認定NPO法人
日本システム監査人協会報
2016年7月号
No.184
— No.184（2016年7月号）<6月25日発行> ——————————

今月号のテーマは

「システム監査の多様性」です。

「システム監査」という「しくみ」を
様々な局面で有効活用してみませんか？

写真提供：仲会長

巻頭言

『 視座を変える 』

会員番号 1342 安部晃生（副会長）

私事で恐縮だが、この6月に、私の所属している中小企業診断士の研究会で『損保代理店　成功の秘訣』（同友館）を上梓した。その中で「損保代理店におけるＩＴ活用」というテーマが私の担当だった。担当したのはよいが、損保代理店におけるＩＴ業務の実務経験があるわけでもなく、どう書けばよいのか手探りの状況で、かなりの悪戦苦闘であった。しかし、いろいろと悩みながらも、文献調査や損保代理店へのインタビューを重ね、研究会メンバーのアドバイスなどを得て、なんとか20ページほどの自分の担当分を書き上げることができた。苦労しただけに、こうして本ができてみると感慨深いものがある。

もちろん、私の本業はというと、「システム監査」ではあるのだが、今回「損保代理店におけるＩＴ活用」というテーマの執筆を通じて、経営者あるいは経営コンサルタントの立場からＩＴ活用を考える機会を得て、非常に勉強になった。ＩＴを監査人の立場から見ていると、システム管理基準などの監査のための基準の面からだけＩＴを見てしまう。立場を変えて経営者あるいは経営コンサルタントの立場に立って、ＩＴ活用を考えると、これまで見えていないものがいろいろと見えてきた。

皆さんも、ちょっと自分の立ち位置（視座）を変えてＩＴを考えてみてはどうだろうか。こうしたことが、「ＩＴアセッサ(注)」への道に通じる気がする。

（注）ＳＡＡＪのビジョンにある「ＩＴアセスメント」を担う人材

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＞

2016.6

めだか　【　システム監査の多様性　】

第213回月例研究会は「IoTって何？～IoTによるイノベーションとその課題～」というテーマの楽しい講演だった。ISO/IEC JTC1では、IoT（Internet of Things）は、“an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.”と定義されている。簡単にいえば、IoTとは、「つながる」インフラストラクチャというわけである。

講演の中で、Industry 4.0 Reference Architecture が参考に紹介されている。これは、ドイツで主唱されている第4の産業革命を、時間軸、空間軸、及びビジネスの層別で表現したものである。第1の産業革命のキーワードは「蒸気機関」、第2の産業革命は「電気」、第3の産業革命は「電子」、そして第4の産業革命は「IoT」といえる。これもまた、「つながる」工場というような言葉が使われている。

さて、2016年5月16日のNHK「クローズアップ現代＋」は、「オモロいことはじめまっせ～“笑いの総合商社”の新展開～」というテーマで、吉本興業が47都道府県やアジアのタイなどへ「住みます芸人」を送り込む事業をとりあげている。今のまま東京一極でビジネスがうまくいけば楽だしありがたいがこれからはそうはいかないだろうという経営判断から始めた事業だという。日本やアジアがお笑いで「つながる」ようにもっていこうということだろう。

上記番組で解説している平田オリザ氏は、著書のなかで、“まことに小さな国である日本が衰退期をむかえようとしているとき、「失業者が映画を観に行ったり、生活保護世帯の方が演劇を楽しんだりすると後ろ指をさされる社会、子育て中のお母さんが芝居を楽しむと後ろ指をさされる社会」から、寛容と信頼によって、社会を再び編み替えよう”と言って、瀬戸内海、但馬、東北で進行中の文化資本を地方に蓄積するための教育プログラムを紹介している。笑顔で「つながる」楽しい国を目指そうということだと思う。

システム監査人は、支部大会や部会・研究会活動で「つながる」ことが多いと思う。そういう場面をたいせつにして、社会がIoTで「つながる」時代に、システムの課題を洗い出し、システム監査人に求められるシステム監査の多様性にこたえていきたいと思う。

（空芯菜）

参考資料：「下り坂をそろそろと下る」平田オリザ著　講談社現代新書2363

（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>

2016.6

投稿　【　システム監査の活性化　】

会員番号　0557 仲厚吉　（会長）

認定 NPO 法人に認定されて 1 年が経過しました

当協会は、2015年6月3日に所轄庁の東京都より認定NPO法人に認定され、この6月２日に1年が経過しました。一般のNPO法人との違いは、認定を受けるための基準に適合していることが求められます。基準の要件は次の９点になります。

①パブリック・サポート・テスト（PST）に適合すること
②事業活動において、共益的な活動に占める割合が、５０%未満であること
③運営組織及び経理が適切であること
④事業活動の内容が適正であること
⑤情報公開を適切に行っていること
⑥事業報告書等を所轄庁に提出していること
⑦法令違反、不正の行為、公益に反する事実等がないこと
⑧設立の日から1年を超える期間が経過していること
⑨欠格事由に該当していないこと

※パブリック・サポート・テスト（PST）：
当協会は、実績判定期間内の各事業年度中の寄附金の総額が、3,000円以上である寄附者の数の合計数が年平均100人以上であることという基準（絶対値基準）に適合しています。

認定申請の動機は、当協会が、「公認システム監査人等」の資格を認定し、依頼に応じてシステム監査人を推薦する法人であることを鑑み、当協会が認定NPO法人であることによって信頼性を評価されるように考えたことです。また、会員の皆様のご寄附に、寄附金控除などの税制優遇が受けられる特典もあることです。認定取得は、当協会によるシステム監査活性化の活動に寄与するものと考えています。

2016年度から、従来の事業報告に加えて認定NPO法人の要件を維持している状況を東京都に報告しています。認定の有効期間は、認定の日から5年間で、有効期間の満了後も引き続き、認定NPO法人として特定非営利活動を行いたく考えています。有効期間満了の日の2020年6月2日の６ヶ月前から３ヶ月前までの間に、有効期間の更新申請をする必要があり、2015年度のご寄附の実績をまとめるなど、2016年度より更新申請の準備を始めています。当協会は、システム監査の普及、及びシステム監査人の活動を促進するため、システム監査を核として、IoTの時代に、“ITアセスメント” に取り組んでいきます。

