認定NPO法人
日本システム監査人協会報
2017年6月号
No 195
No.195（2017年6月号）＜5月25日発行＞

先月号に引き続き、テーマは「AIとシステム監査」です。

今後、急速に発展、広がると考えられる「AI（人工知能）」について、システム監査の視点から考えてみませんか。

写真提供：仲　会長

巻頭言

『いよいよ動き出すシステム監査基準＆管理基準の改訂』

会員番号　0555 松枝憲司（副会長）

初版のシステム監査基準は、1985年1月に制定され32年が経過しました。1996年の一部改正の後、2004年の改訂では、現在のシステム監査基準とシステム管理基準の2本立ての構成となりました。その後2007年に「金融商品取引法」への対応という観点から「システム管理基準追補版(財務報告に係るIT統制ガイダンス)」が発表されました。それから10年が経ちましたが、昨年実施されたシステム監査学会のアンケート調査結果では、「システム監査基準／システム管理基準」の見直しの必要性に対しては38.2%が必要であると回答し、金融以外の業種を中心とした当該基準を利用しているグループでは、54.3%が必要であると回答しました。理由としては、現状のITに合っておらず新技術・IT環境への対応、環境変化・経年劣化、セキュリティ環境の変化への対応、法令・制度への対応、内部統制の強化への対応、外部委託管理強化への対応、新基準・国際標準への対応等が挙げられていました。

今回経済産業省で、このシステム監査基準と管理基準の改訂が計画されています。具体的な改訂の方向性等についてはこれから示されることになりますが、本改訂作業には、当協会及びITアセスメント研究会（旧基準研）のメンバも、様々な形で協力していきたいと考えています。

ご興味のある方は是非当研究会にご参加ください。

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：AI 関連

2017.5

めだか　【　AIとシステム監査　】

日本におけるAI研究の主要組織である人工知能学会（JSAI）は、人工知能に関する研究の進展と知識の普及を図り、もって学術・技術ならびに産業・社会の発展に寄与することを目的とする団体であり、2016年6月に国立情報学研究所の山田誠二教授がJSAI会長に就任された際のご挨拶「AIブームに学会は何を残せばいいのか」から抜粋して日本におけるAI研究の状況を見通してみる。

“・・・人工知能AIは，数年前から第3次ブームを迎えているといわれています．正直なところ，私が会長に就任する頃には，このブームもピークアウトしているのでは，と予想していました．しかし，幸いにもその予想は外れ，AIブームは続いており，マスコミではAIの研究成果，企業のAI応用などに関するニュースが連日伝えられています．研究のブームもそうですが，日本でのブームはアメリカでのブームから数年のタイムラグがあるので，まだあと数年，つまり私の在任中は日本のAIブームが続きそうです．さて，このようなAIブームの時に人工知能学会は何をし．何を残すべきなのでしょうか．これを考え実行することが，私の会長在任中の第1の職務と考えています．と言っても，今ゼロから考え始めたのでは，2年の任期中の実現には間に合いませんので，いくつかアイディアを思索中です．ただし，アイディアレベルなので実行を保障するものではありませんし，明言したことに縛られるのも嫌なのであくまでも達成目標ということでお話しさせていただきます．・・・日本のAI 研究は新しい枠組みを提案する研究，強力なオリジナリティーで新研究分野を創出できるような研究がまだ十分ではないということです．実際，AI 研究の研究トレンドは，そのほとんどが欧米発であり，日本のAI 研究はすでに流行っている研究トレンドを周回遅れで追いかけているという印象が拭えません．このような状況の打破に，本学会が貢献することは学会の最重要課題であると認識しています．次に，日本の大学の研究と企業での応用開発のマッチングを促進するシステムを作りたいと思っています．偏見かも知れませんが，日本のメーカーの場合，AIの応用研究をする場合に国内の大学や研究機関よりも海外の大学や研究機関と共同研究・開発を指向する傾向が強いように感じています．それから，現在のITベンチャーでやられているAI応用のデモを見ると，研究レベルでは日本の大学や研究機関で10年以上前にいろいろやられていた枠組みのデジャブが感じられます．つまり，現在そして今後も日本の企業と日本の大学・研究機関が共同研究・開発をすることには大きな可能性があると感じます．ただ，その仲介をするシステムがないため，まだまだ活性化の余地を残していると思われます．おそらく日本のAI研究者・開発者が所属する最大の組織の1つは本学会ですので，そこでそのようなマッチメイキングをシステマティックに行うことには大きな意味があると考えています．・・・”

JSAIでは、日本の企業と日本の大学・研究機関のマッチメイキングに取り組んでいて、2017年は5月に名古屋市（ウインクあいち）で全国大会が開催される。AIへの見通しは、AIがヒトの知能と対立するものとみるか補完しあうものとみるかで相違するが、「AIとシステム監査」に関しては、システム監査を補完する技術としてどんな適用ができるかを探っていきたい。（空心菜）

（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>

2017.5

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、システム監査の新たな展開に向けて、システム監査の活性化、及びシステム監査を核とした「ITアセスメント」と「ITアセッサ」の定着に努めています。ITアセスメント研究会（松枝憲司主査）は、ITサービスの提供者と利用者双方における適切な管理を維持・向上させる活動を、ITアセスメントととらえて、それに必要な活動領域に関する研究を、下記のように行っています。

(1)ITガバナンスに関連する事項

a)　JISQ38500：2015の活用と普及に関すること

b)　ISO/IEC38500関連基準（38501,2,4,5）の日本語化

c)　ISO38503（Assessment of the governance of IT: ITガバナンスの評価基準）のISO化支援

(2)システム管理基準の改訂、活用等

現状のシステム管理基準を現場でより活用できるよう補足・改訂等を研究する。

システム監査学会の遠山暁会長は、当協会第16期通常総会特別講演「現代の情報化実践におけるシステム監査の再考」の総括で、システム監査の課題を次のように挙げています。

