認定NPO法人
日本システム監査人協会報
2017年8月号
No 197
No.196（2017年8月号）<7月25日発行>

会員増強、協会活性化に向けた皆様の忌憚のないご意見をお願いします。

写真提供：仲　会長

巻頭言

今年度も「会員向け活動説明会」を開催します

会員番号 6027 小野修一（副会長）

活性化委員会では、会員増強を活性化に係る重要事項として位置づけ、さまざまな取組みを行っています。会員を増やすためには、新規会員を増やすことと、既存会員の退会を減らすことの両方の取組みが必要です。

新規会員の入会促進のための取組みとしては、月例研究会などのイベントに参加された未入会の方に協会入会のメリットを説明して入会を働きかけること、システム監査技術者試験の試験会場での入会案内チラシの配布などを行っています。

会員を継続していただくためには、研究会などに参加していただき、協会との接点をもっていただくことが効果的であると考えており、そのためのイベントとして、昨年度、「会員向け活動説明会」を開催しました。結果として、活動説明会に参加された会員のうちの何人かが新たに研究会に参加され、活動されています。昨年度の活動説明会に参加された方にお願いしたアンケートでも、こうした会を定期的に開催した方がよいというご意見が多く見られたこともあり、活性化委員会では、今年度も「会員向け活動説明会」を開催することを決定し、準備を進めています。開催日時は**10月21日（土）の午後**、開催場所は昨年度と同じ、茅場町の事務所の近くの貸会議室を予定しています。現在、会の内容について企画・準備を進めています。

今年度の活動説明会開催のご案内、参加者の募集は8月下旬からを予定しています。東京での開催になりますが、参加してみたいという会員の方は、全国、どなたでも歓迎です。

会員を増やし、協会を活性化するための取組みを、活性化委員会では検討、実施しています。10月21日の「会員向け活動説明会」への参加をお待ちするとともに、会員増強、協会活性化についてのご意見をお寄せいただきたく、お願いしたします。　　以　上

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。

＜目次＞

2017.7

めだか　【　[美女と野獣」と魔法使いと　】

美女と野獣は実写版映画も面白い。映画館で映画の世界に入り込むと心が揺さぶられる。野獣の心の中の優しさが、よみがえり育っていくと、自分の心が寄り添ってしまう。

野獣に比べて、見かけは素敵な戦場の英雄が、実は利己主義と戦いを好むだけの「こころの野獣」であり、映画の中で唯一の死者である。多くの村人は表面だけしか見えていないし、目の前にいるオピニオンリーダーの意見だけで動いてしまう。自分自身の心の目で見ないままで、人を傷つけようとしてしまう。もちろん、映画の観客は「自分は違うよ」と思いながら客席という安全地帯から眺めているので、映画を楽しめる。

物語の概略は次のとおりである。ある王様がわがままに育ってしまい、自分の楽しみだけで行動し、他人や社会全体の苦しみを理解できなくなっていた。この状況の裏にある真因を知った魔法使いが、王様を野獣に変えてしまった。その時に、改善の期限を明確に示し、改善のツールもいくつか残しておいた。さらに、期限が迫った時に、美女を派遣し、積極的に改善活動をさせた。デッドラインを超えるときに、王様の心はよみがえった。全体のイベントをコントロールしていたのは魔法使いともいえる。但し、人々の心を魔法で変えたのではなく、人々が自ら行動し変化するようにしむけたのである。

さて、企業や組織が活動では、「必要悪」などという奇妙な概念が正当化されているケースがある。あるいは、「個別には正しい努力をしているが、全体では何かおかしい」と感じるが何もできないことがある。むしろ、「変化をさせようという努力が悪である」とみなされるのが通例かもしれない。このような時に、監査人は何をどのようにすべきか。定型化した監査には限界がある。つまり、監査チェックリストと実態を比較する作業は、実態が劣化する業務システムに警鐘を鳴らせるだろう。しかし、チェックリスト自体も経時劣化や表面的な監査対策により、問題を検出できなくなっている場合もあるだろう。

これに対して、監査自体の問題点も探し続けることが必要である。国際標準は更新され続けているし、ITの大衆化も急激に拡大しているし、地球規模のITリスクも高まっている。そのような中では、監査の視点も方法も積極的に改善を進めるべきである。

企業や組織所属していても、状況認識を充分にできる監査人となって、現在の状況と不具合点の兆候を感じ、真因を洞察することが重要である。そして、長期的鳥瞰的な戦略を構築し、ピンポイントで警鐘を鳴らし、改善の方策も示す。しかも、かかわっている人々が自らの信念で行動していくように仕向ける。そうすると、企業や組織の文化が変わっていく。

私は、システム監査人として、この魔法使いのようになりたい。（佐官眼智）

（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>

2017.7

めだか　【　システム監査とＩＴガバナンス - コーポレート・ガバナンス　】

システム監査とITガバナンスを考えるにあたって、先ず、コーポレート・ガバナンスについて考えたい。コーポレート・ガバナンスは、「G20／OECDコーポレート・ガバナンス原則」（以下、OECD原則）が世界標準であり、日本のコーポレート・ガバナンス・コードも整合している。OECD原則の６原則を挙げる。

1．有効なコーポレート・ガバナンスの枠組みの基礎の確保：コーポレート・ガバナンスの枠組みは、透明で公正な市場及び資源の効率的な配分を促進するべきである。また、法の支配と整合的で、実効的な監督と執行を支えるものであるべきである。

2．株主の権利と公平な取扱い及び主要な持分機能：コーポレート・ガバナンスの枠組みは、株主の権利を保護するとともにその行使を促進し、少数株主、外国株主を含む、全ての株主の公平な取扱いを確保するべきである。全ての株主は、その権利の侵害に対して、有効な救済を得る機会を有するべきである。

3．機関投資家、株式市場その他の仲介者：コーポレート・ガバナンスの枠組みは、投資の連鎖（investment chain）全体を通じて健全なインセンティブをもたらし、良いコーポレート・ガバナンスに貢献するような形で株式市場が機能することを支援するものであるべきである。

4．コーポレート・ガバナンスにおけるステークホルダーの役割：コーポレート・ガバナンスの枠組みは、法律又は相互の合意により確立されたステークホルダーの権利を認識するべきであり、会社とステークホルダーの積極的な協力関係を促進し、豊かさを生み出し、雇用を創出し、財務的に健全な会社の持続可能性を高めるべきものである。

5．開示及び透明性：コーポレート・ガバナンスの枠組みにより、会社の財務状況、経営成績、株主構成、ガバナンスを含めた、会社に関する全ての重要事項について、適時かつ正確な開示がなされることが確保されるべきである。

6．取締役会の責任：コーポレート・ガバナンスの枠組みにより、会社の戦略的方向付け、取締役会による経営陣の有効な監視、取締役会の会社及び株主に対する説明責任が確保されるべきである。

OECD原則で使われている「取締役会（board）」は、「監査委員会（supervisory board）」を意味し、「幹部経営陣（key executives）」は、「経営役員会（managing board）」を意味することになる。「情報技術 – ITガバナンス（JIS Q 38500：2015）」では、上部のITガバナンスと基部の事業プロセスに分けて相互の働きをモデル化している。OECD原則を参照して「情報技術 – ITガバナンス（JIS Q 38500：2015）」を理解する必要がある。（空芯菜）

（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>

2017.7

投稿　【　システム監査の展開　】

会員番号 0557 仲厚吉　（会長）

当協会では、「システム監査」を核とした「ITガバナンス」、「ITアセスメント」、及び「ITアセッサ」の定着を図るようにITアセスメント研究会（松枝憲司主査）が次の課題に取り組んでいます。

(1)ITガバナンスに関連する事項

a) JISQ38500：2015の活用と普及に関すること

b) ISO/IEC38500関連基準（38501,2,4,5）の日本語化

c) ISO38503（Assessment of the governance of IT: ITガバナンスの評価基準）のISO化支援

(2)システム管理基準の改訂、活用等

現状のシステム管理基準を現場でより活用できるよう補足・改訂等を研究する。

また、システム監査の展開をテーマとして、「ITガバナンス」の6原則、「情報セキュリティガバナンス」の6原則により、ITと情報セキュリティのアセスメントを行っていくことは重要であると思います。

