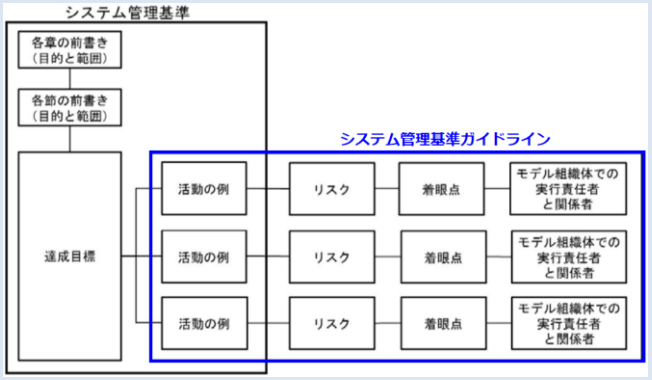
認定 NPO 法人
日本システム監査人協会会報

2023 年 11 月号
No 272

No.272（2023 年 11 月号）<10 月 25 日発行>

(注目情報)
今号の[巻頭言]は、松枝会長による『システム監査・管理基準ガイドラインの公表』です。



巻頭言　『システム監査・管理基準ガイドラインの公表』

会員番号：0555　松枝憲司（会長）

皆様ご存じの通り 2023 年 8 月 10 日に、日本システム監査人協会の HP において「システム監査・管理基準ガイドライン」を公表いたしました。（＊1）本ガイドラインについてはシステム監査関係団体で策定し、代表団体である日本システム監査人協会の HP で公表することとなっております。ガイドラインは基準の実施方法（How）や活動例の着眼点、実施・書式等も記載したものですが、公表されたガイドラインには基準も含まれており、実用上はガイドラインだけで利用できるように構成されています。

また本ガイドラインは、今後テーマ別のガイドラインの策定や公表したガイドラインの定期的見直し等、継続的に取組んでいく事業です。そのため日本システム監査人協会とシステム監査学会は、本ガイドラインの策定に関する協定書を 10 月 1 日付で締結いたしました。両会ともに本ガイドラインの策定についての責任を共有して、本ガイドラインの普及・活用のために継続的に取り組んでまいります。

9 月 23 日には基準ガイドラインに参画した関係団体の講師により「システム監査・管理基準ガイドラインの活用」をテーマに、半日の特別月例会を開催いたしました。セミナーでもお話ししましたが、最も重要ことは本ガイドラインを広く内外に活用してもらうことです。そのため本ガイドラインは、利用規約に従えば誰でも自由に利用可能で商用利用も可能となっています。（＊2）会員の皆様には、是非とも各現場で活用していただくとともに、組織内外への PR もお願いしたいと思います。また本ガイドラインに関する投稿ができるようにしましたので、皆様のご意見をお待ちしています。

本作業はボランティアです。多くの皆様のご協力とご支援をお願いいたします。

＊1＜システム監査・管理ガイドラインサイト：https://gl.systemkansa.org/公表ガイドライン

＊2　同上「著作権と利用規約」ページ　　以上

<目次>

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。

2023.10

めだか　【　この変化の時代にシステム監査が目指すもの - ワクチンを考える - 】

この変化の時代にシステム監査が目指すものを考える。この変化の時代とは、大きくは気候変動、戦争、ウイルスによるパンデミック等であり、システム監査が目指すものとは、正しさである。現代において私たちは常に変化と共にあることを知りシステム監査を考える。

資料を読むと、“人はなぜ病気になって、それをこじらせて死んでいくのか” を科学的にうまく解説している。日本では、現在、感染症、がん、生活習慣病が三大疾病である。

ここで、皮膚に傷ができた場合の白血球の働きを追ってみると、白血球はマクロファージ、リンパ球、顆粒球からなっていて、そのうちマクロファージはサイトカイン（たんぱく質）を出す。マクロファージ、顆粒球や、リンパ球のうちのナチュラルキラー細胞は、ばい菌を食べる。また、サイトカインを受けて、リンパ球のうちのヘルパーT 細胞に伝え、そして、リンパ球のうちの B 細胞は抗体を作り、キラーT 細胞は、ばい菌をとかす酵素をつくる。そして、治る。しかしながら、治らない場合は、サイトカインを受けて、血管が広がり、全身が赤く腫れて、敗血症で死ぬ。

感染症では、1928 年、世界初の抗生物質、つまり細菌を殺すお薬であるペニシリンが発見された。そして、抗生物質が発見される以前は、敗血症で死んでいたが、抗生物質の登場によって敗血症で死ぬ人は激減した。抗生物質は、ほとんどすべての細菌をつぶすことができる。ペスト、コレラ、赤痢、結核、梅毒、淋病、ハンセン病、発疹チフス、腸チフス、産褥熱、盲腸炎などは、治せる病気になった。しかし、抗生物質は、真面目におくすりとして飲んでいることが必要だ。抗生物質だけは、途中で止めては耐性菌ができる。結果、敗血症で死ぬことになる。

抗生物質はウイルスやカビには効かずそれらの感染症対策にはならない。さて、天然痘ウイルスは、日本に仏教と同じ時期に海を渡ってやってきた。奈良の大仏も、天然痘の流行を抑えるために作ったのではないかといわれている。世界中で天然痘ワクチン接種が行われて、1977 年を最後に、自然での感染はゼロになり、1980 年に天然痘根絶宣言がでた。結局、現在に至るまで、天然痘を治す薬は一つもできなかったし、有効な治療法も見つかっていない。ワクチンは、予防に役立ち人類の知恵の勝利である。また、2023 年、mRNA 研究がノーベル賞を受けた。コロナワクチンに貢献したことが評価されたという。

この時々刻々と変化する時代に根本的なものはなにか、システム監査が目指すもの、すなわち正しさを考え、さまざまな出来事と自らの役割に対してあらためて考えてみる必要がある。（空心菜）

資料：「ねじ子の人が病気で死ぬワケを考えてみた」森皆ねじ子 著 王様文庫三笠書房

（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>

2023.10

【投稿】デジタル変革（圧）が強まる中で、人材確保にシステム監査はどう向き合うべきか

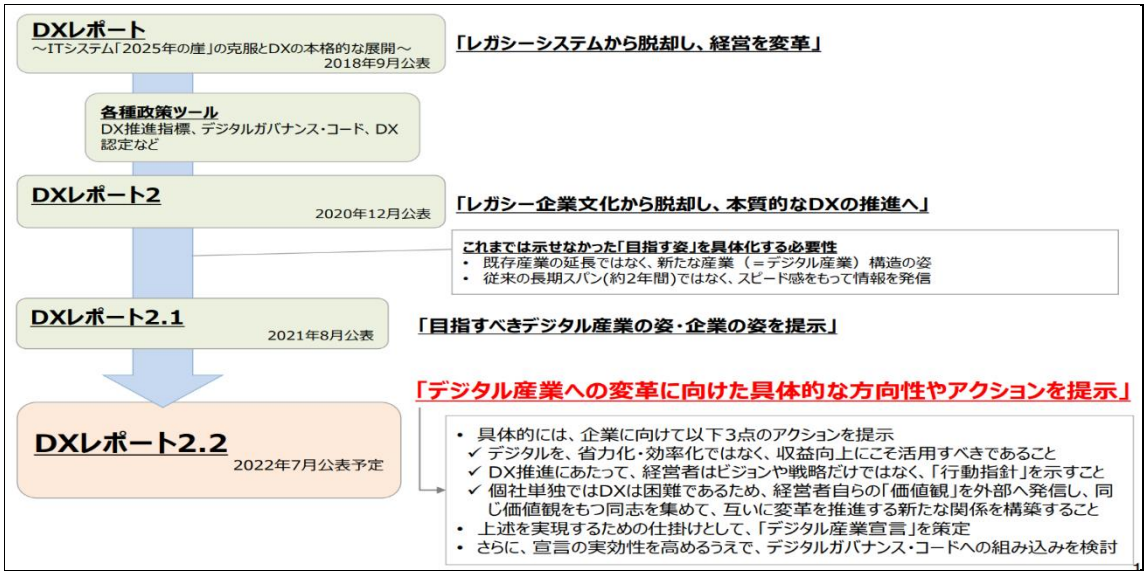
会員番号　0436 大石正人

感染症の蔓延に国際紛争によるエネルギーその他の資源や需要構造の要因も加わり、2020 年から 2022 年にかけての労働市場の大幅な変化に、様々な業界、業種が難しい対応を迫られています。情報政策も所管してきた経済産業省も、かねて IT 投資の需要及び構造変化と、人材ギャップにつき、指摘していました。少し古いですが（2017 年前後）、以下は今も度々引用される同省の委託報告書の記載（抜粋）です。

> 経済産業省が構築した IT 人材の需給モデルに基づきわが国 IT 人材数の推計を行った結果、若年層の人口減少に伴って、2019 年をピークに IT 関連産業への入職者は退職者を下回り、IT 人材は減少に向かうと予想される。また、IT 人材の平均年齢は 2030 年まで上昇の一途をたどり、高齢化が進展することも予想される。その一方で、IT 需要予測から推計される IT 人材需要との需給ギャップから 2030 年までの IT 人材の不足数を推計すると、労働集約業態となっている日本の IT 人材の低生産性を前提とすれば、将来的に 40～80 万人の規模で不足が生じる懸念があることも試算された。　（「第 4 次産業革命スキル習得講座認定制度（仮称）」に関する検討会「IT 人材育成の状況等について」経済産業省より要約抜粋）

