

CSAの方へ、CSA活動報告記事、資格更新申請手続きのお知らせがあります。会報テーマ”情報システム部門のためのシステム監査”の記事が、今号にも3編投稿されています。みなさんと一緒に考えて行きたいと思います。



多摩湖の夕日と富士山(11月)

巻頭言

2014年の活性化委員会の活動を振り返って

会員番号 6027 小野 修一 (副会長)

月日の経つのは早いもので、2014年も残り僅かになりました。

日本国内においても、世界レベルでも様々なことがあった一年でしたが、会員の皆様にとって、今年ほどのような一年だったでしょうか。

当協会では、2014年もシステム監査活性化委員会(略称、活性化委員会)を設け、各研究会・委員会・部会・担当の代表メンバーで委員会を編成し、当協会の活性化、および会員すなわちシステム監査人の活性化、さらにはシステム監査の活性化につなげるための討議と具体的取組みを、組織横断的に進めてきました。

今年の活動の中で特筆すべきこととしては、8月に拡大活性化委員会を開催し、集中的な討議を行ったことが挙げられます。2007年に当協会が発表した『システム監査これからの10年』の中で、10の大きな提言を行っています。いずれの提言も言ってみれば活性化の提言であり、この拡大活性化委員会において、10の提言に対する取組み状況を再確認し、今後取り組むべき課題を明確化し、新たな活性化施策を策定しました。今後は、ここで策定した活性化施策の実行とそのフォローアップを中心に活動を展開していきます。

活性化委員会のもう一つのテーマは、当協会のビジョンの設定です。ここでのビジョンは、3年後を見据えた当協会のあるべき姿と位置付けています。来たる2015年の活性化委員会は、活性化施策の実行のフォローアップと併せて、ビジョンについての検討を進めていきます。ビジョンを明文化し、当協会が会員の皆様とビジョンを共有して活動を進めていける形を作りたいと思っています。会員の皆様のご意見とご協力を、今まで以上によりしくお願いいたします。

2015年が、会員の皆様にとって良い年になりますよう、お祈りしています。

[<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>

○ 巻頭言	1
【2014年の活性化委員会の活動を振り返って】	
1. CSA活動報告	3
投稿【日・ASEAN 情報セキュリティ活動への参加報告】	
2. めだか	8
【情報システム部門のためのシステム監査】	
【部門長の味方】（情報システム部門のためのシステム監査）	
3. 投稿	10
【情報システム部門のためのシステム監査】	
4. 本部報告	11
【第196回 月例研究会(2014/10/30)「オープンデータの推進」】	
講師：内閣官房 政府CIO補佐官・経済産業省 CIO 補佐官 平本 健二氏	
【「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」その4】	
～「経済産業省ガイドライン」の読みこなしポイント～	
5. 注目情報	24
【大規模・複雑なシステムの障害診断の新手法を提案】	
【2014年の10大セキュリティ事件ランキング】	
【平成27年度春期 情報処理技術者試験実施日は平成27年4月19日】	
【2014年に発覚した主な情報漏洩事件】	
6. セミナー開催案内	25
【協会主催イベント・セミナー等のご案内6件】	
【外部主催イベント・セミナーのご案内2件（会報担当収集分）】	
7. 協会からお知らせ	28
【CSA/ASA資格をお持ちの方へ：資格更新申請手続きについて】	
【年会費納付時期について】	
【新たに会員になられた方々へ】	
【協会行事一覧】	
8. 会報編集部からのお知らせ	32

注目

注目

投稿 【 日・ASEAN 情報セキュリティ活動への参加報告 】

会員番号 0898 竹下 和孝

最近参加した、日・ASEAN 情報セキュリティ・シンポジウムおよび ASEAN 情報セキュリティ・マネジメントシステム研修の様子を紹介します。

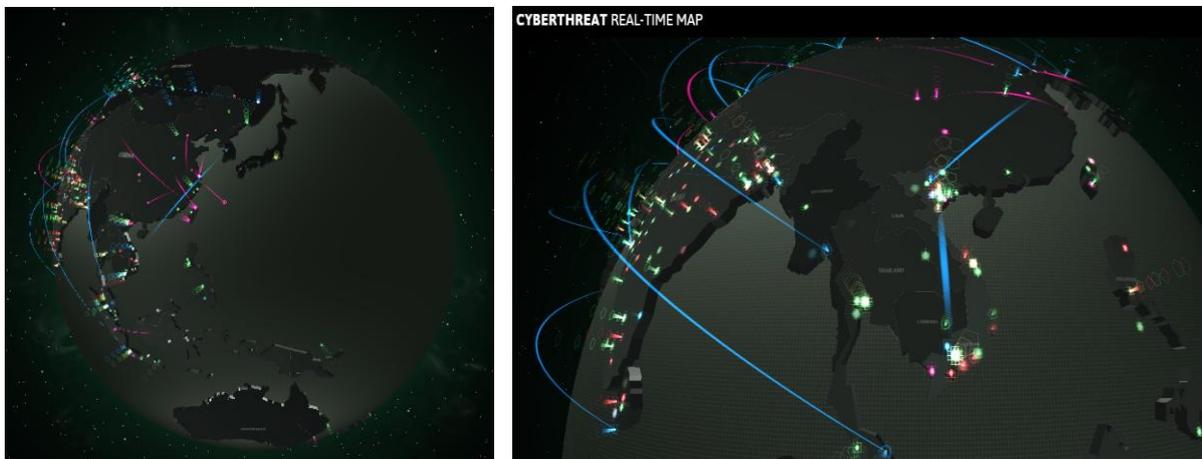
1. 東南アジア地域のセキュリティ事情
2. 日・ASEAN 情報セキュリティ・シンポジウム
3. タイの IT エンジニア
4. 情報セキュリティ・マネジメントシステム研修
5. シーロム通りの3人のエンジニア

1. 東南アジア地域のセキュリティ事情

マレーシア航空 370 便が 2014 年 3 月 8 日に消息不明となり、その4ヵ月後の 2014 年 7 月 17 日(現地時間)には、ウクライナ上空を飛行中のマレーシア航空 17 便(MH17)が墜落し、約 300 人の乗員・乗客が死亡という痛ましい事件が起きたことは、未解決事件としても記憶に新しいことです。

インターネット上のメール交信や SNS 上のメッセージ交換の状況把握が、これらの事件発生時の状況や原因究明にも活用されているようです。国家間規模のサイバーテロ活動が行われていることを追跡調査することでも、情報アクセスの発信元から着信先を突き止めることで、不正侵入が行われている状況を把握することができます。

どこの国から攻撃が仕掛けられているか分かるツールの使用例(左:東南アジア地域、右:拡大)



出所 CYBERTHREAT <http://cybermap.kaspersky.com/>

東南アジアにおける最近のセキュリティ事件の例としては、韓国で発生した大規模なサイバー攻撃が記憶に新しいでしょう。2013 年 3 月 20 日 14 時ごろに、韓国の銀行や放送局が同時多発的に狙われ、韓国の当局により大規模なサイバー攻撃によるものと判断され、大きく報道されました。

この攻撃による被害は、攻撃された銀行だけでなく、銀行 ATM、インターネットバンキング等の取引が同時に停止し、多くの国民にも影響を与えたサイバーテロだったということに特徴があります。一般の人が利用するサービスの停止という被害が長期にわたり継続した事例で、危機認識を高める機会にもなったわけです。

従来のサイバー攻撃は、攻撃対象およびその周りの組織への被害の影響でとどまっていましたが、この事件では

直接の攻撃対象ではない一般の市民生活への大きな影響、それが攻撃目的であった可能性も高いといわれています。また、今後、このような攻撃が日本を標的として準備される可能性もあり、日本の重要インフラといわれる電力、発電所など基幹産業や金融、病院、交通機関などの事業も攻撃に備えておく必要性の議論が高まっているわけです。

セキュリティ対策は特定の企業内、組織内だけにとどまらず、より広い範囲での連携が求められていると感じています。私達は、好むか好まないかに関わらず、地球上の市民としてそのような流れから逃れることは難しいのです。

2. 日・ASEAN 情報セキュリティ・シンポジウム

2014年10月7-8日に、日・ASEAN 情報セキュリティ政策会議が東京で開催されており、翌9日に開催された日・ASEAN 情報セキュリティ・シンポジウム(公開)に参加しました。各国からのプレゼンテーションを拝見すると、ASEAN本部のあるインドネシア、成長著しいベトナム、ミャンマー、そしてタイなど、現地事情が報告されていました。

この政策会議は7回目の開催で、参加国の政策立案担当者が日・ASEAN における情報セキュリティ関連の情報共有体制を更に強化し、グローバル化するサイバー脅威に対応するため、日・ASEAN における情報セキュリティ関連の情報共有体制の確立及びその強化と、インシデント発生時の各国連携による迅速な対処を目的とする、というための定期的な情報交換と討議の場でした。

技術的な相互連携や被害発生時の相互連絡や支援は、すでに内閣官房情報セキュリティセンター(NISC)や、総務省、経済産業省の情報セキュリティ対策室を通じて、JPCERT/CC、IPA など国内の専門部門との交流や連携方法が検討されていることは、シンポジウムが3回目の開催であったことから推定できます。



そして2014年11月の月上旬、ASEAN 現役エンジニア、管理者を対象に開催された5日間の研修会で、私は情報セキュリティ・マネジメントシステム(ISMS)研修セミナーの講師を務める機会を得ました。

研修会場は、タイの首都バンコクのほぼ中心部にあるホテルのコンファレンス会場です。そのホテルは、バンコク MRT (Mass Rapid Transit、地下鉄) シーロム(Silom) 駅と高架鉄道システム BTS (Bangkok Skytrain) のサラデー駅に隣接していて、徒歩2-3分でアクセスでき、多くの人々が参加する立地条件は優れています。サラデー駅は、シーロム通りの路上に、高架形式で建設され、シーロム(Silom) 駅には高架上の連絡通路でつながっています。空港からも高速道路を利用すると、渋滞がなければ30分程度で直結している便利な場所にあります。

シーロム通りの周辺は、タイ名物のマッサージ店や屋台という伝統的なイメージの商店街と、再開発され新築された大きなビルが複合型商業施設として賑わっています。近所で働く人々や家族で食事やショッピングに訪れる利用客で早朝から深夜まで混雑する商業地域で、シーロム通りはその商業地域を南北につなぐ幹線道路のひとつでもあります。日本語の看板も多く、見渡すだけで日本の大手コンビニエンスストアの店舗が複数店舗は見つかるほど。日本企業がタイの人々の生活に密着した事業展開を進めているようです。早朝 7 時ごろに訪問すると、通勤通学の途中と思われる客で長い行列ができていました。

3. タイの IT エンジニア

タイでは最近、金融機関が大規模なハッキング被害を受け、電力、通信、医療機関など重要インフラに分類される組織やサービスでハッキングや標的型攻撃の不安が高まっています。被害と影響の大きさから重要インフラとして有効な対策を講じたいわけですが、個々の企業や組織の頑張りでの対処できるものではありません。

