



認定 NPO 法人

日本システム監査人協会報

2024 年 3 月号

No. 276

No.276 (2024 年 3 月号) <2 月 25 日発行>

今月号の注目記事

【投稿】

「羽田空港事故が示唆する
インシデント管理の重要性」

巻頭言

『能登半島地震と情報共有』

会員番号 : 0608 三谷慶一郎 (副会長)

今般の能登半島地震により、被害に遭われた方々に心よりお見舞い申し上げます。穏やかなお正月の夕方に突然起こったマグニチュード 7.6、最大震度 7 という大地震によって、多くの住民や住居等に甚大な被害が発生し、2月中旬に至っても1万3千人を超える住民が避難生活を続けています。個人的な話で恐縮ですが、私は石川県金沢市の出身で、能登にも親族等は多いため、今回の地震は全く他人事には思えません。

デジタル技術は、被災時や被災後において大きな力になることは間違いありません。今回の地震でも安定した通信環境を維持するために低軌道衛星通信「Starlink」が設置され、ドローンの導入によって孤立地域への薬の配送等が行われました。また、JR 東日本が提供した 1 万 8 千枚の Suica によって様々な場所を日々移動している避難民の現在地をトレースしようとしています。

一方、迅速で効率的な復旧活動に欠かせない、被災情報の共有に関しては課題も見えてきています。報道によれば、今回、道路寸断などにより事前に指定されていた避難所以外の避難や孤立集約等が多く発生したため、準備していた情報システムでは網羅的な被災状況の管理が難しくなったようです。また、地方自治体、自衛隊、災害派遣医療チーム (D-MAT) が発災後の活動によって得られた現地の情報を、それぞれの組織が保有している情報システムに入力してきたため、情報全体を共有することが困難な状況が生まれたそうです。石川県ではこれに対応するために「データ集約・可視化アプリケーション」をごく短期間で開発しました。現地では多くのシステムエンジニアの献身的な頑張りがあったと推察します。

複数の主体が持つデータの共有化や、ニーズの変化に応じて柔軟に対応できるエンジニアリング力の確保は、災害時だけでなく今後社会全体としてDXを推進する上でも大きなテーマになると考えます。今回のような貴重な経験を蓄積していくことが何より重要だと思えます。

被災地の一日も早い復興をお祈りいたします。

各行から Ctrl キー+クリックで
該当記事にジャンプできます。

<目次>

○ 巻頭言	1
【 能登半島地震と情報共有 】	
1. めだか	3
【 この変化の時代にシステム監査が目指すもの - 科学革命 - 】	
2. 投稿	4
【投稿】 羽田空港事故が示唆するインシデント管理の重要性	
【投稿】 デジタル社会の一般市民に安心の担保を	
【コラム】 システム監査のための会計・法律・数学・理科・教育課程再入門 (3)	
3. 本部報告	14
第 284 回月例研究会 講演録 テーマ：「企業価値向上と監査機能の高度化」	
4. 支部報告	18
【北海道支部】 2024 年度 1 月の月例研究会	
【中部支部】 「IT ガバナンス監査研修の実現に向けて」 — (第 2 回) IT ガバナンス監査研修の設計と実施結果—	
5. 注目情報	26
【 IPA 「情報セキュリティ 10 大脅威 2024」 】	
【 警察庁 「ランサムウェアによる暗号化被害データに関する復号ツールの開発について」 】	
6. セミナー開催案内	27
【 協会主催イベント・セミナーのご案内 】	
7. 協会からのお知らせ	28
【 2024 年度春期 公認システム監査人及びシステム監査人補の募集 】	
【 新たに会員になられた方々へ 】	
【 協会行事一覧 】	
8. 会報編集部からのお知らせ	32

めだか 【 この変化の時代にシステム監査が目指すもの - 科学革命 - 】

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。



資料では、サピエンス（現生人類）の“歴史の道筋”を、三つの重要な出来事に置いている。“約7万年前”に始まった認知革命、“約1万2000年前”に歴史の流れを加速させた農業革命、そして、“500年前”に始まった科学革命である。ここでは、“科学革命”について考えてみる。主題は、“科学が進歩するには、研究だけでは十分ではない。進歩は、科学と政治と経済の相互作用に依存している。”である。また、“科学革命”以前と違って、“科学革命”では、“無知の発見”があったといわれるという。

つまり、“科学革命”では、“近代科学は、最も重要な疑問に関して集団的無知を公に認めるという点で、無類の知識の伝統がある。”という視点だ。それは、“a 進んで無知を認める意思。（近代科学は私たちがすべてを知っているわけではないという前提に立つ。） b 観察と数学の中心性。（近代科学は無知を認めた上で新しい知識の獲得を目指す。この目的を達するために近代科学は観察結果を収集しそれから数学的ツールを用いてそれらの観察結果を結びつけ包括的な説にまとめ上げる。） c 新しい力の獲得。（近代科学は説を生み出すだけでは満足しない。近代科学はそれらの説を使い新しい力の獲得とくに新しいテクノロジーの開発を目指す。）”である。

そこで、“とくに注意を向けるべきものが二つある。帝国主義と資本主義である。科学と帝国と資本の間のフィードバック・ループは、過去500年にわたって歴史を動かす最大のエンジンだったと言っよういだろう。”ということである。また、“帝国を建設するにも科学を推進するにも絶対必要なものが、お金である。現代の軍隊も大学の研究所も、銀行がなければ維持できない。”そして、“経済の近代史を知るためには、本当はたった一語を理解すれば済む。その一語とはすなわち、「成長」である。”と言われている。結論として、“産業革命以来、世界人口はかつてない勢いで増えている。1700年には、世界で約7億人が暮らしていたが、現在では、70億人に達しようとしている。”そして、“家族とコミュニティの崩壊”がありストレスの源となっている。また、“AIは、ナイフ形の石器や原子爆弾と違い、自ら、決定を下すことのできる最初のツールとなった。”と思われる。

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：「サピエンス全史 下 文明の構造と人類の幸福」Y・N・ハラリ 著 河出書房新社

（このコラム文書は、投稿者の個人的な意見表明であり、S A A Jの見解ではありません。）

<目次>

【投稿】羽田空港事故が示唆するインシデント管理の重要性

会員番号 0436 大石正人

2024年1月2日夕刻に発生した羽田空港での日航機と海上保安庁機の接触炎上事故（羽田空港事故）について、真因の解明には運輸安全委員会の調査・報告を待たなくてはなりません。事故が発生したC滑走路の復旧に加え（1月8日に運用再開）、管制官とパイロットとの更新記録の公開や、発生から1週間で、国土交通省から「航空の安全・安心確保に向けた緊急対策」（以下、緊急対策）が発表される（9日）など、慌ただしい経過をたどってきました。

事故の真因は運輸安全委員会の調査など年単位の究明を待たなくてはなりません。根本には羽田空港が世界有数の「混雑度」である、という事実があります。英国OAG（航空・旅行データ調査会社）によると、世界の空港提供座席数（2023年、国際線と国内線の合計）で、羽田はアトランタ国際空港、ドバイ国際空港に次いで第3位です。（注）FlyTeam ニュース <https://flyteam.jp/news/article/140252>

東京など首都圏へのビジネス・省庁などの機能集中、人口の集積により、東京と他の地方空港とを結ぶ稠密な国内線網が形成されているところへ、近年はインバウンドと呼ばれる海外からの旅行者の呼び込みにも注力する中で、羽田を発着点とする旅行・移動需要は高まる一方です。羽田空港と都心などとアクセスの良さから、発着枠の拡大ニーズは根強く、これまでも風向きによる飛行ルートの変更などにより、発着可能数の拡大を図ってきました。年間の発着回数は1993年度の19.6万回から2018年度には45.5万回へ増加、感染症蔓延期の減少を経て、2022年度は41.3万回に回復し、発着頻度は2,3分に1回と「JR山手線並み」とされています。年末年始も羽田空港はほぼフル回転だったとされ、事故の発生した1月2日は帰省先や旅行先からのUターン需要で、特に夕刻にかけては、到着便も相当数に上っていたはず。そうした時間帯に、能登半島地震への支援物資運搬のために被災地（新潟基地）へ向かう海上保安庁の固定翼機が飛び立とうとしていました。羽田航空基地に所属する同海保機も様々な任務で発着を繰り返しており、2日も警戒業務などに当たった後、新潟へ向かう手はずでした。

利便性が高く稼働率が目いっぱい首都中核空港として、羽田は平素から、能力を最大限に引き出すべく、相当な無理をして運行管理がなされているといえます。羽田に限りませんが、混雑度の高い空港は、常にギリギリの状態で運用されている、とよいでしょう。

インバウンド需要の増加を図る、という国の施策のかけで、航空機の安全確保が、空港の混雑度に見合った内容に見直されてきたのか、この点を問うマスコミの論調は目立ちませんでした。例えば、管制システムは安全度を高めるために十分なサポートができるよう改善、機能向上が図られているのか、誘導路や停止線などの高輝度化と視認性の改善措置はとられているか、管制官の配置は混雑度に見合って増員や訓練の充実策がとられているか、などなど、素人が思いつくだけでも、確認すべき観点はたくさんありそうです。

深刻な事故の再発を防ぐため、国土交通省も「羽田空港で発生した航空機衝突事故を踏まえ、滑走路路上における航空機等の衝突防止のためのさらなる安全・安心対策を検討するため」、1月16日に有識者及び関係団体（航空会社とパイロットの団体）から構成される「羽田空港航空機衝突事故対策検討委員会」を設置し

ました。2024年1月19日に「第1回 検討委員会」が開催され、第1ステップとして既報の1月9日の緊急対策、第2ステップとして同検討委員会の開催と中間とりまとめ（今夏を予定）、第3ステップとして、運輸安全委員会の調査報告を受けた抜本的対策、という対処の道筋が示されました。

運輸安全委員会が調査対象とする事故や重大インシデントは、事故や事故につながりかねない顕現化した事象です。最新の委員会年報（2022年版）でみると、2021年中に調査対象となった事故が21件、事故につながる重大インシデントと認定されて調査したのが15件、となっています。

このほか、2014年7月から、航空安全情報自発報告制度の運用が開始されました。航空事業者や個人の操縦士等はこれらの法令等で規定されているトラブルが発生した時は、国土交通大臣への報告が義務付けられています。これに対し、航空安全情報自発報告制度に基づく「ヒヤリ・ハット」報告は、航空関係の業務に携わる個人又は組織から、自発的に報告される点が異なります。日本も締結している国際民間航空条約では「義務報告制度では捕捉しにくい安全情報を収集・分析・関係者と共有するため、自発的な報告制度を確立すること」が求められていることに応えるものとなっています。報告に基づく分析結果や改善提案は航空関係者に情報還元されるほか、国土交通省（航空局）にも提供されますが、「この場合も個人や会社名を特定される情報の提供はない」としています。

どのくらいの報告がなされているか、は同制度を運用する公益財団法人航空輸送技術研究センターのサイトでは確認できませんでしたが、報告制度発足後1年程度の間65件の「ヒヤリ・ハット」事象が報告されていたようです。年3回発行されているfeedback資料の最新分（2023-02号）では211件の事例が掲載されていますので、報告件数はかなり増えてきた印象です。

（注）「運輸安全委員会ダイジェスト」2015年9月15日（通算18号）のトピックス「航空分野における「ヒヤリハット」について」およびFEEDBACK - 航空安全情報自発報告制度を参照。

https://jihatsu.jp/publications_cat/feedback/

2022年中の年間運行回数が国内線で82万回、国際線で8万回に上る中で、こうした事故や重大インシデント、ヒヤリ・ハットの件数をどう評価するかは別にして、大事故の未然防止のために、分析結果の教訓を生かすことは極めて重要です。事故や重大インシデントはもちろん、ヒヤリ・ハットの情報を収集、分析し、重大事案に至る手前で回避するための方策を講じることは、予兆管理の基本的なアプローチとされます。過去の事故や重大インシデント、ヒヤリ・ハットを個々にみると、パイロットや整備士、さらには航空管制官といったヒューマンファクター、機体や機器などハード要因のほか、燃料のゆとりや飛行時間の制約、気象条件や飛行場の立地といった環境的要因など、様々な要因が複雑に絡み合っていることがわかります。また海外の事例では、日本の運輸安全委員会のような公的機関の調査報告書が、のちに提起された訴訟などをきっかけにした再調査で、真因をとらえそこなっていたことが判明したケースもあります。

