなかったという。本物でない事を鳥が鳴き声で知らせたというから、監視も識別もアラートも機能していたようだ。

IT を使った識別においては、バイオメトリックス分野の認証技術が日進月歩である。今秋発売の iPhone 5s は指紋認証機能を搭載したが、早くもドイツのハッキング集団が偽造指紋でのロック解除を宣言している。北欧では店頭のタブレットを使った顔認証支払いシステムの実用化が始まるが、クレジットも使えるので文字通り「顔で付けが利く」わけだ。米国では埋め込み型医療機器(IMD)への不正アクセス対策のため、心拍から生成する乱数をパスワードにした認証も考案されている。また特定の作業をしている場面を想像した際の、脳波信号の形状を使った個人の識別も研究中だ。

さて物語の結末のパターンも多様である。襲われた瓜子姫は殺害される事もあれば、無事に救出され祝言を挙げて終わる場合もある。加害者の天邪鬼はといえば、退治されたり逃げおおせたりだ。説話ならハッピーエンドでなくても「騙されると痛い目に遭う」という教訓の形で役に立つかも知れないが、現実社会での「犯人が捕まらず被害者が泣き寝入り」というのは絶対に避けねばなるまい。IT 犯罪においては警察当局の誤認逮捕などもってのほか、ITセキュリティエンジニアも組織内の不正を確実に摘発できるよう、日々の研鑽を怠らない事が不可欠である。また当然ながらシステム監査人も、なりすまし対策の有効性を判定する力量が求められることを、肝に銘じておくべきであろう。

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
“ 皆様のご参加、ご協力を頂き、協会の活性化活動を強力に推進中です。”

2013. 10

会長コラム　【　次期会長の立候補、推薦受付を開始しました　】

会長 沼野伸生

当協会の本年度も残すところ 2 ヶ月余りとなり、私が会長に就任して 1 年 10 ヶ月が経ちました。
この間の、皆様のご理解、ご協力、ご参加、そしてご支援に心から感謝しています。

さて、私は本年12月末の任期満了をもって会長を退任致します。
これは、これまで長く協会活動に携わり、また会長を経験した者として、会長職は、適任とされる新たな人に次々に引継がれていくことで、協会の活力維持、協会活動の活性化、そしてシステム監査の社会への一層の普及促進という息の長い活動が維持できると考えていることからです。

当協会は、会勢の著しい低下に取敢えず歯止めがかかり、少しずつ変化の兆しも見えてきました。
例えば、会員の減少傾向は取り敢えず止まり、新規会員も徐々に増加し、また、財政基盤についても昨年度末で本部現預金残高が10百万円弱まで回復し、今年度も黒字決算が見込めそうな状況になっています。
しかし、この状況が安定的、恒常的なものとして根付くかはまだまだ予断を許さないので、この変化の兆が途切れないよう、前任会長が次期会長を推薦（実質指名）するこれまでの方式を改め、選任の透明性を高め、新会長の下での一致協力した協会運営によって会勢低迷の脱却をより確実にする必要があると私から理事会に提案し、理事会の審議を経て以下のスケジュールで円滑に次期会長に協会運営を引き継ぐことになりました。

・10月末まで、立候補、及び推薦（但し、被推薦者了解の下）を受付。
・11月理事会で、次期会長候補による来年度の事業方針案、予算編成方針案の説明。次期会長選任。
・12月理事会で、来年度予算、事業方針の確定。（現会長任期満了）
　（1月から新体制での新年度の活動実質スタート）
・2月総会

定款により、会長は理事の互選と定められていますので、立候補者、推薦者、被推薦者は理事に限られます。従って、一般の会員の皆様には直接的に今回の次期会長選任に関わって頂くわけではありませんが、次期会長の選任は協会の今後の運営、活動に大きく関係しますので、是非関心を持って頂ければと思います。

会長職は「システム監査の社会への普及促進」に強い志のある人が、ボランティア精神を発揮し、関係者と協力・協調して目標達成に向けて協会を強く牽引していく役割を担います。
多くの立候補者、被推薦者を得て、所信も披露して頂き、理事による多数決で新会長を選出し、新会長の下で協会が一致団結して、引続きシステム監査の社会への普及促進に一層強力に取組んでいくことを期待したいと思っています。

以上

2013. 10

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）

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

当研究会は、日本国内は元より、海外も視野に入れたシステム監査に関する基準類の研究、基準類をベースにしたシステム監査人が実践で使えるツールの策定などを行っています。

本会報では、現在、当研究会で行っている活動である IT Audit の ISO 化（ISO 30120）および IT ガバナンスの ISO（ISO 38500）の JIS 化の動きについてご報告しています。いずれの活動にも、当研究会メンバーが参加しています。

IT 監査−IT ガバナンスの評価を支援する監査のガイドライン（ISO30120:PTDR）については、目次（仮訳）ができており、今回の会報でご紹介しています。ご一読ください。

2. 情報セキュリティ監査研究会

毎月、当研究会で研究・討議を行っ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、前回に引き続き「プライバシー・バイ・デザイン」について、興味深い情報を提供しています。ぜひ、報告の内容をお読みください。また、研究活動に参加してみたいと思われる方は、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、当研究会でまとめた『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。

先にシステム監査活性化プロジェクトから募集させていただきました、システム監査の活性化につながる施策やアイデアの提案については、合計8つの御提案をいただきました。提案は、活性化プロジェクトの活動の参考にさせていただくと同時に、そのうちのいくつかの施策提案については、実施に移すべく企画・準備を始めています。経過につきましては、随時、会報を通じてご報告していきます。

以上

2013.10

【　システム監査基準研究会　報告　】（連載）

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

現在は、先月報告しました８月の東京会議で検討したISO30120(IT-Audit)PDTRに対するコメントへの対応結果に基づいた原案修正の作業中です。

また9/24(火)のCSAフォーラムにおいて、ISO30120(IT-Audit) の検討状況とISO38500(ITガバナンス)のJIS化について、CSAフォーラム参加者の方に報告しました。その資料の一部を紹介します。

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

以上

2013.10

【情報セキュリティ監査研究会だより その７ ― プライバシー・バイ・デザイン 第2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、8月から新たなテーマ「プライバシー・バイ・デザイン」に取り組んでおります。研究会では、アン・カブキアン著、「プライバシー・バイ・デザイン　プライバシー情報を守るための世界的新潮流」をテキスト(以下、左記の書を「テキスト」と称します)として、他の周辺情報も交えつつ、「プライバシー・バイ・デザイン」の意義、影響、PIAやシステム監査との関係などを議論しております(会報10月号参照)。

前回は、プライバシー・バイ・デザインのご紹介という趣旨で、主にテキスト第1章で展開されるプライバシー・バイ・デザインの定義、意義あるいはその革新性等をご説明いたしました。今回は、第2章で例示されるプライバシー・バイ・デザインの事例について、そのひとつをご紹介したいと思います。事例としては、プライバシー・バイ・デザインの提唱者であるカブキアン博士がテキストの事例紹介(テキスト第2章第4節「プライバシー保護転換技術の例」、P119－132)の筆頭に挙げている“Biometric Encryption（BE）”を取り上げます。これを取り上げた理由は、紹介されている他の技術と比較して最も革新的かつチャレンジブルであり、博士自ら、これに関する論文を書いているからです。また、プライバシーの保護にも最も直接的に関わりますし、当研究会のテーマである情報セキュリティにも最も近いものであるからです。さらには、プライバシー・バイ・デザインの目標である、「プライバシー保護 vs セキュリティ」という対立の図式から、両者をともに達成する「Win－Winモデル」への転換を実現しているからです。

なお、今回は説明の都合上、テキスト、参考資料の名称、URL等については、報告の冒頭に示します。

本報告は、情報セキュリティ監査研究会内部の検討結果であり、日本システム監査人協会の公式の見解ではないことをお断りしておきます。また、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、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ので是非ご参加ください。参加ご希望の方、また、ご意見やご質問は、下記アドレスまでメールでご連絡ください。 security ☆ saaj.jp （発信の際には“ ☆ ”を“@”に変換してください）

【報告テーマ】プライバシー・バイ・デザインの事例ご紹介 --- Biometric Encryption (BE)

《参考資料等について》

テキストではわずか4ページしか記載がなく説明が不十分なので、カブキアン博士のBiometric Encryptionに関する原論文（資料1）を参考にした。また、この論文でも技術的な説明が少なく、十分理解できなかったので、下記に示す資料2も参照した。

＜テキスト＞

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

＜資料１＞

Ann Cavoukian、Alex Stoianov、“ Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy”、2007 年 3 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/images/resources/bio-encryp.pdf

＜資料2＞

独立行政法人情報処理推進機構(IPA)、「2005 年度未踏ソフトウェア創造事業 （未踏ユース)」採択案件
「指紋を鍵とするファイル暗号化システムの開発」、田中英朗（東京工業大学大学院 総合理工学研究科）
http://www.ipa.go.jp/files/000006551.pdf

１．従来の暗号システムの問題点

共通鍵暗号システムにおける共通鍵にせよ公開鍵暗号システム(PKI)における秘密鍵にせよ、暗号システムにおいては、鍵をセキュアに管理しなければならないという問題がある。これらの鍵は通常128ビットあるいはそれ以上の長さであるから人は記憶することができず、どこかに保存しておかなければならない。この保存されている鍵がセキュリティの脆弱性の大きな原因になっている。もう一つの問題は、これらの鍵の管理者が必要だということである。この管理者が故意にせよ過失にせよ暗号鍵を漏らすという人的なリスクが存在する。

２．　Biometric　Encryption（BE）とは何か、その問題点と解決事例

Biometric Encryptionを直訳すると「生体情報による暗号化手法」ということになり、その意味が正確に伝わらなくなるおそれがある。ここでは訳さずに、Biometric Encryption(本文中では略称、「BE」)と記すことにする。

BEとは、一言でいえば、暗号システムにおける「鍵」をBiometricsすなわち生体の個体識別情報で実現するものである。そこにはいくつもの問題が存在する。ひとつは、常に復号化時に再現可能なものでなければいけないという鍵の要件を満足することが難しいことである。生体情報は一般に揺らぎがあるから、同一人の同一情報、たとえば指紋であっても、暗号化のときと復号化のときで情報が異なることがあり、暗号化したデータが復号化できななくなる可能性がある。これを解決するためには、生体情報を冗長にして揺らぎに対する耐性を強くすることが一般的であるが、十分な耐性を得るためには相当な冗長度が必要になる。ある手法では、必要な冗長度を確保するために、暗号鍵の長さが暗号化対象のデータの長さの4000倍にもなってしまう例がある。これでは実用に堪えない。

この問題を解決するために、資料2の指紋を鍵とするファイル暗号化システムでは二種類の工夫をしている。

(1)指紋情報を直接、ファイルの暗号化鍵に用いるのではなく、ファイル暗号化には共通鍵を用い、その共通鍵に対して指紋情報を鍵として暗号化する、すなわち二段階の暗号化を行う。これにより指紋情報で暗号化する暗号化対象のデータの長さが短くなり、また、暗号鍵の長さが最終的な暗号化対象であるファイルの長さに無依存になる。

(2)位置ずれの大きな指紋画像は復号化に失敗することが多いので、指紋の位置ずれを検出して位置ずれの確認をできるようにしたり、暗号化の際に同じ指紋画像を4枚用いた平均画像をあらかじめ取得しておいて、これを用いて暗号化する等、生体情報の揺らぎを直接、少なくする種々の工夫を行っている。

これにより、暗号化・復号化に要する時間も、位置ずれの問題に対する対応も実用上問題ないレベルになった。

３．　Biometric　Encryption（BE）の利点

BEの利点としては、まずはオリジナルのバイオメトリック情報はどこにも保存されず、したがって、漏れることも盗まれることもなく、また管理者も不要になることである。さらに人が鍵を生成する必要もない。すなわち従来の暗号システムにおけるセキュリティ確保の最大の問題であった鍵の管理の問題を、本質的に解決することができる。

次に、バイオメトリック情報とユーザ識別子を結び付ければ、たいへん強固な本人認証システムを実現できる。

また、BEは、ひとつのバイオメトリック情報を複数のアカウントで用いることができる。しかも、そのバイオメトリック情報は本人しか持ちえないから、他人がアカウント相互間でのリンクを行うことは不可能になる。