首都バンコクでは、政情不安、デモや大規模水害による工業団地の浸水が事業活動に影響を及ぼしたことは記憶に新しいでしょう。課題は、現地でのリスクマネジメントや情報セキュリティ活動をどのように考え、計画し、実質的な対処の準備を進めておくか、ということです。事故を起こした後での対策なら比較的容易にセキュリティ活動への予算配分や活動の優先度を高めることができるでしょう。それでも、予算や人員、スキルなどは最小限しか割り当てられず、不可欠な水準での準備ができる状況ではない場合が多いのです。未知の分野が多いからです。したがって、現場のエンジニアの能力や経験アップへの期待が高まるわけです。

タイの IT 分野でのエンジニアは、日本の情報システム技術者試験やスキル標準と同等の仕組みを導入していて、エンジニア養成が図られています。日本のスキル標準レベル1からレベル7のような知識や習熟度に応じたランクが更に細かく分類された仕組みを導入しており、採用時の資格認定や給与・処遇に直結しているようです。

エンジニアという仕事は、新しい開発や技術に挑戦するイメージがありますが、仕事の多くの時間は検証や設計・試作・運用やオペレーションなどの繰り返し作業を伴います。またエンジニアが担当する仕事も、1人で担当する仕事、複数のエンジニアでチームを組んでプロジェクト形式で活動するような仕事に分かれます。

さらに経験を積むとそのチームを運営する進捗管理、技術管理、品質管理、予算管理、業績管理などの管理業務を任せられるようになると、次第に技術を磨く機会が少なくなり、会議の準備や会議進行、プレゼンテーションや報告も面倒に感じる元エンジニアもできます。技術一筋、現役のエンジニアでいたいと感じる瞬間でしょう。

さらに新しい経験やよりよい処遇を求めての転職は当然のことですので、良質な経験者の確保、能力に応じた適材適所の人事配置、人材育成にも力を注ぐ必要があります。情報セキュリティのように新しい分野では、知識習得だけでなく経験の蓄積や人材育成の緊急性も高いわけです。

4. 情報セキュリティ・マネジメントシステム研修

現在、アジア諸国のなかでも急速な経済発展を実現し、IT 基盤の充実と情報システムの運用環境を整備している国もありますが、最も多くの失敗事例を持っているのは、まだ日本がダントツでしょう。セキュリティ被害や多くの事故を経験し、さらに国際的な認証である ISMS 認証件数の半分以上は、日本の企業や組織によるものです。

優れたセキュリティ技術、セキュリティ対策を講じた機器や装置であっても、情報機器を利用し運用するのは「人」であり「組織的な活動」です。組織で働く内部・外部の人々が日夜の運用に従事しています。

ISO31000 が定める「不確かさ」を想定することで、想定外の状況は少なくなったとはいえ、想定内の事象としてどこまで備えておくかは永遠の課題でしょう。

実際、被害の想定や許容水準の設定は容易ではありません。

要するに、わからないことだらけです。

しかも入念な事前対策を行っても、被害発生を防止できるわけではありません。

このような不安が渦巻く中で、改訂された ISO/IEC27001:2013 に基づく ISMS 規格の概要解説と実践構築のための研修が企画されました。初日から4日目までを情報セキュリティ対策の組織作りを目的とする集中トレーニングとし、JIPDEC が担当し、5日目に情報セキュリティの技術的な解決手法を紹介するという内容です。

とはいえ、ISO/IEC27001:2013に基づく国際規格の制度運営や活用推進は、国内ではJIPDECが推進していますが、ASEAN諸国の重要インフラを運用する組織が直面していると思われる課題までを把握し、支援する役割までは用意できているわけではありません。

相談を受けて、手探りながらセキュリティ上の課題分析、セキュリティ強化のための組織づくり、管理策の選定の手法や点検、監査、マネジメントレビューの方法など、ISO/IEC27001:2013に基づく国際規格の活用方法を紹介して、実践方法を演習形式のノウハウとして紹介すればよいのではないかと、との仮説を立てました。その後は、やってみながら参加者の反応に応じて調整することとしました。CSAとしての実践経験と問題解決が試されるわけです。

さらに一方向の講演や講義ではなく双方向のコミュニケーションを前提にとの現地からの強い希望があり、ASEAN諸国向けに現地で実施する研修は、ケーススタディ方式を中心に5日間とするカリキュラムとなりました。

主としてタイの重要インフラを企画・運用するエンジニアを対象に案内され、公開研修会が開催されました。

5. シーロム通りの3人のエンジニア

さて、研修参加したエンジニアの多くが心をひとつにした、次の「シーロム通りの3人のエンジニア」のエピソードをご存知でしょうか。シーロム通り(Silom road)は、下図の赤線部分にある賑やかな通りです。

(バンコク中心部の繁華街)



◆シーロム通り(Silom road)の3人のエンジニア

シーロム通りを歩いていると、3人のエンジニアに会った。

一人目のエンジニアに話を聞くと、
「私は与えられた業務、役割を一生懸命にこなしている」。

二人目のエンジニアは、
「私はNo.1のエンジニアになるため、スキルを磨いている」。

三人目のエンジニアは、
「町やネット環境を守るために、毎日努力している。
時間があるなら一緒に手伝ってこないか」
と協力を求めて仲間を増やしていった。

あなたは、どのタイプのエンジニアを目指しますか。

このエピソードは、情報セキュリティは、一人の力では限界があり、皆の力を合わせて活動することで、トラブルを早期発見、素早く対処でき、より強固になるというイメージがして、研修5日間の全体総括のときに紹介したものです。

質疑の流れから、夢中でこのような話を創作していたのですから、本心でしょう。

今回の研修受講者であるエンジニア達に、どのタイプのエンジニアを目指すか、と聞くと、三人目と応えてくれて、メッセージとして伝えたかったことに共感してくれたようで、ちょっと感動を覚えました。

その勢いで、「一緒に町、地域、国全体やそのネット環境を守りましょう」と締めくくりました。

そのときのエピソードです。だから、その場を共有した参加者、関係者以外はまだ知りません。でも似たような話は記憶にあるかもしれません。その現代エンジニア版です。

決して二番目のエンジニアのスタイルを否定するわけではありません。

不具合や異常を早期発見し、修復するには、優れたスキル・経験があることで素早く発見でき適切な対応ができます。その優れた技術力や着眼点、アイデアは、一般には達成できないような正確さ、効率、時間で問題解決ができる場合が多い、ましてセキュリティ事件が発生した場合の一次対応、原因追求、解決案作成と是正処置までをスムーズに実施するには、技術力がないと対応できません。

しかし、そんな二番目のスタイルを目指すエンジニアも、普段は三番目のスタイルのエンジニアのひとりとして、腕を磨くことで、磨きあげたスキルを活用できる場面が増えるのです。

協働作業のシナリオが、参加者にとって新鮮で実践的だったと評価いただきました。

ケース研修でグループメンバーの異なる経験や知識をあわせて討論し、協力することにより、よりよい報告ができあがり、良い発表ができたという共有体験が評価されたわけで、講師としては狙い通りの反応を得て嬉しく思いました。

失われた20年を経験した日本では、まだ将来の方向を模索している場面が多いように思われます。

日本が経験した高度成長時代には、この二番目と三番目のスタイルのエンジニアがバランスよく相互に研鑽した時期だったのではなかったでしょうか。次回、東京オリンピックが計画通りに開催されるとすれば、その国家行事を活用して安心安全で豊かな社会を目指していた前回当時の熱意や志を後輩に伝える継承活動も重要な役割のひとつではないでしょうか。

IT 活用の場面は急激に進展し、私達 CSA もその先頭に立ち試行を繰り返してきたと思います。多くの失敗もありました。日本的な慣習の良さのひとつは、その失敗を相互に学び共有し、同じ間違いを繰り返さないように組織内・業界内で競争して品質を高めてきたことでしょう。

そこで、課題分析や問題解決への視点が経営への貢献に直結するように、情報システムと情報セキュリティ確保の効率性や有効性評価の観点からモニタリングやコントロールを組み立て、情報セキュリティ活動への取り組みを強化するよう、もっと経営者の意思決定を支援してはいかがでしょうか。

出国前に治安情報を確認すると、「夜間、路上強盗が発生していることから、繁華街周辺の路地を通る際、注意して欲しい。(在タイ日本国大使館)」と掲示されているのを見ると緊張します。

邦人男性の被害者は、深夜、コンビニエンスストアで買い物して、宿泊先ホテルに向かって歩道を歩いていたところ、前後から現れた複数の若者に棒状の凶器等で突然襲われ、持っていた現金、クレジットカード、旅券が入ったバックを奪われ、額付近を負傷した、という犯罪事例も紹介されています。

先に紹介したシーロム通りは、繁華街の一角を占めていて、路上で警備している警察官の数も目立ちました。

ケーススタディ最後の木曜日は、年に1回、満月の夜に川の神様に感謝する日 Loy Krathong (ロイ・カトーン)で、川を流れるバナナの葉で作られ、果物やお菓子上で飾られたカトーン(灯籠)が水辺に浮かび、幻想的で美しい祭りの日でした。

外国からの観光客も多く訪れていて、危ないから川沿いには近づかないようにとの研修参加者の助言を守り、ホテル近くにある公園の貯水池まで出かけて、小さな子供連れの家族にまぎれて見事な飾りつけや遠くに聞こえる花火の音を体感することができました。1週間の滞在中、ケーススタディ運営のことで思考満杯だったので、しばし休息のひとつでした。

ということで、シーロム通りの3人のエンジニアのエピソードは、研修の主要なテーマだったケーススタディと共に忘れることのできない記憶となり、今回の研修会を印象づけてくれました。研修内容については、次の機会に紹介します。

以上

[< 目次 >](#)

めだか 【情報システム部門のためのシステム監査】

情報システムのうち公共機関の情報システムは社会インフラであり、その障害は多くの人々に被害をもたらすリスクとなる。リスクに対して情報システムにシステム監査が求められるべきと思う。中でも公共機関で個人情報を取り扱う情報システムの構築や保守は、障害が起きないように、また法令等へのコンプライアンスや本人同意の利用目的に齟齬が生じないようにシステム監査を制度化あるいは法制化するように求めていく、これは情報システム部門のためのシステム監査につながる活動であると思う。

さて、ウィキペディア(Wikipedia)で、冬至について調べてみた。“秋分から春分までの間、北半球では太陽は真東からやや南寄りの方角から上り、真西からやや南寄りの方角に沈む。冬至の日にはこの日の出(日出)・日の入り(日没)の方角が最も南寄りになる。なお、1年で日の出の時刻が最も遅い日・日の入りの時刻が最も早い日と、冬至の日とは一致しない。日本では、日の出が最も遅い日は冬至の半月後頃であり、日の入りが最も早い日は冬至の半月前頃である。”とある。

また、“日本では冬至にはカボチャの煮物を食べる風習や柚子湯に入る習慣がある。中国北方では餃子を、南方では湯圓(餡の入った団子をゆでたもの)を食べる習慣がある。冬至(あるいは、冬至から翌日にかけて、冬至の直後、など)には、世界各地で冬至祭が祝われる。太陽の力が最も弱まった日を無事過ぎ去ったことを祝う日である。クリスマスも起源は冬至祭(ユール)である。”ともある。

