



認定 NPO 法人

日本システム監査人協会報

2016年3月号

No. 180

— No. 180 (2016年3月号) <2月25日発行> —

◎今月号の注目記事

「情報処理安全確保支援士制度（案）」

経済産業省公表

（関連記事：巻頭言、注目記事）

◎第15回通常総会が2月22日に開催

（4月号で総会特集を掲載）



ダイヤモンド箱根駒ヶ岳

2016年2月5日撮影 神奈川県二宮町吾妻山より

写真提供：藤井 仁志

巻頭言

『情報処理安全確保支援士と SaaJ』

会員番号 555 松枝憲司(副会長)

政府は 2016 年 2 月「サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律案」を閣議決定し国会に提出しました。改正案は、昨年発生した年金情報流出事件が、内閣サイバーセキュリティセンター（NISC）によるセキュリティ評価・監査が特殊法人にまで及ばなかったことが遠因になったとの反省を踏まえ、NISC が行うセキュリティ評価・監査の対象範囲を、行政機関（中央省庁）から独立行政法人や特殊法人にも拡大すること及びサイバーセキュリティに関する助言を行う国家資格「情報処理安全確保支援士（以下支援士）」を新設することが骨子となっています。

この支援士は、現行の「情報処理技術者試験」とは別の位置づけで、試験合格者の登録制とし、企業などは経済産業省が整備する登録簿を参照して人材を探せるようにし、一定期間での講習受講を義務化した更新制とするとのこと。このような制度は、資格更新制である当協会の CSA やシステム監査等を行っている企業のシステム監査台帳や情報セキュリティ監査台帳への登録制度をなぞっているように見えます。

支援士は、企業内にいて情報処理の安全を確保・助言する当事者であり、監査人は支援士の活動を含めて評価するという役割の違いがありますが、企業における安全な情報の処理を担保していくという目的は共通だと思います。

当協会のシステム監査活性化委員会で検討した SaaJ のビジョンにもあるように、システム監査人を中心に、支援士も含めシステム監査以外の専門家のスキルも取り込んだ“IT アセスメント”の定着に取り組むことにより、安全性が高くかつ有効な IT 活用が行える社会の実現について支援していきたいと考えています。

各行から Ctrl キー+クリックで
該当記事にジャンプできます。

(各記事末尾には目次へ戻るリンク有)

<目次>

○ 巻頭言	1
【 情報処理安全確保支援士と SaaJ 】	
1. めだか	3
【 システム監査の課題 】	
2. 投稿	4
【 システム監査の活性化 】	
【 時事論評 】 AI (人工知能) の進化とシステム監査の終焉？	
3. 本部報告	8
第 210 回 月例研究会講演録	
【 最近のインターネットバンキングに係る不正送金事犯の現状と対策_】	
講師：警察庁 生活安全局 情報技術犯罪対策課 指導第一係 課長補佐 小竹一則 氏	
4. 支部報告	12
【 近畿支部 第 157 回定例研究会 】	
「システム監査の多様性について」	
5. 注目情報	16
■ 【 情報処理安全確保支援士制度 (案) を公表 】 (経済産業省)	
■ プレス発表	
【 「情報セキュリティ10大脅威 2016」 を発表 】 (独立行政法人情報処理推進機)	
6. セミナー開催案内	18
【 協会主催イベント・セミナーのご案内 】	
7. 協会からのお知らせ	19
【 新たに会員になられた方々へ 】	
【 S A A J 協会行事一覧 】	
8. 会報編集部からのお知らせ	21

めだか 【 システム監査の課題 】

システム監査の大きな課題のひとつは、システム監査の技法が情報技術(IT)の進歩にどのように追従し、IT の健全性を監査していくことができるかということであると思う。この課題を考えるため、情報技術(IT)は、技術(Technology)のひとつであるため、先ず、技術(Technology)とは何であるかを考えてみた。参考資料1によれば、他の動物に比べて人類を人類らしくした技術(Technology)は、6つの発明からなるという。

人類を人類らしくした発明	発明の内容
1. 弓矢(飛び道具)	トラやゾウなど他の動物を弓矢によって圧倒し、後に鉄砲、ミサイルの発明になった。
2. 加熱加工	加熱加工で土器や、金属をつくり、青銅器、鉄器などの機器や機械を製作した。
3. 牧畜	動物を自分の意思に従わせる方法を発明し、後に人を奴隷として使役した。
4. 農耕	時間的な計画、空間的な設計、種子の貯蔵などノウハウを伝承することが生まれた。
5. 文字	情報のあり方が変わった。知識を蓄積し、遠方にも伝えることができるようになった。
6. 通貨	通貨、お金を使うようになって、「経済」が生まれ、所有と流通の概念が確立した。

東京国立博物館の「始皇帝と大兵馬俑」展を見学したが、上記の人類を人類らしくした発明の原型を見ることができた。情報技術(IT)は、上記の「5. 文字」の発明が進化し、情報のあり方が発展したものであるが、それは、そのほかの技術(Technology)にも適用され、応用されている。参考資料1には、現在の金融では、「リスクを伴う金融に耐え得るだけの知恵が必要」と書いている。情報技術(IT)の進歩がさまざまであっても、システム監査対象のリスクとそのコントロールを分析するという知恵は、IT の健全性を監査していくうえで重要であると思う。

情報技術(IT)のうち人間自身に関わる研究は、手塚治虫先生が描いた「鉄腕アトム」の世界から、ロボット工学者の石黒浩教授の「アンドロイドは人間になれるか」という研究に発展している。参考資料2で、教授は、小学校五年のときに、親だったか先生だったか、大人から「人の気持ちを考えなさい」と叱られ、この言葉に衝撃を受けたと書いている。また、本当のところ、大人は、「人の気持ち」や「考える」ということは何も分かっていないで言っているということに気が付いたとも書いている。

システム監査の技法が情報技術(IT)の進歩にどのように追従し、IT の健全性を監査していくことができるかという話にもどると、課題解決の道筋は、IT 社会で求められる監査にリスク・アプローチで取り組み、システム監査の技法を試行錯誤していくうちに、見えてくるように思う。



(空心菜)

参考資料1:「大激震」 堺屋太一著 実業之日本社

参考資料2:「アンドロイドは人間になれるか」 石黒浩著 文春新書1057

(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 >](#)

