特定非営利活動法人
日本システム監査人協会報

2011 年 6 月発行
No 124

No. 124（2011 年 6 月　発行）

会報電子版の記事　目次

めだか　【 データセンタにて思うこと　】　　**投稿**

久しぶりに某企業のデータセンタに入館し、サーバの管理状況等をチェックしてきた。相変わらず、空調音が響く、独特の空間ではある。

さて、そのデータセンタであるが、震災以降、西日本のデータセンタには、企業からサーバを移設したい旨の引合いが多く、需要に応じきれない状況だという。

東日本、特に東京電力管内での今夏の電力不足を見越し、今のうちに、比較的影響が少ない西日本にサーバを移してしまおうという駆け込み需要であろう。

多くの引合いが来ているということは、その全てが特定の地域に根ざした企業ということでもなかろう。いわゆる大企業も多く含まれていることは想像に難くない。

そのこと自体は、BCPの観点から言って誠に結構なことであるのだが、ここで「泥縄」という言葉を思い出した。泥棒を捕まえてから、縄をなうという意味であるが、震災そしてそれに連なる電力不足という現実を目前にして、データセンタの疎開を考えているということに他ならないではないか。

もちろん、東日本にあるデータセンタのバックアップとして、西日本にもデータセンタを置くという趣旨であるならば、大変結構なことなのであるが、東日本のデータセンタを撤収して、文字通り、西日本に移設するつもりであるならば、結局同じことであることは小学生にでもわかる道理である。言うまでもなく、次の災害がどこで起こるかは、神ならぬ身、わかるはずもあるまい。

仕事柄、多くの会社のシステムを拝見してきたが、日本中いや恐らく世界的に見てもその名を知らない人のほうが少ないのではないかと思われる大企業においても、データサーバやドメインコントローラを一箇所または一地域に集中して配置し、バックアップテープすらも、遠隔地に保存しているわけではない企業もさほど珍しくはないのが現状である。

恐るべきことに、ある国際的有名メーカーにおいて、都内2カ所にあるデータセンタを1カ所に統合することすら、真剣に検討していたこともあった。

国際的な企業であればこそ、全世界とまでは行かなくとも、せめて国内各地にでも、二重化三重化してサーバを配置し、万一の災害からデータを守るべきであろうし、コスト的にそこまでは難しいような企業にあっても、せめてバックアップデータはデータセンタから離れた遠隔地に、厳重に預けて保管しておくべきではなかろうか。

今回の事態を受けて、このことに気づく企業が多いことを切に望む。

（S）

（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。　）

特別報告　　**投稿**

■ 東日本大震災を体験して

高橋典子（No.1201）

2011年3月11日14時46分　震度7の東日本大震災が起きました。

会社で仕事中、突然の大きな横揺れが数分続きました。免震ビルの18Fは通常のビルに比べ揺れが長く続きますが、ロッカーは耐震固定されていたため、事務所内の被害はありませんでした。エレベータや電気が止まり、窓の外には高架上に止まっている新幹線や傾いた駐車場のビルが見えました。

夕方、雪がちらつく中、18Fから階段で外に出ると街灯も信号も店の電気も消え、車のライトだけが光っていました。仙台駅も閉鎖され、暗闇の中ヘリコプターの音。異様な感じです。携帯はつながらず、メールも数回に1度しか送信できません。交通機関は一部のバス路線を除いて全面ストップです。

地震直後から4月末の再開直前まで高架の上で止まっていた新幹線

避難所の様子

21時過ぎに家に辿り着くと全てのインフラが使えず、玄関の金魚鉢が倒れ散乱。暗闇の中、とても住める状態ではないと懐中電灯とPCと毛布を家から持ち出し、車で避難所の小学校に家族全員で避難しました。避難所では、石油ストーブの薄明かりの中、ダンボールの上に毛布を敷いて寝ましたが、固い床、寒い室内、とても熟睡できる状態ではありません。（このときが原因で風邪を引きました）

避難所では携帯もつながらず、携帯のバッテリを気にしてワンセグも使えません。日中は家に帰って片づけをしたものの、18時の食事が終わった後は何もすることがありません。ラジオを聞きながら、うたた寝していると、人がたくさんいるにもかかわらず陸の孤島にいる感じがして、だんだん感覚が麻痺していきます。

コンビニやスーパー、ガソリンスタンドも閉鎖。 店の前の長蛇の列は開店しているか開店予定の証拠。地下鉄や電車が止まり、ガソリン不足で自家用車通勤も出来ず、バスは長蛇の列。

自宅は海岸とは遠く岩盤が固いのか家の中は物が散乱し、ドアの開閉がおかしくなりましたが、団地の家々の外見は何事もなかった様に見えました。インフラの復旧も仙台市内では早い方で、3/14に電気、3/19に水道、3/26には大阪ガスの方に都市ガスを開栓して頂きました。

被災したビルの立入り禁止の貼紙（被害状況で黄、赤）

4月7日午後11時32分には震度6強の宮城県沖地震かと思われる余震もありましたが、電気は翌日の夕方には復旧し、水道や都市ガスは止まりませんでした。ただ、仙台市内は場所や建物によっては、3月11日より被害がひどかった地域もありました。

5月の連休からは新幹線も地下鉄も復旧。街も復興してきました。余震は頻繁に起こり、一ケ月以上続いたので、最近は震度4ぐらいでは皆、平然と仕事をしています。

飲み会も地震の話題で盛り上がります。先日、仙台空港方面に行きましたが、以前と景色が一変し、津波の爪痕が残り、ガレキや潰れた車の山、津波で被害のあった家々を見て悲惨な状況を改めて認識しました。

津波で歯抜けになった防風林と潰れた車

ここからは、今後の地震に備えて、皆様への参考情報です。

・まず震災直後は、電気、ガス、水道のインフラは全く使えず、携帯もつながらなくなりました。

・懐中電灯は必須です。

・断水ではトイレの水がまず問題です。風呂の残り湯を使用して凌ぎました。雪をお風呂に入れて溶かし水として使用した人もいたそうで、お風呂の残り湯は直ぐに捨てずに溜めて置くことがお勧めです。給水所に水をもらいにいく水筒やペットボトル、タンクもあると良いですね！

・ガスの復旧はインフラの中では一番遅く、ポットや電磁調理器で何回かお湯を沸かしてお風呂に入りました。カセットコンロも非常に有効です。

・ガソリンスタンドは停電で機械が止まり、給油ができなくなりました。一部のガソリンスタンドが再開した時は長蛇の列。前の晩から並ぶ人も多く、10Lや20L限定での給油。車のガソリンや灯油（まだ寒かったので）は満タンにして置けばよかったと後悔しました。

・食料の確保も課題です。コンビニ以外のほとんどのお店が震災直後閉店しており、何も購入できません。数日後に、日中の時間限定で一部のコンビニやスーパーが営業を始めましたが、2～3時間待ちは普通で、並んだ挙げ句に購入できる商品は1人10品。購入できる商品も牛乳や納豆等の日配品や生鮮品は無く、野菜やカップラーメンやそば等の種類限定です。カップラーメンやレトルトカレー等の非常食も用意して置くべきでした。

・小さなお子さんがいる家庭では、紙おむつ、粉ミルクの調達に苦労されていました。

・オール電化の家庭でも、給湯器が壊れた家が多かったとのこと。
（地震の揺れにともない、水が揺れるので壊れやすいそうです）

・タイムリーに情報を得る唯一の手段が小さなラジオで、私が使っていたラジオは電池の持ちもよく、単4電池1本で3日間、聞く事ができました。AMは電波ノイズがひどく、ラジオからTVの1chの音声をずっとイヤホンで聞いて状況を把握しました。

震災後の仙台駅
（工事中のシートが全面に）

・新聞は河北新報が翌日には号外が出て、その後も毎日、地域のお店の開店情報や自治体の情報、被災者の情報等がこまめに掲載され、さすが地元誌です。

・停電時に携帯のバッテリが課題で、今はやりのスマートフォン（私はiphone）はバッテリがすぐ無くなって使えません。私は、車のシガーライターからACアダプタの変換器を使ってPCを充電し、そのPCから家族全員の携帯をUSBで充電していました。避難所では、手回しの携帯充電器が結構有効だったとの話なので一家に一台は用意しておくことをおすすめします。

・全国の色々な方からご支援のメールを頂きました。ありがとうございました。twitterやFacebook、有効な震災サイトを教えて頂きましたが、地震直後の3日程度は、電波状態が非常に悪く、メールが何回かに1回、遅延しながらやっと送受信できる程度でサイトを見る事はとてもできませんでした。携帯のつながり具合は、docomo, au→softbank→willcomで、私は野生の感!?が働いたのか震災当日の午前中にdocomoに行って、たまたま契約したモバイルWifiのおかげで震災後4～5日でインターネット接続ができました。

今回の震災直後から、全国の方々から激励のメールやお電話を数多くいただき、皆様のお心遣い、ありがたさを実感しました。本当にありがとうございました。東北支部も6月から活動を再開します。システム監査人として何かできることは無いか、東北支部メンバーと考えながら行動していきたいと思います。今後とも、ご支援をよろしくお願いいたします。　以上

研究会、セミナー開催報告、支部報告

■ 2011 年システム監査基準研究会の活動計画と状況報告

松枝　憲司（No.555）
kmatsueda＠nifty.com

（報告の概要）

これまで 3 年間は研究会員が持ち寄ったテーマについて、その検討過程の成果物を月 1 回の研究会の場で検討する方法で進めてきました。そして研究会内のレビューが済んだ成果物については会員向けに公開し、パブリックコメントを求めてその結果を反映させたうえで、一般公開する手順で進めてきました。

2011 年度の研究テーマとして挙がっているのは、下記の項目になります。

しかしながら、今年の 3 月以降は「IT Audit の ISO 化への対応」が SAAJ にとっての最優先事項となったため、本研究会の中に「ISO-WG」を立ち上げて、ISO の国際会議への対応等を月に 2 回程度実施しております。

（報告内容）

1．2011年の主な研究テーマ

(1)Web システムにおける監査のポイント(開発・利用)【基準研内レビュー済み】
　①「Web システム開発管理における監査の視点」
　②「Web システム開発管理におけるシステム管理基準活用のポイント
(2)PMにおける監査のポイント　　【原案作成着手】
　①PMBOK と管理基準の対応及び原案作成
(3)BCMにおける監査のポイント　　【原案作成中】
　①「事業継続管理における監査のポイント」
　②「事業継続管理における監査のポイント一覧」
(4)システム監査の視点の整理(特に有効性)　【検討中】
(5)IT Audit の ISO 化への対応について　【国際会議向け原案作成支援等】
(6)JASA との連携　　【検討中】

2．出版関係

既にご案内の通り、本研究会が主体となって執筆・編集しました2冊の実践マニュアルが、森北出版より装いも新たに再出版することが出来ました。

「情報システム監査実践マニュアル第2版」(赤本)
「J-SOX 対応 IT 統制監査実践マニュアル」(黄本)

なおこの2冊の印税については、編著者のご了解のもとに全額を「IT Audit の ISO 化への対応」の費用として充てることとしております。

本研究会は門戸を開いておりますので、基準研以外の方でご興味のある方は、是非ご連絡ください。

以上

■ 第 161 回月例研究会受講報告

中山 孝明(№1143)

・ テーマ　　第 17 回企業IT動向調査 2011(2010 年度調査)
・ 日時、場所　2011 年 4 月 26 日(火)18:30～20:30、御茶ノ水　総評会館
・ 講師　　社団法人 日本情報システム・ユーザー協会(JUAS) 常務理事 原田 俊彦氏

【 テーマ 】

本テーマである「企業のIT動向の調査」は経産省の委託を受けて毎年度行われているもので、今回の講演はその調査結果の分析内容を説明いただいたものです。今回の調査と分析は 2010/11 から 2011/2 にかけて実施され 2011/3 にプレスリリースされています。なお、当日配布資料の元データが JUAS のホームページからダウンロードできますので、講演内容をさらに深掘り研究したい方や欠席された方は参考にされるといいと思います。

