特定非営利活動法人
日本システム監査人協会報

2014年5月号
No 158

No. 158（2014年5月号）＜4月20日発行＞

芽吹きや新緑が日ごとに目に映え、自然のパワーを強く感じます。

システム監査のパワーも、根強く芽や枝を広げています。

巻頭言

テーマ：　情報化社会のためのシステム監査

会員番号 0557　仲　厚吉　（会長）

現在のペーパーマネーとグローバルな世界では、組織は生き残るため、変化に応じた組織改革と、状況把握のための高度な情報収集が必要になります。システム監査人は、「CLICK, CHANGE or DIE」の理解、即ち、インターネットの時代に、「インターネットから情報をクリック、ダウンロードし、そして利用し変化しなければ、死あるのみ」を、肝に銘じて考え行動する必要があると思います。今こそ、情報化社会のためのシステム監査が求められる時代になっていると思います。

＜目次＞

今年 4 月

2014.04

めだか　【　システム監査と業務監査　】　　（情報化社会のためのシステム監査）

改めて話題にしたい。システム監査と業務監査が、それぞれ並立している現状に、どの程度の必然性があるだろうか。今後も有意な区分として残るだろうか。そもそも、システム監査のテリトリーをどのように表現すればよいだろう。情報システムの信頼性や安全性・有効性などに関すること、という説明で十分だろうか。もう少し丁寧に、ハードウエア・ソフトウエア・ネットワークなどで構成する装置や機器と、それを開発・運用する業務処理と、そこで扱う情報や知識やドキュメントまで、と説明すれば足りるだろうか。いずれも違うと言わざるを得ない。

会報テーマ「情報化社会のためのシステム監査」を考えるとき、システム監査の作業範囲や、システム監査人が着眼する範囲はどこまでか、これは、システム監査の目的と役割に関する極めて重要なことだろう。

情報システムは、組織の業務処理、ビジネスプロセス、災害対策、経営情報、リスク、ガバナンス、コンプライアンスなど、事業のあらゆる範囲に及んでいる。消費者活動や社会制度も含めて、情報システムに支えられて運営されている。これは、今や縷々述べることではなくなっている。そして、経営監査、監査役監査、会計監査、税務監査、医療監査など、監査の分野は多々あるが、それらが対象にする業務は、すべて情報システムによって構成され実現されている。社会的責任や説明責任もまた、情報システムなしには成し遂げられない。

一方で、例えば、企業等における内部監査組織では、監査部の中にシステム監査室があったり、監査部員が業務監査担当とシステム監査担当に分かれていたりする。このような分担の場合、システム監査のテリトリーはどこからどこまでなのだろうか。正直疑問がある。システム監査自身が自らの役割を狭めてはいないだろうか。

経緯は別にして、現在のシステム監査には、経営の内部統制機能や、ビジネス部門などの業務処理プロセスの問題点洗い出しも、その役割として課せられている（システム監査技術者試験）。情報システムが、経営方針や戦略目標や組織目的を実現するための監査が求められている（システム監査基準）。このような引き合いを出すまでもなく、組織内の全部署の、現場から経営層の隅々まで、情報システムの利活用の状況を点検するのが、システム監査テリトリーだ。利活用の状況とは日常業務そのものになる。例えば、情報セキュリティ管理にしても、外部委託先管理にしても、業務監査とシステム監査で分けていては、弊害こそあれメリットはない。

現在いくつかの組織にある、業務監査とシステム監査の区分は撤廃すべきではないか。直ちに撤廃すべきであると思う。業務監査とシステム監査を、体制もノウハウも完全に融合させれば、組織内監査に新たなパワーが創出される。経営に貢献する監査力が増強する。システム監査には、営業支援から不正防止まで広範囲の課題解決力があることも、余り知られていなかった。一体化と融合で、システム監査はその役割をさらに発揮することができるだろう。

情報化社会では、システム監査のテリトリーは、あらゆる組織・制度・分野に及ぶとするのがごく自然だ。それが、情報化社会におけるシステム監査のファンダメンタルだと思う。

（山の彼方）

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

2014.04

投稿　【　情報化社会の大きなうねりとシステム監査　】

会報テーマ「情報化社会のためのシステム監査」を受けて

会員番号　1143　中山　孝明

情報化社会に生じている一つの側面に関心を持っている。これをうねりとタイトルしているが、具体的には組込みシステムの動向についてだ。会報テーマを受けて、このうねりとシステム監査とのかかわり合いを考える。情報化社会の大きなうねりに対して、システム監査はどのように対処すべきかについて。

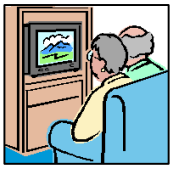
うねりを一つの側面と書き出したが、これは間もなく正面になるか、既に正面に来ている存在と思う。先ずは、この組込みシステムの動静を再確認し理解を深めることが、システム監査にとって重要なことと考える。

周知のことだが、大分以前から、組込みシステムはシステム監査の主題の一つになっている。システム監査技術者試験制度の対象者像・役割・技術水準・シラバスでは、5年前(2009年)から組込みシステムに関するスキルを求めている。同時に、エンベデッドシステムスペシャリスト試験の対象が、組込みシステムと明確に表現され、応用情報技術者、ITストラジスト、プロジェクトマネージャほかの資格においても、組込みシステムが明示されている。システム監査技術者試験の午後Ⅱ問題では、この時期から組込みシステムが登場している。

書き出しで側面と表現したのは、システム監査人の実態感覚とのギャップを勝手に推察していることもある。我が身の浅学を脇に置くが(ご教授願いたい趣旨も含めて)、組込みシステムに対する意識や経験の度合いをおもんぱかった。組込みシステムをテーマにしたシステム監査事例を耳にせず、組込みシステムの監査手法を論じたものも目にしていないこともある。

ところで、現況、組込みシステムは情報化社会の中でどのような位置づけであろうか。テレビやエアコンなど家電だけでなく、特に自動車への応用が顕著であることは広く知られている。

システム監査において、情報システムリスクを考える重要なポイントに、外部/内部環境の変動要因がある。組込みシステムの現況と方向性を見定めるとき、このシステム監査の視点を当てはめると分かってくることも多い。この点から組込みシステムそのものに関するリスク要素を3点考える。

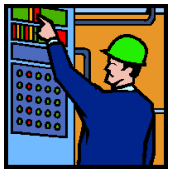


1点目は、ネットワーク接続だ。

つい最近までスタンドアロンであった家電が、今や当たり前にネット接続機器となり、テレビやゲーム機などがネット接続で日常的に使用されている。ゲーム機からの情報漏えい事故が大きな問題になった事例もある。ビジネスでも複合機がネット接続され、その意識の薄い使用者の複合機から情報漏えい事故が発生した事例もある。

2点目は、普及のスピードと範囲だ。

特定の機器だけでなく、一般に普及している身の回りのほとんどが電子機器となり、ソフトウエアで動作している。人は機器の指示に従い行動を委ねている。果たして、財産的な損害や人体への被害が発生していないと言えるのだろうか。ライフラインのシステムにも当然組み込まれているだろうが、その具体的な位置と内容が見えないのが歯がゆい。



3点目は、ネット攻撃の昨今の状況だ。

ネット接続されているものは、常に外的脅威にさらされている。例えば、ネットバンキングへの悪巧みのテクニックには

驚くばかりで、収束の気配さえ感じられない。一般社会に広く根付きつつある組込みシステムの防御策には、大いに関心がある。

続いて、組込みシステムに起きている最近の事例について、システム監査の観点で考える。　（表1）

・コンピュータでエンジンとモーターを制御	・電子部品が増え制御ソフトの不具合が見つけにくい
・部品の品質管理が追い付かなかった	・コスト削減のため複数車種で部品を共通化
・変速機を制御するプログラム	・一つの共通部品の故障が影響する範囲が大きい
・電気を流す装置に必要以上の電気を流したミス	・座席に人がいても空席と認識してしまう
・燃費性能を高めるためのシステムが一段と複雑	・パワーステアリングが突然作動しなくなる可能性

この表は、本年3月と4月の新聞記事（※1）から、組込みシステムに起因すると思われる事象を、筆者理解でリストアップした。これは自動車のリコール記事で、A社車種は8万台、B社車種は99万台（輸出分を含め190万台）、C社車種は105万台、外国D社車種は175万台と追加150万台のリコールであった。いずれも今年2月～3月の発表分で、記事では「リコール続出」「大型リコール続く」とタイトルしている。

表1は、組込みシステムの品質問題、つまりソフトウエアのバグと認識して間違いないだろう。この内容と規模は、自動車業界にとどまらず、情報システムにかかわる者全体の、情報化社会の構造的問題としてとらえるべきと考える。表1は、表面に出た事象であって、解決すべき課題は、背後で行われているソフトウエア開発作業のなかにあることは自明のことと思う。

表1の事象を、システム監査の立場で見透かせば、たちまち多くのチェック項目・点検個所が思いつく。これらは、従来からのソフトウエア開発・運用の全工程（SLCP：Software Life Cycle Process）における管理事項および、そこから生じてくるものとまったく同様だ。何ら変わらないことが良くわかる。もちろん、組込みシステムには特有の性質もあるので、その一端を気付く範囲で挙げてみる。　拙い理解レベルは一笑に付して欲しい。　（表2）

・動作するOSが様々	・顧客嗜好を反映した複雑なロジックで構成
・ソフトウエア言語が様々	・コンピュータではない機械のなかで動作
・デバッグはハードウエアの動作と一体検証が必要	・開発標準は一部の先進企業が策定
・新製品の常でコストと開発期間が優先される	・監査など第三者検証は今後の課題

組込みシステムの品質問題は、特に信頼性/安全性/機密性に意を払う必要があると思うが、その内部点検にしろ、第三者検証にしろ、システム監査人からみて、さほどのハードルがあるとは思えない。要件定義からソフトウエア仕様まで確定や、ソフトウエアテストから運用テストと評価までの工程などは、どのようなシステムでも管理項目や留意点は共通している。必要な手順と作業は省略してはならない。システム監査もまた、現在用いている基準・指針や点検手法の大部分がそのまま適用可能だ。併せて、組込みシステム関係の公開資料もいくつかある（一例※2）。