会員の皆様には協会活動及びご寄附などにご協力のほどをお願い申し上げます。

以上

<目次>

2016.6

第 213 回月例研究会：講演録

【　IoT って何？　～IoT によるイノベーションとその課題～　】

会員番号　2589 林　昭夫

【講師】独立行政法人 情報処理推進機構 技術本部 ソフトウェア高信頼化センター 調査役
工学博士　田丸　喜一郎　氏

【日時・場所】2016年5月26日（木）18：30～20：30

【テーマ】「IoTって何？　～IoTによるイノベーションとその課題～」

【要旨】

"IoT"は今や日常的に使われ、誰もが知っている用語ではあるが、立場が違えば解釈も異なるため、人によってこの解釈が随分と異なっている。
この講演では"IoT"の由来と定義、及びそれを活用した事業の展開とともに見えてくる課題、更には顕在化してくるリスクについて分かり易く解説し、 IoTの利用状況・利用環境に関連した不具合を想定したシステム監査の必要性についても触れている。

【講演録】

1．Iot（Internet of Things）の定義

用語の定義について、これまで"物のインターネット"と訳され、それが使われているため誤解が生じて混乱していた。ISO/IEC では、Iotの定義を次のように定めている。

「an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.」

「物理世界と仮想世界の情報を処理し、それらが相互作用できるように物・人・システム・情報資源をインテリジェントサービスにより相互接続するインフラ」と訳される。（講師の田丸喜一郎氏訳）

2．ステークホルダにより見方が異なるIoT

(1) サービスにとってのIoT

IoTで接続された数多くの端末から集めたビッグデータを活用して、高度なサービスを提供するSI系サービス

(2) 端末/ユーザにとってのIoT

IoTで接続された種々のサービスをワンストップで提供する。必要なサービスを組み合わせ、お好みのスタイルで提供できる、自動車、住宅業界などが行っているサービス

全体としてはネットワークを通して、端末同士もサービス同志もつながって行くものと考えられる。また、IoTシステムはクラウド、広域ネットワーク、近距離ネットワークの３層構造で考えられる。

３．IoTの特徴とその課題に対応する技術キーワード

(1)業界を跨ってシステムが連携してサービスを提供

●システムエンジニアリング　●SQuaRE(ISO/IEC2500シリーズ）

（2）組込み、モバイル、クラウドがネットワークで接続

●M2M…無線技術（WiSUN、BLEなど）　●ビッグデータ

（3）連携する個々のシステムが独立に新陳代謝しながら継続的に変化

●モデルベース（SySML、MATLAB/Simulinkなど）　●形式手法（形式的使用記述とモデル検査）

●IV&V（Independent Validation & Verification）と認証

（4）一つの障害が広範囲に波及・影響するリスク

●機能安全とセキュリティ　●アシュアランスケース（GSN,D-CASEなど）と障害対応（DEOSプロセスなど）

４.IoTを活用した事業イノベーションと課題

（1）IoTを活用した事業イノベーションの検討について

調査企業149、複数選択可で、最も多いのが、“IoTに対応した既存製品・システムの拡充による事業の拡大”で、54.4%が検討しており、次に、“利用情報の活用による製品・サービスの高付加価値化（ビッグデータ活用など）”で42.3%、３番目に、“コア技術を活用した新規事業分野への展開”で40.9%の企業が、IoTを活用した事業イノベーションを検討している。

（2）IoTに関連した取り組みの状況と課題

調査企業163、複数選択可で、既に研究・開発に着手している（36.8%）、IoT製品・システムを市場に提供している（25.2%）、IoTサービスを市場に提供している（9.2%）となっており、将来の事業として準備している（30.7%）、どのように取り組むか検討中（31.3%） を含めると殆どの企業が既に着手、若しくは検討していることが分かる。

（3）IoTに取り組む際の課題

企業がIoTに取り組むにあたっては、現在様々な問題に直面しており、効果的な活用に対し大きな壁となっている。

①人材不足（IoTビジネスの企画・設計要員不足、ビッグデータ活用やネットワークの技術者不足、セキュリティ・障害対応、その他）

②関係する規格への適合、認証取得の問題、ビジネスモデルの構築、新規投資の難しさ、他

（4）課題の解決に有効な策と高度化すべき技術

企業では様々な対策を講じており、先ず、IoT人材に関してスキル、コンピテンシー等の明確化と発掘・育成や、先端技術への開発、投資、或いは産業分野を超えた異業種とのビジネスマッチングの強化等の対応策が講じられている。高度化すべき技術としては、センサ技術、無線技術・ネットワーク技術、及びそれらに伴うセーフティ技術、並びにセキュリティ技術などが挙げられる。

5.IoTに関わる脅威とシステム監査について

IoTの利用状況・利用環境に関連した不具合（＊1～＊3）が年々増加傾向にある。

（1）不具合の原因とされる原因の上位5件

①ソフトウェアの不具合　47.3%

②ハードウェアの不具合　19.6%

③製品・システムの企画・仕様の不具合（＊1）　12.5%

④運用・保守の不具合（＊2）　6.8%

⑤他製品・他システムとの接続に起因する不具合（＊3）　4.7%

このようなIoTの利用状況・利用環境に関連した不具合(＊1～＊3) に関してシステム監査が行われることを期待する。

（2）機能しなかったシステム、緊急時を想定しなかったシステムの事例

●スリーマイル島原発事故（1978年３月発生）

事故原因：機器の故障+運転員のヒューマン・エラー

●エアバスA300型機墜落事故（1994年4月発生）

事故原因：パイロットの操縦ミスと緊急時を想定しなかった自動化システム

6.想定される2020年の社会と脅威の想定

2020年には東京オリンピックが開催されるが、HEMS、AV機器、医療・ヘルスケア、自動車などの製品・サービスがそれに向けて加速するため、「つながる」世界で脅威が更に拡大、深刻化すると想定される。

