認定 NPO 法人
日本システム監査人協会報

2022 年 8 月号
No 257

No.257（2022 年 8 月号）<7 月 25 日発行>

今月号の注目記事
【 重要インフラ事業者の 社会的責任と利用者のリスク管理】

巻頭言

『CSA／ASA 制度発足 20 年における今後の期待』

会員番号：1750　舘岡　均（副会長　認定委員長）

相変わらずコロナ禍が続いている状況ですが、会員の皆様におかれましてはそれを乗り越えてご活躍のことと拝察しています。さて、今年は CSA／ASA 制度が発足して 20 年となり、リーマンショック、団塊の世代の退職、コロナ禍等々の難局がありましたが、皆様のご協力を得て当協会の重要な柱を維持しています。

CSA はペーパーライセンスでなく実務に応じられるシステム監査人として認定されています。そのようなことで、システム監査の実務あるいはその経験をビジネスに活用して実績を重ねて、順調に昇進、あるいはよりランクアップした転職、あるいは定年後の再就職に成功にした方々が多く見受けられ、流石に実力者揃いと実感しています。さらに当協会ホームページの『CSA レポート・体験記』では、その志高いご活躍に敬服しております。

CSA／ASA の活躍の場は、経営陣、内部監査部署（IT ガバナンス、IT 統制など）、情報システム部署、IT ベンダー営業部署（システム提案／超上流工程）／開発部署、さらには、審査機関、監査法人、教育機関、そして弁護士、公認会計士、政府・自治体職員／CIO 補佐官、各種評価委員など多岐に広がっています。情報セキュリティはシステム監査の重要な柱であり、CSA／ASA は情報セキュリティ監査、ISMAP、CSIRT 等々に関連する場でも活躍しています。また、クラウド、IoT、DX、AI 等々のように、専門的な技術の高度化、利用範囲の広がりでシステムが複雑化しており、俯瞰的な視点でのシステム監査が必要となっており、ますます活躍の場は広がっています。このように、CSA は経験を積んだ実力ある監査人として、様々な方面から信頼されています。CSA／ASA 制度発足 20 年の節目に 2022 年度秋期の CSA／ASA 募集（期間　8 月 1 日から 9 月 3 0 日）があり、会員の皆様には身近において CSA／ASA にふさわしい方々に資格を勧奨して下さいますようお願いいたします。多くの方々が応募され、認定され、コロナ禍下での生活様式および社会変化があっても、当協会に心技体に秀でた良き人材が集い、当協会および CSA／ASA が今後ますます発展することを期待しています。　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。

2022.7

めだか　【　この変化の時代にシステム監査が目指すもの - ウクライナ - 】

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、気候変動や新型コロナウイルスのパンデミック等々であり、システム監査が目指すものとは、正しさである。

さて、資料によるとウクライナの歴史は次に俯瞰される。「ロシア帝国やソヴィエト連邦のもとで長く忍従を強いられながらも、独自の文化を失わず、有為の人材を輩出し続けたウクライナ。不撓不屈のアイデンティティは、どのように育まれてきたのか。スキタイの興亡、キエフ・ルーシ公国の隆盛、コサックの活躍から、1991 年の新生ウクライナ誕生まで、この地をめぐる歴史を俯瞰。人口 5000 万を数え、ロシアに次ぎ第二の広い国土を持つ、知られざる「大国」の素顔に迫る。」とある。以下、その目次にて示す。

スキタイの興亡：　スキタイの登場　スキタイ人の建国伝説　建国伝説異説　遊牧の民　騎馬に巧みで勇敢な戦士　動物意匠と黄金への偏愛　ギリシャ世界との結びつき　スキタイの滅亡

キエフ・ルーシ公国の隆盛：　キエフ・ルーシは誰のものか　スラブ人の登場　ハザール可汗国　キエフ・ルーシの建国　ヴォロディーミル聖公とヤロスラフ賢公　キリスト教への改宗　モノマフ公の庭訓　モンゴルの征服　最初のウクライナ国家　キエフ・ルーシの社会と文化

コサックの活躍：　コサックの生い立ち　政治的勢力へ成長　組織と戦闘方法　国民性と生活　先駆者サハイダチニー　フメリニッキーの蜂起　ヘトマン国家の形成　モスクワの保護下に　フメリニッキーの最期　「荒廃」の時代　ヘトマン・マゼッパ　ポルタヴァの戦い　最後のヘトマン　ロシアへの併合　右岸ウクライナ　新ロシア県

1991 年の新生ウクライナ誕生は同時に 70 年続いたソヴィエト連邦が事実上解体したことを意味する。また、350 年を経て、フメリニッキーのウクライナ独立への夢がようやく現実となったことになる。人口は 5000 万人でフランスに匹敵する。面積ではヨーロッパでロシアに次ぐ第 2 位である。石油・天然ガス資源こそ十分ではないが、鉄鉱石はヨーロッパ最大規模の産地である。農業については、世界の黒土地帯の 30%を占める。耕地面積は日本の全面積に匹敵し、農業国フランスの耕地面積の二倍もある。工業・科学技術面では、それを支える科学者・技術者の水準は高く、層も厚い。国民の教育水準は高く、国民性は堅実で忍耐強い。しかるに、共存共栄であるべきところ、いま、ロシアはウクライナに攻めこんでいる。

私たちは、変化の時代に、そして、さまざまな出来事と役割に対し、改めて考えてみることが求められる。

（空心菜）

資料：「物語 ウクライナの歴史 ヨーロッパ最後の大国」黒川祐次著　中公新書 1655

（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>

2022.7

投稿【重要インフラ事業者の社会的責任と利用者のリスク管理】

会員番号　436 大石正人

大手通信キャリアの一角をなすＫ社が、２日半にわたる大規模な通信障害を起こしました。発生後（翌日）社長会見での公表報道では、スマホを含む携帯通信の契約 62 百万（電気通信事業者協会調べ）の６割が影響を受けた可能性があり、物流、自動車（つながる車など）、気象データ収集、銀行の店舗外 ATM、空港スタッフの手配など、通信を前提とした事業所向けにもサービスの中断が発生したため、かなり広範な経済的社会的な問題として大きく取り上げられました。

携帯通信は今や、生活必需品ですし、数時間ならまだしも、足かけ３日間もつながらないとなると、固定電話がない人々はさぞや不便だったと推察します。

また事業会社にとっても、つながる車が「つながらない」のでは全く機能しませんし、通信を前提としたサービスの中断は事業影響を引き起こすのは不可避でした。情報システム分野では、ＩｏＴ（ネットで様々なサービスが連携すること）により、センサーや情報連動による事業展開をもてはやしてきただけに、大前提の通信が途絶した際の「怖さ」を再認識した形になりました。

携帯通信だけをとっても、Ｋ社の契約者数のシェアは主要携帯通信の 26.6%（トップはＮ社の 36.3%）、移動通信事業者としての売上高だけ取ると前事業年度ではＮ社を上回ったとの報道もありますので、プレゼンスが高まっていたことは確かです。

しかし通信障害発生後の広報対応などでは、先の社長会見まで会社としての説明が後手に回り、どうも監督官庁（総務省）の担当官に乗り込まれる事態となり、存在感に見合った対応はとれなかった印象は拭われません。

原因はＫ社の「多摩ネットワークセンターで行っていたモバイルコアルーターの交換作業（通常の保守作業）で、交換後の機器の故障が発生、新機器への経路変更が行われず、通信を安定させる VoLTE（Voice over LTE、ボルテ、と読むようです）の音声通信が断絶し警告が発生した」、とのことです。

（注）２０２２年7月3日配信のＺＤ Net Japan の解説記事による
https://japan.zdnet.com/article/35189873/

業界トップのＮ社も２０２１年１０月に、大規模障害（丸１日、１００万契約に影響）を起こしました。事後に総務省へ提出した報告によると「通信ができない状況の発生要因は、Ｎ社が「IoT 機器」と表現する自動販売機の稼働状況などのデータを収集して同社の回線経由で管理会社などに送信する機器や、タクシーなどに設置される通信を伴う決済処理機器などの位置情報を登録するサーバーの切り替え工事に起因」とされました。

（注）同じくＺＤ Net Japan サイトの解説による。「NTT ドコモ、通信障害で 6 つの原因と見解--復旧手順に認識のズレ - ZDNet Japan」　https://japan.zdnet.com/article/35179239/

いずれのケースも通信機器の交換という「通常の保守作業」のなかで通常の手順で進めていたにもかかわらず、想定外の事象が発生し、それが起点となって、通信の輻輳が起きる、という通信ネットワーク特有の対処の難しい事態を招いています。こうした事態はある意味では今後も日常的に発生する懸念を抱きます。保守作業が「本番サービス」を提供しながら進める手順になっているからです。

システムの保守は、できれば本番サービスが提供されない時間帯に実施したいのが本音です。今回のＫ社や前回のＮ社の事例をみると、本番サービスを止めて作業している形跡はありません。通信の保守にはサービスの中断が許されていないのでしょうか。あるいは保守中は迂回ルートに通信を切り替えることはできないのでしょうか。門外漢にはこうした率直な疑問を抱きます。

この点は事業者も本音では保守作業のための中断時間確保を図りたいと推察されます。しかしあまりに日常的に保守を実施しており、通信（相互にやり取りするエリア）が地域別に提供する前提に必ずしもない以上、迂回手段提供にも限界があるので、結局リスクをとって、本番サービス中に保守を実施している可能性があります。