安全運航のためには、時間や経済性（人的物的コストと航空会社の経営）のもとで、実に多様な要因をクリアしたうえで、一つ一つのフライトを確保し、また航空機相互の距離や飛行ルートなどが複雑に絡み合っています。このため、航空機の安全運航にかかる予兆を適切につかみ、対処するためには、個別の不備事案

を掘り下げただけでも困難なはずですが。ただ数多くの事案を一つ一つ紐解いて対策を立てるのは、安全運行管理に従事する様々な担い手にとっても現実的ではありません。

このため、先述の「航空輸送技術研究センター」のような国土交通省の施策を具体化する組織があるわけですが、残念ながら紹介される事例は国内の関係者からのものであり、feedback レポートを見る限り個別事案の掘り下げ度合いも様々なように見受けられます。

こうした観点から、もう四半世紀前の出版にはなりますが、科学分野の啓発書「大事故の予兆をさぐる」（宮城雅子著、講談社ブルーバックス、1998 年刊）が参考になります。著者は 1968 年に設立した航空法調査研究会で、運行乗務員、航空管制官、整備士に対してインシデントレポートを独自に収集し、精度を高めたうえで、多変量解析の数量化Ⅲ類を適用して、潜在的な関連度を抽出する取り組みを報告書にまとめて出版しました。この仕組みを I R A S（インシデント・レポート・アナライジング・システム）と呼んでいて、その成果を、一般向けに解説した新書になります（同書は出版社で品切重版未定のため、図書館などで参照ください）。20 世紀中に起きた様々な事故の背景に、多くの要因が関連していること。一つ一つの要因の危険度がさほどではなくても、それが重なることによって、危険度が高まること、要因間の関連性を探ることによって、インシデントのパターン（統計学的なクラスター）が見いだされること、などなど示唆に富む結果が得られています。さらにいえば、航空機の安全運航を支援する様々なシステムが開発、導入されることで、異常事態の発生時にかえってパイロットの操縦ミスを誘発する懸念があることも出版当時から指摘していました。ただ、こうした分析は、時間の経過とともに航空事情が変わる中で、著者が従事した航空法調査研究会のような団体が、持続的に取り組みの成果を公表していないため、その後の足取りをたどることはできませんでした。

また、この啓発書の最後に著者は、法令に基づく主務大臣への報告に限界に触れています。報告の範囲が狭いほか、報告内容（項目）が少なく、危険因子の抽出が難しい、という指摘です。また航空会社自身がパイロットなどからの独自の安全報告を受ける事例も当時からありましたが、主務大臣あてと同様件数が少なく、正直に報告すると行政処分や社内処分の対象になりかねない、とすれば報告するインセンティブもそがれる、としています。航空安全情報自発報告制度では、こうした懸念を払しょくする仕組みを構築していますが、公的制度である以上、懸念して報告を手控える傾向が全くなくなった、とは言えないでしょう。

そうだとすると、報告制度発足当初に比べれば、報告件数が増えていることも事実であり、毎回の feedback レポートでも、報告内容は軽微なものを含め、かなり幅広い内容になってきているようです。欲を言えば、今後は海外航空会社や海外の事例を含め、情報を集積し、同じ基準で分析できるよう、データの質を標準化できればいいな、と思います。先述の啓発書でも、機体の整備不良にかかる海外でのインシデントでの教訓が生かされないまま、他の航空会社の同型機でインシデントにつながった事例が紹介されていました。この点では航空機メーカー頼みでは、自社の不備を積極的に開示する姿勢を確実に保障できない可能性もあるため、やはり報告を受ける国を超えた機関同士が、迅速かつ円滑に情報共有する仕組みの構築も望まれます。

そのうえで上述のIRASのような手法を使って、定期的に分析し、インシデントレポートで浮かび上がる傾向などを情報還元し、航空会社や運行管理に当たる要路、所管省庁において、既存の施策の有効性を検証し、改善余地があれば施策の見直しや空港整備、管制体制の改善に繋げていけないでしょうか。

またセンサーなど予兆をつかむツールやデータが充実し（IOT）、AI（人工知能）を活用した分析手法の高度化も進展しているとみられる状況下、定期的な分析手法の向上と既存施策の有効性の検証など、従来以上に有効なアプローチを編み出し選択する余地も広がってきている予感がしています。対策を追加するばかりでは、かえって運行管理の負担を過重にする懸念もあるからです。先述の啓発書の出版から四半世紀、運輸安全委員会のみならず航空安全情報自発報告制度の運用の定着が図られる中で、分析手法の向上と分析結果の活用の充実が進むことで、内外の公的機関も関与する形で、航空機事故の予兆管理や有効な未然防止策が、仕組みとして定着していくことを強く期待します。

同様の課題は、運輸交通の分野だけでなく、広く労働災害や通信・システム障害、火災や爆発、有害物質の流出など、さまざまな「事故」分野に共通する課題です（よく知られる通り、例えば失敗学、と名付けられた学問分野で豊富な事例収集と出版、報告が行われてきました）。

個別事案を掘り下げて再発防止を講じることはもちろんですが、むしろ起きた事故やインシデントのみならず、ヒヤリ・ハット事象を含めて、報告などの仕組みを構築し、分析して、改善に繋げるPDCAサイクルを整備していくことが極めて重要です。情報システムの分野についても、事故やインシデント、ヒヤリ・ハットにかかる情報をもつ公益性について、共通認識が深まり、航空安全運航と同様の意識で取り組みが進むことを願ってやみません。



<目次>

【投稿】 デジタル社会の一般市民に安心の担保を

会員番号 1217 岩原秀雄

英郵便局での冤罪事件で、富士通提供のシステムの不具合が問題となっている。公共性の高いシステムでのトラブルであり、関連知識や情報システムに必ずしも精通していない利用者・一般市民が被害者である。マイナカードのシステム利用をめぐっても一般市民の被害者が報道されている。一般市民の利用時に発生し、発見されるトラブルには「設計時には思いもよらないユニークなトラブル」が見られる事が多い。

EC サイト利用でも多様なトラブルが多いと聞く。EC サイトの旅行大手エージェントで「6 人予約のうち、1 名を解約しようとして、操作を間違え、6 人分が解約となってしまう、代わりの予約がとれず悲しい思いをした。あの時、解約内容確認の MSG 画面があれば・・・」。またこんなトラブルも聞く。「ある相談サイトにトラブル解消法を相談し、解決したので、その時料金を支払った。ただ、その後もそのサイトから料金請求が続いた。不審に思い問い合わせるとサブスク契約になっているという。その旨の MSG 表示は見逃すほどわかりにくい表示だった。」いずれも一般市民が陥りやすいトラブル事例かもしれない。法の規制上はなんらかの不備があったとは言えまい。しかしながら、「EC サイト音痴」が多い一般市民が、まきこまれかねないトラブルである。

「優良 EC サイトマーク」(仮)制度が立ち上がってくれば、デジタル社会では、ネットワークを介して、誰もが何らかの取引を行わざるを得ない。しかしながら老若男女全てが、それらに精通しているわけではない。法制度、各種ガイドラインは複雑し難解でもある。それらをクリアーした安全でわかりやすい EC サイト(システム)であることを認証する審査制度ができないものだろうか? この際、公共性の強い EC サイト(ないしそのシステム)も対象にして。

この制度では、法令等の遵守・セキュリティの確保は当然の要件として、一定期間の利用を前提にした「認証確認利用期間」の設定を要件にしたい。一般市民の利用を前提にして、その利用実績を踏まえた意見・評価を重要な認証の要件にすべきと思う。画面合成、生成 AI などの利用拡大に伴って、ますます利便性が増す一方で、合法ではあるがわかりにくい EC サイトや フェイクサイトも増えている。利用者である多くの一般市民を保護し、利便性の高い安心できる EC サイトであることを認証する制度があってほしい。

P マーク制度は 25 年を過ぎ、この間の関係者の苦節は大変なものであったと思料するが、デジタル社会を支える制度として定着し、個人情報保護に、評価を得ている。生成 AI をめぐり、政府は安全性に関する専門機関「AI セーティ・インスティーチュート AISI」を立ち上げるという。デジタル社会に生きる一般市民を保護し、安心して利用できる EC サイト(システム)であることを認証する制度も発足させたいものである。

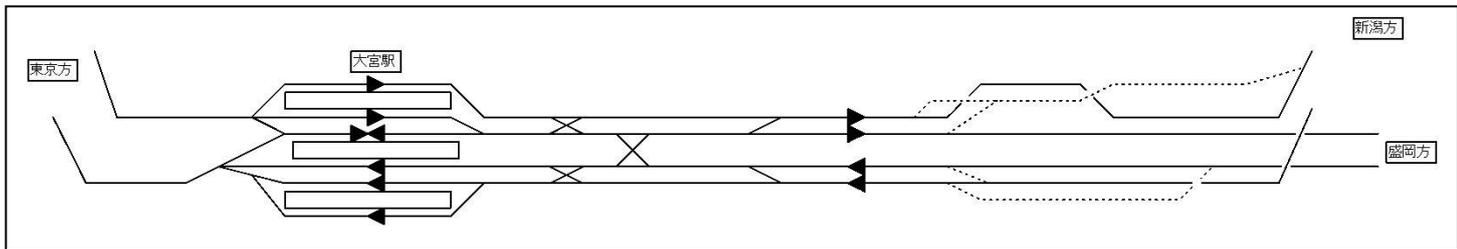
<目次>

【コラム】システム監査のための会計・法律・数学・理科・教育課程再入門（3）

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.はじめに ～ 品質不正及び事故の多発【システム監査の専門家の出番】

2024 年は年初から災難続きである。石川県能登地方で大震度、羽田空港での JAL と海保空輸機の衝突事故に続き、1 月 23 日には新幹線の上野～大宮間で架線が垂れ下がり、北海道・東北・秋田・山形・上越・北陸の各新幹線が東京～大宮間で終日運休となった。現在、大宮駅での折り返しは 16 番線のみが可能であり、折り返しに長時間を要し、大きな混乱が発生した。大宮駅の東京方に 2 線の折り返し線があれば、上記のような混乱は回避できた筈である。再発防止のためにも直ちに着工するべきであり、国土交通省は JR 東日本について技術的助言(行政指導)を行うべきである(→文献[7]を参照,下図は[8]より引用)。



また、大阪の南海電鉄の踏切において、列車通過前に遮断棒が上がり、列車と自動車とが接触するという事故が発生した(→[9])。システムの外部監査の法律による義務化が必要であると考えられる。

§2.メーカーや IT 事業者の品質に関する不祥事【システム監査の専門家の出番】

昨年末から 1 月に掛けて自動車メーカーの品質管理で大問題が発生したが、システムのバグが、英国での冤罪事件(700 人以上が起訴、自殺者・失業者多数)の原因となったり、検査データの組織的改竄が明らかとなった。我が国の産業競争力を損なう深刻な事態であり、甚だ遺憾である(→[10-11])。やはり、**システムの外部監査の法律による義務化**が必要である。具体的には、会社法第 327 条及び第 328 条において「会計監査人」とあるところを「会計監査人及びシステム監査人」と改め、第 337 条の 2(システム監査人の資格)を新設し、「システム監査人たる資格」は経済産業大臣の定める「システム監査技術者」とするべきである。