「ITガバナンス(JIS Q38500:2015)」の6原則	「情報セキュリティガバナンス（JIS Q27014:2015）」の6原則
①　責任	①　組織全体の情報セキュリティを確立する。
②　戦略	②　リスクに基づく取組みを採用する。
③　調達	③　投資決定の方向性を設定する。
④　パフォーマンス	④　内部及び外部の要求事項との適合性を確実にする。
⑤　コンフォーマンス	⑤　セキュリティに積極的な環境を醸成する。
⑥　人間行動	⑥　事業の結果に関するパフォーマンスをレビューする。

ITガバナンス6原則と情報セキュリティガバナンス6原則は文言や順位が少し相違していて、なかでも、ITガバナンス“⑥人間行動”と、情報セキュリティガバナンス“⑤セキュリティに積極的な環境を醸成する。”は原則が違っているようにみえます。

しかし、「情報セキュリティガバナンス（JIS Q27014:2015）」を読むと、“⑤セキュリティに積極的な環境を醸成する。”の説明は、“情報セキュリティガバナンスは、人間の行動に基づいて構築することが望ましく、これには全ての利害関係者の変化するニーズが含まれる。なぜならば、人間の行動は、適切なレベルの情報セキュリティを支持するための基本的な要素の一つであるからである。様々な利害関係者の目的、役割、責任及び資源間の調和、調整などが不十分な場合は、これらが互いに摩擦を起こし、その結果、事業目的の達成に失敗することになる。したがって、様々な利害関係者の間の調和及び方向性の一致が極めて重要である。・・・”としています。

二つの6原則は同様の原則であり、管理策は別にして、同様に取り組んでいけばよいと考えられます。

<目次>

2017.7

特別月例研究会：講演録

【IT ガバナンスの国際規格（ISO/IEC 38500 シリーズ）と今後の展開について】

～各国の IT ガバナンスの現状と国際標準の活用～

会員番号　0124 原善一郎、2506 野嶽俊一（IT アセスメント研究会）

【日時・場所】2017 年 6 月 3 日（土）13:00～16:45　機械振興会館地下 2 階ホール

【テーマ】IT ガバナンスの国際規格（ISO/IEC 38500 シリーズ）と今後の展開について

～各国の IT ガバナンスの現状と国際標準の活用～

【主催】一般社団法人 情報処理学会　【共催】認定 NPO 法人日本システム監査人協会

【後援】日本 IT ガバナンス協会、ISACA 東京支部、大阪支部、名古屋支部、福岡支部

システム監査学会、情報セキュリティ大学院大学、日本セキュリティ・マネジメント学会

金融情報システム開発センター

【要旨】

本セミナーでは、企業や組織で IT ガバナンス、IT 投資、システム監査、情報セキュリティ等を担当している方々を受講者として想定し、本分野に関する国際標準化とその実務に携わる専門家 3 名を選定した。講師の方々には、各々が関連する最近の IT ガバナンス、コーポレート・ガバナンス事案の紹介、国際動向、また、JTC 1/SC 40 で作られた国際標準がその解決、防止にどのように役立つのか、実際にどのように使われているのか等をご講演いただいた。

そして本セミナーを通し、SC 40 が策定している国際標準への理解とさらなる活用、適切で効率的な組織の IT ガバナンスの対策推進を期待したいと考えている。

【講演録】

<オープニング>

【コーディネータ】平野 芳行 氏（JTC 1/SC 40 専門委員会　委員長）

JTC1 の活動は以下の通り：

IT ガバナンス及び IT サービス管理に関する標準、ツール、枠組み、ベストプラクティス及び関連する文書を作成。その IT 活動領域には、監査、デジタルフォレンジック、ガバナンス、リスクマネジメント、アウトソーシング、サービス運用及びサービス維持が含まれる。

尚、SC27（セキュリティ）及び SC38（クラウドサービス環境）の適用範囲は除外。

[ISO]　　[IEC] ISO と IEC が共同で JTC1 を立ち上げ

＼　／

[JTC1] Joint Technical Committee 1（第一合同技術委員会）

｜

[Many SCs]　多くの Sub Committee（分科委員会）が存在

｜

[SC40] IT サービスマネジメント＆IT ガバナンス [←今回のテーマ]

｜

＋－[WG1] IT ガバナンス

｜

＋－[WG2] ISO/IEC 20000 の維持及び開発

｜

＋－[WG3] ITES-BPO (IT-enabled service business outsourcing)

｜

＋－[WG4] IT サービスマネジメントインフラストラクチャ

＜ビデオメッセージ（セッション１）＞

【テーマ】IT Governance in SC40WG1

【講師】　Peter Brown 氏（SC40WG1 Convener）

※Brown 氏は、イギリス国内で BSI のコーポレート・ガバナンスの代表者

【翻訳】　原田 要之助 氏（情報セキュリティ大学院大学）

・WG1 にて"IT ガバナンス"と"コーポレート・ガバナンス"の整合性を取る。

（発行済み）

①ISO/IEC/TS 38500

・IT ガバナンスのコアスタンダード

②ISO/IEC/TS 38501

・IT ガバナンスのインプリメンテーション

③ISO/IEC/TR 38502

・IT ガバナンスのストラクチャード・モデル及びプリンシプル

（supporting 規格）

④ISO/IEC/TR 38504（2016/09 発行）

・テクニカルレポート及びプリンシプルの作り方（企画を作る為の企画）

⑤ISO/IEC 38505

・ビッグプロジェクトのひとつ。データマネジメントのガバナンス

（最新発行した規格）

⑤-1 ISO/IEC 38505-1（2017/04 発行）

・コアプリンシプル

（開発中の規格）

⑤-2 ISO/IEC 38505-2

・マネジメント層のリスクコントロール

⑤-3 付録：ケーススタディー（中国でのケース）

・データマネジメント、データガバナンスのベストプラクティス

⑥ISO/IEC 38506（2018～2019 年の発行を目指す）

・IT イネーブル・サービス

・製品、サービス、サプライチェーン等に対するガバナンスおよびリスクマネジメント

（プロジェクトの見直し（missing））

⑦ISO/IEC 38503

・IT ガバナンスのアセスメント

－当初は"Auditing"で進めていたが日本からのインプットだけでは不足

・Auditing と Governance の関係を見直す

－Audit　　：単発的なもの

－Assessment：継続的なもの（←こちらにフォーカスを当てる）

ボードが内部からどのようにプロセシングしていくか？

ガバニングボディからのコントロールが重要

（将来）

⑧ISO/IEC 38502 の更新

＜セッション２＞

【テーマ】Strategies for the world of data / Governance of IT within Microsoft

【講師】　Geoff Clarke 氏（マイクロソフト　アジア地域標準化マネージャ）

○Strategies for the world of data

・組織は適切な戦略を築いているか？：目的の明確化

・ガバニングボディの役割：投資の決定

（直訳は難しいのでカタカナ表記[日本では「取締役会」に近い]）

・リスク：不確実性（何もしないのもリスク）、リスクアペタイト（リスク選好）が重要

・制約：外部要因および組織の規範

・組織が作る「データ」の戦略：ビジネス戦略全体をサポート

・バズワードが実際のものに：ユーザはそれを認識しているか？

・時代は変わった：全てのビジネスは「データ」に影響を受けている

Ex) UBER：データによって TAXI 業界を変革した

・ユーザのデータを吸い上げて製品やサービスを向上：

個人情報やオプトアウトはどうする？

潜在的なリスク（セキュリティやプライバシー）

法的な責任にどう対処して行くか？

・マイクロソフト：「パッケージソフト」から「クラウドサービス」へ変革

・全てのビジネスは「データビジネス」へ：ガバナンスフレームワークを持つことが必要

ステークホルダーは何を望んでいるか？

ガバニングボディは全ての責任を負う

ビジネスはデータを最大限活用しているか？

データのアクセスコントロールは適切か？

・ISO/IEC 38505 Governance of Data のデータアカウンタビリティ・マップ

18 のマトリックス（38505-1：データ戦略～データ方針）

	Value（価値）	Risk（リスク）	Constraints（制約）		Policies（管理策）
Collect（収集）					
Store（格納）					
Report（レポート）					
Decide（決定）					
Distribute（配付）					
Dispose（廃棄）					