（1）信頼できるIoTの実現・運用に向けて

●全体システムを意識したハザード・リスク分析……上流からの品質の確保

●品質の「見える化」、「見せる化」……対他業界、対利用者、対社会

●運用時に高まり続けるリスク……システム間の相互作用、セキュリティリスクの増加

●リスクモデルに対応した取組み……運用段階での取り組みが重要

●運用段階での取組みの課題……業界を跨るシステムとリスクの拡大防止

（2）安全安心なIoTの実現に向けて開発者に認識してほしい重要ポイント 「つながる世界の開発指針」

大 項 目		指　　針
方針	つながる世界の安全安心に企業として取り組む	指針1　安全安心の基本設計を策定する（方針策定）
		指針2　安全安心のための体制・人材を見直す（体制構築）
		指針3　内部不正やミスに備える（企業文化の醸成）
分析	つながる世界のリスクを認識する	指針4　守るべきものを特定する（対象の特定）
		指針5　つながることによるリスクを想定する（つながるリスクの想定）
		指針6　つながりで波及するリスクを想定する（波及リスクの想定）
		指針7　物理的なリスクを想定する（物理的リスクの認識）

設計	守るべきものを守る設計を考える	指針8　個々でも全体でも守れる設計をする（多重防御）
		指針9　つながる相手に迷惑をかけない設計をする（波及防止）
		指針10　安全安心を実現する設計の整合性をとる（設計の整合）
		指針11　不特定の相手とつなげられても安全安心を確保できる設計（未知対応）
		指針12　安全安心を実現する設計の検証・評価を行う（検証・評価）
保守	市場に出た後も守る設計を考える	指針13　自身がどのような状態かを把握し記録する機能を設ける（状態把握）
		指針14　時間が経っても安全安心を維持する機能を設ける（経年維持）
運用	関係者と一緒に守る	指針15　出荷後もIoTリスクを把握し、情報発信する（情報収集・発信）
		指針16　出荷後の関係事業者に守ってもらいたいことを伝える（関係者への伝達）
		指針17　つながることによるリスクを一般利用者に知ってもらう（利用者の啓発）

http://www.ipa.go.jp/files/000051411.pdf

（3）IoT 時代の解決すべき課題

●業界を跨ったシステム、●連携する個々のシステムの継続的な変化、●一つの障害が広範囲に波及・影響するリスク、●急速に変化する利用形態への対応などがある。今後の社会は、高齢者、IT 弱者も IoT を使わなければ生活できないが、それに対する公共サービスが未整備で、IoT 教育もまだ不十分である。ただ、水平分業化が進み機動力のある中小企業が主役になる可能性もある。

7.質疑、感想

質疑応答：

Q:　IoT の Reference　Architecture のマップは、IoT における情報セキュリティにおいてはどのように利用したらよいのか？

A:　マップ上の、Communication Layer、Information Layer、Function Layer、或いは Development、Installation、Operation など使用する領域はいろいろあるが、Reference Architecture は、Balance Architecture とも言え、全体を俯瞰するマップとして使ってもらえれば良いのではないかと思う。

Q:　IoT により誰もがネットワークを利用する現状でサイバーセキュリティに関する教育についてどのように考えておられるのか？

A:　難しい問題であるが、子供は幼少期から触れており、大丈夫であろうが、高齢者は教育に限界がある。教えるよりも社会的な仕組み制度で保護・救済するほうが効果的であると思っている。

Q:　IoT におけるシステム監査に関するお話が出たが、一般的には情報セキュリティリスクを中心に守ることばかりが強調されおり、新しいビジネスチャンスなどでシステム監査に期待されるものはないのかご意見を伺いたい。

A:　先程話したように、現在、ビジネスの企画・デザインができる人がいない。その領域で、企画・デザインにおいてこのビジネスが大丈夫だろうかという評価が、監査でできるなら良いのではないか。工程を追いかけるよりはその方が先であろうと思う。

8.感想

日頃、良く耳にし、目に触れる IoT という用語は、何となく理解はしているものの、ぼんやり漠然とした解釈のまま使用してきた用語の一つであった。本講演では、用語の定義から始まり、とてもよく整理された、分かり易い内容で、これまでは特別興味のある分野ではなかったが、知らないうちに話に引き込まれていた。講演の内容がとても良く理解できたと思う。

以上

<目次>

2016.6

「新個人情報保護法]がＰＭＳに及ぼす影響　～ＰＭＳハンドブック読者！必読！～　　第３回

会員番号　1795　藤澤　博（個人情報保護監査研究会）

今月号では「第四章　個人情報取扱事業者の義務等」から解説します。今回ご紹介する条項は、すべて未施行で、交付の日（2015年9月9日）から二年を越えない範囲において施行される予定です。

法改正にあたり、最終改定では、**第24条～第26条**が新設され、例えば**第25条**は（第三者提供に係る記録の作成等）となります。しかしながら、2016年6月1日現在、政府の法令サイトでは、**第二十五条は（開示）のまま**と公表されています。

http://law.e-gov.go.jp/htmldata/H15/H15HO057.html

この連載では、最終改定の内容について解説するため、現行の条項番号を**漢数字**で、最終改定後の条項番号をアラビア数字で区別して、ご紹介していきます。

第３項【2016年１月１日から施行】（第1回連載内容を以下のとおり訂正します）

（中略）**第25条**（第三者提供に係る記録の作成等）、**第26条**（第三者提供を受ける際の確認等）、
第27条（保有個人データに関する事項の公表等）、**第30条**（利用停止等）
第32条（開示等の請求等に応じる手続）、**第34条**（事前の請求）、
第37条（匿名加工情報の提供）　　（以下略）

この連載の前回までの内容は、以下のサイトで閲覧できます。
目次 ＝http://1.33.170.249/saajpmsHoritsu/000PIPHoritsu.html

第四章　個人情報取扱事業者の義務等

第一節　個人情報取扱事業者の義務

第十五条(利用目的の特定)

個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。

2　個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と~~相当の~~関連性を有すると合理的に認められる範囲を超えて行ってはならない。

※“相当の”　が削除された理由：“相当の”を判断することが困難であるという理由だと考えられます。“あらかじめ本人の同意を得ないで、特定された利用目的の達成に必要な範囲を超えて個人情報を取り扱ってはならない。”原則には変わりがありません。

第十六条(適正な取得)

個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。

2　個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、**本人の同意を得ることが困難であるとき。**

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
五　当該要配慮個人情報が、本人、国の機関、地方公共団体、第７６条第一項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合　六　その他前各号に掲げる場合に準ずるものとして政令で定める場合

