特定非営利活動法人
SAAJ 日本システム監査人協会報

［特集］ＣＳＡフォーラム

ＣＳＡフォーラムも５回目を迎えます。

ＳＡＡＪが運用しているＣＳＡ（公認システム監査人）制度では、ＣＳＡ相互の研鑽の場として、フォーラムを開催しています。これまでに、次のように５回のフォーラムを開催し、少人数ならではの贅沢な環境で発表者と参加者の緊密な討議、懇親を持ちながら、議論を盛り上げてきております。

これまでのところ東京に限定して開催していますが、これまでの開催状況は次の通りです。

【第１回ＣＳＡフォーラム】2008年9月30日
テーマ：「ＣＳＡの成功法則」
発表者：竹下 和孝　氏
【第２回ＣＳＡフォーラム】2008年11月26日
テーマ：「ＣＳＡに求められる新たな役割」
発表者：三谷 慶一郎　氏
【第３回ＣＳＡフォーラム】2009年1月27日
テーマ：「ＣＳＡ実践報告＆基準研紹介」
発表者：松枝 憲司　氏
【第４回ＣＳＡフォーラム】2009年3月25日
テーマ：「内部監査から見たシステム監査」
発表者：島田 祐次　氏
【第５回ＣＳＡフォーラム】2009年6月1日
テーマ：「組織人を幸せにするマネジメントシステムを目指して」
発表者：桜井 由美子　氏

今回は、そのうちの、第二回以降の開催報告をまとめてお届けします。

第２～４回ＣＳＡフォーラム開催記録

記録：斉藤　茂雄（№6005）

【はじめに】

ＣＳＡフォーラムはＣＳＡ・ＡＳＡを対象にシステム監査に関する実務や事例研究、理論研究を通して、ＣＳＡ・ＡＳＡのシステム監査業務に役に立つ研究を行うことを目的に2008年に発足した。

第1回目は昨年9月30日に開催し、内容は協会会報No.106（2009年2月発行）に報告させていただいた。その後フォーラムを3回開催し、報告が大変遅くなってしまったが今回ここに概略を報告し記録する。

【第２回ＣＳＡフォーラム】
テーマ：「ＣＳＡに求められる新たな役割」
発表者：三谷 慶一郎　氏
（株式会社ＮＴＴデータ経営研究所
パートナー・情報戦略コンサルティング本部長）
会　場：東京都港区芝　ＮＥＣ第２別館
日　時：2008年11月26日　18：30～20：30

■発表内容

――ＩＴ投資を取り巻く環境
――ＩＴマネジメントとは
――効果創出とＣＳＡ
――効率的投資とＣＳＡ
――リスク低減とＣＳＡ
――経営者に気づきを与える

三谷氏は日本電信電話株式会社、株式会社ＮＴＴデータを経て、1993年より現職に従事し、企業や行政機関における情報化戦略立案や情報システム企画等に関連するプロジェクトを多数手懸ける。近年は、ＣＩＯが行なうべき役割・機能に関する調査等に取り組んでいる。主な著書に「ＣＩＯのＩＴマネジメント」「ＩＴ統制監査実践マニュアル」などがある。

目次（報告者）

発表前段では諸外国と対比した日本のIT投資の特性の解説があった。「我が国のIT投資は緩やかに上昇を続けているものの、伸びは停滞し、米国や韓国と大きな開きが出ている。」「攻めのIT投資・守りのIT投資と言った時、日本は攻めのIT投資効果にあまり期待していない。」「IT投資と生産性向上との相関で見ても米国では相関が高いとする傾向があるのに対し、日本では相関が低いとの評価が多く、特に非製造業においては相関係数はかなり低いものとなっている。」とのことである。三谷氏は「企業等が、IT投資効果の最大化を目指し、健全なITマネジメントを実現するために、CSAに求められることが多く存在するはずで、従来のCSAの役割を超えた議論が必要。」と強く主張する。三谷氏が考えるCSAに求められる新たな役割のポイントを簡単に述べる。

1. 効果創出に向けたCSAの役割

CSAとして「IT投資の有効性評価に関与する・関与する力をつける」といった意識・意欲が必要。今後、企業のIT投資の有効性「開示」の第三者評価が求められる可能性もある。有効性評価には「効果可視化」をいかに行うかがポイント。ITガバナンス協会が提唱しているVal-ITも参考になる。

2. コスト適正化に向けたCSAの役割

ITコストが「適正なコストであることを評価する」ことは容易でないが、これをシステム監査人に求めてくることも十分ありえる。「高いか安いか」ではなく、「適正なプロセスを経て投資が行われているか」を第三者的に確認することは可能。

3. リスク低減に向けたCSAの役割

リスクを可視化し、低減させることは、システム監査人の基本的役割。

4.「経営者に気づきを与える」という役割

企業にとって経営層がITを経営資源のひとつと認識し、IT投資が自らのミッションであることに気づくことが重要。「外部の識者や中立的立場」でITが欠かすことの出来ない経営資源であることを経営層に理解させることもCSAのひとつの役割。

■所感

第3回フォーラムも第1回同様30名近い参加者を得ることができた。三谷氏の発表は「従来の枠を超え、システム監査のドメインを広げていくことが重要。」「経営者の役に立つと認知されることが、CSAの地位向上にもつながる。」ということで締められたが、CSAのあり方を考え、CSAとしての活動を模索する参加者にとって、大変貴重なご発表であった。

【第3回CSAフォーラム】

テーマ：「CSA実践報告＆基準研紹介」
発表者：松枝 憲司 氏
（株式会社ビジネスソリューション 代表取締役）
会　場：東京都品川区大崎 日立情報システムズ 本社
日　時：2009年1月27日　18：20～20：20

■発表内容

――CSA活動
・自己紹介＆各種実績紹介
・CSA資格の活用
・2009年度のビジネスチャンス
――システム監査基準研究会
・研究会の実績紹介
・2009年度活動計画

松枝氏は独立系のソフトウェアハウスに25年勤務し、その間システム監査の業務経験があったことから、2002年2月起業して今日に至った。起業当時は「ノウブランドCSA」であり、非常に「リスキーな出発」だったと回想する。成功するには「良質なブランドを創って行くしかない」と考え、多くの関連資格の取得と当協会等関連団体への所属と活動、著作活動に心がけてきた。協会編の「実践マニュアル3部作」をはじめ、特に「図解でわかる部門シリーズ情報システム部」は10,000部以上の発行部数を数えている。

松枝氏は起業当時と比較して「システム監査ビジネスを取り巻く環境は」大きく変わったと見ている。「都銀統合等大規模システムの事故多発」から始まり、「コンプライアンス関連事故」「個人情報保護法や関連セキュリティ事故の多発」「日本版内部統制報告制度（J-SOX）執行」等々の環境。過去「内部統制」というと言葉の説明が大変だったが現在では一般用語になるなど、これらを背景に「システム監査ビジネスは確実に増大」し、ビジネスの「土壌が整って来た」と実感している。

フォーラムでは松枝氏の流通・サービス・製造等官公庁も含めた多業種での実績の紹介があった。内容はシステム監査のみではなく、システム構築支援、セキュリティ関連支援、セミナー・研修の実施、またはこれらの複合、更には企業再生・経営改革計画支援といった分野にと、幅広い実績を持つ。松枝氏は「システム監査を実施し、経営者に監査報告と助言提案を行い、結果としてその後のビジネスに繋がるケースが多い」と言う。「経営者に直接報告できるシステム監査は非

常に有効な営業ツール」でもあると言う。「CSAなんて…」と思う方も居るが、松枝氏の体験では「CSA：公認監査人」という「中立で独立したシステム監査人」という評価と何より全国で600名程度の希少価値のある集団である点にアピール力があるので、積極的にCSAという肩書きを前面に出しているということである。

現在考えているビジネスチャンスとして「企業再生/経営革新計画的アプローチ」と「After J-SOX」の紹介があったが、報告は別の機会に譲りたい。次に、松枝氏が当協会で積極的に携わってきた「システム監査基準研究会」の紹介があったが、既に多くの場面でその成果を見ているので、報告は省略する。

■所感

第3回フォーラムでは「独立CSAのビジネス実践報告」という生々しいビジネス事例を交えた大変貴重なお話がうかがえた。CSAというステータスをアピールしてビジネスに活かすことについては心強く思う方が多いのではないか。また、CSAフォーラムでは例会の後、発表者を囲んで懇親会を開いているが、その席で基準研に入会し松枝氏と共に活動をしたいという方が3名も現れ、フォーラムの狙いのひとつである「CSAの連携」に実りを得ることもできた。

【第4回CSAフォーラム】

テーマ：「内部監査から見たシステム監査」
発表者：島田 祐次 氏
（東洋大学　総合情報学部　教授）
※発表当時：中央大学大学院客員教授、
東京ガス株式会社 監査部 監査マネジャー）
会　場：東京都品川区大崎 日立情報システムズ 本社
日　時：2009年3月25日　18：20～20：20

■発表内容

――システム監査を取り巻く状況の変化
――二つの側面をもつシステム監査
――ISACA/ITGIの動向
――IIA（内部監査人協会）の動向
――システム監査（内部監査）の現状
――システム監査の取組事例
――システム監査の付加価値向上に向けて

島田氏は東京ガス株式会社で早くからシステム監査業務に関係し、2000年には同社監査部に所属し会計監査に始まり、業務監査、システム監査業務に従事した。この間個人情報保護や内部統制、ERMにも携わって来た。一方では日本大学の非常勤講師、中央大学大学院の客員教授なども歴任し、CSAは勿論公認情報システム監査人（CISA）、公認内部監査人（CIA）等の資格を持つと共に、「COBIT実践ガイドブック」「内部監査人のための実務ハンドブック」「最新J-SOX法がよ～くわかる本」「情報システム監査の基礎と実践」等々多くの著作も手懸けている。今回のフォーラムでは島田氏監査業務についての深い造詣に基づくお話がうかがえた。

紙面の関係から主なスライドタイトルを元に紹介する。

1.「システム監査を取り巻く状況の変化」「二つの側面をもつシステム監査」

主なスライド：「混沌とするシステム監査」「システム監査に関する不安」「位置づけの再確認の必要性」「ITガバナンスとは何か？」「ITガバナンスとコーポレートガバナンス」「ITガバナンスとIT統制の概念整理」「J-SOX、会社法、情報セキュリティの関係」「システム監査と情報セキュリティ監査との違い」「個人情報保護監査との違い」「内部監査と外部監査の二つの側面」「内部監査の2つの目的」

情報セキュリティ監査、個人情報保護監査、IT統制といったシステム監査の概念の錯綜状態の提示とこれらの状況整理、解説をいただきシステム監査の位置づけの再確認を行った。

2.「ISACA/ITGIの動向」「IIA（内部監査人協会）の動向」「システム監査（内部監査）の現状」

主なスライド：「COBITとシステム監査の関係」「COBITを監査で使うメリット」「COBITを使った監査の視点」「Val IT（IT投資の企業価値ガバナンス）とは？」「GTAGとは」「GTAGの主要項目1～11」「情報システム監査の実施状況」「監査対象項目の状況」「監査テーマの状況」

IIAが公表したGTAG（Global Technology Audit Guide）のGTAG－1～GTAG－11の主要項目見出しを日本語訳で紹介いただいた。GTAGはIIAが経営者に対するITマネジメントとコントロールのガイダンスとして出したもので、ITマネジメントとコントロールの要点がトピックス的にまとめられている。

3.「システム監査の取組事例」

主なスライド：「コーポレートガバナンス強化の取り組み」「情報システム監査の実施体制」「情報システム監査の取組みの概略」「“総合監査”導入の経緯」「総合監査の実施方法」「総合監査の視点」

東京ガス株式会社様の内部監査及び情報シス

テム監査の紹介をいただいた。

4.「システム監査の付加価値向上に向けて」

「主なスライド：「なぜ監査は嫌われるのか？」「付加価値とは何か」「システム監査の価値向上サイクル」「多面的な分析の必要性」「多面的な評価の必要性」「監査工学の必要性」」

システム監査の付加価値向上にはシステム監査の品質向上が必要。監査プロセスの向上に加え役に立つ指摘や助言が重要。そのためには監査人のスキルを向上させて、専門職としてのステータスを高めることが大切。

■所感

第4回フォーラムは、日頃著作やセミナー等の講師でもご活躍の島田氏の幅広い有益なお話を無償で且つ少人数で拝聴できるという、CSAフォーラムならではのパフォーマンスの高い集まりであった。本稿を起こすに当りスライドを再読し、システム監査にまつわる諸事項の論点が凝縮されたスライドであることに改めて気づかされた。また、筆者は自社内システム監査を仕事にしているが、他社の監査体勢、監査手法等の情報を知る機会はまれであり、その意味でも今回のお話は貴重で、特に総合監査の考え方は参考になり感謝している。

以上

CSAフォーラムについて

CSAフォーラムはCSA・ASAを対象にシステム監査に関する実務や事例研究、理論研究を通して、CSA・ASAのシステム監査業務に役に立つ研究を行うことを目的に2008年に発足しました。本活動を通じCSA・ASA同士のフェイスtoフェイスの交流を図ることにより、相互啓発や情報交換を行い、CSA·ASAのスキルを高め、よってCSA・ASAのステータス向上を図ることも狙いにしています。

フォーラムの開催は隔月で1回30名程度の参加を原則としています。参加は本フォーラムに賛同頂いたCSA・ASAの方に事前登録頂き、各開催に先立ち事前登録者に開催案内し、参加いただく形態をとっています。

お問合せは以下までメールにてお願い致します。

特定非営利活動法人 日本システム監査人協会
CSAフォーラム事務局
（csaforum01@friend.ocn.ne.jp）

日本システム監査人協会 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

No.947 梶川 明美

平成20年11月15日㈯、日本システム監査人協会設立20周年記念講演会と西日本支部合同研究会を北信越支部で開催いたしました。当日は他支部やITコーディネータ協会からも多数の参加を頂いて盛会となりました。

