特定非営利活動法人
日本システム監査人協会報

2014年11月号
No 164

No. 164（2014年11月号）＜10月25日発行＞

新テーマ「情報システム部門のための
システム監査」の始まりです。事業展開を
支える大黒柱に思いを馳せてみませんか？
他にも興味深い記事が満載です！

写真提供：藤澤博会報主査

巻頭言

テーマ：システム監査とＳＡＡＪの曲り角

会員番号555　松枝　憲司（副会長）

日本にシステム監査基準が制定されたのが1985年、任意団体としてのSAAJ（以下協会）設立が1987年で、既に四半世紀以上経過している。この間、欲しい情報を世界中から入手できるツール（システム）を誰もが持つことができるようになり、内部統制が現代人の基礎知識となり、情報セキュリティに関する事件や事故が日常茶飯事となっているこの時代に「システム監査」が全く元気がない。私の周りでは、ビジネスとしてのシステム監査の話をほとんど聞かなくなっている。マスコミに取り上げられることもないし、システム監査という用語自身を目にしなくなっている。それに呼応するようにシステム監査技術者試験の受験生も減少の一途である。

協会は設立以来「システム監査の普及」を目的としてきたが、一体どうしたことなのであろうか。

続きは、投稿記事「システム監査とSAAJの曲り角」をご覧ください。

＜目次＞

2014.10

めだか　【情報システム部門のためのシステム監査】

情報システム監査というのは受ける情報システム部門側からすると依然として「余計な仕事が増えるだけの面倒なもの」という印象を受けます。当方からするとまずこの認識違いを変えていかないといけないと思っています。情報システム監査は、決してネガティブなものではなく、情報システム部門にとって「継続的に改善する」機会であるということです。

何故、ネガティブな印象を与えてしまうのか？ということを考えてみたときに、思い当たるのは情報システム監査が「不足していることの特定と何が問題であるかの特定」であり、「これまでの仕事の仕方を変えさせられる」という印象が強いからではないでしょうか？しかし、情報システム監査の意義は決して不足・問題点の特定ではなく、どのようにすればより良くなれるかにあり、無駄な作業の削減にあると思います。

当方も、かつては情報システム監査に対してネガティブな印象しか持っておりませんでした。本格的に情報システム監査を受けることになったのは、米国SOX法に基づいたIT内部統制監査への対応の時でした。本監査まで時間が限られている中、とても苦労したことを今でも思い出します。監査を受けている間は、当時の手続きの問題点が次々と浮かび上がり、監査人の方と時間をかけてどのような視点で業務を改善していけばよいのか協議しました。この当時は、システム監査基準などのフレームワークも全く不勉強な状況でしたので、本当に大変でしたが、社内の規則や業務手順を整備し、情報システム部門内の手続きを全て変えていきました。監査人の方と色々協議し、どのような視点で業務を改善していけばよいのか、この時実施していったことが根本的な業務の見直しに繋がり、当方の中でベストプラクティスのようなものが出来上がっていった気がします。また手続きの改善によって無駄な作業が削減され、情報システム開発における品質も向上したと思います。情報システム監査の意義というものに気づかされたのはまさにこの経験によってだと考えています。

前職でIT部門を率いる立場になった際に上記での情報システム監査を通じて得た経験・知識がとても役に立ちました。IT部門の一からの立ち上げだったため、情報システム部門としての手続きを作成する必要がありました。以前で苦労した経験により、社内の規則や手順書の整備を滞りなく行うことができました。同年に日本版SOX法のIT内部統制監査を受けましたが、特に大きな指摘事項はありませんでした。この成功はかつて苦労していなければ絶対に成しえなかったことであり、監査人の方からの指摘があってこそだと思います。

情報システム部門の皆さんに申しあげたいことは、情報システム監査はできるだけ数多く経験していただきたいということです。部門内の手続き等は定期的に見直さないといけないと思いますが、通常業務に追われ中々その機会を見いだせないということも多いかと思います。情報システム監査はある意味そのような機会を「良い意味で」強制的に与えてくれる機会であり、改善のきっかけを与えてくれるタイミングです。何かを改善するというのは部門全体の経験や知識を向上する良い機会となります。このような経験や知識の向上は、情報システム監査を実施するという立場になった時も有効です。昨今、システムベンダーやクラウドサービスなど外部のリソースを使ってシステム開発や運用をすることが当たり前となってきています。そのような外部サービスを利用するにあたり、そのベンダーやサービスの品質に問題ないことを判断するためには、事前評価や情報システム監査が必要になってきます。苦労して情報システム監査を受けてきた情報システム部門にとっては、監査をするための規則・手続きの整備、どのような視点で監査をすべきなのかという視点が蓄積されており、監査の質が自然と高いものになると思います。情報システム監査を前向きに捉え、より良い情報システム部門を目指してください！　　（あきぼう）

（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＞

2014.10

めだか　【　情報システム部門のためのシステム監査　】

わが国のシステム監査というと、その基準は、平成16年10月8日に情報セキュリティ監査制度との整合性の観点を踏まえて経済産業省から公表された、新「システム監査基準」と「システム管理基準」である。その後、内部統制報告書提出制度の開始、つまり金融証券取引法の成立を契機に、財務報告の信頼性という観点で追補版が公表されている。また当協会ではオフショア開発に係るシステム管理基準や個人情報を取り扱う情報システムへのシステム管理基準を策定し発表している。各企業は、システム監査に当たってこれらの基準を参考にそれぞれのシステム管理基準を設けて情報システム部門のためのシステム監査が運用されている。

奈良県いかるがの里にある法隆寺は、世界最古の木造建築物であるとともにわが国の国宝が多数保存されていることで有名である。法隆寺を訪問し国宝を拝観するとき7世紀のわが国を彷彿とさせられるのは私だけではないと思う。金堂の釈迦三尊や夢殿の久世観音は、聖徳太子のお姿を映した仏像であるといわれている。法隆寺は、わが国に仏教を普及させたシステムセンターと言える。法隆寺を建造した棟梁、そして、わが国のような地震、かみなり、火事、台風そして戦争という災害の多い国で、7世紀から21世紀まで法隆寺を守り続けてきた先人に大いに敬意をささげたい。法隆寺五重塔は、東京スカイツリーと同じ耐震設計になっているというから驚きである。法隆寺の開発コンセプト、設計、建造と保守の過程は、あたかも情報システムにシステム監査基準やシステム管理基準があるようである。あるいは、むしろ勉強しなければならないものである。

情報システムは、人間が集まって構築や保守を行うものであるから、その人間集団の強みや弱みが現われると思う。仏教によると、縁起の法というものがあり、「原因」があってその結果がストレートに結果になるわけではなく、「縁」という生育条件のようなものの働きがあって、その結果、「結果」になると言う。畑に野菜の種を蒔くと、それから、水をやり、苗が出たら風から守ってやる、大きくなるよう肥料もやって、といった世話をすると良い野菜ができるようなものである。また「結果」を楽しむのが「報」であるといわれている。「報」とは情報システムがカットオーバーしたときの打上げの際の楽しさのようなものと思う。保守は地味だが情報システムの維持に重要であり、ときには保守が順調であることを楽しむことが大切であると思う。

情報システム部門のため、情報システムの構築や保守が利用目的に有効で、かつ情報システムに障害が起きないよう、法令等への準拠に齟齬が生じないよう情報システムを世話していくことが大切であると思う。またシステム監査が円滑に行われるようシステム監査を制度化あるいは法制化することを粘り強く求めていきたいと思う。

（空心菜）

（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＞

2014.10

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）

9月の月例研究会は、講師に東京海上日動リスクコンサルティング株式会社上席主席研究員　指田朝久氏にテーマを「首都直下地震の被害想定の警告　～　情報システムのバックアップは本当に機能するか　～」として講演頂きました。講演は、“2013年末に公表された政府の首都直下地震の被害想定は、東日本大震災を踏まえて前回2005年に公表された想定を大きく変えている。しかしながらその被害想定の内容はあまり認識されていない。本セミナーでは今回公表された被害想定を解説し、企業はどのように対応すればよいかについて提言する。”という内容でした。首都直下地震の被害に過酷事象も想定外とはしないため、初めて聴くものにはショッキングな被害の想定で、情報システム部門のためのシステム監査において情報システムのバックアップは機能するかをあらためて見直す必要があることを認識させられました。詳しくは月例研究会報告をお読み頂きたいと思います。

一般社団法人日本内部監査協会　第48回内部監査推進全国大会が、9月25日、26日に東京都内で開催され、私と力　副会長が参加しました。大会に参加し情報システム部門のためのシステム監査という観点で当協会が担うべき役割について考えました。〈大会テーマ〉は、「組織体の揺るぎなき成長に内部監査の貢献を　～　Progress Through Sharing　～」です。

〈大会テーマ〉は、

“国際的な金融危機から7年が経過しました。この間、世界経済では、先進国のけん引力が弱まり、新興国についても低成長が懸念されるなど、その先行きは依然不透明なままです。

こうした中、日本経済は、緩やかな回復基調にあるといわれているものの、市場競争の激化や、急速に進展したグローバル化などに起因して、組織体を取り巻く経営環境は厳しい状況が続いております。環境の変化に対して常に感度を高め、柔軟な経営を展開し、苛烈な競争を乗り越えて発展、成長を目指すことが、従来にもましてあらゆる組織体に求められております。

さらに、一連の企業不正を契機として、あらためてコーポレート・ガバナンスの重要性が見直されています。会社法の改正に伴い新たな機関設計の枠組みが加わったことで、日本のコーポレート・ガバナンスの一層の充実が期待されており、これを効果的に機能させ、市場の信頼に応えることもまた、組織体に課せられた使命であります。

今こそ、組織体の経営目標の効果的な達成に役立つ内部監査が、組織体の健全かつ効率的な経営、ひいてはその揺るぎない成長に貢献することが求められております。“ と解説されています。

当協会は、ITガバナンスの国際規格 ISO/IEC 38500（Corporate governance of information technology）のJIS規格化の進展と並行して、ITガバナンスのPDCAのうち、Checkの役割を担うシステム監査の制度化・法制化を図っていくよう活動を始めています。上記のコーポレート・ガバナンスの一層の充実を推進する日本内部監査協会や、日本におけるITガバナンス普及活動の中心である日本ITガバナンス協会などに協力し、システム監査の普及促進を事業目的とする当協会の存在を世に知らしめ、また会員等の情報システム部門のためのシステム監査への支援活動を強化していきます。

以上

＜目次＞

2014.10

投稿　【　システム監査とＳＡＡＪの曲り角　】

会員番号　555　松枝憲司

日本にシステム監査基準が制定されたのが1985年、任意団体としてのSAAJ（以下協会）設立が1987年で、既に四半世紀以上経過している。この間、欲しい情報を世界中から入手できるツール（システム）を誰もが持つことができるようになり、内部統制が現代人の基礎知識となり、情報セキュリティに関する事件や事故が日常茶飯事となっているこの時代に「システム監査」が全く元気がない。私の周りでは、ビジネスとしてのシステム監査の話をほとんど聞かなくなっている。マスコミに取り上げられることもないし、システム監査という用語自身を目にしなくなっている。それに呼応するようにシステム監査技術者試験の受験生も減少の一途である。

協会は設立以来「システム監査の普及」を目的としてきたが、一体どうしたことなのであろうか。

（1）システム監査の曲り角

設立当初の経緯等より協会が最も拠り所としているものが経済産業省の「システム監査基準」と「システム管理基準」である。システム監査基準解説書では「システム監査は、企画・開発・運用・保守という情報システムのライフサイクルに従って、特に情報システム構築・運用の全体最適化を目的とした監査」と位置付けている。またシステム監査は、信頼性、有効性や経済性など広範囲な視点で総合的に監査するとしている。

一方でシステム監査基準制定後、急速な IT 社会の進展に伴い、社会的、経済的に重要な事項について、各種制度等が設定されるようになり、広く浸透してきた。主なものを以下にあげる。

制定	制度・基準	概要　（ ）内は当該制度の適用数
1985	システム監査基準	1996 年改訂
1998	Pマーク	プライバシーマーク認定制度（13,760 社）
1999	J ISQ15001	個人情報保護マネジメントシステム
2003	情報セキュリティ管理基準	情報セキュリティ監査基準とセット
2004	システム管理基準	コントロールを適切に整備・運用するための実践規範。 システム監査基準とセット
2005	ISMS　ISO/IEC27001	情報セキュリティマネジメントシステム　（4,547 組織）
2005	IT サービス ISO/IEC20000	IT サービスマネジメントシステム　（193 組織）
2005	個人情報保護法（施行）	個人情報を取り扱う事業者の遵守事項等
2006	金融商品取引法の内部統制報告制度	J-SOX。2008 年度以降の上場会社に適用（3700 社程度）
2008	IT ガバナンス ISO/IEC38500	2014 年に JIS 化
2012	事業継続　ISO22301	事業継続マネジメントシステム　（74 組織）

これらの多くは、制度のためのマネジメントシステムの構築と運用を要求しており、そのマネジメントシステムの改善の為に定期的な「監査」を求めている。しかしながらそれらの監査は、各マネジメントシステムのための監査であって「システム監査」とは呼んでいない。30 年前のシステム監査基準の観点からすると、これらの後発の制度に関する監査もシステム監査の守備範囲である。しかしながらテーマに特化した制度における監査では、システム監査的視点を含むが、その他の各制度から要求される事項がメインであるため、システム監査がクローズアップされることはない。

企業からすれば、制度化されているものは優先的に対応せねばならず、制度に関連した監査をとおして、システムに関する監査も実施済みという認識ではないかと想像される。

ここで「システム監査」を「システム管理基準に基づく監査」と定義すると、個別制度における監査でカバーしきれない項目（視点）は何があるであろうか。以前システム監査と情報セキュリティ監査の相違点が議論された際、「システム監査」特有の視点としてシステムの有効性（業務目的達成への貢献度や投資対効果等含めたもの）があげられていた。しかし有効性に関する具体的な監査項目について、管理基準に明記されているわけではない。

このような中で、ITガバナンスの国際基準である「ISO/IEC38500：2008」が今年 JIS 化される予定である。ISO38500 は 6 つの原則から構成されているが、その中には、経営者の責任や、ビジネス戦略と IT 戦略の整合性、IT 調達における透明性等を含んでおり、システム管理基準の情報化戦略に関する項目をカバーしている。またITのパフォーマンスの視点では、ビジネスの要求を満足させるITサービスのレベルを重視しており、システムの有効性に係る項目に該当していると個人的に思っている。それに加えて ISO38500 で定義している IT ガバナンスに関する監査のガイドライン（ISO/IEC38503）の案について、日本（特に協会）主体で検討しているところである。仮に本ガイドラインが ISO 化（TR）された場合、システム管理基準の存在が決定的に希薄になってしまうのではないかと懸念している。

以上のようなことから、「今のシステム管理基準は、一部の内部監査での活用程度しか存在意義がなくなっており、それに伴いシステム管理基準に基づく監査のニーズが生まれなくなった」のであろうと推論している。

（2）SAAJの曲り角

全くの個人的見解であるが、上記「システム管理基準に基づく監査」の衰退が、協会勢力の衰退に直結していると考えている。このような状況において協会が存続し続けていくには、「システム監査」を再定義し、協会の活動の目的等を見直しすることが必須であろうと考えている。以下は私見である。

①（協会にとっての）システム監査の再定義

協会活動の目的であり根幹をなしている「システム監査」は、今のままでは衰退するばかりである。

「システム」が「IT」に置き換わっている時代に、協会としてどのように定義して、世にその必要性を問い直すのかが重要である。

②システム管理基準の改訂

上記①に関連して「システム管理基準」をどのように位置づけるのか、既存の各制度との関連性も明確にしたうえで改訂案を検討する。その際にはシステム監査学会との連携を検討する。

③ITガバナンス国際基準(JIS38500)の国内普及への主導的取組み

個人情報保護に代表されるように個別に制度化されたものは、情報やITの信頼性や安全性をテーマにしたものが大半である。その中で今年度JIS化される予定のJIS38500は、ビジネスとITの有効性等を取り扱っており、経営に役立つITという視点は経営者にとってもアピールできる可能性がある。そのため国内への普及について、主導的立場でITガバナンスの構築に関して取組んでいくことで、結果として会員のビジネスの拡大に貢献する可能性がある。またJIS38500が普及すれば、現在検討中である「ITガバナンスに関する監査のガイドライン」の制定後には、ITガバナンスの監査という視点でのビジネスにも繋がる可能性が高まることを期待する。

