特定非営利活動法人
日本システム監査人協会報

2012年10月号
No 139

No. 139(2012年10月号)＜9月20日発行＞

今月号も
興味ある記事・新しい記事満載です。
ぜひ　一読を！

コスモス(愛知・なばなの里)

会報電子版の記事　目次

〈目次続く〉

投稿

めだか１　【各当事者がシステム監査の本質的な弱点を認識して（システム監査のすすめ）】

“システム監査のすすめ”をテーマとした会報も今月が最後のようです。

そこで、最後の“システム監査のすすめ”で、あえてシステム監査の本質的な弱点について考えてみたいと思います。

（尚、ここでは、所謂“助言型”の監査はコンサルティングの範疇と考え、“保証型”の監査を想定します。）

私は監査人としての経験から、監査には次の３つの大きな、また、しっかり認識すべき本質的な弱点があると考えています。

まず一つは、監査人の監査対象に関し保有する情報量は限られるということです。

そもそも監査人には、監査であるが故、監査対象からの独立性が求められます。これは、監査人は監査対象に何ら責任、権限を持つ立場にない、すなわち監査対象からは第三者的立場の人であるということを意味します。

従って、監査人は監査対象について十分情報収集するとはいっても、やはりそこには本質的な限界があると考えなければなりません。

二つ目は、監査は内部統制も拠り所としてサンプリングで実施するので、論理的には不適合の発見漏れがあり得るし、また、内部統制の弱点（限界）は監査の弱点ともなるということです。

そして三つ目は、計量化された規準と物理的対象物の対比による測定、計測と異なり、監査は監査人による、評価規準と実態とのギャップ判断を踏まえた意見表明であり、理屈の上では監査結果の再現性があるとしても、実際は監査人の人間であるが故の不完全性や、評価規準の曖昧さ等によって、監査人により判断が異なる（監査結果の再現性がない）場合もあり得るということです。

そして、この３つの弱点に対し、監査では“合理的”という言葉を充てて、被監査部門自らの正当性の主張に対し、監査人が“合理的な保証”を与えると整理しているようです。ここで“合理的”とは、監査人が必要な注意を払い、行うべき確認手続を踏んだ上で出した結論の意見表明は、相応の信頼性を持つということです。

監査依頼者も、監査人も、そして監査人の結論（意見表明）を利用する人も、この弱点をよく認識した上で、完璧ではないが人間の知恵の産物である“監査”を、関係当事者相互の信頼関係維持に役立てていこうという姿勢が必要ではないかと思います。

特に、急速に進歩・発展するＩＴに関しては、その影響力の大きさの裏側にあるリスクを認識しつつも、しかし関係当事者がそれを恐れず積極果敢に利・活用し、社会の一層の質の向上に役立てていく、そのための人間の知恵の一つとしてシステム監査が求められていると考えてはいかがでしょうか。

（広太雄志）

（このコラム文書は、投稿者の個人的な意見表明であり、SAAJの見解ではありません。）

めだか２　【見えざる手と同感（システム監査のすすめ）】　　投稿

「見えざる手（invisible hand）」は、アダム・スミスの『国富論（An Inquiry into the Nature and Causes of the Wealth of Nations）』にある言葉です。ここでいう「見えざる手」は、市場の価格調整メカニズムを意味していると言われています。「見えざる手」は、『国富論』で1か所のみに出てくると言われており、その箇所を引用します。

“どの個人も、できるだけ自分の資本を国内の労働を支えることに用いるよう努め、その生産物が最大の価値をもつように労働を方向づけることにも努めるのであるから、必然的に社会の年間の収入をできるだけ大きくしようと努めることになる。たしかに個人は、一般に公共の利益を推進しようと意図してもいないし、どれほど推進しているかを知っているわけでもない。[中略]個人はこの場合にも、他の多くの場合と同様に、見えざる手に導かれて、自分の意図の中にはまったくなかった目的を推進するのである。それが個人の意図にまったくなかったということは、必ずしも社会にとって悪いわけではない。自分自身の利益を追求することによって、個人はしばしば、社会の利益を、実際にそれを促進しようと意図する場合よりも効果的に推進するのである。（『国富論』四編二章）”

しかし、市場参加者の利己心だけでは、市場が公共の利益を促進しないことは言うまでもないと思います。アダム・スミスは、『国富論』とともに、人間本性を洞察し、『道徳感情論（The Theory of Moral Sentiments）』を出しており、『道徳感情論』の中で、秩序を導く人間本性、繁栄を導く人間本性、国際秩序の可能性について議論をすすめています。人間本性は、利己心の働きとともに、「同感（sympathy）」が働くとしています。『道徳感情論』では、人間本性は、感情や行為の「対象」について、当事者としての自分の中に、もうひとりの胸中の公平な観察者(impartial spectator)としての自分がいて、「同感」の意思やフェアプレイの態度が表われると言われています。

さて、アダム・スミスによる人間本性への洞察や調整メカニズムを考えてみたいと思います。マネジメントシステムにおいて、「見えざる手」とは、事業運営において、PDCAサイクルが回ることによって、事業の良循環が自律することに比定されると思います。また、「同感」とは、マネジメントシステムの教育や監査の視点で考えてみると、教育によって、もうひとりの胸中の公平な観察者としての自分が育てられて同感し、また、監査によって、もうひとりの胸中の公平な観察者としての自分があらためて表われて同感することとに比定すると考えて良いと思います。

ここで、教育は、マネジメントシステムの管理者などが、それを担う役割であると思います。監査は、被監査者の胸中に公平な観察者としての自分が表われて同感するための働きかけであると考えると、監査人の役割や責任の本質が見えてくるようです。システム監査人として、このように考え、情報システムの健全性のために、システム監査をすすめていきたいと思います。

「アダム・スミス 『道徳感情論』と『国富論』の世界」 堂目　卓生　著（中公新書）

アダム・スミス：18世紀、人間の理性を重んじる啓蒙の世紀のイギリスの経済学者・倫理学者

（空心菜）

（このコラム文書は、投稿者の個人的な意見表明であり、SAAJの見解ではありません。）

めだか３　【システム監査人が〝醍醐味〟を感じるとき　（システム監査のすすめ）】　投稿

〝醍醐味〟いい響きです。　〝醍醐味〟どんな味でしょう。

（辞書で味わってみると→深い味わい。本当のおもしろさ。美味の最高のもの。最高の味わい。）

システム監査において、システム監査人が醍醐味を感じるのはどのようなときでしょうか？

CSA、ASA 100人に聞きました。

『あなたがシステム監査で醍醐味を感じるのはどのようなときですか？』

この質問の回答を分類したところ次のような傾向が表れました。

A.内面に関すること　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・○○％
- a1.自己の能力向上が図られた　・・・・・・・・・・・・・・・・・・・・・・・・・✖件
- a2.精一杯仕事をしたと自負できる　・・・・・・・・・・・・・・・・・・・・・・・✖件
- a3.監査チームで切磋琢磨した　・・・・・・・・・・・・・・・・・・・・・・・・・✖件
- a4.・・・　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・✖件

B.成果に関すること　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・△△％
- b1.監査結果（報告書）が高評価を得た　・・・・・・・・・・・・・・・・・・・・・✖件
- b2.改善提案が定着・根付いている　・・・・・・・・・・・・・・・・・・・・・・・✖件
- b3.システム部門の現場から喜ばれた　・・・・・・・・・・・・・・・・・・・・・・✖件
- b4.・・・　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・✖件

←これは、
フィクションです。

※CSA：公認システム監査人
ASA：公認システム監査人補

このようなアンケートをした場合、実際はどのような結果が得られるか。大変興味があります。

システム監査の状況は様々です。例えば、組織内の監査人は宮仕えならではの苦労や歯がゆさがあるでしょうし、外部の監査人は作業上の制約があったとしても気がねなく指摘できる面があるかも知れません。醍醐味は苦労や困難と表裏の関係にあると思いますので、それぞれの監査人によって感じる醍醐味は異なることでしょう。
醍醐味という美味を感じられる五感を大切に監査活動することは、結果としていい仕事をすることにもつながると思います。

私自身はいつどこでどんな醍醐味を感じただろうか。経営にインパクトのあるシステムリスクを発見し改善案に結びつけたときがそうであったか、目の付けどころや状況判断に関心を寄せられたときであったか、聞く力・伝える力が日々増していると実感したときだったか。

システムを点検・評価するたびに感じていたわけではないが、思い起こしてみればシステム監査をしている場面だけでなく、システム監査の意義を感じて参加する諸活動にも醍醐味を感じたものがあります。

このような醍醐味は、「マズローの欲求段階説」のどこに位置付けられるのでしょうか。
この味覚はどこで感じるのでしょうか。視・聴・触・味・嗅の五感でしょうか。
その味覚を敏感にして醍醐味を逃さずに味わいたいと思っています。

用例：登山の醍醐味

（山の彼方）

（このコラム文書は、投稿者の個人的な意見表明であり、SAAJの見解ではありません。）

めだか４　【クラウド事業者のシステム監査（システム監査のすすめ）】　　投稿

「クラウドサービスの利用」という形態を選択する企業が広がりを見せ、情報システムを「所有」から「利用」へと移行しています。このような状況下で「グローバル・クラウド時代に向けたシステム監査のあり方」をテーマにした講演会の開催、システム監査研究会の報告等がインターネット上を賑わしています。

ただ、現状としては、利用する企業などは事業者がどの程度の安全性を確保しているか分からず、国際的に統一された指針がないことが問題視されています。

経済産業省の動向について、2012年8月30日の日経新聞朝刊で次のような記事が掲載されました。

“経済産業省はクラウドサービスの安全性向上に向け、米国や英国と連携して国際的な指針を作る方針だ。サーバー攻撃や災害が発生してもデータが消失しないようにする。本格的な普及をにらんで安全対策を強化する。・・・<中略>・・・経済産業省は米国や英国と共同で、工業製品などの国際的な安全基準を決める国際標準化機構（ISO）などで基準の策定に着手する。英米など15カ国程度が参加し、2014年4月をメドに最終案を固める。・・・<中略>・・・新たにまとめる指針は国際標準になる見込みで、各国はサービスを提供する事業者などに指針に沿った安全性の強化を求める。同省は国内向けの指針も改定する。具体的には、利用者から預かっているデータの保管を徹底することなどを盛り込む国際基準に先駆けて2013年4月にまとめる。”

経済産業省では、国内向けの指針、国際標準化に向け取り組まれているが、指針等が公表されるまで、システムの仕組みもグローバル化し、変化しています。当然、監査のあり方を見直す必要があると思われます。