（注）https://www.meti.go.jp/shingikai/economy/daiyoji_sangyo_skill/pdf/001_s03_00.pdf

IT 人材の育成については、その後も様々な施策が講じられていますので、状況に変化はあるはずですが、例えばいわゆる DX レポートも、順次更新版が公表されているように（最新版は 2022 年 7 月のバージョン 2.2、下図参照）、デジタル産業をはじめとしたデジタル変革（DX）を迫られる事業主体やそれを担う人材育成に対する要請事項は高度化しています。



（出所）「デジタル産業への変革に向けた研究会」DX レポート 2.2（概要）
https://www.meti.go.jp/shingikai/mono_info_service/covid-19_dgc/pdf/002_05_00.pdf

ただこのＤＸレポート 2.2 でも指摘されている通り、IT 投資の主体が効率化などで、それを従来型の IT 人材が支える構図は大きく変わらず、デジタル変革の成果を上げている事業体は一部にとどまり、担い手となる IT 人材不足が繰り返し指摘されている状況です。このため、一方では新卒・転職市場を中心に、IT 人材（候補）の争奪戦は激しさを増しており、他方では、既存の IT 人材を含め、全社的な学び直し（リスキリング）により、デジタル変革の素養がある人材層の厚みを拡張したり、デジタル変革マインドの涵養に注力する動きが増えているようです。

こうしたデジタル変革の実現手段として、従来のような「内製型システム開発」を選択する企業よりは、いわゆるクラウド型システムによる外部サービスを、自社のニーズに合わせて取捨選択する企業が主流になりつつあるとされています。こうしたクラウドファーストの考え方は、デジタル変革の成果を競うトレンドのなかで、企業トップにも理解浸透しているとしても、果たして自社の人材が、外部リソースの活用を適切に行えているか、を自ら確認する意識が十分かというと、心もとない気がします。

というのも、クラウド型システムは、競合他社での採用例も増えていることなどから、ともかくデジタル変革の実績が上がっていればよい、という発想に傾きがちだからです。おそらく、自組織においてクラウド型システムの採用が増えているから、という理由で、経営者がそのリスクを検証する組織やシステム監査を強化しよう、という発想はなく、その余力があるなら、ただでさえ不足している,一層デジタル変革を推進する人材の方を充実させたい、と考えるのではないでしょうか。

以上のような流れを反映して、システム監査のあり方や手法も変革を迫られています。

システム監査の担い手の多くは、従来型の IT 開発の経験者が多いはずですし、業務経験はあっても、現時点でデジタル変革の最前線で活躍した人材は例外的でしょう。また企業や事業体によると思いますが、デジタル変革やクラウド型サービスの採用は、多くの場合、事業を展開する現場主導で進められ、企画段階からシステム部門が関与する余地は少なくなっていると聞いています。

もちろん、この点は企業や事業体によってさまざまとは思いますが、従前のように IT 投資案件のすべてについて、一旦システム部門で全社的なリスク評価も含めて審査してから、という手順は、迅速な推進が求められるデジタル変革の取り組み（圧力）のなかで、だんだん踏まれなくなっている印象を持ちます。

また多くの場合、クラウド型システムを提供する企業は海外のメガ IT 企業であり、個々の契約先からのシステム監査などを受け入れる事例は少なく、検証可能な利用履歴（ログ）や、自社で実施したリスク評価書・監査報告書などを、契約先に提供する事例がほとんどのようです。契約先が多岐にわたる中、やむを得ないことですが、こうした評価書なり報告書なりを受領し、その内容を検証するのが、クラウド型システムを採用している事業部門の場合、おそらくはシステム監査部門ほどの専門性やリスク感度は持てないと想像されます。

もちろんシステム部門自身が基幹システムをクラウド化している場合は、IT にかかる統制システムを構築したうえで、システムを運用しているはずですから、少し時間がたてば、こうしたシステム運用の経験があるシステム監査人材が、ローテーションによりシステム監査部門に配属されるようになるでしょう。

またそれを待たなくても、IT 統制の考え方自体は、クラウド型システムを選択するかどうかにかかわらず、不変なはずです。その意味では、クラウド化しても、システム監査の実施に支障はない、との見方もあるでしょう。

しかしながら繰り返しになりますが、クラウド型システムを提供するメガ IT 企業に対し、自社のシステム部門では得られない情報を踏み込んで得ることは極めて困難なので、どこからか先は、監査証跡の確保を断念せざるを得なくなるでしょう。課題が判明しても採用後の是正が困難なケースも十分想定されます。

またクラウド型システムの採用の目的の一つに、システム部門のスリム化を挙げる事例も多いようです。これまで自前システムを維持してきた人材が高齢化したり、必要とされる IT スキルが変化したりすることで、人材の構成が変化し、むしろデジタル変革の担い手確保の方に強い関心が向いてきているのは先述の通りです。こうした状況を反映し、（統計的には確認できませんが）システム監査部門の陣容も横ばいないしやや縮小に向かっている、とみておいた方がよさそうです。

こうした制約や変化は、システム（資源や運用）のアウトソーシング（システムの共同運用を含む）が盛んになった数十年前から伏在していた問題でした。クラウドファーストの考え方が主流になったことで、ある意味ではどんな企業、事業体においても、システム監査部門が共通に直面するようになったといえます。今後もデジタル変革への要請が強まる方向にあるとすれば、また特に足元では生成 AI の活用などが急務になっている状況では、IT 人材の恒常的な不足が解消することはとても望めない状況です。クラウド型システムの採用も当然の前提になり、システム部門のスリム化も避けられないでしょう。

こうした状況を反映し、システム監査の担い手は一段と確保が難しくなり、またデジタル変革の成果ばかり求める経営者の発想が変わらない限り、人材の重点配分も望めない予感がします。こうした隙を狙って、例えばランサムウエア攻撃の被害や、個人情報の漏えい事案の発生などの事例が増えています。こうした事例は潜在的には平素のシステム管理（IT マネジメント）の脆弱性に起因していますが、システム監査、情報セキュリティ監査が有効に機能し、必要な提言とそれに基づく IT 統制が有効に働いていれば、未然防止できる可能性は高まるはずです。

どの企業、事業体も、実際にセキュリティ侵害の事例や被害が身辺で発生し、自組織の問題に発展すると、ようやく我が事として、組織内の IT 統制システムを強化しますが、時間の経過とともに、IT 統制の仕組みを維持するためのシステム監査などの人材配分への関心を失い、先述のようにデジタル変革やクラウド型システム（生成 AI 等）を活用したサービスの導入など目先の成果ばかりに目が向きがちになるのです。

デジタル変革の推進やクラウド型システムの採用に当たっては、先に公表されたシステム監査・管理基準やガイドラインの内容を十分踏まえるなど、IT 統制やシステム監査の整備といわば両輪で推進することが、IT ガバナンスの観点からも強く望まれます。

<目次>

2023.10

【時事論評】RPA 導入裏マニュアル 3

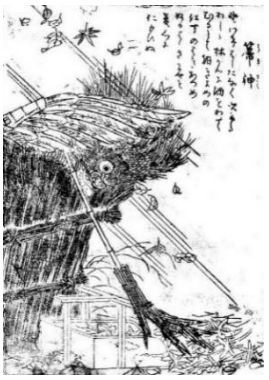
会員番号　0707 神尾博

1.DX 人材

本稿では、筆者が RPA（Robotic Process Automation）の企画・開発・運用、そして各種のリサーチを通じて得た「DX（Digital Transformation）人材」についての知見をいくつか紹介する。と言うと大上段な印象を受けられるかもしれないが、諸氏のビジネスシーン等で役立つヒントになりそうなものを、整理して綴ったものと理解いただきたい。

まずは、ご存じの読者も多いだろうが、DX と RPA の関係について改めて整理しておきたい。経済産業省や総務省の「DX」の定義を読み解くと、①IT 技術とデータを活用②社会や顧客に貢献する製品・サービスの提供③企業競争力の向上④スピード感を持った変革のための手段といった項目が挙げられる。したがってアプリ間データ連携等が主機能である RPA や、ChatGPT を始めとする生成 AI は、DX のサブセットである。

ところで、現代は PC やタブレット等の画面の中だけではなく、リアルワールドでもロボット共存前提社会になってきている。たとえば 1980 年代以降の製造業の FA（Factory Automation）のみならず、オフィスビルでの警備やファミレスの配膳にもロボットが普及し始めた。家庭でも一部では「ルンバブル」という言葉まで使われるようになり、購入者にとってロボット掃除機が動き回りやすいための段差の改善等は、当然の事前準備/事後対応となっている状況である。



RPA は自身の命令を忠実に、そして我慢強く実行してくれることから「デジタルレイバー」とも呼ばれる。それでは、同じレイバー（労働者）として、DX の一部である RPA を相棒として使いこなせる人材確保の要件という観点から話を進めていこう。

