認定 NPO 法人
日本システム監査人協会報

2015 年 9 月号
No 174

No. 174（2015 年 9 月号）＜8 月 25 日発行＞

今月のキーワードは、

ガバナンス、ＢＣＰ・減災、サイバー攻撃です。

お楽しみください。

写真提供：仲会長

巻頭言

テーマ：ガバナンスを評価する監査という考え方

会員番号 6027 小野修一（副会長）

去る7月 21 日、IT ガナバンスと情報セキュリティガバナンスに関する JIS 規格が制定されました。IT ガナバンスに関する規格は「JIS Q 38500:2015」、情報セキィリティカバナンスに関する規格は「JIS Q 27014:2015」です。

それぞれの規格では、それぞれのガバナンスを次のように定義しています。

IT ガバナンス;組織の IT の現在及び将来の利用を指示し、管理するシステム。（JIS Q 38500:2015）
情報セキュリティガバナンス;組織の情報セキュリティ活動を指導し、管理するシステム。
（JIS Q 27014:2015）

そして、「JIS Q 27014:2015」には、IT ガバナンスと情報セキュリティガバナンス、さらにコーポレートガバナンスを含めた関係が規定されています。

☞ 関連記事続き:

＜目次＞

各行から Ctrl キー+クリックで
該当記事にジャンプできます。
（各記事末尾には目次へ戻るリンク有）

＜目次＞

2015.8

めだか 【 システム監査人の喜び 】

経済産業省より2015年7月24日付でコーポレート・ガバナンス・システムの在り方に関する研究会の報告書「コーポレート・ガバナンスの実践～企業価値向上に向けたインセンティブと改革～」の News Release があった。

背景には、グローバル競争時代の中、企業の「稼ぐ力」の向上に、中長期的な収益性・生産性を高めるため、スチュワードシップ・コードの策定（2014年2月）、社外取締役の確保に向けた改正会社法の施行（2015年5月）、コーポレートガバナンス・コードの策定（2015年6月適用開始）等の取組みがある。2015年6月30日に閣議決定された「日本再興戦略」改訂2015においても、企業の「稼ぐ力」の更なる向上のために、コーポレート・ガバナンスの強化が課題として位置付けられている。また、東芝の会計処理問題から監督機能が課題となっていることがある。

報告書の基本的な考え方は、中長期的な企業価値向上のためのインセンティブ創出、取締役会の監督機能の活用、監督機能を担う人材の流動性の確保と社外取締役の役割・機能の活用、具体的な取組（プラクティス）と制度の双方を踏まえた検討の必要性 となっている。別紙として、（1）我が国企業のプラクティス集、及び英米における取組の概要（参考資料）、（2）会社役員賠償責任保険（D&O保険）の実務上の検討ポイント、（3）法的論点に関する解釈指針 が取りまとめられている。（3）の 法的論点に関する解釈指針 では、以下の事項に法的解釈を整理し論点を明確にしている。

1）上程事項
取締役会への上程事項の範囲を決定する上での考慮事項を示し、一定の場合には、その範囲を限定的に考えることができる旨を示している。

2）社外取締役の役割・機能等
社外取締役のさらなる活用に向けて、社外取締役が行った場合に社外性を失う「業務執行」に当たらない行為の例示や、社外取締役の監視義務の範囲に関する考え方を示している。

3）役員就任条件
役員就任条件の一つである会社補償について、社外取締役を活用した一定の要件の下で、活用が可能なことを明らかにしている。

4）新しい株式報酬の導入
欧米における中長期のインセンティブ報酬と同様の仕組みを我が国で導入するための手続きを整理している。

企業は、コーポレート・ガバナンス・システムを運用するよう求められている。システム監査人は、コーポレート・ガバナンス・システムの一環であるITガバナンスにおいてITリスクに応じたコントロールが適切に整備・運用されているか、また情報システムがその目的に照らして有効であるかを監査し、代表者に報告を行う責任がある。その責任のひとつひとつを果たすことにシステム監査人の喜びがあると思う。

（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。）

＜目次＞

2015.8

投稿【　システム監査人の魅力　】

会員番号　0557　仲　厚吉　（会長）

「情報技術－IT ガバナンス JIS Q 38500:2015」が、日本規格協会より 2015 年 7 月 21 日付で発行されました。当協会では、副会長の力利則 氏、理事の清水惠子 氏が原案作成委員としてかかわっています。IT ガバナンス規格は、適用範囲に、“この規格は、組織の経営陣（オーナー、取締役会の構成員、経営者、パートナー、上級取締役又はその他これらと同等の人）のため、組織内で効果的、効率的及び受け入れ可能な IT 利用に関する原則について規定する。この規格は、組織によって使われる IT サービスに関係したマネジメントプロセス及び意思決定のガバナンスに適用できる。これらのマネジメントプロセスは、組織内の IT の専門家若しくは外部のサービス提供者によって、又は組織内の事業部門によって管理することが望ましい。”と規定しています。

また、“さらに、この規格は、経営陣への助言、情報提供、支援などを行う人々への指針を示す。その人々には次の者を含む。”とあって、“ -上級マネージャ、 -組織内で資源を監視するグループの構成員、 -法律又は会計のような外部の業務又は技術の専門家、 -専門家、小売り関係者又は専門家の団体、 -ハードウェア、ソフトウェア、通信及びその他の IT 製品の供給業者、 -内外のサービス提供者（コンサルタントを含む。）、 -IT 監査人”を挙げています。

IT ガバナンス規格では、良好な IT ガバナンスのための枠組みとして、六つの原則、すなわち、責任（Responsibility）、戦略（Strategy）、取得（Acquisition）、パフォーマンス（Performance）、適合（Conformance）、人間行動（Human Behavior）の原則を提供しています。IT ガバナンスには、IT の利活用における事業必要性と、事業圧力が内外から掛かってきます。また、IT ガバナンスの構図は、「IT ガバナンス （（評価（Evaluate）、指示（Direct）、モニタ（Monitor））」と、「事業プロセス （IT プロジェクト、IT 運用）」の二つになっていて、「IT ガバナンス」は、「事業プロセス」との間で、「計画・方針」を指示し、「プロトコル」を評価し、「パフォーマンス＆適合」をモニタするというモデルになっています。

当協会では、2015 年 8 月 21 日（金）18 時 20 分より第 27 回 CSA/ASA フォーラム（日立システムズ本社・大崎）で、CSA 利用推進グループ主査 力利則 氏により IT ガバナンスについて講演会を開催します。また、12 月 14 日（月）18 時 30 分より第 209 回月例研究会（機械振興会館地下 2 階ホール・神谷町）で、IT ガバナンスをテーマにセミナーを開催します。

当協会は、2001 年（平成 13 年）9 月に定款を制定し、「本法人は、システム監査を社会一般に普及せしめると共に、システム監査人の育成、認定、監査技法の維持・向上をはかり、よって、健全な情報化社会の発展に寄与することを目的とする。」としています。今後、システム監査人の魅力は、IT ガバナンスの JIS 規格制定を契機に、IT ガバナンスを通じ、IT 監査人として健全な情報化社会の発展に寄与する活動のなかに育まれていくと思います。

以上

＜目次＞

2015.8

投稿【 ガバナンスを評価する監査という考え方 】

会員番号 6027 小野修一（副会長）

活性化委員会で議論していることですが、この「ガバナンス」というシステムをシステム監査の対象に見据えてはどうでしょうか。「ガバナンス」というシステムを対象にした監査をシステム監査と捉えてはどうでしょうか。

・「ガバナンス」というシステムが、組織の実態に則して構築されていること
・「ガバナンス」というシステムが、組織の経営および業務活動に有効かつ効率的に機能していること
・「ガバナンス」というシステムの安全性・信頼性が確保されていること

などをシステム監査で評価します。情報システムが「ガバナンス」というシステムの中核に位置していることは異論のないところですので、システム監査には情報システムの安全性、信頼性、効率性、有効性などの観点での評価が含まれることは当然です。

当協会も協力して進められているシステム監査の ISO 化も、こうした考え方に結びつけられます。その ISO のタイトルは、「IT audit」から「IT assessment」に変更されたとのことです。システム監査という名称も変更を検討する必要があるかも知れません。

今年から来年にかけて、システム監査を取り巻く環境は大きく変わりそうです。当協会はそうした環境変化に的確かつタイムリーに対応していかなくてはなりません。活性化委員会では、現在策定を進めている「ビジョン」の中に、この新たな考え方、新たな対応を盛り込むべく検討を行っています。

