認定NPO法人
# 日本システム監査人協会報
2017年12月号
No.201
No.201（2017年12月号）<11月25日発行>

今月号から四半期テーマは

**「システム監査人に求められる能力」**です。

写真提供：仲会長

## 巻頭言

### 「公認システム監査人認定制度の特別認定制度改定について」

**会員番号　1750　舘岡均（副会長）**

公認システム監査人認定制度発足から１５年が経ており、会員の多くの方が、公認システム監査人（CSA）、システム監査人補（ASA）となって、活動を発展されておられますこと、誠にご同慶の至りです。

おかげ様にてCSA／ASAは、官公庁、監査法人、教育機関、銀行、ITベンダー、一般企業等々のように多くの組織において活躍しています。また中立な立場が重視される第三者評価委員、弁護士、会計士、大学／大学院教授・講師、組織のCIO補佐官、IT統制の監査人、PMO、プロジェクト監査人、等々の職務にても活用されるようになってきています。

会員の皆様には既にご存知のように、さらに発展を期して「公認システム監査人認定制度の特別認定制度」を、この度2017年6月8日に改定いたしました。制度発足時からこれまで、社会とその要請の変化に対応して、活発に活動して成長している他団体の資格についても、「特別認定制度の対象資格」に加えて、CSA／ASA になるためのキャリアパスを広げ、SAAJに参加するプロフェッショナルの幅を広げて、切磋琢磨し、相乗効果によりCSA／ASAのさらなる発展を目指しています。

具体的には、「特別認定制度の対象資格」に新たに、情報処理安全確保支援士、米国公認会計士、内部監査人、QMS主任審査員／エキスパート審査員、公認情報セキュリティ監査人、を加えました。その結果、協会ホームページ「お問い合わせ」による確認および相談、さらには今年度の秋期資格認定申請においてASA認定実績がありました。

つきましては、会員の皆様におかれましても、CSA／ASAにふさわしい方々に資格をご勧奨下さり、CSA／ASAの発展および当協会の発展にご支援を賜りますようよろしくお願い申し上げます。

以上

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。

# <目次>



注目記事

2017.11

**めだか【システム監査人に求められる能力】**

多くの組織、事業者は、事業目的の達成を効果的に行うために、マネジメントシステムを運用し、システム監査は、マネジメントシステムの「PDCA サイクルの枠組み」で、IT にかかわる「C」の役割である。マネジメントシステムの運用は、網羅的に対策を講じるよりも、目的達成の効果を考え、リスクを洗い出して対応するアプローチをとることが多い。リスクアプローチでは、ステークホルダーとの「コミュニケーション及び協議」による「組織の状況の確定」から、「リスクアセスメント」、「リスク対応」、そして「モニタリング及びレビュー」のプロセスをとる。

マネジメントシステムでいう「原則」は、“Principle”の訳であるが、望ましい考え方や、結果としてあるべき姿の提示である。「マネジメントシステム監査のための指針（JIS Q 19011:2012）」は、監査の原則として、「高潔さ」、「公正な報告」、「専門家としての正当な注意」、「機密保持」、「独立性」、「証拠に基づくアプローチ」の６原則を示している。

情報技術サービスのマネジメントシステム（ITSMS）は、「情報技術－サービスマネジメント－第１部：サービスマネジメントシステム要求事項 JIS Q 20000-1:2012」と「情報技術－サービスマネジメント－第２部:サービスマネジメントシステムの適用の手引き JIS Q 20000-2:2013」で標準化されている。本規格は、１適用範囲、２引用規格、３用語及び定義、４サービスマネジメントシステムの一般要求事項、５新規サービス又はサービス変更の設計及び移行、６サービス提供プロセス、７関係プロセス、８解決プロセス、９統合的制御プロセス、で構成されている。情報技術サービスにおいてシステム監査を行う場合に基準となる規格であり、基本を理解しておきたい。

システム監査人に求められる能力は、日進月歩の情報技術に関する知見であるし、自分の「強み」を見つけて、システム監査人として「切磋琢磨」していく性質であると思う。参考資料を読むと、“競争で強みを見つける”ことの重要性を説いている。また、“個人も企業も、競争のプレッシャーから自分だけが逃げ切ろうとしていては、社会は衰退するばかりである。弱者への配慮は必要だが、競争を弱めるための一律の規制は、競争のメリットを損なうことになりかねない。規制が競争を促進し継続させるためのものであるかどうか－そのルール作りをするのが政府の役割であり、適切な判断のために有効な情報を提供するのが経済学の役割である”、と書いている。システム監査人には、日進月歩の情報技術を「共に学ぶ」ことと、自分の「強み」を見つけて「切磋琢磨」するという二つの能力が求められている。（空心菜）

参考資料：「競争社会の歩き方 自分の「強み」を見つけるには」大竹文雄著 中公新書 2447

（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>

2017.11

**投稿【システム監査の新たな展開】**

会員番号 0557 仲厚吉 （会長）

当協会は、システム監査の普及・促進を図るため 1987 年 12 月 12 日に設立され、30 年の活動実績があります。この 30 年で、システム監査人が係わる業務は、情報処理システム監査から、情報システムの品質管理、情報セキュリティ、内部統制における IT リスクとコントロール、個人情報保護、サイバーセキュリティ、そしてビッグデータと AI などに展開してきました。また、協会ではシステム監査人が職業倫理をもって行動するように「システム監査人倫理規定」を制定しています。システム監査の新たな展開は続いていきますが、システム監査人倫理規定の遵守は、変わらずに大切なものです。「システム監査人倫理規定」抜粋を以下に示します。