そしてこれらの利点は、同時に以下のようにプライバシー保護という観点でも利点になる。鍵の管理も管理者も不要になることで、個人情報の漏えい等のリスクが減る。また、アカウント相互間でリンクができないので、他人が、ある人の個人情報をその人の複数のアカウントから得られる情報を用いてトレースすることが不可能になる。さらに、強固な本人認証システムは、成り済ましを抑止し、成り済ましによる個人情報の漏えい等を抑止できる。すなわち、従来はトレードオフの関係にあった「認証とセキュリティ」と「プライバシー保護」の関係を、Win-Win の関係に転換することができる。

おわりに

BEの実装を説明しないとBEの実態が理解できないので、強引に資料2による説明を行ったが、BEの実装は技術的にたいへん難しく、申し訳ないが十分な説明になっていないと思っている。今に至るもBEがなかなか本格化しないのも、この実装上の問題が、情報セキュリティという大問題に対して十分に解決したとはいえないからであろう。しかし、これが実現したら最後の利点で述べたような計り知れない効果をもたらす。敢えて紹介した所以である。

以上

2013.10

（連載）「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 13 章

会員番号：0557 仲 厚吉（個人情報保護監査研究会）

第13章　適正管理

13.1　安全管理規程

個人情報保護法　第 20 条では、“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。”と定めています。そのため、適正管理の具体的な対策について「3430 安全管理規程」に規定します。

13.2　正確性の確保

個人データを正確かつ最新の内容に保つために、以下のことを規定します。

a)	記録を作成する場合は、作成者、作成日、更新日、承認者、承認日付を明確にする。
b)	ファイル名を付けるときのルールを定める。　例：営業課業務フロー20130901.xls
c)	記録に文書番号を附番する場合のルールを定める。　例：EGY-20121225-005
d)	入力するときには、誤入力チェックを行う。
e)	改訂箇所は色分けするなどして明確にする。

13.3　安全管理措置

日常的に守らなければならない「安全」ルールを徹底するために、申請書や管理台帳などの「様式」を整備します。これらの「様式」には、日付、承認欄などを設定し、都度「3430 安全管理規程」を閲覧しなくても、規定した様式を使用することで、ルールが守られるという「安心」に繋がります。

13.3.1　情報機器の安全管理

- システム機器・ID 管理台帳
- 情報機器「持出」許可申請書
- 情報機器「持込」許可申請書
- 携帯端末使用許可申請書

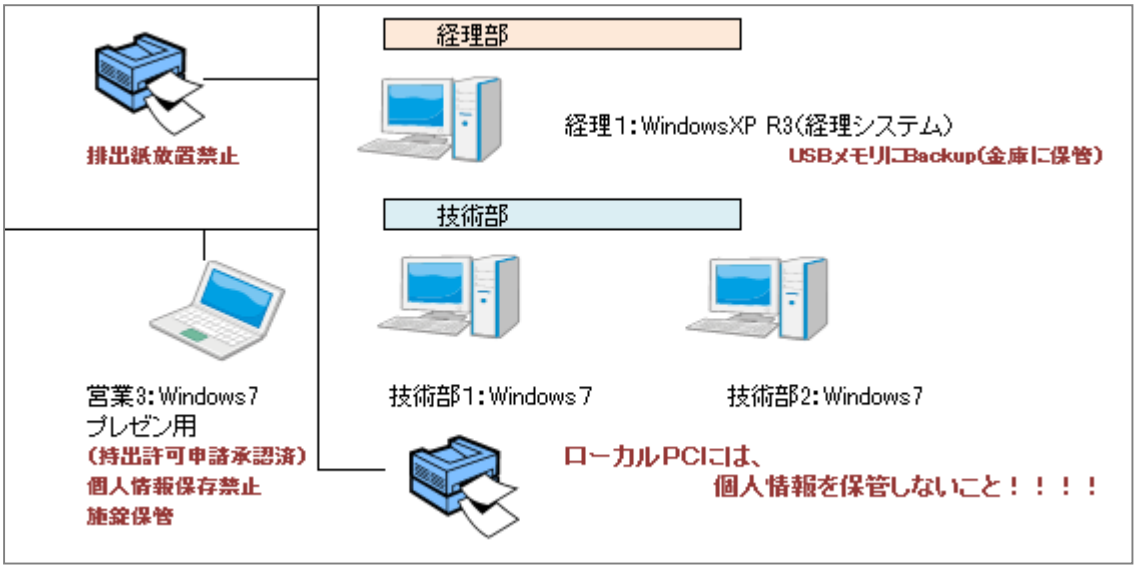
システム部	情報機器「持出」許可申請書	
この申請書は、部門で管理し半年後に廃棄してください。 ① 機器の種類は、わかりやすく記入のこと。 例:ノートPC、USBメモリ、CDR、DVDなど ② 管理者は、期間における機器の管理を行う社員名を記入のこと。		承認部門 安全管理責任者 承認 201 / /
持ち出しの内容		
①機器の種類、台数 (周辺機器、媒体についても記入のこと)		
暗号化の方式 (該当するものすべてに☑) 複数台数持ち出しで、方式が異なる場合は、個別に申請すること。	□1.ログインID　□2.ログインパスワード　□3. □4.指紋認証　□5.USBトークン　□6.リモ □7.個人情報ファイルのパスワードを英数混合で8文字 □8.フォルダのアクセス権限設定　□9.ハードディ	
外部でのインターネット接続	□有効(下記に接続形式を記入↓)　□無効	
接続形式		
②個人情報の有無	□なし　□あり:下記に内容、件数を記入↓	

「携帯端末使用許可申請」の一部

	利用にあたっては下記を有効にすること。(システム部が記入)		
設定する 暗号化の方式 (該当のすべてに☑)	□1.ナンバーロック	□2.リモート(遠隔)ロック	□3.リモート(遠隔)データ消去
	□4.指紋認証	□5.顔認証ロック	□6.ICカードロック

13.3.2　ネットワーク管理

- 3432-011　サーバー利用申請書
- 3432-013　情報ネットワーク構成図　（下記は、ネットワーク図の一部分）
- 3432-311　アクセスログ・Ｗｅｂ点検記録



13.3.3　個人情報の移送、送受信時の管理

- 3319　個人情報取得・返却・廃棄・消去管理表

取得日	本人	① 種類	媒体	保管場所	注意事項	保管期間	返却日	廃棄日
2013/9/10	★村☆夫	電子メール	メール	人事部専用PC		不採用決定後2週間	date	date
2013/10/5	★村☆夫	応募書類一式	紙	人事部キャビネットA(常時施錠)	面接時	不採用決定後2週間		
2013/9/15	☆田★子	電子メール	メール	人事部専用PC		不採用決定後2週間		

13.3.4　執務室の整理整頓、保管場所

- 3432-211　入退館安全確認記録簿
- 3432-221　鍵・ID カード管理簿

13.3.5　入退館、入退所及び入退室管理

- 3432-012　フロアマップ（セキュリティ区画）
- 3432-212　来客入退館カード貸出簿
- 3432-213　サーバー室入退室記録簿

管理部	来客入退館カード貸出簿			
貸出カード番号	貸出日時	対応社員名	対象者区分	出頭者氏名／来
xxx-123421	2011／　／ ：		□出張者／□面会者	
xxx-123422	2011／　／ ：		□出張者／□面会者	
xxx-123423	2011／　／ ：		□出張者／□面会者	

2013.10

（連載）「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 14 章

会員番号：0557 仲 厚吉（個人情報保護監査研究会）

第１４章　従業者の監督

14.1　機密保持誓約書

従業者は、入社時に業務で知り得た個人情報を含む機密情報の守秘義務を課せられ、その証として「343101 機密保持誓約書」に署名します。　　下記は「機密保持誓約書」の事例

機密保持誓約書

私は、入社に際し下記の事項を遵守し履行することを誓約します。

１．貴社の就業規則、諸規程等に従い誠実に勤務すること。
２．私の履歴書、職務経歴書等の入社時提出書類記入事項は真実に相違ないこと。
３．社員として貴社の対面を汚すような行為をしないこと。
４．故意又は重大な過失により損害を会社に与えたときは、その責任を負うこと。
５．下記の機密情報保持義務を遵守すること。

（機密保持の確認）
在籍中は、次に示される情報(以下「機密情報」という) に関する書類等一切について原本はもとよりその複写物、電子データ等については、業務に必要なもの以外利用しません。また業務上利用する場合は、定められた安全管理対策を守り、漏えい、改ざん防止に努めます。

①販売・企画・技術資料・原価・価格決定の情報
②財務・人事・プロジェクト等に関する情報
③関連会社の情報または他社との業務提携に関する情報
④上司により部内機密情報として指定された情報
⑤とくに機密保持対象として指定された情報

なお個人情報を取り扱う場合は、1件でも機密情報として認識して取り扱います。
また開発中の製品やサンプル等についても同様に、業務に必要なもの以外利用しません。

（機密の帰属）
機密情報は貴社に帰属し、私に帰属するものでないことを確認します。

（退職後の機密保持の誓約）
貴社を退社した後においても機密情報を漏洩もしくは利用しません。

（賠償責任）
上記に違反し貴社の機密情報の利用および漏洩した場合、私に法的な責任が生ずることを十分に理解し、それにより貴社が被った損害について相当の賠償を致します。

以　上

※　「343101 機密保持誓約書」は、従業者のみを対象とします。派遣元との守秘義務契約を締結している受入派遣社員に対しては「誓約書」を取得してはなりません。

14.2　罰則規定

「3301 個人情報取扱規程」５.罰則　に、PMS に違反した者等に対しては、「就業規則」に従い懲戒の対象となるとともに、会社に損害を与えた場合は、損害賠償請求を行うことがあることを規定します。

2013.10

（連載）「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 15 章

会員番号：0557 仲 厚吉（個人情報保護監査研究会）

第１５章　委託先の監督

個人情報を委託した場合、個人情報の取り扱いの責任はすべて自社にあります。

15.1　委託先管理台帳

契約の有無にかかわらず、すべての個人情報の委託先を「343401 委託先管理台帳」に特定します。

部門	①種類	委託先会社名（業務内容）	②書類区分	（契約書以外のみ記入）	③当社契約者名	④相手先契約者	委託する個人情報	初回評価結果	契約締結日	再評価予定日
総務	6従業員関連	ヤマト運輸（機密文書リサイクルサービス）	2相手先契約書	宅配便約款	2総務部長	2組織責任者	従業員履歴書、給与台帳他	95点	2012/9/1	2013/9月
広報	1〇〇事業関連	ＡＢＣ広告社	1標準契約書		3部門長	1代表者	社員の氏名、顔写真	100点	2010/6/1	2013/9月

委託先として認識から漏れやすい事例	
Webサーバー	個人情報を取得する画面がある場合。
メールサーバー	個人情報の一時保管がある。
従業者の名刺印刷	名刺の漏えいは、悪用されるリスクがある。
配送	宅配、郵送、バイク便など
情報機器の保守	コピー機や印刷した結果が機器のメモリーに保管される。

15.2　委託先の調査・選定

すべての委託先が、自社と同等の安全管理対策が講じられているかどうかを調査し、「343402 委託先調査票」を作成します。個人情報のリスクに応じて、立ち入り調査が必要なケースもあります。評価結果は、客観的に妥当性を示すレベルが明記されていなければなりません。

委託内容：総会案内状の発送　★600 件
実施期日：201★年★月 15 日　発送予定

	201　/　/	201　/　/

NO	評価項目 A：下記が〇の場合、合格とする。（以降評価不要。）	評価（〇×）
1	委託先は、プライバシーマーク認証を取得している。	×

NO	評価項目 B：　■現地調査　□電話　□アンケート	評価（〇×）
1	委託先は、個人情報保護方針を制定し、公表していること ＜必須＞確認した内容：　ホームページ　http://www.　を確認した。	〇
2	社員は、個人情報の取り扱いについて、責任者から教育を受けていること ＜必須＞確認した内容：　2013 年 5 月の教育記録を確認した。	〇
3	委託した個人情報は施錠された書庫等に保管していること ＜必須＞確認した内容：　現地調査で施錠を確認した。	〇
4	事務所への入退室について記録していること 確認した内容：　2013 年 6 月の入退室記録を確認した。	〇
5	委託した個人情報をパソコン、サーバー等に取り入れている場合、パソコンに個別のユーザＩＤ、パスワード設定をしていること 確認した内容：　システム管理者にヒアリングした。	〇
6	個人のパソコンを会社に持ち込んでいないこと 確認した内容：　現地調査で情況を確認した。	〇