2. インソーシング

DX 人材確保のもっとも手っ取り早い手段は社内調達であると、躊躇なく主張される方も多いかもしれない。なるほど、2023 年のテレビのドキュメンタリー番組によると、某百貨店にてメタバースの 3D 制作の 4 名の前職はバイヤーや店頭のサービスマネージャであり、IT 技術者ではないと紹介されていた。しかしながらこのように DX 人材を、社内での処方で遍く見出すことができるケースが大半なのだろうか。

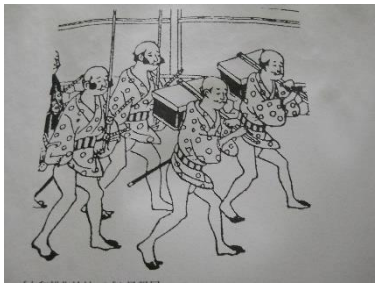
実はプログラミング能力は、正規分布ではなく約 40%がマスターでき、できない者が約 60%のフタコブラクダ分布になるという実験結果が、2006 年に英国の学者によって発表されており、この理論は現在でも概ね広く支持されている。RPA 開発はローコードとはいえ、プログラミングに必要なアルゴリズムの理解・構築は必須である。したがって業務にアサインする場合は、人員を適正かつ公正に選別しておかないと、経営資源の無駄使いはもとより、指名から漏れた人材からの不満が組織に充満し事業全体への悪影響も免れまい。

余談だが、最近は学習塾等で「成績が上がらなければ受講料無料」を謳う、成績保証制度なるものが存在するそうだが、フタコブラクダ理論を当てはめると社会人向けのプログラミング教育でこれをやるなら、相当なリスクヘッジが必要だろう。

3. アウトソーシング

外部からのリソースの調達といえば、委託、派遣、準委任。いずれにせよ、ベンダーロックインには要注意だ。派遣や準委任の場合は作業場所が社内になるケースも多いため、毎日顔を合わせているということで、管理面において油断が生じ、BP（Business Partner）ロックインになりそうな場面に遭遇したことがある。

また、外注業者や外注 SE を、実際に RPA 化対象の業務を行う担当者や、一緒に開発する社内 SE と相談せずに、勝手に決める管理職も困り者だ。その場合は、便宜を図る代わりに不正な利益を得ている可能性も疑ってよいだろう。最近では IT 業者でのとってつけたような社内教育のみという錬金術で「なんちゃって SE」をでっち上げるケースも多いという。徳川時代の渡り中間も品格や能力面の低い者が多かったというが、先に述べたフタコブラクダ理論を認識し、経歴書の学歴（理系の方がよい）や情報処理試験の合格状況をしっかりとチェックしたい。



他の選択肢としては海外オフショアがある。たとえばインド。年配の方には「山岳地帯に住む聖者の下で修行して、超人的な力を身に着ける」という、特撮番組の主題歌からのイメージを持つ方も多いかもしれない。ずいぶん前の話だが、近畿の製造業種の某工場の 2000 年問題対応に、当日本システム監査人協会でプロジェクトを組んだが、その際のメンバの方の「IT 技術者を求めインドに調査に赴いた」との近況報告には当時は感服したものだ。現在では日本を凌駕する IT 大国インドを、コスト減を主目的としたアウトソーシングの対象と考えるのは的外れであろう。

一方で戦時下にあるウクライナはオフショアの対象となるだろう。ウクライナは SETM を中心とした教育レベルが高く、NPO によって全ウクライナ人が無料でプログラミング技術を学べる仕組みも確保されている。生成 AI 等により、言語の壁は従来よりも大幅に下がったといえる。むしろ凡愚な日本人より、プログラム自体の可読性を担保できる人材であれば大歓迎だ。

4.セキュリティ&ガバナンス

RPA も一般的なソフトウェア開発の例に漏れず、単に粛々とプログラム作成を進めるメンバだけでは、プロジェクトとして破綻してしまうということを、筆者は痛感した。特に非機能要件である保守性とセキュリティについて事例紹介したい。まずは保守性の方だが、プログラムの可読性を確保するための規約や、サブルーチン化してライブラリとしての登録等である。そうした手順等を取りまとめて管理する仕組みと人材が必須になる。

セキュリティでは、ライセンス形態によっては、PC のマシン名+ユーザ名+キーに同じものを使うことで、ID のなりすましが可能になるケースもある。また RPA の自動実行では、実行者とサーバ管理者とログイン ID やパスワードを共有する必要があるが、こうした問題について運用管理での対応を立案・実施できる人材が存在しなければ、リスクは軽減されないのである。

5.マネジメント

さて「DX はトップの意気込み次第」の真偽であるが、IPA の「DX 白書 2023」によると、2022 年度の「IT 業務に見識がある役員の割合」の日米比較では、3 割未満と回答したのが、日本が 72.2%、米国が 39.1%である。また「DX の取組の成果」については、成果が出ていると回答したのが、日本が 58.0%、米

国が 89.0%だ。役員の IT リテラシー度合がすべて成否の要因ではないだろうが、白書ではこの差を DX 推進に影響を与える懸念があると指摘している。そもそもフタコブラクダ理論について、処方を用意できている企業役員等の幹部職はどのくらいの割合でいるだろうか？

実は筆者自身、経営者の IT リテラシーは必要条件かもしれないが、十分条件ではないことを実感した。まず、管理職にしても IT リテラシーの低さは致命傷だろう。RPA 開発初級者には、他人の書いたプログラムを読みながらの修正や派生開発から入っていくのがよいと提言しても、「簡単なものを一から組ませる」の一点張りだったというのはいかがなものか。学習機関のプログラミング講座でも、最初はコードを少し変えてみて動きを確認するのが常道であるにもかかわらずだ。社員においては、プログラミング能力以外でも質が悪いとどうしようもない。「魚を与えるのではなく釣り方を教えよ」を実行しようとしても、自らスキルを磨かず他人に頼っていればなんとかなると危機感のない社員も少なくなかった。

RPA に限らず、そもそも人事で必要なのはスクリーニングである。まともな人を重用すること以上に、おかしな人を昇進させないことが重要だ。「悪貨は良貨を駆逐する」方が、ダメージが大きいのは自明である。

6.オワコン？

2022 年から続く生成 AI の大ブレークの中で「生成 AI は RPA の代替となるか？」という疑問が未解決な読者も多いだろうが、それにお答えしよう。まず、生成 AI は対話型のツールであり、RPA はあらかじめ指定した通りに動作するロボットプログラムという違いがある。また、堅実な処理が決まっていてゆらぎが許されないものについては、RPA の得意とするところである。そして多少の誤謬を受容して作業効率を上げるには、生成 AI が持って来いだ。このように用途や要求品質が異なるため、たとえば、生成 AI に作成した RPA のプログラミングのチェックをさせたり、効率的なリファレンスに利用したりするといった補完的な関係になる。鉄砲伝来以降も、砲撃と白兵戦との併用は長きに渡って続いたのと同様である。

なお次の社内システム大改修では、RPA の主機能であるアプリ間の連携等が仕様に含まれることになるであろう。RPA を可読性の高い構造にしておけば、要件定義は「この RPA のビジネスロジックを組み込んでください」で事足りるので効率的だ。そうした新システムが増えれば、RPA 需要も徐々に減少していくだろう。

最後に「RPA スキルはポータブルスキルかどうか?」について述べておきたい。RPA 開発におけるアルゴリズム作成の考え方は、プログラム言語が別でもほぼ不変であり、特にビジネスロジックについてはそうだ。これは生成 AI において、プロンプトエンジニアに必要とされる正しい言葉・文章の能力が、ビジネスシーンで有益なのと同様である。諸氏は安心してリスキリングに励んでいただきたい。

（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。画像は Wiki により著作権保護期間満了後のものを引用しています。）

<目次>

2023.10

【コラム】システム監査のための数学・教育課程・法律・会計再入門（11）

会員番号　1644 田淵隆明　（近畿支部　システム監査法制化推進プロジェクト）

§1. インボイス制度、遂に施行される

[1]付加価値税(VAT)の世界標準

10 月 1 日、「インボイス制度」が施行されたが、大きな混乱は発生しなかった。我が国の「消費税」をはじめとする「付加価値税」(英：VAT=Value Added Tax, 仏：Taxe sur la valeur ajoutée,独：Mehrwertsteuer, 中：增值税)の世界標準は次のとおりである(→文献[1-3])。

① インボイス方式　→我が国では 2023/10/01 に施行。

② 複数税率　→標準税率＝3%(自動車のみ 6%)の複数税率で導入されたが、1987 年に 5%均一となった。2019/10/01 に本格的な複数税率に移行。

③ 税込み経理の禁止　→税法では禁止されていないが、2021 年 4 月 1 日強制適用の企業会計基準第 29 号「収益認識に係る会計基準」では禁止。なお、IFRS15 でも禁止。

幻の「売上税」では①と③は満たされていた。論語には「民信なくば立たず」(民衆の信用がなければ、政治はうまく行かない)という名言があるが、1988 年 5 月の「売上税」廃案の経緯を思い出す。結果として、①のインボイス方式への移行には、実に 34 年 6 か月を要している。これで、消費税を 3 段階以上に細分化することも容易となり、2013 年 12 月の与党税調で検討が合意された「担税力に応じた新税」(高額飲食税やグリーン車・グランクラス等の通行税の復活 etc.)も可能になると思われる。

