特定非営利活動法人
SAAJ 日本システム監査人協会報

特集１．公認システム監査人の認定状況と継続教育

鈴木　信夫(継続教育プロジェクト主査)

(1) 公認システム監査人の認定状況

平成15年度(Ｇ３)の公認システム監査人、システム監査人補の申請数は、公認システム監査人(CSA)88、システム監査人補(ASA)53である。Ｇ３のCSA申請の特徴としては、すでにASAとして認定された方々が、協会主催の監査実践セミナーに参加し、システム監査に強い自信を持たれて申請されている。この方々は昨年に続き、本年も面接を受けているが、１年でこうも変わられるかという印象である。

Ｇ３内定段階でのCSA者数は、CSA申請者88に対し、CSA内定は67で、76%である。21人がASAとして認定予定である。

＜公認システム監査人等人数＞　03.11.16 現在

	G0	G1	G2	G3(内定段階)	計
公認システム監査人	34	126	93	67	320
システム監査人補	0	69	122	74	—
補で次年度に監査人への申請者	0	0	31	0	—
当該年度の補	0	69	91	74	234
計	34	195	184	141	554

(2) 公認システム監査人等継続教育セミナーの活動状況と今後の予定

当協会公認システム監査人認定委員会では、CSA等の継続教育対応の一環として、継続教育部会(部会長、橘和副会長)の中にプロジェクト体制を組んで、協会主催のセミナーを企画、実施しており、平成15年度は別紙のように実施した(月例研究会とは別途)。

＜今後の予定＞

現在、東京で次回を予定している。各支部では東京での内容に準じてそれぞれ設定するようお考えいただく。

1. 狙い：
市場として大きく展開しそうな自治体の動向を探る一端として、自治体のIS関係者から話を伺う。
2. セミナータイトル：
「電子自治体の今、これから」(仮称)
3. 年月日：
2004年１月31日(土)　13：30から17：00

目　次

4. 場所：
東京都港区、機械振興会館会議室、
6階66会議室(スクール形式で90名)
5. 講師：
1) 三鷹市企画部情報推進室
新藤　豊氏
2) ① 柏崎市総合企画部 情報化総合戦略室長
植木　幸雄氏
② 柏崎市情報化関連業務受託共同企業体 事務局長
(株式会社柏崎情報開発センター業務部事業企画室)
渡辺　靖(おさむ)氏
6. 両市にお願いした理由：
1)三鷹市；
日経パソコンの今年度「e都市ランキング1位入賞」。
講演内容：現在、市で実施されている情報システムの概要および重点事項として、「申請・届出に伴う公金の電子収納」。
質疑も入れて1時間30分程度。
2)柏崎市；
日経ガバメントテクノロジー「自治体サイトの使いやすさ全国第1位」。
講演内容：市の情報システムに関わる全業務を地元企業共同体にアウトソーシング。市役所のご担当(約40分)：アウトソーシング決断の経緯など、公表されているいろいろな金額については、必ず出していただく。
KSU(柏崎市情報化関連業務受託共同企業体)ご担当(約30分)：SLAを中心に市の業務を受けた側のいい点、難しい点、および自治体業務アウトソーシングの今後の見通しなど。
お2人に対する質疑応答(20分ほど)、合わせて1時間30分程度。
7. 参加料金：
協会会員3,000円、非会員5,000円。
8. 周知方法：別途ML等による。

＜平成15年度活動状況＞

＜東京＞

1. 主催：日本システム監査人協会
2. 日時：平成15年８月１日(金)13：30−17：30(懇親会18：00−20：00)
3. セミナータイトル：情報セキュリティ監査基準を解説する
4. 場所：東京港区、機械振興会館、６階会議室６−66
5. 講演内容(実施順)
   ・情報セキュリティ監査基準の実務的解説
   協会副会長　和貝　享介
   (経済産業省情報セキュリティ監査研究会委員、監査法人トーマツ　代表社員)
   ・わが国の情報セキュリティ政策について
   経済産業省情報セキュリティ政策室　課長補佐　山崎琢矢氏

＜広島＞

1. 主催：日本システム監査人協会
2. 後援：中国経済産業局/ITコーディネータ協会
3. 日時：10月24日(金) 14:00−18:00(懇親会18：00−)
4. 場所：広島県生涯学習センター(ばれっとひろしま)(広島市東区)
5. セミナータイトル：情報セキュリティ監査基準を解説する
6. プログラム：
   ・開会の辞　日本システム監査人協会副会長　橘和　尚道
   ・わが国のIT戦略と情報セキュリティ政策
   中国経済産業局産業部情報政策課　課長補佐　向井　裕 氏
   ・情報セキュリティ監査基準の実務的解説　本協会副会長　和貝　享介
   ・閉会の辞　本協会中国支部長　大谷 完次

＜大阪＞

1. 主催：日本システム監査人協会
2. 協賛：情報システムコントロール協会(ISACA)大阪支部
3. 日時：10月25日(土)　13：30−17：30(懇親会18：10−)
4. 場所：松下IMPビル５階会議室
5. セミナータイトル：情報セキュリティ監査基準を解説する
6. プログラム：
   ・開会の辞　日本システム監査人協会副会長　橘和　尚道
   ・ごあいさつ　近畿経済産業局産業企画部情報政策課長　森畑　通夫氏
   ・情報セキュリティ監査基準の解説　本協会副会長　和貝　享介
   ・情報セキュリティの動向　情報処理振興事業協会セキュリティセンター
   企画調査グループリーダー　日下　保裕氏
   ・閉会の辞　本協会近畿支部長　石島　隆

特集２．SAAJ研究部会の活動状況と今後の予定

システム監査基準研究部会活動報告

三井情報開発株式会社
総合研究所　本田　実

研究会の趣旨

システム監査基準の改定の状況把握と当協会としての今後の対応案検討

研究会のメンバー(敬称略)

橘和 尚道、勝田 敦彦、力 利則、沼野 伸生、芳仲 宏、本田 実(研究会主査)

研究会の活動日程及び今後の予定

10/２(木)第1回打合せ
10/14(火)第2回打合せ
11/ ４(火)第3回打合せ
11/20(木)第4回打合せ予定
12月以降３月まで２回／月開催予定

情報セキュリティ監査基準研究会(主査は木村理事)と連携をとるために、必要に応じて主査が相互に研究会に出席することとした。

成果物(予定)

「システム監査基準改定に当たっての当協会の今後の対応」報告書(仮称)

研究会の内容

経済産業省では、今年度４月より情報セキュリティ監査制度を運用開始した。最近の情報技術の進展、活用の高度化、リスクの増大などに伴い、1996年に改定されたシステム監査基準も見直しの必要性があるとの認識のもとに、日本情報処理開発協会では経済産業省の依頼により「システム監査基準検討委員会」を創設した。

委員会には経済産業省山崎課長補佐、大崎係長を迎えて、(財)日本情報処理開発協会が事務局、各関連団体(日本システム監査人協会、(財)金融情報システムセンター、日本公認会計士協会、(社)日本情報システムユーザー協会、情報システム・コントロール協会、システム監査学会、日本内部監査協会)及び有識者が委員となっている。現在は、監査基準WGと管理基準WGを発足させ各基準案を作成中である。

当協会からは橘和副会長(当協会の代表として参加)と本田(システム監査学会代表)が委員会のメンバーとして参加している。

当研究会では、橘和副会長及び本田からの委員会の活動状況の報告と当協会としての今後の対応について検討する予定である。現状は、主に委員会の活動状況の報告が中心である。

研究会で報告した委員会の活動状況は、以下のとおりである。

① 委員会活動日程
　７/1、８/5、８/28、９/12、来年１月(予定)、来年３月(予定)
② パブリックコメント
　来年２月(予定)
③ 監査基準WG活動日程
　９/22、10/20、11/10、11/18、12/８(予定)、12/15(予定)
④ 管理基準WG活動日程
　９/30、10/14、10/28、11/11、11/25、12/９(予定)、12/22(予定)
⑤ 委員会の主な方針・課題・意見等
・来年３月までにシステム監査基準を改定する。
・システム監査の呼称はそのままとする(情報システム監査とはしない)。
・システム監査基準と情報セキュリティ監査制度の関係を明確にする。
・情報セキュリティ監査制度の体系に合せ、システム監査基準とシステム管理基準(仮称)に分ける。
・新しく作成する基準はシンプルにして、詳細は解説書で解説する。今回は解説書の作成を行わない(来年４月以降)。

・解説書についても単に1参考書ということでなく、ある程度の権威を待たせた方がよい。

⑤監査基準WGの主な方針・課題・意見等

・システム監査基準はシステム監査人の行為規範とする。
・用語の定義が必要であるが、具体的に載せる用語については検討中。
・基準は内部監査を前提とし、外部監査にも適用できるものとし、外部監査特有の項目は契約などで規定する。
・COSO ERMの考えを取り入れるべきである。
・コントロールの概念を明示した方がよい。

⑦管理基準WGの主な方針・課題・意見等

・システム管理基準は、システム監査人の判断指針、及び組織体としての管理基準の拠り所とする。
・現行基準の問題点を整理する。
・現行監査基準の実施基準が該当するが、企画・開発・運用・保守以外に、情報戦略を追加する。
・ITガバナンスを何らかの形で考慮する。
・SLCとして、共通フレームやJIS X 0160等を考慮してはどうか。

情報セキュリティ監査研究部会活動報告

「情報セキュリティ基準」を対象にした研究活動について経過報告と研究会参加のお誘い

2003年11月15日

No.0148 木村 裕一

今年度の活動として、表記部会が設置されて、「セキュリティ技法研究会」のメンバーが中心に取り組んでおり、現在の活動状況を紹介する。

1. 活動テーマ

1.1 テーマ

テーマを「情報セキュリティ監査実践ワークシートの作成」とする。この春、経済産業省が情報セキュリティ監査研究会報告として発表した「情報セキュリティ監査基準」を材料に、情報セキュリティ監査の実践において利用できるワークシートの作成(XMLによる)と活用を課題とする。

1.2 内 容

ワークシートは、具体的には監査対象・目的に応じて「情報セキュリティ管理基準」の項目を取捨選択できるツールとする。限られたメンバーで進めることから、ある程度分野と範囲を絞ってワークシートを作成することになる。検討は次の内容に分かれる。

(1) 「組織体においては、本管理基準を基礎として、リスクアセスメントの結果等に基づき、独自に必要とする項目を追加、あるいは削除して活用することができる」(経済産業省情報セキュリティ研究会資料より引用)とあるので、情報セキュリティ管理項目のXMLタグに属性を付与して、監査実施時に、この属性により必要項目をピックアップできるようにする方法が考えられる。このタグの付与方法が、ひとつの検討課題になる。

(2) また、「情報セキュリティ監査基準」に基づき監査を進めるに当たっての計画立案—目的設定、対象の選定、監査体制の整備等、監査実施—監査証跡の入手、評価、調書の作成、等々について「システム監査基準」との対比も考えにいれて検討する必要がある。

(3) ツールについては、メンバーのYK氏から、この考えに基づくツールの雛形を提供してもらい、これをベースに進める考えである。

(4) 出来ればワークシートを実際に使って結果を評価し、仕組みに反映し、使い方に反映させる場を作ることも狙いとしたい。

2. 研究過程と成果へのアプローチ

実践ワークシートの作成は、情報セキュリティ管理項目のナレッジベース化を図るものである。その企画案は次のとおりである。

＜情報セキュリティ管理項目のナレッジベース化 企画案＞

1. 背景

情報管理セキュリティ管理項目は、レファレンスモデルとしての位置づけである。すなわち、適用にあたっては、これを参照元として、各組織体へのカスタマイズ化が必要である。そのためには、他の各種規格との対応(JIS X5080、ISMS、ISO15408など)が必要であり、かつ、組織体の規程集との対応などが必要となる。また、各管理項目について、監査人としての経験を積み上げていくことが必要となる。

2. 必要となるもの

以上の要求を満たすために、管理項目の電子化(文書に関するデータベース)とそれの事例等を蓄積、検索できる、所謂、ナレッジベースを構築する必要がある。

3. 企画

上記の目的のために、情報管理セキュリティ管理項目のXMLによるタグ、属性付けによる電子的管理を行う。

4. 開発工程

(1) 情報管理セキュリティ管理項目の電子化：EXCEL化、並びに、XMLによるウェブ閲覧

(2) 属性付け

①管理項目についてグレードをつける。

最低限必要なもの(Minimum, Must)／あるのが望ましいもの(Better)／あって欲しいもの(Best)など

②また、業種にあっては変化するもの(流通業、物流業、製造業、サービス業、金融業など)

(3) 各人の経験に基づくエピソード収集

(4) 上記の属性、エピソードの蓄積とそれの検索システム構築

3. 研究会の経過

(1) 現在はまだアプローチ段階で、下記の研究会の経過に見られるように実際のケースを各回6～10名程度の参加者により勉強中である。今からでも研究会に参加することは全くハンディなしで取り組むことが可能であると考えられるので、皆さんの参加をお待ちします。

(2) これまでの研究会の経過(開催日、開催場所、テーマ、発表者等)

4月15日(火) 協会事務局

「今年度の研究テーマについての検討会」

5月30日(金) 協会事務局

①「情報セキュリティ監査基準教育に関する検討」

②「情報セキュリティ監査基準のツール化とその進め方」木村陽一

③「CISSPについての紹介」木村陽一

6月18日(水) 日本橋久松町区民館

①「JISX5080：2002についてと、その検討コメント」木村陽一

②「Webにおけるセキュリティ上の問題—CSS、ユーザ認証など」

7月15日(火) 人形町区民館

「6月度の続き」

9月2日(火) 人形町区民館

①「セキュリティ分科会活動—情報セキュリティ監査制度の情報管理セキュリティ管理項目についての説明作成、セキュリティ知識体系の整理」、「プロセス革新」木村陽一

②「ウイルス/ワームは何故移るのか」

木村陽一

9月16日(火) 人形町区民館

「個人情報での安全対策の考え方とマネジメントシステム」 木村裕一

10月14日(月) 人形町区民館

「ISMS監査—ISMS認証と情報セキュリティ監査」 木村陽一

11月13日(木) 人形町区民館

「某社のISMSの取り組み状況—ISMS導入、監査の実施について」 金子長男

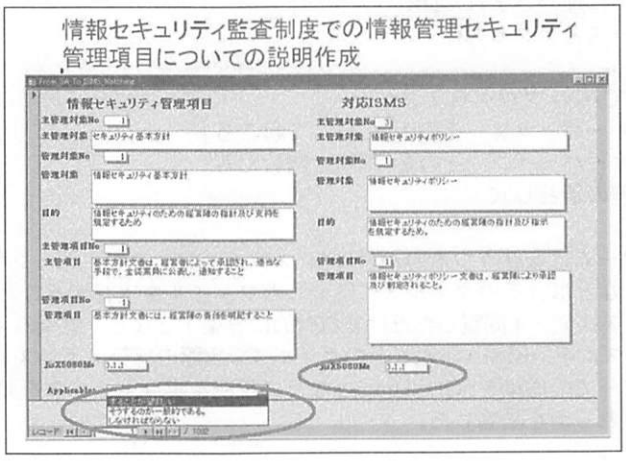
4. 各回の研究会の検討内容の紹介

以下に、研究会の検討内容、結果の一部を紹介する。

4.1 情報セキュリティ監査基準のツール化について

現在、ISMS監査においては、情報資産のリスクアセスメント後、そのリスク対応計画としてISMS詳細管理策127項目をどのように適用して、それを実施していくかが求められている。適用宣言書に、そのISMS詳細管理策の実施乃至は除外の理由を明確にする必要がある。その際に、その実施手順等を各種マニュアル又は規程に盛り込んで対応するかと思われる。そうした際に、その管理基準とマニュアルの項目、規程の条項とのマッピングが必要となる。また、ISMS詳細管理策の詳細化としては情報セキュリティ管理基準もあり、それの活用も必要となる。