推察するに、監督官庁（総務省）にはこういう着眼点や発想はまず浮かびません。ただ「サービスの中断は起こすな、顧客に迷惑をかけるな」こうした発言が先行しがちです。省庁は通信にかかる実務の担い手でもなく、現場の実情に十分な関心を払わないからです。

通信は電気、ガス、水道などと並ぶ重要インフラ、と位置付けられ、特に情報セキュリティ侵害への備え、という観点からＮＩＳＣ（内閣サイバーセキュリティセンター）が各種のガイドラインを出したり、セキュリティ侵害にかかる横断的な対処訓練を実施しています。こうした取り組みにも事業継続の視点は含まれますが、その

起点はあくまでセキュリティ侵害や自然災害など共通のシナリオに基づく内容が主体です。

例えば通常のシステム・ネットワーク障害を視野に置いた事業継続の推進、啓発は必ずしも十分に行われていないのです。背景には各事業分野を所掌する省庁（事業者の監督官庁）との調整の難しさが想定されます。２０２２年6月１７日にＮＩＳＣが主催したサイバーセキュリティ戦略本部（本部長は内閣官房長官）第 34 回会合、および同会合で決定された「重要インフラのサイバーセキュリティに係る行動計画」（第５次に相当します）を見てみましょう。

まず会議録に見る通信事業者を所掌する総務大臣の発言は、サイバーセキュリティの重要性を強調し、NICT（国立研究開発法人情報通信研究機構）をノウハウ活用に言及する内容となっています。また7月１６日まで意見募集中の「ICT サイバーセキュリティ総合対策 2022」（案）も、文書名の通り、専らサイバーセキュリティに特化した内容にとどまっています。

こうしたなかでシステム監査の立場から、多少でも救われる思いがするのは、ＮＩＳＣの行動計画の「IV. 計画期間内の取組、1. 障害対応体制の強化」に「(7) 監査検証」として、「重要インフラ事業者等は、自組織の重要インフラサービスに係る障害対応体制の運用状況やリスクアセスメントに基づく適切な管理策の整備の状況を検証するために、監査検証が必要である。」との言及があることです。リスクマネジメントプロセスを順に記載したくだりにすぎないのですが、少なくとも国のサイバーセキュリティ戦略の一環として、監査検証の必要性が盛り込まれているからです。

重要インフラ所管省庁において大切なのは、重要インフラサービス事業者に対して、提供するサービスごとのリスクや業務の特性に合わせて、マネジメントプロセスを構築するよう求めること、そのうえで、マネジメントプロセスの有効性を監査検証により確認する体制の構築を求めること。さらには所管省庁も問題が起こってからの対処ではなく、できるだけプロアクティブに（先回りする発想で）、事業者の自主点検やできれば定期的な監督・検査を実施すること、だと思います。

重要インフラ事業者が提供するサービスは、事業分野により濃淡はありますが、国民生活の維持（安心社会の実現）のうえで不可欠な、公共性の高いものがほとんどです。まずは事業者自身が業務やサービスの特性を踏まえて、そのプレゼンスに相応しいリスクマネジメントプロセスを構築し、サービス中断を最小限にとどめる努力を続けるとともに、定期的な点検や保守を、場合によっては利用者の協力も得ながら、本番サービスに影響を極力及ぼさない安全な環境で実施することが大切です。

そのうえで、不測の事態に備えた事業継続計画と万一の事態発生時の迅速な広報体制を整えたうえ、できれば定期的にシミュレーションや机上訓練を実施し、経営層の関与を求めます。監査検証の担い手は、自社サービスや業務の特性や環境変化が、リスクマネジメントプロセスにきちんと反映されていることを確認したうえで、仕組みがきちんと機能することを第三者の目線で確認することが重要です。こうしたアプローチは、事業拡大や競合企業との差別化、収益最優先の経営姿勢が支配的だとまず採用されません。監査検証のコストを省いてしまう懸念が強いのです。

こうした問題点は昨今の製造業における品質不正事案とも相通じるものを感じます。平板な言い方ですが、重要インフラ事業者における自らのサービス・事業の公益性の十分な自覚的行動を期待し、それを促す所管省庁の役割期待を確認することも監査検証に求められていると強く感じています。

最後に、利用者の側も、携帯通信などのサービスにつきリスク管理の観点から、こうした事業者のマネジメントプロセスの有効性を評価し、サービスの購入先を判断したり、もし事業継続の要請上、中断リスクを避けることが不可欠であれば、一部に見られるように、複数手段の確保など、コストをかけても自衛策が必要になるやもしれません。また、各事業者においては、積極的にマネジメントプロセスの有効性を情報開示することも大切なＣＳ（顧客満足）確保になるでしょう。

今回の大手通信事業者の大規模長時間通信障害をきっかけに、繋がるのが当たり前、という感覚だけでは生活利便は確保できないことにも思いを致す必要がありそうです。つまり多少効率性は犠牲にしても、手間をかけることによって、却ってサービスや機器を使いこなすスキルが身についたり、万一に備えて活用方法を考える意識が高まる効果も期待できる、ということのようです。

以上の諸点をシステム監査にどう応用すればよいのか、は今後の課題にしたいと思いますが、いずれにしても（安全性、信頼性に止まらない）効率性以外の価値をシステムデザインに取り入れているか、そうした視点でサービスを提供しようとしているか、をシステム監査人の視点として持ちうる可能性を指摘しておきたいと思います。

<目次>

2022.07

【エッセイ】施餓鬼会

会員番号　0707 神尾博

祖先への供養として、現在は 8 月中旬に催されることが多い盂蘭盆会（うらぼんえ）。同じ時季に施餓鬼会（せがきえ）が併せて行われることもあり、こちらは生前の悪行により餓鬼となって苦しんでいる、親族以外の亡者に広く功徳を施すものである。餓鬼には多くのバリエーションがあるようだが、最も知られているのは、生前に贅沢をしていくら食べても飢えを満たせなかったり、手に取ったものが全て火になって食することができなかったりといった責め苦を負う者たちで、人間の物欲や飽食を戒める存在とされている。

ビッグテックも、際限のないデータ収集をリソースにして、市場における利益の寡占化の勢いはとどまる所を知らない。2021 年 8 月には、GAFA の株式価値は 7 兆 500 億ドル（約 770 兆円）に達し、日本企業全体のそれを越えたと報道された。日本の国家予算（約 500 兆円）をも大幅に上回っている。そもそもこうした富の集中は、ネオリベラリズム（新自由主義）という形で、インターネットの拡大を背景にした IT 産業の興隆よりも前から、全世界に浸透しつつあった。我が国でも 2000 年代初頭に「構造改革」の名の元にそうした流れへ大きく舵を切り、現在も拡大の一途を辿っている。

ついにというか、ビッグテックへ過度の権益を抑制するため、「Web3.0」という新たなインターネットのアーキテクチャも囁かれ始めた。Web3.0 はブロックチェーン技術を使い、ノード同士を P2P（ピア・ツー・ピア）で相互接続するもので、データは分散して持つことになり、特定のサイトに集中しない。また、変更履歴がデータに追加されていくので改竄も困難である。

P2P は Winny 事件で一世を風靡したが、ここに来てあらためて科学技術の価値中立を尊重することの重要性を認識する機会となったのではないか。

さて、誰もが死後には六道のいずれかに送られるというが、餓鬼道、畜生道、地獄道は、その中の三悪道と言われている。現在の Web2.0 は先に述べた通り、際限のない飽食の餓鬼道状態といえよう。一方で人の道を外れた犯罪や、違法アダルトの巣窟と化しているダークウェブは、いわば畜生道か。そして Web3.0 がネット社会の民主化に寄与するという理念の半面、取り締まりや責任の主体が無いため、悪意を持つ者を排除できない等で裏目に出るなら、多くの人々を地獄道に突き落とすことにもなりかねない。引き続き動向を注視していきたい。

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

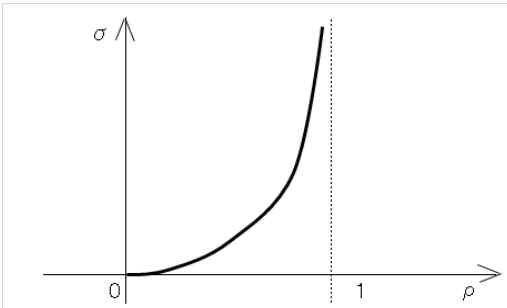
2022.7

【コラム】システム監査のための、法律・会計再入門（8）

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.システム監査の法的義務化の必要性

７月２日(土)未明、某大手携帯電話会社で大規模な通信障害が発生した(→文献[8])。ネットワーク輻輳が原因である。ネットワーク・スペシャリスト試験に「待ち行列」があるが、平均待ち時間は概ね次のようになる(→文献[10])。



ρ ： 込み具合(0≦ρ＜1)

σ ： 平均待ち時間

関係式： $\sigma = \frac{\rho}{1-\rho}$

$\lim_{\rho \to 1-0} \sigma = +\infty$

ここで重要なことは、込み具合ρが 1 に近づくと、平均待ち時間σは途中から急激に大きくなり、無限大になってしまうことである。世間的にはσとρは比例すると考えている人々も少なくないが、実はこのようになっているのである。