「アダム・スミス『道徳感情論』と『国富論』の世界」では、18世紀イギリスの世相として、光と闇が交錯する時代であったことが示されている。光の側面は、政治の民主化、大西洋貿易システムの確立と経済の発展、生産技術の革新、知識の進歩と普及、また、闇の側面は、格差と貧困、財政問題、アメリカ植民地問題であったと書かれている。アダム・スミスは、これらの課題に対して、道徳感情論で秩序を導く人間本性を、また、国富論で繁栄の一般原理を論じている。「新・国富論 グローバル経済の教科書」は、現在のグローバル経済の課題を、アダム・スミスの時代から投影して、今の時代に光と闇を映し、新・国富論として課題の解決を論じている。

年末に当って、みなさん、業務や棚卸、大掃除に忙しいと思うが、歴史に学び考えることは大切なことだと思う。冬至祭は太陽の力が最も弱まった日を無事過ぎ去ったことを祝う日である。冬至を祝い情報システム部門の人やシステム監査人にとって新しい年が良き年であるよう祈念したいと思う。



(空心菜)

[参考]:

「アダム・スミス『道徳感情論』と『国富論』の世界」 睦目 卓生 著 中央公論新書刊(中公新書 1936)

「新・国富論 グローバル経済の教科書」 浜 矩子 著 文芸春秋刊(文春新書 894)

(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>](#)

めだか 【部門長の味方】**(情報システム部門のためのシステム監査)**

システム監査は、情報システム部門長やCIOのよき理解者だ。理解者というよりも“味方”と言った方が近いと言える。これは当たり前過ぎることといっているが、会報テーマ「情報システム部門のためのシステム監査」を受けて、システム監査人の一人として強調する。

情報システム部門を率いる部門長が日夜闘っていること腐心していることは多種多様だ。この重要性や実現への方策を共有し推進するという点で、システム監査と情報システム部門は味方同士だ。

例えば部門長の方に確認したい。担当部門がシステム監査(内部監査、外部監査を問わず)を受ける場合、次のようなことは当然のように実現されているだろうか。

- ・担当部門の現状について、事前の監査リーダとのすり合わせや協議は、価値観一致まで行われているか？
- ・監査での着眼点や重点事項は、すり合わせや協議の結果が反映された内容になっているか？
- ・監査からの指摘は、定型チェックリストなどによる〇×ではなく、実態に即した判断・評価になっているか？
- ・監査からの改善提案は、環境変化や組織間の問題を含めて担当部門が納得できるものになっているか？
- ・フォローアップ監査では、自部門に限らず関連部門との組織的な課題も含めて取り上げられているか？

このようなことが実現されている状況で“システム監査は部門長の味方”に否定的な意見は出てこないと思うが、今もなお、システム監査は受けたくないとか煩わしいとか苦手とかの声が残っていることもあるようだ。これは何か昔の出来事を引きずっているのだろうか、各種監査や検査などの印象や語感から生じているのだろうか。少なくともシステム監査を嫌うような感覚は全く心外というほかはない。

情報システム部門もシステム監査部門も同じ事業目的実現の職責を担っている。情報システム部門に課題があるならば、そのソリューションを共に考えシステム監査の立場で課題解決に向けて果たすべき役割がシステム監査にはある。システム監査は、情報システム部門やその他の部門の仕事振りに対して、横からのチェックや表面的な評価をしたり問題点の指摘だけで済ましたりするものではない。監査で把握した事実から組織的な対処を要する課題を浮かび上がらせてシステム監査自らが動くことに他ならない。

部門長の方に再度問いたい。ここで述べたようなシステム監査の姿は既知のことだろうか。自社のシステム監査では当然に実施されているだろうか。あるいはシステム監査への見方に少し変化が生じたかも知れない。システム監査が行われる際に、システム監査に望むことやシステム監査が果たすべきことを、部門長が堂々と率直に主張することは部門運営に大きな効果をもたらす。

だからと言って、システム監査を好きになったとまで部門長が公言するのには抵抗もあるかも知れないが、システム監査を上手に利用して欲しい。と言うのも、既にシステム監査は情報システム部門長の味方であり応援者を自覚しており、情報システム部門の役に立つ存在であることがシステム監査の生きがいであるから。



(山の彼方)

(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 >](#)

投稿【 情報システム部門のためのシステム監査 】

会員番号 0557 仲 厚吉 (会長)

情報システム・ユーザー会連盟主催 第35回システム監査講演会(2104年10月21日 きゅりあん 東京都品川区)に、斉藤(茂)理事、館岡理事、力副会長と参加を致しました。当協会は同講演会の後援団体になっております。当日、会場で大友中部支部長にお会いし、他にも当協会関係者のお姿を拝見しました。基調講演は、経済産業省 商務情報政策局 情報処理振興課長 野口 聡 氏による「情報セキュリティ政策について」でした。わが国の情報セキュリティ政策の今後の方向性についてわかりやすい講演だったと思います。

講演の中で、情報セキュリティ専門家の育成、特に情報セキュリティ分野で若い優秀な人材を育てることを強調されていました。それとともに、情報システムを利用するユーザー側の情報セキュリティへのリテラシー向上という観点で2016年から新たな情報処理技術者試験「情報セキュリティマネジメント(仮称)」の追加を検討し始めたことに言及されていました。当協会では IT ガバナンスの視点で情報システム利用者側の情報セキュリティ・リテラシーの向上をとりあげていきたいと考えています。



IT ガバナンスは、ISO/IEC 38500(Corporate governance of information technology)として国際標準になっており、現在、ISO/IEC 38500のJIS規格化が進んでいます。IT ガバナンスは、6つのプリンシプル、Responsibility、Strategy、Acquisition、Performance、Conformance、Human behavior で構成され、PDCA を回して、システム監査はそのCすなわちCheckの役割を担います。IT ガバナンスがJIS規格になると社会的な認知に拍車がかかることを期待でき、当協会は、ISO/IEC 38500のJIS規格化を契機に、関連団体と協力してシステム監査の制度化・法制化を提言していくよう取り組みます。また、当協会システム監査基準研究会のメンバーが参加している IT Auditすなわちシステム監査のISO化への取り組みは、ISO/IEC 38500のJIS規格化の進捗に並行して進めています。

日本ITガバナンス協会の主催でITGI Japanカンファレンス2014(2104年11月13日 ヒューリックホール浅草橋 東京都台東区)が開催されます。当協会は同カンファレンスの後援団体になっており、私と力副会長が参加いたします。テーマは、「ITガバナンスを深く学ぶ」～ITリスク管理の視点を交えて～ となっています。

当協会では、2008年2月18日の創立20周年記念講演会で「システム監査のこれからの10年に向けた提言と当協会の今後の取り組み」について発表を行っており、ホームページに報告資料を掲載しています。このシステム監査のこれからの10年の提言と取り組みに関して、当協会システム監査活性化委員会では、「システム監査のこれからの10年に向けた提言と当協会の今後の取り組み」を見直し、残る4年間に取り組むべき協会活動の方向性を確認しています。その中で情報システムの有効性監査がテーマとしてとりあげられており、そのひとつとして、情報システム構築プロジェクトを失敗なく有効に進めるためのシステム監査あるいはシステム管理のポイントを研究していくことは有意義であると考えています。

情報システム部門のためのシステム監査へ会員の皆様のご協力をお願い申し上げます。

[<目次>](#)

第196回 月例研究会 (2014年10月30日開催)

会員番号 0608 三谷 慶一郎

【講演テーマ】 「オープンデータの推進」
【講師】 内閣官房 政府 CIO 補佐官・経済産業省 CIO 補佐官 平本 健二氏
【日時】 2014 年 10 月 30 日 (木曜日) 18:30~20:30
【場所】 機械振興会館 地下 2 階ホール
【講演骨子】: 講演者より

2020 年に向け世界最先端 IT 国家創造宣言が現在進められているが、その中核となるオープンデータ、オープンガバメントの動向、及び、IT 政策の取り組み状況や課題について解説を行う。番号制度、パーソナルデータ、セキュリティの話ではなく、攻めの IT 戦略が話の中心となる。

【講演概要】
1. 「世界最先端 IT 国家創造宣言」

2 年前の 8 月 10 日に新しく政府 CIO 室が設立されている。私はこの部署で政府 CIO 補佐官として行政情報化の推進を行っている。特に本日お話しするオープンデータ等の「攻めの IT 投資」を主に担当している。

「世界最先端 IT 国家創造宣言」は、2013 年 6 月にまとめられた最新の IT 戦略である。この宣言は閣議決定されたものである。これまでも政府の IT 戦略はいろいろまとめられてきたが、閣議決定されたものはかなり珍しい。閣議決定は各大臣の了承をとったものであるため、実現に向けた各省の推進力はかなり強いものになる。

『世界最先端IT国家創造宣言』(2013.6閣議決定)
基本理念

1. 閉塞を打破し、再生する日本へ
 2. 世界最高水準のIT利活用社会の実現に向けて
- 目指すべき社会・姿**


1. 革新的な新産業・新サービスの創出及び全産業の成長を促進する社会

- ・ 日本国内外どこからでもアクセス可能となるオープンなプラットフォームを通じて、信頼性の高い公共データが提供され、民間や個人が保有するデータと自由に組み合わせ利用でき、**新産業・新サービスが創出される社会**を実現する。

2. 健康で安心して快適に生活できる、世界一安全で災害に強い社会

- ・ 医療・介護、健康、エネルギー、防災・減災などの分野において、我が国が抱えているリスク、課題点を正しく認識、把握、分析した上で、ITとデータを活用した新しい社会システムを構築することにより、様々な社会的課題の解決を図るとともに、多様な新しいサービスを創出する。これらを通じて、**健康で安心して快適に生活できる社会**を実現するとともに、**世界一安全で災害に強い社会**を実現する。

3. 公共サービスがワンストップで誰でもどこでもいつでも受けられる社会

- ・ 全ての行政サービスが、簡便な手段で電子的に受けられることを原則とし、少子高齢社会、離島を含む地方の活性化、人材の流動性などの基盤として、安心して使い勝手が良く、ワンストップで誰でもどこでもいつでも受けられる、**「便利なくらし」社会**を実現する。

基本理念としては、「閉塞を打破し、再生する日本へ」ということと「世界最高水準の IT 利活用社会の実現に向けて」という二つが設定されている。この宣言の目標年次は、2020 年である。実は最初にこの宣

言を作った時にはまだ東京オリンピックは決まっていなかった。その後、東京オリンピックが決定したことを受けて、今回実施した宣言の改定の中で、「ITを使ってオリンピック、パラリンピックに向けて有効な基盤を構築していこう」ということが盛り込まれている。従来のIT政策は、1～2年程度の比較的短い周期で作り直しているが、この宣言は比較的中長期をカバーするものとなっている。各省庁にとっても慌てて短時間で成果を出す必要がなく、安心して取り組んでもらえるようになっている。遠藤政府CIOは、よく「小さな成果をひとつひとつ積み重ねていこう」ということを言われる。この宣言もそのように進めていくべきだと考えている。