指針が公表されるまで、クラウド事業者の監査の視点は、以下の内容となります。

1. 安全管理措置
   - ・クラウド利用者に識別情報を発行・更新・廃棄する機能を提供しているか。
   - ・不正アクセス対策として、侵入検知システム（IDS）やDos/DDos攻撃対策等を実施しているか。
   - ・最新動向を反映した信頼性の高い脆弱性診断（ペネトレーションテストなど）を実施しているか。
   - ・システムログやクラウド事業者のシステム管理者や運用担当者の作業ログを取得し、チェックし、保管しているか。
   - ・バックアップの周期、媒体、保存期間、保管場所等を定め、運用しているか。
   - ・保管している個人情報や機密情報を必要に応じて暗号化しているか。
   - ・データセンターは、耐震構造・免震構造、停電対策、空調、消火、雷対策を採用しているか。
2. 契約書、利用規約、約款、サービス内容、内部規程、記録等
   - ・サービス稼働率、障害発生頻度、障害時の回復目標時間などのサービスレベルを定めているか。
   - ・クラウド事業を営む国、データセンターが所在する国を明らかにしているか。
   - ・情報セキュリティ管理者及び苦情・相談窓口を公表しているか。

クラウド利用者は、クラウド事業者との契約前、契約後、上記のチェックを怠らないようにすることが大切です。

参考文献 ： クラウドサービス 安全利用のすすめ IPA　2011.11.8 第２版

（くぎ煮）

（このコラム文書は、投稿者の個人的な意見表明であり、SAAJの見解ではありません。）

投稿

■【個人情報システム監査の提言】　　会員番号 557　仲　厚吉（個人情報保護監査研究会）

個人情報保護監査研究会では、経済産業省システム管理基準に個人情報保護コントロールを追補するよう提言しています。ここでコントロールとは、監査チェック項目をいいます。事業者が、個人情報の取扱いで情報システムを利用している場合、個人情報保護監査の中で、個人情報を取り扱う情報システム（以下「個人情報システム」という）への監査が求められます。個人情報システムへの監査を行うにあたっては、監査チェックリストの中に、個人情報保護コントロールを追加して監査します。当研究会では、事業者が個人情報システムを利用している場合、監査チェックリストの中に、以下のシステム管理基準個人情報保護コントロールを規範として、コントロールを追加して監査することを提言しています。

【システム管理基準個人情報保護コントロール】

VI. 共通業務() 8. 個人情報保護(12)

8.1 個人情報の取扱いに関する方針(4)

(1) 個人情報の取扱いに関する方針の策定及び公表並びに責任体制の確保は、個人情報の保護に関連する法令等に準拠して定めること。

(2) 個人情報の取扱いに関する方針に基づいて、個人情報システムの開発、運用及び保守の計画を定め、個人情報保護管理者が承認すること。

(3) 個人情報システムの開発、運用及び保守の計画は、計画を実施及び運用するため、方法、体制等を明確にすること。

(4) 個人情報システムの開発、運用及び保守の計画は、個人情報の正確性の確保及び個人情報の漏えい、滅失又はき損のリスクに応じ、必要かつ適切な安全管理措置を明確にすること。

8.2 本人の権利・利益の保護(6)

(1) 個人情報システムは、個人情報の取得に当って、利用目的を明示し、利用目的の偽りなどにならない措置を講じること。

(2) 個人情報システムは、個人情報の入力に当って、本人から利用目的の認識又は同意を得る措置を講じること。

(3) 個人情報システムは、個人データの利用に当って、取得に際して特定した利用目的に合うように出力を制限する措置を講じること。

(4) 個人情報システムは、保有個人データの開示等の求めに応じる措置を講じること。

(5) 個人情報システムは、苦情及び相談の処理に応じる措置を講じること。

(6) 個人情報システムは、個人情報の保管期間と廃棄の過程が明確である措置を講じること。

8.3 個人情報の利活用(2)

(1) 個人情報システムは、個人情報の有用な利活用のため、個人データベース等を維持管理する措置を講じること。

(2) 個人情報システムは、個人情報の保護に関する法令、ガイドライン等に準拠し、個人情報を公共のために提供できる措置を講じること。

個人情報保護監査研究会では、上記の個人情報保護コントロールについてさらに詳細化したサブコントロールを提言しています。 詳しくは、当研究会にお問い合わせください。

以上

■【マネジメントシステム規格の動向】　　会員番号 1790　吉谷 尚雄（個人情報保護監査研究会）

現在、ISO9001(品質)、ISO14001（環境）、ISO27001（情報セキュリティ）を始めとして、多くのマネジメントシステム規格が発行され、審査機関により認証が実施されています。

複数のマネジメントシステムの認証を受審する企業にとって、方針、目標管理、マネジメントレビュー、文書管理、記録管理、内部監査、不適合、是正処置など、同じ ISO 規格にも関わらず規格要求事項に差異があり、その項目番号、用語の定義も異なっていることから、多くの企業にとって規定類の重複を招いています。

ISO9001(品質)、ISO14001（環境）、ISO27001（情報セキュリティ）を始めとして、多くのマネジメントシステム規格が発行され、審査機関により認証が実施されています。複数のマネジメントシステムの認証を受審する企業にとって、方針、目標管理、マネジメントレビュー、文書管理、記録管理、内部監査、不適合、是正処置など、同じ ISO 規格にも関わらず規格要求事項に差異があり、その項目番号、用語の定義も異なっていることから、多くの企業にとって規定類の重複を招いていました。

ISO では、ISO/IEC 規格を制定する際に従うルールのひとつである、“ISO/IEC Directives（専門業務用指針）補足指針の附属書 SL”（以下、附属書 SL）が 2012 年 5 月に発行しました。今後制定・改正される ISO マネジメントシステム規格について、目次タイトルとその構成の共通化、（分野共通の）要求事項の共通化、（分野共通の）用語の定義の共通化が定められています。

今後の ISO マネジメントシステム規格の制定と改訂により、規格要求事項の3割程度が共通化されることから、企業の規定類のスリム化、シンプル化を見据えた統合マネジメントシステムの構築が進むと予想されます。

・ISO22301(事業継続)「緊急事態に際し組織が事業を継続していくためのマネジメントシステム」が 2012 年 5 月 15 日に正式発行されています。JIS 化(日本語)も予定されており、共通化の全貌が明確になります。
・ISO39001（道路交通安全）「道路における交通事故死亡者，重傷者の根絶を目標とするマネジメントシステム」は 2012 年 11 月正式発行が予定されています。
・ISO27001(情報セキュリティ)は 2013 年 10 月正式発行を目指しています。
・ISO14001(環境)は 2015 年正式発行を目指しています。
・ISO9001(品質)は 2015 又は 2016 年正式発行を目指しています。

ISO が目指している統合マネジメントシステムは、単に品質／環境マニュアル等を頂点とする企業の規定類を統合することや、審査機関が品質／環境等の審査を効率的に同時や連続して実施することではありません。個々の企業に ISO マネジメントシステム構築以前から企業に存在する本来の業務プロセスへの統合です。その統合の核となるのが、新しいマネジメントシステム規格 6.1 項「リスク及び機会への取り組み」です。個々の業務プロセスに対してどのようなリスクがあり、リスク対策がどのようにされているかの視点です。業務プロセスのリスク分析を行い、リスクの高い部分のリスクを発生する前に下げる。（未然防止）と考えれば、新しい要求事項の共通化の中で“予防処置”が項目から消えたことが理解できるものと思います。

6.1 リスク及び機会への取り組み(JIS化前の仮訳、××には例として“品質”等が記述されます。)

××マネジメントシステムの計画を策定するとき，組織は，4.1 に規定する課題及び 4.2 に規定する要求事項を考慮し，次の事項に取り組む必要のあるリスク及び機会を決定しなければならない。

－　××マネジメントシステムが，その意図した成果を達成できることを確実にする。

－　望ましくない影響を防止，又は低減する。

－　継続的改善を達成する。

組織は，次の事項を計画しなければならない。

a)それらのリスク及び機会への取組み。

b)次の事項を行う方法。

－　その取組みの××マネジメントシステムプロセスへの統合及び実施。

－　それらの取組みの有効性の評価。

以上

■【システムの上流工程の監査と予兆型監査の重要性】　　会員番号 2090　遠藤　誠

これまでの金融機関の内部監査部門がシステム監査を実施してきているが、どうして上流工程の監査が十分には実施できていなかったのであろうか。内部監査部門の企業内における位置づけや内部監査部門の歴史等、その理由は多種多様と思われるが、中心となっている理由は以下の五点ではないかと思われる。

第一に、本社の企画・業務部門や管理部門等は、経営の方針や戦略そのものを構想する部署であり、経営と密接に結びついた組織である、ということがあげられると思う。これらの部門への内部監査の実施は、直ちに経営への監査を行うことと同義語になるということである。本社の中枢部門が、経営陣に諮りながら練り上げた構想そのものを監査するとは「畏れ多いこと」という意識はどの金融機関にもみられるところである。また、上記のような背景から、一般的には「本社無謬説」が実質的には存在しており、監査そのものの対象とするという発想すら起きない企業も多いのである。

第二に企画構想段階の監査については、監査の常道である、「明確なエビデンス」がなかなか提示できないという根本問題がある。さまざまな問題（将来大きなリスクを惹起させそうな検討不足や仕組みの不備など）を発見しても、それが発現する絶対的な確証が得られない、ということである。例えば、開発規模に比べて、開発期間の確保が十分でなく、特にシステムテスト期間が通常の半分程度しか確保されていないケースがあったとしよう。
こういうケースに対して、「絶対に安定的なカットオーバーは不可能」と断言できないという悩みである。せいぜい「うまくいかない蓋然性が高い」としかいえないのである。こういう状況に対して、「経営がそのリスクを取っている」と言い切られてしまうと、内部監査部門がそれ以上は追及できない。このため、相当の見識や力量のある内部監査部門でも、結果監査を選択しがちなのである。結果監査のなかで、大規模なトラブルになったようなケースを取り上げれば、「テスト期間の確保が十分ではなかった」とか、「変更管理が十分にできておらず、プロジェクトリスクの管理ができていない」等々、事実に即してどんな厳しい指摘をしても、監査を受ける方は「ご指摘ごもっとも」と答えるしかない。裏付けのある、絶対

的な事実を積み上げながら、方針の不徹底や仕組みの問題を追究するという内部監査のプロセスからいえば、結果監査のほうがやりやすいのは当然である。 しかし、結果監査では遅すぎるのである。起きてしまった原因を、後からいくら言い募られても、失敗したプロジェクトは戻ってこない。リスクベースの予兆監査、つまり、事が起きてから監査するのではなく、事が起きる前に、早い段階で警告を発する役割を担っているシステム監査が絶対に必要である以上、この関門を乗り越えなければならない。
このため、プロジェクトの上流工程を対象とした本社の中枢部門を対象に内部監査を行うためには、被監査部門側に「監査を受ける文化」を醸成しておかなければならないと思われる。この役目こそ、経営陣に求められる、きわめて大事な機能なのである。

第三に、システム監査に従事する内部監査人の経歴や専門知識の問題があると思われる。この上流工程の監査を本社の中枢部門に対して行うためには、システム部門に在籍して大きな開発プロジェクトのプロジェクトマネージャーの経験があることや、本社の中枢部門に在籍して、会社の戦略や方針を検討してきたといった経験が必要になるのである。最近やっと、大手の金融機関で、開発や経営企画、システム企画の経験者をシステム監査専門家にしようと試み始めた。しかしながら、システム監査に従事する内部監査の専門家の大部分は、システム部門の大規模開発の経験年数よりも、運用や保守経験が長い人が登用されるケースが比較的多い。日本の金融機関におけるシステム監査が、運用や保守を中心に実施されてきた理由はこうした背景があるのではないか。つまり、「監査すべき分野」からの発想ではなく、「監査できる分野」の発想で、監査領域が決められてきたというのが、多くの企業の実情であったと考えられるのである。

