認定 NPO 法人
日本システム監査人協会報

2023 年 9 月号
No 270

No.270（2023 年 9 月号）<8 月 25 日発行>

(注目情報)
サイバーセキュリティ経営可視化ツール Ver2.1 公開（IPA 公表）

巻頭言

『CSA/ASA 資格のアピールを！』

会員番号　2581　斉藤茂雄（副会長　CSA 利用推進 G）

話題の生成 AI で「公認システム監査人資格」について尋ねてみました。数週間前の“チャット GPT”では「公認情報システム監査人（CISA）」のこととの解説でした。本稿執筆時点では、システム監査人についての一般論の解説になっていて、少し進化したようですが、当協会の認定資格とは認知されていません。因みに Google の“Bard”では当協会の認定資格との説明があり、マイクロソフトの”Bing チャット“ではさらに正確な解説になっており、少し安心しました。

私が担当している「CSA 利用推進 G」は、公認システム監査人（CSA）・システム監査人補（ASA）資格の認知度向上と活躍の場の増大を目標の一つにしていますが、まだまだ不十分です。今回はささいな内容ですが、認知度向上のため、すでに資格をお持ちの方に以下 2 点をご案内します。

1．お名刺への資格ロゴの表示
　資格取得者の方は可能であれば皆様の名刺に、資格名とロゴを表示して名刺交換時等に資格についてご紹介ください。
　【ロゴ使用規定】: https://www.saaj.or.jp/csa/csalogokitei.html

CSA のロゴ　ASA のロゴ

2．資格認定カードの作成
　CSA/ASA 資格者は資格認定カード（有償・有効期限あり）の作成が可能です。資格証明用として携帯しご利用ください。
　【認定カード申請手続き】: https://www.saaj.or.jp/csa/pdf/nintei_card_shinsei.pdf

認定カードサンプル

協会では現在秋期の CSA/ASA 資格取得者を募集中（目次参照）です。未取得者の方の資格取得は勿論ですが、お知り合い・後輩等にお薦めいただくなど資格者増に、すべての会員の方のご協力をお願いいたします。

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。

2023.8

めだか　【　この変化の時代にシステム監査が目指すもの - 日本を買う - 】

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。

資料である「中国人が日本を買う理由」を読めば、今、何故、中国の富裕層が日本に移住するケースが増えているかがわかる。例えば、“上海の激しいロックダウン（都市封鎖）を目の当たりにして、このまま中国にいたらどうなるんだろうと思うと恐ろしくなり、日本への移住を決意した。”という人がいる。中国では、“中央の指示が 1 回なら、その下は 2 回、さらにその下は 3 回というように下へ行けば行くほど、どんどん（締め付けは）厳しくなってくる。”という。つまり、“いちばん下の人に強い権限が与えられ、法律などを持ち出しても、法律が通用しない、だからこの国は怖い。” という。そして、“ストレスのない生活が送れる日本に来られて本当に良かったです。”といっている。

この人のように、コロナ禍以降、日本への移住を決意した中国人は少なくない。この人の場合は、ビジネスビザで入国し、就労ビザに切り替えたが、近年、日本に移住する富裕層は、「経営管理ビザ」を取得することが多いという。10 年で「経営管理ビザ」の取得者は約 3 倍になり、2022 年は 6 月までの半年ですでに 1 万 4615 人となっている。日本で事業をしようとする中国人が増えたことが表れているという。在日中国人が経営する不動産会社の多くは、特定の行政書士と業務提携し、顧客に対してビザ取得に関するサポートを行っている。来日を希望する人は、ビザの取得と不動産取得をほぼ同時進行で行うからということだ。

ここ数年、日本は文句のつけようのない移住先として認識されている。カナダやイギリスは英語が通じるが中国から遠くて冬は寒いし、シンガポールは言葉が通じるけれども生活コストが高い。その点、日本は近いし、（生活コストが）安い、（子どもが一人で外出しても）安心、安全。食事も安くて美味しく、コスパがいい。それに、日本語はよく分からなくても漢字の標識や看板である程度は理解できるし、顔つきも似ているので街に溶け込んで緊張感が少ない。気候風土も似ている。その上、不動産の利回りも安定している。また、彼らが日本で不動産を買う目的として「老後の不安」をあげているという。ふつう、「日本買い」の背景は、「政治」とは関係なく、人生につながっていると思う。

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：「中国人が日本を買う理由」中島恵 著 日経プレミアシリーズ

（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>

2023.8

【投稿】生成ＡＩ等の活用が進むなかで、内部統制やシステム監査はどう臨むべきか

会員番号　0436 大石正人

生成ＡＩの盛行でさまざまな分野でのＡＩ活用が一段と進展しているようです。少し前には人間の思考を超越する汎用ＡＩの登場（いわゆるシンギュラリティ＝技術的特異点の問題）が取りざたされていましたが、手軽に活用できる生成ＡＩが相次いで登場し普及し始めたことで、その活用実績を競う風潮が目立ち、いわば「ＡＩ狂騒曲」的に大流行りの状態です。今や研究機関に止まらず、企業も自治体や官公庁も（教育機関までも)、「生成ＡＩの活用は検討しません」とは言いづらくなっている様子です。

リアルタイムでの活用現場にいないため、以下は巷の雑誌やネット情報を大雑把に眺めている範囲で、ＡＩの活用がリスク管理やシステム監査にとって、どんな意味合いを持つのか、素人目線で考えてみたいと思います。

第一に、システム監査のテーマや対象として、所属組織におけるＡＩや生成ＡＩの導入（以下、生成ＡＩ等の導入）をどう考えればよいか、という観点です。

これは従来からある「新技術の導入」あるいは「新手法の活用」にかかるリスク管理、ないしはプロジェクト管理、に類似するものと捉えることができるのではないでしょうか。

新技術の導入、と捉えた場合すぐに思いつくのは、１）生成ＡＩ等の活用に伴うリスク特性の評価が行われ、それに基づく対策が講じられているか、２）組織体として生成ＡＩ等の活用にかかるガイドラインを策定し、組織内に周知しているか、３）ガイドラインの遵守状況をモニタリングする責任部署が定められ、定期的に組織全体としての遵守状況を確認し、経営陣への報告や、問題のある活用事例については該当部署に是正を求めているか、などの諸点です。

生成ＡＩ等のリスク特性として、すでに幅広く指摘されているポイントには、例えば、業務面で秘匿すべき組織内の機密情報、個人情報の入力や、知的財産その他の侵害有無、生成ＡＩ等の活用により導き出された結果の妥当性の検証、などが挙げられますが、活用シーンの変化、深化に合わせて、さらに掘り下げて捉えていくことが求められます。

第二に、企業としての内部統制システムやガバナンスの一環として「生成ＡＩ等の活用」を位置づけ、利害関係者に対し、企業としてのガバナンスコードや準拠しているガイドラインを提示できるよう、説明責任を負える体制が構築できているか、の確認です。