15.3　委託先との契約締結

委託先とは、以下の内容を含めた「3434-03 個人情報委託契約書」によって、契約を締結します。

A	委託者及び受託者の責任の明確化
B	個人情報の安全管理に関する事項
	・漏えい・盗用防止
	・範囲外加工・利用禁止
	・範囲外複写禁止
	・委託契約期間
	・契約終了後の返還・消去・廃棄
C	再委託に関する事項
D	個人情報の取扱い状況に関する委託者への報告の内容及び頻度
E	契約内容が遵守されていることを委託者が確認できる事項
F	契約内容が遵守されなかった場合の措置
G	事件・事故が発生した場合の報告・連絡に関する事項

ただし、委託先との間で契約が締結できるとは限りません。例えばデータセンタや宅配事業者とは、利用条件を示す「約款」の内容に問題がないことを確認することが一般的です。

15.4　委託先の定期的な再評価

委託先における安全管理措置が、維持されているかどうかを定期的に評価する必要があります。委託する個人情報の内容によっては、アンケート形式でもよい場合があります。

- 3434-06 委託先調査票（自己評価・再評価用）

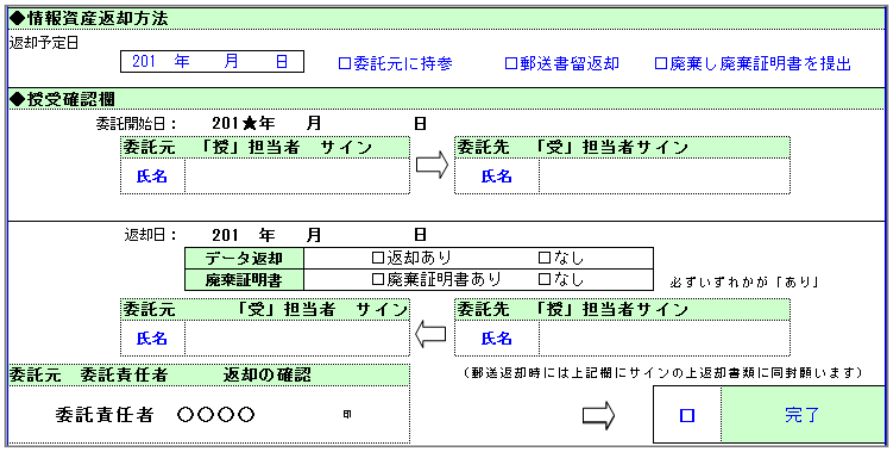
15.5　委託先との個人情報の授受

個人情報の授受が発生する都度、授受記録が不可欠です。

- 3434-04
  委託業務指示書
  （右は一部）

- 3434-05
  委託業務指示管理台帳

委託先に廃棄・消去までを依頼した場合は、「廃棄証明書」の取得を記録します。



15.6　委託先評価基準の見直し

委託先評価基準は、社会状況の変化に応じて陳腐化していないことを定期的に確認する必要があります。

■

次回は、「第 16 章　本人の権利」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. 10

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	認定委員会・部会・研究会	支部・特別催事
9月	12日 会計:予算実績中間報告 12日 事務局:会費未納状況まとめ	7日 事例研:「事例に学ぶ課題解決セミナー」 18日 月例研:「システム監査の実践的な進め方」 24日 CSAフォーラム:「IT-Auditの ISO化とITガバナンスの JIS化」(大崎)	21-22日 近畿支部:「システム監査体験セミナー(実践編)」
10月	10日 会計:9月末予算実績対比表の理事会報告	22日 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を巡る動向」	
11月	14日 理事会:次期会長選任 14日 会計:予算申請提出依頼(11/30〆切) 20日 事務局:会費未納者除名通知発送 30日 会計:2014年度予算申請提出期限	16日 認定委員会:CSA面接 20日 認定委員会:CSA・ASA更新手続案内〔申請期間 1/1～1/31〕 21日 CSAフォーラム:システム監査人のスキルと育成(仮称)	16日 近畿支部:「事例に学ぶシステム監査の基本と応用」 23日 北信越支部:西日本支部合同研究会 28-29日 東北支部:支部設立10周年記念システム監査実践セミナー
12月	1日 会計:2014年度予算案策定 12日 理事会:2014年度予算案、会費未納者除名承認 13日 会計:支部会計報告依頼(1/11〆切り) 13日 事務局:役員改選公示 13日 事務局:通常総会開催通知メール 20日 会計:2013年度経費提出期限 27日 事務局:2014年度会費請求書・寄附願い発送〔1月1日付〕	7日 事例研:「事例に学ぶ課題解決セミナー」 ・認定委員会:CSA面接結果通知	・北海道支部:支部総会(日時未定) 14日 東北支部:支部総会・支部設立10周年記念講演会
2014年	**理事会・事務局・会計**	**認定委員会・部会・研究会**	**支部・特別催事**
1月	10日 通常総会開催案内掲示 11日 会計:支部会計報告期限 15日 事務局:総会資料〆切 20日 会計:2013年度決算案 25日 会計:2013年度会計監査 31日 償却資産税申告	・認定委員会:CSA・ASA更新申請受付〔申請期間 1/1～1/31〕 20日 認定委員会:春期公認システム監査人募集案内〔申請期間 2/1～3/31〕 ・(CSAフォーラム)	・中部・近畿支部会計監査 17日 近畿支部:支部総会
2月	6日 理事会:通常総会議案承認 21日 通常総会 (活動成果発表)　新役員	・認定委員会:CSA・ASA春期募集(2/1～3/31)	
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		

※注　定例行事予定の一部は省略。

2013.10 投稿

【第 184 回 月例研究会 報告】

会員番号 0010 北出 磯秋

【講演テーマ及び講師】

「クラウドサービス利用の実態と点検・監査(検査)のポイント」

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 研究員 河野 省二 氏

【日時と場所】

2013 年 8 月 21 日(水)18:30~20:30 機械振興会館 地下 2 階ホール

【講演概要】

１．本日のテーマ

・「情報セキュリティは、IT を最大に活用するための最小限の安全確保」

情報セキュリティは、PC 持ち出し禁止、USB メモリ利用禁止、クラウド利用禁止ではなく、これらを「利用するためのセキュリティ」を考えることである。IT の利用を前提にして、IT を安全に利用するための最小限のセキュリティを考えることである。

2. クラウドを使ったビジネスの展望(日本のクラウド事情ってどうなっているの？)

(1) クラウドのある生活の将来像

・クラウドコンピューティングでは、大量の情報集積・分析・処理が可能である。ネットワークで接続された大規模な情報処理基盤を誰でも活用できるようになると、ベンチャーの事業創出や既存企業の新事業進出から個人の創造に至るまで、イノベーション参加者のすそ野が飛躍的に拡がることが期待される。

・クラウドコンピューティングにより実現するデータ共有と高度な協働作業は、分野横断的に多様な主体が参加するイノベーションを促す。例えば、クラウドコンピューティングを基盤とした新しいサービスとして、パーソナライズド広告(ワンツーワンマーケテイング)、ヘルスケア・健康アドバイス、遠隔介護、拡張現実、映画配信、モバイル教育・個別指導・学習進捗管理、高度遠隔・在宅医療、医療情報照会、行政サービス(住民税・戸籍・福祉)などが出現するであろう。これらのサービスをユーザがいつでも、どこでも(自宅でも、移動中でも、職場でも、旅先でも)利用できるようになる。

(補足説明)

クラウドコンピューティングとは、「ネットワークを通じて、情報処理サービスを、必要に応じて提供／利用する」形の情報処理の仕組み(アーキテクチャ)をいう。データ処理や保存を行う情報処理基盤の基幹部分が利用者の所有する端末から切り離され、クラウドサービスを提供する事業者において集中管理されることにより、ハードウェアやソフトウェアの仮想化・規格化・共用化が進み、規模の経済が実現する。これにより、①利用者負担の軽減、②IT 資本の性能・効率の向上、③情報環境の多様化・偏在化・リアルタイム化、④大規模データの蓄積・共有という 4 つの側面において非連続的な進展が期待される。経済社会への影響(世の中を変える力)という面では、「PC/Windows」、「商用 internet/web」に次ぐ、情報通信技術の第三の変革(クラウドコンピューティング革命)が生起しつつある。(「クラウドコンピューティングと日本の競争力に関する研究会」報告書 2010 年 8 月 16 日 経済産業省より)

(2) クラウドサービスにおける事業

・技術開発の推進

信頼性向上技術(高稼働率:99.999%、高データ保護、障害時復旧技術)、安全性向上技術(個人が特定されないようにする匿名化技術)、高速化技術(流れ込んでくるデータを利用したリアルタイムサービスの実現)などの技術開発が進められている。具体的には、分散ファイルシステム(Hadoop など)上で稼働する NoSQL(リレーショナルデータベース管理システム以外のデータベース管理システム(DBMS)であり、関係モデルによらずに安価なサーバを大量に並べて並列処理することで処理性能を向上させるもの)や SSD、マルチコアなどの技術開発が進められている。

・実証事業

医療分野、交通分野、データ基盤分野、社会基盤分野などでクラウドコンピューティングを利用したサービスを提供するために実証事業が行われている。例えば、医療分野では、健康保険組合のレセプト情報や健康管理事業者のヘルスレコードを大量(18 億件/年)に蓄積して、これらを匿名 ID で付き合わせ、分析・処理して疫学研究や薬剤研究に役立てる実証事業が実施されている。

(3) クラウドに関する政策のロードマップ

・政府は、①イノベーションの創出、②制度整備、③基盤整備、を推進することにより、2020 年度までに、累計 40 兆円超の新サービス市場の創出、情報処理に関わる CO_2　排出を 90 年比で約7%削減、グローバルマーケット獲得による市場シエアの拡大、を計画している。

① イノベーションの創出

- 新サービス創出のための業種横断的アライアンスの形成
- 革新的社会システムの実証(医療、交通、教育、電力などの分野)
- 社会システムの輸出・クラウドサービスの国際展開の支援

② 制度整備

- プライバシーに配慮したデータ利活用・流通の制度整備(匿名化の活用など)
- クラウドサービスの品質・責任関係の透明化
- 政府によるクラウドサービスの活用促進
- データの越境移動やクラウドサービスの国際展開円滑化に向けた国際ルールの策定

③ 基盤整備

- 高信頼性・環境負荷低減技術の開発促進と標準化
- データセンタの集約、連携、立地の促進
- 機器・端末(組み込みシステム)の高度化
- クラウド時代に合わせた人材育成強化

２．クラウドサービスにおける責任

(1) プロバイダの責任

・クラウドサービスを提供するプロバイダ(クラウド事業者ともいう)とクラウドサービスを利用する利用者(クラウド利用者ともいう)の責任範囲を約款や契約などで明確に定めること。例えば、データの管理権がどちらにあるか、バックアップの責任範囲など、を定めることである。

・SLA(Service Level Agreement)に応じたサービスを提供するために必要な運用体制を整えること。

・クラウド利用者がこれらの体制について確認できるようにすること。
・自らが提供するクラウドサービスを構成する他のプロバイダ（連携クラウド事業者ともいう）が提供するクラウドサービスの SLA についても十分に理解すること。

(2) 利用者の責任
・自らの IT サービスの管理目標に応じることができるクラウドサービスを選択すること。そのためには、あらかじめ以下の事項を明確にして、それらの事項が導入を予定しているクラウドサービスにより実現できることを確認する必要がある。
- 利用する IT サービスに関連する許容レベルの設定
- システムの最大許容停止時間、必要なバックアップ、インシデント対応に必要な情報など

３．クラウドサービスによるリスクの変化
(1) クラウドサービスではユーザのリソースがプロバイダ側にある。
- ハードウェアリソース（インフラ管理のデータ）
- オペレーションやサービスのリソース（ログ管理）
- ユーザ管理（アクセスログ）
- データの物理的管理
-

