特定非営利活動法人
SAAJ 日本システム監査人協会報

21世紀のシステム監査という仕事

No.898 竹下 和孝

1. システム監査の展望

「システム監査」という仕組みを上手に活用することで、業績を飛躍的に向上させ、顧客の満足度が高まり、社員も喜んで働く、そういう組織を実現できたらどうでしょうか。そしてその飛躍のきっかけが「システム監査」にあったとすれば、経営者は強制されなくても、こぞって「システム監査」を実践するでしょう。社員は、「システム監査」を楽しみ、学生は監査スキルの講座や演習を受講し、監査評価に優れた企業を目指して、就活（就職活動）するでしょう。

今、「監査」と名前のついた業務では模索が続いており揺れています。企業の不祥事、幹部や社員による不正が発見され、また情報漏えいやボットネットによる企業のWebサーバへの攻撃は減らないどころか急増している。社員の処遇も低下し、国際競争は激化の一方で仕事のノルマはますますきつくなる。世界的な金融危機の影響を受けて消費が低迷する産業では、失業や長年勤めた会社も廃業の危機にある。読者が経営する、または勤務する企業の状況はいかがでしょうか。

会社勤務はストレスにまみれていますが、特定業務の外部委託や下請けとして活動する企業や、個人で活動する自営業者、派遣先の無い派遣契約者はもっと厳しいといわれています。

私たち監査人は「監査」を通じて企業の事業活動の活性化、業務の効率化に寄与することで利用者や消費者に適正なサービスを還元することなどを目的として活動しているが、この「監査」事業は、ようやくビジネスとしての存在が認知され始めた状態だと思います。

大企業で、組織運営を効率的にすすめる必要性のある規模の組織、金融機関やITへの依存度の大きい企業やIT活用を軸足として成長してきた業界では、情報システム面での投資金額も人材の配置規模も無視できない大きさです。だから早期から、効率性、有効性の評価が求められてきましたが、それ以外の企業ではまだまだ。内部統制のように強制された監査が定着し、次の姿を見出すまで大波と小波に揺れるのでしょうか。

オリンピックのような国際試合に出場するようなトップクラスの選手は、一流のコーチの指導の下に、自己の能力を最大限に発揮できる身体能力と精神力を身につけるよう、日ごろから訓練しています。ビジネスの世界でも、世界クラスの競争を続ける業界や企業では、社内に第三者的な立場で無駄や課題を発見して、不良の発生を未然に防ぐよう活動しています。また専任の組織と人材が配置されています。

でも多くの場合、製品の品質に限られてしまっている。

TQCのTotalの範囲が、会社経営の全体から見ると部分最適にとどまっているため、せっかくの改善が事業の継続的な成長に結びついていない場合が多いのです。

監査も、システム監査も、情報システム監査も同様でしょう。

日本システム監査人協会が展開した、20周年記念イベントも、全国で講演会が開催され、企

目次（報告者の敬称略）

業経営の継続的な改善の手法として、システム監査をどのように活用していくか、識者を交えて活発な議論が展開された、と聞きます。せっかくの議論の盛り上がりが、講演会場だけに、またその講演の前後の時期にとどまってしまっては、もったいないでしょう。

本稿は、議論だけでは成果に結びつかないので、ここでは、監査人が目指す「21世紀型の監査」を実現するきっかけを仕掛けてみたい、と企画しています。

2. システム監査の変容

システム監査はこの10年でどのように変化し、また今後の10年ではどのように成長するのでしょうか。

現在のシステム監査の変化の特徴は、企業内監査として実施される位置づけが強かったシステム監査が、企業の外部で活動する監査人や監査法人など、独立した組織から評価されるシステム監査の分野が広がっていることが掲げられると思います。ISOの普及定着とともに、監査機能は、ISOマネジメントシステムのなかでPDCAサイクルを構成する４本柱のひとつとして位置づけられています。

ISOの適合性評価の仕組みでは、監査は内部監査とともに審査機関により適合性評価の対象として、定期的に監査する仕組みが定着しています。監査、審査と表現は異なりますが、もともとは、Audit（他人の目で見ること、聴くこと）の翻訳です。さらに、システム監査の一部として考えられていた情報セキュリティ分野は、インターネットの急速な発展とともに増大するリスクに対応するため、情報セキュリティ監査として独自の基盤を築いたことも大きな変化です。

21世紀に突入して9年となりますが、その間に「IT、情報・システム分野の監査」という分野でどのような状況変化、ニーズの変化、さらには、監査を実施する制度や体制面での変化があったか、思いつくままに列挙してみたのが次の一覧です。

・金融検査、個人情報保護監査
・ISO監査（品質、環境、ISMS、ITSMS）
・情報セキュリティ監査
・内部統制監査（IT統制監査）
・自治体などが取り組む第三者評価
・公認システム監査人制度
・ネットビジネスの監査
・事業継続監査（BCP/BCM監査）
・監査人（女性、若手、実務務経験が豊富な世代）
・職業としてのシステム監査

これらのキーワードをどのように組み合わせて読むかは、監査人ひとりひとりの立場、興味や姿勢、職務経歴などで異なるでしょう。
ここでは、情報・システム分野の監査の範囲は
・個人情報保護監査
・ISO監査（品質、環境、ISMS、ITSMS）
・情報セキュリティ監査
・内部統制監査（IT統制監査）
・自治体などが取り組む第三者評価
・公認システム監査人制度
などが開始され、利用者の増大とともに、普及、定着しつつあります。

さらに、新しい需要やキーワードとして、
・ネットビジネスの監査
・事業継続監査（BCP/BCM監査）
などの分野への監査が期待されるので、監査の担い手として、
・女性、若手、
・実務経験が豊富な団塊世代を中心とした監査人がもっと活躍できるよう、
・職業としてのシステム監査
を考えてみたいと思います。

ほんの10年前、システム監査といえば、企業内でおこなう内部監査としてのシステム監査と会計監査の一環で外部の専門家により実施される外部監査という分類がされていたのと比べると多様性がひろがっているように思います。別の言い方では、会計監査、業務監査、監査役監査という分類の仕方がありました。1970年ころから企業での利用が本格的となった高価なコンピュータシステム（当時はEDPシステム）の効果的な活用という観点から、事業戦略を支える情報戦略という舞台への転換が進みつつあり、その舞台のイメージが見えてきたといっても過言ではないと思います。

情報システムへの仕組みの仕込み内容（システム設計そのもの）は、企業活動のノウハウの塊（か

たまり）であり、企業競争力を左右するものでもあったので、そう簡単に外部へ開示する内容ではなかったのです。在庫や支払い確認などの情報照会や伝票発行処理に時間がかかりすぎると、顧客は他社（他の店舗）へ逃げてしまい､情報サービス内容の質が問われるようになり、またオープン化技術の進展、アウトソースや異業種を連携したサプライチェーンを構築するため、大規模なパッケージ機能を活用した事業展開の早期化が求められるようになり、BPR手法により再構築された事業分野に標準化された業務手順をソフトウェアで実装する流れが高まりました。

これが21世紀に入ると急激な変化を見せました。情報セキュリティ監査の普及です。
霞ヶ関の官庁街を震撼させたホームページの改ざん（サーバをハッキングされて、画面情報を改ざんされた）事件は、最近では、DDOSやボットネットなど、愉快犯から悪意を持ったハイテク犯罪者集団に進化し、組織的な犯行が国境をまたいで広まる一方、犯人の摘発や検挙はなかなか進まない状況にあります。

一方で、金融危機、経済危機に見舞われた状況から回復するには、ここの企業は経費を節約しながら、顧客満足度の向上と事業の効率化をはかり経営体質を強化するしかない。自己資金で不足するは、他人からの借り入れによりまかなうのと同様、経営体質強化も自分で実践して、不足するノウハウや工数は外部の専門家の経験とノウハウを導入するほうが早いのです。