既に著名な政治哲学者や経営学者、テクノロジーの専門家などから問題提起されている通り、生成ＡＩ等の技術が悪用されることへの懸念が表明されています。

毎度のことながら、ともすると産業振興や新技術へのキャッチアップにばかり目が向きがちな我が国の政府や中央省庁には、こうした倫理なり民主主義社会への脅威なりについての危機感が、概して薄く感じられる傾向にあります。しかしＳＤＧｓなどのグルーバルな視点での事業展開や、様々な価値観を持った利害関係者との対話において、生成ＡＩ等の活用につき、説得的な対外説明ができることは、組織体の価値にも、中央省庁の場合には政府の信頼性にも、大きな影響を及ぼす可能性があります。生成ＡＩ等の活用をめぐる市場の動向や流れに任せた業務運営は、対応を誤ることで組織体の信任を傷つける懸念があります。

このため、内部統制システムやガバナンスの有効性、という観点から、こうした問題意識を踏まえた対応が組織体としてできているのか、継続的に確認することは極めて重要です。

第三に、内部統制やシステム監査業務における生成ＡＩ等の活用方針の検討です。第一、第二に述べた通り、自組織内での活用事例の有無にかかわらず、今後、内部統制や内部監査・システム監査業務において、生成ＡＩ等の活用事例がますます増えていくことが予想されます。

代表的には独立監査人として会計監査などの業務を担う監査法人では、程度の差こそあれ、監査業務においてＡＩ的な手法を採用して、業務の効率化を志向していますし、業務部門が外部コンサルの支援を受ける中で、生成ＡＩ等を活用する事案が増えてくるものと予想されます。

システム監査を担う部門においても、自組織内における事例や、他の組織体におけるこうした手法にかかる取り組み事例につき、積極的に情報収集を行い、自らの業務への活用可能性とともに、リスク要因も検討することが早晩必要になってくると思われます。

このため、組織的な生成ＡＩ等の活用指針が定められ、活用にかかるリソースの手当てが検討される段階では、内部統制やシステム監査でも他の業務部署と同様に、情報の提供にとどまらず活用部署の一つとして、存在感を主張することも大切だと考えます。

第四に、以上の前提として、内部統制やシステム監査の担い手におけるＡＩリテラシーの向上の必要性、が指摘できます。

すでにＤＸ（業務のデジタル変革）への取組み、あるいはアジャイル手法によるシステム開発などに対する監査業務でも認識されている通り、内部統制やシステム監査を担う部門においては、新たな手法に対応したスキルアップの機会が少ないように感じます。

こうした背景には、内部統制やシステム監査業務の担い手は多くの場合、それまでの経験が最先端というより、旧来支配的だったシステム開発やプロジェクト管理の手法、あるいは従来型の業務改革の経験がベースになっている傾向が強いことがあると推察します。

生成ＡＩ等の活用が自組織内に広まると、第一に述べた通り、生成ＡＩ等活用を前提とした業務の妥当性検証などが、システム監査等のスコープに入ってくるだけでなく、内部統制やシステム監査の分野でも、こうした活用技法を前提とした業務プロセスの再構築が必至となる可能性が高い、と見込まれます。

第三に述べた部門としてのリソース配分の主張と併せて、生成ＡＩ等の活用を前提として内部統制やシステム監査のスキルシートの見直しを進めながら、監査従事者に対する継続的なスキルの蓄積、あるいは必要があれば外部のノウハウも活用したコソース型の監査の取組みなども、検討が望まれます。

いずれにしても、生成ＡＩ等の活用が自組織にとって優先度の高い取組みになれば、内部統制やシステム監査業務部門としても、対象業務の見直しやその優先度の組み換え、その前提となるリソースの配分や要員のスキルマップの見直しは避けられないでしょう。

生成ＡＩ等の活用が急速に進む中で、すでに先進的な組織においては、内部統制システム運用の一環として、生成ＡＩ等のリスク評価やシステム監査のあり方につき、再検討に着手しているものと推察されます。その意味で、ここで改めて言及するまでもないのかもしません。

しかし繰り返しにはなりますが、有識者から警鐘が相次いで鳴らされるほど、生成ＡＩ等の活用はこれまでにないインパクトをもって、人倫や労働を含む人間社会に根本的な変革をもたらす懸念があります。内部統制やシステム監査業務も、ある意味でこれまでとは次元の違う課題に直面している予感がしています。

このため、業務部門における生成ＡＩ等の活用の進展と歩調を合わせて、内部統制やシステム監査としての指針や取組み方針を策定することが求められます。先端的な取組みを進めようとしている組織体ほど、所管省庁の方針や同じ業界内の横並び的な動きを待たずに、自らの意志と責任において検討を急いでいただけるよう、心から願ってやみません。

併せて、内部統制やシステム監査を担う分野からも、生成ＡＩ等の活用にかかる様子見ではなくむしろ、プロアクティブで先回りした情報発信や問題提起が増えていくよう、強く期待しています。

<目次>

2023.8

投稿　【　情報システムに用いられる暗号技術の安全性評価　】

会員番号　2837 山本慎一郎　（九州支部）

去る 7 月 26 日に、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」の改定に関するシンポジウムが開催されました。

CRYPTREC とは、デジタル庁などの省庁、及び情報通信研究機構などの行政法人が共同で運営する、暗号技術の適切な運用方法等を調査・検討するプロジェクトです。主として、電子政府（デジタル技術を活用した行政機関）で用いる電子機器の暗号技術を対象としていますが、その資料は民間企業においてもひとつの指針となっており、情報システムのセキュリティに関する重要なポイントとなっています。

情報システムの安全性と暗号技術

まず、そもそもの問題として、情報システムの安全性と暗号技術がどのように関わっているかを見てみます。

例えば、多くのシステムで採用されているアカウント機能。ID やパスワードを入力して、システムにログインするものですが、これらの ID やパスワードがサーバ上にそのまま保存されることはまずありません。多くの場合、「ハッシュ化」と呼ばれる、元のデータに戻せない暗号化が施されて保存されています。これにより、『システムの管理者がデータを盗み見ても、利用者が入力するパスワードを知ることができない』などの安全性が確保されています。

次に、ネットワークに目を向けてみます。近年爆発的に普及したテレワークなどの勤務形態では、「VPN（Virtual Private Network）」と呼ばれる技術がよく利用されています。この技術では、インターネットという大衆に公開されているネットワークを使いながらも、送受信するデータを暗号化することで、第三者が見てもどんなデータか分からない仕組みになっています。なお、こちらの場合は、先ほどの元に戻せないハッシュ化ではなく、受け取った側が元に戻せるような、原始的な意味での「暗号化」が施されています。

暗号技術の隙とサイバー攻撃

一方で、「VPN」と聞くと、近年のランサムウェアを用いたサイバー攻撃の原因として、ニュースでよく耳にします。ですが、ほとんどの VPN では、『接続する際のアカウントの認証』と『認証した後のデータの暗号化』がセットになっています。これだけ聞くと、サイバー攻撃の被害に遭う要素はないように思えます。

