SAAJ 日本システム監査人協会報

自治体に対するアンケート集計結果

法人部会

本年１月～２月に自治体を対象に実施致しましたアンケート結果の集計・分析作業が終了いたしましたので、その結果をご報告致します。

法人部会および日本システム監査人協会では、このアンケート結果を今後の啓蒙・普及活動の参考にさせていただきたいと考えています。

回収結果

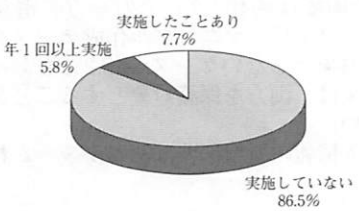
配　布：143自治体
（東京特別区、東京・神奈川・埼玉・千葉の市）
回　答：52自治体
回答率：36.4%
回答部門別内訳
情報処理担当部門：42
監査担当部門　：4
両　部　門　：6

● 法人部会コメント
過去に行ってきたアンケートに比べ、高い回答率となった。特に東京都の特別区では、23区中14区から回答をいただき、回答率は60.9%と非常に高い数字となった。
アンケートは情報処理担当部門、監査担当部門の両方に送り、「相談の上で回答していただきたい」としたが、回答は情報処理部門からが大半であった。後の結果と合わせてみると、自治体の監査担当部門では、システム監査についての意識はあまり高くないといえる。

I. システム監査に関して

1. システム監査の実施

a．実施していない。　45
b．年１回以上実施している。　3
c．実施したことがある。　4



実施していない理由
検討中　7
人材がいない　5
経費面の理由　3
必要性を認めない　3
システム評価を実施　2
自己管理による　1
全面外部委託　1

2. システム監査の実施体制（複数回答可）

a．自組織のシステム監査部門　1
b．自組織の監査／検査部門　1
c．自組織のシステム部門　1
d．外部委託　5

3. システム監査の実施で最も重視している観点

a．信頼性　2　b．安全性　4
c．効率性　3
d．その他　2
（運用とメインテナンス、プライバシ保護条例の遵守）

4. システム監査の予算計上

a．いる　3
（概算予算金額　30万円、100万円、500万円）

5. システム監査の浸透

a．思う　2　b．思わない　6

思わない理由
システム監査の必要性が知られていない
システム監査の知識不足
情報処理自体が専門視されている

6. 安全性の監査で重要視しているテーマ（複数回答可）

a．災害対策及び災害復旧計画　7
b．外部者によるネットワークへの不正アクセス　2
c．組織内部者による不正アクセス　2
d．プライバシ情報保護策　8

7. 信頼性の監査で重要視しているテーマ
(複数回答可)

a．システムのバックアップ対策	8
b．2000年問題や新郵便番号へのシステム対応	1
c．エンドユーザの教育	2
d．アウトソーシング先の信頼性	4
e．その他	1

(準拠性)

8. 効率性の監査で重要視しているテーマ
(複数回答可)

a．C／Sシステム等への切換えの投資評価	3
b．システムのコストパフォーマンス評価	7
c．ソフトウェア管理コストの評価	2
d．住民向け情報発信コストの評価	1

◆システム監査について寄せられた意見

・システム監査の実施によるメリット、デメリット、経費について、またどのような課題があるかを知りたい。
今後の方向性は？

・話題になっている割に実態がよく分からない。ハード、ソフト以外の各業務アプリのシステム監査については、実際にはむずかしいと思う。

・他自治体、特に市町村(本市と同程度規模のところがより良い)の状況などについて、ご教示いただきたい。

・システム監査に注目しているが、システム監査制度を網羅的に把握していない状況である。システム監査制度の効果と経費などの研修などの実施を希望します。

● 法人部会コメント
システム監査の実施経験のない自治体が86.5%である。アンケート先の自治体の規模にバラツキはあるものの、総じていえば、自治体にシステム監査は普及していないといえる。
未実施の理由に「人材難」や「予算不足」があがっており、中には「必要性を認めない」という回答もあった。
小規模な自治体であれ、取扱っている情報はプライバシに係わるものも多く、情報の機密性の保護や災害時の対策は自治体にとって非常に重要な問題である。一旦事故が起きると大きな問題になるので、情報セキュリティを確保するシステム監査の有用性を再認識し、まず、手のとどく範囲から実施していただきたい。

II. 個人情報保護および情報公開に関して

1. コンピュータが取り扱う個人情報の所管部署

a．業務システムごと	38
b．統一部署	10
c．業務システムごとと統一部署の両方	2
d．決まっていない	2

2. 個人情報保護条例の制定

a．はい 45 c．いいえ 7

2－1．条例の対象部門(複数回答可)

a－1．公的部門のみ	31
a－2．民間部門のみ	1
a－3．公民両方	12

2－2．保護対象データ(複数回答可)

b－1．電子計算機処理データのみ	19
b－2．マニュアル作成データのみ	2
b－3．両方	24

3. 情報公開条例の制定

a．はい 37 c．いいえ 15

3－1．公開の対象となる機関(複数回答可)

a－1．首長及び部局	37
a－2．議　会	28
a－3．教育委員会	37
a－4．選挙管理委員会	36
a－5．人事委員会	8

3－2．請求権者

b－1．住民に限定	0
b－2．住民や勤務者に限定	26
b－3．限定していない	9

3－3．これまでの公開請求

c－1．あ　り	32
c－2．な　し	3

公開請求文書例
市内小中学校長期欠席者数、教育委員会議事録、食糧費の支出に関するもの
業者登録名簿、市長交際費関係書類、契約

● 法人部会コメント
今回は首都圏の調査であり、86.5%の自治体で「個人情報保護条例」が定められており、全国的に見て非常に高い結果となった(全国では約40%)。その一方、電算処理データ主体でマニュアル作成データを保護の対象としないケースが42.2%もあった。本来は、両方を保護対象とすることが望ましい。
個人情報の所管部署は73%が統一されてお

らず、業務システムごとになっている。このことは、個人情報の管理の難しさを示している。
「情報公開条例」は71.2%が制定しており(全国で約12%)、対象機関は首長局部、教育委員会、選挙管理委員会がほとんどすべての自治体で公開対象となっている。また、公開条例を定める自治体のうち、86.5%が実際に公開請求を経験しているという興味深い結果となった。
ネットワーク化や情報公開の流れの中で、自治体としてもアウトソーシング先を含めた民間部門の個人情報保護は取組みが急がれる課題といえる。

III. 業務の外部委託と共同センターに関して

1. 情報処理業務の外部委託状況

a. 委託せず、すべて内部要員で処理している。 2
b. 内部要員による処理が主であるが、一部技術者の派遣を受けている。 12
c. 業務の一部を外部に委託している。 31
d. 情報処理業務をすべて外部に委託している。 6

2. 委託先(複数回答可)

a. 自治体の共同センター 1
b. 自治体の関連・関係企業 2
c. 一般の民間情報処理企業 31
d. 自治体関連・関係企業と民間の両方 4

3. 委託業務の内容(複数回答可)

a. システム企画業務 9
b. システム設計業務 28
c. プログラム開発業務 35
d. システム運用業務 29
e. システム保守業務 30

4. 委託業務契約について

4－1. 委託先との契約に委託先の業務実施状況の検査規定を載せているか
a. はい 22 b. いいえ 15
4－2. 委託先との契約に機密保持(セキュリティ)に関する規定を載せているか
a. はい 39 b. いいえ 1
4－3. 委託先との契約に委託先からの納品物の検収手続を載せているか
a. はい 29 b. いいえ 7
4－4. 委託先との契約に委託先へのシステム監査の実施を載せているか
a. はい 4 b. いいえ 34

5. 委託先の業務の検査、成果物受け入れの検収、およびシステム監査の実状

5－1. 委託先の業務実施状況の検査の実施
a. はい 26 b. いいえ 11
5－2. 成果物の検収の組織的な実施
a. はい 25 b. いいえ 11
5－3. 委託先に対するシステム監査の実施
a. はい 3 b. いいえ 35

● 法人部会コメント
すべてを内部要員で処理しているケースは少なく、一部を委託しているケースを含めると95%の自治体が外部に業務委託している。進歩の著しい情報技術を自治体内で習得するのは、難しくなってきており、人材のローテーションの面、コストの観点から見ても、外部委託のメリットは大きいと思われる。
民間に業務を委託しているケースが95%を越えており、ほとんどが機密保持の契約をしている。しかし、システム監査の実施を委託契約に盛り込み、実施しているケースはほとんどない。
今回制定された「個人情報保護ガイドライン」により、外部委託先(民間)での情報漏洩防止のためのシステム監査の認識は高まると思われるので、外部委託契約にシステム監査の実施を盛り込み、実施することが望ましい。

IV. 災害対策に関して

1. 「住民記録システム」のプログラムおよびデータのバックアップの採取

プログラム		データ	
a-1. 毎日	15	b-1. 毎日	45
a-2. 週1回以上	14	b-2. 週1回以上	3
a-3. 月1回以上	13	b-3. 月1回以上	2
a-4. 年数回定期的	2	b-4. 年数回定期的	1
a-5. 不定期	4	b-5. 不定期	0

2. 「住民記録システム」におけるデータの外部保管

a. 行っている 47 b. 行っていない 4

保管場所
a－1. 同一建物内 6
a－2. 同一敷地内 0
a－3. 敷地外 41

保管媒体
b－1. 磁気テープ 44 b－2. FD 0
b－3. MD 0 b－4. CGMT 2

外部保管におけるセキュリティ状況
c－1．関係者以外、絶対にアクセス不可 14
c－2．関係者以外でも許可をとればアクセス可 3
c－3．誰でもアクセス可 0
c－4．外部第三者に保管を委託 30

3. 本番システムが災害、重大障害で使用できなくなった場合の対応

a．業務を代替できる(バックアップ)施設・設備を、自組織体内に持っている。 7
b．外部の団体・業者との契約により、バックアップ施設・設備を確保している。 12
契約先の団体・業者は
b－1．他自治体 5 b－2．業者 6
c．バックアップ施設・設備を持つ計画がある。 5
d．バックアップは考えていない 24
理由 経費 11
マニュアルで対応 2
検討予定 1
未対応 1
不要 1

4. 緊急事態を想定したコンティンジェンシ・プラン

a．策定している 14
コンティンジェンシ・プランに基づいた訓練
a－1．定期的に行っている。 3
a－2．非定期だが行っている。 5
a－3．行っていない。 6
理由 見直し 1
経費 1
b．策定を計画している。 8
c．策定する予定はない。 25
理由 検討予定 2 対応困難 2
個別対応 1 現実とのギャップ 1
余裕なし 1 できない 1
未対応 1

● 法人部会コメント
バックアップは概ね短いサイクルでとられている。「年数回しかとらない」、「プログラムのバックアップをとっていない」などのケースは、特殊な事情があるのではないかと考えられる。
バックアップデータの外部保管はほとんどの自治体で行われているが、その際に情報漏洩防止策を講じる必要があり、この点のチェックがシステム監査の対象となる。
バックアップデータの外部保管を行っていない自治体は、そのことの必要性を再認識していただきたい。
コンティンジェンシープランの策定は、計画中を含めても半数に満たず、情報システムのリスク管理の重要性の認識を高めることが期待される。

V. 2000年問題に関して

1. 2000年問題への対応状況をお聞きします。

a．既に対応済み 5
b．現在対応作業中 31
c．これから対応する予定 16
d．対応はしない 0

2. 2000年問題への対応内容はどうですか。

a．現行プログラムの修正のみを行う 37
b．ほとんど新規にシステム開発する 3
c．他の案件と合わせて改良する 7
d．その他 3

3. 2000年問題への対応体制はどのようなものですか(複数回答可)。

a．社内の担当部署が対応 18
b．社内プロジェクトで対応 1
c．アウトソーシングで対応 14
d．社内＋アウトソーシング 12
e．その他 4

4. 2000年問題対応の費用の概算を教えて下さい。

a．1億円以上 5
b．5千万円以上～1億円未満 1
c．1千万円以上～5千万円未満 16
d．1千万円未満 24

5. 2000年問題の解決を主導したのはどなたですか(複数回答可)。

a．自治体の長 5
b．議会 0
c．監査委員 0
d．住民 0
e．自治体の情報システム部門長 40
f．その他 3
(業者)

◆2000年問題について寄せられた意見
・要員不足から修正費が高くなっている。数年前からこの問題に取り組んでおけば、もう少し安い費用で対応可能だったことを考えると、情報システム業界の対応に疑問を感じる。
・第1に、複数年に分散させた対応が可能であったが実現されなかったことと、第2に、この課題をきっかけに資産管理を行えなかったことが残念である。
・対応が必要となるプログラムの本数が膨大であり、業者に委託した場合、数千万円の予算が必要であったことが、自己開発プログラムが多く、金銭的にも予算化が困難であったため、すべて職員によって対応することとした。また、7桁問題とも時期的に重なったため、要員確保が困難であった。

● 法人部会コメント
対応が必要であるとの認識は浸透している。しかし、対応策の実施状況はあまり良いとはいえず、回答時点(98年2月)で対応済みが10%、1998年中に対応が終わるところを含めると対応済みは45%に過ぎず、対応が遅いと考えられる。
対応内容は、「現行プログラムの改訂で我慢する」という答えが多い。古いシステムは捨てて、新規開発、または再構築をするという回答件数は3件であり、予算や時間の制約があるため、現行の手直しで終わってしまうところが多い。民間企業ではシステム再構築というケースが多いので、それに比べてかなり意識が違っているように感じられる。

VI. 郵便番号7桁対応に関して

1. 郵便番号7桁対応への対応状況

a．既に対応済み	22
b．現在対応作業中	26
c．対応予定	4
d．対応はしない	0

2. 郵便番号7桁対応への対応内容

a．現行プログラムの修正のみ	42
b．ほとんど新規にシステム開発	2
c．他の案件と合わせて改良	5
d．その他	3

3. 郵便番号7桁対応への対応体制はどのようなものですか(複数回答可)。

a．社内の担当部署が対応	21
b．アウトソーシングで対応	14
c．社内+アウトソーシング	14
d．その他	2

4. 郵便番号7桁対応の費用の概算を教えて下さい。

a．1億円以上	0
b．5千万円以上～1億円未満	1
c．1千万円以上～5千万円未満	20
d．1千万円未満	27

5. 郵便番号7桁対応の解決を主導したのはどなたですか(複数回答可)。

a．自治体の長	2
b．議会	0
c．監査委員	0
d．住民	0
e．自治体の情報システム部門長	39
f．その他	5

◆郵便番号7桁対応について寄せられた意見
・郵便料金の値下げなど利用者のメリットが欲しい
・費用対効果が得られない
・郵政省の費用削減を補助金として交付して欲しい
・メリットがないが、公共機関として協力する
・マスコミでの広報では7桁対応しないといけないように受け取られ不愉快
・バーコード対応で郵便料金削減を見込んでいる

● 法人部会コメント
郵便番号7桁化については、上記の通り、「費用対効果が得られない」、「メリットはないが公的機関として協力する」などの意見が数件あったものの、アンケートに回答した52自治体すべてが対応していることが分かった。

第58回月例研究会報告

開　催　平成10年６月24日(水)
場　所　機械振興会館会議室
テーマ　「システム監査制度のあり方」
講　師　通産省情報処理振興課安全指導係長
　　澤野　弘　氏

No.526　富山　伸夫

はじめに

今回は、協会でご指導を受けている通産省の澤野氏にお願いして、システム監査の普及に関し、現状認識と今後のあり方について、会員の方々とデスカッションを行うことを目的に開催したところ、大勢の参加と積極的な発言があり、充実した研究会となりました。