お世話になった皆様方に深く感謝申し上げます。

1.日 時：平成20年11月15日㈯
13:00～17:30
2.会 場：富山地鉄ホテル 11F会議室
3.テーマ：「システム監査これからの10年について」
4.後 援：経済産業省 中部経済産業局
富山県 特定非営利活動法人
ITコーディネータ協会
日本システムアナリスト協会
NPO法人 ITコーディネータ富山
特定非営利活動法人
石川県情報化支援協会
特定非営利活動法人
福井県情報化支援協会
5.次 第：
13:00～13:10
開会挨拶 日本システム監査人協会
副会長 和貝 享介 氏

13:10～14:10 基調講演1
「IT管理と現在の課題について」
城西国際大学客員教授 櫻井 通晴 氏
14:10～15:10 基調講演2
「IT投資対効果の最大化に向けて」

日本システム監査人協会
副会長　三谷 慶一郎 氏
15:20～16:20　講演
「金融機関と決済システム
システム監査の視点から」
日本銀行金融機構局企画役　大石 正人 氏
16:20～17:20　北信越支部活動成果
「戦略性のシステム監査手法研究」
北信越支部　システム監査研究チーム
チームリーダ　森　広志
「情報セキュリティアセスメント
運用構築アプローチ手法研究」
北信越支部　セキュリティ監査研究チーム
チームリーダ　宮本 茂明
17:20～17:30　閉会挨拶
日本システム監査人協会　北信越支部長
森　広志
17:40～19:40　懇親会
富山地鉄ホテル 11F レストラン アルシェフ

●基調講演１

「IT管理と現在の課題について」

城西国際大学　客員教授　櫻井 通晴　氏
（報告　№583　白井　正）

1. 講演概要

企業価値の向上を指向する戦略的IT投資を実現するためには、現行システムの問題点、CIOの重要性、IT投資の評価手法、IT内部統制、アウトソーシング、ITSS(IT Skill Standard)といった多くの観点からの考察が必要である。

最終的には適切なITガバナンスを実現するための人材の育成が重要であり、それがコーポレート・レピュテーションの向上、ひいては企業価値の向上をもたらす。

2. 講演要旨

巨大化、複雑化、硬直化し、継ぎはぎだらけとなって、ブラックボックス化してしまった現行の大多数のシステム環境において、戦略的IT投資を実現するためには、以下の諸点から考察する必要がある。

⑴CIOの役割と現状

経済産業省商務情報政策局「CIOの機能と実践に関するベストプラクティス」全18回の座長の経験から、わが国におけるCIOの役割と現状が見えてきたが、CIOには経営革新を遂行するに際しての役割（IT革新なくして経営革新なし）、あるいは、コスト、プロセス、効果等を可視化することによる経営とITとのコネクション（つなぎ）としての役割などが重要である。

また、ITの水準と経営効率とを調整するためのITガバナンスを考える場合においても、CIOの役割は重要である。

⑵IT投資の評価

ITの投資水準と経営効率とを向上させるためには、先ずIT投資の評価を正しく行う必要がある。

IT投資の理論的評価モデルとしては、費用便益アプローチより総合評価アプローチが望ましいと考えるが、基盤整備効果、戦略的効果、経済的効果のうち、計数で表わし難い戦略的効果をいかに評価するかが重要である。

IT投資を総合的に評価するためには、非財務的効果（財務、顧客、内部、学習と成長といった視点）を評価できる、あるいは無形の資産を可視化できる等の特徴を有する、バランスト・スコアカードの適用を考える価値は大きいものと考える。

また、導入の負担はたしかに大きいが、戦略マップ（戦略的優先順位の定義）作成の意義も大きい。

なお、一時ERPがブームとなったが、欧米でのベスト・プラクティスを受入出来るか否か（服にあわせるか、体にあわせるか：トヨタCIO）によって、導入効果の評価は分かれる。

⑶IT内部統制

内部統制もまた、企業価値を維持・創造するうえで重要である。

すなわち、内部監査人は、業務監査、会計監査だけでなくコンプライアンスとコーポレート・ガバナンスの質を高めることにより、経済価値、社会価値、組織価値を含む企業価値を

向上させることができる。

この点については、業務監査、会計監査ではない、経営監査といった視点で論ずることも有用である。なぜなら、新しい意味での内部統制は、従来議論されてきた経営監査をコンプライアンス（法令順守）と読み替えたと解釈することができるからである。

なお、内部統制は企業のあらゆるレベルの者によって遂行されるプロセスであるが、ITに関しては、コーポレート・ガバナンス、ITガバナンス及びITマネジメントの位置づけ、相互の関連が重要である。

ここで、コーポレート・ガバナンスにおいては、米国のトレッドウェイ委員会組織委員会（COSO）の内部統制フレームワークが、またITガバナンスにおいては、IT統制の国際的ガイドラインであるCOBITのフレームワークが必須の概念として重要な意味を持つ。

⑷アウトソーシング

IT投資の1形態としてのアウトソーシングについても、その成功の要件について検討する必要がある。

日本では、導入された制度、システム等の事後評価を行うことは少ないが、安値受注の弊害、不当な導入後保守料等の問題を排除するためには、事後評価も重要である。

ここでは、サービスレベル・アグリーメント（SLA）の活用が有効であるが、それも含めてパートナー会社との連携強化が必須である。

⑸IT人材の育成とITSS

IT投資の成功のための最も重要なファクターは人である。

ユーザーとベンダーのIT人材を、いかに効率的に育成するかが重要となるが、ITSS（IT Skill Standard；ITスキル標準）は人材育成のための1つの解答となる。

ここまで、戦略的IT投資を実現するための考察を行ってきたが、なぜ戦略的でなければならないか。それは戦略的なIT投資によってより大きな企業価値の向上が実現できるからである。

加えて、現代の社会においては、企業価値の向上を果たすためには、コーポレート・レピュテーション（企業の評判）の向上が必須になってきた。

コーポレート・レピュテーションを向上させるためには、適切なITガバナンスによる信頼性、透明性、好感度を高めていくことが必要であり、ここでは、CIOをはじめとする人材の育成が課題となる。

このように考えると、ITガバナンスは終局的には人間の問題に帰着する。

（所 感）

私事で恐縮であるが、十数年も前、社会人として地元の大学の人文系博士課程に進んだ際、ソフトウェアの開発費に係わるテーマで論文を書いた。私の博士課程は単位取得満期退学と言う形で終わったが、それはさて置き、当時、国内のその分野で参考となるものは、殆どすべてが櫻井先生に係わるものであったことを思い出す。

当時の私は、ソフトウェア会計という特定の分野のみを対象としていたが、実は、先生の関心は、既に企業価値向上を指向した管理会計に向かっておられ、全てがそのための基礎研究であったとのことである。講演後にその点を確認させて戴き、己の視野の狭さを恥じた。

今回の先生の講義も、様々な論点が全て「企業価値」に向かっておられ、非常に明快であった。先生が企業経営の現場で活躍されている理由を、改めて理解した次第である。

●基調講演２

「IT投資対効果の最大化に向けて」

日本システム監査人協会
副会長　三谷　慶一郎
（報告　№1403　竹村　徹也）

1. 講演概要

「システム監査人これからの10年」は、IT投資効果の最大化を目指し健全なITマネジメントを実現するために、従来の役割を超えて、パフォーマンス（効果創出）、コスト（効率的投資）、及びリスク（リスク軽減）の３要素を、システム監査の視点から管理して最適化を図っていく事が重要となる。更に経営者への気付きを与えるという役割を持つ事が必要になる。

2. 講演要旨

⑴IT環境を取り巻く環境

①IT投資の伸び

日本は緩やかに上昇を続けているものの、

90年前後のバブル経済崩壊後伸びは停滞しており、米国と大きな開きが発生している。
②IT投資総額
IT投資の日本はGDPに占める比率は３％～４％で非常に安定した水準を維持しており、社会活動を行う上で必要不可欠な要素となっている。
③攻めのIT投資ＶＳ守りのIT投資
日本では米国と比較して「攻めのIT投資効果」が少ない。
④維持・非戦略領域中心のIT投資
銀行業界におけるIT投資配分を例にとってみても、前向きに使う側への投資が少ない。
⑤IT投資と生産性向上との相関
日本は米国と比べると明らかにIT投資と生産性向上との相関性が低い。特にサービス業での生産性が低い。
⑥IT投資に関する効果の実感
IT投資効果があったという声は国際的に見ても少ない。しかし十分効果があったという実感は、日本が米国・韓国より10%低い。この差は何故かを分析する必要がある。
⑦マイナス方向のスパイラル
企業がIT投資対効果の最大化を目指し、健全なITマネジメントを実現するために、システム監査人のやるべき事は多い。

⑵ ITマネジメントとは

ITマネジメントはパフォーマンス（効果創出）、コスト（効率的投資）、及びリスク（リスク軽減）の３要素を、管理して最適化を図ることである。

⑶効果創出（パフォーマンス管理）

①パフォーマンス管理とは
日本ではIT投資に対して定量的評価を実施している企業は少ない。事後評価を定期的に実施している企業は、更に少ない。情報システムを企画した段階で想定していた効果がキチンと創出されていることを評価するために、効果の可視化は必須。効果の可視化はステークホルダーとのコミュニケーションツールであり、合意を得ることが効果創出には重要であり、成功の秘訣となる。効果創出はシステムだけでなく、業務プロセスの最適化、IT活用能力（ケイパビリティ）が必要である。
②効果創出に向けたシステム監査人の役割
システム監査人に第三者としての「有効性評価」を要望されているが、説明責任は大きくなってきている。システムだけでなく、業務プロセス・人・組織を含めて、効果を出すために何が足りないかを評価する事が重要であり、システム監査の視点は有効である。

⑷効果的投資（コスト管理）

①コスト管理とは
コスト削減はパフォーマンス低下、リス増大と表裏一体であることを留意し、ITポートフォリオという考え方で、リソースを最適配分し、IT投資案件に絶対額のみでなく意味を考える。「幾ら使うか」より「何に使うか」の管理が大事である。
②コスト適正化に向けた、システム監査人の役割
企業において適正なコストを維持することは困難であり、過剰要求しがちである。適正なコストであることを評価する事は容易でないが、システム監査人に求められる可能性がある。高いか安いかでなく、適正なプロセスを経て投資が行われているかを第三者的に確認し、調達プロセス・IT全般統制の適正性を監査する。

⑸リスク低減（リスク管理）

①リスク管理とは
情報システムを企画・開発・運用する上で発生する可能性のあるリスクを可視化し管理する。
②リスク低減に向けたシステム監査人の役割
リスクを可視化し低減させる事はシステム監査人の基本的役割である。開発側と利用側の狭間に課題があることが多いため、システム監査人が第三者として評価する。

⑹経営者に気づきを与える

①経営層がITの重要性に気づくこと
日本では経営層がITを自分のミッションと考えていないため、ITを十分活用した経営が出来ていない。又ITはコストとしてしか認識していない。このためにうまくITが使えていない。経営層がITを経営資源の一つと認識し、IT投資が自らのミッションであると気付く事が重要である。ITの持つ爆発的なイノベーションの力が変革の原動力となる。
②「経営者に気付きを与える」というシステム監査人の役割
経営者には外部の識者や中立的組織として、

成功事例を含めITがビジネスに与える効果だけで無くマイナス面を含めて、経営者とのコミュニケーションを継続する事で、ITの重要性に気付いてもらう事もシステム監査人の役割の一つのとなるのではないか。

（所 感）

私の中で漠然としていたシステム監査人の将来の役割を、豊富なデータを基に分りやすく講演していただき感謝いたします。企業のあるべき姿を実現するためにはITの力が今後ますます必要になります。

システム監査人の視点でITマネジメントを可視化し、ITの重要性を経営者に気付かせるという従来のシステム監査人の役割を超えた提言には胸躍るものを感じます。システム監査人にコンサルティング的な新たな意義を感じます。

●講　演

「金融機関と決済システム ーシステム監査の視点からー」

日本銀行　金融機構局　企画役
大石 正人　氏
（報告　№1587　清水 尚志）

1.講演概要

金融機関の基本的な役割の中で最も重要な決済サービスは、電気や水道、公共機関に並ぶ大切なライフラインのひとつであり、この機能が停止した場合、社会生活に大きな影響を与える。この点を踏まえて金融機関のシステム概要と、監査の視点を説明する。

2.講演要旨

⑴金融機関の提供する決済サービス

我々の生活の中における「給与振込」や「口座振替」「送金」などは、資金決済である。この業務を担っている金融機関は、預金業務や金融商品の販売、金融機関相互の資金の融通などを行っているが、この業務全てが資金決済を必要としている。このように金融機関は「金融市場の参加者」として、また「決済システムの参加者」として決済システムを利用している。

⑵決済サービスを支えるインフラ

決済サービスを支えるインフラには「個別金融機関が運営するシステム」と「中央決済機関が運営するシステム」がある。

個別金融機関のコンピュータシステムは、「勘定系システム」を中心に「全銀システム」のように他金融機関との送金（振込）を媒介するシステムや「ＡＴＭ：自動現金受払機」の相互利用する仕組みなど外部接続する部分、インターネットバンキングのためのシステムなどが接続されている。

それとは別に顧客情報の管理する「情報系システム」がある。金融機関のシステムは、勘定系と情報系が密接に接続された、大変複雑なシステムである。

一方、中央決済機関のシステムは「資金決済システム」と「証券決済システム」があり、様々な制度と仕組みを担当する機関がそれぞれのシステムを構築し運営している。

このような様々なシステムを経由して決済される資金量は1日に約150兆円を越える資金量である。日本のGDP(500兆円)であることから、約３日でＧＤＰ相当額を決済する経済の大動脈であり、決済業務を止めないことが大変重要である。

⑶決済インフラの特性

金融機関のコンピュータシステムに求められる信頼性と安全性は大変高度なものである。個別金融機関に求められる特性として、

①決済の信頼性（誤りなく、時限までに決済できる）
②サービスの継続性（中断することがない）
高セキュリティ（情報漏洩やなりすましを防御しているか）があげられる。また、金融機関全体として、
①ネットワークが問題なく繋がっている（物理的・論理的）
②決済機関が基地と決済機能を果たす
③システミックリスク（将棋倒し的影響）の備えができているかが求められている。