[2]軽減税率の歴史

付加価値税の歴史は、なんと 5～6 世紀の東ローマ帝国に遡る。ただし、当時は「前段階の控除」はなく、「取引高税」(例えば、1 ノミスマに対して 1/8 の 9 ケラティオン(※宝石のカラットの語源))であった。

当時から、税率は均一ではなかったようである。現在でも多くの国々で、軽減税率は食料品に設定されているが、**それはエンゲルの法則に由来している。**すなわち家庭の全支出に対する食料品の支出の割合は「エンゲル係数」と呼ばれており、これは小中学校の家庭科で学習する。**エンゲル係数は貧困家庭ほど高い**ことが統計的に得られており、**食料品に軽減税率を適用することは逆進性の緩和の観点で極めて合理的な制度**である。

[3]インボイス制度施行後の消費税の会計処理・税務処理**【システム監査専門家の出番】**

インボイス制度に反対する人々の論拠として「免税事業者が消費税分を貰えなくなる」という批判がある。しかし、冷静に考えれば分かることであるが、**免税事業者は本来消費税を課してはならない**のである。

★「内税(総額)表示/外税表示/総合表示」の税額表示方式と「税込経理/税抜経理」の経理方式の違いについては区別が必要である。例えば、JR 各社などは「内税表示」で「税抜経理」である。

●内税(総額)表示・・・本体価格＋消費税額の合計額を表示する方法

●外税表示・・・・・本体価格＋税などの表示方法(BtoC では原則禁止)

●総合表示・・・・・本体価格と消費税額と合計額を別個に表示する方法

〇税込経理・・・・・「仮受消費税(流動負債)」、「仮払消費税(流動資産)」の科目を用いず、前者は売上高、後者は仕入高に含める経理方式。ただし、企業会計基準第 29 号及び IFRS15 では認められない。納税時に「租税公課/未払消費税」の仕訳を起こす。

〇税抜経理・・・・・「仮受消費税」、「仮払消費税」の科目を用い、消費税部分を分離する経理方式。

〔設例 1.1〕単価 30,000 円の商品甲を一個販売した場合の、次の場合の仕訳を示せ。消費税率は 10%とし、会計処理は、企業会計基準第 29 号及び IFRS15 に準拠するものとする。

(1) 課税事業者 A が「30,000 円＋税別」で販売した場合
(2) 課税事業者 A が「33,000 円(税込)」で販売した場合
(3) 課税事業者 A が「本体 30,000 円、消費税 3,000 円」で販売した場合
(4) 免税事業者 A が「30,000 円＋税別」で販売した場合
(5) 免税事業者 A が「33,000 円(税込)」で販売した場合
(6) 免税事業者 B が「本体 30,000 円、消費税 3,000 円」で販売した場合
(7) 課税事業者 C(インボイス手続き未了)が「30,000 円＋税別」で販売した場合
(8) 課税事業者 C(インボイス手続き未了)が「33,000 円(税込)」で販売した場合
(9) 課税事業者 C(インボイス手続き未了)が「本体 30,000 円、消費税 3,000 円」で販売した場合

〔解答〕

(1)　売掛金　33,000　/　売上　30,000
　　/　仮受消費税　3,000

(2) 企業会計基準第 29 号及び IFRS では、「税込経理」は認められないので、(1)と同じ仕訳。

(3)　(1)と同じ。

(4)　免税事業者は「仮受消費税(流動負債)」、「仮払消費税(流動資産)」を計上できないので、

　売掛金　33,000　/　売上　33,000

(5)　(4)と同じ。

(6)　免税事業者は「仮受消費税(流動負債)」、「仮払消費税(流動資産)」を計上できないので(4)と同じ。

(7)～(9)インボイス手続き未了の場合であっても、C 社は課税事業者であるので、(1)と同じ。

※1.(4)(6)は消費税法の趣旨に反する表示方式であり、望ましくない。**会計上の正確な販売単価は 33,000** である。法人税法上も**益金＝30,000 ではなく、益金＝33,000 で計算**される。**【要注意】**

〔設例 1.2〕設例 1.1 の各場合において、仕入側の会計処理はどうなるか？

〔解答〕(1)～(3)：

・三分割法の場合：　仕入　30,000　/　買掛金　33,000
　仮払消費税　3,000　/

・売上原価対立法の場合：　商品　30,000　/　買掛金　33,000
　仮払消費税　3,000　/

(4)～(6)：免税事業者からの仕入については、本来、仮払消費税は存在しないので次のようになる。

・三分割法の場合：　仕入　33,000　/　買掛金　33,000

・売上原価対立法の場合：　商品　33,000　/　買掛金　33,000

(7)～(9)：インボイスの届け出の有無は、会計上は無関係であるので、(1)～(3)と同じ。

〔設例 1.3〕設例 1.2 の各場合において、仕入側の「仕入税額控除額」はどうなるか？ただし、課税売上割合は 100%とする。

(1)～(3)：(控除対象外消費税額)＝0 であり、(仕入税額控除額) ＝3,000

(4)～(9)：本則では(仕入税額控除額) ＝0

経過措置として、

2023/10/01～2026/09/30 の場合は、(控除額)＝33,000×10/110×0.8＝2,400

2026/10/01～2029/09/30 の場合は、(控除額)＝33,000×10/110×0.5＝1,500

§2.公共インフラにおけるバックアップの重要性

先月号で、公共インフラのバックアップの重要性について取り上げたところ、読者の方々からメールや電話等でご意見を頂いた。今回はその続編である。ご意見は naboo_wisdom@gakushikai.jp までお願いします。

[1]北海道新幹線

先日、札幌市は 2030 年の冬季オリンピック誘致の断念を発表した。極めて残念なことである。北海道新幹線の延伸にも影響が出ると懸念されている。そうした中、4 月に新市長が誕生した函館市は、函館本線の一部 3 線軌条化(青函トンネル付近及び箱根登山鉄道などで実績あり)による函館駅乗り入れに関する調査を 9 月から開始した。年度内に答申が出る予定である(→文献[4-6])。

ただし、盛岡より北のホーム有効長は 12 両、八戸より北は 10 両という制約がある上、JR 東日本の E5 系の後継車両は(360km/h の営業運転に備えて)先頭車のノーズ部分が先頭車の半分程度を占める車両のデザインであり、**座席定員の大幅減**が予想される。そのため、先頭車が 4 両組み込まれる「ミニ新幹線併結方式」は困難であると考えられる。また、道内の移動需要は本州連絡よりも多いことを考えると、早朝・深夜を除けば①②を新函館北斗で対面乗り換えとするのが現実的であると考えられる。

・東京～新函館北斗～札幌直通の速達型「はやぶさ」(新函館北斗～札幌無停車)

・札幌～新函館北斗～函館の途中駅停車型(新八雲・長万部・倶知安・新小樽停車)

※懸案の長万部～函館間の貨物輸送については国・北海道・JR 北海道などが維持することで合意が成立した。今後は費用の負担割合が課題となる(→文献[7])。なお、藤城・砂原両支線の維持も貨物の為には必須である。

[2]第二青函トンネルによるバックアップ機能

先月号で、第二青函トンネルは、下北半島の大湊市～函館市が適切であると記載したが、現状では津軽海峡ルートで現在の青函トンネルに平行して建設する構想のほうが有力なようである。お詫びして訂正します。ただ、大規模な断層が多数存在することから、海底トンネルを近接して設置した場合に大規模地震で同時に被災する可能性が高いことを考えると、やはり、下北半島～函館ルートのほうが妥当であると考えられる。水深は 200m 程度であり、現在の技術ならば可能と考えられる。勿論、鉄道も複線にするのは当然である。将来的には、新函館北斗で分岐して内浦湾の海底を通り、室蘭に直結することが望ましい。

[3]関西本線による名阪間のバックアップ機能

現在、関西本線の亀山(三重県亀山市)～柘植(三重県伊賀市、草津線連絡)～伊賀上野(三重県伊賀市、伊賀鉄道連絡)～加茂(京都府木津川市)61km の存廃が危ぶまれている。これについては**JR 東日本・JR 九州が導入した電車/気動車の蓄電池型ハイブリッド車両の導入が最良の解決策**であると考えられる。JR 九州の車両はバッテリーでの走行可能距離は約 90km とのことであるので、両端駅に充電設備を設ければ十分に実現可能と考えられる。先

月号では 3 案を提言したが、②が最もハードルが低そうである(→文献[8,9])。
① 草津線(草津～柘植間)は電車として、関西本線(柘植～亀山)の 20km はバッテリーで走行。
② 関西本線(亀山～柘植～伊賀上野)の 34.6km はバッテリーで走行、伊賀鉄道(伊賀上野～上野市～伊賀神戸、出資比率近鉄 98%、伊賀市 2%の近鉄傘下の第三セクター)は電車として走行。
⇒三重県内で完結するので、三重県・伊賀市・亀山市は補助金を出しやすいと考えられる。
③JR 片町線の松井山手～木津と関西本線(木津～加茂)は電車として、関西本線(加茂～柘植)の 41km はバッテリーで走行。⇒松井山手～木津～月ヶ瀬ならば京都府内で完結するので京都府からの補助金は出やすい。