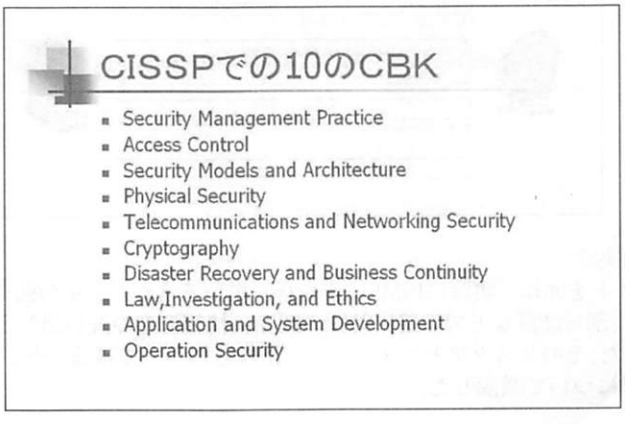
この様に、ISMS詳細管理策、情報セキュリティ管理基準、社内規程・マニュアルなどのそれぞれの対応付けが求められる。ISMS詳細管理策と、情報セキュリティ管理基準はおおもとのJISX5080との対応が存在する。これらを参考に、ISMS詳細管理策、情報セキュリティ管理基準との対応関係と、それにまつわる監査実務の知識ベースを作ることが可能な入れ物を可能とするツールを作成することを議論した。そのためには、XML等の使用で柔軟性を持ったナレッジベースの構築を企画することとなった。現在、それぞれの管理項目のJISX5080での紐付け等を行い下記のような参照画面の作成を行っている。



4.2 セキュリティ監査に必要となるBody Of Knowledgeについて

PWBOKなどでの知識分野の知識について羅列することで、その知識体系を明確にする方法がある。所謂、Body Of Knowledgeである。セキュリティに関してはCISSP等の試験で、そのCommon Body Knowledgeがある程度、明確にされている(旧のunixなどの知識が求められているが)。これの紹介を行った。10の知識分野は下図の通りである。

これらを参考に、情報セキュリティ・監査におけるBody Of Knowledgeについて討論した。



4.3 セキュアプログラミングの実際

IPAのホームページで掲載されているセキュアプログラミング講座について、詳細の説明会を実施した。特にクロスサイトスクリプティング、バッファオーバフローなどのメカニズムについて監査できるように説明を行った。その内容は下記の通り。(項番は上記サイトのテキストと同じである)

第1章 セキュアWebプログラミング
1−1. クライアント側入力チェックは安全でない
1−2. クロスサイトスクリプティング
1−3. Webページとユーザ認証
1−4. クエリストリングから情報が漏れる
1−5. hiddenは危険(セッション変数を利用しよう)
1−6. Webフォームの選択項目が危ない

第2章 セキュアデータベースプログラミング
2−1. SQL組み立て時の引数チェック
2−2. スクリプトに埋め込まれたDBパスワード
2−3. データベースとアクセス権

第6章 セキュアC/C++プログラミング
6−1. バッファオーバーラン その1「こうして起こる」
6−2. バッファオーバーラン その2「危険な関数たち」
6−3. 文字列処理の落とし穴

4.4 ウィルス/ワームはなぜうつるのか(日経システムインテグレーション等から)の説明

従来のウィルスなどは、そのウィルスに感染したファイルを実行することで感染が拡大していったが、最近のウィルスはメール閲覧しただけで自動的に感染するなど、感染のメカニズムが変わってきている。このメカニズムを、Klezメールなどのウィルスで実際の感染メカニズムを説明した。また、バッファオーバーフローでの感染をSQL Slammerなどで説明を実施。それらを元に監査項目としてどのような対応が求められるかを議論した。

4.5 ISMS監査の実際

ISMSユーザガイドを元に、実際にISMS監査を行っている者から、その監査での問題点などを抽出して議論した。特に、部分認証などでの適用範囲の問題、情報資産の洗い出しとそのグルーピング化などについて議論。また、そのリスクアセスメントの方法などについて議論した。ISMSのプラン段階では、次図のような対応について議論した。

システム監査事例研究会(事例研)活動報告

No.679 吉田　裕孝

毎月第一水曜日18：30から三井物産(地下鉄大手町C-5出口)内会議室で月例会を開催しております。SAAJ会員であればどなたでも歓迎しますので、ご都合がつく時に参加してみてください。

システム監査事例研究会は、主として次の２つの活動を実践しております。

いつも和やかな雰囲気の中、まじめにシステム監査の実践に取り組んでおります。SAAJ会員と同じ目的をもって共同作業を体験できる場でもあり、とても刺激的な研究会です。

尚、システム監査普及サービスを希望される企業・団体を、常時募集しておりますので、システム監査受診を希望されている企業、団体のご紹介あわせ宜しくお願いします。

1. システム監査普及サービス

このサービスはシステム監査を希望される企業・団体に対して、「システム監査の普及・啓発を図る」目的で実施しているものです。このため、監査にかかる報酬は無償とし、監査の実施に要した実費(通信交通費、調査費用、報告書作成費用等)のみのご負担で、被監査企業・団体の情報システムの問題点を洗い出し、解決へ向けてのアドバイスをいたします。

現在、すでに20社以上の実施実績があり、私どものシステム監査を受けられた会社は、その監査結果を有効に活用されています。

2. システム監査実務・実践セミナーの開催

このセミナーは「システム監査人の実務能力の維持・向上」のため、昨年からは４回／年開催しています。既に15回以上の開催実績があります。事例研究会で実施したシステム監査普及サービスの事例を教材として、実践で得たノウハウを会員の皆様と共有することを目標にしています。特に、システム監査技術者試験には合格したもののシステム監査を経験されていない会員の方には、システム監査の実際を短期間で体験する絶好の機会ではないでしょうか。このセミナーを受講してシステム監査の実際を体験し、システム監査能力の向上を図りましょう。

事例研究会の問い合わせ先：
三輪智哉　電子メール アドレス：t_miwa@st.rim.or.jp

掲載論文

ISMS認証制度とシステム監査

ーシステム監査の課題と提言ー

No. 1015
公認システム監査人　黒川　信弘

要　旨

コンピュータシステムが社会構造を下支えするインフラと化した現在、その信頼性の確保は喫緊の課題である。加えて、コンピュータウィルスの蔓延や不正アクセスの多発、ネットワークを活用したサイバー犯罪の急増なども社会不安を助長している。このような中、システム監査は情報セキュリティ監査と相まって、今後のコンピュータシステムの信頼性確保の切り札として多くの期待をされている。本稿では、ISMS認証取得の経験をベースにシステム監査の課題と提言をまとめる。

キーワード：ISMS認証制度、情報セキュリティ、情報セキュリティ監査、公認システム監査人

1. はじめに

2002年４月のみずほ銀行統合におけるシステムトラブルでは、口座振替の処理遅れ、ATM障害、二重引き落とし、振込みの遅延など、多くの顧客に対する影響と莫大な被害が発生した。その後も、金融機関での類似トラブルが多数発生している。また、2003年3月１日に東京航空交通管制部で発生したシステム障害は航空機の欠航や遅れによって約27万人に大きな影響を与えた。さらには厚生年金の220億円の未払いと24億円の過払いという前代未聞のトラブルも発覚したことは記憶に新しい。これらはいずれもコンピュータプログラムのバグが原因であり、十分なシステムテストを実施していなかったことが起因していると思われる。

コンピュータが生まれて半世紀が経った。当初、莫大な電力と広大な場所を取るコンピュータは、それが一体何に使えるのかさえ分からないような真空管のお化けであった。50年かけて僅か数ミリ角のチップに進化したコンピュータは、電気・水道・ガス・電話などのライフラインはもちろんのこと、交通、金融、流通、医療、製造など市民の社会生活から企業の基幹部分まで多くの分野で無くてはならない存在になってきている。既にコンピュータシステムは、それ無くしては社会生活が立ち行かないほどに市民生活の中に深く入り込み、社会経済や産業構造を下支えしているのである。

しかし、冒頭に紹介したように、その割には、それらコンピュータシステムの信頼性、安全性に関して無関心な部分が垣間見えてくるのは何故であろうか。本稿は、システム監査人としての視点から、重要な社会インフラとしてのコンピュータシステムの監査とはどうあるべきかを論じたものである。特に、昨今話題のISMS認証取得を完了した経験をもとに、実際の企業内の事業化システムに対する情報セキュリティの取り組みをベースに、システム監査、或いは情報セキュリティ監査についてその課題と方向性について提言する。

2. 現代社会の抱えるシステムの課題

ITの高度化とともに求められるシステムの機能も高度化、複雑化し、その実施タイミングも加速度的に高速化している。それに対応すべくシステムの企画・開発・運用の関係者も相当の努力をしているが、目まぐるしく進展するIT化の動きに人間の方が追従できていないようだ。求められる機能、アーキテクチャ、手法、スキル、マネジメントなどいろいろな視点における課題が浮き彫りになっている。しかし、一番の問題は、コンピュータシステムというものがこれほどまでに経済・産業構造を支えるインフラとして機能してきた現代において、多くの企業においては依然に技術課題としてしか認識されていないことではなかろうか。みずほ銀行の例も経営者はシステム統合に直接関わっていなかったと言う。システム依存度の高い金融機関でもそういう状況である。今後のコンピュータシステムは、経営課題として経営者自らが十分な経営資源を確保して先導して行かねばならない時代になったのである。

3. 情報セキュリティという新たな課題

インターネットというオープンなネットワークが国内に定着してから５年以上が過ぎた。既に多くのコンピュータシステムはオープンネットワーク対応に移行しており、それに伴ってまた新たな課題が噴出してきた。情報セキュリティの問題である。2003年１月末にはコンピュータウィルスによって韓国を中心に世界的

規模のネットワーク麻痺が発生した。不正アクセスによる重要なコンピュータシステムへの不正侵入も後をたたない。それに加えて最近では個人情報などの機密情報漏洩が大きな社会問題化しつつある。その上、コンピュータウィルスのために、ニューヨーク近郊の列車が止まったり、カナダの空港で旅客機が飛ばなくなったという現実社会での大きな被害が発生するようになった。コンピュータシステムには、既に述べた問題に加えてこのような新たな脅威が急増している時代である。

情報セキュリティとは、企業や個人の保有する貴重な情報資産を上記のようなリスクから守る機能である。筆者の所属する企業においても、ネットワークを活用する商品やサービス事業が多く存在し、顧客の信頼を勝ち得るためには情報セキュリティの機能を充実する必要に迫られている。当社の場合の情報資産とは以下のようなものである。(図1参照)

① 顧客から預かった情報
(機密情報、個人情報など)
② 当社のソリューション
(製品、システム、サービスなど)
③ 社内の基盤情報
(経営情報、技術情報、人事情報、情報環境・設備など)

これらの多様化した情報資産を機密性、完全性、可用性という観点からその健全性を確保することが情報セキュリティである。(図2参照)

このたび、当社内のネットワークサービス事業においてISMS認証[1]を取得した。筆者はその認証取得プロジェクトのリーダとして情報セキュリティマネジメントシステムの構築から運用、内部監査、ISMS審査など多くを経験した。以降にISMS認証取得の具体的な経験を交えてシステム監査を論じる。

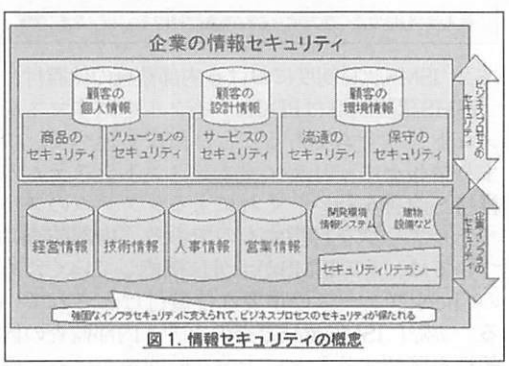


図1. 情報セキュリティの概念

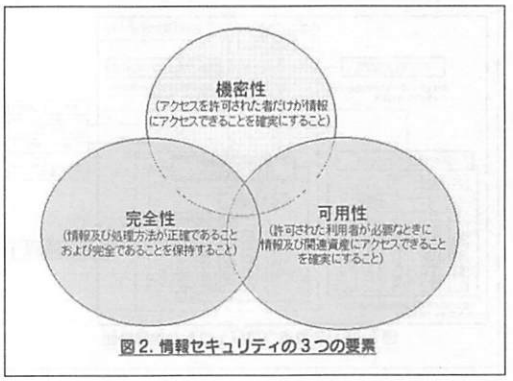


図2. 情報セキュリティの3つの要素

4. ISMS認証制度について

ISMSとは多種多様なセキュリティインシデントに対して体系的、網羅的な対策を実施するための組織的な取り組みを言う。所謂、PDCAサイクルをまわす情報セキュリティのためのマネジメントシステムである。JIPDEC[2]では、「個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスク評価により 必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用することである」[3]と定義している。

ISMS認証制度については、グローバルには英国規格のBS7799-2、日本国内ではJIPDECのISMS適合性評価制度が存在している。いずれも情報セキュリティマネジメントシステムの第三者評価制度であり、前者は全世界で420社以上、後者は国内で240社以上[4]の事業体が認証を取得している。

5. ISMS認証取得プロジェクト

当社ではネットワークサービス事業において、その多様な事業展開や拡大発展を期して顧客の信頼を獲得することを大目標とし、情報セキュリティの第三者評価制度であるISMS認証を取得する取り組みを実施した。2002年9月から開始したプロジェクトは2003年3月に無事認証取得を完了し、現在、そのISMSを順調に稼動させ、次の拡大展開を進めている。図3にISMS認証取得とその運営管理のための体制を示す。

[1] JIPDEC-ISMS V2.0 及びBS7799-2(2002)
[2] 日本情報処理開発協会　ISMS適合性評価制度の認定機関
[3] ISMS情報セキュリティマネジメントシステム適合性評価制度の概要(2002年4月)による
[4] 2003年11月時点

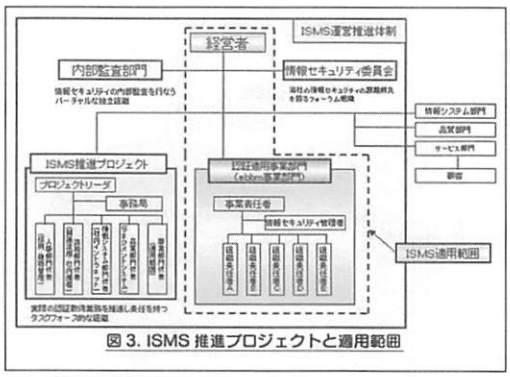


図3. ISMS推進プロジェクトと適用範囲

6. ISMS認証制度とシステム監査

6.1 ISMS認証制度におけるシステム監査の位置付け

ISMS認証基準V2.0では、第6の4項に内部監査の要求事項があり、その中に「②識別した情報セキュリティ要求事項に適合していること」という条項がある。また、付属書の詳細管理策の12(3)に、システム監査の考慮事項がある。これら内部監査とシステム監査の関係は必ずしも明確とは言えない。ISMSの構築と運用においては、情報セキュリティ監査とシステム監査の両方を要求しているようにも受け取れる。