個々の金融間が決済リスクへの備えができていても、他の金融機関に問題があった場合、「決済が予定通りできなくなることに伴う損害の発生の可能性」いわゆる決済リスク（流動性リスク・業務リスク・信用リスク・法務リスク・etcが複合したリスク）が残る。しかもこのリスクは、「システミックリスク（将棋倒しの危険性）」を含む。

また、決済リスクは、単に金融機関相互の問題だけではなく、社会インフラの問題の影響を強く受ける。例えば「電力」「通信」の遮断は、決済システムにとって大きなリスクとなる。

⑷事業継続管理の重要性

このように「決済サービスの継続性」をいかに担保するかが重要となるが、以下の点が重要である。

①運営体制の整備とPDCAに基づくリスク管理
・システム管理基準等に基づく全社的な管理
・情報システムが有する基盤、提供サービスの内容や規模、特性に応じた対処

②サービス中断に繋がるリスクシナリオに即した事業継続管理
・自社の情報システムとして、複雑化した決済サービスを中断なく提供するために、集中決済金融機関と連携した対応が不可欠である

昨今、決済システムは、インターネットバンキングなどセキュリティ対策を始めとしたテクノロジー面での対応の難しさや、デリバリーチャネルの充実や金融機関の経営統合などによるサービスの複雑化、グローバルサービスの提供とこれを支えるグローバルオペレーションに相応した事業継続体制の確立による管理の高度化が必要となっている。

個別金融機関としては、決済システムに与える影響を念頭において「金融グループのコングロマトリックス化」「アウトソーシング利用時の問題点」「システミックリスクの存在」に目配りする必要がある。

決済システム全体として「事業継続管理」「金融機関の状況のモニタリング」「政府や金融当局がオーバーサイトの観点から、継続的に関与し、必要に応じてその状況をサービス受給者にも公開する」ことが重要である。このような管理の十分性の検証は第三者の目で行う必要がある。さらには相互依存性も意識した横断的な検証も必要である。(訓練を含めたPDCAサイクルの実施)

⑸事業継続監査の着眼点

決済サービスにかかる事業継続性の監査のポイントは以下のとおりである。

①決済サービスが中断を許されないものとの認識に立って、平素から情報システムの管理体制を構築しているか。
②事業継続管理体制をモニタリングし、訓練等を通じてリスク管理を見直し、環境変化に対応して高度化するPDCAサイクルが確立しているか。
③システム移行などの際は対応機関を含む十分な資源配分を行っているか。
④サービスの享受者や集中決済機関との疎通テストなど必要な手順を踏んでいるか。
⑤金融機関や集中決済機関側のリスク管理体制の整備や平素からのモニタリングが十分行われているか。

(所 感)

個別金融機関のシステム障害は「システミックリスク」により他の金融機関へリスクが伝播し、幅広い個人生活や企業活動に深刻な影響を与えることを分かりやすく説明して頂いた。
そのような特性を持った金融機関において特に事業継続性の観点の監査が重要である点が他業界のシステム監査との違いであると感じた。

●北信越支部活動成果1

「戦略性のシステム監査手法研究」

システム監査研究チーム　チームリーダ
森　広志

北信越支部では、20周年記念事業として、システム監査、並びに情報セキュリティ監査の２つの研究チームを設け、平成19年３月の年度総会を皮切りに、３ケ月毎の各県持ち回りの県例会で研究報告と意見交換を計６回実施しております。システム監査研究チームに於きましては、戦略性監査手法を研究テーマとして、平成19年６月の富山県例会からスタートし、研究報告を計５回実施しました。

⑴テーマ選定

現在、日経情報ストラテジー誌での戦略的なIT活用事例の紹介は、既に3千件を超え、過去のSIS（戦略的情報システム）の模範的事例である、座席予約システムや宅配システムなどは、現在ではあたりまえシステムとなっています。

今後10年のシステム監査は、経営戦略にITを活用した事例(以下、SM/I(Strategic Management using Information

Technology)；経済産業省の「IT経営」と同意と考える。) が、大半を占めるのではないかと考えました。

又、システム監査基準解説書にもあるように、「システム監査では、組織体の経営方針及び戦略目標の実現に情報システムがどのように貢献しているかを監査要点又は着眼点にしなければならない。」ことから、戦略性の監査手法の一例をテーマとして研究することとしました。

⑵「IT経営」におけるSM/Iシステムの特徴

経営戦略にITを活用した情報システムとはどのようなものをいうのか、多様な意見があるため、調査を行った結果、以下の3つの特徴を持つシステムがSM/Iシステムと言えることが分かってきた。

①情報システムの目的は、競争力強化、企業価値向上等、経営戦略の要件であること。
②顧客・取引先に開かれたオープンな情報ネットワークシステムを活用している。
③経営トップダウンによるシステム構築であること。

この3つの特徴は以後、システム監査手法を考える上で、重要なポイントとなりました。

⑶戦略性監査の特徴と対応

経営戦略にITを活用したシステムを監査する上での特徴と対応を以下に述べます。

①戦略性監査を行うにあたり、対象企業では、継続的に情報セキュリティ・IT内部統制監査が実施されており、信頼性、安全性がクリアしていることを条件としました。
②経営・現業・ITを融合した三位一体のビジネスモデルを策定し、企業価値を最大化、競争力強化を成功させるためには、組織内においても経営・現業・IT分野の関係者が、それぞれに、他分野を理解し歩み寄ることが重要です。このためITケイパビリティ向上に役立つように配慮する必要があります。このことは、トップダウンでのシステム構築以外を採用している企業でも重要と考えます。
③経営戦略にITを活用した際の経営成果への影響について、企業全体の観点で把握する必要があります。当チームでは企業価値評価によるフリーキャッシュフロー算出やROM (Return On Management) を検討しました。但し企業価値については、「株式時価総額＝企業価値」とは捉えず、有形資産、無形資産（人的資源コアコンピタンス・トータルコンピタンス、知的財産権、従業員のやりがい感）を含めた、広い視点から企業価値を考えることとしたいと考えます。
④SM/Iシステムの特徴である、顧客、取引先に開かれたオープンな情報システムを監査するにあたり、ネットワークを中心としたIT面の管理項目や、組織コミュニケーションの活用により計画目標との評価活動を通じ、企業活動をコントロールが重要と考え、当チームではITガバナンス協会のエンタープライズ・ガバナンス・モデルを、システム監査基準の補完として利用することとしました。

⑷ 予備調査に使用するチェックリスト作成

1つの企業をモデルに、予備調査に使用するチェックリストを作成した。

対象の企業の経営戦略は、企業の競争力を高めるため、トータルコンピタンスを強化し継続的な発展を図ることとし、数値目標としては、企業が保有する有利子負債の利子率よりも高い資本利益率（ROA）を設定しており、従業員規模は、5百名から3千名ほどの製造業又は、サービス販売業とした。

監査のポイントとしては、「①経営戦略と情報戦略の整合性が取れていること。」、「②経営成果、IT投資効果がえられていること。」、「③PDSAサイクルが継続して運営されていること。」としました。

チェックリストの作成は、DMM（Diamond Mandala Matrix）を利用し、レベル0のマトリックスを、①経営戦略の適合性、②経営成果、③情報戦略、④情報企画、⑤経営組織、⑥内部プロセス、⑦学習と成長、⑧PDSAサイクルの８項目とし、更にそれらの項目をレベル1のマトリックスに展開し、８項目を埋めていく方法で行いました。

DMMのレベル1での展開が完成したら、各メンバーに、レベル0の項目別で分担割りを行い、項目別のチェックリストを作成後、それを、１つのチェックリストに纏めるというやり方で作成。作成後、各メンバーにチェックリストを確認頂き、完成としました。

⑸ システム監査実施手順での工夫

予備調査の最初に、対象企業のCDF（重

要成功指標）について、監査メンバーで仮設を行う。この仮設したCSF（重要成功指標）をDMMチェックリスト作成に役立ててゆく。又、改善報告についても、必要に応じSWOT分析を行い､改善案としての､CSF（重要成功指標）を作成する。なお､予備調査には、企業価値評価、ITケイパビリティ診断も行うが、依頼内容、企業規模、必要に応じて手順を追加・削除する等、柔軟性を持たせることとしました。

⑹研究テーマの取り纏めを終えて

今回、戦略性のシステム監査手法をテーマに研究活動を行いましたが、下地については、３年前から、ITガバナンス協会のエンタープライズ・ガバナンス・モデルの研究報告など、以前からありました。昨年は、EA（エンタープライズ･アーキティクチャ）について学習、今年は、企業価値評価のおさらい、IT経営とBA（ビジネス・アナリスト)、ROMについて学習することができました。

SM/Iシステムの特徴が、ネットワークを中心とした情報システムであることから、ITガバナンス協会のエンタープライズ･ガバナンス･モデルに繋がり骨組みができました。

又、SM/Iシステムの特徴である、競争力強化から、IT経営に繋がり、BAによる三位一体のビジネスモデルからITケイパビリティの重要性に繋がりました。

又、メンバーの皆さまから、

・DMM作図に至った論理的理由を明らかにすること(木村07年09月)。
・継続的なPDSAの実施が重要ポイントであること(國谷07年12月)。
・企業価値＝株式時価総額と捕らえることが危険であること(白井07年12月)。
・戦略性監査の理論面について整理・充実を図ること(尾島07年12月)。
・予備調査の最初に、対象企業のCSF(重要成功指標)について、監査メンバーで仮説を行うことで、監査の品質を高めること(栃川08年6月)。等、数々の提言やアイティアを出して頂きました。

平成19年12月の石川県例会で、一通り戦略性監査の研究が纏まったので、メンバーの皆さまに、報告をすると、反響が大きく質問や意見が次々になされたため、20年度も戦略性監査の研究会を実施しました。20周年記念講演まで課題が持ち越されたものもあり、今回発表させて頂いたものもあります。

今回の20周年記念講演では、幸いにも管理会計の大家である櫻井教授にご教授頂ける機会を得、企業価値向上に関し示唆を受けることができました。ご協力頂いた研究チームメンバーの皆さまに感謝申し上げるとともに、今後とも戦略性監査の内容の充実に努めてゆきたいと思います。

●北信越支部活動成果２

「情報セキュリティアセスメント運用構築アプローチ手法」

セキュリティ監査研究　チーム　チームリーダ
宮本　茂明

2007年より情報セキュリティ監査研究チームを設け、支部会員のスキルアップを図る場として活動推進中です。その活動の一つである「情報セキュリティアセスメント運用構築アプローチ手法」研究について報告します。

⑴テーマ選定

多くの組織体では、情報セキュリティに関する管理の脇組みが構築され、セキュリティ内部監査/外部監査が実施され、世の中で標準的な技術的対策がとられているにもかかわらず、セキュリティ事故/情報漏洩が起こっています。

セキュリティ対策のためには、改善活動のようにトップダウンとボトムアップ両面のアプローチが有効ではないかと考え､ボトムアップ･アプローチによる情報セキュリティ点検改善研究に取り組みました。

⑵ボトムアップ・アプローチ手順

①各現場での情報のライフサイクルを通して残存リスクを詳細に抽出
②現場でのチェックシートをもとにしたセキュリティ点検（セルフアセスメント）
③セキュリティを現場で考える相談会
④組織文化や業務形態にあったセキュリティ対策を検討実行

（情報セキュリティ点検推進者（監査人）の役割：現場点検指導／ヒヤリ・ハットの確認収集／現

場対策指導／組織的対応の見極め）

この研究の第一ステップとして、セキュリティ・アセスメント・チェックシート雛形整備を行いました。セキュリティ事故事例/報道やヒヤリ・ハット想定等からチェック項目ネタだしを行い、チェック項目対応として確認方法とセキュリティ対策改善方法事例をまとめました。

今後、このセキュリティ・アセスメント・チェックシート試行適用・評価を行い、ボトムアップ・アプローチによる情報セキュリティ点検運用モデルの研究につなげていければと考えています。

●観　光

No.947　梶川　明美

講演会翌日は、半日コースで富山市内観光を楽しんでいただきました。

富山駅北口から、地域に密着した安全・安心・快適で環境に優しい路面電車のライトレールに乗って富山市北部の岩瀬へ。江戸期から明治期にかけて日本海を行き来する北前船で栄えた岩瀬の町並みを散策し、酒蔵をのぞいたり、名物の三角どら焼きでおやつタイムにしたり。国指定重要文化財になっている北前船回船問屋「森家」を見学しました。北前船で栄えた当時の様子や富山で配置薬業が盛んになった過程、乗組員を束ねるマネジメント技術など示唆が多く、館長さんの巧みな話術に聞き入りました。

次は薬種商の館「金岡邸」の見学へ。「金岡邸」は国登録有形文化財で、明治初期の店舗を復元した母屋では日本国内外で産する薬の原料や製造道具、売薬に関する資料が展示されています。管理人さんに説明を受けながら邸内を案内してもらいました。富山藩が薬の品質管理や売薬さんの教育・指導に力をいれて、確固たる信用を確保したことを知り、現代にも通じるものを感じました。先の森家とあわせ、富山の産業の成り立ちと発展の理由について理解が深まりました。

気さくで優しい櫻井先生をはじめ、お付き合いくださった三谷副会長、大石さん、森支部長とゆったりとした楽しい時間を過ごすことができ、どうもありがとうございました。もっと時間があればまだまだご案内したいところがたくさんあったのですが、またの機会を楽しみに。

●最後に

No.848　森　広志

当講演会は、先ず研究チーム作りから始まり、約２年間少しずつ準備を行って、実施にこぎつける事ができました。

ご参加の皆さま、講師の皆さま、御準備頂いた会員の皆さま、本部よりのご支援、他支部からご参加とご協力誠にありがとうございました。今回は、システム監査の古くて新しい課題の一つである、効果把握について解決を見出すことによりシステム監査普及に役立つと思い、櫻井教授と三谷副会長にご講演をお願い致しました。受講者確保は二の次と考え、専門的な講演内容となりましたが、櫻井教授の人気のため講演会場は満席となりました。