澤野氏講演要旨

１．現状認識

①システム監査基準の認知度および利用度は、大企業では高いものの中規模以下の企業では高いとは言えず、基準の利用状況は平均で30%程度に留まっている。
②システム監査技術者試験の志願者数の推移は、減少傾向にある。試験区分の拡大にともない、他の技術者試験に流れたことによるものも理由の１つであろうが、試験内容がニーズに合っているのか精査する必要がある。
③システム監査企業台帳制度は、91年に創設され、平成９年で64社の登録がある。500部作成し、主な図書館、商工会議所に配布しているが、これの利用率や認知度につき評価する必要がある。
④システム監査人協会は、87年に設立されているが、合格者数に比し個人会員の組織率は16%強にとどまっている。協会として、システム監査の普及にどう取り組んでいくのかが今後の課題である。
⑤システム監査学会は、システム監査の理論的体系構築を議論するところと認識しており、実務者団体としてのシステム監査人協会との連携を期待している。しかし、日本学術会議での認識のされ方を見ても、学会レベルにおける、システム監査に対する認識の低さがうかがわれる。
⑥システム監査白書は、隔年に発行されてシステム監査の現況を示しており、行政が施策を立案する上で参考にしているが、今後は、何を訴え、誰に読ませようとするのかを、より明確にする必要がある。
⑦システム監査Ｑ＆Ａは、システム監査を行うプロのためのツールとして用意されたものであり、システム監査の普及に役立つよう期待している。

２．今後のあり方(活性化の方策)

・研究発表会等をとおして技術のレベルアップを図るとともに、システム監査に対するＰＲ活動が必要であると認識している。そのためのイベントを考えることも必要だ。現行の施策についても、現状認識を踏まえて改善してゆく必要がある。
・システム監査制度の法制化については、以下の理由から、考えていない。
すなわち、システム監査の実施者により、アウトプット(監査結果)の品質にばらつきがあること、および、会計監査のように、処理(方法)が正しいか正しくないかという点について断定ができないことが挙げられる。
・システム監査の本来の趣旨は、情報サービス業の品質をよくすることにあり、今は自助努力で社会的気運を高めることが大切であると考えている。

３．システム監査の活用について

①ＪＩＳＡの勉強会などに出席して、システム監査に対する問題意識を伺うとともに、業界としてシステム監査に取り組むことの必要性についても問題提起をしているところである。
②システム監査に対する経営者の関心は、処理効率(コストパフォーマンス)、処理の正確性、安全性、代替手段等である。これらのニーズに対し、適切にミートするプログラムを提案することが求められている。
③現状のシステム監査に対する不満については、監査報告書の内容が期待と異なること、システム監査の結果明らかになった問題点を解決するためのコストがわからないこと、システム監査の実施者により監査結果のバラツキが大きい、などがある。これらについては、普及が進めばもっと顕在化してくると思われる。
④今後の進め方としては、意識調査、課題の抽出、意見交換会、セミナーなどをつうじて、システム監査の有効性を訴えていくことが大切である。
⑤システム監査の関連動向として、一つに、コンピュータ保険がある。加入時の査定にシステム監査が行われる。二つ目として、プライバシーマーク制度がある。認定を受けるためには、システム監査を行っている

ことが必要である。この制度は比較的取得し易く、普及すると思われるので、タイアップ等考えると有効かもしれない。

最後に、日本におけるシステム監査は、総論では必要性を認めつつも、実行が伴っていないのが現状であり、セキュリティ意識が薄い。欧米では、ＣＩＯを置いて責任者を明確にしているし、責任を果たさないと株主から突き上げられる。今後、日本においても情報漏洩に対する訴訟を起こされることも考えられるので、企業としてどの程度のセキュリティ対策が必要か、システム監査を実行する立場からも検討しておくことが必要である。

以上、個人的な感想を述べたが、本日は、皆さんのご意見を多く伺いたいと思っている。

質疑応答および意見発表

山口氏：個人でシステム監査をやっている。一部上場企業でトップが外部からの監査で見て貰えといっても、監査役、担当役員が反対する。やらざるをえないように規制することも必要ではないか。

橘和氏：金融検査部の通達を見たが、「システム監査を含む自己責任原則による内部監査の結果を確認すること」などとある。多少流れが変わってきている。

澤野氏：世の中は規制緩和の方向に進んでおり、なるべく民間の自助努力に任せたいと思っている。また、システム監査は、ユーザーによって期待する監査内容が異なるとともに、システム監査の実施者によっても深さが異なる。
通産省で実施している情報処理サービス業情報システム安全対策実施事業所認定制度の３年ごとの更新審査時に、システム監査の所要日数と人数の報告があるが、100人日かけている事業所もあれば、２人日で済ませているところまでバラツキが大きい。
この安全対策実施事業所は、銀行の情報処理センターでも取得する動きがあり、地方自治体における委託事業所の選定基準に使われている例もある。

三谷氏：自助努力でやっていてもどの程度か、協会などでクラス認定する方法もある。

荒川氏：システム監査のバラツキが大きいのは、抽象度が高いからだ。金融検査部から監査の有資格者の教育方法を問いあわせてきている。
ISO9000の認証をソフトハウスが受けると、この審査はシステム監査そのものだが、審査員はシステム監査を全然知らない人がほとんどである。
この認証が欲しいのはお墨付きが貰えるからだ。
金融機関にシステム監査のＤＭを送っても、外資系は敏感だが国内は鈍感だ。

山口氏：システム監査企業台帳で、有資格者数が多い会社、少ない会社とばらついている。会計事務所で行っているシステム監査には、お座なりでなっていないものがある。

澤野氏：システム監査企業台帳は、いわばイエロブックのようなイメージでとらえており、できるだけ多くの選択肢をユーザーに与えることが重要と考えている。
将来的には、web等の電子媒体をとおして提供していきたい。

梅津氏：監査人の資質のバラツキが大きいということだが、報告書にしてもこのクラスならこれくらいという雛形が必要だ。監査の項目にしても、効率性・有効性など誰がやってもそこそこで専門性が見えない。安全性・信頼性には技術的専門性がある。監査項目の絞り込みが必要となる。

澤野氏：最近では、セキュリティコンサルタントなど、安全性の評価がホットになってきている。

三谷氏：効率性は、システム監査の１つの領域として、ユーザを意識していけばいい。

橘和氏：システム監査がコンサルティングになるのは、基準の定義からも当然のことだ。有効性を中心において信頼性、安全性も見ていくことになる。

山口氏：決算資料が翌月末にしか出ないという会社があった。トップに翌月４の日にしましょうといって、いろいろ監査していったら、10の日には出来るようになった。
システム監査はここまで踏み込むべきだと思う。

森末氏：セキュリティに特化するのは難しい。セキュリティホールを見つけるなど、ＯＳ通信にまたがるようなものは特にそうだ。2000年問題でもＯＫの結論はだせない。細かいことではなく、改善方向の枠組みを見ていくことが重要だ。

澤野氏：最終的には顧客のニーズにあったサービスをしていくことが重要だ。今のキーワードは「セキュリティ」であり、不正アクセスやネットワーク脆弱性チェックの会社は10社以上もある。
ユーザーの要求にきめ細かく対応できるプログラムを用意することが重要である。

芳仲氏：新薬開発の関係で海外から監査にくるが、監査報告書を出さなければ安いな

どちぐはぐなものがある。また、厚生省のＧＣＰでも、「監査をやれ」、「モニタリングをやれ」と言ってきている。(注、GCP：Good Clinical Practice 臨床試験基準)

松枝氏：協会の事例研では有効性監査の事例が多い。クライアントのレベルに応じた改善提案を出している。先般98年度の実務手順書ＦＤを会員に配布した。これをベースに「実践マニュアル」の出版を計画中だ。

和貝氏：会計監査には、監査基準、企業会計原則、財務諸表規則などが整備されているが、情報システムにはシステム基準のようなものが見当たらない。

三谷氏：セキュリティのCC(Common Criteria)のようなデファクトな基準があればいい。

中野氏：情報システムの内部規定はない。システム監査基準に合わせて社内で作ればいい。平成５年に「情報システム規則集」を作ったことがある。

打矢氏：システム監査は、情報化社会の仕組みとして必要とされてきた。世の中のニーズに合わせていくこともあるが、なにかのお墨付きも必要ではないか。

岩田氏：コンサルタントをやっているが、システム監査は、情報システム部門やユーザ会などに対するＰＲが足りない。山梨のあるシステム部門は、システム監査は敵だと思っていたという。社長は外の話なら聞くからだ。

荒川氏：今、協会で組織委員会をもって、会員増加すなわちシステム監査活性化のための議論をはじめている。

澤野氏：システム監査は、本来、義務で受けるのではなく、良くしたいと思って外部にチェックして貰うことだ。ニーズがあってそれにミートさせればセキュリティビジネスは増える。経営者が何を期待しているか、情報システム部門からの説明だけでなく、外からも聞きたいと思っている。
いずれにしても、通産省としては、通産公報やweb掲載を含め、可能な限りシステム監査の普及に関してバックアップしてまいりたいと考えている。

中尾事務局長：大勢の参加と熱心な討議で大いに盛り上がり、有り難うございました。

(全員起立拍手)

第57回月例研究会報告

開　催　平成10年５月８日
場　所　機械振興会館
講　師　日本ノーベル(株)取締役副社長
　　菊本　正紀　氏
テーマ　「ISO9000品質システムの審査登録と維持」

No.526　富山　伸夫

講演要旨

１．ISO9000シリーズについて

ISO9000シリーズは、ISO／TC176で1987年に制定された品質に関する一連の国際規格であり、製品そのものの品質ではなく、製品を設計・供給するためのシステムが満たすべき要求事項を規定している。ここで、品質(Quality)とは、「あるものの明示された又は暗黙のニーズを満たす能力に関する特性の全体」として、定義されている。

シリーズとなっている規格の一番中心は、ISO9001である。これがフルスペックで、その他はサブセット(部分規格)と周辺的な規定がある。

「ISO9001：Quality systems-Model for quality assurance in design, development, production and servicing」
「品質システム－設計・開発、製造、据付け及び付帯サービスにおける品質保証モデル」

わが国の標準化は、JISの制定で推進されているが、ISO規格に対応して整合させることがWTO／TBT(World Trade Organization/Technical Barriers to Trade) 協定で義務付けられているので、実質同じ規格が定められている(JIS Z9900シリーズ)。(ISO9001の内容説明あり、省略)

２．品質システム審査登録制度について

品質システム審査登録制度には、次の４つの審査登録がある。

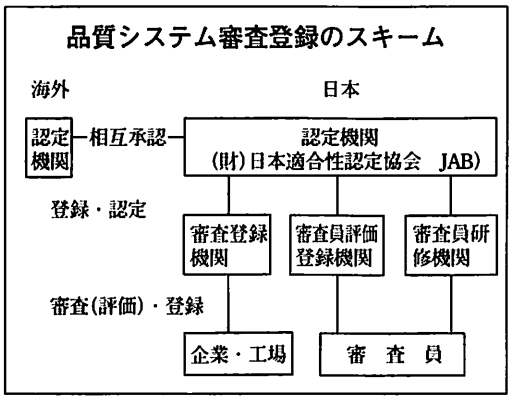
A．企業・工場等の品質システムがJIS Z 9901～9903(ISO 9001～9003)に適合しているかを、第三者機関である審査登録機関が審査し、適合している場合にはその企業工場等を適合供給者として登録・公表する。

B．審査登録機関が適切な能力を有していることを認定・登録・公表する。

C．審査員研修機関が適切な能力を有していることを認定・登録・公表する。

D．審査員が適切な資格および能力を有していることを評価・登録・公表する。

このスキームを図示すると次のとおりである。



ここで用語について説明すると、「登録」は米国系の用語法(「認証」は欧州系)で、認証とするとＰＬ法で認証者側も訴えられる恐れありということがあるようだ。

相互承認は、各国の認定機関間または審査登録機関の間で、相互に夫々が承認したものを承認することによって、別々に審査登録しなくてもよいという取り決めである。

品質監査(Quality Audit, ISO8402)は、「品質活動及びそれに関する結果が計画に合致しているかどうか、並びにこれらの計画が有効に実施され、目的達成のために適切なものであるかどうかを判断するために行う体系的かつ独立な審査」をいう。

審査には、予備審査、本審査、再審査(３年に１回)、維持審査(１年２回又は１年１回)がある。審査は、書類審査(品質マニュアル、手順書、品質記録)と実地審査があるが、日本では品質記録の習慣がないため厳しいものがあるようだ。

日本での導入の経緯は、EC統合やGATTの協定などをうけ、1991年以来若干の経過を経て、1993年11月、財団法人日本適合性登録認定協会(JAB)が設立された。ここで上記スキームにある業務を推進している。

3. 品質システム監査について

ソフトウエア分野における審査登録については、最初ISO9001はソフトウエアには向かないということで、ISO9000-3が作られたが、これはガイドライン(基準文書ではない)なので、実際はISO9001をソフトウエアに当てはめたガイド(日本科学技術連盟SPC見解)等により、審査登録機関の審査が行われている。

情報技術で認定された審査登録機関は現在７機関があり、受審登録した企業数は150社以上におよんでいる。情報技術はあまりなく、他産業の輸出や政府調達、自動車部品や大企業の購買管理に適用されだしているためである。

品質システム監査の指針は、JIS Z9911に規定されている。この第２部に品質システム監査委員の資格について、教育・訓練・経験・個人的特質・管理能力・能力の維持等細かい規定がある。

4. ソフトウエア・プロセス評価について

米国国防省が外注ソフト会社を審査するために、SEI(Softwear Enginering Institute)に委託して研究させたCMM(Capability Maturity Model)をモデルにSPA(Softwear Process Assessment)が、ISO/IECの作業部会WR10において、TR15504として検討されつつあり、今年度中に国際規格となる動きがある。

CMMモデルは５段階だが、SPAでは６段階を規定している。

レベル０： 不完全な(Incomplete)
レベル１： 実施された(Performed)
レベル２： 管理された(Managed)
レベル３： 確立された(Established)
レベル４： 予想できる(Predictable)
レベル５： 最適化(Optimizing)

ISO9000は、このレベルでいうと２と３の間位に相当する。SPAは、SLCP(ソフトウエア・ライフサイクル・プロセス)にそって、品質プロセスを細かく規定しようとしている。

日本ではNTTなどISO9000では物足りないとする企業が出つつあり、欧米カナダではSPAによる審査を考えるむきもあり、第２のISO9000になる可能性がある。

質　疑

Q：SPAとSPICEの位置づけは？
A：SPAは規格名、TR15504は規格No.、SPICEはこのための作業プロジェクト名です。
Q：ISO9000-3の内容は？
A：現在1997年12月に改訂された ISO9000-3は、9001をそのまま使用し、ソフトウエアのガイドを追加したもので、実際に審査に使われる事はないであろう。現在改訂中のISO9001はどの分野でも使えるものにしようとしている。
Q：ISO9000を取得することのメリットは？
A：ソフトウエアの手戻りコストをカウントし

てみる。Tick ITではソフトウエアの仕損費が20%と書いてある。品質プロセスを入れるコストは6～7%だが、9001のどこを重点にやるかを見定めて、第三者にプロセスが見えるようにしてゆくと、仕損費が減って大きなコストダウンになる。

Q：ISO9000では、どのあたりが重要か？

A：ロスコストは何であるか。自社を9000でマッピングしてみてどこが足りないか検討してみると、最小限の適用で効果が上がる。上流でのデザインレビューが非常に重要である。

Q：上流でレビューということだが、スパイラルとかパッケージを使った時などは？

A：納期の前にお客の要求定義がはっきり書けているかが問題だ。日本語の教育の問題もある。ユーザ要求がちゃんとあって、検証と妥当性確認を、手順を踏んでやってゆくことにつきる。

Q：TQCとISO9000を一緒にやったら？

A：日本では当然そうなる。TQMにはボトムアップもトップダウンもある。
農耕民族ではなあなあがきくが、狩猟民族では契約とか教育がなくてはやれない。システムの規定の仕方が文化の差を表している。

感　想

ISO9000による品質システム審査登録の全体像が明確となり、大変勉強になった。また、システム監査とからめて考えると、ソフトウエアの品質向上のための方向性が、より一層重要度を増して来ていることを痛感した。

公開鍵方式暗号化ソフト（ＰＧＰ）の使い方の紹介

セキュリティ・技法合同研究会

はじめに

最近話題になっている公開鍵方式の暗号化ソフトであるPGPをセキュリティ・技法合同研究会で研究してきた。入手も簡単で使い易く、研究会員同士で使えるようになったので紹介する。