以上

＜目次＞

2014.10

第１９４回　月例研究会　（２０１４年８月２０日開催）

会員番号 0056　藤野明夫　（情報セキュリティ監査研究会）

【講演テーマ】「個人情報影響評価 PIA の考え方と実施手順　ープライバシーバイデザインとしての PIAー」

講師:一般財団法人日本情報経済社会推進協会(JIPDEC)

電子情報利活用研究部 部長 坂下哲也氏

日時: 2014 年 8 月 20 日(水曜日)18:30～20:30

場所:機械振興会館　地下 2 階ホール

【講演骨子】

「行政手続における特定の個人を識別するための番号の利用等に関する法律」(平成 25 年度法律第 27 号)(以下、「社会保障と税番号法」又は「番号法」)に基づき、平成 28 年1月より私たちに「番号(以下、マイナンバー)」が付与される。現在、国、行政機関、地方公共団体等では、その導入に向け、“特定個人情報ファイルを保有する前に安全な取扱いがなされることを評価し、宣言する「特定個人情報保護評価」(以下、PIA)”を実施している。JIPDECでは、平成 25 年度に複数の地方公共団体の協力の下で「特定個人情報保護評価」を試行し、実効性が高い手順を取りまとめ、平成 26 年度から評価機関の支援を行っている。本会では、PIA実施における対策等を解説するとともに、政府戦略に基づくマイナンバーの利用について検討されているモデル(ID連携トラストフレームワーク)等について紹介する。

【講演概要】

〔はじめに〕　言葉の定義

個人情報については、しばしば、言葉の問題で誤解が生じるので、まず言葉の定義を明確にする。

- 個人情報:生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述などにより特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することとなるものを含む)　＜個人情報保護法第2条第1項など＞
- 特定個人情報:個人番号をその内容に含む個人情報　＜番号法第2条 8 項＞
- パーソナル情報:個人と連結可能な情報の総称。この中には、位置情報、購買履歴、血圧などの生体情報なども含まれる。＜経済産業省「パーソナル情報研究会報告書」(2008 年 11 月)など＞

１．特定個人情報保護評価とは

特定個人情報保護評価とは、特定個人情報ファイルを保有しようとする又は保有する国の行政機関や地方公共団体等が、 個人のプライバシー等の権利利益に与える影響を予測した上で特定個人情報の漏えいその他の事態を発生させるリスクを分析し、 そのようなリスクを軽減するための適切な措置を講ずることを宣言するものである。番号法第 27 条に基づき、国、地方公共団体等に義務付けられるものである。

番号法第27条には、「行政機関の長等は、特定個人情報ファイル(中略)を保有しようとするときは、当該特定個人情報ファイルを保有する前に、特定個人情報保護委員会規則で定めるところにより、次に掲げる事項を評価した結果を記載した書面(「評価書」という。)を公示し、広く国民の意見を求めるものとする。当該特定個人情報ファイルについて、特定個人情報保護委員会規則で定める重要な変更を加えようとするときも、同様とする。」とある。この条文を根拠に、2014 年 4 月 20 日に特定個人情報保護委員会が公表した「特定個人情報保護評価指針」(資料1)等に基づいて実施される。

その評価すべき対象は、「特定個人情報ファイルを取り扱う事務」であり、「事務」単位で評価する。ちなみに、「特定個人情報ファイル」とは、個人番号を含む個人情報ファイル(保護法2条2項の個人情報データベース)である。業務の

中の特定個人情報がデータベースのシステムのファイルに入ると特定個人情報ファイルになる。評価の時期は、原則としてシステムの要件定義段階までに実施しなければならない。

その方法は、しきい値によって分かれる。対象となる事務の個人情報ファイルに存在する人数が、千人未満では評価不要である。千人以上の場合、特定個人情報保護評価を行う。

特定個人情報保護評価の必要性が低いものは、基礎項目評価書を公開する。基礎項目評価は、対象人数が千人以上 1 万人未満と1万人以上10万人未満で一定の場合（特定個人情報を取り扱う職員・ 外部委託先の人数は 500 人以上でないこと、または、過去一年以内に、漏えい等の重大事故を発生させてないこと）は、基礎項目評価のみを実施、公開すればよい。基礎項目評価書の内容は、個人のプライバシーの保護の宣言等である。

必要性が高いものは、重点項目評価を実施し、自治体の裁量で意見を聴取・委員会で審議し、公開する。重点項目評価は、対象となる事務の個人情報ファイルに存在する人数が、1万人以上10万人未満で一定の場合（特定個人情報を取り扱う職員・ 外部委託先の人数は 500 人以上であること、または、過去一年以内に、漏えい等の重大事故を発生させていること）と10万人以上 30 万人未満で一定の場合（特定個人情報を取り扱う職員・ 外部委託先の人数は 500 人以上でないこと、または、過去一年以内に、漏えい等の重大事故を発生させてないこと）に実施する。重点項目評価書の記載内容は、基礎情報、業務システムの概要、特定個人情報ファイルの取扱工程（フロー）図等である。

特に必要性が高いものは、全項目評価を実施し、評価書を公開し、委員会の審査を経て、公開する。全項目評価は、10万人以上 30 万人未満で、過去一年以内に漏えい等の重大事故を発生させた場合、または、特定個人情報を取り扱う職員・ 外部委託先の人数は 500 人以上である場合と、30 万人以上の場合に実施する。全項目評価は、以下に述べるように負荷がかかるものである。評価の結果を市民に全て開示し市民の意見を聴取し、これを反映し、第三者委員会に諮って、同委員会にて審査承認後、政府委員会に報告する（PDF でアップロード）。ただし、政府は直ちにこれを見ることはしない。事故が起きたときにはじめて、この報告を参照する。重点項目評価書の記載内容は、基礎情報、事務の内容、特定個人情報ファイルの概要（特定個人情報ファイル記録項目を含む）、特定個人情報ファイルの取扱いプロセスにおけるリスク対策、その他のリスク対策、開示請求、問合せ等である。

２．特定個人情報保護評価と PIA

特定個人情報保護評価の説明に関する政府の資料では、「米・加・新（NZ）・英等の諸国で行われているプライバシー影響評価（Privacy Impact Assessment：PIA）に相当するもの」と説明されている。特定個人情報保護評価のもとなった PIA について説明する。

そもそも、PIA はカナダで始まった。1990 年代に、カナダのオンタリオ州情報・プライバシー・コミッショナーのアン・カブキアン博士が提唱し、実施されている。米国も 2002 年の電子政府法で PIA の実施が義務付けられている。これらの国では、『PIA は国や行政機関において、新しい技術・情報システムで企画・提案されたプログラムやポリシーが、基本的なプライバシー要件に適合しているかどうかの判断を支援するプロセス』と定義されている。

PIA は、プライバシー・フレームワーク、プライバシー・アセスメント及びプライバシー・アーキテクチャの三つの構成要素からなる。プライバシー・フレームワークは、法制度、ガイドライン、規制等を参照して作成されるプライバシー保護要求水準と、その測定基準から構成される。プライバシー・アセスメントは、設計仕様の評価（システムを作る前、仕様設計の段階で評価）、及び、対象システムを使用する業務における個人情報の収集・利用・管理・廃棄についての影響分析と対策（対象システムへのポリシー、教育、運用の設計がなされているか等及び収集・利用・管理・廃棄についてPDCA サイクルがきちんとまわるかどうかチェック）の評価から構成される。プライバシー・アーキテクチャは、影響分析結果を基に、要求水準を満たすための措置（ルール、教育、技術など）である。

ただし、カナダ、米国等では、評価の対象が「システム単位」であるのに対して、日本の特定個人情報保護評価は、「事務単位」である。

３．特定個人情報保護評価方法と各種の標準

一方で、その評価を実施する際には、「物差し」が必要である。海外で実施されている PIA も、国際標準等を用いて、その評価が適切か否かを確認している。

JIPDECが実施した試行において、参照した標準は、JIS Q 15001（個人情報保護マネジメントシステム－要求事項）、ISO/IEC 27000 シリーズ（情報セキュリティマネジメントシステム：ISMS）及び ISO15408（Common Criteria：CC）である。

JIS Q 15001 は、プライバシーマークの基となっている規格で、個人情報の取扱いに関するリスクを適正に管理するプロセス（個人情報保護マネジメントシステム：PMS）を構築するための要求事項である。特定個人情報は、個人情報であり、その適切な保護を目指す規格であることから、この規格が最も適応するのではないかと考えた。また、ISO/IEC 27000 シリーズは、情報セキュリティリスク（プライバシー、機密、情報技術など）を評価する国際標準である。プライバシーも守るべき対象ではあるが、JIS Q 15001 のように個人情報保護に特化したものではなく、情報セキュリティ一般の標準である。番号法の第 12 条において安全管理措置義務が定められていることから、ISO/IEC 27000 シリーズを適用する選択肢もあるのではないかと思われる。番号法 27 条1項の評価事項と各標準を表1の様に対応づけることができる。

表１　評価事項と標準の対応

27 条 1 項の号	内容	対応する標準
1	特定個人情報ファイルを取り扱う事務に従事する者の数	JIS Q 15001 （JIS Q 15001 で均質なPIAを行うことができる）
2	特定個人情報ファイルに記録されることとなる特定個人情報の量	
3	行政機関の長等における過去の個人情報ファイルの取扱いの状況	
4	特定個人情報ファイルを取り扱う事務の概要	
5	特定個人情報ファイルを取り扱うために使用する電子情報処理組織の仕組み及び電子計算機処理等（電子計算機処理（電子計算機を使用して行われる情報の入力、蓄積、編集、加工、修正、更新、検索、消去、出力又はこれらに類する処理をいう。）その他これに伴う政令で定める措置をいう。）の方式	ISO/IEC 27000 ｼﾘｰｽﾞ ISO/IEC 15408 JIS Q 15001
6	特定個人情報ファイルに記録された特定個人情報を保護するための措置	
7	前各号に掲げるもののほか、特定個人情報保護委員会規則で定める事項	－

また、評価のプロセスで参照する業務面及びシステム面の情報と各種規格等との関係を表2に示す。

表２　評価プロセスと参照規格の関係

評価の観点	評価のプロセスで参照する情報		参照する規格等
	業務面（人に関するもの）	システム面	
必要最低限の個人情報の取得になっているか。	①当該業務に関連する法令や条例 ②国民・住民から取得する特定個人情報の項目一覧（申請書等）など	①特定個人情報ファイルの項目一覧 ②システム・セキュリティのルールなど	①法令、政省令 ②ガイドライン（地方公共団体における番号制度の導入ガイドラインなど） ③JIS Q 15001:2006 個人情報保護マネジメントシステム－要求事項
必要な運用手順となっているか。	①業務手順書 ②委託先・外注先の選定基準（番号法 11 条は、委託・再委託に厳しい） ③職員の教育カリキュラムや手順など	①文書管理システム等の運用手順 ②データ提供・受理時のセキュリティ規則 ③バックアップ、消去等の手順など	①ISO 27000 ファミリー ②JIS Q 15001:2006 個人情報保護マネジメントシステム－要求事項
適切なセキュリティ対策が施されるか。	①入力手順などシステム利用マニュアル ②受理書類等の保管手順 ③管理手順など	①宛名システム等との連携手順(東京都は連携宛名システムの下に各自治体がぶら下がっている) ②アクセス制御等のセキュリティ規則など	①地方公共団体における情報セキュリティポリシーに関するガイドライン(平成 22 年 11 月版) ②ISO 27000 ファミリー ③JIS Q 15001:2006 個人情報保護マネジメントシステム－要求事項 ④CC（Common Criteria：ISO/IEC15408）

４．試行の実施

上述の提案に基づき、JIPDEC で、東京都、三鷹市、千葉市等で試行を実施した。試行した業務は、住民基本台帳、国民健康保険など11業務である。期間は、昨年９月から今年3月までで、この推進にあたっては、プライバシーマーク審査員の方にも御協力を頂いた。

試行は、①地方公共団体が、対象業務（システム）を選定、②関係書類（要件定義書（もしくは設計書）、データフロー、業務手順書、規程類）を準備、③JIPDEC において全項目評価書を作成、④第三者点検のための確認を想定し、プライバシーマーク審査員による内容確認を実施、という手順である。

東京都は要件定義書、データフローがあったが、それ以外の自治体では要件定義書、データフロー等が揃っていることは少なかった。理由として、ベンダーのパッケージを使用していることが上げられる。そのため、パッケージの使用説明書から要件定義書、データフローを起こす作業を行わなければならなかった。また、全項目評価では、評価書を作成し、市民に公開し、市民の意見を反映した上で、審査会等の第三者の点検を以て、国に提出する。そこで、第三者点検を想定し、JIPDEC のプライバシーマーク審査員によるチェックを実施した。

ファイル、項目、その関連が分る資料から、特定個人情報を取り扱うシステムを特定・整理する。次にシステム分析書を作成する。その例を下記に示す（図１）。ここでは、パッケージを使用しているため、パッケージのマニュアルしかなく、ヒヤリングで多分こういうデータが行くのだろうと想定して、このデータフロー図を作成した（図１）。この例では、母親識別番号、父親識別番号は、社会保障と税番号を使う部分になるものと想定される。

また、事務毎に想定されるリスクをすべて洗い出してリスク分析を行った。

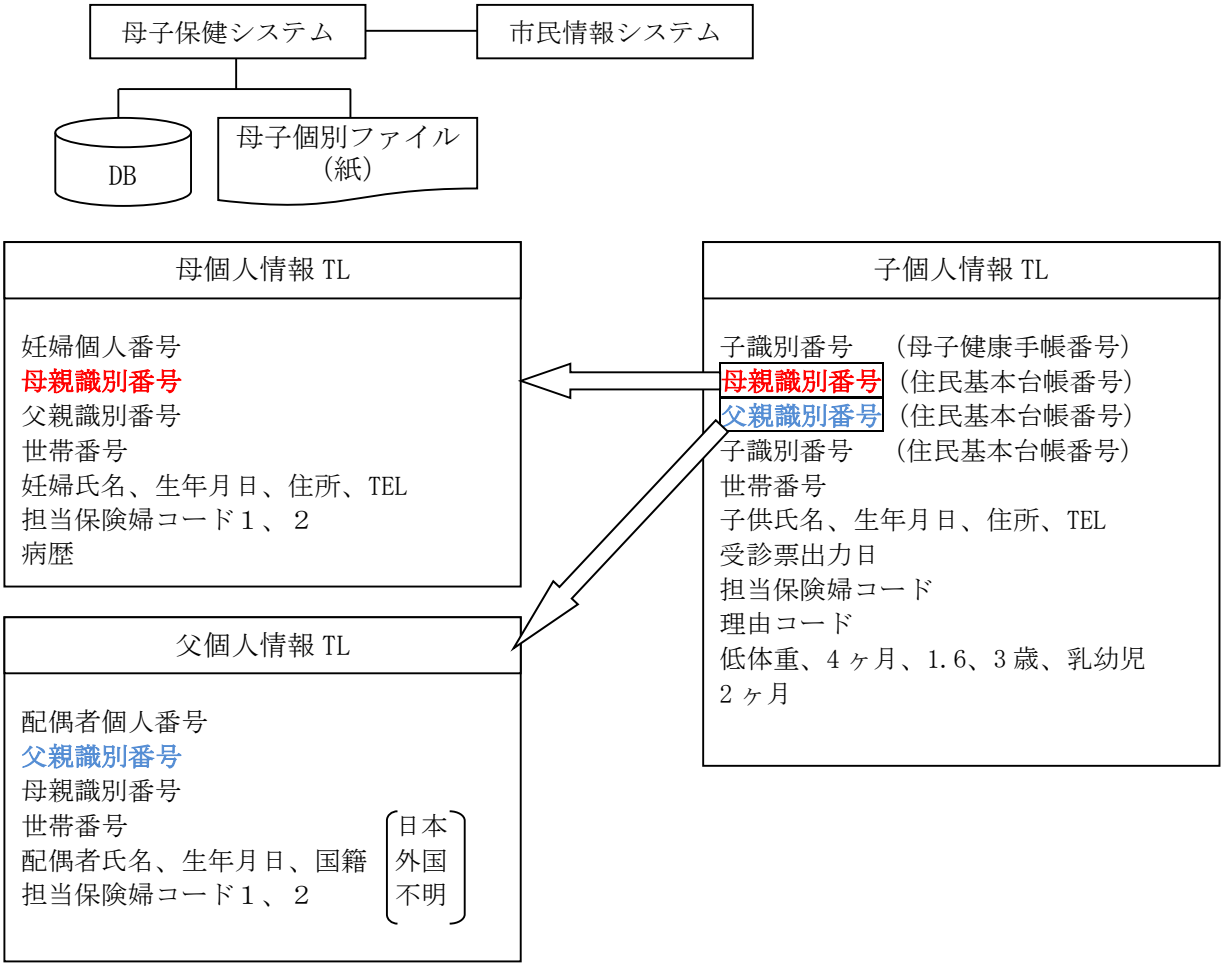


図１ データフロー図

５．事前調査

事前調査においても、業務面、システム面の両面から分析を行い、実際に評価の対象となる業務を特定することが必要である。よって、この作業には、業務部門・情報システム部門の両部門から人材が参加し進めることが肝要である。