○ITガバナンスの実現への寄与まで監査目的を拡大することによって、システム監査の役割期待が増幅するが、正しく「舵を取る」なかで、矛盾やジレンマが発生する。

○IS（情報システム）を社会構成主義的発想でのITと人間その他コンテキストとの関係的存在として認識・構成することによって、能動的・積極的な環境適応レベルのガバナンスの実現も可能になる。

○能動的・積極的な環境適応レベルのガバナンスの実現を目指す限り、段階的・順序的な設計の枠組みによる伝統的な監査手順は、有効性が低下する。

○ISの企画・開発段階でも人的・組織変革が連動し、システムの利用段階で人的・組織的変革と共にシステムの再設計・開発が連動することを前提にした監査枠組みを確立する必要がある。

○組織体の能動的・積極的環境適応において鍵を握る意図せざる偶発的な創発的行動や判断・波及的効果をいかに監査として評価・検査するかが課題である。

「ITアセスメント」は、「ITガバナンス」の6原則である責任、戦略、調達、パフォーマンス、コンフォーマンス、人間行動の原則に沿って、評価、指示、モニタのEDMサイクルがきちんと回っているかを評価し、また、変化する環境のもと、ITにかかわる経営課題や、ITを利活用する人々のニーズに応えていく能動的・積極的なアセスメント活動といえます。「システム監査」は、情報システムの信頼性、安全性、有効性について、独立した立場から監査し、当該システムの責任者に報告し、あわせて、報告書の公表により、システム責任者の社会的説明責任を果たすことを支援する活動です。システム監査人には、「システム監査基準」と「システム管理基準」のもとで能動的・積極的なアセスメント、具体的には、適用業務の環境変化に応じて、管理策をアップデートして監査することが求められます。

<目次>

2017.5

第２２１回月例研究会：講演録

【　AI/IoTの品質保証と次世代技術　】

会員番号　2581　斉藤　茂雄

【講師】日本アイ・ビー・エム株式会社　東京基礎研究所　インダストリーソリューションサービス
品質エンジニアリング　部長　細川 宣啓 氏

【日時・場所】2017年3月28日(火)　18時30分～20時30分　機械振興会館　B2F　ホール

【テーマ】「AI/IoTの品質保証と次世代技術」

【要旨】

人工知能技術やIoT技術に関するビジネスへ注目が集まって久しいが、多くのプロジェクトが実験やパイロットの域を出ないのも実情である。実ビジネスへの適用障壁は様々あると言われているが、本講演では、その最たる例である「人工知能の品質保証」について取り上げる。

はじめに人工知能用のハードウェア、ソフトウェアの現状、先進研究を述べ、次にAIに対する品質保証の立ち遅れや現状の問題点を指摘する。最後にこれら解決の糸口や、どのようにこの技術を捉え産業を発展させるべきか考える。今回の講演が、あまり知られることのない人工知能の品質保証について、皆様の一助の考となることを期待する。

【講演録】

１．人工知能は今「どこまで」実現できているか？

自動車の自動運転の商用化、患者の遠隔診療への適用、軍事への利用など人工知能技術の適用範囲は広がっている。人々には漠然と、人工知能（コンピュータ）は人間を超えるという意識があり、一部には「人工知能によって人類が絶滅する」といった恐怖と危機感を抱く者もいる。

確かにコンピュータの性能面には飛躍的なものがある。シンギュラリティ（Singularity）という言葉があるが、この概念では「人工知能が全人類の処理能力を超える点は2045年に到来する。」と考えられており、これが量子コンピュータなどの実用化により、2038年にアップデートされたという説もある。

しかしながら、実際はそれほど単純な話ではない。たとえば、「人間ひとり相当のリアルタイムな深層学習をノイマン型コンピュータで実現するためには」、

・莫大な計算能力　6Exa　FLOPS（4億8千万個のプロセッサコア、480ペタバイトメモリ・・・）
・巨大な設備空間　東京ドーム1.8個相当の設備面積
・膨大な消費エネルギー　2.4GWhの電力消費、120万キロワットの原子炉が２つ必要

が必要との試算もあり、おおよそ実現不可能に思える。

一方、大量のデータを取り込み、このデータにより成長する「人工知能」には人間の「右脳」に相当する判断力を求めることは非常に難しい。「だいたい」や「お世辞」「恋愛感情」をどうデータとして教え込むのだろうか。未踏の領域でもある。

２．人工知能は何が問題か

先のような状況を踏まえ、生物の脳の仕組みを模した回路で構成する半導体チップとして、「ニューロモーフィック・デバイス」が開発されつつある。このデバイスは以下の特徴を持つ。

・動作時の消費エネルギーが極めて少ない

・高いリアルタイム性能→実時間での物体認識を実現

・高い欠陥耐性と信頼性→製造プロセスのバラツキやランダム欠陥に高い耐性＆並列化による冗長性

・高いスケーラビリティ→１つのデバイスから数万個のデバイス連結まで対応

このハードウェアデバイス技術はすばらしいが、「活用」面で大変な課題がある。人工知能技術発展の本質的課題といえる。

（１） ソフトウェア開発環境の充実

・これまでの一般的なソフトウェア開発とは大きく異なる開発環境

・プログラミング言語：Corelet が Matlab で動作

・シミュレーター：Compass

（２） 人材の育成

・ニューラルネット、深層学習の深い知識

・ニューロモーフィック・デバイスの知識

（３） 品質保証

・従来のシステム検証手法が適用できない

・実世界の状況に応じて挙動の正しさが変わってくる→普遍性を求めることが難しい

・品質や信頼性の定義はまだこれから→検証シナリオの爆発的な増大

上記の課題の中で特に人材の問題は大きい。ディープラーニング、ニューラルネット等の人工知能についての専門教育を受けた人材はまだほとんど居ないといっても良い。

更に最も問題なのは、これらのシステムを束ねて「品質保証」する人間が居ないということである。人工知能技術に対する「品質保証」には従来の古典的品質保証技法、デバッグ技法はほぼ通用しない。大量のデータを小さなアルゴリズムのプログラムに取り込んで、出てきたアウトプットが意味を持つ人工知能には、プログラム自体の品質の意味は薄れている。プログラムのバグは取ることは出来るが、出てきたアウトプットが実用に耐えられないという「品質不良」をどうするのか。また、データによって成長する人工知能は、検証のシナリオが増大し、この膨大さにどう対処するかという問題もある。