因みに、昭和60年1月に制定されたシステム監査基準は、以下のような対策[4]が基本になっている。

① 自然災害対策・・・
耐火・耐震構造、消火設備等
② システム障害対策・・・
回線二重化、システム二重化、バックアップ等
③ 防犯対策・・・
アクセスコントロール機能、入退室管理、端末識別機能等

一方、平成7年に制定されたBS7799をベースにしたISMS認証基準の詳細管理策[3]は次のようになっている。

① 情報セキュリティ基本方針
② 組織のセキュリティ・・・
インフラ・第三者アクセス・第三者委託
③ 情報資産の分類／管理・・・
情報資産の責任と分類
④ 人的セキュリティ・・・
職務定義・教育訓練・事故誤動作への対処
⑤ 物理的／環境的セキュリティ・・・
区画・装置・管理策
⑥ 通信／運用管理・・・
運用手順・システム計画・不正ソフトウェア・情報システム管理・ネットワーク管理・媒体管理・組織間の交換
⑦ アクセス制御・・・
ネットワーク／OS／アプリのアクセス制御・監視・モバイル
⑧ システムの開発／メンテナンス・・・
アプリケーション・暗号・ファイル・開発サポートプロセス
⑨ 事業継続管理
⑩ 適合性・・・
法的要求事項への適合・セキュリティポリシー準拠・システム監査

システム監査基準は物理的な対策を重視しており、ISMS認証基準はネットワーク面、人的側面をより強化した基準になっている。もともと監査する観点が異なるものではあるが、ISMSの構築から運用を進めるにあたって、情報セキュリティ監査とシステム監査の相違や位置付けが不明確になっているのは混乱を招くもとである。恐らく内部監査はISMS認証基準の適合度を確認するものであるから、機密性・完全性・可用性という観点からの情報セキュリティ監査を行うことになろう。一方、ISMS要求事項の一つとして安全性・信頼性・効率性の観点から適用範囲の対象業務監査を行うことがシステム監査の役割であろう。ここでは、システム監査は、ISMS構築・運用のための一要求機能なのである。それらの関係を図4に示す。

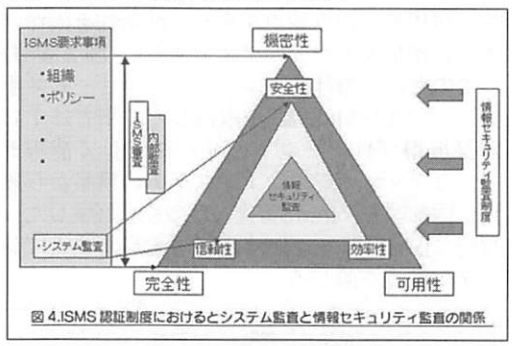


図4.ISMS認証制度におけるとシステム監査と情報セキュリティ監査の関係

6.2 ISMS認証制度における内部監査の位置付け

ISMS認証制度はPDCAサイクルを回すマネジメントシステムであることは前にも述べた。つまり情報セキュリティマネジメントシステムの維持・改善を行い、それによるシステムのスパイラルアップを目指すものである。内部監査については、そのISMSが十分に機能していくためのCheckフェーズの重要な位置付けとされている。実際にISMS認証審査の中でも内部監査の信頼性を確認することに十分な時間をかける。確認されるのは次のような点である。

① 監査体制(監査人の能力・育成のための教育や資格・独立性)
② 監査範囲
③ 監査頻度
④ 監査目的と監査方法
⑤ 監査結果報告
⑥ 是正処置

ISMSが継続的に維持・改善され、組織にとって有効なシステムとして機能していくためには、内部監査の能力が十分であることが必要となる。

6.3 情報セキュリティ監査とシステム監査

一般的にシステム監査は、安全性・信頼性・効率性という観点からシステムの監査を行う。安全性とは機密性・正確性・適時性・準拠性、信頼性とは正確性・適時性・準拠性、効率性とは、採算性・生産性というシステムの評価指標と関連する。その安全性の部分が、情報セキュリティ監査として特だしになったという理解もある。つまり機密性・完全性・可用性という観点から監査を行う情報セキュリティ監査である。特に完全性をブレークダウンすれば、正確性・網羅性・正当性・妥当性・整合性・適時性・認証性(証拠性)・一貫性・準拠性という評価観点になる。(図5参照)

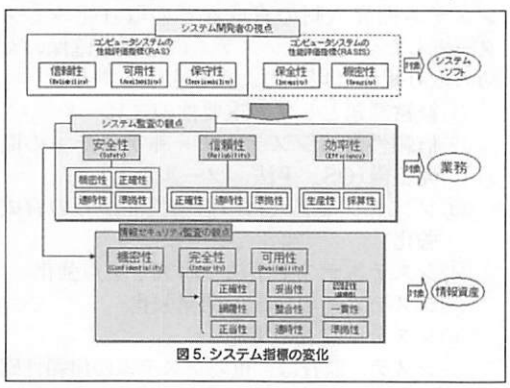


図5. システム指標の変化

社会生活がネットワーク化され、コンピュータシステムがインフラとして社会構造を下支えする状況になり、システム監査の観点も変わっていく必要がある。それは有効性、信頼性、安全性である。有効性とは、システムの目的適合度を言い、目的に対する成果の達成度である。(表1参照)

市民生活を支えるシステムは、その有効性を最も求められるべきである。その中には効果性、効率性の観点が盛り込まれる。次に信頼性、そして安全性の観点が重要になる。今後、システム監査の視点は、図6.のように有効性を中心に、信頼性、安全性を確認するものに変貌する。

表1. システムの種類と目的

システムの種類	応用分野	目的	システムの評価観点
経営支援・技術支援システム (意思決定支援／経営支援／設計支援)	企業	経営資源	有効性(効果性、効率性、準拠性) 安全性(機密性、正確性、適時性、準拠性) 信頼性
業務システム (会計管理／納買管理／販売管理／在庫管理／給与計算)	企業	組織内の 機能業務の効率化	有効性(効果性、効率性、準拠性) 安全性(機密性、正確性、適時性、準拠性) 信頼性
制御／監視システム (機器コントロール監視／ライン管理／対象物管理監視)	工場、交通、通信 ライフライン	適正な制御	有効性(効果性、効率性) 信頼性(正確性) 安全性(完全性、可用性)
科学技術計算システム (計算／データ管理／データ分析)	気象、設計 シュミレーション	正しい結果	有効性(効果性) 信頼性(正確性、適時性) 安全性(機密性、完全性)
オンラインシステム (銀行ATM／座席予約／オンデマンド)	銀行ATM、鉄道 ホテル、CATV	正しく早い要求対応 (適正な顧客サービス)	有効性(効果性、効率性) 信頼性(正確性、適時性) 安全性(機密性、完全性、可用性)
決済システム	金融機関	迅速で正しい決済	有効性(効率性、準拠性) 信頼性(正確性、適時制) 安全性(機密性、完全性、可用性)
情報提供システム	自治体、企業	正しい提供	有効性(効果性、効率性) 信頼性(正確性、適時性)

安全性については情報セキュリティ監査の一環で確認できる部分が多い。

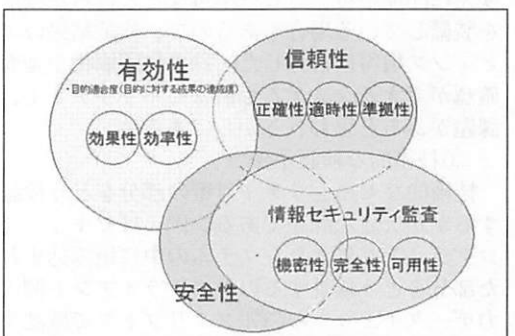


図6. 新たなシステム監査の視点

6.4 内部監査の実施状況とその課題

ISMS構築と運用開始の中で内部監査を実施した。ISMS構築直後の内部監査は、監査員3名でトータル3日間実施した。監査対象は、認証適用範囲部門とISMS推進プロジェクトの大きく2部門であり、全部で11の組織に及んだ。7人の責任者へのヒアリングと現場視察及びエビデンス確認を実施した。機密性、完全性、可用性の観点から監査を実施した結果、13件の不適合と15件のオブザベイションを指摘した。不適合事項の大半は、文書類の作成不備と規程類の職場への徹底不足と言う内容であった。

その2ケ月後、内部監査のフォローアップ監査を延べ2日間実施したが、新たに構築されたISMSが適切に運用され始めたようで、不適合事項13件のうち1件のみは再フォローアップが必要となったが、残り12件は是正処置実施の確認ができた。

以上のように当社としても初めての情報セキュリティ監査を実施して、以下のような多少の混乱が発生した。

①外部委託業者への監査

例えば最近主流のシステム運用スタイルであ

るiDC[5]へのアウトソーシングを実施している場合、外部委託業者への監査をどう進めるべきであろうか。経営視点が異なる組織体であるから委託側の手前勝手な押し付けもできないであろう。委託業者との契約書の内容確認だけでは不十分であるが、どこまで外部企業に委託側のISMSの役割を求められるのかが課題である。ISMS構築を理由に新たな関係構築の契機とすることも可能ではある。

②エビデンスの確保

上記のような場合のエビデンスをどう確保するかが課題である。iDCの運用基準や実体の証拠を確認することに困難な部分が存在する。

他にも機密情報の管理などにおいて、秘匿性ゆえに印刷不可、コピー不可などと言った機能を装備している場合もあるので、検証結果のエビデンス取得に苦労した。殊更に印刷物や画面確認ができるシステムも情報セキュリティ上、課題があると思われるからである。

③技術的な検証手法

技術的なセキュリティ対策の部分をどう検証するかが大きな課題である。例えばセキュアプログラミングによりシステムの中に組み込まれた部分をどう検証するのか。クライアント側入力データチェックのCGI[6]スクリプトまで確認するのか。そこまでの技術や知識ノウハウを監査人全員が保有することはほぼ不可能に近いと思える。当然、そのようなケースでは、適切な人材を確保して対策細部を検証することになるが、そうすると内部監査に関するコストもかなりのものになる。

④監査ツール

セキュリティ対策を実施した結果の検証において、サーバ類の脆弱性検査などを実施することがある。そのようなケースでは、市場にある脆弱性検査ツールなどを活用することになるが、これにも多くの課題がある。ISMS詳細管理策にも記述されているが、検査対象以外への悪影響を無くすためにネットワークの切り離しや、独立したネットワークでの検証、或いはIPアドレスの付け替え、ファイアウォール越しでの模擬攻撃など、手間とコストのかかる監査ツールをどう使いこなすかも今後の監査における大きな課題である。

7.システム監査の課題とシステム監査人の役割

7.1 システム監査のニーズ

会計監査などに比べるとシステム監査は一般企業の中ではほとんど実施されて来なかったに等しい。日本国内でシステム監査を受けている企業は20%にとどまり、地方自治体では4.7%にすぎない[7]というデータがある。経済産業省の情報処理技術者試験でもシステム監査技術者を4500人ほど輩出してはきたが、恐らく合格者の大半はシステム監査業務を実際に経験していないに違いない。それだけ日本社会はシステム監査業務が必要ないほど安全で万全？なシステム基盤に支えられた社会であったと言えよう。[5)]

しかし、冒頭に記したようにもはやそのような安全な社会はどこかへ消え去り、凶悪犯罪の多発、外国人や少年犯罪の急増、地震や異常気象などによる自然災害の続発、医療事故の多発、テロの恐怖や不景気のための失業率UPによる社会不安の蔓延など様々なリスクに満ちた社会となりつつある。そのような中で、北米で発生した大規模停電騒ぎやインターネット経由でのサイバー犯罪の多発などが重なり、システムの高度な信頼性を求める声が高まって来ている。

その解決策としてソフトウェア開発工程の標準化など信頼性の高いアーキテクチャの開発やシステム開発人材の育成などの取り組みもスタートした。それらシステムの信頼性確保のための取り組みは以下のようなものがある。

①経営課題としての重要性のアピール
②信頼性あるシステムアーキテクチャの開発整備(OS，手法、ツールなど)
③ソフトウェア人材の信頼性面からの育成強化
④システムテスト手法の研究と重点強化
⑤システム運用技術の開発強化
⑥システム監査の実施

システム監査は、重要システムの信頼性確保の手法として社会から嘱望されている。

[5] Internet Data Center　顧客のサーバを預かって顧客に必要なネットワーク運用サービスを提供する設備

[6] Common Gateway Interface: WWWサーバとサーバ上で動く他のプログラムやスクリプトとのインターフェース

[7] 日本経済新聞2002.8.16による

7.2 システム監査の課題

米国企業のエンロンやワールドコムにおける粉飾決算に見られる会計監査の問題が指摘されて監査法人業界の再編は世界的規模に至っている。日本国内でも、三菱自動車のリコール隠し、東京電力の原子力発電所トラブル隠し、三井物産の不正入札事件、雪印の集団食中毒事件と牛肉偽装事件、日本ハムの牛肉偽装事件などトラブル隠しやリスク対応不備など多くの企業で不祥事が発生している。その結果、企業のコンプライアンス(法令遵守)とアカウンタビリティ(説明責任)重視の経営と言う透明性確保の取り組みは急ピッチで進んでいる。そのような状況の中で監査という機能に社会的な熱い目が集まっているのも確かである。もはや経営インフラと化したコンピュータシステムの信頼性確保のためのシステム監査は益々その重要性を増しており、システム監査という機能への社会的要求も大きくなりつつある。ただ、制定から20年になろうとしているシステム監査基準について見直しの時期に差し掛かっているのも事実である。システム監査が日本社会に根付いて来なかった理由として以下のようなものが考えられる。

①システム監査をしなくても問題は発生していない
・忙しくてシステム監査どころではない
②システム監査の効果が分からない
・誰が監査できるのか？
・どんな基準で監査するのか？
・監査が企業成果にどう結びつくのか？
③曖昧さを好む日本社会
・欧米型契約社会と異なる同質の世界

7.3 公認システム監査人の役割

前項のシステム監査の課題に対して、公認システム監査人が率先して実施すべきことを以降に提言する。

① 監査事例のアピール

監査側からの社会への強烈なメッセージアピールが欲しい。言い換えればシステム監査事例のPRである。監査をした結果、健全性を保ち危機を脱した企業事例を積極的に公表する努力が要る。そのためのいろいろ課題はあるにしても、システム監査の効用を社会は知りたがっている。

② 監査人のスキルアップ

監査人の資格としては、国家資格である情報処理試験のシステム監査技術者、及び公認システム監査人や公認情報システム監査人(CISA)などが存在する。しかし、これ以上多くの資格を作っても市場は混乱するばかりである。今後は、これらの人材のさらなるスキルアップを強力に推し進めるべきである。監査人としてのオフィシャル教育を定期的に受けるなどの施策が必要ではないだろうか。

また、情報セキュリティ面の監査スキルも修得する必要がある。特に、ISMS認証基準に示されている要求事項については公認システム監査人も具体的に修得すべきである。また、技術面、法規面、管理面、モラル面など情報セキュリティ特有の領域については、それらのスキルを保有するに越したことは無いが、それぞれ専門の人材を有効に活用するスキルを保持することが肝要である。

③ 新たなシステム監査基準作り

関係諸団体で新たな社会情勢の要望に応えられるように、次代に向けての新たなシステム監査基準作りを既に進めている。今後は、図6.に示したような新たな監査視点が必要と考える。監査という特性上、権威なり基準と言うものが必要であるので、行政とも連携して社会的な枠組みやルールの構築と実績作りが重要である。