↑　↑　↑

※38505-2 では Policies が加わる

・ISO/IEC38505 を用いて　データ戦略～データ方針～データ管理　の体制を構築は、「データ集積と利用」の高度化により、ビジネス構想や業界項構造が変化する時代に企業が生き延びる必須条件

○Governance of IT within Microsoft

・マイクロソフトの IT ガバナンスは 4 つのエリアからなり、デジタルトランスフォーメーションを支える

デジタル戦略

スキル

カルチャー

サクセス

・マイクロソフトの IT 部門：

顧客（組織内部）向けサービスを提供しマイクロソフトの変革そのものを支えている

・People / Process / Technology がキーワード

・企業運営費（営業費用）の 5%を IT 投資に活用：

この 5%が残りの 95%に好影響を与える

・マイクロソフトのセキュリティガバナンス：

IRMC (Information Risk Management Council) によってコントロールされている

・CIO による経営層への透明性の確保

ガバナンスの明確化

BI ダッシュボード

サイバーセキュリティ

・成功要因(CSF)

エンド to エンド・エクスペリエンス

アウトカムベースド KPI

イネーブリング・データセキュリティ

データインパクト

＜セッション３＞

【テーマ】第 1 部「IT ガバナンスの海外における現状」

第 2 部「今後のデジタルトランスフォーメーションのガバナンスについて」

【講師】　原田 要之助 氏（情報セキュリティ大学院大学教授）

(1)IT ガバナンスの各国の現状

SC 40 に来日した IT ガバナンスの専門家へのインタビューをとりまとめて報告した。ISO/IEC 38500 が国際規格となって 5 年経過した。日本でも 2015 年に JIS Q 38500 となっている。

また、政府の IT 関連の資料では IT ガバナンスがよく使用されている。先進国では、OECD のコーポレート・ガバナンスの指針が出たことや株式市場の活性化のためにコーポレート・ガバナンスは重視されている。日本でも安倍政権は、成長戦略の重点課題としてコーポレート・ガバナンス・コード及びスチュワードシップ・コードを作成して、企業経営の透明化と投資家に日本企業の信頼性向上を図っている。今日では IT が経営と密接な関係となっているため、IT ガバナンスはコーポレート・ガバナンスの一部を担う観点からも、企業の経営者にとって重要なものとなってきている。

今回は、IT ガバナンスの規格について議論するために SC 40 に来日した各国の有識者に IT ガバナンスの現状と課題について語ってもらった。発表では、この内容を紹介した。

インタビュー対象国：

①オーストラリア、②南アフリカ、③オランダ、④ポルトガル、⑤中国

インタビュー内容：

1. IT ガバナンスのガイドラインはありますか（政府，民間を問わず）

①②：あり、③④：なし、⑤：国内規格準備中

2. IT ガバナンスのカバー範囲は、IoT や AI など新しい IT 分野を含んでいますか
①：あり、②：普及低、③：これから、④：なし、⑤「IT 治理」: IT ガナバンス
3. 企業の経営者は IT ガバナンスについての認知度は高いですか
①：高い、②：IT の問題、③：中小はこれから、④：これから、⑤：政府主導
4. 経営で IT を重視しているか（IT は企業経営にとって莫大な投資やセキュリティなどの運用費がかかります。経営者は、この事実をどう捉えていますか
（仕方がないと捉えている企業が多いのか、前向きに捉えているか））
①：積極的、②③：消極的、④：関心薄、⑤：政府主導
5. ISO/IEC 38500 や ISO/IEC 27014 などの IT に関するガバナンスの規格の各国における位置づけはどうなっていますか。ある場合には利用されていますか
①②：採用、③④⑤：不採用
6. 政府の IT ガバナンスの取り組み方（政府内部に IT に関する責任ポストはあるか）
①②⑤：あり、③④：なし
7. 政府や企業がITのトラブルや情報漏えいが起きたときにはITガバナンスの問題と捉えられているか（年金機構の情報漏えいの場合には政府が IT のガバナンスの問題として、長官が謝罪会見をした)、各国で、このよう場合の取り組みはどうなるか
①：長官や CEO、②組織 No.2、③④：事例なし、⑤：事例による
8. IT ガバナンスの普及に向けて各国で進めている方策について
①②：推進中、③：国内規格（BiSL）と併せて、④⑤：セミナー等
9. システム監査は IT ガバナンスにとって重要な機能と考えていますか。監査以外に IT ガバナンスの実効性を担保するのは何ですか
①②：民間・政府共に実施、③：政府機関等、④：一部で実施、⑤：実施
10. グローバルな IT ガバナンスは必要ですか。その場合、ISO/IEC 38500 が役立ちますか。
①③：必要、②：不明、④：EU 内で必要、⑤回答保留

(２)今後のデジタルトランスフォーメーションのガバナンスについて

○ガバナンス

・プリンシパル＝エージェント理論：
株主と経営者の利益は必ずしも一致しない：コーポレート・ガバナンスの必要性
企業の利害関係とステークホルダーの要求をコントロールする

・組織を正しい方向に導く考え方：エンロン事件から SOX 法制定へ

・コーポレート・ガバナンス・コード：
組織のガバナンスに対する指針
リーマンショック後の組織のガバナンス強化策
主要国で導入済み。日本でも安倍政権下で推進

・シュチュワードシップ・コード

機関投資家などによる投資先企業の株主総会などへの行動原理

米国には存在しないが、日本では存在

・TC309 コーポレート・ガバナンスの規格化

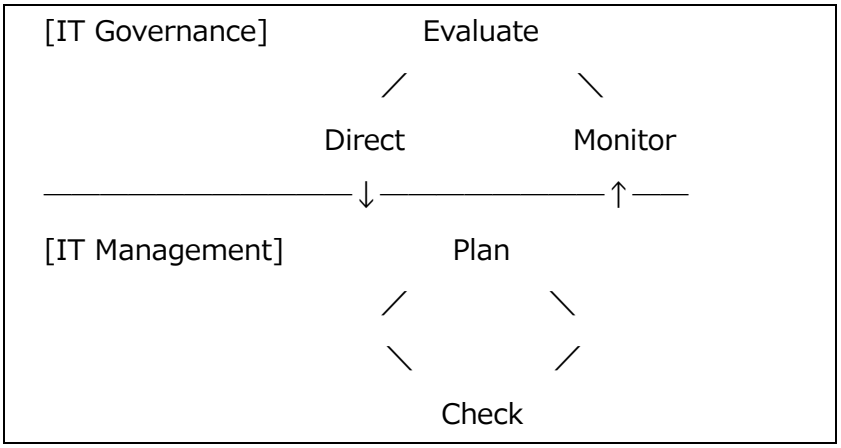
日本でも経産省が検討。但し各国の動向を伺う程度

○IT ガバナンス

・コーポレート・ガバナンスの一部

・EDM モデル (Evaluate[評価]、Direct[指示]、Monitor[監視]：経営層

・下位に IT マネジメントによる PDCA モデル：マネジメント層



・情報セキュリティガバナンス

JIS Q 27014:2014 にて規定されるも、IT ガバナンスとの重複部分の議論が必要

○デジタルトランスフォーメーション

・アルビン・トフラー「第三の波」（1980 年）にて提唱：情報化、デジタル化

・BPR の次にくる段階：ビジネスそのものを変えてしまう

Kodak 社の事例：写真フィルムのトップベンダの倒産

NTT 社の事例：電話回線からインターネットへ。従業員 30 万人が数分の一に

・デジタル化の脅威はボードメンバの責任

IT ガバナンスはデジタル化まで見ていかないとダメ

「IT による効率化、IT の利活用」しか見ていないと、取り残される

＜原善一郎の感想＞

ISO/IEC38503　IT アセスメント　を規格として発行するための見込みが見えていない。

何をすれば進むのかを見直す必要がありそうである。

＜野嶽俊一の感想＞

各国の背景や制度・国民性等により、用語に対する認識が異なるのは致し方ないところではある。

しかしながら、「Audit（監査）」に係わる見解が異なるのは如何なものか。日本においても監査は決して単発的や一時的だけのものではない。継続的な監査やフォローアップを含めた指摘事項の改善に係わる検証も行っている。そもそも監査における「３つのコントロール（予防的コントロール、発見的コントロール、是正的コントロール）」も含め、JTC1/SC40 に正しく伝えていく必要があるのではないか。