投稿【 システム監査の活性化 】

会員番号 0557 仲 厚吉 (会長)

当協会は、IT(情報技術)の利活用が日常化するなか、情報処理システムへの監査をはじめ、情報セキュリティ、内部統制、事業継続、個人情報保護、IT ガバナンスなどの IT 利活用の場面で、システム監査の普及・促進、及びシステム監査人の活躍の場を広げる活動に取り組んできました。2016 年度より、当協会は、新たに SAAJ のビジョンを掲げて、システム監査の活性化に取り組みます。

■SAAJのビジョン(3年後に目指す姿)

- 社会の多様な要請に対応し、信頼性・安全性が高くかつ有効な IT 活用を実現することを目標として、IT サービスの提供者と利用者双方における適切な統制を維持・向上させる活動を、既存のシステム監査を核にした“IT アセスメント”としてとらえる。
そのうえで、SAAJ の活動を“IT アセスメント”の定着に焦点を当てて取り組む。
- これにより、会員を含むシステム監査人のビジネス機会の増大を図り、SAAJ の知名度向上、会員の拡大に繋げる。

2016 年 1 月 1 日より、マイナンバー制度が施行され、会員の皆様が勤務されている企業・団体では、個人番号関係事務取扱担当者を定めるなど実務に取り組み始めていると思います。マイナンバーに関して、2016 年 2 月 13 日の朝日新聞朝刊に、次のような記事が掲載されています。

■個人番号カード活用初認定

- 総務省は 12 日、マイナンバーカード(個人番号カード)の IC チップを利用できる事業者として、ケーブルテレビ放送を支援する民間企業「日本デジタル配信」と、一般社団法人「スマートテレビ連携・地域防災等対応システム普及高度化機構」「ICT まちづくり共通プラットフォーム推進機構」を、それぞれ認定した。政府・地方自治体以外もカードを活用できるようにする初の認定。
カード情報を読み取り、スマートフォンなどで予防接種の記録を閲覧できるようにしたり、災害時にテレビに避難情報を配信したりするサービスを計画しているという。

2016 年 1 月 1 日より個人情報保護委員会が設置されています。当協会では、2 月 22 日(月)の通常総会後の特別講演に、個人情報保護委員会委員長堀部政男氏を講師にお招きし、ご講演をお願いしています。

当協会では、SAAJ のビジョンが指し示す方向に目標を定め、個人番号カードの活用が図られるなど IT の利活用が日常化する社会に必要なシステム監査の活性化に取り組み、健全な IT 社会の発展に資する活動を行っていきます。協会活動に当たって会員の皆様の、より一層のご協力をお願い致します。

以上

[<目次>](#)

【時事論評】AI（人工知能）の進化とシステム監査の終焉？

会員番号 0707 神尾博

1. IoT/M2M、ビッグデータよりAIに注目！

甚だインパクトのある表題かもしれないが、システム監査人は、このパラダイムシフトから目を背け惰眠を貪るべきではないとの見地から、本稿にて敢えて警鐘を鳴らさせて頂く。もはやAI(Artificial Intelligence)はシステム監査の未来展望に際し、いや現在のITを語るにおいても、無視できない技術要素となってきた。

振り返ると18世紀後半の第一次産業革命以降での機械化、そして1980年代以降のマイクロプロセッサの高性能化や普及による情報システム化やIT機器の多機能化は、それぞれ肉体労働者とホワイトカラーとの違いこそあれ、本質的には単純作業の人間からの置き換えが中心だった。これにより、生産性の向上や劣悪環境からの解放といった福音がもたらされた。

ところがAIは、人間の人間たる所以であり、最後の砦とも言える知的活動をも、侵食・剥奪していくのである。最近のITトレンドを代表する、IoT/M2Mやビッグデータはそれ単体では、機能や効果は情報システムやIT機器の部分集合でしかない。しかしAIはこれらのみならず、従来の自動機械、あるいは人間をも含めて、社会的にもビジネス的にも最上位の階層として君臨するようになる、まずはこれを押えておきたい。

2. AIの利用分野の拡大とその背景

現在、AIの利用分野は日々拡大を続けている。たとえば、チェスに比べて複雑度が高いと言われてきた将棋でも、複数の棋士の持つ大局観の機械学習により、各段にレベルが上がった。他にも犯罪発生の予測、自動翻訳、フォレンジックによる企業の不正調査やセキュリティ分野におけるSIEM(Security Information and Event Management)等、枚挙に暇がない。変わったところでは、SNS不倫サイトで会話ロボットが人間女性へのなりすましまでやっていたというから驚きだ。

米国の著名なクイズ番組で、2011年に人間のチャンピオン相手に勝利したIBM社のWatsonは、クラウドサービスのプラットフォームでの、一部の機能の提供が開始されている。(なお同社の公式見解では、WatsonはAIではなく「コグニティブ(認知)コンピューティングシステム」であるとしている)

さらには制御系では、LIDAR等のセンシング技術の発達との相乗により、自動運転車の本格的な実用化はもう目の前だ。交通事故の90%以上が運転ミスによるもの(2013年、米国Eno Center発表)であるため、激減が期待できる。ちなみに、航空機は1980年代からオートパイロット化が進んだが、自動車の場合は障害物にほとんど遭遇しないはるか上空とは、検知や制御において、桁違いの複雑さや精緻さへの対応が要求される。

これらの実現の背景には、数々の技術ブレークスルーがある。システム監査人は、単に利用分野といった表面的な捉え方のみでなく、本質の理解が損なわれないよう、そこから押えておくべきだろう。

最も注目すべきは「機械学習」である。そして、この機械学習のうちで「ディープラーニング(深層学習)」と呼ばれる「DNN(多層ニューラルネットワーク)」を使う手法がある。そのDNNは、人間の脳を模したアーキテクチャであり、あらかじめ人間が用意した解答から、AIがルールやパターンを導き出す教師あり学習と、それ無しでAIが単独で獲得する教師なし学習がある。この機械学習では、「知識表現」と呼ばれる、コンピュータ自身が理論や法則を理解・処理できるような技術が用いられる。まとめると「限定的ではあるが、理論や法則をAIが自ら理解し、さらに導き出すようになった」、これを念頭に置いておいて頂きたい。

