特定非営利活動法人
日本システム監査人協会報

2014年6月号
No 159

No. 159（2014年6月号）＜5月20日発行＞

さわやかな初夏の季節がやって来ました。
外に出て、新鮮な空気をおなか一杯に
吸い込んで、鋭気を養いましょう。

長安寺　五百羅漢（箱根仙石原）

巻頭言

テーマ:IT時代に重要な人のインテグリティを補強する仕組み

会員番号 6027 小野修一(副会長)

現在の社会は、IT および IT システムなしには機能しない社会になっています。IT システムが社会の隅々にまで普及し、それは、我々の仕事や生活に大きな恩恵を与えてくれています。今後も、新しい IT、IT システムが我々の未来を変えてくれることでしょう。

しかし、IT がいかに進歩・発展しても、それを使うのは人です。したがって、IT を使いこなすための人のインテグリティが強く求められます。インテグリティとは、完全無欠な状態ということです。IT を使いこなすための知識、モラル、問題への対処能力などが人に十分に備わっていなければ、IT を使いこなせないどころか、過ちを起こし、それが事故に繋がってしまう危険性があります。

しかし、100%完全無欠な人はいません。インテグリティを高める努力を怠ってはいけませんが、人は知識不足、経験不足などから、過ちを起こしてしまいます。そのことを前提に、IT システムには人の不完全な行動をコントロールする仕組みが必要です。

どのようなケースで人は過ちを起こしやすいのかを過去の事例などを参考に整理し、過ちを起こさない、または過ちを起こしても事故につながらない効果的なコントロールの仕組みを提案することも、システム監査人の重要な役割だと思います。

＜目次＞

2014.04 撮影　犬山城

2014.05 投稿

めだか【　システム監査を何のために行うのか？
（情報化社会のためのシステム監査）　】

「あなたは、何のためにシステム監査を行っているのですか？」と問われて、皆さんならどう答えるでしょうか？

最近、P. F. ドラッカー著『現代の経営』(注)の中にある三人の石工の話を読んで、「何のためにシステム監査を行うのか？」について、考えさせられた。この三人の石工の話とは、次のようなものである。

（注）P. F. ドラッカー著『マネジメント』にも、同様の話がある。

＊＊＊＊＊＊＊＊＊＊

ある人が工事現場の脇を通りかかり、汗を流して働いている数人の石工に、「何をしているのか」と問いかけました。

一人目の人は、こう答えました。「これで食べている」と。

二人目は、手を休めずに答えました。「国で一番腕のいい石工の仕事をしている」と。

最後の一人は、目を輝かせて答えました。「教会を建てている」と。

―上田惇生監修・佐藤等編著『実践するドラッカー[思考編]』より引用―

＊＊＊＊＊＊＊＊＊＊

この石工の話を、システム監査人にあてはめると、システム監査を行う目的・動機としては、以下が考えられる。

① 自分の生計を立てるために、監査を行っている

② レベルの高い監査を目指して監査を行っている

③ 監査対象組織のため、社会のために監査を行っている

どれも間違っているわけではない。ドラッカーも、各人各様の目的・動機を持つことは認めている。だが、組織としての成果を出す「マネジメントの人間」は、第三の男だとドラッカーはいう。

三つのケースを個別に考えてみよう。

①の目的・動機には、「自分」しかない。そうした目的で監査しても、システム監査の品質は考慮されず、単に「こなすだけの監査」に陥ってしまう。

②の目的・動機をもった監査人は、「レベルの高い監査」という目標をもって監査にあたるため、①の監査人に比べると、より良い成果を出せそうである。しかし、「レベルの高い監査」がどうあるべきかの視点が適切でないと、結果として「監査対象組織の為にならない監査」に陥る危険性もある。たとえば、多くの指摘をあげることに力点がいってしまい、監査対象組織にとって対応優先度の低い指摘ばかりを並べてしまうような対応は頂けない。

③の目的・動機には、①②のシステム監査人にはなかった「監査対象組織のため」「社会のため」というシステム監査の品質を評価するための視点がある。「監査対象組織のため」とは、監査対象組織の問題点・課題を見つけ、その解決の方策を考えてあげることであり、「社会のため」とは、そうした監査対象組織の改善への対応を通して、情報化社会への健全な発展に寄与することといえるであろう。

こうして、3つの目的・動機を比べてみると、③の目的・動機で監査するのが当然だという気になるのだが、これまで、①②の監査に流されることはなかったと言い切れない思いも残る。

①②の監査に陥らないために、初心に返って、「監査対象組織・情報化社会への貢献」を意識して監査にあたることが重要であると、三人の石工の話を読んで、改めて感じた次第である。

（やじろべえ）

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

＜目次＞

2014.05

めだか　【　5 月のカレンダー　】　　（情報化社会のためのシステム監査）

5 月のカレンダーの挿し絵や写真には、田植え風景や新緑の山など、季節の人々の営みや自然の遷り変わりを用いているものが多い。

今月、忍野八海近くの山に登り、左右の麓まで遮るもののない富士、手の届きそうな富士を眺めながら、5 月の色と匂いを感じて来た。スミレの群生、マメザクラのトンネル、ミツバツツジ、自生のボケなどの彩りとともに、木々の新芽も薄緑・濃い緑・薄赤など様々な形容を見せていて、日頃使われていなかった我が身の五感のどこかが呼び覚まされたような気がしている。この季節は山全体がパワースポットになっていると思う。色の華やかさよりもそれをもたらしているものに、ただならない力強さや迫力のようなものを感じた。自然現象は季節や一定のサイクルで繰り返しつつ、我々にも分かる形でパワーを見せている。繰り返すこと自体のパワー、変化を遂げるパワー、目的達成のパワーがある。特に 5 月のカレンダーには、そのような出現・創造を感じるものがある。