また、目指すべき社会の姿としては、①革新的な新産業・新サービスの創出及び全産業の成長を促進する社会、②健康で安心して快適に生活できる、世界一安全で災害に強い社会、③公共サービスがワンストップで誰でもどこでもいつでも受けられる社会の3つが示されている。今日お話しするオープンデータの推進は、ひとつめの「革新的な新産業・新サービスの創出及び全産業の成長を促進する社会」の中の一丁目一番地、つまりもっとも重要な位置付けのひとつとして「オープンデータ・ビッグデータの活用の推進」という項目としてあげられている。具体的な施策としては3つある。ひとつめは、「データカタログサイト」。これは、全省庁が保有しており、Webサイトによって公開されているデータを共通的に検索できるサイトを開発することである。

二つめは「共通の語彙（ごい）」つまりボキャブラリの基盤構築である。政府が公開しているデータは、省庁毎に同じような言葉で示されていても定義が異なるものが多く存在する。例えば、家族を数える「世帯数」は、ドミトリーで1つと数えるのが本来であるが省略する場合がある等、統一が取れていない場合がある。また、家屋の被災時によく言われる「半壊」についても自治体毎に定義が異なるようだ。定義が異なるとデータをマッシュアップすることができなくなる。このようなことを防ぐために用語の統一を推進していくことがこれである。

3つめは、パーソナルデータの利活用のルールである。オープンデータにおいてもパーソナルデータに関する議論がある。取り扱うデータは、個別データではなく集計したマクロなデータなのだが、例えば企業データについても、分類のやり方によっては個社を特定してしまうことになる場合がある。例えば中京地区であればトヨタだとわかってしまうなど。あるいは過疎地域における高齢者のような場合も、人口がごく少ない場合は、何歳以上というくくりで個人が特定してしまう可能性もある。このようなパーソナルデータに関するルールを明確化することが行われている。活断層の場所の公開を行っている自治体は半分程度であるようだ。すべての自治体でオープンにしていないのは、活断層の場所がわかることによって、家屋の資産価値が落ちたらまずいとこの考えかららしい。また、集計表だけでなく個表もオープンにしてくれという声も聞くがさすがにこれはできない。どこまでオープンにするかはとても難しい問題である。携帯電話の位置情報を活用して人口密度マップを作ることが実証実験として行われている。これを上手く使えば、どのような性別・年代の人が今どこにどのくらいいるか、さらにはどこの居住地から来た人がどの程度いるかということもわかるようになる。これを上手く使えば、マーケティングに活用もできるし、まちづくりや災害対策にも活用することができる。個人情報だからと全てについて規制をかけてしまったらこのような社会的メリットを享受できなくなる。米国では家の写真を撮ると即座に資産価値がわかったり、北欧では所有者の収入がわかったりするようなサービスが開発されていると聞く。日本国内だけを規制すると国際競争力が失われてしまう可能性もある。一方、情報発信元の情報を災害時に発信したらという議論があるが、広島で避難した家を狙った火事場泥棒が出たということも聞いたことがある。なかなか難しい問題だ。

さらに、「公共サービスがワンストップで誰でもどこでもいつでも受けられる社会」に関連する「利便性

の高い電子行政サービスの提供」においては、オープンデータの観点からは、「データフォーマット、用語、コード、文字等の標準化・共通化を進め、また API の公開していく」ことと「今後整備する情報システムにおいては、国際標準に適合した文字情報基盤を活用することを原則とする」ことが述べられている。平成6年くらいから市民本位の電子政府を構築する、といったことは言われていたが今日まであまり大きな成果は上がっていない。現在最も活発に行われているのは IT ガバナンスの強化であり、個別システム開発に関して年間 100 回以上のレビューが行われている。また、システム調達のガイドラインの構築も行われているのだが、昨今は従来のウォーターフォール型開発だけでなく、アジャイル型開発や IT アウトソーシング等様々な調達形態があるため取りまとめがなかなか難しい。政府全体で 5000 億円くらいのシステム投資が行われているため、数%削っただけでもその効果は大きい。さて、この電子行政サービス構築に関しては、先に述べた通り標準的な文字基盤を構築している。この領域を標準化することによって、全体としてのシステム開発の効率化を狙っている。具体的には、文字統合のための委員会を開いて、名前などに使われている変体仮名の整理等を行っている。戸籍は対象者が死亡後 150 年データを保存する必要があるため、200 年持つ仕組みを作りたいと考えている。

2. 電子行政オープンデータ戦略の推進

平成 24 年 7 月に IT 戦略本部で決定された電子行政オープンデータ戦略においては、いくつかの基本原則が設定されている。

電子行政オープンデータ戦略の推進について

(平成24年7月 | IT戦略本部決定)

- 意義・目的
 1. **透明性・信頼性向上**
 - 行政の透明性の向上、行政への国民からの信頼性の向上
 2. **国民参加・官民協働推進**
 - 創意工夫を活かした公共サービスの迅速かつ効率的な提供、ニーズや価値観の多様化等への対応
 3. **経済活性化・行政効率化**
 - 我が国全体の経済活性化、国・地方公共団体の業務効率化、高度化
- 基本原則
 1. 政府 **自ら積極的に** 公共データを **公開** すること
 2. **機械判読可能** で **二次利用が容易な形式** で公開すること
 3. **営利目的、非営利目的を問わず** 活用を促進すること
 4. **取組可能な公共データから速やかに** 公開等の具体的な取組に着手し、成果を確実に蓄積していくこと

3

まず「政府自ら積極的に公共データを公開すること」、これが大前提の考え方になる。また、「機械判読可能で二次利用が容易な形式で公開すること」という原則もある。省庁において従来ホームページで公開されているデータは、PDF 等で再利用が不可能なものが多い。これでは二次的に活用することができないので、オープンデータとは言えない。編集不可能な形式で PDF にしている省庁は、「公共データが改ざんされるのが怖いから」とよく言うが、読めない形態で提示したものを見ながら国民が新たにデータを打ち込むときにミスの方がよっぽど危ない。また様々な形式のデータを合わせて出すときに PDF の方が便利だという話

も聞く。最近では PDF と元々の形式の両方を出してもらうことをお願いしている。「営利目的、非営利目的を問わず活用を促進すること」というものもある。経済産業省では、アイデアボックスという電子掲示板サイトを使い、パブリックコメントを積極的にもらったり、官民での討論を行ったりしていた。掲示板はよく言われる通り「炎上」する可能性もあるが、やってみると案外議論は自然に常識的なところに落ち着くようだ。ただ、発言者はやはり限定されてくる。オープンデータを活用して新しいサービスを考えることを目的としたアイデアソンやハッカソンは毎週のように行われているが、これもだんだんいつものメンバーに閉じてしまって、幅広く参加の輪が広がるようにはなかなかならない。このあたりは今後の課題だ。「取得可能な公共データから速やかに公開していく」ことも示されている。やはりパーソナルデータの要素があるものは難しいので、そこからできるだけ遠いところから始めていく。例えば身近なデータだと、ごみの収集日とか、AED の設置場所、あるいは様々な観光資源に関するデータ等が有望である。

2013 年 6 月に行われた G8 サミットにおいて、「オープンデータ憲章」というものが採択されている。G8 でオープンデータに関する議論がされたわけだから、我々はとても注目していたが、残念ながらあまり新聞などには報道されなかった。オープンデータは、元々行政の透明性を上げるというオープンガバメント活動の中から生まれている。従って、ODA で提供されたお金がどのように使われたのかを公開することやマネーロンダリングのような観点からの議論が多かった。オープンデータ憲章では、オープンデータを「未開発の資源」と捉えている。従来の行政情報化の推進とは異なり、オープンデータの推進は実はあまりコストがかからない施策であるとも言われている。

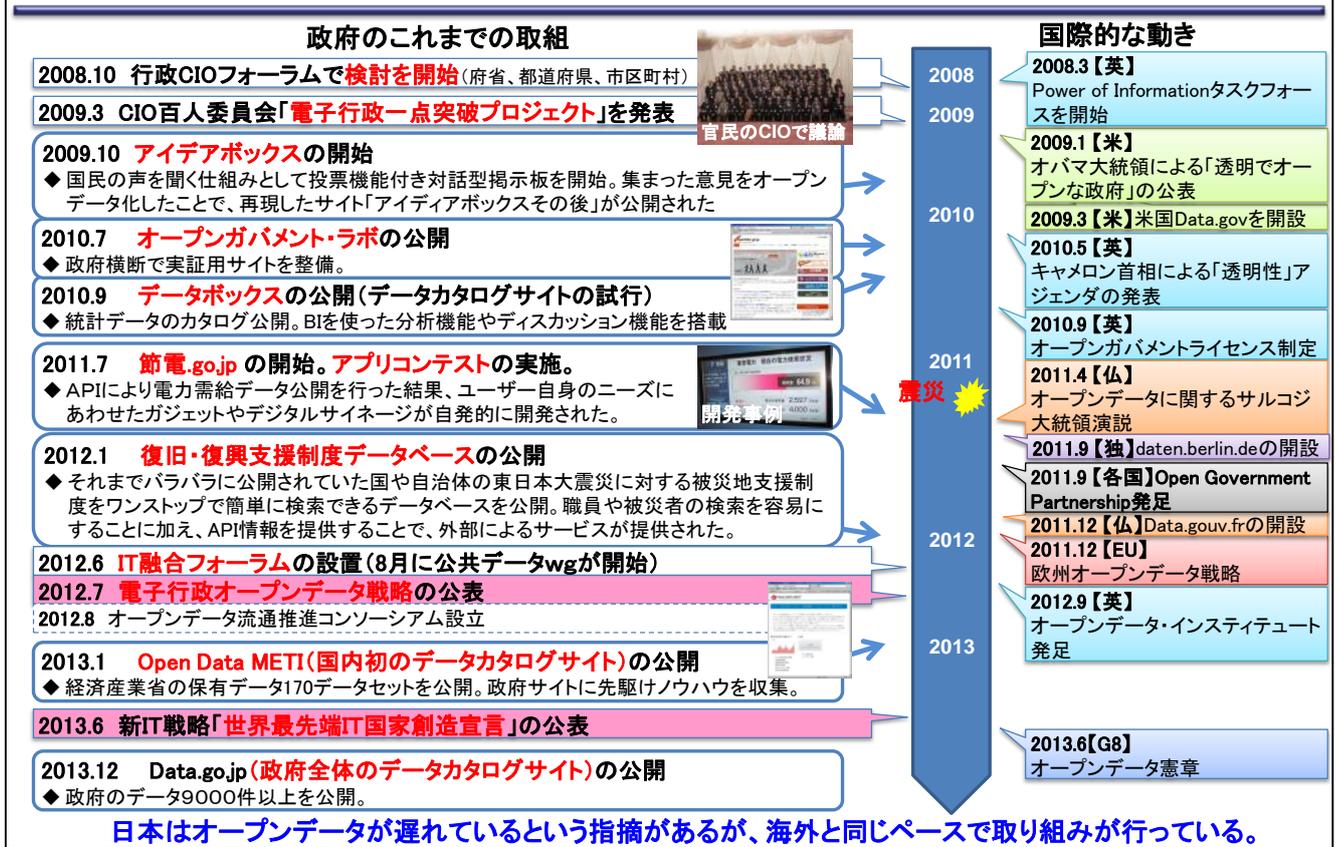
オープンデータ推進のロードマップとしては、「二次利用を促進する利用ルールの整備」「機械判読に適したデータ形式での公開の拡大」「データカタログ（ポータルサイト）の整備」「公開データの拡大」「普及・啓発、評価」といった取り組みが予定されている。データカタログサイトとしては「DATA.GO.JP」が作られている。これは複数の機関が保有・公開するデータの案内や横断的検索の機能を備えたポータルサイトである。パーソナルデータの利活用に関する制度見直し方針も整理されている。2014 年 6 月に大綱が決定、公表されており、2015 年 1 月の通常国会に法案を提出する予定である。これによってパーソナルデータかどうかという線が現状よりもクリアになると思う。

