

JSSA ニュース

2012. 1. 1 No. 142

【発行】システム監査学会 <http://www.sysaudit.gr.jp>

—*— 今号の記事 —*—

- 1.年頭挨拶「2012年に期待すること」・・・ 1
- 2.<報告>設立 25 周年記念第 24 回公開シンポジウム・・・ 2
- 3.研究会のページ・・・ 3
- ・第 4 回定例研究会報告

- 4.FISA 主催「システム監査講演会」参加報告・・・ 4
- 5.お知らせ/編集後記・・・ 5



システム監査学会 会長 松尾 明

会員の皆様、新年あけましておめでとうございます。

今年から陰の 50 年から陽の 50 年に転換するといわれていますが、見える化が進み、アラブの春にみられるように世界的に ICT の技術を用いた知識・知恵(見識)の共有が急速に進む情報過多の時代の中で、知恵を総動員して胆識(鑑識眼)につなげて行動していく競争の時代に入ったと思われます。世界中が共通のスタートラインにならび始める中で、皆様の知恵を総動員して強い日本の ICT 基盤を作り上げ、活用し胆識にしていけることを支援できるシステム監査学会であればと祈念しております。

現在、辰年にあやかりシステム監査学会の隆盛の次の 25 年間になればと思い、中期・年度計画を理事の方々のお力をお借りして作成しています。その中でいくつかの考え方のメッセージを皆様と共有することで進めています。そのいくつかを紹介します。

1.COSO-ERM

まず、わが国の金融機関にみられるように世界的な内部統制の考え方は、COSO から COSO-ERM にシフトしてきていることです。COSO は、モニタリングを上位にすえ、PDCA を業務執行においてコントロールとして回すものであり、製造業の TQC ではコントロールは受け入れられていましたが、金融業の金融検査マニュアル対応で COSO が認知され、J-SOX で企業にモニタリングの言葉がやっと認知されました。社会的には皮肉なことに福島第一原子力発電所の事故で広くモニタリングは認知されました。

COSO-ERM では、内部統制の目的を、COSO の業務の有効性と効率性、コンプライアンス、財務報告の信

頼性の 3 つの目的の中の財務報告を経営報告に変更し、さらに戦略を 1 つ追加しました。

構成要素に目的設定と事象認識を追加し、戦略・ガバナンスを担当する経営者、取締役会をとりこみ、リスク管理では、リスク評価をリスク評価・リスク対応に分割・詳細化しています。経営目的のために積極的に受容するリスク選好をいれていることにも注目する必要があります。単純化していえば、企業価値を高める戦略を上位層だけでなく COSO の対象とする業務執行の下位業務層にまでモニタリングを活用しながら、価値とこれを阻害するリスクの管理を求め価値を高めようとするものです。

2.オープン ICT 技術の職・個多様利用への対応

クラウドコンピューティング、スマートフォン、SNS 対応、組込みソフト、ライフラインの運用システムなどで技術標準が公開されている UNIX、LINUX などのオープン技術の利用が主流になり始めています。

これらの技術は、より個人の最終利用者が直接的に情報を利用し、企業組織業務と個人の利用の境が明確でないまま、多様な形で利用を支援し始めています。

これらの技術をどのように企画、導入、運用していくのかは、これからの社会、企業、個人にとって大きな課題です。この場合に一番大切なのは、各業務担当の利用者が業務を見据えて、情報・データを把握・分析できる能力(ケイパビリティ)であり、それを前提とできる訓練が行われるようにすることが重要です。

オープン ICT 技術に対応するために、プロセスオーナー、ICT 担当部門、ベンダサイドに何が期待されているかをシステム監理基準、監査基準の中に取り込んでいく必要があります。

3.システム監査の対象とする範囲と判断規準の見直し

システム監査は、IT を核として検討されてきましたが、COSO-ERM の対応やオープン技術活用の対応を考えると、対象とする組織・業務の範囲が多様で、継続的に変化していくものと考えられます。これは、クラウドコンピューティング、SNS の利用などで協業・共同事業を行うなどの参入、撤退が容易にできるため、ビジネスモデル、ビジネスプロセスの範囲を把握してシステム監査の範囲を明確にする必要があります。