§3.システム・インテグレータ認定・登録制度の復活の必要性【システム監査の専門家の出番】

上記のような品質管理上の問題が発生する原因としては、2 つの要因が考えられる。

- ①「第一次ゆとり教育」(昭和 41～52 年度生まれ)によって、文系の大半と理系の一部が「確率・統計」を履修しておらず、「必要条件と十分条件」が分からず、統計的推測・評価が分からない人が多い。
- ②2003 年のシステム・インテグレータ認定制度の廃止、2010 年の同登録制度の「事業仕分け」による廃止により、情報処理試験有資格者の社会的地位が急落し、価格競争が暴走した。

★①については、後述するように徐々に改善傾向がみられるが、②については(税制優遇は別として)旧制度を手直して再開するべきである。そして、中央省庁や地方自治体は入札の必須要件または重要な加点要素とするべきである。

§4.最先端の科学技術の動向

昨年来、核融合や量子コンピュータの分野で、急速に科学技術が進歩している(→文献[12-18])。

「自社で研究・開発するよりも権利を買ったほうがトク」という、2006 年以降の悪しき慣習は直ちに排斥するべきである。そのためにも、**2006 年の会計基準の改悪 = 研究開発費の一律費用処理 = 企業会計基準「実務**

対応報告第 19 号は**自社開発の最大のネック**であるので、この悪しき基準を即時廃止し、IFRS の非上場企業への一般開放及び個別財務諸表への適用を直ちに認めるべきである。

なお、自動車のマツダが**ロータリー・エンジンの開発チームを再結成**した。この技術は電気自動車(EV)との相性が良く、我が国の産業競争力の大きな柱に成長する可能性があるので、経済産業省も積極的に支援するべきである(→文献[19])。次世代新幹線のプロトタイプであった小田急電鉄の 50000 型 VSE の技術は我が国の至宝である。経済産業省・国土交通省は国費を投じてでも動態保存するべきである。

§5. 「脱ゆとり教育」の流れ

学問の世界では「論理の順番」と「歴史の順番」と「発想の順番」は一致しないことが多い。また、戦後、学者の世界では「実験が絶対的に優先」か「理論が絶対的に優先」かという不毛な二項対立が暴走した。しかし、天王星と海王星の発見の経緯をみれば、この議論が当を得ていないことはよく理解できる。

○天王星：ドイツ生まれの音楽教師 Frederick William Herschel(旧名：Friedrich Wilhelm Herschel)が 1781 年に自宅の望遠鏡で偶然発見。この功績により、Sir の称号を得る。

○海王星：1821 年にフランス人天文学者 Alexis Bouvard が『天王星の天文表』(des tables pour la planete Uranus)において、天王星の軌道に変動を及ぼす第 8 惑星の存在を予言。

→1846 年 8 月にフランス人 Urbain Jean Joseph Le Verrier が第 8 惑星の天球上の位置を計算。

→同年 9 月に Berlin 天文台の Johann Gottfried Galle が発見。

[1]3 次元ベクトルの外積

「第一次ゆとり教育」において、槍玉に上がったものの 1 つが「ベクトルの外積」である。ベクトルの外積は、電磁力やモーメントの基本であり、非常に重要なものであるが、強烈なバッシングの対象となった。特に、内積と異なり、特定の次元 ($n=3$ と $n=7$ のみ)でしか定義されないことから、物理からの数学の完全分離を主張する Bourbakist の攻撃対象にもなった。

〔ベクトルの外積の例〕

①円運動の速度(m/s)： $\vec{v} = \vec{\omega} \times \vec{r}$ …角速度： $\vec{\omega}$ (rad/s)，回転軸上の点を原点とする位置ベクトル： \vec{r} (m)

②力のモーメント(J)： $\vec{N} = \vec{r} \times \vec{F}$ …力： \vec{F} ，回転軸上の点を原点とする位置ベクトル： \vec{r} (m)

③電磁力： $\vec{F} = q\vec{E} + q(\vec{v} \times \vec{B})$ …電荷： q (C)，電場： \vec{E} (N/C)，速度： \vec{v} (m/s)，磁束密度： \vec{B} (wb/m²)

★このように「ベクトルの外積」は非常に重要である。心ある人々の長年の努力が実って、新課程の「数学 C」では、ついに**「ベクトルの外積」が教科書でも復活**した(写真は数研出版)。また、**行列と一次変換も復活**した。しかも 4×4 行列の積も教科書に出ているので、物理で重要なロドリゲスの公式(3 次元の回転軸と有限の回転角から行列を求める公式)及びその逆なども、理系上位受験者には必要となるであろう(→文献[1-3])。

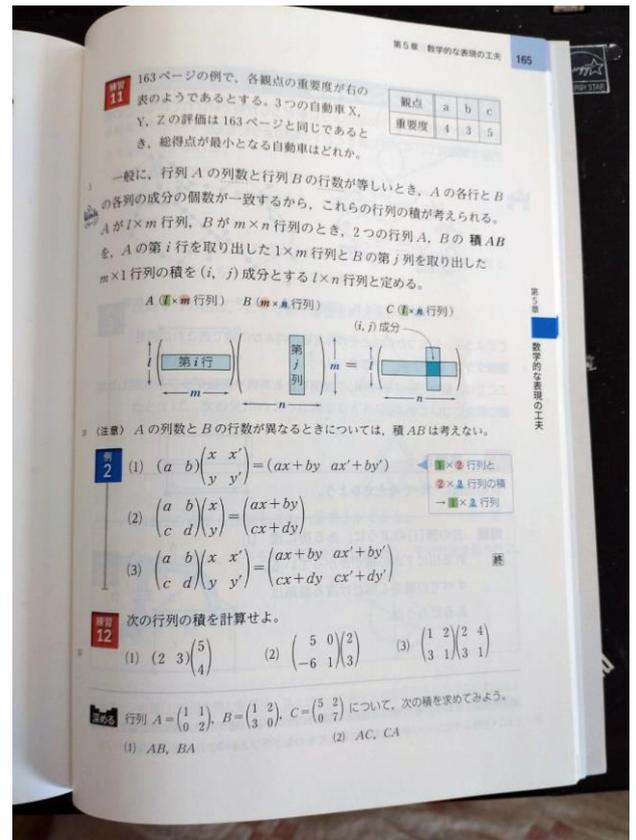
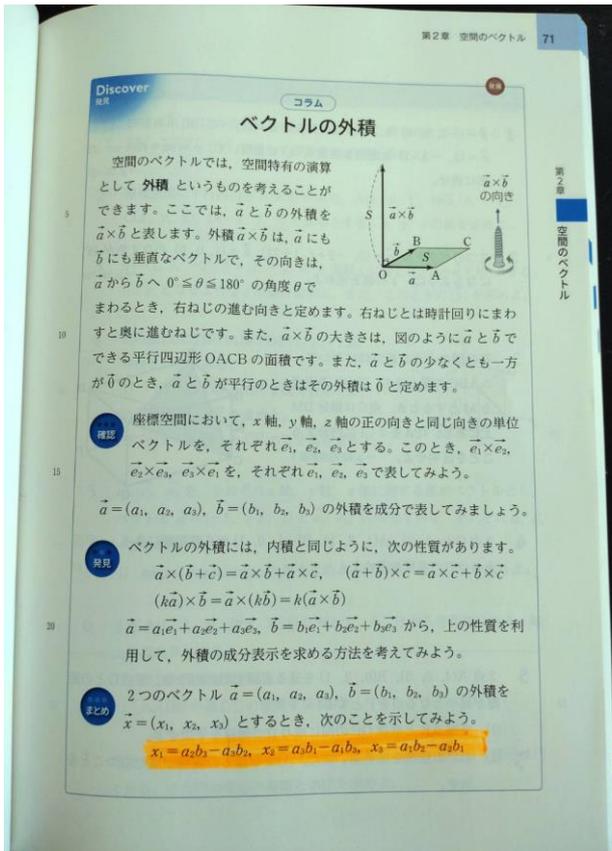
ただし、「物理」のカリキュラムとの関係性を考えると、**ベクトルは高 2 の最初から学習しておくべき**なので、文部科学省は直ちに以下の布告を行うべきである。

①「数学 C」の「ベクトル」と、「数学 B」の「統計的な推測」を入れ替える。

②「物理基礎」の 1 年次配当をしないよう指導する、最低でも、非推奨とする。(6 年一貫制は除く)

※現在、「数学 B」と「数学 C」を高校 2 年から同時履修している学校もあるが、週 1 単位ずつでは中間テストが成立しにくいなどの弊害も生じている。また、高校 2 年の 3 学期から「数学 C」を履修しているケースも多いが、「物理基礎」の進捗には間に合わない。そのため「物理基礎」の授業では、公式だけを詰め込むことになり、学生の消化不良の元凶となっている。

中長期的には、現在の数学 I と II (2 次方程式の虚数解)については、「第一次ゆとり教育」以前のように中学 3 年に降ろすべきである。また、三角関数については、現行の「数学 II」の部分「数学 I」に、指数関数と対数関数も「数学 I」または「数学 A」に降ろすべきである。



※1.現在、英語の過去形と動名詞は**小学校6年生**である。芸術と体育と書道を削ってでも、数学と英語を約2年間前倒し、**ドイツや戦前の日本のように高校物理は全て微分・積分の応用として教育する**ように戻すべきである。そして、**ドイツのように、ベクトル解析・テンソル・微分方程式を高校に降ろすべき**である。

[2]波動

物理基礎の教育現場を見ていると、波動の単元で躓く学生が非常に多い。特に、y-x 図において「微小時間経過後の波形から振動速度の方向を読み取る技法」の牽強付会ぶりは失笑を禁じ得ない。これは全て、GHQ によるカリキュラム改変と、1947 年の数学者と物理学者の分断の結末である。

★1 次元の弦を伝わる波動も平面波も、波動関数は、本来次のような 2 変数関数である。

$$y(t,x) = A \sin(\omega t - kx + \theta_0) \tag{5.0}$$

ここで、振幅 :A(m),角振動数: ω (rad/s),時刻:t(s),角波数:k(rad/m),位置(m):x,初期位相: θ_0 であり、周期を T(s),波長を λ (m),振動数を f(Hz=1/s),波数を Λ (1/m)とすると、次式が成立する。

$$\omega T = k\lambda = 2\pi(\text{rad}) \tag{5.1}$$

$$fT = \Lambda\lambda = 1 \tag{5.2}$$

$$\text{同一位相面} : \omega t - kx + \theta_0 = (\text{一定}) \tag{5.3}$$

しかし、現在の高校のカリキュラムでは本質の(5.0)に触れず、その x=0 の断面：

$$y(t,0) = A \sin(\omega t + \theta_0) \tag{5.4}$$

を x=0 における媒質の運動を表すものとして y-t 図で表している。また、t=0 の断面：

$$y(0,x) = A \sin(-kx + \theta_0) = -A \sin(kx - \theta_0) \tag{5.5}$$

を t=0 における波形を表すものとして y-x 図で表している。

★ここで、波動の位相速度(伝播速度)は(5.3)の両辺を t で微分して、

$$k \frac{dx}{dt} = \omega \quad \Leftrightarrow \quad \text{位相速度(伝播速度)}: \quad \mathbf{v} = \frac{dx}{dt} = \frac{\omega}{k} \quad (5.6)$$

一方、媒質の振動速度は(5.0)を t で 1 回偏微分することにより、振動加速度は 2 回偏微分することで得られる。

$$\text{媒質の振動速度:} \quad \frac{\partial y(x,t)}{\partial t} = A \omega \cos(\omega t - kx + \theta_0) \quad (5.7)$$

$$\text{媒質の振動加速度:} \quad \frac{\partial^2 y(x,t)}{\partial t^2} = -A \omega^2 \sin(\omega t - kx + \theta_0) = -\omega^2 y(x,t) \quad (5.8)$$

★このように、波動は 2 変数関数の最大最小・偏微分等の知識を前提としており、数学のカリキュラムの改善が必要である。また、一部の教科書では角波数 k の記述がなく、初学者の躓きの原因となっている。