ですが、実際には『接続する際のアカウントの認証』が無力化している場合があります。大別すると 2 つのパターンがあり、ひとつは利用する機器（ルータ）のパスワードが初期設定のままになっているパターン、もうひとつは利用する機器のファームウェア（OS）が古く脆弱性が残ったままになっているパターンです。これらの弱みに付け込み、攻撃者は管理者になりすまして VPN へ侵入し、サイバー攻撃を行います。

いずれのパターンでも、根本的な原因はシンプルなものです。ですが、パスワードが推測されやすかったり、脆弱性により暗号技術が使われないルートで侵入されてしまっては、どれほど優れた暗号技術でも無力です。この点については後程も触れますが、**暗号技術の種類だけで安全性は評価できない**という点には、注意が必要です。

CRYPTREC 暗号リストについて

では改めて、CRYPTREC が今回改定した資料、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」について見ていきます。

CRYPTREC 暗号リストには、3 つの異なるリストがあります。

1. **電子政府推奨暗号リスト**

これは文字通り推奨されている暗号技術のリストであり、CRYPTREC によって安全性や実装性能が確認されているものになります。端的に言えば、『**現時点では、安全で効果的と考えられる暗号技術**』のリストになります。

2. **推奨候補暗号リスト**

こちらは、将来的に推奨されるようになる可能性のある暗号技術のリストになっています。現時点では、安全性や利用実績などに十分な根拠がないものの、定期的な調査等でそれらが確認されれば、先の電子政府推奨暗号リストへ昇格されます。

3. **運用監視暗号リスト**

最後のリストは、逆に解読されるリスクが高まるなど、『**安全性が十分でなくなった暗号技術**』が記載されるものになっています。電子政府推奨暗号リストに記載された暗号技術であっても、コンピュータの進歩や暗号解読方法の研究などにより、安全でなくなることがあります。CRYPTREC では、そのような「危殆化」についても常に調査しており、安全性が不十分と判断されれば、電子政府推奨暗号リストから降格されることになります。

（参考　https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022.pdf）

このような 3 つのリストが、CRYPTREC 暗号リストには定められています。システム監査人として、特に注視すべきなのは、最初に挙げた**「電子政府推奨暗号リスト」**、及び最後に挙げた**「運用監視暗号リスト」**の 2 つになります。これらの活用方法について、詳しく考えてみたいと思います。

電子政府推奨暗号リストの活用方法

「電子政府推奨暗号リスト」は、先にも述べた通り、『現時点では、安全で効果的と考えられる暗号技術』のリストです。情報システムで利用されている暗号技術がこのリストに含まれているのであれば、**機能としては安全に設計されている**と判断できます。

ただし、機能として安全に設計されていても、設定や使用方法が誤っている場合には、安全でない状態になることがあります。例えば、どれだけ安全な暗号技術を使用していても、アカウントの貸し借りが横行していたり、退職者のアカウントがいつまでも残っていると、不適切な利用を許してしまうことになります。

また、前項でも触れたように、それまで安全だった暗号技術が、技術の進歩に伴って安全でなくなるケースもあります。例えば、2002 年度の資料では電子政府推奨暗号リストに記載されていた「RC4」という暗号技術は、2012 年度の改定で運用監視暗号リストに降格となり、今回の改定ではついに運用監視暗号リストからも削除されました。このように、いま安全な暗号技術が、5 年後、10 年後も安全であるとは限りません。

従って、「電子政府推奨暗号リスト」に記載されている暗号技術であるというだけで評価するのではなく、その**運用方法や安全性の動向も加味したうえで、総合的な判断を行う**必要があります。

運用監視暗号リストの活用方法

「運用監視暗号リスト」については、利用している時点で、システムの安全性に対して一定のリスクが存在していると考えるべきです。CRYPTREC 暗号リストにおいても、次のように書かれています。

“互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。”

（CRYPTREC 「電子政府における調達のために参照すべき暗号のリスト」より）

ただし、引用文にもある通り、システムの互換性を維持するために利用することについては、ある程度容認されます。一般に、情報システムの暗号技術を変更するためには、多大なコストが必要です。従って、部分的、段階的な移行が必要となります。このような移行期において、全体としての互換性を維持するために、一部のシステムで運用監視状態の暗号技術を利用することは容認される、というのが前述の考え方です。

もっとも、それはあくまでも移行を前提とした妥協であり、リスクが無くなるわけではない点には注意が必要です。システム監査人としては、**対象の組織がリスクを正しく認識しており、それに対して適切な管理を実施していること**を、確認する必要があります。

進歩する計算能力と 2030 年問題

システム監査を行う際のリスク評価については、CRYPTREC 暗号リストの活用がひとつの判断材料になることが分かりました。一方、中長期的な視点では、**「2030 年問題」**という問題点が指摘されています。

「2030 年問題」とは、端的に言うと、『**2030 年までに使用を終えるべき暗号技術について、新しい暗号技術への置き換えが、2030 年までに終わらない**』という問題です。CRYPTREC など各国の研究機関では、どの暗号技術がいつごろに安全でなくなるか試算を行っています。現在広く利用されている暗号技術でも、2030 年までに安全でなくなると目されているものがありますが、日本では対応が進んでいないのが実情です。

その結果何が起きるかというと、2030 年前後に、各組織で利用されている情報システムが、一斉に安全でなくなるということです。システム監査の面からは、安全性に関する評価が悪化することが予見されますし、それを踏まえて各組織が一斉に対応を検討するような事態になれば、事前に対応するよりも高いコストが必要となることも懸念されます。利用者側としては、システムベンダー側の対応を待つしかないのも事実ですが、現状の評価だけでなく、中長期的な安全性も考慮した評価、対策が望まれます。

おわりに

このように、情報システムの安全性において、暗号技術というのは非常に重要な役割を担っています。その一方で、システムの根幹部分にも深く関わっているため、最新の暗号技術に追従するのは容易ではありません。かといって、安全でない暗号技術を使い続けると、サイバー攻撃の被害に遭ったり、情報漏えいのリスクが高まるなど、システム全体の安全性が脅かされることになります。

加えて、暗号技術と聞くと、どうしても専門的な知識が必要と考えがちです。ですが、CRYPTREC 暗号リストなどを活用すれば、ある程度の判断は可能です。これらの資料も参照しながら、リスクやコスト、そして組織に求められる特性を踏まえて、情報システムの安全性を評価することが求められていると思います。

<目次>

2023.8

【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（9）

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

マイナンバー・カードと保険証の紐付けのトラブルが頻発しているが、最大の要因は IT 業界の人材の劣化にあると思われる。その元凶は 2003 年の「SI 認定制度」の廃止と 2010 年の「SI 登録制度」の廃止にあることは明らかであると思われる。国民生活の根幹をなす問題であるだけに、政府は緊急に「SI 認定・登録制度」を復活(租税特別措置法による優遇は切り離して良い)し、公共調達における指標・加点要素とするべきである。また、地方自治体も情報処理有資格者の人数を入札審査における加点要素とする条例を制定するべきである。