さらに深掘りして、組込みシステムがもたらす、うねりに関するリスク要素を2点考える。

1点目のうねりは、組込みシステムの用途と役割だ。

決して新しいものではないが、認識を超える速度で利用範囲を広げており、我々には常に目あたらしく耳あたらしく映る。一般企業等の業務システムに組込みシステムが行き渡るのは今後か、あるいは既にか。自動車産業のほかにも、工場やプラントなどが主要業務の場合には、組込みシステムが経営の根幹を支えていると言ってもいいだろう。改札の料金誤計算のニュースを耳にすれば、入

出力装置の部品（組込みシステム）を予想するし、金融やネットやエネルギー業界など、情報システムが装置産業においては、そのうねり（波及もインパクト）も大きく速いものと思う。

2点目のうねりは、組込みシステムの成長性だ。

情報化社会は、今後、組込みシステムが大きなポジションを占めていくだろう。従来のメインフレームやサーバによるシステムは、組込みシステムと一体的で機能する構成となり、システムの信頼性/安全性/有効性/機密性なども、組込みシステムとトータルで評価することになる。ハードウエアとソフトウエアという単純対比の用法ではなく、ハードウエアと一体となったアプリケーションというもの大きな存在になっていく。身の回りの装置・機械・器具・什器が、あたかも物理的に動作しているようで、その実はソフトウエアのロジックで動く。このような場所からも、システム監査人が扱う情報システムリスクの、新たな脅威と脆弱性が発生して来るに違いない。

本稿は、「情報化社会のためのシステム監査」という会報テーマに臨んで、情報化社会とはどのようなものかに思いを馳せた。組込みシステムの動向は以前からの関心事でもあった。組込みシステムには多くの長所や可能性があるからこそ利用が進んでいる。このような考えから本稿に至ったが、システム監査人の役割と目標について、その方向性の一つが自身のなかで明確になってきたと考えている。

情報システムリスクのあるところ即ちシステム監査の領域であり、システム監査はリスクに立ち向かう立場だ。だが、情報システムは敵ではなくパートナーであり、組込みシステムはそのパートナーの一人だ。

システム監査は、パートナーが懸念するリスクを進取果敢に追究し、パートナーとともに健全な情報化社会の実現を目指したい。

（※1）

読売新聞（2014.3.7、3.29、4.2の記事）、（注：本稿投稿の4.2以降もリコール記事の続報がされている）

（※2）

・エンベデッドシステムスペシャリスト試験のシラバス　http://www.jitec.ipa.go.jp/1_13download/syllabus_es_ver2_0.pdf

・組込みシステムの情報セキュリティガイド（METI）　http://www.chubu.meti.go.jp/technology_jyoho/sesaku/security.htm

・組込みソフトウエア産業実態調査（METI）　http://www.meti.go.jp/policy/mono_info_service/joho/2008software_resarch.html

・組込みスキル標準（IPA）　http://www.ipa.go.jp/sec/softwareengineering/std/etss.html#section2

・組込みシステムのセキュリティへの取り組みガイド（IPA）　https://www.ipa.go.jp/security/fy20/reports/emb_app/

以上

2014.04

投稿　【　情報化社会のためのシステム監査　】

会員番号　0557　仲　厚吉　（会長）

第13期通常総会で特別講演「リーマン・ショックに立ち向かうガバナンス - 新COSOの簡単な理解 - 米国中央政府のGreen Reportを中心として」を聴講しました。日本ITガバナンス協会会長でシステム監査学会会長でもある松尾明講師より、ITガバナンスの全般にわたる方向性について、分かり易くお話しを聞くことができました。講演の冒頭、講演の目的である新COSOの簡単な理解として、「CLICK, CHANGE or DIE」の理解、即ち、インターネットの時代には「インターネットから情報をクリック、ダウンロードし、そして利用し変化しなければ、死あるのみ」、これが新COSOの本質である、とのお話が印象的でした。

2008年9月15日に、米国の住宅バブルであるサブプライムローンの破綻からリーマン・ブラザーズ証券の倒産があって、それが引きがねとなり、リーマン・ショックが起きました。その後、5年を経過し、書店に、「リーマン・ショック　5年目の真実」という本が並ぶようになっています。当時から現在に至るまでの出来事を関係者へのインタビューで綴った本です。システム監査人には、是非、一読していただければと思います。この本は、「第1章　混沌の先　危機が世界を変えた」、「第2章　あの時」、「第3章　米国資本主義の変質」、「第4章　日本も揺れる」、「第5章　欧州が火種」、「第6章　新興国の台頭」、「第7章　危機は去ったか」から構成されていて、危機後の秩序は、まだ手探りであると、結論付けています。

リーマン・ショックは、なぜ起きたのか、「大激震」という本を読み返しました。「通貨は金や銀だから通用するのではない。需要と供給が均衡していれば価値を保ち流通する」ということから、1971年の米国による金ドル交換停止以後、いかなる物資にも裏づけられていないペーパーマネーの米ドルが、世界の基軸通貨として流通しています。通貨の供給に見合う需要をつくるために、投資対象を広げる必要があります。信用度の低い投資、例えば、低所得層への住宅ローン、いわゆるサブプライムローンが証券化され投資対象になりました。ハイリターン・ハイリスクの金融商品だから、ある段階までよく見えますが、サブプライムローンの返済が滞って破綻してしまいました。

現在のペーパーマネーとグローバルな世界では、組織は生き残るため、変化に応じた組織改革と、状況把握のための高度な情報収集が必要になります。システム監査人は、「CLICK, CHANGE or DIE」の理解、即ち、インターネットの時代に、「インターネットから情報をクリック、ダウンロードし、そして利用し変化しなければ、死あるのみ」を、肝に銘じて考え行動する必要があると思います。上記の特別講演では、米国中央政府が内部統制基準であるGreen Reportを公表したことが紹介されています。今こそ、情報化社会のためのシステム監査が求められる時代になっていると思います。

参考資料1:「リーマン・ショック　5年目の真実」 日本経済新聞社編、日本経済新聞出版社
参考資料2:「大激震」 堺屋太一著、実業乃日本社
参考資料3:http://www.gao.gov/assets/660/657383.pdf

以上

2014.04

【情報セキュリティ監査研究会だより その１３ ― プライバシー・バイ・デザイン 第８回】(連載)

会員番号 0056　藤野明夫(情報セキュリティ監査研究会)

はじめに

情報セキュリティ監査研究会では、アン・カブキアン著、「プライバシー・バイ・デザイン　プライバシー情報を守るための世界的新潮流」をテキスト(以下、左記の書を「テキスト」と称します)として、「プライバシー・バイ・デザイン」の意義、影響、PIAやシステム監査との関係などを議論しております。この概要を、2月21日に開催された日本システム監査人協会第13期総会の後の特別講演会において、「Privacy by Design　ご紹介と問題提起」と題して発表し、さらに会報4月号で報告いたしました。

これをもって「テキスト」解読を中心とした当研究会の活動の一応のまとめといたしましたが、本号では、その延長といたしまして、現在、経済産業省が中心となって推進している「ID連携トラストフレームワーク」をご紹介しようと思います。ID連携トラストフレームワークは、会報12月号で報告したFIM(連携アイデンティティ管理)の一つのインプリメント形態であり、プライバシー・バイ・デザインの一要素であります。今回のご紹介は、主に下記の参考資料1に基づいておりますが、皆様には会報12月号10、11ページを適宜、ご参照願います(会報は協会ホームページからダウンロードできます)。

なぜ、ここで、ID連携トラストフレームワークをご紹介するかというと、後述するように、この仕組みを実行する上で監査人が必須のプレイヤーになるからです。この仕組みに参加する事業者がID連携トラストフレームワークの保証レベル毎に満たすべき技術、運用面での監査要件を満たすかどうかを、監査人が監査し認定機関に報告します。認定機関は、この報告に基づいて当該事業者を認定します。この認定を得ることによって、当該事業者はこの仕組みへの参加が可能になります。以上のように監査人は、まさに「トラスト」を保証するキープレーヤーの役割を果たしますが、この仕事はシステム監査人にぴったりであります。これが会報4月号での当研究会報告の最後に記した、プライバシー・バイ・デザインはシステム監査人に新たな活躍の場を与える、という言明の一つの例になると考えます。

本報告は、情報セキュリティ監査研究会内部の検討結果であり、日本システム監査人協会の公式の見解ではないことをお断りしておきます。また、我々の力不足のため、誤りも多々あるかと存じます。お気づきの点がございましたら適宜ご指摘いただきたいと存じます。ご興味のある方は、毎月20日前後にSAAJ本部会議室(茅場町)で定例研究会を開催しておりますので是非ご参加ください。参加ご希望の方、また、ご意見やご質問は、下記アドレスまでメールでご連絡ください。 security ☆ saaj.jp （発信の際には“ ☆ ”を“@”に変換してください）

＜テキスト＞

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

＜参考資料1＞ 経済産業省「ID連携トラストフレームワーク概要」

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

＜参考資料2＞ ISO Guide 65

http://www.iajapan.nite.go.jp/asnite/pdf/pcg101_01.pdf

＜経済産業省「ID連携トラストフレームワーク」のホームページ＞

上記の参考資料1もこのホームページに掲載されております。

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

【報告】「ＩＤ連携トラストフレームワーク」ご紹介

１．ＩＤ連携トラストフレームワークが求められる理由

インターネットにはユーザIDが必要である。パスワードと一体になって本人確認を行うためである。ここでの問題は、ユーザIDは、サービス単位、少なくともサービスを提供する事業者単位に最低一つが必要になるため、インターネットサービスが普及するにしたがい、各利用者は、多数のユーザIDとそれと一体になったパスワードを管理しなければならないことである。参考資料1によれば、我々が記憶可能なユーザID・パスワードの組み合わせは平均3.15組、ユーザIDを使ってログオンするサイト数は平均19.4である。このため、利用者は、同一のユーザID・パスワードを複数のサイトで用いる傾向にある。万一、どこかのサイトでこれが漏えいした場合、さまざまなサイトに不正にアクセスされてしまう恐れがある。

一方、事業者は、利用者に対して、サービス提供に必要な種々の個人情報の入力を求めるが、これが正確か否かは、利用者の誠意にかかっている。もし、客観的に信頼できる情報を入手しようとすれば膨大なコストがかかる。