会員の皆様のご意見をお願いいたします。

以上

＜目次＞

2015.8

投稿　【　阪神･淡路大震災記念　人と防災未来センター訪問録　】

会員番号　898　　竹下和孝

目次:･人と防災未来センター訪問録
- ･命を守る実践
- ･風水害、東日本大震災
- ･「鉄人28号」発見。神戸の街にガオー
- ･未来志向のシステム監査

防災訓練が実施される9月が近いですが、どれほど真剣に避難訓練、防災チェックなどの行事に参加しているでしょうか。訓練とはいえ、本番そのものの臨場感を持ち準備不足を知るにはどのような方法が有効でしょうか。

今から20年ほど前のことですが、私が経験した英国での火災避難訓練では、避難に要した時間が当初計画を超えた場合には、同席する官庁の消防･防災担当の判断でやり直しを指示される、という場面に遭遇しました。当時の状況としても、災害訓練のありかたとして大変印象深い経験をさせていただいたわけです。

さて、国内では実際に規模の大小にかかわらず事故や災害に遭遇することは多く、いろいろな場面で、チェック、訓練、実践することができます。しかし、大規模な災害に対しては被災地を訪問する、実際に被災者の経験を聞くのが役に立つでしょう。 以前から計画していた「阪神･淡路大震災記念　人と防災未来センター」(略称DRI)を訪問することができました。DRIは、Disaster Reduction and Human Renovation Institution　の略称で減災がコンセプトです。DRIでは震災発生･被災時の状況や復興までの足取りを、映像記録が中心なので迫力があります。

■人と防災未来センター訪問録

地震発生時刻を示した時計の針オブジェ

人と防災未来センターの西館(左)と東館(右)

展示物見学の流れは、まず、西館へ入館して受付を終えると、上映のタイミングを待つため、所定の人数ごとにグループ分けされ、エレベータで4Fへ案内されます。各種団体や学校の研修としての利用も多いようです。

私が参加した時は、外国からの20人ほどのグループと一緒になりました。DRIを訪問するなんて凄い！

映像の再生が始まる前に、会場の担当者から注意事項が説明されます。その後、外国グループの添乗員と思われる人が、これから上映される映画の概要と注意事項を中国語で補足説明していました。

後で振り返ると、これはとても重要な情報で、場合によっては体調を壊すほどインパクトがある映像についての注意なのです。 その映像とは、・・・震災当時の「1.17シアター」という臨場感あふれる映像です(約7分)。

最初の映像が一撃を加えます。周りが崩れ落ちる地震の事実を再現したその迫力に、足を踏ん張り、身構えるほどでした。地震の揺れに慣れていない外国からの訪問者には、多分、驚愕の連続でしょう。

夜明け前の静かな早朝が一転する地震発生当時の様子を、複数個所からの映像で体感するので、市街地の様子、オフィス街の様子、電車の路線での様子、高速道路での様子、そして一般家庭の様子など、あの日の朝の被災状態を繰り返し再現しています。つまり、映像では繰り返し「そのとき」を体験します。

映像とともに流れる効果音は、地震発生当時の様子、実態を限りなく再現したものであろうと思われるもので、決して過剰に効果を狙ったものではないと思われます。

映像中に挿入される字幕は、流れる音声とほぼ同じで、衝撃的な画面の場所や簡単な解説が続きます。

外国人のグループはトランシーバを利用していたようなので、たぶん、いくつかの言葉に対応したナレーションや説明がされていたものと思います。

センターのある地域全体が大規模復興拠点のひとつ

センターの海側は公園、広域避難場所として整備

でも私たちは、その中の一つの場面しか経験していないわけで、被災者の立場で考えると、自分の周りは何がどうなっているのか、想像もつかない。真冬の早朝でもあり、日の出前の周りはまだ暗い。

また、初期の段階で送電線は切断され停電しているので、多くは暗闇の中での出来事。

これだけでも、恐怖の中の出来事であったことが想像できます。

まだ就寝中の自分の身に何が起きたのか、家財道具が倒れてくるが、その周りがどうなっているのか、自分の体を支え、平常心を取り戻そうとするだけで精一杯の時間が、数分、続く。

やっと大きな揺れが収まって、我に返る。が、しかし、自分の体が動けばいいが、動かない場合にはどうするのか。近くにいるはずの周りの人は、家族の安否はどのように確認できるのでしょうか。

ここでの教訓は、大震災の発生時には、その場その場での個人の判断で、命を守る、命をつなぐ行動が必要で、普段の予防対策、感覚として身につける訓練、とっさの自衛行動が大事だということを痛感します。

映像の上映が終わって、次の順路が紹介される。幸いに、体調を崩した人はいない様子。
そこで再び、先の添乗員が外国語で解説を始める。これは中国系アクセント、たぶん、台湾の中国語かな。

その後、少し歩いて隣の部屋へ行くと、ジオラマ模型で再現された震災直後の町並みが紹介されています。震災時に多くは焼失したと聞くが、焼け残った遺品、当時の写真、地震発生時刻を示した大きな時計などの展示物。大規模な火災の後、力強く復興されていく町並みなどをドラマ仕立てに紹介しています。鑑賞の時間は自由なので、関心を持つテーマの前に足を止め、団体がきたらいったん退避して、また見に来ればいい。というスタイルで、これらは制限時間なしで見学できます。多くの見学者は次々に足早で去っていきます。

復興支援をする側、支援される側の観点からテーマが整理され、用意されています。個人だけでなく、自治体、町内会、ボランティアなど、いろいろな立場からの関心を十分に満たすほど充実しています。体験者自らが、自分たちの経験を後世に残すための努力をしていることへの理解を深めることができます。

都市型の大規模地震としては、米国サンフランシスコで発生した地震が思い出されるが、国内では最初の大都市直撃の被災記録であり、ここまで詳細の分析を加えた資料は大変貴重だと思う。だからこそ、外国からの訪問者も多いのであろう。

■命を守る実践（援助を受けるためにも必要）

後半の掲示物を見ると、国際災害救助隊として、欧州のスイス、英国、フランス、ドイツなど地震発生直後からぞくぞく支援に乗り込んでいることがパネルに記録されています。日本国政府と災害対策本部の設置や救助活動開始と、ほぼ同時進行的に、外国からの救助隊が駆け付けてくれています。被災直後の数日が命を保つための救助活動に重要な時間であることを知り、遠隔地にも関わらず国際援助を黙々と実践する姿がある。そのスピードには驚くばかりです。このような外部からの援助を受けるにも、受ける側の体制整備が必要です。

命を守る4つの実践パンフレット
（耐震化・室内安全・備蓄・避難）

地震など自然災害や天災の発生は防ぐことはできい。
しかし、減災の考え方を広げ実践することで、震災の被害は小さく、少なく、時間も短くすることができるという考えで構成されています。
映像や展示パネルを見るだけでなく、訪問者ひとりひとりが、
自分で感じ、考え、行動に移すための自覚を促すように、設計され、学習教材として、実践パンフレット（写真左）などが用意されています。
そこでは、災害からあなたや家族の命を守る4つの実践として、耐震化・室内安全・備蓄・避難が掲げられています。
機会があったら、再度、家族と一緒に訪問したいと思いました。

●DRI名称：阪神・淡路大震災記念 人と防災未来センター
●TEL：078-262-5050
●住所：神戸市中央区脇浜海岸通1-5-2
●検索：http://www.dri.ne.jp

実際の被災者がそれぞれの体験を報告する語り部コーナーが印象的でした。
ここまでの展示物は歩きながら立って見学するので、パネルの展示物を見るのにも時間がたつと疲れてきます。
語り部コーナーでは映像を見ながら、録画された体験談を見る(聴く)事ができます。10人ほどの椅子と小スペースが用意されており、語り部の映像は、場面ごとや役割ごとに選択でき、自動再生されます。

■風水害、東日本大震災 (東館の展示テーマ)

連絡通路から東館へ移動すると、そこは水の大切さと、水害、台風など風水害に関する展示がされていました。
津波で大きな被害をこうむった東日本大震災の被害状況の画像を、3Dメガネを借りて学ぶことができます。

東日本大震災では、津波に流されて内陸まで漂流し、そのまま残された大型タンカーが印象的でした。
また、原子力発電所が被災し、原子力発電所そのものが廃炉にむけた対応を進める中で、被災し被爆した近隣地域では、復興もまだ手付かずの地域が残されていることは、大変痛ましいことです。
一方で、東日本大震災の避難所の運営や水、食料などの援助物資の配給には、神戸市役所が蓄積した記録や手順が役立っているそうです。このように貴重な経験を共有できる体制を活用できることは素晴らしい。

