特定非営利活動法人
SAAJ 日本システム監査人協会報

セキュリティ技術俯瞰

文責　編集担当　木村陽一

セキュリティ技術については、企業での要員のスキル評価などのために、体系化され、そのカリキュラムも作られつつある。また、海外では、認定試験が行われている。今回、日本でのセキュリティ・スキル・マップ、海外における情報システム・セキュリティ・プロフェッショナル認定資格試験等を参照して、そこで体系化されている技術分類を紹介する事にした。

セキュリティ技術俯瞰

セキュリティ技術についてシステム監査人として、どれくらい把握すべきかと言うことについては議論のあるところである。といって、知らないわけにもいかない。とりあえず、いろんな団体からの資料を基に、セキュリティ技術の俯瞰をしてみた。本来は、ここの技術に対してショートコメントをつけるべきであるが、今回は、時間的制約で、分類の紹介だけを行う。今後、コラム的に各テーマを追いかけることができればと考えている。

* 情報セキュリティ・スキル・マップ

IPA（独立行政法人情報処理推進機構）とJNSA（日本ネットワークセキュリティ協会）での情報セキュリティの人材育成にかかる調査研究「情報セキュリティのためのスキルマップがある。目的は、技術を体系化すると言うことよりも、企業や組織で実際の業務にだずさわる人に使ってもらうこと。即ち、情報セキュリティ人材の採用時、企業や組織の人材育成の目標や効果測定の評価基準として、教育機関でのカリキュラムやテストの参考資料として、というのが目的となっている。以下に情報セキュリティスキルでの技術の大分類と、中分類を記載する。なお、記載に当たり下記のURLを参照にした（詳細は、下記URL参照）。

独立行政法人 情報処理推進機構セキュリティセンター
http://www.ipa.go.jp/security/fy15/reports/skillmap/

1. 情報セキュリティマネジメント
   マネジメント技術、リスク分析技術、情報セキュリティポリシー、情報セキュリティ監査、関連知識

2. ネットワークインフラセキュリティ
   ネットワーク設計技術、ネットワークアクセスコントロール、VPN、無線LAN

3. アプリケーションセキュリティ
   (ア) Web
   Webサーバに対する脅威、Webサーバのセキュリティ対策、Web サーバの運用、Webアプリケーション設計、Webブラウザのセキュリティ、Web 関連プロトコルの基礎知識

目　次

特　集　セキュリティ技術俯瞰 1
コンピュータフォレンジックと法制度 4
選挙無効判決　【関連記事　中部支部報告】 6
研究会報告　第 111 回月例研究会報告 7
第 112 回月例研究会報告 9
支部報告　中部支部 13
北信越支部 第 1 回システム監査実践セミナー開催結果の報告 19
SAAJ 理事会議事録 21
第 114 回月例研究会案内 22
saajML 運用規約（CSA） 23
編集後記 24

（イ）電子メール
メールサーバに対する脅威、メールサーバのセキュリティ対策、メールクライアントのセキュリティ、メールサーバの運用
（ウ）DNS（Domain Name System）
DNSサーバに対する脅威、DNSサーバのセキュリティ対策と構成、DNSサーバの運用

4. OSセキュリティ
（ア）Unix
ログ管理、パッチ運用管理、サービスの管理、ファイルシステム管理、アカウント管理
（イ）Windows
構成・設定管理、パッチ適用管理、監査、ログ管理、プロセス管理、サービス管理、ファイルシステム管理、アカウント管理、ネットワーク管理
（ウ）Trusted OS
強制アクセス制御の概念（MAC：Mandatory Access Control）

5. ファイアウォール
ファイアウォールの導入・運用、NAT、ネットワークアクセスコントロール

6. 侵入検知
侵入検知の導入・運用、侵入検知のシステムの機能、検出アルゴリズム、検出方法、侵入検知システム

7. ウィルス
管理体制、感染後のポリシー、予防ポリシー、発病、検出方法と駆除、感染、種類

8. セキュアプログラミング技法
Webアプリケーション、DB、アプリケーション全般、XML、PHP、Java、Perl、VB/ASP、C/C++、UNIX、コンパイラ・仮想マシン、Windows

9. セキュリティ運用
定常運用時のセキュリティ確保、異常時の対応、運用関連情報（脆弱性管理、対策情報、攻撃情報、被害情報）

10. セキュリティプロトコル
アプリケーション層、トランスポート層、ネットワーク層、データリンク層

11. 認証
パスワード認証、バイオメトリクス認証、認証デバイス、認証プロトコル、Web認証、システム認証、シングルサインオン

12. PKI（Public Key Infrastructure）
PKIの利用、証明書と認証、証明書失効、信頼モデル、契約モデル、記述とデータ方式、規格、公開リポジトリ、認証局の構築と運用、法的枠組み、PKIの要素技術、PKIが提供するサービス

13. 暗号
公開鍵暗号、共通鍵暗号、ハッシュ関数、暗号用乱数、鍵管理、ゼロ知識証明、その他の暗号方式、暗号解読・強度評価

14. 電子署名
電子署名の利用、電子署名の要素技術、電子署名の仕組み、電子署名の利点、不正アクセス手法、遠隔不正侵入・操作、サービスの停止、盗聴行為、偵察行為、情報収集、古典的不正アクセス技法

15. 法令・規格
基準・指針・ガイドライン等、法令、国際標準規格、国際ガイドライン、不正コピー防止と電子透かし、不正コピー対策、権利管理技術（DRM）の要素技術、権利記述言語の標準化、法的要件、電子透かしの基本概念、電子透かしの方式、電子透かしの応用形態

＊ 情報システム・セキュリティ・プロフェッショナル認定資格（Certified Information System Security Professional CISSP®）

CISSP®は、米国のNPO（非営利団体）である(ISC)2（International Information Systems Security Certification Consortium）が認定をしており、全世界で30,000名以上（2004年9月現在）が認定を保持している。また、米国連邦政府におけるセキュリティ関連職従事者及びコントラクターにおいて必須資格として認定されているInformation Systems Security Engineering Professional（ISSEP）には、CISSP®取得が前提である。米国の幾つかの企業では、セキュリティ関連業務従事者には、CISSP®を保持することが要件となっている。

ここでは、10のドメインに分けたセキュリティ分野におけるグローバルレベルの共通知識、ベストプラクティスを網羅したCommon Body of

Knowledge (CBK)を発表している。その10のドメインについて以下に記す。ドメイン名とそこに含まれる技術を下記の URL を参照した（詳細は、下記URL参照)。

(ISC) 2 Institute Japan
https://www.isc2.org/japan/index.html

また、以下の書籍も参照した。
ALL IN ONE CISSP® Certification EXAM GUIDE
Shon Harris 著

1. 情報セキュリティマネージメント

組織の情報資産保護の立案、組織でのセキュリティ体制の構築、ポリシー、スタンダード、ガイドライン、プロシージャの定義、リスク分析など。

2. エンタープライズセキュリティアーキテクチャ

コンピュータとネットワークの一般的な構成、企業組織におけるアーキテクチャ設計、様々なセキュリティモデル、コモンクライテリア、ISO15408などのセキュリティ標準・規格など。

3. アクセス制御のシステムと方法論

アクセス制御の概念と方法、アクセス制御に必要なツールと技術、情報システムの動作、使用状況、内容を分析するためのテスト方法及び監査機能

4. アプリケーションセキュリティ

アプリケーションをセキュアにするための原則、アプリケーションソフトウェア設計のエンジニアリング方針、悪質なコードを把握し、それらからの保護手段、開発されたソフトウェアの評価、認証、認定など

5. 運用セキュリティ

情報セキュリティの制御、運用者のセキュリティ管理手法など

6. 暗号学

暗号学の基本概念、公開鍵と共通鍵、暗号方式・アルゴリズムのタイプ、鍵の配布と管理、暗号解読・攻撃方法、デジタル署名など

7. 通信、ネットワーク、インターネットのセキュリティ

ローカルエリア、ワイドエリア、リモートアクセス (ワイヤレス含む)、またインターネット、イントラネット、エクストラネット、ネットワーク通信用プロトコル及びネットワークセキュリティ用プロトコル、各種ネットワークにおけるセキュリティ対策 (ファイアウォールなど) など

8. 物理セキュリティ

施設、データ、媒体、機器、サポートシステム、およびオフィス備品に対するリスク分析など。

9. 事業継続計画

事業継続計画 (BCP)、災害復旧計画とBCPとの違いや事業影響度分析、様々なバックアップ手法など

10. 法、捜査、倫理

コンピュータ犯罪に適用される法律と法的問題、フォレンジック、グローバルで共通した法 (ライセンス問題、知的財産権、輸出・輸入問題等) など。

* (ISC) 2®の正式名称は International Information Systems Security Certification Consortium です。
* (ISC) 2® は International Information Systems Security Certification Consortium の登録商標です。
* CISSP® は International Information Systems Security Certification Consortium の登録商標です。

以上が、それぞれのセキュリティ技術の分類の紹介である。情報セキュリティ・スキル・マップと、情報システム・セキュリティ・プロフェッショナル認定の内容の違いは、前者はOSセキュリティ、ファイアウォール、侵入検知、ウィルス、不正アクセスなどを軸にあげていること、後者は物理セキュリティ（火事などのリスク）とBCPなどが含まれることなどであろう。

監査も米国企業改革法などを鑑みると、様々の法令や規則などに対する準拠性だけでなく、運用上のリスクを評価してそれをいかにコントロールしているかを検証して評価することが求められつつある。情報セキュリティに関しても、マネジメントプロセスが存在して、うまく動いていることは必要であるが、今後、それぞれのリスクに対してどのようにコントロールしているか、それが適正であるかが問われることになる。そうなると、そこで適用されている技術の妥当性や、使い方が適正であるかを検証して評価することになる。その意味では、監査人も、セキュリティ技術に対する専門性を求められると考える。今後、皆さんの、セキュリティ技術に対する知見を会報等で共有できればと考える。

今号は、セキュリティ技術について、会員の皆様に対してメイリングリストで記事の募集を行った。

今回、会員の秋元さんに寄稿いただいた「コンピュータフォレンジックと法制度」は、では、

10「法、捜査、倫理」に対応する。ここでは押収したPCの内容が、改ざんされていないことを示すハッシュ値などの技術的な側面と、それが法的な意味を持つための条件などが議論されている。

また、6月と7月の月例研究会で取り上げたられていた、e-文書、タイムスタンプは、スキルマップでは 12 PKI、13 暗号、14 電子署名、CISSP®では6 暗号などの応用ということに対応する。