④ 情報セキュリティ監査との共存共栄

2003年4月より経済産業省は情報セキュリティ監査制度を開始した。電子情報の管理体制強化のため国際ルールに従った監査の統一基準を作成し、新たな情報セキュリティ監査制度として運用を開始したのである。この統一基準のもとでの監査を中央省庁に義務付けるとともに、地方自治体や企業にも監査実施を促していくようである。ISMS認証制度を立ち上げたばかりなので両者の関係が不明確な感じがするが、相乗効果を発揮してシステムの信頼性向上に役立てばこの上ないことである。

8. おわりに

コンピュータウィルスや不正侵入など派手なインシデントが急増しているため情報セキュリティがクローズアップされているが、本質的には情報セキュリティ監査もシステム監査の一部である。ただ、現在のシステム監査基準は若干時代に即していない部分があるので、前記の提言のような新たな衣替えをして、信頼の置けるコンピュータシステム創出に向けて社会貢献を実践して行きたい。

既に米国では情報セキュリティ監査基準が民間ベースで整備されており、一般の多くの企業が年に一回の監査を受けている状況である。また、システム監査を実施する監査人としても、IT系以外の領域から弁護士、公認会計士、中小企業診断士、日本経営品質賞審査員などがシステム市場にも進出してきている。加えて、IT系

のシステム監査技術者、公認情報システム監査人、公認システム監査人、BS7799リードオーディタ、ISMS審査員などもシステム監査人としての従来に優る活躍を始めており多種多彩な人材が揃いつつある。こういった面からもシステム監査市場が今後ますます活況を呈してくると思える。

本稿では、筆者が経験したISMS認証取得の事例を交え、システム監査の課題提起と新たな提言を行った。既にシステム監査は研究的・実験的な位置付けを過ぎ、社会に役立つ実践的・実証的なフェーズにある。その効果や貢献度を社会へアピールするために日本システム監査人協会の活動が存在するとも言える。今後とも切磋琢磨して我々システム監査人の存在価値を高めることにも貢献して行きたい。

＜参考文献＞

1) (財)日本情報処理開発協会 「ISMS情報セキュリティマネジメントシステム適合性評価制度 －ISMS認証基準(V2.0)－」(平成15年4月21日)
2) British Standards Institution「Information security management system -Specification with guidance for use」(2002.9.5)
3) (財)日本情報処理開発協会「ISMSガイドV1.0」(平成14年4月1日)
4) 通商産業省「システム監査基準」昭和60年1月、平成8年1月改訂
5) 黒川信弘 「月刊セキュリティ研究」(SRIセキュリティ総合研究所)2003年8月号 p44,45

黒川信弘
パナソニック システムソリューションズ社
技術士(情報工学、総合技術監理)
情報セキュリティアドミニストレータ
ISMS審査員／システム監査技術者
kurokawa.nobuhiro@jp.panasonic.com

三支部(近畿・中部・北信越)合同研究会

研究会プログラム

No.947 梶川 明美

1. 日 時：10月4日(土)～5日(日)
2. 日 程：

第一部 セミナー(敦賀短大教室)

北信越支部長 挨拶
東京本部理事 挨拶
セミナー1
「ユビキタス社会における個別マーケティングと必要なシステム監査」
北信越支部会員・敦賀短期大学 経営学科
教授 黒目 哲児氏
セミナー2
「個人情報保護に関する制度の現状と今後の課題」
近畿会会員・システムアナリスト協会長
清水 順夫氏
セミナー3
「個人情報保護の取り組みや、その教育の考え方(告発文化を創らないこと＝責務を認識すること)」
リコーシステム開発株式会社
事業戦略室技術推進グループ
吉川 博晴氏 技術士(情報工学)
中部支部長 挨拶

第二部 懇親会(民宿"はまと")

自由討議と懇談

第三部 見学会(若狭路博会場)

セミナー１講演録

No.978　北信越支部
森田　清隆

テーマ：ユビキタス社会における個別マーケティングと必要なシステム監査
講　師：北信越支部会員・敦賀短期大学
経営学科教授　黒目哲児氏

＜概説＞

ユビキタスという言葉をよく耳にするようになった。ユビキタスの技術により、便利に快適に安全に過ごすことが出来るようになる。その中で、ユビキタス社会における個別マーケティングでは、従来では考えられない程多くの個人情報を入手することが出来るようになるため、きわめて細かい個別マーケティングが出来るようになる。その反面、プライバシーとのかね合いなどの種々の問題が発生する。このユビキタス社会において、いかにシステム監査するかを論じる。

＜ユビキタス社会＞

ユビキタスとはあまねく存在することであり、「遍在」である。従来のコンピュータは、ある場所に固まって存在する「偏在」であった。ユビキタスという言葉を提唱したのは、1988年ゼロックス社のマクワイザ博士で神があらゆる場所に存在するという意味のラテン語が元である。1984年に東大の坂村健氏がトロンの中で超機能分散システムという言葉で概念を提唱している。現在はユビキタスという言葉が通用している。

ユビキタス社会の条件は、

・コンピュータ同士がネットワークにつながれ互いにコミュニケーションできる
・人はコンピュータの存在を意識しないでコンピュータの恩恵にあずかることが出来る
・コンピュータはその相手または状況に応じその都度違う対応をする

の３つであり、ユビキタス社会における必要な技術は

・ネットワーク：近距離間無線技術、常時接続ブロードバンド技術、IPv６
・コンピュータ：マイクロコンピュータ、多様なセンサー、アクチュエーター
・それらを使いこなすコンテンツ：対応、状況に応じた判断行為、ナレッジマネジメント的学習機能

の３つである。まとめると、ユビキタス社会では「多様なネットワーク技術で結ばれた、多様なコンピュータの間を、多様な形式の情報が行き来することにより、多様な処理やサービスがおこなわれる」。

＜個人情報との関連＞

ユビキタス社会では個人は無意識のうちに観測され、その情報は大量に保存されている。そして黙っていてもこちらの状況に合わせて情報が与えられるようになる。ユビキタス社会は、介護サービスやホームセキュリティ等の安全性の追求、時間節約や提案サービス利用による快適性の追求、消費者と一体になった商品開発やサービス企画等の知的情報の共有の結果もたらされる価値創造を目指している。その個別対応のレベルを決める要素としては、情報を受発信するオブジェクトの性格とその時点での状況、おかれている場所と環境、要求するサービスのレベルがある。

サービスレベルとしては、1.情報交換、2.モニタリング、情報検索、3.必要時情報発信、4.解決策の提案、5.解決策の実施、の５段階がある。

＜個別マーケティングに与える影響＞

従来ある過去一時点での静的な属性情報を持っていたが、これは第一段階。第二段階は複数の過去時点での履歴情報が加わったデータウェアハウス技術へ発展する。第三段階はユビキタスコンピューティング技術により、個人の連続した履歴情報と個人を取り巻く連続した環境情報を得ることが出来るようになる。ユビキタス社会ではこの情報を活用していくことになる。ユビキタス社会における個人情報の活用としては、

・個人情報が時間と環境の要素とともに連続的に収集できることから、現時点での実際の情報に基づく最適提案をおこなう
・個人情報を取り巻く環境情報が共有できることから、共通の環境情報により結びつけられたコミュニティを形成する

ことがある。

大量の個人情報を得られるため、企業側のサービスが過剰になり、かえって拒否反応を引き起こすおそれがある。併せて個人情報の一人歩きへの不安を招くようになる。より便利に、

より親切に、が可能になると同時に、より危険に、より過剰になっていくこともあり得る。対応としては、パーミッションマーケティングを前提とした、個人を主体とした控えめな「コンシェルジュサービス」が必要である。

<ユビキタス社会におけるシステム監査>

現在に至る技術の延長線上でおこなって行くべきものであるが、ユビキタス社会の技術の方向性が明確でないことが、必要な監査のあり方を不明確にしている。ユビキタス社会におけるシステム監査の特徴としては、次のポイントが考えられる。

1. 特異性
   - ・個人をありのまま再現できる時間的、物理的な環境情報を含んだ個人情報が対象であること。
   - ・膨大な数のコンピュータからなるオープンシステムがその基盤であること
2. 個人情報の安全性確保
3. 顧客対応
   - ・個人情報を収集する段階における必要な対応
   - ・個人情報を利用する段階における必要な対応
4. 新情報技術利用に対するシステム監査
   - ・ネットワーク技術におけるシステム監査の特異性
   - ・データベース管理技術におけるシステム監査の特異性

<まとめ>

ユビキタス社会におけるマーケティングは、個人に対するさりげないサービスの提供であり、これは膨大な個人情報を無償で企業に提供している消費者の正当な権利である。ユビキタス社会の個別マーケティングに対するシステム監査視点としては、個人の権利をいかに守るかということと、いかに行き届いたサービスを提供できるかということにある。

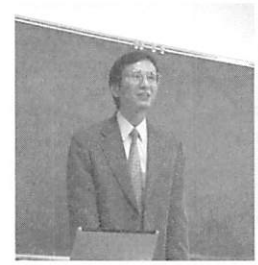
通信販売における個別マーケティングへの適用を例として挙げたりしていただき、わかりやすく興味のもてる内容でした。

セミナー2　講演録

No.765　北信越支部
笹岡　晴雄

テーマ：個人情報保護に関する制度の現状と今後の課題

講　師：近畿支部会員
システムアナリスト協会会長
清水順夫氏



（1）講師自己紹介

（2）なぜ個人情報保護がテーマとなる理由
住基ネットの稼動、個人情報保護法の成立に加え、個人情報の漏洩事件が相次でいる。しかし、一般的な傾向として個人情報保護に関する関心は低すぎるという危機感がある。

（3）新個人情報保護法が制定されるまでの経緯

1970　国民総背番号制→反対により中止
1980　OECDプライバシーガイドライン
→その意義について再認識
1988　旧新個人情報保護法(行政機関対象)
1998　プライバシーマーク制度
1999　JIS Q 15001
宇治市住民基本台帳データ漏洩事件
1999　住基ネット法案提出
2003　個人情報保護関連5法成立

（4）海外の個人情報保護法
欧州は1970年代から個人情報保護に関する法律が存在していた。背景として、行政情報のデータ化が行なわれていたようである。

1973　スウェーデン　データ法
1977　旧西ドイツ　連邦データ保護法
1978　フランス　データ処理・データファイルおよび個人の自由に関する法律
ノルウェー、オーストリア

これらは公的部門だけでなく、民間部門も規制対象であった。

（5）OECDプライバシーガイドライン8つの原則
OECDガイドラインでは以下の8つの原則を

定めている。

1. 収集制限の原則、2. データ内容の原則、3. 目的明確化の原則、4. 利用制限の原則、5. 安全保護の原則、6. 公開の原則、7. 個人参加の原則、8. 責任の原則

しかし、なぜ、経済協力機構が個人情報保護について定めようとするのか。

(6) OECDのプライバシーガイドライン

ガイドラインの目的は以下の通り。

プライバシーと個人の自由を保護／プライバシーと情報の流通を調和／経済的社会的関係の発展に対する不当な障害を回避

つまり、個人のプライバシーを守るとともに、個人情報が経済活動に適切に活用されるようにルール作りをしている。これが経済協力機構が個人情報保護について関わる理由。

(7) 各国の法制度の特徴

EU→公的部門と民間部門を包括。

米国→公的部門のみ包括して規制→民間は必要に応じ個別の法律により規制

日本→2003年の新法以前は公的部門のみ包括して規制。民間は条例もしくは自主規制。

セキュリティにおいて日本は後進国であるという認識である。

(8) 新個人情報保護法での変化

新法以前との大きな相違点は以下の通り。

基本方針を法律で明示(専門的には基本法と一般法が一緒になっているといえる)公的部門と民間部門ともに法制化された。

(9) 新個人情報保護法制定の難航

1999年に検討開始。住基ネット稼動までに整備されるはずが難航した。取材や報道の自由と相反する面があること、「個人情報」が示す範囲が広いことが難航した理由と考えられる。

(10) 個人情報の定義

個人情報保護法による定義では個人の住所録ですら規制の対象となりかねない。

(11) 過剰規制とならないための対処

目的を明示、規制対象をレベル分け、「個人情報取扱事業者」が対象。報道、著述、学術、宗教、政治に関しては適用除外とした。

(12) 個人情報のレベル分け

個人情報、個人データ、保有個人データ

(13) 個人情報保護法の構成

第1章 総則
第2章 国および地方公共団体の責務
第3章 個人情報の保護に関する施策等
第4章 個人情報取扱事業者の義務
第5章 雑則
第6章 罰則
附 則

(14) 個人情報取扱事業者の義務

個人情報→利用目的の特定、目的による制限、適正な取得、利用目的の通知

個人データ→個人情報の項目に加え、正確性の確保、安全管理措置、従業者の監督、第三者提供の制限

保有個人データ→個人情報の項目に加え、保有個人データに関する事項の公表などの措置、開示、訂正などの措置、利用停止

(15) OECD 8原則との対応

[OECD 8原則]	[個人情報保護法]
目的明確化、利用制限の原則	15、16、23条
収集制限の原則	17条
データ内容の原則	19条
安全保護の原則	20、21、22条
公開の原則	18、24、25、26、27条
責任の原則	31条

(16) 個人情報保護に関する課題

(以下、講師の私見)

基本法として制定されたこと、民間まで包括した法制という点では前進したが課題は多い。

1. 保護法の解釈上の問題→スペシャリスト、研究者に期待
2. そもそも法律は事態の後追い→民間の認証制度も活用できる
3. 住基ネットの脆弱性への対処→システム監査の出番と言える。
4. 団体や企業の認識不足
5. ネットワーク上での個人情報の氾濫→オープンなセミナーを通して企業、個人の啓蒙活動を行なうのが望ましい。

セミナー3　講演録

No.808　中部支部
若原　達郎

テーマ：個人情報保護の取組みと教育について
副　題：告発文化を創らない
講　師：リコーシステム開発株式会社
　　技術士(情報工学)吉川博晴氏

01年度に「プライバシーマーク制度」取得を行ったリコーシステム開発株式会社様での具体的な取組みをご紹介いただいた。

＜講演要旨＞

1. 推進に当たって悩んだこと

今回教育担当としてプライバシーマーク取得活動を推進するに際しての考慮点は以下のとおり。

（1）どこまでが個人情報だ？
例えば名刺について、名前だけでも個人情報なのかどうか、電子メールアドレスはどうか等、悩みながら線引きをしてグレーゾーンをなくしていった。

（2）どこまでやればいいの？
個人情報保護には膨大なコストが必要といわれるが、会社として身の丈にあったセキュリティ対応を構築すればよい。人の手を介して済むものは済ませ、社員教育で補えるものは補う。社員の意識向上につなげることがポイント。

（3）仕組みだけでは100%防ぐことは無理なのでは？
罰則規定による牽制もあるが、不正を働こうとすればいくらでも出来るし、事件の多くが内部犯罪である。最終的には個人のモラルであると考え、社会的な責務を果たす必要性を教育で実施した。

2. 留意したこと、実施したこと

具体的に実施した施策は以下のとおり。

・入退室管理(カードキーで開錠)
・清掃業者、廃棄業者との機密保持契約
・PC管理の徹底
・バックアップデータの遠隔地保管
・情報の共有化(Notes DBの活用)

PC管理の徹底とともにそれまでフロアに散在していたサーバを、専用スペースを設定して集約し、さらにその周辺からコピー機や打合わせスペースを排除して、理由もなく近づけないような状況を作り出した。

また会議室のネットワークソケットやノートPCには施錠する、倉庫や机のメディアを廃棄して整理する等、「監視の死角をなくす」観点から施策を実施している。

3. 現場の不満と教育方針

具体的な施策の実施に際して出てきた現場の不満に対し、以下のように対応した。

（1）能書きはいいからマニュアルにしろよ
「書いてないことはやらなくてよいのか」という観点で教育と運用にあたった。あくまで自分の問題として捉え、マニュアルは参考の位置づけにするといった姿勢を奨励した。