阪神淡路大震災の印象として記憶に残るのは、次のような光景と共に火災による被害の大きさでした。
・高速道路の高架が折れている画像、その先端には墜落をまぬがれたバスが残っている
・大きなビルが倒壊している。マンションの1階部分が、隙間もないほどつぶれている
・オフィス街のビルでは、窓ガラスは破損して落下、多くの看板や広告塔も落下。

被災から20年がたって、被害にあった高速道路は新築、補強され復旧し、復興住宅が建設され、神戸の繁華街は賑わいを取り戻し、住宅地は再建されていました。復興した神戸の街並みは、復興住宅、復興マンションがそびえたつ新しい街並みを示していました。さらに、首都圏地震を想定した対策提言コーナーも印象的でした。

■「鉄人28号」発見。神戸の街にガオー

白黒のイメージの鉄人

帰路、ちょっと足を伸ばして、震災当時に最も被害が大きかったという長田町付近で復興の状況を探索。

そこで発見したのが、JR新長田駅南側、駅前ではありません。1ブロック離れていて、商店街のビルを抜けると、そこが若松公園で、直立時には18mにも達するという長身の「鉄人28号」が公園中央に設置されています。

この巨大なモニュメントは、リモコンで操作しても動くわけではないのですが、実際の大きさの1/1スケールだそうです。

「鉄人28号」は、1956年から少年雑誌に連載され、アニメ化された人気作品でした。当時は雑誌もアニメも白黒の時代なので、写真左のイメージですね。

中は鉄骨、外は耐候性鋼板製。重量はおよそ50トン。両足の下、深さ6mに埋められたおよそ150tの基礎で支えられているとの紹介をWikipediaで見つけました。

神戸出身の漫画家、故・横山光輝さん作品で長田の復興とまちを盛り上げようと、震災復興と地域活性化のシンボルとして商店街の方々が中心となり募金活動して設置されたそうです。

その周囲は「鉄人広場」として整備されていて、真夏日には憩いに必要な影が少ないのですが、春秋の夕方や週末には家族連れで賑わう場所でしょう。

現在の広場をカラーで見ると、こんな威容でした。人の姿が足首ほどの位置にあります。

やはり大きかったんですね、鉄人は。

「鉄人28号」のアニメが人気を得ていたころ、ロボットとしてオペレータの操作に従う「鉄人28号」は、人口頭脳を持ち自発的に行動する鉄腕アトムと対照的でした。当時の子供だけでなく大人にとっても魅力的な未来を示す創造物でした。当時の夢の世界は、実現しているものも多いことに気づきます。

正義の味方、鉄人28号

その後の20年ほどは順調に経済の規模も、家庭の所得も生活の質も上がっていったので、その成長の軌跡を重ね合わせながら、地域社会の復興を願いながら、踏ん張ろうとの決意を新たにしたのかなとは、私の勝手な創造です。そう思うと、住宅や商店街の回りを見渡すと、見事に再建された町並みをしっかりと見せていただきましたよ、と熱い気持ちがこみ上げてきます。

最近の制御用ロボットや人型ロボットを見ると、さすがに自由に空間を移動するロボットはまだまだですが、機能的には「鉄人28号」に近いものが実現できています。宇宙開発で活躍する自動装置やドローンのような空間を移動する無人飛行装置を組み合わせることができれば、夢ではない、と思える時代になりました。

■未来志向のシステム監査

この数年間、セキュリティ対策に注意が先行して、どうしても保護、防衛という守りの姿勢に気持ちが慣らされていますが、セキュリティ以外の分野に目を向けると、ITをより活用して豊かな社会構築を目指すという分野を開拓することができればシステム監査の対象も広がっているということでしょう。

システム監査人には、IT活用の先発隊として活躍してきた元システムズエンジニアの方々が多いと思いますが、現在やこれからの時代に向けて、どのように安全で効率的な無人装置や有人機器の運行を支援することができるでしょうか。コンピュター機器の内部から外を見ると地上に限らず、地下、海底、宇宙、そしてサイバー空間など、活躍の舞台は無限に広がります。

もっと夢を語ることで新しい社会秩序の構築に力を入れるような活動をしたい、システム監査人としても、新しい技術や仕組み構築に知恵をひねり出すような積極的なシステム構築に注力していた頃が懐かしいと感じました。

帰路、新神戸駅から新幹線に乗車すると、そのあたりは六甲山地の一角。ずいぶんと長いトンネルだなと改めて実感します。そういえば山陽新幹線はトンネル新幹線と揶揄されていたことを思い出します。こういう場所で開通しているので港町神戸のイメージとは違う存在感を示しています。神戸の繁華街まで行くにはJRの乗り継ぎはなく地下鉄を利用します。開通当時の設計者は、高速鉄道の利便性である速度を損なわないように、できるだけ直線的に電車を運行させるような路線を描くと、必然的に山肌を這うような路線ではなく、トンネルで一直線に通過するような設計にならざるを得なかったのでしょう。

長いトンネルを抜けると大阪伊丹空港へ発着する飛行機の姿が見えてきました。羽田空港から伊丹空港までの飛行時間は1時間未満としても、空港までの移動時間、飛行機の出発までの待ち時間を考慮すると、新幹線と航空機はよきライバルの関係にあることもうなずけます。新大阪－東京間は、2．5時間で移動でき、新大阪－博多間の2．5時間を加えると、東京－博多間を最短で5時間で移動することができています。

私にとって新幹線を利用する利点は、発車時刻の5分前に着席しても十分余裕があるという便利さ、手軽さです。格安航空会社LCCは、成田空港や関空を拠点としているので飛行時間以外に空港までの移動時間と費用が発生しますが、それでも魅力的な価格でどのようにシェアが変化するか、今後の展開が大変興味深い分野です。

この交通機関の安全性については、法制化され行政機関が直接行う監査の需要があり、高度な情報システムを搭載した新型車両や交通システムも広がっています。

交通安全マネジメントシステムなど、システム監査の経験を活かせる分野もあり、どのように参加できるかなあ、などと思いを重ねていると、飛行機の見える空間はなく、すでに京都駅を過ぎたようです。

以上

＜目次＞

2015.8

第 204 回月例研究会講演録【 最近のサイバー攻撃と対策の解説 】

会員番号 0557 仲 厚吉

講師 ： 独立行政法人 情報処理推進機構(IPA) 技術本部 セキュリティセンター 情報セキュリティ技術ラボラトリー
主任研究員 渡辺 貴仁 氏

日時・場所 ： 2015 年 7 月 14 日(火)18:30 - 20:30、機械振興会館 地下 2 階ホール (神谷町)

テーマ ：「最近のサイバー攻撃と対策の解説」

要旨 ：

日本年金機構や東京商工会議所など世の中を震撼させる情報漏洩事件が発生している。改めて標的型メールによるサイバー攻撃についてその仕組みと、組織としての対策の考え方や標的型攻撃メールの見分け方、ウイルス活動の痕跡の確認ポイントについて解説する。

また経済基盤である情報システムから社会基盤である制御システムへとサイバー攻撃の対象は多様化しており、先日警察庁からも制御システムに向けた脆弱性の探索アクセスが増加したとの発表がなされた。制御システムへの攻撃による被害事例を紹介し、現状の危険性やリスクを踏まえ、経営層が実施すべきポイントや設計・開発・導入段階および運用段階に担当者がどの様な対応を取るべきかについて解説する。

講演録 ：

1. 情報セキュリティ 10 大脅威 2015

情報システムの管理者は、情報システムが利用目的に沿って安全、有効かつ効率的に機能するよう対策に努めています。しかし、情報システムへの脅威は以前よりも増しているのが現状です。独立行政法人 情報処理推進機構(IPA)は、「情報セキュリティ 10 大脅威 2015」を発表し、2014 年において社会的影響が大きかったセキュリティ上の脅威について、「10 大脅威執筆者会」の投票結果に基づき、次のように順位付けしています。

http://www.ipa.go.jp/security/vuln/10threats2015.html

(1)	インターネットバンキングやクレジットカード情報の不正利用～個人口座だけではなく法人口座もターゲットに～
(2)	内部不正による情報漏えい～内部不正が事業に多大な悪影響を及ぼす～
(3)	標的型攻撃による諜報活動～標的組織への侵入手口が巧妙化～
(4)	ウェブサービスへの不正ログイン～利用者は適切なパスワード管理を～
(5)	ウェブサービスからの顧客情報の窃取～脆弱性や設定の不備を突かれ顧客情報が盗まれる～
(6)	ハッカー集団によるサイバーテロ～破壊活動や内部情報の暴露を目的としたサイバー攻撃～
(7)	ウェブサイトの改ざん～知らぬ間に、ウイルス感染サイトに仕立てられる～
(8)	インターネット基盤技術を悪用した攻撃～インターネット事業者は厳重な警戒を～
(9)	脆弱性公表に伴う攻撃～求められる迅速な脆弱性対策～
(10)	悪意のあるスマートフォンアプリ～アプリのインストールで友人に被害が及ぶことも～