※システム導入においては、IT 技術だけではなく、業務知識も非常に重要である。その為には、公認会計士・税理士・弁護士・行政書士・司法書士・土地家屋調査士・弁理士などの士業も加点要素とする必要がある。

§2.消費税の本則課税の計算例

今回は前回の設例の解答から始める。(→文献[1-3])

〔設例 2.1〕C 社は製造業を営んでいる。2013 年 3 月期において、自動車の売上(税抜)は 4,900,000,000 であり、鉄道車両の売上(税抜)は 4,700,000,000 であり、個人向け不動産賃貸収入が 100,000,000 あった。また、受取利息が 300,000,000、受取配当金が 400,000,000 であった。固定資産の取得はなく、課税仕入(A)(税込)は 3,520,000,000、課税仕入(B)(税込)は 88,000,000、課税仕入(C)(税込)は 1,760,000,000 であり、全ての仕入先は課税事業者であった。 消費税率は 10%とする。

この場合について、以下の問いに答えよ。

(1)課税売上高を求め、区分経理の要否を判定せよ。

(2)区分経理で「個別対応方式」(消費税法第 30 条第 2 項第 1 号)による場合の納税額を求めよ。

(3)区分経理で「一括比例配分方式」 (消費税法第 30 条第 2 項第 2 号)による場合の納税額を求めよ。

(4)会計上の納税額を求めよ。

(5)(2)～(4)の場合、納税額の大小を示せ。

〔解答〕

(1)まず、各種の売上及び収入の判定を行う。

・自動車の売上　4,900,000,000　→　課税

・鉄道車両の売上　4,700,000,000　→　課税

・個人向け不動産賃貸収入　100,000,000　→　非課税

・受取利息　300,000,000　→　非課税

・受取配当金　400,000,000　→　不課税

よって、

(課税売上高(税抜))＝9,600,000,000＝**(課税標準)**　(2.1)

(非課税売上高)　＝400,000,000　(2.2)

よって、「課税売上割合」を K とおくと、

K＝9,600,000,000 / (9,600,000,000＋400,000,000)＝0.96　(2.3)

従って、課税売上割合は 96%であるが、(2.1)より課税売上高(税抜)が 5 億円を超えるので区分経理が必要。

(2)（課税標準に関する消費税額）＝9,600,000,000×0.1＝960,000,000　(2.4)

課税仕入(A)、課税仕入(B)、課税仕入(C)に対する仕入税額をそれぞれ a,b,c とすると、次のようになる。

$$\begin{cases} a = 3{,}520{,}000{,}000 \times 10/110 = 320{,}000{,}000 & (2.5) \\ b = 88{,}000{,}000 \times 10/110 = 8{,}000{,}000 & (2.6) \\ c = 1{,}760{,}000{,}000 \times 10/110 = 160{,}000{,}000 & (2.7) \end{cases}$$

よって、「個別対応方式」による場合の控除対象仕入税額は次のようになる。

(控除対象仕入税額）＝320,000,000＋160,000,000×0.96＝473,600,000　(2.8)

従って、納税額は次のようになる。

（納税額）＝960,000,000－473,600,000＝**486,400,000**　(2.9)

(3)「一括比例配分方式」の場合、控除対象仕入税額は

（控除対象仕入税額）＝（320,000,000＋8,000,000＋160,000,000）×0.96＝468,480,000　(2.10)

従って、納税額は次のようになる。

（納税額）＝960,000,000－468,480,000＝**491,520,000**　(2.11)

(4)「会計上の納税額」は、仮払消費税の全額が控除対象となるので、

(控除対象仕入税額）＝320,000,000＋8,000,000＋160,000,000＝488,000,000　(2.12)

従って、納税額は次のようになる。

（納税額）＝960,000,000－488,000,000＝**472,000,000**　(2.13)

(5)納税額の大小は次の通り。

（一括比例配分方式による納税額）＞**（個別対応方式による納税額）**＞**（会計上の納税額）**　(2.14)

※1.(2.9)及び(2.11)より、**(一括比例配分方式による納税額)**－**(個別対応方式による納税額)**

＝**491,520,000**－**486,400,000**＝5,120,000　(2.15)

★この差額は 5,120,000 もある。つまり、課税売上高が 96 億円の場合でも 512 万円の差異が生じている。仮に、課税売上高が 9600 億円の大企業の場合、その差額は 5 億 1200 万円に上る。これは企業経営者にとって、無視できるような差額ではない。

※2.(2.11)及び(2.13)より、**(一括比例配分方式による納税額)**－**(会計上の納税額)**

＝**491,520,000**－ **472,000,000** ＝19,520,000　(2.16)

★この差額は 19,520,000 にもなる。つまり、課税売上高が 96 億円の場合でも 1952 万円の控除対象外消費税額(営業外費用)が生じている。仮に、課税売上高が 9600 億円の大企業の場合、その控除対象外消費税は 19 億 5200 万円に上る。これは企業経営者にとって、深刻な問題であると思われる。

§3.新リース会計基準の公開草案 ～ 実は"骨抜き" ～ 趣旨を没却する例外条項が温存

新リース会計基準は 5 月 2 日に公開草案が発表され、パブリック・コメントは 8 月 4 日に締切られ既に公表されている。今回は団体から 32 通、(筆者も含めて)個人から 13 通のコメントが寄せられた。当初は IFRS16 に近いものになることが予想されていたが、実際の公開草案を見ると、不動産についてオン・バランス増えるものの、「例外処理が本則よりも圧倒的多数派」という**現行のリース会計基準(企業会計基準第 13 号)の轍を踏むことが確実な"骨抜き"の基準草案**であることが明らかとなった。まことに遺憾である(→文献[4,5])。

現行のリース会計基準では所有権移転外リースについて「300 万円以下ルール」と「1 年未満ルール」が存在している。**これらは本来の趣旨を没却する例外規定**であるが、公開草案のままでは、そのまま温存されてしまうことになるのである。つまり、社用車やコピー複合機のオフ・バランスが事実上継続されることとなる。