【記録者所感】

細川氏には、「人工知能」の「品質問題」に取り組む数少ない研究者として、先端研究者の視点で「人工知能の可能性」と「人工知能の未熟さ・危うさ」について、事例を交えながら熱く語っていただきました。筆者は日頃「コンピュータの進歩はすごい。人工知能の進化で世界は様変わりする」と漠然と考えていましたが、「品質問題」という視点で課題の多さを知り、「目からうろこが落ちた」思いでした。

なお、今回は、上記内容のほか、「量子コンピュータ」や IoT の進化型としての「Edge Computing」の概念など沢山の興味深いお話もいただきました。

以上

<目次>

2017.5

支部報告　【　北海道支部 2017 年 4 月の研究会について　】

会員番号　1474 菊地圭（北海道支部）

北海道支部では、以下のとおり 2017 年 4 月の月例研究会を開催しました。

・日時：2017 年 4 月 21 日（金）18:30-20:30
　参加者：6 名
・会場：札幌市男女共同参画センター OA 研修室（札幌市）
・演題：「改正個人情報保護法のポイントについて」
・講師：北海道支部　菊地圭

＜概要＞

5 月 30 日から施行される改正個人情報保護法や関連する出来事について、公開情報を元に浅く広く紹介し、参加者同士で討議しました。SAAJ 北海道支部 Facebook ページを通して参加申込のあった 3 名を迎えて、賑々しい研究会となりました。（画像は、その際の告知に使用したページです）

＜講演内容＞

1．最近のトピック

最近の出来事として、①プライバシーに関する一般の不安（札幌市で計画されていた「顔認証」の実証事件が、市民からの声によりで中止されたこと）　②技術の進歩と、活用の方向性、およびプライバシーインパクト（人影や歩き方から個人を識別する技術の進歩）　の 2 点を紹介しました。

また、2003 年の個人情報保護法施行から発生した主な事件事故や、交通系 IC カード利用履歴の外部提供、同意前に個人情報を自動送信する欠陥からメーカーの解散に発展した事例、購買履歴を糸口に本人が気づく前に病気や妊娠を判定される事例などについて事例共有し、それぞれの問題点を討議しました。

2．主な改正点と背景

まず「個人情報」の定義についてクイズを通して共有した上で、法改正の概要を経産省資料を基に①個人情報保護委員会の新設　②個人情報の定義の明確化　③個人情報の有用性を確保するための整備 ④いわゆる名簿屋対策 ⑤その他（5000 人要件の廃止など）を紹介しました。また、改正の背景として、①国際的な商取引への対応 ②利活用と保護の両立 をキーワードに紹介しました。

3．個人情報を取り扱う組織への影響

概要の紹介として、ガイドラインの変更と、第三者提供に関わる記録や匿名加工情報の扱いについて点検が必要であることを示しました。また、5000 人要件に該当していなかった組織は対応の準備が必要であることを紹介しました。

4．システム監査の視点から見た改正対応

ＳＡＡＪの資料を基に、システム監査と情報セキュリティ監査それぞれの定義を参照した後、経営層が抱く問題意識（ＩＴガバナンスの視点から十分な対応ができているか 等）と、システム監査人としての視点

（単なる法令準拠や改正対応の確認のみならず、ＩＴガバナンスに寄与するために個人情報の利活用も視野に入れた取り組みをしているか等）について触れました。

5．各認証制度との関係について

主な認証制度として、①プライバシーマーク認証制度　②ＩＳＭＳ認証制度　③クラウドセキュリティ認証制度 を紹介し、それぞれの認証基準や個人情報保護に関する要求事項の概要、規格改定の動向について紹介し、討議を行いました。参加者からは、①～③以外の認証制度について質問があり、道内企業の取得動向などについて情報交換しました。

6．まとめ

JNSA の調査では毎年約 4%の人が媒体の盗難・紛失などの事象に遭遇しており、トレンドマイクロ社の調査では事件事故対応の流れが文書化され定期見直しされている企業は 4 割弱に過ぎないとの事です。

また、市民感情としての個人情報の価値観の変化（個人情報保護を「当たり前」と捉えつつも、利用規約の不明確なスマートフォンアプリに個人情報を登録する、ＳＮＳにアップロードした顔写真に他人をタグ付けする 等）や、企業における個人情報の取り扱いの危うい例が見受けられます（例：防犯カメラ画像の目的外利用、採用希望者のＳＮＳ投稿をチェック 等）

上記の事実を元にして、講師の私見に過ぎませんが、①個人情報に関する事件事故はなくならず、ますます深刻化する恐れ　②法令改正と実社会の動きには、これからもギャップが残ること　③法令の変化を把握しない企業は知らぬうちに法令違反となる可能性があること　に触れました。

今回の発表は、法改正の概要を紹介した「入り口」であるため、今後に向けた中間のまとめとして①今回の法改正は現行法の問題を修正したもの　②個人情報取り扱いの理想型は「保護」「活用」の両立　③理想型に到達するまで色々なトラブルやあつれきが想定されること（特にクラウド、ビッグデータ、IoT 周辺）と考えました。システム監査人は、それらのトラブルやリスクを敏感にキャッチし、保護ｖｓ活用の調和が取れるように被監査側に発信できる貴重な立場であるため、今後の活躍が必要、と述べて締めくくりました。