（前段とは、無理な脈絡というよりは、それはそれとして）

情報化社会の進展は、繰り返しつつの変化ではなく、従前のものを陳腐化させて常に新たな形を創造している。より効率的・生産的・コストダウンを追及し変化するのは至極合理的なことで、この傾向はさらに速くなるに違いない。注目すべき顕著な現象は、ロジック（論理による仕組み）が影響力を強めていることだろう。情報化社会は、これまでも物理的な行為をロジックに置き換えてきている。例えば、証券取引所から立ち合いがなくなり、株式取引はかなり前からアルゴリズムロジック売買が中心で、まばたきの間に入出力も値決めも終わってしまう取引が延々と続く、まったく手の届かない世界になっている。

負の面では、止まることのないウイルス攻撃やフィッシング詐欺など、これらへの対応はあたかも必要経費のごとき様相を呈しており、最近では、IE(インターネット・エクスプローラー)の欠陥や、3D プリンタ拳銃のニュースなど、ロジック社会の怖さを突きつけられている。これまでは、ネットから離脱や遮断をすれば怖い面には合わないと思っていたが、これも3D プリンタ拳銃でいとも簡単に無力となってしまった。

情報化社会が進む方向は多様だが、その歩みは人間の営みの自然な姿であろうし、我々が求めているものの結実であるはずだ。一つハッキリと言えることは、情報化社会の負の面がさらに多様化していることだ。30 年前の IT 社会には負の面はなかったと思う。負の面は、有用なものを本来目的から逸脱（悪用）することから発生する。これは、物事の成熟に伴い自ずと付随するもので、ある意味で歴史は繰り返すと同じかもしれない。

そんな中で、システム監査は目先の変化に惑わされず、骨太の立ち位置から揺るがないことが重要だ。時々発生するインシデントなどに左右されず、根幹にあるガバナンスにこそ着目すべきだ。情報化社会がどのような形を創り上げようとも、人間が創り上げていることに着目することが、システム監査の骨太の立ち位置であると思う。システム監査の対象は情報システムそのものよりも、そこで行われている人間の行為、つまりガバナンス行為だと考えている。

（山の彼方）

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

＜目次＞

2014.5

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）

賢い人は「勘定」と「感情」の二つの視点を持っている。これは、公認会計士の山田真哉氏（『さおだけ屋はなぜ潰れないのか?』の著者）が最近の講演会で話していた言葉です。また、夏目漱石は「草枕」で、“智に働けば角が立つ。情に掉させば流される。意地を通せば窮屈だ。とかくに人の世は住みにくい。”と書いています（岩波文庫）。システム監査人は、この二つの視点、つまり、システム管理基準に照らして不備や不十分を指摘する視点と、それを被監査部門が納得感を持って聞くことができる説明を行うための視点を、うまく使い分けて監査に当る必要があると思います。

第190回月例研究会で「企業IT動向調査2014（13年度調査）～データで探るユーザー企業のIT動向～」を聴講し、一般社団法人日本情報システム・ユーザー協会常務理事である浜田達夫講師より、情報システム・ユーザー企業のIT動向について、分かり易くお話しを聞くことができました。私にとって、印象的であったのは、従業員1000人以上の大企業では、IT戦略策定と戦略実行の役割分担が進むと予測されるということです。情報システムの維持・管理はもちろん重要な役割ですが、こちらはアウトソーシングしても、IT部門の時間をより戦略策定に割けるようにするとみられる傾向があらわれてきています。

最近、話題になっている「ビッグデータ」の活用は、一般消費者向けビジネスに取り組むBtoC企業を中心に導入が始まっているものの、まだまだ、導入する目的の明確化や人材の育成が課題となっています。しかしながら、IT部門の時間をより戦略策定に割けるようにするという傾向から、IT部門は、戦略策定を行うため、ビジネスデータを分析する役割を担うようになることは間違いないと思います。

システム監査人として、「ビッグデータ」活用のための情報システム導入の目的の明確化や人材の育成とは何かということに関心を持ち参考資料を探したところ、「データサイエンティスト養成読本」という書籍がありました。同書には、人材の育成という点で一般社団法人データサイエンティスト協会がスキルの標準化とキャリア形成のために活動を始めているという記事があります。

ビジネスデータの活用は、例えば、消費者が商品（モノ）の購入に当たって買いたいモノに欠品が無くまた不良在庫が無いよう在庫を勘定すること、それに会員制を追加して、会員（ヒト）のためにお得感に訴えるサービスを提供し購買を継続するよう分析を図っています。インターネットでグローバルの時代になり、Web通販等が普及しビジネスデータが膨大な量になったことが、「ビッグデータ」の活用につながっています。IT部門がビジネスデータの分析者としての役割を期待される時代になり、システム監査人にも、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きていると思います。