この企業IT動向調査は JUAS が 1994 年度以降 17 年間継続実施しており、定点観測的な項目と各年度の重点テーマから構成されていますので、経年変化を踏まえた分析など貴重な活動であると認識しています。

月例研究会では昨年も 2009 年度の企業IT動向調査をテーマとして採り上げており、我々システム監査人が IT 動向を把握するうえで価値あるテーマになっていると考えます。

講演で説明された項目は次のとおりです。

1. 回答企業のプロフィール
2. トピックス　①新規テクノロジーの採用、② IT 予算、③情報セキュリティ
3. 重点テーマ　①IT 投資マネジメント、②グローバル IT 戦略
4. IT 人材

幅広い視点の分析、業種別の傾向、年度ごとの変化など多岐にわたる内容で量的にも質的にも濃いものです。その内容を以下に報告いたしますが、報告者の理解レベルの限界で概略報告にとどまっております。JUAS のホームページからダウンロードできる資料には調査方法、分析結果と説明、図表等が詳細に盛り込まれていますので参考にしてください。

【 回答企業のプロフィール 】

- アンケート調査は、1,144 社の IT 部門と 1,075 社の経営企画部門から有効回答
- インタビュー調査は、45 社の IT 部門長から回答
- 回答企業を 7 つの業種グループ(建設・土木、素材製造、機械器具製造、商社流通、金融、重要インフラ、サービス)に分類し業種特性を踏まえて分析
- 回答企業を従業員数でみると、全体では大企業(1,000 人以上)、中堅企業(300 人以上)、中小企業(300 人未満)が各 1/3 程度となっているが、業種別では「商社・流通」と「サービス」は中小企業が 4 割強

【 トピックス ①新規テクノロジーの採用 】

- 仮想化、OSS(オープンソースソフトウエア)の OS とミドルウェア、BI(ビジネスインテリジェンス)それぞれが導入拡大中。BI は超大企業(売上高 1 兆円以上)では 2/3 が導入済
- EA(エンタープライズアーキテクチャー)、SOA(サービス指向アーキテクチャー)はいまだ対応途上
- パブリック・クラウドの SaaS は普及が堅調で、パブリック・クラウドの中では最も早く成熟と予想。超大企業(売上高 1

兆円以上）では半数が SaaS を活用済

- パブリック・クラウドの IaaS と PaaS は様子見姿勢だが、導入検討中の企業が約 30%（09 年度比倍増）
- スマートフォン、タブレットデバイスは導入済み 10%前後で、検討中は 40%弱
- クラウド・コンピューティングの定義・本質を理解しているIT部門は全体の 3/4
- クラウドによるIT部門の業務・責任の変化を 7 割が認識
- クラウド導入に慎重姿勢のIT部門が 2/3。セキュリティ対策を懸念する指摘が最も多い

【 トピックス ② IT 予算 】

- IT予算は 2010 年度が底。2011 年度はプラスに転じるが力は弱い。リーマンショック以降 1/2 の企業がIT予算を削減する一方 1/4 の企業は積極的なIT投資を計画
- 売上高に占めるIT予算は金融が 3%台と突出。全体では 09 年度は 1．13%、10 年度は 1．18%
- 売上高に占めるIT予算比率は 2000 年度からの 10 年間で 1/2 に低下。要因はハードウェア技術の進歩、システム寿命の長期化、仮想化等のシステム技術変化、IT関係者のコストダウン努力
- 国際比較では、IT予算比率は北米の 1/4、欧州・アジアパシフィックの 1/3、ラテンアメリカの半分以下
- 保守運用費は伸び率が初めてマイナス 1%となった（歴史的出来事）

【 トピックス ③情報セキュリティ 】

- 第三者評価の利用状況（自社に対する評価）は、システム監査の利用は全体で 43%となっており、業種別では金融が 77%、次いで商社・流通が 46%。情報セキュリティ監査の利用は全体で 32%となっており、業種別では金融が 63%、次いで重要インフラが 35%
- 第三者評価の利用状況（自社に対する評価）でプライバシーマークと ISMS 適合性評価は、サービス業の利用が高く特にプライバシーマークの利用は 2 位の重要インフラの 3.5 倍
- 委託先の評価としては、プライバシーマークの利用が 27%、ISMS 適合性評価の利用が 23%、情報セキュリティ監査の利用が 19%。利用している理由は、委託先の情報セキュリティレベルの確認と情報セキュリティ事故防止が圧倒的に多い
- 自社及び委託先に対して情報セキュリティの第三者評価を利用しない理由は、「必要性がよくわからない」と「社内負荷が大きい」が多い

【 重点テーマ ① IT 投資マネジメント 】

- IT 投資で解決したい中期的な経営課題は、リアルタイム経営（迅速な業績把握、情報把握）と業務プロセスの効率化（省力化、コスト削減）が 2 本柱
- 大企業は、グローバル化への対応と IT 開発・運用のコスト削減を重視
- IT 投資の中期的な重点分野は、1 位：経営情報・管理会計、2 位：生産・在庫管理、3 位：販売管理
- 売上規模が大きい企業ほど経営戦略と IT 投資の整合性がある。これは CIO の有無の傾向と一致
- IT 投資効果の事前評価を常に実施している企業は 4 割で、事後評価を実施している企業は 1 割
- IT 投資効果の評価に利用している指標は、情報システムの運用・費用に関する指標や業務プロセスの変革に関する指標が多い。財務指標やバランス・スコアカードの利用は少ない

【 重点テーマ ②グローバル IT 戦略 】

- 全業種でグローバル化への対応が IT 戦略の重点課題に浮上。特に素材製造、機械器具製造が目立つ

- IT 拠点のグローバル展開は、運用拠点について海外事業拠点に分散している企業が少なくない
- グローバルでの IT 資産の標準化は、現状では海外事業拠点に任せている企業が多数派。グローバルの標準化を進めようとする企業も多い
- IT マネジメントのグローバルな組織化は、将来的には本社 IT 部門で管理の意向。IT 資産別では会計・インフラは集中管理、人事総務・販売は分散管理という傾向
- 回答企業の自由記入欄には、海外拠点の人材不足、多言語への対応、コミュニケーション、日本国内基準の展開、ビジネス慣行の違い、ベンダーとの連携などの問題点や障壁に関する声が出ている

【 IT 人材 】

本項目は配布資料にはなかったが講師からスライドを用いて 30 分程度説明された。残念ながら報告者の席からはスライドの小さな文字は読み取れず内容の理解は困難でした。

本報告をするにあたって、JUAS ホームページの資料をもとにして講師が説明したであろう項目名を以下にリストアップすることとします（スミマセン）。

- 事業部門と IT 部門の要員構成、情報子会社の有無と IT 要員数の傾向、IT 要員の経歴の動向、IT 要員に求められる能力と充足度、IT 部門への期待、CIO・IT 部門長の経歴など
-

・・・・・講演の概略は以上のとおりです・・・・・

＜質疑応答＞

1、 東日本大震災によりバックアップセンターの設置状況にも関心が集まっているが JUAS で実態把握をしているかとの質問があり、実態把握は今後の JUAS 活動の対象になるだろうとの説明があった。

2、 IT 人材のスキル向上策についての JUAS の取り組み状況の質問があり、JUAS の研修事業（セミナー）など各種活動のなかで取り組んでいるとの説明があった。

＜報告者感想＞

企業 IT 動向の全般にかかわる分析結果の詳細説明は大変興味を引くものでした。報告者はシステム監査を「経営トップから現場の担当者の方まで、各層の業務や職責に応じた課題を解決に導く」と位置づけている（自 HP）こともあり、今回の内容は IT 全般に関して企業や担当者の認識と実態を知る貴重な材料となりました。自分なりの分析もしてみたいと思っています。

講演資料には「情報セキュリティとシステム監査」に関する項目が設けられ講師から説明がありましたが、JUAS のホームページからダウンロードする資料にはない項目でした。講師が月例研究会用に追加されたものと推察し配慮に感謝したいと思います。

講演資料にない項目の説明が 30 分程あった点は、例えば JUAS のホームページから資料をダウンロードして持参してほしい旨を月例研究会の事務局からメール配信できたならば受講者の理解の助けになった部分もあったのではないかなど、と工夫の余地を感じました。

以上

■九州支部　特別講演会報告　：2011 年 3 月 24 日 18:30-20:30／天神パークビル（福岡市）

中溝　統明

第153回月例研究会で講師いただいた株式会社東京証券取引所の鈴木義伯様に福岡でご講演を頂きました。本講演は昨年 12 月に開催予定でしたが、諸事情で延期となり、また東日本災害の発生直後で開催が危ぶまれる状況でもありましたが、鈴木様のご好意により無事開催することとができました。九州支部で初めて試みた講演会に20名の参加をいただき盛会となりました。以下、講演内容について報告をさせていただきます。

テーマ:「東証新売買システム(arrowhead)の開発とその後の状況
（ 開発プロセスの改善と新しいビジネスモデル出現 ）」
講師 :株式会社東京証券取引所
専務取締役・最高情報責任者(CIO) 鈴木 義伯 氏

鈴木氏は、東京証券取引所の CIO として新株式売買システムの開発を推進・統括された立場からテーマについて講演されました。

＜講演内容＞

1． arrowhead 開発の背景

取引所の評価項目の一つにITの高速性が追加された。そこには、ICT構成要素(SSD、CPU、メモリ等)の処理能力、記憶容量、回線速度において飛躍的な性能向上があり、かつ市場に求められるニーズがある。ニーズとは、注文・約定処理の高速化、取引注文の小口化、及び取引件数の急増である。

開発にあたり海外調査も踏まえて arrowhead 開発の基本コンセプトがまとめられた。それは、高性能、信頼性、拡張性において世界最高水準の機能を有する現物(株式、CB等)の立会取引に係わる次世代システムとするというものである。

2． Arrowhead 稼動後の状況

平成22年1月4日から本稼動した。付き合せをリアルタイムに変更したことによりTICK回数が増加している。また、注文受付レスポンスは目標値である10ミリ秒を大幅に下回る平均2ミリ秒で安定し、情報配信件数は従来の4倍以上に増加している。

さらに、コロケーションサービス(新しいビジネスモデル出現)の占める注文件数・売買代金は市場シェアを拡大している。

稼動品質においては、稼動当初に多少発生したが軽微なもので、システム全体として安定傾向にある。金融業界のバグ密度と比較しても、大変良好な品質状態である。

3． プロセス改善への取組み

従来の開発プロセスにない改善策を取入れた。これらは皆様が取組まれる開発プロジェクトの参考となり大いに役立つ内容である。

(1)開発フェーズに踏み込んだ発注者責任の明確化、(2)上流から設計とテスト項目作成の並行作業と前工程の品質は次工程で確保するフィードバックW字モデル、(3)要件定義起因のバグ削減にむけた要件トレース・各工程別要件トレーサビリティ、(4)全体リスクを低減するために、リスクスコア算出・リスク低減計画・リスク状況把握によるリスク管理とPDCAサイクル、(5)工程毎／サブシステム毎の要件変更・品質目標の実績(目標差異)評価

4． 非機能要件への取組み

arrowhead 開発の基本コンセプトを達成するために、非機能要件をシステム方式で追及した。高性能、拡張性、信頼性別に目的にあったマネジメント計画を立案し工程別作業を徹底することで実装に辿りついた。成果は次のとお

り。

(1)ミリレベルの応答(2)短期間でキャパシテイ拡張(3)信頼度 99.999%達成

5.　arrowhead 成功の鍵

成功の鍵の一つには、システムトラブルでの信用回復が喫緊であり世界の取引所に匹敵するシステムを求める危機意識があった。さらに、経営責任者によるプロジェクト推進体制を築き、発注者責任を明確にして、上流工程完璧主義に徹し、質を追求した。

6.　今後に向けた取組み

東証は今後も魅力ある市場作りに取組む。(1)arrowhead の更なる高速化、利便性向上、(2)arrowhead(現物)、Tdex+(デリバティブ)で、すべての市場に高速アクセス、(3)arrowhead の販売