また、評価や助言の判断基準もとすれば、セキュリティやインテグリティにポイントを当てていましたが、ここで普遍的なものに再整理する必要があるように思われます。

COSO-ERM の経營業務の有効性・効率性、経営報告情報の信頼性、コンプライアンス、戦略を財務諸表監査のフレームを離れたところでも練り上げていく必要があります。

エンタープライズアーキテクチャで先行されている企業では、ガバナンスの対象として経營業務の有効性に品質(Q)と納期(T)を、効率性にコスト(C)をいれてKPIを検討しています。

経営報告情報の信頼性については、KPI 以外に KRI などのリスク管理を織り込むだけでなく、あたり前品質としてのインテグリティをディペンダビリティとして拡充して検討する動きがあります。具体的な KPI、KGI などのパフォーマンス測定のみジャメント値などを知恵として整理し、データベース化することで胆識に高めることが期待されています。これはリスク管理の業務執行レベルのモニタリングを動かすための重要な課題であると思われま

会員の皆様がたの知恵もお借りして、中期計画を充実させていきたいと思います。ご支援のほどよろしくお願いいたします。

<報告>



情報化月間参加行事

システム監査学会設立25周年記念 第24回公開シンポジウム

想定外脆弱性時代のシステム監査

大阪にて開催

システム監査学会設立 25 周年記念第 24 回公開シンポジウムが、2011 年 11 月 12 日(土)、大阪成蹊大学相川キャンパス(大阪市淀川区)において、統一論題「想定外脆弱性時代のシステム監査」と題し、開催された。

本大会の参加者は、学会員、会員外、および招待者を合わせて 100 名を超え、参加率はほぼ 100%という盛況な開催となった。

午前の基調講演では、(株)神戸製鋼所顧問(元代表取締役副社長、鉄鋼事業部門長)光武紀芳氏に「想定外脆弱性時代の経営－阪神大震災から学ぶ教訓と対応－」というテーマでご講演いただいた。

近年、大手銀行のシステム障害や国際的サイバー犯罪、東日本大震災と原子力発電所事故など、多くの想定外の事故が多発した。光武氏からは、阪神大震災での神戸製鋼所の危機事態で、どのように修復したかの経験を教訓に、「組織力」とそこに働く「仲間たちに培われた力」が大切であることを改めてご提示いただいた。

午後からの研究発表では、「想定外脆弱性」と「システム監査関連」の 2 セッションに分かれて、大学関係者(教員、大学院生)や企業関係者など、計 11 件の多彩な研究発表が行われた。

「想定外脆弱性」のセッションでは、クラウドシステムの概念や利便性、ネット家電のセキュリティなど、システム監査の技術に関する新時代の課題をテーマとした発表が行われた。また、「システム監査関連」のセッションでは、IT ガバナンスや自治体システムなど、本会の中核となる知識や経験をテーマに、システム監査のあ



基調講演(神戸製鋼所 顧問 光武紀芳氏)

り方の研究発表が行われた。各セッションとも白熱した討論が行われ、大変意義のある研究発表であった。

全プログラム終了後には、大阪成蹊大学内にあるレセプションルームで懇親会が行われ、約 50 名が参加した。はじめに大阪成蹊学園理事長・大学学長の石井茂氏より、大阪成蹊大学における伝統あるシステム監査学会の大会開催に対するお礼が述べられ、また、会員同士では、発表時間で十分に満たされなかった問題について話し合いがなされるなど、活発な情報交換が行われる大変盛り上がった懇親会となった。



懇親会風景

最後に、本会の松尾明会長から、今回の公開シンポジウムでの成功を高く評価され、関係者にお礼の言葉を述べられた。

本大会に向けて多くの関連学会・団体・組織からご後援・ご協賛を受けました。そして、ご参加いただいた皆様には厚く御礼申し上げます。

大会実行委員会

実行委員長 松田 貴典 (大阪成蹊大学)

事務局 小倉 哲也 (大阪成蹊大学)