やはり、**高度情報処理試験の有資格者による、システムの外部監査の法的な義務化が必要**であると思われる。

また、モルヒネを誤って適正量の 100 倍投与してしまったために、患者が死亡するという痛ましい医療事故が発生した(→文献[10])。この事故は、この報道によれば、医師と薬剤師の二重のミスにより発生したとあるが、①医師による
システムへの処方量入力の際に異常値が入力できないように設計する、②異常値を検知したらアラートが出る、ようなシステムの設計にしておけば、今回の事故は未然に防げた蓋然性が極めて高いと思われる。この点についても、システムの外部監査は非常に有益である。**【システム監査専門家の出番】**

【解決方法】①会社法第 328 条を改正して、「会計監査人」を「会計監査人およびシステム監査人」とする。
②金融商品取引法の第 2 章に「システム監査人」の設置義務を追加する。

§2.国産の新型コロナ治療薬の緊急承認審査

７月に入り、再び、新型コロナ感染者が増加に転じている。6 月下旬に「医薬品・医療機器等法」が改正され、米国の制度に似た医薬品の「緊急承認」の制度が創設され、6 月 20 日に審査が行われる予定である(→文献[7])。本書の原稿締切日の段階では審査を迎えていないが、緊急承認が行われるよう、切に祈るばかりである。次の感染症の流行に備えて、**「研究開発費の一律費用処理(大半が税法上損金不算入)」という異常な状態は直ちに是正する必要**がある。

①財務諸表規則等を改正して、国際会計基準(IFRS)のように研究開発費を無形固定資産に計上可能にする。
②財務諸表規則等を改正して、繰延資産の「開発費」の定義を法人税法に揃える。
③国際会計基準(IFRS),修正国際基準(JMIS)を個別財務諸表を含めて全ての企業が自由に使えるよう規制緩和にする。

§3.SAP のためのドイツ語入門

今回も引き続きドイツ語の語順を取り上げる。今回は動詞 nehmen に話法の助動詞 können(日本語:できる,英

副文における基本構造				受動の動作主	目的語	(否定)	述語形容詞	直後以降に要求するもの		本動詞		直前に要求するもの	
								原形	代用不定詞			過去分詞	原形
話法の助動詞有り								未来を作る	完了を作る			受動を作る	
	態	完了か		von＋与格				werden	haben	分離成分	本体部分	werden sein	話法の助動詞
1	能動	×	現在		(△)	(nicht)	(△)			(▲)	●		○
2	能動	×	過去		(△)	(nicht)	(△)			(▲)	●		○
3	能動	×	未来		(△)	(nicht)	(△)	○		(▲)	●		○
4	能動	○	現在		(△)	(nicht)	(△)		○	(▲)	●		○
5	能動	○	過去		(△)	(nicht)	(△)		○	(▲)	●		○
6	能動	○	未来		(△)	(nicht)	(△)	○	○	(▲)	●		○
7	動作受動	×	現在	△	(△)	(nicht)	(△)			(▲)	●	○(weden)	○
8	動作受動	×	過去	△	(△)	(nicht)	(△)			(▲)	●	○(weden)	○
9	動作受動	×	未来	△	(△)	(nicht)	(△)	○		(▲)	●	○(weden)	○
10	動作受動	○	現在	△	(△)	(nicht)	(△)		○	(▲)	●	○(weden)	○
11	動作受動	○	過去	△	(△)	(nicht)	(△)		○	(▲)	●	○(weden)	○
12	動作受動	○	未来	△	(△)	(nicht)	(△)	○	○	(▲)	●	○(weden)	○
13	状態受動	×	現在	△	(△)	(nicht)	(△)			(▲)	●	○(sein)	○
14	状態受動	×	過去	△	(△)	(nicht)	(△)			(▲)	●	○(sein)	○
15	状態受動	×	未来	△	(△)	(nicht)	(△)	○		(▲)	●	○(sein)	○
16	状態受動	○	現在	△	(△)	(nicht)	(△)		○	(▲)	●	○(sein)	○
17	状態受動	○	過去	△	(△)	(nicht)	(△)		○	(▲)	●	○(sein)	○
18	状態受動	○	未来	△	(△)	(nicht)	(△)	○	○	(▲)	●	○(sein)	○

語:can,仏語:pouvoir,希臘語: δύναμαι,羅語: possum)を伴う場合である(→文献[1-5]に関連)。

★具体的な例文：Er kann einen Apfel nehmen.(話法の助動詞有り、分離成分無し)では次の通り。

副文における肯定文/否定文				従属接続詞		受動動作主	目的語	(否定)	直後以降に要求するもの		本動詞	直前に要求するもの		ピリオド
話法の助動詞有り	分離成分無し								原形	代用不定詞		過去分詞	原形	
	態	完了か				von＋与格			未来を作る	完了を作る		受動を作る	話法の助動詞	
									werden	haben		werden sein		
1	能動	×	現在	, dass	er		einen Apfel	(nicht)			nehmen		kann	.
2	能動	×	過去	, dass	er		einen Apfel	(nicht)			nehmen		konnte	.
3	能動	×	未来	, dass	er		einen Apfel	(nicht)	wird		nehmen		können	.
4	能動	○	現在	, dass	er		einen Apfel	(nicht)		hat	nehmen		können	.
5	能動	○	過去	, dass	er		einen Apfel	(nicht)		hatte	nehmen		können	.
6	能動	○	未来	, dass	er		einen Apfel	(nicht)	wird	haben	nehmen		können	.
7	動作受動	×	現在	, dass	ein Apfel	von ihm		(nicht)			genommen	werden	kann	.
8	動作受動	×	過去	, dass	ein Apfel	von ihm		(nicht)			genommen	werden	konnte	.
9	動作受動	×	未来	, dass	ein Apfel	von ihm		(nicht)	wird		genommen	werden	können	.
10	動作受動	○	現在	, dass	ein Apfel	von ihm		(nicht)		hat	genommen	werden	können	.
11	動作受動	○	過去	, dass	ein Apfel	von ihm		(nicht)		hatte	genommen	werden	können	.
12	動作受動	○	未来	, dass	ein Apfel	von ihm		(nicht)	wird	haben	genommen	werden	können	.
13	状態受動	×	現在	, dass	ein Apfel	von ihm		(nicht)			genommen	sein	kann	.
14	状態受動	×	過去	, dass	ein Apfel	von ihm		(nicht)			genommen	sein	konnte	.
15	状態受動	×	未来	, dass	ein Apfel	von ihm		(nicht)	wird		genommen	sein	können	.
16	状態受動	○	現在	, dass	ein Apfel	von ihm		(nicht)		hat	genommen	sein	können	.
17	状態受動	○	過去	, dass	ein Apfel	von ihm		(nicht)		hatte	genommen	sein	können	.
18	状態受動	○	未来	, dass	ein Apfel	von ihm		(nicht)	wird	haben	genommen	sein	können	.

主文における肯定文/否定文					第2位置	受動動作主	目的語	(否定)	直後以降に要求するもの		本動詞	直前に要求するもの		ピリオド
話法の助動詞有り	分離成分無し								原形	代用不定詞		過去分詞	原形	
	態	完了か			定動詞	von＋与格			未来を作る	完了を作る		受動を作る	話法の助動詞	
									werden	haben		werden sein		
1	能動	×	現在	Er	kann		einen Apfel	(nicht)			nehmen			.
2	能動	×	過去	Er	konnte		einen Apfel	(nicht)			nehmen			.
3	能動	×	未来	Er	wird		einen Apfel	(nicht)			nehmen		können	.
4	能動	○	現在	Er	hat		einen Apfel	(nicht)			nehmen		können	.
5	能動	○	過去	Er	hatte		einen Apfel	(nicht)			nehmen		können	.
6	能動	○	未来	Er	wird		einen Apfel	(nicht)		haben	nehmen		können	.
7	動作受動	×	現在	Ein Apfel	kann	von ihm		(nicht)			genommen	werden		.
8	動作受動	×	過去	Ein Apfel	konnte	von ihm		(nicht)			genommen	werden		.
9	動作受動	×	未来	Ein Apfel	wird	von ihm		(nicht)			genommen	werden	können	.
10	動作受動	○	現在	Ein Apfel	hat	von ihm		(nicht)			genommen	werden	können	.
11	動作受動	○	過去	Ein Apfel	hatte	von ihm		(nicht)			genommen	werden	können	.
12	動作受動	○	未来	Ein Apfel	wird	von ihm		(nicht)		haben	genommen	werden	können	.
13	状態受動	×	現在	Ein Apfel	kann	von ihm		(nicht)			genommen	sein		.
14	状態受動	×	過去	Ein Apfel	konnte	von ihm		(nicht)			genommen	sein		.
15	状態受動	×	未来	Ein Apfel	wird	von ihm		(nicht)			genommen	sein	können	.
16	状態受動	○	現在	Ein Apfel	hat	von ihm		(nicht)			genommen	sein	können	.
17	状態受動	○	過去	Ein Apfel	hatte	von ihm		(nicht)			genommen	sein	können	.
18	状態受動	○	未来	Ein Apfel	wird	von ihm		(nicht)		haben	genommen	sein	können	.