情報システムの利用者が実施すべきセキュリティ対策の基本は変わりません。情報システム管理者は、情報資産(被攻撃対象)の把握、自発的なセキュリティ対策への取組み、対策の計画と予算の確保を行うことが求められます。攻撃

の糸口と情報セキュリティ対策の基本をまとめると次のようになります。

攻撃の糸口	情報セキュリティ対策の基本
ソフトウェアの脆弱性	ソフトウェアの更新
ウイルス感染	ウイルス対策ソフトの導入
パスワード窃取	パスワード・認証の強化
設定不備	設定の見直し
誘導(罠にはめる)	脅威・手口を知る
その他の重要な対策:文書によるセキュリティ対策の明文化、システムによる制限や強制、バックアップやシステムの冗長化、検査や監査、認証の取得 等	

「情報セキュリティ 10 大脅威 2015」のうち、上位 5 位の脅威の概要は、次のようなものです。

(1) インターネットバンキングやクレジットカード情報の不正利用～個人口座だけではなく法人口座もターゲットに～

ウイルスに感染したパソコンが不正送金の被害に遭う、また、フィッシング詐欺により入力した認証情報が窃取される等により、インターネットバンキング被害額は、2014 年は前年の 2 倍の被害額、1,876 件、29 億 1,000 万円となっています。1 件あたりの被害額が増加し、法人・地銀の被害が急増する傾向があります。法人口座は取引限度額が高いため高額被害になります。銀行が啓発するセキュリティ対策の実施が求められています。

・ウイルス対策、脆弱性の解消(セキュリティパッチ)の実施、及び銀行が提供する専用のウイルス対策ソフトの採用。

・セキュリティレベルの高い認証方式(ワンタイムパスワード、電子証明書)の利用。

銀行が指定した正規の手順で電子証明書を利用します。法人向けインターネットバンキングでは、標準的な認証としてパスワードと電子証明書による2要素認証を採用します。また、マルウェア(不正プログラム)は電子証明書と秘密鍵をエクスポートし攻撃者サーバへ送信するので、それを封じるため 「エクスポート不可」と設定し、「秘密キーの保護」の設定を「中また高」とします。予め証明書はバックアップしオフラインで保管しておきます。法人のインターネットバンキングでは、できれば、インターネットバンキング専用パソコンの利用が望まれます。

(2) 内部不正による情報漏えい～内部不正が事業に多大な悪影響を及ぼす～

従業員・職員が故意に内部情報を持ち出し私的に利用し転売する事件が発生しています。事件によって企業・組織の信用が失墜し、被害者から補償・賠償が求められます。2014 年の事例として、通信教育大手から膨大な個人情報が漏えいした事件(委託先企業の社員が 3,504 万件の個人情報を持ち出して被害企業は顧客に総額 200 億円の補償を発表)が報じられています。事件の発生要因として、動機(処遇の不満、借金による生活苦)、機会(不正行為ができる環境)、正当化(自分勝手な理由づけ)が挙げられます。

(3) 標的型攻撃による諜報活動～標的組織への侵入手口が巧妙化～

ネット経由のスパイ活動により標的とされた企業・組織の情報が流出する事件が報じられています。標的組織への侵入手口が巧妙化し、取引先や関連会社を踏み台にして本丸を狙う傾向があります。メールのやり取りの後、ウイルス入りのメールを送る手口(やり取り型)や、ウェブサイトに導かれてウイルスに感染させられる手口(水飲み場型)の攻撃があります。

(4) ウェブサービスへの不正ログイン～利用者は適切なパスワード管理を～

パスワードを窃取されウェブサービスを不正利用されて被害をこうむる事件が報じられています。複数サービスでパスワードを使い回す利用者が被害を受けています。

・SNS サービスでログインされ友人になりすましてプリペイドカードを購入される。

・ポイントを不正利用される。

被害を防止するため、パスワードは、長く複雑なパスワードを設定します。ID がメールアドレスのサービスでは、サイトごとにパスワードを違える必要があります。不正なログインに気づく、または防止するための機能を使うのも有効です。

(5) ウェブサービスからの顧客情報の窃取～脆弱性や設定の不備を突かれ顧客情報が盗まれる～

ウェブサービスから個人情報が窃取される事件が多発しています。クレジットカード情報が窃取されると金銭被害に発展します。2014 年には、OpenSSL の脆弱性を狙った攻撃があり、894 件のクレジットカード情報が漏えいしています。ウェブサイト運営者は、安全なウェブサービスの構築に、セキュリティを担保した設計と開発が求められています。

2. 内部不正による情報漏えい

2014 年に内部不正事件の報道が相次いでいます。事例を2つ挙げて説明します。

・内部関係者による個人情報漏えい

2014 年 7 月、株式会社ベネッセコーポレーションの顧客データベースを保守管理するグループ会社(株式会社シンフォーム)の委託先の元社員が、顧客の個人情報を名簿業者へ売り渡す目的で、記憶媒体にコピーし流出させたとして不正競争防止法違反の疑いで逮捕された。

・海外への技術情報の流出

2014 年 3 月、東芝のフラッシュメモリーの研究データを不正に持ち出し、転職先である韓国の半導体大手SKハイニックスに提供したとして、東芝と業務提携していた半導体メーカー サンディスクの元技術者が、不正競争防止法違反(営業秘密開示)容疑で逮捕された。

不正行為を働く動機を高める要因は、処遇面の不満に関する項目が上位に3つ、すなわち不当だと思う解雇通知を受けた(34.2%)、給与や賞与に不満がある(23.2%)、社内の人事評価に不満がある(22.7%)、になっています。内部不正に関する企業の実態調査で内部不正への気持ちが低下する対策が講じられていないという報告もあります。例えば、社内システムにログインするための ID やパスワードの管理が徹底されていても、社内システムの操作の証拠が残るような対策がとられていないと内部不正の防止策が有効でないことがあります。情報が漏えいしてしまったときは、発見・報告に続いて、初動対応、調査、通知・報告・公表、抑制措置と復旧、事後対応という過程で対応していきます。IPA では、「情報漏えい発生時の対応ポイント集」を公表しています。

http://www.ipa.go.jp/security/awareness/johorouei/

IPA では、「組織における内部不正防止ガイドライン」を作成しています。ガイドラインでは、基本方針、資産管理、物理的管理、技術・運用管理、証拠確保、人的管理、コンプライアンス、職場環境、事後対策、組織の管理の 10 の観点で 30 の対策項目を挙げています。

http://www.ipa.go.jp/security/fy24/reports/insider/

3. 標的型サイバー攻撃

標的型サイバー攻撃の報道事例では、2015 年 6 月に、“”不正アクセスで年金情報 125 万件が流出か（NHK）“や、”標的型メール、東商も被害・・・1 万件超情報流出か（読売新聞）“、等が大きく報じられています。

攻撃者は、標的とする企業や団体の身辺を調査し攻撃を仕掛けます。先ず、もっともらしいメールを標的や関連組織（子会社、委託会社、取引先、加入協会など）に送信して情報収集を行います。IPA を騙ったメールの事例もあります。標的型サイバー攻撃の流れは 7 段階になります。

	段階	内容
(1)	計画立案	攻撃者は、一連の攻撃の基となる情報の収集を行い、本格的な攻撃に向けた準備をする。
(2)	攻撃準備	システム内部に侵入するための攻撃環境を作る。
(3)	初期潜入	メールを標的ユーザに送付しマルウェアに感染させる。
(4)	基盤構築	コネクトバック通信（リモートコントロール通信経路）を開設し、各種ツールを用いて試行錯誤しながら内部のネットワークやサーバの位置情報を把握する。
(5)	内部侵入・調査	前段階で確保した攻撃基盤をベースに次々と端末を乗っ取りながら侵害範囲を広げていく。
(6)	目的遂行	複数の端末とサーバを攻撃者のコントロール下に置き、最終目的に応じた攻撃を行う。
(7)	再侵入	目標組織のシステムに確保したコネクトバック通信を用い継続的に再侵入しシステム内探索を継続する。