事前調査の事例を一つだけ紹介する。この例は医療費支給に関する事務を対象としている。まず、事務に関連する法規をすべて書き出す。また、手続で用いられる書類をすべて書き出して、情報の真正性、番号法による変更点を書き出し、下表のように整理する（表 3）。なお、システムがなければ、PIA 実施の対象にならない。

表 3　医療費の支給申請に関する事前調査

医療費の支給申請（医療機関で 10 割の医療費を支払った場合等）			
関連法規	内容		
高確法　第 77 条	療養費支給要件		
高確法施行規則　第 47 条	療養費支給申請における申請書記載事項		
東京広域条例　第 21 条1項	申請書様式制定（別記第 26 条様式）		
東京広域条例　第 21 条 2 項	通知書様式制定（別記第 23・23 の2・24 号様式）		
申請に要する書類・情報	現行		番号法による変更点
	記載情報	情報の真正性	
後期高齢者医療療養費支給申請書（別記第 26 号様式）	被保険者番号	保険証	不明
	被保険者氏名	保険証	
	被保険者生年月日	保険証	
	入院外来区分	（国保連）	
・・・・・・	・・・・・・	・・・・・	・・・・・
システムの有無	無		
処理の流れ			
現行（マニュアル名）		番号法による変更点	
申請方法：窓口又は郵送（業務手順書）			
申請書・レセプト・領収証を受理し、記入事項を確認する。（同上）		住基システム等により個人番号の真正性を確認する。	
申請書のみコピーし、受付の記録を保管する。（同上）			
毎月 10 日、申請書・意見書・領収書の原本を国保連へ送付（同上）			

６．特定個人情報保護評価におけるリスク対策の考え方

特定個人情報保護評価で重視される「リスク対策」については、プライバシーマークの規格である JIS Q 15001 にある「特定した個人情報について，個人情報の取扱いの各局面におけるリスク（個人情報の漏えい，滅失又はき損，関連する法令，国が定める指針その他の規範に対する違反，想定される経済的な不利益及び社会的な信用の失墜，本人への影響などのおそれ）を認識し，分析し，必要な対策を講じる手順を確立し，かつ，維持しなければならない」という考え方で進めることを推奨している。一方で、多くの自治体ではリスク分析を実施した経験を有しないため、各局面におけるリスク認識、分析、対策立案、残存リスク把握を例示し、自治体職員と共に、分析を行った（表 4）。

表 4　各局面におけるリスク認識、分析、対策立案、残存リスクの把握の例

局面	リスク	対策	残存するリスク
収集	漏えい、郵送時の盗難、破壊（滅失・き損等）、改ざん、入力ミス、同意の取り忘れ等	窓口マニュアル（担当の規定など）、入力チェック手順など	受取ミスなど
保管	紛失、破壊、盗難、改ざん、不正アクセス、ウィルス感染、ファイル交換ソフト、規定違反等	保管手順、管理台帳の整備（規定）バックアップ手順	外部からの侵入など
利用	不正出力、内部からの不正アクセス、誤送信、目的外利用、操作ミス、ID の使い回し	アクセス制御、セキュリティ対策、システムマニュアル	他人の ID 利用など
委託提供	輸送時の盗難、破壊、契約上の問題、目的外利用、不正入手	委託先の選定基準（セキュリティ評価等）	委託先のリスク
廃棄	未処理による放置、再利用、不正持ち出し	・廃棄マニュアル ・ハードウェアの破壊等の手順	記録ミスなど

7．JIPDEC で取り組んでいること

特定個人情報保護の全体について説明する研修を実施している。1回あたり、3時間程度の講義を行い、評価書を作成する方法や、点検の観点を学ぶものである。出張研修も可能である。

また、作成された評価書（全項目評価・重点項目評価が対象）について第三者点検前の確認を行っている。具体的には、自治体によって作成された評価書、関連する規程を預かり、プライバシーマーク審査員が「適合性・妥当性」の確認を行い、その評価書に対して、「確認書」を発行するものである。審査会に諮る前に「確認書」を受けとり、審査会を効率よく通すという効果がある。なお、政府の指針による適合性とは、提出された特定個人情報保護評価の実施が、特定個人情報保護評価指針に定める実施手続等に適合して行われていることをいい、妥当性とは、特定個人情報保護評価書に記載されている内容が、この指針に定める特定個人情報保護評価の目的等（本人のプライバシー等権利利益の保護）に照らして妥当と認められることをいう。

JIPDEC としては、地方公共団体に対して、しきい値としては基礎項目評価書でとどまるものであっても、重点項目評価、又は全項目評価を実施しておくことを推奨している。もともと、番号法では、提出された評価書を特定個人情報保護委員会が審査することを規定しているが、実際の運用は、評価書の第三者点検は地方公共団体で実施し、特定個人情報保護委員会には報告するだけでよい（事故等が発生するまで、特定個人情報保護委員会では、評価書の内容を見ない）ように変更された。基礎項目評価書だけを報告するのでは、事故等があった場合に、どこまで対応していたのかを説明することが難しくなると考えている。第三者点検を行わずに済む場合であっても、特定の業務のみ、評価書だけは作成し、提出しておいた方が良いのではないか。可能であれば、全項目評価し、報告アップロードしておくことを推奨しているする。

地方公共団体の取り組み状況を簡単に紹介する。宮城県は県が主導的に推進し、ガイドライン等を作成し市町村を啓発している。尼崎市は市町村で最初に特定個人情報保護評価を調達した。杉並区、目黒区、八王子市などはガイドラインを作成し庁内で推進している。秋田市、青森市、門真市なども積極的に取り組んでいる。

8．民間におけるマイナンバーの利用と ID 連携トラストフレームワーク

次に、民間におけるマイナンバーの利用を考えてみたい。図 2 に就職・転職における利用の例を示す。現在、就職や転職を行う際の、卒業証明書や、資格証明書は紙であることが多い。求職者は、これらを揃えるために手間がかかっており、電子化することで、効率よく活動することができるのではないかと言うニーズが顕在化している。この場合、各種証明書の電子化はもとより、オンラインで本人確認を行う仕組みも必要になってくる。

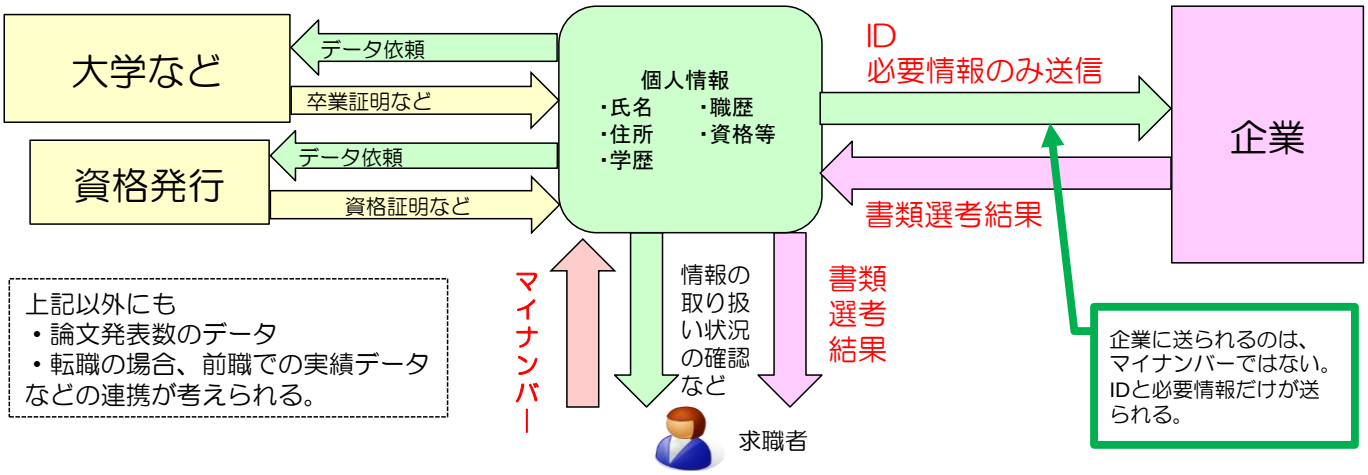


図 2 就職・転職における利用

この例では、中立的な機関が仲立ちをして、マイナンバーによる確実な本人認証（マイ・ポータルとの連携など）を担保しながら、採用側の企業は、マイナンバーそのものの提供を受けることなく、求職者の属性情報を取得することがで

きる仕組みを目指している。マイナンバーを利用する理由は、全ての国民が保有するためである。(運転免許証や、住基カードは、全ての国民が有しているものではなく、サービス享受の機会を平等に与えることができない。)

次に、健康保険(医療)サービスの手続きの簡素化の例を考えてみる(図 3)。

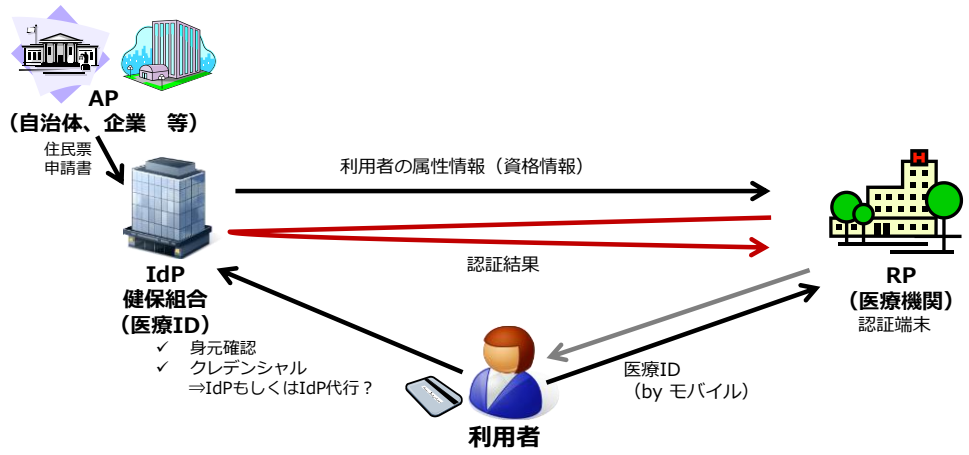
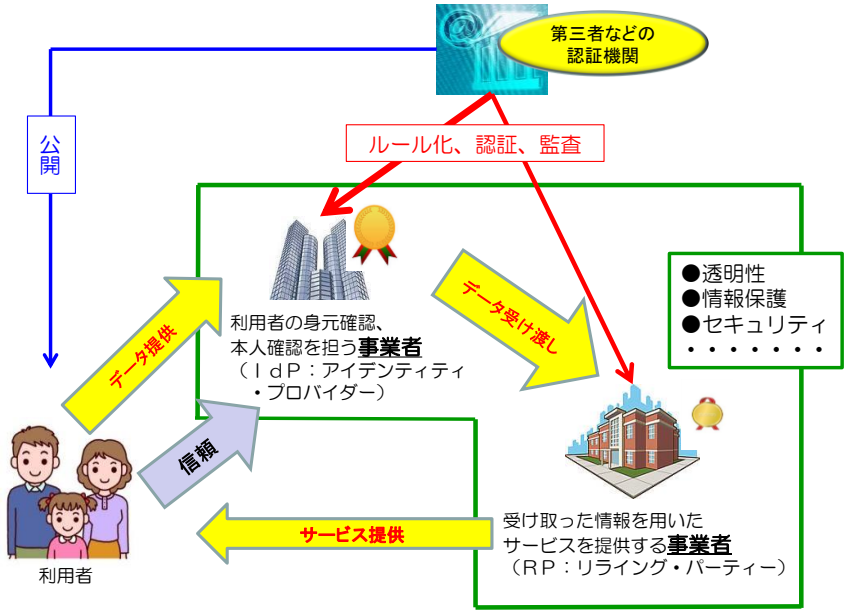


図 3 健康保険（医療）サービスの手続きの例

健康保険組合が ID を発行し、様々な医療サービス提供の際の手続きを簡素化したいとするニーズは顕在化している。一方で、医療情報という機微な情報を扱うために、確実な本人認証や、セキュリティの高いデータ運用の仕組みが必要になる。前者の場合、マイナンバーを用いることが考えられる。ここでは、マイナンバーは、健保組合と自治体等が知るのみで、医療機関にはマイナンバーは通知されない。本人認証を行う健保組合は、医療機関からの問い合わせに○×のみを返す。いわばトラストアンカーとしてマイナンバーが使われる。これにより、保険証が手元になくても被保険者であることを証明でき、保険証の失効確認が出来、医療費未収が防げる等の効果がある。

図 3 において示された、サービス提供に不要な個人情報を、サービス提供者たる医療機関に渡すことなく、かつ、確実に本人であることを保証しつつ、必要な利用者の属性情報のみを提供するというフレームワークが、「ID 連携トラストフレームワーク」である(図 4)。前述のような、顕在化しているニーズを具体化するために、政府の「世界最先端 IT 国家創造宣言」においても、その推進が明記され、取り組まれている。



この他に、利用者の属性情報を提供する役割を担う**事業者**がある。
これを、
ＡＰ：アトリビュート
・プロバイダー
と称する。
図 3 では自治体がこれに当たる。

図 4　ID 連携トラストフレームワークの概念

利用者の身元確認、本人確認を担う事業者をアイデンティティ・プロバイダー(IdP)という。アイデンティティ・プロバイ

ダーは、本人確認を主たる機能とし、どこへどのようなパーソナルデータが渡されているかを利用者に可視化するといったことも行う。また、IdP から受け取った情報を用い、サービスを提供する事業者をリライング・パーティ（RP）という。このような形にすることによって、RP は必要ないパーソナルデータを取得せずに済むというメリットがある。

さらに、本人の属性情報を提供する事業者をアトリビュート・プロバイダー（AP）という。AP は、IdP が保有する利用者のパーソナルデータでは不足する（例えば、資格情報など）場合に、その不足する属性情報を提供するものを言う。IdP は利用者の同意の下に、AP から属性情報を受け取る。この全体を利用者が信頼して使えるように第三者機関が認証監査を行う。これらの全体が ID 連携トラストフレームワークである。

ID 連携トラストフレームワークの「トラスト（TRUST）」とは、インターネット上（非対面の環境）で、利用者である個人に関する（認証により当該属性の確からしさが確認された結果を含む）属性の集まりやサービスの受け渡しを行う企業群に対して、利用者が、「その相手を信用して任せられる（信用、信頼）」状態をいう。なお、IDは、識別子の意味ではなく、アイデンティティ、すなわち、属性のことである。ID 連携トラストフレームワークとは、確実にその人のものと確認された属性情報（アイデンティティ）が連携する信頼（トラスト）のフレームワークである。

９．今後の展望

「世界最先端 IT 国家創造宣言」が、平成 26 年 6 月 24 日に閣議決定された。この宣言では、「ヒト」、「モノ」、「カネ」と並んで「情報資源」を、新たな経営資源とし、その活用による経済成長を目指すことが謳われている。分野・領域を超えた情報資源（ビッグデータ、オープンデータ）の収集・蓄積・融合・解析・活用により新たな付加価値を創造していく。