研究会のページ

<2011 年度第4回定例研究会>

日時:2011年10月13日(木) 18:00~20:00

テーマ:情報セキュリティ2011の概要

発表者:内閣官房情報セキュリティセンター
参事官補佐(基本戦略策定グループ)
伊貝 耕氏

参加者:35名

1. 情報セキュリティ先進国の実現に向けて

近年は、コンピュータ/インターネットが普及し、情報システムが経済社会生活に深く根ざしている。情報システムへの依存度が高まっていくにつれ、止まってしまった時の影響も大きくなっている。国民の生活に影響が出ないようにすることが政府としての役割である。

2000年1月に各省庁のHPが改ざんされたことをきっかけに、2000年2月に政府機関を対象とする内閣官房情報セキュリティ対策推進室を設置した。2005年4月には、活動範囲を国民や一般企業など国内全体に広げ、内閣官房情報セキュリティセンター(NISC)を設置した。また、3か年の情報セキュリティ基本計画を策定し、現在は、第2次情報セキュリティ基本計画を包含した「国民を守る情報セキュリティ戦略」の中で、大規模なサイバー攻撃事案等の脅威の拡大、急速な技術革新の進展、社会経済活動の情報通信技術への依存度の増大、グローバル化の進展などの課題に取り組んでいる。

2. 情報セキュリティ政策のフレームワーク

複雑化・高度化する情報セキュリティ事案について、NISCが各省庁や海外機関、重要インフラ企業、セキュリティ関係企業等のハブとなり、官民連携の取組みを行っている。

主な活動は以下の3点である。

- ①政府機関統一基準等により、政府機関の情報セキュリティを確保

- ②重要インフラ(情報通信、金融、電力など)10分野における安全基準の整備等、重要インフラ行動計画に基づく官民連携による重要インフラ防護

- ③一般企業・個人に向けた情報セキュリティの普及・啓発活動

3. 政府機関の取組み

「政府機関の情報セキュリティ対策のための統一基準」を策定し、政府全体の情報セキュリティ水準の向上を図っている。各政府機関は本基準を踏まえて対策を実施し、NISCが対策実施状況の検査・評価を実施することによってPDCAサイクルを回している。

大規模なサイバー攻撃事案等の脅威が現実化しており、情報セキュリティ問題が起こることを前提とした取組みになってきている。政府機関において標的型不審メールを模擬したメールを12政府機関の約5万名に対して送付し、模擬メールの中の添付ファイルを開封するかどうかといった訓練も実施した。

外部からのサイバー攻撃などの情報セキュリティ問題に対して、政府機関の緊急対応能力強化を図るために、2008年4月から情報収集分析システム(GSOC)の運用を開始し、政府機関の情報システムの24時間監視や、不正プログラムの情報収集および分析などを行っている。

4. 重要インフラ企業の情報セキュリティ対策

情報通信、金融、電力など10分野の重要インフラ企業とその所管省庁、その他関係機関をNISCによって調整・連携し、安全基準等の整備や情報共有化の体制強化、共通脅威の分析や演習などによって防護対策の向上に努めている。

また、分野横断的な対策についても、2009年2月に設置したセプターカウンシルにより、重要インフラの共助活動の場として、情報の共有や対策の向上を図ることにより、サイバー攻撃などから被害の拡大を防止する体制を構築している。

5. 企業、個人への普及啓発の推進

情報セキュリティの確保に関して、約8割の国民や企業が不安を感じており、スマートフォン等モバイル環境の高度化やクラウドコンピューティングの利用拡大など

利用環境の変化や、高齢者、若年層といったインターネット利用者層の多様化、情報セキュリティ脅威の高度化や多様化による課題も浮かびあがってきている。

政府も情報セキュリティ月間などの活動により、国民の情報セキュリティについての意識向上につながる活動を行っているが、特に情報セキュリティに対して無関心である層へのアプローチが難しく、国民一人ひとりに情報セキュリティ文化を定着させるのはとても大変である。