★リニア中央新幹線の三重県内の停車駅は亀山市に建設することが内定しており、亀山駅のほか、関西本線の井田川駅、紀勢本線の下庄駅、亀山 IC 付近(関西本線亀山駅～関駅間に新駅設置)の 3 か所が有力視されており、亀山～柘植～伊賀上野間が再活性化することは十分に考えられる。蓄電池型ハイブリッド車両併結による都心から非電化区間への直通化としては、山陰本線(大阪・京都から城崎→鳥取または岡山から伯耆大山→鳥取)、会津鉄道(東武鉄道浅草/JR 新宿－鬼怒川温泉から会津田島→会津若松)なども検討に値すると思われる。

§3.新制度における大学入試の出題科目

秋になり、2025 年度入学試験の要綱も出そろってきた。文系の数学については数学 C は「ベクトル」(2 次元・3 次元)のみの大学が多く、複素数平面は除外されるケースが多かった。しかし、共通テストの数学ⅡBC においては、数学Ⅱの「数列」・「統計的な推測(確率分布、二項分布、正規分布、推定・検定)」、数学 C の「ベクトル」、「複素数平面」から 3 分野選択となるため、事実上文系も「複素数平面」は必須と考えられる。なぜなら、統計的な推測は確率密度関数や $\exp(-x^2/2)$の積分が登場するなど、数学Ⅲの知識が一部必要であり、文系にはリスクが高いと考えられるためである(→文献[2,3])。なお、共通テストの範囲外ではあるが、現行の数学 B には移動平均・最小二乗法による回帰分析、数学 C には行列が含まれている。

以前から指摘しているように、ベクトルは高 2 に、指数・対数・三角関数(の $0°\leqq\theta\leqq180°$以外の部分)は高 1 に降ろすべきである。従って、数学 1・A の半分は中学に降ろす必要があるため、結果的に中 1 の半分程度を中学から小学校に降ろす必要がある。その為には、小学校の教科担任制の拡充が必要であり、算数と理科についても積極的に導入するべきである。また、各地で消化不良が多発している「物理基礎」の高 1 配当はしないように文部科学省は指導を行うべきである。
★一橋大学が後期試験で数学Ⅲを導入した。大変喜ばしい。全大学に数学の入試を義務化し、理系は理科二科目を義務化するべきである。また、大学入試外国語を二ヶ国語とし、卒業要件を三ヶ国語とすべきである。

※以上述べたことは筆者の私見であり、いかなる団体をも代表するものではありません。また、法令の適用・会計基準の適用、及び、医学的所見については、必ず、御自身で顧問会計士、弁護士、司法書士、行政書士、医師・薬剤師、その他の専門家の方々への御確認・照会をお願いします。

<参考文献>
[1]「軽減税率」田淵隆明が語る、IFRS&連結会計 Ver7〔Ⅰ〕〔Ⅱ〕(2022/04/18)
[2]「軽減税率」田淵隆明が語る、数学・理科カリキュラム再考(2023/06/12)
[3]「軽減税率」田淵隆明が語る、数学・理科カリキュラム再考〔Ⅱ〕(2023/10/30 予定)
[4] 【速報】新幹線の乗り入れはフル規格の可能性！並行在来線は存続へ！函館市が北海道庁へ牽制か？ https://www.youtube.com/watch?v=GMDhrFiUIz8
[5] 【ゆっくり】函館～新函館北斗直通ミニ新幹線構想まじめに検討すれば説 https://www.youtube.com/watch?v=QVIUP9fbW1E
[6]【前面展望】ありがとうノースレインボー 下り特急ニセコ 函館～札幌 https://www.youtube.com/watch?v=O2KhbR15G9E
[7] 函館～長万部間、貨物列車の存続で合意 - 今後は費用負担が焦点に https://news.mynavi.jp/article/20230802-hakodatehonsen/
[8]【4K 前面展望】関西線（加茂～亀山）https://www.youtube.com/watch?v=BIYJjTWkdQc
[9]【4K 前面展望】伊賀鉄道　伊賀神戸→上野市→伊賀上野 https://www.youtube.com/watch?v=Zf0AjwK6vw0

<目次>

2023.10

第 280 回特別月例研究会　講演録

テーマ：「システム監査・管理ガイドラン活用のポイント」

～システム監査・管理基準の改定とガイドラインの公表～

会員番号　1200 豊田諭、2552 柳田正

【講師】経済産業省 サイバーセキュリティ課 課長補佐 三田真史（みた まさし）氏

システム監査学会 石島隆（いしじま たかし）氏

システム監査学会 鈴木夏彦（すずき なつひこ）氏

日本システム監査人協会 基準改訂委員会 松枝憲司（まつえだ けんじ）氏

日本システム監査人協会 カ利則（ちから としのり）氏

【日時・場所】セミナー開催日：2023 年 9 月 23 日（土曜）13：30-17：00 (Zoom ウェビナー)

【講演骨子】

2023 年 4 月に改訂された経済産業省のシステム監査・管理基準をいろいろな立場の人に、実践的に利用してもらうことを目的に「システム監査・管理基準ガイドライン」が策定されました。

本ガイドラインは「システム監査基準ガイドライン」「システム管理基準ガイドライン IT ガバナンス編」「同 IT マネジメント編」で構成され、基準を包含しているため、ガイドライン単独で利用が可能です。

その特徴や具体的な活用方法等について、策定に携わった関係団体のメンバーが解説します。

【講演録】

1．システム監査基準・システム管理基準の改訂について

経済産業省　三田真史氏

IT と経営戦略を連携させ、企業価値の創出を実現するための IT ガバナンスの実践が重要になってきていることに加え、情報活用とそれに伴うリスクへの対応も必要となってきている。このようなシステム監査を巡る状況の変化等を踏まえ、システム監査基準・管理基準の改訂・見直しを実施した。改訂・見直しに当たっては、原則等の普遍的な部分について監査基準・管理基準を改定し、実施方法等の実践部分については切り離してガイドラインとして別冊化して、システム監査に知見のある民間団体においてアップデート等を図っていくこととしている。

システム監査基準については、システム監査人の倫理が監査の前提であることをより明確にするために、倫理規定部分を基準から切り離した構成に整理し、監査の責任等組織としての対応のあり方等を追記し、ガバナンス、マネジメント、コントロール及びこれらの統合的な視点を追記した。

システム管理基準については、アジャイル開発や AI 活用等の新たな手法・技術等にも対応できるよう、国際規格の考え方なども踏まえ、各プロセスを細分化して再整理するなどの改訂を実施した。

企業価値の創出を実現するための IT ガバナンスの実践に向けて、システム監査基準、管理基準及びガイドラインを活用するようお願いする。

2. 改訂システム監査・管理基準とガイドラインについて

システム監査学会 石島隆氏

IT（Information Technology）のみでなく、OT（Operational Technology）の大幅な進展等の環境変化にも幅広く対応できる基準を目指して、監査基準・管理基準ともに国際基準の考え方を取り入れた。また、IT ガバナンス及び IT マネジメントにおける基本となるプロセスを管理基準の対象とし、アジャイル開発、AI システム、IoT などにも応用できるフレームワークとすることを改訂の方針とした。

システム監査基準は、システム監査が効果的かつ効率的に行われるよう、システム監査のあるべき体制や実施方法等を示しているが、IT 環境の継続的な変化とシステム監査に対するニーズの多様化、及び監査人の倫理の重要性が高まっていることを踏まえて改訂した。

システム管理基準は、IT システムの利活用の進展状況に対応しやすい内容となることを企図し、IT ガバナンス編と IT マネジメント編で構成した。このうち、IT マネジメント編においては、システムライフサイクルにおける基本となる活動に基づいて細分化したプロセス毎に記載しているため、その組み合わせによって様々なプロセスモデルや情報システムの導入形態に応用可能である。

システム監査基準には、監査にとって普遍的な内容を記述し、システム監査基準ガイドラインには、実施方法等のシステム監査を取り巻く環境の変化への対応が期待される、より具体的な内容を例示している。

システム管理基準はチェックリストではなく、監査対象のあるべき姿を示し、監査における判断尺度となるものである。システム管理基準で示した内容の取捨選択、関連する他の基準やガイドライン等からの必要項目の追加、タイムリーに改訂ができるように民間団体が管理するシステム管理基準ガイドラインの項目からの選択等を行い、組織体の状況に適合したシステム監査のための基準を整備することが望ましい。今後、システム監査の実践に資するテーマ別ガイドラインを関係団体で整備していく予定である。

3. システム監査ガイドラインの概要と活用のポイント

日本システム監査人協会 カ利則氏

システム監査は、システムの信頼性等を確保し、企業に対する信頼性を高める重要な取組である。システム監査が効果的かつ効率的に行われるためには、システム監査のあるべき体制や実施方法等が示される必要がある。システム監査基準とガイドラインは、このニーズに応えるために制定されている。

システム監査基準は監査にとって普遍的な内容を記述し、システム監査ガイドラインはより具体的な内容を記述しており、そのため環境の変化に迅速に対応できるように民間団体が整備する体制に変更になった。