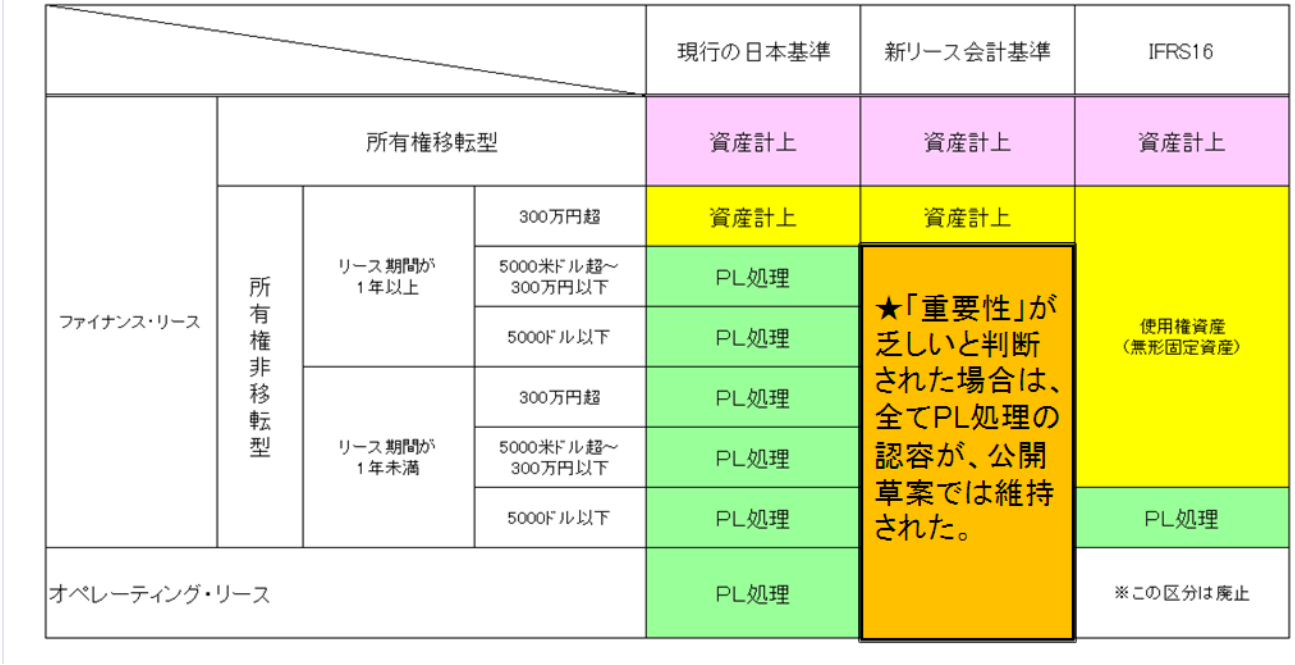
★**【骨抜き条項】**いわゆる「300 万円以下ルール」が温存されてしまう。
公開草案では、焦点であった**「社用車」と「コピー複合機」**については、賃貸借処理が温存可能となる。
⇒おそらく、**「例外処理が圧倒的多数派」という原状は変わらない**と思われる。

★**【骨抜き条項】**いわゆる「1 年未満ルール」が温存されてしまう。
公開草案では、航空機・豪華客船・大型貨物船・タンカーなども、契約期間=11 カ月、354 日(回教暦)などにすれば賃貸借処理が可能。
⇒おそらく、**「例外処理が圧倒的多数派」という原状は変わらない**と思われる。

【会計基準のガラパゴス化の懸念事項】
・ROE の歪みなどは放置され、IFRS16 との金額面での差異は放置される。
・日本会計基準の信憑性が低下し、我が国の産業の国際競争力の低下に繋がる。
・IFRS・米国基準・中国基準との差異が顕在化し、我が国の証券市場がガラパゴス化する。
★2008 年の轍を踏んだ形であり、早晩、「新リース会計基準」の見直しが不可避になると予想される。

【税制との整合性の懸念事項】
・本来、減価償却費のみが費用化されるところが、全額賃貸借処理を許容することになる。
・**本来の趣旨を没却する抜け穴に**より、「新リース会計基準」は"ザル基準"となり、「租税特別措置法」など、税制のありかたとの整合性が問題になることが懸念される。
・与党税制調査会・政府税制調査会などで問題になる可能性がある。
⇒法人税法・所得税法における、**所有権移転外リースに関する「賃貸借処理」の否認に発展する可能性も否定できない。 税制との平仄を合わせて、少額の定義は「20 万円未満」とするべきであり、例外は「1 年未満、かつ、20 万円未満」とするのが本来の趣旨に合致している。**

※所有権移転型リースの場合は、償却資産税の借手の負担となるため、実務上資産の個別管理が必要となるため、資産計上する/しないにより、経理部の実務上の負担が大きく変わる訳ではない。



				現行の日本基準	新リース会計基準	IFRS16
ファイナンス・リース	所有権移転型			資産計上	資産計上	資産計上
	所有権非移転型	リース期間が1年以上	300万円超	資産計上	資産計上	使用権資産（無形固定資産）
			5000米ドル超～300万円以下	PL処理	★「重要性」が乏しいと判断された場合は、全てPL処理の認容が、公開草案では維持された。	
			5000ドル以下	PL処理		
		リース期間が1年未満	300万円超	PL処理		
			5000米ドル超～300万円以下	PL処理		
			5000ドル以下	PL処理		PL処理
オペレーティング・リース				PL処理		※この区分は廃止

§4.SAP のためのドイツ語の勧め

元々、筆者は SAP に関する業務は制度会計(FI)や連結会計(FC)がメインであったが、最近は管理会計(CO)に携わることが増えている。

[1]配賦(Umlage)と付替(Verteilung)

管理会計の 1 つの要素として、コストの配分がある。SAP には「配賦」と「付替」が存在する。「付替」と聞くと、1 対 1 の写像のような印象を受ける人も少なくないようであるが、**両者とも「統計キー数値」や「固定比率」等を用いた複数の部門(原価センタ)への配分が可能**である。両者には次のような相違点がある。

①配賦(Umlage)　→　製造原価や仕掛品の原価を計算するために、「活動タイプ」(労務費・経費など)毎の「二次原価要素」を用いて、センダ(Sender)部署らレシーバ(Anfänger)部署への費用の振替を行う。

②付替(Verteilung) →　発生した一次原価要素(費用項目)を、そのままの勘定科目でセンダ(Sender)部署からレシーバ(Anfänger)部署への費用の振替を行う。

[2]ラテン語・ギリシャ語における「天国」のイメージ　～　実は**複数の階層**があると認識されている!

家内は以下のクリスマス・ソング「神の御子は今宵しも」をラテン語で歌うのが好きであった(→文献[6])。

(1)Adeste fideles laeti triumphantes, venite, venite in Bethlehem!
Natum videte Regem Angelorum.
Venite adoremus,venite adoremus,venite adoremus, Dominum.

(2)Deum de Deo, Lumen de lumine. Gestant puellae viscera.
Deum verum, genitum non factum.
Venite adoremus,venite adoremus,venite adoremus, Dominum.

(3)**Gloria in excelsis Deo**.
Venite adoremus,venite adoremus,venite adoremus, Dominum!

青字の部分は、同じくクリスマス・ソングの定番の「荒野の果てに」(Les Anges dans nos Campagnes)の最後の 1 節と同じである。厳密には、青字の部分の文末は、英語の be 動詞に相当する esse の接続法・3 人称・単数の sit が省略されており、

Gloria in excelsis Deo sit.