第四に、監査する側の人的問題にも関連するが、「企画構想段階やシステムのカットオーバー段階の監査手法が確立していない」、ということがあげられると思う。金融検査マニュアルには、「取締役会は、情報技術革新を踏まえ、金融機関全体の経営方針に沿った戦略目標の中に、経営戦略の一環としてシステムを捉えるシステム戦略方針を盛り込んでいるか。」という記述があり、経営戦略とシステム戦略の同期性を確認するよう求めている。しかしながら、総論ではよく理解できる課題ではあるが、実際の監査のなかで、この内容の監査をするのは至難のワザである。例えば、個別の開発プロジェクトを監査対象に取り上げたとしよう。「このプロジェクトの開発の目標は、当社の経営戦略と軌を一にしていますか？」等という単純な質問では、当然のことながら被監査部門からは立て板に水のごとく、見事な返答が返ってくるだろう。この問題についていえば、そもそも経営戦略自体が不明確かつ曖昧なため、どんなプロジェクトでも経営戦略に合致する、といえる構造になっていることが意外に多いのである。つまり、こういう場合の問題提起は、経営戦略そのものが問題、ということになるのである。また、新規業務の開発プロジェクトの監査を実施したとしよう。この場合、どういうビジネスモデルをつくり上げるのか、そのなかでどういう新技術や新製品を投入するのか、どのメーカーやベンダーと組むのが最適なのか、開発工数を減らすためにはどんな工夫を行ったのか、また、想定開発規模やマーケットの状況、あるいは競争他社の出方、等を睨みながらシステムの稼働開始日をいつにするかを決めたのか、等が大きな監査ポイントになる。このなかで、開発中のリスクと開発後・本番稼働後におけるリスクをそれぞれ洗い出し、ベストシナリオだけでなく、開発プロジェクトの大きさや複雑さによってはワーストシナリオを含む複数シナリオを用意し、それぞれに対応したリスク管理プランの検討結果を監査することも必要になる。リスク管理プランは、通常、プロジェクト組織の形態やプロジェクトマネージャーの選定、あるいは各種、各棟のレビューの頻度と内容等を決めることが大事であるが、さらに、経営レベルでのモニタリングの頻度やモニタリリング事項を確認することもきわめて大事なリスク管理計画であり、この内容の監査も重要なポイントである。また、リスク管理が破たんする場合を想定し、どのタイミングで危機管理計画を策定するのかも確認する必要がある。こういった監査のポイントは、大規模な開発プロジェクトを多数経験したり、本社部門

でこういう企画・構想を実際に練った経験がないと、なかなか出てはこない着眼点なのである。

最後に、カットオーバー段階の監査にはこの段階特有の困難さもあるため、この監査を躊躇する傾向がある。カットオーバー直前の監査を行う場合、本社部門もシステム部門も通常は大変な激務の真っ只中にある。このため、監査を受ける余裕がないのが普通であり、「どうして、こんな時期に監査をするのか」というお叱りを受けるケースが多い。しかしながら、金融庁の金融検査マニュアルでは、「システムの移行判定基準等を策定し、当該基準等に基づきシステムの移行を決定しているか。」という記述があり、経営者が移行の決定に責任を有していること、その決定の妥当性をしかるべき部署が確認することを求めている。ここでも経営者のリーダーシップが求められている。あらかじめ、重要な大規模プロジェクトは、カットオーバーをする前にシステムリスクの専門部署および内部監査部門が確認するプロセスがあることを事前に認知させる段取りが必要であろう。

今日の金融機関のシステムリスク管理の在り方を考えると、伝統的な結果監査から今日的な予兆的監査の重要性はますます高まっているのであり、実務を重ねて、システムの上流工程の監査ができる人材を醸成し、「上流工程監査を受ける文化」づくりの時期にもうすでに来ている。

以上

新たに会員になられた方々へ

新たに会員（個人、法人）になられたみなさま、当協会はみなさまを熱烈歓迎しております！
平成24年1月1日から8月31日の間に新しく会員になられた方は、36名いらっしゃいます。

【システム監査人協会に入会して】

会員番号:2093　谷口洋一

本年の4月にシステム監査人協会に入会いたしました。現在は、プライバシーマークの審査員をしております。
審査業務において情報セキュリティに関する知識は、必須のものと思い入会いたしました。
バックグラウンドとしましては、司法書士事務所、行政書士事務所で法律系の事務をして参りましたので、情報セキュリティには強い方ではなく、独学で、情報処理技術者試験の勉強をしてきた程度にとどまります。
情報セキュリティの世界は日進月歩で進化を続けておりますので、貴協会のセミナーや勉強会に積極的に参加して、最新の動向を勉強させていただきたいと考えております。
そして、今後も情報セキュリティに関する知識の研鑽に努め、プライバシーマークの審査業務に活かしていきたいと思っております。
さらには、ゆくゆくは、システム監査のスキルを身につけていきたいと思っております。
今後とも、よろしくお願いいたします。

先月に引き続き、協会の活用方法や各種活動に参加される方法などの一端をご案内します。

ご確認ください

・協会活動全般がご覧いただけます。 http://www.saaj.or.jp/annai/index.html
・会員規定にも目を通しておいてください。 http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・みなさまの情報の変更方法です。 http://www.saaj.or.jp/members/henkou.html

特典

・会員割引や各種ご案内、優遇などがあります。 http://www.saaj.or.jp/nyukai/index.html
　セミナーやイベント等の開催の都度ご案内しているものもあります。

ぜひ参加を

・みなさまの参加をお待ちしている活動です。 http://www.saaj.or.jp/shibu/index.html
　業務都合などに合わせて参加できます。門戸は低く広く見学も大歓迎です。

ご意見募集中

・みなさまからのご意見などの投稿を募集しております。
　ペンネームによる「めだか」や実名投稿があります。多くの方から投稿いただいておりますが、さらに活発な利用をお願いします。この会報の「会報編集部からのお知らせ」をご覧ください。

出版物

・協会出版物が会員割引価格で購入できます。 http://www.saaj.or.jp/shuppan/index.html
　システム監査の現場などで広く用いられています。

セミナー

・セミナー等のお知らせです。 http://www.saaj.or.jp/kenkyu/index.html
　例えば月例研究会は毎月100名以上参加の活況です。過去履歴もご覧になれます。

CSA・ASA

・公認システム監査人へのSTEP-UPを支援します。
　「公認システム監査人」 と「システム監査人補」で構成されています。
　監査実務の習得支援や継続教育メニューも豊富です。
　CSAサイトで詳細確認ができます。 http://www.saaj.or.jp/csa/index.html

会報

・PDF会報と電子版会報があります。 (http://www.saaj.or.jp/members/kaihou_dl.html)
　電子版では記事への意見、感想、コメントを投稿できます。
　会報利用方法もご案内しています。http://www.saaj.or.jp/members/kaihouinfo.pdf

お問い合わせ

・右ページをご覧ください。 http://www.saaj.or.jp/toiawase/index.html
　各サイトに連絡先がある場合はそちらでも問い合わせができます。

沼野会長1行メッセージ:　“企業経営にシステム監査がさらに活用される時代が来ると思います。”

協会からのお知らせ

■【会員増強プロジェクト（連載中）】

4月から活動を開始した本プロジェクトも半年を経過し、皆様のご協力もあり、成果が表れてきています。会報では、本プロジェクトの取組みを順次ご報告していますが、今号では、月例研究会と会報担当の取組みについて、ご報告します。

今後とも、会員増強への皆様のご理解、ご協力をよろしくお願いします。

【１．月例研究会の取り組み】

当協会の会員として、一番参加しやすい活動が、月例研究会（支部においても定例の研究会）であると考える。会場に出かけてゆくということが出来れば、特に準備をせずともシステム監査人に必要な情報などを得て、情報交換が出来るのがメリットである。そのような位置づけにある月例研究会では、新規会員の勧誘、継続的に会員になっていただくことの施策を以下のように進めている。

１．会員の参加費の引き下げ

会員の参加費の引き下げ（従来の 2000 円を今年 4 月から 1000 円とした）により参加を容易にし、会員になるメリットを増やす。これは前の主査である沼野会長の案を今年度から実施に移したものである。

会員会費の引き下げをまかなう対策として、これまでより費用の安い会場を選定している。なお、会場の変更により従来は使えたテーブルがなくなり、不便を懸けていたが、7 月からは簡易テーブルが利用できるようになり多少は改善されている。

２．月例研究会のテーマの選定の工夫

月例研究会のテーマを興味深く会員に役に立つものとするよう、従来から研究会の担当理事が年間計画を作成し、それを基に進めている。年度初めに基本の計画を立てて進める一方で、新しいテーマについても取り入れるように随時テーマの見直しをして、会員に役に立つテーマの選定に努めている。なお、今年度はメンバーも大幅に交代して異なった視点からの選定を行っている。

なお、今年度冒頭に月例研究会に対する要望の把握のため、アンケートを実施したが、テーマの選定の参考にさせていただいている。

３．月例研究会を広く案内する

システム監査関連の団体に対して、月例研究会を広く案内する。これまではＩＳＡＣＡの会員に案内をしていただいているが、システム監査学会などに働きかけをするよう進めている。これは参加者を増やすこととあわせて、会員になることのメリットを知ってもらい入会を勧めるものである。

なお、月例研究会への直接的な参加は、場所的に関東地域会員に限定されるので、以前から月例研究会の様子をビデオ撮影しＤＶＤにて配布して、支部の定例研究会にて活用していただいている。これも間接的ながら、会員の獲得、継続に役に立っているのでないかと考えている。その意味で、支部の皆さんからの意見をいただき、月例研究会活動を通じての有効な施策があれば取り入れてゆくこととしたい。

以上

（理事　木村　裕一）

【２．会計担当の取り組み】

協会の会計を預かる者として、今後協会がシステム監査の普及、会員サービスの充実等を推進していくために必要な財務基盤を確保する意味から、会員の増強＝会費収入の増強は、欠かせないものと考えています。
こうした観点に立って、会計では、会員増強プロジェクトの一環として、以下のような対応を進めています。

1．会費未収金削減に向けて

協会の会費収入について、最大の問題点と考えているのは、以下のとおり会費の未収金（会費未納）の比率が高まっているという点です。

	2009年度	2010年度	2011年度
会費収入（A）	10,024千円	9,730千円	9,279千円
未収入金（B）	1,484千円	1,950千円	2,134千円
未収金比率（B／A）	14.5%	20.0%	23.0%

会費未納は当該会員の協会離れの表れともいえます。会費未納者へのコンタクトをとって、地道に会費納付をお願いすることが、そうした会員の協会離れを防ぐことに繋がるものと考え、次のような対応を進めています。