第 1 条（目的）この規定は、システム監査人が最低限遵守すべき職業倫理の規範を定めることを目的とする。
第 2 条（使命）システム監査人は、情報システムの信頼性・安全性・効率性・有効性を高めるため、その専門的知識と経験に基づき誠実に業務を行い、情報化社会の健全な発展に寄与することを使命とする。
第 3 条（責務）システム監査人は、情報システムを総合的かつ客観的に点検・評価し、関係者に助言・勧告するものとする。
第 4 条（監査基準・手続き）システム監査人は、システム監査の基準、手続きを明らかにし、それに基づきシステム監査を行わなければならない。
第 5 条（監査報告）システム監査人は、監査結果の報告にあたって、知り得た全ての重要な事実を明らかにするものとする。
第 6 条（守秘義務）システム監査人は、正当な理由なく業務の遂行に伴い知り得た機密情報を他に漏洩し、または窃用してはならない。
第 7 条（独立性）システム監査人は、常に独立の立場を堅持しつつ、適切な注意と判断によって業務を遂行し、特定人の要求に迎合するようなことがあってはならない。
第 8 条（公正不偏）システム監査人は、業務を誠実に果たし、常に公正不偏の態度を保持しなければならない。
第 9 条（社会的信頼の保持）システム監査人は、自らの使命の重要性に鑑み、高い社会的信頼を保持するよう努めなければならない。
第 10 条（名誉と信義）システム監査人は、深い教養と高い品性の保持に努め、システム監査人としての名誉を重んじ、いやしくも信義にもとるような行為をしてはならない。
第 11 条（システム監査人間の規律）システム監査人は、みだりに他のシステム監査人を誹謗し、名誉を傷つける等の行為をしてはならない。
第 12 条（自己研鑽）システム監査人は、システム監査を行うのに必要な専門能力および監査技術の向上に努めなければならない。

当協会は、「不易流行」、つまり、変わらず大切にするものを維持し、変わっていくものには素早く対応する活動を続けていきます。会員の皆様のご協力をお願い致します。

<目次>

2017.11

**時事論評【アゲインストクラウド化する世界】**

会員番号　0707 神尾博

1.クラウドの限界?

電力供給は原発や火力といった大規模集中から、スマートグリッド等の中小規模分散へ。一方で IT はさらにクラウド化が進むという、定説/通説を信奉されている方も多いはずだ。実は私も、数年前（2012 年）頃はこれを支持していた。ところが、その後に入手した数々の情報から、最近は IT のクラウド化への邁進については、懐疑的なスタンスに移ってきている。むしろ、その正反対で、雲への逆風が烈しくなっているという「Against Cloud」を支持・主張する立場だ。専門家の間では通信量や機密性等の限界がささやかれ始めた一方で、巷では今後もクラウド化に拍車がかかるといった意見も相変わらず健在だ。果たして真実は何処に？この場を借りて、いくつかの観点からこの命題を考察してみたい。

2. Capacity（負荷）の問題

InternetWorldStats.com によると、2016 年 6 月末時点でのインターネット人口は、某女性お笑いタレントの「35 億!」も凌駕する 38.4 億人とされている。また 2017 年には、スマホ等のモバイルデバイス数は、すでに人類の総人口を超えているという。こうした利用の急激な拡大、データ量の激増により、世界中に張り巡らされたネットの伝送能力が、限界に近付いているという説をご存じだろうか？

英国王立協会の発表ではそのタイミングは 2023 年頃であり、ベル研究所のホフマンによると、もう数年早い時期だとされている。伝送能力は通信路の帯域幅と S/N 比によって決定する、シャノン限界によるものだという。当然ながら、全世界に張り巡らされた光ファイバー網の伝送能力も、この制約から逃れることはできないとされていた。

ところが 2015 年にはカリフォルニア大学サンディエゴ校の研究チームが、この速度限界の突破に成功したと発表している。もっともこの技術の採用にしろ、現状スペックでの網の増強にしろ、インフラとして機能し始めるには、設備敷設までのタイムラグがあるため、別の手立ても不可欠だという。

たとえば、データをそのままネットに流すのではなく、あらかじめタグ付けした後の中継ノードでの取捨選択や、リアルタイム性の要求度によるネットワーク上での処理の仕分け等の仕組が、提唱されている。フォグコンピューティング/エッジコンピューティングでの、一旦 IoT ゲートウェイにデータを集約し IP 網に中継するという形態も、その一例と言えるだろう。このように通信データの中味を区分せず何でもかんでもクラウドというのは、すでに見直され始めている。

3. Confidency（機密性）の問題

2013 年のスノーデンの暴露による、NSA(米国国家安全保障局)のネット上のありとあらゆる通信記録の盗聴・収集活動は、全世界に衝撃を与えた。私自身はその時点で、すでに 2011 年刊行の、米国防総省の元幹部による文献によって、サイバーセキュリティの観点からの ISP（Internet Service Provider）での通信監視の可能性については既知だったため、さほどのインパクトは受けなかったと記憶している。

これで、クラウド上にデータを置かないに越したことは無い、また通信路は暗号化だ（実はこれすら怪しいが）といった機運が一気に広がった。さらには NSA が収集データを集約して保管していたという事実が、別の方策の重要性も示唆しているという。それはクラウド/オンプレミスにかかわらず、用途が異なるデータは、分散しておく方が賢明だということである。たとえば企業の場合は、人事データと財務データ、取引先データと電子メール等の関連性の低いデータは、それぞれ仮想化を用いてネットワーク分離したり、物理的に別のロケーションに配置したりして被害の局所化を図るというものだ。

不要な大規模データの収集や、DLP（Data Loss Prevention）の細緻すぎる設定等による過剰な情報封鎖も見直され始めている。2013 年頃からセキュリティベンダーが「王冠の宝石」と呼び、最重要な情報を徹底して絞り込むことが先決であると唱えるようになってきた。

一方で、個人用途でもこの流れの「パーソナルクラウドストレージ」と称する製品が、発売されている。出先から自宅に設置した NAS にアクセス出来るというもので、クラウドサービスのような運用費や会員登録は不要である。こうしたコモディティ化は、クラウド嫌いには吉報だろう。

4. Dependability（信頼性）の問題

ISO では一般に知られている「Reliability」に対し、保全性や可用性も含めた広義の信頼性を「Dependability」と定義している。クラウドベンダー、特に大手はこの信頼性も高いと印象付けられており、実際そのようだ。これがクラウドの普及拡大を後ろ押ししていた一要因だろう。

ところが最近では、サーバ、ストレージ、ネットワーク、管理ソフトウェアを統合・パッケージ化した HCI（ハイパーコンバージドインフラ）の登場により、事情は変わりつつある。とにかくシステムの立ち上げが非常に速い。各ベンダーは「梱包を解いて数十分から数日」などと PR している。また管理ツールが洗練され、運用/保守のスキル確保やコストの圧縮にも寄与できる。さらには必要最小限のリソースで開始して、需要に応じ拡張するというスケーラビリティもクラウドの利点であったが、HCI はこちらもクリアしたようだ。こうした状況を受けて、実際に各所でオンプレミスへの回帰の傾向もあるという。