が正書法としての文である。直訳すれば「天のいと高きところにて、神に栄光がありますように」となる。Deo は男性名詞(第二変化)Deus の単数与格であるが、注意が必要なのは excelsis である。これは男性名詞(第三変化)の**複数**奪格である。つまり、天国は複数の階層があると意識されているのである。

英語では"Sunday Prayer"で知られる主の祈り(Oratio Dominica / Ἡ Κυριακὴ Προσευχὴ)の冒頭部分は、ラテン語では"Pater noster, qui es in caelis"、ギリシャ語では"Πάτερ ἡμῶν, ὁ ἐν τοῖς οὐρανοῖς"であるが、caelis は男性名詞(第二変化)caelus の**複数**奪格、οὐρανοῖς は ὀυρᾰνοςの**複数**与格である。しかも、ギリシャ語のはサンスクリット語と同様に「双数」を有するので、その「複数形」は「3 個以上のもの」を意味する。

フランス語でも"Notre Père, qui es aux cieux"であり、天国は複数形 cieux である。英語の天国は heaven であるが、現在は単数形として扱われているが、よく見ると複数形語尾の-en が付いている。我々日本人の多くのイメージとは異なり、キリスト教文明においては天国には複数の階層が存在すると考えられているようである。やはり、「天にまします我らの父よ」ではなく「諸天にまします我らの父よ」と訳すべきだったと思われる。(翻訳とは恐いものである、とつくづく思う)。「天と地はあなたのもの」というフレーズも、ラテン語では、"Tui sunt caeli, et tua est terra"であり、天国は複数形、地上は単数形で扱われており、動詞も天国は 3 人称複数形 sunt、地上は 3 人称単数形 est である。

天界に複数の階層があると考えられていたのは西洋だけではない。京都の多くの古刹には曼荼羅がある。胎蔵界も金剛界も、天界に複数の階層があるように描かれている。天国に複数の階層があると意識する場合としない場合で、人々の世界観やモラルにどのような影響があるのか大変興味深い。総合選抜制の下で公立高校に競争の無かった兵庫県東部の教育現場を見て来た筆者としては複雑な思いである。皆様はどのようにお考えだろうか？

※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]「田淵隆明が語る、医療機関の損税問題とその"処方箋"：～消費税導入以来の制度上の盲点～
～国民の大半の理解を得られる処方箋は何か?」(2023/6/12)
[2]「「軽減税率」田淵隆明が語る、数学・理科カリキュラム再考」(2023/6/12)
[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)」(近刊)
[4] 企業会計基準公開草案第 73 号「リースに関する会計基準（案）」等の公表
https://www.asb.or.jp/jp/accounting_standards/exposure_draft/y2023/2023-0502/comment.html
[5] https://www.asb.or.jp/jp/wp-content/uploads/2022_0414.pdf
[6] Enya, Adeste Fideles　https://www.youtube.com/watch?v=HiMuelud5uA

<目次>

2023.8

【 エッセイ 】屏風闚

会員番号　0707 神尾博

2016 年に、世界各国の数多くの監視カメラ映像が、ロシアのサイト「Insecam」で暴露されていることが発覚した。2023 年 8 月現在では、数万台もがサイトに登録されている。Insecam に限らず、こうした不正利用はセキュリティ設定の甘い機器がターゲットにされやすいため、念のため注意喚起しておきたい。パスワードはメーカ出荷時のままではなく複雑なものに変更する、ファームウェアを最新バージョンに更新する、メーカのサポート切れ製品は直ちに利用停止する等だ。サイバー戦争を鑑みれば、特定国が開発した製品も回避した方が良いかもしれない。

さて、江戸時代の画家・鳥山石燕が描いた「屏風闚（びょうぶのぞき）」は、文字通り屏風越しに覗き見をする妖怪である。男女の情事を盗み見続けた屏風が魔物化したとも言われている。石燕の作品には「倩兮女（けらけらおんな）」という妖怪もあり、こちらは塀越しに覗き込みながら大笑いする巨体が印象的だ。

時間軸を COVID-19 発生直後に移そう。在宅勤務が本格化した 2020 年には、PC 画面での会議や打ち合わせが急拡大し、新しい IT 技術やサービスは例にもれずというか、攻撃の対象となった。有名どころでは「Zoombombing（ビデオ爆撃）」がある。Zoom 会議の URL について推測やソーシャルメディア等での収集により、会議を盗聴したり乱入して妨害したりするものだ。こちらの防御としては、会議の URL を参加者のみに通知する、参加用のパスコードを設定する、該当の Web 会議アプリを最新に更新する等が挙げられる。

ところで、リアル出社の時代から、キー入力を背中からの覗き見るショルダーハッキングという手口が存在したが、2020 年には米国の大学で、Web 画面越しにキーボード入力文字が特定されるという危険性についての報告があった。相手の肩や腕の動きから指の動きを推測し、入力文字の見当を付けるというのものだが、ただし精度はさほど高くないという。二人羽織ならどうだろうか？などと想起してしまう。

最近、某 NPO にて「役員会の Web 会議の録画を視聴したい」という申し入れに遭遇した。利用用途もあやふやな状況で、個人情報満載の映像を要求するのはいかがなものか。また昨今、ソーシャルエンジニアリングとしての悪用、たとえば宗教法人の勧誘への利用等の危惧もあり、いかにも薄気味悪い。屏風の語源は「風を屏（ふえぐ）防ぐ」用途からだというが、IT の様々な悪風への対策も怠りなきよう。

（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>

2023.8

第 279 回月例研究会　講演録

テーマ：「令和 4 年改正電気通信事業法について」（特に特定利用者情報規律及び外部送信規律）

会員番号　0555 松枝憲司

【講師】総務省 総合通信基盤局 電気通信事業部 利用環境課　小林央典（こばやし　ひろのり）氏

【日時・場所】セミナー開催日：2023 年 7 月 20 日（木曜）18：30-20：30(Zoom ウェビナー)

【講演骨子】

2023 年 6 月 16 日から施行された改正電気通信法のうち、特定利用者情報規律及び外部送信規律について、電気通信事業における個人情報等の保護に関するガイドライン及びその解説を踏まえ、解説。

【講演録】

1．電気通信事業ガバナンスに関する現状と課題

電気通信サービスの重要度が向上する一方、これらサービスに対するリスクも高まっている。また、令和３年度の調査によれば、インターネットを利用し、インターネットの利用に不安を感じている人のうち約９割が、その不安の内容として、個人情報やインターネット利用履歴の漏えいを挙げた。

2. 令和４年改正電気通信事業法について

電気通信事業を取り巻く環境変化を踏まえ、電気通信サービスの円滑な提供及びその利用者の利益の保護を図るため、電気通信事業法の一部を改正する法律が、2022 年６月に成立。

3. 特定利用者情報の適正な取扱いに関する規律

（1）概観

「利用者の利益に及ぼす影響が大きい電気通信役務」を提供する電気通信事業者に対する規律

①特定利用者情報の取扱規程の策定・届出

②特定利用者情報の取扱方針の策定・公表

③毎事業年度、特定利用者情報の取扱状況を自己評価、取扱規程・取扱方針に反映

④上記事項の統括責任者の選任・届出、職務遂行義務

⑤特定利用者情報の漏えい時の報告

（2）電気通信事業における個人情報等の保護に関するガイドライン（第４章）及びその解説の概要

１.特定利用者情報の適正な取扱いに係る規律の対象者

規律対象となる役務は、報告対象役務となっている電気通信役務ごとに、以下の区分に応じて、前年度における１か月あたりの当該電気通信役務の提供を受けた利用者の数が一定数以上となるもの。