情報システムの利用者は受信メールが標的型メールではないか常に注意を心掛ける必要があります。また、OS やアプリケーションを常に最新の状態にして、ウイルス対策ソフトを利用し定義ファイルは最新化しておく必要があります。

情報システムの管理者は、マルウェア感染を防止するため、ウイルス対策ソフト、IDS/IPS（攻撃検知/阻止システム）の導入、セキュリティパッチの適用とともに、ネットワーク分離設計、管理者権限の最小化、ファイル共有の制限などを行い、情報システムの利用者への啓発活動に取り組む必要があります。早期発見のためのログの監視も必要です。

IPA では、「『高度標的型攻撃』対策に向けたシステム設計ガイド」を用意しています。企業等の組織においては、基本的なセキュリティ対策以外にも情報が外部に流出しないための対策、つまり、入口突破されても攻略されない内部対策を講じる必要があります。

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

標的型攻撃メールの見分け方として、知らない人からのメール、誤って自分あてに送られたようなメール、これまで届いたことのない公的機関からのメール、組織全体への案内、心当たりのない決済や配送通知、ID やパスワードなどの入力を求めるメール、知らない人からの添付ファイルのあるメールには注意が必要です。不審な通信を行っている端末を発見した際は、該当の端末をネットワークから切り離し、ファイアウォールやプロキシサーバでブロックします。継続的な脆弱性対策の実施が重要です。

4. 制御システムセキュリティ

(1) 制御システムのセキュリティリスク

制御システムとは、エネルギー分野（電力、ガス等）や石油・化学、鉄鋼業等のプラントにおける監視・制御、機械・食品等の工場の生産・加工ラインなどで多くの企業に利用されているシステムや、社会インフラ（電力、ガス、水道、鉄道、等）で利用されているシステムをいいます。下記は制御システムと情報システムの比較表です。

	制御システム	情報システム
セキュリティの優先順位	システムが継続して安全に稼働できることを重視	情報が適切に管理され、情報漏えいを防ぐことを重視
セキュリティの対象	モノ（設備、製品） サービス（連続稼働）	情報
技術のサポート期間	10 年～20 年	3～5 年
求められる可用性	24 時間 365 日の安定稼働 （再起動は許容されないケースが多い）	再起動は許容範囲のケースが多い
運用管理	現場技術部門	情報システム部門

制御システムにおいて、近年、情報システム同様に、ウイルス感染や不正アクセス等のサイバー攻撃のリスクが増大しています。例えば、監視制御のための PC に適切なセキュリティ対策がなされていないと、LAN を経由して生産ラインやプラントで使われているコンピュータがウイルスに感染し、数億円規模の損失を与えるリスクが危惧されます。

経営層が制御システムのセキュリティリスクに実施すべき事項は、対策マネジメント組織を構築する、サプライチェーン全体で考える、現状の対策状況を確認するように指示を出す、等があります。設計・開発・導入段階では、調達時の要求仕様にセキュリティ要件を含める、運用・保守契約においてセキュリティに関する項目を含める、等が重要です。運用段階では、被害の原因になっている USB や入れ替え端末にセキュリティ対策を講じる、セキュリティ更新プログラム（パッチ）を適用する、等が必要です。

IPA では、制御システム利用者のための脆弱性対応ガイド 「重大な経営課題となる制御システムのセキュリティリスク」～制御システムを運用する企業が実施すべきポイント～ を公開しています。
https://www.ipa.go.jp/files/000044733.pdf

受講した感想:
講演は最近のサイバー攻撃と対策の解説に多岐にわたっていて、かつ内容が濃かったと思います。講師が初めに強調されたように情報システムの利用者が実施すべきセキュリティ対策の基本は変わりません。また、情報システムの管理者は、情報資産（被攻撃対象）の把握、自発的なセキュリティ対策への取組み、セキュリティ対策の計画と予算の確保を行うことが求められます。標的型サイバー攻撃は怪しいメールの開封が引き金になります。安易に怪しいメールを開封しないことが重要です。標的型サイバー攻撃を被った日本年金機構と東京商工会議所は、利用者が二次被害に遭わないようホームページに留意点を公表し注意喚起をお願いしています。是正処置は、予防処置に比較して何倍もの人手と、費用や時間が掛かることを肝に銘じたいと思います。

以上

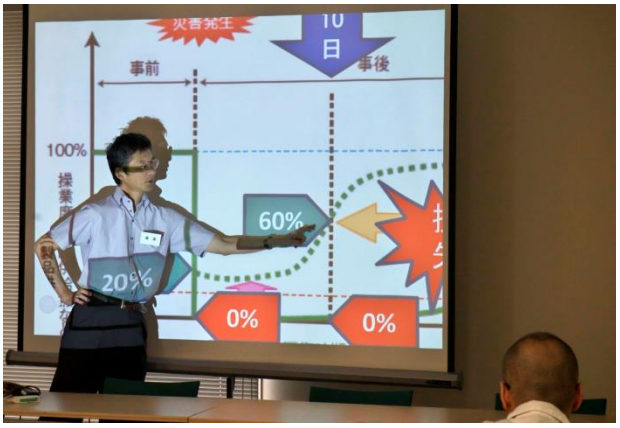
＜目次＞

2015.8

支部報告　【　ＩＴ－ＢＣＰ体験セミナー　開催結果報告　】

会員番号 1709 荒町 弘 （近畿支部）

１．セミナー名称　：　ＩＴ－ＢＣＰ体験セミナー
２．開催日時　：　２０１５年６月２７日（土）１０：００～１７：００
３．開催場所　：　大阪大学中之島センター　６０８教室
４．当日参加者　：　受講者　７名
スタッフ　荒町、松井、金子、尾浦、伊藤（ＢＣＰ研究プロジェクト）
広瀬



５．開催概要

当セミナーは、ケースシナリオを使った体験演習により IT-BCP のポイントを把握することを狙いとし、昨年度から開始したセミナーです。災害初動の基礎知識や体験演習、IT-BCP の現状と危機対応の原理原則など、IT-BCP の必要性やポイントについて学んでいただくセミナーとして今年も開催しました。

カリキュラムは2つの講義と演習2題から成り、午前はオリエンテーションの後に講義1つ、お昼休みを挟んでのグループ演習を実施し、チームごとの発表および解説を経て、2つめの講義を行うといった流れで 1 日コースのプログラムを終えました。各演習の最後に検討した結果をチーム単位にまとめて発表いただき、講師講評を踏まえて受講者全員で成果の共有を図りました。

５．１　オリエンテーション（担当：荒町）

はじめに、セミナー開催にあたり、オリエンテーションとして以下の説明からスタートしました。

・SAAJ近畿支部BCP研究プロジェクトの活動概要
・IT-BCPの普及状況や東日本大震災の教訓としての災害時における初動の重要性
・本日のカリキュラムや当セミナーの目的とするところについて

５．２　講義１　（担当：尾浦）

午前の講義として、「災害初動の基礎知識」～～情報収集力と防災想像力を高める～～ と題した講義を行いました。災害時の初動期のうちでも発災期（最初の3時間）に焦点を当て、BCP発動までの社内の動きを想像してもらうとともに、平成7年の阪神淡路大震災や平成26年の広島土砂災害の事例説明を交えてBCP作成時や検証時の視点について講師自らの経験談を交えながら説明を行いました。

管理者としての立場の方が、危機事象に際して下すべき決断内容と決断に必要となる情報を事前に想定するとともに、危機可能性を察知した際には更に想像力をはたらかせつつ、自ら必要な情報を取りに行く姿勢が必要であるということ。そして、このように「防災想像力を働かせることができるということ」が発災期の情報収集において決定的な差になるということについて事例を通じて説明を行いました。

５．３　グループ演習　（担当：金子）

近畿圏で 30 店舗の運営を行う中堅流通業の企業A社を舞台とし、受講者にはA社のIT管理部門の社員の立場になっていただき、あらかじめ設定した9つのシーンに対し、各演習のテーマに沿ってIT管理部門としてどのように対処すべきか個人で検討の上、チームとしての見解をまとめました。まとめた内容は、模造紙にシーンごとにポストイットも活用しながら書き出し、2チームそれぞれのリーダ役の方から発表を行いました。

検討内容に対して意図的にタイトな時間設定とし、限られた時間内で多数の案件を一度に迅速に意思決定する重要性に気付いていただく狙いで、インバスケット研修の手法を採用しました。