※一の「法令に基づく場合」とは、弁護士など、守秘義務を負った専門家が、本人の犯罪経歴について調査をするなど、特殊な場合に限定されると考えられます。
“本人の同意を得ることが困難であるとき”という条件は重要です。経済産業省GLでは、原則として、取得した後に、本人に通知をすることが望ましいとされています。

第十八条（取得に際しての利用目的の通知等）
個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。
2　個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電磁的記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。
（以下省略）

※「個人情報データベース等」のうち、一定の規則で匿名化したものを、第三者提供できるようにするため、カッコ書きに　**“電磁的記録”**が追加されました。

第十九条（データ内容の正確性の確保等）
個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない。

※ 特定個人情報ガイドライン第4－3－(3)Ｂ（保管制限と廃棄）では、継続して保管できる事例として、以下が記述されています。
＊　（中略）従業員等から提供を受けた個人番号を給与の源泉徴収事務、健康保険・厚生年金保険届出事務等のために翌年度以降も継続的に利用する必要が認められることから、特定個人情報を継続的に保管できると解される。

※　特定個人情報ガイドライン（別添）特定個人情報に関する安全管理措置（事業者編）
Ｅ 物理的安全管理措置ｄ（個人番号の削除、機器及び電子媒体等の廃棄）に、以下の具体的な廃棄方法が記載されています。**事業者は、これを参考にして、リスクに応じた対策を安全管理規程等に定める必要があります。**
«手法の例示»

＊ 特定個人情報等が記載された書類等を廃棄する場合、焼却又は溶解等の復元不可能な手段を採用する。
＊ 特定個人情報等が記録された機器及び電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段を採用する。
＊ 特定個人情報ファイル中の個人番号又は一部の特定個人情報等を削除する場合、容易に復元できない手段を採用する。
＊ 特定個人情報等を取り扱う情報システムにおいては、保存期間経過後における個人番号の削除を前提とした情報システムを構築する。
＊ 個人番号が記載された書類等については、保存期間経過後における廃棄を前提とした手続を定める。

【中小規模事業者における対応方法】

○ 特定個人情報等を削除・廃棄したことを、責任ある立場の者が確認する。

第二十三条(第三者提供の制限)

（中略）

2　個人情報取扱事業者は、第三者に提供される個人データ（要配慮個人情報を除く。以下この項において同じ。）について、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、個人情報保護委員会規則で定めるところにより、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出たときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。

一　第三者への提供を利用目的とすること。
二　第三者に提供される個人データの項目
三　第三者への提供の方法
四　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。
五　本人の求めを受け付ける方法

3　個人情報取扱事業者は、前項第二号、第三号又は第五号に掲げる事項を変更する場合は、変更する内容について、個人情報保護委員会規則で定めるところにより、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出なければならない。

4　個人情報保護委員会は、第二項の規定による届出があったときは、個人情報保護委員会規則で定めるところにより、当該届出に係る事項を公表しなければならない。前項の規定による届出があったときも、同様とする。

5　次に掲げる場合において、当該個人データの提供を受ける者は、前各項の規定の適用については、第三者に該当しないものとする。

一　個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託することに伴って当該個人データが提供される場合
二　合併その他の事由による事業の承継に伴って個人データが提供される場合
三　特定の者との間で共同して利用される個人データが当該特定の者に提供される場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

6　個人情報取扱事業者は、前項第三号に規定する利用する者の利用目的又は個人データの管理について責任を有する者の氏名若しくは名称を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

※ 第２項は、オプトアウト規定（本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止する）です。プライバシーマークでは、現在オプトアウトは不適合とされていますので注意が必要です。

※　オプトアウト規定に従い（あらかじめ本人から同意を得ずに）第三者提供をしようとする場合、事業者は、一～五の項目を個人情報保護委員会へ届出るとともに、個人情報保護委員会は、その内容を公表します。

※ 第５項の三は、共同利用について規定しています。プライバシーマークでは、共同利用は第三者提供の一類型とされていますが、新法では、“第三者に該当しない”という概念が導入されました。（現行の経済産業省GLでも同様の概念です。）しかし、“直接本人から取得”ではありませんので、必要事項を公表する必要があります。

第24条（外国にある第三者への提供の制限）　（新設）

個人情報取扱事業者は、外国（本邦の域外にある国又は地域をいう。以下同じ。）（個人の権利利益を保護する上で**我が国と同等の水準にある**と認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるものを除く。以下この条において同じ。）にある第三者（個人データの取扱いについてこの節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している者を除く。以下この条において同じ。）に個人データを提供する場合には、前条第一項各号に掲げる場合を除くほか、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。この場合においては、同条の規定は、適用しない。

※“我が国と同等”　の判断基準は、今後、個人情報保護委員会規則に定められる予定です。本人の同意を得ることができれば、自由に外国に提供してよいのかどうか、疑問の残るところです。また本人から、“我が国と同等の水準”であるか、と、事業者は説明責任を求められることでしょう。

第25条（第三者提供に係る記録の作成等）　（新設）

個人情報取扱事業者は、個人データを第三者（第2条第五項各号に掲げる者を除く。以下この条及び次条において同じ。）に提供したときは、個人情報保護委員会規則で定めるところにより、当該個人データを提供した**年月日**、当該**第三者の氏名又は名称**その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない。ただし、当該個人データの提供が第23条第一項各号又は第五項各号のいずれか（前条の規定による個人データの提供にあっては、第23条第一項各号のいずれか）に該当する場合は、この限りでない。

2　個人情報取扱事業者は、前項の記録を、当該記録を作成した日から個人情報保護委員会規則で定める期間保存しなければならない。

※第2条第五項各号に掲げる者とは、国の機関等を指します。

※今後、第三者提供する場合、個人情報保護委員会規則で定められる事項の記録を作成し、保管することになります。

第26条(第三者提供を受ける際の確認等)　　(新設)

個人情報取扱事業者は、第三者から個人データの提供を受けるに際しては、個人情報保護委員会規則で定めるところにより、次に掲げる事項の確認を行わなければならない。ただし、当該個人データの提供が第23条第一項各号又は第五項各号のいずれかに該当する場合は、この限りでない。

一　当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者（法人でない団体で代表者又は管理人の定めのあるものにあっては、その代表者又は管理人）の氏名