又、当支部は、銀行関係者の割合が多いこともあり、大石理事に講演をお願いしました。又、宮本さんや私の方で、支部の研究報告も行うことができて良かったと思います。受講者からの質問も活発になされ、受講者の皆さまにも満足頂けたのではと感じています。

懇親会では、竹村さんの名司会で、富山の冬の味覚、カニを味わって頂き、グルメ気分を満喫することができました。

今回ご参加を逃された方も含め、次回ご来訪をお待ちしております。

平成21年度第３回理事会議事録

日本システム監査人協会

1. 日　時：平成21年３月12日㈭18：30−20：30
2. 場　所：星稜会館　3F会議室
3. 出席者：鈴木㈱、小野、吉田㈱、馬場、竹下、和貝、岩崎、遠藤、金子、斎藤、成、仲、中山、山田、吉田（近畿支部）、田中（中部支部）

メールによる委任状（17名）　出席者計：33名/40名

4. 議題
   ⑴会員除名の件

5. 資料
   ⑴田村名義認定カード偽造問題の経緯

6. 審議事項

6.1 会員除名の件について

田村名義のCSA認定カード偽造問題のこれまでの経緯について、鈴木会長から資料⑴の説明があった。

定款第11条（除名）に基づき、田村氏に弁明の機会を与える旨文書で通知した。その後、資料の通り、やり取りし、3月28日に福岡市において、会長が田村氏と会い弁明を受けることとなった。

結果は、次回理事会で報告する。

7. 報告事項（各担当理事）

7.1 事務局（馬場/金子）

⑴総会は無事終了し、63名の会費の入金があった。

⑵総会の出席者は次の通り。

・出席権者数（はがき送付数）：977名
・はがき返信数：503名
・出席者数492名（委任状427名含む）

7.2 中部支部（田中）

3月例会予定

⑴日時：3月14日㈯14：00～17：00

⑵議事：

1）連絡事項
2）報告「SAAJ通常総会＆記念講演の報告」　早川　晃由様
3）講演1「中小企業のセキュリティ監査」　大野　淳一様
4）講演2「SaaSについて」　関口 幸一様

⑶会場：東桜第一ビル

7.3 近畿支部（吉田）

●2009年度支部総会 兼 第19回システム監査勉強会

1. 2009年度近畿支部総会

⑴日時：平成21年2月21日㈯ 15：20～16：35
⑵場所：大阪府商工会館　701号室
⑶議題：

1）2008年度の活動報告及び決算について
2）2009年度の事業計画及び予算について
3）支部規約の改正について（総会成立要件を本部定款に合わせる）

出席者：26名、委任状：77名 全議案が可決された（支部会員170名に対して過半数の出席者、委任状があり、有効に成立）

2. 第19回システム監査勉強会

⑴日時：平成21年2月21日㈯ 13：00～15：10
⑵場所：大阪府商工会館　701号室
⑶テーマ：「株式会社サウンドハウスにおける個人情報流出事件と対応（Web攻撃の脅威に立ち向かうには）」

講師：株式会社サウンドハウス　代表取締役社長　中島尚彦　氏

SAAJ本部第138回月例研究会（2008/7/29）のVTRを視聴し討議した。

出席数：32名

●第112回定例研究会（予定）

日時：平成21年3月19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：「いざという時に役立つBCPへの改善アプローチ」
講師：松井 秀雄　氏

●システム監査実践セミナー 2日間コース（近畿支部主催）は次の日程で参加者募集中

日時：平成21年6月27日㈯～ 6月28日㈰

●システム監査入門セミナー

実践セミナーの簡易版を企画しています。次の日程で準備中

日時：平成21年8月8日 13：00～17：00

●西日本支部合同研究会

今年は、近畿支部が幹事となり、秋の開催に向け準備中です

7.4 和貝副会長

20周年記念プロジェクトで作成した資料の

磁気ファイルを預かっているため、資料の保管方法及び今後の取扱について、プロジェクト会議を開催し検討する。

7.5 山田理事
理事就任の挨拶をされた。
私の研究テーマとして、中国市場向けのオフショア開発について取り組みを行っているが、当協会の活動の一つとして推進してゆきたい。
具体的には、既にシステム監査基準研究会で「オフショア開発のためのシステム管理基準」を作成するよう検討を進めている。

7.6 CSA利用推進（斎藤）
第4回CSAフォーラムを下記の通り開催する。
・日時：3月25日㈬ 18：20
・場所：日立情報システムズ
・テーマ：「内部監査から見たシステム監査」
・発表者：島田理事

7.7 中山理事
事例研究会で新たなセミナーを立ち上げについて検討している。
検討メンバーとして参加し、数回検討会議を行った。検討メンバーは8名。

7.8 事例件（吉田（裕））
事例研究会で1日コースの新セミナーを企画している。新セミナーは、システム監査の専門家向けセミナーでなく、受講対象者をIT関連の実務者、管理者向けとし、セミナーを通じて、システム監査をIT現場に普及させてゆきたい。
（会長）
内部監査協会が、放送大学に「内部監査」の講座を開設したとのこと。
講座開設には、テレビの場合数千万円ほど費用がかかると言われているが、システム監査の普及の方法として放送大学に講座を開設するという手段もあるため、視野に入れてほしい。

7.9 法人部会（小野）
⑴法人会員について
・㈱ジェイマックが退会した。
・㈲キャリアブリッジの入会希望があった。
⑵法人部会で自治体向けにDMを出す予定であるが、それについて各支部に下記の協力依頼を予定する。
①DMの案内状に当該地域の支部長の氏名を入れる。
②DMの宛先に部署名を入れたいので、部署名の調査。自治体の一覧表を後日送付するので、それに基づき調査願いたい。

7.10 20周年プロジェクト（小野）
報告書「システム監査これからの10年」の中の「今後の取組み計画」について、進め方・体制を検討する。

7.11 月例研究会（仲）
3月中に企画会議を開催し、今年度の月例研究会の取り組み（開催時期、担当者、テーマ等）について検討する。

7.12 会計報告（仲）
旧の銀行口座を2つ廃止した。
・みずほ銀行　北沢支店
・三菱東京UFJ銀行　新宿西支店

（以下はメール報告）
7.13 中四国（溝下）
－実績－
2月度月例会
日時：2008年2月18日㈬ 18：30～20：30
内容：「郵便局株式会社における
SaaS活用の概況について」
場所：広島市まちづくり市民交流プラザ 会議室A
－予定－
3月度月例会
日時：2008年3月25日㈬ 18：30～20：30
内容：「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－」
場所：広島市まちづくり市民交流プラザ 会議室B

7.14 北信越支部（森）
3月14日に富山市で年度総会を実施する。

7.15 九州支部（福田）
●2月度月例会（第219回）
日時：2月28日㈯ 13：00～17：00
会場：早良市民センター 第2会議室
内容：ビデオ視聴
第143回月例研究会
「経済産業省の情報セキュリティガバナンス構想」
報告事項
・通常総会参加報告（福田）

・「パーソナル情報研究会報告書－個人と連結可能な情報の保護と利用のために－」について（続き～討論）（舩津さん）

（開催予定）

●３月度月例会（第220回）
日時：3月28日㈯ 15：00～17：00
会場：早良市民センター 第１会議室

●４月度月例会（第221回）
日時：4月25日㈯ 13：00～17：00
会場：早良市民センター 第１会議室

7.16　東北支部（高橋）
月例会
1. 日時：3月7日㈯　14時00分～17時
2. 場所：コラッセふくしま　302A会議室
3. 内容：・連絡、報告事項
・勉強会「IT統制監査実践マニュアル」の勉強会（第2部 第3～5章）

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

次回理事会開催予定
日　時：平成21年4月9日㈭　18：30～
場　所：星陵会館　3階会議室

平成21年度第４回理事会議事録

日本システム監査人協会

1. 日時：平成21年4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）、竹下、馬場、金子、岩崎、榎本、遠藤、大石、山田、鈴木（実）、仲、中山、松枝

メールによる委任状（19名）　出席者計：32名/40名

4. 議題
⑴情報セキュリティ教育事業者連絡会（ISEPA）への加入の件
⑵会員除名の件
5. 資料
⑴情報セキュリティ教育事業者連絡会（ISEPA）のホームページ
⑵田村氏　弁明機会記録
6. 審議事項
6.1 情報セキュリティ教育事業者連絡会（ISEPA）への加入の件
鈴木会長から、下記の目的達成のため情報セキュリティ教育事業者連絡会（ISEPA）へ加入したいとの提案があった。
⑴加入目的
①教育事業者のWGへの参加
②情報セキュリティ教育業界の情報収集
③NPO間で相互認証のためのWGへの参加
④情報セキュリティ大学院大学との協力関係維持
⑵ISEPAの概要
①名称：情報セキュリティ教育事業者連絡会（Information Security Education Providers Association、略称ISEPA）
②事務局：JSNA（日本ネットワークセキュリティ協会）内に設置
③ISEPAの事業：業界横断的な人材育成支援体制の整備し、人材育成に関する情報を広く社会に発信するための様々な取り組みを推進する。
④代表者：与儀 大輔　氏
⑤加入料：無料
⑥加入条件：「JSNAへの入会が条件」と思われると会長から説明があったが、理事会終了後ISEPAから、JSNAの入会は必須条件ではないこと、特別会員（NPO相互協力目的）としての加入が可能との連絡があった）
⇒審議の結果　本提案は承認された。

6.2 会員除名の件
会長から、本人から直接弁明を聞いたが、田村氏には協会の名誉を傷つけたことに対する責任があると認めたため、田村氏の除名の提案があった。
⑴田村氏弁明機会の概要説明
日時：平成21年3月28日㈯ 13：30～14：10
会場：福岡市早良市民センター　第一会議室
出席：田村氏、会長 鈴木（信）、九州支部長 福田
内容：資料⑵「田村氏弁明機会記録」の通り
⑵今後の除名手続き
①本人通知：除名通知文を内容証明郵便で本人宛に発送する。
②除名の事務処理実施
③当協会ホームページに除名を公表する
⇒本提案は、審議の結果満場一致で承認された。

7. 報告事項（各担当理事）

7.1 会報（竹下）

・次回108号は5/15原稿締切

・予定記事：新任理事の挨拶（これまで未掲載者対象）
論文の投稿あり。
なお、投稿の促進につながるよう論文投稿基準の見直しを行う。

7.2 岩崎理事

内部監査人協会が出している「放送大学」の講座について調査したので紹介する。

・放送チャンネル：関東地上デジタル放送12

・放送日時：毎週月曜日23：00～23：45

・講座名：「組織運営と内部統制」

7.3 教育研修委員会（鈴木実理事）

今年の春の認定制度に修了証書が間に合わないというトラブルが発生したため、再発防止のため、特別認定講習マニュアルについて、再テストを行った場合の研修結果の提出期限を設けるなどの見直しを考えている。

7.4 事務局（馬場）

・新任理事2名の担当は、次の通りとした。

・大石理事：月例研究会、基準研究会、認定委員会

・山田理事：会報、基準研究会、認定委員会

・近畿支部から依頼があった支部助成金の分割払いを実施する。
分割割合や振込手数料の負担について検討している。

7.5 事務局（金子）

・事務所の鍵の施錠に関して、施錠しているがセンサーが稼働していない場合があるため、施錠の際はセンサー作動（青ランプ点灯）を十分確認してほしい。

・一階のメールボックスの番号鍵の施錠を確認してほしい。

7.6 基準研究会（松枝）

今年度は、次のプロジェクトが進行している。

①「ソフトウェア国際取引における監査のポイント」Ver2.0作成

②プロジェクトマネジメント監査のポイント

③BCMにおける監査のポイント

④Webシステムにおける監査のポイント（開発・利用）

⑤システムの有効性監査のポイント

⑥COBIT4.1とシステム管理基準のマッピング作業

7.7 月例研究会（大石）

・5月月例研究会は、経済産業省情報処理振興課に「ソフトウエア信頼性ガイドライン第2版」を依頼している。現在、回答待ちである。

・6月月例研究会は6/17㈬に決定、内容は当協会顧問弁護士の藤谷弁護士にソフトウェアの裁判外紛争解決の枠組みについて、ご自身が立ち上げられた「IT－ADRセンター」の紹介も含め公演いただく。

・7月月例研究会は、東京三菱フィナンシャルグループに「システム統合を含めたシステム監査の取り組み」について講演していただくことが決定した、なお日程は検討中。

7.8 会計（仲／榎本）

⑴支部からの支部会計報告の提出時期について「標準日程」を取り決めた。

・第1四半期～第3四半期の標準日程：四半期最終月翌月の「暦日14日」とする。（当日が土・日曜日の場合は次の月曜日）

・第4四半期（12月末）：総会日程が前提となるため、別途詳細日程を連絡する。
今年の第一四半期は4月14日㈫締め、第二四半期は7月14日㈫締めとなる。

⑵旧口座への振り込みが5名あったため、新口座に切り替えるよう本人に通知した。

（以下はメール報告）

7.9 月例研究会（沼野）

⑴3月31日㈫に平成21年度の月例研究会企画会議を開催し1年間の月例研究会テーマ候補、各人の担当割を決定した。

⑵4月の月例研究会は以下を予定し準備を進めている。

①開催日：4月28日（火）

②テーマ：金融機関の情報システムにおける暗号技術に関するもの（調整中）

③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

7.10 北信越支部（森）

北信越支部年度総会報告

1. 日時：2009年3月14日㈯ 13：30－17：30

2. 場所：アーバンプレイス富山 8階会議室

3. 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

7.11 近畿支部（吉田）
●第112回定例研究会
日時：平成21年3月19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：「いざという時に役立つBCPへの改善アプローチ」
講師：松井 秀雄 氏
出席数：34名
●第20回システム監査勉強会（予定）
日時：平成21年4月18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：「IT経営の実現に向けて
～IT経営協議会とIT経営憲章」
講師：経済産業省商務情報政策局情報政策課
企画官：平井 淳生 氏
SAAJ本部第139回月例研究会（2008/8/25）のVTRを視聴し、討議します。
テーマ2：「CIOとガバナンス」
講師：早稲田大学大学院教授
国際CIO学会会長 小尾 敏夫 氏
SAAJ本部第140回月例研究会（2008/9/25）のVTRを視聴し、討議します。
●システム監査実践セミナー2日間コース（近畿支部主催）
参加者募集中です。
日時：平成21年6月27日㈯～ 6月28日㈰
●システム監査入門セミナー
実践セミナーの簡易版です。只今参加者募集中です。
日時：平成21年8月8日㈯ 13：00～17：00
●西日本支部合同研究会
次の日程で、準備中です。
日時：平成21年11月14日㈯PM～15㈰AM