＜所感＞

鈴木様のシステム開発に対する熱意がこぢんまりした会場に充満し、参加の皆さんとともに大変興味深く聞かせていただきました。

まず、打ち解けた喋りの中に潜む CIO の迫力に驚きました。また、プレジデントレビューやプロジェクトの足並み合わせ等による責任ある仕事のやり方、技術者は IT を社会の重要な仕組みに組み込む役割を担う。これらを企画開発プロセスのシステム監査視点に取入れるべきと感じました。

さらに、取引所のビジネス環境は年々変化しており、マーケットの要求に応えるために世界最高水準を狙われていることを認識しました。これより、取引所システムの動向に関心が高まりました。

以上

■近畿支部　第126回定例研究会報告　：　2011 年 5 月 21 日

小河裕一（No1710）

テーマ　国際会計基準(IFRS)のシステム対応の落とし穴　～あなたの知らない意外な盲点～

講師：株式会社アロウズコンサルティング社　マネージャー　田淵隆明氏

日時：2011 年 5 月 21 日　18：30～20：30

場所：大阪大学中之島センター　2階　講義室1

1．講演概要

・(制御系以外の)ソフトウェアは PL 法対象にならない。そのため、ソフトウェアの不備や仕様不足によって誤った会計報告を提出した場合、ユーザである報告者にペナルティが課せられる。

・3月決算である企業の場合、2015/3 に IFRS 移行しなくてはならないため、2013/3 には新システムで IFRS にのっとった形での BS の作成を行わなくてはならない。（報告は2年間分のため）

1年間トライアルを行うと考えると 2012/3 にはシステム導入を完了させて運用を始めないといけない。

・IFRS と GAAP の両方で開示しなくてはならない期間は 2 重元帳方式も可能だが、大変パワーが必要となるため、個別会計データは現地の GAAP で作成し、組換えデータのみ作成することが望ましい。

・現行の多くの連結会計システムでは「少数株主持分」は一科目に合算されてしまうが、　「連結包括利益計算書」を作成するためには、内訳科目毎に分離して連結処理する必要がある。

・現在、日本では「三分割法（英米法）」と「売り上げ原価対立法（大陸法　IFRS 基準）」が使われているが、IFRS では「大陸法」しか使用されない。

・IFRS において、キャッシュフロー計算書は「直説法へ一本化する」方向で検討されている。→現行の多くの連結会計システムでは「売上原価」(「製造原価」を含む)は一科目に合算されてしまうが、直接法の「連結キャッシュフロー計算書」を作成するためには、内訳科目毎に分離して連結処理する必要がある。

・中国では来年から、事実上、直接法・間接法双方のキャッシュフロー計算書が必要。

・近々、研究開発費が「費用処理」から「無形固定資産」への計上に変わっていく。

→これは、IFRS への一致であるとともに、2005 年以前への回帰でもある。

・ゆとり教育のため、会計に携わっている人でも「複利計算」ができない人もいる。

→しかし、これは改善されつつある。

・今後システムインテグレータの優遇制度復活を求めていくことで、システムの品質向上へ向けた活動に結び付けていく。

2．所感

当日、私は開始直前に会場へ到着したのですが、ほぼ満席状態でした。それだけ IFRS 移行に関する事は皆、重大な関心ごとなのだろうと認識しました。私自身、会計には直接関わっていないため、講演の中で始めて聞く単語も多かったです。

しかし、簡単な例をあげてわかりやすく説明をしていただけたため、IFRS 移行に向けて現行の連結会計システムにはさまざまな問題があることが、大変よくわかりました。

また、システムを作成したり改修するベンダーだけでなく、導入したユーザ、そして導入されたシステムを監査するシステム監査人にいたっても IFRS のしくみのみならず複利計算といった基本的な数学知識を身につけたうえで、今後の対応をしていかなくてはいけないということが、今回の講演で理解することができました。

以上

■ 平成 23 年度 北信越支部総会研究報告

以下のとおり平成23年度 北信越支部総会を開催し研究報告を行いました。

日時:2011年5月7日(土)13:00-17:00　会場:富山国際会議場 206会議室(富山市)

◇研究報告 1

「事業戦略と評価方法について」

森 広志　(No.848)

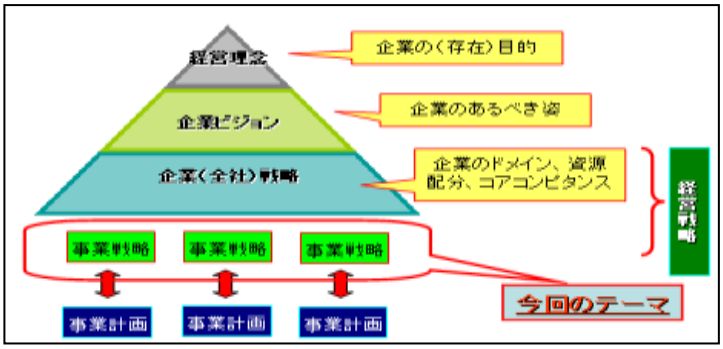
北信越支部のシステム監査研究チームでは、IT経営に関するシステム監査についての研究を行っています。平成21年より2ヵ年間、「IT経営ロードマップ」にある事例研究について、参加者の皆さまと議論をしてきました。今年度は、ビジネスモデル策定や情報戦略策定方法等について、学習と研究に取り組んでゆきたいと思います。

今回は、私の方で、図書「戦略経営バイブル(著者:高橋宏誠)」を読み、戦略的経営について今まで気づかなかった点や重要と思う点をパワーポイントで説明し、皆さまからご意見を受けました。全部は紙面で説明できませんが、以下に抜粋を書きます。

1. テーマの選定理由

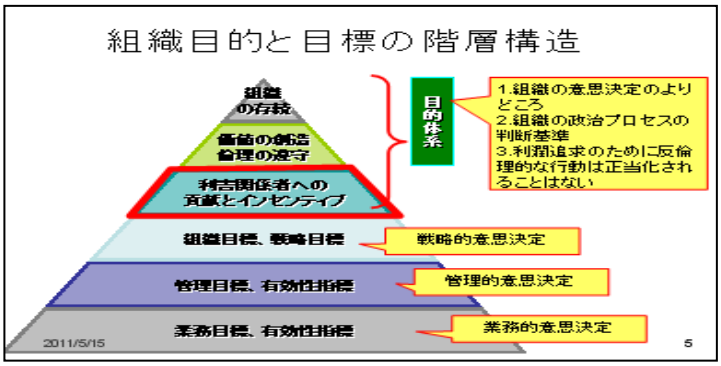
先ず、図1にある「事業戦略」(緑の網掛け部分)をテーマとして選定した理由は、特に、事業戦略の内容や品質が不十分だと、システム監査やITコンサル等を行う場合、その技術が十分あっても、的をえた指摘や提案が困難になると感じたためです。

経営理念や企業ビジョンの把握は、「いわずもがな」ですが今回は「事業戦略」にスポットを当て、あるべき策定方法を検討することとしました。



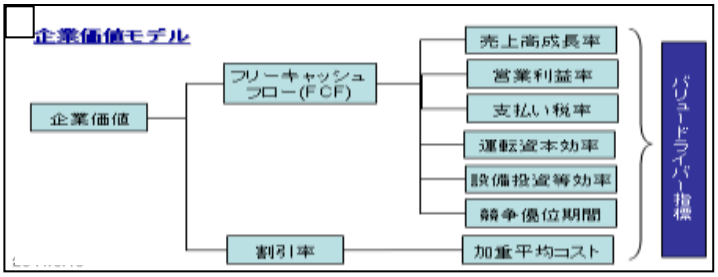
2. ステークホルダーの貢献とインセンティブ

各々のステークホルダーがどのように組織に貢献し、又、組織からインセンティブの提供を受けるかについて、優先順位も含め議論の余地のあるところですが、全社経営のみならず、一事業に於いても、これを整理し、常に心に留めおくことで、価値創造やコンプライアンス順守の基盤を形成する上で、重要であると考えます。



3. 企業価値を向上させるための基本の考え

企業価値創造を確実に実行するため、企業価値モデルを活用しバリュードライバー指標の感度分析により重要なバリュードライバー指標を特定します。この企業価値を左右する重要なバリュードライバーが事業戦略にリンクし、日々の意思決定で従業員が



戦略実行にオーナーシップを持つことにより、戦略ギャップを埋めることが可能となると考えます。

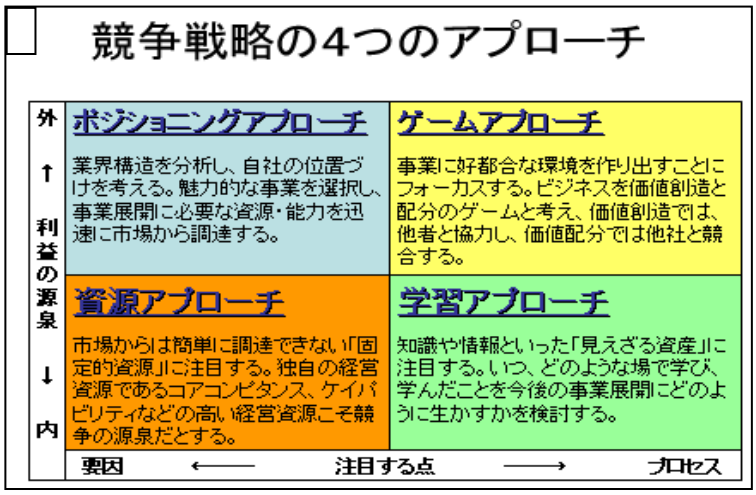
また、3つの事業の基本スタンス(コストリーダシップ、差異化、集中)とバリュードライバーの関連性を検討し企業価値向上対策の重要成功要因、重要成功指標を導出します。

「事業の基本スタンス」と「バリュードライバ」の関係

コストリーダーシップ	バリュードライバ	差異化
・低価格の維持 ・規模の利益を目指したシェア拡大	売上高成長率	・最高価格の請求 ・プレミア顧客の開拓
・規模の利益の追求 ・学習効果を高める仕組の構築 ・調達コストの削減、・固定費削減	営業利益率	・買い手が必要としない部分の費用削減 ・効率的な製品差異化
・資金の最小化 ・債権の早期回収化 ・在庫の圧縮	運転資金	・資金の最小化 ・差異化レベルにあった在庫管理 ・買掛金で最高の条件を引出す
・固定資産の活用 ・生産効率の向上 ・最適価格の資産の取得	設備投資	・最適な生産効率を得る設備の取得 ・最適価格での資産の取得
・最適資本負債比率 ・安価な資金調達	資本コスト	・最適資本負債比率 ・安価な資金調達

4. 競争戦略の4つのアプローチ

企業価値創造を念頭に置き競争戦略を考案しますが、その支援を行う一つに、「競争戦略の4つのアプローチ」があります。縦軸で、利益の源泉を企業体の外あるいは内に求めるか、また横軸で、利益の源泉を、利益を生み出すプロセスと捉えるか、あるいは、要因と捉えるか、という観点から「ポジショニングアプローチ」「資源アプローチ」「ゲームアプローチ」「学習アプローチ」の4つに分けることができます。「ポジショニングアプローチ」



では、業界の中で、自社をどう置付けるかの観点から、成功要因となる資源が自社に不足していれば、社外から迅速に調達し、これにより競争優位の獲得を目指します。

「資源アプローチ」では、競争優位をもたらす独自の経営資源を競争の源泉と考え、具体的な事業内容を設定する前に資源蓄積を行います。このため事業ドメイン見直しなどの将来構想構築などが重要な意義を持ってきます。

(感想)

以前から、経営に役立つシステム監査を模索しており、ＩＴ経営を監査することもその一つかと思っております。そのためには戦略的経営を理解することが重要ですが、どのような企業にも妥当する普遍的な戦略は存在しないといわれています。経営環境、組織特性、戦略における人や組織、企業文化など多様な変数が係わる中で、経営責任者は、最適な競争戦略を自らの洞察力や発想により構築する必要があるからです。しかしながら今回の学習により企業価値創造をバックボーンとし、それを最大化することを主眼に工夫を凝らしてゆけば良いのではないかと考えるようになりました。今後とも皆さまのご意見や感想を賜りながら、研究活動を続けてゆきたいと思います。