ちなみにこれらの源泉として、ビッグデータを高速処理できるHPC(High Performance Computer)の存在が欠かせないことも、付け加えておく。

3. ホワイトカラーへの影響は確実・甚大

2013年に英国・オックスフォード大学のオズボーン准教授等により発表された論文「雇用の未来」。「経営に役立つシステム監査」を標榜される方々なら、当然ご存じだろう。それには、先進国でこれから10年でなくなる仕事、残る仕事が一覧アップされている。消滅すると予測された方から、比較的システム監査と関連の深そうなものをチェックしておこう。

まずは被監査部門からの、コンピュータオペレータや同サポートデスクは予想通りの印象だ。それから、会計士、会計・経理及び監査の事務員。現在の財務会計はIT化が前提だから、この分野のシステム監査業務も、かなりのダメージを食うとの見立てが妥当だろう。それなら計数分析はAIに任せるとして、監査報告書のような文書作成はどうだろう？ 実は、米国新聞の企業決算レポートは、すでにAIが執筆しているのだ。またコンプライアンスはシステム管理基準に記載されていて重要な監査項目だが、過去の判例の分析等のAI化によって、米国では弁護士助手はおろか、弁護士の選別・淘汰も始まっているという。

他では、米国の研究者・カーツワイルが2005年に発表した著書での「シンギュラリティ」が物議を醸している。AIが自らの改良を重ね、圧倒的スピードで進化していくというものだ。氏は、人間を凌駕し制御不能となるのは2045年頃と予測している。もしそうなれば、消え去る仕事のランキング付けどころでは済まなくなる。

さて、これらの文献等によると、パターン認識を含む大量データ処理中心での、AIとの勝負は早々に諦めた方がよいという事になる。一方で、創造性やコモンセンス等が人間における真の最終防衛線というのが、通説のようだ。これらを踏まえ、本題のAIとシステム監査との関係に移りたい。

4. システム監査は終焉しない

結論から言うと、必ずしも全員が悲観する必要はない。システム監査はけっして終焉などしないと見る。少なくともシンギュラリティまではそうだ。いや、シンギュラリティ自体に懐疑的な研究者は多い。主な理由としては、「そもそも現在のAI技術は、人間の脳を持つ一部の機能を模倣しているに過ぎない」といったところが挙げられている。

しかしひょっとすると到来するかもしれないシンギュラリティまで、システム監査人はどう過ごすべきか？ ここまでに述べてきた「AI関連の技術ブレイクスルー」「AIが人間を卓越する領域・仕事」部分の行間を読めば、解のヒントが隠されている。

さて、これからも残るシステム監査のひとつとして、まずはAIそのものへのシステム監査というのはどうだろう？ たとえば「AIのアルゴリズムやプログラム、APIの提供方法等に関する品質評価」である。新技術においては、それら特有の監査上の知見の取得は、優秀な人間の方が先になるのではないか。なお、IPAの公式見解でも、システム監査の対象を企業の情報システムに限定せず、エンベデッド(組込)についても言及があるため、ファームウェアとしてAIを内蔵したロボットも監査対象として問題はない。

もうひとつは、公共や組織における情報システムや製品への、AIの実装・利用に関してである。「経営や経済活動の効率化、社会生活の向上のためにAIを活用していないことを指摘し改善勧告する」といったところはいけそう。たとえば、コンパクトで安価な同時自動通訳機が、市場に提供され始めそうな情勢になれば、「企業での社員教育や自己啓発テーマでのTOEICの必要度は？」「公教育における英語の適正な授業時間や教員数は？」といった提起や助言が想定される。

5. システム監査人は淘汰される

だが現状では、絶望が待ち受けているシステム監査人は、少数に留まらない可能性がある。たとえば先に述べたように、財務・会計分野のみに拘泥するシステム監査人は、言わずもがなである。監査対象ITのコンプライアンスは、大半をAIが代行チェックしてくれるようになるだろう。また企業の基幹システムや対外サービスに次々とAIが搭載されていけば、AI関連の情報へのアンテナの感度と理解力が追い付かない者は、アサインから漏れるに違いない。

さて、ここではそれ以前の問題についても警告しておこう。高所大局・マクロの視点が欠けるシステム監査人は、AIが席卷する近未来はおろか、現時点でも好ましくない存在であるという事を。たとえばマイナンバーを説明するなら、いきなり個人情報保護の視点から捉えるのではなく、まずは前段として、それを含めての制度自体の有効性・有用性を語れるかどうかといったところが、力量の判定材料になる。いずれAIが、そうした全体最適を学習してしまう時期が来るだろうが、それまではシステム監査サービスの利用側が、監査人の選別をしなければならないのである。

ところで「システム監査人はAIにどう対応、いや対抗するか?」については、更なる情報を切望される読者も多いはずだ。私は本稿以外にも、いくばくかの解答を得ているつもりではあるが、まずは自身で模索して頂きたい。最初から「自主的な探求」を放棄する者は、戦わずして「機械学習」に屈しているわけだから。

最後に、本稿作成に際してご助言頂いた安本哲之助氏、田淵隆明氏に対し、この場を借りて御礼を申し上げる次第である。

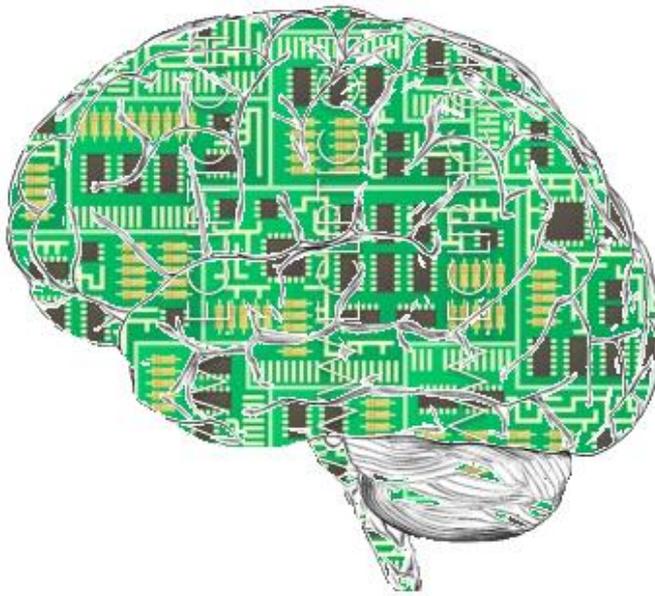


Photo by Gengiskanhg - ArtificialFictionBrain (出典:ウィキメディア・コモンズ)