・無料の電気通信役務：　「利用者数 1,000 万人以上」の電気通信役務を対象

・有料の電気通信役務：　「利用者数 500 万人以上」の電気通信役務を対象

なお、情報規律の対象外の電気通信事業を営む者についても特定利用者情報の適正な取扱いが推奨される。

2.情報規律の対象者の指定に際して報告を求める情報

報告対象者は、報告対象役務の提供者のうち、前年度の利用者数が

①無料の電気通信役務の場合：900 万以上　②有料の電気通信役務の場合：450 万以上
である者。
報告内容は、該当する電気通信役務と利用者数（前年度経過後 1月以内に報告）
次の②、③の分類で報告し、他の分類への変更があった場合（例：②の報告をした者は、「②→③」又は「②→①」の変更が生じた場合、③の報告をした者は、「③→②」又は「③→①」の変更が生じた場合）のみ変更報告をする。
①無料の場合：900 万未満（有料の場合：450 万未満）
②無料の場合：900 万以上 1,000 万未満（有料の場合：450 万以上 500 万未満）
③無料の場合：1,000 万以上（有料の場合：500 万以上）

3.情報規律の対象となる特定利用者情報の内容
・利用者には、契約締結者に準ずる者として、「継続的に電気通信役務を利用するための識別符号を付与された者」が含まれる
・特定利用者情報には、通信の秘密に該当する情報に加え、利用者を識別できる情報のうち、データベース等を構成する情報が該当

4.情報取扱規程の記載事項
・特定利用者情報の安全管理に関する事項
・特定利用者情報の委託先の監督に関する事項
・情報取扱方針の策定及び公表に関する事項
・特定利用者情報の取扱状況の評価に関する事項
・従業者の監督に関する事項

5.情報取扱方針の記載事項
・取得する特定利用者情報の内容（取得方法を含む。）に関する事項
・特定利用者情報の利用の目的及び方法に関する事項
・特定利用者情報の安全管理の方法に関する事項
・利用者からの苦情又は相談に応ずる営業所等の連絡先に関する事項
・過去 10 年間に生じた特定利用者情報の漏えい事故の時期及び内容の公表に関する事項

6.特定利用者情報の取扱状況の評価を行うべき事項
・直近の事業年度における情報取扱規程及び情報取扱方針の遵守状況
・直近の事業年度における特定利用者情報の漏えい

7.特定利用者情報統括管理者の要件
事業運営上の重要な決定に参画する管理的地位にあることに加え、利用者に関する情報の取扱いに関する安全管理又は法令等に関する業務、若しくはこれを監督する業務に通算して 3 年以上従事した経験（他業種を含む）を有すること（これと同等以上の能力を有すると認められる場合を含む）

8.報告が必要となる特定利用者情報の漏えい
・利用者の数が 1,000人を超える特定利用者情報の漏えいが生じた場合等

4. 外部送信規律

（1）概観

「利用者の利益に及ぼす影響が少なくない電気通信役務」を提供する電気通信事業を営む者に対する規律であり、そのような電気通信役務を提供する際に、利用者に関する情報を外部送信する指令を利用者に送信する場合、送信前に、当該利用者に確認の機会（通知又は公表、同意取得、オプトアウト措置のいずれか）を付与する必要がある。

（2）電気通信事業における個人情報等の保護に関するガイドライン（第５章）及びその解説の概要

1.外部送信規律の対象

以下のようなサービスで、ブラウザやアプリケーションを通じて提供されるものが対象。

・利用者間のメッセージ媒介等、SNS・電子掲示板・動画共有サービス、オンラインショッピングモール等、オンライン検索サービス、各種情報のオンライン提供（例：ニュース配信、気象情報配信、動画配信、地図等）

2.通知又は容易に知り得る状態

・通知又は利用者が容易に知り得る状態に置く際に満たすべき要件

・通知の場合及び容易に知り得る状態に置く場合に共通して満たすべき要件（日本語で記載、等）のほか、各場合における個別の要件が定められている

・通知又は容易に知り得る状態に置くべき事項

情報送信指令通信ごとに以下を記載

・送信されることとなる利用者に関する情報の内容

・利用者に関する情報の送信先となる電気通信設備

・送信されることとなる利用者に関する情報の利用目的（情報送信指令通信を行う電気通信事業者の利用目的、及び、利用者に関する情報の送信先となる者の利用目的のいずれも）

3. 措置を取ることを不要とする情報

・利用者が電気通信役務を利用する際に送信をすることが必要な情報

・符号、音響又は影像を適正に表示するために必要な情報（OS、ブラウザ情報等）、その他当該電気通信役務の提供のために真に必要な情報　等

・電気通信事業者が利用者に送信した識別符号であって、当該電気通信事業者に送信されるもの

・利用者が同意している情報

4. オプトアウト措置

・オプトアウト措置に際して利用者が容易に知り得る状態に置くべき事項について

質疑応答

以下の項目等についての質問があり、丁寧な回答をいただいた。

Q：「５．情報取扱方針の記載事項」において、事業途中で（年度途中で）国内サーバーから海外サーバーに変更があった場合に報告（連絡）時期について。

Q: 外部送信規律について、フローチャート③の「独立して」をどう解釈すべきか分からない。例えば

「自らの本来業務の遂行手段として自己の情報発信をしている企業 HP」の内で広告効果測定のために情報送信指令通信をしている場合や、同 HP 内で提携企業の広告枠などを設けてクリック数に応じて報酬を得ている場合について、いずれも独立してサービスを行っている訳ではないと解し外部送信規律の対象外と考えてよいか。

Q：今回の改正における規律はどの程度の拘束力があるのか？　登録や届出を怠った場合など、違反した際の罰則等について。

所感

通信技術の発展に伴い、スマートフォンを中心に、FinTech、シェアリング・エコノミー、AR/VR 等の分野における新たなサービスが創出され電気通信サービスは、国民生活や社会経済活動にとって極めて重要な基盤としての役割を果たしており、安定的で信頼性の高い電気通信サービスの提供を確保していく重要性が高まってきている。一方で電気通信サービスに対するリスクが高まっており、これに対応すべく令和 4 年に電気通信事業法が改正された。中でも特定利用者情報の適正な取扱いに関する規律においては、事業者が自らの実態を踏まえた情報の適正な取扱い体制を確保すること、また外部送信規律において、利用者の知らない外部送信がなくなることで、利用者は安心・安全で信頼できるサービスを選択することが可能となる。このような法律の改正の内容は、現在の社会的環境からは必然のものであり、システム監査人もよく理解しておく必要がある。今後は電気通信サービス事業者の規律遵守を保証するためにも内部、外部の監査等が求められてくるものと思料する。