最後に、直近で必要な対応として、組織の主な課題には①法改正への対応 ②匿名加工情報など新しい制度への対応 ③5000 人要件撤廃に伴う対応要否 をあげました。さらに個人の課題として ①関係している団体（ＰＴＡ、町内会など）について 5000 人要件撤廃の影響を確認すること、②改正にかかわらず、自分自身と家族の個人情報とプライバシーを大切に扱うことを提案しました。

＜最後に＞

講師自身も漏洩を複数経験（もちろん漏らされる方）しており、個人情報保護やプライバシーについて特に問題意識を持っています。また、個人情報の保護と活用の両立も必須と考えている一人です。

われわれシステム監査人としては、「法制度」「実社会」「ＩＴ」それぞれの面から個人情報やプライバシーについて理解を深めておく必要があると思います。

今後の研究会では、ガイドライン（通則編、外国にある第三者への提供編、第三者提供時の確認・記録義務編及び匿名加工情報編）や、法改正後の社会の動きをテーマに取り扱いと考えています。

以上

<目次>

2017.5

支部報告　【　近畿支部　第１６４回定例研究会　】

会員番号　０６４５ 是松 徹　（近畿支部）

１．テーマ　「これまでのシステム監査からこれからのシステム監査を考える」

～事故、犯罪、法制度の歴史的課題からICT時代のシステム監査を考察する～

２．講師　　大阪成蹊大学　名誉教授　　大阪経済法科大学　客員教授

松田　貴典　氏

博士（国際公共政策）／技術士（情報工学）／公認システム監査人

３．開催日時 ２０１７年1月２０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

ＩＣＴの高度化が生み出した豊かな情報化社会に潜む「情報システムの脆弱性」を念頭に置き、システム監査に関連する事故や犯罪、法制度等の歴史的課題からシステム監査を振り返るとともに、これからのシステム監査について課題を含めて幅広くお話しいただきました。

＜講演内容＞

５－１　ICTの高度化にともなうビジネス活用の進化とシステム監査を俯瞰

- 電子計算機として普及しはじめた1960年代のEDPSの時代から、現在のICTによる「U-Japan」構想に至るまで、ビジネス活用における進化が続いている。
- ICTの高度化に伴い、2010年代からクラウド／IoT／ITガバナンス／ビッグデータといった概念が監査対象となり、情報システムの多様性やコンプライアンス問題等が監査の課題として浮上してきた。

５－２　銀行が体験したコンピュータ犯罪と脆弱性

- 1981年に某銀行行員がオンライン端末を不正操作して巨額の現金他を横領するオンライン横領・詐欺事件が発生した。本事件は、裁判官により社会インフラとなったコンピュータシステムが内部要員により容易に悪用され得る弱点（脆弱性）を潜在化させることを明らかにされ、社会に大きな影響を与えた。
- 本事件を契機に法改正がなされ、「電子計算機使用詐欺罪」が新設された。このように何かがあると法律が変わる流れであり、先行して予防するまでにはなかなか至らないのが現実である。

５－３　個人情報の漏洩と法・制度への影響

- 1989年に行政機関を対象とした旧法が施行されたことを皮切りに、個人情報保護法の全面施行（2005年）、番号法の施行（2015年）と運用開始（2016年）、改正個人情報保護法／番号法の施行（2017年）と法・制度の整備が進められてきた。
- その一方で、1999年に発生した地方自治体での住民票データ22万人分の流出以降、国内における

個人情報漏洩事件等が続いている。IC乗車券の利用履歴のベンダー提供や大手教育出版系企業における事例は個人情報保護法改正の背景ともなった。

- これらを通し、社会における大量の個人情報の散在、組織の隠蔽体質、プライバシー侵害への危険性・不安の増大、プライバシーパラドックス、ビッグデータとしての個人情報の利用が困難等の問題がクローズアップされてきた。
- 監査との関連では以下のように考える。
  - 特定個人情報保護評価では、リスク対策の監査と自己点検が求められる。また、罰則が強化されるためコンプライアンス視点での監査も重要となる。
  - ネットワークビジネスの高度化を背景に社会は厳格な個人情報保護を求めており、ビジネスプロセス全体や経営視点での監査の実施、外部監査の義務付け等の監査の進化が要請される。
  - 個人情報保護マネジメントシステムの監査は内部監査として行うが、監査意見の強化と指摘改善を図るために、少なくとも年1回の外部監査が必要である。

５－４　情報資産の保護とコンプライアンス監査

- 情報システムに関する法的な問題は、経営者自身の無知、従業員の無知・考慮不足等による違法行為が多い。システム監査人は助言・勧告のみならず、緊急改善を指摘することが求められる。
- 【著作権法の侵害行為】：ソフトウェア不正コピーの重大事件（事例紹介4件）が散発している。さらに、ビジネス情報に関連した著作権侵害行為（一般的侵害行為、企業や組織内での違法行為）が発生しているが、企業や組織ぐるみの犯罪行為を引き起こすことがあり、当事者の違法性認識が薄い場合も多い。最近のDeNA事件（まとめサイトでの他人の著作物の無断転用等）は、組織的な「情報倫理」「企業倫理」の欠如例と言えよう。
- 【インターネット取引の対応】：ビジネスプロセスとして以下があり、それぞれに対応する法律・制度等が存在する。①Web広告・宣伝、②通信による契約、③商品発送、④決済、⑤その他（Webサイトの安全性確保）　例えば、①のWeb広告・宣伝プロセスでは、特定商取引、景品表示法、著作権法、消費者契約法、不正競争防止法等による法的規制が存在する。
- 【不正競争防止法の侵害行為】：代表的な事例としてインターネット「ドメイン名」事件がある。（事例紹介3件）　また、話題となった不正競争防止法関連事件が見受けられる。（事例紹介8件）ICT関連として、事例を通して不正競争行為とされる行為の類型が整理できる。
- 【コンピュータウイルス関連】：ウイルス作成による事件を契機にウイルス作成・配布を不正指令電磁的記録に関する罪（コンピュータウイルス作成罪）とする刑法改正が行われた。（2011年施行）　最近のウイルス関連事件では、パソコン遠隔操作事件（男性4名の誤認逮捕を誘発）、スマホ遠隔操作の一斉摘発があげられる。ウイルスの作成やバラマキ防止の法改正は後追いの対応であり、スマホのぞき見等からストーカー行為に発展する事例もあり、「情報倫理」の問題として幼い頃からの教育が必須と考える。
- ICTが高度化すると情報システムの多様化が起こり、コンプライアンス監査がより求められる。コンプライアンス監査はICT関連のみではないものの、ICTに関連する監査は「法とICT」の両面から