そこで、企業や組織の経営者はどこからどのように手をつけていくかについて、限られた経営資源を有効に配分する判断を行う。その判断は、優れた経営者の長年の経験と勘のように、合理的な裏づけを確認するため検査、評価・診断、審査・監査など、経営の状態を正しく知る必要があります。売り上げと利益、社員、在庫、情報処理の量などの指標だけで判断できる時代は過ぎており、多くの評価指標を整理するためにもIT活用が有効です。

3. システム監査の七変化

1）システム監査（1980年代後半）

経済産業省のシステム監査基準に基づいて、情報システムの企画・開発・運用などの活動が、①設計書や仕様書のとおり構築され、無理なく間違いなくデータ作成･処理しているか(信頼性)、②限られた資源を投入した費用や投資に対して、予算内で開発運用され、目的通りの成果をだしているか（有効性・効率性)、③利用している情報機器の性能、組み合わせ、設置場所はトラブルが起きないよう管理されているか（安全性）などを判断する場合に、システム監査を行います。

金商法（金融商品取引法）が施行され、情報システムの監査は注目されるようになったといわれています。システム監査は、企業の経営者が業務効率を改善することを支援する機能を持っています。内部統制の一環として実施されるシステム監査が、経営の効率性および有効性を高めるためにシステム監査の比重を高めるよう、早期に実現できるよう期待しています。

情報システムに関する内部統制のためには、企業情報システムの信頼性、安全性、有効性を評価する「システム監査」が欠かせないのですが、現状では本格的なシステム監査を実施する機会は不足しているのではないでしょうか。定期健康診断は精密検査を必要とする状況を判定するために必要なのです。組織の診断や情報システムの監査は、チェックリストやヒアリングによる確認で発見することが難しい分野も増えています。微妙な状況を判定する判断力と経験を備えた監査人は不足しています。

2）マネジメントシステム監査の進展

ISOの規格（品質、環境、ISMS、ITSMSなど）に基づく監査やJISQ15001に基づく個人情報保護監査は、1990年代中頃より順次始まり、すでに15年が経過しようとしています。。

個人情報保護は、本人の権利を尊重して扱うよう定められた「個人情報保護法」にもとづく制度ですが、プライバシーマークの認証を付与された企業が、定期的に実施するよう義務付けられている監査です。

ISMS、PMSのようにマネジメントシステムとして制度が作られたものに対する監査で必要なことは、新たに情報セキュリティ上の脅威が発生し、変化していく中で、どのように情報セキュリティをマネジメントする体制を運用し、実際に運用しているのかを監査するということ

です。複数のマネジメントシステムは、相互に組み合わせると、より組織力の強化が図れます。

3) 情報セキュリティ監査の進展（2000年頃から）

情報セキュリティ監査は、情報セキュリティ監査基準、同管理基準の制定に始まり、英国発のBS7799からISO27001（ISMS）として本格的に世界中での認知が高まっています。

海外の現地法人、子会社、関係会社を含めて、情報セキュリティに関する共通の基準をもとに、整備を進める動きが加速しています。いまや情報システムが企業活動の根幹を揺るがすほどの影響力を持ち始めたからです。

情報セキュリティ監査の対象は、情報システムではなく情報資産や情報を扱うプロセスであることに特徴があります。情報システムのセキュリティではなく、書類、データ、情報システム、ネットワークや情報機器など「情報資産」のセキュリティを扱います。カメラ付き携帯電話の普及も、情報の漏洩という側面では、大きな脅威となる可能性があります。USBメモリーに関しても、使用する（逆に、使用禁止する）ルールを明らかにして、新しい保存媒体、可搬媒体としての運用する（ということを監査する）ことが大切です。

まず、リスクアセスメント（情報資産に対して、想定される危険性の可能性を評価すること）が事業の規模や複雑さに適した方法であることが大事であり、その結果を基に効果的な対応計画を作り、その対策が実施されているかどうかを評価していきます。

さらに、PCI DSS（Payment Card Industry Data Security Standard）は、クレジットカード情報や取引情報を保護するために、クレジットカード業界が独自に策定したグローバルセキュリティ基準です。PCI DSSは、ISMSやプライバシーマーク制度と異なり、個々の事業者だけでなく、カード発行会社、カード加盟店、決済データの処理事業者など、顧客のカード／取引情報を共同で利用している事業者全体で保護していきます。

クレジットカードの情報は、スキミングされて他人に勝手に利用される事件が起きているため、消費者保護の観点でも法改正（改正割賦販売法）により、事業者の枠を超えた業界横断的なカード情報の適正管理義務が課せられるわけです。クレジットカードによる支払い（一括・分割の双方）について、カード事業者の加盟店は「クレジットカード番号等保有事業者」に該当するため、厳格なカード情報管理が求められるわけで、実務的な影響は大きいでしょう。

4) 公認システム監査人制度の発足（2002年）

システム監査技術者試験は、情報システムの企画開発運用などのスキルを身につけた人が、監査対象とする情報システムを第三者として評価するシステム監査人になるための入門資格。情報処理技術者試験の一区分として毎年実施されるが、その難易度は非常に高い。システム監査人としての実務経験を踏まえて、スキルアップを図っていく仕組みが、経済産業省の指導のもと、日本システム監査人協会が認定、運用する公認システム監査人（CSA）の制度です。

しかしながら、ビルを建設する場合の一級建築士や、企業の財務状況を監査する公認会計士と比べると一般への認知度は少ない。公認システム監査人は、職業として、企業や組織の情報システムを構築運用する場合の安全性・効率性などを評価して解題を抽出する専門家である。しかしながら、ITの専門家や実務家の位置づけから、公認システム監査人として独立、社会貢献への道を開いたことへの意義は大きい。（企業内の実務家から、社会で活躍する社会起業家へのパスポートとして、いっそうの活用が期待できます）

5) 内部統制監査の進展（2000年代中頃から）

財務報告に関する内部統制が、(1) 事業経営の有効性・効率性を高め、(2) 企業の財務報告の信頼性を確保し、(3) 事業経営に関わる法規の遵守を促し、(4) 資産の保全を図る

という目的のために、ルールを定めているか。またルール通りに運用されているかを確認する仕組みが内部統制監査であり、ITを活用している業務に対し、IT面からその実現を支援するのがIT統制監査の役割といえるでしょう。。

株主総会での決算報告とともに、初年度にあたる内部統制報告の一部が公開され始めていますので、今後の内部統制（監査）の進め方について見直しが加えられると思われます。

財務報告のもととなる企業活動で、内部統制の対象とする分野も非常に広いので、事業領

域の全てを短期間でカバーしていくことは難しい。そこで、リスクの度合いの大きい内容（現実となったときに事業経営に与えるダメージの高いものから優先着手するリスクアプローチが広がっています。

6）第三者評価制度

都道府県などの自治体では、公共施設の運用管理を民間企業に委託することで、利用者サービスの向上を図ってきましたが、この分野でも指定管理者、介護サービス・福祉、学校などに対する第三者評価制度が始まっています。

例）指定管理者第三者評価制度
（出典：横浜市のホームページ）

横浜市の指定管理者第三者評価制度は、次のような特徴があります。

指定管理者制度を導入した全ての施設を対象に、次の2つの方式で第三者評価を実施し、評価結果をホームページや施設内等で公表し、指定管理者の業務改善や今後の制度運用に活用している。

①市内に同種施設が複数存在する区民利用施設（地区センターなど300施設）について、複数の民間の評価機関を選定し、評価を実施している。

②その他の施設（600施設）については、専門性や施設特性等を考慮して、施設所管局区が設置する外部評価委員会で評価を実施している。

このような分野では、評価者の育成とスキルアップが必要で、ISOの内部監査員育成と同様に、幅広い監査の仕組み作りに貢献することが期待できます。

7）新しいタイプの監査分野

①ネットビジネスの監査

汎用大型コンピュータからサーバを組み合わせた分散型、ネットワークを利用したアウトソース型、Webを中心とする情報処理の機能サービスなど、情報処理の形態が益々複雑になっています。これらを一時に切り替えるのでなく併行利用しながら切り替えていくことに難しさが潜んでいます。