★具体的な例文：Er kann einen Apfel annehmen.(話法の助動詞有り、分離成分有り)では次の通り。**話法の助動詞がある場合は、主文であっても分離動詞は常に文末の述部に配置されるので、分離しない。**

副文における肯定文/否定文				従属接続詞		受動動作主	目的語	(否定)	直後以降に要求するもの		本動詞	直前に要求するもの		ピリオド
話法の助動詞有り	分離成分有り								原形	代用不定詞		過去分詞	原形	
	態	完了か				von＋与格			未来を作る	完了を作る		受動を作る	話法の助動詞	
									werden	haben		werden sein		
1	能動	×	現在	, dass	er		einen Apfel	(nicht)			annehmen		kann	.
2	能動	×	過去	, dass	er		einen Apfel	(nicht)			annehmen		konnte	.
3	能動	×	未来	, dass	er		einen Apfel	(nicht)	wird		annehmen		können	.
4	能動	○	現在	, dass	er		einen Apfel	(nicht)		hat	annehmen		können	.
5	能動	○	過去	, dass	er		einen Apfel	(nicht)		hatte	annehmen		können	.
6	能動	○	未来	, dass	er		einen Apfel	(nicht)	wird	haben	annehmen		können	.
7	動作受動	×	現在	, dass	ein Apfel	von ihm		(nicht)			angenommen	werden	kann	.
8	動作受動	×	過去	, dass	ein Apfel	von ihm		(nicht)			angenommen	werden	konnte	.
9	動作受動	×	未来	, dass	ein Apfel	von ihm		(nicht)	wird		angenommen	werden	können	.
10	動作受動	○	現在	, dass	ein Apfel	von ihm		(nicht)		hat	angenommen	werden	können	.
11	動作受動	○	過去	, dass	ein Apfel	von ihm		(nicht)		hatte	angenommen	werden	können	.
12	動作受動	○	未来	, dass	ein Apfel	von ihm		(nicht)	wird	haben	angenommen	werden	können	.
13	状態受動	×	現在	, dass	ein Apfel	von ihm		(nicht)			angenommen	sein	kann	.
14	状態受動	×	過去	, dass	ein Apfel	von ihm		(nicht)			angenommen	sein	konnte	.
15	状態受動	×	未来	, dass	ein Apfel	von ihm		(nicht)	wird		angenommen	sein	können	.
16	状態受動	○	現在	, dass	ein Apfel	von ihm		(nicht)		hat	angenommen	sein	können	.
17	状態受動	○	過去	, dass	ein Apfel	von ihm		(nicht)		hatte	angenommen	sein	können	.
18	状態受動	○	未来	, dass	ein Apfel	von ihm		(nicht)	wird	haben	angenommen	sein	können	.

主文における肯定文/否定文					第2位置	受動動作主	目的語	(否定)	直後以降に要求するもの		本動詞	直前に要求するもの		ピリオド
話法の助動詞有り		分離成分有り							原形	代用不定詞		過去分詞	原形	
	態	完了か			定動詞	von＋与格			未来を作る	完了を作る		受動を作る	話法の助動詞	
									werden	haben		werden sein		
1	能動	×	現在	Er	kann		einen Apfel	(nicht)			annehmen			.
2	能動	×	過去	Er	konnte		einen Apfel	(nicht)			annehmen			.
3	能動	×	未来	Er	wird		einen Apfel	(nicht)			annehmen		können	.
4	能動	○	現在	Er	hat		einen Apfel	(nicht)			annehmen		können	.
5	能動	○	過去	Er	hatte		einen Apfel	(nicht)			annehmen		können	.
6	能動	○	未来	Er	wird		einen Apfel	(nicht)		haben	annehmen		können	.
7	動作受動	×	現在	Ein Apfel	kann	von ihm		(nicht)			angenommen	werden		.
8	動作受動	×	過去	Ein Apfel	konnte	von ihm		(nicht)			angenommen	werden		.
9	動作受動	×	未来	Ein Apfel	wird	von ihm		(nicht)			angenommen	werden	können	.
10	動作受動	○	現在	Ein Apfel	hat	von ihm		(nicht)			angenommen	werden	können	.
11	動作受動	○	過去	Ein Apfel	hatte	von ihm		(nicht)			angenommen	werden	können	.
12	動作受動	○	未来	Ein Apfel	wird	von ihm		(nicht)		haben	angenommen	werden	können	.
13	状態受動	×	現在	Ein Apfel	kann	von ihm		(nicht)			angenommen	sein		.
14	状態受動	×	過去	Ein Apfel	konnte	von ihm		(nicht)			angenommen	sein		.
15	状態受動	×	未来	Ein Apfel	wird	von ihm		(nicht)			angenommen	sein	können	.
16	状態受動	○	現在	Ein Apfel	hat	von ihm		(nicht)			angenommen	sein	können	.
17	状態受動	○	過去	Ein Apfel	hatte	von ihm		(nicht)			angenommen	sein	können	.
18	状態受動	○	未来	Ein Apfel	wird	von ihm		(nicht)		haben	angenommen	sein	können	.

★英語の can と異なり können は本動詞としても用いられる。また、現在分詞や過去分詞も存在する。本動詞の場合の過去分詞は gekonnt であるが、助動詞として用いられる場合の過去分詞は原形と同形の können であり、原形が 2 つ続いているように見える。そのため、現在完了では次のようになる。(können が助動詞として用いられる場合の hat(英語の has に相当)の位置に特に注意されたい。
・本動詞の場合：Er hat es **gekonnt**.　　/ ,dass er es **gekonnt** hat.(彼はそれができた。)
・助動詞の場合：Er hat es machen **können**. / ,dass er es **hat** machen **können**. (彼はそれを為すことができた。)

★言語は重要である。日本語で「自然科学」という場合、数学を含むか否かは学閥によって異なる。**英語の Natural Science は Mathematics(数学)を含まないが、ドイツ語の Naturwissenschaft は Mathematik(数学)を含む。**
米国では物理を無視する純粋数学(SMSG 式の Bourbakism)を Mathematics、応用数学を Math.と呼んで区別している。
　以前、「ベーシック・インカム」には、①「既存の社会保障に上乗せするして一律給付する方式」と②「既存の社会保障を廃止・削減し、それを財源にして一律給付する方式」があることを取り上げた。近年では「労働市場の流動化」というフレーズがマスコミで独り歩きしている。これも①「勤労者の雇用を保証した上で、自発的な転職をしやすい環境を整える」という意味と、②「終身雇用を破壊して、解雇規制を撤廃して労働市場を流動化する(結果として賃金水準は下がる)」という、全く逆の意味で使われている。言語とは、実に、恐ろしいものである。

§4.消費税のインボイス制度についての補足

　消費税を始めとする付加価値税(VAT：英：Value Added Tax,仏：Taxe sur la valeur ajoutée,　独：Mehrwertsteuer)の世界標準は次の 3 原則である。(→文献[1-3])

①インボイス(税額票)方式
②複数税率と、(広範な)非課税品目・軽減税率品目
③税込経理の禁止(「仮受消費税」、「仮払消費税」を必ず使用する)　　※表示の内税と区別が必要

　この内、②は 2019 年 10 月に施行され、③は 2021 年 4 月に企業会計基準の改正により、大企業には強制適用となった。
最後に①が 2023 年 10 月に施行されることとなる。
　今回は①の端数処理についての留意事項を述べる。文献[6]の P9 には次のような注意書きがある。

記載に当たっての留意点

Point　「税率ごとに区分した消費税額等」の端数処理

○　適格請求書の記載事項である「税率ごとに区分した消費税額等」に 1 円未満の端数が生じる場合には、一の適格請求書につき、税率ごとに 1 回の端数処理を行います。
※　端数処理は、「切上げ」、「切捨て」、「四捨五入」など任意の方法で行うこととなります。
○　したがって、「税率ごとに区分して合計した対価の額」に税率を乗じるなどして、計算することとなります【例①】。
※　例えば、一の適格請求書に記載されている個々の商品ごとに消費税額等を計算し、端数処理を行い、その合計額を「税率ごとに区分した消費税額等」として記載することは認められません【例②】。

このことを具体的な例で説明すると、次のようになる。

インボイス移行後は廃止　　**インボイスへの記載内容**

	品目	税区分	単価	数量	本体価格	明細単位の計算(a)			税区分合計の計算(b)		
						消費税額	(小計)	税込金額	税区分毎の本体価格合計	消費税額	税込金額
1	本	10%	3,964	1	3,964	396		4,360			
2	鉛筆(ダース)	10%	19	7	133	13	651	146	6,519	652	7,171
3	ビール	10%	346	7	2,422	242		2,664			
4	チョコレート	8%	187	17	3,179	254		3,433			
5	コーヒー	8%	147	13	1,911	153	569	2,064	7,120	570	7,690
6	食パン	8%	203	10	2,030	162		2,192			
7	切手	0%(非課税)	83	25	2,075	0		2,075			
8	家賃	0%(非課税)	75,300	1	75,300	0	0	75,300	100,954	0	100,954
9	保険料	0%(不課税)	23,579	1	23,579	0		23,579			
	伝票合計				114,593	1,220		115,813	114,593	1,222	115,815