のアプローチが必要であり、システム監査人が監査を行うことになる。

５－５　これから求められる監査技術の進化への対応

- 2010年に検事による証拠データの改竄事件が発生した。この時にはデジタルフォレンジック技術により証拠データを抽出し、改竄が判明した。当技術は、不正アクセスや機密情報漏洩等の犯罪における捜査手法として注目されているが、外部からの侵入やデータ改竄がないか、情報セキュリティ監査や安全対策の面からも重要な技術であり、システム監査人が修得すべき技術である。
- このところ大きな不正会計事件が発生している。（事例紹介2件）　会計監査手法の進化として、試査からCAAT等による精査の方向性が出てきているが、今後（将来）はAIによる精査と分析が考えられる。AIにより常時監視される「継続的監査」が実施されることも想定される。

５－６　これからのIoT時代に備えてIoTセキュリティの監査をどのように考えるか

- IoTには固有の課題が存在する。（IPA「IoT開発におけるセキュリティ設計の手引き」参照）　これを踏まえて品質管理に「セキュリティ品質」を定義し導入する。
- IoTのライフサイクル（方針、分析～運用・保守）における各工程別で監査を実施する。監査では各工程でのガイドライン遵守状況から問題点等の洗い出し・分析を行い、PDCAの「C」だけでなく管理基準の改訂に繋げる「A」の役割も果たす。（IoTコンソーシアム・総務省・経済産業省「IoTセキュリティガイドライン1.0概要」参照）
- セキュリティ管理基準は、企業内と業界で統一する。

５－７　これからのシステム監査の課題

- 高度情報化時代では脆弱性に関して視野を広げる必要がある。（ICTの脆弱性のみが「脆弱性」ではない。）
  - 脆弱性には、①情報技術（IT）側面、②経営管理・組織的側面、③国際・社会的側面、④法・倫理的側面の４つの側面が存在し、潜在化する。
  - 脆弱性は脅威の現実化（顕在化）の誘因となる。脆弱性に対するコントロールの強弱で脅威の現実化（顕在化）する「リスク」が発生し、高くも低くもなる。従って、リスクの起因となる脆弱性を押えることが重要である。
- 高度化・複雑化・多様化する情報化の時代のシステム監査は、監査対象に特化した専門監査人が必要であり、必要によっては業界や事業活動独自の管理基準の活用やサブコントロールの作成が望ましいと考える。これからの時代にも主旨・体系等が独自基準のベースとなるシステム監査基準・管理基準はさらに重要となると考えられ、まずは時代に即した当基準の改訂が急務である。
- システム監査は組織体のITガバナンスの実現に寄与し利害関係者に説明責任を果たす役割があるが、今なおこの実現に十分至っていない。進化と多様化する「情報システムの脆弱性」を俯瞰し、求められるシステム監査を追及することが経営者に寄り添う監査の実施には肝要である。

６．所感

事故・犯罪の過去事例や法制度を振り返り、これらと紐づいたシステム監査の課題を具体的に取り上げていただくことで、改めてシステム監査と社会との接点やシステム監査の全体像を見直す有益な機会となりました。中でも、①多様化する情報システムに対してはコンプライアンスの視点が重要であること、②法的な問題は経営者自身の無知、従業員の無知・考慮不足等に起因することが多いこと、③法と IT の両面からのアプローチがシステム監査人に要請されること、④今日では、脆弱性を ICT の脆弱性のみが対象になっているが、これでは視点が狭く、経営や組織、社会、法律等の側面まで拡げることが重要である等、システム監査の視点の多様化の必要性が印象に残りました。

また、システム監査基準・管理基準が 2004 年以降に改訂されずにその実効性が気になっていましたが、将来の動向を見据えた上でその重要性について言及されたことを受け、当基準の位置付けや意義について再認識をさせていただきました。今回のご講演は盛りだくさんの内容であり、1.5 時間ではとてももったいない状況であり、また是非続編を拝聴したいと感じた次第です。

以上

<目次>

2017.5

支部報告　【　近畿支部　第１６５回定例研究会　】

会員番号　1709 荒町 弘

１．テーマ　　「事業継続計画（ＢＣＰ）の概要とＩＴ－ＢＣＰについて」

２．講師　　京セラ株式会社　本社　経営推進統括部　経営企画部
事業継続計画課責任者　野原 英則 氏

３．開催日時　２０１７年3月１７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

講師の所属する組織では、２０１１年の東日本大震災の後、事業継続に対する会社の取り組みを明確にすべく、経営企画部門に組織を設置し、ＢＣＰ策定に取り組んで来た。講師の野原氏はその部署の責任者としてＢＣＰの運用状況の点検評価及び継続的な改善を担っている。

企業にとってＢＣＰ策定と運用は経営上の必須事項であるとの認識のもと、ＩＴ部門での経験もいかしてＩＴ－ＢＣＰの策定と運用管理についても担当している。企業にとってのＢＣＰとは何なのか、という基礎部分からステップを踏んだＢＣＰ策定の手順の紹介、そして、そのステップを応用したＩＴ－ＢＣＰ策定手法について、国が示すガイドラインを活用しての取り組み方法を紹介いただいた。