6. 所感

世の中から交通事故や犯罪がなくならないように、情報セキュリティ事故やサイバー攻撃もなくなることはな

いであろう。まずは、いかに被害を少なくするか、事故前提の対策を重視する必要があるだろう。他方、日本人的思考として、安心を求めるあまり、えてして完全なものを求めがちである。特にインターネットの世界において完全なものはあり得るのだろうか。どこかで割り切り、国民にもリスクテイクをせまる必要があるだろう。どういった方針で、どこまでの対策を実施するか、その辺りのさじ加減は、組織の文化が現れる。

当然ながら、政府主導での情報セキュリティの推進活動が必要であるが、国民も経営者としてのセンスが問われるところである。

(桃澤正和 記)

第6回定例研究会のご案内

【テーマ】「藤沢市におけるIT業務継続計画(BCP)の取り組み」

【講演者】藤沢市 参事 兼 IT 推進課課長 大高 利夫氏

【開催日】2012年1月20日(金)18:00-20:00 (開場 17:45~)

【場所】六本木ファーストビル1階 JIPDEC 第2会議室(東京都港区六本木 1-9-9)

※これまでと会場が異なりますので、ご注意ください。

地図はこちら <http://www.sysaudit.gr.jp/iten.html>

六本木ファーストビルでは来館者の入館チェックを行っていますので、ご協力よろしくお願いします。

【詳細・申込】 <http://www.sysaudit.gr.jp/kenkyukai/2011teirei6.pdf>

《 〃 FISA主催 システム監査講演会 参加報告 〃 》

2011年10月13日に開催された情報システム・ユーザ会連盟(FISA)主催のシステム監査講演会に参加したので、その概要を報告する。

このシステム監査講演会は、毎年10月の情報化月間のイベントの1つとして開催されているもので、今回で第32回を数える歴史のある講演会である。

毎年、システム監査を取り巻くさまざまな話題を取り上げてきており、今回は、とりわけ今年を象徴するテーマをとり上げた講演会となった。

1. ご挨拶

FISA会長の開会の辞に続いて、経済産業省商務情報政策局情報処理振興課高橋課長からご挨拶をいただいた。高橋課長はご挨拶の中で、ビジネス活動の中でのIT利活用の進展が進み、大量データ処理が行われる環境ができあがったが、そうした環境を競争力のあるビジネス創造につなげるためにも、情報セキュリティの確保が重要であり、経済産業省は、そのための施策を強力に推進していく、と表明された。また、参加者の皆様には、この講演会を通して、情報セキュリティ、さらには危機管理についての関心を高めていただきたい、と述べられた。

2. 基調講演

『サイバーセキュリティに関する今後の課題』と題して、

経済産業省商務情報政策局情報セキュリティ政策室産業分析研究官である福田健一氏から、基調講演をいただいた。

今年の半ば頃から、中央省庁や公的団体を狙ったサイバーテロが頻発しており、まさに時期を得たテーマの講演であった。

サイバーテロは今日に始まったことではなく、2000年頃から発生した。しかし、時代とともにその内容が高度化し、また、その影響範囲も広範化してきている。経済産業省ではそうした状況を深刻にとらえ、2010年に「サイバーセキュリティと経済研究会」を立ち上げ、有識者を集めて検討を行い、2011年7月に中間とりまとめを行った。中間とりまとめでは、情報セキュリティ政策を取り巻く環境の変化と現状認識を整理した後、新しい3つの政策を提言した。その3つとは、①標的型サイバー攻撃への対応、②制御システムの安全性確保、③情報セキュリティ人材の育成、であり、それぞれについて実現に向けた工程表を作り取組みを進めている。また、研究会ではその他の政策分野についての言及も行っており、今後の対応を検討している。

3. 講演

『ERMを活用した危機管理体制の強化』と題して、東京ガス(株)総合企画部副部長の吉野太郎氏から、ご講演をいただいた。

3.11 の東日本大震災発生以降、官民を問わず、危機管理についての関心が急速に高まっており、基調講演と同様、今年を象徴するテーマの講演であった。

該社はわが国を代表する社会インフラ企業であり、その社会的使命の大きさを背景に、危機管理および事業継続計画(BCP)については、全社的経営課題としてとられ、対応を行ってきた。3.11 を機に、それまでの危機管理体制・BCP の見直しを行った。大地震に代表される災害対応についても、3.11 の反省も踏まえて見直しを行った。