このように会報編集委員では、今回の俯瞰分類に沿って今後の技術面での整理を行いたいと考えている。会員諸氏の積極的な投稿、実務面での経験談の紹介を期待する。

コンピュータフォレンジックと法制度

No.895 秋元智広

1. コンピュータフォレンジック

コンピュータフォレンジックと言う言葉を聞いたことがある諸兄は多いと思う。フォレンジックとは法廷を意味する米語であり、一般には、PCやハードディスク、ネットワークなどについて、詳細な証跡を収集し、分析を行なう手法をコンピュータフォレンジックと言う。ただし、厳密に言えば、フォレンジック技法は法廷証拠として耐えうる手段で行われた手続きを保証したものであり、セキュリティ専門家が言うフォレンジックは往々にして意味が異なる。

たとえば、コンピュータやネットワークなどの技術に国境はなくなりつつあるが、法律の適用範囲は主権に基づいて厳格に決定される。そして、フォレンジックは法律に準拠した手続きを求められる。つまり、米国のコンピュータフォレンジックは日本国内においてそのまま適用できない場合がよくあるのである。

こう言われてもぴんとこない人は多いだろう。具体例を示せばわかりやすいかもしれない。たとえば、コンピュータフォレンジックで多く利用されているデファクトスタンダードソフトウェアがある。このソフトウェアはきわめてよく出来ており、証拠価値を担保するための仕組みを技術的に保証している。そのソフトウェアは、PCを調査する際に、ハードディスク内容を一つの大きなファイルに複写し、捜査官の持ったPCに保存する。そして、そのファイルのハッシュ値を日付とともにその場で印刷し、所有者のサインを求めるのである。

このサインの法的な意味は明白である。もし、捜査官が恣意的にファイルを変更し、証拠を捏造すればハッシュ値が変わるので、情報に関しての一貫性を担保している。また、所有者が元のPCのデータを改変しても、捜査官のPCには複写したものがある。そのファイルのハッシュ値と日付を記載した書類へのサインがある以上、そのソフトウェアが技術的に問題を持つことを（所有者が）証明しなければ、同一のハッシュ値を持つファイルに対する抗弁は意味を持たない。

しかし、日本国内ではこのソフトウェアはほとんど利用されない。それは、日本国内において、この手法では証拠価値が担保されないからである。それは技術的な問題ではなく、日本の法廷において、ハッシュ値が同一性を担保する証拠として認められないのである。米国などでこのソフトウェアが利用されるようになったのは、その実効性が広く法廷内で議論され、認知されたためである。

このように、技術面からだけでコンピュータフォレンジックを判断することは大きな危険を伴う。

2. フォレンジック技法と監査手続きの相違

フォレンジック技法は、一般的に仮説検証型のアプローチをとる。すなわち、既に問題が発生した後、その原因を究明するのがフォレンジックの基本的な立場である。簡単に言えば、フォレンジックでは、被疑者を合理的に推定した後、それを証拠で担保するのである。被疑者を合理的に推定するためには、該当の技術的な知識だけでは不足で、業務知識や監査経験、場合によっては捜査経験が求められる事が往々にしてある。証拠価値の担保方法に関しては、さらに法知識と訴訟を前提とした実務的手続きを熟知している事が求められる。

一方で、監査技法はシステムに関する問題点を網羅的に調査するため、不正やインシデントが発生した事後にはほとんど意味を持たない。監査は予防的な側面がきわめて大きく、フォレンジックとは立場が異なっていると言ってもいいだろう。不正を現実にありえるものとして対応していくためにはフォレンジック技法が極めて重要である。今後は、監査的な視点においても、不正対策としてのフォレンジック技法が重要な視点となってくるだろう。

このフォレンジック技法は一朝一夕で身につけられるものではなく、実際に監査手続きを行なうに当たって、不正が発生しえる事を意識し続け、その対応を考えていく事が必要になるだろう。

3. 具体的な事例

不正が現実にありえるものとして対応したフォレンジックと、監査技法でどのような差異が出るか簡単に事例解説をしてみよう。具体的な事例として、フォレンジック対応を意識した社内PC利用規定を考えてみる。

監査上の考え方の一つとして、社内PC利用規定に実効性を持たせるために利用者に対して同意書を求め、PC利用に関して事前同意を求める事が考えられる。同意書には、「社員Aは社内PC利用規定を熟読して、それに関して事前に同意する」旨が記載されることになるだろう。そして、同時に情報管理について社内教育をしていく事が重要だと言えるだろう。これは予防的な意味で十分価値のある対処方法である。

しかし、この考え方では不正の発生を前提としたフォレンジックでは耐えられない。フォレンジックを考慮した場合、同意書は個人単位ではなく、PC単位に要請する事になるはずである。当然、人によっては複数の同意書を提示しなければならない事になるだろう。記載に内容に関しても、「手順や技術的な問題がある場合を除き、PC内の情報の証拠価値に対する異議を唱えない」、「社内PCは業務目的でのみ利用されるものであり、私用目的で利用する事はない」や、「事前に個人に通知する事なくPCの調査をする事に事前に同意する」旨の記載がされるのが一般的である。

おそらく前述の監査的な視点で策定した個人単位に取得した同意書をもとに、別途承諾書なく個人利用のPCを調査する事は、いくつかの深刻な問題を生じさせる危険性がある。

フォレンジックに対応した同意書が、個人単位ではなく、PC単位に求める理由は簡単である。調査した時、「それは私のPC（情報）ではない」という主張を事前に排除するためである。また、利用者に知られる事なくPC調査を行なう前提があるため、業務目的以外の利用禁止を明示し、事前の調査同意も取得しておく必要がある。この意図は、「私のプライバシーがはいっているので調査しないで欲しい」という主張を排除するためである。

このように、フォレンジックを意識した書類には、様々な視点を考慮した記述が求められる。

4. 証拠価値の担保

フォレンジック技法でその中核となる知識の一つに、証拠価値を担保した取り扱いがある。これは、法廷で証拠たり得る価値のある取り扱いを求められるものであり、一般のセキュリティ調査とはその厳密性で大きく異なる。

換言すれば、ネットワークやハードディスクを調査した際に、客観的にその内容が調査されている事を示さなければならないという事である。調査によって、証拠物件が変質される可能性がある場合（ほとんどの調査はこの条件を満たすであろう）は、オリジナルの状態を保証する何らかの仕組みを用意しなければならない。

たとえば、情報漏洩が予想されるPCがあった場合、調査に関する事前同意があったからといって即座に調査してはならない。これは、「調査作業の中で本来存在していなかった情報が書き込まれた」という主張を看過する事になるであろう。一般的には、調査者以外の立ち会いの下で、そのPCのハードディスクを物理的に2台以上複写し、書類でそれらを示す事がまず必要である。この場合、2台複写したハードディスクのうち一台は、調査委員会などで封印の上保管し、残るもう一台を調査目的に利用するなどの厳密な取り扱いが必要である。その書類に関しても必要な項目が網羅されていなければ、証拠価値が毀損されてしまうため、十分な注意が必要である。

5. これからの監査技法

フォレンジックを意識した対応とは、換言すれば、不正の発生を想定した対応であり、すでに、会計監査においては、不正を意識した各種手続きが重視され始めている。

コンピュータフォレンジックは、技術知識、業務知識、法務知識がバランスよく満たされた状態で初めて機能するものであり、これは一般の監査と何ら変わるものではない。ただ、フォレンジックは不正を行なう人の存在を具体的に想起することと、また、一つの手順のミスが全体を無意味なものにしてしまうと言う点で、遙かに厳密な取り扱いを求められるものである。

ここまでで説明してきたように、これからの監査手法にはフォレンジックを意識した対応が求められる事はほぼ間違いない。これからのシステム監査には、このようなフォレンジックの視点を内包した作業を心がけていかなければならないと私は考える。

電子投票市議選無効判決

広報担当　鈴木　信夫

報道によれば、6月8日、最高裁判所第2小法廷（今井功裁判長）は、2003年7月の岐阜県可児市議会選挙での電子投票トラブルをめぐり有権者らが岐阜県選挙管理委員会に選挙の無効（やり直し）を求めた訴訟の上告審で、県選挙委員会の上告を棄却した。この結果、有権者らの申し立てを退けた県選管の裁決を取り消し、選挙を無効とした名古屋高等裁判所の判決が確定した。電子式選挙での選挙無効が確定したのは初めてである。

6月11日、可児市選挙管理委員会は、再選挙の投票日を8月21日と決めた。再選挙は電子投票ではなく、自書式で行われる。可児市は岐阜県南部にあり、人口10万余、市議会の定数は24である。

同可児市議選挙で、投票機が一時停止するなど投開票でトラブルがあり、選挙後、有権者らが可児市選管に選挙結果に不服ありとして異議を申し出て却下され、さらに県選挙管理委員会に選挙無効を申し立て却下されたため、名古屋高裁に選挙無効の訴えを提起していた。

県選管では、裁決前に、電子投票式システムについて、岐阜県にある共立コンピュータサービス㈱と契約してシステム監査を実施した。共立コンピュータサービスには、当協会会員が在籍している。システム監査報告書は、投票機のログ解析結果などを提示し、事実関係の根拠として、県選管の裁決や名古屋高裁の判決に引用されている。

電子投票方式とは、公職選挙法の特例法である「地方公共団体の議員及び長の選挙に係る電磁的記録式投票機を用いて行う投票方法等の特例に関する法律」により実施されるものをいう。

今回のシステムは、投票端末（クライアント機）とシステムを制御する主装置（サーバ機）で構成され、記録媒体は光磁気ディスクで原本と複写の2枚で対になっている。全29投票所で、投票端末189台（予備29台を含む）、投票サーバ58台（予備機9台を含む）で実施された。選挙人は、入場券を提示して投票カードを受け取り、投票端末にカードを挿入して投票画面を呼び出して投票する。

名古屋高裁の判決によれば、午前7時の投票開始後、午前8時半ころから午前9時半ころにかけて、各投票所で投票の記録の失敗や投票記録の遅延という異常が発生した。異常の原因は投票サーバ内の放熱が不十分となり、端末との応答ができない状態になったことである。異常状態は全29ヵ所で発生し、うち1回が17ヵ所、2回が11ヵ所、3回が2ヵ所である。異常が発生した投票所では、投票機の電源を切って再起動したり、第2サーバに切り換えたり、本体の扉を開け、団扇で扇ぐなどの対応が取られた。