（第１部）事業継続計画（BCP）概論

事業継続への取り組みが高まりつつある背景と事業継続計画とは、といった基本部分の解説について、内閣府の示すガイドラインでの定義と国際規格であるＩＳＯ２２３０１の定義について説明いただいた。内閣府公表の日本国内におけるＢＣＰの策定状況としては、大企業では「策定済み」が６割程度、「策定中」を合わせると８割程度の普及率であるが、中小企業においては、「策定済み」が３割程度、「策定中」を加えても４割程度の普及率であり、まだまだこれからという感が強い。また、ＢＣＰの策定はできたが、実効性のあるＢＣＰとするためには、定期的な訓連や点検評価による継続的な改善が必須となるが、企業の現場では、なかなかそのような時間をつくること自体が難しいといった現実がある。

次に、ＢＣＰ策定の基本的なステップとして、方針策定から是正・見直しまでを７つのステップに分けてその取り組みについて解説いただいた。ポイントは以下のとおり。

【ステップ１：方針策定】

全てを守るのは難しいという前提でもって、事業戦略やステークホルダーの要求に基づき方針策定から継続的に改善していくための体制を確立する必要がある。

【ステップ２：リスク／事業影響度分析】

災害の特定から事業への影響を確認し、目標復旧時間／レベルを考える。重要な経営資源は５Ｍ＋１Ｅ＋１Ｉの視点で分析する。重要な経営資源が想定災害発生時に受ける影響を予測し、かつ、現在の経営状況でどの程度の事業中断が許容できるのかを把握する。

【ステップ３：戦略・対策の検討・決定】

重要な経営資源に対する対策の考え方として、「被害を最小化するための対策」「被災したとしても早期に復旧するための対策」「復旧するまでの代替策」の３段階で考える必要がある。また、早期復旧対策を考えるプロセスでは、原因から想定被害を導き出す原因事象で考えるアプローチだけでなく、被害が起こった場合にどうするか、といった結果事象から対策を考えるアプローチも有効である。事業継続戦略を考えてから対策に考える方法もあるが、対策を考える中で事業継続戦略が決まるという考え方もある。

【ステップ４：対策実施】

ＢＣＰは経営であるという認識のもと、リスクを許容する選択肢やリスクファイナンスで対応することも必要。

【ステップ５：行動計画の作成】

初動と復旧のそれぞれのフェーズにおいて、時間の流れ（タイムライン）に応じた組織のとるべき行動と役割分担を明記するようにする。各組織間で相互の行動を理解し合い、各部門が連携のとれた対応行うことが重要。

【ステップ６：訓練実施】

自部門の復旧対応が他部門の復旧の妨げとなることがあるため、全体で調整し、全体を俯瞰した事業復旧が求められる。

【ステップ７：是正・見直し】

是正・見直しの対象が、特定組織の改善事項であるのか、他組織に共有すべき改善事項なのかを判断し、他組織に共有すべき改善事項があれば、組織全体に是正を促す。あくまで経営判断として行うことであるとの認識事項である。

（第２部）「中央省庁における情報システム運用継続計画ガイドライン」をもとに IT-BCP を考える

中央省庁の情報システム担当者に向けのガイドラインとして手引書である標題のガイドラインを企業の情報システム担当者向けとして読み替えてみた。具体的には、IT-BCP の策定と運用の流れについて、第１部で紹介した活動ステップ１～７と比較して解説いただいた。

１．基本方針の決定

優先復旧すべき重要システムについて定め、合意形成する段階である。ポイントは業務システムだけでなく、そのシステムを支える共通情報インフラが対象範囲から漏れないようにすること。

２．実施・運用体制の構築

実施・体制を考えるうえでのポイントは、IT 部門の位置づけである。全社的な IT 部門であるのか、例えば事業部内 IT 部門であるのかとうことである。

３．想定する危機的事業の特定

IT-BCP の対象とする危機的事象について決定する。ここでのポイントは、関連部門の業務継続計画で

対象とした危機的事象だけでなく、情報システム特有の危機的事象（故障・ウイルス感染・不正アクセス等）も対象として考え、関係部門やユニットごとの BCP との整合性を持たせること。

４．情報システムの復旧優先度の設定

この段階でのポイントは、優先業務と情報システムとの関連を整理することである。IT 担当と業務担当の目線は異なるということを前提に、部門を越えた十分なコミュニケーションを取り、優先復旧後の設定を行う必要がある。目標復旧時間（IT-RTO）設定にあたっては、代替手段による業務継続も考慮したうえで優先復旧対象業務の RTO を基準として設定する。

５.被害状況の想定

危機的事象が発生した際に重要な情報システムに係る重要な経営資源を明らかにする。重要な経営資源の選定は、５M＋１E＋１I（*）の視点で行うということがポイントである。

(*)　5M:Machine（機械・設備）、Material（資材品・サービス）、Man（作業者）、Method（作業方法）、Measurement（検査・測定）　１E：Enviroment（環境）　１I：Information System（情報）

また、実効性ある対策を策定することが目的であるため、軽すぎる被害状況の想定にしないことが重要である。

６．現状対策レベルの確認と脆弱性の評価

ここでの留意すべき点は、情報システムごとに、IT-RTO を達成できる対策レベルにあるのかを評価する。情報システムの復旧継続を困難とさせる重大な脆弱性について最低限評価しておく必要がある。

・危機的事象発生時の体制と連絡方法の整備状況

・同一拠点内でのハードウェアの対策状況

・重要なデータのバックアップ状況

・ハードウェアやソフトウェアの再調達が困難になる可能性の有無の把握

７．構成要素ごとの目標対策レベルの設定（復旧戦略の策定）

情報システムを IT-RTO 内に復旧させるための、復旧対策の計画を立案し、目標復旧レベルを設定し、目標レベルを達成できるように管理していくことを定める（復旧戦略の策定）。

８．事前対策計画の検討

目標対策レベルと現状対策レベルのギャップを解消し目標対策レベルに近づけるための方策をシステムごとに検討し、事前対策計画を作成する。予算等の関係から、目標として定めた対策をするに実施することが難しい場合には、「優先的に取り組むべき対策」を整理していくことが望ましい。