二　当該第三者による当該個人データの取得の経緯

2　前項の第三者は、個人情報取扱事業者が同項の規定による確認を行う場合において、当該個人情報取扱事業者に対して、当該確認に係る事項を偽ってはならない。

3　個人情報取扱事業者は、第一項の規定による確認を行ったときは、個人情報保護委員会規則で定めるところにより、当該個人データの提供を受けた年月日、当該確認に係る事項その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない。

4　個人情報取扱事業者は、前項の記録を、当該記録を作成した日から個人情報保護委員会規則で定める期間保存しなければならない。

※ 第26条は、第十七条（適正な取得）と関連しています。つまり、不正な手段で取得した個人情報でないことを確認することが目的です。

※ 現行の経済産業省GLでは、下記のように記載されています。

第三者から個人情報を取得する場合には、提供元の法の遵守状況（略）を確認し、個人情報を適切に管理している者を提供元として選定するとともに、実際に個人情報を取得する際には、その都度、例えば、取得の経緯を示す契約書等の書面を点検する等により、当該個人情報の取得方法等を確認したうえで、当該個人情報が適法に取得されたことが確認できない場合は、偽りその他不正の手段により取得されたものである可能性もあることから、その取得を自粛することを含め、慎重に対応することが望ましい。

※ 第26条が施行された後は、第三者から提供を受ける場合、個人情報保護委員会規則で定められる事項の記録を作成し、保管することになります。

※ 第26条**第２項**に違反した場合は、**十万円以下の過料**に処せられることになります。（新法罰則第88条）

・・

次回は、「第四章の続きで、第27条　保有個人データに関する事項の公表等」から解説します。

バックナンバー目次 ＝　http://1.33.170.249/saajpmsHoritsu/000PIPHoritsu.html

「ＰＭＳハンドブック」の読者専用ダウンロードサイトでは、新個人情報保護法、番号利用法の改正を反映した規程・様式集を公開しています！！

SAAJ「ＰＭＳハンドブック」ご紹介サイト：http://www.saaj.or.jp/shibu/kojin.html

認定NPO法人日本システム監査人協会　個人情報保護監査研究会　■

<目次>

2016.6

支部報告　【　近畿支部　第１５９回定例研究会　】

会員番号　２５９１ 近藤 博則

１．テーマ　「事例に学ぶ情報漏えい事故とそのセキュリティ対策
～情報セキュリティ監査のポイント」

２．講師　ＮＴＴ西日本ビジネス営業本部　クラウドソリューション部
セキュリティサービスグループ　主査
粕淵　卓　氏

３．開催日時　２０１６年5月２０日（金）　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

講師はＮＴＴ西日本にてセキュリティの専門家として活躍され､またIT関連の資格を多数保有されており、各種メディアへの記事を執筆されている。今回は講師の実施したセキュリティに関する実験、IPAが公開した２０１６年セキュリティの１０大脅威、日本年金機構の情報漏えい事件、自治体情報セキュリティ対策を題材にそれぞれの脅威・対策について講演いただいた。会場からの質疑応答も活発に交わされた。

＜講演内容＞

(ア) １０の疑問を試して解明　セキュリティ大実験室

講師が実施し雑誌の記事としてまとめられた、１０の疑問を試して解明　セキュリティ大実験室から、８個の実験を取り上げ解説いただいた。

① ウイルス対策ソフトは無料でも十分か？

５７７個の検体について、有料版、無料版を用いてどれくらい検出できるかを実験した。有料版は８割の検出率、無料版は４割の検出率となり、予想通りの結果であった。また、同様の実験をUTM製品でも行った。UTM製品では検出率にばらつきが出たが、これは製品の特性によるもので、高検出率のものはパフォーマンス（通信速度）を犠牲にしていることがあるため、一概に検出率が高いものがよいとはならないとの事であった。

② 圧縮や暗号化されたウイルスを検知可能？

圧縮や暗号化した１０種のウイルスを通信経路上に配置したUTM製品で検出できるかを実験した。結果、製品や圧縮形式により検出率が異なったが、いずれの製品でも６階層のフォルダーに入れてLZH圧縮した物、AESで暗号化した物は検出できなかった。ウイルス対策は通信経路上のみでなく、端末でも行う事が重要であるとの事であった。

③ Excelのパスワード保護は有効か？

Microsoft Excelが備えるパスワード保護機能を使用して暗号化したファイルを用いて、パスワード解析にどれくらいの時間がかかるか実験した。解析には総当たりでパスワードを試す自作

ツールと市販ツールを使用した。自作ツールでは数字４桁のパスワードは７分弱、市販ツールでは１分弱で解析可能であった。一般に必要と言われる英数記号を組み合わせた８桁のパスワードは、市販ツールの予測では４コアCPUの端末で解析に１３万年以上かかるとされ、パスワードの強度はある程度保たれているとの事だった。

④　無線LANのSSIDを隠すのは効果あるのか？

SSIDを隠蔽する設定（ステルスモード）に設定したAPを用いて、正常に通信できる端末と解析ツールを導入した端末を用意し実験した。APに誰も接続していない状態であれば、SSIDを見る事はできなかったが、正規ユーザがAPに接続すると、正常に通信できる端末からSSIDが送信されるため、解析ツールにSSIDが表示された。SSIDの隠蔽によるセキュリティ向上は限定的であり、端末側の電池の持ちが悪くなる等デメリットもあるとの事であった。

⑤　セキュリティワイヤーは頑丈か？

複数のセキュリティワイヤーと入手しやすい工具を用いて実験した。セキュリティワイヤーは、ワイヤー径２．２mm、４mm、５．５mmの物、工具は、１０８円のニッパー、家庭用のペンチ、ワイヤーカッターであった。ワイヤーカッターを使用すれば、どれも切断する事が可能であった。セキュリティワイヤーには、心理的な抑止効果、持ち去りに対する盗難対策として一定の効果があるが、工具を使えば切断できるため長時間の盗難対策とするのは不十分である。長時間保管するには鍵のかかるキャビネットや引き出しがよいとの事であった。

⑥　スマホの顔認証は正確か？

スマホに搭載されている顔認識機能について、メガネをかけたり、ひげをつけたりする変装をしても認識するか、本人の写真を本人と認識するか、双子の一方がもう一方になりすます事が可能かについて実験した。また、今回の試験にあたっては、まばたき設定（認証の際にまばたきをする必要がある）は無効にして行った。結果、メガネ、ひげの有無、写真でも高確率で認証を突破できた。また、二卵性の双子であっても認証を突破できた。スマホの顔認証は安全性の高い認証方式ではないとの事であった。