上図は価格表示が「外税」の場合の例である。**赤枠の方法は明細単位での四捨五入**であるが、2023 年 10 月からは右端の**青枠の方法(税率毎に本体価格を合計した後に税率を乗ずる方式)**に統一される。また、価格表示が「内税」の場合も、**税率毎に税込価格を合計し、税率を掛けて割り返す方式に統一**される。この制度は 2023 年 10 月 1 日から施行されるが、システムの都合上、年度の途中で計算方法が変わると極めて煩雑になるので、**3 月末決算の会社の場合、システムの改修は 2023 年 3 月末が事実上のタイムリミット**となる。

我々、システム監査技術者としては、クライアント等の基幹システム及びレジスター等が、新制度に対応できているか否か早急に調査する必要がある。　**【システム監査専門家の出番】**

★なお、先日の講演でも感じたことであるが、この制度改正については国民の間に広く周知されているとは言い難い。
財務省及び税務当局は早急に「政府広報」等を通じて国民に周知を図る必要がある。また、システム監査人も、周知を図る必要があると考えられる。

※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・会計基準の適用等については、必ず、御自身でご担当の顧問会計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、IFRS&連結会計〔Ⅰ〕〔Ⅱ〕："In Varietate Concordia", EU の知恵に学べ　IFRS では何故そう考えるのか?　Ver7 (2022/04/18)
[2]「「軽減税率」田淵隆明が語る、医療機関の損税問題
[3]「「軽減税率」田淵隆明が語る、数学・理科カリキュラム再考」(2022/07/18)
[4] SAP のオンライン・マニュアル https://lyricsodus.com/skill/SAP.html?genre=(KKF6M%20OR%20KKF6N)&lang=ja-JP
[5] SAP のトランザクション・コード一覧(SE93 でも検索可能)http://www.enjoyops.de/interessantes/index/ja/tcod/tcod_k_ja.php5
[6] 適格請求書等保存方式の概要 ～インボイス制度の理解のために～(国税庁)
https://www.nta.go.jp/taxes/shiraberu/zeimokubetsu/shohi/keigenzeiritsu/pdf/0020006-027.pdf
[7] 塩野義コロナ飲み薬、20 日にも再審議　国産初、緊急承認も初で注目
https://www.asahi.com/articles/ASQ756DWHQ75UTFL01H.html
[8] KDDI"通信障害"復旧せず　交換機に障害で通信混雑…アクセス制限し交通整理中
https://news.yahoo.co.jp/articles/145abcc19ee7daac45ace3d8cd168a88eea162ba
[9] サルでもわかる待ち行列　http://objectclub.jp/technicaldoc/monkey/s_wait
[10] 東京・国分寺市のクリニックでモルヒネ 100 倍誤処方　93 歳男性死亡　警視庁が医師と薬剤師を書類送検
https://news.yahoo.co.jp/articles/8752ce505577a100bf81d205073e8828ae2c1376

<目次>

2022.7

第 268 回月例研究会：講演録

テーマ：JUAS「企業 IT 動向調査 2022」の結果からみる、デジタル経営の分岐点

会員番号　2449 億谷和彦（月例研究会）

【講師】一般社団法人日本情報システム・ユーザー協会（JUAS）

シニアマネージャー　山畔秀雄　（やまくろひでお）氏

【日時・場所】2022 年6月 15日(水)18 時 30 分～20 時 30 分、オンライン(Zoom ウェビナー)

【テーマ】JUAS「企業 IT 動向調査 2022」の結果からみる、デジタル経営の分岐点

【要旨】

企業 IT 動向調査は 28 回目を迎えました。2021 年度調査は「デジタル経営の分岐点」を重点テーマに掲げ実施しました。DX 推進、情報セキュリティ、IT 投資の動向など、調査からみえてきた現状と今後の見通しを解説します。

【講演録】

Ⅰ．企業IT動向調査2022（2021年度調査）の概要

2021年度の重点テーマは「デジタル経営の分岐点」であり、今、IT部門は企業経営の中でどのような役割を果たしていくことが求められ、どのようなシナリオを描くことが求められているのかを探った。

アンケート（4499社に依頼し、回答率25.2%）とインタビュー（ユーザー企業11社のIT部門長対象）による調査を実施した結果を、以下の通り、ご説明いただいた。

1. 業績とIT予算

2. DXの取組みと進展

3. セキュリティとガバナンス

4. IT部門の役割とありかた

5. 総括と提言

Ⅱ．「1. 業績とIT予算」

21 年度の企業業績は、「増収増益」が 30.4→52.6%と大幅増となる見込みで、景気の回復傾向が顕著、また「減収減益」の割合が 42.1→21.2%に減少しており、景気のＶ字回復が顕著である。

特に関心の高い 3 つの「喫緊の経営課題」の内、IT が重要視されている順番は①働き方改革、業務ﾌﾟﾛｾｽ **大**②顧客、ｻｰﾋﾞｽ、新ﾋﾞｼﾞﾈｽ **中**③人材育成や組織開発 **小** である。

IT 予算の DI 値は、21 年計画では 29.6 ポイントとなり、新型コロナ禍前の水準まで回復。さらに 22 年予測では、32.4 ポイントと過去最高水準となる見込み。

IT 予算増加の主な理由は、20 年と同様に「業務のデジタル化対応」「基幹システムの刷新」「基盤整備・増強」。さらに、22 年は「事業変革に向けたデジタル化対応」と回答した割合が大幅増。

DX の進捗度合いと IT 予算に相関がみられ、DX の進捗度合いが高いほど IT 予算を増加させる傾向があり、DX

を進めるためには、継続した IT 予算の確保が不可欠である。

今回、2021 年度 9 月～10 月の調査によるため、ウクライナ情勢によりその後の状況は反映していない。

Ⅲ．「2. DXの取組みと進展」

１．DX

DXが推進できている企業は4社に1社、業種・規模による差があるものの、成果や進捗が実感できていない企業が多い。明確な推進組織の定義がないことも要因の一つ。また、専任CIOの設置による効果が見受けられる。

DX推進における課題は人材・スキル、体制、戦略の不足があがる。特に、不足感が際立っていたのはDXの企画推進およびデータドリブンでの業務革新人材である。

DX推進の取組実施状況はテレワーク（在宅勤務）にかかわる単純自動化の要素で成果が出ている一方、創造・革新にかかわる要素は検討されつつあるが、具体的な取組みや成果には至っていない。

２．未来に向けたテクノロジー活用

引き続き、新型コロナ禍に対応するテレワーク（在宅勤務）を実現するテクノロジーやフレームワークの新規導入が顕著。

「人と結びつく技術」が企業で新たに導入を求めるテクノロジーになってきており、今後注目すべき。

導入しようとするテクノロジーで先行する業種グループの導入事例を参考に、各企業の個別条件等を重ね合わせ活用していくことが効果的である。

３．データ活用とレガシーシステムの対応

データ活用に取り組んでいる企業は全体として増加傾向が続いており、データを活用していく姿勢が定着してきている様子がみえた。

DX を推進できていると自認する企業では、組織横断的なデータ活用の取組みが進んでいる。一部組織での深いデータ活用も大事であるが、社内横断的なデータ活用の取組みを進める、面的な拡がりも重要。

データマネジメントとレガシーシステム刷新の必要性は、過去数年で経営者の理解を得られた模様、今後は具体的なリソースの確保が課題になる。

Ⅳ．「3. セキュリティとガバナンス」

１．情報セキュリティ

今後(3年後)のセキュリティ関連費用は半数以上の企業が増加を見込んでおり、今後も継続的に対策は強化されると考えられる。

セキュリティ費用の増加理由からも、セキュリティ対策はDX施策や新規システム導入に対してだけでなく、全方位的な対策が必要であると分かった。

セキュリティ施策の重点箇所は売上高や業種グループにかかわらず「防御」「検知」が中心となっている。今後、重点施策を決めた戦略的な推進が必要である。

２．グループ・グローバルITガバナンス

グループ・グローバルITガバナンスは、規模の大きい企業で重視。特に「セキュリティ」、「インフラ」、「IT戦略」においてガバナンスが進んでいるが、いずれも道半ばで最大の課題は、「体制の不足」。

DX推進度が高い企業は、グループ・グローバルITガバナンスもしっかりと実施。DXを進めるうえでITガバナンスは必要なものと推察される。

各国のIT関連法制度やIT機器・ソフトウェア・サービス調達に関するリスク（IT地政学的リスク）への対応はほとんどの企業で受け身・アドホック。ただし、金融・保険では基準・ポリシーを作成したり、事前に調達制限したりと入念に対応している。

Ⅴ．「4. IT部門の役割とありかた」

１．IT基盤・システム開発

「テレワーク環境」に必要なIT 基盤の整備は大きく進んだ。クラウドの活用については、DX 推進に積極的な企業、売上高規模の大きい企業を中心に拡大している一方で、リソース面（人材・スキル・予算）の課題でそこに至れていない企業も存在する。

システム開発の工期・予算・品質遵守状況は全て悪化傾向。何らかの構造的・組織的問題が背景にあることがうかがえる。

DX推進には開発内製化率を高めることが有効。ノウハウの蓄積やアジャイル開発の促進などが目的であるが、高付加価値のIT を実現するには社外リソースの一時的な活用だけでは立ち行かない状況であることがうかがえる。