● 従来、会費未納者に対しては、10月～年度末で連絡・督促を行ってきましたが、以下のとおり今年度はそれを早めるとともに、協会理事による電話コンタクトもお願いしています。
①7月に、6月末現在で会費の納付が確認できない会員に対し、会費納付の確認メールを発信しました。
②8月には、会費未納者に対して、会費の再請求を文書で送付しました。
③9月には、協会理事にお願いして、未納者への電話コンタクトを行い、状況を確認していく予定です。

● 10月以降についても、会費納付の促進努力を続けていきたいと思いますので、ご協力のほど、よろしくお願いします。

2．その他

会費納付の促進・利便性向上の観点から、以下についても対応を検討中です。

(1)会費請求時期の早期化
従来は、2月の総会終了後に会費の請求書を発送しておりましたが、来年度は1月には請求書を発送し、会員の皆様に、より早く連絡がいくよう対応していきたいと考えています。

(2)会費納付方法についての検討
会費は銀行振込・郵便振替での納付をお願いしてきましたが、口座振替等が利用できないか調査・検討を行っているところです。

以上
（会計担当理事）

■【ISO化推進プロジェクト（連載中）】　　2012.09 投稿

【　システム監査基準研究会　】

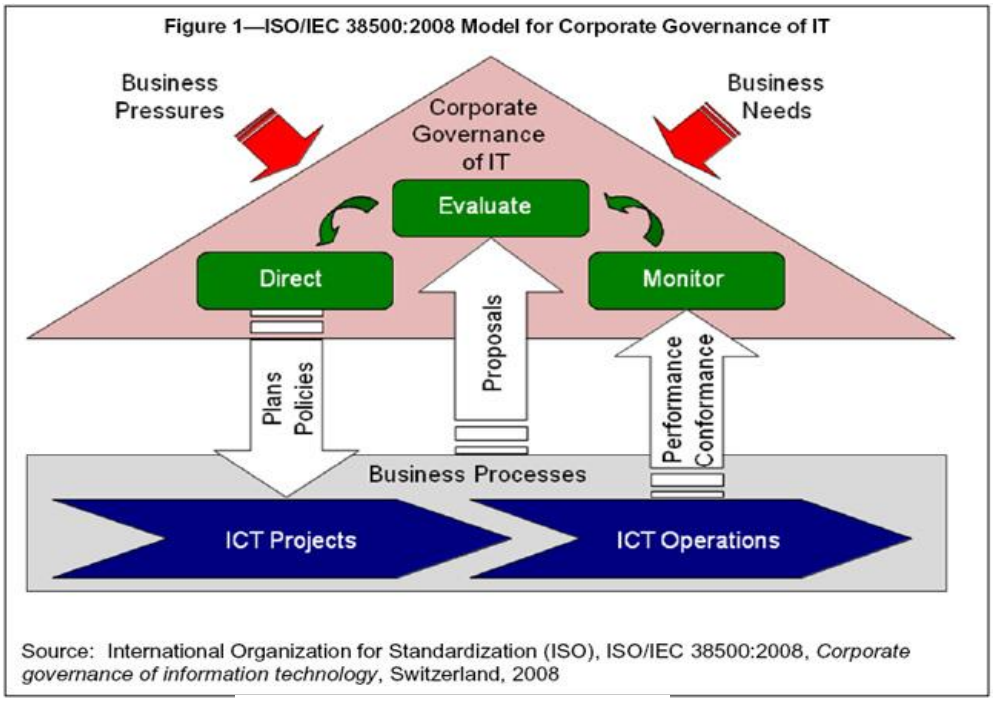
システム監査のＩＳＯ化に関する報告（第3回）

システム監査（IT Audit）に関する国際標準化の動きがあり、当協会ではシステム監査基準研究会のメンバーでこの活動をバックアップしています。この活動の取組みや進捗状況等について定期的にお知らせしています。第3回は、前回に続き「ISO/IEC　30120_WD2」(以下ガイドライン)のスコープについて報告します。

2. 本ガイドラインのスコープについての議論

IT ガバナンスの基準である ISO/IEC38500：2008 では、下図のモデルを提唱しています。上位の三角形が経営者層（GB：ガバナンスボディ）で、IT ガバナンスに関する Evaluate（評価）と Direct（指示）と Monitor（監視）を行います。GB の指示により、マネジメント層が IT の構築やITを利用した各種ビジネスプロセスを実行し、適宜実行状況等を報告することになります。

前回の報告で、本ガイドラインのタイトルを「IT Audit － IT ガバナンスの評価を支援するための監査ガイドライン」と紹介しましたが、現在議論となっているのが、IT Audit のフレームワークを考える上で、上位のITガバナンスとの関連やPrinciple の構成とその具体化、Product／Processの組み込み等についてです。さらに IT Audit の結果としてGB自体への指摘・提言があった場合の対応も議論になりました。IT Audit は GB の指示を受けて実施するビジネスプロセスが対象なので、PDCA サイクルに沿った Audit　Criteriaにすべきであるという意見です。



出典：ISO/IEC38500：2008

日本としては GB に対してGBの是正策も報告すべきであるという意向であることを主張しています。その方向性について 9 月上旬にダブリンで開催された国際会議で議論されました。本会議には、基準研メンバーである松尾理事が出席しました。本会議の内容や方向性等につきましては会報11月号にて報告致します。

本件に関するお問合せ先：（システム監査基準研究会）松枝憲司　kmatsueda@nifty.com

■【公認システム監査人・システム監査人補の募集】

協会では、公認システム監査人認定委員会より、会員の皆様へ、『公認システム監査人・システム監査人補の募集』応募をご案内しております。会員の皆様で、まだ、公認システム監査人（CSA）・システム監査人補（ASA）の資格をお持ちでない方々は、CSA・ASAの資格を取得して活動なさるよう応募をお願いします。公認システム監査人制度につきましては次の協会ホームページをご参照ください。

http://www.saaj.or.jp/csa/shosai.pdf

システム監査技術者試験と関連性のある資格の所有者、例えば、高度情報処理技術者、公認会計士、技術士、ITコーディネーター、主任審査員などの方々は、特別認定制度により、一定の教育を受けることなどを条件として同様に認定することになります。

特定非営利活動法人公認システム監査人協会
会員の皆様へ

『公認システム監査人・システム監査人補の募集』応募のご案内

公認システム監査人認定委員会

会員の皆様には、益々御隆盛のこととお喜び申し上げます。
日頃、公認システム監査人協会会員として月例会・セミナー等に御参画いただきありがとうございます。
さて、表記の件、協会では毎年春秋に『公認システム監査人・システム監査人補の募集』を行っております。協会会員の皆さまで、認定資格をお持ちでない方々に、情報提供の一環で、ご案内をさせていただいております。もし、認定資格取得のご意向をお持ちでしたら、この機会にご応募をお願い申し上げます。
認定資格を必要としない方々には、大変失礼なご案内となりますことをお詫び申し上げますとともに、今後とも、協会へのご協力をよろしくお願い申し上げます。

詳しくは、下記ホームページを御参照の上、御応募ください
「2012 年度秋期公認システム監査人及びシステム監査人補の募集について」
http://www.saaj.or.jp/csa/csaboshu.html

■【認定 NPO 法人について】

No. 557　仲　厚吉(副会長・事務局長)

協会事務局では、当協会の継続的発展を考えて、現在の一般の NPO 法人から公益法人である認定 NPO 法人にかわることのメリットとそれによって発生する責務を調査しております。認定 NPO 法人への要件相談のため、8 月 28 日 11 時から 1 時間、飯田橋にある東京ボランティア・市民活動センターを訪問しました。その結果、明らかになった認定 NPO 法人への要件と対応策を報告します。

要件と対応策:

1. パブリック・サポート・テスト(PST)をクリアしていること

役員やその家族など以外の寄附者から 3,000 円以上の寄附金を年平均 100 人以上集めることで対応します。2012 年度はクリアしており、2013 年度以降も寄附をお願いしていきます。2014 年度に認定申請の予定です。

2. 活動のメインが共益的な活動でないこと

会員のみの共益的活動とともに、誰でも当協会のサービスを受けられる活動、例えば、月例研究会参加、CSA・ASA 資格認定、ISO 化支援等での一般への公益的活動をアピールします。会報は電子版になって会員のみの記事は限定した運用になっています。協会ホームページの見直しと会計上の取組みを検討します。

3. 組織運営等が適正であること

組織運営等は、年2回、監事の監査を受けており、総会後、法務局登記、都庁へ事業報告を行っています。2012 年 4 月 1 日から改正 NPO 法が施行されたため会計計算書類、登記事項で対応が必要になっています。また、認定 NPO 法人として追加になる組織運営等について調査して対応します。

4. 事業活動について一定の要件を満たしていること

定款に則って事業活動を行っていきます。認定のための一定の要件を満たした事業活動になるように、認定 NPO 法人に追加になる要件、例えば寄附金は 70%以上を NPO 事業費に充当などについて調査して対応します。

5. 情報公開が適正であること

認定申請資料について、一般の人から閲覧の請求があった場合、応じることができるように準備します。

6. 法令違反等がないこと

協会活動において法令違反等は発生しておりません。法人税の収益事業として申告する事業活動はなく、都税は免除、源泉税、消費税は法令に則って納付しています。

7. 設立から 1 年を超えていること

当協会は、2002 年度に NPO 法人として東京都の認証を受け、2012 年度に至っています。

以上

■【SAAJ 会員システム（その 2）】

【　事務局　】

★SAAJ会員システム　https://www.saaj.or.jp/members_site/KaiinStart

「SAAJ会員システム」Topics

① 2012年8月より、会員システムのマニュアルが表示されるようになりました。
　パスワードの再発行の手順、個人情報変更の手順などを掲載しています。

② 会費をお支払いただきますと、約1週間で、「会費納入日」に反映されるようになりました。
　※10日以上経過しても反映されない場合は、jimu@saaj.jp　宛にご連絡ください。

前回からの続き：　4. 個人情報変更

左側メニューから「個人情報変更」を選択します。

★マニュアル：16ページ　5【会員情報を変更する場合】

注意：

① 変更は、上書きで行ってください。
会員は、白抜き枠内のみ変更できます。
グレー枠の内容は、訂正できません。

② 最後に「確認画面」ボタン　→「実行」を押してください。

※ 編集画面のレイアウトは、
機能追加により変更することがあります。

会員情報変更画面　（上段）

確認画面へ

会員番号	9910	
会費納入日	2012年2月10日	
CSA/ASA認定日	2012年2月27日	
入会年月日	2001年10月1日	
CSA/ASA認定番号	K09999	
有効期限	2014年12月31日	
氏名	漢字	(姓)テスト　(名)第ナコ
	カナ	全角カタカナで入力してください。 (姓)テスト　(名)ハナコ

【ポイント！】連絡・請求先：　○勤務先　●自宅

【お願い】原則として、連絡先は **ご自宅** を選択してください。
勤務先を選択した場合でも、できれば **ご自宅** の欄にも入力してください。

【会員メーリングリストとの関連】

連絡・請求先に入力したメールアドレスが、**会員メーリングリスト**に登録されます。
月例会やセミナーのご連絡、協会からのご連絡が正しく届くために、
メールアドレスを変更された場合は、必ず訂正をお願い致します。
※パスワードを忘れたときにも、仮パスワードが登録メールアドレス宛に送信されます。