(このコラム文書は、記事提供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>

第 210 回月例研究会講演録【最近のインターネットバンキングに係る不正送金事犯の現状と対策】

会員番号 0557 仲 厚吉

講師：警察庁 生活安全局 情報技術犯罪対策課 指導第一係 課長補佐 小竹一則 氏

日時、場所：2016 年 1 月 21 日(木)18:30 - 20:30、機械振興会館 地下 2 階ホール (神谷町)

テーマ：「最近のインターネットバンキングに係る不正送金事犯の現状と対策」

要旨：

日本年金機構の個人情報の流出、DDoS 攻撃やランサムウェア感染による企業恐喝の発生など、サイバー空間における脅威が高まるなか、平成 26 年に過去最悪の被害となったインターネットバンキングに係る不正送金事犯についても、その被害は、平成 27 年上半期で約 15 億円に達するなど、深刻な状況が続いている。

本講演では、これらサイバー空間における脅威の情勢に触れつつ、最近の不正送金事犯の手口について事例を交えて紹介し、効果的な対策について考察を加えたい。

講演録：

I. インターネットを取り巻く現状 ～高まるサイバー空間の脅威

国内のインターネット利用者数は、平成 25 年末に初めて 1 億人を突破し、13～59 歳までの年齢階層では利用率は 9 割超えになっている。サイバー犯罪の検挙状況では、平成 26 年中のサイバー犯罪の検挙件数は 7,905 件、ネットワーク利用犯罪検挙件数は過去最高を記録、不正アクセス禁止法違反の検挙件数は 364 件で前年比 -616 件となっている。

また、サイバー犯罪に質の変化があり、現在は、金銭取得目的で、かつ、個人による犯行から組織的犯行になっている。サイバー空間の脅威(平成 27 年上半期)の実態は、次表のようになっている。

インターネットバンキング不正送金～被害額約 15 億円～過去最悪を超える？
標的型攻撃～メール件数 1,472 件(前年同期 6.8 倍)
不審なアクセス(探索行為)～1 日 1IP アドレス当たり 684.9 件(昨年同期比 1.5 倍)

「日本年金機構情報流出事案」は、日本年金機構に対する外部からの不正アクセスにより、個人情報が外部に流出した事件で、2015 年 6 月 1 日に同機構から公表と謝罪があった。同事案は、同機構の職員が電子メールに添付されたファイルを開封、あるいは URL からダウンロードしたファイルを実行したためウィルスに感染し、感染端末を通じて機構内が保有する 125 万件の年金加入者個人情報が流出したものである。

この事案では、職員が業務のために基幹システムに保管する「年金加入者個人情報」をファイル共有サーバにデータを持ち出して利用していたが、パスワードを掛けて運用していなかったと報告されている。

標的型攻撃メールへの備えにおいて最も重要なことは、「サイバー攻撃対策は単なる技術的問題ではなく組織運営上の課題」であることを組織に周知徹底することである。

職員パソコンに感染させない → 平素から標的型攻撃メール訓練を！ ～「不審なメールを開かない」を身につけさせる
メインシステムに感染させない → 職員パソコンとメインシステムの分離 ～クレームを装ったメールなど業務上開かざるを得ないメールがあることから感染することを想定した対策が必要！
サイバー攻撃の脅威 → 非常に大きなリスク要因と捉える必要あり！ 情報セキュリティ部門に任せきりにしない！ ～組織運営上の課題である！

II. インターネットバンキングに係る不正送金事犯の現状

インターネットバンキング不正送金は、次のような3つの過程を経て行われる。

1	ユーザの ID・PW の不正取得 ①フィッシング : 金融機関を装い電子メールを送信、セキュリティ向上のためと偽り、メールに添付された偽のデータ入力画面へ誘導 ヴィッシング : 電話による ID・PW の聞き出し スミッシング : SMS メールを送信してフィッシングサイトに誘導 ②ウィルス感染: 何らかの手段でウィルスを送り込んで利用権者の知らない間に ID・PW を取得
2	不正送金の実行(送金指令) ①犯人のパソコンで ②プロキシ(中継)サーバ経由 ③ウィルス感染した第三者のパソコン経由
3	移動先口座からの現金化 ①現金引出役(出し子)による引き出し ②仮想通貨・プリペイドカード等への交換(引き出し行為なし)

上記のそれぞれの過程で不正送金事犯への被害防止対策を講じる必要がある。

インターネットバンキングに係る不正送金事犯の発生状況 ～平成 27 年上半期

発生件数 754 件
被害額 約 15 億 4,400 万円
～金融機関が阻止した額を除いた実被害額は約 13 億 7,500 万円

検挙状況 ～平成 27 年上半期

58 事件 88 人を検挙 昨年上半期比(－11 事件、－45 人) 昨年下半期比(+12 事件、－12 人)
※日本人被疑者が増加 51 人(58.0%) 口座売買関係被疑者が多数

Ⅲ. 被害防止対策

インターネットバンキングに係る不正送金事犯への被害防止対策として、取るべき方針は次の二つである。

1. 被害防止対策は、すべてのユーザパソコンが感染しているスタンスで対策を！！
2. できる対策はすべてやる！！ ～複合的な対策の実施

金融機関に対して、次の三つの要請を行っている。

1. <金融機関が取るべき対策> ワンタイムパスワードの導入 ～二経路認証システムの導入、セキュリティ対策ソフトの無償配布、送金限度額の引き下げ
2. <法人向けサービスへの対策> 電子証明書のセキュリティの強化 ・エクスポート機能の無効化 ・IC カード等への格納方式の採用 事前登録先以外の振り込みの当日送金の制限 <法人向けサービス利用者への呼びかけ> 取引申請者と承認者との間で異なる端末の利用、送金限度額の必要な範囲内での引き下げ、 不審なログイン履歴がないかの確認
3. <利用者による被害防止対策の促進> インターネットバンキング利用端末へのセキュリティ基本対策の徹底！！ 基本ソフト(OS)、ウェブブラウザ等、インストールされているソフトウェアを常に最新の状態に更新 金融機関が提供するサービスを利用！！ ワンタイムパスワードは携帯電話のメールアドレスで受信