以上

◇研究報告 2

「クラウド・コンピューティングの情報セキュリティについて」

宮本 茂明(No.1281)

クラウド・コンピューティングに関する情報セキュリティの現状課題について，IPA『情報セキュリティ白書 2010』，ASPIC『解説クラウド・セキュリティ・ガイダンス』，Cloud Security Alliance「CSA クラウド・セキュリティ・ガイダンス Ver.1.0 日本語版」，経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン 」にそのポイントが分かりやすくまとめられています．

今回は，これらの文献をもとにクラウド・コンピューティングの情報セキュリティについて整理し，その概要を報告しました．

クラウド・コンピューティングには，ビジネス推進上の大きなメリットが期待される一方リスク管理すべき事項も技術面だけでなく，グローバルな法的側面の対応等多岐にわたってきています．

クラウド・コンピューティング導入にあたっては，「CSA クラウド・セキュリティ・ガイダンス」にある『クラウド・コンピューティングの利用により削減されたコストの一部は、事業者のセキュリティ能力の監視の強化、および、継続中の詳細な監査のために支払われるべきである』という考え方をベースに進めることが重要であり，クラウド利用者及びクラウド事業者間の信頼関係を構築する上で，第三者によるシステム監査/情報セキュリティ監査の重要性が増してくると考えます

今後，SAAJ 北信越支部情報セキュリティ監査研究チームとして，今回課題認識した事項の中から深掘りするテーマについて研究していきたいと考えます．

以下に今回の研究報告の概要を示します．

1. クラウド・コンピューティング

- クラウドの定義

NIST(米国　国立標準技術研究所)によるクラウド・コンピューティングの定義は次のようになっている．

「(複数のユーザーにより)共有され、(最適環境を)設定・調整可能なコンピューティング資源に、簡易且つオンデマンド・ベースでネットワークからのアクセスが可能な形態(モデル)のこと。当該コンピューティング資源は、最小限の管理努力やプロバイダーの関与だけで、迅速に提供され、解除される。」

- クラウドの特徴(本質的な特徴)
  - ✓ On Demand and Self Services
  - ✓ Broad Network Access
  - ✓ Resource Pooling
  - ✓ Rapid Elasticity
  - ✓ Measured Services
- クラウドのサービスモデル
  - ✓ SaaS：Software as a Service
  - ✓ PaaS：Platform as a Service
  - ✓ IaaS：Infrastructure as a Service
- クラウドサービスの種類(クラウドのデプロイモデル)
  - ✓ 「プライベートクラウド」

特定のユーザー(企業)が利用することを前提に構築・運用されるクラウドサービス

- ✓ 「パブリッククラウド」
  インターネットを介して不特定多数を対象に提供されるクラウドサービス
- ✓ 「ハイブリッドクラウド」
  パブリック・クラウドと従来システムあるいはプライベートクラウドを組合せ，シームレスに連携させる利用形態

➢ クラウドサービスのメリット

- ✓ 「スケール性」:セキュリティ手段がより安く実装される
- ✓ 「差別化要因」:最関心課題であり、プロバイダとしては、差別化要因としうる
- ✓ 「セキュリティ管理のための標準化されたインターフェース」:
  セキュリティ対策の負担軽減/日々の実行の手間からの開放
- ✓ 「資源の迅速かつ最適なスケール化」:使用した分だけ支払
- ✓ 「監査および証拠収集」:
  仮想化マシーンの利用に応じたフォレンジック・イメージを提供しうる
- ✓ 「初期値およびアップデートの適時の、効果的な適用」:
  ソフトウェア・バージョンアップやアップデートをクラウドサービス事業者に任せることで負担軽減

➢ クラウドサービスのデメリット

- ✓ IT資源と情報資産が集中し共用されているリスク
  一度セキュリティが破られたり事故が起こると，大きな被害となる可能性

2. クラウドにおける脅威

➢ クラウドにおける攻撃パターン

①外部からクラウドへの攻撃
②クラウド環境内部から他のクラウド利用者への攻撃
③クラウドを踏み台とした攻撃
④コンピューティングパワーの悪用（パスワード解析や暗号解読等）
⑤攻撃以外の原因（停電，システム不具合等）でクラウド・サービスが停止/環境への攻撃

➢ Cloud Security Alliance　“Top Threats to Cloud Computing V1.0”では，以下の脅威が報告されている.

- ✓ 「クラウドコンピューティングの不正および犯罪目的の利用」
- ✓ 「安全ではないインターフェースおよびAPI」
- ✓ 「悪意ある内部者」
- ✓ 「共有技術（Shared Technology）問題」
- ✓ 「データ消失または漏えい」
- ✓ 「アカウントもしくはサービスのハイジャック」
- ✓ 「未知のリスクのプロフィール」

➢ ENISA（欧州ネットワーク情報セキュリティ庁）報告書 では，具体的な利用にさいしての脅威として以下が報告されている.

- ✓ 「ガバナンスの消失」

- ✓ 「ロックイン」
- ✓ 「障害の分離」
- ✓ 「コンプライアンス リスク」
- ✓ 「マネージメントのインターフェイスの毀損」
- ✓ 「データ保護」
- ✓ 「データ消去の不完全」
- ✓ 「悪意ある内部者」
- ✓ 「その他」

3. クラウドにおけるセキュリティ上の課題

3.1 仮想化技術に関連するセキュリティ課題

- 仮想化技術は、新しい技術であり、いまだ発展途上
- 技術的な問題点
  - (1)仮想化自体が、サイドチャンネル攻撃の危険を引き起こす可能性がある
  - (2)仮想マシンモニタを乗っ取られると被害が甚大である
  - (3)仮想マシン自体の脆弱性をついた攻撃が可能である
  - (4)物理的なエラーが攻撃のきっかけとなりうる
  - (5)キャッシュ共有・メモリの覗き見等の攻撃が可能である
- 仮想化技術ベンダ等からの脆弱性に関する情報の入手
- 攻撃を防ぐ隔離技術の研究・開発
  - ✓利害のある処理を同時に実行しない
  - ✓物理的にサーバを分離する等の実行ポリシーを履行できる技術

3.2 データ保全・通信上の安全に関する課題

- クラウド上で利用が安心してデータを扱うために「消失・漏えい・消去・改ざん」の課題を解決し，データを安全に管理する必要がある
- ネットワークを利用することによる課題
  - ✓ 漏えいクラウド事業者のセキュリティレベルおよびネットワーク途上におけるセキュリティの問題がそのまま問われることになる
    - (1)機密性(データの漏えい、通信の傍受)
    - (2)完全性(無権限改ざん、通信途上での改変)
    - (3)可用性(物理的利用不可能、DoS 攻撃)
  - ✓ 重要なデータ等は，利用者でも何らかの管理策をとっておくことが望ましい
  - ✓ データ漏えいや消去に関しては，データ漏えいを想定しデータを暗号化する等の対策を行う必要がある

3.3 ユーザ認証や機器認証に関連する課題

3.3.1 アイデンティティ管理

- アイデンティティ・プロビジョニング

- ✓ 利用しうる状態(プロビジョニングーユーザに対する権限の割付け)であるか利用し得ない状態(デ プロビジョニングーユーザに割付けた権限の解除)であるかを安全に、かつ時宜に、管理するという問題に対処しなければならない
- ✓ 利用組織において、いままでのアクセス管理をクラウドサービスの利用にまでに拡張しなければならない

➢ 認証
- ✓ ユーザの認証を、信頼できる方法で管理することが重要
  - ▫ クレデンシャル情報の管理
  - ▫ 認証処理の委譲
  - ▫ クラウド全般のトラスト管理

➢ フェデレーション

「アイデンティティやさまざまな資格・権限情報を、個々のドメイン間で流通させるための合意、標準、技術を意味する」
- ✓ 管理をする事業者が、お互いに安全に、認証手続を統一してすることができるように、フェデレーションを組むのが、利用者の便宜という観点からも求められる

➢ アクセス管理およびユーザ・プロファイル管理
- ✓ クラウドサービスの環境では、ユーザのプロファイルおよびアクセス管理の情報が種々の組織から提供されることになるために、きわめて、困難な作業となる
- ✓ その管理手法が監査可能な手法でなされる必要がある

3.3.2 クラウドにおける認証技術

➢ 利用端末におけるユーザ認証を実装
- ✓ 端末の権限外利用や第三者の成りすまし利用を防止
- ✓ 新たな機器認証−端末の物理的管理 TPM(Trusted Platform Module) セキュリティチップ搭載 PC [TCG(Trusted Computing Group)による規格化進行中]
- ✓ 端末の利用に対するアクセス管理

➢ クラウドサービスへのログオンにおいてそのサービスの利用を許可されたものだけが利用できそれ以外が排除されるための認証の仕組みを実装
- ✓ ユーザ認証技術　　シングル・サインオン
  - ▫ 標準化・実用化されている枠組み活用　　SAML, OpenID
- ✓ ユーザ管理
  - ▫ ユーザ側のユーザ管理
  - ▫ クラウド側のユーザ管理
    - ・ アクセス管理機能の実装
    - ・ ユーザのアイデンティティ管理システムとの統合/連携が理想

3.4 監査証跡に関する課題

➢ デジタルフォレンジック
- ✓ 不正アクセスや機密情報漏えい等のインシデントが発生した場合に原因を究明する仕組み
- ✓ 監査証跡のためのログ管理技術

- 適切なログの記録範囲を決めることが課題
- 圧縮する仕組み
- 大量のログを検索・分析する仕組み

✓ デバイスやアプリケーション等が改ざんされていないことを保証するログ採取
- TPM を用いた機器認証技術により解決

3.5 暗号・鍵管理技術

➢ 暗号技術
- ✓ データ保全
- ✓ 完全性
- ✓ 利用者・機器認証

➢ 鍵管理技術
- ✓ 各利用者に対して暗号技術を利用するための暗号鍵管理
  - 強固な暗号化は、鍵管理と並んで、クラウドコンピューティングにおいてデータを保護するために利用するコアのメカニズムである

3.6 クラウド事業者の運用管理

➢ システムに対するオペレータのアクセス管理と特権管理
➢ 外部ネットワークからの不正アクセスに対する適正な防御装置とモニタリング
➢ ウィルス感染，不正侵入，Web 改ざん等のインシデントへの対応能力の確保と体制の維持
➢ システムの脆弱性を排除するための適正なパッチ対応，アップデート管理，更新管理等
➢ アプリケーションの脆弱性をモニタリングし適正に是正すること
➢ 障害時の対応

3.7 制度，ビジネス，ガバナンス

3.7.1 クラウド事業者の経営リスク，事業継続，コンプライアンス等への対応

➢ サービスのきめ細やかさの欠如
➢ サービス自体のレベルの問題について
- ✓ 重要データの漏えいの際の責任の不明確さ
- ✓ サービスの可用性以外についての不明確さ
- ✓ サービス事業者をサポートする第三者（外注業者など）について、言及もしくは定義がされることもなく、利用者において、ガバナンス上での課題やリスクをもたらしているといわれている

➢ クラウドサービスプロバイダの事業継続性懸念について
- ✓ サービスプロバイダーの突然の倒産もしくは、サービスの中止
- ✓ サービスプロバイダーのサービス品質がさまざまな理由により低下
- ✓ 契約更新時において容認できないレベルのコストの増大

➢ データのライフサイクル管理における困難性
- ✓ データ複数のコピーの存在
- ✓ クラウドサービスプロバイダとの契約関係終了後についてのデータに関する権限の不明確さ

