特定非営利活動法人
日本システム監査人協会報

2013年8月号
No 149

No. 149（2013年8月号）＜7月20日発行＞

早めの梅雨明け、猛暑・・・
夏バテで体調を崩していませんか？

今月号も、ためになる情報満載です。
ご一読ください！

2013.07 投稿

めだか　【　システム監査の使いみち（ガバナンス）　】

ガバナンスやITガバナンスという言葉がシステム監査の話題としてよく言われている。そこで、ガバナンスやITガバナンスに関して、システム監査の使いみちを考えてみたい。

「おどろきの中国」という本を読むと、ガバナンスの欠如が組織体に最悪の結末を導いた事例がある。昭和の時代、満州において、日本の関東軍（もともと遼東半島と南満州鉄道の付属地の警備を担当する部隊の名称）の一部の軍人による満州を手に入れようとした陰謀があり、それを政府や、陸軍首脳に相談なしで実行したという張作霖爆殺事件（1928年）があった。その後、満州事変（1931年）が起きたが、これは、周到に準備された関東軍の組織的な作戦行動で、柳条湖で鉄道が爆破された（日本軍の自作自演）のを口実に、関東軍が満州全域を制圧したという事変である。以降、国際連盟脱退、日中戦争、太平洋戦争と続いて、その結末は、日本の敗戦である。

組織体の一部が、組織体の意志にないことを実行することは、組織体のガバナンスの欠如といえる。組織体のガバナンスが有効であれば、組織体の一部が組織体の意志に違反した行動をとれないはずである。組織体のガバナンスを有効にする方法のひとつとして、定款、内部統制、内部監査などがある。組織体のITガバナンスとなると、組織体のガバナンスのうちITにかかわるものだろう。ITは、Information Technologyの略語で、米国では略して、「Technology」と言うようだ。ITガバナンスは、近々、ISO 38500をJIS化して日本語化されると聞いている。

組織体が、ITを利用する際に心得ておくべきことで、情報システム全般にかかわることは、「システム管理基準」として公表されている。これは、今から9年前、平成16年10月8日に策定されたものであるが、基本形といえる。

「システム管理基準」では、**“システム監査の実施は、組織体のITガバナンスの実現に寄与することができ、利害関係者に対する説明責任を果たすことにつながる。”** としている。

また、“時々の関連技術動向、関連法令、及び社会規範などを考慮し、それらを反映した詳細なサブコントロール項目を策定することが望ましい。”としている。それを受けて、平成19年3月30日に、「システム管理基準追補版（財務報告に係るIT統制ガイダンス）」が公表されている。当協会の個人情報保護監査研究会では、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　追補版（個人情報システムに係るIT統制ガイダンス）」を策定し、普及を図っている。

情報処理技術者試験に、「システム監査技術者試験（レベル4）シラバスー情報処理技術者試験における知識・技能の細目ー」があり、平成24年5月に、Ver2.0 が公表されている。これは、システム監査人が監査で取り扱う細目を、情報処理技術者試験における知識・技能の視点から、説明していると言える。

（空心菜）

参考:「おどろきの中国」 橋爪大三郎・大澤真幸・宮台真司　著　講談社現代新書

（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。）

2013.7 投稿

めだか 【 業界用語や輪切りの駆逐 】　（システム監査の使いみち：投稿）

今月からの会報テーマ「システム監査の使いみち」に接して、筆者は方法論や処方箋としての使いみちではなく、使いみちをどのように表現すべきか、どのように伝えるべきか、ということを先ずイメージした。

システム監査の使いみちについて、システム監査人はその知見・経験・関連情報をもとにしてスラスラとよどみなく述べることができるだろう。熱弁や力強く語ることも多いと思う。一方で、それを語る場合の用語や表現方法はどのようなものだろうか。システム監査の定義用語や基準・ガイドラインの項目名のオンパレードになっていないだろうか。

先月号で筆者は「So What」というタイトルで、システム監査が如何に役立つか発信、もっと分かり易く伝える、平たく語るなどの重要性について述べた。これは「システム監査活性化への提言」というテーマを受けてであったが、今月のテーマ「使いみち」にも大いに通じるところがあるので、さらに新たな視点で考える。それは業界用語や輪切りの駆逐だ。

【業界用語】 システム監査の使いみちを語るとき、監査用語、基準の名称、点検項目名などの多用は避けなければならない。要するに業界用語だからだ。特定分野の専門用語を用いた説明は利用者に理解されずに拒絶反応を植え付けてしまいかねない。勘違いや行き違いを生むもとにもなる。自分たちの説明のし易さなどから安易な業界用語への依存をやめる必要がある。専門用語は我々システム監査人の範囲にとどめて、利用者に対しては利用者目線の言い方をする必要がある。

例えば、「①有効性⇔効率性」と「②信頼性⇔安全性」について、左辺/右辺の使い分けを我々の認識だけで安易に用いてはいないだろうか？　左辺/右辺の違いを得心してもらえる説明方法や用例を持ち合わせているだろうか？　左辺/右辺の意味合いを利用者に補足説明しつつ用いているだろうか？

その他にも何気なく用いてもさほど問題ないだろうと、たかをくくって説明している場合もあるかも知れない。例えば、「③監査目的と監査テーマ」、「④監査対象と監査範囲」、「⑤監査項目と監査要点」、「⑥セキュリティポリシーとセキュリティスタンダード」など。

【輪切り】 使いみちの重要なもう1点はタスク分けだ。タスク分けとは筆者の表現だが、ビジネスプロセスに適した監査の使いみちのことをいう。つまり、どの業務を監査するかというときに、我々はともすると、開発だ、運用だ、外部委託管理だ、データ管理だなどと基準やガイドラインの項目建てを念頭においてしまう傾向がある。現実の職場はそのような部品の集合体ではなく、複合的・重層的に絡み合った仕事であると分かっていても監査人の思考回路が利用者ニーズに適さなくなっている例かも知れない。

タスク分けは、例えればチーズ棒を輪切りにするのではなく縦に裂いた状態のように、ビジネスプロセスの一連の過程に対するシステム監査の使いみちのことで、このような利用者視点の使いみちを提案する力や説明方法が求められていると思う。

使いみちはすでにある。見せていないか、霧があるか、どちらかだ。

（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。 ）

2013.07 投稿

めだか【「報告」目的が拡大された新COSO内部統制フレームワーク（システム監査の使いみち）】

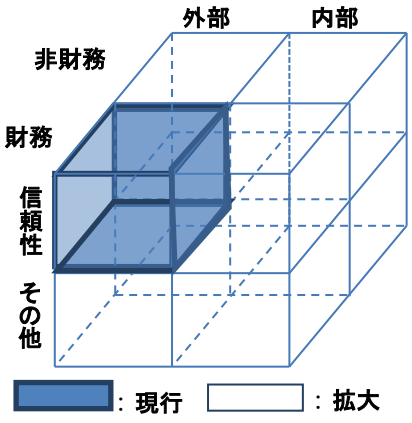
2010年11月から始まったCOSOの「内部統制の統合的枠組み」（通称：COSO内部統制フレームワーク）見直しプロジェクトは、3年に亘る作業を終え、本年5月14日に改訂「内部統制の統合的枠組み」（以下、「新COSOレポート」）を公表した。

平成18年6月に金融商品取引法が成立し、平成20年4月以降開始の事業年度から適用が開始された日本の内部統制報告制度に大きく影響を与え、関係者が挙（こぞ）って勉強した、あの「内部統制」のデファクトスタンダードの改訂である。

新COSOレポートの詳細、及び我々への影響は、まずは今後の専門家の解説に譲るとして、ここでは特に私が改訂の大きなポイントと考える、「報告」目的の拡大を取上げ、今月からのめだかテーマ「システム監査の使いみち」の視点で少し考えてみたい。

ご承知の通り、COSO内部統制フレームワークでは、内部統制を、①「業務の有効性・効率性」、②「財務報告の信頼性」、③「関連法規の遵守」の3つの目的の達成に合理的な保証を提供することを意図し組織構成員により遂行されるプロセスとしていた。しかし、新COSOレポートでは、この②「財務報告の信頼性」を、単に「報告」と変更している。そして識者はその意図を、社会で重要性が増している非財務情報の報告や、信頼性に限らない多くの観点からの報告、そして外部報告だけでなく内部報告をも含む幅広い「報告」にその目的を拡大したものと解説している。

「報告」目的の拡大



確かに、内部統制を「自己管理の仕組み」と捉えている私としては、内部統制のデファクトスタンダード（COSO内部統制フレームワーク）では「財務報告の信頼性」と、報告を限定的に捉えている点に少し違和感があった。これは、主として長い会計監査（財務諸表監査）の歴史の中で内部統制が議論されてきたことが背景にあったと察するが、今回の改訂で、その違和感が払拭され、社会の実態により合った「内部統制」の枠組みに更に近づいたと評価したい。

そこで、システム監査の一層の普及・促進への思いを込めて、めだかテーマ「システム監査の使いみち」の視点からこの点を捉えると、内部統制の「報告」目的が“財務諸表の信頼性”に限定されず、幅広い「報告」になったことは、その中に情報社会の中で注目される組織の情報システムに関する報告も含まれることになり、内部視点では、情報システムに関する「報告」目的を合理的に支える、内部統制の構成要素の一つであるモニタリング活動の中でシステム監査の役割（使いみち）が高まる可能性が期待でき、また、外部視点では、内部統制で支えられる、組織の情報システムに関する「報告」に信頼性を付与するシステム監査の活用、利用が高まる可能性も見込まれると考えるのは深読みし過ぎであろうか。そこまで言わないまでも、これまでのシステム監査の本質が変わるわけではないが、新COSOレポートによって、内部統制のフレームワークの中で、「報告」目的の観点からは、システム監査がより合理的に位置づけられる（据わりがよくなる）と思えるのだが如何だろうか。

（広太雄志）

（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。）

2013.07 投稿

投稿 【 システム監査の活性化（定款） 】

会員番号 0557 仲　厚吉（システム監査活性化プロジェクト）

当協会の事業活動は、全て定款をもとに行われています。システム監査の活性化にあたって、定款の定める、目的、事業、事業の種類を、あらためて認識することは、協会活動の基本を知ることだと思います。定款第3条で、当協会は、システム監査を社会一般に普及せしめると共に、システム監査人の育成、認定、監査技法の維持・向上をはかり、よって、健全な情報化社会の発展に寄与することを目的とするとしています。

当協会は、システム監査を社会一般に普及せしめる等のため、定款第4条の、(1) 社会教育の推進を図る活動、(2) 国際協力の活動、(3) 前各号に掲げる活動を行う団体の運営などを、事業活動としています。具体的には、定款第5条に事業の種類を定めていて、実際に、会報・ホームページ・メール、部会・研究会、システム監査人の育成、公認システム監査人等の認定、支部における活動などの事業を行っています。

システム監査の活性化を図るためには、先ず、協会活動の基本を知り、次に、現在の社会や経済の状況、技術の進歩を認識して事業活動を行い、外部の期待を喚起してそれに応えていくこと、そして他団体との連携を強化していくことが重要であると思います。

システム監査活性化プロジェクトでは、会員、部会・研究会、委員会、CSA利用推進、支部の皆さんへ活性化プロジェクトへのご協力を呼びかけています。システム監査活性化プロジェクトのメンバーとして、システム監査の活性化に力を尽くしたいと思います。

（目的）
第3条　本法人は、システム監査を社会一般に普及せしめると共に、システム監査人の育成、認定、監査技法の維持・向上をはかり、よって、健全な情報化社会の発展に寄与することを目的とする。
（事業）
第4条　本法人は、前条の目的を達成するため、次の種類の特定非営利活動を行う。
(1) 社会教育の推進を図る活動
(2) 国際協力の活動
(3) 前各号に掲げる活動を行う団体の運営又は活動に関する連絡、助言又は援助の活動
（事業の種類）
第5条　本法人は、第3条の目的を達成するため、特定非営利活動に係る事業として、次の事業を行う。
(1) システム監査に関する啓発・広報活動
(2) システム監査の事例・技法等に関する調査・研究
(3) システム監査に関する研究会・講習会の開催と援助
(4) システム監査人の養成及び継続育成教育
(5) システム監査人の認定制度の運営
(6) システム監査人行動基準・倫理規定の策定と維持
(7) その他、本法人の目的を達成するために必要な事項

以上

2013.07 投稿

時事論評 【 ミリタリーIT パラドックス 】

会員番号 0707、神尾博(クボタシステム開発株式会社勤務)

１．ミリタリーIT を知ろう

東シナ海や朝鮮半島での国際緊張の高まりにより、今年に入って我が国の国防関係の話題が、以前より頻繁にマスコミで取り上げられるようになった。例えば中国軍の FCS（Fire Control System）レーダー照射事件や、国内米軍基地へ配置されたオスプレイの訓練飛行状況等である。

システム監査人は国防関係では、政治的、政策的な場所からは距離を置きながらも、ミリタリー技術、特に IT 関連の技術動向を知っておいた方が良いというのが、以前からの私の持論である。理由としては①近年は軍事や兵器のハイテク化、IT 化が目覚ましい②新技術は軍事から民生へ展開・普及することが多い（これは最近では少し事情が違う＝後述）③ミリタリーIT は、計算・通信・制御技術等の融合の集大成であるといった点が挙げられる。そこで誌面をお借りして、諸氏にいくつかのミリタリーIT の意外性の話題について、システム監査的視点からの考察を紹介しよう。

２．COTS（Commercial　Off　The　Shelf）パラドックス

IT 関係者へは今さら改めて申し上げる必要も無いが、元々、コンピュータは大陸間弾道弾の軌道計算を目的として開発されたものである。さらにはレーダー、GPS、そして最近ではロジスティクスに使用される RFID（Radio Frequency IDentification）等、IT 分野でも軍用から民生への展開（スピンオフ）は枚挙に暇がない。防衛という国策のためなら、最新技術への莫大な開発費の投入が可能だからだ。

ところが一方では、急速に COTS と呼ばれる民生品の利用（スピンオン）が進んでいる。例を挙げると Panasonic のタフブック、Windows、Linux、SAP、OracleDB、ActiveDirectory、TCP/IP である。背景には兵装の急速な IT 化がある。コンピュータや通信は、ムーアの法則に基づき民生品の性能向上のスピードが早い。兵器では、機構部はそのままで IT 部分のみ性能向上を行う場合も多いため、オープンアーキテクチャでないと、サポート切れ製品の換装やグレードアップがやりにくいといった事情からも COTS 化に拍車をかけているという。このライフサイクルや将来のシステム拡張は、システム管理基準でも言及されている。

COTS 化が進み、民生品として輸出された製品の軍事転用といった事態も生じている。ゲーム機のコントローラが、地雷処理機材に利用されたという例もある。システム管理基準にも情報化投資の効果や法令の順守に関する項目があるが、この分野では両立は難しそうだ。

３．CI（Cyber　Infrastructure）パラドックス

IT セキュリティの専門家なら、ご存知の方も多いだろう。電気、ガス、水道、交通機関等の、国民生活に直結した重要インフラにおける、制御システムのネットワーク化が最も遅れている国が、サイバー戦争での防衛面（攻撃面ではない）で有利という、いわゆる「サイバー攻撃の非対称性」である。一見、ネットワークインフラが充実している国家の方が、情報戦略等での圧倒的な優位性を持つような印象を受ける。しかし

実情は、国内に守るべき対象を持たない方が、防御のための余分な設備やマンパワーを裂かないで済むといった効果が、凌駕しているのである。

ちなみに制御系への攻撃の歴史は意外に古く、1980 年代には CIA がカナダと共謀し、旧ソ連へ納入したポンプとバルブの制御装置に不正コードを仕組み、パイプラインを爆発させたという実績がある。また米軍とイスラエル軍がイランの核開発施設へ仕掛けた Stuxnet は有名だが、一方で米国の電力網からは論理爆弾（ロジック・ボム）が次々と発見されているという。

なおこの非対称性という言葉そのものは決して真新しい概念ではない。そもそも大国へのテロやゲリラ戦も該当するし、20 世紀の終盤には米国の政府機関において、早くも重要インフラへのテロ攻撃の危惧について言及されている。ただしこの時点では通信ケーブルや制御設備への物理的攻撃を中心に考えられていたようだ。システム監査では情報システムの「安全性」に該当するだろう。

４．UAV（Unmanned　Aerial　Vehicle）パラドックス

だからといって先進国は軍事において全てが不利というわけではない。ハイテク兵器による逆方向の非対称性も存在する。9.11 同時多発テロを契機に、米軍はアフガンにプレデター等の UAV（無人航空機）投入を強化し、米国本土からの通信衛星を経由した遠隔操作で武装集団への攻撃を続けている。そして一方のアフガンゲリラは、手製爆弾を抱いた自爆テロや旧式の銃器で応戦するという図式となっている。そうなった理由はシステム監査で言われる「効率性」である。軍用パイロット 1 人養成には 3～5 年、約 6 億円がかかるそうだ。プレデターの方は 1 機が約 20 億円、ただし遠隔操縦施設も必要になる。対して貧しい国では、調達に技術やコストがかからない手段を選択せざるを得ない。それに人命、特に少年兵の命が含まれていることは痛ましい限りだ。

システム管理基準には人的資源管理の項目がある。軍人、特に兵士というと筋肉隆々の体育会系を連想する方も多いだろうが、こうした UAV の登場によって先進国では、配属場所によってはゲーマー的なセンスの持ち主の方が圧倒的に高パフォーマンスということも、あり得る状況になった。

また新規なシステムの形態として、好むと好まざるとに係わらず、同盟国へのクラウドサービス「WaaS（Weapon as a Service）」も技術的には十分可能な時代になり、まさに「Wars is Waas」が実現するかもしれないことも指摘しておこう。

５．VTOL（Vertical Take-Off and Landing）パラドックス

代表的な VTOL（垂直離着陸機）であるオスプレイは、エンジン&プロペラ部全体が傾くというティルトロータ機構等、非常に複雑な構造を持つ。すなわち空気力学的に飛行に適していない形状のものを、コンピュータ制御で無理矢理に飛ばしているというのが実情だ。制御コンピュータは、センサ等の情報を収集し、エルロン、ラダー、エレベータ等で機体の方向や傾きを調整したりエンジンを駆動したりして、最適と判断した状態へと導く。その処理すべき情報量が毎秒何万といったスケールのため、人為的ミスや強風等の外乱には弱いという宿命を持たざるを得ない。システム監査では「信頼性」に該当する問題だ。

ここはひとつ、わが国の水道橋重工プロジェクトの高さ 4m の搭乗型ロボット「KURATAS（クラタス）」の操作用ソフトウェア「V-Sido（ブシドー）」に注目したい。機体の各パーツとシミュレータのリアルタイ