異常状態は多くの投票所で、午前9時台に回復したが、午前10時台になった所が9ヵ所、午前11時以降になった所が2ヵ所あった。異常発生時間は、短い所で9分間、長い所で1時間23分間、全投票所での合計時間は15時間33分間（完全停止時間は2時間4分間）である。

異常発生時間中の投票機の状態は不安定で、投票の記録の成功も認められる一方、投票の記録の失敗や遅延もあり、これらが混在した状態にあったとされ、最後まで投票できなかった投票カードが13枚あり、また、実際には光磁気ディスクに投票の記録がされながら投票端末がその情報を受信できなかったため、選挙人、投票管理者、投票立会人、投票事務従事者の全員が投票の記録ができたことを認識できず、不良カードとして処理した投票カードが15投票所で合計25枚発生した。さらに、端末に挿入した投票カードが投票端末から排出されなかったなどにより、正常に使用できなかった投票カードが12投票所で26枚発生した。

開票は、開票所に各投票所の光磁気ディスクを集め、電子投票集計機で集計され、不在者投票分などと合わせられる。光磁気ディスクでの集計は、3回の再開票でも市全体の投票数などと一致した。しかし、選管側が各投票所のログなどをチェックした結果、投票者数と投票数の差が出てきた。判決では、選挙結果に影響を及ぼす虞があると認定しているのは合計27票としている。

最下位当選者の得票数が1361票、次点者の得票数は1326票でその差が35票、27票は動く虞があるとしているわけであるから、後は、トラブルで投票をせずに帰った受付前の待機者が8票以上あれば、選挙結果に異動を及ぼすことになる。

名古屋高裁は、1000人を上回る待機者の証言から、再度投票所を訪れることができなかったため、投票しなかったと推測ないし認定できる選挙人9名を含む多数のものが投票機の異常により投票を断念せざるを得なかったと認め、選挙無効の判断を下している。

裁判では、特例法4条1項1号、選挙人が一の選挙において二以上の投票を行うことが防止できるものであること、同条同項2号、投票の秘密が侵されないものであること、同条同項4号、電磁的記録式投票機の操作により公職の候補者のいずれを選択したかを電磁的記録媒体に確実に

記録することができるものであること、同条同項5号、予想される事故に対して、電磁的記録式投票機の操作により公職の候補者のいずれを選択したかを記録する電磁的記録媒体の記録を保護するために必要な措置が講じられているものであること、同条同項7号、権限を有しない者が電磁的記録式投票機の管理にかかる操作をすることが防止できるものであること、同条同項8号、選挙の公正かつ適正な執行を害しないものであることなども争われている。

名古屋高裁は、これに対し、特例法4条1項1号、4号、5号及び8号の条件を一時的に具備していない状態にあったとしている。

システムとして、2，3時間の連続運転に耐えられなかったことは問題であろう。ただし、メインがダウンした時、サブを立ち上げるまでの許容時間は如何ほどであろうか。まったく無しといくらかあるのでは、システムのコストが違ってくる。また、仮に、いくらかあったとして、システム回復時刻を予告できるであろうか。待機者に、「何時になるかわかりません」というのと、「何分くらいです」といえるのでは、運用上違う。しかし、ここでも予告した時間と大幅に違った時に、どう責任が取れるかという問題が出てくる。

電子式投票をふやしたいとは思われるが、解決すべき問題も多い。

H17.3.9 名古屋高等裁判所選挙無効確認請求事件
http://litigator.jp/decree2005/H170309-2.html

岐阜県公報　可児市議会議員選挙に係る選挙の効力に関する審査の申立てに対する裁決
http://www.gifu-kouhou.jp/gougai/pdf/04091002.PDF

可児（カニ）市
HP　http://www.city.kani.gifu.jp

第111回月例研究会報告

日　時：2005年5月23日
場　所：中央大学駿河台記念館280号会議室
演　題：「システム監査基準の改訂とその経営的意義」
講　師：特定非営利活動法人
日本システム監査人協会
副会長　橘和尚道　氏

報告者 No.1397　近森健三

1．講演要旨

平成16年10月に改訂されたシステム監査基準について、講師が改訂の検討ワーキンググループの委員として参画された立場から、その趣旨や意義について、実際の議論における論点も交えながら解説された。

(1) はじめに
- IT投資の目的が、単なる現場の合理化から経営革新へと大きく変化しつつある中で、国際的動向も踏まえつつ、情報システムに係る新たな「システム監査基準」及び「システム管理基準」を策定した。
- IT　投資が企業全体の経営最適化に資するよう、経営戦略の観点や、情報通信技術の最新動向と情報セキュリティ監査制度との整合性の観点を踏まえた。
- 「システム監査は、組織体の情報システムのリスクに対するコントロールが、適切に整備・運用されていることを担保するための有効手段となり、また組織体のITガバナンスに寄与し、説明責任を果たす役割を持つ。」という、経営的な位置づけを明確にした。

(2) 新システム監査基準の解説
Ⅰ．前文
- 情報システムリスクの拡大により経営リスクが増大し、情報システムにまつわるリスクのコントロール（＝内部統制）の整備・運用が重要な経営課題となっている。
- 米国企業改革法、有価証券報告書等の適正性に関する確認書等、内部統制についての説明責任の意義が高まっている。
- 情報システムのコントロールには、戦略目標の実現や効率性への貢献といった攻めのコントロールと、信頼性の確保や法令等への準拠といった守りのコントロールがある。

・コントロールの目的としては、COSO や経済産業省・リスク管理・内部統制に関する研究会（03.6）における整理が参考になる。
・監査人の行為規範である「システム監査基準」を独立させた。また、情報セキュリティ監査基準と平仄を合わせ、行為規範に「品質管理」を加えた。
・従来の「助言型監査」だけでなく、「保証型監査」にも本基準を利用可能とした。

Ⅱ．システム監査の目的
・「コントロール」「リスクアセスメント」「ITガバナンス」という新しい用語を取り入れて定義した。

Ⅲ．一般基準
・専門能力に関し、システム監査技術者試験の対象者像・役割には経営からの視点や内部統制機能の改善という要素が盛り込まれており、新システム監査基準の考え方を先取りしたものとなっている。
・品質管理について、情報セキュリティ監査基準と同趣旨のものが盛り込まれた。

Ⅳ．実施基準
・監査の手順に関し、予備調査は実施しない場合があるとの議論があったが、情報システムの形態や開発・管理手法が絶えず変化しているため、予備調査の重要性は変わらないとの趣旨から、予備調査を残した。
・監査調書は、監査人が善管注意義務を果たした証左となるため重要である。
・他の専門職の利用について、外部監査の場合は再委託禁止の契約に留意する必要がある。

Ⅴ．報告基準
・基本的に情報セキュリティ監査基準と同趣旨である。
・保証型監査への対応として、「監査の依頼者」「外部への開示」という旧基準にはなかった用語を取り入れている。
・同じ趣旨から、報告書の記載事項として、「制約又は除外事項」という限定付保証意見の概念を採用した。

(3) 新システム管理基準の解説
・経営戦略に沿って効果的な情報戦略を立案し、効果的なシステム投資を行い、またリスクを低減するコントロールを整備・運用する規範として、「情報戦略」（47 項目）が盛り込まれており、旧基準から大きく変貌した。

(4) 経営監査としてのシステム監査の視点
・システム監査人は、経営者の役割・責任体制を評価、経営戦略・情報戦略の評価、全体最適化方針・目標と経営戦略との整合性、情報システムのあるべき姿の明確化、全体最適計画とその遂行状況、情報システム部門の組織・資源の状況、情報化投資計画・投資効果の評価の状況、情報システムの信頼性・安全性の状況、といった視点を持つことが求められている。

(5) おわりに
・CIO が情報システム部門に対し主として求めている能力は「情報システムを活用した戦略の立案」であるという調査があるが、情報戦略の立案者は CIO なのではないか。
・システム監査人は、システム監査の立場から、情報システム部門に対して、CIO の情報戦略立案のために十分な情報提供がなされているかどうかを問う必要がある。
・システム監査人は経営監査能力を求められており、情報システム全般の動向把握のための研究や監査技術の研鑽を怠ってはならない。

2．質疑応答

(Q1) （意見として）今回の基準改訂によってシステム監査が ISO に近似してきた。また経営監査としてのシステム監査という観点については、戦略層を監視するのは監査役であり、システム監査人のミッションがそれと重なってしまう。システム監査は本来監査役がやるべきテーマであるが、過渡的に第三者であるシステム監査人がその役割を担うということなのか。システム監査人協会として、システム監査人の活動を、米国型（SOX 法監査）、欧州型（ISO）のどちらの方向に持っていこうとしているのか関心がある。

(Q2) 新システム監査基準においては全体最適化や戦略の観点のウェイトが高くなっているが、現場の感覚では、果たして実際にシステム監査において経営戦略の観点からの指摘ができるのかとも思う。基準では言わば理想的な形を示しているということなのか。

⇒今次改訂において情報戦略に関する項目をこれほど盛り込まれたのは、検討ワーキンググループにおいてシステム監査に経営監査的な位置づけが求められるようになってきたとの認識が強かったからである。システム全体の有効性や効率性の観点からの監査ができなければシス

テム監査としての意義が薄れてしまう。是非積極的に取り組んで頂ければと考えている。

3．感想

新システム監査基準について、改訂の趣旨や論点となった事項について、当時の議論を交えながら解り易く解説して頂いた。情報技術の進化のスピードと企業戦略の見直しのサイクルとが必ずしも同調している訳ではなく、多くの企業にとっては、経営戦略と情報システムとの整合性についてはそれ自体が永遠のテーマとなっているケースが多いのではないだろうか。システム監査においては、このテーマに対して、情報システムを軸としたアプローチではなく、あくまでも経営戦略を座標軸におき、それが情報戦略に投影される仕組みが構築されているか、現状の情報システムと経営戦略とのズレを発見し、見直し、改善してゆくような内部統制が構築されているか、という観点からアプローチすることが重要となると感じた。

第112回月例研究会報告

1. タイトル

講演テーマ
「システム監査で押さえておくべき情報セキュリティ技術のポイント」
講　師　エヌ・ティ・ティコムウエア株式会社　木村　歳修　氏
会　場　中央大学　駿河台記念館280号会議室