またデータ破損の際のバックアップの古さを表す、目標復旧地点（RPO）がゼロの実現を標榜する製品もあり、システム障害等からの回復力の優秀さがうかがえる。HCI に加えて、機械学習によるハードウェア系以外の自動復旧技術が向上すれば、インシデントや災害時等においても、そうしたインフラの導入で、労せずして事業継続ができるケースが増えるだろう。

5. Survivability（抗堪性）の問題

インターネットは ARPANET に端を発するが、その開発過程で迂回路を持つパケット方式の通信形態が採用された。一般に流布している「元々は軍事目的の研究」ではなかったようだが「一部が損傷しても自律的なルーティング」というアーキテクチャは、抗堪性（こうたんせい）に優れていると言えよう。しかしその後の商用サービスの爆発的拡大により効率性を重視したため、通信会社の基地局（以下、「局」）を中心としたスターネットワークが基幹となってしまった。局の設備や局間の伝送路の能力強化に集中投下することにより、急激な通信量の増加に対応できるというメリットは大きい。しかし一方で弊害も顕在化している。

そのひとつが、権力者によるネットへの接続制限だ。2011 年のエジプト革命では、政府による国民へのネット遮断が行われた。大手 ISP 数社に命令し、ユーザの 90%以上をアクセス不能に追いやったのである。ISP のブロック開始はわずか数分、完了までは数十分程度。この事件でスター型そのものが、結果的に民主主義社会のハザードソース（危険源）であることが実証された。これはクラウドへの集中においても同様のはずだ。

もうひとつは地震等の自然災害の脅威だ。日本の IX（Internet Exchange）は、東京の大手町に集中しており、ここが壊滅すると海外のクラウドサービスも実質的に使えなくなる。また、同じ地域の携帯電話や有線通信は、同一局を経由することに変わりはない。したがって「システム/データの海外クラウドへの配置や、同一エリア内での通信経路の有線/無線での冗長化は、災害時に有効」は、素人同然の妄言であると心得ておきたい。

これに対し、端末が中継機能も担うことで局を介さないメッシュ型（無線の場合はアドホック型）の優位性が、各方面で評価されている。特に携帯電話同士での中継は圧倒的な抗堪性実現の可能性があるが、ノード自体が絶えず移動することによるルーティングの問題や、経路を冗長化する場合の、通信量の負荷とパケット到達可能性とトレードオフ等、本格的な普及にはまだまだ課題が多い。

6.システム監査人も限界？

さて、クラウドコンピューティングの歴史を紐解くと、Google、Amazon、Microsoft が本格的な商用サービスを開始したのは 2008 年、プライベートクラウドの本格普及は数年の遅れ。これが今の 2017 年にとって何を意味するか？HCI やエッジコンピューティングといった新技術の勃興の項でも触れたように、当時の「10 年後を見据えた IT インフラ」という謳い文句は、いよいよ怪しくなってきたといえよう。

これから先についても、データセンターでの処理がデータベースサーバ、Web サーバ、メールサーバ中心から、GPU （Graphics Processing Unit）による機械学習へというパラダイムシフトを考え合わせれば、当て推量はなおさら危険だ。

このことは「経営に役立つシステム監査（あるいは IT コンサル）」の標榜は、常に技術革新をキャッチアップすることが前提、いやそうであってもパラダイムシフトの時代には無力である可能性も高いことを心得ておくべきだろう。それができない輩がいるなら、もはや彼らの力量は限界であり、これからの伸び代すら疑わしい。

最後にこの場を借りて、本稿をレビュー頂いた安本哲之助氏、そして執筆の参考にさせて頂いたコラムや文献の著者である、多士済々な欧米の科学者や識者には敬意を表したい。

（このコラム文章は、記事提供者の個人的な意見表明であり、SAAJ の公式見解ではありません。写真は著者撮影です。）

<目次>

2017.11

## エッセイ【チョウのコピー天国】

会員番号　2089 阪口博一

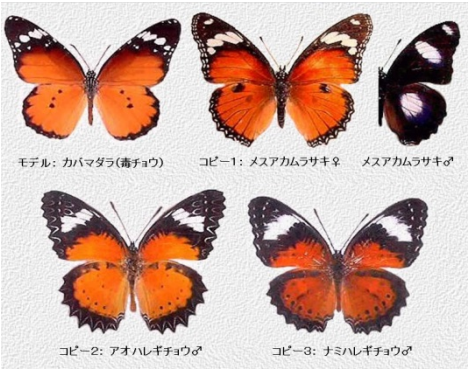
「擬態」という言葉をご存じだろうか。葉や花、枝に似せた姿で環境に溶け込み、捕食者に見つけられないように隠蔽的な姿になることをいうが、逆に目立つ擬態も存在する。チョウを例にとっても、種類が多い熱帯地方では、まさしく「コピー天国」といった感じで、同じ派手な模様を持った何種類ものチョウが同じところを飛び回って、分類学者を困惑させている。

翻って、企業内にもコピーの氾濫が見られる。監査をしていると、手がけたプロジェクトの障害、不具合などインシデント記録として、個人情報などの複写を個人所有し保存している事例が観察される。以前は紙媒体であったが、今はオリジナルとともにデジタルファイルとして保管されることが多くなった。尋ねてみると、自分が拘わったプロジェクトにかかるネガティブデータは、何かの折に必要になるかもしれないので、手元に保存したい。正当な記録が保管されていても、面倒な手続きが必要で、アクセスに手間が掛かるなどの理由から控えを保存するのだという。本人曰く、機密性については「物理的、技術的セキュリティ施策は十分に考慮している」と主張する。しかしその量が半端なく、もはやどれが本当に重要かの選別がされておらず、また、組織全体としての可用性、完全性を考慮しているとは考えられない。

チョウのコピーには生死にかかわる理由がある。一般的に「毒」を持つ生物は派手な色をしていることが多いが、これは「警戒色」と呼ばれ、捕食者に自己が危険であることを誇示する。さらに進んで、毒のあるもの同士が互いに似通っていると、捕食者の側からすると、「とにかくああいう模様のやつは、みんな毒を持っている」と認識することになるので、擬態の効果が高まると考えられている（これは「ミューラー型擬態」と呼ばれる）。そうすると毒を持たないものも、この模様を真似ると補食から免れることになるので同じような模様に進化する（こちらは「ベイツ型擬態」と呼ばれる）と考えられている。