Ⅳ. 日本における官民連携の推進 ～JC3 の活動

一般財団法人 日本サイバー犯罪対策センター(JC3)は、産業界、学術研究機関、捜査機関の間で、これまで以上に情報や知識・経験、ノウハウを共有することで、サイバー犯罪の実態を解明し、背後に存在する犯罪者らの追跡・特定を図るとともに、その脅威を軽減・無効化するための枠組みとして活動している。

・サイバー空間の脅威に対し、産学官(警察)が連携した形でのプロアクティブな対応をする。
・海外機関と連携し、有益な情報を収集、発信する。
・サイバー空間全体を俯瞰し、産学官それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を組織内外で共有する。

警察の活動では、C&C サーバ (command and control server) 対策や、MITB(Man in the Browser)対策、ネットバンキングウイルス無力化作戦などが講じられている。

※C&C サーバとは、外部から侵入して乗っ取ったコンピュータを利用したサイバー攻撃で、踏み台のコンピュータを制御したり命令を出したりする役割を担うサーバコンピュータのこと。MITB 攻撃とは、悪意の攻撃者がユーザの PC にトロイの木馬などのマルウェアを侵入させて通信を監視し、オンラインバンクにログインされた後の通信を乗っ取り、ユーザの預金を盗み取る攻撃のこと。

サイバー犯罪に対処する上で、警察における問題意識は次のようなものである。

警察活動を通じて特定の脅威については詳細に把握できる。しかし、被害者が被害に気付かなかつたり、警察に届け出なかつたりすることから警察では把握できていない事案も極めて多く、情報の把握には限界がある。

JC3 への期待は、次のものである。

産学官がそれぞれの強みを活かしつつ相互に補完し合うことで、サイバー空間の脅威に関する事象の全貌を把握し、その大本に対処することが可能になる。

V. 質疑応答、及び受講した感想

講演後の質疑応答では、ビジネスメールの内容を盗聴してビジネスメールを差し替えるという BEC (Business E-Mail Compromise) 犯罪の状況や、現金引出役(出し子)について等、質問があり、重要なメールは電話・FAX で別途確認する必要性や、現金引出役(出し子)を逮捕する際の課題等について回答があった。

日本という国は、四囲を海に囲まれた島国であるためか、ともすれば、日本人は、安全な国に住んでいると思って生活しています。ところが、インターネットはグローバルネットワークで、そこには海外を隔てる海などは無いのに、日本人は日本が安全な国では無いことを忘れがちです。

インターネットの利用者は、サイバー犯罪者は金銭取得目的で、かつ、個人による犯行から組織的犯行になっていることを忘れてはならないと思います。また、最近では、海外からの脅威のみならず国内でもサイバー犯罪者が台頭しているということです。国民は、サイバー犯罪に対処する警察活動に協力していくよう求められています。私たちは、サイバー犯罪被害やその予兆はすみやかに警察に届け出るなど今まで以上に協力していく必要があると思います。

以上

[< 目次 >](#)

支部報告 【 近畿支部 第157回定例研究会 】

会員番号 2591 近藤 博則

1. テーマ 「システム監査の多様性について」
2. 講師 システム監査人協会 近畿支部
林 裕正 氏
3. 開催日時 2016年1月15日(金) 19:00~20:30
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

システム監査の多様性とシステム開発プロジェクトの監査という2つのテーマについて講演いただいた。それぞれのテーマについてお話いただいた後、会場の参加者から意見を発表してもらったディスカッション形式で行われた。参加者からは、テーマを超えてシステム監査の発展についても意見が述べられた。

<講演内容>

(ア) システム監査の多様性

① テーマ選定の背景

今回のテーマを選定した背景として、システム監査学会で2012年に開催された公開シンポジウムの開催趣旨から、多様なシステム監査の必然性が求められていること。システム監査学会におけるシステム監査の多様性 研究プロジェクトのプロジェクト概要からICTを利用した情報システムが高度化し適用範囲が広がるに従って、情報システム関連の評価に対する要求も高度化・多様化し、システム監査においても従来と違う視点が求められている。という所から、システム監査が多様化してきている現状を感じテーマとして選定されたとのことだった。



② 多様性に関する視点

なぜシステム監査が多様化してきたのかについて3つの視点からまとめられていた。第一に対象組織の多様性の視点として、従来からの民間企業に加え、公共団体、非営利団体、教育機関等が増えてきたこと。次に目的の多様性の視点として、信頼性・安全性・効率性に加えて、適法性・利便性・経営戦略適合性が加わってきたこと。最後に技術の進歩からリスク拡大・変容の視点として、クラウド、ビッグデータ、SNS、オープンソース、スマホ、仮想化等が加わってきたことをあげられていた。

③ システム監査学会主催イベント 統一論題、システム監査講演会 講演テーマ、システム監査技術者試験出題範囲、公認システム監査人の得意分野、システム監査に関係した出来事を概観し、多様な変化を遂げて現在に至るシステム監査の流れを紹介された。

④ 多様性をもたらす要因

上記の多様な変化を遂げたシステム監査の流れを下敷きにして、システム監査に多様性をもたらす要因についてまとめられた。まず、IT の進化によるリスクの多様化に由るもの。次に、事件・事故が発生した際の再発抑止・減災に由るもの。国際会計基準等グローバル化を迫られる外圧に由るもの。これらを契機とした法制度の整備による規制・促進により、システム監査にも多様性をもたらされると結論づけられていた。

⑤ 多様化するシステム監査に向けて

多様化したシステム監査において大切なものについて、「監査(Audit)は「聴く」という意味を持つ。「聴く」ためには、相手と向き合う事が大切。」という言葉から、システム監査スキルはもとより、「聴く」ための技術スキル、「聴く」ための業務・業種・技術に関する知識が必要とまとめられていた。また、これに対応するためには一人の監査人では限界があるため、「チーム医療」に準え「チーム監査」が有効ではないかと提唱されていた。