携帯電話を利用したネットサービス、さらにはSaaS、クラウドコンピューティングなど、新しい利用形態が増えています。モバイルPCからネットPC、PDAとの組み合わせ、これらの機器の性能向上により、個人と個人が携帯し利用する情報機器を中心とした情報サービスの利用形態が増えると、利用者の安全性を阻害する要因も増えますので、新しいIT知識と監査手法が必要となってきます。ネットビジネス部門の監査や、ネット型ビジネス（を行う企業）に対する監査が始まっています。

②ＣＳＲ監査

CSR体制は、企業が社会的責任（CSR）を果たすために、独自に設定し又は顧客・得意先が要求する方針・基準に基づいて構築し運用しますが、ここでも監査の要求があります。PDCAのCの部分です。

CSRに取り組む企業の多くでは、EMS（環境マネジメントシステム）を運用していて、環境報告書を作成してCSR報告と称している会社もあります。

ISO規格や自社・取引先の行動規範（CoC）に基づいた「CSR監査」（内部監査、サプライヤー監査等）によって、組織のCSR体制の自己評価・外部評価を行っています。

まだ国内外の事例も少ないので、ケーススタディを通して顧客・取引先からの期待に応える「CSR監査」を作っていく必要があります。

③BCM監査（事業継続マネジメント監査）

前述の「マネジメントシステム監査の進展」でも触れさせて頂きましたが、日本が世界でも稀に見る自然災害リスクの高い国であるため、BCM監査の必要性は高まると思われます。製造業では、研究開発拠点や中核部品の製造工程を抱えている企業が多いため、特定の工場や取引先の被災は、サプライチェーン全体に影響を及ぼすリスクがあるからです。

有難くない話題ですが、首都圏直下型地震のリスクは高まり、過去にも地震だけでなく、サリン事件や大型台風や集中豪雨のたびに、交通網は遮断されていることは事実です。

BCM監査には、国際規格としてのBS25999という先行規格が制定されISO化の準備が進められています。またしても英国のBS規格が先行しているわけですが、基本書として体系的な取り組みが整理されています。監査というよりは、

消防・防災訓練のように毎年の安全点検として定着させる工夫が効果的です。

4．職業としてのシステム監査

このような状況で、職業としてのシステム監査はどのように見えるのでしょうか。
より積極的に情報発信して、正しい情報をもとに理解者を増やしていく必要があるとの考えから、昨年、取材を受け、高校生向けの職業しらべのガイドを務めました。

キーワードは、

「システム監査は、どんな仕事」

「システム監査は魅力ある職業、やりがいのある職種」

であり、システム監査人になるためには、どのような学習、職種選択をして経験をつんでいくか、という「仕事調べ、職業への適性、進路指導」の補助教材作成でした。

ご承知の通り、システム監査という職業は、セミナーを修了し、試験に合格すれば、システム監査という役割を果たせるわけではありません。また監査部門に配属された、監査法人に採用され就職しても、職業としてのシステム監査実務を経験していく必要があります。たくさんの困難を経験することで、トラブルの原因や関係者の状況がわかる監査人になれます。

職業としてキャリアを積む具体的な展開については、システム監査人各位のご協力、全国支部での活動にも織り込んで頂きたい内容を準備中です。続きは次回に紹介させて頂く予定です。

このような活動を進めるシステム監査人は、高度な専門職としての職業意識をもとに、日ごろの研鑽を継続することが前提です。

ここに改めて、「システム監査人協会倫理規定」を掲げて、システム監査を職業として行うものは、倫理規定に掲げた12項目を確認して肝に銘じたい。

システム監査人倫理規定

平成14年2月25日制定
特定非営利活動法人
日本システム監査人協会

（目的）
第１条　この規定は、システム監査人が最低限遵守すべき職業倫理の規範を定めることを目的とする。

（使命）
第２条　システム監査人は、情報システムの信頼性・安全性・効率性・有効性を高めるため、その専門的知識と経験に基づき誠実に業務を行い、情報化社会の健全な発展に寄与することを使命とする。

（責務）
第３条　システム監査人は、情報システムを総合的かつ客観的に点検・評価し、関係者に助言・勧告するものとする。

（監査基準・手続き）
第４条　システム監査人は、システム監査の基準、手続きを明らかにし、それに基づきシステム監査を行わなければならない。

（監査報告）
第５条　システム監査人は、監査結果の報告にあたって、知り得た全ての重要な事実を明らかにするものとする。

（守秘義務）
第６条　システム監査人は、正当な理由なく業務の遂行に伴い知り得た機密情報を他に漏洩し、または窃用してはならない。

（独立性）
第７条　システム監査人は、常に独立の立場を堅持しつつ、適切な注意と判断によって業務を遂行し、特定人の要求に迎合するようなことがあってはならない。

（公正不偏）
第８条　システム監査人は、業務を誠実に果たし、常に公正不偏の態度を保持しなければならない。

（社会的信頼の保持）
第９条　システム監査人は、自らの使命の重要性に鑑み、高い社会的信頼を保

持するよう努めなければならない。
（名誉と信義）
第10条　システム監査人は、深い教養と高い品性の保持に努め、システム監査人としての名誉を重んじ、いやしくも信義にもとるような行為をしてはならない。
（システム監査人間の規律）
第11条　システム監査人は、みだりに他のシステム監査人を誹謗し、名誉を傷つける等の行為をしてはならない。
（自己研鑽）
第12条　システム監査人は、システム監査を行うのに必要な専門能力および監査技術の向上に努めなければならない。
（規定の改廃）
第13条　この規定の改廃は、理事会の承認を得なければならない。

「付　則」
この規定は、平成14年2月25日から施行する。

会報掲載主要記事一覧（99号－109号）

会報編集部では、99号で特集を組み、1－99号までの記事を俯瞰して、次の10年のシステム監査について話題を提供しました。その後、100－109号を発行しましたので、一覧を掲載します。

号（発行月）	各号の目次
99号（07.12）	特集1：会報にみるシステム監査人協会の歩み －アイデンティティを模索し続けた20年－ 会報掲載主要記事一覧 特集2：北海道支部・東北支部合同研究会開催報告 内部統制と個人情報漏えいリスク 「個人情報保護マネジメントシステム構築のための実務者養成セミナー」のご案内 第131回月例研究会報告 （投稿）公認システム監査人レポート　2007 夏 （投稿）公認システム監査人レポート　2007 秋 第４回　内部統制セミナー受講者募集のご案内 J-SOX対応のITに係わる内部統制評価を疑似体験してみませんか!! （紹介）会員執筆図書
100号（08.02）	1. システム監査人の仕事紹介 2. 20 周年講演会案内 3. これからの10 年アンケート速報 4. CSA －ホームページ紹介 5. 第4 回内部統制セミナー報告 第10 回システム監査実務セミナー報告 7. 近畿会システム監査実践セミナー 2 日間コース報告 6. 個人情報保護研究会報告 8. 法人部会セミナー報告（熊本市、千葉市） 9. 理事会議事録9,10,11 回 10. 韓国の電子政府法 11. システム監査研究会実践マニュアル 12. 事例研第5 回及び6 回内部統制セミナー案内 13. 金融庁の職員募集 14. エッセイ論文の募集
101号（08.04）	1. 日本システム監査人協会20 周年総会特集… 20周年記念講演会ご挨拶、講演1、講演2、講演3 投稿「記念講演会を聴いて」 2. 第7期総会資料