そもそも、「波動」については三角関数の微分・積分の知識が不可欠であるので、全て「物理基礎」から除外するべきである。また理数探求Ⅱの時間を増やし(現在 2~6 単位)、ウラとなる文系コースの学生には、ドイツ語/フランス語を教えるべきである。大学入試における①数学 IAIIBC の義務化、②外国語の 2 か国語の義務化、③理系学部における理科 2 科目及び数学 III の義務化、④医学・薬学・歯学・看護系における AO 入試の全面禁止、⑤推薦入試の定員の 1/5 以下への制限、及び、卒業要件の外国語 3 か国語化などは急務である。

§6.高校「数学 I」のカリキュラム

[1]目的が不明確で唐突に感じる単元の配列

高校生の多くは「数学 I」で躓く。その大きな理由の一つが「単元の目的が不明確であること」である。例えば、唐突に次の因数分解の公式が登場する。(→文献[1-3])

$$a^3 + b^3 + c^3 - 3abc = (a+b+c)(a^2 + b^2 + c^2 - ab - ac - bc) \quad (6.1)$$

あるいは、1 の立方根の 1 つである $\omega = (-1 + i\sqrt{3})/2$ を用いた次の因数分解の公式も登場する。

$$\begin{aligned} a^3 + b^3 + c^3 - 3abc &= (a+b+c)(a^2 + b^2 + c^2 - ab - ac - bc) \\ &= (a+b+c)(a + \omega b + \omega^2 c)(a + \omega^2 b + \omega c) \end{aligned} \quad (6.2)$$

また、4 次式を「複二次式」と呼ばれる $x^2 = X$ と置いた式への式変形や、因数分解の補助手段としての「因数定理」やその一般形である「剰余定理」が唐突に登場する。なぜだろうか？

[2]「代数学」の目的

因数分解など「数学 I」の「式と計算」を発展させたものは「代数学」である。そもそも「代数学」は紀元前から「代数方程式を解くこと」を通して発展してきたものである。「剰余定理」や「因子定理(因数定理)」も代数方程式の解法のアлゴリズムの一環であることを理解すれば、全体の見通しが良くなる(→文献[1,4-6])。実は(6.2)は Cardano の公式を補完し不適解を除外するための公式であり、複二次式は Ferrari の公式の根幹である。

★実は「式と計算」や「解(の基本対称式)と係数の関係」等は、1 次~4 次の方程式を解くためのプロセスである。よって、下のアルゴリズムを理解すれば、唐突感は低減する筈である。なお、5 次以上の方程式には「代数的演算」(四則演算と冪乗根)による解の公式は存在しないことが、Galois と Abel により証明されたが、正二十面体ではなく、4 次元正単体である正五胞体を用いた証明が分かりやすいと考えられる(→文献[1,2,4-6])。

※★、▲、■はそれぞれ 2 次、3 次、4 次方程式の解の公式を使用することを示している。

次数	1		2		3			
左辺	☆(1 次方程式)	1 次の項なし	(1 次×1 次)に分解可能	分解不可 ★	1 次 2 次の項なし	(2 次×1 次)に分解可能	(1 次×1 次×1 次)に分解可能	分解不可 ▲
	$ax + b$	$x^2 - k(\text{定数})$			$x^3 - k(\text{定数})$			
解	↓	↓	↓	↓	↓	↓	↓	↓
	$x = \frac{-b}{a}$	$x = \pm \sqrt{k}$	☆☆へ	解の公式	$x = \sqrt[3]{\text{定数}}$	★☆☆へ	☆☆☆☆へ	Cardano の式
					$x = \sqrt[3]{\text{定数}} \omega$	二次方程式と一次方程式に帰着	3 個の一次方程式に帰着	
					$x = \sqrt[3]{\text{定数}} \omega^2$			
		2 個の一次方程式に帰着						

次数	4					5以上		
左辺	1次~3次の項なし	(3次X1次) に分解可能	(2次X2次) に分解可能	(2次X1次X1次) に分解可能	(1次X1次) (1次X1次) に分解可能	分解 不可 ■	最高次数と 多項式	その他 の場合
	$x^4 - k$						$x^n - k$ (定数)	
	↓	↓	↓	↓	↓	↓	↓	↓
解	$x = \pm \sqrt[4]{(定数)}$	▲☆へ	★★へ	★☆☆へ	☆☆☆☆へ	Ferrariの の式	複素数 平面上の 円上の 正n角形	※未解決
	$x = \pm i \sqrt[4]{(定数)}$	三次方程式と 一次方程式に 帰着	2個の 二次方程式 に帰着	二次方程式と 2個の 一次方程式に 帰着	4個の 一次方程式に 帰着			解の公式は 存在しない

§7.【要注意】相続登記の義務化について 【システム監査の専門家の出番】

不動産登記法の改正により、2024/04/01 から相続登記の義務化が施行される。また、2026/04/01 から住所移転及び(婚姻等による)氏名変更登記の義務化も施行される。これらはいずれも**施行以前に相続が開始したり、住所移転及び氏名変更が発生した場合にも遡及適用**される。筆者は特定行政書士でもあるが、今年に入って5件以上、「相続登記の義務化が遡及適用されること、及び、罰則があること」を知らない人に会った。過去に相続が発生し、相続登記が未了の人は速やかに登記をされることをお勧めする。注意して頂きたいのは、**相続放棄を家庭裁判所に申述し、その認容審判を受けない限り、「法定相続人」からは除外されない**ので、**当該不動産を受領しない相続人も含めて**、相続人全員の実印及び印鑑証明(未成年者の場合は民法826条に定める「特別代理人」の実印及び印鑑証明)が必要であることである。

なお、システム監査人としても、クライアント企業で斯様な事案が発覚した場合は、お知らせするべきであると考えられる。(登記については、相続人本人が登記申請を行うか、司法書士に依頼して下さい。)

※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・会計基準の適用等については、必ず、御自身で顧問会計士、弁護士、司法書士、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、数学・理科カリキュラム再考」(最新版 2024/01/08)
- [2] 「軽減税率」田淵隆明が語る、数学・理科カリキュラム再考(II)」(最新版 2024/01/08)
- [3] 「軽減税率」田淵隆明が語る、IFRS&連結会計 Ver7」(I)(II)(2022/4/18)
- [4] 正五胞体を用いたガロア理論の証明～なぜ、正十二面体、正二十面体ではないのか?～
<https://www.youtube.com/watch?v=3sxWZwWqzRc>
- [5] 正五胞体を用いたガロア理論の証明Ⅱ～正五胞体と正二十面体の類似点と相違点～
https://www.youtube.com/watch?v=8bmtinhu_ts
- [6] 正五胞体を用いたガロア理論の証明Ⅲ～方程式の解の配置から図形が見える～
<https://www.youtube.com/watch?v=MoKZWki-OGI>
- [7] 1月23日に起きた東北新幹線架線トラブル https://www.youtube.com/shorts/M3L4EHB_NbU
- [8] <https://twitter.com/derivative/status/702867939553218560/photo/1>
- [9] なぜ? 電車が踏切通過の際に遮断機が上がる 動き出した車と接触 南海電鉄「原因を調査中」 過去にも別の踏切で同様の事故 <https://video.yahoo.co.jp/c/16778/9192954c1885681aff01240a97b2ff37b9d09c2b>
- [10] <https://newsdig.tbs.co.jp/articles/-/952461?display=1>
- [11] <https://www.yomiuri.co.jp/economy/20240112-OYT1T50147/>
- [12] JAXA 無人機が月面着陸 <https://www.nikkei.com/article/DGXZQOUC1664F0W4A110C2000000/>
- [13] <https://news.mynavi.jp/techplus/article/20240119-2866403/>
- [14] 原子をナノチューブへ一列に閉じ込めた「一次元気体」の撮影に成功!
<https://nazology.net/archives/144065>
- [15] 細胞核内のDNAが二重らせんの逆ねじりでゆるむ仕組みを解明
<https://www.kyoto-u.ac.jp/ja/research-news/2024-01-24>
- [16] 核融合発電「原型炉」開発着手へ、量研機構が主体に <https://newswitch.jp/p/40257>
- [17] 核融合炉の中核部品は日本とロシアが独占 夢を見た欧州は後手に
<https://xtech.nikkei.com/atcl/nxt/column/18/00138/042801030/>
- [18] 高速炉「常陽」、アクチニウム225製造も目的に がん治療に活用へ
<https://www.asahi.com/articles/ASS277QYWS27UJHB00N.html>
- [19] <https://news.ntv.co.jp/n/htv/category/society/ht43d42346ba64489dab0d9a0a40def7f4>

<目次>

第 284 回月例研究会 講演録**テーマ：「企業価値向上と監査機能の高度化」**

会員番号 0819 永井孝一（個人情報保護監査研究会）

【講師】 一般社団法人 実践コーポレートガバナンス研究会 代表理事 大谷 剛（おおたに ごう）氏**【日時・場所】 2024年1月24日（水）18時30分～20時40分、オンライン（Zoom ウェビナー）****【要旨】**

企業価値向上に向けた、監査機能の高度化について、リスクとコントロールと監査領域、監査責任役員によるプロフェッショナル・パートナーシップとしての三様監査、将来財務情報である非財務情報の開示充実、の3つの視点から解説する。

【講演録】**1. リスクとコントロールそして監査****● COSO フレームワーク**

- ・ガバナンスの中に ERM があり、ERM の中に内部統制があるという構造になっている。
- ・抽象的な概念としてのガバナンスと、個別具体的な内部統制をつなぐのが ERM(リスクの認識・評価)である。
- ・ガバナンスの外側を各国の法令が取り囲んでいる。

● COSO-ERM(2017)

- ・ミッション、ビジョンおよびコアバリューを入力として、戦略の策定、事業目標の体系化、実践とパフォーマンスというプロセスを通していくことで、価値の向上というアウトカムに結びつける構造になっている。
- ・経営のあらゆる面にリスクがあり、あらゆる面でコントロールが必要になる。従って経営の全領域において内部監査が重要になるといえる。

● COSO キューブ(2013)

- ・業務の有効性・効率性、報告（財務・非財務）の信頼性、コンプライアンスの3つの目的を達成するために、統制環境、リスク評価、統制活動、情報と伝達、モニタリング活動の5つの構成要素を組織のすべての単位で実行されるプロセスで、すべてのマネジメントが理解する必要があるものである。
- ・COSO キューブを使いこなすことが内部監査人には求められる。
- ・統制環境が重要である。リスク管理委員会にてリスクの識別と評価（発生頻度とインパクト）の下に優先順位付けがされ、その報告を受けた取締役会がディスカッションを行い、それを受けて全社的にどのようなコントロールを運用するかという統制活動、外部への開示・内部への開示という情報の伝達につながる。

2. プロフェッショナル・パートナーシップとしての三様監査

●取締役会、監査役会等および内部監査部門の新たな役割

- ・取締役会は、中長期的な企業価値の向上の観点から、自社のサステナビリティを巡る取組みについて基本的な方針を策定すべきである。また、人的資本・知的財産をはじめとする経営資源の配分や、事業ポートフォリオに関する戦略実行の監督を行うべきである。

●三線モデル（3つのディフェンスライン）と二系統の報告経路（デュアルレポーティングライン）

- ・内部統制の基本体制は、第一線が事業部門のマネジメントコントロール、内部統制手段で、第二線は管理部門による財務管理、セキュリティ、リスクマネジメント、品質、検査、コンプライアンス活動、第三線が内部監査である。
- ・最後の砦としての内部監査は、第二線が十分に第一線を見ているかをしっかり監査し、その確認のために第一線の監査を行うものである。