さて、人間世界に戻って、コピーが氾濫する理由は、大きく２つあると考える。ひとつは、何でも手元にないと安心できない個人の資質であり、もうひとつは実際に必要となった場合に、簡単にアクセスできないという可用性の問題である。重要なデータが厳重に保管されるというのはもちろん必要であるが、一方でアクセス権限を適切に設定し、過去のデータが死蔵されることなく、いつでも利用可能となっていなければ、保有している意味がない。

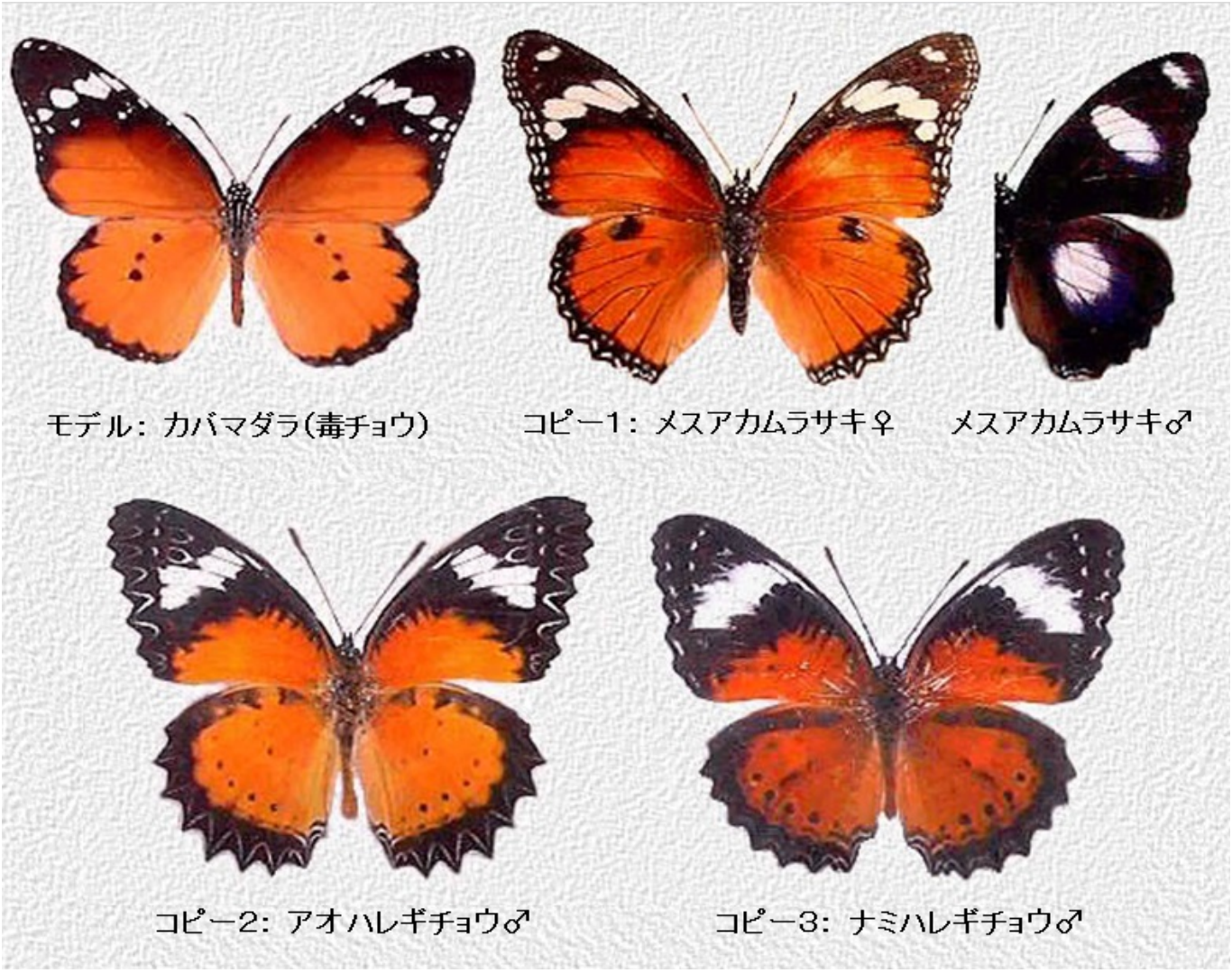
監査人としては、個別保管を制限した上でデータベース化し、適切なアクセス制限のもと、社員に公開し有効利用できるよう提案するのが正しい方向性であろう。熱帯の島々では、真似る方のチョウは、コピー元となる毒チョウの種類に倣い、島毎に模様が多様に変化するらしい。組織も自己の環境に適応し、しなやかな進化と適応を期待する。




（このエッセイは、記事提供者の個人的な意見表明であり、SAAJ の公式見解ではありません。画像は著者撮影です。）

<目次>

＜拡大画像＞


モデル：カバマダラ(毒チョウ)
コピー1：メスアカムラサキ♀
メスアカムラサキ♂
コピー2：アオハレギチョウ♂
コピー3：ナミハレギチョウ♂

2017.11

**法人部会報告　【　リテラ・クレア証券株式会社様　情報セキュリティセミナー　実施　】**

会員番号　7075 佐々野未知　（理事、法人部会）

法人部会では、2017 年 10 月 14 日（土）、リテラ・クレア証券様からの依頼を受け、情報セキュリティセミナーを実施しました。リテラ・クレア証券様は東京駅のすぐ近くに本社オフィスを構える、老舗の証券会社です。同社は東京の三澤屋証券（1947 年創業）と大阪の今川證券（1916 年創業）の合併により誕生し、2001 年にリテラ・クレア証券へと社名を変更、2013 年から大和証券グループの一員となられています。

情報セキュリティについては、年間計画に基づく内部講師による支店毎での研修実施や社内電子掲示板での注意喚起を行っているものの、年に 1 度全社員が集まる場で専門家による研修を行うことにより、改めて「情報セキュリティの重要性」を再認識し、対応に万全を期す機会としたいということで、今回の情報セキュリティセミナーを企画されたとのことです。会場は TKP 東京駅八重洲カンファレンスセンターの会議室で、同社役職員約 120 名の皆様が受講されました。講師は当協会理事で法人部会の佐々野未知が務めました。セミナーの時間は 60 分で、事前に主催者である経営企画部企画課様のご要望をお伺いした上で、以下のような内容としました。