	3. 中部支部合宿報告 4. 第134回月例研究会報告 5. 自治体向けセキュリティセミナー（昭島市様） 6. 新任・退任理事挨拶 7. 平成20年度第1 回理事会議事録 8. PMSセミナー案内
102号（08.06）	1. 特集：CSA 活動紹介（松枝さん、榎本さん）、ご存知ですかCSA SAAJ活動紹介1（システム監査事例研究会、システム監査基準研究会、個人情報保護監査研究会、セキュリティ監査研究会、法人部会） SAAJ活動紹介2（北海道、東北、北信越、中部、近畿、中四国、九州） 2. 2008年第3回、第4回理事会報告 3. 第135回月例研究会報告（横瀬さん） 4. h社監査普及サービス報告（大田さん、矢島さん） 5. 第11回システム監査実務セミナー報告（小佐野さん、末廣さん、高谷さん、高橋さん） 6. 新任理事紹介（島田さん） 7. 投稿（アクセス権失効管理（藤岡さん）、CSA活動レポート（竹下さん）） 8. 第12回システム監査実務セミナー受講者募集 9. 第8回内部統制セミナー受講募集 10. 図書推薦（日本版内部統制“成功”の秘訣）
103号（08.08）	1. 特集：九州支部　20周年記念イベント報告 2. 2008年第5 回、第6回理事会報告 3. 第36回月例研究会報告（竹下）、第137回月例研究会報告（西宮） 4.第6回内部統制セミナ参加報告（門川） 5. CSAフォーラム開催案内 6. 投稿：CSA活動レポート（竹下） 7. 第12回システム監査実務セミナー参加者募集
104号（08.10）	1. 特集：近畿・中四国支部　20周年記念イベント報告 2. 2008年第7回、第8回理事会報告 3. 富山県情報セキュリティセミナー報告 4. 第138回、139回月例研究会参加報告（牧野さん、福田さん） 5. 第8回内部統制セミナー開催報告（鈴木実さん、佐藤さん） 6. 北信越支部便り（長野県例会、麻生さん、森さん、梶川さん、木村さん） 7. 投稿：CSA活動レポート（竹下） 8. 第9 回及び第10回内部統制セミナー開催案内 9. 会計担当、事務局・会報担当からのお知らせ
105号（08.12）	1. 東北支部20周年記念講演会報告 2. 第9回理事会議事録 3. 法人部会報告（清瀬市） 4-1. 第12回システム監査実務セミナー開催結果の報告 4-2. 実務セミナー参加者感想（浜崎さん） 4-3. 第9回内部統制セミナー実施報告 5. 近畿支部第18回システム監査勉強会 6-1. CSAレポート（竹下） 6-2. 書評『実践現場発信のJ－SOX』 7-1. 第10回内部統制セミナー募集案内 7-2. 第13回システム監査実務セミナー案内 8. 会計担当からのお知らせ（訂正）
106号（09.02）	1. 特集：システム監査人からのメッセージ「日本困難で委員会（日本、こんなんでいいんかい）」へのお答え（鈴木会長）「社会の期待とシステム監査」（清水さん） 2. 創立20周年記念講演会（中部支部）開催報告（大野さん、栗山さん、中村さん、安井さん、浦田さん、若原さん） 3. 2008年12月度　理事会報告 4. 第142回月例研究会報告（藤野さん） 5. 第1回CSAフォーラム記録（斉藤さん）

	6. 九州支部大分合同セミナー開催報告（藤平さん、梶屋さん、諸藤さん） 7. 近畿実践セミナー受講者募集 8. 第11回内部統制監査人セミナー受講者募集 9. 再掲載　事務連絡 10. 注意　お知らせ
107号（09.4）	1. 第8期日本システム監査人協会総会特集 2. 第8期総会記念講演報告（太田さん） 3. 第8期総会資料 4. 新任理事のご挨拶（大石さん、山田さん） 5. 第10回内部統制監査人セミナー開催報告（沼野さん、大竹さん） 6. 第141回月例研究会報告（吉田さん） 7. 第144回月例研究会報告（市川さん） 8. 平成21年度第1回理事会議事録 9. 平成21年度第2回理事会議事録 10. 第12回内部統制監査人セミナー受講者募集
108号（09.6）	1. 特集：CSAフォーラム 2. 北信越支部20周年記念講演会＆西日本支部合同研究会開催報告 3. 平成21年度第3回理事会議事録 4. 平成21年度第4回理事会議事録 5. 平成21年度第5回理事会議事録 6. 投稿論文：「一般企業を対象とする『個人情報漏えい防止』に向けた評価チェックリストの活用」（宮下重美） 7. 会報掲載論文募集要項 8. 会員除名の公告
109号（09.8）	1. 21世紀のシステム監査という仕事 2. 主要記事の項目一覧（99-108号）録 3. 6月理事会議事録 4. 7月理事会議事録 5. 第145回月例研究会報告（渡辺さん） 6. エッセイ論文募集 7. 第13回内部統制監査セミナーの案内 8. 編集後記

平成21年度第6回理事会議事録

日本システム監査人協会

1. 日　時：2009年6月11日㈭18：30－20：30
2. 場　所：星稜会館　3F会議室
3. 出席者：鈴木㈱、小野、馬場、田中、吉田㈱、福田、竹下、山田、力、斎藤、吉田㈱、橘和、大石、鈴木㈱、仲、榎本

メールによる委任状（12名）　出席者計：28名/40名中

4. 議題
   ⑴審議事項（予定なし）
   ⑵報告事項

5. 資料
   ⑴継続教育要項に関するお知らせ（案）、継続教育「2年更新版」（案）および同「3年更新版」（案）

6. 審議事項
   特になし

7. 報告事項（各担当理事。以下敬称略）

7.1「継続教育要項」の件（鈴木信夫）
前月検討の「継続教育要項」に関する修正案の説明があり、内容の検討を行った（資料参照）。要点は以下の通り。
・継続教育報告書は2年乃至3年分まとめての報告を認める。
・適宜、申告内容を協会側から問い合わせる

ことで、内容の担保を行う。
・要項変更に併せ、公認システム監査人制度細目の条文変更も必要(ホームページも含む)。
・継続教育要項に関するお知らせ（案)、継続教育「２年更新版」（案）および同「３年更新版」（案）の最終校正は事務局で行い、再度案内する。

7.2 情報セキュリティ教育事業者連絡部会（ISEPA）の件（鈴木信夫）
・部会例会に出席。
・懸案の情報セキュリティ大学院との協業はすぐには進まない様子。

7.3 法人部会（小野）
・各支部から、全国の市への自治体向けセミナー案内（DM）が送付完了。
・某市より照会があった。資料送付後、回答待ち。
・法人部会メンバー企業の参照を協会HPのトップページより行えるよう検討をお願いしたい。

7.4 事務局（馬場）
・会費を2年以上未納の34名について、会員規定6条に基づき除名処分とする。
・各支部長宛てに支部名簿（会費納入状況を反映）を送付するので会費納入状況を確認いただきたい。
支部助成金は6月末日現在の会費納入状況で支払いを予定している。

7.5 中部支部（田中／メールをもとに編集）
①中部支部　5月例会実施報告
日時：5月16日㈯14：00～17：00
出席者：20名
会場：岐阜県大垣市　ドリームコア
マルチメディア研修室1（3F）
内容：
講演Ⅰ：「デジタルジャパンにおける
医療情報システムへの期待」
田原 保　様
講演Ⅱ：北信越支部「医療機関の
個人情報保護監査研究」活動状況報告
宮本 茂明　様

②次回：7月11日　講演　SaaSについて

7.6 近畿支部（吉田博一／メールをもとに編集）
①第113回定例研究会
日時：5月15日㈮ 18：30 ～ 20：30
場所：大阪市立大学文化交流センター大セミナー室
テーマ：「プロジェクト管理と工事進行基準」
講師：雑賀 努　氏
（株式会社ニイタカ監査室　当支部会員）
出席数：40名