(2) 上記のリソースを管理できるようするためにはセキュリティマネジメントシステムの見直しが必要である。
- ログに頼った管理手法からリアルタイムな管理
  クラウドサービスでは、ダッシュボードと呼ばれる画面が用意され、クラウドサービスの使用状況（稼働状況、資源の使用状況、パフォーマンス状況、イベント・メッセージなど）がリアルタイムで確認できる。また、これらを外部プログラムから確認するための API（Application Program Interface ）が準備されている。
- 様々な管理策、手順書の見直しが必要
-

(3) 見直すべきセキュリティポリシー
・クラウドサービスを導入するに当たり、セキュリティマネジメントシステムに必要な情報が正しく取得できるか、また判断するための情報が十分に得られるか、をウォークスルーなどで検討し、それができなければクラウドサービスを導入すべきではない。
・IT サービスのインソーシングをしてからクラウドサービスに乗り換えるとうまくいく可能性がある。米国では、インソーシング（システム開発や運用などの業務を外部の事業者にアウトソーシングしていた事業者がその業務を自社に取り戻すこと）することにより社内に子会社的なものを作って「システム」と「コンテンツ」を分離させていたので、クラウドサービスへの乗り換えがスムーズにいったと言われている。

４．安全なクラウドサービスの選び方（どんなプロバイダを選べばいいの？）
(1) クラウドサービスに関する事故を調べてみると
・ハードウェアの問題によるもの
電源ダウン、二次電源の誤動作、スイッチングハブの誤動作などが報告されている → これらはデータセンタ側のファシリティの問題である → ユーザはこれらに対して何も対策を講じることができない。せいぜいバックアップを取

ることしかできない

・オペレータの誤操作

保守作業の準備不足、オペレータの知識不足 → これらはプロバイダ側のエンジニアの質の問題である → ユーザはプロバイダ側の運用体制などを知ることも必要

・アクセス権の奪取

コンソールの管理者権限の奪取、アプリケーションのアクセス権の不正利用 → プロバイダ側に問題はない→ ユーザはアクセス権の管理をまじめに考えるべきである

(2) 事故に対するユーザ側の対応

・ユーザはこまめにバックアップを取る必要がある。システムの重要性に鑑みてプロバイダ A のバックアップをプロバイダ B に取るという選択肢も考えられる。

・パスワードの正しい管理

パスワードは 8 文字、3 文字種類でもアタックされてしまう。できればワンタイムパスワード、できなければ二要素認証、それもできなければログインごとのパスワード変更が必要である。

(3) 良いプロバイダとは？

となると、良いプロバイダの条件は、以下の通りとなる。

・バックアップが取りやすいこと

バックアップをすぐに活かすためには、バックアップの互換性が取れるプロバイダをもう1件以上探しておくことも重要である。

・パスワードのオプションが豊富であること

ワンタイムパスワード、二要素認証などの選択肢があることが重要である。

５．クラウドセキュリティガイドライン

(1) クラウドセキュリティガイドライン

・正式名称は、「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」である。これは経済産業省情報セキュリティ政策室が企画した利用者向けのクラウドサービスにおけるセキュリティガイドラインである。初版は 2011 年度版として 2011 年 4 月 1 日に公表されている。この度、2013 年度版として改定が行われ、2013 年 8 月 1 日～31 日の予定でパブリックコメントを募集している。

・利用者が安心してクラウドサービスを利用できるように、サービスの選択や利用について、情報セキュリティマネジメントにおいて何をすることが望ましいかを記載したガイドラインである。

・クラウドサービスを利用するときに検討すべき管理策が記載され、これらの管理策から内容を選択して利用する。

・クラウドサービスの利用促進のためのガイドラインであり、クラウドサービスの利用を差し止めるものではない。

(2) クラウドセキュリティガイドライン策定の背景

・クラウド利用者は、クラウドサービス利用においてセキュリティ上の不安が払拭できず、クラウド事業者(プロバイダ)に対して、情報セキュリティ監査及び JISQ27000 ベースのセキュリティ管理を望んでいる。

・本ガイドラインは、クラウド事業者における「情報セキュリティ」及び「システム運用」が見えないことに起因する不安を「見える化」することにある。

(3) クラウドセキュリティガイドラインの構成

・JISQ27002 をベースにした以下のような内容になっている。

1. 適用範囲
2. 引用規格
3. 用語及び定義

　　} JISQ27002 に準拠した導入部分

4. クラウドサービス利用における情報セキュリティガバナンス及び情報セキュリティマネジメント　→ 本ガイドラインにおける考え方
5. セキュリティ基本方針
6. 情報セキュリティのための組織
7. 資産の管理
8. 人的資源のセキュリティ
9. 物理的及び環境的セキュリティ
10. 通信及び運用管理
11. アクセス制御
12. 情報システムの取得、開発及び保守
13. 情報セキュリティインシデントの管理
14. 事業継続管理
15. 順守

　　} JISQ27002 の管理策部分

16. 附属書 A クラウドサービス固有のリスク
17. 附属書 B クラウド利用におけるリスクアセスメントの考え方

　　} クラウド固有のリスク関連情報

18. 付録クラウド利用における実施の手引の一覧　→ 監査のチェックリストに活用できる

(4) 今回のクラウドセキュリティガイドラインの改定について

・クラウドサービスにおけるリスクの見直し

2011 年度版は、「利用前の懸念事項」を中心にリスクを検討し、対策を記載した。2013 年度版は、「実際の事故」をベースにした対策を記載した。「実際の事故」は、次の「(5) クラウドサービスにおける事故の現状」を参照してください。

・より具体的な記述に一部変更

情報提供などについて、必要に応じて詳細に項目を記載した。また、JISQ27002 の抽象度にとらわれず、具体的に記載できる部分は内容を訂正した。

・事業者自身のセキュリティ

事業者が自らの事業継続などを前提とした対策も一部追加した。

(5) クラウドサービスにおける事故の現状

・調査によるとクラウドサービスにおける事故・障害の多くは、下記に示すようにソフトウェアのバグや運用管理のミスに起因している。

＜調査事例の発生年別内訳＞

2011 年 20 件、2012 年 31 件 （計 51 件）

＜調査事例の発生国の内訳＞

米国 35 件、日本 12 件、韓国 2 件、他 2 件 （計 51 件）

＜調査事例の問題別の内訳＞

ソフトウェア 12 件、ハードウェア 3 件、設計 3 件、運用・管理 9 件、ファシリティ 7 件、サービス妨害 1 件、不正アクセス 9 件、他1件、非公開 6 件 （計 51 件）

・国内クラウド事業者へのインタビューによる事故・障害の実例

＜トラブル原因別件数(N=23)＞

システム障害 17 件（74%）、人為的ミス 5 件(22%)、外部攻撃 1 件(4%)

＜トラブルの説明＞

システム障害:　ハードウェア、ソフトウェアのトラブル

人為的ミス:　運用手順が明確でないため発生したミス、通信事業者とのコミュニケーション不足により発生したミス等によるデータ滅失

外部からの攻撃: DDoS であるが、実害は少ない

６．クラウドセキュリティガイドライン活用ガイドブックについて

(1) 活用ガイドブック策定の背景

・ガイドラインは、JISQ27002 をベースとしているために、慣れていない人には読みにくいものとなってしまった。

・活用ガイドブックは、ガイドラインを説明したものではなく、ガイドラインの使い方を説明している。これをきっかけにガイドラインを活用して欲しい思いで作成している。

・「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」のさらなる活用のために、最新のインシデント事例を基に作成している。

・クラウド利用者だけでなく、クラウド事業者も利用できるように、それぞれの活用シーンを事例として提供し、ガイドラインを様々な用途で活用できるように解説している。

(2) 活用ガイドブックの構成

・活用ガイドブックは、以下の構成と内容になっている。

1. はじめに
   クラウドサービス利用におけるインシデントの調査をもとに、インシデントの傾向と対策を解説している。
2. クラウドセキュリティとは
   クラウドの構造を解説し、構造上の問題点や運用上の問題点を明確にして、事故が発生する原因やクラウド利用者やクラウド事業者の責任を明確にしている。
3. ガイドラインを活用したリスク分析手法
   クラウドの構造やインシデントを受けて、クラウドサービスにおける様々リスクについて解説するとともに、クラウドセキュリティガイドラインの参考となる項番を参照し、重点的な対応ができるようガイドしている。調査結果を前提とした内容になっており、ガイドラインの重点項目がわかるような構成となっている。
4. クラウド利用者のためのガイドライン活用
   クラウドサービスを利用したシステム構築、クラウド事業者の選択、クラウドサービスの契約、インシデントレスポンスの 4 つのポイントについて、利用者の目線で解説している。
5. クラウド事業者のためのガイドライン活用
   クラウドサービスの構築、セキュリティホワイトペーパーの活用、第三者認証の活用、監査の活用の 4 つのポ

イントから事業者の目線で解説している。利用者に安全にサービスを提供するための情報発信だけでなく、事業者組織の情報セキュリティマネジメントについても解説している。また、クラウドセキュリティガイドラインを監査チェックリストとして活用した内部監査の手続きや方法も解説している。

6. その他の活用
クラウドセキュリティガイドラインのクラウド監査人への活用提案、クラウドサプライチェーン管理者への活用提案を行っている。
7. 最後に
8. 付録
事業者、利用者共に活用できる「契約書のサンプルと解説」、「サービスレベル合意のサンプルと解説」が用意されている。

７．クラウドセキュリティガイドラインの国際的位置づけ

(1) クラウドセキュリティガイドラインの国際標準化

・クラウドセキュリティガイドラインを国際標準化するために、英訳して 2010 年 10 月に JTC1SC27 の秋季ベルリン会合に提案した。この提案は、参加国に受け入れられ、現在 2015 年の発行を目標に作業が進められている。
・米国の NIST、Cloud Security Alliance などの事業者団体、ISACA や ITU-T などの団体もクラウドサービスの技術的な観点やシステム監査の観点から提案を行い、日本のクラウドセキュリティガイドラインをベースにした国際標準が策定されている。
・現在策定中のこの標準は、ISO/IEC 27017 として 2015 年 10 月に発表される予定になっている。
・ISO/IEC 27001（JISQ27001）をマネジメントシステムの標準として、また、ISO/IEC 27017 を管理策の標準として選択することで、クラウド固有のセキュリティ認証が受けられるような仕組みも国際標準化会議で検討されている。

(2) ガイドラインの今後

・国際標準ができたらそちらに移行
ISO/IEC 27017 は、日本のクラウドセキュリティガイドラインと親和性が高いため、JIS 化することで本ガイドラインを置き換えることができる。一方のクラウドセキュリティガイドライン活用ガイドブックは、ISO/IEC 27017 が発行された後でも活用できるよう既に調整が済んでいる。
・事業者向けの管理策も多く提供される
国際標準化会議の場でも事業者向けの管理策が望まれており、監査を積極的に行いたい意向である。また、事業者向けの管理策も多く盛られており、クラウド事業者にも利用できるガイドラインとなっている。

８．Q／A

＜要望 3 件＞

利用者として、非常に解り易く読み易い工夫をしたガイドブック等を策定していただき、
感謝しております。次の3点について要望したい。

① ガイドブックにおけるリスク分析の部分とガイドラインのリスク説明の部分が重複しているので、統合すると更に解り易くなると考えるが、いかがですか。
② ガイドブックのリスク分析において、ガイドラインにおける関連管理策が引用されており非常に有益であるので、更に、詳細化していただければ、助かります。

③ ガイドラインの「クラウドサービスの関連情報」欄で「期待される」という用語を使っている。これまでは、「期待される」という用語を使用していないので、定義・意味を明確にしていただきたい。

＜回答＞

① ガイドブックとガイドラインの策定チームが異なっており調整しているが、今後、更に、調整していきたいと考えている。

②③ パブリックコメントで提出願い検討したい。

＜質問1＞

「利用者と事業者間の情報格差を解消するためのガイドラインのワーディングについて」

クラウドサービスにおける利用者と事業者との情報格差が存在する点に関連して、ガイドラインの要求事項では、・・・することが望ましい・・・、should＝望ましい、としている。両者間の情報格差の解消にむけて利用者サイドに立った「強い表現」としていただけないかと考えるがいかがですか。