⑦　SSLでURLフィルタリングは機能するのか？

プライバシー保護のため通信が暗号化されるHTTPSを用いるWebサイトが増えている。これらのサイトへの通信に対してURLフィルタリングが機能するかについて実験した。実験には一般によく利用されるプロキシサーバとUTMを用意した。結果、プロキシサーバではドメイン単位でのフィルタリングは可能であったが、ディレクトリ単位ではフィルタリングできなかった。UTMではデフォルト設定の場合、ドメイン単位でもフィルタリングできなかったが、HTTPS通信を復号化する機能を有効にしたところ、ディレクトリ単位でのフィルタリングも可能であった。しかし、HTTPS通信を復号化するには機器のリソースを多く必要とするため通信に対するパフォーマンスは低下するとの事だった。

⑧　パスワードの別送に意味はあるのか？

重要なファイルをメールで送付する場合ファイルを暗号化し、パスワードは別メールでの送付す

る事を義務付けている企業がある。一見安全そうに見えるこの対応であるが、ネットワークを盗聴できる攻撃者であれば、ファイルを添付したメールもパスワードが記載されたメールも盗聴でき、暗号化ファイルを簡単に復元できるはずであるため実験し確認した。結果、パケットキャプチャを行えば、メールを復元し暗号化したファイルとパスワードから復号化したファイルを入手する事ができた。この事から、特に重要なファイルをメールで送付する際には、パスワードを別メールではなく電話等別の手段で通知する等の対応が必要だろうとの事だった。

(イ) ２０１６年セキュリティの１０大脅威

IPAが公開した２０１６年セキュリティの１０大脅威から４つを取り上げ解説いただいた。

① 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

ウイルス感染やフィッシングサイトから不正入手した情報から､個人になりすまし不正送金や利用が行われている。フィッシングの手口はどんどん巧妙になってきており、ぱっと見では正規のサイトと見分けがつかなくなっている。個人でできる対策としては、OS・ソフトウェアの更新、サイトへアクセスした際にSSL通信になっている事の確認等があるとの事であった。

② 標的型攻撃による情報流出

メールの添付ファイルやWebサイトを利用してPCをウイルスに感染させ、そのPCを遠隔操作する事で組織や企業の重要情報を搾取する攻撃が後を絶たない。攻撃者は対象の組織、企業を徹底的に調べ上げ攻撃手法を検討し実施してくる事から､侵入を許す事も少なくない｡対策としては、OS･ソフトウェアを常に最新の状態に保つこと｡また､侵入されない事を目標とするのではなく、侵入される事を前提とし、侵入に早く気づく、情報資産を外部送信させない等の対策により多層防御する事が重要であるとの事だった。

③ ランサムウェアを使った詐欺・恐喝

データを人質に取り、金銭を要求する被害が増えている。侵入経路としてはメール添付やWebサイトからであり、これまでは不自然な日本語のものが多かったが、流暢な日本語によるものも登場しており、より注意が必要となっている。対応としては、バックアップからの復元が主な物となるため定期的なバックアップが重要であるとの事だった。

④ ウェブサービスへの不正ログイン

他のWebサービスと同じパスワードの使い回しや、推測できるパスワードを設定していた為に、Webサービスを不正利用されてしまう被害が増えている。対策としては、パスワードは使い回さない、長く複雑なパスワードをしようする等があるとの事だった。

(ウ) 日本年金機構の情報漏えい事件

日本年金機構からの１２５万件の個人情報漏えい事件について､原因と対策を解説いただいた。ここでは日本年金機構に届いたとされる不審メールの特徴について紹介があり､不審メールはフリーメールサービスを利用して送信されていた｡仕事上よくありそうな件名のメールであっても､フリーメールから送付されてきたメールであれば、慎重に取り扱う必要があるとの事だった。

(エ) 自治体情報セキュリティ対策

本年よりマイナンバーの利用が開始されることに伴い、自治体では抜本的なセキュリティ対策我も止められており、その内容について解説いただいた。ポイントとしては、マイナンバー利用事務系のネットワークと他のネットワークを分離し、ここの端末に対しては情報の持ち出し不可設定や二要素認証（パスワード＋生体認証、ICカード認証）を用いる事。LGWAN環境とインターネットメールとの通信経路を分割し、両システム間で通信を行う場合には、メールを無害化するとの事だった。

(オ) セキュリティ監査における私の考え方

講師が実施する事があるセキュリティ監査において、意識しているポイントとして、次の事をあげられていた。セキュリティ対策においては、やるべき事柄は山のようにあるため、技術的対策・物理的対策・人的対策が完璧に実施できている所はまずない。このため、できていない事を細かく指摘しても、被監査部門から疎まれるだけで実効性のある監査はとはならない。指摘事項とすべきは、受容レベルを大きく超える物や、セキュリティ対策の弱い状態で公開さているサーバがあった場合であるとの事だった。また、監査において一番重要なポイントは、被監査部門との信頼関係であるとの事だった。

６．所感

本講演ではセキュリティに関する話題を一通りおさらいする事ができ、筆者個人、とても有意義だった。また、所々に挟まれる講師の経験に基づいた一言からたくさんの気付きを得る事ができた。特に長くて複雑なパスワードを記憶する方法として紹介された、手帳にキーワードを書き、残りを記憶しておくやり方はすぐ実生活で取り入れた。本講演の途中、ブレイクとして紹介された錯視が印象に残ったので紹介させていただく。錯視とは、見た情報が実際とは異なって知覚される現象のことをいい、ものの形や大きさ、明暗、色、動きなど、ものの見かけ全般にわたり現れる錯覚のことである。簡単に錯覚してしまう脳を持つ者として、巧妙な攻撃者からの攻撃をかわすためには、とっさの対応に頼るだけでなく、日頃からのOS・ソフトウェアの最新化が重要であると認識を新たにした次第である。