⑥ 会場からの意見

- ・システムを取り巻く技術も多様化してきており、リスクを見抜くことも難しくなっているが、監査人としては見抜くための力を研鑽し続けなくてはならないと感じた。
- ・現在、監査業務に携わっているが、サイバーセキュリティの分野については、外部の協力を得ている。
- ・これまでは理屈がわかっていたらよかったが、今は勉強していないと世の中についていけないと感じる。
- ・チーム監査は必要だと感じるが、コストも必要となる。チームもクラウド的に遠隔から参加する等の対応も必要ではないかと感じた。
- ・多様化でシステム監査は厳しき局面を迎えている。ネットワーク・IOT・クラウドなどは総合力がないと評価できない。監査人としてはネットワークを組み合わせながら、チームで監査することが必要と感じた。
- ・書類を電子化しクラウドへ保管する場合等、e 文書法の電子媒体保管との兼ね合いを整理するかが問題と感じている。
- ・保証型の監査が求められると感じている。マイナンバーで自治体に対し保証型監査のニーズが高まればと感じる。
- ・システム監査が普及していないのはなぜなのか。マイナンバーはよい機会と考えるが、世間に対するアピールが弱いのではないかと。
- ・IT への依存度が高まれば、監査も多様化し、スコープも広がっている。IT が専門細分化してきている現状に監査人が対応しきれないのではないかと。IT の専門家に監査の知識を習得してもらうのがよいのではないかと。
- ・日本では法が情報に対して権利を与えていない。システム監査が法の足りない部分を補完してほしいと考えている。
- ・クラウド事業者は、監査を受け付けていない場合も多く、直接監査できない場面が多い。こういった場合に有効なのが格付けと考えている。格付けに対して監査人がステータスを見ていく必要があると考えている。
- ・経営者がリスクと感じていてもベネフィットがなければシステム監査を行わない。システム監査の認知度を向上するためには経営者へのアプローチが必要。

(イ) システムプロジェクトの監査

① 失敗プロジェクトの理由

雑誌の記事より、失敗プロジェクトの理由として「営業が無理をして受注した」「技術継承がうまくいかずプロマネ力が衰えた」「リスク管理に対して過信した」という有識者の分析、「技術的に高いレベルの案件だった」「もともと赤字を見込んでいたが、想定以上の赤字になった」という Sier の言い分を紹介し、最後に「SE稼働率維持のためリスクのある案件を受注したため」(景気が好転し、企業が IT 投資に積極的になれば解消する)という雑誌編集者の見解を示された。

② SI ベンダーの取り組み

失敗プロジェクトに対する SI ベンダーの取り組みとして、案件開始前の段階でリスクを管理する。提案段階やプロジェクト計画段階でリスクを開示する。早い段階でプロジェクトの大方針を顧客と共有する。リスク管理を現場任せにしない。第三者による品質評価を実施する。利用部門の関与度合いを確認する。定期的に顧客の満足度を確認する。等を挙げられていた。



③ 監査のチェックポイント

情報サービス産業協会「ソフトウェア開発委託取引における受注チェックシート」を参考に、リスクを整理し確認して置くことの重要性について示された。

④ プロジェクト監査での指摘事項

実例に近い話として、プロジェクト監査時の指摘事項を紹介いただいた。「現行システム機能を踏襲」が前提条件であったが、肝心の現行システム機能が分かる人やものが十分ではない。2つの商談が発生しており、双方とも提案しないといけないが2つとも受注すると SE 体制が十分に取れない。別ベンダーが途中まで実施した作業を引き継いで作業する条件であるが、前行程の作業品質が不明である。と言ったものであった。

⑤ システム開発プロジェクトの成功とは

そもそもシステム開発プロジェクトが成功するとはどういうことかと言う問いに対して、「QCD 目標の達成」をベースに、「要求通りシステム」を構築し、「システムの安定稼働」を支え、「業務がうまくいく」ことを担保する。これにより、「関係者が満足」する。これがプロジェクトの成功であると説明されていた。

⑥ 会場からの意見

- ・社内でのプロジェクトの成功とはコストを抑えてシステムを構築すること。ある意味、監査を端折っても結果が良ければそれで良いとする風潮がある。ここをなんとかしたと思っており、普及に努めたい。
- ・システム監査の多様性はシステムが多様化してきていることによると思う。システム監査が経営にどう貢献

できるかをアピールする必要がある。

- ・プロジェクト成功の定義は難しい。経営がプロジェクト発足時に何を指すのかを表明できるかにかかってくると思っている。システム監査は一番のリスクに対し保証が与えられることが重要ではないか。
- ・多様性に対応するためには、システムよりも人を監査できるかが重要ではないかと考える。
- ・監査は時代の影響を受けると感じている。監査には幅広い知識を得ておく必要があると思う。
- ・システム監査が多様化してきており、監査人のスキルも多様化を求められている。例えば公認医療監査人の様な専門監査人制度が必要ではないか。システム監査を定着するためには経営者への訴求が必要と考える。CIO へ向けたシステム監査の普及活動が必要ではないか。
- ・個人経営者や中小企業には実はお金がある。社員の福祉など目に見えるものにはお金を出すが、目に見えないものにお金を出さない。このため、システム監査にはお金がつかない。システム監査を経営者に説明できるようにしなければいけない。例えば、システム監査をすると儲かる、監督官庁から求められる、ISO のように第三者へアピールできる。など、外に向けた発信が必要と感じている。

6. 所感

システム監査に限らず、システムを取り巻く環境はめまぐるしく変化し、開発者や運用者はそれに追いつくのに精一杯となっている。このような現状に対してシステム監査人として、どのような貢献ができるであろうか。日々業務に邁進するシステムに携わる方々に、外部からの客観的な視点を持ち込むことにシステム監査人としての存在意義があるのではないだろうかと改めて感じた。

個人として研鑽に励むのはもとより、定例研究会等に参加して監査人同士のつながりを広げることも大切ではないかとこの度の会を通して感じた。また、他の参加者の自分と異なる視点からの意見も大変参考になり、非常によい刺激となった。

以上



河津桜

写真提供: 仲会長

[< 目次 >](#)

注目情報 (2016. 1～2016. 2)**■【 情報処理安全確保支援制度(案) を公表 】 経済産業省 平成28年1月**

以下に概要を掲載しますが、法律改正は完了し、資格を作ることは決定しているようですが、まだ制度の詳細については決まっていないとのことです。(WG情報)

【情報セキュリティ人材の育成確保について(中間報告)】

- ・「実践的な能力を適時適切に評価できる試験制度の充実を図る」(「日本再興戦略」)を踏まえ、良質な情報セキュリティ人材の供給のために、情報セキュリティスペシャリスト試験をベースとした登録制度の創設を目指す。