＜回答＞

今回の表現は、JIS の標準用語を使用し、should＝望ましい、としている。クラウドのガイドラインでは、「安かろう、悪かろうという事業者のサービスは許さない」という姿勢は控えるよう意識して、「望ましい」の表現レベルで策定している。事業者から情報開示がないという点は望ましくないが、「サービスをスポットで利用する場合があること」、「クラウドサービスにおける消費者契約の取扱（注：消費者契約の免責事項）」の考え方もあり、事業者をあまり縛らない（注：サービス内容を強制しない）」との考え方から、「望ましい」の表現としているので、理解されたい。

＜質問2＞「ENISA のクラウドサービスのリスク見直しについて」

ガイドブックでは、クラウドサービスのリスクについて、ENISA の利用リスクを引用しているが、今回の検討ではその後の故障・障害実績を収集し分析している模様であるので、日本として、クラウドサービスのリスクを見直す試みはないですか？

＜回答＞

ENISA が提案したクラウドサービスのリスクについては、提案後、数年たっているが、改訂の提案などがなく、動きが鈍いのが現状である。今後のこのリスク評価の見直しについては、経済産業者も意識している模様である。しかし、多くの企業へのインタビューなどによると、（例えば、法律的リスクについても）物理的に分離して対応している場合が多く、現地（国）の法律に沿ったリスク回避策を講ずることとしているので、あまり大きな問題としては理解していない。なお、講演の時間が十分取れない部分について補足説明したい。ガイドブックでは、クラウドサービス事業者の2年間の事故障害状況を公表ベースで集計し掲出しているが、ヨーロッパは1件であり、非常に少ない。これは、ヨーロッパではクラウドサービスが少ないのではないかと推測しており、クラウドサービスの利用が、アメリカと日本にかなり偏っている状況もあって、この状況が事故障害件数へ反映されている模様である。ヨーロッパでのクラウド利用は、アメリカで開発されたサービスをリセールして利用するが、日本ではこれを国内で熱心に開発するなどの取組みをしているのが現状である。国際規格を議論する会議などでも、日本とアメリカが主体となっている。

＜質問3＞

「クラウドのサプライチェーン、API に関連する点検・監査（検査）の方法について」

ガイドブック等では、クラウドにおけるサプライチェーン、API について解説しているが、点検・監査（検査）の方法が複雑となってきている。これらへの対応方法をアドバイス願いたい。

＜回答＞

間もなく公開予定の ISO/IEC 27002 では、「サプライチェーンマネジメント」の項目が設定されているので、これに対応し解説している。以下、「クラウドのサプライチェーン、API に関連する点検・監査（検査）の方法」について、いくつかの対応例を説明する。

例えば、API について、利用者が、「複数サービスの API を組み合わせて利用する場合」、と「複数の API を使用しているサービスを利用する場合」がある。即ち、利用者からみると、「複数ベンダーと対応する場合」、と「1ベンダーと対応する場合」がある。

この際は、監査等の対象をどこにするか、「複数ベンダーに対して監査等をする」、「1 ベンダーを信用し絞って監査等をする」の方法があり、事業継続の対応をどこまで確認するかである。例えば、1ベンダーを信用し絞った場合は、利用サービスのリダンダンシー（冗長性）、バックアップ方式、インシデント対応策の監査等になると考える。自社で複数の API を利用する場合も、それぞれを意識することは当然である。

また、中間事業者が提供するサービス、グーグル・アマゾン等を利用する場合も、API サービスが中止となった際の事業継続を確認しておく必要がある。

次にクラウドサーバをみると、これまで、ウェブサーバとウェブクライアントを対象としてきたが、ブラウザを含め関連する各種の API と利用環境との整合条件として、サービスが安全かどうか、クライアントが安全かどうか等の、各種の確認が必要であり非常に複雑になってきている。利用者側でセキュリティが確保できるかの観点からは、どのサービスを使うかではなくて、どのサービスをどのリンケージ？で使うかが監査等の対象となる。API の作りについては、標準的なプロトコル・データフォーマットか、独自様式となっているかなども監査等の対象となる。

契約の世界をみると、「基盤サービス事業者が他社の各種サービスをインテグレートしてサービス提供する場合」、「他の事業者が基盤サービスに各種サービスをインテグレートしてサービス提供する場合」がある。後者では、契約に対するユーザ責任が大きくなってきており、契約内容、サービス利用、サービスのシステム構成などについて確認が必要であり、監査等の範囲が広くなる。

【所感】

今日、PC/Windows、Internet/Web に次ぐ第三の変革として「クラウドコンピューティング革命」が起きつつある。これは、「IT の所有」から「IT の利用」への転換を促す大きな「IT のパラダイムシフト」であるといえる。政府は、クラウドコンピューティングを安全・安心に普及させて、2020 年までに累計で 40 兆円超の新サービス市場創出とクラウドの活用による CO_2削減の構想を立て、制度面や基盤面の整備、イノベーションの創出を図ろうとしている。

クラウドサービスを提供するクラウド事業者が十分なセキュリティ対策を講じていても、利用者がクラウドサービスを利用するのには、ためらいや不安がある。そこで、経済産業省は、利用者がクラウドサービスを安心して利用できるように、情報セキュリティマネジメントにおいて何をすべきかを記載したクラウドセキュリティガイドラインを策定した。今般、そのクラウドセキュリティガイドラインを改定すると共に新しく活用ガイドブックを策定した。活用ガイドは、ガイドラインの使い方を説明したものである。いずれも、具体的な説明があり、わかりやすい内容になったという感触を持っている。

クラウドコンピューティングの進展により情報処理の形態が所有から利用へと大きく変わることから、情報システムの信頼性・安全性・効率性を監査するシステム監査人にとっても、この変化に対応するために、クラウドセキュリティガイドラインの内容を理解することは有効であると考える。

以上

2013. 10 投稿

【第 185 回 月例研究会 報告】

会員番号 1760 斎藤由紀子 （事務局）

日　　時: 2013年9月18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:「システム監査の実践的な進め方～チェックポイントと実務上の留意点～」
講　　師: 東洋大学 総合情報学部 教授 島田 裕次 氏

＜講演骨子＞

今までのシステム監査をはじめとする内部監査の実務経験及びシステム監査に関する研究を踏まえて、システム監査の実践的な進め方について説明する。具体的には、付加価値の高いシステム監査、経営に役立つシステム監査の実現を目ざすためには、どのように取り組むべきか、5つの論点に整理して考えていく。

（講師から頂いた講演骨子より）

＜講演概要＞

論点1「システム監査の目的を再認識」
論点2「準拠性の監査から有効性・効率性の監査へ」
論点3「多面的な視点で監査を実施する」
論点4「リスクアプローチから目的アプローチへ」
論点5「外部化を前提とした監査」

＜講演内容＞

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.「システム監査の目的を再認識」

(1)システム監査とは

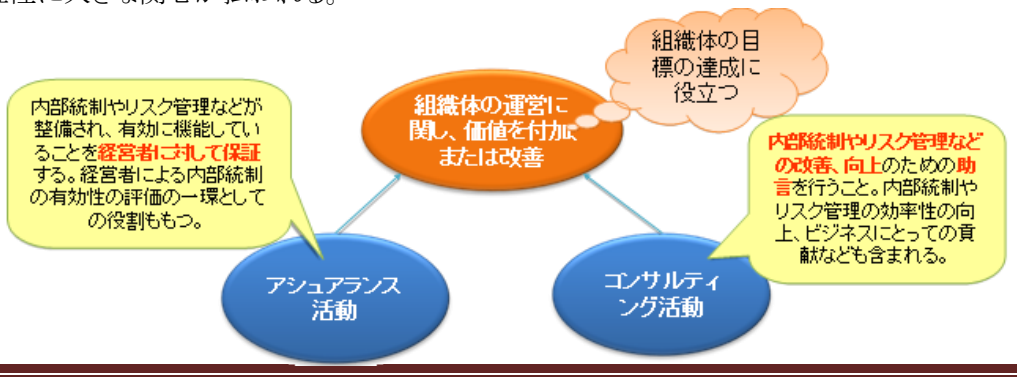
・システム監査は、ITガバナンスの確立状況を点検・評価することが目的である。
・情報セキュリティは、ITガバナンスに含まれるものであり、別の概念ではない。
・ITガバナンスとコーポレートガバナンス、コーポレートガバナンスと内部統制、内部統制とITガバナンスの概念整理をしておく必要がある。

(2)内部監査と外部監査の2つの側面

・内部監査では、情報セキュリティだけではなく、情報システムの有効性、効率性に大きな関心が払われる。
・外部監査、特に会計監査人が財務諸表監査の一環として実施している場合や内部統制監査の場合には、財務報告に係る信頼性や正確性に大きな関心が払われる。

(3)内部監査の定義

・内部監査は、組織体の運営に関し価値を付加し、また改善するために行われる。



(4) IT統制評価との比較

	IT統制評価	システム監査
目的	財務報告の信頼性に係るIT統制の有効性の評価	ITガバナンスの確立・運用状況の点検・評価
義務	必須	任意
評価対象	財務報告に係る情報システム（全社統制、IT全般統制を含む）	全ての情報システム（財務報告に係らない情報システムも含む）
評価の視点	インテグリティ	戦略性、有効性、効率性、インテグリティ、可用性、機密性など
手法	質問、サンプリング、観察、再実施	質問、サンプリング、観察、ログやデータ分析など（サンプリングは必須ではない）
責任	経営者への評価責任 評価手順や手続に問題があれば会計監査人が指摘	経営者に対する監査責任
柔軟性	低い	高い
判断基準	リスクに対するコントロールの有効性	経営にとっての有効性、業務改善
実施主体	内部統制の評価担当部署（内部監査人,財務部門など）	内部監査部門（外部への委託もあり）

(5)情報セキュリティ監査との比較

	システム監査	情報セキュリティ監査
監査の目的	ITガバナンスの確立・維持状況を点検・評価	情報資産のセキュリティの点検・評価
監査対象	情報システム	情報資産（情報システム以外の情報資産も含む）
監査の視点	戦略性、有効性、効率性など幅広い視点	セキュリティ（機密性、可用性、インテグリティ）
監査の判断尺度	システム管理基準 COBIT	情報セキュリティ管理基準 ISO/IEC 27001
備考	情報システムが監査対象となり、記憶や口頭によるコミュニケーションは監査対象外	情報セキュリティ管理基準は、情報システムに関するセキュリティが中心

2.「準拠性の監査から有効性・効率性の監査へ」

(1)準拠性監査とは

・規程やマニュアルに従って業務が行われているかどうか監査する。

・業務の根本的な改善のためには、規程やマニュアルで定められていることの目的を考える必要がある。

(2)有効性監査とは

・ビジネス目標の達成に役立っているかどうか（IT化目的を達成しているかどうか）を点検・評価するものである。

・ITの有効性監査では、情報システムがビジネス目標（売上・利益の拡大、顧客の獲得、コスト削減等）の達成に貢献させるための仕組みやプロセスがあるかどうかを確かめる。