報告者　No.851　大野　勇進

2. はじめに

今回の講師、NTT コムウェア㈱セキュリティコンサルタント木村歳修（きむらとしなが）氏は、ISMS審査員、ITコーディネータ、システム監査技術者／プロジェクトマネージャ／情報セキュリティアドミニストレータ情報処理技術者、MCP、BS7799 Specialist等の資格を保有しておられ、現在、情報セキュリティポリシー策定支援、ISMS認証取得支援をはじめ、個人情報保護関連のセキュリティコンサルタントを中心に、ISMS審査員、セミナー講師としても活動中です。

本日は、最新情報セキュリティ技術のポイントを解説していただき、知識の整理とポイントを習得できると期待しているという紹介で、講演が始まりました。

3. 講演概要

3.1. アジェンダ

下記のアジェンダにそって、まずは、最新技術動向を説明し、次に本日のメインテーマを説明しますということで、解説をいただきました。

【アジェンダ】

Ⅰ．最新の情報セキュリティ技術の動向
　1．安全管理措置のポイント（個人情報保護法20条）
　2．最新ウイルス・ハッカー対策
　3．生体認証
　4．暗号化
　5．e-文書法
　6．ICタグのセキュリティ
　7．IP電話のセキュリティ

Ⅱ．情報セキュリティ技術の組合せや選択のポイント

Ⅲ．情報セキュリティ技術に対する監査のポイント

3.2. 最新の情報セキュリティ技術の動向

システム監査と情報セキュリティ監査は目的が違うので並立できます。

・システム監査
　情報システム構築・運用の全体最適化の観点からの監査
・情報セキュリティ監査
　情報セキュリティ確保の観点からの監査

本日は情報セキュリティ管理基準にそった情報セキュリティ技術の説明が主になります。

情報セキュリティ規格・基準の説明があり、特にISMS認証基準2003の構成を説明いただきました。

3.2.1. 安全管理措置のポイント（個人情報保護法20条）

事業者は、個人情報保護法第20条安全管理措置により、リスクに応じた、必要かつ適切な措置を講じなければならない。

事業者を所管する各省庁において、審議会の議論等を経て、20分野について30のガイドラインが策定され事業者はそれぞれの所轄省庁のガイドラインを精査し実施することが必要です。

安全管理措置のポイントは①組織的安全管理措置②人的安全管理措置③技術的安全管理措置④物理的安全管理措置の、以上4分野にわたってバランスよく情報セキュリティ対策を実施することです。

最近の事例に見るように個人情報はお金になると認識され、顧客情報の漏洩が今後も危惧されます。

情報漏洩の主原因は、①アクセス管理が不十分②データの持ち出し手段の制限措置が不十分の2点が考えられます、この2点を事前にチェックすることがリスクマネジメントです。

こうしたセキュリティ事件からの教訓として、下記の3点がいえます。

教訓1：あらゆる業種で流出事件が多発
明日は我が身
教訓2：経営者の意識の甘さ
顧客拡大戦略で顧客保護意識が薄れた
痛い目に合わないとわからない
リスクマネジメントの欠如
教訓3：性悪説で対策を打つ必要がある

3.2.2. 最新ウイルス・ハッカー対策

ホームページ改ざん、情報漏えい、データ破壊、消去、サービス妨害（DOS）、迷惑メール中継、フィッシング詐欺のような多発する情報セキュリティ事件・事故による有形無形の損失が発生しています。

事業者が情報漏えいした場合の影響は、

・情報資産の損失

ハードの復旧、ソフトの修復、データの再作成費用、再発防止のためのセキュリティ改善費用等が発生します。

・社会的信用の失墜

賠償損害、慰謝料、謝罪広告費用、顧客離れ、株価暴落が考えられます。

また、米企業が懸念するITセキュリティの脅威は下記の通り。（参考）

ウイルスおよびワーム
外部からのハッキングまたはクラッキング
身分詐称およびフィッシング
スパイウエア
サービス拒否（DoS）攻撃
スパム
無線／モバイル・デバイスのウイルス
内部者による攻撃
未公表の脆弱性を突くゼロ・デイ・アタック
ソーシャル・エンジニアリング
サイバー攻撃

これらの脅威に対する対策を事前に打っておくことが重要です、それでもさまざまなリスクが残っていますたとえば未知のウイルス対策、Botにも注意が必要です。

3.2.3. 生体認証

さて、そんな脅威の中、認証技術が重要性を増しています。

認証技術は下記の場面で必要です。

1．ネットワークノードの認証（対向のIP-VPN装置の認証等）
2．業務アプリアプリケーション利用時の認証（グループウェア、勤怠管理ソフトウェア等）
3．ファイルサーバ等のフォルダ・ファイル単位でのアクセス制御
4．利用者の識別及び認証（端末認証、ドメイン認証等）

本人認証の種類は記憶（パスワード）、持ち物（専用カード）、生体認証（指紋、虹彩、声紋、静脈等）がありますが、最近生体認証が注目されています。

生体認証も万全ではありません、他の認証技術との複合化が重要です。

3.2.4. 暗号化

暗号化技術の利用局面は、通信経路の暗号化、記憶媒体の暗号化がありますが、暗号化ツールには、いろいろ問題点があり使ってみなければわからない点があるので、全社導入の前にチェックが必要です。

3.2.5. e-文書法

「個人情報保護法」と同じくH17.4.1に施行されたe-文書法とは、簡単に言えば「紙以外での保存は認めない」と規定している多くの法令を、「スキャナで読み取った電子文書も条件つきで原本としていいですよ」という法令に一括改正してくれる法令です。

注目点は下記のとおりです。

・保管コストの削減効果は経済界全体で年間約3,000億円です。
・電子文書は「カラー文書はカラーで、モノクロ文書はモノクロで」が原則です。
・電子署名やタイムスタンプ等が技術要件として求められます。
・具体的な技術要件は、これから法令毎に決められることになるため、事業者の本格的な対応はH18年度以降になりそうです。

3.2.6. ICタグのセキュリティ

ICタグとは大きさが1ミリ角以下というゴマ粒大のIC（集積回路）チップにIDを記録し、無線電波で読み出しを行う小さなタグ（荷札）で下記のような特徴があります。

・バーコードが数十桁に対して、ICタグは数千けたの情報を保存できます。

・小さな取り付けスペースがあれば容易に導入でき、複製・偽造が困難で、書き換えができます。
・ICタグが付けられた複数の対象物の情報を一括読み取りできます。
・電波で交信するために汚れ・ほこり等の影響を最小限に抑えることができます。
・アンテナ側からの非接触電力伝送で動作するため電源が不要です。

また、今後の利用が期待される分野は、①医薬品や患者にICタグを付けて安全を管理する医療・薬品分野、②産地や賞味期限、流通経路等をICタグに記録し、トレーサビリティを実現する食品分野、②在庫管理の分野等です。

但し、技術の問題もあります。

(1) どの無線電波を使うか？
・使う電波によって届く距離が違う
・無線LANのセキュリティ対策
Wi-Fi Protected Access（WPA）方式
暗号化技術Wired Equivalent Privacy(WEP)
Extensible Authentication Protocol（EAP）等

(2) ICタグの低コスト化の問題
バーコードコスト：2円 vs ＩＣタグコスト：100円

(3) プライバシーの問題
自分の個人情報が自分でコントロールできない恐れがある。
購入した品物に取り付けられていたICタグが、気づかないうちにさまざまな場所で読み取られ、個人の行動が追跡されてしまう恐れがある。
リアルタイムで存在がわかる。
⇒個人監視やストーカーに使われたら・・・・心配？

上記の問題を認識しながら活用することが必要であるが、今後活用が期待され、また確実に普及していくでありましょう。

3.2.7. IP電話のセキュリティ

IP電話とは電話をかける相手との間の通信経路を、インターネットで使用されているIPプロトコルベースで構築した電話ネットワークのこと。

1つの回線を多数の会話で併用できるなどの点で従来の電話よりも回線の使用効率がよく、その分従来の電話よりも低いコストで利用できる。

IP電話と一口で言っても、IP化する場所によって様々な種類があります。
・通信事業者内のネットワーク、インターネット経由等
・電話機、IP電話機、パソコン（IPテレビ電話）等

但しIP電話のセキュリティは基本的にパソコンと同じ、脅威としては、DoS攻撃、不正利用、盗聴等です。

LANポートに「パケット・キャプチャ・ソフト」をインストールしたパソコンを接続することで盗聴される恐れがあります。

無線IP電話も盗聴に弱く、IP電話にもセキュリティ・ホールがあるので、セキュリティパッチを適用する必要があるが、対応が不十分になっています。

DoS攻撃を受けるとほとんどのIP電話サーバがダウンします。

セキュリティパッチは、手作業で一台一台対応しなければいけないケースが多いが“Windows Update”のようにネットワーク経由でセキュリティパッチをダウンロードできる機器もあります。

3.3. 情報セキュリティ技術の組合せや選択のポイント

多くの企業や組織では、事業を行うに当たって情報システムが広範に用いられ、組織の戦略や目的達成に大きく関わっています。

そのため、組織の経営戦略とIT戦略を整合させ、IT投資を適切に管理し、IT要員やその体制、ITに関するリスクのコントロールなどフレームワークを確立すること、すなわち「ITガバナンス」「セキュリティガバナンス」が極めて重要となってきています。

3.3.1. リスクアセスメントに基づく対策

脅威と脆弱性が結びつくと、リスクが顕在化し、情報資産に損失が発生する、この点を注意しバランスの取れたセキュリティ対策を行うことが重要です。

「脅威の例」
不法侵入による盗難、破壊
不正アクセスよる情報漏えい、改ざん、破壊
内部関係者による不正参照、不正持出し、紛失
災害（地震、火災、水害、風害、停電等）
不正ソフト、ウイルスによるデータの改ざん・消去
機器故障、操作ミスによるデータ等の消失

「脆弱性の例」
物理的、技術的な弱点
セキュリティ対策が未実施又は不十分
社員等の意識やモラルが低い

セキュリティ対策機能とは、抑止、防止、検知、回復の4種類をいう、リスクアセスメントに基づく対策としてはこれらをバランスよくおこなうことです。

●「抑止」人に対して、故意によるセキュリティ犯罪や違反を思い止まらせる等、脅威

が発生する可能性を低減することを主目的として法令や組織内ルールの整備を行う。
具体例→不正アクセス禁止法による罰則、組織内の懲戒手続による懲戒処分

●「防止」脅威が顕在化した場合に被害の発生を未然に防ぎ、被害拡大を防止することを主目的として予め対策を行う。
具体例→ファイアウォール、ウイルス対策ソフト、ユーザ認証、ファイル・ネットワーク経路の暗号化、役職員、システム管理者の教育・訓練等