さらに、複数事業者間で連携しようとすると、利用者の信頼性のみでなく個々の事業者の信頼性も問題になる。

２．ＩＤ（アイデンティティ）と保証レベル

Webサイトや企業、病院等の公共サービス事業体等では、個人を識別し特徴づける情報（これを属性情報という）を管理することで、利用者を管理している。このような状況における「個人に関連する情報の集まり」をID（アイデンティティ：Identity）という。属性情報は、ユーザID、氏名、住所、メールアドレス、生年月日、性別、メールアドレス、学歴、所属、家族構成、購買履歴等々である。

ID（アイデンティティ）は、確からしさが問題になる。インターネットサービスは、この確からしさが保証されて初めて成り立つからである。しかし、その要求される確からしさの程度は、提供されるサービスによって異なる。ID連携トラストフレームワークでは、確からしさの保証を、提供されるサービスの内容に応じてレベル付けしている（表1参照）。

保証レベル	登録（個人の身元情報の登録）の基準	認証(当人であることの確認)の基準	発行方法	例
1	不要	パスワード(6桁以上)	Webサイトより発行、又は電子メール	SNSが提供する無料の旅行案内やグルメサイト名など
2	信用ある機関の登録情報の参照	パスワード(8桁以上)	登録住所へ郵送など	社員証による決済など
3	公的身分証明書	パスワード(8桁以上)とソフトウェアトークン(電子メールで送付した乱数の入力など)	電子メール送信と郵送を併用など	診療履歴を受け取るなど
4	対面での確認	ハードウエアによる認証(ハードウエアトークン)	手渡し、本人限定受取郵便など	

表1．保証レベル（LOA：Level Of Assurance）

３．ＩＤ連携トラストフレームワークの仕組み

ある事業者が管理しているユーザIDを、他の事業者のサービスでも使えるようにする仕組みが、「ID連携」である。トラストフレームワークを利用することで、ID連携がスムーズに行えるようになる。

「ID連携トラストフレームワーク」は、ID連携を行う事業者に求められる要件を明確にルール化し、第三者による認

証や、定期的な監査によって、事業者と、その事業者間のID連携の信頼性を担保することで、その構築コストの圧縮を図るとともに、利用者への透明性を担保するものである。

図1にトラストフレームワーク無のID連携を、図2にトラストフレームワーク有のID連携を示す。

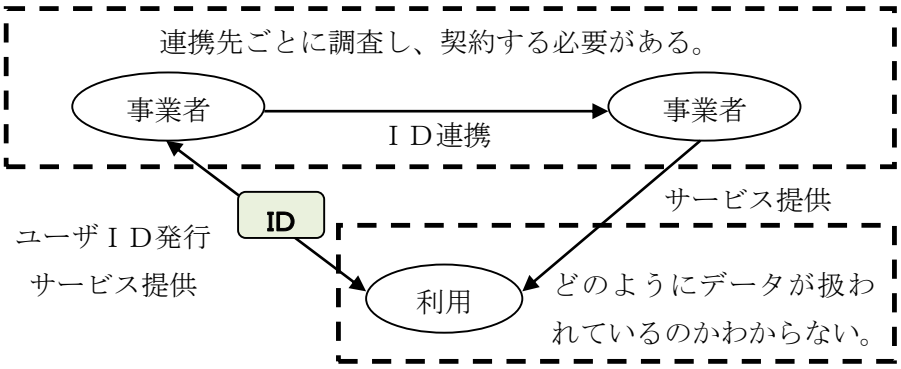


図1. トラストフレームワーク無のID連携

図1に示すように、現状では、事業者間でID連携をしようとすると、以下のような問題が生じる。まず、連携する事業者間で、個別に契約する必要がある。これでは、いつでも、誰でも繋げられるというインターネットの優れた特性を活かすことができない。つぎに、利用者からみると、事業者Aから事業者Bにどのようなデータが受け渡され、また、事業者Bがそれをどのように取り扱っているのかが分からない。かといって、利用者が事業者Bと個人情報の提供に関して利用目的の開示や同意といった個別のやり取りをするとすれば、事業者Bが直接、利用者から個人情報を取得するのと同じことで、そもそも事業者Aと事業者Bが連携する意味がない。

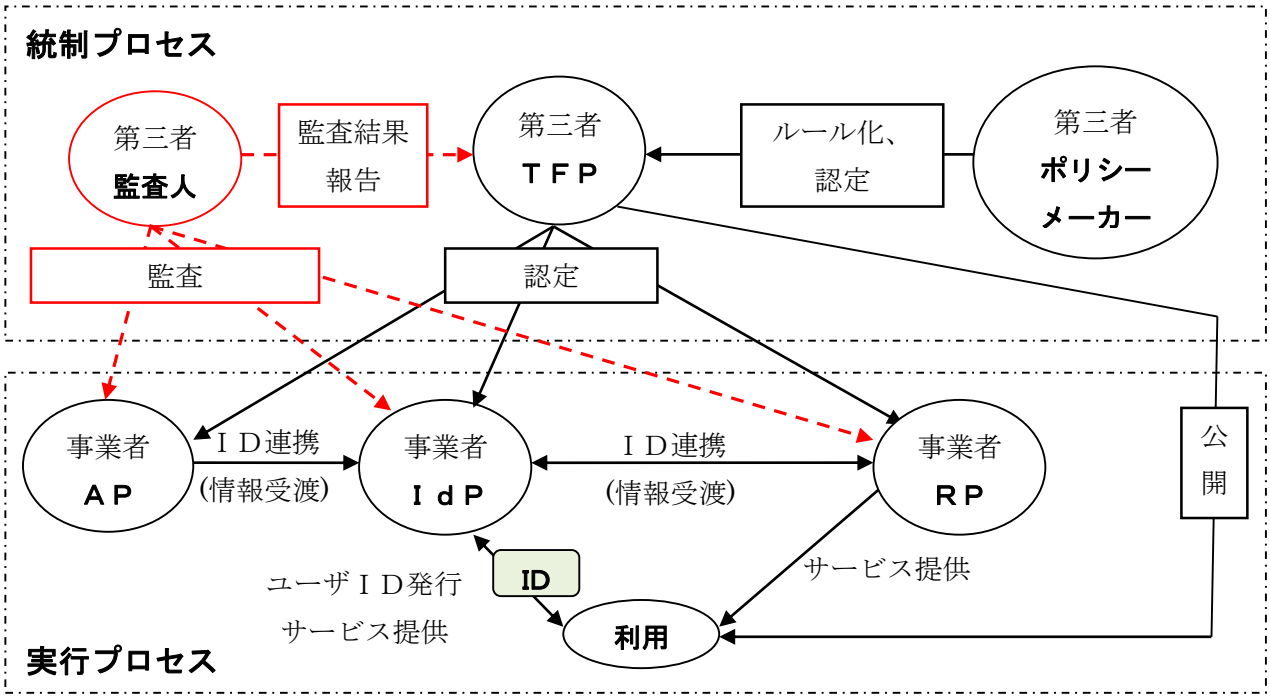


図2. トラストフレームワーク有のID連携

この問題を解決するために考え出されたのが、図2に示すトラストフレームワークによるID連携である。

以下、図2における各プレイヤーの役割を示すことにより、トラストフレームワークの機能を説明する。

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

① **ポリシーメーカー**:政府や業界

トラストフレームワークにおける要求事項やルール及びトラストフレームワーク・プロバイダの認定基準を策定する。これらの認定/認証業務は、ISO Guide 65(参考資料2参照)の基準に則して行われる。

② **TFP**(トラストフレームワーク・プロバイダ):第三者機関

ポリシーメーカーが策定したルールに基づき、保証レベル(LOA)を定義し、保証レベル毎に事業者が満たすべき技術、運用面での監査要件を作成する。

また、監査を行う監査人(アセッサー)を認定し、アセッサーの監査結果に基づき、事業者を認定する。

③ **監査人**(アセッサー)

トラストフレームワーク・プロバイダが作成した監査要件に基づき、参加事業者に対して監査を実施する。

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

① 利用者

サービスを受ける主体。自分自身を証明する情報を、認証する主体に渡す必要がある。

② **IdP**(アイデンティティ・プロバイダ)

利用者を認証する主体。保証レベルによって、IDの確からしさの確認を行う。

③ **RP**(リライング・パーティ)

IdPから、必要な属性情報***のみ***を受け取り、利用者にサービスを提供する。

④ **AP**(アトリビュート・プロバイダ)

利用者が求めるサービスを提供するにあたり、IdPが保有する属性情報だけでは足りない場合に、該当する属性情報を、IdPやRPに提供する。

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

4．おわりに

冒頭に記したように、この仕組みを運用する上で、監査人(アセッサー)が大きな役割を担っていることがお分かりいただけのではないか。各事業者を監査し、この仕組み全体が適正に運用されていることを保証するのが監査人の役割だからである。これあるがゆえに、利用者は、安心して自身のデータを提供できるのである。この監査人に求められる資質は、ITに通暁していること、個人のデータが活用される業務の内容を正しく理解する能力があること、そして、「監査」に関する専門的スキルと経験を持っていることである。

まさにシステム監査人にぴったりの仕事ではないだろうか。

今後、この連載のテーマのひとつとして、今回、ご紹介したID連携トラストフレームワークのようなプライバシー・バイ・デザインをめぐるインプリメントレベルでの新たな動向をご紹介し、できれば、そのなかでシステム監査人の新たな活躍の場を検討していきたいと思う。

以上

2014.04

【　システム監査基準研究会　】

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

○IT-ＡｕｄｉｔのＩＳＯ化について

先月に引き続き、9/24(火)の CSA フォーラムにおいて報告しました ISO30120(IT-Audit)についての資料の一部を紹介します。

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

5.2.1 監査プログラムの概観　（要約: 仮々訳）（続き）

プリンシプル-6　人的行動 ITに関する方針、実践及び決定は、「プロセスに関わる人々」の現状及び進化するニーズをふくむ、人的要素を尊重すること。
プロセス 1. IT活動が、識別された人的行動についての一貫性を評価するプロセス 2. 人的行動に関係するITリスクが管理できていることを評価するためのプロセス
プロダクツ 1.　人的行動に関するポリシーと手順 2.　教育とトレーニング 3.　人的行動に関する報告書

Human Behaviour Principle: IT policies, practices and decisions demonstrate respect for Human Behaviour, including the current and evolving need of all the 'people in the process'.
Process: ➢ The process for ensuring that IT activities are consistent with identified Human Behaviours. ➢ The process for ensuring that IT risks identified related to human behaviours are managed.
Product: ➢ The policies and procedures for Human Behaviour. ➢ The education and training. ➢ The report for human behaviour.