IT 総合戦略本部において平成 26 年6月 24 日に「パーソナルデータの利活用に関する制度改正大綱」が決定された。これは、「本人の同意がなくてもデータの利活用を可能とする枠組みの導入」、「基本的な制度の枠組みを補完する民間の自主的な取組の活用」、「第三者機関の体制整備等による実効性ある制度執行の確保」の3つの領域で構成される。

一方で、ビッグデータは、経済成長と技術革新の強力な原動力になる反面、消費者の個人データを管理する企業と消費者の間に大きな不均衡を生む可能性を残している。

ビッグデータやオープンデータの積極的な活用は今後、急速に進展していく。そのなかで様々な問題が生じてくるが、これらに対処するために、特定個人情報保護評価、プライバシー影響評価（PIA）や ID 連携トラストフレームワークのような社会的な制度の充実や施策が図られねばならない。

〔まとめ〕

データ利用は今後も進展していくだろう。データを利用する者には、『適切なマネージメントの履行』、『情報を資産として捉えること』、『消費者（国民）へ示すこと』がますます求められていく。マイナンバー以外でも、PIA のような情報公開が進んでいく。その対応には、マネジメントにも、システムにも精通した専門家によるチェックが求められていくだろう。その観点からも、システム監査に係るニーズは高まっていくのではないか。

【質疑】

質問：独立行政法人で外部委員の方に委員会に出席の都度に謝金を支払っている。支払いが年間5万円を超える場合、支払調書を作成している。税務署に提出する源泉徴収の支払調書にマイナンバーを記載することになるか？この支払調書は独立行政法人の行政システムから交付されるが、PIA を実施しなければならないか？

回答：税務署に提出する源泉徴収の支払調書にマイナンバーを記載しなければならない。委員会を構成する委員からマイナンバーを集めなければならない。これに伴い、システム構築も必要な場合もある。ただ、これについては、PIA の対象か否かは、対象事務か否かで判断する。基本的に、事業者は、主に源泉徴収等で個人番号を使うことが想定されているので、評価実施は義務付けられていない。一方で、、生保、損保、証券会社では、被保険者

や株主からマイナンバーを取得しなければならない。最近では、このマイナンバーを適切に管理して漏れのないようにしなければならないという事から、PIA を実施しないといけないのではないかという機運が高まっている。今後は、対策として PIA を実施する事業者も増えることになるかもしれない。

質問：義務ではないが、実施した方がベターとの意味か？

回答：事業者の場合は、義務ではないが、実施しなければいけないことになるケースもあり得るのではないかということ。民間向けガイドラインのなかに出てくる可能性はあると思う。（2014 年 10 月現在、政府で民間向けガイドラインの作成作業中である。）

質問：事務単位に評価するのに、宛名システムを切り出して PIA 評価することには違和感がある。お考えをお聞かせ願いたい。

回答：PIA は事務単位で評価するのが通常である。しかし、PIA のやり方自体は自治体に任されている。作業量を考慮すると、システム単位に分けてアクセス制御等をまとめて検討した方がよいのではないかと試行の際に考え、共通システムは、それ単位に PIA を行い、事務システムの PIA でそれを参照する事を推奨するようになった。

質問：金融機関が源泉徴収により源泉所得税を控除する。マイナンバーで自分のところのシステムで名寄せのキーにしたり、他の用途に使う。これも、やはり PIA を受けなければいけないのか？
それともう一つ、PIA は JIS Q 15001 と関連性を持たせたものとなるのか？

回答：まず、後段の方から。PIA は、プライバシー・バイ・デザインという考え方でできていて、PDCA サイクルを考えると結果として JIS Q 15001 を用いると効率よく管理できるという事で参照している。また、前段の民間事業者が PIA を強いられるかだが、民間には源泉徴収等の作業で用いる場合を想定し、評価を強いていない。しかし、罰則規定があるので、事故が起きないように実施した方がいいという事業者が増えていることは事実である。

質問：JIS Q 15001 は諸外国から評価されているか？

回答：EU の会議では JIS Q 15001 を国際規格にしないかといわれている。
プライバシーマーク等の仕組みを通じて、きちんと個人情報保護を事業者のマネジメントシステムとして機能させているのは日本だけなのではないか。海外、特に EU でも、日本の仕組み自身は非常に評価されている。

質問：JIS Q 15001 は、諸外国から実効性を評価されていると考えてよろしいか？

回答：そのとおり。

質問：講義のなかで、パッケージの場合、ドキュメントがない場合があるとされているが、こういう場合は困るというご説明を伺いたい。パッケージを売っている立場として、当然に標準的ドキュメントはあるはずなのだが。

回答：試行を行った自治体の例では、パッケージの運用マニュアルがあった。運用マニュアルがあっても業務マニュアルがないと分からない。また、データベース仕様がなかった。業者からは納品したと言われたが、自治体からは出てこなかった。どこまで納品されているかわからなかった。マイナンバーの導入を通じて、そのようなドキュメント管理もきちんとできると良いのかもしれない。

質問：マイナンバーの導入は、スケジュールがタイトである。現実感として義務付けられている PIA は、どこまで実施されているとお考えか？

回答：資料 P55「平成 24 年以降、自治体の調達が活発化（JIPDEC 調べ）」で記載されている自治体（記録者注：宮城県、尼崎市、杉並区、目黒区、八王子市、秋田市、青森市、門真市）は比較的しっかり行っている。茨城県では、県庁のセミナーに全市町が集まっていただいた。このうち、10 万人を超えているのは、水戸市、つくば市、土浦市のみで、それ以外は、10 万人を超えていないと伺った。多くは基礎項目評価のみで終わる。一方で、個人情報の漏えい事故などを通じて、首長や議会からの指示で、基礎項目評価で済むところを重点項目評価に切り替える自治体も増えている。

質問：PIA そのものを行うのは、事務なりシステムなりが設計された時点でのお話しである。では、その設計されたシステムなり、事務なりが、きちんと事務ルールにより、PIA 評価がされた時点での設計通りカットオーバーされ、運用されているかどうかの、いわゆるポスト PIA 的なモニタリングに関しては、この PIA 制度のなかでは規定されていないようである。そのへんはいかがか？　事故が起こるまで実態が全然違う裏マニュアル等が作られ、それで運用が行われていたということもありえる。罰則規程でそこは担保をしているのか？

回答：PIA はそこまでを担保していない。あくまでアセスメントなので、PIA は全て市民公開するものである。努力義務で5年に1回やり直し規定がある。事務を統合し、廃止した場合は評価のやり直しがある。。一方で、PIA という作業は、特定個人情報の取り扱いプロセスを確認し、リスクを分析し、措置が必要な部分を確認するものであるので、PDCA サイクルを国や、自治体の事務に定着させるには意義があるのではないか。

【記録者の補足と所感】

たいへん内容の濃い講演であった。記録者として、まずは、特定個人情報保護評価のイメージを掴んでいただき、それから、マイナンバーと ID 連携トラストフレームワークの関係を理解していただくことに意を用いた。

今回の講演は、広範な内容を表や図を用いて説明された。結果として本記録もそれらを使わないと十分な説明ができず、紙数が多くなってしまった。また、かなりの部分を割愛せざるを得なかった。ご容赦願いたい。

JJIS Q 15001、すなわち、プライバシーマーク制度が諸外国で高く評価され、ISO 化を求められているという話に感激した。従来、プライバシー・コミッショナーがいない日本は、世界的にみると個人情報保護に関してレスペクトされていなかったが、プライバシーマーク制度のおかげで、やっと世界が認めるようになったということであろう。

【参考情報】

〔参考資料〕

資料 1：特定個人情報保護評価指針　　http://www.cao.go.jp/bangouseido/ppc/pia/pdf/shishin.pdf

〔ウェブサイト〕

・社会保障と税番号制度（内閣官房）　　http://www.cas.go.jp/jp/seisaku/bangoseido/

・ID 連携トラストフレームワーク　　http://www.meti.go.jp/policy/it_policy/id_renkei/

〔文献〕

・瀬戸洋一他著 『プライバシー影響評価 PIA と個人情報保護』（中央経済社）

・瀬戸洋一・JIPDEC『情報化社会の個人情報保護と影響評価―韓国におけるプライバシー影響評価から見るアセスメントのあり方』（勁草書房）

・岡村久道著『よくわかる共通番号法入門』（商事法務）

・水町雅子「番号法による民間企業への実務上の影響（上）」（商事法務 NO.2006）

・日経コミュニケーション編『ライフログ革命』（日経 BP、2010）

・堀部政男・JIPDEC 編『プライバシー・バイ・デザイン』（日経 BP、2012）

・坂下哲也「パーソナル情報を取り巻く最近の動向」（信学技法、2012）

・坂下哲也「サービスのパーソナライズ化とデータ利用」（情報処理 vol54　No11、2013.11）

・坂下哲也「個人データを宝の山に　日米欧の議論の行方」（日経エレクトロニクス 2 月 17 日号、2014）

以上

＜目次＞

2014.09

第 195 回　月例研究会　２０１４年９月１８日開催

会員番号 0436 大石正人 （当協会理事）

【講演テーマ】首都直下地震の被害想定の警告～情報システムのバックアップは本当に機能するか～
【講師】東京海上日動リスクコンサルティング株式会社 上席主席研究員 指田朝久氏
【日時】2014 年 9 月 18 日(木曜日) 18 時 30 分～20 時 30 分
【場所】機械振興会館 地下 2 階 ホール
【講演骨子】講師より

2013年末に公表された政府の首都直下地震の被害想定は東日本大震災を踏まえて前回2005年に公表された想定を大きく変えている。しかしながらその被害想定の内容はあまり認識されていない。

本セミナーでは今回公表された被害想定を解説し、企業はどのように対応すればよいかについて提言する。このように書くとありふれた内容に思われるかもしれないが、政府は首都直下地震につきかなり踏み込んだ被害想定を行ったことを理解していただきたい。

政府は今回はじめて具体的なライフラインの途絶時間を公表した。その内容をみると情報システムの稼働に大きな影響を与える電力の被害想定が大幅に悪化したことがわかる。また通勤困難、飲食料入手困難さらに非常用発電機に不可欠な燃料の調達困難などがあり、これらを含め政府は過酷事象も想定外としないように求めている。

それを踏まえると首都圏における経済活動が困難であり、企業はこれらを正しく踏まえたBCPを構築することが必要である。

【講演概要】

1．政府等の主な取り組み

この１年、政府は政策的に法律改正等に取り組んできた。最も大きいもののひとつは①「国土強靭化基本法」であり、新たな国土軸の創出がうたわれています。また②災害対策基本法について、自治体の広域応援等を盛り込んだ改正の実施、③首都直下型地震対策特別措置法の制定、④南海トラフ地震に係る地震防災対策に関する特別措置法への改正（特措法の一本化）、⑤大規模地震防災・減災対策大綱の制定（地域別5大綱の統合）も図りました。一方経団連も、防災に関する委員会が 2014 年 2 月に報告書「企業間のBCP／BCM連携の強化に向けて」を出し、規制緩和、時限立法での対応など、産業界としての申し入れを行ったところです。

2．首都直下地震の想定の変更要点

2013 年に変更された首都直下地震の想定の要点は以下の通りです。

① 2005 年に想定された東京湾北部地震は当面発生しないー最新の地震学知見で関東大震災時に同震源域も同時に活動していたことが判明。

②発生時期が近付いていることは事実だが、震源は特定できないー企業、行政は各々の主要拠点直下での地震発生を想定した取り組みの必要性を示唆。

③想定マグニチュードはM7．3と不変ー阪神・淡路大震災の規模を踏襲したものに過ぎず、それ以上にならないという保証はない。

④南関東地震（M8．2、関東大震災の再来）は切迫せずー絶対ないと言い切れないので、耐震化などの対策は進めるべき（高層ビルの長周期地震動対策、東西動脈の分断対応）。

⑤津波想定は東京湾入口で津波高10m（外房など太平洋岸の大津波避難計画の策定）、湾内1～2m（東日本大震災時と同じ）－南関東地震、延宝房総沖地震等の再来を想定した内容。

この結果、被害想定についても、以下のように変化しました（支障率は地震発生 1 日目の想定）。

項目	2013 年新想定　東京南部	2005 年東京湾北部
家屋の損失	最大610千棟	最大850千棟
うち地震火災による焼失	412 〃	650 〃
揺れによる全壊家屋	175 〃	150 〃
死者	最大 23,000 人	最大 11,000 人
うち地震火災による	16,000〃	6,200〃
建物倒壊 〃	6,400〃	3,100〃
避難者	約 720万人	約 700万人
帰宅困難者	約1700万人	約 650万人
電　力支障率	約　50%（23 区 50%）	6.1%（東京 12.9%）
上水道支障率	約 30-50%（23 区 50%）	25.7%（東京 33.3%）
ガ　ス支障率	約 10-30%（23 区 30%）	12.3%（東京 19.9%）
通信支障率	規制停電の影響で 50%以上	4.8%（東京　9.3%）

（2013 年 12 月 19 日内閣府公表「首都直下地震の被害想定と対策について」の解説・詳細版：TRCリスクマネジメント最前線 2014No13）

新想定をみると、東日本大震災の経験を踏まえ、帰宅困難者が大幅に増加しています。また支障率が大きく悪化していますが、これでもライフライン単独での支障のみ考慮しており、相互依存は考慮されていません。またライフラインの復旧が、人的・物的資源の不足（ライフライン事業者の従業員不足、燃料や工事車両不足）により想定通り進まない可能性がある点にも留意が必要です。

3．首都直下地震の被害

(1)被害の特徴としては以下が挙げられます。

①政府関係機関や経済中枢といった首都中枢機能への影響が生じ、全国への波及の惧れがある、②巨大過密機能を襲う被災がどういったものになるかよくわからない、③膨大な被災者が発生し、火災に逃げ惑い、帰宅も困難になる、④深刻な交通麻痺に陥る、⑤電力供給が不安定化する、⑥情報が混乱する、⑦復興・復旧のための土地（具体的にはがれき置き場、住宅用地、等）が不足する、などです。

(2)こうした被害はどんな様相を呈するでしょうか。

建物については、木造家屋を中心に多くが損壊します。火災が同時多発し延焼は 2 日程度続きます。この間①5 割が停電し、最悪 1 週間回復しない、②電話も不通になり（1 日以上は 9 割の通信規制）、長期化の場合は携帯電話の使用も不安定化する、メールの遅配も生じる可能性がある、③主要道路の開通まで 1～2 日間を要し、一般道のガレキによる不通区間が大量に発生、深刻な交通麻痺が発生し、復旧に 1 カ月以上を要する、④鉄道の運転再開に、地下鉄で 1 週間、他の会社線で 1 カ月を要する、⑤燃料の備蓄があっても、タンクローリー不足、深刻な交通渋滞により、

非常用発電向けの重油や軽油・ガソリンの供給が困難になります。都心部は中心部から外延部にかけてドーナッツ状に延焼するため、3 つのエリアに分断され、都心部で被災した人々は 3 日間、この内円部に足止めされます。

なお上表の火災の被害想定では、以前の想定より風速を小さくする一方、東日本大震災の事例等を踏まえてシビアに見直しが行われていますが、他方で、幹線道路での自動車の渋滞により30m道路の延焼防止機能が働かない可能性までは想定していませんので、更に厳しい結果も予想されます。

電力についてみると湾岸の火力発電所が点検と被災で運転を停止し、復旧には 1 週間から数カ月を要します。供給能力は夏場のピーク需要の約 5 割を賄える程度まで低下します。需給バランスが崩れることにより、発災直後は 5 割の地域で停電し、通電の再開は需要見合いになりますから、需要抑制のため計画停電の措置が取られます。

なお国土交通省は更にシビアな想定を置いています。

避難者 720 万人は指定避難所の収容可能数を超過します。食糧や救援物資の需要不足が続き、食料は 3,400 万食不足します。災害発生 1 週間後でも停電率が 5 割、断水は最大 3 割が継続し、冷暖房の利用、飲料水の入手（最大 1,700 万リットル）、水洗トイレの利用が困難化します。2007 年の中越沖地震のように真夏に発生すれば最悪の事態になります。仮設トイレも不足し、し尿処理やごみ収集も遅延します。燃料類の供給も遅れが生じます。