ムでの同期等により、突風等の環境や急変する現象にスムーズに対応できるという。ソフトウェアは物理モデルが同一であればサイズを問わないというから、プラモ並みの実験機でもデバグが可能になる。

また 10 年以上も前には相次ぐ民間航空機事故を受けて、ソースコードを公開すればバグの発見やユーザインタフェースの改善によって、事故の減少につながるといった意見もあった。しかしながら軍用機では軍事機密、また時代が変わり民間機においてもサイバーテロ対策のため、ソースコード開示は否定的な情勢であり、こうした安全へのアプローチは事実上塞がれてしまっている。

６．もっとミリタリーIT を知ろう

目まぐるしく戦争の形態は変革している。斬新なコンセプトの兵器も目白押しだ。人間の頭蓋内にパルス波や不可聴音を直接照射し、潜在意識にダメージを与える脳内音声兵器が実用段階まで進んでいる。クラゲやハエをモチーフにした生物型ロボットは、偵察・諜報用途に開発中だ。

指揮所や戦闘機等のデータリンクが進み「ネットワーク中心戦」と呼ばれている。状況を認識し利用する手段は、C4ISR（指揮・統制・通信・コンピュータ・情報・監視・偵察）と呼ばれる諸機能の融合体である。そして交戦では、センサからの入力データをコンピュータで自動判定し、シューターを作動させる。サプライチェーン等の一般ビジネスでの情報管理は「need to know」が主流だが、一瞬の意思決定で勝敗の帰趨が決まるミリタリーでは、キル・チェーンの短縮のため「 need to share」へと変質してきている。

イスラエルは、先に述べた通り米国とともに Stuxnet を画策するほどの、極めて優秀な国民性であり、徴兵制では理工系の学生はサイバー軍へ行くという。徴兵制というと、泥水の中の匍匐、炎天下や雪山の行軍しか連想できないのは、もはや化石人間だ。このように利用分野に拘わらず、常に新しい IT 技術の動向に注目しておかなければ本質を見失うことは、システム監査人として心に留めておくべきであろう。

なお最後に、本稿作成に際してレビュー頂いた安本哲之助氏、田淵隆明氏に対し、この場を借りて御礼を申し上げる次第である。

以上

新たに会員になられた方々へ

Welcome

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。

ご確認ください

・協会活動全般がご覧いただけます。 http://www.saaj.or.jp/annai/index.html
・会員規定にも目を通しておいてください。 http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・みなさまの情報の変更方法です。 http://www.saaj.or.jp/members/henkou.html

特典

・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。

ぜひ参加を

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

ご意見募集中

・みなさま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。

出版物

・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

・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。

CSA・ASA

・公認システム監査人へのSTEP-UPを支援します。
　「公認システム監査人」 と「システム監査人補」で構成されています。
　監査実務の習得支援や継続教育メニューも豊富です。
　CSAサイトで詳細確認ができます。 http://www.saaj.or.jp/csa/index.html

会報

・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

お問い合わせ

・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。

沼野会長からの一行メッセージ
“会員の総力を結集してシステム監査活性化を！”

2013.07 投稿

会長コラム 【 システム監査活性化施策の立案、展開を会員の総力で 】

会員番号 0841 沼野伸生(会長)

2013年度の総会後初の理事会（3月）では、総会で承認頂いた計画を基に、2012年度の“守り中心の活動”（まずは衰えた会勢の挽回を）の成果も踏まえ、2013年度は“守りながら必要な攻めの施策展開”をとし、具体的には、「会員増強PT」をシステム監査の活性化を強力に推進する協会内の母体（「システム監査活性化PT」と後に改称）に衣替えし、予算措置した政策予備費も活用し一層積極的な施策展開を図ることを決めました。（2013.4 号の会報（「会長コラム」）でも報告。）

その後、「システム監査活性化PT」（リーダ：小野副会長）は、協会内各部会、研究会、委員会等を協力にリードし、精力的な検討、活動を重ねています。

例えば、上期の各研究会、部会等の主な動きのポイントは以下の通りです。

（毎月発行される会報でPT、及び各部会等の活動経過が詳しく報告されています。）

・事例研究会：実務セミナー、課題解決セミナー、白熱教室、WSS試行先募集対応などを計画的に推進。

・月例研究会：友好団体を通して参加者募集案内を拡大。例えば、7月開催の月例研究会は6月中に190人超の申込みがあり、早々に申込みを締切ることも検討する状況。

・会報部会：プレゼンツール Prezi を導入し、会報の一層の読み易さ、及び訴求力向上にも着手。

・個人情報保護研究会：「PMS 構築ハンドブック」簡易版の会報掲載、HPでの公表を開始。

・法人部会：システム監査導入実態調査の実施検討に着手。

・CSA・ASA利用促進G：6月に初めて「CSA・ASA全体交流会」を東京で開催。

・CSA・ASA認定委員会：昨年度は実施しなかった継続教育セミナーを6月に東京で開催。　など

しかし、限られた理事がボランティア精神で知恵を絞って検討・実施する施策だけでは自ずと限界があるのも事実です。一方、情報社会の進展と相俟って、これからの安全・安心そして快適な社会の発展にはシステム監査がもっともっとその役割を果たしていく必要があることも事実です。

そこで、今期の政策予備費の活用も視野に、「システム監査活性化PT」には、PTメンバーだけでなく、再度協会内の支部も含めた全ての組織に、また更に、当協会会員の一人ひとりにもシステム監査活性化を自分の問題、テーマとして捉え検討、提案して頂く機会を作ってもらうことについて検討をお願いしています。そこで提案された施策は「システム監査活性化PT」で検討した上で、いくつかについて、提案者と「システム監査活性化PT」が協力してその実現を図っていくことを想定しています。

「システム監査活性化PT」での検討結果にもよりますが、近々、「システム監査活性化PT」から会員の皆様に具体的依頼、案内が発せられるのではと思います。

その際には、是非、会員の皆様のご理解、ご協力、具体的提案をお願いしたいと思います。

現役員体制での協会運営も残すところ半年を切りました。

会員の総力を結集してシステム監査活性化を更に強力に進める新たな具体策を定め、実施に着手し、新たなメンバーも加わる次の役員体制でその実現を確実にし、システム監査普及という当協会の役割を引続き着実に果たしていかなければならないと思っています。　以上

2013.07 投稿

協会からのお知らせ（システム監査活性化プロジェクト）

会員番号 6027 小野　修一（活性化PT　主査）

今月の会報では、システム監査の活性化につながる活動を行っている当協会の研究会や担当組織の中から、4つの活動について、ご紹介します。

1. 情報セキュリティ監査研究会

毎月、研究会で勉強・討議している話題の中から、会員の皆様に知っていただきたい、よろしければご一緒に議論に加わっていただきたい情報をご紹介しています。今回は、「ビッグデータにおける個人的な情報の価値」という、まさにホットなテーマで、研究会で参考文献を輪読しながら意見交換を行いましたので、その論点をご紹介します。こうした活動にご関心をおもちの方がいらっしゃいましたら、お気軽にご連絡をください。お待ちしています。

2. 個人情報保護監査研究会

研究会でまとめた『個人情報保護マネジメントシステム実施ハンドブック』簡易版の内容を、毎月の会報で、順次ご紹介をしています。

システム監査人の主要な活動分野の一つである個人情報保護マネジメントシステム（PMS）の構築・評価を行う際の参考にしていただければとの考えで、ご紹介しているものです。なお、このハンドブックをベースにした PMS 構築の実践ノウハウを身に付けていただくセミナーも計画しています。セミナーの実施が決まりましたらご案内しますので、ご参加ください。

3. 法人部会

当協会の会員区分は、個人会員と法人会員に分かれています。法人会員は、企業・団体として会員登録していただくもので、年会費の金額に応じた人数まで、個人会員と同じ扱いでセミナーや研究会に参加できます。法人会員の大きな目的は、それぞれの企業・団体が行っているシステム監査ビジネス・活動を拡大させることであり、個人会員の目的とは異なっています。

月1回の法人部会では、法人会員の代表者が集まり、テーマを決めて討議・意見交換を行います。それぞれの企業・団体が行っている活動について、話せる範囲内で話合い、意見交換をしています。

システム監査の活性化につなげるための活動として、システム監査の実態調査のアンケート調査を計画しています。アンケート調査実施の際には、ご協力をお願いします。

4. 事例研究会

事例研究会の活動は、事例を基にした各種セミナーの企画・実施と、実際のクライアントに対して行うシステム監査普及サービスの大きく2つです。

皆様の所属企業・団体あるいはお知合いの企業・団体で、システム監査を受けてみたいというところがありましたら、ぜひ、システム監査普及サービスをお勧めください。また、システム監査の実務的・実践滝手法を習得したいという方は、事例研究会主催のセミナーの受講をお勧めします。

今回ご紹介した以外にも、当協会では、活性化プロジェクトを中心に、各研究会、委員会、担当組織が活発な活動を行っています。会員の皆様の活動への積極的な参加、ご意見をお願いいたします。

2013.07 投稿

【 法人部会 】

会員番号 6005 斉藤 茂雄 （法人部会）

法人部会は協会の法人会員（約30社）から構成される部会です。主たる活動として自治体などへの情報セキュリティやシステム監査セミナーの講師派遣を行っています。また、月例のミーティングを実施し、ITやシステム監査に関するガイドライン等の輪読などの勉強会も行っており、同時にオフタイムの情報交換も大事にして会員相互の交流を深めております。

活性化プロジェクト関連の活動としては、昨年度はSAAJでの法人会員のメリット増強をテーマに活動し、例えば法人会員企業の社員であれば一律に月例研究会参加費を会員価格とするよう提案し、実現いたしました。

今年度はシステム監査活性化を推進するについて、まずは昨今の各団体・企業におけるシステム監査の実態を知ろうということで、「システム監査の実態に関するアンケート調査」をテーマに掲げ、現在準備作業を行っているところです。作業はまだ着手した段階で、これから秋口にかけてアンケートの実施、年内に結果のまとめを行う計画で進めております。この調査にご興味がある方は、法人会員に限りませんので、是非活動に参加頂ければと思います。

以上

2013.07 投稿

投稿 システム監査事例研究会だより 2013 年 6 月

会員番号 0750 畠中道雄(システム監査事例研究会 主査)

【6月度事例研報告】

開催日時:2013 年 6 月 5 日(水) 18:30～20:30

開催場所:八丁堀区民館

1. 活動報告

1.1 第 10 回課題解決セミナー終了(久野)

6月1日受講者20名、講師:久野茂、浜崎元伸氏で開催した。

多くの受講者が次回も受講したいと答えている。

1.2 活性化プロジェクト報告(畠中)

6月4日プロジェクト会合について報告された。

2. 事例研の今後の運営に関する提案(大西)

月例会を中心とする、事例研の運営について、大西氏から次のような問題提起と提案があった。

2.1 問題提起

① 監査サービスの依頼がない現状では、(システム監査セミナー(実践・実務セミナー)を除くと、)システム監査に関する技能・ノウハウを習得できることを期待して事例研に入ってきた会員は、足が遠のき、一方、事例研としても、その監査技能・ノウハウを継承(＝伝承)する機会が減って、ノウハウの伝承が困難になってきている。すなわち、監査の素人を一人前の監査人に育て上げるプロセスを、事例研が提供出来なくなりつつある。

② 実践・実務セミナーに関しても、受講者が減り開催回数が減ってきたことにより、講師の講習・指導テクニック及びノウハウの継承(＝伝承)が困難になりつつある。

2.2 提案

会員が監査技法・ノウハウを習得でき、かつ事例研内でもノウハウが蓄積・継承できるようにための提案である。中山氏提案の白熱教室、及び三輪氏提案の旧教材を使った模擬監査(事例研月例会で6か月ぐらいかけ行なう)の延長線上にあり、会員及び事例研の[基礎体力]強化を狙ったものである。

① 監査の基本技法に関し、監査ステップごとに、重要ポイント・tips(コツ・秘訣)・注意点(禁止事項含む)・失敗事例等を学ぶ。

特に個人のノウハウや経験の継承を目指す。

② 監査に用いられる基準及びツール等の、重要ポイント・注意点・使い方・tips 等を学ぶ。

③ セミナー講師の講習テクニック(tips 含む)・指導ノウハウを、事例研内に蓄積し、その継承(＝伝承・移転)を図る。

2.3 習得・継承の方法

① 現教材に沿って、監査プロセスをたどり、必要に応じて教材を見直す。

② ベテラン監査人のノウハウを見える形に残す。

（ベテラン監査人が解説・伝授したノウハウの内容を、若い人が文書化・図解化・デジタル化等してまとめる。）

③ 成果をホームページ(サイボウズ Live 等含む)に（事例研会員限定等で）公開して共有してもらう。

・出席者からは賛同の意見が出された。

・対応方法としては、

①専門プロジェクトを立ち上げて、全体計画を作成、

②月例会の中で計画を実行していく、

③月例会と別にプロジェクト会議を開催、など。

3. 白熱教室

中山氏が欠席のため、7月に持ち越し。

畠中から、マイナンバー制について、データ管理（一意識別キー）の観点から意見交換したいという提案があった。議論は次回以降。

4. 次回

7月3日（水）　八丁堀区民館

出席者が現状程度で推移する場合は、8月以降は協会事務所で開催する予定。

以上

2013.07 投稿

投稿 システム監査事例研究会だより 2013 年 7 月

会員番号 0750 畠中道雄(システム監査事例研究会 主査)

【7月度事例研報告】

開催日時:2013 年 7 月 3 日(水) 18:30～20:30

開催場所:八丁堀区民館

1. 活動報告

1.1 第 11 回課題解決セミナー準備(畠中、中山)

9月7日開催、講師は中山氏と入谷氏。運営の詳細

① 講義を入谷氏、簡易演習を中山氏

② 講義内容をビデオ化し、地方の方あるいは支部に販売又は無償提供を検討する。

③ 事務局作業は講師に兼務していただく。

1.2 第 22 回監査実務セミナー(畠中)

8月31、9月1日、9月14・15日 東京で開催、募集中。

1.3 第 25 回監査実践セミナー開催(近畿支部主催)(畠中)

9月21・22日 大阪で開催、募集中。

1.4 第 26 回監査実践セミナー開催計画(東北支部主催)(畠中)

11月29・30日 山形で開催予定。

イベント名:SAAJ 東北支部 10 周年記念事業「システム監査セミナー」

講師1名の派遣依頼に対して、小倉氏を派遣。

1.5 第 10 回課題解決セミナーのアンケート結果報告(中山)

概ね好意的な評価であった。再受講も期待できる。

2. ワークショップ支援サービス

2.1 機械製造会社

社員の情報リテラシー向上から始めたい。

2.2 医薬品新薬申請業務支援会社

IT全般統制に関するセミナーの開催を希望している。

いずれも、少し時間を置いた後、様子を確認してみる。その結果で、ワークショップ支援サービスの範囲で、さらに詳しいヒヤリングあるいはフリートークをさせていただく。

自社システムのレベル感を知りたいということであれば、監査サービスの提案をする。

3. 事例研の運営改善

先月提案があった、事例研の運営に関する提案について、具体的な取り組みを始めることにした。

具体的には、事例研メンバーで分担して、監査目的別の監査モデルを想定した講義を受け持ってもらい、監

査のプロセスを学ぶ。畠中から事例研メンバーに打診し、担当範囲、時期を具体化する。

4. 白熱教室

5月に「システム監査人の役割、期待される技術水準、対象者像」を検討した際、取扱いが不明確であった組込みシステムについて、中山氏から「組込みシステムのセキュリティへの取組みガイドライン」が紹介された。

5. 次回

8月7日（水） SAAJ協会事務所

以上

2013.07 投稿

【 情報セキュリティ監査研究会だより その4 】

会員番号 0056 藤野明夫(情報セキュリティ監査研究会)

はじめに

情報セキュリティ監査研究会の活動状況の会報連載は、本号で第4回になります。第1回は研究会の雰囲気をご紹介するために3月21日に開催された第11回情報セキュリティ研究会の様子(テキスト第7章第5節の輪読)をお伝えしました。第2回は、そもそも当研究会として何を求めて活動しているかについてご説明いたしました。第3回は、テキスト(*1)第3章に関する議論と第4章の一部を抜粋してご紹介しました。第5章は「起業」に関する論考ですので、本会では検討しませんでした。今回は、テキスト第6章についての議論をご紹介いたします。資料のURL等については文末に示します。

【輪読のテーマ】テキスト第６章「ビッグデータにおける個人的な情報の価値」(*2)

＜本章の議論の観点＞ 本章においては、以下のことが論じられている。

個人情報の経済的価値や便益、社会的効用について、消費者(個人情報提供者)とサービス供給者(個人情報を利活用する企業、公的機関等)の立場で論じている。

＜個別の議論＞

６．１節　プライバシーに関する経済的考え方

〔論者の主張〕

本章のイントロとして個人情報の活用によって消費者(個人情報提供者)と活用者(企業)の双方に便益が得られる例を、自動車保険に関するドライバー(保険契約者)の属性情報の開示と保険料率の関係で説明している。もし、契約者の属性情報(年齢、仕事で使用する、休日しか使用しない、家族構成等)が保険会社側に開示されないとすると、保険会社はすべての契約者に対して事故率の高い属性を持つドライバーに合わせた、高く、かつ同一の保険料率を適用せざるを得なくなる。すると事故率の低い属性を持つドライバーにとっては割高な料率になり、魅力的な保険ではなくなってしまい、結果的に事故率の高いドライバーが主たる契約者となり、保険料率をますます高くすることになる。逆に属性を開示すれば、過去のデータの蓄積から属性に応じた事故率が算出でき、ドライバー個別に、そのリスクに応じた妥当な保険料率の適用が可能になって、ドライバー(消費者)にとっても、保険会社(サービス供給者)にとっても高い効用がえられることになる。

従来、個人情報保護の問題というと、漏えいしたときのリスクといった情報の秘密性(Secrecy)が中心的課題となってきたが、この他にAutonomy(自分自身によるデータコントロールの確保)やSeclusion(放っておかれることの権利)という面にも留意することが必要であり、制度設計をする上でも重要な課題である。また、これらに対する防護策にも社会的コストが発生している。

〔研究会内の議論〕

個人情報の開示とビッグデータ活用における経済的効用をたいへんわかりやすく解説している。ドライバーの属性情報という個人情報を開示し、これを保険会社が蓄積すれば、属性と事故率との関係というビッグデータ的解析が可能になり、結果としてドライバーの属性に応じた適切な保険料率の適用ができ、消費者、サービス供給者ともに高い便益を得ることができる。イントロとしてたいへん適切な議論である。