生年月日		1960 年 2 月 24 日 生まれ
所属支部		○北海道 ○東北 ○北信越 ○中部 ●関東 ○近畿 ○中四国 ○九州
紹介会員		会員番号　氏名
連絡・請求先		○勤務先 ●自宅
勤務先	住所	〒 103 － 0025 【住所検索】 住所1　東京都中央区日本橋茅場町2－8－8 住所2(建物名以降)　共同ビル(市場通り)6F
	名称	NPO法人 日本システム監査人協会
	所属	事務局
	役職	
	TEL(勤務先)	03 － 3666 － 6341
	TEL(携帯)	－ －
	FAX	03 － 3666 － 6342
	E-mail	携帯電話以外のメールアドレスを登録してください。 jimu@saaj.jp
自宅	住所	〒 170 － 0012 【住所検索】 住所1　東京都豊島区上池袋●丁目●番地 住所2(建物名以降)
	TEL(自宅)	03 － 3xxx － xxxx
	TEL(携帯)	090 － 88xx － 8x8x
	FAX	03 － 3xxx － xxxx
	E-mail	携帯電話以外のメールアドレスを登録してください。 saajjk7@saaj.jp

★ＣＳＡ・ＡＳＡの「公開名簿」の内容変更方法は、次回会報で！！

CSA公開名簿：　http://www.saaj.or.jp/members_site/CSAPublicList
ASA公開名簿：　http://www.saaj.or.jp/members_site/ASAPublicList

理事　斎藤由紀子

■【会長コラム】

夏休みの自由研究

会長　沼野伸生

会長コラムは、4月から毎月、システム監査や協会運営に関するテーマを取り上げ、私が日頃思っていることを率直に書き綴ってきました。

そこで、今月は少し趣を変えて、“夏休みの自由研究”と題し、私が今年の夏休みの時間潰し？に行った簡単なシステム監査に関する調査について紹介したいと思います。

この調査の目的は、経営にシステム監査がどの程度活用されているかの一面を、企業が金融商品取引法に基づき毎年提出する有価証券報告書へのシステム監査関連の記述状況でザックリ見てみようというものです。

具体的には、金融庁のEDINETシステム（金融商品取引法に基づく有価証券報告書等の開示書類に関する電子開示システム）を利用し、1年間に金融商品取引法に基づき企業から提出された有価証券報告書を全文検索し、“システム監査”、“IT監査”、“IT統制監査”などの記述が何社位あるかを見るものです。

調査結果の概要は以下の通りでした。

○調査日：平成24年8月15日
○調査対象期間：平成23年8月1日～平成24年7月31日（1年間）
○有価証券報告書提出会社数：4,419社
○会計監査人の補助者としてシステム監査担当がいることの記述がある有価証券報告書：
　187社（提出会社の約4.2%）
○上記以外で、システム監査に関し何らかの記述がある有価証券報告書：45社（提出会社の約1.0%）

有価証券報告書は企業の開示情報（書類）の代表的なものですが、その中で何らかの形でシステム監査に触れている企業は約5%（20社に1社程度）である。そしてその内容は、会計監査人の補助者としてシステム監査担当がいることの記述が殆どで、それ以外でシステム監査に関し何らかの記述（システム監査の導入・活用など）がある有価証券報告書は約1%（100社に1社）程度でした。

この割合が、企業経営にシステム監査がどの程度活用されているかをそのまま表しているとは思いませんが、システム監査に関する情報が、企業の情報開示に欠かせない項目の一つになるのには、情報社会といわれる今日ですが、もう少し時間が必要なようです。

このような結果でしたが、その中には、当協会が認定している公認システム監査人（CSA）や、ISACAの公認情報システム監査人が役割を果たしていることを積極的に開示している企業も見られ、最後にほんのちょっと元気も貰った、夏休みの自由研究でした。

以上

研究会、セミナー開催報告、支部報告

■【西日本支部合同研究会の結果報告】

【全体報告】　　№350 鶴岡 通

日本システム監査人協会（ＳＡＡＪ）では、第 10 回西日本支部合同研究会を、以下の通り開催致しましたので、ご報告致します。

月末の 6 月 30 日（土）にもかかわらず総勢 55 名の方に参加頂き、盛会の内に開催・閉会することができました、ご後援頂き団体のみなさま、ご来賓・ご講演のみなさま、及び、ご参加頂いたすべてのみなさまに感謝致します。

西日本支部合同研究会 in FUKUOKA

【日　時】　平成 24 年 6 月 30 日(土)13:00～17:00

【場　所】　福岡県 Ruby・コンテンツ産業振興センター　セミナールーム
（福岡市博多駅東 1 丁目 17-1）

【テーマ】　「災害に備えたシステム監査」
人災・天災と様々な災害が情報システム（ICT）に影響を与え、その波及範囲の規模・責任が日々拡大しております。それに備えて現在あるべきシステム監査を問う。

【主　催】　日本システム監査人協会
北信越支部、中部支部、近畿支部、中四国支部、九州支部

【後　援】　九州経済産業局、システム監査学会、　ISACA 福岡支部
特定非営利活動法人　ＩＴコーディネーター協会、福岡ＩＴコーディネーター推進協議会
日本ＩＴストラテジスト協会

【次　第】

司　会　　日本システム監査人協会　九州支部長　中溝 統明氏

13:00-13:05　開催挨拶　日本システム監査人協会　九州支部長　中溝　統明氏

13:05-13:15　会長挨拶　日本システム監査人協会　副会長　小野　修一氏

13:15-13:55　講演 1　「事業継続計画とシステム監査」

日本システム監査人協会　北信越支部　梶川　明美氏

13:55-14:35　講演 2　「BCP の観点を意識したシステム監査項目の検討」

日本システム監査人協会　中部支部　副支部長　澤田　裕也氏

14:35-15:15　講演 3　「東日本大震災を踏まえた事業継続面の課題」

日本システム監査人協会　中四国支部　理事　大石　正人氏

13:30-16:10　講演 4　「コンシューマライゼーションとその影響」

日本システム監査人協会　近畿支部　支部サイトＷｅｂ主査

永田　淳次氏

16:10-16:50　講演 5　「インフラ系制御システムとシステム監査」

日本システム監査人協会　九州支部　福田　啓二氏

16:50-17:00　閉会挨拶　日本システム監査人協会　九州支部　副支部長　舩津　宏氏

【懇親会】

17:45-20:00　　和食の店　福太郎（博多駅筑紫口店）にて

【観　光】（費用実費）

7 月 1 日（日）　・博多祇園祭　9:30～12:00　福岡市内　飾り山笠巡り

１．参加者概要と開催背景

参加人数は、発表者 6 名を含めて総勢 55 名で、日本システム監査人協会 31 名（九州支部 13 名、中四国支部 5 名、近畿支部 4 名、中部支部 4 名、北信越支部 2 名、他支部 3 名)、後援団体 13 名（ＩＳＡＣＡ福岡支部 4 名、システム監査学会 3 名、ＩＴコーディネーター6 名)、一般 11 名と盛況であった。

西日本支部合同研究会は、九州支部では 2007 年 5 月に福岡市で開催してから、2 回目の幹事として開催となりました。

今回は、2011 年 3 月 11 日に発生した東日本大震災を受けて、少し考える時期を置いて、テーマを「災害に備えたシステム監査」として、5 月に開催案内を作成して募集を開始し致しました。

２．開会挨拶

日本システム監査人協会　九州支部　支部長　中溝　統明氏

参加者や発表者へのお礼と、配布資料の確認を兼ねてあいさつで、西日本支部合同研究会は、５支部（北信越、中部、近畿、中四国、九州）が参加して開催されるものです。

今回のテーマは「災害に備えたシステム監査」として、最近発生している、色々な事件（クラウド利用における脅威、ツイッターの被害、サイバー攻撃、）や予測不能な災害が発生しているなか、各支部よりプロフェッショナルな方に発表をして頂きます。

参加者の皆様に有益な情報提供の場に成りましたらと思います。

３．会長挨拶

会長挨拶　日本システム監査人協会　副会長　小野　修一氏

東京本部より、ご多忙のなか、小野修一副会長に遠路ご出席頂きました。

ご挨拶では、「会員増強プロジェクト活動報告」として、即実施するもの、速やかに実施するもの、中長期的に検討し順次実施するものと３つに分類し、そのなかで、即実施すべきものについて、詳細にご説明された後に、支部の皆さんからのご意見、ご協力をお願いしますとした。

【各講演１～６は、省略致します。】

４．閉会挨拶

日本システム監査人協会　九州支部　副支部長　舩津　宏氏

システム監査学会理事　九州支部長でもあり、システム監査学会では、年２回の研究大会等が開催されています。

今回の西日本合同支部研究会のように、各支部間での情報交換を持ちまわりで実施できていることは、すばらしいことで、有意義な機会ではなかったでしょうか。

今後とも、西日本支部合同研究が継続されますように願っております。

５．懇親会

食の店　福太郎（博多駅筑紫口店）にて、26 名の参加

場所は、初回と同じ場所、同じ会場で行われ、進行は、前支部長の福田啓二氏の音頭で始まりました。

ＩＳＡＣＡ福岡支部の会長（この度、４月に発足）諸藤雅之氏による乾杯で開宴された。恒例の自己紹介では、参加者の思いや気持ちが伝わり、全員の紹介が終わるころには、終宴時間となりました。

最後に、博多手一本の予行練習をした後に締められた。

「よー、チャ・チャ、まひとつ、チャ・チャ、**いおうて**、チャ・チャンがチャ」

６．観　光

観光は、博多の売りである「山が有るから博多たい」と言われるように、山笠の開催に合わせて、今回は合同支部研究会を設定致しました。飾り山（静）では有りますが、追い山（動）への感情の高まりの雰囲気を味わっていただけたら幸いです。

【所　感】

今回の開催は、殆どを中溝支部長にお任せするような形で開催されました。企画、会場手配、案内文作成、後援団体へのご依頼、資料準備、司会進行から、取りまとめと後援団体への報告までお願いすることになり、ご苦労に感謝致します。

今回の主な作業分担を下記に示す。

[受　付]　荒添美穂、溝田明美
[会　計]　居倉圭司、中溝統明
[機材手配]　福田啓二、居倉圭司
[設　営]　諸藤雅之、小野哲夫、前田弘幸
[写　真]　堤薫（中部支部）、居倉圭司
[タイムキパー]　諸藤雅之
[記　録]　溝田明美、居倉圭司、荒添美穂、
　　舩津宏、小野哲夫、鶴岡通
[司　会]　中溝統明
[事務局]　中溝統明
[懇親会]　福田啓二、諸藤雅之

他、合同研究会の進行に関係されました方に、感謝すると同時に、今後この会が益々盛んになり、会員相互の意見交換の場、レベルアップの場として、日本システム監査人協会の会員増強の一助になりましたら幸いです。