<目次>

2023.8

注目情報（2023.7～2023.8）

■～「サイバーセキュリティ経営可視化ツール Ver2.1 公開」～（IPA）

IPA（独立行政法人情報処理推進機構)セキュリティセンターは 2023 年 7 月 28 日に、「サイバーセキュリティ経営ガイドライン Ver3.0」で定める重要 10 項目の実施状況を 5 段階の成熟モデルで可視化（レーダーチャート表示）できるツールとしてサイバーセキュリティ経営可視化ツール Ver2.1 を公開した。企業は自社のサイバーセキュリティ対策状況を定量的に把握することで、サイバーセキュリティに関する方針の策定、適切なセキュリティ投資の実行等が可能となる。

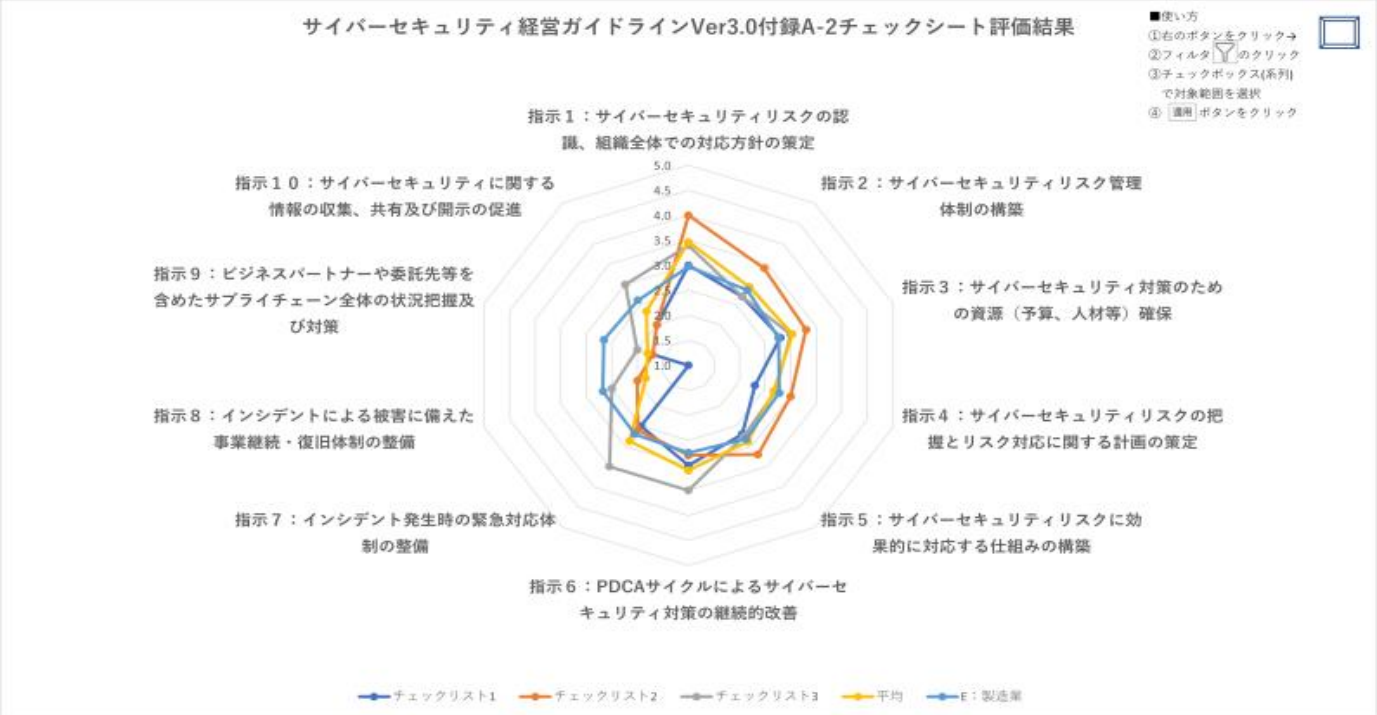
対象利用者

原則として、従業員 300 名以上の企業・組織を対象。

但し、従業員 300 名未満の企業・組織を対象としないものではなく、グループ企業との比較等にも活用可能。

ツールの使い方

- チェックリストの 40 個の設問に、自社の状況に最も近い選択肢（成熟度）を選ぶ。
- 全設問について回答すると、可視化結果シートの表示が自動的に更新される。
- チェックリストの「重要」列は、特に優先的に対応すべき項目を確認する際に活用する。
- 複数の企業（グループ企業等）を比較したい場合、同じ Excel ファイル内に企業毎のチェックリストを作成し、それぞれ回答を記入する。その後、可視化結果シートで比較したい企業を選択すると、各社の回答結果がレーダーチャート上にオーバーレイ表示（下図）される。



<目次>

2023.8

【 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280回	日時	2023 年 9 月 23 日(土) 13:30～17:00
	場所	オンライン（Zoom ウェビナー）
	テーマ	「システム監査・管理ガイドライン活用のポイント ～システム監査・管理基準の改定とガイドラインの公表～」 ガイドライン関係団体合同オンラインセミナー
	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 力利則（ちから としのり）氏
	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。 (*) https://gl.systemkansa.org/ 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。
	参加費	SAAJ 会員／ガイドライン関係団体／非会員 1,000 円 特別月例研究会のため、どなたも会員価格でご参加いただけます。 Zoom ウェビナーには、Peatix 申込時のメールアドレス以外からはご参加できませんのでご注意ください。
	お申込み	https://www.saaj.or.jp/kenkyu/kenkyu/280.html

<目次>

2023.8

【 外部主催イベント・セミナーのご案内 】

■ ITGI Japan Conference 2023		
第36回	日時	2023 年 11 月 16 日（木）　13:00～18:00
	主催	日本 IT ガバナンス協会
	場所	霞が関ナレッジスクエア（スタジオ・ラウンジ） 〒100-0013 東京都千代田区霞が関 3-2-1 霞が関コモンゲート　西館ショップ＆レストラン 3F（西館奥 エスカレーター上がる）（ハイブリット開催） https://www.kk2.ne.jp/kk2/header_link/access.html
	テーマ	イノベーションと IT 経営について考える(仮)
	開催案内	https://itgi.jp/index.php/conference/itgijapan-2023

<目次>

2023.8

協会からのお知らせ　【2023 年度秋期 公認システム監査人及びシステム監査人補の募集】

2023 年度秋期 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_autumn.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。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 ----------

2023 年 8 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

2023 年度秋期
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、2023 年度秋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

2023 年 8 月 1 日（火）～2023 年 9 月 30 日（土）（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_autumn.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>

2023.8

【 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。

<目次>

【　ＳＡＡＪ協会行事一覧　】　赤字：前回から変更された予定			2023.8
	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
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
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 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
	前年度に実施した行事一覧		
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
3 月	3：年会費未納者宛督促メール発信 9：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 10：第 275 回月例研究会	
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

<目次>

2023.8

【 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>

2023.8

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>