（2）こんなに多くをやるんじゃ、やってられない
「社会人として当然あるべきスキルであり、具体的な判断は現場で行わなければならない」という意識付けを行った。実際、運用が回りだすと当たり前になってしまうものだ。

4. 告発ではなく事件防止へ

最近、内部告発事件も出ているが、「告発」は信頼関係の瓦解であり最終手段である。

プライバシーマークはじめ、コンプライアンス経営の目指すところは、意見が通り改善が常に行われ、改めて告発するまでもないマネジメント体制へ至ることである。個人情報は至るところにあり、人にはミスがつきものである。ソフトウェアのバグ摘出と同様に、事件の予防を仕組みで改善することが重要である。

5. 質疑応答：事故発生時の処罰は？

事件が軽微ということもあるが、事故を起こした本人を責めるのではなく、その原因を考えさせる指導を行い、同時にルールなどを含めた改善の実施を行っている。現行の仕組みにも不備はあるからだ。

三支部合同研究会を開催、参加して

支部長感想

No.848　北信越支部長　森　広志

三支部合同研究会は、北信越支部設立時に提案があり、三支部役員の皆様方からも熱心な賛成がありました。皆さまの賛成と協力があれ

ば、大方の行事は実現できると考えています。三支部合同研究会が開催された福井県敦賀市は、三支部の地理的な中心地で、特に今年は若狭路博という大きな地元イベントの開催時期に合わせた実施となりました。

今回の研究会は、特に地元福井県の黒目教授に大変なご尽力を頂き、敦賀短期大学の教室、地元の民宿やバスもチャータ頂く等、手厚い配慮に頭が下がる思いでした。又、今回の研究会は、福井県商工会議所連合会の後援を賜ると共に、ITコーディネータ協会のITCA後援セミナー認定を受けました。特に当日は、SAAJ本部より鈴木理事にお越し頂き、ご挨拶頂くとともに三支部合同研究会を盛上げて頂きました。講演概要を述べると、

① 個人情報履歴(ユビキタス情報)により親切でさりげない個別マーケティングにより、高度の顧客満足を実現できる。(黒目講師)

② 個人情報保護法は良く考えられているが、セキュリティ対策面の濃淡があり研究・解明の必要がある。又、一般の方にも個人情報保護法を知らしめてゆくことが大切。(清水講師)

③ 個人情報保護の実務面ではマニュアルに頼らず個人情報を各人がコントロールできるスキルを持つことが大切、告発ではなく、転ばぬ先の杖体質を作る。(吉川講師)

以上簡単に纏めてみましたが、図らずも講演順番の上下連携が取れ、理解しやすかったと考えています。続く懇親会では、黒目教授にお手配頂いた評判の民宿で、海の幸を囲み、夜遅くまで議論が尽きませんでした。翌日は、若狭路博見学でしたが私は残念ながら所用があり早朝出立しました。朝日が差し込んだ三方五湖、初めて乗った小浜線の列車、最後まで思い出深い三支部合同研究会でした。今回の開催にあたり、ご準備お世話頂いた全ての皆様方に改めて御礼申し上げます。

No.47 近畿支部長 石島 隆

10月4日、5日の両日にわたり、北信越支部、中部支部及び近畿支部の三支部合同研究会が、福井県敦賀市で開催されました。まず、はじめに、開催にご尽力いただいた北信越支部の皆様、遠方からご参加いただいた鈴木信夫理事、中部支部及び近畿支部の参加者の皆様に厚く御礼申し上げます。

今回の合同研究会の企画は、1日目に午後から研究会を行い、夜は懇親会、2日目は若狭博覧会を見学するものでした。北信越支部の黒目哲児会員、梶川明美会員らのご尽力により、短期間に実現の運びとなったものです。

研究会のテーマは、「個人情報」であり、黒目哲児会員からは個人情報のマーケティングへの活用の観点から、清水順夫会員(近畿支部)からは個人情報保護法、ゲストスピーカーの吉川博晴様(リコーシステム開発㈱)からは企業における個人情報保護の具体的な取組みについてご講演いただき、さまざまな観点から「個人情報」を考えることができました。

黒目哲児会員の講演では、ユビキタス社会のマーケティングのあり方として「コンシェルジェ・サービス」のご提言がありました。これは、ヨーロッパの高級ホテルのコンシェルジェのように、顧客のニーズを掴んでさりげないアドバイスをすべきであるというもので、ともすれば監視社会となる可能性もあるユビキタス社会におけるプライバシーとビジネスとの調和を考えた注目すべきご提言であると感じました。

次に、清水順夫会員の講演では、わが国及び海外の個人情報保護に関する法制度の経緯から紐解いた上で、この度成立した個人情報保護関連5法に関して主要な論点を解説していただきました。OECD8原則のビジネス上の背景など、基本から学ぶことの大切さを再認識しました。

さらに、吉川博晴様の講演では、リコーシステム開発㈱様の社内での個人情報保護に関する取組みについて、実際に推進事務局を担当されているご経験に基づいて、具体的な悩みと解決策について、実例を用いて解説され、粘り強い努力によって改善を図られている様子に感銘を受けました。ホイッスルブローイング(内部告発)が叫ばれている昨今ですが、「告発ではなく事故防止へ」という、日本企業の文化を生かす取組みが印象的でした。

このように、バランスのとれた講演テーマの構成であり、時宜を得た有意義な研究会であったと思います。

夜は、風光明媚で知られる三方五湖の湖岸近くの民宿に泊まって懇親会を開催しました。魚や蟹の料理に舌鼓を打ち、お酒をいただくにつれて盛り上がり、ついには、三支部合同研究会を三支部の輪番で毎年行う方針も確認されました。来年は近畿支部担当で秋の京都にて、再来年は中部支部担当で「愛・地球博」会場の近くにて開催という計画です。

今後とも、人と人とのつながりを大切にして、思いやりのあるネットワーク作りをしていきたいと考えております。関係者の皆様、ありがとうございました。

NO.339 中部支部長 山崎 拓

北信越支部・東北支部の設立、今回の研究会と2003年は、協会にとって、東京だけでなく、地方の活動も充実してきた年となったと思います。情報技術は、東京への一極集中であるとよく言われています。当協会においても同様で、本部の研究会は、毎月充実した内容で行われておりますし、各種活動も活発です。しかし、我々地方在住の支部会員にとっては、本部の研究会は、東京出張に合わせて参加するのが、精々です。そこで、各支部では、月例会などを行っています。中部支部においても、隔月で例会を実施していますが、支部会員各位からの情報提供、情報交換に留まっているのが、現状です。このような状況下、今回の三支部合同の研究会を開催できたことは、画期的なことだと思います。支部合同の研究会は初の試みであり、大げさかもしれませんが、歴史的にみて、記念すべき研究会であったと考えます。

今回の研究会は、2003年6月の北信越支部設立記念総会において、合同の研究会の開催を三支部の幹部が合意したことが契機です。北信越支部が中心に企画し、とんとん拍子で実現しました。開催日が、運動会・文化祭のシーズンで、自分自身も含め、対象のご家族をお持ちの会員も多いはずで、参加者数を心配しましたが、盛況のうちに終了することができました。研究会の詳細については、他の方が記載されると思いますので、省略しますが、いろいろな意味で、システム監査技術、知識の研鑽につながりました。

さて、システム監査を普及するためには、地道な努力、継続がポイントではないかと考えております。この研究会も同様、継続して実施していく重要であります。現時点では、会員が対象ではありますが、最終的には非会員の方にもオープンにできるような研究会まで発展させてはどうかと思います。

今後の研究会の予定は、2004年、近畿支部、2005年は、私ども中部支部担当になり、企画いたします。内容については、順次発表されますので、ご期待いただきたいと思います。そして同時に、会員各位の積極的な研究成果のご発表・ご参加をお願いするものであります。

参加者感想

No.737 中部支部 関口 幸一

私が敦賀行きを決めたのはほとんど土壇場になってからでした。なかなか北陸へ来ることができませんでしたが、中部支部の会合等へ森さん梶川さんが良く出席されていたこともあり、一度は出てみたいなと思っていました。幸い仕事も都合が付き何とか参加できることとなりました。

まず、今回地元の方を除いては敦賀に1番乗りしました。帰りは逆に遅めを準備してしまいました。そのため敦賀に4時間以上(研究会の時間を除いて)滞在する羽目になってしまいました。駅前を探訪する時間がありましたのでそのレポートからお伝えしたいと思います。まず、最初に敦賀は空気がきれいです。都会から参加された方々は口をそろえて言っておられました。

敦賀での発見1：駅前の通りには松本零士の「銀河鉄道999」と「宇宙戦艦大和」のオブジェが並んでいて通りの端から端を巡ることとなってしまいました。

敦賀での発見2：陰陽師の安倍晴明が研鑽を積んだところだそうでした。

時間通りに皆さんが集合され、バスに乗って敦賀短期大学へ。バスはぐるぐる回り道をしましたが、結果的には敦賀駅から西へほぼまっすぐに約4キロメートルの地点でした。

3方のお話をお聞きした後、さらに西へ三方五湖のはずれまでいき民宿にて楽しい2次会でした。噂通りお魚は新鮮で美味しかった。お酒も旨かった。結構遅くまでみんなで盛り上がりました。お湯も温泉で満足満足。

翌日は更に西へ出て小浜市へ、開催中の「若狭路博」の見学でした。無料の博覧会のため見所は少なく結局港の市場にて焼き鯖を買って小浜駅から敦賀駅まで単線でのんびりした電車の旅でした。途中丁度彼岸花のシーズンでそこここに赤い花の固まりを見ることができました。

No.1267 北信越支部 角屋 典一

10月4日(土)近畿・中部・北信越支部の三支部合同による研究会が、私の地元である福井県の敦賀市で行われました。今回の実施については、敦賀短期大学の黒目教授の多大なご尽力によって実現できたことに深く感謝いたします。

当日は、教室は敦賀短期大学内、また、穏やかな秋の日差しの中と恵まれた環境の中で実施されました。研究会の講演テーマは

(1) ユビキタス社会のおける個別マーケティングと必要なシステム監査
(2) 個人情報保護に関する制度の現状と今後の課題
(3) 個人情報保護の取り組みや教育の考え方(告発文化を創らないこと＝責務を認識すること)

でした。

（1）の講演はユビキタス社会をマーケティングの変化の中でとらえ、今後システム監査をどのように対応していくのかという点を問題提起されていました。

（2）、（3）の講義はまさに今トピックスである個人情報保護に関する講演であり、時代の要請にあったものでした。個人情報保護法については、私としてもこれから勉強しなければならない課題と考えておりましたので興味深く拝聴しました。個人情報保護法の原文もいただき、今後勉強するためのよい触発になりました。

研究会終了後は、地元の民宿にて、若狭湾で釣れた魚介類のご馳走をいただきながら、参加された方々と楽しく懇談しました。始めてお会いする方々が多かったのですが、おいしい料理もそこそこに、講演の中であった「監査」と「認証」についての指摘に関する議論もあり、楽しい雰囲気の中、充実した懇親会となりました。

私は銀行の関連会社に勤務しており、個人情報保護についてこれからどのように取り組むべきか大きな課題となっています。まだまだ、銀行内部でも認識が低く、今後具体的な検討課題にブレークダウンさせていく必要性を痛感しています。これからの研究会などでいろいろな情報交換をさせていただければと考えております。

最後に今回の研究会のためにご尽力いただいた講師ならびに事務局の皆様、本当にありがとうございました。

No.128　近畿支部　清水　順夫

三支部合同研究会にて、「個人情報保護に関する制度の現状と今後の課題」という内容でお話しをさせていただきました。日本システム監査人協会の例会等でお話しさせていただくのは、講師業も生業（なりわい）のひとつとするようになってからは、今回が初めてなのです。それというのも、本会は、そうそうたる専門家集団であり、そのような方々の前でお話しさせていただくのは、どちらかというと「広く浅く」タイプである清水としては、なかなか勇気のいることだったからです。今回それでもお引き受けしたのは、三支部合同という初のイベントであったことと、テーマがそろそろ勉強しないといけないと思っていた個人情報の保護に関するものだったのが大きな理由です。幸いにして、参加された皆様のご協力により、清水の話も無事に終わり、清水の前後に黒目様、吉川様に貴重なお話をいただけましたので、なかなかおもしろい研究会になったのではないかと思っております。

今回の研究会では、自身の準備も含め、あらためで個人情報保護に関して勉強させていただきましたが、住基ネットの問題を初めとして、世間でいろいろ取りざたされている割には、市販されている資料も少なく、真の問題点がしっかり認識されていないのではと強く感じました。その点では、今回の合同研究会のテーマに個人情報保護を選ばれた、各支部幹事の方々視点は、的確に時代をとらえたものと敬服いたします。ただ、個人情報保護に関しては、まだまだ多くの問題を抱えています。研究会当日もお話ししましたが、本会のなかでの研究にとどまらず、広く一般に啓蒙活動を行うことが、専門家集団としての日本システム監査人協会に期待されることではないかと考えております。

情報システムユーザー会主催 システム監査講演会報告

No.750　畠中　道雄

日時：平成15年10月21日　10：15～16：30
場所：大井町　きゅりあん

1. 情報化月間参加行事として情報システム・ユーザ会主催のシステム監査講演会が開催された。各団体から合わせて700名を超える参加があり、テーマに対する関心の高さを物語っている。以下にご報告いたします。
2. 始めに「情報セキュリティ監査制度の概要と課題について」と題して、経済産業省商務情報政策局情報セキュリティ政策室　山崎　琢矢　課長補佐より、①情報セキュリティ監査制度とは、②企業活動における制度活用の期待、③情報セキュリティ総合戦略と今後の政策展開、に関する講演があった。

   ①情報セキュリティ監査制度は次の4つのポイントからなる制度で、（1）企業等の情報セキュリティ対策について、（2）客観的に定められた国の基準に基づいて、（3）独立した専門家が、（4）評価する、制度である。監査を受ける主体は国・自治体・企業であり、監査を行う主体は情報セキュリティ監査企業台帳に登録された事業主体で、情報セキュリティ管理基準、並びに情報セキュリティ監査基準に基づいて監査を行う。