- ✓ クラウド事業者を切り換える必要性が突然生じた場合、従前利用していたデータの移植が困難であるとか、コストがきわめて高くなるというリスク

➢ クラウド事業者の監査に関する事項
- ✓ 監査/審査要求に対応できるログ・エビデンス管理の提供が必要

3.7.2 個人情報保護/プライバシー保護

➢ データの保管場所の問題
- ✓ 各国での法制度の違い/管轄する司法権による強制開示の可能性
- ✓ 物理的な場所をユーザが指定できることが求められる

3.7.3 法的手法による対応

➢ データの独立性についての規定
- ✓ クラウドサービスにおいて各利用者ごとのデータは、 それぞれ独立して保存されるべきことが求められる

➢ データのアクセスに対する規定
- ✓ クラウド事業者の従業員が、利用者のデータにアクセスする場合のアクセス制限、閲覧制限、アクセスログなどのアクセスに関する規定および保護措置についても契約において定め保証を受けることが求められる

➢ 技術的な手段の利用についての規定
- ✓ クラウド事業者において、一定のセキュリティ措置がとられるのは、当然のことであり、これについての契約の定め、保証なども有効

➢ データの所有権限に関する定め　・・・形態によってはプログラム著作権の課題も
- ✓ クラウドサービスの利用者は、サービス事業者に対して「データの保有者」であることを確保したいと考えている

➢ セキュリティ手段に対する定期的なモニタリング権限の定め
- ✓ クラウドサービス契約では、企業がこうしたモニタリングやテストを実施する権限を盛り込んでおく必要がある。さらに、企業経営者は、モニタリングやテスト実施のためのプラン策定や組織体制の構築を行わなければならない

➢ 法的遵守事項についての定め
- ✓ 法律、規制、国際規格、および、関連するベストプラクティスは、企業がデューデリジェンス（契約締結前）やセキュリティ監査（契約期間中）を実施することでこうした義務を満たしていることを明らかにすることを要求している

➢ 円滑な契約終了のための定め
- ✓ 企業はクラウドサービス事業者に委託した情報データに対する責任を有し、情報データを回収するか、あるいは、もはや不要な場合その内容を消去する必要がある

3.8 その他　物理・人的セキュリティ

➢ 建物やサーバ室, システムへの物理的アクセス管理
- ✓ ルール
  - ▫ アクセス範囲の限定
  - ▫ 単独アクセスの禁止

- 入退室記録の取得
- 複数人作業
- レポーティング

➢ 継続的な教育やコンプライアンス意識の醸成も重要

4. ガイドライン

➢ 企業・団体
- ✓ Cloud Security Alliance
  「CSA クラウド・セキュリティ・ガイダンス Ver.1.0 日本語版」
- ✓ Open Cloud Manifesto 等

➢ 政府機関
- ✓ 日本 経済産業省
  「クラウドサービス利用のための情報セキュリティマネジメントガイドライン 」
- ✓ 米国 NIST
- ✓ 欧州 ENISA 等

➢ 各種業界の監査基準
- ✓ 日本会計士協会監査基準委員会報告書 18 号
- ✓ SAS70
- ✓ 米国公認会計士協会（AICPA）が定めた、アウトソーシングサービスなどの受託業務に関する内部統制を評価するための監査基準
- ✓ PCI DSS： クレジット業界におけるグローバルセキュリティ基準
- ✓ HIPAA： 米国 医療保険の相互運用性と説明責任に関する法律

4.1「解説クラウド・セキュリティ・ガイダンス」

（日本クラウドセキュリティアライアンス,特定非営利活動法人 ASP・SaaS インダストリ・コンソーシアム）

「CSA クラウド・セキュリティ・ガイダンス Ver.1.0 日本語版」を日本のクラウドサービスの提供者・利用組織に分かりやすく解説

➢ IT 枠組の統合とリスクマネージメント
- ✓ クラウドコンピューティングの利用により削減されたコストの一部は、事業者のセキュリティ能力の監視の強化、および、継続中の詳細な監査のために支払われるべきである
- ✓ ミッションクリティカルなビジネスや個人情報のホスティングを行う際に、適正評価を行うのは利用者側の責任である

➢ データに対するリスクの評価
- ✓ データの所在、とりわけデータのコピーがどのように作られ、どのようにコントロールされているかを理解しなければならない
- ✓ プライバシーインパクトアセスメントを含む外部リスク評価を実施すべきである

➢ クラウド事業者の選択
- ✓ クラウド事業者の財政的実行可能性を念頭に置かなければならない
- ✓ 事業者は第三者によるリスク評価を定期的に行い、その結果を利用者が利用できるようにしなければならな

い

- ✓ クラウド事業者とそれにかかわる第三者の関係は明示されなければならない
- ✓ クラウド事業者の主なリスクとパフォーマンスの指標を理解し、利用者の観点からそれらをモニターおよび測定できなければならない
- ✓ 利用者は、クラウド事業者の事業継続およびディザスタリカバリープランを調査すべきである
- ✓ 利用者は、クラウド事業者のインフラストラクチャーの物理的依存関係を調査すべきである
- ✓ もし実行可能であるならば、クラウド事業者によるビジネスの変化が顧客経験に影響を与えるかどうかを評価するために、そのクラウド事業者の別の利用者を見つけるべきである
- ✓ クラウド事業者の顧客サービス機能を定期的にテストし、彼らのサポートレベルを判断すべきである

➢ 技術的対応策

- ✓ リスクマネージメントの観点からいえば、クラウド中に存在する非暗号化データは、利用者にとっては「失われたもの」と考えるべきである
- ✓ クラウド事業者にとってID 管理を成功させる秘訣は、堅牢なフェデレイティッドID管理アーキテクチャーを持つことと組織の内部に対する戦略を持つことである
- ✓ 仮想化されたOS は、サードパーティーのセキュリティテクノロジーで補強し、クラウド事業者単独のプラットフォームへの依存を減少させるべきである

➢ 法的対応策

- ✓ 契約はすべての基準となるものであり、組織独自の要求とクラウドコンピューティングのダイナミックな性質に基づいて交渉できるものでなければならない
- ✓ 契約にはサービスレベルアグリーメント（SLA）を盛り込む
- ✓ クラウド事業者の遵守すべき法令と利用者の遵守すべき法令の間にギャップがある可能性があることを理解すべきである
- ✓ そのギャップを明確にするために適正評価が必要であるクラウド事業者は、その情報セキュリティシステムが、利用者のデータを正確で信頼できる状態で保管されているという利用者からの要求に対して、それを保証するように求められる
- ✓ クラウド事業者によるデータの二次的な利用の可能性を理解し、必要に応じてこれを禁止するための契約の文言を盛り込む
- ✓ ストレージの地理的な場所を確かめる
- ✓ 国境を越えたデータの移動がある可能性を洗い出し、必要に応じて契約の文言にそれを禁止する条項を盛り込む

➢ 実施・測定・検証と開示

- ✓ 規制の権限やビジネスの必要性がすぐに変化するように、オンデマンドの監査の正当性を維持しておくことが重要である
- ✓ 利用者は、クラウド事業者のオンサイト査察をいつでもできるようにすべきである
- ✓ SAS70 TypeII 監査やISO27001 認証は、広くセキュリティの能力を評価でき、両方を活用することで他のいかなる認証よりも信頼がおける

4.2「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」

経済産業省から 2011 年 4 月にクラウドサービス利用のための情報セキュリティマネジメントガイドラインが公表された

- ガイドラインの目的

  情報セキュリティ管理，情報セキュリティ監査に活用することにより，クラウド利用者とクラウド事業者における信頼関係の強化に役立てる

- 特徴

  クラウドサービスを全面的に利用することにより生ずるリスクの変化に対応するため，
  JIS Q 27002（実践のための規範）の管理策に，
  「クラウド利用者のための実施の手引」と
  「クラウド事業者の実施が望まれる事項」を追加

5. 課題解決のための関与者の役割

- クラウド事業者にとってのセキュリティの課題
  - ✓ 期待
    - 安全性，信頼性，可用性について利用者が判断できる情報開示　セキュリティポリシー，SLA
    - 稼働率保障
    - 可用性保障
  - ✓ セキュリティ課題に対するクラウド事業者の予防，監視，対策のための努力
    - CSIRT　組織内のコンピュータセキュリティ問題を専門に扱うインシデント対応チーム
  - ✓ クラウドに関連する業界全体でセキュリティに関する情報共有の仕組み
    - インシデントや関連脆弱性の対する包括的な防止体制
- データやプロセスのポータビリティ，ロックインの排除
  - API/データフォーマットの共通化，標準化
- クラウド利用者にとっての課題
  - ✓ アクセス権の管理
    - 利用者内での異動や退職等を考慮
    - 権限のプロビジョニング（配置とその管理）に関する要件を体系的に制御するための枠組み整備
  - ✓ クラウドサービスの委託範囲判断
    - ビジネスプロセスや保有データの重要性
    - 利用するクラウドサービスの信頼性，セキュリティ
- 中立的立場から整備が検討されるべき課題
  - ✓ サービスレベルや情報セキュリティ対策に関する情報の開示基準
  - ✓ サービスレベルや情報セキュリティ対策に関する監査基準

[参考文献]

- 「IPA 情報セキュリティ白書 2010」2010 年 9 月　独立行政法人 情報処理推進機構

- 「解説クラウド・セキュリティ・ガイダンス」 2010 年 12 月
  日本クラウドセキュリティアライアンス

特定非営利活動法人 ASP・SaaS インダストリ・コンソーシアム
www.cloudsecurityalliance.jp/report/10kaisetsu.pdf

- 「CSA クラウド・セキュリティ・ガイダンス Ver.1.0 日本語版」 2010 年 3 月
  Cloud Security Alliance (著),
  ASPIC (特定非営利活動法人 ASP・SaaS インダストリコンソーシアム) (翻訳)

- 「クラウドサービス利用のための情報セキュリティマネジメントガイドライン 」
  2011 年 4 月　経済産業省
  http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html

以上

■ 東北支部の活動報告

高橋　典子(No.1201)

＜役員会＞
日時:平成23年5月23日　18:30～20:00
場所:富士通東北システムズ　会議室
内容:東日本大震災後の東北支部の活動再会に向けて

【東北支部の今後の予定】

東日本大震災により中断していた東北支部の活動再開の場として、6月度月例会兼研修会を、年初の計画通り下記の日程で、山形県寒河江市で開催することにいたしました。

＜SAAJ東北支部　月例会兼研修会＞
開催日時　:2011 年 6 月 25 日(土)～6 月 26 日(日)
6/25(土)11:00-13:30　そば打ち体験(紅葉庵)(会員懇親イベント)
14:00-17:00　研修会part1
(ディベート　テーマ:マネジメント信仰が会社を滅ぼす？)
6/26(日)09:00-12:00　研修会part2
(震災を受けて－体験からのBCP)
会場　:ホテルサンチェリー
〒991-0031 山形県寒河江市本町一丁目 2-23
(TEL:0237-83-5000(代) FAX:0237-83-5005)

以上

(この投稿は 5 月号に掲載したレポートの続きです。3 章は 7 月号に掲載予定です。)　　(投稿)

■保証業務に係る公表文書の調査研究と保証型システム監査の一考察 (2章)

榎本　吉伸

2.「財務情報等に係る保証業務の概念的枠組みに関する意見書」(金融庁企業会計審議会:2004 年 11 月 29 日)における保証業務の概要

「財務情報等に係る保証業務の概念的枠組みに関する意見書」(以下、意見書)は、保証型システム監査の議論を進めるに当たって規範となるべき枠組みである。ここでは、まず保証業務のフレームワークを学び理解する為に、その概要を紹介する。

2.1 「意見書」公表の背景・目的等

2.1.1 「意見書」審議の背景

①信頼性の確保に対する社会からの多様な期待

近年、財務諸表以外の財務情報の開示とその信頼性の確保に対する社会からの多様な期待が高まりつつある。また、財務情報の信頼性の確保に係る費用対効果の観点から、監査の水準には至らないが一定の信頼性が確保できる業務(いわゆるレビュー業務)が増大している。さらには、内部統制等の財務情報以外の事項にも独立の立場からの信頼性の確保が求められる状況にある。