●「検知」脅威が実際に発生した場合にその発生を迅速に発見し、脅威に対してすばやく対応を可能とすることを主目的として予め対策を行う。
具体例→システムのアラーム監視、ログ解析、侵入検知システム(IDS)の導入等

●「回復」脅威の顕在化により発生した被害を正常状態に復元することを主目的として対策を行う。
具体例→事業継続計画、証拠となるログの管理、バックアップツールの導入等

3.3.2. 情報セキュリティ管理の成熟度

組織のISMSの成熟度とは下記の5段階と定義している

0．情報セキュリティポリシーが作成されていない
1．ポリシーはあるが、実行されていない
2．ポリシーを策定し、行動を起こしている
3．全体のマネジメントサイクルが回っている
4．見直しが定期的に行われている
5．全てのサイクルが有機的に結合している

3.3.3. 情報セキュリティ実施の重要成功要因

下記が重要である。
1. 事業目的を反映したセキュリティ基本方針、目的、活動
2. 組織文化に合ったセキュリティの実施方法
3. 目に見える形での経営陣の支持及び責任
4. セキュリティ要求事項、リスクアセスメント及びリスクマネジメントの十分な理解
5. 管理者・従業員に対するセキュリティの効果的な普及
6. 全従業員・請負業者への情報セキュリティ手引の配布
7. 適切な教育及び訓練の実施
8. ISMSの実施状況評価、改善提言のフィードバック

情報セキュリティ管理の成熟度により要求されるセキュリティレベルが違うので、人的対策、技術的対策、物理的対策、組織的対策を実施し、序々にレベルを高度化していくサイクルを実現することが重要です。

3.4. 情報セキュリティ技術に対する監査のポイント

監査のポイントは下記のとおりです。
・企業の成熟度に見合った指摘をする。
・情報セキュリティマネジメントシステム（管理のしくみ）が有効かつ効率的に機能しているかという視点が必要です。
→個別最適より全体最適
・情報セキュリティ技術の監査する側にもIT＋セキュリティの知識がなければ指摘ができない。
→ IT の知識が無い場合、被監査部門の人に操作してもらい、必要な監査証跡を見せてもらう。
・その他の法令・制度等の知識も必要！
IT コーディネータのフレームワークとシステム監査のフレームワークの違い、ISMS プロセスにおける PDCA モデル、個人情報保護法とプライバシーマークの違い、プライバシーマークと ISMS の違いのポイントを知ることも重要です。

4. 感想

短時間のセミナーにこれだけの内容を解説していただきありがとうございました。

短時間であったので、表面的な内容になってしまったのが残念でありましたが、情報セキュリティ技術の整理になり、知識の確認ができました。

資料の不備があり質問もその点の確認にとどまったのも残念でした。

主題の情報セキュリティ技術に対する監査のポイントだけについて、もう一度解説していただきたいと感じました。

今後も技術面での進歩は急速に起こると考えられますので、常に技術面の理解を監査に反映する努力が求められ、監査人としてのスキルアップの必要性を感じた研究会でありました。

JSAG・SAAJ 中部オープンフォーラム 2005

～地方におけるIT技術者の「貢献、育成、連携」～

主催　：NPO 法人　日本システム監査人協会（SAAJ）　中部支部　日本システムアナリスト協会（JSAG）　中部支部

後援　：中部経済産業局、岐阜県、（財）ソフトピアジャパン、（株）名古屋ソフトウェアセンター、（株）三重ソフトウェアセンター　NPO法人ITコーディネータ協会、NPO法人ITC中部

が、下記のような日程・プログラムで行われた。その内容を中部支部から報告していただいた。

1. 開催

開催日時：2005年5月28日（土）　13：00－17：30
会　場　：岐阜県大垣市　ソフトピアジャパン　センタービル
出席者　：

2. 参加者

セミナー参加者	126人	（一般参加者112人、講師・招待者14人）
懇親会参加者	62人	
宿泊者	25人	
オプショナルツアー（万博見学）	16人	

3. プログラム

◆SAAJ四支部合同研究会/JSAG全国大会（並行開催）

13：00 － 13：45	SAAJ四支部合同研究会 講演「電子投票のシステム監査」 SAAJ中部　大野　淳一　氏 於：11F　会議室	JSAG全国大会 各支部からの活動状況報告 中部、関東、関西、九州、北海道 於：1F　セミナーホール

◆合同オープンフォーラム

司会　今尾ひな子　氏
於：1F　セミナーホール

14：00 － 14：15	開会挨拶 実行委員長/JSAG中部　石井成美 来賓挨拶 ソフトピアジャパン理事長　熊坂　賢次　氏 NPO法人SAAJ副会長　鈴木　信夫　氏 メッセージ紹介 中国科学院計算技術研究所副所長 樊建平（ファン・シャオピン）　様より
14：15 － 15：15	セミナー「貢献」「コモンズ型ネットワークと社会貢献」 ソフトピアジャパン理事長　熊坂　賢次　氏
15：15 － 16：00	セミナー「貢献」「これからのIT人材の育成」 JSAG関東・SAAJ正会員　原田　奈美　氏
16：00 － 16：15	休憩
16：15 － 17：15	パネルデスカッション「連携」 「地方におけるIT技術者団体のネットワーク」 コーディネータ　実行委員長　石井　成美 パネラー 近畿地区　清水　順夫　氏 北信越地区　森　広志　氏 九州地区　福田　啓二　氏 中部地区　岡田　博基　氏
17：15 － 17：30	閉会挨拶 SAAJ中部　原　善一郎
	移動
17：40 －	懇親会 於：1F　スリーキャッスル

合同オープンフォーラム開催

実行委員長　石井　成美（No.1224）

情報通信技術の発展に伴い、IT技術者の活躍の場が広がっています。しかし地方におけるIT技術者の活躍はまだ始まったばかりです。その活動を支援し、地域に貢献していくためには、地方におけるIT技術者および技術者団体の交流・連携が必要と考えます。そこで、SAAJ四支部合同研究会とJSAG全国大会を、「愛・地球博」が開催されている中部地区で同日開催し、加えて「地方におけるIT技術者の『貢献、育成、連携』」について議論するフォーラムを企画致しました。システム監査人、システムアナリスト、ITコーディネータなど、120名を超える方々のご参加と、各関係団体からのご後援を頂き、無事開催することが出来ました。全国からご参加と情報提供頂きました各支部の皆様、フォーラムを盛り上げて頂きました講演者、パネラーの皆様、懇親会、二次会を盛り上げて頂きました方々、そして業務ご多忙の中、フォーラムの準備、運営に携わって頂いた中部の仲間の皆様全員に、厚く御礼申し上げます。

今回のテーマでもありますが、パネルディスカッションの最後に、IT技術者の連携、育成、貢献を参加者全員に呼びかけ、拍手の嵐の中でフォーラムを終了できたこの感動を一生忘れません。

ご参加頂きました皆様のご活躍・ご発展をお祈りしますと共に、地域間での交流も深め、更なる連携を強化して行けます様、今後共宜しくお願い申し上げます。

石井

情報処理団体交流への貢献

SAAJ中部支部長 大野　淳一氏（No.784）

中部支部では、他支部や他の情報処理関係団体と積極的に交流を図るといった方針で活動しています。支部の限られた人や予算の中で会員の能力向上及び社会貢献をするには、各方面の組織、人材との協調が重要であると考えるからです。今回の四支部合同研究会を兼ねたオープンフォーラムの開催もそうした活動方針に沿ったものです。

本フォーラムは、中部経済産業局をはじめ多くの公的機関からの後援により開催することができました。特に財団法人ソフトピアジャパンには、会場の提供や理事長熊坂様の講演など格別の支援をしていただき大変感謝しています。参加者は126名。遠方からも多数参加していただきました。

フォーラム終了後に、多くの参加者から、とても有意義であった、参考になった、所属団体の活動に生かしていきたい、新たな活動に発展させていきたいなどの声が聞かれました。図らずも大きな波及効果を感じることができました。

フォーラムの運営にあたっては、ＳＡＡＪ会員として比較的年数の浅い方にも大いに活躍していただきました。また入会して間もない方からも積極的な協力の申し出がありました。活動を継続し発展させていくためには、多くの人を巻き込み、中心となる人が次々と入れ替わっていくのが望ましいと思います。フォーラムの運営上スムーズに行かないこともありました。関係組織との合意形成や案内が遅れたり、運営協力の申し出に迅速に応じられなかったりなど。それぞれ多忙な支部会員のボランティアに頼った活動であり、なかなかうまく行かないこともあります。いずれにせよ本フォーラムのようなイベントの運営を通じて、支部の結束力が高まり、活動が充実していくと考えます。さて、来年は九州支部が加わり、『西日本支部合同研究会』となります。ますます充実した活動になるように努めたいと思います。

第１部 SAAJ 四支部合同研究会

講演「電子投票のシステム監査」

講演者　大野　淳一　氏（No.784）
報告者　山内　英樹（No.1398）

SAAJ4 支部合同研究会として、中部支部長・大野氏より『電子投票のシステム監査』について講演を頂きました。電子投票という、情報システムとしては試行段階、かつ先例の乏しい事象を対象にした監査プロセスについて要点をご紹介頂きましたので、その内容を紹介します。

投票という事象の特殊性とそれをかんがみた考慮のポイントがある。即ち、やり直しができないという１回性から、トラブル予防、本番同等の受け入れテストが必要であること、電子投票の３つに分類される成熟度に応じた選定・調達の考慮点と変更管理の必要性、選挙管理委員会は独立した監査主体でもあるが、それを自覚する必要性、データの原本性と訴訟が起こされたときでも耐えられる客観性を保たせるログの保管の必要性がある。また、これらの根拠として、遵法性が問われる。

電子投票をすすめるために「電子投票特例法（H.13年）」、「電子投票導入の手引き（H.17年）」等の法令が順次整備されている。

監査対象としては特殊なケースではありますが、我々が普段めったに経験できない分野からの知見を与えて下さったこと、および、システム監査行為としての共通項・関わりあいを追体験することができました。さらに普遍化すると、電子化の成熟度・習熟度の高くない事象のシステム構築と監査、公的システムへの監査人の関わりあいといった点で、必ずしも多くの者が経験できない事象を、体験できました。大野さん、ありがとうございました。