2014.04

「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 24 章

会員番号：1790　吉谷尚雄（個人情報保護監査研究会）

第24章　マネジメントシステムの統合化

24.1　マネジメントシステム規格（MSS 規格：Management System Standard)

個人情報保護マネジメントシステム（JIS Q15001:2006）では、「マネジメントシステム規格の正当性及び作成に関する指針」（ISO Guide 72:2001）に基づき、他のマネジメントシステム規格との構造の整合性に配慮するよう求めています。

また、2012 年 5 月 1 日には、ISO/IEC Directives（専門業務用指針）の「統合版 ISO 補足指針」として、マネジメントシステムの統合化のための「MSS 共通テキスト」が取りまとめられました。

※ご参考（一般財団法人日本規格協会）：http://www.jsa.or.jp/itn/pdf/shiryo/iso_supplement_sl234.pdf

24.2　統合マニュアルを作成する場合の基本事項

マネジメントシステムの統合化では、「3.4.5 教育」、「3.5.2 文書管理」、「3.5.3 記録の管理」、「3.7.2 監査」、「3.8 是正処置及び予防処置」、「3.9 事業者の代表者による見直し」の統合を主眼として行うことをお勧めします。共通項目として実施することで、従業者にとっても、理解しやすく年間スケジュール、研修講師、内部監査員の手配についても、高いパフォーマンスを得られる結果となります。

24. 3　統合マニュアルの構造

ＰＭＳにおける、1．適用範囲～　3.4.4 個人情報に関する本人の権利、までは、ＰＭＳ個別のマニュアルとします。保護対象である個人情報の特定、リスク分析については個別の要求事項に従うためです。ここでは、「統合版 ISO 補足指針」、JISQ27001:2014(**ISO27001:2013**)を参考に、個人情報保護マネジメントシステム（**PMS**）を含める場合の事例をご紹介します。

PMS:3.4.5　教育　(ISO27001:2013：7.2 力量)

事業者は、次の事項を行う。

a) 事業者の PMS／その他 MS に関連する業務を行う従業者に必要な、力量を決定する。
b) 従業者が、適切な教育、訓練、経験に基づいて、力量を備えることを確実にする。
c) 該当する（教育対象）には必ず、必要な力量を身につけるための処置をとり、処置の有効性を評価する。
d) 力量の証拠の情報は、文書化して保持する。

PMS:3.4.5　教育　(ISO27001:2013：7.3 認識)

事業者は、事業者の管理下で働く従業者に次の事項に関して認識を持たせる。

a) PMS／その他 MS 方針
b) PMS／その他 MS の有効性に対する自らの貢献
c) PMS／その他 MS 要求事項に適合しないことの意味

PMS:3.5.2 文書管理　(ISO27001:2013：7.5　文書化した情報、7.5.1 一般)

事業者の PMS／その他 MS には、次の事項を含める。

a) PMS／その他 MS の要求事項

b) PMS／その他 MS の有効性のために必要であると事業者が決定した事項

PMS:3.5.2 文書管理、3.5.3 記録の管理　(ISO27001:2013　7.5.2 作成及び更新)

文書化した情報を作成及び更新する際、事業者は、次の事項を確実にする。

a) 適切な識別及び記述　(例：タイトル、日付、作成者、参照番号)

b) 適切な形式　(例：言語、ソフトウエアの版、図表)　及び媒体(例：紙、電子媒体)

c) 適切性及び妥当性に関する、適切なレビュー及び承認

PMS: 3.5.2 文書管理、3.5.3 記録の管理 (ISO27001:2013　7.5.3 文書化した情報の管理)

文書化した情報の管理に当たって、事業者は、該当する場合には、必ず、次の行動に取り組む。

PMS／その他 MS の計画及び運用のために、事業者が必要と決定した外部からの情報は、必要に応じて特定し、管理する。

a)文書化した情報は、必要なときに入手可能かつ利用に適した状態に置く。

b)文書化した情報が十分に保護されている(例：機密性の喪失、不適切な使用及び完全性の喪失からの保護)

c)配付、アクセス、検索及び利用。

d)読み易さが保たれることを含む、保管及び保存。

e)変更の管理(例：版の管理)

f)保持及び廃棄

PMS:3.7.2 監査　(ISO27001:2013　9.2　内部監査)

事業者は、PMS／その他 MS が次の状況にあるか否かに関する情報を得るために、あらかじめ定められた開隔で内部監査を実施する。

a) PMS／その他 MS に対して事業者自体が決定した要求事項、及び規格が要求する要求事項に適合する。

b) 有効に実施され、維持されている。

c) 頻度、方法、責任及び計画に関する要求事項及び報告を含む、監査プログラムの計画、確立、実施及び維持されている。監査プログラムは、関連するプロセスの重要性及び前回までの監査の結果を考慮に入れる。

d) 各監査について、監査基準及び監査範囲を明確にする。

e) 監査プロセスの客観性及び公平性を確保する監査員を選定し、監査を実施する。

f) 監査の結果を関連する事業者の管理層に報告することを確実にする。

g) 監査プログラムの実施及び監査結果の証拠として、文書化した情報を保持する。

PMS:3.8 是正処置及び予防処置　(ISO27001:2013　10.1 不適合及び是正処置)

不適合が発生した場合、事業者は、次の事項を行う。

a) その不適合に対処し、該当する場合は次の事項を行う。

1) その不適合を管理し、修正するための処置をとる。

2) その不適合によって起こった結果に対処する。

b) 不適合が再発又は他のところで発生しないようにするため、次の事項によって、その不適合の原因を除去するための処置をとる必要性を評価する。

1) その不適合をレビューする。
2) その不適合の原因を明確にする。
3) 類似の不適合の有無、又は、それが発生する可能性を明確にする。

c) 必要な処置を実施する。
d) とった全ての是正処置の有効性をレビューする。
e) 必要な場合には、PMS／その他 MS の是正処置を行う。 是正処置は、検出された不適合のもつ影響に応じたものとする。
f) 不適合の性質及びとった処置の文書化した情報を保持する。
g) 是正処置の証拠として、文書化した情報を保持する。

PMS:3.9 事業者の代表者による見直し　(ISO27001:2013　9.3 マネジメントレビュー)

代表者は、事業者の PMS／その他 MS が、引き続き、適切、妥当かつ有効であることを確実にするために、あらかじめ定めた間隔で、PMS／その他 MS をレビューする。
マネジメントレビューは、次の事項を考慮する。

a) 前回までのマネジメントレビューの結果とった処置の状況
b) PMS／その他 MS に関連する外部及び内部の課題の変化
c) 次に示す傾向を含めた、PMS／その他 MS のパフォーマンスに関するフィードバック
1) 不適合及び是正処置
2) 監視及び測定の結果
3) 監査結果
4) 各目的の達成
d) 利害関係者からのフィードバック
e) リスクアセスメントの結果及びリスク対応計画の状況
f) 継続的改善の機会

事業者の代表者による見直しからのアウトプットには、継続的改善の機会、及び PMS／その他 MS のあらゆる変更の必要性に関する決定を含む。
事業者は、事業者の代表者による見直しの結果の証拠として、文書化した情報を保持する。

2015 年には個人情報保護法の改定が予定されています。ビッグデータに象徴されるパーソナルデータ利活用や、個人情報保護のグローバル化に対応する見直しに向けて、保護と活用の観点から、各法令の整備も行われます。マネジメントシステムの統合化による、パフォーマンス向上へのニーズはますます高まっていくことでしょう。

次回は、「第 25 章　システム管理基準　個人情報保護コントロール」をご紹介します。＞目次へ

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

2014.04

支部報告　【　北信越支部　2014 年度 北信越支部総会・研究会 報告　】

会員 No.1281　北信越支部 宮本 茂明

以下のとおり2014年度 北信越支部総会・研究報告会を開催しました.

・日時:2014 年 3 月 15 日(土) 13:00-17:00　　参加者:10 名

・会場:富山国際会議場(富山市)

・議題:

- ✧ 年度支部総会
  - ・ 2013 年度活動/会計報告
  - ・ 2014 年度活動/会計計画
- ✧ 本部総会報告
- ✧ 研究報告:

「金融サービスを巡る不正事案について ー外部委託管理に何が不足していたかー」

長谷部 久夫 氏

「プロジェクトマネジメントの今後について」

森 広志 氏

「ビッグデータ時代のプライバシー保護 -現状の課題-」

宮本 茂明 氏

◇研究報告 1

「金融サービスを巡る不正事案について ー外部委託管理に何が不足していたかー」

報告者（会員 No.1766　長谷部　久夫）

平成25年以降、金融機関が提供する利便性が高く、 広く活用されているサービスで以下の2つの重大な不正事案が発生している。

(1)インターネットバンキングによる不正送金事案

(2)ATM運用管理業務におけるお客さまカード情報の不正取得、預金の不正引出し事案

上記の2つの事案については、非対面で行われる取引チャネルで発生したこと、およびシステム運用管理業務を外部委託(インターネットバンキングは自営行有り)しているという共通点がある。これらの事案について発生状況、発生原因、および想定される対策を報告した。報告終了後、参加者とは根本的な発生原因等について意見交換させていただいた。

1. 金融機関における外部委託管理態勢

議論を深めるため、報告者が関与した金融機関の外部委託管理態勢について以下のとおり説明した。

(1)外部委託管理態勢

ア. 規程・基準

顧客保護等管理方針に基づき、業務を外部委託する場合における顧客情報や顧客への対応の管理に関する組織体制、役割、方法等を定め、外部委託管理の適切性を確保することを目的として規程・基準を整備している。

イ. 管理体制

上記の規程において外部委託管理責任者、外部委託管理部署、および外部委託担当部署を規定し、役割・責任を明確にしている。

(2)外部委託先の管理プロセス

ア. 外部委託先の選定・契約

イ. 外部委託先に対する日常的な管理・監督

ウ. 外部委託先の定期評価

エ. 外部委託先に対する監査

重要な外部委託業務においては、個人情報保護、およびセキュリティにかかる管理要件を規定する管理要件書等を整備し、契約上も義務づけている。管理要件書については、当局監督方針等に基づく現行プロセスの評価やトラブル再発防止策から不足項目を洗い上げ、継続的に整備に取り組んでいる。　また、管理要件の遵守状況等につき、再委託先以下を含め、立入り監査を実施し経営へ報告している。