②第21回システム監査勉強会（予定）
日時：6月20日㈯ 13：00 ～ 17：00
場所：大阪大学中之島センター 2階 講義室1
テーマ１：「郵便局株式会社における
Saas活用の概況について」
講師：郵便局株式会社 本社 システム企画部
担当部長　石塚 真由美　氏
SAAJ本部第141回月例研究会(2008/10/29)のＶＴＲを視聴し、討議します。
テーマ２：「情報大航海時代の到来
－リアルとネットを結ぶ知的情報アクセス基盤－」
講師：慶應義塾大学　環境情報学部
教授　小川 克彦　氏
SAAJ本部第142回月例研究会(2008/11/25)のＶＴＲを視聴し、討議します。

③システム監査実践セミナー２日間コース（近畿支部主催）（予定）
参加者募集終了。15名の申し込みがあった。
日時：6月27日㈯～ 6月28日㈰

④システム監査入門セミナー（予定）
実践セミナーの簡易版です。只今参加者募集中。9名の申し込みがあった。
日時：8月8日㈯ 13：00 ～17：00

⑤近畿支部20周年＋1シンポジウム（仮称）（予定）
日時：8月29日㈯PM
内容：20周年記念シンポジウムで提起されたシステム監査の課題について、議論を深めたいと思っています。

⑥西日本支部合同研究会（予定）
日時：11月14日㈯PM ～ 15㈰15時
内容：一日目　施設見学　懇親会
二日目　研究会　基調講演
大阪成蹊大学　松田貴典教授

7.7 九州支部（福田／メールをもとに編集）

①５月度月例会（第222回）

日時：5月23日㈯ 13:00 ～ 17:00

会場：西南学院大学
西南コミュニティセンター２階
プロジェクトルーム

内容：ビデオ視聴「ビジネス・プロセス・マネジメント（BPM）入門」

報告事項

⑴経済産業省「情報セキュリティ関連法令の要求　事項（案）」の紹介（舩津）

⑵セキュリティ技術トピック（その４）
（福田）　参加：9名

②（開催予定）６月度月例会（第223回）

日時：6月20日㈯ 13：00 ～ 17：00

会場：早良市民センター　第3会議室

内容：ビデオ視聴 「金融業務における情報セキュリティと暗号技術―暗号アルゴリズムの世代交代問題を中心に―」

報告事項⑴セキュリティ技術トピック（その４～５）（福田）

③（開催予定）７月度月例会（第224回）

日時：7月25日㈯ 13：00 ～ 17：00

会場：早良市民センター　第1会議室

④（開催予定）8月度（第225回）

日時：8月22日㈯ 13：00 ～ 17：00

会場：早良市民センター　第1会議室

7.8 会報（竹下）

・今月号は、20周年最終報告およびCSAフォーラム特集を行った。
また「標準的評価手続き」に関する論文の投稿があった。

・ベネッセからの中学・高校生向けの「システム監査とはどのような仕事か？」の取材に応じた旨の報告があった（紹介の動画を鑑賞）。

・次回は7/15原稿締め切り

7.9 システム監査基準研究会（山田）

①オフシェア開発基準（v0.94）作成。今後の予定は以下の通り。

・基準研のメンバー全員に公開して意見収集の予定。今はシステム監査項目全体との調整を行っている。

・9月理事会にて紹介予定。その後、SAAJメンバー対象にパブリックコメント依頼を提示。

・一般企業にて実際に活用を試み、10月には一般公開予定。

7.10 CSAフォーラム（力）

・CSAフォーラムの特集を今月号会報に掲載。

・次回6回目は7/23日で、小野さんに講演依頼。

7.11 依頼事項（斉藤）

・情報システムユーザー会の講演会集客のために、出席者には「継続資格ポイント」を付与することを案内文に明記したい旨、理事会で了解いただきたい（全員、了解）。

7.12事例研（吉田裕孝）

・7月23・24・25日　12回内部統制セミナー開催予定。現在申込４名だが実施予定。

・ISEPA（7.2項）の件は、もう少し様子を見る。

7.13 月例会（大石）

・6月度月例会は、現在申込者84名で少し厳しい。

・7月度月例会は東京三菱UFJの方に講師をお願いする予定。

7.14 教育研修委員会（鈴木実）

・先般ご報告した、特認研修機関とのトラブルの調整を継続して行っている。

【以下はメール報告】

7.15 北海道支部（大舘）

・5月VTR勉強会

日時：5月25日㈪ 18：30～20：30

場所：㈱富士通北海道システムズ　会議室

テーマ：「経済産業省の
情報セキュリティガバナンス構想」

講師：経済産業省 情報セキュリティ政策室
清水 友晴　氏

出席数：7名

7.16 北信越支部（森）

支部間交流として、中部支部5月例会と北信越支部福井県例会にて、講師の相互派遣を実施中です。

①中部支部　5月例会実施報告
日時：5月16日㈯
会場：岐阜県大垣市ドリームコア
マルチメディア研修室
内容：北信越支部「医療機関の個人情報保護監査研究」
活動状況報告　北信越支部
宮本 茂明　氏

②北信越支部年度総会報告
日時：3月14日㈯13：30 ～ 17：30
場所：アーバンプレイス富山8階会議室
議題
⑴年度総会
・昨年度行事報告と今年度行事計画について
・昨年度会計報告と今年度予算について
⑵発表
「経営とITについて」 國谷　吉英　氏
⑶支部研究会
1) システム監査研究会経過報告
「IT経営ロードマップ」について
森 広志　氏
・事例研究：JFEスチール
2) 情報セキュリティ監査研究会経過報告
「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」概要説明　宮本 茂明　氏

7.17 中四国支部（溝下）
①5月度月例会
日時：5月16日㈬13：00 ～ 17：00
内容：「ＩＴ投資効果の最大化に向けて」他
場所：広島県健康福祉センター　総合研修室

②6月度月例会
日時：6月17日㈬18：30 ～ 20：30
内容：「ビジネス・プロセス・マネジメント（BPM）入門」
場所：広島市まちづくり市民交流プラザ
会議室Ａ

議事録確認
議　　長　　鈴木　信夫
議事録署名人　　馬場　孝悦、榎本　吉伸
以上

平成21年度第７回理事会議事録

日本システム監査人協会

1.日　時：2009年7月9日㈭18：30－20：00
2.場　所：星稜会館　3Ｆ会議室
3.出席者：鈴木（信）、力、沼野、吉田（裕）、馬場、金子、岩崎、大石、木村、桜井、仲、松枝、吉田（近畿支部）
メールによる委任状（19名）　出席者計：32名/40名中

4. 議題
⑴審議事項なし
⑵報告事項
5. 資料
⑴日本銀行金融機構局公表資料

6. 審議事項
なし

7.報告事項（各担当理事）
7.1 大石理事
⑴日本銀行金融機構局の公表資料について
大石理事の所属する日本銀行において、地域銀行108行に対し、勘定系システムの「システム共同化」(複数の金融機関がシステムを共同で外部委託すること）の実態調査のためアンケートを実施。その取りまとめ結果の概要について報告があった。
資料名：「金融機関におけるシステム共同化の現状と課題」
7.2 事務局（馬場／金子）
⑴支部助成金について
支部助成金の算出について、毎年６月末を基準日とし算出していたが、支部の要請により今年は７月末を基準日として算出することとした。
⑵メーリングリストの改善について
メーリングリストを利用しやすくするため、改善を行うこととし、6/30にUISと第一回打ち合わせを行った。
⑶第9回総会の日程・会場について
来年の第9回総会の会場予約を行った。
・開催日時：2月19日㈮13：00 ～
・会　　場：機械振興会館　B3
第2研修室（140名収容可能）
（今年の第8回総会会場と同じ場所）