後段のAutonomyとかSeclusionといった問題は、ビッグデータ固有の問題ではないが、SNSを含むビッグデータの進展にしたがい、そのリスクが俄然、大きくなってきたものである。この問題は人権に直接関わるものだけに、人によって意見に隔たりがあるし、ある種の思想的な要素も強く持つ領域であり、微妙、かつ、やっかいな問題である。

プライバシー保護に関するOECD80年勧告も“Autonomy”がその基調にある。

６．２節　ビッグデータの出現による費用便益バランスの変化

〔論者の主張〕

「個人情報の便益」は、

①「金銭的な社会厚生（消費者余剰＋生産者余剰）」から、
②「個人情報を収集分析するコスト（生産者サイド）」と、
③「個人情報を供与することのコスト（個人サイド）」を、
減じたものである。

「金銭的な社会厚生」①は、位置情報を活用した終電に関するプッシュサービスや、車のドライバーに対する最適経路提供サービスなどで実現している。また、センサー系のデータの拡大や情報処理能力の向上は、②を押し下げる効果があることは明らかであり、①と②に限れば、個人情報の社会的な経済価値は上昇している。

一方、③の個人サイドからみた「個人情報を提供することのコスト」はどうであろうか。従来、あまり議論されてこなかったが、③の問題は、金銭的コストというよりは、個々人の感じ方、いわば、心理的コストというべきものであり、一律に論じることができない。さらに③にはもうひとつ大きな問題がある。それは本人が意識しない状況でデータが蓄積され活用される可能性があるということである。個人情報の提供に当たって、Autonomyが存在しない。たとえば、携帯電話で自分の位置情報が取られるのが嫌だから携帯電話を持たないという選択枝は存在しない。携帯電話を持つという意思決定をした瞬間に、位置情報の通知が少なくともサービス提供者に行われてしまう。その他にも、本人が意識しないうちに個人情報が勝手に取得されているという可能性もある。

明らかに①は増大し、②は減少しているのであるから、「個人情報の便益」は全体として増大しているといえそうであるが、③のコストは、心理的コストであり定量化が困難で、さらにAutonomyの欠如という重大な問題を孕んでいるが故に、もしかするとマイナスになる可能性がある。ここがビッグデータの社会的効用を考えるときの難しさである。

〔研究会内の議論〕

これも、いかにも経済学者らしい論理的、かつ、明解な主張と問題点の指摘である。「個人情報を供与することのコスト」は、ビッグデータの問題を考える上で、もっとも本質的かつ最大の課題である。第3章(*3)で検討されている匿名性の問題や、本節で論じられているAutonomyの問題等、個人の側からみたビッグデータの問題は、ほぼ、ここに集約されるであろう。

6．3節　ビッグデータの社会的効用を高めるための方策

〔論者の主張〕

前節で述べたように、ビッグデータの出現によって社会全体として経済的なメリットを享受できる可能性が十分高い。したがって、③の個人の心理的なコストを下げて、これらのコストをいれても社会全体の便益がプラスになるような方策を考えることが重要である。

心理的コストを下げる方策のひとつは、「知らないうちにどのような情報を把握されているのか分からず、またどのようにデータを利用されるのか分からない。」という状況を解消することである。それには、把握するデータの内容と利用方法について情報公開を進めることであり、その最適な方法は、当該データを利用したサービスモデルを構築することである。

6．1節で述べた自動車保険の例でいうと、ドライバー個人の属性の提供によってドライバー個人のリスクに見合った保険料率が適用され、個人にとっては個人個人の個別の属性による統計的予想事故率見合いの魅力的なサービスが受けられ、サービス提供者にとってはリスク見合いの保険料が受け取れるというビジネスモデルになっている。

もうひとつの方策は、国や公的機関がデータ利用に関するガイドラインを提供することによって、「どのように使われるか分からない」という不安を和らげることである。ただし、このガイドラインは画一的なものであってはならず、業界ごと、個人が提供するデータのセンシティビティ等によって個別に策定されることが必要である。

さらに、心理的コストは個人個人で大きく異なることにも留意しなければならない。FacebookやTwitterなどのSNS利用者は、概して個人情報の提供に関する心理的コストが低い。それに対して、SNSの非利用者は、心理的コストが概して高い。

データの2次利用にあたっては、イノベーションを促進するために、データの匿名化をして複数者が利用することで、よりオープンな形態をとることも考えられる。ただデータの匿名化には種々の問題がある。その手法を検討し、

匿名化されたデータに対するガイドラインを整備する必要がある。

〔研究会の議論〕

「個人情報を供与することのコスト」③を下げるという、ビッグデータを考える上で最も中心的な課題に関する議論である。論者の主張するように、把握される情報の明示とその利用方法の開示およびデータ提供者たる個人のメリットの提示、すなわち、提供者と利用者の双方のWinWinモデルとなるようなビジネスモデルの構築が肝要であるということには賛成である。

また、SNS利用者と非利用者の間には、心理的コストに関して大きな乖離があることも頷ける。いずれにしても、この部分の議論が最も重要であるので、より個別具体的な検討が必要である。

6．4節　ビッグデータを用いたビジネスモデル

〔論者の主張〕

「マルチサイド市場(multi-sided market)」という経済学上のコンセプトを紹介する。マルチサイド市場とは、2以上の市場を持っている財やサービスを総称するものである。この典型例であるクレジットカードビジネスは、カードの利用店から手数料を徴収するとともに、カードの利用者からも会費を取る、すなわち、利用店と利用者という二つの市場を持っている。この場合、二つの市場は密接に関連している。

ビッグデータの出現によって、このマルチサイド市場の可能性が大きく広がってきた。

たとえば、JR東日本のウォーターサービスのSUICA対応端末を用いた売れ筋飲料の分析などのサービスは、一般消費者と飲料メーカの両者が関係するマルチサイド市場ビジネスである。SUICAを用いて飲料を購入することにより、SUICAに蓄えられている個人の属性情報と購入商品のマッチングができ、販売機ごとの売れ筋商品の把握が可能になるので、飲料メーカにとっては、販売機ごとに最適な商品の補給や配置が可能になり、また消費者にとってもSUICAによる情報提供によって割引が適用され、双方にメリットがある。これをさらに敷衍すれば、消費地の顧客特性に合わせた肌理細かい商品開発や宣伝活動が展開でき、消費者にとっても自分の嗜好にあった商品の提供が受けられる可能性があり、正の経済的効果が期待できる。

このように、ビッグデータを用いて新たなビジネスモデルを考える際には、従来、独立であった複数の市場を結合し、そこから新たな経済的価値を生み出すことがヒントとなる。

〔研究会の議論〕

異種のデータの組み合わせから、まったく想像していない効果を得る、というのがビッグデータの大きな特徴のひとつであり、この特性を「マルチサイド市場」という経済学上のコンセプトをベースに、かつ、身近な事例をもとに極めて分かりやすく、明解に説明している。情報セキュリティ監査研究会の課題ではないが、このような新しい側面の理論的探求に関する知識も、われわれシステム監査人の身につけておくべき素養のひとつかもしれない。

【資料】

(*1) IPA（独立行政法人情報処理推進機構）編、2012 年 3 月発行
「くらしと経済の基盤としての IT を考える研究会報告書　つながる IT がもたらす豊かなくらしと経済
～ ビッグデータの価値と信頼 ～」）
URL　http://www.ipa.go.jp/about/research/2011bigdata/
情報セキュリティ研究会では、昨年から本年にかけて、本テキストの輪読を行なってきました。

(*2) 同上　第6章　ビッグデータにおける個人的な情報の価値　　東京大学　元橋　一之

(*3) 同上　第3章　質的に異なってきた IT 利用への対応　　慶應義塾大学　折田　明子

【情報セキュリティ監査研究会への参加について】

当研究会にご興味をもたれましたら、是非、ご参加いただきたいと存じます。毎月20日前後にSAAJ事務局で定例研究会を開催しております。参加ご希望の方、当会報をご覧になってご意見やご質問のある方は下記アドレスまでメールでご連絡ください。 security ☆ saaj.jp （発信の際には“ ☆ ”を“@”に変換してください）

以上

2013.7 投稿

「個人情報保護マネジメントシステム実施ハンドブック」簡易版　第６章

会員番号：1795　藤澤　博（個人情報保護監査研究会）

第6章　リスクなどの認識、分析及び対策

目的外利用や、漏洩、き損により、本人にどんな影響があるか、例えば本人が被る被害や、その賠償、信用失墜、顧客との取引停止となることなどを「リスク」として認識します。

6.1　リスクなどの認識

特定した個人情報に対し、各局面において想定されるリスクを洗い出します。

（各局面：個人情報の取得・入力、利用・加工、移送・送信、保管・バックアップ、消去・廃棄の状況）

法	「目的外利用」リスクの事例	参考：対策の事例
16条	利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。	「個人情報管理台帳」を整備して、従業者に個人情報の利用目的を認識させる。
17条	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。	受託する場合でも、委託元が適切に取得した個人情報であることを確認し「個人情報取扱申請書」などにより、管理者の承認を得る。
18条	利用目的を、本人に通知し、又は公表しなければならない。	書面で取得する場合は書面で本人に通知する。 本人に書面で通知できない場合や、受託する場合はホームページに公表する。

法律第20条では、“漏えい、滅失又はき損の防止”　を定めているのでその観点からも見てみましょう。

	第20条「漏えい」リスクの事例	参考：対策の事例
1	領収証を他の人に発送してしまった。	・窓あき封筒を使用する。 ・発送前に複数の人でダブルチェックする。
2	メールの誤送信 BCCで発信すべきところを、CCで発信してしまった。	・一時保留機能で再チェックする。 ・添付ファイルにパスワードを設定する。
3	ノートＰＣを電車の網棚に忘れた。 携帯を紛失した。	・端末ロック、遠隔ロックを設定する。 ・ファイルを暗号化設定する。

	第20条「滅失」リスクの事例	参考：対策の事例
1	ハードディスクがクラッシュした。	・外付けハードディスク等にバックアップを取る。 ・外部データセンターにバックアップを取る。
2	停電で作成中のデータが消失した。	・UPS（無停電電源装置）を設置する。 ・ノートＰＣに変更する。
3	顧客データを別のデータで上書きしてしまった。	・バックアップしてから作業を始める。 ・別名で保存してから訂正するなど、文書管理ルールの見直しを行う。

	第20条「き損」リスクの事例	参考：対策の事例
1	原本をFAXし、ジャムって破損した。	フラットベッド型FAXを導入する。
2	コーヒーを書類の上にこぼした。	休憩コーナー、休憩時間など職場環境を整備する。
3	ハッカーが侵入し、データが書き変わってしまった	・ファイヤーウォールを設定する。 ・ログの記録と点検を行う。

6.2　リスク分析表の作成

ライフサイクルごとに、想定されるリスク（利用目的の通知漏れ、同意の取得忘れ、漏えい、滅失又はき損、目的外利用など）のリスクを洗い出し、対策を検討します。

以下は、従業者情報のリスク分析の事例です。（縮小版）

業務フロー／リスク分析表(兼　運用監査チェックリスト)										保護管理者
										承認
部門		管理部		業務名　「従業員管理」						
業務フロー		採用から従業員管理および退職に至る従業員情報管理業務								2012/4/1
ライフサイクルおよび業務名		台帳	個人情報管理台帳に記載の個人情報名	取得手段入力	媒体	コピー	想定されるリスク	リスク対策	規程・様式	残存リスク
取得	採用業務	1 2 3	履歴書 職務経歴書 成績証明書	本人・直接手渡し	紙	禁止	利用目的の通知漏れ	1．面接キット「同意書(応募者用」	「個人情報取扱規程」3.4.2.4	－
							書面による同意の取得漏れ			
							漏洩(紛失)	1．保管管理者の限定	「安全管理規程」4	－
								2．施錠管理	「安全管理規程」4	－
		4	応募者からの同意書		紙	禁止	漏洩(紛失)	1．保管管理者の限定	「安全管理規程」4	－
								2．施錠管理	「安全管理規程」4	－
移送		－	(応募書類の返却)	－	紙	－	漏洩(誤送付)	1．簡易書留で送付	「安全管理規程」9	
								2．送付表の保管	「安全管理規程」9	－
利用		5	応募者リスト 採用結果票	面接者が記入	紙	禁止	目的外利用(期限を超える保管)	「廃棄記録」による確認	「安全管理規程」4	－
取得	入社手続	1～10	入社時取得書類 従業者現況表 住民票 同意書	本人・直接手渡し	紙	禁止	利用目的の通知漏れ	1．入社手続キット「同意書(従業者用」	「個人情報取扱規程」3.4.2.4	
							書面による同意の取得漏れ	2．授受記録(明細)	「安全管理規程」2	－
保管	従業員管理						目的外利用(期限を超える保管)	台帳見直し時の点検	「安全管理規程」4	
							漏洩(紛失)	保管管理者の限定	「安全管理規程」4	
								施錠管理	「安全管理規程」4	
利用		11	人事管理データ	入力	人事部サーバー	バックアップ	漏えい(不正アクセス)	アクセス権限を1名のみに設定	「安全管理規程」8	ログの不取得のため、不正アクセス検知不可
		12	イントラ登録データ	入力	サイボウズ	バックアップ	漏えい(不正アクセス)	アクセス権限設定	「安全管理規程」8	－
								アクセスログ取得と点検	「安全管理規程」8	－
		13	人事異動稟議書 辞令 人事通達等	入力	人事部サーバー	バックアップ	毀損(誤入力)	担当者と部門長による二重チェック	「安全管理規程」6	－
							漏えい(不正アクセス)	アクセス権限を1名のみに設定	「安全管理規程」8	11と同じ
				印刷	紙	回付	漏えい(不正持ち出し)	通達番号管理、回付先管理	「安全管理規程」6	－
		16 17	年金手帳 雇用保険被保険者証	本人・直接手渡し	紙	禁止	漏洩(紛失)	常時施錠管理	「安全管理規程」3	
								授受記録	「安全管理規程」2	－

6.2.1　リスク対策が規定されているかどうかの確認

「3313リスク分析表」で講じるとした対策が、「3301個人情報取扱規程」や「3430安全管理規程」などに、規定されているかどうか確認し、その規程名称と条項番号を記入します。

※　規定が無い場合は「要規定」「規程なし」などと記入し、6.3リスク対策を規定する手順に進みます。

6.2.2　残存リスクの確認

検討した対策が、予算その他の事情で講じられない場合は、残存リスクとして記載します。

残存リスクと認識する前に、「3801是正・予防措置報告書」によって対策を立案する場合もあります。

6.2.3　「リスク分析表」の提出と承認

各部門長は、「3313 リスク分析表」について、個人情報保護管理者の確認・承認を得ます。個人情報保護管理者は、部門で認識されたリスクが、全社で共通して発生すると判断した場合は、組織全体で講じるべき対策を検討します。

6.3　リスク対策を規定する

講じるとしたリスク対策が規定されていない場合は、以下の手順で規定します。

a) 部門長は「3801 是正・予防措置報告書」によって、対策の立案とともに規定するよう立案する。
b) 個人情報保護管理者は、具体的な規程の条文を立案し、「3801 是正・予防措置報告書」に添付して代表者もしくは役員会の承認を得る。
c) 個人情報保護管理者は、改定した規程について従業者に通知し、常時閲覧可能とする。

6.4　リスク分析の見直し

個人情報保護管理者は、毎年 PMS 運用年度のはじめに策定した「3303PMS 年間計画書」に従い、「3313 リスク分析表」見直しを実施するよう、部門長に通達します。また、少なくとも以下の事象が発生した場合には、都度見直しを実施します。

1	「3311 業務フロー」および「3312 個人情報管理台帳」を変更したとき
2	業務に関連する法令・規範等の改定があったとき
3	組織変更等により、業務の流れが変わったとき
4	事業所の移転・模様替え等で、安全管理上の変更が発生したとき
5	情報システムの導入・変更など、セキュリティ環境が変わったとき
6	緊急事態発生後、是正・予防処置を講じるとき

※「3313 リスク分析表」の提出は、メール添付ファイルによる提出、共有ファイルサーバー上の「提出用フォルダ」への保存など、電子ファイルで提出することが一般的です。

個人情報保護管理者は、保管フォルダを年度ごとに分けて、「3313 リスク分析表」の履歴を残します。

プライバシーマークの更新審査は２年ごとで、定期的な見直しが、計画に従って２回以上行われていることについて審査されます。

2013.7 投稿

「個人情報保護マネジメントシステム実施ハンドブック」簡易版　第７章

会員番号：1795　藤澤　博（個人情報保護監査研究会）

第７章　緊急事態への準備

緊急事態は、“起きるもの”　として準備する必要があります。

そのため、緊急事態の認識の発生を監視し、検知し、緊急対応し、復旧するための手順を確立しなければなりません。個人情報の漏えい、滅失、き損もしくは法令違反に気付いた者が、速やかに責任ある者まで連絡できるよう手順を定め、いつでも参照できるようにしておきます。

7.1　緊急事態の定義

緊急事態が発生したときは、経済的な不利益、社会的な信用の失墜、本人への影響などを考慮し、その影響を最小限とするため、緊急事態を以下の３つのレベルに区分けて定義します。

また、委託先で発生した事故・事件についても、自社に責任がありますので同様に取り扱います。

レベル	影響度　(事例)	影響	責任者
A (高)	１個人情報が社外へ流出（紙、電子データ） ２個人情報をき損・滅失しサービス不能状態が継続 ３影響範囲が特定できず被害が拡大する恐れ	多数の顧客	代表者
B (中)	１個人情報が社外へ流出（回収可能） ２個人情報をき損滅失してサービス不能状態（短時間） ３影響範囲が特定でき被害が拡大の恐れがない	特定の顧客	代表者
C (低)	上記に相当する事態が発生したが、事前に検知した。 その結果、外部顧客、取引先に影響ないと判明した。	被害なし	個人情報保護管理者

7.2　緊急事態の体制

代表者は、緊急事態発生時に指揮をとり早期解決を図ります。各部門長、連絡先（内線番号、携帯電話番号）、連絡ルートなどを「3371 緊急時連絡網」に定めておきます。

7.3　緊急事態発生時の措置

緊急事態発生の連絡を受けた代表者は、「緊急対策会議」を招集し、以下の措置を決定します。

1	本人への連絡（必須）	当該漏えい、滅失又はき損が発生した個人情報の内容を本人に速やかに通知し、又は本人が容易に知り得る状態におく
2	関係機関（必須）	関係省庁、個人情報保護団体、JIPDEC など
3	警察	サイバーテロ等の恐れがある場合
4	社内通知（必須） 公表（自社ＨＰ公表、 マスコミ発表）	二次被害の防止、類似事案の発生回避などの観点から、可能な限り事実関係、発生原因及び対応策を遅滞なく公表する。