勿論、組織を生かすも殺すもその責任は Governing body にある事は論を待たない。しかしながら Governing body がミスリードをしてしまいそうな時、（内部であろうが外部であろうが）Audit が有効に機能すべきではないのか？

先ず Governing body による Assessment があり、さらに Auditor による Audit という２段構えによる Governance の実現が、より有効であろうと考える。

また日本国内においても、コーポレートガナバンスと IT ガバナンスを分離して考えず、コーポレートガナバンスに寄り添う形で IT ガバナンスが整合性を取っていく必要があろうと考える。

＜目次＞

2017.7

第３１回ＣＳＡフォーラム開催報告
【クラウドセキュリティと監査、FISC、FINTECH 最新動向】

会員番号　2581 斉藤 茂雄（CSA 利用推進 G）

第31回は、一般社団法人クラウド利用促進機構運営委員の渥美俊英様に講師をお願いしました。渥美様は株式会社電通国際情報サービスで永く金融系システムの開発を経験され、その後アマゾンウェブサービスジャパンに入社、クラウド利用支援業務を担当し、退職後も引き続きいくつかの企業でクラウド利用推進の顧問役、アドバイザを担っています。また業界での活動も多く、業界基準やガイドラインの整備に携わっておられます。フォーラムでは、AWSクラウドの成長の姿、大手企業におけるAWS活用のインパクト、メガバンクでのAWS採用などの紹介がありました。また、FISC安全対策基準のクラウドに関する変更やFINTECH最新動向など盛り沢山のお話をいただきました。

クラウド利用がSaaS事業者のサービスを利用するだけでなく、企業が基幹システムの構築・運用環境として利用して、システム構築のコストダウン、開発の俊敏化などの大きな成果を産む時代になっていることを改めて知りました。今後システム構築のスタイル、組織、監査方法など、システム部門や監査のあり方が大きく変貌していくだろうことを強く感じた２時間でした。

開催の概要は以下です。終了後講師を囲んで短時間ですが懇親会を実施しました。

タイトル：「クラウドセキュリティと監査、FISC、FINTECH 最新動向
～メガバンクがクラウドを採用する背景～」

概要；（当日使用スライドのコンテンツより抜粋）：

① **AWS クラウドの進化と真価、セキュリティと統制の新段階**
IaaS・PaaS 市場の動向/AWS の機能拡張・改善のスピード/90 以上の AWS サービス群/大手企業が語る AWS の価値/AWS のセキュリティ、統制/SOC2 監査報告書とは？/AWS のセキュリティの進化

② **金融機関のクラウド利用事例　ソニー銀行、JNB、MUFG**
AWS サミット 2017 注目の話題 その１つは、“金融機関の AWS 利用”/クラウド利用事例

③ **安全対策基準と金融機関向け AWS セキュリティリファレンス**
FISC 安全対策基準 第８版追補改訂-クラウドに関する主な変更点/FISC 対応 AWS セキュリティリファレンス　1.3 版 構成

④ **国内 FINTECH と海外の動向、金融庁、FISC の動き**
FINTECH、始まりは米国/人材、資金から一気に FINTECH が増大/日本における FINTECH の動き/金融機関のデジタルイノベーション像/金融庁の FINTECH への動き/ FINTECH への具体的アクション/FINTECH に関する有識者検討会報告書/金融イノベーションを支えるコミュニティ

⑤ **製造業、公共調達とクラウド**
製造業界、日本自動車工業会でもクラウド利用推進/公共系でも AWS 利用推進の動き

開催日時： 2017 年７月 10 日（月） 18 時 30 分～20 時 30 分

開催場所： 中央区日本橋兜町 12-7 兜町第３ビル　NATULUCK 茅場町新館２階大会議室

ＣＳＡフォーラムはＣＳＡ・ＡＳＡの皆様が､｢システム監査に関する実務や事例研究､理論研究等｣を通して､システム監査業務に役に立つ研究を行う場です。ＣＳＡ・ＡＳＡ同士のフェイスｔｏフェイスの交流を図ることにより、相互啓発や情報交換を行い、ＣＳＡ・ＡＳＡのスキルを高め、よってＣＳＡ・ＡＳＡのステータス向上を図ります。ご参加のお問い合わせはＣＳＡフォーラム事務局：csa@saaj.jp まで（@は小文字変換要）

ＣＳＡ利用推進Ｇのキャッチフレーズ
＊＊ＣＳＡ・ＡＳＡを取得してさらに良かったと思ってもらえる資格にしましょう！！

＜目次＞

2017.7

支部報告【北信越支部 2017 年度 福井県例会・研究報告】

会員番号　1281 宮本　茂明（北信越支部）

以下のとおり2017年度 北信越支部福井県例会を開催しました。

・日時：2017年6月10日（土） 13:00-17:00　　参加者：6名

・会場：福井市総合ボランティアセンター 研修室B

・議題：１．研究報告

「ＩｏＴのセキュリティと監査の方向性について」　　小嶋　潔　氏

「匿名加工情報の取扱いについて」　　宮本　茂明　氏

２．西日本支部合同研究会 北信越支部報告検討

◇研究報告　1

「ＩｏＴのセキュリティと監査の方向性について」

報告者 (会員番号　1739　小嶋　潔)

１．はじめに

今日、IoT は速に普及しつつあり、2020 年にはインターネットにつながるモノは 200 億個とも 500 億個とも予想されています。IoT を利活用することで、様々なイノベーションや経済成長を促すことが期待されており、政府も「日本再興戦略」において強力に推進していることから、新聞で IoT に関する記事を見ない日はないと言っても過言ではないような現状です。このような明るい未来予想の一方で、IoT はモノがＰＣ化してインターネットにつながるようなものなので、ＰＣやスマホと同様にサイバー攻撃等の脅威にさらされることになります。

政府やＩＰＡ等からは、セキュリティガイドライン等が相次いで発表されており、IoT の開発等に関しては一定の方向性が示されています。しかし監査に関しての取組みは、あまり情報がなく、まだまだこれからという感じがします。個人的にも IoT についてあまり深く考えたことはなかったのですが、今回 IoT をテーマに取り上げ、システム監査において IoT をどう取り扱うべきか、その方向性について検討してみました。

２．IoTのリスクとセキュリティ

IoT には大きな成長や付加価値が期待される一方で、情報セキュリティの確保に加え、生命の危険への対策をも含む安全確保が必要となります。コネクテッドカーやスマートハウスのように長期間の利用や不具合が発生した場合には生命に危険の及ぶようなモノ、センサー機器のようにリソースに制約があるモノ、多様な性質を持った機器やネットワークで構成されていたり、このような IoT システムやこれを利用したサービス特有の性質を踏まえたセキュリティ対策の検討が必要です。平成 27 年 9 月閣議決定のサイバーセキュリティ戦略においても、IoT 機器やシステム、サービスのセキュリティが確保された形での新規事業の振興やガイドラインの策定等の制度整備、技術開発等を進めることとされています。

IoT のリスクには、①脅威の影響範囲や度合いが大きい、②IoT 機器のライフサイクルが長い、③IoT 機器の監視が行き渡らない、④IoT 機器のネットワーク側の環境や特性の相互理解が不十分、⑤IoT 機器の機能性能が限られている、⑥開発者が想定しない接続が行われる可能性がある、といった特徴があります。

3．IoTに関する開発指針やガイドライン

（1）「つながる世界の開発指針」IPAソフトウェア高信頼化センター　2016年3月

IoTのリスクに対して早急に対策を行う必要があるということで、IoTのリスクに対して守るべきものを守れる機器やシステムを開発することは、国際競争力の強化にも寄与すると期待されるとして、様々なモノがつながって新たな価値を創出していく「つながる世界」ならではの機器やシステムに関わる企業が、安全安心に関して最低限考慮すべき事項を「つながる世界の開発指針」としてとりまとめたものです。