参考資料：「データサイエンティスト養成読本
ビッグデータ時代のビジネスを支えるデータ分析力が身につく！」 技術評論社

＜目次＞

2014.05

【情報セキュリティ監査研究会だより その１４ ― プライバシー・バイ・デザイン 第９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。

3月と4月に開催した定例の研究会で、今後の研究テーマについて検討した結果、引き続き、「プライバシー・バイ・デザイン」をテーマに研究を続けることになりました。全体の概要は一段落しましたので、今後は、そのなかの個別の要素についてやや深く検討していくことにいたしました。当面は、FIM(連携アイデンティティ管理)、そのなかでもトラストフレームワーク、次にPIA(プライバシー影響評価)を取り上げる予定です。トラストフレームワークについては、既に概要を会報5月号でご紹介いたしましたが、今回は事例を二つご紹介したいと思います。

ひとつは、日本における先行事例、学術連携フェデレーション「学認」、もうひとつは、米国の行政サービスに係る本格的な取り組みである、Identity Credential and Access Management、“ICAM”です。両者とも、主に資料1と資料2を参考にしております。紙数の関係で詳しいご紹介ができません。「学認」についてさらに詳しくお知りになりたい方は、参考ホームページに記載いたしました学認ホームページをご参照ください。また、ID連携トラストフレームワーク全般につきましては、同じく経済産業省の該当のホームページをご参照ください。

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

＜資料１＞ 経済産業省「ID連携トラストフレームワーク概要」
http://www.meti.go.jp/policy/it_policy/id_renkei/tf_gaiyou.pdf

＜資料２＞ 2014 年 3 月 14 日開催、経済産業省主催シンポジウム「アイデンティティ連携が生み出す社会」資料
http://www.meti.go.jp/policy/it_policy/id_renkei/0314symposium.pdf

＜資料３＞ ISO Guide 65
http://www.iajapan.nite.go.jp/asnite/pdf/pcg101_01.pdf

＜資料４＞ ICAM 「Trust Framework Provider Adoption Process」
http://www.idmanagement.gov/sites/default/files/documents/FICAM_TFS_TFPAP_0.pdf

＜参考ホームページ＞

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

【報告】「ＩＤ連携トラストフレームワーク」ご紹介その２

１．ＩＤ連携トラストフレームワークの概要

事例のご紹介の前に、今回、初めてご覧になる方のために、ID連携トラストフレームワーク（以降、「トラストフレームワーク」）を再度、ご紹介する。この部分は、会報2014年5月号(158号)の記事の抜粋であり、既に、ご欄になった方は飛ばしていただきたい。

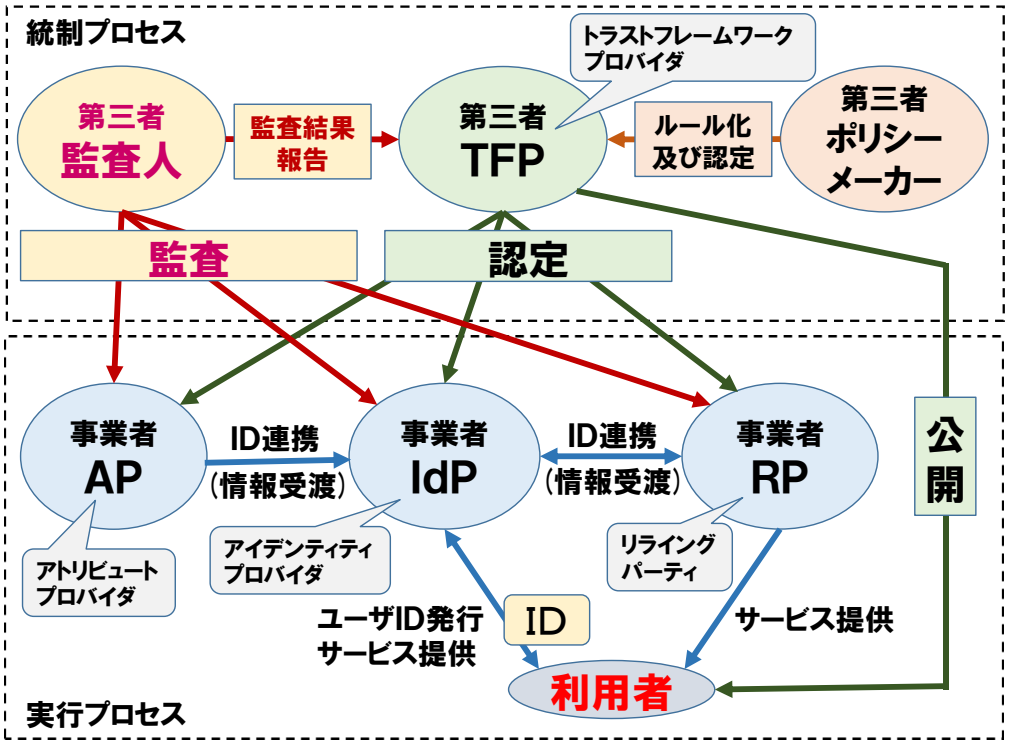


図1. トラストフレームワークによるID連携のイメージ

図1に、トラストフレームワークによるID連携のイメージを示す。各プレイヤーの役割の紹介を通じて、トラストフレームワークの機能を説明する。

（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(資料3)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。