１．情報セキュリティとは　～基本知識と概念の整理

1-1　情報セキュリティとは？　1-2　情報セキュリティの脅威とリスク、インシデント

２．身近に潜む情報セキュリティの脅威とリスク

2-1　情報セキュリティの 10 大脅威 2017　2-2　マルウェア　2-3　パスワードクラック

2-4　標的型メール攻撃　2-5　水飲み場型攻撃　2-6　DoS 攻撃/DDoS 攻撃　2-7　Web 攻撃

３．情報セキュリティ対策はじめの一歩

3-1　情報セキュリティ対策の重要性・必要性

3-2　従業員が注意すべき 8 つのセキュリティ対策

(1)電子メールのルール、(2)無線 LAN のルール、(3) ウェブ利用のルール

(4)事務所の安全管理、(5)持ち出しのルール、(6)安全な情報の廃棄

(7)ソーシャルエンジニアリング対策、(8)SNS 利用時の注意点

3-3　コンピュータウィルス（ランサムウェア）に感染してしまったら

セミナーは、皆様最後まで熱心に受講してくださいました。終了後には「1 時間という短い時間でしたが、実例も交えた分かり易い説明もあり、受講者から非常に好評を得た。」とのご評価もいただきました。また、これまで社内研修や e-ラーニングを使用した研修は行っていたが、改めて外部講師による研修により、社員一人一人の情報セキュリティに対する知識と意識が深まることとなったとのことでした。

リテラ・クレア証券様の取組みにご協力できたことを、講師として、また当協会として大変に嬉しい気持ちをもって、セミナーを終了しました。今後のリテラ・クレア証券様のご発展を祈念致します。

<目次>

2017.11

**イベント報告【(2017 年度)関東地区主催　会員向けＳＡＡＪ活動説明会】**

会員番号　2581 斉藤茂雄（理事）

システム監査活性化委員会では、昨年に続き会員活動（会員同士のコミュニケーションを含む）活性化を目的に、SAAJ の各研究会・部会活動にご参加頂けるよう、「(2017 年度)関東地区主催会員向け SAAJ 活動説明会」を開催致しました。

昨年は直近 3 年間に新規ご入会いただいた関東地区会員の皆様をメインの対象者として開催しましたが、今年は特に限定せず全会員を対象に実施し、関東以外の支部からの 2 名を含む、23 名の方にご参加いただきました。

※他地区及び 2012 年以前入会の方にもご参加いただきました。

1．開催日時：2017 年 10 月 21 日(土)　13:30～19:00 (17:40～交流会)

2．開催場所：NATULUCK 茅場町 新館　2 階大会議室

3．参加者　：23 名(交流会 13 名)　理事 14 名

4．プログラム

| | 内容 | 時間 | 担当 |
|---|---|---|---|
| 13:30 | 開会の辞 (会長挨拶) | 5分 | 仲会長 |
| 13:35 | SAAJの研究会及び部会からの活動内容説明 | 55分 | 各主査 |
| 14:30 | 休憩 | 10分 | – |
| 14:40 | セミナー(1)<br>「発注サイドのプロジェクトマネジメントと監査」 | 80分 | 原田理事 |
| 16:00 | 休憩 | 10分 | – |
| 16:10 | セミナー(2)<br>「ITガバナンスのアセスメントとシステム管理基準の見直しについて」 | 75分 | 松枝副会長 |
| 17:25 | 閉会の辞　（挨拶） | 5分 | 力副会長 |
| 17:30 | 休憩(受講証明書配付　・アンケート回収、会場再セッティング) | 10分 | – |
| 17:40 | 交流会 | 80分 | – |
| 19:00 | 終了 | – | |

５．開催内容（司会：カ副会長）

最初に、仲会長より本説明会への参加の謝辞と主旨についてご挨拶いただきました。

5.1　SAAJ の研究会及び部会からの活動内容説明

研究会及び部会の主査より、目的・活動概要・メンバ・活動実績の紹介と共に、メンバの募集内容や参加メリットについて説明を行いました。

1. 会報部会～主査：藤澤理事
2. 法人部会～主査:加佐見理事
3. 月例研運営委員会～主査:カ副会長
4. システム監査事例研究会～主査:野田理事
5. 情報セキュリティ監査研究会～主査:舘岡副会長
6. ITアセスメント研究会～主査:松枝副会長
7. 個人情報保護監査研究会～主査:斎藤(由)副会長
8. PJM(プロジェクトマネジメント)のシステム監査研究会～主査:原田理事
9. 認定委員会～委員長：舘岡副会長
10. CSA利用推進グループ～主査:斉藤(茂)理事

5.2 セミナー(1)「発注サイドのプロジェクトマネジメントと監査」

PJM(プロジェクトマネジメント)のシステム監査研究会主査の原田理事より、標記タイトルで来春2月出版に向け執筆中の同名（仮題）の著作の紹介を交えて、システム開発プロジェクトの失敗事例とどうすれば失敗を未然防止できるかというテーマで講演いただきました。


プロジェクトの失敗事例、システム構築における調達の多段構造の開発プロジェクトでよくある問題、トラブルを未然防止するためのプロジェクトの各プロセスでの留意事項等々盛り沢山の内容でした。また、協会発行本の目玉として執筆している、プロジェクト監査についても、プロジェクト監査をどう考え、各開発プロセスの中にどう組み込み、何を見ていくかという「さわり」の紹介もありました。

5.3 セミナー(2)「ITガバナンスのアセスメントとシステム管理基準の見直しについて」

ITアセスメント研究会主査の松枝副会長より、ISO及びシステム管理基準の整備について講演いただきました。

ITガバナンスの国際規格である、ISO38500シリーズの現状、ISO38500、ISO38501、ISO38502、ISO38504の各概要に加え、ISO38500シリーズとISO/JISQ27014（情報セキュリティガバナンス）との関係などをお話いただきました。そして当協会が予てから制定に向けて尽力しているISO38503（ITガバナンスのアセスメント）の進捗状況と今後の方向性についても説明がありました。