以上

<目次>

2016.6

注目情報（2016.5～2016.6）

■「企業における情報システムのログ管理に関する実態調査」報告書の公開【IPA】

6月9日、IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）は、企業における情報システムのログの管理実態を把握し、最適なログ管理の指針を提案するため、「企業における情報システムのログ管理に関する実態調査」を実施し、その報告書を2016年6月9日（木）に公開しました。

https://www.ipa.go.jp/security/fy28/reports/log_kanri/

標的型攻撃などのサイバー攻撃や、内部不正による情報漏えい等の情報セキュリティインシデントが発生した時の事実調査では、情報システムのログからその痕跡・証拠を得ることが重要であり、さらには早期発見や抑止の観点からも情報システムのログ管理は必要不可欠です。一方で、その管理手法は中小企業(*)を含め広く知られているとは言い難い状況です。本調査では、企業における情報システムのログ管理の実態をログ管理製品／サービス提供事業者20社、ユーザ企業11社、有識者3名について調査し、セキュリティ対策を強化するためのログ管理の課題を明らかにすると共に中小企業に適用可能な最低限実施すべきログ管理の指針を提示することを目指しました。

■ 法人番号の利活用について　【日本公認会計士協会】

6月16日、日本公認会計士協会は、国税庁から、法人番号の利活用に関する知らせを受けて、法人番号の利活用促進に関する資料を掲載しました。

http://www.hp.jicpa.or.jp/ippan/jicpa_pr/news/20160616era.html

<目次>

2016.6

【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215回	日時：2016年 7月 26日（火曜日）18:30～20:30 場所：機械振興会館 地下2階ホール	
	テーマ	システム監査の現状と課題、システム監査人に望むこと（仮題）
	講師	日本大学 商学部教授　堀江正之 先生
	講演骨子	近日公表予定

■SAAJ 事例研究会（東京）【課題解決セミナー】

1日又は半日	日時：2016年 7月 23日（土曜日）予定 場所：調整中	
	テーマ	事例に学ぶ課題解決
	講師	小佐野、野田、濵﨑（事務局）
	詳細	近日公表予定　過去開催　https://www.saaj.or.jp/kenkyu/jirei.html

【外部主催イベント・セミナーのご案内】

■「FISC 全国説明会」及び「安全対策基礎セミナー」

（札幌、仙台、大阪、名古屋、福岡、岡山、東京）

日時：2016年 7月 28日（札幌）～　8月 25日（東京）　各地複数日 各地の開催日及び申込は　https://www.fisc.or.jp/event/event_detail/?e=454	
内容	「FISC 全国説明会」 (1) 平成 28 年 5 月発刊の『金融機関等のシステム監査指針（改訂第 3 版追補）』を金融機関等をはじめ多くの方々に利活用いただくため、改訂の概要を解説します。 (2) 平成 28 年 6 月に取りまとめを予定している「金融機関における外部委託に関する有識者検討会」の報告書の考え方を正しく理解していただくため、「安全対策の基本原則」、「リスクベースアプローチに従った IT ガバナンス」及び「リスク管理の在り方」等について解説します。 「安全対策基礎セミナー」 安全対策に関する実務経験の浅い方などを対象として、以下のカリキュラムに沿って、安全対策基準の意義、目的、位置付け、構成等に加え、実務での活用事例やインシデント事例に関連する安全対策基準の項目を説明し、安全対策の基本となる考え方や基礎知識を習得します。 (1) FISC 安全対策基準の概要 (2) 設備基準について (3) 運用基準について (4) 技術基準について

<目次>

2016.6

【 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。

・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

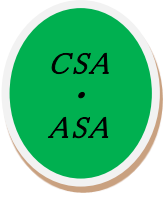
・セミナーやイベント等の会員割引や優遇　http://www.saaj.or.jp/nyukai/index.html
公認システム監査人制度における、会員割引制度など。

・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。

・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。

・「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

・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。



・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

・会報のバックナンバー公開　http://www.saaj.or.jp/members/kaihou_dl.html）
電子版では記事への意見、感想、コメントを投稿できます。
会報利用方法もご案内しています。http://www.saaj.or.jp/members/kaihouinfo.pdf