2．トラストフレームワーク事例：学術連携フェデレーション「学認」

全国の大学等と国立情報科学研究所(NII)が連携して、「学術認証フェデレーション(学認:GakuNin)」の構築及び運用が2009年度から開始された。学術認証フェデレーション(以下、「学認」)とは、学術e-リソースを利用する大学等と学術e-リソースを提供する機関・出版社等から構成された連合体のことである。

学認はトラストフレームワーク・プロバイダである。各大学、工業高等専門学校等がアイデンティティ・プロバイダになる。また、リライング・パーティ(学認のホームページでは、サービスプロバイダ(SP)という言葉を用いている)は、出版社、学会等である。2014年1月14日より学認の運用はNIIの事業として行うことになった。

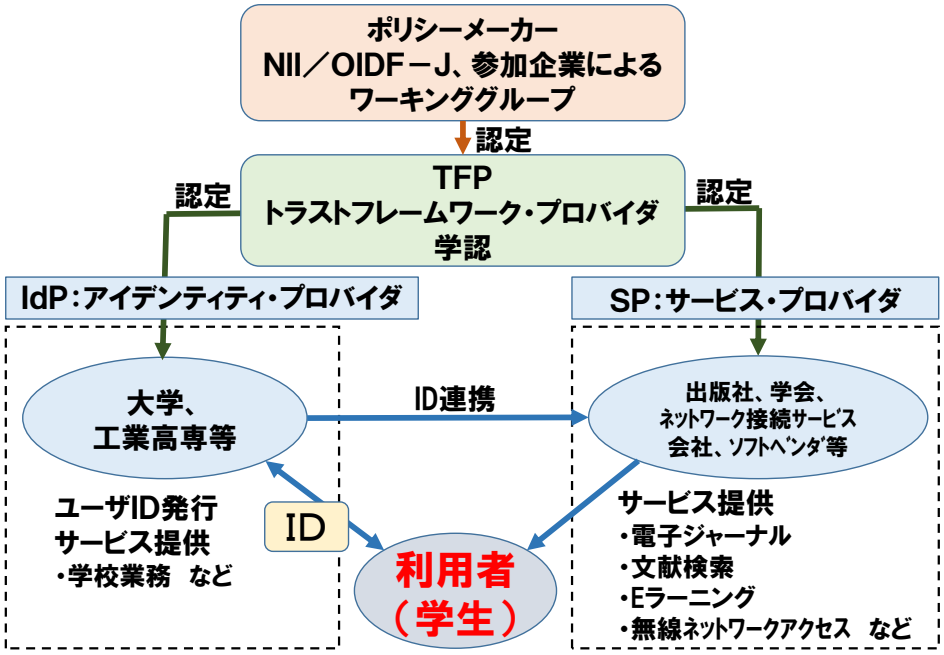


図2．学術認証フェデレーション「学認」

ポリシーメーカーは、NII、OpenIDファウンデーション・ジャパン(OIDF－J)及び参加企業によるワーキンググループである。TFP(トラストフレームワーク・プロバイダ)は、学認、IdP(アイデンティティ・プロバイダ)は、大学、工業高専等、SP(サービス・プロバイダ)は、出版社、学会、ネットワーク接続サービス会社、ソフトベンダ等である。SPが提供するサービスの内容は、コンテンツ系サービスとして、電子ジャーナル、機関リポジトリ、文献検索、論文・業績

情報管理、開発環境(ソフトウェア)等、基盤系サービスとして、無線ネットワークアクセス、Eﾗｰﾆﾝｸﾞ、テレビ会議、メーリングリスト、クラウド環境等である。

2014年2月末現在で、SPは120組織、IdPは119機関、利用者数はID数で90万に達している。なお、文部科学省によれば、高等教育人口は350万人、うち8割が学生である。すでに学認の利用者は結構な割合を占めている。

３．トラストフレームワーク事例：米国政府における取組み「ＩＣＡＭ」

ICAM(Identity, Credential, and Access Management)とは、民間企業が提供し、市民が別の目的で所有している認証手段を、米国政府が利活用するために定められた認定の仕組み(＝トラストフレームワーク)である。既に使われている民間のアイデンティティ・プロバイダの発行したユーザIDを使って、行政サービスを受けられることを目指している。図3にOIX(Open Identity Exchange)がTFPの役割を担っているトラストフレームワークの事例を示す。

この事例では、例えば、Googleの発行したユーザIDを用いて、米国連邦政府機関である国立衛生研究所が提供するPubMed(日本を含む世界約80カ国で発行される生物医学系文献の検索サイト)等のｻｰﾋﾞｽへのアクセスが可能になる。

なお、ICAMは、OIXの他にkantara Initiative、In Common等の複数のTFPを認定している。ICAMは、TFPAP（Trust Framework Provider Adoption Process）（資料4）に従って民間のTFPを評価・認定する。認定を受けたTFPがIdPの評価・認定を行う。