7.4　再発防止措置

緊急事態が収まりまたは最悪の状態から脱した時期に、類似案件が再発しないよう、「是正・予防処置報告書」によって再発防止策を策定し、実施します。再発防止策は、緊急事態発生部門だけでなく、同様の事態が発生する可能性のある部門に対しても教育し、実施します。

7.5　関係機関への事故報告

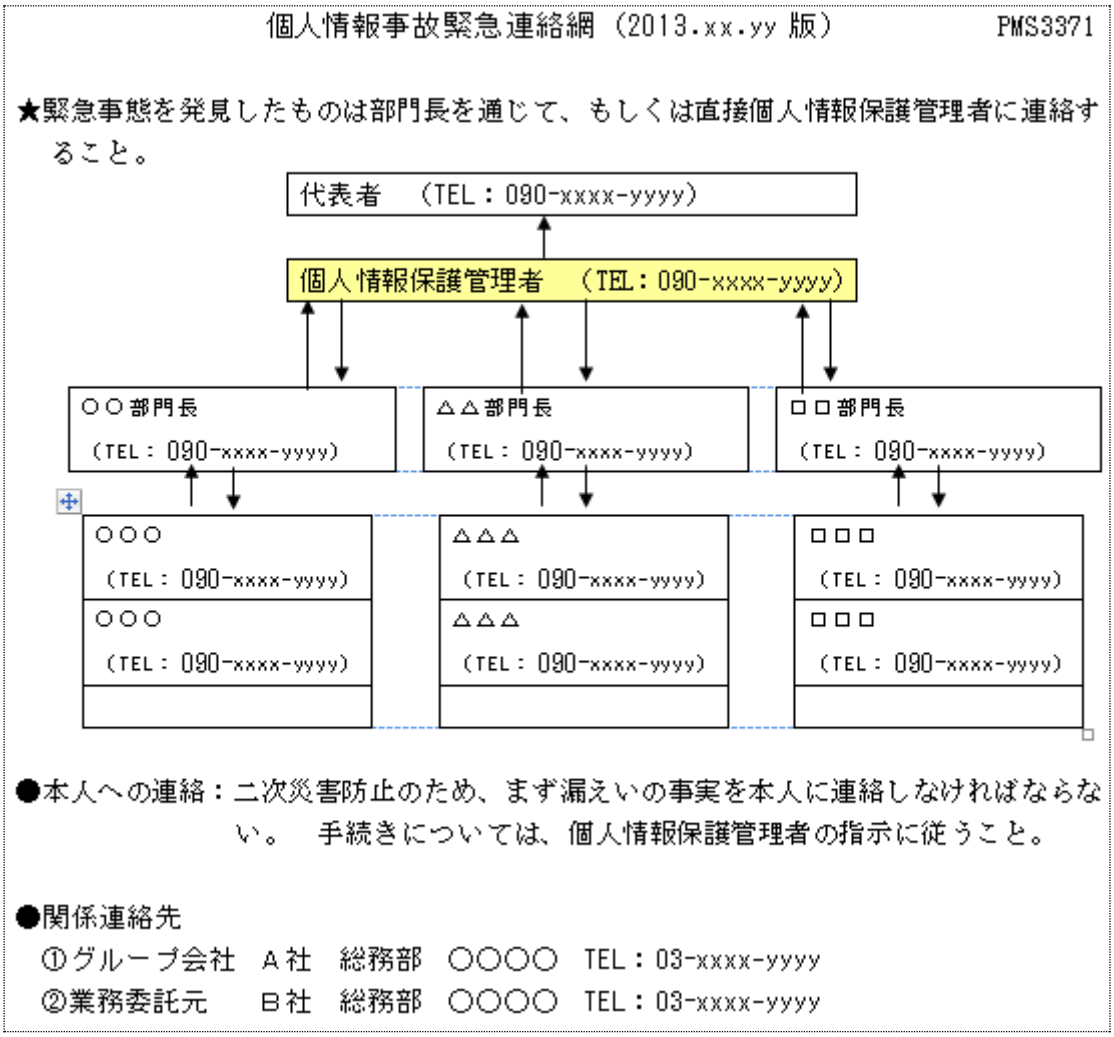
個人情報保護管理者はレベルＡ、Ｂ、Ｃを問わず、すべての緊急事態発生について、「3373 事故報告書」を作成し、社長の承認を得て審査機関（一般財団法人 日本情報経済社会推進協会（JIPDEC）プライバシーマーク事務局など）に報告します。

※　プライバシーマークを取得していない事業者は、監督官庁に報告します。

7.6　緊急事態への準備・対応に関するマネジメントレビュー

個人情報保護管理者は、１年間に発生した緊急事態の発生の内容と対応結果、サイバーテロなどの外部環境の変化、技術の進歩などを踏まえ、緊急事態への準備・対応に関する手順について有効性を評価し、マネジメントレビューのインプットとして報告します。

ご参考：「緊急時連絡網」の事例



次回は、「第８章　個人情報の取得、利用および提供に関する原則」
「第９章　本人から直接書面によって取得する場合の措置」を予定しています。

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

2013.07 投稿

協会からのお知らせ　【　会費納付等のお願い　】

会員番号 0557 仲 厚吉(事務局長)

事務局では、2013 年度会費未納の会員の皆様へ督促メールを送信し 6 月 28 日までに未納の場合に「会費納付のお願い」状を 6 月 30 日付で送付しました。また、未納分が 2012 年度と 2013 年度の 2 年分の会員の皆様へ同様の「会費納付のお願い」状を送付しました。

拝啓、平素は協会の運営にご協力いただきまして誠にありがとうございます。さて、年会費の納入状況を確認しましたところ、下記の通り会費が未納となっております。改めて請求書を送付いたしますので、早急にご納付下さるようよろしくお願いします。既に納付済の方には失礼の段ご容赦願います。尚、会費の未納が続きますと協会の規定により会員資格を継続できないことになりますので、協会の趣旨をご理解の上、ご対応よろしくお願い致します。敬具

■未納分:2013 年度会費　:金 10,000 円

1. 払込期限:本状到着後 1 か月以内
2. 振込先:　以下のいずれかの口座にお振込お願いします。

(1)郵便振替口座:00110-5-352357
　加入者名:日本システム監査人協会事務局
(2)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
　(振込手数料はご負担願います)

銀行振込の際は、会員番号 4 桁(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、メールまたは FAX などで振込内容をお知らせください)

■ご寄附のお願い

協会では会員の皆様にシステム監査の普及促進のためご寄附のお願いをしております。上記の会費納付と同じ振込先口座に、一口 3,000 円のご寄附を、お振り込みいただければ誠に幸いでございます。なお、協会から寄附者名簿を所轄庁の東京都に提出することがございます。また、御礼のため会報に寄附者氏名を公表することがございます。

■会員登録情報の変更のお願い

会員におかれて連絡先の住所やメールアドレス等の変更がある場合は、会員登録情報の変更をお願い致します。協会ホームページの「会員登録情報の変更についてご案内」の画面から変更できます。何とぞよろしくお願い致します。

http://www.saaj.or.jp/members/henkou.html

以上

2013.07 投稿

協会からのお知らせ　【　協会行事一覧　】

会員番号 0557 仲 厚吉(事務局長)

2013 年	理事会・事務局・会計・認定	部会・研究会	支部・特別催事
7 月	(会計)支部会計報告依頼:14 日必着 (事務局)会費督促状発送〔7 月1日付〕	(月例研)「実演によるサイバー攻撃の仕組み解説」:24 日 (CSA フォーラム)「6ヶ月で構築する PMS」:29日	(支部)本部助成金収入 (近畿支部)支部創設25周年記念研究大会:6 日
8 月	(認定)秋期 CSA・ASA 募集:8/1～9/30 (会計)中間期会計監査:中旬 (理事)会費督促電話:8/10～末	(月例研)「クラウドインシデント」:21 日 (基準研・ISO)「ISO/IEC 東京会議」:8/19～8/22 (事例研)「実務セミナー」:31 日	
9 月	(会計)予算実績中間報告:12 日	(事例研)「課題解決セミナー」:7 日 (CSA フォーラム)	
10 月			
11 月	(認定)CSA・ASA 更新手続案内 〔申請期間 1/1～1/31〕 (認定)CSA 面接 (会計)2014 年度予算申請提出期限:30 日	(CSA フォーラム)	(北信越支部)西日本支部合同研究会:23 日
12 月	(会計)2014 年度予算案:1日 (理事会)2014 年度予算案・役員改選・会費未納者除名承認:12 日 (認定)CSA 面接結果通知 (会計)2013 年度経費〆切:20 日 (事務局)通常総会・役員改選公示 (事務局)2014 年度会費請求書・寄附願い発送〔1月1日付〕		(東北支部) 支部総会・支部設立 10 周年記念講演会:14 日
2014 年	**理事会・事務局・会計・認定**	**部会・研究会**	**支部・特別催事**
1 月	(認定)CSA・ASA 更新申請受付 〔申請期間 1/1～1/31〕 (会計)支部会計報告依頼:14 日必着 (事務局)総会資料〆切:15 日 (会計)2013 年度決算案:中旬 (会計)2013 年度会計監査:下旬	(CSA フォーラム)	(近畿支部)支部総会:17 日
2 月	(認定)CSA・ASA 春期募集:2/1～3/31 (理事会)通常総会議案承認:6 日 (通常総会):21 日	(通常総会特別講演)	

※注　定例行事予定は省略。

2013.07 投稿

研究会、セミナー開催報告、支部報告

■【CSA・ASA 継続教育セミナー　受講報告】

会員番号 0557　仲　厚吉(会報)

1.日　時 ： 2013 年 6 月 15 日(土) 13:30～16:45
2.場　所 ： 機械振興会館 地下 3F研修室1
3.テーマ・講師 ：
①「フィッシングの動向について　狙われる金融機関」
フィッシング対策協議会(JPCERT/CC)事務局　山本　健太郎　氏
②「フィッシング摘発　警察の取り組みについて」
警察庁生活安全局 情報技術犯罪対策課　警視　吉田　光広　氏

・テーマ①について

＜講演骨子＞ はじめに、フィッシング対策協議会についてのご紹介があった。続いて、日本のフィッシングの現状、世界のフィッシングの現状、フィッシング対策に関してご説明があった。

＜受講感想＞ フィッシング対策協議会は、フィッシングの攻撃対象となり得る事業者や、防御手段を提供し得る事業者などにより構成される協議会を運営し、フィッシングに関する情報収集・提供、動向分析、技術面の検討などを行うとしています。フィッシングメールは、よく見ると怪しい文章だが、ユーザーは騙されてフィッシングサイトへ誘導され、フィッシングサイトは、クレジットカードのサイト、プロバイダのＷｅｂメール、オンラインゲーム、ＳＮＳサービスなどを騙っています。また、銀行の第二認証情報を詐取するフィッシングもあり、“セキュリティ強化の為”や、“サーバのバージョンアップを行いましたので”等のもっともらしい文面で銀行の第二認証情報を詐取するフィッシングである等、ユーザーとしては、フィッシングの事例をできるだけ知っておいて、フィッシングに備える必要があると感じました。

・テーマ②について

＜講演骨子＞ はじめに、フィッシング摘発の警察の取り組みについてのご紹介があった。続いて、不正アクセス禁止法違反検挙事例（フィッシング組織の初検挙)、サイバー犯罪の現状、改正不正アクセス禁止法について、不正アクセス禁止法違反検挙事例（フィッシング組織の検挙２)、インターネットバンキング対象のフィッシング等認知状況、刑法のウィルスに関する罪について、不正指令電磁的記録罪検挙事例、ネットショップを舞台とした不正アクセス・詐欺等事件、連続自動入力プログラムを利用したリスト攻撃の発生など、フィッシング摘発の事例紹介のご説明があった。

＜受講感想＞ フィッシング犯罪事例をもとに摘発現場の話を聞きました。初検挙されたフィッシング詐欺組織は、幹部グループ数名が、詐欺実行犯数名をネットでリクルートし、詐欺実行犯は面識のない者同士の組織において気軽に犯罪に手を染めていたものです。フィッシングの摘発は、たいへんな取り組みをされての成果であることが良くわかりました。

以上

■北信越支部 「2013 年度 福井県例会 報告」

以下のとおり2013年度 北信越支部総会・研究会を開催しました.

・日時:2013 年 6 月 8 日(土)13:00～17:00　　参加者:10 名

・会場:アオッサ AOSSA(福井市)

・議題:

- ✧ 報告 1:「情報セキュリティ 組織の内部不正に対する研究の紹介
  ―人的脅威対策に関する犯罪理論の応用―」
  角屋 典一 氏
- ✧ 報告 2:「外部委託先管理とシステム監査」
  小嶋 潔 氏
- ✧ 西日本支部合同研究会 in Kanazawa 運営検討

◇研究報告 1

「情報セキュリティ 組織の内部不正に対する研究の紹介
―人的脅威対策に関する犯罪理論の応用―」

報告者(会員 No. 1267 角屋 典一)

1. 大手ベンダーで発生した不正事案を契機に内部不正について考察してみた。IPA の発表、そのほかの論文を紹介しながら、組織の内部不正について対応方法を検討してみた。
   まずは、当該大手ベンダーがホームページ上に掲載した再発防止策の内容について、私見を述べ疑問点をいくつか洗い出した。
2. 次に、先進的に実施されている米国の内部不正対応を紹介し、さらに日本の対応状況について説明した。
   内部不正の特徴は、組織外部からの不正(攻撃)比べて件数は圧倒的に少ないものの、1件当たりの被害額は企業にとって大きな損害を与える額となることである。
3. 日本の調査としては、財団法人社会安全研究財団の「情報セキュリティにおける人的脅威対策調査報告書 平成 22 年 3 月」を参考に発表した。文献にある調査票の項目を表形式にまとめ、どのような観点から調査を行ったかを具体的に検討してみると、人的脅威をモデル化するための必要事項が見えてきた。
   調査票に基づく不正事案の調査や過去の事案を参考にして分析モデルを使用して類型化を行うと、内部不正は以下の4つの類型にまとめることができる。
   - システム悪用
   - システム破壊
   - 道具的犯行としての情報流出
   - 表出的犯行としての情報流出

   内部不正を分析した結果、情報セキュリティは「技術的なシステム」や「モニタリング」だけでなく人によって支えられているということに気づかされる。そし入社前、在職中、退職期、退職後といった時期に応じた対策の重要性を強調している。

   従って、情報セキュリティ対策は、システム側、「情報」側からの検討だけでなく、人的側面を含めた諸要素のガバナンスが非常に重要であり、このような観点から組織のリソースの効果的配分が必要となってくる。

4. 具体的な対策を考えるうえで、セコム株式会社 IS 研究所の「セキュリティ実現の視点からみた内部要因事故抑制手法」の内容を紹介しながら検討した。

文献の中で、本来の「セキュリティ」とは「オペレーション（日々の営み）が運営主体によってあらかじめ定められたプランに則って運営され、理由の如何によらず、それが阻害されないこと」であり、セキュリティ対策によってそもそも守るべきは「組織のオペレーション」であると定義している。

留意点として

- 組織のセキュリティを考える場合、人・物・金、そして情報などをまもることに目が向かいがちであること。
- 本来のセキュリティ対策において守るべき対象は、いかなる場合においても「組織のオペレーション」であること。
- ヒューマンエラーや内部不正は、組織で働く人が根源となる脅威であり、この脅威に対応するためには「そこで働く人に『魔がささない』『ミスがでない』『不正ができない』組織環境」が必要であること。

があげられている。

次に、内部不正抑制に応用可能な犯罪理論を紹介している。

- 犯罪は「犯罪企図者」が「犯罪の機会」に遭遇することで成り立ち、この成立要件が満たされなければ、原理的に犯罪は起こりえないこと。
- この成立要件を崩す手法として「犯罪機会論」と「犯罪原因論」という2つの考え方の防犯方法論があること。
- その他の応用可能な犯罪理論として、「不正のトライアングル理論」、「日常活動理論」、「合理的選択理論」と「性弱説」、「割れ窓理論」を紹介している。

ここでは、犯罪機会論、犯罪原因論の考え方を融合させた「状況的犯罪予防論」、「組織論（組織文化）」の二つの観点から、組織に対する防犯理論を展開している。

「状況的犯罪予防論」による内部不正対策は、予防策の増強（物理的にできない）、発覚リスクの増強（やると見つかる）、利得の抑制（割にあわない）、誘因の排除（その気にさせない）、弁解余地の排除（言い訳を許さない）の 5 大項目を基本にして細分化した具体的な対策を説明している。

「組織論」による内部不正抑制対策では、募集と就職時（適格人材雇用と強化開始）、就職後数か月（組織文化の定着）、在職中（ミス/重圧、誘惑対応、ES 向上）、重要ポスト異動時（職責再認識、職権乱用抑制）、退職時（リスクを残さない）の5大項目を基本として細分化した具体的な対策を説明している。

まとめして、組織の内部で発生している不正やヒューマンエラーは組織のオペレーションを内部から蝕む「組織の生活習慣病」とでも呼ぶべきものであり、「組織の生活習慣」を変化させるためには、組織で働く人々の意識を変え、行動を、ひいては従業員一人ひとりの考え方と習慣を改めさせる必要性を強調している。

5. これまでの検討から、内部不正対策について考察するきっかけとなった大手ベンダーがホームページ上に掲載した再発防止策の内容を検証してみると、「新たな企業文化の醸成」に対する取組が不十分であることが推察され、監査人や外部委託管理者としての委託元は、この点に注視した対応が今後求められる。

［参考文献］

・IPA テクニカルウォッチ
『組織の内部不正防止への取り組み』に関するレポート

2012 年 3 月　独立行政法人情報処理推進機構
・「組織内部者の不正行為によるインシデント調査」報告書
2012 年 7 月　独立行政法人情報処理推進機構
・「情報セキュリティにおける人的脅威対策に関する調査研究報告書」
2010 年 3 月　財団法人 社会安全研究財団
情報セキュリティにおける人的脅威対策に関する調査研究会
・「セキュリティ実現の原点から見た 内部要因事故抑制手法」
セコム株式会社 IS 研究所　甘利 康文、新井 真司、内田 順一
2012 年 3 月 JNSA Press 第 33 号 NPO 日本ネットワークセキュリティ協会

以 上

◇研究報告 2

「外部委託先管理とシステム監査」

報告者（会員 No. 1739 小嶋 潔）

勤務先の業務委託先における不祥事発生を受け、外部委託先管理の強化の一環としてシステム監査において取り組むべき課題と対応策について検討しました。

1. 一般的に外部委託先管理で求められていること

（1）外部委託業務のシステムリスク管理

（ア）外部委託する業務のシステムリスクを特定し、サービスの質や存続の確実性等のリスク管理上の問題点を認識し、的確、公正かつ効率的に遂行できる能力を有する者に委託する。