(1)演習１（災害発生直後の初動対応）

初動としてIT管理部門はどのように対応すべきかを検討しました。

・優先順位付け、どの部署の誰にどのように指示を行うか等

(2)演習２（ＩＴ－ＢＣＰのポイント検討）

IT管理部門として、何を事前に準備・計画していればより適切な対応が可能であったかを検討しました。

・行動計画／ルール、危機対応時に有効な文書／資料、ダメージを少なくする事前対策等

(3)講師講評／演習の解説　（担当：尾浦・金子）

各チームの発表内容に対し、講師側から実務体験も踏まえて講評を行いました。また、9つのシーンの設定の背景と初動対応、及びIT－BCP策定のポイントについて解説しました。

５．４　講義２：訓練・演習で鍛えるＩＴ－ＢＣＰ　（松井氏）

午後の講義として、「IT-BCP の現状と危機対応の原理原則」～想定外への対応～ と題した講義を行いました。

講義の概要としては、IT-BCP の現状と課題、「想定外」への対応は可能か？、IT-BCP の原理・原則という流れで講演を行いました。自治体の情報システムに関する IT-BCP の現状や重要データの保管状況など、の参考データを参照しての IT-BCP 普及状況の解説を行う一方で、東日本大震災に代表されるような、「想定外」の事態に対しての対応力をいかに付けていけばよいか、という点に対する解決の糸口についていくつかの視点から解説を行いました。

「想定外」にも対応できるような取り組みとして大切なこととして、「IT-BCP の原理原則」、「BCP の 5 原則」、「危機管理の 4 原則」について触れながら、日頃の訓練・見直し・改善等の取組みの重要性についての講演を行いました。

６．受講された皆様の感想

受講された皆様からは、以下のようなご意見をいただきました。（アンケートから抜粋）

・初動対応演習で他の参加者からも気付きを得られた。
・時間を区切って複数の課題を検討する訓練は効果があると思いました。
・IT-BCPの重要性やポイントが良く分かりました。
・A社の説明、チームのミッション、ネットワーク図等の理解する時間が不足気味と思われる。
・演習によりIT-BCPのポイントを理解することができました。
・テキスト及びケーススタディ共、よく検討されており、完成度が高いと思います。
・土・日で実施してもらったほうが、参加しやすいので良かったです。
・トイレ休憩をもう少し増やして欲しい。一般と会員の参加費用の差をもう少し拡げても良いのでは？
・ケーススタディの時間が少し短かったと思います。
・2～3時間くらいの方が参加し易いです。
・自然災害以外にも、パンデミックやサイバーテロなどBCP発動される原因は今後増々多種になると思います。そのような状況でIT部門として何を準備すればいいか教えて欲しい。

７．感想

IT-BCP に関する気付きを提供するという方針で昨年の半日コースから変更して今年は1日コースにて当セミナーを実施しましたが、ケース演習の題材となっているA社の業務内容や情報システムの運用状況に関する理解に時間が不足しているようでありました。一方で限られた時間での意思決定・判断を行うといった演習方法は、昨年に続き受講者の方からも好評を得たのではないかと思います。

また、講義については、昨年は 30 分の講義に比べて今年の 60 分の講義にしたことで受講者のより深い理解を促すことができたのではないかと思います。そして、災害に備えた事前準備の重要性や、企業活動の基盤を担う情報通信基盤や各種 IT ツール等に関する BCP 対策についても考える良い機会を提供できたのではないかと思います。演習で発表いただいた内容は、講師側で用意していた正解とは異なった視点の優れた解答もあり、スタッフ一同大いに勉強させていただきました。

受講者の皆様、スタッフ／関係者の皆様、ご協力ありがとうございました。

以上

＜目次＞

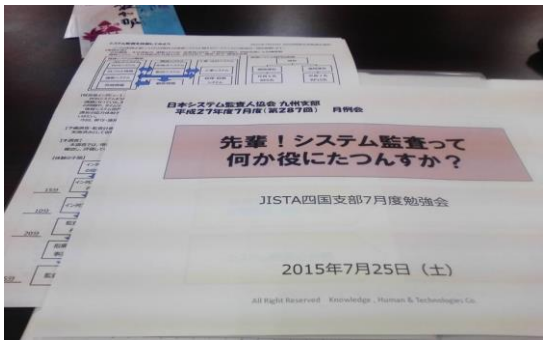
2015.8

支部報告　【　第２８７回（平成 27 年 7 月）月例会に参加して　】

会員番号　0350 鶴岡通　（九州支部会員）

7月25日の九州支部月例会（勉強会）は、JISTA 四国支部で開催されたシステム監査に関する講演に Skype（注）で九州支部も合同で参加致しました。その経緯と感想を述べます。

１、合同開催の背景



この度の勉強会は、JISTA（Japan IT Strategist Association：日本ITストラテジスト協会）の四国支部で開催されたシステム監査に関する講演のテーマ「先輩！システム監査って何か役にたつんすか？」を JISTA のメーリングで6月18日に知り、九州支部月例会の勉強日と開催日も時間帯も重なっていることと Skype で参加できることから、九州支部長に連携できないかのご相談を行いました。

＜私の知りたかった内容＞

①システム監査がどのように、システム技術者に受け取られており、どのような感想を持っているか。

②その中から、システム監査の進むべき道が見えて来るのではないか。

③Skype を活用した勉強会の有効性の確認

・どこまで、会議に活用できるのか。

・活用できるならば、本部の理事会や各部会の会合などに応用できないか。

・活用に当たり阻害要因となるものがあるのか。

２、準備で想定されるご苦労

①開催元の JISTA 四国支部副支部長の伊祁（いき）様との共同開催の打診と交渉

②PC で Skype の環境設定

支部会員のPCに Skype ソフトのインストールと動作確認。

③事前に講演内容の確認と時間調整

④講演のレジュメの入手と内容

事前に講演内容のレジュメ（A4 版の1枚）を入手

レジュメの内容（学習時間160分）

・システム監査の歴史、目的、対象、手順の理解（45分）

・システム監査のワークショップ（60分）

・知っておくべき監査にはどのようなものがあるか（45分）

・システム監査を活用しましょう（10分）

・質疑応答（20分）

⑤支部内への通知と公表

⑥開催資料の準備

参加人数に応じた講義資料のコピー

⑦開催当日の動作確認と資料配布

⑧開催時の進行

トラブル時の対応、参加者に感想の依頼など

⑨その他

３、受講した感想

講演教材と講義内容は、以下の通り

①システム監査の理解

システム監査の歴史、目的や概要を勉強し、次にシステム管理基準のポイントを説明された。

②ワークショップ

事例企業は、地元の百貨店を対象にして、システム概要、規模、問題点等を記載した資料を元に、「保守・運用に関して改善のアドバイス」をして欲しい。

監査手順に従い、予備調査→監査計画→本調査→インタビュー項目作成→インタビュー実施→監査調書作成→指摘事項の事実確認→監査報告と摸擬監査形式で進行して行った。

③情報システムを取巻く各種規程・基準・監査

ISO9001s（QMS）、ISO27001（ISMS）、ISO14001s（EMS）、JISQ15001（PMS）、ISO20000（ITSMS）、ISO21500（PMBOK）、ISO22301（BCMS）、ISO31000（RM 原則及び指針）、会計監査、税務監査など多数の概要と IT 部門との関わりを解説。

会社法、金融商品取引法、内部統制の進め方、IT 統制などの紹介と、システム監査人協会発行の書籍「情報システム監査実践マニュアル」、「IT 統制監査実践マニュアル」を紹介している。

④システム監査の意義

受講者からのシステム監査に対する、有意義性や感想を求めたが活発な意見はなかった。

＜私の知りたかった内容と結果＞

①システム監査がどのように、システム技術者に受け取られており、どのような感想を持っているか。

⇒教材は、システム監査の概要からワークショップ、各種監査、システム監査に有意義について考える内容になっていました。

また、教材は、ワークショップでシステム監査の本質を体験するとても有効な、教材になっておりました。

反省する点としては、最後の「システム監査の意義」についてで、システム監査に対する色々な意見を聞けるかと思いましたが、活発な意見もなく、ただ聴講するだけに終わってしまった。

②その中から、システム監査の進むべき道が見えて来るのではないか。

⇒今回の「先輩！システム監査って何か役にたつんすか？」の勉強会からでは、時間もないことから、システムを理解するに留まり、システム監査に対する意見や要望もなく、システム監査の将来展望の参考になる情報は得られなかった。