1. ＰＧＰの背景

1.1　PGPとは何か?

PGP(Pretty Good Privacy)とは、Phil Zimmermannによって開発された暗号化ソフトであり、公開鍵暗号、共有鍵暗号、鍵の管理をサポートしている。これを使って、暗号化と電子署名ができるものである。

＜概要説明＞

共有鍵とは、対象鍵とも言われているが互いに共通の鍵を持って暗号/復号するものであり、アルゴリズムとしては、以下のものがある。

・DES(Data Encryption Standard)
　ANSI標準で56ビットの鍵を使用する
・トリプルDES
　上記のDESを異なる鍵で3回実行したもの。
・RC2,RC4
　RSA社が特許権を持つ暗号アルゴリズム
・IDEA(International Data Encryption Algorithm)
　スイスのチューリッヒ産でAscom-Techが特許を持つが、フリーソフトやシェアウェアのソフトに使うことは自由。
・スキップ･ジャック
　アメリカの国家安全保障局(NSA)が民間向けに開発したアルゴリズム。

公開鍵とは2つの鍵で、どちらかで暗号化すれば他方の鍵でしか復合化できない方式で、非対称鍵ともよばれる。この一方を公開鍵として広く世の中に知らしめる。(知らしめる方法とそれの本人確認については次回の機会に)。アルゴリズムとしては下記のものがある。

・Diffie-Hellmanアルゴリズム互いにセッション鍵を生成することから始める方式。
・RSAアルゴリズムPGPに使用されている方式

他にも最近では楕円曲線などの方式があるらしい。

1.2 PGPの手順

さて、PGPの手順は以下の通りである。
まず、共有鍵方式の鍵を生成する。PGP国際版の場合上記のIDEAの鍵を生成して、それで送るべき電文を暗号化する。
次に相手の公開鍵を手に入れて、それで上記のセッション鍵を暗号化する。
上記の共有鍵方式の暗号化された電文と、公開鍵方式で暗号化されたこの電文を解くためのセッション鍵の両方を送る。
受け取った方は、自分の秘密鍵でセッション鍵を取り出す。
このセッション鍵で、暗号化された電文を復号化する。

PGP自体は上記の様に共通鍵方式と、公開鍵方式の両方を使用している。

この章の目的は、手順を詳しく説明することではなく、PGPが提起している問題を記載することにある。特許の問題、輸出規制の問題などを説明するために、簡単な手順を説明させてもらった。従って、電子署名の方法などについては割愛させてもらう。

1.3 PGPが提起している問題

PGPが提起している問題は下記の2(3かも)つである。

・国家の安全(公共の安全)とプライバシー
・輸出規制と特許
・(フリーソフトのあり方)

①国家の安全とプライバシー

暗号化された通信を行うことは日本では問題がないが、無線で暗号を使うことは違法である国がある。米国の場合は、国家安全の為に(又は、犯罪捜査活動の為に)、米国連邦政府は一定の手続をとれば盗聴ができる為の通信機器を設計する様な法案が通った。(いわゆるデジタルテレフォニ計画)。すなわち全てに通信機器に上記のスキップジャックという機密のアルゴリズムを持ったクリッパーを通信機器に付けそれを解く鍵は政府が寄託するという方式をとる。現時点ではどうなっているのか調査していないが、下記のサイトなどでは、メディアを使った反対運動などが見られる。(自宅の鍵を、政府に預けますかというスローガンを見た。)

http://www.computerprivacy.org/

従って、PGPなどの強力な暗号化ソフトが容易に使えると言うことは政府にとって大きな脅威となっている。

プライバシーと公共の安全、さて、あなたならどちらの立場に立ちますか?

②特許と輸出規制

RSAのアルゴリズムは特許をアメリカ国内でとっている。従って、アメリカ国内ではPGPはRSAのライブラリーを使う必要がある。しかし、アメリカ、カナダ以外の国では特許として成立していない。これは論文等で先に発表されており、公知の事実であるということで成立していない。
また、暗号自体はアメリカでは武器であり輸出規制の対象となっている。従って、共有鍵のある一定の長さ以上(RC2, RC4)のものは輸出できない。
では、何故、我々がPGPを使えるのか?
それは、まずPGPの公開鍵方式の特許はアメリカ(カナダ)以外では成立していないので、アメリカで使用するのでなければ問題はない。では、どうやってアルゴリズムを持ち出したのか。一番はじめはネットを通じて漏れ出た。(これは違法らしい) 今では、アルゴリズムを出版しそれを外国でボランタリーでOCRで読ませて作られている。(本の輸出は問題とならない)
では、共通鍵方式は、上記のスイス産のIDEAを使用するので輸出規制にはかからないと言う仕組みになっている。IDEA自体は商用以外ではフリーである。(商用に使う場合は、IDEAの特許料を払う必要がある。)これがPGP国際版の仕組みである。
逆にアメリカではRSAライブラリーをライセンス供与された所のものを買うか、MITのライブラリーでフリーのものを使ったPGPを使うこととなる。
国際版と、アメリカ版(カナダ)ではこの様な違いがあるが原理は同じなので互換性が保証されている。

この様に、PGPが提起している問題は多岐にわたっている。単にPGPを使うだけでなく、この裏に潜んでいる問題点を吟味する必要がある。監査人協会の方々が使われる場合、フリーなソフトがあるという認識だけでなく、この問題を議論していただければと考える。

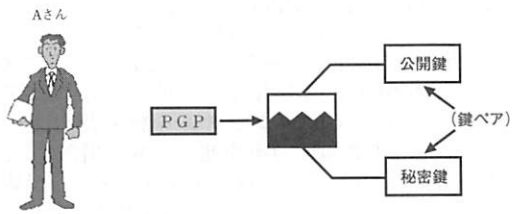
閑話休題
何故、Pretty Good Privacyという名前なのか?
Zimmermannがラジオ番組「Prairie Home Companion」のファンであり、そのスポンサーが「Ralph_s Pretty Good Groceries」だったからだそうだ。

2. ＰＧＰで出来ること

(1)メールの秘匿と認証が出来る。
・メールの暗号化
(第三者には秘密が守られる)――――秘匿
・メールの電子署名(途中で改竄されてないこと及び確かに本人からのメールであることが証明出来る)――――認証
認証については、次号の会報で紹介する。
(2)秘匿はどうやって行うのか。
PGPを使った秘匿の方法を以下、記述する。

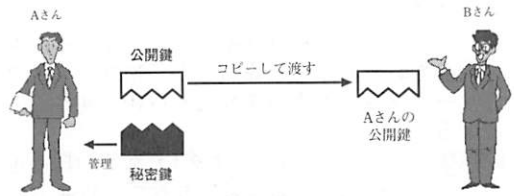
① ＡさんはＰＧＰで公開鍵と秘密鍵の鍵ペアーを生成する。

図1　鍵ペアの作成



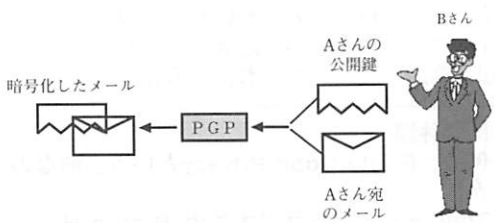
② Ａさんは公開鍵を送信相手(Ｂさん)に渡す。秘密鍵は他人に見られないよう厳重に管理すること。

図2　公開鍵を相手に渡す



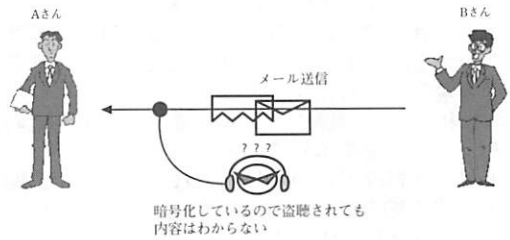
③ Ｂさんは、Ａさんの公開鍵でメールを暗号化する。(ＢさんもＰＧＰが必要)

図3　暗号メールの作成



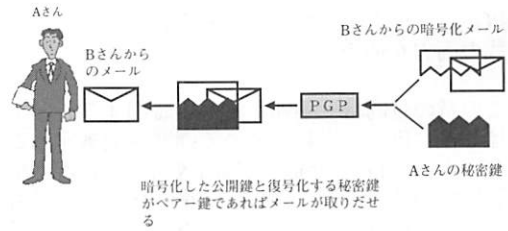
④ Ｂさんは暗号化したメールをＡさんに送信する。
送信は一般のメールソフト(何でも良い)を使用して行う。

図4　暗号メールの送付



⑤ Ａさんは、受け取ったＢさんからの暗号メールを自分の秘密鍵を使って復号化する。

図5　暗号メールの解読



3. ＰＧＰを使ってみよう。

3.1　ＰＧＰの入手

(1)国際版PGPのホームページ　http://www.pgpi.com からダウンロードする。
(2)プログラム名：PGP553I-win95nt.exe (自己解凍型の圧縮プログラム)の最新バージョン5.5.3iをノルーウエーのサイトからダウンロードする。
(注)・非商用利用の場合は無償である。
・国際版はバージョン番号にｉが付いている。

3.2　鍵ペアの生成

(1)自己解凍したらソフトの使用許諾の確認があり、鍵の生成が始まる。
(2)画面に従い順次、次の項目を入力する。
①名前、メールアドレス
②鍵タイプ――DSS選択
③鍵サイズ――2048選択
④鍵有効期限――Never expires選択
⑤パスフレーズ(パスワードとして使用する長い文章)
(同じものを二回入力するので注意が必要)
⑥Send my key to the keyserver now　は選択しない。
⑦マウスを動かし乱数生成。
(3)鍵ペア(公開鍵と秘密鍵)が作成される。
(4)タスクバーにアイコンが登録される。今後は全てこのアイコンを使う。

3. 3 暗号メールのやりとり

3. 3. 1 準 備

暗号メールをやり取りする前に、PGPのインストールが完了していることを確認する。PGPをインストールすると、「PGPtools」というプログラムが登録される。このツールボタンを使って暗号化と復号化を行う。

図6 PGPtools ボタンの説明

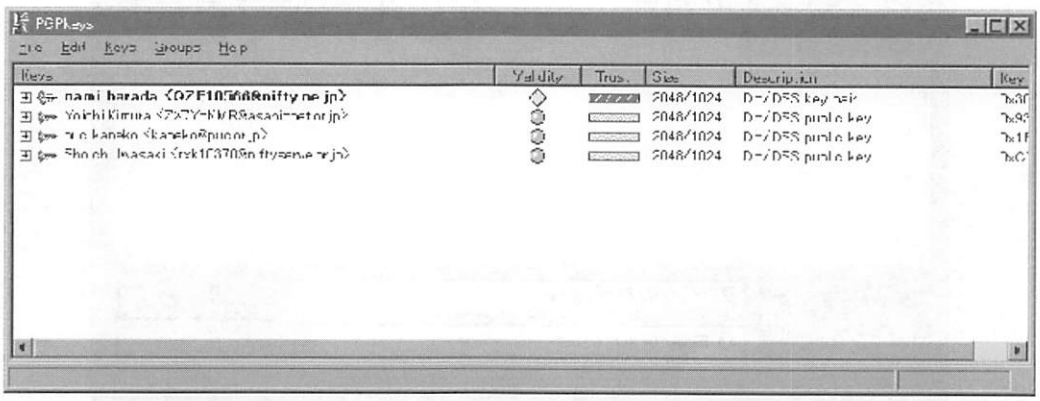
番号	名称	機能
①	鍵ホルダーの起動	PGP鍵ホルダーを起動する。
②	ファイルの暗号化	ファイルを暗号化する。
③	署名ファイルの指定	署名するファイルを指定する。
④	署名＋暗号化	署名するファイルを指定して暗号化する。
⑤	暗号ファイルの復号化	暗号ファイルを復号化する。
⑥	ファイルの削除	ファイルを削除する。

3. 3. 2 自分の公開鍵を送る

暗号メールをやり取りするには、事前に自分の公開鍵を相手に送っておく必要がある。自分の公開鍵を送る方法について紹介する。

(1)「PGPtools」から「鍵ホルダー」を起動(図6の①をクリック)する。(図7の画面が出てくる。)

図7 鍵ホルダーの画面



(2)一覧から自分の鍵を選択する。
(3)タイトルバーの[Edit]－[Copy]で、自分の鍵をクリップボードにコピーする。
(4)メールソフトなどで、自分の鍵を挿入したい箇所で[貼り付け]を実行する。すると、以下のようにクリップボードから自分の公開鍵が貼り付けられる。

```
----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 5.5.3i for non-commercial use <http://www.PGPi.com>
mQGiBDVBOasRBADuAko.j72xw12hKhGOwsdlvDXtgM66F+5bGSheFZ106nL8PY6W
WAFO1FqacldqdqY4LvRPGbTvwppC/sVQZeIkZ8kYmBL83/B9iS4UuqqD7MZ6hT3X
                              :
—END PGP PUBLIC KEY BLOCK—
```

※ 例のように、相手へのメールに貼り付けた結果、-BEGIN PGPの後が、PUBLIC KEY BLOCK になっていることを確認する。

(5)当該メールを相手に送信する。

3. 3. 3 相手の公開鍵を教えてもらった時

暗号メールに先立って、メール相手の公開鍵を教えてもらい、自分の鍵ホルダーに登録しておく必要がある。メール相手の公開鍵を教えてもらった時の方法について紹介する。

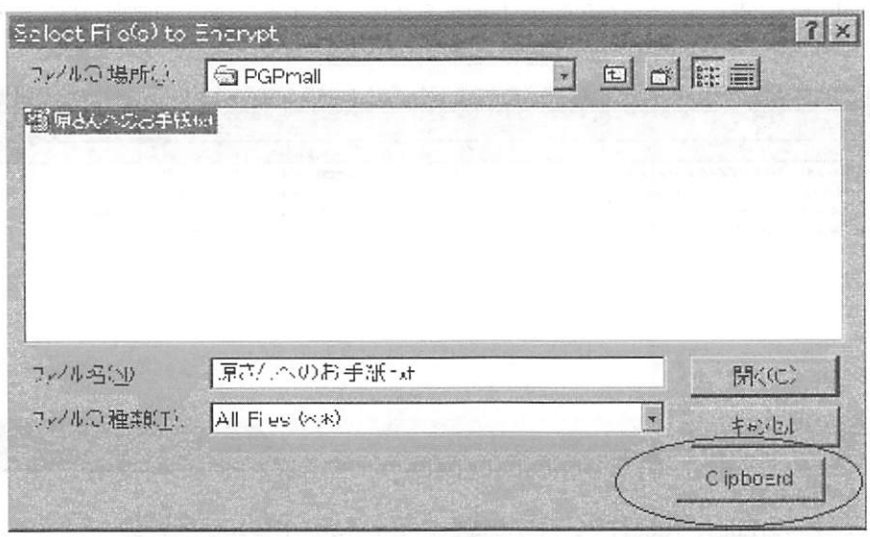
(1) メールなどから相手の公開鍵をコピーする。
—BEGIN PGP PUBLIC KEY BLOCK—から
—END PGP PUBLIC KEY BLOCK—までを、この行も含めてコピーする。
※この時、BEGINとENDの行もコピーする。
(2) 「PGPtools」から「鍵ホルダー」を起動(図6の①をクリック)する。(図7の画面が出てくる。)
(3) タイトルバーの[Edit]－[Paste]を実行すると、クリップボードから相手の公開鍵が取り込まれる。
(4) 鍵ホルダーの一覧に、今もらった相手の公開鍵が登録されていることを確認する。

3. 3. 4 暗号化したメールを送るとき

いよいよ暗号化メールの送信である。暗号化したメールを送る方法には、いくつかの方法がある。ここでは、「クリップボードの中身を暗号化する方法」と「ファイルを指定して暗号化する方法」の2つについて紹介する。ここに挙げた以外の方法や操作もあるので、各自で試してみてほしい。