2. 金融サービスを巡る不正事案

(1)インターネットバンキングによる不正送金事案

ア. 発生状況

利用者になりすましてインターネットバンキングで不正送金するといった犯罪による被害額は、平成 25 年は 14 億 600 百万円になり、平成 23 年の 3 億 800 万円、平成 24 年の 4,800 万円を大きく上回る。被害者の居住地は 47 都道府県に広がり、金融機関は 32 銀行にのぼっている。

攻撃手法は、利用者端末をウィルス感染させた上でログイン情報を盗んだり、正常に処理されているように見せかける「Man in the Browser」、更に「Man in the Middle」など、巧妙化している。

イ. 発生原因

(ア)セキュリティ対策の不足

インターネットバンキングに関するリスクの分析、セキュリティ対策の策定・実施、 効果検証、対策の評価・見直しといったPDCAが機能していなかった。利用者端末のウィルス等の不正プログラム対策は外部委託先・金融機関ともに管理不能とし、管理要件書上の役割があいまいだった。

(イ)利用者への説明、注意喚起の不足

インターネット上での暗証番号等の個人情報の詐取の危険性、および被害拡大の可能性など、様々なリスクについて利用者に対する説明、注意喚起が不足していた。

(ウ)外部機関との連携不足

不正事案の情報収集において、金融関係団体や金融情報システムセンター(FISC)の調査のほか、金融庁・日銀・警察当局からの情報を活用すべきだったが、取組みが不足し対応が後手に回った。

ウ. 想定される対策

(ア)セキュリティ対策の強化

利用者端末がウィルス感染した場合にも不正送金が行われないよう、①ワンタイムパスワード、②取引用ブラウザとは別の携帯電話等の機器を用いる取引認証の導入、③ウィルス感染状況を検知、警告を発するソフトの導入と、取引を遮断する対処、④セキュリティ対策ソフトの無償配布など、個人・法人等の利用者属性を勘案し、セキュリティ対策の強化に努める。

(イ)利用者への注意喚起

利用者に対して、①セキュリティ対策ソフトの導入、②パソコン OS 等を最新状態に更新、③各金融機関が導入し、推奨するセキュリティ対策の積極的な利用、④被害を最小限度に抑えるため、払戻し等の限度額をできるだけ低く設定すること等について注意喚起する。

(ウ)業界内での情報共有

不正な預金の払戻しにかかる被害内容や犯罪手口等を業界内で共有し、同様の手口による被害の未然防止・拡大防止に努める。

(2)ATM運用管理業務におけるお客さまカード情報の不正取得、預金の不正引出し事案

ア. 発生状況

某金融機関は、平成 26 年 2 月にカード偽造事件で逮捕された ATM システム委託先の元社員が昨年、キャッシュカード 80 口座、クレジットカード 52 口座の合計 132 口座の情報を不正取得し、カードを偽造したうえで数千万円(48 口座、合計約 2,400 万円)を引き出したと発表した。

上記の金融機関は、ATM 保守管理業務を外部委託し、委託先は保守管理業務を再委託していた。再委託先は関連会社に保守を再々委託しており、容疑者は再々委託先の元社員。

元社員はATM保守管理業務における解析作業を通じ、ATMを利用した顧客のカード情報を取得。その情報を元にキャッシュカード等を偽造し、顧客の口座から現金を引き出していた。

イ. 発生原因

(ア)口座番号、暗証番号のログ保存

ATM に蓄積された「解析用ログ」は口座番号と暗証番号を含んでいた。委託先が解析用ログをATMからサーバへ取込む際、および再々委託先へ MO ディスクで渡す際は暗号化していたが、再々委託先は復号しログ解析しており、口座番号と暗証番号を平文で参照可能だった。

(イ)業務権限の集中

容疑者一人にATM障害解析に関わる以下の業務権限が集中し、相互牽制が働かない体制だった。

a. ATM障害発生時の取引履歴の入手

b. 取引履歴の解析

c. ソフトウエア保守業務で使用する機器の管理 (＋カード発行)

ウ. 想定される対策

(ア)外部委託先における次のような業務の実施内容について、委託元としての点検を強化する。

(例) ①データの授受、②データの保管、③データの廃棄、④作業時間、作業場所の管理、
⑤鍵、カードの管理、⑥アクセス管理、⑦職務分離の実施、⑧ファイル管理、等

(イ)外部委託先の監査結果の報告を受けた場合、監査結果を分析・評価してフォローする。

(ウ)外部委託先が再委託(再々委託以下を含む)を行う場合は、契約書等の取決めに従って手続を行うとともに、委託元として再委託先以下の業務実施状況を把握する。

(エ)上記(ア)～(ウ)を適切に行うため、外部委託契約書、セキュリティ管理要件書、および個人情報管理要件書等を必要に応じて制改定する。また、ハードウエア保守業務等、形式上では外部委託契約が結ばれていなくとも、その実態において外部委託と同視しうるものを管理対象とする。

3. 不正事案の根本原因と今後の取組み

経営の非対面チャネルに対するリスク認識が甘く、最優先の経営課題と位置づけて取締役会等で必要な検討を行うなどの取組みが不足していた。このため、外部委託先との役割分担、監査権限、提供サービス水準等の取決めが不足し、顧客データの管理を監視、追跡できる態勢になっていなかった。また、リスク分析、セキュリティ対策の実施、効果検証、対策見直しのPDCAが機能していなかった。

今後、両事案を通じて認識した不備を改善し、外部委託管理態勢の強化に取り組む所存である。

◇研究報告 2

「プロジェクトマネジメントの今後について」

報告者（会員 No. 848　森　広志）

システム監査の効果を高めるため、日々進化を遂げるプロジェクトマネジメントを理解しておくことは重要と考えます。何より情報システムは、プロジェクトマネジメントの工程を経て生み出されるからです。

自分の認識しているプロジェクトマネジメントは、PMBOKを中心としたプロジェクトマネジメントプロセスと、企業体のシステム開発標準や、共通フレームの開発プロセス等のプロダクトプロセスをミックスさせたものですが、実際のシステム開発プロジェクトでは、納期や予算が重視されて、品質やリスク管理が後手に廻る事で、運用開始時に予期せぬエラーの出現など、対応に追われることもあると考えます。

システム開発プロジェクトの成功率（納期、予算、品質をベース）は約3割と言われます。この解決策に決まって登場するのがプロジェクトマネージャの早期育成です。重要テーマであり、他の模範となる優れた組織体の事例も多数ありますが、一般的な企業では、優秀なプロジェクトマネージャ（ITスキル標準4以上）の育成は早期とはいかず、多少とも時間を要すると考えます。（参考：全国台のプロジェクトマネージャ平均スキルレベル、3．4（出所：2011 年度調査レポート(iSFR)）また、プロジェクト要員やステークホルダーに加えて、組織体としてもプロジェクトマネジメントの理解に努めるのは、更に時間を要すると考えます。

情報サービス企業には、プロジェクト管理基準を整備されているところが多いと思いますが一般企業に於いても、プロジェクトマネージャ育成と共に、プロジェクト管理基準を策定する事がシステム開発プロジェクトの推進に重要であると考えます。今回は、プロジェクト管理基準を初めて作成する、あるいは改定する場合、プロジェクトマネジメントとしてPMBOK、プロダクトプロセスとして共通フレーム2013の活用を考えてみました。共通フレーム2013をプロジェクトマネジメントに活用という観点で考えると、プロジェクトプロセスとして、プロジェクト計画プロセスから測定プロセスまで8項目が整備され、組織のイネーブリングプロセスとして、プロジェクトポートフォリオ管理プロセス、人的資源管理プロセス、品質管理プロセスなど、8項目が整備されています。これらを活用する事でプロジェクトマネジメントプロセスの品質向上に繋がり、プロジェクトの成功に役立つと考えます。又、システム開発自体の付加価値創出の観点から、企画、要件定義に於ける要求品質の確保や、運用、保守を充実させ情報システムを育成する事で、使えるシステムを実現してゆく観点が盛り込まれており、今後は従来のプロジェクトマネジメント加え、システム開発の価値創造を考慮した、プロジェクトの推進を行ってゆく必要があると心得ました。

◇研究報告 3

「ビッグデータ時代のプライバシー保護 -現状の課題-」

報告者（会員 No. 1281　宮本　茂明）

2013 年 9 月新潟県例会で梶川明美様よりビッグデータの現状と方向性について報告をいただいた。今回は、報告の中にあったプライバシー保護の課題について、JR 東日本 Suica 乗降履歴データ外販の事例と、政府の「パーソナルデータに関する検討会」技術検討ワーキンググループの公開資料をもとに、技術面、制度面から課題詳細を確認してみた。

1. JR 東日本 Suica 乗降履歴データ外販事例

2013 年 7 月 JR 東日本はビッグデータ利活用ビジネスとして、Suica 乗降履歴データを外販したが、利用者に事前に周知しなかったことへの苦情や批判が寄せられたため、継続的なデータ提供を 7 月末に中止し、当面外販を見送ることになったとの報道があった。

このケースを見てみると、乗降履歴データ外販にあたっては、氏名や連絡先を除いており、個人を特定できない情報として販売していて、個人情報保護法に照らせば、個人情報に当たらないものであった。ただし、性別、生年月、乗降駅名、利用日時、鉄道利用額は販売されており、利用者への説明責任を果たすべきだったというものであった。

現在、JR 東日本では、除外要望のある顧客のデータについては社外販売のデータから除外する対応をとっている。

〈参考情報〉

・JR 東日本「Suica に関するデータの社外への提供について」2013 年 7 月 25 日

http://www.jreast.co.jp/press/2013/20130716.pdf

ビッグデータ利活用ビジネスのプライバシー保護においては、事前説明だけの問題でなく、技術的、制度的問題もある。この乗降履歴データ外販の課題が取り上げられた時期を同じくして、政府でもビッグデータ利活用に向けた「パーソナルデータに関する検討会」が開催され、乗降履歴の考察も含め、技術面、制度面から課題が検討された。