7.12 CSA利用推進（力）
⑴第4回CSAフォーラムを下記の通り開催しました。
・日時：3月25日㈬ 18：20 ～ 20:30
・場所：日立情報システムズ（大崎）
・テーマ：「内部監査から見たシステム監査」
・発表者：島田裕次氏
・20数名のCSAの参加者を得て、島田理事の熱のこもったご発表に参加者は大いに感銘を受けた。システム監査を取り巻くいろいろな動向を鋭い視点からご説明いただいた。
⑵第5回CSAフォーラム予定
・日時：6月1日㈪
・場所：日立情報システムズ（大崎）
・テーマ：（未定）（女性CSAの活躍）
・発表者：桜井由美子氏
・事前登録の上、ぜひご出席下さい。
⑶第6回予定7月23日㈭ 小野 修一 氏

7.13 中四国支部（溝下）
－実績－
●3月度月例会
日時：2008年3月25日㈫ 18：30～20：30
内容：「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－」
場所：広島市まちづくり市民交流プラザ 会議室B
－予定－
●4月度月例会
日時：2008年4月15日㈫ 18：30～20：30
内容：「経済産業省の情報セキュリティガバナンス構想」
場所：広島市まちづくり市民交流プラザ 会議室A

7.13 中部支部報告（田中）
●3月例会
日時：2008年3月14日㈮ 14：00～17：00
場所：東桜第1ビル会議室（出席者18名）
内容
⑴事務連絡：14：00 ～ 14：30
⑵報告：14：30～14：50
「SAAJ通常総会&記念講演の報告」
早川 晃由 様
⑶講演Ⅰ：15：00～15：50
「中小企業のセキュリティ監査」
大野 淳一 様
⑷講演Ⅱ：16：00～16：50

「SaaSについて」関口　幸一　様
3. 次回例会予定：5月16日㈯ 14：00 ～
大垣市ソフトピアジャパン

7.15 九州支部（福田）
●3月度月例会（第220回）
日時：3月28日㈯ 15：00～17：00
会場：早良市民センター 第１会議室
内容：報告事項
⑴中小企業向けSaaS活用基盤整備事業について（溝田）
⑵セキュリティ技術トピック（その2）～XSSについて（福田）
参加：11名
（開催予定）
●4月度月例会（第221回）
日時：4月25日㈯ 13：00～17：00
会場：早良市民センター 第１会議室
内容：ビデオ視聴　通常総会記念講演
●5月度月例会（第222回）
日時：5月23日㈯ 13：00～17：00
会場：早良市民センター 第2会議室

7.16 法人部会（小野）
・自治体向けセミナーに加えて民間企業向けセミナーの案内を、Webサイトに掲載しました。
・自治体向けセミナーのDM、関東地区および全国都道府県は、次回の法人部会（4/28）でDM作成し発送します。
・自治体向けセミナーのDM、全国の市については、各支部長宛にDM作成、発送に係る作業協力を依頼しました。

7.17 20周年事業のフォロー（小野）
・プロジェクトを開き、確認･討議を行いました。
・講演データの扱いについては和貝副会長から、提言への取組みのフォローについては三谷副会長から、ご報告をお願いします。

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

次回理事会開催予定
日　時：平成21年5月14日㈭　18：30 ～
場　所：星陵会館　3階会議室

平成21年度第５回理事会議事録

日本システム監査人協会

1. 日時：平成21年5月14日㈭ 18：30－20：00
2. 場所：星稜会館　　３Ｆ会議室
3. 出席者：鈴木（信）、小野、竹下、力、吉田（裕）、馬場、金子、岩崎、榎本、大石、橘和、木村、斎藤、成、仲、福田（九州支部）
メールによる委任状（16名）　出席者計：32名/40名

4. 議題
⑴継続教育要項の変更案（更新期間の短縮）

5.資料
⑴継続教育要項（改定案）
⑵日本セキュリティマネジメント学会第23回全国大会のご案内

6. 審議事項
6.1 継続教育要項の変更案（更新期間の短縮）
鈴木会長から、継続教育要項の改定案が提案され、資料：継続教育要項（改定案）に基づき説明があった。
⑴改定の目的
①更新期間を短縮し、更新内容の強化を図る。
②更新料の早期回収を図る。
⑵改定内容の概要
①現行3年の更新期間を2年に短縮する。
②継続教育の実績報告は、現行では1年毎の報告を求めているが期間を2年に変更し、更新時に2年間纏めて報告する。
（毎年の実績報告は行わなくてよい）
③適用は、2010年に更新を受ける者及び2010年に新規取得する者からとする。
例１：2009年末に認定が切れる者は2010年更新のため適用される。
例２：2009年春の申し込みにより新規に認定を受けた者（2009年認定者）は適用されず、次回更新から適用される。
⇒審議の結果　本提案は承認された。
なお、「継続教育要項」改定案の文書の表現方法について、意見が出されたため、文書の見直しを会長に一任した。

7. 報告事項（各担当理事）
7.1 事務局（馬場／金子）
⑴協会ホームページについて
・協会ホームページを改定し、新ホームページを5月2日から公開した。
・全体の構成、タグ、インデックスについての改善要望は事務局へ提出してください。
・各記事のコンテンツの変更は、従来通り主査を通じUISに依頼してください。
⑵メール管理の改善について
・当初の改善計画通り、次のテーマである「メール管理の改善」の取り組みを開始する。

7. 2月例研究会（大石）
・5月～7月までの研究会開催予定は決定している。内容は沼野副会長のメール報告の通りである。
・8月以降の企画を検討中である。

7.3 九州支部（福田）
●4月度月例会（第221回）
日時：4月25日㈯ 13：00～17：00
会場：早良市民センター 第1会議室
内容：ビデオ視聴　通常総会記念講演
報告事項
⑴クレジット産業向け"PCI DSS"とISMSユーザーズガイドについて（中尾）
⑵セキュリティ技術トピック（その3）（福田）
（開催予定）
●5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」
●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
●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

7.4 会報（竹下）
・次回108号は5/15原稿締切りです。原稿未提出の方は提出してください。

7.5 CSA利用推進（力）
⑴第5回CSAフォーラム開催　申込受付中
・日時：6月1日㈪
・場所：日立情報システムズ（大崎）
・テーマ：「組織人を幸せにするマネジメントシステムを目指して」
・発表者：桜井由美子氏
⑵第6回CSAフォーラム開催
・日時：7月23日㈭
・場所、テーマは検討中
・発表者：小野修一氏
※：その他報告
資料⑵日本セキュリティマネジメント学会第23回全国大会のご案内について報告があった。同大会は、力氏が大会実行委員長を務めている。

7.6 事例研究会（吉田（裕））
⑴システム監査サービス
都内の自動車部品メーカからシステム監査サービスの依頼があり、提案書を提出した。
⑵第12回内部統制セミナー（7月23日～25日（3日間）
ホームページに公表し募集中である。
これまでに3人の申し込みがあった。6人以上で開催する。

7.7 法人部会（小野）
・自治体向けセミナーの案内をDMで、関東地区および全国都道府県に発送した。
・全国の市については、各支部でDM作成、発送の準備中である。

7.8 会長報告
・JNSAに加入した。特別会員としての加入のため会費は無料
・JNSAの部会として位置づけられている「情報セキュリティ教育事業者連絡会」（以下「連絡会」という）の定例会に参加した。
日時：4月28日㈫
会場：新橋JNSAの会議室
・連絡会は、情報セキュリティ大学院大学と産学協業関係にあり、連絡会が提供できる教育メニューを大学側に提示できる関係である。この教育メニューにSAAJのセミナーを含めることが可能である。

（以下はメール報告）
7.9 月例研究会（沼野）
⑴5月月例研究会：5月25日㈪
テーマ：「高度情報化社会を見据えた情報

システム・ソフトウェアの信頼性向上に向けた取組み」
講演者：経済産業省商務情報政策局情報処理振興課
総括補佐　奥家 敏和　氏
⑵6月月例研究会：6月17日㈬
テーマ：「IT－ADR」（仮題）
講演者：弁護士法人エルティ総合法律事務所
所長弁護士　藤谷 護人　氏（当協会顧問弁護士）
⑶7月月例研究会：7月28日㈫
テーマ：「金融機関におけるプロジェクト監査への取組事例」
講演者：株式会社三菱東京ＵＦＪ銀行
監査部業務監査室 上席調査役　金田 雅子　氏

7.10 北海道支部（大舘）
●4月勉強会
日時：4月22日㈬ 18：30～20：30
場所：Ｌプラザ（札幌市男女共同参画センター）会議室
テーマ：「金融機関のシステム統合　Part2」
講師：ＳＡＡＪ北海道支部　五十嵐 洋介　氏
出席数：16名
●5月ＶＴＲ勉強会（予定）
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

7.11 中四国支部（溝下）
－実績－
●4月度月例会
日時：2008年4月15日㈬ 18：30～20：30
テーマ：「経済産業省の情報セキュリティガバナンス構想」
場所：広島市まちづくり市民交流プラザ 会議室Ａ
－予定－
●5月度月例会
日時：2008年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

7.12 近畿支部（吉田）
●第20回システム監査勉強会
日時：平成21年4月18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：「IT経営の実現に向けて　～IT経営協議会とIT経営憲章」
講師経済産業省商務情報政策局情報政策課
企画官　平井 淳生　　氏
ＳＡＡＪ本部第139回月例研究会（2008/8/25）のＶＴＲを視聴し、討議します。
テーマ2：「CIOとガバナンス」
講師：早稲田大学大学院教授
国際CIO学会会長　小尾 敏夫　氏
ＳＡＡＪ本部第140回月例研究会（2008/9/25）のＶＴＲを視聴し、討議します。
出席数：36名
●第113回定例研究会
日時：平成21年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）
●システム監査実践セミナー 2日間コース
（近畿支部主催）
参加者募集中。早期割引で16名の申し込みがあった。
締め切り：5月31日㈰
日時：平成21年6月27日㈯～ 6月28日㈰
●システム監査入門セミナー
実践セミナーの簡易版です。只今参加者募集中です。
日時：平成21年8月8日㈯13:00 ～ 17:00
●20周年から1年たち次のステップを考える研究会（仮称）
次の日程で、準備中です。
日時：平成21年8月29日㈯PM
●西日本支部合同研究会
14日に見学会・懇親会、15日に研究会の予定で、準備中です。
日時：平成21年11月14日㈯PM
～15㈰15時

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

次回理事会開催予定
日時：平成21年6月11日㈭　18：30～
場所：星陵会館　3階会議室

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（No.1186）

1. 概要

個人情報保護法の全面施行後、はや4年近くになるが、個人情報漏えいなどの事故が減少していない。もともと、個人情報保護法（以下、法と略称）は法規制としての遵守内容を示しているが、その手法はなんら指定していない。従って、事業者は各種認証取得、管理・技術標準をベースに対策を講じながら不安を感じている。このため、効果的な情報漏えい等防止を図るべく、『直接的対策群』『間接的対策群』『多発事故防止対策群』の3群12項目について、一般企業向けの「具体的提言」をまとめた。

この「具体的提言」をベースに「個人情報漏えい防止評価チェックリスト」を作成し、重点的、総合的な対策を効果的効率的に実施するよう提案する。

なお、『直接的対策群』とは事故発生を直接的に防止する「直接対策の策定体系・方法」である。『間接的対策群』とは直接対策を支える経営機能、業務標準化、教育研修などの機能・活動等である。『多発事故防止対策群』とは、事故統計に基づいて多発事故を重点的に防止する対策である。【図表3-2参照】

これらの重点的、総合的な対策群の点検・評価等により事故減少をねらう。

2. 個人情報漏えい等の現状

（2007年値：JNSA2008年資料等による）

・漏えい人数は、2006 年と比較し大規模なインシデントにより大幅に増加した。
　しかし、インシデント件数は2005 年以降、やや、減少傾向にある。
・漏えい原因は、管理ミス、作業者によるヒューマンエラーが全体の70％程度を占めている。
　媒体・経路では、紙媒体・USB記録媒体・PC・携帯が多い。
・委託先の漏えい事故：事故全体の約40％を占めた。