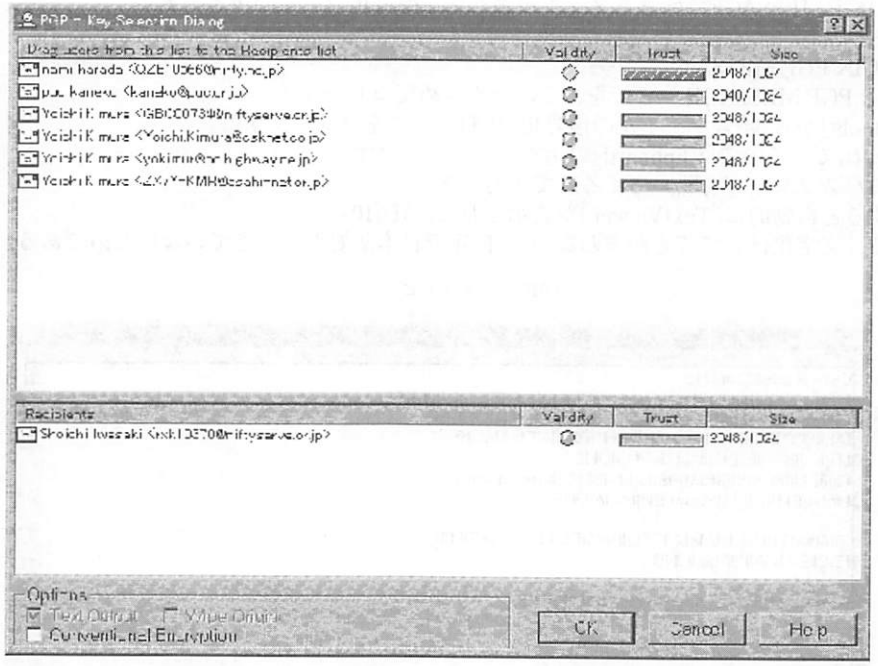
◆クリップボードの中身を暗号化する方法
(1) 暗号化したいメールを作成し、本文を範囲指定して[コピー]をし、クリップボードに入れる。
(2) 「PGPtools」から「ファイルの暗号化」を起動(図6の②をクリック)する。
(3) 図8の指定ウィンドウが出てくるので、右下の「Clipboard」ボタンをクリックする。

図8 暗号化ファイルの指定ウィンドウ



(4) [PGP Key Selection Dialog](図9)が出てくるので、送る相手を上のウィンドウからドラッグして下のウィンドウに入れる。

図9　PGP Key Selection Dialog



(5) 右下のＯＫをクリックする。
※この時何もおきないが、クリップボードの中には暗号化されたテキストができている。
(6) メール本文に貼り付けを実行する。(各メールソフトにて実行する。)
以下のように—BEGIN PGP MESSAGE—で始まり—END PGP MESSAGE—で終わる文字列が展開されれば完成である。

```
—BEGIN PGP MESSAGE—
Version: PGPfreeware 5.5.3i for non-commercial use <http://www.pgpi.com>
qANQR1DBwU4D3eJSyW4cbxgQCADcYrMrQStpWLMG/zKyi6NH9CrUxRSnfMg9wIzR
+re/lZCM7f/pYYbUB77xaBsXKTqZjREoII+4MwtJw1p8TBmIHeKHlFpN6SGAzhi+
                    :
hOSqGKvGQOQ6kOb5p8/ffYzl7uiZg3myzgNxzTok9uqTRlHO/0yXhd+I5jEON4tx
djHxMWH6XQSJHIhkAEwwfCLdbW7vAw==
=PST0
—END PGP MESSAGE—
```

(7) 相手にこのメールを送る。

◆ファイルを暗号化して添付する方法
※送るファイルは、表計算シート、図、写真、ワープロ文書など何でもよい。
(1) 送りたいファイルをあらかじめ作成して保存しておく。
(2)「PGPtools」から「ファイルの暗号化」を起動(図6の②をクリック)する。(図8が出てくる)
(3) 送るファイルを指定して「開く」をクリックする。
(4) クリップボードの場合と同様に、(4)、(5)、(6)を行う。
(7) 指定したファイルと同じディレクトリに、拡張子が「PGP」のファイルができているので、これを添付ファイルとして送信する。

3. 3. 5 暗号化したメールをもらったら(復号化)

BEGIN PGP MESSAGEで始まるメールが来たら、復号化ツールの出番である。

(1) 各メールソフトで、暗号化された範囲を選択し、コピーする。
—BEGIN PGP MESSAGE—から
—END PGP MESSAGE—までを、この行も含めてコピーする。

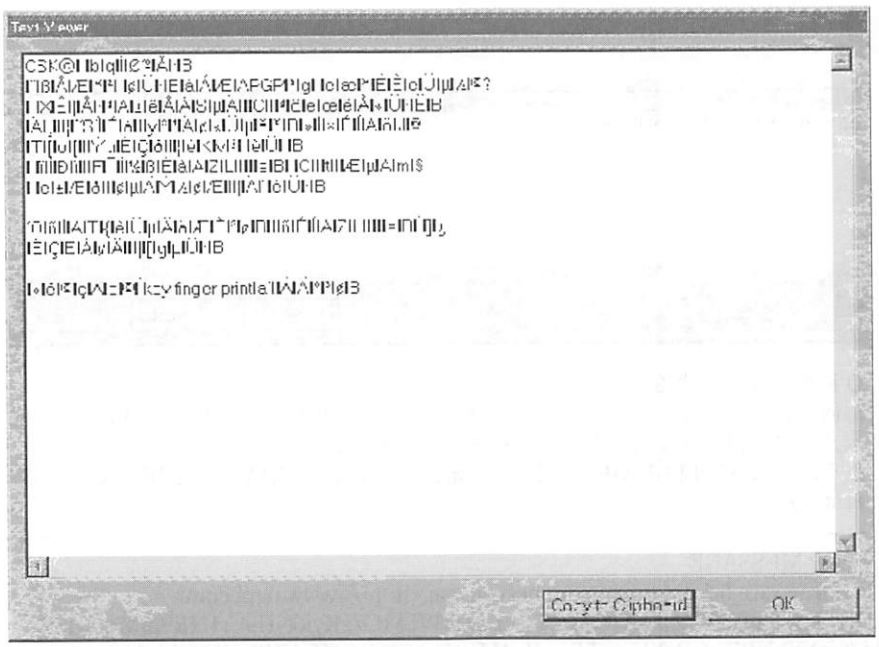
(2) 「PGPtools」から「暗号ファイルの復号化」(図6の⑤)をクリックする。
図8が出てくるので「Clipboard」のボタンをクリックする。

(3) 自分のパスフレーズを聞いてくるので入力する。

(4) 完了すると自動的に「TextViewer」が表示される。(図10)

※ この時、文字化けしててもかまわない。(PGPで日本語処理ができていないためである)

図10 テキストビューワー



(5) 右下の「Copy To Clipboard」をクリックして内容をコピーする。

(6) ワープロソフトや表計算など、当該ソフトウェアに貼り付ける。

おわりに

次回会報では、電子署名とフィンガープリント等について紹介する。

PGPの研究に当たっては、(有)バリアフリーの林様にPGPの一般的事項についてアドバイスを受けた。

本記事に関する問合せは、下記宛にお願いする。

nagao.kaneko@nifty.ne.jp

セキュリティ&技法研究会のホームページも参照いただきたい。

http://www.geocities.com/SiliconValley/Network/7626/

「情報セキュリティポリシーの必要性と策定方法」

～企業は従業員(人)による情報セキュリティの維持に、どう対処すべきか～

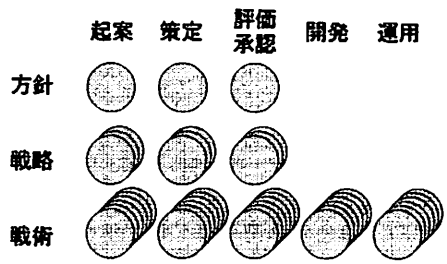
第２回(全３回)

日本ヒューレット・パッカード株式会社
マネージング・コンサルタント　佐藤　慶浩

戦略と戦術

方針を起案、策定して承認を得ると、それに従って情報システムの戦略を考えていく。情報システムの戦略が出来上がれば技術の選定、すなわち戦術ができる。５Ｗ１Ｈでいうと、方針はWhyとWhatで、何故、何をやるかということだけを決めればいい。戦略は、WhoとWhereとWhenで、誰がどの部署でいつまでにやるのかということである。戦術は、Howの部分で、どうやって実現するのかだけを論議する。WhyとWhatのところは経営会議にかける領域として十分成り立つ。逆に、戦術の部分がちょっとでも入ると、取締役の方は最新のテクノロジーは分からないので承認されない。

セキュリティ方針の位置づけ

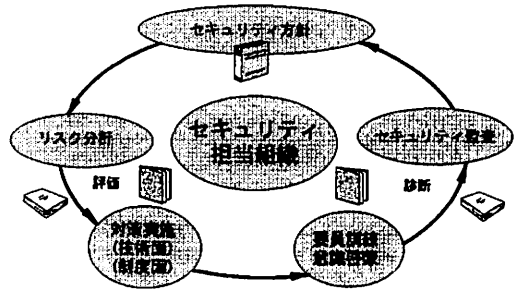


方針が経営会議で決められると、次はその方針に従った戦略、戦術の段階だが、これは階層的に増えていく。１つの方針に沿った形で、開発部門、営業部門、人事部門など部門別に、また営業部門であれば、受発注システムと顧客サポートシステムとでは違った情報技術の構築があるからである。ただし、いずれにしても方針は１つでなければならない。

重要なことは、「明日の営業活動が止まってしまってでもセキュリティは守らなければいけない」とかは方針策定の段階で議論しておかないと、結果的には誰も守ってもらえないものになってしまうということである。その価値観を作るのがセキュリティ方針である。

セキュリティ方針の運用

セキュリティ方針の運用



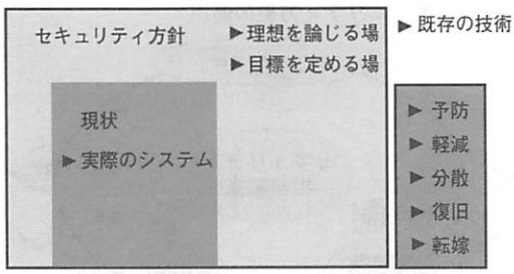
セキュリティ方針ができるとWhyとWhatが決まり、Whatが決まるとWhatに対しての情報システムセキュリティのリスク分析が行われる。この分析によって具体的な実施策を作っていくことができる。対策実施に関しては、技術と制度がある。技術というのは設定すれば設定したとおりにコンピュータが実行するが、制度面、人の面に関しては手順書を書いても手順書どおりやるかどうかはわからない。このため人に関しては要員の訓練、意識啓蒙が必要になってくる。また対策の実施、要員訓練、啓蒙が正しく行われているかはセキュリティに関する監査で評価する。監査の結果、方針に不十分なものがあれば方針を更新することもある。新たなリスクが出てきたらリスク分析を行う。たとえば、手順書を作っているのに従業員が守っていないということであれば、要員訓練を徹底するということで、方針に沿うように戻していくことができる。このため、セキュリティ方針の維持は運用の対象であることを忘れてはならない。

この中核に情報セキュリティの担当組織というものを位置づけることができる。これは責任を持たされてやる仕事であり、セキュリティを責任担当としてやるということである。必ずしも部署名が必要だということではなく、営業、情報システム、開発などから選抜して、セキュリティ担当タスクフォースを作ってもよい。

セキュリティ方針の定義

実際のシステムはセキュリティ方針をすぐに満たす必要はない。つまり、現状が全てを満たすような限られた条件の中で方針を策定すべきではない。セキュリティ方針は自分の会社のセキュリティに関しての理想を論じる、あるいは目標を定める場にすべきである。そうでないと、結果的にセキュリティ方針の更新の頻度が多くなり、また経営層の承認を取るのが難しくなってくる。

セキュリティ方針とシステム



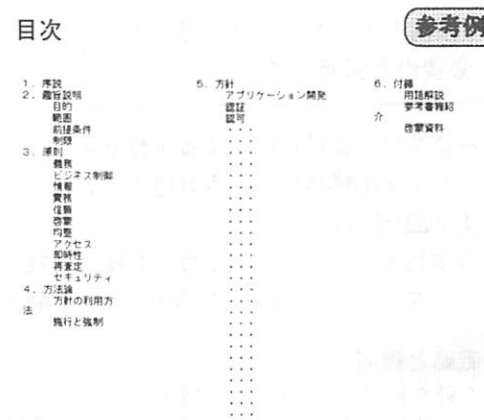
方針が承認された後のセキュリティガイドラインを作成する上での観点として、予防、軽減、分散、復旧、転嫁がある。まずはセキュリティの問題を予防し、万一セキュリティに問題が起こってしまったら何らかの軽減をしなければいけない。それから、応急処置が終わった後には、復旧をする。復旧のためには予め何らかの事を分散しておかねばいけない。さらに復旧で年度予算以外のお金が出てしまったということに備えて保険がある。ただし、保険は現状では情報システムセキュリティについてはほとんど機能しない。なぜならば、一般的に保険の対象は情報の価値ではなく、労働の工数になっているからである。付加価値は査定してもらえない。また、通常の保険の約款では、企業内でセキュリティ侵犯があった場合には保証の対象外となる。このことから事実上、情報システムのセキュリティの転嫁は非常に難しい。

重要なのは「セキュリティを守るのは常識だ」という言葉で済ませてはいけないということである。なぜ自分の会社がセキュリティに取り組んでいるのかを論じないといけない。営業マンにとってのセキュリティの常識と、情報システムにとってのセキュリティの常識というのはまだまだ違う。コンピュータ上に倫理観というものが確立されれば「セキュリティを守るのは常識だよ」という言葉ですませられるかもしれないが、セキュリティの常識という言葉は人によって、部署によって、部門によって違う。この意味で、セキュリティ方針を考える時に企業では必ずこれを論じておかないと、実際には理想も目標も違うものになっていく。その観点からもセキュリティ方針を作らなければいけない。

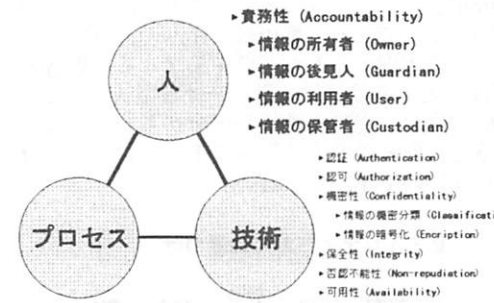
セキュリティフレームワーク

系統立てた構造を有するセキュリティ方針のことを当社ではセキュリティフレームワークと呼んでいる。方針とフレームワークとは包括的な関係になっている。

目次 参考例



方針抽出の観点例（一部）



一般的に、セキュリティフレームワークは先頭に「序説」、次に「目的」、言葉を定義した「原則」があり、「方法論」、「方針」となる。個々の方針は非常に端的なもので、通常２ページくらいに収める。普通の企業でコンピュータシステムを構築しようとすると、方針のステートメントは30～40くらいだが、ブレイクダウンをどこまでやるかという問題でありカテゴリーでまとめてもよい。人とプロセスと技術を考えなければいけないと言ったが、システム関連の人はエンジニアなので技術のところは容易にブレイクダウンできるが、人に関して何を考えていけばいいのかは難しい問題だと思う。人の観点で物事を考える際の切り口としては、情報の所有者、利用者、情報サービスの提供者の３種類がある。情報サービスの提供者としての立場、あるいは情報システムの利用者の部分はある程度分かるが、所有者の立場も忘れてはならない。この所有と利用と提供という言葉は、技術者にはヒントになるのではないか。

情報システム部長日誌 連載第２回

No. 999　新城　道彦

海外生産拠点の一つに中国広州工場がある。事務所が香港にあり、生産ラインが広州にある。経済特区の中ならまだいいが、設備や人件費の安さを求めて、さらに内地に入っている。

オフコンの本体が香港にあり、広州には20台近い端末がある。両方とも現地スタッフにＥＤＰの担当者がおり、日常の運用はどうにか対応してもらっているが、やや専門性は薄く、少しややっこしい話は東京からの応援で当たっている。先日、技術開発担当に応援要請があり、その出張報告があった。

香港、中国間の通信回線でトラブルが多発し、その診断と対策を求められたという。元々電力事情や回線の品質には問題があるため、中国側の端末にはそれぞれにＵＰＳ(無停電対策装置、瞬停があっても内蔵している電池で対応するもの)を付けるなど、日本より"贅沢"にしてあるのに、それでもダメなのかというのが正直なところである。