２．ワークスタイル変革

テレワーク(在宅勤務)はIT基盤の整備によって定着しているが、今後の予定は多少出社日を増やす傾向にある。

オフィス縮小など業績改善の対策のためにもテレワーク(在宅勤務)の維持は欠かせない。

テレワーク(在宅勤務)がもたらす弊害を減らすために、「長時間労働の防止」や「コミュニケーション機会の創出」など、IT以外の施策に多くの企業が取り組んでいる。

３．IT組織・人材

IT部門の要員数DI値は過去最高。人材不足（要員数、スキルとも）への対応が重要な課題となっている。

DXが進んでいる企業においては、全体的に人員の充足度が高い。特に企画系要員に顕著な差がある。

DXが進んでいる企業においては、充足度を高めるために、ジョブ型人事制度の採用をはじめ、新たな人事施策を採用している。

Ⅵ．「5. 総括と提言」

今回の動向調査の結果から、IT部門がリーダーシップを発揮できる領域や機会がますます拡がり、自らの意思と力でトランスフォームしていく**「分岐点」**に立っていることを再認識した。

DXリスタートにあたり、当調査のエッセンスが凝縮された**「DX成熟度のセルフチェック」**を実施してみることをお勧めしたい。

【所感】

第266回月例研究会でもDXに関する講演があったように、今回の講演により、従前の情報化、電子化、ＩＴ化と言った単なる現業の効率化の範囲ではなく、今後の企業の存続から業態変革までを考慮したＤＸ（デジタルトランスフォーメーション）に向けて、大企業、特に待ったなしの金融・保険業を先頭に始まっている様子が理解できました。益々、今後の動向から目が離せず、来年のJUAS様の講演が待たれます。

以上

<目次>

2022.7

支部報告【北信越支部 2022 年度福井県例会/6 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 2022 年度福井県例会/6 月リモート例会を開催しました。

・日時：2022 年 6 月 4 日（土）　　現地参加者：6 名、リモート参加者：6 名

・会場：福井市現地会場とリモート（zoom）のハイブリッド開催

・議題：　研究報告

「サイバーセキュリティ強化とオペレーショナルレジリエンスについて」　小嶋　潔　氏

「銀行勘定系システムの現状と課題」 大石 正人　氏

「リスクマネジメントフレームワークについて」　宮本　茂明

◇研究報告 1

「サイバーセキュリティ強化とオペレーショナルレジリエンスについて」

会員番号 1739　小嶋　潔

本年 2 月に金融庁から「金融分野におけるサイバーセキュリティ強化に向けた取組方針（Ver.3.0）」が公表されると共に、これと相前後して、政府からはサイバーセキュリティ対策の強化についての注意喚起が再三行われている。このサイバーセキュリティ強化の取組方針の概要と、近年当局が重視しているオペレーショナルレジリエンスについて報告する。

（1）取組方針改定の経緯

金融庁では、「金融分野におけるサイバーセキュリティ強化に向けた取組方針」（2015 年 7 月 Ver.1.0 策定、2018 年 10 月 Ver.2.0）に基づき、金融業界と連携して金融分野のサイバーセキュリティ管理態勢の強化に取り組んできた。Ver.2.0 では東京オリンピック・パラリンピックを見据えたサイバーセキュリティの強化を新たな重要課題として位置付けていたが、金融機関やその顧客に被害を及ぼすサイバーアクシデントは発生しなかった。他方、Ver.2.0 以降デジタライゼーションは一層加速し、データの利活用や新たなビジネスチャンスを捉えた新しいプレイヤーの金融分野への参入がさらに進んだ。加えて、新型コロナウィルス感染症の拡大は、リモートワークやオンラインでの商品やサービス提供の普及といった社会のデジタル化にも影響を与えたが、これらの非対面・非接触型の業務の脆弱性を狙ったサイバー攻撃や、ソーシャルエンジニアリングを用いた巧妙なサイバー攻撃も増加した。Ver.2.0 から 3 年が経過し、金融分野のサイバーセキュリティを巡る状況が日々変化する中でサイバー空間における脅威は一層高まっており、新たな課題・脅威に対する対応方針を Ver.3.0 としてアップデートしたもの。

（2）新たな取組方針 Ver.3.0 のポイント

【①モニタリング・演習の高度化】

金融機関の規模･特性やサイバーセキュリティリスクに応じて、検査･モニタリングを実施し、サイバーセキュリティ管理態勢を検証し、共通の課題や好事例については業界全体を通じて傘下金融機関に還元し、金融業界全体のサイバーセキュリティの高度化を促す。特に 3 メガバンクについては、サイバー攻撃の脅威動向の変化への対応や海外大手金融機関における先進事例を参考にしたサイバーセキュリティの高度化に着目しつつ、モニタリングを実施する。地域金融機関については、サイバーセキュリティに関する自己評価ツールを整備し、各金

融機関の自己評価結果を収集、分析、還元し、自立的なサイバーセキュリティの高度化を促す。サイバー演習については、引き続きサイバー攻撃の脅威動向や他国の演習等を踏まえて高度化を図る。

【②新たなリスクへの備え】

キャッシュレス決済サービスの安全性を確保するため、リスクに見合った堅牢な認証方式の導入等を促す（セキュリティバイデザインの実践）。クラウドサービスの安全な利用に向けて、利用実態や安全対策の把握を進めるとともに、クラウドサービス事業者との対話も実施する。

サイバー攻撃が高度化・複雑化し、また、金融サービスの提供において、外部委託が拡大するとともに、サプライチェーンが複雑化・グローバル化していることを踏まえれば、事前にサイバーセキュリティリスクを全て洗い出したうえで施策を講じ、インシデントを未然に防止することは一層困難な状況となっている。サイバーセキュリティ管理の範囲は、インシデントの未然防止から、インシデント発生時の検知、特定、対応、業務の早期復旧や顧客影響の軽減といったレジリエンス（いわゆる復元力）の強化へと拡がっている。そのため、金融庁では、インシデント発生時におけるサイバーレジリエンスの強化に向けた取組みを金融機関に促していく。

【③サイバーセキュリティ確保に向けた組織全体での取組】

経営層の積極的な関与の下、組織全体でサイバーセキュリティの実効性の向上を促す（セキュリティ人材の育成含む）。

【④関係機関との連携強化】

サイバー攻撃等の情報収集･分析、金融犯罪の未然防止と被害拡大防止への対応を強化するため関係機関（ＮＩＳＣ、警察庁、公安調査庁、金融ＩＳＡＣ、海外当局等）との連携を強化する。

【⑤経済安全保障上の対応】

政府全体の取組の中で、機器･システムの利用や業務委託等を通じたリスクについて適切に対応を行う。

（3）オペレーショナル・レジリエンスについて

2021 年 3 月 31 日にバーゼル銀行監督委員会による「健全なオペレーショナル・リスク管理のための諸原則の改訂」として「オペレーショナル･レジリエンスのための諸原則」、「オペレーショナル･リスク管理のための諸原則」の２つの原則が公表された。前述のサイバーセキュリティ強化に向けた取組方針 Ver.3.0 の「新たなリスクへの備え」の中でも『サイバーレジリエンスの強化』が謳われているので、上記２原則の内、オペレーショナル･レジリエンスについて説明する。

システムリスクはオペレーショナル･リスクに分類されるが、ここ数年、オペレーショナル･リスク管理に関する考え方やアプローチが大きく変化している。すなわち、オペレーショナル･レジリエンスという概念の登場である。オペレーショナル･レジリエンスは、「混乱下においても銀行の重要な業務を継続的に運営する能力」を指しており、2018 年に英国金融規制当局により初めて提示され、21 年 3 月にバーゼル銀行監督委員会が「オペレーショナル･レジリエンスの諸原則」を公表した。その目的は、金融システムの重大な運用上の失敗を引き起こす可能製のある、パンデミック、サイバー攻撃、技術的欠陥や自然災害などのイベントによる業務運用への影響を吸収する能力を強化することにあり、昨年から今年にかけてみずほ銀行グループの大規模障害に象徴されるように、現在金融機関に対して強く要請されているものである。

オペレーショナルレジリエンスとは、テロやサイバー攻撃、自然災害等の発生時においても、重要な業務を継続できる能力を言うが、業務中断が起こり得ることを前提に、その影響が許容水準内に収まるよう態勢整備を求める

ものである。ＢＣＰ等の個別のプロセス整備だけでなく、業務中断による影響の軽減･緩和、初動･回復に繋げるキャパシティの確保等、包括的な検証と態勢整備が求められている。想定する問題事象とその対策を纏めるといったリスク管理的アプローチだけでなく、失敗に至る原因を事前に想定し、因果関係を遡りながら脆弱性を除去するリバースエンジニアリング的アプローチに基づくもので、組織横断的な取組にあたり、経営陣のトップダウンによるコミットメントを求めている。

ＩＴシステムへの依存度の高まりやサイバー攻撃の増加、大規模システム障害やパンデミックの発生等、近年のオペレーショナル・リスクを取り巻く環境変化、業務プロセスの相互依存度、ひいては金融システム全体の相互関連性の高まり。これらを踏まえると、未然に事故や障害を「防ぐ」ための態勢整備だけでは不十分であり、オペリスク管理を尽くしてなお、業務中断が発生しうる現実に向き合う必要がある。非現実的な‘zero tolerance’に拘泥するのではなく、現実的に甘受可能な許容水準を検討･設定することが重要ということ。

すなわち、重要な業務とその遂行に不可欠な経営資源を特定し、それらの相互依存関係を整理する。重要な業務に関して、業務中断やその影響時の許容可能な水準を設定し、シナリオ分析や訓練を通じて、上記水準が適切であるかを検証し、必要に応じ追加的措置を講じる。以上を経営陣のコミットメントの下、組織横断的に反復継続することが必要となる。