②公認会計士の行う業務の拡大

一方で、企業のさまざまな活動に関するコンサルティング等非監査業務の拡大により、監査人による監査業務と非監査業務の範囲の明確化が一層重要となっている

また、国際会計士連盟の国際監査・保証基準審議会において進められている「国際監査基準」においては、従来の監査業務のみならずレビュー業務などを包括した“Assurance Engagements”(保証業務)という概念により、関連する業務の枠組みを整理している。

2.1.2 「意見書」公表の目的

①保証業務の概念的枠組みの整理

わが国では、保証業務の枠組みを、保証業務の公益性の観点から、企業会計審議会において、幅広い関係者による議論を通じ、保証業務の意味を確認し、その要件と範囲の明確化を図ることにより、監査を初めとする保証業務に対する社会からの信認を確保することを目的として、保証業務の概念的枠組みの整理を行った。

上記の背景を踏まえて、企業会計審議会では平成 16 年 11 月 29 日に、これを「財務情報等に係る保証業務の概念的枠組みに関する意見書」として公表した。

②本意見書の位置付けと本レポートの関係

意見書の位置付けとして、「本意見書は、「監査基準」のように、特定の保証業務を前提として適用されることを意図するものではない。したがって、本意見書に示された概念的枠組みが直接に業務上の規範となるものではないが、個々の保証業務に関する基準等は、本意見書における概念的枠組みを基礎として設定されることになる。」とある。

また「本意見書では、財務情報等に係る保証業務に関する概念整理を行うことを主たる目的としているが、内部統制など財務情報以外の事項を対象とした業務も含めた幅広い観点から、包括的に保証業務の概念を整理し、その中で財務情報等に係る保証業務も位置付けられるという枠組みを採っている。したがって、本意見書に示された概念的枠組みは、財務情報以外の事項を対象とする保証業務にも援用することが可能と考えられ、今後、各方面において活用されることが期待される。」と明言されている(傍点筆者)。

ここに、本レポートで考察する「保証型システム監査」のフレームワークも、この意見書の枠組みをベースとして議論を展開する。

2.2 意見書における保証業務の概念的枠組み概要

2.2.1 保証業務の定義

意見書には、保証業務の定義として「保証業務とは、主題に責任を負う者が一定の規準によって当該主題を評価又は測定した結果を表明する情報（以下、「主題情報」という。筆者注記：研究報告（後述）における「確認書」等）について、又は、当該主題それ自体について、それらに対する想定利用者の信頼の程度を高めるために、業務実施者が自ら入手した証拠に基づき規準に照らして判断した結果を結論として報告する業務をいう。」とある。

この保証業務の定義でのキーポイントは、次の3項である。

・保証対象は「主題情報あるいは主題自体」であるということ。

・業務の目的は「想定利用者の信頼の程度を高めるため」である。

・実施手続きとしては「業務実施者が自ら入手した証拠に基づき規準に照らして判断した結果を結論として報告する」ことを言う。

意見書では、以下の各項で上記キーポイントについて詳細に説明されている。

ただ、ここで留意すべきことは、意見書「二 保証業務の意味」で述べられている保証業務内容である。

意見書には「保証業務は、通常、一定の規準によって主題を評価又は測定した結果を表明する情報（ 以下、「主題情報」という。）を主題に責任を負う者が自己の責任において想定利用者に提示することを前提として行われる。主題に責任を負う者が自己の責任において主題情報を想定利用者に提示しない場合に、業務実施者が、主題それ自体について一定の規準によって評価又は測定した結果を結論として表明する保証業務があるが、この場合においても、業務実施者は、主題それ自体に対する責任を負うものではなく、主題それ自体の信頼の程度を高めることに責任を負う。」とある（傍点筆者）。

ここでは、「主題情報」を提示されることが前提であり、この提示の有無で監査報告書の記載様式を各々限定していることに留意いただきたい（詳しくは後述）。

この場合、保証の対象が主題情報の場合はノンダイレクト監査で、主題それ自体が保証対象の場合はダイレクト監査になるが、この違いを明確にして監査することははなはだ困難で、意見書には詳しい記載がない。

ただ重要なことは、“保証”とは**「業務実施者が、主題それ自体について一定の規準によって評価又は測定した結果を結論として表明する保証業務の場合においても、主題それ自体の信頼の程度を高めることに責任を負う」**ことである。

2.2.2 保証業務の分類

①合理的保証業務と限定的保証業務

保証業務は、保証業務リスクの程度により、合理的保証業務と限定的保証業務に分類される。

・合理的保証業務

合理的保証業務では、業務実施者が、当該業務が成立する状況のもとで、積極的形式による結論の報告を行う基礎として合理的な低い水準に保証業務リスクを抑える（筆者注記：積極的形式とは、一定の規準に照らして適正性や有効性等が認められるかどうかを報告する形式）。

・限定的保証業務

これに対して、限定的保証業務では、合理的保証業務の場合よりは高い水準ではあるが、消極的形式による結論の報告を行う基礎としては受け入れることができる程度に保証業務リスクの水準を抑える（筆者注記：消極的形式とは、一

定の規準に照らして適正性や有効性等がないと考えられるような事項が発見されなかったかどうかを報告する形式)。

②保証業務の事例

「保証業務の定義及び分類によれば、以下の業務はそれぞれ次のように理解される」とあり、3つの保証業務事例を挙げている。

・財務諸表の監査

通常の財務諸表監査のことで、主題情報たる財務諸表を規準たる会計基準で測定し、想定利用者の財務諸表に対する信頼の程度を高めるために、合理的保証業務たる監査手続を実施し、企業の財政状態等を適正に表示しているかどうかについて積極的形式により結論を報告する。

・内部統制に係る保証業務

内部統制の“有効性”に係る保証業務を行う事例を挙げている。意見書の公表時期と日本における内部統制議論の活発な時期とが合致したためであろう。

・限定的保証業務としてのレビュー業務

この項では、唐突に「レビュー業務」の記載があり、その定義や内容の説明もなく、なぜ限定的なのかの記載も無い。後述の「合意された手続」のように説明が欲しい。

まとめると、保証業務／合意された手続の分類として、意見書では以下のように定義している(筆者によるまとめ)。

呼び名	業務内容	報告形式／特記事項	事　例
監　　査	合理的保証業務	積極的形式による結論	・財務諸表監査 ・内部統制に係る保証業務
レビュー	限定的保証業務	消極的形式による結論	・四半期レビュー
合意された手続	(非保証業務)	(特記事項)合意内容を十分理解している合意当事者以外の者に当該報告書を提示すべきでない	・証券会社における顧客資産の分別管理に関する合意された手続業務

2.2.3 保証業務実施の前提

①業務実施者の倫理(省略)

②保証業務を適正に遂行できるものであるかどうかの判断

意見書曰く、「想定利用者の範囲やニーズの内容、主題に責任を負う者の特徴、契約の条件、主題の性格、規準の特徴、入手可能な証拠、報告の方法等について、保証業務を適正に遂行できるものであるかを判断すること。」

③業務実施者の責任

意見書曰く、「業務実施者は、保証業務について要請される要件[筆者注記:上記、2項目および次項、保証業務の要素等]及び保証業務の実施に関する基準[筆者注記:一般に認められた公正妥当な基準]に準拠して適切に業務を行わなかった場合には責任を負う。」

2.2.4 保証業務の定義に合致しない業務

意見書では、保証業務の定義に合致しない業務として特に以下の4業務を挙げ、保証業務の要件を明確にしている。

①合意された手続

業務実施者が、主題に責任を負う者又は特定の利用者との間で合意された手続に基づき発見した事項のみを報告する業務(「**合意された手続**」という。)(傍点筆者)

②財務諸表等の調製

財務情報の作成及び作成への関与を行う業務（「財務諸表等の調製」という。）

③助言や調査

主題に責任を負う者の経営又税務上の判断に関わる助言や調査等を行う業務

④税務申告書の作成及び納税者の代理を行う業務

第 1 項の「合意された手続」は重要だが、次の項で説明される「保証業務の要素」が理解されないままに、ここで議論するのは比較もできず早急であろう。

今後の理解のために、ここで保証業務との違いを明確にしておくと、“保証業務が保証業務に適合する規準（特に規準の要件の中立性／客観性が重要）に基づき実施するのに対して、合意された手続は当事者同士が合意した手続（固有の規準を含む）に基づき実施する”ことである。合意された手続が保証業務の定義を満たさない理由として、意見書では「実施される手続が主題に責任を負う者又は限られた利用者との間の合意によって特定されるため、業務実施者が自らの判断により証拠を入手しないこと、及び、手続の結果のみが報告され結論が報告されないことから」という。

「保証業務の定義に合致しない業務」の説明を次項の後に記述するのが親切であろう。

2.3 保証業務の要素

保証業務の要素として、以下の5要素が挙げられ、続く各項でそれぞれの要素に関する適格な要件が明確にされている。

① 業務実施者、主題に責任を負う者及び想定利用者の三当事者の存在

② 適切な主題

③ 適合する規準

④ 十分かつ適切な証拠

⑤ 合理的保証業務又は限定的保証業務について適切な書式の保証報告書

2.4 保証業務に関わる当事者

①三当事者の存在

当然のこととして保証業務は、業務実施者、主題に責任を負う者及び想定利用者からなる三当事者が関わることにより成立する。各当事者についての意見書の詳細な記載は省くが、「主題に責任を負うもの」の記載には留意が必要なのでここに挙げる。

②業務実施者（監査人等の保証業務を実施する者）

③主題に責任を負う者

意見書には「主題に責任を負う者が、主題情報を自己の責任において想定利用者に提示する場合と、これを提示しない場合がある。」とある。

主題情報とは、次章で後述する公認会計士協会の「公認会計士が行う保証業務に関する意見書」における「確認書」等を示すのであろう。内部統制監査で言えば、「内部統制報告書」に該当する。

④想定利用者

想定利用者とは、業務実施者が作成した保証報告書を利用する者と定義される。さらに意見書には次のように「主題に責任を負う者は、想定利用者の1人になることはできるが、唯一の利用者になることはできない」とある。主題に責任を負う者が唯一の利用者になる場合は保証業務とは言えないということである。理由の明確な説明はないが、自分だけのために自分を保証することに意味はないからであろうか。保証業務の“保証”たる所以である。

2.5 保証業務における適切な主題

① 主題の要件

意見書には「保証業務における適切な主題は、識別可能であり、一定の規準に基づいて首尾一貫した評価又は測定を行うことができ、かつ、業務実施者が主題情報に対する保証を得るために十分かつ適切な証拠を収集することができるものをいう。」とある。

適切な主題の要件をまとめると以下の3点となる。

・識別可能であること

・一定の規準に基づいて首尾一貫した評価又は測定を行うことができる

・業務実施者が主題情報に対する保証を得るために十分かつ適切な証拠を収集することができる

「識別可能であること」とは、明確でないが、他者への説明可能性と考える。

② 主題の事例

意見書には、保証業務の対象となり得る主題および主題情報について、以下の例を挙げている。ここでは全ての例を確認する。特にITシステムについての記載があるので参考にされたい。

・財務諸表で表示又は開示される企業の財政状態、経営成績及びキャッシュフローの状況を主題とすると、財務諸表の表示又は開示が主題情報となる。

・非財務的な成果又は状況を主題とすると、その効率性や有効性を示す指標が主題情報となる。

・設備能力のような物理的な特徴を主題とすれば、その記録や仕様が主題情報となる。

・内部統制やITシステムのようなシステムやプロセスを主題とすれば、それらの有効性について示すものが主題情報となる（筆者注記：ITシステムの場合は、有効性のみでなく、効率性・信頼性・安全性などを示すものも主題情報と考えられる）。

・コーポレート・ガバナンスやコンプライアンス又は人的資源管理のような行為を主題とすれば、その遵守状況や有効性を示すものが主題情報となる。

③ 主題の性格

主題の性格とは以下に整理される。

・定量的か定性的か

・客観的か主観的か

・確定的か予測的か

・一定時点に関するものか一定期間にわたるものか

これらの性格は、業務実施者が主題情報に係る保証を得る際の正確性及び入手可能な証拠の説得力に影響する。意見書に曰く「このため、保証報告書には、かかる主題の性格を記載する必要がある。」