調査の結果、ネットワークを制御しているルータやハブにＵＰＳが付いていなかったという。端末にＵＰＳを付けて、ルータ等に付けないなどということがあるものかといえば、こんないきさつだそうである。

香港のベンダの初めの見積にはもちろんＵＰＳも入っていたが、もう少し安くならないかと突き返したため、２回目の見積はそれらを落とし、安くなって出てきた。現地では、これで作動するかというチェックはしたが、作動はしますとの返事で、それで導入したのだという。

ベンダの営業のセリフとして、論理的に作動はするが、システムとして安定的に運用できないものを"動く"といっていいのであろうか。

似たような話は日本でも聞く。ユーザの質問に「それは出来ません」といういい方はするなという教育をしている所もあるそうである。確かにソフトの世界であるから、やってやれないことは何もない。ただし、ユーザとしては、それが費用対効果を含め、システムとしてあるべきものかどうかを問うているわけだから、あるべきシステムとしてどうかという部分は、そちらの判断ですとなると、ベンダとしての専門性はどこにあるのかということになる。

一方、ユーザ側の問題としても、ベンダにそんな"親切な"行動様式を期待するのは時代遅れであり、置かれた環境の中で使用する機器と費用との兼ね合いなどは自己責任で判断しなければならない、その能力がなければ余計な手間暇がかかるということであろう。あるいは、日本ではあり得ることも海外では期待できない、世界標準で考えていかざるを得ないということか。技術は右肩上がりで進歩するが、気働きなどという部分は退歩することもあるようである。

一週間後、東京本社５階のＬＡＮのサーバに障害が出て、５階の利用部門のデータが全滅したという。サーバの磁気ディスクも二重になっておらず、フロッピィディスクへのバックアップも十分とってないという泣きたくなるような話で、海外の悪口をいっているどころではない。

そういえば、このサーバの設置も、とにかく試験的に早く、安くやってみたい、最小限の構成でいいから入れたいということであった。費用の捻出は利用部門の責任であり、われわれとしては「リスクはあるよ」と警告はしたが、何がなんでもという強い助言はしなかった。設置後、今までは何事もなく経過し、そうなると追加して手も打たず、油断があったということになる。

システムの安全性への意識はあっても、一定限度の経済性の裏付けがないと、情けない話が絶えないようである。

近畿会だより

＜近畿会 第56回定例研究会第２部報告＞

No.209　松田　貴典

テーマ　：原子力発電所の見学と情報システムの脆弱性を考える
第２日目(第２部)：情報システムの脆弱性討論会
コーディネータ：川端純一(敦賀市役所)
問題提起者：神尾　博(クボタシステム開発(株))
　　：松田貴典(日本ユニシス(株))
開　催　：98年３月６日13時から７日13時まで
出席者　：20名

前回報告の第１部「関西電力　美浜発電所　見学会」に続き、今回は第２部で「情報システムの脆弱性について」の討論を行った。

討論に先立ち、日本ユニシスの松田氏から、「情報システムの脆弱性」をテーマに、また、クボタシステム開発の神尾氏から「制御システムのセキュリティ問題(「バーチャル」から「器物、生命」の危機へ)」をテーマに、問題提起を願い、後半でコーディネータ川端氏による討論に入った。

「情報システムの脆弱性」：

日本ユニシス　松田貴典

情報システムの脆弱性とは、「情報システムの構築に伴い情報技術の特性により不可避的に発生する欠陥(弱点)」である。

脆弱性は、企業や事業体が情報システムを構築することで、業務システムや管理システム等から得られる「効用」に反して発生し潜在化する。また、脆弱性は、情報技術(ＩＴ)が本来もつ特性(例えば、情報のデジタル化され、記録は電磁的であること等)に起因して発生し、企業や事業体の業務システムや管理システムの中に内在する。

グローバルネットワーク時代の情報通信システムは、システムの健全化の手法である「システム監査」「セキュリティマネジメント」「リスクマネジメント」等を進化させることが必要である。そのためには、基準やガイドラインをベースとした帰納的なアプローチに加え、脆弱性の演繹的な理論研究を実施することが必要である。

それが健全なる情報化社会の発展に重大な意義をもつものと考える。

「制御システムのセキュリティ問題」：

クボタシステム開発　神尾　博

情報システムの通信システム・制御システムとの融合が進む昨今、工場はもとより交通、医療などの公共分野やＨＡ(Home Automation)等においても、不正アクセスやウイルス、バク等によるリスクが増大してきている。制御システムの場合、メカニズムに対し直接コントロールをおこなうため、これらの脅威により電子データのみならず、人命や器物が直に被害を受けることとなり、このためその対策は従来の情報システムのセキュリティとは異なったアプローチが必要になってくる。

今回は「原発」という制御を内包するシステムの見学直後ということに鑑み、この問題提起は絶妙のタイミングであった。以下、討論の主要な発言内容である。

1. まず、システム監査の在り方の問題である。

・システム監査の学問的位置づけについて明確にすべきである。
企業、組織体が活用する情報システムは拡大する一方である。
古くは会計情報システムを中心にシステム監査が機能してきたが、その後経営システムの一環として情報システムをとらえるのが一般的となっているように広義な情報システムに変わってきている。
これからはシステムの概念を広くとらえるのが適切であろう。加えて一方では、制御系システムについてもコンピュータが多用されており、このコントロールも無視しえない。
この分野のシステムにおいても社会性をもったシステムが存在し、生命や市民生活に密接なかかわりをもっている。
このように対象とするシステムは拡大しており、この事実は軽視できない。

・システム監査もこの趨勢をキャッチアップしていく必要がある。したがって、ジャンルごとに監査チェックポイント等整理しつつ領域を拡大していかねばならないものと考えられる。

・システム監査の範囲を整理する必要がある。
当初計算機(カリキュレータ)からスタートしたが、いまやメールに代表されるようにコミュニケーションツールとしてのウエイトも大きくなった。また、制御系にもコンピュータが多用され、コントロール機能をになう部分も重要度を増した。

2. 次に情報システムの有効活用とその評価の討議になった。

・情報システムは企業経営のために使ってきたはずであり、トップマネジメントがどのように考えているかのアプローチから着手すべきであろう。

・技術論よりも組織論からのアプローチが望まれる。

・同感である。経営者は今日をどのようにかせぐかが課題であり、情報システムはどう貢献しているか有効性評価を求めているのである。中小企業では経営者の当面の課題となっている。

・有効性の評価は必要と考えるが、具体的に有効性を測定する手法があるのであろうか。

・有効性評価に関してはむしろコンサルティングの領域ではなかろうか。
システム監査とはわけて考えるべきではないか。システム監査では信頼性、安全性が中心となるのではないか。
この保証に力点をおくべきである。

・効率性の評価はコンサル領域と考える。

3. 次に議論は、教育・情報倫理にも及んだ。

・不具合や不正アクセス等技術的な解決には限界があり、あらたな法による統制の強化や倫理、教育の充実も必要である。しかし、これらも解決には限界があろう。
課題はますます深刻なものとなろう。

・敦賀地区では小中学校までインターネットの導入計画がある。
有害情報から児童を保護するにつき検討中である。

なんらかのフィルターで制御することになろうが、誰が判断するのか、その判断が妥当なのか、行き過ぎると検閲になり、憲法問題にもなりかねず、悩ましい問題が起こっている。

4. 最後に社会システムとその知的財産にまで討議が進んだ。

・図書館の閲覧権は将来有料になるのであろうか、知的財産権は人類の幸せのため開放されるべきものではなかろうか、知的な評価で報われるのが本当の姿ではないか。
・知的財産権はビジネスを前提としたものとそうでないものがあるはずで、それを分けて論議するのがわかりやすいのではないか。ビジネスを前提としたものはそのコストを社会として認識しなければならない。
・公共的システムなどの社会的システムについては監査が必須である。
本来は企業の責任で解決すべきものであろうが。

以上、主要な討議内容であったが、議論はつきなく帰路のバスの中まで続いた。

近畿会 模擬監査に参画して

No.561 日高 祐子

ある大阪の中堅アパレルメーカー(以下、B社と称します)より、近畿会にシステム監査の依頼があったのは昨年の11月、先方への報告会が本年5月12日ですから、約半年をかけ、近畿会での二度目の模擬監査をやっと終了することができました。チームは、ワーキングメンバー5名と数名のサポートメンバーの編成です。

・模擬監査依頼の経緯

B社の経営コンサルタントが今回の模擬監査のリーダーと懇意の間柄であり、昨年11月、このコンサルタントの方を通して近畿会へ打診がありました。

今回のシステム監査は、その導入時点から現在に至るまでの問題点を整理し、2000年対応を前提とした次期システム構築の際に、同じ失敗を繰り返すことなく、何に気を付ければ良いかということを洗い出して欲しい……というのがB社社長の目的でした。というのも、日々毎日の業務において非常にパフォーマンスの悪い処理があり、一部の帳票は、夕刻出力指示を出し、翌朝やっと出力されるという状態であるとのことでしたし、またある処理においては、処理終了の目処がたたずランさせることが出来ないという事でした。

また、一方で蓄積されたデータをエンドユーザが自由に加工し活用したいという要望がありながら、基幹システムに与える影響が大きく、活用のためのツールが導入されておりながら使用できないとの事でした。

プレヒヤリングの段階で、導入されているハードウェアのパワーはそのデータ量等から察するに、決して不十分なものではなく、何か他に必ず究明し解決せねばならない原因があると思われました。

・B社のプロフィール

B社は、大阪に本社を置く婦人服(主としてセーターなど)の卸売業を営む会社。年商23億、従業員数150名強の規模です。

国外を含む仕入先に対し、素材・デザインなどの製品仕様を発注し、納品された製品を全国の百貨店に納めておられます。

・監査のポイント

前述したとおり今回の監査の目的は、「現行システム導入時の問題点および現行システムの問題点を明確にすることにより、次期システムの導入をより有効なものとする。」ことにあり、B社の企業規模およびシステムが対象とする業務から考えますと、所謂システム監査の三大観点である「信頼性・安全性・効率性」はさて置き、「有効性」が最重要項目であり、且つB社社長の求められているところであろうと、メンバーの意見が一致しました。

「有効性」という観点に重心を置きながら、下記のようなパーツに分けて監査を実施しました。

1．社内の情報システムへの取り組み状況
2．前回導入時の問題点
3．次回導入の進め方
4．現状システムの問題

・監査日程

・第一回目…ヒヤリング(97.11.27 18:30-20:00)
ヒヤリング対象は社長およびA氏。
A氏は、総務経理部門所属。現行システム構築の際の検討メンバーの一人でもあります。
・第二回目…ヒヤリング(98.1.22 18:30-20:45)
ヒヤリング対象は社長および営業部門グループリーダーのB氏、C氏。
B氏、C氏は現システムの主たるユーザーです。
・第三回目…ヒヤリング(98.2.19 14:00-16:30)
ヒヤリング対象は総務部門D氏、企画部門E氏、システム担当のF氏です。

・第四回目……実査(98.2.23 15:10-17:00)
システム導入時の契約書等およびシステム仕様書等を実査しました。
第一回目・第二回目はメンバー全員で訪問し、第三回目以降はヒヤリング担当と実査担当の二手に別れて実施しました。

・監査結果のポイント

結果報告として、下記をポイントに提言させて頂きました。

1.「業務の流れの分析」の重要性

現行システムが先進的構想に基づき構築されたものであるにも関わらず、当初の目的をすべて実現するには至らなかったのは、「業務の流れの分析」が充分に行われなかった事に起因する。

次回は、システムの活用により改善すべき部分と、システム外の業務の流れそのものの見直しにより改善せねばならない部分を明確に整理し切り分けることが重要である。

2. パッケージ、委託先等の選定

残念ながら、現行システム導入時のパッケージや委託先の選定は業界知人やディーラーに奨められるままに決定された。

その結果B社にとって適切な選択が行われず、パッケージカスタマイズ費用が大きく膨らんでしまった。複数の候補先の比較検討、またコンサルタント等専門家の助言を加味した判断が必要である。

3. 社内体制・教育の必要性について

構築されたシステムを有効に活用していくためには、情報化の目的の周知徹底、情報化における社内の役割分担と責任の明確化、システム担当者・利用部門双方の継続的教育が必要である。

また、改善提案、見直し提案が反映される仕組み造りがよりシステム導入の効果を発揮させていく。

・感　想

期間は6ケ月と長期にわたったものの、年末・年明けをも含み、実働にさいた時間はさほど多くなかったように思います。

何よりも今回の模擬監査で印象に残ったことは、下記の二つです。

一つは、B社の規模でコンピュータシステムを導入し、うまく活用できず、しかもどうして良いのかわからず、また、誰に相談して良いかもわからず立ち往生されている企業が多くあるのではないかということです。

「システム監査」を業として成り立たせていこうとすれば、いくらでどの位の労力を費やして……という壁に忽ちぶつかりますが、本当はB社のように「本当に困っている人達」の力になっていくことも「システム監査」の普及のためには重要な役割を果たすのではないかということです。

もう一つは、この期間になされたメンバーとのミーティングの効率の良さ。何から手を付けて良いのか分からない混沌とした状態を目の前にしながら、予想した半分位の時間の中で、意見が意見を呼び、一つの方向へと収束し、成果が上がっていく心地良さ……焦点のずれたやり取りやねじれの関係のやり取りのない、実り多い議論を何度も経験することができました。

ある監査人協会のメンバー曰く、「それを一度経験してしまうと、虜になってしまう」……とか。

今回のこの経験を共にできたB社の方々、そしてチームメンバーとこの「出会い」に感謝し、ここで得た「パワー」を今後も大切にしていきたいと思います。

中国支部だより

No. 387　安原　節男

今年も厳しい暑さのなか、8月6日'原爆の日'を迎えました。引き続いてのお盆を過ぎれば広島の新年度が始まる感じです。

前回の「支部だより」でもお知らせしましたとおり、今年から四国の会員の方も支部構成員になられ賑やかになりましたが、中・四国の広範囲な会員分布のなかで、どのような活動ができるのか、頭をイタめております。会員の皆様のご意見をいただきながら、頑張っていきたいと思っています。

私案としては、今年もやはり各ブロック(広島・岡山・松江・高松)での「顔つなぎを兼ねた研修会」を実施したい、と考えています。テーマとしては、私が携わった2件ばかりの監査事例が「タタキだい」になればと思います。

問題は、ブロック単位では構成メンバーが少ないうえに、ご多忙な方ばかりで、研修会へご参加いただくうえでの日程調整が苦しいことです。しかし、これも支部の宿命でしょう。

なお、6月に開設しましたＳＡＡＪ中国のメーリングリスト(offan@hiroken.ne.jp)の活用状況も「いまひとつ」です。よろしくお願いします。

九州支部だより

No.307 行武 郁博

6月の例会で、「電気通信事業における公然性を有する通信サービスに関するガイドラインおよびマニュアル(案)」(社団法人テレコムサービス協会)について検討しましたのでその概要を報告します。

平成9年5月21日に電気通信事業者団体である社団法人テレコムサービス協会より公然性を有する通信サービス、いわゆるホームページサービスに関しての自主規制案として掲題のガイドラインおよびマニュアル案(以下公然性通信ガイドラインという)を公開し広く利用者等の意見を求めている。

平成10年1月5日に電子通信サービスにおける情報流通ルールに関する研究会が「インターネット上の情報流通ルールについて(報告書)」(以下情報流通ルールという)を発表し当事者が守るべきルールや規制、プロバイダーの責任等について述べ、現行法制下においては法的規制よりも接続事業者の自主的対応が最も望ましいと結論ずけている。接続事業者の自主的規制案である公然性通信ガイドラインに情報流通ルールがどのように反映されているか興味が持たれる。