・IT化の目的自体がビジネス目標の達成に貢献しているか確かめることが重要である。

【例えば】変更管理の監査では・・変更管理の見方を変えてみると？

・変更依頼書に基づいて変更作業を行っているか？

・事前に承認を受けているか？

↓

・変更作業の多い情報システムはないか？

➢　システム機能や業務プロセスに問題はないか？

- システムが老朽化していないか？

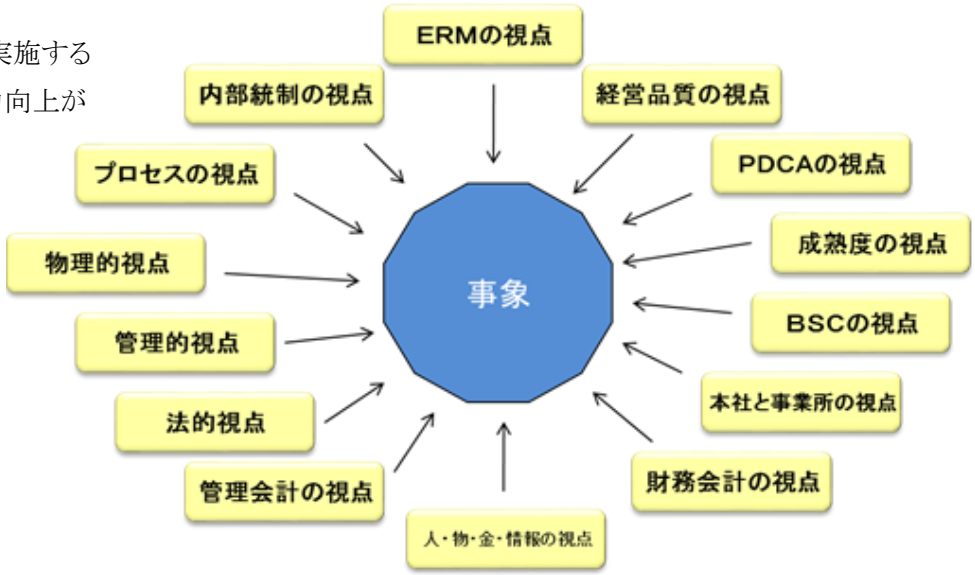
・類似の変更作業が発生していないか？
- システム機能として組み込んだらどうか？
- 業務プロセスに問題はないか？

・変更作業は効率的に行われているか？
- ボトルネックはないか？
- 無駄な作業はないか？

3.「多面的な視点で監査を実施する」

(1)多面的な視点とは

・付加価値を生む内部監査を実施するためには、内部監査人の能力向上が不可欠である。特に、事象を多面的に捉える能力が重要である。



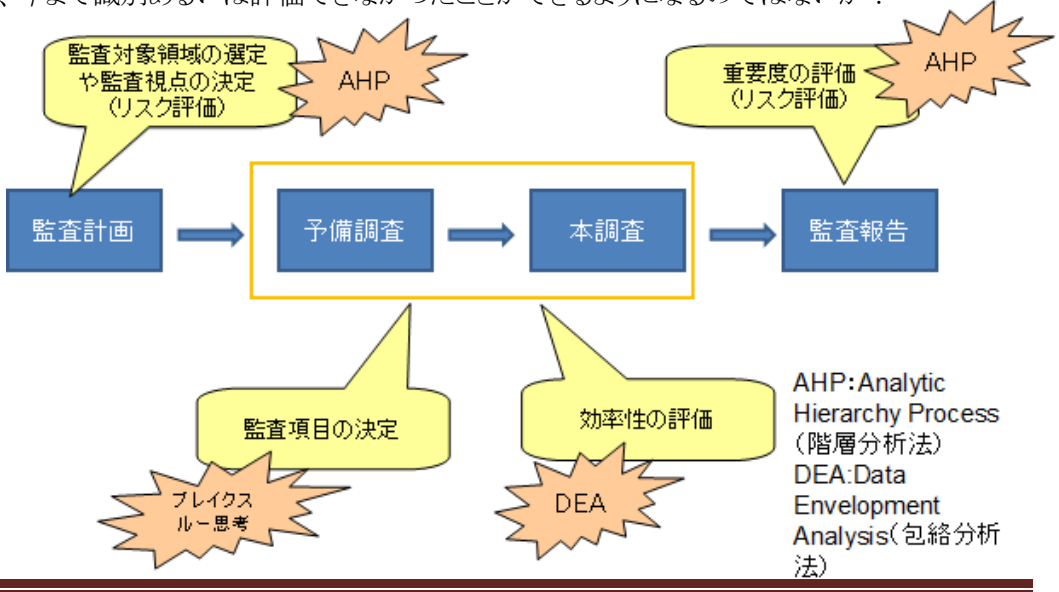
(2)工学的アプローチの必要性

・多面的な視点ということで、参考までに工学的アプローチを紹介する。

・監査は、もともと会計監査を中心に発展してきた。その後、業務の適切性を点検・評価する業務監査へと拡大した。また、監査論は，会計学や経営学の一分野又は関連分野から研究されてきた。

・一方、工学の研究者は、監査についての知見はほとんどないので、どのような研究が求められているのか認識されていない。

・工学の手法を用いれば、今まで識別あるいは評価できなかったことができるようになるのではないか？



4．「リスクアプローチから目的アプローチへ」

(1)ブレイクスルー思考とは？

・ブレイクスルー思考は、1990年ナドラー及び日比野によって公表された問題解決の手法である。

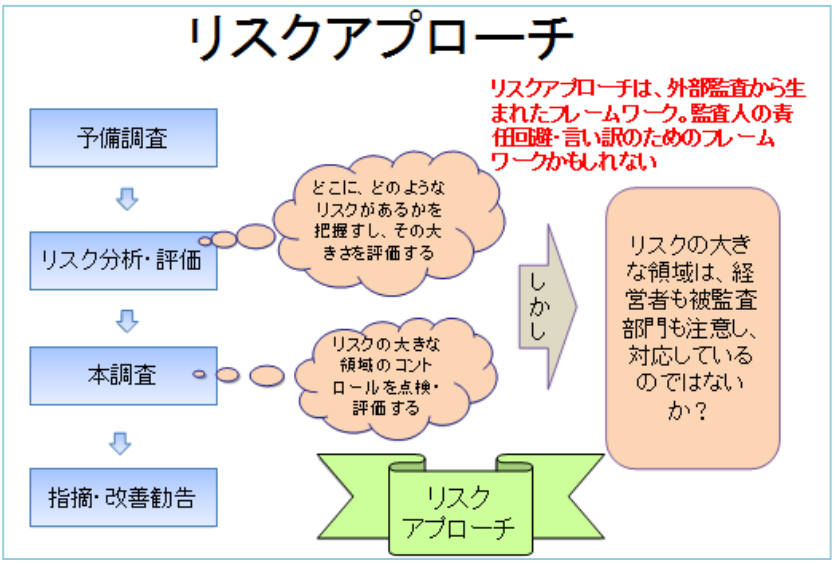
・思考のパラダイムシフト(「デカルト思考」(問題分析)と異なる思考)であり、事実の確認の前に「コンポン」、すなわち「目的」を確認することが重要だとしている。

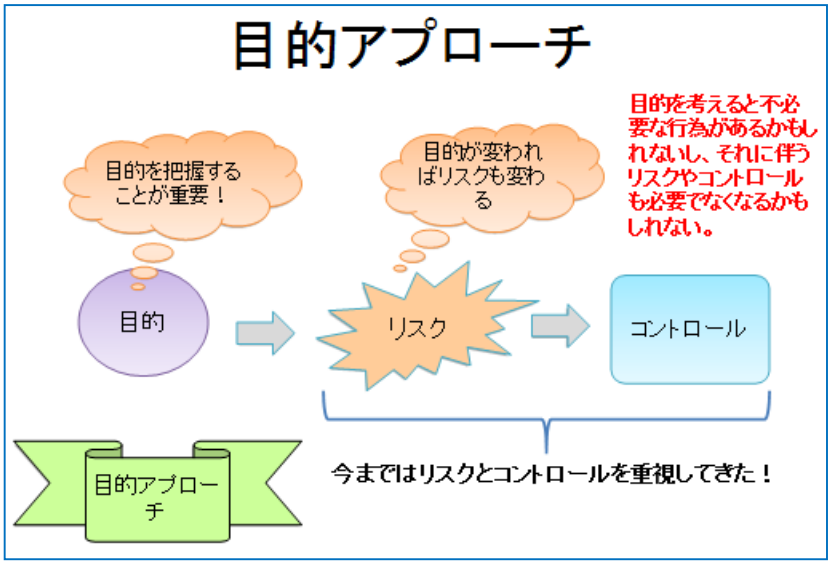
・統合・連動・全体を強化する認識、つまりシステムとして捉えることを行う。このシステムとは、「果たすべき目的をもち相互関係をもつ総体」のことをいう。

(2)なぜブレイクスルー思考なのか？

・ブレイクスルー思考では、原因分析ではなく、目的からアプローチすることが大きな特徴である。目的は、リスクと深く関係するので、リスクの視点からアプローチするのではなく、目的の視点からアプローチすることは有効である。

・監査対象をシステムとして捉えるので、監査対象を体系的に監査することができる。





(3)どのように監査を行うのか？

例えば、次のような視点でシステム監査を実施したらどうか？

・アプリケーションシステムについては、次のような視点で監査する。

- この情報システム（ERP、クラウド等）の目的は？
- 似たような目的のシステムはないか？
- 他の方法で目的を達成できないか？
- 新しい技術を使えないか？
- 将来、この情報システムでビジネスに対応できるか？

・システム部門については、次のような視点で監査する。

- 開発部門、運用部門、保守部門の目的は？
- 目的を阻害している要因はないか？
- 外部委託の目的は？それを達成しているか？
- あなたの仕事の目的は？何のために起票、承認、確認を行っているのか？

5.「外部化を前提とした監査」

(1)外部化への対応が重要

・IT関連業務のうち、どの領域を外部委託しているか？

- 企画、開発
- 運用、保守
- ITインフラ
- 入力、出力　など

・外部化にかかわるリスクを多面的に評価しているか？

- 開発、運用、保守の品質
- 情報保護
- 知的財産権（開発ノウハウ、業務ノウハウの保護を含む）
- リーガルリスク
- ベンダーロック　など

(2)外部委託先に関する監査

・外部委託先の選定が適切に行われているか？

- 選定基準（ISMS、プライバシーマーク等の認証取得状況、内部監査の実施状況）
- 作業管理

・契約が適切に締結されているか？

- 契約書（機密保持、損害賠償、従事者の監督、再委託の禁止等）

・外部委託先の従事者に対する管理が適切に行われているか？

- 教育指導、日常管理
- 作業場所、作業状況の視察

・アクセス管理は適切に行われているか？

- ユーザID、パスワードの管理
- 媒体へのアクセス

(3)IT子会社の監査

・内部統制（金商法）の視点から、そのまま監査を行ってしまうと、内部統制の有効性評価の結果と同じになってしまい、システム監査の付加価値が生まれない。

・様々な認証を取得している場合

- 取得によるメリット(売上件数・金額の増加、取引先の拡大などへの寄与)
- 「マネジメントシステムの内部監査」との統合などの効率向上

・外部からの業務受託の有無によって、監査の視点が異なる

(4)クラウドの監査

・多様なITを組み合わせて活用する態勢があるかどうかを確かめる。

・ユーザ企業側とクラウドサービスの提供側では求められる要件を認識して監査を行う。

・利用目的、クラウドの種類によってリスクは異なり、監査対象領域も異なる。

監査での質問項目 (例)

質問(例)	確認内容
IT戦略においてクラウドの導入方針が明確になっているか。	・導入してよいサービスの明確化 ・利用目的の明確化(コスト、開発費の低減、開発期間の短縮、要員の外部化など) ・自社の競争優位を確保との関係 ・自社開発、パッケージ調達との比較基準(開発費、利用期間、開発期間など)
クラウド利用におけるリスクについて、リスク分析したか。	・リスクの網羅性 ・リスクの把握は、どのような手順で行ったか?(誰が、いつ、どのようにして行ったのか?)
リスク分析の結果、どのようなリスクを把握したか。	・クラウドサービス自体に関するリスク ・クラウドサービスと自社システムとのインターフェースに関するリスク ・自社システムに及ぼすリスク
把握したリスクの大きさをどのように評価したか。	・クラウドが利用できなくなったら社内業務にどのような影響が生じるか、顧客にどのような迷惑をかけるか ・時間軸で考えること。許容時間は? ・世界各地で発生した災害・事故などがクラウドサービスに影響を及ぼすか ・復旧までの手順をどうするか
クラウドサービスの選定をどのように行ったか。	・複数案(機能・価格・継続利用性など)の比較・検討 ・利用規約の確認 ・ベンダーの評価 ・提供機能とクラウド化する自社業務のF&G分析 ・自社業務プロセスの見直し
リスクへの対応策(コントロール)を検討したか。	・リスクとコントロールの整合性 ・コントロールの費用対効果 ・暗号化ツールの利用
クラウドサービスに関するモニタリングを行っているか。	・ベンダの経営状況 ・ベンダの社会的な評判 ・社内の利用状況
クラウドのBCPを策定しているか。	・クラウドのレスポンスが低下したとき、利用ができなくなったとき ・自社システムへの影響

