第８６回月例研究会報告

No.243　打矢隆司

テーマ：ＣＯＢＩＴ３の概要
日時：平成１４年1月２５日午後6時半より
場所：労働スクエア東京７０２号室
講師：
公認会計士ビジネスインテグレーション主宰
上川公認会計士・税理士事務所代表
日本公認会計士協会東京会コンピュータ委員会委員長
公認会計士、税理士、CISA、システム監査技術者、ＩＴコーディネータ（インストラクター）
上川真一　氏（かみかわ）
参加：約７０名

はじめに

上川真一さんは、上記の様に、IT関係の資格をお持ちのうえで、主に外資系企業をお相手としたコンサルティング事務所を主宰されています。また日本公認会計士協会東京会でコンピュータ委員会委員長を勤められる等、業界団体でも活動されています。監査法人勤務時に、COBIT に関し日本における最も熱心な伝承者である（と筆者が感覚的に思っているだけですが）松尾明先生に感化されCOBITをシステム監査の実践にも適用されております。

COBIT は全体を解説したものが無く、ベールに囲まれたものでしたが、上川氏はユーモアのある滑らかな語り口でその全様を明らかにしてくれました。

研究会参加者は会場に補助椅子を入れても収容しきれず、１０名以上の方が立ち見の場所も確保できずお帰りになる程でした。

１．講演概要

(1)背景

①設定主体

ＣＯＢＩＴの版権はＩＳＡＣＡの上位承認権限機関である Information Systems Audit and Control Foundation(ISACF)とＩＴガバナンス協会に属している。ステアリングコミティの中核となった組織や団体は米国の大手会計監査法人／コンサルティングファーム／ハードウェアベンダーなどの法人と、SWIFT／AICPA／JICPAなどの団体である。

(2)COBITとは

COBIT とは、Control Objectives for Information and related Technology「情報技術のコントロール目標」の略である。COBIT は1996年に発行以来、ほぼ２年おきに改定されている。前バージョンまではコントロール目標とシステム監査手続きの体系的指針であったが、2000年７月に第３版が発刊された。成熟度モデルの成熟度評価やバランストスコアカードのスキームが取り入れられ、よりマネジメント指向で経営者に親和的なガイドラインとなっている。換言すれば経営者のための IT ガバナンス指南書に変貌してきた。

正式な日本語訳は ISACA 東京支部基準委員会が作成中と聞いている。一方で自社内での COBIT 適用を目指し、また自主勉強会等で要訳・抄訳資料を作成する方が多く、最近では自分も含め IT コーディネータの方々が活発に輪読活動されている。

(3)COBITの内容

①全体概要

環境変化のなかで求められること

1)　ITはビジネスと連動し、ビジネスを実現可能にし、利益を最大化する

2)　IT資源は責任をもって利用される

3) IT に関連するリスクは適切に管理される

②フレームワーク

1) COBITキューブ

IT プロセス、情報規準(クライテリア)、IT 資源の３次元空間。ビジネスの要求事項を可能にするＩＴプロセス、そのＩＴプロセスを支えるＩＴ資源の状況を把握し、情報規準の観点からコントロールする。各要素は下記の通り。

ａ）ＩＴプロセス

ドメイン、プロセス、アクティビティへとブレークダウンされる。

ｲ) ＩＴドメイン

計画と組織、調達と導入、
デリバリーと支援、モニタリング
からなる。

ﾛ) ＩＴプロセス

ＩＴ戦略、方針と手続き、
フィージビリティスタディ、
受け入れテスト、変更保守管理、
コンティエンジェンシー策定、
問題管理、等から成る

ﾊ) 活動（アクティビティ）

新しい問題の記録、分析、
ソリューション提起、
ソリューションのモニタ、
既知の問題記録から成る

ｂ）ＩＴ資源

人、アプリケーション、技術、施設、
データに分類される。

ｃ）情報規準（クライテリア）

←ビジネス要件

ｲ) ビジネス要件

下記３つの要素で構成される。

・品質要件（Q、C、T）
・受託責任（ＣＯＳＯレポート）
・セキュリティ要件
（機密性、インテグリティ、可用性）

ﾛ) クライテリア

下記の７つで構成される
有効性、効率性、機密性、
インテグリティ、可用性、
準拠性、信頼性

③コントロール目標

３４のプロセス毎に３～３０項目の詳細コントロール目標が設定されている。

④監査ガイドライン

公開許可が得られないところということで、英文のままの資料ですが、どう監査するかの観点が書かれています。

⑤管理者ガイドライン

肝は下記の事項。

・戦略的な選択とベンチマークのための成熟度モデル
・プロセスを適切にコントロールするためのＣＳＦ
・ＩＴプロセスのゴール達成をモニタするためのＫＧＩ
・各々のＩＴプロセスのパフォーマンスをモニタするためのＫＰＩ

２．質疑応答

Q: COBIT が監査証明となりうるのか？アメリカでの動向を知りたい。

A: AICPA の SysTrust が COBIT をベースにしていると聞く。だとすれば COBIT は保証サービスの規範になりうる。

Q:「モニタリング」の意味は？第三者的なものか？

A: ここではまず経営者が結果に向けた過程

(KPI)をモニタリングするということ。

Q: ビジネス要件のクライテリア（有効性、効率性、機密性、インテグリティ、可用性、準拠性、信頼性）について、個々の違いがよくわからないが

A: COBIT の管理者ガイドライン Appendix にその説明が、また個々のプロセス別の Control Objectives との関係は「Control OBJECTIVES」の冊子が一番分かりやすく、参照してほしい。

Q: COBIT を使ってシステム監査をする上で、どう感じるか？

A: 日本のシステム監査基準はざっくりしたものであるが、COBIT は「何を守るために何が必要なのか、マネジメント要件と関わる IT 要件」の関係を示唆しているので、関係が明らかになり、分かりやすい。

Q: COBIT 自体はかなり構造化された形になっているが、クライテリアの定義については、きちんと定義できないような世界があるのではないかと思われるが、どうか。個人の判断で決める部分があるという認識でよいのか？

A: おっしゃるとおりで、クライテリアの部分の定義は難しい。(ISACF のような)一定の権威のガイドラインに先ず従って見ていくのが現実だと思う。

３．感想

上川さんのお話は、言葉を選び、内容を簡潔に伝えるものでした。また配布された資料は IT ガバナンス協会の公開資料を基に、全編をバランスよくサマライズしたものであったことも、全貌が把握できた大きな理由だったと思います。

ＩＴコーディネータのなかでもＣＯＢＩＴは重視されているのですが、翻訳されたものとしては成熟度モデルの部分やＩＴプロセス毎に設定されたＫＧＩ／ＣＳＦ／ＫＰＩの表、プロセス別コントロース目標の表など断片的なものだけでしたので、当日多かった IT コーディネータとしての参加者は霧が晴れたという共通認識をもたれたのではと思います。

短い講演時間だけではＣＯＢＩＴの全体を伝えきれるものではありませんが、上川さんは１０４頁にも及ぶパワーポイント資料を配布してくれました。これを読むことが全貌把握の早道だと思います。

上川さんは我々と同じシステム監査技術者ですが、その多彩な能力と活躍ぶりには驚きます。大変多くのことのを学び、刺激を受けることが出来ました。この様な方を探しあて、講演をして下さることを説得してくれ、研究会を盛り上げて下さった影の関係者にも深くお礼申し上げます。また当報告は No.706 原田奈美 理事が公演中に書いて下さったメモを基に記述しております。質疑応答の部分など、的確なまとめに助けられております。

以上