③Skype を活用した勉強会の有効性の確認

・どこまで、会議に活用できるのか。

⇒環境設定や通信手段の問題はあるようですが、事前準備（カメラ、マイク、事前資料、トラブル時の連絡方法など）をしっかり行えば、意見交換ができるツールだと分かりました。

・活用できるならば、本部の理事会や各部会の会合などに応用できないか。

⇒通信手段と事前の準備を行えば、システム監査人協会でも有効に活用できると思いました。

・活用に当たり阻害要因となるものがあるのか。

⇒通信手段の確保として、回線速度、容量、品質、通信料金などを明確にして準備しておくこと。事前の準備として、資料の事前配布とその資料の読みこなしを行って置くこと。

Skype で講義が進行する中で、音声が聴き取りにくかったり、途切れたり、映像が映らなくなるトラブルが発生しました。他の通信手段として、トラブル時の対応用に、携帯電話等を活用した、連絡ルートを確保して置く必要性を感じました。

４、開催した結果

今回の勉強会は、システム監査学会、ISACA 福岡支部との合同では有りますが、九州支部、開設依頼の参加者が20名と大盛況であったことは、システム監査に対する興味や期待などを図り知ることができ、大変有意義であったと思います。

これを機会に、システム監査の将来性について、Skype などを活用した他の団体との意見交換が活発になり、意見交換をつうじて方向性が見えて来ることを願っております。

最後に、

・開催元の JISTA 四国支部長の土屋様、副支部長の伊祁様、講師の広瀬様には、ご丁寧なご指導と対応をして頂きありがとうございました。

講義資料も講義内容も良く整理され、まとめられておりました。ワークショップを通じて、システム監査を体験する良い資料だと思います。

しかし、私の一番知りたかった、「システム監査の意義」であまり意見が出なかったことは、まだシステム監査そのものが、漠然として受け取られているのかなと思いました。

・福岡の会場では、JISTA 会長の大熊様に参加して頂き、相互の連絡とスムーズな進行にご協力をして頂きました。

・一番苦労したのが Skype の接続環境で、Wi-Fi 環境がないことから、SAAJ 九州副支部長の荒添さんにルータをお借りしての開催となりました。

・最後に、無理難題を快く引き受けて頂き、準備から開催まで実施して頂きました、SAAJ 九州支部長の中溝さんには多大なご苦労をお掛け致しました。

この場をお借りして、ご協力頂きました皆様に、感謝申し上げますとともにお礼申し上げます。

今後とも相互交流や意見交換を重ねて、互いの見識を広めて知恵を出し合って行けたらいいなと思います。

ご協力、ありがとうございました。

(注)Skype とは、無料で楽しめるコミュニケーションソフトです。Skype 同士なら、世界中どこへでも無料で通話チャットができ、Web カメラをパソコンに接続すればビデオ通話もできます。
Skype(スカイプ)は、「Sky peer-to-peer」の略になります。

以上

<

＜目次＞

2015.8

注目情報（2015.7～2015.8）※各サイトのデータやコンテンツは個別に利用条件を確認してください。

■【IoT社会を見据えた国内初の業界横断的なソフトウェア開発指針の策定に着手】

2015年8月5日 独立行政法人情報処理推進機構

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）技術本部ソフトウェア高信頼化センターは、自動車・HEMS(*1)などの製品がインターネットや製品同士で相互に接続する「IoT(*2)社会」を見据え、“つながる”製品に組み込まれたソフトウェアの信頼性を確保するためのソフトウェア開発指針の策定に着手し、本日8月5日、検討会を発足しました。

(*1) HEMS（Home Energy Management System）：スマートメーター等との接続により、家庭の消費電力を管理・制御するシステム。スマート家電と呼ばれるような家電機器の遠隔制御などを可能とする。

(*2) IoT（Internet of Things）：様々なモノがインターネットに接続し、情報をやり取りすること

http://www.ipa.go.jp/about/press/20150805_2.html#L2

参考：米国におけるIoTに関する取り組みの現状（IPAニューヨーク事務所：アメリカの最新IT事情9

http://www.ipa.go.jp/files/000047543.pdf

■【Internet Explorer の脆弱性対策について(CVE-2015-2502)】

2015年8月19日 独立行政法人情報処理推進機構

2015 年 8 月 19 日に Internet Explorer に関する脆弱性(CVE-2015-2502)の修正プログラムが 1 件公表されています。

この脆弱性を悪用された場合、アプリケーションプログラムが異常終了したり、攻撃者によってパソコンを制御され、様々な被害が発生する可能性があります。

Microsoft 社は「悪用の事実を確認済み」と公表しており、攻撃が行われた場合の影響が大きいため、できるだけ早急に修正プログラム（MS15-093）を適用して下さい。

以下の Microsoft 製品が対象です。

·Internet Explorer 7

·Internet Explorer 8

·Internet Explorer 9

·Internet Explorer 10

·Internet Explorer 11

https://www.ipa.go.jp/security/ciadr/vul/20150819-ms.html

＜目次＞

2015.8

【協会主催イベント・セミナーのご案内】

■月例研究会（東京）

第206回	日時:2015 年 9 月 15 日(火)　18:30～20:30　場所:機械振興会館　地下 2 階　ホール	
	テーマ	「マイナンバーがもたらす社会の大変革　－制度施行直前チェックを含めて-」
	講師	一般財団法人 日本情報経済社会推進協会(JIPDEC) 電子情報利活用研究部 部長 坂下 哲也 氏
	講演骨子	いよいよ平成28年1月から「行政手続きにおける特定の個人を識別するための番号の利用等に関する法律」(平成 25 年度法律第 27 号;以下「番号法」)が施行され、個人番号(以下、「マイナンバー」)・法人番号の利用が開始される。一方で、施行まで半年を切ったものの、当協会のセミナーアンケートでも、準備を進めている事業者は 30%程度しかおらず、周知が足りない状況である。マイナンバーは、国内に住民票を有する全ての国民に付番され、一生変わらないものであることから、その管理には十分な注意が必要である。 一方で、全ての国民にユニークな識別子が付与されることによって、オンライン上での本人確認や、添付書類の削減などが期待されており、その利活用についての検討も活発に議論されている。 本講演では、マイナンバーを取り扱う事業者が留意するポイントの解説、現在検討されている利活用ソリューションの紹介と、それによる社会インフラの変化について解説する。また、IT が進展することによって、様々なデータを利用するにあたり、事業者が対応すべきポイントについて解説する。 (参考 URL) ・社会保障と税番号制度(内閣官房) : http://www.cas.go.jp/jp/seisaku/bangoseido/ ・JIPDEC 支援サイト:http://www.jipdec.or.jp/project/mynumber_support.html (参考書籍) ・影島広泰著『マイナンバー制度への実務対応』(清文社) ・榎並利博著『マイナンバー制度と企業の実務対応』(日本法令) ・袖山喜久造『マイナンバー制度と企業の実務』(税務研究会出版局) ・JIPDEC 編『特定個人情報保護評価の進め方』(アマゾン・プリントオンデマンド) ・瀬戸洋一他著 『プライバシー影響評価 PIA と個人情報保護』(中央経済社)
	お申し込み	日本システム監査人協会ホームページ
第207回	日時:2015 年 10 月 23 日(金)　18:30～20:30　場所:機械振興会館　地下 2 階　ホール	
	テーマ	「失敗した IT プロジェクトの真の原因に迫るマンダラ図の紹介」(仮題)
	講師	特定非営利活動法人　日本システム監査人協会 近畿支部　会員　松井　秀雄　氏
	講演骨子	詳細確定次第、HPでご案内いたします。
第208回	日時:2015 年 11月19日(木)　18:30～20:30　場所:機械振興会館　地下 2 階　ホール	
	テーマ	「リスクマネジメントと危機管理　～想定内と想定外原点に戻って考える～」(仮題)
	講師	東京海上日動リスクコンサルティング株式会社 上席主席研究員　指田　朝久　氏
	講演骨子	詳細確定次第、HPでご案内いたします。

■システム監査体験セミナー（実践編）（大阪：近畿支部主催）

	システム監査体験セミナー（実践編）	
	日時：2015 年 10 月 24 日（土）13:00～20:00 /25 日（日）10:00～17:00	
	概要	・本セミナーは、システム監査を実際に行う機会が少ない現状において、システム監査技術者や公認システム監査人を目指される方、内部監査ご担当者やシステム監査にご興味をお持ちの方々に、模擬体験を通したシステム監査能力向上の機会をご提供することを目的としております。特に内部監査人養成は企業の内部統制整備に欠かせない要件となっており、この機会を利用した監査実務の体験は短期間での養成に最適と考えます。今回の監査テーマは昨年度と同様に「現行システムとユーザニーズの適合性、経営戦略と情報システムとの適合性」という、経営者の視点に立ったテーマと致しました。
お申し込み		HPでご案内中です。 （http://www.saaj.or.jp/shibu/kinki/taiken20151024.html）