クラウドサービスの利用の広がりや、ＦｉｎＴｅｃｈ企業等と連携した決済サービス等が拡充する中、外部委託業務や連携サービスを含めた業務プロセス全体を実効的に管理し、オペレーショナル･レジリエンス（業務の強靭性）を確保する重要性が高まっている。サイバーセキュリティに関しては、外部委託先に対するサイバー攻撃により顧客･業務データを窃取または破壊される事案や、連携サービスの脆弱性を悪用され顧客資産を窃取される事案が発生するなど、金融機関がリスク管理を高度化すべき範囲が拡大している。このため、リスクが高いと考えられる金融機関に対して、検査等で情報セキュリティ特にサイバーセキュリティの実効性を検証するほか、規模を拡大したサイバー演習を通じて、事案発生時における金融機関の対応･復旧能力の向上を図る必要がある。

◇研究報告　2

「銀行勘定系システムの現状と課題　～環境変化と変わらない重要性～」

会員番号　436 大石正人

（はじめに）

銀行は預金取扱金融機関のひとつですが、銀行法上もあるいは機能上も、預金という本源的機能をもとに、貸出（信用仲介）、為替・送金や決済の役割を担っています。

（銀行のサービスライン）

従来型のフルバンキングサービスは多岐にわたりますが、それらのサービスの一部は銀行間のネットワークを通じて実現されます。つれてこうした業務を支えるシステムも、対外接続系、資金証券系・国際系、あるいは情報系システムや営業店システムなど行内系システムなど多岐にわたりますが、その中核にあるのが勘定系システムであることは変わりません。

銀行の勘定系システムは、第１次から第３次までのオンラインシステムの世代交代を経て、変貌を遂げていま

すが、こうしたなかで以下のような取り組みを進めてきました。

（勘定系システムをめぐるこれまでの取組み）

第一にアウトソーシングが進展し、その比率は９割以上に達しています。第二に地域金融機関では業態内での共同化が進展していることも無視できません。第三にさらに進んで最近はクラウド化に踏み切る動きもみられています。こうしたなかで、次のように対処が必要な様々な課題に直面しています。

（勘定系システムをめぐる年来の課題）

１）メインフレームを主体としたシステムの構築、運営が主体ですが、高信頼性と高コストの両立が困難です。

２）ＩＴベンダーとの協業と共同化という面は、特定銀行をベースにした勘定系システムパッケージの活用が主流で、システムを稼働させるベンダーロックインのリスクがあります。

３）ＩＴ技術の革新、という意味では、オープンイノベーションの採用を試みる動きが見られています。

４）銀行の経営環境、収益構造の変化の面では、企業などは資金余剰主体に、調達手段も多様化するなかで、預金貸出と利差を活用した収益モデルから手数料主体に転換が必要となっています。

（銀行経営を巡る環境変化と対応）

１）装置産業としての銀行、という面では、物理的な店舗やシステムが固定費として収益の圧迫要因になりうるため、メガバンクを始めとしてコスト構造改革を続々と打ち出しています。年来のシステム更新を達成した途端に、リテール事業のインフラとして減損処理に踏み切った事例もみられます。

２）非来店型サービスの拡充を図る動きも活発です。ネットバンキングはもちろんのこと、最近はアプリ活用サービスもスマホファーストのなかで存在感を増しています。他方で、店頭改革も様々な形で進められており、銀行内銀行方式の活用による店舗ネットワークの再編やコロナ禍で非接触対応も加速した感があります。

３）決済サービスの多様化、新規参入も相次いでいます。例えばATM専業銀行や、銀行業への異業種参入が相次ぐほか、キャッシュレス決済、Fintech、オープンAPI、あるいはエンベデッドファイナンス、といった、金融のアンバンドリング、あるいはリバンドリングの荒波が押し寄せています。旧来のフルバンキングからすれば、結局は「良いとこ」どりでは、との印象はぬぐえませんが、中央銀行もフィンテック研究の手を緩めないなど、時代の趨勢を端的に表しています。

４）政府の成長戦略計画を踏まえた競争政策の観点から、公取委が経済分析室を設置したり、銀行間サービスの手数料水準の妥当性など、「モノをいう」機関として存在感を増しています。

（勘定系システムは「土管」になってしまうのか）

それでは銀行の勘定系システムが情報通信キャリアのように「土管」と呼ばれる存在とみなされてよいのか、といえば、実は以下のように銀行口座で日々当たり前のように処理されていることが、国民生活の基盤をなしていることを忘れてしまってはいけない、と考えます。例えば以下のような点を再認識頂くことが大切です。

１）経済主体の資金管理（送金、収納）のアウトソーシングの動きについて、サービス享受者である預金者は必ずしも意識していませんが、実は取引先ごとの個別対応も幅広く残存していて、なくなると大変困るのです。例を挙げると、企業、事業者の場合は給与事業体内の資金管理、商業取引、資金調達、地方自治体や公営事業体の場合は、公共料金の収納管理や指定金融機関制度の存在（割に合わないので、金融機関から返上の動きもみられます）、家計の場合は現金、財やサービスの購入、住宅ローンなど、です。

２）銀行間の決済の利便性も見逃してはなりません。内国為替決済制度には全銀システムが支えになっています

が、メガバンク相互では個別決済も併用されています。また資産運用市場や市場取引も含めて、その他の国内資金決済システムや、ロシアへの金融制裁手段として話題になったSWIFTのような国際取引にかかる決済サービスの存在も重要です。

3）店舗やATMネットワークが充実していることで、転居先、旅先、外出先でも現金の出し入れや買い物の決済など、銀行サービスを途切れなく利用できる環境が提供されています。

4）取引銀行は、かねて会社の経歴書記載項目です。口座保有がその事業体の信用度を表象しているのはなぜなのか、社会的ステータスの意味合いを今一度考えてみる必要があります。

（勘定系システムの安定稼働～障害の影響と対処）

以上のような利便性をきちんと提供し続けるためにも、銀行サービスの中核的機能を支える勘定系システムの安定稼働は大前提となります。一刻も止めてはならない、という考え方が日本独自の過剰品質要請である可能永はありますが、利用者利便の確保のためには、改めて安定稼働の基盤を再確認する必要があります。

1）影響の及ぶ範囲は、冒頭の複雑多岐なシステム構成に起因し、窓口、チャネル（ＡＴＭ、ネットバンク）、送金や口座振替、遅延と不整合など様々なケースが考えられます。

2）原因についても、システム開発時や提供された市販ソフトの潜在バグ、システム上限値、ネットワークや機器障害、手順ミス、システム移行時の考慮不足ないし不測の事態発生が想定されます。またテクノロージーの深化とともに、様々な事象の複雑化が技術面だけでなく、ITシステムの提供元がマルチベンダー化していることで、対処が難しくなっています。

最近発生した代表例はメガバンクで1年間に12件ものシステム障害が起こったケースですが、専門誌の執筆者がシステム開発プロジェクト完了後の「振り返り」に見立てて「ポストモーテム」と題した刊行物も参考になるやもしれません。

3）システム障害の背景（原因のさらに上流にある潜在的な問題）としては、システムや機器の老朽化、システム統合や移行といったイベント起因、点検の不備、臨時作業や異例処理時の考慮不足など、障害が起きるべくして起きてしまう要因について、ITガバナンス的な視点からも考察が必要です。

4）直接的な障害発生抑止の施策、再発防止といった対処としては、あたりまえのことをきちんとやるしかなく、統合的な運用監視（開発から運用移行時の引継も重要）、システムや運用管理のフィージビリティを含めた品質と点検、稼働後のモニタリング体制、システムや機器の適時の更新、計画的なシステムダウン訓練、全社的なコンティンジェンシープラン、移行リハーサルの実施など、数え切れませんが、それだけ高い信頼性を求められる重要インフラだともいえます。なおこうした前提として、システムの開発、運用を担う人材の育成・確保、資源の確保、IT部門だけでなくシステムを利用するサービス部門を含めたマネジメントの強固さ（レジリエンシ―）の確保も極めて重要です。アウトソーシングやクラウド化の進展で、人材のスキルセットがどうあるべきか改めて考察を迫られています。

（さいごに）

改めて「銀行勘定系システムの変わらない重要性」という点から、今回の報告を振り返ります。

1）取引結果や時限性の高信頼性、は勘定系システムの最も重要な観点です。処理手順、処理能力など、勘定系システムを運用する主体は、自らのプレゼンスに見合った投資、体制を整備する必要があります。技術基盤をわが物

にするとともに、システム部門の体制整備や担い手の確保、安全投資余力を持つ（安全投資枠を確保しているメガバンクの事例もあります）ことも大切です。

2）口座保有の利便性とコストに見合った収入確保の道も、今後とも重要です。なかなか現実には難しいですが、例えば 採算を明示したうえで利害関係者の理解を得る戦略の妥当性は、このところの 競争政策の観点からの「提言」に先回りして対応していくことの重要性を示しています。一方で当局による被監督コスト、世間を含めた品質過多要求の可能性（数分でも ATM を止めちゃダメ、などの要求）についても、解決の道筋を見出していかなくてはなりません。