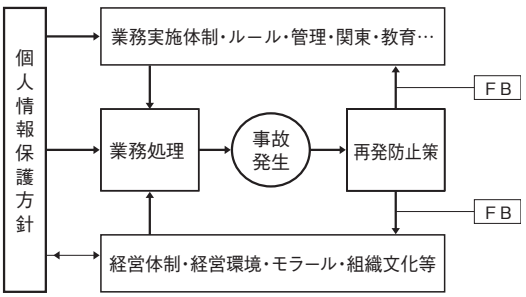
3. 個人情報取扱いの構図と事故防止対策の方向性

次の手順で検討の方向性を定めた。【図表3-1、図表3-2参照】

①「個人情報処理・事故発生に関わる構図」をレビューし、9テーマを設定する。
②テーマ（9項目）から、実践対策アプローチの方向性（3群・12対策）を得た。

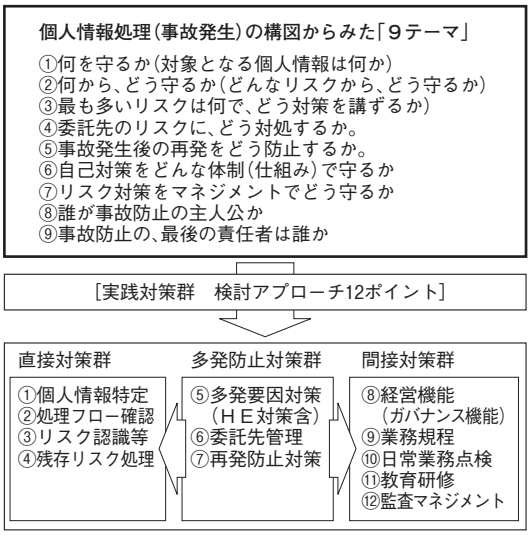
なお、ここでは、法20条の「安全管理措置」を対象として、「個人情報」までを含めることとし、法16、17、23条等で規定する「個人情報の取扱」は除外した。

【図表3-1　個人情報処理、事故発生に関わる構図】



FB:フィードバック

【図表3-2　実践対策アプローチの方向性】



4. 直接的対策群の検討と提言

『直接的対策群』の具体的な処理フローを【図表4-1】に示す。

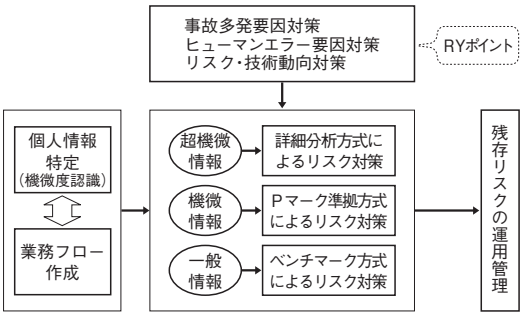
4-1「個人情報価値＋多発事故要因」重視型リスク認識方式の採用

この「提言方式」の骨子は次のとおりである。【図表4-2参照】

①特定した個人情報の重要性を勘案したリスク認識等の方法を採用する。
②特に、事故多発傾向にある要因を意識的に重視した対策を組み込む。

③事業者の効果的、効率的なリスク対策作成の方法を提言する。

【図表4-1 個人情報特定～リスク認識～残存リスクの流れ（概要図）】



【図表4-2「個人情報価値＋多発事故要因」重視型リスク認識等方式】

個人情報区分	一般情報	機微情報区分	
		機微情報	超機微情報
リスク認識等方法	ベースライン方式	Pマーク準拠方式	詳細分析方式
業務フロー作成	○	○	○
リスク分析作業	○	○	○
リスク評価作業	―	○（定性的実施）	○（定量的実施）
参照対応策群	JISQ15001 PMS実施資料	JISQ127002：2006（実施規範）	JISQ127002：2006（実施規範）等*1
対応策策定方法	トップダウン的	リスク分析結果による	リスク分析結果による
記事	過剰対策を除去	Pマーク方式を準用	
評価（的確性）	○	○～◎	◎
（効率性）	◎	○	△
（適用可能性）	◎	○	△
（業務統合性）	◎	◎	◎

*1：PCIDSS ＝ Paymet Card Industry Security Standard も参照

⑴「提言方式」の概要

リスク認識等方式として、『ISMSユーザーズガイド』では、「組合せアプローチ」を推奨しているので、「提言方式」では、「ベースライン方式」・「Pマーク準拠方式」・「詳細分析方式」（いずれも仮称）を併用する。

⑵「提言方式」における処理

1）個人情報特定の段階で、“個人情報の機微度”により3区分し、以後、区分に応じた「リスク認識等の方式」によってリスク対策を策定する。

2）“個人情報の機微度”3区分には、JNSAの「JOモデル」を活用する。即ち、「通常レベル」（例示：住所・氏名など）、「機微レベル」（例示：クレジットカード番号のみ）、「超機微レベル」（例示：口座番号と暗証番号）とする。

3）具体的なリスク認識等の処理（リスク分析、リスク評価、参照する対策群、対策の策定）は【図表4-2】のとおり、機微度のレベル毎に対応させて進める。なお、通常レベルで使用する『JISQ15001ＰＭＳ実施のガイドライン』（JIPDEC資料）は、経済産業分野の指針（ガイドライン）が例示する対策に準拠している。

4）必要に応じて、個人情報の「本人認識の容易度」、「大量な個人情報取扱など量的な要素」を勘案したレベルの高いリスク認識等方式を使用する。

⑶事故多発要因・ヒューマンエラー要因に対する重点対策の反映

事故多発要因等の重点対策データベース集『RYポイント』（5-1参照）をリスク対策に、明示的にハイライトして組込む。

⑷『提言方式』の評価

本方式は次のような効果を目標としたものである。【図表4-2参照】

①対策的確性・・個人情報機微度に応じてリスク認識等方式を変える

②効率性・・・・普通レベルの機微度ではトップダウンで対策を策定する

③適用可能性・・認識等作業負荷と効果のバランスを狙った方式を適用する企業の作業負担を極力低減し、企業対応の適用度を上げる。

④業務総合性・・今後の対策レベルアップと業務改善効果の可能性を有する。

4-2 個人情報の特定

⑴現状と課題

これまでの事故事例によると、個人情報の基本的な取扱が不適切である。その原因として、①守るべき個人情報を特定していない、②機微度、注意すべき個人情報を意識し特定していない、③個人情報特定の必要性の認識、取扱方法の教育研修等が不足している、と判断される。

このため、「漏えいの“対象となる個人情報に何があるか”を確認し、記録し、管理する」ことが必要であり、特に、いわゆる「センシティブ情報」（機微情報）、注意すべき媒体、手段等を峻別し特定することが、多発事故防止対策の第一歩である。

⑵提言する主なチェックポイント

・個人情報を明確に特定し、必要項目を一覧表等に登録管理しているか
・業務フローの流れに沿ってすべての個人情報を特定しているか
・機微情報、多発事故要因となる情報、大量情報等を特定し明示しているか
・個人情報所有の棚卸しを定期及び適時、実施しているか
・個人情報特定は取扱部門の従業者を含めて、

教育研修効果も得ているか
〈参考〉企業情報（機密情報）の特定も同時に含める方法がある

4-3 業務処理フローの確認

⑴ 現状と課題

個人情報をどう処理するかを業務の流れに沿って個人情報毎に確認していないため、具体的なリスク認識等が実施できず、事故につながるケースが推定できる。また､業務フローの作成･確認は業務標準化と業務改善の源泉ともなるものであり、事故防止は勿論のこと、業務の無理・無駄を改善し、一層の業務効率向上につながる可能性を認識すべきである。

⑵提言する主なチェックポイント

・個人情報毎の業務処理フローを詳細に確認しリスク確認につなげているか
・個人情報の取得手段・媒体・中間生成を意識し処理フローを確認しているか
・事故の多発要因等、場所、時間、作業者等を意識しているか
・例外処理を把握し統合・削除するなど個人情報漏えい対策につなげているか
・同様処理フローになるものはまとめて効率化をはかっているか

4-4 リスク認識等（リスク分析・評価・対策）と残存リスクの管理運営

⑴リスク認識等の課題:前述のとおりである。

⑵リスク認識等の「提言する主なチェックポイント」

・個人情報毎に個人情報の流れに沿って忠実にリスク認識等をしているか
・個人情報を伝達する媒体・経路、取扱場所、事故多発要因を意識してリスク認識等をしているか
・リスク認識等の結果を規程類･教育･日常点検･監査等へ反映しているか
・リスク認識等は残存リスクを含めて、適時に見直して、記録管理しているか
・リスク認識等の結果から経営判断により対策を決定しているか

⑶残存リスクの「提言する主なチェックポイント」

残存リスク管理の対象は、リスクとして、①安全対策を講じていない、②対策を講じてもこれ以上の対策ができない、③安全対策を講じることによって新たに発生するリスク、などの「未対応部分」である。

これらについてリスクが顕在化しないか、次のように点検し、監視をする。

①「日常点検」の中で顕在化がないか､を確認する。
②「教育等」により、日常活動の中で、顕在化しないか観察する。
③監査項目の中で取上げ、監視する。
④定期的なリスク認識の際に、重点的に再検討する。
⑤代表者によるマネジメント・レビューで定期的にその是非判断をする。

なお、リスク顕在化時の重要度を目安に、管理すべきものをある程度限定する。

また、残存リスクは経営者の判断を得て実行に移す必要がある。

5. 多発事故防止対策の検討と提言

これまでの各種事故統計からみた多発事故原因に対し、①事故多発要因対策、②委託先管理、③事故発生後の再発防止、の重点的対策を検討し、効果的、効率的な取組みが要請される。

5-1 個人情報多発事故とヒューマンエラーの再発防止

⑴個人情報多発事故の傾向（課題）

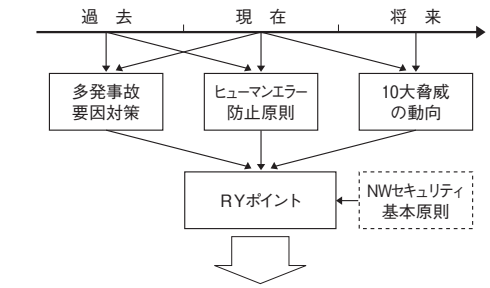
・管理ミスを含めたヒューマンエラーが多い
・漏えい媒体、経路には、USBなど可搬記録媒体、PC、紙類が多い。
・情報の誤送付・保管・廃棄・紛失のミスが多い。
・情報システム管理に関わる漏えい、不正行為が増加傾向にある。

⑵重点的な対策の実施

現状の課題に対応するため、事故発生統計、ヒューマンエラーの研究成果などを反映した『RYポイント』を直接的対策、間接的対策に組みこむ。

・『RYポイント』とは､"Red-Yellow point"の略称であり、要点のみをコンパクト化した、多発事故防止重点対策の「ポイント集」である。

【図表5-1 構成と活用方法の概要】



リスク対策への反映	規程類への反映	マネジメントへの反映
個人情報特定 フロー図作成 リスク認識等→対策策定	規程類対策の明示	日常点検・委託先管理 監査実施・ マネジメントレビュー
教 育 ・ 研 修 の 実 施		

注 多発事故要因の対策：日本情報処理開発協会資料
ヒューマンエラー防止原則：研究論文：斉藤敏雄ほか
10大脅威の動向：情報処理開発機構資料
NWセキュリティ基本原則：MS-ISAC,2006『Top Ten Cyber Security Tips』

【別図１：『RYポイント』一般要約版･管理版】に示す。

・『RYポイント』の構成と活用方法の概要を【図表5-1】に示す。

構成内容は、次の３要素をベースとして、対策に置換えている。

〈多発事故課題〉＋〈エラーの定性的課題〉＋〈リスクの今後の動向〉

⑶活用の方法

1) 直接的対策として、個人情報特定からリスク対策策定までの流れの中で事故多発要因を明示的に捉え､具体的対策に反映（明記等）をする。例えば、作業方法、媒体別のリスク認識等の段階で、『ＲＹポイント』を対策検討の際に「意識的」に組込み、対策策定時にトップダウン的に折込む。

2) 間接的対策としては、経営取組み姿勢、ルール化、教育研修、実施監査な直接対策実施を支える「仕組み」に明示的に反映する。例えば、

・関連する規程・手順、日常作業マニュアル等に『RYポイント』を明示して従業者の注意を促し、実施を求める。

・業務手順と一体化して含め、ポイントとしてマークする。

・教育研修では、研修内容・研修方式に反映する。なお、気づきを与える集合教育研修では、重点的なテーマとし『エラー防止の心得ルール』（情報を扱う時の心得）も取扱い、自ら考えさせて定着を促す。

・日常点検においても、『RYポイント』（管理版）を使用して、点検内容・点検方法・点検周期を組み込む。

・監査に組み込んで適用状況の監視と有効性を確認する。

3) 注意点

・『RYポイント』は多発事故統計からの注意点を明示したものであり、実施中の基本的対策が含まれていない可能性があるので、別途、基本事項を網羅した「対策チェックリスト」等の併用が必要である。

・『RYポイント』は、情報セキュリティ環境、対策システム化とあわせて逐次改訂・維持していく必要がある。

5-2 委託先管理の強化

⑴現状における問題点と基本認識

1) 法と主管庁の指導

法22条では、委託先に対する適切な監督を規定し、経済産業分野の指針（ガイドライン：平成20年2月再改訂）で、次を骨子とする指導を強化している。また､JISQ15001規格3.4.3.4でも規定している。

①委託先を適切に選定すること。

②委託先との間で必要な契約（技術的条件提示を含む）を締結すること。

③委託元は、委託先における委託個人データの取扱状況を把握すること。

2) 調査結果からみた実態

委託先の監督管理状況について、経済産業省の調査結果によれば、①選定評価の実施は大きく遅れている、②契約締結をせずに委託している事業者が存在する、③定期的な契約履行状況の点検監督をあまり実施していない、がある。

⑵対応策の基本

①業務委託の全責任は委託元に存在するとの認識に立ち対応方法を検討する。

②委託先選定評価、契約内容、委託実施確認をバランス良く実施する。

③委託元・委託先間では、Win－Winのパートナー関係を確立維持する。

⑶提言する主なチェックポイント

・委託先評価は経済産業分野の指針（ガイドライン）にある18項目を基本とし、業種・委託業務に適合する項目を評価した上、委託先を選定しているか

・契約事項には安全管理措置項目を設定し、実施を確認しているか

・委託先選定・契約・指示・監督に情報漏えい防止対策として『ＲＹポイント』を活用しているか

・必要最小限の個人情報（内容）のみを委託先へ渡すほか、クレジット情報等の管理・監督を徹底しているか

・継続的な委託先の再評価と安全管理対策の実施状況を確認しているか

〈注意点〉

・再委託先の事故発生防止を意識して対策を講じているか

・委託先管理処理を法務契約部門のみに任せず、全社的体制で対応しているか

5-3 個人情報事故発生後の再発防止対策

⑴現状と課題

緊急時対応管理のうち、①事業継続計画、②事業継続管理、③事故発生の再発防止管理、があるが、③の参照情報が少ないことから、ここに

絞って提言する。

特に、「真の原因究明をした後、対策を講じているか」「対策指示の実施までを確認しているか」「諸対策を水平展開しているか」などに課題がありそうである。

⑵事故発生後・処理フローの提言

①真の原因を追求して、リスク認識等を実施し直す。現象と原因を混同している場合が多いので、「真の原因追究」と対策を実施する。必要により、原因究明対策ツール「4M-4Eマトリックス」を使用する。