第２部オープンフォーラム セミナー講演「貢献」

講演「コモンズ型ネットワークと社会貢献」

講演者ソフトピアジャパン理事長　熊坂　賢次氏
報告者　河田　一宏（NO.1359）

講演は、コモンズ型ネットワークが今後の貢献モデル型の社会に果たす役割について、大局的な視点から解説していただいた。

まず、コモンズ型ネットワークの本質であるクリエイティブコモンズとコラボレーションについて説明があった。クリエイティブコモンズ（共有可能な創造物）は、創造性は私有よりも共有の対象である場合が重要であり、クリエイティブコモンズは、分業ではなくコラボレーションによって獲得されるべきという内容である。

そして成功する条件として、以下の説明をされた。

・自由な個性
・異質なものへの挑戦
・貢献への使命感
・語ることへの気楽さ
・対面での頻度の多さ
・信頼することの勇気
・まずは許容すること
・スーパーフラット

コモンズ型ネットワークは、インターネットに代表される自律分散協調型のネットワークが基盤となり、成立しつつあるとの説明があった。自律した個やグループが分散配置され活動しているが、ゆるやかなネットワークにより全体で協調活動している姿である。この姿は今回のセミナーのような、今後の連携のあり方も示しているように感じた。

続いて、社会システムとしてどのようなモデルがあり、どのように変遷しているかの説明があった。官が公の領域を扱う計画モデルから、現在は民が私の領域を扱う市場モデルへ移行しつつあり、さらに貢献モデルへの移行が説明された。

貢献モデルはネットワークコミュニティであり、その特徴として、豊かさと情報共有、相互低情報支援・探索があると説明された。例として、地域コミュニティ、ボランティア、NPO ネット

ワークを挙げられた。近年のNPOの社会的認知度向上やボランティアの一般化という流れは、貢献モデルの社会への移行という、大きな社会的な潮流のひとつであることが理解できた。

そして最後に、我々が手にしているテクノロジーやネットワークを基盤として、貢献モデルの社会をどのように作り出すか真剣に考える時期が来ていると結ばれた。まさに、システム監査人協会やアナリスト協会は、知識やノウハウをボランティアベースで社会に還元しようと活動している。我々のネットワークも自律分散協調型であり、自律分散した組織がゆるやかに連携する形をとっている。つながりはゆるやかであっても、貢献モデルベースのネットワークであり、次の社会をつくる重要な起爆剤になりうる。「貢献」の意味だけでなく、我々がさらなる「連携」に気づき、こうして行動を始めていることの意義を強く認識できた、すばらしい講演であった。

セミナー講演「育成」

講演「これからのIT人材の育成」
～反復型開発を推進するIT人材
とそのキャリアパス～

講演者 原田 奈美 氏 (NO.709)
報告者 小幡 哲也 (NO.957)

講演は、新しい開発プロセスである反復型開発の有用性と反復型開発におけるIT人材の役割、その育成に向けての課題と対応策について、IT技術者に向けて分かり易く解説したものである。

最初に、ITプロジェクトの現状と課題について触れ、プロジェクトのQCDが想定外となる原因は、従来のウォーターフォール型開発では、Webベースのソフトウェア開発のような新しい開発パラダイムに適用するには限界があるという考え方を提起した。

新しい開発パラダイムには、新しい開発プロセスが必要で、多くの経験から生まれた成功のための実践原則として、反復型開発が登場したというものである。反復型開発とは、反復ごとにシステムの機能を少しずつ開発・テストして、早い時期に動くモジュールを作ってしまうというもので、高いビルを建てる時に、躯体工事、外装工事、内装工事を同時進行で少しずつ進める手法に似ているとして分かり易く説明された。確立された計画と評価基準を最初から決めておいて、開発を進行させるので、結果として早い時期に実行可能なリソースが生成されるため、リスクを可視化できるという考え方である。

反復型開発におけるIT人材の役割として、6区分（分析系、開発系、管理系、テスト系、生産・サポート、その他）に分類して、更に30種類に細分化している。ただし、30人必要という訳ではなく、スキルセットにして、ひとりで何役もできるようにスキルアップすることが必要ですということである。

開発チームの標準編成としては、6区分の内、ユーザ部門のその他を除いた、5つの役割をセットにして、管理者をトップにしたツリー状ではなく、リングにして編成し、開発者とテスターを明確に分けること、プロジェクトサポートを入れること等が特徴で、また、開発フェーズごとに人員を配置するという考え方である。

IPAスキル標準については、コンサル会社が作成したもので、反復型開発には、それとは異なる役割セットが必要であり、特に、テスト担当者、ユーザ部門代表が重要な役割ですという説明があった。弊社の人事担当者は、IPAスキル標準を参考にして、キャリアパス制度を考えているようなので・・・。

反復型開発を実践する人材育成プランとしては、5つの役割区分でステップを踏んだ育成プランが必要で、座学だけでは難しく、育成プランをプロジェクト計画に組み込んで、実践の中で経験を積ませることが大切で、新しい時代に対応するためには、早急に実行する必要があるということであった。

今回のフォーラムに参加している、システムアナリスト、システム監査技術者は、反復型開発で重要な役割を果たすスキルセットの一部をすでに持っているので、頑張ってくださいというような激励で講演は締めくくられた。

講演終了後の質疑応答も活発で、納期遅れの言い訳にしている、ユーザの要求が変わることを前提で開発するという発想の転換が必要ですという話もあった。

私自身が、アプリケーション開発を主な仕事としてきたので、共感できることが多く、技術革新の中で時代にあった人材育成の重要さを改めて認識できた講演であった。

パネルディスカッション「連携」

「地方における IT 技術者団体のネットワーク」

コーディネータ　実行委員長　石井　成美氏
パネラー近畿地区　清水　順夫氏
北信越地区　森　広志氏
九州地区　福田　啓二氏
中部地区　岡田　博基氏
報告者　山崎　敏夫　(No.962)
山内　英樹　(No.1398)

各地区の代表者が、それぞれの所属団体の活動状況について「貢献」「育成」「連携」という各キーワードに従って各支部の活動や状況の紹介をした。各地区に共通の問題することは、地方でセミナーを開催しようとすると、地方で講師を探すのはほとんど不可能で東京から講師を呼んでいる。たとえ地方の優秀な講師がいても東京ブランドの講師ではないため、聴衆者を集める苦労する。このような人材不足や活動の難しさが提起された。このような問題への対応するための努力の様子や、地方の時代を感じさせる変化の兆しも伝えられた。

各氏の印象に残った主張は次の通り。清水氏「技術士との連携、『人材』は地方にもいる。徒党を組んでまずは行動し、存在を示すところから目的・活動・貢献が生まれる」。森氏「既存の会社組織と新しい NPO・ボランティアシップによる組織が社会の両輪をなす」これを柔道の加納治五郎の師匠、武田双六の貢献を事例に紹介（話の面白さが伝えられない雑文をお詫びします）。福田氏「監査人による貢献、出し惜しみをしない」。岡田氏「貢献の恩恵、大学や若者へ（と）のアプローチの必要性、ボランティアは甘えを捨てて、まず善良な管理者としての自覚が必要」。

各氏のキーワードをつなげて解釈すると「情報技術者に関連する我々は、ボランティアという新しい可能性を持つ組織として、情報処理業界や地域に積極的に貢献し、業界の先頭集団として人財（注）を育成していくべきである。この貢献や育成するために、まだまだ弱い我々の組織力を強化するため、個の集まりの交流からネットワークを立ち上げ、より進んだ連携へと結びつけていこう。」ということになろうか。

石井氏には、「貢献、育成、連携」をキーワードに各地区の代表者から貴重な意見を引き出していただいた。最後に、討論の流れをより円滑に、またスパイスも振っていただいた司会の今尾氏にも感謝します。

（注）筆者のこだわりで、あえて人財

第３部ネットワーク作り（懇親会）

若原　達朗 (No.808)

「岐阜県大垣市という地方にいながら、中央の著名な方だけでなく、地方の一般の会員と交流できるなんて...」今回のイベントに関する私の感想はこの一言に尽きます。それを最も感じたのが、総勢62名が参加した懇親会です。いただいた名刺の住所は関東から九州までと広範囲であり、またメーリングリスト等でおなじみの著名な方だけでなく、この機会がなければお会いすることもなかったかもしれない方まで様々で、非常に有意義な時間となりました。

今回のイベントのベースとなった四支部合同研究会は、北信越支部の設立イベントに近畿支部、中部支部からも参加したことがきっかけで始まりました。それまで他支部の方とお会いする機会は、総会等の東京でのイベントに限られていたのですが、今回3回目となるこの研究会は、毎回懇親会においてその支部の方々と直接交流することができ、大変貴重な機会だと感じています。

今回の懇親会では、参加者の方々にたくさんの著書をご提供いただき、ビンゴゲームの景品とする趣向でした。そのため会場にいらっしゃる著者を探してのサイン大会となり、大いに盛り上がりました。私も景品としていただいた本を抱えて会場を探し回り、運良く著者のサインをゲットすることができました。

開始当初の３支部にから中四国支部、九州支部も加わって研究会も拡大し、より多くの方と交流できるようになりました。不慣れな事務局にもかかわらず、遠方から参加いただいたみなさま、本当にありがとうございます。今後も東京でのイベントを中心とする「ハブ＆スポーク型」の交流だけでなく、それぞれの地方が直接つながる、いわば「ネットワーク型」の交流を続けていきたいと思います。

JSAG/SAAJ

中部合同オープンフォーラムを終えて

オープンフォーラム事務局
原 善一郎 (No.124)

感謝、感謝、感謝です。

参加いただいた皆様、ありがとうございます。現在、この報告書を読んでいただいている皆様、ありがとうございます。講師をしていただいた皆様、ありがとうございます。すばらしい講師の皆様が、手弁当で駆けつけてくださいました。

財団法人ソフトピアジャパンの理事長熊坂様、東京の原田奈美様、ほか各地からおいでいただきました。また、地元のソフトハウスであるファイブの今尾社長様はもうひとつの本業であるフリーのアナウンサーとして無料でお手伝いいただきました。

さらに、中国では科学院計算技術研究所の日本窓口として弓長様が私たちのイベントと研究所副所長様との仲を取り持っていただきました。

数多くの組織・団体のご後援もいただきました。一つ一つが力となっております。そして、スタッフとして活躍いただきました皆様には去年の7月からの長期間にわたって、色々な立場でご活躍いただきました。これらの全ての方がこのイベントのために、また、自分自身のために、さらには世界のために、それぞれの方法でご参加いただけた結果が今回のイベントとなりました。