   企業等の情報セキュリティ対策については、「日々変化する」脅威に対するPDCAサ

イクルの構築に資するものでなければならないと考えられ、専門性の高い外部の者の評価を受けることが有効であるとしている。
客観的に定められた国の基準として、改善のプロセスまで包含した管理項目を定めた情報セキュリティ管理基準と、監査主体の行為規範を定めた情報セキュリティ監査基準とがある。情報セキュリティ監査は法定監査ではないが、これらの基準を国が示すことで、監査結果に対し公定力や信頼を付与することになる。
管理基準は132のコントロールと952のサブコントロールからなる2層構造であり、監査基準は一般基準・実施基準・報告基準の3本柱から策定されている。実際には、これらの基準のすべてを監査しなければならないわけではなく、個別の組織が必要とする監査項目を決めることになる。これをカスタマイズと呼ぶ。さらに業界別・業種別のモデルが必要ではないかとの観点から、ガイドラインに沿って管理基準モデル、監査基準モデルの作成が進められている。
情報セキュリティ監査は独立した専門家が評価を行う。このために用意されているのが、監査企業台帳である。またNPO日本セキュリティ監査協会の設立を支援してきた。
評価については保証型と助言型があり、保証型はセキュリティ対策が基準に準拠していることを保証し、助言型は基準とのギャップを指摘する。監査の進め方としては、助言または一部の保証を利用しながら、段階的にレベルを向上させていくことを想定している。
＜企業活動における制度活用の期待＞
ISMS認証制度がシステムの認証(組織の管理体制を保証する)であるのに対し、情報セキュリティ監査では、個別の組織のニーズに応じた実際の個々の対策についての保証(一部の保証)が可能であり、また、今後どのような対策を講じていくべきかという助言も可能である。情報セキュリティの事故は起こるものという前提で、事故を予防する(リスクを低減する)ために助言型の監査を利用し、事故発生時のリスクを分散させるために保証型の監査を利用するとよい。
＜システム監査との関係＞
現在、あるべき「システム監査」のあり方、およびシステム監査基準の改訂が検討されている。その理由としては、現行のシステム監査基準(昭和60年)が最新の技術動向に追いついていない、セキュリティ監査とは別の意義をもつ、ITガバナンスの視点が不足している、監査基準と管理基準は分離すべきである、などがある。
この中で、セキュリティ監査とシステム監査は、必要性や目的が異なると考えており、セキュリティ監査をシステム監査に含まれるものとは考えていない。
＜情報セキュリティ総合戦略と今後の政策展開＞
一言で言えば「電子政府イニシアティブ」。
電子政府に必要な道具は用意できたと考えており、ITが社会の神経系を担う時代に入ったと認識している。このため、セキュリティ対策は個々の主体が自己責任で行っているだけでは対応できない時代になった。すなわち、リスクが拡大し変質した。
＜3つの戦略＞
戦略の基本目標を、経済・文化国家日本の強みを活かした世界最高水準の高信頼性社会の構築と位置づけ、その要となる情報セキュリティ対策について、3つの戦略と42の施策項目を提言している。
① しなやかな事故前提社会システムの構築(高回復力、被害局限化の確保)
② 高信頼性を強みとするための公的対応の強化
③ 内閣機能強化による統一的推進

3. 2つ目は「事業継続計画と情報セキュリティ・マネジメント」と題して、株式会社インフォセックのCTO永宮直史氏が講演した。
本日のキーメッセージは、①事業継続計画は企業の存続に不可欠、②データセンターに加え、本社などの枢要な施設も対象に、③業務の流れに即し、グループ企業なども視野に置く、④リスクマネジメントは「経営」と「管理」の両面が大切、事業継続も同様。
始めに、9．11同時テロにおけるリーマンブラザースの対応が紹介された。同社では、事件発生とともに「尋常ならざる事態」と判断し、事業継続計画を発令する。本社がなくなり、データセンターもなくなったのに、翌日には少なくともある種の業務を、本社機能を別の場所に移して

継続できた。どうしてできたのか。それはバックアップサイトがうまく機能したためである。責任者が避難の最中に連絡して、手順通りの動きをした。本社ビルがなくなることを想定して、事務所として使えるホテルを手配できる体制があった。約5000台の端末が全く使えなくなったが、あらかじめ用意された契約に従って手配できた。崩壊前の機能はほぼ回復できた。1週間通常通りの業務ができなかった、という以上のインパクトはなかった。

また、ニューヨーク大停電の例も紹介された。この停電でどういうインパクトがあったのか。発生した時間帯が幸いして、電子的な取引は行われていなかった。しかしこの後、スナップショットで取引の経過を記録しようという動きが始まった。9月11日の経験は活かされた。

一方、依存度が高くなった携帯電話が、停電で全く使えなくなった。交通信号が麻痺、広域で大渋滞、誰がどこにいるか、帰ってくるかどうかもわからない状況になった。自家発電の担当技術者がいない、連絡できない。このため不慣れな人が自家発電装置を起動させたため、非常用電源から火災が発生した。バックアップ用の電源がだめになった。情報配信の会社はニューヨークとトロントで完全二重化していたが、通信会社も停止した。15日にすべてのシステムは復帰したが、通信輻輳でサービス低下。ストレージ会社と緊急連絡。幸い自家発電で編集テキストはバックアップできた。

危険はどこかに潜む。予想もしなかった事態で、たくさんの企業が本社の入ったビルを失った。災害の中でどうやって生きていくか。運だけに左右されてはいけない。特に企業は。災害でも生き残れる企業を考える。教訓として、①電話だけに頼ってはいけない。あらゆる手段で所在を確認し、連絡が取れるようにする。②緊急マニュアルは簡潔に。③訓練は必ず行い、真剣に。④普段から燃料などの供給に配慮。⑤要員を確保。

BCP(事業継続計画)に欠かせないのが情報基盤、パソコンによる業務遂行が増えた。枢要なデータが格納され、意思決定がデスクトップ上で行われる。このような中では個々のデータセンターを押さえるだけでは済まない。システムダウンによってどれくらいの時間を耐えられるかは、比較的簡単に出せるのではないか。何を優先させるか、体系的に考えていない場合が多いが、個別のリスクに応じた復旧が考えられるはず、あるいは他の手段で同様のサービスレベルを維持することを考えていかなければならない。何を優先し、企業として最低限担保しなければならないことは何か、を考える。

忘れがちな本社機構、次の点に注意。

- 意思決定機構が働かない企業は対応が後手に回る、致命傷になる。
- 緊急時の対応がきちんと動くか。
- 社長が意思決定できない時の代行者は決まっているか。

4. 3つ目は「CSKグループにおけるシステム監査の取り組みについて」と題して、CSKネットワークシステムズ　取締役人事総務本部長角田善弘氏の講演があった。

システム関係の監査は98年頃から充実を図り、2002年に組織体制として明確化した。最初に注目したのはBS7799、どうやって監査を進めるか、という問題にぶつかった。最初はドキュメントのチェック、それだけでよいのか。ここで壁にぶつかる。何をどうすればよいのか、最初からできたわけではなく、実態把握を行い、学習効果を狙った。

段階的な実施目標を立てた。①ネットワークの運用実態、②ネットワーク管理者にかかわる業務、③ネットワークを利用した監査モデル　ログもとっていない、ネットワークがわからない、アクセス権限の設定変更の遅れが見られた、ダウンロード後の情報の取り扱い状況を問題視した、機器関係ではＰＣを社外に持ち出すことがあり、BIOSロックの設定が必須、会社で認めていないソフトをインストールする、ウィルス対策ソフトを入れていない・稼動させていない・バージョンが古い、ログ情報、各部門サーバではログの管理は無防備、管理者が理解不足。このような状況では一人1台ＰＣを使っているだけでも、リスクは高い。監査する過程で何らかのツールが必要だと認識した。

規程、組織の整備をこの段階で行った。レベルは最初から分けられていたわけではない。自分で実際に作業してみるなど

の時間をかなりかけている。実際に現場に出向いて調べてきた。自己監査ツールは課題に対し、早期実施を目指し導入した。予防することを目的としたツールで全社対象のツール。当初紙で提出させたが、その後、EXCELに。
SECレポートは自己監査ツールよりさらに情報セキュリティに関する事項の強化を図るために導入したツールである。どこが悪いから問題だ、とわかればよい。ある程度性善説に基づいて作っている。600箇所くらいのチェックポイントがあり、実際にやってみると、本音で回答がもらえるので、どこを改善する必要があるかわかる。試行錯誤の中で責任者のコメントをつけさせる。
C－Forceは情報資産の管理レベルを網羅的に向上・維持させる目的で導入した。カバー率の向上が問題だったので、導入した。生の声を聞けた。若い人が回答することにより、改善しなければならない点が出てくる。アンケートに近いツールで、その都度バリエーションを変えて実施する。ネットワーク管理者がWeb関係の設定を行うが、ネットワーク管理者に任せている中で、パッチあてなどがきちんと行われているのか、チェックする必要があった。ＮＴサーバ関係のマニュアルをかなり読み込んだ。
COMPASSはリスク分析用。システム監査だけでなく、どのような問題が起きているのか、それに対してどのように取り組んでいくのか、方針を立てる時にこのようなツールを使った。ある程度まとまった時点でビジュアル化して見せる。内部統制の状況も入れている。

5. 4つ目は「三菱東京フィナンシャルグループ(MTFG)におけるシステム監査の取り組みについて」と題して、監査部上席調査役　金田　雅子氏より講演があった。
＜MTFGの経営課題への取り組みについて＞
いろいろな施策、収益強化策として、事務システムの共通化、共同化、銀行業務システムの標準化でグループ全体のコストダウンを図る。また、事務システムセンターを統廃合。
内部監査においては、システム監査の高度化を図る。内部監査とは営業店や本部が機能しているかを監査室、監査部という組織でモニタリングを行う。グループ共通施策は監査委員会で決定する。施策にはどのようなものがあるか。監査体制強化のための実務指針の策定、各種ガイドラインの作成。作成にあたって次の3点に留意した。①実践済みの監査手法との整合性、②内容の定期的見直し、③監査業務の支援を目的とする、あくまでも参考資料。
金融機関の視点でシステム監査を取り巻く動向をみると、システム監査体制の一層の充実強化が必要と認識し、施策を展開した。具体的には部門・個別業務・テーマ別システム監査を実施、監査項目、要点を網羅的にカバーした。重点テーマとして、システム開発にかかわるプロジェクトマネジメント(PM)、顧客情報管理、情報セキュリティ管理態勢、システム監査手続き書のレベルアップ、教育研修の充実。今年に入ってPM２回、BCM２回研修を実施した。
＜ＰＭ(プロジェクトマネジメント)監査＞
根拠のない見積もり、過大な仕様、等々、投資額の大きいプロジェクトでこのような問題が起きると大変だが、結果としてプロジェクトが成功したと言い得ない場合がある。対象としてプロジェクト管理と開発プロセスの二つに分けて考える。PMBOKの考え方をベースに監査し必要に応じて改善提案する。各作業内容をみるだけの監査ではない。テストケースの内容を見るだけでなく、一連のプロセスが有効にコントロールされているかをみる。ガイドラインを一言でいうと、着眼点。プロジェクトマネジメントプロセスは６つ、36の監査項目を設ける。監査項目、コントロール目標にチェックポイントをいくつか置いている。約200個。これらはすべて被監査部門に対しオープンにしている。監査経験があると、チェックポイントだけで何をみればよいか、誰に聞けばよいか、わかる。
監査の品質を確保するために、チェックポイントごとに、どの資料のどこに着目すればよいか、どの組織のどのような人に聞けばよいかが必要、これが監査手続きにまとめられている。評価視点も成熟度モデルの考え方を参考にチェックポイントごとに設けている。適切に実施されなかった場合、実態がかけ離れている場合は、高いレベルの改善提案はしない。
＜ＢＣＭ(Ｂｕｓｉｎｅｓｓ　Ｃｏｎｔｉｎｕｉｔｙ Ｍａｎａｇｅｍｅｎｔ)監査＞
業務継続体制の整備について認識が高まりつつある。導入プロセス、維持管理プ

ロセスに着目し監査で、少なくとも一巡していると認識している。必ずしも最初からある必要はない。被監査部門も受け入れやすい。
検証ポイントは狭義のCP(Contin uity Plan)の場合、いかに脅威から早期に回復させるか。広義のCPの場合、可用性を確保すること。ここで監査人による偏りをなくすため、ガイドラインの必要性が出てくる。構成は事例研究集とチェックポイント集の2部構成。事例研究集(事例は過去2年)は、監査を通して予防可能だったのか、実際に起きた事例をもとに説明しているので、被監査部門がわかりやすい。チェックポイント集は被監査部門(対策本部、コンピュータセンター、国内本部、国内営業店、海外、コンピュータシステム)ごとに作成した。チェックポイントの情報源はFISCの指針など。

日本システム監査人協会主催 第99回月例研究会報告

No.561 日高 祐子

開　催：2003年9月30日(火)
場　所：中央大学　駿河台記念会館　520会議室
講　師：金融庁検査局　総務課　特別検査官
　　市川雅也氏
テーマ：
「システムリスク検査ー金融機関等における多様化する情報システムリスクへの対応についてー」

当日、受付前には長蛇の列ができ、また会場内は三人掛けテーブルに三人が着席してもまだ収容できず、遅くに到着された方は椅子を持ち込んでの参加となる盛況振りであった。昨今の状況において、システム監査を考える場合の、当講義テーマと講師への関心の高さが窺えた。
講義要旨
1. 金融庁について
金融庁の任務は、金融機関の安全を確保し、預金者・保険契約者・有価証券投資者の保護と金融の円滑を図ることである。この任務遂行の為、金融庁「監督局」は金融機関に説明を求め行政処分等を行う。また、同「検査局」は金融機関に出向き検査を実施する。
2. 事務ガイドラインと銀行法
金融庁ホームページには、「事務ガイドライン」が掲載されており、かなりの頻度で改訂がなされている。当ガイドライン「経営姿勢」の項目では、システムに関わるリスクを経営陣が如何に認識しているかを問い、この認識が充分でないと基本方針が具体化されないと考えられている。また同「経営管理」の項目では、顧客に関する情報管理について、これが適切に行われていることを《検証できる体制》があることが求められており、顧客情報の漏洩が行われていないことを《証明できるかどうか》という観点で、検査がなされる。しかしながら、検査局による立入検査は「健康診断と捉え、健康体であっても更に病気がないかを検証し、悪いところがあれば是正するというスタンスで望んで欲しい。」と力説された。
3. 金融検査マニュアルとシステムリスクの定義
「金融検査マニュアル」では、リスクを信用リスク・市場性リスク・流動性リスク・事務リスク及び　システムリスクの5種類に分類し、認識している。システムリスクとは、コンピュータシステムのダウン等により、顧客等に損失が発生するリスクであるが、昨今システムリスクへの対応は多様化を極めている。
4. システムリスク管理態勢の確認検査項目
数々のシステムリスク管理態勢の確認検査項目の内、特に当講義において強調された部分は、
・経営陣のリスク管理への関与、すなわち「コンピュータ関連はIT部門に任せている。」という状態ではなく、「システムリスク管理の基本方針」等が経営のレベルで討議されているか？
・セキュリティスタンダード等の評価基準が存在し、且つ日々改訂されているか？
であり、また外部委託管理については、「事務ガイドライン」の平成15年6月末改訂において「章」への格上げがなされているとのことである。
5.システム統合リスクについて
経営陣がシステムの専門家であることは稀であるが、システム統合が何故必要なのかを理解でき、「システム統合が順調に進んでいるか？」を経営陣が判断できる基準がなければならない。往々にしてセキュリティレベルの低いところからリスクは発生するが、例えば、各工程完了の承認ルールにおいて差異がある場合、品質にばらつきが生じることとなる。業務要件の確定から工程の承認ルールの統合等、経営陣が必要であることを認識すべき項目は多々ある。また、不測事態への対応としては、統合計画に比して遅延した場合等の見直し基準、発動権限者及び発動基準、システム統合の中止・延期に関わる判断基準の存在が経営陣の判断のために必要である。

大切なことは、顧客の目でリスクが考えられており、顧客に対してきちんとした対応ができることである。最後に、システム統合時においては、内部監査体制を整備することは非常に難しく第三者機関による評価、すなわち外部監査

がミニマムスタンダードとされていることを付加された。

記念月例会 第100回月例研究会報告

No.557 仲 厚吉

開 催：2003年10月27日(月)
場 所：ワーカーズサポートセンター601会議室
講 師：(有)ビジネス情報コンサルティング
代表取締役 小野修一氏

ー第100回月例研究会「情報化投資の有効性評価」を受講してー

今や情報システムは業務作業や顧客、取引先情報の収集において企業経営に必要と経営者に認知されていると思います。小さな商店においてもパソコンと会計ソフト及び顧客、取引先一覧を整理する表計算ソフトやワープロソフトがあります。