次に、もう一つのテーマとして、現在経済産業省主導で進めている、「システム監査基準と管理基準の見直しプロジェクト」の状況、見直しの基本方針、基準改定に向けた今後の活動計画などについて紹介がありました。この見直し作業は、システム監査に関係した活動を行っている国内の4団体(システム監査学会、ITGI、ISACA、日本システム監査人協会)が共同で作業しており、当協会は委員会参画に加え、ワーキンググループにて、「システムの運用フェーズ」「アウトソーシング管理」などの重要な基準の見直しを分担して作業を進めているとの説明がありました。


6. 受講された皆様の声(アンケート結果：23 名)　－アンケート抜粋－

(1)SAAJ 研究会・部会：　未所属 21 名、所属済 1 名、昔所属していた 1 名

(2)活動内容説明で興味を持った研究会・部会　(複数回答)：

プロジェクトマネジメントのシステム監査研究会 8 名、情報セキュリティ監査研究会 6 名、
システム監査事例研究会 4 名、個人情報保護監査研究会 4 名、法人部会　2 名、
IT アセスメント研究会 1 名、ＣＳＡ利用推進グループ 1 名、検討する 1 名　等

(3)今後のウェルカム・イベント：　毎年開催希望　18 名、　隔年開催希望　2 名、

(4)全体の感想・ご意見：

- それぞれの研究会、部会の活動状況が、わかりました。
- 協会（公認システム監査人も）の認知度を上げるため、企業向けのセミナーを定期的に開催すべき。
- 貴重なご講演ありがとうございました。特に「発注サイド～」は参考になりました。
- 月例研究会では 2 時間と限られた時間でもあり、土曜日の昼などにまとまったレクチャーを受けられるのは内容も濃く、有難いと思います。

7. 所感

今回は 23 名の方にご参加いただき、昨年より若干増の開催となりました。セミナーについては両セミナー共に非常に好評で、特に「発注サイドの～」については活発な意見交換もあり、もっと時間が欲しかったというご意見や、本が出版されたら是非購入するという感想が複数ありました。「IT ガバナンス～」についても、基準の整備が具体化したら、再度セミナーを開催するよう要望がありました。

交流会には理事を含め 26 名の方が参加され、自己紹介や交流が盛況に行われました。今後も継続的に開催していくことにより、交流の場が広がっていくことが期待できる会合となったものと実感しております。

なお、アンケートの中に、イベントは土曜日に行って欲しいというご意見が複数ありました。多くの会員に対して協会活動への参加機会を広げ、システム監査の活性化を図って行く必要性を、改めて感じました。

以上

<目次>

2017.11

**注目情報（2017.10～2017.11）**

## ■「サイバーセキュリティに関する金融機関の取り組みと改善に向けたポイント― アンケート（2017年4月）調査結果 ―日本銀行金融機構局】

10月16日、日本銀行機構局は当座預金取引先金融機関のうち411先を対象に、サイバー攻撃の脅威や自社の対策状況などの現状に対する認識、経営資源の割り当てスタンス、実際のリスク管理状況などについて調査するため、実施したアンケート結果を公開した。

http://www.boj.or.jp/research/brp/fsr/fsrb171016.htm/

## ■「公衆無線LANセキュリティ分科会」の開催【総務省】

総務省では、本年10月に公表した「IoTセキュリティ総合対策」を踏まえ、サイバーセキュリティタスクフォースの下に「公衆無線LANセキュリティ分科会」（主査：後藤厚宏　情報セキュリティ大学院大学　学長）を設置し、公衆無線LANにおけるセキュリティ上の課題を整理し、必要な対策について、検討を行うことが、11月16日公表された。

http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000133.html

## ■「サイバーセキュリティ経営ガイドライン」【経済産業省】

経済産業省では、独立行政法人情報処理推進機構（IPA）とともに、大企業及び中小企業（小規模事業者を除く）のうち、ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するため、「サイバーセキュリティ経営ガイドライン」を策定しました。

サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3原則」、及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO等）に指示すべき「重要10項目」をまとめています。

http://www.meti.go.jp/policy/netsecurity/mng_guide.html

<目次>

2017.11

**【 協会主催イベント・セミナーのご案内 】**

**■SAAJ 月例研究会（東京）**

| | | |
|---|---|---|
| 第227回 | 日時：2017年11月27日（月曜日）18:30～20:30<br>場所：機械振興会館 地下2階ホール | |
| | テーマ | 「リスクマネジメントとシステム監査」 |
| | 講師 | 横浜国立大学　リスク共生社会創造センター　センター長<br>大学院　環境情報研究院　教授<br>工学博士　　野口　和彦　氏 |
| | 講演骨子 | リスクマネジメントは、好ましくない影響の減少から不確かな影響の最適化へとその活用が変化している。しかし、そのリスクを最適するマネジメントシステム自体にもリスクが存在する。<br>健全な経営には、マネジメントの健全性を確認しつつ高度化を目指すことが重要であり、マネジメントの持つリスクを的確に把握し改善することが求められている。<br>本講演は、最新のリスクマネジメントの要点を整理しつつ、マネジメントのＰＤＣＡへの適用を論じる。 |
| | お申込み | https://www.saaj.or.jp/kenkyu/kenkyu/227.html |
| 第228回 | 日時：2017年12月15日（金曜日）18:30～20:30<br>場所：機械振興会館 地下2階ホール | |
| | テーマ | 「事業者が考えるデータ利用及び今後の展望や課題」 |
| | 講師 | 日本情報経済社会推進協会　常務理事<br>電子情報利活用研究部担当（部長兼務）<br>認定個人情報保護団体事務局担当<br>坂下 哲也　氏 |
| | 講演骨子 | 官民データ活用推進基本法も成立し、データを利用したサービス検討が活発になっている。本講義では、最近のデータ利用を取り巻く産業界等の状況を俯瞰し、今後の展望や解決すべき課題について解説する。<br>１．データを利用したサービスの事例<br>２．官民データ活用推進基本法以後の動き<br>３．パーソナルデータに関する動き<br>４．パーソナルデータ以外のデータ活用と課題 |
| | お申込み | 近日、以下のＨＰでご案内いたします。<br>https://www.saaj.or.jp/kenkyu/kenkyu/228.html |