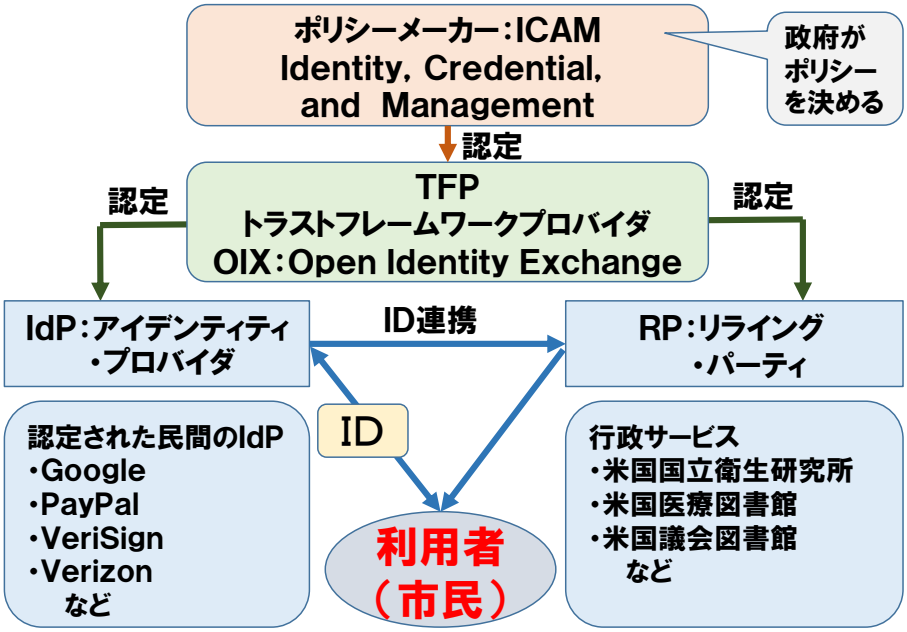


図3. ICAM: Identity, Credential, and Access Management

おわりに

ご紹介したとおり、トラストフレームワークは、明日の話ではなく、一部ではあるが既に実現しており、着々と実績を挙げている。このシステムが適正かつ公正に機能するためには、第三者による監査の果たす役割が極めて重要であり、現時点でこれがどの程度機能しているのか、システム監査人としては気になるところである。当研究会でも、今後、この問題も調査研究していく予定である。

＜目次＞

2014.5

「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 25 章

会員番号：0557　仲厚吉（個人情報保護監査研究会）

第25章　システム管理基準　個人情報保護コントロール

個人情報を取り扱う情報システム（以下、“個人情報システム”という。）を利用している場合、システム監査が必要になります。本章では、経済産業省システム管理基準に、個人情報保護監査研究会が個人情報保護コントロールを追補し、個人情報システムへのチェック項目の例としました。当研究会では、事例として監査用の「3726g_情報システム開発の安全性チェックリスト」を策定しています。実際の監査に当たっては、それぞれの個人情報システムの特徴に応じてチェック項目を選定します。

25.1　システム管理基準　個人情報保護コントロール

Ⅵ．共通業務　８．個人情報保護（12）

個人情報システムに対するシステム管理基準（個人情報保護コントロール）として、以下の３分類、12 項目を設定しました。末尾のカッコ付数字は、項目の数です。

8.1　個人情報の取り扱いに関する方針（4)

(1)	個人情報の取り扱いに関する方針の策定及び公表並びに責任体制の確保は、個人情報の保護に関連する法令等に準拠して定めること。

（主旨）組織体経営上の重要事項である個人情報の保護に関連する法令順守を行うため、個人情報の取扱いに関する方針の策定及び公表について定め、責任体制を確保する必要がある。

1. 組織体は、国の個人情報保護に関する法律及び施行令並びに基本方針に則って、個人情報の取扱いに関する方針の策定及び公表並びに責任体制の確保を行うこと。
2. 個人情報の取扱いに関する方針の策定及び公表並びに責任体制の確保について、文書化され、組織体の長が承認していること。
3. 個人情報の取扱いに関する方針の策定及び公表並びに責任体制の確保について、関係者に周知徹底し、従業者の啓発を行うこと。
4. 責任体制の一環として、個人情報の取扱いの委託について、委託の有無や、委託する業務の内容を明らかにする等、委託処理の透明化を進めること。
5. 組織体が認定個人情報保護団体に所属する場合、その旨、本人に明確な表示となる措置を講じること。

(2)	個人情報の取り扱いに関する方針に基づいて、個人情報を取り扱う情報システム（以下"個人情報システム"という。）の開発及び保守の計画を定め、個人情報保護管理者が承認すること。

1. 個人情報システムの開発、運用及び保守の計画は、文書化され、個人情報保護管理者が承認していること。
2. 個人情報システムの開発、運用及び保守の計画は、関係者に周知徹底していること。
3. 個人情報システムの開発、運用及び保守の計画は、緊急事態を特定するための手順、それらにどのように対応するかの手順を準備していること。
4. 個人情報システムの開発、運用及び保守の計画は、「共通番号」を使用する個人情報システムの

場合、あらかじめ、「共通番号」にかかわる個人情報の漏えい、滅失又はき損による影響範囲を認識し、影響度を分析し、対策を講じることができるように準備していること。

(3)	個人情報システムの開発及び保守の計画は、計画を実施及び運用するため、方法、体制等を明確にすること。

（主旨）個人情報システムの開発、運用及び保守の計画を実施及び運用するために、方法、体制等を明確にする必要がある。

1. 個人情報システムの開発、運用及び保守の計画は、実施及び運用するため、個人情報保護の要件を仕様化しシステム化する方法を確立していること。
2. 個人情報システムの開発、運用及び保守の計画は、実施及び運用するため、資源、役割、責任及び権限を明確にしていること。
3. 個人情報システムの開発、運用及び保守の計画は、実施及び運用するため、委託先を利用する場合の選定基準を明確にしていること。