９．非常時の対応計画の検討

非常時の対応として、まず重要なことは、現場でリーダーシップを発揮して組織をあるべき方向・活動に導くキーマンの存在である。いざというときに、このような行動をとれるキーマンを育成する、あるいはそのような意識付けを行っておくことが重要である。また、システムベンダや OB・OG による外部からの応援なども考えておく必要がある。

１０．教育訓練計画・維持改善計画の検討

教育訓練における目的は、大きく以下の３つがある。

・平常時の情報システム運用継続計画の維持改善活動への理解の向上

・非常時対応計画の理解と対応系能力の向上

・事前対策内容の動作確認と検証

（第３部）「IT-BCP 策定モデル」をもとに監査の視点で、IT-BCP の課題を考察する

NISC（内閣サイバーセキュリティセンター）から「IT-BCP 策定モデル」が示され、その中で、東日本大震災の事例をもとに検討すべき諸課題について指摘しており、実効性の高い計画策定のモデルとして取りまとめが行われている。以下は、諸課題の例である。

(1)非常時の意思決定に関する在り方

（IT-BCP 策定時に IT 部門と関連部門を含めた連携体制づくりの必要性）

(2)非常時の情報収集・伝達・発信や業務系の情報システムの在り方

（災害発生後の情報システムの制約事項（リソース状態等）を前提とした計画の必要性）

(3)データの消失を回避するための対策の在り方

（大規模災害時に同時被災しない場所でのデータ保管について）

(4)教育・訓練の在り方

（訓練は、情報システム切替／切戻の手順確認＋IT-BCP の継続的改善も目的であるということ）

実効性の高い IT-BCP であることをどのように確認・評価すればよいか。野原氏が実際に監査するにあたり、確認すべきポイントについて紹介いただいた。

・目標復旧時間（RTO）に対して訓練時の結果はどうであったか。

（訓練は２年に１回くらいの頻度で行っている）

・本番系と別サイトに構築したコールドスタンバイ環境とのデータの整合性。

・復旧作業にあたるオペレータの移動時間。

（所感）

このたびの講演では、実効性ある IT-BCP の策定とその維持管理に必要となる準備から対策の検討と実践について、細かな点を含めて理解を高めることができました。ご説明の内容をお聞きして、各種ガイドラインの読み込みと、野原氏ご自身が所属企業の事業継続計画の実践責任者として日頃実践していることから得られる知見の豊かさを感じました。

経営層に対して IT-BCP の必要性を説明しても、経営に資する IT-BCP という観点で理解を得るのは難しいと感じていました。IT-BCP は戦略の一部であり、災害発生時の業務復旧戦略としての IT-BCP という認識であれば経営層からの理解も得やすいのでは考えます。参考となる講演、ありがとうございました。

以上

<目次>

2017.5

【　注目情報　】

■「世界中で感染が拡大中のランサムウェアに悪用されているMicrosoft製品の脆弱性対策について」公表【ＩＰＡ】

2017年3月15日(日本時間)にMicrosoft製品に関する脆弱性の修正プログラム MS17-010が公表されました。この脆弱性がランサムウェアの感染に悪用され国内を含め世界各国で被害が確認され、英国では医療機関において業務に支障が出るなどの深刻な影響が発生しています。ランサムウェアに感染するとコンピュータのファイルが暗号化され、コンピュータが使用できない被害が発生する可能性があります。 今回観測されているランサムウェアは Wanna Cryptor と呼ばれるマルウェア（WannaCrypt, WannaCry, WannaCryptor, Wcry 等とも呼ばれる）の亜種であると考えられます。

※ランサムウェアとは、「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語です。感染したパソコンに特定の制限をかけ、その制限の解除と引き換えに金銭を要求する挙動から、このような不正プログラムをランサムウェアと呼んでいます。

IPA　https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html
Microsoft　https://technet.microsoft.com/library/security/MS17-010
JPCERT　https://www.jpcert.or.jp/at/2017/at170020.html

■「FinTech（フィンテック）に関する初めての総合的な報告・提言「FinTechビジョン」を取りまとめました」公表【経済産業省】

経済産業省は2016年7月より「FinTechの課題と今後の方向性に関する検討会合」を開催し、FinTechが経済社会に与えるインパクトや課題、今後の政策の方向性等に関し、経営者等ハイレベルな視点から議論を行ってきました。FinTechに関わる実務家や有識者の意見等も踏まえ、今般、総合的な報告・提言として「FinTechビジョン」を取りまとめました。

http://www.meti.go.jp/press/2017/05/20170508001/20170508001.html

<目次>

2017.5

【 協会主催イベント・セミナーのご案内 】

■SAAJ 月例研究会（東京）

特別月例研究会	日時：2017年 6月 3日（土）13時～17時 場所：機械振興会館 地下2階ホール	
	テーマ	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 ～各国の IT ガバナンスの現状と国際標準の活用～（共催：情報処理学会）
	講師	４講演を予定。 平野 芳行　様（SC40 国内委員会長） 原田 要之助　様（情報セキュリティ大学院大学） Geoff Clarke　様（Microsoft） Peter Brown　様（SC40WG１ Convener）
	講演骨子	本セミナーでは、企業や組織で IT ガバナンス、IT 投資、システム監査、情報セキュリティ等を担当している方々を受講者として想定し、本分野に関する国際標準化とその実務に携わる専門家３名を選定しました。講師の方々には、各々が関連する最近の IT ガバナンス、コーポレートガバナンス事案の紹介、国際動向、また、JTC 1/SC 40 で作られた国際標準がその解決、防止にどのように役立つのか、実際にどのように使われているのか等をご講演いただきます。 本セミナーを通し、SC 40 が策定している国際標準への理解とさらなる活用、適切で有効かつ効率的な組織の IT ガバナンスの対策推進を期待したいと考えています。
	お申込み	HPでご案内中です。 https://www.saaj.or.jp/kenkyu/kenkyu/tokubetsu_20170603.html
第224回	日時：2017年 7月 3日（月）18時30分～20時30分 場所：機械振興会館 地下2階ホール	
	テーマ	「ＩｏＴにおけるサイバー攻撃の実態とその対策」
	講師	横浜国立大学大学院環境情報研究院 准教授　　吉岡克成　様
	講演骨子	インターネットに接続された様々な機器・システムの中にはセキュリティ対策が不十分なものも多く、サイバー攻撃の対象となっている。本講演では、サイバー攻撃観測システムにより明らかとなったIoTにおけるサイバー攻撃の実態と、IoTマルウェアの収集・分析・駆除、製造者や公的機関への通知を通じた対策について説明する。
	お申込み	詳細確定次第、ＨＰでご案内いたします。
第225回	日時：2017年 9月 5日（火）	
	テーマ	「未定」
	講師	日本 CISO 協会 アドバイザ ビジネスブレークスルー大学大学院客員研究員 岡田良太郎 様
	講演骨子	詳細確定次第、ＨＰでご案内いたします。
	お申込み	詳細確定次第、ＨＰでご案内いたします。