（2）「IoT セキュリティガイドライン」IoT 推進コンソーシアム、総務省、経産省　平成 28 年 7 月

本ガイドラインは、IoT機器やシステム、サービスの供給者及び利用者を対象としてサイバー攻撃などによる新たなリスクが、モノやその利用者の安全や、個人情報・技術情報などの重要情報の保護に影響を与える可能性があることを認識したうえで、IoT機器やシステム、サービスに対してリスクに応じた適切なサイバーセキュリティ対策を検討するための考え方を、分野を特定せずにまとめたものです。

（3）「安全な IoT システムのためのセキュリティに関する一般的取組」内閣サイバーセキュリティセンター　平成 28 年 8 月 26 日

IoT システムについては、モノが接続されることから、IT と物理的システムが融合したシステムとして捉える必要があり、同システムが提供されるサービスには、従来の情報セキュリティの確保に加え、新たに安全確保が重要となります。また、将来個々のシステムが相互に接続されることを見据え、システム相互間の接続が新たな脆弱性となる懸念があることを踏まえ、セキュリティ・バイ・デザインの思想で設計、構築、運用されることが不可欠です。

こうしたことを実現するためには、早急にすべての IoT システムに係る設計、構築、運用に求められる事項を一般要求事項として明確化し、その上で、個々の分野の特性を踏まえた分野固有の要求事項を追装する 2 段階のアプローチが適切であると考えられます。本枠組は、こうした考え方に基づき、安全なIoTシステムが具備すべき一般要求事項としてのセキュリティ要件の基本的要素を明らかにすることを目的とします。

（4）「IoT 開発におけるセキュリティ設計の手引き」独立行政法人情報処理推進機構技術本部セキュリティセンター　2016 年 12 月

IoT のセキュリティ設計を担当する開発者に向けた手引きとして、参考となる情報をまとめたものです。最初に対象とする IoT を明確化するために、IoT の全体像をモデル化し、各々の構成要素を定義し、次に IoT のセキュリティ設計において行うべき、脅威敏席・対象検討・脆弱性への対応について解説し、セキュリティを検討する上で参考となる、IoT の円のセキュリティガイドを紹介しています。そしていくつかの例題をもとに、IoT システムにおける脅威分析と対策検討の実施例を示しています。

4．IoT に関する開発指針やガイドラインの内容・特徴

前述の各種指針やガイドラインは、基本的には下記のような共通認識のうえに策定されています。

（１）IoT 特有のリスク

（ア）想定しないつながりが発生する

・メーカー以外の事業者でも容易に IoT サービスを構築できるし、ユーザが興味本位でつなげてしまうケースもありえます。このため想定しないつながりが発生し、外部からの攻撃や情報漏洩も懸念されます。

（イ）管理されていないモノもつながる

・企業の情報システムと異なり、IoT には管理担当者がいないモノもつながります。（自動車や家庭の住宅設備、ウェアラブル機器、果ては廃棄される機器など）このため、悪意ある者が直接機器やシステムに不正なソフトウェアを埋め込んだり、廃棄された機器からデータやソフトウェアを読み出すことも比較的容易です。長期間経過して、適切に保守されていないものも混在します。

（ウ）身体や財産への危害がつながりにより波及する

・家電や自動車等、事故や誤操作により身体や生命の危険、財産に損害を及ぼす可能性があります。単体なら範囲は限定的でも、つながることで被害が広範囲に波及することも懸念されます。

（エ）問題が発生してもユーザにはわかりにくい

・物理的な故障は分かりやすいのですが、ソフトウェア上の問題は目に見えません。IoT ではつながることによる問題が発生してもユーザが気付かない可能性が高くなります。

（２）IoT のセキュリティ対策

（ア）IoT の性質を考慮した基本方針を定める

・経営者が IoT セキュリティにコミットする

・内部不正やミスに備える

（イ）IoT のリスクを認識する

・守るべきものを特定する

・つながることによるリスクを想定する

・つながることで波及するリスクを想定する

・物理的なリスクを認識する

・過去の事例に学ぶ

（ウ）守るべきものを守る設計を考える

・個々でも全体でも守れる設計をする

・つながる相手に迷惑をかけない設計をする

・安全安心を実現する設計の整合性をとる

・不特定の相手とつなげられても安全安心を確保できる設計をする

・安全安心を実現する設計の検証・評価をする

（エ）ネットワーク上での対策を考える

・機器等がどのような状態かを把握し、記録する機能を設ける

・機能及び用途に応じて適切にネットワーク接続する

・初期設定に留意し、認証機能を導入する

（オ）安全安心な状態を維持し、情報発信・共有を行う

・出荷・リリース後も安全安心な状態を維持する

・出荷・リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える

・つながることによるリスクを一般利用者に知ってもらう

・脆弱な機器を把握し、適切に注意喚起を行う

（３）一般利用者のためのルール

一般利用者も日常生活の中で IoT 機器を利用しています。IoT 機器を適切に取り扱わないと、IoT 機器の利用に不都合が生じるだけでなく、自分やその家族などになりすまして不正利用されたり、個人情報が漏れたり、IoT 機器が悪用されて他の利用者に迷惑をかける可能性もあります。そのようなリスクに対して、一般利用者が IoT セキュリティ対策として守るべきルールがあります。

（ア）問い合わせ窓口やサポートがない機器やサービスの購入・利用を控える

・何か不都合が生じたときに適切に対処することが困難で、接続する機器のアップデートを適切に行うこともできないので、安全安心に機器やサービスを利用できないことになります。

（イ）初期設定に気を付ける

・インターネットに接続する機器のパスワードが他の人に漏れると、インターネット経由で機器が乗っ取られ、不正利用される恐れがあります。機器を始めて使う際には、ID/パスワードの設定を行い購入時のパスワードのままとしない、他の人とパスワードを共有しない、生年月日等の推測しやすいパスワードを使わない、などの注意が必要です。

（ウ）使用しなくなった機器については電源を切る

・使用しなくなった機器や不具合の生じた機器をインターネットに接続したまま放置すると、知らず知らずのうちにインターネット経由で機器が乗っ取られ不正利用される恐れがあります。

（エ）機器を手放す時はデータを消す

・機器を廃棄、売却、貸し出す場合は、機器に記憶されている情報の削除を行わないと個人情報が漏洩する恐れがあります。

（４）開発時・設計時の留意事項

（ア）セキュリティ設計を行う手順

・対象とする IoT 製品やサービスのシステム全体構成を明確化する

・システムにおいて、保護すべき情報・機能・資産を明確化する

・保護すべき情報・機能・資産に対して、想定される脅威を明確化する

・脅威に対抗する対策の候補を明確化する

・どの対策を実装するか、脅威レベルや被害レベル、コスト等を考慮して選定する

（イ）脆弱性への対応での留意点

・開発段階での対応

①新たな脆弱性を作り込まない

②既知の脆弱性を解消すること

③残留している脆弱性を検出・解消する

④製品出荷後の脆弱性の新たな発見に備える

・運用段階での対応

①継続的な脆弱性対策情報の収集

②脆弱性対策情報（更新ソフトウェアを含む）の作成

③脆弱性対策情報の利用者への通知

④更新ソフトウェアの製品への適用

５．IoT に関する監査の方向性についての検討

（１）現実には、IoT 機器や IoT システムについて、監査を行うようなケースは中々ないかもしれませんが、一般的には、前述の各開発指針、セキュリティガイドライン、セキュリティ設計の手引きに準拠した、開発、運用、利用を行っているか、という点が監査の１つの方向性として考えられます。監査の視点としては、例えば下記のような視点が考えられます。

・経営者が IoT システムのつながる世界の安全安心に関する基本方針を定め、セーフティ設計、セキュリティ設計の指針を制定すると共に、継続的に維持すための体制を整備し、人材を確保・育成しているか。

・内部不正やミスの発生可能性を認識し、対策を検討しているか。また、ミスが発生した場合でも安全安心を守る対策を検討しているか。

・各 IoT システムにおいて、守るべきモノを特定し、本来機能や情報の安全安心を保つよう検討しているか。

・想定しないつながれ方をしても安全安心を保つよう対策を検討しているか。また、他の IoT システムとつながることにより、他へ波及するリスクや他から波及してくるリスクを想定し、対策を検討しているか。

・IoT システムに係る物理的なリスクを想定し、対策を検討しているか。

・IoT 機器の廃棄時のリスクを把握し、対策を検討しているか。

・これらのリスクの特定・把握と、それに応じた対策の検討については、各 IoT 機器や IoT システム毎にそれぞれ異なることになると考えられるし、想定できないリスクに晒されることもあり得るので、想定できないリスクに対応した運用でのリスク回避も検討しているか。