オープンデータの推進体制については、IT 総合戦略本部の配下に、電子行政オープンデータ実務者会議が作られており、慶応大学の村井純先生に主査をお願いしている。会議の配下にはデータ WG とルール・普及 WG が組織化されておりここでより具体的な作業が行われている。特にルールは重要だと認識している。様々な省庁の保有するオープンデータを活用する場合、省庁ごとに活用のためのルールがバラバラだと、最も厳しいルールに引っ張られてしまう恐れがある。政府統一利用規約を作ったので普及していきたい。

3. 具体的な取り組み

日本のオープンデータの取り組みは実は世界全体からみても最先端を走っている。2008 年に経済産業省で実施された行政 CIO フォーラムで検討が開始されているが、これは英国の Power of Information タスクフォースが立ち上がったのと同じような時期に当たる。その後、日本は 2011 年に東日本大震災に遭遇するが、結果として復旧・復興をテーマにオープンデータの推進はより実践的な形で進められることとなった。象徴的なのが震災直後の電力需給データの公開だ。計画停電データ等も積極的に公開されていった。日本のオープンデータへの取り組みは遅れているものではなく、少なくとも海外と同程度のペースで進められていると言っていい。

オープンデータのこれまでの取組



以下、国内におけるオープンデータに関連する具体的な取り組み事例について述べていく。

- Where does my money go? :

地方公共団体の予算内容を公表するアプリケーションである。少し前に流行った「世界が100人の村だったら」のイメージに近い。Web画面に自分の所得を入力すると、それがどのあたりにどの程度使われたかを表示するもの。これを活用することによる最大のメリットは、利用者が税金等に対して「一人称での参加意識」を持つようになることである。英国のハッカソンで作られたものを日本語化したもので、既に100自治体くらいがこれを活用している。たくさん使われ始めているので、開発元から協力してほしい旨の要求が来るようになったそうだ。日本では自治体毎に微妙に会計区分が異なるので自治体の横並び比較はまだ難しいようだ。
- 復旧・復興支援制度データベース :

国、県、市町村における災害復興時の各種支援制度を一括検索可能なデータベース。災害復旧・復興時の自治体等による支援制度は、阪神淡路大震災を契機に作られ始めたもので、中越地震の頃にはデータベース化がされはじめていたが、まだ使い勝手はよくなかった。現在の復旧・復興支援制度データベースは各種団体で行われている600の制度が蓄積されている。このデータベースは、APIが公開されており、民間における様々な人々が関連するアプリケーションを作っている。よく行政が作るWebサイトは使いにくいと言われているが、このデータベースは極力シンプルな機能を提供することに特化し、インターフェイスを通じて、民間などでサービスを自由に作ってもらうことを指向している。
- 鎌倉ゴミバスターズ :

ゴミの収集情報などを公開したもの。いろんなキャラクターを使った親しみやすい画面で、ゲーミフィケーションを取り入れたサービスで、楽しみながらゴミ捨てができるようになっている。

- **5374.com :**

同様にゴミの収集情報、分別情報を公開したもの。シンプルでわかりやすいアプリケーションを追及し、コードもオープンソースで公開している。このアプリケーションのおかげで、行政へのゴミ関連の問い合わせ件数が減ったといわれている。

- **さばえぶらり :**

福井県鯖江を中心とした観光情報やグルメマップを提供している。メガネをかけたレッサーパンダがキャラクターとして使われている。同様の観光に関するオープンデータは全国各地で実証実験が実施されている。

- **Fix My Street :**

街にある様々な問題を Web にアップし、その情報を市民全体で共有し議論するサービス。千葉市などで実施されているものである。例えば、「道に穴が空いている」等という情報を登録する。面白いのは必ずしも自治体の担当部局が問題を解決するだけではなくて、それを見た別の市民が対応してもかまわないこと。「何日までに直します」と自治体が答えたのに対して、近所の住民が「とりあえず穴を埋めておきました」という状況の変化がオープンにわかるところが興味深い。現場の写真をアップすることになるので、個人情報課題になるケースもあるが、それほど大きな問題は起こっていないようだ。

- **Sinsai.info :**

元々は、ハイチ地震やニュージーランド地震で使われたアプリが母体になったもの。東日本大震災の被災後数時間でボランティアによって立ち上がった。避難所情報や給水拠点など災害対策情報を共有するものである。

- **きらり川口ゆめマップ :**

AED の設置場所や、市の保有する施設情報を公開している。生活情報と防災情報を同じアプリケーションで扱えるので、日常使っているアプリで避難所などの検索ができるようになる。

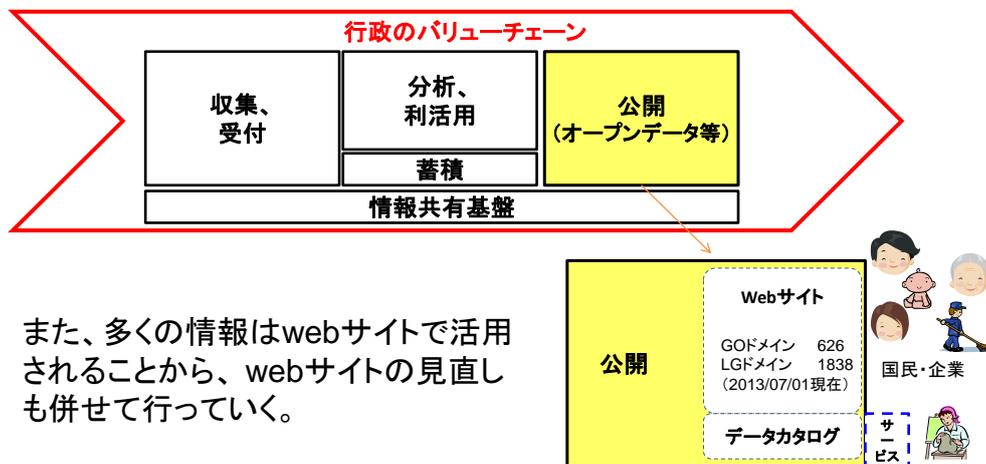
4. オープンデータからオープンガバメントへの回帰

現在、官民がコラボしながらアイディアソンやハッカソンが開催され、オープンデータに関する議論が進んでいる。オープンデータを推進することは行政にとって国民との会話を進めていくことになる。オープンデータの推進は、行政の一般職員により大きな責任を持ってもらうことにつながるだろう。

オープンデータがオープンガバメントという思想から生まれたものであることは先に述べた通りである。そして、今後はオープンデータの推進がもう一度オープンガバメントへと回帰していくと考えている。オープンデータを進めるためには、日常の行政事務の中で整理されたデータを使っていることが前提になる。そのため、データ利用を前提とした行政プロセスの見直しが必要となる。オープンデータは民間への情報公開を意味しているが、本来の行政におけるバリューチェーンを考えると、まずデータの収集、受付があり、その後収集したデータを蓄積し、分析・利活用を行うフェーズがある。そしてそのあとに公開されることになる。日本ではまだまだ公開のフェーズばかりに注目が集まっているが、例えば最初のデータ収集・受付時において、その後オープンに使ってもらうことを前提とした標準ルールを作る等やるべきことは多い。米国ではデータの分析・利活用についてもビジネスインテリジェンスの側面から活発な活動が行われている。

電子行政と一体でのオープンデータ推進

- 日常の業務の中で、整理したデータを使っていなければ、公開の作業を持続的に行うことは難しい。
- そのため、データ利用を前提とした行政プロセスの見直しが必要となる。



電子行政分野におけるオープンな利用環境整備のためのアクションプランとしては、新たな利便性の高いサービスを生み出すために、コンテンツとして組み合わせ自由な素材群を整備していくことがあげられる。先ほど述べたデータカタログもこの位置づけになる。さらに、コンテンツを整備していく上で、ガバナンスの強化、具体的には、ルール、ドメイン、コード、用語、文字等の標準化・共通化を行う基盤整備が必要になる。行政が利用する文字コードについては、今年度中に大部分を整備できる見込みである。用語、コードについては今後重要になるテーマになる。例えば府省については共通コードがあるが、独立行政法人には統一的なコードはない。「山」や「職業」を表すコードにも複数異なるコードがあり統一されていない。ドメインについても政府関連機関はすべて `go.jp` に統一されているように見えるが、実はノン `go` ドメインのサイトも結構ある。例えば住民基本台帳カードの総合サイトは、`juki-card.com` である。将来民間側に移管する可能性がある行政業務に関連したサイトはノン `go` ドメインのものが多く、これはある程度仕方ないことである。

データ標準を進めることによって、国から自治体まで、行政と民間の間でも正しく容易に情報交換できる仕組みができあがる。今、共通の語彙を作成することに力を入れている。共通語彙基盤は、Infrastructure for Multi-layer Interoperability の頭文字をとって、IMI と呼ばれている。これはそのまま「意味」を表していると考えてもらっていい。情報を正しく効率的に交換、活用していくために、様々な用語を構造的に定義していくことを目指している。IMI は、人、物、場所、日付等どの分野でも利用されるコア語彙と、病院、駅名等の分野固有の語彙であるが、他の分野から参照されやすいドメイン共通語彙、各分野での利用に特化したドメイン固有語彙の3つに分かれている。実際には全ての用語を標準化するのは現実的ではないので、参照する段階においてのみ使われる中間標準的なものを活用していく。米国では911以降テロ対策として情報共有のニーズが高まりっており、NIEM (National Information Exchange Model) というプロジェクトにおいて共通語彙の整備が進んでいる。用語の標準化を進めることで効率的な情報共有が行われるようになり、最終的には行政組織の資質向上や関連コストの削減なども可能になる。

オープンデータは、目立つキーワードではあるが、これ自体に惑わされることなく、行政の透明性を向上させるオープンガバメントや電子行政において利用者本位のサービスを実現することなども含めてボトムラインからの改革が必要だと考えている。