次回は、北信越支部の幹事で金沢市を予定しているとのこと、ご案内を楽しみにしております。

参加されたみなさん、ありがとうございました。

■【第１７３回月例研究会受講報告】

会員番号 1795 藤澤 博

講演テーマ及び講師 :

1.「改正不正アクセス禁止法について」:

警察庁生活安全局情報技術犯罪対策課係長　吉田　裕紀　氏

2.「標的型攻撃メールの特徴と対策」

情報処理推進機構IPA技術本部　セキュリティセンター調査役　木邑　実　氏

日時 : 2012年7月20日(金)18:30～20:30

場所 : 機械振興会館　地下2階　ホール

講演概要:

【講演－１：改正不正アクセス禁止法について】

平成 24 年 3 月 31 日(法律第 12 号)に「不正アクセス禁止法」が改正されたが、この改正の内容について、配布資料「改正不正アクセス禁止法について」が使用され、説明が行われた。主な項目は次のとおりである。

1. 改正前の不正アクセス禁止法の概要

2. 社会情勢

①インターネットの普及状況

②サイバー犯罪情勢の深刻化

③フィッシング行為の急増

3. 不正アクセス禁止法の改正について

①取締面の対策:不正アクセス防止対策の強化

②禁止・処罰するフィッシング行為の類型

③防御面の対策:情報セキュリティ関連事業者団体に対する情報提供

1. 改正前の不正アクセス禁止法の概要

サイバー犯罪の防止・電気通信に関する秩序の維持を目的として、以下の対策が定められている。

①取締面の対策:

1)不正アクセス行為の禁止・処罰(3 条・4 条)

・プログラムの脆弱性を狙って、目的端末を利用可能にしてしまう行為。

2)他人のID・パスワードの無断提供の禁止・処罰(4 条・9 条)

・他人の ID・パスワードを奪取・盗用して、その者になりすましてアクセス認証を越える行為。

・なりすまし以外の攻撃手法を用いて認証サーバーをだまし、それに従属する目標の端末を利用可能にする行為。

②防御面の対策:

1)アクセス管理者による防御措置(5 条)

・不正アクセスに遭わないように、常に適切な管理措置を講じる努力義務がある。

2)都道府県公安委員会による援助(6 条)

・被害発生時の応急対策

3)国家公安委員会・総務大臣・経済産業省大臣による情報提供等(7 条)

・不正アクセス行為の発生状況の公表　　・セキュリティ技術の研究開発状況の公表

・広報啓発

2. 社会情勢

インターネットの普及とともにサイバー犯罪、フィッシング行為が増加している。

①インターネットの普及状況

【H11 年度末】:インターネットの利用者数:2,706 万人、人口普及率(利用率):21.4%

【H22 年度末】:インターネットの利用者数:9,462 万人、人口普及率(利用率):78.2%

②サイバー犯罪情勢の深刻化

サイバー攻撃による ID・パスワードの不正取得。**現行法では不処罰。**

【H13 年】:不正アクセス検挙件数:　66 件、不正アクセス人員:　51 人

【H22 年】:不正アクセス検挙件数:1,598 件、不正アクセス人員:123 人

③フィッシング行為の急増

企業になりすまして偽メールを送信し、ID・パスワードを入力させてだまし取るフィッシングが増加。

現行法では不処罰。

【H17 年】:フィッシングサイト件数:　291 件

【H21 年】:フィッシングサイト件数:1,786 件

3. 不正アクセス禁止法の改正について

サイバー攻撃及びフィッシング行為の急増に伴い不正アクセス禁止法が以下のように改正された。

①取締面の対策:

ネットバンキングの不正送金、クレジットカード詐欺、営業秘密の取得等の不正行為及び不正取得が可罰化され、法定刑が、1 年から 3 年に引き上げられた。

1)フィッシング行為の禁止・処罰(3 条・11 条)

2)ID・パスワードの不正取得の禁止・処罰(7 条・11 条)

3)不正アクセス行為に係わる法定刑の引上げ(11 条・12 条)

②防御面の対策:

情報セキュリティ関連事業者団体(*)に対し、国による以下に示す新たな援助策が追加された。

・不正アクセス行為の手口に関する個別具体的な情報の提供

・不正アクセス行為の実態を踏まえた助言

1)情報セキュリティ関連事業者団体に対する情報提供(10 条)

＊情報セキュリティ関連事業者団体(2 社):ISOG－J、フィッシング対策協議会

＜主な質疑応答＞ 「防御面の対策」画面について

1. 情報セキュリティ関連事業者団体について　(「防御面の対策」画面について)

Q:2 団体が例示されているが、他にもあるか。

A:現在この 2 団体である。今後増えてゆく可能性がある。

Q:このような団体になるための条件とか、HPから申請できるのかなどの方法は？

A:法律上で規定があるわけではない。団体が自分のところはこのような活動をしていることを申し出てもらうことになる。(Q:その場合吉田さんに連絡することでよいか。A:良いです)

2. アクセス管理者の役割と活動　　(「防御面の対策」画面について)

Q:クラウドシステムの場合には、アクセス管理者とはユーザの登録や管理をする者と考えて、この場合にもアクセス管理者向の情報提供があるか。

A:完全に始まっているわけでないので、クラウドのケースは事例がまだ無い。

Q:情報は例示や技術的推奨などの内容が表示されるか？

A:法律上"ここまで行え"というのではない。一般的に努力してください、守ってくださいという方向性を示すものになる。

3. 海外からの不正アクセスなどへの対処

Q:海外からの不正アクセスに対する対応は出来るのか。

A:(不正アクセス事例ではないが)インターネット上のわいせつ画像がタイのサーバー上にある場合について、タイと協力して犯人を捕まえた。日本のコンピュータに対しての犯罪には日本に捜査権限があるが、実際にはそれが海外で行われた場合には犯人のいる国の警察と協力して解決することになる(サイバー犯罪条約を日本も受託した)。

以上

【講演－2:標的型攻撃メールの特徴と対策】

最近発生したサイバー攻撃の内容と新しいタイプの攻撃の分析と対策について、配布資料「標的型攻撃メールの特徴と対策」が使用され、説明が行われた。主な項目は次のとおりである。

1. 某重工業企業の事件と脅威の動向
2. 標的型攻撃メール
3. 新しいタイプの攻撃
4. 対策の全体像とIPAの取組
5. J－CSIPの紹介(＊)

＊:当日は時間が足りなくて紹介いただけなかったJ－CSIPについて、資料を提供戴きましたので、掲載します。

1. 某重工業企業の事件と脅威の動向(報道ベース)

①事件の経緯

・某重工業企業が所属する業界団体の職員の PC がウイルスに感染し、関係企業とやり取りしていたメール情報が盗まれた。

・盗まれたメールを使用し、関係企業に対して、標的型攻撃メールを送付された。その関係企業の中に某重工業企業等が含まれていた。

②某重工業企業の被害

・標的型攻撃メールを受信後、ウイルスは広域に社内拡散した。11 事業所、83 台の PC やサーバー。

・端末に感染したウイルスにより内部サーバーへ侵入され、一部の情報を抜き取られた可能性がある。
抜き取られた情報を攻撃者のサーバ(米国サーバ)へ送付された模様。

・機密情報の流失は確認されていない。

③今回の事件の教訓と対策

・標的型攻撃は、攻撃目標に関係する組織も狙っている。

・組織関係や業界団体活動に大きな支障を生じる可能性が大。

・セキュリティがあまいと、関係する組織にも大きな脅威となる。

・対策としては、各組織が社会的責任として十分なセキュリティ対策を取り、業界が一丸となってセキュリティレベルの向上を図る。

④脅威の動向

・上記のような事件は、世界中で発生している。

・これらの不正侵入は、金銭的な対価でなく、企業や政府の機密情報や知的財産そのものを入手することを目的に実行されている。

2. 標的型攻撃メール

①標的型攻撃メールの定義

情報窃取を目的として特定の組織に送られるウイルスメール

②標的型攻撃メールの特徴

・送信者名として、実在する信頼できそうな組織名や個人名を詐称する。

・受信者の業務に関係の深い話題や詐称した送信者が扱っていそうな話題

・ウイルス対策ソフトを使っていてもウイルスが検知されない場合が多い。

・メールが海外からの IP アドレスから発信される場合が多い。

・感染しても、PC が重くなるとか、変なメッセージが表示されない。

・外部の指令サーバーと通信している。

・長期間にわたって標的となる組織に送り続けられる。（内容は、毎回異なる。）

③ウイルスメールの形態の変化

マスメール型ウイルスメール　⇒　標的型攻撃メール　へ変化

	マスメール型	標的型攻撃
ターゲット	セキュリティ対策が不十分な PC	特定の組織の情報
宛先	不特定多数	少数の組織
送信者	知らない人	信頼できそうな組織や人物
ウイルス対策ソフト	大半は検知	ほとんど検知不可
話題	誰にでも関係のある話題	受信者に関係の深い話題
記述言語	ほとんど英語	日本語など受信者が通常使う言語
添付ファイル	実行形式（exe）	Pdf や doc などの文書ファイル
感染拡大	感染した自身の PC から再発信	再発信せず
感染後の症状	何らかの異常な症状	特に気付くような症状なし

3. 新しいタイプの攻撃（IPA）

①「新しいタイプの攻撃」の定義

ソフトウェアの脆弱性を悪用し、複数の既存攻撃を組み合わせ、ソーシャル・エンジニアリングにより特定企業や個

人を狙った攻撃の総称。

②「新しいタイプの攻撃」の事例

・Google、Yahoo!　を狙った攻撃

・イランの原子力施設を狙った攻撃

・日本を含めた重工業企業への攻撃

・米国セキュリティ関連企業を狙った攻撃

これらの攻撃は、海外では

「APT（advanced persistent threat：高度かつ継続的な脅威）」とも呼ばれる攻撃手法である。

③「新しいタイプの攻撃」の分析

【事前調査】：ターゲットとなる組織を攻撃するための情報を収集する。

【初期潜入段階】：標的型メールや USB メモリ、Web サイト閲覧を通してウイルスに感染する。

【攻撃基盤構築段階】：侵入した PC 内でバックドアを作成し、外部の C&C サーバーと通信を行い、新たなウイルスをダウンロードする。

【システム調査段階】：　情報の存在箇所特定や情報の取得を行う。

【攻撃最終目的の遂行段階】：　攻撃専用のウイルスをダウンロードして、攻撃を遂行する。

④「新しいタイプの攻撃」対策の考え方

組織の守るべき資産の明確化、リスクの評価に基づいて、一つの対策でなく、多層の防御が重要。

・脅威は極力上流で食い止める。

・侵入阻止できなかった場合の攻撃活動の抑止。

・最後の砦となる守るべき情報の保護の強化

・システム全体の監視と証跡の分析

・組織全体のセキュリティマネジメントやコンテンジェンシープランの整備。

4. 対策の全体像とIPAの取組

①対策の全体像

情報セキュリティ対策に抜けはないかを見直すチェックリストとして活用してください。

【入口対策】

・システムへの入口と経路での防御：ファイアウォール、侵入検知システム／防止システム等

・脆弱性対策：定期的な脆弱性診断、ウェブアプリケーションファイアウォール（WAF）等

・標的型攻撃ルートでの対策：スパムフィルター、URL フィルター等

【出口対策、情報保護】

・ウイルス活動の阻害及び抑止：端末間、他部署間のネットワーク通信の制限等

・アクセス制御：ユーザ認証等

・情報の暗号化：通信路の暗号化、ファイルの暗号化、暗号鍵管理等

【監視、管理統制】：

・システム監視、ログ分析：ネットワークログ取得・分析、サーバログ取得・分析等

・管理統制及びコンテンジェンシープラン（事前準備・事後対応）：危機対応体制の整備等

②IPAの取組

・サイバーセキュリティ注意喚起サービス「icat」

「icat」をイントラネットのポータルサイトに表示することにより、IPAが発信している緊急に実施すべきセキュリティ対策情報を従業員に直接周知することができる。

・MyJVN バージョンチェッカ機能

攻撃に利用されやすいソフトウェアのバージョンが最新か簡単にチェックできる。毎週各々がチェックするのが良い。監査の項目としても薦めたい。

・JVNiPedia 脆弱性対策 DB(15,000 件突破)