システム監査では監査人の倫理が重要であり、誠実性、客観性、監査人としての能力及び正当な注意、秘密の保持を、倫理に関して監査人が守るべき 4 つの原則としている。

システム監査ガイドラインは 64 ページあるが、是非、システム監査に携わるメンバーで読み合わせをすることをお勧めする。

システム監査ガイドラインはより具体的に書かれていて、民間団体で迅速に対応できるので、意見をお願いする。

4．システム管理基準ガイドライン（IT ガバナンス編）の概要と活用のポイント

日本システム監査人協会 基準改訂委員会 松枝憲司氏

システム管理基準（IT ガバナンス編）の主な改訂項目と内容は以下のとおりである。

①「情報システムのガバナンス」から「IT システムの利活用のガバナンス」へ

② 取締役等（ガバナンス機関）と経営者（経営の執行責任者）の役割を識別

③ EDM に加えて「ステークホルダーへの対応」を追加

④「IT ガバナンスの実践」と「IT ガバナンス実践に必要な要件」で構成

⑤ IT マネジメントとの連携の明確化（IT マネジメント編の各プロセス）

システム管理基準（IT ガバナンス編）の国際基準等との関係は以下のとおりである。

① ISO/IEC38500（IT ガバナンス）等の改訂の状況を反映

② IT ガバナンスを組織のガバナンス（ISO37000）の一部として位置づけ等

IT ガバナンスは、システム管理基準ガイドライン前文で「組織体のガバナンスの構成要素で、取締役会等がステークホルダーのニーズに基づき、組織体の価値及び組織体への信頼を向上させるための IT システムの利活用に係る機能であり、組織体における IT システムの利活用のあるべき姿を示す IT 戦略と方針の策定及びその実現のための活動である」と定義している。

システム管理基準では、「組織体の取締役会等は、ステークホルダーのニーズに基づき IT ガバナンスを実践する実行責任と、ステークホルダーに対する IT ガバナンス全体の説明責任を負う」としている。

組織としての IT ガバナンスの達成目標は、Ⅰ．効果的な IT パフォーマンスの実現、Ⅱ．責任ある IT 資源管理の実施、Ⅲ．組織体における倫理的行動の確保、等が設定されるとしている。

IT ガバナンスに関する監査やアセスメントのスコープとしては、IT ガバナンスの活動と IT ガバナンス活動の目標達成及び IT ガバナンスの成果が考えられる。また監査とアセスメントの実施者としては、内部監査部門、監査役、外部監査人、経営者・取締役等が想定されるが、監査の場合は、スコープと組織体の実態に応じた適切な監査人を選定する必要がある。

5．システム管理基準ガイドライン（IT マネジメント編）の概要と活用のポイント

システム監査学会 鈴木夏彦氏

システム管理基準（IT マネジメント編）では、経営方針及び IT ガバナンス方針に基づいて策定した IT 戦略の目標を達成するために、IT システムの利活用に係るコントロールを実行するための達成目標と管理活動の例を記載している。IT マネジメントの体制については、経営者が IT システムの利活用について責任を負う領域が IT マネジメントであり、経営者は、IT 戦略に基づいて目標を達成する実行責任と取締役会等への説明責任を負うとしている。

改訂にあたっては、IT ガバナンスと IT マネジメントのつなぎ、JISX0170 システムライフサイクルプロセスを参考にした拡張性、多様なシステムライフサイクルモデルへの応用等を考慮した。

システム管理基準ガイドライン（IT マネジメント編）は、「システム管理基準」を利用するに当たって、より具体的な IT ガバナンス及び IT マネジメントに関する着眼点等を例示することにより、システム監査を実践する際の参考とすることを目的に策定した。

システム監査におけるシステム管理基準ガイドラインの活用について、以下の 5 つの実践事例と活用による期待効果が紹介された。

・保証を目的としたシステム監査：監査項目の選定、監査手続の作成、監査報告書の作成

・助言を目的としたシステム監査：組織体の IT システム管理方針の整備・改善、IT 部門等のコントロールの記述

ガイドラインを有効活用することで、組織体の IT マネジメント強化及び改善を促進し、組織体の価値向上につながることが期待できる。

6. システム監査・管理ガイドラインの運営について

日本システム監査人協会 松枝憲司氏

本ガイドラインは、関係団体（代表団体、連携団体、協力団体、オブザーバ）により構成される運営委員会が作成・更新し、代表団体の HP で公表する。

代表団体：日本システム監査人協会

連携団体：システム監査学会

協力団体：日本内部監査協会、日本公認会計士協会

オブザーバ：経済産業省

経済産業省の方針、関連する各種ガイドライン等の動向、各団体の研究会等での研究成果等をベースに定期的に見直すことを想定している

システム監査のテーマ別ガイドラインの優先テーマ候補として、システム監査におけるリスクアプローチ手法、アジャイル開発・DevOps の監査、が挙げられている。

質疑応答

以下の項目等についての質問があり、それぞれに丁寧な回答をいただいた。

Q：システム監査の対象として、クラウドサービスの利用時に、監査項目など、どのような点に注意が必要でしょうか？

Q：システム監査ガイドラインは、情報セキュリティ監査基準と併用することが標準と考えてよろしいでしょうか？

Q：「 ガイドラインの著作権は日本システム監査人協会に帰属するが「利用規約」に従い原則として自由に利用可能」とのことですが、ガイドラインを活用した出版やウェブサイトでの扱い（紹介を超える解説等）などについては、事前の許諾など制約はあるのでしょうか？

Q：情報セキュリティ監査基準、管理基準は改定の計画はありますか？

Q：テーマ別ガイドラインに関して、ロボット活用や OT 関連を含めて拡張する予定はありますか？

Q：今般のシステム監査基準、システム管理基準策定の中で主要な論点はどういったもので、その中で今回の両基準に反映せず将来の課題などとなった点はどのようなものがあり、その対応予定などありますでしょうか？

Q：「ガバナンスに責任ある者」は監査役等とするのが一般であるが、システム監査基準ではそれを取締役会としているが、その理由は何か？

所感

システム監査基準・管理基準、同ガイドラインについて、改訂に直接携わった方からその趣旨などを詳細に説明いただけたことは貴重な機会でした。タイトルにもあるように、これをどう活用させていくか、全ての使う人が走りながら考えていくことが重要と改めて実感しました。

<目次>

2023.10

支部報告【北信越支部 2023 年度長野県例会/9 月リモート例会報告】

会員番号　1281 宮本 茂明（北信越支部）

以下のとおり北信越支部 2023 年度長野県例会/9 月リモート例会を開催しました。

・日時：2023 年 9 月 9 日（土）　　現地参加者：9 名、リモート参加者：2 名

・会場：現地会場（松本商工会議所）とリモート（zoom）のハイブリッド開催

・議題：　研究報告/情報提供

「ゼロトラストにおける動的ポリシー」　栃川　昌文　氏

「SASE とは？」　宮本　茂明

「重大システムインシデント事例の紹介・スタディ」　宮島　正彦　氏

「コンピュータ犯罪について」　荒牧　裕一　氏

◇研究報告

「ゼロトラストにおける動的ポリシー」

会員番号 1354　栃川　昌文

2022 年 3 月の例会で宮本さんから「ゼロトラスト」の報告があり、その後も EDR に関する情報提供などがありました。そして、2023 年度は「ゼロトラスト」を例会のメインテーマにすることが決まりました。2023 年 6 月の例会では、梶川さんから「ゼロトラスト」について NIST の考え方を中心に話がありました。

こうした経緯から、「ゼロトラスト」の背景や考え方・概念は何となく分かったつもりですが、具体的にどう実現するのかを考えると、いろんな疑問が出てきましたので、自分なりにいろいろ調べて、今回の報告を行いました。

「ゼロトラスト」を実現するための重要な事項が「動的ポリシー」です。サービス利用者やサービス提供元の状態を常に把握して、認証を動的に行う（ついさっきまで使えていたのに、環境を変えたことで使えなくなる）ことです。これを実現するためには、Identity(アイデンティティ)が重要となります。アカウント名、パスワードだけでなく、多要素認証、クライアントの IP アドレス、OS の種類など確かに本人だと判断できるに足る情報をかき集めて認証することになります。一方、動的に認証を行うためには、監視が重要なファクターであり、監視をするには Identity がなければいけません。つまり、認証と監視を Identity で結び付けて実現することになります。

こうしたことから、IdaaS や EDR などの製品が最近脚光を浴びています。しかし、これらの製品が連携して使えなければ「動的ポリシー」の実現はできません。いろいろと調べてみると、製品間の連携は一部の製品ではできているようですが、標準化も含めていろんな製品が相互につながるという状況にはなっていないようです。また、製品間の連携を実現するためには高度なスキルが必要であり、この分野の人材も十分ではないようです。

更に、監視ログの解析などの自動化も進んでいますが、最終判断は人間がしなければならないこともあり、SOC の役割がこれまで以上に重要になっています。 1 社で SOC を持つのは大変なので、業界で共有の SOC を持つ動きも出始めています。

このように「ゼロトラスト」の概念は先行していますが、実装に向けては乗り超えなければならないハードルがたくさんあることが分かりました。こうしたこともあり、最近では「SASE」という考え方も出てきました。

いずれにしろ、ダイナミックに認証条件を変化させるというシステムは、これまでの考え方とは大きく異なり、ある意味パラダイムシフトだと思います。システム監査においても、こうした新しい考え方に沿った監査手法を考えなければならないときが来ているように思います。