【質疑】

- ・ 質問 1: 「新サービスの創出」がオープンデータ活用の目的として掲げられているが、無償ならともかく、ビジネスになるようなアプリケーションはなかなか出てこないように思える。このあたりはどのようにお考えか？
- ・ 回答 1: やはりビジネスベースのサービスを作り出すのは容易ではないと思う。今、観光などをテーマにインキュベータの方々の協力を得ながらビジネスマッチングを行うことも検討している。また、ある自治体でよいアプリケーションができて、公開されているオープンデータが異なるため、現段階ではなかなか他の自治体にアプリケーションを横展開することが難しい。このあたりもビジネス化の障害になっている。
- ・ 質問 2: オープンガバメントの動向は大変興味深いお話だった。全容を掴むためにはどのようなサイトを見ればよいか？
- ・ 回答 2: オープンデータ流通推進コンソーシアム (<http://www.opendata.gr.jp/>)、オープンナレッジファンデーションジャパン (<http://okfn.jp/>) 等を参照していただきたい。また、OPEN METI の方からツイッターによって、ハッカソンやアイデアソンのスケジュール等もお知らせしている。これらの活動にも是非参加していただきたい。
- ・ 質問 3: オープンデータを推進していくためには、自治体側のモチベーションがとても重要だと思うが、実際のところどうなのか？
- ・ 回答 3: 正直なところ自治体毎にかなり温度差があるのが現状。やはり推進の中心となるキーマンがいるところが積極的に頑張っている。オープンデータの面白いところは、従来の IT 政策のように自治体の情報政策課から検討がはじまるのではなく、議会で議員の方から「当自治体におけるオープンデータへの取り組みはどうなっているか」という質問から検討がはじまるのが少なくないことだ。うまく進めている自治体には行政、民間の双方にキーマンがいたりする。また、情報政策課長から広報課長に変わった方がオープンデータを広報の一環で始めたというケースも見たことがある。広報誌自体のオープンデータ化はよいテーマのひとつだ。自分の住んでいる自治体の広報誌だけでなく、近隣の広報誌とか、田舎の父母の住んでいる場所の広報誌を見たいという要望は少なくないようだ。
- ・ 質問 4: 国際化という視点ではいかがか。海外の状況とデータで比較することはよくありそうな気がする。
- ・ 回答 4: 十分ある。多言語対応という点でも力を入れている。語彙基盤を整備することによって、翻訳効率も高くなる。貿易統計等各国の基本データを多言語化して、比較することは重要なことだと考えている。

以上

[<目次>](#)

～「経済産業省ガイドライン」の読みこなしポイント～
 「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」その4
 2-2-3. 個人データの管理（法第19条～第22条関連）

会員番号 6005 斉藤茂雄（個人情報保護監査研究会）

2-2-3. 個人データの管理（法第19条～第22条関連）

2-2-3-1. データ内容の正確性の確保（法第19条関連）

法第19条

個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければならない。

事業者は、保有する個人データを、それぞれの利用目的に応じて、その必要な範囲内で正確性・最新性を確保すればよく、一律に常に最新化する必要はない。

※個人情報保護監査研究会注：例えば、クレジットカード情報等は、利用目的の達成において必要最小限の保存期間を設定し、保存場所を限定し、保存期間経過後は適切かつ速やかに破棄することが望まれます。

2-2-3-2. 安全管理措置（法第20条関連）

法第20条

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない

個人データが漏えい、滅失又はき損等をした場合に、本人が被る権利利益の侵害の程度を考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとしなければなりません。

【必要かつ適切な安全管理措置を講じているとはいえない場合】

事例1) 非公開の個人データが事業者のウェブ画面上で公開されている状態を事業者が放置している場合

事例2) 個人データにアクセスする必要がなくなった従業員について、事業者がアクセスできる状態を放置していた場合で、その従業員が個人データを漏えいした場合

事例3) 本人がサービスを受けるために登録していた個人データが、システム障害により破損したが、復旧できず本人がサービスの提供を受けられなくなった場合

事例4) 個人データに対してアクセス制御が実施されておらず、アクセスを許可されていない従業員がそこから個人データを入手して漏えいした場合

事例5) 個人データをバックアップした媒体が、持ち出しを許可されていない者により持ち出し可能な状態になっており、その媒体が持ち出されてしまった場合

事例6) 委託する業務内容に対して必要のない個人データを提供し、委託先が個人データを漏えいした場合

※個人情報保護監査研究会注：経産省GLでは、リスクに応じた必要かつ適切な安全管理策を講じるよう示しており、最も注目すべきリスクが、「本人が被る権利利益の侵害」です。しかし、すべての個人情報に対し、一律に安全管理措置を講じることを求めているではありません。

※ご参考(2014年9月26日に追加された、経産省GL改正案。アンダーライン部分・以下同様)
特に、中小企業者においては、事業の規模及び実態、取り扱う個人データの性質及び量等
 に応じた措置を講じることが望ましい。

※個人情報保護監査研究会注:経産省GL改正案では、「特に、中小企業者」と言っていますが、大企業でも同じことです。現行の経産省GLでも、例えば、以下の安全管理措置の義務違反とならない事例を挙げています。

【安全管理措置の義務違反とはならない場合(従業者の監督及び委託先の監督の義務違反ともならない場合)】

事例1)内容物に**個人情報が含まれない荷物**等の宅配又は郵送を委託したところ、誤配によって宛名に記載された個人データが第三者に開示された場合

事例2)書店で誰もが容易に入手できる**市販名簿**(事業者において全く加工をしていないもの)を処分するため、シュレッダー等による処理を行わずに廃棄し、又は、廃品回収に出した場合

組織的な安全管理措置

組織的な安全管理措置とは、安全管理について従業者の責任と権限を明確に定め、安全管理に対する規程や手順書(以下「規程等」という。)を整備運用し、その実施状況を確認することをいいます。

【組織的な安全管理措置として講じなければならない事項とその例示】

① 個人データの安全管理措置を講じるための組織体制の整備

個人情報保護管理者の設置

作業責任者の設置及び担当者の限定

監査責任者の設置/監査実施体制の整備

漏えい等の事故が発生又は発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備

漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備

※ご参考(2014年9月26日に追加された、経産省GL改正案。)

- ・個人データの安全管理の実施及び運用に関する責任及び権限を有する者として、個人情報保護管理者(いわゆる、チーフ・プライバシー・オフィサー(CPO))を設置し、原則として、役員を任命すること
- ・個人データの取扱いを総括する専門部署の設置、及び個人情報保護管理者(CPO)が代表者となり、社内の個人データの取扱いを監督する「管理委員会」の設置
- ・個人情報保護対策及び最新の技術動向を踏まえた情報セキュリティ対策に十分な知見を有する者が社内の対応を確認すること(必要に応じ、外部の知見を有する者を活用し確認することを含む)などによる、監査実施体制の整備

※個人情報保護監査研究会注:組織において個人データを安全に管理するには、統一的なルールを定めこれを維持・運用する組織体制の整備が必要です。さらに経産省GL改正案では、組織体制について、実質的な監督管理能力、並びに、情報セキュリティについての監査能力を持った監査体制の整備を求めています。

② 個人データの安全管理措置を定める規程等の整備と規程等に従った運用

- 個人データの取扱いに関する規程
- 情報システムの安全管理措置に関する規程
- 建物、部屋、保管庫等の安全管理に関する規程等
- 委託先の選定基準、委託した個人データの取扱状況を確認するためのチェックリスト等
- 定められた規程等に従って業務手続が適切に行われたことを示す監査証拠の保持

※ご参考(2014年9月26日に追加された、経産省GL改正案。)

【個人データの取扱いに関する規程等に記載することが望まれる事項の例】

(1) 取得・入力、(3)利用・加工

……………スマートフォン、パソコン等の記録機能を有する機器の接続を制限し、媒体及び機器の更新に対応する。

※個人情報保護監査研究会注:スマートフォンの持ち込み・接続による漏えい事故が発生したことによる、追加改正案と思われます。

USBポートの無効化などの対策を講じるだけでなく、規定する必要があります。

③ 個人データの取扱い状況を一覧できる手段の整備 (詳細省略)

④ 個人データの安全管理措置の評価、見直し及び改善 (詳細省略)

人的安全管理措置

※個人情報保護監査研究会注:人的安全管理措置とは何かについては、経産省GL改正案で文言が追加されたため、改正案を掲載します。

※ご参考(2014年9月26日に追加された、経産省GL改正案。)

人的安全管理措置とは、従業者(「個人情報取扱事業者の組織内にあつて直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員(正社員、契約社員、嘱託社員、パート社員、アルバイト社員等)のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。)に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう

【各項目を実践するために講じることが望まれる手法の例示】

① 雇用契約時における従業者との非開示契約の締結、

及び委託契約等(派遣契約を含む。)における委託元と委託先間での非開示契約の締結

- 契約終了後も一定期間有効であるようにすることが望ましい。
- 非開示の義務を、就業規則等の社内規程に規定することも考えられる。
- 社内規程に非開示の義務を規定する場合には、特に、労働基準法第89条及び第90条を遵守する必要がある。
- 個人情報保護と営業秘密の保護はその目的範囲等が異なるため、従業者の「納得感」の向上の観点から、秘密保持契約は峻別する(別書面であるか否かは問わない)ことが望ましい。
- 非開示契約に違反した場合の措置に関する規程の整備

- ② 従業者に対する内部規程等の周知・教育・訓練
- 役割及び責任を定めた内部規程等についての周知
 - 役割及び責任についての教育・訓練の実施
 - 必要かつ適切な教育・訓練が実施されていることの確認

物理的安全管理措置

物理的安全管理措置とは、入退館(室)の管理、個人データの盗難の防止等の措置をいいます。

【物理的安全管理措置として講じなければならない事項】

① 入退館(室)管理の実施

※ご参考(2014年9月26日に追加された、経産省GL改正案。)

【各項目を実践するために講じることが望まれる手法の例示】

・[入退館\(室\)の記録の保存](#)

※個人情報保護監査研究会注:経産省GL改正案に追加された「記録の保存」は、事故発生時の原因究明等、検証のために必要な措置です。

② 盗難等の防止

- 個人データを記した書類、媒体、携帯可能なコンピュータ等の机上及び車内等への放置の禁止
- 離席時のパスワード付きスクリーンセイバ等の起動によるのぞき見等の防止
- 個人データを含む媒体の施錠保管
- 氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管

※ご参考(2014年9月26日に追加された、経産省GL改正案。)

【各項目を実践するために講じることが望まれる手法の例示】

・[入退館\(室\)の際における業務上許可を得ていない記録機能を持つ媒体及び機器の持ち込み及び持ち出しの禁止と検査の実施](#)

・[カメラによる撮影や作業への立ち会い等による記録又はモニタリングの実施](#)

③機器・装置等の物理的な保護

- 機器・装置等の、安全管理上の脅威(例えば、盗難、破壊、破損)や環境上の脅威(例えば、漏水、火災、停電)からの物理的な保護

技術的安全管理措置

技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいいます。

【技術的安全管理措置として講じなければならない事項とその例示】

①個人データへのアクセスにおける識別と認証

- ID とパスワードによる認証、生体認証等の実施
- 使用できる端末又はアドレス等の識別と認証の実施

②個人データへのアクセス制御

- 個人データへのアクセス権限を付与すべき者の最小化
- アクセス権限を有する者に付与する権限の最小化
- 個人データを格納した情報システムの利用時間の制限
- 個人データを格納した情報システムへの権限の無いアクセスからの保護(例:ファイアウォール、ルータ等の設定)
- 個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証(例:ウェブアプリケーションのぜい弱性有無の検証)