【情報処理安全確保支援制度の創設】

- ・政府機関や企業等のセキュリティ対策強化に向けては、専門人材の確保・育成が肝要であるが、その数は国全体で不足している。
- ・現在、IPAや民間団体によりセキュリティの能力を測る試験が複数実施されているものの、人材の所在が見える化されておらず、日進月歩のセキュリティ知識を適時・適切に評価できるものとなっていない。
- ・最新のセキュリティに関する知識・技能を備えた、高度かつ実践的な人材に関する国家資格である「情報処理安全確保支援制度」を創設。

【情報処理安全確保支援試験】

- ・情報処理安全確保支援以下、「情確士という。)試験は、情確士として安全な情報システムを設計、開発、運用するために必要な情報セキュリティに関する知識・技能を有するか否かを評価する。
- ・新設する情確士試験については、試験実施時点の最新の情報セキュリティの知識・技能を測定しているSC試験

をベースに情確士試験を新設し、情確士として必要となる情報セキュリティの知識・技能を有するか否かの評価することとする。

【情報処理安全確保支援士の登録制】

- ・情確士制度では、政府機関や企業等の情報セキュリティ対策を強化するため、情確士を見る化し、活用できる環境とするため、情報処理安全確保支援士登録簿(以下、「登録簿」という。)を整備するとともに、登録事項の公開を行う。
- ・登録事項の公開に関しては、可能な限り情確士を見える化し、企業等で活用できる環境とすることが重要である。一方で、情確士が企業内で従事する業務の性質上、情確士個人がサイバー攻撃等の標的となることも想定されることから、こうした点を十分に留意しつつ、登録事項の公開方法を検討する必要がある。

詳細は、以下のURLにアクセスして下さい。

http://www.meti.go.jp/committee/sankoushin/shojo/johokeizai/shiken_wg/pdf/001_04_00.pdf

[< 目次 >](#)

■ プレス発表

【「情報セキュリティ10大脅威 2016」を発表】

2016年2月15日

独立行政法人情報処理推進機構

IPA(独立行政法人情報処理推進機構、理事長:富田 達夫)は、情報セキュリティ上の脅威のうち、2015年に社会的影響が大きかったトピックなどを「10大脅威選考会」の投票によりトップ10を選出し、「情報セキュリティ10大脅威2016」として順位を発表しました。

URL:<https://www.ipa.go.jp/security/vuln/10threats2016.html>

「情報セキュリティ10大脅威 2016」は、2015年に発生し、社会的に影響が大きかったと考えられる情報セキュリティの脅威に関する事故・事件から選出したものです。また選出は、情報セキュリティ分野の研究者、企業の実務担当者など69組織108名のメンバーからなる「10大脅威選考会」の審議・投票を経たものです。

今回は従来の総合的な10大脅威とは別に、影響を受ける対象の違いから「個人」と「組織」という新たに2つの分類で10大脅威を選出しました。

「情報セキュリティ10大脅威 2016」個人別・組織別 順位 ()内は総合順位、(ー)はランク外です。

個人（カッコ内は総合順位）	順位	組織（カッコ内は総合順位）
インターネットバンキングやクレジットカード情報の不正利用（1位）	1位	標的型攻撃による情報流出（2位）
ランサムウェアを使った詐欺・恐喝（3位）	2位	内部不正による情報漏えい（8位）
審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ（7位）	3位	ウェブサービスからの個人情報の窃取（4位）
巧妙・悪質化するワンクリック請求（9位）	4位	サービス妨害攻撃によるサービス停止（-）
ウェブサービスへの不正ログイン（5位）	5位	ウェブサイトの改ざん（6位）
匿名によるネット上の誹謗・中傷（-）	6位	対策情報の公開に伴い公知となる脆弱性の悪用増加（10位）
ウェブサービスからの個人情報の窃取（4位）	7位	ランサムウェアを使った詐欺・恐喝（3位）
情報モラル不足によるサイバー犯罪の低年齢化（-）	8位	インターネットバンキングやクレジットカード情報の不正利用（1位）
職業倫理欠如による不適切な情報公開（-）	9位	ウェブサービスへの不正ログイン（5位）
インターネットの広告機能を悪用した攻撃（-）	10位	過失による情報漏えい（-）

[< 目次 >](#)

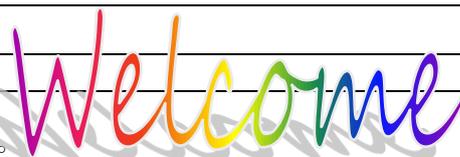
【協会主催イベント・セミナーのご案内】

■月例研究会（東京）

第 2 1 1 回	日時:2016年3月2日(水曜日) 18:30~20:30 場所:機械振興会館 地下2階 ホール
	テーマ 「クラウドサービスのセキュリティ規格 ISO/IEC27017」
	講師 特定非営利活動法人日本情報セキュリティ監査協会(JASA) 事務局長 永宮 直史 氏
	講演骨子 2015年12月に発行されたISO/IEC27017は、経済産業省の「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ン」を下敷きに、日本が提案し、規格化されたものです。ISO/IEC27002をベースに、クラウドサービス固有の管理策や実施の手引きを記載したISO/IEC27017の狙いやその特徴を解説します。
	お申込み 日本システム監査人協会ホームページ http://www.saaj.or.jp/kenkyu/kenkyu/211.html
第 2 1 2 回	日時:2016年4月25日(月曜日) 18:30~20:30 場所:機械振興会館 地下2階 ホール
	テーマ 「企業IT動向調査2016(15年度調査) ~データで探るユーザー企業のIT動向~」 (仮題)
	講師 一般社団法人 日本情報システム・ユーザー協会 常務理事 浜田 達夫 氏
	講演骨子 詳細確定次第、HPでご案内いたします。
第 2 1 3 回	日時:2016年5月26日(木曜日) 18:30~20:30 場所:機械振興会館 地下2階 ホール
	テーマ 「IoTって何? ~IoTによるイノベーションとその課題~」(仮題)
	講師 独立行政法人 情報処理推進機構(IPA) 調査役 田丸 喜一郎 氏
	講演骨子 詳細確定次第、HPでご案内いたします。