<目次>

2017.10

**【 外部主催イベント・セミナーのご案内 】**

**■ISACA 東京支部（東京）**

| | | |
|---|---|---|
| 2017年11月例 | 日時：2017年11月29日（水曜日）18:30～20:10<br>場所：（財）日本教育会館一ツ橋ホール<br>東京都千代田区一ツ橋2-6-2 TEL03-3230-2831 | |
| | テーマ | 平成 29 事務年度　金融行政方針（仮） |
| | 講師 | 金融庁検査局総務課<br>システムモニタリング長<br>片寄　早百合　様 |
| | 講演内容 | 平成29事務年度金融行政方針について解説する。 |
| | お申込み | ＨＰでご案内中です。<br>http://www.isaca.gr.jp/education/annai.html |

<目次>

2017.11

**協会からのお知らせ【 年会費請求書を発送 】**

会員番号　1760 斎藤由紀子　（事務局長）

会員各位

いつも、協会活動へのご協力を賜りありがとうございます。

早速ですが、会員規程に従い、2018 年度年会費の請求書を、2017 年 12 月 1 日付で発送いたしますので、ご準備のほどよろしくお願い致します。

【会員規程】　http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf

第３条（会費）：会員は、当該年度（１月～１２月）の年会費を、請求書に記載された期日までに支払わなければならない。いったん支払われた会費は返却しない。

**【2018 年度会費請求の内容】**

＜金額＞ 正会員個人：￥10,000－　　（非課税）

正会員団体：￥10,000.-　～　￥100,000.-　（非課税）

＜払込期限＞2018 年 2 月末日

なお、正会員団体に限り、「納付期限延長願い」をご提出いただくことで、納入期限の延長が可能です。

（原則 2018 年 4 月末期限。ただし時期についてはご相談ください。）

お申し出先： http://www.saaj.or.jp/toiawase/index.html　（事務局）

＜振込先＞ **郵便振替口座**：00110-5-352357　（請求書発送時に振込依頼書を同封します）

加入者名：日本システム監査人協会事務局

**銀行振込口座**：みずほ銀行八重洲口支店（普通）2258882

口座人名：特定非営利活動法人日本システム監査人協会

トクヒ）ニホンシステムカンサニンキヨウカイ

※銀行振込の際は、«会員№»４桁の数字を氏名の前に付けて下さいますようお願い致します。

（会員番号が付けられない場合は、メールで振込内容をお知らせください。）

※振込手数料はご負担願います。

**【重要事項：2017 年度会費未納の場合】**

一部の会員の方について、2017 年度会費のお支払が確認できません。2017 年 12 月 31 日までに納付が確認できない場合は、除名処分となりますので、至急お手続きいただきますようお願い致します。

なお、http://www.saaj.or.jp/kenkyu/index.html　の「会員ログイン画面へ」から、会員ページにアクセスしていただきますと、会費のお支払状況をご確認いただくことができます。

**【ご寄附のお願い】**

協会では、運営基盤のより一層の改善を図りたく、一口 3,000 円のご寄附をお願い申し上げます。

2017 年 10 月末現在、認定 NPO 法人の継続基準である、年間 100 人以上のご寄附の人数に達しておりません。12 月中のご寄附へのご協力をよろしくお願いいたします。

＜寄附金額＞　￥3,000/一口　ご寄附は、何口でも承ります。

＜振込先＞　ご寄附は、協会会費に合算して、会費振込先にお振込みください。

＜東京都への個人情報の提供＞法令に基づき、寄附者名簿（氏名、ご住所）を、認定 NPO 法人所轄庁の東京都へ報告致します。何卒ご了承賜りますようお願い致します。

【会費、ご寄附等に関するお問い合わせ先】： http://www.saaj.or.jp/toiawase/index.html　（事務局）

以上

<目次>

2017.11

**協会からのお知らせ（予告）【第 17 期通常総会の開催】**

会員番号　1760 斎藤由紀子（事務局）

**日本システム監査人協会（SAAJ）会員各位**

## ■第 17 期通常総会のご案内

日本システム監査人協会の第 17 期通常総会を、下記の通り開催致します。

万障お繰り合わせの上ご出席をお願い申し上げます。

総会、懇親会の参加申込は 2018 年 1 月末より、協会ホームページにて受け付けます。

- **1．日時：2018 年 2 月 23 日（金）**　13 時 30 分～（受付開始：13：00）
- **2．場所：**東京都港区芝公園 3 丁目 5 番 8 号 機械振興会館　地下 3 階　研修 1 室
- アクセス：http://www.jspmi.or.jp/kaigishitsu/access.html
- **3．第 17 期通常総会　議事**（予定）　13 時 30 分 ～ 15 時

13:30 開会

- (1) 2017 年度　事業報告の件
- (2) 2018 年度　事業計画の件
- (3) 2018 年度　予算の件
- (4) 理事選任の件
- (5) その他