■中堅企業向け「6ヶ月で構築するPMS」セミナー（東京）

申し込み常時受付中	概要	個人情報保護監査研究会著作の規程、様式を用いて、6 ヶ月でPMSを構築するためのセミナーを開催します。 詳細をHPでご案内しています。（http://www.saaj.or.jp/shibu/kojin.html）
	基本コース	月 1 回（第 3 水曜日）14 時～17 時（3 時間）×6 ヶ月 ※他に、月 2 回の応用コースなどがあります。
	料金	9 万円/1 名～（1 社 3 名以上割引あり）
	会場	日本システム監査人協会 本部会議室（茅場町）
	テキスト	SAAJ『個人情報保護マネジメントシステム実施ハンドブック』

【外部主催イベント・セミナーのご案内】

■ＩＳＡＣＡ東京支部 2015 年　月例会予定（東京）

日時： 2015 年 9 月例会 9/30（水）開催予定 18:30-20:10(受付開始：18:00) 2015 年 10 月例会 10/27（火）開催予定 19:00-20:40(受付開始：18:30) 2015 年 11 月例会 11/25（水）開催予定 18:30-20:10(受付開始：18:00) 2015 年 12 月例会 12/22（火）開催予定 19:00-20:40(受付開始：18:30)	
詳細	http://www.isaca.gr.jp/education/index.html

＜目次＞

2015.8

新たに会員になられた方々へ

Welcome

新しく会員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。
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/index.html
・会員規程にも目を通しておいてください。 http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・皆様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

・各支部・各部会・各研究会等の活動です。 http://www.saaj.or.jp/shibu/index.html
　皆様の積極的なご参加をお待ちしております。門戸は広く、見学も大歓迎です。

ご意見募集中

・皆様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。

＜目次＞

【 ＳＡＡＪ協会行事一覧 】 赤字:前回から変更・追加された予定			2015.8
2015 年	**理事会・事務局・会計**	**認定委員会・部会・研究会**	**支部・特別催事**
8 月	(理事会休会) 29: 中間期会計監査	1: 秋期 CSA・ASA 募集開始～9/30 24: 第 205 回月例研究会	
9 月	10: 理事会	15: 第 206 回月例研究会	5-6:西日本支部合同研究会 (開催場所:岐阜)
10 月	8: 理事会	23: 第 207 回月例研究会	18: 秋期情報処理技術者試験
11 月	12: 理事会 13: 予算申請提出依頼(11/30〆切) 支部会計報告依頼(1/8〆切) 18: 2016 年度年会費請求書発送準備 23: 会費未納者除名予告通知発送 30: 本部予算提出期限	中旬:秋期 CSA 面接 19: 第 208 回月例研究会 20: CSA・ASA 更新手続案内 〔申請期間 1/1～1/31〕 27: CSA 面接結果通知	
12 月	1: 2016 年度年会費請求書発送 2016 年度予算案策定 10: 理事会:2016 年度予算案 会費未納者除名承認 第 15 期総会審議事項確認 11: 総会資料提出依頼(1/8〆切) 15: 総会開催予告掲示 18: 2015 年度経費提出期限	10: CSA/ASA 更新手続案内メール 14: 第 209 回月例研究会 18: 秋期 CSA 認定証発送	
1 月	8: 総会資料(〆) 16:00 13: 総会・役員改選の公示 14: 理事会:通常総会資料原案審議 15: 総会開催案内掲示・メール配信 20: 2015 年度決算案 23: 2015 年度会計監査 26: 総会申込受付開始(資料公表) 31: 償却資産税・消費税	1-31:CSA・ASA 更新申請受付 21: 第 210 回月例研究会 20: 春期 CSA・ASA 募集案内 〔申請期間 2/1～3/31〕	8: 会計:支部会計報告期限 ※2016 年 2 月 22 日(月) 第 15 期通常総会・特別講演 25: SAAJ 創立記念日
2015 年	**以下は、過去に実施した行事一覧**		
2 月	5 日 理事会:通常総会議案承認 22 日 第 15 期通常総会・特別講演 25 日 法務局:資産登記、活動報告提出 28 日 年会費納入期限	CSA・ASA 春期募集(2/1～3/31) 28 日-3 月 1 日 事例研:第 25 回システム監査実務セミナー(前半)	
3 月	2 日 東京都への事業報告書提出 2 日 年会費未納者宛督促メール発信 12 日 理事会	4 日 第 200 回月例研究会 14-15 日 事例研:第 25 回システム監査実務セミナー(後半)	
4 月	9 日 理事会 末日 法人住民税減免申請	認定委員会:新規 CSA/ASA 書類審査 中旬 認定委員会:新規ASA認定証発行 28 日第 201 回月例研究会	19 日 2015 年春期情報技術者試験
5 月	14 日 理事会 29 日 年会費未納者宛督促メール発信	中旬 認定委員会:新規 CSA 面接 29 日第 202 回月例研究会	
6 月	3 日 認定 NPO 法人東京都認定！ 4 日 会費未納者督促状発送 11 日 理事会 12 日～会費督促電話作業(役員) 末日 支部会計報告依頼(〆切 7/14) 末日 助成金配賦額決定(支部別会員数)	10 日 認定委員会:CSA 面接結果通知 16 日 第 203 回月例研究会 18-19 日 事例研:第 27 回システム監査実践セミナー(日帰り 2 日間コース)	
7 月	8 日 支部助成金支給 9 日 理事会	1 日 秋期 CSA・ASA 募集案内 〔申請期間 8/1～9/30〕 14 日 第 204 回月例研究会 20 日 認定委員会:CSA 認定証発送	14 日 支部会計報告〆切

＜目次＞

2015.8

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

2015 年度の年間テーマは、「システム監査人の魅力」です。これまでは「システム監査」に焦点を当ててきましたが、今年度は「システム監査人」に焦点を当てて考えてみたいと思います。8 月号から 11 月号までは、「システム監査人の喜び」をテーマといたします。皆様の幅広いご意見をお待ちしています。

会報テーマは、皆様のご投稿記事づくりの一助に、また、ご意見やコメントを活発にするねらいです。会報テーマ以外の皆様任意のテーマももちろん大歓迎です。皆様のご意見を是非お寄せ下さい。

□■ 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(毎月メール配信)を利用してください)
2. 会員投稿 (Word の投稿用テンプレート(毎月メール配信)を利用してください)
3. 会報投稿論文 (「会報掲載論文募集要項」及び「会報掲載論文審査要綱」があります)

□■ 会報投稿要項 (2015.3.12 理事会承認)

・投稿に際しては、Wordの投稿用フォーム(毎月メール配信)を利用し、会報部会(saajeditor@saaj.jp)宛に送付 して下さい。
・原稿の主題は、定款に記載された協会活動の目的に沿った内容にして下さい。
・特定非営利活動促進法第2条第2項の規定に反する内容(宗教の教義を広める、政治上の主義を推進・支持、又は反対する、公職にある者又は政党を推薦・支持、又は反対するなど)は、ご遠慮下さい。
・原稿の掲載、不掲載については会報部会が総合的に判断します。
・なお会報部会より、表現の訂正を求め、見直しを依頼することがあります。また内容の趣旨を変えずに、字体やレイアウトなどの変更をさせていただくことがあります。

会報記事は、次号会報募集の案内の時から、締め切り日の間にご投稿ください。
バックナンバーは、会報サイトからダウンロードできます(電子版ではカテゴリー別にも検索できますので、ご投稿記事づくりのご参考にもなります)。
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】(当協会ホームページ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: 認定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/

■会報は会員への連絡事項を含みますので、会員期間中は、会員へ配布されます。
会員の所属や登録メールアドレス等の変更は、当協会ホームページ会員サイトより変更してください。
会員でない方は、購読申請・解除フォームに申請することで送付停止できます。
【会員でない方の送付停止】 http://www.skansanin.com/saaj/register/

■□■SAAJ会報担当
編集委員: 藤澤博、安部晃生、久保木孝明、越野雅晴、桜井由美子、高橋典子、西宮恵子、藤野明夫
編集支援: 仲厚吉 (会長)、各支部長
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)

＜目次＞