③個人データへのアクセス権限の管理

- 個人データにアクセスできる者を許可する権限管理の適切かつ定期的な実施
- 個人データを取り扱う情報システムへの必要最小限のアクセス制御の実施

④個人データへのアクセスの記録

- 個人データへのアクセスや操作の成功と失敗の記録

※ご参考(2014年9月26日に追加された、経産省GL改正案。)

・[個人データへのアクセスや操作の成功と失敗の記録及び不正が疑われる異常な記録の存否の定期的な確認](#)

- 採取した記録の漏えい、滅失及びき損からの適切な保護

⑤個人データを取り扱う情報システムについて不正ソフトウェア対策

- ウイルス対策ソフトウェアの導入
- オペレーティングシステム(OS)、アプリケーション等に対するセキュリティ対策用修正ソフトウェアの適用

⑥個人データの移送(運搬、郵送、宅配便等)・送信時の対策

- 個人データの移送時における紛失・盗難に備えるための対策
- 個人データを送信する際の、個人データの暗号化等の秘匿化

⑦個人データを取り扱う情報システムの動作確認時の対策

- 情報システムの動作確認時のテストデータとして個人データを利用することの禁止

⑧個人データを取り扱う情報システムの監視

- 個人データを取り扱う情報システムの使用状況の定期的な監視
- 個人データへのアクセス状況(操作内容も含む。)の監視

※ご参考(2014年5月16日に追加された、経産省GL改正案。アンダーライン部分)

・[個人データを取り扱う情報システムへの外部からのアクセス状況の監視\(例えば、IDS・IPS等\)](#)

※個人情報保護監査研究会注:

IDS:Intrusion Detection System 侵入検知システム。コンピュータやネットワークに対する不正行為を検出・通知する

IPS:Intrusion Prevention System 侵入防止システム。不正行為を検出・通知・遮断する。

次回は、「2-2-3. 個人データの管理(第21、22条関連)」の読みこなしポイントを掲載します。
バックナンバー目次 <http://1.33.170.249/saajpmsMETIGL/000METIGL.html>

(↑バックナンバー目次のURLが変更となりました。)

個人情報保護監査研究会 <http://www.saa.or.jp/shibu/kojin.html>

■
[<目次>](#)

注目情報 (2014. 10～2014. 11) ※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。

■ **大規模・複雑なシステムの障害診断の新手法を提案 (2014/11/19)**

～ システムズエンジニアリングに基づき、迅速かつ的確に診断する手法を JASA と共同開発 ～

IPA(独立行政法人情報処理推進機構、理事長:藤江 一正)SEC(ソフトウェア高信頼化センター)は、大規模・複雑なシステムで障害が発生したときに、迅速かつ的確に診断する手法を、JASA(一般社団法人組込みシステム技術協会)と共同で開発し、取りまとめました。

本手法では、シミュレーションによる障害の再現を行う方法を採用しており、実際のシステムを毀損することなく、想定されるすべての障害を仮想的に発生させて検証することができます。としている。

<http://www.ipa.go.jp/sec/info/20141119.html>

■ **2014 年の 10 大セキュリティ事件ランキング (2014/11/12)**

マカフィー株式会社(日本法人)は、日本国内の経営層や情報システム部門などのビジネスパーソンを対象に「2014 年のセキュリティ事件に関する意識調査」を実施し、その結果を基にした 2014 年の 10 大セキュリティ事件を発表した。本記事は 11 月 12 日のNHKでも放送されている。

<http://www.mcafee.com/jp/about/news/2014/q4/20141112-02.aspx>

■ **平成 27 年度春期 情報処理技術者試験実施日は平成 27 年 4 月 19 日 (日) (2014/10/19)**

IPA(情報処理推進機構)から、平成 27 年度春期のシステム監査技術者試験などの実施案内が公表された。

https://www.jitec.ipa.go.jp/1_02annai/h27haru_exam.html

■ **2014 年に発覚した主な情報漏洩事件 (2014/10/09)**

日経コンピュータ記事「JAL が最大 75 万件の顧客情報漏洩 ドコモ、佐川、ヤマト、JR 東も攻撃受ける」の中に、2014 年に発覚した主な情報漏洩事件一覧表が掲載されている。記事では、漏洩の原因としては明らかにリスト型攻撃が多い。もはや同じ ID とパスワードを使い回さないよう、注意喚起するだけでは不十分で、多段階認証などの仕組みを整えることが、事業者側に求められる。としている(本記事は会員(無料会員)ログインが必要)。

<http://itpro.nikkeibp.co.jp/atcl/column/14/346926/100700073/?ST=security&P=1>

[<目次>](#)

2014.11

【 協会主催イベント・セミナーのご案内 】

■月例研究会（東京）

第198回	日時:2014年12月16日(火)18:30~20:30 場所:機械振興会館 地下2階多目的ホール	
	テーマ	企業におけるセキュリティ戦略
	講師	日本アイ・ビー・エム株式会社 IBM Computer Security Incident Response Team (CSIRT) IT Forensic Analyst 守屋 英一 氏
	講演骨子	<p>本年3月、NTT 出版より「サイバーセキュリティ」という本を出版させて頂きました。本書では、サイバー攻撃を社会的背景、技術的対策、法律および企業経営などの様々な視点から問題の解決に向けて解説しています。</p> <p>本講演では、本書の内容を踏まえて、サイバー攻撃及び内部犯行による企業への影響に対して、企業が取り組むべきセキュリティ戦略について解説させていただきます。</p>
	お申し込み	HPでご案内中です。 http://www.saa.or.jp/kenkyu/kenkyukai_sokuhou201412.html

第199回	日時:2015年1月20日(火)18:30~20:30 場所:機械振興会館 地下2階多目的ホール	
	テーマ	インターネットバンキングに係る不正送金事犯の現状と対策
	講師	警察庁 生活安全局 情報技術犯罪対策課 指導第一係 課長補佐 小竹 一則 氏
	講演骨子・お申し込み	確定次第、HPでご案内します。

■西日本支部合同研究会 in OSAKA（大阪）

申し込み受付中	日時:2014年11月29日(土)13:00~17:00/11月30日(日)10:00~11:30 場所:[1日目]国際カンファレンスプラザ A-3 会議室(大阪市中央区安土町 2-3-13 大阪国際ビル) [2日目]大阪府「津波・高潮ステーション」(大阪市西区江之子島 2-1-64)	
	テーマ	ICTによる災害に強いしなやかな社会の実現とシステム監査の重要性
	開催趣旨	<p>来年は、阪神・淡路大震災の発生から20年の節目の年となります。次に来る大震災等の大規模災害に対し、予防力に回復力を加味した「レジリエンス」を高め、強くしてしなやかな社会の構築を目指すことが必要となってきました。今回は、これらを背景に「ICTによる災害に強いしなやかな社会の実現とシステム監査の重要性」をテーマとして、西日本支部の会員各位より発表していただきます。また、2日目は、大阪府の防災啓発施設である、「津波・高潮ステーション」を見学し、津波災害を大スクリーンで体感していただきます。</p>
	講師、講演概要、お申し込み	<p>詳細はHPでご案内しています。</p> <p>http://www.saa.or.jp/shibu/kinki/nishi_godo_kenkyu2014.html</p>

[<目次>](#)

■近畿支部第149回定例研究会（大阪）

日本システム監査人協会近畿支部と ISACA 大阪支部の合同講演会

申し込み受付中	日時:2014年12月13日(土)15:00~17:00 場所:大阪大学中之島センター 3階 講義室301
	テーマ 地域情報化と防災 ～CATVネットワークを利用した緊急告知と 地方公共団体のICT-BCPの現況～
	講師 (株)嶺南ケーブルネットワーク 顧問(情報通信担当) JKソリューションズ 代表 前敦賀市総務部技監(情報管理・IT推進) ITコーディネータ・システム監査技術者・SAAJ 会員 川端 純一 様
	講演骨子 巨大地震の脅威や、異常な集中豪雨などの異常気象による市民の被害を最小にするためには、迅速で正確な市民のライフスタイルに合わせた多様な情報伝達が必要です。巨大災害発生時の地方公共団体の防災実務を支える情報通信ネットワークとして、広く市民に親しまれているCATVネットワークを活用した緊急告知方法と、種々多様なメディアの利活用についてご紹介します。さらに、発災時の災害対策本部実務を支える庁内情報通信ネットワークや、各種業務アプリケーションの運用管理の業務継続を図ることは最重要課題です。ここでは、地方公共団体のICT-BCPの現況と課題、さらに評価についてご紹介します。
お申し込み	HPでご案内中です。(http://www.saa-j.or.jp/shibu/kinki/kenkyukai149.html)

■システム監査普及サービス(全国)

申し込み常時受付中	情報システムの健康診断をお受けになりませんか。実費のみのご負担でお手伝いいたします。
	概要 経験豊富な公認システム監査人が、皆様の情報システムの健康状態を診断・評価し、課題解決に向けてのアドバイスをいたします。これまでに多くの監査実績があり、システム監査普及サービスを受けられた会社等は、その監査結果を有効に活用されています。 システム監査の普及・啓発・促進を図る目的で実施しているものです。監査にかかる報酬は無償で、監査の実施に要した実費(通信交通費、調査費用、報告書作成費用等)のみお願いしております。ご相談内容や監査でおうかがいした情報等は守秘します。 詳細はHPでご案内しています。(http://www.saa-j.or.jp/topics/hukyuservice.html)
お問い合わせ	システム監査事例研究会主査 大西 (Email: jireiken@saa-j.jp)

■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.saa-j.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」(非売品)

[<目次>](#)

■公認システム監査人特別認定講習（東京・大阪）

開催中	公認システム監査人(CSA: Certified Systems Auditor)およびシステム監査人補(ASA: Associate Systems Auditor)の資格制度にもとづく、認定条件を得るための講習です。	
	概要	システム監査技術者試験と関連性のある各種資格の所有者については、特別認定制度に基づく本講習により、CSA・ASA 認定申請に必要な資格要件を満たすことができます。特別認定制度の詳細はHPで公開しています (http://www.saa.or.jp/csa/shosai.pdf)。
お申し込み	講習開催スケジュールと申し込み先をHPでご案内しています。 (http://www.saa.or.jp/csa/tokubetsu_nintei.html)	

【 外部主催イベント・セミナーのご案内 】

■第14回CFOフォーラム・ジャパン2014（東京）

日時:2014年12月2日(火) 9:00~18:30	
場所:経団連会館 国際会議場 経団連ホール	
テーマ	日本企業の競争力強化と企業価値創造に向けて —不確実なボーダレス経済をリードするCFOの課題—
詳細	http://www.cfo.jp/cforum2014/