（イ）委託契約では、サービス水準、委託先との責任分担、監査権限、再委託手続き等について規定する。

（ウ）委託業務が適切に行われていることを定期的にモニタリングすると共に、受託先の内部管理や開発・運用管理の状況について、報告を受ける態勢を整備する。

（エ）委託先に対して、内部監査部門またはシステム監査人等による監査を実施する。

（2）外部委託先の検証

（ア）委託先が業務委託を受けた業務について、システムリスクを認識・評価しているか。

（イ）委託者による監査または外部監査を定期的に受けているか。また外部監査を実施した場合は、委託者に対して監査結果を報告しているか。

（ウ）企画段階、設計・開発段階、テスト段階において、委託者によるユーザーレビューやユーザーテストが実施されているか。

（エ）システム開発管理状況について、品質管理部署等により客観的に評価する態勢を整備しているか。

（オ）システム運用状況について、委託者に対して報告する事項を定め定期的に報告し、システム障害発生時の連絡態勢を、あらかじめ定めているか。

2. 我が社における従来の外部委託先管理態勢

（1）委託業務の内容と範囲の明確化、業務委託に伴うリスク評価、委託先の財務面の健全性確認、委託業務遂行

能力の確認、情報管理態勢の確認等により委託の是非の事前確認を行うと共に、契約書の要件を事前に検証しています。

(2)委託先の委託業務の遂行状況及び委託情報管理や顧客対応状況について定期的に(年1回)モニタリングを行っている。モニタリングでは、委託先の経営状況や委託業務の質、情報管理体制、報告の実施状況等を確認します。

(3)個人情報の処理を委託する重要な外部委託先に対しては、立ち入り監査を実施しています。

以上のとおり、一般的な外部委託先管理について常識的に態勢整備し、従来は監査も含めて特に問題なく運用されてきました。しかしながら、不正事件発生を機に管理態勢を強化せざるを得ない状況にあります。

3. 委託先における不正事件の発生

(1)犯人は、業務委託先の協力会社のSEで、事業立ち上げ当初から業務に従事しており、極めて専門的な知識を持っていた。その知識と経験を利用して取引情報を特殊なツールにより抜き出し、顧客の個人情報を不正に取得し悪用するという事件が発生しました。

(2)発生原因

(ア)各種セキュリティ対策が内部関係者の悪意ある攻撃に対して不十分で、要員に対するセキュリティ教育と倫理観の醸成が不十分であった。

(イ)開発担当者が取引情報を不正に取得できた、情報に対する不正アクセスの検知が不十分、本番運用中システムから開発環境へデータ持ち出しが可能、開発用端末でUSBメモリが使用可、といった点でセキュリティ対策が不十分であった。

(ウ)委託者による、委託先のリスク管理状況に対するモニタリングや牽制等のガバナンス態勢が不十分で、システムリスク管理の観点での踏み込みが甘かった。

(3)委託先による再発防止策

(ア)取引情報の引き出しを可能とした特殊なツール機能を削除し、取引情報へのアクセスを検知し運用管理者にアラート通報する。

(イ)本番環境から開発環境へのアクセスルートを遮断し、開発環境から本番環境へデータを移送する場合は受け渡しフォルダを経由し、本番と開発の両環境への同一人物によるアクセスを不可能とする。端末のUSBポートを物理的に閉塞すると共に、ソフト的にも利用制限を行う。

(ウ)開発担当が本番環境で作業する際には、複数名作業を必須とし、一人でも離席する場合は端末操作キーを運用担当者に返却する。外部委託先へのセキュリティ教育の徹底と不正に対する懲戒処分や社会的制裁についても周知する。

4. 我が社の外部委託先管理強化策

事件を受け、我が社においても外部委託先管理を強化すべく、下記のような対策を行っています。

(1)外部委託先管理強化

(ア)個人情報の取扱いの再委託がある外部委託先を対象に、再委託先の管理強化を行う。

(イ)常駐するベンダーの開発要員に対するセキュリティ教育を行う。

(ウ)社外へ個人情報を送付して業務委託している先への監査項目を見直し、立ち入り監査を実施する。(監査

項目としては、重要情報の暗号化の実施、本番と開発環境の分離、本番作業の相互監視体制、USB等外部媒体の使用禁止等の確認）

（2）自社のコンピュータセンターにおける情報漏洩防止として、外部媒体の使用を制限する。また、サブシステムについて、開発担当者が本番環境にアクセス可能なケースがないか確認し制限する。

5．システム監査の課題と限界

（1）委託先再発防止策と委託者による監査の限界

（ア）セキュリティ対策上の不備が今回の問題以外にないかどうかについて、委託者がどれだけ把握していけるか、本当に開発・運用のリスク管理状況を検証できるか疑問です。システムに抜け道がないかをチェックすることは現実的に不可能ですし、そのような知識や情報は、ひょっとすると委託先の技術者に依存するしかないかもしれません。

（イ）したがって委託元としてどれだけ頑張って立ち入り調査を実施しても、結局は表面的・形式的な監査しかできないのではないかという懸念は、残念ながら拭いきれません。

（2）我が社の管理強化策の不十分な点

（ア）開発環境から本番へのアクセスが可能な場合のアクセス検知やアクセスログの検証が不足。せっかく本番環境へのアクセスログを取得している場合でも、量的問題や時間的な制約を理由として、ログのモニタリング検証を行っていないケースが多い。

（イ）事務センターにおける情報漏洩防止対策を強化し、また銀行外での個人情報の業務処理委託先の立入り監査項目追加は行っているが、銀行外のベンダーの開発拠点におけるセキュリティチェック強化の観点が抜けている。特にリモートメンテナンスでサーバにアクセスする場合において、情報セキュリティ管理状況の現場立ち入り調査を行うことが必要である。

（3）監査の限界と改善策の検討

（ア）個人的には、システム監査を行っても残念ながら自らセキュリティ上の不備を発見することは、かなり至難だと思います。個々のシステムの詳細な内容をすべて把握することは無理ですし、ましてや特殊なシステム仕様を検証しろと言われても、不可能に近いものがあります。担当者にヒアリングした際に、嘘をつかれても気付かないかもしれません。

（イ）しかしながら、様々な不正や障害情報を参考にしながら、監査において着目すべきポイントやアプローチの仕方を充実させ、システム部門に対して必要なチェック項目を確認させることにより、セキュリティを向上させることは一定可能だと考えられます。

（ウ）したがって、今後も常に広くインシデント情報を収集し、被監査部署が把握し実施しているセキュリティチェック項目に不足がないかを検証し、不足があればこれを指導してチェックさせることが、私個人としてはシステム監査の方向性の一つではないかと考えている今日この頃です。

以 上

■【 近畿支部主催　システム監査体験セミナー（入門編）開催結果について 】

会員番号 01345 広瀬克之

近畿支部では、2013 年 6 月 22 日(土)、常翔学園大阪センター（西梅田）を会場として、システム監査体験セミナー（入門編）を開催しました。

10 時から 17 時までの 1 日コースで、スーパーマーケットに対するシステム監査のケーススタディを主な内容として、13 名の方にご参加いただきました。

●講義 ＆ チェックリスト作成

最初にセミナーの説明やスタッフ及び受講者の自己紹介を行った後、「システム監査概要」の講義を行いました。

その後、本日のケーススタディで学習する内容を監査手順に従って説明し、受講者を 4 チームに分けて、インタビュー項目の洗い出しを行い、チェックリストをまとめていただきました。

●インタビュー ＆ 監査報告書作成 ＆ 監査報告会

午後からは、作成したチェックリストを用いて、店舗営業部とシステム課それぞれのキーマンに対するインタビューを体験いただきました。

インタビュー後は監査結果を監査報告書にまとめ、監査依頼者にあたる監査室長およびインタビューに回答した現場キーマンに対してチーム単位で監査報告していただきました。本セミナーではチェックリスト作成から、監査報告会までをロールプレイで体験いただきましたが、いずれの監査チームとも、監査室長以下からの質問・反論に対して適切に回答されていました。

●監査エピソード

ケーススタディの合間にセミナースタッフの監査経験を基にしたエピソードを紹介しました。1 回目「コンサルタントの同席」、2 回目「報告書の記載内容」というテーマで、短い時間ですが、受講者にとっては、今後監査に何らかの関与する際に、有益な内容であったと思います。

受講されたお二人から感想文を頂戴しました。

――

セミナーでは大変お世話になり、ありがとうございました。
監査の意義や方法の講義、インタビュー形式の実践と、短い時間に一連のエッセンスが凝縮されており、また受講生とほぼ同数という沢山のスタッフの方にサポートして頂き、事前知識の無い私でも、楽しく参加することができました。

体験型のワークショップは、セミナーの醍醐味でした。管理基準に沿って現場から情報を汲み上げ、報告書として纏める重要性と難しさは、講義だけでは得られないものだと思います。
業務で IT を構築している側が、監査側の視点を知ることはとても有意義です。同僚や同業者にも勧めたいと思います。
（Y.F）

――

監査の実践への理解を深め、営業活動に役立てたい。シンプルな動機で体験セミナー（研修）に臨んだ。場面設定が工夫された教材は助けとなった。問題点から仮説をたて、どのような監査基準項目でチェックポイントを設定するか。具体にどのような質問で言葉を引き出すか。研修での監査チームとしての共同作業で、インタビュー結果（調書）から報告書を作成することの奥深さ。研修は良き経験となった。企画、開発、運用、保守のシステムライフサイクルおけるシステム監査の意義は依然高い。IT ガバナンスの強化に資するべく、今後に活かしてゆきたい。

末尾で恐縮ながら、お世話になった監査チーム各位、並びに準備運営を頂いた事務局各位の御協力御尽力に厚く御礼申し上げます。（永井克則）

――

今回受講されたみなさんは、多くはシステム監査の学習になじみが薄い方でしたが、システム監査を体験するうえで有益であったとのアンケート結果をいただいています。また、スタッフサポートがよかったというご意見や、タイムマネジメントをもう少ししっかりするように、というご意見もいただきました。これらを参考に今後とも、より良いセミナーが提供できるよう努力していきたいと考えています。

以　上

2013.07 投稿

特集 【 月例研究会報告 】

■第 181 回月例研究会報告

日時:2013 年 5 月 21 日(火曜日) 18 時 30 分～20 時30 分

演題:『金融機関等コンピュータシステムの安全対策基準・解説書』及び
『金融機関等におけるコンティンジェンシープラン策定のための手引書』の
改訂に伴う追補版について

講師: 財団法人 金融情報システムセンター(FISC)
監査安全部 西村 敏信 部長 様
鬼頭 克巳 総括主任研究員 様
岡田 昌一主任研究員 様

報告者 №0148 木村 裕一

【概要】

『金融機関等コンピュータシステムの安全対策基準・解説書』(以下「安全対策基準」とも表示:第Ⅰ部とする)、及び『金融機関等におけるコンティンジェンシープラン策定のための手引書』(以下「コンテ手引書」とも表示:第Ⅱ部とする)の改訂に伴い、去る3月1日にそれぞれ発刊した追補版についてご説明いただきました。この記録は資料からの引用を主としました。

なお、資料からの引用は明朝字体で、記録者による記述は当字体で表示します。

＜第Ⅰ部＞

「安全対策基準」:クラウドサービスに関わる現状の留意点、スマートデバイスの業務利用における留意点、インターネットバンキングにおけるセキュリティの確保、また、金融庁によるシステムリスク総点検の結果、及び東日本大震災やシステム障害に関する日本銀行のレポート等を踏まえ見直した内容について。

＜第Ⅱ部＞ (→P6から)

「コンテ手引書」:東日本大震災での被災から復旧に至る過程において、業務継続態勢整備として有効と考えられる施策や、政府や各省庁等からの防災・減災対策に対する検討結果等を踏まえ見直した内容について。

＜第Ⅰ部＞

テーマ:『金融機関等コンピュータシステムの安全対策基準・解説書』の改訂

経緯

平成23年3月に実施した『金融機関等コンピュータシステムの安全対策基準・解説書』(以下『FISC安全対策基準』という)全面改訂後、金融機関等におけるコンピュータシステムをとりまく様々な情勢の変化を受け、「安全対策基準改訂に関する検討部会」にて継続検討を行い、『第8版追補』を発刊することとなった。

今回の主な検討事項は次のテーマである。

●クラウド利用に関わる課題、留意点
●スマートデバイスの業務利用における留意点
●東日本大震災やシステム障害に関する各種ガイドライン・レポートとの比較分析
全体の構成（改訂の有無など）は次のとおり。

No	主要テーマ	改訂有無	No	その他のテーマ	改訂有無
1	**クラウドサービスを対象とした安全対策基準の対応付け**	**有**	1	【運50】の渉外端末の管理を対象とした安全対策の十分性の確認	有
2	**セキュリティ脅威の実情に照らした 記述内容の見直し**	**有**	2	CSIRTの整備に係る調査及び検討	有
3	**システム障害に関するリスク管理態勢**	**有**	3	関連法制の動向を踏まえての対応	無
4	**東日本大震災を踏まえた安全対策基準の検証**	**有**	4	PCIDSS(Ver2.0)と安全対策基準とのギャップ分析	無
5	**スマートフォンのセキュリティ**	**有**	5	関連ガイドライン等の最新動向を 踏まえての対応	無
6	**NISCの「安全基準等」への対応**	**無**	6	暗号関連（電子政府推奨暗号リストの改訂）	無
7	**通信技術の動向への対応**	**有**	7	事故犯罪事例に係る調査及び検討	無
8	**外部委託管理（オフショア開発）**	**無**			

以下は今回の改訂の主要テーマの中で取り上げられた特徴的な項目である。改訂の例として次の項目の取り上げ考え方を紹介する。詳細は配布資料を参照願いたい。

1．クラウドサービスを対象とした安全対策基準の対応付け

(1)検討の背景
①金融機関のクラウドサービスの利用にあたっては、従来のシステムとは異なる様々なリスクが懸念されている。
クラウドサービスの利用は、金融機関においても個別業務システムの分野では、既に普及段階に入りつつある。
一方で、基幹系システムや個人情報を扱うシステムへの適用については、従来のコンピュータシステムとは異なる様々なリスクが懸念されており、そのメリットには魅力を感じつつも、導入に踏み切れないでいる金融機関等もあるものと思料された。
②今後の安全対策のあり方の検討
以上のような背景のもと、金融機関等におけるクラウドサービスの利用の現状を踏まえ、セキュリティに関する懸念及び対策、関係法令や各種ガイドライン等について幅広く調査分析を行った。
調査の結果として「顕在化している課題・問題点」が散見されたことから、その課題・問題点について FISC 安全対策基準への反映の必要性も含め、検討することとした。

(2)検討内容

FISC安全対策基準の対象に関する基本的な考え方（本基準の対象）
1　顧客にオンラインサービスを提供するコンピュータシステム
2　他の金融機関等との決済業務に使用するコンピュータシステム
3　顧客データを扱うコンピュータシステム
4　サービスを提供するために金融機関等が顧客に提供するハードウェア・ソフトウェア
上記以外の主要なコンピュータシステムについては、主管部門を問わず、各金融機関の業務の実態に即して、本基準を適宜取り入れる。

（3）検討の経緯

①クラウド利用状況調査として金融機関等及びクラウド事業者にクラウドサービスの利用状況のヒアリングを実施した結果、 以下のような課題・問題点が明らかとなった。

分類	課題・問題点（主なもの）
契約・SLA	契約書チェックが疎か、SLAの扱いが区々
セキュリティ	外部にデータを預けることへの不安
内部統制	クラウドが外部委託契約ではないという認識
監査	データセンターの所在を開示しない例

②同課題・問題点に対するFISC安全対策基準上の管理の考え方と、該当する基準項目を整理した。

③改訂の要否及び内容の検討

該当するFISC 安全対策基準の改訂の要否を検討し、さらに、改訂が必要となる事項をどのような形でFISC 安全対策基準に盛り込むのかを検討した。

（4）主な論点

①委託契約ではないクラウドサービスの利用も外部委託に相当するのか？

実態として業務を委託していれば、外部委託に該当する。他の外部委託と同様に適切な外部委託管理が必要。

②クラウドサービスを利用している業務のうち、検討の対象とするのはどの業務か？

「FISC安全対策基準の対象に関する基本的な考え方」で対象としているものとする。

③今回の検討はクラウドサービスに関するリスク全般を網羅していないのでは？

今回の検討対象は、調査によって明らかとなった「既に顕在化している課題・問題点」について

検討したもの。

④参照の利便性を考慮すべきでないのか？

対象となる基準項目を各々改訂するのではなく、基準を新設し、必要事項をまとめることとした。ただし、既存の基準項目についても、必要に応じて参照することとする。

（5）検討結果

クラウドサービスに関し、「既に顕在化している課題・問題点」について、対応が必要な項目をまとめ、基準項目を新設

した。
なお、クラウドサービスについては、今後も引き続き検討を行う予定である。

新設基準

【運108】クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。

主な内容	狙い
クラウドサービスの利用にあたっては、**外部委託管理**の考え方に準じて適切なリスク管理が必要	クラウドサービスの利用は業務の外部委託であることの明確化
契約には、クラウド事業者との間の**管理境界・責任分界点**に関する取り決めを盛り込むこと	利用者・事業者双方が責任をもって管理する範囲の明確化
本基準項目で参照していない基準についても必要に応じて参照すること	当基準だけを参照すれば良いということではないことの明確化
参照基準に「委託契約」の文言がある場合、サービスを利用するための契約に読み替えて参照すること	契約形態に関わらず外部委託管理が必要であることの明確化

2. セキュリティ脅威の実情に照らした 記述内容の見直し
(1)検討内容
安全対策実施状況調査の結果から浮き彫りになったセキュリティ脅威等として次がある。
① 本人確認機能における認証方式
② 標的型攻撃に対する対策の有効性
③ 各種法改正の動向

(2)主な論点と検討結果
今回の改訂においては、特に、預金等の不正払い戻しが発生している「個人顧客を対象とする」「インターネットバンキング」に限定して、認証方式を強化するよう記載することとする。
改訂基準として、運用項目1件、技術項目3件の改定を行った。

3. システム障害に関するリスク管理態勢
(1)検討の経緯
金融庁の監督指針、金融検査マニュアル等の改正に伴うFISC安全対策基準の十分性の検証及び改訂の必要性の検討を行った。そのギャップ分析の結果、次のような改定を行った。

(2)検討結果

主な改訂基準	内容
【運1】セキュリティ管理方法を具体的に定めた文書を整備すること。	セキュリティ関連文書の策定にあたっては、**経営層が指示し、承認すること**とした。