⑷事務室の定期電源保守について
事務室がビル電気設備保守のため次の通り停電となる。
停電時間帯：7月20日（月：祭日）
9：00 ～ 12：00
サーバ、PC停止時間帯：
7月17日㈮17：00 ～ 7月21日㈫13：00

7.3 認定委員会（岩崎）
CSA秋の募集案内をホームページに公開した。
・今回募集から、認定料について会員と会員外で別料金設定を行った。
・認定有効期間の変更（3年を2年に変更他）は平成22年春募集分からとする。
確認事項：UISへのホームページ変更依頼メールには、CCで事務局担当者及び案件責任者へも送ること。

7.4 事例研究会（吉田（裕））
・第12回内部統制監査人セミナー（2009/7/23 ～）は参加者5人で開催する。
・第14回システム監査実務セミナー（2009/8/29 ～）は募集中。
現在の応募者は1名。

7.5 CSA利用推進（力）
・第5回CSAフォーラムは6月1日に実施した。
・第6回CSAフォーラムは7月23日㈭に開催する。テーマは「CIOとシステム監査」、講師は小野理事

7.6 近畿支部（吉田）
●システム監査サービスについて
2つの企業から「システム監査サービス」の引き合いがある。
本部事例研究会と協力し実施する。
●第21回システム監査勉強会
日時：6月20日㈯13：00～17：00
場所：大阪大学中之島センター 2階 講義室1
テーマ１：「郵便局株式会社におけるSaaS活用の概況について」
講師：郵便局株式会社 本社 システム企画部 担当部長：石塚 真由美　氏
SAAJ本部第141回月例研究会（2008/10/29）のVTRを視聴し、討議しました。
テーマ２：「情報大航海時代の到来」
－リアルとネットを結ぶ知的情報アクセス基盤－」
講師：慶應義塾大学　環境情報学部 教授　小川 克彦　氏
SAAJ本部第142回月例研究会（2008/11/25）のVTRを視聴し、討議しました。
出席数：33名
●システム監査実践セミナー２日間コース（近畿　支部主催）
日時：6月27日㈯～ 6月28日㈰
受講者数：16名
●第114回定例研究会(予定)
日時：7月17日㈮ 18：30 ～ 20：30
場所：常翔学園大阪センター 301教室
テーマ：「IFRS（国際財務報告基準（国際会計基準））と情報システム」
講師：武田 雄治　氏
（公認会計士　武田公認会計士事務所所長）
●システム監査入門セミナー（予定）
実践セミナーの簡易版です。只今参加者募集中。10名の申し込みがあった。
日時：8月8日㈯ 13：00 ～ 17：00
○近畿支部20周年＋1シンポジウム（仮称）（予定）
日時：2009年8月29日㈯PM
内容：20周年記念シンポジウムで提起されたシステム監査の課題について、議論を深めたいと思っています。
○西日本支部合同研究会（予定）
日時：11月14日㈯PM～ 15㈰15時
内容：一日目　施設見学　懇親会
二日目　研究会　基調講演
大阪成蹊大学　松田貴典教授

7.7 基準研究会（松枝）
各課題は、年度当初の計画に基づき進捗している。
研究会に参加するメンバーが増えてきた。

7.8 月例研究会（沼野）
⑴7月月例研究会について
7月28日㈫月例研究会は「金融機関におけるプロジェクト監査への取り組み事例」を発表する。
講師は、三菱東京UFJ銀行　監査部業務監査室　上席調査役　金田氏
現在200名の参加申し込みがある。
⑵8月の月例研究会について
8月31日㈪に下記内容で開催予定

テーマ：J－SOX　1年目の総括と、2年目に向けた経営者、そしてシステム監査人に向けてのアドバイスなど（調整中）
講師：あずさ監査法人パートナー遠藤誠氏（当協会理事）
9月以降の月例研究会は現在調整中。

7.9 会計（仲）
前期の会計監査の日程が決定した。
会計監査：8月15日㈯ 13：00 ～ 17：00

7.10 会長
平成20年度末の認定失効状況は次の通り。
・公認システム監査人失効通知者数：68人、内、復活した者：23人
・システム監査人補失効通知者数:60人、内、復活した者：6人

（以下はメール報告）

7.11 法人部会（小野）
自治体向けセミナーの照会が2自治体からありました。対応中です。

7.12 北信越支部（森）
〈北信越支部 福井県例会〉-
1.日時：6月20日㈯ 13：00－17：00
2.会場：福井繊協ビル 803号室
例会出席者：14名
角屋様，栃川様，森様，國谷様，福田様，小嶋様，森田様，清水様，宮本（ITC福井；木戸様，坪田様，齋藤様，佐藤様），
（講師：中部支部　大野様）
3.例会議題
⑴挨拶及び連絡
⑵報告「J－SaaSとクラウド」 栃川 昌文　氏
⑶「中小企業のセキュリティ監査」
中部支部）大野 淳一　氏
⑷システム監査研究会報告　森 広志　氏
「IT経営ロードマップ」より
・事例研究：イオン株式会社、ウォルマートのＩＴ戦略など
⑸情報セキュリティ監査研究会経過報告
宮本 茂明　氏
⑹研究会ビデオの貸し借り

7.13 中四国支部（溝下）
－実績－
6月度月例会
日時：6月17日㈬ 18：30 ～ 20：30
内容：「ビジネス・プロセス・マネジメント（BPM）入門」
場所：広島市まちづくり市民交流プラザ 会議室A
－予定－
7月度月例会
日時：7月15日㈬ 18：30 ～ 20：30
内容：「金融業務における情報セキュリティと暗号技術―暗号アルゴリズムの世代交代問題を中心に―」
場所：広島市まちづくり市民交流プラザ
会議室B

7.14 北海道支部（大舘）
●6月勉強会
日時：6月25日㈭18：30 ～ 20：30
場所：㈱富士通北海道システムズ　会議室
テーマ：「ソフトウェア開発における
モデル契約書」
講師：岡田 昌彦

7.15 中部支部（田中）
支部活動計画　7月支部例会（予定）
1.日時及び場所
7月11日㈯ 14：00 ～ 17：00
東桜第1ビル　5－1会議室
2.内容
⑴事務連絡
⑵講演Ⅰ
「CMMIとその導入に向けて」
安井 秀樹　様
⑶ご講演Ⅱ
「SaaS（技術編）」　関口 幸一　様

7.16 東北支部報告（高橋）
1.公認システム監査人の面接　1名対応
2. 5月例会
日時：5月23日㈯ 14：00 ～ 17：00
場所：アエル 28階 エル・ソーラ仙台「研修室2」
議事内容
1.連絡、報告
⑴本部情報
⑵その他
・9/12㈯-13㈰の山形合宿について
2.勉強会：「SaaS勉強会」第1回 J-SaaSについて
①基本事項の解説／説明

②現在のJ-SaaSの状況
③今後の普及への意見交換　(別紙)
次回：7/18㈯　14：00～17：00
仙台AER6階 情報・産業プラザ「特別会議室」
勉強会「クラウドコンピューティングに関する情報交換」
3.ワークショップ
10月24日のアナリスト協会の全国大会を仙台実施に合わせITCみやぎと共催で10月23日～24日に実施予定。

7.17 九州支部（福田）
●6月度月例会（第223回）
日時：6月20日㈯13：00～17：00
会場：早良市民センター　第3会議室
内容：ビデオ視聴「金融業務における情報セキュリティと暗号技術―暗号アルゴリズムの世代交代問題を中心に―」
報告事項⑴参加イベント報告（舩津）
⑵セキュリティ技術トピック（その4～5）（福田）
（開催予定）
●7月度月例会（第224回）
日時：7月25日㈯13：00～17：00
会場：早良市民センター　第1会議室
●8月度月例会（第225回）
日時：8月22日㈯13：00～17：00
会場：早良市民センター　第1会議室