2.6 保証業務における適合する規準

2.6.1 規準の要件

保証業務における適合する規準の定義として、意見書には「主題に責任を負う者が主題情報を作成する場合及び業務実施者が結論を報告する場合に主題を評価又は測定するための一定の規準」とあり、以下のような5つの要件を備えている必要があるという。規準は重要な項目なので、全文を紹介する。

①目的適合性

想定利用者による意思決定に役立つ結論を導くのに資する規準であること。

②完全性

各業務環境の下で得られる結論に影響を与える要因のうち関連する要因のいずれもが省略されていない規準であること。

③信頼性

同一の環境で同一の資格を有する業務実施者が利用するとき、主題の評価又は測定を合理的にかつ首尾一貫して行うことができる信頼性のある規準であること。

④中立性

偏向のない結論を導くのに資する中立的な規準であること。

⑤理解可能性

明瞭かつ総合的な結論を導くことに資するもので、著しく異なる解釈をもたらすことなく、保証業務を構成する三当事者にとって理解可能な規準であること。

以上、「保証業務における適合する規準の定義」とあるが、意見書は会計監査や内部統制監査等の保証業務をベースにしているため、上記の基準の定義は会計監査等における基準の定義として明確にされた一般論で、特に保証要件を担保する基準の定義として固有の項目はないと考える。

2.6.2 規準の適用

規準は次の2つに分類され、適用については以下の通りである。

・確立された規準（法令のほか、一般に公正妥当と認められる企業会計の基準など）

業務実施者は、個々の保証業務について規準の適合性を評価するが、主題が確立された規準により評価又は測定されている場合には、当該規準が業務実施者における適合する評価又は測定の規準となる。

・主題に応じて個別に策定される規準（筆者注記：システム監査では重要）

個別に策定される規準については、上記規準の要件に基づき業務実施者が特定の業務に対する規準としての適合性を評価して適用する。

後述するが、システム監査において有効性や効率性を監査目標とする場合は、「主題に応じて個別に策定される規準」が考えられる可能性があるが、その場合は規準としての妥当性の評価が重要である。

2.6.3 想定利用者の利用可能性

主題がどのように評価又は測定されているのかを理解するためには、想定利用者にも規準が理解可能であり、利用可能であることが求められる。想定利用者にとって理解可能・利用可能な規準とは、以下のような規準である。

①公表されている規準

②主題情報において明示されている規準

③保証報告書において明示されている規準

④広く一般に理解を得られている規準

但し、意見書には次の制限項目がある。「規準が特定の想定利用者にのみ利用可能である場合、又は、特定の目的にのみに適合するものである場合には、当該規準に基づいた結論を報告する保証報告書の利用は、当該特定の利用者又は特定の利用目的に制限される。」

2.7 十分かつ適切な証拠

2.7.1 証拠の入手

証拠の入手については基本的事項なので詳細を見る。意見書には「業務実施者は、主題情報に重要な虚偽の表示が含まれていないかどうかについて、職業的専門家としての懐疑心をもって保証業務を計画し、実施し、十分かつ適

切な証拠を入手する。証拠収集のための手続の種類、実施の時期及び範囲を決定する際には、業務実施者は、重要性、保証業務リスク及び利用可能な証拠の量及び質を検討する。」とある。この説明のなかのキーワードについては、以下の通りである。

2.7.2 職業的専門家としての懐疑心

意見書曰く、「業務実施者は、主題情報に重要な虚偽の表示が存在する可能性を考慮し、職業的専門家としての懐疑心をもって保証業務を計画し、実施する。職業的専門家としての懐疑心とは、業務実施者が証拠として入手した情報の妥当性について探究心をもって批判的に評価することを意味する。」とある。

前提として「また、業務実施者は、証拠として利用する情報の信頼性について、当該情報の作成及び保存に関する内部統制を含めて検討する。」必要がある。

2.7.3 証拠の十分性および適切性

証拠の十分性および適切性については、最も重要なことであるがその妥当性の評価は難しい。意見書には以下の3項目が挙げられている。

①量的な十分性及び質的な適切性

業務実施者は、証拠の量的な十分性及び目的適合性や信頼性などの質的な適切性を勘案して、必要とされる証拠を入手することが求められる。単に証拠の入手量を増やすことにより質的な適切性を補うことはできない。また、効率的に証拠を入手することが求められるが、費用上の観点から、十分かつ適切な証拠の収集を省略することは妥当ではない。

②証拠の信頼性

証拠の信頼性は、その源泉と性格だけでなく、証拠が入手された状況によっても影響を受ける。また、業務実施者は、入手した証拠が他の源泉からの証拠又は異なる性格の証拠と首尾一貫していない場合には、その不一致を解消するために追加的な証拠を必要とするかどうかを判断することになる。

③証拠の十分性と適切性の評価

業務実施者は、保証報告を裏付ける証拠の十分性と適切性を評価する場合には、職業的専門家として懐疑心をもって判断することが求められる。

しかしこの説明だけでは、具体的な評価方法や尺度が明示されておらず、評価することは無論のこと、評価の妥当性を判断できない。

2.7.4 重要性

意見書曰く「業務実施者が、証拠を収集する手続の種類、実施の時期及び範囲を決定するとき、並びに、主題情報に虚偽の表示があるかどうかの判断をするときに、重要性が考慮される。特定の業務に係る重要性や質的及び量的な要因の相対的な重要性の評価は、業務実施者の判断に委ねられるが、業務実施者は、重要性を考慮するに当たっては、想定利用者の意思決定に影響する要因を理解して判断し、相対的な重要度、主題の評価又は測定に対する種々の要因の影響の程度、及び想定利用者の利害等といった、量的並びに質的要因の観点から検討を行うことが求められる。」

2.7.5 保証業務リスク

①保証業務リスクとは

保証業務リスクは、会計監査における監査リスクと大きく差異がない。意見書には「保証業務リスクは、主題情報に重要な虚偽の表示がある場合に業務実施者が不適切な結論を報告する可能性をいう。」とあり、ここでは主題情報を対象としており、主題それ自体の保証について言及されていない。保証業務リスクは、一般に次の要素から構成される。

・固有リスク

関連する内部統制が存在していないとの仮定の上で、重要な虚偽の表示がなされる可能性をいう。

・統制リスク

重要な虚偽の表示が、関連する内部統制によって適時に防止又は適時に発見されない可能性をいう。

・発見リスク

業務実施者により重要な虚偽の表示が発見されない可能性をいう。

②証拠収集手続の選択、実施の時期および範囲の決定

「業務実施者は、保証業務リスクを合理的保証業務又は限定的保証業務に求められる水準に抑えるため、固有リスク及び統制リスクを個別に又は結合して評価することにより、発見リスクの水準を決定し、それに基づいて、証拠を収集する手続の選択、実施の時期及び範囲を決定する。」

③保証の水準

・合理的保証業務においては、積極的形式で業務実施者の結論を報告する基礎として、合理的保証が得られる業務環境にある限り、業務実施者は、合理的な低い水準となるまで保証業務リスクを抑える。限定的保証業務においては、保証業務リスクの水準を、合理的保証業務における水準よりも高く設定することができる。

・しかし、限定的保証業務においても、証拠を収集する手続、実施の時期及び範囲を組み合わせることによって、業務実施者は、消極的形式で報告を行う際の基礎としては十分に有意な保証水準を得ることにより、想定利用者にとっての信頼性を確保することが必要である。

2.7.6 証拠収集手続の種類、実施の時期および範囲

意見書には以下の通り。

①合理的保証業務において

合理的保証業務においては、業務実施者は、積極的形式により結論を報告するために、次のような相互に関連性のある系統だった業務プロセスを経て、十分かつ適切な証拠を得る必要がある。

・主題及び内部統制を含む業務環境の理解

・業務環境の理解に基づく主題情報に重要な虚偽の表示が存在するリスクの評価

・リスクの評価に応じ、業務全般の計画の策定、実施すべき手続の種類、実施の時期及び範囲の決定

・識別されたリスクに明確に関連付けられた手続の実施

・証拠の十分性及び適切性の評価

②限定的保証業務において

限定的保証業務においても、主題及び業務環境の理解を含む相互に関連性のある系統だった業務プロセスは必要であり、手続の適用を通じて十分かつ適切な証拠の収集が求められる。しかしながら限定的保証業務における十分かつ適切な証拠の収集手続の種類、実施の時期及び範囲は合理的保証業務に対して限定的である。

一般に、限定的保証業務であるレビューでは、主に分析的手続及び質問によって、レビューにおいて求められる十分かつ適切な証拠が得られると考えられている。

2.7.7 利用可能な証拠の量と質

意見書には、利用可能な証拠の量と質について、次の2項の記載がある。

①業務実施者が利用可能な証拠の量及び質は、主題が予測的である場合などの主題又は主題情報の特徴による影響、主題に責任を負う者からの制約や物理的な制約による影響を考慮して検討する。

②業務実施者が、環境的要因や主題に責任を負う者又は契約の当事者から制約を受けることにより、十分かつ適切な証拠が入手できない場合には、結論の報告に必要な基礎を得ることはできない。

2.8 保証報告書

意見書には、「業務実施者は、適用した一定の規準や実施した手続に関する事項などを含めて、業務を実施して得た保証に関する結論を保証報告書により報告する。」とある（傍点筆者）。

更に「保証報告書には、当該保証業務が合理的保証業務であるのか又は限定的保証業務であるのかの区別が明確に理解されるように記載する。」とある。

・合理的保証業務の保証報告書

合理的保証業務の保証報告書では、対象となる主題又は主題情報について、保証業務リスクを合理的保証業務に求められる水準に抑えるための手続を実施した結果を報告する。

その場合、すべての重要な点において、一定の規準に照らして適正性や有効性等が認められるかどうかの結論を報告する（「積極的形式」という）。

・限定的保証業務の保証報告書

限定的保証業務の保証報告書では、対象となる主題又は主題情報について、保証業務リスクを限定的保証業務に求められる水準に抑えるための手続を実施した結果を報告する。

その場合、すべての重要な点において、一定の規準に照らして適正性や有効性等がないと考えられるような事項が発見されなかったかどうかを報告する（「消極的形式」という）。

2.9 **意見書における「保証業務における概念的枠組み」まとめ**

2.9.1 保証業務の定義

意見書での保証業務の定義は以下の通りである。

「保証業務とは、主題に責任を負う者が一定の規準によって当該主題を評価又は測定した結果を表明する情報（以下、「主題情報」という。）について、又は、当該主題それ自体について、それらに対する想定利用者の信頼の程度を高めるために、業務実施者が自ら入手した証拠に基づき規準に照らして判断した結果を結論として報告する業務をいう。」

2.9.2 保証業務の要素

この定義により、保証業務成立の要件として5つの要素が挙げられている。

① 業務実施者、主題に責任を負う者及び想定利用者の三当事者の存在

② 適切な主題

③ 適合する規準

④ 十分かつ適切な証拠

⑤ 合理的保証業務又は限定的保証業務について適切な書式の保証報告書

既に見たように、意見書には上記の各要素に関する適格な要件が示されている。

先に、“保証”とは「業務実施者が、主題それ自体について一定の規準によって評価又は測定した結果を結論として表明する保証業務の場合においても、主題それ自体の信頼の程度を高めることに責任を負う」と述べた。しかし意見書には、十分な証拠に基づき一定の規準によって評価又は測定した結果を結論として表明する手続（筆者注記：以下「評価の方法」と呼ぶ。）についてはなにも触れられていない。