日本システム監査人協会 (SAAJ) とか、日本システムアナリスト協会 (JSAG) とか、そのほかにも多数のITの技術者団体があり、それぞれが独自の活動をしています。地方では、それぞれが独立した団体として動くには規模が小さすぎるために、充実した活動を行うことが難しい状況です。そこで、自然発生的に団体の連合会のような物ができています。中部地方では日本システム監査人協会と日本システムアナリスト協会が相互乗り入れ方式で毎月の例会の開催や、大きなイベントは共同開催となっています。しかし、それぞれは独自の活動もしています。この緩やかなつながりこそ、インターネット時代の社会の有り方を示しているのではないでしょうか。

理論的な説明を (財) ソフトピアジャパンの熊坂理事長様が示していただけました。そして、「情報技術者関連団体連合会」構想を長年にわたって温めていただいていたJSAG会長の清水順夫様の心をリマインドしていただけました。JSAGで語り継がれている「じょうだんれん」が「冗談連」構想ではなく「情団連」という団体として産声を上げる日も近いでしょう。

そして、その役割は、「各団体がオリジナルな情報を提供し」、「情団連は情報をほしがっている人と情報を提供する人の仲立ちをする」という物になるかも知れません。地域は日本だけではなく、地球上を網の目のようにつなげていくのかも知れません。ハードのインフラとしてはインターネットもそのひとつでしょう。私利私欲のためではなく、公利公欲のためでもなく、他利他欲のために働く組織になるのかも知れません。

少なくとも、その組織は従来型のものではなく、地球を包んでしまっているインターネットや会社や個人の生活に入り込んでしまったITや情報通信手段の上に成り立つ、未来型のものになるであろうと期待しています。

日本システムアナリスト協会の全国大会と日本システム監査人協会四支部研究会との合同研究会というハイブリッドな大会を両協会にとって始めて開催できました。そしてそれは東京でもなく大阪でもなく中部の田舎町であるということは、物理的な地域を超えて技術者の交流が進んでいるという証でしょう。

10年後に振り返ると今回の大会が両協会の新しい関係の節目となっていることを期待して止みません。そして、その歴史の証人として皆様がご参加いただけたであろうことに感謝をいたします。

北信越支部だより

No.848 森 広志

北信越支部では、3ケ月毎に各県を持ち回りで県例会を実施しています。今回は、福井県で例会を実施しました。従来例会は、会員の参加を中心としたものですが、今回の福井県例会では、始めて公開セミナー形式とし会員以外の方も参加頂く形式と致しました。

又、昨年から北陸地区の上級システムアドミニストレータからの参加希望がありましたので、上級システムアドミニストレータ連絡会に後援を頂き交流を図ることができました。

以下に、最近実施した福井県例会について簡単にご報告いたします。

福井県例会

1.日 時 6月19日（土）13時30分～

2.場 所 繊協ビル803号（福井県）

3.後 援 福井県商工会議所連合会
NPO ITコーディネータ協会
NPO福井県情報化支援協会
上級システムアドミニストレータ連絡会

4.参加者 25名

5.スケジュール

・セミナー1 13時30～15時30分
「地方公共団体の情報セキュリティ」
敦賀市企画部情報管理課兼IT推進課
課長 川端純一氏
内容：総務省における地方公共団体の情報セキュリティ監査ガイドラインの策定経験に基づきセキュリティ監査、セキュリティ対策の詳細なポイントや最新情報をお話いただきました。

・セミナー2 15時30分～17時30分
「地方公共団体の情報セキュリティ監査実施内容」
講師：福井ネット株式会社
マネージャ 角屋典一氏
有限会社 ビジネス・アイ
取締役 栃川昌文氏
きむら経営会計
公認会計士 木村 善路氏

内容：NPO福井県情報化支援協会の情報セキュリティ監査チームが実施した、地方公共団体の情報セキュリティ監査の監査経緯や手続の概要や今後の情報セキュリティ監査の動向についてお話を頂きました。

6.その他 17時30分～17時40分
「研究会ビデオ貸出について」

7.懇親会
（感想）今回の福井県例会は、部会長の角屋氏を中心に福井県会員の全面協力を得、福井県でご活躍中のITコーディネータの先織理事長、上級システムアドミニストレータ連絡会の吉崎会長、ベテラン有名講師の川端氏、公認システム監査人や公認会計士で固めた情報セキュリティ監査チームなど、多士済々のメンバーの多大なご協力がありました。参加者25名ですが、四国や近畿、中部からも参加があり、北陸地区実施としては盛況と思います。講演内容も専門的で密度があり、詳細な資料説明もあり満足できるものでした。又、懇親会も上級システムアドミニストレータ連絡会やITコーディネータの方々も参加されとても楽しく過ごすことが出来ました。例会を実施するごとに、各県でそれぞれ特色が出てくるように思っています。今後も例会が継続するように工夫してゆきたいと思います。

システム監査実践セミナー2日間コース開催結果の報告

No.735 三輪 智哉

平成17年度第1回システム監査実践セミナー（通算21回目）が、さる6月4～5日日の2日間に渡り、千葉市美浜区の「海外職業訓練協会(OVTA)」において開催されました。

今回は、受講者13名、講師4名の合計17名の参加を得て、成功裏に開催することができました。

以下、その実施結果概要についてご報告いたします。

1. システム監査実践セミナーの特色

2003年、協会の特定非営利法人化及び公認システム監査人制度発足に伴い、事例研究会では、従来のシステム監査実践セミナーの内容をリニューアルして、「システム監査実践セミナー2日間コース」及び「システム監査実務セミナー4日間コース」の2種類のセミナーを開催しております。今回はリニューアル後、通算10回目の開催となりました。

その特色は、事例研究会が「システム監査普及サービス」として実際にシステム監査を実施した被監査企業の監査事例をベースとして教材を作成し、実際には4～6ヶ月かけて実施したシステム監査の実際を足かけ2日間に凝縮して、実

地に体験してもらうという、極めて実践的な演習を主体としたセミナーとなっていることです。

受講者3～4名で1つの監査チームを形成し、監査依頼者の意向確認からはじまってシステム監査報告会に至るまで、チームのメンバーが協業して、システム監査手順を実地に体験することになります。

システム監査の実際を体験できるだけでなく、さまざまな経験や技術を持っている他の受講者との密度の濃い協力を通して、10年来の既知の友人のような関係を創ることができ、この点だけをとっても1度参加してみる価値がありそうです。

また、被監査企業からシステム監査の依頼を受けた後監査報告書の作成まで、システム監査の手順の全てを4日間で体験していただく「システム監査実務セミナー4日間コース」も実施しており、こちらは9月3日～4日及び17日～18日の4日間に渡り、今回と同じ会場において開催する予定となっております。

システム監査を実際に経験したことのない方には、是非1度参加されることをお勧めいたします。

2. 今回のセミナーの日程

今回も、過去のセミナー同様、次のような日程で実施しました。

システム監査の予備調査、本調査、さらには監査報告書の作成を経て監査報告会までを、1泊2日（約26時間）の間に体験してもらいます。

第1日目の日程が終了した夜10時過ぎからは、受講生と講師が入り交じっての懇談会も催され、日ごろの業務などの話に花が咲きました。

3. 受講者について

今回は、13名の方々にご参加をいただきました。うち6名は非会員の方（入会申請中の方を含む）で、システム監査とはどういうものなのか、体験をしていただくことができました。

受講者の受講の目的では、実務経験の経歴とするためとした方が6名、実務のための準備とした方が3名、勉強のためとした方が4名いらっしゃいました。

その受講目的が達成されたかどうかについて伺ったところ、十分達成されたとする方が6名、まあまあ達成されたとする方が7名で、一応の満足は頂いたものと考えております。

4. 教材について

事例研究会が実施したシステム監査普及サービスでのシステム監査事例をベースとして教材を作成しており、今回の教材は、店舗運営に係わる情報システムについての「現在までのシステム化・情報化の妥当性評価」及び「新情報システム企画の情報戦略と情報化計画の妥当性の評価」が監査テーマとなっている事例を使用しました。

5. 講師について

講師は、システム監査技法などに関する説明やセミナー終了後の講評を行うほか、被監査企業の役員や従業員に扮し、システム監査人となった受講生から、予備調査及び本調査時の質問に回答したり、システム監査報告会の際にはシステム監査人に質問をするなど、実践的な役割も演じました。

今回の講師は、事例研究会のメンバーの中から、次の4名が担当しました。

鈴木　実　　吉田裕孝
沼野伸生　　三輪智哉

6. 受講結果アンケートの集計結果について

一方、本セミナーの難易度について聞いたところ、課題によっては、難しかったと回答される方が5～6名に達しました。これは、今までシステム監査の経験をしたことがない方の受講が増えているためと考えられ、それだけシステム監査が社会に普及してきている結果であろうと推測されます。

今回受講された13名は、SAAJの会員が7名（法人会員を含む）、会員外の方は6名となっております。また、ITコーディネータ（補を含む）の資格を保有されている方が5名おり、会員外へのシステム監査の普及の意味でも重要な役割の一端を担っているという感想を得ました。

受講料については、高いと回答された方が2名だったのに対し、ちょうど良いと回答された方が10名、未回答の方が1名で、ほぼ妥当な金額なのではないかと思います。

7. 実践セミナーの今後

事例研究会が主催して実施する本セミナーは、通算で21回、リニューアル後で10回の開催となりました。協会の常設的な活動として定着したものと考えています。

しかしながら、最近受講申込者が頭打ちで、他団体との新たな取り組みも必要な時期になっていると考えております。

また、IT の世界はシステム技術や利用形態の変化がめざましく、これに対応したシステム監査の方法も日々変化せざるを得なくなっています。

そのため、本セミナーを今後も続けていくためには、これからのシステム監査に即応した教材の改訂や製作が重要であると認識しており、

「システム監査普及サービス」を受けていただく被監査企業を発掘し、新たな監査事例の実践を積み重ねていくことが不可欠です。

システム監査普及サービスを希望される企業・団体からの散発的な引き合いもありますが、まだ十分に案件があるわけではなく、会員の皆さんから、システム監査を受けたい企業・団体のご紹介をいただければ幸いです。ご協力をよろしくお願いいたします。