議事録確認
議　　長　　鈴木　信夫
議事録署名人　　馬場　孝悦、金子　長男
以上

第145回月例会報告

No.1362　渡辺　孝

日時：2009年4月28日㈫18：30～20：30
場所：御茶ノ水　総評会館
講師：日本銀行金融研究所
情報技術研究センター長　岩下直行　氏
演題：
「金融業務における情報セキュリティと暗技術
－暗号アルゴリズムの世代交代問題を中心に－」

■講演内容
⑴日本銀行金融研究所情報技術研究センター（CITECS）について
⑵従来の金融情報システムの特徴
⑶インターネット・バンキングの普及と金融機関のセキュリティ対策の変質
⑷偽造キャッシュカード問題とその教訓
⑸暗号アルゴリズムの世代交代問題
⑹暗号を巡る専門家と実務家（ユーザー）のギャップ－「128bit SSL」という用語を巡って
⑺これからの課題

1.日本銀行金融研究所情報技術研究センター（CITECS）について

日本銀行金融研究所情報技術研究センター（CITECS）は、金融機関が情報化社会において直面する新たな課題に適切に対処していくために2005年4月1日付けで設立され、①国際標準化活動、②重要情報インフラ保護対応、③情報セキュリティ技術に関する研究、等を行っている。

2.従来の金融情報システムの特徴

金融機関の運営する情報システムに対する一般的なイメージには、「高度な安全性が要請される」、「旧弊な技術」、「最先鋭のセキュリティ・システム」といった様々なものがあるが、その特徴としては、①閉ざされたネットワーク、②高額な取引金額、③充実した障害対策等があった。しかし、インターネット・バンキング等のオープン・ネットワーク化の進展により、金融情報システムは変化していくこととなった。

3.インターネット・バンキングの普及と金融機関のセキュリティ対策の変質

現在、87%の金融機関がインターネット・バンキングを提供中であるが、インターネット・バンキングは、①外部から見えるシステムである、②利用者のリテラシーに依存する、③攻撃されやすい、④セキュリティ等のノウハウの蓄積に時間がかかった、という点で従来の外部接続システムと大きく異なっていた。

インターネット・バンキングはフィッシィングやスパイウェア等に狙われやすいため、利用者の認証技術が重視され、これまでに時代とともに様々な方式が登場してきた。専用ソフト方式は複雑で利用者に受け入れられず、その後登場したSSL＋パスワード認証方式はセキュリティ上の問題があった。その後、乱数表によるチャレンジ・レスポンス方式、ワンタイムパスワード方式といった、より安全な方式に移行したが、いずれの方式も完璧ではなく、様々な課題を抱えている。

4.偽造キャッシュカード問題とその教訓

2004年頃から偽造キャッシュカードによる不正預金取引が急増、社会問題化し、金融機関の情報セキュリティ対策に関する世間の関心が高まった。被害額が少ない割に偽造キャッシュカード問題が社会問題化した理由として、他の偽造犯罪とは異なり、一般の消費者（預金者）が被害にあい、その当時はまだその損害が補償されないという性格によるところがあった。

偽造キャッシュカード問題の原因として、①偽造の容易な磁気ストライプカードであること、②4桁の暗証番号の限界、があったが、また、日本特有の問題として、預金限度額の高さもあった。このため、被害を限定するための緊急逃避的な対策として、預金引出限度額の引き下げが実施された。そしてこの対策の方が、ICカードや生体認証などの事前防止対策よりも被害の沈静化にはより有効であった。

現在、偽造カード対策は、次のステップとして、①全面的なICカード化、②暗証番号の適正化、③金融機関内部における暗証番号の取り扱いの厳格化、に向かっている。

現状、短期的な課題と中期的な課題として考えるならば、短期的な課題としては、磁気ストライプカードと4桁暗証番号による預金引出、IDとパスワードだけのオンライン・バンキング、カード番号と氏名をSSL入力するだけのクレジットカード取引、といったセキュリティ上の問題の解決を、長期的な課題としては、暗証技術の脆弱性や生体認証による攻撃法に対する問題の解決を、それぞれ挙げることができる。

5.暗号アルゴリズムの世代交代問題

「暗号アルゴリズムの2010年問題」とは、現在金融分野で利用されている暗号アルゴリズム（2key-トリプルDES〈共通鍵暗号〉、1024bitRSA〈公開鍵番号〉、SHA-1〈ハッシュ関数〉）が、2010年以降、その安全性の観点からみた寿命が尽き、利用に適さなくなると指摘されていることである。

CRYPTREC（電子政府推奨暗号の安全性を評価･監視するプロジェクト）は､2003年2月に「電子政府」における調達のための推奨すべき暗号のリスト（電子政府推奨暗号リスト）を公表し、その利用を働きかけてきた。しかし、その電子政府推奨暗号も、今回の世代交代の対象となっている。現在、CRYPTRECでは、リストの改定作業を進めている。

金融業界にとって、現在使用している暗号技術の強度の低下は、看過できない問題であり、それは過去において、DES暗号の強度低下やRSAの鍵長の問題からの経験知として得たものである。

しかし、現在生じている暗号技術の強度低下に関して、直接的な攻撃の成功が、未だ発表されていないことや強度低下がどれだけインパクトのあるもので、どの程度のスピードで顕在化するか把握できていないことで、次世代暗号への移行をコスト面含め慎重に見極めたいという声も根強い。コスト面では、新規システムへの次世代暗号の導入については今と大差ないが、既存システムに利用されている従来型暗号の次世代暗号への置換えにはかなりのコストがかかると考えられている。

6. 暗号を巡る専門家と実務家（ユーザー）のギャップ―「128bit SSL」という用語を巡って

暗号の安全性評価、コストとリスク等に関して、専門家と実務家の間にギャップが生じてい

る。また、金融機関のホームページ上は、「128bit SSL」を採用している旨の表記にとどめているものの、実際にはそれよりもさらに安全な暗号アルゴリズムが既に実装済であり、表記と実態とが乖離しているケースもある。今後は、①専門家側が評価に当たって実務上の影響を分析し、考慮する枠組みを整備するとともに、②ユーザー側が評価結果を実務にきちんと反映させる体制に、徐々に移行していくことが必要ではないかと考える。

7.これからの課題

金融情報システムのセキュリティに残された課題として次のようなものがある。

①海外では、暗証番号はＡＴＭで暗号化することが一般的だが、日本では暗号化は必須とは考えられていない。これについては、海外のクレジットカードブランドからの批判もあり、国内でも暗号化を実施している金融機関が出てきている。

②現在、回線番号やICカードで一般的に使われている暗号アルゴリズムは、あと僅かで安全性の保証が切れる見込み（暗証技術の「2010年問題」）である。

③キャッシュカードをICカード化し、生体認証を導入しても、それに対応していない磁気ストライプを利用したキャッシュカードは引き続き大量に流通しており、スキミング犯罪の芽は摘まれていない。

④生体認証技術については、生体情報の偽造を用いた攻撃法の存在が指摘されているが、中身がブラックボックスのため、どのようなリスクがあるのか評価が難しい。

⑤インターネット・バンキングやファームバンキングは、フィッシングやスパイウェアによって暗証番号や乱数表情報の一部が漏洩し、不正な送金が行われるリスクが一部で顕在化している。

従来の金融情報システムにおけるセキュリティ対策は、クローズド･ネットワークを前提に、情報の秘匿が基本とされた。このため、一旦新しい脅威が発生すると、その対応が後手に回ってしまう傾向があった。金融機関にはインターネット・バンキングへの攻撃や偽造カード問題に対して適切に対処できなかったという反省があり、銀行システムがインターネットの技術を取り入れて遅ればせながら変革を進めようとする中で、新しい考え方に基づく情報セキュリティへの適切な対応が必要とされている。そのためには各金融機関内における情報セキュリティ技術に関する専門家の育成と、業界内で適切に情報を共有する体制を整備・強化していくことが求められている。