「SASE とは？」

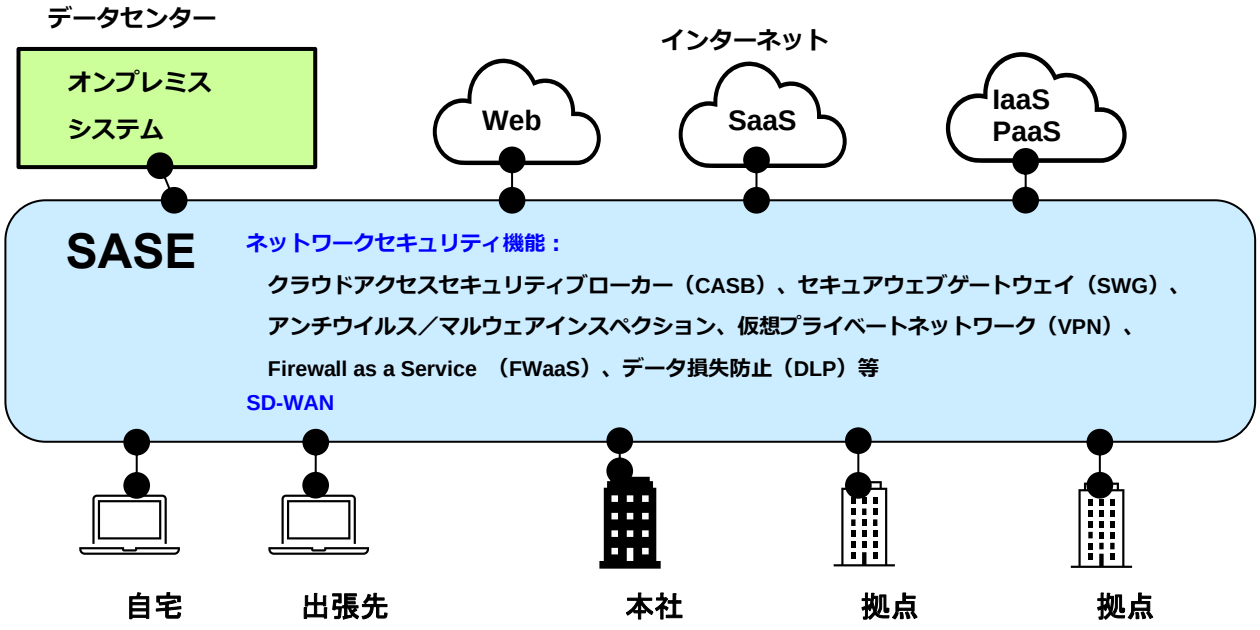
会員番号 1281 宮本 茂明

（SASE の概要）

最近、ゼロトラストに関連する情報セキュリティソリューションの紹介等で、「SASE」（サシー）という用語を目にする機会が増えてきています。Wikipedia 英語サイトの「SASE」掲載内容から、その概要を調べてみました。（https://en.wikipedia.org/wiki/Secure_access_service_edge）

「SASE」(Secure Access Service Edge：セキュア・アクセス・サービス・エッジ)」という用語は、2019 年にガートナー社によって作られたものです。

「SASE」は、単一のクラウドコンピューティングサービスとして、データセンターではなく、接続元（ユーザー、デバイス、IoT デバイス、エッジコンピューティングの場所）に直接、SD-WAN（Software-Defined Wide Area Network）とセキュリティ制御の機能を、ネットワークエッジで提供するものです。



SD-WAN は、WAN 全体のトラフィックを制御するネットワーク・ハードウェアまたはソフトウェアの集中制御により、広域ネットワーキングを簡素化し、低遅延を実現する技術です。プライベート WAN 接続をインターネットブロードバンド、LTE、5G 接続等と組み合わせることができます。

「SASE」のセキュリティ制御の機能として、クラウドアクセスセキュリティブローカー（CASB）、セキュアウェブゲートウェイ（SWG）、アンチウイルス／マルウェアインスペクション、仮想プライベートネットワーク（VPN）、Firewall as a Service（FWaaS）、データ損失防止（DLP）等の機能があります。

（SASE の特徴）

- 複雑性の軽減：「SASE」は、クラウド・コンピューティング・モデルを採用し、SD-WAN とセキュリティ機能のすべてを単一のベンダーに任せることで、複雑さを軽減しています。
- ユニバーサル・アクセス：「SASE」アーキテクチャは、主にデータセンターをベースとしたアクセスとは対照的に、あらゆる場所のあらゆるエンティティからあらゆるリソースへの一貫した高速で安全なアクセスを提供するように設計されています。
- パフォーマンス：遅延の影響を受けやすいビデオ、VoIP、コラボレーション・アプリケーションに特に有効な、遅延を最適化したルーティングにより、アプリケーションやサービスのパフォーマンスが向上します。
- 一貫したセキュリティ：すべての SD-WAN 接続とセキュリティ機能に対して、単一のクラウド・サービスを介して一貫したセキュリティを提供します。セキュリティは同じポリシーのセットに基づいており、アプリケーション、ユーザー、デバイスの場所や宛先（クラウド、データセンター・アプリケーション）に関係なく、どのようなアクセス・セッションに対しても同じクラウド・サービスによって同じセキュリティ機能が提供されます。

（SASE の標準化）

「SASE」ソリューションの標準化は、米国 MEF で SASE サービス定義（MEF W117）委員会が設立され、検討が進められている段階です。

（SASE ソリューションに関する意見交換）

例会参加のみなさんから、SASE ソリューションに関し以下のような意見が出されました。

- ゼロトラスト環境構築時、各セキュリティ製品を整合をとりながら導入するのは、専門の技術者でないと難しく、整合がとれているか検証するのも容易ではない状況にある。SASE ソリューションは単一のクラウドコンピューティングサービスとして提供されるので、セキュリティ製品間の整合に関する懸念が解消されるのではないか。
- SASE ソリューションは単一のクラウドコンピューティングサービスのため、ベンダロックインの懸念がある。
- SASE ソリューションのクラウドコンピューティングサービスを、利用者側からシステム監査することは難しいので、SASE ソリューションの第 3 者システム監査報告書の提供を求めることになるのではないか。
- ゼロトラスト環境を整備したり、SASE ソリューションを導入したりする事業者と、従来環境で運用する事業者とで、情報利用環境の使い勝手やセキュリティ面で大きな格差が生まれてくるのではないか。

今後も SASE ソリューションに関連する情報を継続的にフォローしていきたいと考えています。

「重大システムインシデント事例の紹介・スタディ」

会員番号 2746　宮島　正彦

実際に発生したシステムインシデント２ケース「ホームページサービス停止事案」及び「ホームページのバス運行情報等更新不能事案」を題材に、実際に作成された三段表（「事故の概要と経緯」「問題点と発生原因、

リスクと課題」「再発防止策、課題解決策」）により、システム監査のあり方や再発防止策の有効性・実効性等について議論を行った。

議論を通じて得られた知見や意見は、実際に行われたシステム監査に活かすことができた。

「コンピュータ犯罪について」

会員番号 0655　荒牧　裕一

コンピュータ犯罪に関して、1987 年の電磁的記録不正作出等の制定から 2023 年の盗撮処罰法までの変遷を整理して発表した。

刑事罰に関する法解釈は罪刑法定主義が厳格に適用されるため、IT 技術等の進歩によって生まれた新しい犯罪にすぐには対応できず、実際の事件が起きてから後追いで法律が整備されることが多い。その代表例として、コンピュータ犯罪の先駆けともいえる 1981 年の伊藤素子事件を始め、ホワイトテレホンカード偽造事件、CA 盗撮事件等を挙げ、なぜ当時の法律では処罰できなかったのかについて解説しながら紹介した。

◇長野県例会後記

当支部は、北信越地区の各県持ち回りで総会・例会を開催しており、会議後には懇親会も開催しています。コロナ禍をきっかけとして、リモート参加も可能になりましたが、現地参加の楽しみは各地での懇親会です。今回の懇親会では馬刺しや桜鍋などを味わいながら、例会では語り尽くせなかった話で盛り上がりました。

懇親会では、システム監査の次の担い手（中堅・若手）に、どうベテランの知見を伝えればよいか、議論になりました。以前に比べ担当が細分化し、修羅場もなかなか体験できません。まずは例会（オンラインも含め）参加者を着実に増やして、魅力を伝えることから始めては、といった意見が出ました。

またクラウド化などが進む中で、システム監査の主体的実施には制約が大きく、監査の立ち位置を改めて確認する必要があるのでは、との意見も出ました。次回以降の定例会の中で議論できると良いと思います。

（懇親会こぼれ話）

長野県例会の松本開催は９年ぶりでしたが、多くの会員が参加して、活発かつ楽しい懇親会となりました。会場の馬肉料理専門店「新三よし」は元々明治 32 年創業の料亭で、歴史を感じさせる風情のあるお店です。

―新三よし 桜鍋

なお、中世の延喜式には、御牧（天皇直轄の牧場）が甲斐、武蔵、信濃および上野国に 32 カ所開設され、そのうち半数の 16 カ所が信濃国との記録があります。松本市内の肉屋では昭和 40 年代までは桜肉（馬肉）が普通に売られ、桜鍋専門料理店もありました。

松本市図書館で調べもの相談したところ、馬肉食文化は、現在では隣接する伊那市や飯田市などのもので、松本在住者には必ずしも根付いておらず、むしろ観光客や松本来訪者向けの飲食店が多い、ということです。確かに国内の統計では、熊本の生産及び消費量が圧倒的に多く、長野は生産量も消費量も少ないようです。