～おわりに～

(1)今後の監査テーマ(例)

・今後の監査テーマとしては、例えば、次のようなものが考えられる。
・システム開発プロジェクトの監査
・クラウドコンピューティングの監査
・スマートフォンの監査
・サイバーテロ対策の監査
・外部委託管理の監査
・海外拠点・海外子会社の監査
・代理店・販売店の監査
・消費税対応の監査
・IFRS対応の監査

・その他（SNSの監査、BYODの監査ほか）

各社のリスクを考えて、監査対象領域、重点監査項目を決めることが重要である。

(2)システム監査の課題と期待

・システム監査の重要性は認識されているが、思うようにシステム監査が進展していない。

・課題
- 人材の確保
- 監査スキルの向上
- IT統制（J-SOX）から有効性監査へ
- CAATs（コンピュータ支援監査技法）

・期待
- 経営の役に立つシステム監査の推進（情報システムの有効性、開発・運用の効率性、システム開発プロジェクト、データ活用などに関する監査）
- 情報システム監査をIT人材の育成の場として活用
- 企業グループとしてのIT化の推進に貢献する情報システム監査

＜主な質疑応答＞

Q1：内部監査における、システム監査の課題など、事例をお聞きしたいが？

A1：IT統制の有効性監査で手いっぱいの企業が多いが、日本内部監査協会が「内部監査実施状況調査」で監査テーマを公表しているのでこれを参考にするとよいと思う。人材育成については、内部監査人を育てるために、社内公募制などでやる気のある人を活用する事例もある。また、社外コンサルを1～2年の長期で契約し、監査チェックリストを策定する事例がある。

Q1：目的アプローチと、リスクアプローチの比較について、今一度お聞きしたいが？

A1：ここで強調しておきたいことは、リスクに注目するだけではなく、リスクの基になる目的（ビジネス目的）に注目することが大切ではないかということである。なお、目的アプローチは、監査の着眼点を捉えるときに有効である。リスクアプローチは計画立案時に役に立つ手法である。目的を捉えずして監査はできない。

＜報告者所感＞

島田教授は、東京ガス㈱にて監査部情報システム監査グループマネージャーを努められ、2000年以前からビジネス改革と情報セキュリティの両面から研究活動を行われる中で、2003年「情報セキュリティ監査制度」2007年「J-SOX法がよーくわかる本」、「内部監査人の実務ハンドブック」など、数多くの著書を世に出されてきた。今回の研究会では、まずシステム監査を原点から問い直し、システム監査の目的を再認識することから最も重要であると、強い信念で話をはじめられた。特に印象に残ったのは、論点3「多面的な視点を持つ」ことの重要性の部分で、「監査の着眼点が分からずに悩んでいる内部監査人が少なくない。どのように監査の着眼点を決めるのか？」と質問が出され、よい監査をするには、スペシャリストとしての経験を重ねるとともに、多面的な視点を持つゼネラリストとして研鑽を積むことが要求されるのだとあらためて痛感した。

講義の中では、IT統制評価、セキュリティ監査との比較や、どのように監査を行うのか？といった具体的な課題を提議いただき、また今後のIT環境の変化として避けて通れないクラウド事業者の監査項目についても、事例を示していただくなど、大変実り多き講演をいただいた。

島田裕次教授には、改めて深くお礼を申し上げます。ありがとうございました。

以上

2013.10 投稿

【北信越支部　「2013 年度新潟県例会 報告」】

以下のとおり2013年度 北信越支部新潟県例会を開催しました.

・日時:2013 年 9 月 7 日(土)13:00～17:00　　参加者:11 名

・会場:まちなかキャンパス長岡 (新潟県長岡市)

・議題:

- ✧ 報告 1:「クラウドにおけるセキュリティの確保」　神田 英一朗 氏
- ✧ 報告 2:「ビッグデータ 宝の山♪」　梶川 明美 氏
- ✧ 「システム監査の普及促進」に関する意見交換 － 西日本支部合同研究会 in Kanazawa テーマ検討 －

◇研究報告 1
「クラウドにおけるセキュリティの確保」

報告者(会員 No. 1632 神田 英一朗)

私はクラウドサービスの一つである、VPS(Virtual Private Server)を使用した Web アプリケーション開発を本業としている。情報投資に余裕のない中小企業が、企業の基幹業務も含めこのような基盤上に業務システムを構築する際のセキュリティの確保を何処まですべきなのか、C/S 型システムと比較して弊社の事例を報告し会員各位からのご意見をうかがう機会とした。

1. C/S 型システムの特徴

(1) 旧来のホスト集中型システムと比較して優れた点

効率のよい分散処理のため、以下の様な優れた点がある。

- レスポンスの速さ
- GUI による高操作性
- コスト軽減

(2) C/S 型システムの劣る点

全てのクライアントにアプリケーションをインストールすることに起因し、以下のような劣る点がある。

- インストールの手間
- 障害発生時の復旧工数が大きいこと…可用性の低さ
- クライアントのバージョン管理の煩雑さ
- クライアント機への依存性の高さ
- ライセンス料の負担

(3) オンプレミスのリスク

- 安定した電源確保の必要性
- 落雷・地震・津波・水害等の災害対策
- 計画停電、節電対策
- 中小企業では管理者が不在

2．クラウド利用の特徴

(1) クラウド利用の利点

- コストの大幅削減
- ハードウェアの自社管理が不要
- スマホ、タブレット端末の利用が可能
- クライアントがOSに依存しない

(2) クラウド利用の問題点

インターネット利用が前提となるため、以下の様な問題がある。

- なりすましなどによる情報漏えい
- 不正アクセスによる情報書き換え、破壊
- スパム攻撃などによるアクセス不能

(3) クラウド利用による事件事例

- グーグルグループの誤った設定による中央官庁内部情報漏えい
- Gamil アカウントが露見しスパムの踏み台に利用された

3．弊社の推奨するクラウド利用

(1) VPS の利用

- 計画停電・節電対策
- 極めて安価な利用料金

(2) メールサーバーに Google Apps 利用

- サーバーへの不正アクセス管理から解放

(3) DropBox、Google Drive の利用

- USB メモリーの紛失による情報漏えいを回避
- 共有ファイルとしての利用

(4) サイボウズ Live の利用

他組織との情報交換・情報共有は有意義なのでグーグルグループに代わる手段として

- 招待制なので Google Group より安全

4．VPS の利用

(1) 不安感

- システムダウンのリスクはどうか？
- 情報漏えいは発生しないか？
- なりすまし等不正アクセスはないか？
- 安いから不安

(2) 利用した感想

- オンプレミス環境よりはむしろシステムダウンのリスクは小さい。
- 回線速度などによるボトルネックは業者によってはかなりある。十分な選定が必要。
- リスクへの対策は絶対に必要。どこまですべきか。

5.　弊社で行っている VPS でのセキュリティ対策

(1) アクセス制御となりすまし対策

- 基本的にベーシック認証＋ログイン認証
- 端末認証を行うケースもある(メールで本人確認、マスタおよび Cookie との一致による認証)
  - ①　使用する PC、スマホで使用出来るメールアドレスをユーザ登録しておくことが前提
  - ②　初めてログインする時端末認証のメールを送信(Cookie クリア時も)
  - ③　メール中の URL クリックで端末認証番号が使用するブラウザの Cookie とユーザーマスタに保存
  - ④　牽制機能として、アクセスログを採取し、ログイン認証エラーを記録

(2) データの暗号化とバックアップ

- データベース接続のパスワードは暗号化しているが、データは暗号化していない。
- VPS 内で定時に曜日ごと7世代管理、さらに別の VPS にバックアップを暗号化転送。

(3) 通信の暗号化

- SSL 認証
- SSL-VPN は通信速度が低下することと、クライアントソフトが必要なので利用していない。

6.　意見交換

大企業や銀行、官庁などではクラウド利用そのものが許可されていない現状の中で、中小企業では利用が加速されている。大企業との情報交換等が中小企業でも進んでいるため、野放しでの利用状態は看過できない、との意見もあった。

以上

◇研究報告 2
「ビッグデータ　宝の山♪」

報告者(会員 No. 0947　梶川　明美)

6～7年前の地方公共団体向けセミナーで、世界中の情報を蓄積して活用するグーグルの構想について聞く機会があった。まだビッグデータという言葉は世の中に出ていなかったと思うが、なんと斬新な計画だろうと脅威すら感じたことが記憶に残っている。ビッグデータとまでは行かないまでも、保有データを高度に活用することにより、データの持つ潜在能力を引き出せるような気がしている。

ビッグデータの現状と今後の方向性について考察した。

[ビッグデータの分類]

- データの構造により、構造化データ及び非構造化データに分類される。また、広義では、ビッグデータを処理するための技術や人材・組織を含める場合もある。
- データの発生源により、インターネット等、M2M、オープン(パブリック)データに分類することもできる。

[ビッグデータ流通量の推移]

- 産業別では、9 産業(サービス業、情報通信業、運輸業、不動産業、金融・保険業、商業、電気・ガス・水道業、建設業、製造業)の、構造化及び非構造化データ計 17 種の合計による推移をみると、2005 年から 2012 年の 7 年間で、約 5.5 倍に拡大した。
- メディア別では、電子カルテ、画像診断、GPS、RFID といったM2M系データの伸びが大きい。

［ ビッグデータの活用 ］

- 以前は顧客獲得や商品開発等の商品販売に活用されることが多かったが、最近では医療、社会インフラ、防災等様々な分野で活用されており、データ活用のすそ野が広がっている。
- いろいろなデータの活用方法を見ていくことで、自組織の持つデータや他からの購入データとの組み合わせも含めたデータの可能性について想像力を膨らませたい。

［ 今後の方向性 ］

- プライバシー保護

  情報流出防止対策は当然であるが、リスクを低減するために、個人識別情報の匿名化・分離も検討する。

  最近議論となった情報収集による報道事例から、利用者への丁寧な説明により理解を得るといった、情報利活用の透明化を高める取り組みが必要である。

  特にセンシティブデータについては、どこまでよくてどこからダメか、公開範囲等についてあらかじめ検討しておく。

- データ保全

  ICTの高品質化・低価格化により、迅速で大容量のデータ流通・分析・活用が可能となった。

  しかしながら、むやみにため込むのではなく、データのバックアップや廃棄時期を見極めるなど、データのライフサイクルについて考えることも大切であろう。

- 人材育成

  ビッグデータを分析し、有用な意味や洞察を引き出せるデータサイエンティストの育成が急務である。

  しかし、もっと必要なのは、ビッグデータをどう使うかを自ら考え、生み出すことのできる創造力やセンスを持つ人材ではないだろうか。

以上

◇「システム監査の普及促進」に関する意見交換
－西日本支部合同研究会 in Kanazawa テーマ検討－

会員 No.1281　宮本 茂明

11 月に開催する「西日本支部合同研究会 in Kanazawa」のテーマ「システム監査の普及促進」に関し，新潟県例会参加者のそれぞれのシステム監査と関わりを起点に意見交換を行った．以下にその概要を報告する．

[システム監査の浸透]

- 10 年前から比べると「システム監査」という言葉は，浸透してきている．

[経営に有効なシステム監査]

- 監査対象である企業等の経営に対してシステム監査の価値を示すことが重要．
- システム開発や運用の現場における不備を指摘するのみにとどまらず，経営に全社的な管理態勢の整備を指導していくことが求められる．
- 経営にとって有効なシステム監査であるべき．
- 経営を指導できる高い見識とスキルを持ったシステム監査人の育成が課題．

［金融機関におけるシステム監査］

- 金融機関では行政の指導により，経営に対してシステムリスク管理態勢の整備が求められ，システム監査がその一つの方策として位置づけられている．
- システムリスクの多様化に対応し，金融機関では情報システムのコントロール構築，及び当該コントロールが効果的に機能していることの第三者検証である「システム監査」は重要性を増している．
- システムリスク管理のPDCAにシステム監査を組込むことで，リスク管理態勢がレベルアップし，事故発生件数の減少や重大事故の未然防止等の成果が出ている．
- 内部監査としてシステム監査は活性化しており，良い循環が生まれている．