●三線モデルの論点

- ・三線モデルの論点には、以下のようなものがある。

経営者は3つのディフェンスラインを整備・運用しているか。

3つのディフェンスラインは有効に機能しているか。

独立性、専門性、監査資源の十分性の観点から、内部監査部門は有効に機能し、その監査品質は監査責任役員及び会計監査人が依拠できるレベルか。

●IIA（内部監査人協会）の新三線モデル

- ・内部監査部門はマネジメントと対等な協同関係にあり、ガバナンス機関から指揮命令を受けて、報告義務を負うという、内部監査人への期待を示したものである。

●内部監査の成熟度モデル

- ・準拠性の検証者としての Ver.1.0 から、信頼されるビジネスアドバイザーとなる Ver.4.0 までの内部監査の成熟度モデルである。
- ・準拠性監査は基本中の基本で、Ver.1.0 ができた上での Ver.4.0 であることは言うまでもない。

●三様監査の高度化

- ・健全な懐疑心を共通して持ちながら、監査責任役員、会計監査人による法定監査と、内部監査人による任意監査を行うことが三様監査の姿である。
- ・会計監査人の独立性・専門性、内部監査部門の独立性・専門性、監査責任役員の監査リテラシーとビジネスリテラシーをベースとして、監査責任役員のリーダーシップによるプロフェッショナル・パートナーシップを発揮して、三様監査を高度化していくことが期待される。

●留意すべき経営リスクと監査フロンティア

- ・留意すべき経営リスクと監査フロンティアには、以下のようなものが考えられる。

企業風土・文化の劣化

マルチステークホルダー間の調整不全

資本コスト概念の不在（PBR1 倍割れ問題）

非財務情報の取扱いの軽視（ESG/SDGs への対応遅れ等）

IT ガバナンスの未成熟（取締役会の課題認識）
サイバーセキュリティ・リスクへの対応遅れ
AI リスクへの準備不足

3. 財務情報と非財務情報（記述情報、サステナビリティ情報、将来情報）

●財務情報と非財務情報

・経済的価値に関する将来情報、及び社会的価値に関する過去情報と将来情報のような非財務情報を将来財務情報と呼び変えて共有する必要がある。

●ESG と SDGs の異同

・ESG は、各企業がそれぞれの要素を財務状況等に対して、将来的にどのような影響を与えるかを分析し戦略に落とし込み、説明責任を果たすべきという（機関）投資家側の視点である。

・SDGs は、2030 年までに貧困撲滅、地球保護、全ての人々が平和と繁栄を享受できるようにするための企業側の責任を示すもの。イノベーション、科学技術とそれらを支える資金確保を前提に、マルチステークホルダー間のパートナーシップによる社会課題の解決を目指している。

・この SDGs の立ち位置が、監査責任役員、内部監査人に求められている。

●市場価値に占める無形資産（Intangible Assets）の割合

・将来的に価値を産み出す蓋然性が高い非財務情報の占める割合が、日本は欧米等に比べて低く、ガバナンス改革の必要性がある。

●適切な情報開示と透明性の確保

・上場会社は、経営戦略の開示に当たって、自社のサステナビリティについての取組みを適切に開示すべきである。また、人的資本や知的財産への投資等についても、自社の経営戦略・経営課題との整合性を意識しつつ分かりやすく具体的に情報を開示・提供すべきである。

・気候変動に係るリスク及び収益機会が自社の事業活動や収益等に与える影響について、必要なデータの収集と分析を行い、国際的に確立された開示の枠組みである TCFD（気候関連財務情報開示タスクフォース）またはそれと同等の枠組みに基づく開示の質と量の充実を進めるべきである。

●PBR 1 倍割れ問題：リスクとコントロールの観点から

・PBR 1 倍割れは、資本コストを上回る資本収益性を達成できていない、あるいは、成長性が投資者から十分に評価されていないことが示唆される 1 つの目安と考えられる。

・計画に基づき、資本コストや株価を意識した経営を推進するとともに、株主との対話に関するコーポレートガバナンス・コードの原則を踏まえつつ、開示をベースとして、海外投資家を含む投資者との積極的な対話を実施していくことが期待される。

・これまでの取組みや成果の状況に関する分析を行ったうえで、将来の成長ストーリーをしっかりと説明していく必要がある。

●将来情報に対するセーフハーバー・ルール

・説明を記載するに当たっては、例えば、当該将来情報について社内で合理的な根拠に基づく適切な検討を経たものである場合には、その旨を、検討された内容（例えば、当該将来情報を記載するに当たり前提とさ

れた事実、仮定及び推論過程)の概要とともに記載することが考えられる。

- ・将来情報が根拠ある情報として取締役会で議論されて、考えぬいた結果として公表されたものであるか、内部監査人によるモニタリングが期待される。
- 将来情報の記述と虚偽記載の責任及び任意開示書類の参照に対する意見
 - ・「企業内容等の開示に関する留意事項」において、将来情報を含む非財務情報の適切性や虚偽記載リスクに対する考え方が具体的に示されたことは、ガイドラインとして歓迎したい。
 - ・これを受けて各社は、虚偽記載リスクの増加を抑えるための統制活動を高度化し、かつプロセス自体を積極的に開示すべきである。例えば執行側の責任として、非財務情報の生成から開示に至るプロセスについて、ガイドラインが求める経営者の認識、前提、仮定等の合理性を織り込んでもらいたい。
 - ・また取締役会等ガバナンス機関の責任として、このプロセスに対する規律付けが役割として期待される。
 - ・開示ガイドラインはより詳細な情報の参照先として、統合報告書等を示しているが、各社は当然にこれら任意開示書類の信頼性の担保に対しても、従前に増して留意すべきである。
- 小括
 - ・COSO-ERMは、リスクとコントロール（内部統制）あるところ、全ての領域を監査領域として示唆する。
 - ・ERMを、パーパスを入力とし、価値創造を出力とするバリューチェーンとして見直すことにより、監査領域の広がりを確認できる。
 - ・広がる監査領域に対して、三様監査の実効性確保は必須である。
 - ・三様監査を監査責任役員のリーダーシップによるプロフェッショナル・パートナーシップとして再定義する。
 - ・非財務情報の開示充実は、PBR1倍割れ問題等今日的課題と密接不可分である。
 - ・内閣府令改正や内部統制報告制度改訂の内容を精査することで、新たなリスクに対するコントロール内部統制構築の方向性と監査スコープの広がりが見えてくる。

【所感】

リスクとコントロールと監査、監査責任役員によるプロフェッショナル・パートナーシップとしての三様監査、財務情報と将来財務情報について理解ができ、また将来情報の開示の充実に寄与するシステム監査への今後の大きな期待も理解でき、大変参考になった。

以上

<目次>

支部報告 【 北海道支部 2024 年度 1 月の月例研究会 】

会員番号 1448 宮崎雅年 (北海道支部)

北海道支部では、以下のとおり 2024 年度 1 月の月例研究会を開催しました。

- ・日時：2024 年 1 月 12 日 (金) 18:30～20:30 参加者：3 名
- ・会場：札幌市男女共同参画センター 研修室 2 (札幌市)
- ・演題：『「情報セキュリティ白書 2023」を読んで』
- ・講師：北海道支部長 宮崎 雅年 氏

<講演概要>

IPA (情報処理推進機構) では、「情報セキュリティ白書」を 2008 年から毎年発行しており、昨年で 16 冊目を数える。この白書は、前年度の情報セキュリティの概況に始まり、情報セキュリティに関する国内外の政策や脅威の動向、インシデントの発生状況、被害実態など定番トピックのほか、毎年タイムリーなトピックを新たに取り上げている。

この白書には、情報セキュリティに関する国内外の官民の各種データおよび資料を数多く紹介しており、情報の網羅性と参照性の高さが特徴であり、自身の研鑽だけでなく、教育・研修の資料作りにも参考となるもので、講師は 2012 年から毎年購入している。(全文 PDF 版は、IPA の Web サイトから無償ダウンロード可能)

最新刊の「情報セキュリティ白書 2023」では新たなトピックとして、下記をとりあげている。

- ・国内では、ランサムウェア攻撃による大きな被害が報告された
- ・政策面では、「サイバーセキュリティ 2022」「重要インフラのサイバーセキュリティに係る行動計画」「国家安全保障戦略」等が公表された
- ・AI、特に生成系 AI に注目が集まった年であった。ウクライナ侵攻では、虚偽情報生成に AI が用され、情報の信頼性に対する課題が深刻化した

なお、本発表の内容は講師の個人的意見であり、講師が所属する企業・団体の意見を代弁するものではない。

<講演内容>**1. 2022 年度の情報セキュリティの概況**

2022 年度に起きた情報セキュリティインシデント・事件として、CISA がロシアのウクライナに対するサイバー攻撃情報を開示したこと、地方自治体の業務委託先が個人情報を保管した USB メモリを紛失したこと、イタリアの地方行政機関がランサムウェア攻撃でサービスを停止したこと、ENISA がランサムウェア脅威実態を報告したこと、親ロシア系攻撃集団が国内組織に DDoS 攻撃をしたこと、家具製造小売の持ち株会社が不正アクセスを受けて約 132,000 アカウント分の個人情報が流出したこと、大阪府の病院にランサムウェア攻撃があって電子カルテシステムに障害が発生したこと、入力フォーム支援サービス事業者のサービスが不正アクセスを受けて入力情報が流出したこと、IPA が学術関係者・シンクタンク研究員等を標的とし

たサイバー攻撃について注意喚起したこと、厚生労働省が医療機関等のサイバーセキュリティ対策で注意喚起したこと、オーストラリアの保険会社の個人情報 970 万人が漏えいしたこと、フランスの病院がランサムウェア攻撃により患者を緊急移送したこと、保険会社の委託先に不正アクセスされて顧客情報が流出したこと、米国ソーシャルテクノロジー企業に GDPR 違反で 3 億 9 千万ユーロの制裁金を科せられたこと、IPA が Emotet の攻撃活動再開を観測したこと、などが挙げられる。

また、情報セキュリティ政策・イベントとして、IPA が「組織における内部不正防止ガイドライン」第 5 版を公開したこと、警察庁にサイバー警察局、関東管区警察庁にサイバー特別捜査隊を新設したこと、「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律案」が成立したこと、第 28 回日 EU 定期首脳協議が開催されてデジタルパートナーシップ合意したこと、G7 エルマウサミットが開催されたこと、「デジタル社会の実現に向けた重点計画」が閣議決定されたこと、NISC が「重要インフラのサイバーセキュリティに係る行動計画」を公開したこと、総務省が「ICT サイバーセキュリティ総合対策 2022」を公開したこと、IPA がビジネスメール詐欺の特設ページを開設したこと、EU がデジタル製品の「サイバーレジリエンス法案」を公開したこと、ISMAP-LIU が運用を開始したこと、米国が「AI 権利章典」を公開したこと、経済産業省が「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」を公開したこと、EU の重要インフラの統一セキュリティ規格「NIS 2」が成立したこと、EU が AI 法修正案を公開したこと、安全保障関連 3 文書が閣議決定したこと、米国で国防授權法 2023 が成立したこと、経済産業省が「クレジットカード決済システムのセキュリティ対策強化検討会報告書」を公開したこと、日米豪印の 4 カ国（QUAD）で連携したサイバーセキュリティ月間を実施したこと、経済産業省が「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を公開したこと、IPA が「サイバーセキュリティ経営ガイドライン」を改訂したこと、米国が新サイバーセキュリティ戦略を公開したこと、などが挙げられる。

2. 情報セキュリティインシデント・脆弱性の現状と対策

2022 年度に世界で観測されたインシデントの発生状況では、ウクライナ情勢によるセキュリティインシデントの急増、フィッシングおよびランサムウェア、情報漏えいが挙げられる。

国内において注目される脅威として、Web サイト改ざん、フィッシングおよびランサムウェアによる被害が挙げられる。

3. 情報セキュリティインシデント、手口、対策

ランサムウェア攻撃では被害件数が増加傾向を継続しており、その要因としてランサムウェアをサービスとして提供する「RaaS (Ransomware as a Service)」と呼ばれる攻撃モデルの普及や、攻撃者の組織化・分業化が挙げられる。セキュリティベンダーの調査によると、被害組織は製造業や医療等の様々な業種や公共機関で被害が確認されている。