3】セキュリティ管理体制を整備すること。	体制の確立にあたっては**経営層が指示し、承認すること**とした。
【運62】関係者への連絡手順を明確にすること。	重大な障害、災害については、**想定される最大リスク等を含め**、経営層への報告を適宜行う必要があるとした。
	障害・災害時の連絡、召集対象に**「重要なシステムを委託している外部委託先」**を追加した。
【運90】外部委託における業務組織の整備と業務の管理、検証を行うこと。	委託先の業務の点検または監査の結果として認識した問題点について、**「その影響度に応じて、経営層へ適切な報告を行う必要がある」**ことを追記した。

4．東日本大震災を踏まえた安全対策基準の検証

（1）主な論点

①非常時のコンピュータシステムの継続稼働については、自家発電装置の稼動時を想定した記載が必要ではないか？

非常時に備えた自家発電設備の定期点検の内容として、「燃料容量や冷却水の確保による、非常時の運転可能時間」を考慮することが必要であるとする。

②障害時・災害時の連絡手順を定めるにあたって、通信途絶時等の対応を考慮すべきではないか？

通信途絶時の対応例として、災害時優先通信を連絡手段の例に含めることとする。

③外部委託契約の締結について考慮点を記載すべきではないか？

目標復旧時間やSLAどおりに委託業務を遂行できない場合の対応策を事前に考慮しておくことが望ましいとする。

④障害時・災害時の復旧手順を見直すべきではないか？

バックアップシステム（バックアップサイトを含む）への切替え時の社内システムへの影響確認、切戻しについての考慮が必要であるとする。

⑤バックアップサイト保有の必要性について、より一段高いレベルの記載が必要ではないか？

資金決済等の重要なシステムについては、原則としてバックアップサイトを保有することが必要であるとする。ただし、保有しない場合は、代替手段について経営層による承認を必要とすることとする

その他、つぎの主要テーマ（P2に表示）についても説明がなされた。（記録は省略）

5.スマートフォンのセキュリティ

6．NISCの「安全基準等」への対応

7．通信技術の動向への対応

8．外部委託管理（オフショア開発）

なお、Q&Aについては第2部　5項に記載

＜第Ⅱ部＞

テーマ:『金融機関等におけるコンティンジェンシープラン策定のための手引書』の改訂に伴う
追補版について　（東日本大震災の教訓を反映）

1. 発刊の経緯

『コンティンジェンシープラン策定のための手引書（第3版追補2）』発刊の目的

平成 23 年3月の東日本大震災の経験を踏まえ、わが国全体として防災・減災対策への関心が大きく高まっており、この経験を将来へ向けた貴重な教訓として役立てていこうとする動きが活発化している。

当センター（FISC）では、「東日本大震災影響調査プロジェクトチーム」を設置し、東日本大震災によって金融機関等が受けた被害や対応状況などの事実関係、その後に金融機関等で検討された諸施策などを調査し、今後の業務継続態勢に関する論点について整理を行い、機関誌などで報告してきた。

機関誌に掲載の震災レポート

「東日本大震災における金融機関等の対応状況について」『金融情報システム』平成24年春号
「東日本大震災を踏まえた業務継続態勢整備の方向性」『金融情報システム』平成24年秋号

また、上記の震災レポートの他、第1部で説明した「安全対策基準改訂に関する検討部会」における2つの検討テーマ（「システム障害に関するリスク管理態勢」「東日本大震災を踏まえた安全対策基準の検証」）における検討結果も合わせ、金融機関等が有効に活用することを目的として、『金融機関等におけるコンティンジェンシープラン策定のための手引書（第3版）』（『コンテ手引書』）の『追補2』を発刊した。

今回の改訂により、『コンテ手引書』の構成は次のようになる。

第3版 ＋ 第3版追補 ＋ 第3版追補2

2. 改訂の概要

今回の改訂は、東日本大震災の影響をテーマとし、『震災レポート』の内容と他団体等のガイドライン等とのギャップ分析結果をもとに行った。

《検討テーマ》

（1）震災レポート

（2）他団体等のガイドライン等とFISCガイドラインとのギャップ分析

《改訂の範囲》

『コンテ手引書』 の各編	改訂のポイント	『コンテ手引書』との関係
第1編	改訂の背景や事業影響度分析の考え方を追記	読替え
第2編	「3. 本手引書の構成」について全体の構成を追記	読替え
第3編	「停電対策」「関連先の考慮」「業務継続態勢整備」「経営層の関与」「障害対応」について更新・追記	読替え

第4編	「バックアップサイトの実効性」「関連先の考慮」「業務継続態勢整備」「長期間拠点使用不可リスク」「帰宅困難者対応」「障害対応」について更新・追記	読替え
第5編	「障害対応」「具体例」について更新・追記	読替え
第6編	自然災害以外のリスク 「障害対応」「具体例」について更新・追記	読替え
第7編	資料編として、『震災レポート』2編と事業影響度分析の手法に関する国内外の動向を調査したレポートを追加	追加

3. 改訂内容の紹介

主な改訂内容について、以下に紹介する。

(1)策定にあたって

① 検討内容

『震災レポート』にて紹介した事業影響度分析(BIA)の考え方は、新たな考え方として、今後のコンティンジェンシープラン策定に際し有効な考え方であるため、『コンテ手引書』のプロセスに影響を与えず、この考え方を紹介するため、第1編に記載することを検討。

② 検討結果

コンティンジェンシープラン策定のプロセス説明の中で、リスク洗い出しの際の新たな視点として、重要業務が停止した場合のリスクを先に考える事業影響度分析の考え方を追記した。

(2)緊急事態 (リスク) の洗い出し

① 検討内容

・外部委託先との契約の際、不確実性の想定についての追記を検討

・停電の影響が長時間、断続的、広範囲におよぶ場合の追記

② 主な論点

・緊急事態(リスク)の考慮について、一定の地域への立入禁止リスクなども明記すべきではないか？

③ 検討結果

・緊急事態(リスク)が長時間、広範囲にわたる場合の考慮として、計画停電だけでなく、コンピュータセンター等が立入禁止になる場合などを、例示として追記

・緊急事態(リスク)発生時に外部委託が契約どおりに対応できない可能性の考慮を追記

(3)緊急時対応策の骨子の決定

① 検討内容

・外部委託先のサービス供給が不可能である場合の考慮の追記を検討

・目標復旧時間の検討について追記を検討

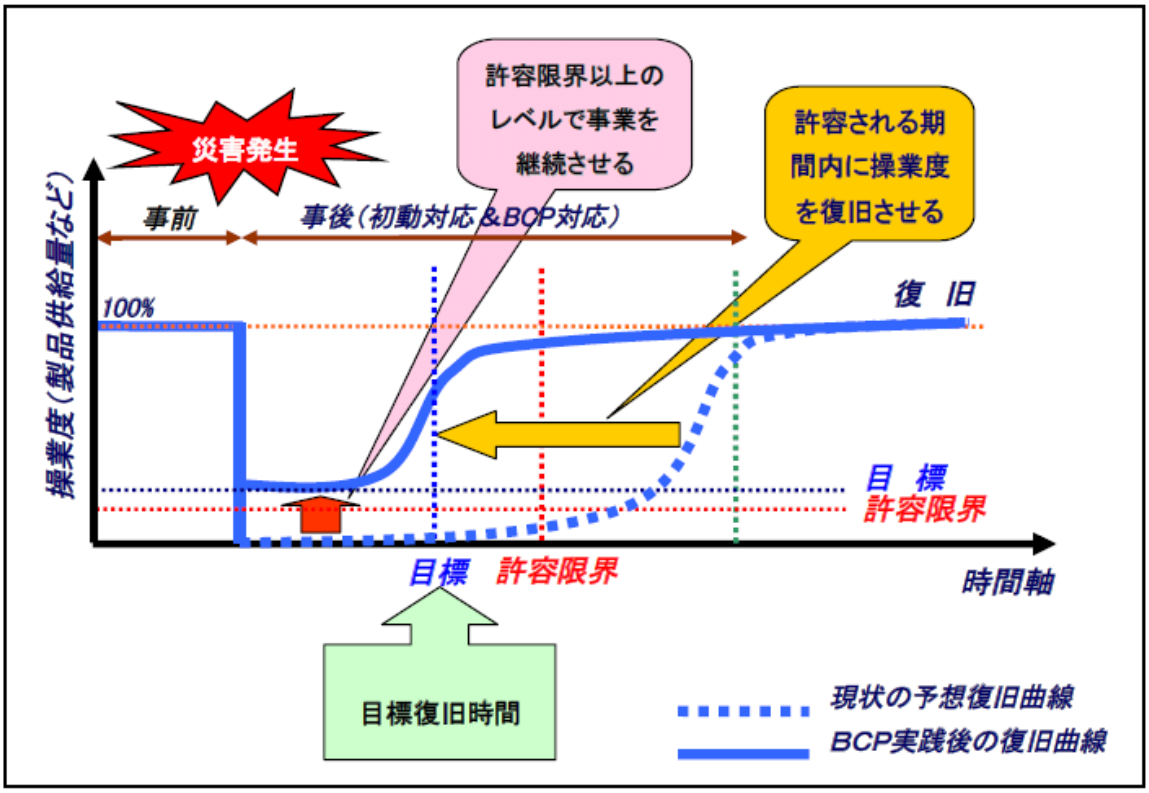
② 検討結果

・外部委託先に依存する代替手段が機能しなくなる可能性の考慮を追記

・業務の目標復旧時間の設定検討について追記

・業務の目標復旧時間のイメージ図について追記

図表２　事業継続計画（BCP）の概念



（内閣府編「事業継続ガイドライン　第二版」（平成 21 年 11 月）をもとに FISC にて作成）

(4)コンティンジェンシープラン策定の基本方針の決定

① 検討内容

・経営層がコンティンジェンシープランの重要性を認識することについて追記を検討

・経営層がシステムやシステムリスクを把握していることについて追記を検討

② 検討結果

・経営層がコンティンジェンシープランの基本方針決定（承認）する際のシステムリスク認識について追記

・コンティンジェンシープラン更新を経営層が承認する際、状況変化に応じてシステムリスクなどが見直されていることを確認することを追記

5. 質疑応答　（鬼頭氏、西村氏により回答を頂いた。）

(1)質問1　安全対策の改訂　配布資料　第1部　P12

「クラウドサービスを対象とした安全対策基準の対応付け（3／5）」

＜質問＞

クラウドサービスを利用する際に監査がしづらいという話があった。実際現場で悩ましい問題である。大きな

クラウドサービス事業者には実質的認証があったりする。それで監査を省略できるか、信用できる会社との契約を締結するなどが考えられる。これについて、ガイドラインなどの議論があるのか。

＜回答＞

今回の改訂においては、クラウドサービスの利用について、外部委託の範疇と捉えられることから、監査は外部委託同様に必要であるとしている。

クラウドサービスの利用についての課題は、今後も出てくると認識しており、今後も継続的に検討が必要と考えている。

(2)質問 2　安全対策 配布資料 P24 (当記録P5 参照)

「システム障害に関するリスク管理態勢」において、〔運1〕〔運3〕。

＜質問＞

“経営層が指示し、承認すること とした。”とある。

リスク管理態勢をボトムアップからトップダウンにしたとのことである。主旨は分かるが、“経営層が指示し”は、それが出来ていると想定しているのか、あるいはあるべき姿としているものか。

＜回答＞

“経営層が指示し”の主旨は、大規模システム障害が発端になっている。

内容についてリスク管理態勢は経営層が主体的にやらなければならないという認識であり、それがあるべき姿であると考えている。

(3)質問 3 「コンテ手引書」 配布資料　P40

「緊急時における要員確保について」

＜質問＞

“緊急対応する代替要員を検討することも望ましい“と記載されている。

大規模災害では、キーマンが被災することもありうる。

考え方としてキーマンの代替の考え方は分かるが、現実的に考えられるか疑問。

＜回答＞

議論の中で代替要員を確保することは、目指すべき姿としてあげた。

現実には難しいこともあるが、目指すべきは、一人の人が欠けて業務が止まることが無いように、事前に準備をしてもらいたい、というのが主旨である。

(4)質問 4　安全対策　配布資料 P30

「東日本大震災を踏まえた安全対策基準の検証(4／5)」

＜質問＞

バックアップ体制については、以前は60Km ほど離れていれば OK という記述があった。広域災害が起こったことを踏まえてどれくらい離れていれば OK であろうか。

＜回答＞

相当以前の安全対策の中には、距離60Km 離れていればという記述があったが、現状は距離の記載はない。

今回の大規模災害でも関西や九州は被害が無かったことを考えると、距離は離れていたほうが良いが、中央防災会議などでも一概に安全な距離というものはないとしているため、各種リスクをメインサイトとバックアップサイトで共有しないようにするという観点で、できることを行う必要がある。例えば、管轄が違う電力会社や地域にサイトを持つといったことも考えられる。また、バックアップサイトを保有することは原則であるが、保有すること自体が現実的ではない場合、代替手段をいかに確保するかを、予め検討して先に取り決めしておくことが重要である。

＜記録者の感想＞

非常に盛り沢山の内容を短時間に報告・説明していただいた。配布資料は細かく丁寧に作成されているので、資料だけでも参考に出来るようになっているのは大変ありがたい。

その中で考え方がきちんと表現されていることは参考になる。われわれはよく理解しておきたいものである。また、短時間であったが、質疑応答でシステムの管理者や監査人から見ての疑問が出され、まだこれからの検討課題であることや、今回の改訂の考え方が回答されて意義深いものになった。

講師としてご来場を頂いた西村部長、鬼頭総括主任研究員、岡田主任研究員の皆さんには、深くお礼を申し上げます。有難うございました。

以上

■ 第 182 回月例研究会報告

日時:2013 年 6 月 17 日(月曜日) 18 時 30 分～20 時30 分

場所:機械振興会館　地下 2 階　ホール

演題:「個人情報影響評価 PIA の要諦とシステム監査との関係」

講師:公立大学法人首都大学東京　産業技術大学院大学

教授　瀬戸洋一　氏

報告者 Ｎｏ．1186　宮下重美

1. 講演要旨

プライバシーなど個人情報を利用するシステムの構築にあたり、プライバシーリスクを事前評価することにより、適切なコストで安全なシステムを構築することが可能である。プライバシーリスクの事前評価に関する世界的な規準としてプライバシー影響評価(Privacy Impact Assessment)がある。保護対象とするデータは機微情報だけではなく、いわゆる個人情報であるため、日本や韓国では、個人情報影響評価(Personal information Impact Assessment:PIA)と呼んでいる。本講演では、プライバシー影響評価、個人情報影響評価の2つの言葉を同じ意味で使う。一般的な専門用語として利用する場合はプライバシー影響評価、日本や韓国における状況の説明の場合は個人情報影響評価と使い分ける。

個人情報保護の体系的な対策としてプライバシーバイデザイン(計画的なプライバシー対策)PbD のコンセプトが提案されている。この PbD における PIA の位置づけを明確にし、システム監査との比較における PIA の要諦を紹介する。

なお、項目構成は次のとおりである。　　(講演資料の項番を詳細化し、項目を再設定している)

(1)はじめに　(2)個人情報漏えいの状況
(3)PIA の対象とする個人情報　(4)プライバシーバイデザインの考え方
(5)プライバシー影響評価　(6)個人情報影響評価の手順と手法概要
(7)プライバシー影響評価の事例　(8)個人情報影響評価実施の効果
(9)日本における個人情報影響評価 PIA の制度化と展開　(10)個人情報影響評価 PIA と監査の相違
(11)国際規格 ISO2230 は PIA とプライバシー適合性監査の両方へ適用できるか？

2. 講演の内容

(1)はじめに

例えば、原子力発電所の建設を考えてみよう。建設にあたり、「環境影響評価」を実施し、問題なければ建設できる。しかし、形骸化した環境影響評価がなされておれば危険なことになり、これら建設費、廃炉費用などを国民が負担することとなる。

PIA も同様に、PIA を実施することは容易であるが、効果あるように(形骸化しないように)実施することが難しい。

(2)個人情報漏えいの状況

個人情報漏えい事故の発生状況は、JNSA 資料によれば、個人情報保護法実施以来、減少しておらず、年間発生件数は数百件、想定損害賠償額も数百億円台である。発生業種も多岐にわたっており、大きな問題を抱えている、といえる。

(3)PIA の対象とする個人情報

PIA の適用範囲を考える際に、個人情報法保護法でいう個人情報、プライバシーを問題にする機微な個人情報などがあるが、PIA の対象範囲とする個人情報は、いわゆる広義の個人情報とする。

(4)プライバシーバイデザインの考え方

1)プライバシーバイデザインの定義

・プライバシーバイデザイン(「計画的プライバシー対策」)は、プライバシーリスクを最小限にするための原則をいう。

・定義は、『システムの開発・運用においてプロアクティブ(proactive:事前)にプライバシー対策を考慮するというコンセプトであって、企画から保守段階までのシステムライフサイクルで一貫した取り組みを行うこと』となる。

(カナダオンタリオ州のプライバシーコミッショナー:Ann Cavoukian 博士が 1990 年代に提唱)

2)プライバシーバイデザインのコンセプト

ユーザプライバシーの尊重を基本として、計7項目で構成する。

・プロアクティブ(事前)　・デフォルト設定でプライバシー

・設計時に組込むプライバシー対策

・ポジティムサム(セキュリティ対策とプライバシー対策においてゼロサム的なアプローチではなく、すべての正当な利益をポジティブサムの方法で対応する)

・end to end ライフサイクル　・可視化と透明性

3)プライバシーバイデザインの適用事例

・適用領域としては、情報技術、組織、社会基盤などにわたる。

・例示すれば、監視カメラ(Video Surveillance)、空港における全身スキャニング(Whole Body lmaging)、RFID タグなどの各種プライバシー対策がある。

4)プライバシーデザインの実施方法

・プライバシーデザインは、総合的なプライバシー対策であり、企画・設計・開発・運用のフェーズで、システム・組織面から実施するものである。

・PIA(個人情報影響評価)は ISO22307 をベース(国際標準適合)とすることが適切である。

5)企画構築と運用におけるプライバシー対策の必要性

・プライバシー対策の基本は、構築と運用で考慮する必要があり、その具体的手法が PIA である。

・企画設計段階で PIA を実施し、包括的なプライバシー問題を事前に把握し、考えうる対策をたてる。

・技術で安全は確保できても、安心は確保できない。包括的技術対策および情報提供者の信頼を得るのが PIA である 。データ提供主体、システム運用者など、ステークホルダーの合意形成を行う。

・運用においては、P マークなどの制度を利用し、運用者自身から生じるリスクを低減する。

(5)プライバシー影響評価

1)プライバシー影響評価の概要

プライバシー影響評価とは、個人情報に関するリスクアセスメント手法をいう。

「個人情報の収集を伴う新たな情報システムの導入にあたりプライバシーへの影響度を"事前"に評価し、その回避、または、緩和のための法制度・運用・技術的な変更を促す」ための一連のプロセス をいう。