15:00 閉　会

（休　憩）

- **4．特別講演**　15 時 30 分～17 時

15:30　開演

- 演題：調整中
- 講師：調整中

17:00　閉演

- **5．懇親会**　17 時 30 分 ～ 19 時

17:30 開場　（機械振興会館地下 3 階会議室）

20:00 閉場

<目次>

| 【　ＳＡＡＪ協会行事一覧　】　赤字：前回から変更された予定 | | | 2017.11 |
|---|---|---|---|
| **2017** | **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 | 9：理事会<br>9：予算申請提出依頼（11/30〆切）<br>支部会計報告依頼（1/9〆切）<br>18：2018 年度年会費請求書発送準備<br>25：会費未納者除名予告通知発送<br>30：本部・支部予算提出期限 | 11,18,25：秋期 CSA 面接<br><br><br>下旬：CSA・ASA 更新手続案内<br>〔申請期間 1/1～1/31〕<br>30： CSA 面接結果通知 | |
| 12 月 | 1： 2018 年度年会費請求書発送<br>1： 個人番号関係事務教育<br>14：理事会：2018 年度予算案<br>会費未納者除名承認<br>第 17 期総会審議事項確認<br>15：総会資料提出依頼（1/9〆切）<br>15：総会開催予告掲示<br>19：2017 年度経費提出期限 | <br><br><br>15： CSA/ASA 更新手続案内メール<br>〔申請期間 1/1～1/31〕<br>26：秋期 CSA 認定証発送 | 12:協会創立記念日 |
| 1 月 | 9： 総会資料提出期限 16：00<br>10：役員改選公示（1/25 立候補締切）<br>11：理事会：総会資料原案審議<br>27：2017 年度会計監査<br>30：総会申込受付開始（資料公表）<br>31：償却資産税・消費税申告 | 1-31：CSA・ASA 更新申請受付<br><br>19： 春期 CSA・ASA 募集案内<br>〔申請期間 2/1～3/31〕 | 6：支部会計報告期限 |
| 2 月 | 1：理事会：通常総会議案承認<br>27：法務局：資産登記、活動報告提出<br>理事変更登記<br>28：2018 年度年会費納入期限 | 1-3/31：CSA・ASA 春期募集<br><br><br>下旬：CSA・ASA 更新認定証発送 | <br><br>23：第 17 期通常総会<br>役員改選 |
| 3 月 | 1：NPO 事業報告書、東京都へ提出<br>5：年会費未納者宛督促メール発信<br>8：理事会 | 1-31: 春期 CSA・ASA 書類審査 | |
| 4 月 | 12：理事会<br><br>30：法人住民税減免申請 | 初旬：春期 CSA・ASA 書類審査<br>中旬：春期ＡＳＡ認定証発行 | 15：春期情報技術者試験 |
| | 前年度に実施した行事一覧 | | |
| 5 月 | 11：理事会 | 中旬：春期 CSA 面接<br>16：第 223 回月例研究会「企業 IT 動向調査 2017」 | |
| 6 月 | 4：年会費未納者宛督促メール発信<br>8：理事会<br>15：会費未納者督促状発送<br>15～：会費督促電話作業（役員）<br>30：支部会計報告依頼（〆切 7/14）<br>30：助成金配賦額決定（支部別会員数） | 3：特別月例研究会「ＩＴガバナンスの国際規格（ISO/IEC 38500 シリーズ）と今後の展開について」<br>中旬：春期 CSA 面接結果通知<br>22-23　システム監査実践セミナー(晴海)<br>下旬: 春期 CSA 認定証発送 | 認定 NPO 法人東京都認定日（2015/6/3） |
| 7 月 | 5：支部助成金支給<br>13：理事会 | 3：第 224 回月例研究会「IoT におけるサイバー攻撃の実態とその対策」<br>下旬：秋期 CSA・ASA 募集案内 | 14：支部会計報告〆切 |
| 8 月 | （理事会休会）<br>26：中間期会計監査 | 1：秋期 CSA・ASA 募集開始～9/30 | |
| 9 月 | 14：理事会 | ～　秋期 CSA・ASA 募集中　～9/30 迄<br>2：第 19 回「事例に学ぶ課題解決セミナー」<br>5：第 225 回月例研究会「IoT 時代のセキュリティを実現する 3 視点とシフトレフト」<br>14-15 & 28-29：第 30 回システム監査実務セミナー(日帰り 4 日間コース) | 30：西日本支部合同研究会 in Fukuoka(福岡) |
| 10 月 | 12：理事会 | 21:SAAJ 活動説明会（東京茅場町）<br>30：第 226 回月例研究会 | 15：秋期情報処理技術者試験 |

<目次>

2017.11

## 【 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。
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**

・ホームページでは協会活動全般をご案内　http://www.saaj.or.jp/index.html
・会員規程　http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・会員情報の変更方法　http://www.saaj.or.jp/members/henkou.html

**特典**

・セミナーやイベント等の会員割引や優遇　http://www.saaj.or.jp/nyukai/index.html
公認システム監査人制度における、会員割引制度など。

**ぜひご参加を**

・各支部・各部会・各研究会等の活動。　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。

**ご意見募集中**

・皆様からのご意見などの投稿を募集。
ペンネームによる「めだか」や実名投稿には多くの方から投稿いただいております。
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**

・「情報システム監査実践マニュアル」「６か月で構築する個人情報保護マネジメントシステム」などの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

**セミナー**

・月例研究会など、セミナー等のお知らせ　http://www.saaj.or.jp/kenkyu/index.html
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**

・過去の会報を公開　https://www.saaj.jp/03Kaiho/0305kaihoIndex.html
会報に対するご意見は、下記のお問合せページをご利用ください。

**お問い合わせ**

・お問い合わせページをご利用ください。　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>

2017.11

**【 会報編集部からのお知らせ 】**

1．会報テーマについて
2．投稿記事募集
3．会報 200 号及び SAAJ 創立 30 周年記念号について

**□■ 1． 会報テーマについて**

2017 年度の年間テーマは、「システム監査の新たな展開」です。四半期テーマは、2 月号から 4 月号が「技術革新とシステム監査」、5 月号から 7 月号までが「AI とシステム監査」、8 月号から 10 月号までは「システム監査とＩＴガバナンス」でした。11 月号は会報 200 号記念号で四半期テーマの掲載はお休みさせていただきましたが、12 月号から 2018 年 2 月号までは「システム監査人に求められる能力」としますので、皆様のご投稿をお待ちしています。

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 の投稿用フォーム（毎月メール配信）を利用してください。
2．会員投稿　　：Word の投稿用フォーム（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」をご確認ください。

**□■ 会報投稿要項　（2015.3.12 理事会承認）**

・投稿用フォームは、毎月メール配信する Word ファイルを利用してください。
　http://www.saaj.or.jp/members/kaihou_dl.html　からもダウンロードできます。
・投稿は、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。
・表紙の写真も、随時募集しています
・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。

**□■ 3．会報 200 号、SAAJ 創立 30 周年**

1．会報も 200 号を迎えることができました。これも、会員の皆様の投稿等による支えや編集委員の方々のご苦労があったればこそで、この場を借りて感謝申し上げます。
2．本年 12 月 12 日は、1987 年の SAAJ 設立総会から 30 年になります。創立 30 周年記念の企画も今後ご案内させていただきますので、ご協力をお願い致します。

<目次>

2017.11

**会員限定記事**

【本部・理事会議事録】（会員サイトから閲覧ください。会員パスワードが必要です）

https://www.saaj.or.jp/members_site/KaiinStart

ログイン ID（8 桁）は、年会費請求書に記載しています。

■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、会員宛の連絡事項を記載し登録メールアドレス宛に配信します。登録メールアドレス等を変更された場合は、会員サイトより訂正してください。

https://www.saaj.or.jp/members_site/KaiinStart



■□■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
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>