3）個別システムと決済システムの安定稼働が信頼性の基盤、であることも忘れてはなりません。銀行は、勘定系システムを通じてサービスを提供している、重要インフラの担い手（電気・ガス・水道・通信などと並ぶ）です。資金決済サービスは生活や経済を支える血液循環といえます。大規模災害で地域が被災した時にも金融措置で支えるのは銀行（保険会社、証券会社などとともに）です。

4）一国の信用システムの維持は担い手である銀行の健全性が基礎になります。振り返ると、いつもは何の支障もなく銀行サービスを利用していた(business-as-usual の）状況が、一旦 信用不安に見舞われると、開店前から銀行店舗に列をなすなど、人心が動揺する経験を 1997 年（山一証券自主廃業など）、2008 年（リーマンショック）と潜り抜けたはずです。もし銀行口座が凍結されたら（あってはなりませんが、世界を見渡すと事例があります）、当たり前で意識していなかった銀行サービスの提供のありがたみを感じるはずです。

いずれにしても、はやりのブティック的な金融サービスに目を奪われ、勘定系システムを単なる「土管」だと考えるのは不適切です。今回の報告が、要路の皆さんにおいて、勘定系システムの変わらない重要性を再認識していただくきっかけになれば幸いです。

◇**研究報告 3**

「リスクマネジメントフレームワークについて」 会員番号 1281 宮本 茂明

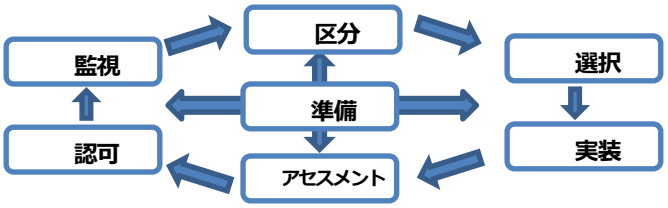
今回の北信越支部例会で先に報告いただいた事項を考える際、リスク管理をいかに行うかということが重要になってくると考えます。米国政府では「NIST SP 800-37　Revision 2：組織と情報システムのためのリスクマネジメントフレームワーク –セキュリティとプライバシーのためのシステムライフサイクルアプローチ–」に基づき、重要インフラを含め、政府機関システムについて、具体的に体系化されたアプローチでリスクマネジメントを推進しています。このフレームワークの概要を報告し、例会参加者とリスクマネジメントについて、意見交換を行いました。

（米国政府におけるリスクマネジメントフレームワークの目的）

重要インフラの情報システム、コンポーネント製品、サービスがシステム開発ライフサイクルを通じて十分に信頼でき、経済および安全保障上の利益を支えるのに必要なレジリエンスが提供されるように、強化していくことを目的としています。

自動化の拡大、高価値資産の保護を強化するための米国政府システムとネットワークの統合、標準化、最適化などによるシステムの近代化（モダナイゼーション）が、米国政府の重要な目標となっています。

（リスクマネジメントフレームワークの構造）



・リスクマネジメントの**準備**：セキュリティとプライバシーのリスクを管理するための背景・前提・共通認識当、優先順位を確立することにより、組織レベルおよびシステムレベルの観点からリスクメネジメントを遂行する準備を行います。

・情報システムの**区分**：損失のインパクト分析に基づいて、システムと処理する情報を区分します。

・セキュリティ管理策の**選択**：システムの初期のセキュリティ管理策セットを選択し、必要に応じて管理策をテーラリングして、リスクアセスメントに基づいてリスクを受容可能なレベルまで低減します。

・セキュリティ管理策の**実装**：セキュリティ管理策を実装し、システムおよびその運用環境内で管理策がどのように採用されているかを説明します。

・セキュリティ管理策の**アセスメント**：セキュリティ管理策をアセスメントして、管理策が正しく実装され、意図したとおりに動作し、セキュリティとプライバシー保護の要件を満たすことに関して望ましい成果が得られるかどうかを判定します。

・情報システムの**認可**：組織の運営と資産、個人、他の組織、および国家に対するリスクが受容可能であるという判定に基づいて、システムまたは共通の管理策を認可します。

・セキュリティ管理策の**監視**：システムおよび関連する管理策を継続的に監視し、管理策の有効性のアセスメント、システムと運用環境の変更の文書化、リスクアセスメントとインパクト分析の実施、およびシステムのセキュリティとプライバシー保護態勢の報告を行います。

リスクマネジメントフレームワークの中で、ツール等を使い自動化できるところは効率的進めるアプローチをとるようにしており、リスクマネジメントの自動化技術情報を今後フォローしていきたいと考えています。

<参考情報>

- NIST SP 800-37　Revision 2「Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy -」（2018 年 12 月）
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

以上

<目次>

2022.7

注目情報（2022.6～2022.７）

■ 情報セキュリティ白書2022（IPA）

IPA（独立行政法人情報処理推進機構）では、「情報セキュリティ白書」を 2008 年から毎年発行しています。本白書は、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他、その年ならではの象徴的なトピックを取り上げています。

国内外の官民の各種データ、資料を数多く引用しトピックを解説しており、情報の網羅性と参照性の高さが特長で、情報セキュリティ分野の全体把握が容易です。

また、本白書は次のような使途で利用されています（2021 年版の読者アンケートより）。

学習・自己研鑽
対策強化・予算策定等、上位者への説明資料
新人研修・従業員教育
所属組織の注意喚起、啓発資料
教材、人材育成プログラム
資格取得、試験対策
セミナー・講演資料用

URL：https://www.ipa.go.jp/security/publications/hakusyo/2022.html

■「サイバーレスキュー隊（J-CRAT）活動状況 2021年度下半期」を公開しました（IPA）

IPA は、標的型サイバー攻撃の被害拡大防止のため、2014 年 7 月 16 日、経済産業省の協力のもと、相談を受けた組織の被害の低減と攻撃の連鎖の遮断を支援する活動としてサイバーレスキュー隊（J-CRAT：Cyber Rescue and Advice Team against targeted attack of Japan）を発足させました。

最新の活動状況については、以下の年度および半期報告と、公開する技術レポートを参照下さい。
URL：https://www.ipa.go.jp/security/J-CRAT/index.html

<目次>

2022.7

【 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270回	日時	2022 年 9 月 2 日(金) 18:30～20:30
	場所	オンライン（Zoom ウェビナー）
	テーマ	ISMAP の現状について
	講師	山口達也　氏
	講演骨子	ISMAP については、施行後 2 年が経過しました。この 2 年間でも細かなものも含め様々な修正が入り、2022 年 6 月には ISMAP-LIU という新しいスキーム案も公表されました。また、現場においても政府機関のみならず民間での活用も確実に広がりつつある状況にあります。本講演においては、この 2 年間で制度が変わったところ、現場における活用事例等を中心に紹介すると共に、現在検討されている新しいスキーム等の概要についても月例研究会開催時点における公表情報を元に解説します。
	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/270.html

<目次>

2022.7

【 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.saaj.or.jp/index.html
・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			2022.7
	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
7月	5：支部助成金支給 14：理事会	9-10: 第 39 回システム監査実務セミナー (日帰り 4 日間コース後半) 13：第 269 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） 6：中間期会計監査	1：秋期 CSA・ASA 募集開始～9/30 18：第 38 回 CSA フォーラム	
9月	8：理事会	2:第 270 回月例研究会 30:秋期 CSA・ASA 募集締切	
10月	13：理事会	7:第 271 回月例研究会	
11月	9：　予算申請提出依頼（11/28〆切） 支部会計報告依頼（1/9〆切） 10：理事会 16：2023 年度年会費請求書発送準備 28：会費未納者除名予告通知発送 28：本部・支部予算提出期限	 調整中：第 272 回月例研究会 中旬：秋期 CSA 面接 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	
12月	1：　2023 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：2023 年度予算案 会費未納者除名承認 第 22 期総会審議事項確認 10：総会資料提出依頼（1/9〆切） 14：総会開催予告掲示 20：2022 年度経費提出期限	12：第 273 回月例研究会 16：　CSA/ASA 更新手続案内メール 〔申請期間 1/1～1/31〕 23：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 12：理事会：総会資料原案審議 28：2022 年度会計監査 31：償却資産税・消費税申告 31：総会申込受付開始（資料公表）	1-31：CSA・ASA 更新申請受付 21：春期 CSA・ASA 募集案内 〔申請期間 2/1～3/31〕	6：支部会計報告提出期限
2月	2：理事会：通常総会議案承認 28：2023 年度年会費納入期限	2/1-3/31：CSA・ASA 春期募集 下旬：CSA・ASA 更新認定証発送	17：第 22 期通常総会
	前年度に実施した行事一覧		
3月	4：年会費未納者宛督促メール発信 10：理事会 28：法務局：資産登記、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 4:第 265 回月例研究会	
4月	14：理事会	18:第 266 回月例研究会 初旬：春期 CSA・ASA 書類審査 中旬：春期 ASA 認定証発行	17:春期情報技術者試験・情報処理安全確保支援士試験
5月	12：理事会	18:第 267 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 9：理事会 21：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 7/11） 30：助成金配賦決定（支部別会員数）	上旬：　春期 CSA 面接 15:第 268 回月例研究会 18-19: 第 39 回システム監査実務セミナー (日帰り 4 日間コース前半) 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）

<目次>

2022.7

【 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

2022 年の会報年間テーマは

「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>

2022.7

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】　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：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>