復旧工事の面でも、都心部での集中・輻輳により大幅に遅延します。鉄道は地震後 1 カ月でも 6 割の復旧に止まります。市街地の火災で高速道路の高架橋の変形の可能性があり、数カ月にわたり首都高速 3，4 号、湾岸線が通行停止になります。道路に滞留・放置車両が残存し、救急活動の支障になります。排水機械の機能不全が、海抜零メートル地帯の浸水災害を引き起こします。250 岸壁の被災、東京湾内への石油類の流出で船舶の入港が困難になります。

このため経済的被害は建物等の直接被害で約 47 兆円、生産・サービス被害で約 48 兆円、合計約 95 兆円が見込まれるため、その軽減のために国と経団連が各企業の事業継続計画の促進を働きかけることで認識を一致させました。

政府としては首都直下地震への対処（特に事前防災）について、中枢機能の確保、被害軽減の観点から以下のような課題への対策を取りまとめていく方針です。

①首都中枢機能の継続性確保の観点から、政府全体としての業務継続体制の構築、情報の収集や集約、発信体制の強化、金融決済機能等の継続性、企業の事業継続の備え等に取り組みます。このうち政府のBCPは作成公表されました。

②震源域が特定できないことから、首都圏全般で建築物、施設の耐震化等を推進します。

③出火防止対策として、感震型電源ブレーカー等の普及を促進します。

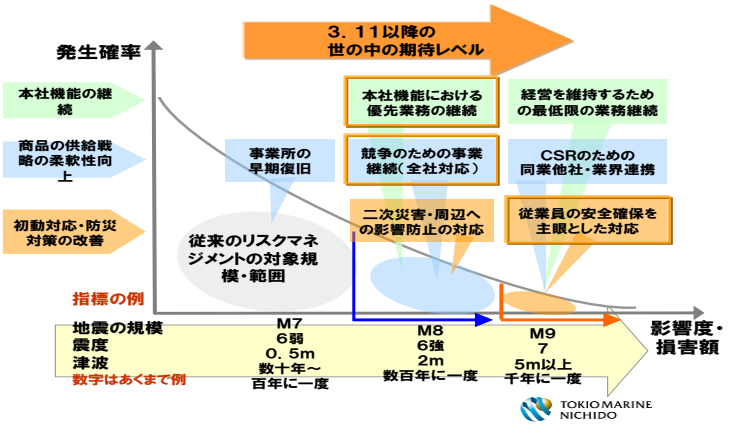
④2020 年五輪東京大会に向け、外国人観光客への防災情報の伝達等につき早急な対策を講じます。

また 2014 年 6 月 3 日には国土強靭化基本計画を閣議決定しました。

4．首都圏直下地震の政府被害想定を読み解く

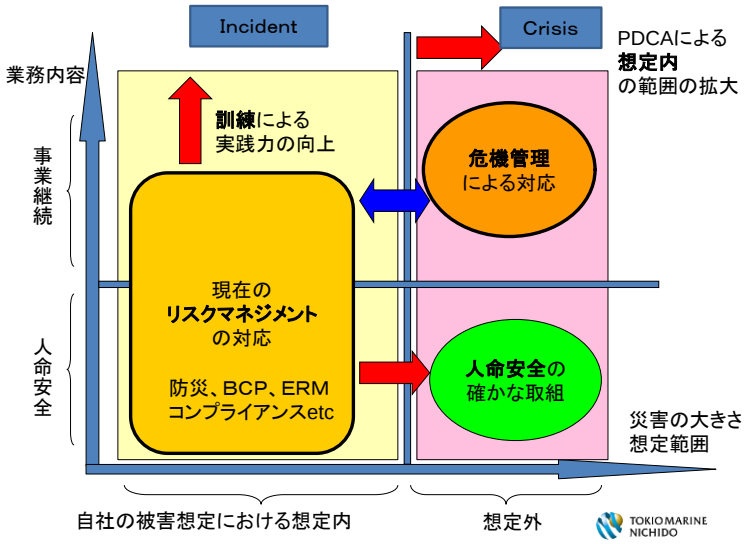
改めて政府の首都直下地震の被害想定を踏まえると、これから対応を考える上でのポイントは第一に「どこで地震が起きるか不明」であり、第二に「この被害想定は最大ではない」の 2 点であり、前者は企業として一番致命傷になる直下地震の想定を示唆しており、後者はより過酷事象を例示している、ということです。

企業経営をめぐって東日本大震災以降のリスクマネジメントを考える上で、重要なのは世の中なりステークホルダーの認識や要求レベルがより厳しくなり、経済合理性は意識しつつも、標準シナリオのほかに過酷事象、というように複数のシナリオを用意することが経営戦略として求められるようになったことです。



こうした観点から、レベルを分けて想定を置いて対応することも必要です。南海トラフ地震を例にとると、まずレベル 1（南海トラフ被害想定 2005 年、M8クラスを念頭）では人と経済の双方を守る対策を講じます。コスト対効果を踏まえ、例えば堤防の建設はこのレベルで構築します。レベル2（南海トラフ被害想定 2012 年、M9クラスを念頭）では人命を守る対策を優先し、例えば避難計画を策定します。そして業種によってはレベル 3 として、レベル 2 を超える災害の発生可能性も念頭に、対策を講じます。

ここで東日本大震災の教訓を災害の大きさについての想定と想定外の事態を横軸に、これに対応した業務内容（人命の安全性確保、事業継続）を縦軸にとって整理してみると、現在のリスクマネジメントでは一定の想定のもとに事業継続計画を策定し、訓練による実践力を高める、というアプローチをとっています。これはいわばインシデント対応です。シナリオ（想定）を超える事態においては、人命の安全確保を確実にしたうえで、事業継続の面では危機管理モードで対応します。この領域になるといかにチェックポイント（やるべきこととその優先順位）を挙げられるかが問われ、企業経営者は意思決定を通じてその真価を問われるわけです。



それでは政府資料に基づく想定外事態における過酷事象とはどんなイメージなのでしょうか。それを例示すると、東京湾岸の火力発電所での大規模被災とそれに伴う電力事情の悪化、湾内への油流出による海上火災、放送やインターネットの業務停止、堤防決壊等による海抜ゼロメートル地帯の浸水（ハリケーン・カトリーナ来襲により米ニューオー

リンズでは 1 カ月間水が抜けませんでした）、高層ビルの被災、数万人規模でのエレベータへの閉じ込め、燃料・食糧等の供給停止（特に避難所に行かず自宅等へ留まる人のケア）等が起こります。また復旧活動の面で、首都圏には建設業者が少なく不通道路の啓開が難しかったり、ガレキ処分場の確保ができなかったりするため、相当な遅れが見込まれます。また電力など社会インフラの復旧時間の見積もりは、その他のインフラの 100％使用可能性を前提としており、多重的な被災を考慮した場合にはさらに遅れる点も考慮が必要です。

このほか、経団連危機管理タスクフォースの会合で首都直下地震対策検討ワーキンググループ増田主査は、火災による 3 地域への分断とそれに伴う移動や生活物資の供給困難を踏まえ、企業には 1 週間の備蓄、出勤や業務実施が困難になることの認識、全社員を対象とした訓練の実施、を求めています。つまり、避難所に行かない人の衣食住が政府の対応計画のスコープ外になっていること、首都圏立地の企業活動について被災者保護優先のため政府により活動を制限される可能性があることを念頭に置いて、被災地の外への役職員の移動、更には重要拠点の移転や代替拠点の確保を考える必要があると思います。

5. バックアップシステムは稼働できるのか

バックアップシステムの稼働条件としては、まずシステムサイドでは、センターやサーバーの二重化やオフサイトバックアップを確保するほか、これに使用するデータやデータベースの取得（紙媒体を含むバイタルレコード＜重要情報資産＞）とバックアップ、代替通信ネットワークへの接続、端末や保守要員の確保、リモートメンテナンスの実施体制の構築が必要です。発災時には、サーバーが被災する、休日夜間に発生した場合にはシステム要員やその交代要員の確保が困難になったり、保守要員が帰宅困難者になります。物流の麻痺により、非常用発電機燃料の確保が困難になるほか、被災地要員の衣食住も確保出来難くなります。ちなみに、非常用発電機から出火したケースが最近発生したことを考えると、電気系統の不稼働などの事態もありうることへの認識も必要です。

また要員が確保できても、非常時のデータセンターへの入館ができない、切替手順書が未作成だったり、手順の習熟者が限られている、手順書がペーパーレスで停電により参照できない、無人運転のケースで、リモート保守のためには、災害時に外部接続機器の稼働が前提になっている、テスト環境がない、バックアップ側に切り替えた後の切り戻し手順が設計されていない、といった懸念事項もあります。

なお、バックアップシステム稼働に当たり、入居ビルの耐震安全性についても注意が必要です。一般には新建築基準法に準拠した建物は大丈夫だと認識されていますが、実際には、災害応急対策活動に必要な機能を有する施設かどうか、等に対応して、構造体・建築非構造部材・建築設備ごとに、より厳しい基準が設けられています。自社のバックアップ機器の設置ビルの基準充足状況にも関心を払うことが大切です。

次にユーザーサイドからみたバックアップシステムの稼働条件ですが、ユーザーの場合には、システムによりサービスを受ける（バックアップ）業務の範囲、復旧目標時点や目標時間等、業務継続計画の認識がどうなっているかが重要です。そのうえでシステムを利用する要員やオペレーション場所の確保、代替事務処理のためのマニュアル、帳票などを準備のうえ、事務への習熟や訓練等、教育を行います。バックアップの前提となるメールや掲示板がその対象から漏れていると業務が遂行できません。以上について、被災地、非被災地各々について検討し、応援ができる体制の構築が必要です。

このほかの配慮事項としては、計画停電の可能性（1 カ月以上の停電需給バランス調整）があり、メイン・サブサイトが、ともに計画停電域になりうる関東や山梨静岡の一部にある場合、同時に影響を受ける懸念が挙げられます。

ではクラウドサービスを利用している場合にはどうでしょうか。同サービスの場合、サーバーについてメインまたはサブのいずれかが非被災地にあり、被災を免れる可能性が高い、とは言えます。また非被災地にいるユーザーは機能が期待できます。しかしながら、オンプレミスの場合と同様、通信規制・通信支障に伴うネットワークへの影響、中継サーバーの停電による停止、バックアップサイトへの円滑な切り替え可否、計画停電の影響や在宅勤務者の衣食住確保などの課題は共通しています。

ここでIT関連で懸念事項として挙げられている点について考えてみましょう。

Q1：安否確認システムは機能するか。

A：首都圏での同システムの同時稼働に伴い、発信数の増大でシステム容量の超過や、通信網の機能不全による携帯電話あるいはメールの機能不全、通信規制の可能性もあるため、100％の依存は危険です。

Q2：ツイッターやSNSの有効性はどうか。

A：停電のなかった地域では東日本大震災でも有効性が確認されましたが、東北地方の多くでは停電により携帯電話の中継器のバッテリー切れから携帯電話が機能せず、情報収集手段としても限界がありました。首都圏では発信数が膨大になると想定されるため、通信数の抑制等の取り組みが必要です。

Q3：過酷事象で指摘されている、インターネット業務停止に伴う具体的な被害想定はどうか。

A：インターネット全体にどのような影響が生じるかは不明です。首都圏で業務を行う多くのプロバイダーはサーバーをはじめ多数の情報機器を首都圏に集積させています。このため計画停電や非常用発電機用の燃料不足から、プロバイダーのサーバーが停止する懸念があります。

Q4：通勤不能への代替措置として、在宅勤務は有効か。

A：在宅勤務の有効性が確保されるためには、自宅が停電しておらず、インターネットが接続でき、業務システムにつきバックアップサーバーにスムーズに切り替えられる、等の前提条件が整う必要があります。

【出典】

・「首都直下地震の被害想定項目及び手法の概要～人的・物的被害～」（平成25年12月、中央防災会議首都直下地震対策検討ワーキンググループ）
・「評価対象とする自然災害等を巡る現状及び課題」（平成 26 年 1 月 22 日、経済産業省商務流通保安グループ 電力安全課）
・経済産業省産業構造審議会保安分科会電力安全小委員会「電気設備自然災害等ワーキンググループによる検討結果」（平成 26 年 4 月 25 日）
・国土交通省；首都直下地震対策計画第一版；平成 26 年 4 月 1 日
・「国土強靭化基本計画」の概要；平成 26 年 6 月 3 日閣議決定

【参考文献】

・「企業の地震リスクマネジメント入門」東京海上日動リスクコンサルティング株式会社編著；日科技連
・「必ずやってくる首都圏巨大地震」；Newton 2014 年 10 月号

【質疑】

質問 1:首都圏直下型地震で震度 7、という時のインパクトを具体的に教えてください。
回答:倒壊家屋が 3 割に達するが、どこで起きるかわからないので、ポイントは自社の拠点が震度 6 強を超えるレベルに堪えうるのか、にあります。

質問 2:被災したオフィスは再使用できない、との理解で良いでしょうか。
回答:その理解で良いです。新建築基準法では安全で逃げられるかどうかがポイントであり、被災すれば二度と使用はできません。

質問 3:幹線道路に自動車が積滞するとのことだが、これを排除する対策はありますか。
回答:警視庁は最近方針を改悪しました。大地震が発生した場合、従来は、環状 7 号線の内側での通行禁止でしたが、東日本大震災後、都心から外への通行の許容に方針を変更しました。運転者の基本動作としては、被災時には車を動かさず、キーを付けたまま停止して避難してほしいと思います。

質問 4;テレビやラジオなど放送も支障が生じるとのことだが、マスメディアの影響をどう見ればよいでしょうか。
回答:東京タワーやスカイツリーなど電波塔が被災する影響が大きいです。このためNHKの場合、衛星放送の大阪への切り替えを想定しています。受信者の立場としては、ワンセグサービスの利用も考えられます。

質問 5:エレベータへの閉じ込めが多数発生するとのことだが、近接階での停止などの機能との関係はどうでしょうか。
回答:直下型の場合は間に合いませんので、閉じ込められる人が多数出ます。保守員の駆けつけまでの時間を考慮し、現在エレベータサービス各社では、ビルオーナーでも復旧措置が取れるタイプへの改修を進めています。

質問 6:南海トラフの危険性がクローズアップされているが、関東や北海道など他の地域は大丈夫ですか。
回答:今回の政府想定の見直しは、東日本大震災の発生を踏まえたものとなっています。この地震の発生により、再発の可能性は低下したとも見なせますが、絶対大丈夫とも言い切れません。
　余談ですが、全国各地に海岸段丘がみられ、中にはおよそ想像しがたい大きな隆起のものもあります。もっと大きな巨大災害も想定外であるとは言い切れない、というのが歴史的地学的知見だと思います。

質問 7:都心部はドーナッツ状に延焼するとのことだが、通信網も影響を受けるのではないでしょうか(世田谷ケーブル火災の時も、大きな影響が出たくらいなので)。
回答:今回は電力の需給バランスと火力発電所の影響を中心に想定を置いており、変電所の焼失による影響とか、さらには電力供給を受ける通信網の焼失の影響までは考慮されていません。

質問 8:建物の倒壊や火災による死者への対処策についてはどうでしょうか。
回答:米国などでは死者を包むシートの準備や安置場所の確保まで視野に入れてマニュアル化しています。日本では言霊信仰、とでもいうのでしょうか、対策の必要性を言い出すこと自体が禁句になっている気がします。現実には医師による生死の見極めや遺体の確認、付き添いの必要性等、職域で対応すべきことが発生します。

質問 9:ガスの支障率が低いのはなぜでしょうか。

回答：ガス会社がガス管のリニューアルや切換装置の更新を進めていることが大きいです。ただ老朽化したビルでは耐震性の低いガス管が残っているケースもあるため、注意が必要です。

質問 10：地震が発生すると流言飛語のような事態も予想されますが、正しい情報を得るためにはどういった配慮が必要でしょうか。
回答：組織的な内容の確認が重要と考えます。そのためには第一に情報発信元の信頼性を確認すること（できるだけ大本の情報源で確認すること）、第二に、情報の確からしさを高めるため、複数の情報源を付き合わせること、が大切です。ISO22320を参照してください。
広島の豪雨でも消防と警察の公表で、行方不明者数等に食い違いが生じました。東日本大震災でも同様の食い違いが解消されないままになっています。
また東日本大震災でも、自治体は情報発信しているのにアクセスの集中でウエブページが繋がらない事態が発生しました。ボランティアでのミラーサイトの立ち上げなど、支援策も有用です。