②再発防止のため、緊急対策と恒久対策を策定し、有効性の事前評価をする。
その対策の直接効果と、費用、運用面への影響等とのトレードオフも評価する。

③再発防止対策をルール化する（規程化）

④対策の実施と徹底をする（実施指示、実施確認、教育研修の実施、日常点検）

⑤対策効果の検証（確認監査と監視、対策の妥当性を事後評価する）

⑥事故事例の水平展開（普遍化、関連処理への展開を含む）。なお、主役であり問題の解決策を握る「従業者」を巻き込むことが望ましい。

⑶委託業務事故の注意点

・事故原因により、自社（委託元）と委託先の対策とを峻別する。
・委託先選定体系等（方法・組織体制等）を評価し直す必要も発生する。
・委託契約内容（事故防止対策の仕様を含む）を確認するシステムを見直す
・すべてにおいて、ビジネス・チェーンとして自社と同様の認識が必要である。

6. 間接的対策の検討と提言

事故発生時には、直接対策（緊急及び恒久的対策）を講ずるのは当然であるが、事故原因を掘り下げていくと「間接的対策」が必要な場合が多い。

しかし、急を要する直接対策は実施しても、「間接的対策」までの徹底は十分ではないことが想定され、前項の再発防止対策とも関連する。

6-1 経営者及び経営機能に関する対策

⑴現状と課題

経営者は企業倫理、企業の存続性を強く意識して企業経営を指揮している。個人情報保護、個人情報漏えい防止についても、企業倫理上の課題であり、事故発生時には企業存続を危くすることもあることから、重要な課題である。

しかし、直接的な利潤を得ることができなく、事故発生時の応急対策に多くの勢力がさかれ、多発・頻発を招く経営体制・環境の改善が不十分であることも想定される。

以上を踏まえて、次のような経営者の取組みが要請される。

①個人情報漏えい事故防止に向け、方向を示して組織体制を具体的に強化し、業務遂行の指揮とフォローアップを行う。

②経営者の責務を再認識して、個人情報漏えいに向けた「自らの姿を見せる率先的実践」を行う。現行標準としては、JISQ15001規格3.9、JISQ27001:2006規格. 5.1がある。

⑵提言する主なチェックポイント

・トップは、個人情報漏えい防止に対し、積極的な関与姿勢と実質的な取組みを示し、全従業者の参画を求めているか
・経営目標・方針に個人情報保護（個人情報漏えい防止）を掲げ、経営機能全般を見据えた計画的、組織的な取組みをしているか
・推進実務責任者には取締役レベル・実力者を配置して全社的体制を敷き、具体的な業務分担と責任権限を明確化しているか
・事故防止と経営管理を一体化するためBSC等の経営ツールを使用しているか
・トップによる「ガバナンス＆マネジメント・レビュー」を実施しているか
レビュー軸は、C:コミュニケーション、S:情報共有、O:目的思考の徹底、かつ、S:迅速、S：着実性である。項目は、JISQ15001規格3.9を参照する。
なお、このキーワードは「インシデント管理」にも共通する。

〈注意点〉

・事故防止に向け、①弱い組織をなくす「全員参加」、②人の育成とセキュリティ技術継承を常時心がけた「全員レベルアップ」、の2点が要請される。

6-2 業務標準化に関する対策

⑴現状と課題

個人情報保護・事故防止はルールに基づく業務実施とマネジメント活動とがベースとなるので、ルール化、即ち成文化した規程によりこの仕組みを動かす標準化の意義は大きい。また、企業組織体において、業務品質、効率的業務遂行を維持するために、規程類（手順・様式を含む）の整備・運用は必須条件である。

しかし、必ずしも十分とは言えない企業があり規程類運用が有効性に疑問がある。

⑵提言する主なチェックポイント

・業種・規模など身の丈にあわせ体系化したルールがあり、部門別・階層別に「すべきこと、やらねばならないこと」を明記した内容となっているか
・事故多発防止対策をねらった施策を意識しラベリングした『ＲＹポイントの活用』を規程類に導入し定着させているか
・規程類の具体的作成・維持体制には現場実務者を含めているか
・規程類を業務の進め方とともに進化させ適切な改訂を実施しているか
・規程内容について経営判断を得ながら、実行支援を得ているか（経営的観点からの全社的バランスが必要である）

⑶業務標準化に関連した今後の課題

人間能力の限界を認識し、人間のみに頼らず、システム等による解決方法もバランス良く導入する必要がある。また、従業者の自主性、ルールのあり方とを意識し、常に、実施目的を明確に周知し理解を得る業務の進め方が要請される。

6-3 日常業務点検管理と是正・予防措置

⑴現状と課題

個人情報保護、個人情報漏えい防止は、従業者の日常活動の中で業務を遂行する際に作り込まれていく。この作り込みは日常業務の自主点検で確認できる。

JISQ15001規格3.7.1でも規定しているが、有効に機能しているか疑問である。

⑵提言する主なチェックポイント

・日常点検は、従業者・管理者の階層別、業務部門別に、計画的に実施しているか
・事故防止対策として、『ＲＹポイント』を活用して点検目的・項目・内容・周期を定め、品質作込みと従業者意識啓発のツールとして使用しているか
・日常点検計画は、業務実態と動向、経営成熟度等を考慮し、逐次見直しているか
・日常業務点検を、作業標準遵守、教育研修等と連動させているか
・日常点検結果その他の課題は、問題特定、是正措置・決定実施、効果と有効性の確認、をしているか（JISQ15001規格3.8の規定内容が参考になる。）

6-4 教育研修等に関する対策

⑴現状と課題

企業は従業者「人」で構成され、従業者教育が企業活動の原点である。

個人情報保護、情報漏えい防止に関しても、教育研修の重要性は大きいが、残念ながら、教育研修が十分機能しているか疑問である。

経済産業省の調査結果によると、①実施頻度が少ない、②未実施者が存在する、③実施後の評価が不十分である、④資料配布の留まるケースが多など、重要度認識に比較して実施が遅れている。

⑵提言する主なチェックポイント

・教育研修は、個人情報保護の取扱、事故防止対策の実践と徹底を図ることを目的とし、更には、安全管理マインドの醸成を求めているか
・共通内容を含め、部門別階層別に全員に対し教育研修を計画実施しているか
・作業者等の人間的特性、心理的特性を踏まえた上、テーマの選定、実施方法、実施周期、効果測定確認方法を工夫しているか
（特に、「ＲＹポイント」の事故事例、「ＲＹポイント」の事故事例、ヒヤリハット事例、「エラー防止の心得ルール」事例で気づきを与える研修等の利用、を検討する。）
・実施時期は、入社時、配置換時、期末首、朝礼時を含め日常的に継続的に何らかの機会を捉え、かつ、日常点検、監査などと連携した効果を目指しているか
・各種の教育研修、罰則等と連携し「情報モラルの向上」を図っているか

〈注意点〉

教育の最終目標は、リスクを的確に察知し、リスク防衛措置が働くよう育成することである。更に、“目的を明確に示し”“実行を確保”することが必要である。

また、教育研修に規程・マニュアル類を超えた力量の涵養を期待する。

具体的な実施事例としては、『経済産業省取組実践事例調査資料』が参考となる。

6-5 監査機能に関する対策

⑴現状と課題

マネジメントシステムにおいて、各段階の効果と課題を確認しフィードバックさせ、システム全体の改善と向上を図る重要な機能である。このため、第三者的な視点から監査が実施されれば、個人情報漏えい防止効果が期待できる。

しかし、年１度の監査で「監査チェックシート」を埋めていく程度の認識であるならば、効果が期待できないのではないか、と危惧する。

⑵提言する主なチェックポイント

・ルール監査、実施状況監査、特別監査があり、目的に沿って実施しているか
・すべての組織、従業者を対象として計画的に

実施しているか
（場所・内容・時期：実施頻度はマネジメントシステムの成熟度で決める）
・「ＲＹポイント」、リスク認識結果、残存リスクの点検を監査項目に含めているか
・内部監査における監査員の公正性、品質確保、指導力を維持しているか
・監査実施後の的確な是正措置をフォローアップしているか

〈注意点〉
・昨今の社会情勢・技術動向から必要により外部特別監査も適時導入する
・監査の枠を超えた「経営者のマネジメント＆ガバナンスレビュー」と連動させる
・監査の品質向上が課題であり、メジャー（尺度）の的確性も要請される。
・監査実施関係者の指導力、スキル向上がないと本来の機能が発揮できない。

7.「個人情報漏えい防止評価チェックリスト」の活用

⑴対象と目的

一般事業者を対象として、本論文に基づく「提言する主なチェックポイント」について点検評価を行い、「事故防止体制」と「重点的対策」とを『総合的』に確認し強化することを目的とする。
これらの点検評価結果により事故対策の段階的、選択的実施が可能である。（プライバシーマーク認定事業者でも部分的な利用は可能と考える。）

⑵評価要素と構成

次の５対策群110項目で構成する。
〈詳細は**【別図2】**を参照〉
「体系・体制群」＋「具体的対策群」⇒110項目
（3群11区分）　（2群）　（5群）
・「体系・体制群」は事故防止にむけた「仕組み」としての対策群である。
・「具体的対策群」はＲＹポイント重点対策群など具体的な対策群である。
なお、基本的安全管理対策は、物理的・技術的対策等の共通的基本対策である。

⑶活用方法の概要

①活用事業者は、⑵項の評価項目を点検し、スコアを得ることにより、当該事業者の「個人情報漏えい防止能力」を総合的に評価（認識）する。
②マクロ・アプローチによる評価結果の活用：
各対策群のバランスのとれた複合的対策要素について、事故防止対策を評価する。群別スコアを図示して正五角形となるよう歪みを正すような「対策強化」が期待される。
③ミクロ・アプローチによる評価結果の活用：
対策群内の各項目スコアを検討し課題の根本的な解決策を検討、実施する。
この際、規程があるにも関わらず実施していない項目の検討が重要である。
④評価を定期的に実施し、段階的、選択的な対策実施により能力向上を図る。

8. まとめ

個人情報漏えい防止に向けて、一般企業現場用の「個人情報漏えい防止評価チェックリスト」を作成し、重点的、総合的な対策を実施するよう提案をまとめた。

これらの重点的、総合的な一連の対策実施により、効果的、効率的に事故減少化が図られることを期待している。関係者のご利用により、ご意見と示唆をいただきながら、より充実した施策としてブラッシュアップを図っていきたい。

最後に、ご指導いただいた放送大学大学院原島准教授、関連資料を参照引用させていただいた関係者の方々、及び、各種のご教示と示唆をいただいた方々に深くお礼を申しあげます。

（終）

この論文は、放送大学大学院平成20年度・修士論文「個人情報漏えい防止に向けた実践的取組み」（H20.12提出）を抜粋し要約したものである。

≪引用・参考文献≫

⑴個人情報保護法：「個人情報の保護に関する法律」平成15年法律第57号（H15.5.30）
⑵日本工業規格JISQ15001－2006『個人情報保護マネジメントシステム－要求事項』㈶日本規格協会（H18.5.20）
⑶日本工業規格JISQ27001－2006『情報技術－セキュリティ技術－情報マネジメントシステム－要求事項』㈶日本規格協会（2006.5.20）
⑷『2007年情報セキュリティインシデントに関する調査報告書』日本ネットワークセキュリティ協会（2008年6月13日）（P42.個人情報の機微度”に関する「JOモデル」を含む）
⑸『平成19年度個人情報の保護の関する法律施行状況の概要』内閣府（平成20年9月）
⑹『経済産業分野の事業者における個人情報の保護に関する取組み実態調査2008報告書』経済産業省商務情報政策局・㈶日本情報処理開発協会（平成20年2月）
⑺日本情報処理開発協会『（平成19年度）（平成18年度）個人情報の取扱いにおける事故報告にみる傾向と注意点』㈶日本情報処理開発協会、（平成20年6月10日）（平成19年6月11日）

(8)『平成18年度個人情報の保護の関する法律施行状況の概要』内閣府(平成19年9月)
(9)『個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン』(平成20年2月29日厚生労働省・経済産業省告示第1号)
(10)河野龍太郎他、『ヒューマンエラーを防ぐ技術』日本能率協会MGC(2006.9.15)
(11)宇賀克也、『個人情報保護法の逐条解説』(第2版)有斐閣(2005.2.28)
(12)『JIS Q 15001:2006をベースにした個人情報保護マネジメントシステム実施のためのガイドライン―第1版―』P43. (財)日本情報処理開発協会(2006.8)
(13)『ISMSユーザーズガイド-JIS Q 27001:2006(ISO/IEC 27001:2005)対応』(財)日本情報処理開発協会(平成20年1月31日)
(14)GMITS3:「JIS TR X 0036-32001 ITセキュリティマネジメントのガイドライン」。
(15)中田亨『ヒューマンエラーを防ぐ知恵:ミスはなくなるか』書籍・科学同人出版(2007.3.20)
(16)齋藤敏雄、研究論文『情報セキュリティのためのヒューマンエラー分析枠組み』第21回システム監査学会(09, 2007)P2.(『エラー防止の心得ルール』(情報を扱う時の心得)を含む)
(17)『ヒユーマンエラーの事例と影響』システム監査学会(2007年9月12日)
(18)『10大脅威 ますます進む「見えない化」』独立法人情報処理開発機構(2008.5)
(19)MS-ISAC(2006)『Top Ten Cyber Security Tips』News-Letter OCTOBER 2006 Volume 1
(20)樋口晴彦『組織行動のまずい!!学』 書籍・祥伝社(2006.7.5)
(21)MBWA(Management By Walking Around):T.Jピーターズ他著、大前研一訳『エクセレント・カンパニー』㈱講談社(1983.7)
(22)BSC(Ballanced Scorecard):吉川武雄、『バランス・スコアカード入門』生産者出版(2001.2.22)
(23)『平成19年度個人情報保護の適正な保護に関する取組実践事例調査・報告書』経済産業省(平成20年2月)
(24)PCIDSS:『PCIデータセキュリティ基準・完全対策』山崎文明監修、日経BP社(2008.4.14)
(25)日本システム監査人協会・個人情報保護監査研究会『個人情報保護マネジメントシステム実践マニュアル』工業調査会(2006)
(26)堀部政男他『個人情報マネジメントシステム要求事項の解説』日本規格協会(2006.6.30)
(27)「4M-4Eマトリックス」:4つのMで要因分析を行い、4つのEで対策をたてる。
4M:Man(人間)、Machine(物、機械)、Media(手段、方法)、Management(管理)
4E:Education(教育)、Engineering(技術)、Enforcement(強化)、Examples(事例)