実務上では「評価の方法」は保証業務においては十分な議論が必要な重要課題である。私見を後述する。

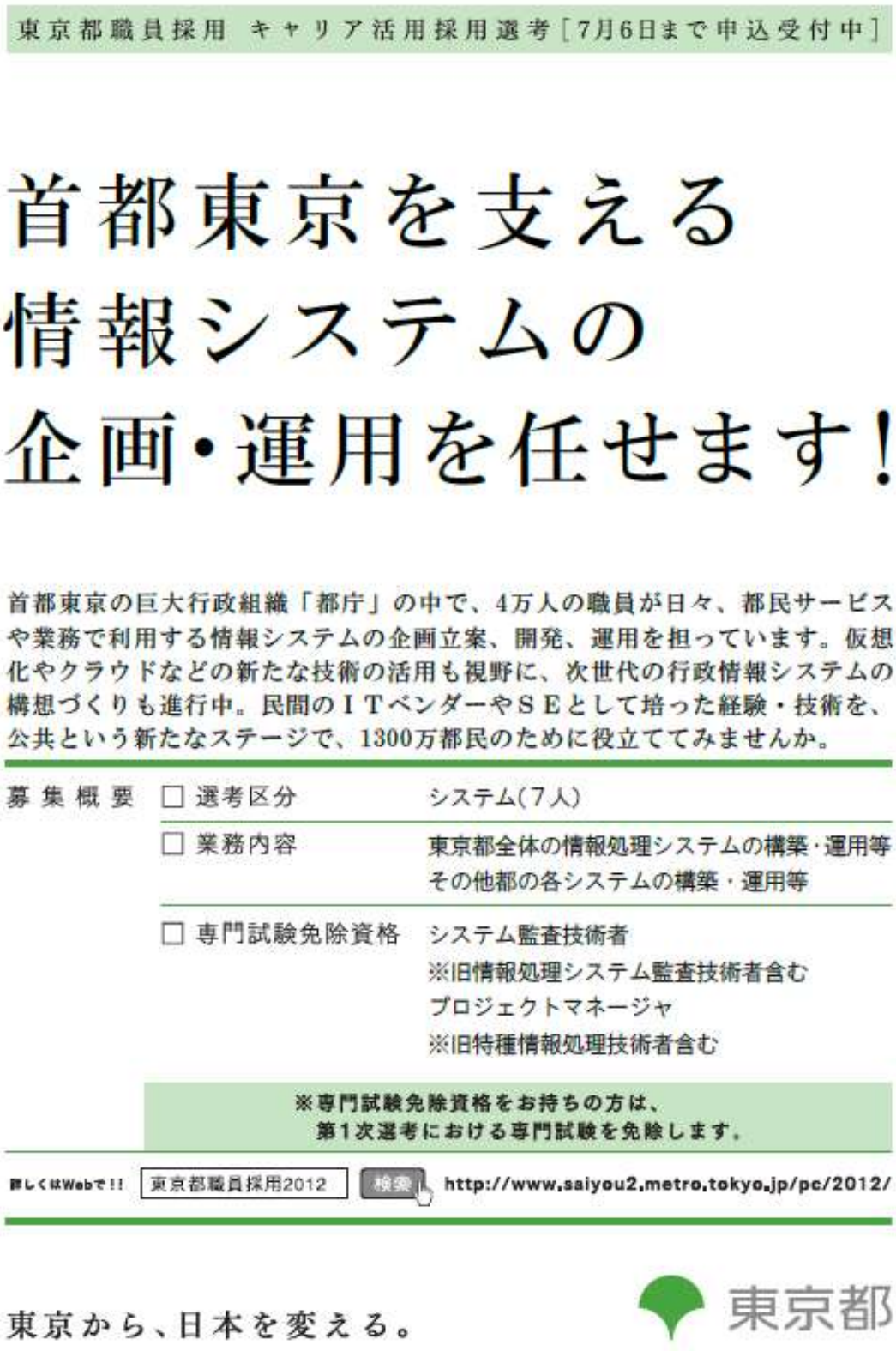
次章では、監査・保証実務委員会研究報告第 20 号「公認会計士等が行う保証業務等に関する研究報告」を学ぶ。

以上

注目情報（6/1～6/30）

■ **東京都職員採用情報**

http://www.saiyou2.metro.tokyo.jp/pc/2012



■ システム監査学会主催　第 25 回研究大会（2011/6/10（金）10：00-16：40）

【テーマ】　「リスクマネジメントとシステム監査－東日本大震災からの考察－」
【日　時】2011 年 6 月 10 日（金）10：00-16：40　（開場 9：30-）
【会　場】機械振興会館ホール（地下 2 階）　東京都港区芝公園 3-5-8
http://www.jspmi.or.jp/kaikan.htm
【主　催】システム監査学会（JSSA）　【定　員】200 名
【参加費】・システム監査学会会員、後援団体会員　5,000 円
（日本システム監査人協会会員の方は「会員」価格でご参加いただけます）
・一般：8,000 円
【申込・詳細】http://www.sysaudit.gr.jp/taikai/2011taikai.html

■ ISACA 大阪支部　総会と設立 25 執念講演会のご案内
http://www.isaca-osaka.org/25th/isaca_osaka_25th.pdf

1. 日時 ： 2011 年 6 月 18 日(土)12:30～17:00

2. 会場 ： 大阪研修センター
(1) 所在地
大阪市淀川区十三本町 1-12-15 ドルチェヴィータファースト 3F
TEL:06-6302-4040(代)
(2) 交通
阪急「十三駅」西口から徒歩 3 分
(3) 地図
http://www.kaigishitsu.ne.jp/accessmap/index.html
かに道楽から3つ先のビル、自転車屋の1つ先のビル。ケーキ屋(ハンブルグ)の手前。

3. スケジュール
12:30～13:30　総会
(終了後30分間休憩)
14:00～16:55　記念講演会
17:30～19:30　懇親会

※ ISACA大阪支部会員以外の方は記念講演会からの出席となりますのでご注意下さい。

以上

全国のイベント・セミナー情報

■第 18 回システム監査実務セミナーの開催について　（某日某所でのインタビュー）

この 8 月 27-28 日及び 9 月 10-11 日の 4 日間に亘って開催される、「第 18 回システム監査実務セミナー」について、主催するシステム監査事例研究会の担当理事、三輪さんに話しを伺いました。

記者（以下、「記」）：システム監査実務セミナーについて、教えてください。

三輪理事(以下、「三」)：システム監査実務セミナーは当協会の設立目的のひとつでもある、「システム監査人の実務能力の維持・向上」を目的に、年 2 回開催している、きわめて実践的なセミナーです。

これまで、通算 17 回開催され、延べ 200 人近いシステム監査人にご活用いただいています。

記） どんな内容なのですか？

三） **システム監査事例研究会**では、システム監査の普及とシステム監査人の教育を目的として、実費のみでのシステム監査をご提供してきており、これまで、約 30 社からのご依頼を受け、監査を行ってきました。

これらの貴重な事例について、被監査企業様のご了承をいただき、匿名化した上で教材化したものを使って、ロールプレイング方式で、実際のシステム監査を疑似体験いただく内容となっています。また、システム監査を通して、経営に役立つさまざまなノウハウをご提供できるように、日々、教材のブラッシュアップも図っています。

日程としては、1 泊 2 日×2 回で、計 32 時間の合宿型セミナーです。

記） それは、大変実践的ですね。どんな方が参加されているんでしょうか？

三） **システム監査技術者試験**には合格したもののシステム監査参加機会のない方や内部監査部門でこれからシステム監査にも取り組まれようとしている方、公認システム監査人の資格認定を目指している方など、さまざまな方にご参加いただいています。

J-SOX 導入直前のセミナーでは、公認会計士や監査法人の職員の方にも多くご参加いただきました。

私としては、難しいことは抜きにして、「とにかくシステム監査を実際に体験したい」という方にご参加いただければと思っています。

記） さまざまなバックグランドの方が参加されていますが、皆さんにご満足いただけるのでしょうか？

三） **大変実践的**なセミナーですから、監査理論などの難しいことはとりあえず置いて、ロールプレイと格闘していくので、理解しやすいようです。

監査理論については、ロールプレイの節目節目で、講師からご説明していきますから、実践に即して理解できるので、とっつきにくい監査理論についてもスムーズに吸収できるようですよ。

毎回のセミナーの後、受講いただいた方にアンケートをしていますが、満足度については、非常に高い評価を頂戴しています。

記） 実際、リピーターの方もいらっしゃると聞きましたが？

三） **そうなんですよ**。2 回 3 回と、何度も受講していただけるファンの方もいらっしゃいます。教材の数が多いので、い

ろいろな監査事例を疑似体験できるということで、何度も受講くださっているのだと思います。

記） こういう高度なセミナーの講師をするのは大変だろうと思うのですが、どんな方が担当されているのですか？

三） **教材となった監査事例**を実際に監査した方や、教材化に携わった方など、その事例の裏の裏まで知り尽くした方にお願いしています。

だからこそ、紙の上だけではない、ナマの知識をお伝えできると考えています。

また、ロールプレイは 3-5 名程度のチームで行いますが、各チームに担当講師 1 名とチューター(講師補助員)1 名がついて、細かいところまで指導が行き届くように工夫しています。

記） マンツーマンに近い形なのですね！セミナーでは、ただ学習するばかりではなく、楽しいこともあるそうですが？

三） **3-5 名程度**の少人数でチームを組んで、協力してロールプレイを行っていただきますので、メンバー同士が非常に懇意になることが多いです。セミナーを通じて、貴重な人脈を築いていただければ、うれしいことですね。

また、1 日目と 3 日目の演習終了後に、夕食をかねて懇親会を行っていますが、ざっくばらんな雰囲気の中で、経験豊富な講師から、これまで経験されてきたシステム監査の裏話や、システムを通じた経営のあり方、今後のシステム技術の動向など、貴重なお話を聞くこともできますよ。

記） セミナーを受講するメリットはどんなものがありますか？

三） **システム監査**についての理解を深めることは当然ですが、他にも、公認システム監査人の認定に必要な実務経験 1 年分、同じく資格更新に必要な継続教育 32 時間分として認定されます。また、ITC や ISACA など他団体の継続教育時間にも算入が可能な場合がありますので、詳細は各団体にお問合せください。

記） 1 泊 2 日×2 回ということですが、セミナーや宿泊の会場は、どんなところを使うのですか？

三） **都心にある**研修特化型ホテルで開催しています。東京駅や羽田空港からのアクセスも良いので、地方から参加される方にも便利かと思います。

先ほども申しましたとおり、演習そのものはもちろん、懇親会も意義深いものになっていますから、是非ご宿泊いただきたいのですが、ご家庭の事情などで宿泊が難しい場合は、演習終了後、お帰りいただくことも可能です。ご希望の方は、お気軽にセミナー事務局にお問合せください。

記） 受講料はいくらなのでしょうか？

三） **4 日間で**、一般 189,000 円のところ、SAAJ 会員の方には 168,000 円でご提供しています。もちろん、期間中の宿泊費、食費込みの料金です。

記） 私も参加してみたくなってきました！申し込みはどうすればいいのでしょう？

三） **まだ、定員**までには若干の空きがありますから、お早めにどうぞ。協会のホームページから申込みができます。

URL は以下のとおりです。

http://www.saaj.or.jp/kenkyu/jitsumuseminar18.html

記：今日は、お忙しいところお時間をいただき、ありがとうございました。

以上

■ 【東京・月例研究会の案内】

【6月の月例研究会】

開催日時　：6月29日（水）　午後6時半から8時半
場　　所：御茶ノ水　総評会館2階大会議室
講演テーマ：「りそなグループにおけるシステム監査（監査実務を中心に）」
概　要　：１．システム監査の体制　　２．監査の実施手順
　　３．内部評価　　４．過去に実施した主なシステム監査の概要
講　演　者：りそなホールディングス　内部監査部　田原公正　様

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）

■ □■ＳＡＡＪ会報編集担当より

会員の皆様からの、投稿をいつでも募集しております。 気楽に投稿ください。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）
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。
投稿用アドレス:saaj-kaihoh ☆ yahoogroups.jp （☆は投稿時には＠に変換してください）

■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：竹下和孝、仲　厚吉、安部晃生、成 楽秀、桜井由美子、清水恵子、山田 隆、片岡 学、
木村陽一、藤野明夫　　投稿用アドレス：saaj-kaihoh☆yahoogroups.jp（☆は安全対策）