（２）IoT システムそのものの採用にあたっては、例えば様々なシステムのリモート保守の中で、IoT 機器によりハードの保守情報を遠隔で自動収集したりすることは、普通にあり得ることだと思われるので、このような仕組みを採用しているか否かの把握とセキュリティの確保について、監査項目とすることもアリだと思います。

（３）さらに、監査というよりシステム部門の役割かもしれませんが、自社だけでなく取引先企業が IoT 機器や IoT システムを作成・導入するような場合に、コンサルティング的にリスクやセキュリティ対策に関するアドバイスができるよう、各種ガイドラインや開発指針をある把握していることは有用だと思います。

以上

◇**研究報告　2**

「匿名加工情報の取扱いについて」

報告者 (会員番号　1281　宮本 茂明)

1．はじめに

改正個人情報保護法が2017年5月30日からすべての事業者に適用された。改正点の１つとして、個人情報の有用性を確保（利活用）するため、匿名加工情報に関する加工方法や取扱い等の規定の整備が行われている。福井県例会では、匿名加工情報の取扱いに関連するガイドライン等について紹介し、参加者の方々と意見交換を行った。

＊ 匿名加工情報：特定の個人を識別することができないように個人情報を加工し、
当該個人情報を復元できないようにした情報

2．匿名加工情報の取扱い

匿名加工情報の制度は、個人情報を特定の個人を識別できないように加工した情報について、一定のルールの下で本人の同意を得ることなく目的外利用及び第三者提供を可能とすることにより、事業者間におけるデータ取引やデータ連携を含むパーソナルデータの利活用を促進するものである。今後、新事業や新サービスの創出が期待されている。

匿名加工情報を取り扱う上での制約としては以下のものがある。

（１）作成時の制約

・　基準に従った適正な加工

[匿名加工情報の加工基準]

①　特定の個人を識別することができる記述等の削除

②　個人識別符号の削除

③　情報を相互に連結する符号の削除

④　特異な記述等の削除

⑤　個人情報データベース等の性質を踏まえたその他の措置

・　加工方法等情報の漏えい防止（安全管理措置）

・　作成時の公表義務（情報の項目）

（２）提供時

・　提供時の公表・明示義務（情報の項目、提供方法）

・　識別行為の禁止：他の情報と照合することを禁止

・　安全管理措置等（努力義務）：安全管理措置、苦情処理等を講じ、その内容を自ら公表

匿名加工情報の取扱いに関し、個人情報保護委員会から『個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）』、レポート『匿名加工情報　「パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて』、Q&A『「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するＱ＆Ａ』が公開されている。

匿名加工情報を取り扱う際には、匿名加工情報の要件を満たしているか、第三者による評価も有効だと考える。

3．匿名加工情報等IoTデータ流通・利活用に向けた動向

匿名加工情報の取扱いに関して留意点が多いことから、事業者がプライバシーとの関係で炎上を懸念して萎縮する傾向や事業者間でのデータ共有を行わず一社で囲い込む傾向が懸念されている。こういった状況を受け、経済産業省、総務省によるIoT推進コンソーシアム・データ流通促進WGでは、データ流通に際して生じる課題をユースケースベースで「判例」的に整理し公表するとともに、事業者の指針となるガイドライン等によるルール整備を推進している。2017年6月時点で以下の事例集、ガイドライン等が公開されている。

- 「新たなデータ流通取引に関する検討事例集」ver1.0

　　平成29年3月　IoT推進コンソーシアム、総務省、経済産業省

・ IoT推進コンソーシアム・データ流通促進WGにて、個別事例（平成28年1月から平成29年3月までに扱った20件の事例）を前提として、委員から助言があった内容を基にまとめたもの。データ流通取引を伴うBtoBビジネスを検討している事業者にとって、検討すべき事項や解決の参考となるもの。

- 「カメラ画像利活用ガイドブック」ver1.0

　　平成29年1月　IoT推進コンソーシアム、総務省、経済産業省

・ カメラ画像を事業者が利活用するにあたり、生活者とそのプライバシーを保護し、適切なコミュニケーションをとる際の配慮事項を、ユースケースを基に整理したもの。

- 「データの利用権限に関する契約ガイドライン」Ver1.0

　　平成29年5月　IoT推進コンソーシアム、経済産業省

・ 事業者間の契約においてデータの利用権限を公平に取り決めるための手法や考え方を示すもの。あらゆる事業者の契約おいて、当該契約に基づく取引に関連して創出されるあらゆるデータに関する権限を定める際に活用できるもの。

- 「データ流通プラットフォーム間の連携を実現するための基本的事項」

　　平成29年4月　IoT推進コンソーシアム、総務省、経済産業省

・ データ流通事業者が、多種多様なデータを提供していく中で、データ利用側がアクセスしたいデータを容易かつ効率的に見つけ利活用を図るために、データ連携における共通化することが必要な最低限の項目を整理したもの。

4．おわりに

個人情報に関連するシステム監査は、これまで個人の権利・利益の保護の側面で行われるものが多かった。今後は、併せて、匿名加工情報等IoTデータ流通・利活用における個人情報の有用性の側面からのシステム監査を進めることも重要になってくると考える。

以上

<目次>

2017.7

支部報告　【　近畿支部　第１６６回定例研究会　】

会員番号　2606 坂野 嘉則　（近畿支部）

１．テーマ　「事業継続マネジメント（BCM）の本質とは？」

２．講師　株式会社マネジメント総研 代表取締役　小山 俊一氏

３．開催日時　２０１７年5月１９日（金）　１８：３０～２０：３０

４．開催場所　大阪大学中之島センター　２階　講義室２０１

５．講演概要

事業継続マネジメント（BCM）の本質を理解することを目的とし、事業継続計画（BCP)、事業継続マネジメント（BCM)、事業継続マネジメントシステム（BCMS）について、事例を交えて解説していただきました。

5-1.そもそも「BCP」とは？

「BCP」の定義、防災計画との違い、事業継続の考え方、起源と展望についてお話いただきました。

5-2.BCP の使われ方

阪神・淡路大震災、米国同時多発テロ、新潟中越・中越沖地震、東日本大震災、熊本地震での事業継続事例についてお話いただきました。

5-3.BCP の策定

BCP の策定状況、策定の動機、策定上の課題、策定のために協力を得る先、主な参考ガイド、参考ガイドの内容例についてお話いただきました。

また、事業影響度分析の目的と方法、リスクアセスメントの目的と方法、事業継続対策の検討方法等について具体的にお話いただきました。

5-4.改めて「BCP」とは？

「BCP」について、よく見られる誤解を例に挙げ、改めて「BCP」の目的、特性及び留意点等についてお話いただきました。

5-5.BCMS（ISO 22301）

BCMS の全体像と、その中での BCP の位置づけについてお話いただきました。

また、リスク管理の例として、「事業継続方針」「リスク選好」「リスクアセスメント」の関係、対策の考え方について事例をもとにお話いただきました。

5-6.BCM の本質を考える

有事の幅、平時の効果、事業継続のマネジメントについて、お話いただきました。

そして、BCM の本質について、以下のようなお話をしていただきました。

・事業を継続する上で想定すべき有事は、地震だけでなく、キーマンの病気・事故、設備故障、取引先の倒産なども考えられる。また、災害発生という原因事象だけではなく、資源喪失という結果事象に着目することが重要である。そして、資源喪失という事態の発生を予防するとともに発生時の備えをするこ

とが、事業としてのレジリエンシー確保（事業継続）につながる。

・喪失してはいけない資源は、自社の強みとなる経営資源である。これが強化されるということは、自社の強みとなる経営資源を機動的に使えるようになること、すなわち、経営戦略上の選択肢が増えることを意味する。そして、この選択肢を事業の発展に生かすことが、ゴーイングコンサーン（真の事業継続）につながる。

・ISO 31000（リスクマネジメント－原則及び指針）では、リスクとは「目的に対する不確かさの影響」と定義されている。事業継続リスクとは、ゴーイングコンサーンの道筋に向かう不確かさの影響であり、これをマネジメントすることが、事業継続マネジメントである。