2.「パーソナルデータに関する検討会」技術検討ワーキンググループによる課題検討

2013 年 9 月から政府の IT 総合戦略本部にて、ビッグデータ利活用に向けた「パーソナルデータに関する検討会」が開催され、その技術検討ワーキンググループで匿名化技術に関する議論が行われている。

〈参考情報〉

・IT 総合戦略本部 「パーソナルデータに関する検討会」技術検討ワーキンググループ 2013 年

http://www.kantei.go.jp/jp/singi/it2/pd/index.html

このワーキンググループの公開資料から匿名化技術に関するポイントを整理した。

・「非個人情報」が高度な情報通信技術の活用により個人を識別することができる情報となる可能性

現行法の一般的な解釈では、個人情報取扱事業者がその保有する個人情報を、匿名化により特定の個人が識別される可能性が無い状態へ加工した場合「非個人情報」となり、現行法の規制の外で第三者への提供等が自由に行える。しかし、現行法制定時よりも照合対象の入手可能な情報が多く存在し、技術が進展したことにより、「容易照合性」の範囲が拡大し、他の情報と容易に照合して特定の個人を識別することができる可能性が高まっている。

技術検討ワーキンググループでの検討に当たって、「個人情報」等の用語について、下記のように整理して議論されている。

・「匿名化」:無名化、仮名化、属性削除、一般化、k-匿名化(同じレコードが複数存在し一意に個人(A さん)であることをも識別できないような状態にすること)

・「特定」:ある情報が誰の情報であるかが分かること

・「識別」:ある情報が誰か一人の情報であることが分かること

「特定」「識別」の定義を踏まえ、個人情報を加工することにより作成される情報を 3 つのカテゴリーに分類

- 識別特定情報(「個人情報」):個人が(識別されかつ)特定される状態の情報
  (それが誰か一人の情報であることがわかり、さらに、その一人が誰であるかがわかる情報)
- 識別非特定情報:一人ひとりは識別されるが、個人が特定されない状態の情報
  (それが誰か一人の情報であることがわかるが、その一人が誰であるかまではわからない情報)
- 非識別非特定情報:一人ひとりが識別されない(かつ個人が特定されない)状態の情報
  (それが誰の情報であるかがわからず、さらに、それが誰か一人の情報であることが分からない情報)

・乗降履歴による考察

鉄道の乗降履歴をサンプルデータとして、乗降履歴が個人と結びつけられる条件について検討されている。

- 氏名の削除を行い、個人を特定しうる属性情報を削除する一方で、仮名化により個人を識別できるようにし、その利用者の移動経路実績や他のサービスの利用履歴と照合可能な場合は、誰かは分からないにしてもその利用者の行動を捕捉できる恐れが残る。
- 直接個人を特定しうる情報を削除し、仮名化を行わない場合でも、利用者が一人しかいない経路がある場合、乗降記録からその利用者は識別される。
- 識別化の可能性を低減する方法として、乗降者数が少ない駅や乗降者数が少ない経路の情報を捨てることが考えられる。しかし一方で、経路情報を削除するなど識別化の困難性を高める措置を行うと、情報としての有用性が低下することとなる。

・個人が識別された事例

公開された「非個人情報」から、他の情報と照合して特定の個人を特定された米国の事例が報告されている。

- マサチューセッツ州が公開した医療データから州知事の情報が特定された。(1997 年米国)
- 米国インターネットサービス企業 AOL が研究目的で公表した検索履歴データからユーザが識別された。(2006 年米国)
- 映画レンタル・サービスの Netflix は映画推薦アルゴリズムコンテストのために匿名化したユーザの視聴履歴データをコンテスト参加者に提供したが、映画情報サイト IMDb(Internet Movie Database)で公開されているユーザレビューとを結びつけることで、一部の個人が特定された。(2006 年米国)

・インターネットに存在するアクセス可能な大量データと削除不可能な大量のコピーの存在

非特定化・非識別化技術を施された情報であっても、ある属性値から、インターネットに公開されている情報等を突き合わせることで個人が特定化されることがある。

- インターネットに公開されたデータを常時高速で巡回して複製を作っている。この結果、一度、流出した個人情報を削除するのは難しくなっている。
- 長期間にわたって収集・保持する情報から、個人の行動の特徴が明確になり、その特徴的な行動から個人の特定されるリスクは高まっている。
- Web 検索技術・サービスが進んでおり、ある情報に対して組み合わせるべき情報も容易に見つかるようになっている。
- 画像情報や映像情報そのものに個人に関わる多数の固有情報を含んでいる。
- テキストへのリンクについて、画像や映像には説明が付随していることが多く、例えば顔写真の場合、付随情報として氏名が記載されていることもある。
- 自動記録メタデータについて、デジタル画像、映像、音声ファイルの多くは、撮影時に位置情報や作成者、作成時間等のメタデータが自動的に生成され、画像データと同時に保管される。つまり画像データ単体で識別・特定が可能な場合が多い。

・技術面での課題のまとめ

- あらゆる情報について、識別非特定情報または非識別非特定情報への加工を実現する汎用的な技術・手法は存在しない

- 特定の情報について、識別非特定情報または非識別非特定情報への加工を実現する技術・手法の適否については、ケースバイケースで判断すべきである

匿名化の汎用技術がない状況において、ビッグデータ利活用を進めるには、パーソナルデータの利活用に関する制度面でのカバーが必要な状況にある。

3.「パーソナルデータの利活用に関する制度見直し方針」

「パーソナルデータに関する検討会」の検討結果を受け、2013 年 12 月政府の高度情報通信ネットワーク社会推進戦略本部により、「パーソナルデータの利活用に関する制度見直し方針」が提示され、2014 年 3 月には内閣官房にパーソナルデータ関連制度担当室が設置された。今後 2014 年 6 月を目途に大綱が決定・公表され、その後パブリックコメント、法案作成が行われ 2015 年 1 月の通常国会への法案提出が計画されている。

〈参考情報〉

・「パーソナルデータの利活用に関する制度見直し方針」2013 年 12 月 20 日
http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/dec131220-1.pdf

・パーソナルデータ関連制度担当室の設置について　2014 年 3 月 1 日　内閣官房
http://www.kantei.go.jp/jp/singi/it2/pd/info_h260301.html

- **パーソナルデータの利活用に関する制度見直しの方向性**
  - ビッグデータ時代におけるパーソナルデータ利活用に向けた見直し
  - プライバシー保護に対する個人の期待に応える見直し
  - グローバル化に対応する見直し

- **パーソナルデータの利活用に関する制度見直し事項**
  - 第三者機関（プライバシー・コミッショナー）の体制整備
  - 個人データを加工して個人が特定される可能性を低減したデータの個人情報及びプライバシー保護への影響に留意した取扱い
  - 国際的な調和を図るために必要な事項
  - プライバシー保護等に配慮した情報の利用・流通のために実現すべき事項

4. 今後の北信越支部での研究テーマ

ビッグデータ時代のプライバシー保護について今後引き続き以下の点について研究を進めていこうと考えている。

- パーソナルデータの利活用に関する制度見直しのフォローアップ
- プライバシーを守る IT サービス技術動向

以上

2014.04

支部報告　【　近畿支部第１４５回定例研究会報告　】

会員番号　1710　小河裕一　（近畿支部）

１．テーマ　：「中小企業におけるリスク認識の手法について」
～　JNSA 西日本支部 WG 活動を通じて　～

２．講師　　：富士通関西中部ネットテック株式会社
ＪＮＳＡ西日本支部　嶋倉　文裕氏

３．開催日時：2014 年 3 月 20 日（木）　18：30～20：30

４．開催場所：大阪大学中之島センター２階　講義室 201

５．講演概要　：

講師が JNSA（日本ネットワークセキュリティ協会）の西日本支部情報セキュリティチェックシート WG 活動におけるアウトプットをもとに、以下の事項に対して講演を頂いた。

○「第一次情報セキュリティチェックシート WG」での活動
○「出社してから退社するまでのリスク対策 WG(9to5 リスク WG)」での活動
○「第二次情報セキュリティチェックシート WG」での活動

「第一次情報セキュリティチェックシート WG」での成果

まず作成したチェックシートは以下のような特徴を持っていた。

・可用性を重視した作りとなっている。
・自らが対策を行うよりも「委託の積極的な活用」も取り込んだシートになっている。
・ISO/IEC2700 を絞り込み、システム管理基準も取り込んだ38項目のチェックシート。
（経営層向け　17項目、責任者・担当者向け　21項目）

アンケート形式でチェックリストの有用性を調査したところ、有用とした企業はごくわずかであった。
この原因として組織（中小企業）側のトラブル経験が無い（もしくはトラブルと思っていない）ためリスクを正しく認識している企業が非常に少ないためであるということが判明した。
このことから、まず「情報資産台帳の作成からリスクを認識してもらう」活動にシフトした。
しかし、ここでも「情報資産」と「固定資産」の区別がつかない企業もあり、ここからも「リスク認識につながらない」と判断した。

http://www.jnsa.org/result/2008/west/0812report.pdf

「出社してから退社するまでのリスク対策 WG(9to5 リスク WG)」での成果

資産の洗い出しからではリスク認識にはつながらない。
日常業務の中でヒューマンエラーを少なくする仕組みを考慮することで社員の意識向上とスキルアップを図った。
さらに IT 系と非 IT 系の業務と分類して洗い出した。この結果を手引書へとまとめた。

http://www.jnsa.org/result/2010/chusho_security_tebiki_110330.pdf

「第二次情報セキュリティチェックシート WG」

この WG での作業は情報セキュリティチェックシートと 9to5 手引書の紐付けであった。
チェックシートは ISMS ベースであり範囲が広く、また管理策からはトラブル事象に結びつきにくい状況であった。このため、手引書と結びつくことで対策を理解しやすくなる。
今回のセキュリティチェックシートは上位層と下位層に分割。
上位層はリスクとは関係なく、情報セキュリティ対策を持続的に行うためのフレームワークという位置づけ。
下位層は ISMS とシステム管理基準から抜粋したセキュリティ対策とシステム管理。
どんなトラブルが起きえるのか？や判断基準も追記している。
これらのチェックシートは自分たちの仕事のやり方に潜むリスクを認識して、現状を把握し
対策を検討する場合に使用できる。