平成17年度第6回理事会議事録 日本システム監査人協会

平成17年6月9日（木）18：30～20：00於：三井物産（株）会議室
出席者：橘和、富山、鈴木(信)、小野, 岩崎、大石、竹下、吉田、松枝、仲、力、芳仲、馬場

1. 審議事項

(1) 平成17年度秋期公認申請募集の件

公認システム監査人・システム監査人補の秋期募集を8～9月、10～12月認定するという提案があり、承認された。

2. 報告事項

（1）監査基準プロジェクト（主査：本田理事→小野副会長）

・監査基準プロジェクトの主査を本田理事から小野副会長に交代する（本田理事が多忙のため)。また、松枝理事, 大石理事を副主査とする。
・「赤本」の出版時期をキープできるようにチェックポイントは6月中，本文は6月末一次原稿 UP、7月末レビュー UP、8月は全体レビューと取り纏め、9月上旬入稿の予定である。

（2）事例研究会（吉田理事）

・実務セミナー（9/3－4, 9/17－18）は金融のテーマで FISC の基準を使用するため、FISC の了解を得た。
・5月25日に FISC 第一部会にc社の監査について発表した。

（3）会報（竹下理事）

・今回の会報は個人情報保護の特集で、発送準備中である。
・86号はセキュリティ技術の特集を企画している。会員に執筆依頼の予定。

（会報に企業名がでることについて検討され、記事の内容が会員に役立つものであれば問題ないという結論になった。）

（4）法人部会（小野副会長）

・自治体向けセミナーの DM を関東地区は6月発送予定。地方は各支部に発送依頼する（今年度はシステム監査を加えて5テーマとした)。

（5）月例研究会（仲理事）

＜第111回（H17.5.23）＞
テーマ：「システム監査基準の改訂とその経営的意義 －システム監査人に求められる経営監査の視点－」
講 師：日本システム監査人協会 副会長 橘和 尚道 氏
参加者：計129名（会員:84名、理事:8名、非会員:37名）
場 所：中央大学 駿河台記念館

＜第112回(H17.6.28)＞
テーマ：「システム監査で押さえておくべき情報セキュリティ技術のポイント」
講 師：NTTコムウェア（株）セキュリティコンサルタント 木村 歳修 氏
場 所：中央大学 駿河台記念館

＜第113回（H17.7.20）＞
テーマ：「タイムスタンプの最新動向」
講 師：株式会社NTTデータ経営研究所 情報戦略コンサルティング本部長・エグゼクティブコンサルタント 三谷 慶一郎 氏
場 所：中央大学 駿河台記念館

＜第114回（H17.8.22予定）＞
テーマ：「COSO-ERM」（仮題）
講 師：日本内部監査協会常務理事・淑徳大学講師 山本 明知 氏
場 所：未 定

（6）認定委員会（鈴木（信）副会長）

・公認システム監査人の申請は 33 名（要件未達1名で面接対象者 32 名）で6月4日に面接を終了した。(公認システム監査人内定者 23 名)
・また、システム監査人補の申請者は 18 名であった。

（7）メーリング担当（岩崎理事）

・公認システム監査人のメーリングに一会員からの広告メールが流れ、会員より苦情がきている。
・→公認システム監査人のメーリングが適正に運営されるようにメーリング担当理事が

メーリングの利用規定を整備していくこととした。

（8）会計担当（馬場理事）
・上期の会計監査は 9 月 18 日に実施される。上期の締めが早くできるように協力をお願いしたい（会計報告が遅い支部があるので、遅くならないように協力ください）。
・交通費などの小額請求分に対して、請求／支払方法の改善要望があるので会計担当で検討して提案したい。

（9）その他
・5 月 28 日大垣で四支部合同研究会（中部支部主催）が開催され、本部を代表して鈴木（信）副会長が出席した。
・6 月 15 日の近畿支部定例研究会にて小野副会長が講師を担当。引き続き行われる支部総会にもオブザーバーとして出席予定。
・システム監査学会の HP に、「システム監査用語プロジェクト」がまとめた「システム監査の用語の定義と解説」が発表された。
・このほか、関連学会，団体の動きについての報告があった。

以 上

議長 橘和尚道
議事録署名人 馬場孝悦
岩崎昭一

＜次回理事会開催予定＞
平成17年7月14日（木）18:30～
三井物産（株）15階金属A会議室
（地下鉄大手町C5出口）

第 114 回月例研究会「組織目標達成に役立つ COSO ERM」のご案内

組織体のコントロールを確かめることが監査の仕事ですが、コントロールが適切であるためには、リスクを軽減するコントロールであるべきで、さらにそのリスクは、ビジネス目標達成に関連するものであるべきです。内部コントロールの定義として世界各国で採り入れられてきた COSO は COSO ERM に改訂され、さらに進化しています。

今回の月例研究会では、COSO ERM の最新動向についてご紹介頂ける事になりました。

COSO ERM は、組織体の使命、戦略目標、戦略、業務目標、リスク、コントロール、モニターリングの流れに沿った全社的取組みの枠組みを示しています。

講師は当分野でご活躍されている、日本内部監査協会常務理事の山本明知氏です。

1. テーマ 「組織目標達成に役立つ COSO ERM」
2. 日時 2005 年 8 月 22 日（月）
18 時 30 分～ 20 時 30 分
3. 場所 中央大学 駿河台記念館285号会議室
4. 講師 日本内部監査協会常務理事
淑徳大学兼任講師
JSSM コーポレート・ガバナンス研究会主査
山本 明知氏
5. 会費 会員 2,000 円 非会員 3,000 円
6. 参加申込
日本システム監査人協会ホームページの申し込みフォーム(SSL対応)にて、
2005年8月16日（火）までにお申し込みください。
7．申込み受理
お申込みの受付ができた場合、特に確認メールは発信いたしませんので、ご了解願います。定員超過で、参加いただけない場合は、メールでその旨お知らせいたします。
申し込み確認画面をプリントし当日受付へご提示下さい。
8．参加費の授受
参加費は、当日受付で、現金でお払いいただき、同時に領収書をお渡しいたします。（請求書は発行いたしません）。
9．会場案内
所在地 〒101-8324
東京都千代田区神田駿河台3-11-5
中央大学駿河台記念館

SAAJ メーリングリスト運用規約
（公認システム監査人等用）

平成17年7月14日
NPO日本システム監査人協会

1．目的

本規約は、特定非営利活動法人日本システム監査人協会（以下「SAAJ」という。）認定の公認システム監査人及びシステム監査人補（以下「公認システム監査人等」という。）用に設定するメーリングリスト（以下「ML」という。）の運用規約を定め、公認システム監査人等相互の情報交換及びSAAJ事務局からの情報提供を円滑に行い、公認システム監査人等のレベルの向上に寄与することを目的とする。

2．ML アドレス

saaj-csa01@mlc.nifty.ne.jp （注)MLアドレスは、安全性確保のため変更することがある。

3．ML への登録対象者

SAAJ認定の公認システム監査人及びシステム監査人補並びにSAAJ事務局（公認システム監査人認定委員会を含む）とする。

4．ML への登録

MLへの登録は、希望者のみとする。また、登録メールアドレス（以下「アドレス」という。）は、原則一人1アドレスとする。

なお、携帯電話用のメールアドレスは、登録することができない。

5．ML 運用上の約束

(1) 一般常識となっているネチケットを守ること。
(2) コマーシャルベースのメールは送信しない。ただし、協会からの発信を除く。
　　例：自己が主催（関係）する研修会・セミナ等の案内、商品の宣伝、各種勧誘　等
(3) SAAJ 事務局が発信する主な内容
　① 公認システム監査人制度に関する事項
　② 他関連団体等のセミナ等の案内
　③ 協会承認の広告メール
　④ その他、公認システム監査人等に対し有益と思われる情報
(4) 着信メールの転送の禁止
本MLの登録アドレスに着信したメールを本人以外（例えば、他のメーリングリスト）に自動転送しないこととする。

6．ML 運用上の約束を守らなかった場合の措置

上記5項で定めた約束を守らなかった場合は、本MLにおいて発信者に対し警告を発し、一定期間（2週間程度）経過後、本MLへの登録を抹消する。発信者（ML抹消者）は、抹消後1年間は、本MLへのアドレスを登録することはできない。

なお、本措置について、登録を抹消する権限については、ML担当に委ねるものとする。

7．登録・変更・登録抹消

MLへの登録・変更・登録抹消については、ML担当者までメールで連絡する。
連絡内容は、以下のとおりとする。
① 氏　　名：
② 認定番号：
③ 旧アドレス（登録抹消）：
④ 新アドレス：

8．ML 運用者および連絡先

本MLの運用は、SAAJ理事会におけるML担当とし、責任者は、ML担当主査とする。
連絡先は、SAAJ事務局又は、ML担当とする。
SAAJ事務局：saajjk1@titan.ocn.ne
ML担当　　：owner-saaj-csa01@mlc.nifty.ne.jp

以　上

《編集後記》

個人情報漏洩問題をはじめ、今日ほどセキュリティ問題が注目を集めていることはないのではないか。セキュリティの確保が十分に行われなければ、始まったばかりのインターネット革命が頓挫しかねない。システム監査人としてもセキュリティに関する技術的、法的、社会的知識を深めなければならない。そこで、今回からセキュリティ技術に関する連載を開始することにした。連載を始めるにあたり、セキュリティ技術の全体像を掴むために「セキュリティ技術俯瞰」を、また、各論の第一回として、極めて今日的な話題であるコンピュータ犯罪追跡手法「コンピュータフォレンジック」を掲載した。

セキュリティ技術（純粋の技術だけではなく、マネジメント、法制度等を含む）の連載は、会員各位の投稿による。ご協力をお願いしたい。

可児市の電子投票市議選の選挙無効の判決が最高裁で確定するという前代未聞の事件があった。本件は、今回確定した名古屋高裁の判決に、事後に行われたシステム監査の報告書が引用されているなど、本協会に関係の深い事件である（「選挙無効判決」記事参照）。

セキュリティ問題といい、選挙無効判決といい、コンピュータネットワークシステムが社会インフラとしていよいよ大きな位置を占めてきたことが実感される。インフラとしてのシステムの安全性、信頼性の確保をミッションのひとつとする我々システム監査人の任の重さを痛感する。（藤野 明夫）

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　〒103-0025
東京都中央区日本橋茅場町2-8-8
共同ビル（市場通り）6階65号室
TEL. 03(3666)6341　FAX. 03(3666)6342
事務局メール：saajjk1@titan.ocn.ne.jp
ホームページ　http://www.saaj.or.jp/

会報担当委員
竹下　和孝　池島　晃
富山　伸夫　須田　勉
吉田　裕孝　木村　陽一
仲　厚吉　藤野　明夫
力　利則　山田　正寛

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