1. 公然性通信ガイドラインの特徴

公然性通信ガイドラインを中心に情報流通ルールと比較してその特徴と思われる点を以下列挙する。

(1)公然性を有する通信サービスに限定
情報流通ルールでは公然性を有する通信の他に1対1の通信、電子メールについても言及しているが、公然性通信ガイドラインでは不特定多数を対象とする通信に限定し電子メールサービス等特定者を対象とする通信については規定していない。しかし情報流通ルールにも記述されているように、電子メールサービスについても違法有害な情報についての苦情が寄せられているとのことであり、今後とも十分に予想される。本ガイドラインの公然性通信以外への拡充が望まれる。

(2)プロバイダーの責務を規定
情報流通ルールでは、プロバイダーの法的責任の規定化には慎重であるが、プロバイダーには通信の主要当事者として情報流通ルール形成に貢献する責務があることは明確にすべきであると述べている。公然性通信ガイドラインでは表現の自由の尊重、情報の自由な流通と共有化促進とともに個人情報の保護や違法有害な情報流通の防止、利用者への啓発に努めることを規定している。情報流通ルールに添った記述となっている。

(3)違法有害な情報発信に対する措置を約款等で規定
違法有害な情報として9項目の情報を挙げ、これらについて苦情が寄せられた場合、当該情報発信者への警告、改善、削除、利用の停止、契約の解除等を行うこと、また、苦情処理対応窓口の一元化等を約款等で定めるべき事項としている。これについても情報流通ルールに添った記述となっている。

(4)青少年保護対策
違法有害な情報からの青少年の保護対策としてレイティング、フイルタリング等の開発、導入を図るべきこと、青少年ＩＤの発行や成人ＩＤの使用制限、青少年との契約についての保護者の同意等青少年対策は情報流通ルールに比べると、多項目に亘った規定となっている。形骸化せずにどこまで有効に実施できるか運用が問題であろうと思われる。

(5)高額利用対策
情報流通ルールにはない事項であるが、青少年に限らず成人の場合についても利用料金が高額に及ぶ場合の条項を約款等で規定すべきであるとしている。高額とはどの程度なのかは述べられていない。

(6)発信者情報の開示
発信者情報の開示については、「苦情事例の匿名形式での公開」に止まっており、情報流通ルールが一定の要件、適切な手続きのもとではあるが発信者を特定する情報を開示することの検討を要望していることに比べると消極的な対応となっている。

(7)犯罪捜査への協力
犯罪捜査への協力については、現行法令に則った対応とし、令状捜査、任意捜査等の一定の手続きを経ての協力規定である。「オフラインで違法なものはオンラインでも違法」という原則に添ったものといえよう。

2. システム監査との関連

情報流通ルールで述べられているように、大学や企業のネットワークの管理者は電気通信事業者ではないが、技術的、機能的にはプロバイダーと同様の役割をはたしている。特に違法有害な情報流通への対応については本ガイドラインに準じた対応が必要である。従って、システム監査においても、当該情報システムが違法有害な情報に対する対策、管理体制が適切であるかを監査項目として監査を行わねばならないと思う。新たなシステム監査の視点が求められることとなろう。

中部支部だより

中部支部 No. 124 原 善一郎

差別問題といえば、セクハラ。

みなさん、セクハラをしないように気を付けましょう。という話題なら、特に、ＳＡＡＪの会報に載せる必要はございません。

この会報の読者である、会員のみなさんは、決して差別をしようとする気持ちをお持ちの方はいらっしゃらないでしょう。しかし、冷静に考えると、私たちは本当に差別をしていないのでしょうか。気がつかないうちに差別をしていないでしょうか。

不公平(アンフェア)の結果が差別であるとすると、公平であるという事を考えなければなりません。多くの場合、機会均等と言う言葉に置き換えられるでしょう。もちろん、聡明な皆様ならば、結果均等は決して公平という事ではないとお考えでしょう。

情報処理業界においては、性別による不公平さは他の業界よりすくないと言われております。確かに、私の所属する輸送用機器工業界よりも少ないように思われます。先日、協会の女性の方とお話をしていた折に、「女性はキャリアを認められにくいか」という話題になりました。そうすると、その女性の方は、「そもそも、そういう発想が出てくること自体、変だ。差別思想を持っている証拠だ」と指摘されました。私の主張は、性別による差別が存在しており、そのことは不合理だというもののつもりでした。しかし、この事自体がすでに「差別を容認する土壌かも知れない」と考えるようになりました。

機会均等とすると言う事は、全く同じ物を用意するという事ではありません。それは、平均身長において性別による差が見られるのにも拘わらず、全く同じ大きさの椅子や机を準備するのか、差を認めて、それぞれに応じた大きさの物を用意するのかという議論に似ております。

また、多数の所属するグループが正常で、少数派が異常だという考え方をしがちですが、これも、よく検討すべき課題です。私たちは、ハンディキャップのある人たちは異常だと無意識に考えていないでしょうか。目の不自由な人のために各種の配慮がいろいろなところにしてあります。これは、とても重要な事でしょう。しかし、目が不自由でない人がたまたま多くいて、その人たちの都合で社会の施設が構築され、不自由な人には不都合になっているだけなのではないでしょうか。つまり、各種の配慮をする時にすら、私たちは「目が不自由な人が異常だ」という差別意識を持っているという事です。

このように、ひとたび、差別意識の観点で疑問を持つと、いままでの考え方に多くの疑問が見えてきます。もちろん、厳密な機会均等などというものは達成する事はできませんし、無意識のうちの差別意識を完全に無くす事も不可能でしょう。しかし、自分はなにかを差別していないかと常に自問自答する必要があるのではないでしょうか。

振返って、ＳＡＡＪでは、理事に女性が少なく、引き継がれてきたのは会報担当という場所だけでした。これでいいのでしょうか。私は、ぜひ、もっと多くの女性の方に理事としていろいろなご意見を頂く必要があるのではないかと思います。また、協会自体が東京主体の運営となっているのではないでしょうか。インターネットが発達した今日では、これをもっとうまく使う工夫ができるでしょう。どのようにしたら良いかと言う点は、それぞれの立場で考え、それぞれにアイディアを提案していくべきではないでしょうか。

追伸：中部支部恒例の合宿を予定しております。
期　日：1998年11月14～15日
場　所：長野県
その他の詳細は未定
連絡先：電子メールでお名前と会員番号をお知らせ下さい。
zenichiro.hara@nifty.ne.jp

二伸：協会へのご意見を届ける方法はいろいろあります。
協会のPATIO(nifty) にて意見発表：
蓮見理事 (MHE02226)へ電子メールを送る
中部支部のメーリングリストで議論する：
原善一郎(znhara@pacific-ind.co.jp)へメールを送る
近畿会のメーリングリストに参加する：
(近畿会会長へ連絡をする)
理事会で取り上げてもらう：
協会の事務局経由へＦＡＸを送る

入会に当たっての一言

No.774 宍戸 恒裕

'97年８月に入会させて頂きました、宍戸と申します。

私は現在、製造会社の情報システム・グループにてシステムの運用・保守、企画・開発全般を担当しております。

元々は製造現場の出身で、コンピューターとの関わりは、金型部門を担当していた時にＮＣテープ作成の為に、独学でプログラム作成に挑戦した時からです。その後、生産管理システムの構築プロジェクトに参加し、ＭＲＰ理論などを勉強しました。

システム監査との出会いは、会社の株式上場への対応と、システム全般の勉強の必要性を感じた為でした。担当するシステム範囲が広がるにつれ、体系立った勉強が必要だと感じました。

勉強は、会社の通信教育制度にあった「システム監査」コースを利用しました。一応コースが終了出来たので、試験を受けて見たところ、ラッキーにも合格出来ました。「完走を目指し、とにかく全問回答」の方針が良かったかな、と思います。取引先のＳＥさんから受験前に、「書かないとゼロです。違っていても、とにかく書いておけば、、」とのアドバイスを思い出して、ガンバリました。

協会の存在は、インターネットのホームページで知りました。資料を請求してみたところ、親切なご案内を頂き、また、九州支部からもメールでご案内を頂きました。

「真実の意外性」

No. 707 神尾 博

今回は多くの情報処理の教科書にも書かれ、また一般にも信じられていることが、必ずしも真実ではないという例をひとつ紹介させていただきたい。

ではさっそく第１問である。ここに全く同じコンピュータシステムが２台ある。一方の信頼性(稼働率)は0.9である(ということはもう一方も0.9)。これらのコンピュータを２台デュアルシステムで動かした場合の信頼性を求めよ。

とまあ、「そんなのも分からなきゃ、システム監査試験はおろか情報処理２種もしんどいよ。」という声が聞こえてきそうだが。

たぶん皆さんはこう答えるだろう。「１－(１－0.9)＊(１－0.9)＝0.99」。試験では正解である。が……

コンピュータの障害にはおおまかに２種類あって、それは「ハードウェア障害」と「ソフトウェア障害」であることは皆さん御存知の通り。

まず、この「１－0.9=0.1」がすべてハードウェアによるものである場合について考えてみよう。カタストロフ的災害(地震や火事)の場合はどうか？ デュアルシステムのコンピュータは２台ともほぼ同じ場所にあるので、まず間違いなく２台ともやられる。が、このような災害は確率的には非常に低いので無視して良いと判断する。次に経年劣化の問題である。一般にハードウェアの故障は時系列的には「バスタブ曲線」と言って初期不良の値が高く、だんだん降下しながら定常化し、更に経年劣化で徐々に上がってくるという現象を示す。しかし設問に「0.9である」と書かれていることは「一定」の言葉こそ無いが、「0.9で一定である」と解釈できることは明らかである。従って経年劣化も考えなくて良い。

しかるにハードウェア的障害は２台それぞれランダムに起きると考えられるから、0.99で正解である。たとえばモータとかポンプ、更にロジックICを使った「マイコントレーニングキット」の様な単純な回路とかならこれでよい。

一方、ソフトウェアの場合はどうか？ ソフトウェアのバグは同じ条件下では必ず同じ結果＝障害を起こす。つまり再現性がある。ということは２台は同時に止まる。それどころか10台並べても100台並べても信頼性0.9は変わらない。

なんだ。屁理屈こねるな、お前。と思っておられる貴方。現に航空機の多重系マイコンシステムのソフトウェアは、同じ機能のフローを、異なるＣＰＵやプラットフォームで別会社に開発させているという事実をどう見る？

これは人間にも言える。同じ人間は同じ考えを持つ(おかしな表現で失礼！)わけであるから、自分の開発した情報システムのチェックなどできようはずがない。

だから「システム監査は絶対必要である」というオチである。

続いて第２問。「デュアルシステムの信頼性の計算」と「(巨大な)ソフトウェアには必ずバグがあり、バグによる障害は再現性があること」。本当に初心者に教えなければならないのはどっちだ？

協会メンバーの皆様の討議を通じて、いろんなヒントやご指導が頂けたらと思います。私もお役に立てる部分が有れば努力して行くつもりですので、今後ともよろしくお願いします。

No.775 太田 政敏

皆様はじめまして、昨年8月に準会員として入会させていただいた太田といいます。

私は、日本の最西端の長崎に在住し情報処理サービスの企業に勤めております。

主な業務は、顧客のニーズにあったシステムを開発することです。近年、システムを作るにつけ、いろんな角度からシステムを診断、評価したりすることがとても重要と思うようになりました。と言うのも私の手掛けている開発ソフトのほとんどが客先要求の処理結果のみを重要視したシステムに留まり、安全性、信頼性、効率性を考えた健全なシステム評価には至っていません。こんな疑問を考えている折り、ふとしたきっかけで昔(20年前)アプリケーションのソフト開発で労苦を共にした友人と出会い、システム監査人協会で活躍中と聞いて早速私も支部の研究会に参加させていただきました。支部の研究会はリラックスした雰囲気の中で活発に意見交換をされ皆様すごく勉強されていることが解り、ちょっと焦り気味になり反省しております。システムは情報をコントロールする生きものです。発展、変化する社会と共に変わります。システムに新しいソフトを取り込むと効果も生み出すがいつ発生するかわからない副作用(異常)も潜んでいます。それを未然に防ぐのがシステム監査であると私には伝わってきました。また、研究会内容も具体的に取り上げられシステム監査の実用化に向けて邁進されています。常に新しい情報をキャッチし意識して物事の動きを観ないといけないと思いました。今は皆様について行くのが精一杯です。若くないけど頑張りますのでよろしくお願い致します。

No.778 山口 芳彌

(有)山口システム監査の山口 芳彌(やまぐちよしみつ)昭和11年8月11日生です。

昭和35年京都大学卒業、大手乳業会社に入社、経理、原価管理、工場建設事務等を7年経験して、コンピュータ部門に16年所属、SE等を4年経験後、同部門の管理職を12年(5年間部門長)つとめました。

その後コンピュータ部門から転出、8年間、工場経営等の業務に従事しました。

更に、機械電機部品の中堅商社に転職し、全社経営情報オンライン化企画の立案、海外子会社のコンピュータ導入、営業情報国際オンラインを10ケ月で完成等を行いました。

このように、コンピュータ業務に、約20年従事しましたが、一方で、コンピュータシステムユーザーの経験年数も15年あり、システム監査の重要性、必要性については、充分に理解しているつもりです。

システム監査人協会入会の動機は、第一は、会員の皆様から学び、自己研鑽を行いたいことです。

第二は、会員の皆様と協力して、システム監査の普及と監査人の地位向上に微力ながらお役に立ちたいと考えたことにあります。

各企業、団体の業務システムの中に占めるコンピュータシステムの割合は、急速に拡大しています。すなわち、システム監査は、組織体経営上、必要不可欠なものとなりつつあります。

システム監査というと、とかく、コンピュータ技術レベルの議論になりがちですが、経営次元での必須事項であることを、PRし、社会的な合意を得るよう努力する必要があると考えています。

このためには、例えば、安全性の部分だけでも法定監査化することを働きかける等も必要と思います。

そして、安全性以外の部分は、従来通り任意監査として残すといった柔軟な方式を考えてもよいのではないでしょうか。

とりとめのない自己紹介になりましたが、何卒よろしくご指導をお願いします。

No.780 蔵田 好実

皆様、始めまして昨年の9月に入会させていただきました蔵田(アシダ)と申します。気がつけばもう一年近くにもなっております。私自身、情報システム監査に対して興味を持ち始めていた時に、近畿会会長より「社外の企業に対してシステム監査(模擬監査)をする機会がある。今、システム監査人協会に入会すればメンバーとして参画できるぞ」っといった誘惑にのせられて入会させて頂きました。(この世界に引っ張っていただき感謝しております)その後、近畿会で月例研究会報告の講師をさせていただいたり、今やドップリとシステム監査人協会につかって

おります。システム監査の領域もここ数年で少しづつ注目されてきていると感じております。無尽蔵にシステム化投資を行ってきた現実に対して、客観的に評価を求められる時代となってきたと思います。また、ネットワーク時代の到来はシステムの自由度が増した分、セキュリティー等のシステム監査領域のテーマに関心が持たれてくるでしょう。システム監査が独立した業務として成り立つ日はもう少し先になるかも知れませんが、情報システムの上流過程(コンサル領域等)では、まさに今求められているノウハウも多くあると感じております。とかくシステム監査領域は独自でノウハウを高めるのが難しい領域であり、システム監査人協会での活動はスキルの向上・業界動向の把握には格好の場であると感じております。私自身、システム監査人としてのスキルを当協会の活動を通じて高めていきたいと考えております。
今、システム監査領域のノウハウを身につける事は将来の自分に大変プラスになると信じ、今後とも皆様のご指導を受けながらがんばっていきたいと考えております。よろしくお願いいたします。くれぐれも幽霊会員とならないよう、がんばります！