小さな企業を立ち上げる場合において100万円の情報化投資によるパソコンとソフトなどの購入が生み出す企業経営における有効性の算盤をはじくことはその必要性から経営者判断は簡単でしょう。しかし大中規模の企業において10億円の情報化投資が生み出す有効性判断の尺度は確立されていないと思います。情報化投資の投資回収を試算する場合に、今回、第100回月例研究会における、「情報化投資の有効性評価」の講演を受講して有効性評価尺度の体系について理解することができました。詳細については講師の著書を読んで勉強したいと思います。

講演において最も印象的なことは講師が情報化においては費用対効果という言い方よりも投資対効果という言い方をされていることです。費用というとコスト、コストというとコストダウンあるいはコストカットというように、無駄なことを省くイメージになります。果たして情報化の本質は無駄なことあるいは必要悪でしょうか。

経営においては売上粗利の最大化が企業目標であり、そのために株主からの投資をつのり経営者が人材や設備に投資をするサイクルが継続的に行われ、顧客への売れ筋商品をマーケティングし製造または仕入れて販売するなかで情報化投資が行われます。情報化投資が役に立つようにまわしていくために有効性評価が必要になります。また、その企業に卓越的なコアコンピタンスは自前で持ち、どの企業にも共通な部分は業界で標準化を行う、あるいは外注することも有効性評価のひとつの視点になると思います。

システム監査の視点から見て、システム監査は、元来、ホストコンピュータが対象であったと思います。2000年(Y2K)問題をクリアした後、21世紀に入り、インターネットの活用が家庭にも当たり前になる時代、便利で役に立つインターネットを安全に使いたいという願いが情報セキュリティ監査を生んだと思います。住基ネットにおいても市民側のネットワークはインターネットになっています。

システム監査の有効性評価において情報化投資を役に立つようにまわしていくために責任体制の明確化という視点も必要だと思います。業務体制や技術が確立されていても責任体制や権限があいまいではうまくまわらない結果となるため、第3者のチェックが必要になります。ここにシステム監査人及びシステム監査人協会の働き場があると確信します。

平成15年度第9回理事会議事録 NPO日本システム監査人協会

平成15年10月度 理事会議事録
開催日時：2003年10月8日(水)
18：45ー21：00
場所：三井物産㈱ 15階会議室
出席者：橘和、小野、蓮見、鈴木(信)、吉田、片寄、勝田、竹下、馬場、打矢、木村

＜審議事項＞

1. 推薦制度 (担当：小野副会長)
推薦制度について、前回理事会にて審議された意見を基に法人部会にて検討した案の説明があり、運営委員会の設置、推薦書発行、推薦依頼、費用の負担、権利と責任、訴訟、本制度の運営等について審議した。その結果、さらに検討するべき事項が出され、再度検討し次回に提案することとなった。

＜報告事項＞

2. 事例研報告 (担当：吉田理事)
(1)システム監査 2日間コース ITC認定コースの申請を出していたが、10/3認定された。
11月の近畿会、11月末の東北支部で実施するコースが該当する。
(2)来年の事例研究会 4回(4日間コース、2日間コース各2回)予定している。
最初の日程は、1月31日(土)、2月1日(日)、2月14日(土)、2月15日(日)である。
(前に予定していた日程が変更になっているので注意)
3. 会 計 (担当：蓮見副会長)
会計監査の指摘事項への対処は理事会

メーリングリストのとおり。
9月末で会計上の四半期になる。各支部は7-9月の会計処理の報告、各理事は担当業務について経費の請求処理等を行うこと。

4. 公認システム監査人認定申請等
(担当：鈴木(信)理事)

(1)9月末の申請状況
公認システム監査人　88名
公認システム監査人補　51人

(2)審査面接　10月8日までに実施した結果
公認システム監査人　16名

(3)今後の審査面接予定
10月11日　名古屋　面接委員
(アサイン済み)
10月12日　大阪　第1回　面接委員
(アサイン済み)
10月25日　東京、福岡　面接委員未定
(アサインこれから)
11月1日　東京、仙台　同上
11月8日　広島　同上
11月15日　東京、富山　同上
未定　大阪　第2回　同上
(面接委員未定(アサインこれから)分については、協力を願う)

5. 技術交流会の件(中部　原善一郎氏からの連絡があった事項についての報告)
(担当：鈴木(信)理事)
原氏が中国科学院　計算技術の団体の副所長と交流あり。IT技術者の交流の機会があるので、システム監査について含めた交流をできるように持っていきたいので、本部も入れて考えたい。どのように行動するか。
→経済産業省の活動と関連している可能性あり。片寄理事から鈴木(信)理事に関連情報を寄せてもらう事となった。鈴木理事に動いてもらう。(当関連情報を議事録末尾に"参考"として記載する。)

6. "安全管理を民間格付け"(日経新聞10月8日朝刊の記事)に関して
(担当：鈴木(信)理事)
「協会として売り込んでゆくかどうか、渉外活動として、営業に出ることは意味のあることである。」との意見が出された。
関連事項として、「経済省山崎さんには、沼野理事より8/1に、本件公表後の講演をご依頼し、ご承諾を得ている。月例研での実施を計画しているが、実施時期等は未定である。」

7．月例研究会　(担当：勝田理事)

(1)第99回研究会
参加者　155名+3名　これまでにない参加者数で大きな会場に変更して開催した。盛況であった。しかし、受付等に関する不手際(名簿にもれ、返事がない、席が足りない)があり、参加者からクレームがあった。本件について今後の対処を話し合った。
意見：「お客さんの扱いの基本が出来ていない。」「お金をもらっている。」という基本的なところを認識する必要がある。
申し込み名簿の作成方法、受付けたかどうかの確認連絡(するか否か)、断る場合に連絡する、等について討議した。
暫定処置、根本的な対策、それぞれできるところから手をつけて実施することとする。HP担当とも連絡を取り、実施する。100回目の研究会について、「満員で申し込みを受付られない場合は返事をする」が、「申し込みに対して受付が出来た場合は返事を出さない」旨の表示は入れることにする。

(2)第100回研究会
小野副会長による「情報化投資の有効性評価」をテーマに2003年10月27日(月)にワーカーズサポートセンター601会議室にて開催する。案内手配済み。

8. 会報　76号について　(担当：竹下理事)

(1)原稿は11月16日締め切り、発行12月初旬予定
特集：研究会特集　月例研究会(9月、10月)、JUASシステム監査セミナ、事例研、その他
応募論文(1篇)を間に合えば取り上げる。
査読を進める。

(2)編集委員公募して、6名(首都圏)に参加してもらえる。
会員からみた会報のあり方を研究したい。

(3)記事の長さについて　1ページは800字であるから、見出しがページの上に繰るような編集をしたいので、800字単位としてもらえれば見栄えが良くなり好都合である。

(4)編集長　力理事

9. 三支部合同研究会が実施され鈴木(信)理事が参加した。　(担当：鈴木(信)理事)
詳細は別途

10. 法人部会　(担当：小野理事)

(1)アイビスジャパン(株)様(東京)が法人会員として入会した。

(2)システム監査企業台帳、および情報セキュリティ監査企業台帳の中の当協会会員でない企業(各約50社)宛に当協会のDM(案内、入会申込書、会報)を発送した。

11. 日本セキュリティ監査協会(JASA)について

(担当：木村理事)
第3回の設立準備会に出席した。
設立総会が10月16日(木)にメルパルク東京にて開催される。協会からは、鈴木(信)理事が出席する。

12. 近畿会　(担当：馬場理事)

(1) 9月12日　1日セミナー　協会メンバー以外を対象にしたセミナーで、23名受講。
公認システム監査人のポイントのために出席していた人がいた。

(2) 9月19日　定例研究会　講師：吉田氏
39名参加
自治体がシステム開発に並行してシステム監査を実施した事例

(3) 10月4日－5日　3支部合同研究会
25名参加
本部を代表して鈴木理事に参加いただいた。

(4) 実践セミナー　11月1日－2日
現在13名の申し込み。
ITC認定等　吉田理事、沼野理事にご支援いただいた。

議　　長　：　橘和　尚道
議事録署名人：　竹下　和孝　　木村　裕一

＜次回理事会開催予定＞

平成15年11月12日(水)　18：30－
三井物産㈱15階金属A会議室(地下鉄大手町C5出口)

(参考)：片寄理事から理事会翌日に寄せられた関連情報

中国のシステム監査普及協力関係で理事会にてお話のでたITSSと相互認証についてお知らせします。

アジアの各国のIT資格試験の相互協力は「IT資格相互認証」といって、各国の資格制度を日本でも情報処理試験同等の力があると認めましょうというもので、実は契約締結自体はJIPDECが2002年に行っていました。その中に実は中国もありました。既に中国では信息産業部というところで試験を実施しているそうです。

この件は今年できたITSSとは直接は関係なさそうです。申し訳ありませんでした。
ITSSのITスキル標準センターはIPAの中に7月に出来ているそうですから、いずれにしても窓口は情振課ということでしょうか。

平成15年度第10回理事会議事録
NPO日本システム監査人協会

平成15年11月度理事会議事録
開催日時：2003年11月12日(水)
18:45－21:00
場　所：三井物産㈱　15階会議室
出席者：橘和、岩崎、打矢、小野、勝田、金子、鈴木(信)、力、富山、沼野、馬場、蓮見、本田、松枝、水野、吉田、和貝

＜審議事項＞

1. 推薦制度　(担当：小野副会長)
・推薦制度について、前回理事会にて審議された意見について法人部会にて再検討し、作成した下記の案について説明があり、審議の結果、特に当協会の責任については弁護士のレビュを受けることを条件に、制度化することに決定した。
・検討資料
推薦制度最終案
推薦制度運営委員会規約案
推薦制度書式最終案

2. 第3回総会日程等　(担当：富山副会長)
・総会日は、2004年2月23日(月)に決定することが承認された。
・上記に先駆けて役員選挙公示、役員立候補者届出等があるが、これらに関する規定についてNPOとしての整備が必要とのことから、次回理事会で規定改定案につき審議を予定する。
・総会にあわせて実施する恒例の講演については、次回月例研究会企画会議で検討する。
・総会日については、次回会報に公示する。

＜報告事項＞

1. 動向報告　(担当　橘和副会長)
・社会保険庁より「社会保険オンラインシステム刷新可能性調査専門家会議」につき協会からの専門家の派遣依頼があり、鈴木(信)理事を推薦した。
・10月16日にNPO日本セキュリティ監査協会の創立総会が開催され、協会から橘和副会長、鈴木(信)理事が参加した。
・協会の継続教育プログラムとして、「情報セキュリティ監査セミナー」が8月の東京に続き、広島(10月24日)、大阪(10月25日)で開催された。中国経済産業局の向井裕課長補佐、近畿経済産業局の森畑通夫課長、森家隆文係長、IPAの日下保裕氏にご協力いただいた。セミナー講師として和貝副会長が担当し、継続教育部会担当の橘和副会長が認定業務を兼ねて参加した。
・システム監査基準検討委員会(委員長：鳥居壮行駿河台大学教授)が7月に発足している。協会からは、橘和副会長と、本田理事が参加している。来年3月に新基準

公表に向けて、監査基準、管理基準担当のワーキンググループ単位の検討が進んでいる。
・システム監査学会では、「システム監査専門監査人認定制度(案)」を10月24日のシンポジュウムで公表した。その概要を報告したところ、「学会は学術団体であり本来の役割と違うのではないか」、「狭い技術的分野の専門性を目指してニーズあるか」、「学会に制度運営のボランティアパワーがあるか」、「商標と役務が登録・保護されている『公認システム監査人』の商標登録に抵触すると思われる」、「同じ目的の学会とは互いに連携する必要があり、調整すべきではないか」等の意見が出された。今後の進展の状況によっては、協会内での検討、学会への提言等に関係する事項である。

2. 事例研報告　(担当：吉田理事)
・東北支部での「システム監査実践セミナー」が11月23、24日に開催される。受講生は10人である。
・2004年1月に「システム監査実務セミナー」として4日間コースを実施する予定であり、近日中にホームページ等で募集する。

3. 会計　(担当：蓮見副会長)
・平成15年度特定非営利活動に係る事業会計の9月までの状況について報告があった。

4. 公認システム監査人認定状況　(担当：鈴木(信)理事)
・申請者：
公認システム監査人　88名
システム監査人補　53名
上記中公認システム監査人登録内定者は、53名、システム監査人補内定者は、17名、未面接者が17名残っている。なお、昨年度は公認システム監査人が253名、システム監査人補が191名であったので、差し引き累計で500名を大きく超える認定者が出る予定である。

5. メール関連　(担当　岩崎理事)
・月例研究会のメールによる参加申し込み受付についての取扱いを検討中である。
・協会900名体制のメールシステムのあり方について、検討中である。

6. システム監査基準研究部会
(担当　本田理事)
・システム監査基準検討委員会での「システム監査基準」改訂検討の状況報告とそれに併行して、研究部会で検討を進めている旨、報告された。

7. 継続教育セミナー第二回
(担当　鈴木(信)理事)
・情報セキュリティ監査セミナーに続く第二回セミナーを次に予定する。
日時・場所：
平成16年1月31日(土)
13:30～16:50 機械振興会館
テーマ：
「電子自治体の今、これから」
講師：三鷹市役所、柏崎市役所ほかより招請

8. 月例研究会　(担当　勝田理事)
・11月19日に企画会議を開催する。1月以降の半年間程度のテーマ及び講師の検討を行う。
・第3回総会の記念講演のテーマ及び講師について検討する。
・12月3日の月例研究会については既に67名の申し込みがあり、締切日(11月26日)までには更に増員が予想され、締め切りの検討が必要かもしれない。また、関連団体ISACAにも、開催の旨紹介することとする。

9. 会報　(担当：力理事)
・第76号の原稿は11月16日締め切り、発行12月初旬を予定する。「研究部会」を特集する。
・12月4日に、応募参加した新編集委員を含めて編集会議を開催する。
・第77号の発行は、2月上旬を予定する。

10. 法人部会　(担当：小野理事)
・エヌ・アイ・コンサルティング(株)が法人会員として入会した。

11. 近畿支部　(担当：馬場理事)
・11月1、2日に「システム監査実践セミナー」を開催した。吉田理事、沼野理事に支援いただいた。
・10月25日に「継続教育セミナー」を開催した。(上記　1．参照)
・12月12日に「韓国のIT事情・eコマース事情」のテーマで定例研究会を開催する。

議　長：橘和　尚道
議事録署名人：鈴木　信夫　和貝　享介

＜次回理事会開催予定＞
平成15年12月10日(水)　18:30～
三井物産㈱15階金属A会議室(地下鉄大手町C5出口)

支部便り

北海道支部便り

No.893　波部　洋子

10月末、初雪を待つばかりの札幌です。アスファルトを踏みしめながら歩いていると、夏靴

で歩けるのもあとわずか、と思ってちょっと寂しくなります。冬の北海道で女性がヒールのある靴で歩いていると感心するあなた、それは冬靴です。中にボアが敷き詰めてあり、底はスパイクさながら。日本の大部分で普通に履く靴は、こちらじゃ夏靴です。車のタイヤと一緒ですね。そろそろ冬タイヤに交換する時期です。

さて、支部活動のご報告です。

(1) 9月の研究会

10月3日に「システム開発/保守のアウトソーシング受託における品質改善活動」をテーマに、研究会を開催しました。講師は会員の五十嵐さんです。五十嵐さんの職場での品質改善活動の状況をお話いただきました。非常に実践的な内容を、具体的な数値をあげてお話いただいたので、とても盛り上がりました。他の皆さんの状況をお聞きしたり、実際の仕事の参考になるものです。本では得られない現実の話と実施テクニックは貴重なものでした。会場はいつもの北海道立市民活動促進センター、参加者は会員7名、非会員2名の計9名です。