国内外の主要なソフトウェアの脆弱性情報を日本語で掲載しており、企業のシステム管理者に活用してもらいたい。

・IPAテクニカルウォッチ　レポート「標的型攻撃メールの分析」

IPA に届けられた 70 件余りの標的型攻撃メールを分析した。

・サイバー情報共有パートナーシップ（J-CSIP）

標的型攻撃に関する情報を共有することで、被害の防止や極小化を図る取組。重工関連 9 社でスタートし、現在、電力、ガス、化学、石油業界に拡大中。

・「新しいタイプの攻撃」の対策に向けた設計・運用ガイド

・「標的型サイバー攻撃の特別相談窓口」の設置

5. J－CSIPのご紹介

①J-CSIP メンバー企業実施項目

・組織内への注意喚起・初動対策　⇒　メール開封を回避

・メールサーバのアーカイブの検証　⇒　攻撃痕跡検証

・防御対策　⇒　メールフィルタのチューニング

・検証結果のフィードバック　⇒　再度の情報共有

②IPA の貢献

・J-CSIP メンバー許可の下に、重要組織に対する最新の攻撃情報の知見の共有、およびマルウェア検体の提供を行う。

・迅速な解析、より広く深い解析による、情報共有内容および対策対応の高度化を図る。

・今後想定される攻撃に対する事前対応、システム対策など組織的セキュリティ力の向上を図る。

＜感想＞

今回の公演テーマ「改正不正アクセス禁止法について」及び「標的型攻撃メールの特徴と対策」は、インターネットの利用者が急激に増加する中、それに伴ってサイバー犯罪が増加し、その手口も一層複雑・巧妙化し、政府関係組織、国の機密情報を扱う企業等へ不正侵入する「新しいタイプの攻撃」が報告されている。その「新しいタイプの攻撃」がどのようなものか、また、それに対し、どのような対策を打てばいいのか、警察庁の不正アクセスの取締り、そして、IPA における対策が非常に興味ある内容でした。

マスメール型ウイルスメールから標的型攻撃メールへ変化している「新しいタイプの攻撃」に対し、さまざまな活動を行っておられる現状を解り易く、説明して戴いたことに感謝し、感想とさせて戴きます。

以上

【第 173 回月例研究会受講報告 終わり】

参考 【標的型サイバー攻撃に関わる IPA の取組】

資料提供:情報処理推進機構IPA技術本部　セキュリティセンター調査役　木邑　実　氏

1. **サイバーセキュリティ注意喚起サービス「icat」**

http://www.ipa.go.jp/security/vuln/images/icat_brochure_01.pdf

・標的型攻撃メールでは、PDF ファイルや MS WORD ファイル、EXCEL ファイルのようなデータファイルにウイルスを仕込み、そのデータファイルを表示するのに利用される、Adobe Reader、FlashPlayer、MS Office、JRE などのソフトウェアの脆弱性を悪用してウイルスに感染させる事例が多くなっています。

・IPAは、利用者の多いソフトウェアの脆弱性を悪用した攻撃が実際に発生している場合に、その脆弱性の修正を促すなどの緊急対策情報や注意喚起を発信しています。

・右に示すような情報画面をイントラネットのポータルサイトに表示することにより、IPAが発信している緊急に実施すべきセキュリティ対策情報を従業員に直接周知することができるサービスです。

2. **MyJVN バージョンチェッカ**

http://jvndb.jvn.jp/apis/myjvn/#VCCHECK

・攻撃に悪用されやすいソフトウェアのバージョンが最新か簡単にチェックできるサービスです。

パソコンを利用している従業員が毎週チェックすることをお勧めします。

3.　JVNiPedia 脆弱性対策 DB(15,000 件突破)

http://jvndb.jvn.jp/

国内外の主要なソフトウェアの脆弱性対策情報を日本語で提供するサービスです。

企業のシステム管理部門が、組織内で利用されているソフトウェアの脆弱性対策情報を把握し、適切な対策を実施することで、不正アクセスの被害を予防することに役立ちます。

4．ＩＰＡテクニカルウォッチ　「標的型攻撃メールの分析に関するレポート」

http://www.ipa.go.jp/about/technicalwatch/pdf/111003report.pdf

・IPA に届けられた 70 件余りの標的型攻撃メールを分析しました。
・メール受信者をだますテクニックや対策をまとめてあります。

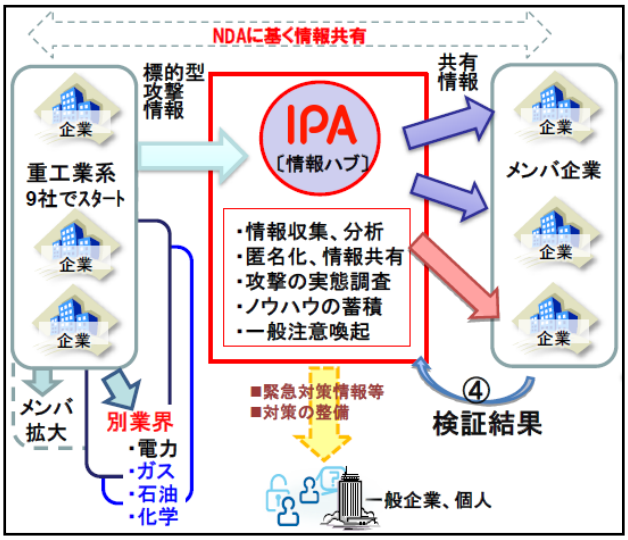
5．サイバー情報共有イニシアチブ（J-CSIP）

http://www.ipa.go.jp/security/J-CSIP/index.html

標的型攻撃に関する情報を NDA(秘密保持契約)に基づき共有することで、メンバー企業の被害の防止や極小化を図る取組みです。

IPA が情報ハブとなり、攻撃を受けた企業の情報を匿名化して、メンバー企業に提供します。

メンバー企業は共有情報を元に、同様の攻撃が来ていないか調査したり、出口対策を行います。



重工関連 9 社でスタートし、現在、電力、ガス、化学、石油業界に拡大中です。

６．「新しいタイプの攻撃」の対策に向けた設計・運用ガイド

http://www.ipa.go.jp/security/vuln/newattack.html

・「新しいタイプの攻撃」は非常に巧妙であり、従来のファイアウォールやウイルス対策ソフトなどによる入口対策だけでは、被害を防ぎきれません。

・ウイルスがシステムに侵入することを前提に、ウイルスから攻撃者に送信する情報が外部に出ないようにする出口対策や、情報を暗号化するなどの総合的な対策を設計するのに必要なノウハウが記載されています。

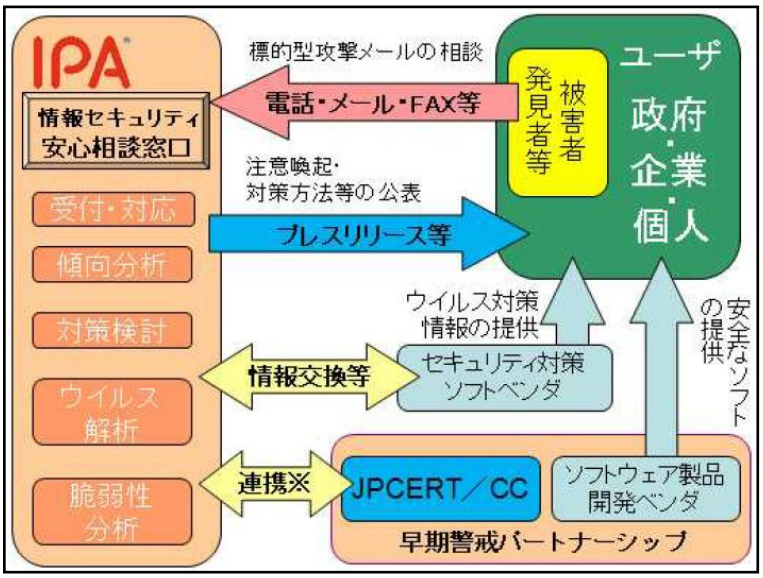
７．「標的型サイバー攻撃の特別相談窓口」の設置

http://www.ipa.go.jp/about/press/20111025.html

標的型攻撃メールは、メール受信者をだます巧妙なテクニックが駆使されていたり、ウイルス対策ソフトで検知されない添付ファイルがついているなどの理由で、ウイルスと気付かずに添付ファイルを開いたり、リンクをクリックしてしまい、被害に遭う可能性が高い。

標的型攻撃メールの可能性がある不審メールを受信した企業等の相談に応じるとともに、受信したメールを簡易解析し、対策情報を提供します。

国内の主要なセキュリティ対策ベンダにウイルス検体を提供し、ウイルスパターンファイルに反映してもらいます。



注目情報（2012/9）

■【〈IPA〉スマートフォンの中の個人情報が狙われています】（2012/9/5 発表）

2012 年 8 月は、スマートフォン（Android OS）の電話帳の中身を窃取する不正なアプリケーション（以下、アプリ）の情報が多く見受けられました。これは悪意を持った攻撃者が、不正なアプリをダウンロードさせるリンク先が書かれたメールを、不特定多数の利用者にばら撒いていたためです。

この不正なアプリは、ウイルスそのものですが、発見当初、セキュリティ対策ソフトを導入していても検知されないことがあり、インストール後に起動してしまうと情報窃取の被害に遭ってしまうものでした。なお、アプリの名前や送られてきたメールの文章は全て日本語であるため、日本人を狙った攻撃だと考えられます。

IPA では、この不正なアプリを入手し解析を行いました。ここでは、攻撃者が不正なアプリを利用者のスマートフォンへインストールさせるまでの手口と、解析結果をもとに不正なアプリの動作の一例を解説し、被害に遭わないための対策を紹介します。

図 1-1：不正なアプリが情報を流出させるイメージ図

http://www.ipa.go.jp/security/txt/2012/09outline.html

■【〈IPA〉ウイルス届出状況　】（2012/9/5 発表）

1. ウイルス届出状況　2012.9.5

8 月のウイルスの検出数※1 は、24,189 個と、7 月の 25,487 個から 5.1%の減少となりました。また、8 月の届出件数※2 は、961 件となり、7 月の 877 件から 9.6%の増加となりました。