No. 781 長嶋 仁

みなさん、はじめまして。
建設会社に9年、システムインテグレータに6年勤務した後、6月より技術士事務所を開業した長嶋と申します。建設会社では建築設備の設計・施工管理、ＣＡＤシステムの構築、メインフレーマに出向してのＳＥ業務などに従事し、システムインテグレータではパッケージソフトの開発を含むＳＥ業務に携わりました。今後は中小企業における情報システムの活用、情報社会のなかで個人や企業がコアコンピタンスを如何に発揮していくか？、健全な自由主義社会の発展のために情報システムはどうあるべきか？、などのテーマを中心に活動していきたいと考えております。
これまでシステム監査は、ある程度の規模の企業でないと導入・実施の対象にはならなかったでしょうし、中小企業では話題にものぼらないというのが実状です。しかし、中小企業の情報システムもネットワーク技術の進展、オープン化という大きな流れの中で、インターネットや外部企業との接続が急激に進みつつあります。
そこで、システム監査へのさらなる要求がでてくるのではないかと感じます。一企業内での業務の情報システムへの依存度増大という現象に限らず、企業と外部社会とのかかわりの中で情報システムの信頼性、安全性をみていく必要があります。
また、システム監査には狭義のシステム監査と広義のシステム監査があると言えます。前者は、会計監査などと同様に情報システムが法令・基準などに準拠しているかどうかの文字通りの監査です。後者は、有効性・戦略性の監査に代表されるようにユーザ企業のニーズに基づくコンサルティングの色彩の強い監査です。対象の多様性と変化のスピードの速さなどから、すべてが法的根拠のあるものになることはないでしょう。(その是非も当然含めて。)このことがシステム監査が普及することの難しさの一因ではあると思います。追風と逆風が入り混じったような状況ですが、実際に情報システムを活用する現場レベルから、その啓蒙・普及に貢献したいと考えます。
最後に、すでに何回か参加させていただいた研究会は、情報システムをめぐる多彩な演題が選ばれ、たいへん有益です。講師やスタッフの方々の多大なご努力に感謝申し上げます。以上、自己紹介とシステム監査に対する想いなど書かせていただきました。どうぞよろしくお願いいたします。

No.784 大野 淳一

皆さんはじめまして、共立コンピューターサービス(株)(岐阜県大垣市)の大野です。昨年11月に本社が移転し、そこで会社がご近所になった日本システム監査人協会中部支部のＨ氏のお誘いを受け、今年の１月に入会しました。システム監査技術者試験には平成７年度に合格しました。現在は、システム監査部門に所属し、自社のシステム監査を行っています。システム監査業務に従事するようになって、４年目になります。これまでは、システム監査の各種基準や解説書等を自分なりに解釈して実務に適用してきましたが、常に、自分の考え方が妥当であるのかといった疑問が頭の片隅にありました。
中部支部の例会には、４回出席しました。出席されている方には、いろんな職場のいろんな立場の方がいらっしゃいます。岐阜県出身の方が意外と多いのにも気がつきました。そういっ

た方たちが、気取ることなく本音で語ってくれます。また、私のような若輩者でも対等に扱ってくれます。普段から自己啓発に努め、情報処理試験や他の各種試験に挑戦されている方々の口先だけでない本物を例会での議論や2次会での何気ない会話の中から感じました。

システム監査に関する情報を得るだけでなく自分の考え方を深いところでゆさぶるような刺激を協会の活動を通じて得られることを期待しています。また、協会の活動を通じて得られたものを今の仕事に生かすことが、微力ながら、システム監査の普及や日本システム監査人協会の発展にも寄与するものと考えます。今後ともどうぞよろしくお願いします。

No.785 吉田 登

開発から維持・運用までシステムサイクル全般にわたるよい情報システムを効率的に、経済的に製作するにはどのようにするか、かって情報システムの仕事に携わった私には今もって大きな関心事である。システム監査人の責務もこのような観点から考えている。

たいへん大雑把に言ってしまえば、情報システムの製作段階、運用段階においても、それぞれの活動が健全に行われるよう監査することは不可欠であるが、システムの善し悪しを根本的に決定してしまうのは設計段階であり、設計段階における監査はより重要なものと考える。

システム監査という事柄を未だよく理解できていないと自ら思うが、システム監査の特性はこのような点に由来するのだろう。完成された情報システムについてその是非、良否を云々するのではなく、情報システムが作られていくプロセスに関わっていくことが不可欠であり、システム監査のポイントであろうと考えている。

このような大変あいまいな考えでシステム監査ということに関心を持ちつづけているが、具体的なシステム監査活動の経験は非常にかぎられている。現職、監査役という職務の中で機会を捉えてシステム監査の具体的な活動ができればと思っている。しかし、残念ながら、昨年来体調を崩し、今は健康回復が第一課題になってしまっている。

No.786 井戸 克彦

皆様、はじめまして。1月に入会させて頂きました井戸と申します。私は、いわゆるソフトハウスに勤務しております。私どもでは、、鉄道、電力関係の制御系システムを中心にシステム開発業務を行っております。私は、10年ほど名古屋と東京の事業所で開発業務を担当した後、現在は、名古屋事業所で開発部門の管理を行っております。当社では、情報処理技術者試験の資格手当が支給されるため、その間に2種、1種、特種、オンライン、プロダクションエンジニア、プロジェクトマネージャ、システム監査の各試験に合格しました。システム監査は、平成2年秋の試験で合格し、その時に、監査人協会の入会案内を頂いたのですが、何しろ動機が不純(お金に目が眩み、合格することが目的でした)、システム監査技術よりも、システム開発技術に目が行っていたという理由で、あまり考えもしないでお断りしました。従いまして、最近までシステム監査に関する知識は無に等しいものでした。(今もそれに近い状況です)

3年前から、他事業所の開発業務における部門内監査を実施する立場になりました。部門内監査と申しましても、ISO9000に準拠した社内規定の運用状況を中心としたものでして、システム監査基準からはほど遠い内容になっているのが実状です。最近は、プロトタイピングや、クライアント・サーバーシステムなど新しい手法や新しいシステム形態での開発が増加しておりまして、監査の着眼点を変える必要性を感じていました。そんな時、ＳＡＡＪのホームページを拝見し、心機一転、システム監査を一から勉強し直すつもりで、入会を決意しました。その意味で、6月に頂いた「新システム監査基準実務手順書'98」は、私のような初心者には非常に有用で、是非活用させて頂きたいと思います。

今後は、微力ながら、協会活動に少しでもお役に立てればと考えております。ご指導ご鞭撻のほどよろしくお願い申し上げます。

No.788 後藤 知久

はじめまして。私は通信販売の(株)セシール(高松市)のクレジットサービス部に勤務し、現在当社の金融システムを担当しています。

コンピューターメーカ(富士通)のSEを約15年、監査法人系コンサルタント会社(ビジネスブレイン太田昭和)のシステムコンサルタントを約

4.5年経験した後、平成5年に当社に入社しました。

情報処理技術者試験ではじめて受験したのがシステム監査で、4回目の平成元年の受験で合格し、以後、(前職で)公認会計士の方と協力しシステム監査の実経験を3回しています。

現在の職務ではシステム監査と直接関係していませんが、いずれこの経験を生かす機会があるかもしれませんので、システム監査の最新の情報を入手したいと思いSAAJに入会しました。

特に、最近の数年間のダウンサイジング化、パソコンやインターネットの急速な普及など、情報化社会を取り巻く環境変化はめまぐるしいものがあり、それに伴い、新たなリスクが出現し、システム監査のテーマも従来より広がりを持ってきているものと考えます。

一方、この変化のスピードに対し、私個人の知識や経験は遅々たるものがあり陳腐化しつつあることを懸念しています。

従って、皆様と交流することにより、新しい分野の知識を取得するとともに、普遍的な分野については更に深めて行きたいと考えています。

ちなみに現在、以下のテーマに関心があります。

1. メインフレームとオープン系サーバ(NT等)の動向
   特に投資効果の観点とセキュリティ面からどう棲み分けるべきか。
2. プライバシーと個人データの保護
   情報システム構築上、どのような配慮が必要か。
3. インターネット等オープン系ネットワーク
   自社システムにどのように取り入れるべきか。

何分、四国(高松市)ののどかな田園地帯で暮らしていますので、皆様と直接交流することは困難と思いますが、インターネット等を最大限に活用して頑張りたいと考えていますので、よろしくお願いします。

No.792 前橋 雅夫

皆様はじめまして。1月に入会いたしました前橋と申します。現在、精密機械メーカの情報システム部門に勤務し、おもにシステム運用管理業務を担当しております。システム監査につきましては、試験勉強程度の知識があるだけで、実際にシステム監査を実施したことも、被監査部門として監査されたこともない全くの素人です。そのような私ですが、日本システム監査人協会では、次の2大テーマの実現に向けて活動していきたいと思っております。

第1のテーマは、システム監査人として、実際にシステム監査を体験することです。先にもお話しましたが、私にはシステム監査の経験がありません。とにかく、システム監査を一度経験してみないことには何も始まらないと考え、当協会の「システム監査事例研究会」に参加することにいたしました。事例研究会では、一般企業を対象に模擬監査を実施しており、実際にシステム監査を体験することができます。今後は事例研究会での活動を中心に、システム監査の実践経験を積んでいきたいと考えております。

第2のテーマは、情報処理業界の人脈ネットワークを広げることです。企業内部の情報システム部門におりますと、業界の動向などは、専門誌、セミナー、イベント等から得ることが多くなります。ビジネスという枠を超えて、外部企業の方とお話をして情報を得るような機会はほとんどありません。当協会には、様々な分野から多数の方が参加されています。アフター研究会(?)もOKですので、そのような方々と、現場の実状に迫った情報交換をしていきたいと考えております。

このような活動を通して、システム監査技術者という資格を、実のあるものにしていきたいと思っております。ご指導の程よろしくお願いいたします。

No.793 井沢 澄雄

このたび、日本システム監査人協会に入会させていただいた、井沢澄雄と申します。

自己紹介をさせて頂きます。

富山県出身で大学進学と共に石川県に移り、就職によって東京に出てきました。学生時代は情報処理工学科で情報技術の基礎を学び、その後大学院(修士課程)にて人工衛星リモートセンシングデータ(主に海洋域)の画像処理に関する研究を行いました。

就職後は、官庁向けのOSI(開放型システム間相互接続)関係の業務を約2年、サーキット場の総合経営管理システム開発プロジェクトを約2年、官庁外郭団体向けのシステム開発業務を約7年担当して現在に到っています。

プロジェクトマネージャ兼システムアナリスト兼アプリケーションエンジニアといったところが現在の職種です。(情報処理技術者試験も当

該区分のものは取得しています)

また、これまでの業務経験を生かして技術士(情報工学部門。科学技術庁登録)となり、社外技術者との交流も増えているところです。

システム監査技術者試験に合格したものの、実際にシステム監査を行う機会が無く、当協会での活動を通じて監査技術を向上させていきたいと思っています。

【日本システム監査人協会報 No.48】の「金融検査士制度にシステム監査技術者の活用を申し入れ」といった記事に接し、システム監査技術の重みを感じています。

No.794 井戸田 博樹

はじめまして、昨年システム監査技術者の試験に合格しました井戸田と申します。現在私は、学校法人(私立学校)の情報システム部門に奉職しております。皆様はあまり学校法人の情報システムについてご存じ無いと思いますので簡単にご紹介致します。

学校法人は、基本的には私企業と変わりませんが、経営目的が異なります。具体的には、学生生徒の豊かな人格形成に資するために、ゴーイング・コンサーン(継続性)がより一層重視されます。

情報システムは大きく区分すると、利用目的および利用者から教育・研究システムと事務システムに分かれます。教育・研究システムは、学生の情報教育(情報リテラシー教育、語学教育、専門教育)、各種研究、学術情報の発信・収集に利用されます。高度な教育研究を実現させるために、インターネットやマルチメディアを駆使しています。

一方、事務システムには入試、教務(成績管理)、就職、会計等の基幹業務系システムと、情報共有を目指し、ＥＵＣ、グループウェア等による情報系システムがあります。最近は事務システムのセキュリティを確保しながら、教育研究システムと事務システムをいかに統合するかが話題になっています。

学校法人の情報システムにおいては、信頼性、安全性の向上はもちろんのこと、特に個人情報保護が重要です。この点については一般企業以上に注意を払っています。そして、効率性・有効性については、利用目的に照らした適正規模による継続投資が重視されます。

また、最近は特に、不特定多数の学生が利用する教育システムのＴＣＯ削減をいかに実現させるかが悩みのタネとなっています。

学校法人でもシステム監査が重視されるべきなのですが、本学では、監査法人による会計監査の一環で行われているだけで、個人情報保護や効率性・有効性の観点からの監査は行われていません。当分の間は、監査的な視点をもって、情報システム業務に携わることが、システム監査技術者としての私の使命であると考えています。学校法人にはシステム監査技術者の方が少ないようですが、情報交換をしたいと希望しておりますので、ぜひご連絡をお待ちしております。

No.797 塚本 克行

皆様はじめまして、今年の２月に入会した塚本と申します。

自分では、まだ若いつもりでいますが、システムとの関わりは、既に18年となります。

主にＳＥとしてシステムに関わってきましたが、６年程前から、社内システムの標準化推進と監査の担当となり、監査業務に興味を持ちました。試験にも何度かチャレンジしましたが、担当中にはさっぱり合格出来ず、担当を離れた後になってようやく合格(96年秋試験)することが出来ました。

合格した当初は、担当業務も忙しく入会を見合わせてきましたが、ようやく業務も落ち着いてきたことから仲間入りさせていただくことにしました。

監査人としての活動は全然できておりませんが、定例の研究会では興味のある題材(ISO9000、帳簿書類の電子データ化)も多く、可能な限り出席して、いろんな刺激を受けて、自分を高めて行きたいと考えております。

まだまだ勉強不足ではありますが、監査人としての今後の抱負をもって、私の挨拶に替えたいと思います。

ワールドカップ・フランス大会では、私のようなにわかサッカーファンでも、世界の一流のプレイを堪能することができました。それは、一流の選手同士が最高の舞台で技術を競ったこともさることながら、一流の審判が適確な判断でゲームを裁いたことも大きな要因であると考えます。

システム無しでは、ビジネスの世界も、日常生活も、成りたたない現状においては、『良いシステムが正しく運用される』ことは大切なことではないでしょうか。

将来は、選手(ＳＥ)としてゲーム(システム開発・保守・運用)に参加するのでなく、審判(監査人)として参加することで、感動的なプレー(良いシステム)をファン(社会)に提供していきたいと考えています。

そのためには、自己研鑽は勿論のこと、システム監査の普及にも微力ながらも貢献していければと考えていますので、今後ともご指導のほどよろしくお願いします。

No. 798　岡田　宏三

(株)ニッセイコンピュータの岡田です。

昭和33年生まれの40歳ですので、あまり若手とはいえませんが、本年より、新メンバーとして協会の一員に加えていただきました。(旧)特種情報処理試験に合格して以来、システム監査試験を受験すること既に５回、今度もダメかな？と思っていた今年の１月、ようやく念願かなってシステム監査技術者試験に合格することができました。私ども(株)ニッセイコンピュータの監査室には、協会の副会長である安本監査担当部長(当時、現監査室顧問)がおられますが、早速お声をかけていただくこととなり、渡りに舟とばかりに入会させていただくこととなりました。

実を申しますと、情試に合格するまでは、日本システム監査人協会の事につきましては、何も存じ上げてはおりませんでした。しかし、システム監査技術者試験に合格した限りは、その知識を社会において役立てていきたい、また自らのスキルアップをはかっていきたい、という気持は以前から持っておりましたので、安本副会長からのお誘いがあった時には、本当にうれしさで一杯になりました。

本年３月には、システム監査学会との合同研究会へ出席させていただくことができ、参加されたメンバーの真摯な姿勢に打たれました。

現在、実務上においては、開発部門のプロジェクトリーダーを勤めておりますので、直接にはシステム監査にたずさわっている訳ではありませんが、日本ガイドシェア(システム監査部会)への参加をさせていただいており、監査人協会以外においても切磋琢磨する場として、活用させていただいています。

今後とも、システム監査技術者として恥ずかしくないように、勉強を続けていきたいと考えております。これからも、日本システム監査人協会の活動に積極的に参加して参りたいと考えておりますので、どうかよろしくお願いいたします。

会員の書いた本の紹介

No. 555　松枝　憲司

会員３名(渡辺和宣、小野修一、中西昌武)の方が共著に参加した書籍を紹介します。

『システムコンサルタントになる本』

情報システム研究会著、日本能率協会マネジメントセンター、230ページ、1800円。

本書では、システムコンサルタントは、「経営・業務およびＩＴ・情報システムに関する知識・スキルをもとに、経営戦略や経営目標に対して、ＩＴによる具体的な解決方法を、情報戦略やシステム化テーマとして提示したり、その情報システム構築を支援する役割」であると定義しています。中小企業診断士やシステムアナリストやシステム監査技術者を想定しています。

内容は

第１章　システムコンサルタントとは
第２章　システムコンサルタントの役割と仕事
第３章　システムコンサルタントになるための条件
第４章　システムコンサルタント・ビジネスの実際
第５章　システムコンサルタント６人のキャリアと生活

という構成です。

カリフォルニア州立大の一色浩一郎先生が、まえがきと各章のコラム(米国での状況を紹介)を担当されています。

第５章では、各人の今までの生い立ちや現在の１週間の生活ぶりを紹介しており、面白くなっています。

私自身コンサルタントを自認しているのですが、これを読んで、一流と二流の違いがわかった気がします。

今後コンサルティングのメソドロジーについても、是非紹介してほしいと思います。

皆さんご一読下さい。

システム監査未経験の会員のみなさんへ
システム監査実践セミナーに参加し、システム監査の実際を体験してみませんか!!