特に、トヨタ自動車株式会社は、取引先が侵入型ランサムウェア攻撃を受けたことから、国内全 14 工場 28 ラインの稼働を停止すると 2022 年 3 月 1 に発表した。

医療機関における被害事例として、侵入型ランサムウェア攻撃により、大阪市の地方独立行政法人大阪府立病院機構大阪急性期・総合医療センターの電子カルテシステムに被害が発生したことが挙げられる。

侵入型ランサムウェア攻撃の手口は、ネットワークへの初期侵入、ネットワーク内の侵入範囲拡大、データ窃取、データの暗号化・システム停止、窃取したデータの公開というステップで行われ、顧客への DDoS 攻撃、顧客や利害関係者への連絡が近年確認されている手口である。

侵入型ランサムウェア攻撃への対策として、バックアップの取得が復旧計画が挙げられるが、バックアップを取得するだけでなく、リストアのテストを行う等して、バックアップからの復旧が可能なことを確認しておくことが重要である。

標的型攻撃はメールにおける騙しの手口と添付ファイルの手口がある。添付ファイルの手口は Microsoft Office の脆弱性やマクロ機能を悪用する手口のほか、オンラインストレージサービスを悪用する手口がある。

標的型攻撃への対策は、利用者向けの対策として不審メールに対する注意力の向上、オンラインストレージサービスを悪用した手口の周知、マクロ機能の危険性の周知、ウイルス感染を想定した訓練と教育のほか、システムによる技術的な対策として不審メールを確保できる仕組みの確立、適切な修正プログラムの適用、ホワイトリスト化やブラックリスト化によるファイルの実行防止がある。

ビジネスメール詐欺では、「日本語化」された CEO を詐称する攻撃が現れている。

ビジネスメール詐欺への対策は、周知徹底と情報共有のほか、電子署名によるなりすまし防止、送金処理のチェック体制強化、類似ドメインへの対策等がある。

DDoS 攻撃を行うボットネットが増加しており、サービスおよびソフトウェアの脆弱性を悪用されたり、ウイルス感染させられたコンピュータのほか、ルータおよび IoT 機器を攻撃対象とした手法も取り入れられている。

DDoS 攻撃の被害に遭った場合の対策は、アクセスログや通信ログ等の確認、想定外の IP アドレスからのアクセスを遮断、監視の継続があり、攻撃に加担しないための対策は、OS やファームウェアを最新の状態に維持、パスワードを初期値から変更、組織内から外向けの通信の監視がある。

Microsoft 製品などソフトウェアの脆弱性を悪用した攻撃が報告されている。

特に VPN 製品の脆弱性を対象として攻撃が続いている。VPN 製品に限らず、ソフトウェアの脆弱性に対して迅速な対応が求められる。

ばらまき型メールへの対策は、一般利用者における対策としてセキュリティソフトの導入、不用意にメールや添付ファイル内の指示に従わない、OS やソフトウェアのバージョンを常に最新に保つ、Word ファイルや Excel ファイルを開いたときにマクロを有効化しない、組織・企業における対策として不審なメールを受信した際の報告窓口を設ける、ウイルス感染を想定した利用者の訓練と教育を行う、不審なメールを確保できる仕組みの確立、適切な修正プログラムの適用、特定のファイル形式について実行許可・禁止の設定、公開されているばらまき型メールに関する注意喚起情報を組織内で共有がある。

4. 情報セキュリティを支える基盤の動向

国内の情報セキュリティ政策は、政府全体として「サイバーセキュリティ戦略」の見直し、重要インフラの情報セキュリティ対策強化があり、経済産業省として産業サイバーセキュリティ研究会、政府情報システムのためのセキュリティ評価制度（ISMAP）、J-CSIP（サイバー情報共有イニシアティブ）がある。

警察庁では、2022年4月に「警察におけるサイバー戦略」を改定し、組織基盤の更なる強化および人材育成の取り組みが行われた。

国外の情報セキュリティ政策の状況は、国際社会と連携した取り組みがあり、日米のサイバー連携のほか、EU 諸国および ASEAN 諸国とのサイバー連携がある。

セキュリティ人材の不足という認識から情報セキュリティ人材の育成として、経済産業省および関係省庁等の取り組みがあり、産業サイバーセキュリティセンターによる中核人材育成プログラムのほか、情報セキュリティ人材育成のための国家試験および国家資格として情報セキュリティマネジメント試験、情報処理安全確保支援士制度がある。

制御システムの情報セキュリティのほか、IoT の情報セキュリティの重要性が高まっている。特に IoT の情報セキュリティ対策強化の取り組みとして、IoT 関連セキュリティガイド等の改訂・新規発行、IoT 機器に対する規制の強化がある。

5. 制御システムの情報セキュリティ

制御システムは、電力、ガス、水道、輸送・物流、製造ライン等、我々の生活を支える重要インフラを管理し、制御するシステムである。制御システムのインシデントは増加の傾向にある。かつて制御システムはインターネットに接続していないからサイバー攻撃と無縁とされていたが、外部から持ち込まれる情報端末・機器や媒体に対する正確なセキュリティポリシーを確立し、管理策を策定し、継続的に取り組むことが重要である。

6. IoT の情報セキュリティ

IoT (Internet of Things) 技術の普及とともに、セキュリティ設定が不十分なまま、あるいは脆弱性を有したままインターネットに接続されたコンピュータ以外の機器 (IoT 機器) が増大することにより、サイバー攻撃の対象となる脅威が拡大傾向にある。

7. クラウドの情報セキュリティ

クラウドサービスの利用は増加傾向にあるが、利用者および委託先の設定ミスに起因するインシデントが多数発生している。

8. 最後に

ウイルス対策ソフトおよびソフトウェアを最新の状態に維持するだけでは不十分だが、個人や小規模事業者にそれ以上の技術的な対策を求めるのは過大な要求でしょう。しかし、最新のセキュリティ動向の情報を共有することで、先行する類似の事例を回避することは可能でしょう。

限られた誌面の中ですべてを紹介するのは困難であるので、IPA の Web サイトから本書を無償ダウンロードしてご一読いただけると幸いです。

「IT ガバナンス監査研修の実現に向けて」

— (第2回) IT ガバナンス監査研修の設計と実施結果 —

会員番号 中部支部 IT ガバナンス監査演習 WG

(第1回から続く)

8. 研修の設計に向けての提案

図表-6 演習の振り返りによる研修の設計に向けての提案

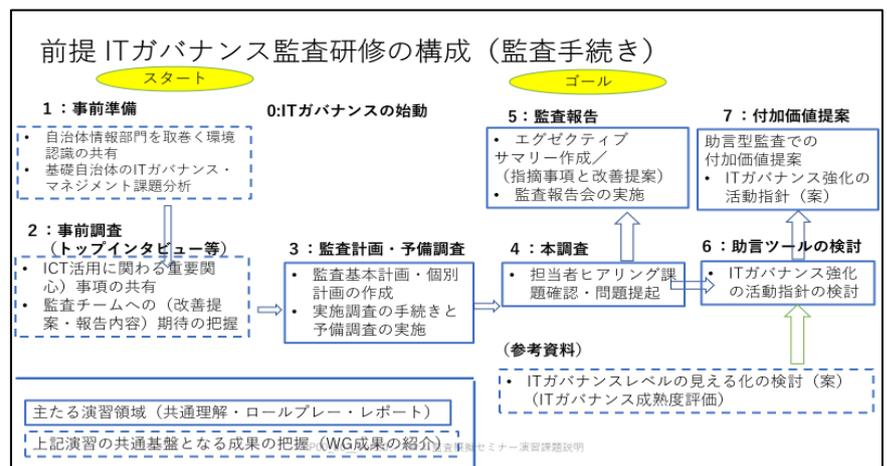
項目	提案
①事前の座学が必要	<ul style="list-style-type: none"> 自治体と自治体におけるITガバナンス'マネジメント課題の現状理解のため、基礎知識の提供が必要。 基礎知識に関する資料は学習のポイントを明確化し、必須のものに絞り、参加者の負担を軽減する。
②集合研修の内容	<ul style="list-style-type: none"> 集合研修の冒頭で、オンラインコンテンツに基づく自習の理解が、監査に向けて準備できているか、宿題で確認する。 インタビュー・ヒアリングの体験は重要で、かつ貴重な機会となることから、論点を絞って演習する。 模範解答の提示による学習も考慮し、演習結果を模範解答として活用する。 研修では個別監査計画「企画・事後評価」に監査テーマを絞込む。 ITガバナンス監査の成果物として、エグゼクティブサマリー・監査報告は重要で、ロールプレーを組み込むことで、研修の緊張感が生まれる。但し、サマリーの項目(見出し)はあらかじめ与え、報告が拡散しないよう留意する。
③研修の目標	<ul style="list-style-type: none"> ITガバナンス監査を理解しようとして、従来のシステム監査をベースにすると混乱するので、ITガバナンス監査・助言型監査を前提として明示する。 この手順でやれば一応ITガバナンス監査ができそうという感想が到達目標か。参加者に持ち帰ってもらう目標の明確化、ブレイクダウンが必要。
④研修の運営	<ul style="list-style-type: none"> 監査チームがディスカッションに割ける時間を最大限確保することが好ましい、また監査チームの構成によって、研修の進め方もバリエーションが生まれる。 チーム作業で、チーム内のコミュニケーションを活性化する。 監査(研修)チームには、サポーターが参加し、方向性を大きく逸脱しない様導く必要がある。 研修参加者には、監査チームの役のみとし、被監査組織はWGメンバーが演ずる。 集合研修の時間は2日が目安である。 研修参加者には監査未経験者を含めてほしい。

9. 研修(トライアル版)の準備作業

(ア) 研修の設計

図表-7 IT ガバナンス監査研修の構成

演習の振り返りをもとに、図表-7 に示す IT ガバナンス監査研修の構成とした。監査研修の流れで、ほぼ一直線でワークとして進められる監査手続き部分は、その手続きを理解するという趣旨で、監査演習の成果品をフォローすることとし、集合研修に先立つ事前演習の自習範囲とした。(ステップ1、2、3の前半)



集合研修では、グループ作業を重視し、予備調査の後半から本調査を中心にロールプレーを含めて体験してもらうことにした。(ステップ3の後半、4、5) また、助言型監査として行う IT ガバナンス成熟度の評価や IT ガバナンス強化の活動の指針については、通常システム監査手順には含まれないことから、助言型監査における付加価値提案として位置づけ、助言ツールの適用の在り方について、講義と一部演習によって進めることとした。(ステップ6、7)