【別図 1-1:『RYポイント』一般要約版】〈目的別・媒体別区分〉

1	**取扱共通** ①取得・利用する個人情報は必要最小限度とする ②機密・一括大量の個人情報は厳重に扱う(保管・保護方法、利用方法等) ③個人情報は、原則として社外に持出さない。(持出しは許可制とする) ④高機密度情報・大量情報の取扱は複数人によるダブルチェックをする ⑤例外処理は極力避ける。例外処理時は承認処理とし、事後確認をする ⑥机、作業場所の整理整頓を励行する
2	**メール(メルマガ含む)・FAX・宅急便等の取扱** ⑦メール・FAX・宅急便等の誤送付・送信がないよう、相手・内容をダブルチェックする(←受領確認) ⑧メール送信はCCとせず、BCC、専用ソフト等を使用する
3	**ノートPC・記録媒体・携帯電話** ⑨移送・授受時、媒体(メール添付含)は暗号化(PWロック含)し、移送手段を選択する ⑩携帯PCの持出、社外PCの持込みを禁止し、やむ得ない場合は許可制とし措置確認する ⑪記録媒体・PCの持出の際は暗号化と利用時の注意を遵守 ⑫多量情報を含むUSB、媒体、紙などの記録媒体は取扱ルールを遵守する ⑬盗難防止のため車を施錠し、PCの放置を厳禁、運搬ルールを遵守する ⑭携帯電話はセキュリティ・ロックを行い、帯同し、内部情報を最小限にする ⑮ノートPC・記録媒体の廃棄時には個人情報を確実に除去・消去・廃棄する
4	**個人情報の利用・授受・保管・廃棄** ⑯オフィス・個人情報保管場所を施錠管理し、アクセス者を限定し、点検する ⑰利用(アクセス)記録を残し定期的に取扱状況を点検する ⑱移送・授受時は授受記録を残し取扱状況を点検する ⑲保存期限管理をし、廃棄を第三者が点検し、記録する

5	**ＰＣ端末・インターネット・システム等の取扱・操作** ⑳ ID ／パスワードの仕組み（ポリシー）を守る（桁数・期限等・共有の禁止） ㉑ウィルスソフトの自動更新、パッチ処理を励行する（ボット・マルウェアを含む） ㉒ネット・セキュリティ対策を守る（メール添付物の開封注意。業務以外のウェブ使用禁止）
6	**システム管理者の特別措置**（★：Step up 項目） ㉓ウェブページのセキュリティ対策（SQL 対策等）を実施する ㉔ウェブページへの公開作業ルールを定め、公開時にはダブルチェックする ㉕ファイル交換ソフトの定期点検をし、無許可インストールを禁止する ★㉖ ID ／ PW、アクセス権の付与・削除等ルールを遵守し、第三者の定期点検をする ★㉗情報システムの設定条件を点検する（初期設定、サービス運用中の変更等） ★㉘技術動向・社会動向による新しい脅威情報を入手し、先手のリスク対策を実施指導する

〈情報を扱うときの心得（10 ヶ条）〉

①確認の習慣を身につける	⑤作業途中で中座しない	⑨自分を良く知る
②結果を想像する	⑥体調管理を心がける	⑩周りにも気を配る
③無理をしない	⑦作業準備を行う	
④大切なものを扱っているとの意識を持つ	⑧後があると思わない	

【別図 1-2：『ＲＹポイント』管理版】〈取扱ライフサイクル別・階層別区分〉

区分	RY ポイント	目　的	担当者	管理者	記事
取得入力	①取得・入力作業の限定 （担当者、場所、端末、取得方法等）	誤入力・改ざん防止	○		
	②授受記録、保管	授受確認	○		
移送送信	③ネット送受時の暗号化・ＰＷ化	盗聴・漏えい防止	○		
	④メールのＢＣＣ扱い（ツール使用含）	漏えい防止・誤り防止	○		
	⑤媒体・移送等手段の選択	漏えい・紛失防止	○		
	⑥移送時の媒体暗号化・ＰＷ化	紛失・漏えい時対策	○		
	⑦運搬ルール遵守（運搬・移送・送信）	紛失・盗難防止等	○		
	⑧発送内容・あて先の点検・受領確認	誤り防止	○		
	⑨発送（引渡し）記録、保管	発送・引渡確認、誤り防止	○		
利用加工	⑩利用加工処理の限定（作業者、作業場所、作業端末等、無断複写複製等の禁止）	漏えい・不正アクセス防止、誤操作防止	△	△	
	⑪識別情報の発行・更新・削除・点検ルールの実施（共有禁止含む）	不正アクセス防止	△	◎	
	⑫アクセス権の発行・更新・削除・点検ルールの実施（ＮＫＬＰ＊）	不正アクセス防止等	○	◎	
保管ＢＫ	⑬クリアーデスク	盗難・不正・紛込み防止	○		
	⑭媒体施錠保管と把握管理(鍵管理含）	盗難・不正アクセス防止	○		
	⑮バックアップ実施	情報保存（可用性）	○		
消去廃棄	⑯保管期限に基づく点検（廃棄、記録）	事故リスク源最少化	○		
	⑰廃棄時の点検確認、記録	誤り廃棄防止	○		
	⑱ＰＣ・媒体等の廃棄処理	漏えい防止	○		
全般共通	⑲オフィス・個人情報保管場所の施錠	盗難・漏えい防止	○		
	⑳携帯ＰＣの盗難防止	盗難・不正アクセス防止	○		
	㉑機微・大量情報処理の二重確認	誤り防止	○		
	㉒個人情報社外持出しの許可・点検	盗難・漏えい防止	○		
	㉓携帯ＰＣ等の持出し許可制実施	盗難・漏えい防止	○		
	㉔携帯電話取扱（帯同・セキュリティ対策）	盗難・漏えい防止	○		
	㉕ネットキュリティ対策の遵守（メール開封注意。業務外のウェブ使用禁止）	インターネットリスク防止（マルウェア対策を含）	○		

システム共通	㉖ＰＷポリシーの遵守（桁数・使用期間等、共有禁止）	不正アクセス防止等	○	△	
	㉗ウィルスソフト自動更新、パッチ処	不正アクセス防止・ボット等対策	△	◎	
	㉘ウェブページ・セキュリティ対策（XSS.SQL対策等）	ネットによる漏えい・改ざん等防止		◎	
	㉙ウェブ公開作業のダブル点検	誤操作防止		◎	
	㉚アクセスログ取得、点検、保管	不正アクセス防止・情報保存		◎	
	㉛ファイル交換ソフトの使用禁止・点検（無許可インストール禁止を含）	漏えい・不正アクセス防止	○	◎	
	㉜情報システムの設定条件点検（初期設定、運用中の変更等）	漏えい・不正アクセス防止		◎	
	㉝新脅威情報入手と対策実施・指導	先手のセキュリティ対策		◎	

＊ NKLP: Needs to know, least priviledge
記事《担当者対策》○：日常業務にて実務的関与。△：認識として関与が必要。
《管理者対策》◎：主として管理者関与。△：システム対処も必要。
なお、管理者はすべての項目に関し、システム的・体制的関与が必要

【別図2】【個人情報漏えい防止評価チェックリスト】

各対策群・項目の現状レベル・バランスを総合的に評価しレベルアップする（5対策群・110項目）

「体系・体制群：55 項目」 仕組みとしての対策群〉	「具体的対策群：55 項目」 〈具体的な実施対策群〉
①直接対策群（15） ・個人情報特定管理 ・業務フロー作成確認 ・個人情報リスク認識等管理 **②多発防止対策群（15）** ・多発事故・HE対策管理 ・委託先監督管理 ・事故発生後対応管理 **③間接対策群（25）** ・経営機能・ガバメント管理 ・業務標準管理 ・日常点検管理 ・教育研修管理 ・監査機能	**④「ＲＹポイント」重点対策群（25）** ・取扱共通 ・移送手段取扱 ・ノートPC・媒体等取扱 ・個人情報利用／授受／保管／廃棄 ・PC端末等の操作 ・システム管理者の措置 **⑤「基本的安全管理対策」（30）** ・物理的安全管理対策 ・技術的安全管理対策 ・人的安全管理対策 ・組織的安全管理対策 ・正確性確保対策 （④と重複5項目を除く） 経済産業分野指針の例示の127項目から選択）

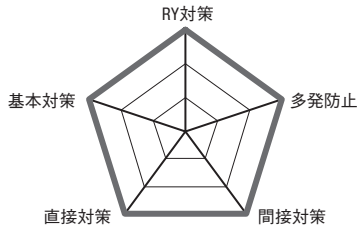
〈評価「スコア」値の例示〉…問題解決型の独自スコアを採用…
3：対策が規程に有。その対策を実施している → 評価結果として、十分である
2：対策が規程に有。その対策を実施してはいる → 当面能力があっても将来は不明
1：対策が規程に有。その対策を実施していない → なぜ対策が未実施か課題である
0：対策が規程に無。 → 大きな課題である

【活用例】

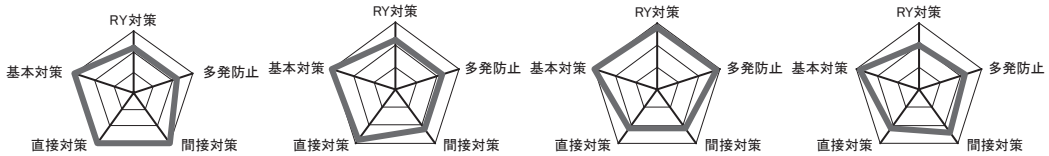
〈マクロ･アプローチによる改善〉
バランス良い各対策群構成に改善
フルスコア値との比率で表示

〈ミクロアプローチによる改善〉
個別対策のスコア値による
徹底改善の実施

【個人情報漏えい防止評価チャート】例示
理想的な評価チャート
〈マクロアプローチ〉



漏えい防止評価チャートの典型的なパターン例《マクロアプローチ》



①〈多発防止等対策が弱い〉
多発防止対策・RY対策共に弱い。
⇒多発防止・RY対策を重点的に強化する。

②〈多発防止等対策・間接対策が弱い〉
多発防止対策・RY対策と間接対策（支える仕組み）が弱い。
⇒多発防止対策、RY対策、間接対策を強化する。

③〈直接対策・間接対策の仕組みが弱い〉
一応の多発防止等対策は講じているが、直接・間接対策（「対策策定の仕組み」と「支える仕組み」）が弱い。
⇒現在は特段の問題がないようであるが、今後の事業展開と外部セキュリティ動向に対応できるよう体質改善（「仕組み（直接・間接対策）」の強化）を行う。

④〈各種対策が全般的に不十分〉
多発防止等対策のほか、各種対策実施が不十分である。
⇒・早急に多発防止等対策を強化する・平行して、体質改善（各種の仕組み強化）を行う。

会報掲載論文募集要項

会員の皆さんより、会報掲載論文を募集します。

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。

会報掲載論文審査要綱

理事会提案　2003.7
最終改訂　　2003.10　判定基準（点数）改訂

1. **論文審査委員会**
応募論文が提出されたら、編集委員長は、応募条件を満たしているかを判断する。
応募条件を満たしていない場合、直ちに却下する。
(応募条件：字数の制限、応募者は会員であること)
応募条件を満たしている場合、直ちに、編集委員の中より、２名の審査委員を任命する。
編集委員長を含めて３名で審査委員会を構成する。
論文提出者を、審査委員に加えることはできない。
編集委員長が論文提出者の場合、編集委員長を除いた編集委員会で3名を選出し、審査委員会を構成する。
審査委員名は公表しない。
2. **審査委員は、提出した論文を査読し、判定基準表に基づき、点数を出す。**
判定基準は、会員からの要望があれば公表する。

2009年4月20日

会員除名の公告

特定非営利活動法人日本システム監査人協会
会長　鈴木　信夫

協会は、本年4月9日の理事会で、会員番号1395田村丈夫氏を、定款第11条第1項第2号により除名することに決しました。

定款第56条により、ここに公告します。

以上

（編集後記）

今回の新型インフルエンザへの対応で印象に残ったのは、感染の疑いがある場合の「停留」、住所地の保健所による個人の追跡調査、さらに、ウイルスの遺伝子検査により、新型かどうかを判定するという報道の裏に読み取れる、現在の医療情報システムの状況です。政府、出先の官庁間や自治体間が共同して対処するために必要な情報の共有と連携、開業医や病院間の情報ネットワークの連携、診療情報の標準化、遺伝子情報を含む個人情報の提供と管理のありかたなど、考慮し改善するテーマが見えてきます。今後の監査の姿として、現代社会が求める水準を早く充足できるよう、システム監査で指摘し、改善できる姿をイメージしています。（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
山田　隆　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