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」のために、毎年システム監査実践セミナーを開催しております。第3回目の「システム監査実践セミナー」を下記の日程にて開催いたします。

実践セミナーは、事例研究会で実施した模擬システム監査の事例を教材として、実践で得たノウハウを会員のみなさんと共有することを目標にしています。

システム監査試験合格のあと、システム監査を経験されていない会員のみなさん、この機会を利用し、システム監査の実際を体験して、システム監査能力の向上を図りましょう。皆さんの参加をお待ちしています。

記

システム監査実践セミナー概要

1．日　　時　平成10年11月7日(土)～8日(日)
　　第一日目　13:00～20:00、第二日目 9:00～15:00
2．場　　所　海外職業訓練協会　〒261 千葉市美浜区ひび野1丁目
3．費　　用　15,000円程度(宿泊費、食費を含む)
4．セミナー内容　事例研が実施した模擬システム監査(U社)をケーススタディとして取り上げます。
　　セミナー用にアレンジした「システム監査依頼書および企業情報」を教材として、5人程度のグループにわかれて、予備調査、本調査、監査報告の実際を体験して頂きます。
5．講　　師　事例研究会メンバーの模擬システム監査経験者5名
　　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
　　協会会員(準会員、法人会員を含む)、先着順20名。(最小催行人員8名)
7．申し込み先　日本システム監査人協会　事務局宛下段の申込書にて申し込み下さい。
8．申し込み期限　10月9日(金)
9．問い合わせ　商船三井システムズ(株)統括部　鈴木　TEL:03-5473-6114
　　E-MAIL:suzuki-min@dm.molis.co.jp
　　GFG01442@nifty.ne.jp

送付先：日本システム監査人協会
　　FAX.No. 03－5350－9269

日本システム監査人協会
平成10年度システム監査実践セミナー参加申し込み書

年　月　日

会員No.(法人名)	
氏　　名	
資料送付先 〒－住所	
自　　宅	電話ＮＯ.　　ＦＡＸ－ＮＯ.
勤 務 先	電話ＮＯ.　　ＦＡＸ－ＮＯ.
E-MAIL アドレス	

ＳＡＡＪ所有ビデオテープ貸出規定 1998年７月制定

1. 基本事項

(1) 貸出しは当協会会員(含む法人会員、準会員)に限定する。
(2) 会員と事務局との連絡は、所定の書式によるFAX通信で行う。
(3) 貸出し期間は２週間以内とする。場合により通算６週間までの継続貸出しが出来ることとする。
(4) ビデオテープの貸出し、返却は宅配便又は郵便を使用する。
(5) 貸出料は１回につき、１本2,000円とし、２本以上の場合は２本目からは１本につき1,000円とする。(1本：2,000円、２本：3,000円、３本：4,000円、…)
(6) 送料は送付側負担とする。
(7) 貸出テープを紛失または毀損した場合は、１本につき3,000円を再作成費として支払うものとする。

2. 借出し手続き

2. 1 借出し

(1) 手続き：借出し希望者は「ビデオテープ借出・継続借出申込書」に所定事項を記入しFAXにて申込む。
料金を振り込んだ受取り書等の写しを同時にＦＡＸする。
(注)ビデオの特定は「ビデオテープ番号」による。
(2) 事務局対応：
a) 借出し希望のビデオが手元にある場合。
宅配便又は郵便により借出し希望者に送付する。
「ビデオテープ」と資料がセットである場合、その両方を送付する。
b) 借出し希望のビデオを貸出し中等の理由で、直ちには貸出しが出来ない場合。
「ビデオテープ貸出し連絡書」にてその旨を借出し希望者にFAXで連絡し、後日の貸出とする。

2. 2 継続借出し

(1) 手続き：借出し者が期間終了前に、「ビデオ借出・継続借出申込書」を事務局宛FAXで提出する。
(2) 事務局対応：
a) 他に借出し希望者がいない場合に限り、更に２週間以内の借出し期間の延長を認める。
(通算で６週間まで、費用の追加無し)
b) 他に借出し希望者が居る場合は、「ビデオテープ貸出し連絡書」により、継続希望者に継続貸出しできないことを連絡する。この場合、借出し者はビデオテープを返却すること。

2. 3 保管・管理

(1) 「ビデオテープ」を借出した会員は、返却まで、善良な管理者としての注意義務を負うものとする。
(2) 紛失、毀損
貸出した「ビデオテープ」が、万一、紛失、毀損した場合、借出し者は再作成費用として、１本につき3,000円を負担するものとする。

2. 4 返却

借出し者は使用後(借出し期間内)、速やかに、借出しビデオテープのみを「料金差出人払い」の宅配便又は郵便で事務局に返送する。
資料は、借出し者のものとし、返却は不要とする。

3. 貸出料振り込み口座

銀 行 名：第一勧業銀行
支 店 名：北沢支店
口座種類：普通
口座番号：１０５３４８８
口座名義：日本システム監査人協会
(注)振込手数料は借出し者負担。

日本システム監査人協会御中　　平成　　年　　月　　日

ビデオテープ借出・継続借出申込書

貴協会のビデオテープを借出し・継続借出しいたしたく、「ＳＡＡＪ所有ビデオテープ貸出規定」を承認の上、下記の通り申し込みます。

記

<table>
<tr><td colspan="2">会員番号</td><td colspan="2"></td></tr>
<tr><td colspan="2">会員名</td><td colspan="2"></td></tr>
<tr><td colspan="2">ビデオテープ番号
ビデオテープ名称
資料要否</td><td colspan="2">要　　否　　(どちらか○)</td></tr>
<tr><td rowspan="4">貸出種類</td><td rowspan="3">1．新規借出し</td><td colspan="2">ビデオテープ　　本　　円</td></tr>
<tr><td>希望期間</td><td>平成　　年　　月　　日から
平成　　年　　月　　日まで（２週間）</td></tr>
<tr><td>送金確認</td><td>振込日付（　　年　　月　　日）
（振込済依頼書控えを一緒にＦＡＸしてください）</td></tr>
<tr><td>2．継続</td><td>期　間</td><td>平成　　年　　月　　日まで（通算で６週間まで）</td></tr>
<tr><td rowspan="6">送付先・連絡方法</td><td>住所</td><td colspan="2">〒□□□-□□□□</td></tr>
<tr><td>企業名
(自宅の場合空白)</td><td colspan="2"></td></tr>
<tr><td>所属</td><td colspan="2"></td></tr>
<tr><td>電話番号</td><td colspan="2"></td></tr>
<tr><td>ＦＡＸ番号</td><td colspan="2"></td></tr>
<tr><td>E-mail番号</td><td colspan="2"></td></tr>
<tr><td colspan="2">その他</td><td colspan="2">使用目的がグループ研究の場合、グループ名等</td></tr>
</table>

事務局使用欄

申込受付	貸出	返却	借出継続

貸出ビデオ一覧表(台帳)

◆月例研究会◆

管理番号	開催数	開催日	テーマ・タイトル	講師(所属支部・会員番号)	講師所属会社
VT037	第37回	H7.1.23	ネットワーク構築の考慮点について	海野 守	味の素システムテクノ(株) 情報処理事業部 副部長
VT038	第38回	H7.4.24	「コンピュータのバックアップ」について	鴫野正勝	(株)ワンビシアーカイブズ 関東事業所 副事業部長
VT039	第39回	H7.5.30	新開発手法「クリーンルーム」について	佐藤和夫	日本ＩＢＭ開発製造品質 プロセスプログラム次長
VT040	第40回	H7.6.30	新システム開発手法 Mai Dvo Clu 要件定義の手法について の紹介	木ノ下勝郎	オーロラシステム設計事務所
VT041	第41回	H7.7.28	「ＰＬ法とソフトウェア」について	内布 光	(株)日立情報システムズ
VT042	第42回	H7.10.6	Unicode その光と影	荒川幸式 (関東293)	日本ユニシス(株)ITｺﾝｻﾙﾃｨﾝｸﾞ室
VT043	第43回	H7.12	ＣＡＬＳの概要と情報システムに与える影響	平本健二	(株)ＮＴＴデータ経営研究所 コンサルタント
VT044	第44回	H8.3.6	ファイアウォールとインターネットセキュリティ	堀越繁明	日本ユニシス(株)オープ企画推進部
VT045	第45回	H8.5.28	本格的C/Sシステム開発経験とシステム監査の視点	打矢隆史 (関東243)	三井物産(株)三井ﾄﾗﾝｽﾎﾟｰｸｾﾝﾀｰ
VT046	第46回	H8.10.24	東京海上におけるソフトウエアの品質管理	勝田敦彦 (関東328)	東京海上火災保険(株)情報ｼｽﾃﾑ部
VT047	第47回	H8.11.20	ネットワークコンピューティングの最新動向	遠藤和弥	日本ユニシス(株) ｵｰﾌﾟﾝ技術部ITｺﾝｻﾙﾃｨﾝｸﾞ 室長
VT048	第48回	H9.1.20	インドの情報産業と海外でのソフト開発について	五十嵐敬 (関東220)	カシオ計算機(株)羽村技術センター 開発部１２開発室室長
VT049	第49回	H9.5.30	ＥＲＰ導入とシステム監査の視点	牧野恭人 (関東362)	(株)産能コンサルティング 取締役コンサルティング部長
VT050	第50回	H9.6.25	コンピュータウイルスの現状と対策	中村 達	情報処理振興事業協会 セキュリティセンター長
VT051	第51回	H9.7.18	新監査基準実務手順書	小野修一、松枝憲司	日本ユニシス(株)、(株)第一コンピュータサービス
VT053	第53回	H9.10.31	「2000年問題」の対応方法とその状況	本村昭二	ソフトウエアジェネレーション(株) 代表取締役社長
VT054	第54回	H9.12.2	情報セキュリティ方針の必要性と策定方法	佐藤慶浩	日本ヒューレットパッカード(株) ﾌﾟﾛﾌｪｯｼｮﾅﾙ・ｻｰﾋﾞｽ事業本部
VT055	第55回	H10.1.23	電子認証サービスの現状と将来	外川政夫	日本ベリサイン(株)取締役営業本部長
VT056	第56回	H10.3.20	大蔵省・通産省におけるシステム監査の取組み動向	荒川幸式	日本ユニシス(株)ＩＴｺﾝｻﾙﾃｨﾝｸﾞ室
VT057	第57回	H10.5.8	ISO9000品質システムり審査登録とその維持	菊本正紀	日本ノーベル(株) 取締役副社長
VT058	第58回	H10.6.24	最近のシステム監査を取りまく状況	澤野 弘	通商産業省情報処理振興課 安全指導係長

◆近畿月例会◆

管理番号	開催数	開催日	テーマ・タイトル
VK015	第15回近畿	H2.7	システム監査計画の立案と効果を満足する施策の実施について
VK016	第16回近畿	H2.9	システム監査の実施手順とサポートシステム
VK017	第17回近畿	H2.9	コンサルタントから見たシステム監査
VK018	第18回近畿	H3.1	銀行業におけるシステム監査
VK019	第19回近畿	H3.3	アメリカ大手企業のシステム監査の最新状況について
VK020	第20回近畿	H3.5	システム開発・保守における効率性の意識について
VK021	第21回近畿	H3.7	経営者のためのシステム監査
VK022	第22回近畿	H3.9	ＫＰＭＧにおけるＥＤＰコントロールに関する考え方
VK024	第24回近畿	H4.1	当社(関西NEC)におけるシステム監査への取組について

◆総　会◆

管理番号	開催数	開催日	テーマ・タイトル	講師(所属支部・会員番号)	講師所属会社
VZ080	第８回	H7.2.17	懇親会		
VZ081	第８回	H7.2.17	特別講演・クライアントサーバーシステムとシステム監査	松尾 明	中央監査法人
VZ090	第９回	H8.2.16	記念講演・「ディジタル・キャッシュ」	太田和夫	ＮＴＴ情報通信研究所
VZ091	第９回	H8.2.16	研究発表会・「阪神大震災特別プロジェクト」		
VZ092	第９回	H8.2.16	映像記録　阪神大震災	毎日放送	
VZ100	第10回	H9.2.21	記念特別講演・「目を覚ませ御人好しの日本人」	ビル・トッテン	(株)アシスト　代表取締役
VZ101	第10回	H9.2.21	記念講演・「システム監査人に物申す」 他特別ﾌﾟﾛｼﾞｪｸﾄ報告「新ｼｽﾃﾑ監査基準実務手順書」	川野佳範 (関東39)	監査法人トーマツ トータルサービス部代表社員

新規入会個人会員

番号	氏　名	勤務先・所属	
828	平山　公一	三菱電機(株)福岡事業所	装生技課
829	国方　重孝	ミズノ(株)	検査役室
830	石川　容	東芝情報システム(株)	システム本部第二システム事業部
831	斎藤　尚志	日本電気ソフトウエア(株)	ビジネスソリューション事業企画部
832	神野　郁也	日本生命保険相互(株)	財務企画部
833	片桐　修	セントラルシステムズ(株)	第一営業部
834	則包　英希	(株)日立情報システムズ	カスタマサービス部
835	森本　優	日本火災情報サービス(株)	顧問
836	堀　正純	(株)ユリーカ	東京開発センター

お知らせ

1．システム監査実践セミナー

今年も、開催します。システム監査未経験の方は、是非ご参加下さい。
詳しくは、32頁に、開催要領と申込書があります。

2．研究会ビデオの貸し出し

協会が行った研究会のビデオテープが借りられます。
貸出規定、申込書、目録が33～35頁にあります。

3．ＥＤＰユーザー団体連合会のシステム監査講演会

平成10年度の標記講演会のパンフレットを同封致します。
本年も当協会が上記講演会の後援を致します。
情報化月間参加の、内容の充実した講演会ですので、奮ってご参加頂きたく、ご案内致します。

訂正　前回の会報48号に誤植がありましたので訂正します。

訂正個所	誤	正
4頁右側上から17行目	実戦順守計画	実践順守計画
8頁左側下から17行目	意義	異議

発行所　日本システム監査人協会
発行人　橘和　尚道
事務局　〒151-0073
東京都渋谷区笹塚２－１－６
笹塚センタービル５Ｆ
(株)産能コンサルティング内
TEL. 03(5350)9268 FAX. 03(5350)9269
ホームページ　http://www.saaj.or.jp/
※ご連絡はなるべく郵便または、FAXでお願いします

会報担当(ご投稿、ご意見、ご要望は下記まで)
三谷慶一郎　(株)NTTデータ経営研究所
TEL. 03(5467)6321　FAX. 03(5467)6322
QZG07732@niftyserve.or.jp
金子　長男　(財)公営事業電子計算センター
TEL. 03(3343)4560　FAX. 03(3343)6758
kaneko@puc.or.jp
富山　伸夫　(株)データ総研
TEL. 03(5695)1651　FAX. 03(5695)1656
GFF00037@niftyserve.or.jp
片寄早百合　日本NCR(株)
TEL. 03(5456)6156　FAX. 03(5456)6436
Sayuri.katayose@Japan.NCR.COM
吉田　裕孝　三井物産(株)
TEL. 03(3285)2058　FAX. 03(3285)9939
Hi.Yoshida@xm.mitsui.co.jp