【感想】
政府の被災想定の見直し内容を可視化して説明いただいたうえ、インシデント対応からクライシス対応まで視野に入れた対処こそ企業経営者の責任、とした説明はわかりやすく、参加者の満足度は極めて高かった、と推察されます。
今回のセミナーをきっかけに、首都圏に立地する組織体において、ありうるべき首都圏直下地震への対処を着実に進めることの重要性とともに、その進捗状況をシステム監査の立場からもきちんと見ておく必要性が痛感されました。
講師はNPO事業継続推進機構・副理事長ほかを務められる傍ら、政府所管の各種委員の要職としても活躍されていますが、今後も同分野を中心に発信を続けて頂きたいと思いますし、当協会としても連携していければ、と希望しています。

以上

＜目次＞

2014.10

第 24 回ＣＳＡフォーラム(2014/9/8)「測量・地図とＧＩＳ～国家インフラから市民インフラへ」

会員番号　6005　斉藤　茂雄　（CSA 利用推進 G）

CSA 利用推進グループでは有限会社セキュアランス　代表取締役の田附喜幸（たつきよしゆき）氏をお迎えし、第 24 回CSAフォーラムを開催しました。田附氏は国際航業株式会社に入社し、GIS（地理情報システム）の導入、研究・開発や ISO（QMS、EMS）及び PMS の構築に従事されました。その後有限会社セキュアランスを設立し、現在は ISO 審査員として審査活動を行うと同時に、GIS 導入コンサル、審査登録機関審査室業務などを行っておられます。

地理情報は生活のインフラとして無くてはならないものの一つです。身近なカーナビや防犯から、地球レベルの気象解析など様々な分野に活用が進んでいます。しかしこんなに身近な地理情報について、実は地図の製作にはどんな歴史があり、どんな技術を用いて来たのか、どんな問題があるのか等々、殆ど知識がないのは私だけでしょうか。今回のお話で、測量の基準点が元々日本で用いていたものと国際基準系とでかなりズレがあり、場合によっては普段見ている地図が、ズレたままのものというお話があり、ビックリでした。その他沢山の興味深いお話の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簡単な懇親会も実施しました。

タイトル：「測量・地図とＧＩＳ～国家インフラから市民インフラへ」

概要（開催案内の講師コメントより）：

古代より権力者は、その人民（戸籍）と土地を把握することに努力してきた。特に近代以降は、精密な地図を作成し、維持することが重要となり、まさに重要な“国家インフラ”であった。第二次大戦以降、日本においては急激な“社会インフラ”（特に道路）の整備を支える技術として、地図の製作が行われた。

更に、ICT 技術の進展に伴い、デジタル化された地図情報を使う技術「GIS」が、民間を含めた様々な分野で使われており、重要な“市民インフラ”となっている。

なお、利便性には常に“問題点”という影が存在するが、最後にこの点についても述べたい。

スライド目次：

1. 測量と国家
2. 測量・地図・GISの基礎知識
3. 地図情報のIT化
4. 測量・地図作成プロセスのIT化
5. 関連する法規制と国の施策
6. GISの標準化
7. 日本版GPS衛星

開催日時： 2014 年 9 月 8 日（月） 18 時 30 分～20 時 30 分

開催場所： 品川区大崎1－2－1（株）日立システムズ　本社

■■■■■■■■■――■■■■■■■■■

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＞

2014.10

～「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３
2-2-2. 個人情報の取得関係（法第 17 条～第 18 条関連）

会員番号　6005　斉藤茂雄　（個人情報保護監査研究会）

経済産業省は9月26日に、(株)ベネッセコーポレーションに対し、個人情報の保護に関する法律（以下「法」）第34条第1項の規定に基づき、委託先も含めた個人情報の保護に関する実施体制の明確化、および情報セキュリティ対策の具体化を行うよう勧告しました。また、同日、「経済産業省ガイドライン」の改定について、2回目のパブコメが発表されました。 そこでは、今回のテーマの「適正取得」に関しても改正案が追加されています。

2-2-2. 個人情報の取得関係（法第17条～第18条関連）

（１）適正取得（法第１７条関連）

法第１７条
個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。

事業者は、秘密として管理されている事業上有用な個人情報で、公然と知られていないものを、不正に取得、または不正に使用・開示した場合には、不正競争防止法により刑事罰が科されることがあります。

【個人情報取扱事業者が不正の手段により個人情報を取得している事例】

事例1）親の同意がなく、十分な判断能力を有していない子どもから、取得状況から考えて関係のない親の収入事情などの家族の個人情報を取得する場合

事例2）法第23条に規定する第三者提供制限違反をするよう強要して個人情報を取得した場合

事例3）他の事業者に指示して上記事例1）又は事例2）などの不正の手段で個人情報を取得させ、その事業者から個人情報を取得する場合

事例4）法第23条に規定する第三者提供制限違反がされようとしていることを知り、又は容易に知ることができるにもかかわらず、個人情報を取得する場合

事例5）上記事例1）又は上記事例2）などの不正の手段で個人情報が取得されたことを知り、又は容易に知ることができるにもかかわらず、当該個人情報を取得する場合

※個人情報保護監査研究会注：事業者が、優越的な地位を利用して取得する場合も不正の手段とみなされる可能性があります。

※ご参考（2014年9月26日に追加された、経産省GL改正案）

また、第三者から個人情報を取得する場合には、提供元の法の遵守状況（例えば、オプトアウト、利用目的、開示手続き、問い合わせ・苦情の受付窓口をホームページに明記されていることなど）を確認し、個人情報を適切に管理している者を提供元として選定するとともに、実際に個人情報を取得する際には、その都度、例えば、取得の経緯を示す契約書等の書面を点検する等により、当該個人情報の取得方法等を確認したうえで、当該個人情報が適法に取得されたことが確認できない場合は、偽りその他不正の手段により取得されたものである可能性もあることから、その取得を自粛することを含め、慎重に対応することが望ましい。

※個人情報保護監査研究会注:オプトアウトとは、個人情報を第三者提供することについて、本人がNo！と言ったら、提供を止めることです。また、本人の了解を得ずにDMを郵送し、本人が停止を求めてきたら、送付を停止するというというケースもオプトアウトです。

経済産業省GL改定案に追加された「適正取得」の項目は、ベネッセコーポレーションの名簿売買（第三者提供）の事件を重く受け止めて、再発防止の観点から厳しいガイドラインが示されたものです。名簿業者から名簿を購入することまでは禁止されていませんが、提供元についても「評価」するよう求めています。 ホームページや契約書を点検しただけでなく、何をもって、適正取得であると判断したのかを文書に記録し、責任ある者の承認を得ることは不可欠です。

（２） 利用目的の通知又は公表（法第１８条第１項関連）

法第１８条第１項

個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

個人情報を取得する場合は、あらかじめその利用目的を公表することが望ましく、もし公表していない場合は、取得後速やかに、その利用目的を、本人に通知するか、又は公表しなければなりません。

法施行前から保有している個人情報を、単に保有しているだけであれば、この規定は適用されませんが、利用するのであれば、利用目的等を本人の知り得る状態におく必要があります。

※個人情報保護監査研究会注:解説で、「電話帳、カーナビゲーションシステム等の取扱いについての場合を除く」とあり、他人が作成したこれらのデータは個人データに該当しないとされています。しかしこれらのデータをもとに、新たに個人情報を加えたり、加工したりする場合は、その利用目的を、本人に通知するか、又は公表しなければなりません。

【本人への通知又は公表が必要な事例】

事例1）インターネット上で本人が自発的に公にしている個人情報を取得する場合

事例2）インターネット、官報、職員録等から個人情報を取得する場合

事例3）電話による問い合わせやクレームのように本人により自発的に提供される個人情報を取得する場合（本人確認や問い合わせに対する回答の目的でのみ個人情報を取得した場合を除く。）

事例4）個人情報の第三者提供を受ける場合

事例5）個人情報の取扱いの委託を受けて、個人情報を取得する場合

（３） 直接書面等による取得（法第１８条第２項関連）

法第１８条第２項

個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

本人が、書面等による記載、入力画面への打ち込み等を行うことにより、直接本人から個人情報を取得する場合には、あらかじめ、その利用目的を明示しなければなりません。口頭によって取得する場合に都度説明すること

までは義務化されていませんが、あらかじめ利用目的を公表するか、速やかに、本人に通知し、又は公表しなければなりません。また、人の生命、身体又は財産の保護のために緊急に必要がある場合も、あらかじめ明示する必要はありませんが、取得後速やかに利用目的を、本人に通知し、又は公表することが求められます。

【あらかじめ、本人に対し、その利用目的を明示しなければならない場合】

事例1）申込書・契約書に記載された個人情報を本人から直接取得する場合

事例2）アンケートに記載された個人情報を直接本人から取得する場合

事例3）懸賞の応募はがきに記載された個人情報を直接本人から取得する場合

※個人情報保護監査研究会注：「あらかじめ」とは、「取得する前に」という意味です。

（４）利用目的の変更（法第１８条第３項関連）

法第１８条第３項

個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。

事業者は、社会通念上、本人が想定することが困難でないと認められる範囲内で利用目的を変更した場合は、変更された利用目的について、本人に通知、又は公表します。

※個人情報保護監査研究会注：本人の想定外の利用目的の変更を行う場合は、本人から、明示的な同意を得る必要があります。

（５）適用除外（法第１８条第４項関連）

（ｉ）本人又は第三者の権利利益を害するおそれ（法第１８条第４項第１号関連）

法第１８条第４項第１号

前３項の規定は、次に掲げる場合については、適用しない。

１　利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合は、本人に通知、又は公表する必要はありません。

事例）いわゆる総会屋等による不当要求等の被害を防止するため、当該総会屋担当者個人に関する情報を取得し、相互に情報交換を行っている場合で、利用目的を通知又は公表することにより、当該総会屋等の逆恨みにより、第三者たる情報提供者が被害を受ける恐れがある場合

（ⅱ）当該個人情報取扱事業者の権利等を害するおそれ（法第１８条第４項第２号関連）

法第１８条第４項第２号

２　利用目的を本人に通知し、又は公表することにより当該個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合

利用目的を本人に通知し、又は公表することにより企業秘密に関すること等が他社に明らかになり、事業者の権利又は利益が侵害されるおそれがある場合は、前項と同様に、本人に通知、又は公表する必要はありません。

事例1）通知又は公表される利用目的の内容により、当該個人情報取扱事業者が行う新商品等の開発内容、営業ノウハウ等の企業秘密にかかわるようなものが明らかになる場合

事例2）暴力団等の反社会的勢力情報、疑わしい取引の届出の対象情報、業務妨害行為を行う悪質者情報を取得したことが明らかになることにより、情報提供を受けた企業に害が及ぶ場合

（iii）国の機関等への協力（法第１８条第４項第３号関連）

法第１８条第４項第３号
３　国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。

国の機関等が法令の定める事務を実施する上で、民間企業等の協力を得る必要がある場合であり、協力する民間企業等が国の機関等から受け取った個人情報の利用目的を本人に通知し、又は公表することにより、当該事務の遂行に支障を及ぼすおそれがある場合は、同様に、本人に通知、又は公表する必要はありません。

事例）公開手配を行わないで、被疑者に関する個人情報を、警察から被疑者の立ち回りが予想される個人情報取扱事業者に限って提供する場合、警察から受け取った当該個人情報取扱事業者が、利用目的を本人に通知し、又は公表することにより、捜査活動に重大な支障を及ぼすおそれがある場合

（iv）利用目的が自明（法第１８条第４項第４号関連）

法第１８条第４項第４号
４　取得の状況からみて利用目的が明らかであると認められる場合

個人情報が取得される状況から見て利用目的が自明であると認められる場合は、本人に通知、又は公表する必要はありません。

事例1）商品・サービス等を販売・提供する場合、住所・電話番号等の個人情報を取得する場合があるが、その利用目的が当該商品・サービス等の販売・提供のみを確実に行うためという利用目的であるような場合

事例2）一般の慣行として名刺を交換する場合、書面により、直接本人から、氏名・ 所属・肩書・連絡先等の個人情報を取得することとなるが、その利用目的が今後の連絡のためという利用目的であるような場合（ただし、ダイレクトメール等の目的に名刺を用いることは自明の利用目的に該当しない場合があるので注意を要する。）

※個人情報保護監査研究会注：
事例1）は、例えばクリーニング店やデリバリーサービスなどで受取人を特定するために個人情報を取得するなどのケースに限定されます。
事例2）と同様に、BtoBにおける請求書や見積書等の伝票に記載された担当者名等、企業内での出張旅費申請書、緊急時連絡先一覧なども「利用目的が自明」と判断できるでしょう。
日常業務における、管理の簡素化も必要ですが、「利用目的が自明」を適用する場合、事業者の都合で拡大解釈しないよう、注意が必要です。

次回は、「2-2-3. 個人データの管理（法第19条～第22条関連）」の読みこなしポイントを掲載します。
ガイドライン改正案についても言及する予定です。
バックナンバー目次 http://www.saaj.jp/saajpmsMETIGL/000METIGL.html
個人情報保護監査研究会 http://www.saaj.or.jp/shibu/kojin.html

■

＜目次＞

2014.09

北信越支部 「2014 年度 長野県例会 報告」

会員 No.1281　北信越支部 宮本 茂明

以下のとおり2014年度 北信越支部長野県例会を開催しました.

・日時:2014 年 9 月 13 日(土) 13:00-17:00　　参加者:7 名

・会場:松本商工会館 606 会議室(長野県 松本市)

・議題:

✧ 研究報告:

「外部委託先に対するシステム監査の課題について」

藤原 康弘 氏

✧ 意見交換:

「コンティンジェンシープランの策定とそれに対する監査」

(2014 年度 SAAJ 西日本支部合同研究会での報告に向けての意見交換)

◇研究報告

「外部委託先に対するシステム監査の課題について」

報告者(会員 No. 0115 藤原 康弘)

1 はじめに

外部委託先のシステム監査について、最近起きた事件や、問題点等を考えながら、その課題について検討したい。なお、この発表は、私の個人的な見解である。

2 スルガ銀行・日本IBM裁判

システム業務委託契約は、請負契約であるか、準委任契約であるか、契約が破綻し委託者と受託者との間で裁判となった場合に問題となることが多い。最近は、委託したプロジェクトの段階により異なるとされ、請負と準委任の混合契約あるいは新しい無名契約とされている。

この裁判は、スルガ銀行が、要件定義段階でのプロジェクト失敗について、契約不履行と不法行為の責任を主張したものである。これに対し、裁判所は、日本IBMのプロジェクトマネジメント義務違反による不法行為責任を認めたものである。また、契約の段階により、受託者のプロジェクトマネジメント義務と、委託者の協力義務の双方の責任の違いを認めている。

両者とも最高裁に上告中なので法的な決着は付いていないが、プロジュクトの開始に当たり、契約者双方の責任と義務を明確にして始めることにより、紛争を予防する必要があることは確かである。この点について、システム監査はどう関与していくか課題である。

3 クラウドの利用

クラウドの利用について、プライベートクラウドは、従来の外部委託と同様であると考えてよいとされる場合が多い。しかし、企業秘密との関係から、開示してもらえない情報は残る。立ち入り監査が可能であっても、システム監査は受託者の制限を受ける。

一方、パブリッククラウドは、従来の委託先管理では困難で、顧客情報や、重要な企業機密には利用できないとか、撤退リスクがあるからコア事業に適用すべきでないといった意見が多いようである。しかし、それでは、パブリッククラウドは事実上利用できなくなる。セキュリティ上、譲れないものについて受託者の責任を明確にして第三者による保

証を付けることにより、委託者の責任を軽減できないかと思う。なお、顧客への責任は、委託者に残ることには確かである。

4 ベネッセ個人情報流出事件

外部委託先の社員による犯罪を見ると、①直接の委託先より再委託先で発生している、②金銭目的で、顧客情報の流出が多い、③容疑者は高度情報技術者で、大きな権限を付与されていたという点に特徴があると思われる。