6．所感

BCP、BCM、BCMS について分かりやすく解説していただき、その場で理解できました。自社の業種の特性および強み・弱みを意識した BCP を策定し、PDCA サイクルを回して有効に機能させるには経営者の積極的な関与と人材の確保が必要であるため、BCM を構築・運用することができれば、結果として、自社の強みにつながると考えます。

<目次>

2017.7

支部報告　【　近畿支部　第５７回システム監査勉強会　】

会員番号　０６２０ 小山 正弘

１．テーマ　　「公会計とシステム監査」及び
「某基礎自治体におけるシステム・トラブル対応の進展」

２．講師　　ジョイント・ホールディングス（株）IFRS グループ・ディレクター
公認システム監査人、公共政策・IFRS コンサルタント
田淵 隆明氏

３．開催日時　２０１７年6月１７日（土）１５：００～１７：００

４．開催場所　大阪大学中之島センター ２階 講義室２０１

５．講演概要

講師は近畿支部会員であり、支部において「システム監査法制化研究プロジェクト」の座長を務めておられます。今回は、公会計とシステム監査及び某基礎自治体におけるシステム・トラブル対応の進展について幅広い視点からお話しいただきました。

講演の目次は以下の通りです。

＃１：（はじめに）我が国の製造業が苦境に陥った原因　～我が国を苦しめる８つの元凶～
＃２：日本の会計基準（JGAAP）と制度改正のタイムテーブル
＃３：公会計と企業会計の関係
＃４：消費税複数税率化
＃５：消費税を巡る新たな課題
＃６：某自治体のシステム・トラブルとシステム監査

はじめに、全体的な課題認識として、我が国の製造業が苦境に陥った原因について、講師のロビー活動による情報も踏まえ説明されました。＃３では、来年４月から実施される地方公共団体会計の「発生主義」・「複式簿記化」への対応や、期末一括仕訳でなく日々仕訳を採用される自治体での移行リハーサル実施など、システム監査上の課題について話をされました。

また、＃４では、複数税率対応のポイントは、「明細単位で消費税の計算ができること」であり、各社の対応状況について話をされ、「包括的間接税における複数税率は、世界中、どこでも実施している制度であり、５%の段階において、将来の引き上げが中長期的な不可避な流れの中で、複数税率は不可避であった。システムベンダとして、将来拡張性を考慮しなかったのはまさに設計ミスと言わざるを得ない」と見解を述べられました。

＃５では、制度上生じている矛盾や病院などの医療機関における損税問題について具体的に示され、システム監査を実施する際の確認事項、留意点を話されました。

・脱税防止効果は強化された

・簡易課税は縮小される方向

・益税は消滅するが、損税は残る

・煩雑な「課税売上割合」の計算も残ってしまった

＃６では、２０１４年８月４日に自治体の基幹システムが丸１日停止したシステム・トラブルについて、２０１６年３月１９日の研究会に引き続き、その後の議会の動き、システム対応、技術・知識の習得面等について話をされました。

[直接原因]　負荷分散装置のファームウェアのバグによる過負荷

[根本原因]　共同利用していたデータセンターのＷｅｂサーバ、ＡＰサーバ、ＤＢサーバは筐体分離されていたが、負荷分散装置は、単一障害点（Single Point Of Failure）になっていたため、他の自治体の業務への影響を回避するため、再起動は午後５時３０分まで待つことになった。

[その後の議会の動き]

２０１６年３月１０日の予算特別委員会（企画総務委員会所管質疑）

・ＣＩＯアドバイザーに「システム監査技術者」、「公認システム監査人」だけでなく、「情報処理安全確保支援士」の確保に努める。

・「情報セキュリティマネジメント」、「情報セキュリティスペシャリスト」の受験を推進

⇒　自前で「情報処理安全確保支援士」の確保に動いている。

２０１６年９月３０日の決算特別委員会（企画総務委員会所管質疑）

・情報政策課では、継続的な人材育成として、ＩＣＴ人材育成計画に基づき、職員を情報セキュリティに関する専門研修や、実践的サイバー防御演習などに派遣し、実務上必要な知識を習得させている。

・専門企業を活用して定期的に情報セキュリティの技術面での評価を行い、情報セキュリティについて高度な知見を有するＣＩＯ・ＣＩＳＯアドバイザーからもご意見をいただきながら、新たな技術の導入による改善を実施している。

２０１７年３月２３日の予算特別委員会（補充質疑）

・職員を情報セキュリティ等に関する専門研修に派遣し、実務上必要な知識を習得させている。資格などについては、若手職員を中心に、情報セキュリティマネジメント試験の受験など、自己啓発に取り組んでおり、合格者も出ている。

最後に、講師は、ご自身の経験から「ＡＩに負けないよう、ぜひ専門家として、身近な問題について社会に働きかけてください。２年、３年と取り組めば、ルール、運用も変わります。変えていくことができます」と、結ばれました。

上記に関しては、次の講師による本部会報への投稿内容及び近畿支部報告内容も参照ください。

2015年8月号　No.173：【 基礎的自治体のシステム・トラブルに見る、自治体のシステム運用・監査の課題 】

2015年12月号　No.177：【基礎的自治体のシステム・トラブルに見る、自治体のシステム運用・監査の課題<第2回>】

2016年6月号　No.183：【 近畿支部報告 第１５８回定例研究会」 】「会計・税制改正を巡るシステム監査のあり方」

６．所感

本講演では、来年４月に迫った公会計の改正や消費税制の新たな課題について、身近な事ながら気付いていない矛盾、問題点を認識し、システム監査人としての観察眼について考える機会となりました。

また、某自治体のシステム・トラブル対応については、関心があっても関係者でないとなかなか知ることができない事項を、議会での質疑や取材活動を精力的に継続され、自治体側も計画的に改善取組されていることを知りました。関係者皆さまのご努力に敬意を表しますとともに、自身の業務において周囲への啓発に努めたいと感じました。

以上

<目次>

2017.7

注目情報

■「ネットワークビギナーのための情報セキュリティハンドブック」電子書籍の無料配信を開始（NISC）

内閣サイバーセキュリティセンター（NISC）では、サイバーセキュリティに関する普及啓発活動の一環として、インターネット上のトラブルから身を守るための方法を分かりやすく解説した「ネットワークビギナーのための情報セキュリティハンドブック」を作成し、Web サイトにて公開しております。　このたび、特に夏休みを控えた小中高校生の皆様など、広く国民の皆様に本ハンドブックに触れていただき、安心してインターネットを使える社会の実現に向けて御協力いただきたいとの希望を込めて、本ハンドブックを電子書籍化し、無料で配信することといたしました。

URL：　http://www.nisc.go.jp/security-site/news/ebook-handbook.html

■企業の目的に応じた IT 人材育成に利用できる「i コンピテンシ ディクショナリ 2017」を公開（IPA）

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）HRDイニシアティブセンターは、組織内の人材育成や組織力強化に活用できるツールとして提供している「i コンピテンシ ディクショナリ（以下、iCD）」の最新版「iCD2017」を公開しました。併せてiCDをウェブサイトから利用できる「iCD活用システム」と、ポータルサイトである「iCDオフィシャルサイト」も機能の追加・強化を行いました。

	項目	変更点
タスクディクショナリ	UI デザイン	新規追加
	IoT システム・サービスのライフサイクル	新規追加
	コールセンター	新規追加
	事業継続マネジメント	強化
	セキュリティ領域*	新規追加
	データサイエンス領域*	新規追加
スキルディクショナリ	IoT 技術に関するスキル・知識	新規追加
	セーフティに関するスキル・知識	新規追加

* 4 月 7 日に発表した ITSS+への対応

プレス発表URL：　https://www.ipa.go.jp/about/press/20170620.html
iCD URL：　http://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/index.html