(4)	個人情報システム開発及び保守の計画は、個人情報の正確性の確保及び個人情報の漏えい、滅失又はき損のリスクに応じ、必要かつ適切な安全管理措置を明確にすること

（主旨）個人情報システムの開発、運用及び保守は、計画の段階で、個人情報の正確性の確保及び個人情報の漏えい、滅失又はき損のリスクに応じ、必要かつ適切な安全管理措置を明確にしている必要がある。

1. 個人情報システムの開発、運用及び保守の計画は、個人情報を、それぞれの利用目的の達成に必要な範囲内において正確かつ最新の内容に保つための情報処理の措置を明確にしていること。
2. 個人情報システムの開発、運用及び保守の計画は、個人情報の漏えい、滅失又はき損のリスクに応じた安全管理措置を明確にしていること。
3. リスクは、個人データの取扱いの流れに従い、取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄など、その局面ごとに認識していること。
4. 安全管理措置は、本人が被る権利利益の侵害の大きさや、事業の性質及び個人データの取扱状況等を考慮していること。
5. 個人情報システムの開発、運用及び保守に当って、既存のアプリケーションを利用する場合は、アプリケーションの安全性を確認していること。

8.2　本人の権利・利益の保護(６)

(1)	個人情報システムは、個人情報の取得に当たって、利用目的を明示し、利用目的の偽りなどにならない措置を講じること。

（主旨）個人情報システムによって、個人情報を取得するときは、利用目的の表示が、利用目的の偽りなどにならない措置を講じる必要がある。

1. 個人情報システムは、個人情報を取得する画面の利用目的の表示が、偽りの表示になっていないこと。
2. 個人情報システムは、個人情報を取得する画面の利用目的の表示が、正しくかつできるだけ具体的な表示、例えば、その取り扱う事業内容を勘案して顧客の種類ごとに利用目的を限定して示すなど、本人にとって明確な表示になっていること。

3. 個人情報システムは、個人情報の取得元又はその取得方法（取得源の種類等）を可能な限り具体的に表示していること。

(2) 個人情報システムは、個人情報の入力に当たって、本人から利用目的の認識又は同意を得る措置を講じること。

（主旨）個人情報システムによって、個人情報をシステムに入力するときは、個人情報の利用目的を明示して本人から利用目的の認識又は同意を得る措置を講じる必要がある。

1. 個人情報システムは、個人情報をシステムに入力するとき、個人情報の利用目的を明示して本人から利用目的の認識及び同意を得る措置を講じていること。
2. 個人情報システムは、個人情報をシステムに入力するとき、本人の選択によって利用目的を限定できるように措置を講じていること。

(3) 個人情報システムは、個人データの利用にあたって、取得に際して特定した利用目的に合うように出力を制限する措置を講じること。

（主旨）個人情報システムによって、個人データを利用するに当っては、取得に際して特定した利用目的に合うように出力を制限する措置を講じる必要がある。

1. 個人情報システムは、個人データの利用に当たって、取得に際して特定した利用目的の目的外利用にならないように出力を制限する措置を講じていること。
2. 個人情報システムは、個人データの利用に当たって、第三者への提供によって目的外利用になることのないように、出力を制限する措置を講じていること。

(4) 個人情報システムは、保有個人データの開示等の求めに応じる措置を講じること。

（主旨）個人情報システムは、個人情報の本人に対して保有個人データの開示等の求めに遅滞なく応じる措置及び保有個人データを出力する措置を講じる必要がある。

1. 個人情報システムは、本人に対して開示等の求めに遅滞なく応じる措置を講じていること。
2. 個人情報システムは、求めに応じて保有個人データを出力する措置を講じていること。
3. 個人情報システムは、保有個人データについて本人から求めがあった場合には、ダイレクトメールの発送停止など、自主的に利用停止に応じる措置を講じていること。
4. 個人情報システムは、求めに応じて個人情報の取得元又はその取得方法（取得源の種類等）を可能な限り具体的に出力できる措置を講じること。

(5) 個人情報システムは、苦情の処置に応じる措置を講じること。

（主旨）個人情報システムは、本人の苦情及び相談に対して、適切かつ迅速な処理ができる措置を講じる必要がある。

1. 個人情報システムは、本人の苦情及び相談に対して、正しく適切な処理ができる措置を講じていること。
2. 個人情報システムは、本人の苦情及び相談に対して、迅速な処理ができる措置を講じていること。

(6)個人情報システムは、個人情報の保管期間と廃棄の過程が明確である措置を講じること。

（主旨）個人情報システムは、個人データの保管に当たって、法令等や業務要件に適合する保管期間が特定され、その保管期間を超える保管又はそれ以前の誤廃棄がないように、保管期間と廃棄の過程が明確である措置を講じる必要がある。

1. 個人情報システムは、個人データの保管に当たって、法令等や業務要件に適合する期間保管され、その保管期間を超える保管がないこと。
2. 個人情報システムは、個人データの保管に当たって、法令等や業務要件に適合する期間保管され、それ以前の誤廃棄がないこと。