プライバシー影響評価の確立とその流れを概観すると、次のとおりであるが、各国の社会的背景、事情、法的手段等により、その内容は必ずしも同一とはいえない。

・1990 年代後半に体系化が進められ、2008 年に国際標準規格を発行した。(ISO22307)

その後、各国の個人情報保護監督機関や行政機関が、各国事情に応じたガイドライン等を公表 している。

・オーストラリア、カナダ、香港、アイルランド、英国(英国連邦)、米国などで利用されており、これらの国では政府機関で義務化している。

・医療やバイオメトリクスなどを利用する民間企業でも義務化されている

・EU のプロジェクト SAPIENT(防犯カメラ)は PIA を実施した。

EU では、バイオメトリクスなど個人情報を扱うシステムの構築に際し、2011 年にプライバシー影響評価 PIA のフレームワークを用いることを endorse(承認)している。

・「プライバシー 影響評価」は「環境影響評価 EA(日本)」と対比するとアナロジーが存在する。

・国際標準規格(ISO22307)はフレームワークだけであるので、現在、SC27 では、PIA のメソドロジーの標準化の議論が進んでいる。(ISO29134　WD の段階)

2)プライバシー影響評価の目的

①個人情報を運用するシステムに対して、個人情報提供者(データ主体)の「プライバシー」に与える「脅威」(リスク)を測定・評価し、その結果から

・「プライバシー」リスクの低減に有効な情報を見出す

・この情報にもとづき、事業・施策システム設計・調達などに必要な具体的提案(改善案)を選出する

・個人情報運用システムの透明性を確保し、システム運用者とデータ主体の間の信頼関係形成を支援する

②事前対策を促すという実質的な意図もある。

3)日本におけるプライバシー保護に PIA が必要な理由

事業者を対象とする事後措置的な行政法である「個人情報保護法」と「プライバシー保護」とは補完関係にあり、対象が少人数(例えば一人)でも、「利用者の重要なプライバシーを適正に保護する」ものが PIA である。 また、PIA は、

ステークホルダーとの問題の共有化を可能にしている。

4)プライバシー影響評価の構成

法律・ガイドライン・契約上のポリシー・国際標準などをインプットとして、次の3項目で構成している。

①プライバシーフレームワーク

・法的側面　　・プライバシー要件とプライバシー測定条件の定義

②プライバシーアセスメント

・運用上の側面　・分析とチェックによる問題抽出

③プライバシーアーキテクチャー

・技術的な側面　・抽出された問題に対する技術的対応 PET(Privacy Enhancing Technologies)

5)プライバシー影響評価に関する各国の状況

①世界各国の PIA を「法律・ガイドライン・ポリシー」「独立検証機関の有無」「実施主体」「行政法との位置づけ・予算承認など」の観点からみると、それぞれ状況が異なる。

②日本のマイナンバー法(通称)を見ると次のとおりである。

・法律等　　:「行政手続きおける特定の番号を識別するための番号の利用等に関する法律」で、特定個人情報に関連するシステムについて情報保護評価の実施を義務付ける

・独立検証機関:行政分野では三条委員会を設置

・実施主体　　:行政機関および一部民間企業・団体

・備　考　　:行政分野の三条委員会では情報保護評価報告書の承認を行う。不適切な場合は、システムの接続運用を拒否することで実効性を担保する。また、評価結果は公開とする。

(詳細については「別紙」参照)

③国際標準規格 ISO22307 の要求事項

米国の提案により、2008 年に国際規格が策定され、要求事項のみ明確であるが、具体的手順等は実施者に委ねられている。

＜手順概要＞

・PIA 計画:PIA の適用範囲を定義、適用される法令・規格を特定、対象システムを調査

・PIA 評価:個人情報の業務プロセス分析、データフロー分析、PIA 報告の結論と勧告を作成

・PIA 報告:評価・分析した事項を文書化、報告書を関係者間でレビュー

＜実施体制＞

・十分な専門知識　:PIA 実施者は必要な専門知識を持つメンバーを選定する必要性

・独立性と公共性　:対象システムに関する利害関係に対する中立性の確保を行う必要性

・意思決定の際の利用:PIA の実施結果を、対象システムの意思決定を行う際に利用する必要性

④日本における個人情報影響評価 PIA 実施フレームワークとその整備状況

日本では、現在のところ、民間利用も考慮した、PIA 実施に関する法律がなく、コモンロー、社会制度でもないが、国際標準規格 IS022307 のフレームワークに準拠することが適切である。

なお、マイナンバー法で特定個人情報の PIA を義務付けた。

・PIA を具体的に実施するために、国際標準 ISO22307 に準拠した体系(ハンドブック、マニュアル)が、産業技術大学院大学:瀬戸洋一教授により提言されている。

マイナンバー法における PIA については「情報保護評価ガイドライン(案)行政機関用」等が作成さ

れている。

・今後、関連するシステム開発にあたっては、PIA 評価チーム、実施依頼組織が参照すべき「分別マニュアル（マイナンバー：行政、医療、金融等）」を策定することが必要である。

⑤日本における PIA 実施体制

・公的分野の実施根拠は「法律」「予算承認との関連あり」、基準による「監査的要素」があり、公開性を求めている。

・公共性の高い事業分野、民間分野の実施根拠は「ガイドライン」等が想定され、公共性の高い事業分野から民間分野になるに従い、「コンサル的な要素」が強く、非公開である。

（6）個人情報影響評価の手順と手法概要

産業技術大学院大学：瀬戸洋一教授により提言している以下の方法を紹介する。なお、我が国では唯一の PIA 手法である。

1）個人情報影響評価の手順(ガイドライン)

①予備評価：プロジェクトにおける個人情報の取得・利用・開示の実施の有無を評価して、PIA が必要かどうかを判断。例えば、行政では、PIA 実施時の予算措置のために必要である

②プロジェクトの記述：プロジェクトの目的と個人情報の取扱いの有無を含め、プロジェクトの概要を記述する

③情報フローマッピング：プロジェクトにおける個人情報の取扱いの流れを記述し、マッピングする

④個人情報影響評価：プロジェクトがどのように個人情報に影響を与るかを特定、分析する

⑤プライバシー管理：特に、プロジェクトの目標を達成する一方で、個人情報への影響を改善する代替的な選択肢を検討する

⑥勧告(PIA 報告書作成)：上記の情報と勧告を含む最終 PIA レポートを作成する

2）個人情報影響評価におけるリスク分析の位置づけ

・各国の PIA の現状を調査すると、リスク分析手法が明文化されていない。このため、PIA におけるリスク分析の位置づけを明確にした「PIA のリスク分析手法」を検討し開発・公開している。

・従来は、参考規程類（法令、ガイドライン、社内規程）から「評価シート（要求事項）」を作成し、PIA の対象となる技術設計（評価対象文書：システム企画・設計書）を評価し、PIA 報告書を作成し、見直し・改善を図っていた。このため、リスクの洗出しが不明確であった。

・検討後に開発した方法は、技術設計内容を業務処理の流れ（ライフサイクル）にそって、プライバシーリスクを含めリスク分析を実施し「リスク分析表」を作成することとした。

この結果をもとに、「評価シート（要求事項）」と対比して相互に評価を行うこととした。なお、この相互評価については、「双方向ギャップ分析」で後述する。

・これらにより、制度設計を変更する道すじを明確にして、制度・技術両面からの評価・見直しを支援することとした。

3）リスク分析手法の具体的な提案

瀬戸洋一教授は、前記2）項を含めて、次の二つの提案をしている。

①「どのように」（内容）の観点

PMS の発想および ISO31000 のプロセス　→ リスク分析のプロセスを明確化

②なんのために（位置づけ）の観点

リスク分析結果から制度と技術の両面で「双方向ギャップ分析」

→ 制度設計、技術設計の変更を促すルートを明確化

4）リスク分析のプロセスの明確化・・・前記3）①の提案

ISO31000:2009 をもとに、PMSの考え方を踏まえたリスク分析を策定している。その骨子は次のとおりである。

①PIA 計画

②対象システム分析

③プライバシー（個人情報）リスク識別：個人情報の識別、リスクシナリオの識別、計画済み対策の識別

④プライバシー（個人情報）リスク分析：影響度の評価、発生可能性の評価

⑤プライバシー（個人情報）リスク評価：必要なリスク対応検討、プライバシー影響評価

⑥プライバシー（個人情報）リスク対応

⑦PIA 及び対応プロセスの記録

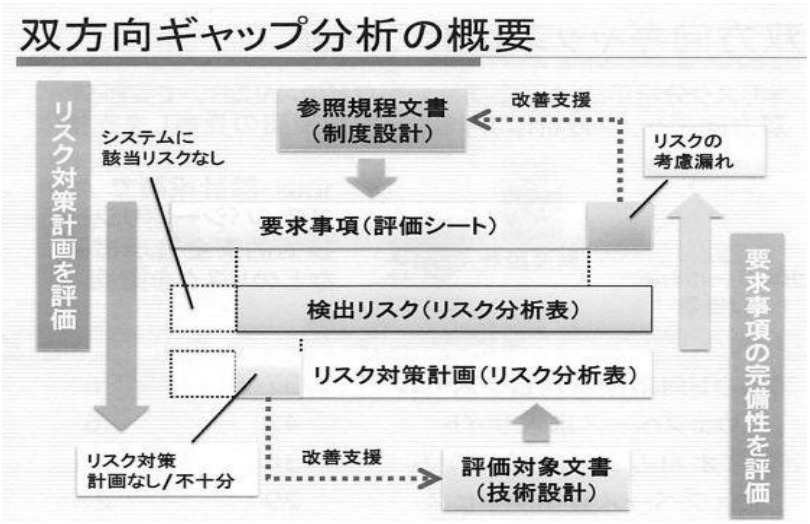
なお、全ブロックと「監視及びモニタリング」「コミュニケーション及び協議」とが連携する。

5)「双方向ギャップ分析」の提案・・・前記3)②の提案

・画期的な手法である「双方向ギャップ分析」により、制度・技術両面の見直しを支援するよう方式を提案する。

なお、具体的な分析は「要求事項（評価シート）」「検出リスク(リスク分析表）」「リスク対策計画(リスク分析表）」で実施する。

（講演会資料抜粋）



・ポイントは、次の点にある。

「要求事項（評価シート）」における“リスクの考慮漏れ”の改善支援　→　要求事項の完備性を評価

「リスク対策計画(リスク分析表）」における“リスク対策計画なし、不十分”の改善支援

→ リスク対策計画を評価、

・提案の「双方向ギャップ分析」については、医療福祉分野などの PIA において検証済みであり、制度・技術両面の見直しの支援を確認し、リスクの可視化ができた。

(7)個人情報影響評価の事例

1)日本における個人情報影響評価の実施実績

・2006 年度官庁の依頼により、入国管理システムで PIA を試行

・2007 年度 SSR 産学戦略的研究フオーラムで日本における実施に関する研究を推進

・瀬戸洋一:「プライバシー影響評価のアセスメント手法に関する調査研究」

（平成 19 年度産学戦略的研究フォーラム海外連携型調査研究、2008 年 3 月）

・2009 年度・民間企業の依頼により、認証サービスシステム関する PIA 実施

・産業技術大学院のプロジェクト「ライブビデオ」に関し PIA を実施

・2010 年度および 2011 年中小企業同友会の依頼により、グループウエアなどのクラウド化に対し PIA 実施

・2012 年度ディジタル健診データ EHR システム（クラウド利用を含む）における PIA 実施。公共機関的なケース、医療的なケースとして注目に値し、関連情報も存在するので、必要に応じて、参照されたい。

2）欧州におけるプライバシー影響評価の概要

・ヨーロッパにおいて、データ保護作業部会 29 条に署名した RFID の PIA フレームワークが企業により開発された。

・EC は、新しいデータ保護法に PIA を含めることとしている。

・EC 委員会の文書 EU(COM)2010/609/EC、4 Nov.2010)では、PIA を個人データ保護における包括的なアプローチとしている。

3）米国におけるプライバシー影響評価の法的な根拠

・2002 年電子政府法第 208 条

事前にプライバシー影響評価を実施することを義務付け、予算を要求するシステムに対する PIA 報告書の写しの提出

・国土安全保障法第 222 条

DHS 省内でチーフプライバシーオフィサーCPO(Chief Privacy Officer)を任命することを義務付け、CPO はプライバシー保護を確立することを保証、CPO は DHS によって実施された PIA を承認する権限をもつ。

・スマートグリッドの PIA に関する文書を NIST が公表している。

4）その他の動向

・国内外で、防犯監視カメラ（痴漢防止カメラを含む）があるが、日本では設置実施の説明責任が不十分なものがある。

（8）個人情報影響評価実施の効果

1）効果的なプライバシー影響評価の概要

①早期における対策により本当の効果が得られる

ステークホルダーへのコンサルテーション　情報フロー分析

②関連する法律への遵守

③プライバシーのリスクと対策

リスク軽減あるいは回避のためのソリューションの一つ

明確な助言が可能であり、構築における計画書(設計書）へのフィードバック

透明性　結果は皆がアクセスできるように公開される

・具体的に、どう役立つか、説明が難しい面もある。

・海外の評価例もあるが、様々であり、明確な評価基準は不明である。

2）プライバシー影響評価の有効性評価における課題

・海外の先行事例では、PIA の有効性を前提とした PIA 報告書に対する評価事例はあるが、フレームワーク自体の有効性評価は存在しない。

・PIA フレームワークの有効性評価のイメージとしては、インシデント発生面から、PIA 実施システムと、PIA 非実施システムとを比較する方法が存在するが、実際的でなく、別の評価指標が必要である。

3）新たな個人情報影響評価の有効性評価方法の提案

次の二指標を瀬戸教授は提案し、評価を実施している。

①プライバシー（個人情報）リスクの可視化

PIA を実施しなければ捕捉できなかったプライバシー（個人情報）リスク、ステークホルダーが見過ごしたリスクを検出できたか

→ 企画・設計段階で、PIA実施により明らかになった不適合事項（件数）を「有効性」を評価した結果、とみなす

②プライバシー（個人情報）保護意識の改善

PIA を実施することで、ステークホルダーのプライバシー（個人情報）意識が改善したか

→ PIA 実施依頼組織のプライバシー（個人情報）保護意識の推移を評価、

10 分野 73 項目の質問を PIA 実施前後に実施し、認識を確認

この際、副次的な効果として、本部と現場との間での意識の乖離が減少、個人情報保護への全社レベルの取組み強化、が期待できる

4）個人情報影響評価の実施効果（まとめ）

①早期に問題を顕現化する。

事後ではなく、事前にプライバシー問題を検知、安全管理策を構築して、必要以上の投資を抑制する。

②プライバシー問題を事後ではなく、事前に明確にする。

③プライバシーのミスによる混乱、あるいはコスト増を避ける。

④プライバシーリスクを防ぐため組織に証拠を残す。（信頼性の低下、ネガティブな評判へのダメージ）

⑤関連する法律への準拠　　⑥リスクマネジメント目標を支援

⑦説明のつく意思決定を強調　　⑧ステークホルダーへプライバシーの重要性を実証する

（9）日本における個人情報影響評価の制度化と展開

・マイナンバー法の実施に伴う PIA 適用については、内閣府からガイドラインの素案が示されている。

・PIA の適合性評価については、国内で JIS 化が必要であり、また、第三者機関での適合性評価の仕組み（認証機関）の検討が必要である。

・PIA に関わるリスク分析手法を提案しているが、この内容を検討し標準化する必要がある。

・PIA に関わる人材育成はその主体、内容など、体系的、体制的な検討が必要である。

民間では、PMS のスキルをもつ者も存在するので、PIA の本質を理解されれば大きな力になる。

・瀬戸教授の大学でも PIA に関する体系・手法検討、標準化、人材育成プログラムの作成など、制度化対応を含めて、積極的な参画をしているので、利用ねがいたい。

（10）プライバシー影響評価と監査との相違　（出典:ISO22307 Q&A より）

①監査は個別的な業務システムの現時点における法律やガイドラインなどのコンプライアンス要件との適合性レベルを判断し、将来的な法律との不適合を回避するためのステップである。

②PIA と監査の類似性は、同様の技能を用い、プライバシー侵害を回避しようとするところにある。

③監査は主として既存システムを対象とし、必要とされるポリシー、規格や法律との適合性を検証するためのものである。

④PIA はシステム開発の初期段階で用いられ、プライバシーに関する最適のオプションや解決策を特定するのに役立つ。

⑤監査の場合は、法律、ガイドラインなどの適合性基準を正しいとして実施するが、PIA の場合は、システムへのリスク分析

により、現在のガイドラインなどのコンプライアンス要件の妥当性評価を行うこと、が大きく異なる点である。

(11)国際規格 ISO22307 は PIA とプライバシー適合性監査の両方へ適用できるか？など

（出典:ISO22307 Q&A より）

①PIA が ISO22307 に従って実施されたと主張するのは適切であるが、適合性監査が ISO22307 に従って実施したと主張するのは適切ではない。なぜならば、ISO22307 はフレームワークのみであり、管理基準が明確化してないからである。

②プライバシー適合性監査が報告書を含むものであった場合は、当該の報告書は次に提案されるシステム変更の PIA において出発点として利用できる。

③ISO22307 において参考情報を提供する付属書一式は、適合性監査の準備する助けとなる。

したがって、適合性監査に報告書の構造を適用し、監査の実施に当たって ISO22307 を適用することは適切である。PIA 報告書の雛型は情報セキュリティ監査の基準に基づき作成しているので理解し易い構成である。

④民間対応の PIA は情報セキュリティ監査における「助言型的な内部監査」に相当し、公共対応の PIA は「保証型監査」に相当すると、ほぼ、理解して良い。

(12)その他

①ハンドブック及びマニュアルの目次、情報セキュリティ監査と個人情報影響評価との対比　が「講演資料」に添付されていた。

②参考となる各種資料は、教員サイトからダウンロード可能であり、「産業技術大学院大学瀬戸洋一」で検索できるので活用して欲しいと、瀬戸洋一教授からアナウンスがあった。

③個人情報影響評価に要する稼働

・システム規模等によるが、中規模で、3－4月、4～5名程度と想定する。

・システム設計段階において、個人情報影響評価は要件定義後に実施する点を考慮すると、1～2月程度で実施することが求められる。

・費用は韓国の事例から想定すると、中規模で 500 万円程度、大規模で 1500～2000 万円程度と考える。

④参考:「マイナンバー法における情報保護評価の概要」を ＜別紙＞ に示す。

3. 質疑応答

(1)PIA の範囲（スコープ）において、非技術的事項である人的、組織的事項（要件）はどう扱うのか

PIA の範囲は（ハードウェアの）システムのみであり、組織などの運用体制等は評価対象としていない。

但し、PIA を実施する際は、制度としての組織のコンプライアンス的なポリシー・規程等は対象としており、助言的な意味合いがある。

(2)PIA における簡易形、詳細形の評価・分析区分について説明ねがいたい

PIA は出来る範囲で実施するとの発想で、コストも考慮して区分している。「簡易形」はテンプレート化されており、システムの上流工程では簡易形とならざるを得ない。この区分は英国の例を参考にしている。