６．所感

講師の嶋倉氏が JNSA の WG 活動で作成された集大成を発表いただきました。講義の中でも述べておられましたが、ISMS 等の管理策ではなかなかトラブル事象に結びつかないため中小企業だけでなくとも「セキュリティ」に対する実感が無く、対策までたどりつかないと思われます。
そんな中で「日常業務の流れ」と「管理策」を結びつけてチェックシートとして成果とされたことは、非常に有益な資料になったのではと想像できます。

次のステップとしては、会場から質問も出たが「いかに成果物を世間で認知してもらい幅広くセキュリティ対策のために使ってもらうことができるか」を考えてもらうことに違いありません。

今回聴講いただいた方々にも、一度成果である「チェックシート」を活用してみた上で周囲に広めていただきたいと考えております。

以上

2014.04

注目情報（2014.02～03）※各サイトのデータやコンテンツは個別に利用条件を確認してください。

■ 全府省庁等の参加による大規模な政府サイバー攻撃対処訓練を初実施

内閣官房情報セキュリティセンター（NISC）などが、2014 年 3 月 18 日に表題訓練の初実施を公表しています。

http://www.nisc.go.jp/active/kihon/pdf/318.pdf#search='%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E6%94%BB%E6%92%83%E8%A8%93%E7%B7%B4'（内閣府）

http://j-net21.smrj.go.jp/watch/news_tyus/entry/20140319-10.html（中小企業基盤整備機構）

■ 情報セキュリティ普及・啓発プログラム の改定の方向性について（案）

内閣官房情報セキュリティセンター（NISC）は、2014 年 3 月 14 日に表題資料とどなどを公開しています。

http://www.nisc.go.jp/conference/seisaku/jinzai_wg/

■ 労働者派遣法の改正

「労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律等の一部を改正する法律案」

厚労省が 2014 年 3 月 11 日に提出した法律案、要綱、条文などが公開されています。

http://www.mhlw.go.jp/topics/bukyoku/soumu/houritu/186.html

■ＩＰＡ：「2014 年 3 月の呼びかけ」、「2014 年 4 月の呼びかけ」

経営者・マネジメント層向け「 組織内部の不正行為にはトップダウンで、組織横断の取り組みを 」

～現状チェックと対策ポイントの見直しで効果的に内部不正を防止～

独立行政法人情報処理推進機構（IPA）は、2014 年に入り、金融機関や行政機関において業務に携わる者による情報窃取等の不正行為の報道を受けて、2013 年 3 月に公開した「組織における内部不正防止ガイドライン」をもとに内部不正を防止するための対策を説明しています。

http://www.ipa.go.jp/security/txt/2014/03outline.html

「あなたのパソコンは 4 月 9 日以降、大丈夫？」～ 使用中パソコンの判別方法、乗り換えプランを紹介 ～

マイクロソフト社 Windows XP と Office 2003 のサポートが 2014 年 4 月 9 日に終了したことを受けて、ご自身のパソコンがサポート終了の対象か否かの確認方法、および乗り換えの選択肢の紹介と、やむなくサポート終了後に Windows XP および Office 2003 を使い続ける場合の制限事項について解説しています。

http://www.ipa.go.jp/security/txt/2014/04outline.html

■ＪＩＰＤＥＣ： ISMS ユーザーズガイド JIS Q 27001:2014 対応の公開

一般財団法人日本情報経済社会推進協会（JIPDEC)は、 2014 年 3 月 20 日に発行された ISMS の要求事項である JIS Q 27001:2014 に対応した ISMS ユーザーズガイドを公開しました。(4月 14 日)

http://www.isms.jipdec.or.jp/JIP-ISMS111-30.html

2014.04

【　協会主催イベント・セミナーのご案内　】

■月例研究会（東京）

第190回	日時:2014 年 4 月 25 日(金)18:30～20:30　場所:機械振興会館　地下2階多目的ホール	
	テーマ	企業 IT 動向調査 2014(13 年度調査)～データで探るユーザ企業の IT 動向～
	講師	一般社団法人　日本情報システム・ユーザー協会(JUAS)　常務理事　浜田達夫氏
	講演骨子	JUAS は、経済産業省 商務情報政策局の監修を受け、「企業 IT 動向調査 2014」を実施いたしました(調査期間:2013 年 10 月～11 月)。1000 社の IT ユーザ企業の回答から、定点観測と重点テーマを通して IT 投資や IT 戦略方針など、世の中の動向を俯瞰していきます。
	お申し込み	ご案内とお申込み方法を HP でご案内しています。 (http://www.saaj.or.jp/kenkyu/kenkyukai190.html)
第191回	日時:2014 年 5 月 22 日(木)18:30～20:30　場所:機械振興会館　地下2階多目的ホール	
	テーマ	ISMSの最新動向(仮題)
	講師	一般財団法人　日本情報経済社会推進協会(JIPDEC)　センター長　高取敏夫氏
	講演骨子	詳細確定次第、HPでご案内いたします。
	お申し込み	

■システム監査実践セミナー（東京）

第26回	日時:2014 年 5 月 15 日(木)～16 日(金)＜日帰り 2 日間＞ 時間:両日 9:30～17:00　会場:　晴海グランドホテル(最寄り駅　都営地下鉄大江戸線勝どき駅)	
	概要	・システム監査人の実践能力の維持・向上のためのセミナーです。 ・ロールプレイを中心とした演習ベースのきわめて実践的なコースで、経営に役立つシステムの実現に資するシステム監査の方策を理解・修得することを目標にしております。 ・修了者には、当協会が認定する公認システム監査人(CSA)の認定に必要なシステム監査実務を、半年間経験したものとみなされます。
お申し込み		HPでご案内中です。 (http://www.saaj.or.jp/kenkyu/jissenseminar26.html)

■公認システム監査人特別認定講習（東京・大阪）

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

■中堅企業向け「６ヶ月で構築するＰＭＳ」セミナー（東京）

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

■システム監査サービス（全国）

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

2014.04

協会からのお知らせ【　新任理事・新任監事のご紹介　】

今年度新役員 8 名について、前号に引き続き、4 名の本部理事・監事の方をご紹介します。

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

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

会員番号 1697 大西 智（本部理事）

新任理事の大西智と申します。どうぞ宜しくお願いいたします。本年より、前任の畠中主査よりバトンタッチして頂き、システム監査事例研究会（以下、事例研）の主査を務めさせて頂いております。

当協会には、2008 年 4 月に入会させて頂きました。システム監査の実務経験がないため、同年 9 月、CSA フォーラム懇親会でご相談したところ、事例研参加を勧められ、翌月、システム監査普及サービスを通してシステム監査の実際を経験できる場としての事例研に、参加させて頂きました。事例研では、「事例に学ぶ課題解決セミナー」の立上げに参加させて頂き、中山副会長始め先輩メンバーの方よりご指導いただいて、（リスク[脅威・脆弱性]低減対策である）コントロールの不備（＝穴）の見える化としての観点から、システム監査について色々勉強させて頂きました。また、実践・実務セミナーでは、鈴木実理事より、講師の心構え・ノウハウ等をご教授頂き、三輪理事にはセミナー事務局運営についてご伝授頂いて、各セミナーの事務局並びに講師も務めさせて頂いております。

ここ数年、事例研としましては、システム監査普及サービスの受託がございません。是非受託し、実務経験のない方に、監査の実際を経験できる場を提供できるよう努めて参りたいと存じますので、ご協力の程、宜しくお願いいたします。

会員番号 2485 向後雅代（本部理事）

はじめまして、この度、理事に就任しました向後雅代です。

83年にNECに入社し、約13年間半導体系の事業部で生産管理及び制御系のSEをしていました。その時、情報システム監査を受査したことから、情報システム監査に興味を持ち、96年にシステム監査部門へ異動、システム監査技術者には、01年に合格しました。公認システム監査人は、昨年秋に取得しました。現在は、ルネサスエレクトロニクスの内部監査室でJ－SOXの評価者、情報セキュリティ監査を中心に内部監査全般を担当しています。情報システム監査領域に限らず、内部監査全般に関して勉強途中です。

また、趣味は、料理全般です、趣味がこうじて、栄養学や薬膳料理に興味を持ち、こちらの方も勉強中です。今春高校生になる一児の母であり、義母の介護と仕事や趣味以外でも忙しい日々を過ごしています。

理事の仕事は、どこまでできるかわかりませんが、みなさんの協力を得て、精一杯頑張らせて頂きます。よろしくお願いいたします。

会員番号　2461　佐々野未知（本部理事）

はじめまして。この度、新しく理事に就任しました佐々野ともうします。

私は、上智大学を卒業、専門職にあこがれて公認会計士をめざし、合格後は 1998 年から 4 年間を米国 NY の監査法人に勤務していました。4 年間というと思い当たる方もいらっしゃるかもしれませんが、2001 年に 9.11 を現地で経験し、自分の根本を見つめなおす機会となりました。その後日本に帰国し、2006 年に今の会社をたちあげ、コントロールソリューションズという会社で、リスク管理にまつわるコンサルティングサービスを提供しています。いくつかの現場を経験した中で、痛切に感じたのは、リスク管理の現場でもシステムを切り離して考えることはできない、ということです。自分と会社の発展のためには、サービスにシステムを組み込んでいくことが不可欠だと思い、システム監査人の資格を目指しました。今後は、協会の研修や人事交流を自らのスキルアップにつなげるとともに、理事として、システム監査人協会の発展に微力ながら貢献させていただきたく所存です。どうぞ皆様のご指導・ご鞭撻のほど、何卒よろしくお願い申し上げます。

会員番号　0148 木村裕一（監事）

富山監事の退任の後を受けました、新任監事の　木村裕一　です。

これまでは、月例研究会の担当理事として勤めてきました。

私の月例研究会への関わりは月例研究会の初めのころからで、20年以上かと思います。

現在研究会ビデオを配布していますが、研究会の内容が東京だけで消えてしまうのはもったいなく考えて、支部での活用を考えて私が最初個人持ちのビデオカメラで始めたことです。それ故ビデオを支部で活用していただけていることは、うれしく感じるところです。長い間、皆さんにご協力いただいてやってこれました。感謝いたします。ありがとうございました。