8.3　個人情報の利活用（２）

(1)個人情報システムは、苦情の処置に応じる措置を講じること。

（主旨）個人情報システムは、個人情報の有用な利活用のため、個人データベース等を維持管理する措置を講じる必要がある。

1. 個人情報システムは、個人情報の有用な利活用のため、個人データベース等を、正確かつ安全に、維持管理する措置を講じていること。
2. 個人情報システムは、個人情報の有用な利活用のため、個人データベース等を、有効かつ効率的になるように、維持管理する措置を講じていること。

(2)個人情報システムは、個人情報の有用な利活用のため、個人情報の保護に関する法令等に準拠して個人情報を公共のために提供できる措置を講じること。

（主旨）個人情報システムは、個人情報の保護に関する法令、ガイドライン等に準拠し、個人情報を公共のために提供できる措置を講じる必要がある。

1. 個人情報システムは、個人情報の保護に関する法令、ガイドライン等に準拠し、個人情報を公共のために提供できるように、検索する措置を講じていること。
2. 個人情報システムは、個人情報の保護に関する法令、ガイドライン等に準拠し、個人情報を公共のために提供できるように、出力する措置を講じていること。

■

次回は「第 26 章　プライバシーマーク認定後の維持・運用のポイント」をご紹介します。＞

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

＜目次＞

2014.5

注目情報（2014.03～2014.04）　※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。

■OpenSSL の脆弱性に対する、ウェブサイト利用者（一般ユーザ）の対応について（2014.4.16）
IPA（独立行政法人情報処理推進機構）
http://www.ipa.go.jp/security/ciadr/vul/20140416-openssl_webuser.html

■更新：Internet Explorer の脆弱性対策について(CVE-2014-1776)（2014.4.30）
IPA（独立行政法人情報処理推進機構）
http://www.ipa.go.jp/security/ciadr/vul/20140428-ms.html

■Adobe Flash Player の脆弱性対策について(APSB14-13)(CVE-2014-0515)（2014.4.30）
IPA（独立行政法人情報処理推進機構）
http://www.ipa.go.jp/security/ciadr/vul/20140430-adobeflashplayer.html

■2014 年版 情報セキュリティ 10 大脅威(2014.3.31)
IPA（独立行政法人情報処理推進機構）
http://www.ipa.go.jp/security/vuln/10threats2014.html

■モバイルマルウェアを用い 2 要素認証のコードを盗む手口に注意（2014.4.28）
内閣官房情報セキュリティセンター（NISC）
http://securityblog.jp/news/20140428.html

■平成 25 年中の不正アクセス行為の発生状況等の公表について（2014.3.27）
警察庁
http://www.npa.go.jp/cyber/statics/h25/pdf040.pdf

■日本監査研究学会　第36回　東日本部会　開催
http://www.dobunkan.co.jp/audit/bukai/index.html
◆第36回　東日本部会
開催日　2014 年 5 月 24 日（土）
開催校　中央大学
準備委員長　藤沼亜起
開催場所　中央大学後楽園キャンパス
（〒112-8551　東京都文京区春日 1-13-27）
統一論題テーマ「会計判断と監査判断－虚偽記載に伴う課徴金納付事例を取り上げて－」

＜目次＞

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の最新動向とISO/IEC27001(JIS　Q 27001)改定
	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	ISO及びIECの合同専門員会ISO／IEC　JTC1/SC27においてISO／IEC27000ファミリーの標準化作業が進められている。 ISMSの国際標準であるISO／IEC27001(第1版)の改定版が 2013 年 10 月にISO／IEC27001(第 2 版)として発行された。 ISO/IEC27001(第2版)は、ISO　MSS共通要素を取り込んだ規格となっている。 本講演では、ISMSの最新動向とともに、ISO／IEC27001の改定のポイントについて概説する。
	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。 (https://www.saaj.or.jp/getsurei/getsurei_form.html)
第192回(予定)	日時:2014 年 7 月 3 日(木)　18:30～20:10　場所:機械振興会館　地下2階多目的ホール	
	テーマ	クラウドセキュリティガイドライン改訂版に係る改訂のポイント(仮題)
	講師	経済産業省　商務情報政策局　情報セキュリティ政策室　室長補佐　上坪健治氏 特定非営利活動法人　日本セキュリティ監査協会(JASA)事務局長永宮直史氏
	講演骨子	詳細確定次第、HPでご案内いたします。
	お申し込み	
第193回	日時:2014 年 7 月 22 日(火)　18:30～20:30　場所:機械振興会館　地下2階多目的ホール	
	テーマ	「情報セキュリティの最新の脅威の動向」(仮題)
	講師	独立行政法人　情報処理推進機構(IPA)技術本部　セキュリティセンター 情報セキュリティ技術ラボラトリー　　主任研究員　　渡辺　貴仁　氏
	講演骨子	詳細確定次第、HPでご案内いたします。
	お申し込み	

■システム監査実践セミナー(東京)