<目次>

2017.7

【 協会主催イベント・セミナーのご案内 】

■SAAJ 月例研究会（東京）

第225回	日時：2017年　9月　5日（火曜日）18:30～20:30（開場18:00） 場所：機械振興会館 地下2階ホール	
	テーマ	「IoT時代のセキュリティを実現する3つの視点とシフトレフト」
	講師	株式会社アスタリスク・リサーチ　代表　　岡田　良太郎 様 （日本 CISO 協会アドバイザ、ビジネスブレークスルー大学大学院客員研究員）
	講演骨子	IoTエコシステムによるサービス構築においてセキュリティを組み込み、また管理することの必要性をうたわれています。しかし、その実践は不可解で面倒なものと捉えられがちで、結果的になしくずしになる危険性があります。本講演では OWASP Top 10 IoT Vulnerabilities を用いて想定される問題を概観しつつ、ビルトイン・セキュリティの実践の足がかりとなる「シフトレフト」コンセプトの適用を論じます。 ※資料の事前配布はありません。撮影も禁止です。
	お申込み	協会ＨＰで受付を予定

【 外部主催イベント・セミナーのご案内 】

■日本セキュリティ・マネジメント学会（JSSM）

第31回全国大会	日時：2017年7月30日（日） 場所：情報セキュリティ大学院大学 神奈川県横浜市神奈川区鶴屋町2-14-1	
	統一論題	「IoT 時代のセキュリティ・マネジメント」
	開催内容	学会 HP でご確認ください。 http://www.jssm.net/wp/?page_id=2577

■日本橋法人会

日時：2017年 8月 4日（金）13時30分 ～ 15時00分 場所：日本橋公会堂　4階 大ホール 中央区日本橋蛎殻町 1-31-1 TEL03-3666-4255 定員：200名（定員になり次第締め切ります）　　聴講料：無料	
テーマ	古田 貴之氏に聴く「ロボット技術で未来を創る」開催のご案内 ～2020 年東京オリンピックでのロボット技術応用実装を目指す～
開催内容	詳細は下記をご覧ください。 http://www.nihonbashi-hojinkai.or.jp/sample/pdf/29-08-04.pdf
参加お申込み	下記、イベント参加申込フォームよりお申込みください http://www.nihonbashi-hojinkai.or.jp/postmail_top/mousikomi.html

<目次>

2017.7

【 新たに会員になられた方々へ 】

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。
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。

・ホームページでは協会活動全般をご案内　http://www.saaj.or.jp/index.html
・会員規程　http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・会員情報の変更方法　http://www.saaj.or.jp/members/henkou.html

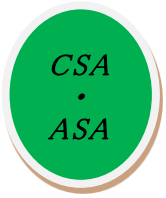
・セミナーやイベント等の会員割引や優遇　http://www.saaj.or.jp/nyukai/index.html
公認システム監査人制度における、会員割引制度など。

・各支部・各部会・各研究会等の活動。　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。

・皆様からのご意見などの投稿を募集。
ペンネームによる「めだか」や実名投稿には多くの方から投稿いただいております。
この会報の「会報編集部からのお知らせ」をご覧ください。

・「情報システム監査実践マニュアル」「６か月で構築する個人情報保護マネジメントシステム」などの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

・月例研究会など、セミナー等のお知らせ　http://www.saaj.or.jp/kenkyu/index.html
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。



・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

・会報のバックナンバー公開　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

・お問い合わせページをご利用ください。　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：前回から変更された予定			2017.7
2017	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
７月	5：支部助成金支給 13：理事会	3：第 224 回月例研究会「IoT におけるサイバー攻撃の実態とその対策」 下旬：秋期 CSA・ASA 募集案内 〔申請期間 8/1～9/30〕	14：支部会計報告〆切
８月	（理事会休会） 26：中間期会計監査	1：秋期 CSA・ASA 募集開始～9/30	
９月	14：理事会	2:第 19 回「事例に学ぶ課題解決セミナー」 5：第 225 回月例研究会「システムセキュリティ確保の眠れない夜」 14-15 & 28-29：第 30 回システム監査実務セミナー(日帰り 4 日間コース)	30：西日本支部合同研究会 in Fukuoka(福岡)
10月	12：理事会	21:SAAJ 活動説明会（東京茅場町）	16：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（1/6〆切） 18：2018 年度年会費請求書発送準備 25：会費未納者除名予告通知発送 30：本部・支部予算提出期限	11,18,25：秋期 CSA 面接 下旬：　CSA/ASA 更新手続案内 〔申請期間 1/1～1/31〕 30：　CSA 面接結果通知	
12月	1：　2018 年度年会費請求書発送 1：　個人番号関係事務教育 14：　理事会：2018 年度予算案 会費未納者除名承認 第 17 期総会審議事項確認 15：総会資料提出依頼（1/9〆切） 15：総会開催予告掲示 19：2017 年度経費提出期限	15：　CSA/ASA 更新手続案内メール 〔申請期間 1/1～1/31〕 26：秋期 CSA 認定証発送	
	前年度に実施した行事一覧		
１月	9：　総会資料提出期限 16：00 12：理事会：総会資料原案審議 28：2016 年度会計監査 30：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 17：第 220 回月例研究会 20：　春期 CSA・ASA 募集案内 〔申請期間 2/1～3/31〕 26～27：システム監査実践セミナー	6：支部会計報告期限 25：SAAJ 創立記念日
２月	2：理事会：通常総会議案承認 27：法務局：資産登記、活動報告提出 理事変更登記 28：★年会費納入期限	1～3/31：CSA・ASA 春期募集 下旬：CSA・ASA 更新認定証発送	24：第 16 期通常総会
３月	1：NPO 事業報告書、東京都へ提出 6：年会費未納者宛督促メール発信 9：理事会	1-31:　春期 CSA・ASA 書類審査 4:　事例に学ぶ課題解決セミナー(お茶の水) 11-12&25-26：システム監査実践セミナー 28：第 221 回月例研究会	
４月	13：理事会 30：法人住民税減免申請	初旬：春期 CSA・ASA 書類審査 中旬：春期ＡＳＡ認定証発行 19：第 222 回月例研究会「サイバー攻撃被 を軽減するための研究開発と人材育成の 動向」	11：WindowsVistaSP2 サポート終了 15：近畿支部　第 56 回システム監査勉強会（大阪） 16：春期情報技術者試験
５月	11：理事会	中旬：春期 CSA 面接 16：第 223 回月例研究会「企業 IT 動向調 2017」	
６月	4：年会費未納者宛督促メール発信 8：理事会 15：会費未納者督促状発送 15～：会費督促電話作業（役員） 30：支部会計報告依頼（〆切 7/14） 30：助成金配賦額決定（支部別会員数）	3：特別月例研究会「ＩＴガバナンスの国際 格（ISO/IEC 38500 シリーズ）と今後 の展開について」 中旬：春期 CSA 面接結果通知 22-23　システム監査実践セミナー(晴海) 下旬:　春期 CSA　認定証発送	認定 NPO 法人東京都認定日 （2015/6/3）

<目次>

2017.7

【 会報編集部からのお知らせ 】

1．会報テーマについて
2．投稿記事募集

□■ 1． 会報テーマについて

2017 年度の年間テーマは、「システム監査の新たな展開」です。四半期テーマは、2 月号から 4 月号が「技術革新とシステム監査」、5 月号から 7 号までが「AI とシステム監査」でしたが、8 月号から 10 月号までは「システム監査とＩＴガバナンス」、11 月号から 2018 年 1 月号までは「システム監査人に求められる能力」です。皆様のご投稿をお待ちしています。

システム監査人にとって、報告や発表の機会は多く、より多くの機会を通じて表現力を磨くことは大切なスキルアップのひとつです。良識ある意見をより自由に投稿できるペンネームの「めだか」として始めたコラムも、投稿者が限定されているようです。また記名投稿のなかには、個人としての投稿と専門部会の報告と区別のつきにくい投稿もあります。会員相互のコミュニケーション手段として始まった会報誌は、情報発信メディアとしても成長しています。

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」をご確認ください。

□■ 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。
・表紙の写真も、随時募集しています
・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。

会報記事への投稿の締切日は、毎月 15 日です。
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。
http://www.saaj.or.jp/members/kaihou_dl.html

<目次>

2017.7

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。会員パスワードが必要です）

https://www.saaj.or.jp/members_site/KaiinStart

ログイン ID（8 桁）は、年会費請求書に記載しています。

■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、会員宛の連絡事項を記載し登録メールアドレス宛に配信します。登録メールアドレス等を変更された場合は、会員サイトより訂正してください。

https://www.saaj.or.jp/members_site/KaiinStart

■□■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
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>