該社の危機管理・BCP のベースには全社レベルでのリスク管理(ERM)があり、その中にはERMの遂行状況に対する内部監査も組み込まれている。

4. パネルディスカッション

講演会の最後のプログラムは、『システム監査は危機管理に対していかに貢献できるのか?』をテーマにしたパネルディスカッションであった。

パネラーは、先に講演された吉野氏、日経コンピュータ誌編集記者の福田崇男氏、慶応義塾大学特別招聘教授で GTE(株)常勤監査役の榎木千昭氏、日産自動車(株)グローバル内部監査室課長の池田晋氏の4氏、コーディネータは東洋大学総合情報学部教授の島田祐次氏であった。パネラーの4氏は、榎木氏がリスクマネジメント・危機管理の学術的専門家、福田氏が3.11以降のシステムリスクについて取材・情報発信を行っ

てきたジャーナリスト、吉野氏がユーザ企業のリスクマネジメント・危機管理の推進者、池田氏がリスクマネジメント・危機管理に対する内部監査推進者という立場であった。

最初に、4人のパネラーからテーマに沿った発表が行われた。それぞれ、ご自分の活動分野におけるテーマと関連した話、3.11 が及ぼした影響などについて発表された。

その後、会場の参加者から事前に提示された質問に答える形で、島田氏のコーディネートの下、活発なパネルディスカッションが行われた。

3.11 以降、危機管理・BCP の重要性に対する意識は、多くの分野で高まっている。危機管理・BCP の策定に挑戦する企業、見直しに取り組む企業が、どのような姿勢で、またどのような点に注意して取り組めばよいか、大いに参考になる討議であった。また、危機管理・BCP を実効性のあるものにしていくために、客観的視点からの評価、検証、助言、すなわち監査が大いに貢献をする、システム監査人が貢献しなければならないという話も説得力があった。特に私が印象に残ったのは、3.11 の検証をしっかりと行い(過去に対する監査)、現状の危機管理・BCP の問題点を明らかにし(現在に対する監査)、これからの危機管理・BCP のあり方を提言する(将来に対する監査)という方向性が必要という島田氏の意見であった。

(小野 修一 記)

◆◇◆お知らせ◆◇◆

一般財団法人日本情報経済社会推進協会(JIPDEC)では、「情報化白書 2012-激動の時代の情報化」の発刊を記念して、大阪で「情報化白書 2012 発刊記念シンポジウム in 大阪-生活情報化とセキュリティ」を開催します。

日時: 2012年2月15日(水) 13:30~17:00 (受付開始 13:00)

場所: [TKP 大阪梅田ビジネスセンター カンファレンスルーム 13A](#)

(大阪府大阪市福島区福島 5-4-21 TKP ゲートタワービル)

参加費: 無料 (会場では、情報化白書の割引販売を予定しています)

定員: 90名(定員になり次第、申込締切)

詳細・申込受付: <http://www.jipdec.or.jp/publications/hakusho/2012/event/index2.html>



2011年は、大震災と原発事故で、日本人が決して忘れることのない年になりました。いずれも“想定外”だと言われています。たしかに、今までの思考からすると“想定外”だったのだと思います。国、自治体、東電、災害や原発の専門家、住民、すべてに“想定”する思考がなかったのだと思います。

今は、大震災からの復興と原発事故の収束が最重要課題ですが、併せて、災害や事故を“想定”する思考の確立も急ぐ必要があります。二度とこのような悲劇を起こさないために。

(小野)

*** JSSA ニュース No.142 ***

発行/システム監査学会

2012.1.1 発行 ©JSSA,2012

編集発行人/松尾 明

編集/小野修一、川辺良和、清水恵子、清水政幸、内藤裕之、福田 健、牧野 豊

<事務局> 〒106-0032 東京都港区六本木 1-9-9 六本木ファーストビル JIPDEC 内

電話 03-5860-7556

※事務所移転により、住所&電話番号が変わりました

問合せ先 <http://www.sysaudit.gr.jp/toiawase/index.html>