< 目次 >

【 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。



ご確認
ください

- ・協会活動全般がご覧いただけます。 <http://www.saa.or.jp/index.html>
- ・会員規程にも目を通しておいてください。 http://www.saa.or.jp/gaiyo/kaiin_kitei.pdf
- ・皆様の情報の変更方法です。 <http://www.saa.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.saa.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.saa.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、見学也大歓迎です。



ご意見
募集中

- ・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。



出版物

- ・協会出版物が会員割引価格で購入できます。 <http://www.saa.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.saa.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.saa.or.jp/csa/index.html>



会報

- ・PDF会報と電子版会報があります。 (http://www.saa.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.saa.or.jp/members/kaihouinfo.pdf>



お問い合わせ

- ・右ページをご覧ください。 <http://www.saa.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 >](#)

【 SAAJ 協会行事一覧 】 赤字：前回から変更された予定			2016.2
2016 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	8: 総会資料(※) 16:00 13: 総会・役員改選の公示 14: 理事会:通常総会資料原案審議 20: 2015 年度決算案 23: 2015 年度会計監査 28: 総会申込受付開始(資料公表) 31: 償却資産税・消費税	1-31:CSA・ASA 更新申請受付 20: 春期 CSA・ASA 募集案内 [申請期間 2/1~3/31] 21: 第 210 回月例研究会	8: 会計:支部会計報告期限 25: SAAJ 創立記念日
2 月	4: 理事会:通常総会議案承認 25: 法務局:資産登記、活動報告提出 理事変更登記 29: 年会費納入期限	1~3/31:CSA・ASA 春期募集	22: 第 15 期通常総会・特別講演 個人情報保護委員会 委員長 堀部 政男 氏
3 月	1: NPO 事業報告書、役員変更届東京 都へ提出 7: 年会費未納者宛督促メール発信 10: 理事会	2: 第 211 回月例研究会 5-6: [事例研] 第 27 回システム監査実務 セミナー(前半) 上旬:CSA・ASA 更新認定書発送 19-20: [事例研] 第 27 回システム監査実 務セミナー(後半)	
4 月	14: 理事会 末日 法人住民税減免申請	初旬 新規 CSA・ASA 書類審査 中旬 新規 ASA 認定証発行 25: 第 212 回月例研究会	予定:春期情報技術者試験
5 月	12: 理事会 26: 年会費未納者宛督促メール発信	中旬 認定委員会:新規 CSA 面接 26: 第 213 回月例研究会	
6 月	2: 会費未納者督促状発送 9: 理事会 10~: 会費督促電話作業(役員) 末日 支部会計報告依頼(※切 7/14) 末日 助成金配賦額決定(支部別会員数)	10:認定委員会:CSA 面接結果通知	2015/6/3:認定 NPO 法人認定
2015 年	過去に実施した行事一覧		
7 月	8 日 支部助成金支給 9 日 理事会	1 日 秋期 CSA・ASA 募集案内 [申請期間 8/1~9/30] 14 日 第 204 回月例研究会 20 日 認定委員会:CSA 認定証発送	14 日 支部会計報告※切
8 月	(理事会休会) 29: 中間期会計監査	1: 秋期 CSA・ASA 募集開始~9/30 24: 第 205 回月例研究会	
9 月	10: 理事会	15: 第 206 回月例研究会	5-6: 西日本支部合同研究会 (開催場所:岐阜)
10 月	8: 理事会	23: 第 207 回月例研究会	18: 秋期情報処理技術者試験
11 月	12: 理事会 13: 予算申請提出依頼(11/30※切) 支部会計報告依頼(1/8※切) 18: 2016 年度年会費請求書発送準備 25: 会費未納者除名予告通知発送 30: 本部・支部予算提出期限	中旬:秋期 CSA 面接 19: 第 208 回月例研究会 20: CSA・ASA 更新手続案内 [申請期間 1/1~1/31] 27: CSA 面接結果通知	
12 月	1: 2016 年度年会費請求書発送 2016 年度予算案策定 10: 理事会:2016 年度予算案 会費未納者除名承認 第 15 期総会審議事項確認 11: 総会資料提出依頼(1/8※切) 15: 総会開催予告揭示 18: 2015 年度経費提出期限	10: CSA/ASA 更新手続案内メール 14: 第 209 回月例研究会 18: 秋期 CSA 認定証発送	

< 目次 >

【 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

2016 年度の年間テーマ:「システム監査の活性化」、四半期テーマ:システム監査の課題(2016.2~2016.4)に決まりました。

システム監査人にとって、報告や発表の機会は多く、より多くの機会を通じて表現力を磨くことは大切なスキルアップのひとつです。良識ある意見をより自由に投稿できるペンネームの「めだか」として始めたコラムも、投稿者が限定されているようです。また記名投稿のなかには、個人としての投稿と専門部会の報告と区別のつきにくい投稿もあります。会員相互のコミュニケーション手段として始まった会報誌は、情報発信メディアとしても成長しています。

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、投稿ボタ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 (「会報掲載論文募集要項」及び「会報掲載論文審査要綱」があります)

□■ 会報投稿要項 (2015.3.12 理事会承認)

- ・投稿に際しては、Wordの投稿用フォーム(毎月メール配信)を利用し、会報部会 (saajeditor@saaj.jp)宛に送付して下さい。
- ・原稿の主題は、定款に記載された協会活動の目的に沿った内容にして下さい。
- ・特定非営利活動促進法第2条第2項の規定に反する内容(宗教の教義を広める、政治上の主義を推進・支持、又は反対する、公職にある者又は政党を推薦・支持、又は反対するなど)は、ご遠慮下さい。
- ・原稿の掲載、不掲載については会報部会が総合的に判断します。
- ・なお会報部会より、表現の訂正を求め、見直しを依頼することがあります。また内容の趣旨を変えずに、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。

会報記事は、次号会報募集の案内の時から、締め切り日の間にご投稿ください。

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：認定 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、会員期間中は、会員へ配布されます。

会員の所属や登録メールアドレス等の変更は、当協会ホームページ会員サイトより変更してください。

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。

【会員でない方の送付停止】 <http://www.skansanin.com/saaj/register/>

Copyright(C)2016、認定 NPO 法人 日本システム監査人協会

掲載記事の転載は自由ですが、内容は改変せず、出典を明記していただくようお願いします。

■□■ 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、高橋典子、西宮恵子、藤野明夫

編集支援：仲厚吉 (会長)、各支部長

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)

[< 目次 >](#)