■ＳＡＡＪシステム監査実践セミナー（東京）

第31回	日時：2017年 6月 22日（木）～6月23日（金） 9:30～17:00（進行状況により若干の変更が生じる場合があります。） 場所：晴海グランドホテル（申込み状況により変更する場合があります）	
	概要	当協会のシステム監査事例研究会「システム監査普及サービス」で実施したシステム監査事例を教材として、ロールプレイングを中心とした演習によりシステム監査を修得することを狙いとしたきわめて実践的なコースです。
	お申込み	ＨＰでご案内中です。 http://www.saaj.or.jp/kenkyu/jissenseminar/jissenseminar31.html

【 外部主催イベント・セミナーのご案内 】

■システム監査学会　研究大会（東京）

設立30周年記念研究大会	日時：2017年 6月 2日（金曜日） 場所：機械振興会館　ホールおよびB2-1号室	
	統一論題	「システム監査の過去・現在・未来 ― システム監査の歴史・課題と将来展開 ―」
	開催内容	システム監査学会 HP でご確認ください。 http://www.sysaudit.gr.jp/taikai/2017_30th_kinen_taikai.html

<目次>

2017. 5

【 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

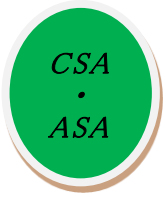
・セミナーやイベント等の会員割引や優遇　http://www.saaj.or.jp/nyukai/index.html
公認システム監査人制度における、会員割引制度など。

・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>

【　ＳＡＡＪ協会行事一覧　】　赤字:前回から変更された予定			2017.5
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
５月	11：理事会	中旬：春期 CSA 面接 16：第 223 回月例研究会「企業 IT 動向調査 2017」	
６月	1：年会費未納者宛督促メール発信 8：理事会 10：会費未納者督促状発送 9～：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）	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」 中旬：春期 CSA 面接結果通知 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 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」 下旬：秋期 CSA・ASA 募集案内〔申請期間 8/1～9/30〕	14：支部会計報告〆切
８月	（理事会休会） 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		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）	16：秋期情報処理技術者試験
	前年度に実施した行事一覧		
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	12,19,26：秋期 CSA 面接 15:第 218 回月例研究会 17～18：第 29 回システム監査実務セミナー（東京：晴海） 20: CSA･ASA 更新手続案内〔申請期間 1/～1/31〕 29：IT アセスメント研究会 30： CSA 面接結果通知	5-6：西日本支部合同研究会 in Matsue（開催場所：松江）
12月	1： 2017 年度年会費請求書発送 1： 個人番号関係事務教育 8： 理事会：2017 年度予算案 会費未納者除名承認 第 16 期総会審議事項確認 12：総会資料提出依頼（1/9〆切） 15：総会開催予告掲示 19：2016 年度経費提出期限	7：第 219 回月例研究会 15： CSA/ASA 更新手続案内メール〔申請期間 1/1～1/31〕 26：秋期 CSA 認定証発送	2：北海道支部総会 10：東北支部総会＆講演会
１月	9： 総会資料提出期限 16：00 12：理事会：総会資料原案審議 28：2016 年度会計監査 30：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 17：第 220 回月例研究会 20： 春期 CSA・ASA 募集案内〔申請期間 2/1～3/31〕 26～27：システム監査実践セミナー	6：支部会計報告期限 25：SAAJ 創立記念日
２月	2：理事会：通常総会議案承認 27：法務局：資産登記、活動報告提出 理事変更登記 28：★年会費納入期限	1～3/31：CSA・ASA 春期募集 下旬：CSA・ASA 更新認定証発送	 24：第 16 期通常総会
３月	1：NPO 事業報告書、東京都へ提出 6：年会費未納者宛督促メール発信 9：理事会	1-31: 春期 CSA・ASA 書類審査 4: 事例に学ぶ課題解決セミナー(お茶の水) 11-12&25-26：システム監査実践セミナー（東京：晴海） 28：第 221 回月例研究会	
４月	13：理事会 30：法人住民税減免申請	初旬：春期 CSA・ASA 書類審査 中旬：春期ＡＳＡ認定証発行 19：第 222 回月例研究会「サイバー攻撃被害を軽減するための研究開発と人材育成の動向」	11：WindowsVistaSP2 サポート終了 15：近畿支部　第 56 回システム監査勉強会（大阪） 16：春期情報技術者試験

<目次>

2017.5

【 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

□■ **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。先月号までの四半期テーマ「技術革新とシステム監査」に続いて、「技術革新」の中でも特に今話題の「AI」に焦点をあてて、「AI とシステム監査」を、今月号から 7 月号までの四半期テーマとしました。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。
・表紙の写真も、随時募集しています
・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。
http://www.saaj.or.jp/members/kaihou_dl.html

<目次>

2017.5

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

ID 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>