第14回	「事例に学ぶ課題解決セミナー」[2014/6/7, 於・東京]のご案内 (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。)	
	概要	情報システムの事故・障害で、企業や顧客が損失を被る事例が後を絶ちません。システム監査の専門家が事故・障害の原因を解き明かし、システム監査の観点から見た有効な解決策を示します。 事故・障害の原因は報道だけでは分かりません。事故・障害事例をリスクとコントロールの視点で分析して、皆様の課題解決に役立つ説明をします。 情報システムの利用者から運営者、経営者から担当者まで多様な階層・職種の方のキャリアアップに、当セミナーをご活用下さい。 事故・障害を未然に防ぐシステム監査の役割とその有効性の理解向上にも役立ちます。 自社システムの信頼性・安全性をさらに高めたいと考えておられる経営者、役員の方、IT 部門長の方など、多くの皆様の参加をお待ちしています。 受講修了後、受講証明書をお渡ししています。
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の実施（東京・大阪）

計画中	◎情報システムに関する知識コース　2014年7月13日～14日（2日コース） ◎システム監査に関する知識コース　2014年6月23日～24日（2日コース）　東京 2014年 7 月 20 日～21 日（2日コース）　東京 2014年 8 月 10 日～11 日（2日コース）　東京 2014年 9 月 14 日～15 日（2日コース）　東京	
	概要	特別認定講習は、SAAJが認定した特別認定講習実施機関が、CISA、ITコーディネータ、情報セキュリティ プロジェクトマネジャ等の高度情報処理技術者試験合格者など、SAAJの定める資格取得者に対し、SAAJの定めるカリキュラムに基づき講習を実施するものです。特別認定講習を受講し、所定のテストに合格した場合には、「公認システム監査人」、「システム監査人補」としての申請が可能です。
お申し込み	講習開催スケジュールと申し込み先をHPでご案内しています。 （http://www.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）

＜目次＞

2014.05

図書紹介：「サイバーセキュリティ」　～幅広いサイバーリスクへの理解と取り組みのために～

会員番号　0148　**木村裕一**

最近益々脅威の度合いを深めているサイバーセキュリティについて、大変参考になる図書が出版されましたので、紹介いたします。

「サイバーセキュリティ」
サイバーセキュリティと経営戦略研究会　（編）
NTT出版　（2014年3月）発行
価格：2400円＋税

本書は「サイバーセキュリティと経営戦略研究会」編纂の図書であり、執筆者は2012年11月の月例研究会（テーマ：SNSの情報セキュリティを考える）の講師を務めていただいた守屋　英一氏と各分野の専門家6名の方々である。サイバーセキュリティは現在個々のシステム・企業を狙うだけでない。TVシステムもインターネットも銀行も、いや社会インフラ、国家そのものもその狙いに入れているものになっていることは、皆さんがご存知のとおりです。われわれシステム監査人は、単に自社、あるいは顧客のコンピュータシステムに関わる問題として狭い範囲で捉えるのではない、幅広い、また先を見通した理解をもって対処する必要があります。その意味でサイバーセキュリティの全体像をさまざまな立場の専門家が意見交換しながら、検証し、著されたこの図書は、現時点で最善の書のひとつであると考えます。本書の一番の特徴は、その中で述べられている“サイバーセキュリティを考える上でのフレームワーク、つまり概念の体系を提示することを目的としてきた。”ことです。このことは目次を紹介するのが、一番内容を俯瞰できることになるので次に示します。

第1章　サイバー攻撃の実態と課題
第2章　サイバー空間の成立とセキュリティ
第3章　日本のサーバーセキュリティ関連組織の現状
第4章　サイバースペースの国際安全基準
第5章　サイバーリスクと価値創造のマネジメント
第6章　サイバーセキュリティ法
第7章　サイバーセキュリティにどう立ち向かうか

たとえば第 3 章では、政府の政策などが良く報道されていますが、それらがどのように結びついて全体としてどのような意味を持っているか解説しています。サイバーセキュリティについては、我々の今後長く付き合ってゆかねばならない重要なテーマでもあります。本書では各章ごとに基本事項から現状、また課題までを体系的に整理し解説されており、サイバーセキュリティに取り組んでゆくのに、貴重な参考図書として推奨します。

以上

＜目次＞

2014.05

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

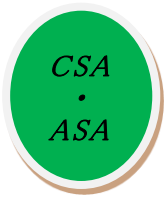
・会員割引や各種ご案内、優遇などがあります。 http://www.saaj.or.jp/nyukai/index.html
　セミナーやイベント等の開催の都度ご案内しているものもあります。

・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。

＜目次＞

2014. 05

【　協会行事一覧　】

2013 年	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
11 月	14 日 理事会:次期会長選任 14 日 予算申請提出依頼(11/30〆切) 16 日 2014 年度役員改選準備開始 20 日 会費未納者除名通知発送 30 日 会計:2014 年度予算申請提出期限	16 日 認定委員会:CSA 面接 18 日 第 187 回月例研究会 20 日 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〕 3 日 第 192 回月例研究会 22 日 第 193 回月例研究会	14 日 支部会計報告〆切
8 月	(理事会休会) 会費督促電話作業(役員) 中旬 中間期会計監査	秋期公認システム監査人募集 8/1～9/30	30～31 東北支部:合宿研修会 30～31 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。

＜目次＞

2014.05

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。

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
編集支援：　仲厚吉　（会長）
投稿用アドレス：　saajeditor ☆ saaj.jp （☆は投稿時には＠に変換してください）
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━