・お問い合わせ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>

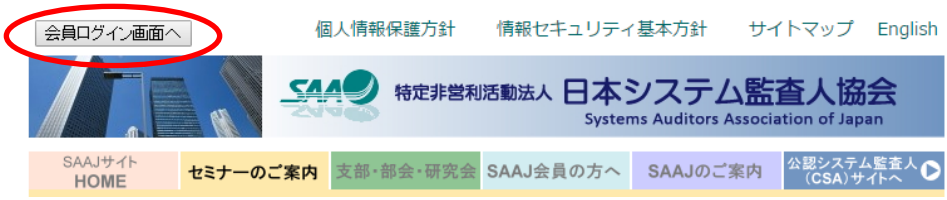
2016.6

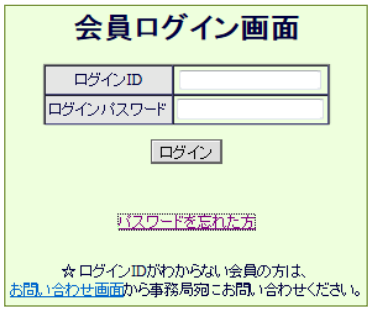
協会からのおしらせ　【年会費お支払状況をご確認ください】

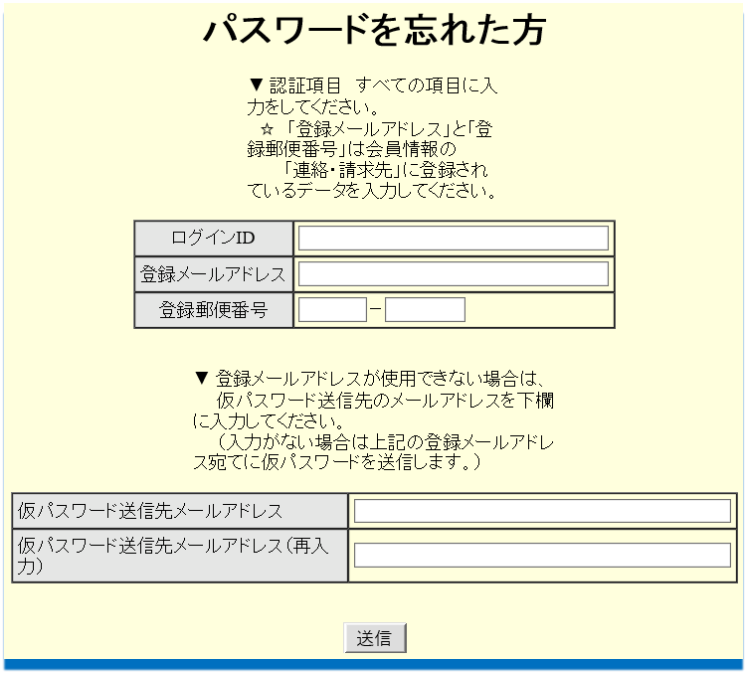
会員番号　1760 斎藤由紀子　（事務局）

2016 年度下半期となりました。今一度、会費納入状況のご確認をお願い致します。

1．会員ログイン画面

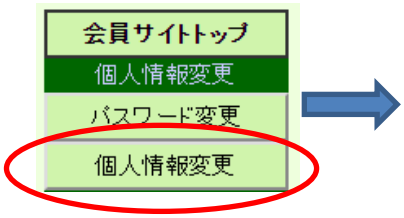






退職等によって、
メールアドレスなどが変更されても
元のアドレス（登録メールアドレス）
と、新しいアドレスの両方を入力して
パスワードを受け取ることができます。

2．会費納入の確認方法



会費納入日	2016年度　2016年2月22日
CSA/ASA入金日	2015年1月29日
CSA/ASA認定日	2015年1月1日

人事異動や、退職などで、住所やメールアドレス等の変更がありましたら、
連絡先についても、訂正をお願い致します。

個人情報確認、変更に関するお問い合わせ：https://www.saaj.or.jp/toiawase/saaj_toiawase.html

<目次>

2016.6

協会からのおしらせ　【年会費の督促について】

会員番号　1760 斎藤由紀子　（事務局）

事務局では、2016 年度会費の納入が確認できない会員の方へ、2016 年 6 月中旬に「会費納付のお願い」状を送付しました。会費未納の方は至急お振込みをお願い致します。支部助成金は 6 月末までに会費支払い済みの会員数に応じて支払われますので、ご協力をお願いします。

拝啓、

平素は協会の運営にご協力いただきまして誠にありがとうございます。さて、年会費の納入状況を確認しましたところ、下記の通り会費が未納となっております。改めて請求書を送付いたしますので、早急にご納付下さるようよろしくお願いします。既に納付済の方には失礼の段ご容赦願います。尚、会費の未納が続きますと協会の規定により会員資格を継続できないことになりますので、協会の趣旨をご理解の上、ご対応よろしくお願い致します。

敬具

請　求　書

（組織名）
（氏名）　様
会員 ID：xxxxnnnn

内訳	金額
２０１６年度年会費	１０，０００円
（SAAJ 年会費は非課税です）	
（請求金額合計）	１０，０００円

<払込期限>　2016 年 6 月 30 日（火）
<振込先>　郵便振替口座：００１１０－５－３５２３５７
加入者名：日本システム監査人協会事務局(添付の払込票)

銀行振替口座：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

※尚、お振込手数料はご負担お願いします。銀行振込の際は、会員番号（nnnn）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、メールまたは FAX などで振込内容をお知らせください）

■ご寄附の募集について

2015年度は、1月から12月末までに100人を超えるご寄附をいただき、認定NPO法人（2015年6月3日認定）の継続条件をクリアすることができました、ご協力に篤く御礼申し上げます。

今後もご寄附の募集につきましては時期を問わず継続しておりますので、上記会費納付と同じ振込先口座に、一口3,000円のご寄附をいただきますよう、引き続きご協力をお願い申し上げます。

なお、ご寄附は確定申告の控除対象となります。確定申告に必要な領収書は、年度末の12月に一括発送する予定です。また、特定非営利活動促進法第44条に基づき、ご寄附者の氏名、住所、金額を東京都に報告致します。あわせてご了解いただきますようお願い致します。

本件に関するお問い合わせ：https://www.saaj.or.jp/toiawase/saaj_toiawase.html

<目次>

【　ＳＡＡＪ協会行事一覧　】　赤字：前回から変更された予定			2016.6
2016	**理事会・事務局・会計**	**認定委員会・部会・研究会**	**支部・特別催事**
6 月	9：理事会 14：会費未納者督促状発送 15～：会費督促電話作業（役員） 30：支部会計報告依頼（〆切 7/14） 30：助成金配賦額決定（支部別会員数）	10：　CSA 面接結果通知 21：第 214 回月例研究会	2015/6/3：認定 NPO 法人 東京都認定日
7 月	5：支部助成金支給 14：理事会	1：秋期 CSA・ASA 募集案内 〔申請期間 8/1～9/30〕 20：認定委員会：CSA 認定証発送	14：支部会計報告〆切
8 月	（理事会休会） 27：中間期会計監査	1：秋期 CSA・ASA 募集開始～9/30	
9 月	14：　理事会		
10 月	13：　理事会		秋期情報処理技術者試験
11 月	10：　理事会 13：　予算申請提出依頼（11/30〆切） 支部会計報告依頼（1/6〆切） 18：　2017 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 20：　CSA・ASA 更新手続案内 〔申請期間 1/1～1/31〕 30：　CSA 面接結果通知	 2016 年 5-6：西日本支部合同研究会 （開催場所：松江）
2015	**過去に実施した行事一覧**		
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〆切） 15：　総会開催予告掲示 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	
1 月	8：　総会資料（〆）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：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：第 27 回システム監査 実務セミナー(後半)	
4 月	14：理事会 30：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	17：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：新規 CSA 面接 26：第 213 回月例研究会 26～27：第 28 回システム監査 実務セミナー（2 日間コース）	

<目次>

2016.6

【 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 年度の年間テーマは「システム監査の活性化」です。システム監査の活性化について、皆様といっしょに考えてみたいと思います。5 月号から 7 月号までの四半期テーマは「システム監査の多様性」です。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ます。システム監査が多様化してきている現状に対し、会員各位の意見を募るべく、四半期テーマとしました。

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：「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。

会報記事への投稿の締切日は、毎月 15 日です。

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してください）。

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

会員限定記事

【本部・理事会議事録】（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

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

■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。
■会員以外の方は、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。
【会員以外の方の送付停止】　http://www.skansanin.com/saaj/register/

■□■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>