(イ)研修（トライアル版）の準備作業

図表—8 研修（トライアル版）の準備作業の経過

項番	日付	実施内容（すべてオンラインでの会合）	備考
1	2023.03.25	支部研究会にてITガバナンス監査研修（トライアル版）の構想説明	
2	2023.04.23	①SAAJ全体におけるITガバナンス監査研修（トライアル版）の位置付け ②ITガバナンス監査研修（トライアル版）の説明と意見交換	
3	2023.05.20	①ITガバナンス監査研修（トライアル版）の確認 ②フェーズごとの研修教材の確認/見直し フェーズ0：ITガバナンス監査の始動 ITガバナンス監査支援依頼 フェーズ1：事前準備（1） 被監査組織を取り巻く環境	研修教材については、監査演習でのインプット・アウトプットの多くの成果品を流用する。
4	2023.06.03	①フェーズごとの研修教材の確認/見直し フェーズ1：事前準備（1）に関する資料の検討 被監査組織・監査委員監査の基礎知識のレビューと資料の縮約	演習のオリエンテーションで使用した資料をベースに事前準備（予備知識の修得）の資料を一旦編集したが、研修の目的と研修の期間さらには研修参加者が事前準備に割ける時間を考慮し、資料を「被監査組織・監査委員監査の基礎知識」としてレビューし縮約した。
5	2023.06.24	①ITガバナンス監査研修（トライアル版）の概要説明 ②フェーズごとの研修教材の確認/見直し フェーズ1：事前準備（1）に関する資料の見直し結果 フェーズ2：事前調査 重要関心事項と監査の論点整理	演習では事前調査の方法として、ITガバナンスレベルチェックシートの提案を行ったが、演習の監査チームの意見を反映して、チェックシートに代わる代替案を検討した。検討の結果、「重要関心事項と監査項目・監査要点」と「監査項目・監査要点とヒアリング（本調査）の論点」の二段階の整理によって、事前調査を完了することとした。
6	2023.07.16	①フェーズごとの研修教材の確認/見直し フェーズ3：監査計画・予備調査 フェーズ4：本調査（前半）	
7	2023.08.20	①フェーズごとの研修教材の確認/見直し フェーズ4：本調査 フェーズ5：監査報告 エグゼクティブサマリーの編集	監査演習のアウトプットである監査報告書（案）をもとに、研修時に行うトップへのエグゼクティブサマリーの様式について、改めて検討し、監査結果の報告とマネジメント層への助言・提言にとどまらず、監査結果を踏まえたガバナンス層への助言・提言を含めることとした。
8	2023.09.17	①ITガバナンス監査研修（トライアル版）の実施計画（支部研究会報告） ②フェーズごとの研修教材の確認/見直し フェーズ6：助言ツールの検討 フェーズ7：付加価値提案 ITガバナンス成熟度自己点検シートのレビューと意見交換	演習ではITガバナンス成熟度自己点検シート（案）を提案していたが、レビューは十分ではなかった。研修資料として整備するにあたって、WGメンバーがもう一度レビューし直し、内容について質疑を重ね、現実解としての妥当性を検証し、成案を得ることができた。
9	2023.10.15	①ITガバナンス監査研修（トライアル版）の実施スケジュール確定 ②研修教材の確認/見直し（最終） シナリオファイルとナレーションファイルの整備	研修資料の利用の流れ（シナリオファイル）と研修資料の解説（ナレーション付ファイル）を整備し、これをもとにWG1メンバーが研修時に欠けても、残りのメンバーで対応できるよう事業継続性を高めた。研修参加者はシナリオファイルを開きスライドショーの指示に従って研修を進めることができる。また研修資料で解説が必要な資料ではPPTのナレーション付ファイルを自動再生もしくは動画再生することで、内容の理解を深めることができるものとした。

10. ITガバナンス監査研修（トライアル版）の実施報告

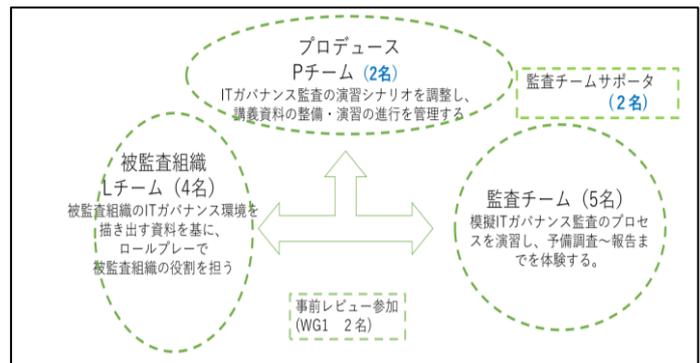
トライアルであることから、参加者を支部内に留め、他支部の参加を控え、ミニマムの体制で実施した。支部会員の絶対数が少なく、高齢化していることから、新たな取組にどの程度参加が得られるか危惧していたが、幸い若手を含む5名の研修参加者を得て実施することが出来た。

(ア)ITガバナンス監査研修の体制

図表—9 ITガバナンス監査研修の体制

研修の体制は、図表—9の通りで、研修参加者（監査チーム）のプロフィールは、研究部門、民間企業の経営企画部門、内部監査部門、BCPやセキュリティのコンサルタント部門に在職者であった。

研修運営には、WG1から、Pチーム2名、Lチーム4名、監査チームサポータ2名が参加した。



(イ)研修のスケジュール 図表—1 0 研修スケジュール（オンライン研修期間：2023.11.05～11.29）

項番	フェーズ	研修用資料	所用時間
—	キックオフ	<ul style="list-style-type: none"> 研修スケジュール、配信コンテンツの利用方法、用語解説 ケース及び演習課題の概要 システム監査基準・システム管理基準のポイント 	1時間
0	ITガバナンス監査の始動	<ul style="list-style-type: none"> システム監査業務支援依頼書と依頼者意向確認（議事録） 監査チームキックオフミーティング（議事録） 	自習 1時間半
1	事前準備	<ul style="list-style-type: none"> 被監査組織に関する基礎知識とわたしたちの市情報システム概要 情報システム調達指針 自治体における監査委員監査 	
2	事前調査	<ul style="list-style-type: none"> 重要関心事項に関する調査報告（抄録）とトップインタビュー議事録（演習結果） 監査チームミーティング1（議事録）（演習結果） 監査基本計画/監査個別計画書（企画・事後評価）と現状調査表（模範解答） 自治体のITガバナンス課題 重要関心事項と監査項目・監査要点 	自習 1時間半
3	予備調査（1）	<ul style="list-style-type: none"> 企画事前・事後評価に関わる統制の状況に関する精読資料とレビューシート（複数）（調達マニュアル、IT調達計画書等） 調達マニュアル運用状況調査結果（抄録）と調達マニュアルにかかわるアンケート調査結果 調達ガイドライン比較表（他市との内容比較） 宿題：当市の課題・問題点（記入用紙）→研修当日までに事前提出 	

注)演習結果：研修資料としてWG1の演習結果を活用した部分

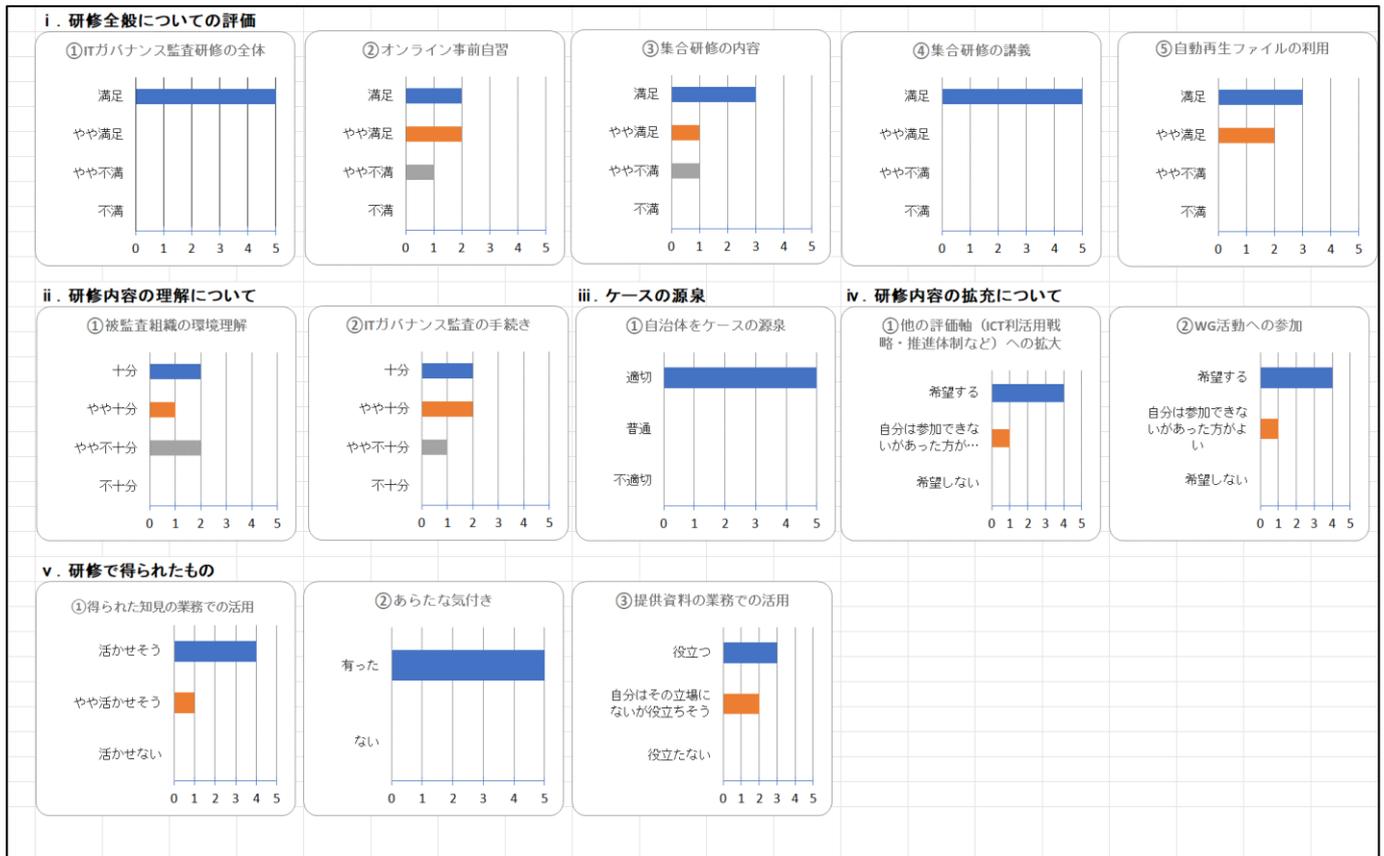
図表—1 1 研修スケジュール（集合研修：2023.12.2～12.3）

項番	フェーズ	研修用資料	所用時間
3	予備調査（2）	<ul style="list-style-type: none"> 宿題:企画・事後評価における主なコントロールは何ですか？ ——宿題結果の講評—— 監査項目・監査要点とヒアリングの論点（演習シート） ——演習：論点整理と発表—— 監査項目・監査要点とヒアリングの論点（模範解答） ヒアリングの基礎（解説） 調達マニュアルに関するヒアリング調書（記入様式） ——演習：ヒアリング調書の整備—— 	2時間半
4	本調査	<ul style="list-style-type: none"> 調達マニュアルの運用状況に関するヒアリング対応（想定回答：被監査組織の担当役用） ヒアリングの想定回答の趣旨（被監査組織の担当役用） ——演習：ヒアリングと調書の作成—— 調達マニュアルに関するヒアリング調書（模範解答） 	2時間
5	監査報告	<ul style="list-style-type: none"> 監査結果報告書（案）（演習結果） エグゼクティブサマリー様式例示（演習用の様式） ——演習：エグゼクティブサマリー作成と監査報告—— 監査報告のポイント、及びエグゼクティブサマリー（模範解答） 	3時間
6	助言ツールの検討	<ul style="list-style-type: none"> ITガバナンス成熟度評価自己点検シート（案）（企画・事後評価の分野） ——演習：自己点検シート（案）の適用—— ITガバナンス成熟度評価自己点検シート（他自治体との水準比較） 	45分
7	付加価値提案	<ul style="list-style-type: none"> エグゼクティブサマリー（模範解答：付加価値提案付き） IT調達計画書・評価書レビューシート（適用結果） 	45分
8	研修参加者への情報提供	<ul style="list-style-type: none"> ITガバナンス監査報告（エグゼクティブサマリー：本研修コースが指すもの） ITガバナンス成熟度評価 自己点検シート（全6分野）（案）と各種レビューシート（案） 	15分