■第9回 青山学院 公開シンポジウム（東京）

日時:2014年12月20日(土) 13:30~17:30	
場所:青山学院大学青山キャンパス 17号館 6階 本多記念国際会議場	
テーマ	わが国監査法人の将来像—業容、人材、及び品質管理の観点から—
概要	第一部 (13:40~14:30) 特別講演 岩田 喜美枝 氏 (公益財団法人 21世紀職業財団 会長) 「女性はもっと活躍できる—人生を豊かに、企業を元気に—」 第二部 (14:40~15:30) 基調講演 森 公高 氏 (日本公認会計士協会 会長) 「わが国会計プロフェッションの将来像—10年後の会計士業界を見据えて—」 (15:50~17:30) パネルディスカッション 「わが国監査法人の将来像—業容、人材、品質管理の観点から—」
お問い合わせ	青山学院大学大学院 会計プロフェッション研究センター 「第9回公開シンポジウム」担当 TEL: 03-3409-6047(受付時間:月~金 9:00~11:30 / 12:30~21:00) 詳細: http://www.aoyama.ac.jp/sp/info/event/2014/01775/

[<目次>](#)

協会からのお知らせ

【CSA/ASA資格をお持ちの方へ：資格更新申請手続きについて】

2015年度公認システム監査人及びシステム監査人補の更新手続きのお知らせです。

- ・資格認定期限が2014年12月31日で満了となる方について、認定の更新手続きを行います。
- ・資格更新申請の受付期間は2015年1月1日(木)から1月31日(土)までの1か月間です。
- ・今回の更新対象者は、資格認定番号が下表の方です(2014年度よりすべて2年度ごとの更新です)。

	取得年度	CSA 認定番号	ASA 認定番号	2015年1月更新	ご参考 2016年更新
1	2002年度	K00001～K00253	H00001～H00193		○
2	2003年度	K00254～K00320	H00194～H00263		○
3	2004年度	K00321～K00357	H00264～H00316	○	
4	2005年度	K00358～K00401	H00317～H00384		○
5	2006年度	K00402～K00447	H00385～H00433		○
6	2007年度	K00448～K00478	H00434～H00473	○	
7	2008年度	K00479～K00518	H00474～H00514		○
8	2009年度	K00519～K00540	H00515～H00538	○	
9	2010年度	K00541～K00553	H00539～H00557	○	
10	2011年度	K00554～K00568	H00558～H00572		○
11	2012年度	K00569～K00580	H00573～H00586	○	
12	2013年度	K00581～K00596	H00587～H00595		○

- ・資格更新申請には、更新申請書や継続教育実績申告書などの提出が必要です。準備をお願いします。
- ・更新手続きの詳細は、HPの「CSAの資格をお持ちの方へ」(<http://www.saa.or.jp/csa/forCSA.html>)をご覧ください。

[＜目次＞](#)

協会からのお知らせ 【年会費納付時期について】

会員番号 1760 齋藤由紀子（事務局長）

会員各位

昨年までは、1月1日付で当該年度(1月～12月)の年会費を請求していましたが、2014年7月10日理事会にて、「会員規程」が改定されたことに伴い、今回、次年度年会費の請求書を、2014年12月1日付で発送いたしますので、ご準備のほどよろしくお願い致します。

【改定後の規程】

第3条（会費）：会員は、当該年度(1月～12月)の年会費を、請求書に記載された期日までに支払わなければならない。いったん支払われた会費は返却しない。

【2015年度会費請求の内容】

<金額> 正会員個人:2015年度会費 ¥10,000- (消費税非課税)

正会員団体:2015年度会費 ¥10,000.- ~ ¥100,000.- (消費税非課税)

<払込期限>2014年2月末日

ただし、正会員団体に限り、事業年度予算等の事情による、「納付期限延長願い」をご提出いただくことで納入期限の延長が可能です。

お申し出先: <http://www.saa.or.jp/toiwase/index.html> (事務局)

<振込先> 郵便振替口座:00110-5-352357 (請求書発送時に振込依頼書を同封します)

加入者名:日本システム監査人協会事務局

銀行振込口座:みずほ銀行八重洲口支店(普通)2258882

口座人名:特定非営利活動法人日本システム監査人協会

トクヒ)ニホンシステムカンサニンキョウカイ

※銀行振込の際は、《会員No.》4桁の数字を氏名の前に付けて下さいようお願い致します。

(会員番号が付けられない場合は、メールで振込内容をお知らせください。)

【2014年度以前の会費未納の場合】

一部の会員の方について、2014年度の会費のお支払が未だ確認できません。2014年12月31日までに納付が確認できない場合は、除名処分となりますので、至急お手続きいただきますようお願い致します。

【ご寄附のお願い】

協会では、運営基盤のより一層の改善を図りたく、一口3,000円のご寄附をお願い申し上げます。

<寄附金額> ¥3,000/一口 ご寄附は、何口でも承ります。

<振込先>ご寄附は、協会会費に合算して、会費振込先にお振込みください。

<東京都への個人情報提供>

法令に基づき、寄附者名簿(氏名、ご住所)を、所轄庁の東京都へ報告致します。

何卒ご了承賜りますようお願い致します。

<ご寄附についてのお問合せ>: <http://www.saa.or.jp/toiwase/index.html> (事務局)

[<目次>](#)

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。

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。

- ・協会活動全般がご覧いただけます。 <http://www.saaaj.or.jp/index.html>
- ・会員規程にも目を通しておいてください。 http://www.saaaj.or.jp/gaiyo/kaiin_kitei.pdf
- ・皆様の情報の変更方法です。 <http://www.saaaj.or.jp/members/henkou.html>

- ・会員割引や各種ご案内、優遇などがあります。 <http://www.saaaj.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。

- ・各支部・各部会・各研究会等の活動です。 <http://www.saaaj.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。

- ・協会出版物が会員割引価格で購入できます。 <http://www.saaaj.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。

- ・セミナー等のお知らせです。 <http://www.saaaj.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。

- ・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.saaaj.or.jp/csa/index.html>

- ・PDF会報と電子版会報があります。 (http://www.saaaj.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.saaaj.or.jp/members/kaihouinfo.pdf>

- ・右ページをご覧ください。 <http://www.saaaj.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 >](#)

2014.11

【 SAAJ協会行事一覧 】			
2014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
11月	13日 理事会 14日 予算申請提出依頼(11/30〆切) 支部会計報告依頼(1/10〆切) 18日 2015年度年会費請求書発送準備 20日 会費未納者除名予告通知発送 30日 予算申請提出期限	中旬 認定委員会:CSA 面接 19日 第197回月例研究会 20日 CSA・ASA 更新手続案内 〔申請期間 1/1~1/31〕 28日 認定委員会:CSA 面接結果通知	29日 西日本支部合同研究会 (開催場所:大阪市)
12月	1日 2015年度年会費請求書発送 2015年度予算案策定 11日 理事会:2015年度予算案、 会費未納者除名承認 12日 第14期総会資料提出依頼(1/9〆切) 19日 会計:2014年度経費提出期限	6日 法制化検討PT 事前打合せ 6日 事例研:第16回課題解決セミナー 10日 認定委員会:CSA/ASA 更新手続 案内メール発信 16日 第198回月例研究会 20日 CSA 認定証発送 21日 第25回 CSA フォーラム	13日 東北支部:支部総会
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
1月	8日 理事会:通常総会議案審議 9日 総会開催案内掲示・メール配信 9日 総会資料(〆) 19日 会計:2013年度決算案 24日 会計:2013年度会計監査 31日 償却資産税・消費税	認定委員会:CSA・ASA 更新申請受付 〔申請期間 1/1~1/31〕 20日 第199回月例研究会 20日 春期公認システム監査人募集案内 〔申請期間 2/1~3/31〕	10日 会計:支部会計報告期限 16日 近畿支部:支部総会
2月	5日 理事会:通常総会議案承認 6日 総会資料公表 20日 第14期通常総会・特別講演 25日 法務局:資産の変更登記、 活動報告書提出 28日 年会費納入期限	CSA・ASA 春期募集(2/1~3/31)	
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	
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	19日 2015年春期情報技術者試験
以下は、昨年:2014年の行事一覧です。			
5月	8日 理事会 29日 会費未納督促メール	認定委員会:新規 CSA/ASA 面接 15-16 事例研:システム監査実践セミナー 22日 第191回月例研究会	
6月	12日 理事会 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)	7日 事例研:第14回課題解決セミナー 10日 新規 CSA/ASA 承認 10日 CSA フォーラム	28日 近畿支部:システム監査体験セミナー(入門編):
7月	1日 会費未納者督促状発送 8日 支部助成金支給 10日 理事会	1日 秋期公認システム監査人募集案内 〔申請期間 8/1~9/30〕 3日 第192回月例研究会 22日 第193回月例研究会	14日 支部会計報告〆切
8月	(理事会休会) 会費督促電話作業(役員) 23日 中間期会計監査	秋期公認システム監査人募集開始~9/30 20日 第194回月例研究会 30-31日 事例研:第24回システム監査実務セミナー(前半)	30~31日 東北支部:合宿研修会 30~31日 近畿支部:システム監査体験セミナー(実践編)
9月	11日 理事会	13-14日 事例研:第24回システム監査実務セミナー(後半) 8日 第24回 CSA フォーラム 18日 第195回月例研究会	6~7日 中部、北信越支部 /JISTA 中部合同合宿
10月	9日 理事会	30日 第196回月例研究会	25日 近畿支部:IT-BCP 体験セミナー

※注 定例行事予定の一部は省略。

[<目次>](#)

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

2014 年度の年間テーマは、「〇〇〇のためのシステム監査」とし、四半期ごとに「〇〇〇のための」について具体的なテーマを設定して、システム監査に関する皆様からのご意見ご提案を募集しています。

これまで2月号から4月号までが「公(おおやけ)のためのシステム監査」、5月号から7月号までが「情報化社会のためのシステム監査」、8月号から10月号までが「次世代のためのシステム監査」をテーマとし、様々なご意見ご提案をいただきました。ありがとうございました。

11月号から1月号までの3か月は、「情報システム部門のためのシステム監査」をテーマにしています。今号も前号に引き続いて皆様から記事の投稿をいただいています。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、投稿ボタ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（論文投稿規程があります）

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。システム監査にとどまらず、情報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します。ただし、投稿された記事については、表現の訂正や削除を求め、又は採用しないことがあります。また、編集担当の判断で字体やレイアウトなどの変更をさせていただきますことがあります。

次の投稿用アドレスに、次号会報募集案内メールに添付されるフォーマット(Word)を用いて、下記アドレスまで、メール添付でお送りください。

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）

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一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: 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/toiwase/>

■会報は会員への連絡事項を含みますので、会員期間中の会員へ自動配布されます。

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。

【送付停止】 <http://www.skansanin.com/saaj/>

Copyright(C)2014、NPO 法人 日本システム監査人協会

掲載記事の転載は自由ですが、内容は改変せず、出典を明記していただくようお願いします。

■□■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、中山孝明、藤野明夫

編集支援: 仲厚吉 (会長)

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>](#)