■所　感

岩下氏は一見するとやはり銀行員風、メガネをかけて髪形は７：３分け、スピーチには切れがあった。約80枚にもなるスライドを使用した講演を、ポイントを漏れなく説明したうえで、時間どおりに終わらせたことには驚嘆した。

講演内容もホスト系を中心とした旧来型の金融情報システム（いわゆるレガシーシステム）からインターネット・バンキングシステムを中心とした新しい金融情報システムへの変遷にセキュリティ技術を絡めた説明は大変わかりやすいものであった。

金融取引は私たちにとって身近なものであり、そのセキュリティに関する問題は他人事ではない。我々公認システム監査人（補）としても「暗号アルゴリズムの世代交代問題」を注視し、氏の危惧する「暗号化に関する専門家とユーザーとの間の認識のギャップ」を埋めるような活動を展開できるように努力していきたいものである。

以　上

エッセイ・論文募集

会員の皆様、SAAJ 会報の読者の皆様

会報編集部では、次の通りエッセイ（論文募集要項に該当しない投稿）、論文を募集しています。会員の積極的な投稿（電子メールで簡単に送付できます）をお願いいたします。

また、会報の電子化、会員外むけ情報発信やメルマガ発行などについて、皆様のご意見を寄せてください。

投稿先：saaj-kaihoh @ yahoogroups.jp

本号の特集で紹介した「システム監査を広げる」事例研究と議論に参加しませんか。
若い世代のSE職によるシステム監査に対する考え方、システム監査試験の合格を目指す方、SEとして監査人として活躍していられる女性、あるいはシステム監査人として企業活動の活性化や地域社会への貢献に関心をお持ちの方など、歓迎します。上記の投稿先へお問合せください。

エッセイ募集要項

SAAJ 創設20 周年のイベント開催中から、記念講演会や論文集の発行など、各専門部会および支部ごとに、活動の成果をまとめて発表する場も増えてきたと思われます。
会員、読者の皆様も、是非、手記にまとめて気楽に投稿いただき、システム監査の歴史に記録を残しませんか。会報編集部が支援させていただきます。エッセイの投稿には記名をお願いすること以外には、特に制約はなく、自由な創意工夫が反映できます。

会報掲載論文募集要項

1．論文の内容
　システム監査･セキュリティ監査(関連を含む)の実務の裏づけのある内容で、システム監査･セキュリティ監査(関連を含む)の啓発、普及、理論深化、情報提供、実践、手法開発等　に役立つ論文。既発表論文は除く。

2．字　　数：６千字以上、１７千字　程度（図表を含める。上限は目安とする）

3．提出方法：ＭＳ-Wordで作成し、会報編集委員会あて送付する。
（メールに添付する場合は、パスワードを設定する）

4．審　　査：会報編集委員会内に設ける論文審査委員会にて、審査を行い、掲載に値するか、及び内容の優劣を判断し、掲載する場合は、２万円以上、６万円の範囲で原稿料を支払う。審査の内容は公表しない。

5．ここに掲載した論文は、公認システム監査人（補）継続教育で、10時間/1稿として認める。

6．掲載論文募集締め切り：常時受け付けとし、会報編集委員会より打ち切りのお知らせがあるまで継続する。

第13回内部統制監査人セミナー開催のご案内

8月24日㈪、25日㈫、26日㈬3日間の日程で、内部統制監査の実践能力を修得するための内部統制監査人セミナーを開催します。

以下に記載の特典もございますので、是非受講をご検討ください。

＊本セミナー修了者は、公認システム監査人の認定申請にあたり日本システム監査人協会が別に定める所定の期間をシステム監査実務経験期間に算入することができます。

＊修了者又は受講者が、公認システム監査人又はシステム監査人補である場合、セミナーの実時間を継続教育の認定時間に算入することができます。

1. 内容：

1.1 財務報告に係わる内部統制に関する基礎知識を習得していることを前提に、IT全社統制・IT全般統制・IT業務処理統制のポイントを説明します。

1.2 受講者は外部のコンサルタントとして、被監査企業の内部監査部から、内部統制の評価と助言を依頼されたと想定し、

①IT全社統制・IT全般統制・IT業務処理統制について、被監査企業から提供された内部統制成果物とヒヤリングに基づいて内部監査を実施します。

②監査によって把握した問題点や課題を指摘し、改善提案を含む監査報告を行ないます。

2. 日程及び会場：

	日　時	会　場
第13回	2009年8月24日㈪～8月26日㈮ （3日間共、AM10：00～PM5：00）	情報セキュリティ大学院大学（IISEC） JR横浜駅西口下車徒歩3分

情報セキュリティ大学院大学：http://www.iisec.ac.jp/about/map.html

3. 費用：費用：147,000円（一般）、126,000円（SAAJ会員）
（費用には、教材費・食事代・消費税が含まれます。）

4. 受講していただきたい方：

・J－SOX対応担当者、ITの内部統制の評価・監査に関わる管理者及び担当者。
・ITの内部統制の構築、運用に関わる管理者及び担当者
・その他IT内部統制の知識を整理したい方

5. 募集人員：各回20名（最小催行人員6名）
最少催行人数に達しない場合は、開催を中止することがあります。

6. 受講申し込み方法：当協会ホームページ（http://www.saaj.or.jp/）から
来る8月10日までにお申込み下さい。

以上

（編集後記）

監査の担い手としてのシステム監査員（候補者）は、女性、若手、団塊世代など、年齢層も多様となり、監査員の育成研修の場面や監査対象も広がっています。また会員の藤谷弁護士から紹介いただいたIT－ADR（ITの開発運用に関わる裁判外の紛争解決）に対しても、システム監査人が持つ経験が評価されているようです。しかしながら、紛争当事者の双方にシステム監査人が支援する形を早期に定着させて、問題解決を早期発見する、というよりも、問題となる前に課題を整理して計画変更、関係者の条件を調整して「争いごと」に要する時間や費用、重要な機会の消失を防ぐことが可能であれば、より付加価値を高めることができると考えます。

今回は、システム監査をITが関係する分野への広がりを加速させるには、どのような方法があるか、またシステム監査の技術経験をもっと広く普及させるにはどうするか、という観点から素材を提示しました。これから試行を重ねていきます。

これからの監査人の活動について、数名の方にご意見を伺いながら、叱責を覚悟でまとめました。最後に次の質問を一緒に考えてみてください。

あなたは、

1）（一般的に）監査と聞いて、うれしいでしょうか。
2）（被監査側の立場で）監査をうけて、うれしいでしょうか。
3）（監査側の立場で）監査をして、うれしいでしょうか。

これらの3つの立場で、喜ばれるような監査にするには、どうすればいいでしょうか。

このように自由に、監査活動について意見交換をしていける方、ぜひご意見を寄せてください。

（竹下）

発行所　特定非営利活動法人　日本システム監査人協会
発行人　鈴木　信夫
事務所　〒103−0025
東京都中央区日本橋茅場町2−8−8
共同ビル（市場通り）6階65号室
TEL. 03（3666）6341
FAX. 03（3666）6342
事務局メール　saajjkl@titan.ocn.ne.jp
ホームページ　http://www.saaj.or.jp/

会報担当委員
竹下　和孝　吉田　裕孝　仲　厚吉
桜井由美子　成　楽秀　片岡　学
木村　陽一　須田　勉　藤野　明夫
山田　正寛

※会員のみなさまからの投稿（連載、随筆等何でもOK）を募集します。記名記事は薄謝進呈します。書籍紹介欄もありますので、執筆された方はお知らせ下さい。
会報担当メール　saaj-kaihoh@yahoogroup.jp