熊本、会津、長野が馬肉の三大消費地、というのはかつてのイメージだったようです。

以上

<目次>

2023.10

【 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282回	日時	2023 年 11 月 20 日（月） 18:30～20:30
	場所	オンライン（Zoom ウェビナー）
	テーマ	「JIS Q 15001:2023 個人情報保護マネジメントシステム-要求事項」改定について
	講師	JIPDEC（一般財団法人 日本情報経済社会推進協会） 常務理事　坂下哲也（さかした てつや）氏
	講演骨子	2023 年 9 月 20 日「JISQ15001：2023」が発行されました。経済産業省において令和 2 年個人情報保護法改正の対応、また、同法令和 3 年改正を踏まえ規律移行法人をカバーし、更に EU との補完的ルールなど盛り込む内容になっております。形式も従来の法令との重複を無くし、構成を整えています。本日は、どのような改正がなされたのかポイントを解説致します。また、CBPR を巡る国際的な動向も解説します。なお、規格自体は日本規格協会より御購入頂き御覧頂きたくお願い致します。 日本規格協会： https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=JIS+Q+15001%3A2023
	参加費	SAAJ 会員 1,000 円　非会員 3,000 円
	お申込み	https://www.saaj.or.jp/kenkyu/kenkyu/282.html

■SAAJ 月例研究会（東京）		
第283回	日時	2023 年 12 月 18 日(月) 18:30～20:30
	場所	オンライン（Zoom ウェビナー）
	テーマ	ISMAP 制度改善概要と今後
	講師	あずさ監査法人 Digital Advisory 事業部長 山口達也(やまぐち たつや)氏
	講演骨子	2020 年 6 月にスタートした ISMAP 制度も制度開始から 3 年が経過し、クラウドサービスリストへの登録サービスも５０サービスを超える状況となってきています。しかしながら一方で、運用を開始したからこそ判明した課題等もあり、これを受けて本年７月より制度改善も始まりました。本講義では、これまでに認識されてきた課題とそれに対する今回の制度改善の概要をご説明すると共に、今後 ISMAP がどのように活用されていく可能性があるのかについて考察します。
	参加費	SAAJ 会員 1,000 円　非会員 3,000 円
	お申込み	https://www.saaj.or.jp/kenkyu/kenkyu/283.html

<目次>

2023.10

【 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　https://www.systemkansa.org/
・会員規程　https://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・会員情報の変更方法　https://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　https://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。　https://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。

・「発注者のプロジェクトマネジメントと監査」
・「６か月で構築する個人情報保護マネジメントシステム」
・「情報システム監査実践マニュアル」　などの協会出版物が会員割引価格で購入できます。
https://www.saaj.or.jp/shuppan/index.html

・月例研究会など、セミナー等のお知らせ　https://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。
https://www.saaj.jp/04Kaiin/60SeminarRireki.html

・公認システム監査人へのSTEP-UPを支援します。
「CSA：公認システム監査人」と「ASA：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。　https://www.saaj.or.jp/csa/index.html

・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。

・お問い合わせページをご利用ください。　https://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			2023.10
	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
10 月	12：理事会	14-15:第 42 回システム監査実務セミナー (日帰り 4 日間コース後半) 26:第 281 回月例研究会	8:秋期情報処理試験・情報処理安全確保支援士試験 14:東北支部設立 20 周年記念＆ワークショップ 2023
11 月	9：　予算申請提出依頼（11/27〆切） 支部会計報告依頼（1/7〆切) 9：理事会 16：2024 年度年会費請求書発送準備 27：本部・支部予算提出期限 27：会費未納者除名予告通知発送	中旬：秋期 CSA 面接 20:第 282 回月例研究会 下旬：CSA・ASA 更新手続案内 〔申請期間 1/1～1/31〕 下旬：CSA 面接結果通知	4：会員活動説明会
12 月	1：　2024 年度年会費請求書発送 1：　個人番号関係事務教育 14：総会資料提出依頼（1/9〆切) 14：総会開催予告掲示 14:　理事会：2024 年度予算案承認 会費未納者除名承認 第 23 期総会(2/16)審議事項確認 20：2023 年度経費提出期限	15：　CSA/ASA 更新手続案内メール 〔更新申請期間 1/1～1/31〕 18：第 283 回月例研究会 22：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 9：役員改選公示(1/22 立候補締切) 11：理事会：総会資料原案審議 22：17:00 役員立候補締切 27：2023 年度会計監査 31：償却資産税申告期限 31：総会申込受付開始（資料公表）	1-31：CSA・ASA 更新申請受付 22：春期 CSA・ASA 募集案内 〔申請期間 2/1～3/31〕 24：第 284 回月例研究会	8：支部会計報告提出期限
2 月	1：理事会：通常総会議案承認 29：2023 年度年会費納入期限 29：消費税申告期限	2/1-3/31：CSA・ASA 春期募集 下旬：CSA・ASA 更新認定証発送	16：13:30　第 23 期通常総会
3 月	1：年会費未納者宛督促メール発信 14：理事会 28：法務局：活動報告書提出、 東京都：NPO 事業報告書提出	1-31:　春期 CSA・ASA 書類審査 11：第 285 回月例研究会	
	前年度に実施した行事一覧		
4 月	13：理事会	初旬：春期 CSA・ASA 書類審査 8-9：第 40 回システム監査実務セミナー (日帰り 4 日間コース前半) 17：第 276 回月例研究会 中旬：春期 ASA 認定証発行 22-23：第 40 回システム監査実務セミナー (日帰り 4 日間コース後半)	16　春期秋季情報処理試験・情報処理安全確保支援士試験
5 月	11：理事会	10：CSA フォーラム 18：第 277 回月例研究会 中旬・下旬土曜：春期 CSA 面接	
6 月	1：年会費未納者宛督促メール発信 8：理事会 19：年会費未納者督促状発送 21～：会費督促電話作業（役員） 28：支部会計報告依頼（〆切 7/10） 30：助成金配賦決定（支部別会員数）	上旬：　春期 CSA 面接 15：第 278 回月例研究会 中旬：　春期 CSA 面接結果通知 中旬～下旬：　春期 CSA　認定証発送	3:認定 NPO 法人東京都認定日 （初回：2015/6/3）
7 月	5：支部助成金支給 13：理事会	20：第 279 回月例研究会 中旬：秋期 CSA・ASA 募集案内	11：支部会計報告〆切
8 月	（理事会休会） 5：中間期会計監査	1：秋期 CSA・ASA 募集開始～9/30	10:システム監査基準・管理基準ガイドライン公表
9 月	14：理事会	23:(土)13:30 第 280 回特別月例研究会 30-10/1:第 42 回システム監査実務セミナー (日帰り 4 日間コース前半) 30:秋期 CSA・ASA 募集締切	

<目次>

2023.10

【 会報編集部からのお知らせ 】

1．会報テーマについて

2．会報バックナンバーについて

3．会員の皆様からの投稿を募集しております

□■ 1． 会報テーマについて

2023 年の会報年間テーマは、昨年に引き続き

「この変化の時代にシステム監査が目指すもの」

です。

様々なことが変化、進化していく時代の中で、システム監査人は何を目指す必要があるのか、システム監査は何を目的として、実施すべきなのか、その対象範囲やシステム監査人に求められるスキルはどうなるのかという点について、整理・検討が必要なタイミングではないかと考え設定しています。

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． 会報のバックナンバーについて

協会設立からの会報第１号からのバックナンバーをダウンロードできます。

https://www.saaj.jp/03Kaiho/0305kaihoIndex.html

□■ 3．会員の皆様からの投稿を募集しております。

募集記事は次の通りです。

■ **募集記事**

1.	めだか	匿名（ペンネーム）による投稿 原則１ページ　下記より投稿フォームをダウンロードしてください。 https://www.saaj.jp/03Kaiho/670502KaihoTokoForm2.docx
2.	記名投稿	原則４ページ以内 下記より投稿フォームをダウンロードしてください。 https://www.saaj.jp/03Kaiho/670502KaihoTokoForm2.docx
3.	会報掲載論文 （投稿は会員限定）	現在「論文」の募集は行っておりません。

■投稿について　　「会報投稿要項」

・投稿締切：15 日（発行日：25 日）

・投稿用フォーマット　※毎月メール配信を利用してください。

・投稿先：　saajeditor@saaj.jp　宛メール添付ファイル

・投稿メールには、以下を記載してください。

- ✓ 会員番号
- ✓ 氏名
- ✓ メールアドレス
- ✓ 連絡が取れる電話番号

・めだか、記名投稿には、会員のほか、非会員 CSA/ASA、および SAAJ 関連団体の会員の方も投稿できます。

- ✓ 会員以外の方は、会員番号に代えて、CSA/ASA 番号、もしくは団体名を表記ください。

■注意事項

・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。

お問い合わせ先：　saajeditor@saaj.jp

<目次>

2023.10

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 丁目 16 番 7 号 本間ビル 201 号室

■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】　https://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：竹原豊和、安部晃生、金田雅子、越野雅晴、坂本誠、辻本要子、豊田諭、野嶽俊一、柳田正、山口達也

編集支援：会長、各副会長、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>