［行政施策・指導］

- 金融機関を例に考えると，企業等の経営にシステムリスク管理態勢の整備を義務づけることが必要であり，その方策としてシステム監査の価値が高まることが期待される．

［システム監査効果のアピール］

- システム監査の効果事例を外部アピールすることで，システム監査を世の中に広く知らしめ，「システム監査の普及促進」に繋がっていく．そのためには，システム監査効果の見せ方に工夫・検討が必要．
  - ✧ システムリスク管理にかかる情宣活動
  - ✧ 外部へのシステム監査価値のアピール
  - ✧ 組織マネジメントに対する監査結果の「価値」可視化
  - ✧ プロジェクト品質保証としてのシステム監査可視化
    - ✓ 監査結果の「価値」可視化にあたって，これまでの監査結果からシステム監査効果の評価指標を検討し，その後監査計画段階から KGI,KPI として可視化計画策定が考えられるが，定量的に表すのは難しく研究が必要．

［中小企業におけるシステム監査］

- 中小企業の IT 経営，IT リテラシは上がってきており，システム監査ニーズもあると思うが，コスト面がネック．
- 中小企業の場合，システム監査にかけるコストは大企業に比べ抑える必要があり，監査テーマ別メニューのような形でアプローチできると良いのではないか．

［外部委託業務の監査］

- リスクのコントロールには，委託元企業等が委託先における業務遂行状況を適切に管理することが不可欠であり，それには有効な立入り監査実施が必要．
- 委託先において，多くの委託元からの立入り監査の個別対応に苦慮している状況もある．
- 委託先立入り監査をコストパフォーマンスよく実施できる枠組みが必要．

［監査スキル強化］

- システム関連技術の進歩が速く，多岐にわたることから，システム監査人も関連技術を適宜タイムリーにカバーする必要がある．

以上

2013.10 投稿

【近畿支部　第１４１回定例研究会　報告】

報告者：No.0645　是松　徹

1. テーマ　:「私が経験したシステム監査の実態について」
2. 講師　　:関電システムソリューションズ株式会社 経営改革推進本部 人財部 椋野 誠司 氏
3. 開催日時:2013 年 9 月 20 日(金) 18:30 ～ 20:30
4. 開催場所:大阪大学中之島センター 3階 講義室 301
5. 講演概要:

講師が経験された下記業界のシステム監査について、監査手順等の実態を苦心された点を含めて具体的に講演いただいた。

・運輸会社のシステム監査
・証券会社のシステム監査
・地方自治体の情報セキュリティ監査
・通信事業者のシステム監査

実施実績では、ご自身のキャリア形成(監査資格取得)と対比させて各監査の実施時期を説明いただいた。

監査人の守秘義務から各監査に関する資料配布が難しい旨のご説明をいただいており、今回の報告内容もこの点を踏まえ、限定した記述にとどめている。

①運輸会社のシステム監査

助言型監査として 2004 年に実施した。顧客経営層からは、監査を通した現行システムの見える化を要請された。

②証券会社のシステム監査

助言型監査として 2005 年に実施した。検査マニュアルに定められた内容を網羅的に確認する手続きで監査を進めた。監査での助言内容は方向性のレベルであり、監査後に別契約を締結してコンサルティングを実施した。

③地方自治体の情報セキュリティ監査

2005 年、2006 年に実施した。2005 年は顧客から保証型監査を求められ、10 年保証とした。

④通信事業者のシステム監査

助言型監査として 2007 年に実施した。内部統制の整備・運用状況を評価した。

⑤全体の振り返り

特に苦労した点として、助言の落とし所をどこに持っていくか(コンサルティングとの違い)、保証にあたって何をその拠り所とするか(言明書等の考えはなかった)を挙げられた。さらに、各監査を通じて抱いた所感として、監査の円滑な遂行には監査開始前と監査報告会前の監査対象部門との事前合意(握り)が非常に重要であることを強調された。

6. 所感

講師ご自身の実体験を踏まえた説得力のある貴重なお話を伺うことができました。個々の監査内容もさることながら、とりわけ全体の振り返りの中で説明いただいた助言とコンサルティングとの切り分けや監査対象部門との事前の握りについては、私も業務としている内部監査遂行の過程でたびたび考えさせられる点であり、大いに参考となりました。

講演後の Q&A では、保証型監査について何人かの方から拠り所等に関する質問がだされ、保証型監査への参加者の関心の高さが伺えました。

また、初めて実施した監査(運輸会社のシステム監査)では協会主催のシステム監査実践セミナーの受講や赤本が非常に役立ったとのお話をいただき、近畿支部のセミナーグループの一員として、システム監査体験セミナー等の推進に向けて意を強くした次第です。

以上

2013.10

注目情報（2013.9～2013.10）　※各サイトのデータやコンテンツは個別に利用条件を確認してください。

■ＩＰＡ（独立行政法人情報処理推進機構）

インターネットサービス利用時の情報公開範囲の設定に注意！（2013.10.1）

http://www.ipa.go.jp/security/txt/2013/10outline.html

■ＩＰＡ（独立行政法人情報処理推進機構）

組織における内部不正防止ガイドラインを公開（2013.9.4）

http://www.ipa.go.jp/security/fy24/reports/insider/index.html

■ＮＩＳＣ（内閣官房情報セキュリティセンター）

情報セキュリティ国際キャンペーン実施中（2013.10～2013.11）

http://www.nisc.go.jp/security-site/campaign/index.html

■ＮＩＳＣ（内閣官房情報セキュリティセンター）

国民を守る情報セキュリティサイト（広報：初心者向け、スマートフォン利用者向け、家庭向け、会社向け等）

http://www.nisc.go.jp/security-site/index.html

■警察庁

平成 25 年上半期のサイバー犯罪の検挙状況等について（2013.9.25）

http://www.npa.go.jp/cyber/statics/h25/pdf01-1.pdf

■総務省

スマートフォン安心安全強化戦略の概要（2013.9）

http://www.soumu.go.jp/main_content/000247676.pdf

■ＮＩＣＴ（独立行政法人 情報通信研究機構）

nicter の大規模ダークネット観測網によって観測された通信（ダークネットトラフィック）の一部をリアルタイムに視覚化（Web でリアルタイム提供）

http://www.nicter.jp/nw_public/scripts/index.php#nicter

■トレンドマイクロ

勤務先における業務ファイル共有実態調査（2013.9.17）

http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20130925063001.html?cm_re=articles-_-press-_-1380090599

■日経ＢＰ

スルガ銀-IBM 裁判控訴審、第一審より減額（2013.9.26）

http://itpro.nikkeibp.co.jp/article/NEWS/20130926/507010/

以上

2013.10

【　協会主催イベント・セミナーのご案内　】

■月例研究会（東京）

第186回予定	日時:2013 年 10 月 22 日(火)18:30～20:30、 場所:機械振興会館 地下2階ホール		
	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を巡る動向	
	講演骨子	012 年 11 月に MCF(一般社団法人モバイル・コンテンツ・フォーラム)が発表した「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」について、その内容、策定の背景、発表後の状況等について解説します。また、アプリケーションによるプライバシー侵害の実態とアプリケーション提供者、業界、関連する行政や団体等の取り組みについて、国内外の事例や動向も含めて俯瞰します。	
	講師	寺田 眞治 氏　一般社団法人モバイル・コンテンツ・フォーラム 常務理事 (株式会社オプト 中国・韓国事業推進室 プロジェクトマネージャ、 北京欧扶特信息科術有限公司 董事長、香港オプト 董事長)	
	お申し込み	HPからお願いします。(http://www.saaj.or.jp/kenkyu/kenkyukai186.html)	
第 187 回予定		日時:2013 年 11 月 18 日(月)18:30～20:30 テーマ:新 COSO について	※詳細は HP でご案内します。 場所:機械振興会館 (都合により 12 月分を 11 月に開催)
第 188 回予定		日時:2013 年 11 月 28 日(木)18:30～20:30 テーマ:共通フレーム 2013 について	

■事例に学ぶ課題解決セミナー（東京）

第12回予定	日時:2013 年 12 月 7 日(土)13:00～17:00、 場所:晴海グランドホテル	
	概要	・実際の事故事例をもとに未然防止策のポイントを学びます。 ・事例講義と簡易演習でそれぞれ異なる事例を用います。 ※詳細および募集要項は HP でお知らせします。
開催方法		・年 4 回の定期開催ですが、企業様などへの出張セミナーも常時受け付けています。

■公認システム監査人特別認定講習（東京・大阪）

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

■中堅企業向け「６ヶ月で構築するＰＭＳ」セミナー（東京）

申し込み常時受付中	概要	個人情報保護監査研究会著作の規程、様式を用いて、6 ヶ月でPMSを構築するためのセミナーを開催します。 詳細をHPでご案内しています。(http://www.saaj.or.jp/shibu/kojin.html)
	基本コース	月 1 回(第 3 水曜日)14 時～17 時(3 時間)×6 ヶ月 ※他に、月 2 回の応用コースなどがあります。
	料金	9 万円/1 名～(1 社 3 名以上割引あり)
	会場	日本システム監査人協会 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)

■「事例に学ぶシステム監査の基本と応用」半日コース（大阪）

日時:2013 年 11 月 16 日(土)13:00～17:00、 場所:大阪市　常翔学園 大阪センター	
概要	・経験豊富な監査人による監査事例から学ぶ監査の基本・応用です。 （内部監査実施における課題解決に役立てて下さい） ・情報システム監査に関心を持たれる方や、実際に監査関連業務に携わっている皆様に、監査実施の場面における課題やその解決について、経験豊富な監査人が事例講演をします。 ・ITコーディネータの方には、ITコーディネータ知識ポイントが　1ポイント付与されます。
お申し込み	HPでご案内中(http://www.saaj.or.jp/shibu/kinki/jirei20131116.html)

■西日本支部合同研究会開催（金沢）

日時:2013 年 11 月 23 日(土)13:00～17:00、 場所:金沢市　IT ビジネスプラザ武蔵　6F　交流室1	
概要	・経営活動を支える情報システム環境のシステム監査に対する社会の期待、ニーズに呼応し、システム監査の普及促進について考察、議論ができればと考えております。 ・IT コーディネータ実践力ポイント[4 時間 1 ポイント(上限無し)]が付与されます。
お申し込み	HPでご案内中(http://www.saaj.or.jp/shibu/hokushinetsu/nishi_godo_kenkyu2013.html)

■システム監査サービス（全国）

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

【　外部のイベント・セミナーのご案内（会報担当収集分）】

■日本セキュリティ・マネジメント学会　第 26 回学術講演会

日時、場所	2013 年 11 月 26 日(火)13:30～17:40(開場 13:00) 東京電機大学　千住キャンパス　1 号館 2 階 1205-1206 教室
テーマ	SNS のセキュリティとマネジメント
詳細、申し込み先	http://www.jssm.net/jssm/jssm05_2013.htm

■青山学院大学大学院　第 8 回公開シンポジウム

日時、場所	2013 年 12 月 21 日(土)14:00～17:30(開場 13:30) 青山学院大学　青山キャンパス 17 号館　6 階　本多記念国際会議場
テーマ	メディアが問う　わが国の会計および監査の課題
詳細、申し込み先	http://www.aoyama.ac.jp/sp/info/event/2013/01466/

以上

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

今号から 3 か月間は「システム監査の未来」がテーマです。このテーマで会報記事を募るとともに魅力ある編集を行ってまいります。テーマの詳しいご説明を今号では巻頭記事に掲載いたしました。皆様から様々なご意見ご提案を会報に寄せていただき、会報がシステム監査を活性化する議論の場となれば幸いです。

□■ 2. 会報の記事に直接コメントを投稿できます。

会報の記事は、

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

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

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

など、環境により、様々な利用方法をされていらっしゃるようです。

もっと突っ込んだ、便利な利用法はご存知でしょうか。気にいった記事があったら、直接、その場所にコメントを記入できます。著者、投稿者と意見交換できます。コメント記入、投稿は、気になった記事の下部コメント欄に直接入力し、投稿ボランをクリックするだけです。動画でも紹介しますので、参考にしてください。

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

□■ 3. 会員の皆様からの投稿を募集しております。

分類は次の通りです。

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

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

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

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

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

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）
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━