(ウ)研修参加者のアンケート調査結果

● 集計結果

図表—12 研修参加者のアンケート結果



● アンケートの各項目についてのコメントの要約

図表—13 研修参加者の評価のコメント

i. 全般的評価	
① 研修の内容	新しい試みであるにもかかわらず、実践的な監査プロセスを体験でき満足しました。
② オンラインによる事前の自習の進め方	自主学習の方法に満足であるという一方で、オンラインの集合研修の希望が半数有った。
③ 集合研修の演習の進め方	演習の構成には満足であったが、演習のグループワークの時間が足りなく消化不良の声もあった。
④ 集合研修の講義内容	興味深い内容、ポイントがわかりやすいなど、全員が満足の解答であった。
⑤ シナリオファイル・ナレーション付き自動再生ファイル (注)	満足の解答が多かったか、テンポが単調で、再生時間に拘束されるなど、改善の指摘があった。 (注) 講義の資料にはナレーション付き自動再生ファイルを提供し、講義の自動化を図った。
ii. 研修内容の理解について	
① 被監査組織を取巻く環境の理解	事前学習では十分ではなかったが、集合研修の講義・演習で理解が進んだとの意見が多かった。
② ITガバナンス監査手続きの理解	理解が進んだという意見の一方、残念ながら消化不良という意見もあった。
iii. ケースの源泉	
① ケース選択の妥当性	自治体をケースの源泉としたことについて、理解が示された。
iv. 研修内容の拡充	
① 監査研修の対象範囲の拡大	「ICT活用戦略・推進体制」や「人材育成」の監査テーマへの拡充について希望が確認された。 (今回は個別監査テーマ「企画・事後評価」で実施)
② WG1の活動への参加	WG1の継続とともに、5名中4名がWG活動への参加意思を示された。

以下第3回に続く

<目次>

注目情報 (2024.1~2024.2)**■IPA「情報セキュリティ10大脅威 2024」**

IPA（情報処理推進機構）は2024年1月24日、「情報セキュリティ10大脅威 2024」を発表した。

「情報セキュリティ10大脅威 2024」は、2023年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約200名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものである。

10大脅威 2024では、個人の10大脅威の順位は掲載せず、五十音順で並べている。これは、順位が高い脅威から優先的に対応し、下位の脅威への対策が疎かになることを懸念してのことである。

<https://www.ipa.go.jp/security/10threats/10threats2024.html>

■警察庁「ランサムウェアによる暗号化被害データに関する復号ツールの開発について」

警察庁は2024年2月21日、ランサムウェア LockBit によって暗号化されたデータを復号するツールを開発したと発表した。

1. LockBit 被害データ復号ツールの概要等

関東管区警察局サイバー特別捜査隊において、ランサムウェア LockBit によって暗号化された被害データを復号するツールを開発し、2023年12月、警察庁サイバー警察局からユーロポールに提供した。ユーロポールでは、世界中の被害企業等の被害回復が可能となるよう、2024年2月、日本警察が開発した復号ツールとして情報発信し、その活用を促すことを発表した。

この度の情報発信については、日本警察とユーロポールにおいて、この復号ツールの有意性が実証され、ランサムウェア対策を世界規模で進める観点から実施することとしたものである。

なお、関東管区警察局サイバー特別捜査隊では、リバースエンジニアリング解析に基づき、数ヶ月以上の期間を費やして、ランサムウェア LockBit の暗号化の仕組みを分析し、復号ツールを開発した。

2. 日本警察の今後の対応

日本国内の被害企業等に対して、最寄りの警察署への相談を促すと共に、相談があった場合には、その求めに応じ、復号ツールを活用して被害回復作業を実施することとしている。

<https://www.npa.go.jp/news/release/2024/20240214002.html>

[<目次>](#)

【 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 285 回	日時	2024年3月11日（月） 18:30～20:30
	場所	オンライン（Zoom ウェビナー）
	テーマ	IT ガバナンスのアセスメント規格（JIS Q 38503）について
	講師	日本システム監査人協会 会長 松枝憲司（まつえだ けんじ）氏 理事・IT アセスメント研究会主査 松尾正行（まつお まさゆき）氏
	講演骨子	ISO/IEC 38503-2022（Assessment of the governance of IT）は ISO/IEC 38500 シリーズ規格のうち唯一のアセスメント規格として 2022 年 1 月発行された。これを受けてわが国では JIS Q 38503（IT ガバナンスのアセスメント）として発行予定である。 この規格は日本の提案に基づき、ISO で開発を進めたものである。ISO プロジェクトの Co-Editor 及び JIS 化委員会の幹事を務めた経験を踏まえ、IT ガバナンスのアセスメントの原則ベースモデルとフレームワーク、アセスメントの手法と成熟度判定、他規格との関連、今後の動向などを解説する。
	参加費	SAAJ 会員 1,000 円 非会員 3,000 円
お申込み	https://www.saa.or.jp/kenkyu/kenkyu/285.html	

■ SAAJ 月例研究会（東京）		
第 286 回	日時	2024年4月22日(月) 18:30～20:30
	場所	オンライン（Zoom ウェビナー）
	テーマ	グローバルな越境移転ツール（CBPR 認証制度）について
	講師	(一財)日本情報経済社会推進協会 認定個人情報保護団体事務局 事務局長 奥原早苗（おくはら さなえ）氏
	講演骨子	令和 5 年 6 月に、第 3 回 G7 データ保護・プライバシー機関ラウンドテーブル会合が開催され、個人情報保護委員会の Web サイトでは、議論された内容が公開されています。そのうち、「行動計画」では、移転ツールの今後についても触れられており、グローバル規模で安全に情報をやりとりする手段として注目が高まっています。国内でしか製品・サービスを展開していないので、「越境データ」や「移転ツール」などは無縁だなど思っているのではありませんか？ APEC CBPR 認証システムの審査機関 JIPDEC より、グローバルな越境移転ツールの概要を紹介させていただきます。
	参加費	SAAJ 会員 1,000 円 非会員 3,000 円
お申込み	https://www.saa.or.jp/kenkyu/kenkyu/286.html	

<目次>

協会からのお知らせ 【2024 年度春期 公認システム監査人及びシステム監査人補の募集】

2024 年度春期 公認システム監査人及びシステム監査人補の募集の〔公告〕が協会のホームページに掲載されています。資格取得を企図されている各位はご参照願います。〔公告〕の概略は下記の通りですが、申請書等の資料のダウンロードなども、ホームページからお願い致します。

(<https://www.saaj.or.jp/csa/csaboshu/csaboshu.html>)

[補足]

システム監査技術者試験の合格者以外でも、従来から情報セキュリティその他の高度情報処理技術者試験合格者、中小企業診断士、公認会計士、技術士、ITC、CISA、ISMS/プライバシーマーク主任審査員などの各位も、「特別認定講習」を修了することでシステム監査人補の認定申請が出来ました。2017年からこれに加え、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、公認情報セキュリティ監査人が、「特別認定講習」を修了することでシステム監査人補の認定申請が出来るようになりました。さらに2023年12月に特別認定制度を改定し、PMI (Project Management Institute) が認定するプロジェクトマネジメントの資格「PMP (Project Management Professional) 」を加えました。また、申請前直近6年間のシステム監査実務経験（実務経験みなし期間）が2年以上あれば、公認システム監査人の認定申請が出来ます。（<https://www.saaj.or.jp/csa/csaboshu/620301CSAASAbosyuyoko.pdf>）

----- 記 -----

2024 年 2 月 1 日

認定特定非営利活動法人日本システム監査人協会

公認システム監査人認定委員会

2024 年度春期**公認システム監査人及びシステム監査人補の募集について****〔公告〕**

認定特定非営利活動法人日本システム監査人協会（以下、協会という）は、公認システム監査人認定制度（2002 年 2 月 25 日制定）（以下、制度という）に基づき、「公認システム監査人(Certified Systems Auditor : CSA)」および「システム監査人補(Associate Systems Auditor : ASA)」を認定するため、2024 年度春期公認システム監査人およびシステム監査人補の募集を行います。募集の概要と申請書等の資料の入手方法は、以下のとおりです。

1. 認定資格

公認システム監査人およびシステム監査人補とする。

2. 申請条件

- (1) 認定申請者は、経済産業省が実施するシステム監査技術者（旧情報処理システム監査技術者）試験に合格していること。（制度 2（5）特別認定制度に基づく特別認定講習の修了により、上記試験の合格者と同様に取り扱う者を含む）
- (2) 公認システム監査人の申請者は、申請前直近 6 年間のシステム監査実務経験（実務経験みなし期間）が 2 年以上あること。

3. 認定申請

(1) 申請書類（記入方法は、募集要項参照）

公認システム監査人およびシステム監査人補の申請書類は、次表のとおりとする。

申請書類	公認システム監査人	システム監査人補	記事
(1)認定申請書	○	○	様式 1
(2)監査実務経歴書	○	—	様式 2
(3)小論文	○	—	様式 3
(4)宣誓書	○	○	様式 4
(5)資格証明（写）	○	○	
(6)申請手数料振込書（写）	○	○	
(7)面接試験	□	—	別途通知

（注 1） ○印の資料一式を申請書類として提出する。

（注 2） □印については、面接試験を実施する。

備考：公認システム監査人とシステム監査人補を同時申請する場合は、公認システム監査人用の申請書類を提出する。

(2) 面接試験

申請書類審査後、認定委員会が別途指定・通知する日時場所において、面接試験を受ける。

4. 募集期間

2024年2月1日（木）～2024年3月31日（日）（同日消印まで有効）

5. 認定申請手数料（消費税 10%を含む）

申請手数料	協会会員	非会員
(1) 公認システム監査人認定申請手数料 （注 1）システム監査人補と同時申請する場合も手数料は同じです。	22,000 円	33,000 円
(2) システム監査人補が申請する場合の公認システム監査人認定申請手数料	11,000 円	16,500 円
(3) システム監査人補認定申請手数料	11,000 円	16,500 円

6. 資料の入手方法

（<https://www.saaj.or.jp/csa/csaboshu/csaboshu.html>）から

【個人情報の取り扱いについて】 ⇒ 「同意する」 ボタンを押下

(1) 「公認システム監査人、システム監査人補 募集要項」

ダウンロード（PDF 形式）

(2) 申請書等様式一式

- ・ 認定申請書（様式 1）：Word 形式
- ・ 監査実務経歴書（様式 2）：Word 形式
- ・ 小論文（様式 3）：Word 形式
- ・ 宣誓書（様式 4）：Word 形式

(3) 公認システム監査人認定制度のダウンロード

- ・ PDF 形式

(4) 「公認システム監査人制度」創設のお知らせ（2002 年 7 月 1 日）のダウンロード

- ・ PDF 形式

(5) 特別認定講習に関する情報

（・特別認定講習機関認定については HP の当該 URL から参照）

以上
<目次>

【 新たに会員になられた方々へ 】

Welcome

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 <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>

特典

- ・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。

ぜひ
ご参加を

- ・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。

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

- ・「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>

セミナー

- ・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>

CSA
・
ASA

- ・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>

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。 <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。

【 SAAJ協会行事一覧 】		赤字：前回から変更された予定	2024.2
	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
2月	1：理事会：通常総会議案承認 29：2024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	
4月	11：理事会	初旬：春期CSA・ASA書類審査 中旬：春期ASA認定証発行 22：第286回月例研究会	21：春期情報処理技術者試験・ 情報処理安全確保支援士試験
5月	9：理事会	日程未定：第287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 11：理事会 19：年会費未納者督促状発送 22～：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 12：第288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 11：理事会	中旬：秋期CSA・ASA募集案内	12：支部会計報告〆切
前年度に実施した行事一覧			
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	
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（1/9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	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：総会開催予告揭示 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	上旬～中旬：秋期CSA面接 18：第283回月例研究会 下旬：CSA/ASA更新手続案内メール 〔更新申請期間1/1～1/31〕 下旬：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	9：支部会計報告提出期限

<目次>

【 会報編集部からのお知らせ 】

1. 会報テーマについて
2. 会報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」の募集は行っていません。

■ 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>

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

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

■□■ S A A J 会報担当

編集委員：竹原豊和、安部晃生、金田雅子、坂本誠、辻本要子、豊田諭、野嶽俊一、
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）

Copyright(C)1997-2024、認定 NPO 法人 日本システム監査人協会

<目次>