(3)PIA におけるリスク分析について説明ねがいたい

検討当初は「評価シート」の作成に重点をおいたが、リスク分析・評価に苦慮した。プライバシーリスクは、ISMS のような CIA 要素では分析・評価できない部分があるため、PMS の発想に基づく業務のライフサイクル（収集・利用・提供など）の流れに沿って分析・評価することとした。これらを組込んで、制度的法的要素と技術的要素による双方向評価を実施す

る仕組みとしている。

＜双方向評価などについては、3. 講演内容 (6)プライバシー影響評価の手順と手法概要、2)～5)を参照＞

(4)第三者監査と対比し、PIA におけるセルフ評価（プライバシー影響評価）者の有責性はどう考えたらよいか

難しい質問である。私は、PIA 自身の内容に関する責任はシステム構築実施責任者にあると考える。ただし、中立、専門的な立場で本件の適正判断をする CPO(チーフ・プライバシー・オフィサー、プライベート・コミッシュナー)にも責務はあると考えるが、明確なことはわからない。

公共分野の場合は、組織外の第三者としての中立的な立場であり、民間分野の場合は組織内で対応することとなる。従って、民間分野の場合は、PIA 的なもの、コンサル的な立場となるのではないか・・・

(5)スマートグリッドにおけるプライバシー問題とは具体的にどのような内容か？

家族の活動内容がある程度把握できる可能性がある。例えば、何時にどのように就寝するかなども。

是非、電力業界でも取組んで欲しいと考える。学会でも問題提起している。

(6)PIA の人材育成に関わる参考意見をいただきたい

システム監査を実施している技術者が一番近い位置にある。PIA の基本的概念の理解と、手法的なリスク分析について理解できればよい。大学でも育成プログラム案を作成しているので、しかるべきところでブラッシュアップして欲しいとねがっている。当大学での各種実績を活用して欲しい。

(7)効果的効率的な PIA のリスク分析手法はないか？

PIA のリスク分析手法は、PMS的な業務分析を実施し、評価は計数的に実施している。PIA はシステムの基本設計段階で実施する方式であるので、詳細設計段階で実施するほど、工数がかからない、と考える。

詳細設計段階では、CC 認証(ISO/IEC 15408)的な手法を考慮することも方法である。

なお、マイナンバー法による PIA を詳細に実施しようとすると、かなり工数がかかるのかな、との思いもある。

4. 感想

マイナンバー法の成立により、注目されている「個人情報影響評価」について、我が国第一人者である瀬戸洋一教授から、概要、事例、効果について、海外の状況を含め講演いただき、非常に有意義であった。

特に、国際標準規格（ISO22307)のフレームワークを具体的に展開した「PMS の考え方を踏まえたリスク分析」「双方向ギャップ分析」「PIA の有効性評価」、これらをベースとした PIA の実務的な「ハンドブック」

及び「マニュアル」の開発などの情報を開示いただき、あらためて、お礼を申し上げたい。

「個人情報影響評価」が求める技術・スキルという点では、システム監査を実施している者が一番近い位置にあるとのことであるので、私共のミッションを十分認識して、活動機会が得られれば、この上ないことであると考えている。

（完）

＜別紙＞「マイナンバー法における情報保護評価の概要」

1. 情報保護評価について

共通番号制度は、①より公平・公正な社会、②社会保障がきめ細やかかつ的確に行われる社会、③行政に過誤や無駄のない社会、④国民にとって利便性の高い社会、⑤国民の権利を守り、国民が自己に関する情報をコントロールできる社会の実現を目指し、導入されるものである

しかしその一方で、番号制度導入により、国家により個人の様々な個人情報が一元管理されるのではないか、

特定個人情報が不正に追跡・突合されるのではないか、財産その他の被害が発生するのではないかといった懸念が考えられる。

そこで、これらの懸念を踏まえ、国民の特定個人情報が適切に取り扱われる安心・信頼できる番号制度の構築のために、特定個人情報ファイルが取り扱われる前に、個人のプライバシー等に与える影響を予測・評価し、かかる影響を軽減する措置を予め講じるよう、情報保護評価を実施する

情報保有機関は、情報保護評価を実施することにより、特定個人情報ファイルを保有することで具体的にどのようなリスクがあり、したがってどのような措置を講ずるべきかという、個人情報保護及びプライバシー等保護のための具体的な検討・評価を体系的に行うことができる。

情報保護評価を通し、抽象的な検討ではなく、具体的かつ体系的な検討・評価を経た措置を講じることができ、それにより、特定個人情報ファイルに係るプライバシー等に配慮した取扱いを確立することを企図するものである。

2. 情報保護評価の目的

① 事後的な対応にとどまらない、積極的な事前対応を行う

② 情報保有機関が国民のプライバシー等の権利利益保護にどのように取り組んでいるかについて、情報保有機関自身が宣言し、国民の信頼を獲得する

③ 個人番号情報保護委員会が確認を行うことで、①②についての厳格な実施を担保する

3. 情報保護評価の対象者

＜義務付け対象者＞

行政機関の長、独立行政法人等、地方公共団体情報システム機構、情報連携を行う事業者

地方公共団体の長その他の機関、地方独立行政法人

＜非義務付け対象者＞

情報連携を行わない事業者（注記：企業など一般事業者）

4. 情報保護評価の対象・実施の仕組み

・特定個人情報ファイルを保有しようとする前に、情報保護評価を実施する

・特定個人情報ファイルの取扱いを変更する場合は、再度評価を実施

＜対象 ＞

①特定個人情報ファイルを保有しようとする場合は、**しきい値評価**を実施

②しきい値評価の結果、プライバシー等に影響を与える可能性があると認められるもの

⇒ **重点項目評価書の作成・公表**　（概ね、1万人以上、10万人未満）

③しきい値評価の結果、プライバシー等に影響を与える可能性が高いと認められるもの

⇒ **全項目評価書の作成・公表、国民の意見聴取、委員会の承認**　（概ね、10万人以上）

（「情報保護評価指針素案（中間整理）の概要」 内閣官房社会保障改革担当室　資料　から引用）

2013.07 投稿

注目情報 （2013.6～2013.7）

■【警察庁、「サイバー犯罪対策　夏休み特集」公開】

2013 年 7 月 10 日　警察庁

警察庁は、夏休みにインターネット利用が増える小・中・高校の児童とその家族向けにサイバー犯罪に関する注意喚起を公開しました。以下の 3 つ注意と広報啓発用リーフレットを公開しています。

(1)出会い系サイト・コミュニティサイト

出会い系・コミュニティサイトでの犯罪は急増しています。18 歳未満の児童が出会い系サイトを利用することは法律で禁止されています。

(2) 不正アクセス

不正アクセスによるオンラインゲームやコミュニティサイトの不正操作事案が急増しています。ID・パスワードが盗み取られないよう、推測が容易なパスワードの使用を避け、複数のサイトで使い回すことはやめましょう。

(3) スマートフォンの不正アプリ

不正アプリをダウンロードしたことにより、個人情報が抜き取られる事件も発生しています。アプリをダウンロードするときは、信頼できるか良く確認しましょう。

警察庁プレスリリース本文　http://www.npa.go.jp/cyber/summer/index.html

■【IPA「情報セキュリティ対策ベンチマーク ver4.2」と「診断の基礎データの統計情報」を公開】

2013 年 6 月 20 日

独立行政法人 情報処理推進機構

独立行政法人 情報処理推進機構（IPA）は「情報セキュリティ対策ベンチマーク バージョン 4.2」と「診断の基礎データの統計情報」を公開した。

情報セキュリティ対策ベンチマークは、組織の情報セキュリティ対策の取組状況（27 項目）と企業プロフィール（19 項目）を回答することにより、他社と比較して、セキュリティ対策の取組状況がどのレベルに位置しているかを確認できる自己診断システムである。診断時の回答項目は、ISMS(*1)認証基準（JIS Q 27001:2006(*2)）附属書Ａの管理策(*3)をベースに作成しており、ISMS 適合性評価制度を用いるよりも簡便に自己評価することが可能となる。

本システムのバージョン 4.2 では、情報セキュリティを巡る環境変化や対策レベルの変化を勘案し、診断の基礎データを最新 2 年 1 ヶ月分のデータに入れ替えた。また、英語バージョン 4.2 も同時に公開しました。

ホームページ　https://www.ipa.go.jp/security/benchmark/benchmark_20130620.html

2013.07 投稿

【 協会主催イベント・セミナーのご案内（東京開催） 】

■システム監査実務セミナー

今回ご案内するセミナーは、COSO-ERM モデルが提唱する、企業のリスク低減を図るためのシステム監査を目指す、「システム監査実務セミナー」（4 日間コース 1 泊 2 日×2 回）です。

企業の経営戦略及び業務の有効性と効率性の向上を図るためには、情報システムの活用が必須であり、その評価・改善を進めるためには、システム監査を実施することが有効です。

これまで実施されてきた業務監査（システム監査）では、現場の業務評価の視点を重視した監査が多く見受けられています。

今後は、コーポレートガバナンス、内部統制の面から、業務評価の視点に加えて、経営リスクに対する業務システムの有効性、効率性、安全性の向上の観点からの評価・改善提案が重要になってきます。

本セミナーは、当協会のシステム監査事例研究会で実施した、「システム監査サービス」の実際の監査事例を教材として、ロールプレイを中心とした演習ベース のきわめて実践的なコースで、全社的リスクマネジメントの枠組み（①経営戦略への貢献、②業務の有効性と効率性、③報告の信頼性、④関連法規の遵守）に ついてよりよく理解し、経営に役立つシステムの実現に資するシステム監査の方策を理解・修得することを目標にしております。

なお、本セミナーを受講した後、事後課題を提出頂き、その内容が適切であると判断された場合には、当協会が認定する公認システム監査人の認定に必要なシステム監査実務を 1 年間経験したものとみなされます。

また、本セミナーは、IT コーディネータ協会の「専門知識研修コース」(5.5 ポイント相当)に認定されています。

記

1. 日程及び会場

2013 年 8 月 31 日(土)～9 月 1 日(日)

2013 年 9 月 14 日(土)～15 日(日) ＜1 泊2日×2＞ どちらか一方のみの参加は不可

時間：土曜は 10:00～19:30、日曜は 09:00～15:00（進行状況により若干の変更が生じる場合があります。）

会場：晴海グランドホテル　〒104-0053 東京都中央区晴海 3-8-1 電話番号： 03-3533-7111

（最寄り駅 都営地下鉄大江戸線勝どき駅下車徒歩8分）

2. 費用

168,000 円（日本システム監査人協会会員）

189,000 円（一般）　　＊費用には、教材費・宿泊費・食事代・消費税が含まれます。

3. 副教材

情報システム監査実践マニュアル(第 2 版) 森北出版社 5,460 円

4. セミナーの概要

前半2日間 8/31 10 時～19 時 30 分、9/1 9 時～15 時

・システム監査実施手順及びシステム監査技法説明（座学）

・監査依頼者意向確認（ロールプレイ）

・トップインタビュー（ロールプレイ）

・監査テーマ決定（チーム作業）

・監査個別計画作成(チーム作業)
・資料収集の検討(チーム作業)

後半2日間　9/14　10 時～19 時 30 分、9/15　9 時～15 時
・予備調査(ロールプレイ)
・本調査(ロールプレイ)
・監査報告書作成(チーム作業)
・事実誤認有無等確認(チーム作業)
・監査報告会(ロールプレイ)

全 33 時間

教材　金融機関のデータセンターに関する監査

5. 受講していただきたい方

情報処理技術者(システム監査)資格保有者もしくは同等の知識を有する方、または内部監査、システム監査の経験がある方(上記条件に当てはまらない方は、お問合せください)

6. 募集人員

定員20名(最小催行人員10名)

7. 受講申込み等

問合せ先:日本システム監査人協会　セミナー事務局　miwa-toshiya@saaj.jp

受講申込み:http://www.saaj.or.jp/kenkyu/jitsumuseminar22.html　より申込みください。

■中堅企業向け「6ヶ月で構築するPMS」セミナー

個人情報保護監査研究会の中堅企業向け「6ヶ月で構築するPMS」セミナーの開催をご案内します。当研究会では、当研究会著作の規程、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。

詳細は、個人情報保護監査研究会主査　斎藤(saajjk7@saaj.jp)までお問い合わせください。

中堅企業向け「6ヶ月で構築するPMS」セミナー

・基本コース:月 1 回(第 3 水曜日)14 時～17 時(3 時間)×6 ヶ月
・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　茅場町オフィス
・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)
　2013 年 5 月号 SAAJ 会報より、「個人情報保護マネジメントシステム実施ハンドブック」簡易版を公開開始！
・セミナーのお申込が多い場合、最大 6 ヶ月お待ちいただくことがあります。
・基本コースの他に、月 2 回の応用コースなどがあります。

■月例研究会

前述「5．1 システム監査活性化プロジェクト」の「月例研究会の活動紹介」の中でも掲載していますが、7 月および 8 月の月例研究会の開催予定は、以下のとおりです。

2013 年 7 月・第 183 回月例研究会

日　時　　：　2013 年 7 月 24 日(水)18:30～20:30
場　所　　：　機械振興会館　地下 2 階多目的ホール
講演テーマ：　「サイバー攻撃の脅威」(仮題)
講　師　　：　独立行政法人　情報処理推進機構　　渡辺貴仁氏

2013 年 8 月・第 184 回月例研究会

日　時　　：　2013 年 8 月 21 日(水)18:30～20:30
場　所　　：　機械振興会館　地下 2 階多目的ホール
講演テーマ：　クラウドインシデント
・利用者側:攻撃発生事例
・事業者側:標準化、国際動向　(仮題)
講　師　　：　独立行政法人 情報処理推進機構
技術本部 セキュリティセンター　　普及グループ　研究員　河野省二氏

以上

2013.07 投稿

【協会主催イベント・セミナーのご案内（大阪開催）】

■第 38 回システム監査勉強会

1. 日時　　2013 年 8 月 17 日（土）13:00～17:00 場所：大阪大学中之島センター
2. 場所　　大阪大学中之島センター
3. 参加費　　日本システム監査人協会会員 無料、 ISACA大阪支部会員 無料、
両協会の会員以外の方 1,000 円
5. 内容　　2013 年 6 月 17 日の SAAJ 第 182 回月例研究会、及び
2013 年 7 月 24 日の SAAJ 第 183 回月例研究会の DVD の視聴。
テーマ1「個人情報影響評価 PIA の要諦とシステム監査との関係」
講師 首都大学東京 産業技術大学院大学 瀬戸洋一氏
テーマ2「実演によるサイバー攻撃の仕組み解説」
講師 情報処理推進機構 セキュリティ技術ラボラトリー 渡辺貴仁氏
6. 申込方法　　協会ホームページから、お申込みください。
http://www.saaj.or.jp/index.html

■システム監査体験セミナー（実践編）

日本システム監査人協会近畿支部では、システム監査人の実務能力維持・向上のため「システム監査体験セミナー（実践編）」を開催し、参加された皆さまより評価を頂いております。

本セミナーは、システム監査を実際に行う機会が少ない現状において、システム監査技術者や公認システム監査人を目指される方、内部監査ご担当者やシステム監査にご興味をお持ちの方々に、模擬体験を通したシステム監査能力向上の機会をご提供することを目的としております。特に内部監査人養成は企業の内部統制整備に欠かせない要件となっており、この機会を利用した監査実務の体験は短期間での養成に最適と考えております。多くの皆さまの参加をお待ちしております。

記

1. 日時　　2013 年 9 月 21 日（土）10:00～20:00 / 22 日（日）10:00～17:00（宿泊はありません）
2. 場所　　大阪産業創造館 （http://www.sansokan.jp/）
〒541-0053 大阪市中央区本町 1-4-5 大阪産業創造館 13F TEL 06-6264-9800(代)
3. 参加費　　日本システム監査人協会会員　　21,000 円（早期申込割引 16,800 円）
その他の方　　26,250 円（早期申込割引 21,000 円）
4. 定員　　16 名（最小催行人員 8 名）
5. 内容　　当協会が実施したシステム監査サービスを基にしたケーススタディです。セミナー用にアレンジした「システム監査依頼書及び企業情報」を教材 として、4 名前後のグループに分かれて、監査計画書作成から予備調査、本調査、監査報告の実際を体験頂きます。

第 1 日目　10:00～20:00

システム監査実施手順及びシステム監査技法説明（講義）

予備調査インタビュー（ロールプレイング）

監査個別計画書作成、発表（チーム作業）

第 2 日目　10:00～17:00

本調査インタビュー（ロールプレイング）

監査報告書の作成（チーム作業）

システム監査報告会（チーム作業）

講師コメント、監査事例の紹介（講義）

ITコーディネータの方には、ITコーディネータ知識ポイントが3ポイント付与されます

なお、今回のセミナーは、時間を短縮するなど、従来当支部（SAAJ 近畿支部）が主催した実践セミナーとは若干内容が異なるため、当協会 SAAJ が認定する「公認システム監査人」の申請に必要な監査実務の「みなし期間」とはなりませんので、ご注意ください。

以上

2013.07 投稿

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

2013 年の会報の基調テーマは、「システム監査の普及促進」であり、3 か月ごとに「システム監査の普及促進」に関連するテーマを取り上げ、皆様と幅広く深く意見交換していきたいと考えています。

今月号から10月号までの会報テーマは「システム監査の使いみち」です。協会においても、「システム監査活性化プロジェクト」を中心に、システム監査活性化に向けて取り組んでいるところです。会報記事が、協会の部会、研究会、支部など、皆様の活動の場での議論の契機となれば幸いです。

□■ 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を利用してください。会報サイトからダウンロードできます)
2. 会員投稿　(Word の投稿用テンプレートを利用してください)
3. 会報投稿論文 (論文投稿規程があります)

これらは、いつでも募集しております。 気楽に投稿ください。

特に新しく会員となられた方（個人、法人）は、システム監査への想いやこれまで活動されてきた内容で、システム監査にとどまらず、IT 化社会の健全な発展を応援できるような内容であれば歓迎いたします。

次の投稿用アドレスに、テキスト文章を直接送信、または Word ファイルで添付していただくだけです。
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）

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：仲 厚吉、安部 晃生、越野 雅晴、桜井 由美子、中山 孝明、藤澤 博、藤野 明夫
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）
━━