(2)10月の勉強会(ビデオ)

10月24日に、10月の勉強会として「システムリスク検査 - 金融機関等における多様化する情報システムリスクへの対応について」(第99回研究会)のビデオ上映およびディスカッションを実施しました。月例会史上最高の参加者だったというウワサのためか、こちらの参加者も多めで、会員7名、非会員4名の計11名でした。上映後のディスカッションでは、情報セキュリティ監査の話も出ました。今回の会場は、札幌市民活動サポートセンター、札幌駅前に新しくできたエルプラザ(札幌市の施設)の一角で、新しくきれいな設備です。人気もあるようで、当日は他の部屋も結構な人出でした。市民活動、盛んなんですね。我々も負けずに頑張らねば。

東北支部便り

西川　雅樹

SAAJの皆さんこんにちは、東北支部の西川です。今この原稿を書いている11/15、仙台はすでに初冬にはいっているのですが、この支部だよりが皆さんのお手元に届く頃、東北は大部分が雪と氷に覆われている事でしょう。

冬も間近な去る11/9、東北支部では第2回目の月例会を仙台で開催しました。8月の特認研修で参加者も大幅増かと思われたものの、遠隔地の方がどうしても参加しづらいこともあってひとまず前回並みの参加者数となり、それでも活発に意見交換、情報交換が行われました。前回の月例会同様、今回も「本部月例研究会ビデオの自宅学習」についてたくさんの強い要望が聞かれました。遠隔地の方が、ビデオによる自宅学習の成果を支部研究会で発表できるようにするなど、研究会運営のあり方について検討することになりました。また、先ほど経済産業省から公表された情報セキュリティ総合戦略についても、参加者各自の立場・仕事を踏まえたいろいろな意見交換が行われました。今回の月例会のトピックスとしては、地元行政が音頭を取って設立が決まった「情報セキュリティ監査ビジネス研究会」があります。詳細は未定ですが、会費無料の特別会員としてアドバイザー的な立場での参画を打診されており、今後支部が地元の情報セキュリティに関してどのような役割を担っていけるのか、非常に楽しみなところです。

なお11/23～24には、東北初のシステム監査実践セミナー(2日間)が仙台で開催される予定です。こちらのほうも地元の動向を踏まえ、東北でのシステム/セキュリティ監査技術向上のプラットホームとして育てていきたいと考えています。もっとも実施にあたっては、東京本部はもちろん各支部のご協力なくしてはまだまだ東北だけで実施できることでもありません。今後ともなおいっそうのご支援・ご教授よろしくお願いいたします。

中部支部便り

No.124 国際部 原　善一郎

中部支部では、2003年9月26日名古屋にて中国科学院計算技術研究所との技術者交流を実施しました。内容は、以下のとおりです。なお、来年3月には、中部支部では北京を訪問する計画です。

参加者：16名

中国科学院計算技術研究所：副所長＆教授ファン=チェンピン博士、フォン=シャオピン博士　他3名、日本事務所　張建、張瑩

SAAJ中部支部：山崎支部長、大野副支部長、萬代、提、斉藤、岡田、若原、原(善)通訳に王氏

情報交換：

・日本のシステム監査の状況
・NPO法人日本システム監査人協会
・同　中部支部と　参加者自己紹介
・中国科学院紹介での技術者交流について
・日本の情報技術について

技術情報紹介：(メンバー会社から紹介)

・東邦ガス：地域防災システム
・日立製作所：ミューチップ、指静脈認証技術

懇談：

・OSの開発についての討論
・勤務時間の長さについて
・中国のソフトの品質向上について
・日中の情報技術者交流の重要性について等

今後の交流：

・SAAJ中部とその関連のグループと定期的に技術者交流を行いたいとの提案があった。中部支部国際部が核となって、日中の情報技術者交流を進めたい。特にシステム監査をキーワードに進めたい。

なお、片寄理事、原田元理事、原純江さん、システムアナリスト協会の中西佳世子さんにも科学院ご一行様の日本の状況調査にご協力いただいたことを申し添えます。

No.957　VRメッセ担当　小幡　哲也

11月14日、岐阜県大垣市のソフトピアジャパンで開催で、「IT社会と情報セキュリティ」というテーマで、セミナーを開催しました。詳細については、次号で詳しくレポートします。参加人数は、約60名でした。

◆ 基調講演　13：30～14：30
「IT社会と情報セキュリティ、今企業がなすべきこと～システム監査」
三口充高氏　NPO日本システム監査人協会　法人会員　日本ユニシス株式会社　システムサービスマネージメント本部　システム監査室　室長

◆ 講座1　14：45～15：30
「転ばぬ先のセキュリティ対策
～後追いの対策にならないために～」
河田　一宏氏
日本システムアナリスト協会 正会員

◆ 講　座2　15：45～16：30
「情報セキュリティをしなやかに維持していくために」
田中　勝弘　氏
NPO日本システム監査人協会　正会員

中国支部便り

No.401　大谷 完次

中国支部では、公認システム監査人等の継続教育セミナーとして、今年度から開始された「情報セキュリティ監査制度」の解説を中心に開催しました。このような監査に関するセミナーは中国、四国地方で初めてのケースであり、受講者が集まるかどうか心配でしたが、四国、九州からの参加者もあり31名の受講者が集まりました。

講演は、まず中国経済産業局向井補佐より制度のe JAPAN戦略での位置づけe JAPAN戦略第2版での位置づけから来年度の予算獲得の動き等を幅広く解説して頂いた。更にメインテーマとして和貝副会長より「セキュリティ監査基準」について詳細に解説して頂いた。たった4ページの基準の1行1行の背景、考え方の解説は説得力があり3時間に渡る講義もアッという間に過ぎていました。継続教育セミナーとして大変有効なセミナーではないかと感じました。

セミナー終了後は、講演者及び橘和副会長を囲んで懇親会を実施し、継続教育についての意見交換、中国経済産業局との意見交換で盛り上がりました。今回のセミナー開催の成果と反省は以下のとおりです。

①中国経済産業局との太いパイプができた。
②セミナーの収支を地域でバランスさせることは容易でない(有料入場者40名以上を確保する必要があるが分散しているため集客が容易でない)。
③これからもITコーディネータ協会等との協力関係を継続する必要がある。
④監査に関する地方自治体の反応が薄いので今後働きかけが必要である。

最後に和貝副会長、橘和副会長、鈴木(信)理事をはじめとするセミナー開催にあたりご協力頂いた協会の皆様、中国経済産業局様及びＩＴコーディネータ協会様に厚く御礼申し上げます。

会報掲載論文募集中

会員(正会員)の皆さんより、会報掲載論文を募集しています。

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、啓蒙、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　8千～16千字程度(図表含める)
※論文審査委員会にて審査を行い、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。掲載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。詳しくは会報No.74(p 27)参照のこと。

第3回システム監査実務セミナー(4日間コース)受講者募集のご案内
システム監査未経験の皆様へ
システム監査実務セミナーに参加し、システム監査の実際を体験してみませんか

NPO法人日本システム監査人協会では、設立目的のひとつである「システム監査人の実務能力の維持・向上」のため、下記の日程で第3回目のシステム監査実務セミナー(4日間コース)を開催いたします。このセミナーは、当協会が既に10回を超える開催実績を持つ、「システム監査実践セミナー」(1泊2日コース)の内容を拡張・充実し、前半(1泊2日)、後半(1泊2日)の延べ4日間で実施する、日本では初めての本格的なシステム監査実務を体験できるセミナーです。

本セミナーでは、当協会事例研究会で実施したシステム監査普及サービスの事例を教材とし、実践で得たノウハウを皆様と共有することを目標にしています。また、このセミナーを受講し、事後課題を提出頂きその内容が適切と判断された場合には、当協会が認定する「公認システム監査人」に必要なシステム監査実務経験を1年間経験したものとみなされます。

システム監査技術者試験には合格したもののシステム監査を経験されていない皆さん並びに公認システム監査人資格の取得を目指されている方は、この機会を利用してシステム監査の実際を体験し、システム監査能力の向上を図りましょう。当協会の会員でない方も大歓迎です。多くの皆さんの参加をお待ちしています。

なお、本セミナーは、以下の資格をお持ちの方の認定セミナーとなっております。

・ITコーディネータ対応専門知識研修コース(獲得知識ポイント5.5ポイント　22時間)

・日本公認会計士協会の継続的専門研修制度におけるCPE認定研修(履修単位：29単位)

記

1．日　　時　(前半)平成16年1月31日(土)～2月1日(日)
第1日目10：00～20：00　第2日目9：00～15：00
(後半)平成16年2月14日(土)～2月15日(日)
第3日目10：00～20：00　第4日目9：00～15：00
※参加は前半、後半の通しとし、どちらか一方のみの参加はできません。

2．場　　所　幕張OVTA(海外職業訓練センター)JR京葉線海浜幕張駅下車徒歩5分
〒261-0021　千葉市美浜区ひび野1丁目1番地　℡043-276-0211

3．費　　用　SAAJ会員：168,000円　　一般：189,000円
(費用には、消費税、宿泊費、食費を含みます。)
テキストとして日本システム監査人協会編「情報システム監査実践マニュアル」(4,200円税別)が別途必要となります。

4．セミナー内容　事例研究会が実施したシステム監査普及サービスをケーススタディとして取り上げます。4～5人程度のグループにわかれ、監査依頼事項の確認、トップインタビュー、監査テーマ・監査計画の作成、予備調査、本調査、監査報告作成、監査報告会などの演習をロールプレイング形式をまじえ、4日間のセミナー実習を通し体験して頂きます。

5．講　　師　事例研究会メンバーのシステム監査普及サービス経験者8名(予定)
講師は監査手順の解説・指導の他、被監査企業の社員の役割も演じます。

6．募集対象者および人員
日本システム監査人協会会員(法人会員を含む)、システム監査技術者試験合格者、あるいは同等の能力を持つ方、システム監査に従事されている方

あるいは従事される予定の方、システム監査を業務に役立てたい方、システム監査技術者試験受験予定の方、ITコーディネータ、公認会計士の方など。定員20名(最小催行人員12名)

7.申し込み先　NPO法人日本システム監査人協会 システム監査事例研究会
事務局担当　太田　香　(E-Mail：otamail@pop21.odn.ne.jp)
※下記の申込内容を記入の上E-Mailでお申込下さい。

8.申し込み期限　平成15年12月26日(金)
※毎回キャンセル待ちの方がいらっしゃいます。お早めにお申込み下さい。

9.問い合わせ　NPO法人日本システム監査人協会
第3回システム監査実務セミナー事務局担当　太田　香
E-Mail：otamail@pop21.odn.ne.jp

以　上

NPO法人日本システム監査人協会
第3回システム監査実務セミナー参加申込書

平成15年　月　日

①会員ＮＯ：(法人会員の場合は法人名)：

②氏　名：

③勤務先名称：

④勤務先所属：

⑤資料送付先：(住　所)〒
(宛　名)
(ＴＥＬ)

⑥連絡先E-MAILアドレス：

⑦請求書　必要　／　不要

⑧領収書　必要　／　不要

⑨システム監査実施経験：　あり　／　なし

⑩当協会主催のシステム監査実践セミナー参加経験：　あり(　年　月)／　なし

⑪当協会主催のシステム監査実務セミナー参加経験：　あり(　年　月)／　なし

⑫テキスト購入希望：　あり　／　なし
(テキスト：日本システム監査人協会編「情報システム監査実践マニュアル」をお持ちでない方には、当日会場にて割引価格(3,600円税込み)で頒布いたします。)

新規入会者一覧

番号	氏名	勤務先・所属		支部／地域
1317	熊谷　克巳	(株)富士通東北システムエンジニアリング	金融システム部	東北
1318	釘本　浩樹	ウィジット(株)		近畿
1319	佐藤　直美	(有)インキューブ		東北
1320	原　秀文	(株)富士通東北システムエンジニアリング	第二システム事業部ビジネスソリューション部	東北
1321	小野寺　司	(株)富士通東北システムエンジニアリング	ビジネスソリューション部	東北
1322	中山　治幸	NTTコムウエア(株)	システム本部第一システム部	関東
1323	小田　善夫	(株)富士通東北システムエンジニアリング	ビジネスソリューション部	東北
1324	椋野　誠司	関電情報システム(株)	ソリューション第二事業部	近畿
1325	白鳥　健次	(株)富士通東北システムエンジニアリング	第一システム事業部 第一公共システム部	東北
1326	藤田　克美	合資会社フジタマネジメントシステム		近畿
1327	石川　智康	トヨタ自動車(株)	車両技術本部	中部
1328	小林　豊弘	小林経営研究所		東北
1329	小林　秀敏	(有)小林ネットワーク設計		関東
1330	冨田　誠	監査法人トーマツ	監査部門	九州
1331	内田　英樹	(株)日立製作所	情公共/九州システム	九州
1332	柳川　制弐	キャノン販売(株)	近畿SE部	近畿
1333	河原　孝尚	世田谷信用金庫	事務部	関東
1334	佐久間　衛	富士ゼロックス(株)	DSMC SB推進統括部	関東
1335	尾関　博	アサヒビール(株)	IT部	関東
1336	稲吉はるな	ｿﾆｰ･ｸﾞﾛｰﾊﾞﾙ･ｿﾘｭｰｼｮﾝｽﾞ(株)	ネットワークサービス事業部	関東
1337	斉藤　幸雄	日本電気(株)	第5金融システム開発事業部	関東
1338	秋山　卓男	昭和監査法人	代表社員	関東
新入法人会員				
6034	齋藤　仁士	アイビスジャパン(株)		関東
6035	竹田　雅敏	エヌ・アイ・コンサルティング(株)		近畿

＜第３期通常総会のご案内＞

NPO日本システム監査人協会の表記通常総会の日程は次の通りです。

万障お繰り合わせのうえ是非ご出席下さい。

日時：平成16年２月23日(月)ＰＭ１：15～

場所：日本ユニシス株式会社(東京都江東区豊洲１－１－１)29階大会議室

内容：記念講演に引き続き、通常総会を行います。総会閉会後に懇親会開催。

<編集後記>

初めてSAAJ会報の編集を担当させて頂いた。大勢の方々に原稿を書いて頂き感謝しています。皆様の原稿をしっかり読めて大いに勉強になりました。地理的に離れている方、面識がない方とも電子メールを使って連絡と原稿収集ができ、ITの進歩によって会報の編集も大きく変わりました。ITの進歩とプロセス・スタイル・意識の革新についてもシステム監査の取り組む領域の一つだと思います。(TC)

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　宮川　公男

事務局 〒163-0716
東京都新宿区西新宿 2-7-1
新宿第一生命ビル16階16W4号室
TEL. 03(3348)4415 FAX. 03(3348)4416

事務局メール： saajjk1@titan.ocn.ne.jp

ホームページ　http://www.saaj.or.jp/

※ 会員専用メーリングリストで様々な情報提供を行っています。ご加入は owner-saaj@mla.nifty.ne.jpにお問い合わせください。また受信アドレスの変更時も手続が必要になりますので、上記アドレスまで連絡してください。

会報担当理事

竹下　和孝　んじゃろ監査事務所
富山　伸夫　富山システム監査事務所
吉田　裕孝　三井物産(株)
蓮見　節夫　蓮見システム監査事務所
水野　英治　東京都
力　利則　日本電気(株)

※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、執筆されたかたはお知らせ下さい。

会報担当メール： saaj-kaihoh@egroups.co.jp