検出数の 1 位は、W32/Mydoom で 15,441 個、2 位は W32/Netsky で 5,888 個、3 位は W32/Mytob で 966 個でした。

2. コンピュータ不正アクセス届出状況（相談を含む）

(1) 不正アクセス届出状況

8 月の届出件数は 9 件であり、それら全てが被害のあったものでした。

(2) 不正アクセス等の相談受付状況

不正アクセスに関連した相談件数は 44 件であり、そのうち何らかの被害のあった件数は 13 件でした。

不正アクセスの届出および相談状況

	3月	4月	5月	6月	7月	8月
届出[a] 計	5	9	10	2	19	9
被害あり[b]	4	7	6	2	18	9
被害なし[c]	1	2	4	0	1	0
相談[d] 計	54	46	50	38	54	44
被害あり[e]	10	9	17	12	26	13
被害なし[f]	44	37	33	26	28	31
合計[a+d]	59	55	60	40	73	53
被害あり[b+e]	14	16	23	14	44	22
被害なし[c+f]	45	39	37	26	29	31

■【最近の個人情報漏えい事故　（ニュースガイア株式会社）】(2012/8/20～2012.9.7 発生分)

2012/09/07 「見つかるサイト.jp」で不正アクセス発生、顧客情報流出の可能性
2012/09/06 Apple 端末のユーザ情報 1200 万件が流出の可能性 － 活動家が一部公開
2012/09/06 個人情報含む PC などが車上荒らし被害に － 富士古河 E&C
2012/09/05 DNA バンク登録患者の情報含む USB メモリを院外で紛失 － 順天堂大付属病院
2012/09/04 8 支店で顧客情報含むマイクロフィルムを紛失 － 岡崎信金
2012/09/03 ファイル共有ソフト経由の個人情報流出、あらたに 279 件の被害が判明 － 秋田市
2012/09/03 4 支店で顧客情報含む帳票の紛失が判明 － 豊和銀行
2012/09/03 婦人服売場で顧客名簿の紛失が判明 － 高島屋日本橋店
2012/08/31 個人情報漏洩で職員を懲戒免職処分に － 神奈川労働局
2012/08/29 プレゼント応募はがきを紛失、誤廃棄の可能性 － 鹿児島放送
2012/08/29 付属病院の患者情報含む USB メモリが盗難被害に － 岐阜大
2012/08/27 過去の成績表が新聞社に郵送、流出経路は調査中 － 長岡工業高専
2012/08/27 顧客や従業員に送信したメールで誤送信が発生 － セントラル短資
2012/08/24 バックアップに利用した職員私用 PC からファイル共有ソフトで情報流出 － 秋田市
2012/08/23 イベント案内メールを誤送信、アドレス 4850 件が流出 － 豊田市
2012/08/23 廃棄カルテが運搬中の車両から飛散 － 浦河赤十字病院
2012/08/22 メルマガ誤送信で読者 125 人のアドレス流出 － 函館市地域交流まちづくりセンター
2012/08/21 コミュニティサイト「みなくる」に不正アクセス － ログイン情報やメルアドが流出
2012/08/21 複数医療機関の患者情報含む USB メモリを紛失 － 名古屋大付属病院
2012/08/20 個人情報含む給水装置工事申込書の紛失が判明 － 大阪市水道局

http://www.security-next.com/category/cat191/cat25

全国のイベント・セミナー情報

■【東京・月例研究会】

※ 会員サービス向上の一環として、今年度から会員会費を 2,000 円から 1,000 円に値下げしております。

過去履歴はこちら→ http://www.saaj.or.jp/kenkyu/getsurei.html

回	日時	テーマ	講師	
第 175 回 月例研究会	9 月 27 日(木) 18:30～20:30	新しい時代のシステム監査を考える	東京海上日動システムズ(株) 代表取締役社長　横塚 裕志様	開催場所は、表下欄外のとおりです。
第 176 回 月例研究会	10 月 26 日(金) 18:30～	コーポレート・ガバナンスとITガバナンス ～監査役の視点から～	アリアンツ生命保険株式会社 監査役　河邊 精一　様	
第 177 回 月例研究会	11 月 21 日(水) 18:30～	SNS の利用とその危険性について	日本アイ・ビー・エム(株) 経営品質・情報セキュリティ推進室 シニアセキュリティアナリスト 守屋 英一様	
第 178 回 月例研究会	12 月 17 日(月) 18:30～	未定	T.M.Aパートナーズ(株) 代表取締役社長 遠藤 誠様	

開催場所:東京都港区芝公園 3-5-8 機械振興会館 地下 2 階ホール
案内図 http://www.jcmanet.or.jp/gaiyo/map_kaikan.htm
(ご注意)昨年までと会場が変わっております。

会報編集部からのお願い

■【ご寄付の中間報告　－２－】

協会事務局では、2012年度事業計画の方向性として定めた、(1)システム監査の普及、促進活動の一層の推進、(2)会員サービスの一層の充実、(3)協会財政の一層の健全化、に沿って協会運営基盤の一層の改善を図るべく、この3月に、定款によって初めて、会費請求書に同封して会員の皆様にご寄附のお願いを申し上げました。会報編集部においても、会報を通じて、ご寄附のお願いとその報告を行ってまいります。

ご寄附は、8月末現在、123人の会員から、40万円を超えるご寄附をいただいております。ご報告とともに篤く御礼を申し上げます。事務局では、1. 寄附の促進、2. 寄附者へのお礼、3. 寄附の活用、4. 寄附活用報告、を推進していきます。また、ご寄附を通じて、当協会が、一般のNPO法人から公益法人である認定NPO法人へかわることを検討しそのメリットまたはそれによって発生する責務について調査を行っております。

寄附者のご芳名の公表につきましては、2012年度末でご寄附をしめて、2013年度はじめに同意を得て会報に公表いたします。また、東京都へ寄附者の氏名、住所を報告することがあり、それについても同意を得て東京都へ報告を行うようにいたします。

■　【会員拡大への皆様のお力添えのお願い 】

協会では、沼野会長、小野副会長・会員増強 PT リーダーを中心に、システム監査に関心をお持ちの周囲の方に是非当協会への入会をお誘い頂きたく、お力添えのお願いを、会員、理事、監事の皆様にお願いしております。その結果、8 月末現在、36 人の入会がありましたが、一方、40 人の退会がありました。退会者には定年退職などそれぞれのご事情があると思います。つきましては、月例会のテーマや会費割引、半期会費によって、新規の入会をお誘い頂きたく、お力添えのお願いを申し上げます。

会報編集部としても、会員増強 PT の活動状況を連載しており、引き続き、会員紹介、勧誘に、ご協力をお願いしてまいります。

■　【公認システム監査人・システム監査人補の資格利用推進の取組み 】

協会では、沼野会長、力副会長・CSA 利用推進 PTリーダーを中心に、公認システム監査人（CSA）・システム監査人補（ASA）の資格利用推進のため、CSA 利用推進プロジェクトを立ち上げております。

会報では、プロジェクトの進捗について引き続き報告してまいります。

以上

会報編集部からのお知らせ

１．会報テーマについて
２．会報記事への直接投稿（コメント）の方法
３．投稿記事募集

□■ １．　会報テーマについて

2012 年 11 月～1 月発行の会報テーマは「システム監査人のやりがい」です（4 月～6 月のテーマは「システム監査人の悩み」、7 月～10 月発行の会報テーマは「システム監査のすすめ」でした）。

近年、情報処理技術者試験のシステム監査の受験者が低迷していると聞きます。また、当協会の会員数も減少傾向にあります。その理由は、システム監査という仕事の意義と面白さが世間に知られていないためであると思います。そこで、今回は、システム監査人としての実務経験が豊かな会員諸氏に、システム監査の意義と面白さを語っていただきたいと思います。もちろん、否定的なご意見も大歓迎であります。

専門職として働く者にとって一番大事なこの点について、議論が盛り上がることを期待します。

・・・・・今月号も多くの方にシステム監査にかかわる記事の投稿をいただきました。・・・・・
・・・・・ありがとうございました。・・・・・

みなさまのご意見等を引き続きお寄せ下さい。また、協会の部会、研究会、支部などの活動の場でも大いに議論をお願いいたします。

□■ ２．　会報の記事に直接コメントを投稿できます

会報の記事は、
1）PDF ファイルの全体を、URL（ http://www.skansanin.com/saaj/ ）へアクセスして、画面で見る。
2）PDF ファイルを印刷して、職場の会議室で、また、かばんにいれて電車のなかで見る。
3）会報 URL（ http://www.skansanin.com/saaj/ ）の個別記事を、画面で見る。

など、環境により、様々な利用方法をされていらっしゃるようです。
もっと突っ込んだ、便利な利用法はご存知でしょうか。

気にいった記事があったら、直接、その場所にコメントを記入できます。著者、投稿者と意見交換できます。
コメント記入、投稿は、気になった記事の下部コメント欄に直接入力し、投稿ボランをクリックするだけです。
動画でも紹介しますので、参考にしてください。
（ http://www.skansanin.com/saaj/ の記事、「コメントを投稿される方へ」 ）

□■　３．会員の皆様からの投稿を募集しております

分類は次の通りです。

１．めだか　　(Word の投稿用テンプレートを利用してください。会報サイトからダウンロードできます)

２．会員投稿　(Word の投稿用テンプレートを利用してください)

３．会報投稿論文 (論文投稿規程があります)

これらは、いつでも募集しております。 気楽に投稿ください。

特に新しく会員となられた方(個人、法人)は、システム監査への想いやこれまで活動されてきた内容で、システム監査にとどまらず、IT 化社会の健全な発展を応援できるような内容であれば歓迎いたします。

次の投稿用アドレスに、テキスト文章を直接送信、または Word ファイルで添付していただくだけです。

投稿用アドレス:saajeditor ☆ saaj.jp (☆は投稿時には@に変換してください)

会報編集部では、電子書籍、電子出版、ネット集客、ネット販売など、電子化を背景にしたビジネス形態とシステム監査手法について研修会、ワークショップを計画しています。研修の詳細は後日案内します。

会員限定記事

【本部・理事会議事録】(会員サイトから閲覧ください。パスワードが必要です)

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

■発行：　NPO 法人　日本システム監査人協会　会報編集部

〒103-0025　東京都中央区日本橋茅場町２－８－８共同ビル６F

■ご質問は、下記のお問い合わせフォームよりお願いします。

【お問い合わせ】　http://www.saaj.or.jp/toiawase/

■送付停止は、購読申請・解除フォームに申し込んでください。

【送付停止】　http://www.skansanin.com/saaj/

■□■ＳＡＡＪ会報担当

編集： 仲 厚吉、安部 晃生、越野 雅晴、桜井 由美子、中山 孝明、藤澤 博、藤野 明夫

投稿用アドレス: saajeditor ☆ saaj.jp (☆は投稿時には@に変換してください)