ベネッセ事件では、USBメモリーへのデータ禁止設定のパソコンから、容疑者のスマートフォンへデータのダウンロードが可能であることを偶然知ったことが犯行のきっかけであったと報道されている。iPhone、Android4.0 以降のスマートフォンによるデータコピーが可能であったということが必ずしも周知されていなかった。しかし、容疑者は、データベースの情報流出防止プログラムを解除しているとも言われ、インターネット経由でも情報を窃取できたのではないかとも言われている。

ログが保存されているだけで監視されていなかったことも問題と言われている。ログ監視によるアラート機能や、カメラによる監視が必要であったかもしれない。

一番重要なことは権限管理である。容疑者は、請負契約の派遣社員であったと思われる。重要な仕事を派遣社員に任せていてよいのかという問題である。自社のデータセンターへの派遣社員について、自社の社員と同様な管理をしているから問題ないという意見があるが、むしろ一緒にいるから信頼し過ぎて管理がおろそかになる可能性がある。少なくとも待遇面は違う。外部委託管理という点から、難しい問題がある。(注)

5 システム監査における課題

以上のような問題点を踏まえてシステム監査における課題を考えると、まず、入り口が重要と思われる。撤退リスクが大きいことから、選定先の検討において、システム監査の関与が重要である。しかし、ブレーキを踏む議論ばかりでなくアクセルを踏む議論もしないと企業競争に勝てないから、難しい判断となる。また、業務ソフトについては、バージョンアップにより、いつのまにかクラウド利用となるケースも増えている。外部委託先の把握が十分かという問題もある。

さらに、重要なことは、外部委託先のシステム監査をどうやっていくかということである。企業秘密を理由に開示されないだけでなく、都合良い資料のみ提示されてもわからない場合もありうる。受託者が念入りに準備したコースに従って監査せざるを得ない場合もある。受託者との信頼関係の中で、本当に有効なシステム監査を実施することは、かなり大変なことである。

委託先における犯罪が続くと、不正防止の観点を取り入れることへの要望が高まってくる。特に内部犯罪については、技術的な面と併せて、人的な側面も重視して検討する必要が出てくる。場合によっては、システム監査の領域を越えるかもしれない。さらに、セキュリティ環境の変化にも対応していかないといけない。

6 まとめ

様々な課題に対応するためには、システム監査の担当者の能力を向上させることが重要である。システム監査の外部委託も安易にしてしまうと、それができない。社内でノウハウを蓄積するとともに、専門職として社外との情報交換の場を持つことが必要かと思われる。

(注) データベース・セキュリティ・コンソーシアムのアンケート調査によると、データベースの管理・運用担当者 1000人からの回答で、「将来データベースの情報をこっそり売却するかもしれない」かとの設問に「そう思う」3.6%、「やや思う」7.1%であるという。(www.db-security.org/20140910news.pdf)

◇意見交換

「コンティンジェンシープランの策定とそれに対する監査」

（2014 年度 SAAJ 西日本支部合同研究会での報告に向けての意見交換）

報告者（会員 No.1281　宮本 茂明）

2014 年度西日本支部合同研究会「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」での北信越支部からの報告を検討するため，「コンティンジェンシープランの策定とそれに対する監査」というテーマで意見交換を行いました．

1．IPA「情報システム基盤の復旧に関する対策の調査報告書」

最初に，IPA の「情報システム基盤の復旧に関する対策の調査報告書」の概要を紹介し，意見交換の糸口としました．

IPA「情報システム基盤の復旧に関する対策の調査報告書」(2012 年 7 月)
http://www.ipa.go.jp/sec/softwareengineering/reports/20120725.html

- 東日本大震災を受け，情報システムの高回復力確保の重要性を再認識し，企業における IT サービス継続計画（IT-BCP）策定の取り組み状況/個別対策の実施状況について，文献，アンケート，ヒアリング調査を実施．
- 東日本大震災の発生前後で、IT-BCP の策定に対する企業の認識は高まっていると言われているが，IT-BCP を実際に「策定済み」の企業は 24.8%，「策定の予定なし」とする企業は 27.4%であった．
- システムの目標復旧時間を 6 時間未満に設定していると回答した企業のうち約 1/4（24.4%）が，システムを冗長化していない．
  （設定した時間内にシステムを復旧するための適切なシステム構成を採用していないといえる）
- 技術的対策として，待機系システムの設置，バックアップサイトの設置などが重要．
  システム構築に関して，仮想化技術やクラウドサービス活用も有効．

2．意見交換

参加者によるテーマに関連し以下のような意見交換を行いました．

＜事業継続計画（BCP)と IT サービス継続計画（IT-BCP）＞

- IT-BCP は，BCP が前提．
- 情報部門が中心となって IT-BCP 策定するケースが多い．災害発生時の体制について，BCP 体制との整合がとれておらず，IT-BCP 対応と BCP 対応で重なって役割を担う人がいて実行性に問題がでることがある．
  IT-BCP 策定にあたっては，情報システムだけでなく，BCP 全体の中で情報システムを考える必要がある．

＜IT-BCP としてのクラウド利用＞

- 東日本大震災時に診療記録が医療機関から消滅し，クラウド化の重要性が表面化した．また、避難住民が流動的になることから、自治体の管理する住民データもクラウド化することが必要と考える．
- 診療データや住民データのクラウド化には，個人情報の漏洩というセキュリティの問題と，緊急時にも利活用できる可用性の確保という，二律背反にある課題の克服が必要になる．また，外字の取り扱いをどうするかといった問題が残っている．
- 首都圏での地震災害や東海～南海という極めて広域な範囲での津波を伴う地震災害を念頭に入れると，コンピュータ環境は AWS のようなクラウド環境にシフトさせるしか解決策はないようにも思える．その環境が海外に及ぶ場合には国内法が適用されないというような問題もある．

- クラウド化すれば安全ということではなく，クラウドサービス拠点が被災し，サービス停止する可能性も検討しておく必要がある．
- クラウド化を進めるためには，システムをほとんど作り直す必要がある．また，クラウド化したシステムをどうシステム監査していくかも重要となってくる．

＜電力/ネットワークの確保＞

- オンプレミスのシステムでは，電源やネットワークの確保が必須．自家発電装置があっても燃料の確保，データセンターに出勤できる社員の確保がキーになってくる．

＜災害時におけるセキュリティ確保＞

- 震災時，免震構造を誇るデータセンターに地域住民が逃れてくるようなケースで，セキュリティ確保と被災者救援の両立という問題もある．

＜災害時における ICT 活用＞

- 地域防災面からみると，原子力災害発生時の「連絡体制の整備，緊急避難経路，道路の渋滞状況等の」情報利活用は ICT の段階まで出来上がっていない現状にある．

＜中小製造業の BCP＞

- 中小製造業の事業継続計画を考えると，事業の IT 依存度が高くないところでは，IT-BCP の優先度は高くない．被災時の製造設備復旧のための資金調達も大きな課題である．

＜金融機関の業務継続態勢整備＞

- 金融機関では，東日本大震災を踏まえた業務継続態勢整備に取り組んでおり，これに対応したシステム監査を実施している．
- 業務継続態勢整備として「バックアップセンターの実効性向上」「通信手段の整備」「電力調達手段の整備」等の取り組みを行っている．

＜リスク評価の監査＞

- BCP,IT-BCP においてリスク評価とそれに対する整備（対策内容）が，企業存続の観点から適切であるかどうかを監査することになる．リスク評価に絶対値というものはなく，事業特性や経営者の覚悟なども加味された会社側のリスク評価を監査人がどこまで評価するのか，することができるのか，監査人の力量が問われる．

＜システム監査による IT レジリエンス向上＞

- システム監査で，IT レジリエンスをこれまでよりもワンランク上げる取り組みにつなげるようにできるとよい．

3．西日本支部合同研究会での北信越支部報告テーマ

意見交換の結果，事業継続計画の課題については切り口が多岐にわたるため，報告テーマはスコープを絞って行うこととしました．北信越支部には金融機関のシステム監査に関係する会員が多いことからスコープを金融機関とし，支部会員から情報を収集し報告することになりました．

・報告テーマ：「金融機関におけるコンティンジェンシープラン策定整備とそのシステム監査」

・報告者　：宮本　茂明

以上

＜目次＞

2014.10

中部/北信越支部　JISTA 中部支部　【合同セミナー(危険予知訓練)】の報告

会員番号　1711　澤田　裕也

１．はじめに

SAAJ中部/北信越支部、JISTA中部支部合同で実施しているセミナーも今年で3年目を迎えた。主催は持ち回りで今年はJISTA中部支部である。私はJISTA中部会員でもあり、セミナー事務局を務めさせていただいた。

２．合同セミナー(開催まで)

4月のJISTA例会で企業システム戦略研究会の青島弘幸さんに「危険予知訓練セミナー」の紹介をいただいた際に、合同セミナーのテーマとしてSAAJ、JISTA会員にぴったりと考え、講師を依頼した。結果、快く講師を引き受けてくださったので、以下のセミナー趣旨で受講者を募集した。

『昨今の不確実性の高いITプロジェクトを成功裡に進める上で、早い段階からリスク・アセスメント(抽出・分析・評価)した上で、適切な事前・事後対策をとるべく、リスク・マネジメントが重要です。しかし、先々を見通す危険予知能力が無ければ、効果的にリスクを抽出することが困難です。危険感度といっても良いでしょう。当セミナーは、産業界で事故防止対策として実践されている危険予知訓練を、ITプロジェクトに応用し、失敗事例から擬似的に失敗経験を積むことで危険感度を高め、危険予知能力の獲得を目指すものです。』

結果、20名の応募があり、会員の興味の高さが伺えた。

３．合同セミナー(当日)

セミナーは9月6日(土)、7日(日)にハートフルスクエアG(岐阜市)で開催された。当日の概要は以下のとおり。

(1)オリエンテーション

藤田JISTA中部支部長の挨拶、全員の自己紹介でセミナーが始まる。

(2)講義

危険予知訓練について以下を中心に約2時間講義をおこなった。

・ITプロジェクトと危険予知の重要性

・危険予知訓練の実施方法(危険状況の把握、危険の分類、危険度の評価、回避策の検討)

(3)演習

4チームに分かれて問題演習を行った。「効果を測定し、経営貢献」をテーマに「稼動して1年経過した基幹業務システムについて、役員への報告会で情報システム部長が性能/機能面でのアピール、企画部長が確固たる経営基盤を確立することができたといったあいまいな報告をする」状況が提示され、「予知される危険および分類」「回避策」について回答をつくりあげ、発表した。

(4)チームディスカッション、発表

各チームで危険予知訓練に関するテーマを決めてディスカッションした。各チームともに熱い議論が交わされていた。

Aチーム:システム監査/プロジェクト管理に危険予知の視点を取り入れる

→危険予知の見える化が必要。

具体例:危険感度の高い人を見える化、プロジェクトの危険感度を見える化(手戻り工数, 残業時間)、失敗経験を見える化(失敗振り返りの吸い上げ)

Bチーム:リスク管理等における危険予知の活用

リスクアセスメント (環境変化の把握からリスク洗い出し)における、危険予知スキルの必要性について。

Cチーム:システム監査の有効利用に関する危険予知事例の作成

小売店のシステム保守業務を対象とした監査における危険予知事例作成。

Dチーム:プロジェクト管理等における危険予知の有効性をどう理解してもらうか

プロジェクト管理において、なぜ危険と予知される項目の洗い出しをしないか。

プロジェクトの危険予知が評価される仕掛けを経営者と顧客の立場に立って考える。

各チームで3時間程ディスカッションし、結果を発表した。質疑、意見交換は予定時間を越える盛り上がりを見せた。


(5)懇親会

危険予知や北信越/中部のご当地ネタ等で盛り上がった。

(6)鵜飼(オプションツアー)

岐阜市の観光名物である鵜飼をオプションツアーとして設定。雨の心配もあったが、無事決行。風情のある鵜飼を間近で見ることができた。

4．さいごに

参加された方より以下の意見をいただいております。

・講義、演習だけではなく、危険予知をテーマとした議論と成果発表があったのが良かった

・システム提案書の必須項目に「プロジェクト管理上のリスク分析」を追加したい。

・成果発表の中であがっていた発注者、受注者でリスクをシェアするリスクパートナーという考え方は目から鱗であった。

・セミナーで学んだ危険予知を既に自社の業務で実践している。

また、北信越支部の梶川さんよりセミナー参加の報告をいただいたので引き続き紹介します。

短い時間ではありましたが、会員の方には役に立つセミナーが開催できたのではないかと考えております。

講師の青島さん、JISTA中部事務局のみなさん、参加いただいた会員の方にお礼申し上げます。

引き続き会員の方のお役に立てるセミナー等イベントを実施していきたいと考えております。

以上

＜目次＞

2014.10

中部/北信越支部　JISTA 中部支部　【合同セミナー(危険予知訓練)】に参加して

会員番号　0947　梶川　明美

JISTA中部支部様のお世話により開催された「危険予知訓練セミナー」に参加させていただいた。

１．セミナーへの期待

東日本大震災の発生後、危機管理について考えることが格段に増えた。様々な事案発生時にあっても業務継続が可能なように取り組みを進めることは、システム部門として当然のことである。また、組織を構成するメンバーの安全をいかにして守るかということも大切であり、起こり得る危険とその結果の発現態様について想定し、日頃からシミュレーションしておくことが重要である。

この「起こり得る危険とその結果の発現態様」を「あらかじめ想定しておく」というのは、とても難しいことだと思う。大地震発生時、普段はどっしりと鎮座している機器類が突如凶器のごとく動き出す、暗闇で空調パッケージの配管が破れて大量の水が噴き出す、バッテリーが破損して希硫酸が流れ出すなど、非常時に起こり得ることに想いが至らなければメンバーを守れないのではないか。一方メンバーは、起こり得る事象をあらかじめ教えられていれば足りるのかというとそうでもなく、自ら気付いて判断し、自分と仲間の身を守る能力が身に付いていないと十分でないのではないか。そんなことを考えていた時に「危険予知訓練セミナー」の案内があって、これぞ求めるものだと思い、参加させていただくことにした。

２．セミナー内容

先々を見通す危険予知能力が不十分であると、効果的にリスクを抽出することが困難である。100の失敗事例から疑似的に失敗経験を積むことで危険感度を高め、想定外を減らすためのより高度な危険予知能力を獲得できる。これが危険予知の考え方のよりどころであり、腑に落ちて共感できた。

予知した危険状況を様々な観点で分類することは、目から鱗であった。認識的リスク、人的リスク、技術的リスク、組織的リスクなど、分類することで、他の危険予知に取り組んだ場合により多くの気づきを得ることができそうである。分類を完全に頭に入れておくと、危機的状況の中にあっても、素早い状況分析と判断ができると思う。

プロジェクト管理の目標達成では、単に人が減らせたということだけでは固定費(人件費)の削減にならない。別の付加価値の高い仕事に余剰人員を移動するということでなければならない。一般的であいまいな表現から、さらに踏み込んで誰が見ても明瞭な効果を出さなければトップを納得させられないのだと理解した。トップが求めているものはこれだったのだと、改めて気づかせていただいた。

プロジェクト管理だけでなく、今後直面する様々な事柄に、より良く対応できるよう鍛錬したい。

３．鵜飼体験

1日目のセミナー終了後の夜、隣県にいながら体験したことのなかった長良川鵜飼に連れて行っていただいた。午前中早い時間に岐阜に到着し、博物館で鵜飼の歴史などについて基礎知識を入れていたことも幸いし、手配してくださった貸し切りの屋形船を操る船頭さん達のお話しは大変楽しく、篝火の暖かさが伝わる至近距離で幻想的な鵜飼を体験することができた。

４．その他

支部等行事への参加により、出席される会員の皆様からいつも刺激を受けている。また、自らの姿勢のありようについて謙虚に振り返ることのできる良い機会となっている。素晴らしい企画でお世話してくださった中部支部の皆様に、深く感謝申し上げます。どうもありがとうございました。

以上

＜目次＞

2014.10

支部報告　【　システム監査体験セミナー（実践編）開催結果報告　】

会員番号　1709　荒町　弘　（近畿支部）

１．セミナー名称　：　システム監査体験セミナー（実践編）
２．開催日時　　：　２０１４年８月３０日（土）　～　８月３１日（日）
３．開催場所　　：　大阪大学中之島センター　講義室２０１