しかし、あまり長い担当はマンネリ化することで、よろしくないと思い、また負担が重いこともあり、このあたりで月例研究会をやり方から内容から刷新をするべきとも思い、理事を退任することにしました。理事の退任の代わりとして監事をおおせつかったわけです。よろしくお願いいたします。

2014.04

協会からのお知らせ　【　新入法人会員紹介　】

会員番号　6066　早川淳一　（法人部会）

フレクサス・セブンは、ITガバナンスの構築・IT戦略の立案からITマネジメントの実践を中心に、企業のIT推進に対してトータルな支援を行うコンサルティング会社です。メンバーはビッグファーム系出身のコンサルタントが中心です。

まだ「システム監査」という形での実務経験は少ないですが、ITプロジェクト評価、ITプロジェクトアセスメントというサービスを通して、システム監査に近い業務経験は豊富に持っております。今後は、システム監査としての視点を持ちつつ、より良いサービスが提供できるように、システム監査人協会の中で勉強し、また日本におけるシステム監査の充実に向けて微力でも貢献できたらと考えておりますので、どうぞよろしくお願いいたします。

（株）Flexas Seven フレクサス・セブン　http://www.flexasseven.com/

2014.04

新たに会員になられた方々へ

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

・協会活動全般がご覧いただけます。 http://www.saaj.or.jp/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
・皆様の情報の変更方法です。 http://www.saaj.or.jp/members/henkou.html

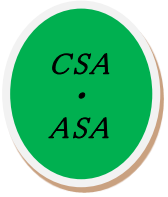
・会員割引や各種ご案内、優遇などがあります。 http://www.saaj.or.jp/nyukai/index.html
　セミナーやイベント等の開催の都度ご案内しているものもあります。

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

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

・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。



・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

・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

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

2014.04

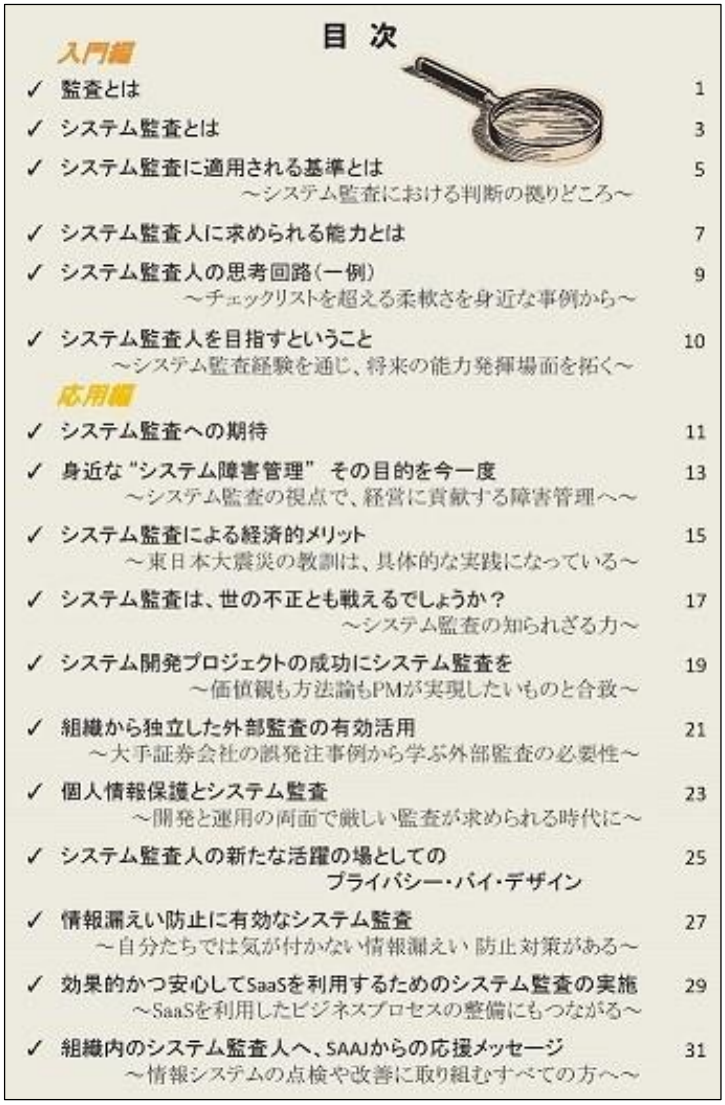
協会からのお知らせ【「システム監査を知るための小冊子」発行について】広くご活用下さい

会員番号　6005　斉藤　茂雄　（法人部会）

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

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

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


目　次

入門編

応用編

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

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

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

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

以上

2014. 04

【　協会行事一覧　】

2013 年	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
10 月	10 日　会計:9 月末予算実績対比表の理事会報告	22 日　第 186 回月例研究会	
11 月	14 日　理事会:次期会長選任 14 日　予算申請提出依頼(11/30〆切) 16 日　2014 年度役員改選準備開始 20 日　会費未納者除名通知発送 30 日　会計:2014 年度予算申請提出期限	16 日　認定委員会:CSA 面接 18 日　第 187 回月例研究会 20 日　認定委員会:CSA・ASA 更新手続案内〔申請期間 1/1～1/31〕 21 日　CSA フォーラム 28 日　第 188 回月例研究会 28 日　認定委員会:CSA 面接結果通知	16 日　近畿支部:「事例に学ぶシステム監査の基本と応用」 23 日　北信越支部:西日本支部合同研究会 28-29 日　東北支部:支部設立 10 周年記念システム監査実践セミナー
12 月	1日　会計:2014 年度予算案策定 12 日　理事会:2014 年度予算案、会費未納者除名承認 13 日　会計:支部会計報告依頼(1/11〆切) 14 日　事務局:第 13 期通常総会資料提出依頼(1/8〆切) 20 日　会計:2013 年度経費提出期限 27 日　事務局:2014 年度会費請求書・寄附願い発送準備〔1月1日付〕	7 日　事例研:「課題解決セミナー」 9 日　認定委員会:更新手続きのご案内メール発信 11 日　CSA 認定証発送	6 日　北海道支部:支部総会 14 日　東北支部:支部総会・支部設立 10 周年記念講演会
2014 年	**理事会・事務局・会計**	**認定委員会・部会・研究会**	**支部・特別催事**
1 月	9 日　理事会:通常総会議案審議 10 日　総会開催案内掲示・メール配信 10 日　役員改選公示 15 日　事務局:総会資料(〆) 20 日　会計:2013 年度決算案 25 日　会計:2013 年度会計監査 31 日　償却資産税・消費税	認定委員会:CSA・ASA 更新申請受付〔申請期間 1/1～1/31〕 20 日　認定委員会:春期公認システム監査人募集　案内〔申請期間 2/1～3/31〕	11 日　会計:支部会計報告期限 17 日　近畿支部:支部総会
2 月	6 日　理事会:通常総会議案承認 21日　通常総会・特別講演	CSA・ASA 春期募集(2/1～3/31) 1-2 日　事例研:第 23 回システム監査実務セミナー(前半)、22-23 日(後半) 5 日　CSA フォーラム 10 日　第 189 回月例研究会	
3 月	1 日　事務局:法務局登記、東京都への事業報告、変更届提出	1 日　事例研:第 13 回課題解決セミナー 25日　CSA フォーラム	
4 月	1 日　認定 NPO 法人申請準備開始	認定委員会:新規 CSA/ASA 書類審査 25 日　第 190 回月例研究会	20 日　2014 年春期情報技術者試験
5 月	8 日　理事会	認定委員会:新規 CSA/ASA 面接 15-16 日　事例研:第 26 回システム監査実践セミナー 22 日　第 191 回月例研究会	
6 月	12 日　理事会 末日　支部会計報告依頼(〆切 7/14) 末日　助成金配賦額決定(支部別会員数)	7 日　事例研:第 14 回課題解決セミナー 10 日　新規 CSA/ASA 承認	28 日　近畿支部:システム監査体験セミナー(入門編)
7 月	1 日　会費未納者督促状発送 初旬　支部助成金支給 10 日　理事会	1 日　認定委員会: 秋期公認システム監査人募集　案内〔申請期間 8/1～9/30〕	14 日　支部会計報告〆切
8 月	(理事会休会) 会費督促電話作業(役員) 中旬　中間期会計監査	秋期公認システム監査人募集 8/1～9/30	30 日～31 日　近畿支部:システム監査体験セミナー(実践編)
9 月	11 日　理事会	6 日　事例研:第 15 回課題解決セミナー	

※注　定例行事予定の一部は省略。

2014.04

会報編集部からのお知らせ

1. 会報テーマについて
2. 会報記事への直接投稿(コメント)の方法
3. 投稿記事募集

□■ 1． 会報テーマについて

2014 年度の年間テーマは、「○○○のためのシステム監査」とし、四半期ごとに「○○○のための」について具体的なテーマを設定して、システム監査に関する皆様からのご意見ご提案を募集しています。

今号(5月号)から7月号までの3か月間のテーマは、「情報化社会のためのシステム監査」です。情報化社会の発展とシステム監査とのかかわりについて、皆様からの幅広いご意見をお待ちしています。

過去2月号から4月号までのテーマは、「公(おおやけ)のためのシステム監査」でした。ご投稿いただいた様々なご意見ご提案、ありがとうございました。

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

□■ 2． 会報の記事に直接コメントを投稿できます。

会報の記事は、

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

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

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

など、環境により、様々な利用方法をされていらっしゃるようです。

もっと突っ込んだ、便利な利用法はご存知でしょうか。気に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(毎月メール配信)を利用してください)
2. 会員投稿　(Word の投稿用テンプレート(毎月メール配信)を利用してください)
3. 会報投稿論文 (論文投稿規程があります)

いつでも募集しています。 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します。なお、会報部会の編集権で、表現の訂正や削除を求め、又は応募を受け付けないことがあります。また、裁量の範囲で字体やレイアウトなどの変更をさせていただくことがあります。

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）

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

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

会員限定記事

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

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

■発行： NPO 法人　日本システム監査人協会　会報編集部
〒103-0025　東京都中央区日本橋茅場町2－8－8共同ビル6F
■ご質問は、下記のお問い合わせフォームよりお願いします。
【お問い合わせ】 http://www.saaj.or.jp/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━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
編集委員： 藤澤博、安部晃生、久保木孝明、越野雅晴、桜井由美子、中山孝明、藤野明夫
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）
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━