４．開催概要

近畿支部では、2014 年 8 月 30 日(土)、31 日(日)大阪大学中之島センターを会場として、システム監査体験セミナー(実践編)を開催しました。受講者は 7 名、2 つの監査チームを編成しての実施となりました。

1 日目は 13 時から 19 時、2 日目は 10 時から 17 時までの 2 日間コースで実施しました。IT 系の建設業や情報通信サービス業などを手掛ける企業を事例とし、「情報システムの現場業務に対する適合度」について外部監査を行い、監査報告では課題および課題解決に向けた方向性を示すという流れでロールプレイを交えながら実施しました。

(1) 講義 ＆ トップインタビュー

最初にコース内容およびシステム監査の実施手順について説明。監査対象企業であるg社の組織の確認をはじめ、社内の情報システム概要や「基幹システムの概要と関連業務の流れ」や「ICT中期計画」等について確認した。その後、受講者はチーム作業を開始し、トップインタビューの準備に入りました。

(2) 予備調査 ＆ 監査個別計画作成

トップインタビューでは、インタビューの目的を的確に伝え、g社が外部監査を依頼した目的のヒアリング、g社の事業展開や外部環境変化、情報システムの役割と今後の期待などについて詳細なヒアリングが実施された。また、従業員アンケートによる情報システムの現場業務への適合度に関する調査結果も踏まえて予備調査の準備が進められました。

情報システム本部長と営業部長向けに20分のインタビューを実施し、その結果を踏まえて監査個別計画書の作成を行い、チームごとに内容を発表していただき1日目のカリキュラムは終了しました。

(3) 本調査 ＆ 監査報告

2 日目は、本セミナーのメインとなる本調査を実施しました。受講者は準備した質問項目に従って、監査対象企業の SI サービス事業等を担当する SE および SE マネージャに対する 30 分間のインタビューを実施しました。トップインタビューおよび予備調査で得た内容から検討された質問内容はよく練られており、短い時間の中で簡潔・的確なインタビューが実施されていました。

本調査実施後は、本調査のまとめと監査報告書作成、そして最終的には今回の監査依頼者であるg社の経営者を含めた被監査部門への監査報告会を行いました。被監査部門からの質問に対して、これまでの議論を重ねた内容を背景に適切な回答で対応されていました。

最後に、講師から監査報告書の紹介や解説と受講者との意見交換などを行い一連のカリキュラムは終了となりました。

５．受講者の皆様の感想

受講された皆様からは、以下のようなお声をいただきました。

・机上の勉強を実践で体験できた点において期待通りでした。一方で、事前の知識のレベルが想像以上に高く（講義がほぼ無く）ロープレが開始されました。チームメンバーに恵まれて助かりました。

・チーム作業で、考え方・まとめ方などの手順等が学べて良かったです。

・大変学ぶところの多いセミナーでした。システム業務、システム監査ともに未経験で、事前配布資料を見た時はいったいどうなるのか・・・と心配でしたが、当日は講師の方々、チームメンバーの皆様のおかげで、調査フェーズ、報告書フェーズともやりとげることができました。

・わからないながら、グループの方に助けられて、報告書ができて良かったです。

・2日間盛り沢山の内容であっという間でした。良い研修でした。感謝です。

・テーマが監査として取組むには難しかったと考える。こういうケースで学ぶことも必要であると考えるが、よりベーシックな、基本的なシステム監査について学んだ上でというステップが適切かと思います。

６．感想

今回の監査は、企業合併や事業多角化を進める g 社における現行システムの現場のニーズへの適合性や経営戦略・情報戦略との適合性について診断するという、新システムの企画・計画段階での監査であり、難易度も高く監査人には高い質問力を問われる監査であったと思います。

監査チームの皆様は限られた時間ではありましたが、議論を尽くして一連の監査手続きに臨んでもらいました。受講者の皆様、本当にお疲れ様でした。

以　上

＜目次＞

2014.10

支部報告【　近畿支部　第１４８回定例研究会　】

会員番号 2083 竹下 健一 （近畿支部）

１．テーマ　　ソフトウェア著作権研究プロジェクト中間報告

２．講師　　大阪成蹊大学名誉教授　松田 貴典 氏

京都聖母女学院短期大学 生活科学科 准教授　荒牧 裕一氏

３．開催日時　　２０１４年９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

講演１　「情報通信技術関係者が知るべき著作権の基礎」

ICT（情報通信技術）が一般社会や企業のなかで深化し、ソフトウェアや情報システムの著作権に関連するコンプライアンス問題は深刻な事態になってきている。近年、ソフトウェアの不正コピーや他人の著作物の無断HP掲載、ソフトウェア開発委託と保守問題など、ICTに関連した事件や訴訟が多発している。このような状況の下で、昨年度より始まった「ソフトウェア著作権研究プロジェクト」の中間報告に併せて、その前提知識としてシステム監査人（広く情報通信に携わる技術者）が知るべき著作権の基礎について説明された。

講演は、「知的財産権と著作権」、「著作物と著作権」、「著作者の権利」など、著作権に関わる一通りの基礎知識

を詳しくご解説された後、システム監査を行うにあたってのソフトウェアの著作権に関わることの説明があった。

（1）プログラムの著作権

・著作権法は1985年に大きく改正され、プログラムが著作権で保護されるようになった。

①プログラムを著作物として明文化。

②著作者には、一身専属性である著作者人格権が付与されることになった。著作者人格権には、公表権、氏名表示権、同一性保持権がある。

③プログラムの創作年月日の登録制ができた。

・「法人等の発意に基づきその法人等の業務に従事する者が職務上作成するプログラムの著作者」を原則として人（法人著作、職務著作）とした。

・ソフトウェアのバージョンアップ、プログラムバグ（間違いや誤り）等によりプログラムの変更や改変が必要となる。著作権法第20条第2項第3号ではプログラムに対する特例として、「特定の電子計算機においては利用し得ないプログラムの著作物を当該電子計算機において利用し得るようにするため」の必要な改変と「電子計算機においてより効果的に利用し得るようにするため」の必要な改変については同一性保持権の侵害にならないとした。

（2）データベースの著作権

・データベースに関する著作権改正は 1986 年に一部実施され、1987 年 1 月 1 日に施行された。

・改正法では、データベースを「論文、数値、図形その他の情報の集合物であって、それらの情報を、電子計算機を用いて検索できるように体系的に構成したものをいう」と定義するとともに、編集著作物とは別に、「データベースでその情報の選択又は体系的な構成によって創作性を有するもの」は、著作物として保護されることになった。

（3）プログラム著作物の登録

・1985年の著作権法の一部改正で、プログラムの著作物の創作年月日の登録制度が設けられた。

・著作権や著作隣接権の譲渡、担保権の設定、出版権の設定には登録をしなければ第三者に対抗することはできない。しかし、現実には、著作権の登録なしに当事者間において、著作権等の譲渡、移転等が行われているわけであり、第三者との関係で対抗要件として登録しておかなければならない。

・登録できるものとしては次のとおりである。① 実名の登録、②第一発行年月日の登録、③創作年月日の登録、④著作権・著作隣接権等の移転等の登録、⑤出版権の設定等の登録。

講演２　「ソフトウェア著作権監査のための各種ツールの提案」

ソフトウェア著作権研究プロジェクトでは、まずソフトウェア著作権をタイプ別に分類し「ソフトウェア著作権チェックリスト」としてまとめた。そして、管理に不可欠な「ソフトウェア管理台帳」の標準化作業を行うとともに、被監査企業の管理水準の目安となる「ソフトウェア著作権管理の成熟度モデル」を作成した。プロジェクトの成果物として、これらのツールの概要の説明をうけた。

（1）プロジェクト発足の経緯と活動状況

・プロジェクト期間　2013年4月～2015年3月（2年間）。

・コンプライアンスのシステム監査（CP 研）の成果を受け、分野別により深い研究の必要性を認識。

・「ソフトウェア著作権」を対象に選んだ理由は、①昔（1970 年）から存在し頻繁に改正がある、②どの企業（業種）で

も共通して問題になる、③違反には刑事罰がありリスクが高い、④内容が複雑で共同研究に適している。

・成果物として以下の3点を作成している。

①「システム監査チェックリスト（ソフトウェア著作権）」

②「ソフトウェア管理台帳」

③「ソフトウェア著作権管理の成熟度モデル」

（２）システム監査チェックリスト（ソフトウェア著作権）

・ソフトウェア著作権に関する注意事項を導入形態別（譲渡契約、ライセンス契約など8形態）に分類。

・特に、委託開発を中心に検討している。

・今年度後半は、「監査の進め方」に関する注意事項をまとめる。

（３）ソフトウェア管理台帳

・SAMユーザーズガイドにおける台帳の項目をたたき台とし、必要な項目を追加している。

・SAMユーザーズガイドは購入を対象としているので、委託開発の場合に必要な項目を検討する。

・関連台帳について

－委託開発の場合、「ライセンス管理台帳」は分けなくても良い。

－委託開発、購入ともに、「関連部材台帳」はソフトウェア管理台帳の該当欄で管理可能である。

（４）ソフトウェア著作権管理の成熟モデル

・ソフトウェア著作権の管理レベルを0～5の6段階に分類（表現はSAMユーザーズガイドに合わせた）。

管理レベル0 ： 管理が存在しない段階

管理レベル1 ： 初期・場当たり的な段階

管理レベル2 ： 反復可能な段階

管理レベル3 ： 定義されている段階

管理レベル4 ： 管理されている段階

管理レベル5 ： 最適されている段階

・それぞれの段階において可能な監査の種類を提示した。

・予備調査の段階で管理レベルについての評価を行う必要がある。

６．所感

最初に松田先生から著作権の基礎内容の解説とソフトウェア著作権におけるポイントを説明されたことで、前提の知識の整理ができ、ソフトウェア著作権研究プロジェクトの中間報告を聴講することができた。研究プロジェクトの成果物である「システム監査チェックリスト（ソフトウェア著作権）」、ソフトウェア管理台帳、ソフトウェア著作権管理の成熟モデルはいずれもシステム監査の現場で実用的に使えるものと感じた。今後さらにブラッシュアップして完成を目指してもらいたい。

以上

＜目次＞

2014.10

注目情報（2014.09～2014.10）※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。

■㈱ベネッセコーポレーション　事故調査委員会報告書の公表（2014/9/25）

㈱ベネッセホールディングスは、㈱ベネッセコーポレーションのお客様情報の漏えいに関して、「個人情報漏えい事故調査委員会」を設置し、事実調査、原因究明および再発防止策の策定に取り組んできたが、このほど報告書を公表した。

PDF は以下のサイトから。

http://blog.benesse.ne.jp/bh/ja/news/m/2014/09/25/docs/20140925%E3%83%AA%E3%83%AA%E3%83%BC%E3%82%B9.pdf?_ga=1.239883456.2135372866.1413294240

経済産業省が、(株)ベネッセコーポレーションに対して個人情報保護法に基づく勧告を行いました。（2014/09/26）

http://www.meti.go.jp/press/2014/09/20140926002/20140926002.html

＜目次＞

2014.10

【　協会主催イベント・セミナーのご案内　】

■月例研究会（東京）

第197回	日時:2014 年 11 月 19 日(水)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	マイナンバーと民間サービスとの連携を目指して
	講師	経済産業省 ＣＩＯ補佐官　満塩 尚史 氏
	講演骨子	平成 28 年度からマイナンバー制度と呼ばれる社会保障・税番号法(「行政手続きにおける特定の個人を識別するための番号の利用等に関する法律」)が利用開始される。このマイナンバー制度では、個人に付与される個人番号(マイナンバー)は、法律で定められた業務以外での利用や他人に提供することはできない。一方、民間サービスにおいても、マイナンバー制度を利用したいという意見もある。前記の通り、個人番号そのものは、利用することはできないが、個人番号を使わないで、ID 連携トラストフレームワークを活用し、民間サービスとマイナンバー制度を連携させ、利活用できる可能性がある。 また、社会保障・税番号制度では、個人に個人番号を付与するだけでなく、法人や行政機関に法人番号を付与し、インターネット経由で法人番号、法人名、本社所在地が、提供される。 ここでは、マイナンバー制度の概要と、マイナンバーを民間サービスで利活用する仕組みとしての ID 連携トラストフレームワークをご紹介します。更には、法人番号の民間利活用に関する期待についてもご紹介します。 《参考ウェブサイト》 ・社会保障・税番号制度のホームページ http://www.cas.go.jp/jp/seisaku/bangoseido/index.html ・新戦略推進専門調査会のマイナンバー等分科会開催状況 http://www.kantei.go.jp/jp/singi/it2/senmon_bunka/number.html ・ID 連携トラストフレームワーク http://www.meti.go.jp/policy/it_policy/id_renkei/
	お申し込み	詳細確定次第、HPでご案内いたします。

■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.saaj.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)

■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.saaj.or.jp/topics/hukyuservice.html ）
お問合わせ		システム監査事例研究会主査　大西（Email： jireiken@saaj.jp ）

【　外部のイベント・セミナーのご案内（会報担当収集分）】

■システム監査学会（JSSA）

第 27 回公開シンポジウムのご案内	
日時	2014 年 10 月 31 日（金） 10:00～16:50
場所	機械振興会館ホール （東京都港区芝公園 3-5-8　地下2階）
テーマ	『安心安全な社会生活とシステム監査』
概要	今日、われわれの社会生活はICTをベースに多種多様なインフラに支えられています。特に、技術的に著しい発展を遂げ、われわれの社会生活に深く入り込んでいるIOT（Internet of Things）およびSNS（Social Network Service）は、安心安全な社会生活に大きな影響を与えつつあります。 今回のシンポジウムは、このような社会環境で「安心安全な社会生活とシステム監査」を統一論題としています。この論題のもとにシステム監査および統制はどうあるべきかについて、各分野でご活躍されている専門家をお招きし、実践的な社会の安心と安全を確保する観点からご講演いただき、議論を深める場を提供させていただきたいと思います。 本学会会員ならびにシステム監査、情報セキュリティ、情報ソリューション、リスクマネジメント、BCP/BCMS 等に携わっている関係各方面の方々のご参加をお待ちしております。
プログラム等	http://www.sysaudit.gr.jp/sympo/27_symposium.html

＜目次＞

2014.10

協会からのおしらせ　【年会費納付時期について 】

会員番号　1760 斎藤由紀子 （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.saaj.or.jp/toiawase/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ヨウカイ

※銀行振込の際は、≪会員№≫4桁の数字を氏名の前に付けて下さいます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の提供＞

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.saaj.or.jp/toiawase/index.html　（事務局）

＜目次＞

2014.10

Welcome

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.saaj.or.jp/index.html
・会員規程にも目を通しておいてください。 http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・皆様の情報の変更方法です。 http://www.saaj.or.jp/members/henkou.html

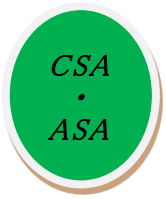
・会員割引や各種ご案内、優遇などがあります。 http://www.saaj.or.jp/nyukai/index.html
　セミナーやイベント等の開催の都度ご案内しているものもあります。

・各支部・各部会・各研究会等の活動です。 http://www.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.saaj.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.saaj.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.saaj.or.jp/csa/index.html

・PDF会報と電子版会報があります。（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

・右ページをご覧ください。 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＞

2014.10

【　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
4 月	1 日　認定 NPO 法人申請準備開始	認定委員会:新規 CSA/ASA 書類審査 25 日　第 190 回月例研究会	20 日　2014 年春期情報技術者試験(9:30～16:30)
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
11 月	13 日　理事会 13 日　予算申請提出依頼(11/30〆切) 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 30 日　2015 年度年会費請求書発送準備	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　支部会計報告依頼　(1/9〆切) 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	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	
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〕	9 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　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		

※注　定例行事予定の一部は省略。

＜目次＞

2014.10

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、「○○○のためのシステム監査」とし、四半期ごとに「○○○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」をテーマとすることとしました。情報システム部門を取り巻く方々に向けてのシステム監査について、皆様から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、投稿ボラ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くことがあります。

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ー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/toiawase/

■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/

■□■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＞